

Actividad 1

**INSTALACIÓN Y CONFIGURACIÓN DE
PFSENSE**

Miquel Rodríguez González

4 de mayo de 2024



Qué es Pfsense

PfSense es una distribución de software de código abierto basada en FreeBSD que se utiliza para convertir un ordenador estándar en un enrutador y firewall de red. Ofrece una amplia gama de funcionalidades para la gestión y seguridad de redes, incluyendo enrutamiento, firewall, VPN, control de ancho de banda, equilibrio de carga, entre otras.

Índice

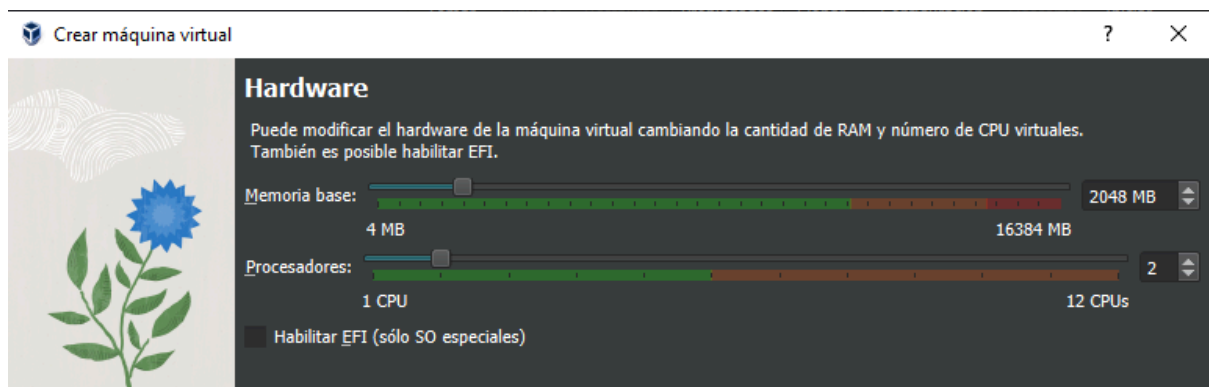
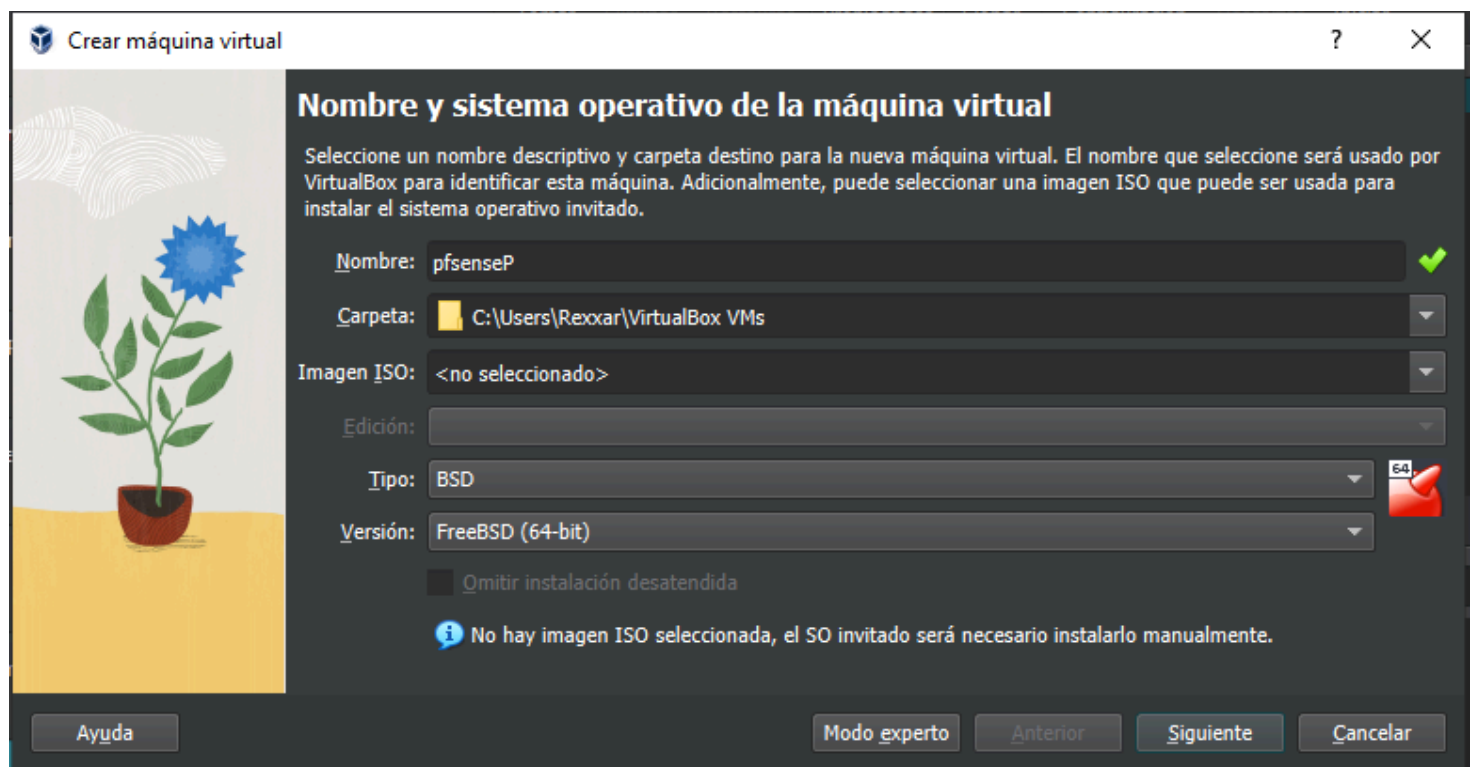
1- Preparación.....	2
2- Configuración de la máquina virtual.....	2
3- Instalación pfSense.....	5
4- Configuración pfSense.....	10
5- Acceso a través de web y configuración inicial.....	12
6- Implementación de normas.....	16
6.1- bloquear el www.corteIngles.com	17
6.2- bloquear puerto 80 http.....	19

1- Preparación

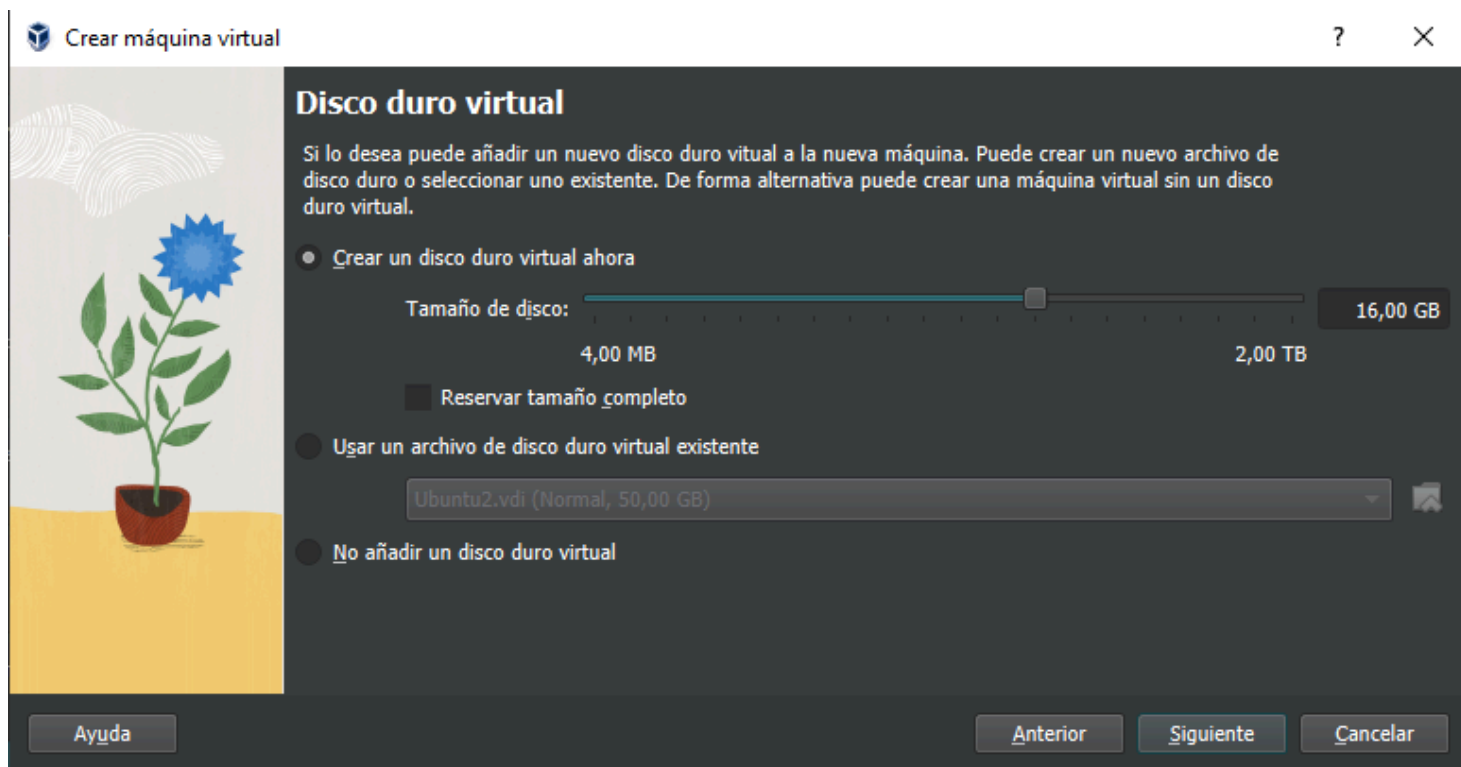
- tener un programa de virtualización
- descargar la iso de pfSense (<https://www.pfsense.org/download/>)

2- Configuración de la máquina virtual

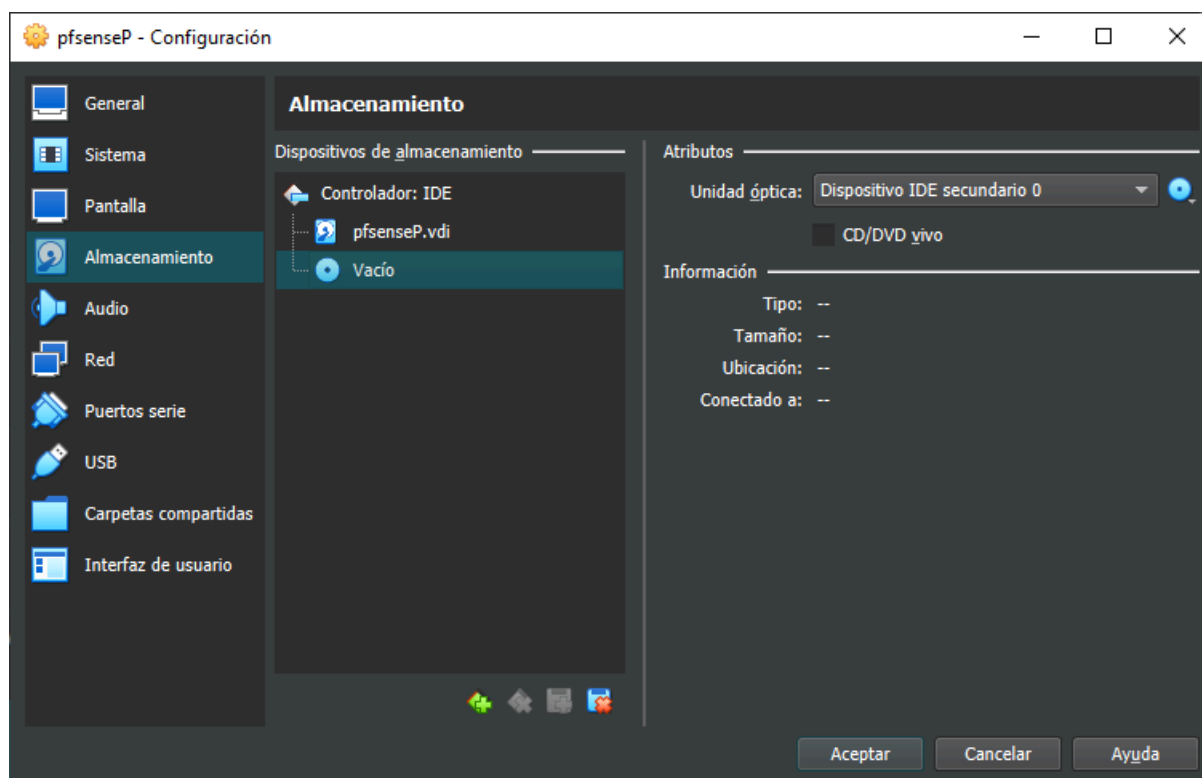
Empezamos



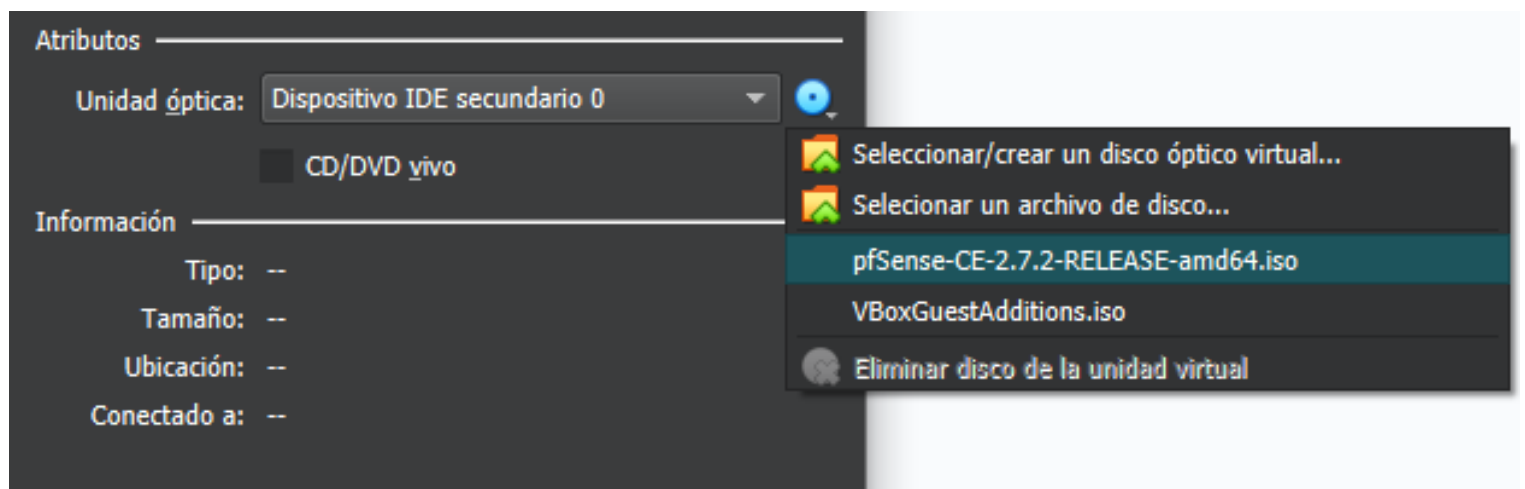
creando una máquina virtual con el sistema FreeBSD 64 bits
Con 2GB de RAM tenemos suficiente para el pfsense



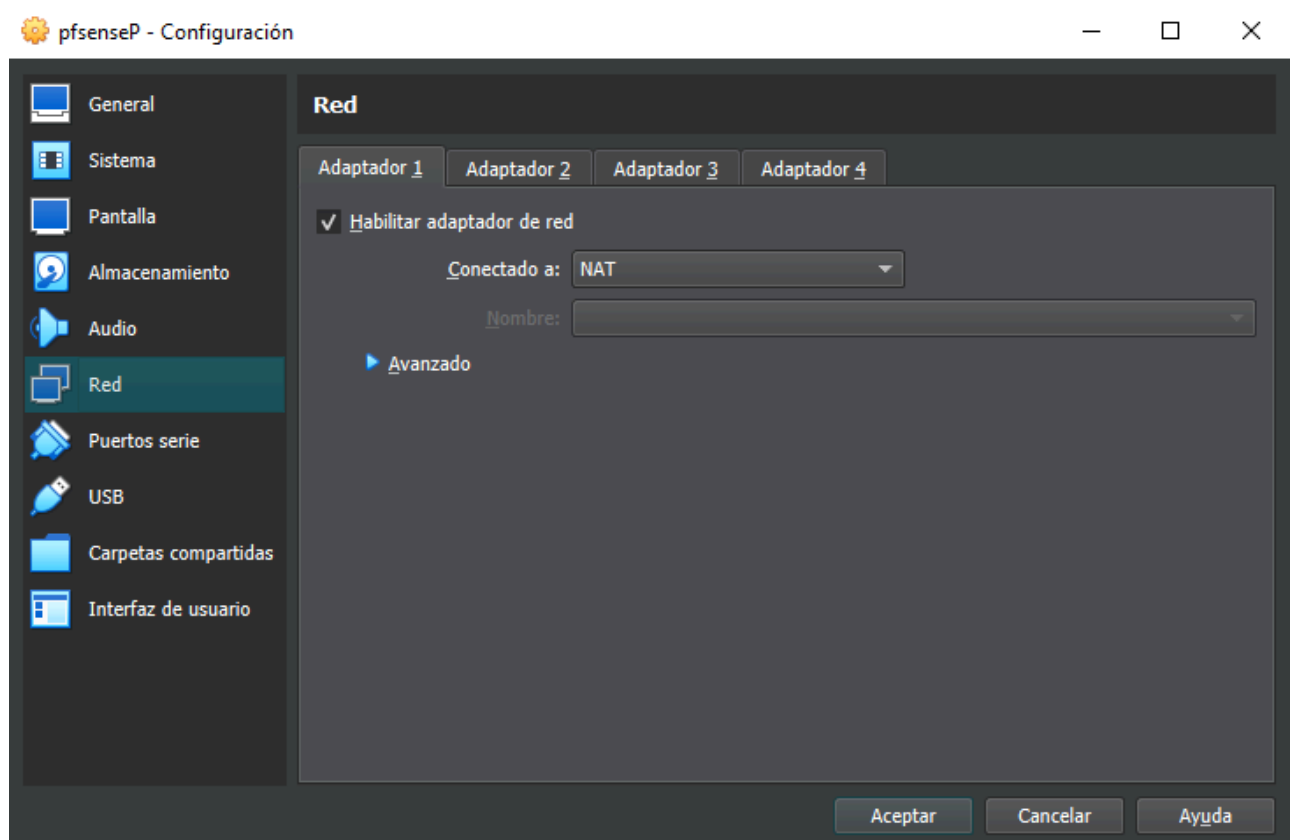
Una vez creada vamos a configuración/Almacenamiento y añadimos un nuevo dispositivo IDE

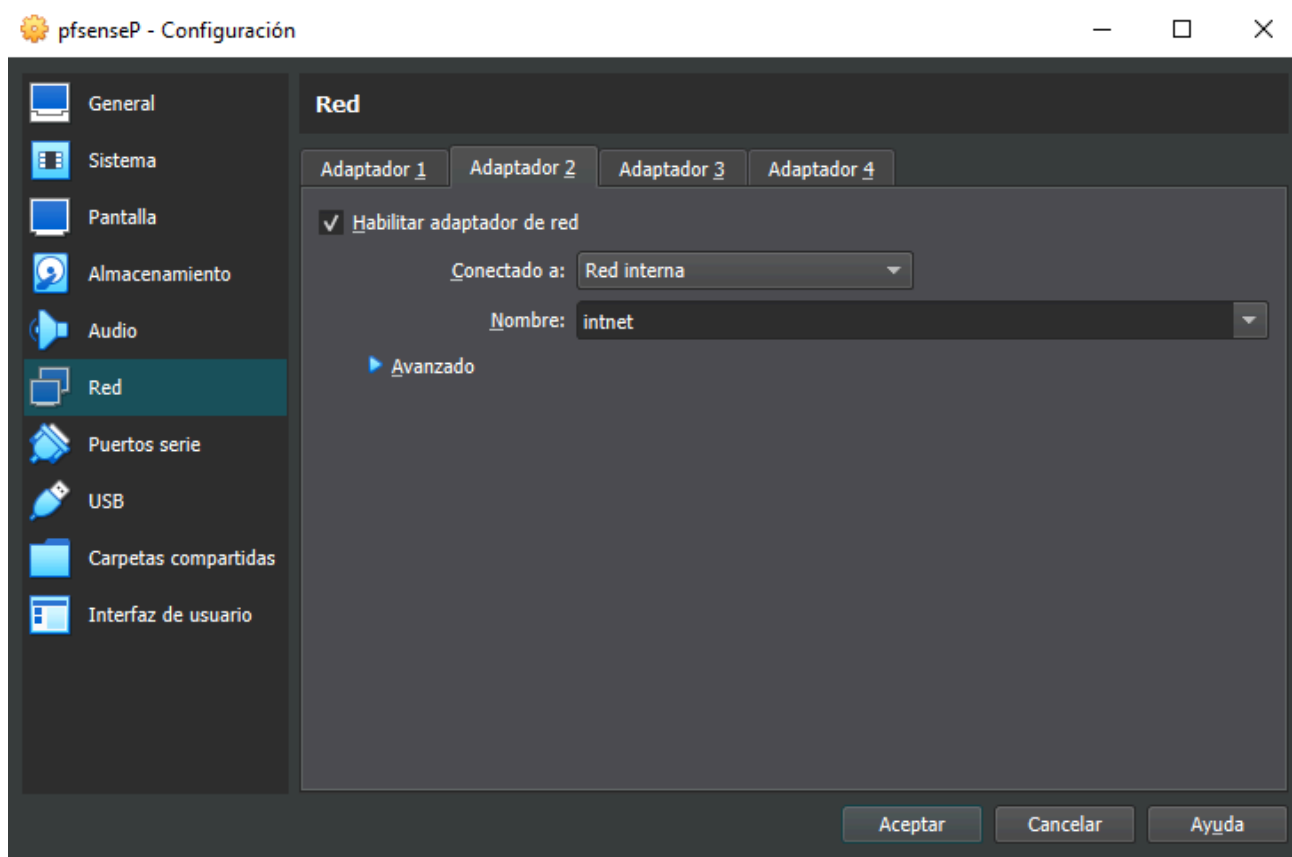


Seleccionamos la iso de pfSense que hemos descargado con anterioridad



Dentro de configuración/Red añadimos dos red una que sea adaptador puente/NAT (la opción que nos funcione) y otra red interna (opcional, solo si tenemos más ordenadores que queramos utilizar junto con el pfSense)





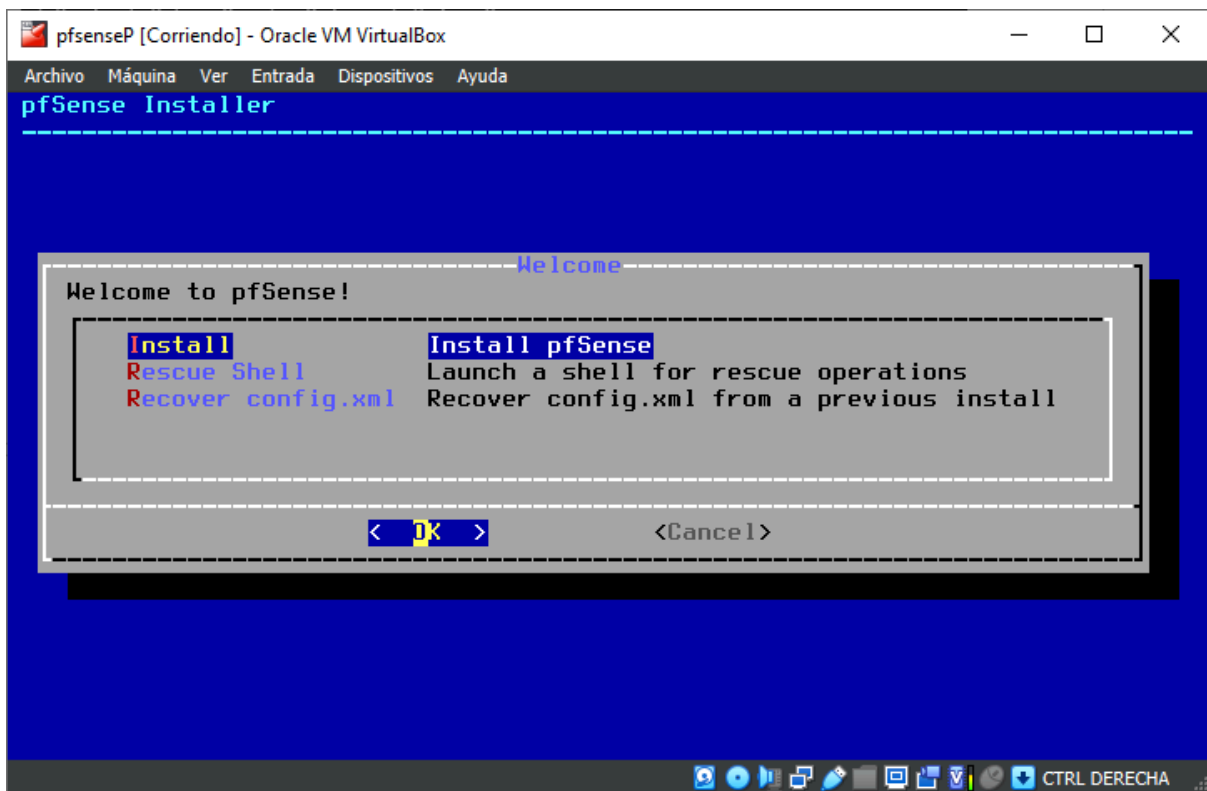
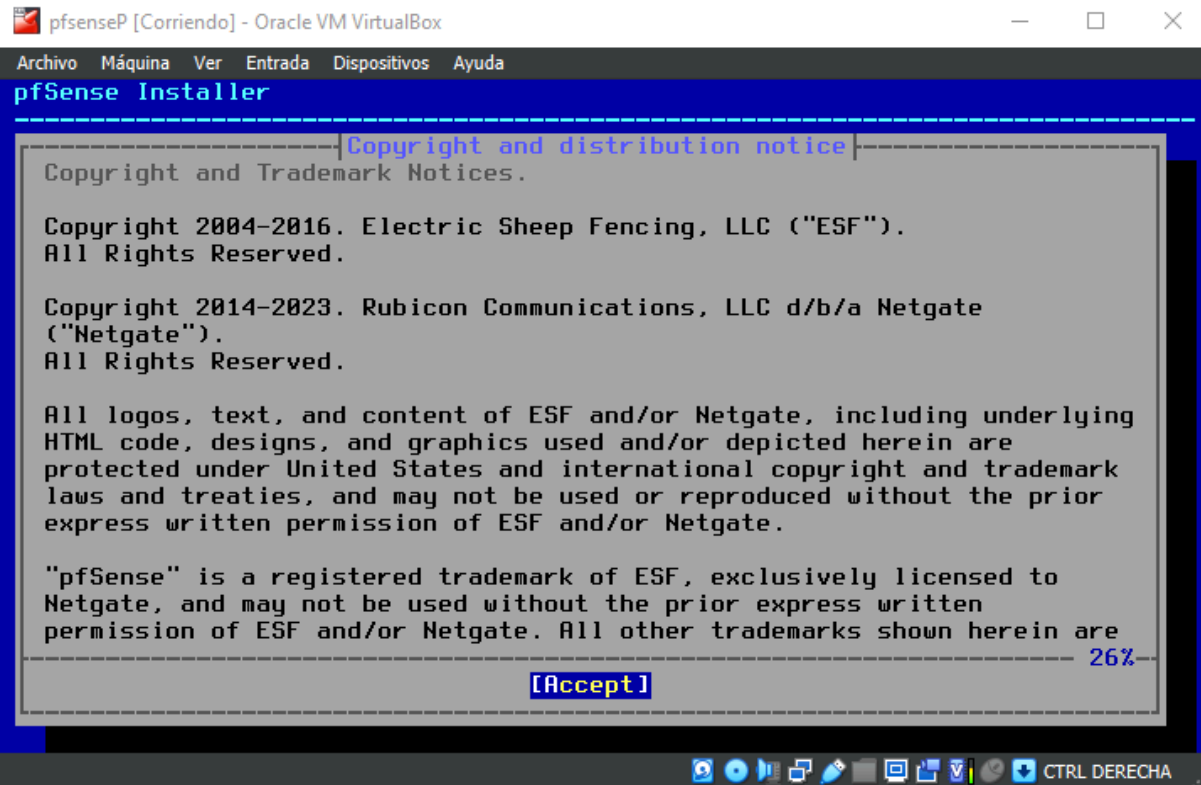
3- Instalación pfSense

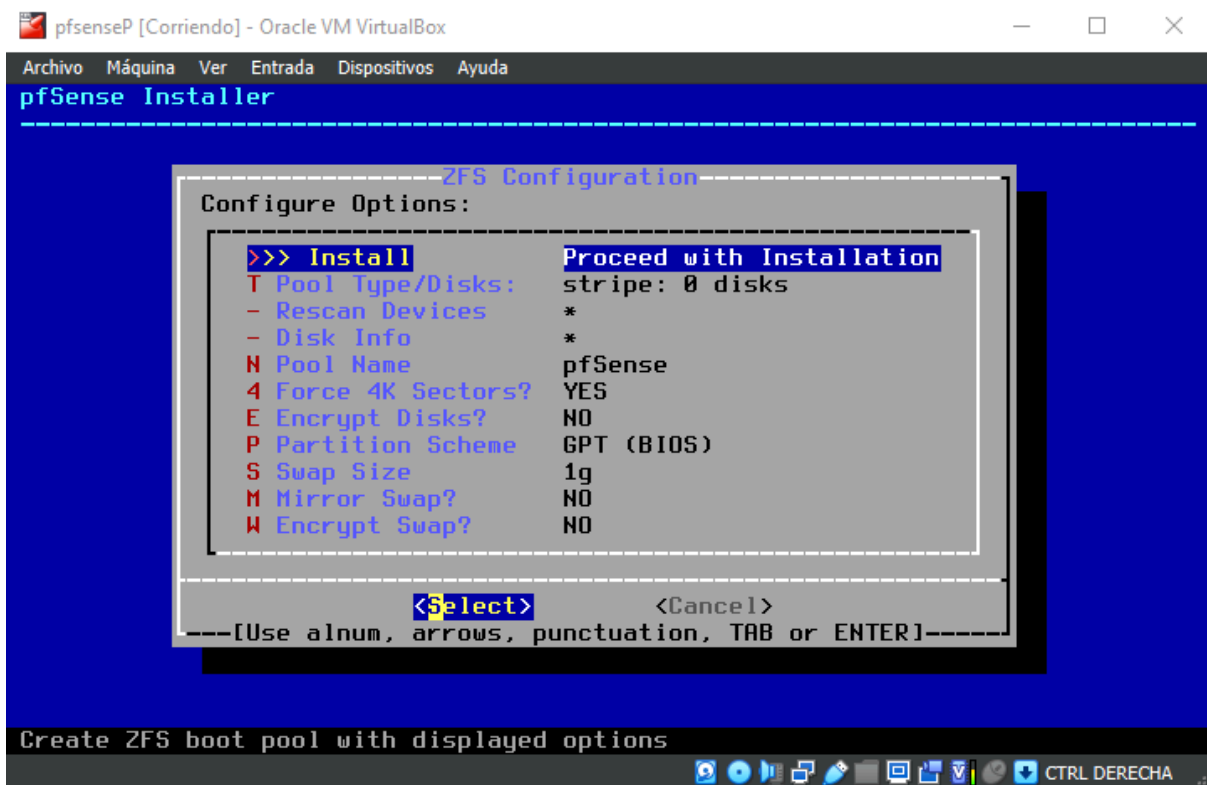
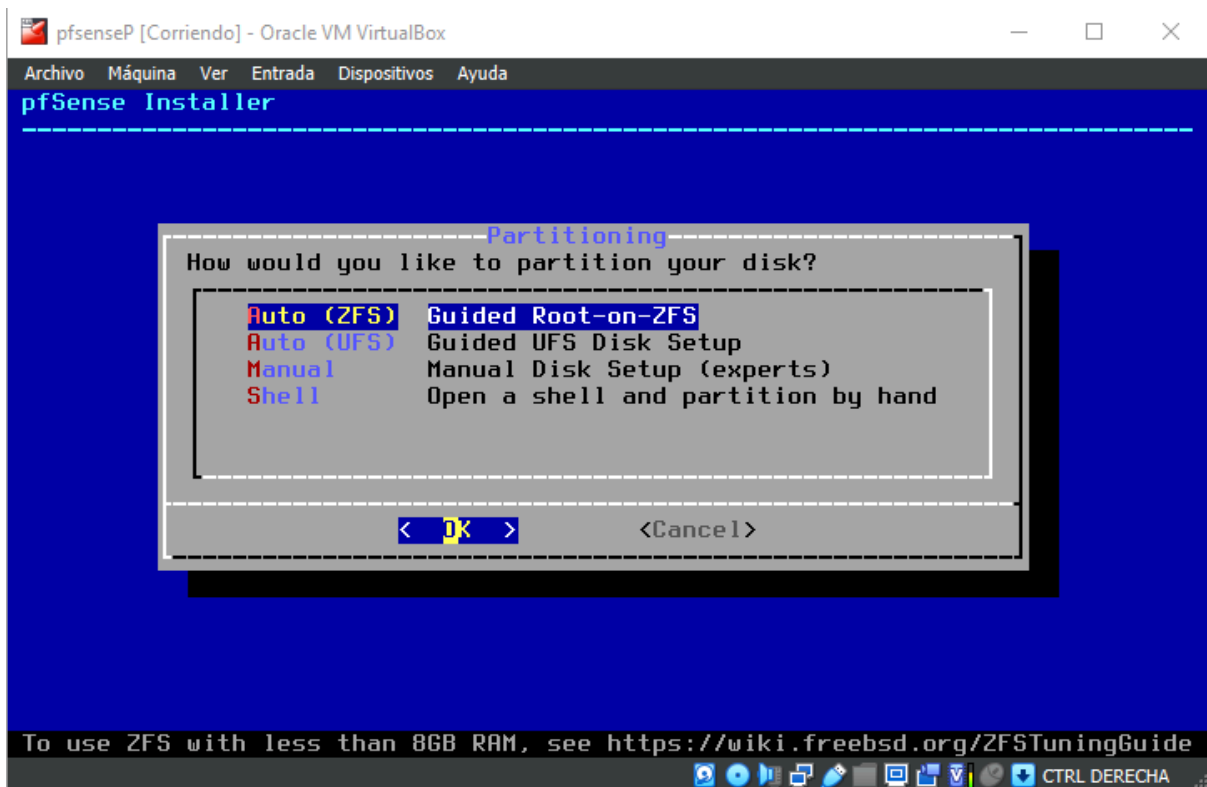
Iniciamos la Máquina

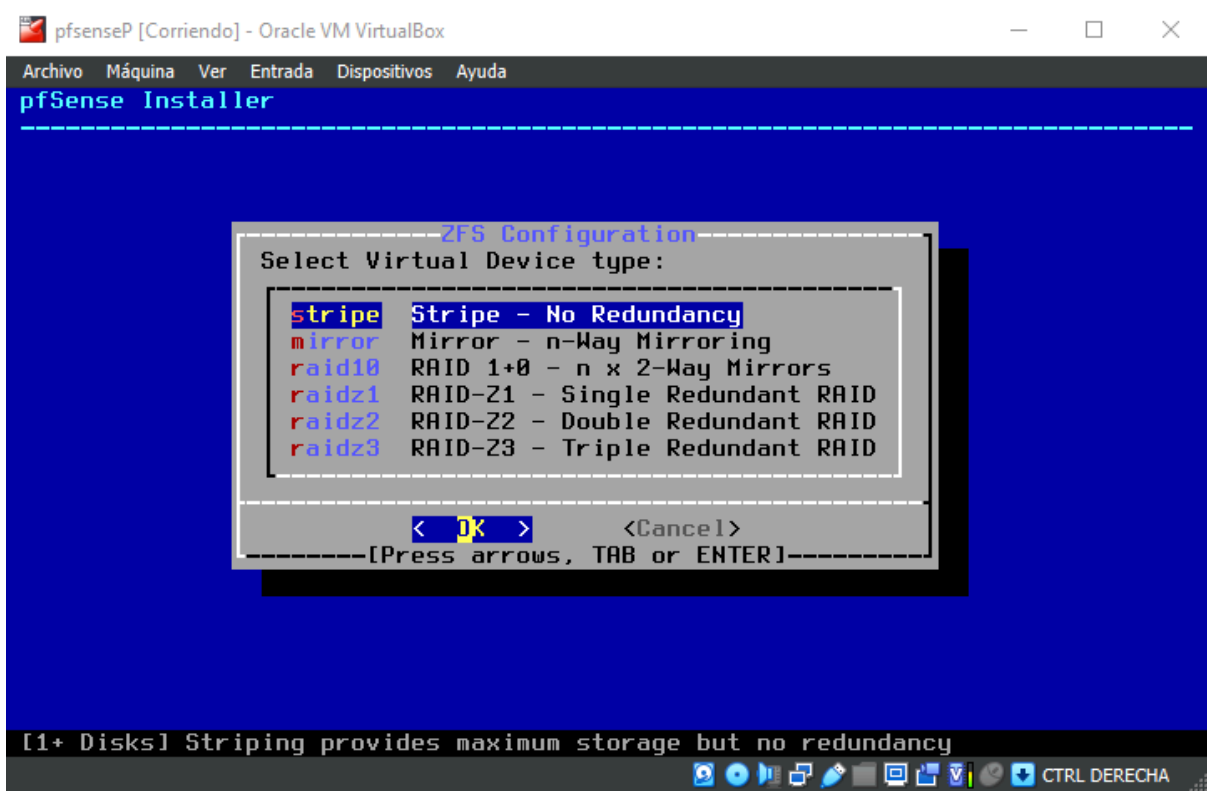
Error: si sale es siguiente error durante la instalación “Enter full pathname of shell or return for /bin/bash”, los más sencillo que podemos hacer es apagar la máquina y volver a iniciar la instalación

```
uhub1: 12 ports with 12 removable, self powered
Root mount waiting for: CAM
Root mount waiting for: CAM
Root mount waiting for: CAM
Root mount waiting for: CAM
ada0 at ata0 bus 0 scbus0 target 0 lun 0
ada0: <VBOX HARDDISK 1.0> ATA-6 device
ada0: Serial Number VB20669c9f-7f7f98c5
ada0: 33.300MB/s transfers (UDMA2, PIO 65536bytes)
ada0: 16384MB (33554432 512 byte sectors)
cd0 at ata1 bus 0 scbus1 target 0 lun 0
cd0: <VBOX CD-ROM 1.0> Removable CD-ROM SCSI device
cd0: Serial Number VB2-01700376
cd0: 33.300MB/s transfers (UDMA2, ATAPI 12bytes, PIO 65534bytes)
cd0: 834MB (427086 2048 byte sectors)
Enter full pathname of shell or RETURN for /bin/sh: █
```

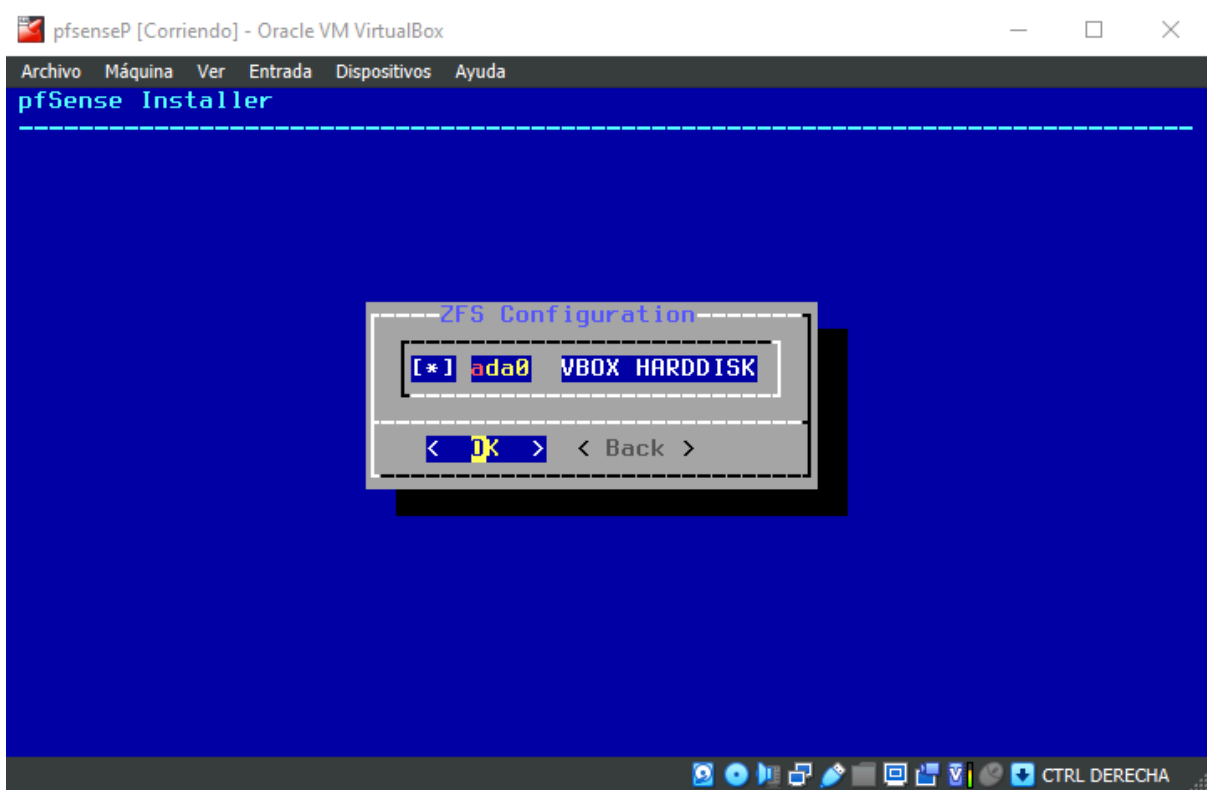
Tras que la instalación se haga correctamente, seguimos los siguientes pasos

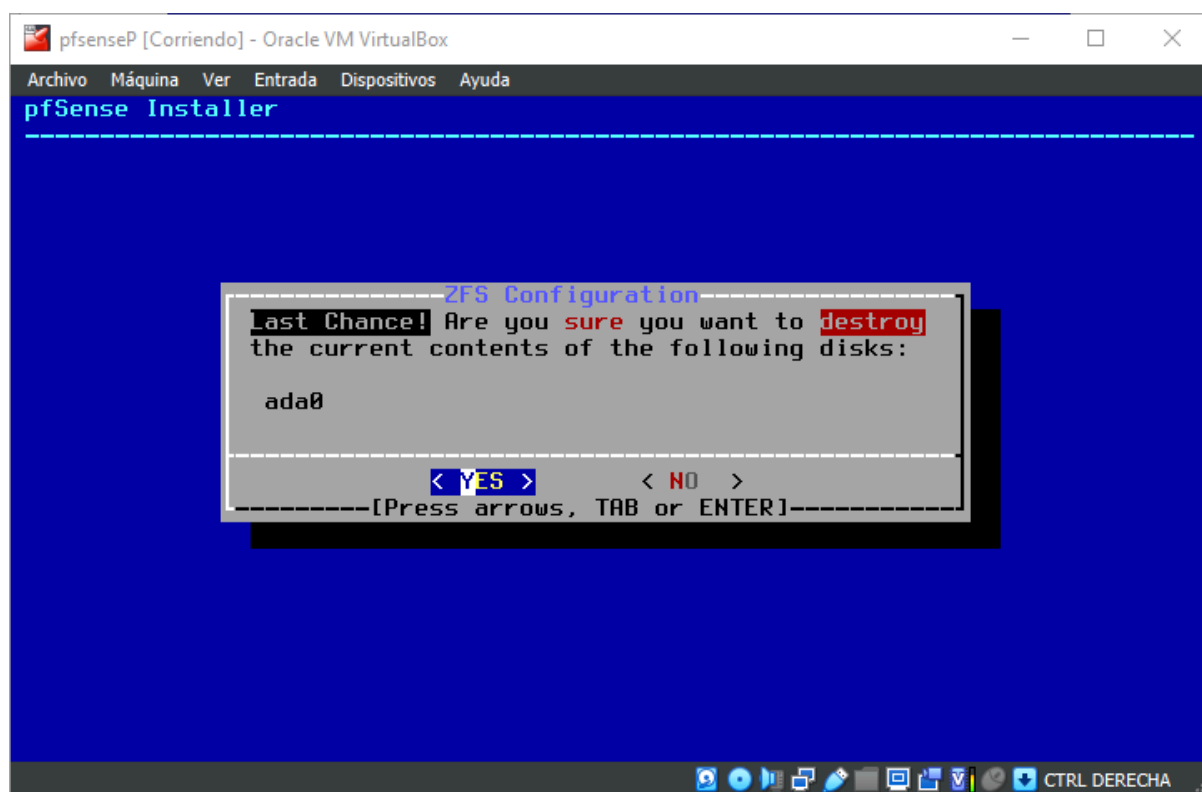




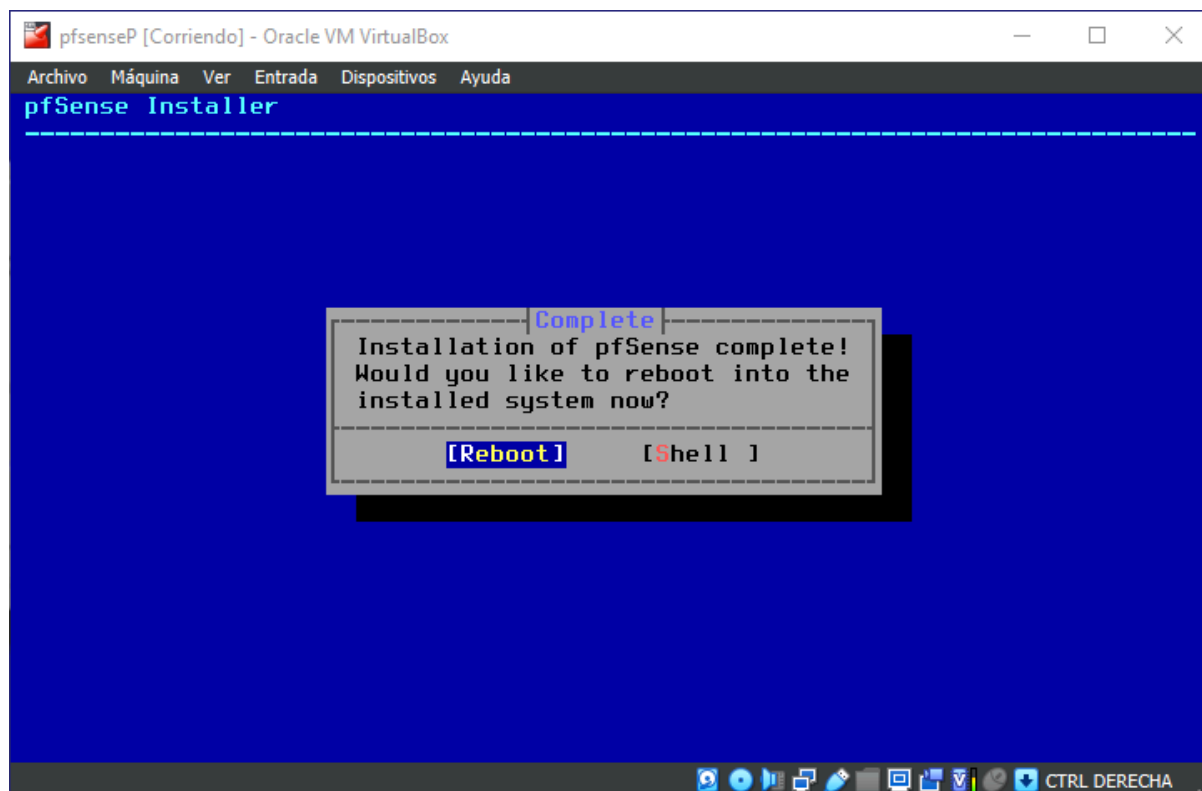


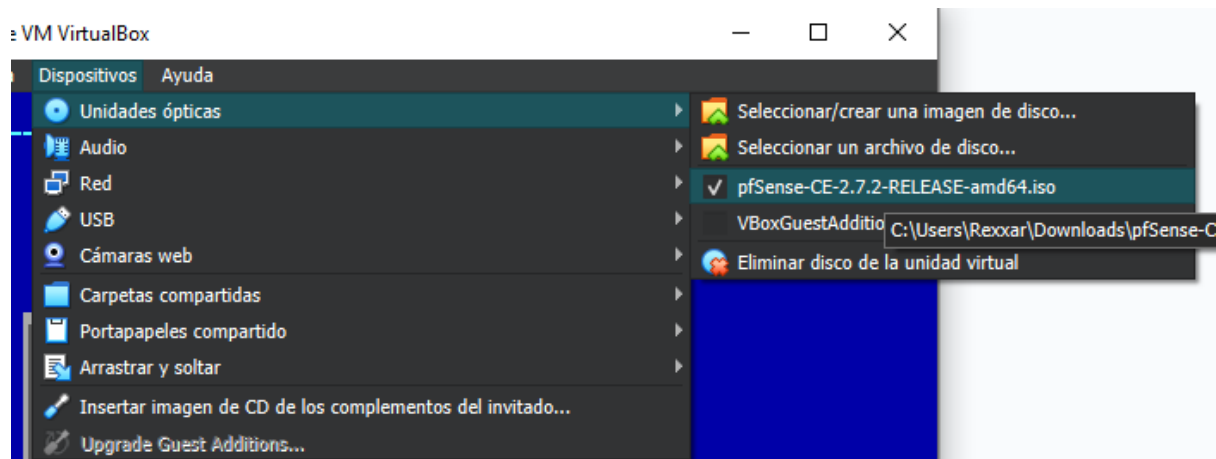
Seleccionamos el disco donde hacer la instalación con el espacio





Hacemos reboot y sacamos el disco de instalación





4- Configuración pfSense

Una vez reiniciado ya tendremos el pfSense, tendremos que configurar las redes para que sean adecuadas. La red LAN hay que ponerla dentro del rango de la red interna

```

pfsenseP [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: 11632d4e3037eaa40d95

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
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:

```

Configuración de LAN:

```
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: 2

Available interfaces:

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

Enter the number of the interface you wish to configure: █

Enter an option: 2

Available interfaces:

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:

> 192.168.10.10 █

Enter the new LAN IPv4 address. Press <ENTER> for none:

> 192.168.10.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.

e.g. 255.255.255.0 = 24

255.255.0.0 = 16

255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):

> 24 █

CTRL DERECHA

```

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.10.10/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.10.10/

Press <ENTER> to continue.

```

5- Acceso a través de web y configuración inicial

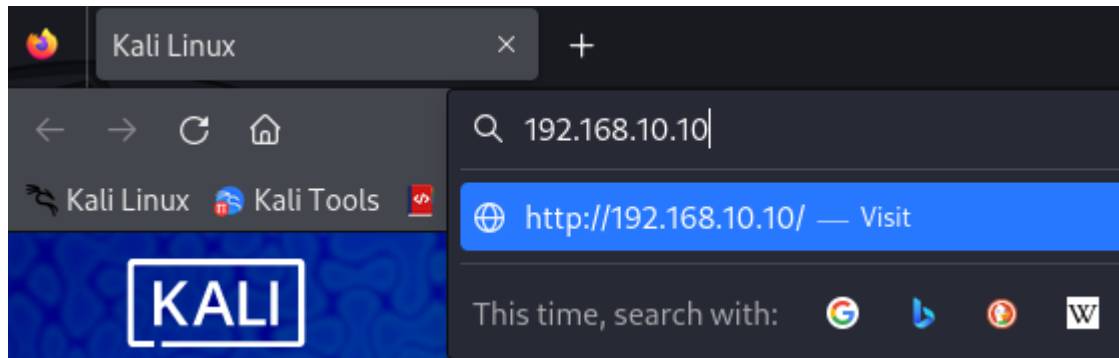
Una vez hecho esto accederemos a pfSense desde otro ordenador

Para ello tenemos que asegurarnos de que el otro sistema está dentro de la red interna, además pondremos que el “default gateway” de esa máquina sea la del pfSense. Configuración de Red de la máquina externa:

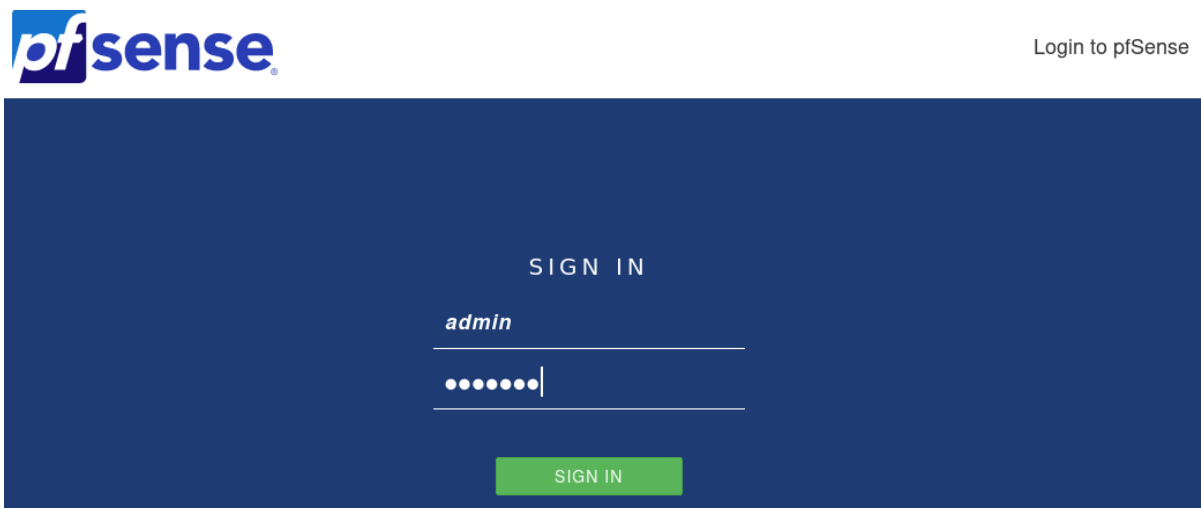
The screenshot shows the 'IPv4 Settings' tab for a connection named 'Wired connection 1'. The 'Method' is set to 'Manual'. Below this, there is a table for 'Addresses' with one entry: Address '192.168.10.160', Netmask '24', and Gateway '192.168.10.10'. Below the table, there are fields for 'DNS servers' (1.1.1.1), 'Search domains', and 'DHCP client ID'. A checkbox for 'Require IPv4 addressing for this connection to complete' is unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons.

Address	Netmask	Gateway
192.168.10.160	24	192.168.10.10

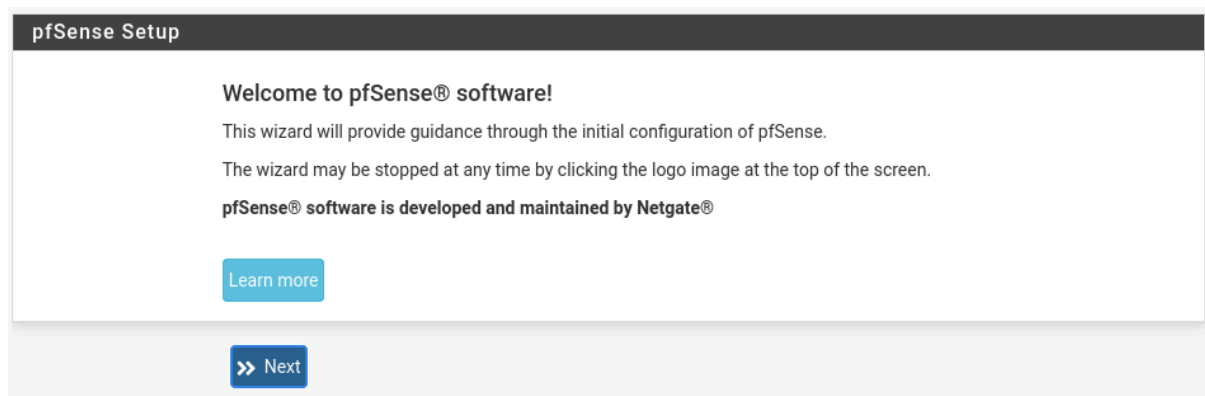
Ahora podemos acceder al pfsense a través de un explorador web



Iniciamos sesión. user: **admin** password: **pfsense**



Una vez dentro seguimos los pasos que nos indican



Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

Learn more

>> Next

Añadimos nombre y DNS si lo deseamos

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 ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

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

RFC1918 Networks

Block RFC1918 Private Networks ☒ Block private networks from entering via WAN

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

Block bogon networks

Block bogon networks ☒ Block non-Internet routed networks from entering via WAN

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

[» Next](#)

en caso de que queramos cambiar la ip de pfSense también lo podemos hacer aquí

Step 5 of 9

Configure LAN Interface

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

LAN IP Address

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

Subnet Mask

[» Next](#)

Añadimos una nueva contraseña

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

Admin Password AGAIN

[» Next](#)

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

Step 8 of 9

Reload in progress

A reload is now in progress. Please wait.

The wizard will redirect to the next step once the reload is completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Una vez le demos al finish ya estaremos dentro

6- Implementación de normas

Importante: después de cada cambio hay que aplicar los cambios.

Para poder crear las siguientes normas accederemos a Firewall/rules/Nat

Firewall / [Rules](#) / LAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/1.45 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	8/538 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	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

6.1- bloquear el www.corteIngles.com

Para poder bloquear el corte inglés lo más fácil es crear un alias que incluya todas las ips del corte inglés. para ello accedemos a Firewall/alias y creamos una nueva con la siguiente configuración

Firewall / Aliases / IP 📊 ?

IP Ports URLs All

Firewall Aliases IP

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

+ Add 📁 Import

Firewall / Aliases / Edit ?

Properties

Name

corteingles

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

Description

bloquear corteingles

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

Type

Host(s)

▼

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN			
<input type="text" value="www.elcorteingles.com"/>	<input type="text" value="Entry added Fri, 26 Apr 2024 08:45:55 +0000"/>	<input type="text" value=""/>	🗑 Delete
<input type="text" value="www.elcorteingles.es"/>	<input type="text" value="Entry added Fri, 26 Apr 2024 08:45:55 +0000"/>	<input type="text" value=""/>	🗑 Delete
<input type="text" value="elcorteingles.es"/>	<input type="text" value="Description"/>	<input type="text" value=""/>	🗑 Delete
<input type="text" value="elcorteingles.com "/>	<input type="text" value="Description"/>	<input type="text" value=""/>	🗑 Delete

con esto listo creamos una nueva norma con la siguiente configuración

Firewall / Rules / Edit

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

LAN

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

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

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

Destination

Destination

☐ Invert match

Address or Alias

corteingles

/

Destination Port Range

(other)

From

Custom

(other)

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

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

Save

Una vez hecho esto ya no podremos acceder al corte inglés

6.2- bloquear puerto 80 http

crearemos un alias con las siguiente configuración (a parte del puerto 80 podríamos añadir otros)

Firewall / Aliases / Edit ?

Properties


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

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

Type

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	<input type="text" value="80"/>	<input type="text" value="http"/>	 Delete
-------------	---------------------------------	-----------------------------------	--

y creamos una nueva norma

Edit Firewall Rule

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

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

 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	<input type="checkbox"/> Invert match	Any		Destination Address /
Destination Port Range	(other)	Puertos	(other)	
	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 checked="" 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	<input type="text"/> 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 checked="" type="checkbox"/> Display Advanced			
<input type="button" value="Save"/>				

ya no podremos utilizar el puerto 80