



Las Fuentezuelas

Departamento de Informática

Informe técnico:

VPN e IDS/IPS en IPFire y pfSense.

Seguridad y Alta Disponibilidad.

Ciclo Superior de Grado Superior en
Administración de Sistemas Informáticos.

Este documento ha sido realizado únicamente con fines educativos. Se ruega que el uso de los contenidos del mismo sean con el mismo fin, y que no sea copiado.

Jorge Navarrete Secaduras.

Jaén, 29 de Enero de 2022.



1	<i>Introducción</i>	1
2	<i>IPFire</i>	1
2.1	<i>¿Qué es IPFire?</i>	1
2.2	<i>Instalación</i>	1
2.3	<i>Acceso a la interfaz web</i>	6
2.4	<i>OpenVPN en IPFire</i>	8
2.5	<i>IDS e IPS en IPFire</i>	13
2.6	<i>Opciones adicionales de protección</i>	15
2.7	<i>Demostración del IDS/IPS (Y port forwarding)</i>	16
2.8	<i>Ejemplos de reglas en firewall</i>	20
3	<i>pfSense</i>	23
3.1	<i>¿Qué es pfSense?</i>	23
3.2	<i>Instalación y configuración inicial</i>	23
3.3	<i>OpenVPN en pfSense</i>	28
3.4	<i>IDS/IPS en pfSense</i>	35
3.5	<i>Demostración del IDS/IPS (Y port forwarding)</i>	39
3.6	<i>Opciones adicionales de protección</i>	43
3.7	<i>Ejemplos de reglas en firewall</i>	49
4	<i>Conclusiones</i>	51
5	<i>Referencias</i>	51



1 Introducción

En esta práctica se instalará un servidor OpenVPN funcional y un sistema de detección y protección de intrusos (IDS e IPS) en IPFire y en pfSense. Por tanto, el documento se dividirá principalmente en dos partes: En la primera se trabajará con IPFire, y en la segunda con pfSense.

Durante toda la práctica se usarán ambos sistemas en máquinas virtuales, en el caso de IPFire se ha usado VMware, y en el caso de pfSense VirtualBox; aunque el proceso no variará, en cualquier caso.

2 IPFire

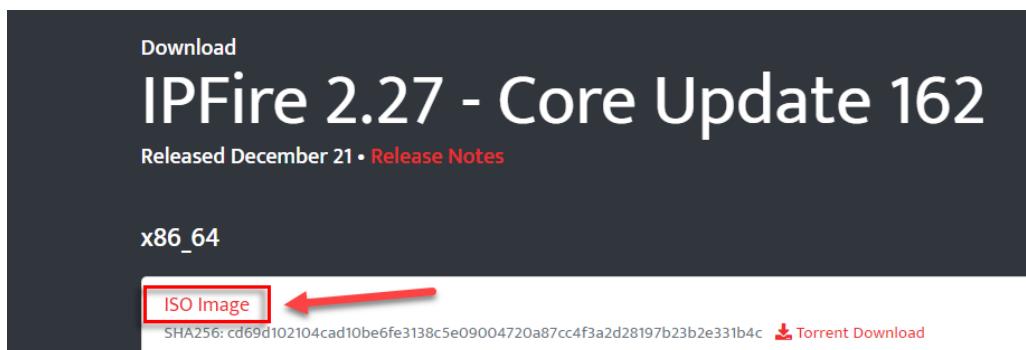
2.1 ¿Qué es IPFire?

Nos encontramos ante una distribución de Linux de código abierto que funciona como enrutador y firewall, destacando por su versatilidad y ligereza. Como es costumbre en estos sistemas, cuenta con una interfaz web para su administración y configuración.

Sus desarrolladores remarcan su seguridad y la potencia de su firewall, el cual nos protege de atacantes gracias a su sistema de detección y prevención de intrusos, así como de ataques de denegación de servicio.

2.2 Instalación

El primer paso para instalar IPFire es descargar su ISO, siempre desde su [sitio web oficial](#), y a poder ser, la última versión disponible.





Al estar trabajando con VMware Workstation 16, comenzaremos creando una máquina virtual, y, a través del asistente, indicar el uso de esta ISO descargada. Es un paso que, igualmente podemos realizar al final de la creación.

Acto seguido, indicamos un nombre y una ruta para los archivos de la máquina virtual. En este caso estoy creando la máquina virtual sobre un HDD, ya que no se necesita gran velocidad de escritura y lectura.

En cuanto a procesador y memoria RAM, IPFire nos expone que los requisitos mínimos son 1GB de RAM junto a un procesador cualquiera de 1GHz o más. Por ello, debido a los pocos recursos del host actual, se le asignará un núcleo de CPU y 1GB de RAM, lo cual podrá ser una limitación a la hora de establecer reglas IDS/IPS.

Respecto al disco duro, para esta distribución necesitamos mínimo 4GB. Como en este sentido no hay problema para asignar más (debido a que el espacio ocupado es dinámico), se le puede dar algo más. Para aumentar algo más el rendimiento, podemos guardar el disco duro virtual en un solo archivo.

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

Installer disc:
No drives available

Installer disc image file (iso):
C:\Users\Navarrete\Desktop\ipfire-2.27.x86_64-full-c
Browse...

⚠ Could not detect which operating system is in this disc image.

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
IPFire

Location:
D:\M\IPFire
Browse...

The default location can be changed at Edit > Preferences.

Memory for the Virtual Machine
How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

128 GB - Memory for this virtual machine: 1024 MB
64 GB -
32 GB -
16 GB -
8 GB - Maximum recommended memory: 6.2 GB
4 GB -
2 GB -
1 GB - Recommended memory: 768 MB
512 MB -
256 MB -
128 MB -
64 MB -
32 MB - Guest OS recommended minimum: 32 MB
16 MB -
8 MB -
4 MB -

Specify Disk Capacity
How large do you want this disk to be?

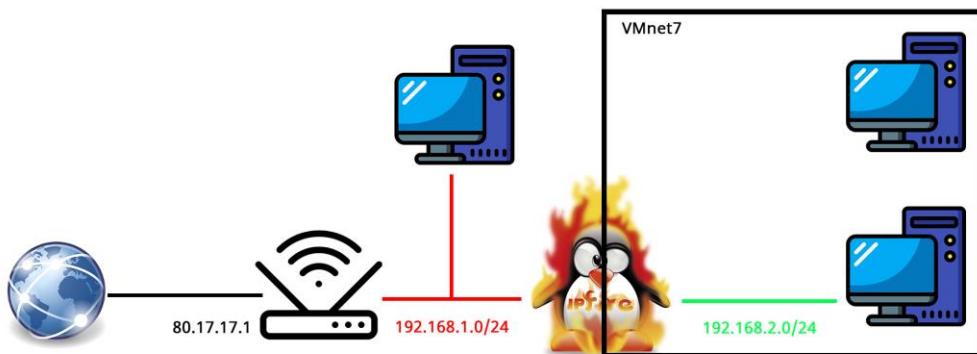
Maximum disk size (GB): 20.0
Recommended size for Other Linux 5.x and later kernel 64-bit: 8 GB

Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

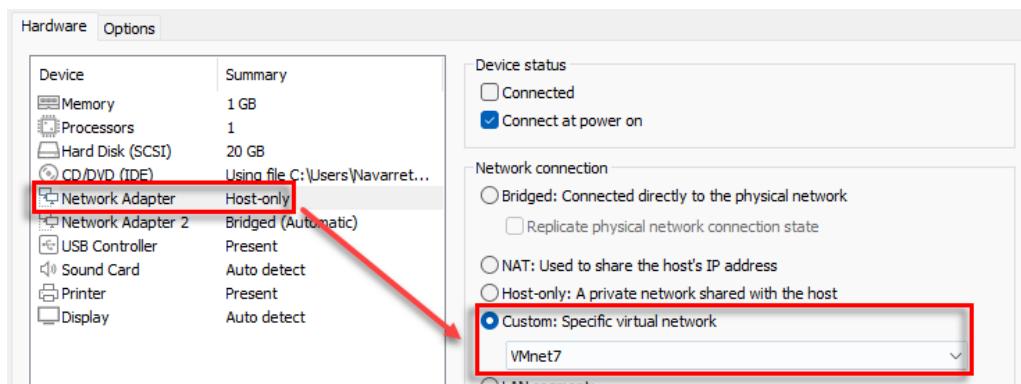
Store virtual disk as a single file
 Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.



Para esta práctica concreta estaré implantando IPFire entre mi red física y una red virtual de VMware. Para ello se configurará uno de los adaptadores virtuales en modo puente (El que será el WAN/red), y otro de ellos en modo Host-Only con la red virtual VMnet7, en la cual se encontrarán otras máquinas virtuales que me interesa securizar.



Se podrían configurar ambos adaptadores virtuales en modo puente sin ningún problema, y crear la subred “verde” en la misma topología física, pero por interés personal he tomado este esquema.



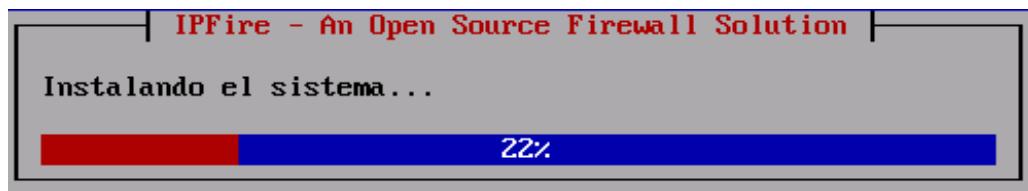
En cuanto finaliza la creación de la máquina virtual y la iniciamos, nos aparecerá la pantalla inicial de IPFire, desde donde se comenzará el proceso de instalación.

El primer paso será simplemente elegir el idioma para la instalación, en todos estos menús nos desplazamos con las flechas y seleccionamos con “Enter”.





A continuación se debe leer y aceptar la licencia (GNU), y, tras ello, el instalador de IPFire borrará todos los datos de los discos que se encuentren conectados al sistema en ese momento. Despues, esperarmos unos segundos para que se complete la instalación.



Pasado ese tiempo, se nos pedirá confirmar el reinicio del dispositivo para completar la instalación. Y, al iniciarla de nuevo sin la ISO en la unidad óptica virtual, comenzará el asistente de configuración inicial. El primer paso es indicar el layout de nuestro teclado.



Continúa solicitando la zona horaria (Europe/Madrid en nuestro caso), el nombre del host donde se ha instalado IPFire, y, de la misma manera, el nombre del dominio.

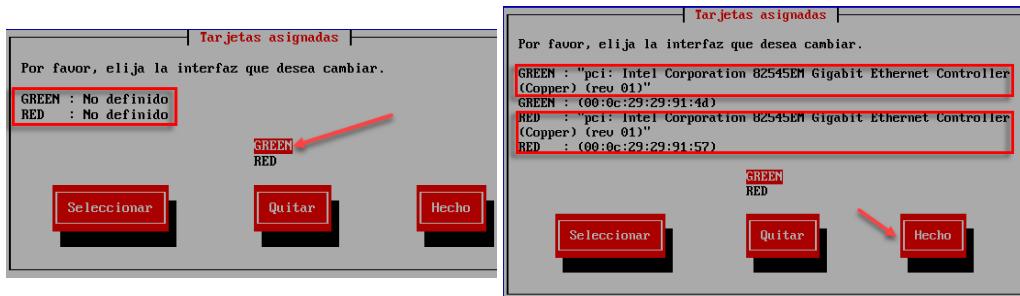


Después de indicar el nombre del dispositivo y de su dominio, estableceremos las contraseñas para el usuario root (con el que se iniciará sesión localmente) y para el usuario admin (con el que se trabajará desde la interfaz web).





Los únicos ajustes algo más delicados en la primera configuración son los que encontramos a continuación. El primero consiste en asignar las tarjetas de red a la interfaz "green" (LAN), y a la "red" (WAN). Simplemente debemos identificar mediante la MAC cuál es la tarjeta de red virtual que nos interesa para cada cual, y, seleccionando "green" y "red", indicar cada tarjeta. En caso de que se deseé contar con una DMZ, añadiríamos una interfaz "orange".



Tras seleccionar "hecho", debemos indicar las direcciones IPs de cada una de las interfaces. Comenzando con la "green", en este caso la estableceré en la red 192.168.2.0/24.



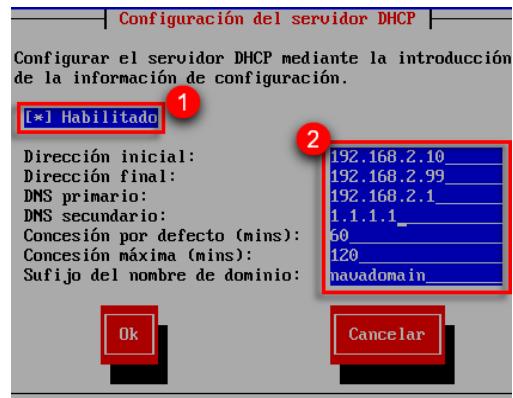
Por otro lado, a la interfaz "red" le indicaré que su dirección IP sea estática. Por defecto usará el DHCP de nuestro router, pero es recomendable establecer una IP fija para siempre tener conocimiento de la dirección.

La puerta de enlace seguirá siendo nuestro router, y la red la correspondiente 192.168.1/24.





Tras seleccionar “hecho” en la ventana anterior, se nos dirige hacia la configuración del servidor DHCP de la interfaz green. Para un funcionamiento total de la red interna, lo habilitaremos e indicaremos como inicio y final direcciones de la red 192.168.2.0/24. También podemos indicar un servidor DNS alternativo.



Finalmente, la configuración inicial de IPFire habrá finalizado, y se iniciará en modo terminal. En este punto podemos comenzar con su configuración a través de la interfaz web.

```
Starting connection daemon...
Starting DHCP Server...
Starting Unbound DHCP Leases Bridge...
Generating SSH key (rsa)...
Generating SSH key (ecdsa)...
Generating SSH key (ed25519)...
Generating HTTPS RSA server key (this will take a moment)...
Generating HTTPS ECDSA server key...
Signing RSA certificate...
Signing ECDSA certificate...
Starting Apache daemon...
Starting fcron...

IPFire v2.27 - www.ipfire.org
=====
NavaSecurity.navadomain running on Linux 5.15.6-ipfire x86_64
NavaSecurity login:
```

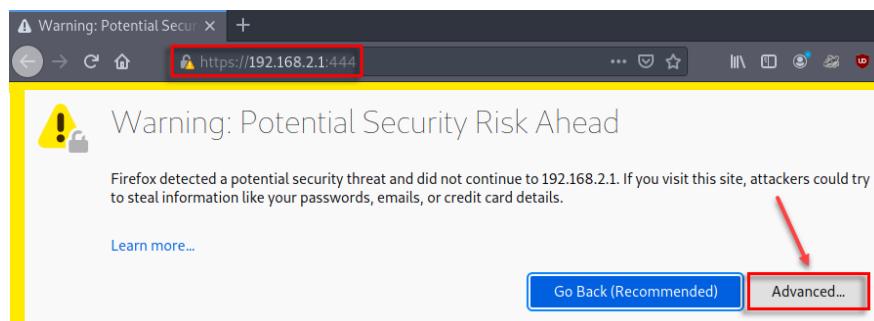
2.3 Acceso a la interfaz web

Con la configuración inicial correcta, al conectar una máquina virtual a la red VMnet7 donde se encuentra la interfaz “green” de IPFire junto a su servidor DHCP, el host recibirá una IP dentro del rango marcado y tendrá total conexión a Internet.

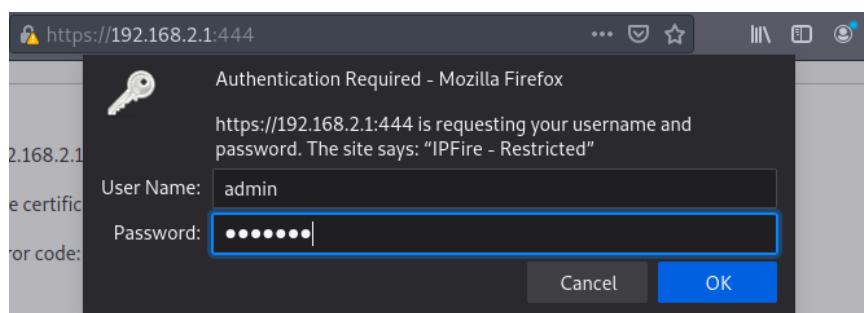
```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 00:0c:29:bd:f3:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.10/24 brd 192.168.2.255 scope global dynamic noprefixroute
        valid_lft 2852sec preferred_lft 2852sec
        inet6 fe80::dc3c:c64f:f9c2:2d02/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[samsepi01@parrot] ~ /Desktop]
$ ping twitter.com
PING twitter.com (104.244.42.129) 56(84) bytes of data.
```



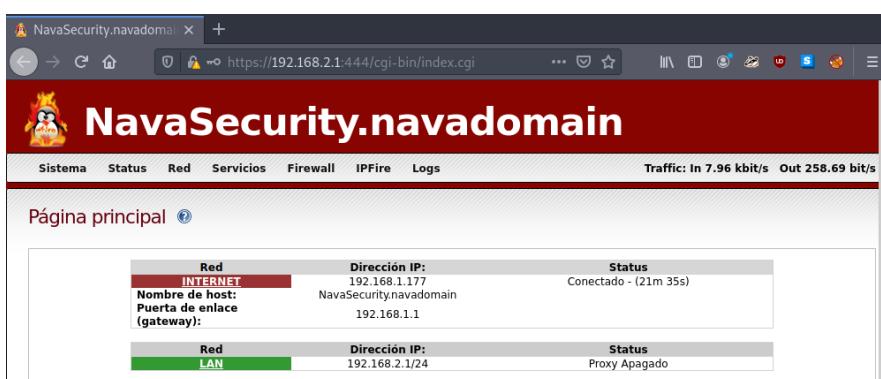
Desde este host, pues, podremos acceder a la interfaz web de IPFire escribiendo en cualquier navegador “<https://IP:444>”, ya que el puerto concreto es el 444. Como sabemos, al tener un certificado auto firmado debemos indicar a nuestro navegador que la fuente es confiable.



Al intentar acceder, será la página web la que nos pida iniciar sesión en el usuario admin a través de una alerta en el navegador. La contraseña de acceso será la que indicamos en la configuración inicial.



A partir de ahora, desde aquí será desde donde trabajaremos con IPFire, tanto para configurar el servidor OpenVPN, el sistema IDS e IPS, el firewall etc. Incluso podemos realizar descargas e instalaciones de módulos desde aquí.





2.4 OpenVPN en IPFire

En este punto usaremos IPFire para implantar un servidor VPN a través del cual se pueda acceder a la zona “green” desde una red externa. El primer paso es generar los certificados root y host desde la pestaña de “Servicios – OpenVPN”.

Autoridades de Certificado

Nombre	Asunto
Certificado Root:	No presente
Certificado de host:	No presente
Diffie-Hellman parameters:	No presente
TLS-Authentification-Key:	No presente

→ **Generar certificados root/host**

Como acostumbramos a hacer en los certificados auto firmados, indicamos un nombre cualquiera de organización y host; escribimos nuestro correo electrónico, ciudad, país etc.

Una vez la información está completa, podemos generar ambos certificados.

Con los certificados root y host generados, volvemos a la pestaña general de OpenVPN para comprobar la configuración general, donde es recomendable que usemos SHA2 como algoritmo para hash, AES-CBC 256 para el cifrado, y activar la protección TLS.

Navasecurity.navadomain

Sistema Status Red Servicios Firewall IPFire Logs

OpenVPN

Generar certificados root/host:

Nombre de organización: * Las Fuentezuelas
Nombre de host de IPFire: * NavaSecurity.navadomain
Su dirección de e-mail: jnavsecB30@g.educaand.es
Su departamento: Seguridad
Ciudad: Jaén
Estado o provincia: Jaén
País: Spain 2048 bit
Difie-Hellman parameters length:
Generar certificados root/host

Sistema Status Red Servicios Firewall IPFire Logs Traffic: In 8.61 kbit

4. Status de OpenVPN / Configuración:

Configuraciones globales

Status actual del servidor OpenVPN: DETENIDO
OpenVPN en RED:

Configuración de red:

Nombre de host/IP para VPN local: NavaSecurity.navadomain Subred de OpenVPN (ej: 10.0.10.0/255.255.255.0) 10.247.188.0/255.255.255.0
Protocolo: UDP Puerto destino: 1194
Tamaño de MTU: 1400

Cryptographic options:

Hash algorithm: SHA2 (512 bit) Encripción: AES-CBC (256 bit)
TLS Channel Protection:

Guardar Static IP address pools Opciones avanzadas de servidor Iniciar servicio



A partir de ahora, podemos iniciar el servidor OpenVPN desde el respectivo botón. Opcionalmente también podemos modificar la subred de OpenVPN, el puerto de destino y el nombre del host, pero no es necesario. En muchos manuales también se suele activar la compresión LZO desde opciones avanzadas, ya que sigue siendo vulnerable y explotable mediante Voracle.

The screenshot shows the '4. Status de OpenVPN / Configuración:' section. At the top, it says 'Status actual del servidor OpenVPN: EJECUTANDO' with a green button-like background. Below that, there's a checkbox labeled 'OpenVPN en RED' which is checked. The 'Configuración de red:' section contains fields for 'Nombre de host/IP para VPN local:' (set to 'NavSecurity.navadomain'), 'Protocolo:' (set to 'UDP'), 'Tamaño de MTU' (set to '1400'), 'Subred de OpenVPN (ej. 10.0.10.0/255.255.255.0)' (set to '10.247.188.0/255.255.255.0'), and 'Puerto destino:' (set to '1194'). The 'Cryptographic options:' section includes 'Hash algorithm' (set to 'SHA2 (512 bit)'), 'Encripción' (set to 'AES-CBC (256 bit)'), and 'TLS Channel Protection' (checkbox checked). At the bottom of the form are buttons for 'Guardar', 'Static IP address pools', 'Opciones avanzadas de servidor', and 'Detener servidor OpenVPN', with the last one being highlighted by a red box and an arrow pointing to it from the status message above.

No obstante, antes de poder conectar un cliente debemos crear el certificado del mismo. Para ello, en la misma ventana y algo más abajo, encontramos el apartado “Control y estado de conexión”, en él seleccionamos “Agregar”.

This screenshot shows the 'Control y Status de conexión:' section. It has a button labeled 'Agregar' which is highlighted with a red box, and another button labeled 'Estadísticas de conexión OpenVPN'.

El primer parámetro a completar será el nombre, es indiferente mientras sea genuinamente descriptivo. También activaremos el Dynamic IP address pool.

The screenshot shows the 'OpenVPN' configuration page. It has a 'Conexión:' section with fields for 'Nombre:' (set to 'VPNjorge'), 'Remarcar:' (set to 'Servidor VPN Navarrete'), and 'Activado:' (checkbox checked). Below that is a 'Choose network' section with a radio button selected for 'Dynamic OpenVPN IP address pool (10.247.188.0/255.255.255.0)'.



Igual que se hizo para el certificado de root y host, se llenarán los datos correspondientes para el certificado de conexión de usuario. Podemos subir un certificado o bien escribir a mano de nuevo correo electrónico, organización, departamento etc. y también una contraseña opcional para importar el certificado.

Autenticación

Subir una solicitud de certificado
 Subir un certificado No file selected.

Generar un certificado:

Nombre completo o nombre de host de Usuario: *

dirección de email de usuario:

Departamento de usuario:

Nombre de organización:

Ciudad:

Estado o provincia:

País:

Válido hasta (days): *

Archivo Contraseña PKCS12:

Archivo Contraseña PKCS12: (confirmación)

* Required field

En caso de necesitarlo, existe la posibilidad de forzar que todo el tráfico de la red se redirija a OpenVPN activando la opción “Redirect gateway”. Así mismo, también se pueden indicar direcciones DNS específicas y, obligatoriamente, elegir a qué interfaz se accede mediante OpenVPN, ya que, si tuviésemos una DMZ en “orange”, podríamos también dirigir el tráfico a ella.

Advanced client options:

Redirect Gateway:

Routing:

IPFire has access to these networks on the client's site

Client has access to these networks on IPFire's site None

Attention! If you change these settings, you have to restart the OpenVPN server that the changes take effect!

DNS1:
DNS2:
WINS:

Con el certificado creado, desde la ventana general del servicio optamos a descargar el certificado o todo el paquete de cliente en un ZIP.

Control y Status de conexión:

Dynamic OpenVPN IP address pool		Remarcar	Status	Acción
Nombre	Tipo			
VPNjorge	Host (Certificado)	Servidor VPN Navarrete	DESCONECTADO	
Leyenda: <input checked="" type="checkbox"/> Activado (click para desactivar) <input type="checkbox"/> Desactivado(click para activar)		Mostrar certificado Editar		Remover
		Descargar certificado Descargar paquete de cliente (zip)		

Autoridades de Certificado



Este archivo comprimido contiene el certificado, la clave y la configuración de conexión OpenVPN. En un cliente Windows con OpenVPN GUI instalado, podemos situar todos los archivos en la carpeta “config” del software para iniciar la conexión.

Este equipo > Disco local (C:) > Archivos de programa > OpenVPN > config		
	Nombre	Fecha de modificación
D-IPFire		
-IPFire	README.txt	15/12/2021 9:57
sonal	ta.key	22/01/2022 13:12
	VPNjorge.p12	22/01/2022 13:24
	VPNjorge-TO-IPFire.ovpn	22/01/2022 14:17

Aunque, antes de ello, para realizar una prueba lo más real posible, se abrirán los puertos del router para permitir la conexión a la VPN desde Internet. Con este objetivo accedemos a la interfaz de configuración de nuestro router y abrimos los puertos 1194, bastaría con hacerlo solo para el protocolo UDP, pero por si se decide cambiar la configuración de OpenVPN, se ha abierto en ambos protocolos.

Configuración Puertos

Rellena los siguientes campos y pulsa el botón **Añadir**. Ten en cuenta que para abrir un rango d

Nombre regla de puertos:	VPN
Dirección IP:	192.168.1.177
Protocolo:	TCP+UDP
Abrir Puerto/Rango Externo (WAN):	1194 (ej: 5001:5010)
Abrir Puerto/Rango Interno (LAN):	1194 (ej: 5001)

Finalmente, debemos modificar ligeramente el archivo de configuración de OpenVPN, cambiando el valor del parámetro “remote” para indicar que se conectará al servidor mediante la IP pública y el puerto.

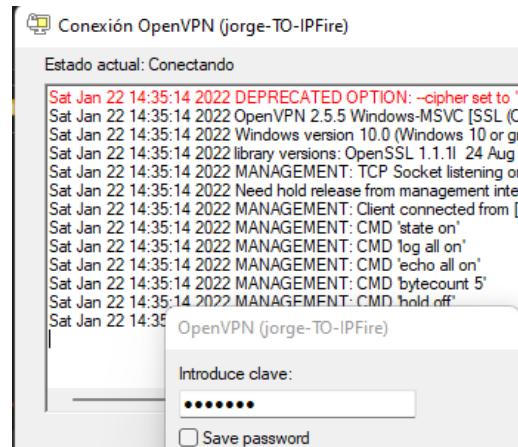
Después debemos guardar este archivo y ejecutar OpenVPN GUI.

```
*VPNjorge-TO-IPFire.ovpn: Bloc de notas
Archivo Editar Formato Ver Ayuda
#OpenVPN Client conf
tls-client
client
nobind
dev tun
proto udp
tun-mtu 1400
#remote NavaSecurity.navadomain 1194
remote [REDACTED] 1194
pkcs12 VPNjorge.p12
cipher AES-256-CBC
auth SHA512
tls-auth ta.key
verb 3
remote-cert-tls server
```



Al abrirlo nos pedirá la contraseña que se estableció en la creación del certificado, en caso de que se hiciese.

Después se comenzará la conexión con el servidor, la cual llevará unos segundos, el icono de OpenVPN cambiará a color verde y se nos dará una dirección IP de la subred de la VPN.



Una vez conectados, desde IPFire podremos identificar al usuario conectado y ver su sesión, dirección virtual, bytes enviados y recibidos etc.

Control y Status de conexión:

Dynamic OpenVPN IP address pool		Nombre	Tipo	Remarcar	Status	Acción
		jorge	Host (Certificado)	Servidor VPN Navarrete	CONECTADO	
Leyenda:		<input checked="" type="checkbox"/> Activado (click para desactivar)	Mostrar certificado	Editar		Remover
		<input type="checkbox"/> Desactivado(click para activar)	Descargar certificado	Descargar paquete de cliente (zip)		

[Agregar](#) [Estadísticas de conexión OpenVPN](#)

NavSecurity.navadomain

Sistema Status Red Servicios Firewall IPFire Logs Traffic: In 7.71 kbit/s Out 452.72 bit/s

Estadísticas de conexión OpenVPN [?](#)

Estadísticas de conexión OpenVPN							
Nombre común	Dirección Real	País	Dirección Virtual	Conectado en	Bytes enviados	Bytes recibidos	Última actividad
Jorge	192.168.1.1:49723		10.247.188.6	2022-01-22 14:35:36	5.74 KB	5.59 KB	2022-01-22 14:35:36

Las estadísticas se actualizaron por última vez el 2022-01-22 14:36:46

[ATRÁS](#)

IPFire 2.27 (x86_64) - Core Update 162 IPFire.org • Support the IPFire project with your donation

Con esto, el servidor OpenVPN desde IPFire queda configurado y totalmente funcional. Posteriormente en esta misma práctica se realizará una configuración similar en pfSense, en el cual, a pesar de que el proceso será ligeramente diferente, el concepto a seguir será el mismo.



2.5 IDS e IPS en IPFire

Uno de los aspectos más útiles a implementar con estos sistemas como pfSense o IPFire es el Intrusion detection system (IDS) y el Intrusion Prevention System (IPS). Con el primero de ellos se detectará tráfico sospechoso en la red mediante reglas SNORT. En el caso de aplicar reglas gratuitas, las más recomendables son las de Emergingthreats Community; deberíamos automatizar su actualización diariamente, o, como mucho, semanalmente.

Sistema de Detección de Intrusiones

Detección de Intrusiones

Daemon DETENIDO

Configuraciones

Enable Intrusion Prevention System Monitor traffic only

Monitored Interfaces

Activado en RED Activado en Green

Guardar

Ruleset Settings

Actualización de reglas SNORT

Emergingthreats.net Community Rules

Automatic Rule Update

Weekly

Guardar

Una vez decidido el paquete de reglas, podemos activar el sistema de detección de intrusiones en la interfaz interna (green) o en ambas, y, habilitar, también, el sistema de prevención de intrusiones.

Sistema de Detección de Intrusiones

Sistema de Detección de Intrusiones

Detección de Intrusiones

Daemon DETENIDO

Configuraciones

Enable Intrusion Prevention System Monitor traffic only

Monitored Interfaces

Activado en RED Activado en Green

Guardar



Es recomendable personalizar las reglas a usar. En algunos casos nos puede interesar activar todas las reglas y monitorizar la red durante una semana aproximadamente para quitar las reglas que nos causan falsos positivos; en otros casos, puede ser más conveniente solo activar las que consideramos oportunas. En este caso he activado las reglas para detectar ataques, exploits, escaneos, ejecución de malware etc.

Reglas del sistema de detección de intrusiones (2022-01-22 17:58:31)

<input type="checkbox"/> 3coresec.rules
<input type="checkbox"/> botcc.rules
<input type="checkbox"/> ciarmy.rules
<input type="checkbox"/> compromised.rules
<input type="checkbox"/> drop.rules
<input type="checkbox"/> dshield.rules
<input type="checkbox"/> emerging-activex.rules
<input checked="" type="checkbox"/> emerging-adware_pup.rules
<input checked="" type="checkbox"/> emerging-attack_response.rules
<input type="checkbox"/> emerging-chat.rules
<input type="checkbox"/> emerging-coimminer.rules
<input type="checkbox"/> emerging-current_events.rules
<input type="checkbox"/> emerging-deleted.rules
<input type="checkbox"/> emerging-dns.rules
<input type="checkbox"/> emerging-dos.rules
<input checked="" type="checkbox"/> emerging-exploit.rules
<input checked="" type="checkbox"/> emerging-exploit_kit.rules
<input type="checkbox"/> emerging-ftp.rules
<input type="checkbox"/> emerging-games.rules
<input type="checkbox"/> emerging-hunting.rules
<input checked="" type="checkbox"/> emerging-icmp.rules
<input checked="" type="checkbox"/> emerging-icmp_info.rules
<input checked="" type="checkbox"/> emerging-imap.rules
<input type="checkbox"/> emerging-inappropriate.rules
<input type="checkbox"/> emerging-info.rules
<input type="checkbox"/> emerging-ja3.rules
<input type="checkbox"/> emerging-malware.rules

Con las reglas establecidas, aplicadas, y el sistema de detección de intrusos activo en la red interna (interfaz "green"), si realizamos cualquier tipo de ataque o si generamos cualquier tráfico sospechoso que choque con alguna regla activa, esta creará una alerta en el registro del IDS.

Realizando un ataque simple desde la propia red interna podemos confirmar que esto es así. En este caso estoy realizando un Nmap a toda la red, y, por supuesto, el sistema IDS nos lo reportará desde su correspondiente log.

The screenshot shows two windows. On the left, a terminal window titled 'samsep10@parrot ~Desktop' displays the command 'nmap -sS 192.168.2.0/24' and its output, which includes scanning ports 53, 81, 444, 1433, 1521, 3306, 5432, 5802, 5810, 5901, 5904, 5906, 5910, 5911, 5915, and 5916. It also lists MAC addresses and scanned ports on 192.168.2.10. On the right, a browser window shows the pfSense log for January 22nd. A red arrow points from the terminal window to the log table, highlighting several entries related to MySQL and PostgreSQL traffic. The log table has columns for Fecha, Prioridad, Información IP, Nombre, and Tipo. Most entries have 'no encontrado' in the Referencias column. One entry for MySQL port 3306 has '192.168.2.10:55140 -> 192.168.2.1:3306' in the Referencias column.

Fecha:	Prioridad:	Información IP:	Nombre:	Tipo:	Más nuevos
01/22 18:31:15	2	192.168.2.10:55140 -> 192.168.2.1:3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traffic	2010937
01/22 18:31:16	2	192.168.2.10:55141 -> 192.168.2.1:3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traffic	2010937
01/22 18:31:17	2	192.168.2.10:55140 -> 192.168.2.1:5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	2010939
01/22 18:31:17	2	192.168.2.10:55140 -> 192.168.2.1:5432	ET SCAN Potential VNC Scan 5900-5920	Attempted Information Leak	2029911
01/22 18:31:17	2	192.168.2.10:55140 -> 192.168.2.1:1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	2010936
01/22 18:31:17	2	192.168.2.10:55141 -> 192.168.2.1:1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	2010936



2.6 Opciones adicionales de protección

Es importante conocer que, en IPFire, podemos bloquear conexiones que provengan de ciertos países activando el "Location block". Este aspecto es útil en ciertas ocasiones: Cuando nos realizan un ataque de denegación de servicio con una botnet formada por equipos que se encuentran en regiones específicas; cuando no deseamos que se pueda acceder a nuestros servicios a través de posibles servidores VPN de tipo no-spy; o bien cuando simplemente queremos que se acceda desde nuestros servicios solo desde nuestro país.

The screenshot shows the IPFire Firewall configuration interface. The top navigation bar includes 'Sistema', 'Status', 'Red', 'Servicios', 'Firewall' (which is highlighted with a red box), 'IPFire', and 'Logs'. The status bar at the top right indicates 'Traffic: In 2.68 kbit/s Out 245.76 bit/s'. Below the navigation, a section titled 'Configuración Location' is shown. A red box highlights the 'Location Block' button. Underneath it, there is a checkbox labeled 'Habilitar bloqueo basado Location:' which is checked. A red arrow points from the 'Location Block' button to the checkbox. A 'Guardar' (Save) button is located below the checkbox. The bottom part of the screenshot shows a table titled 'Países bloqueados' (Blocked Countries) with two columns of country information: Flag, Code, País.

Flag	Code	País
<input type="checkbox"/>	A1	Anonymous Proxy
<input type="checkbox"/>	A3	Worldwide Anycast Instance
<input checked="" type="checkbox"/>	AE	United Arab Emirates
<input checked="" type="checkbox"/>	AG	Antigua and Barbuda
<input checked="" type="checkbox"/>	AL	Albania
<input checked="" type="checkbox"/>	AN	Netherlands Antilles
<input checked="" type="checkbox"/>	AP	Asia/Pacific
<input checked="" type="checkbox"/>	AR	Argentina
<input type="checkbox"/>	AT	Austria
<input checked="" type="checkbox"/>	AW	Aruba
<input checked="" type="checkbox"/>	AZ	Azerbaijan
<input checked="" type="checkbox"/>	BB	Barbados
<input type="checkbox"/>	BE	Belgium
<input type="checkbox"/>	A2	Satellite Provider
<input checked="" type="checkbox"/>	AD	Andorra
<input checked="" type="checkbox"/>	AF	Afghanistan
<input checked="" type="checkbox"/>	AI	Anguilla
<input checked="" type="checkbox"/>	AM	Armenia
<input checked="" type="checkbox"/>	AO	Angola
<input checked="" type="checkbox"/>	AQ	Antarctica
<input checked="" type="checkbox"/>	AS	American Samoa
<input checked="" type="checkbox"/>	AU	Australia
<input checked="" type="checkbox"/>	AX	Åland Islands
<input checked="" type="checkbox"/>	BA	Bosnia and Herzegovina
<input checked="" type="checkbox"/>	BD	Bangladesh
<input checked="" type="checkbox"/>	BF	Burkina Faso

La siguiente herramienta a destacar es "Guardian", para usarla, debemos descargarla como "addon" desde la ventana de Pakfire (ubicada en la pestaña IPfire).

En el apartado de "Addons disponibles" lo buscaremos por orden alfabético y lo seleccionaremos para su posterior instalación mediante el símbolo "+".

The screenshot shows the Pakfire configuration interface. The top navigation bar includes 'Sistema', 'Status', 'Red', 'Servicios', 'Firewall', 'IPFire' (highlighted with a red box), and 'Logs'. A red circle labeled '1' points to the 'IPFire' tab. Below the navigation, a section titled 'Configuración de Pakfire' is shown. A red circle labeled '2' points to the 'Addons disponibles' section. This section lists available add-ons with their names and descriptions. A red circle labeled '3' points to the 'guardian-2.0.2-25' entry, which is highlighted with a blue selection bar.

Addons disponibles:	Addons:
flashrom-1.2-2 foomatic-4.0.9-6 fping-5.0-6 freeradius-3.0.23-14 frr-8.0.1-2 ghostscript-9.55.0-9 git-2.33.1-20 gnu-netcat-0.7.1-1 gnum3d-3.0-7	Por favor elija uno o más elementos de la siguiente lista y haga click en el signo + para instalar Por favor elija uno o más ele click en el signo - para desins



Una vez instalado nos aparecerá en el menú desplegable, y desde ahí accedemos a su configuración. Simplemente, Guardian nos servirá para añadir otra capa de protección en caso de tener un servidor con SSH y/o httpd, ya que detectará de una forma muy fiable los ataques de fuerza bruta sobre ellos, y podrá bloquear al atacante.

The screenshot shows the IPFire web interface with the following details:

- Header:** Sistema, Status, Red, **Servicios** (highlighted with a red box and circle 1), Firewall, IPFire, Logs. Traffic: In 8.54 kbit/s Out 258.69 bit/s.
- Section 1:** Configuración de Guardian. It shows the "Guardian" service status as "DETENIDO".
- Section 2:** Configuration of Guardian. Under "Common Settings":
 - "Enable Guardian:" checked (highlighted with a red box and circle 2).
 - "SSH Brute Force Detection" and "httpd Brute Force Detection" both set to "on" (highlighted with a red box and circle 2).
 - "Log Facility:" Systemlog, "Log Level:" Info.
 - "Firewall Action:" Drop, "Strike Threshold:" 3.
 - "Block Time (seconds):" 86400.
- Action:** A red arrow points from circle 3 to the "Guardar" button.

2.7 Demostración del IDS/IPS (Y port forwarding)

Una vez configurado IPFire en este sentido, es oportuno realizar una prueba real para confirmar su funcionamiento. Antes de nada, abriré un servidor HTTP básico con Python3 en un host ubicado en la subred 192.168.2.0/24, es decir, dentro de la interfaz “green”.

```
> sudo python3 -m http.server 80
[sudo] password for n4v4:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.177 - - [27/Jan/2022 14:54:29] "GET / HTTP/1.1" 200 -
192.168.1.177 - - [27/Jan/2022 14:54:29] code 404, message File not
192.168.1.177 - - [27/Jan/2022 14:54:29] "GET /favicon.ico HTTP/1.1"
```

El objetivo será poder acceder a este servidor a través de Internet, por lo que no solo tendremos que hacer “port forwarding” en IPFire, también en la puerta de enlace doméstica.



Comenzaremos, igualmente, con la configuración del firewall de IPFire. Debemos acceder a “Firewall – rules” y crear una nueva regla seleccionando el botón de “Nueva regla”.

En ella se indicará que la fuente será cualquier red, ya que queremos tener el servidor abierto a Internet; a continuación, activamos NAT y el port forwarding. También debemos añadir como destino la dirección IP local específica del servidor al que redireccionará, así como el protocolo y el puerto de destino.

Sistema Status Red Servicios Firewall IPFire Logs Traffic: In 4.83 kbit/s Out 2.10 kbit/s

Firewall Rules

Source

Source address (MAC/IP address or network): Firewall Todos

Standard networks: Any Location A1 - Anonymous Proxy

NAT

Use Network Address Translation (NAT) Destination NAT (Port forwarding) Firewall Interface: - Automático -

Source NAT

Destination

Destination address (IP address or network): 192.168.2.101 Firewall Todos

Standard networks: Any Location A1 - Anonymous Proxy

Protocol

TCP Source port: Destination port: 80

Tras guardar la regla, esta se hallará indicada en la ventana de reglas del cortafuegos, podremos activar desde aquí el log para que guarde toda la información sobre las comunicaciones que pasan por esta regla.

Firewall Rules

New rule

Firewall Rules

#	Protocolo:	Source	Log	Destination	Action
1	TCP	Any	<input checked="" type="checkbox"/>	Firewall : 80 ->192.168.2.101: 80	<input checked="" type="checkbox"/>
		Green		Internet (Allowed)	

Póliza: Allowed



De esta forma, ya podremos acceder desde otras subredes locales al servidor web abierto temporalmente con Python3.

Para poder acceder a través de Internet, debemos hacer lo mismo en el router de nuestro ISP, abriendo el puerto 80.

El proceso cambiará ligeramente dependiendo del ISP y según el modelo de router; pero, en general, tras iniciar sesión en la página de administración a través de la IP del propio router, existirá una ventana “Ports” o “Port forwarding” para que podamos añadir las respectivas reglas.

Editar

Nombre <input type="text" value="test"/>	Protocolo TCP	Puerto/Rango Externo 80:80	Puerto/Rango Interno 80:80	Dirección IP 192.168.1.199
<input type="text" value="test"/>	UDP	80:80	80:80	192.168.1.199

Después de guardar esa configuración ya tenemos acceso al servidor HTTP a través de Internet, entrando desde un navegador conectado a otra red local introduciendo la IP pública del router; este hace el port forwarding al IPFire, y, a su vez, este lo vuelve a hacer hasta el servidor web.

En el log del firewall se podrán ver todas las comunicaciones, en ellos se indica la dirección IP pública de origen, el puerto etc.

Registros:

Número total de HITS al firewall Enero 27, 2022: 5809

Hora	Cadena	Iface	Proto	Origen Destino	Puerto origen Puerto Dst	País	Dirección MAC
15:08:28	FORWARDFW	red0	TCP	80.26.247.132 192.168.2.101	43512 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	DNAT	red0	TCP	80.26.247.132 192.168.1.199	43514 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	FORWARDFW	red0	TCP	80.26.247.132 192.168.2.101	43514 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	DNAT	red0	TCP	80.26.247.132 192.168.1.199	563(NNTPS) 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	FORWARDFW	red0	TCP	80.26.247.132 192.168.2.101	563(NNTPS) 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	DNAT	red0	TCP	80.26.247.132 192.168.1.199	43516 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	FORWARDFW	red0	TCP	80.26.247.132 192.168.2.101	43516 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	DNAT	red0	TCP	80.26.247.132 192.168.1.199	588(CAL) 80(HTTP)	ES	e4:ab:89:29:a8:ab
15:08:28	FORWARDFW	red0	TCP	80.26.247.132 192.168.2.101	588(CAL) 80(HTTP)	ES	e4:ab:89:29:a8:ab



Se añadió también una regla igual que la anterior, pero para el puerto 22, es decir, el del SSH. Tener SSH abierto a Internet es algo que NUNCA se debe hacer, pero puesto que estamos probando IPFire, me pareció adecuado hacerlo.

The screenshot shows the IPFire NAT configuration. Under 'Destination', the 'Destination address' is set to 192.168.2.101, and the 'Protocol' is set to TCP with port 22. The 'Source port' field is empty.

En el momento que se abrió el puerto 22 en IPFire y en el router doméstico, comenzaron a llegar intentos de inicio de sesión desde una IP alemana, por lo que no tuve ni que pedir ayuda a algún compañero para que me hiciesen una simulación de ataque.

The log viewer shows several failed connection attempts (DROP_INPUT) from the IP 62.171.146.23, which is identified as being from Germany (DE). The attempts were made on port 22 (SSH) and were blocked by the firewall.

Hora	Cadena	Iface	Proto	Origen Destino	Puerto origen Puerto Dst	País	Dirección MAC
15:24:49	DROP_INPUT	red0	UDP	192.168.1.177 192.168.1.255	54915 54915		18:c0:4d:a8:1f:09
15:24:50	DNAT	red0	TCP	62.171.146.23 192.168.1.199	35646 22(SSH)	DE	e4:ab:89:29:a8:ab
15:24:51	DROP_INPUT	red0	TCP	62.171.146.23 192.168.2.101	35646 22(SSH)	DE	e4:ab:89:29:a8:ab
15:24:51	DNAT	red0	TCP	62.171.146.23 192.168.1.199	35646 22(SSH)	DE	e4:ab:89:29:a8:ab
15:24:52	DROP_INPUT	red0	TCP	62.171.146.23 192.168.2.101	35646 22(SSH)	DE	e4:ab:89:29:a8:ab
15:24:53	DNAT	red0	TCP	62.171.146.23 192.168.1.199	35646 22(SSH)	DE	e4:ab:89:29:a8:ab
15:24:53	DROP_INPUT	red0	TCP	62.171.146.23 192.168.2.101	35646 22(SSH)	DE	e4:ab:89:29:a8:ab

Tal y como se aprecia en el “log”, los primeros intentos se “dropean” (“bloquean”) en el propio firewall, y al ser un ataque de fuerza bruta sobre mi SSH, si acudimos a la ventana de Guardian podemos observar que el host alemán que estaba intentando acceder se encuentra bloqueado durante 86400 segundos.

The 'Currently blocked hosts' section shows a single entry: 62.171.146.23, which has been blocked for 86400 seconds.

2.8 Ejemplos de reglas en firewall

Ya que la práctica solicita que se configure el firewall, se crearán algunas reglas de demostración en el cortafuegos de IPFire. Por defecto el firewall permite cualquier tráfico de salida desde la red interna, y, a su vez, bloquea todo el tráfico que intenta acceder a ella.

Por tanto, vamos a imaginar que deseamos acceder solamente desde la red 192.168.1.0/24 al SSH del dispositivo 192.168.2.13 que se encuentra en la interfaz "green". Para ello, creamos una nueva regla para comunicaciones que tengan como fuente (Source) cualquier IP de esta subred, activamos el NAT (port forwarding) igual que anteriormente, y establecemos el destino como el host específico, indicando finalmente el puerto 22.

Sistema Status Red Servicios **Firewall** IPPFire Logs

Traffic: In 2.92 kbit/s Out 0.00 bit/s

Firewall Rules

Source

Source address (MAC/IP address or network): **192.168.1.0/24**

Firewall Todos

Standard networks: Green (192.168.2.0/24)

Location A1 - Anonymous Proxy

NAT

Use Network Address Translation (NAT)

Destination NAT (Port forwarding)

Source NAT

Firewall Interface: - Automático -

Destination

Destination address (IP address or network): **192.168.2.13**

Firewall Todos

Standard networks: Any

Location A1 - Anonymous Proxy

Protocol

Source port: **TCP**

Destination port: **22**

External port (NAT):

Con esta regla activa, puedo acceder al SSH desde mi máquina en la subred 192.168.1.0/24.



Vamos a plantear otro escenario: Queremos que nuestros clientes ubicados en la red "green" únicamente accedan a servidores web mediante HTTPS, y que no puedan hacerlo por HTTP, jugar a videojuegos, usar SSH o Telnet a otros servidores etc. Para ello vamos a empezar creando una regla que va a bloquear TODO el tráfico que tenga como fuente nuestra red interna y como destino cualquier otra red.

The screenshot shows the IPfire Firewall configuration interface. It includes tabs for Source, NAT, Destination, and Protocol. The Protocol tab is active, with the 'Todos' dropdown menu open. A red box highlights the 'Protocol' tab and the 'Todos' dropdown. A red arrow points from the 'Protocol' tab to the 'DROP' button in the action bar below, which is also highlighted with a red box. The action bar has three buttons: ACCEPT (green), DROP (red), and REJECT (cyan).

Con el mismo método crearemos una regla para permitir (Accept) el tráfico HTTPS (puerto 443 con TCP), con la misma fuente y destino que en el caso anterior; y no se nos puede olvidar permitir también el tráfico con destino puerto 53 en TCP y UDP para las DNS, ya que estamos usando las DNS de Cloudflare (1.1.1.1). Después de crearlas, las situamos por encima de la de bloqueo, ya el orden en la tabla de reglas será el mismo orden que usará el firewall para permitir o bloquear los paquetes.

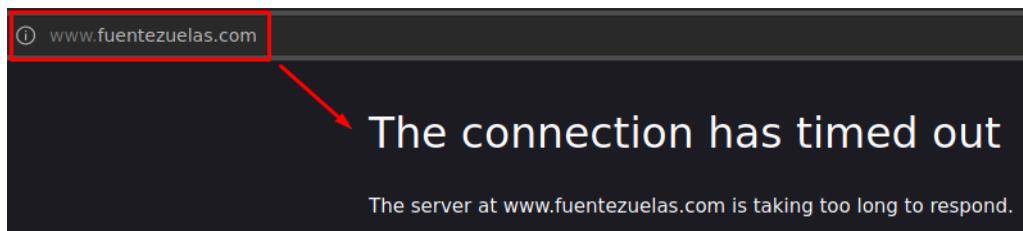
The screenshot shows the IPfire Firewall Rules table. It lists five rules:

#	Protocolo:	Source	Log	Destination	Action
1	TCP	192.168.1.0/24	<input type="checkbox"/>	Firewall : 22 ->192.168.2.13: 22	<input checked="" type="checkbox"/>
2	TCP	Green	<input type="checkbox"/>	Any: 53	<input checked="" type="checkbox"/>
3	UDP	Green	<input type="checkbox"/>	Any: 53	<input checked="" type="checkbox"/>
4	TCP	Green	<input type="checkbox"/>	Any: 443	<input checked="" type="checkbox"/>
5	Todos	Green	<input type="checkbox"/>	Any	<input checked="" type="checkbox"/>

The bottom status bar shows 'Green' and 'Internet (Allowed)'. The first rule (TCP, 192.168.1.0/24 to Firewall: 22) is selected and highlighted with a red box. Rules 2, 3, 4, and 5 are also highlighted with a red box.



Desde este momento, nuestro firewall permite a los usuarios navegar a páginas HTTPS, pero en ningún caso permite el acceso a páginas HTTP o a servicios como videojuegos desde la interfaz “green”, no tendrán ni la posibilidad de hacer un ping.



Y ahora, ¿qué ocurre si por ejemplo solo queremos que nuestros clientes puedan conectarse (o no) a sitios webs específicos? Para el ejemplo, usaremos Moodle Centros, y esta será la única página a la que nuestros clientes podrán acceder.

Antes de nada, debemos conocer la IP (podemos descubrirlo haciendo un simple ping), y modificaremos la regla para permitir el tráfico HTTPS para que, únicamente lo permita si la dirección IP de destino es la de Moodle Centros.

The screenshot shows the configuration of a new firewall rule:

- Source:** Standard networks: Green (192.168.2.0/24)
- Destination:** Destination address: 217.12.30.33
- Protocol:** TCP, Destination port: 443
- Action:** ACCEPT

En general las posibilidades son infinitas, y las reglas a configurar en el firewall dependerá completamente del caso concreto, de si tenemos una DMZ además de la LAN, de si es para uso doméstico, empresarial o educativo etc. Pero el proceso es sencillo y rápido de testear.



3 pfSense

3.1 ¿Qué es pfSense?

pfSense es una distribución gratuita y de código abierto que funciona como firewall y router configurable con administrador de amenazas, balanceador de carga, multi WAN etc. También se pueden instalar módulos al igual que en IPFire, así como implementar el sistema de detección y protección de intrusos.

Es una solución algo más conocida y usada que IPFire, además podemos encontrar algo más de documentación, aunque para algunos casos donde necesitamos solo algunos servicios, puede ser demasiado complejo debido a sus grandes opciones.

3.2 Instalación y configuración inicial

Antes de comenzar con su instalación, descargaremos la ISO de pfSense desde su [sitio web oficial](#); teniendo en cuenta, no obstante, que ya sabemos cómo crear una máquina virtual gracias al [punto anterior](#) de este documento.

En esta ocasión estaremos descargando la última versión (2.5.2) para arquitectura 64bits y en formato ISO desde el servidor de Europa.

Latest Stable Version (Community Edition)

This is the most recent stable release, and the recommended version for all [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall a](#)

[RELEASE NOTES](#) [SOURCE CODE](#)

Select Image To Download

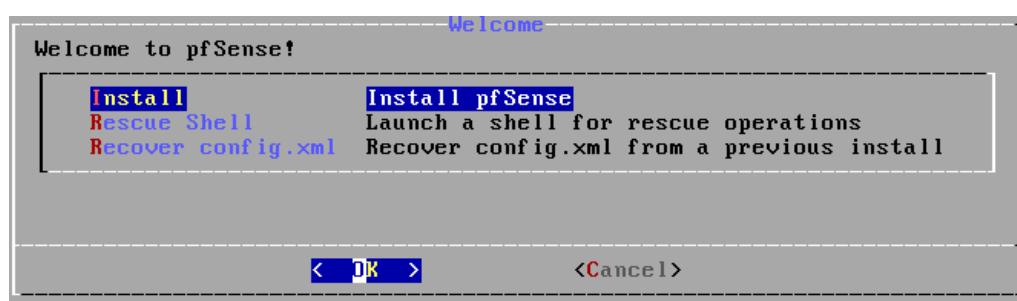
Version: 2.5.2
Architecture: AMD64 (64-bit) [?](#)
Installer: DVD Image (ISO) Installer [?](#)
Mirror: Frankfurt, Germany [?](#)

[DOWNLOAD](#)

Supported by

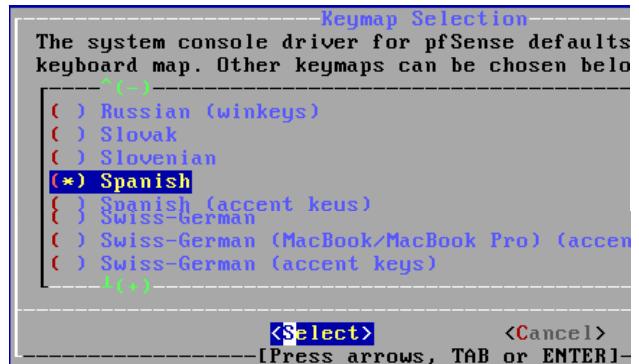
netgate

Después de añadir el ISO a la máquina virtual e iniciarla, en la ventana de bienvenida seleccionamos la opción para instalar pfSense en el sistema.





Al igual que en IPFire, primero debemos seleccionar el layout de nuestro teclado, en esta ocasión será más importante, ya que sí tendremos que escribir más en la consola de pfSense después de su instalación.

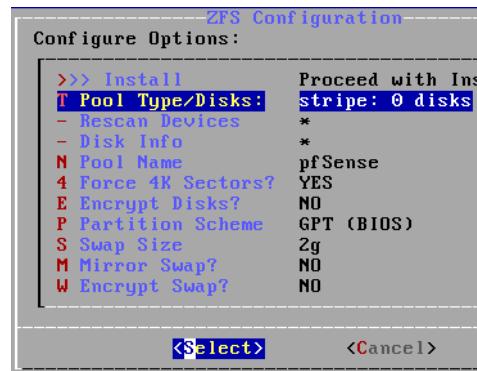


En el siguiente paso decidimos cómo queremos particionar el disco del sistema. Tenemos la posibilidad de realizar el particionado manualmente o incluso por shell, pero las opciones recomendables para instalaciones estándar son las automáticas. Entre ellas encontramos las que usan el sistema de archivos UFS con BIOS o UEFI dependiendo del sistema, o el que usa ZFS.

Para pfSense es recomendable usar ZFS, ya que ofrece un integridad mayor para nuestros archivos, un mejor rendimiento potencial y evita que los archivos se queden corruptos en caso de pérdida de energía y apagado repentino; el único punto negativo es que consume algo más de memoria RAM.

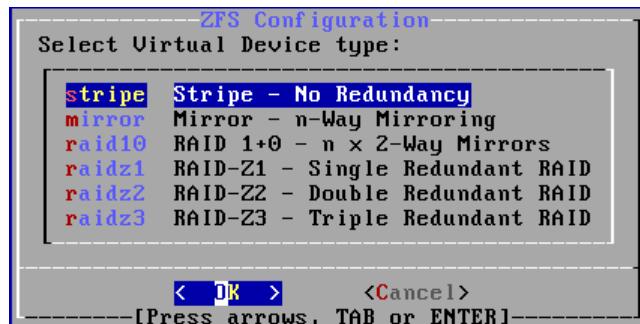


En el siguiente paso, pfSense nos permite elegir ciertas opciones. Entre ellas encontramos la posibilidad de encriptar el disco duro, de modificar el tamaño de swap, y de crear un pool de discos duros para asegurar, así, que no perdamos la funcionalidad ni las configuraciones una vez implementado el sistema.

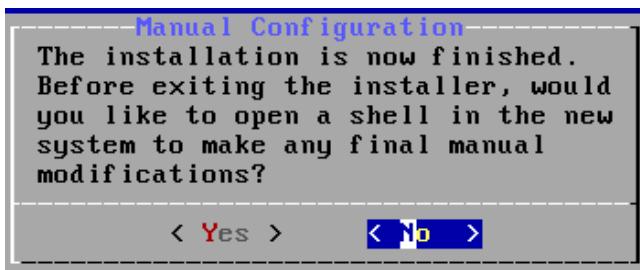




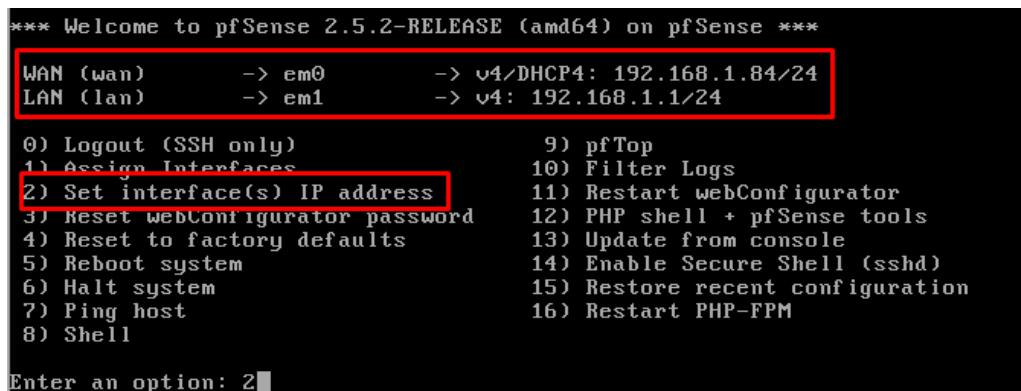
Más concretamente podemos elegir la no redundancia, un RAID 1 (en espejo), un RAID 1+0 (Raid 0 y Raid 1), un Z1 (Redundancia individual), un Z2 (redundancia doble) o un Z3 (redundancia triple).



Después de elegir la configuración ZFS de redundancia, se iniciará la instalación. Después de unos segundos, finalizará y reiniciaremos la máquina.



Una vez iniciada por primera vez, encontraremos el panel de administración en terminal. Principalmente aquí configuraremos los parámetros que en IPFire se configuraron desde el asistente de primera configuración, por ello, seleccionamos la opción 2 para cambiar las direcciones IP.



Comenzaremos cambiando la configuración de la interfaz externa (La que en IPFire llamamos "red") para que no obtenga la dirección IP por DHCP.





En mi caso le doy la dirección IP fija 192.168.1.177, siendo lo único relevante que se encuentre en la red 192.168.1.0/24 para poder establecer su puerta de enlace como la 192.168.1.1 (mi router con salida a Internet).

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.177

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 WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```

A continuación, configuraremos con el mismo método la interfaz interna (que en IPFire conocíamos como “green”). Siguiendo un concepto similar al que usamos anteriormente, también la ubicaremos en la subred 192.168.2.0/24.

```
Available interfaces:
1 - WAN (em0 - static, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1

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 31):
> 24

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

Acto seguido se nos preguntará si deseamos habilitar el servidor DHCP en esta interfaz interna, si nos interesa, indicamos que sí y establecemos el rango de direcciones que podrá dar el servidor DHCP de pfSense; en este caso estoy asignando desde la 192.168.2.10 hasta la 192.168.2.99, aunque podría ser realmente toda la subred.

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.2.10
Enter the end address of the IPv4 client address range: 192.168.2.99
```



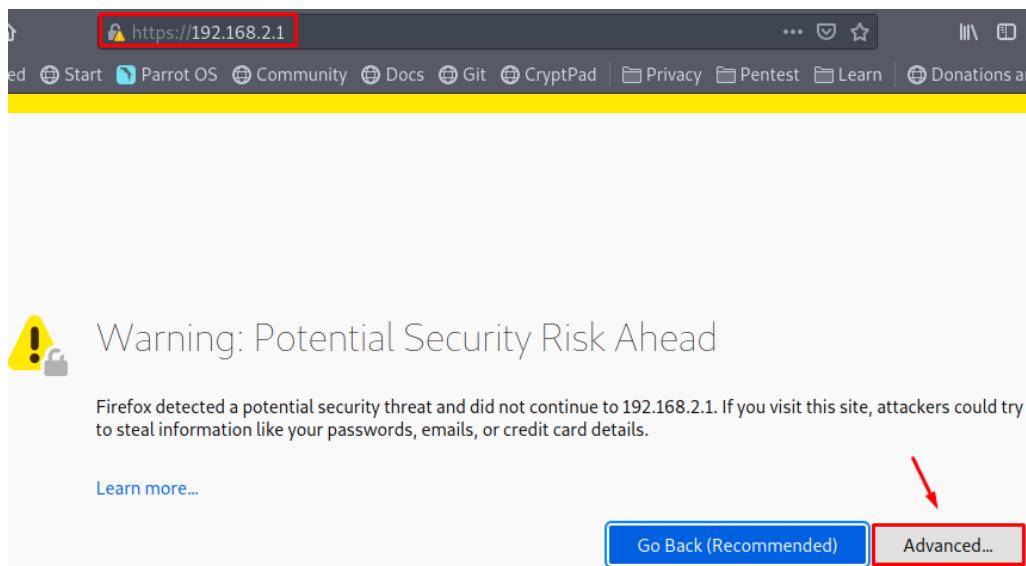
Con estos simples ajustes ya tenemos nuestras dos interfaces perfectamente configuradas.

```
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4: 192.168.1.177/24
LAN (lan)      -> em1          -> v4: 192.168.2.1/24

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
```

Al igual que en IPFire, a partir de ahora seguiremos la configuración desde la interfaz web. En esta ocasión el puerto es el 443, por lo que no necesitamos indicarlo específicamente, eso sí, sí que tendremos que confirmar al navegador que confiamos en el certificado auto firmado.



La primera vez iniciaremos sesión con las credenciales por defecto: usuario "admin" y contraseña "pfsense". Lo primero que haremos, obviamente, será cambiar esta contraseña.

The screenshot shows the pfSense login screen. The title bar says 'pfSense'. The main area has a dark blue background with white text. It says 'SIGN IN' at the top right. There are two input fields: one for 'admin' with the value 'admin' and another for a password with the value 'pfsense' (represented by dots). At the bottom is a green rectangular button labeled 'SIGN IN'.



Con este objetivo, accedemos directamente al apartado “User Manager” desde la pestaña de “System”, y en ella editamos el usuario administrador, cambiando su contraseña y estableciendo una segura.

The screenshot shows the 'User Properties' section of the User Manager. It includes fields for 'Defined by' (SYSTEM), 'Disabled' (unchecked), 'Username' (admin), 'Password' (redacted), 'Full name' (System Administrator), and 'User's full name, for administrative information only'. A red box highlights the 'Password' field.

Finalmente, para terminar la configuración inicial debemos acceder al apartado “General setup” de “System”, y será aquí donde establecemos el nombre del host (hostname), el del dominio y los servidores DNS que usará pfSense.

The screenshot shows the 'General Setup' section under 'System'. It includes fields for 'Hostname' (navarretefirewall) and 'Domain' (navarrete.arpa). Below it is the 'DNS Server Settings' section with a 'DNS Servers' field containing '1.1.1.1'. Red boxes highlight the 'Hostname', 'Domain', and 'DNS Servers' fields.

3.3 OpenVPN en pfSense

Al igual que en IPFire, comenzaremos implementando el servidor OpenVPN, aunque, antes de iniciar la configuración, instalaremos el paquete de exportación de paquetes para OpenVPN a través del Package Manager de pfSense (se usará al final).

The screenshot shows the 'Available Packages' section of the Package Manager. A search term 'openvpn' is entered in the search bar. A red arrow points to the '+ Install' button for the 'openvpn-client-export' package, which is highlighted with a green box.



Con ese paquete ya instalado podemos iniciar la configuración del servidor OpenVPN. Aunque se puede realizar el proceso paso a paso por separado, en pfSense contamos con asistentes que nos facilitan la tarea. Desde la pestaña “Wizard”, por tanto, accedemos al asistente del setup de OpenVPN.

The screenshot shows the first step of the OpenVPN Remote Access Server Setup Wizard. The title bar says "Wizard / OpenVPN Remote Access Server Setup /". The main content area is titled "OpenVPN Remote Access Server Setup" with the sub-instruction "This wizard will provide guidance through an OpenVPN Remote Access Server Setup.". Below it, a note says "The wizard may be stopped at any time by clicking the logo image at the top of the screen." The next section, "Select an Authentication Backend Type", has a dropdown menu labeled "Type of Server" with "Local User Access" selected. A note below the dropdown says "NOTE: If unsure, leave this set to "Local User Access."" A "Next" button is at the bottom of this section, also highlighted with a red box.

El primer paso será generar la autoridad certificadora, igual que hicimos en IPFire. En mi caso ya tenía una, pero se puede crear una fácilmente pulsando sobre el botón “Add new CA”.

The screenshot shows the fifth step of the OpenVPN Remote Access Server Setup Wizard, titled "Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection". It indicates "Step 5 of 11". The main title is "Certificate Authority Selection". The sub-instruction "OpenVPN Remote Access Server Setup Wizard" is present. The next section, "Choose a Certificate Authority (CA)", has a dropdown menu labeled "Certificate Authority" with "navarreteCA" selected. Below it are two buttons: "» Add new CA" and "» Next", both highlighted with a red box. The final part of the screenshot is a detailed configuration form titled "Create a New Certificate Authority (CA) Certificate". It includes fields for "Descriptive name" (navarreteCAv2), "Key length" (2048 bit), "Lifetime" (3650 days), "Country Code" (ES), "State or Province" (Jaen), "City" (Jen), and "Organization" (Fuentezuelas). Each field has a descriptive note below it. At the bottom of this form is another "» Add new CA" button.

Tal y como acostumbramos a hacer, completamos los típicos campos de información para generarnos nuestra propia autoridad certificadora (CA): Nombre de la misma, longitud de clave, código de país, nombre de provincia y de ciudad, nombre de organización...



El siguiente paso es crear el certificado del servidor, al igual que en el paso anterior, yo ya tenía uno creado, pero podemos crear otro más seleccionando “Add new certificate”.

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection
Step 7 of 11

Server Certificate Selection
OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate
Certificate: VPNCert

>> Add new Certificate >> Next

Volvemos a repetir los mismos datos, podemos establecer un tiempo de caducidad en días, por defecto se establecerán 398 días.

Create a New Server Certificate

Descriptive name: OpenVPN Server Cert
A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."

Key length: 2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](#)

Lifetime: 398
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Country Code: ES
Two-letter ISO country code (e.g. US, AU, CA)

State or Province: Jaen
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City: Jen
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization: Fuentezuelas
Organization name, often the Company or Group name.

>> Create new Certificate

Con el CA y el certificado del servidor creado, ahora sí, podemos configurar las opciones del propio servidor OpenVPN. Entre ellas encontramos la interfaz por la que escuchará (La WAN), el protocolo (Podemos UDP o UDP+TCP), el puerto y una descripción.

Server Setup
OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface: WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)

Protocol: UDP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Local Port: 1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description: Servidor VPN para SAD
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.



Ulteriormente confirmamos que se usará autenticación TLS y que los datos se encriptarán mediante AES y ChaCha20. Para una mayor compatibilidad podemos dejar el AES 128 bits, o, para mayor seguridad, podemos dejar únicamente AES 256 bits junto al ChaCha20 de 256 bits.

Cryptographic Settings

TLS Authentication	<input checked="" type="checkbox"/>	Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/>	Automatically generate a shared TLS authentication key.
TLS Shared Key	<input type="text"/>	
DH Parameters Length	<input type="button" value="2048 bit"/>	
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.		
Data Encryption Negotiation	<input checked="" type="checkbox"/>	Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	<input type="button" value="AES-256-GCM"/> <input type="button" value="AES-128-GCM"/> <input type="button" value="CHACHA20-POLY1305"/>	
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.		

Más adelante establecemos los ajustes del túnel VPN. En IPFire no cambiamos la dirección por defecto de la subred de la propia VPN, y, lo único relevante es poner una subred que no esté en uso en nuestra arquitectura, en esta ocasión he usado la 192.168.77.0/24.

Si deseamos que alguna red local sea accesible desde el túnel VPN, podemos indicarla en el apartado “Local Network”, y, al igual que en IPFire no activaremos el Redirect Gateway ni tampoco la compresión por razones de seguridad.

Tunnel Settings

Tunnel Network	<input type="text" value="192.168.77.0/24"/>	This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway	<input type="checkbox"/>	Force all client generated traffic through the tunnel.
Local Network	<input type="text" value="192.168.2.0/24"/>	This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	<input type="text" value="1"/>	Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>	Allow compression to be used with this VPN instance, which is potentially insecure.
Compression	<input type="button" value="Disable Compression [Omit Preference]"/>	Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if



Para finalizar con el asistente, es recomendable marcar las opciones correspondientes para que directamente cree la regla necesaria en el firewall de pfSense. Tras este paso, nuestro servidor OpenVPN será funcional por sí mismo, aunque no tenemos ningún usuario.

The screenshot shows the 'Firewall Rule Configuration' step of the OpenVPN setup wizard. It includes sections for 'Traffic from clients to server' and 'Traffic from clients through VPN'. Both sections have checkboxes for 'Firewall Rule' and 'OpenVPN rule', both of which are checked. A red box highlights these two sections. At the bottom right of the configuration area is a blue 'Next' button.

Por tanto, el siguiente paso es crear usuarios para que se puedan conectar a la VPN que acabamos de implementar. Esto lo podemos realizar en pfSense desde el “User Manager” y haciendo click en “Add”.

The screenshot shows the 'User Manager / Users' page in pfSense. It lists two users: 'admin' and 'jorge'. On the right, there are 'Add' and 'Delete' buttons. A red arrow points to the 'Add' button. Below the list is the 'User Properties' dialog for a new user. The 'Username' field is set to 'navarrete' and has a red box around it. The 'Password' field contains several dots. The 'Group membership' dropdown is set to 'admins'. At the bottom of the dialog, there is a checkbox for 'Click to create a user certificate' with a red box around it.

El usuario podrá tener cualquier nombre y cualquier contraseña, lo único relevante es crear un certificado de usuario seleccionando el “tick” de la parte inferior de la pantalla, el cual indica “Click to create a user certificate”.



Al elegir esta opción, aparecerán en la parte inferior de la pantalla los correspondientes cuadros de texto para indicar el nombre del certificado y para marcar en el desplegable la autoridad certificadora propia.

Create Certificate for User

Descriptive name: NavarreteVPNcert

Certificate authority: navarreteCAv2

Key type: RSA

Key Length: 2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime: 3650

Después de crear el usuario, haremos uso del paquete instalado al inicio de este apartado para exportar los archivos necesarios para establecer la conexión cliente. En él debemos seleccionar “Client export”, e indicar para qué servidor queremos obtener el paquete de cliente. En la parte inferior tenemos opciones incluso para generar un instalador desatendido para Windows.

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote Access Server: Servidor VPN para SAD UDP4:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS: Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

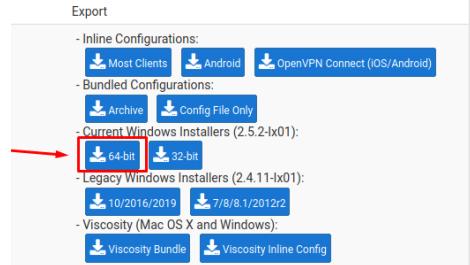
Legacy Client: Do not include OpenVPN 2.5 settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer: Create Windows installer for unattended deploy.
Create a silent Windows Installer for unattended deploy. Since this installer is not signed, you may need special software to deploy it correctly.

Export

- Inline Configurations:
[Most Clients](#) [Android](#) [OpenVPN Connect \(iOS/Android\)](#)
- Bundled Configurations:
[Archive](#) [Config File Only](#)
- Current Windows Installers (2.5.2-lx01):
[64-bit](#) [32-bit](#)
- Legacy Windows Installers (2.4.11-lx01):
[10/2016/2019](#) [7/8/8.1/2012r2](#)
- Viscosity (Mac OS X and Windows):
[Viscosity Bundle](#) [Viscosity Inline Config](#)

Al completar estas opciones, se nos permite exportar en archivos para configurar el cliente mediante configuración inline o bundled, mediante instalador de Windows o mediante Viscosity para Mac.





De vuelta en un cliente Windows, directamente podemos ejecutar el .EXE generado en pfSense, este no solo instalará OpenVPN GUI, sino que también nos dejará en los archivos de configuración el .OVPN, la clave y el certificado del usuario. Es importante recordar que en caso de querer acceder remotamente hay que cambiar la IP del parámetro “remote” en el archivo OVPN.

The screenshot shows a Windows file explorer window with the following contents:

- Nombre (Name):
 - navarretefirewall-UDP4-1194-navarrete.p12
 - navarretefirewall-UDP4-1194-navarrete-config.ovpn
 - navarretefirewall-UDP4-1194-navarrete-tls.key
 - README.txt

To the right of the file list, there is a preview pane showing the contents of the navarretefirewall-UDP4-1194-navarrete-config.ovpn file:

```
navarretefirewall-UDP4-1194-navarrete-config.ovpn: Bloc de notas
Archivo Edición Formato Ver Ayuda
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 192.168.1.177 1194 udp4
verify-x509-name "OpenVPN Server Cert" name
auth-user-pass
pkcs12 navarretefirewall-UDP4-1194-navarrete.p12
tls-auth navarretefirewall-UDP4-1194-navarrete-tls.key
remote-cert-tls server
explicit-exit-notify
```

Al iniciar OpenVPN GUI, nos pedirá el usuario y la contraseña, el cual podemos recordar, y acto seguido comenzará el proceso de conexión. Al terminar, el icono aparecerá en verde.

The screenshot shows two windows of the OpenVPN GUI:

- Conexión OpenVPN (navarretefirewall-UDP4-1194-navarrete-config)**: Shows the connection status as "Conectando". It has fields for "Usuario:" (User) set to "navarrete" and "Password:" (Password) set to "*****". There is also a "Save password" checkbox. Buttons for "OK" and "Cancelar" (Cancel) are visible.
- Conexión OpenVPN (navarretefirewall-UDP4-1194-navarrete-config)**: Shows the connection status as "Conectado". The log pane displays several lines of connection logs, including:
 - Sun Jan 23 16:56:31 2022 OpenVPN 2.5.2 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [AEAD]
 - Sun Jan 23 16:56:31 2022 Windows version: 10.0 (Windows 10 or greater) 64bit
 - Sun Jan 23 16:56:31 2022 library version: OpenSSL 1.1.1k 25 Mar 2021 LZO 2.10
 - Sun Jan 23 16:56:40 2022 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.177:1194
 - Sun Jan 23 16:56:40 2022 UDPv4 link local (bound): [AF_INET]unassigned:1194
 - Sun Jan 23 16:56:41 2022 [OpenVPN Server Cert] Peer Connection Initiated with [AF_INET]192.168.1.177:1194
 - Sun Jan 23 16:56:41 2022 [OpenVPN Server Cert] Peer Connection Initiated with [AF_INET]192.168.1.177:1194
 - Sun Jan 23 16:56:41 2022 OpenVPN: TUN subnet mode network/local netmask = 192.168.77.0/192.1
 - Sun Jan 23 16:56:41 2022 Notified TAP-Windows driver to set a DHCP IP/netmask of 192.168.77.2/255.255.2
 - Sun Jan 23 16:56:41 2022 Successful ARP Flush on interface [6] {851F0231:AB85:406B:BEC0:8C3AA395245}
 - Sun Jan 23 16:56:41 2022 IPv4 MTU set to 1500 on interface 6 using service

Al igual que en IPFire, podremos confirmar la conexión del cliente desde el propio pfSense.

The screenshot shows the pfSense OpenVPN status page with the following details:

Servidor VPN para SAD UDP4:1194 Client Connections: 1

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher
navarrete navarrete	192.168.2.12:1194	192.168.77.2	2022-01-23 15:56:43	4 KiB	12 KiB	AES-256-GCM

Status: Actions:



3.4 IDS/IPS en pfSense

Para el sistema de detección de intrusos usaremos Suricata en lugar de Snort, ya que nos proporciona ciertas ventajas. Una de ellas es que es más rápido ya que puede procesar paquetes de forma simultánea, también soporta la extracción de archivos y es más eficaz con tráfico encriptado; por ello consume algo más de recursos hardware. Para instalarlo acudiremos de nuevo al administrador de paquetes (Package Manager).

The screenshot shows the pfSense Package Manager interface. The title bar says "System / Package Manager / Available Packages". Below it, there are tabs for "Installed Packages" and "Available Packages", with "Available Packages" being active. A search bar has "suricata" typed into it. Below the search bar is a placeholder text: "Enter a search string or *nix regular expression to search package names and descriptions." The main area is titled "Packages" and contains a table with columns "Name", "Version", and "Description". One row shows "suricata" version 6.0.4 with the description "High Performance Network IDS, IPS and Security Monitoring engine by OISF.". To the right of this row is a green button with a white plus sign labeled "+ Install". Red arrows point from the text "A continuación" to the search bar and from the text "Instalar" to the "+ Install" button.

Una vez instalado, accedemos a su configuración desde el menú desplegable de servicios, y lo primero será configurar sus ajustes globales. Aquí activaremos las reglas que queremos usar, y, a diferencia de IPFire, podemos usar varias a la vez; en caso de que no se actualicen las de ETOpen, podemos poner el [enlace](#) manualmente.

The screenshot shows the pfSense Services configuration for Suricata. The title bar says "Services / Suricata / Global Settings". Below it, there are tabs for "Interfaces", "Global Settings", "Updates", "Alerts", "Blocks", "Files", "Pass Lists", "Suppress", "Logs View", "Logs Mgmt", and "SID Mgmt", with "Global Settings" being active. Below the tabs, there are "Sync" and "IP Lists" buttons. The main area is titled "Please Choose The Type Of Rules You Wish To Download". It contains several sections: "Install ETOpen Emerging Threats rules" (checkbox checked), "ETOOpen Custom Rule Download URL" (text input field containing ".://rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz"), "Install ETPro Emerging Threats rules" (checkbox unchecked), "Install Snort rules" (checkbox unchecked), and "Install Snort GPLv2 Community rules" (checkbox checked). Red boxes highlight the "Global Settings" tab, the "Install ETOpen Emerging Threats rules" checkbox, and the "Install Snort GPLv2 Community rules" checkbox.



Desde Suricata podemos directamente establecer el tiempo que estarán bloqueadas las direcciones IPs que creen una alerta, en este caso pondré una hora.

General Settings

Remove Blocked Hosts Interval: 1 HOUR

Please select the amount of time you would like hosts to be blocked. Note: this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode.

Hint: in most cases, 1 hour is a good choice.

Log to System Log: Copy Suricata messages to the firewall system log.

Keep Suricata Settings After Deinstall: Settings will not be removed during package deinstallation.

Tras estos dos ajustes ya personalizados, actualizamos las reglas desde la pestaña "Updates".

Services / Suricata / Updates

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

Update Force

En este mismo apartado podemos indicar el intervalo de actualización de las reglas, e incluso marcar que se cambien “en caliente” al actualizar mientras Suricata está activo y escaneando.

Rules Update Settings

Update Interval: 1 DAY

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Hint: In most cases, every 12 hours is a good choice.

Update Start Time: 00:26

Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Live Rule Swap on Update: Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked

When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.

GeoLite2 DB Update: Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked

When enabled, Suricata will automatically download updates for the free GeoLite2 country IP database.



Después de los ajustes generales, podemos añadir la interfaz donde Suricata estará activo seleccionando el botón “Add”.

The screenshot shows the 'Services / Suricata' interface. The 'Interfaces' tab is highlighted with a red box. Below it, there are tabs for 'Global Settings', 'Updates', 'Alerts', 'Blocks', 'Files', 'Pass Lists', 'Suppress', 'Logs View', 'Logs Mgmt', and 'SID Mgmt'. Under 'Sync' and 'IP Lists', there is a table titled 'Interface Settings Overview' with columns: Interface, Suricata Status, Pattern Match, Blocking Mode, Description, and Actions. In the 'Actions' column for the first row, there is a green button with a plus sign and the word 'Add'.

Dentro de los ajustes de esta interfaz podemos cambiar los ajustes de log, en esta ocasión, además de crear logs para HTTP, también lo hará para TLS.

The screenshot shows the 'Logging Settings' interface. It contains several configuration options with checkboxes:

- Send Alerts to System Log: Suricata will send Alerts from this interface to the firewall's system log. NOTE: The FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.
- Enable Stats Collection: Suricata will periodically gather performance statistics for this interface. Default is Not Checked.
- Enable HTTP Log: Suricata will log decoded HTTP traffic for the interface. Default is Checked.
- Append HTTP Log: Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.
- Log Extended HTTP Info: Suricata will log extended HTTP information. Default is Checked.
- Enable TLS Log: Suricata will log TLS handshake traffic for the interface. Default is Not Checked.
- Enable TLS Store: Suricata will log and store TLS certificates for the interface. Default is Not Checked.
- Log Extended TLS Info: Suricata will log extended TLS info such as fingerprint. Default is Checked.
- Enable File-Store: Suricata will extract and store files from application layer streams. Default is Not Checked. WARNING: Enabling file-store will consume a significant amount of disk space on a busy network!
- Enable Packet Log: Suricata will log decoded packets for the interface in pcap-format. Default is Not Checked. This can consume a significant amount of disk space when enabled.

Todos estos logs podemos exportarlos a un JSON, y será aquí donde activaremos la opción de bloquear a los atacantes cuando generen una alerta (en la imagen está desactivado, pero la acabé activando).

The screenshot shows three stacked configuration sections:

- EVE Output Settings:** Contains the 'EVE JSON Log' option, which is currently unchecked. It says: "Suricata will output selected info in JSON format to a single file or to syslog. Default is Not Checked."
- Alert and Block Settings:** Contains the 'Block Offenders' option, which is currently unchecked. It says: "Checking this option will automatically block hosts that generate a Suricata alert."
- Performance and Detection Engine Settings:** Contains two dropdowns:
 - Run Mode:** Set to 'AutoFP'. A note below says: "Choose a Suricata run mode setting. Default is 'AutoFP' and is the recommended setting for most cases. 'Workers' uses multiple worker threads, each of which single-handedly processes the packets it acquires (i.e., each thread runs all thread modules). 'Single' uses only a single thread for all operations on a packet and is intended for use only in testing or development instances."
 - AutoFP Scheduler Type:** Set to 'Hash'. A note below says: "Choose the kind of flow load balancer used by the flow pinned autofp mode. 'Hash' assigns the flow to a thread using the 5-7 tuple hash. 'IP Pair' assigns the flow to a thread using addresses only. This setting is applicable only when the Run Mode is set to 'autofp'."



Desde la pestaña “LAN Categories” seleccionamos las reglas elegidas. Lo ideal en estos casos suele ser activarlas todas y monitorizar la red durante unos días para eliminar las que den falsos positivos.

Automatic flowbit resolution

Resolve Flowbits Auto-enable rules required for checked flowbits
Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules

Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Select the rulesets (Categories) Suricata will load at startup

- Category is auto-enabled by SID Mgmt conf files
 - Category is auto-disabled by SID Mgmt conf files

Enabled	Ruleset:
<input type="checkbox"/>	Snort GPLv2 Community Rules (Talos-certified)
Enabled	Ruleset: ET Open Rules
<input type="checkbox"/>	emerging-3coresec.rules
<input type="checkbox"/>	emerging-activex.rules
<input checked="" type="checkbox"/>	emerging-adware_pup.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules

Seguidamente, activaremos e iniciaremos Suricata en esta interfaz a través del botón “play”.

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View

Logs Mgmt SID Mgmt Sync IP Lists

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (em1)	AUTO	DISABLED	LAN		

A partir de este momento podemos revisar el log desde el propio Suricata, y, en caso de ver alertas que no consideramos necesarias, podemos deshabilitarlas desde aquí.

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
01/24/2022 17:29:13	⚠️	3	TCP	Not Suspicious Traffic	192.168.2.14	53734	91.189.91.39	80	1:2013504	ET POLICY GNU/Linux APT User Agent

Force-disable this rule and remove it from current rules set via management



Igual que realicé con IPFire, si se hace un nmap sobre la red que monitoriza pfSense, se nos alertará del escaneo.

Alert Log View Filter											
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description	
01/24/2022 17:36:27	⚠️	1	TCP	Web Application Attack	192.168.2.13	44416	192.168.2.14	80	1:2024364 ⊕ ✘	ET SCAN Possible Nmap User-Agent Observed	
01/24/2022 17:36:27	⚠️	1	TCP	Web Application Attack	192.168.2.13	44414	192.168.2.14	80	1:2024364 ⊕ ✘	ET SCAN Possible Nmap User-Agent Observed	
01/24/2022 17:36:27	⚠️	1	TCP	Web Application Attack	192.168.2.13	44410	192.168.2.14	80	1:2024364 ⊕ ✘	ET SCAN Possible Nmap User-Agent Observed	

3.5 Demostración del IDS/IPS (Y port forwarding)

Para comenzar la demostración real del sistema, ya sabemos que debemos “abrir” los puertos, por tanto, accedemos al menú desplegable del firewall y seleccionamos la opción de “NAT”. En el apartado de “Port Forward” seleccionamos el botón “Add”.

The screenshot shows the pfSense Firewall NAT Port Forwarding configuration. The top navigation bar has 'Firewall' selected. The main menu shows 'Firewall / NAT / Port Forward'. Below this, there are tabs for 'Port Forward', '1:1', 'Outbound', and 'NPt'. The 'Port Forward' tab is active. A red arrow points to the 'Add' button in the toolbar at the bottom right of the list table. Another red box highlights the 'WAN address' field in the 'Edit Redirect Entry' form, which is currently set to 'WAN'. The 'Destination port range' dropdown is also highlighted with a red box, showing 'SSH' selected. The 'Redirect target IP' dropdown is highlighted with a red box, showing 'Single host' selected with the value '192.168.2.13'. The 'Redirect target port' dropdown is highlighted with a red box, showing 'SSH' selected.



En la creación de la regla seguimos los mismos conceptos que en el caso de IPFire. Lo primero será establecer la interfaz a la que llegarán los paquetes que queremos redireccionar (WAN), el protocolo (TCP en IPv4) y el puerto (22 de SSH). Después, añadimos la dirección a la que queremos redireccionar, es decir la de nuestro host o servidor (192.168.2.13/24) y su respectivo puerto (22, SSH).

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
Address Family	IPv4
Protocol	TCP
Source	Display Advanced
Destination	<input type="checkbox"/> Invert match. <input type="text" value="WAN address"/> Type <input type="text" value="192.168.2.13"/> Address/mask
Destination port range	SSH From port Custom To port Custom Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP	Single host <input type="text" value="192.168.2.13"/> Type Address Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)
Redirect target port	SSH Port Custom Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).

Acto seguido hacemos lo mismo para redireccionar los paquetes TCP que lleguen al puerto 80 de la tarjeta WAN, al puerto 80 del mismo host (192.168.2.13), en el cual he vuelto a abrir un servidor HTTP simple con Python3. Tras crearlo, pfSense recargará las reglas del firewall y estas se mostrarán en el panel.

Firewall / NAT / Port Forward

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

Port Forward 1:1 Outbound NPt

Rules
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> WAN TCP * * Dest. Address: WAN address Dest. Ports: 80 (HTTP) NAT IP: 192.168.2.13 NAT Ports: 80 (HTTP) Description: Pruebas HTTP Actions: Edit Delete
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> WAN TCP * * Dest. Address: WAN address Dest. Ports: 22 (SSH) NAT IP: 192.168.2.13 NAT Ports: 22 (SSH) Description: Solo pruebas forzadas Actions: Edit Delete

[Add](#) [Up](#) [Down](#) [Delete](#) [Save](#) [Separator](#)



De esta forma, ya podremos acceder tanto al SSH como al servidor web desde fuera de la red interna. Como ya están abiertos los puertos de mi puerta de enlace, también se podrá desde Internet.

En esta ocasión, un excompañero de la facultad me hizo el favor de realizar un escaneo Nmap agresivo sobre mi dirección IP, y un ataque de fuerza bruta sobre mi usuario SSH.

```
xubuntu@xubuntu-virtual-machine:~$ nmap -A 192.168.1.9.2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-27 09:04 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.25 seconds
xubuntu@xubuntu-virtual-machine:~$ hydra -l n4v4 -P '/home/passwords.txt' 192.168.1.9.2 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-27 09:07:
22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 581 login tries (l:1/p:581),
~37 tries per task
[DATA] attacking ssh://192.168.1.9.2:22/
```

De forma instantánea, pfSense detectó el ataque Nmap y bloqueó la dirección IP pública de mi compañero.

The screenshot shows the pfSense Alert Log View Settings and Filter interface. The settings section includes options for Instance to View (LAN LAN), Save or Remove Logs, and Save Settings. The filter section shows the last 250 alert entries. A specific entry from January 27, 2022, at 17:04:12 is highlighted with a red box. This entry is for a TCP connection from 192.168.2.13 to 77.226.225.120 port 55584, identified as a Web Application Attack. The log entry details include the date, time, action (TCP), priority (3), protocol (TCP), class (Misc activity), source (192.168.2.13), destination (77.226.225.120), sport (80), dport (55584), GID:SID (1:2034636), and a detailed description of the ET INFO Python SimpleHTTP ServerBanner.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
01/27/2022 17:04:12	⚠️	3	TCP	Misc activity	192.168.2.13	80	77.226.225.120	55586	1:2034636	ET INFO Python SimpleHTTP ServerBanner
01/27/2022 17:04:12	⚠️	3	TCP	Misc activity	192.168.2.13	80	77.226.225.120	55584	1:2034636	ET INFO Python SimpleHTTP ServerBanner
01/27/2022 17:04:12	⚠️	1	TCP	Web Application Attack	77.226.225.120	55584	192.168.2.13	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
01/27/2022 17:04:12	⚠️	3	TCP	Misc activity	192.168.2.13	80	77.226.225.120	55578	1:2034636	ET INFO Python SimpleHTTP ServerBanner
01/27/2022 17:04:12	⚠️	1	TCP	Web Application Attack	77.226.225.120	55578	192.168.2.13	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)



Para que pudiese continuar con el ataque sobre mi SSH, le quité el bloqueo a su dirección IP pública desde el apartado “Blocks” de Suricata.

The screenshot shows the 'Blocked Hosts Log View Settings' interface. It includes sections for saving hosts, clearing them, and setting refresh and display options. Below this is a table titled 'Last 500 Hosts Blocked by Suricata' with one entry:

#	Blocked IP	Alert Description
1	77.226.225.120	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) - 01/27/2022-17:04:12

A red box highlights the first row of the table. At the bottom, a note says '1 host IP address is currently being blocked.'

En seguida se volvió a detectar que esto era un ataque de fuerza bruta sobre mi SSH, y se volvió a bloquear la dirección IP de origen.

The screenshot shows the 'Alert Log View Settings' and 'Alert Log View Filter' interfaces. It includes sections for saving logs, clearing them, and setting refresh and display options. Below this is a table titled 'Last 250 Alert Entries. (Most recent entries are listed first)' with two entries:

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
01/27/2022 17:07:23	⚠️	3	TCP	Generic Protocol Command Decode	192.168.2.13	22	77.226.225.120	55464	1:2260002	SURICATA Applayer Detect protocol only one direction
01/27/2022 17:07:23	⚠️	2	TCP	Attempted Information Leak	77.226.225.120	55438	192.168.2.13	22	1:2001219	ET SCAN Potential SSH Scan

A red box highlights the second row of the table.

Además, durante los segundos que tuve los puertos abiertos, la misma dirección IP alemana que detectó IPFire me siguió haciendo escaneos y se bloqueó; y otra dirección IP de Lituania se bloqueó porque las reglas la tienen guardada como una IP que se suele usar para atacar.

The screenshot shows the 'Blocked Hosts Log View Settings' interface. It includes sections for saving hosts, clearing them, and setting refresh and display options. Below this is a table titled 'Last 500 Hosts Blocked by Suricata' with three entries. A tooltip for the first entry (IP 192.168.2.1) provides geographical information:

192.168.2.1
IP Address: 141.98.10.82
Country: Lithuania
State:
City:
Latitude: 56.0
Longitude: 24.0

An 'OK' button and a note saying 'are highlighted on the ALERTS tab.' are also visible.



3.6 Opciones adicionales de protección

3.6.1 Arpwatch

Otro de los paquetes muy usados en pfSense es Arpwatch, tal y como nos da a entender su nombre, monitorizará los paquetes ARP y nos informará cuando una nueva dirección MAC se conecte a nuestra red.

The screenshot shows the pfSense Package Manager interface. The top navigation bar has 'System / Package Manager / Available Packages' selected. Below the navigation is a search bar with 'Search term' set to 'arpwatch'. The main area is titled 'Packages' and lists the 'arpwatch' package. The package details show it's version 0.2.0_6, contains tools for monitoring ethernet activity, and reports changes via email. It has a dependency on 'arpwatch-3.1'. A green 'Install' button is visible on the right side of the package entry, with a red box and arrow highlighting it.

Después de instalarlo con el “Package Manager” que ya conocemos, podemos llegar a sus ajustes desde la pestaña de servicios y activarlo en la interfaz LAN. Si tuviésemos un servidor de correo configurado en la red podríamos también hacer que se nos envíe un email.

The screenshot shows the pfSense Arpwatch Settings page. The top navigation bar has 'Package / Arpwatch / Settings' selected. The main configuration area is titled 'General Options'. Under 'General Options', the 'Enable Arpwatch' checkbox is checked and highlighted with a red box. Below this, the 'Interfaces' section shows 'LAN' selected. Other settings include 'Notifications recipient' (with a note about sending many notifications), 'Disable Cron emails' (which disables cron email notifications from other packages), 'Zero padded ethernet addresses' (which uses zero-padded ethernet addresses in *.dat files), and 'Disable CARP/VRRP' (which disables reporting CARP/VRRP ethernet prefixes).



Pero, como no es el caso, en un uso doméstico nos bastará con monitorizar manualmente la base de datos del servicio, nos servirá como log donde se guardarán todos los dispositivos que se conectaron a la interfaz green, junto a la fecha.

Database					
Interface	IP address	MAC address	Vendor	Hostname	Timestamp
LAN	192.168.2.13	08:00:27:8b:9e:3a	unknown		Fri Jan 28 11:54:08 2022
LAN	192.168.2.1	08:00:27:d8:33:d3	unknown	navarretefirewall	Fri Jan 28 11:54:08 2022
LAN	192.168.2.15	08:00:27:37:cb:b7	unknown		Fri Jan 28 11:54:00 2022

3.6.2 pfBlockerNG

El último paquete extra que se mostrará en este documento es quizás el más completo de todos: pfBlockerNG. Como siempre, lo instalamos desde el “Package manager”, aunque debo destacar que existen dos versiones: La oficial y estable tiene varias utilidades de pago; la versión “developer” estará en fase de pruebas, pero todos los servicios son gratuitos. A continuación veremos todo lo que nos puede ofrecer.

Es importante, también, confirmar que en el DNS Resolver de pfSense tenemos marcadas la interfaz de nuestra red como “LAN” y la red de salida en la “WAN”.

The screenshot shows the pfSense Services / DNS Resolver / General Settings configuration. The General DNS Resolver Options section is displayed. Key settings include:

- Enable:** Checked, with a note: "Enable DNS resolver".
- Listen Port:** Set to 53, with a note: "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:** Unchecked, with a note: "Configure 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."
- SSL/TLS Certificate:** Set to "webConfigurator default (61ed5ff9d360f)", with a note: "The server certificate to use for SSL/TLS service. The CA chain will be determined automatically."
- SSL/TLS Listen Port:** Set to 853, with a note: "The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853."

Network Interfaces: A dropdown menu showing available interfaces: LAN, WAN IPv6 Link-Local, LAN IPv6 Link-Local, 17.17.17.1 (pfB DNSBL - DO NOT EDIT), and Localhost. The LAN option is selected.

Outgoing Network Interfaces: A dropdown menu showing available interfaces: All, WAN, LAN, WAN IPv6 Link-Local, and LAN IPv6 Link-Local. The WAN option is selected.



Con esa pequeña comprobación realizada, y con pfBlockerNG instalado, podemos iniciar su asistente accediendo a él desde la pestaña de "Firewall".

The screenshot shows the pfSense Firewall configuration interface. The top navigation bar has 'Firewall' selected. Below it, a breadcrumb navigation bar shows 'Wizard / pfBlockerNG Setup /'. A red box highlights this breadcrumb, and a red arrow points to it from the left. The main content area is titled 'pfBlockerNG Setup' and displays a welcome message: 'Welcome to pfBlockerNG! This wizard will configure an entry level configuration of pfBlockerNG for IP and DNSBL. You can opt-out of this wizard and manually configure pfBlockerNG as required! pfBlockerNG is developed and maintained by BBcan177'. To the right is the pfBlockerNG logo. At the bottom is a 'Next' button.

En el primer paso, indicamos a pfBlocker que la interfaz de la cual se podrá bloquear tráfico de entrada será desde la WAN; y, que la interfaz en la que se bloqueará el posible tráfico de salida hacia direcciones IPs sospechosa o maliciosas será la LAN.

The screenshot shows the 'pfBlockerNG IP Component Configuration' step 2 of 4. It has a sub-header 'pfBlockerNG IP Component Configuration'. The text says 'On this screen the pfBlockerNG IP Category parameters will be set.' There are two dropdown menus: 'Select Inbound Firewall Interface' (set to 'WAN') and 'Select Outbound Firewall Interface' (set to 'LAN'). Both dropdowns have options 'WAN', 'LAN', and 'OpenVPN'. Below each dropdown is a note: 'Select the Inbound interface(s) you want to apply auto rules to:' and 'Select the Outbound interface(s) you want to apply auto rules to:'. At the bottom are 'Back' and 'Next' buttons.

En el siguiente paso antes de finalizar simplemente tendremos que confirmar la dirección IP para la propia configuración del sistema DNSBL, así como el puerto de su interfaz web, no tiene especial importancia y se puede dejar por defecto sin problema.

DNSBL será el servicio de pfBlockerNG que bloqueará direcciones IP peligrosas según varias listas, aunque antes configuraremos uno más sencillo y del cual ya vimos al equivalente en IPFire: el bloqueo según geolocalización.



Con pfBlockerNG ya preconfigurado, podemos acceder al apartado de IP – GeoIP para denegar el tráfico según la geolocalización de la otra dirección IP. Existe la posibilidad de indicar que se bloqueé solo para tráfico entrante, saliente o para ambos casos, además también cuenta con un grupo predefinido llamado “top spammers”.

Name	Description	Action	Logging
Top Spammers	GeoIP Top Spammers	Deny Both	Enabled
Africa	GeoIP Africa	Deny Inbound	Enabled
Antarctica	GeoIP Antarctica	Deny Inbound	Enabled
Asia	GeoIP Asia	Deny Inbound	Enabled
Europe	GeoIP Europe	Disabled	Enabled
North America	GeoIP North America	Disabled	Enabled
Oceania	GeoIP Oceania	Disabled	Enabled

Pero, sin duda, la funcionalidad más potente de este paquete es el DNSBL, con el cual podemos bloquear direcciones IP que se encuentran en listas y repositorios de la comunidad. Por defecto, en “Feeds” se encuentran ya seleccionadas las fuentes de estas listas, aunque se pueden añadir desde fuentes externas, desactivar o eliminar cualquier fuente.

IPv4 Category	Selected		
IPv4	PRI1	Abuse Feodo Tracker	<input checked="" type="checkbox"/> Abuse_Feodo_C2
IPv4	PRI1	> Abuse Feodo Tracker	<input type="radio"/> Abuse_Feodo_C2_med
IPv4	PRI1	> Abuse Feodo Tracker	<input type="radio"/> Abuse_Feodo_C2_Agr
IPv4	PRI1	Abuse SSL Blacklist	<input checked="" type="checkbox"/> Abuse_SSLBL
IPv4	PRI1	> Abuse SSL Blacklist	<input type="radio"/> Abuse_SSLBL_Agr
IPv4	PRI1	CINS Army	<input checked="" type="checkbox"/> CINS_army
IPv4	PRI1	Emerging Threats	<input checked="" type="checkbox"/> ET_Block
IPv4	PRI1	Emerging Threats	<input checked="" type="checkbox"/> ET_Comp



Desde la pestaña “IP” es desde donde activamos el servicio para IPv4 y/o para IPv6, al igual que en el bloqueo por país, pfBlocker nos da a elegir entre denegar tráfico entrante, saliente o ambos.

The screenshot shows the pfBlockerNG interface under the IP tab. It is specifically viewing the IPv4 rules. A single rule is listed:

Name	Description	Action	Frequency	Logging
PRI1	PRI1 - Collecti...	Deny Both	Every hour	Enabled

Below the table are buttons for '+ Add' and 'Save'.

Para comprender las “listas” que está usando podemos ver cualquiera de ellas: En todas encontraremos direcciones IP o rangos de direcciones que se catalogan como maliciosos, spammers o sospechosos. DNSML bloqueará todas las de estos archivos si están activos.

The screenshot shows a browser window displaying a list of IP addresses and their details from the file <https://isc.sans.edu/block.txt>. The list includes:

IP Address	Port	Count	Source	Country	Contact	
45.155.205.0	45.155.205.255	24	8879	SELECTEL	RU	abuse@selectel.ru
45.134.26.0	45.134.26.255	24	8635	SELECTEL	RU	abuse@selectel.ru
45.146.166.0	45.146.166.255	24	8550	SELECTEL	RU	abuse@selectel.ru
89.248.163.0	89.248.163.255	24	7127	INT-NETWORK	SC	abuse@ipvolume.net
167.248.133.0	167.248.133.255	24	5175	CENSYS-ARIN-03	US	abuse@ipvolume.net
185.156.73.0	185.156.73.255	24	5081	SIBIRINVEST	NL	qwalarty@ukr.net
92.63.196.0	92.63.196.255	24	4218	FOPSERVER	UA	vvsg180@gmail.com
91.240.118.0	91.240.118.255	24	3645	GLOBALLAYER	NL	abuse@global-layer.com
193.163.125.0	193.163.125.255	24	3512	CYBER-CASA	GB	>>UNKNOWN<<
45.135.232.0	45.135.232.255	24	3476	SELECTEL-MSK	RU	abuse@selectel.ru
185.191.34.0	185.191.34.255	24	3376	SELECTEL-MSK	RU	abuse@selectel.ru
138.199.32.0	138.199.32.255	24	3368	CDN77 \^_	GB	abuse@cdn77.com

Aunque, para hacerlo funcional y aplicar los cambios de configuración se debe acudir a la pestaña “Update” y forzar la actualización del servicio.

The screenshot shows the pfBlockerNG interface under the Update tab. It displays the 'Update Settings' section. A red box highlights the 'Select 'Force' option' section, which contains three radio buttons: 'Update' (selected), 'Cron', and 'Reload'. Below this are 'Run' and 'View' buttons.



Con pfBlockerNG reiniciado tras la configuración, creará automáticamente la regla en el cortafuegos para bloquear todas las direcciones que se encuentran en su “feed”.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 1.64 MiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
0 / 0 B	IPv4 *	pfB_PRI1_v4	*	*	*	*	*	none	pfB_PRI1_v4	
0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	*	none	OpenVPN Servidor VPN para SAD wizard	

Para testearlo accedí desde mi subred (fuera de pfSense) a una de las direcciones que se consideran peligrosas, ya sea por malware, publicidad masiva, spam, ataques etc.



En el mismo momento exactamente, si intentamos llegar hasta esa dirección IP a través del host conectado a la red LAN de pfSense, no podremos, ya que nuestro firewall nos está protegiendo.

avarreterefirewall.navarre x ⓘ Problem loading page +

ⓘ https://103.243.25.83

Unable to connect

Firefox can't establish a connection to the server at 103.243.25.83.



Tanto en el log como en las alertas del servicio podremos confirmar que la dirección destino se ha bloqueado, y que mi máquina con dirección 192.168.2.13 y hostname "jorge-vb" ha sido la que ha intentado acceder.

The screenshot shows the 'Alerts' tab selected in the pfBlockerNG interface. Under 'Alert Settings' and 'Alert Filter', there are '+' icons. The main table lists 'Deny' entries from January 28, 2024, at various times. Each entry includes Date, IF, Rule, Proto, Source, Destination, GeolIP, and Feed information. For example, at 12:39:48, a TCP-S connection from LAN interface to port 1770008603 was denied by rule pfb_PRI1_v4 from source 192.168.2.13:53390 to destination 103.243.25.83:443.

Date	IF	Rule	Proto	Source	Destination	GeolIP	Feed
Jan 28 12:39:48	LAN	pfb_PRI1_v4 (1770008603)	TCP-S	192.168.2.13:53390 jorge-vb	103.243.25.83:443 Unknown	Unk	ET_Comp_v4 103.243.25.83
Jan 28 12:39:48	LAN	pfb_PRI1_v4 (1770008603)	TCP-S	192.168.2.13:53416 jorge-vb	103.243.25.83:80 Unknown	Unk	ET_Comp_v4 103.243.25.83
Jan 28 12:32:11	LAN	pfb_PRI1_v4 (1770008603)	TCP-S	192.168.2.13:58442 jorge-vb	66.240.236.119:443 census6.shodan.io	Unk	CINS_army_v4 66.240.236.119
Jan 28 12:32:11	LAN	pfb_PRI1_v4 (1770008603)	TCP-S	192.168.2.13:50598 jorge-vb	66.240.236.119:80 census6.shodan.io	Unk	CINS_army_v4 66.240.236.119

3.7 Ejemplos de reglas en firewall

Al igual que se realizó con IPFire, en pfSense crearemos algunas reglas personalizadas en el firewall. Personalmente me gusta más como se muestran las reglas, ya que podemos ver las reglas predefinidas para bloquear cualquier tráfico que intenta acceder a la LAN desde la WAN y las reglas que permiten cualquier tráfico desde la LAN a cualquier destino.

Comenzaremos, pues, desactivando estas reglas predefinidas para permitir el tráfico IPv4 e IPv6 desde la LAN a Internet, ya que configuraremos el mismo ejemplo que en IPFire: solo se permitirá a los clientes conectarse a sitios web por HTTPS.

The screenshot shows the 'Rules / LAN' tab selected in the pfSense Firewall interface. Under 'Floating', 'WAN', and 'LAN' tabs, the 'LAN' tab is active. The table lists several pre-defined rules: 'Anti-Lockout Rule' (Status: 2/517 KiB, Protocol: *, Source: *, Destination: LAN Address, Port: 443, Gateway: *, Queue: *, Schedule: *), 'Default allow LAN to any rule' (Status: 32 /497.56 MiB, Protocol: IPv4, Source: LAN net, Destination: *, Port: *, Gateway: *, Queue: *, Schedule: none), and 'Default allow LAN IPv6 to any rule' (Status: 0 / 0 B, Protocol: IPv6, Source: LAN net, Destination: *, Port: *, Gateway: *, Queue: *, Schedule: none). The last two rules are highlighted with a red box. Action buttons for Add, Edit, Delete, Save, and Separator are at the bottom.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
2 /517 KiB	*	*	*	LAN Address	443	*	*	*	Anti-Lockout Rule	
32 /497.56 MiB	IPv4	*	*	*	*	*	*	none	Default allow LAN to any rule	
0 / 0 B	IPv6	*	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	



Como sabemos, debemos también permitir el tráfico al servidor DNS, es decir, desde la LAN (Source: LAN net), a cualquier red con puerto de destino 53 y con protocolo TCP y UDP.

The screenshot shows the 'Edit Firewall Rule' configuration. In the 'Protocol' field (highlighted with a red box), 'TCP/UDP' is selected. In the 'Source' section, 'Source' is set to 'LAN net'. In the 'Destination' section, 'Destination' is set to 'any' and 'Destination Port Range' is set to 'DNS (53)' (highlighted with a red box). Both the 'Source' and 'Destination' sections have their respective 'Protocol' dropdowns highlighted with red boxes.

Lo mismo haremos para permitir el tráfico HTTPS (puerto 443 y protocolo solo TCP) desde la red interna.

The screenshot shows the 'Firewall / Rules / LAN' interface. The 'LAN' tab is active. A message at the top states: 'The changes have been applied successfully. The firewall rules are now reloading in the background.' Below this, the 'Rules (Drag to Change Order)' table lists several rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1 /1.75 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
✓ 0 /0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			
✓ 0 /0 B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none			
✓ 0 /0 B	IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule	
✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule	

At the bottom of the table, there are buttons for 'Add', 'Delete', 'Save', and 'Separator'.

De esta forma hemos conseguido lo mismo que en IPFire, los hosts conectados a pfSense pueden acceder a páginas como "https://www.twitter.com", pero no a, por ejemplo, "http://www.fuentezuelas.com", ni tampoco a videojuegos etc.



4 Conclusiones

Decidí realizar esta práctica con pfSense además de con IPFire para aprender sobre ambos y llegar a conclusiones respecto a sus diferencias. Después de todo el proceso, a pesar de que la instalación y primera configuración de pfSense es algo más lenta y menos guiada que en IPFire, la interfaz web del sistema de Netgate me parece mejor organizada y con una funcionalidad y estabilidad mucho mayor.

IPFire me ha dado problemas a la hora de mantener su configuración estable durante estos días, también le costaba detectar escaneos y ataques que venían de redes externas (Internet), y, sin embargo, pfSense detectaba rápidamente cualquier ataque y bloqueaba de forma casi instantánea la dirección IP del atacante.

Sin embargo, es cierto que para tareas más simples como implantar un portal cautivo o como para añadir un par de reglas al firewall, IPFire puede llegar a ser más sencillo, ya que su interfaz web no está tan cargada con funcionalidades extra, y, por tanto, para usuarios novatos puede llegar a ser más intuitiva.

Para concluir, debo recalcar que añadir reglas al firewall es algo muy general, y mi objetivo en esta práctica ha sido solo mostrar cómo, dependiendo de lo que deseemos o necesitemos, podemos permitir o bloquear cualquier tráfico según su origen o destino.

5 Referencias

IPFIRE COMMUNITY. *IPFire Wiki*. <Wiki.ipfire.org> [Consulta: 23/01/2022].

NETGATE. *pfSense Documentation*. <Docs.netgate.com | pfSense> [Consulta: 25/01/2022].

LAWRENCE SYSTEMS. *Youtube channel*. <[Youtube.com](https://Youtube.com/TheTecknowledge) | TheTecknowledge> [Consulta: 27/01/2022].

Jorge Navarrete, 2º ASIR.