KeepCoding Bootcamp Ciberseguridad | Edición IX

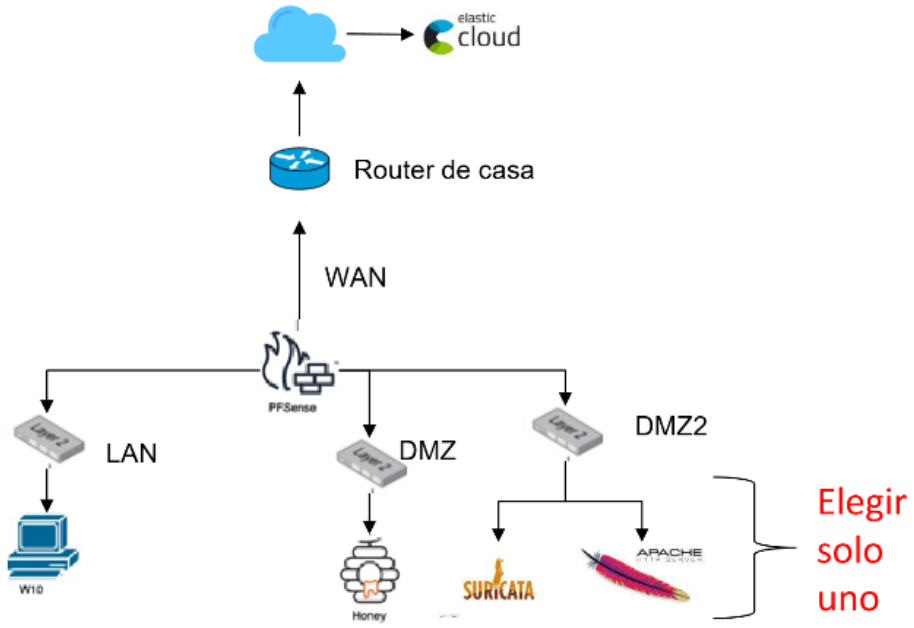
Módulo de Blue Team

Informe Práctica Blue Team
SEGUNDA ENTREGA

Por: Oscar Uriel Tobar Rios
Fecha del Informe: 26/01/2025

Contenido

1 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.

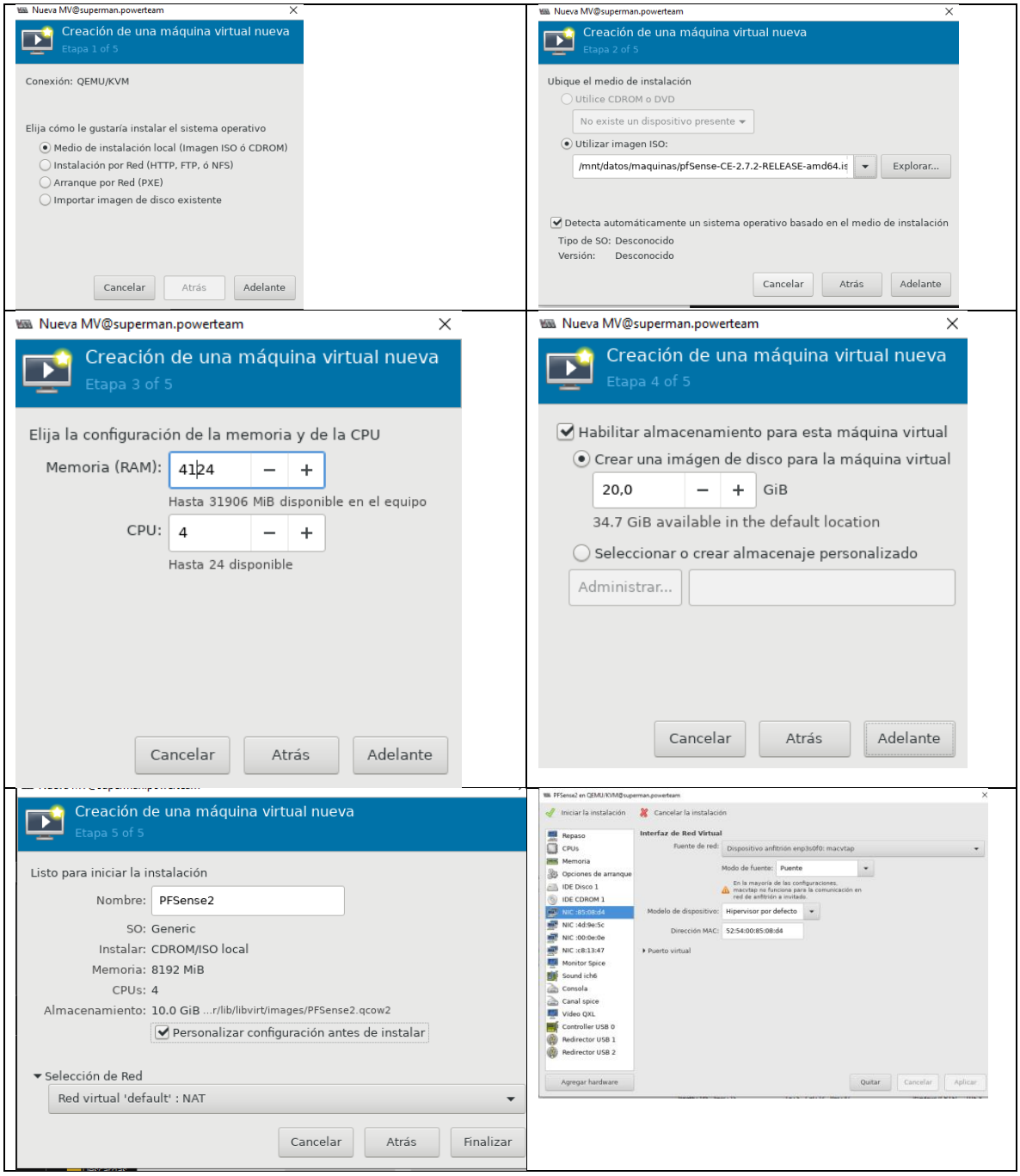
2 PFSense

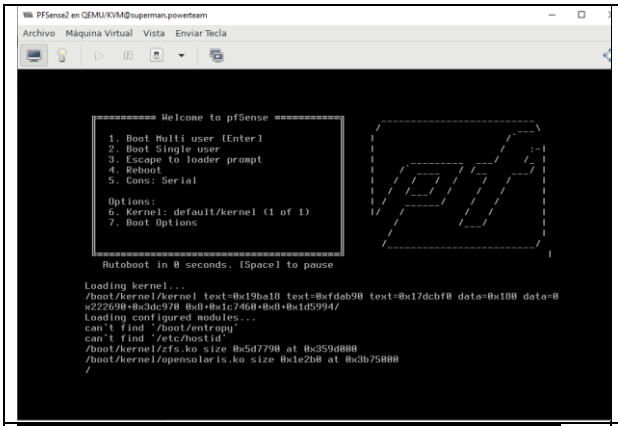
Para poder desarrollar el ejercicio lo primero fue hacer la instalación de PFSense. Se utilizo la versión pfSense-CE-2.7.2 y se instaló en una maquina Oracle Linux sobre el virtualizador

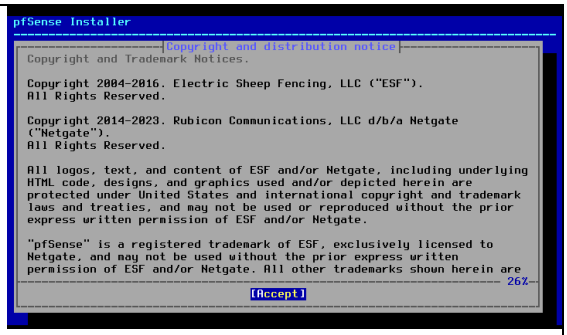
2.1 Instalación

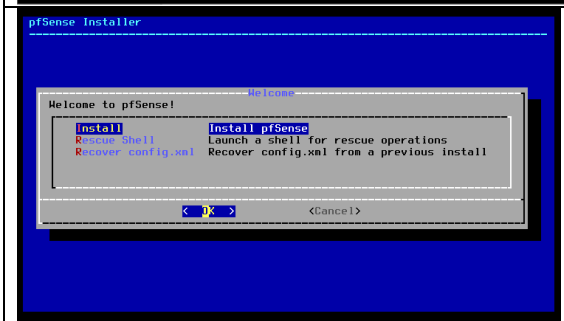
Para la Instalación se utilizo la versión pfSense-CE-2.7.2 y se instalo en una maquina Linux con el virtualizador QEMU, donde se montaron las maquinas virtuales de PFSense, Windows, Kali Linux y Parrot Linux.

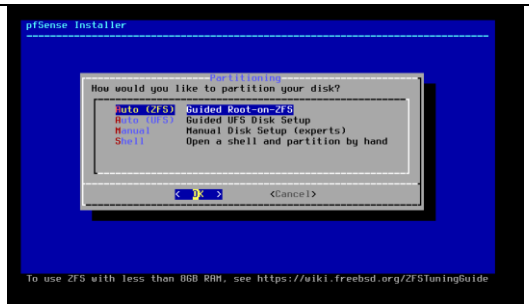
Para la configuración de la maquina virtual de PfSense se habilitaron 4 tarjetas de red y se ejecutó la instalación como se muestra a continuación:

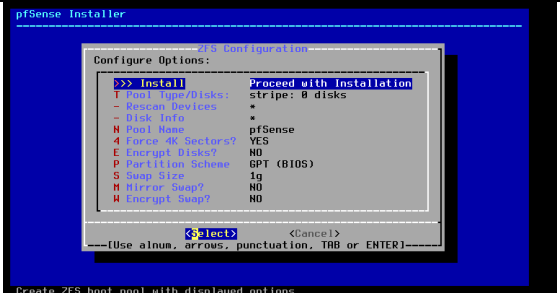



PFSense2 en QEMU/KVM@superman.powerteam
Archivo Máquina Virtual Vista Enviar Tecla
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 0 seconds. [Space] to pause
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
/

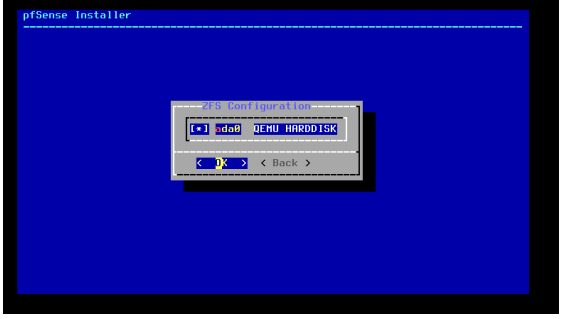

pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or 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]

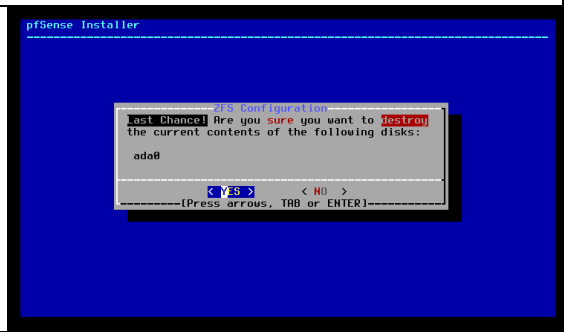

pfSense Installer
Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install
< OK >
<Cancel>

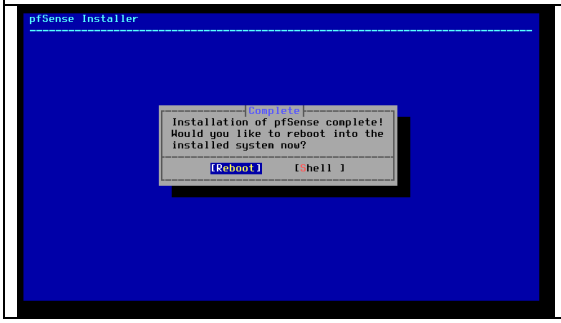

pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide


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

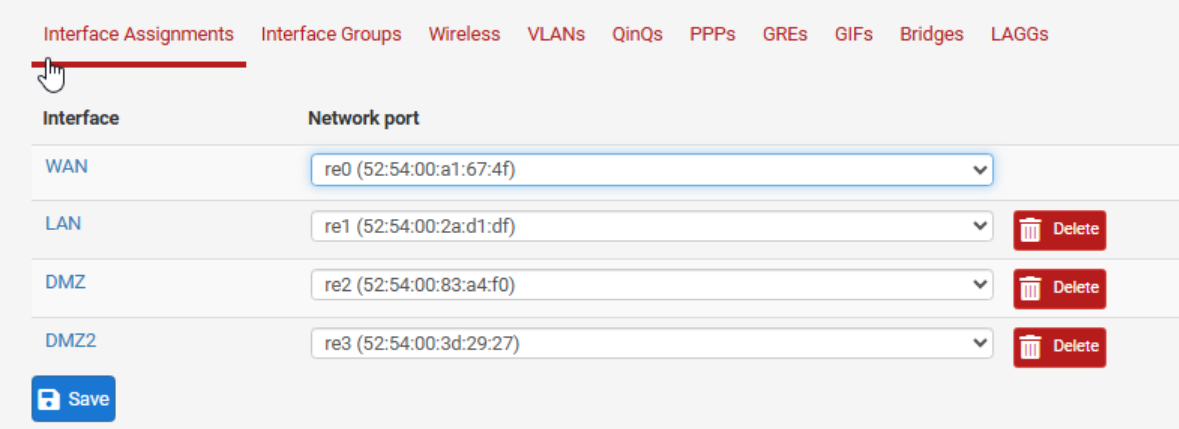

pfSense Installer
ZFS Configuration
[*] ada0 QEMU HARDDISK
< OK > < Back >


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]

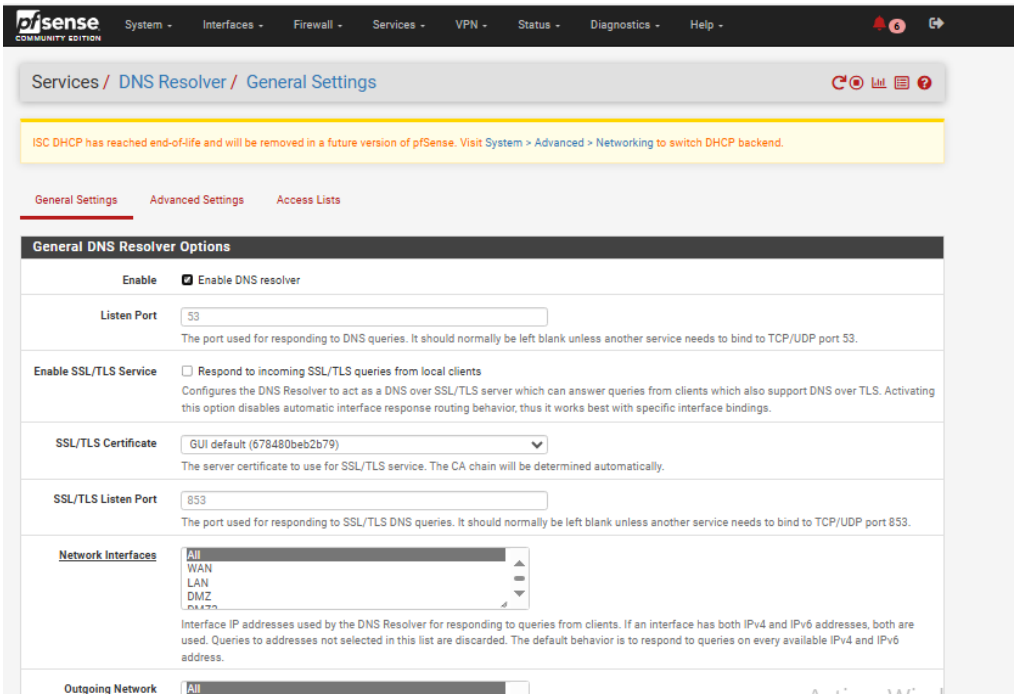
2.2 Configuración

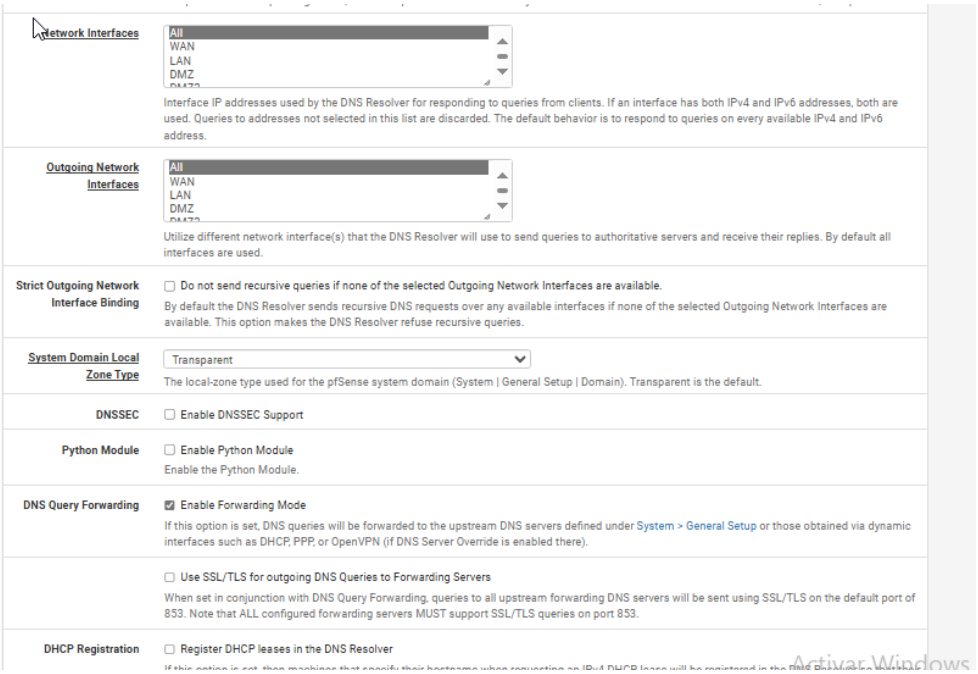
Después de instalar PFSense las tarjeta de Red detectados son las siguientes:



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:



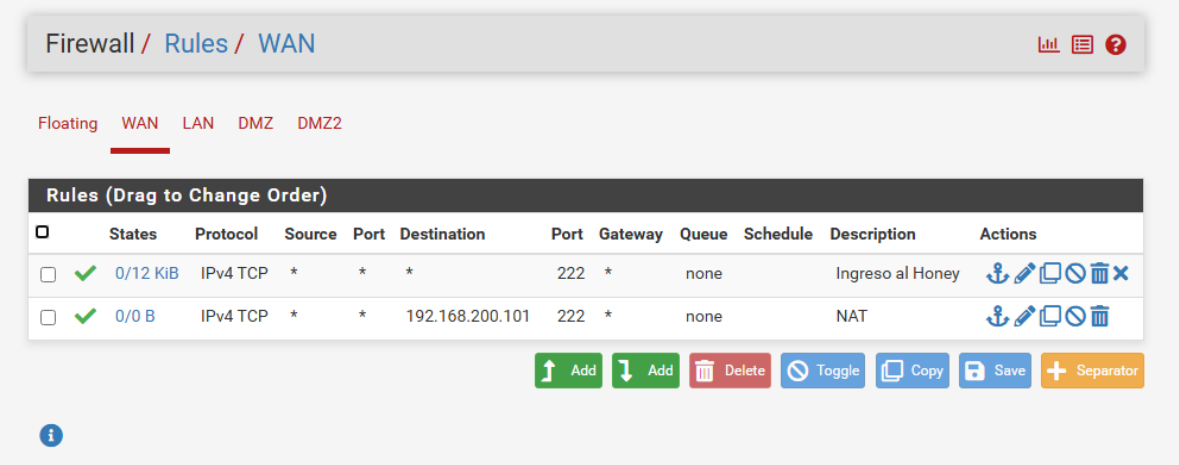


2.2.2 Configuración WAN

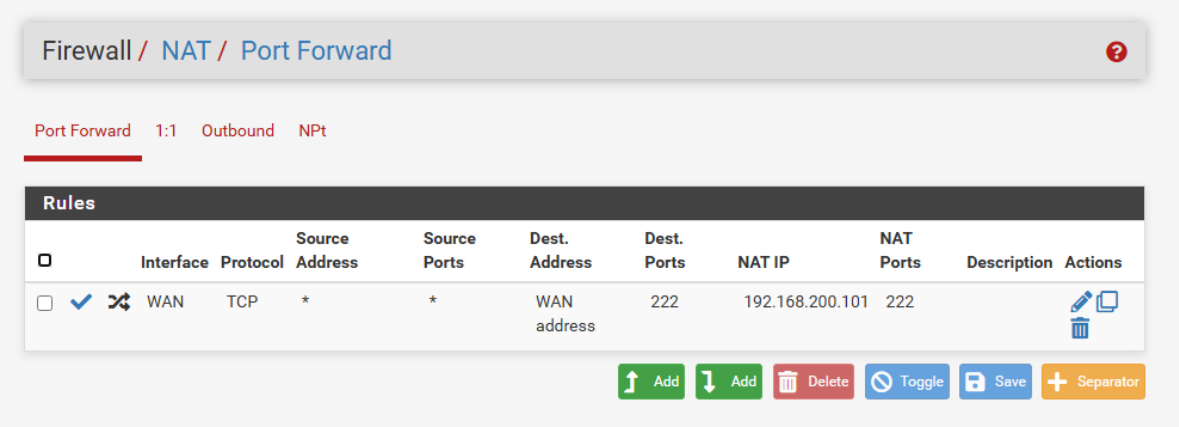
La tarjeta de Red de la WAN identificado internamente como RE0 se configuro en modo Bridge y desde el DHCP del router se le asigna la ip a esta tarjeta. En este caso se le asigno la IP 192.168.0.9. El resumen de esta interface de red es

Nombre: wan
Id: re0
Tipo: Bridge
Mac: 52:54:00:a1:4f
Red:192.168.0.0/24
IP: 192.168.0.13

2.2.3 Configuración Firewall WAN



2.2.4 Configuración Firewall NAT Port Forward



2.2.5 Configuración LAN

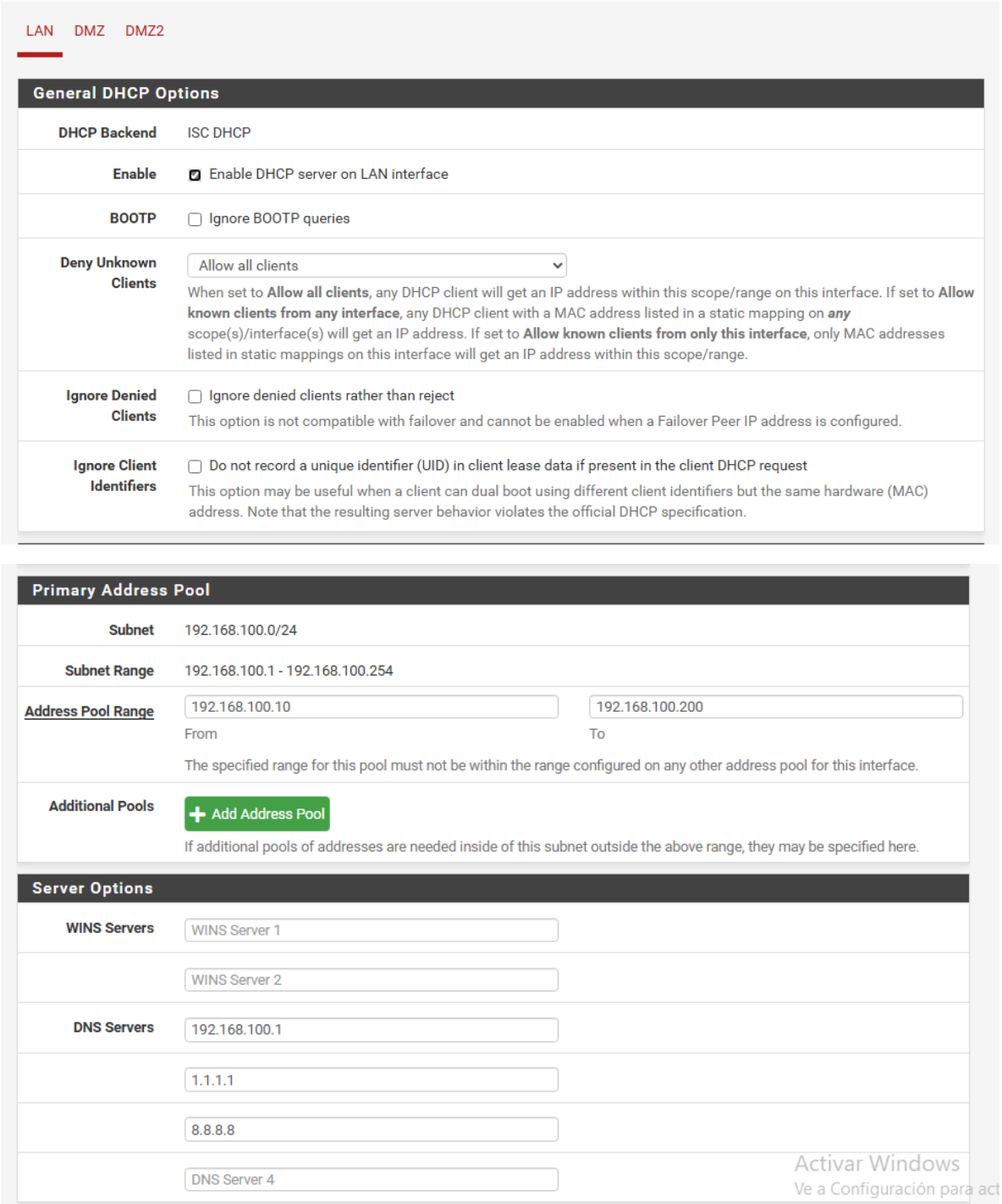
La tarjeta de Red de la LAN identificado internamente como RE1 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red 10.10.0.0/16 y se le asignó la primera IP (10.10.0.1).

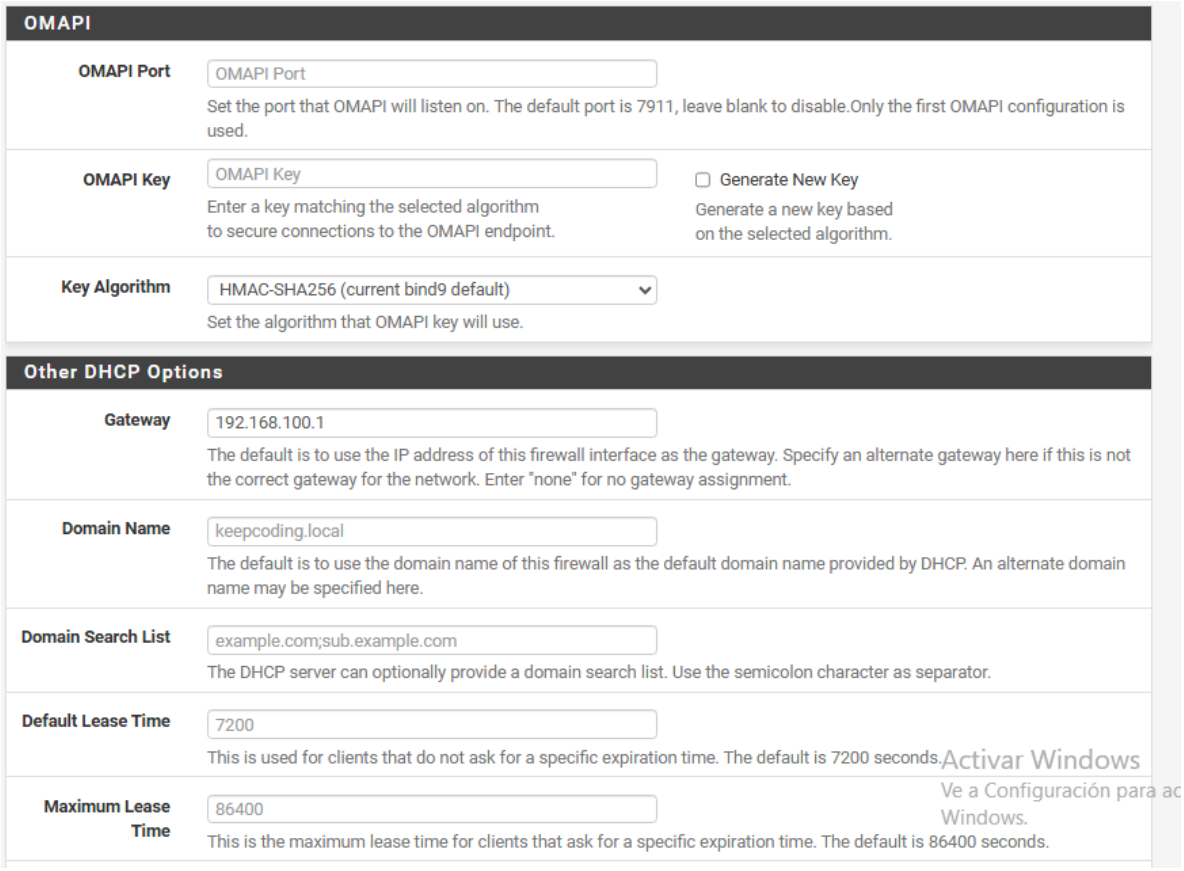
El resumen de esta interface de red es

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

2.2.6 Configuración DHCP LAN

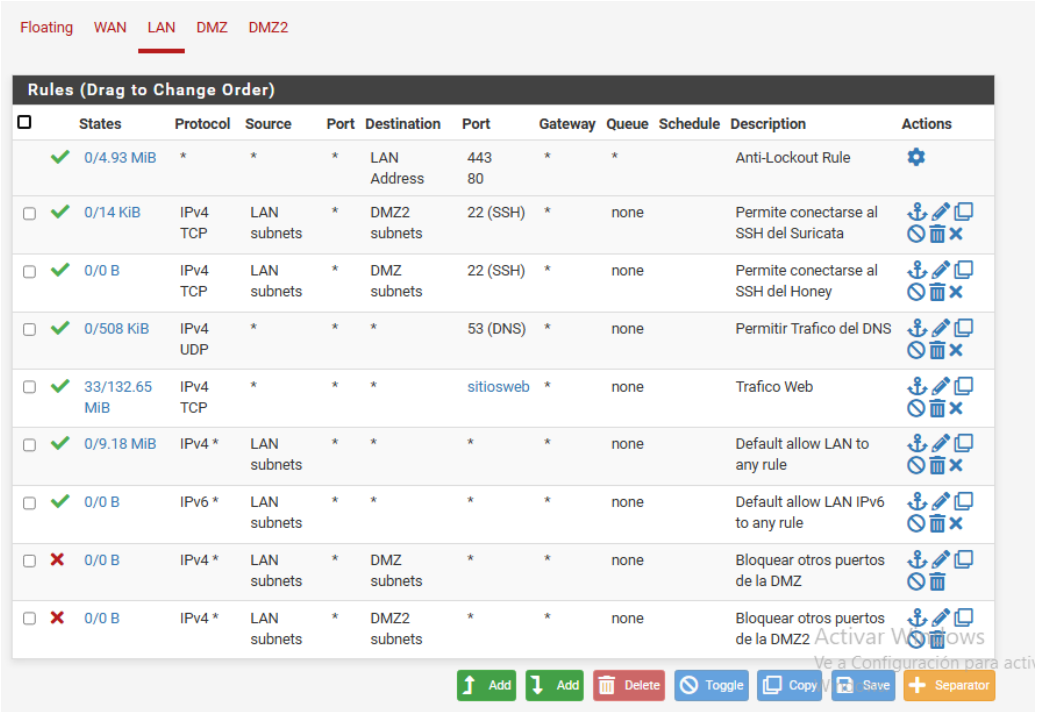
Adicionalmente se configuro un servidor DHCP para que entregue direcciones en el rango 192.168.100.10 – 192.168.100.200





2.2.7 Configuración REGLAS FIREWALL LAN

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



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

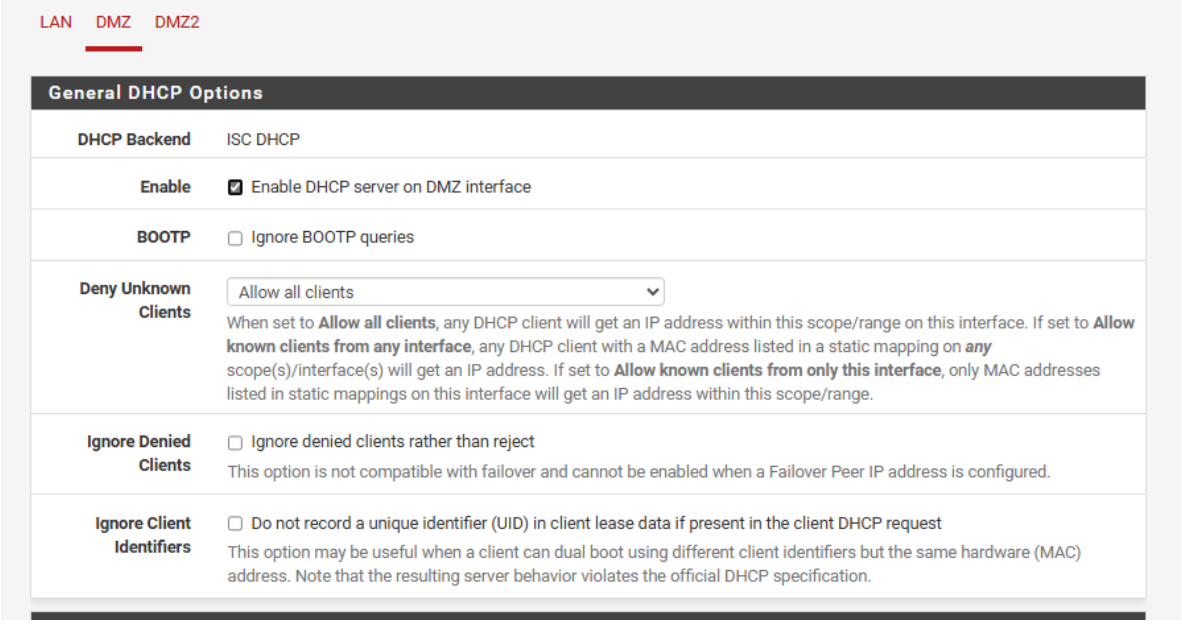
2.2.8 Configuración DMZ

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

2.2.9 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



Primary Address Pool

Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	192.168.200.100 (From) — 192.168.200.150 (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

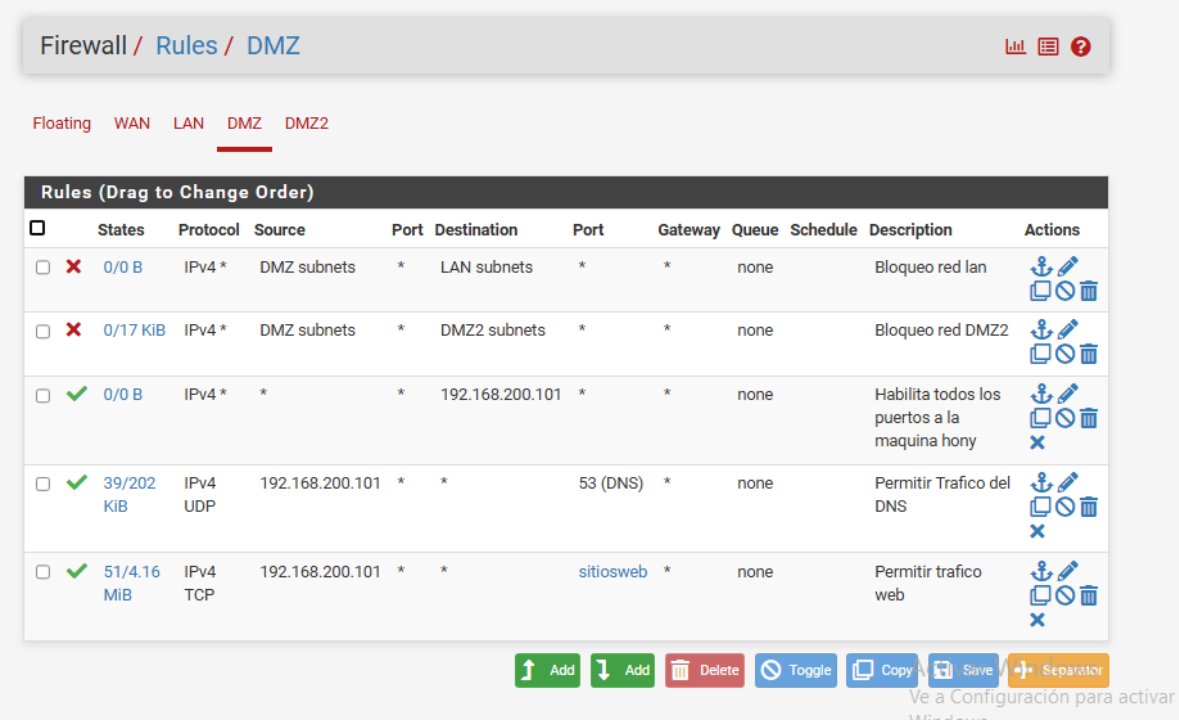
WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.200.1
	1.1.1.1
	8.8.8.8
	DNS Server 4

Other DHCP Options

Gateway	192.168.200.1
	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.

2.2.10 Configuración REGLAS FIREWALL DMZ

Para las reglas del DMZ se establecieron cuatro reglas asi:



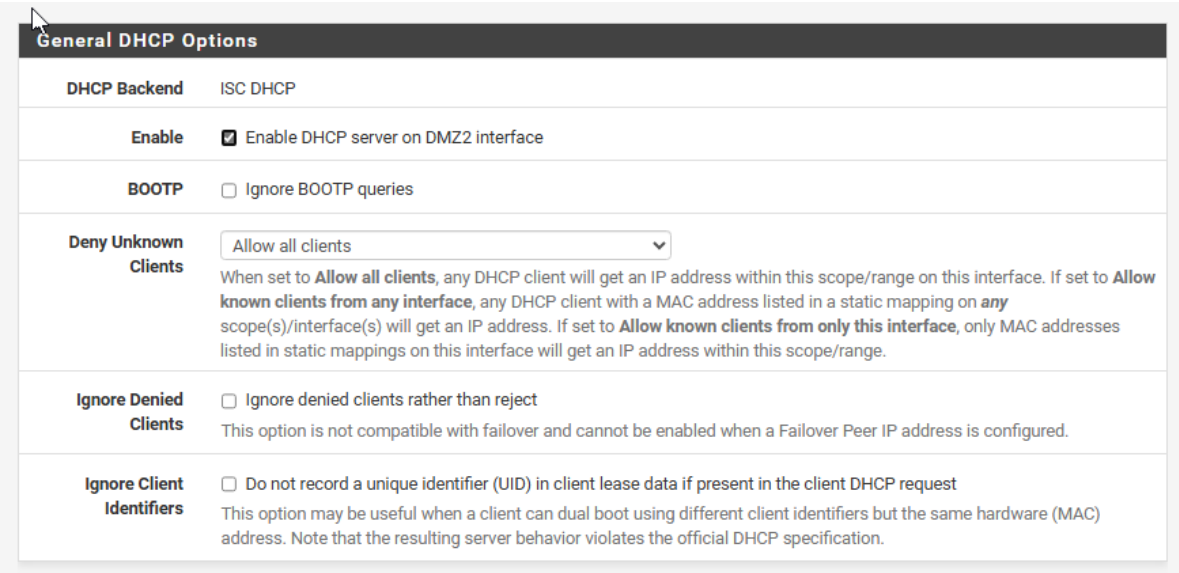
2.2.11 Configuración DMZ2

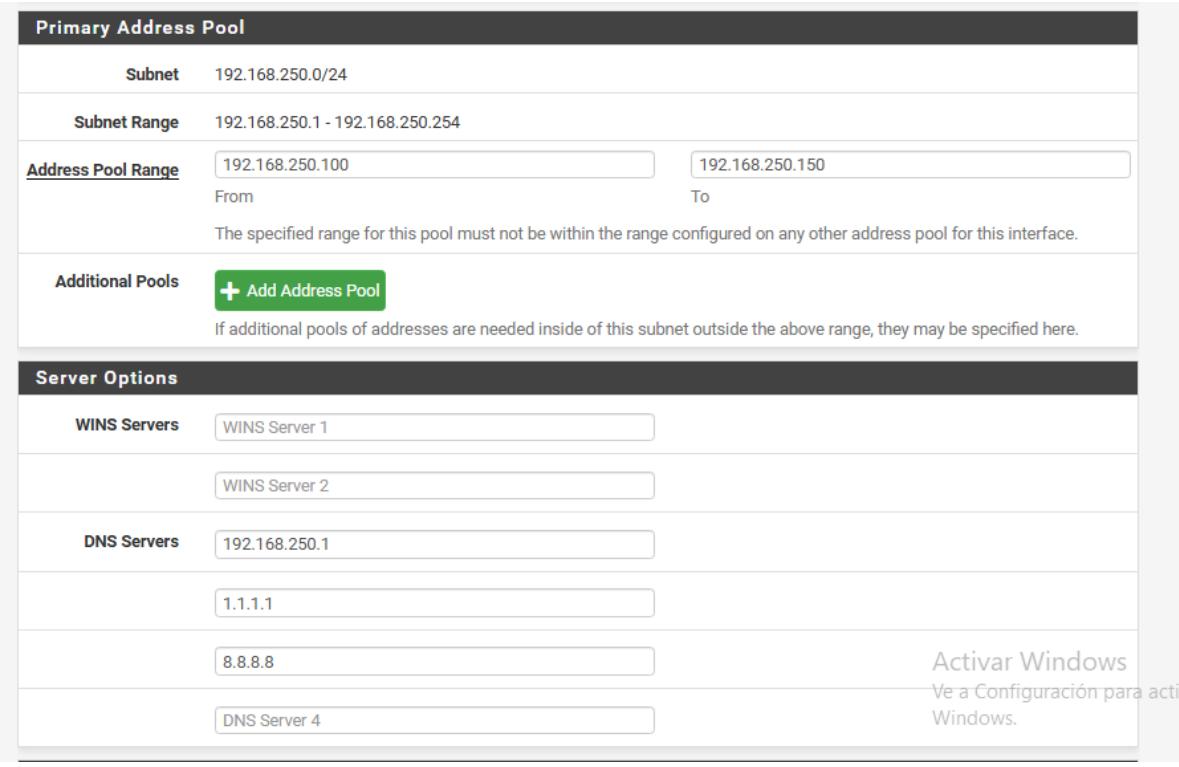
La tarjeta de Red de la DMZ2 identificado internamente como RE3 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red (192.168.250.1).

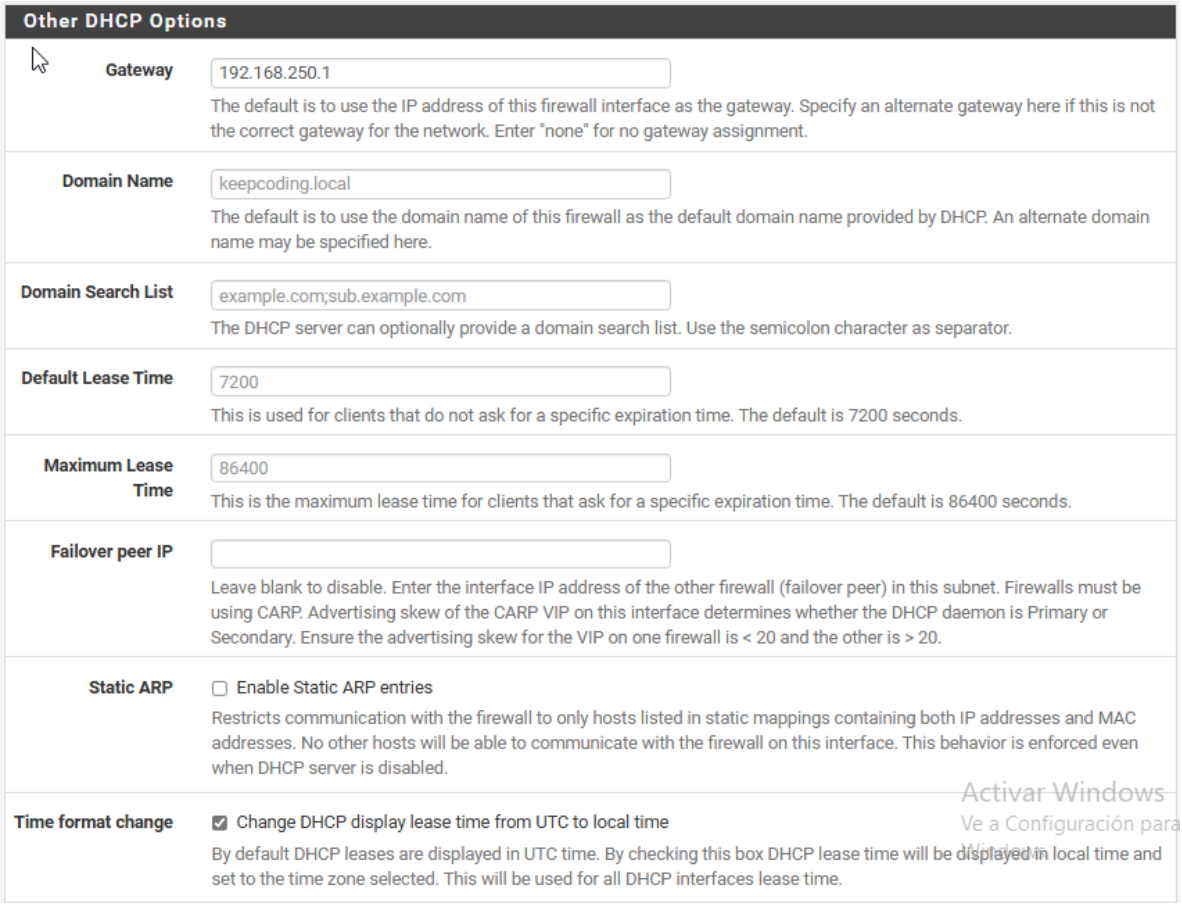
Nombre: DMZ2
Id: re3
Tipo: Interna
Mac: 52:54:00:3d:29:27
Red: 192.168.250.1/24
Rango de IPs: 192.168.250.1 - 192.168.250.254
IP: 192.168.250.1

2.2.12 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

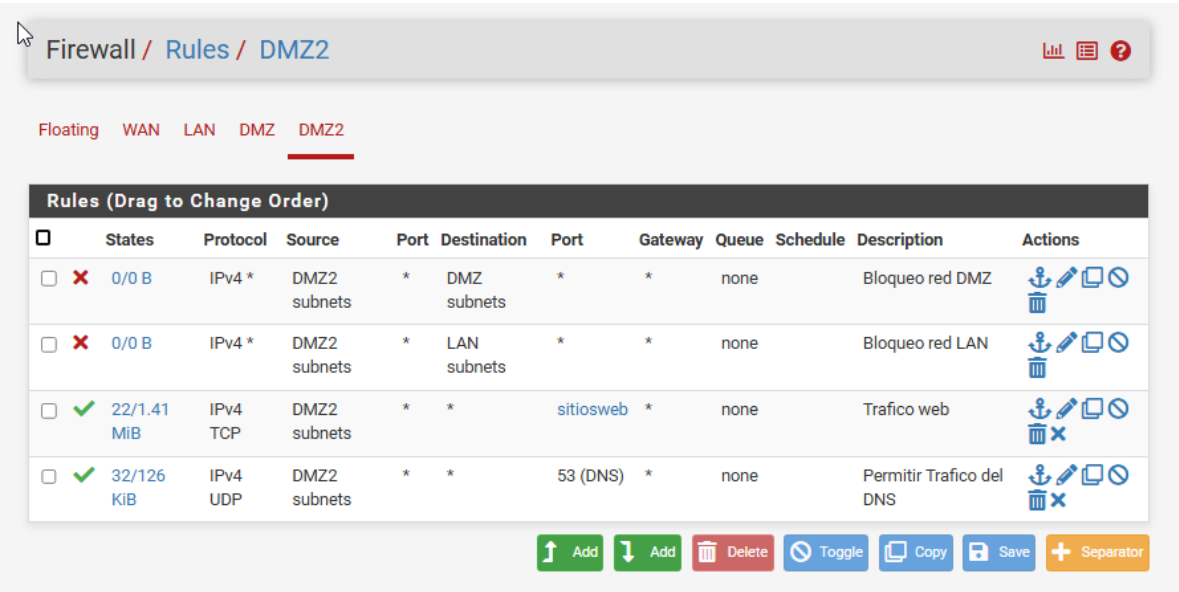






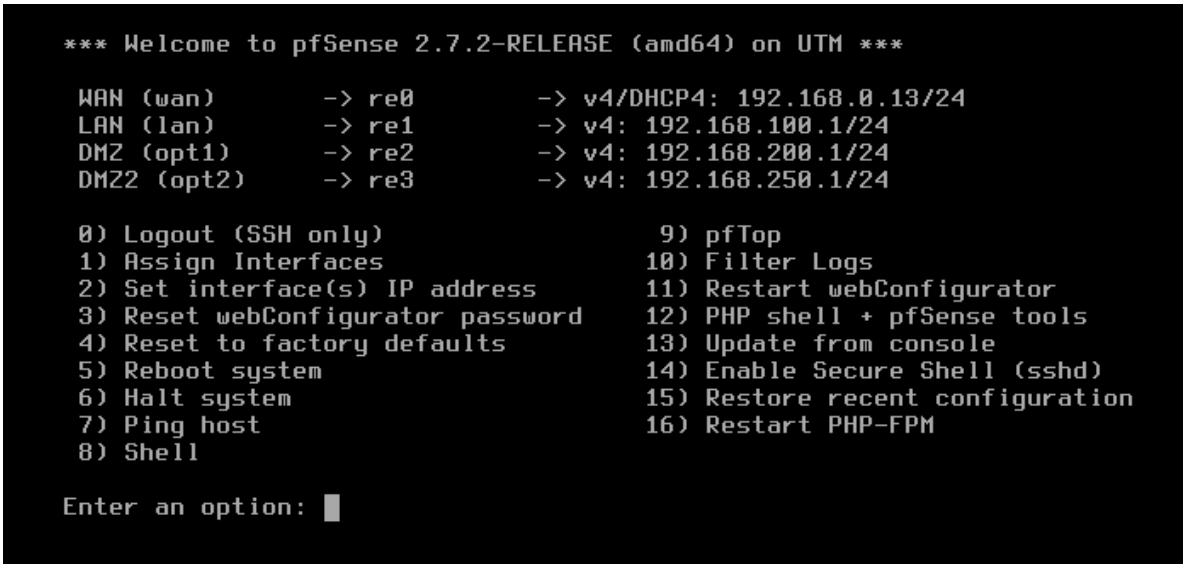
2.2.13 Configuración REGLAS FIREWALL DMZ2

Para las reglas del DMZ2 se establecieron dos reglas asi:



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

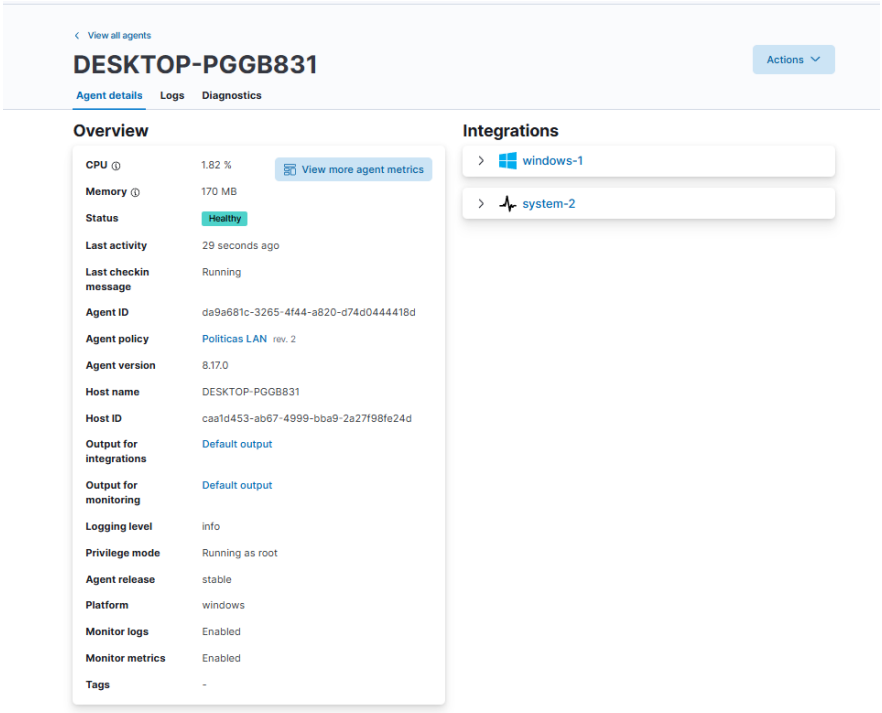
3.1 Configuración Windows 10 (LAN)

3.1.1 Configuración del Agente

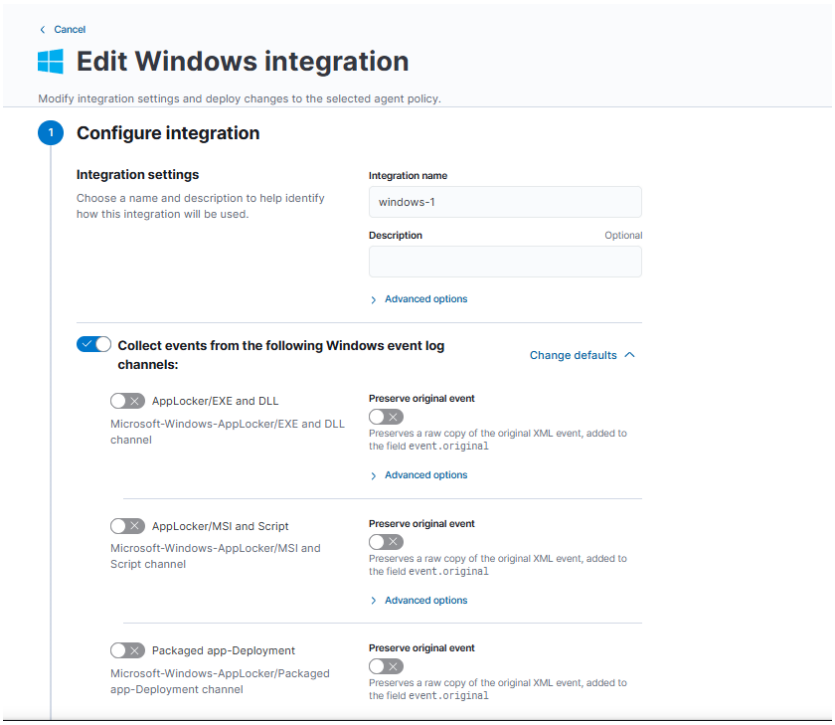
En una máquina virtual de Windows 10 llamada DESKTOP-PGGB831 que instaló el agente de Elastic elastic-agent-8.17.0 para Windows

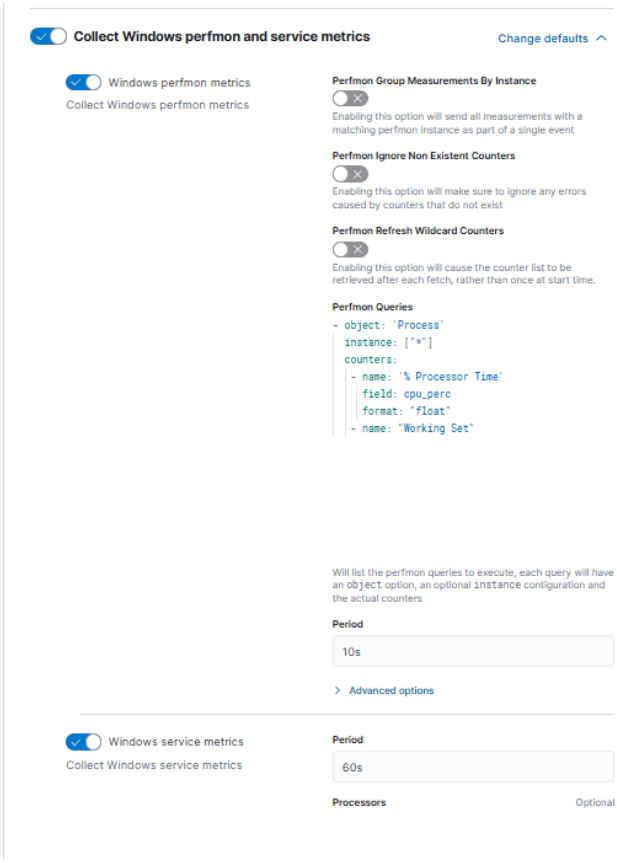
Para su instalación en Windows después de descomprimirlo se ejecuto la instalación con este comando

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

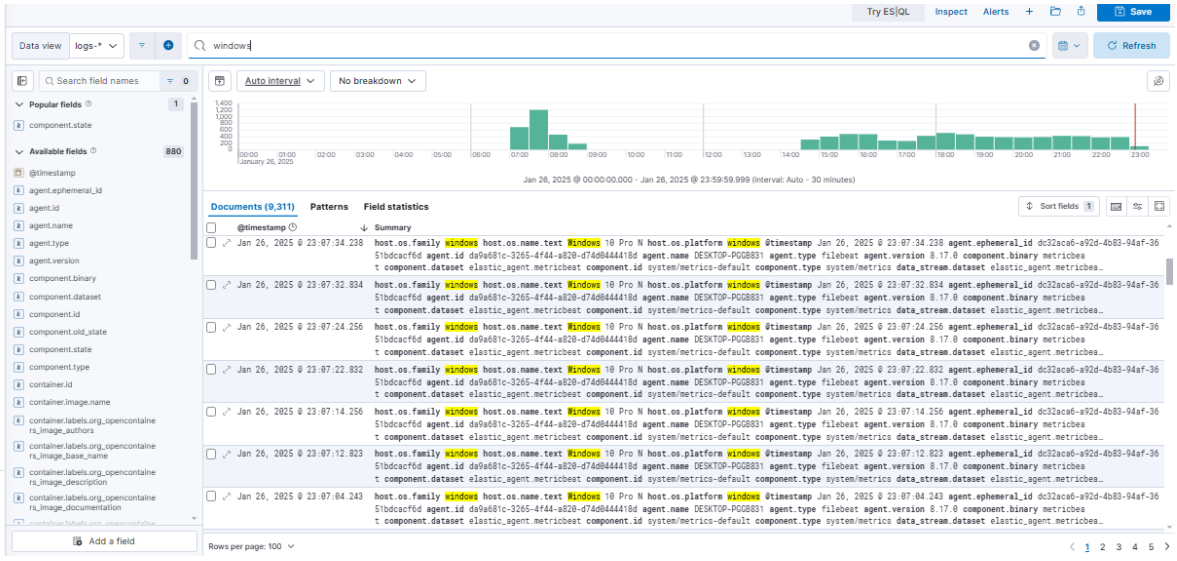


Una vez instalado desde Elastic cloud que añadió una integración para leer los logs de Windows asi:





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/evidenciaswindows3.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/practicaskeepcoding/blob/main/BlueTeam/windows3.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

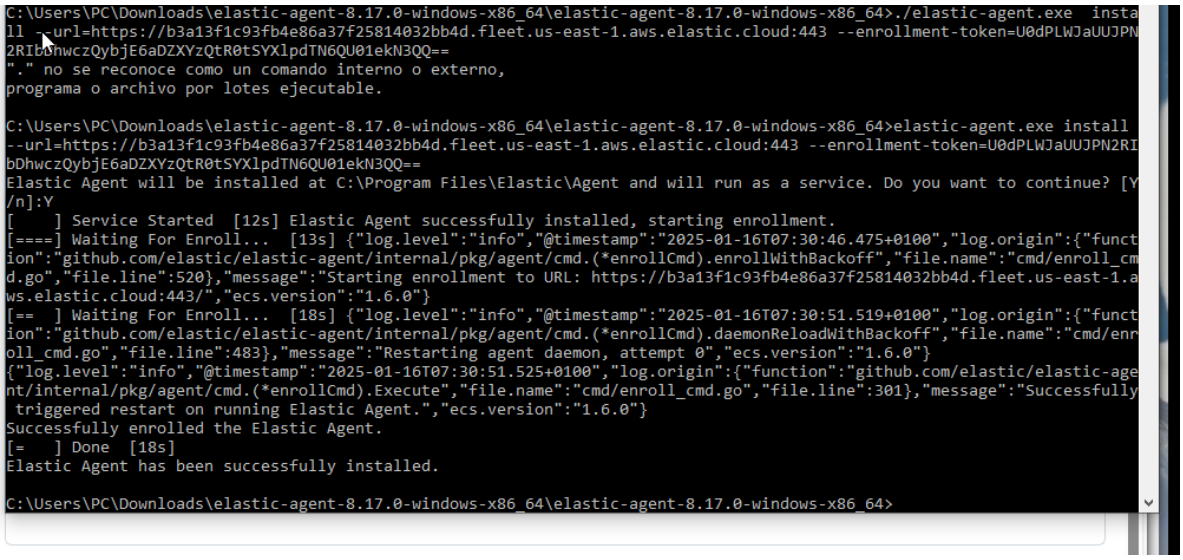
Una vez funcionando que instalo en agente de elastic asi:

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

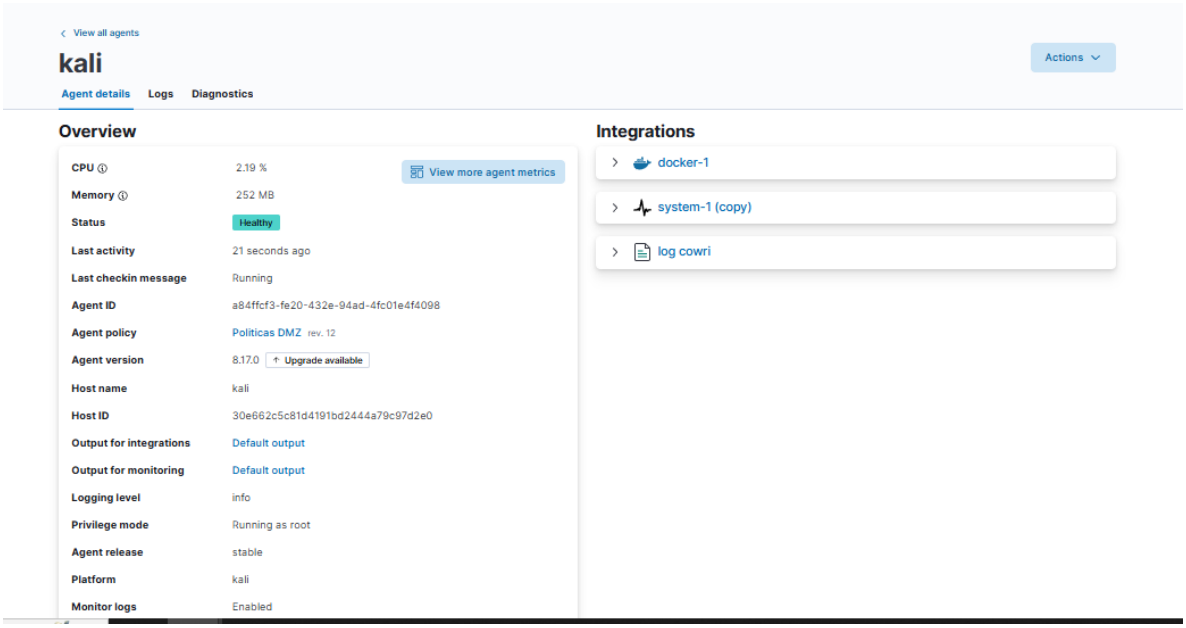
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz

cd elastic-agent-8.17.0-linux-x86_64

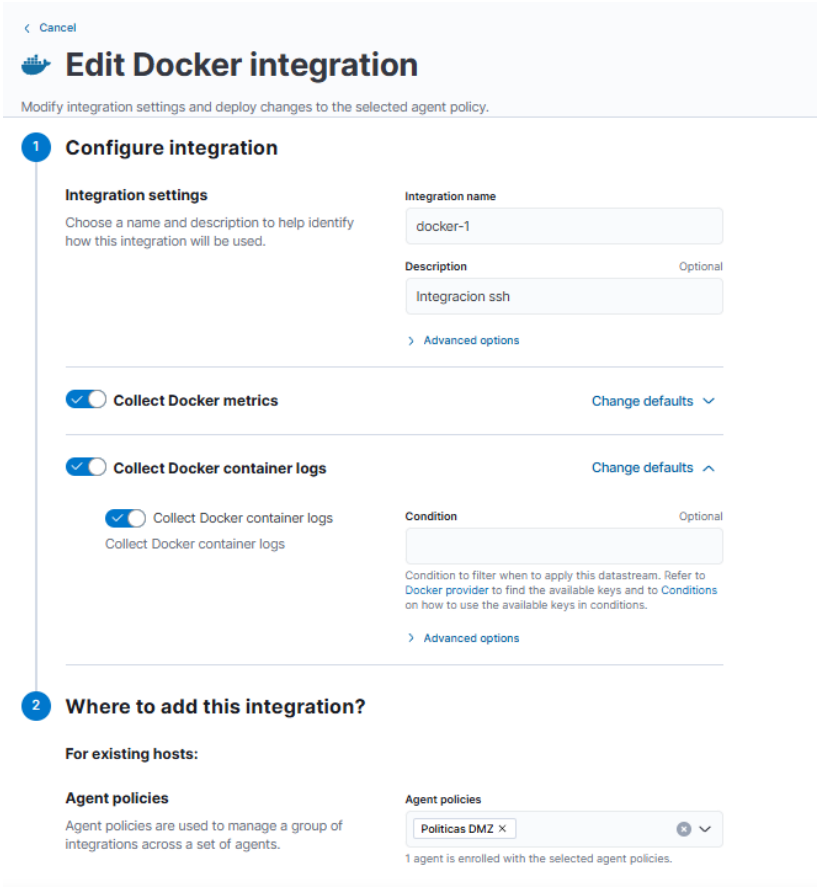
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RIbDhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==



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

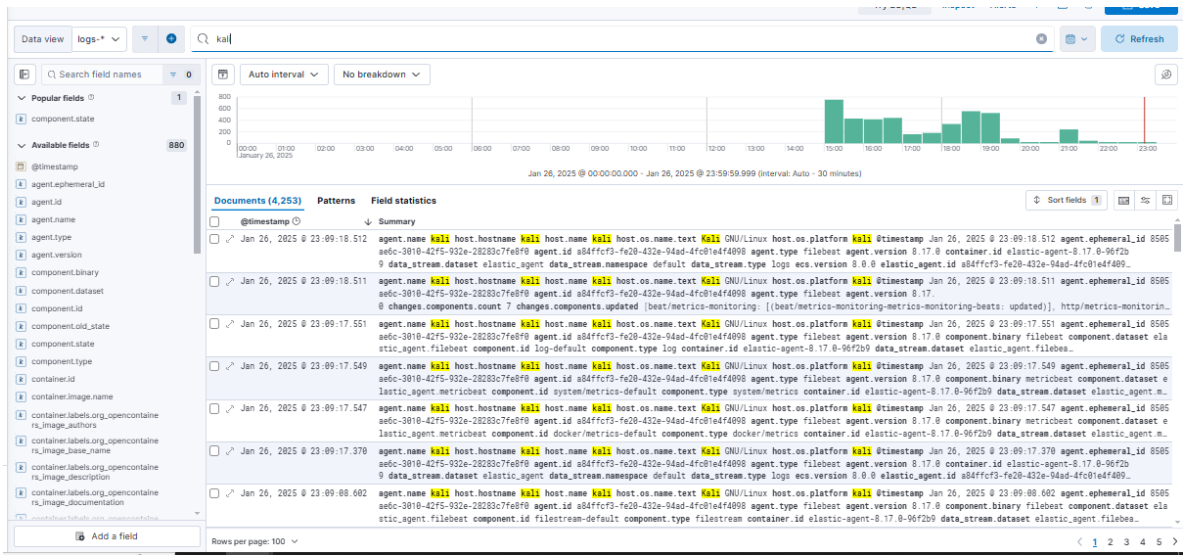


Adicionalmente Tambien se tomo una integración para leer los logs del docker



3.2.3 Evidencias de recepción de logs

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



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

https://github.com/oscartobar/practicaskeepcoding/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/practicaskeepcoding/blob/main/BlueTeam/kali-ssh3.csv

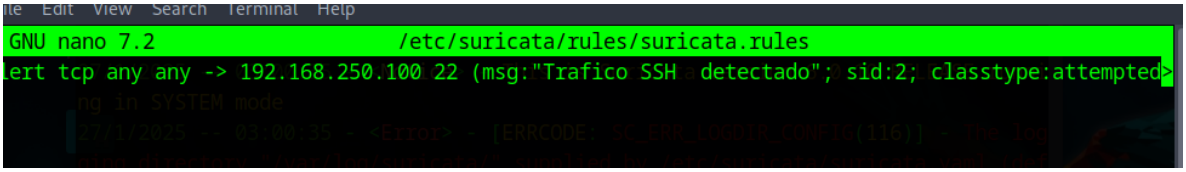
3.3 Configuración Suricata (DMZ2)

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

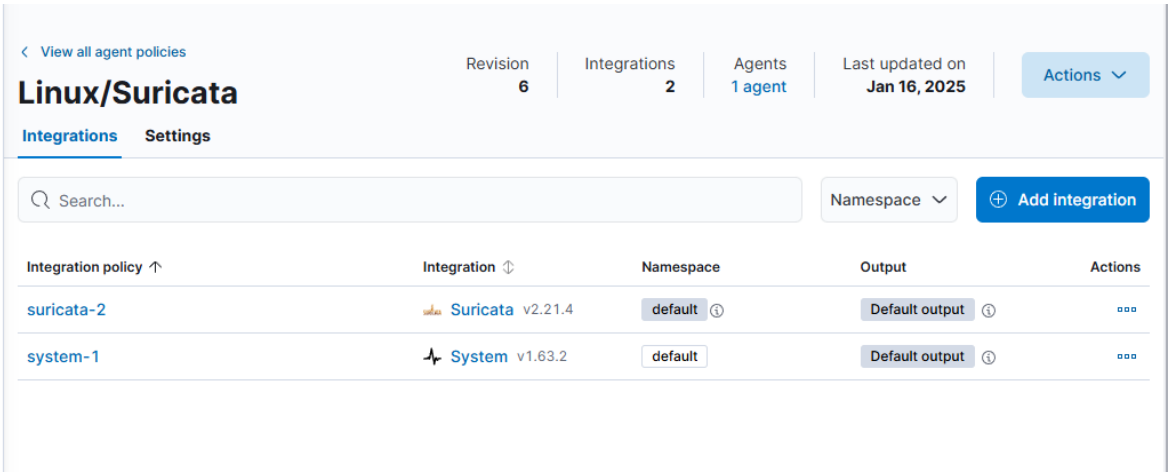
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz

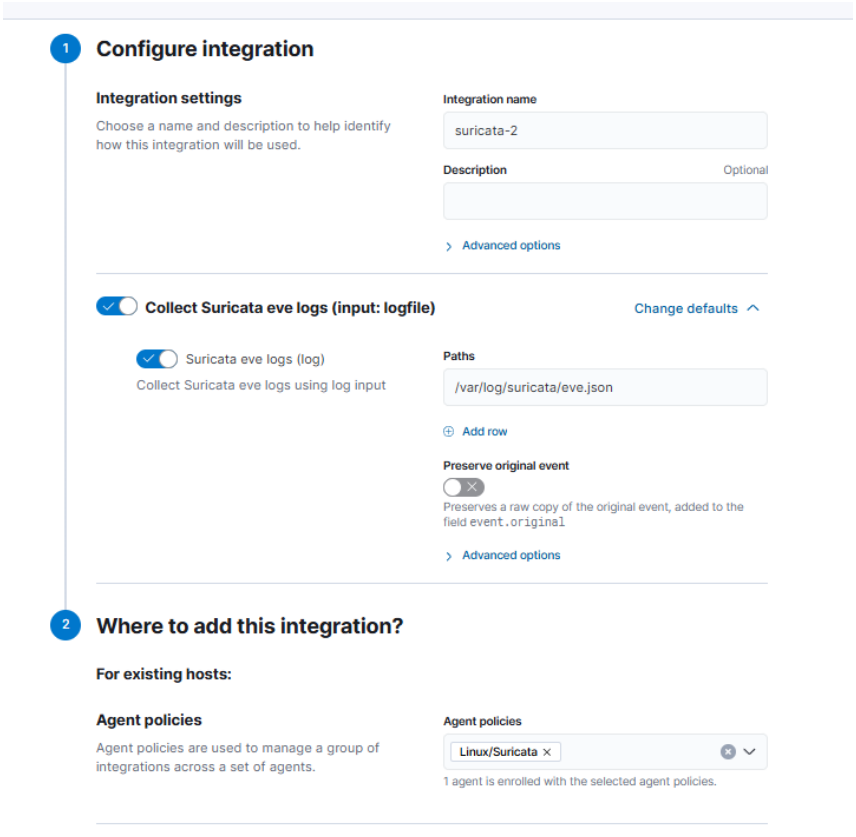
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz

cd elastic-agent-8.17.0-linux-x86_64

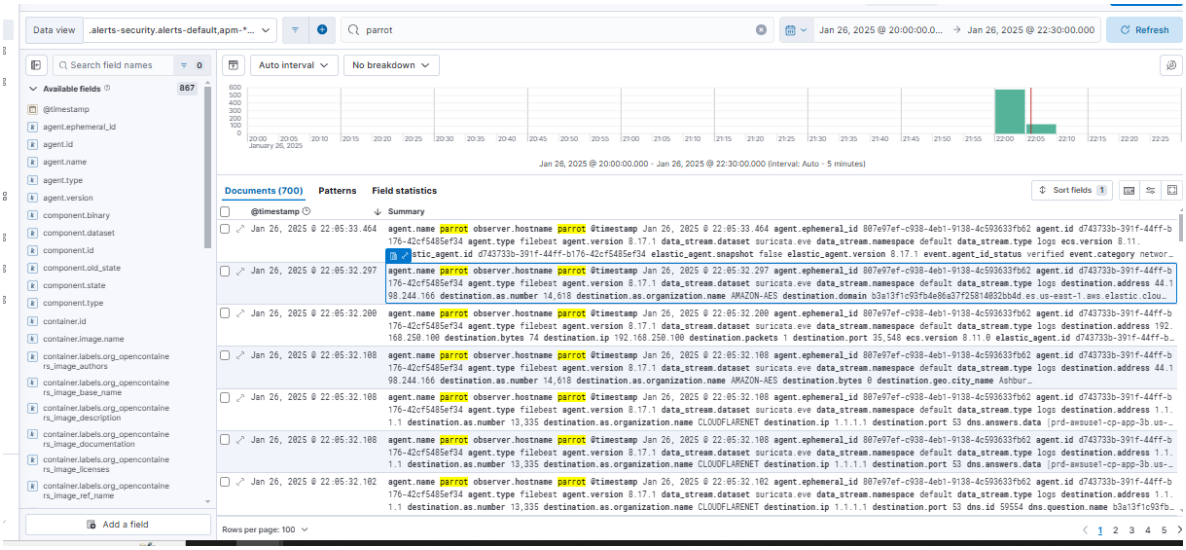
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RIbDhwc2tXbFU6ZVlGSWlHZGJTbFNKajhETWlnd2J5dw==

Luego desde Elastic se configuro una nueva integración asi


View all agent policies
Linux/Suricata
Revision
6
Integrations
2
Agents
1 agent
Last updated on
Jan 16, 2025
Actions
Integrations
Settings
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


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

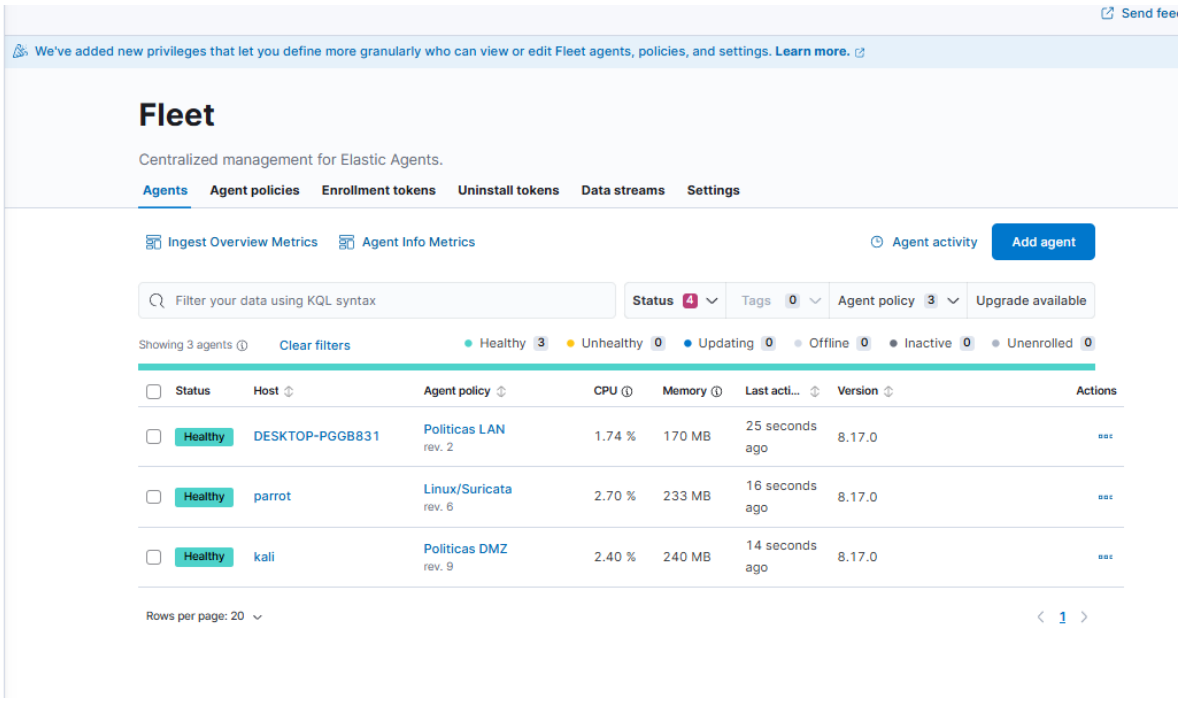
https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciasuricata3.txt

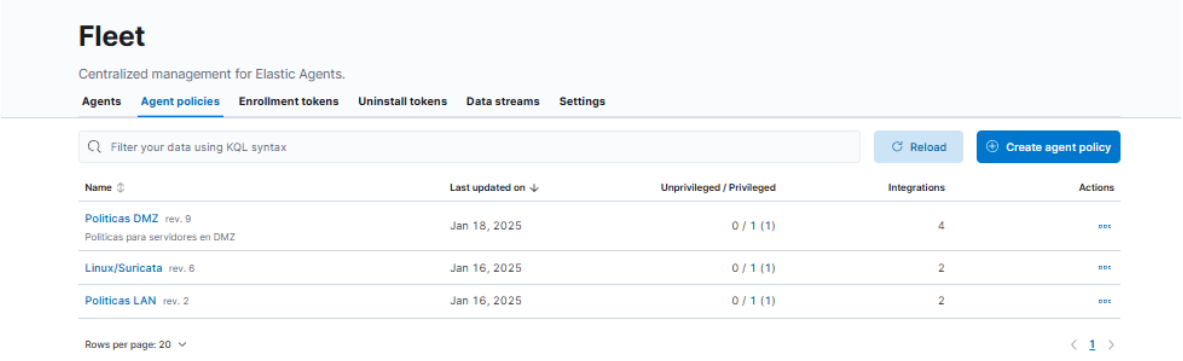
La información de todos los logs de suricata recibidos en elastic y transmitidos desde el parrot el día 26 de enero se dejan aquí

https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/suricata3.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

Politicas para servidores en DMZ

Revision 12 | Integrations 3 | Agents 1 agent | Last updated on Jan 26, 2025 | Actions

Integrations | Settings

Search...

Namespace | Add integration

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


View all agent policies
Linux/Suricata
Revision
6
Integrations
2
Agents
1 agent
Last updated on
Jan 16, 2025
Actions
Integrations
Settings
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