



**Certificado de Profesionalidad en
Seguridad Informática
IronHack - SOC**

**Módulo 2
Práctica 1 - PFSense**

Alumno: Julián Gordon

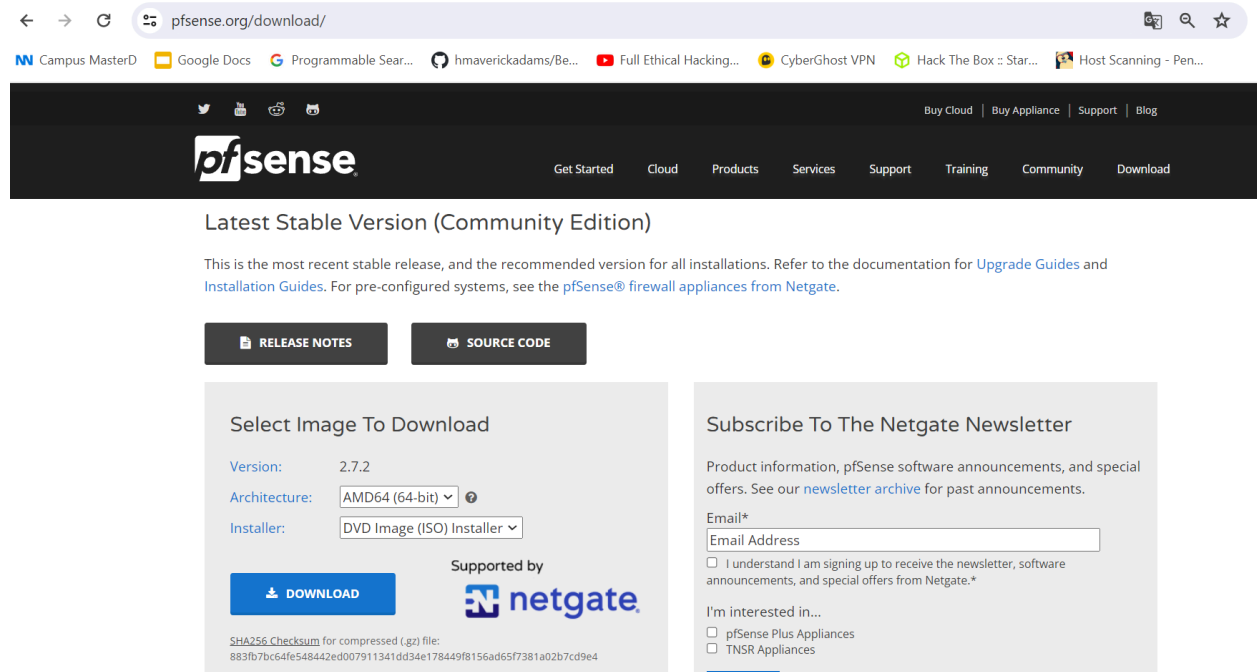
Introducción

En el creciente panorama de la ciberseguridad y la gestión de redes, contar con herramientas robustas y confiables es fundamental para garantizar la integridad y seguridad de las infraestructuras de tecnología de la información. Una de estas herramientas es pfSense, un potente software de firewall y enrutador que ofrece una amplia gama de funcionalidades para la gestión de seguridad de red.

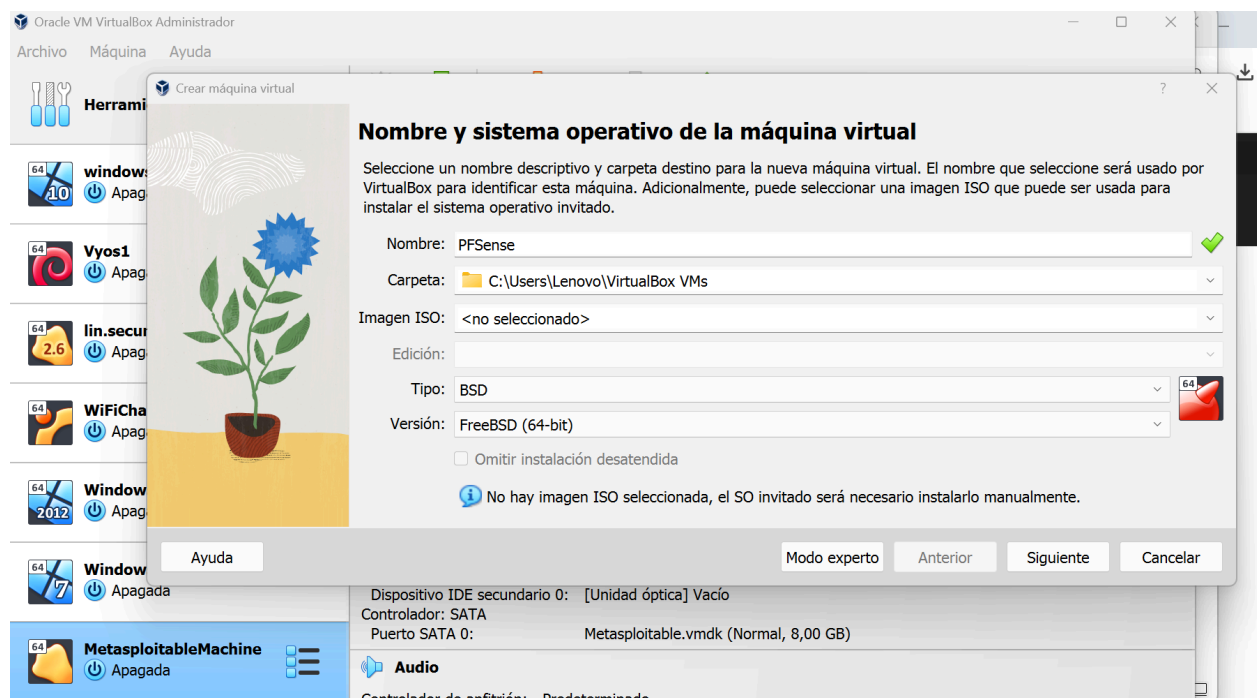
En esta actividad, nos introducimos en el mundo de pfSense, explorando su instalación y configuración en un entorno controlado utilizando una máquina virtual. pfSense, basado en el sistema operativo FreeBSD, se destaca por su versatilidad y su capacidad para adaptarse a las necesidades específicas de las empresas, proporcionando soluciones efectivas para asegurar las redes mientras se mantiene una gestión flexible y accesible.

A lo largo de este trabajo, hemos seguido paso a paso el proceso de instalación y configuración de pfSense, desde la descarga del archivo ISO hasta la implementación de reglas de firewall específicas para gestionar y controlar el tráfico de red. Este trabajo nos ha permitido familiarizarnos con las capacidades de pfSense y comprender su papel crucial en la protección y administración de redes empresariales.

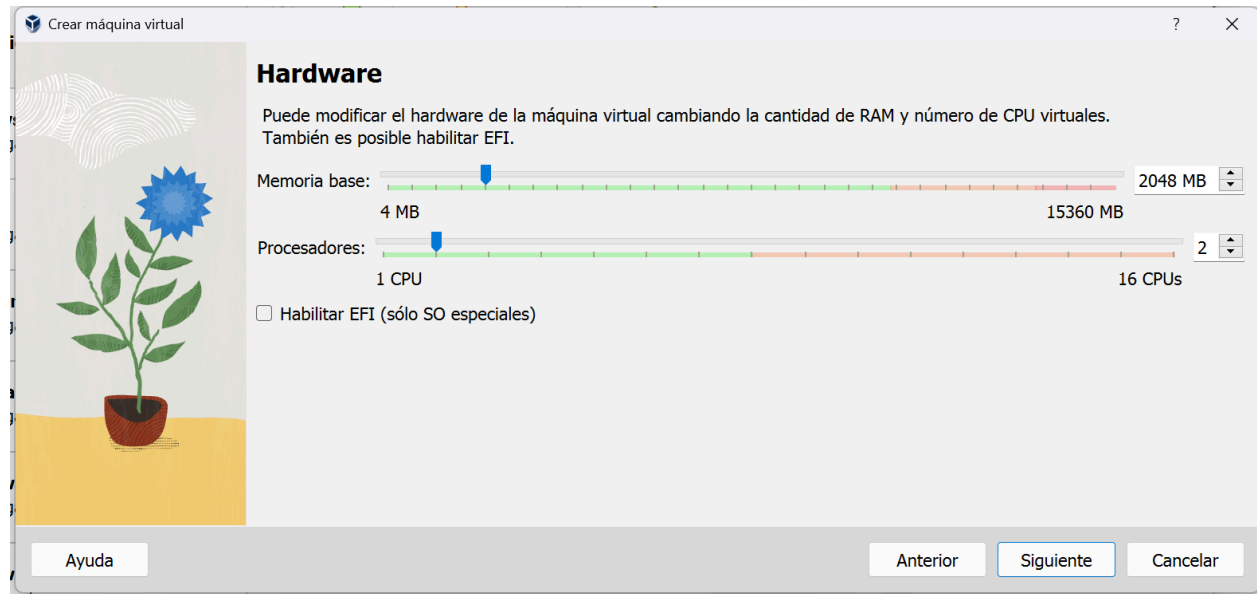
Lo primero que vamos a hacer será descargar la imagen ISO de PFSense. Para ello accedemos a su página web oficial y descargamos la versión compatible con nuestro sistema, en nuestro caso será AMD64(64-bit).



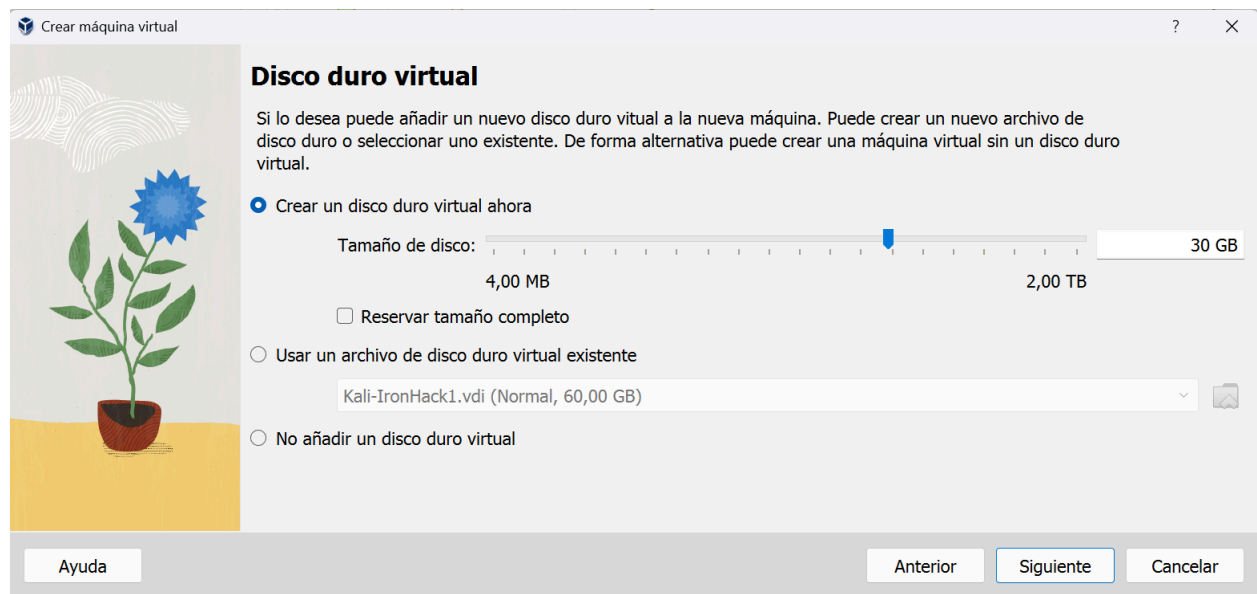
El segundo paso será dentro de Virtualbox, crear una máquina nueva. Le llamaremos PFSense.



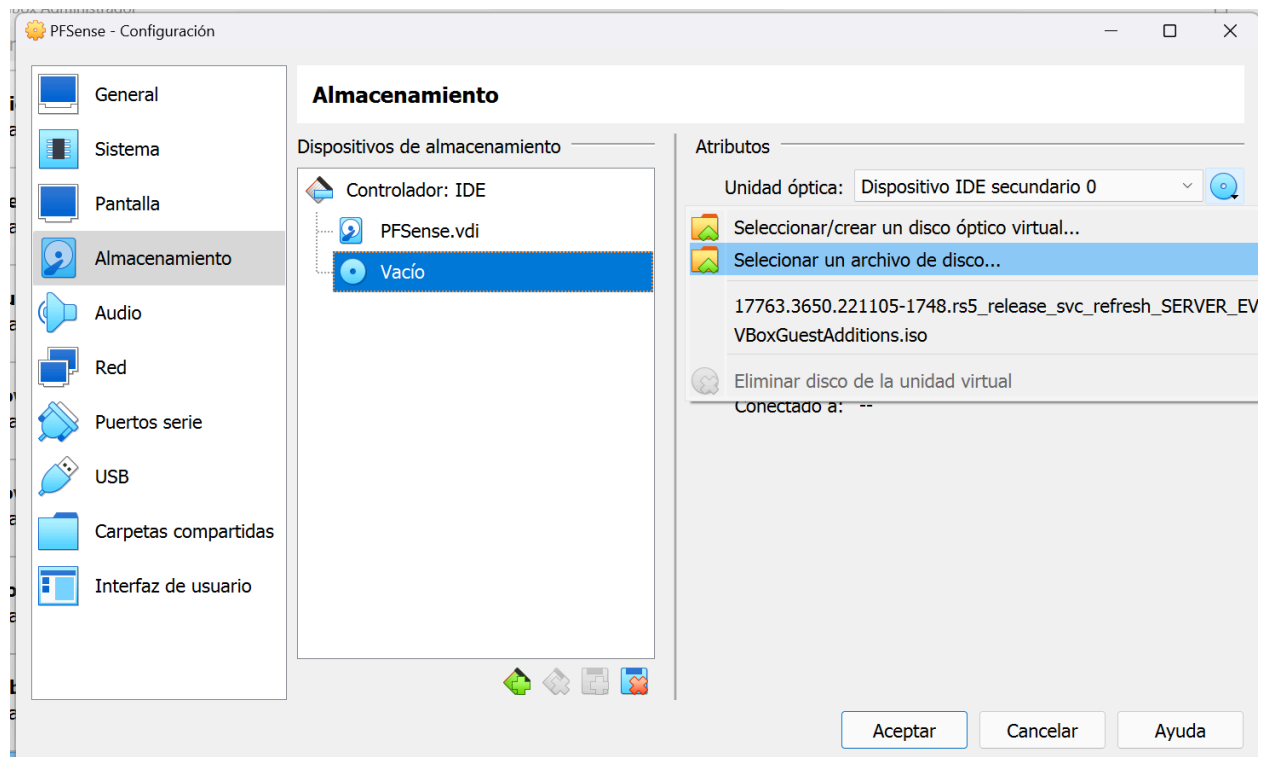
Le daremos 2gb de Ram y 2 procesadores.



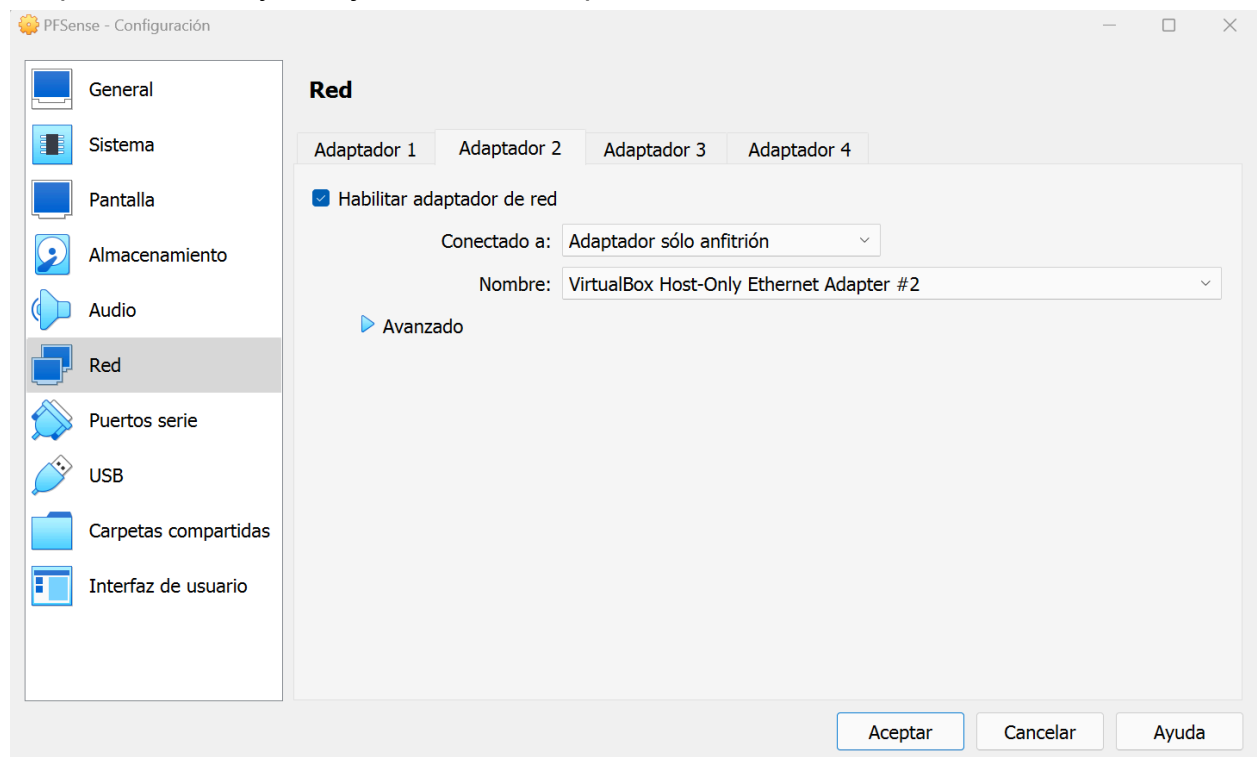
Crearemos un disco duro virtual de 30gb



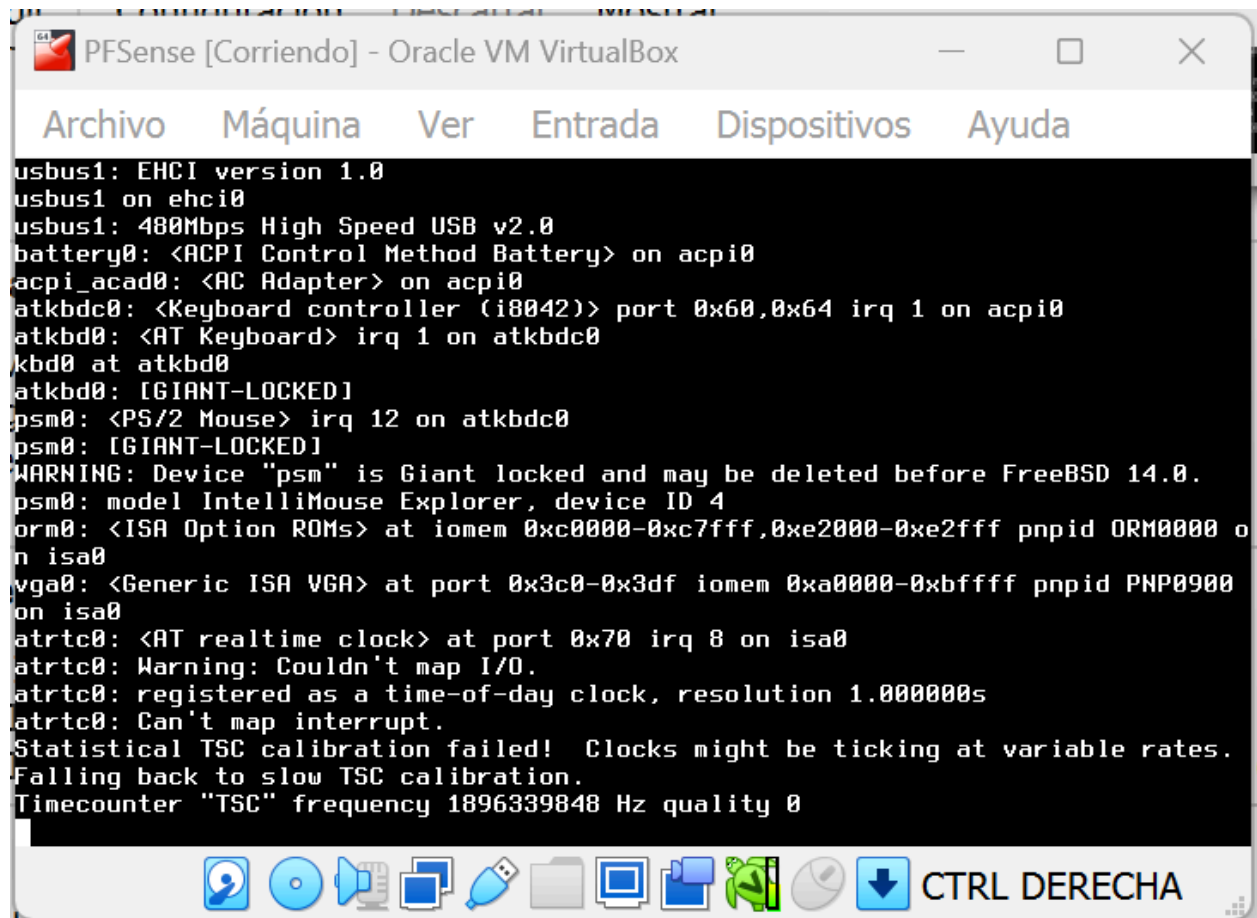
Una vez creada la máquina, vamos a 'Almacenamiento' y cargaremos la ISO que nos descargamos previamente.



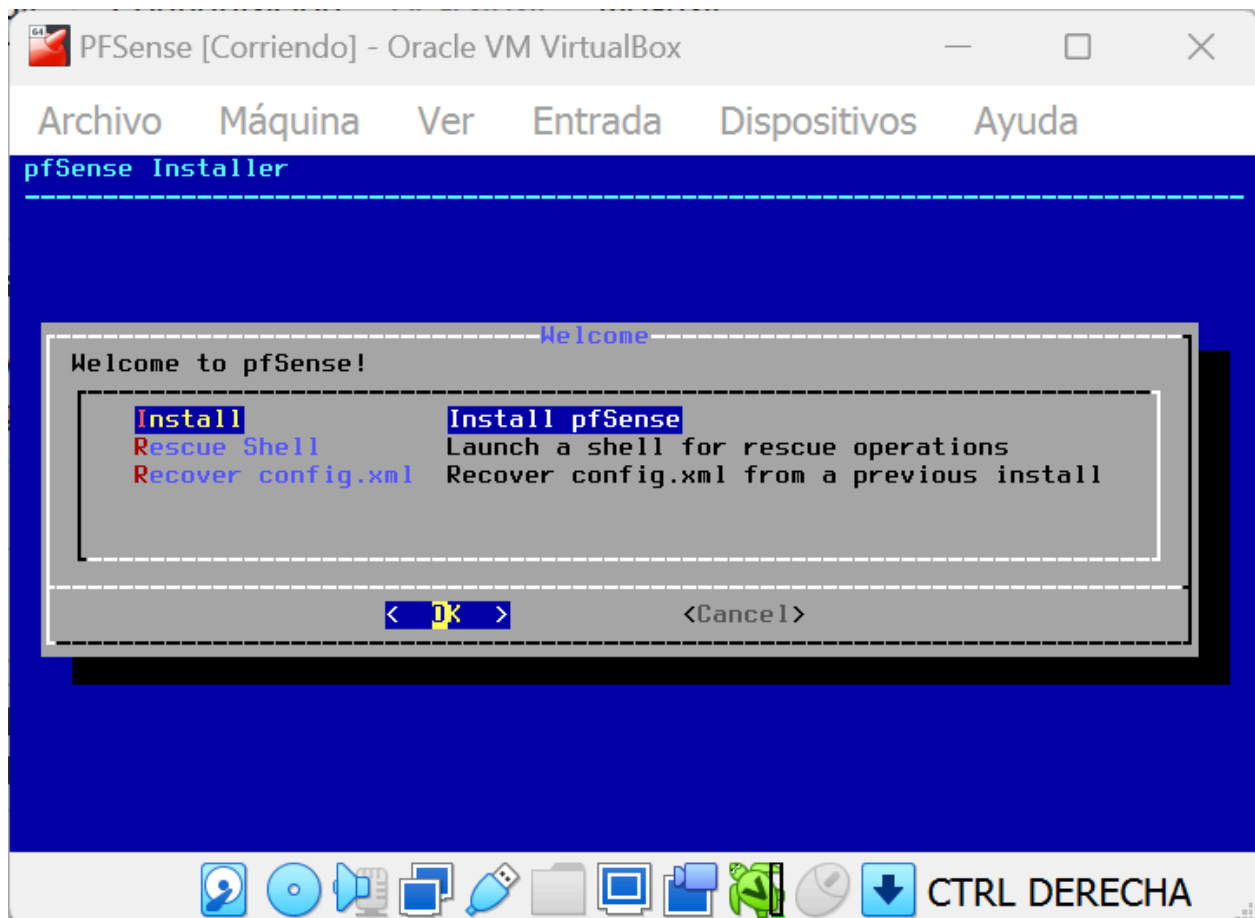
En el apartado de Red, dejamos el Adaptador 1 en NAT y habilitamos un segundo adaptador de red y lo dejaremos en 'Adaptador sólo Anfitrión'



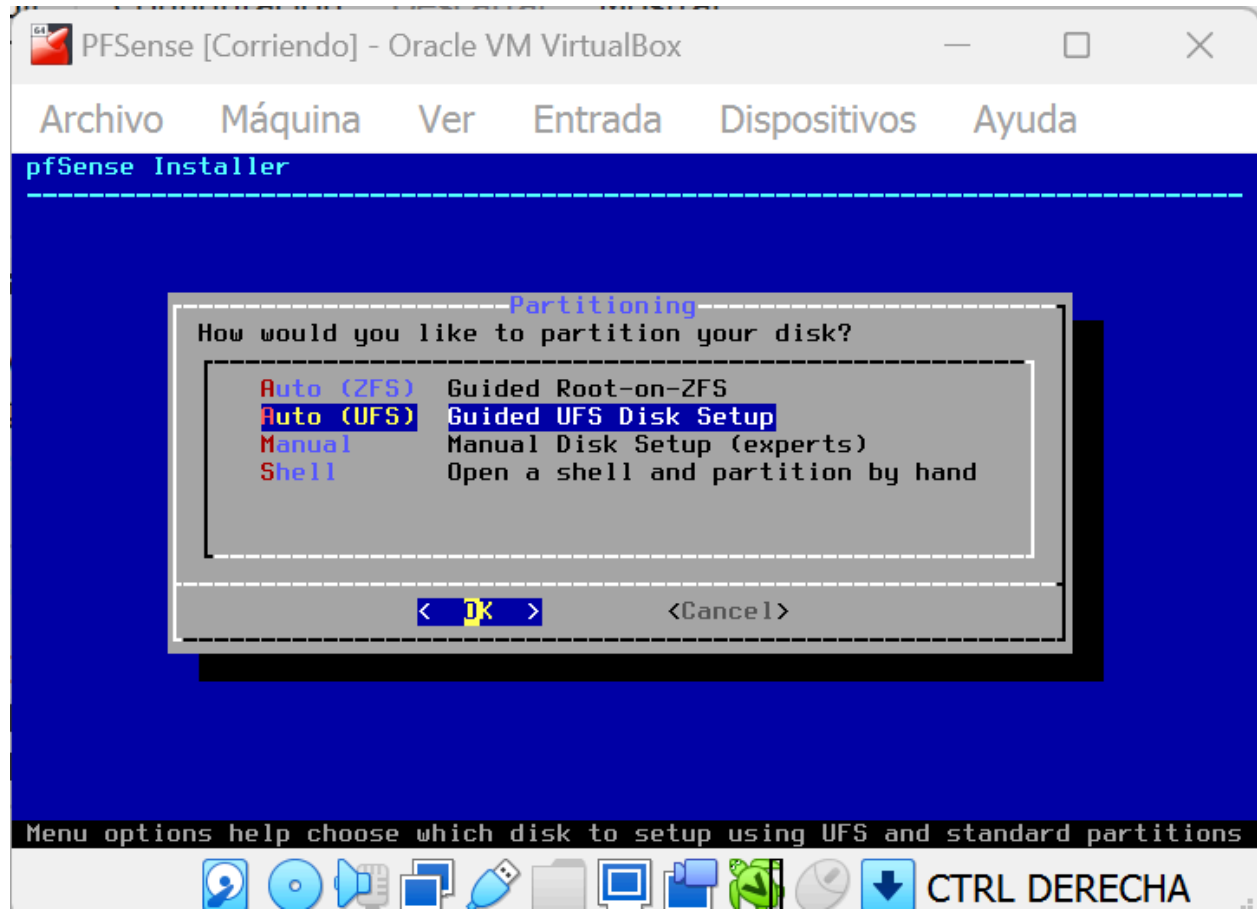
Abrimos la máquina.



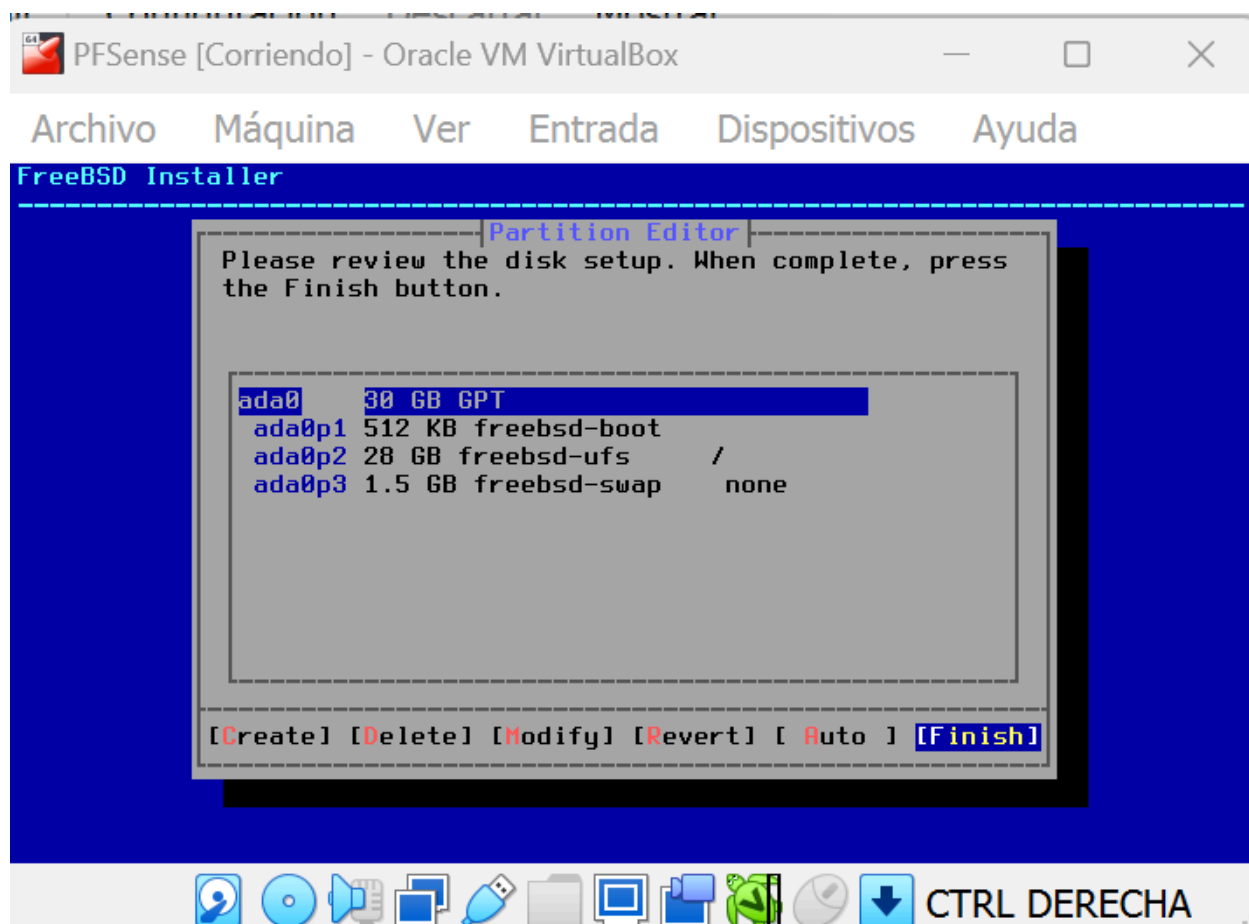
Ejecutamos la instalación.



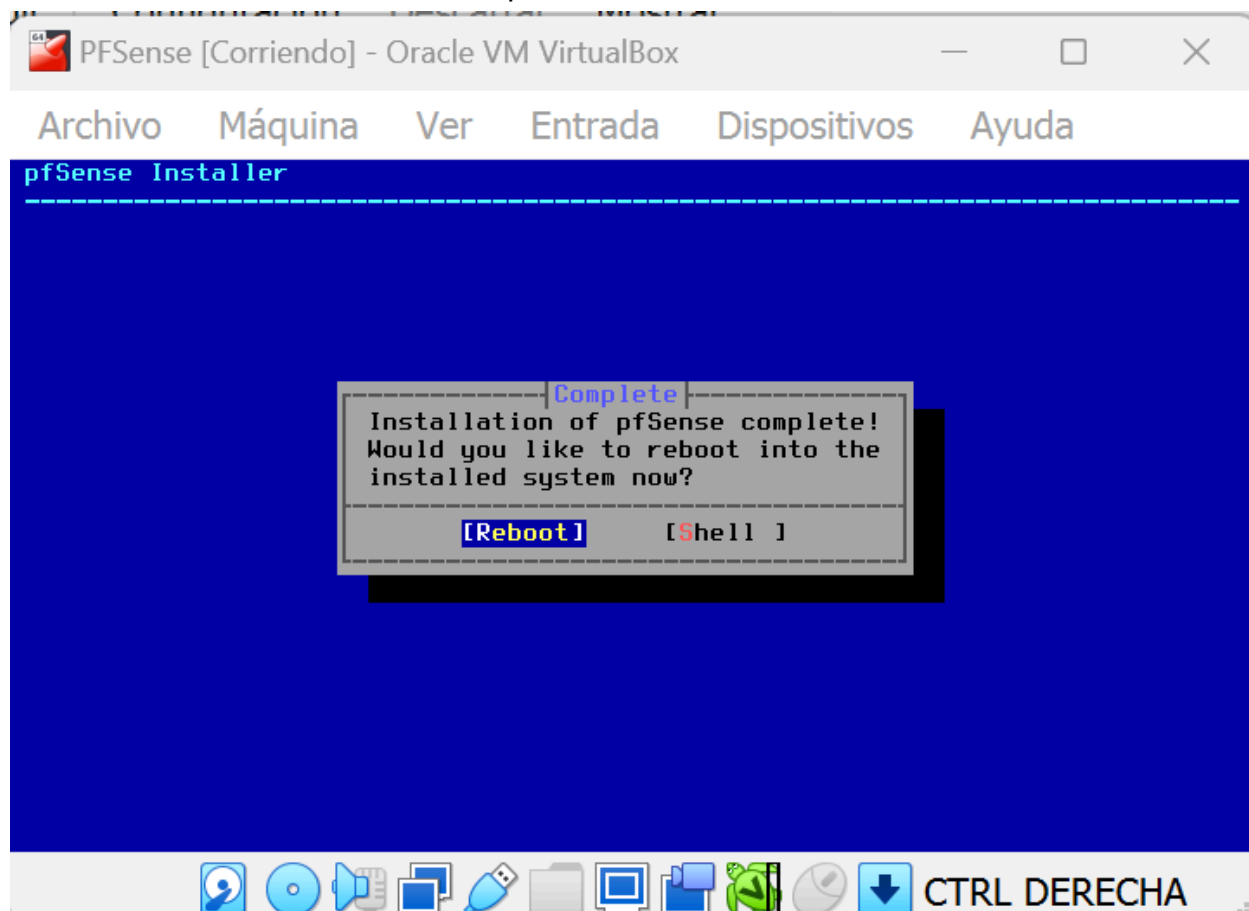
Seleccionamos la opción 'Guided UFS Disk Setup'.



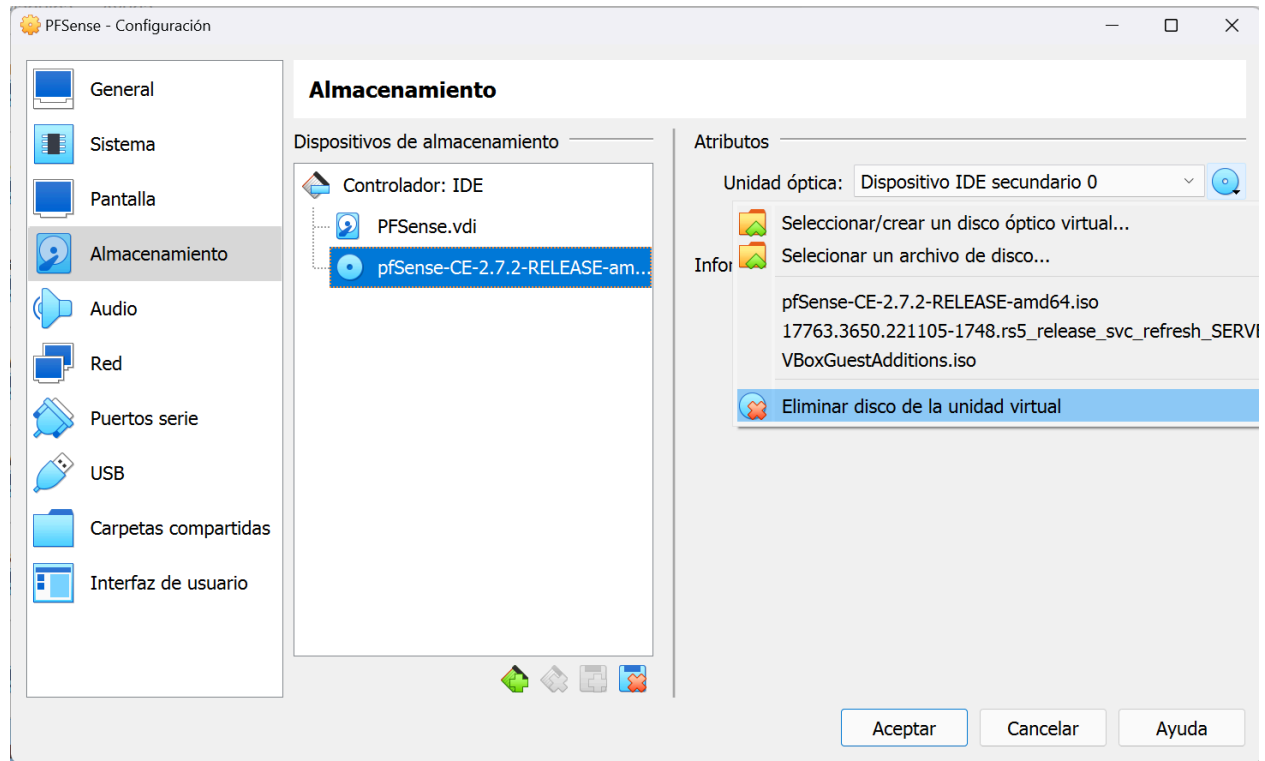
Y terminamos la instalación.



Por último, vamos a reiniciar la máquina.

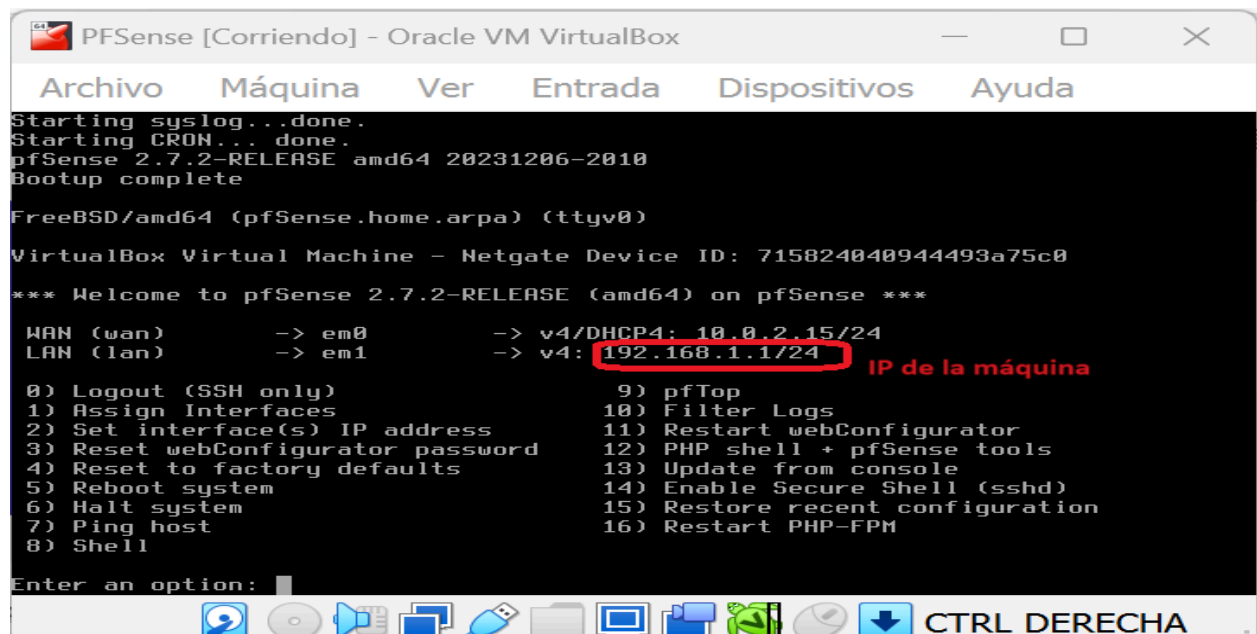


Una vez que la máquina vuelva a encender, la apagamos y quitamos el disco, borrando la ISO que habíamos cargado.



Volvemos a encender la máquina, se terminarán de instalar los paquetes pendientes y se iniciará normalmente.

Podemos observar en la siguiente imagen que la IP que tiene nuestra máquina de PFsense es la 192.168.1.1/24.



Como queremos verla desde nuestra máquina virtual de Windows 10, que está en modo 'adaptador sólo anfitrión', necesitamos que esté en este mismo segmento de red. Para eso abrimos un cmd y ejecutamos el comando 'ipconfig'. Vemos que la IP de Windows 10 es 192.168.56.106.

```
Selecciónar Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.4170]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>ipconfig


Configuración IP de Windows

Adaptador de Ethernet LAN:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::4707:e92d:9f63:d139%9
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : home.arpa
    Vínculo: dirección IPv6 local. . . : fe80::3a03:b87b:e28a:c218%19
    Dirección IPv4. . . . . : 192.168.56.106
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : fe80::a00:27ff:fee7:76f3%19
```



Para modificar el la IP de PFSense, abrimos la máquina, seleccionamos opción 2 > opción 2 > y le daremos la IP 192.168.56.2 y máscara de red 24(255.255.255.0, clase C).

```
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: 2

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.56.2

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
```

Dejamos en DHCP las IPv6 y habilitamos el servidor DHCP en LAN. Le daremos un rango de IPs desde la 192.168.56.3 hasta la 192.168.56.10. Por último, si podremos verlo a través de un HTTP y decimos que sí.

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.56.1

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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) y

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.56.3
Enter the end address of the IPv4 client address range: 192.168.56.10
Disabling IPv6 DHCPD...

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

Confirmamos que el cambio se ejecutó correctamente y vemos que ahora la IP es 192.168.56.2 y está en la misma subred que nuestra máquina de Windows 10.

```
The IPv4 LAN address has been set to 192.168.56.1/24

The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.VirtualBox Virtual Machine - Netgate Device ID: 715824
040944493a75c0

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.56.1/24

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
```

Para comprobarlo haremos un Ping entre las 2 máquinas. Observamos que a pesar de que le hayamos configurado la IP 192.168.56.2 para PFSense, se le asignó la 192.168.56.1 por DHCP. Podemos observar que se ven ambas máquinas en la siguiente imagen.

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . : home.arpa
Vínculo: dirección IPv6 local. . . : fe80::3a03:b87b:e28a:c218%19
Dirección IPv4. . . . . : 192.168.56.106
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::a00:27ff:fee7:76f3%19

C:\Windows\system32>ping 192.168.56.1

Haciendo ping a 192.168.56.1 con 32 bytes de datos:
Respuesta desde 192.168.56.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.56.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.56.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

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

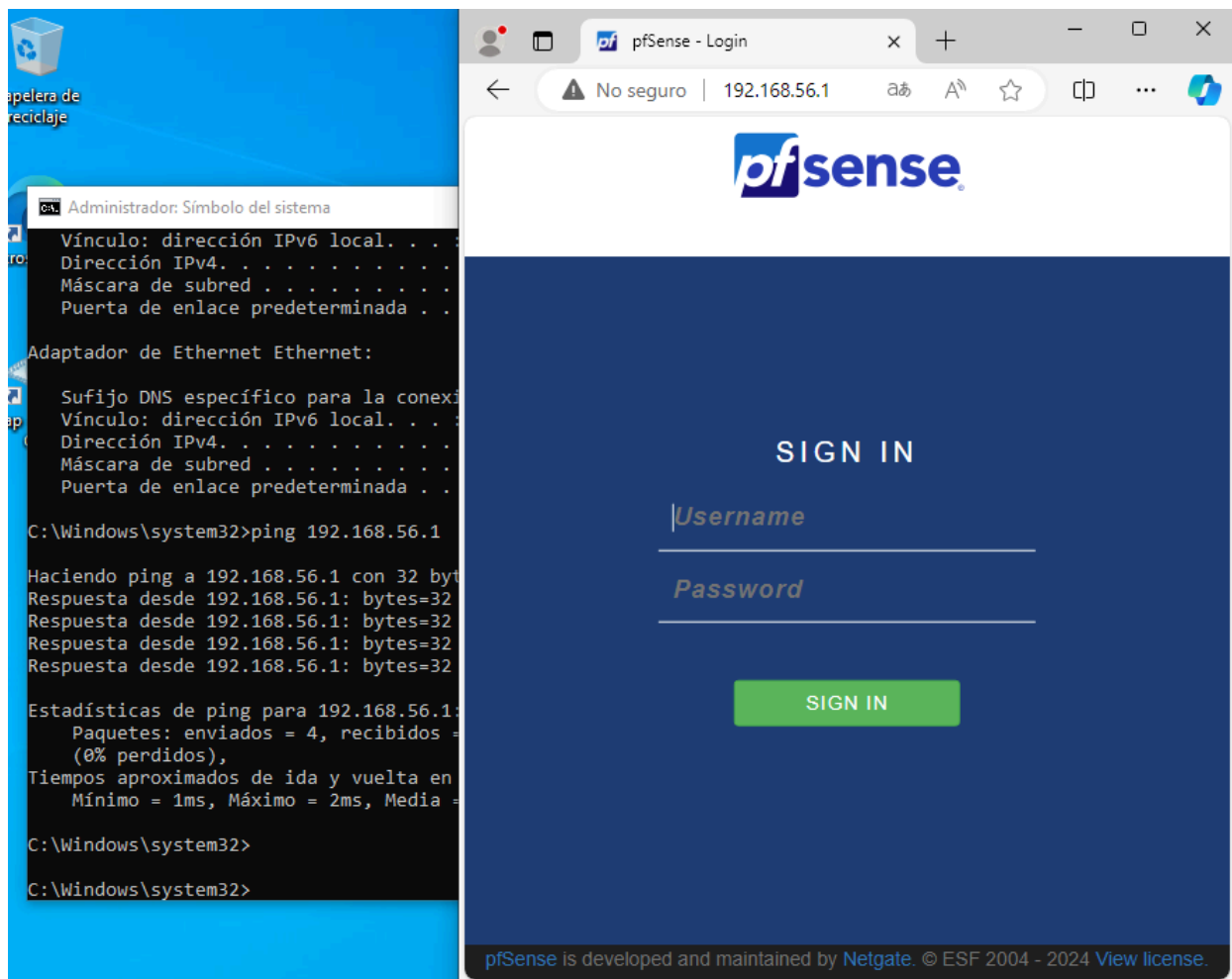
Enter an option: 7

Enter a host name or IP address: 192.168.56.106

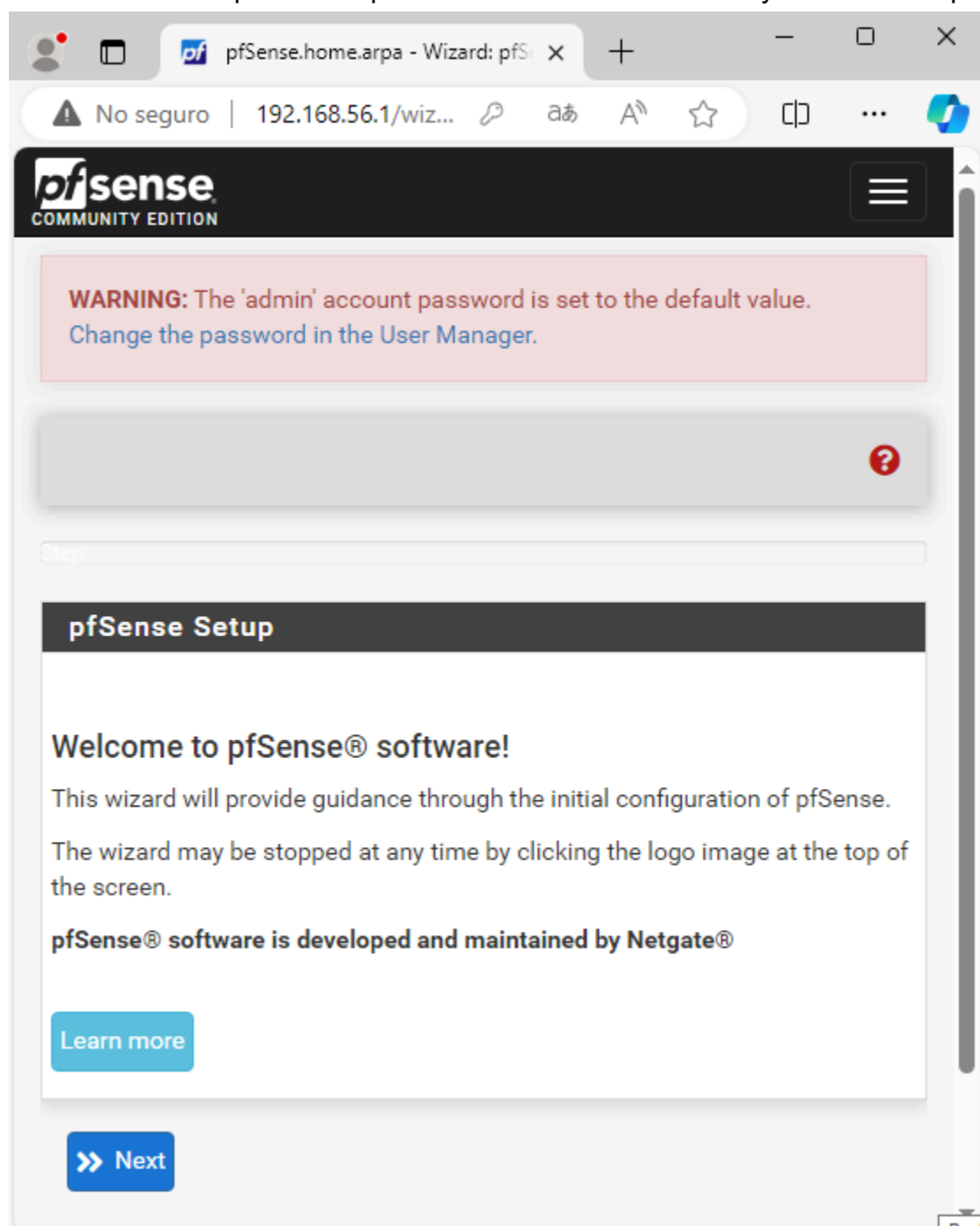
PING 192.168.56.106 (192.168.56.106): 56 data bytes
64 bytes from 192.168.56.106: icmp_seq=0 ttl=128 time=1.857 ms
64 bytes from 192.168.56.106: icmp_seq=1 ttl=128 time=1.687 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=128 time=1.703 ms

--- 192.168.56.106 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.687/1.749/1.857/0.077 ms
```

Además de hacer ping de una a la otra, podemos entrar a la máquina de PFSense, abriendo un navegador y accediendo a la IP.



Las credenciales que vienen por defecto de User es 'admin' y la Password 'pfsense'.



Una vez dentro de la configuración de PFSense, desde Windows 10, le dejaremos el nombre pfSense, nombre de dominio bosquempresa.local, pondremos DNS 1.1.1.1 (Cloudflare) y 8.8.8.8 (google)

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

Configuramos la información horaria del servidor para GMT+2.

The screenshot shows the pfSense Setup Wizard at Step 3 of 9, titled "Time Server Information". The browser address bar shows the URL "192.168.56.1/wizard.php?xml=setup_wizard.xml". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb navigation is "Wizard / pfSense Setup / Time Server Information". A progress bar indicates "Step 3 of 9". The section title "Time Server Information" is displayed. Below it, a prompt says "Please enter the time, date and time zone." The form contains two fields: "Time server hostname" with the value "2.pfsense.pool.ntp.org" and a sub-prompt "Enter the hostname (FQDN) of the time server.", and "Timezone" with a dropdown menu set to "Etc/GMT+2". A blue "Next" button is at the bottom.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Etc/GMT+2 ▾

Next

Dejamos la WAN en DHCP, que es lo que viene por defecto.

The screenshot shows the pfSense Setup Wizard at Step 4 of 9, titled "Configure WAN Interface". The progress bar indicates "Step 4 of 9". The section title "Configure WAN Interface" is displayed. Below it, a prompt says "On this screen the Wide Area Network information will be configured." The form contains a single field: "SelectedType" with a dropdown menu set to "DHCP".

Step 4 of 9

Configure WAN Interface

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

SelectedType: DHCP ▾

Dejamos la IP de LAN en la que tenemos actualmente y lo mismo con la máscara.

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="192.168.56.1"/>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/>

Cambiamos la 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.

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

Avanzamos y terminamos la configuración inicial.

Wizard / pfSense Setup / Wizard 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.

Ahora el siguiente paso en este ejercicio práctico, será configurar una regla de firewall para bloquear todo el tráfico hacia el sitio web www.elcorteingles.com. Esto se logra creando una regla en la interfaz LAN que deniegue el tráfico destinado a las direcciones IP asociadas con ese dominio.

Debemos ir al apartado Firewall > Rules > Add.

pfSense COMMUNITY EDITION System Interfaces **Firewall** Services VPN Status Diagnostics Help

Firewall / Rules / LAN List View ?

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"/>	4/82 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0/1 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Seleccionaremos la interfaz LAN, en Protocol seleccionamos Any, para que bloquee todo tipo de tráfico al sitio web. En Source dejaremos Any, para bloquear el tráfico desde cualquier origen. En Address Family, elegiremos IPv4. Ahora en Destination debemos elegir address or alias y buscar la IP del corteingles.

Para obtener esta IP abrimos una consola y usamos el comando ping ó nslookup seguido de www.elcorteingles.com . Esto nos devolvió la IP 92.123.56.146.

```
C:\Users\Admin>nslookup www.elcorteingles.com
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: e5112.b.akamaiedge.net
Address: 92.123.56.146
Aliases: www.elcorteingles.com
          grupoeci.elcorteingles.es.edgekey.net

C:\Users\Admin>ping www.elcorteingles.com

Haciendo ping a e5112.b.akamaiedge.net [92.123.56.146] con 32 bytes de datos:
Respuesta desde 92.123.56.146: bytes=32 tiempo=15ms TTL=54
Respuesta desde 92.123.56.146: bytes=32 tiempo=13ms TTL=54
Respuesta desde 92.123.56.146: bytes=32 tiempo=14ms TTL=54
Respuesta desde 92.123.56.146: bytes=32 tiempo=17ms TTL=54

Estadísticas de ping para 92.123.56.146:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 13ms, Máximo = 17ms, Media = 14ms
```

Una vez ya tenemos la IP, nuestra configuración de la primer regla de bloqueo al dominio elcorteingles.com se verá así en la siguiente imagen.

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

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

Address or Alias

92.123.56.146

/

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

Rule to block elcorteingles.com




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

Aplicamos los cambios.

Firewall / Rules / LAN



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

 Apply Changes

Vemos la regla creada

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

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"/>	4/157 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	92.123.56.146	*	*	none		Rule to block elcorteingles.com	
<input type="checkbox"/>	0/4 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

Probamos y no funcionó, como suele pasar, es difícil que salga a la primera. El fallo podría ser que elcorteingles.com tenga distintas IPs que vayan variando. Por lo que volvimos a hacer ping y confirmamos que tiene otra IP ahora, por lo que crearemos un Alias y agregaremos IPs a este alias y bloquearemos a través de este Alias.

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

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="23.210.46.124"/>	<input type="text" value="ip corte ingles"/>	
	<input type="text" value="92.123.56.146"/>	<input type="text" value="corte inglish"/>	

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

IP **Ports** URLs All

Firewall Aliases IP

Name	Type	Values	Description	Actions
corte	Host(s)	23.210.46.124, 92.123.56.146	block corte	

Add Import

Ahora creamos una nueva regla con este Alias que creamos y que se llama 'corte'.

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

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

Address or Alias

corte

/

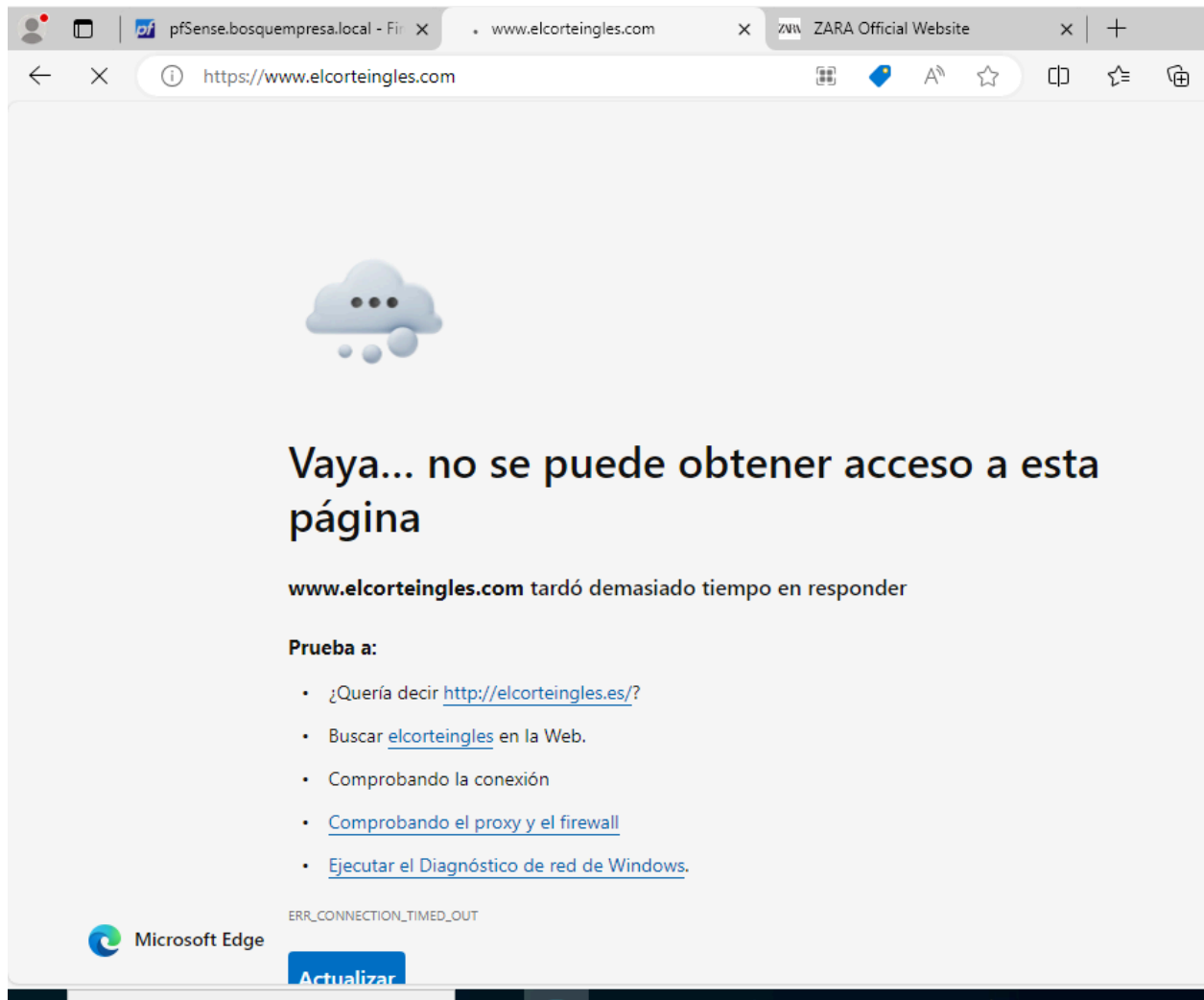
Extra Options

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).

Volvemos a probar y ahora sí que funciona nuestra primera regla!!



Ahora debemos configurar una segunda regla de firewall que bloquee el tráfico del puerto HTTP (puerto 80) para evitar el acceso a sitios web que no utilizan HTTPS. Esta regla debe aplicarse igualmente en la interfaz LAN. Haremos el mismo proceso inicial, Vamos a firewall > rules > add y ahora en Protocolo pondremos TCP. En source y destination pondremos Any. En Destination Port Range, en From pondremos any y en To pondremos HTTP(80).

Get 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
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 this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Any Destination Address /

Destination Port Range any From Custom HTTP (80) 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 Bloqueo HTTP
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](#)

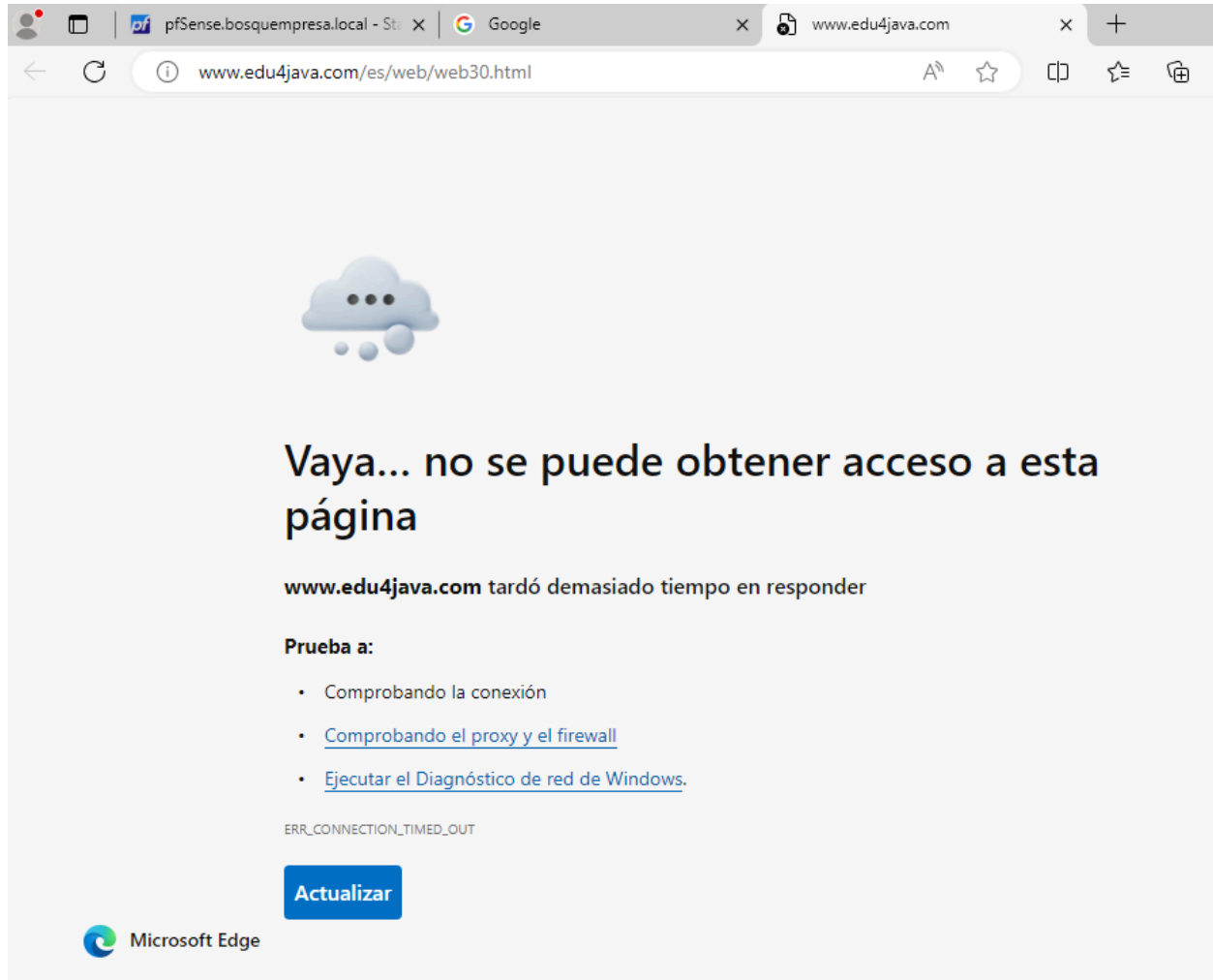
Vemos la regla creada.

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"/>	✓ 2/523 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/13 KiB	IPv4 TCP	*	*	*	*	*	none		Bloqueo HTTP	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	92.123.56.146	*	*	none		Rule to block elcorteingles.com	
<input type="checkbox"/>	✓ 11/49.84 MiB	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	

Para probar esta regla debemos usar una página web HTTP que funcione y no nos debería dejar abrirla.

Usaremos la página web: <http://www.edu4java.com/es/web/web30.html> .

Con esta segunda regla, tuvimos más suerte y funcionó a la primera!



Conclusiones

Durante esta actividad de instalación y configuración de pfSense, hemos explorado las funcionalidades clave de este software de firewall y enrutador, ampliamente reconocido por su confiabilidad y versatilidad en la gestión de seguridad de red. A través de pasos detallados, desde la preparación del entorno virtual hasta la implementación de reglas de firewall específicas, hemos adquirido una comprensión práctica de cómo utilizar pfSense para proteger y controlar el tráfico de red en un entorno controlado.

Al finalizar esta actividad, hemos logrado varios objetivos importantes:

1. Instalación y configuración básica de pfSense: Aprendimos a descargar, instalar y configurar pfSense en una máquina virtual, asegurándonos de tener los recursos necesarios y las interfaces de red configuradas adecuadamente.
2. Implementación de reglas de firewall: Configuramos reglas de firewall específicas para bloquear el tráfico hacia el sitio web www.elcorteingles.com y para bloquear el tráfico del puerto HTTP (puerto 80), demostrando nuestra capacidad para gestionar y controlar el tráfico de red según nuestras necesidades de seguridad.
3. Resolución de problemas: Enfrentamos desafíos y problemas comunes durante el proceso de configuración, como la necesidad de actualizar reglas de firewall debido a cambios en las direcciones IP del sitio web objetivo.

Esta actividad nos ha proporcionado una valiosa experiencia práctica en el uso de pfSense como una herramienta poderosa para garantizar la seguridad y la gestión eficiente de redes empresariales.