

KeepCoding Bootcamp Ciberseguridad | Edición IX

Módulo de Blue Team

Informe Práctica Blue Team

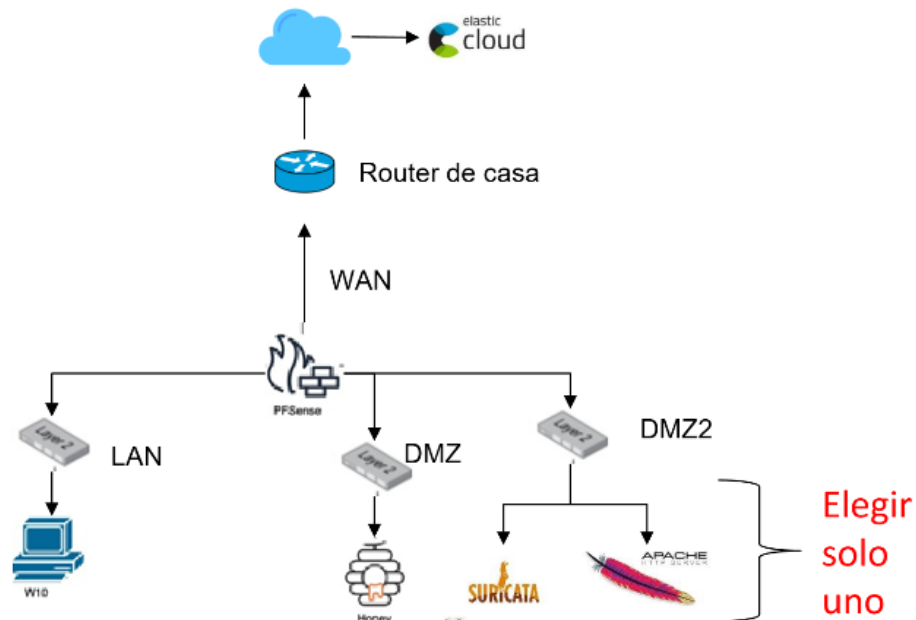
Por: Oscar Uriel Tobar Rios

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.

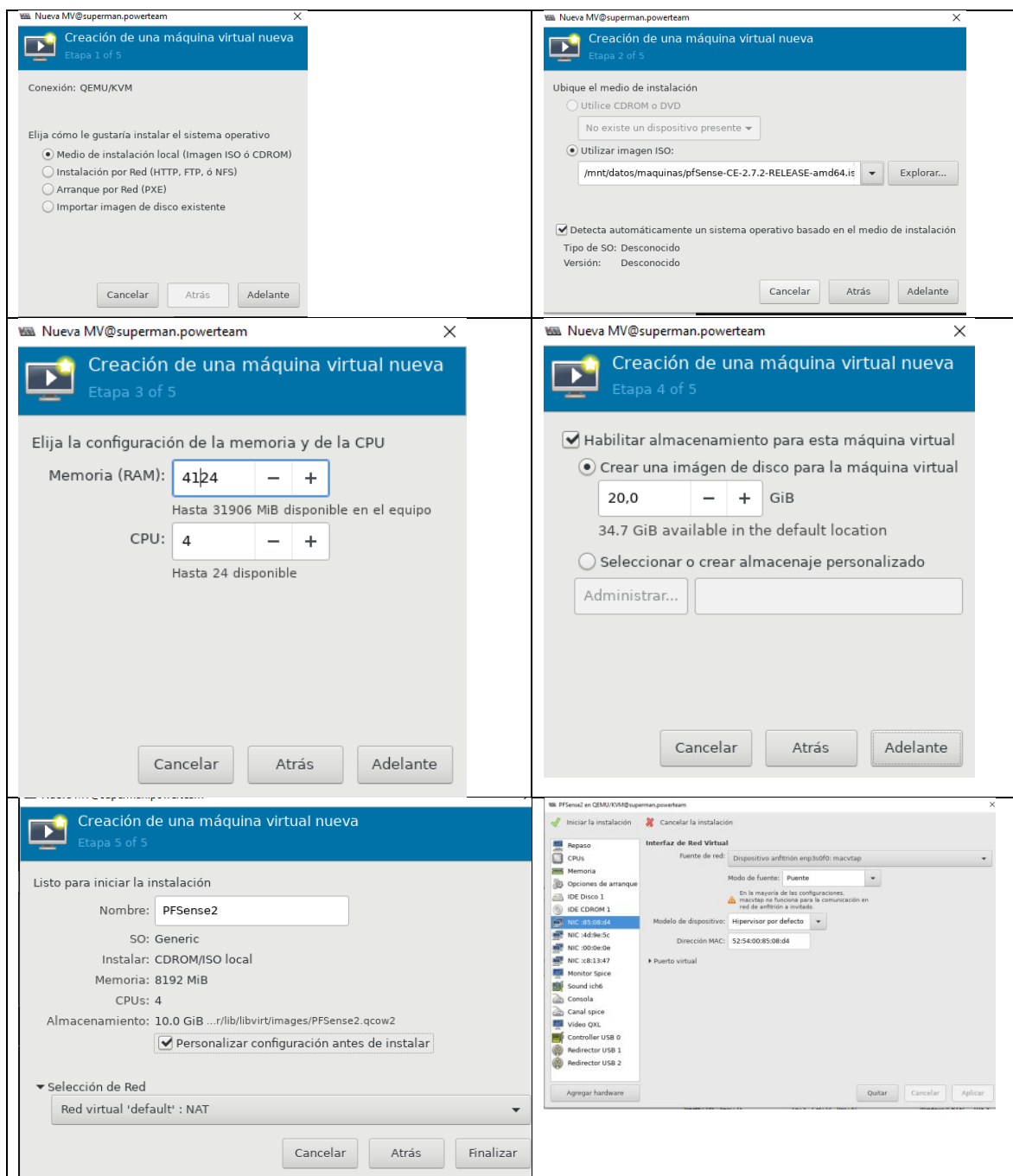
2 PFSense

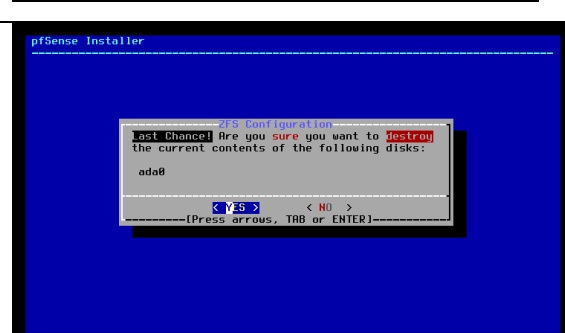
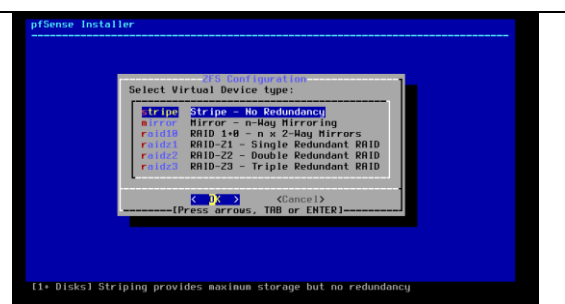
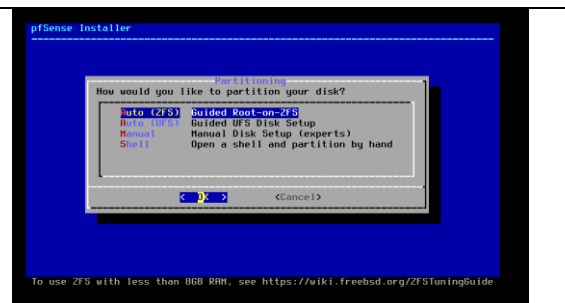
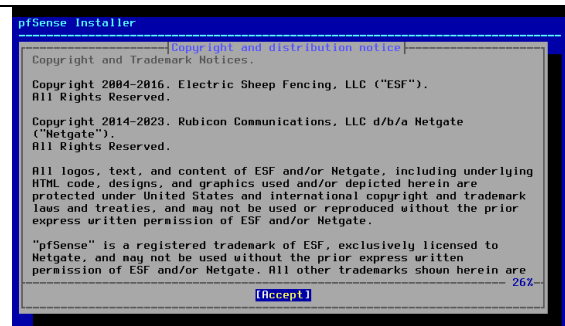
Para poder desarrollar el ejercicio lo primero fue hacer la instalación de PFSense. Se utilizó la versión pfSense-CE-2.7.2 y se instaló en una máquina Oracle Linux sobre el virtualizador

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:



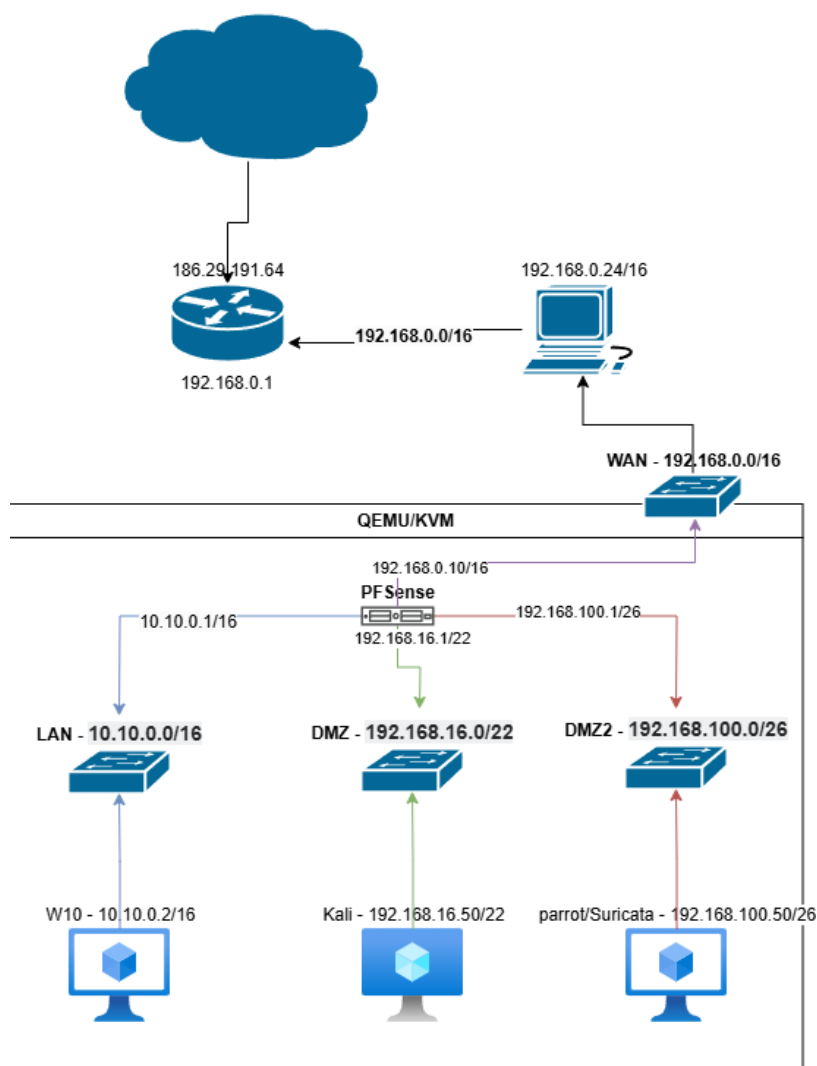


2.2 Configuración

Después de instalar PFSense las tarjeta 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 for the DNS Resolver General Settings. At the top, a navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this, a breadcrumb trail reads 'Services / DNS Resolver / General Settings'. A yellow warning banner 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.' The settings are organized into tabs: General Settings (selected), Advanced Settings, and Access Lists. The 'General DNS Resolver Options' section includes: 'Enable' with a checked 'Enable DNS resolver' checkbox; 'Listen Port' set to 53; 'Enable SSL/TLS Service' with a checked 'Respond to incoming SSL/TLS queries from local clients' checkbox; 'SSL/TLS Certificate' set to 'GUI default (678480beb2b79)'; 'SSL/TLS Listen Port' set to 853; 'Network Interfaces' with a list containing 'All', 'WAN', 'LAN', 'DMZ', and 'DMZ2'; and 'Outgoing Network' set to 'All'. Descriptive text for each field explains its function and default behavior.

This section continues the configuration from the previous screenshot. It includes: 'Outgoing Network Interfaces' with a list containing 'All', 'WAN', 'LAN', 'DMZ', and 'DMZ2'; 'Strict Outgoing Network Interface Binding' with an unchecked checkbox and explanatory text; 'System Domain Local Zone Type' set to 'Transparent'; 'DNSSEC' with an unchecked 'Enable DNSSEC Support' checkbox; 'Python Module' with an unchecked 'Enable Python Module' checkbox; 'DNS Query Forwarding' with a checked 'Enable Forwarding Mode' checkbox and a sub-section for 'Use SSL/TLS for outgoing DNS Queries to Forwarding Servers' which is currently unchecked; and 'DHCP Registration' with an unchecked 'Register DHCP leases in the DNS Resolver' checkbox. A watermark 'Activar Windows' is visible in the bottom right corner.

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 estableció 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

LAN

DMZ

DMZ2

General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on LAN interface

BOOTP

☐ Ignore BOOTP queries

Deny Unknown Clients

Allow all clients

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

10.10.0.0/16

Subnet Range

10.10.0.1 - 10.10.255.254

Address Pool Range

10.10.0.10

10.10.255.245

From

To

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

10.10.0.1

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

Generate a new key based on the selected algorithm.

Key Algorithm

HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

Other DHCP Options

Gateway

10.10.0.1

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.

2.2.5 Configuración REGLAS FIREWALL LAN

En el caso de las reglas de firewall para la red LAN se adicionamos 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"/>	0/0 B	IPv4 TCP	LAN subnets	*	LAN subnets	Webs	*	none			
<input type="checkbox"/>	32/3.85 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input 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 identificado internamente como RE2 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 192.168.16.0/22 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	<input checked="" type="checkbox"/> Enable DHCP server on DMZ interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients</div> <p>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.</p>
Ignore Denied Clients	<input type="checkbox"/> 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	<input type="checkbox"/> 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	192.168.16.0/22
Subnet Range	192.168.16.1 - 192.168.19.254
Address Pool Range	<div>192.168.16.10</div> From <div>192.168.16.50</div> To
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	<div>+ Add Address Pool</div> <p>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</p>

Server Options

WINS Servers	<div>WINS Server 1</div> <div>WINS Server 2</div>
DNS Servers	<div>192.168.16.1</div> <div>8.8.8.8</div> <div>1.1.1.1</div> <div>DNS Server 4</div>

OMAPI

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

Other DHCP Options

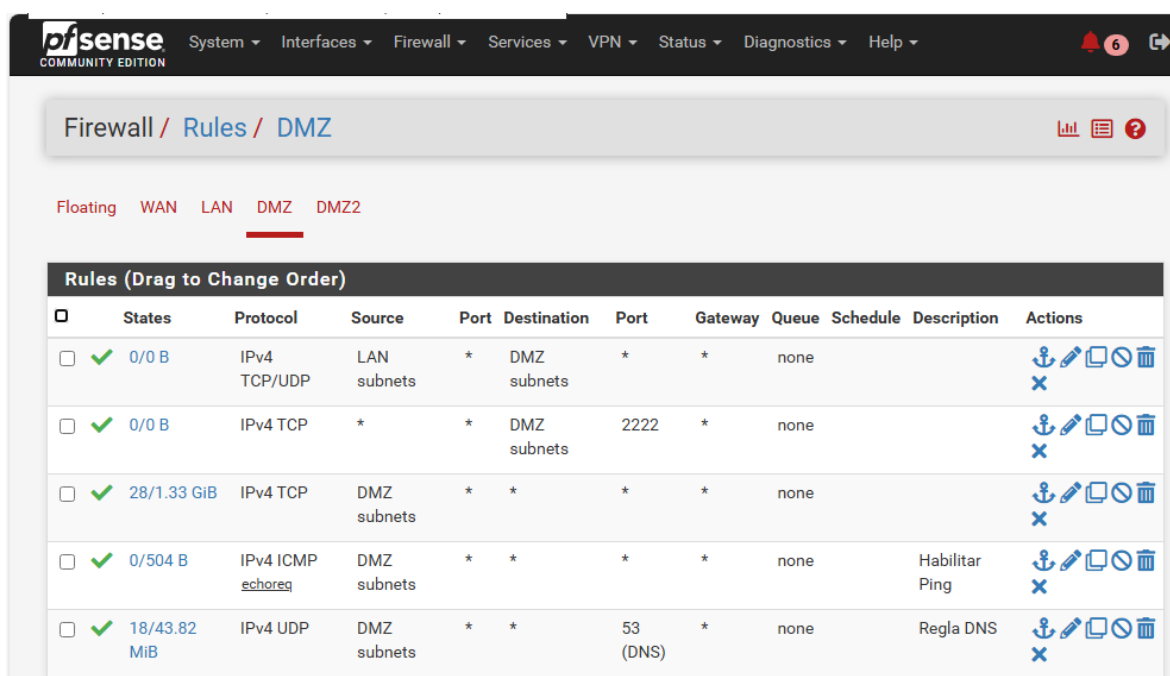
Gateway	<div>192.168.16.1</div> <p>The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter 'none' for no gateway assignment.</p>
Domain Name	<div>practical.blue</div> <p>The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.</p>
Domain Search List	<div>example.com;sub.example.com</div>

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 Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation is 'Firewall / Rules / DMZ'. Below the navigation, there are tabs for 'Floating', 'WAN', 'LAN', 'DMZ', and 'DMZ2', with 'DMZ' currently selected. The main area displays a table of rules under the heading 'Rules (Drag to Change Order)'. The table has columns for 'States', 'Protocol', 'Source', 'Port', 'Destination', 'Port', 'Gateway', 'Queue', 'Schedule', 'Description', and 'Actions'. There are five rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP/UDP	LAN subnets	*	DMZ subnets	*	*	none			[Anchor] [Edit] [Copy] [Delete]
0/0 B	IPv4 TCP	*	*	DMZ subnets	2222	*	none			[Anchor] [Edit] [Copy] [Delete]
28/1.33 GiB	IPv4 TCP	DMZ subnets	*	*	*	*	none			[Anchor] [Edit] [Copy] [Delete]
0/504 B	IPv4 ICMP <u>echo req</u>	DMZ subnets	*	*	*	*	none		Habilitar Ping	[Anchor] [Edit] [Copy] [Delete]
18/43.82 MiB	IPv4 UDP	DMZ subnets	*	*	53 (DNS)	*	none		Regla DNS	[Anchor] [Edit] [Copy] [Delete]

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

LAN

DMZ

DMZ2

General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on DMZ2 interface

BOOTP

☐ Ignore BOOTP queries

Deny Unknown Clients

Allow all clients

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

192.168.100.10

From

192.168.100.50

To

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	<div>OMAPI Key</div> <div>Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.</div> <div><input type="checkbox"/> Generate New Key Generate a new key based on the selected algorithm.</div>
Key Algorithm	<div>HMAC-SHA256 (current bind9 default)</div> <div>Set the algorithm that OMAPI key will use.</div>
Other DHCP Options	
Gateway	<div>192.168.100.1</div> <div>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.</div>
Domain Name	<div>practica1.blue</div> <div>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.</div>

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 <u>echo req</u>	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=U0dPLWJaUUJPN2RlbDhwczQybjE6aDZXZyQtR0tSYXlpdTN6QU01ekN3QQ==
```

[View all agents](#)

DESKTOP-PGGB831

Actions

Agent detailsLogsDiagnostics

Overview

CPU

1.82 %

View more agent metrics

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:

[Cancel](#)

Windows

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

☐ Preserve original event

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

> Advanced options

☐ AppLocker/MSI and Script

Microsoft-Windows-AppLocker/MSI and Script channel

☐ Preserve original event

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

> Advanced options

☐ 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.original

☒
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
Collect Windows service metrics

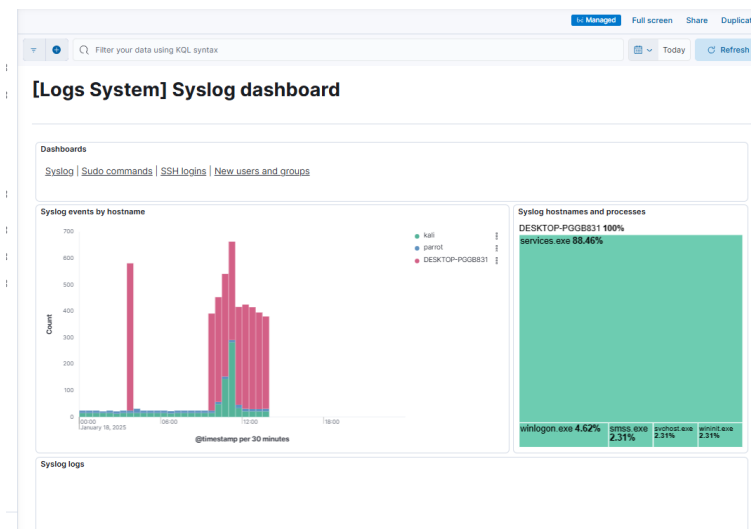
Period

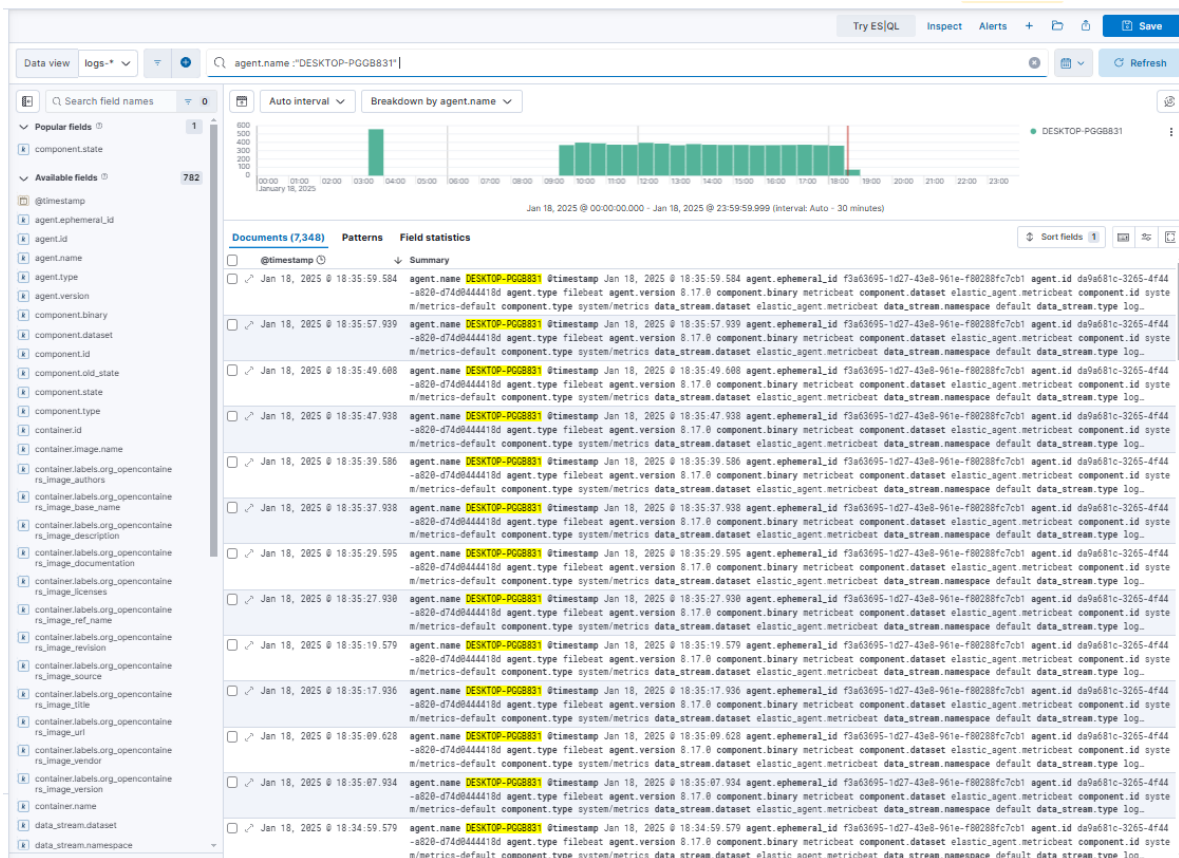
60s

Processors

Optional

3.1.2 Evidencias de recepción de logs





Se deja un ejemplo de uno de los mensajes en

https://github.com/oscartobar/practicaskkeepcoding/blob/main/BlueTeam/evidenciaswindow_s.txt

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/practicaskkeepcoding/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 HonetPod 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                  CREATED        STATUS      PORTS
b84ed29c370f   cowrie/cowrie:latest   "/cowrie/cowrie-env/..." 15 minutes ago 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=QTJNMWJKUUJPN2RibDhwc2tXbFU6ZVlGSWIHZGJTbFNKajhETWInd2J5dw==`

```

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=U0dPLWJaUUJPN2RI
2R1b0nwcZQybjE6aDZXYzQtR0tSYXlpdTN6QU01ekN3QQ==
". 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=U0dPLWJaUUJPN2RI
bDhwczQybjE6aDZXYzQtR0tSYXlpdTN6QU01ekN3QQ==
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":{"functi
on":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cm
d.go","file.line":520},"message":"Starting enrollment to URL: https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.a
ws.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":{"functi
on":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enr
oll_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-age
nt/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

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

Log file path

/home/kali/logs/ssh/cowrie.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 x

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 v

☒ 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 x

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

Description

Optional

> Advanced options

☒ Custom log file
Change defaults ^

Log file path

+ Add row
Path to log files to be collected

Dataset name

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

Politicas DMZ x

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 asi:

```

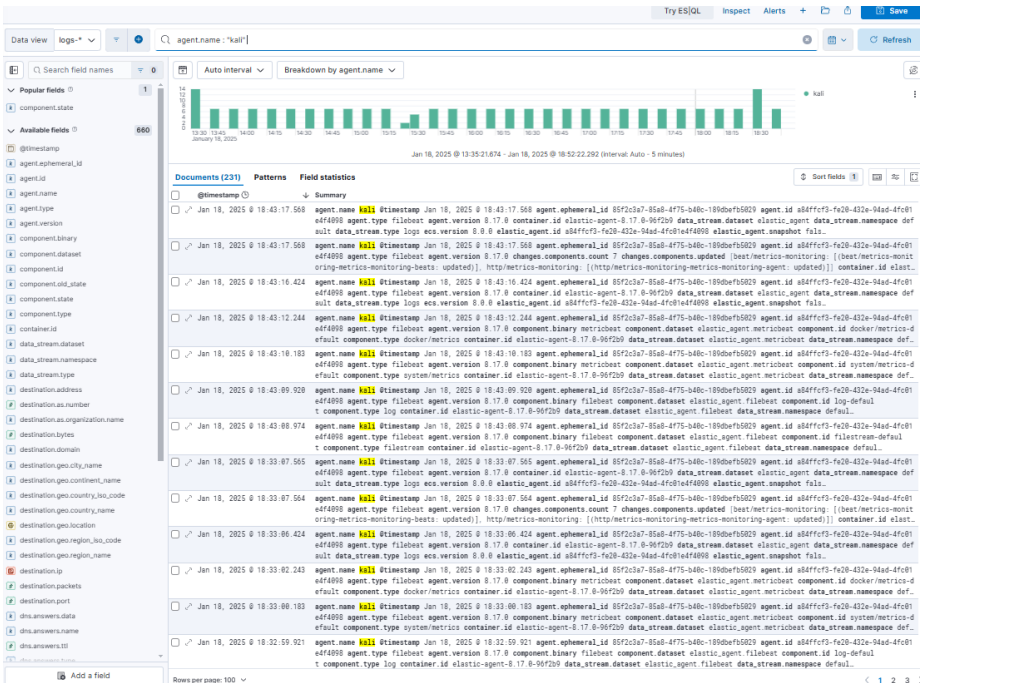
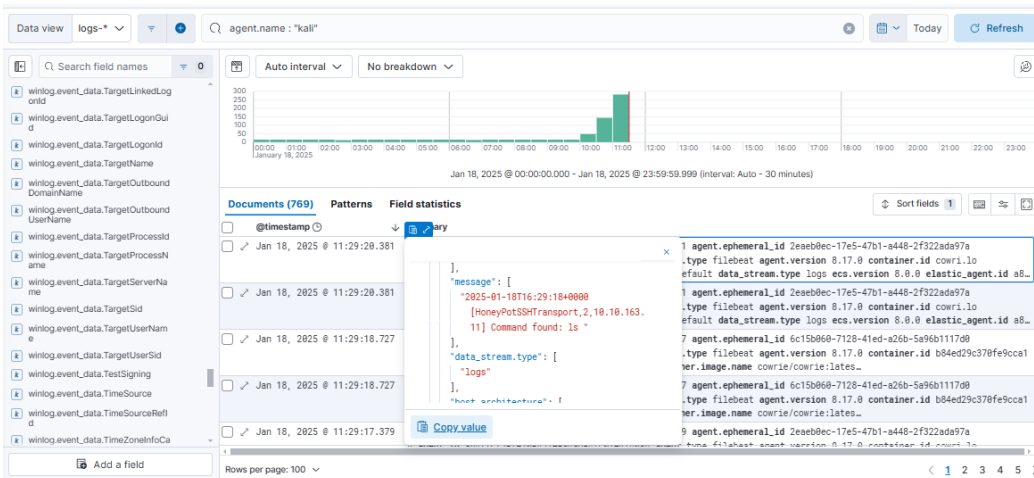
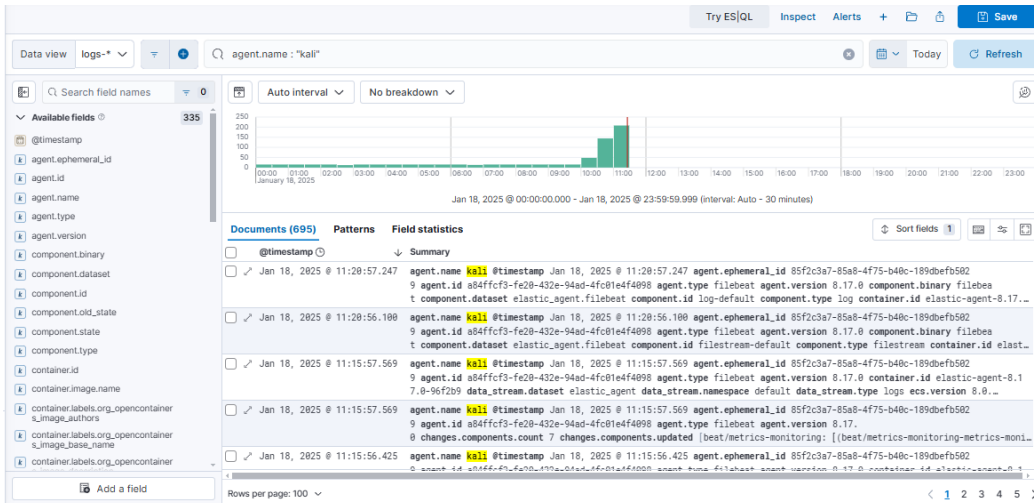
C:\Users\PC\.ssh>ssh root@192.168.16.50 -p 2222
root@192.168.16.50's password:

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#

```

☐ ☒ 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/practicaskkeepcoding/blob/main/BlueTeam/evidenciassh1.txt>

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

3.3 Configuración Suricata (DMZ2)

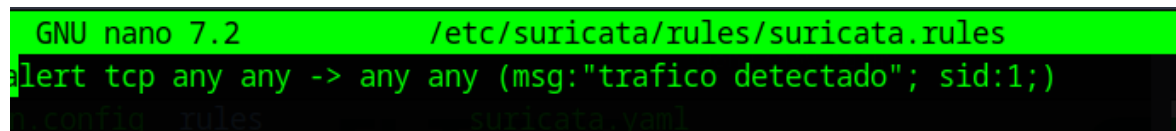
3.3.1 Configuración Suricata

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=QTJNMWJKUUJPN2RibDhwc2tXbFU6ZVlGSWIHZGJTbFNKajhETWInd2J5dw==
```


Luego desde Elastic se configuro una nueva integración asi

[View all agent policies](#)

Revision 6 | Integrations 2 | Agents 1 agent | Last updated on Jan 16, 2025 | [Actions](#)

Linux/Suricata

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

Namespace [▼](#)

[+ Add integration](#)

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

1 Configure integration

Integration settings

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

Integration name

suricata-2

Description

Optional

[Advanced options](#)

☒ Collect Suricata eve logs (input: logfile)

[Change defaults](#) [^](#)

☒ Suricata eve logs (log)

Collect Suricata eve logs using log input

Paths

/var/log/suricata/eve.json

[Add row](#)

Preserve original event

☐

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

[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.

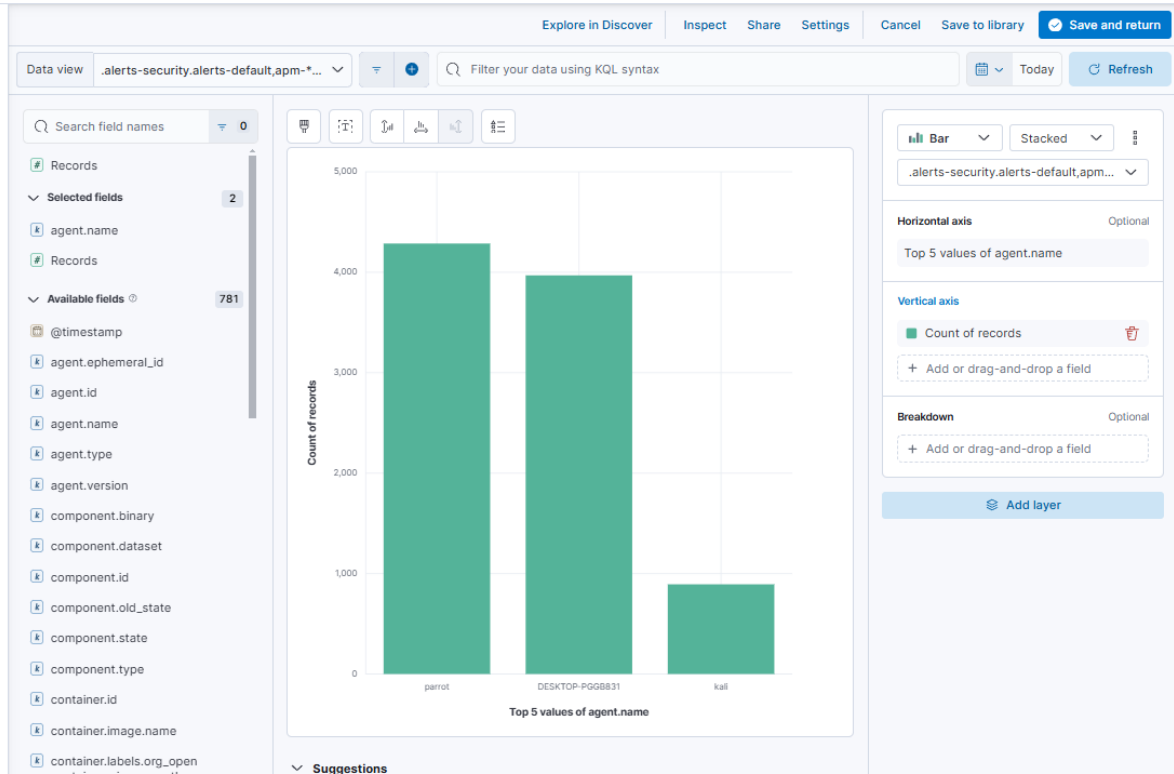
Agent policies

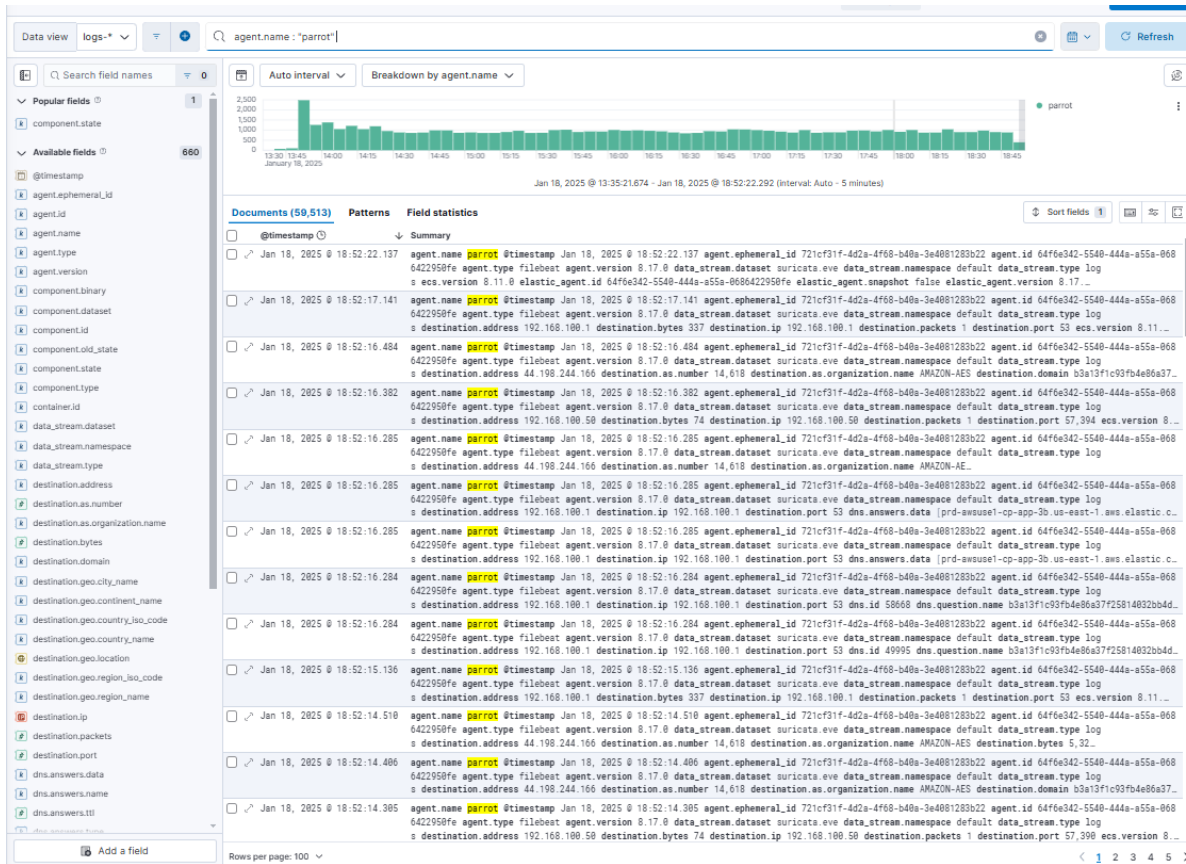
Linux/Suricata [×](#)

[×](#) [▼](#)

1 agent is enrolled with the selected agent policies.

3.3.3 Evidencias de recepción de logs





La información de un mensaje lo puede ver aqui

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

3.4 Agentes

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

[Send feedback](#)

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

Status 4Tags 0Agent policy 3Upgrade available

Showing 3 agents

Clear filters

Healthy 3Unhealthy 0Updating 0Offline 0Inactive 0Unenrolled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last acti...	Version	Actions
<input type="checkbox"/>	Healthy	DESKTOP-PGGB831	Politicas LAN rev. 2	1.74 %	170 MB	25 seconds ago	8.17.0	...
<input type="checkbox"/>	Healthy	parrot	Linux/Suricata rev. 6	2.70 %	233 MB	16 seconds ago	8.17.0	...
<input type="checkbox"/>	Healthy	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](#)

ReloadCreate 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

🔍

Filter data streams

Dataset ▾

Type ▾

Namespace ▾

Integration ▾

🔄 Reload

Dataset ⌵	Type ⌵	Namespace ⌵	Integration ⌵	Last activity ⌵	Size ⌵	Actions
elastic_agent.elastic_agent	metrics	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	37.11mb	...
elastic_agent.filebeat	metrics	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	18.03mb	...
elastic_agent.filebeat_input	metrics	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	7.26mb	...
elastic_agent.metricbeat	metrics	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	31.61mb	...
windows.service	metrics	<div>default</div>	windows	Jan 18, 2025 @ 2:18:15 PM	47.79mb	...
fleet_server.agent_status	metrics	<div>default</div>	fleet_server	Jan 18, 2025 @ 2:17:40 PM	1.18mb	...
fleet_server.agent_versions	metrics	<div>default</div>	fleet_server	Jan 18, 2025 @ 2:17:40 PM	686.23kb	...
system.application	logs	<div>default</div>	system	Jan 18, 2025 @ 2:17:36 PM	1.04mb	...
elastic_agent	logs	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.18mb	...
elastic_agent.filebeat	logs	<div>default</div>	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.32mb	...
system.security	logs	<div>default</div>	system	Jan 18, 2025 @ 2:12:36 PM	19.72mb	...
system.system	logs	<div>default</div>	system	Jan 18, 2025 @ 12:43:43 PM	597.16kb	...
docker.container_logs	logs	<div>default</div>	docker	Jan 18, 2025 @ 11:32:22 AM	390.52kb	...
generic	logs	<div>default</div>	log	Jan 18, 2025 @ 11:32:22 AM	94.71kb	...
docker.event	metrics	<div>default</div>	docker	Jan 18, 2025 @ 11:06:00 AM	24.08kb	...
windows.powershell	logs	<div>default</div>	windows	Jan 18, 2025 @ 9:54:14 AM	87.4kb	...
windows.powershell_operational	logs	<div>default</div>	windows	Jan 16, 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 ▼

<input type="text" value="Search..."/>					Namespace ▼	<button>Add integration</button>	
Integration policy ⬆	Integration ⌵	Namespace		Output		Actions	
docker-1	Docker v2.13.1	<div>default</div> ⓘ		<div>Default output</div> ⓘ		...	
log-1	Custom Logs v2.3.3	<div>default</div> ⓘ		<div>Default output</div> ⓘ		...	
log-2	Custom Logs v2.3.3	<div>default</div> ⓘ		<div>Default output</div> ⓘ		...	
system-1 (copy)	System v1.63.2	<div>default</div>		<div>Default output</div> ⓘ		...	