

# **KeepCoding Bootcamp Ciberseguridad | Edición IX**

## **Módulo de Blue Team**

### **Informe Práctica Blue Team**

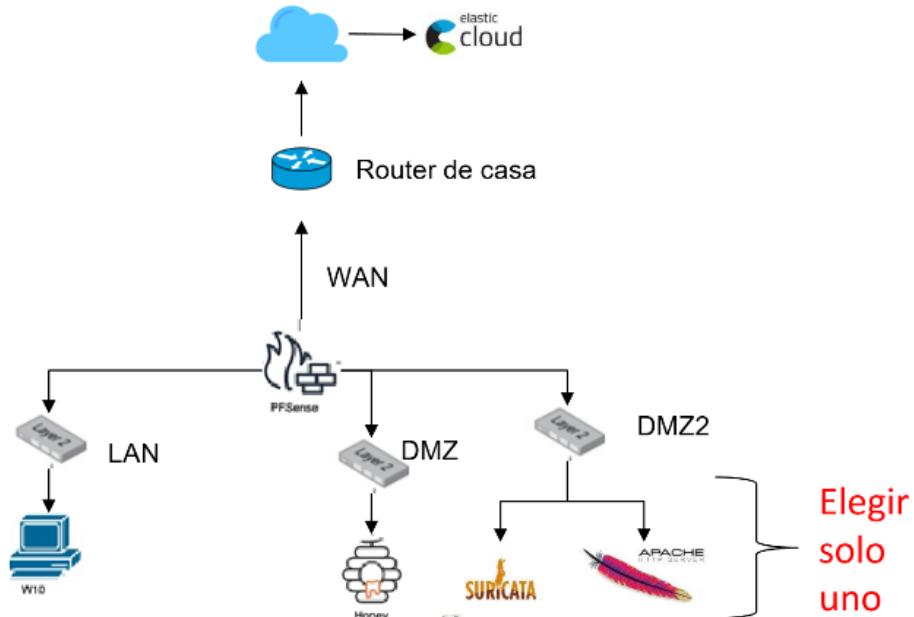
**Por: Oscar Uriel Tobar Rios**

**Fecha del Informe: 18/01/2025**

## Contenido

1	EJERCICIO PROPUESTO .....	3
2	PFSense .....	3
2.1	Instalación .....	3
2.2	Configuración .....	6
2.2.1	Configuración DNS .....	7
2.2.2	Configuración WAN .....	8
2.2.3	Configuración LAN .....	8
2.2.4	Configuración DHCP LAN .....	8
2.2.5	Configuración REGLAS FIREWALL LAN .....	9
2.2.6	Configuración DMZ .....	9
2.2.7	Configuración DHCP DMZ .....	10
2.2.8	Configuración REGLAS FIREWALL DMZ .....	11
2.2.9	Configuración DMZ2 .....	11
2.2.10	Configuración DHCP DMZ2 .....	12
2.2.11	Configuración REGLAS FIREWALL DMZ2 .....	13
3	SIEM (Elastic) .....	15
3.1	Configuración Windows 10 (LAN) .....	15
3.1.1	Configuración del Agente .....	15
3.1.2	Evidencias de recepción de logs .....	17
3.2	Configuración Honey (DMZ) .....	18
3.2.1	Configuración del HoneyPod .....	18
3.2.2	Configuración del Agente .....	19
3.2.3	Evidencias de recepción de logs .....	22
3.3	Configuración Suricata (DMZ2) .....	24
3.3.1	Configuración Suricata .....	24
3.3.2	Configuración del Agente .....	24
3.3.3	Evidencias de recepción de logs .....	25
3.4	Agentes .....	27

# 1 EJERCICIO PROPUESTO



Los requisitos que debe cumplir son los siguientes:

1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
  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.
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.
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.

## 2 PFsense

Para poder desarrollar el ejercicio lo primero fue hacer la instalación de PFSense. Se utilizó la versión pfSense-CE-2.7.2 y se instaló en una máquina Oracle Linux sobre el virtualizador

### 2.1 Instalación

Para la Instalación se utilizó la versión pfSense-CE-2.7.2 y se instaló en una máquina Linux con el virtualizador QEMU, donde se montaron las máquinas virtuales de PFSense, Windows, Kali Linux y Parrot Linux.

Para la configuración de la maquina virtual de PfSense se habilitaron 4 tarjetas de red y se ejecutó la instalación como se muestra a continuación:

**Etapa 1 of 5**

Conexión: QEMU/KVM

Elija cómo le gustaría instalar el sistema operativo

- Medio de instalación local (Imagen ISO o CDROM)
- Instalación por Red (HTTP, FTP, ó NFS)
- Arranque por Red (PXE)
- Importar Imagen de disco existente

**Etapa 2 of 5**

Ubique el medio de instalación

- Utilice CDROM o DVD
- Utilizar imagen ISO:

No existe un dispositivo presente ▾ Explorar...

Detecta automáticamente un sistema operativo basado en el medio de instalación

Tipo de SO: Desconocido  
Versión: Desconocido

**Etapa 3 of 5**

Elija la configuración de la memoria y de la CPU

Memoria (RAM):  - +  
Hasta 31906 MiB disponible en el equipo

CPU:  - +  
Hasta 24 disponible

**Etapa 4 of 5**

Habilitar almacenamiento para esta máquina virtual

- Crear una imagen de disco para la máquina virtual
- Seleccionar o crear almacenaje personalizado

20,0 - + GiB  
34.7 GiB available in the default location

**Etapa 5 of 5**

Lista para iniciar la instalación

Nombre:

SO: Generic  
Instalar: CDROM/ISO local  
Memoria: 8192 MiB  
CPUs: 4  
Almacenamiento: 10.0 GiB ...r/lib/libvirt/images/PFSense2.qcow2  
 Personalizar configuración antes de instalar

Sección de red

Red virtual 'default': NAT

**Interfaz de Red Virtual**

Fuente de red: Dispositivo anfitrión en punto-macvtap

Modo de fuente: Puente

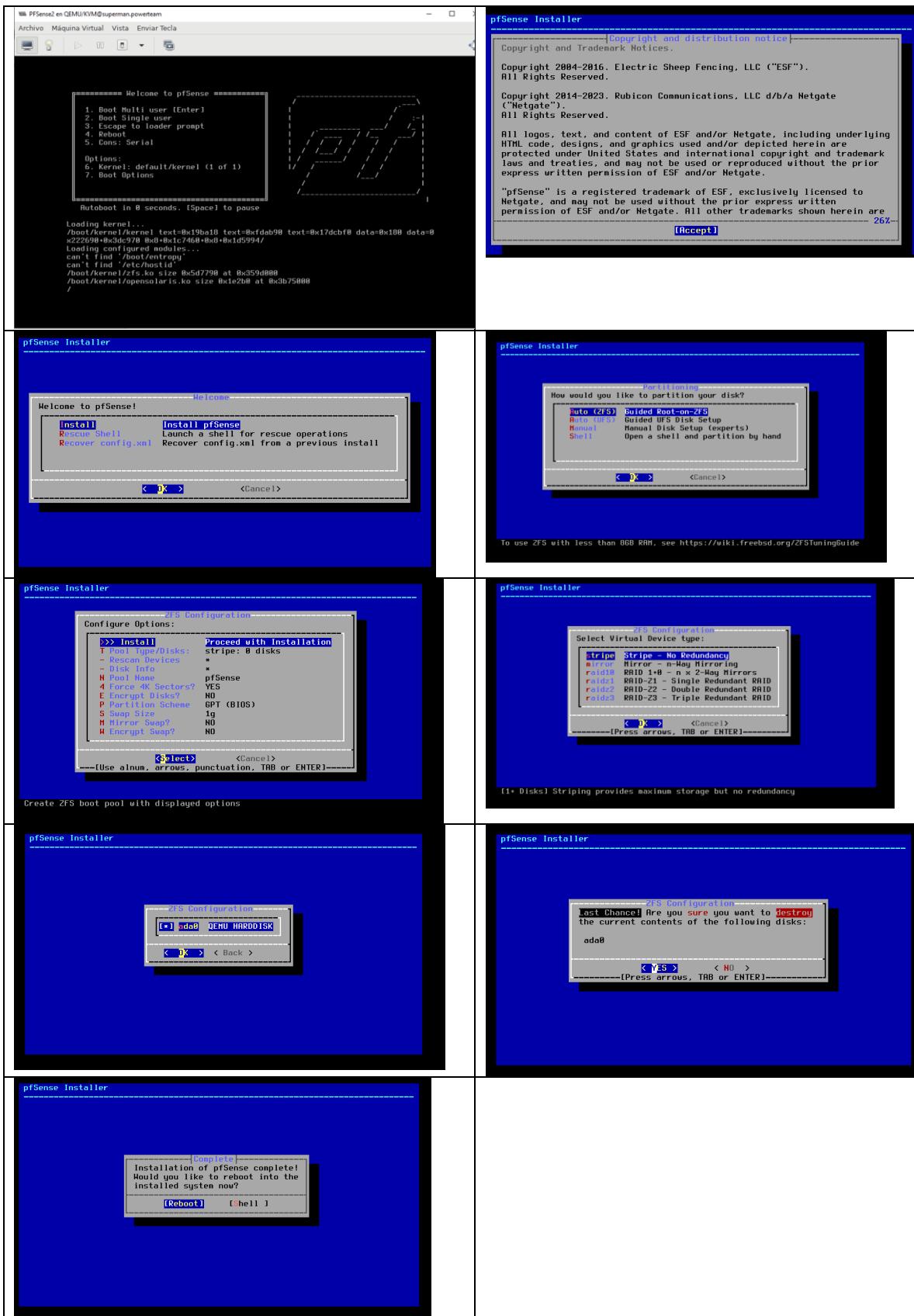
En la mayoría de las configuraciones, esta opción permitirá la comunicación en red de anfitrión a invitado.

Modelo de dispositivo: Hipervisor por defecto

Dirección MAC: 52:54:00:85:08:d4

Puerto virtual

Agregar hardware ▾

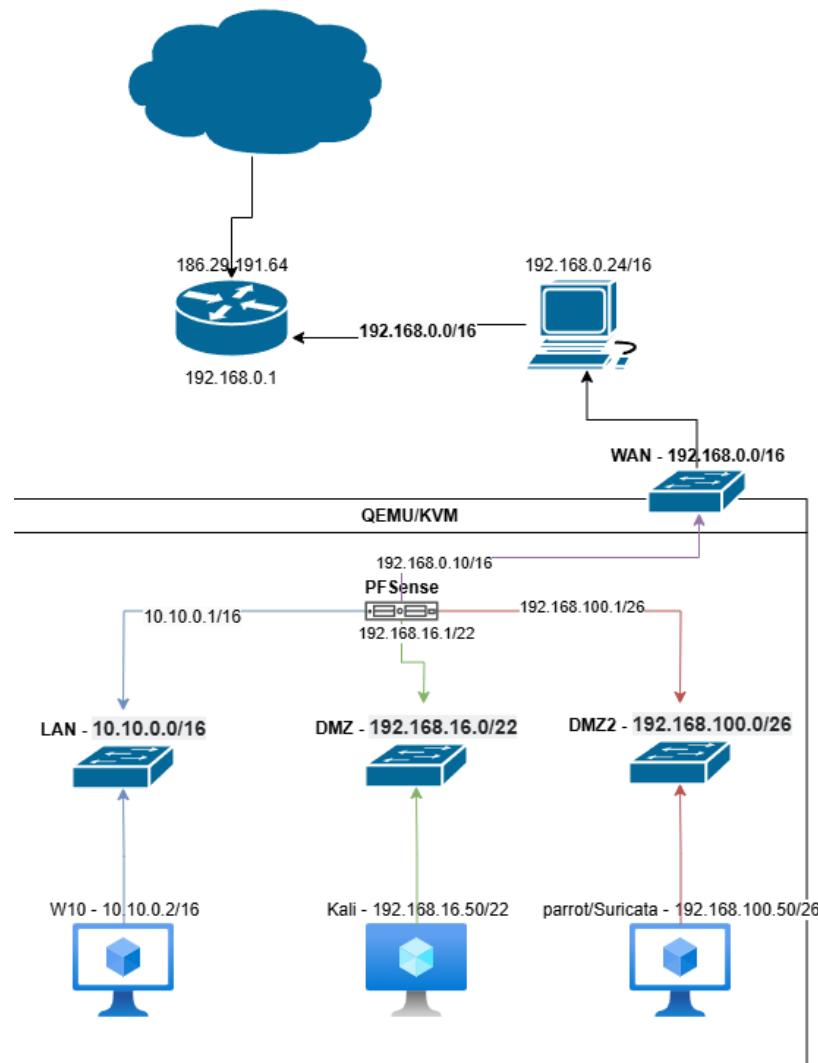


## 2.2 Configuración

Después de instalar PFsense las tarjetas de Red detectados son las siguientes:

```
Valid interfaces are:  
re0      52:54:00:85:08:d4 (down) RealTek 8139C+ 10/100BaseTX  
re1      52:54:00:4d:9e:5c (up) RealTek 8139C+ 10/100BaseTX  
re2      52:54:00:00:0e:0e (up) RealTek 8139C+ 10/100BaseTX  
re3      52:54:00:c8:13:47 (down) RealTek 8139C+ 10/100BaseTX
```

Para establecer la configuración del PFsense se definieron la siguiente configuración para cada red



## 2.2.1 Configuración DNS

Para que los equipos que se encuentran en las redes LAN, DMZ y DMZ2 puedan resolver nombre en internet se configuró un servidor DNS con la siguiente configuración:

The screenshot shows the pfSense web interface under the Services > DNS Resolver > General Settings section. A yellow warning box at the top states: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." Below this, there are tabs for General Settings (selected), Advanced Settings, and Access Lists.

**General DNS Resolver Options**

- Enable:**  Enable DNS resolver
- Listen Port:** 53 (disabled)
- Enable SSL/TLS Service:**  Respond to incoming SSL/TLS queries from local clients
- SSL/TLS Certificate:** GUI default (67480beb2b79) (disabled)
- SSL/TLS Listen Port:** 853 (disabled)
- Network Interfaces:** All (WAN, LAN, DMZ, DMZ2)
- Outgoing Network:** All

**Advanced Settings**

- Network Interfaces:** All (WAN, LAN, DMZ, DMZ2)
- Outgoing Network Interfaces:** All (WAN, LAN, DMZ, DMZ2)
- Strict Outgoing Network Interface Binding:**  Do not send recursive queries if none of the selected Outgoing Network Interfaces are available
- System Domain Local Zone Type:** Transparent
- DNSSEC:**  Enable DNSSEC Support
- Python Module:**  Enable Python Module
- DNS Query Forwarding:**  Enable Forwarding Mode
- DHCP Registration:**  Register DHCP leases in the DNS Resolver

**Notes:**

- ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
- When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.
- Registering DHCP leases in the DNS Resolver will cause their leases when connected to the DNS server to be maintained in the DNS database.

## 2.2.2 Configuración WAN

La tarjeta de Red de la WAN identificado internamente como RE0 se configuro en modo Bridge y desde el DHCP del router se le asigna la ip a esta tarjeta. En este caso se le asigno la IP 192.168.0.9. El resumen de esta interface de red es

**Nombre:** wan

**Id:** re0

**Tipo:** Bridge

**Mac:** 52:54:00:85:08:d4

**Red:** 192.168.0.0/24

## 2.2.3 Configuración LAN

La tarjeta de Red de la LAN identificado internamente como RE1 se configuro en modo de Red interna (solo visible dentro del emulador). Se establecio una dirección IP Fija dentro del segmento de la red 10.10.0.0/16 y se le asignó la primera IP (10.10.0.1).

El resumen de esta interface de red es

**Nombre:** LAN

**Id:** re1

**Tipo:** Interna

**Mac:** 52:54:00:4d:9e:5c

**Red:** 10.10.0.0/16

**Rango de IPs:** 10.10.0.1 - 10.10.255.254

## 2.2.4 Configuración DHCP LAN

Adicionalmente se configuro un servidor DHCP para que entregue direcciones en el rango 10.10.0.10 hasta el 10.10.255.245

The screenshot shows the 'General DHCP Options' configuration page for the LAN interface. The 'DHCP Backend' is set to 'ISC DHCP'. The 'Enable' checkbox is checked, and the 'Ignore BOOTP queries' checkbox is unchecked. Under 'Deny Unknown Clients', the dropdown is set to 'Allow all clients'. A note states: 'When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.' Under 'Ignore Denied Clients', the checkbox is unchecked. A note states: 'This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.' Under 'Ignore Client Identifiers', the checkbox is unchecked. A note states: 'This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.' The 'Primary Address Pool' section shows a subnet of 10.10.0.0/16 and a range from 10.10.0.10 to 10.10.255.245. The 'Address Pool Range' fields show 'From' as 10.10.0.10 and 'To' as 10.10.255.245. A note states: 'The specified range for this pool must not be within the range configured on any other address pool for this interface.' At the bottom, there is an 'Additional Pools' section with a '+ Add Address Pool' button and a note: 'If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.'

**Server Options**

- WINS Servers: WINS Server 1, WINS Server 2
- DNS Servers: 10.10.0.1, 8.8.8.8, 1.1.1.1, DNS Server 4

**OMAPI**

- OMAPI Port: 7911 (disabled)
- OMAPI Key: HMAC-SHA256 (current bind9 default)
- Key Algorithm: HMAC-SHA256 (current bind9 default)

**Other DHCP Options**

- Gateway: 10.10.0.1
- Domain Name: practica1.blue

## 2.2.5 Configuración REGLAS FIREWALL LAN

En el caso de las reglas de firewall para la red LAN se adicionaron una regla

- Regla para permitir consumir sitios web dentro de la misma red LAN

Floating WAN LAN DMZ DMZ2

**Rules (Drag to Change Order)**

#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/10.48 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	LAN subnets	*	LAN subnets	Webs	*	none			
<input type="checkbox"/>	<input checked="" type="checkbox"/> 32/3.85 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

## 2.2.6 Configuración DMZ

La tarjeta de Red de la DMZ identificada internamente como RE2 se configuró en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 192.168.16.0/22 y se le asignó la primera IP del segmento (192.168.16.1).

**Nombre:** DMZ

**Id:** re2

**Tipo:** Interna

**Mac:** 52:54:00:00:0e:0e

**Red:** 192.168.16.0/22

**Rango de IPs:** 192.168.16.1 - 192.168.19.254

**Numero de Hosts:** 1,024

## 2.2.7 Configuración DHCP DMZ

Se configuro un servidor DHCP para la red de DMZ que entregue direcciones en el rango 192.168.16.10 hasta el 192.168.16.50

LAN    **DMZ**    DMZ2

**General DHCP Options**

DHCP Backend: ISC DHCP

Enable:  Enable DHCP server on DMZ interface

BOOTP:  Ignore BOOTP queries

Deny Unknown Clients:  Allow all clients

Ignore Denied Clients:  Ignore denied clients rather than reject

Ignore Client Identifiers:  Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

**Primary Address Pool**

Subnet: 192.168.16.0/22

Subnet Range: 192.168.16.1 - 192.168.19.254

Address Pool Range: From 192.168.16.10 To 192.168.16.50

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

**Server Options**

WINS Servers: WINS Server 1, WINS Server 2

DNS Servers: 192.168.16.1, 8.8.8.8, 1.1.1.1, DNS Server 4

**OMAPI**

OMAPI Port: OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.

OMAPI Key: OMAPI Key

Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.

Generate New Key:

Key Algorithm: HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

**Other DHCP Options**

Gateway: 192.168.16.1

The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter 'none' for no gateway assignment.

Domain Name: practical.blue

The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain Search List: example.com.sub.example.com

Activar Windows

## 2.2.8 Configuración REGLAS FIREWALL DMZ

Para las reglas del DMZ se establecieron cuatro reglas así:

- Permitir protocolo ICMP (el Echo Request) desde las subredes de la DMZ para permitir hacer ping
- Permitir el protocolo UDP hacia el puerto 53 desde las subredes de la DMZ para permitir usar el DNS
- Permitir el protocolo TCP y UDP hacia las subredes de la DMZ desde las subredes de la LAN para permitir desde la red interna LAN probar el honey y demás servicios
- Permitir el protocolo TCP por el puerto 2222 hacia las subredes de la DMZ para permitir probar el honey que en este caso es un SSH por el puerto 2222

The screenshot shows the pfSense Firewall Rules configuration interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A notification bell icon shows 6 alerts. The main title is "Firewall / Rules / DMZ". Below the title, there are tabs for Floating, WAN, LAN, DMZ, and DMZ2, with "DMZ" selected. The main content area displays a table titled "Rules (Drag to Change Order)". The table has columns for Action, Description, Schedule, Queue, Gateway, Port, Destination, Source, Protocol, States, and Actions. There are five rules listed:

Action	Description	Schedule	Queue	Gateway	Port	Destination	Source	Protocol	States	Actions
				*	*	DMZ subnets	LAN subnets	IPv4 TCP/UDP	0/0 B	
				2222	*	DMZ subnets	*	IPv4 TCP	0/0 B	
				*	*	*	*	IPv4 TCP	28/1.33 GiB	
	Habilitar Ping			*	*	*	DMZ subnets	IPv4 ICMP echoreq	0/504 B	
	Regla DNS			53 (DNS)	*	none	DMZ subnets	IPv4 UDP	18/43.82 MiB	

## 2.2.9 Configuración DMZ2

La tarjeta de Red de la DMZ2 identificado internamente como RE3 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 192.168.100.0/26 y se le asignó la primera IP del segmento (192.168.100.1).

**Nombre:** DMZ2

**Id:** re3

**Tipo:** Interna

**Mac:** 52:54:00:c8:13:47

**Red:** 192.168.100.0/26

**Rango de IPs:** 192.168.100.1 - 192.168.100.62

**Numero de Hosts:** 64

## 2.2.10 Configuración DHCP DMZ2

Para la DMZ2 se configuro un servidor DHCP que entregue direcciones en el rango 192.168.100.10 hasta el 192.168.100.50

The screenshot shows a web-based configuration interface for a DHCP server. At the top, there are three tabs: LAN, DMZ (which is selected), and DMZ2. The main content area is divided into two main sections: "General DHCP Options" and "Primary Address Pool".

**General DHCP Options:**

- DHCP Backend:** ISC DHCP
- Enable:**  Enable DHCP server on DMZ2 interface
- BOOTP:**  Ignore BOOTP queries
- Deny Unknown Clients:** Allow all clients (dropdown menu)

When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to Allow known clients from **only** this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

- Ignore Denied Clients:**  Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore Client Identifiers:**  Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

**Primary Address Pool:**

- Subnet:** 192.168.100.0/26
- Subnet Range:** 192.168.100.1 - 192.168.100.62
- Address Pool Range:** From 192.168.100.10 To 192.168.100.50

The specified range for this pool must not be within the range configured on any other address pool for this interface.

- Additional Pools:** [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

**Server Options**

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.100.1
	8.8.8.8
	1.1.1.1
	DNS Server 4

**OMAPI**

OMAPI Port	OMAPI Port	Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.
OMAPI Key	OMAPI Key	<input type="checkbox"/> Generate New Key Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.
Key Algorithm	HMAC-SHA256 (current bind9 default)	Set the algorithm that OMAPI key will use.

**Other DHCP Options**

Gateway	192.168.100.1	The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name	practica1.blue	The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.

## 2.2.11 Configuración REGLAS FIREWALL DMZ2

Para las reglas del DMZ2 se establecieron dos reglas así:

- Permitir protocolo ICMP (el Echo Request) desde las subredes de la DMZ2 para permitir hacer ping
- Permitir el protocolo UDP hacia el puerto 53 desde las subredes de la DMZ2 para permitir usar el DNS

## Firewall / Rules / DMZ2

 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"/>	35/844.49 MiB	IPv4 TCP	DMZ2 subnets	*	*	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 ICMP	DMZ2 subnets	*	*	*	*	none	Habilitar Ping		
<input type="checkbox"/>	29/22.46 MiB	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none	Regla DNS		

Add Add Delete Toggle Copy Save Separator

### 3 SIEM (Elastic)

Basados en la configuración establecida como se muestra a continuación

```
FreeBSD/amd64 (pfSense.practica1.blue) (ttyv0)

KVM Guest - Netgate Device ID: 1da1f41aeb0c85b2dfbc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> re0      -> v4/DHCP4: 192.168.0.9/24
LAN (lan)      -> re1      -> v4: 10.10.0.1/16
DMZ (opt1)     -> re2      -> v4: 192.168.16.1/22
DMZ2 (opt2)    -> re3      -> v4: 192.168.100.1/26

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

Enter an option: █
```

Se procedió a configurar en Elastic CLOUD la configuración de los agentes para configurar en Elvio de logs

#### 3.1 Configuración Windows 10 (LAN)

##### 3.1.1 Configuración del Agente

En una maquina virtual de Windows 10 llamada DESKTOP-PGGB831 que instaló el agente de Elastic elastic-agent-8.17.0 para Windows

Para su instalación en Windows después de descomprimirlo se ejecuto la instalación con este comando

```
.\elastic-agent.exe install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RlbDhwczQybjE6aDZXYzQtR0tSYXlpdTN6QU01ekN3QQ==
```

**Agent details** Logs Diagnostics

### Overview

CPU	1.82 %
Memory	170 MB
Status	Healthy
Last activity	29 seconds ago
Last checkin message	Running
Agent ID	da9a681c-3265-4f44-a820-d74d0444418d
Agent policy	Políticas LAN rev. 2
Agent version	8.17.0
Host name	DESKTOP-PGGB831
Host ID	caa1d453-ab67-4999-bba9-2a27f98fe24d
Output for integrations	Default output
Output for monitoring	Default output
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	windows
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

### Integrations

- > windows-1
- > system-2

Una vez instalado desde Elastic cloud que añadió una integración para leer los logs de Windows así:

**Edit Windows integration**

Modify integration settings and deploy changes to the selected agent policy.

### 1 Configure integration

#### Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: windows-1

Description: Optional

[Advanced options](#)

Collect events from the following Windows event log channels:

[Change defaults](#)

AppLocker/EXE and DLL  
Microsoft-Windows-AppLocker/EXE and DLL channel

AppLocker/MSI and Script  
Microsoft-Windows-AppLocker/MSI and Script channel

Packaged app-Deployment  
Microsoft-Windows-AppLocker/Packaged app-Deployment channel

**Preserve original event**

Preserves a raw copy of the original XML event, added to the field event.event.original

[Advanced options](#)

Collect Windows perfmon and service metrics Change defaults ^

Windows perfmon metrics   
Collect Windows perfmon metrics

**Perfmon Group Measurements By Instance**  
Enabling this option will send all measurements with a matching perfmon instance as part of a single event

**Perfmon Ignore Non Existent Counters**  
Enabling this option will make sure to ignore any errors caused by counters that do not exist

**Perfmon Refresh Wildcard Counters**  
Enabling this option will cause the counter list to be retrieved after each fetch, rather than once at start time.

**Perfmon Queries**

```
- object: 'Process'
  instance: ['*']
  counters:
    - name: '% Processor Time'
      field: cpu_perc
      format: "float"
    - name: 'Working Set'
```

Will list the perfmon queries to execute, each query will have an **object** option, an optional **instance** configuration and the actual counters.

**Period**  
10s

[Advanced options](#)

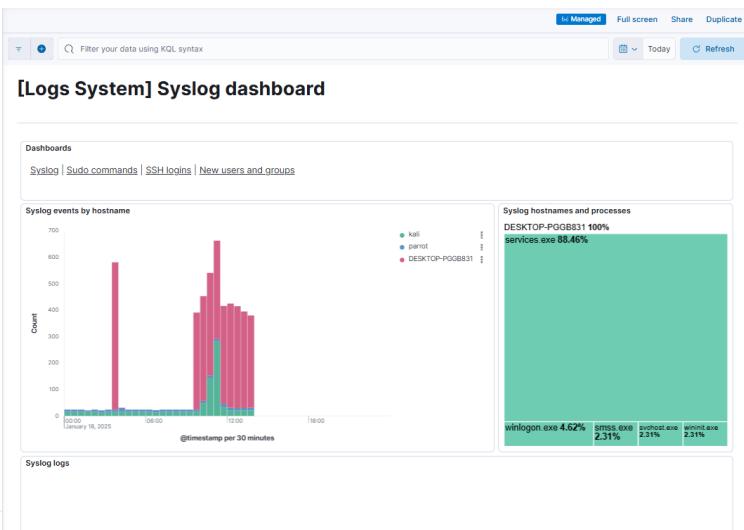
---

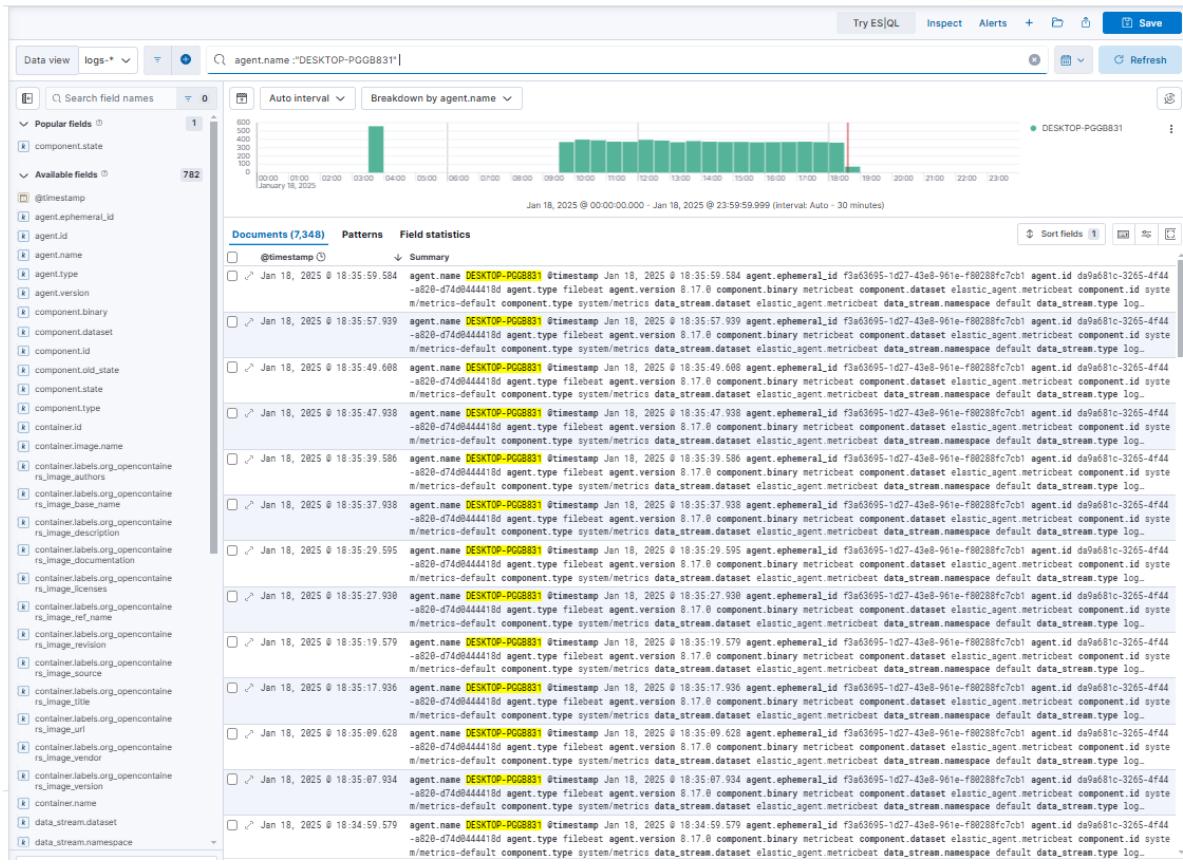
Windows service metrics Optional  
Collect Windows service metrics

**Period**  
60s

**Processors**

### 3.1.2 Evidencias de recepción de logs





Se deja un ejemplo de uno de los mensajes en

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciaswindow.sxt>

EL archivo comprimido con todos los mensajes desde la maquina Windows recibidos en Elastic y exportado para el día 18 de Enero es este

<https://github.com/oscartobar/practicaskeepcoding/blob/1364cdaba9b4cd1433177d6e6ddb/e3109b775dbf/BlueTeam/Discover%20session%20Windows.zip>

## 3.2 Configuración Honey (DMZ)

### 3.2.1 Configuración del HoneyPod

En la Maquina Kali Linux se instalo el Honey que para el ejercicio se instalo un HoneyPod de SSH llamado cowrie

Inicio de honey

```
docker run -d -p 2222:2222 cowrie/cowrie:latest
```

```
(kali㉿kali)-[~/logs/ssh]
$ docker ps
CONTAINER ID   IMAGE          COMMAND
STATUS         PORTS
CREATED        NAME
S
b84ed29c370f  cowrie/cowrie:latest  "/cowrie/cowrie-env/..."
Up 15 minutes  0.0.0.0:2222→2222/tcp, :::2222→2222/tcp, 2223/tcp   kind
_cori
```

```
docker logs -f kind_cori > cowri.log
```

```
(kali㉿kali)-[~/logs/ssh]
$ docker logs -f kind_cori > cowri.log
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

### 3.2.2 Configuración del Agente

Una vez funcionando que instalo en agente de elastic asi:

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RlbDhwc2tXbFU6ZVlGSWIHZGJTbFNKajhETWlnd2J5dw==
```

```
C:\Users\PC\Downloads\elastic-agent-8.17.0-windows-x86_64\elastic-agent-8.17.0-windows-x86_64>./elastic-agent.exe install
11 --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RIBnwczQybjE6aDZXYzQtr0tSY1pdTN6Q01ekN3QQ==
"." no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\PC\Downloads\elastic-agent-8.17.0-windows-x86_64\elastic-agent-8.17.0-windows-x86_64>elastic-agent.exe install
--url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RIBnwczQybjE6aDZXYzQtr0tSY1pdTN6Q01ekN3QQ==
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
[=] Service Started [12s] Elastic Agent successfully installed, starting enrollment.
[==>] Waiting For Enroll... [13s] {"log.level":"info","@timestamp":"2025-01-16T07:30:46.475+0100","log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "520"}, "message": "Starting enrollment to URL: https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443/", "ecs.version": "1.6.0"}
[==>] Waiting For Enroll... [18s] {"log.level": "info", "@timestamp": "2025-01-16T07:30:51.519+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "483"}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2025-01-16T07:30:51.525+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute", "file.name": "cmd/enroll_cmd.go", "file.line": "301"}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
[=] Done [18s]
Elastic Agent has been successfully installed.

C:\Users\PC\Downloads\elastic-agent-8.17.0-windows-x86_64\elastic-agent-8.17.0-windows-x86_64>
```

Luego en Elastic se configuro una integración para logs personalizados en la maquina Kali asi

The screenshot shows the 'Edit Custom Logs integration' page. At the top, there's a 'Cancel' button and a title 'Edit Custom Logs integration'. Below the title, a sub-header says 'Modify integration settings and deploy changes to the selected agent policy.' A large blue circular icon with the number '1' contains the text 'Configure integration'.

**Integration settings**

Choose a name and description to help identify how this integration will be used.

Integration name	log-2
Description	Optional

[Advanced options](#)

**Custom log file**

[Change defaults](#)

Log file path: /home/kali/logs/ssh/cowri.log

[Add row](#)

**Log file path**  
/home/kali/logs/ssh/cowri.log

[Add row](#)  
Path to log files to be collected

**Dataset name**  
generic

Set the name for your dataset. Changing the dataset will send the data to a different index. You can't use - in the name of a dataset and only valid characters for Elasticsearch index names.

[Advanced options](#)

## 2 Where to add this integration?

For existing hosts:

**Agent policies**

Agent policies are used to manage a group of integrations across a set of agents.

**Agent policies**

Políticas DMZ

1 agent is enrolled with the selected agent policies.

Adicionalmente Tambien se tomo una integración para leer los logs del docker

[Cancel](#)

## Edit Docker integration

Modify integration settings and deploy changes to the selected agent policy.

### 1 Configure integration

**Integration settings**

Choose a name and description to help identify how this integration will be used.

**Integration name**

docker-1

**Description**

Optional

Integracion ssh

[Advanced options](#)

**Collect Docker metrics**

[Change defaults](#)

**Collect Docker container logs**

[Change defaults](#)

Collect Docker container logs  
Collect Docker container logs

**Condition**

Optional

Condition to filter when to apply this datastream. Refer to [Docker provider](#) to find the available keys and to [Conditions](#) on how to use the available keys in conditions.

[Advanced options](#)

## 2 Where to add this integration?

For existing hosts:

**Agent policies**

Agent policies are used to manage a group of integrations across a set of agents.

**Agent policies**

Políticas DMZ

▼

1 agent is enrolled with the selected agent policies.

< Cancel

## Edit Custom Logs integration

Modify integration settings and deploy changes to the selected agent policy.

### 1 Configure integration

**Integration settings**

Choose a name and description to help identify how this integration will be used.

**Integration name**: log-2

**Description**: Optional

[Advanced options](#)

**Custom log file**

[Change defaults ^](#)

**Log file path**: /home/kali/logs/ssh/cowri.log

[Add row](#) Path to log files to be collected

**Dataset name**: generic

Set the name for your dataset. Changing the dataset will send the data to a different index. You can't use - in the name of a dataset and only valid characters for Elasticsearch index names.

[Advanced options](#)

### 2 Where to add this integration?

For existing hosts:

**Agent policies**

Agent policies are used to manage a group of integrations across a set of agents.

**Agent policies**: Políticas DMZ

1 agent is enrolled with the selected agent policies.

### 3.2.3 Evidencias de recepción de logs

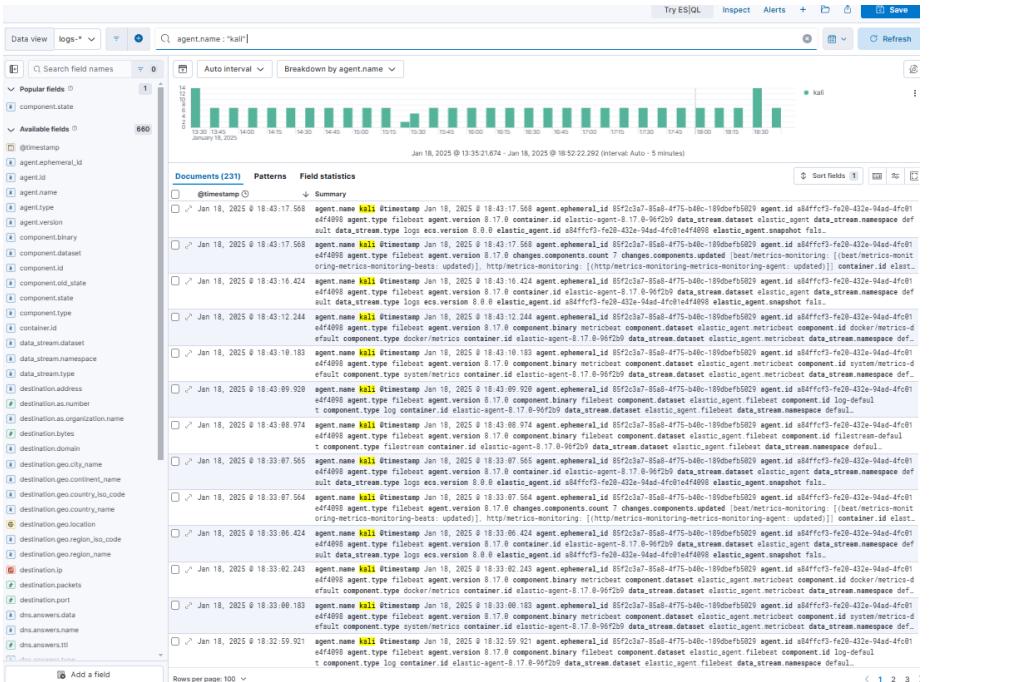
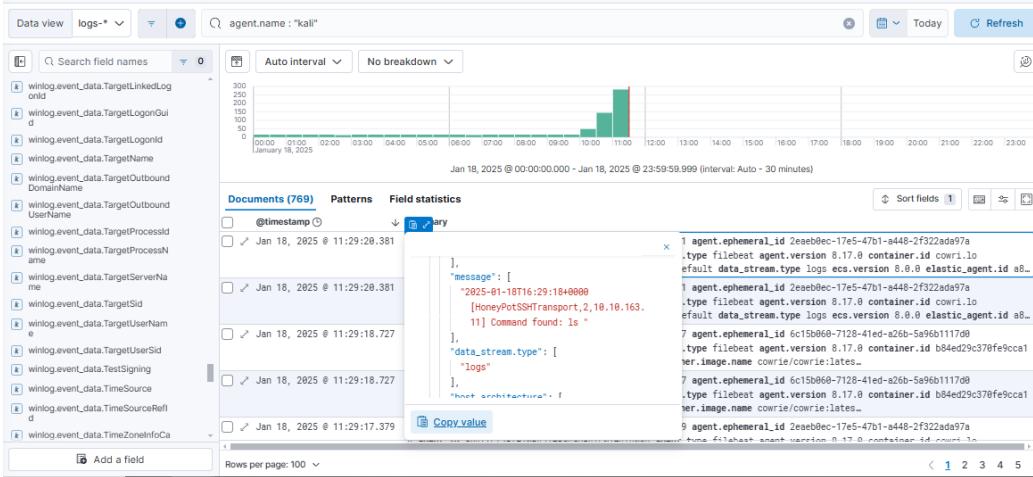
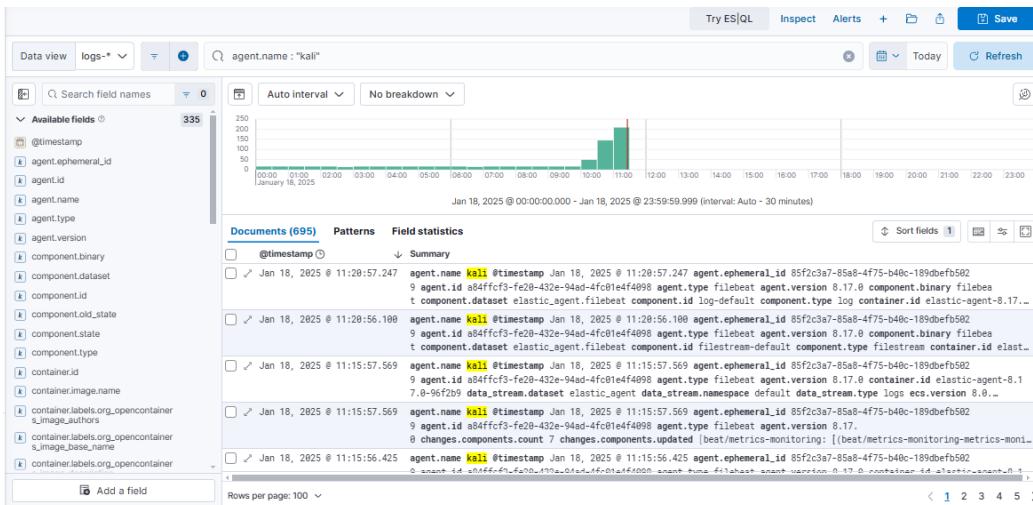
Para el ejemplo se utilizo el honeyPod del ssh instalado para evidenciar que si se genera el log y se transmitió al elastic así:

```
C:\Users\PC\.ssh>ssh root@192.168.16.50 -p 2222
root@192.168.16.50's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# cd a
bash: cd: a: No such file or directory
root@svr04:~# ls
root@svr04:~# mkdir a
root@svr04:~# cd a
root@svr04:~/a# ls
root@svr04:~/a#
```

<input type="checkbox"/>		16/40.69	IPv4 UDP	DMZ	*	*	53	*	none
--------------------------	--	----------	----------	-----	---	---	----	---	------



Se deja un ejemplo dos de los mensajes de el Honey de SSH en

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciassh1.txt>

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciassh2.txt>

El archivo comprimido con todos los mensajes desde la maquina Kali recibidos en Elastic y exportado para el día 18 de Enero es este

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/Discover%20session%20Honey.zip>

### 3.3 Configuración Suricata (DMZ2)

#### 3.3.1 Configuración Suricata

Para la instalación de suricata en el Parrot Linux se ejecutaron estos comandos

```
sudo apt update
```

```
sudo apt install suricata
```

se creo el archivo /etc/suricata/rules/suricata.rules y se aplico esta regla

```
GNU nano 7.2          /etc/suricata/rules/suricata.rules
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)
..config rules           suricata.yaml
```

Luego como administrador se inicio el programa asi:

```
suricata -c /etc/suricata/suricata.yaml -i ens3
```

#### 3.3.2 Configuración del Agente

Se instalo el agente para Linux de elastic asi

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-
linux-x86_64.tar.gz
```

```
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
```

```
cd elastic-agent-8.17.0-linux-x86_64
```

```
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-
1.aws.elastic.cloud:443 --enrollment-
token=QTJNMWJKUUJPN2RlbDhwc2tXbFU6ZVlGSWIHZGJTbFNKajhETWlnd2J5dw==
```

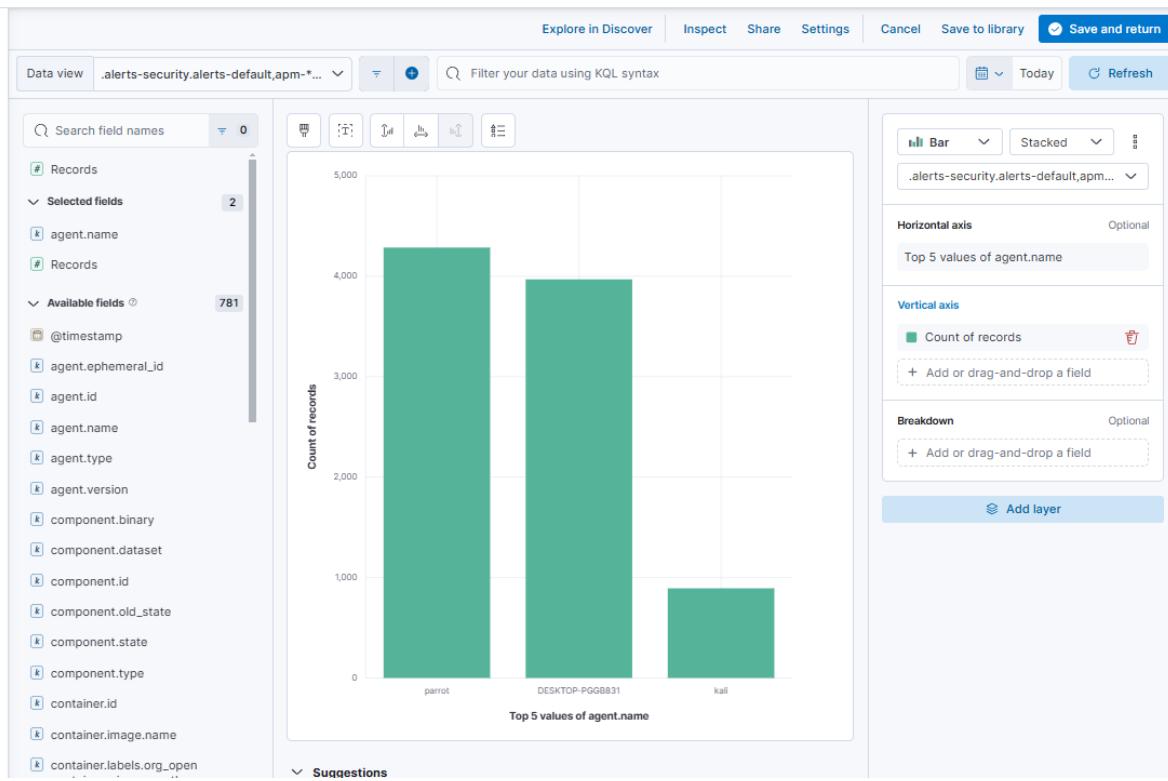
Luego desde Elastic se configuro una nueva integración asi

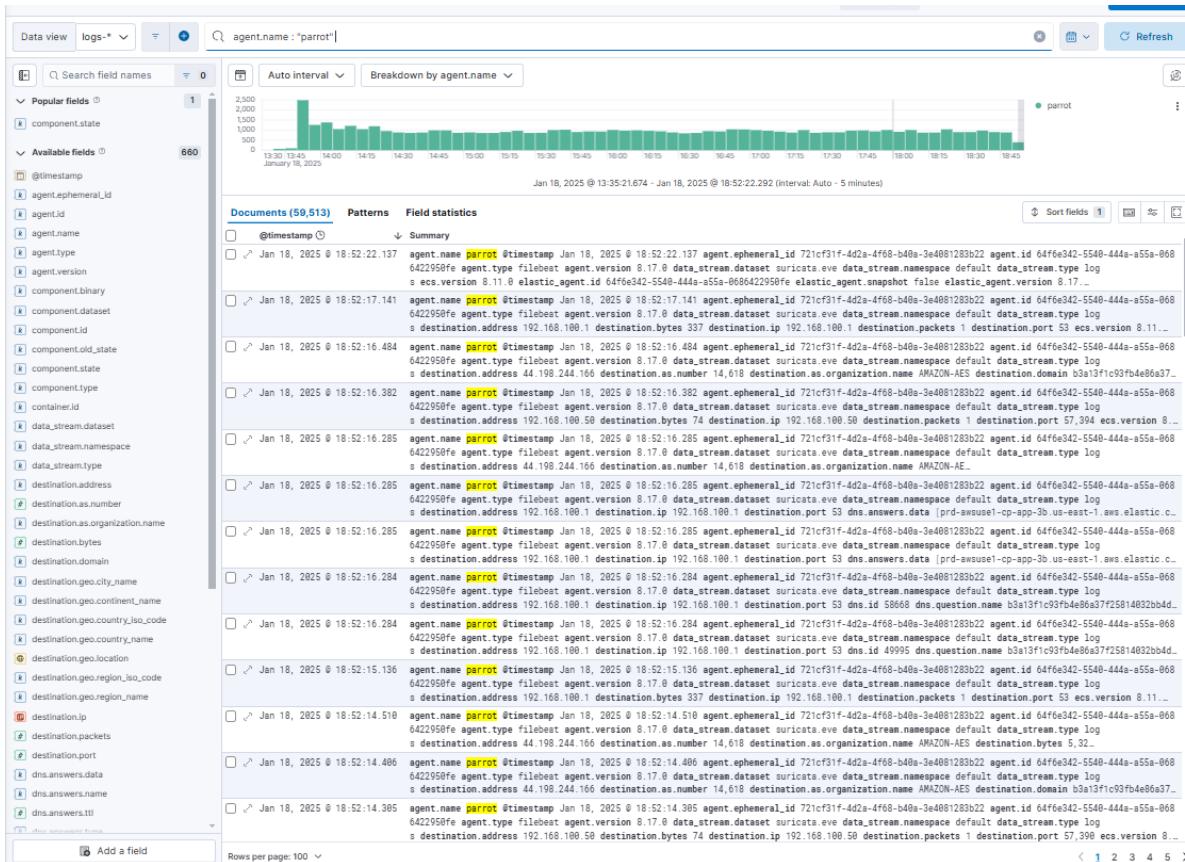
The screenshot shows the 'Integrations' page for the 'Linux/Suricata' policy. At the top, it displays 'Revision 6', 'Integrations 2', 'Agents 1 agent', and 'Last updated on Jan 16, 2025'. Below this, there are tabs for 'Integrations' (which is selected) and 'Settings'. A search bar and a 'Namespace' dropdown are also present. A blue button labeled '+ Add integration' is visible. The main table lists two integrations:

Integration policy	Integration	Namespace	Output	Actions
suricata-2	Suricata v2.21.4	default	Default output	...
system-1	System v1.63.2	default	Default output	...

The screenshot shows the 'Configure integration' step. It starts with 'Integration settings' where you can choose a name and description. The 'Integration name' is set to 'suricata-2' and the 'Description' field is optional. There is a link to 'Advanced options'. The next section is 'Collect Suricata eve logs (input: logfile)', which is checked. It includes a 'Change defaults' link, a 'Suricata eve logs (log)' input (checked), a 'Paths' field containing '/var/log/suricata/eve.json', and a 'Preserve original event' checkbox. There is also a link to 'Advanced options'. The final section is 'Where to add this integration?' under 'For existing hosts', showing the 'Agent policies' section where 'Linux/Suricata' is selected.

### 3.3.3 Evidencias de recepción de logs





La información de un mensaje lo puede ver aqui

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciasuricata2.txt>

La información de todos los logs de suricata recibidos en elastic y transmitidos desde el parrot el día 18 de enero se dejan aquí

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/Discover%20session%20Suricata.zip>

## 3.4 Agentes

La información resumida de los agentes configurados en Elastic es la siguiente

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](#)

Ingest Overview Metrics Agent Info Metrics Agent activity [Add agent](#)

Filter your data using KQL syntax Status 4 Tags 0 Agent policy 3 Upgrade available

Showing 3 agents [Clear filters](#) Healthy 3 Unhealthy 0 Updating 0 Offline 0 Inactive 0 Unenrolled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last acti...	Version	Actions
<input type="checkbox"/>	<span>Healthy</span>	DESKTOP-PGGB831	Politicas LAN rev. 2	1.74 %	170 MB	25 seconds ago	8.17.0	
<input type="checkbox"/>	<span>Healthy</span>	parrot	Linux/Suricata rev. 6	2.70 %	233 MB	16 seconds ago	8.17.0	
<input type="checkbox"/>	<span>Healthy</span>	kali	Politicas DMZ rev. 9	2.40 %	240 MB	14 seconds ago	8.17.0	

Rows per page: 20 < 1 >

## 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
Politicas DMZ rev. 9 Politicas para servidores en DMZ	Jan 18, 2025	0 / 1 (1)	4	
Linux/Suricata rev. 6	Jan 16, 2025	0 / 1 (1)	2	
Politicas LAN rev. 2	Jan 16, 2025	0 / 1 (1)	2	

Rows per page: 20 < 1 >

## Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

Dataset		Type	Namespace	Integration	Last activity	Size	Actions
elastic_agent.elastic_agent	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	37.11mb	...
elastic_agent.filebeat	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	18.03mb	...
elastic_agent.filebeat_input	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	7.26mb	...
elastic_agent.metricbeat	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	31.61mb	...
windows.service	metrics	default	windows	windows	Jan 18, 2025 @ 2:18:15 PM	47.79mb	...
fleet_server.agent_status	metrics	default	fleet_server	fleet_server	Jan 18, 2025 @ 2:17:40 PM	1.18mb	...
fleet_server.agent_versions	metrics	default	fleet_server	fleet_server	Jan 18, 2025 @ 2:17:40 PM	686.23kb	...
system.application	logs	default	system	system	Jan 18, 2025 @ 2:17:36 PM	1.04mb	...
elastic_agent	logs	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.18mb	...
elastic_agent.filebeat	logs	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.32mb	...
system.security	logs	default	system	system	Jan 18, 2025 @ 2:12:36 PM	19.72mb	...
system.system	logs	default	system	system	Jan 18, 2025 @ 12:43:43 PM	597.16kb	...
docker.container_logs	logs	default	docker	docker	Jan 18, 2025 @ 11:32:22 AM	390.52kb	...
generic	logs	default	log	log	Jan 18, 2025 @ 11:32:22 AM	94.71kb	...
docker.event	metrics	default	docker	docker	Jan 18, 2025 @ 11:06:00 AM	24.08kb	...
windows.powershell	logs	default	windows	windows	Jan 18, 2025 @ 9:54:14 AM	87.4kb	...
windows.powershell_operational	logs	default	windows	windows	Jan 18, 2025 @ 1:31:22 AM	27.58kb	...

Rows per page: 20 ▾

◀ 1 2 ▶

[View all agent policies](#)

## Políticas DMZ

Políticas para servidores en DMZ

[Integrations](#) [Settings](#)

Revision 9 | Integrations 4 | Agents 1 agent | Last updated on Jan 18, 2025

Actions ▾

Integration policy	Integration	Namespace	Output	Actions
docker-1	Docker v2.13.1	default	Default output	...
log-1	Custom Logs v2.3.3	default	Default output	...
log-2	Custom Logs v2.3.3	default	Default output	...
system-1 (copy)	System v1.63.2	default	Default output	...