

Actividad 1 – Módulo 2

Instalación y configuración de pfSense

Diego Mucci

01/05/2024

Seguridad Informática

Introducción a pfSense

pfSense es un software de firewall y enrutador que también funciona como una plataforma para la gestión de seguridad de red basada en el sistema operativo FreeBSD. Este software es ampliamente reconocido por su confiabilidad y la gran cantidad de funcionalidades que ofrece, incluyendo VPN, prevención de intrusiones y servicios de balanceo de carga, entre otros. pfSense es una solución ideal para empresas que buscan asegurar sus redes mientras mantienen una gestión flexible y accesible.

Objetivo de la Actividad

El objetivo de esta actividad es familiarizarse con la instalación y configuración básica de pfSense en un entorno controlado utilizando una máquina virtual. Aprenderemos a implementar reglas de firewall específicas para gestionar y controlar el tráfico de red.

Pasos de la Actividad

1. Preparación del Entorno Virtual:

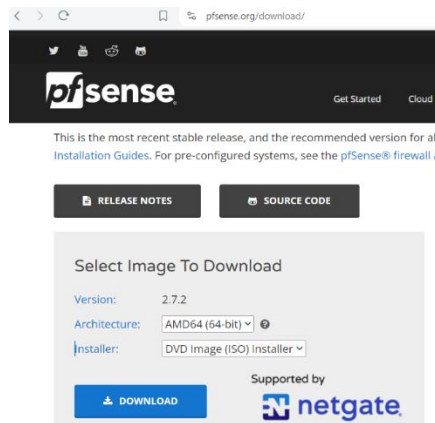
Descargar e instalar un software de virtualización como VMware Workstation o Oracle VM VirtualBox en tu ordenador.

Asegurarse de tener al menos 2 GB de RAM y 20 GB de espacio en disco disponible para la máquina virtual.

Este primer paso lo tenemos ya realizado debido al trabajo previo que venimos haciendo con las máquinas virtuales. Por lo tanto, el entorno virtual está correcto. En mi caso uso un Windows 10, así que me descargué Oracle VM VirtualBox para Windows 10 en su momento.

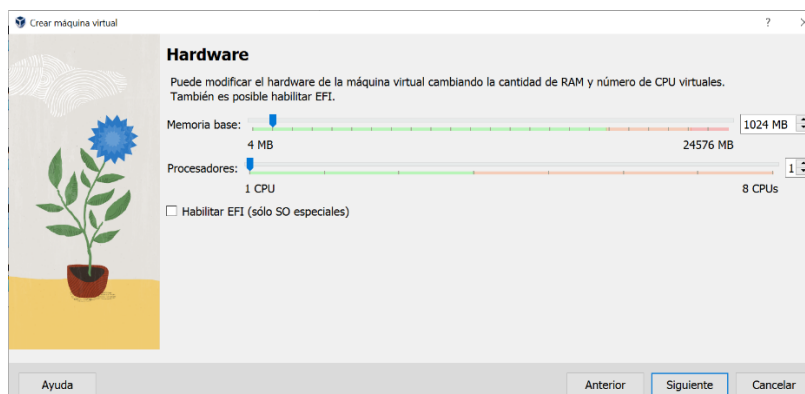
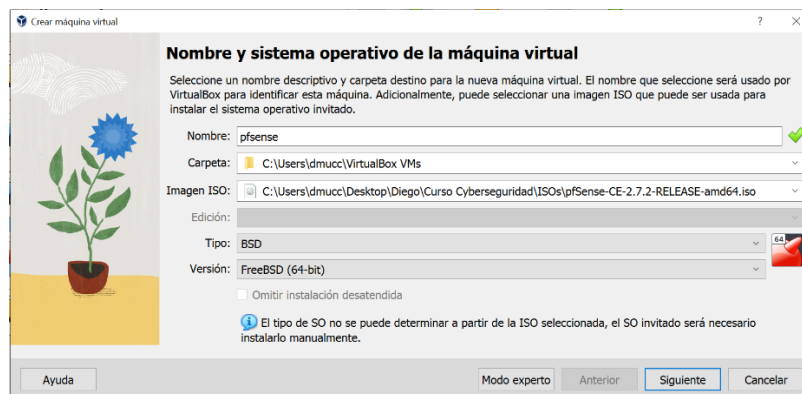
2. Descarga e Instalación de pfSense:

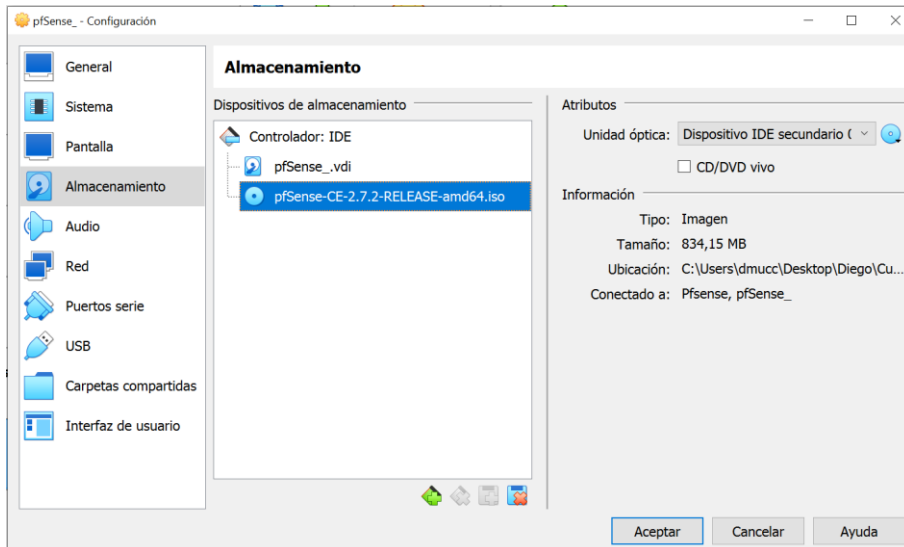
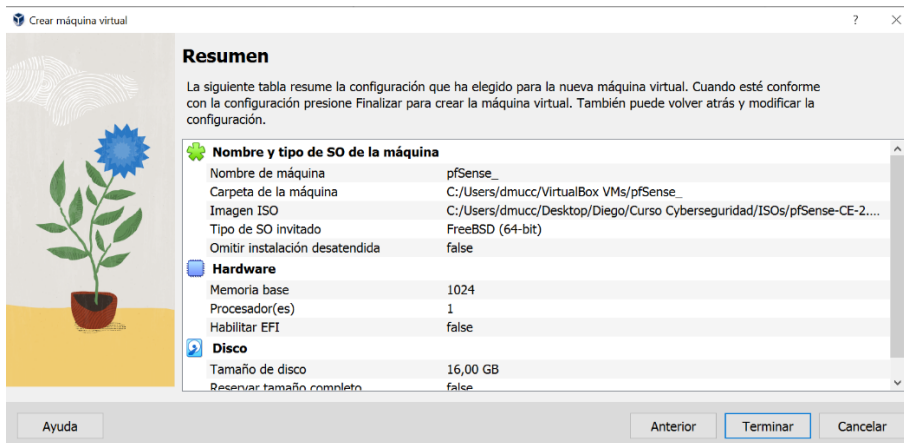
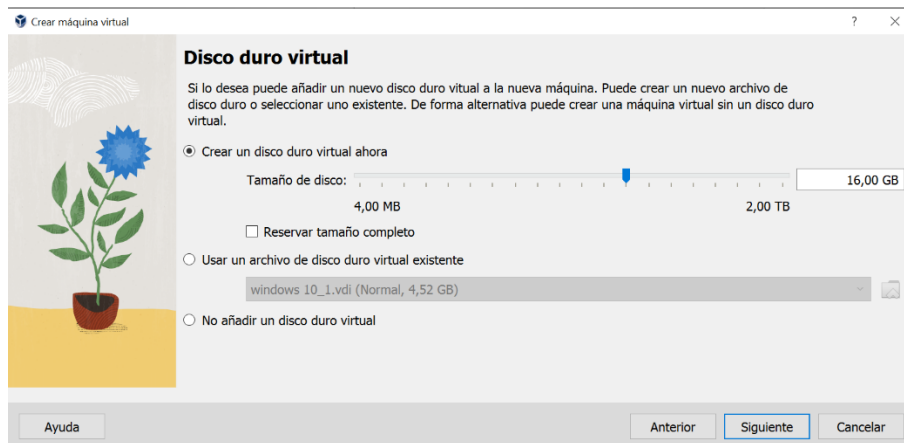
Acceder a la página oficial de pfSense (<https://www.pfsense.org>) y descargar la última versión estable del archivo ISO de pfSense.



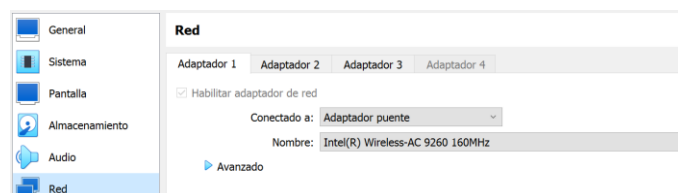
La imagen ISO que debemos descargar viene en formato comprimido, por lo tanto, lo primero que debemos hacer es descomprimir el archivo “.gz”.

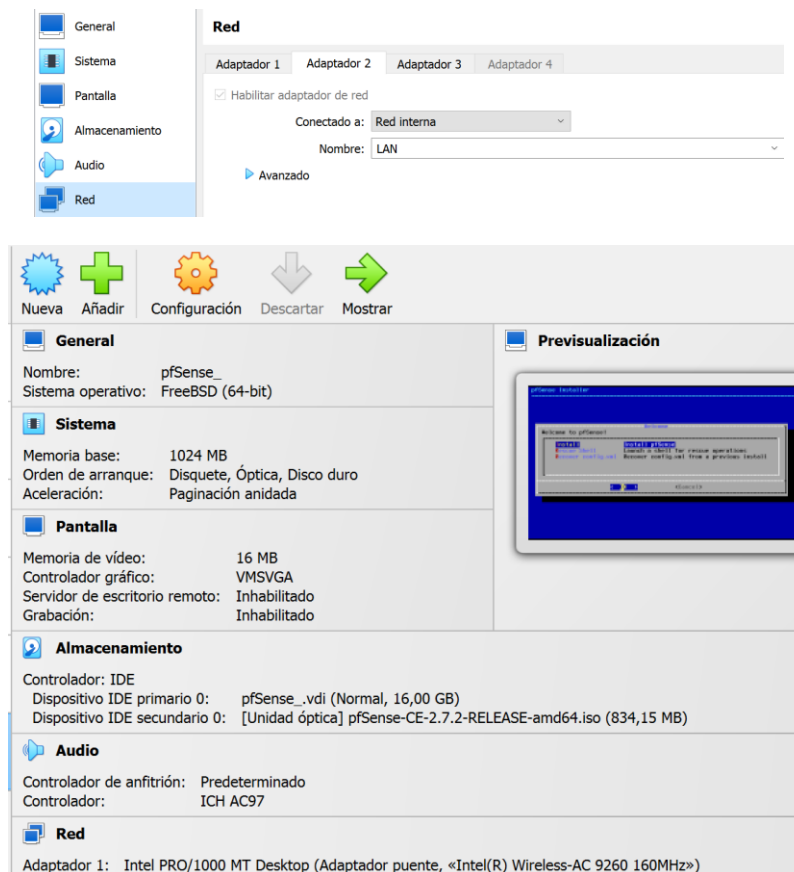
Después creamos una nueva máquina virtual en el software de virtualización y la configuramos para que arranque desde el archivo ISO descargado.



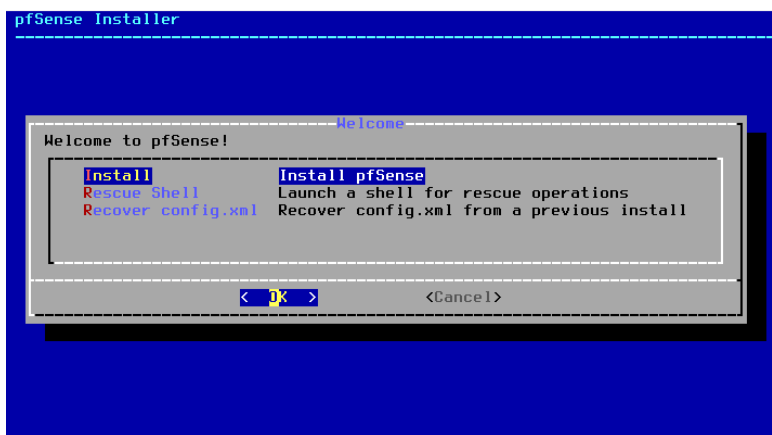


Seguidamente, le vamos a asignar dos tarjetas de red. Una configurada como adaptador puente, que será la WAN (para comunicarse con el exterior) y la otra como red interna, la cual denominaremos LAN (para comunicarse con Kali Linux).





Le damos a la flecha verde “Mostrar” para arrancar el proceso de instalación



Al final de la instalación eliminamos la imagen ISO para que no se vuelva a instalar y que arranque como máquina virtual.

- Configuración de las direcciones IP de pfSense:

```

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:
> 192.168.10.99

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

```

La WAN la dejamos con DHCP y a la LAN le dimos manualmente la IP 192.168.10.99, para que esté en la misma red que nuestra máquina virtual Kali Linux, a la cual le asignaremos más adelante una IP también de forma manual.

A la máscara de red le asignamos el valor 24.

* Nota: nuestro Windows Server tiene la IP 192.168.10.100, es por eso que se decidió darle un número menos, pero lo ideal y recomendable es dar números redondos para las IPs de este tipo de servicio.

```

Configuring filter for dynamic IPsec VPN hosts... done
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: 30a6cee116b76a5b4cd4

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

WAN (wan)    -> em0    -> v4/DHCP4: 192.168.1.135/24
LAN (lan)    -> em1    -> v4: 192.168.10.99/24

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

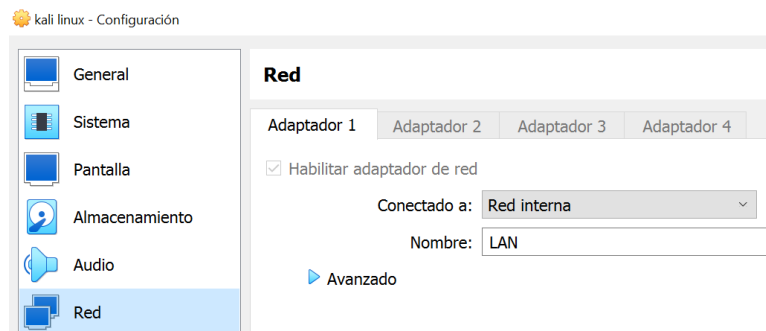
Enter an option:

```

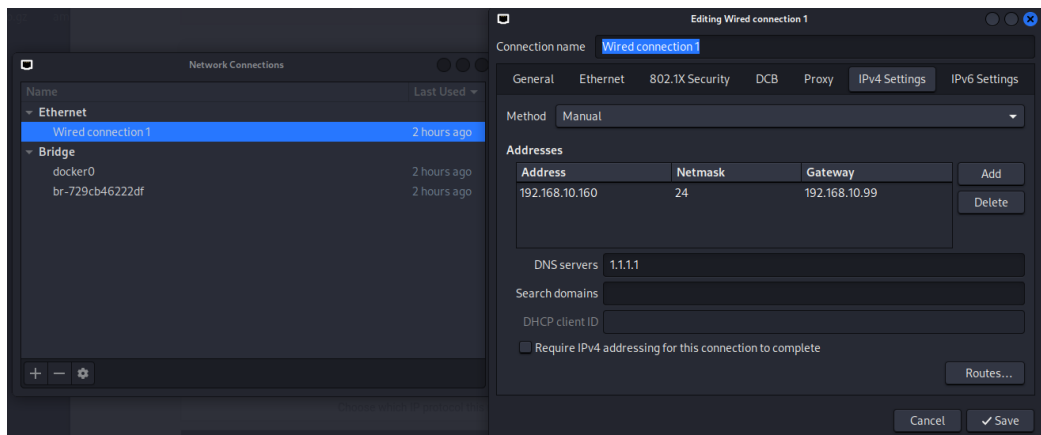
La tarjeta WAN obtiene su IP mediante el servidor DHCP, la cual será 192.168.1.135 tal y como vemos en la captura. Esta es la IP privada que va a conectar todo lo que esté conectado a la red interna con la red externa.

Ahora, en nuestra máquina virtual Kali Linux vamos a configurar la red de la siguiente manera:

- Desconectaremos la tarjeta de red “Adaptador puente” y dejaremos solo la tarjeta de red “Red Interna” a la cual la vamos a denominar LAN (debe tener exactamente el mismo nombre que la de pfSense para que puedan “encontrarse”)

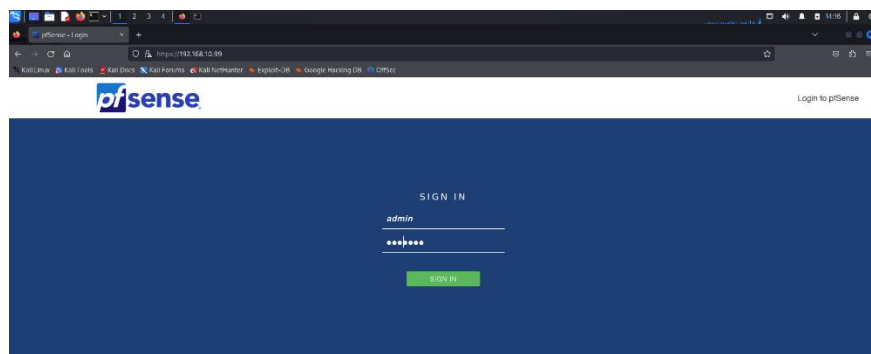


Dentro de la interfaz de red de Kali, le asignaremos una dirección IP de manera manual, una máscara de red y una puerta de enlace, esta última será la misma dirección IP que la LAN de pfSense. Es decir, se conectará a internet a través de pfSense. También le daremos la dirección DNS de Cloudflare, 1.1.1.1, para poder resolver las peticiones web.



3. Configuración de pfSense:

Una vez instalado, accedemos a la interfaz web de pfSense usando el navegador de la máquina host apuntando a la dirección IP asignada a la interfaz LAN de pfSense.



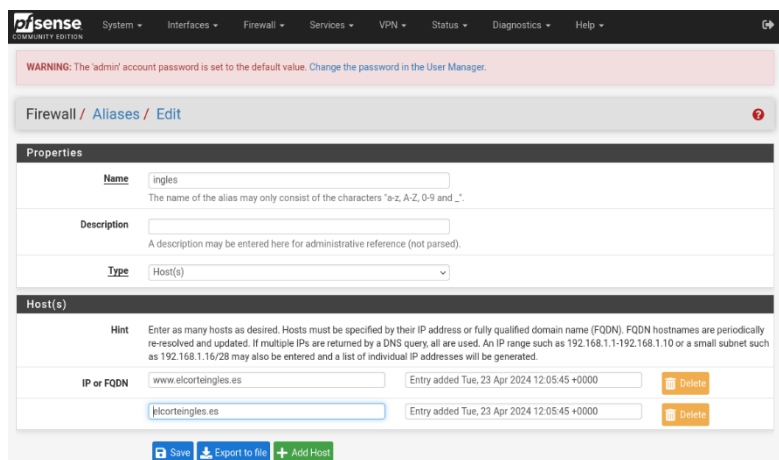
El usuario por defecto es admin y la contraseña es pfsense. Estos valores se los deberíamos cambiar una vez dentro para una mayor seguridad.

Para acabar, configuramos los ajustes básicos iniciales requeridos por el asistente de configuración de pfSense.

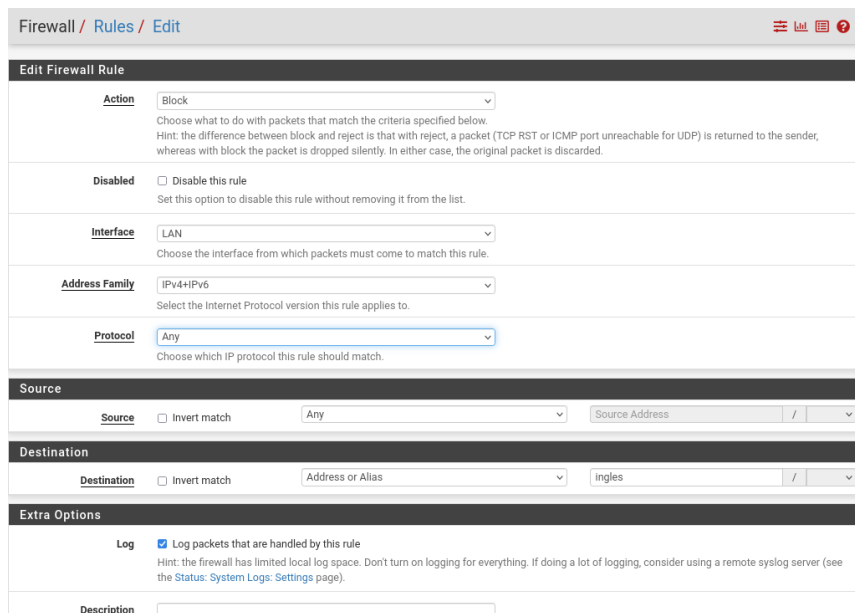
4. Implementación de Reglas de Firewall:

Configuraremos 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.

Primero vamos a crear un alias para la página web de El Corte Inglés así no tenemos que escribir el FQDN o la dirección IP cuando vayamos a bloquear el tráfico hacia este sitio web. A este alias lo llamaremos “ingles”.

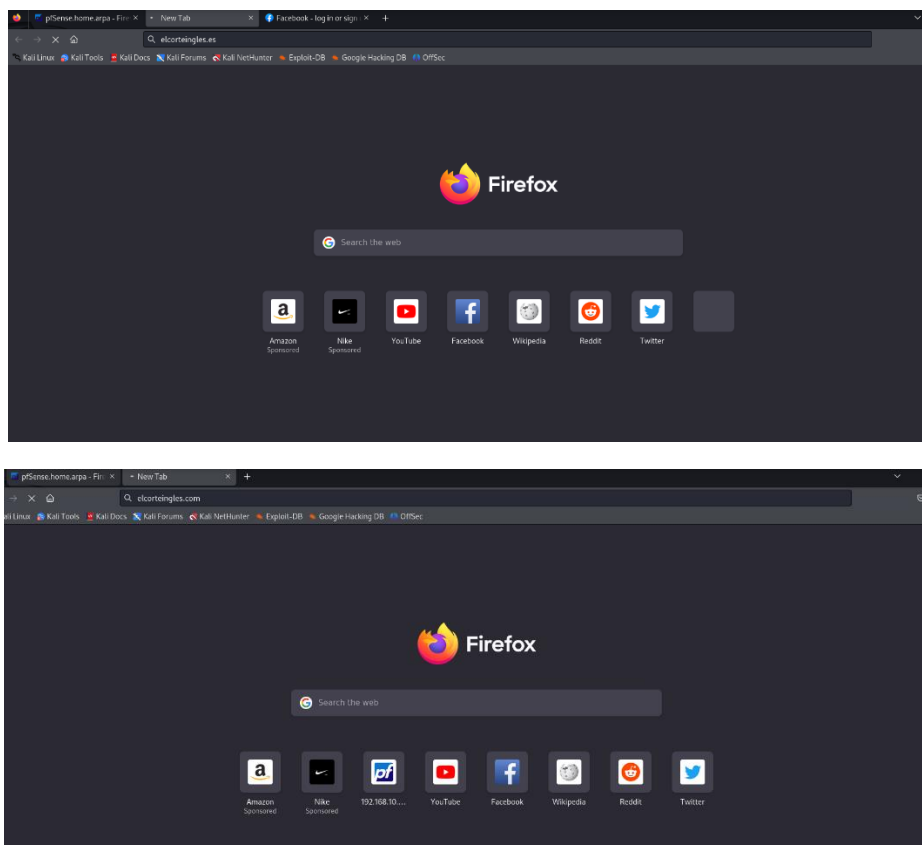


Después crearemos una regla en la interfaz LAN que deniegue el tráfico destinado a las direcciones IP asociadas con ese dominio. Para ello iremos a Rules → Edit y crearemos la regla de la siguiente manera:



Firewall / Rules / LAN											
Floating WAN LAN											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2/3.54 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4+6 *	*	*	ingles	*	*	none			
<input type="checkbox"/>	✓ 10/338.43 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	
Add Add Delete Toggle Copy Save Separator											

Aplicamos los cambios y corroboramos que entre a cualquier sitio web excepto a la web de El Corte Inglés. Como podemos observar en la siguiente imagen, probamos con la página de Facebook y esta sí que cargaba, pero el acceso a la web de El Corte Inglés estaba correctamente bloqueado.



A continuación, configuramos 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. La configuración quedaría de la siguiente manera:

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; otherwise 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:

☐ Invert match

Source: Any Source Address: / /

Destination:

☐ Invert match

Destination: Any Destination Address: / /

Destination Port Range:

Destination Port Range: HTTP (80) HTTP (80)

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

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

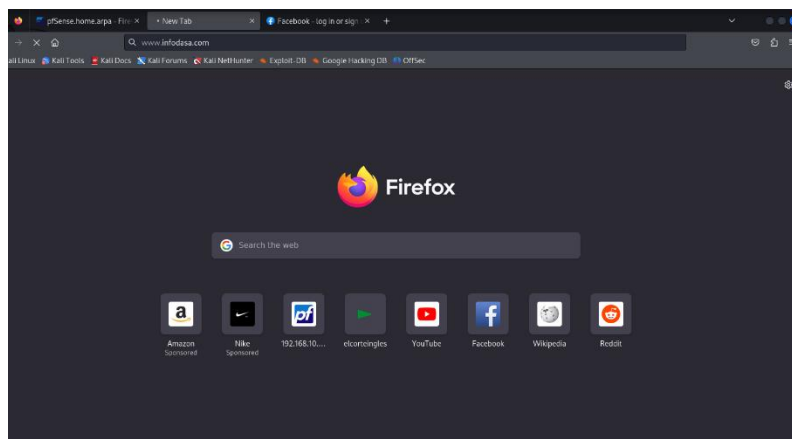
✓ Apply Changes

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"/>	✓ 1/3.81 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4+6 TCP	*	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✗ 0/0 B	IPv4+6 TCP	*	*	ingles	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 5/487.38 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	
<div> Add Add Delete Toggle Copy Save Separate</div>											

↑ Add ↓ Add 🗑️ Delete ⚙️ Toggle 📄 Copy 💾 Save ➕ Separator

Aplicamos los cambios y probamos de entrar a un sitio web que utilice el puerto 80, por ejemplo, www.infodasa.com. Como podemos observar en la siguiente imagen, no se puede acceder a este sitio web, pero sin embargo a facebook.com sí.



Conclusión

La ejecución de esta práctica ha resultado realmente interesante porque nos ha dado a conocer el uso de pfSense, el cual ofrece una solución robusta y flexible para la gestión de redes, especialmente en entornos empresariales. Además, nos ha servido para consolidar todo lo aprendido durante las clases teóricas, asentando mucho más toda la utilidad de un firewall. Aunque solo nos hemos centrado en este tipo de servicio, pfSense tiene capacidad para actuar tanto como firewall, enrutador, VPN, servidor DHCP, proxy y más, todo en una plataforma de código abierto, lo cual lo convierte en una opción atractiva para aquellos que buscan una solución todo en uno para sus necesidades de red.

Buen trabajo

10/10