



RFID TRAFFIC ANALYST

 **pfSense**
– GUIA DE USUARIO –

Xavi Conde
Gerard Soteras



Índice

¿Qué es pfSense?.....	3
Configuración inicial.....	3
Configuración de las redes en pfSense.....	3
Configuración de la red WAN gráficamente.....	6
Configuración del servicio Nginx.....	6




¿Qué es pfSense?

pfSense es una distribución de software basada en FreeBSD utilizada para la implementación de cortafuegos y enrutadores. Se caracteriza por su flexibilidad, seguridad y facilidad de uso, permitiendo a los administradores de red gestionar configuraciones avanzadas a través de una interfaz web intuitiva. Gracias a su amplia compatibilidad con múltiples plataformas y su soporte para plugins y extensiones, pfSense es una solución robusta para redes empresariales y domésticas.

Configuración inicial

Para la instalación de pfSense utilizaremos VirtualBox. Antes de iniciar la máquina virtual, es necesario configurar los adaptadores de red. En esta configuración inicial, agregaremos dos adaptadores: uno para la red WAN y otro para la red LAN.

 **Red**

Adaptador 1: Intel PRO/1000 MT Desktop (Adaptador puente, «Intel(R) Ethernet Connection (14) I219-LM»)
Adaptador 2: Intel PRO/1000 MT Desktop (Red NAT, «ASIX2_LAB»)

Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
ASIX2_LAB	10.20.30.0/24	fd17:625c:f037:141e::/64	Habilitado

Configuración de las redes en pfSense

Al iniciar la máquina virtual, aparecerá una lista de opciones numeradas. Para configurar las direcciones IP de las interfaces, seleccionamos la opción 2.

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

Enter an option: █
```

- **Configuración de la interfaz WAN:** En este ejemplo, asignaremos una IP estática (100.77.20.51). Sin embargo, lo más recomendable es que la dirección IP sea proporcionada por el servidor DHCP de la red. En nuestro caso, la red del aula asigna direcciones en el rango 100.77.20.0/24.



```
Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 100.77.20.51

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 32):
> 24

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

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

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

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

The IPv4 WAN address has been set to 100.77.20.51/24
You can now access the webConfigurator by opening the following URL in your web
browser:

    http://100.77.20.51/
```

- **Configuración de la interfaz LAN:** Esta red pertenece a la configuración previa realizada en VirtualBox. Se activa el servicio DHCP y se establece la red en el rango 10.20.30.0/24. Para la máquina pfSense, configuramos la IP 10.20.30.100 y definimos el gateway en 10.20.30.1.

WAN (wan)	-> em0	-> v4/DHCP4: 100.77.20.51/24
LAN (lan)	-> em1	-> v4: 10.20.30.100/24



Una vez configuradas las interfaces de red, podemos acceder a la interfaz gráfica de administración de pfSense. Para ello, es necesario utilizar una máquina con entorno gráfico conectada a la red LAN.

Si se requiere acceso desde la red WAN, es posible desactivar temporalmente las restricciones de seguridad utilizando el siguiente comando en pfSense (opción 8 para abrir el terminal):

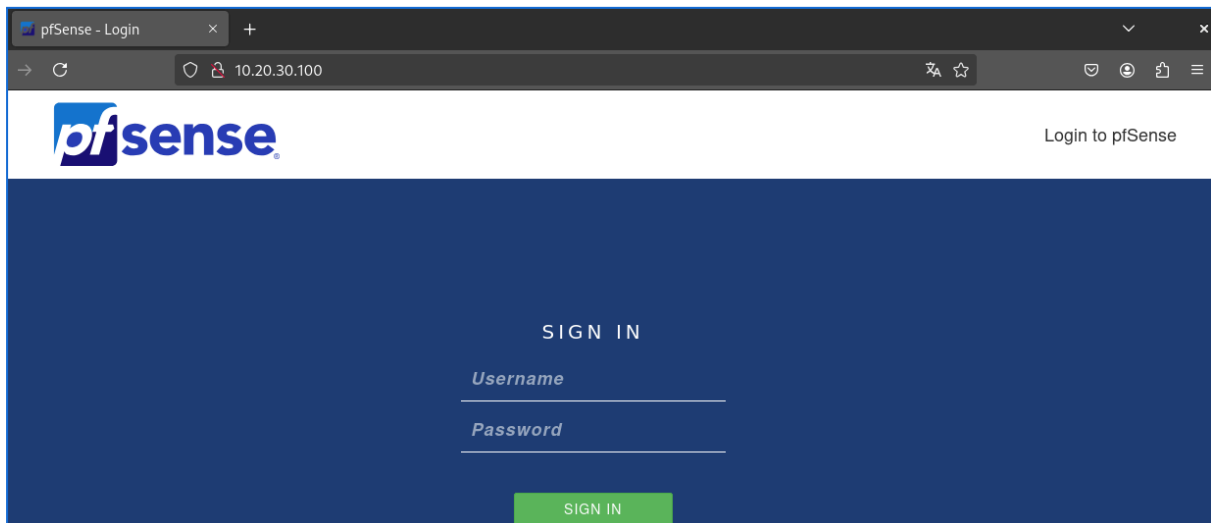
```
pfctl -d
```

Este comando permite acceder a la interfaz de configuración desde la WAN ingresando la dirección IP correspondiente. Sin embargo, esto representa un riesgo de seguridad, ya que puede abrir una puerta de acceso a usuarios no autorizados.

Desde una máquina en la red LAN, al ingresar la dirección IP de pfSense en un navegador, se mostrará la página de inicio de sesión. Por defecto, las credenciales son:

- **Usuario:** admin
- **Contraseña:** pfsense

Se recomienda cambiar la contraseña inmediatamente después del primer inicio de sesión para mejorar la seguridad del sistema.

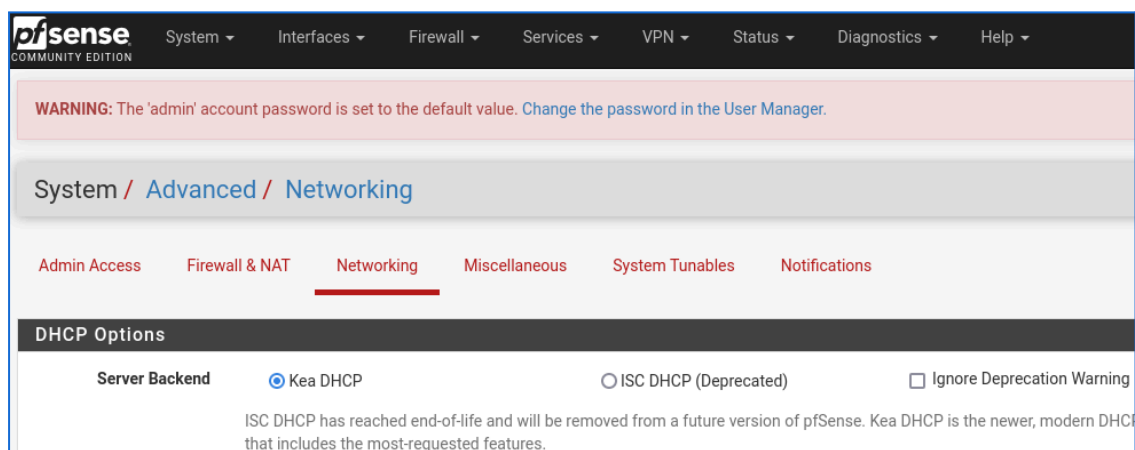




Configuración de la red WAN gráficamente

Para configurar la red WAN desde la interfaz web de pfSense, seguimos estos pasos:

1. Accedemos a la página de configuración de pfSense.
2. Nos dirigimos a **System** → **Advanced** → **Networking**.
3. Activamos la opción **Kea DHCP**.



Configuración del servicio Nginx

Si en la red LAN existe un servidor web con Nginx, podemos configurar pfSense para redirigir el tráfico de la WAN hacia dicho servidor. Para ello, realizamos la configuración en la sección de reglas del firewall:

1. Accedemos a **Firewall** → **Rules** → **WAN**.
2. Configuramos la regla con los siguientes parámetros:
 - **Action:** Pass (permite el tráfico entrante)
 - **Interface:** WAN (interfaz afectada por la regla)
 - **Protocol:** TCP/UDP (protocolos permitidos)
 - **Destination:** IP del servidor Nginx
 - **Destination Port Range:** HTTP 80 – HTTP 80 (puerto de acceso al servidor web)
 - **Description:** Se recomienda agregar una descripción para identificar la regla.



pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾

WARNING: The 'admin' account password is set to the default v

Firewall / Rules / WAN

Floating **WAN** LAN

Edit Firewall Rule

Action

Pass ▾

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Associated filter rule

This is associated with a NAT rule.
Editing the interface, protocol, source, or destination of associated filter rules is not permitted.
[View the NAT rule](#)

Interface

WAN ▾

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

Address Family

IPv4 ▾

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP ▾

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any ▾

Source Address ▾ / ▾ ▾

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Extra Options

Log

☐ Log packets that are handled by this rule

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

Description

NAT

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗ 0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
<input checked="" type="checkbox"/>	✗ 0/18 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	*	*	10.20.30.50	80 (HTTP)	*	none		NAT	⚓ ⚙ ⏏ ⚡

Con esta configuración, cualquier solicitud HTTP que llegue a la IP de pfSense en la WAN será redirigida al servidor Nginx en la LAN.



Comprobación de la IP del servidor Nginx (10.20.30.50)

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:71:8c:3a brd ff:ff:ff:ff:ff:ff
    inet 10.20.30.50/24 brd 10.20.30.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe71:8c3a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Comprobación del servicio Nginx activo.

```
g_soteras@debian:~$ systemctl status nginx
• nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enable
   Active: active (running) since Wed 2025-02-26 17:59:15 CET; 42s ago
```

Accedemos a la página web desde la red WAN introduciendo la IP de pfSense.

