**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

Webgrafia.......................................................................................................................................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. Todos 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

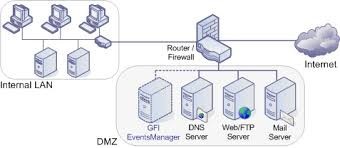
-- los equipos (*hosts*) en la *DMZ* no pueden conectar con la red interna.

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=](http://www.pfsense.org/index.php@option)com\_content&task=view&id=46&Itemid=5

1.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 asi, 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**.

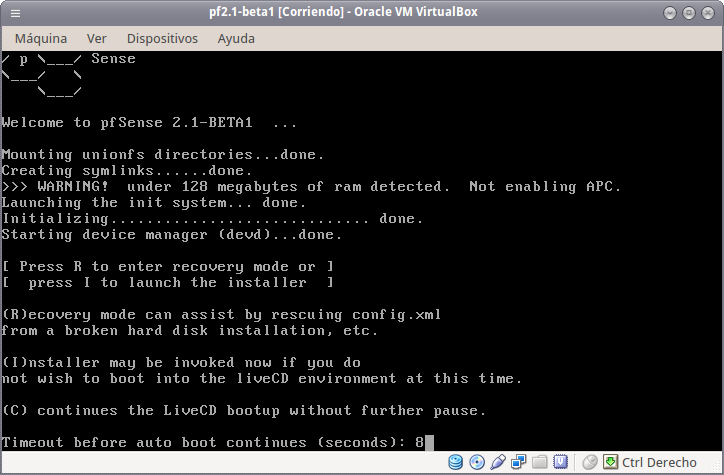
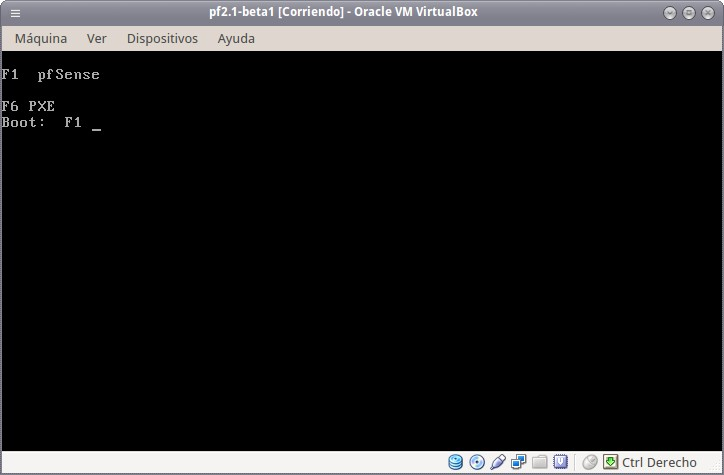
**Preboot eXecution Environment** (**PXE**) (Entorno de ejecución de prearranque), es un entorno para arrancar e instalar el sistema operativo en PCs a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos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

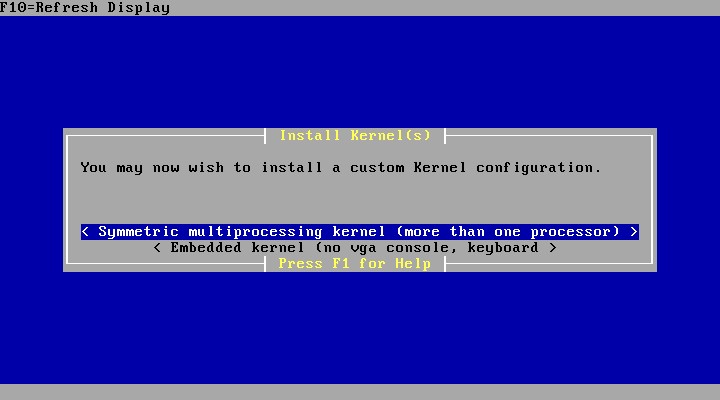
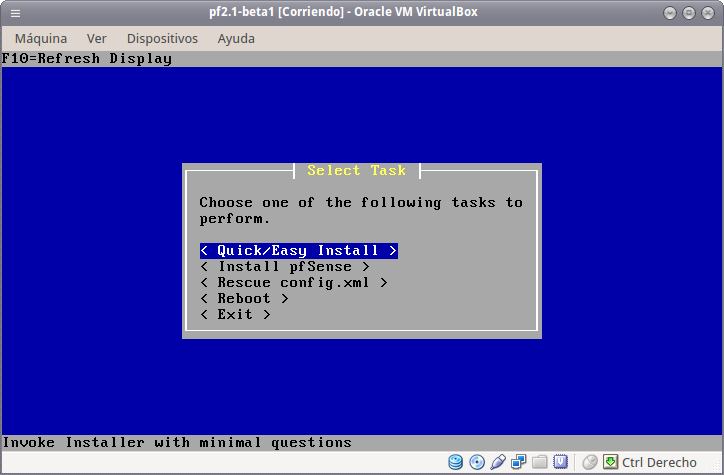
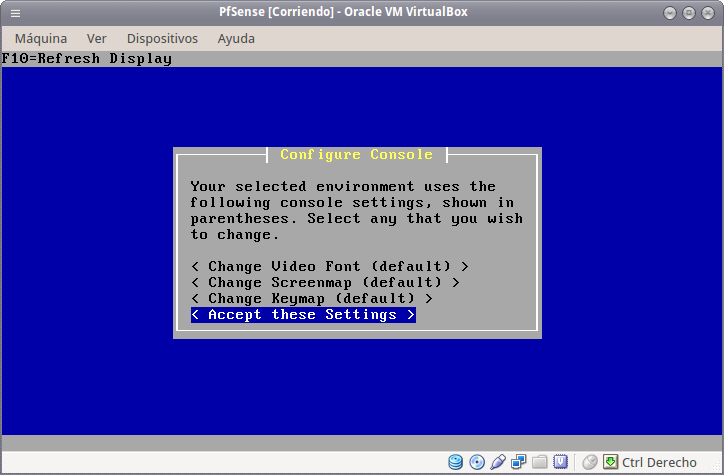
◦ Instalación del PfSense en una máquina con una sola tarjeta de red (mínimo imprescindible tener un WAN)



2ºASIR- Seguridad y Alta Disponibilidad 5/12)

2ºASIR- Seguridad y Alta Disponibilidad 6/12)

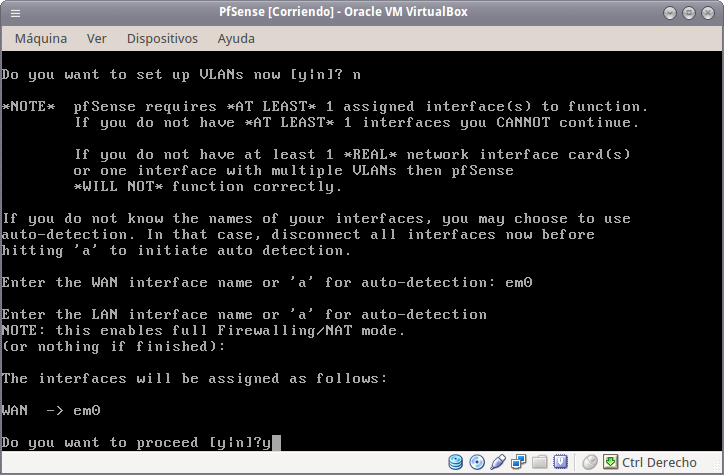
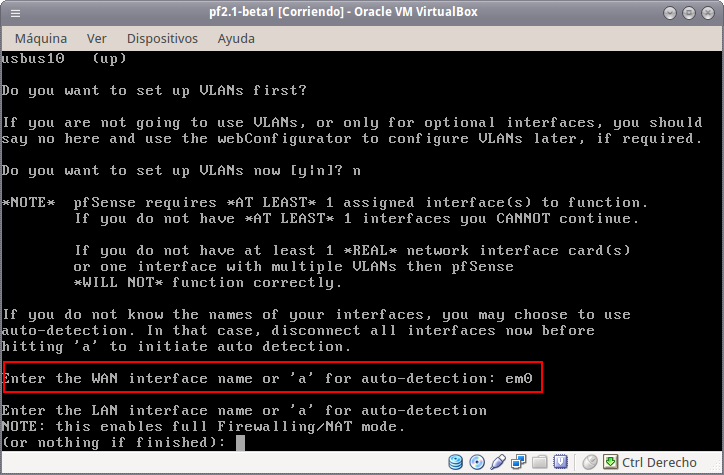
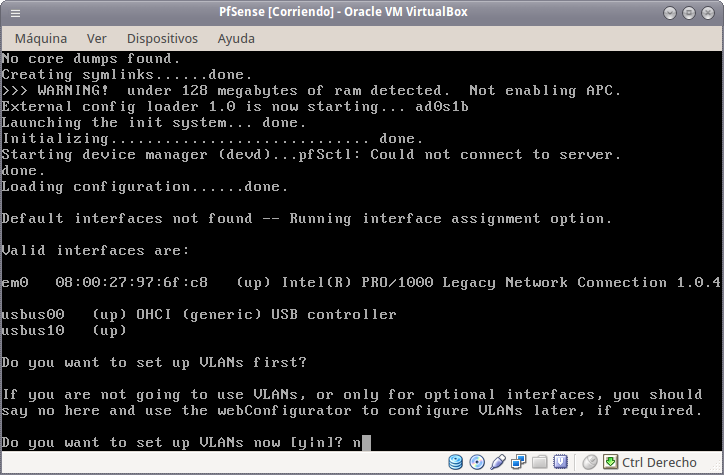
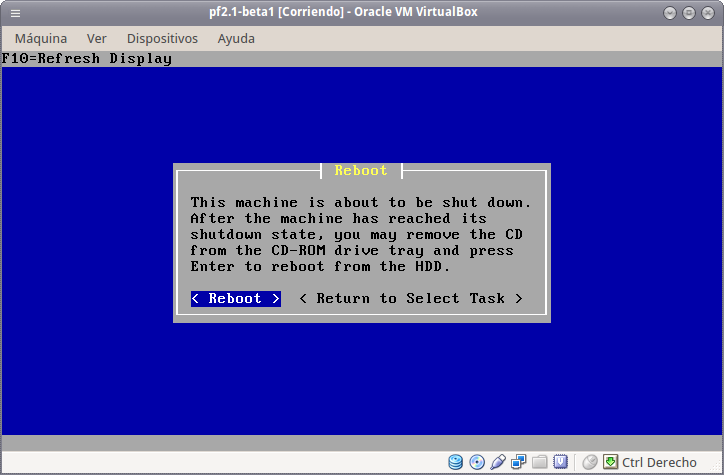
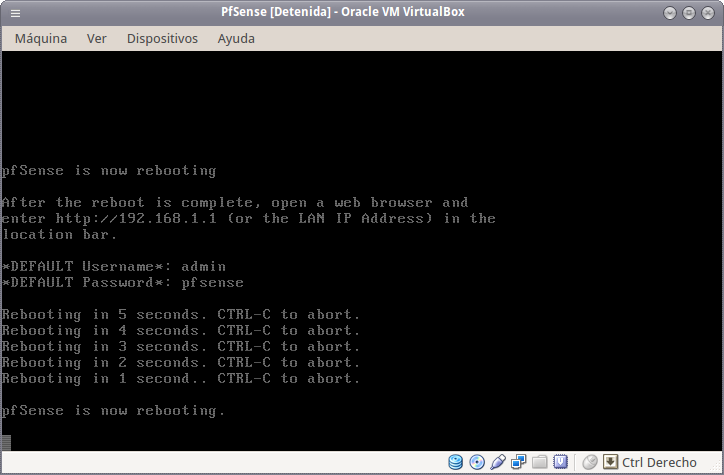
**Tema 2 Segur dad Per metra FW**



2ºASIR- Seg d y lta is li d 7/12)

urida A D ponibi da

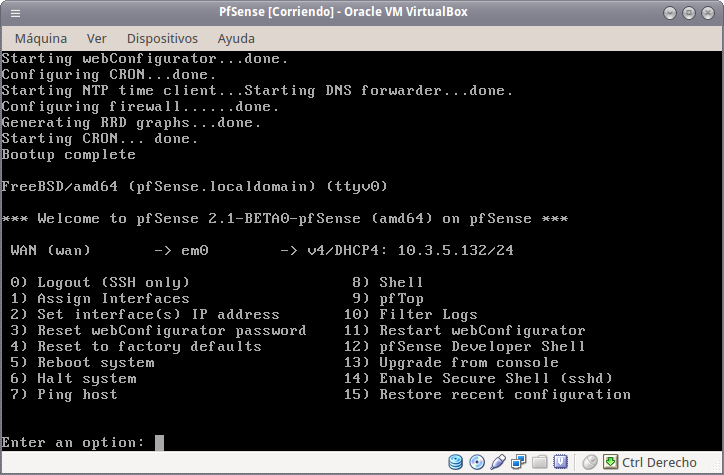
**Tema 2 Segur dad Per metra FW**



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



◦ Captura las imagenes 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

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

◦ Añadiremos la 2º tarjeta de red para la recepción y envio de tramas a/desde la LAN. Añade las capturas correspondientes a la asignación de interfaces y la asignación de IP a la inerfaz recién creada

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

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

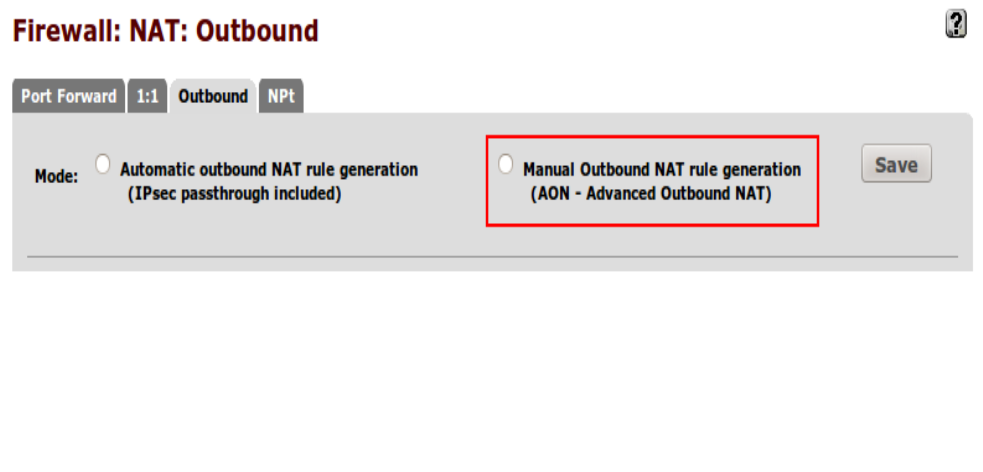
◦ El único usuario que puede gestionar el PfSense es el usuario *admin* que se crea por defecto, create otro nuevo usuario para ti

◦ Captura la pantalla en la que se muestra la tabla de encaminamiento del pf

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

NAT/PortForwarding

Outbound



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

◦ 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

◦ 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 caliene (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](http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica))

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>