

KeepCoding Bootcamp Ciberseguridad | Edición IX

Módulo de Blue Team

Informe Práctica Blue Team SEGUNDA ENTREGA

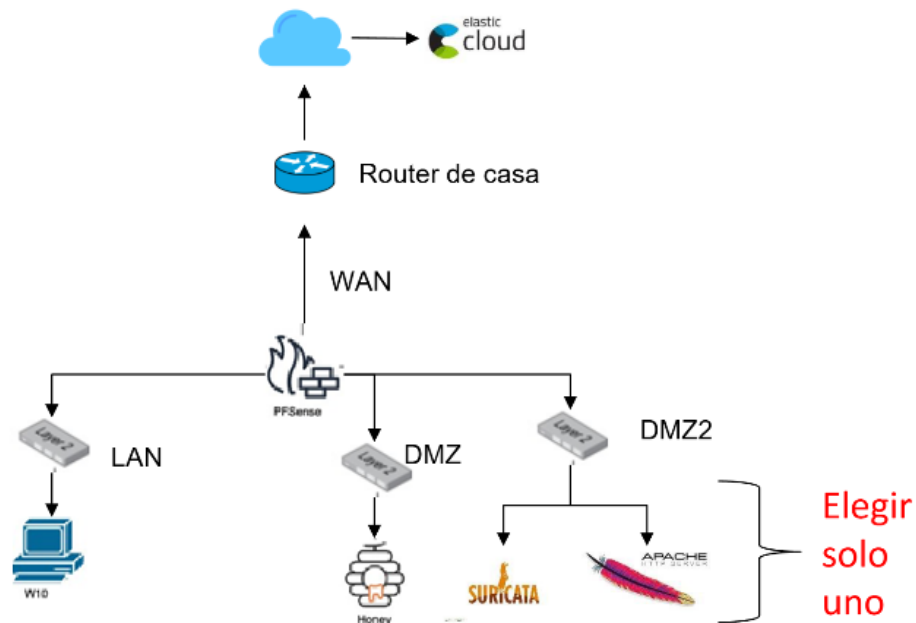
Por: Oscar Uriel Tobar Rios

Fecha del Informe: 26/01/2025

Contenido

1	PFSense	3
1.1	Instalación	3
1.2	Configuración	6
1.2.1	Configuración DNS	6
1.2.2	Configuración WAN	7
1.2.3	Configuración Firewall WAN	8
1.2.4	Configuración Firewall NAT Port Forward	8
1.2.5	Configuración LAN	8
1.2.6	Configuración DHCP LAN	9
1.2.7	Configuración REGLAS FIREWALL LAN	10
1.2.8	Configuración DMZ	11
1.2.9	Configuración DHCP DMZ	11
1.2.10	Configuración REGLAS FIREWALL DMZ	13
1.2.11	Configuración DMZ2	13
1.2.12	Configuración DHCP DMZ2	14
1.2.13	Configuración REGLAS FIREWALL DMZ2	15
2	SIEM (Elastic)	16
2.1	Configuración Windows 10 (LAN)	16
2.1.1	Configuración del Agente	16
2.1.2	Evidencias de recepción de logs	18
2.2	Configuración Honey (DMZ)	19
2.2.1	Configuración del HoneyPod	19
2.2.2	Configuración del Agente	20
2.2.3	Evidencias de recepción de logs	22
2.3	Configuración Suricata (DMZ2)	23
2.3.1	Configuración Suricata	23
2.3.2	Configuración del Agente	23
2.3.3	Evidencias de recepción de logs	25
2.4	Agentes	25

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.

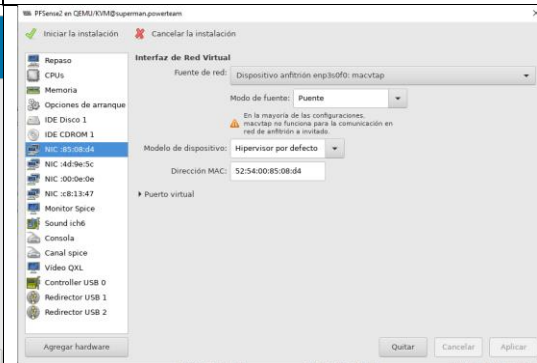
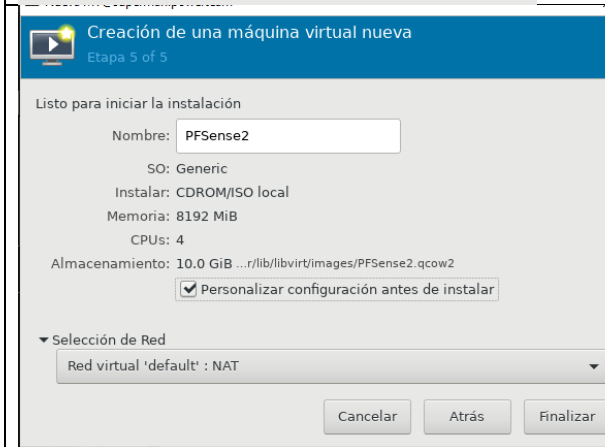
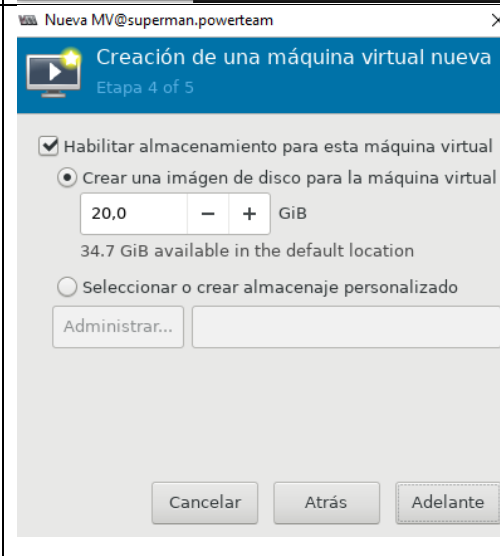
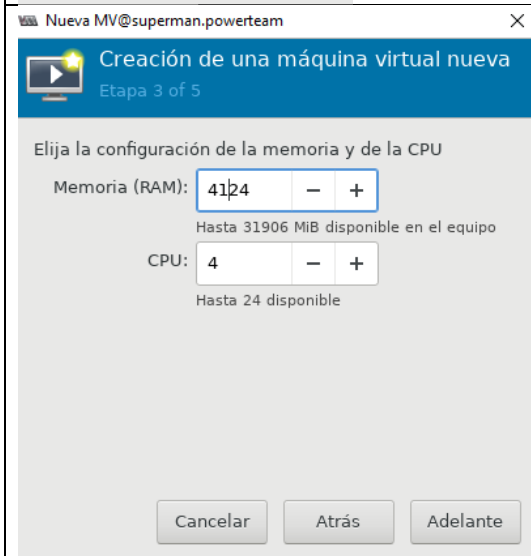
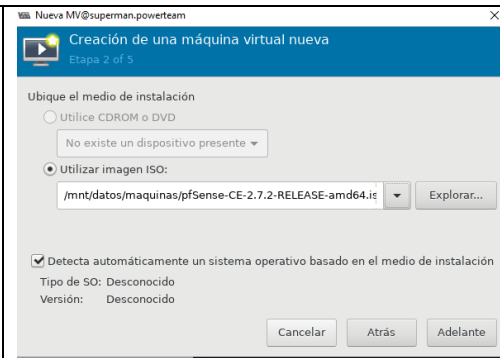
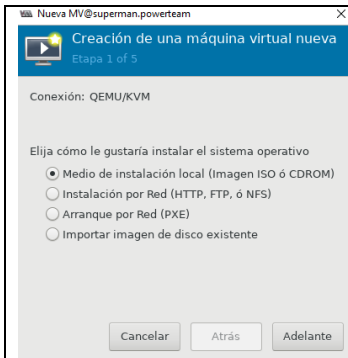
1 PFSense

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

1.1 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 máquina virtual de Pfsense se habilitaron 4 tarjetas de red y se ejecutó la instalación como se muestra a continuación:



1.2 Configuración

Después de instalar PFSense las tarjeta de Red detectados son las siguientes:

Interface	Network port
WAN	re0 (52:54:00:a1:67:4f)
LAN	re1 (52:54:00:2a:d1:df) Delete
DMZ	re2 (52:54:00:83:a4:f0) Delete
DMZ2	re3 (52:54:00:3d:29:27) Delete

Save

1.2.1 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:

Services / DNS Resolver / General Settings

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.

General Settings / Advanced Settings / Access Lists

General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

Network Interfaces
WAN
LAN
DMZ
DMZ2
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Outgoing Network

Network Interfaces	<div> <div>All</div> <div>WAN</div> <div>LAN</div> <div>DMZ</div> <div>DMZ2</div> </div> <p>Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.</p>
Outgoing Network Interfaces	<div> <div>All</div> <div>WAN</div> <div>LAN</div> <div>DMZ</div> <div>DMZ2</div> </div> <p>Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.</p>
Strict Outgoing Network Interface Binding	<input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available. By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
System Domain Local Zone Type	<div>Transparent</div> <p>The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default.</p>
DNSSEC	<input type="checkbox"/> Enable DNSSEC Support
Python Module	<input type="checkbox"/> Enable Python Module Enable the Python Module.
DNS Query Forwarding	<input checked="" type="checkbox"/> Enable Forwarding Mode If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers 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.
DHCP Registration	<input type="checkbox"/> Register DHCP leases in the DNS Resolver If this option is set, then machines that register their hostnames when requesting an IP via DHCP lease will be registered in the DNS Resolver.

1.2.2 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:a1:4f

Red: 192.168.0.0/24

IP: 192.168.0.13

1.2.3 Configuración Firewall WAN

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/12 KiB	IPv4 TCP	*	*	*	222	*	none	Ingreso al Honey	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.200.101	222	*	none	NAT	

Add Add Delete Toggle Copy Save Separator

1.2.4 Configuración Firewall NAT Port Forward

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt

Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	222	192.168.200.101	222	

Add Add Delete Toggle Save Separator

1.2.5 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: 52:54:00:2a:d1:df

Red: 192.168.100.1/24

Rango de IPs: 192.168.100.1 – 192.168.100.254

IP:192.168.100.1

1.2.6 Configuración DHCP LAN

Adicionalmente se configuro un servidor DHCP para que entregue direcciones en el rango 192.168.100.10 – 192.168.100.200

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

192.168.100.0/24

Subnet Range

192.168.100.1 - 192.168.100.254

Address Pool Range

192.168.100.10

From

192.168.100.200

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

1.1.1.1

8.8.8.8

DNS Server 4

Activar Windows
Ve a Configuración para activar Windows

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

☐ Generate New Key
Generate a new key based on the selected algorithm.

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

keepcoding.local

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

The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default Lease Time

7200

This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum Lease Time

86400

This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

1.2.7 Configuración REGLAS FIREWALL LAN

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

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/4.93 MIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ 0/14 KiB	IPv4 TCP	LAN subnets	*	DMZ2 subnets	22 (SSH)	*	none		Permite conectarse al SSH del Suricata	
✓ 0/0 B	IPv4 TCP	LAN subnets	*	DMZ subnets	22 (SSH)	*	none		Permite conectarse al SSH del Honey	
✓ 0/508 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	
✓ 33/132.65 MIB	IPv4 TCP	*	*	*	sitiosweb	*	none		Trafico Web	
✓ 0/9.18 MIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
✗ 0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Bloquear otros puertos de la DMZ	
✗ 0/0 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Bloquear otros puertos de la DMZ2	

Add

Add

Delete

Toggle

Copy

Save

Separator

Nota: se han creado reglas para la administración de las máquinas por SSH desde la red LAN.

1.2.8 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 192.168.200.1/24

Nombre: DMZ

Id: re2

Tipo: Interna

Mac: 52:54:00:83:a4:f0

Red: 192.168.200.1/24

Rango de IPs: 192.168.200.1 - 192.168.200.254

IP: 192.168.200.1

1.2.9 Configuración DHCP DMZ

Se configuro un servidor DHCP para la red de DMZ que entregue direcciones en el rango 192.168.200.100 hasta el 192.168.200.150

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

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	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	<div>192.168.200.100192.168.200.150</div> <div>FromTo</div> <div>The specified range for this pool must not be within the range configured on any other address pool for this interface.</div>
Additional Pools	<div><div>+ Add Address Pool</div><div>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</div></div>
Server Options	
WINS Servers	<div>WINS Server 1</div> <div>WINS Server 2</div>
DNS Servers	<div>192.168.200.1</div> <div>1.1.1.1</div> <div>8.8.8.8</div> <div>DNS Server 4</div>

Activar Windows
Ve a Configuración para
Windows.

Other DHCP Options	
Gateway	<div>192.168.200.1</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>keepcoding.local</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>
Domain Search List	<div>example.com;sub.example.com</div> <div>The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.</div>
Default Lease Time	<div>7200</div> <div>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</div>
Maximum Lease Time	<div>86400</div> <div>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</div>
Failover peer IP	<div></div> <div>Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.</div>
Static ARP	<div><input type="checkbox"/> Enable Static ARP entries</div> <div>Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.</div>
Time format change	<div><input checked="" type="checkbox"/> Change DHCP display lease time from UTC to local time</div> <div>By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.</div>

Activar Windows
Ve a Configuración para a

1.2.10 Configuración REGLAS FIREWALL DMZ

Para las reglas del DMZ se establecieron cuatro reglas así:

Firewall / Rules / DMZ

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloqueo red lan	
<input type="checkbox"/>	✗ 0/17 KiB	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloqueo red DMZ2	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	192.168.200.101	*	*	none		Habilita todos los puertos a la maquina hony	
<input type="checkbox"/>	✓ 39/202 KiB	IPv4 UDP	192.168.200.101	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	
<input type="checkbox"/>	✓ 51/4.16 MiB	IPv4 TCP	192.168.200.101	*	*	sitiosweb	*	none		Permitir trafico web	

Add Add Delete Toggle Copy Save Separator

Ve a Configuración para activar

1.2.11 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 (192.168.250.1).

Nombre: DMZ2

Id: re3

Tipo: Interna

Mac: 52:54:00:3d:29:27

Red: 192.168.250.1/24

Rango de IPs: 192.168.250.1 - 192.168.250.254

IP: 192.168.250.1

1.2.12 Configuración DHCP DMZ2

Se configuro un servidor DHCP para la red de DMZ2 que entregue direcciones en el rango 192.168.250.100 hasta el 192.168.250.150

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ2 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	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	<div>192.168.250.100192.168.250.150</div> <div>FromTo</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
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>192.168.250.1</div> <div>1.1.1.1</div> <div>8.8.8.8</div> <div>DNS Server 4</div>

Activar Windows
Ve a Configuración para activar Windows.

Other DHCP Options

Gateway

192.168.250.1

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

keepcoding.local

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

The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default Lease Time

7200

This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum Lease Time

86400

This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Failover peer IP

Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.

Static ARP

☐ Enable Static ARP entries

Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.

Time format change

☒ Change DHCP display lease time from UTC to local time

By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.

1.2.13 Configuración REGLAS FIREWALL DMZ2

Para las reglas del DMZ2 se establecieron dos reglas asi:

Firewall / Rules / DMZ2

Floating

WAN

LAN

DMZ

DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloqueo red DMZ	
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloqueo red LAN	
<input type="checkbox"/>	22/1.41 MiB	IPv4 TCP	DMZ2 subnets	*	*	sitiosweb	*	none		Trafico web	
<input type="checkbox"/>	32/126 KiB	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	

Add

Add

Delete

Toggle

Copy

Save

Separator

2 SIEM (Elastic)

Basados en la configuración establecida como se muestra a continuación

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

WAN (wan)      -> re0      -> v4/DHCP4: 192.168.0.13/24
LAN (lan)      -> re1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> re2      -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> re3      -> v4: 192.168.250.1/24

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

Enter an option: █
```

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

2.1 Configuración Windows 10 (LAN)

2.1.1 Configuración del Agente

En una máquina 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](#)

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

> Advanced options

☒ Collect Windows perfmom and service metrics
 [Change defaults](#)

☒ Windows perfmom metrics
Collect Windows perfmom metrics

☒ Perfmom Group Measurements By Instance
Enabling this option will send all measurements with a matching perfmom instance as part of a single event

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

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

Perfmom Queries

```

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

Will list the perfmom 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

2.1.2 Evidencias de recepción de logs

The screenshot displays a log management interface. At the top, there's a search bar with 'windowd' entered. Below the search bar, a bar chart shows log volume over time, with a peak around 07:00. The chart is titled 'Jan 26, 2025 @ 00:00:00.000 - Jan 26, 2025 @ 23:59:59.999 (Interval: Auto - 30 minutes)'. Below the chart, a table lists log documents. The first document is a summary of the search results, showing 9,311 documents. The second document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The third document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The fourth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The fifth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The sixth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The seventh document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The eighth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The ninth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type. The tenth document is a log entry from a Windows host, showing details like host name, platform, timestamp, agent name, and component type.

Se deja un ejemplo de uno de los mensajes en

<https://github.com/oscartobar/practicaskkeepcoding/blob/main/BlueTeam/evidenciaswindow s3.txt>

EL archivo comprimido con todos los mensajes desde la maquina Windows recibidos en Elastic y exportado para el día 26 de Enero es este

<https://github.com/oscartobar/practicaskkeepcoding/blob/main/BlueTeam/windows3.zip>

2.2 Configuración Honey (DMZ)

2.2.1 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),
```

2.2.2 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=QTNJNMWJKUUJPN2RlBdhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==
```

```
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=U0dPLWJaUUJPN2RlBdhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==
"." 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=U0dPLWJaUUJPN2RlBdhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==
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

[View all agents](#)

kali

Agent detailsLogsDiagnostics

Actions

Overview

CPU ⓘ2.19 %

View more agent metrics

Memory ⓘ252 MB

Status

Healthy

Last activity21 seconds ago

Last checkin messageRunning

Agent IDa84ffc3-3e20-432e-94ad-4fc01e4f4098

Agent policyPoliticas DMZ rev. 12

Agent version8.17.0

Upgrade available

Host namekali

Host ID30e662c5c81d4191bd244a79c97d2e0

Output for integrationsDefault output

Output for monitoringDefault output

Logging levelinfo

Privilege modeRunning as root

Agent releasestable

Platformkali

Monitor logsEnabled

Integrations

> docker-1

> system-1 (copy)

> log cowri

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

Integration ssh

Optional

[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

Politicas DMZ x

1 agent is enrolled with the selected agent policies.

2.2.3 Evidencias de recepción de logs

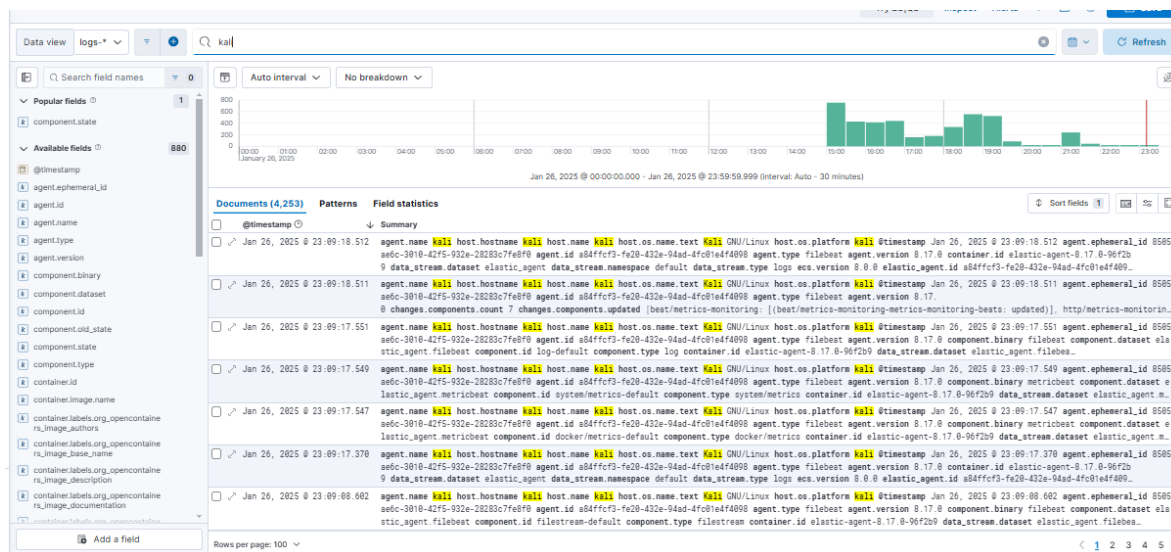
Para el ejemplo se utilizó el honeyPod del ssh instalado para evidenciar que si se genera el log y se transmitió al elastic asi:

```
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/evidenciassh3.txt>

El archivo comprimido con todos los mensajes desde la maquina Kali recibidos en Elastic y exportado para el día 26 de Enero es este

<https://github.com/oscartobar/practicaskkeepcoding/blob/main/BlueTeam/kali-ssh3.csv>

2.3 Configuración Suricata (DMZ2)

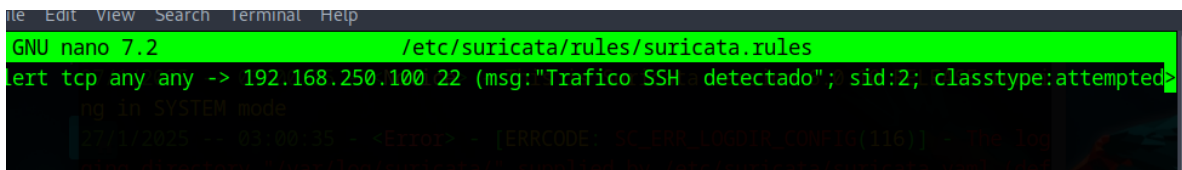
2.3.1 Configuración Suricata

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

A screenshot of a terminal window with a dark background. At the top, a green status bar shows 'GNU nano 7.2' and the file path '/etc/suricata/rules/suricata.rules'. Below this, a rule is being edited: 'alert tcp any any -> 192.168.250.100 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted...'. The text is partially obscured by a dark overlay on the right side of the image.

```
GNU nano 7.2 /etc/suricata/rules/suricata.rules
alert tcp any any -> 192.168.250.100 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted...
```

Luego como administrador se inicio el programa asi:

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

2.3.2 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=QTJNMWJKUUJPN2RibDhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==
```

Luego desde Elastic se configuro una nueva integración asi

[View all agent policies](#)

Revision6Integrations2Agents1 agentLast updated onJan 16, 2025Actions

Linux/Suricata

IntegrationsSettings

Search...NamespaceAdd integration

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

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.

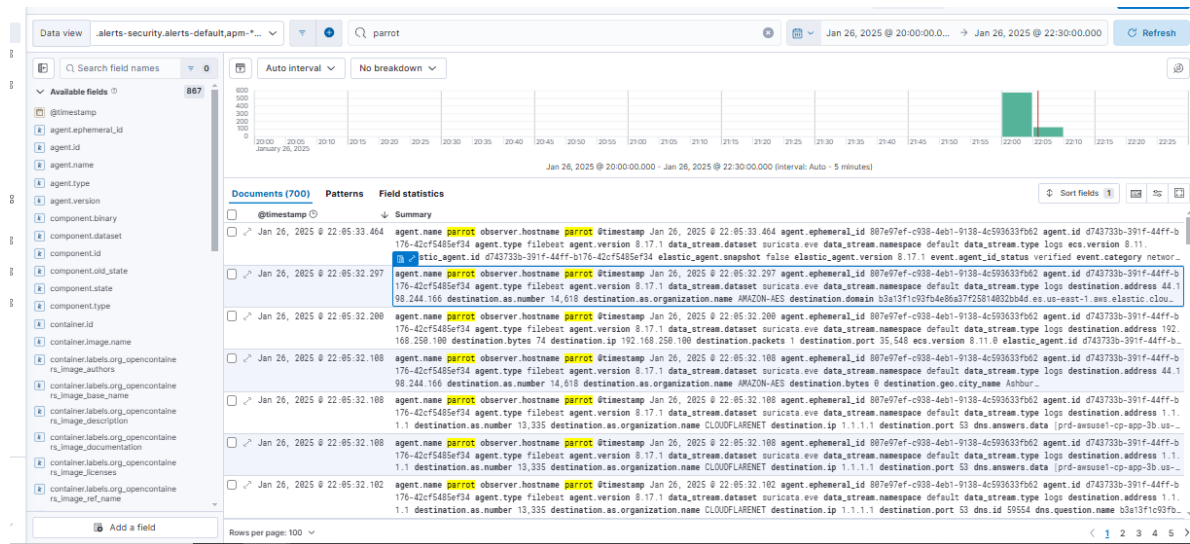
Agent policies

Linux/Suricata



1 agent is enrolled with the selected agent policies.

2.3.3 Evidencias de recepción de logs



La información de un mensaje lo puede ver aqui

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciasuricata3.txt>

La información de todos los logs de suricata recibidos en elastic y transmitidos desde el parrot el día 26 de enero se dejan aquí

<https://github.com/oscartobar/practicaskkeepcoding/blob/main/BlueTeam/suricata3.zip>

2.4 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 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"/>	Healthy	DESKTOP-PGGB831	Politic... 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	Politic... 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](#)

Reload

Create agent policy

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Politic... DMZ rev. 9 Políticas para servidores en DMZ	Jan 18, 2025	0 / 1 (1)	4	...
Linux/Suricata rev. 6	Jan 16, 2025	0 / 1 (1)	2	...
Politic... 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

Last activity

Size

Actions

elastic_agent.elastic_agent	metrics	default	 elastic_agent	Jan 18, 2025 @ 2:18:17 PM	37.11mb	
elastic_agent.filebeat	metrics	default	 elastic_agent	Jan 18, 2025 @ 2:18:17 PM	18.03mb	
elastic_agent.filebeat_input	metrics	default	 elastic_agent	Jan 18, 2025 @ 2:18:17 PM	7.26mb	
elastic_agent.metricbeat	metrics	default	 elastic_agent	Jan 18, 2025 @ 2:18:17 PM	31.61mb	
windows.service	metrics	default	 windows	Jan 18, 2025 @ 2:18:15 PM	47.79mb	
fleet_server.agent_status	metrics	default	 fleet_server	Jan 18, 2025 @ 2:17:40 PM	1.18mb	
fleet_server.agent_versions	metrics	default	 fleet_server	Jan 18, 2025 @ 2:17:40 PM	686.23kb	
system.application	logs	default	 system	Jan 18, 2025 @ 2:17:36 PM	1.04mb	
elastic_agent	logs	default	 elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.18mb	
elastic_agent.filebeat	logs	default	 elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.32mb	
system.security	logs	default	 system	Jan 18, 2025 @ 2:12:36 PM	19.72mb	
system.system	logs	default	 system	Jan 18, 2025 @ 12:43:43 PM	597.16kb	
docker.container_logs	logs	default	 docker	Jan 18, 2025 @ 11:32:22 AM	390.52kb	
generic	logs	default	 log	Jan 18, 2025 @ 11:32:22 AM	94.71kb	
docker.event	metrics	default	 docker	Jan 18, 2025 @ 11:06:00 AM	24.08kb	
windows.powershell	logs	default	 windows	Jan 18, 2025 @ 9:54:14 AM	87.4kb	
windows.powershell_operational	logs	default	 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 12 Integrations 3 Agents 1 agent Last updated on Jan 26, 2025 Actions

<div>Search...</div>				Namespace ▾	<div><div></div>Add Integration</div>
Integration policy ↑	Integration ⇅	Namespace	Output	Actions	
docker-1 <div><div></div></div>	<div><div></div> Docker v2.13.1</div>	<div>default <div><div></div></div></div>	<div>Default output <div><div></div></div></div>	<div>...</div>	
log cowri	<div><div></div> Custom Logs v2.3.3</div>	<div>default <div><div></div></div></div>	<div>Default output <div><div></div></div></div>	<div>...</div>	
system-1 (copy)	<div><div></div> System v1.63.2</div>	<div>default</div>	<div>Default output <div><div></div></div></div>	<div>...</div>	

Linux/Suricata

Integrations Settings

Revision
6

Integrations
2

Agents
1 agent

Last updated on
Jan 16, 2025

Actions

Search...

Namespace

Add integration

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