

INFORME DE BLUETEAM

TITULO:
Informe de redes BlueTeam

CURSO:
BlueTeam / Seguridad de la Información

PROFESOR:
Sergio Vilches Puerta

ALUMNO:
Jordan Andres Diaz Sanchez

TABLA DE CONTENIDO

1. Introducción
2. Infraestructura de red
 - 2.1. UTM
 - 2.2. LAN
 - 2.3. DMZ
 - 2.4. DMZ2
3. Firewall
 - 3.1. Reglas WAN - NAT
 - 3.2. Reglas LAN
 - 3.3. Reglas DMZ
 - 3.4. Reglas DMZ2
4. SIEM (Elastic Cloud)
 - 4.1. Políticas e integración (Windows – Honeypot – Suricata)
5. SIEM (Elastic Cloud – Logs)
 - 5.1. Logs (Windows – Honeypot – Suricata)
6. Conclusión
7. Referencias y Bibliografía

1. INTRODUCCIÓN

En este informe se detalla el diseño y la implementación de una arquitectura de red para un entorno de BlueTeam, este entorno esta diseñado para proporcionar capacidades de monitoreo y defensa frente a posibles amenazas cibernéticas, utilizando una red segmentada que incluye las redes LAN, DMZ y DMZ2, interconectadas a través de un firewall Pfsense. Cada segmento de tiene un propósito específico, con dispositivos configurados para enviar registros de log a un servidor centralizado de Elastic, permitiendo la recolección y análisis de datos en tiempo real. Esta arquitectura busca asegurar la integridad y disponibilidad de la red, mientras se supervisan y gestionan posibles ataques.

2. INFRAESTRUCTURA DE RED

La infraestructura de red se implemento utilizando una UTM (unified Threat Management) basada en Pfsense el cual se configuro para actuar como el punto central de interconexión entre las redes LAN, DMZ, DMZ2, cada una asignada con un rango de direcciones IP dinámicas mediante DHCP esta configuración permite una gestión flexible.

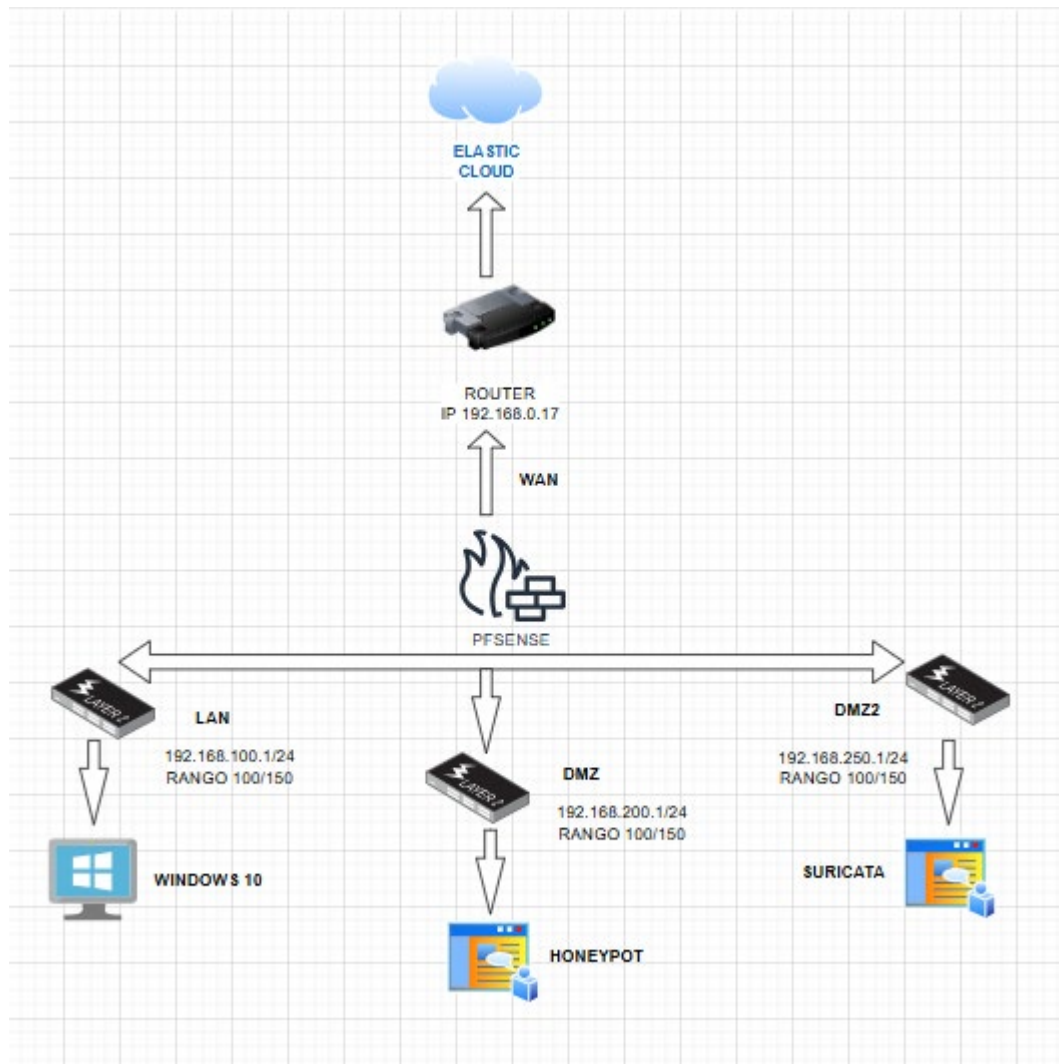


Ilustración 1 Estructura de red

En la red LAN, se encuentra un equipo con Windows 11, configurado para enviar registros al servidor Elastic, que centraliza la recolección y análisis de registros. La DMZ aloja un Honeypot accesible desde la WAN, pero sin acceso a las redes internas, garantizando un entorno aislado para la captura de intentos de intrusión. Por último, en la DMZ2 se implementó una fuente adicional de logs, con opciones como Suricata o Apache Server, para diversificar las fuentes de datos que alimentan el servidor Elastic.

2.1. UTM (unified Threat Management)

El corazón de la infraestructura de red es una UTM (Unified Threat Management) implementada con Pfsense. Pfsense es una solución de firewall de código abierto que proporciona funciones avanzadas de gestión de red y seguridad, incluyendo cortafuegos, VPN, filtrado de contenido y detección de intrusiones.

En esta práctica, Pfsense se configuró para manejar tres redes distintas: LAN, DMZ y DMZ2. Cada segmento está aislado para mejorar la seguridad y se interconecta a través del Pfsense, que actúa como un puente seguro entre ellos. Además, Pfsense administra la asignación de direcciones IP dinámicas a través de su servidor DHCP integrado, asegurando que los dispositivos en cada red reciban configuraciones IP adecuadas sin intervención manual.

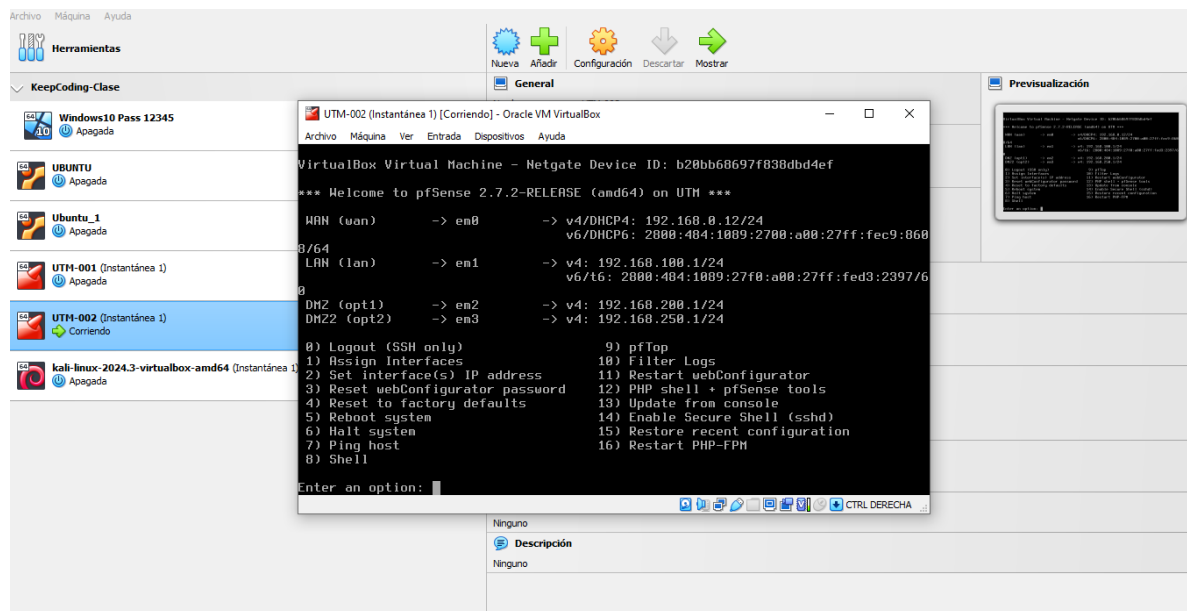
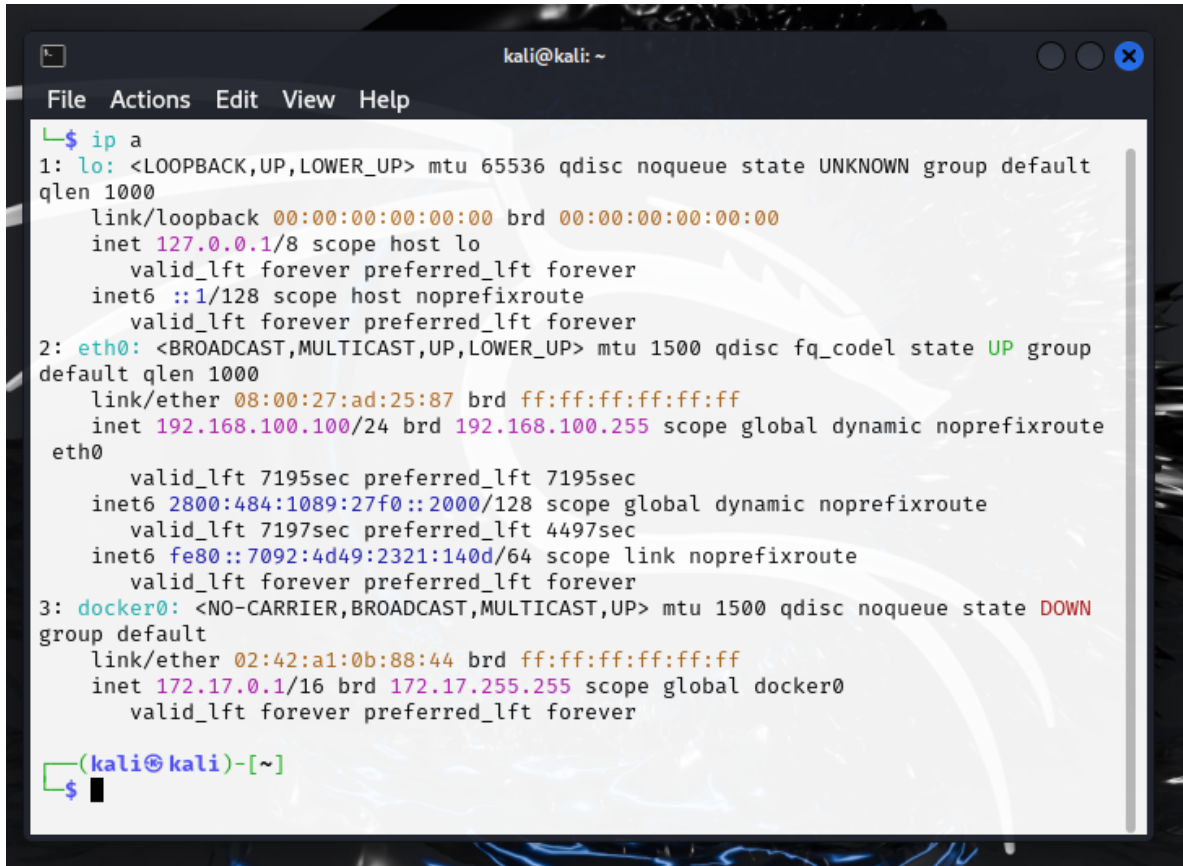


Ilustración 2 UTM-002 Pfsense

2.2. LAN

La red LAN esta infraestructura está diseñada para alojar dispositivos internos, con un enfoque en la seguridad y la facilidad de gestión. En este caso, la LAN contiene un equipo con Windows 11, configurado para enviar registros al servidor Elastic. Esto permite el monitoreo continuo de actividades y eventos del sistema, lo que es crucial para la detección y respuesta temprana a posibles incidentes de seguridad.



```
kali@kali: ~  
File Actions Edit View Help  
L$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group  
default qlen 1000  
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.100/24 brd 192.168.100.255 scope global dynamic noprefixroute  
    eth0  
        valid_lft 7195sec preferred_lft 7195sec  
    inet6 2800:484:1089:27f0::2000/128 scope global dynamic noprefixroute  
        valid_lft 7197sec preferred_lft 4497sec  
    inet6 fe80::7092:4d49:2321:140d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN  
group default  
    link/ether 02:42:a1:0b:88:44 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

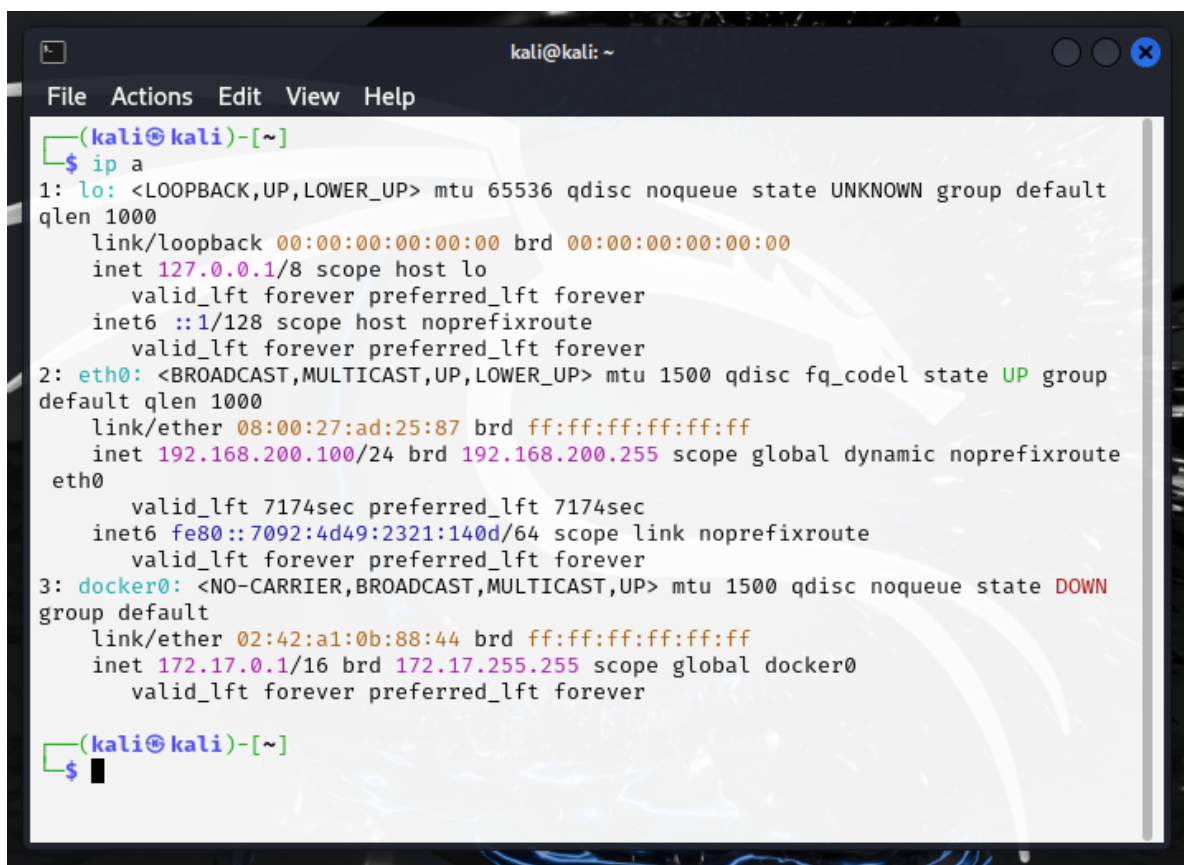
Ilustración 3 Red LAN

Primary Address Pool	
Subnet	192.168.100.0/24
Subnet Range	192.168.100.1 - 192.168.100.254
Address Pool Range	<div>192.168.100.100</div> <div>From</div> <div>192.168.100.150</div> <div>To</div>
The specified range for this pool must not be within the range configured on any other address pool for this interface.	

Ilustración 4 Red LAN rangos

2.3. DMZ

La red DMZ (Zona Desmilitarizada) está diseñada como una zona de seguridad intermedia entre la red interna (LAN) y la red externa (WAN). En esta infraestructura, la DMZ aloja un Honeypot, un sistema que simula ser un objetivo vulnerable para atraer y analizar intentos de intrusión. Este Honeypot está configurado para enviar registros al servidor Elastic, lo que permite monitorear las actividades sospechosas y obtener información sobre posibles ataques.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group  
default qlen 1000  
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.200.100/24 brd 192.168.200.255 scope global dynamic noprefixroute  
        eth0  
        valid_lft 7174sec preferred_lft 7174sec  
    inet6 fe80::7092:4d49:2321:140d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN  
group default  
    link/ether 02:42:a1:0b:88:44 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

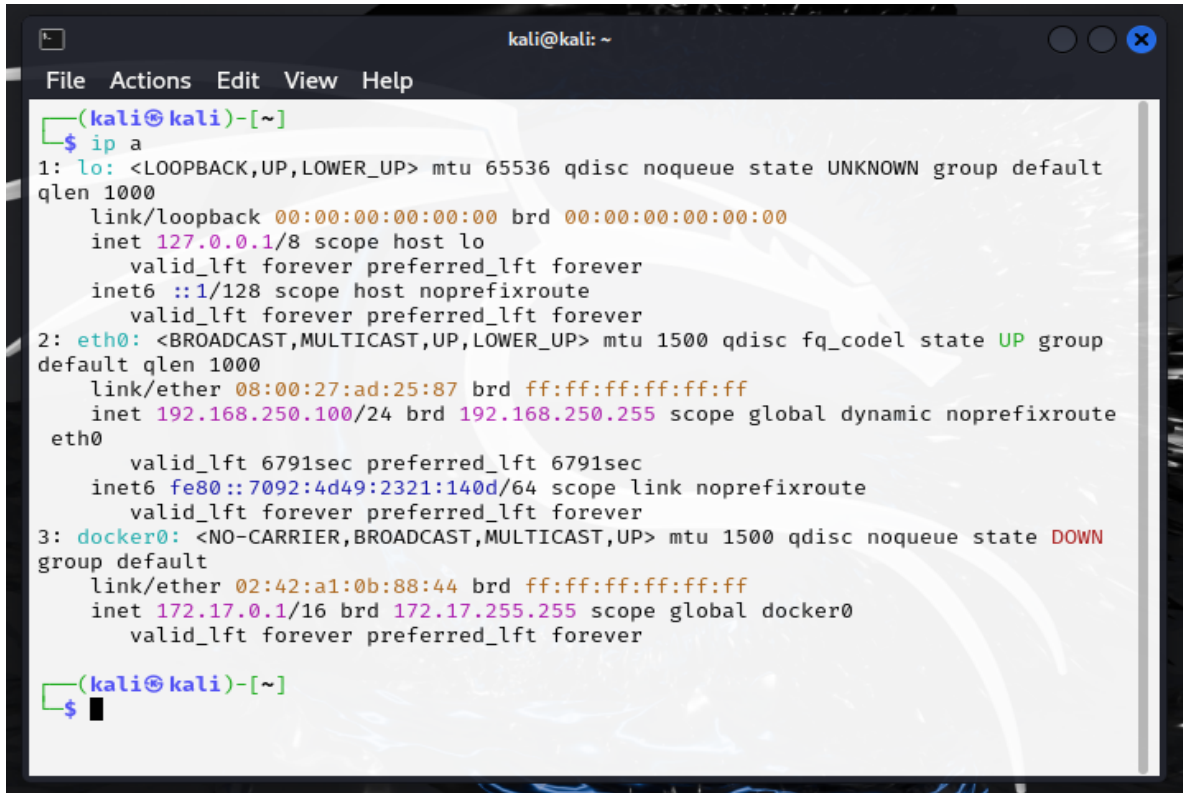
Ilustración 5 Red DMZ

Primary Address Pool	
Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	<div><div>192.168.200.100</div><div>From</div><div>192.168.200.150</div><div>To</div></div>
The specified range for this pool must not be within the range configured on any other address pool for this interface.	

Ilustración 6 Red DMZ rangos

2.4. DMZ2

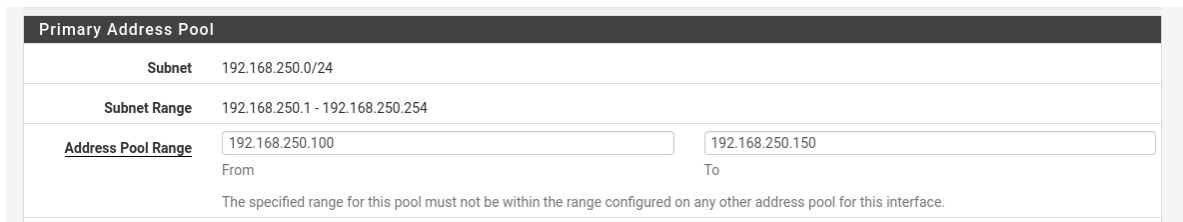
La red DMZ2 se establece como un segmento adicional de la infraestructura de seguridad, destinado a alojar una fuente diferente de logs, complementando la información recopilada en la LAN y la DMZ. En este caso, se implementó un servidor Suricata como fuente de registros en la DMZ2. Suricata proporciona capacidades de detección de intrusiones y análisis de tráfico en tiempo real, mientras que el Servidor Apache genera registros detallados de acceso y errores de aplicaciones web.



```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.250.100/24 brd 192.168.250.255 scope global dynamic noprefixroute eth0
        valid_lft 6791sec preferred_lft 6791sec
    inet6 fe80::7092:4d49:2321:140d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:a1:0b:88:44 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

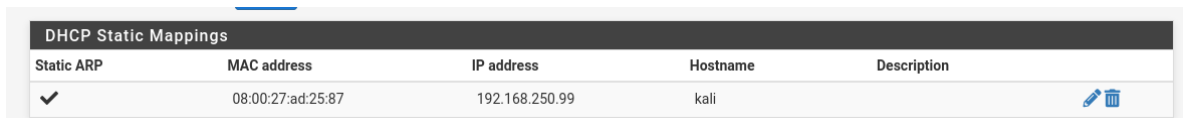
(kali@kali)-[~]
$
```

Ilustración 7 Red DMZ2



Primary Address Pool	
Subnet	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	From 192.168.250.100 To 192.168.250.150
The specified range for this pool must not be within the range configured on any other address pool for this interface.	

Ilustración 8 Red DMZ2 rangos



DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
✓	08:00:27:ad:25:87	192.168.250.99	kali	

Ilustración 9 DMZ2 IP estática

3. FIREWALL

El firewall en esta infraestructura es gestionado por Pfsense, que actúa como la primera línea de defensa contra accesos no autorizados y ataques externos. Pfsense se configura con reglas específicas para controlar el tráfico entre las diferentes redes (LAN, DMZ, y DMZ2) y hacia la red externa (WAN).

Las políticas del firewall permiten únicamente el tráfico necesario, bloqueando cualquier comunicación no esencial para minimizar las posibles superficies de ataque. Por ejemplo, se permite que el Honeypot en la DMZ sea accesible desde la WAN para atraer intentos de intrusión, mientras que se restringe su acceso a otras redes internas. De igual manera, las reglas del firewall aseguran que solo los logs necesarios se transmitirán al servidor Elastic desde cada segmento de la red.

3.1. Reglas WAN - NAT

En esta configuración, se permite el acceso desde la WAN al Honeypot ubicado en la DMZ, para atraer y registrar intentos de intrusión. Esta regla específica permite que el Honeypot cumpla su función sin comprometer la seguridad de las redes internas.

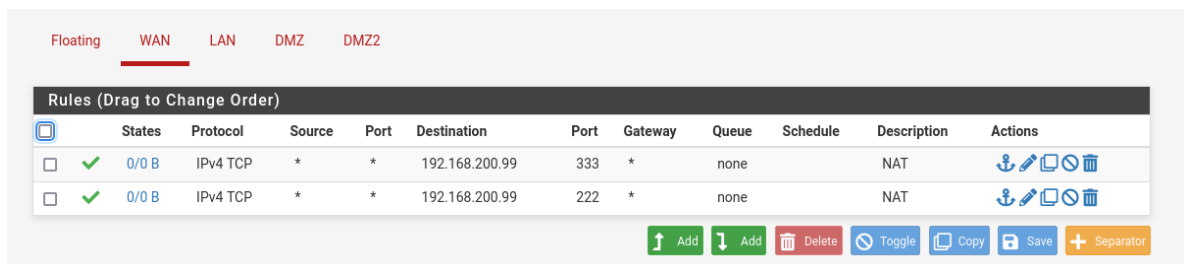


Ilustración 10 Reglas Firewall WAN

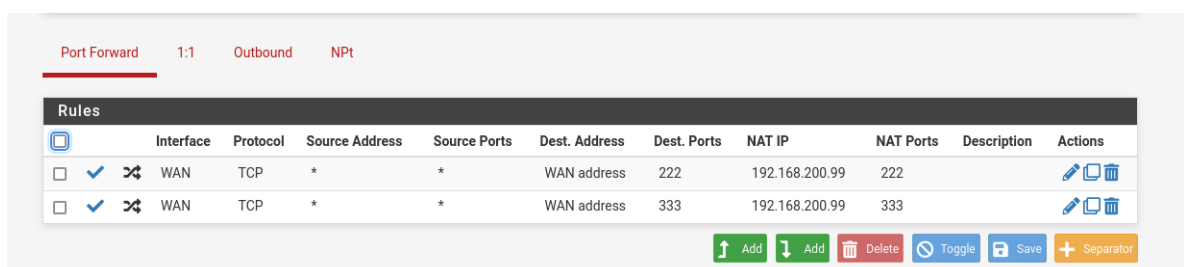


Ilustración 11 Reglas Firewall NAT

3.2. Reglas LAN

Las reglas de firewall aplicadas a la LAN están configuradas para proteger los dispositivos internos mientras permiten el flujo necesario de datos hacia el servidor Elastic. En esta práctica, se permite que el equipo Windows 11 en la LAN envíe registros al servidor Elastic, ubicado en una red interna o externa según la configuración.

Las reglas de la LAN están diseñadas para permitir únicamente el tráfico saliente desde la LAN hacia Elastic, bloqueando cualquier tráfico entrante no solicitado. Esto asegura que el equipo Windows 11 pueda enviar sus registros de manera segura, sin exponer la red LAN a posibles ataques externos o internos no autorizados.

FloatingWANLANDMZDMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	LAN subnets	*	DMZ2 address	22 (SSH)	*	none		Regla adm Suricata	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	LAN subnets	*	DMZ address	22 (SSH)	*	none		Regla adm HoneyPot	
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP echoreq	LAN subnets	*	DMZ2 subnets	*	*	none		Regla de comprobación DMZ2	
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP echoreq	LAN subnets	*	DMZ subnets	*	*	none		Regla de comprobación DMZ	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Block DMZ2	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Block DMZ	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	LAN subnets	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	LAN subnets	*	*	Web	*	none		Salida trafico	

Add

Add

Delete

Toggle

Copy

Save

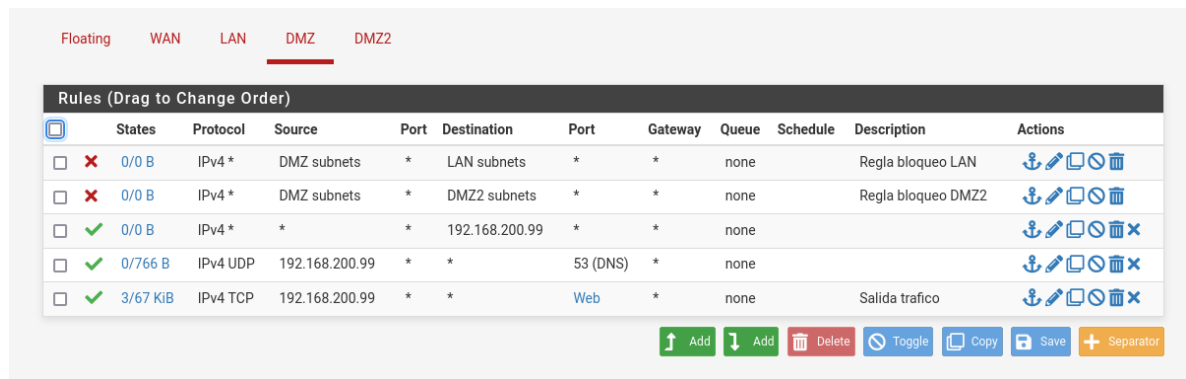
Separator

Ilustración 12 Reglas Firewall LAN

3.3. Reglas DMZ

Las reglas de firewall para la DMZ están configuradas para permitir el acceso controlado al Honeypot desde la red externa (WAN) y asegurar el flujo de logs hacia el servidor Elastic. En esta práctica, el Honeypot en la DMZ está diseñado para atraer y registrar intentos de intrusión, por lo que se permite tráfico entrante desde la WAN hacia el Honeypot mediante una regla específica.

Sin embargo, para mantener la seguridad de la red, se bloquea todo el tráfico saliente desde el Honeypot hacia otras redes internas, como la LAN y la DMZ2, asegurando su aislamiento. Solo se permite el tráfico necesario para que el Honeypot envíe sus registros al servidor Elastic. Esta configuración garantiza que el Honeypot pueda cumplir su función sin comprometer la seguridad de las redes internas.



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules in the DMZ zone. The 'Rules' tab is active, displaying a table of five rules. The first two rules block outgoing traffic to LAN and DMZ2 subnets. The third rule allows outgoing traffic to 192.168.200.99. The fourth rule allows outgoing UDP traffic to 53 (DNS). The fifth rule allows outgoing TCP traffic to the 'Web' service. The interface includes tabs for Floating, WAN, LAN, DMZ, and DMZ2, and a toolbar with buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Regla bloqueo LAN	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Regla bloqueo DMZ2	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	192.168.200.99	*	*	none			
<input type="checkbox"/>	✓ 0/766 B	IPv4 UDP	192.168.200.99	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 3/67 KiB	IPv4 TCP	192.168.200.99	*	*	Web	*	none		Salida trafico	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Ilustración 13 Reglas Firewall DMZ

3.4. Reglas DMZ2

Las reglas de firewall para la DMZ2 están diseñadas para gestionar el tráfico de una fuente adicional de logs, como Suricata o un servidor Apache, hacia el servidor Elastic. En esta práctica, se permite que los dispositivos en la DMZ2 envíen logs al servidor Elastic, asegurando que esta red cumpla su función de proporcionar datos de seguridad adicionales.

Se configuran reglas para permitir el tráfico saliente desde la DMZ2 hacia el servidor Elastic, mientras se bloquea cualquier tráfico no esencial hacia otras redes internas, como la LAN y la DMZ. Además, se restringe el acceso externo (desde la WAN) hacia la DMZ2, permitiendo solo las conexiones necesarias para el envío de registros.

Floating

WAN

LAN

DMZ

DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div><div></div><div>✖</div></div>	0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Block LAN	<div><div></div><div></div><div></div><div></div></div>
<div><div></div><div>✖</div></div>	0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Regla bloqueo DMZ	<div><div></div><div></div><div></div><div></div></div>
<div><div></div><div>✔</div></div>	0/0 B	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div>✔</div></div>	0/0 B	IPv4 TCP	DMZ2 subnets	*	*	Web	*	none		Regla trafico web	<div><div></div><div></div><div></div><div></div><div></div></div>

↑ Add

↓ Add

Delete

Toggle

Copy

Save

Separator

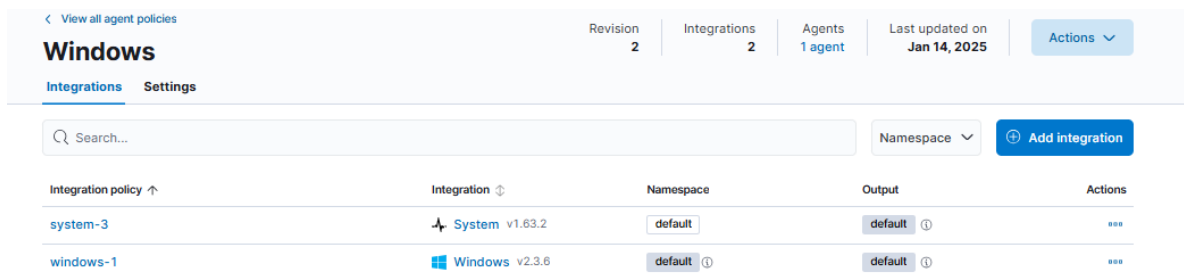
Ilustración 14 Reglas Firewall DMZ2

4. SIEM (ELASTIC CLOUD)

Elastic Cloud actúa como un SIEM (Security Information and Event Management) que centraliza la recopilación, almacenamiento y análisis de logs provenientes de diferentes fuentes dentro de la red. En esta práctica, Elastic recibe registros del equipo Windows 11 en la LAN, el Honeypot en la DMZ y suricata en la DMZ2.

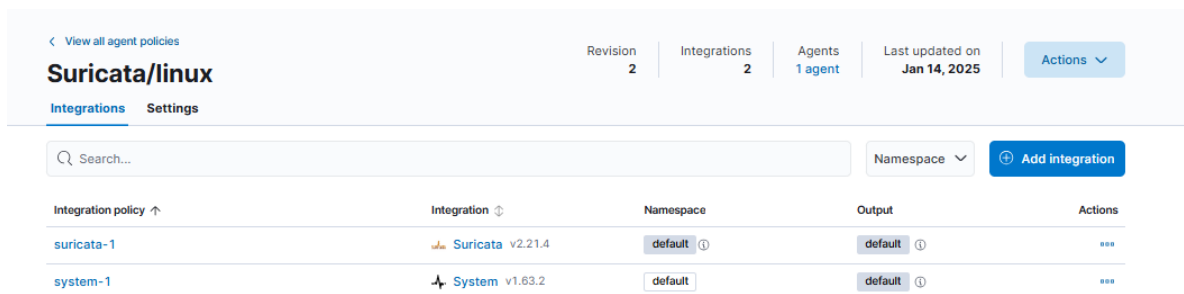
4.1. Políticas e integración (Windows – Honeypot – Suricata)

En Elastic Cloud, las políticas se utilizan para definir la forma de cómo se recopilan, procesan y retienen los logs. Estas políticas permiten configurar reglas específicas para la gestión de datos, como la rotación de registros, la retención de información y las acciones automatizadas en respuesta a ciertos eventos de seguridad.



View all agent policies				
Windows				
Integrations Settings				
<input type="text" value="Search..."/>				
Namespace ▼ Add integration				
Integration policy ↑	Integration ⬇	Namespace	Output	Actions
system-3	System v1.63.2	default	default ⓘ	...
windows-1	Windows v2.3.6	default ⓘ	default ⓘ	...

Ilustración 15 Integración Windows



View all agent policies				
Suricata/linux				
Integrations Settings				
<input type="text" value="Search..."/>				
Namespace ▼ Add integration				
Integration policy ↑	Integration ⬇	Namespace	Output	Actions
suricata-1	Suricata v2.21.4	default ⓘ	default ⓘ	...
system-1	System v1.63.2	default	default ⓘ	...

Ilustración 16 Integración Suricata

The image displays two screenshots from the Elastic Cloud interface. The top screenshot shows the 'Overview' page for an agent named 'kali'. It lists various system metrics and agent details. The bottom screenshot shows the 'Fleet' management page, which provides a centralized view of all agents, including their status, host names, policies, and last activity.

Overview

CPU	2.12 %
Memory	191 MB
Status	Healthy
Last activity	26 seconds ago
Last checkin message	Running
Agent ID	f8bacad2-3c30-4bc6-af53-ed39daadc16f
Agent policy	HoneyPot rev. 2
Agent version	8.17.1
Host name	kali
Host ID	30e662c5c81d4191bd244a79c97d2e0
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	kali
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

Integrations

- system-4
- log-HoneyPot

Fleet

Centralized management for Elastic Agents.

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

Filter your data using KQL syntax

Status: Healthy (2), Unhealthy (0), Updating (0), Offline (0), Inactive (0), Unenrolled (0)

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	HoneyPot rev. 2	2.36 %	191 MB	28 seconds ago	8.17.1	...
Healthy	2a0be205aaf2	Elastic Cloud agent policy rev. 5	N/A	N/A	34 seconds ago	8.17.0	...
Offline	Windows10	Windows rev. 2	N/A	N/A	last week	8.17.0 Upgrade available	...

Rows per page: 20

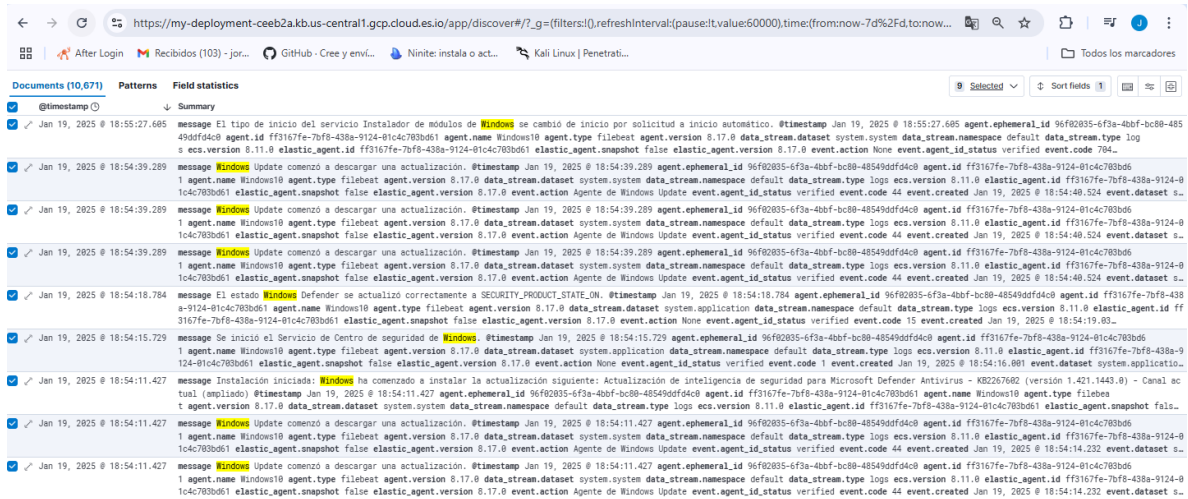
Ilustración 17 Integración HoneyPot

5. SIEM (ELASTIC CLOUD – LOGS)

En Elastic Cloud, los logs juegan un papel crucial al proporcionar datos en tiempo real sobre eventos y actividades dentro de la red. Los logs recolectados de diversas fuentes, como el equipo Windows 11 en la LAN, el HoneyPot en la DMZ y el Suricata en la DMZ2, son centralizados en Elastic para su análisis.

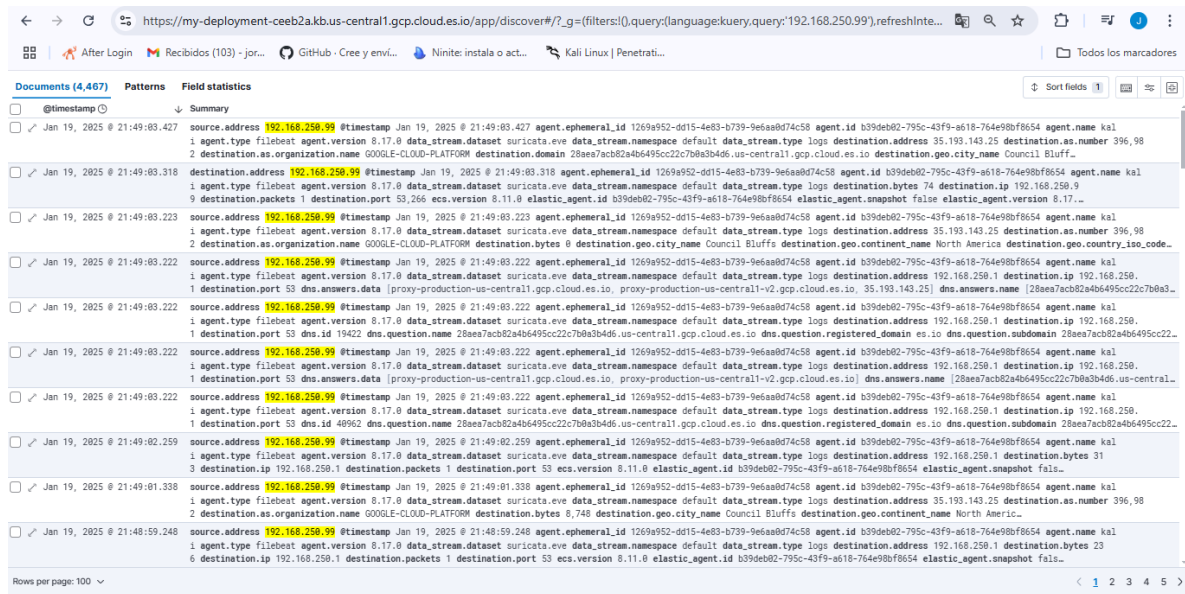
Elastic procesa estos registros para identificar patrones sospechosos, anomalías y posibles amenazas de seguridad. Mediante el uso de paneles y visualizaciones, los logs se transforman en información accesible que permite a los equipos de seguridad monitorear la red de manera eficiente y responder rápidamente a cualquier incidente.

5.1. Logs (Windows – Honeypot – Suricata)



Documents (10,671)	Patterns	Field statistics
<input checked="" type="checkbox"/> @timestamp	Summary	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:55:27.685	message El tipo de inicio del servicio Instalador de módulos de Windows se cambió de inicio por solicitud a inicio automático. @timestamp Jan 19, 2025 @ 18:55:27.685 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action None event.agent_id_status verified event.code 704...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:39.289	message Windows Update comenzó a descargar una actualización. @timestamp Jan 19, 2025 @ 18:54:39.289 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action Agente de Windows Update event.agent_id_status verified event.code 44 event.created Jan 19, 2025 @ 18:54:48.524 event.dataset s...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:39.289	message Windows Update comenzó a actualizar. @timestamp Jan 19, 2025 @ 18:54:39.289 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action Agente de Windows Update event.agent_id_status verified event.code 44 event.created Jan 19, 2025 @ 18:54:48.524 event.dataset s...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:39.289	message Windows Update comenzó a descargar una actualización. @timestamp Jan 19, 2025 @ 18:54:39.289 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action Agente de Windows Update event.agent_id_status verified event.code 44 event.created Jan 19, 2025 @ 18:54:48.524 event.dataset s...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:18.784	message El estado Windows Defender se actualizó correctamente a SECURITY_PRODUCT_STATE_ON. @timestamp Jan 19, 2025 @ 18:54:18.784 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action None event.agent_id_status verified event.code 15 event.created Jan 19, 2025 @ 18:54:19.03...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:15.729	message Se inició el Servicio de Centro de seguridad de Windows . @timestamp Jan 19, 2025 @ 18:54:15.729 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action None event.agent_id_status verified event.code 1 event.created Jan 19, 2025 @ 18:54:16.801 event.dataset system.applicatio...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:11.427	message Instalación iniciada: Windows ha comenzado a instalar la actualización siguiente: Actualización de inteligencia de seguridad para Microsoft Defender Antivirus - KB2376602 (versión 1.421.1443.0) - Canal actual (apilado) @timestamp Jan 19, 2025 @ 18:54:11.427 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:11.427	message Windows Update comenzó a descargar una actualización. @timestamp Jan 19, 2025 @ 18:54:11.427 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action Agente de Windows Update event.agent_id_status verified event.code 44 event.created Jan 19, 2025 @ 18:54:14.232 event.dataset s...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 18:54:11.427	message Windows Update comenzó a descargar una actualización. @timestamp Jan 19, 2025 @ 18:54:11.427 agent.ephemeral_id 96f02035-6f3a-4bbf-bc80-485495df04c0 agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 agent.name Windows10 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.system data_stream.namespace default data_stream.type logs ecs.version 8.11.0 elastic_agent.id fff3167fe-7bf8-438a-9124-01c4c783bd61 elastic_agent.snapshot false elastic_agent.version 8.17.0 event.action Agente de Windows Update event.agent_id_status verified event.code 44 event.created Jan 19, 2025 @ 18:54:14.232 event.dataset s...	

Ilustración 18 Logs WINDOWS



Documents (4,467)	Patterns	Field statistics
<input type="checkbox"/> @timestamp	Summary	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.427	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.427 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 35.193.143.25 destination.as.number 396, 98 2 destination.as.organization.name GOOGLE-CLOUD-PLATFORM destination.domain 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io destination.geo.city.name Council Bluffs destination.geo.continent.name North America destination.geo.country.iso.code...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.318	destination.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.318 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.bytes 74 destination.ip 192.168.250.9 9 destination.packets 1 destination.port 53, 266 ecs.version 8.11.0 elastic_agent.id b39deb02-795c-43f9-a618-764e98bf8654 elastic_agent.snapshot false elastic_agent.version 8.17...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.223	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.223 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 35.193.143.25 destination.as.number 396, 98 2 destination.as.organization.name GOOGLE-CLOUD-PLATFORM destination.bytes 8 destination.geo.city.name Council Bluffs destination.geo.continent.name North America destination.geo.country.iso.code...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.222	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.222 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.ip 192.168.250. 1 destination.port 53 dns.answers.data [proxy-production-us-central1.gcp.cloud.es.io proxy-production-us-central1-v2.gcp.cloud.es.io 35.193.143.25] dns.answers.name [28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io dns.question.registered_domain es.io dns.question.subdomain 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io dns.question.registered_domain es.io dns.question.subdomain 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io]	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.222	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.222 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.ip 192.168.250. 1 destination.port 53 dns.id 48962 dns.question.name 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io dns.question.registered_domain es.io dns.question.subdomain 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io]	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.222	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.222 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.ip 192.168.250. 1 destination.port 53 dns.answers.data [proxy-production-us-central1.gcp.cloud.es.io proxy-production-us-central1-v2.gcp.cloud.es.io 35.193.143.25] dns.answers.name [28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io]	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:03.222	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:03.222 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.ip 192.168.250. 1 destination.port 53 dns.id 48962 dns.question.name 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io dns.question.registered_domain es.io dns.question.subdomain 28aea7acb82a4b6495cc22c7b0a3d46.us-central1.gcp.cloud.es.io]	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:02.259	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:02.259 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.bytes 31 3 destination.ip 192.168.250.1 destination.packets 1 destination.port 53 ecs.version 8.11.0 elastic_agent.id b39deb02-795c-43f9-a618-764e98bf8654 elastic_agent.snapshot false...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:49:01.338	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:49:01.338 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 35.193.143.25 destination.as.number 396, 98 2 destination.as.organization.name GOOGLE-CLOUD-PLATFORM destination.bytes 8, 748 destination.geo.city.name Council Bluffs destination.geo.continent.name North America...	
<input checked="" type="checkbox"/> Jan 19, 2025 @ 21:48:59.248	source.address 192.168.250.99 @timestamp Jan 19, 2025 @ 21:48:59.248 agent.ephemeral_id 1269a952-d015-4e83-b739-9e6aa8d74c58 agent.id b39deb02-795c-43f9-a618-764e98bf8654 agent.name kal 1 agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.1 destination.bytes 23 6 destination.ip 192.168.250.1 destination.packets 1 destination.port 53 ecs.version 8.11.0 elastic_agent.id b39deb02-795c-43f9-a618-764e98bf8654 elastic_agent.snapshot false...	

Ilustración 19 Logs SURICATA1

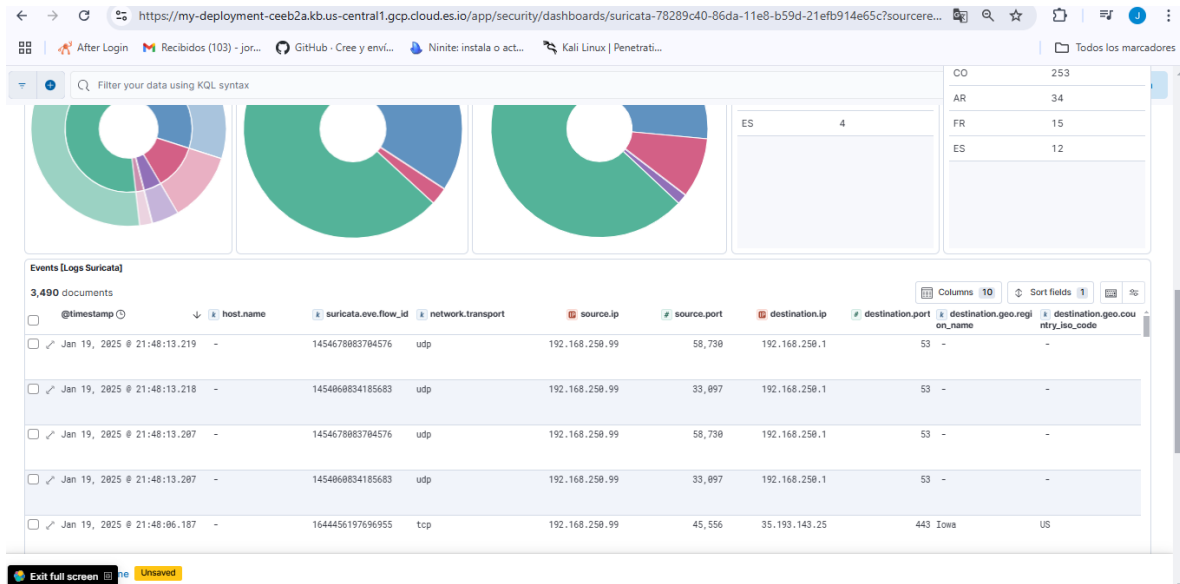


Ilustración 20 Logs SURICATA2

```
kali@kali: /var/log/suricata
File Actions Edit View Help
kali@kali: ~ x kali@kali: /var/log/suricata x kali@kali: /var/log/suricata x kali@kali: ~ x
$ tail -f fast.log
01/19/2025-21:30:47.914563  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:60650 → 35.193.143.25:443
01/19/2025-21:30:48.010253  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:60650
01/19/2025-21:30:52.559880  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:38218 → 35.193.143.25:443
01/19/2025-21:30:52.656978  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:38218
01/19/2025-21:31:02.626258  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:40058 → 35.193.143.25:443
01/19/2025-21:31:07.939916  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:40066 → 35.193.143.25:443
01/19/2025-21:31:08.036432  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:40066
01/19/2025-21:31:09.022373  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:59522
01/19/2025-21:31:19.002204  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:60636
01/19/2025-21:31:22.078703  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:40058
01/19/2025-21:31:29.437757  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:37544 → 35.193.143.25:443
01/19/2025-21:31:29.541167  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:37544
01/19/2025-21:31:32.411639  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:55240 → 35.193.143.25:443
01/19/2025-21:31:32.508287  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 35.193.143.25:443 → 192.168.250.99:55240
01/19/2025-21:31:33.430377  [**] [1:1:0] trafico detectado [**] [Classification: (n
ull)] [Priority: 3] {TCP} 192.168.250.99:55242 → 35.193.143.25:443
```

Ilustración 21 Logs SURICATA Terminal

The screenshot displays the Elastic Security console interface. On the left, a terminal window titled 'Símbolo del sistema - ssh -p 222 root@192.168.0.13' shows a root shell session with the following commands and outputs:

```
root@svr04:~# jordan
root@svr04:~# blue team
root@svr04:~# logs
root@svr04:~# honey pot logs
root@svr04:~#
```

The main console area shows a timeline view of logs. The top bar includes 'Discover', 'Data view', 'Dataset: cowrie', and a search bar. The timeline shows a log entry at '2025-01-29T22:47:39Z' with a message: '2025-01-29T22:47:33 +0800 [HoneyPotSSHTransport,4,192.168.0.17] Command not found: honey pot logs'. The right-hand pane displays the JSON structure of the log entry:

```
{
  "event": {
    "agent_id_status": "verified",
    "ingested": "2025-01-29T22:47:39Z",
    "dataset": "log_honey pot"
  },
  "message": "2025-01-29T22:47:33 +0800 [HoneyPotSSHTransport,4,192.168.0.17] Command not found: honey pot logs"
}
```

Ilustración 22 Logs HONEYPOT

6. CONCLUSION

La práctica de BlueTeam implementada demuestra cómo una arquitectura de red segmentada, junto con herramientas como Pfsense y Elastic Cloud, puede mejorar significativamente la seguridad de una infraestructura. Al separar las redes LAN, DMZ y DMZ2 y aplicar reglas de firewall específicas, se limita la superficie de ataque y se refuerzan las defensas contra posibles intrusiones. La integración de Elastic Cloud como SIEM centralizado permite una gestión eficaz de logs, proporcionando visibilidad completa de los eventos en la red y facilitando la detección temprana de amenazas. Esta configuración no solo asegura una monitorización continua, sino que también prepara el entorno para una respuesta rápida ante incidentes de seguridad, fortaleciendo así la postura general de defensa cibernética.

7. REFERENCIAS Y BIBLIOGRAFIA

- Documentación de Pfsense: <https://docs.netgate.com/pfsense/en/latest/>
- Documentación de Elastic Cloud:
<https://www.elastic.co/guide/en/cloud/current/index.html>
- Documentación de Suricata: <https://suricata.io/docs/>
- Documentación del servidor HTTP Apache: <https://httpd.apache.org/docs/>
- Publicación especial 800-92 del NIST, " Guía para la gestión de registros de seguridad informática":
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>
- OpenAI, "ChatGPT": <https://openai.com/ch>