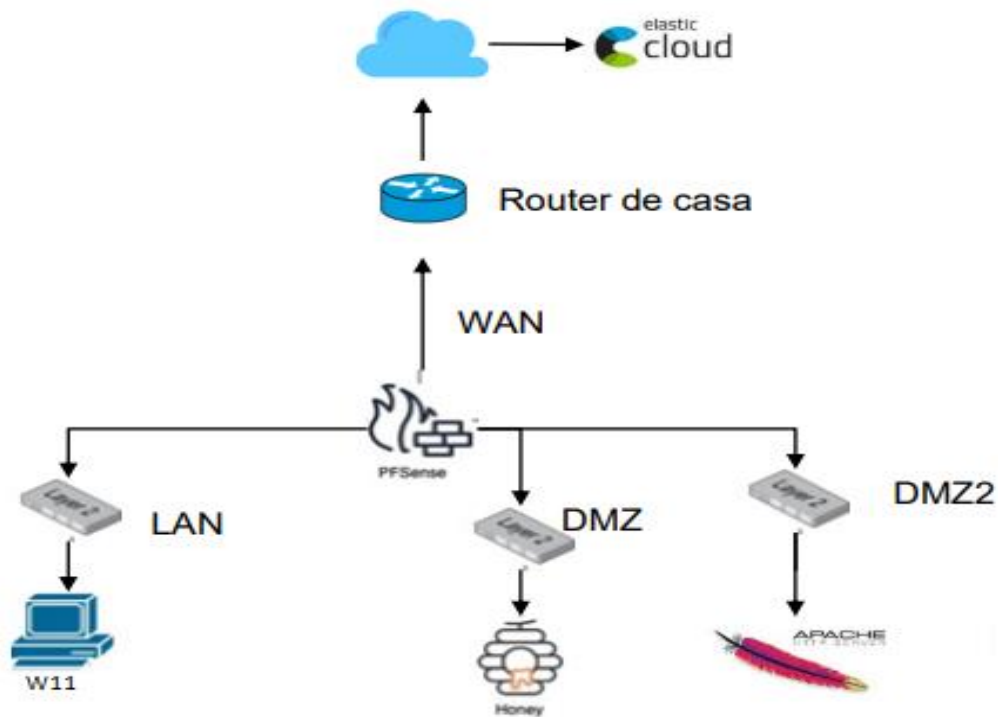


Practica modulo: Blue team Keepcoding

Índice

Esquema red	3
Configuración Pfsense	4
Configuración del Firewall para los accesos a la red externa	30
Configuración de elastic cloud	43
Configuración de un honeypot en la red DMZ	49
Configuración de Apache web server en DMZ_2	51

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 si 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:

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.

Ayuda Modo experto Anterior **Siguiente** Cancelar

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)

Ayuda Anterior **Siguiente** Cancelar

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

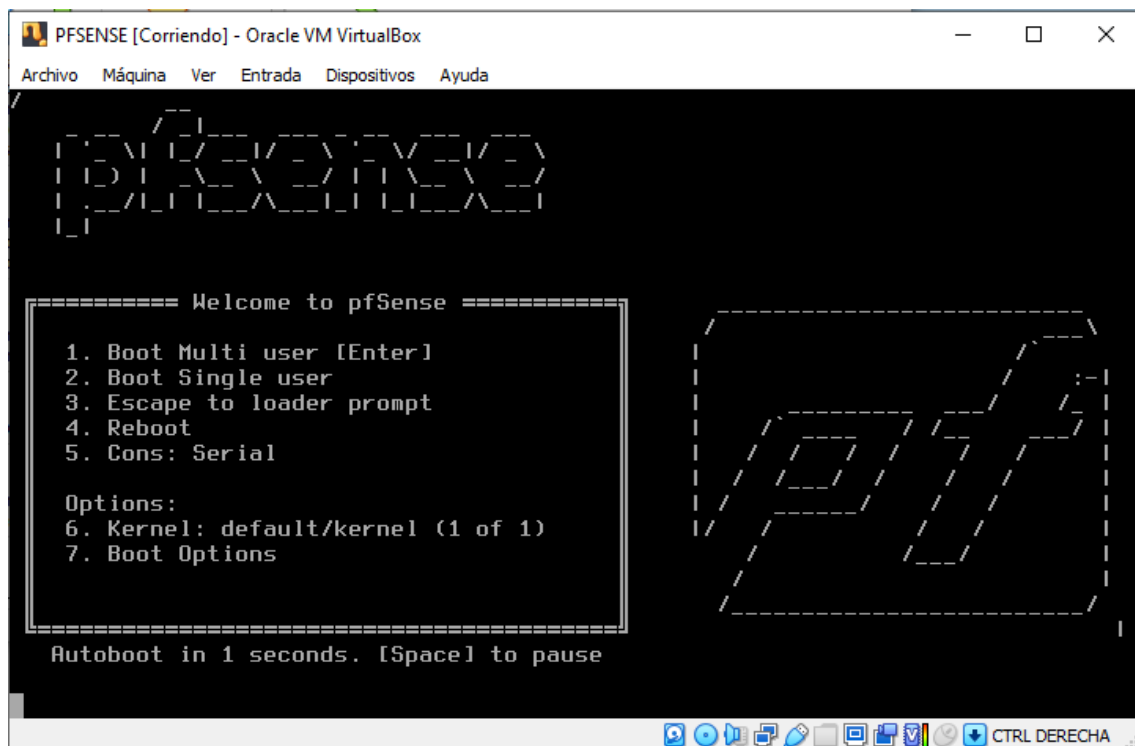
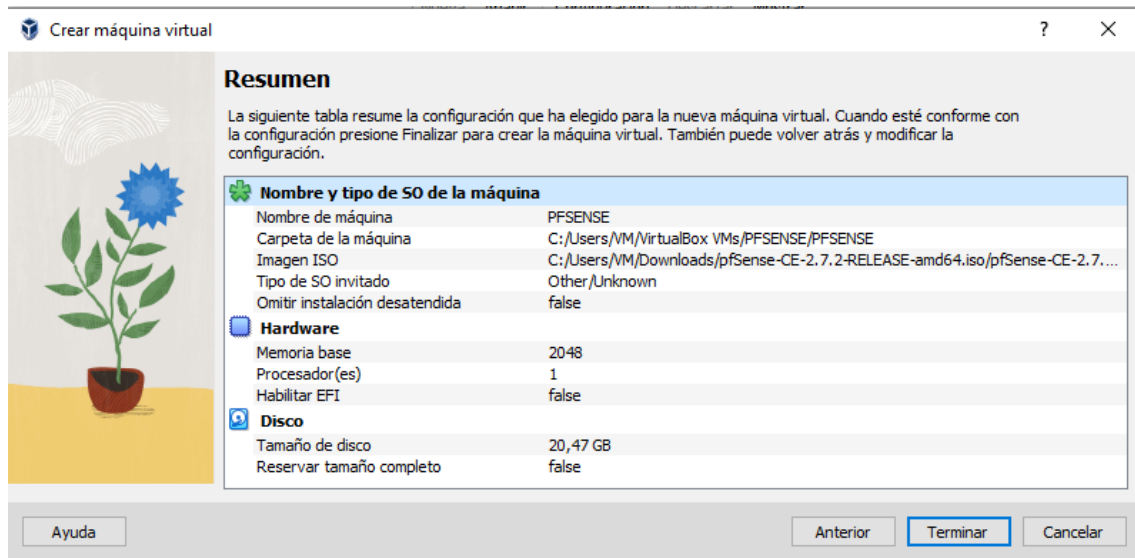
4,00 MB 2,00 TB

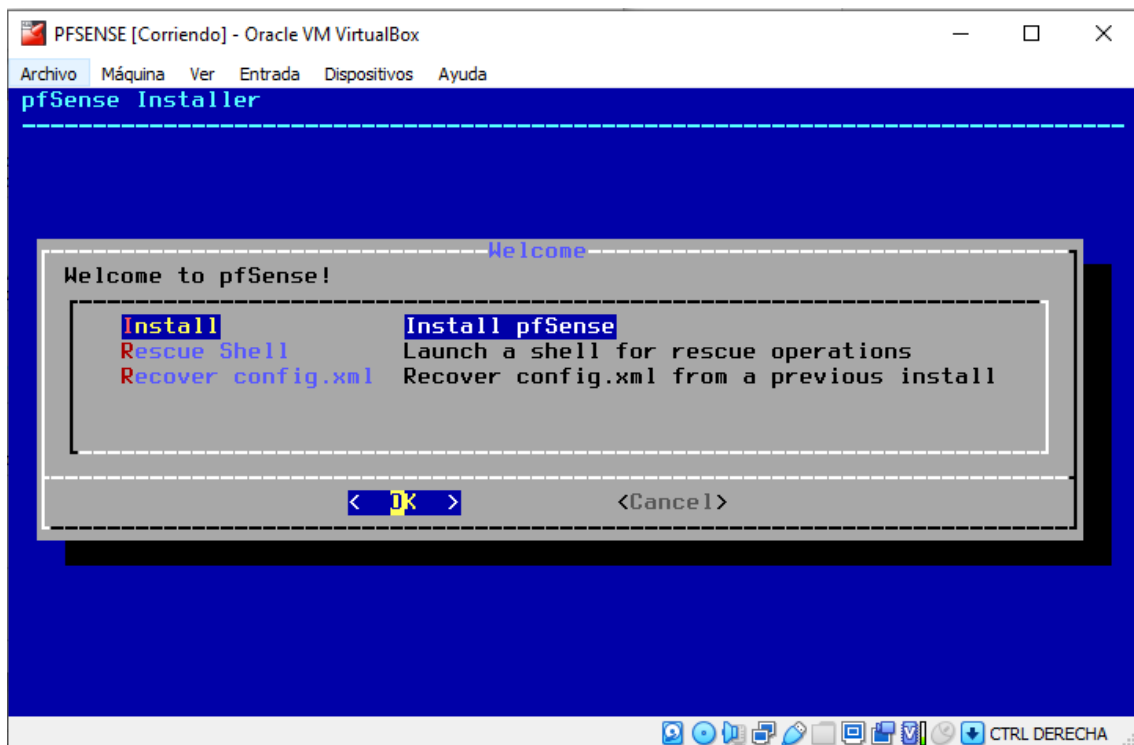
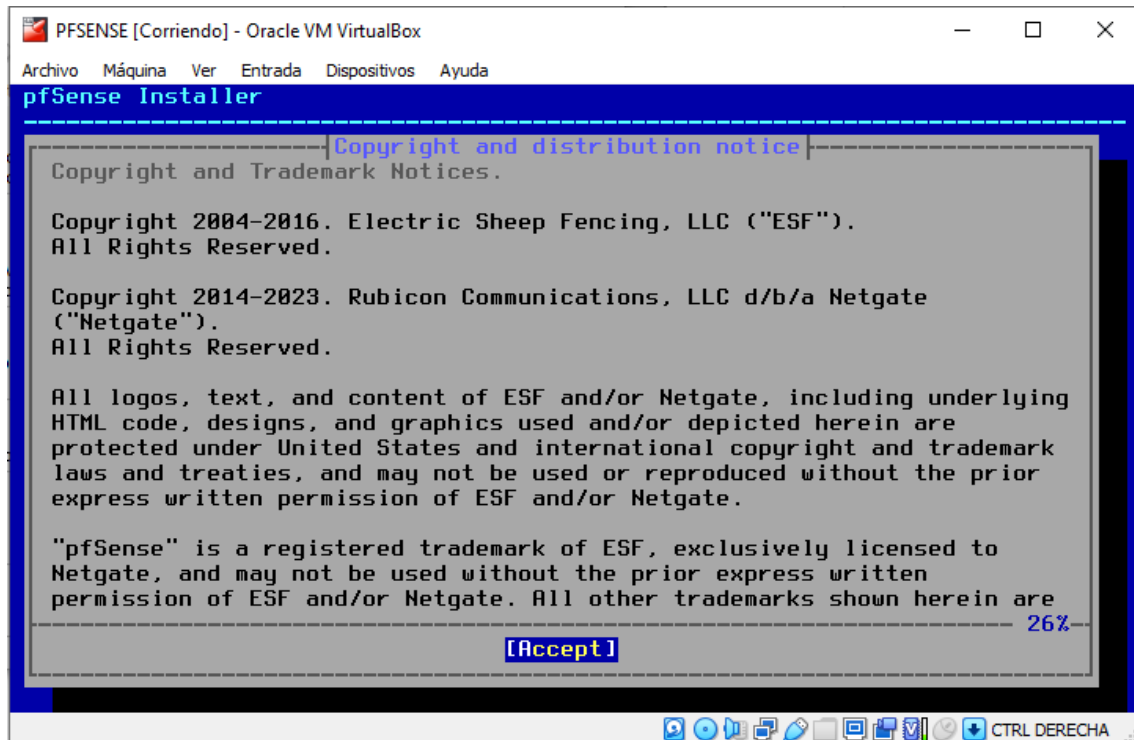
☐ Reservar tamaño completo

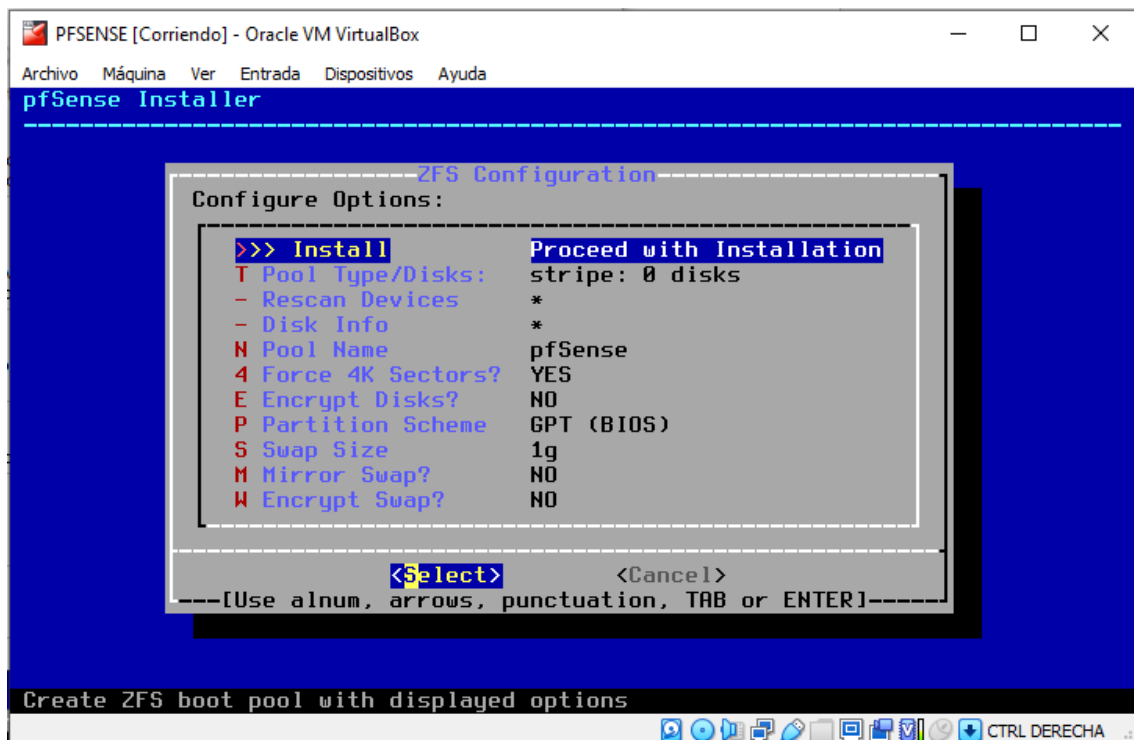
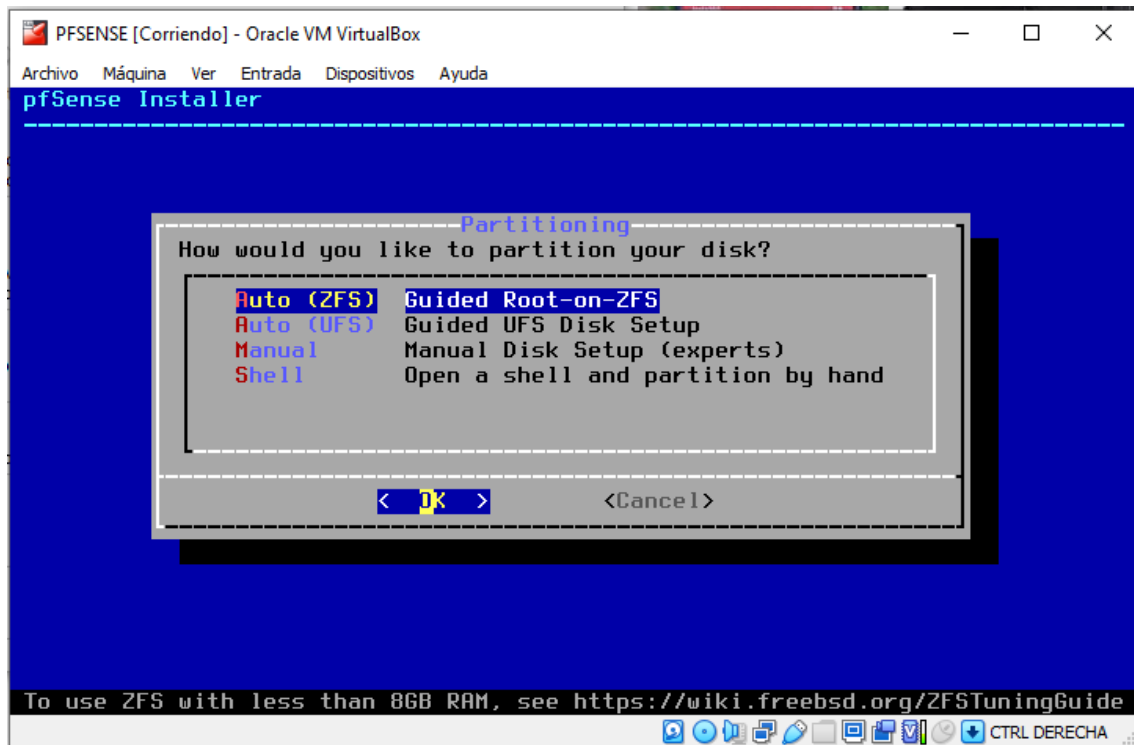
☐ Usar un archivo de disco duro virtual existente

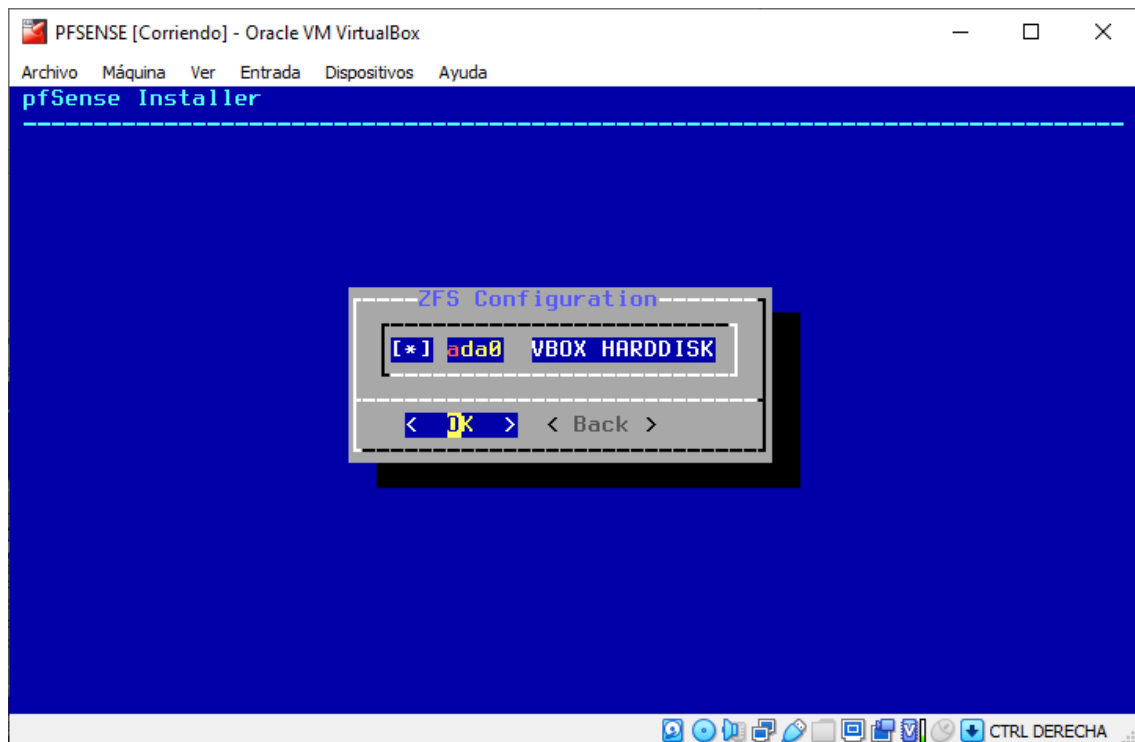
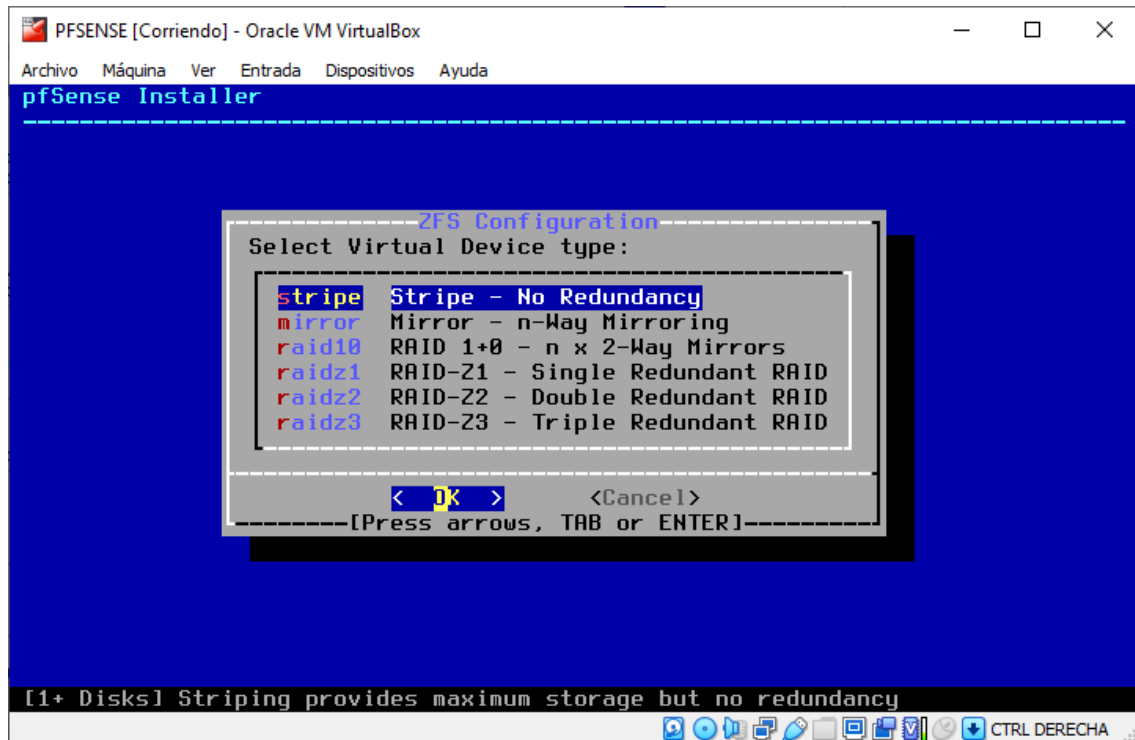
☐ No añadir un disco duro virtual

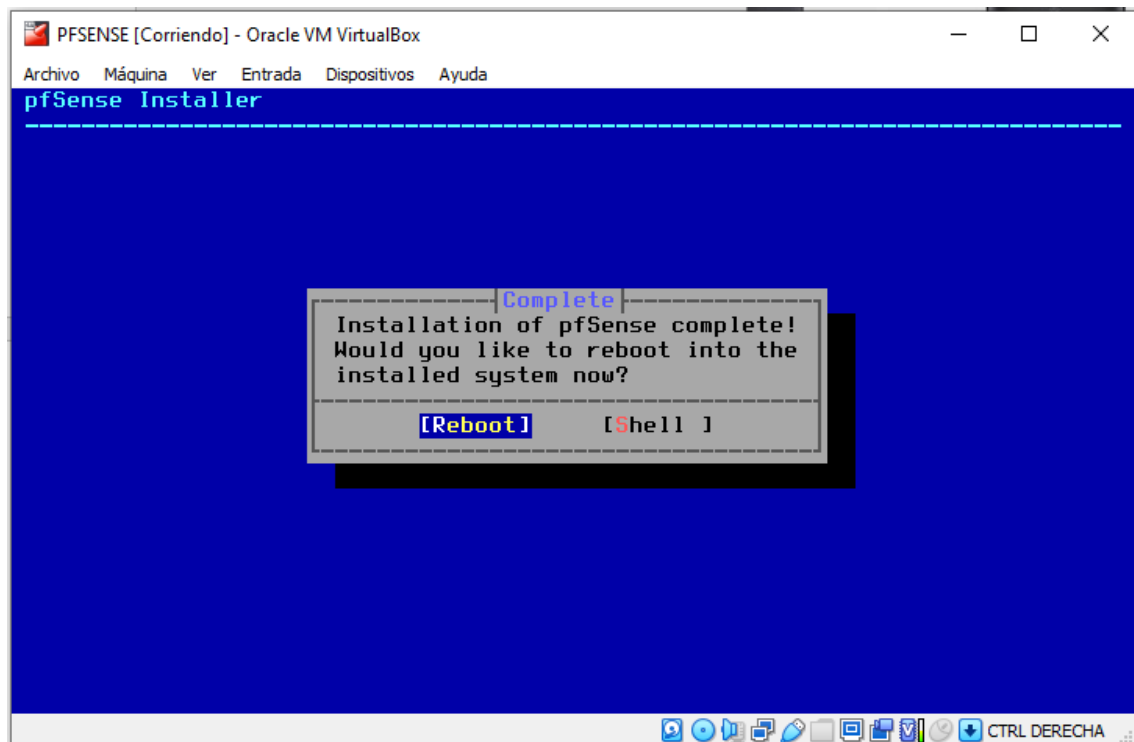
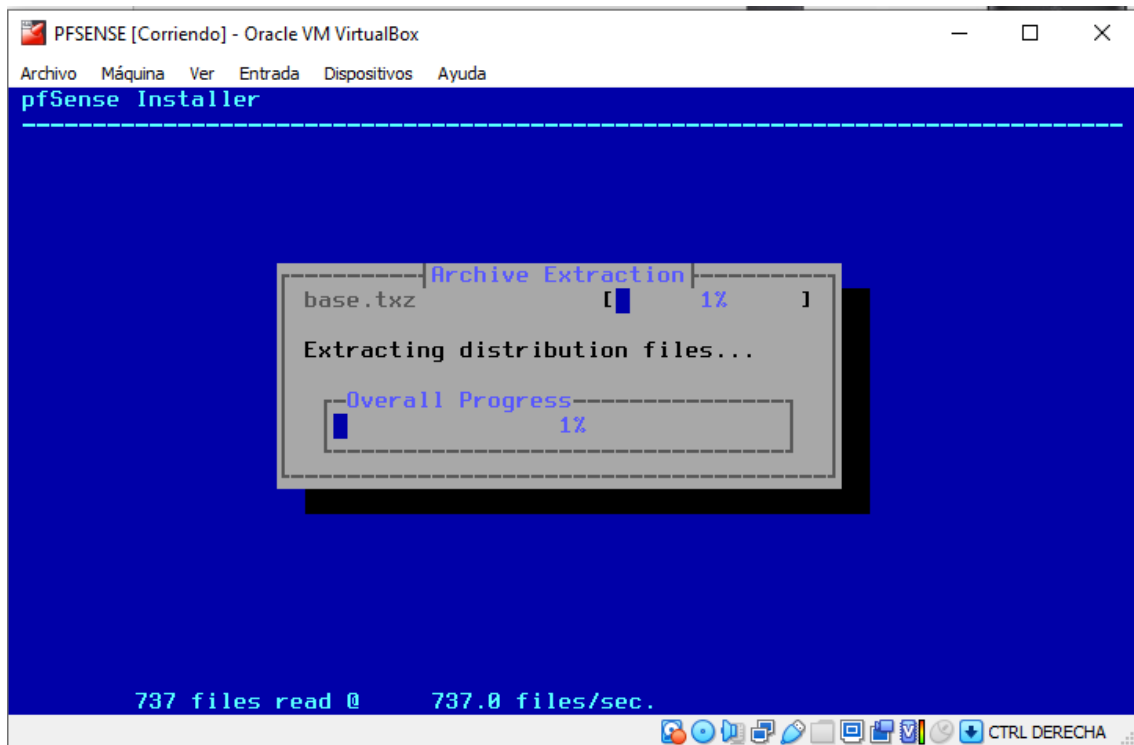
Ayuda Anterior **Siguiente** Cancelar



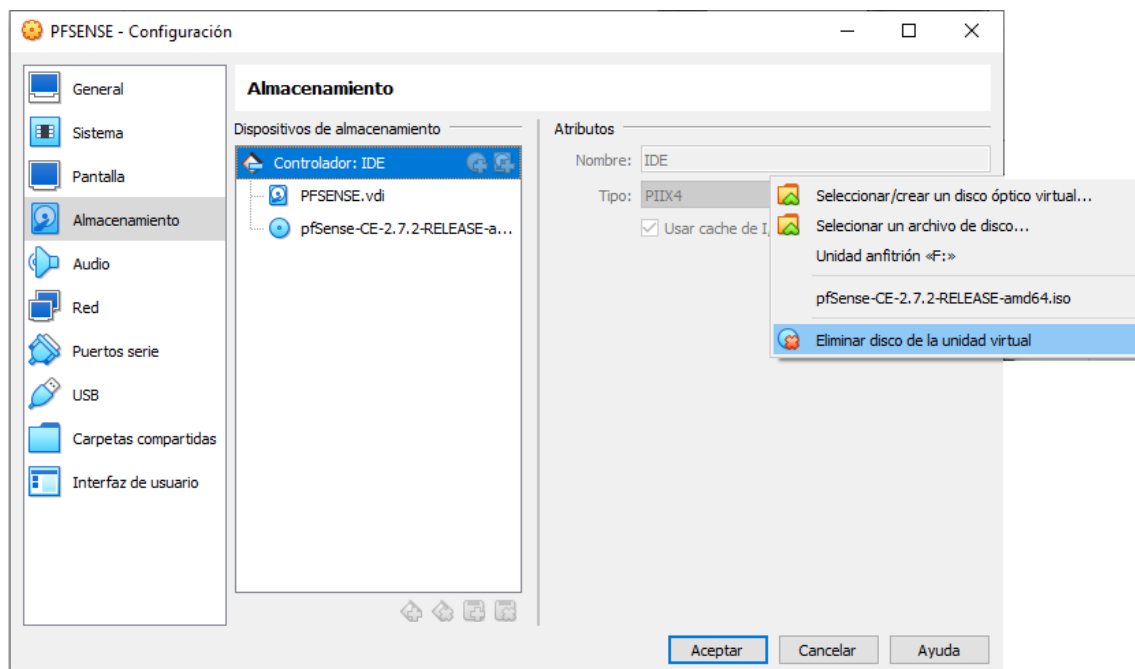




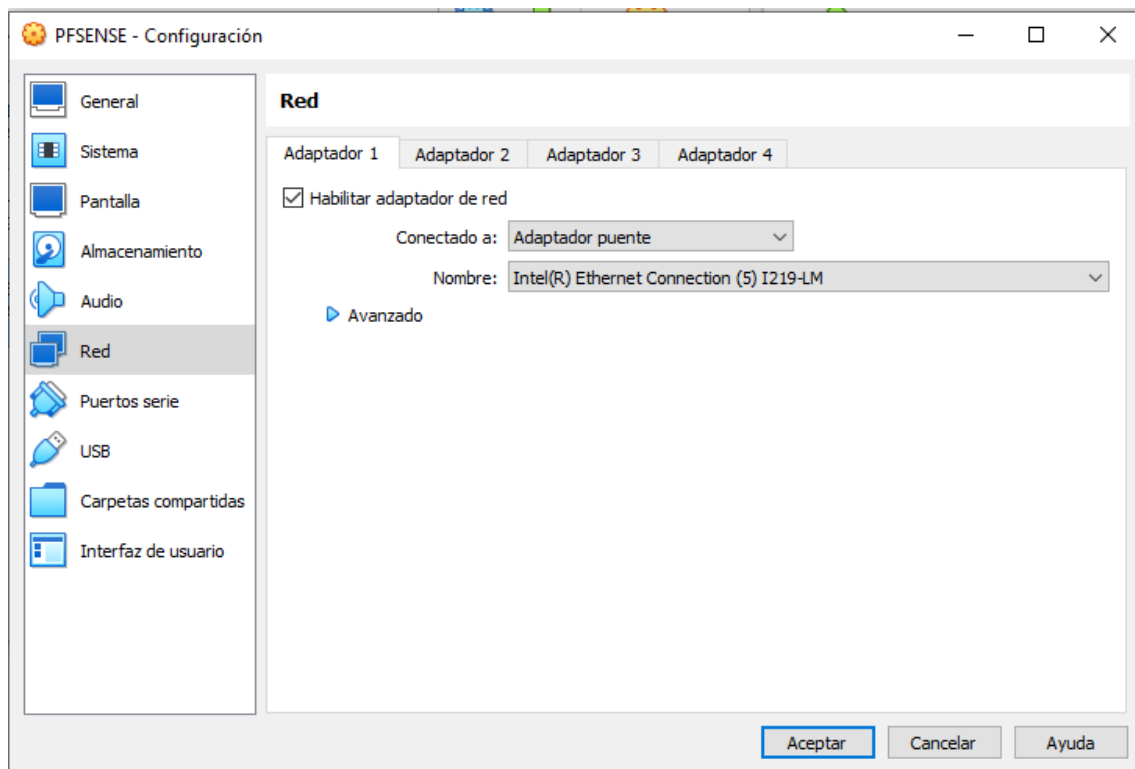


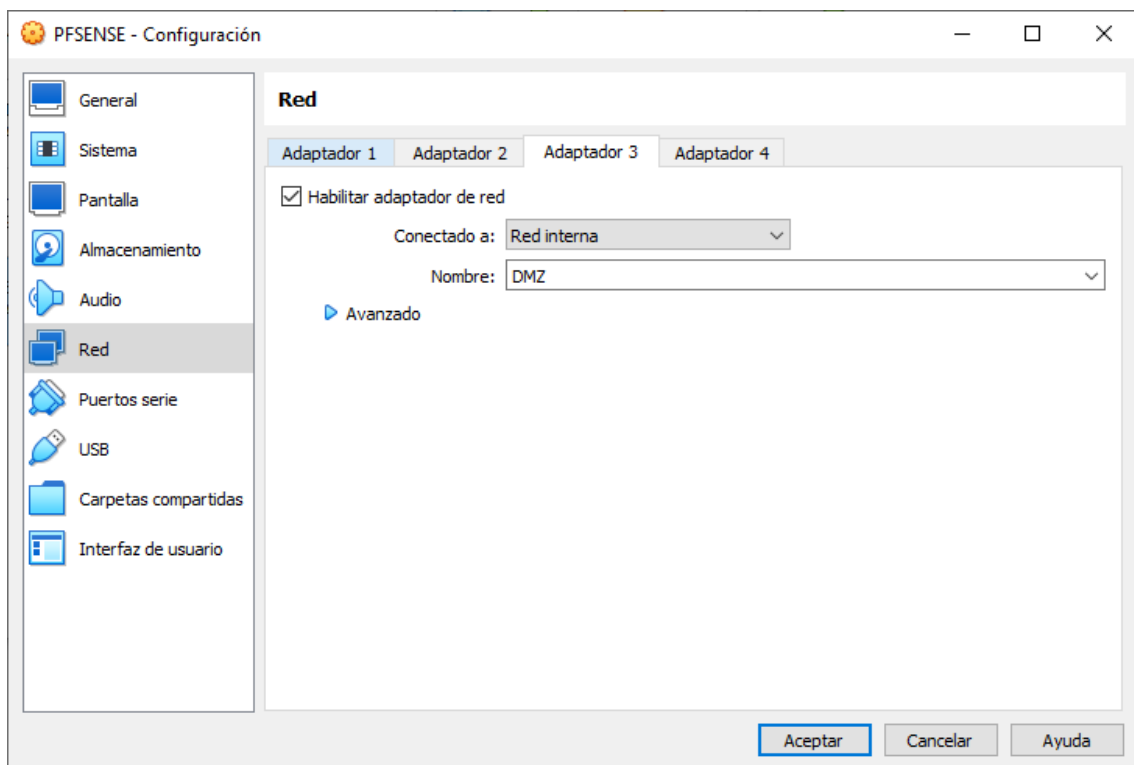
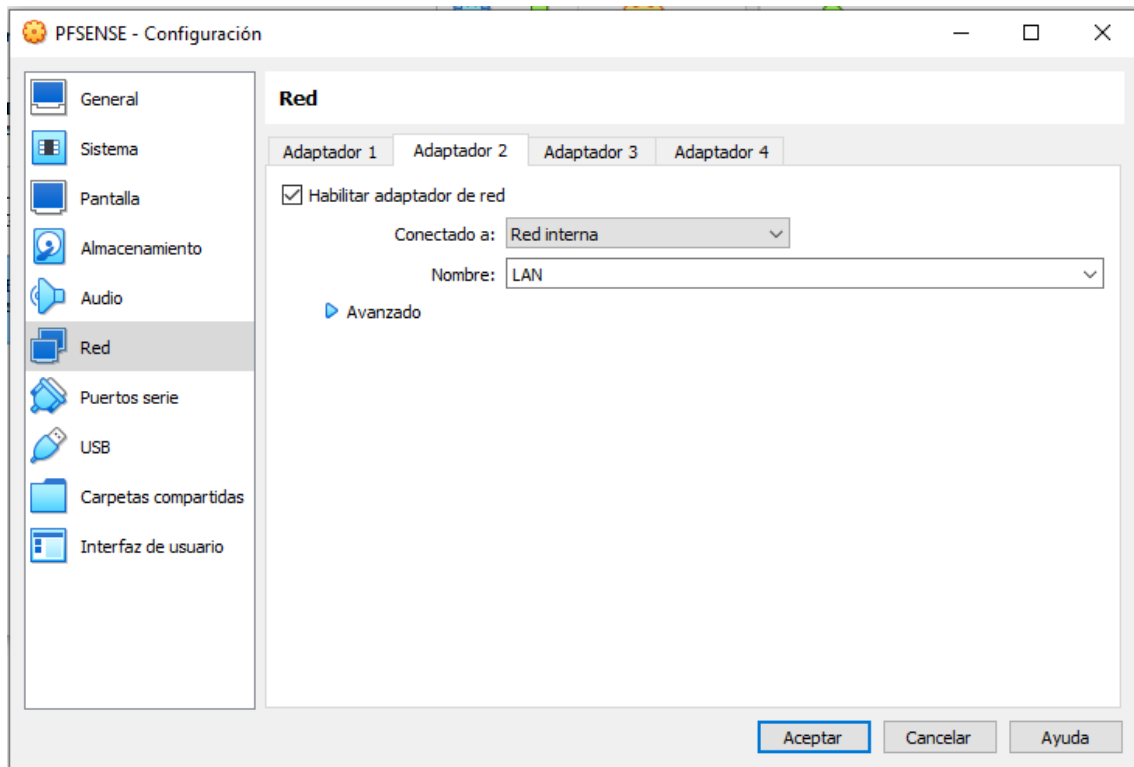


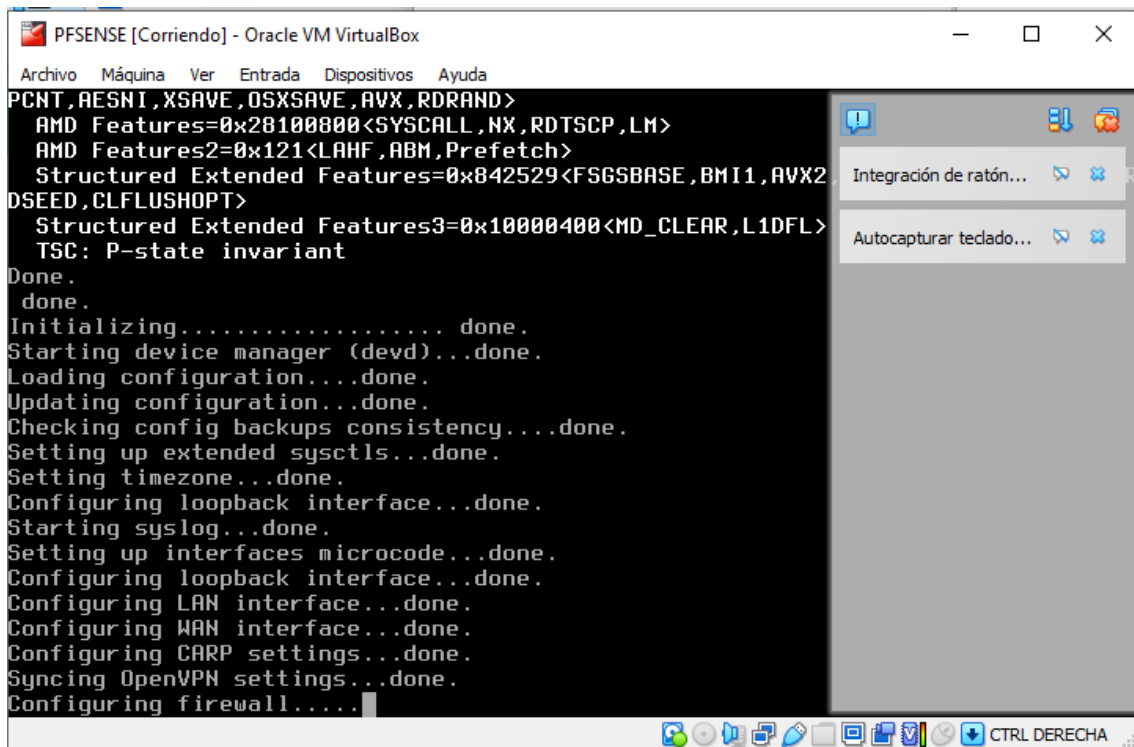
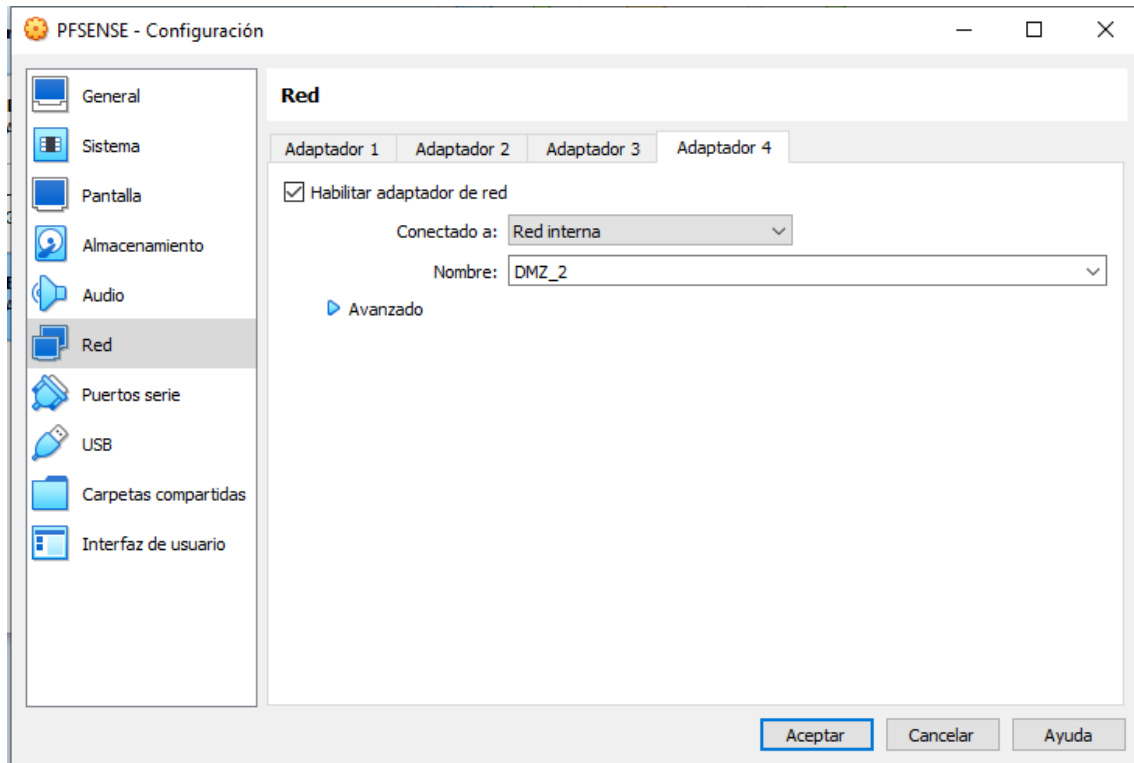
Importante eliminar el disco virtual para que no vuelva a reinstalar el Pfsense

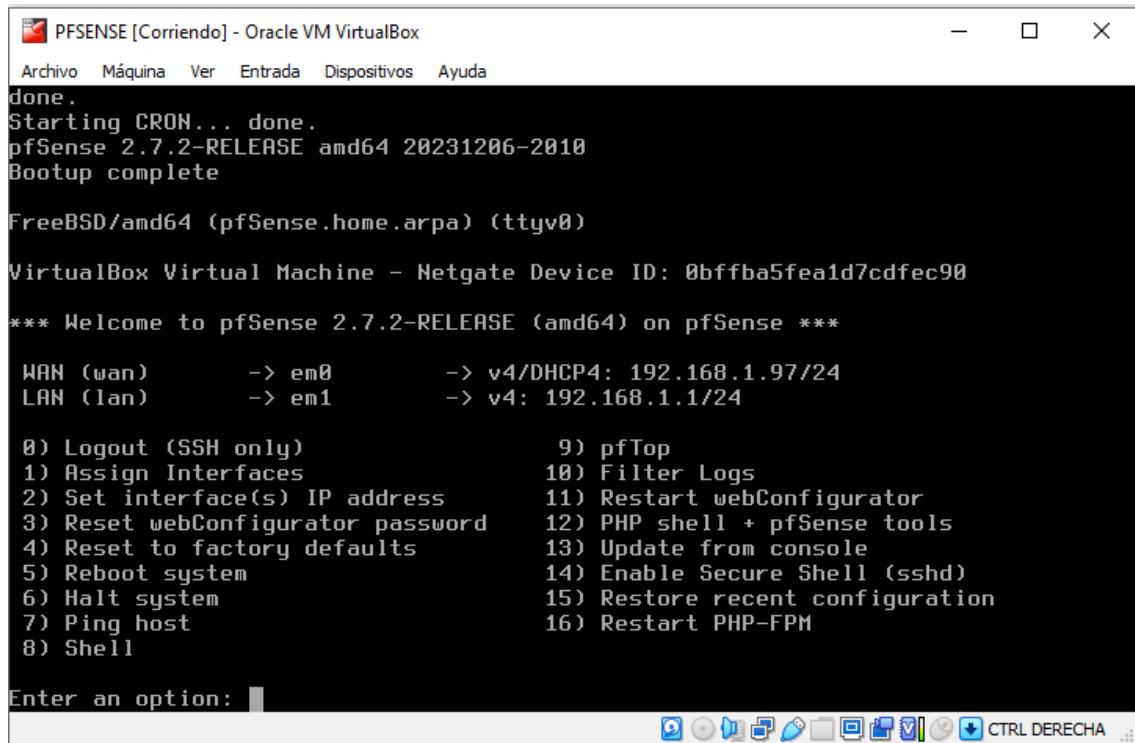


Configuro las tarjetas de red tal y como se requiere para implementar la estructura de red









```
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: 0bffbba5fea1d7cdfec90

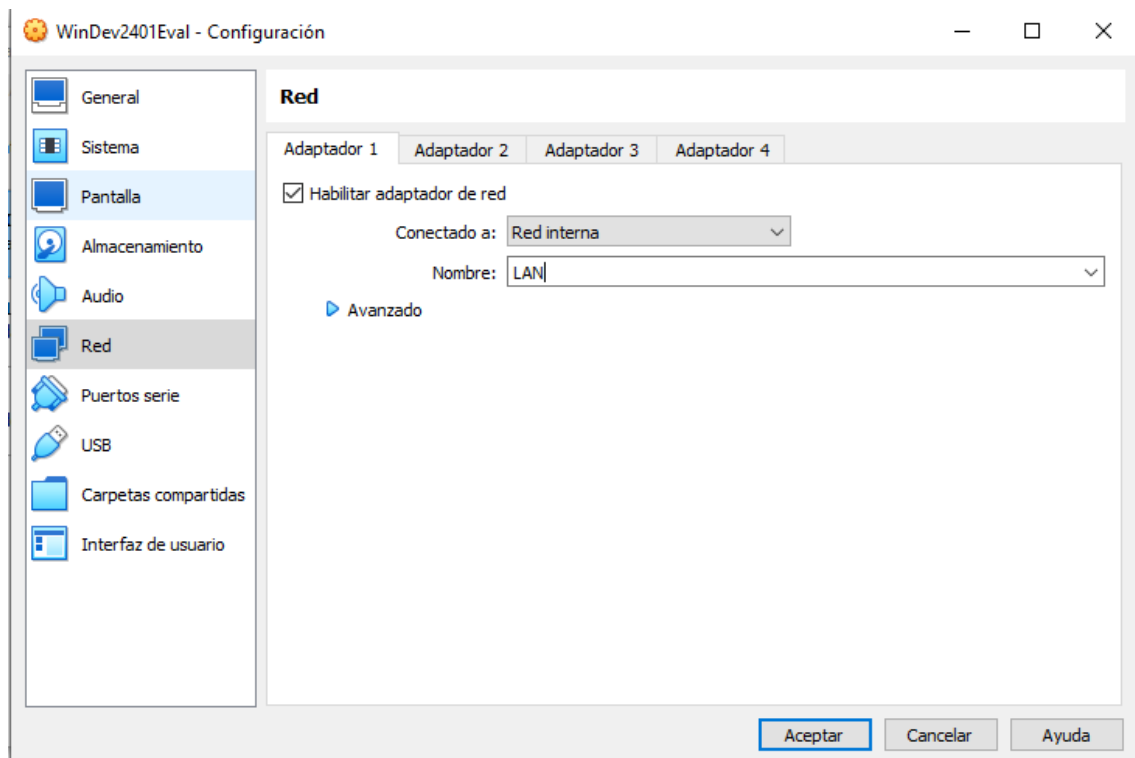
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

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

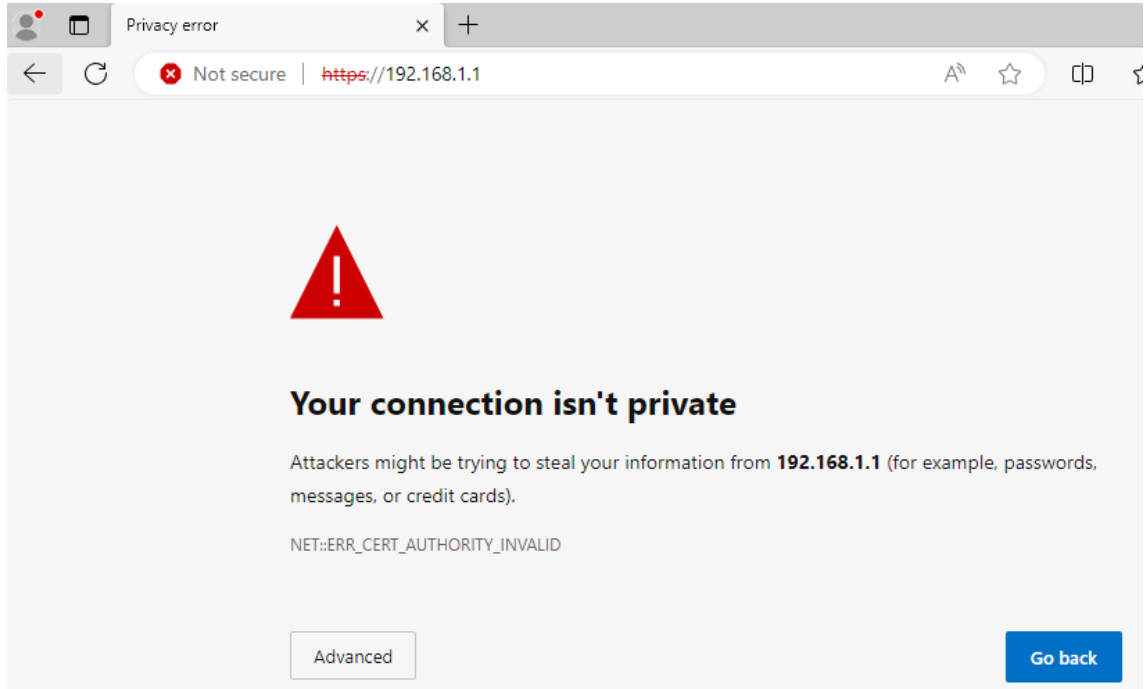
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable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

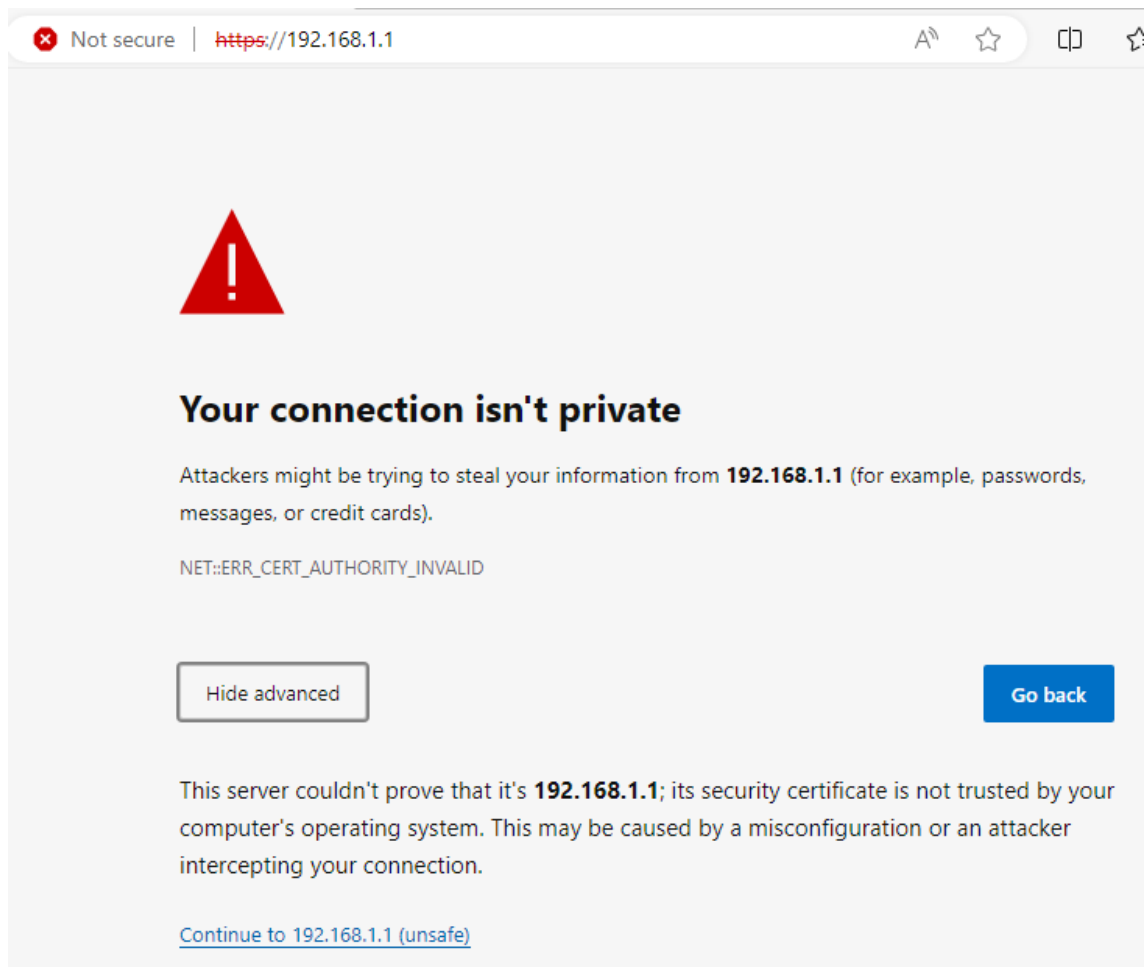
Enter an option:
```

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 coloco la IP de LAN que nos da: 192.168.1.1, ya que esta 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

A screenshot of the pfSense login interface. It has a dark blue background. In the top right corner, the text 'SIGN IN' is displayed in white. Below it, the username 'admin' is entered in a white text field. Underneath the username field is a password field containing five white dots. To the right of the password field is a white eye icon for toggling password visibility. At the bottom right, there is a green rectangular button with the text 'SIGN IN' in white.

Una vez dentro, le doy a siguiente 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.

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.

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

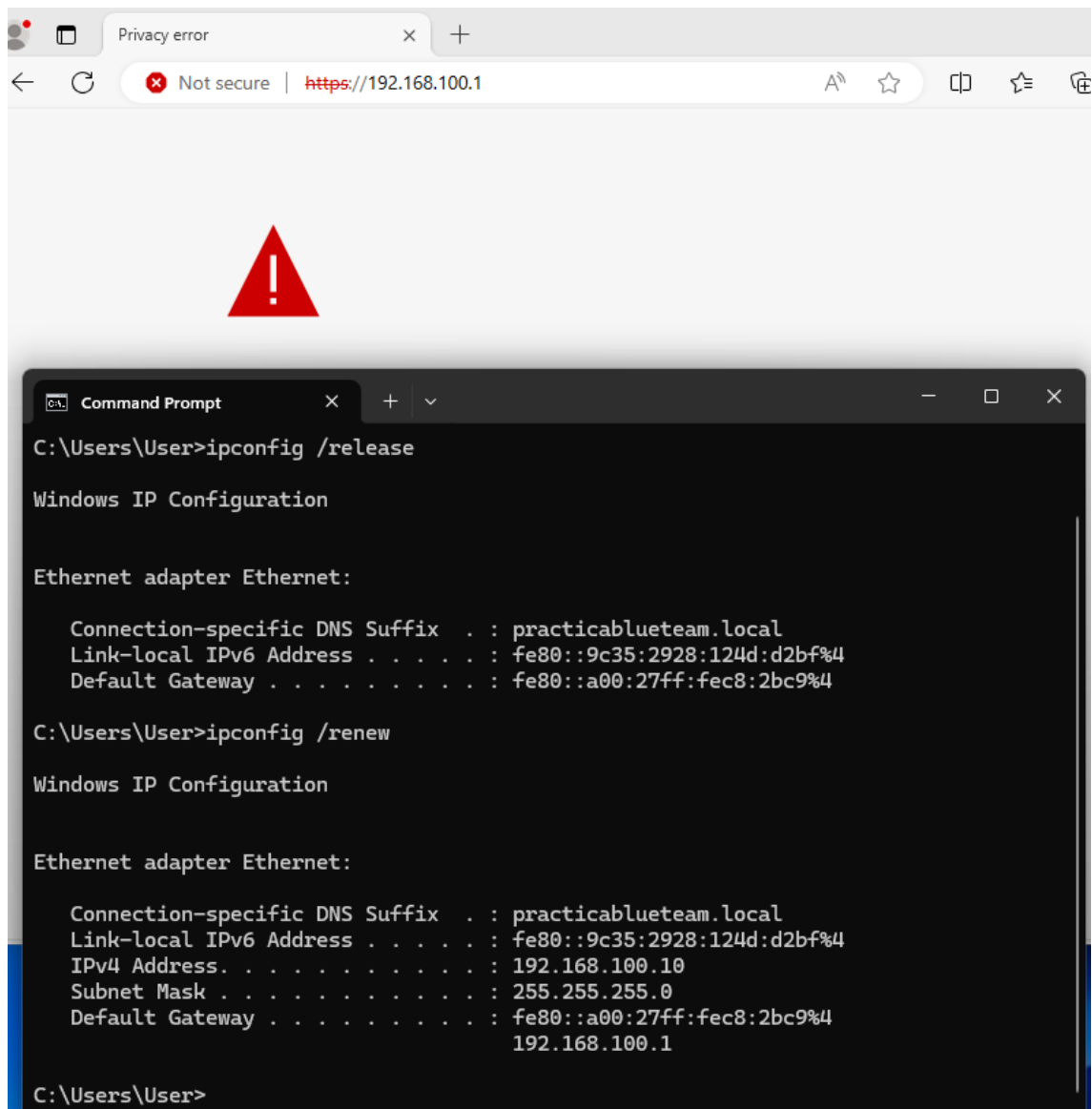
Reload configuration

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

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	<input checked="" type="checkbox"/> Enable DNS resolver
Listen Port	<input type="text" value="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	<input type="checkbox"/> 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	<input type="checkbox"/> 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 esta bien correctamente:

le Tienda Gmail Imágenes

Google

Buscar con Google Voy a tener suerte

Ofrecido por Google en: [català](#) [galego](#) [euskara](#) [English](#)

Services / DHCP Server / LAN

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

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown	<div>Allow all clients</div> <div>When set to Allow all clients, any DHCP client will get an IP address within this scope/range</div>

Primary Address Pool	
Subnet	192.168.100.0/24
Subnet Range	192.168.100.1 - 192.168.100.254
Address Pool Range	<div>192.168.100.100</div> <div>192.168.100.200</div> <div>FromTo</div> <div>The specified range for this pool must not be within the range configured on any other address pool for this interface.</div>
Additional Pools	<div><div>+ Add Address Pool</div><div>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</div></div>

Server Options	
WINS Servers	<div>WINS Server 1</div> <div>WINS Server 2</div>
DNS Servers	<div>192.168.100.1</div> <div>1.1.1.1</div> <div>8.8.8.8</div> <div>DNS Server 4</div>

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

 COMMUNITY EDITION

Interfaces / OPT1 (em2)

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

192.168.200.1

/

24

IPv4 Upstream gateway

None

+ 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](#).

Configuro la interfaz DMZ_2 con la subred 192.168.250.1

Interfaces / OPT2 (em3)

General Configuration

Enable

☒ Enable interface

Description

DMZ_2

Enter a description (name) for the interface here.

IPv4 Configuration Type

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.

LAN DMZ DMZ_2

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input type="checkbox"/> 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	<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	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	<input type="text" value="192.168.200.1"/>
<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>	

Configuración DHCP server DMZ_2

Services / DHCP Server / DMZ_2		    
<p>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.</p>		
<p>LAN DMZ <u>DMZ_2</u></p>		
General DHCP Options		
DHCP Backend	ISC DHCP	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ_2 interface	
BOOTP	<input type="checkbox"/> 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	<input type="text" value="192.168.250.100"/>	<input type="text" value="192.168.250.150"/>
	From	To
<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	+ Add Address Pool	
<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	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
<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>	

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.

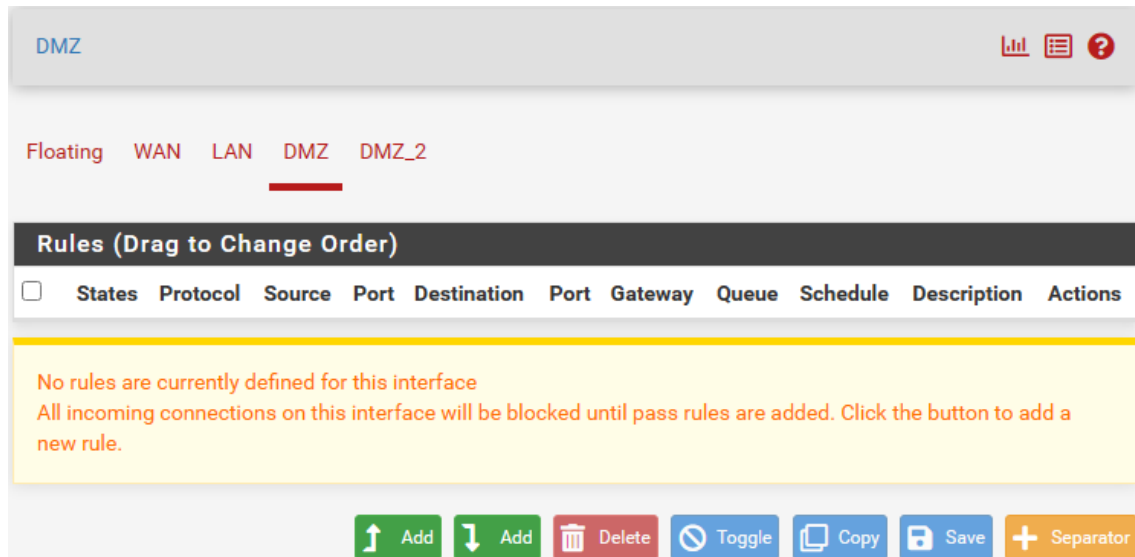
Port	80	HTTP	 Delete
	443	HTTPS	 Delete

Guardo y aplico cambios

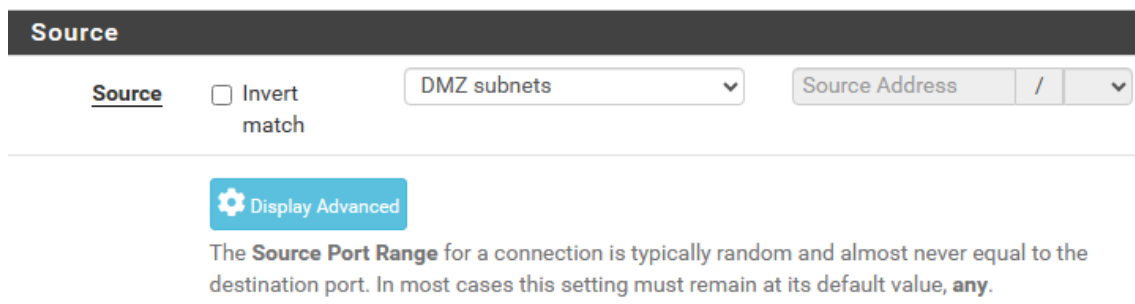
Configuración de las reglas en el firewall

Para la red LAN de manera predeterminada ya tiene los accesos puestos en Pfsense

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 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	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)

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

☐ 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

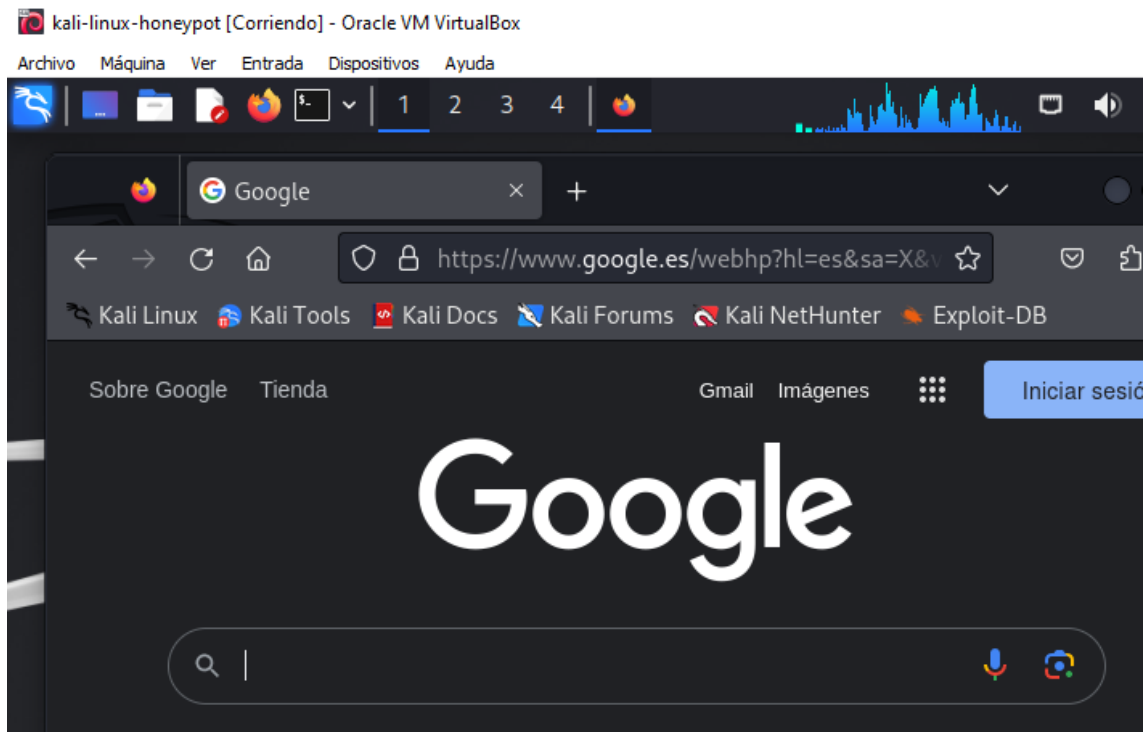
permitir trafico DNS

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	<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>LAN 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 LAN</div>

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 como quedan las reglas configuradas

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"/>	✓ 0/3 KiB	IPv4 ICMP any	*	*	*	*	*	none		ping	   
<input type="checkbox"/>	✓ 0/22 KiB	IPv4 UDP	DMZ subnets	*	*	53 (DNS)	*	none		permitir trafico DNS	   
<input type="checkbox"/>	✓ 2/2.83 MiB	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	<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)

DNS (53)

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

☐ Log packets that are handled by this rule

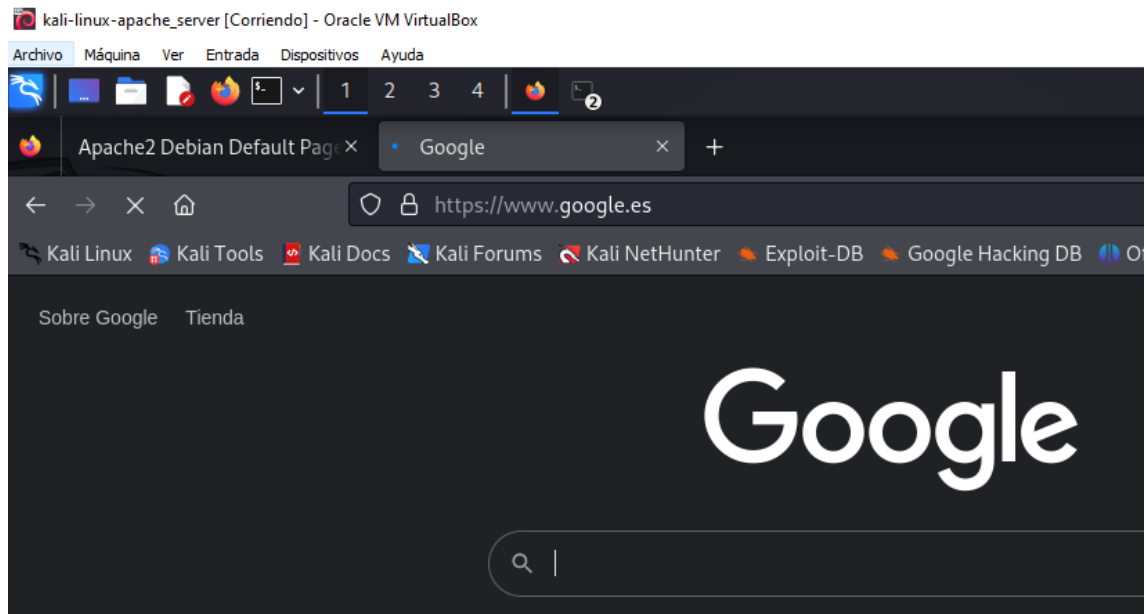
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

permitir trafico DNS

Guardo y aplico cambios

Compruebo que tenga salida y trafico web



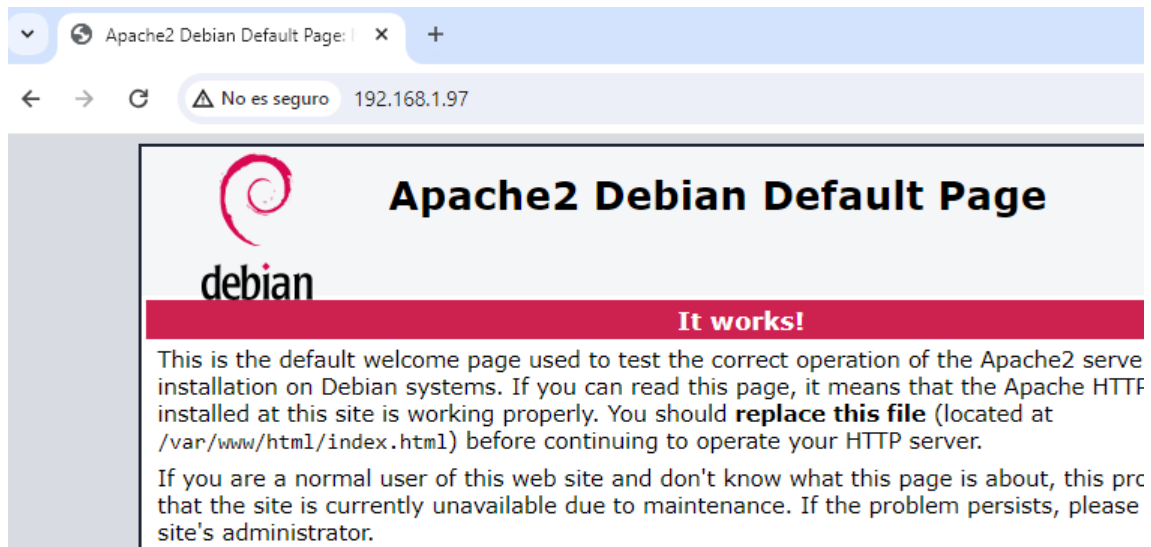
Configuración NAT

Configuración para DMZ_2 servidor apache

Firewall / NAT / Port Forward / Edit			
Edit Redirect Entry			
Disabled	<input type="checkbox"/> Disable this rule		
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.		
Interface	WAN <small>Choose which interface this rule applies to. In most cases "WAN" is specified.</small>		
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>		
Protocol	TCP/UDP <small>Choose which protocol this rule should match. In most cases "TCP" is specified.</small>		
Source	<input type="button" value="Display Advanced"/>		
Destination	<input type="checkbox"/> Invert match.	WAN address <small>Type</small>	Address/mask <small>/</small>
Destination port range	HTTP <small>From port</small>	Custom <small>To port</small>	HTTP <small>Custom</small>
<small>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.</small>			
Redirect target IP	Address or Alias <small>Type</small>		192.168.250.100 <small>Address</small>

192.168.250.100 es donde se encuentra el servidor apache

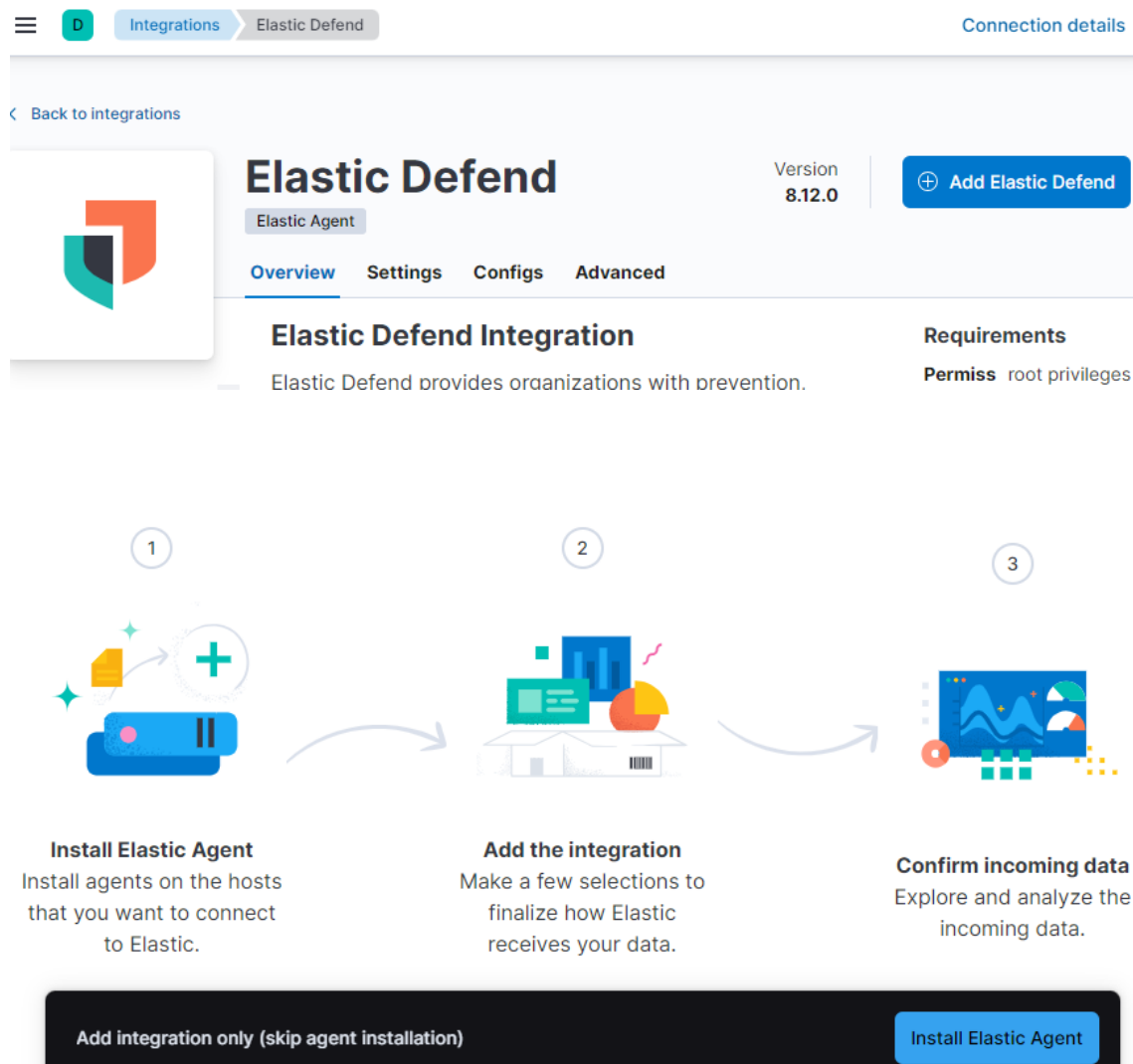
Compruebo que se tiene acceso desde fuera



Configuración de elastic cloud



Me registro y añado el elastic defend

The image shows the "Elastic Defend" integration setup page in the Elastic Cloud console. At the top, there's a breadcrumb trail: "Integrations > Elastic Defend". A "Connection details" link is on the right. The main header for "Elastic Defend" includes the "Elastic Agent" label, the version "8.12.0", and a button to "Add Elastic Defend". Below this, there are tabs for "Overview", "Settings", "Configs", and "Advanced". The "Overview" tab is active, showing the "Elastic Defend Integration" section with a brief description: "Elastic Defend provides organizations with prevention." To the right, under "Requirements", it lists "Permissions: root privileges". A three-step process diagram is shown below: 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.), and 3. "Confirm incoming data" (Explore and analyze the incoming data.). At the bottom, there are two options: "Add integration only (skip agent installation)" and a button to "Install Elastic Agent".

Integración del agente en el Windows 11

1 Install Elastic Agent on your host

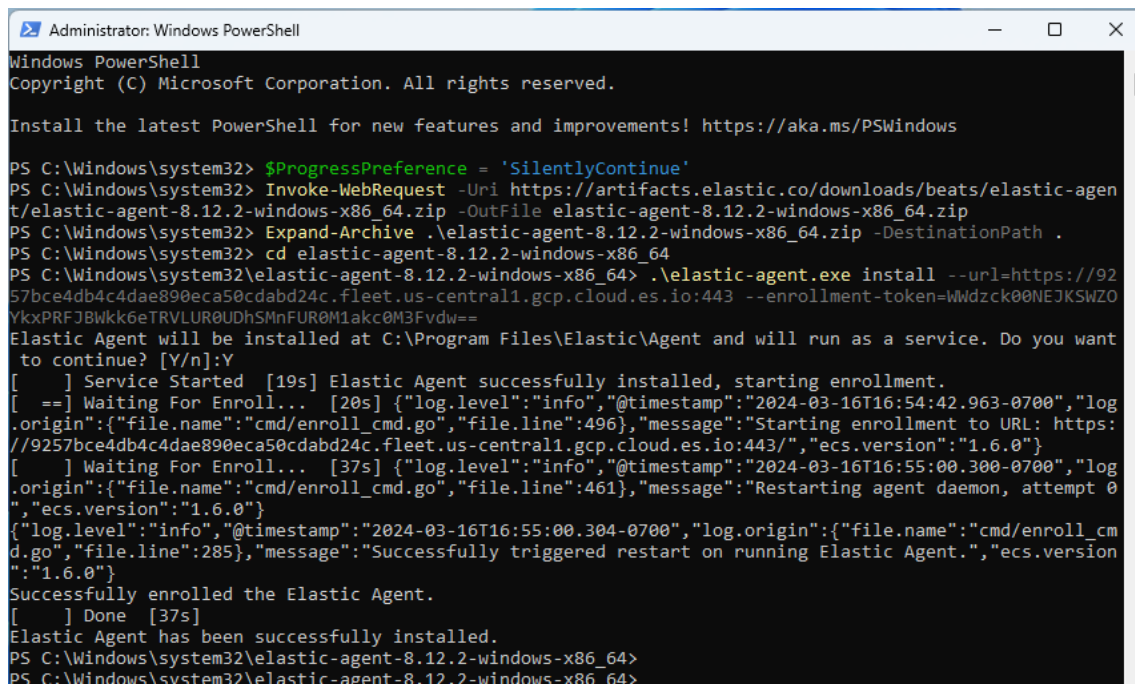
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation 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 -OutFile elastic-agent-8.12.2-windows-x86_64.zip
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-central1.gcp.cloud.es.io:443 --enrollment-token=WWdzck00NEJKSWZ0YkxPRFJBWkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
```

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=WWdzck00NEJKSWZ0YkxPRFJBWkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
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 del agente en el honeypot y en el servidor apache (mismo procedimiento)

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@kali)-[~]
└─$ 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-central1.gcp.cloud.es.io:443/
Wkk6eTRVLUR0UDhSMnFUR0M1akc0M3Fvdw==
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 552M 100 552M    0     0 9668k      0  0:00:58  0:00:58 --:--:-- 10.8M
elastic-agent-8.12.2-linux-x86_64/README.md
elastic-agent-8.12.2-linux-x86_64/elastic-agent.reference.yml
elastic-agent-8.12.2-linux-x86_64/elastic-agent.yml
elastic-agent-8.12.2-linux-x86_64/LICENSE.txt
elastic-agent-8.12.2-linux-x86_64/NOTICE.txt
elastic-agent-8.12.2-linux-x86_64/.build_hash.txt
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/.build_hash.txt
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/LICENSE.txt
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/NOTICE.pf-elastic-collector.txt
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/NOTICE.pf-elastic-symbolizer.txt
```

```
Elastic Agent will be installed at /opt/ElasticAgent and will run as a service. Do you want to continue? [Y/n]:Y
[ == ] Service Started [13s] Elastic Agent successfully installed, starting enrollment.
[ == ] Waiting For Enroll ... [13s] {"log.level":"info","@timestamp":"2024-03-16T20:05:43.470-0400","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 ... [20s] {"log.level":"info","@timestamp":"2024-03-16T20:05:50.192-0400","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":"2024-03-16T20:05:50.196-0400","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 [20s]
Elastic Agent has been successfully installed.
```

We'll save your integration with our recommended defaults.




✓ Windows, macOS, and Linux event collection

You can edit these settings later in the Elastic Defend integration policy. [Learn more](#)

Go back

Confirm incoming data

[Back to integrations](#)



Elastic Defend

Elastic Agent

Version 8.12.0 | Agent policies 1

[+ Add Elastic Defend](#)

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

Views 1

[Hosts](#)

View endpoints in Security app

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](#)

[Status 4](#) [Tags 0](#) [Agent policy 3](#) [Upgrade available](#)

Showing 4 agents [Clear filters](#) [Healthy 4](#) [Unhealthy 0](#) [Updating 0](#) [Offline 0](#)

<input type="checkbox"/>	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version
<input type="checkbox"/>	Healthy	honeypot	My first agent policy rev. 2	0.07 %	27 MB	22 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	apache	My first agent policy rev. 2	N/A ⓘ	N/A ⓘ	38 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	winddev2401eval	My first agent policy rev. 2	0.13 %	26 MB	12 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	5c02420b4e95	Elastic Cloud agent policy rev. 5	N/A ⓘ	N/A ⓘ	28 seconds ago	8.12.2

Se crean las politicas para el honeypot, apache y w11 para recoger los logs del sistema

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings				
<input type="text" value="Filter your data using KQL syntax"/>		Reload	+ Create agent	
Name	Description	Last up... ↓	Agents	Integrations
apache rev. 1		Mar 17, 2024	0	1
w11 rev. 1		Mar 17, 2024	0	1
honeypot rev. 1		Mar 17, 2024	1	1

Y se asignan respectivamente

<input type="checkbox"/>	Healthy	honeypot	honeypot rev. 1	1.49 %	145 MB	25 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	apache	apache rev. 1	N/A ⓘ	N/A ⓘ	13 seconds ago	8.12.2
<input checked="" type="checkbox"/>	Healthy	winddev2401eval	w11 rev. 1	0.12 %	26 MB	27 seconds ago	8.12.2

En la política de apache añado la integración para los logs de apache HTTP server

apache		2	2	1 agent	Mar 17, 2024	Actions
Integrations Settings						
Search...						
		Namespace		Add integration		
Name ↑	Integration		Namespace		Actions	
apache-1 ⓘ	Apache HTTP Server v1.17.0		default		...	
system-3	System v1.54.0		default		...	

Compruebo en discover los logs que va generando

Discover

NewOpenShareAlertsInspectSave

logs-*

Filter your data using KQL syntax

Today

Search field names

0

Available fields 1370

@timestamp

agent.build.original

agent.ephemeral_id

agent.id

agent.name

agent.type

agent.version

cloud.account.id

cloud.availability_zone

cloud.image.id

cloud.instance.id

cloud.instance.name


cloud.machine.type

cloud.project.id

cloud.provider

101,822 hits

Break down by Select field



Mar 17, 2024 @ 00:00:00.000 - Mar 17, 2024 @ 23:59:59.999 (interval: Auto - 30 minutes)

DocumentsField statistics

1 field sorted

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tourDismiss

@timestamp

Document

☒

Mar 17, 2024 @ 02:24:38.763

@timestamp

Mar 17, 2024 @ 02:24:38.763

agent.ephemeral_id

5e0768c8-924c-4f33-b7a9-6f0abb5f1c93

agent.id

87e1c1b2-e153-4a59-8938-0df223d0ab...

Creo un data view con para los logs de apache

Create data view

Name
logs_apache

Index pattern
logs*

Timestamp field
@timestamp

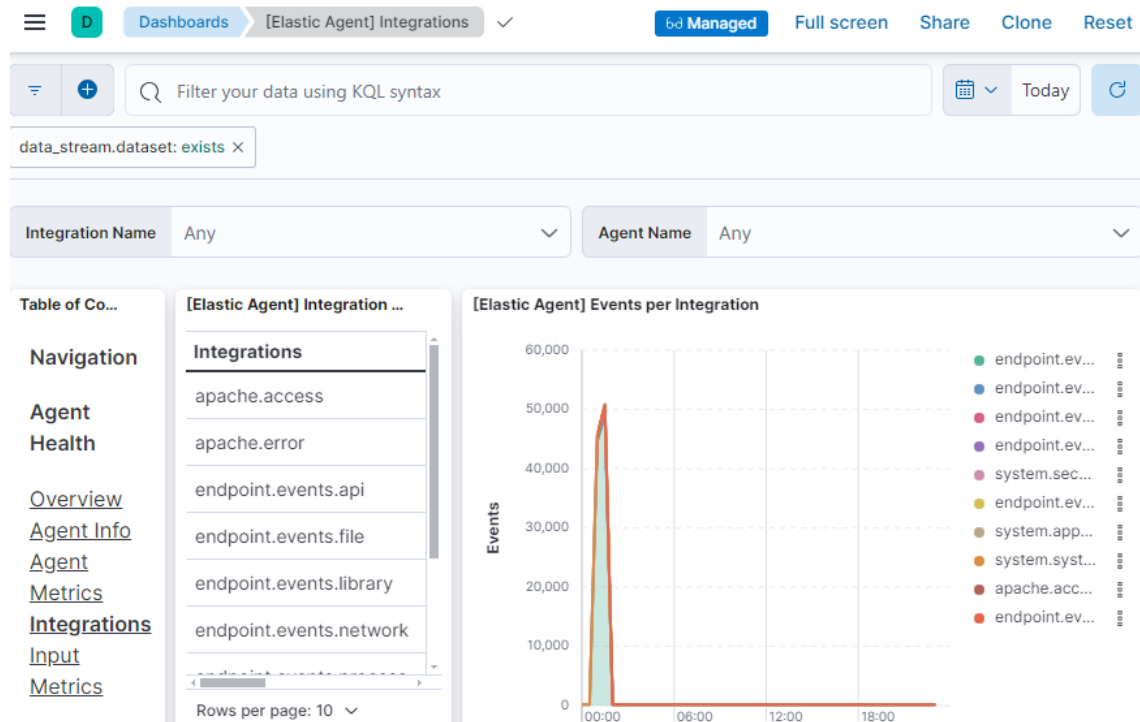
Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 18 sources.

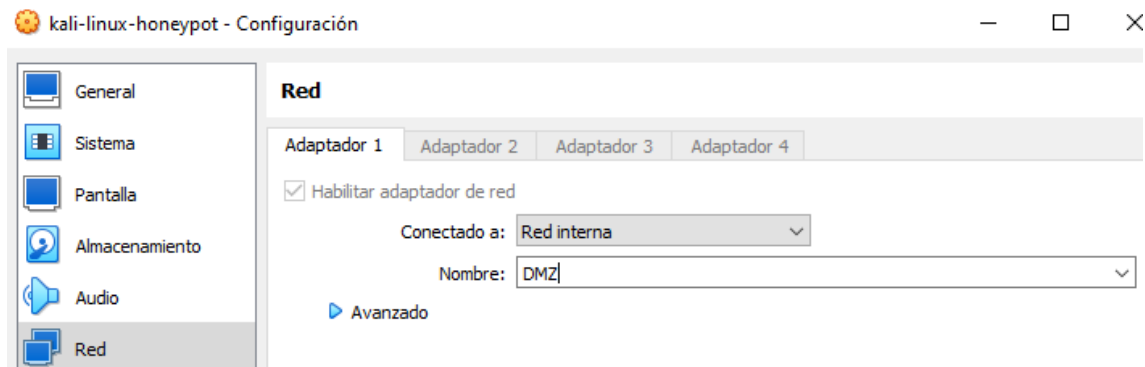
All sources	Matching sources
logs-apache.access-default	Data stream
logs-apache.error-default	Data stream
logs-elastic_agent-default	Data stream
logs-elastic_agent.endpoint_security-default	Data stream
logs-elastic_agent.filebeat-default	Data stream
logs-elastic_agent.metricbeat-default	Data stream
logs-endpoint.events.api-default	Data stream
logs-endpoint.events.file-default	Data stream
logs-endpoint.events.library-default	Data stream
logs-endpoint.events.network-default	Data stream

Reviso en dashboards los logs que va generando el servidor apache



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.



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 esta instalado por defecto, por tanto se instala

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

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

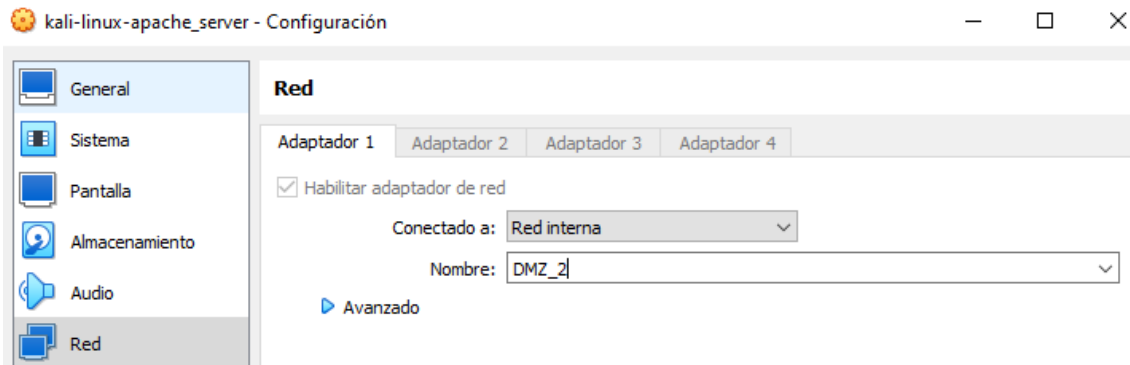
```
sudo docker run -p 2222:2222 cowrie/cowrie
```

```
(kali㉿kali)-[~]
└─$ sudo docker run -p 2222:2222 cowrie/cowrie
Unable to find image 'cowrie/cowrie:latest' locally
latest: Pulling from cowrie/cowrie
```

```
b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationW
arning: CAST5 has been deprecated
b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
2024-03-16T23:29:51+0000 [-] Python Version 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0]
2024-03-16T23:29:51+0000 [-] Twisted Version 23.10.0
2024-03-16T23:29:51+0000 [-] Cowrie Version 2.5.0
2024-03-16T23:29:51+0000 [-] Loaded output engine: jsonlog
2024-03-16T23:29:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 23.10.0 (/cowrie/cowrie-en
v/bin/python3 3.11.2) starting up.
2024-03-16T23:29:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.e
pollreactor.EPollReactor.
2024-03-16T23:29:51+0000 [-] CowrieSSHFactory starting on 2222
2024-03-16T23:29:51+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.Cow
rieSSHFactory object at 0x7f2421bc4510>
2024-03-16T23:29:51+0000 [-] Generating new RSA keypair...
2024-03-16T23:29:52+0000 [-] Generating new ECDSA keypair...
2024-03-16T23:29:52+0000 [-] Generating new ed25519 keypair...
2024-03-16T23:29:52+0000 [-] Ready to accept SSH connections
```

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

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
```

