

Practica modulo: **Blue team**

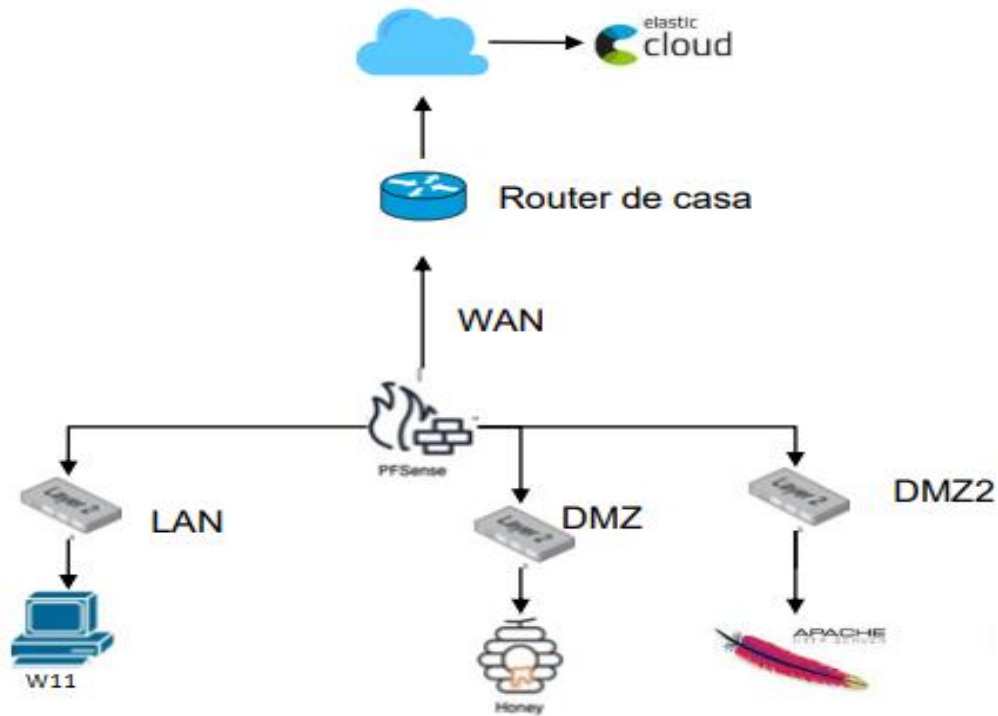


Realizado por: David Fernández Domingo
Email: tecno_g33k@hotmail.com

Índice

Esquema red	3
Configuración Pfsense	4
Configuración del Firewall para los accesos a la red externa	28
Configuración de las reglas en el firewall	29
Configuración firewall para la red DMZ	30
Configuración regla firewall para evitar que la DMZ	34
Configuración NAT	40
Configuración de un honeypot en la red DMZ	42
Configuración de Apache web server en DMZ_2	44
Configuración de elastic cloud	45
Instalación del agente en Windows 11 para integrar en Elastic	46
Integración de logs de Windows 11 en Elastic	47
Instalación del agente en el honeypot para integrar en elastic	48
Integración de logs del honeypot en Elastic	49
Instalación del agente de apache server en Elastic	51
Integración de logs de apache server en Elastic	52
Revisión de logs	54
Comprobación de los logs del honeypot (cowrie)	55
Comprobación de los logs del apache server	55
Visión global de los agentes	56
Visión global de las políticas	56
Visión de como quedan las políticas	56

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

Nombre y sistema operativo de la máquina virtual

Seleccione un nombre descriptivo y carpeta destino para la nueva máquina virtual. El nombre que seleccione será usado por VirtualBox para identificar esta máquina. Adicionalmente, puede seleccionar una imagen ISO que puede ser usada para instalar el sistema operativo invitado.

Nombre: ✓

Carpeta:

Imagen ISO: pfSense-CE-2.7.2-RELEASE-amd64.iso


Edición:

Tipo: 64

Versión:

☐ Omitir instalación desatendida

❗ El tipo de SO no se puede determinar a partir de la ISO seleccionada, el SO invitado será necesario instalarlo manualmente.



Crear máquina virtual

Hardware


Puede modificar el hardware de la máquina virtual cambiando la cantidad de RAM y número de CPU virtuales. También es posible habilitar EFI.

Memoria base: 2048 MB

Procesadores: 1

1 CPU 8 CPUs

☐ Habilitar EFI (sólo SO especiales)



Crear máquina virtual

Disco duro virtual

Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☒ Crear un disco duro virtual ahora

Tamaño de disco: 20,47 GB

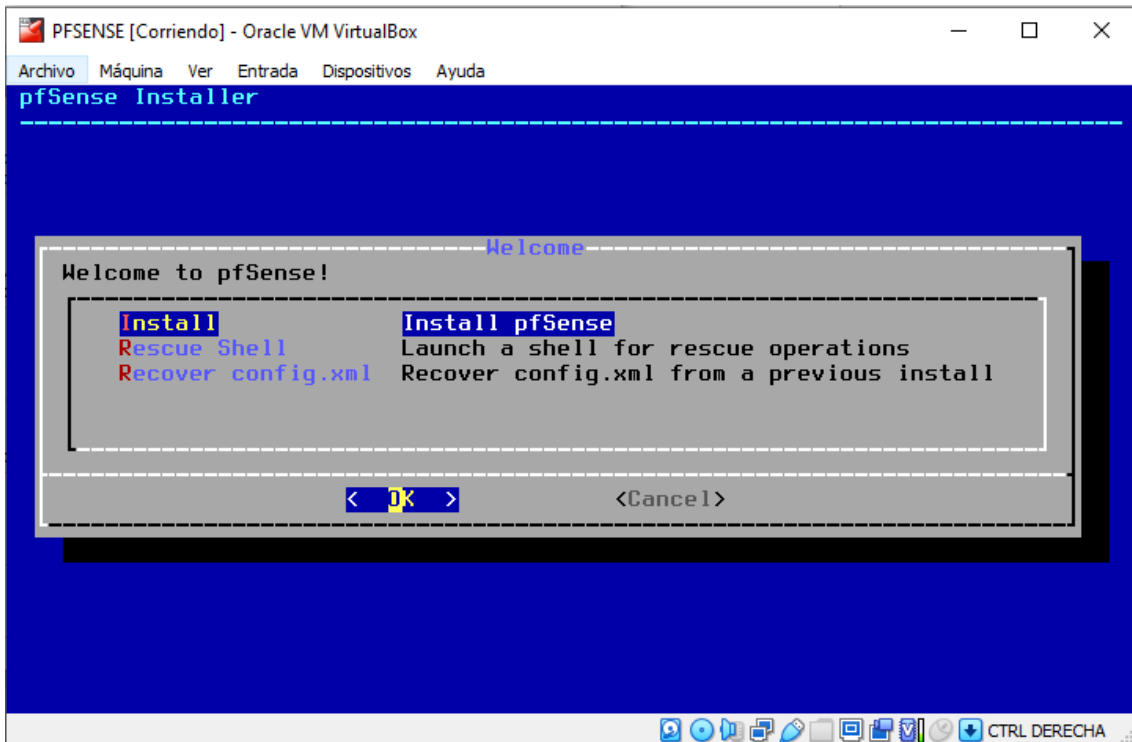
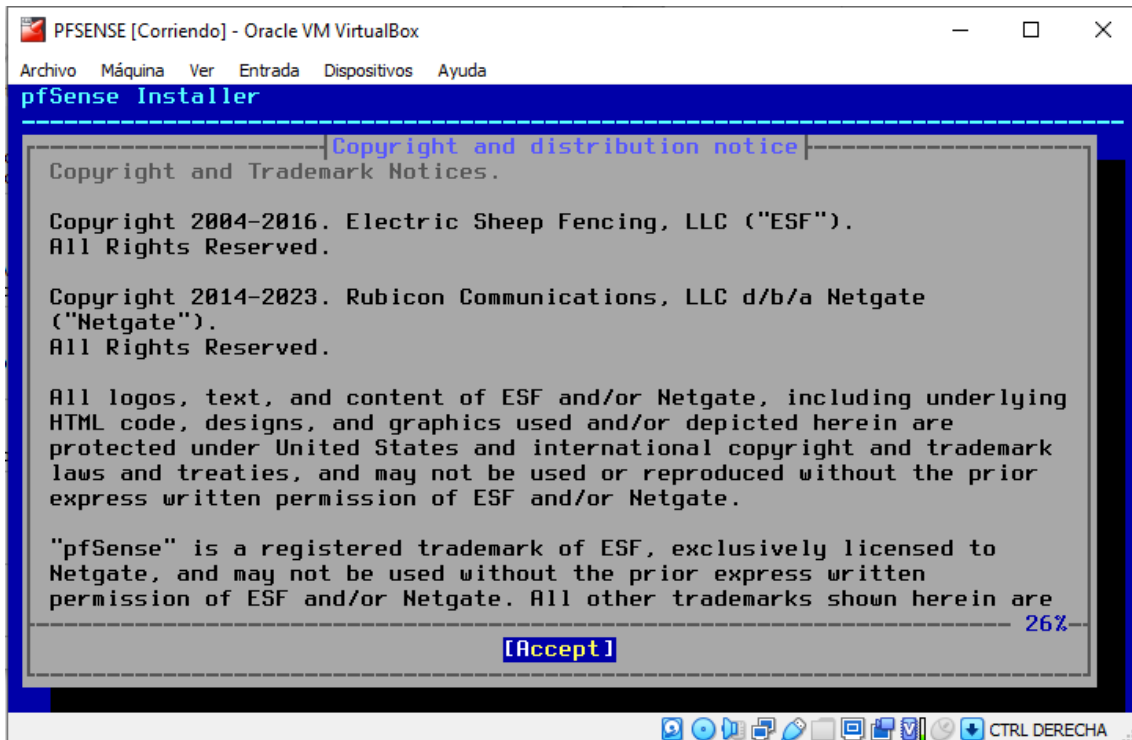
4,00 MB 2,00 TB

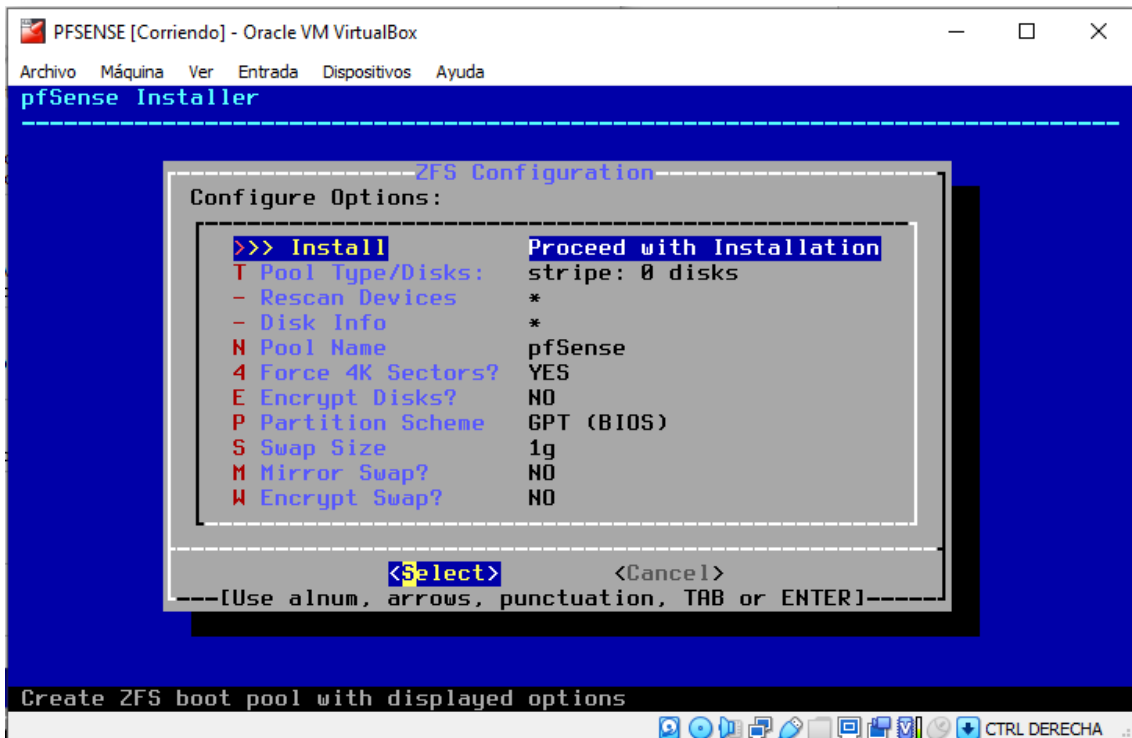
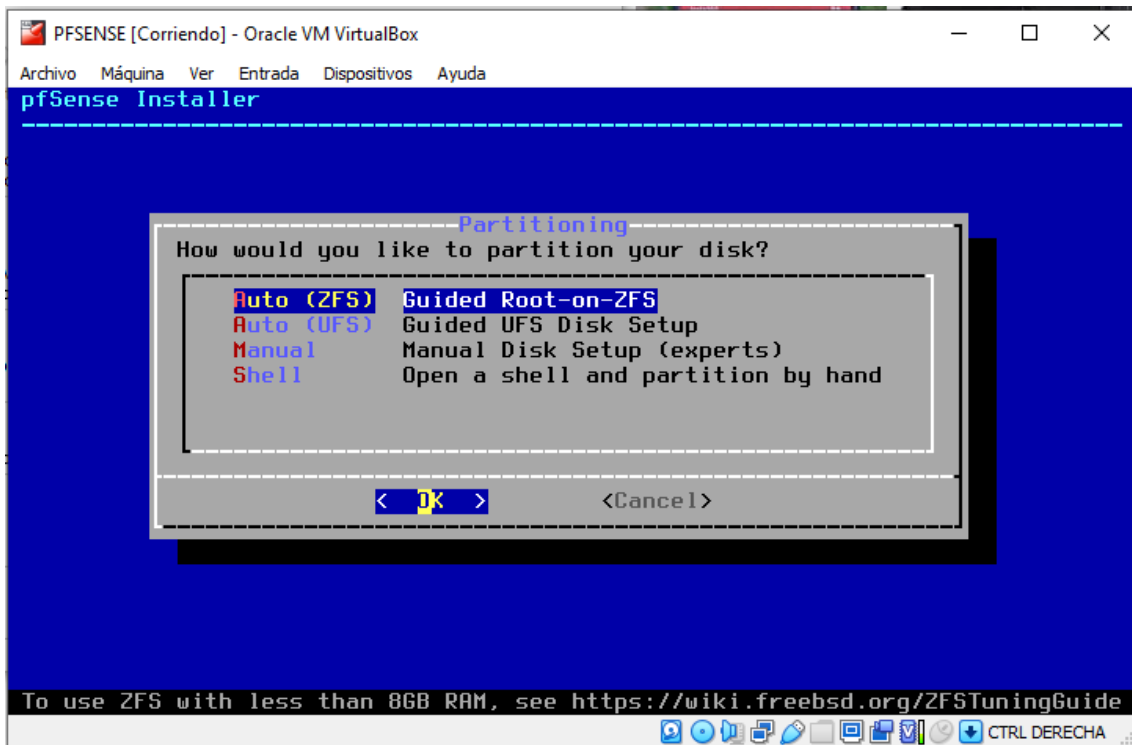
☐ Reservar tamaño completo

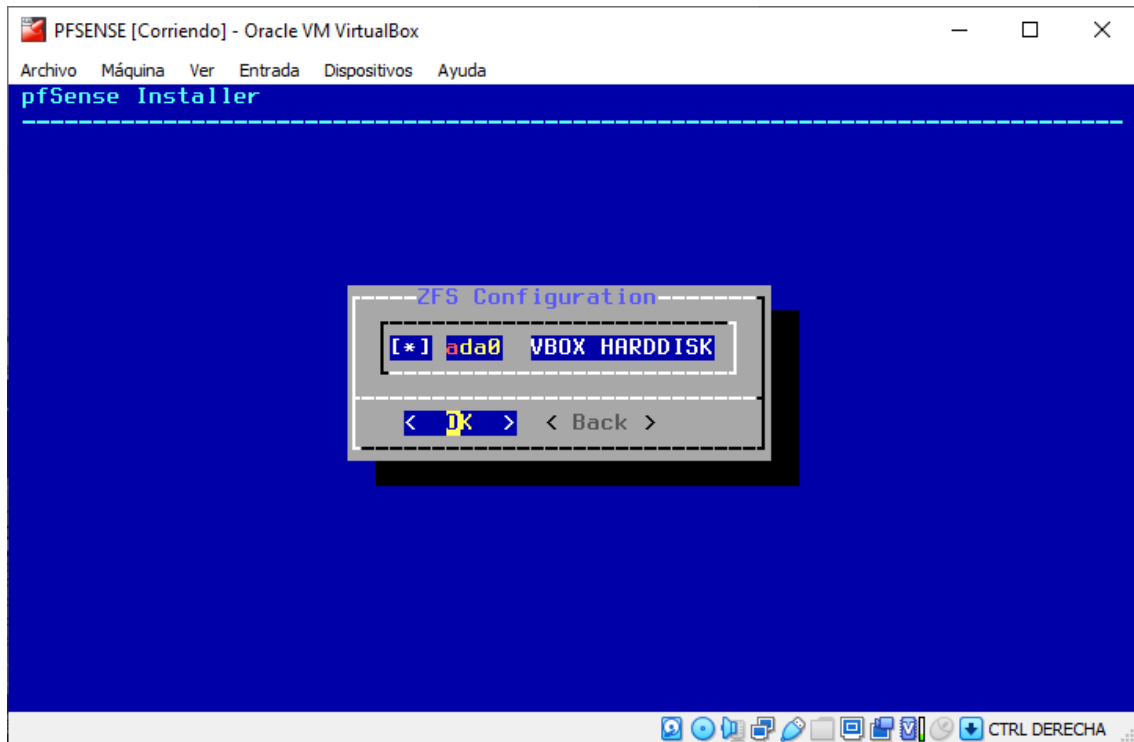
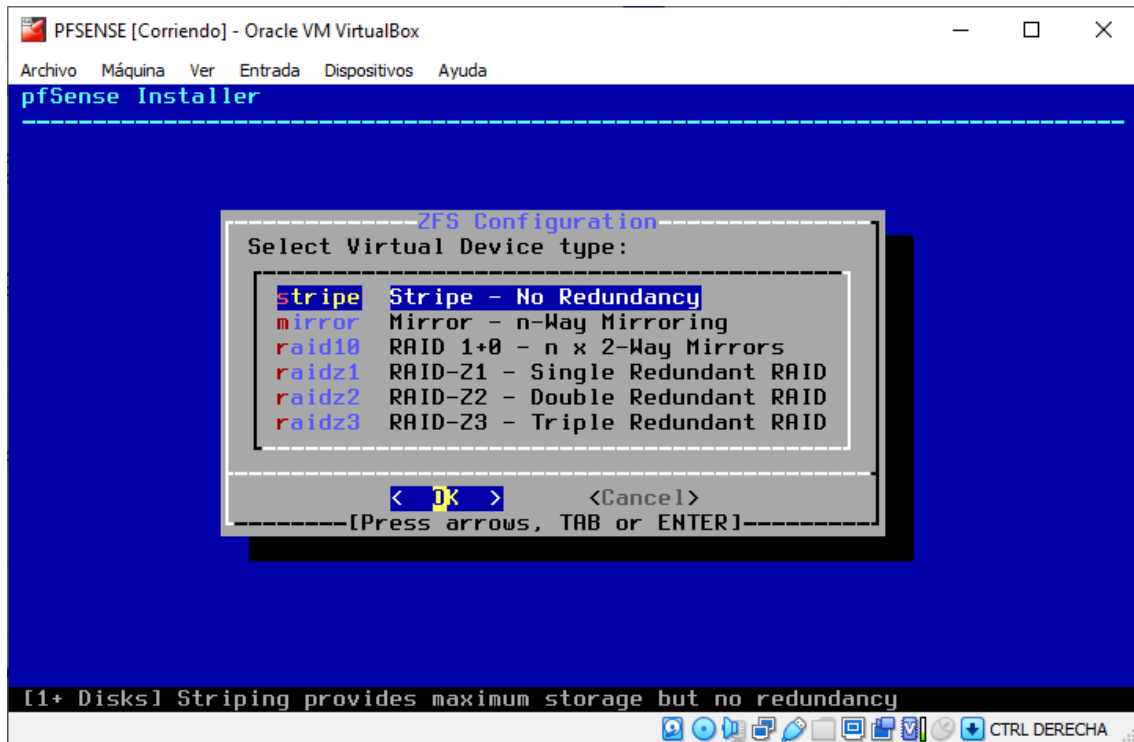
☐ Usar un archivo de disco duro virtual existente

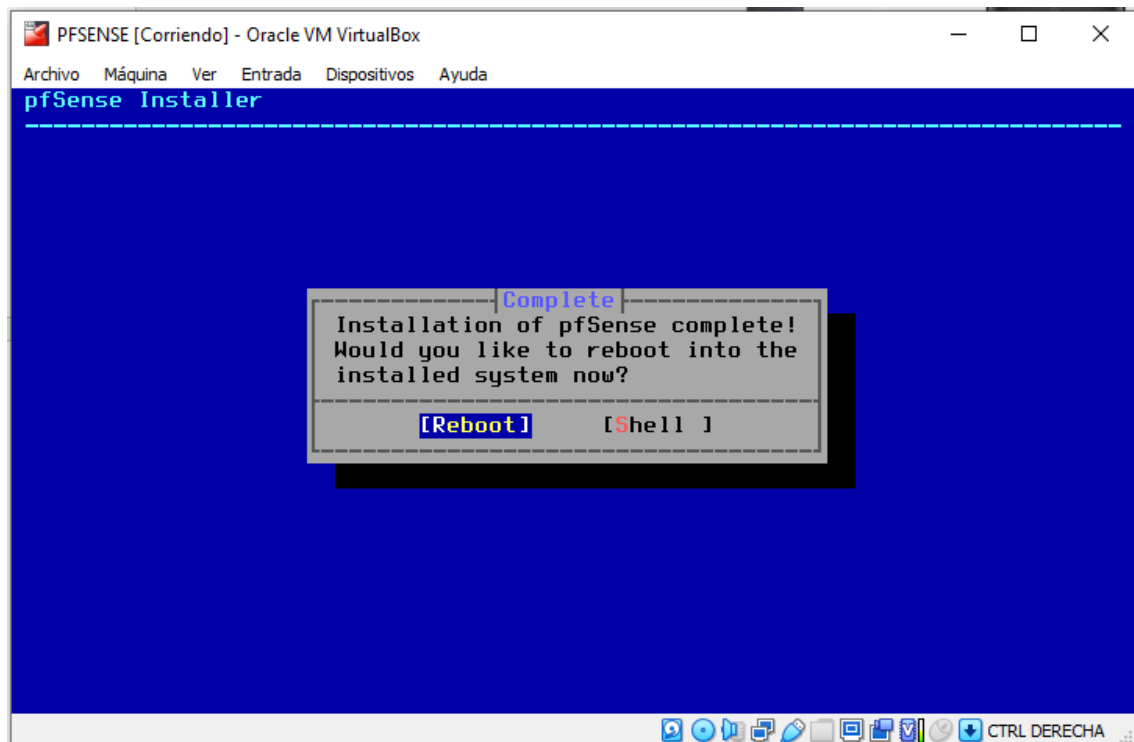
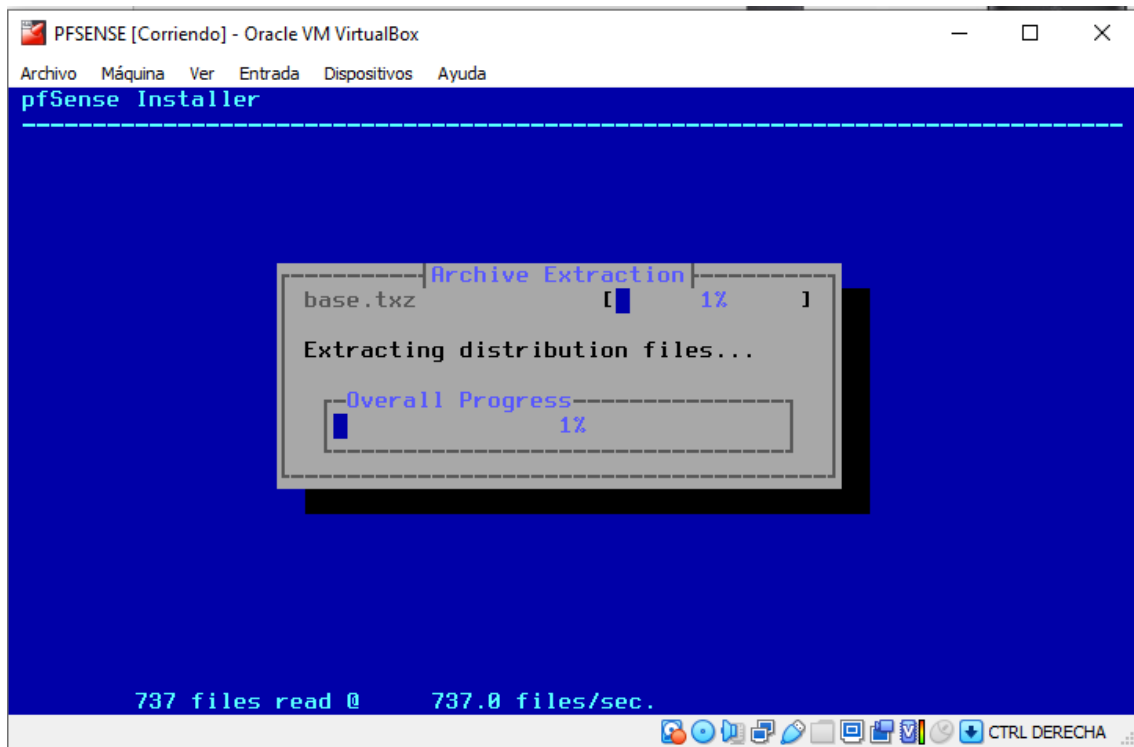
WinDev2401Eval-disk001.vdi (Normal, 125,00 GB)

☐ No añadir un disco duro virtual

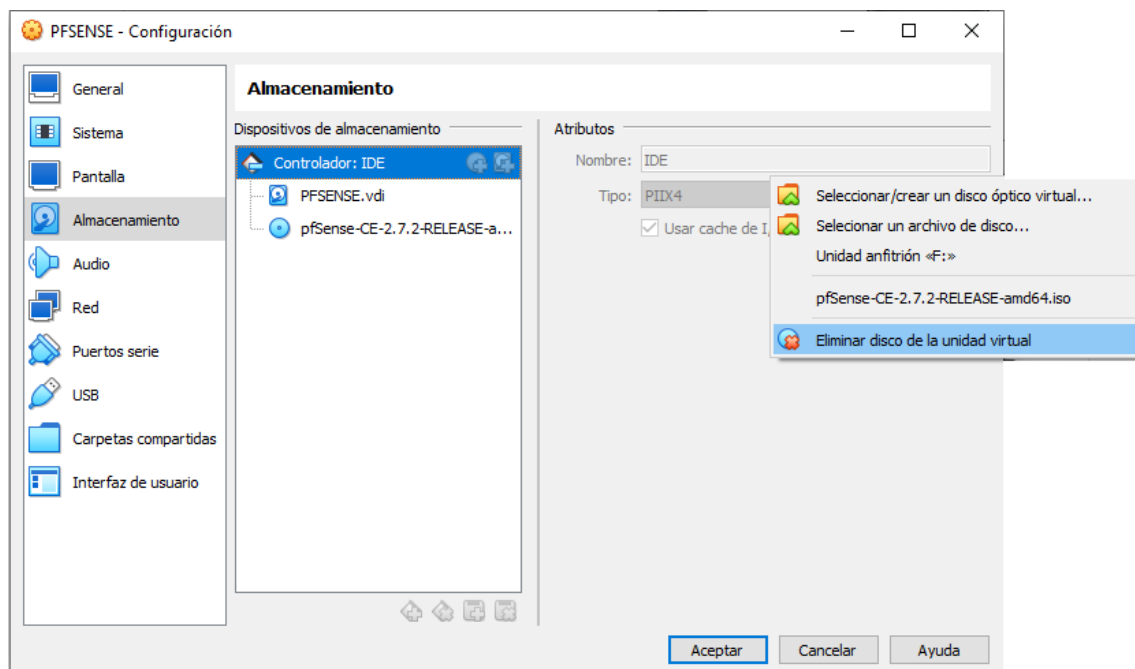




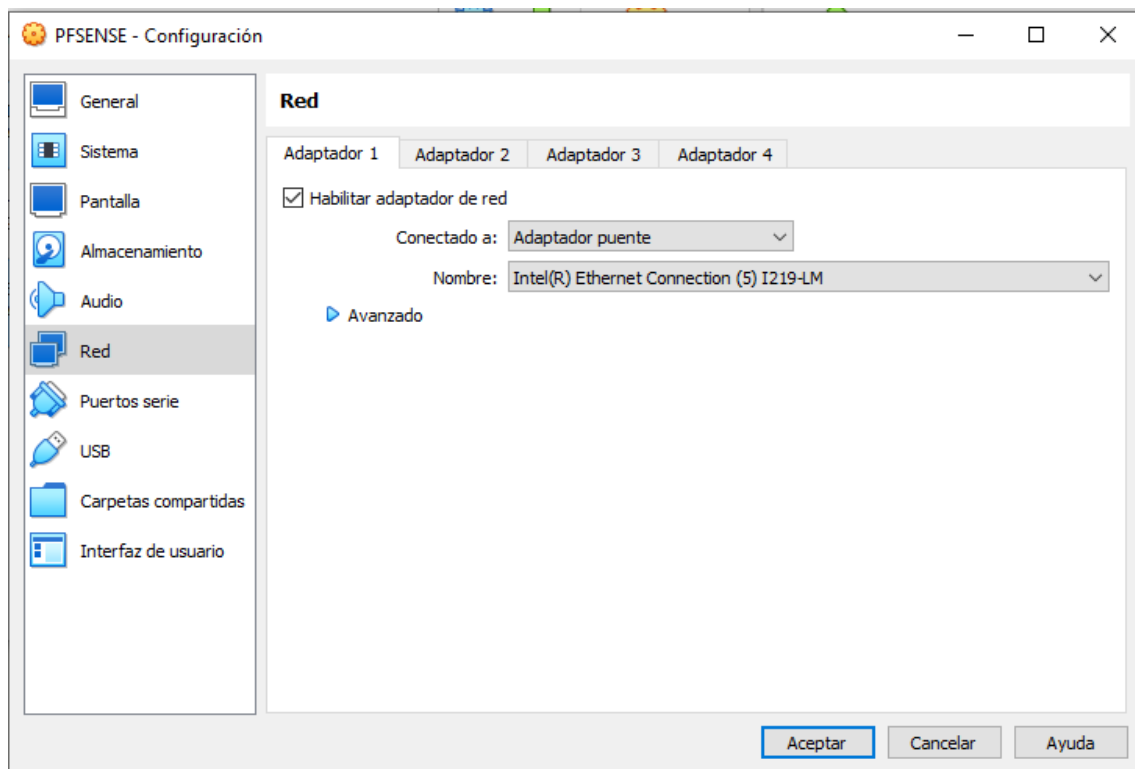


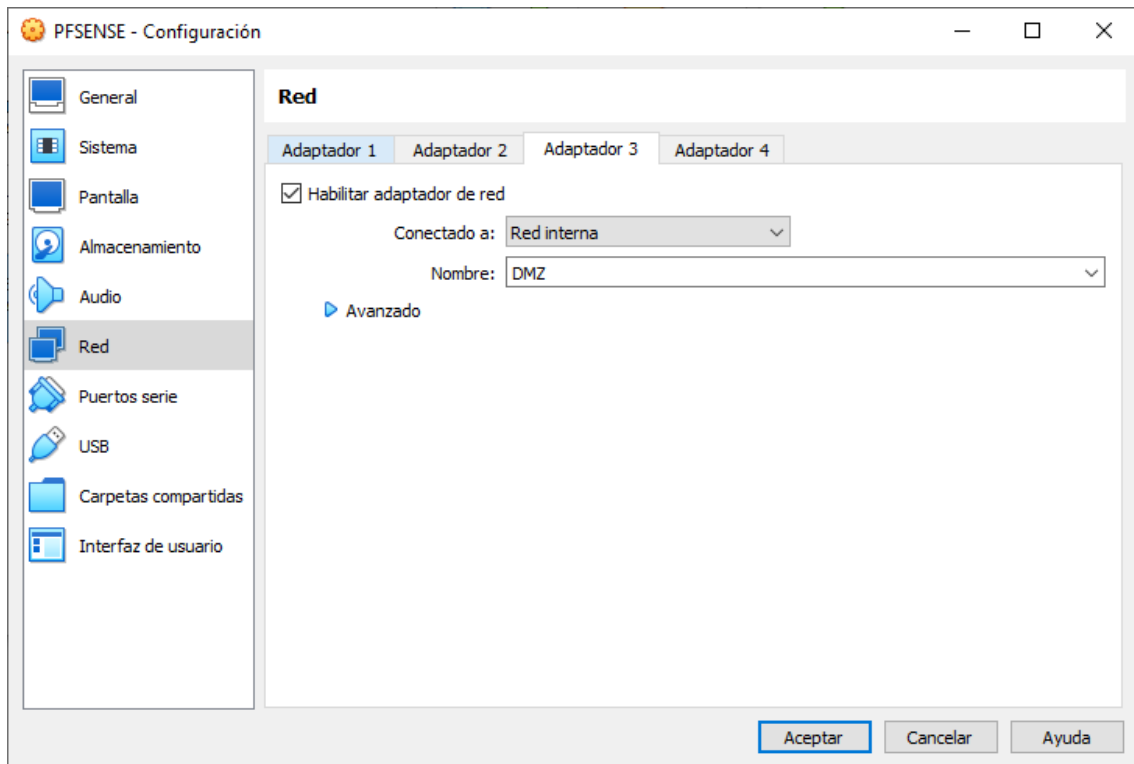
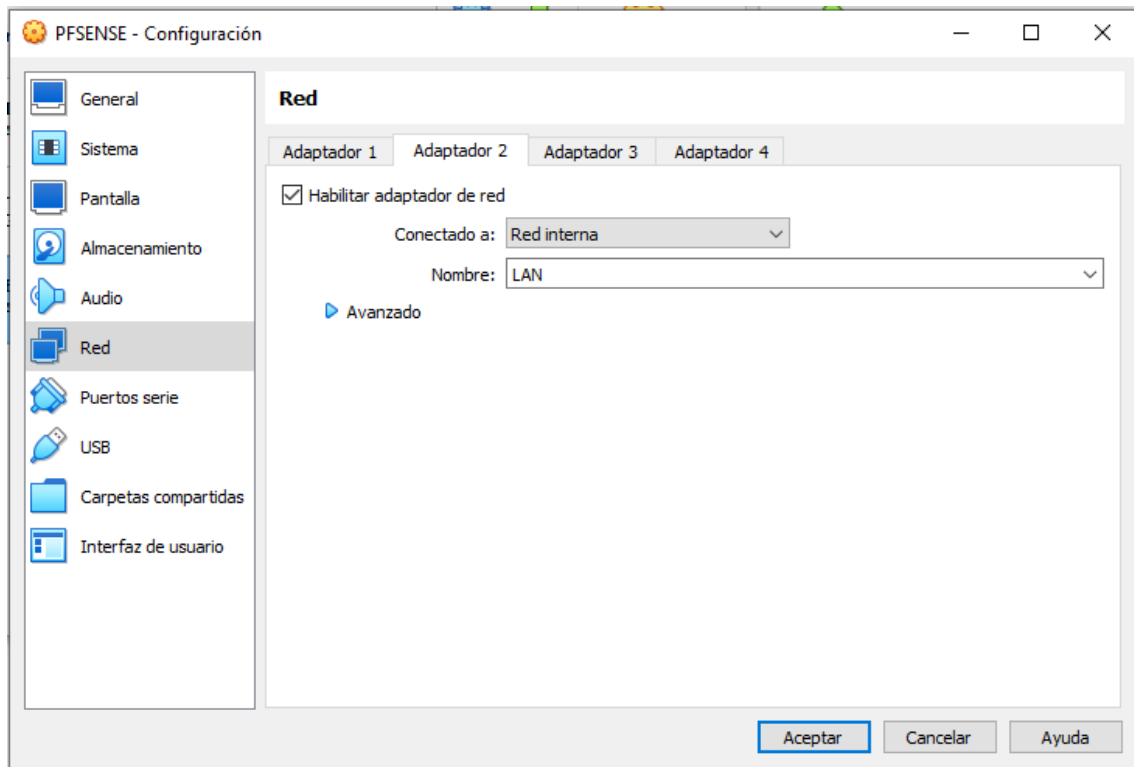


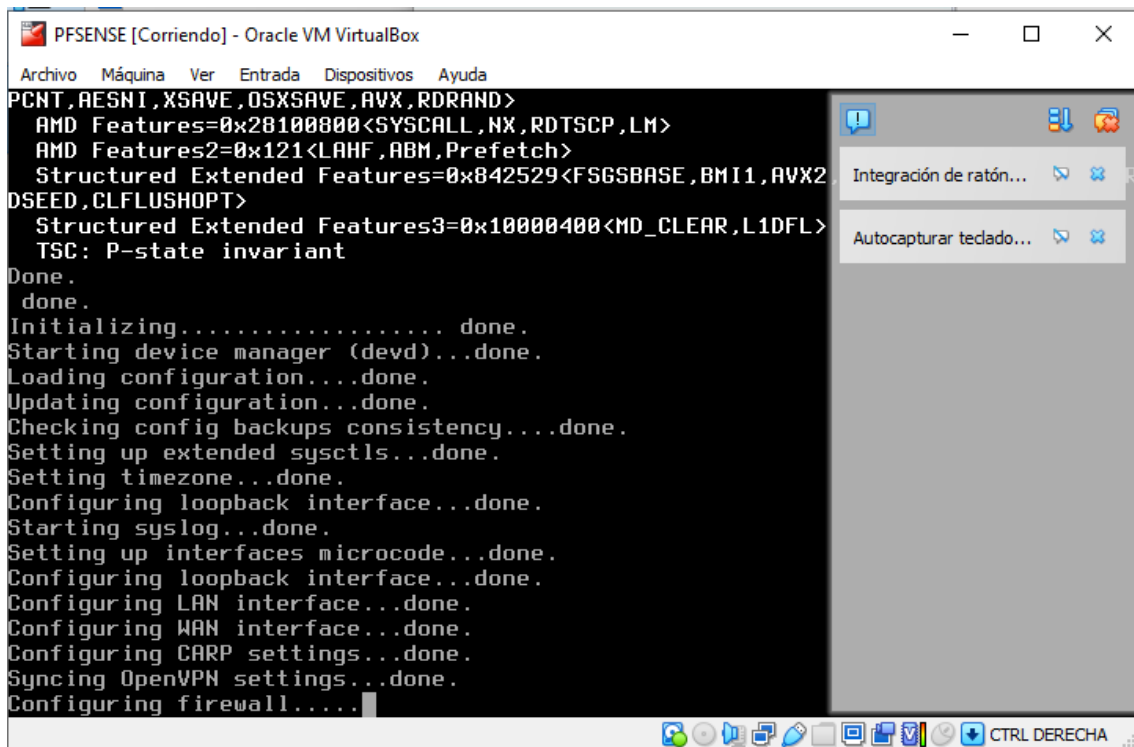
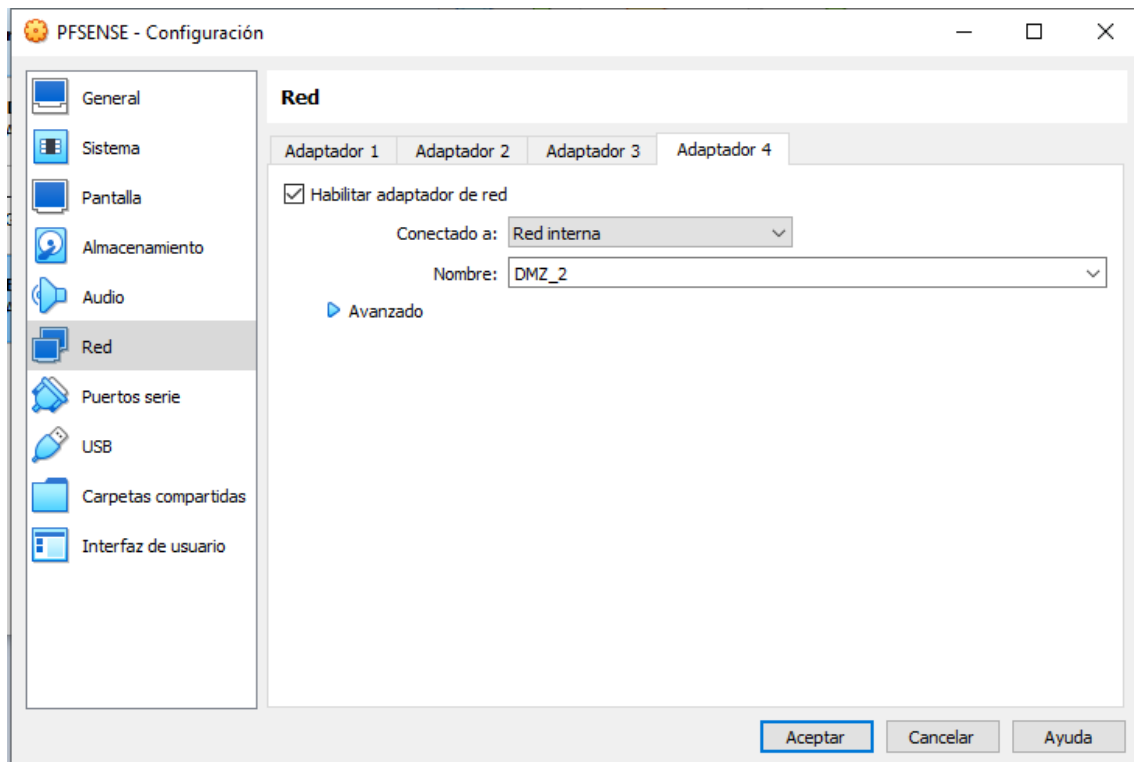
Importante eliminar el disco virtual para que no vuelva a reinstalar el Pfsense



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







```
PFSENSE [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: 0bffb5fea1d7cdfec90

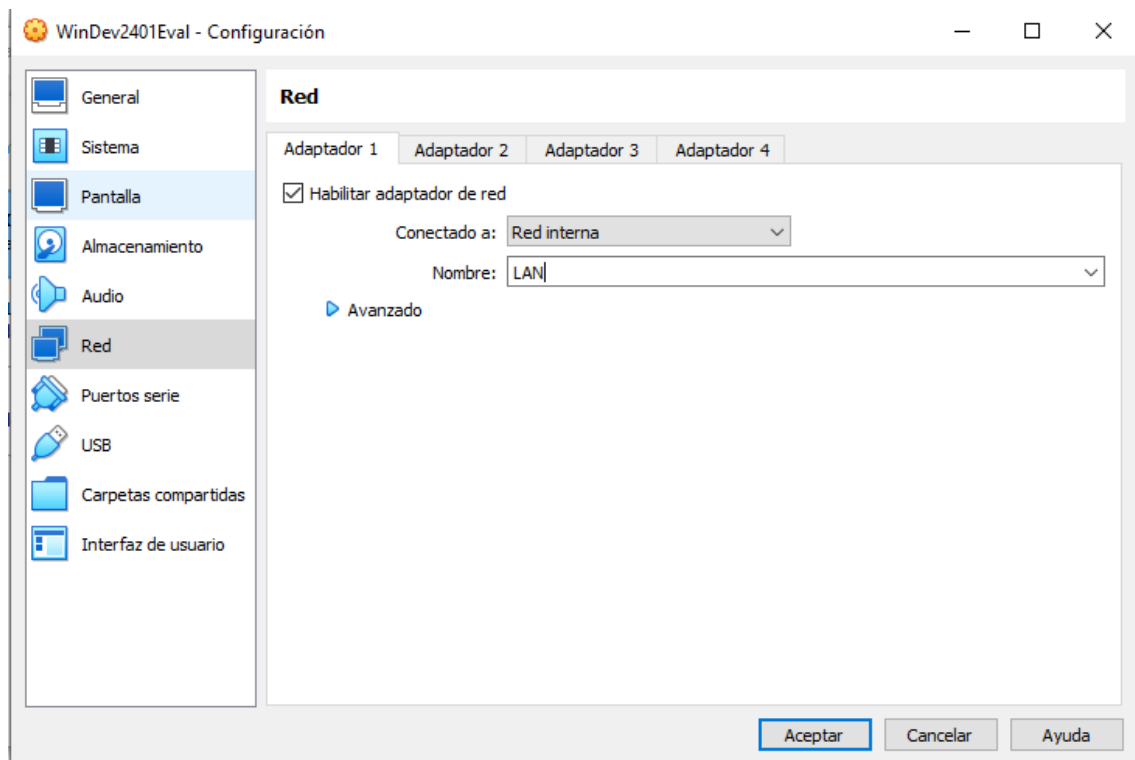
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.97/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

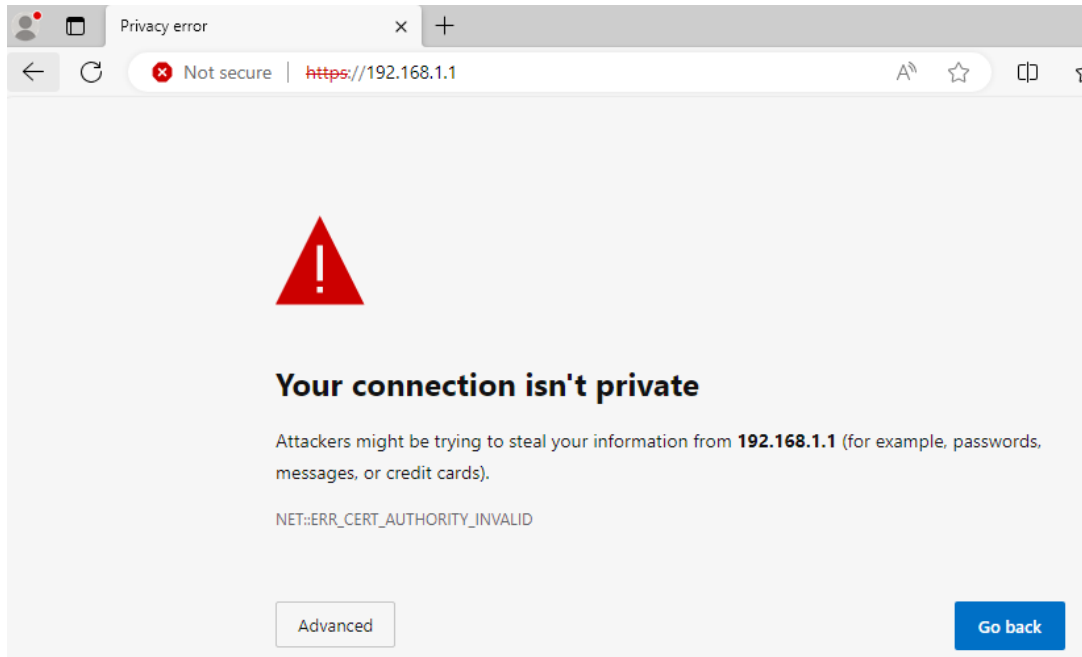
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: 
```

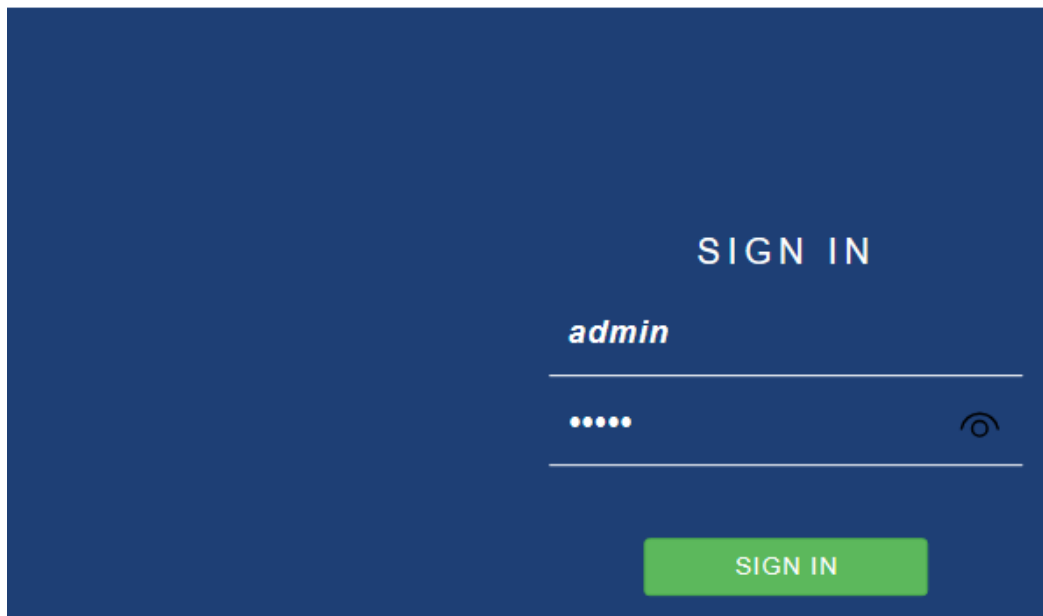
Una vez tenemos el PFSENSE iniciado, pondré Windows 11 para que se encuentre en la red LAN para poder configurar el PFSENSE



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

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / General Information



Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

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.

Primary DNS Server

Secondary DNS Server

Override DNS



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

Wizard / pfSense Setup / Time Server Information



Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname

Enter the hostname (FQDN) of the time server.

Timezone



» Next

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

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

SelectedTypeDHCP

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 Mask32

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.

Wizard / pfSense Setup / Configure LAN Interface ?

Step 5 of 9

Configure LAN Interface

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

LAN IP Address	<input type="text" value="192.168.100.1"/>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/>

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

Wizard / pfSense Setup / Set Admin WebGUI Password ?

Step 6 of 9

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	<input type="password"/>
Admin Password AGAIN	<input type="password"/>

Step 7 of 9

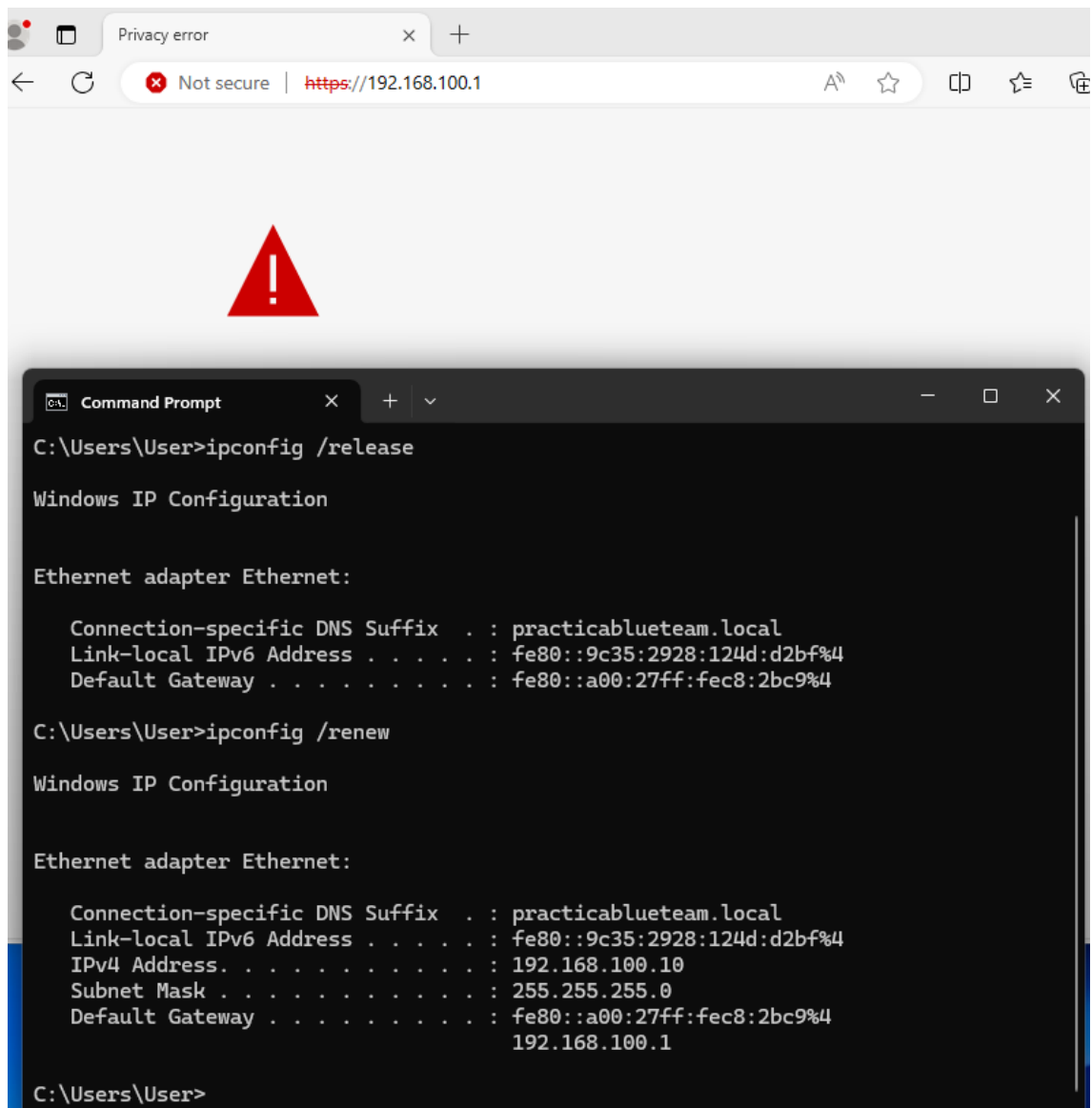
Reload configuration

Click 'Reload' to reload pfSense with new changes.

» Reload

Al darle reload, se reinicia el Pfsense

Entramos con la nueva dirección, 192.168.100.1



Compruebo y configuro para la resolución de nombres y habilito

Services / DNS Resolver / General Settings

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable

☒ Enable DNS resolver

Listen Port

53

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

Enable
SSL/TLS
Service

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

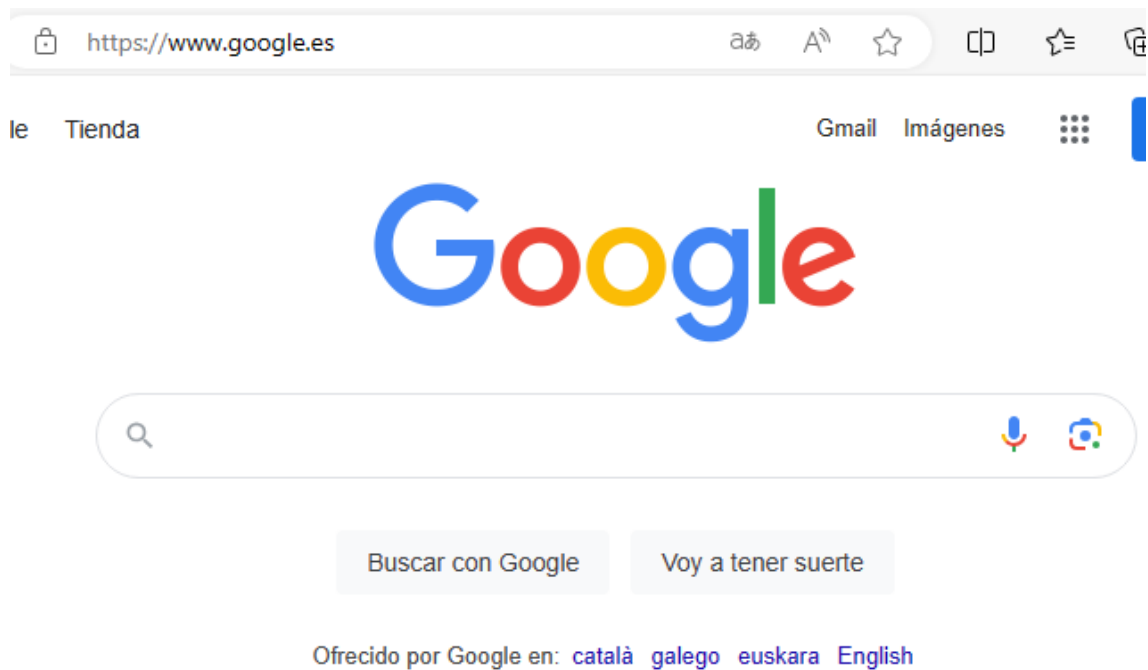
DNSSEC

☐ Enable DNSSEC Support

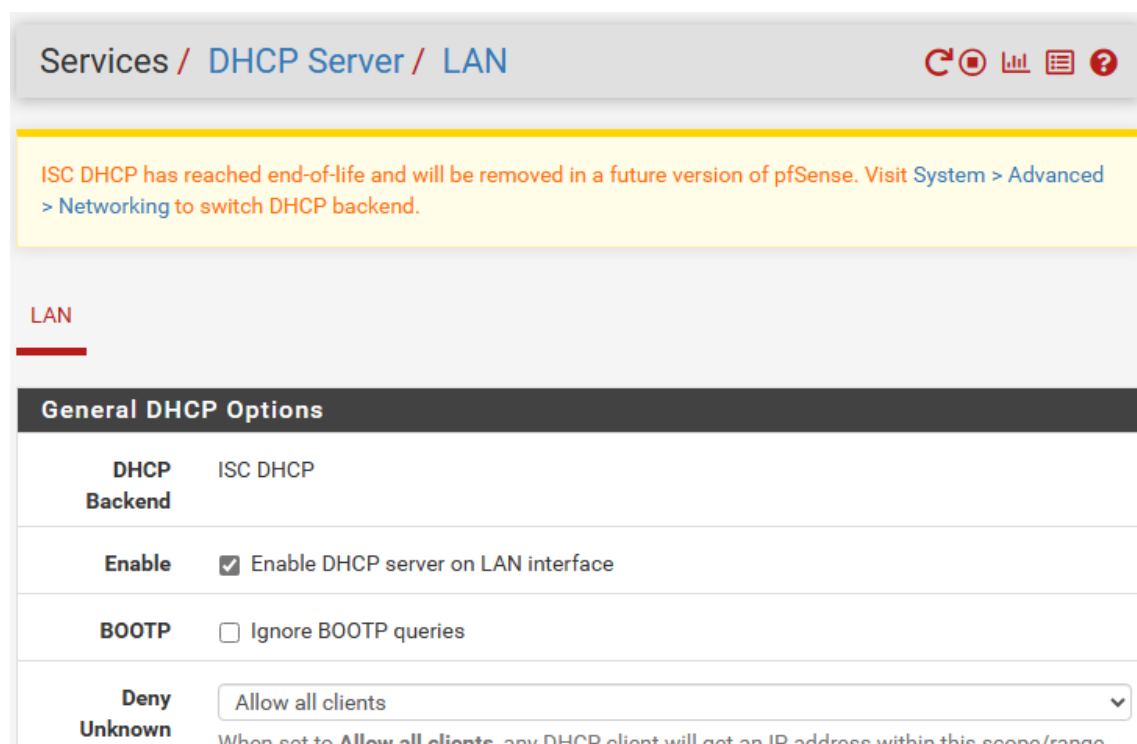
The DNS resolver configuration has been changed.
The changes must be applied for them to take effect.

☒ Apply Changes

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	<div> <input type="text" value="192.168.100.100"/> <input type="text" value="192.168.100.200"/> </div> <div>FromTo</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
Additional Pools	<div> + Add Address Pool </div> <p>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</p>

Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.100.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>
	<input type="text" value="DNS Server 4"/>

Configuramos la puerta de enlace (gateway)

Other DHCP Options	
Gateway	<input type="text" value="192.168.100.1"/> <p>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.</p>

Salvamos y aplicamos cambios

```

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : practicablueam.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  . : practicablueam.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)

Interfaces / Interface Assignments
📊 ?

Interface has been added. ✕



Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges




LAGGs

Interface	Network port	
WAN	em0 (08:00:27:80:f2:a6) ▼	
LAN	em1 (08:00:27:c8:2b:c9) ▼	🗑️ Delete
OPT1	em2 (08:00:27:8c:79:60) ▼	🗑️ Delete
OPT2	em3 (08:00:27:76:40:5d) ▼	🗑️ Delete

💾 Save

Configuro la interfaz DMZ con la subred 192.168.200.1


 

Interfaces / OPT1 (em2)   

General Configuration

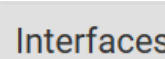

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>




Static IPv4 Configuration

IPv4 Address	<input type="text" value="192.168.200.1"/> / <input type="text" value="24"/>
IPv4 Upstream gateway	<input type="text" value="None"/> 

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Configuro la interfaz DMZ_2 con la subred 192.168.250.1

Interfaces / OPT2 (em3)   

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ_2"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
 On local area network interfaces the upstream gateway should be "none".
 Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
 Gateways can be managed by [clicking here](#).

Compruebo los cambios en Pfsense

```

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

FreeBSD/amd64 (PFSENSE.practicablue.team.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 0bffbba5fea1d7cdfec90
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on PFSENSE ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.97/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.1/24
DMZ_2 (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 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.

LANDMZDMZ_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

192.168.200.150

From

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

192.168.200.1

1.1.1.1

8.8.8.8

DNS Server 4

Other DHCP Options

Gateway

192.168.200.1

The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

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

192.168.250.150

From

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.


Server Options	
WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.250.1
	1.1.1.1
	8.8.8.8
	DNS Server 4

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.	

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

Firewall / Aliases / Ports 


IP Ports URLs All

Firewall Aliases Ports

Name	Type	Values	Description	Actions
------	------	--------	-------------	---------

 Add  Import

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

Firewall / Aliases / Edit 

Properties

Name

webs

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

puertosalidaweb

A description may be entered here for administrative reference (not parsed).

Type

Port(s)

▼

Port(s)


Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port


80

HTTP

 Delete

443

HTTPS








 Delete

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

Configuración firewall para la red DMZ

DMZ

Floating

WAN

LAN

DMZ

DMZ_2

Rules (Drag to Change Order)

☐

States

Protocol

Source

Port

Destination

Port

Gateway

Queue

Schedule

Description

Actions

No rules are currently defined for this interface

All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑

Add

↓

Add

🗑

Delete

🔄

Toggle

📄

Copy

💾

Save

+

Separator

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

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**.

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

Destination			
Destination	<input type="checkbox"/> Invert match	Any	Destination Address /
Destination Port Range	(other)	webs	(other) webs
	From	Custom	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	<input type="checkbox"/> 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.		
Advanced Options	<input type="button" value="Display Advanced"/>		

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

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

UDP

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**.

Destination

Destination

☐ Invert match

Any

Destination Address /

Destination Port Range

DNS (53)

Custom

To

DNS (53)

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

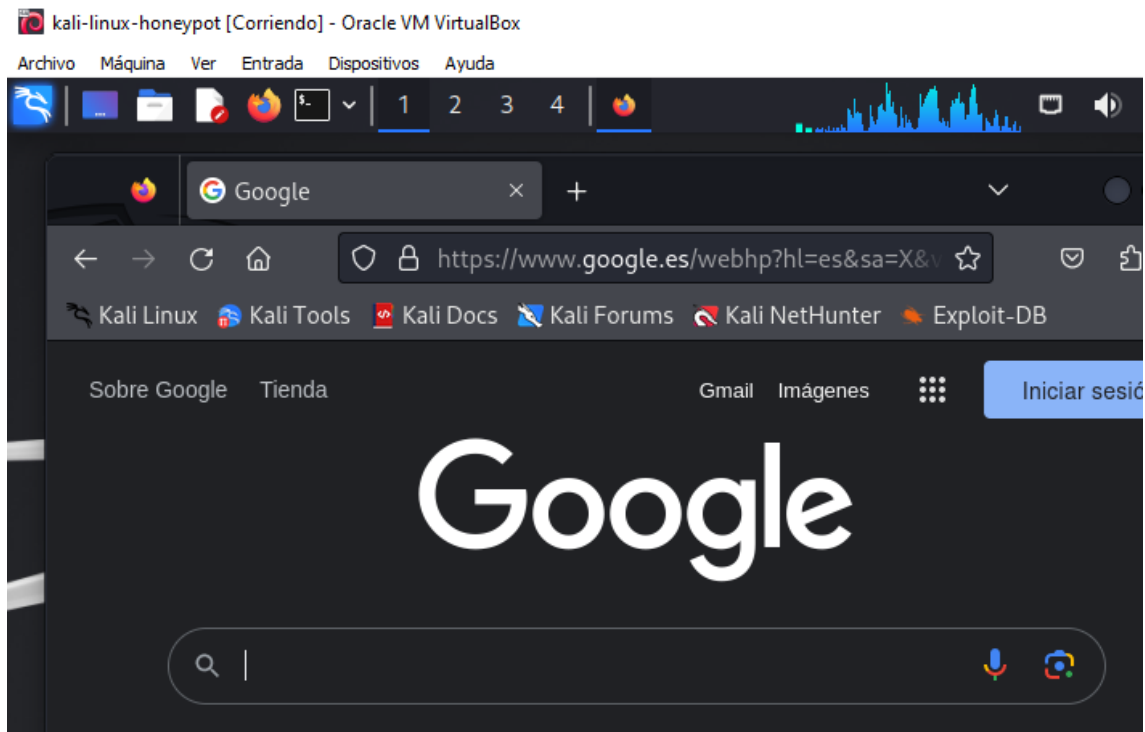
permitir trafico DNS

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.

Advanced Options

Display Advanced

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	<div>Block</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>DMZ</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>

Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>DMZ subnets</div> <div>Source Address /</div>

Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>DMZ_2 subnets</div> <div>Destination Address /</div>

Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div>bloqueo para subnet DMZ_2</div>

Visión global de cómo queda la regla para la DMZ

Firewall / Rules / DMZ											
Floating WAN LAN DMZ DMZ_2											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	none		bloqueo para subnet LAN	   
<input type="checkbox"/>	✗	0/0 B	IPv4 *	DMZ subnets	*	DMZ_2 subnets	*	none		bloqueo para subnet DMZ_2	   
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	*	*	*	*	none		ping	   
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	DMZ subnets	*	53 (DNS)	*	none		permitir trafico DNS	   
<input type="checkbox"/>	✓	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
```

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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match
	DMZ_2 subnets
	Source Address /
Destination	
Destination	<input type="checkbox"/> Invert match
	Any
	Destination Address /
Destination Port Range	(other) webs (other) webs
	From Custom 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	<input type="checkbox"/> 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 protocolo 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

To

DNS (53)

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

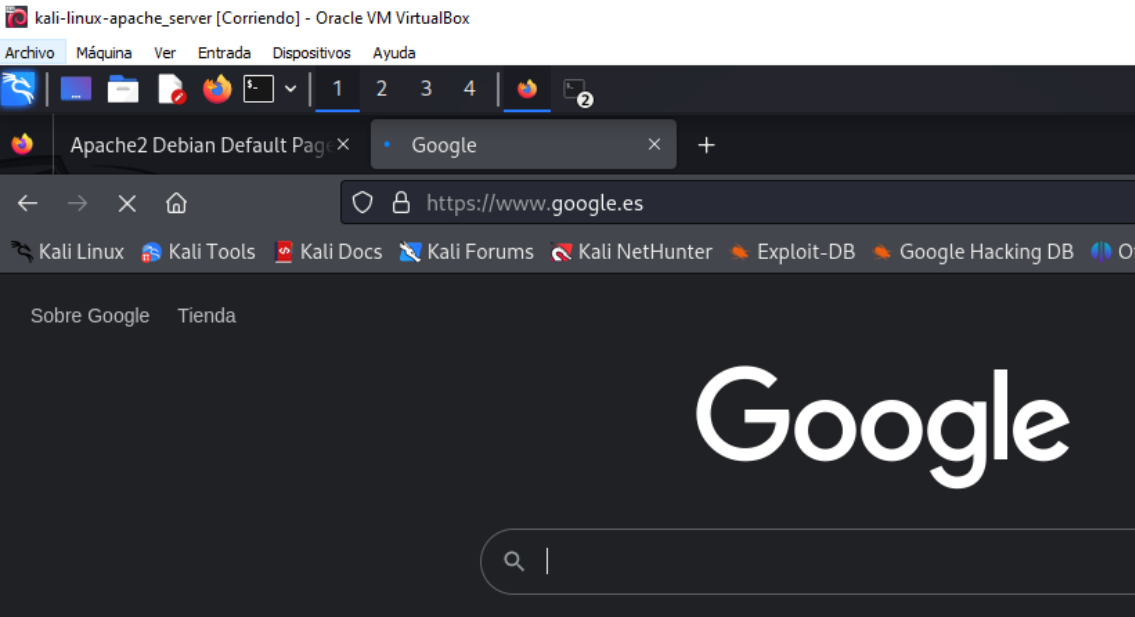
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

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 <u>DMZ_2</u>											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	DMZ_2 subnets	*	LAN subnets	*	*	none	bloqueo subnet LAN	
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	DMZ_2 subnets	*	DMZ subnets	*	*	none	bloqueo subnet DMZ	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	DMZ_2 subnets	*	*	53 (DNS)	*	none	permitir trafico DNS	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	DMZ_2 subnets	*	*	webs	*	none	salida trafico web	

Configuración NAT

Configuración para DMZ_2 servidor apache

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

192.168.250.100

Type

Address

192.168.250.100 es donde se encuentra el servidor apache

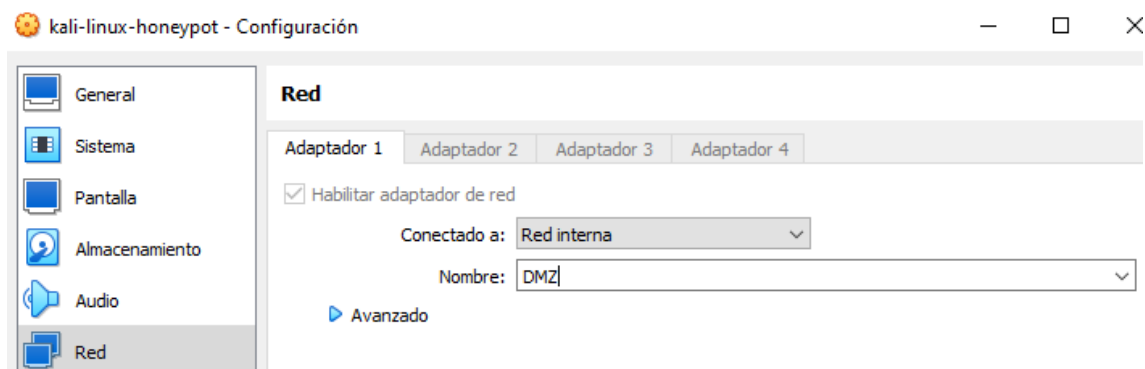
Compruebo que se tiene acceso desde fuera



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
```

```
root@honeypot: /home/kali
File Actions Edit View Help

(root@honeypot)-[/home/kali]
# docker run -p 222:2222 cowrie/cowrie > cowrie.log
Unable to find image 'cowrie/cowrie:latest' locally
latest: Pulling from cowrie/cowrie
```

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
```

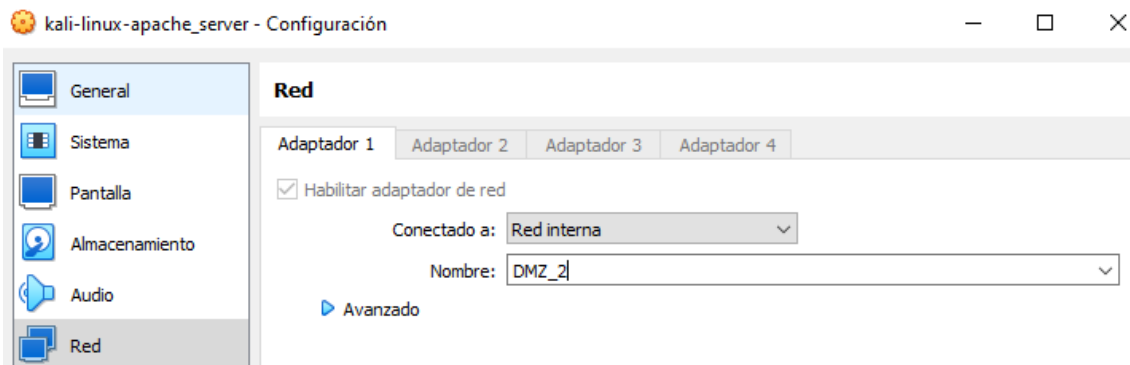
```
Administrator: Command Prompt - ssh -p 222 root@192.168.200.101
Microsoft Windows [Version 10.0.22621.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh -p 222 root@192.168.200.101
The authenticity of host '[192.168.200.101]:222 ([192.168.200.101]:222)' can't be established.
ED25519 key fingerprint is SHA256:SvQPpzUbnPqLF7CMhNjJBheYKLhSai8g6Ne7+jsCLn8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.200.101]:222' (ED25519) to the list of known hosts.
root@192.168.200.101'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:~# whoami
root
root@svr04:~# hostname
svr04
root@svr04:~#
```

Configuración de Apache web server en DMZ 2



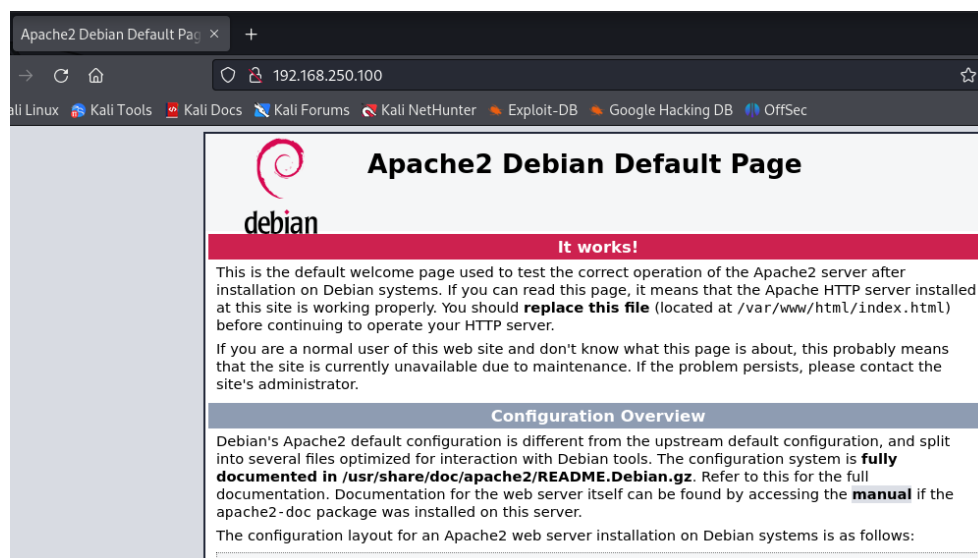
Compruebo que la maquina se encuentre en la red correcta

```
(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

☰


D

Integrations

Elastic Defend

Connection details

< Back to integrations



Elastic Defend

Elastic Agent

Overview

Settings

Configs

Advanced

Version 8.12.0

+ Add Elastic Defend


Elastic Defend Integration

Elastic Defend provides organizations with prevention.

Requirements

Permissions root privileges


1



Install Elastic Agent

Install agents on the hosts that you want to connect to Elastic.


2



Add the integration

Make a few selections to finalize how Elastic receives your data.

3



Confirm incoming data

Explore and analyze the incoming data.

Add integration only (skip agent installation)

Install Elastic Agent



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-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-central1.gcp.cloud.es.io:443 --enrollment-token=WdzcK00NEJKSWZ0YkxPRFJBWkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
```

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-agent/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://9257bce4db4c4dae890eca50cdabd24c.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=WdzcK00NEJKSWZ0YkxPRFJBWkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
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_cmd.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

windev2401eval

Agent details | Logs | Diagnostics

Overview

CPU ⓘ0.99 %

View more agent metrics

Memory ⓘ160 MB

Status

Healthy

Last activity10 seconds ago

Last checkin messageRunning

Agent ID2008816d-c530-4d9e-91a7-181ea0cfc00d

Agent policywindows_policy rev. 1

Agent version8.14.1

Host namewindev2401eval

Logging levelinfo

Agent releasestable

Platformwindows

Monitor logsEnabled

Monitor metricsEnabled

Tags-

Integrations

> system-3

Se crea una politica

< View all agent policies

Revision1

Integrations1

Agents1 agent

Last updated onJun 20, 2024

Actions

windows_policy

Integrations | Settings

Search...

Namespace

Add integration

Name ↑	Integration	Namespace	Actions
system-3	System v1.58.2	default	...

☐ Healthy

windev2401eval

windows_policy rev. 1

1.01 %

160 MB

46 seconds ago

8.14.1

...

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

< View all agent policies

Revision2

Integrations2

Agents1 agent

Last updated onJun 20, 2024

Actions

windows_policy

Integrations | Settings

Search...

Namespace

Add integration

Name ↑	Integration	Namespace	Actions
Elastic_defend ⓘ	Elastic Defend v8.14.0	default ⓘ	...
system-3	System v1.58.2	default	...



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-8.12.2-linux-x86_64.tar.gz
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-central1.gcp.cloud.es.io:443 --enrollment-token=RHZXdU5wQUJ0UHVhN0dJY28xZTQ6OHh6VjZlZzZUZ0dFbWBUk81czFRdw==
% 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 want to continue? [Y/n]:Y
[ == ] Service Started [6s] Elastic Agent successfully installed, starting enrollment.
[ == ] Waiting For Enroll... [7s] {"log.level":"info","@timestamp":"2024-06-20T15:01:14.356-0400","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":517},"message":"Starting 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":"2024-06-20T15:01:16.185-0400","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":480},"message":"Restarting 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

[Back to integrations](#)



Custom Logs Package
ECS Field Mapping

Custom Logs

Elastic Agent

Overview Settings Configs

Version 2.3.1

Add Custom Logs

Custom Logs Package


The Custom Logs package is used for ingesting arbitrary log files and manipulating their content/lines by using Ingest Pipelines configuration.

In order to use the package, please follow these steps:

1. [Setup / Install Elastic Agent](#) at the machine where the logs should be collected from
2. Identify the log location at that machine e.g. `/tmp/custom.log` . Note that

Details

Version	2.3.1
Category	Custom, Custom Logs
Subscription	-
License	LICENSE.txt
Changelog	View Changelog



Add Custom Logs integration

Configure an integration for the selected agent policy.

1 **Configure integration**

Integration settings

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

Integration name

log_cowrie_honeypot

Description

logs del honeypot

Optional

[Advanced options](#)

☒ Custom log file

Change defaults ^

Log file path

/home/kali/cowrie.log

[Add row](#)

Path to log files to be collected

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](#)

2 **Where to add this integration?**

[New hosts](#) Existing hosts

Create agent policy

Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name

honeypot_policy

☒ Collect system logs and metrics ⓘ

[Back to integrations](#)

Custom Logs

Elastic Agent

Version 2.3.1 | Agent policies 1 | [Add Custom Logs](#)

[Overview](#) [Integration policies](#) [Assets](#) [Settings](#) [Configs](#)

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
log_cowrie_honey...	v2.3.1	honeypot_p... rev. 2	system	1 minute ago	Add agent	...

Rows per page: 20

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

[View all agents](#)

honeypot

[Agent details](#) [Logs](#) [Diagnostics](#)

Overview

CPU 1.43 %
Memory 168 MB
Status **Healthy**
Last activity 12 seconds ago
Last checkin message Running
Agent ID 71a36f77-20a5-44e...
Agent policy honeypot rev. 3
Agent version 8.14.1
Host name honeypot
Logging level info
Agent release stable
Platform kali
Monitor logs Enabled
Monitor metrics Enabled
Tags -

Integrations

Assign new agent policy

Choose a new agent policy to assign the selected agent to.

Agent policy
honeypot_policy

The selected agent policy will collect data for 2 integrations:
[System](#) [Custom Logs](#)

[Cancel](#) [Assign policy](#)

Actions

- Assign to new policy
- Upgrade agent
- View agent JSON
- Request diagnostics .zip
- Unenroll agent

honeypot

[Agent details](#) [Logs](#) [Diagnostics](#)

Overview

CPU 1.43 % [View more agent metrics](#)
Memory 168 MB
Status **Healthy**

Integrations

- system-2
- log_cowrie_honeypot

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

[Ingest Overview Metrics](#) [Agent Info Metrics](#) [Agent activity](#) [Add Fleet Server](#) [Add agent](#)

Filter your data using KQL syntax

Status 4 Tags 0 Agent policy 4 Upgrade available

Showing 3 agents Clear filters

Healthy 3 Unhealthy 0 Updating 0 Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	honeypot	honeypot_policy rev. 2	1.65 %	168 MB	30 seconds ago	8.14.1	...



Instalación del agente de apache server en Elastic

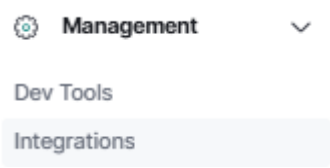
Ponemos en un terminal el código para instalar el agente con el token que nos genera:

```
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=ck1sUk41QUI5U056Z3RnZEVlWg6TTJ5QnE5YndUcm1JTfo0ckJhc0JfQQ==
```

```
root@apache: /home/kali/elastic-agent-8.14.1-linux-x86_64/elastic-agent-8.14.1-linux-x86_64
File Actions Edit View Help

(root@apache)-[/home/kali/elastic-agent-8.14.1-linux-x86_64]
# 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=ck1sUk41QUI5U056Z3RnZEVlWg6TTJ5QnE5YndUcm1JTfo0ckJhc0JfQQ=
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 321M  100 321M    0     0  21.0M      0  0:00:15  0:00:15 --:--:-- 25.7M
elastic-agent-8.14.1-linux-x86_64/elastic-agent.yml
```


Integración de logs de apache server en Elastic



En Management – Integrations

Buscamos y añadimos el Apache HTTP Server

Back to integrations



Apache HTTP Server

Elastic Agent

Version 1.20.0

Add Apache HTTP Server

Overview

Settings

Configs

API reference

Apache Integration

This integration periodically fetches metrics from Apache servers. It can parse access and error logs created by the Apache server.

Compatibility

The Apache datasets were tested with Apache 2.4.12 and 2.4.46 and are expected to work with all versions >= 2.2.31 and >= 2.4.16 (independent from operating system).


Logs

Access Logs

Access logs collects the Apache access logs.

Screenshots

1 of 2



Add Apache HTTP Server integration

Agent policy apache_server

Configure an integration for the selected agent policy.

1

Configure integration

Integration settings

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

Integration name

apache

Description

Optional

Advanced options

Collect logs from Apache instances

Change defaults

Collect logs from third-party REST API (experimental)

Change defaults

Collect metrics from Apache instances

Change defaults

2

Where to add this integration?

New hosts

Existing hosts

Agent policy

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

apache_server

1 agent is enrolled with the selected agent policy.

Back to integrations

Apache HTTP Server

Elastic Agent

Version 1.20.0

Agent policies 1

Add Apache HTTP Server

Overview

Integration policies

Assets

Settings

Configs

API reference

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
apache	v1.20.0	apache_serv... rev. 2	system	54 seconds ago	1	

Rows per page: 20


1

apache



Actions ▾

Agent details Logs Diagnostics

Overview

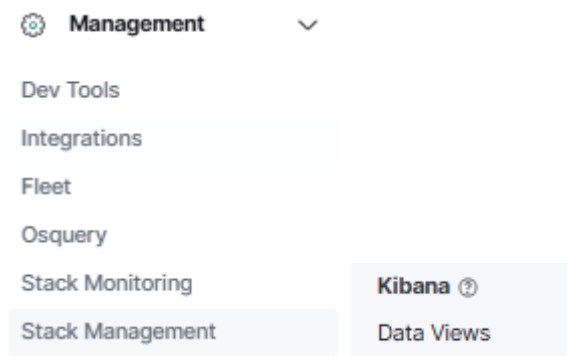
CPU ⓘ	1.19 %	 View more agent metrics
Memory ⓘ	155 MB	
Status	Healthy	
Last activity	35 seconds ago	
Last checkin message	Running	
Agent ID	fc34c1cc-b293-47b3-ba8e-5e24f6599532	
Agent policy	apache_server rev. 2	
Agent version	8.14.1	
Host name	apache	
Logging level	info	
Agent release	stable	
Platform	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

Create data view

Name

Index pattern

Timestamp field

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

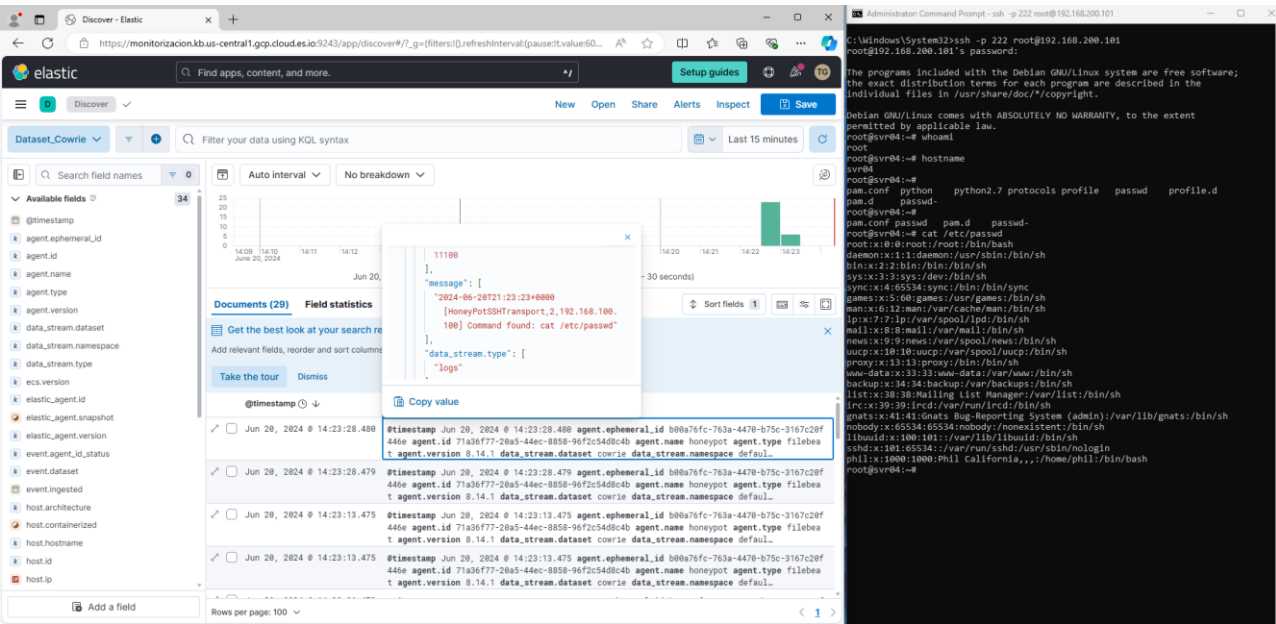
✓ Your index pattern matches 1 source.

All sources	Matching sources
logs-cowrie-default	Data stream

Rows per page: 50

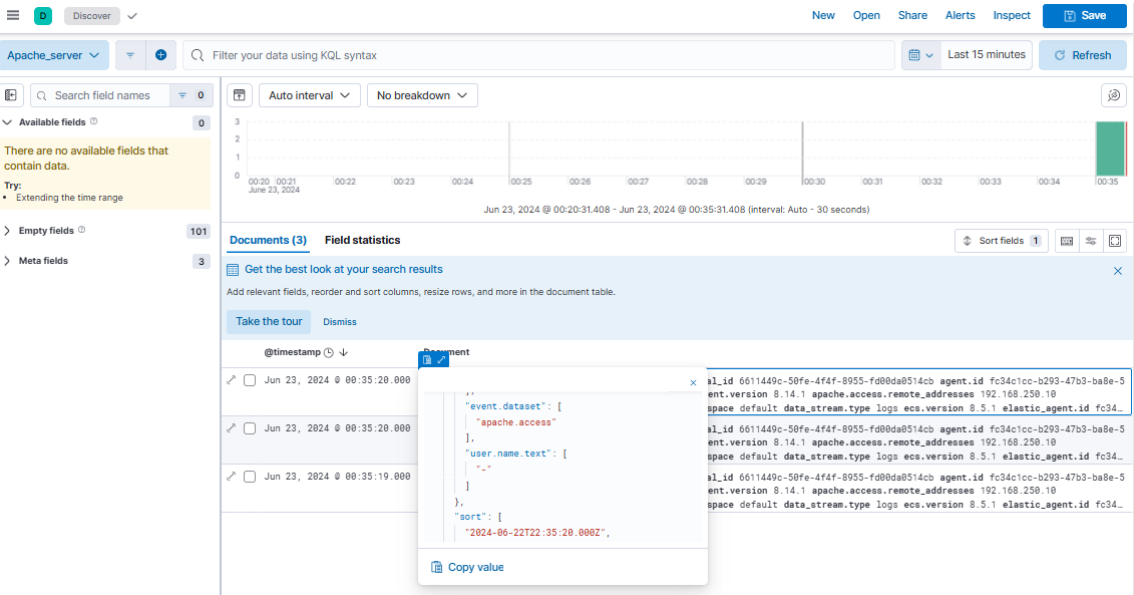
El logs-cowrie-default lo detecta si anteriormente se ha generado para ello un log, por eso habrá que conectarse antes al cowrie por ssh

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

Fleet

Centralized management for Elastic Agents.

[Agents](#)[Agent policies](#)[Enrollment tokens](#)[Uninstall tokens](#)[Data streams](#)[Settings](#)

[Ingest Overview Metrics](#)[Agent Info Metrics](#)

[Agent activity](#)[Add Fleet Server](#)[Add agent](#)

Status4

Tags0

Agent policy5

Upgrade available

Showing 4 agents

[Clear filters](#)

Healthy4

Unhealthy0

Updating0

Offline0

<input type="checkbox"/>	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version	Actions
<input type="checkbox"/>	Healthy	apache	apache_server rev. 2	1.21 %	154 MB	36 seconds ago	8.14.1	...
<input type="checkbox"/>	Healthy	honeypot	honeypot_policy rev. 2	1.22 %	168 MB	31 seconds ago	8.14.1	...
<input type="checkbox"/>	Healthy	windev2401eval	windows_policy rev. 1	1.44 %	163 MB	34 seconds ago	8.14.1	...
<input type="checkbox"/>	Healthy	e0ca55e6605c	Elastic Cloud agent policy ⓘ rev. 5	N/A ⓘ	N/A ⓘ	36 seconds ago	8.14.1 ⓘ	...

Visión global de las políticas

Name	Description	Last update... ↓	Agents	Integrations	Actions
apache_server rev. 2		Jun 20, 2024	1	2	...
windows_policy rev. 1		Jun 20, 2024	1	1	...
honeypot_policy rev. 2		Jun 20, 2024	1	2	...
Elastic Cloud agent policy ⓘ rev. 5	Default agent policy for agents hosted on Elastic Cloud	Jun 20, 2024	1	2	...

Visión de como quedan las políticas

[View all agent policies](#)

Revision2

Integrations2

Agents1 agent

Last updated onJun 20, 2024

Actions

apache_server

[Integrations](#)[Settings](#)

Namespace

[Add integration](#)

Name ↑	Integration	Namespace	Actions
apache	Apache HTTP Server v1.20.0	default ⓘ	...
system-4	System v1.58.2	default	...

[View all agent policies](#)

Revision2

Integrations2

Agents1 agent

Last updated onJun 20, 2024

Actions

windows_policy

[Integrations](#)[Settings](#)

Namespace

[Add integration](#)

Name ↑	Integration	Namespace	Actions
Elastic_defend ⓘ	Elastic Defend v8.14.0	default ⓘ	...
system-3	System v1.58.2	default	...

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	⋮