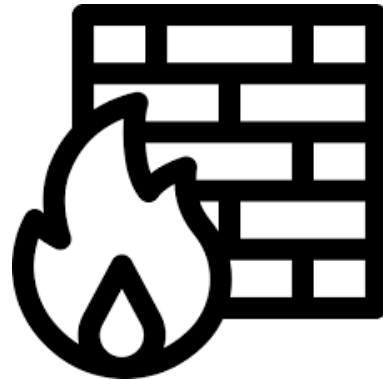


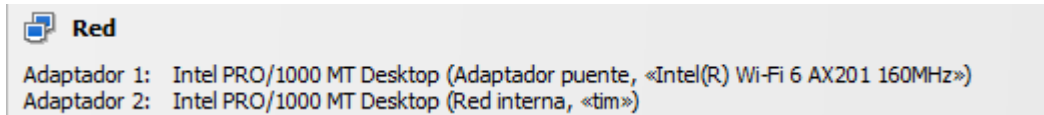
PfSense y Port Forwarding

TMD

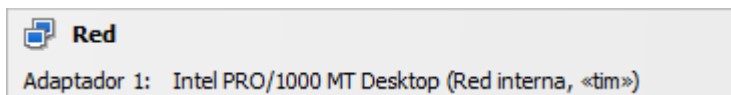


I.1 Configuración del pfSense CLI

Para realizar la instalación de pfSense y configuración de PortForward primero necesitamos dos máquinas virtuales, una para pfSense y otra para visualizar su interfaz de manera gráfica y acceder a los ajustes del administrador. Además vamos a hacer la configuración previa de los adaptadores de red en ambas máquinas. Todo el proceso se va a realizar dentro de VM VirtualBox. Para que la nuestra ubuntu desktop pueda tener conexión a través de pfSense vamos a utilizar red interna. Adaptadores de red de la máquina pfSense.



Adaptador de red del ubuntu desktop para la visualización gráfica del pfSense.



Al iniciar la máquina virtual, vemos la siguiente pantalla:

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.34.44/22
LAN (lan)      -> em1      -> v4: 10.20.30.1/24

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

Enter an option: 
```

Vamos a configurar las dos interfaces de red, para ello vamos a elegir la opción 2 y luego la interfaz que queremos configurar, empezaremos por la WAN.

```
Available interfaces:

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

Habilitamos la asignación por dhcp para que nos dé una ip pública de la máquina del pfsense en IPv4. Para IPv6 no vamos a configurar nada, por lo tanto, queda todo por defecto o deshabilitado según el ajuste. Hacemos el mismo procedimiento para la LAN pero, en este caso le asignaremos una IP estática con 24bits de subnet. Además vamos a asignar el gateway manualmente y habilitar que brinde DHCP hacia otros dispositivos que estén en la misma red en un rango de IPs de .100 a .110.

Comandos importantes a tener en cuenta dentro de CLI:

para deshabilitar firewall: pfctl -d

para habilitar: pfctl -e

I.2 Configuración del pfSense GUI + PortForward

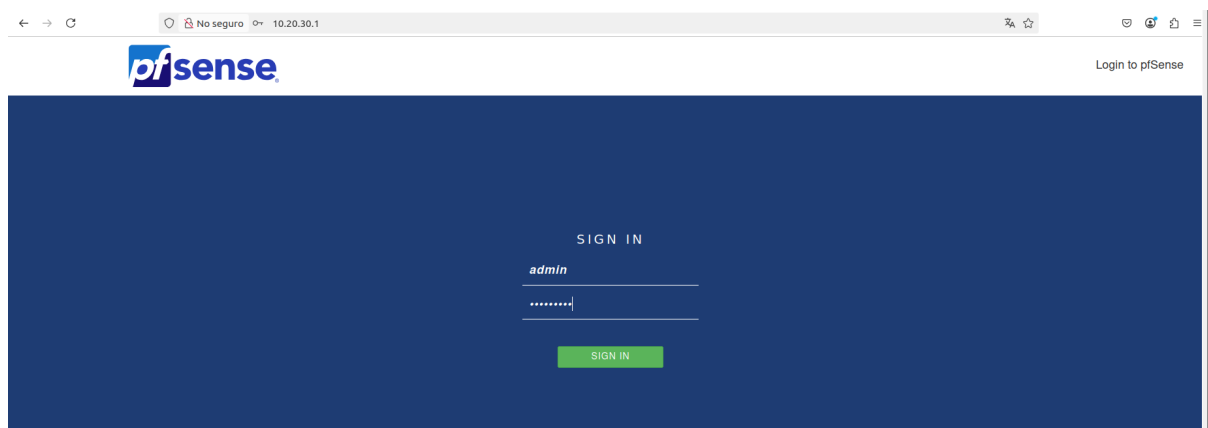
Como podemos comprobar, se nos asignó correctamente la IP a la máquina con interfaz gráfica.

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:98:69:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.20.30.100/24 brd 10.20.30.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7055sec preferred_lft 7055sec
    inet6 fe80::a00:27ff:fe98:69f7/64 scope link
        valid_lft forever preferred_lft forever
```



Para acceder a la configuración del pfSense introducimos la IP estática de la LAN que configuramos antes en el navegador de nuestra máquina.

Las credenciales por defecto son las siguientes:

- Usuario: admin
- Contraseña: pfsense



Nada más entrar comprobamos que las interfaces de red aparecen correctamente en la página principal.

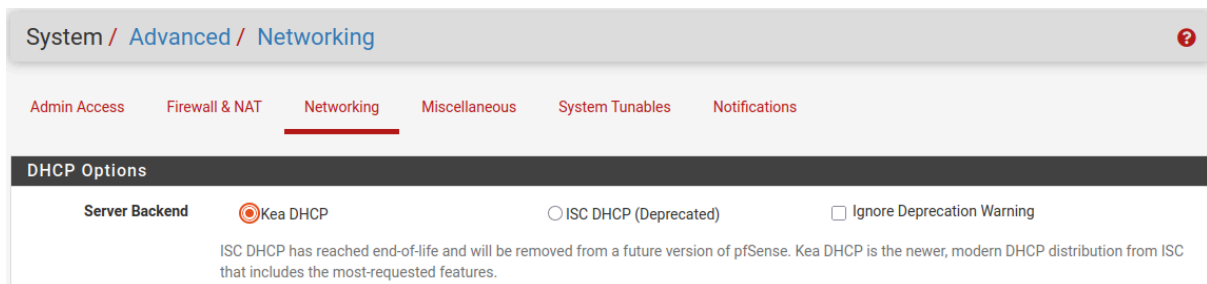
Interfaces ⚙️ - ✖️			
 WAN	↑	1000baseT <full-duplex>	192.168.34.75
 LAN	↑	1000baseT <full-duplex>	10.20.30.1

Para quitar el warning de la contraseña del admin por defecto vamos a la ruta siguiente y lo modificamos.

System / User Manager / Users / Edit

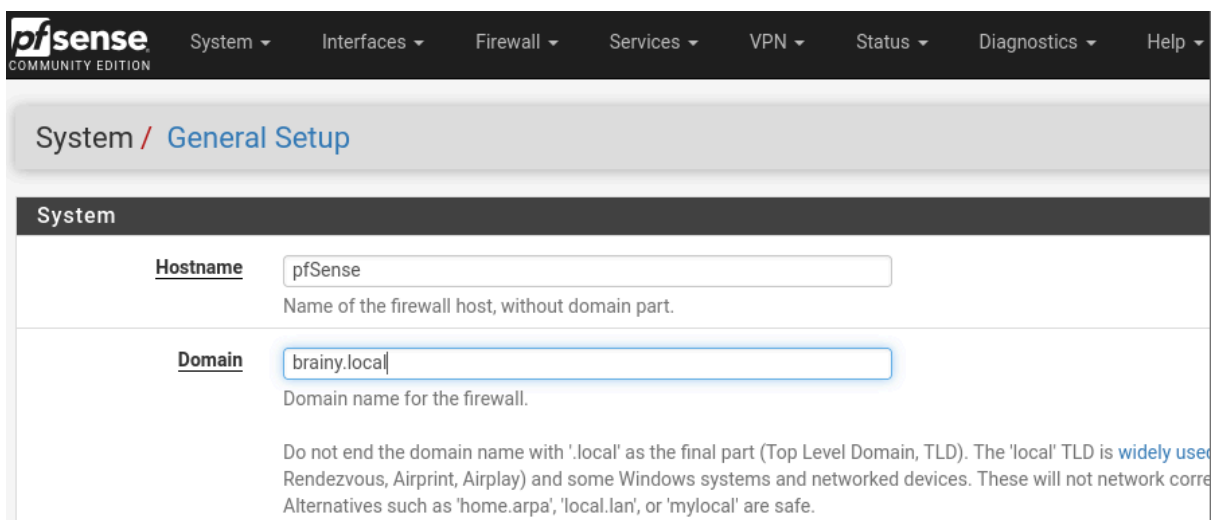


Activaremos el Kea DHCP.



The screenshot shows the 'DHCP Options' configuration page in pfSense. The breadcrumb trail is 'System / Advanced / Networking'. The 'Networking' tab is selected. Under 'Server Backend', 'Kea DHCP' is selected with a radio button, while 'ISC DHCP (Deprecated)' is unselected. There is an unchecked checkbox for 'Ignore Deprecation Warning'. A warning message states: 'ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution from ISC that includes the most-requested features.'

Además vamos a asignar un nuevo dominio, dejaremos el hostname igual, el resultado quedará como: pfsense.brainy.local.

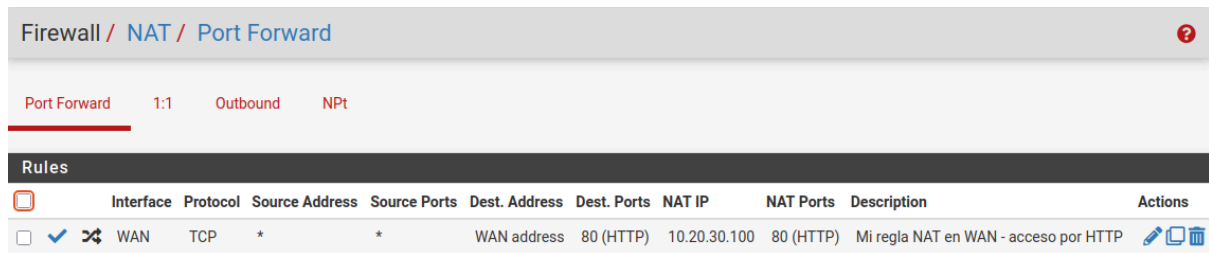


The screenshot shows the 'General Setup' page in pfSense. The breadcrumb trail is 'System / General Setup'. Under the 'System' section, the 'Hostname' is set to 'pfSense' and the 'Domain' is set to 'brainy.local'. A warning message at the bottom states: 'Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The '.local' TLD is widely used for Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.'

PortForward

Vamos a configurar la red WAN y poder hacer PortForward para que podamos ver una página web alojada en un servidor de nuestra red LAN introduciendo la IP del firewall desde la WAN.

Primero configuraremos la interfaz WAN y aplicaremos una nueva regla de firewall, para ello nos vamos por la ruta siguiente: FireWall → NAT → Port Forward



Configuramos una nueva regla con los siguientes parámetros:

- Interfaz: WAN
- Address family: IPv4
- Protocol: TCP
- Destination: WAN address
- Destination port: HTTP (puerto 80 por defecto)
- Redirect target IP: single host - (IP donde esté SERVIDOR WEB)
- Redirect target port: HTTP (puerto 80 por defecto)
- Description: regla NAT en WAN

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

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

Protocol Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

Display Advanced

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


Destination

Destination ☐ Invert match /

Destination Port Range

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

También podemos poner nuestra descripción personalizada de la regla que acabamos de hacer.

Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>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).</small>
Description	<input type="text" value="NAT Mi regla NAT en WAN - acceso por HTTP"/> <small>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.</small>
Advanced Options	 Display Advanced

Esta misma regla se creará automáticamente en Firewall → Rules → WAN
Con esta configuración, cualquier solicitud HTTP que llegue a la IP de pfSense en la WAN será redirigida al servidor Nginx en la LAN.

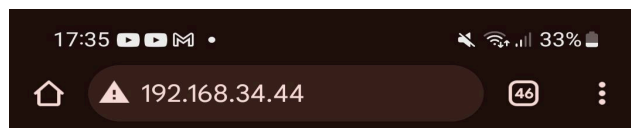
I.3 Comprobación de la regla

Para comprobar que todo funciona correctamente vamos a necesitar ver la misma página web del nginx accediendo por la ip de la interfaz WAN a través del dispositivo móvil.

Primero comprobamos el estado del nginx en nuestra máquina:

```
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-03-24 15:09:16 CET; 48min ago
```

Comprobamos desde el móvil el funcionamiento del PortForward conectándonos por la IP pública de la WAN más el puerto configurado previamente en la regla, en este caso, el puerto 80.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

