

# Memoria Ciberseguridad

---

Evaluación BlueTeam

---



Nombre del Auditor: Kacper Mariusz Koper Mielczarek

Fecha: 20/02/2025

## Índice

<i>Memoria Ciberseguridad</i> .....	<b>1</b>
<i>PfSense</i> .....	<b>3</b>
Instalación PFsense .....	3
Creación de las redes en VirtualBox.....	9
Configuración PfSense.....	<b>12</b>
Pasos iniciales.....	12
Vamos a configurar la resolución DNS .....	16
Configuración DHCP -> DMZ y DMZ2.....	23
Establecer IP estática.....	26
Establecemos alias .....	29
Creamos las reglas de los FW (firewall) .....	29
<i>ElasticCloud</i> .....	<b>34</b>
Creación de cuenta de ElasticCloud.....	34
Configuración ElasticCloud.....	<b>34</b>
Integración de los logs en Windows .....	36
Integración de los logs del Honeypot en Elastic.....	37
<i>Integración de los logs de Apache y Suricata</i> .....	<b>38</b>
Suricata .....	38
<i>Configuración final de las políticas de Elastic</i> .....	<b>40</b>
<i>Logs</i> .....	<b>41</b>
<i>Propuesta de mejora</i> .....	<b>42</b>

## PfSense

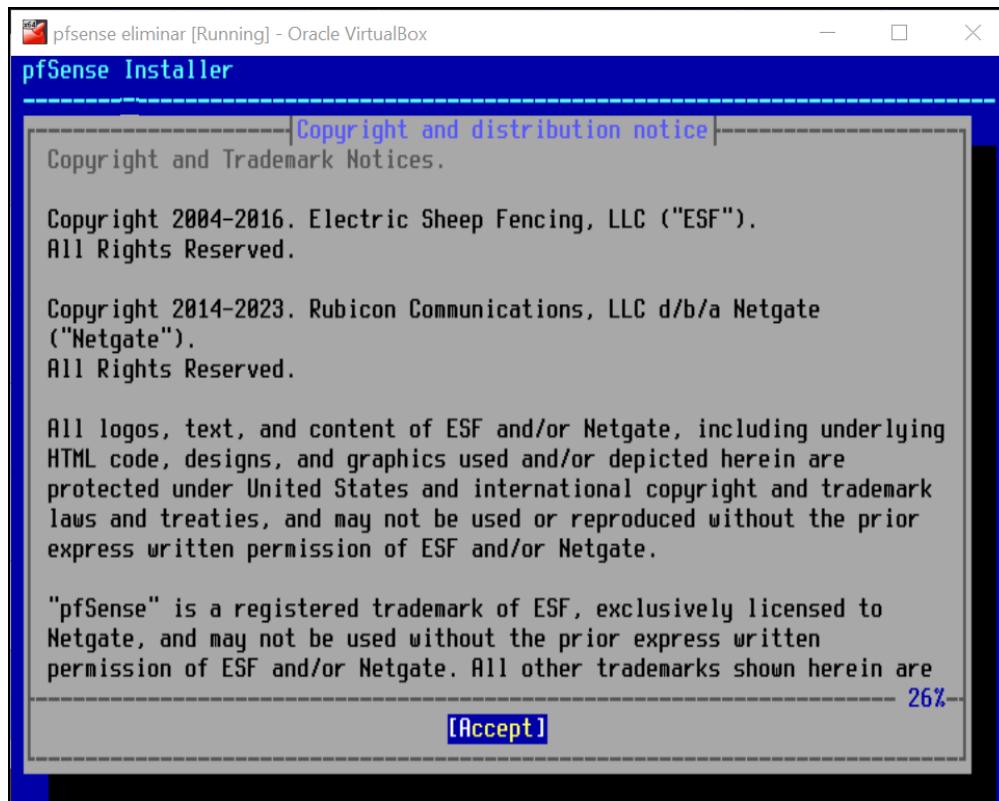
- SO: free BSD
- Memoria: 1024MB
- CPUs: 2
- Almacenamiento: 16GB

### Instalación PFsense

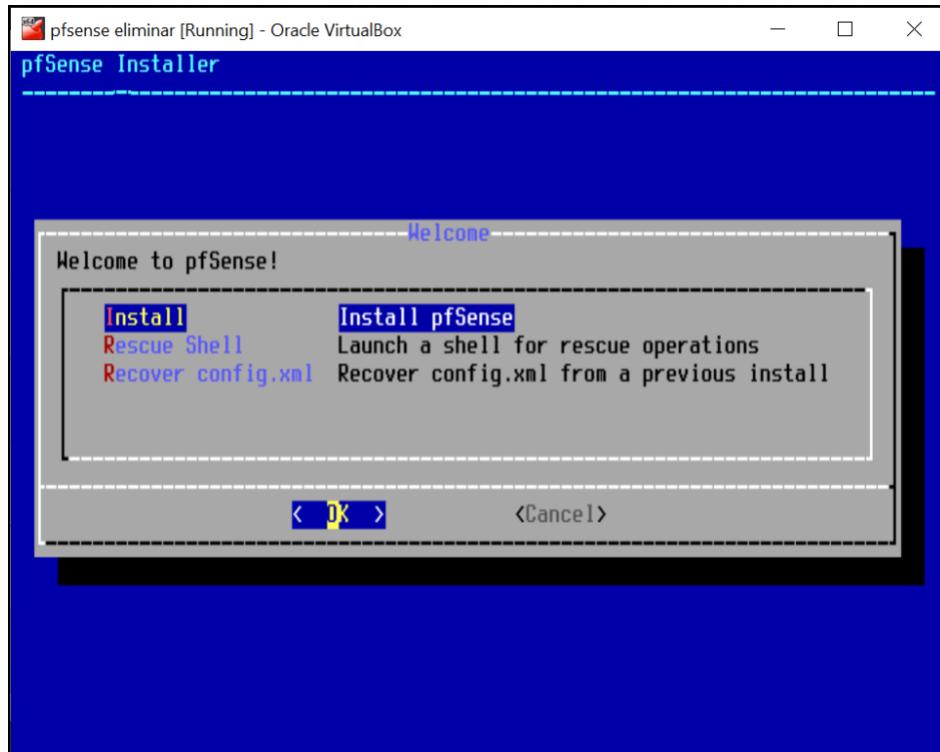
En esta primera etapa de la práctica, se realizó la instalación y configuración inicial de **Pfsense**, un sistema UTM (Unified Threat Management) utilizado para gestionar y controlar el tráfico de red de los equipos conectados. Inicialmente, se procedió con la instalación del sistema y la configuración básica, asignando las interfaces correspondientes para las redes internas (**LAN**) y externas (**WAN**). Este proceso permitió establecer los parámetros iniciales para obtener conexión en red.

Finalmente, se verificó el correcto funcionamiento de la máquina, comprobando que las interfaces asignadas operan según lo esperado. Se obtuvo con éxito el dato de las direcciones asignadas a la **WAN** y la **LAN**, confirmando que el sistema está preparado para proceder a gestionar las diferentes reglas del Pfsense.

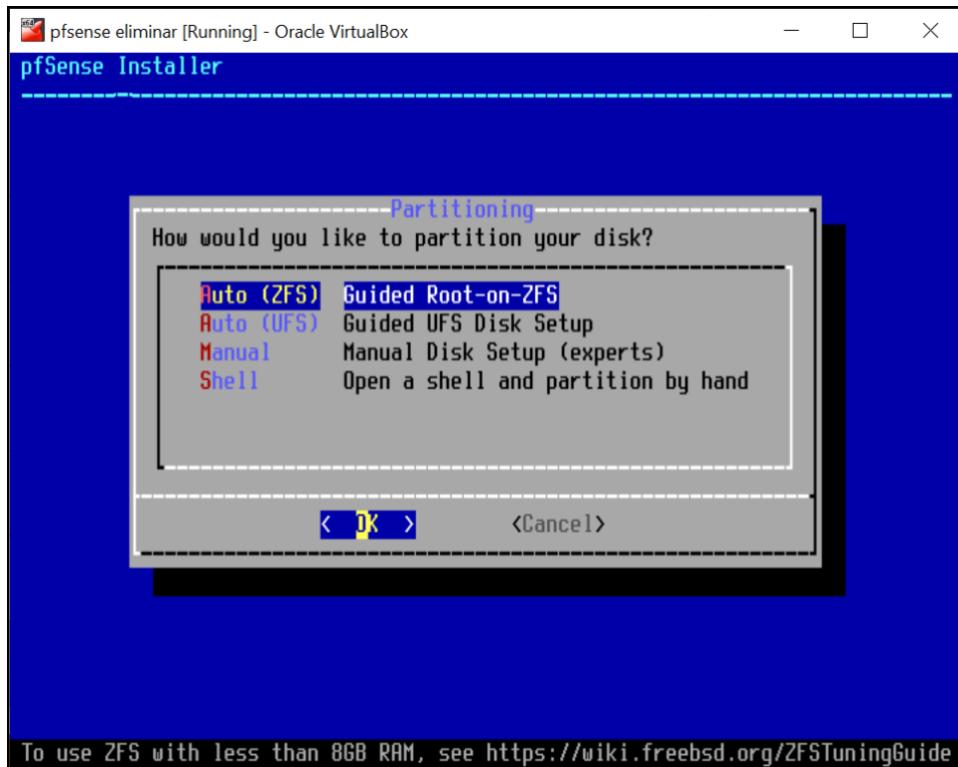
1. Accept copyright.



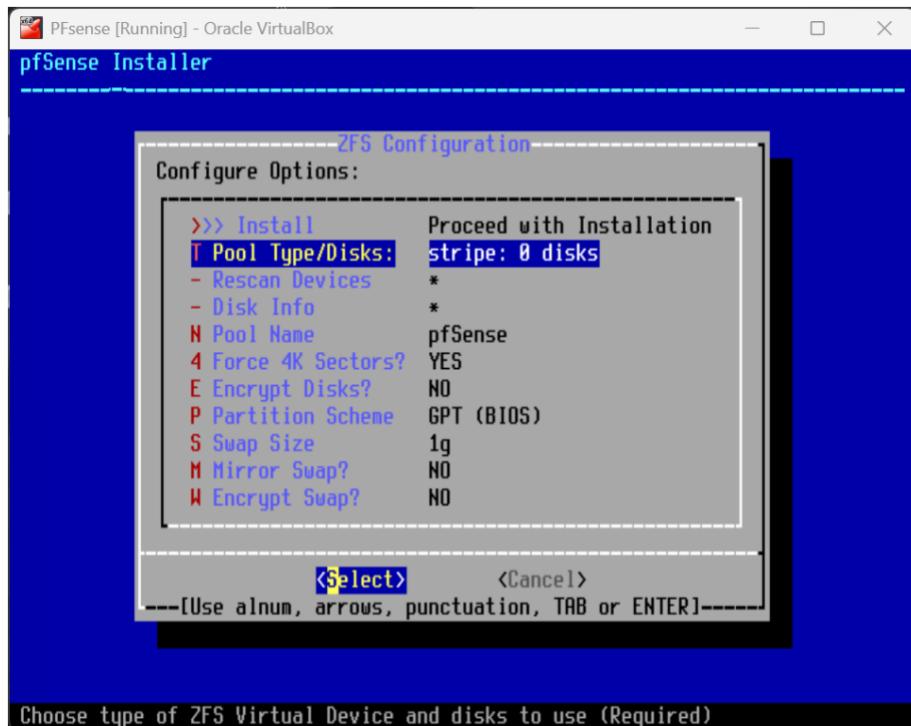
2. Install.



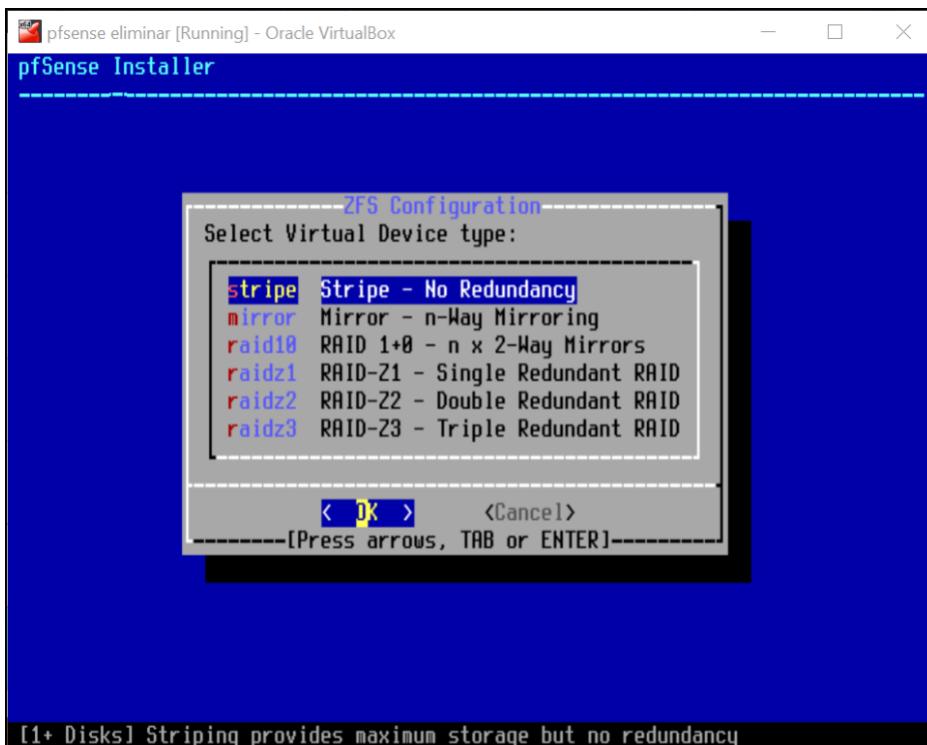
3. Guided Root-on-ZFS.



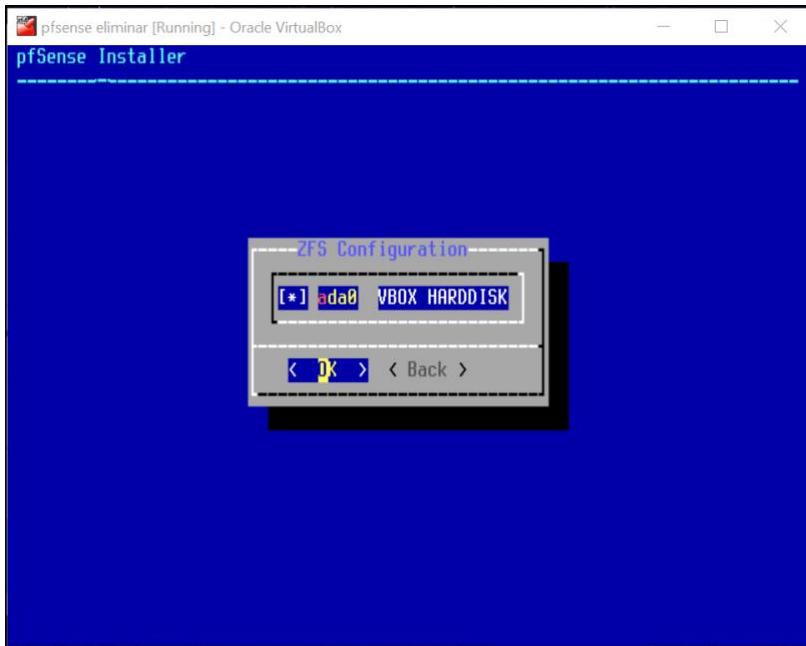
4. Pool Type/Disk.



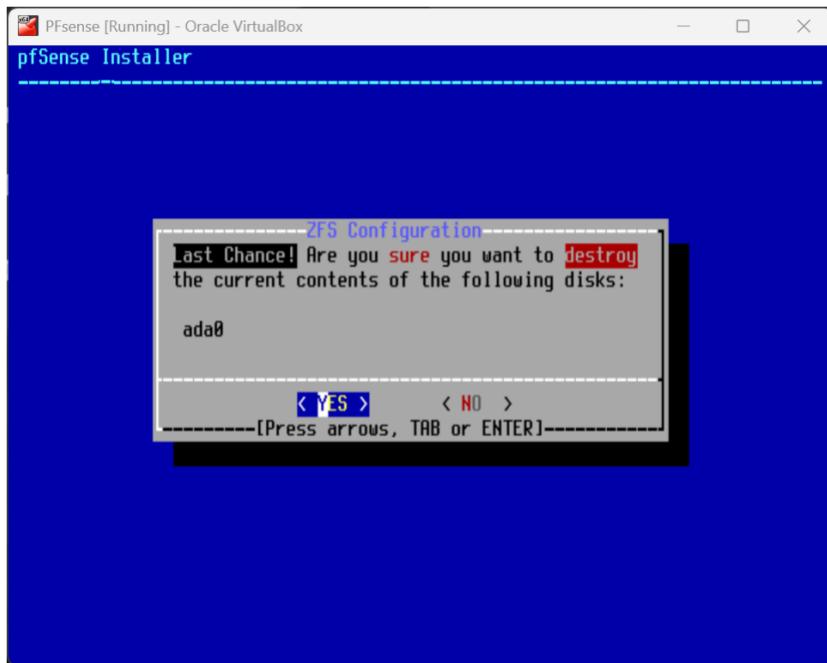
5. Stripe Stripe – No Redundancy.



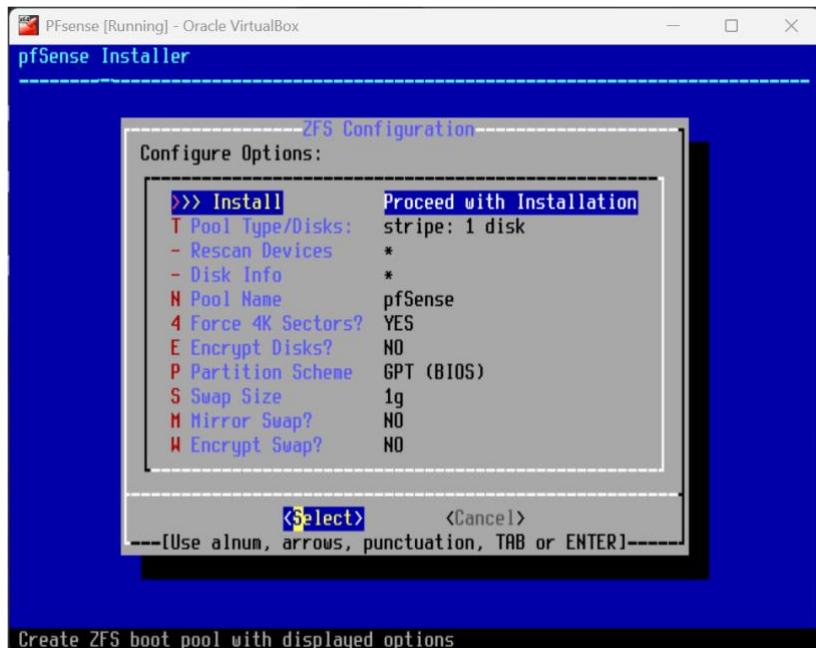
6. ada0 VBOX HARDDISK.



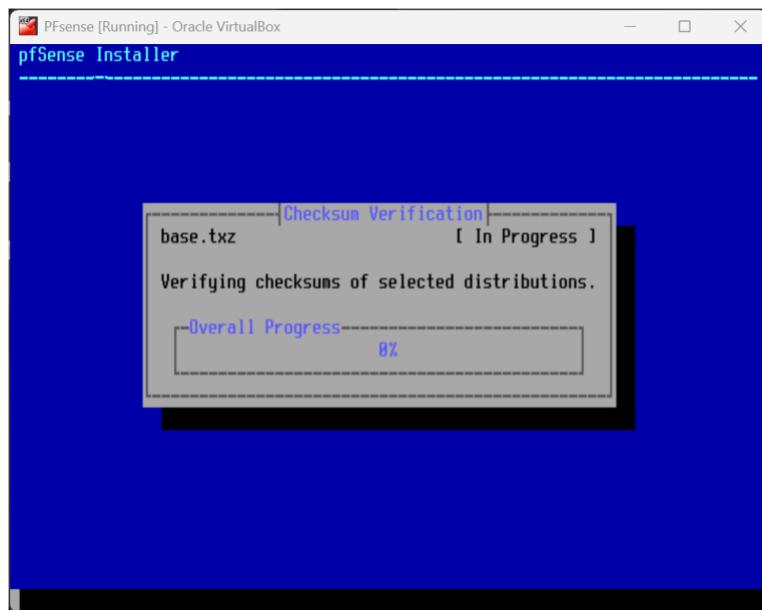
7. Destroy.



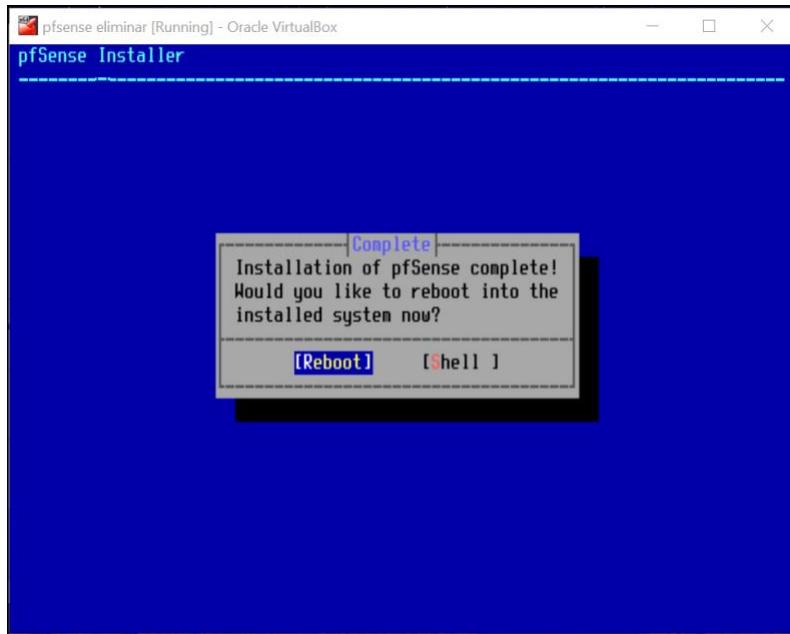
8. Proceed with installation.



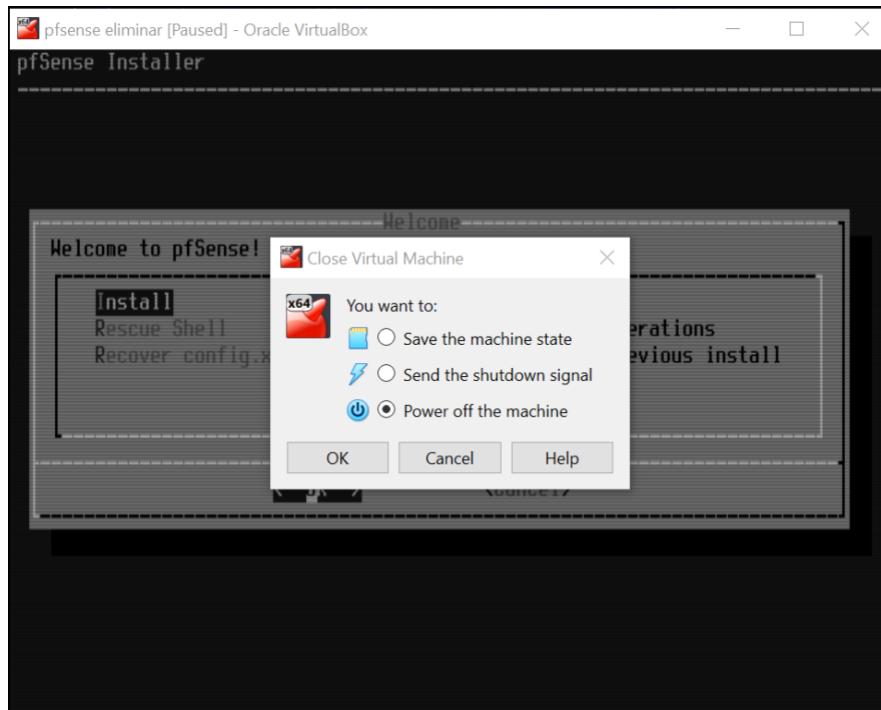
9. Comienza la instalación.



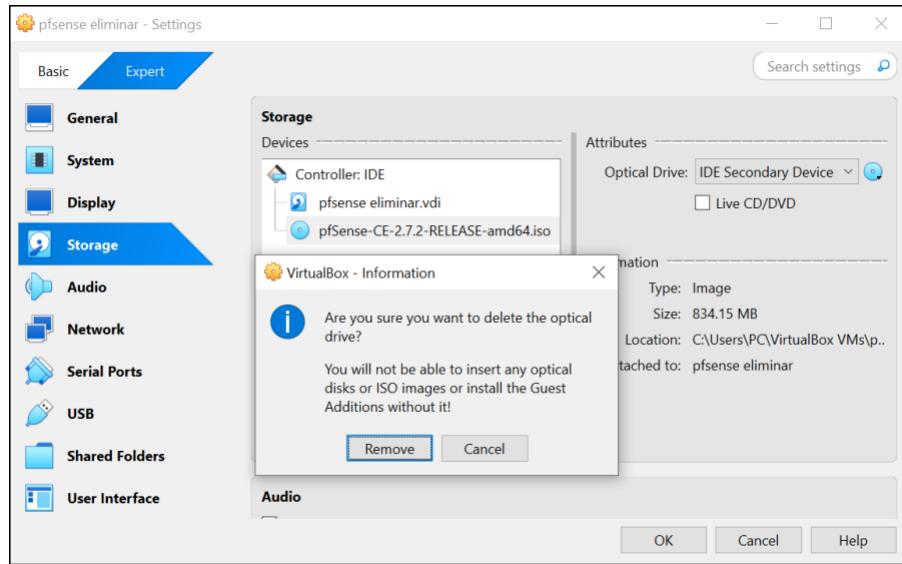
10. Reboot.



11. Apagamos la máquina.

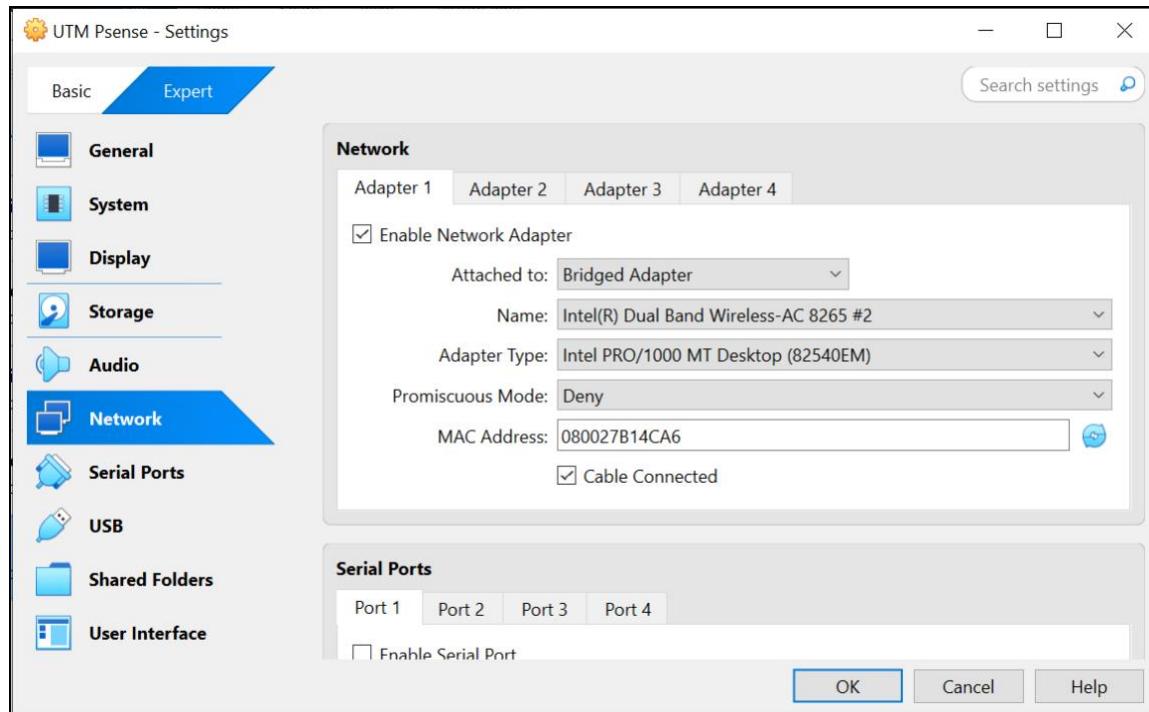


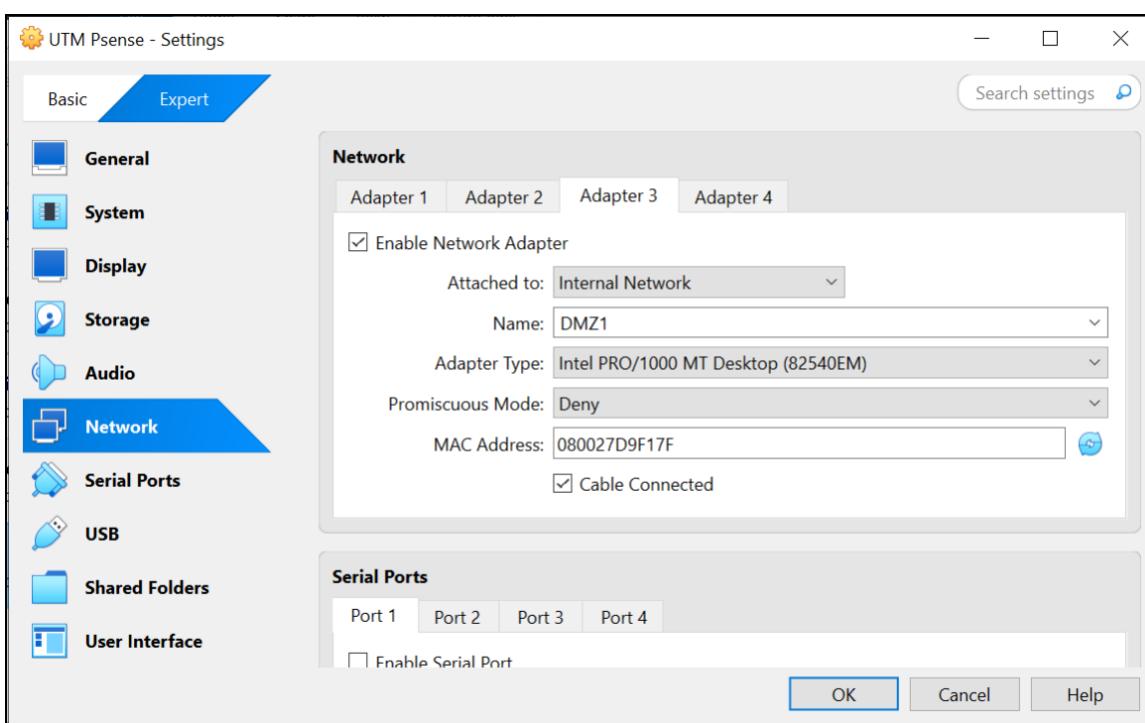
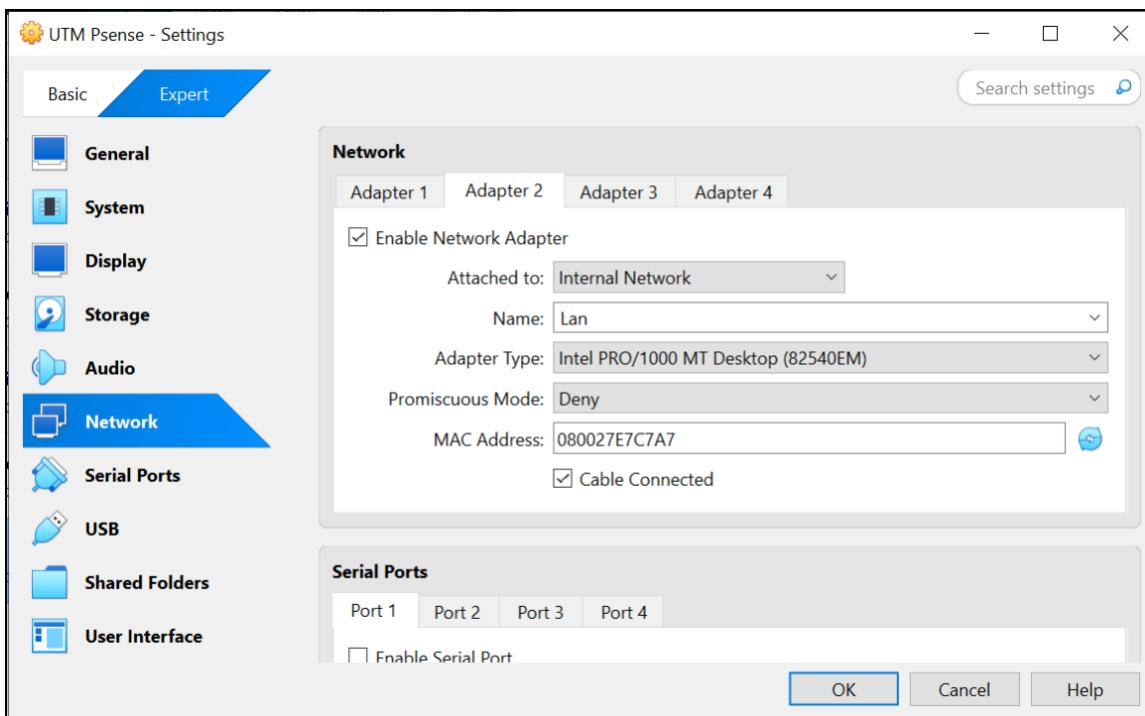
## 12. Eliminamos el disco de instalación.

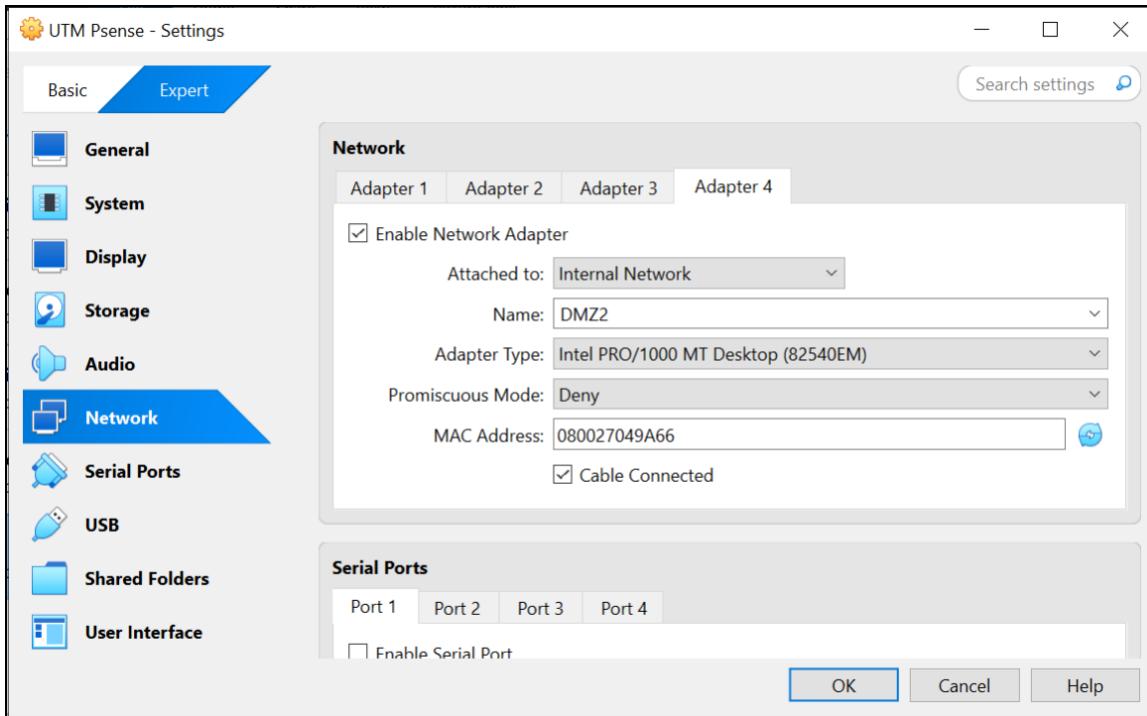


## Creación de las redes en VirtualBox

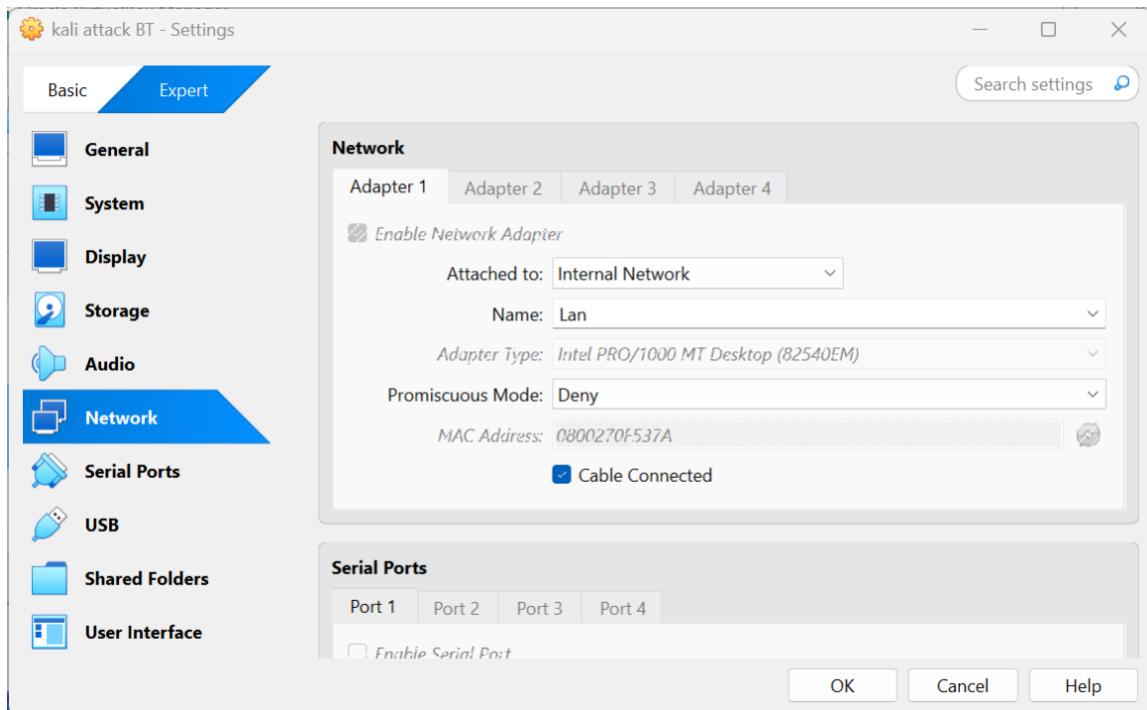
## 13. Añadimos las redes al UTM.







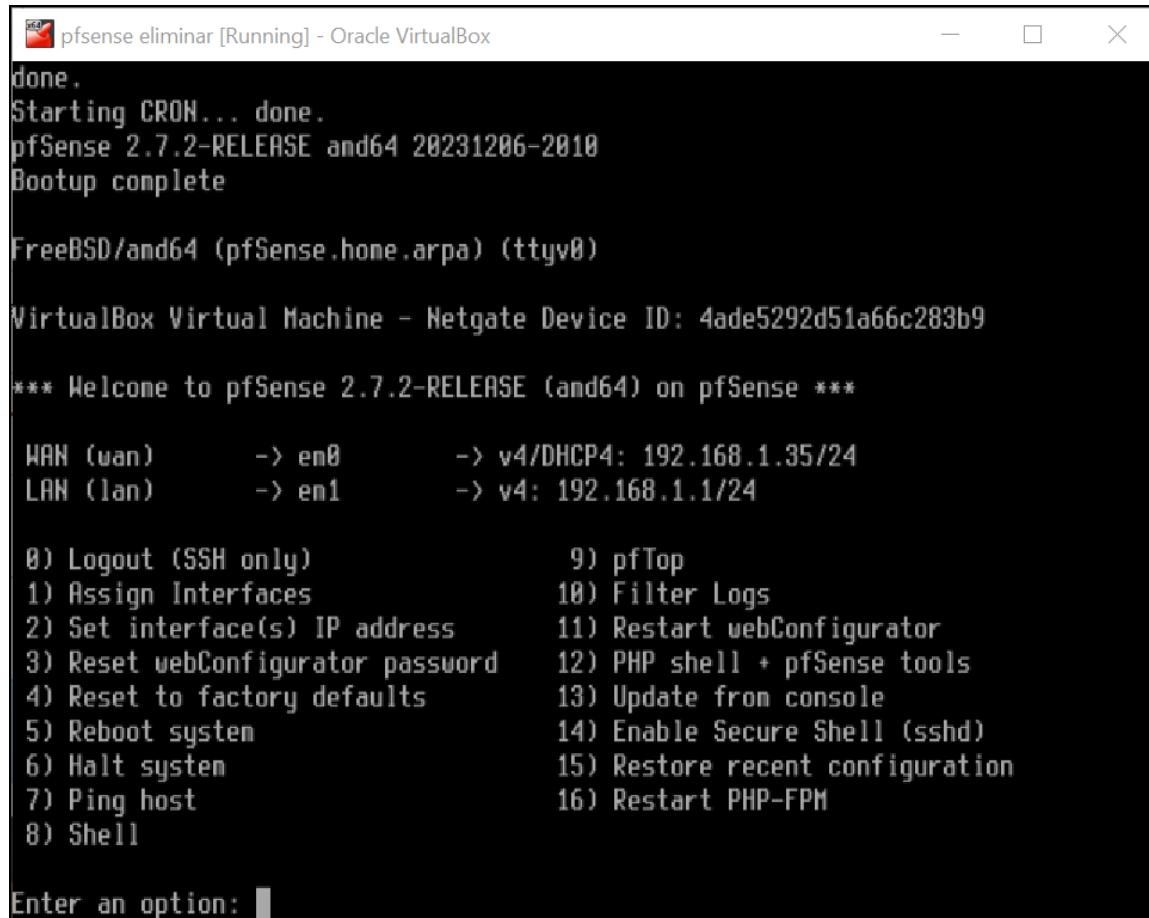
14. Añadimos la máquina Kali a la red interna.



## Configuración PfSense

### Pasos iniciales

15. Iniciamos PfSense.



The screenshot shows a terminal window titled "pfsense eliminar [Running] - Oracle VirtualBox". The window displays the following text:

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 4ade5292d51a66c283b9

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.35/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: █
```

16. Entramos en la máquina UTM.

En esta etapa de la práctica, se inició la máquina virtual con Kali Linux y se estableció conexión con PfSense a través del navegador. Durante este proceso, se llevó a cabo la configuración inicial del sistema.

- a. 192.168.1.1
- b. User: Admin
- c. Pass: pfsense

17. En el System>setup wizzard rellenamos la configuración:

- a. Hostname: UTM
- b. Domain: keepcoding.local
- c. Primary DNS server 127.0.0.1
- d. Secondary DNS server 1.1.1.1
- e. NEXT

On this screen the general pfSense parameters will be set.

<b>Hostname</b>	UTM
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
<b>Domain</b>	keepcoding.local
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
<b>Primary DNS Server</b>	127.0.0.1
<b>Secondary DNS Server</b>	1.1.1.1

<b>Primary DNS Server</b>	127.0.0.1
<b>Secondary DNS Server</b>	1.1.1.1
<b>Override DNS</b>	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	
<b>&gt;&gt; Next</b>	

18. Time server information.

- a. Time server hostname: 2.pfsense.pool.ntp.org
- b. Timezone: Europe/Madrid
- c. NEXT

**Time Server Information**

Please enter the time, date and time zone.

<b>Time server hostname</b>	2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.	
<b>Timezone</b>	Europe/Madrid
<b>&gt;&gt; Next</b>	

19. Dejamos todo en modo DHCP ya que va a ser el PfSense el que actúa como servidor DHCP y permitimos el uso de IPs privadas (RFC1918 y Bogons).

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

**General configuration**

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxx:xx:xxxx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If

RFC1918 Networks

**Block RFC1918 Private Networks**  Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

**Block bogon networks**

**Block bogon networks**  Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

**>> Next**

20. Cambiamos la IP de la LAN a 192.168.100.1

- a. LAN IP address: 192.168.100.1
- b. Subnet Mask: 24
- c. NEXT

Configure LAN Interface

On this screen the Local Area Network information will be configured.

**LAN IP Address**   
Type dhcp if this interface uses DHCP to obtain its IP address.

**Subnet Mask**

**>> Next**

21. Admin password: 123456  
Admin password again: 123456

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password .....  
Admin Password AGAIN .....

» Next

22. Resultado del PfSense tras pulsar enter

```
UTM Psense [Running] - Oracle VirtualBox
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.100.10
1 (Local Database)

FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 92b02f36e4b78d01bdbc

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.34/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

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

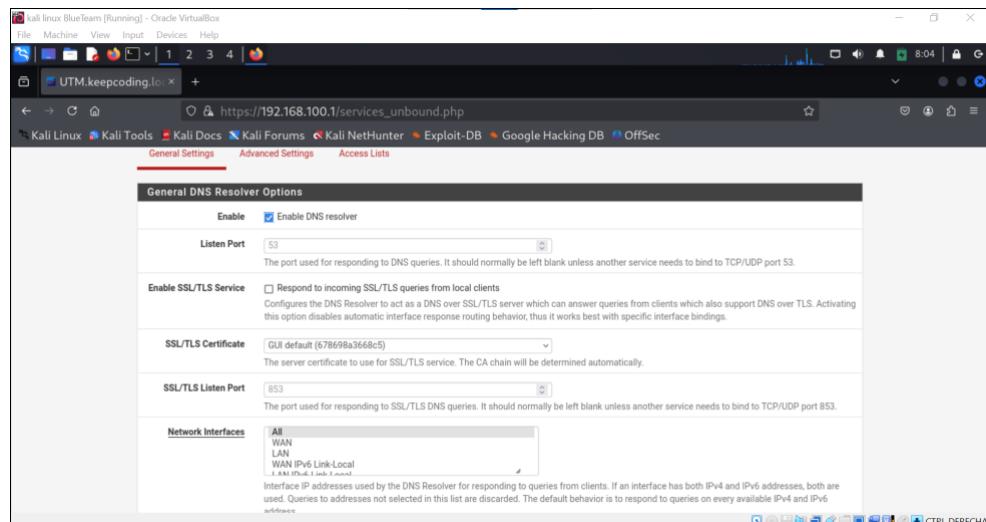
Enter an option: 
```

## Vamos a configurar la resolución DNS

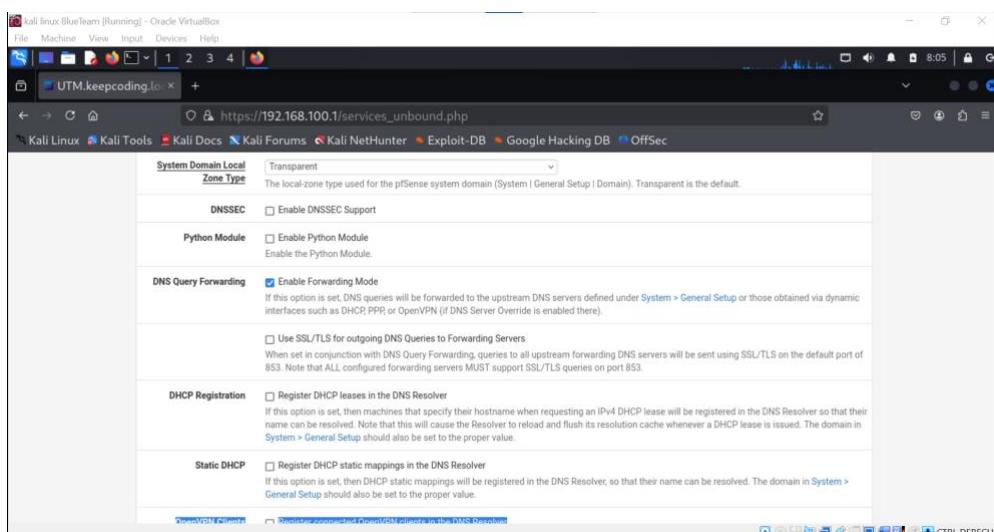
En este apartado, se procedió a asignar direcciones IP dinámicas a las redes LAN, DMZ y DMZ2, estableciendo rangos específicos de direcciones IP para cada una de ellas, con el objetivo de prevenir conflictos. Para ello, se habilitó el servicio DHCP en dichas redes, permitiendo la asignación automática de direcciones IP a los dispositivos conectados. Además, DHCP simplifica la administración de la red al proporcionar de manera centralizada otros parámetros esenciales, como la máscara de subred, la puerta de enlace predeterminada y los servidores DNS, asegurando así una configuración correcta y eficiente en todas las conexiones.

### 23. Services > DNS resolver.

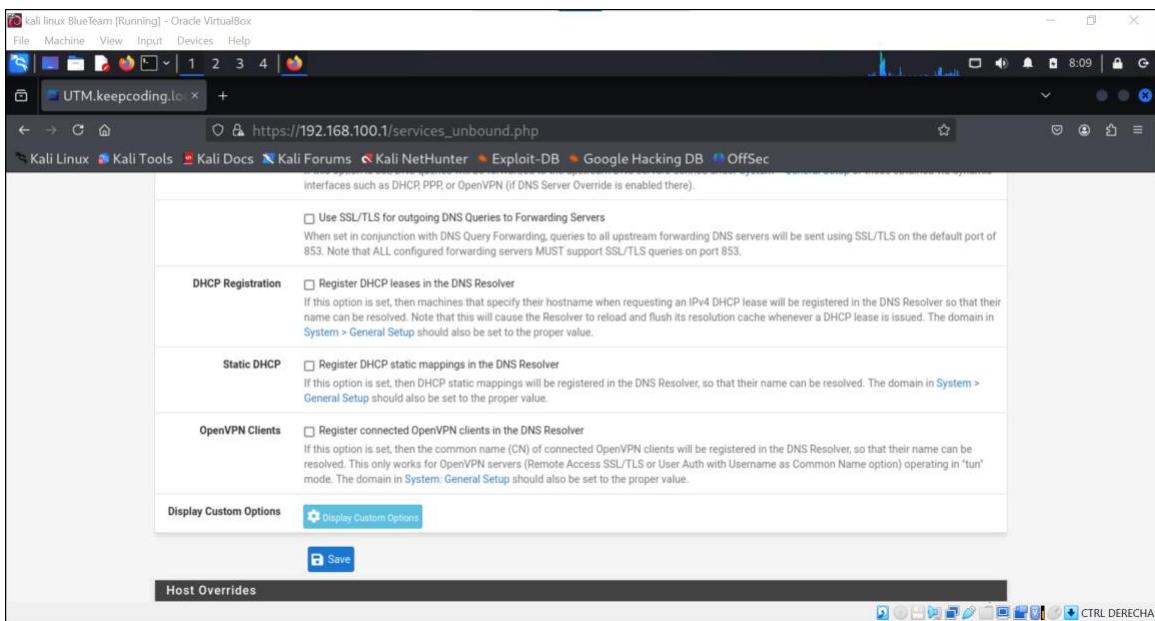
- Comprobamos si está habilitado
- Quitamos el DNSSEC
- Habilitamos el Forwarding mode



The screenshot shows the 'General DNS Resolver Options' configuration page. The 'Enable' checkbox is checked. The 'Listen Port' is set to 53. Other options include 'Respond to incoming SSL/TLS queries from local clients' (unchecked), 'SSL/TLS Certificate' (set to 'GUI default (678698a3668c5)'), and 'SSL/TLS Listen Port' (set to 853). The 'Network Interfaces' dropdown shows 'All' selected, with 'WAN', 'LAN', 'Virtual IPv6 Link-Local', and 'Kali IPv4 Link Local' listed. A note states that if an interface has both IPv4 and IPv6 addresses, both are used.

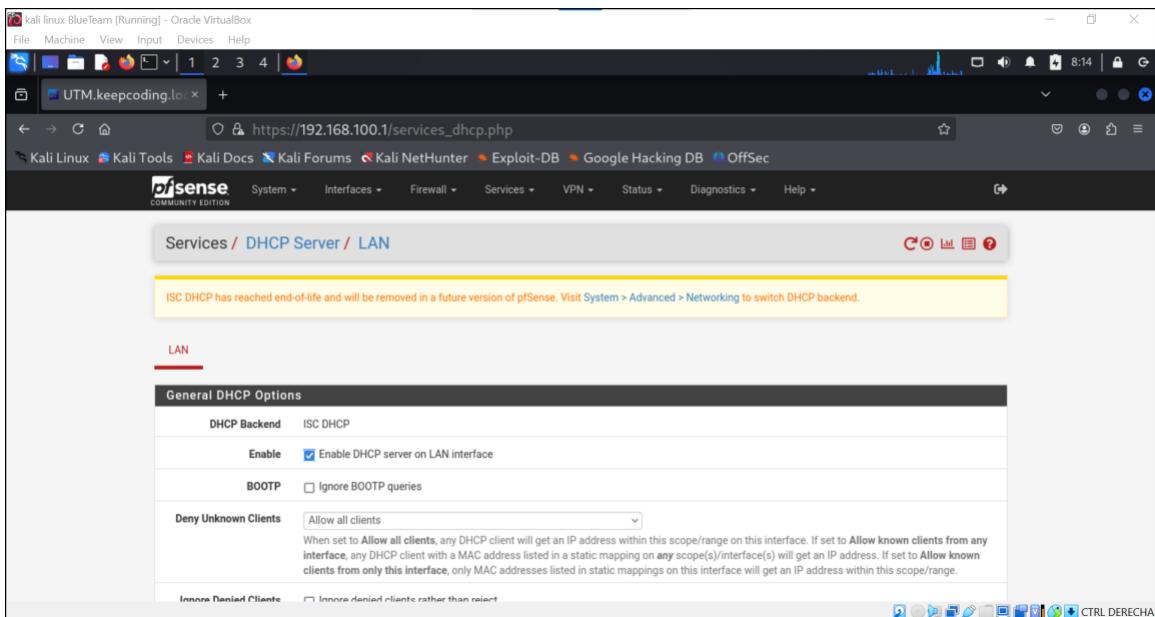


The screenshot shows the 'Advanced Settings' configuration page. The 'System Domain Local Zone Type' is set to 'Transparent'. Under 'DNSSEC', 'Enable DNSSEC Support' is unchecked. Under 'Python Module', 'Enable Python Module' is unchecked. Under 'DNS Query Forwarding', 'Enable Forwarding Mode' is checked. Under 'DHCP Registration', 'Register DHCP leases in the DNS Resolver' is unchecked. Under 'Static DHCP', 'Register DHCP static mappings in the DNS Resolver' is unchecked.



## 24. Configuración del DHCP server en la LAN.

- a. Modificamos el rango de direcciones de la LAN
  - i. 192.168.100.100 to 192.168.100.200



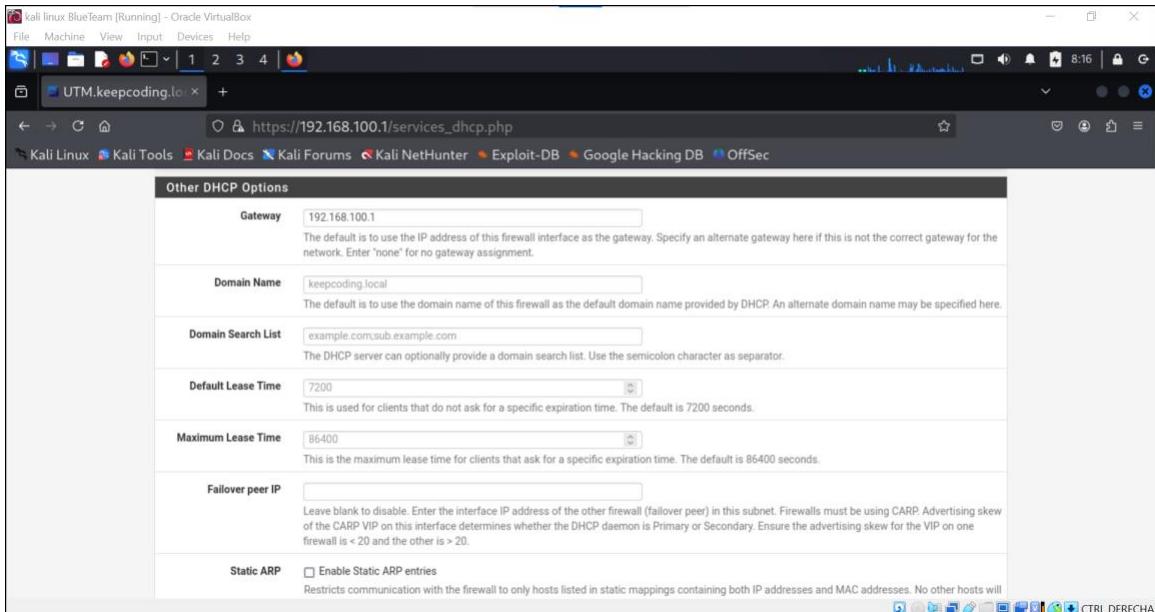
The screenshot shows a web-based configuration interface for a DHCP server. At the top, there are sections for 'Ignore Denied Clients' and 'Ignore Client Identifiers'. Below these is the 'Primary Address Pool' section, which includes fields for 'Subnet' (192.168.100.0/24), 'Subnet Range' (192.168.100.1 - 192.168.100.254), and 'Address Pool Range' (From 192.168.100.100 To 192.168.100.200). A note states that the specified range must not be within the range configured on any other address pool for this interface. There is also a 'Additional Pools' section with a '+ Add Address Pool' button. Under 'Server Options', there are fields for 'WINS Servers' (WINS Server 1 and WINS Server 2).

b. Modificamos los servidores DNS

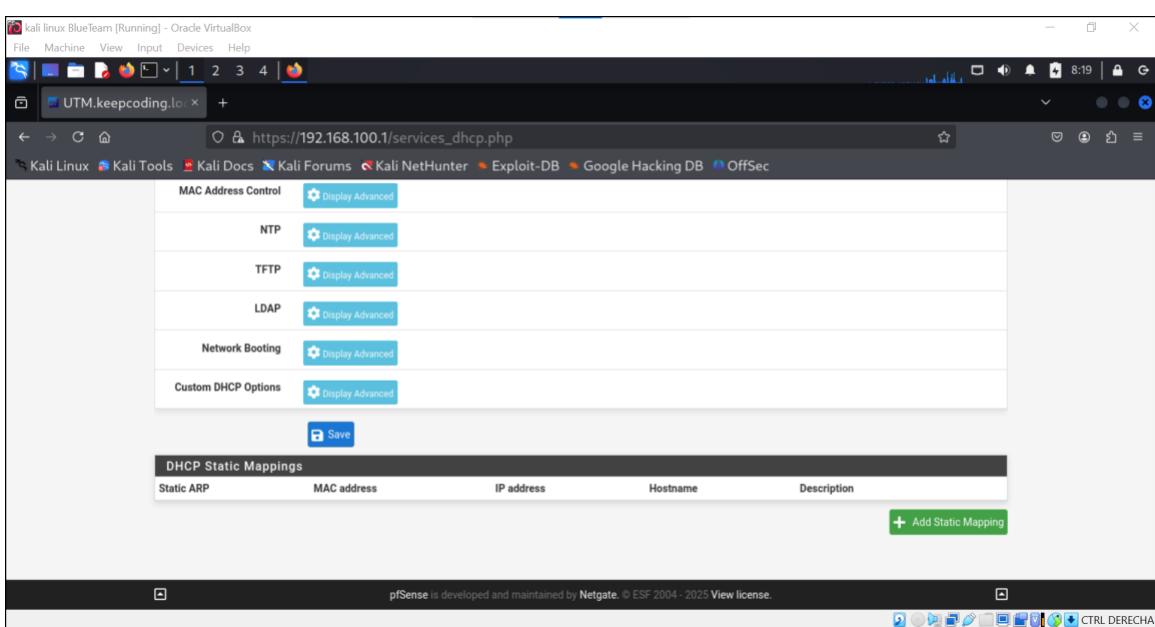
- i. 192.168.100.1
- ii. 1.1.1.1
- iii. 8.8.8.8

The screenshot shows the same configuration interface as the previous one, but with different settings. In the 'Additional Pools' section, there is a note about specifying additional pools of addresses. In the 'Server Options' section, the 'DNS Servers' field contains '192.168.100.1', '1.1.1.1', and '8.8.8.8'. Below this is a 'DNS Server 4' field. In the 'OMAPI' section, there is a 'OMAPI Port' field set to '7911' and an 'OMAPI Key' field containing a generated key.

### c. Modificamos la puerta de enlace/Gateway



The screenshot shows the 'Other DHCP Options' configuration page. The 'Gateway' field is set to '192.168.100.1'. The 'Domain Name' field is set to 'keepcoding.local'. The 'Domain Search List' field contains 'example.com;sub.example.com'. The 'Default Lease Time' is set to '7200'. The 'Maximum Lease Time' is set to '86400'. The 'Failover peer IP' field is empty. The 'Static ARP' checkbox is checked, with the note: 'Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will'. A 'Save' button is at the bottom.

The screenshot shows the 'DHCP Static Mappings' configuration page. It lists several options with 'Display Advanced' buttons: MAC Address Control, NTP, TFTP, LDAP, Network Booting, and Custom DHCP Options. Below this is a 'Save' button. At the bottom, there is a table with columns: Static ARP, MAC address, IP address, Hostname, and Description. A '+ Add Static Mapping' button is located at the bottom right of the table. The pfSense footer at the bottom states: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.'

## 25. Declaramos el resto de las tarjetas de red que nos faltan (DMZs).

pfSense  
COMMUNITY EDITION

Interfaces / Interface Assignments

Interface has been added.

Interface Assignments    Interface Groups    Wireless    VLANs    QinQs    PPPs    GReS    GIfs    Bridges    LAGGs

Interface	Network port
WAN	em0 (08:00:27:b1:4c:a6)
LAN	em1 (08:00:27:e7:c7:a7)
OPT1	em2 (08:00:27:d9:f1:7f)
OPT2	em3 (08:00:27:04:9a:66)

Save

## 26. Configuramos las interfaces -> Interfaces > OPT1

- Descripción -> DMZ
- IPv4 Configuration type -> Static IPv4
- IPv4 Address -> 192.168.200.1/24

pfSense  
COMMUNITY EDITION

Interfaces / OPT1 (em2)

General Configuration

Enable  Enable interface

Description DMZ  
Enter a description (name) for the interface here.

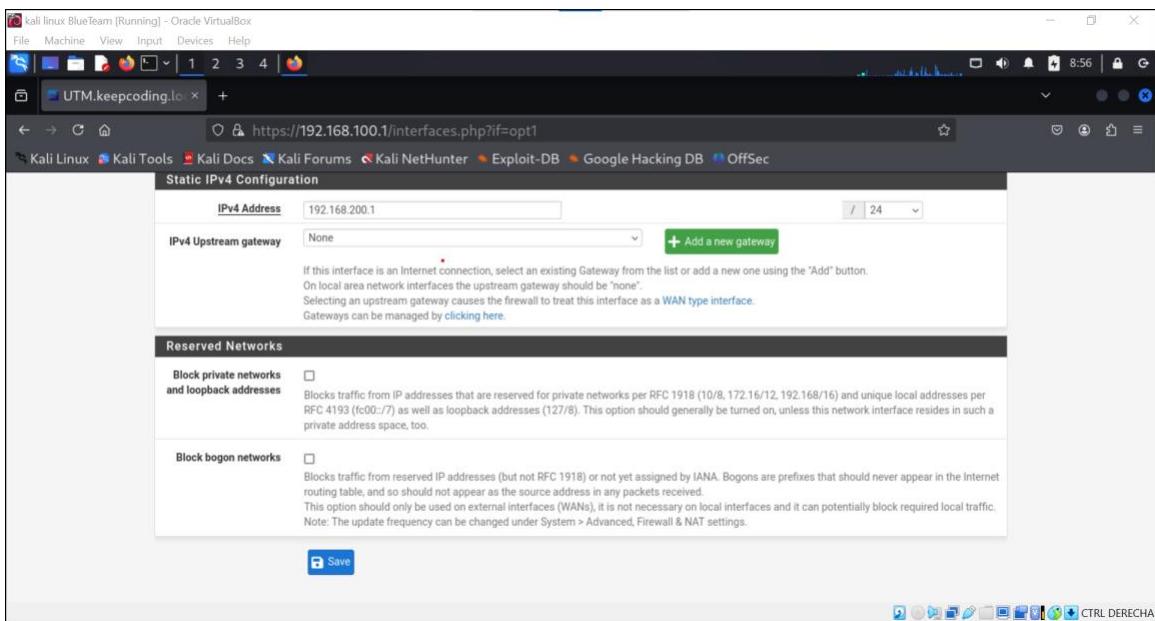
IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address 00:0C:00:00:00:00  
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxxxx or leave blank.

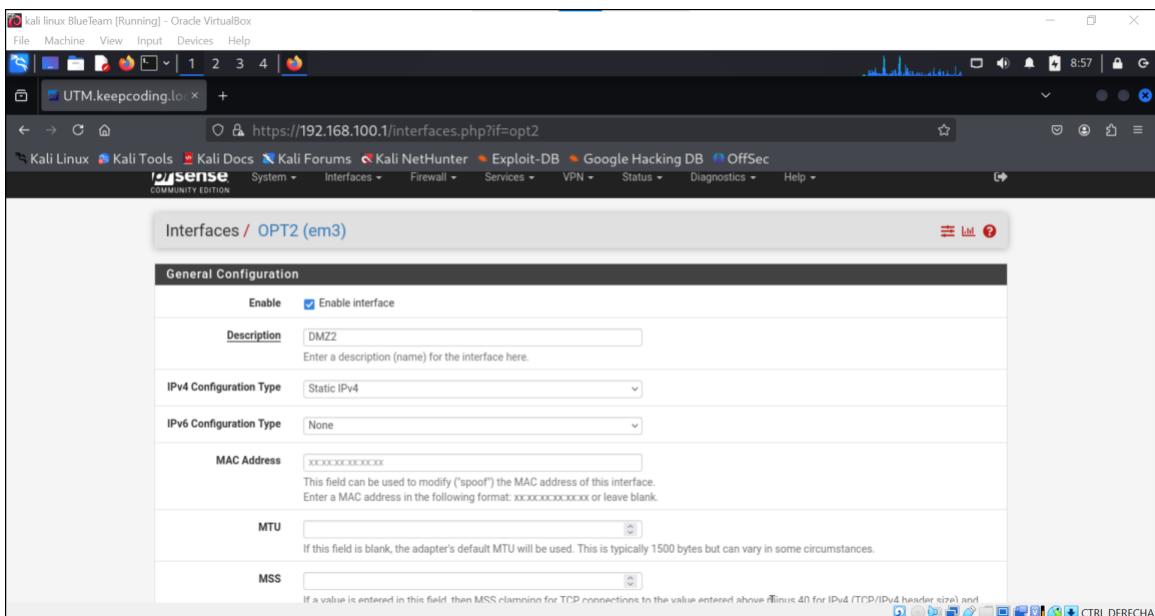
MTU

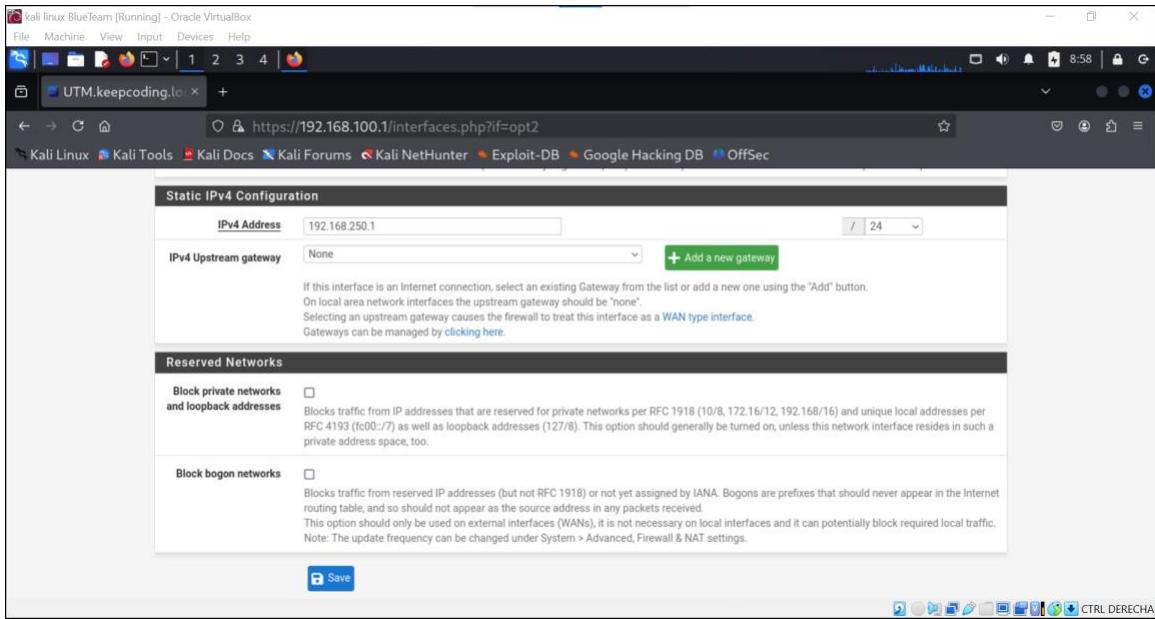
MSS



## 27. Interfaces > OPT2 (Igual que OPT1 pero cambiando la IP).

- a. Descripción -> DMZ2
- b. IPv4 Configuration type -> Static IPv4
- c. IPv4 Adress -> 192.168.250.1/24





28. Ahora vamos a comprobar que en el PfSense aparecen las 4 interfaces.

```
FreeBSD/amd64 (UTM.psense.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 92b02f36e4b78d01bdbc

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.34/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3      -> 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: 
```

## Configuración DHCP -> DMZ y DMZ2

29. Vamos a la configuración del DHCP y habilitamos el DHCP server en esas interfaces.
- Enable DHCP server on DMZ interface
  - Range 192.168.200.100 to 192.168.200.150
  - DNS servers:
    - 192.168.200.1
    - 1.1.1.1
    - 8.8.8.8
  - Gateway 192.168.200.1

The screenshot shows a web-based configuration interface for a DHCP server. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation, there are tabs for LAN, DMZ, and DMZ2, with DMZ selected. The main configuration area is titled "General DHCP Options". Under "DHCP Backend", "ISC DHCP" is selected. The "Enable" checkbox is checked. Under "BOOTP", the "Ignore BOOTP queries" checkbox is unchecked. In the "Deny Unknown Clients" section, "Allow all clients" is selected. A note explains that this allows any DHCP client to get an IP address from this scope. In the "Ignore Denied Clients" section, the "Ignore denied clients rather than reject" checkbox is unchecked. In the "Ignore Client Identifiers" section, the "Do not record a unique identifier (UID) in client lease data if present in the client DHCP request" checkbox is unchecked. At the bottom of the "General DHCP Options" section, the "Primary Address Pool" is defined with a "Subnet" of 192.168.200.0/24.

The screenshot shows the "Primary Address Pool" configuration page. The "Subnet" is set to 192.168.200.0/24. The "Address Pool Range" is defined from 192.168.200.100 to 192.168.200.254. The "Additional Pools" section has a button to "+ Add Address Pool". The "Server Options" section includes fields for "WINS Servers" (containing 192.168.200.1 and 1.1.1.1) and "DNS Servers" (containing 8.8.8.8).

### 30. Interfaz DMZ\_2.

- Enable DHCP server on DMZ\_2 interface
- Range 192.168.250.100 to 192.168.250.150
- DNS servers:
  - 192.168.250.1
  - 1.1.1.1
  - 8.8.8.8
- Gateway 192.168.250.1

Primary Address Pool

Subnet: 192.168.250.0/24

Subnet Range: 192.168.250.1 - 192.168.250.254

Address Pool Range: 192.168.250.100 - 192.168.250.200

From: 192.168.250.100  
To: 192.168.250.200

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 of the above range, they may be specified here.

Server Options

WINS Servers: WINS Server 1 (192.168.250.1), WINS Server 2 (192.168.250.1)

DNS Servers: 192.168.250.1 (1.1.1.1), 8.8.8.8

Key Algorithm: HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

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:

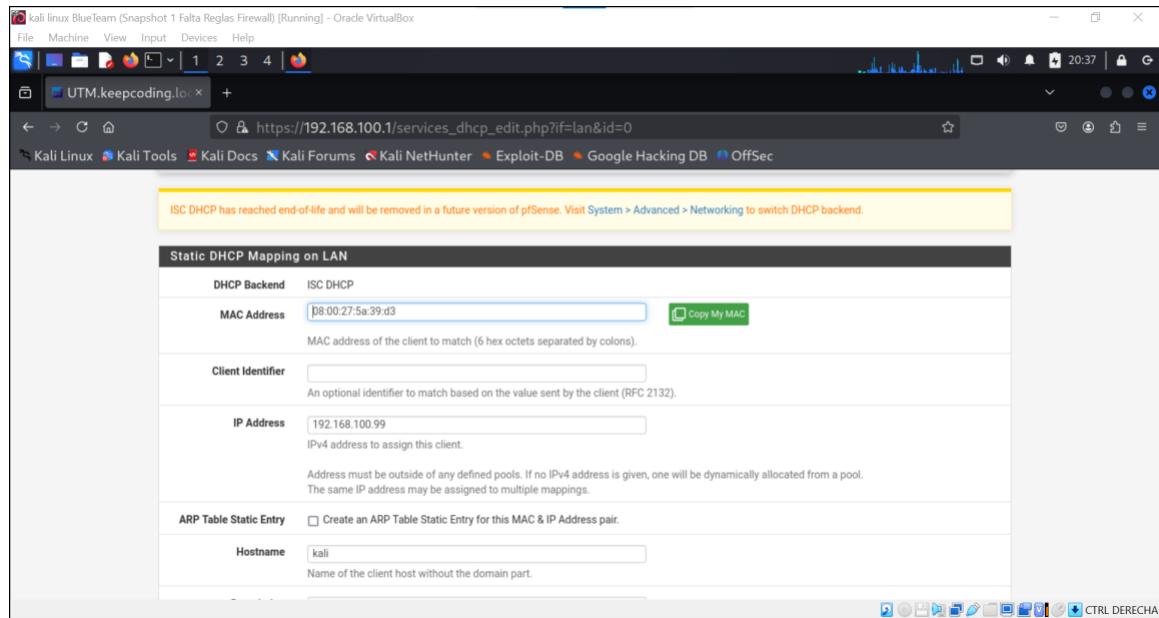
### 31. Comprobamos que funciona todo lo que hemos hecho.

- Cambiamos la Kali de red y nos asigna una IP del rango correcto por DHCP

## Establecer IP estática

En este punto es importante haber establecido una regla principal de puertos HTTP y HTTPS a DMZ y DMZ2, que si no se realiza no dejará acceder a PfSense desde la misma red.

### 32. LAN



```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.99/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 7198sec preferred_lft 7198sec
    inet6 fe80::4a21:3bcc:ff:ff/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

### 33. DMZ

Services / DHCP Server / DMZ / Static Mapping / Edit

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.

Static DHCP Mapping on DMZ

DHCP Backend: ISC DHCP

MAC Address: 08:00:27:5a:39:d3

Client Identifier:

An optional identifier to match based on the value sent by the client (RFC 2132).

IP Address: 192.168.200.99

Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.

ARP Table Static Entry  Create an ARP Table Static Entry for this MAC & IP Address pair.

Hostname: kali

CTRL DERECHA

link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
 valid\_lft forever preferred\_lft forever

(kali㉿kali)-[~]
\$ ip a
1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid\_lft forever preferred\_lft forever
 inet6 ::1/128 scope host noprefixroute
 valid\_lft forever preferred\_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000
 link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
 inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
 valid\_lft 7198sec preferred\_lft 7198sec
 inet6 fe80::4a21:3bcc:90b/64 scope link noprefixroute
 valid\_lft forever preferred\_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
 link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
 inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
 valid\_lft forever preferred\_lft forever

(kali㉿kali)-[~]
\$

## 34. DMZ2

The screenshot shows a web browser window titled "UTM.keepingcoding.io" with the URL [https://192.168.250.1/services\\_dhcp\\_edit.php?if=opt2&mac=08:00:27:5a:39:d3&hostname=kali](https://192.168.250.1/services_dhcp_edit.php?if=opt2&mac=08:00:27:5a:39:d3&hostname=kali). The page is titled "Services / DHCP Server / DMZ2 / Static Mapping / Edit". A yellow warning box at the top states: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The form fields include:

- DHCP Backend: ISC DHCP
- MAC Address: 08:00:27:5a:39:d3
- Client Identifier: (empty)
- IP Address: 192.168.250.99
- ARP Table Static Entry:  Create an ARP Table Static Entry for this MAC & IP Address pair.
- Hostname: kali

The screenshot shows a terminal window titled "kali@kali: ~" with the command `ip a` being run. The output shows the following network interfaces and their configurations:

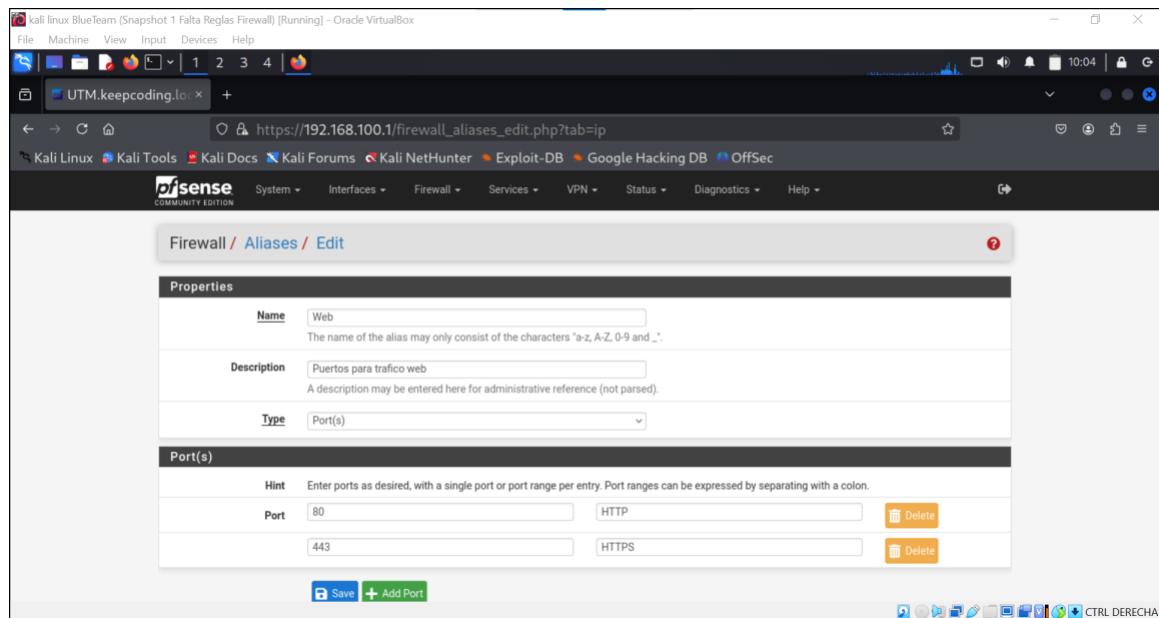
```
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.250.99/24 brd 192.168.250.255 scope global dynamic noprefixroute eth0
        valid_lft 7197sec preferred_lft 7197sec
        inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

## Establecemos alias

### 35. Asignamos alias a los puertos http (80) y https (443)

Vamos a otorgar el alias "Web" a los puertos 80 (HTTP) y 443 (HTTPS), ya que ambos están comúnmente asociados a la transmisión de datos a través de páginas web. El puerto 80 (HTTP) se utiliza para establecer conexiones no cifradas, lo que significa que los datos transmitidos entre el cliente y el servidor pueden ser interceptados y leídos fácilmente por terceros. Por otro lado, el puerto 443 (HTTPS) opera con un nivel de seguridad superior, ya que emplea protocolos de cifrado como TLS (Transport Layer Security), lo que garantiza la confidencialidad e integridad de los datos transmitidos.



## Creamos las reglas de los FW (firewall)

En esta sección se detallan las reglas principales implementadas en el firewall, junto con la validación del correcto funcionamiento del servicio DNS y la definición de políticas específicas para la gestión de las comunicaciones entre las diferentes redes configuradas.

Se establece que la red DMZ estará completamente aislada de las redes internas LAN y DMZ2, sin posibilidad de comunicación en ningún sentido. No obstante, se permitirá acceso bidireccional entre la red DMZ y la red externa WAN, cumpliendo con los requisitos de segmentación y control. Asimismo, se asigna esta red al Honeypot, como parte de la estrategia de detección y análisis de posibles amenazas externas.

Esta configuración refuerza los principios de seguridad perimetral y minimiza los riesgos asociados a accesos no autorizados desde redes externas hacia la infraestructura interna.

### 36. WAN CASO HONEYBOT SSH.

The screenshot shows the pfSense Firewall Rules configuration for the WAN interface. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The pfSense logo is at the top left, followed by a navigation menu with System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A right-click context menu icon is also present.

The main title is "Firewall / Rules / WAN". Below it, tabs for Floating, WAN, LAN, DMZ, and DMZ2 are shown, with WAN being the active tab. The sub-header "Rules (Drag to Change Order)" is displayed above a table.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.200.99	222	*	none	NAT	

Below the table are several action buttons: Add (up arrow), Add (down arrow), Delete (trash can), Toggle (circular switch), Copy (document icon), Save (disk icon), and Separator (plus minus icon). A blue information icon is located on the left side of the table area.

The bottom navigation bar includes icons for Home, Firewall, Services, VPN, Status, Diagnostics, Help, and a right-click context menu. The text "CTRL+DEECHA" is visible at the bottom right.

## 37. NAT CASO HONEYPOT SSH.

### 38. WAN CASO HONEYBOT RDP.

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	192.168.200.99	333	*	none	NAT		

### 39. NAT CASO HONEYBOT RDP.

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

Port Forward 1:1 Outbound NPt

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	333	192.168.200.99	333		

### 40. LAN.

kali attack Clone [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

pfSense.keepcoding.loc +

https://192.168.100.1/firewall\_rules.php?if=lan 67% 16:42

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/255 KIB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0/0 B	IPv4 TCP	LAN subnets	*	DMZ2 subnets	22 (SSH)	*	none		Regla de administración Suricata DMZ2	
0/0 B	IPv4 TCP	LAN subnets	*	DMZ subnets	22 (SSH)	*	none		Regla de administración HoneyPost DMZ	
0/0 B	IPv4 ICMP	LAN subnets	*	DMZ2 subnets	*	*	none		Regla de comprobación de disponibilidad en DMZ	
0/0 B	IPv4 ICMP	LAN subnets	*	DMZ2 subnets	*	*	none		Regla de comprobación de disponibilidad en DMZ_2	
0/0 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Bloqueo red de LAN a DMZ	
0/0 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Bloqueo red de LAN a DMZ_2	
0/0 B	IPv4 UDP	LAN subnets	*	*	53 (DNS)	*	none		Consultas rápidas pero menos seguras DNS por UDP	
0/0 B	IPv4 TCP	LAN subnets	*	Puertos	*	none			Salida tráfico web	

Nota:

Se han creado reglas para la administración de las máquinas por SSH desde la red LAN.

## 41. DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloque red de DMZ a DMZ_2	
0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloque red de DMZ a LAN	
0/0 B	IPv4 *	*	*	192.168.200.99	*	*	none			
0/0 B	IPv4 UDP	192.168.200.99	*	*	53 (DNS)	*	none		DNS	
0/0 B	IPv4 TCP	192.168.200.99	*	Puertos	*	none				

Add Add Delete Toggle Copy Save Separator

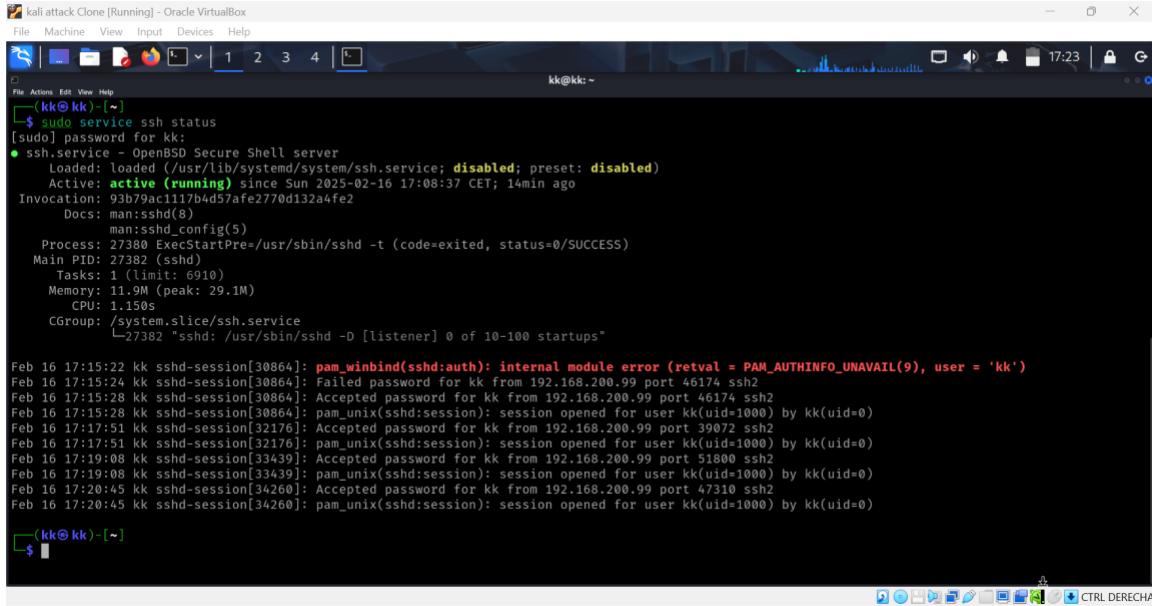
## 42. DMZ2

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloquear red de DMZ_2 a DMZ	
0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloquear red de DMZ_2 a LAN	
0/0 B	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none		DNS	
0/0 B	IPv4 TCP	DMZ2 subnets	*	Puertos	*	none				

Add Add Delete Toggle Copy Save Separator

43. Si quisieramos conectarnos por SSH para administrar la máquina. Habilitamos el servicio de SSH en la máquina deseada.

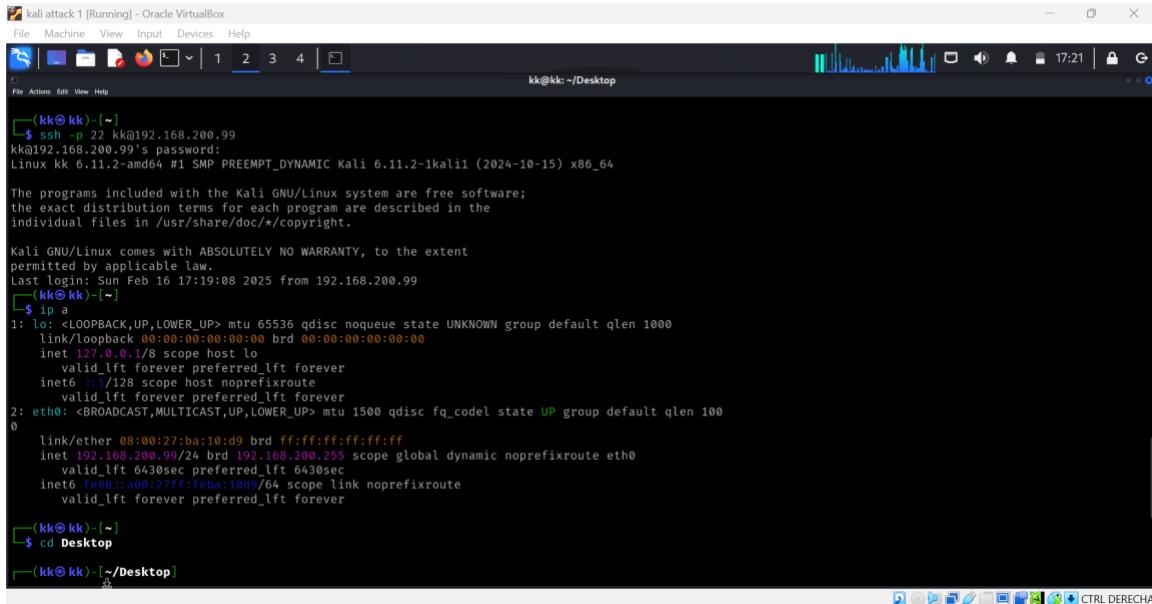


```
(kk@kk) [~]
$ sudo service ssh status
[sudo] password for kk:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Sun 2025-02-16 17:08:37 CET; 14min ago
    Invocation: 93b79ac1117b4d45afe2770d132a0fe2
      Docs: man:sshd(8)
             man:sshd_config(5)
  Process: 27380 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 27382 (sshd)
   Tasks: 1 (limit: 6910)
  Memory: 11.9M (peak: 29.1M)
    CPU: 1.150s
   CGroup: /system.slice/ssh.service
           └─27382 "/usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 16 17:15:22 kk sshd[30864]: pam_winbind(sshd:auth): internal module error (retval = PAM_AUTHINFO_UNAVAIL(9), user = 'kk')
Feb 16 17:15:24 kk sshd[30864]: Failed password for kk from 192.168.200.99 port 46174 ssh2
Feb 16 17:15:28 kk sshd[30864]: Accepted password for kk from 192.168.200.99 port 46174 ssh2
Feb 16 17:15:28 kk sshd[30864]: pam_unix(sshd:session): session opened for user kk(uid=1000) by kk(uid=0)
Feb 16 17:17:51 kk sshd[32176]: Accepted password for kk from 192.168.200.99 port 39072 ssh2
Feb 16 17:17:51 kk sshd[32176]: pam_unix(sshd:session): session opened for user kk(uid=1000) by kk(uid=0)
Feb 16 17:19:01 kk sshd[33439]: Accepted password for kk from 192.168.200.99 port 51800 ssh2
Feb 16 17:19:08 kk sshd[33439]: pam_unix(sshd:session): session opened for user kk(uid=1000) by kk(uid=0)
Feb 16 17:20:45 kk sshd[34260]: Accepted password for kk from 192.168.200.99 port 47310 ssh2
Feb 16 17:20:45 kk sshd[34260]: pam_unix(sshd:session): session opened for user kk(uid=1000) by kk(uid=0)

(kk@kk) [~]
$
```

44. Realizamos la conexión desde la red LAN.



```
(kk@kk) [~]
$ ssh -p 22 kk@192.168.200.99
kk@192.168.200.99's password:
Linux kk 6.11.2-1kalii (2024-10-15) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb 16 17:19:08 2025 from 192.168.200.99
(kk@kk) [~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:ba:10:d9 brd ff:ff:ff:ff:ff:ff
  inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
    valid_lft 6430sec preferred_lft 6430sec
  inet6 fe80::a00:27ff:feb8:10d9/64 scope link noprefixroute
    valid_lft forever preferred_lft forever

(kk@kk) [~]
$ cd Desktop
(kk@kk) [~/Desktop]
```

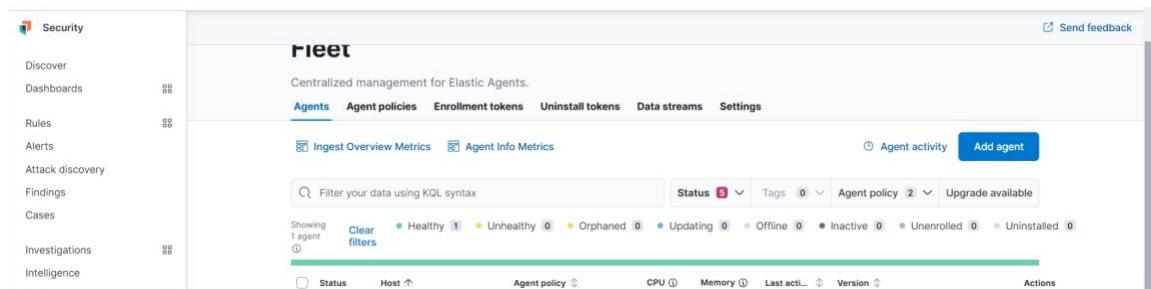
## ElasticCloud

### Creación de cuenta de ElasticCloud

45. Creamos la cuenta de ElasticCloud utilizando la versión de 15 días de prueba proporcionada en la página de Elastic (<https://cloud.elastic.co/registration>)

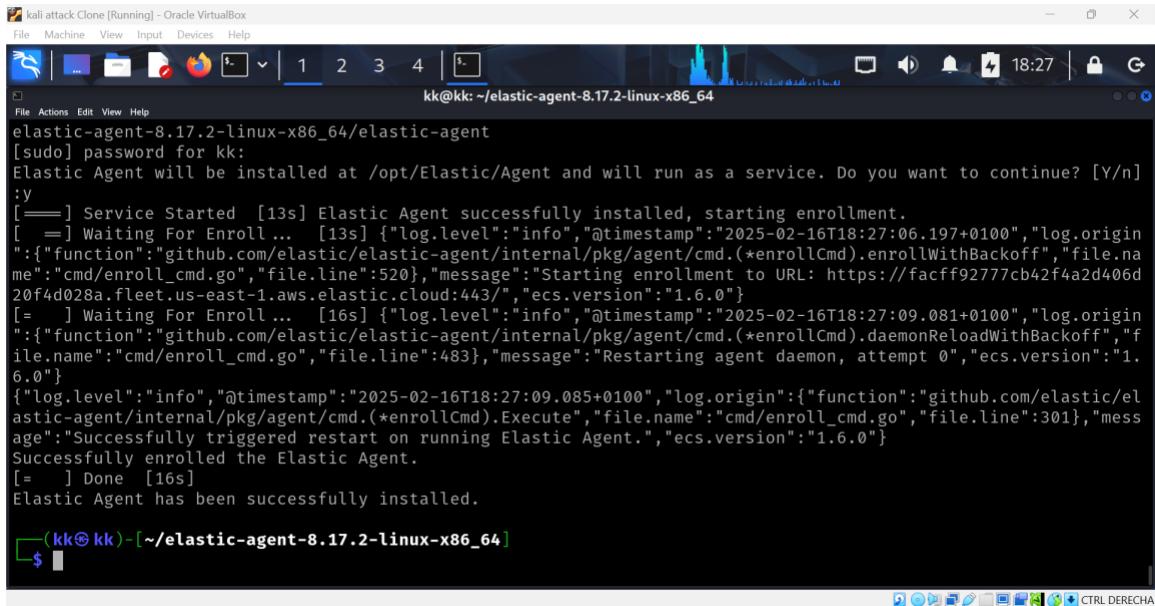
### Configuración ElasticCloud

46. Instalación de los agentes en las máquinas Linux y Windows.
47. En la sección de Fleet añadimos el agente a la política deseada. En ese momento se nos proporcionará un comando para instalarlo tanto en la máquina Linux como en la máquina Windows.
48. Fleet



The screenshot shows the Elastic Cloud interface with the 'Fleet' section selected. The left sidebar includes links for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, and Intelligence. The main 'Fleet' page has a header 'Centralized management for Elastic Agents.' and tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. Below the tabs are two metrics: 'Ingest Overview Metrics' and 'Agent Info Metrics'. A search bar allows filtering data using KQL syntax. A status summary shows 1 agent, all healthy. There are filters for Status (Status, Tags, Agent policy), Upgrade available, and a legend for agent health (Healthy, Unhealthy, Orphaned, Updating, Offline, Inactive, Unenrolled, Uninstalled). At the bottom, there are sorting options for Status, Host, Agent policy, CPU, Memory, Last active, and Version, along with an 'Actions' button.

## 49. Kali

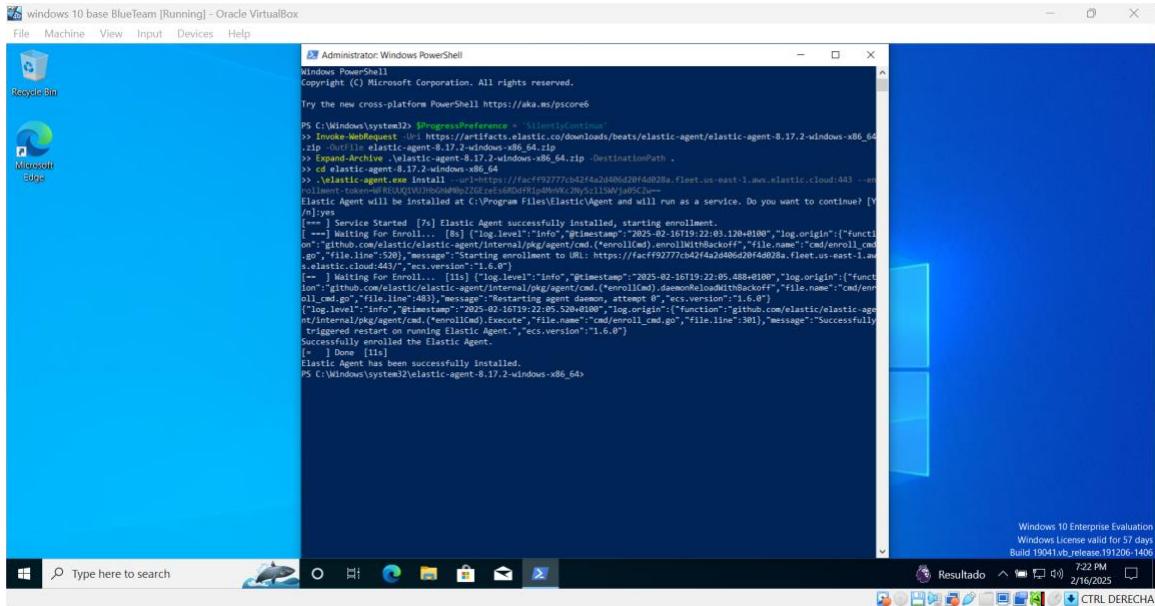


```
kali attack Clone [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4 | [ ]
kk@kk: ~/elastic-agent-8.17.2-linux-x86_64

elastic-agent-8.17.2-linux-x86_64/elastic-agent
[sudo] password for kk:
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]
;y
[==>] Service Started [1s] Elastic Agent successfully installed, starting enrollment.
[==>] Waiting For Enroll ... [1s] {"log.level": "info", "@timestamp": "2025-02-16T18:27:06.197+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://facfff92777cb42f4a2d406d20f4d028a.fleet.us-east-1.aws.elastic.cloud:443/", "ecs.version": "1.6.0"}
[==>] Waiting For Enroll ... [16s] {"log.level": "info", "@timestamp": "2025-02-16T18:27:09.081+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": "2025-02-16T18:27:09.085+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 [16s]
Elastic Agent has been successfully installed.

(kk㉿kk) [~/elastic-agent-8.17.2-linux-x86_64]
```

## 50. Windows



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
>> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.2-windows-x86_64.zip -OutFile C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64.zip
>> Expand-Archive -Path C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64.zip -DestinationPath .
>> cd elastic-agent-8.17.2-windows-x86_64
>> .\elastic-agent.exe install --url=https://facfff92777cb42f4a2d406d20f4d028a.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=d810EQUyVQDfHgqAMpJZGZxex5d0MFP1dM0WVX2Hg5zL1MVjwP9Cw
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 [7s] Elastic Agent successfully installed, starting enrollment.
[==>] Waiting For Enroll ... [8s] {"log.level": "info", "@timestamp": "2025-02-16T19:22:01.129+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "520"}, "message": "Starting enrollment to URL: https://facfff92777cb42f4a2d406d20f4d028a.fleet.us-east-1.aws.elastic.cloud:443/", "ecs.version": "1.6.0"}
[==>] Waiting For Enroll ... [1s] {"log.level": "info", "@timestamp": "2025-02-16T19:22:05.488+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent.(*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": "2025-02-16T19:22:05.520+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 [1s]
Elastic Agent has been successfully installed.

PS C:\Windows\system32> elastic-agent-8.17.2-windows-x86_64
```

## Integración de los logs en Windows

51. Vamos a integrar los logs relacionados con la monitorización de seguridad. Esto nos proporciona la integración “*Elastic Defend*”.

The screenshot shows the 'Elastic Defend' integration page within the 'Integrations' section of the Elastic Cloud interface. The main header displays 'keep-coding-facff9.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/endpoint-9.0.0/assets'. The left sidebar includes links for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, Explore, Get started, Developer tools, Project Settings (with 'Integrations' selected), Stack Management, and Billing and subscription. The central panel features the 'Elastic Defend' logo and navigation tabs for Overview, Integration policies, Assets (selected), Settings, and Advanced. Below these tabs is a 'Views' section with a 'Hosts' card and links to Index templates, Component templates, Ingest pipelines, and Transforms.

52. Evidencias de los logs generados.

The screenshot shows the 'Discover' interface in Elasticsearch, displaying search results for the query '.alerts-security.alerts-default,apm-\*... windows marca'. The interface includes a search bar, time range selector (Last 15 minutes), and refresh button. The left sidebar lists various monitoring and security categories. The main area shows a histogram of event counts over time, followed by a table of 'Documents (2,166)' and a preview of log entries. One entry is highlighted with a red box, showing a complex JSON log entry related to a Windows 10 Enterprise Evaluation 22H2 event involving svchost.exe and InstallService. A 'Copy value' button is visible next to the highlighted entry.

## Integración de los logs del Honeypot en Elastic

53. Ejecutamos el contenedor Docker con el honeypot y mandamos los logs generados a un archivo:

a. docker run -p 222:2222 cowrie/cowrie > cowrie\_practica.log

Incluimos los logs en Elastic con la ayuda de la integración “*Custom Logs*”.

The screenshot shows the 'Add Custom Logs integration' configuration page. It consists of two main sections: 'Configure integration' (Step 1) and 'Where to add this integration?' (Step 2).

**Step 1: Configure integration**

**Integration settings**

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

**Integration name:** log-honeypot

**Description:** logs del honeypot (Optional)

**Custom log file** (checkbox checked)

**Log file path:** /home/kk/cowrie\_practica.log

**Dataset name:** cowrie

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

**Advanced options**

**Step 2: Where to add this integration?**

**New hosts**   **Existing hosts** (selected)

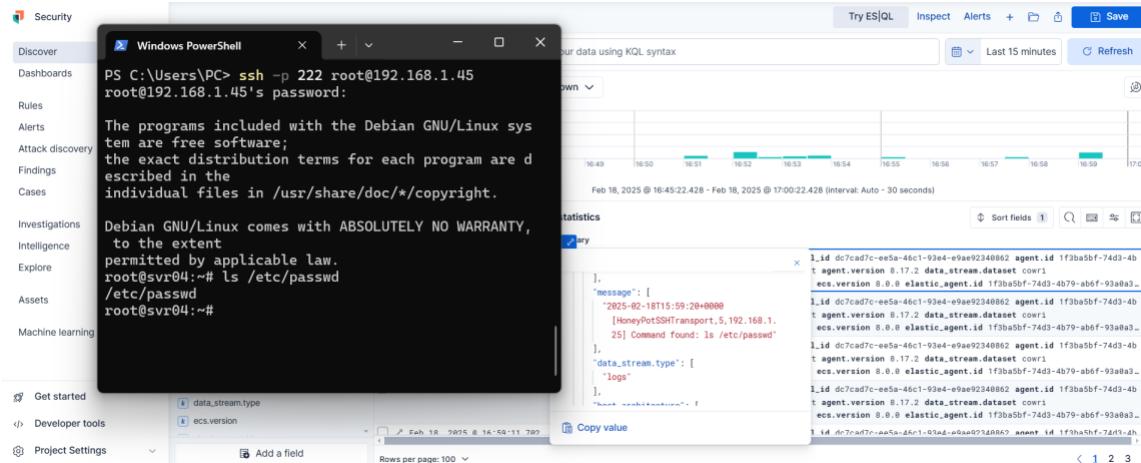
**Agent policies**

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

**Agent policies:** Linux

1 agent is enrolled with the selected agent policies.

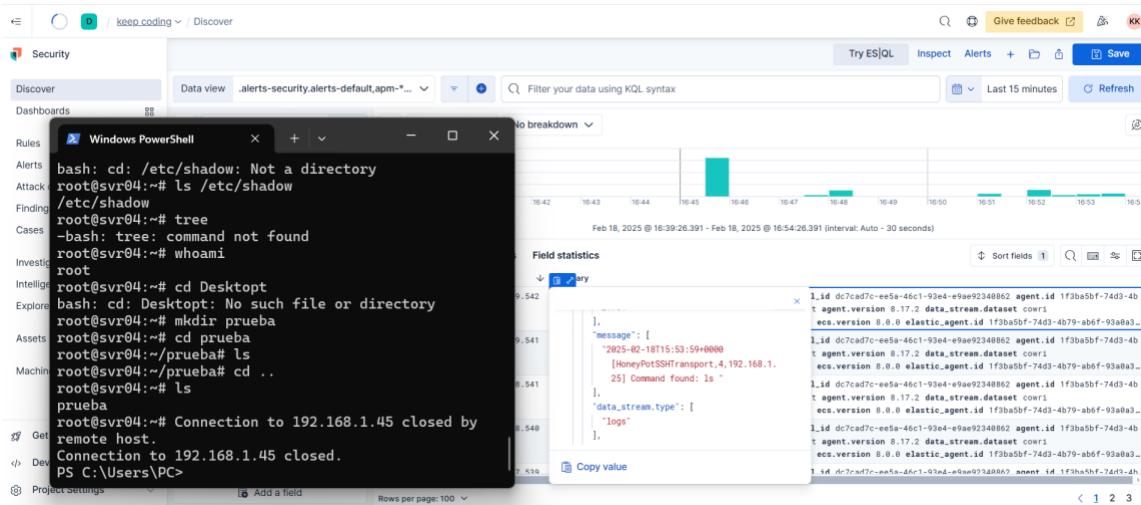
## 54. Revisamos que los logs no están llegando.



```
PS C:\Users\PC> ssh -p 222 root@192.168.1.45
root@192.168.1.45'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:~# ls /etc/passwd
/etc/passwd
root@svr04:~#
```

The screenshot shows a Windows PowerShell window within the Elastic Stack interface. The command entered was `ssh -p 222 root@192.168.1.45`. The password was provided, and the session was established. The user then listed the contents of the `/etc/passwd` file. The interface also displays a timeline of events and a detailed view of the log entries.



```
bash: cd: /etc/shadow: Not a directory
root@svr04:~# ls /etc/shadow
/etc/shadow
root@svr04:~# tree
-bash: tree: command not found
root@svr04:~# whoami
root
root@svr04:~# cd Desktoppt
bash: cd: Desktoppt: No such file or directory
root@svr04:~# mkdir prueba
root@svr04:~# cd prueba
root@svr04:~/prueba# ls
root@svr04:~/prueba# cd ..
root@svr04:~# ls
prueba
root@svr04:~# Connection to 192.168.1.45 closed by
remote host.
Connection to 192.168.1.45 closed.
PS C:\Users\PC>
```

This screenshot shows a Linux terminal session within the Elastic Stack interface. The user is root and attempts to change directory to `/etc/shadow`, which fails because it is a file. They then try to list its contents and use the `tree` command, which is not found. They check their user information, change directory to a non-existent `Desktoppt`, and then create a new directory named `prueba`. Finally, they attempt to change back to the root directory and close the connection. The interface shows a timeline and the log entries for these actions.

## Integración de los logs de Apache y Suricata

### Suricata

Suricata es una herramienta avanzada de detección y prevención de intrusiones que permite monitorear redes para identificar actividades sospechosas. Vamos a documentar su instalación, configuración y personalización mediante reglas diseñadas para detectar eventos específicos, como tráfico de red, intentos de conexión SSH y descargas de archivos PDF. La instalación se realiza actualizando los paquetes del sistema e instalando Suricata, seguida de una ejecución inicial para verificar su funcionamiento.

Además, se describieron procedimientos para analizar y guardar los logs generados, esenciales para el análisis posterior y la respuesta a incidentes. Los logs se almacenan en el directorio /var/log/suricata, y se pueden respaldar mediante compresión y transferencia a un servidor remoto para asegurar su disponibilidad. En conjunto, estas configuraciones convierten a Suricata en una herramienta poderosa para fortalecer la seguridad de la red, proporcionando visibilidad y capacidad de respuesta frente a posibles amenazas. Los logs posteriormente se guardarán en la plataforma web Elastic.

## 55. Integración utilizada.

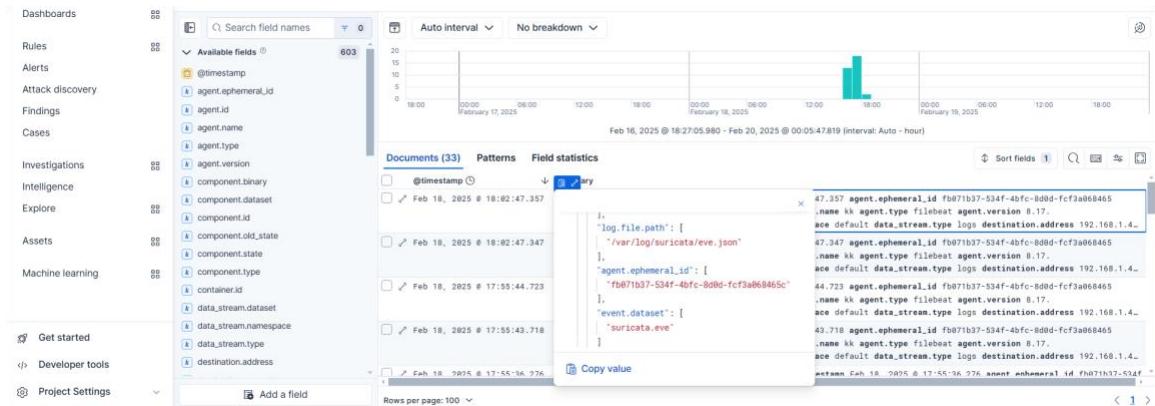
The screenshot shows the 'Suricata' integration page within the Elastic Stack interface. The left sidebar includes 'Discover', 'Dashboards', 'Rules', 'Alerts', 'Attack discovery', 'Findings', 'Cases', 'Investigations', 'Intelligence', 'Explore', 'Assets', 'Get started', 'Developer tools', 'Project Settings', 'Stack Management', 'Integrations' (which is selected), and 'Billing and subscription'. The main content area has a title 'Suricata' with a logo, a 'Compatibility' section stating 'Elastic Agent', and a 'Screenshots' section showing two dashboards. Below these are sections for 'Suricata Integration' (described as reading EVE JSON output) and 'Compatibility' (noted as v4.0.4). A code snippet for an 'eve' event is shown:

```
{
  "@timestamp": "2018-07-05T19:01:09.828Z",
  "agent": {
    "ephemeral_id": "58ad0be4-5de9-e482-89a4-8d93557f8f2e",
    "id": "0a5c1566-c6fd-4e91-b9bd-4883445a980e",
    "name": "docker-fleet-agent",
    "tvoe": "filebeat"
  }
}
```

On the right, there are 'Connection details' and 'Add Suricata' buttons.

## 56. Evidencias de los logs recogidos.

The screenshot shows the Elasticsearch interface with a search bar containing 'Tema2' and a time range from 'Feb 16, 2025 @ 18:27:05.980' to 'Feb 20, 2025 @ 00:05:47.8...'. The results show a histogram with a single bar for '47.819 (interval: Auto - hour)' on February 19, 2025. The results table lists documents with their '\_id', '\_index', '\_score', '\_type', and '\_version'. One document is expanded to show its full JSON content, which includes fields like '@timestamp', 'agent', 'log', 'suricata.eve', 'url', and 'url.domain'. The bottom of the screen shows a scrollable list of log entries.



## Configuración final de las políticas de Elastic

### 57. Fleet

The screenshot shows the Fleet management interface under the 'Security' tab. The left sidebar includes links for Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, Explore, Get started, Developer tools, and Project Settings. The main area is titled 'Fleet' and contains the message 'Centralized management for Elastic Agents.' Below this are tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. A search bar at the top allows filtering by KQL syntax. A table lists two agents: 'Linux rev. 3' and 'Windows rev. 2', showing details like last update date, privilege level (Unprivileged / Privileged), integrations (3 for Linux, 2 for Windows), and actions (three dots). A 'Create agent policy' button is located in the top right of the table area.

## 58. Linux Suricata/HoneyPot

The screenshot shows the 'Security' interface with the 'Discover' tab selected. On the left, there's a sidebar with various navigation options like 'Discover', 'Dashboards', 'Rules', 'Alerts', 'Attack discovery', 'Findings', 'Cases', 'Investigations', 'Intelligence', 'Explore', 'Assets' (which is highlighted), and 'Machine learning'. Below the sidebar are links for 'Get started', 'Developer tools', and 'Project Settings'. The main content area is titled 'Linux' and shows 'View all agent policies'. It includes statistics: Revision 3, Integrations 3, Agents 1 agent, and Last updated on Feb 18, 2025. There are tabs for 'Integrations' (selected) and 'Settings'. A search bar and a 'Namespace' dropdown are at the top. A blue button labeled 'Add integration' is visible. Below is a table with columns: Integration policy ↑, Integration ↓, Namespace, Output, and Actions. The table contains three rows:

Integration policy ↑	Integration ↓	Namespace	Output	Actions
log-honeypot	Custom Logs v2.3.3	default	Default output	...
suricata-linux	Suricata v2.23.0	default	Default output	...
system-1	System v1.66.1	default	Default output	...

## 59. Windows

This screenshot is similar to the previous one but for the 'Windows' environment. The sidebar and overall layout are identical. The main content area is titled 'Windows' and shows 'View all agent policies'. It includes the same statistics: Revision 2, Integrations 2, Agents 1 agent, and Last updated on Feb 18, 2025. The 'Integrations' tab is selected. A table below lists the integrations:

Integration policy ↑	Integration ↓	Namespace	Output	Actions
Windows	Elastic Defend v9.0.0	default	Default output	...
system-2	System v1.66.1	default	Default output	...

## Logs

60. Se adjunta el archivo "Logs\_Elastic.zip" y en el zip "Logs\_en\_Raw.zip" que se encuentran en crudo se encuentran los logs tanto de HoneyPot como de Suricata.

## Propuesta de mejora

Podemos mejorar la siguiente infraestructura al reforzar la segmentación de las redes utilizando VLANs y aplicando reglas estrictas en el firewall PfSense, como limitando solamente el tránsito de los logs hacia Elastic, y encriptando todo tipo de información sensible con ChaCha20-Poly1305.

También habría que separar y eliminar la interacción bilateral entre las redes internas DMZ2 y LAN, tal como ya se hizo con la red DMZ con el honeypot para que solo sea accesible desde la WAN. Además, se habilitaría un sistema de detección y prevención de intrusos (IDS/IPS) como Suricata en el firewall, así como listas blancas para controlar el tráfico permitido y listas negras dinámicas para bloquear direcciones IP maliciosas conocidas.

Además, los logs generados deben segregarse y analizarse mediante herramientas especializadas, configurando alertas en tiempo real para detectar actividad sospechosa como intentos de explotación o conexiones no autorizadas.

Por último, habría que implementar un sistema de copias de seguridad automáticas y periódicas de todos los datos críticos, asegurándose de que las copias sean almacenadas en una ubicación segura y aislada de la red principal.