

Tema 2. Seguridad Perimetral (FW)

Índice

1. ¿Qué es un cortafuegos o Firewall?	1
1.1 Diseño de red. Seguridad por zonas	1
2. Instalación de un FireWall: pfSense	2
2.1 Antes de la instalación	3
2.2 Escenario	3
2.3 Instalación del pfSense	4
Por pasos	4
Webgrafía	11

1. ¿Qué es un cortafuegos o Firewall?

Un **cortafuegos** (*firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todas las tramas que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada una de ellas y bloqueando aquellas que no cumplan los criterios de seguridad especificados.

También es frecuente conectar al cortafuegos a una tercera red, llamada «**zona desmilitarizada**» o **DMZ**, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

1.1 Diseño de red. Seguridad por zonas

En seguridad informática, una **zona desmilitarizada** (conocida también como **DMZ**, sigla en inglés de *demilitarized zone*) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo

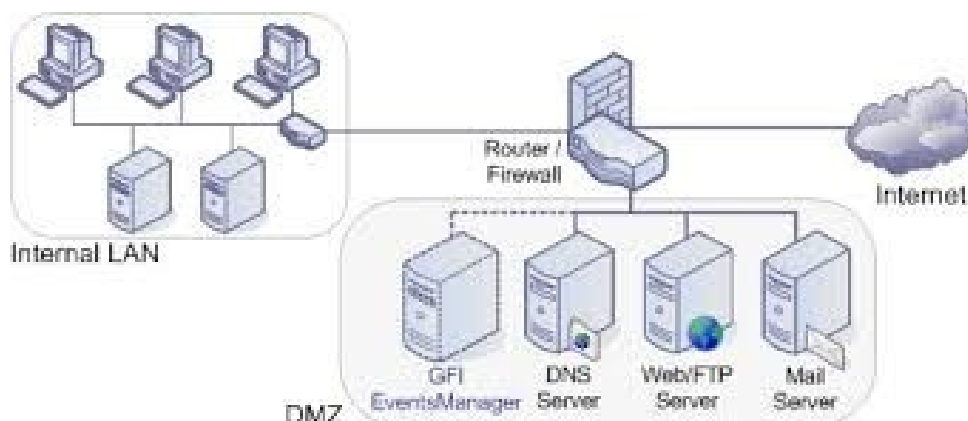
de una *DMZ* es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la *DMZ* solo se permitan a la red externa -- los equipos (*hosts*) en la *DMZ* no pueden conectar con la red interna.

Esto permite que los equipos (*hosts*) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (*host*) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La *DMZ* se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la *DMZ* se controlan generalmente utilizando *port address translation (PAT)*.

Un firewall es relevante particularmente en la implementación de DMZ, ya que es responsable de garantizar que las políticas adecuadas para proteger a las redes locales de DMZ se encuentren habilitadas, mientras que se mantiene la accesibilidad a la zona desmilitarizada (DMZ).



2. Instalación de un FireWall: pfSense

El **pfSense** es una distribución gratuita, de código abierto basada en FreeBSD, con funcionalidades de cortafuegos y router. Es posible actualizar y añadir nuevas características mediante la instalación de los paquetes correspondientes

Algunas de estas son:

- Reglas de cortafuegos

- Reglas basadas en estados de las conexiones
- Portal cautivo, RADIUS
- VPN (IPSec, PPTP, OpenVPN)
- NAT, Port-forwarding
- Redundancia: CARP
- Balanceo de carga
- Monitorizacion

FreeBSD es un sistema operativo para arquitecturas x86 compatibles (incluyendo Pentium® y Athlon™), amd64 compatibles (incluyendo Opteron™, Athlon™64 y EM64T), Alpha/AXP, IA-64, PC-98 y UltraSPARC®. Es un derivado de BSD, la versión de UNIX® desarrollada en la Universidad de California, Berkeley. El soporte para otras arquitecturas está en diferentes fases de desarrollo.

FreeBSD está disponible completamente gratis incluyendo el código fuente.

2.1 Antes de la instalación

- Comprobación de los requisitos Hardware

https://doc.pfsense.org/index.php/Hardware_requirements

- Compatibilidades_

http://www.pfsense.org/index.php?option=com_content&task=view&id=46&Itemid=51.html

2.2 Escenario

- Partiremos inicialmente de una máquina virtual con una sola tarjeta de red, en **modo *bridge*** en la que se instalará el pfSense. Simularemos así, la **WAN**

- Añadiremos a la mv otra tarjeta de red para simular la **LAN**, en modo **“Red aislada”** (en nuestro caso, crearemos una tarjeta de red basada con una gestión de networking “LAN”). De manera que la máquina real pueda también pertenecer a la red interna y tener papel de cliente. Ganamos así recursos puesto que el desktop que necesitamos para la prácticas, ya está instalado en la máquina real. La red en la que vamos a trabajar será la 192.168.100+NºPC.0/24.
- Por último, añadiremos otra tarjeta de red a la mv para emular el acceso a la **DMZ**. La tarjeta añadida trabajará en modo **“Red aislada”** también, pero en este caso sobre la gestión de red “DMZ”. La red en la que vamos a trabajar será la 172.20.100+NºPC .0/24

2.3 Instalación del pfSense

El pfSense permite la instalación a partir de una iso (**LiveCD**) o bien por red, mediante **PXE**.

Preboot eXecution Environment (PXE) (Entorno de ejecución de prearranque), es un entorno para arrancar e instalar el sistema operativo en PCs a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos instalados.

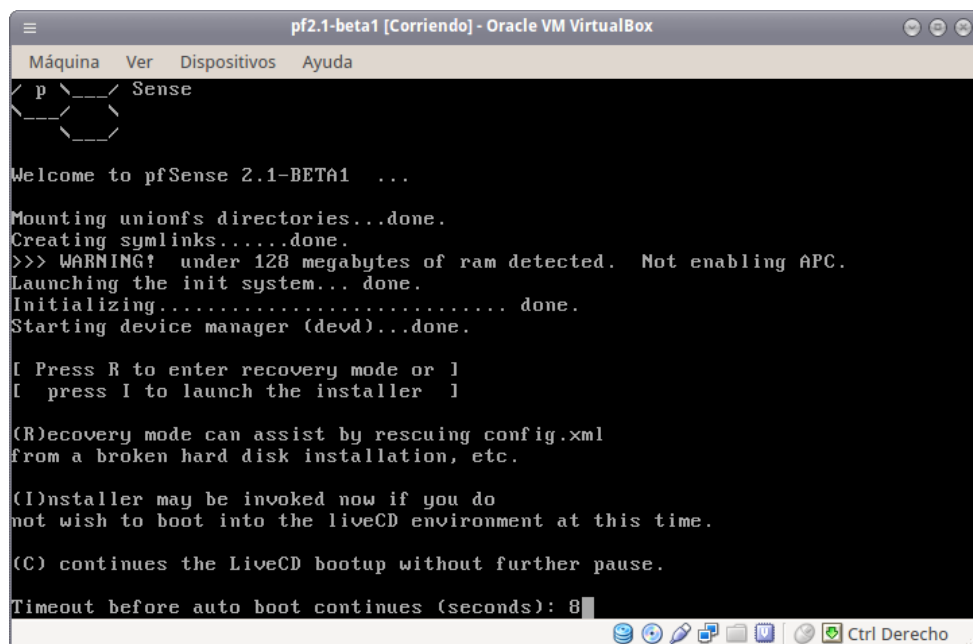
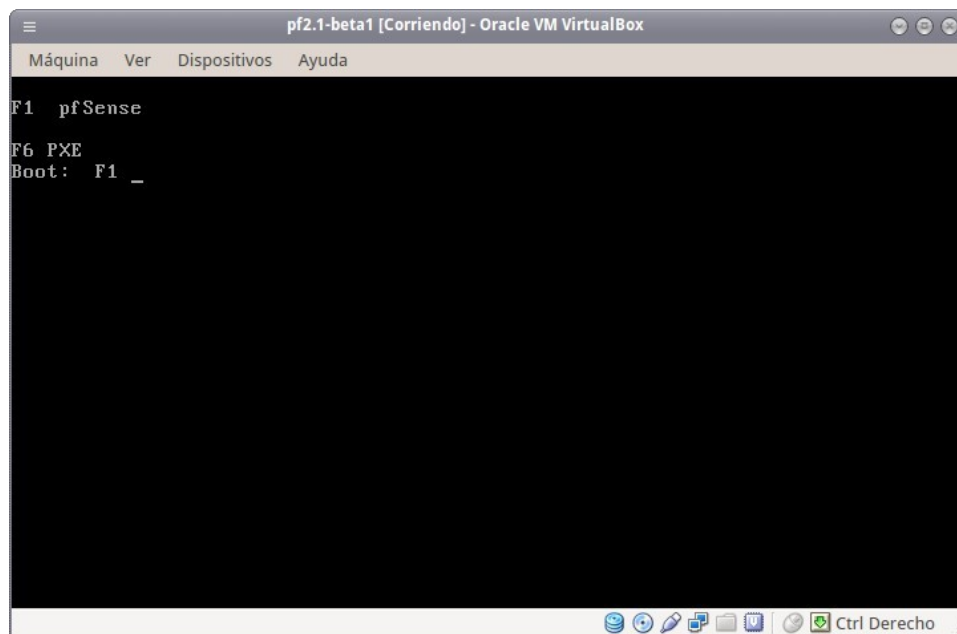
El firmware del cliente trata de encontrar un servicio de redirección PXE en la red para recabar información sobre los servidores de arranque PXE disponibles. Tras analizar la respuesta, el firmware solicitará al servidor de arranque apropiado el *file path* de un *network bootstrap program* (NBP), lo descargará en la memoria RAM del ordenador mediante TFTP, probablemente lo verificará, y finalmente lo ejecutará. Si se utiliza un único NBP para todos los clientes PXE se puede especificar mediante BOOTP sin necesidad de un proxy DHCP, pero aún será necesario un servidor TFTP.

Nosotros, instalaremos el PfSense desde una iso

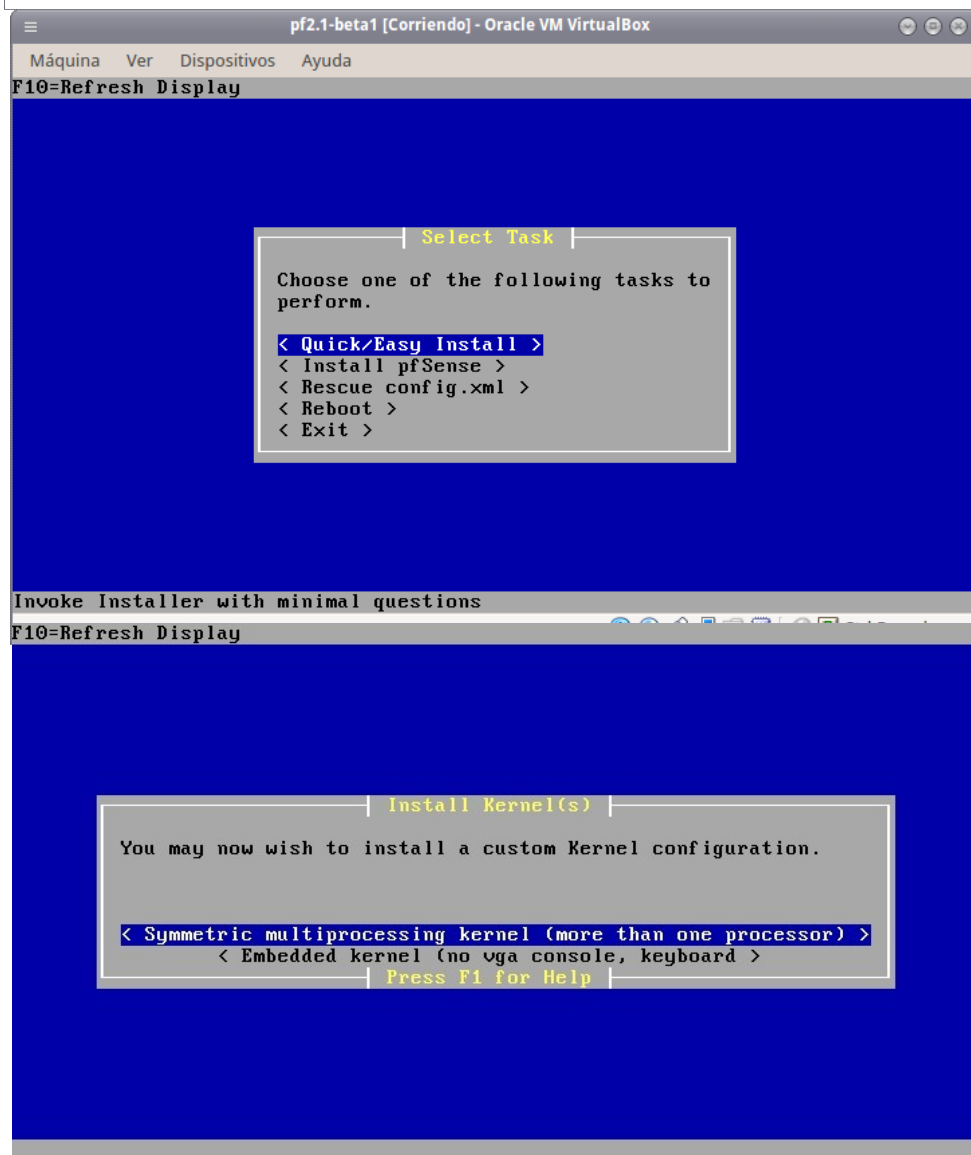
2.3.1 Por pasos

- Instalación del PfSense en una máquina con una sola tarjeta de red (mínimo imprescindible tener un WAN)

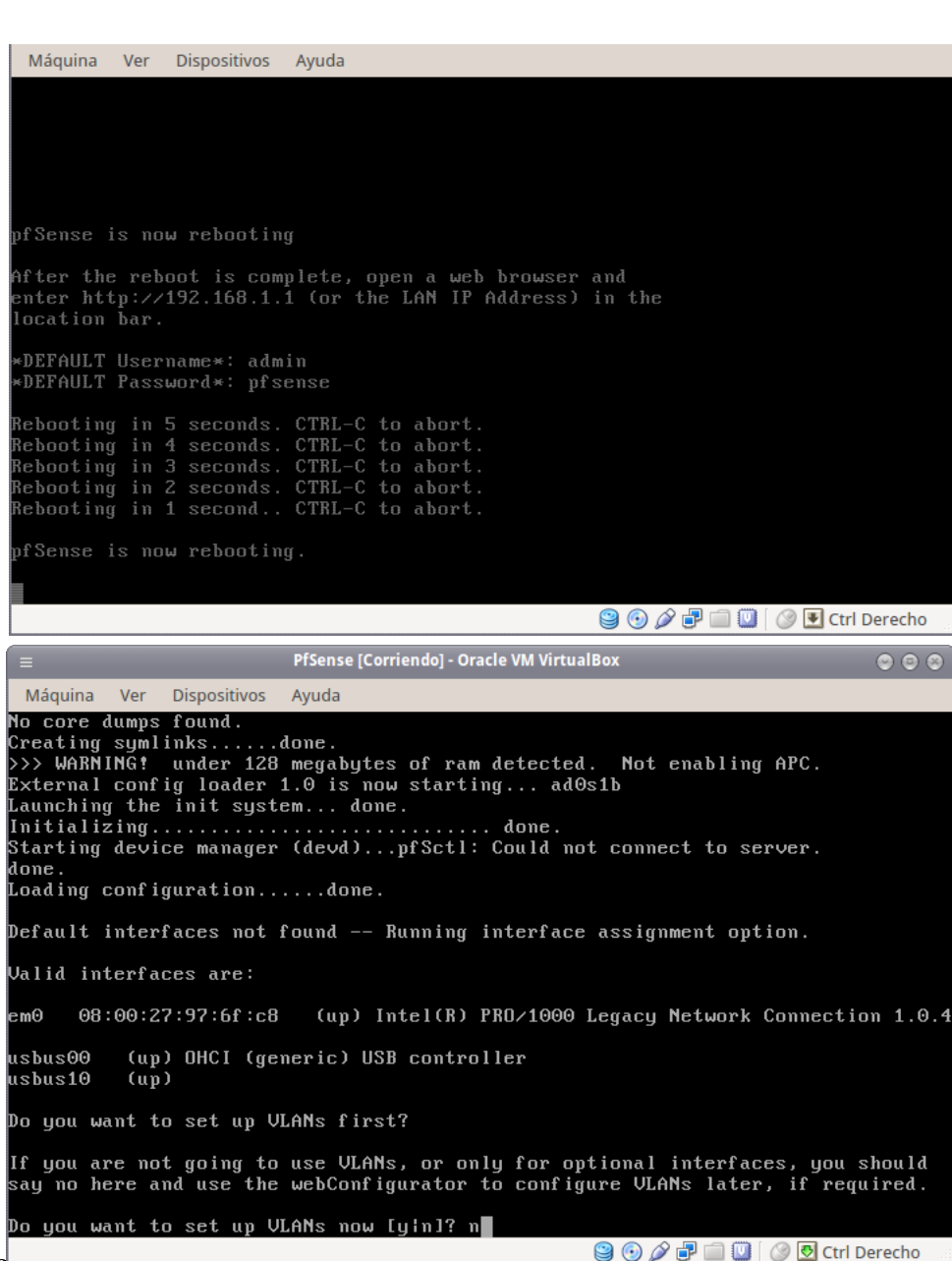
Tema 2. Seguridad Perimetral (FW)



Tema 2 Seguridad Perimetra FW



Tema 2 Seguridad Perimetra FW



```
Máquina Ver Dispositivos Ayuda

pfSense is now rebooting

After the reboot is complete, open a web browser and
enter http://192.168.1.1 (or the LAN IP Address) in the
location bar.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.
Rebooting in 2 seconds. CTRL-C to abort.
Rebooting in 1 second.. CTRL-C to abort.

pfSense is now rebooting.

PfSense [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
No core dumps found.
Creating symlinks.....done.
>>> WARNING! under 128 megabytes of ram detected. Not enabling APC.
External config loader 1.0 is now starting... ad@s1b
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...pfSctl: Could not connect to server.
done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.

Valid interfaces are:

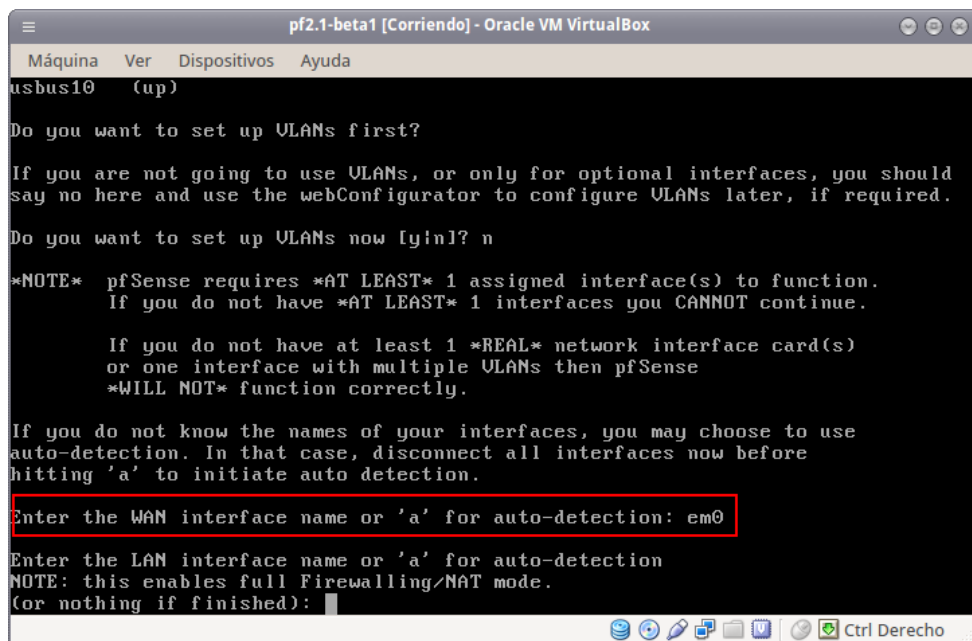
em0    08:00:27:97:6f:c8    (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
usb0    (up) OHCI (generic) USB controller
usb1    (up)

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? n
```

Tema 2. Seguridad Perimetral (FW)



```
pf2.1-beta1 [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
usb10 (up)

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

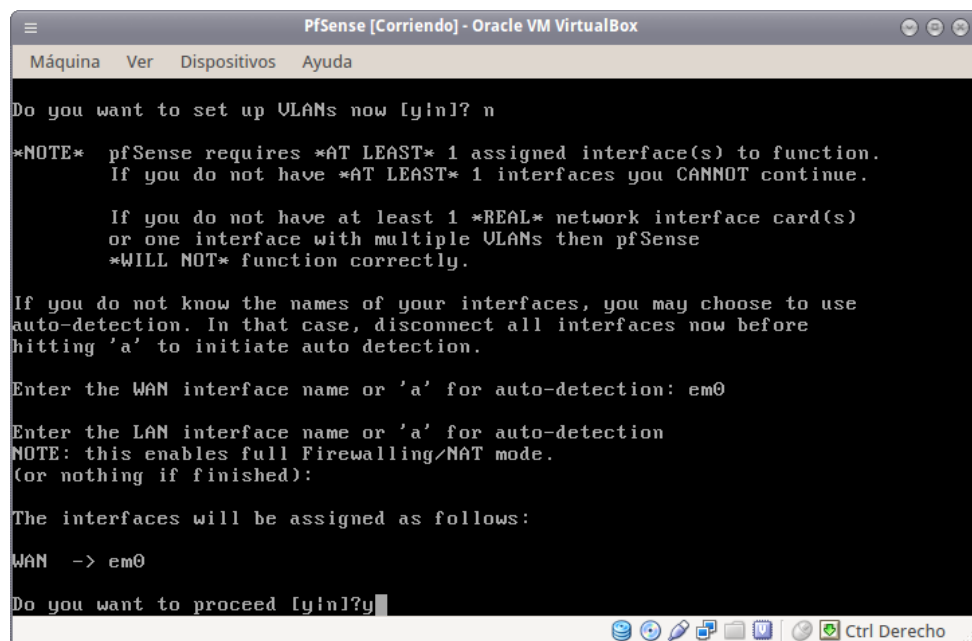
*NOTE* pfSense requires *AT LEAST* 1 assigned interface(s) to function.
If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

If you do not have at least 1 *REAL* network interface card(s)
or one interface with multiple VLANs then pfSense
*WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished):
```



```
PfSense [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda

Do you want to set up VLANs now [y|n]? n

*NOTE* pfSense requires *AT LEAST* 1 assigned interface(s) to function.
If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

If you do not have at least 1 *REAL* network interface card(s)
or one interface with multiple VLANs then pfSense
*WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> em0

Do you want to proceed [y|n]? y
```

Recordad que no debe arrancar desde CD/DVD, sino estaríamos instalando de nuevo el PfSense!

Al reiniciar, el PfSense ya nos muestra las diferentes opciones del menu


```
PfSense [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Starting webConfigurator...done.
Configuring CRON...done.
Starting NTP time client...Starting DNS forwarder...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting CRON... done.
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1-BETA0-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.3.5.132/24

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

Enter an option: 
```

- Captura las imágenes correspondientes al acceso al pfSense desde la WAN. Indica también el tipo de **protocolo** empleado y el **puerto** a través del que se ofrece el servicio, así como en qué **nivel** de la arquitectura TCP/IP se encuentra esta información

\$netstat

```
a026761180j@S04-PC02:~$ netstat -atun | grep :4433
tcp        0      0 172.20.102.1:42911  172.20.102.254:4433  TIME_WAIT
tcp        0      0 172.20.102.1:42912  172.20.102.254:4433  ESTABLECIDO
a026761180j@S04-PC02:~$
```

- Termina de configurar las opciones de DNS, zona horaria, contraseña del administrador, etc desde el acceso GUI al pfSense

System: General Setup

System

Hostname

pfSense
Name of the firewall host, without domain part
e.g. firewall

Domain

localdomain
Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. mycorp.com, home, office, private, etc.

DNS servers

DNS Server	Use gateway
8.8.8.8	none
	none
	none
	none

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

☒ **Allow DNS server list to be overridden by DHCP/PPP on WAN**
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

☐ **Do not use the DNS Forwarder or Resolver as a DNS server for the firewall**
By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on Localhost, so system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers.

Time zone

Europe/Madrid

Select the location closest to you

NTP time server

0.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

- Añadiremos la 2ª tarjeta de red para la recepción y envío de tramas a/desde la LAN. Añade las capturas correspondientes a la asignación de interfaces y la asignación de IP a la interfaz recién creada

The screenshot shows the 'General configuration' tab for a new network interface. The 'Enable' checkbox is checked, and the 'Enable Interface' button is visible. The 'Description' field is set to 'LAN'. The 'IPv4 Configuration Type' is set to 'Static IPv4', and the 'IPv6 Configuration Type' is set to 'None'. The 'MAC address' field is empty, with a note that it can be used to spoof the MAC address. The 'MTU' field is empty, with a note that the default is 1500 bytes. The 'MSS' field is empty, with a note that it will be in effect if a value is entered. The 'Speed and duplex' dropdown is set to 'Advanced'. Below the 'General configuration' tab, the 'Static IPv4 configuration' tab is visible, showing the 'IPv4 address' field set to '192.168.102.254' and the 'IPv4 Upstream Gateway' dropdown set to 'None'. The 'Private networks' section is also visible, with checkboxes for 'Block private networks' and 'Block bogon networks'.

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and duplex - Show advanced option

Static IPv4 configuration

IPv4 address /

IPv4 Upstream Gateway - or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.
On local LANs the upstream gateway should be "none".

Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

- El acceso a la GUI del PfSense ha cambiado. ¿Qué tipo de acceso permite ahora, local o externo?

Por defecto las reglas solo permiten local

- Configura el PfSense para que el acceso a su GUI sea a través de HTTPS y ssh

The image shows two sections of the pfSense web interface. The top section, titled "webConfigurator", has a "Protocol" field with two radio buttons: "HTTP" and "HTTPS". The "HTTPS" option is selected. The bottom section, titled "Secure Shell", has a "Secure Shell Server" field with a checked checkbox labeled "Enable Secure Shell". Below this is the "Authentication Method" section, which has a checkbox labeled "Disable password login for Secure Shell (RSA/DSA key only)". A note below this checkbox states: "When enabled, authorized keys need to be configured for each user that has been granted secure shell access." The "SSH port" field is empty, with a note below it: "Note: Leave this blank for the default of 22."

- El único usuario que puede gestionar el PfSense es el usuario *admin* que se crea por defecto, create otro nuevo usuario para ti

The image shows the "Users" management page in pfSense. The page has tabs for "Users", "Groups", "Settings", and "Servers". The "Users" tab is selected. The page displays the configuration for a user named "ausias". The "Defined by" field is set to "USER". The "Disabled" checkbox is unchecked. The "Username" field contains "ausias". The "Password" field has two input boxes for password and confirmation. The "Full name" field is empty, with a note: "User's full name, for your own information only". The "Expiration date" field is empty, with a note: "Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy". The "Group Memberships" section shows two lists: "Not Member Of" and "Member Of". The "Not Member Of" list contains "admins". The "Member Of" list is empty. Below these lists is a note: "Hold down CTRL (pc)/COMMAND (mac) key to select multiple items". The "Effective Privileges" section shows a table with columns "Inherited From", "Name", and "Description". The "User Certificates" section shows a table with columns "Name" and "CA". The "Authorized keys" section has a checkbox labeled "Click to paste an authorized key." The "IPsec Pre-Shared Key" field is empty.

- En la pestaña de *Firewall/NAT*, indica la utilidad del NAT/Outbound y del NAT/PortForwarding

Outbound

Firewall: NAT: Outbound

Port Forward 1:1 Outbound NPT

Mode: ☐ Automatic outbound NAT rule generation (IPsec passthrough included) ☐ Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)

- Dentro de la pestaña Firewall/Rules, indica las reglas que tienes activas por defecto y justificalo

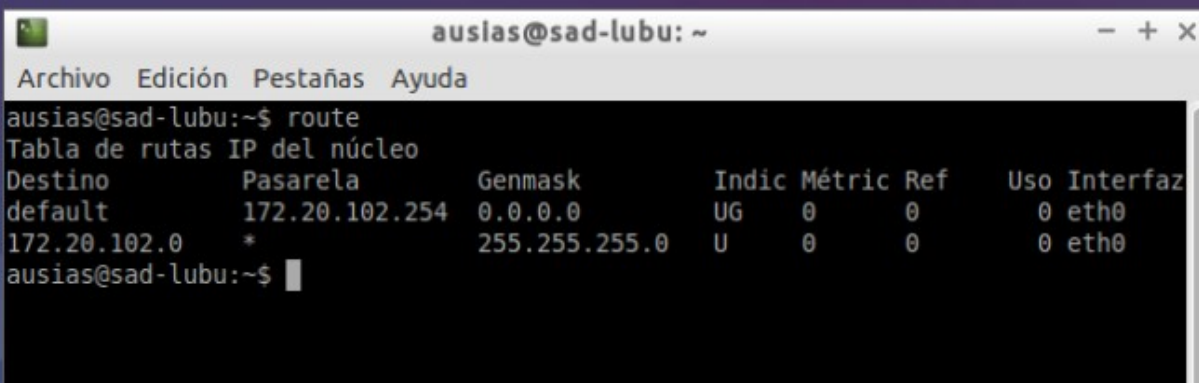
FloatingWANDMZLAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	

- Comprueba que funciona el enrutamiento desde un host de tu LAN. Puesto que no tenemos servidor DHCP, deberás configurar el fichero interfaces para configurar los parámetros de red de manera estática.

- Muestra la tabla de encaminamiento del host de la LAN

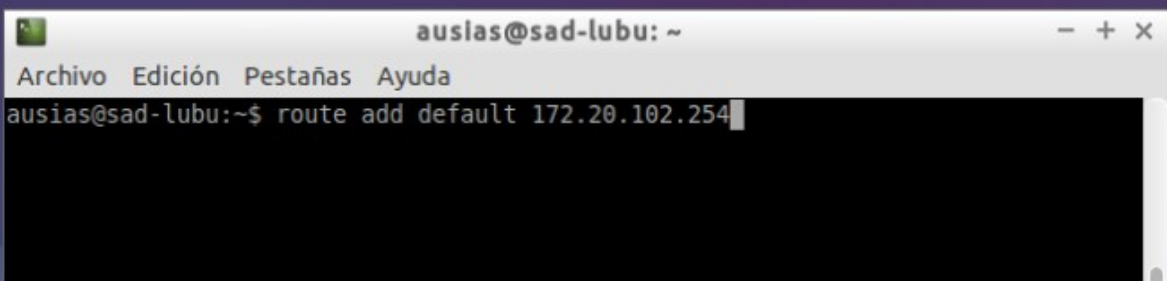
```
$route
```



Destino	Pasarela	Genmask	Indic	Métric	Ref	Uso	Interfaz
default	172.20.102.254	0.0.0.0	UG	0	0	0	eth0
172.20.102.0	*	255.255.255.0	U	0	0	0	eth0

- Elimina la configuración del gw del fichero interfaces, restartea el servicio para asegurarte de que no tienes gw y busca el comando para añadir el gw en caliente (sabiendo que cuando reinicies el servicio, se habrá eliminado este valor de gw)

```
$route
```



Webgrafia

DMZ

http://es.wikipedia.org/wiki/Zona_desmilitarizada_%28inform%C3%A1tica%29

FreeBSD

<http://www.freebsd.org/es/about.html>

Documentación

https://doc.pfsense.org/index.php/2.1_New_Features_and_Changes

Requisitos hardware

https://doc.pfsense.org/index.php/Hardware_requirements

Configuración PfSense - NAT – Outbound – Port

Forwarding

http://www.bellera.cat/josep/pfsense/nat_cs.html