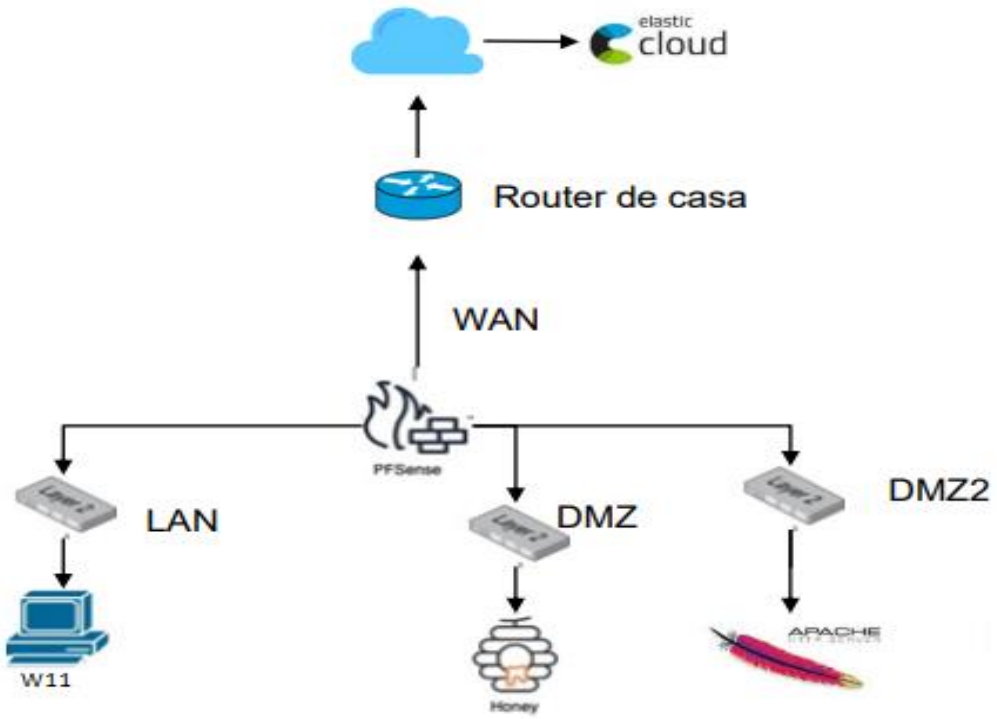
# Practica modulo: Blue team


**Realizado por:** David Fernández Domingo
**Email:** tecno_g33k@hotmail.com

# Índice

**Esquema de red y lo que se quiere implementar**



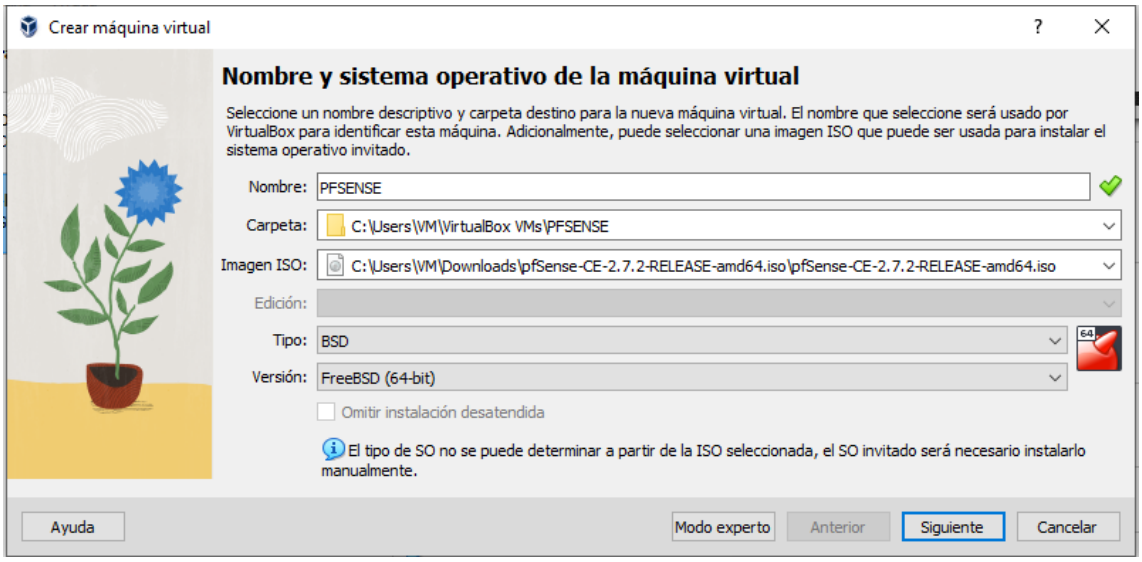

Se van a crear tres redes:

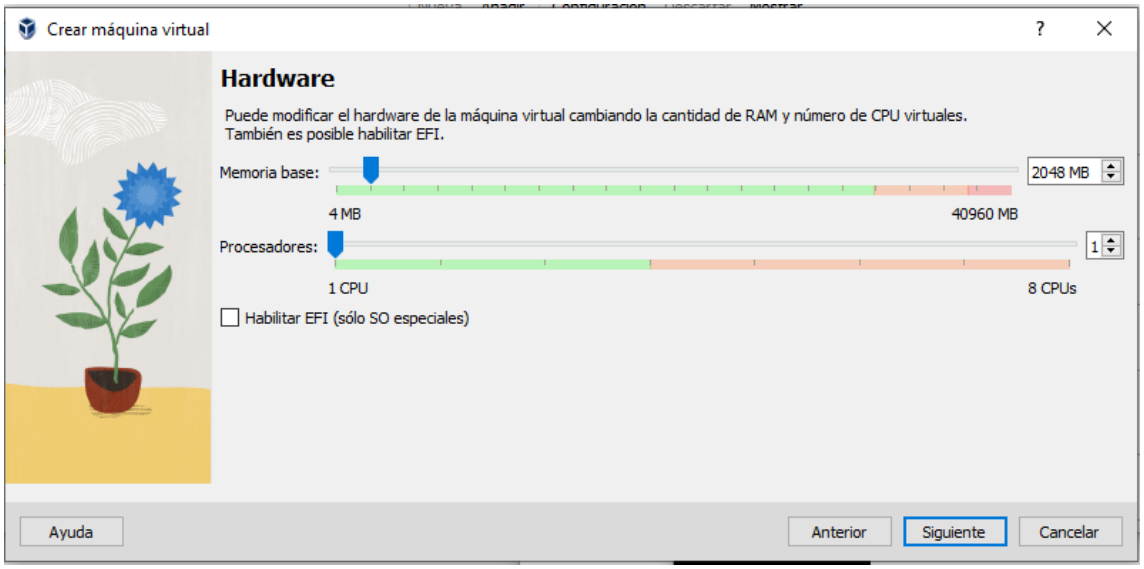
**LAN**, con el sistema Windows 11
**DMZ**, con un honeypot (Crownie) servidor ssh
**DMZ_2**, con un servidor apache web

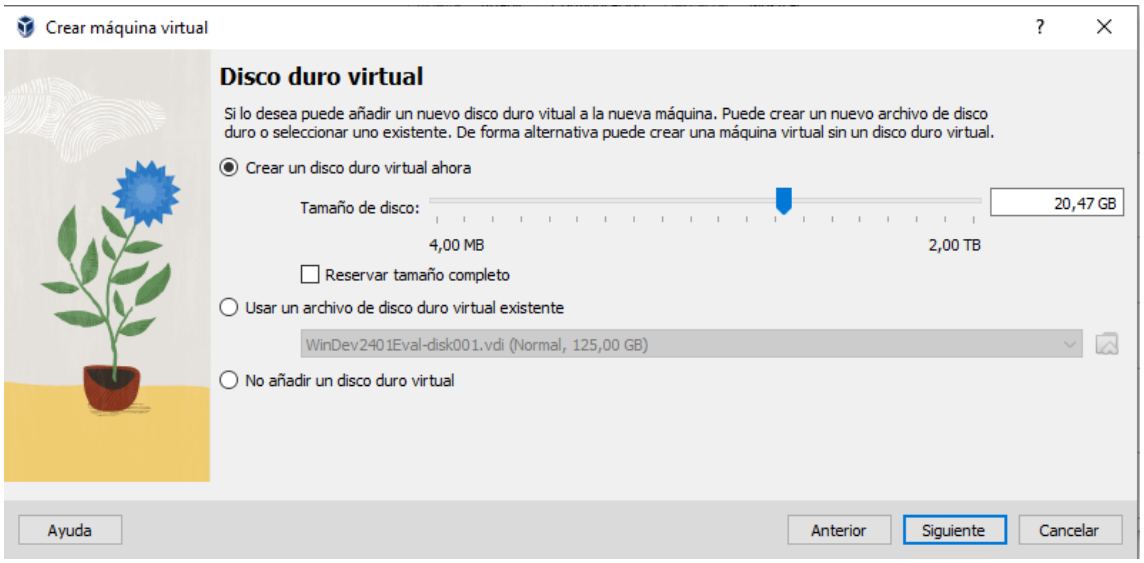
La red DMZ no puede ver al resto de subredes, pero sí tendrá acceso bidireccional a la WAN

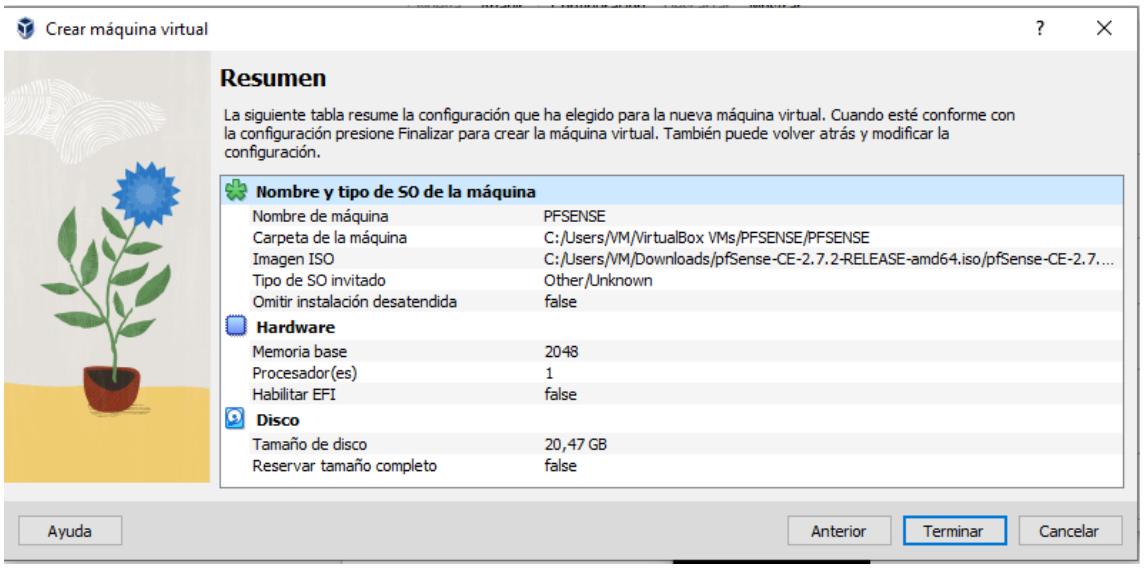
Las tres redes estarán con un agente de elastic cloud el cual enviara los logs de sistema

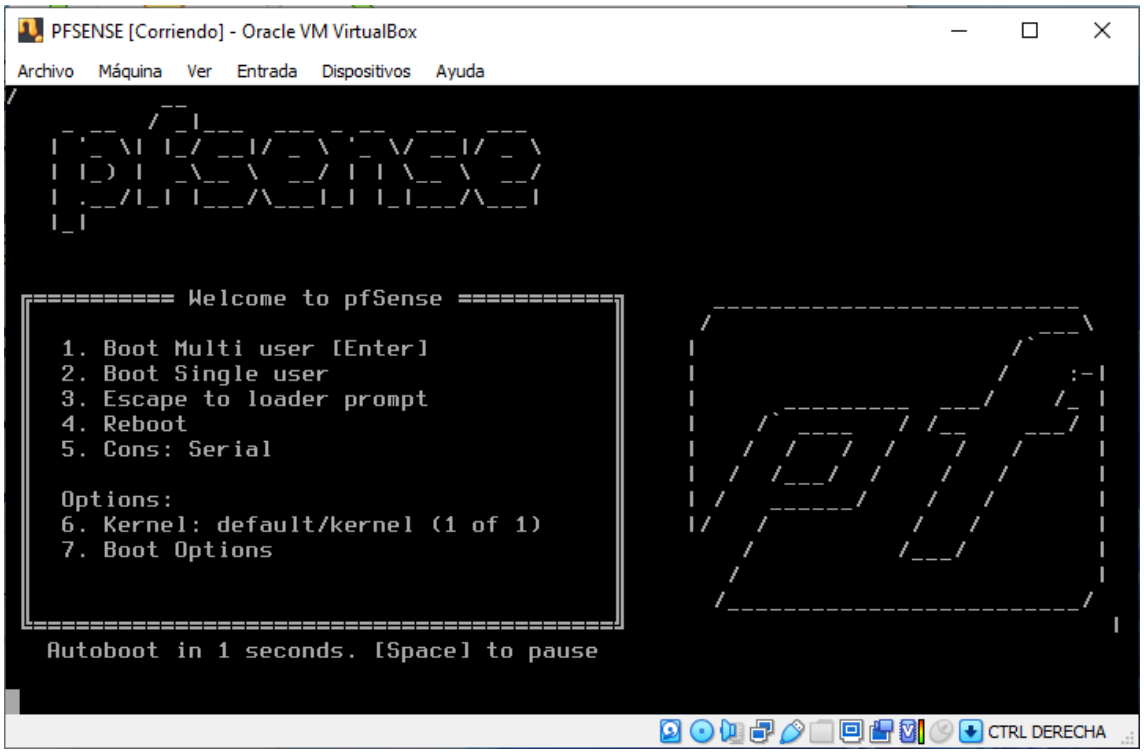
# Configuración PFSENSE

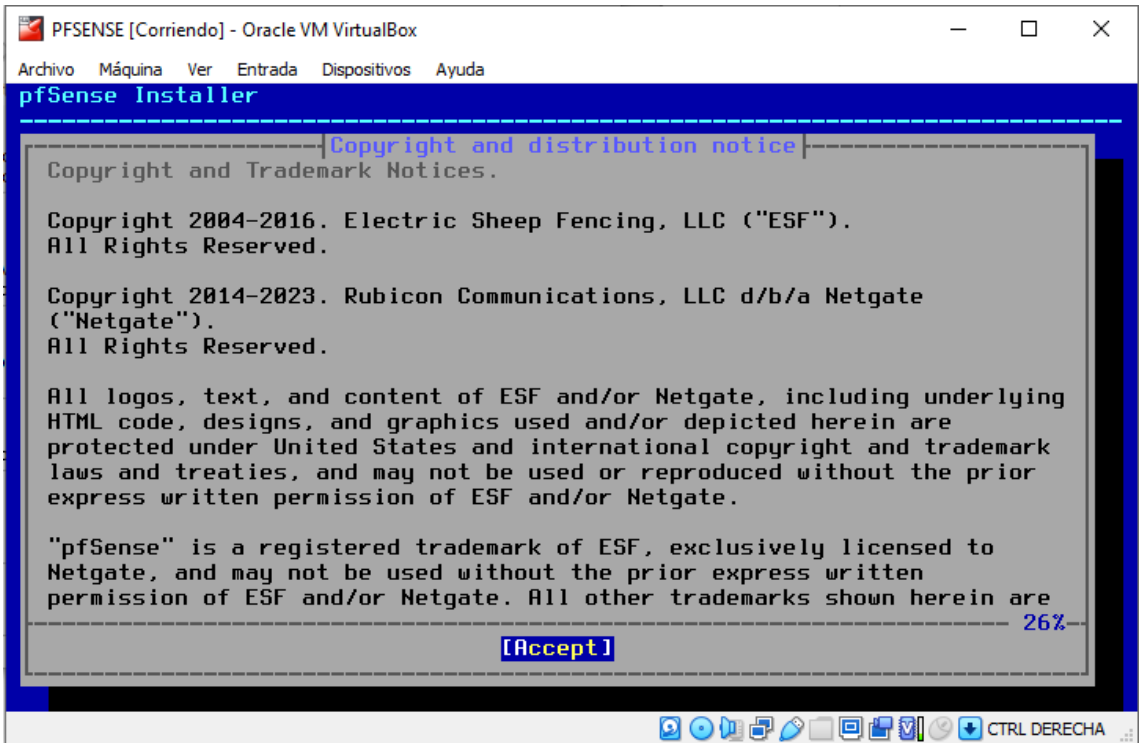


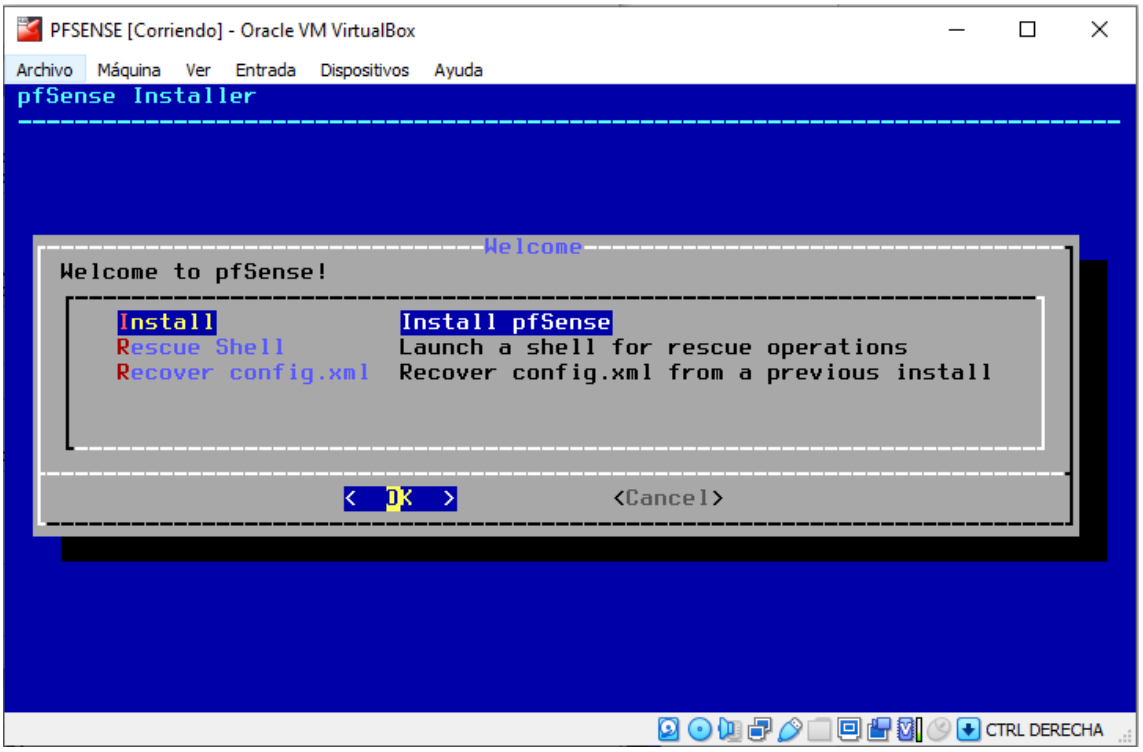



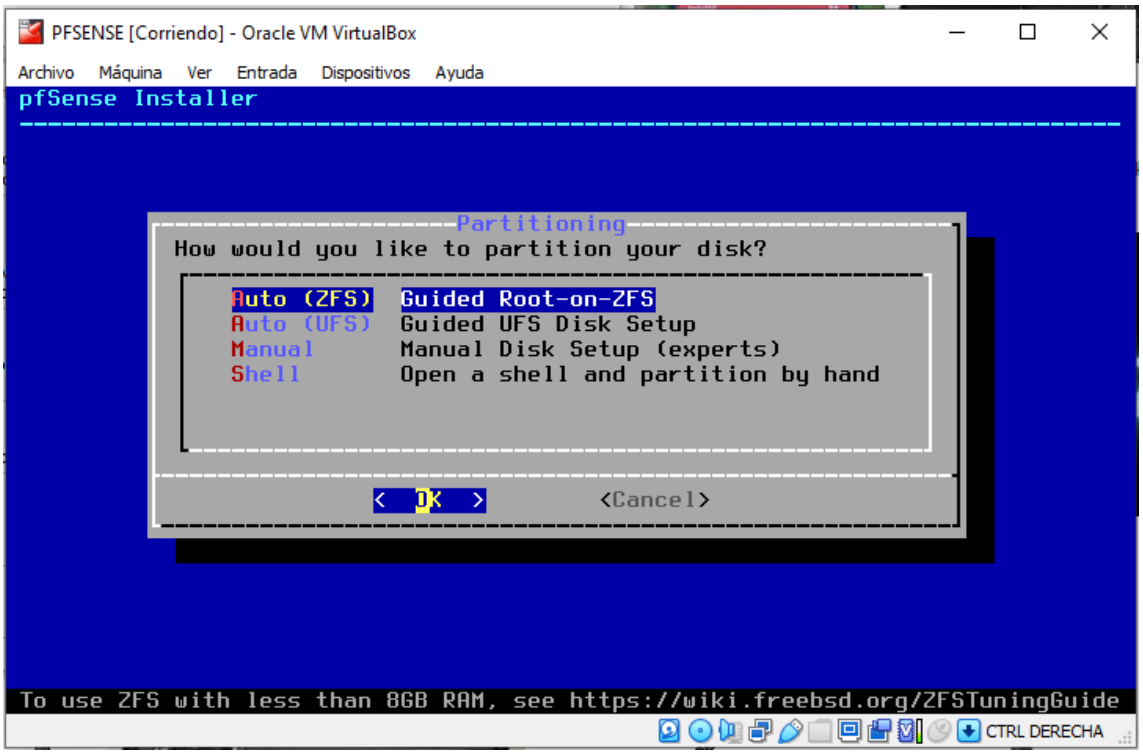



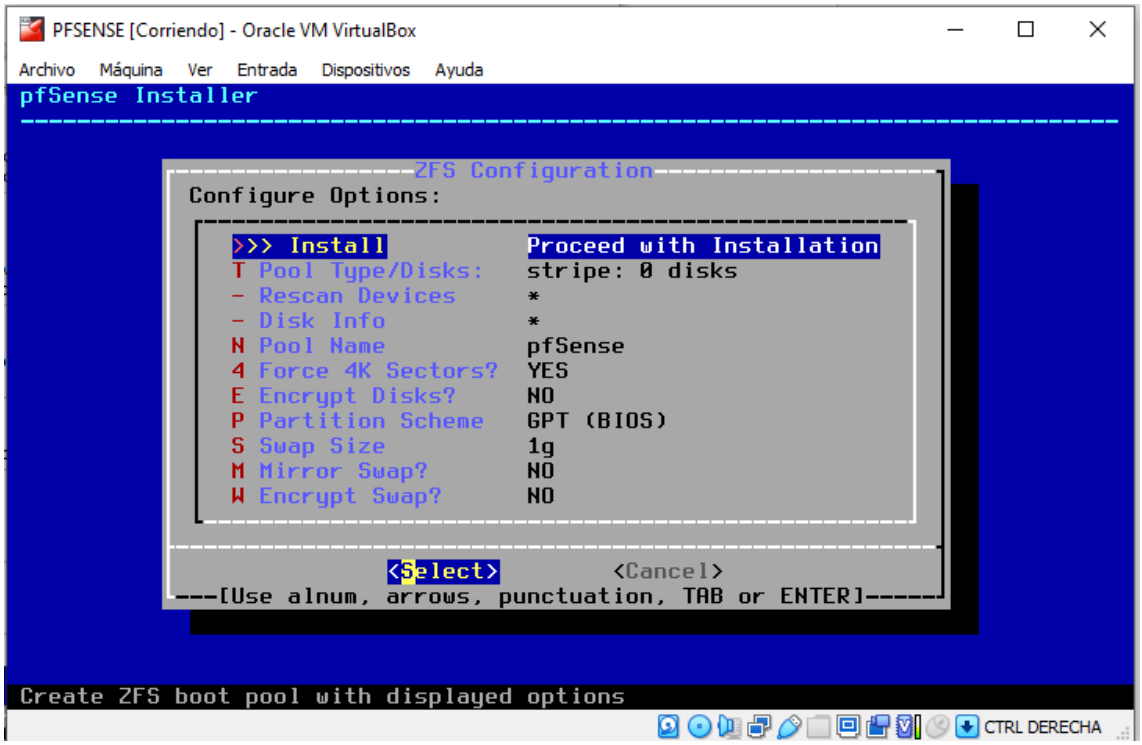

Crear máquina virtual
Resumen
La siguiente tabla resume la configuración que ha elegido para la nueva máquina virtual. Cuando esté conforme con la configuración presione Finalizar para crear la máquina virtual. También puede volver atrás y modificar la configuración.
Nombre y tipo de SO de la máquina
Nombre de máquina PFSENSE
Carpeta de la máquina C:/Users/VM/VirtualBox VMs/PFSENSE/PFSENSE
Imagen ISO C:/Users/VM/Downloads/pfSense-CE-2.7.2-RELEASE-amd64.iso/pfSense-CE-2.7....
Tipo de SO invitado Other/Unknown
Omitir instalación desatendida false
Hardware
Memoria base 2048
Procesador(es) 1
Habilitar EFI false
Disco
Tamaño de disco 20,47 GB
Reservar tamaño completo false
Ayuda
Anterior
Terminar
Cancelar

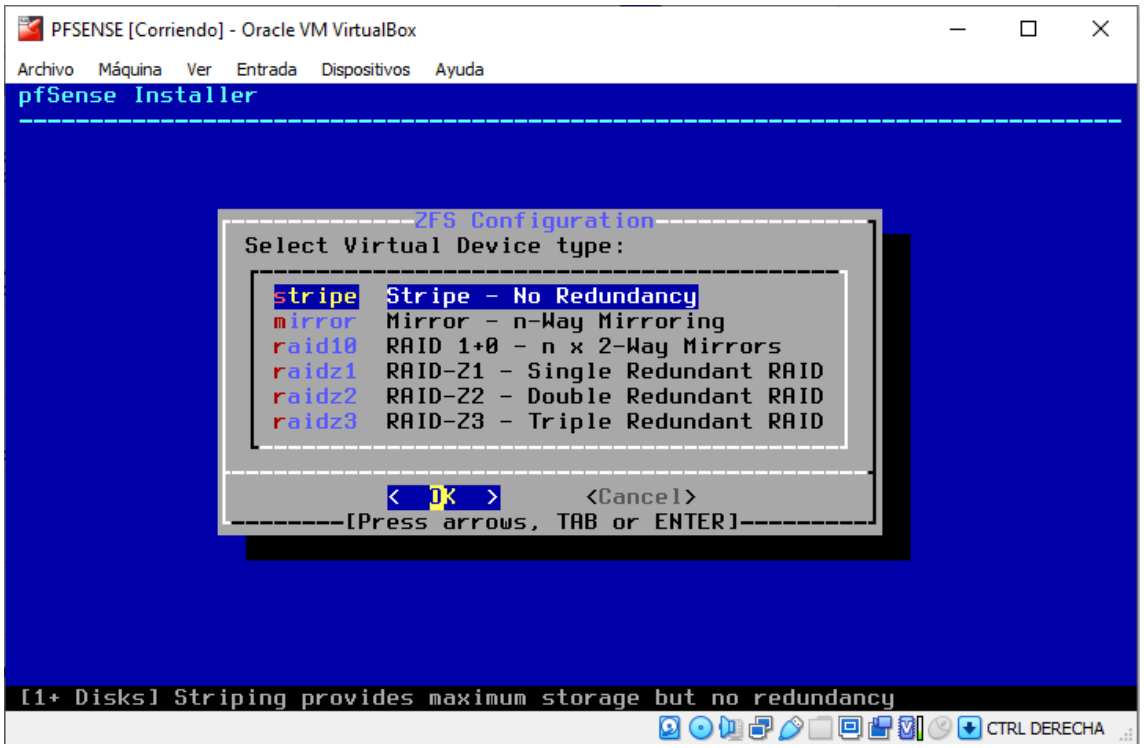

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 1 seconds. [Space] to pause
CTRL DERECHA

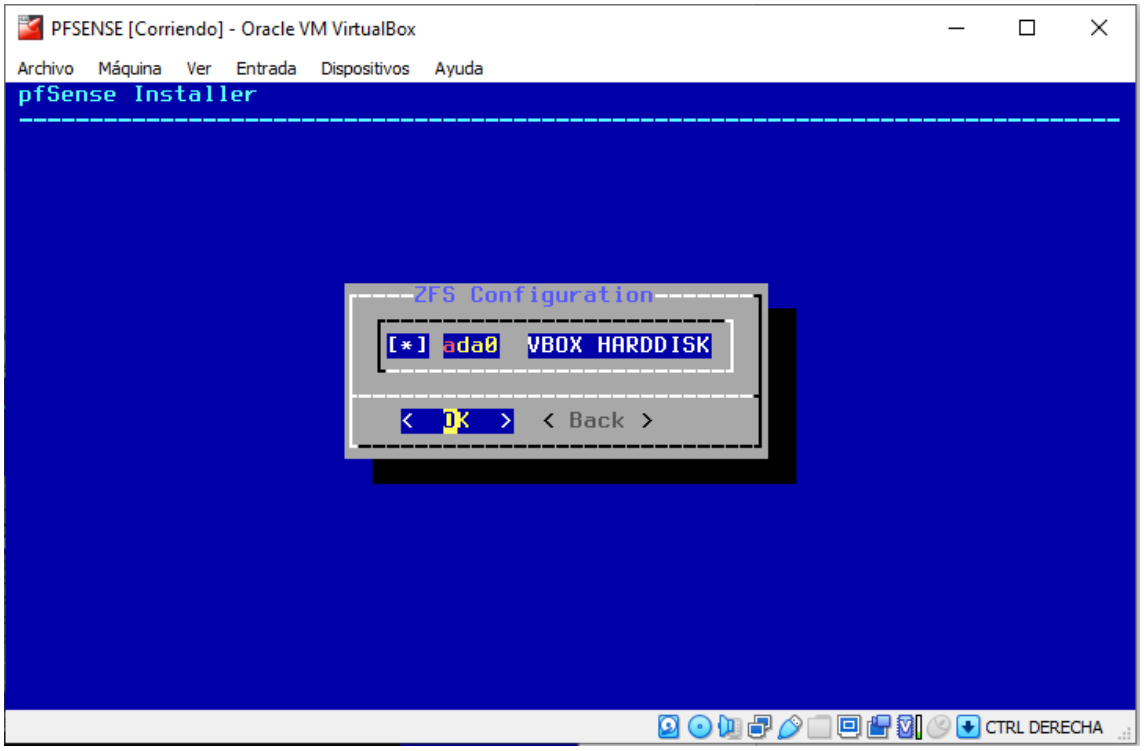

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC 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]
CTRL DERECHA

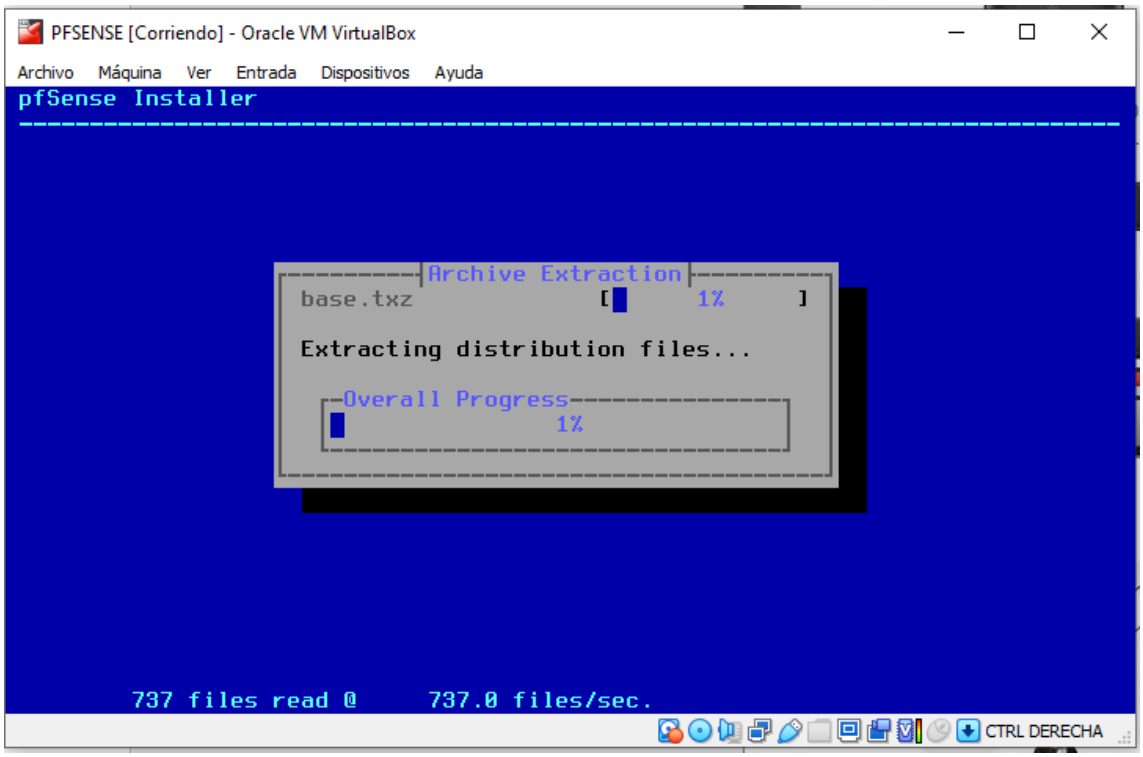

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install
< OK >
<Cancel>
CTRL DERECHA

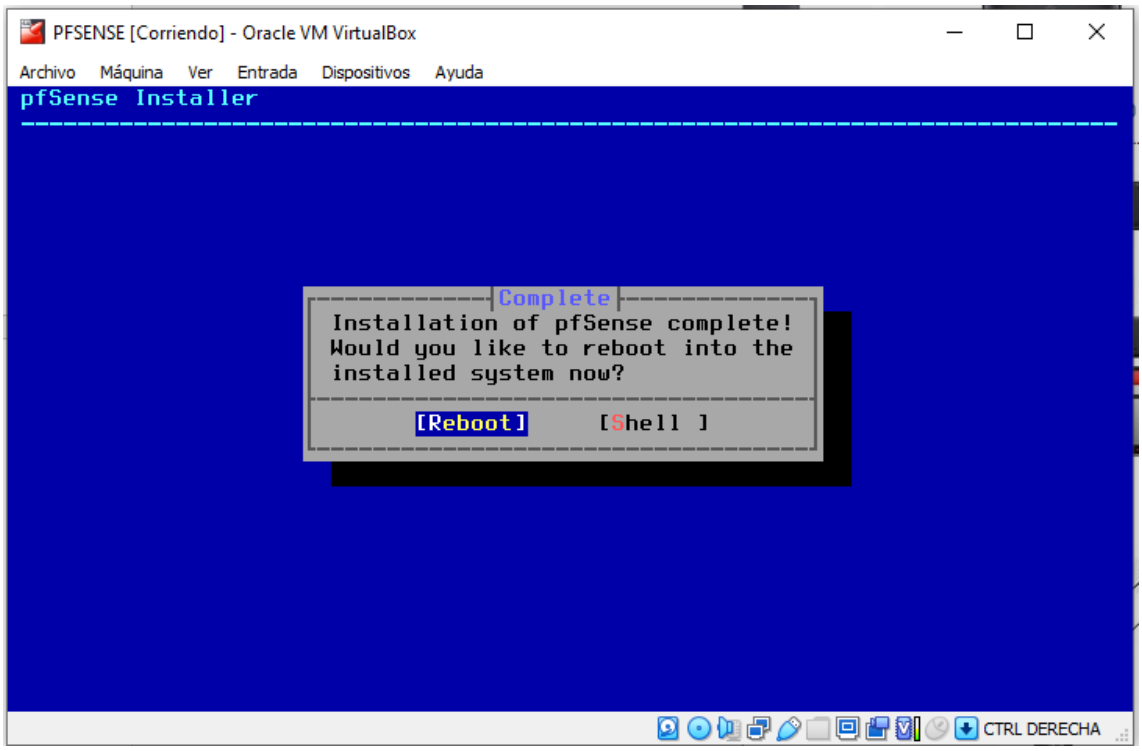

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide
CTRL DERECHA


PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
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
CTRL DERECHA

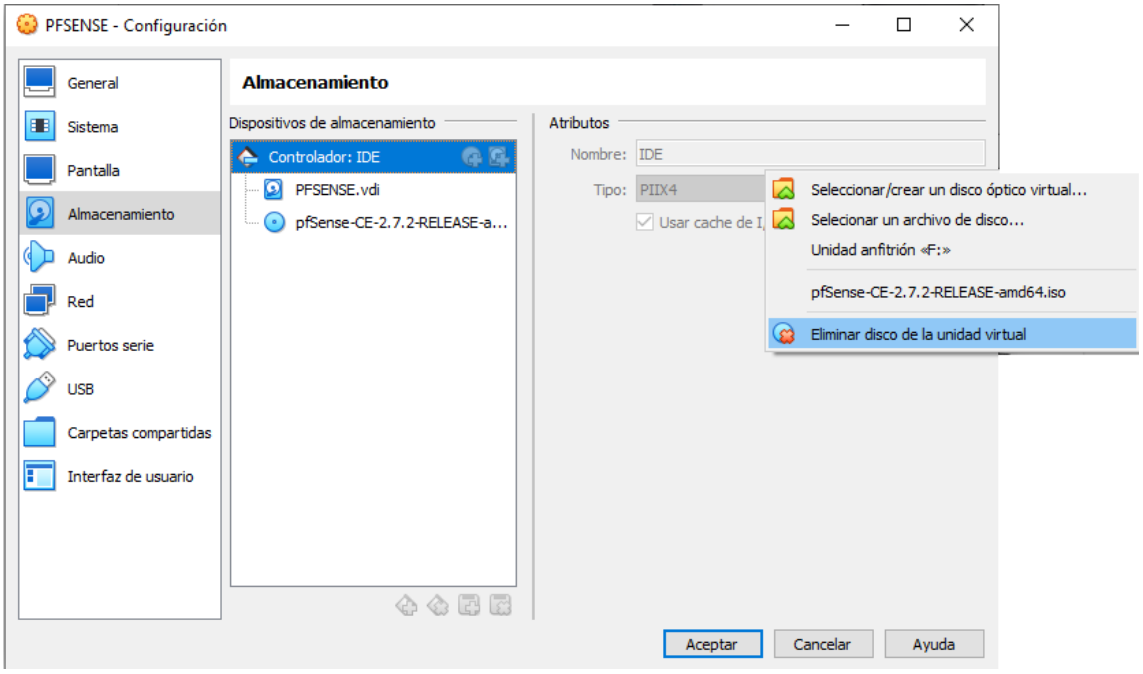

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - 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
CTRL DERECHA


PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
ZFS Configuration
[*] ada0 VBOX HARDDISK
< OK > < Back >
CTRL DERECHA

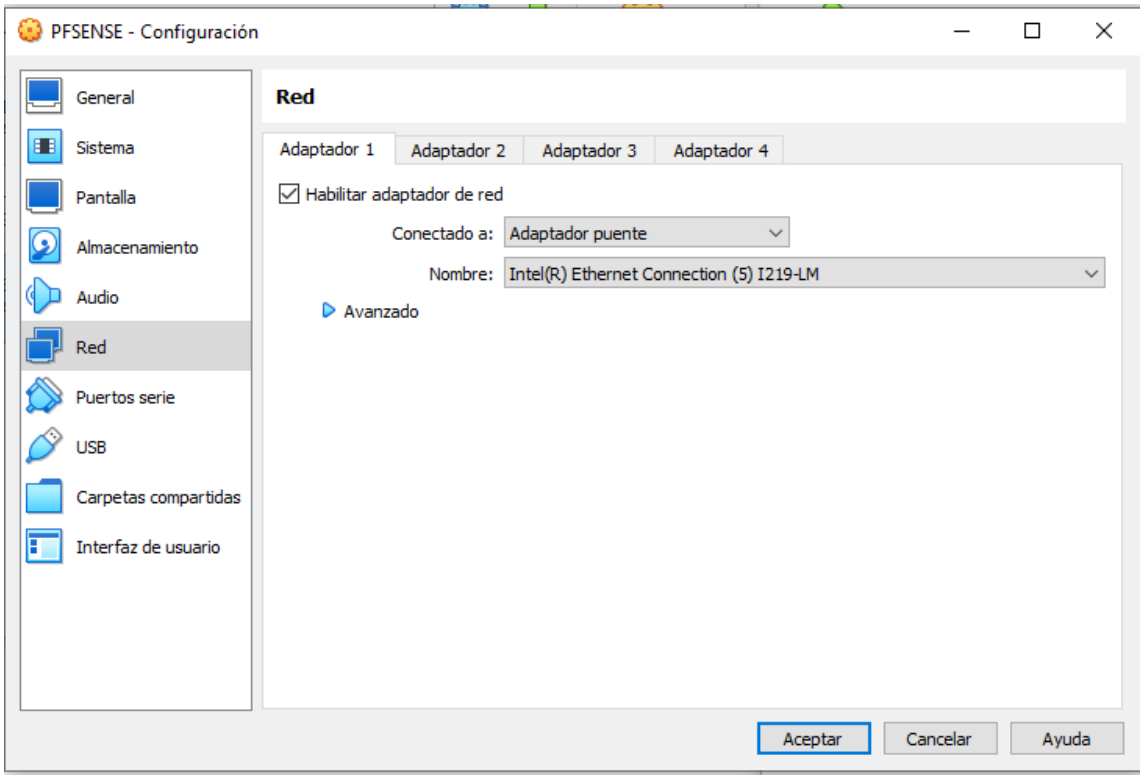

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
Archive Extraction
base.txz [ 1% ]
Extracting distribution files...
Overall Progress
1%
737 files read @ 737.0 files/sec.
CTRL DERECHA

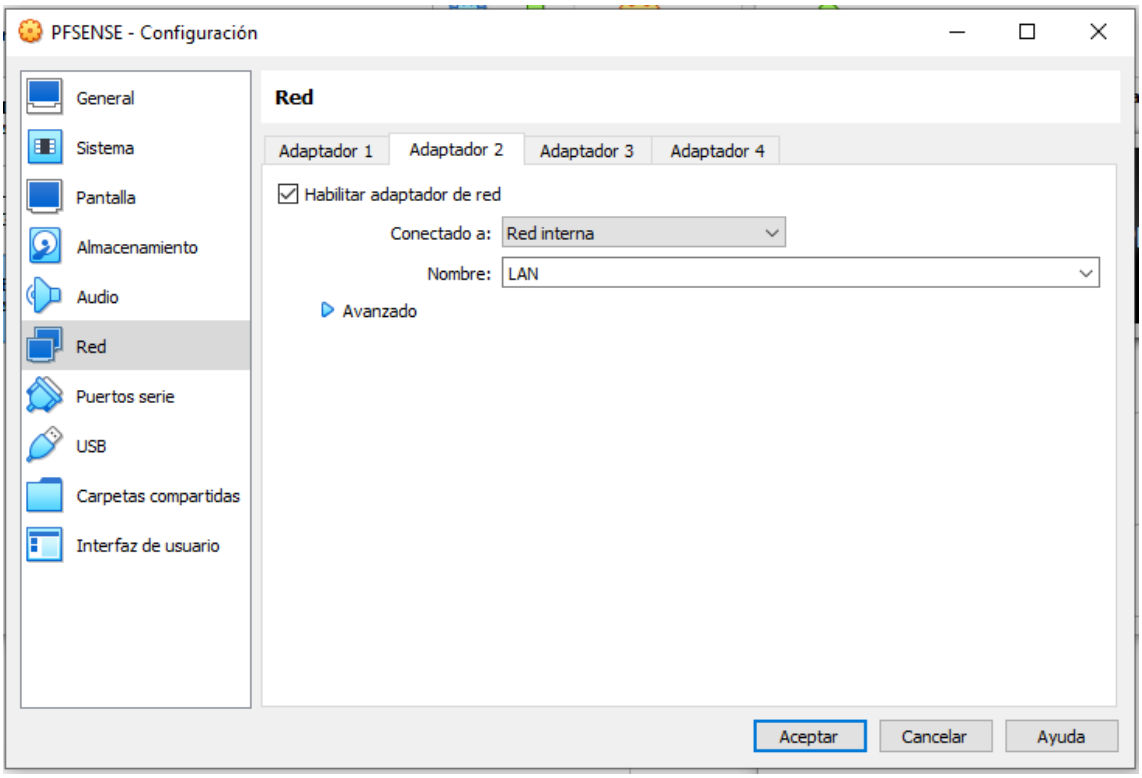

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
pfSense Installer
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?
[Reboot] [Shell ]
CTRL DERECHA

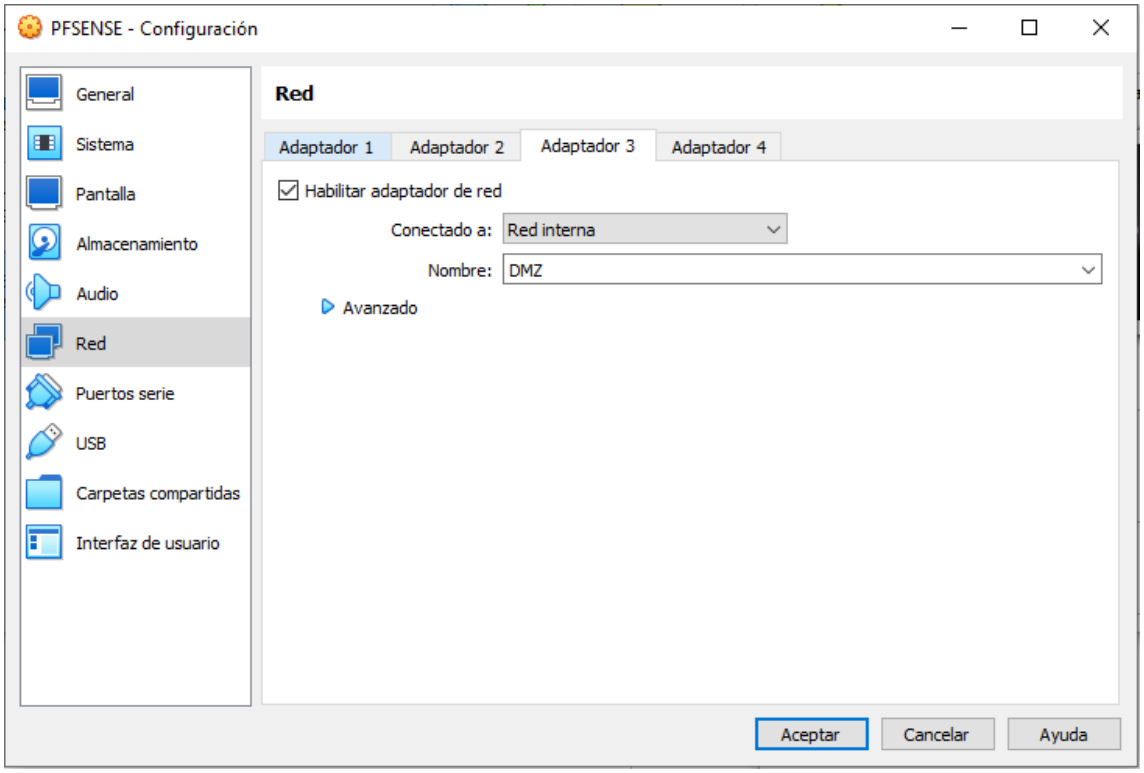
Importante eliminar el disco virtual para que no vuelva a reinstalar el Pfsense

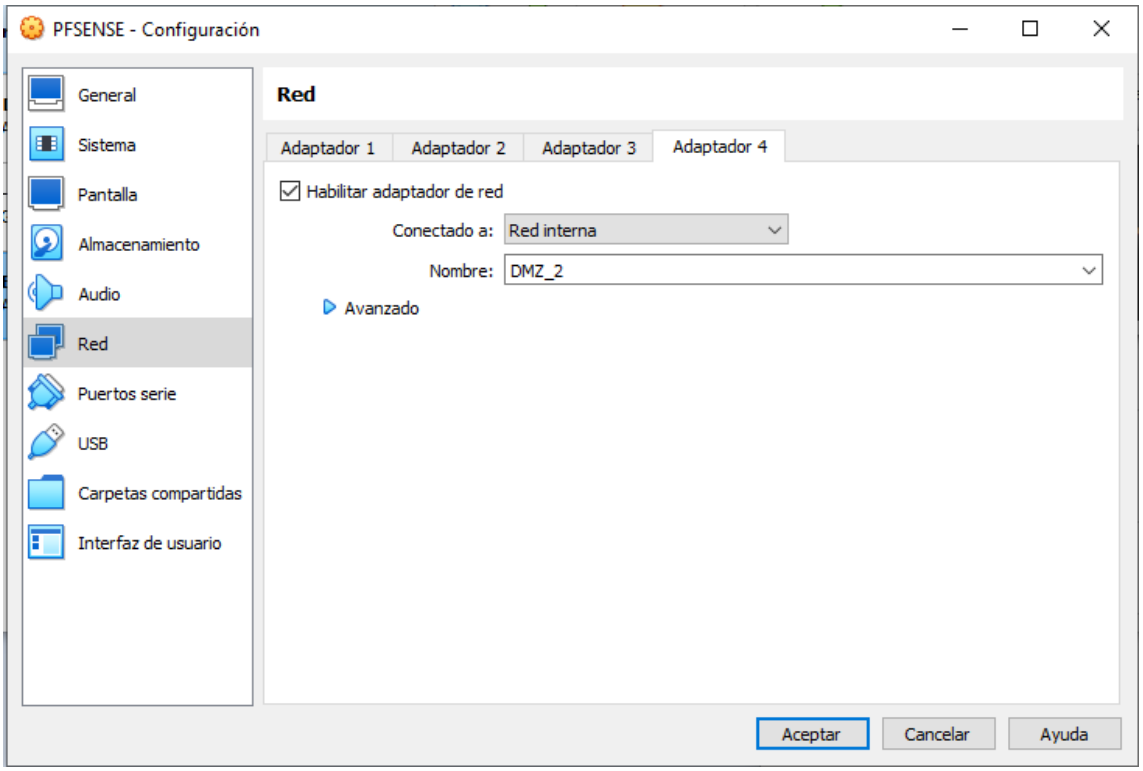


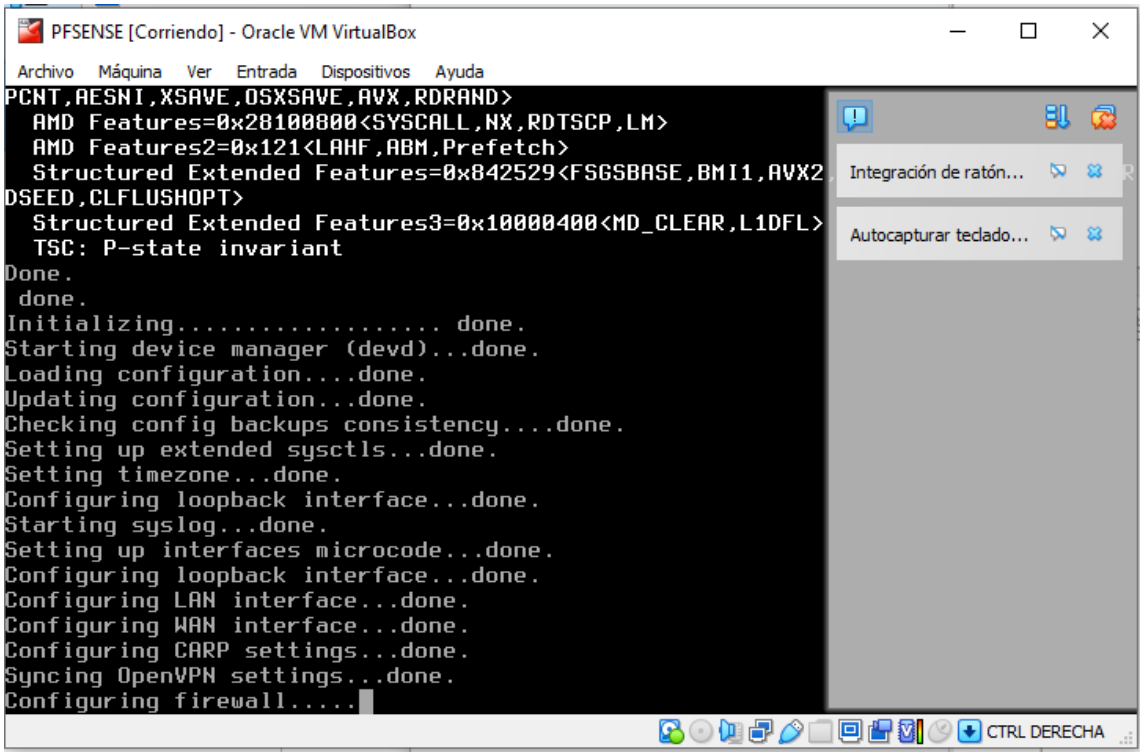

Configuro las tarjetas de red tal y como se requiere para implementar la estructura de red

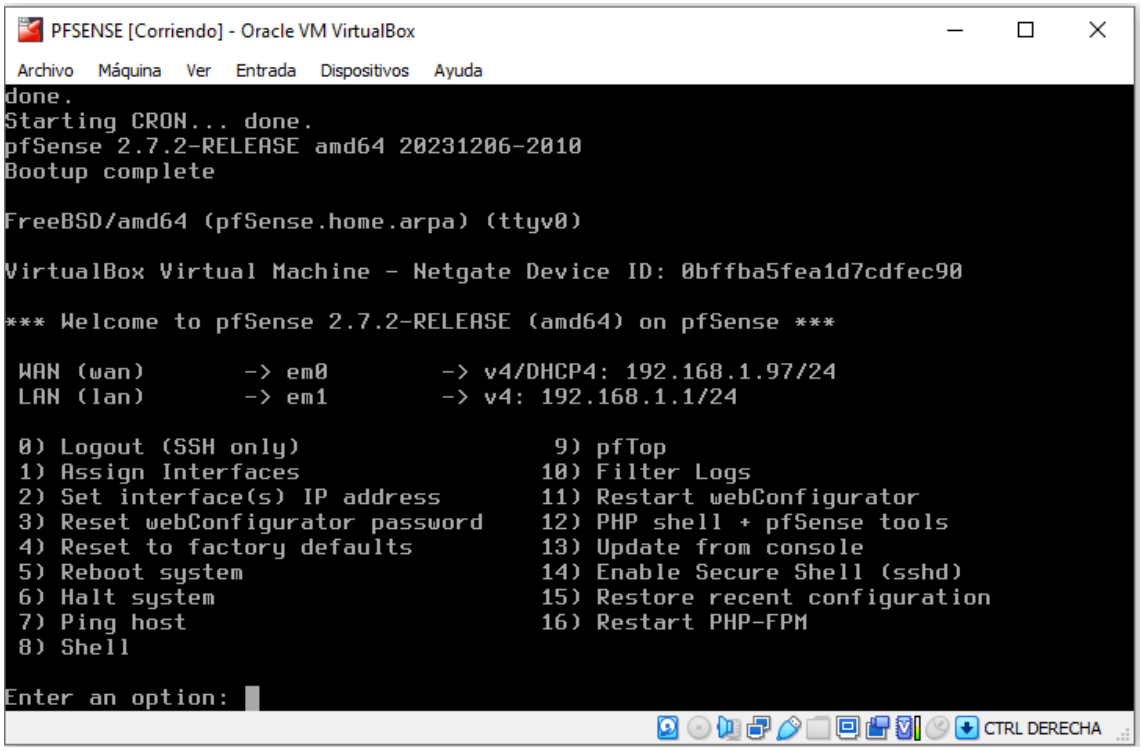



PFSENSE - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
LAN
Avanzado
Aceptar
Cancelar
Ayuda

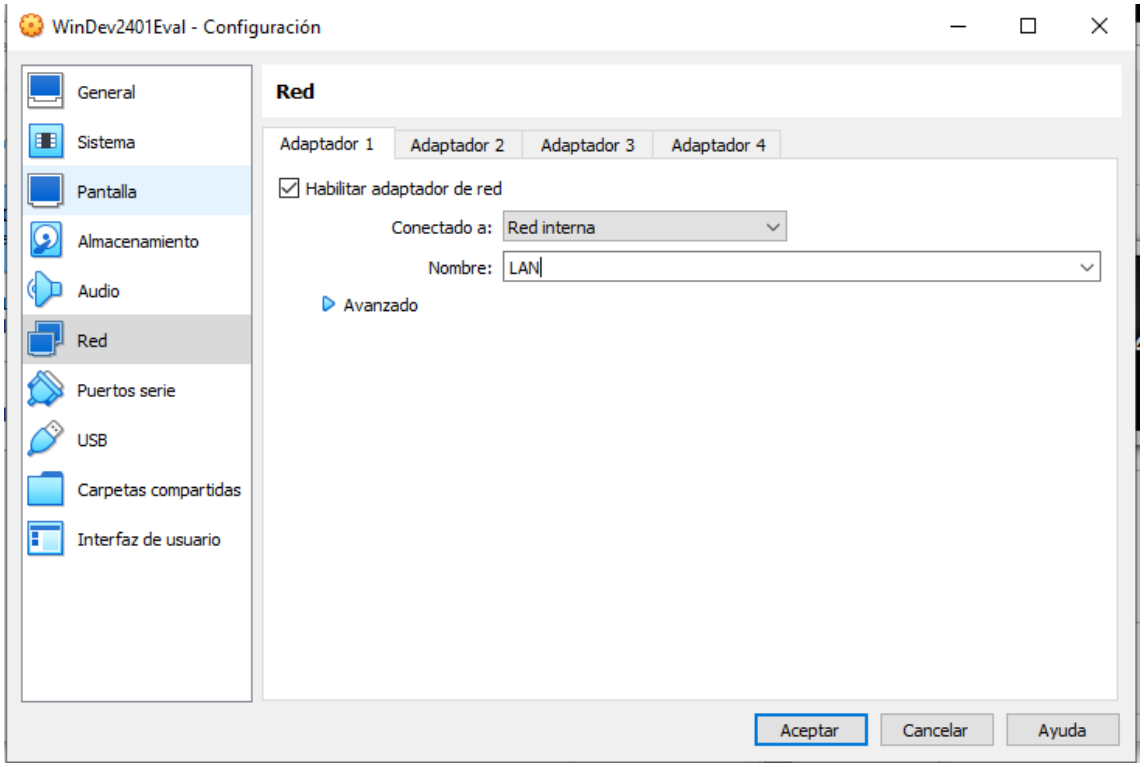

PFSENSE - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
DMZ
Avanzado
Aceptar
Cancelar
Ayuda


PFSENSE - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
DMZ_2
Avanzado
Aceptar
Cancelar
Ayuda

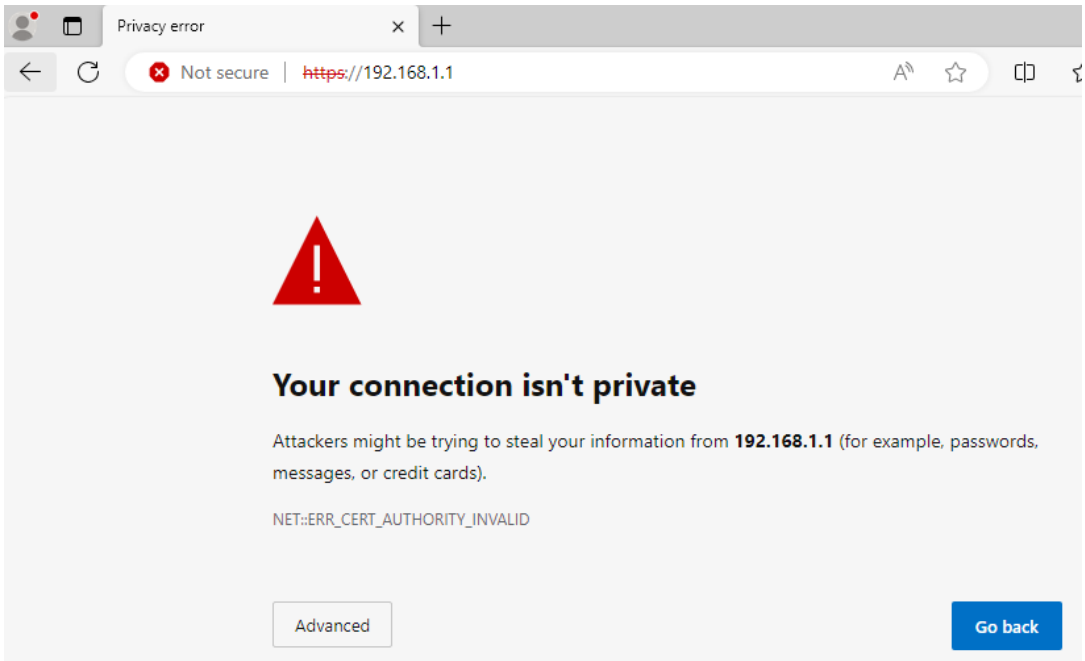

PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
PCNT,AESNI,XSAVE,OSXSAVE,AVX,RDRAND>
AMD Features=0x28100800<SYSCALL,NX,RDTSCP,LM>
AMD Features2=0x121<LAHF,ABM,Prefetch>
Structured Extended Features=0x842529<FSGSBASE,BMI1,AVX2,
DSEED,CLFLUSHOPT>
Structured Extended Features3=0x10000400<MD_CLEAR,L1DFL>
TSC: P-state invariant
Done.
done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration....done.
Updating configuration...done.
Checking config backups consistency....done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring LAN interface...done.
Configuring WAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA



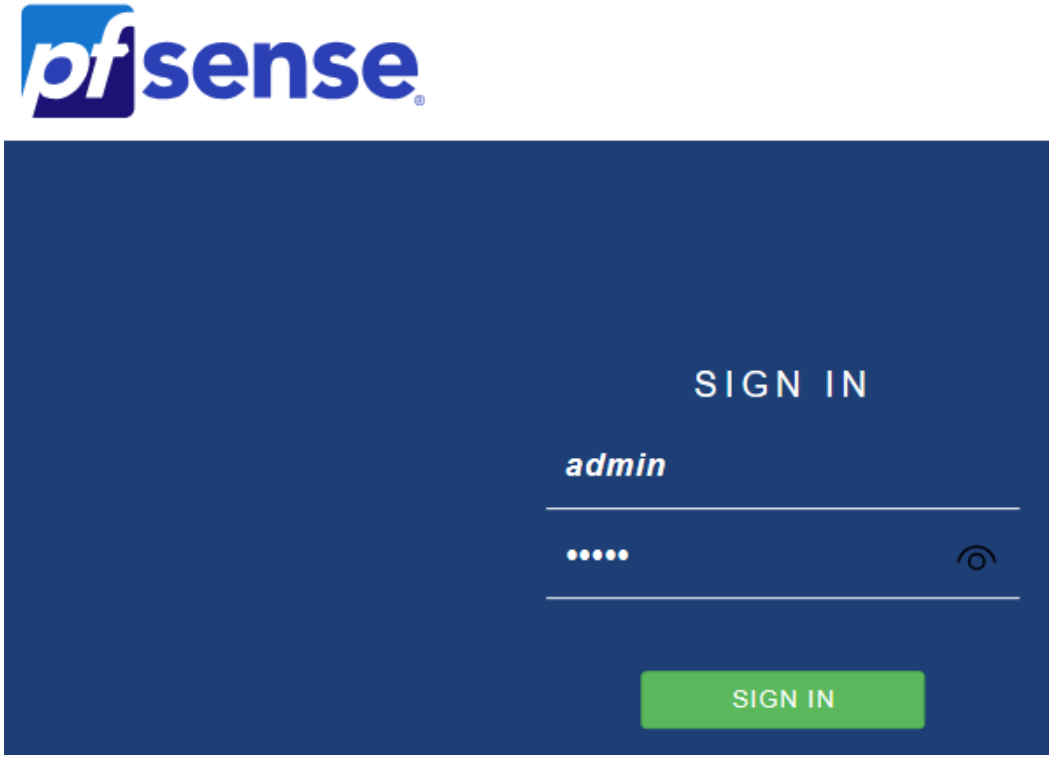

Una vez tenemos el PFSENSE iniciado, pondré Windows 11 para que se encuentre en la red LAN para poder configurar el PFSENSE



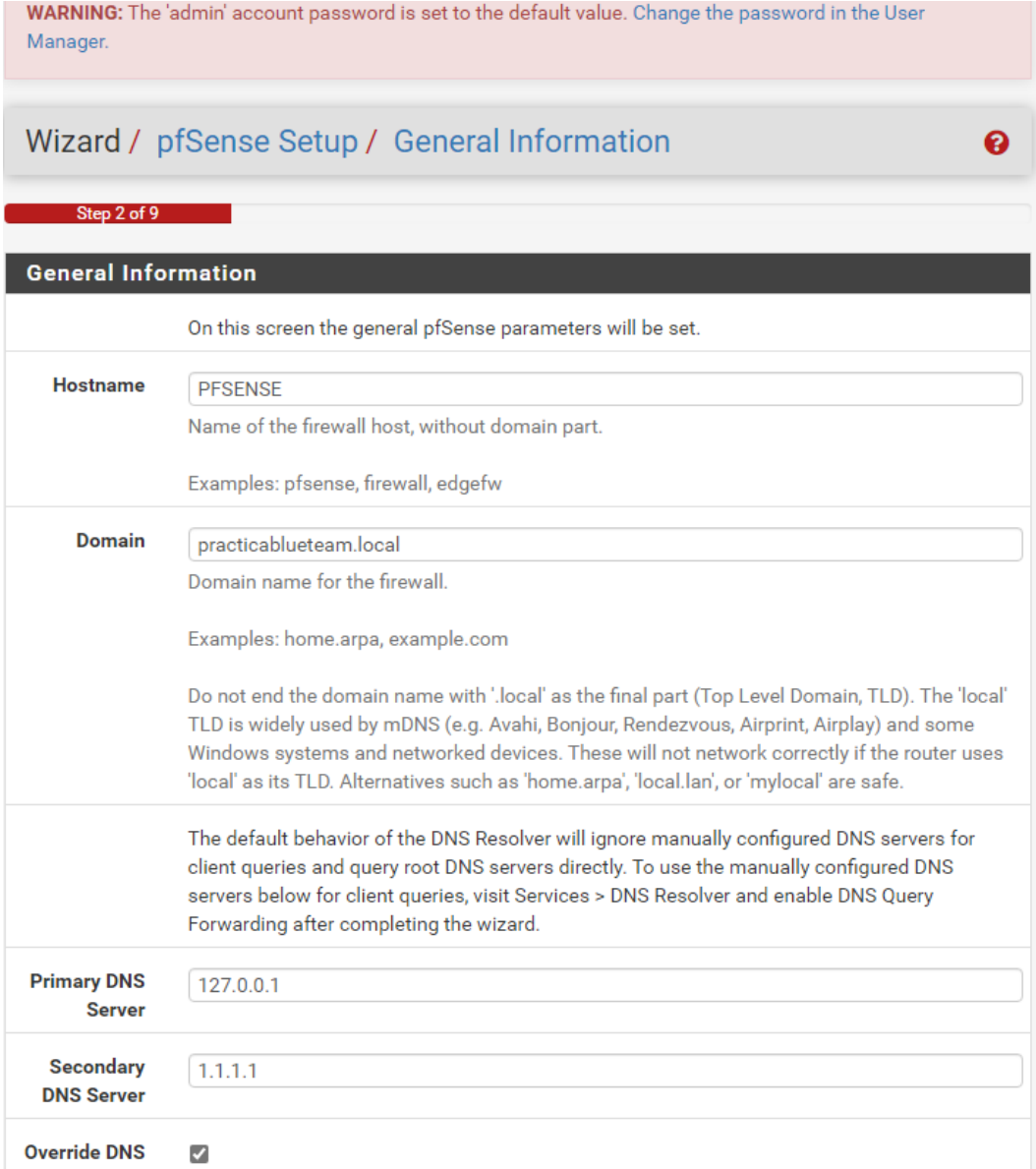
Para poder acceder al PFSENSE, en Windows 11 pongo la IP de LAN que nos da pFSENSE: **192.168.1.1**, ya que está actuando como router



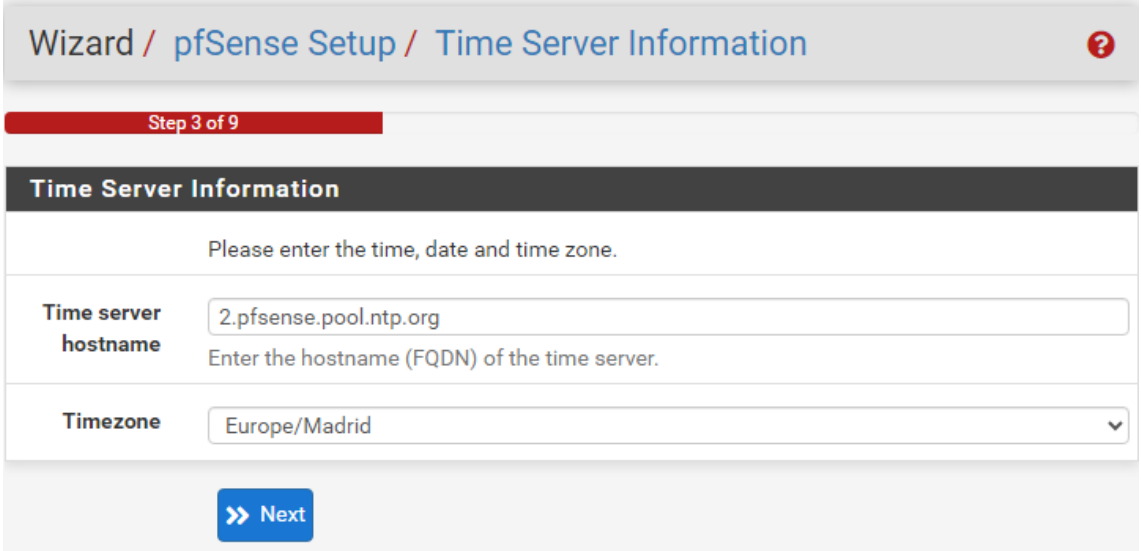

Este aviso aparece porque los datos van por HTTP y no van encriptados, en advanced le damos a Continue, introducimos admin/pfsense




Nos validamos y pulsamos siguiente (next) hasta llegar al paso 2




Configuro hostname y dominio, tambien el DNS primario y uno secundario el 1.1.1.1 (cloudflare)



Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

## Configure WAN Interface

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

**SelectedType** DHCP

## 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: xx:xx:xx:xx:xx: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 this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

## Static IP Configuration

**IP Address**

**Subnet Mask** 32

**Upstream Gateway**

Configuro para que nos bloquee las ip internas

## RFC1918 Networks

**Block RFC1918 Private Networks**

☐ Block private networks from entering via WAN

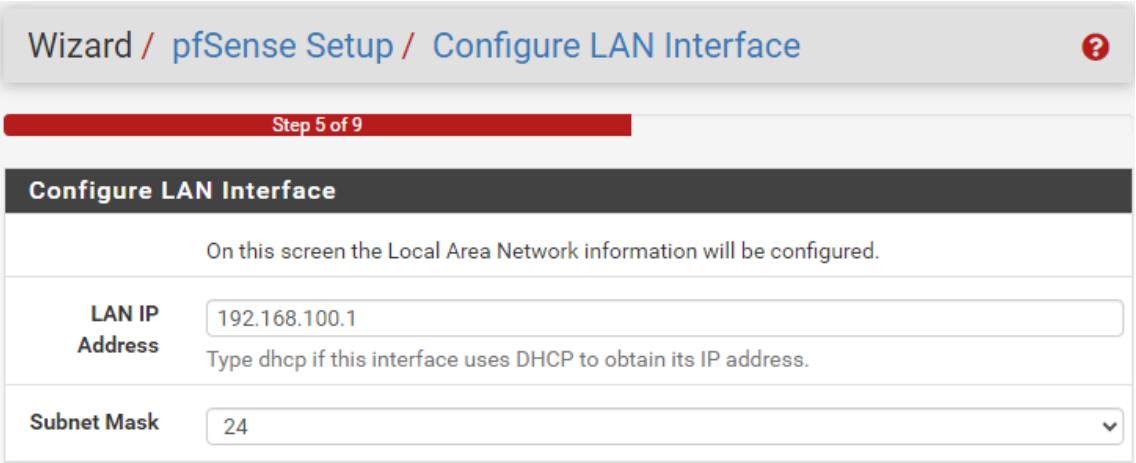
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

## 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.

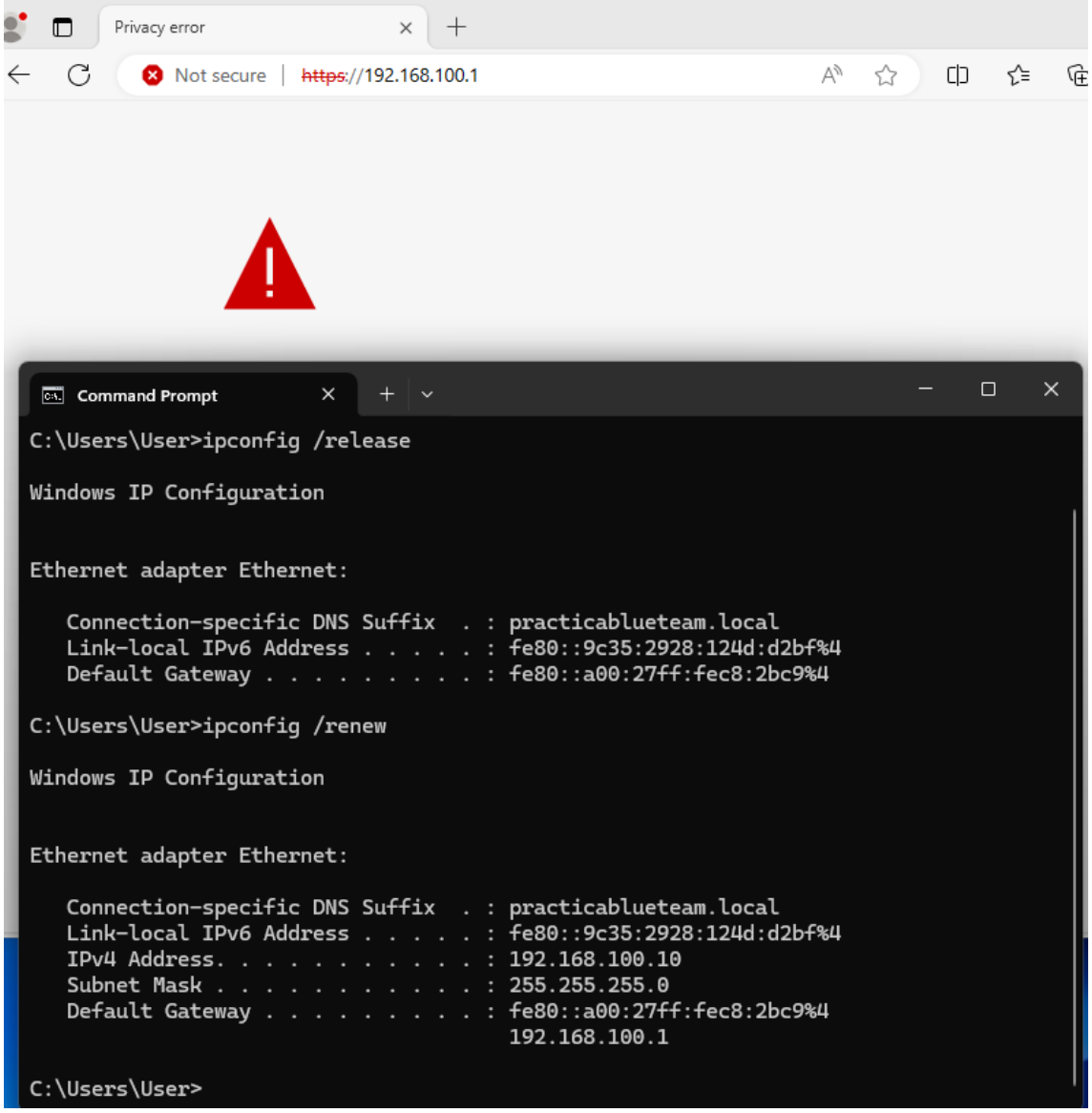



Se configura la subred a la que quiero que pertenezca: **192.168.100.1** y se cambia de contraseña

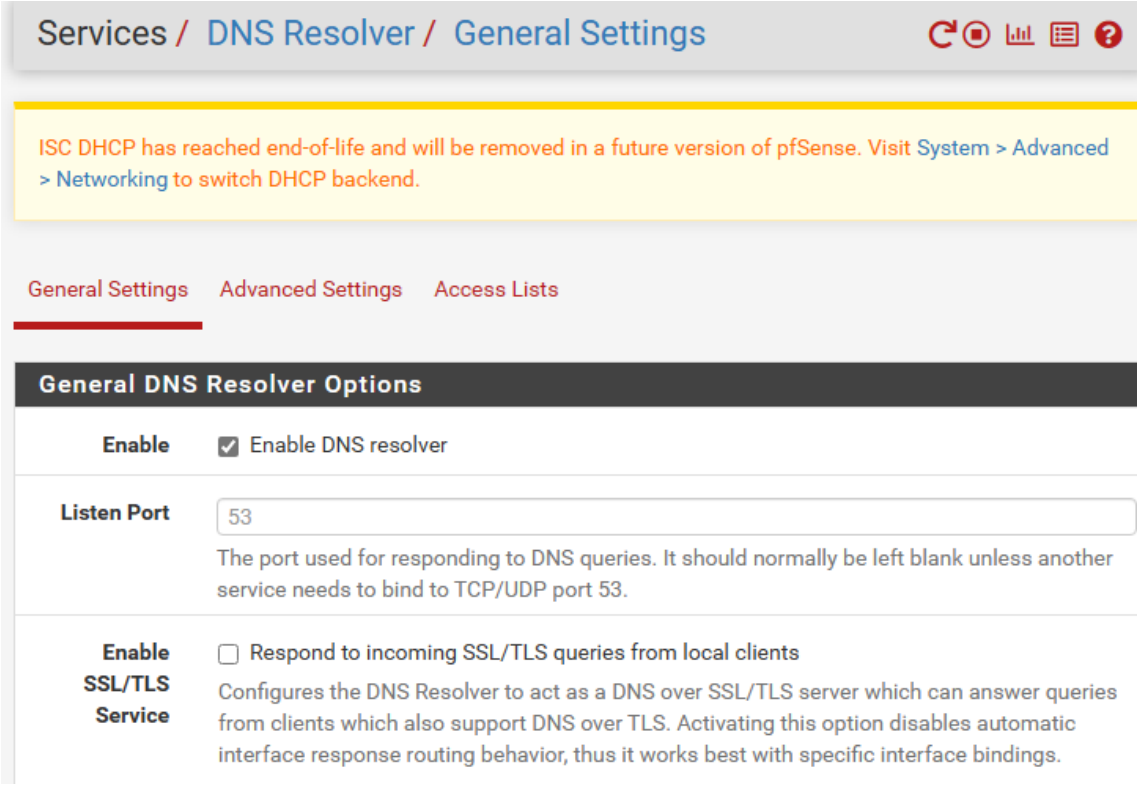


Al darle reload, se reinica el Pfsense

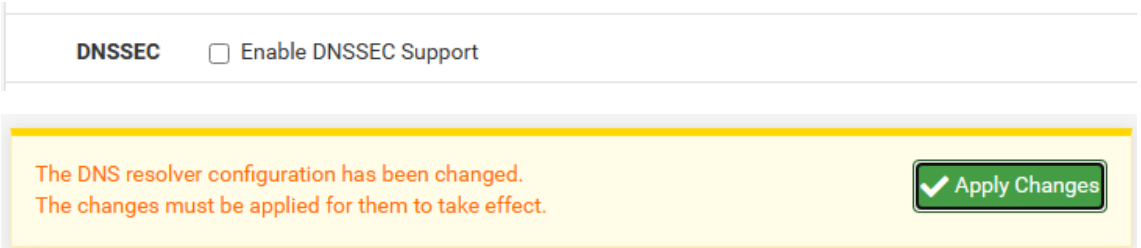
Entramos con la nueva dirección, 192.168.100.1



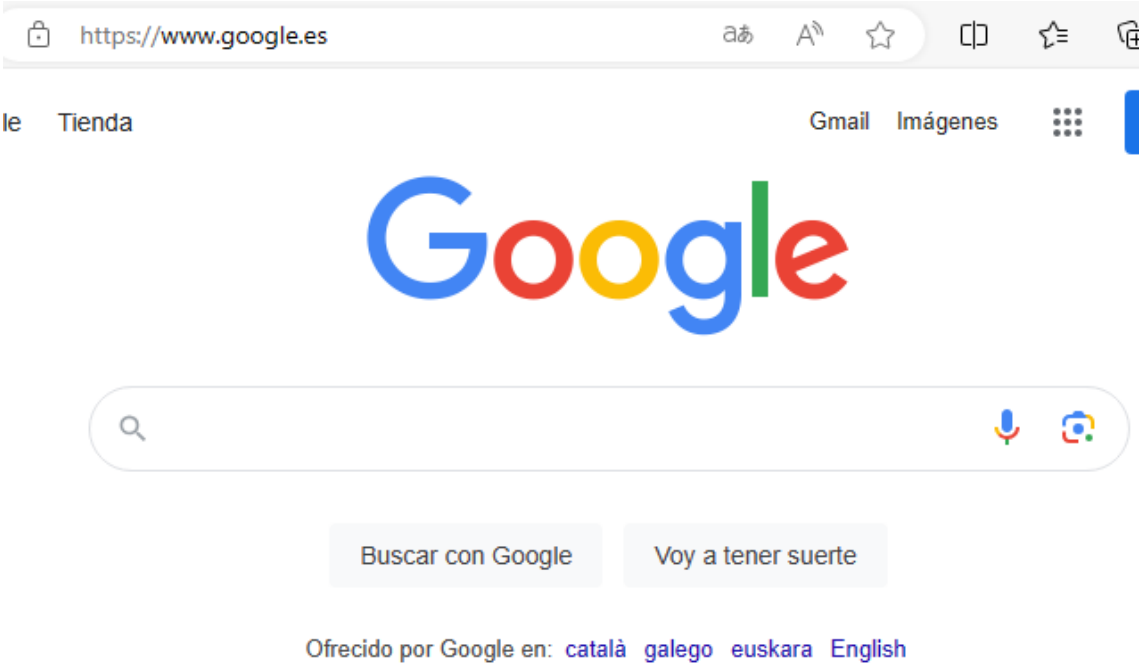

Compruebo y configuro para la resolución de nombres y habilito



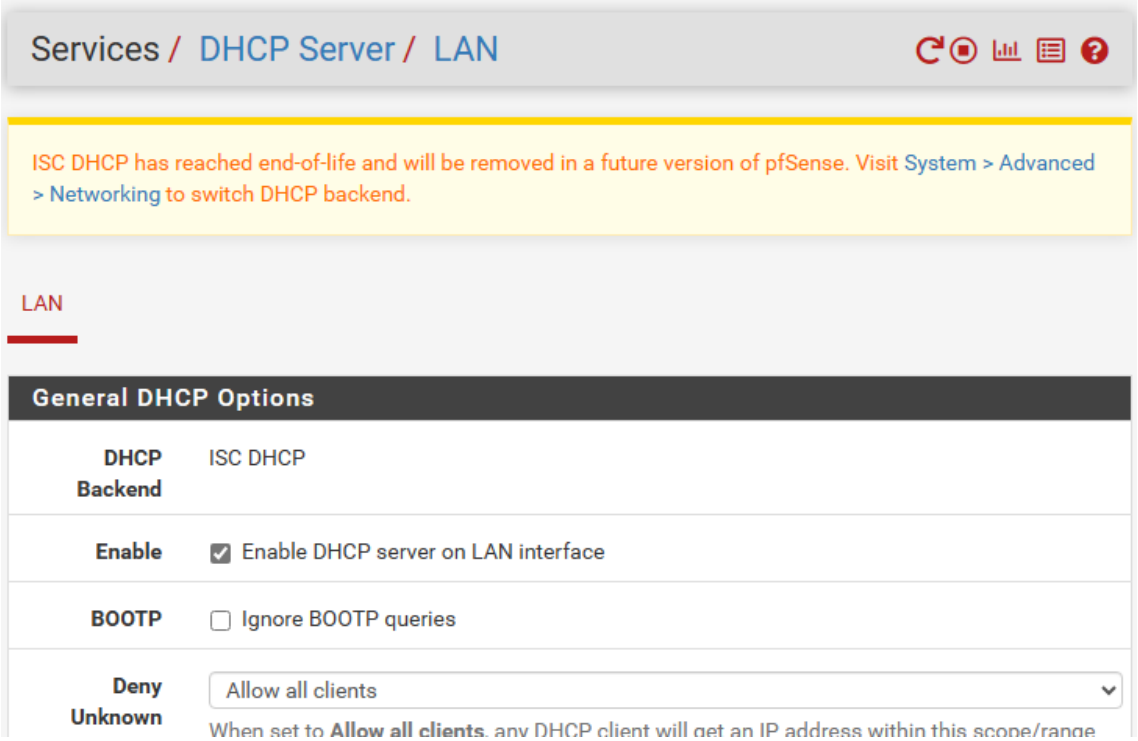

Deshabilito la opción para que nos devuelva la DNS




Ahora compruebo si hay acceso a Google y veo que está bien correctamente:




Configuración del DHCP server en la LAN



**Primary Address Pool**

| | |
|---|---|
| **Subnet** | 192.168.100.0/24 |
| **Subnet Range** | 192.168.100.1 - 192.168.100.254 |
| **Address Pool Range** | 192.168.100.100 From — 192.168.100.200 To<br>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<br>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here. |

**Server Options**

| | |
|---|---|
| **WINS Servers** | WINS Server 1 |
| | WINS Server 2 |
| **DNS Servers** | 192.168.100.1 |
| | 1.1.1.1 |
| | 8.8.8.8 |
| | DNS Server 4 |

Configuramos la puerta de enlace (gateway)

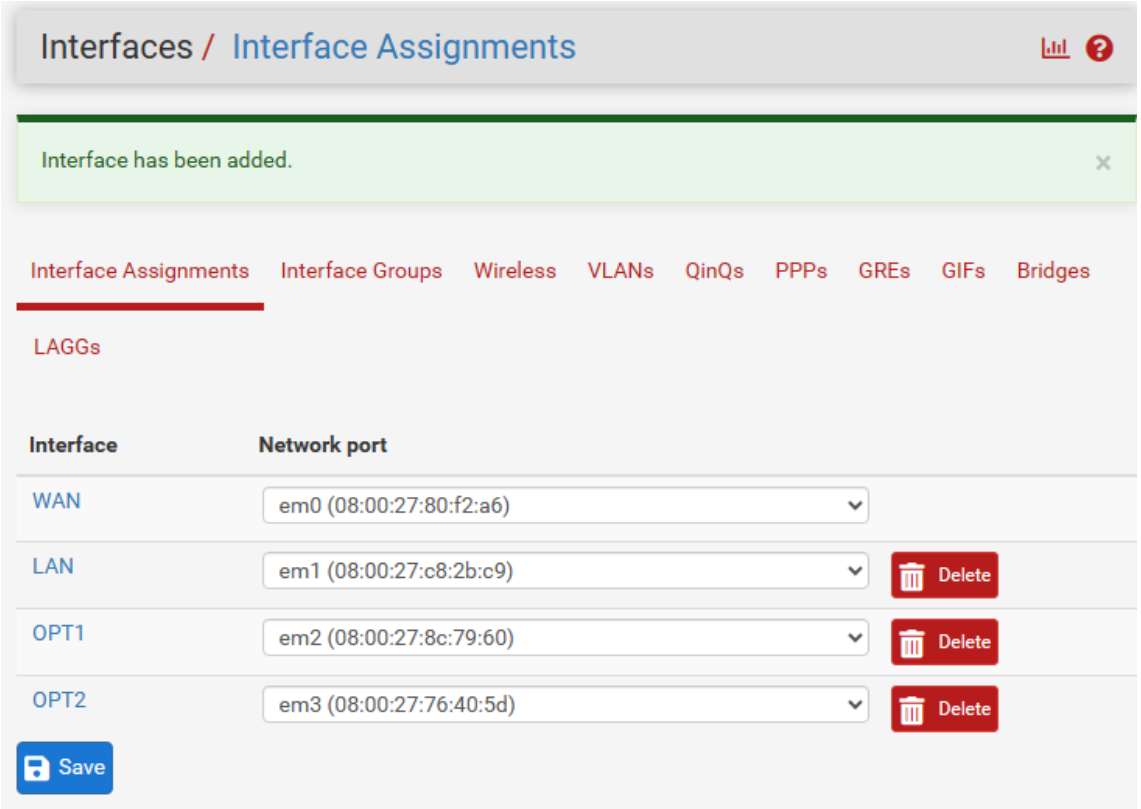
**Other DHCP Options**

| | |
|---|---|
| **Gateway** | 192.168.100.1<br>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. |

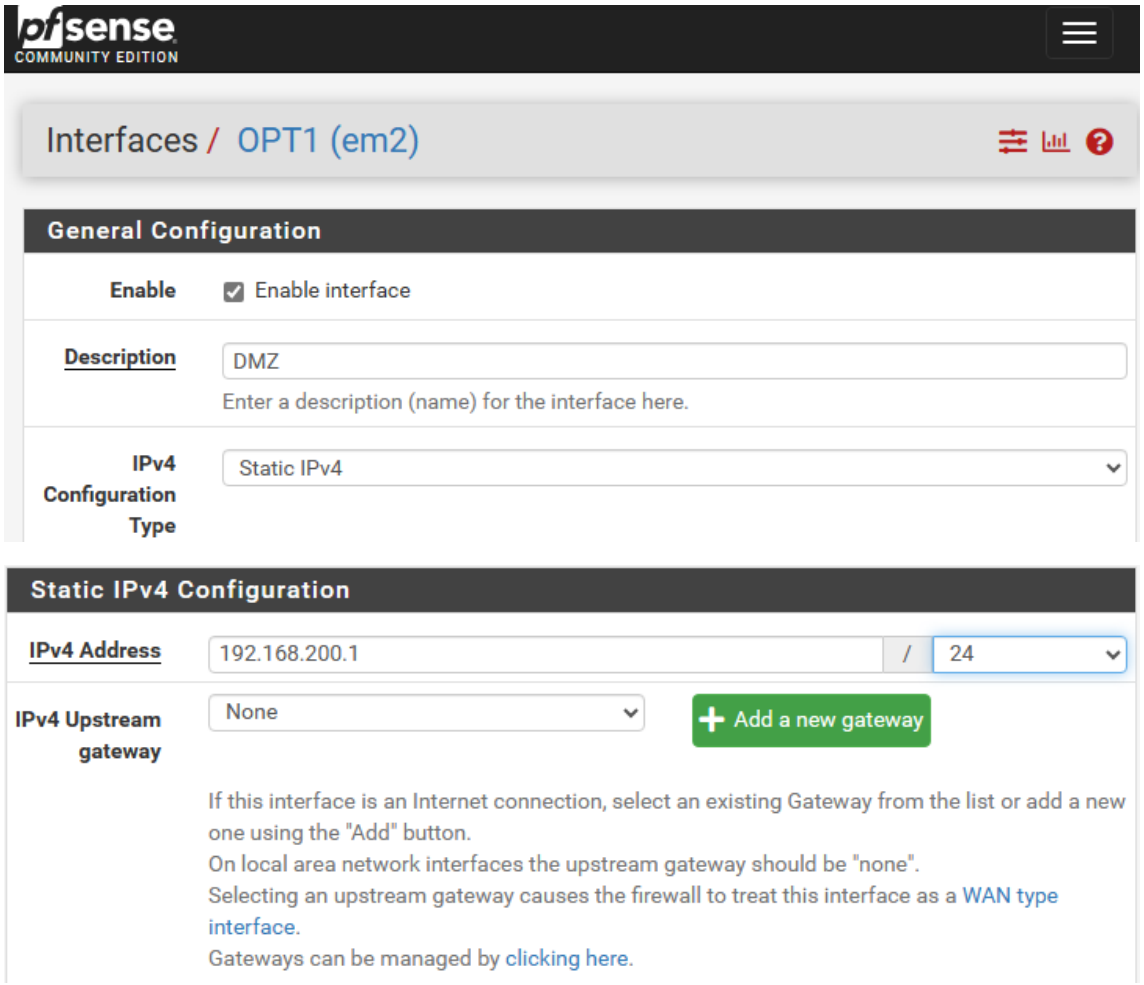
Salvamos y aplicamos cambios

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : practicablueteam.local
   Link-local IPv6 Address . . . . . : fe80::9c35:2928:124d:d2bf%4
   Default Gateway . . . . . . . . . : fe80::a00:27ff:fec8:2bc9%4

C:\Users\User>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : practicablueteam.local
   Link-local IPv6 Address . . . . . : fe80::9c35:2928:124d:d2bf%4
   IPv4 Address. . . . . . . . . . . : 192.168.100.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a00:27ff:fec8:2bc9%4
                                       192.168.100.1
```

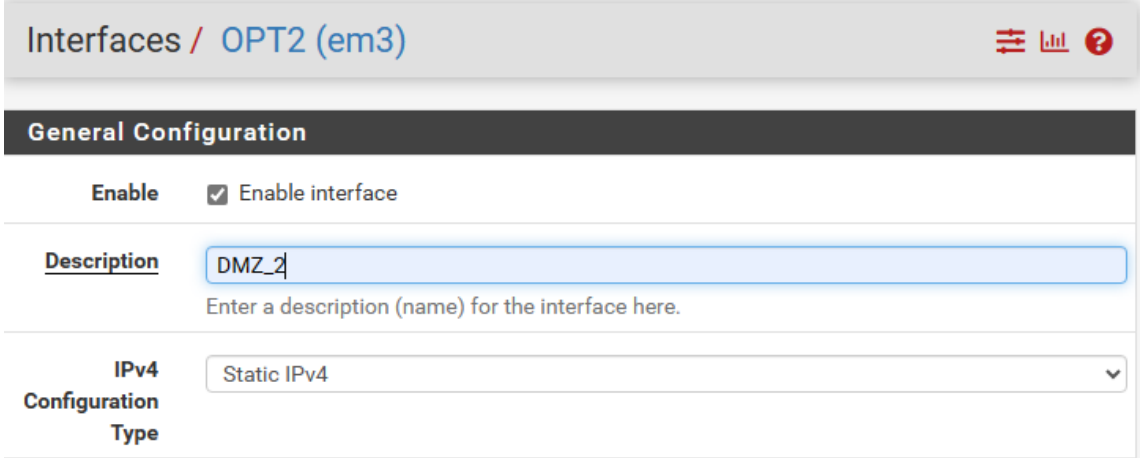
Como anteriormente se crearon 4 adaptadores, dos de ellos ya están configurados pero se necesitan configurar para las subred DMZ (OPT1) y DMZ_2 (OPT2)

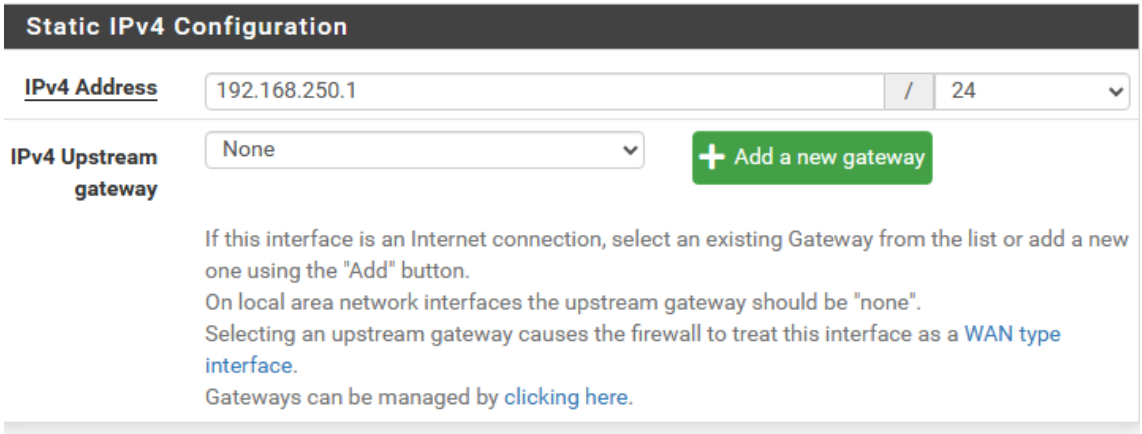


Configuro la interfaz DMZ con la subred 192.168.200.1

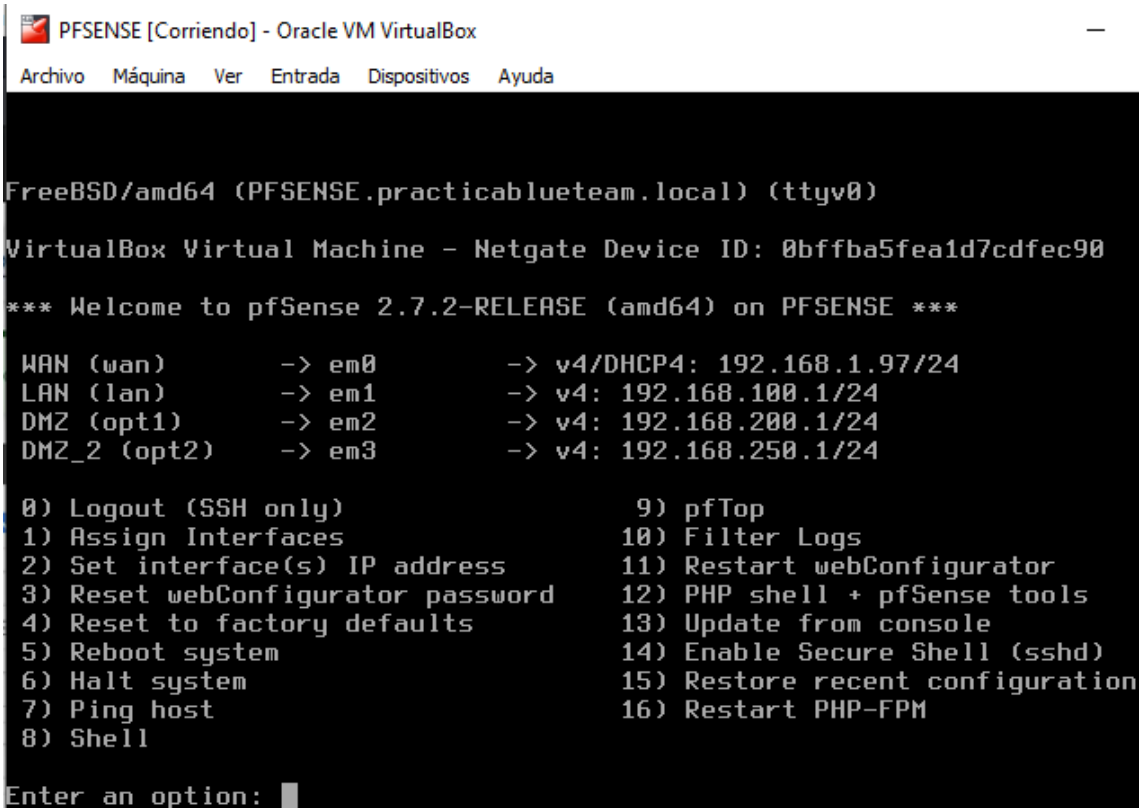



Configuro la interfaz DMZ_2 con la subred 192.168.250.1






Compruebo los cambios en Pfsense



Configuración DHCP server para la red DMZ

Services / DHCP Server / DMZ

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.

LAN DMZ DMZ_2

**General DHCP Options**

| | |
|---|---|
| **DHCP Backend** | ISC DHCP |
| **Enable** | ☐ Enable DHCP server on DMZ interface |

**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)<br>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<br>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<br>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. |

Configuración DHCP server DMZ_2

Services / DHCP Server / DMZ_2

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.

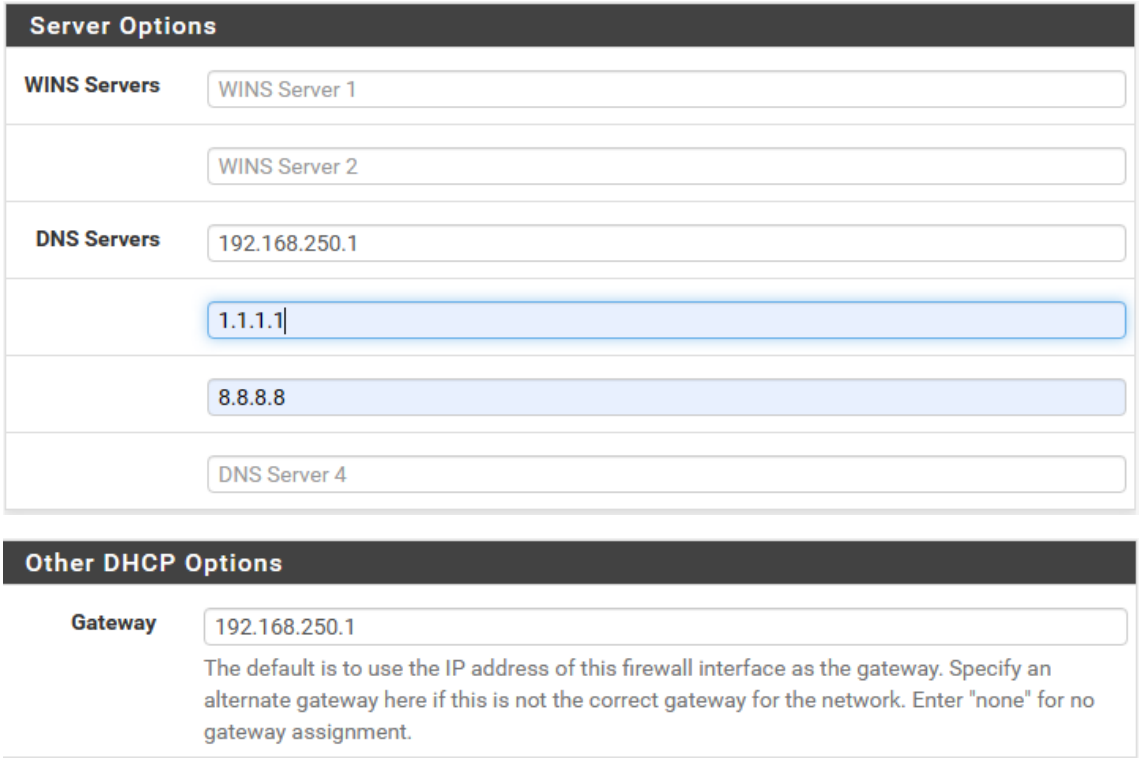
LAN DMZ DMZ_2

**General DHCP Options**

| | |
|---|---|
| **DHCP Backend** | ISC DHCP |
| **Enable** | ☑ Enable DHCP server on DMZ_2 interface |
| **BOOTP** | ☐ Ignore BOOTP queries |

**Primary Address Pool**

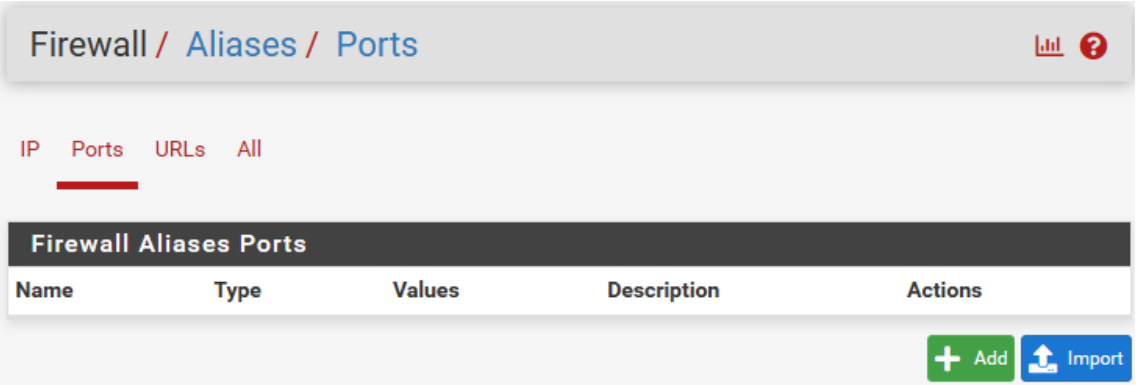
| | |
|---|---|
| **Subnet** | 192.168.250.0/24 |
| **Subnet Range** | 192.168.250.1 - 192.168.250.254 |
| **Address Pool Range** | 192.168.250.100 (From) — 192.168.250.150 (To)<br>The specified range for this pool must not be within the range configured on any other address pool for this interface. |
| **Additional Pools** | + Add Address Pool<br>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here. |



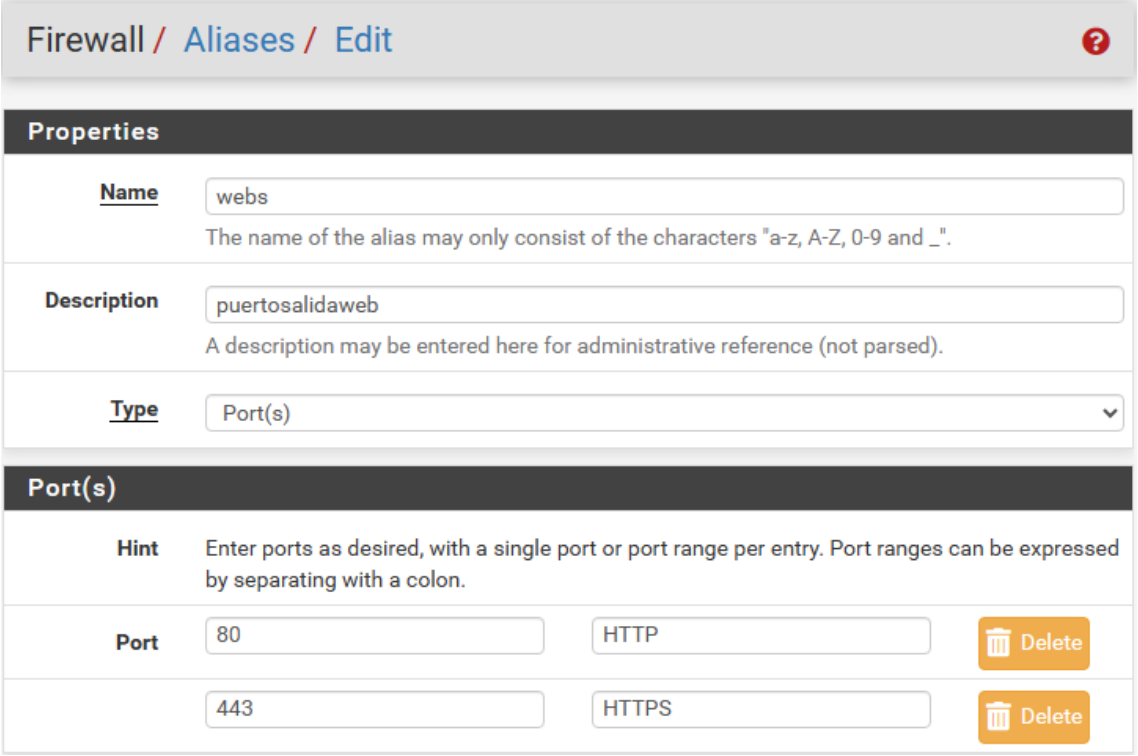

Guardo y aplico cambios

# Configuración del Firewall para los accesos a la red externa

Creando un aliase para la comodidad a la hora de crear después una regla al firewall




Habilito los puertos que dan salida a los protocolos HTTP (80) y HTTPS (443)




Guardo y aplico cambios

# Configuración de las reglas en el firewall

## Configuración firewall para la red WAN

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ_2

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 0/0 B | IPv4 TCP/UDP | * | * | 192.168.250.100 | 80 (HTTP) | * | none | | NAT regla apache server | |

## Configuración firewall para la red LAN

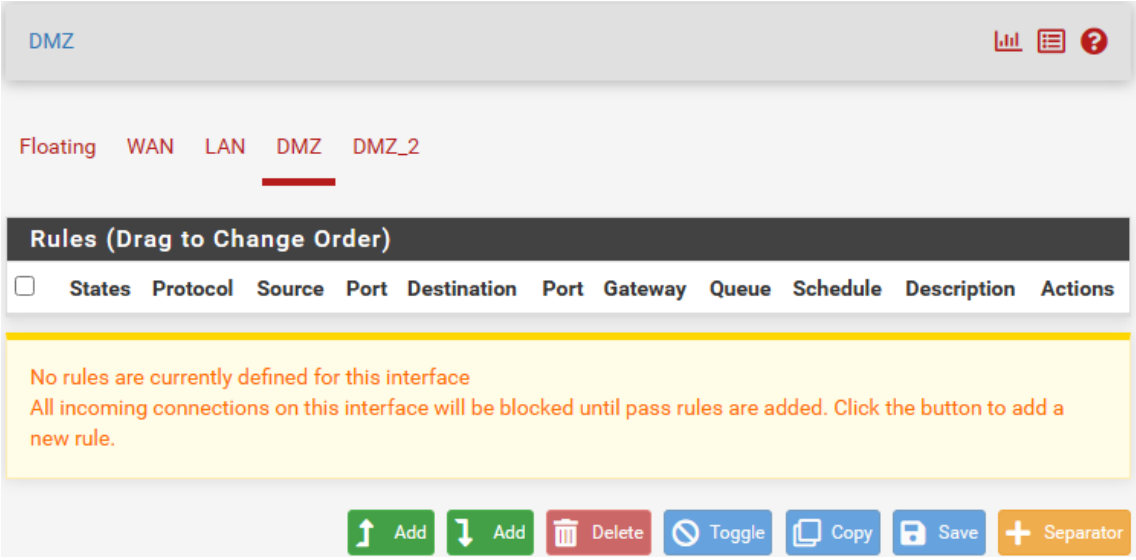
Firewall / Rules / LAN

Floating WAN LAN DMZ DMZ_2

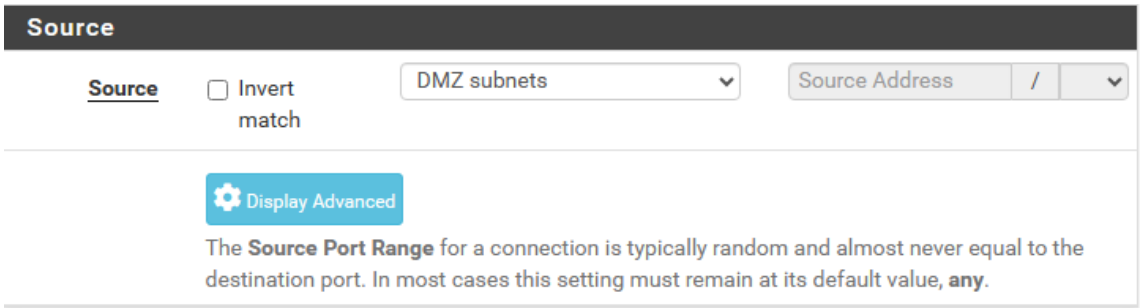
Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 0/2.32 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | |
| ✓ | 0/0 B | IPv4 TCP | LAN subnets | * | DMZ_2 subnets | 22 (SSH) | * | none | | Regla administracion apache_server | |
| ✓ | 0/0 B | IPv4 TCP | LAN subnets | * | DMZ_2 subnets | * | * | none | | comprobacion disponibilidad DMZ_2 | |
| ✓ | 0/0 B | IPv4 TCP | LAN subnets | * | DMZ subnets | * | * | none | | comprobacion disponibilidad DMZ | |
| ✓ | 0/0 B | IPv4 TCP | LAN subnets | * | DMZ subnets | 22 (SSH) | * | none | | Regla administracion honeypot | |
| ✗ | 0/0 B | IPv4 TCP | DMZ_2 subnets | * | * | * | * | none | | bloqueo subnet DMZ_2 | |
| ✗ | 0/0 B | IPv4 TCP | DMZ subnets | * | * | * | * | none | | bloqueo subnet DMZ | |
| ✓ | 69/479 KiB | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | |
| ✓ | 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | |

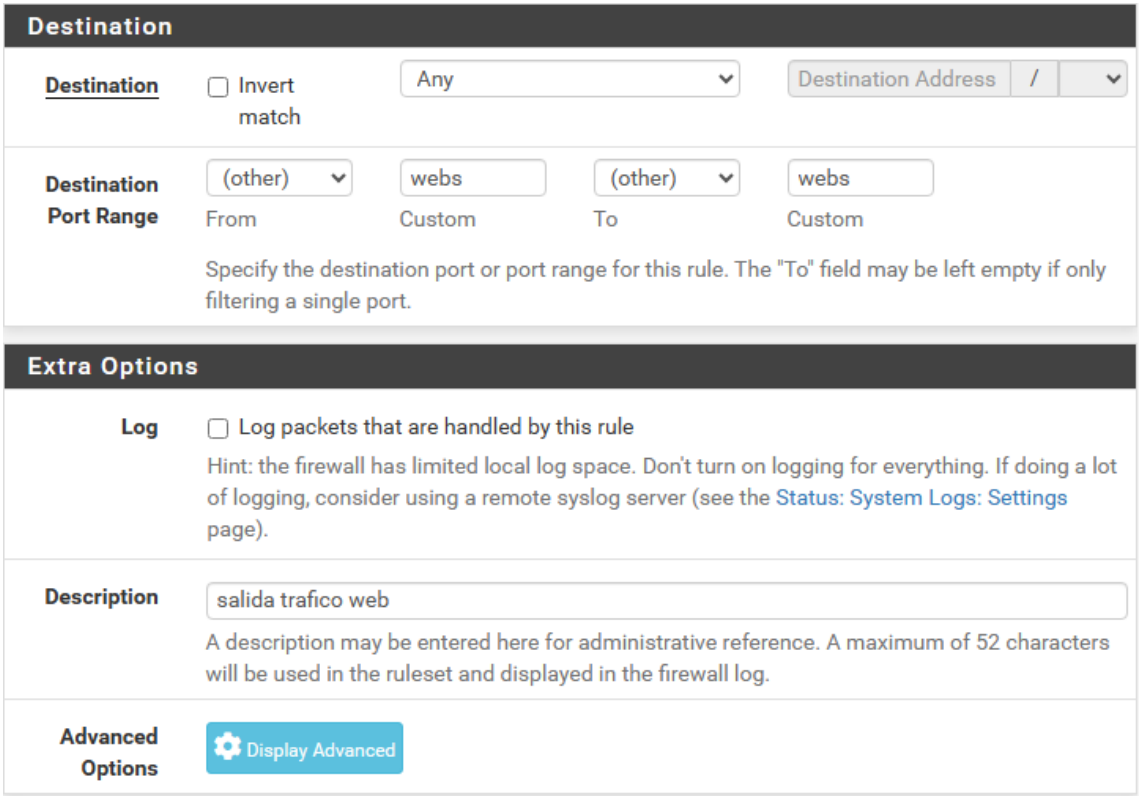
## Configuración firewall para la red DMZ




Por seguridad se configura que la regla en DMZ subnets para que solo las subredes que pertenecen a la DMZ tengan acceso




Configuro el rango de puertos que es denominado como “webs” (creado anteriormente en aliases)




Guardar y aplicar cambios

Con esto estará establecido la salida para el trafico web pero no nos va a resolver los nombres de dominio por tanto, creo la regla para el protocolo DNS (puerto 53)

Firewall / Rules / Edit

**Edit Firewall Rule**

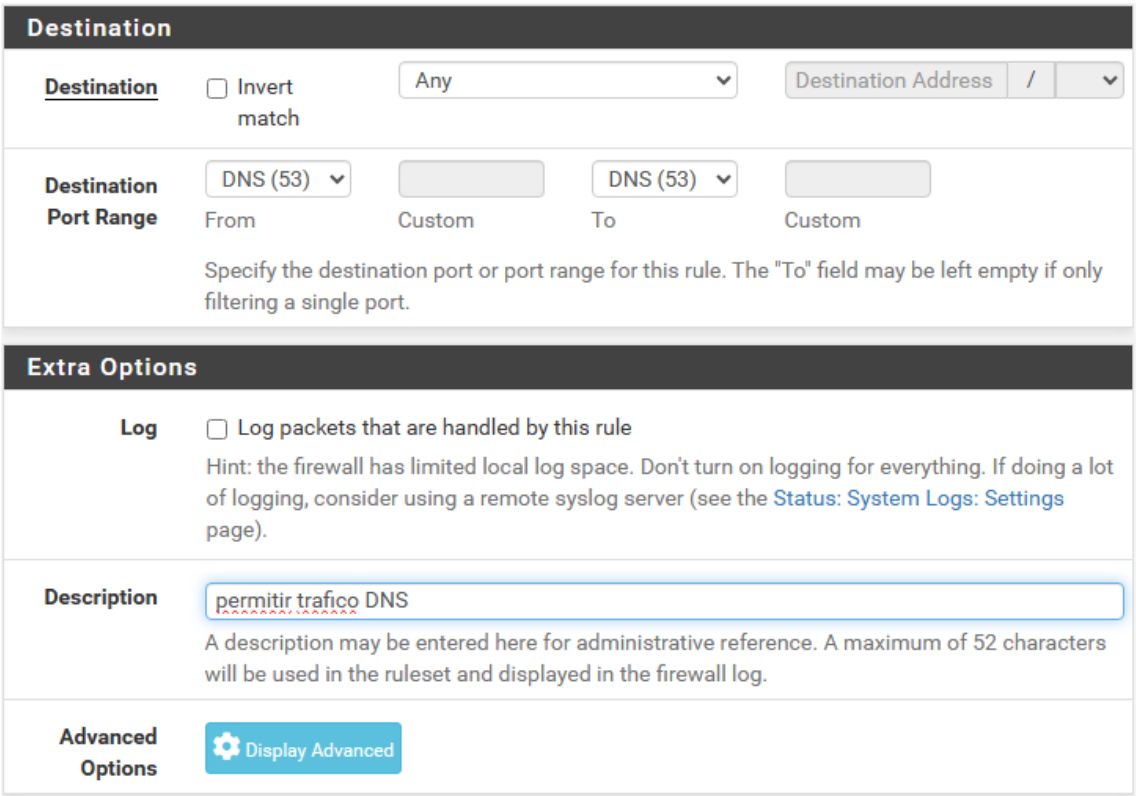
| | |
|---|---|
| **Action** | Pass<br>Choose what to do with packets that match the criteria specified below.<br>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. |
| **Disabled** | ☐ Disable this rule<br>Set this option to disable this rule without removing it from the list. |
| **Interface** | DMZ<br>Choose the interface from which packets must come to match this rule. |
| **Address Family** | IPv4<br>Select the Internet Protocol version this rule applies to. |
| **Protocol** | UDP<br>Choose which IP protocol this rule should match. |

**Source**

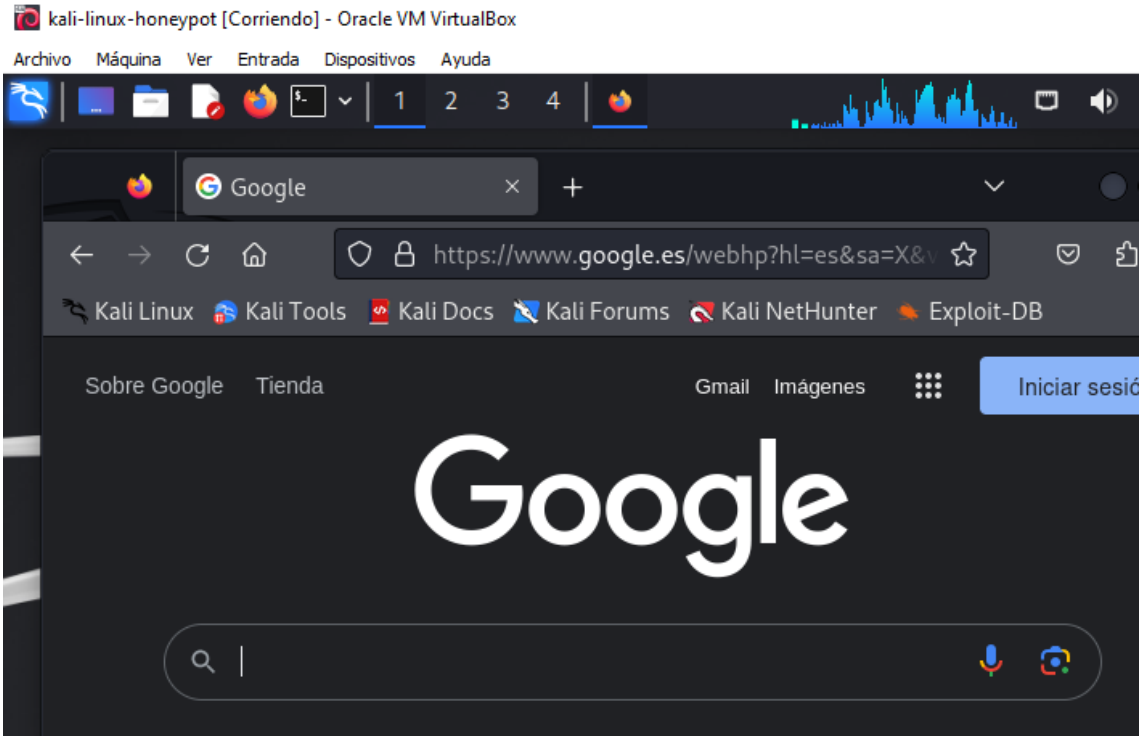
| | | | |
|---|---|---|---|
| **Source** | ☐ Invert match | DMZ subnets | Source Address / |

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.




Compruebo que tiene acceso al exterior



## Configuración regla firewall para evitar que la DMZ tenga acceso a otras subredes

Para bloquear el acceso a la red LAN

**Edit Firewall Rule**

**Action** Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface** DMZ

Choose the interface from which packets must come to match this rule.

**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** Any

Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match | DMZ subnets | Source Address | /

**Destination**

**Destination** ☐ Invert match | LAN subnets | Destination Address | /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description** bloqueo para subnet LAN

Para bloquear el acceso a la red DMZ_2

## Edit Firewall Rule

**Action**: Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**: ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**: DMZ

Choose the interface from which packets must come to match this rule.

**Address Family**: IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**: Any

Choose which IP protocol this rule should match.

## Source

**Source**: ☐ Invert match | DMZ subnets | Source Address | /

## Destination

**Destination**: ☐ Invert match | DMZ_2 subnets | Destination Address | /

## Extra Options

**Log**: ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**: bloqueo para subnet DMZ_2

**Visión global de cómo queda la regla para la DMZ**

Firewall / Rules / DMZ

Floating WAN LAN DMZ DMZ_2

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✗ | 0/0 B | IPv4 * | DMZ subnets | * | LAN subnets | * | * | none | | bloqueo para subnet LAN | |
| ✗ | 0/0 B | IPv4 * | DMZ subnets | * | DMZ_2 subnets | * | * | none | | bloqueo para subnet DMZ_2 | |
| ✓ | 0/0 B | IPv4 ICMP any | * | * | * | * | * | none | | ping | |
| ✓ | 0/0 B | IPv4 UDP | DMZ subnets | * | * | 53 (DNS) | * | none | | permitir trafico DNS | |
| ✓ | 0/0 B | IPv4 TCP | DMZ subnets | * | * | webs | * | none | | salida trafico web | |

Añado la regla de ping para comprobar si tiene acceso a las otras subredes

Compruebo para puerta enlace y subred LAN, no tiene acceso

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2076ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
^C
--- 192.168.100.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1032ms
```

Compruebo para puerta enlace y subred DMZ_2, no tiene acceso

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.250.1
PING 192.168.250.1 (192.168.250.1) 56(84) bytes of data.
^C
--- 192.168.250.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1027ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.250.100
PING 192.168.250.100 (192.168.250.100) 56(84) bytes of data.
^C
--- 192.168.250.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2039ms
```

## Configuración firewall para la red DMZ_2

**Edit Firewall Rule**

**Action** — Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** — ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface** — DMZ_2

Choose the interface from which packets must come to match this rule.

**Address Family** — IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** — TCP

Choose which IP protocol this rule should match.

**Source**

**Source** — ☐ Invert match | DMZ_2 subnets | Source Address | /

**Destination**

**Destination** — ☐ Invert match | Any | Destination Address | /

**Destination Port Range** — (other) From | webs Custom | (other) To | webs Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log** — ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description** — salida trafico web

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Guardo y aplico cambios

Al igual que hice para la DMZ voy a permitir la resolución de nombres para el protoco DNS (puerto 53) en la red DMZ_2

**Edit Firewall Rule**

**Action** Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface** DMZ_2

Choose the interface from which packets must come to match this rule.

**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** UDP

Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match | DMZ_2 subnets | Source Address | /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination** ☐ Invert match | Any | Destination Address | /

**Destination Port Range** DNS (53) From | Custom | DNS (53) To | Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

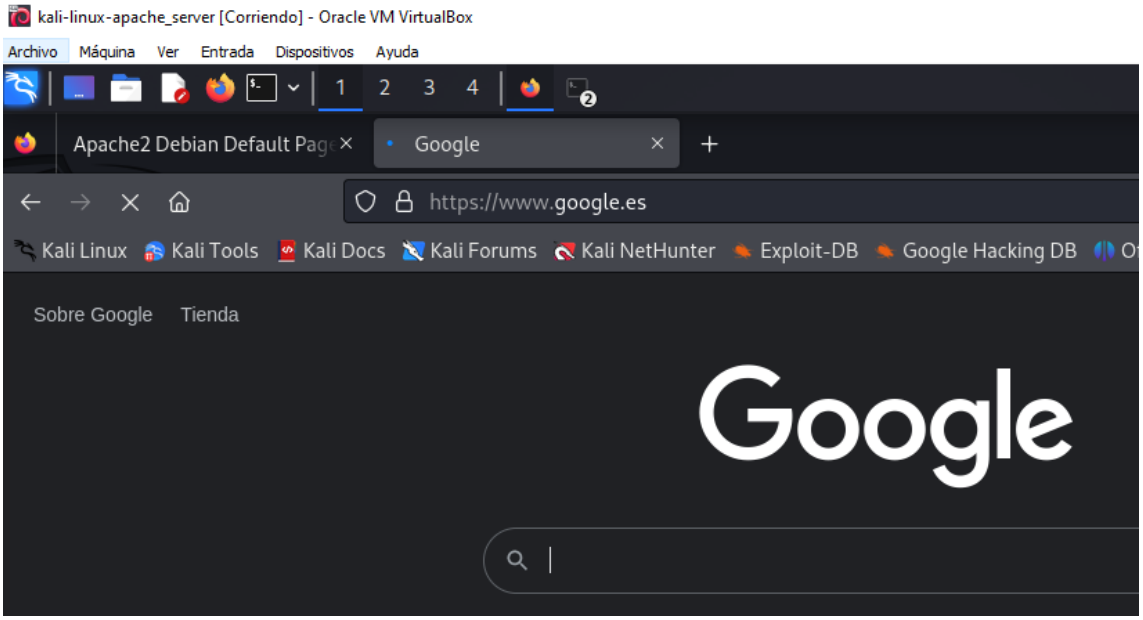
**Log** ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

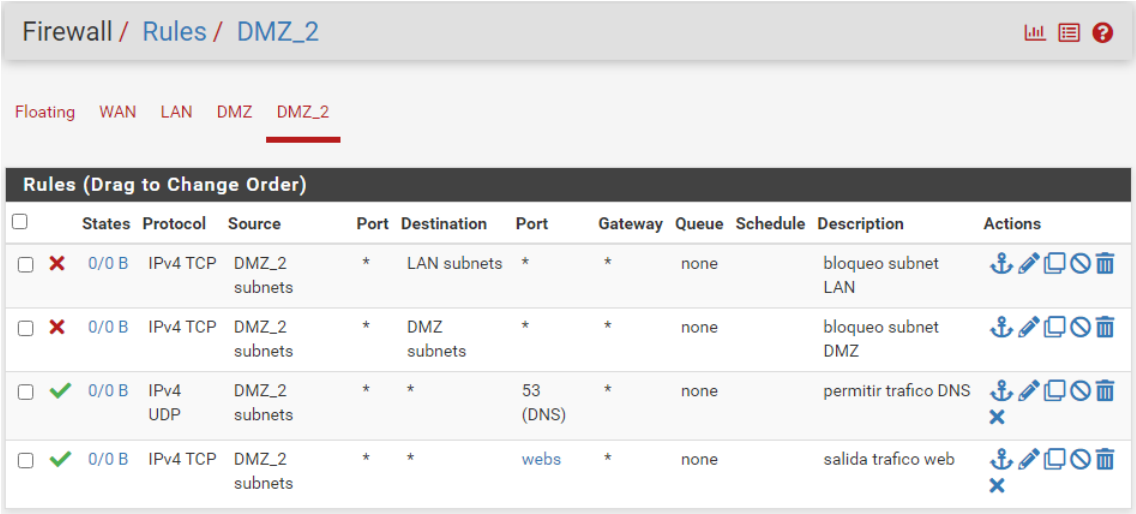
**Description** permitir trafico DNS

Guardo y aplico cambios

Compruebo que tenga salida y trafico web




**Visión global de cómo queda la regla para la DMZ_2**



Firewall / Rules / DMZ_2

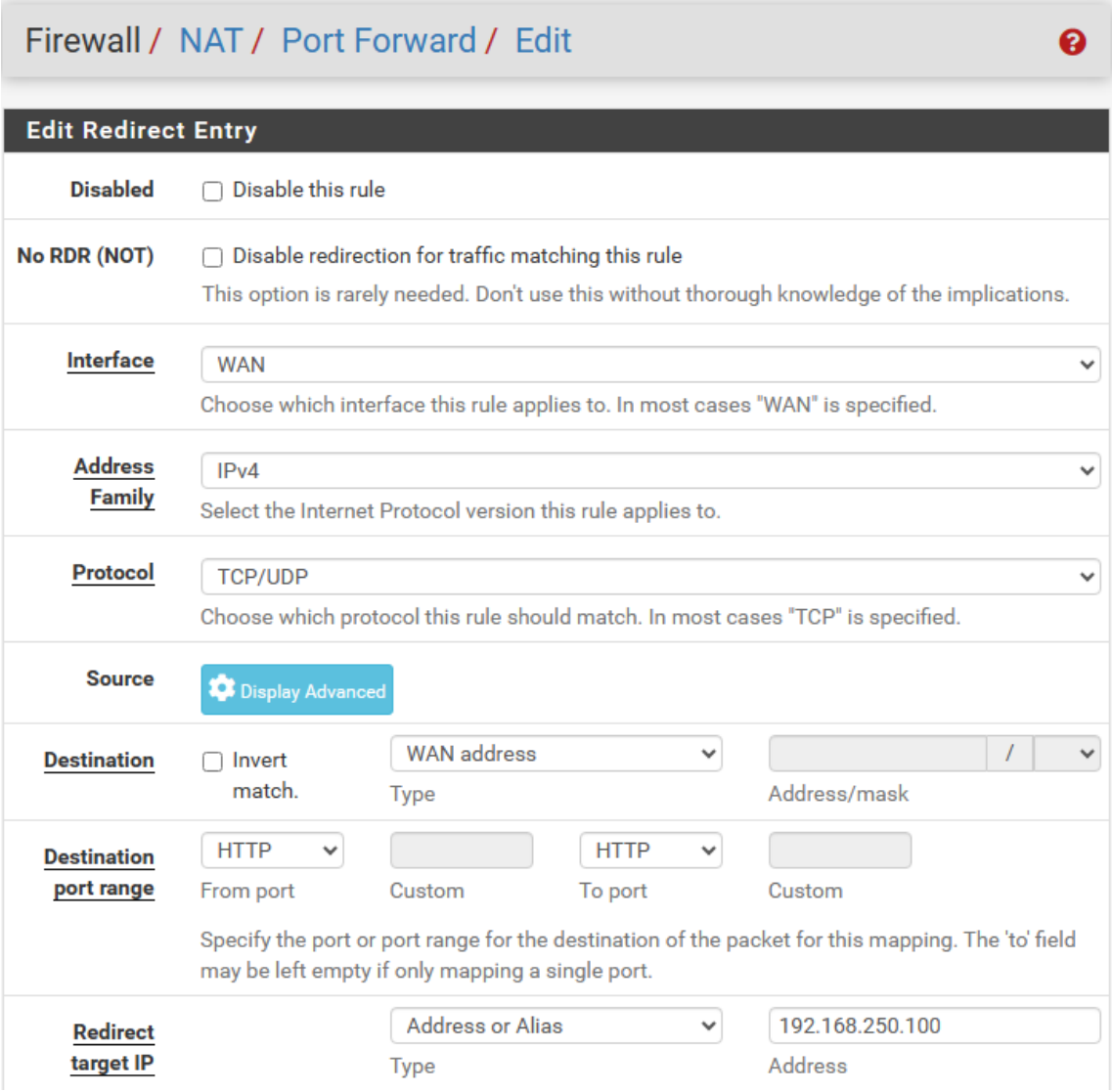
Floating WAN LAN DMZ DMZ_2

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✗ | 0/0 B | IPv4 TCP | DMZ_2 subnets | * | LAN subnets | * | * | none | | bloqueo subnet LAN | |
| ✗ | 0/0 B | IPv4 TCP | DMZ_2 subnets | * | DMZ subnets | * | * | none | | bloqueo subnet DMZ | |
| ✓ | 0/0 B | IPv4 UDP | DMZ_2 subnets | * | * | 53 (DNS) | * | none | | permitir trafico DNS | |
| ✓ | 0/0 B | IPv4 TCP | DMZ_2 subnets | * | * | webs | * | none | | salida trafico web | |

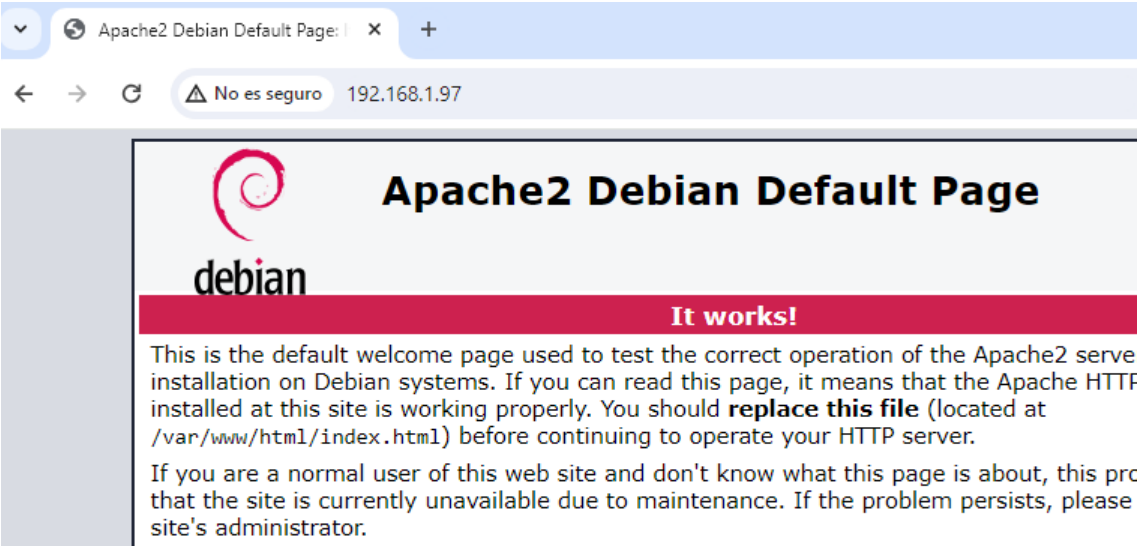
# Configuración NAT

Configuración para DMZ_2 servidor apache




192.168.250.100 es donde se encuentra el servidor apache

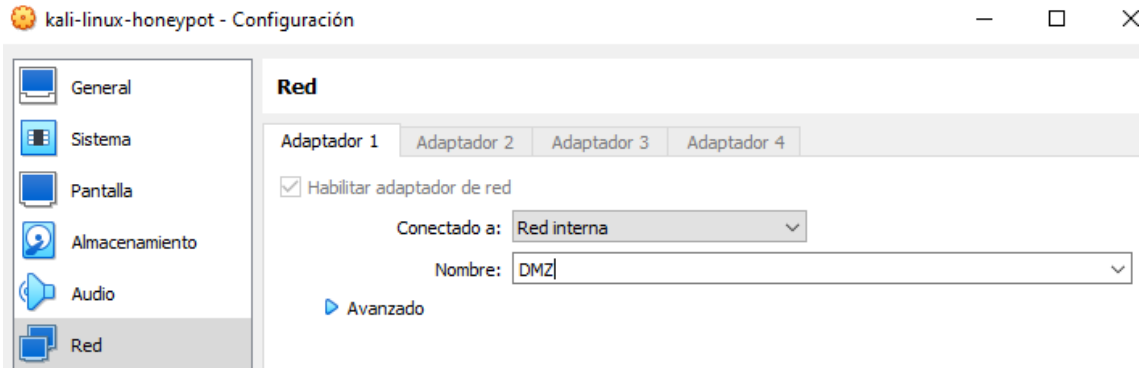
Compruebo que se tiene acceso desde fuera



# Configuración de un honeypot en la red DMZ

La finalidad del honeypot es conseguir despistar al atacante y hacer que pierda el tiempo creyendo que está en un equipo perteneciente a la empresa con datos sensibles.

* La finalidad del honeypot es recopilar información sobre las tendencias de ataques que están ocurriendo e información sobre posibles amenazas dentro de nuestra red. Como objetivo secundario puedes hacer que el atacante se entretenga pensando que es una máquina de la que puede obtener algún beneficio, pero eso es algo secundario.




Compruebo que la Kali que quiero utilizar como honeypot esta en la red es la correcta

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.100  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::25bf:7849:de60:ae6e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 272587  bytes 290592678 (277.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117362  bytes 24554446 (23.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

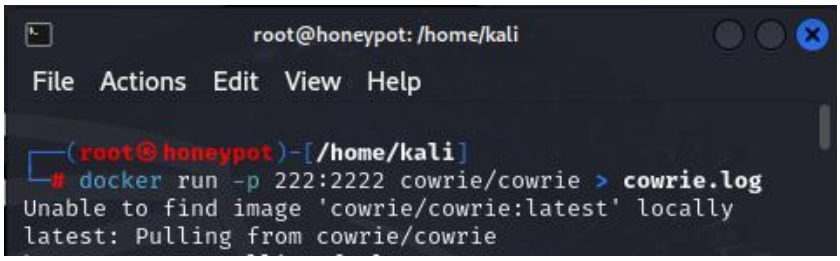
**Instalación del honeypot**

Se usa Docker, no está instalado por defecto, por tanto se instala

```
sudo apt install -y docker.io
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y docker.io
```

```
sudo docker run -p 2222:2222 cowrie/cowrie > cowrie.log
```




Es un servidor SSH el cual puedan entrar y nosotros podremos ver que movimientos y comandos realiza el atacante

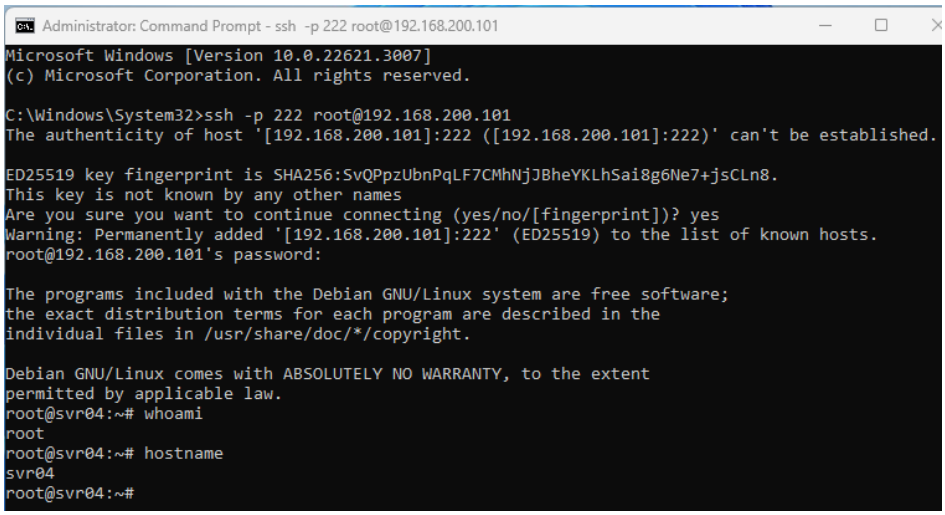
Los logs los genera en:

```
/home/kali/cowrie.log
```

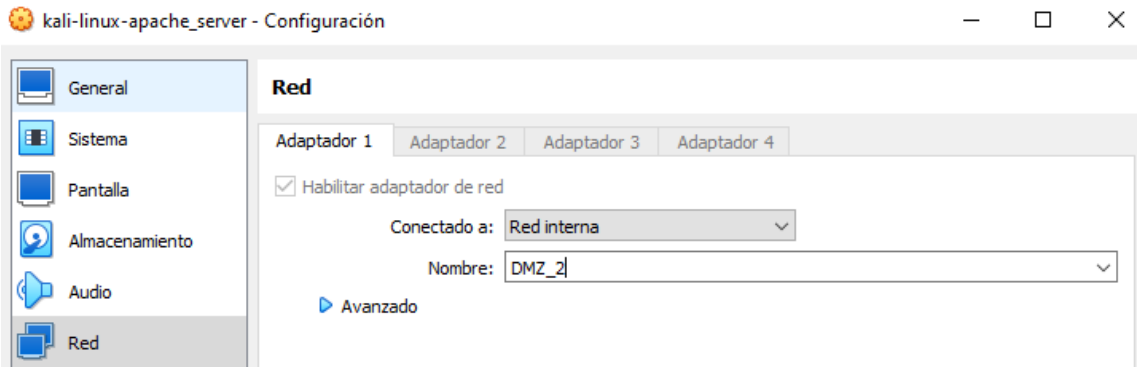
**Tendremos en cuenta esta ruta de logs para más adelante integrarlo en elastic (ver pag. 48 )**

Nos conectamos desde otra maquina (W11) por SSH para comprobarlo

```
ssh -p 222 root@192.168.200.101
```



# Configuración de Apache web server en DMZ_2



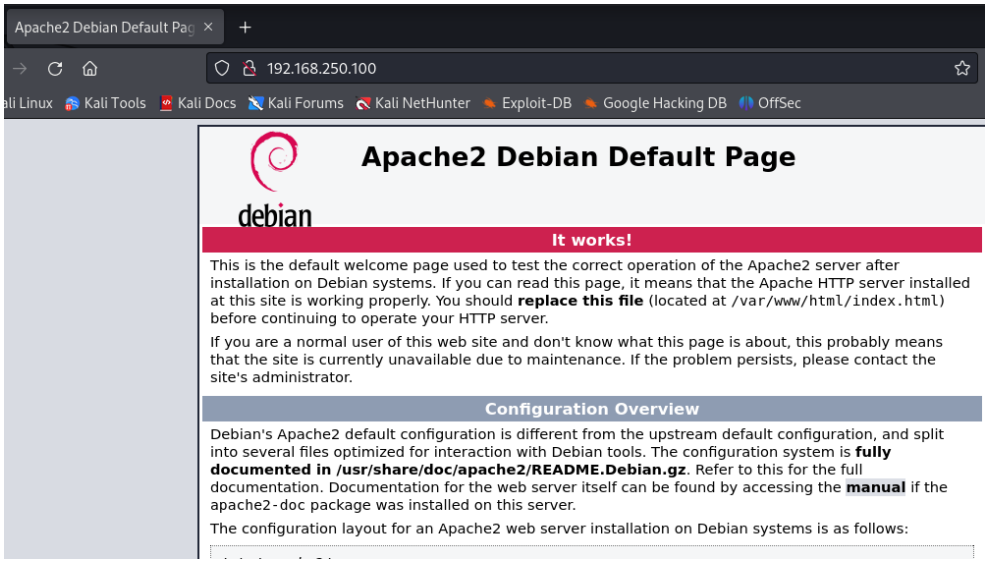

Compruebo que la maquina se encuentre en la red correcta

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.250.100  netmask 255.255.255.0  broadcast 192.168.250.255
        inet6 fe80::25bf:7849:de60:ae6e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 272587  bytes 290592678 (277.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117283  bytes 24536043 (23.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Inicio el servicio de apache

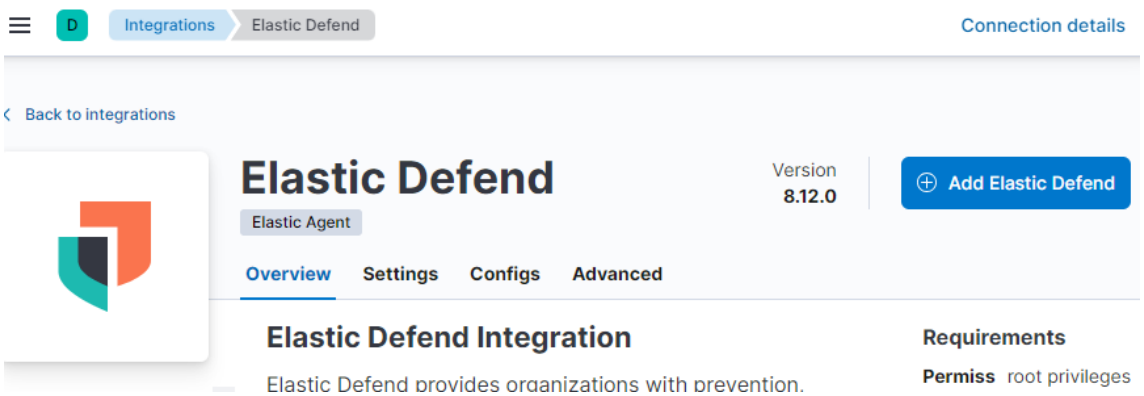
```
service apache2 start
```

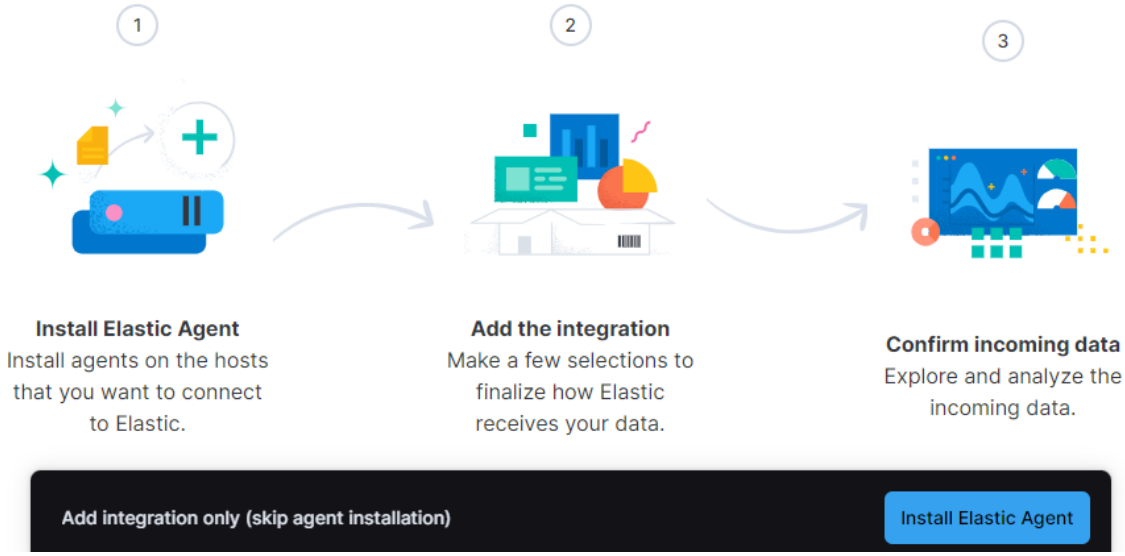
```
┌──(kali㉿kali)-[~]
└─$ service apache2 start
```



# Configuración de elastic cloud


Me registro en https://www.elastic.co/es/cloud y añado Elastic defend



# Instalación del agente en Windows 11 para integrar en Elastic

## 1 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

Linux Tar | Mac | **Windows** | RPM | DEB | Kubernetes

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic
Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.12.2-windows-x86_64
.\elastic-agent.exe install --url=https://9257bce4db4c4dae890eca50cdabd24c.fleet.us-centr
```

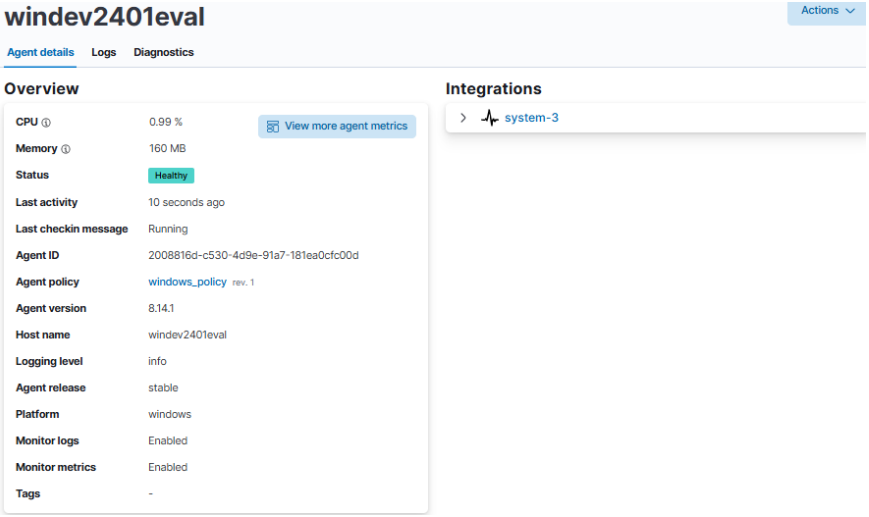
Copy to clipboard

Ejecutamos powershell como administrador y instalamos el agente

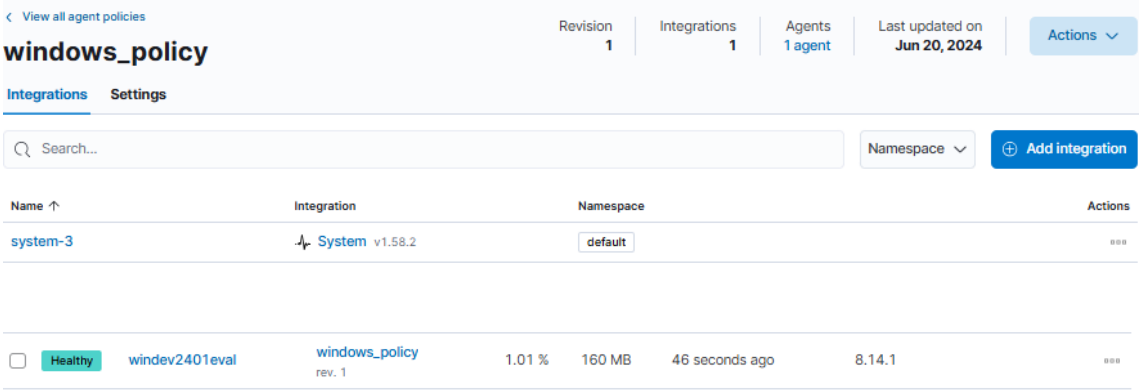
Administrator: Windows PowerShell

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agen
t/elastic-agent-8.12.2-windows-x86_64.zip -OutFile elastic-agent-8.12.2-windows-x86_64.zip
PS C:\Windows\system32> Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .
PS C:\Windows\system32> cd elastic-agent-8.12.2-windows-x86_64
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64> .\elastic-agent.exe install --url=https://92
57bce4db4c4dae890eca50cdabd24c.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=WWdzck00NEJKSWZO
YkxPRFJBWkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
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  [19s] Elastic Agent successfully installed, starting enrollment.
[  ==] Waiting For Enroll...  [20s] {"log.level":"info","@timestamp":"2024-03-16T16:54:42.963-0700","log
.origin":{"file.name":"cmd/enroll_cmd.go","file.line":496},"message":"Starting enrollment to URL: https:
//9257bce4db4c4dae890eca50cdabd24c.fleet.us-central1.gcp.cloud.es.io:443/","ecs.version":"1.6.0"}
[    ] Waiting For Enroll...  [37s] {"log.level":"info","@timestamp":"2024-03-16T16:55:00.300-0700","log
.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0
","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-03-16T16:55:00.304-0700","log.origin":{"file.name":"cmd/enroll_cm
d.go","file.line":285},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version
":"1.6.0"}
Successfully enrolled the Elastic Agent.
[    ] Done  [37s]
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64>
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64>
```

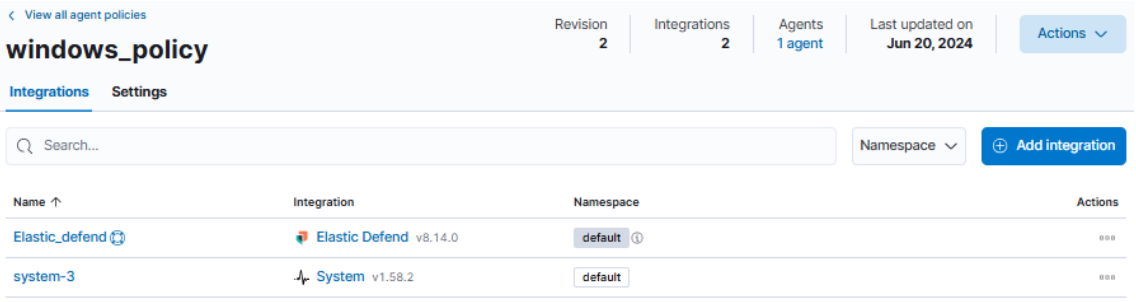
# Integración de logs de Windows 11 en Elastic




Se crea una politica




La configuración por defecto recoge información del sistema, también añadimos Elastic defend



# Instalación del agente en el honeypot para integrar en elastic

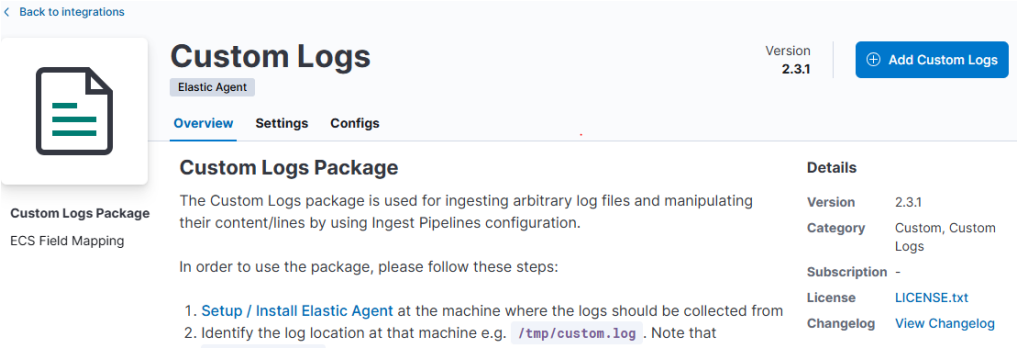
Linux Tar | Mac | Windows | RPM | DEB | Kubernetes

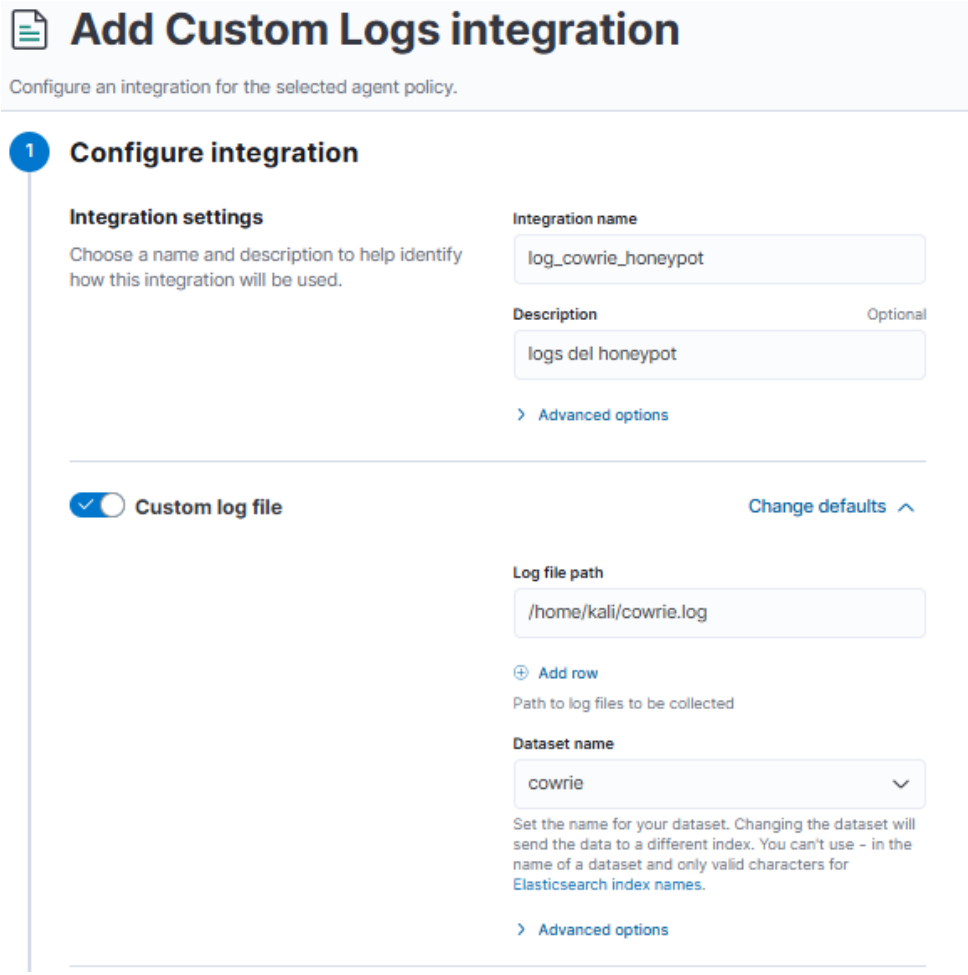
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://9257bce4db4c4dae890eca50cdabd24c.fleet.us-cent
```

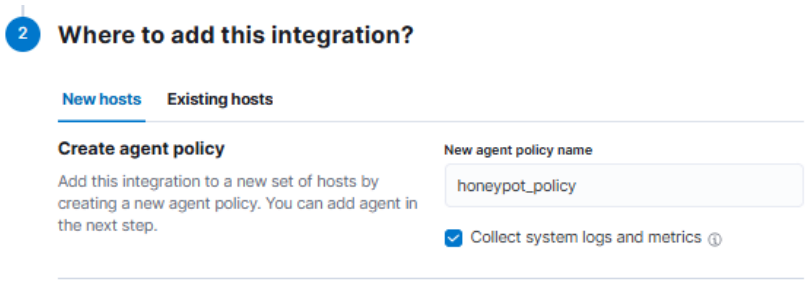
```
kali@honeypot: ~/elastic-agent-8.14.1-linux-x86_64
File  Actions  Edit  View  Help

┌──(kali㉿honeypot)-[~]
└─$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.
14.1-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.14.1-linux-x86_64.tar.gz
cd elastic-agent-8.14.1-linux-x86_64
sudo ./elastic-agent install --url=https://35159e9bf72245b282b7e9585abf5b37.fleet.us-centr
al1.gcp.cloud.es.io:443 --enrollment-token=RHZXdU5wQUJ0OUhvN0dJY28xZTQ6OHh6VjZIZzZUZ0dfbmN
BUk81czFRdw==
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  321M  100  321M    0     0  16.0M      0  0:00:19  0:00:19 --:--:-- 15.5M
elastic-agent-8.14.1-linux-x86_64/elastic-agent.yml
elastic-agent-8.14.1-linux-x86_64/LICENSE.txt
```

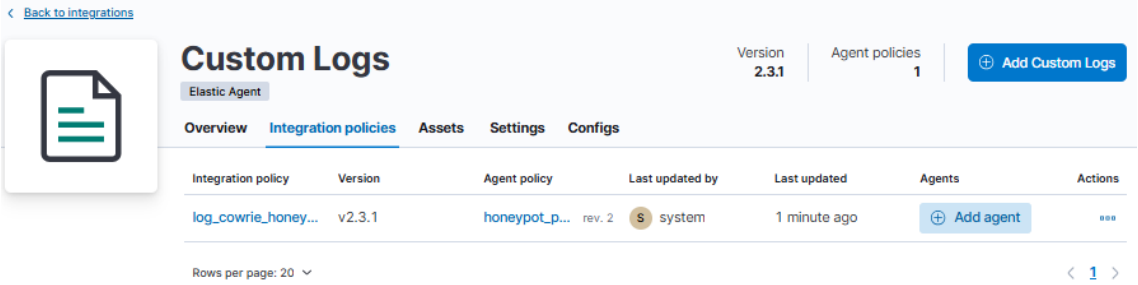
```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you wa
nt to continue? [Y/n]:Y
[   =] Service Started  [6s] Elastic Agent successfully installed, starting enrollment.
[   =] Waiting For Enroll...  [7s] {"log.level":"info","@timestamp":"2024-06-20T15:01:14.3
56-0400","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":517},"message":"Startin
g enrollment to URL: https://35159e9bf72245b282b7e9585abf5b37.fleet.us-central1.gcp.cloud.
es.io:443/","ecs.version":"1.6.0"}
[=== ] Waiting For Enroll...  [9s] {"log.level":"info","@timestamp":"2024-06-20T15:01:16.1
85-0400","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":480},"message":"Restart
ing agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-06-20T15:01:16.202-0400","log.origin":{"file.name":
"cmd/enroll_cmd.go","file.line":298},"message":"Successfully triggered restart on running
Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=== ] Done  [9s]
Elastic Agent has been successfully installed.

┌──(kali㉿honeypot)-[~/elastic-agent-8.14.1-linux-x86_64]
└─$ 
```

# Integración de logs del honeypot en Elastic

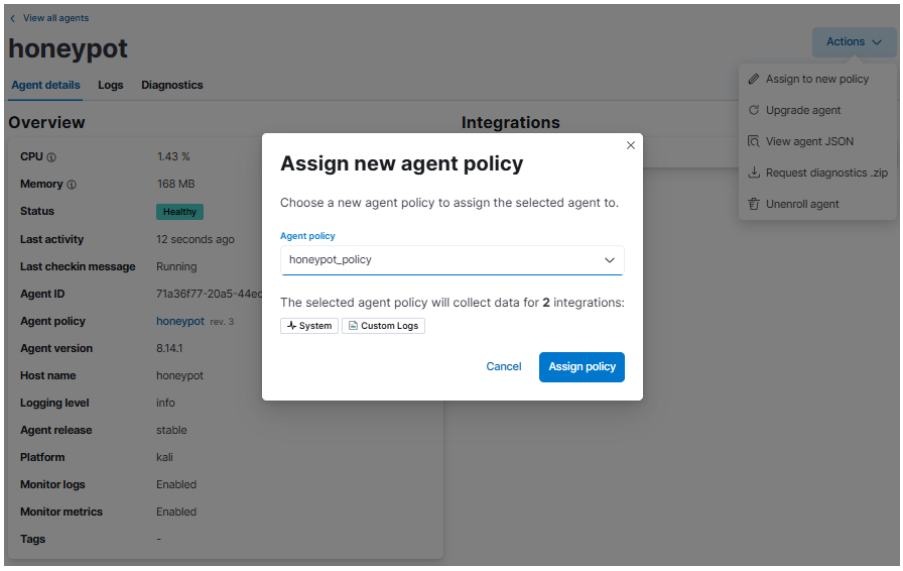


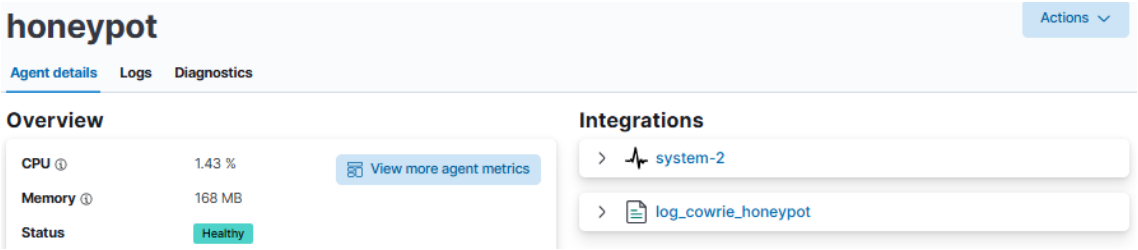



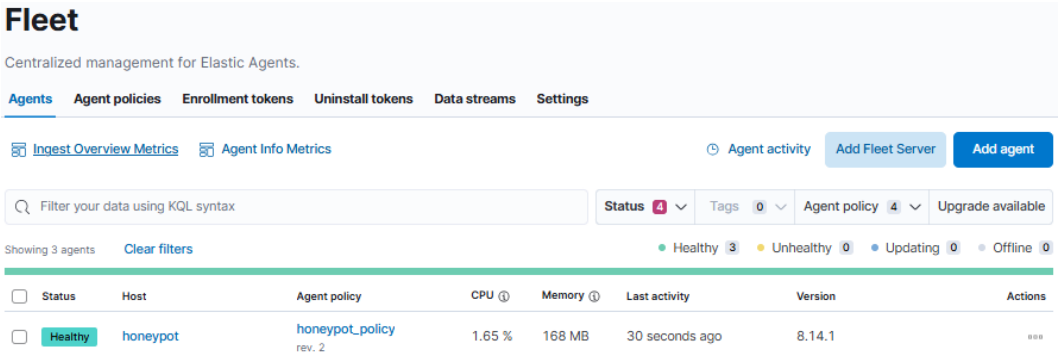






Asignamos al agente (honeypot) en agent policy la política de honeypot que se ha creado



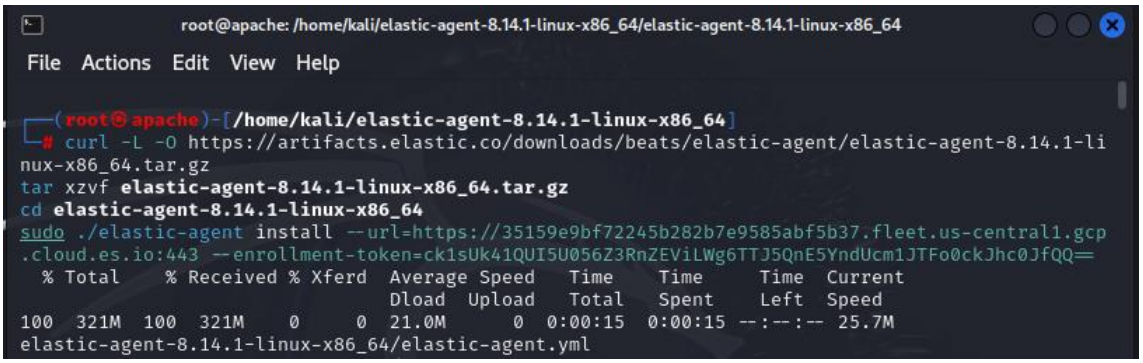



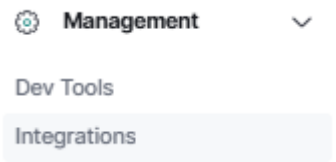
# Instalación del agente de apache server en Elastic

Ponemos en un terminal el código para instalar el agente con el token que nos genera:

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.1-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.14.1-linux-x86_64.tar.gz
cd elastic-agent-8.14.1-linux-x86_64
sudo ./elastic-agent install --url=https://35159e9bf72245b282b7e9585abf5b37.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=ck1sUk41QUI5U056Z3RnZEViLWg6TTJ5QnE5YndUcm1JTFo0ckJhc0JfQQ==
```

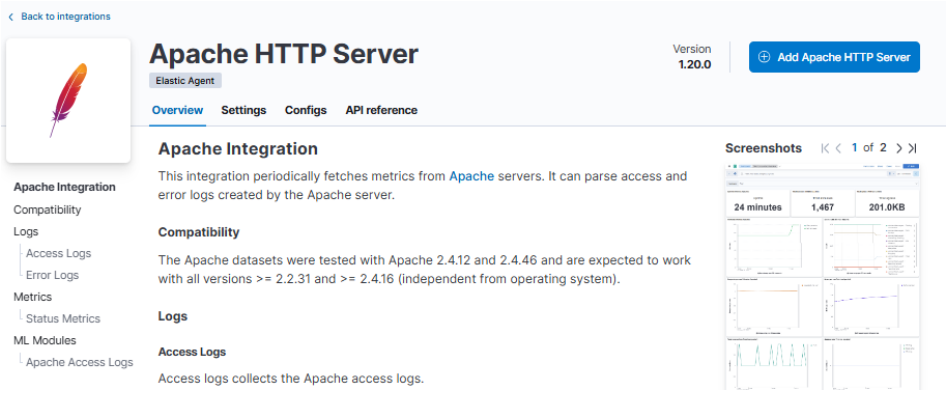


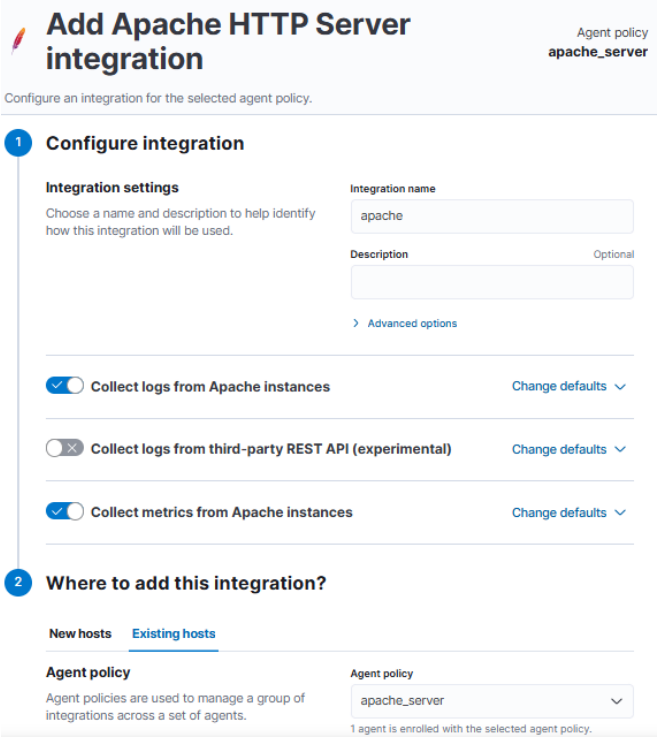
# Integración de logs de apache server en Elastic

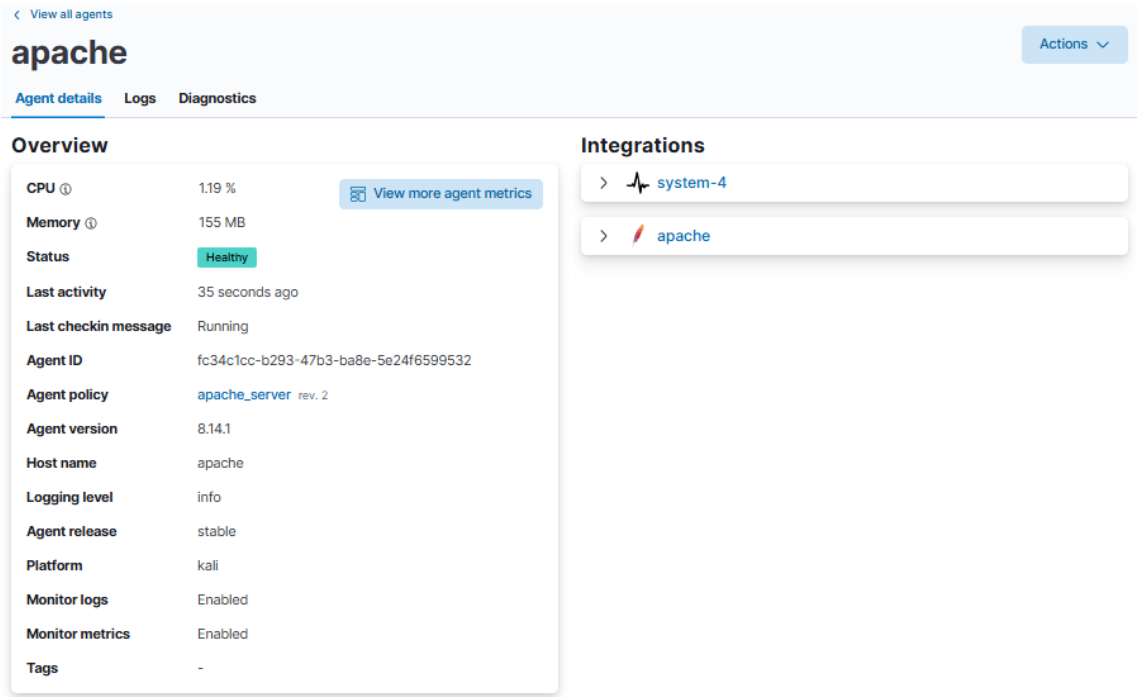



En Management – **Integrations**

Buscamos y añadimos el Apache HTTP Server

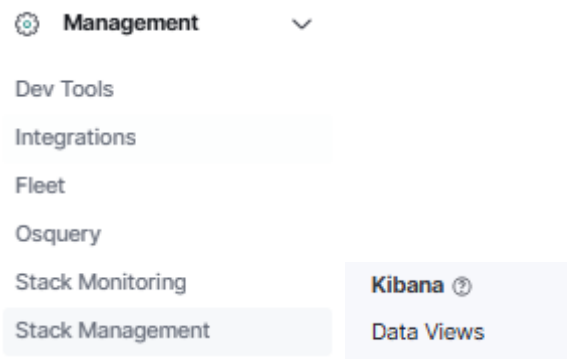


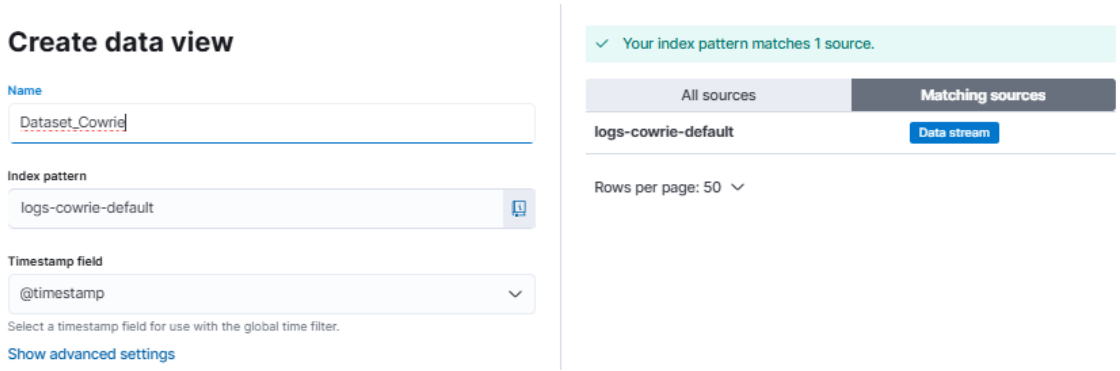


View all agents
apache
Actions
Agent details
Logs
Diagnostics
Overview
CPU
1.19 %
View more agent metrics
Memory
155 MB
Status
Healthy
Last activity
35 seconds ago
Last checkin message
Running
Agent ID
fc34c1cc-b293-47b3-ba8e-5e24f6599532
Agent policy
apache_server rev. 2
Agent version
8.14.1
Host name
apache
Logging level
info
Agent release
stable
Platform
kali
Monitor logs
Enabled
Monitor metrics
Enabled
Tags
-
Integrations
system-4
apache

# Revisión de logs

## Para el honeypot

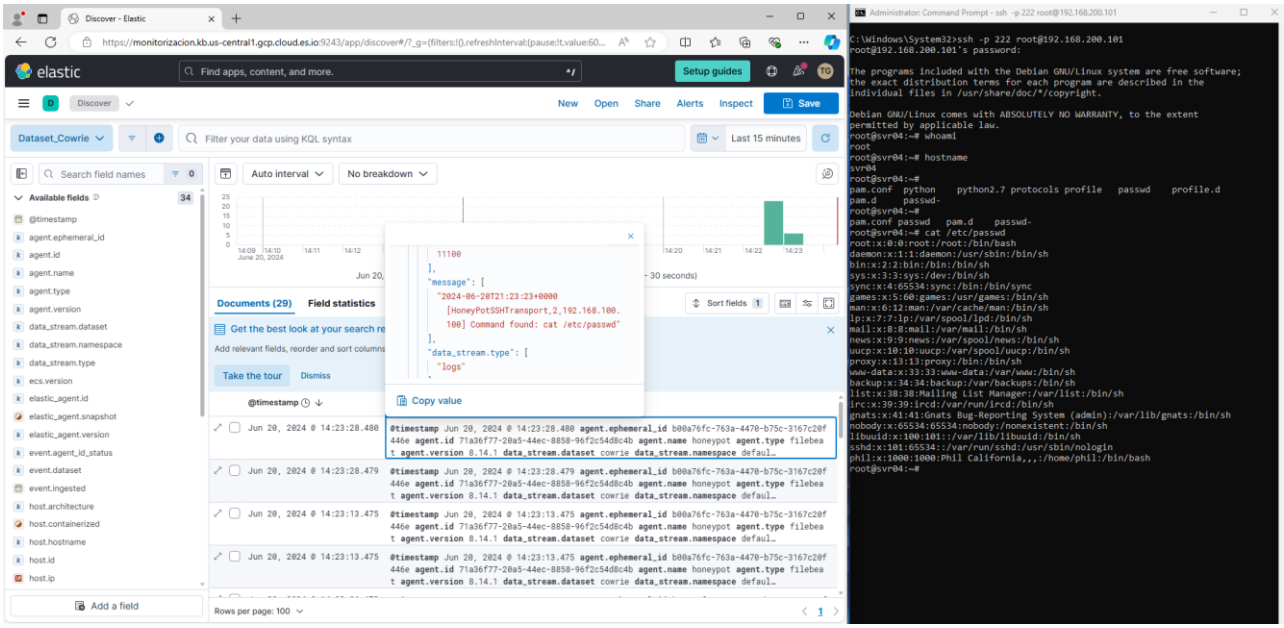



Vamos a Management -> Stack Management y en Kibana -> Data Views, creamos una visualización



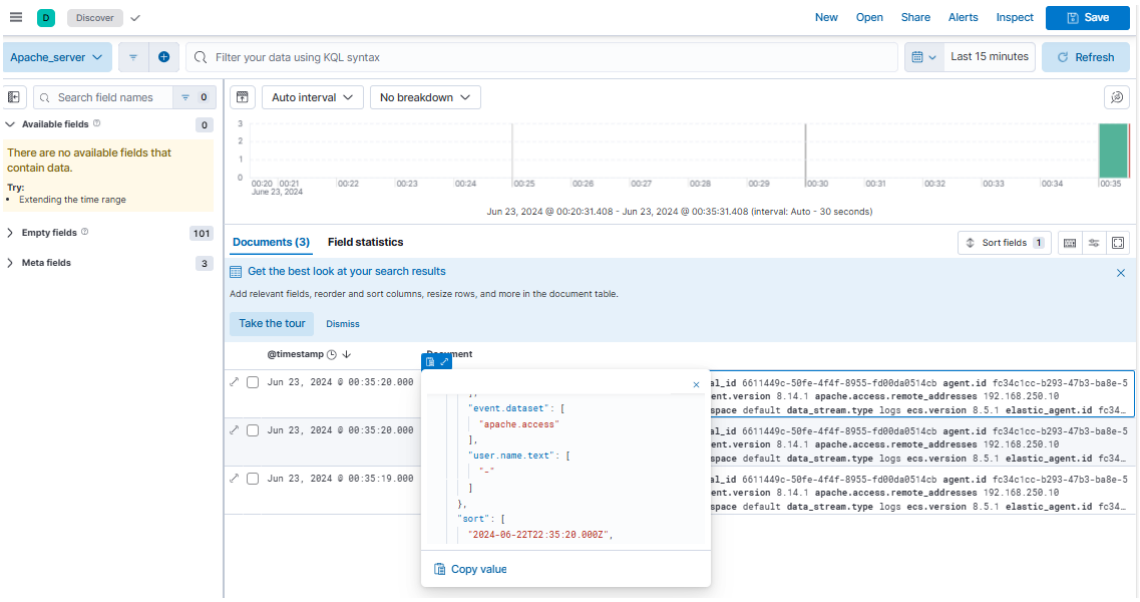

El logs-cowrie-default lo detecta si anteriormente se ha generado para ello un log, por eso habrá que conectarse antes al cowrie por ssh

## Comprobación de los logs del honeypot (cowrie)

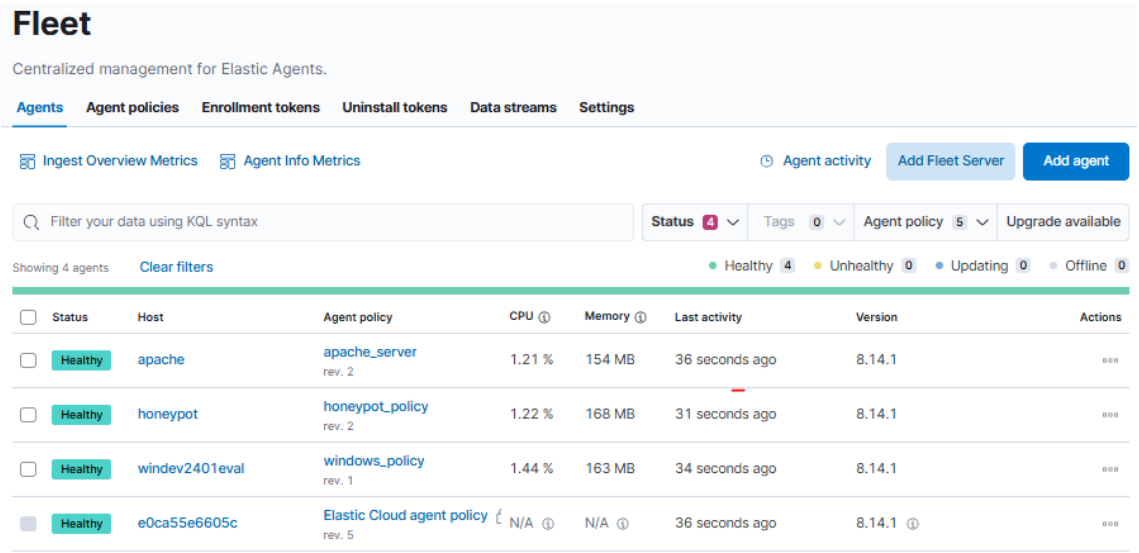



Se puede observar como se consigue saber que comandos ha lanzado desde el servidor ssh

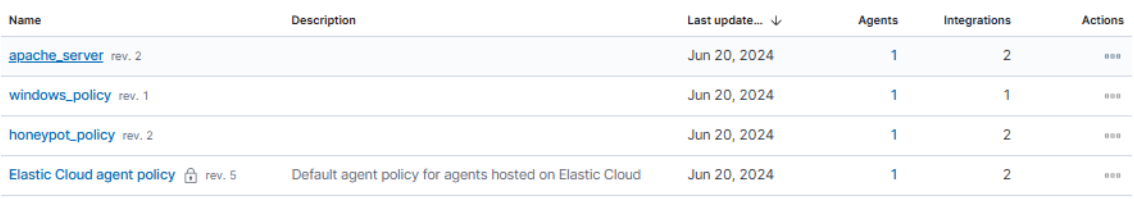
## Comprobación de los logs del apache server



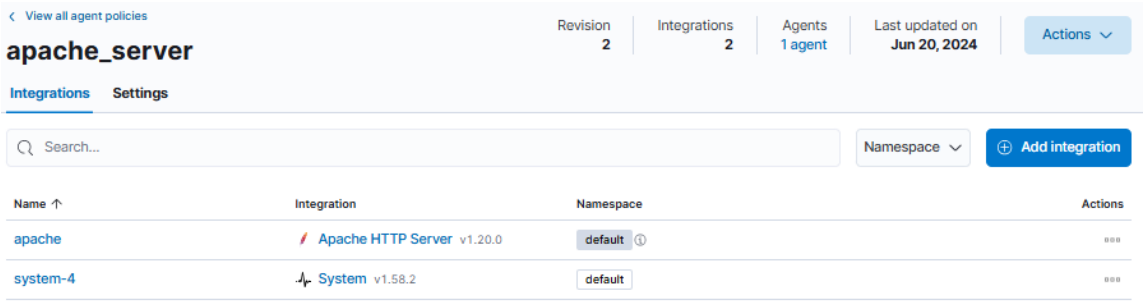
## Visión global de los agentes

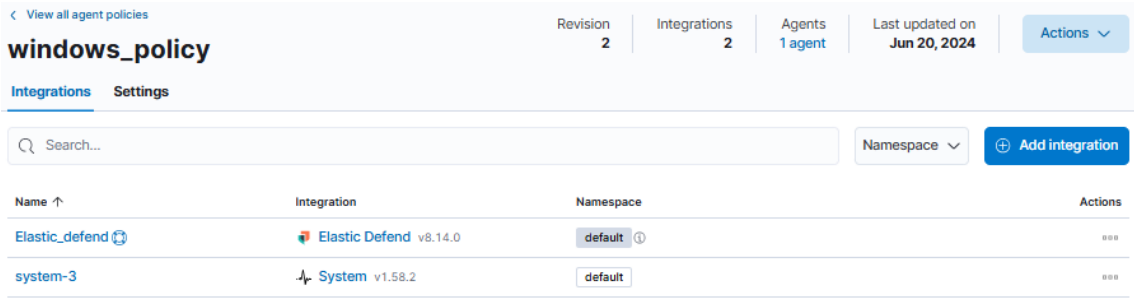


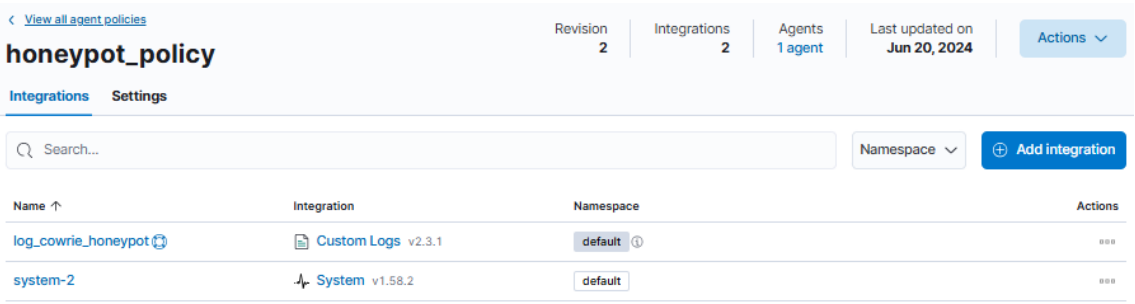

## Visión global de las políticas




## Visión de como quedan las políticas




View all agent policies
honeypot_policy
Revision
2
Integrations
2
Agents
1 agent
Last updated on
Jun 20, 2024
Actions
Integrations
Settings
Search...
Namespace
Add integration
Name
Integration
Namespace
Actions
log_cowrie_honeypot
Custom Logs v2.3.1
default
system-2
System v1.58.2
default