KeepCoding Bootcamp Ciberseguridad | Edición IX

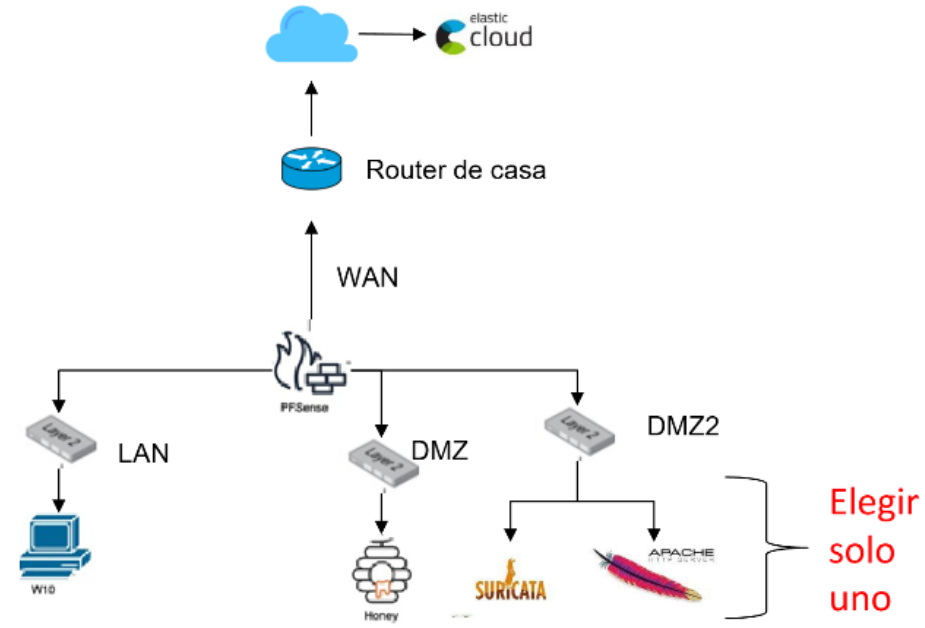
Módulo de Blue Team

Informe Práctica Blue Team

Por: Oscar Uriel Tobar Rios
Fecha del Informe: 18/01/2025

Contenido

1 EJERCICIO PROPUESTO



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.

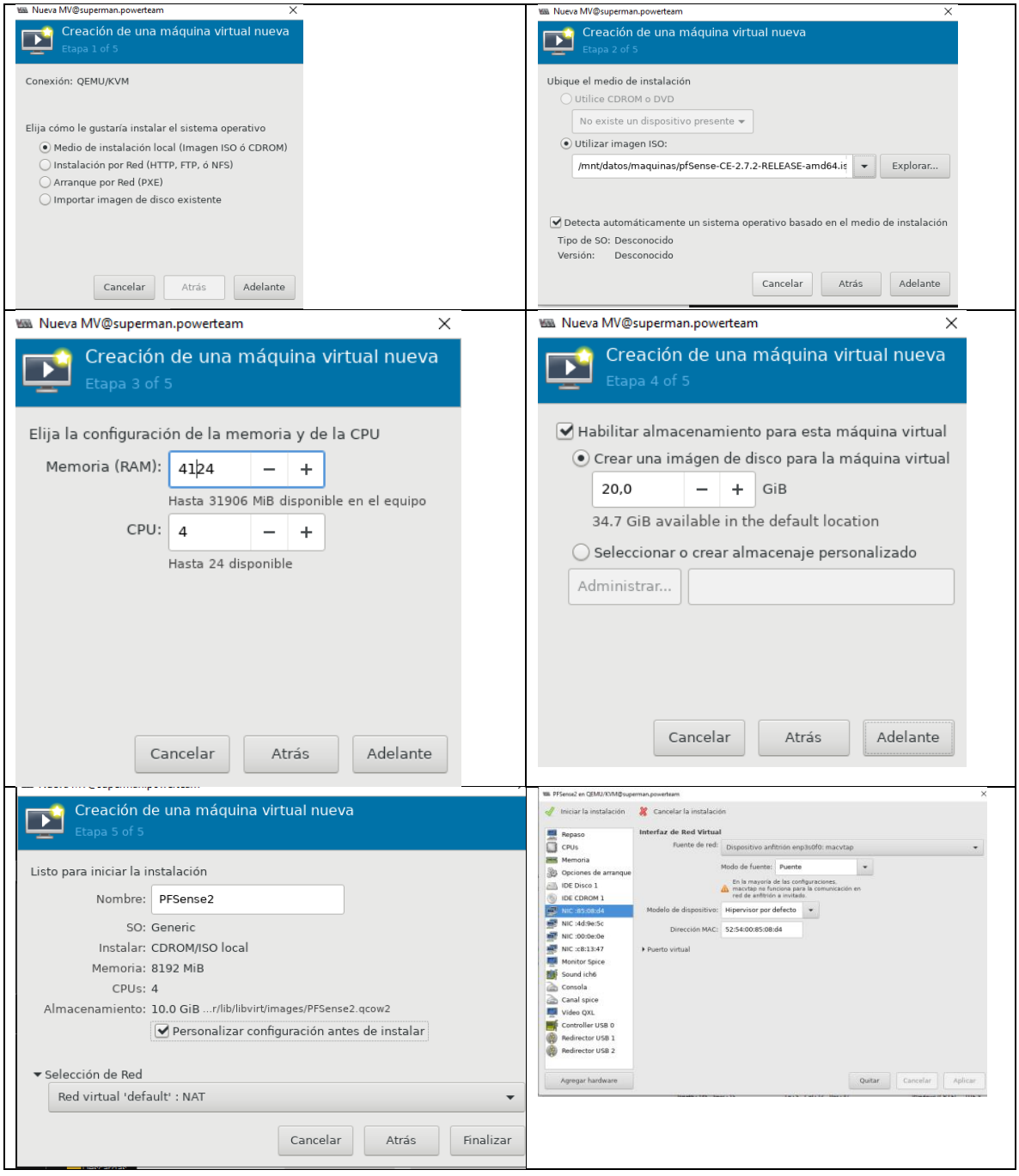
2 PFSense

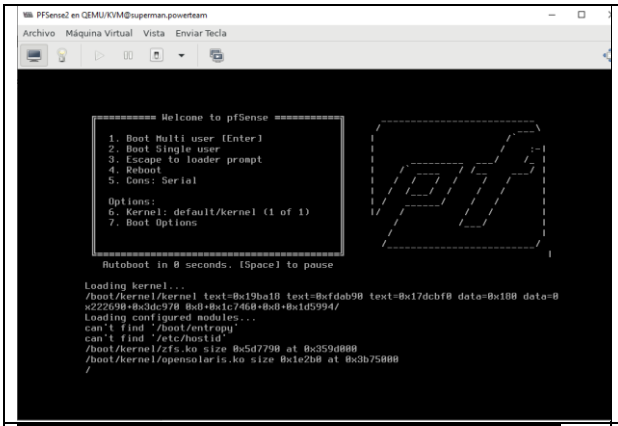
Para poder desarrollar el ejercicio lo primero fue hacer la instalación de PFSense. Se utilizo la versión pfSense-CE-2.7.2 y se instaló en una maquina Oracle Linux sobre el virtualizador

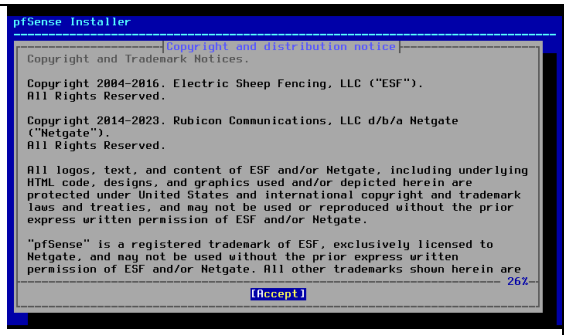
2.1 Instalación

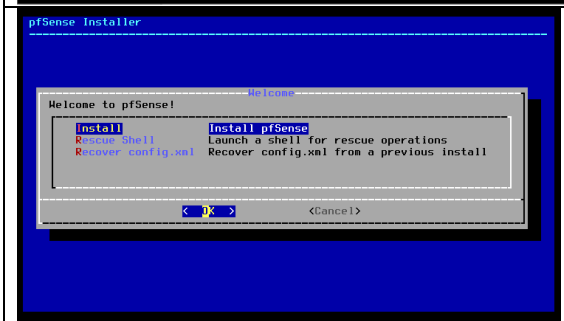
Para la Instalación se utilizo la versión pfSense-CE-2.7.2 y se instalo en una maquina Linux con el virtualizador QEMU, donde se montaron las maquinas virtuales de PFSense, Windows, Kali Linux y Parrot Linux.

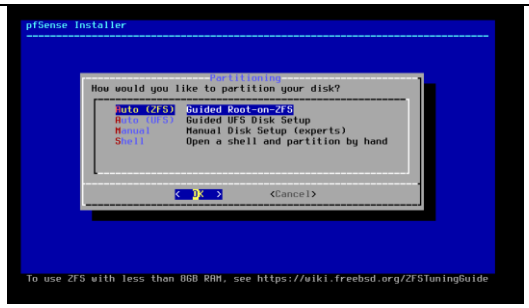
Para la configuración de la maquina virtual de PfSense se habilitaron 4 tarjetas de red y se ejecutó la instalación como se muestra a continuación:

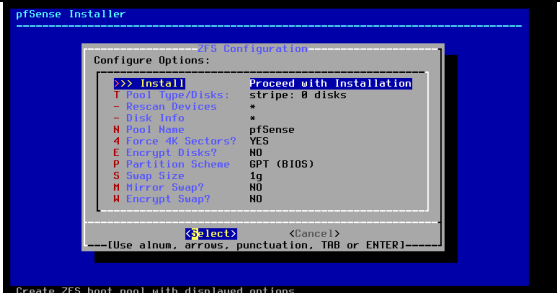



PFSense2 en QEMU/KVM@superman.powerteam
Archivo Máquina Virtual Vista Enviar Tecla
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 0 seconds. [Space] to pause
Loading kernel...
/boot/kernel/kernel text=0x19ba10 text=0xfdab90 text=0x17dcbf0 data=0x180 data=0
x222698+0x3dc970 0x0+0x1c7460+0x0+0x1d5994/
Loading configured modules...
can't find '/boot/entropy'
can't find '/etc/hostid'
/boot/kernel/zfs.ko size 0x5d7790 at 0x359d000
/boot/kernel/opensolaris.ko size 0x1e2b0 at 0x3b75000
/

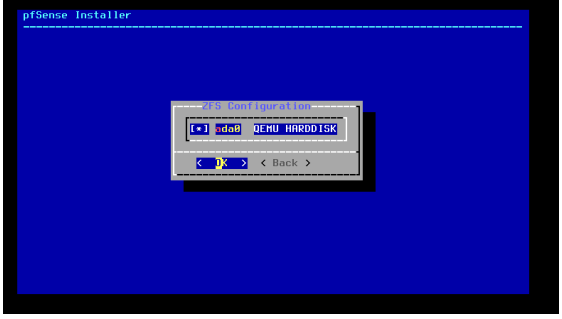

pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are
26%
[Accept]

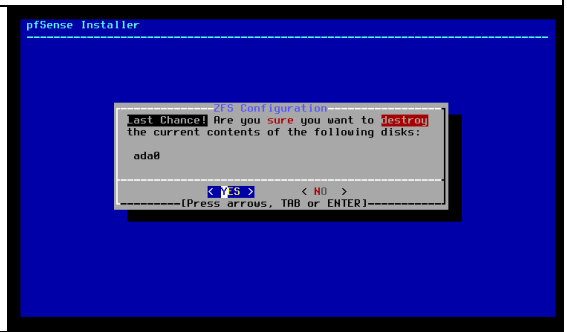

pfSense Installer
Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install
< OK >
<Cancel>

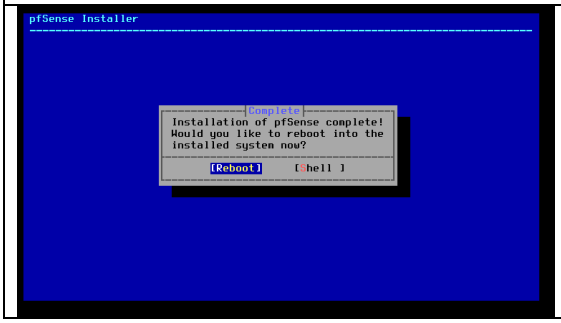

pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide


pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
---[Use alnum, arrows, punctuation, TAB or ENTER]-----
Create ZFS boot pool with displayed options


pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
--------[Press arrows, TAB or ENTER]---------
[1+ Disks] Striping provides maximum storage but no redundancy


pfSense Installer
ZFS Configuration
[*] ada0 QEMU HARDDISK
< OK > < Back >


pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
ada0
< YES > < NO >
--------[Press arrows, TAB or ENTER]---------

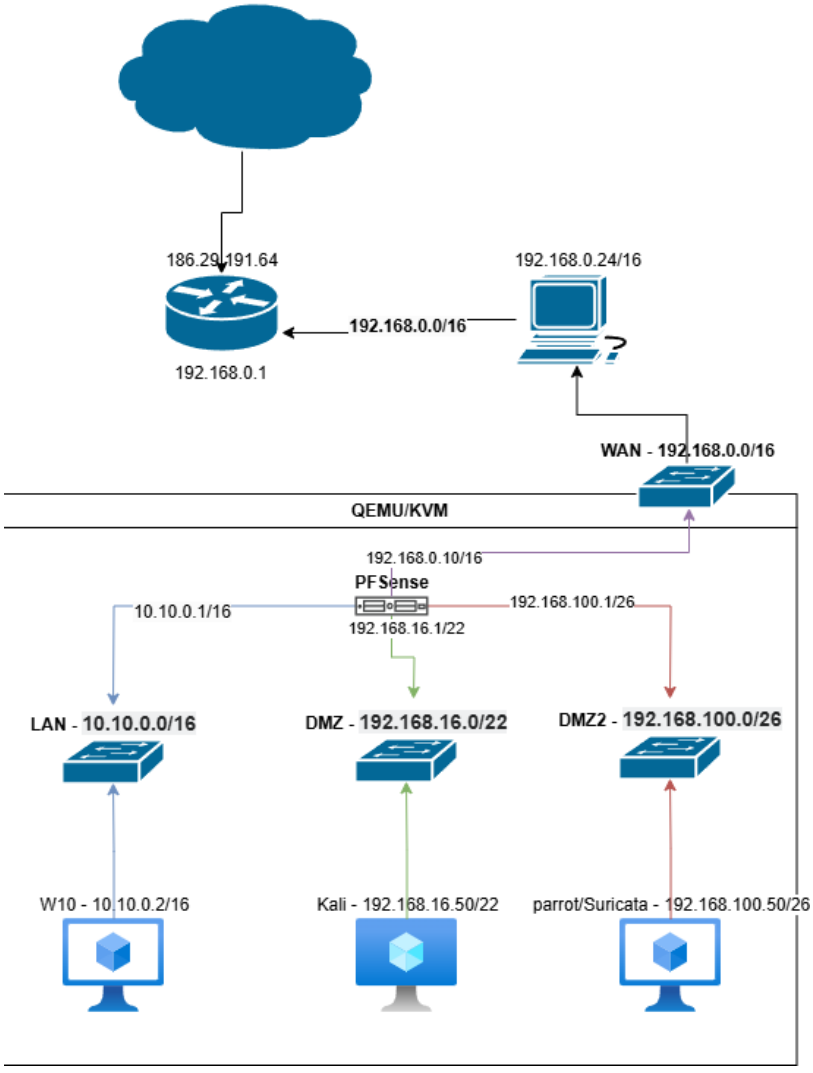

pfSense Installer
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?
[Reboot] [Shell]

2.2 Configuración

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

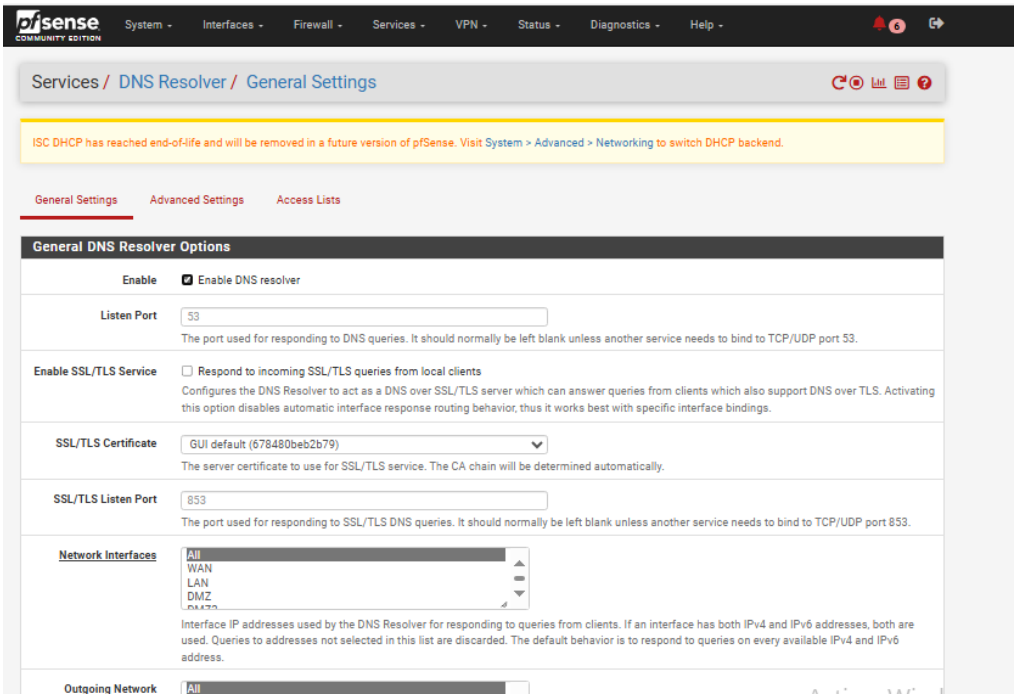
```
Valid interfaces are:

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
```

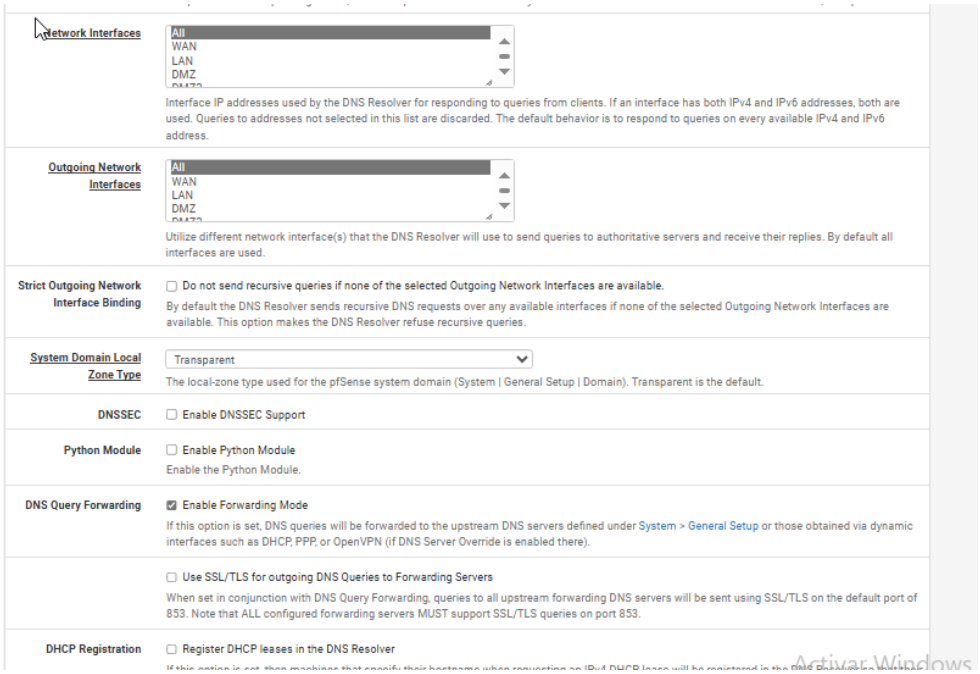
Para establecer la configuración del PFSense se definieron la siguiente configuración para cada red



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:





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

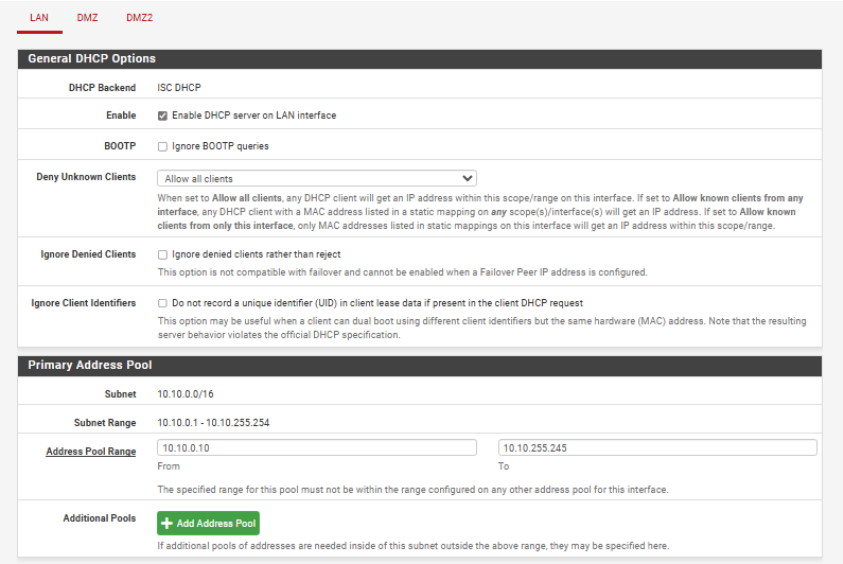
La tarjeta de Red de la LAN identificado internamente como RE1 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 10.10.0.0/16 y se le asignó la primera IP (10.10.0.1).

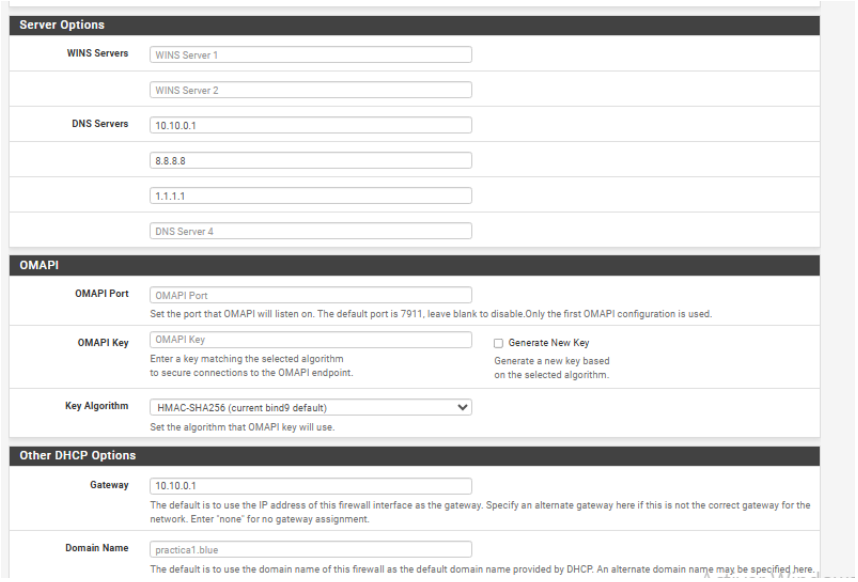
El resumen de esta interface de red es

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

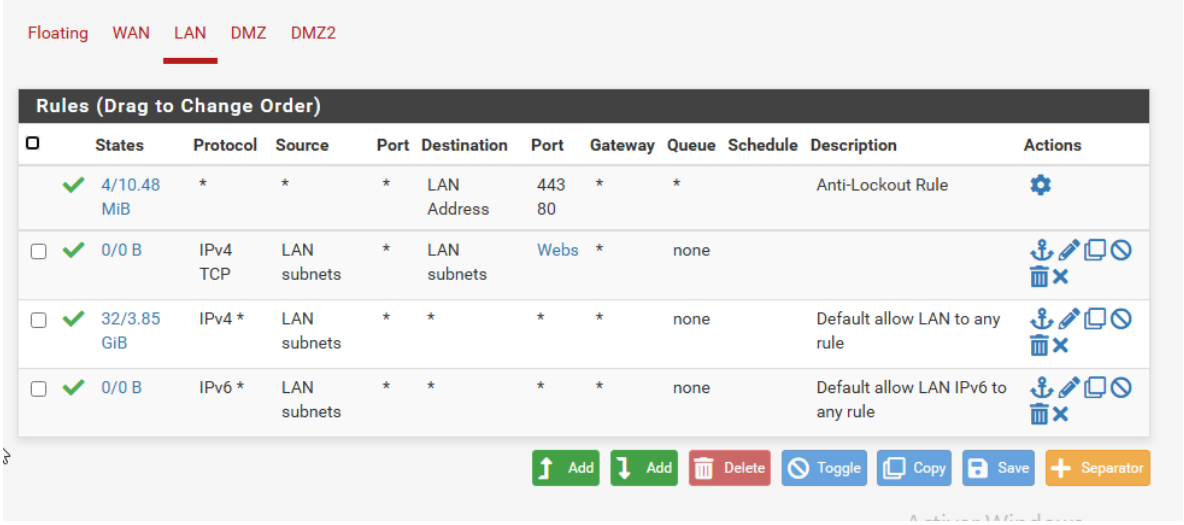




2.2.5 Configuración REGLAS FIREWALL LAN

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

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



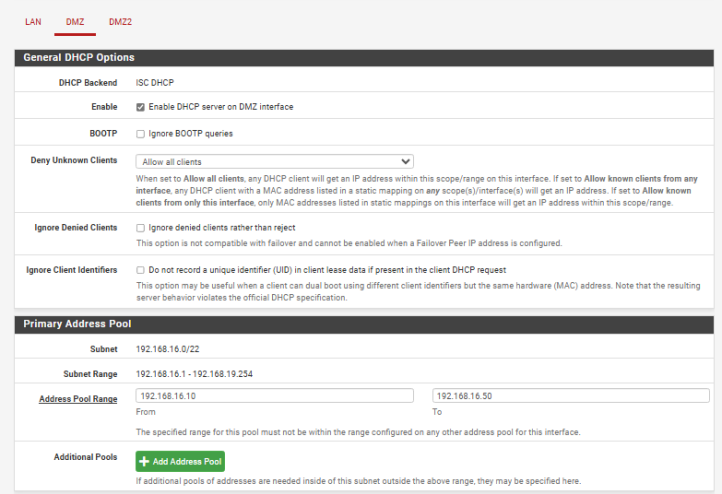
2.2.6 Configuración DMZ

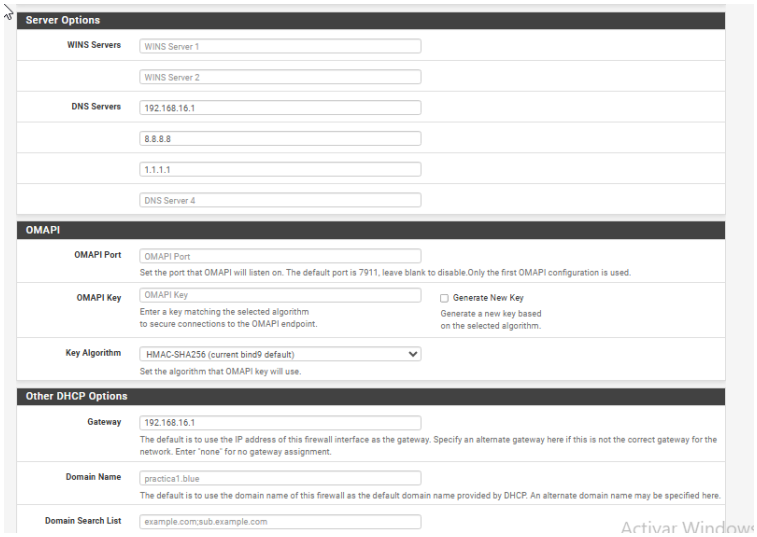
La tarjeta de Red de la DMZ identificado internamente como RE2 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 192.168.16.0/22 y se le asignó la primera IP del segmento (192.168.16.1).

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

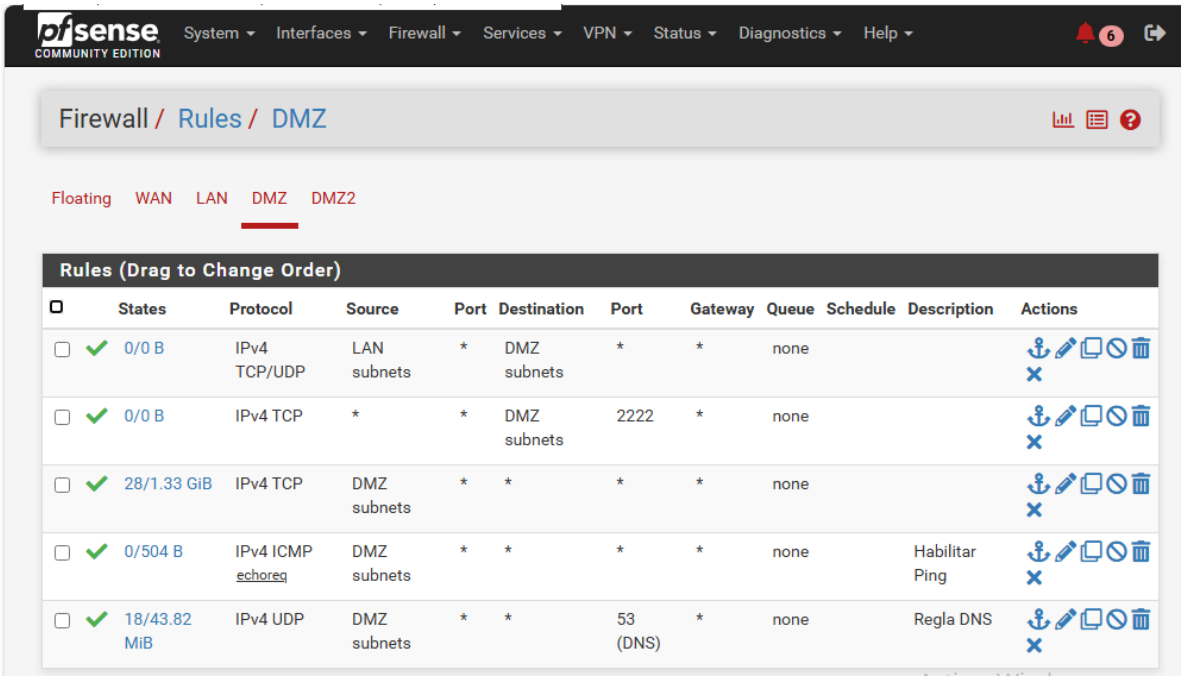




2.2.8 Configuración REGLAS FIREWALL DMZ

Para las reglas del DMZ se establecieron cuatro reglas asi:

- 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 demas 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



2.2.9 Configuración DMZ2

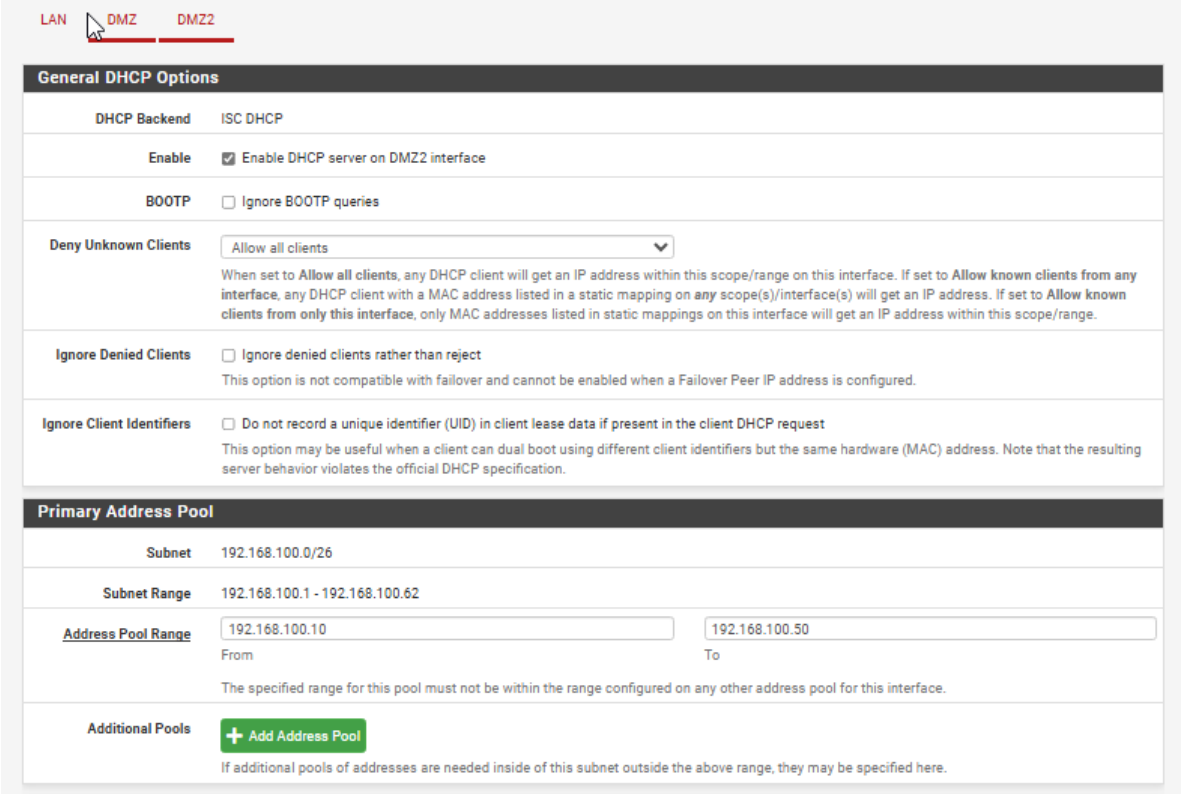
La tarjeta de Red de la DMZ2 identificado internamente como RE3 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 192.168.100.0/26 y se le asignó la primera IP del segmento (192.168.100.1).

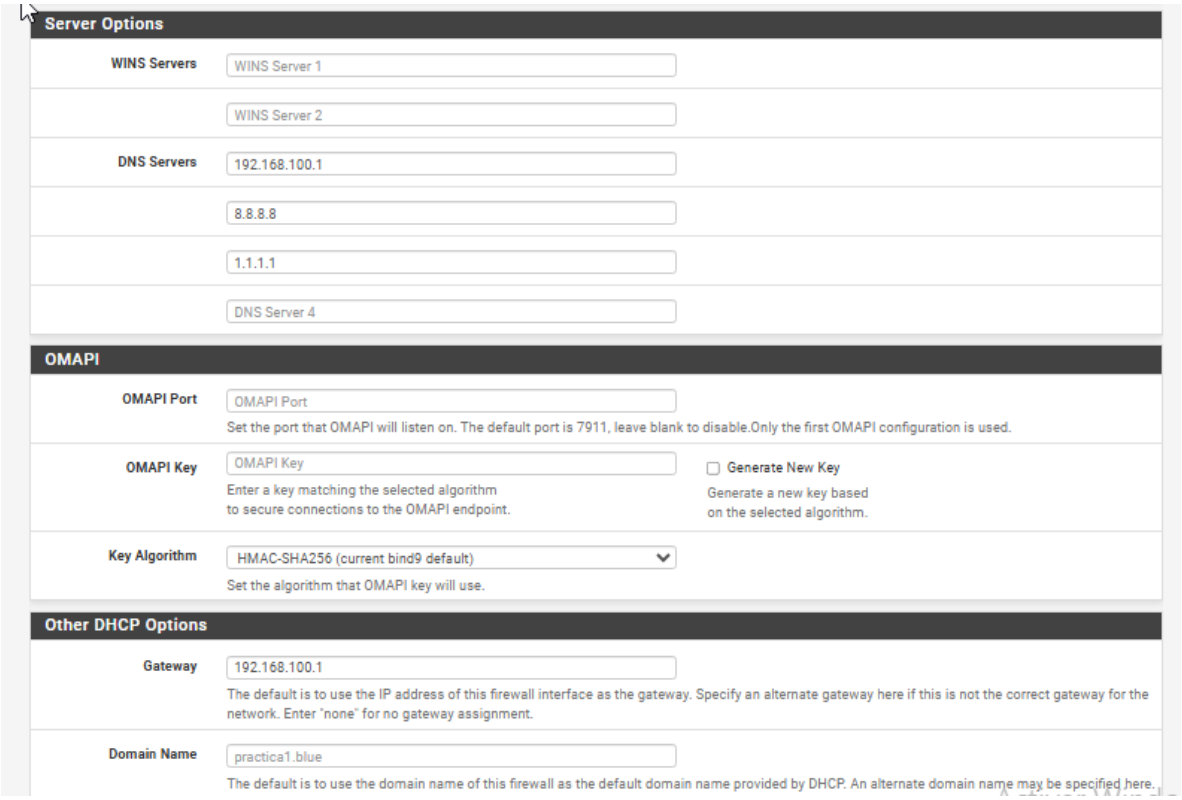
Nombre: DMZ2
Id: re3
Tipo: Interna
Mac: 52:54:00:c8:13:47

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

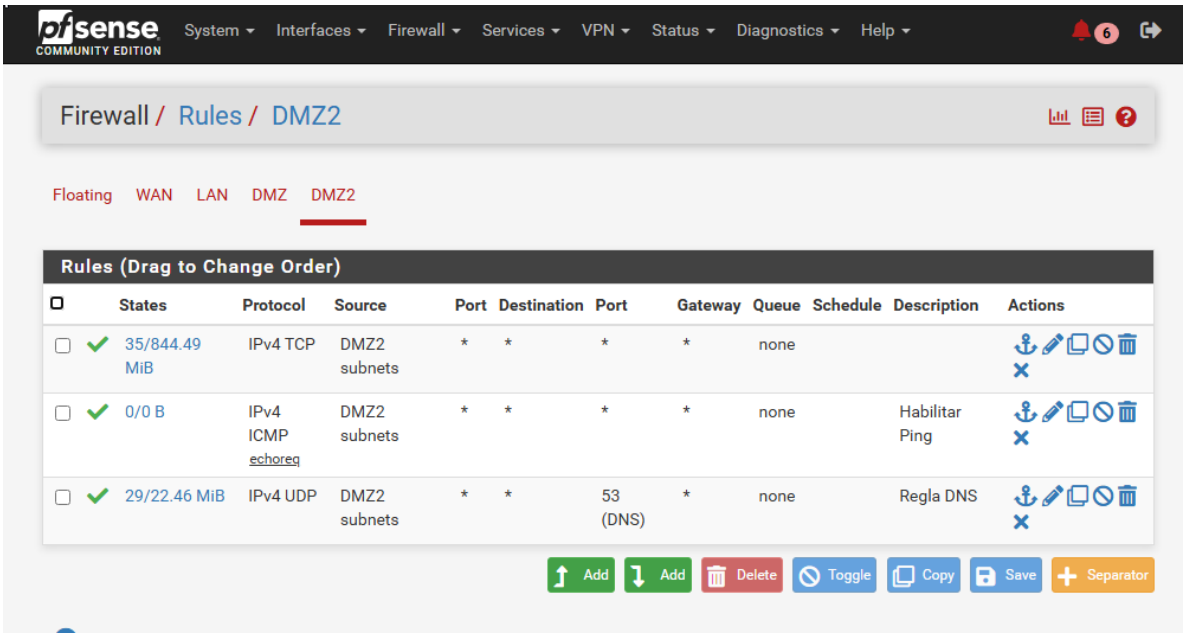




2.2.11 Configuración REGLAS FIREWALL DMZ2

Para las reglas del DMZ2 se establecieron dos reglas asi:

- 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


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
6
Firewall / Rules / DMZ2
Floating
WAN
LAN
DMZ
DMZ2
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
35/844.49 MiB
IPv4 TCP
DMZ2 subnets
* * * * none
0/0 B
IPv4 ICMP echoreq
DMZ2 subnets
* * * * none
Habilitar Ping
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 estabecida como se muestra a continuación

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

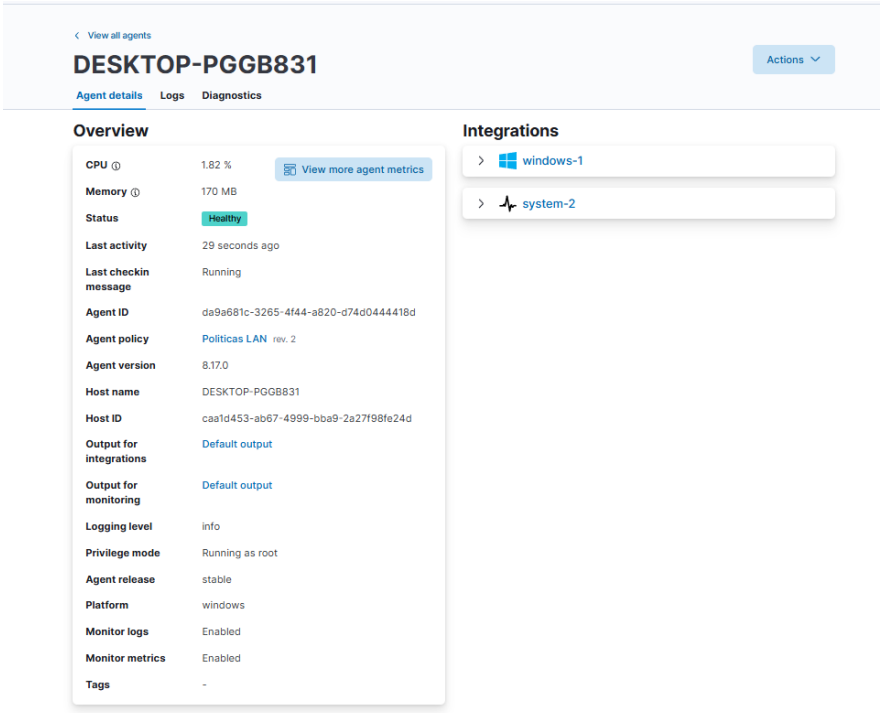
3.1 Configuración Windows 10 (LAN)

3.1.1 Configuración del Agente

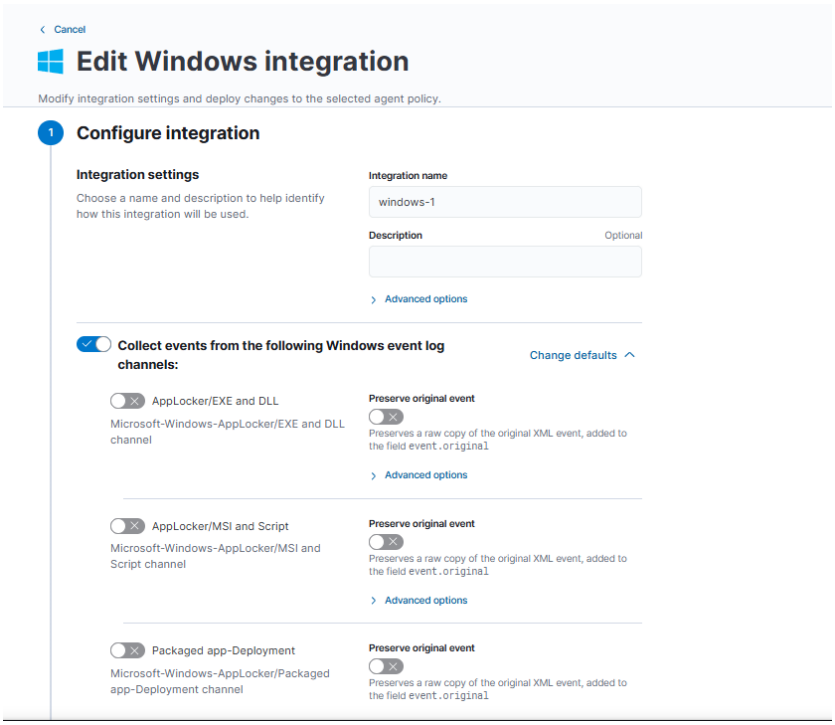
En una maquina virtual de Windows 10 llamada DESKTOP-PGGB831 que instaló el agente de Elastic elastic-agent-8.17.0 para Windows

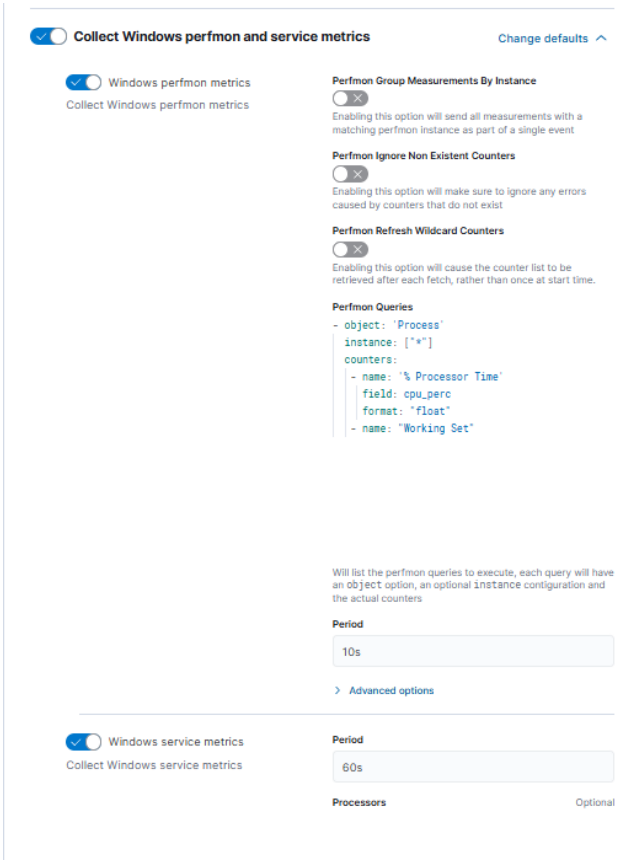
Para su instalación en Windows después de descomprimirlo se ejecuto la instalación con este comando

.\elastic-agent.exe install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RIbDhwczQybjE6aDZXYzQtR0tSYXlpdTN6QU01ekN3QQ==

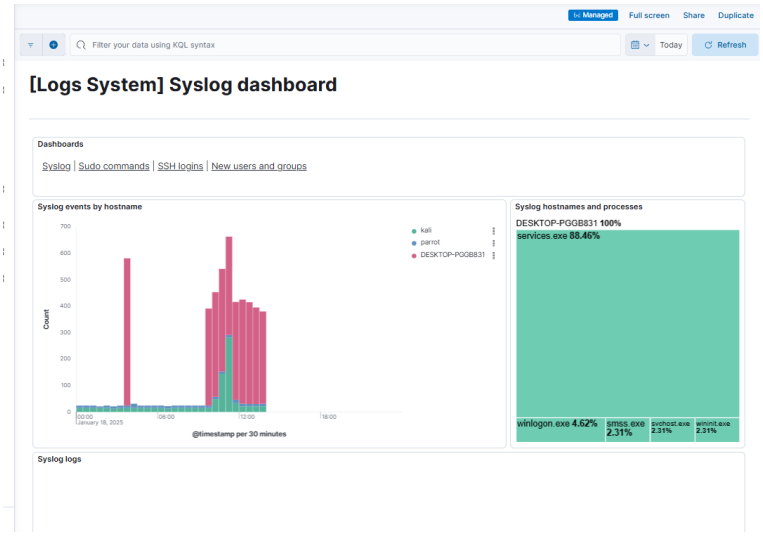


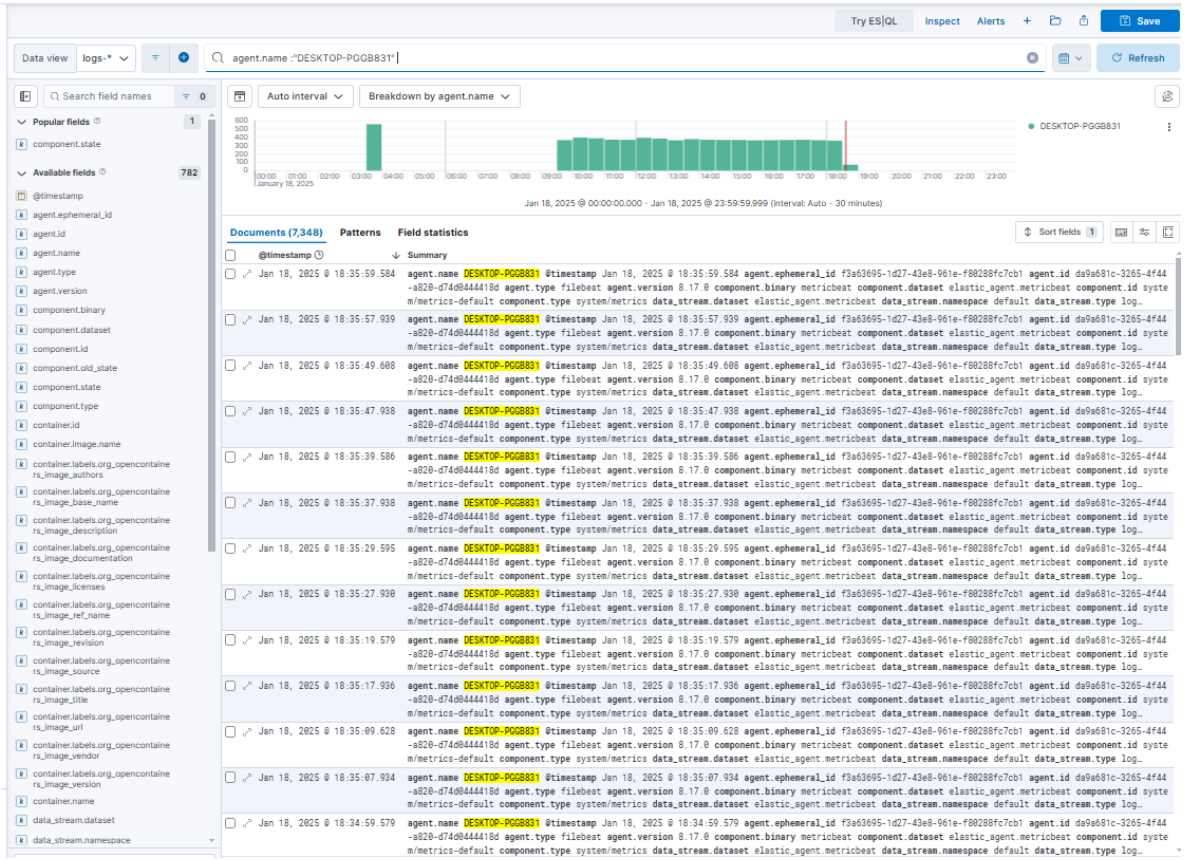
Una vez instalado desde Elastic cloud que añadió una integración para leer los logs de Windows asi:





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/evidenciaswindows.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/practicaskeepcoding/blob/1364cdaba9b4cd1433177d6e6ddbe3109b775dbf/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                                                  NAME
S
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.p
y:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptograp
hy.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryp
tography.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.p
y:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptograp
hy.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryp
tography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

3.2.2 Configuración del Agente

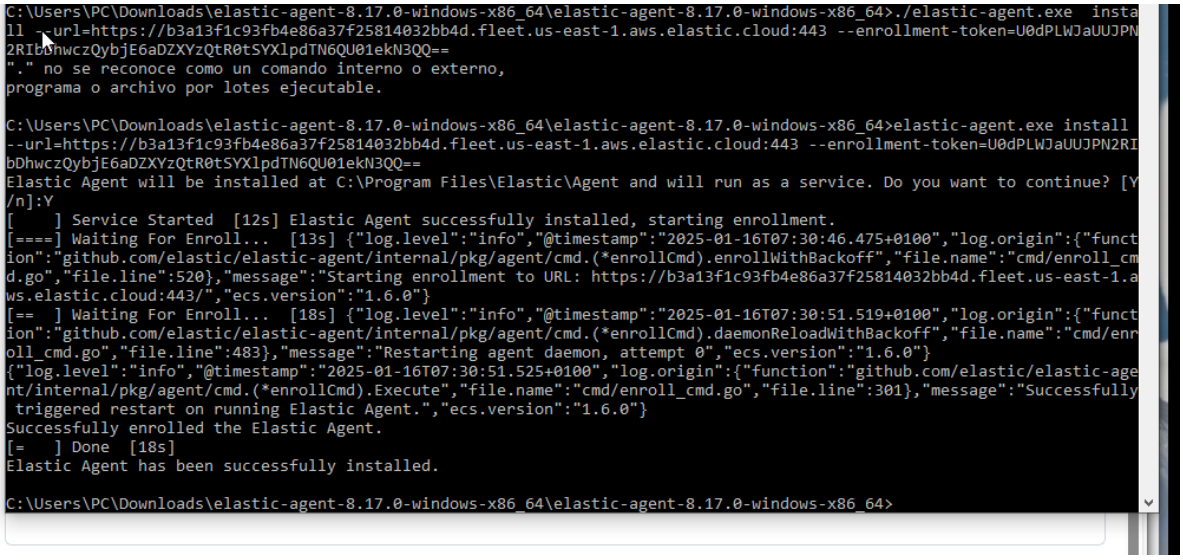
Una vez funcionando que instalo en agente de elastic asi:

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

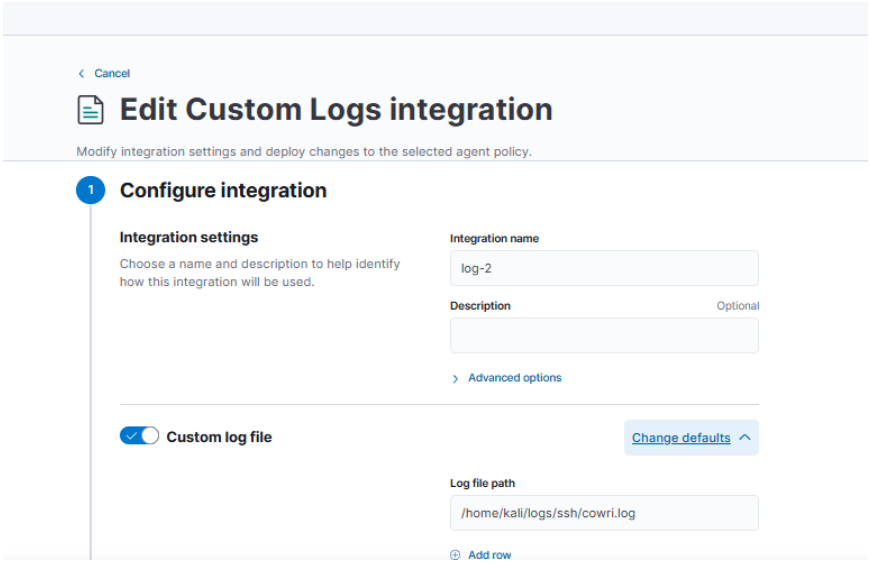
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz

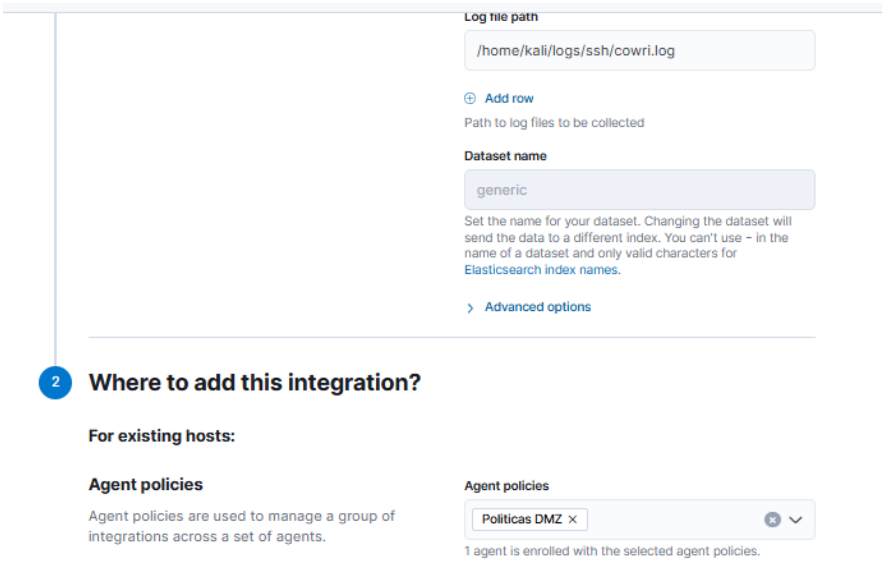
cd elastic-agent-8.17.0-linux-x86_64

sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RIbDhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==

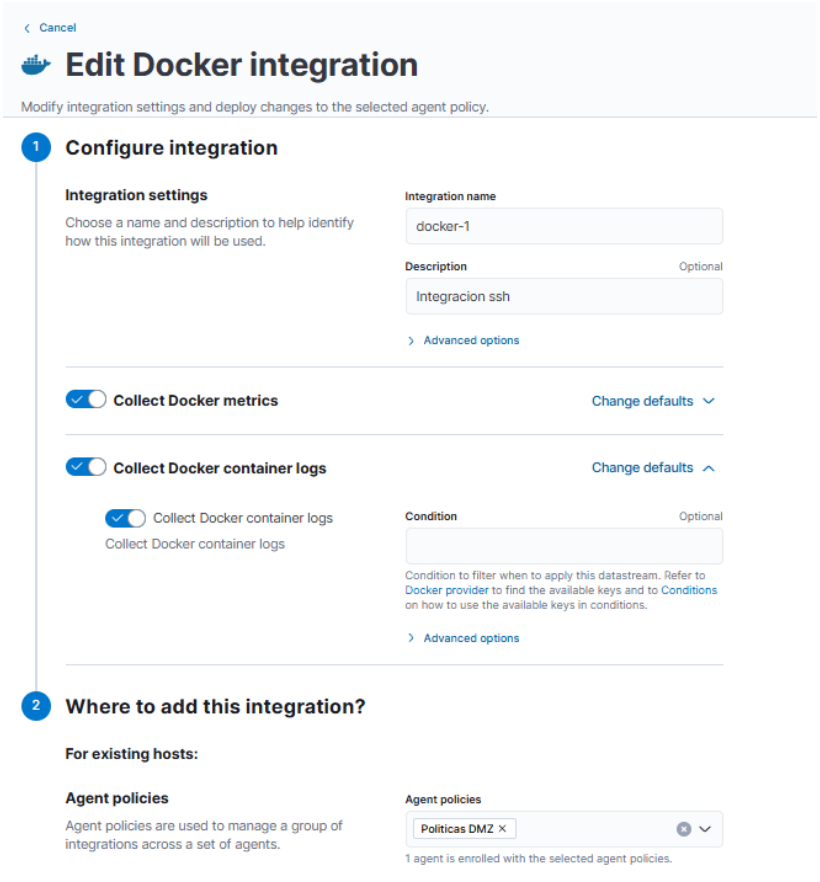


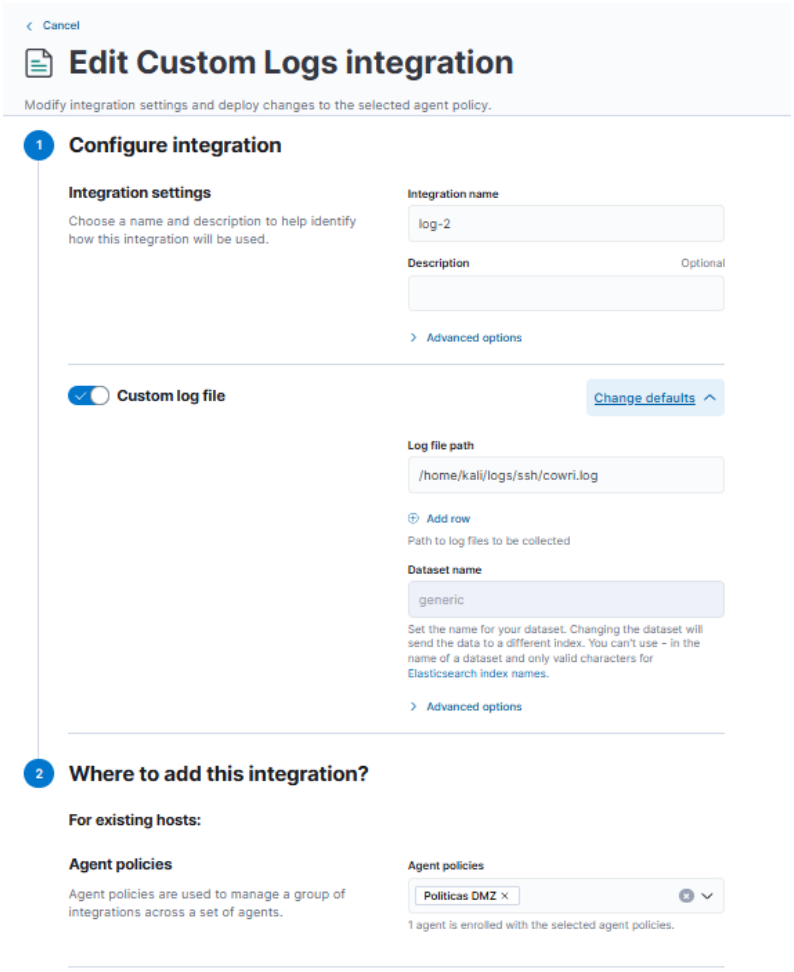
Luego en Elastic se configuro una integración para logs personalizados en la maquina Kali asi





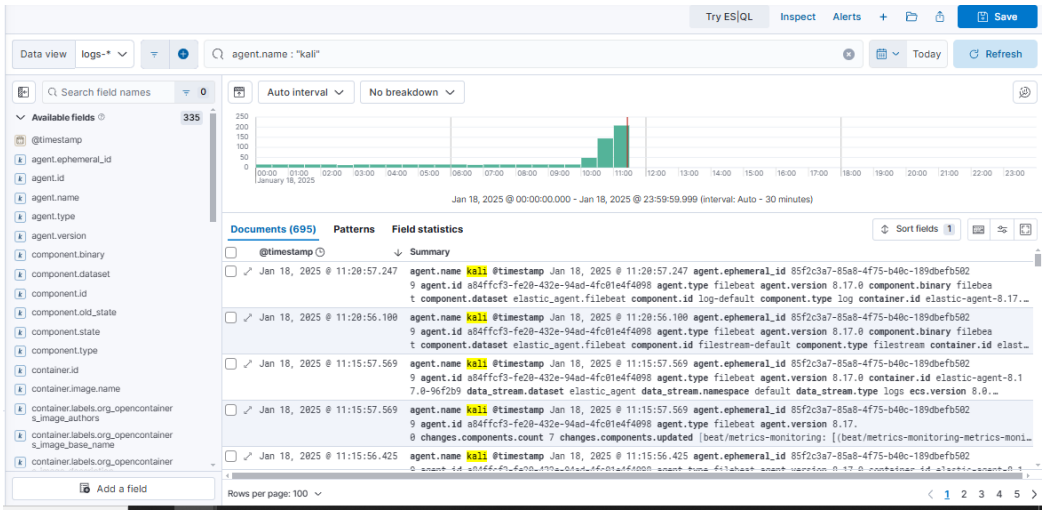
Adicionalmente Tambien se tomo una integración para leer los logs del docker

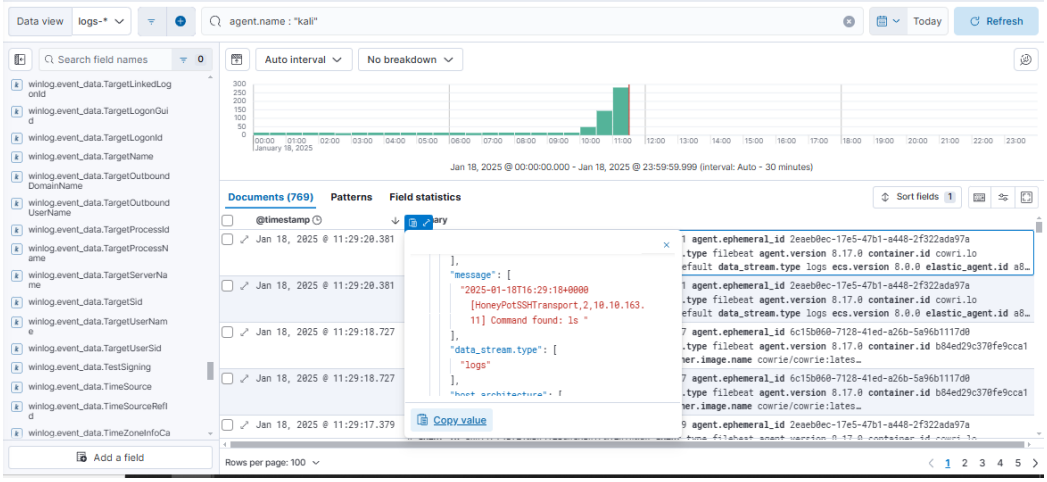


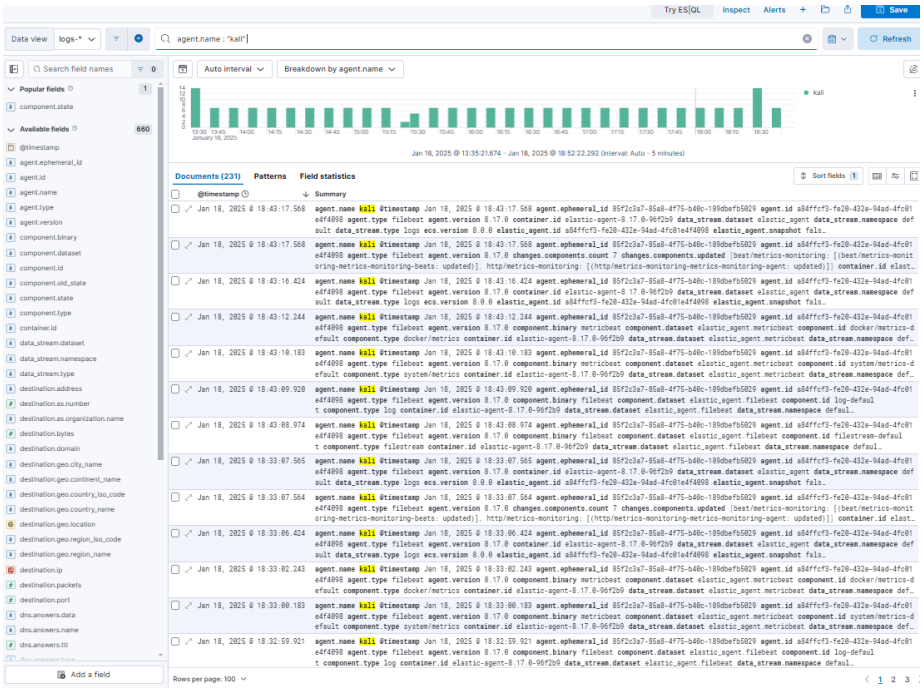


3.2.3 Evidencias de recepción de logs

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


Try ES|QL
Inspect
Alerts
Save
Data view
logs-*
agent.name : "kali"
Today
Refresh
Search field names
Available fields
335
@timestamp
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
component.binary
component.dataset
component.id
component.old_state
component.state
component.type
container.id
container.image.name
container.labels.org_opencontainers_image_authors
container.labels.org_opencontainers_image_base_name
container.labels.org_opencontainer
Add a field
Auto interval
No breakdown
Jan 18, 2025 @ 00:00:00.000 - Jan 18, 2025 @ 23:59:59.999 (interval: Auto - 30 minutes)
Documents (695)
Patterns
Field statistics
Sort fields
@timestamp
Summary
Jan 18, 2025 @ 11:20:57.247
agent.name kali @timestamp Jan 18, 2025 @ 11:20:57.247 agent.ephemeral_id 85f2c3a7-85a8-4f75-b40c-189dbefb502
9 agent.id a84ffcf3-fe20-432e-94ad-4fc01e4f4098 agent.type filebeat agent.version 8.17.0 component.binary filebea
t component.dataset elastic_agent.filebeat component.id log-default component.type log container.id elastic-agent-8.17.…
Jan 18, 2025 @ 11:20:56.100
agent.name kali @timestamp Jan 18, 2025 @ 11:20:56.100 agent.ephemeral_id 85f2c3a7-85a8-4f75-b40c-189dbefb502
9 agent.id a84ffcf3-fe20-432e-94ad-4fc01e4f4098 agent.type filebeat agent.version 8.17.0 component.binary filebea
t component.dataset elastic_agent.filebeat component.id filestream-default component.type filestream container.id elast…
Jan 18, 2025 @ 11:15:57.569
agent.name kali @timestamp Jan 18, 2025 @ 11:15:57.569 agent.ephemeral_id 85f2c3a7-85a8-4f75-b40c-189dbefb502
9 agent.id a84ffcf3-fe20-432e-94ad-4fc01e4f4098 agent.type filebeat agent.version 8.17.0 container.id elastic-agent-8.1
7.0-96f2b9 data_stream.dataset elastic_agent data_stream.namespace default data_stream.type logs ecs.version 8.0.…
Jan 18, 2025 @ 11:15:57.569
agent.name kali @timestamp Jan 18, 2025 @ 11:15:57.569 agent.ephemeral_id 85f2c3a7-85a8-4f75-b40c-189dbefb502
9 agent.id a84ffcf3-fe20-432e-94ad-4fc01e4f4098 agent.type filebeat agent.version 8.17.
0 changes.components.count 7 changes.components.updated [beat/metrics-monitoring: [(beat/metrics-monitoring-metrics-moni…
Jan 18, 2025 @ 11:15:56.425
agent.name kali @timestamp Jan 18, 2025 @ 11:15:56.425 agent.ephemeral_id 85f2c3a7-85a8-4f75-b40c-189dbefb502
Rows per page: 100
1 2 3 4 5


Data view
logs-*
agent.name : "kali"
Today
Refresh
Search field names
winlog.event_data.TargetLinkedLogonId
winlog.event_data.TargetLogonGuid
winlog.event_data.TargetLogonId
winlog.event_data.TargetName
winlog.event_data.TargetOutboundDomainName
winlog.event_data.TargetOutboundUserName
winlog.event_data.TargetProcessId
winlog.event_data.TargetProcessName
winlog.event_data.TargetServerName
winlog.event_data.TargetSid
winlog.event_data.TargetUserName
winlog.event_data.TargetUserSid
winlog.event_data.TestSigning
winlog.event_data.TimeSource
winlog.event_data.TimeSourceRefId
winlog.event_data.TimeZoneInfoCa
Add a field
Auto interval
No breakdown
Jan 18, 2025 @ 00:00:00.000 - Jan 18, 2025 @ 23:59:59.999 (interval: Auto - 30 minutes)
Documents (769)
Patterns
Field statistics
Sort fields
@timestamp
Jan 18, 2025 @ 11:29:20.381
Jan 18, 2025 @ 11:29:20.381
Jan 18, 2025 @ 11:29:18.727
Jan 18, 2025 @ 11:29:18.727
Jan 18, 2025 @ 11:29:17.379
"message": [
"2025-01-18T16:29:18+0000
[HoneyPotSSHTransport,2,10.10.163.
11] Command found: ls "
],
"data_stream.type": [
"logs"
],
Copy value
Rows per page: 100
1 2 3 4 5


Try ES|QL
Inspect
Alerts
Save
Data view
logs-*
agent.name : "kali"
Refresh
Search field names
Popular fields
component.state
Available fields
660
@timestamp
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
component.binary
component.dataset
component.id
component.old_state
component.state
component.type
container.id
data_stream.dataset
data_stream.namespace
data_stream.type
destination.address
destination.as.number
destination.as.organization.name
destination.bytes
destination.domain
destination.geo.city_name
destination.geo.continent_name
destination.geo.country_iso_code
destination.geo.country_name
destination.geo.location
destination.geo.region_iso_code
destination.geo.region_name
destination.ip
destination.packets
destination.port
dns.answers.data
dns.answers.name
dns.answers.ttl
Add a field
Auto interval
Breakdown by agent.name
kali
Jan 18, 2025 @ 13:35:21.674 - Jan 18, 2025 @ 18:52:22.292 (interval: Auto - 5 minutes)
Documents (231)
Patterns
Field statistics
Sort fields
@timestamp
Summary
Jan 18, 2025 @ 18:43:17.568
Jan 18, 2025 @ 18:43:17.568
Jan 18, 2025 @ 18:43:16.424
Jan 18, 2025 @ 18:43:12.244
Jan 18, 2025 @ 18:43:10.183
Jan 18, 2025 @ 18:43:09.920
Jan 18, 2025 @ 18:43:08.974
Jan 18, 2025 @ 18:33:07.565
Jan 18, 2025 @ 18:33:07.564
Jan 18, 2025 @ 18:33:06.424
Jan 18, 2025 @ 18:33:02.243
Jan 18, 2025 @ 18:33:00.183
Jan 18, 2025 @ 18:32:59.921
Rows per page: 100
1 2 3

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

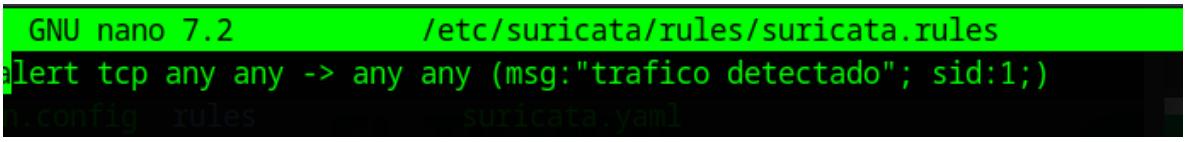
3.3 Configuración Suricata (DMZ2)

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



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

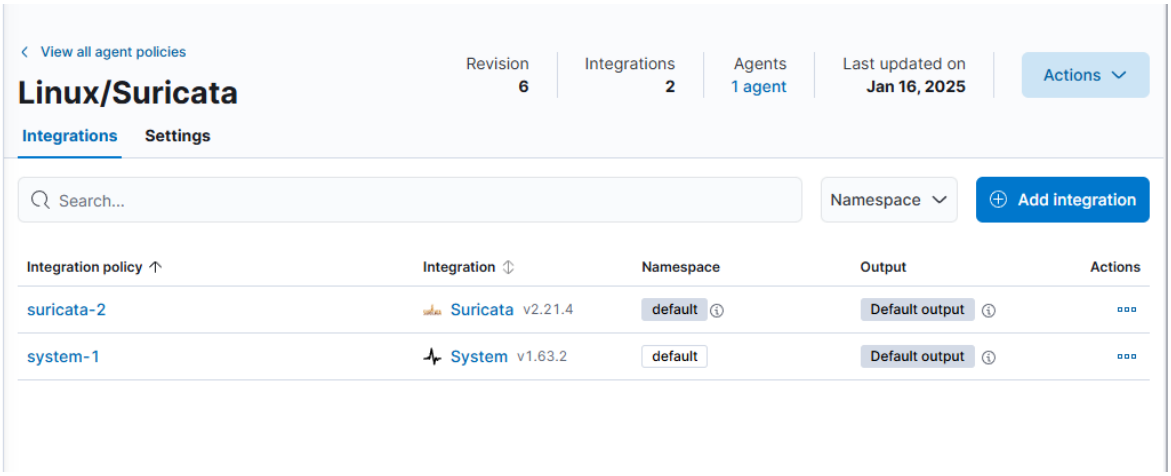
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz

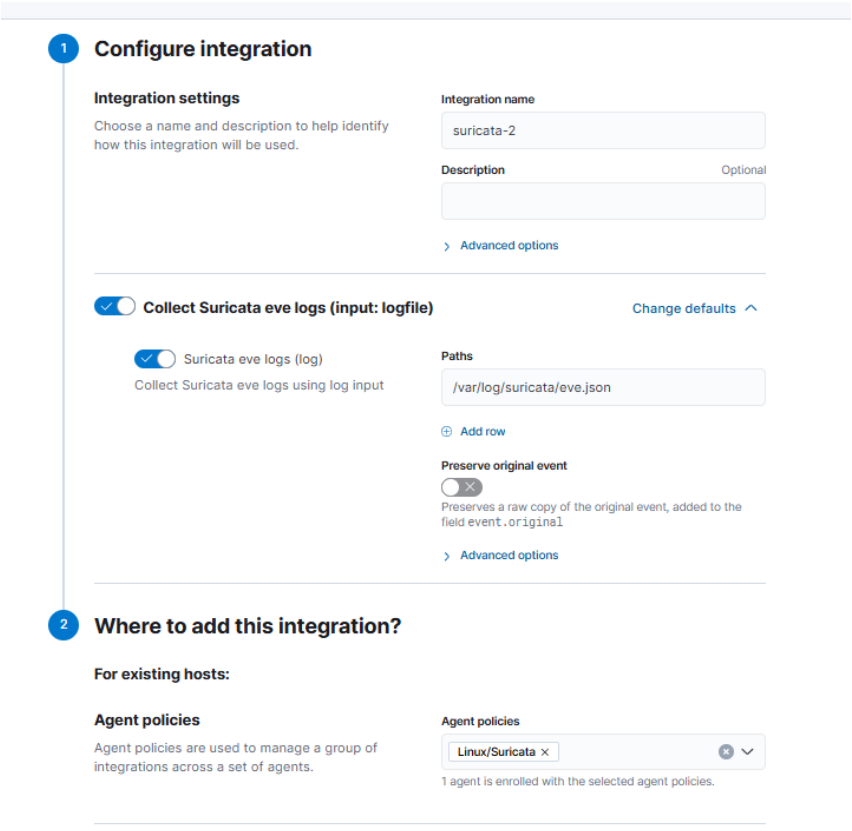
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz

cd elastic-agent-8.17.0-linux-x86_64

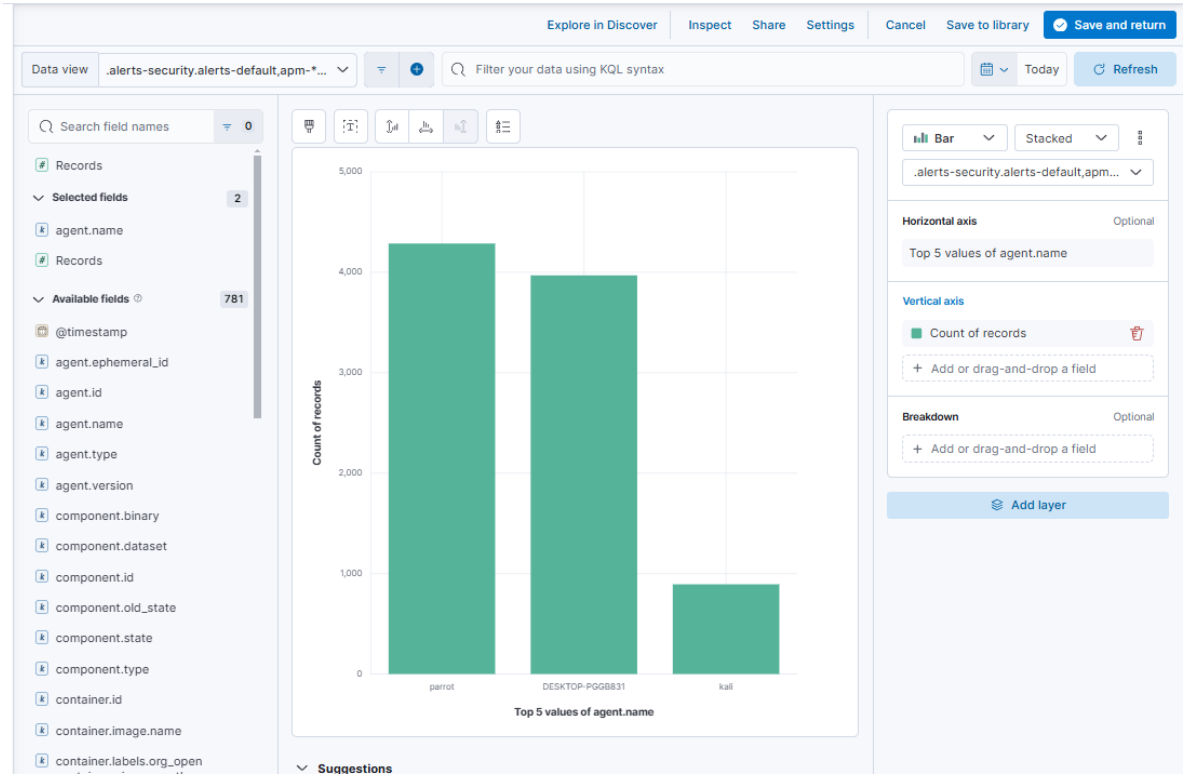
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RIbDhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==

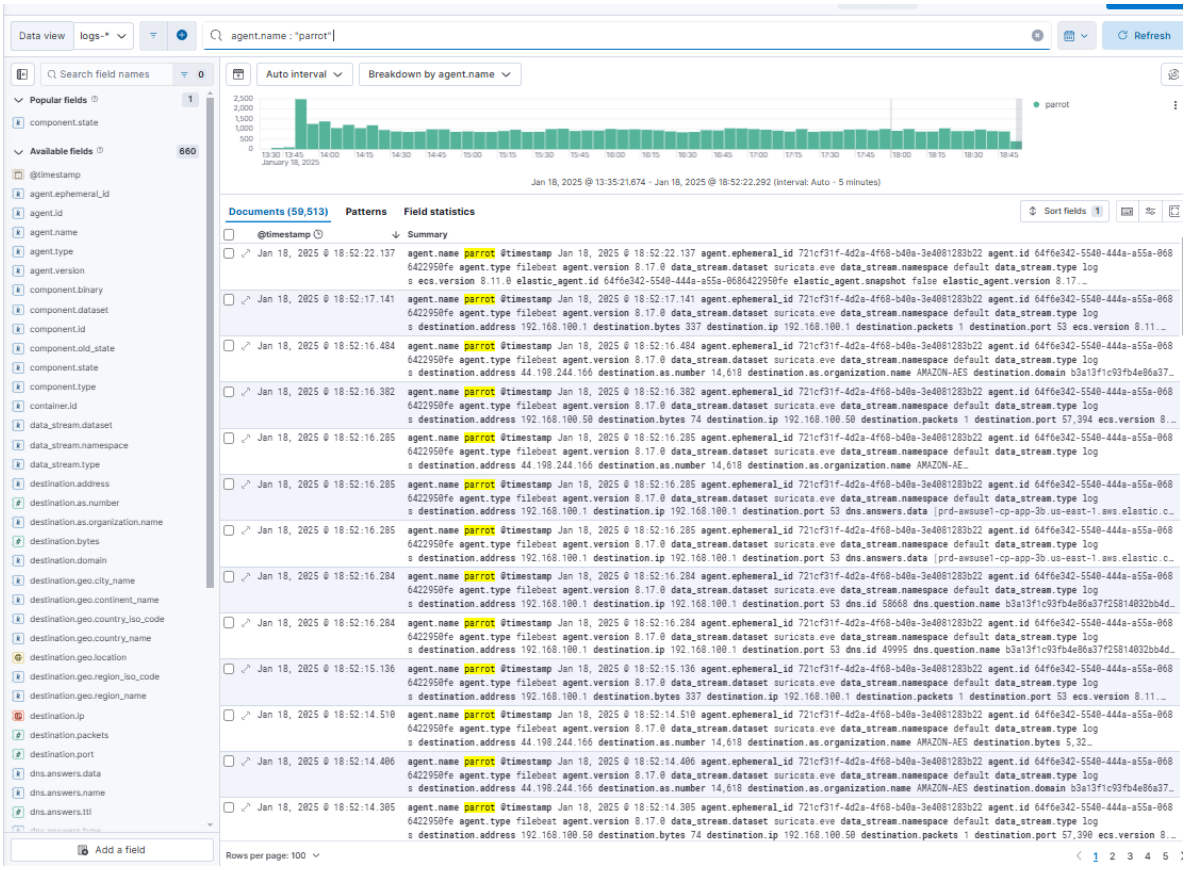
Luego desde Elastic se configuro una nueva integración asi





3.3.3 Evidencias de recepción de logs


Explore in Discover
Inspect
Share
Settings
Cancel
Save to library
Save and return
Data view
.alerts-security.alerts-default,apm-*...
Filter your data using KQL syntax
Today
Refresh
Search field names
0
Records
Selected fields
2
agent.name
Records
Available fields
781
@timestamp
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
component.binary
component.dataset
component.id
component.old_state
component.state
component.type
container.id
container.image.name
container.labels.org_open
5,000
4,000
3,000
2,000
1,000
0
Count of records
parrot
DESKTOP-PGGB831
kali
Top 5 values of agent.name
Suggestions
Bar
Stacked
.alerts-security.alerts-default,apm...
Horizontal axis
Optional
Top 5 values of agent.name
Vertical axis
Count of records
Add or drag-and-drop a field
Breakdown
Optional
Add or drag-and-drop a field
Add layer



La información de un mensaje lo puede ver aqui

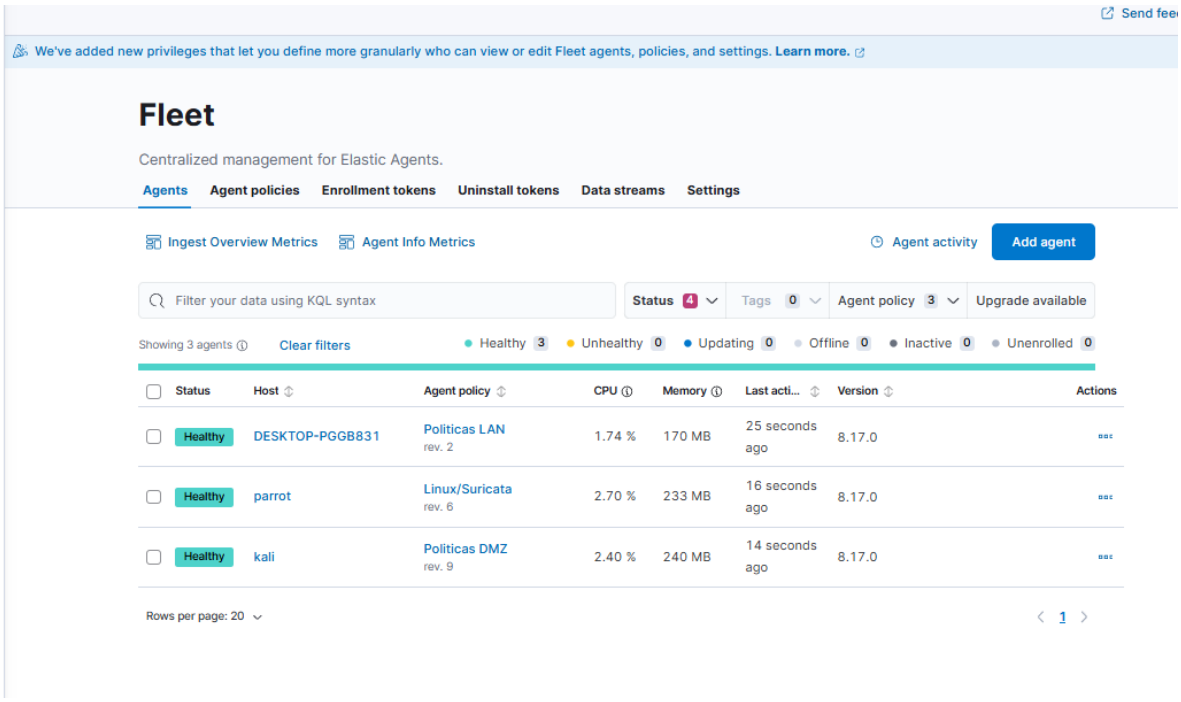
https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciasuricata2.txt

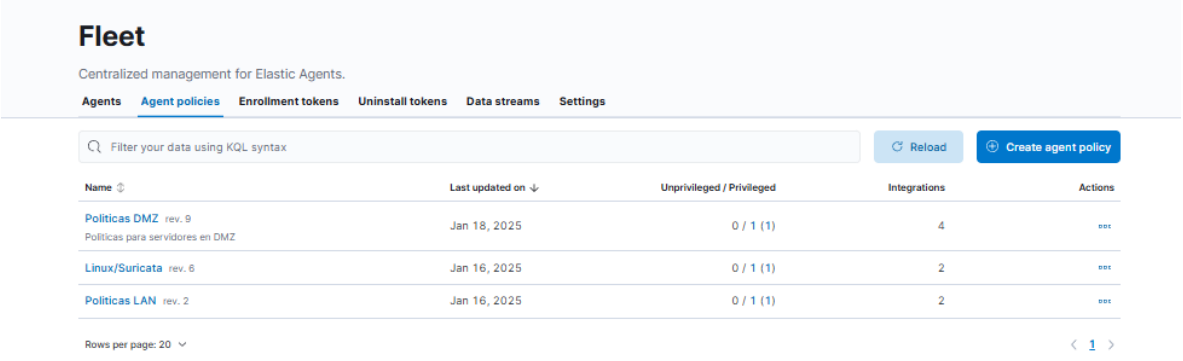
La información de todos los logs de suricata recibidos en elastic y transmitidos desde el parrot el día 18 de enero se dejan aquí

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


Send fee
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
Status
Host
Agent policy
CPU
Memory
Last acti...
Version
Actions
Healthy
DESKTOP-PGGB831
Politicas LAN
rev. 2
1.74 %
170 MB
25 seconds ago
8.17.0
Healthy
parrot
Linux/Suricata
rev. 6
2.70 %
233 MB
16 seconds ago
8.17.0
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
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

Filter data streams

Dataset | Type | Namespace | Integration | Reload

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

Politicas DMZ

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

Actions

Politicas para servidores en DMZ

Integrations | Settings

Search...

Namespace | Add integration

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	