Institut Puig Castellar
Santa Coloma de Gramenet

Seguridad en red, cortafuegos y calidad de servicio

Nom estudiants participants
F. Daniel Ibáñez Encinas
Cristian Piqué Orozco

Curs acadèmic
CFGS Administració de Sistemes Informàtics i Xarxes

Data Lliurament
03-06-2016

Llicències alternatives (triar alguna de les següents i substituir la de la pàgina anterior)

A) Creative Commons:

B) GNU Free Documentation License (GNU FDL)

C) Copyright

Resumen del proyecto:

Es importante que un centro educativo cuente con una arquitectura de red segura, que falle lo menos posible y rechace conexiones intrusas y accesos a contenidos inapropiados.

La finalidad de este proyecto es la de realizar un informe y actividad sobre la herramienta de seguridad pfSense, que es una distribución personalizada de FreeBSD, adaptada para su uso como Firewall y Router. Se caracteriza por ser de código abierto y puede ser instalada en una gran variedad de sistemas. Además, cuenta con una sencilla interfaz web para su configuración.

Habrá que ir explicando paso a paso como realizar el proceso de instalación y aprender a utilizar la distribución, realizando pruebas en máquinas virtuales, y poco a poco ir expandiendo las opciones que nos ofrece dicha herramienta. También habrá que realizar una breve introducción sobre los diferentes apartados que intervienen y conceptos teóricos de todos los campos que puedan ser útiles.

Tendremos que ver el funcionamiento de la red del centro educativo y las posibles medidas implementadas en el mismo para garantizar su correcto funcionamiento y seguridad. Posteriormente habría que implementar las acciones oportunas con pfSense y ver si podemos llevarlas a cabo según vaya evolucionando el estado del proyecto.

Índice

1. Introducción

1.1. Contexto y justificación del trabajo

El proyecto propone el estudio de la herramienta pfSense y la implementación de una máquina que pueda mejorar la seguridad y/o calidad de servicio en la red del centro educativo.

Puede ser un proyecto muy interesante, del cual aprendamos bastante, ya que habrá que comprender el funcionamiento de una red y todo lo que le rodea.

1.2. Objetivos del trabajo

- Estudiar los conceptos teóricos que intervienen, así como las herramientas que pueden ayudar a optimizar el rendimiento.

- Comprender las funciones que debe cumplir una red como la de un centro educativo.

- Proponer las herramientas y políticas de seguridad necesarias, que pretendan mejorar el servicio de la red educativa y fortalecer su seguridad.

- Implementar una máquina que cumpla la función proyectada.

1.3. Enfoque y método a seguir

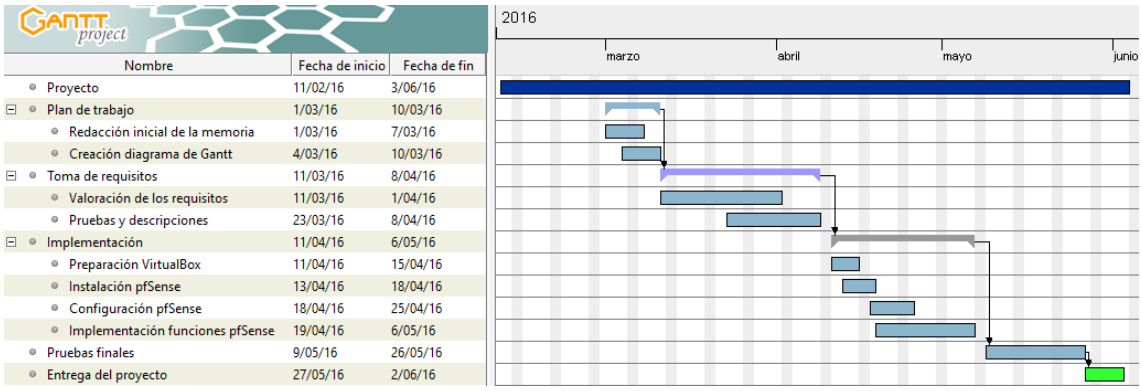
Como inicio, se hará una breve explicación de diferentes conceptos de seguridad y teoría, de todos los aspectos que intervengan en la seguridad.

Será necesario realizar pruebas en máquinas virtuales, para ir conociendo las diferentes características que nos puede aportar la distribución pfSense, hasta poder realizar alguna tarea en un entorno real de trabajo.

Utilizaremos un producto existente, ya que es una distribución creada para realizar de cortafuegos, por lo que la función principal consistirá en implementarla y hacer distintas pruebas.

1.4. Planificación del proyecto

A continuación, veremos toda la planificación del proyecto con un diagrama de Gantt realizado con la aplicación Gantt Project.



Nombre	Fecha de inicio	Fecha de fin
Proyecto	11/02/16	3/06/16
Plan de trabajo	1/03/16	10/03/16
Redacción inicial de la memoria	1/03/16	7/03/16
Creación diagrama de Gantt	4/03/16	10/03/16
Toma de requisitos	11/03/16	8/04/16
Valoración de los requisitos	11/03/16	1/04/16
Pruebas y descripciones	23/03/16	8/04/16
Implementación	11/04/16	6/05/16
Preparación VirtualBox	11/04/16	15/04/16
Instalación pfSense	13/04/16	18/04/16
Configuración pfSense	18/04/16	25/04/16
Implementación funciones pfSense	19/04/16	6/05/16
Pruebas finales	9/05/16	26/05/16
Entrega del proyecto	27/05/16	2/06/16

2. Firewall (cortafuegos)

Muchos de los problemas de seguridad que aparecieron con la interconexión de redes pueden ser remediados o minimizados mediante el uso de determinadas técnicas y controles. Con un **cortafuegos** podemos implementar un nivel de seguridad apropiado permitiendo al mismo tiempo el acceso a los servicios de Internet. Un **cortafuegos** es un sistema o un grupo de sistemas que implementan una política de control de acceso entre dos o más redes, previene el uso y el acceso desautorizado a nuestra red u ordenador.

Todos los mensajes que entran o salen de la Intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados. Podemos imaginarlo como si fuesen dos grandes módulos, uno destinado a bloquear los accesos y el otro a permitirlos. Debemos tener muy claro que tipo de control de acceso debemos implementar.

Un **cortafuegos** nos proporciona un único punto de control que preserva la Intranet del ataque de intrusos. Permite monitorizar la seguridad a través de los logs, que pueden ser revisados periódicamente para poder determinar hipotéticos intentos de acceso. Correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

Existen dos tipos de cortafuegos, por hardware y por software. Los **cortafuegos por hardware** proporcionan una fuerte protección contra la mayoría de ataques que vienen del exterior, son los más utilizados en empresas o grandes organizaciones.

Para usuarios particulares, el cortafuegos más común es un **cortafuegos por software**. Protegerá tu ordenador contra intentos de controlar o acceder a tu máquina desde el exterior, y generalmente proporciona protección adicional contra los troyanos o gusanos más comunes. La desventaja es que protegen solamente al ordenador en el que están instalados y no protegen una red como por hardware.

2.1. Usos frecuentes, problemas y diseños básicos

La desventaja más obvia del uso de **cortafuegos** es que puede bloquear servicios que los usuarios quieran usar, tal como TELNET, FTP, X WINDOWS, NFS (sistema de archivos de red), etc.

De todas maneras este tipo de restricciones no son solo aplicables en los **cortafuegos**, ya que pueden ser implementadas en los hosts localmente. En realidad se debe intentar conseguir un balance que cumpla los requisitos y necesidades de seguridad de los usuarios.

Otro punto a tener muy en cuenta y que en más de una ocasión se deja de lado, es que la configuración de un **cortafuegos** pese a tener muchas ventajas, puede crear un cuello de botella para el tráfico de red.

Cuando se decide instalar un firewall el primer y más importante punto tiene que ver con la política de restricciones aplicable al sistema, por ejemplo todo aquello no especificado se bloquea, esta política pretende que el firewall bloquee todo el tráfico, y las aplicaciones que se deseen dejar pasar deberán ser especificadas individualmente.

Por el otro lado y totalmente opuesto a la primera se encuentra la política de permitir todo aquello que no esté permitido. Esta política supone que el firewall dejará pasar todo el tráfico salvo aquellos servicios que se han considerado peligrosos y que se configurarán caso por caso.

2.2. Tipos de cortafuegos

Como ya comentamos anteriormente, conceptualmente hay dos tipos de firewalls, **nivel de red** y **nivel de aplicación**.

Los cortafuegos de **nivel de red** toman sus acciones en función del origen, la dirección de destino y el puerto en cada paquete IP. Este tipo de firewall tienden a ser muy rápidos y son transparentes al usuario.

Los cortafuegos de **nivel de aplicación** por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una auditoria y logueo del tráfico que pasa a través de él.

Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT, debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original. Este tipo tiende a proveer una auditoría más detallada y un mayor grado de seguridad que los de nivel de red.

Los routers de filtrado de paquetes, que corresponden al primer grupo, toman la decisión dejar pasar o no el paquete que recibe. El router examina cada datagrama para determinar si se aplican sus reglas de filtrado. Las reglas de filtrado se basan en la información contenida en el encabezado del paquete. Esta información consiste en la dirección IP de origen, la IP de destino, el protocolo encapsulado (TCP, UDP, ICMP), el puerto TCP/UDP de origen y de destino, etc. Toda esta información es controlada por las reglas de filtrado definidas, pudiendo ser enrutada si existe una regla que lo permite, descartada si una regla así lo indica y si no existe cualquier otra regla, un parámetro previamente configurado determinará si el paquete pasa o no.

La mayoría de los cortafuegos implementados sobre Internet están desarrollados sobre el concepto de filtrado de paquetes. Este tipo de cortafuegos no son difíciles de configurar debido a que su software contiene una serie de reglas previamente configuradas y fundamentalmente son transparentes al usuario y no exigen instalar ningún software adicional en los hosts.

Por otro lado, cuando se debe personalizar a las aplicaciones específicas de cada empresa, la función se puede hacer algo compleja pues exige una figura de administrador que debe conocer los servicios de Internet, los distintos encabezados de los paquetes y los distintos valores que se espera encontrar en los campos a analizar.

2.3. Arquitectura

Las tecnologías de filtrado de paquetes que se emplean en los **cortafuegos** constituyen una manera eficaz y general para controlar el tráfico en la red. Tales tecnologías tienen la ventaja de no realizar ningún cambio en las aplicaciones del cliente y el servidor, pues operan en las capas IP y TCP, las cuales son independientes de los niveles de aplicación según se establece en el modelo OSI.

3. Calidad del servicio

QoS o calidad de servicio, permiten cubrir los requisitos de servicios de una carga de trabajo o una aplicación al medir el ancho de banda de red, detectar los cambios en las condiciones de red, por ejemplo, congestión o disponibilidad de ancho de banda, y clasificar por orden de prioridad o limitar el tráfico de red.

QoS se puede usar para clasificar el tráfico por orden de prioridad en aplicaciones dependientes de la latencia, como las aplicaciones de streaming de voz o vídeo, y para controlar el impacto del tráfico dependientes de la latencia, como las transferencias masivas de datos.

3.1. Clasificación por prioridad

Identificar correctamente por parte del router el tráfico que nos interesa es una operación vital para luego poder hacer que se le otorgue o no prioridad. Todos los paquetes que cumplen con determinado criterio serán considerados como pertenecientes a un determinada clase de tráfico. La cantidad de criterios que pueden usarse para clasificar e identificar el tráfico dependen de cada router. El tráfico de red está basado siempre en un flujo de paquetes de datos y los clasificadores siempre analizan ciertas características de estos paquetes en forma individual, clasificándolos uno por uno.

Ejemplos de criterios por los que se identifica el tráfico: dirección MAC, IP, o puerto, tanto de origen como de destino, protocolo, tamaño del paquete, SSID, diversas marcas que trae el paquete que le pudieron haber asignado otros sistemas por los que ha pasado previamente, como identificadores de VLAN o de prioridad.

3.2. Acciones

Una vez que el paquete ha sido clasificado, el router le asigna el tratamiento que le hemos configurado para la clase específica del paquete. La principal acción que realiza el router a efectos de controlar el ancho de banda, es asignar el paquete en una de sus colas de salida. Debido a que el ancho de banda de salida del que dispone el router para enviar los paquetes es limitado, lo que hace es planificar la salida obligando a los paquetes a formar diversas filas o colas para poder salir, y todos deben salir por la misma puerta (la cola de transmisión de la interfaz de salida).

Por cada Interfaz de salida, el router tiene predefinidas estas diferentes colas que hace avanzar a distinta velocidad, enviando los paquetes uno a uno, utilizando diversos esquemas de prioridad para cada cola, con lo que logra que los diferentes flujos se muevan a diferente ritmo, en un proceso que tiene por objetivo asignar el ancho de banda escaso a los flujos más privilegiados.

Este proceso es conocido como Gestión del Ancho de Banda y es la parte principal de los sistemas de Quality of Service. En general, la configuración del router nos permite elegir una prioridad para cada clase que definimos y con eso se encarga de meter el paquete en la cola que cumpla nuestra prioridad.

4. ¿Qué es pfSense?

pfSense es una distribución personalizada de **freeBSD** (Sistema Operativo) para usarlo en servicios de redes LAN y WAN tales como cortafuegos, router, servidor de balanceo de carga, etc.

El modelo de desarrollo de **pfSense** es de código abierto, el núcleo de pfSense está basado en el sistema operativo libre llamado BSD, el tipo de núcleo de pfSense es de tipo monolítico, el usado en UNIX.

pfSense cuenta con un gestor de paquetes desde su interfaz gráfica, desde donde se puede acceder remotamente para ampliar sus funcionalidades, al elegir el paquete deseado el sistema lo descarga y lo instala automáticamente.

Existen 60 módulos disponibles para descargar e instalarlos, entre ellos los más comunes son el proxy squid, IMinspector, Snort, ClamAV entre otros.

No es necesario tener conocimientos avanzados sobre línea de comandos de BSD para la utilización de pfSense, ya que casi todo funcionará a través de una interfaz gráfica bastante amigable de cara al usuario final.

4.1. Requisitos de hardware

Para la instalación de pfSense los requisitos de hardware son:

CPU:	RAM:
Mínimo: 500Mhz	Mínimo: 256 MB
Recomendado: 1Ghz o más	Recomendado: 1GB o más

Contar con dos o más tarjetas de red.

4.2. Ventajas e inconvenientes

Como puntos a favor dispone de una interfaz web muy atractiva y totalmente funcional, muchas funciones entre las que destacan: OpenVPN, 'Wake-On-Lan', implementación del protocolo de Calidad de Servicio (permite establecer prioridades según que tipo de tráfico, por ejemplo, telefonía) y es compatible con VLAN a nivel de interfaz (si las tarjetas de red lo son).

Además, permite instalar paquetes creados por desarrolladores externos, pero diseñados específicamente para pfSense e integrados totalmente con su interfaz de administración, como por ejemplo, un sistema de detección de intrusos activo.

Como puntos en contra, al ser una distribución muy joven y activa, el sistema no tiene una buena documentación. De hecho, la mayoría de las funcionalidades no están documentadas y hay que acudir a foros y a tutoriales de usuarios avanzados para tener un conocimiento amplio de la configuración

4.3. Funcionalidades

Firewall: pfSense se puede configurar como un cortafuegos permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.

Servidor PPPoE:

Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, de forma local o mediante radius.

Redundancia:

pfSense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primario.

Monitorizar: A través de un gráfico, pfSense muestra el estado de los siguientes componentes:

-Utilización de CPU y rendimiento total

-Estado del cortafuegos

-Rendimiento individual por cada interfaz

-Paquetes enviados y recibidos por cada interfaz

-Manejo de tráfico y ancho de banda.

5. Introducción a guía de pfSense

En esta guía que a continuación presentamos como parte del proyecto de ASIR, trataremos la instalación, configuración e implementación de la distribución pfSense. La misma, es una distribución UNIX basada en FreeBSD y enfocada al mundo de la Seguridad Informática, permitiendo implementar en cualquier PC un router y un cortafuegos. Este entorno, es completamente imprescindible en cualquier lugar en el que se requiera un conexión a Internet garantizando una mínima seguridad en la misma.

Puede ser que detrás de una conexión a Internet, haya un hogar normal y corriente, pero también puede que haya una empresa, la cual tenga todos sus datos en Internet. En este último caso, es importante ofrecer una buena seguridad a la empresa, por todos estos motivos es importante que cualquier conexión a la red este totalmente securizada.

Para montar la infraestructura necesaria para nuestro propósito, podemos proceder de muchas maneras. La más lógica, sería pensar en montar nuestro router y cortafuegos en una máquina física, que conectada en el resto de la red cumpliera sus funciones. Esta opción, sería completamente viable y funcional sin problemas, pero hoy en día y debido a la revolución de las TIC, cada vez más se empieza a prescindir de lo físico para transportarlo a la red. En el mundo de los Sistemas Operativos, esta técnica se llama "virtualizacion". La misma, consiste en montar todos nuestros servicios en una máquina que no es real, pero que se comporta como tal. Escogiendo esta opción, haremos que el trabajo hecho hoy se pueda seguir manteniendo a lo largo de muchos años.

Para empezar con la virtualización, deberemos escoger una plataforma donde llevarla a cabo. Existen muchas empresas con soluciones de virtualización, la más conocida sea Oracle con VirtualBox. Así que es la que utilizaremos, porque a la hora de implementar el proyecto en otras máquinas o migrarlo, será más sencillo de hacer.

VirtualBox es una solución de virtualización, totalmente libre e integrada en GNU/Linux. Permitiendo que sea soportada por cualquier distribución, lo que nos da una gran libertad a la hora de escoger un Sistema Operativo para ejecutar nuestros servicios. Una vez visto que es la virtualización y la plataforma más conocida para ejecutarla, pasamos a ver la distribución que tendrá nuestra guía, la cual se dividirá en varios puntos, que recogerán los diversos pasos necesarios.

En el primer paso hablaremos sobre los componentes necesarios para instalar VirtualBox, y un breve resumen de su instalación. Una vez instalado, tocará configurar el programa, así como crear las máquinas virtuales. Es decir, el entorno donde se ejecutarán nuestros servicios.

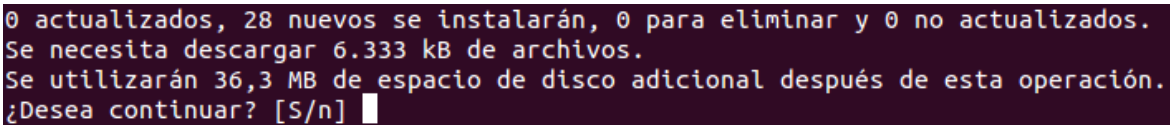
Una vez esté toda la solución de virtualización montada, instalaremos en la máquina virtual correspondiente la distribución pfSense. A partir de aquí nos quedará realizar la configuración inicial y puesta en marcha.

Una vez instalado y configurado pfSense, estaremos en condiciones de empezar a implementar nuestras funciones. Para ello, tendremos que acceder a través de su interfaz web y empezar a configurarlo.

Por último, nos quedará implementar las funciones que vayamos necesitando. Será un camino largo, pero lo importante es que acabe saliendo bien. Espero que encontréis interesante esta guía.

5.1. Instalación del entorno de virtualización (VirtualBox)

Para iniciar el proyecto, lo primero a realizar será instalar VirtualBox desde los repositorios de Ubuntu. Desde el terminal ejecutaremos el siguiente comando “sudo apt-get install virtualbox”.

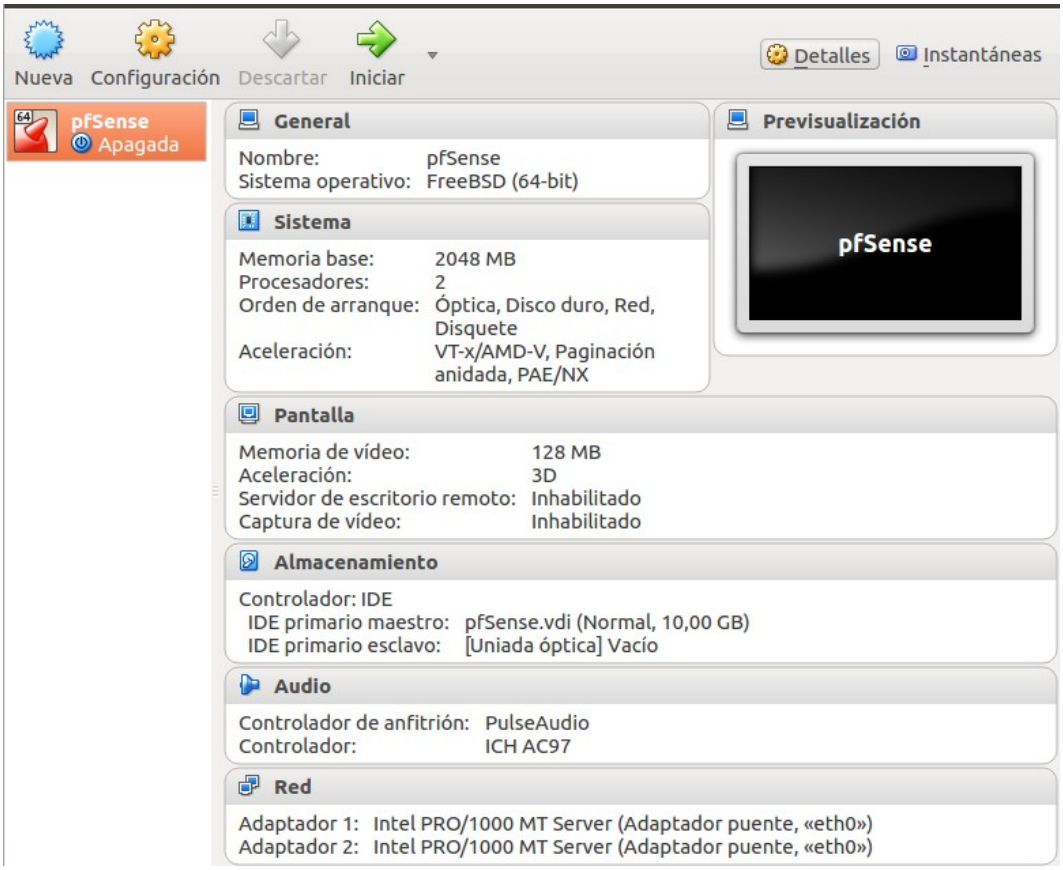


5.2. Configuración del entorno y creación de máquinas virtuales

Una vez instalado VirtualBox, vamos a proceder a crear la máquina virtual que utilizaremos en el proyecto. Pulsaremos en Nuevo donde nos abrirá el asistente de creación.

Primeramente, elegimos el nombre de la máquina y el Sistema Operativo. En nuestro caso, la máquina se llamará “pfSense” y el Sistema Operativo FreeBSD. A continuación, asignaremos la cantidad de memoria RAM para la máquina y disco duro. Para configurarlo, iremos a “Crear disco duro nuevo” e indicaremos el tamaño del mismo.

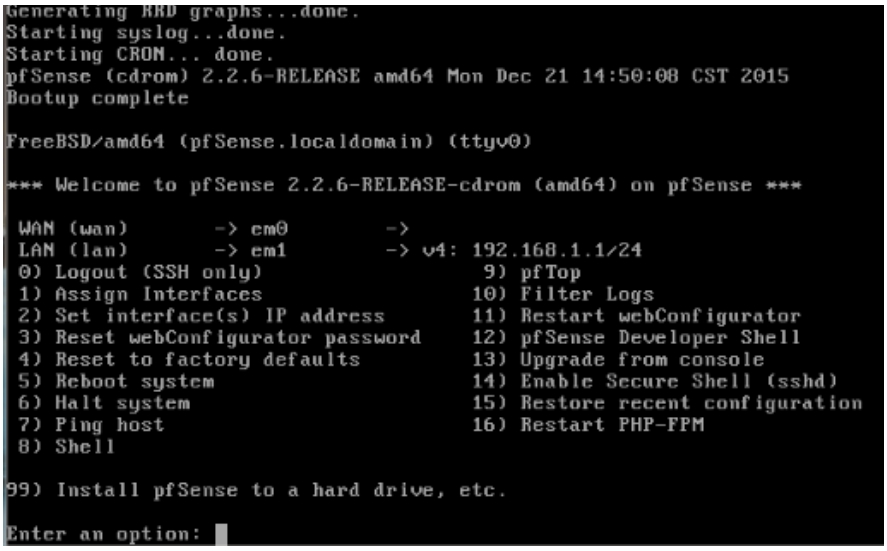
Con la máquina creada, antes de comenzar deberemos ajustar la red y la ISO a arrancar. La red la configuraremos con dos, tres o cuatro tarjetas en modo puente. La primera, que dará salida a Internet y el resto que servirá a los clientes para conectarse a la red. A continuación, para cargar la ISO en la máquina virtual, accederemos al menú de disco duro y en la unidad de CD-ROM seleccionaremos la ISO de pfSense descargada anteriormente.



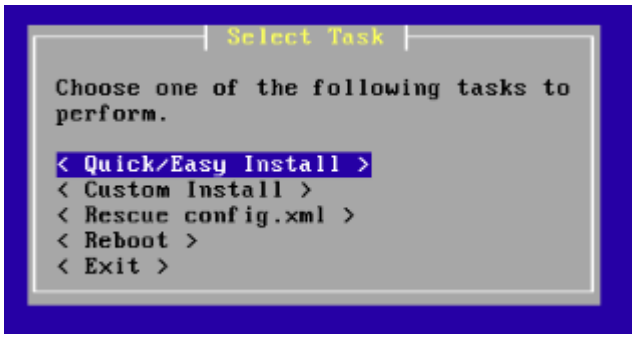
5.3. Instalación de pfSense

Una vez preparada y configurada la máquina virtual, procederemos a instalar pfSense. Así que lo primero a realizar, será arrancar la máquina virtual con la ISO de pfSense y nos mostrará la pantalla inicial.

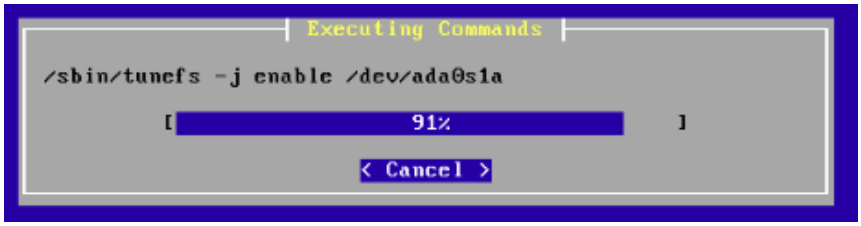
Aquí vemos la pantalla principal, donde nos muestra las diferentes opciones de arranque. Para iniciar pulsaremos 1, ya que el resto de opciones, están reservadas a la configuración de pfSense. Una vez arrancado, accederemos al menú principal, desde donde podremos comenzar la instalación.



Como vemos en la imagen, hemos accedido al live cd, por lo que ahora procederemos a arrancar la instalación, ya que las otras opciones, las configuraremos una vez instalado el sistema. Para arrancar la instalación, pulsaremos la tecla 99.



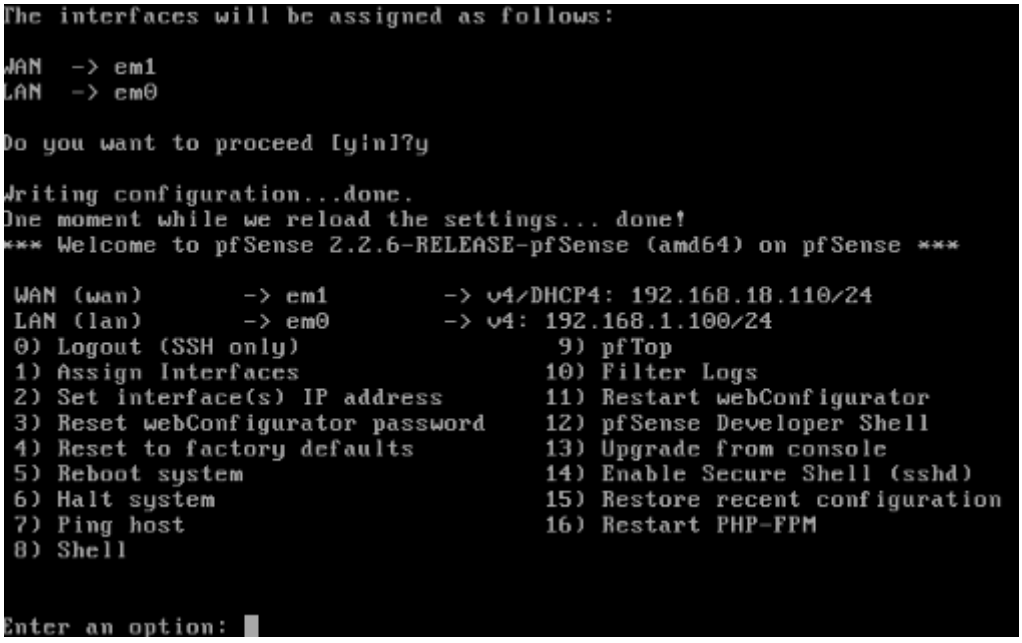
Accederemos al menú de instalación y para comenzar a instalar, pulsaremos “Quick/Easy Install”.



Como observamos a continuación, nada mas pulsar "Quick/Easy Install" comenzará el proceso de instalación y en pocos minutos tendremos el sistema instalado. Este sistema está pensado para funcionar en diferentes tipos de máquinas, por lo que el kernel, nos dará la opción de embeberlo o usar el estándar. Como no tenemos una máquina embebida, usaremos el estándar.

Una vez hecho este paso, ya podemos salir del Live CD para arrancar el sistema, por lo que le daremos a la opción de reinicio. Al reiniciar, será necesario pulsar F1 para comenzar el arranque del sistema, ya instalado en nuestro disco duro.

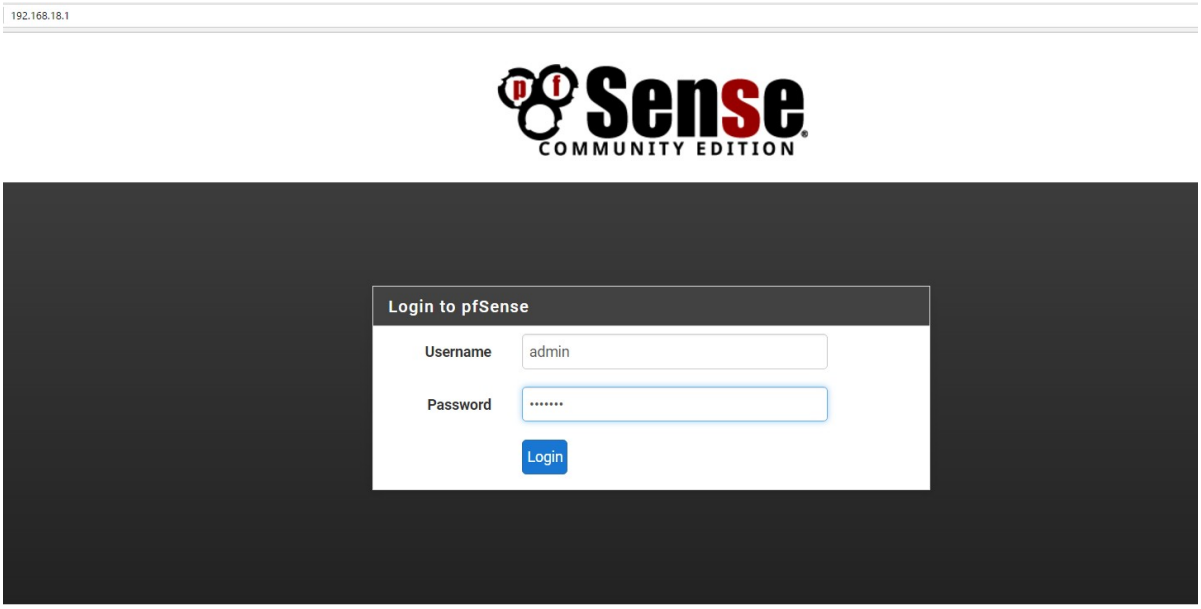
5.4. Configuración inicial y puesta en marcha de pfSense



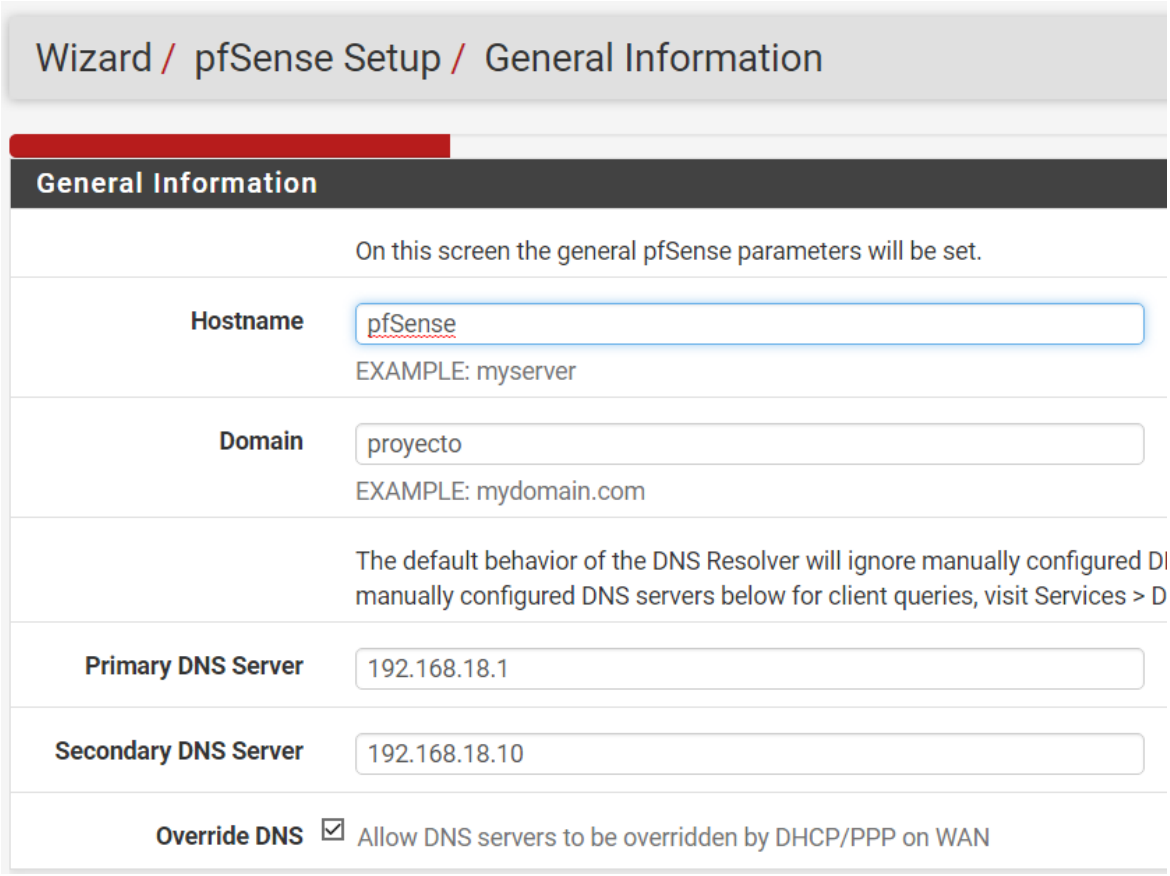
Como en el caso del Live CD, volvemos a la pantalla inicial, pero ahora trabajamos con un sistema instalado. Por defecto, la configuración de red la hace automáticamente, pero en caso de ser necesario, la podemos adaptar a nuestras necesidades con las opciones 1 y 2 del menú respectivamente. Una vez llegados a este punto ya está todo listo. Para continuar el proyecto, accederemos a la IP de pfSense, desde donde accederemos al sistema y a todas sus opciones.

5.5. Acceso Web a pfSense

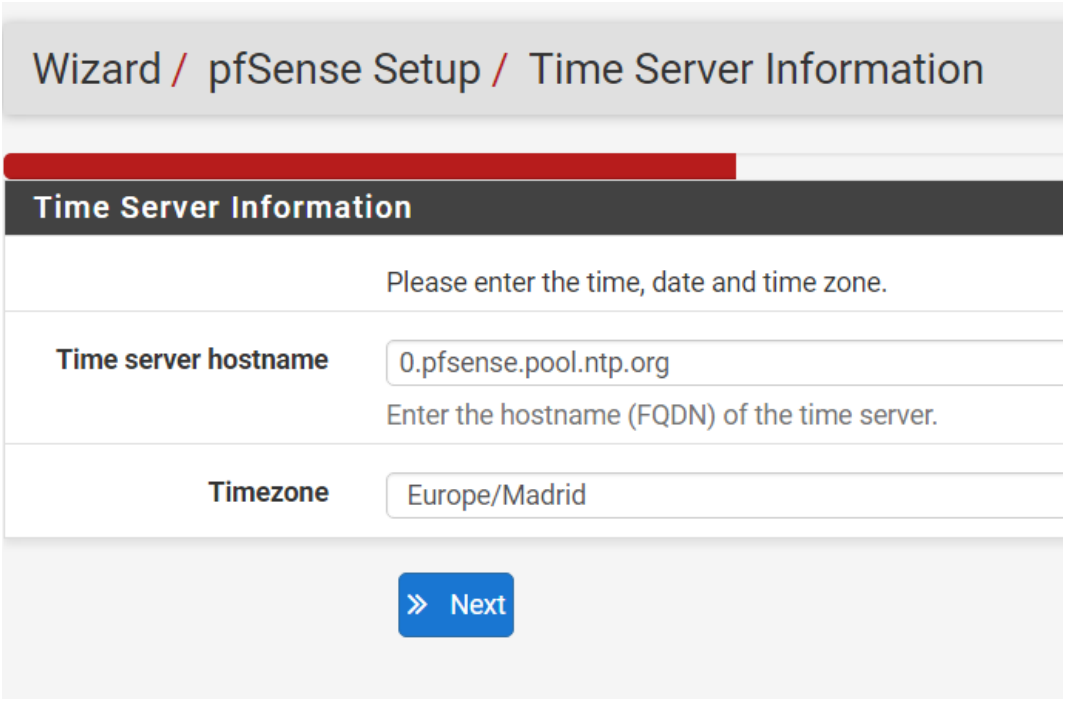
Accederíamos mediante navegador utilizando la puerta de enlace asignada a nuestra LAN de pfSense. Luego la cambiaremos a la red 18 y activaremos el resto de interfaces.



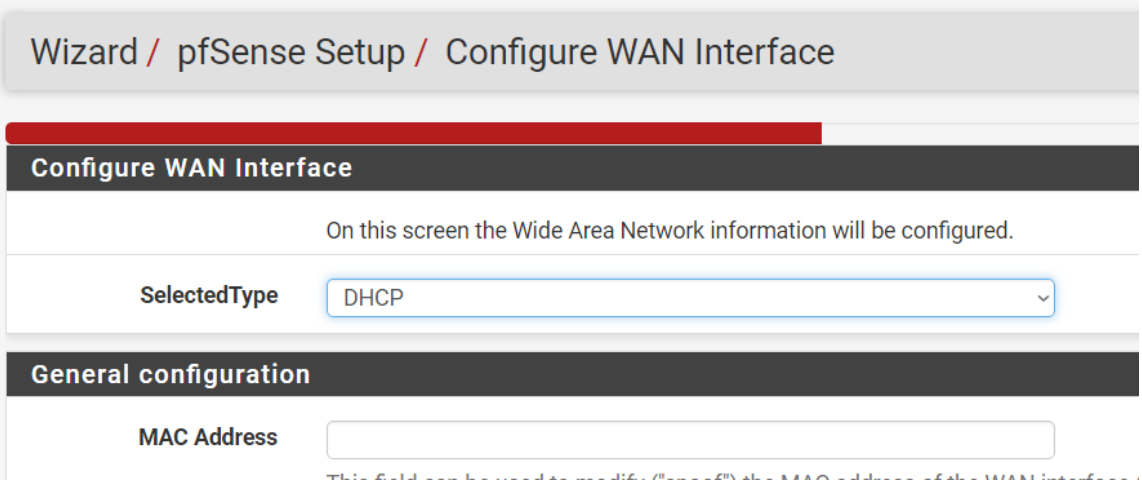
Por defecto el usuario es admin y la contraseña “pfsense”. Dentro accederemos al asistente de configuración inicial. El cual, dejará pfSense listo para trabajar.



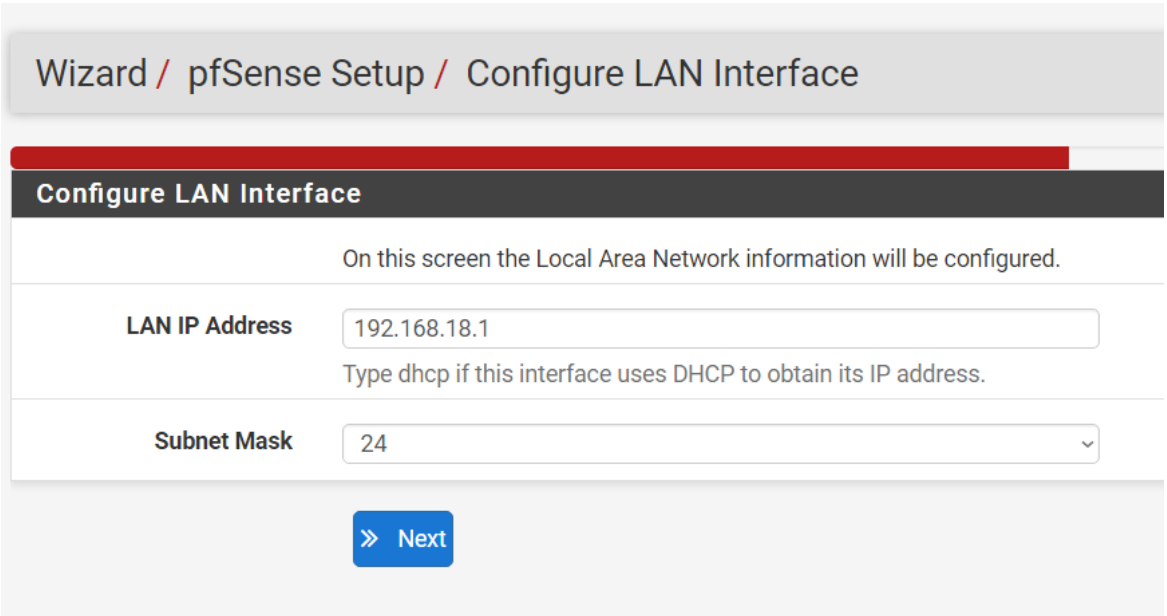
Lo primero a configurar, será el nombre de la máquina, que podemos poner el que queramos y el dominio DNS de la misma en caso de ser necesario. El siguiente paso, es configurar los DNS, pudiendo elegir entre nuestra máquina virtual o los del propio centro.



El siguiente paso es configurar la hora, debido a que estamos implementado un servidor, es recomendado utilizar un servidor NTP, así tendremos siempre la hora correcta. Podemos elegir el que queramos, hacemos clic en "Next" y continuamos configurando.



En esta pantalla, deberemos configurar el tipo de conexión que tendrá cada una de las dos tarjetas que disponemos. La tarjeta WAN es la que ofrece la salida a Internet, así que la configuraremos en modo DHCP. Para que sea el servidor de la red el que nos de la dirección IP de salida a Internet. En cambio, la tarjeta LAN que ofrece acceso a los clientes y a la red, la configuraremos de manera estática, para que se pueda acceder siempre a la red y a todos los servicios de la misma.



Deberemos configurar la IP de la LAN. Por defecto viene la 192.168.1.1, la cambiaremos por 192.168.18.1. En un entorno real, debería estar una red diferente a la WAN.

5.6. Implementación de pfSense en un entorno de pruebas

Una vez finalizado el asistente anterior, ya podemos acceder completamente a pfSense. Por lo tanto, lo que tendremos que realizar a partir de ahora, serán pruebas para comprobar la efectividad de pfSense, en una máquina real de la LAN del centro.

La primera prueba que realizaremos, sera comprobar el funcionamiento del firewall. Para ello, configuraremos una regla que bloquee el acceso a Internet de una máquina de la LAN. Ejecutaremos los siguientes comandos para asegurarnos que nuestra máquina pasa por el cortafuegos.

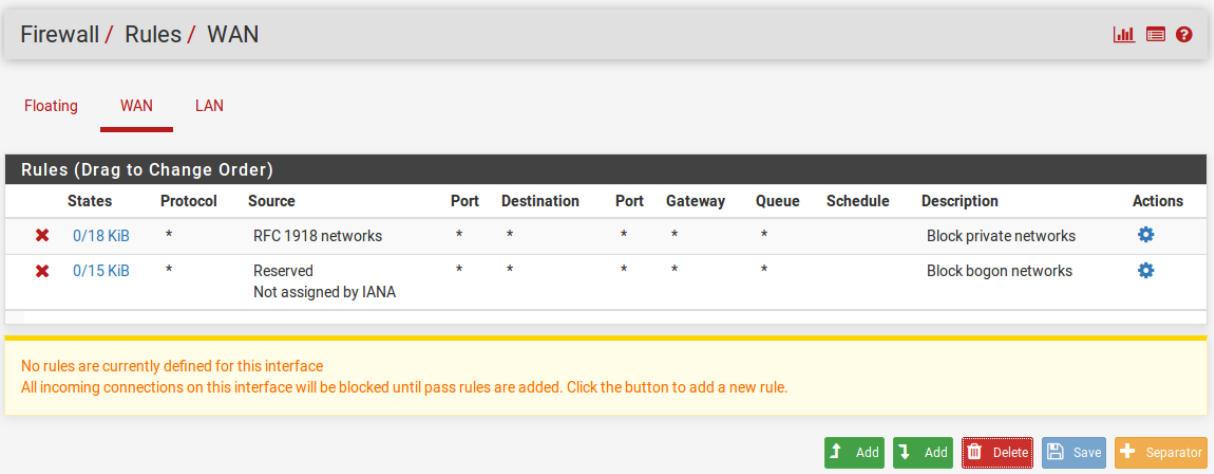
- sudo ifconfig eth0 192.168.18.220 (ip asignada al host)
- sudo route add default gw 192.168.18.215 (puerta de enlace, también tenemos 192.168.18.1 en nuestras pruebas)
- sudo route del default gw 192.168.18.10 (si fuese necesario borrar la predeterminada)
- route -n (para comprobar que esté todo correcto)

```
root@usuari-HP:/home/usuari# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.18.215  0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.18.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.18.10   0.0.0.0         255.255.255.255 UH    100    0        0 eth0
```

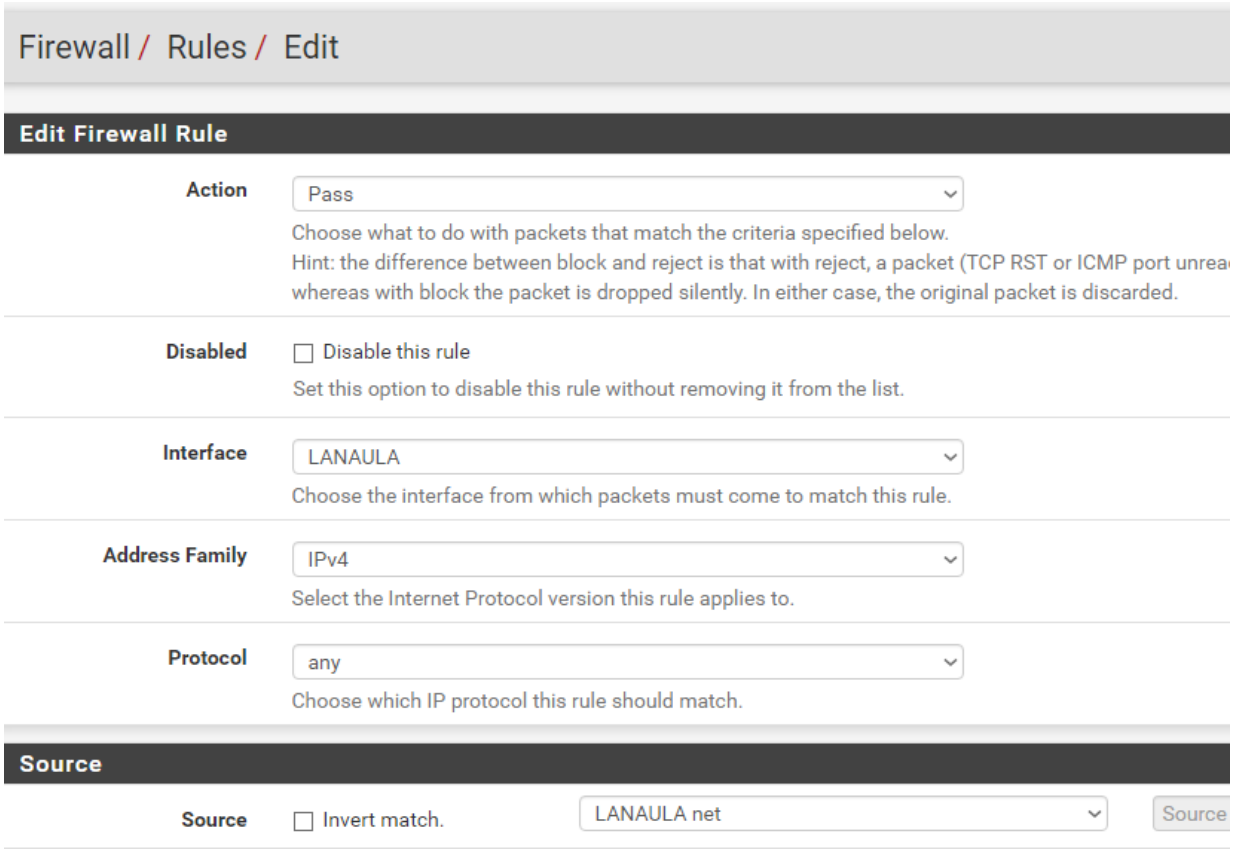
Una vez ejecutados estos comandos, como podemos comprobar en la tabla de rutas, nuestro router para la red y para Internet, es nuestra maquina pfSense. Así que ahora, ya podemos empezar con la primera prueba, que consiste en verificar el funcionamiento del cortafuegos.

Para configurar el cortafuegos, iremos al menú “Firewall”, allí están todas las opciones relacionadas con el mismo. Como la configuración de NAT, QoS, o las reglas del firewall y las IP Virtuales.

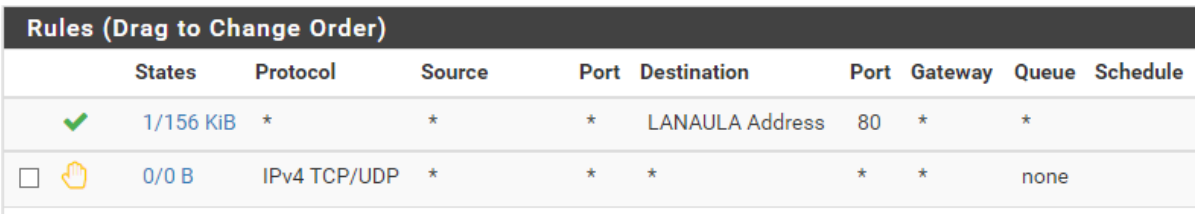
En este caso, para probar el cortafuegos, usaremos las reglas, las cuales permiten regular el tráfico de la red. Así que vamos al menú Firewall y a la opción “Rules” y vemos la siguiente pantalla.



Para configurar la regla, lo primero que debemos hacer es elegir a que interfaz la aplicaremos. Primero daremos acceso a la red a WAN y después haremos lo propio con la interfaz LAN, así que hacemos clic en una de las interfaces y accederemos a la pantalla de las reglas, que es idéntica a la mostrada en la captura de arriba. Pulsaremos en Add para acceder a la pantalla de configuración de la regla que permita el tráfico por ellas.

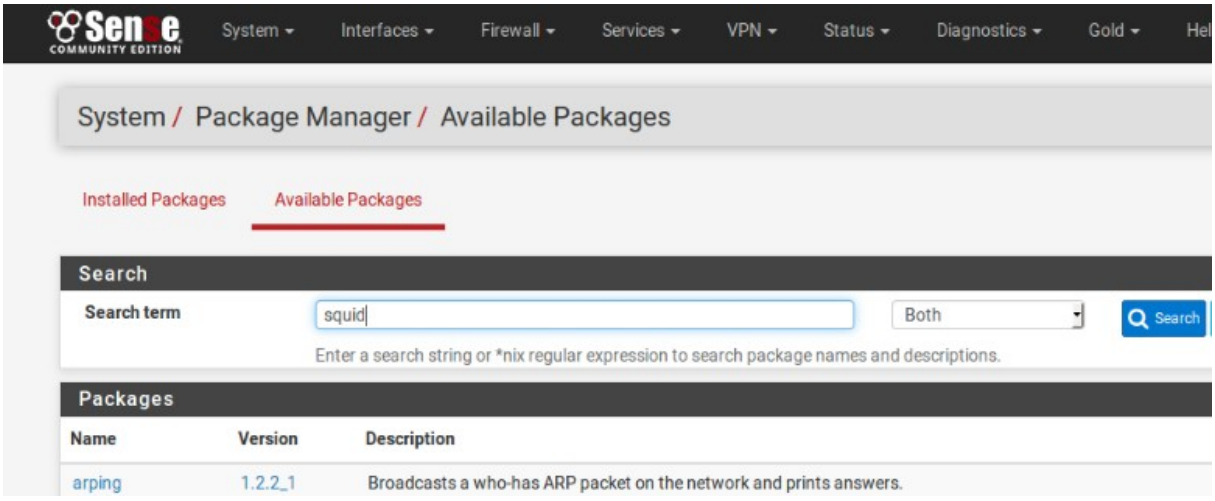


Una vez permitido el tráfico, vamos a hacer una prueba bloqueando el mismo de la interfaz LAN creando una nueva regla. Debemos elegir entre si queremos bloquear o rechazar el paquete, la diferencia entre ambos es que si bloqueamos, el paquete se descarta directamente sin ningún mensaje, y si rechazamos se generará un mensaje de rechazo. Se puede bloquear tanto la interfaz completa como un equipo en concreto asignando una IP, pulsaremos en salvar y aplicar para observar los cambios.

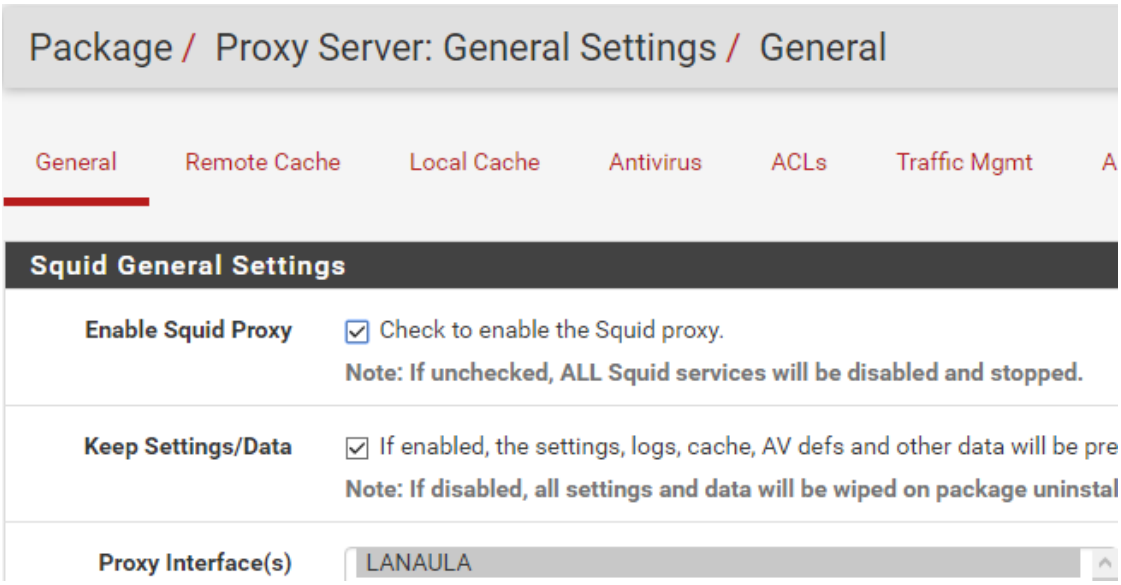


Con la nueva regla, la máquina física ya no puede acceder a Internet, tal y como vemos en la siguiente captura:

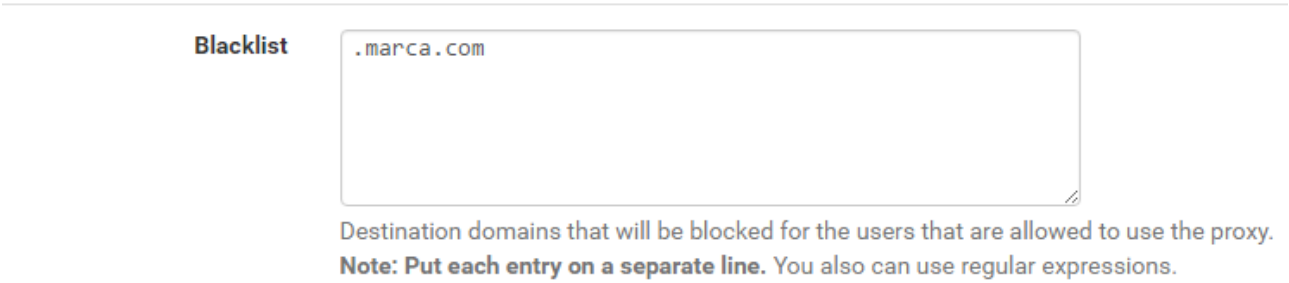
Una vez comprobado que el bloqueo funciona correctamente, volvemos a activar Internet e instalaremos el módulo squid desde "System/Package/Manager/Available Packages", con el que bloquearemos una página web concreta, en nuestro caso la web del diario Marca. Squid es un servidor proxy web caché, que nos ayudará a mejorar el rendimiento de las conexiones o añadir seguridad realizando un filtrado de tráfico.



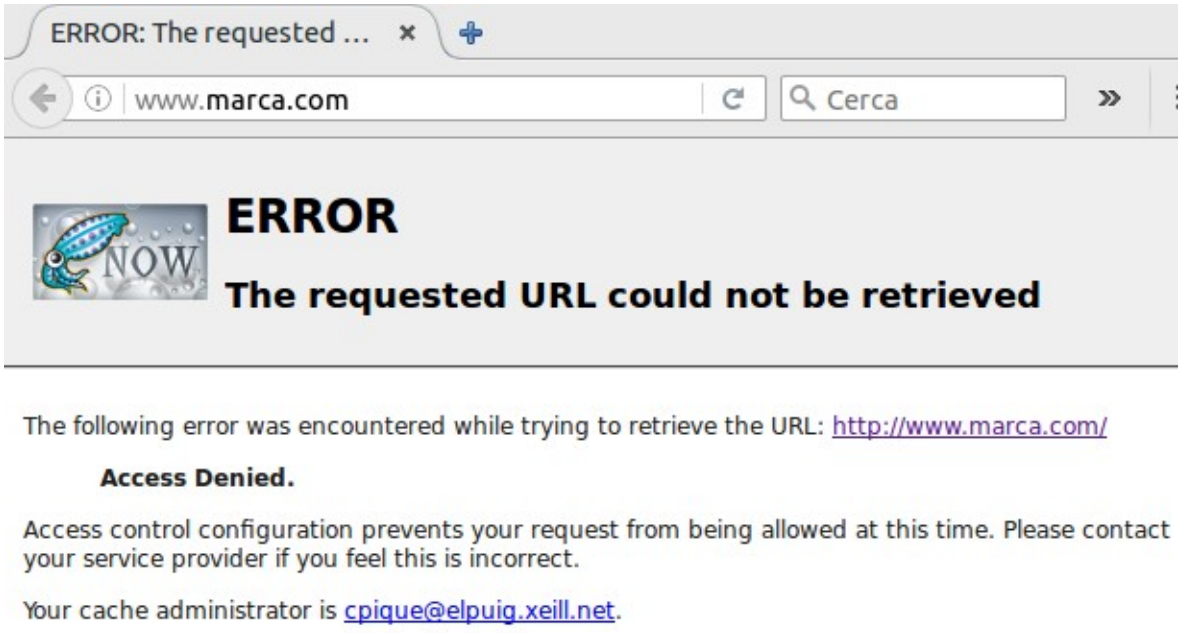
Después de instalar y activar squid, en “Services/Squid Proxy Server” haremos el bloqueo anteriormente comentado.



En ACLs añadimos la web de marca en la lista negra:



Al acceder a marca nos informará del bloqueo:



The following error was encountered while trying to retrieve the URL: http://www.marca.com/

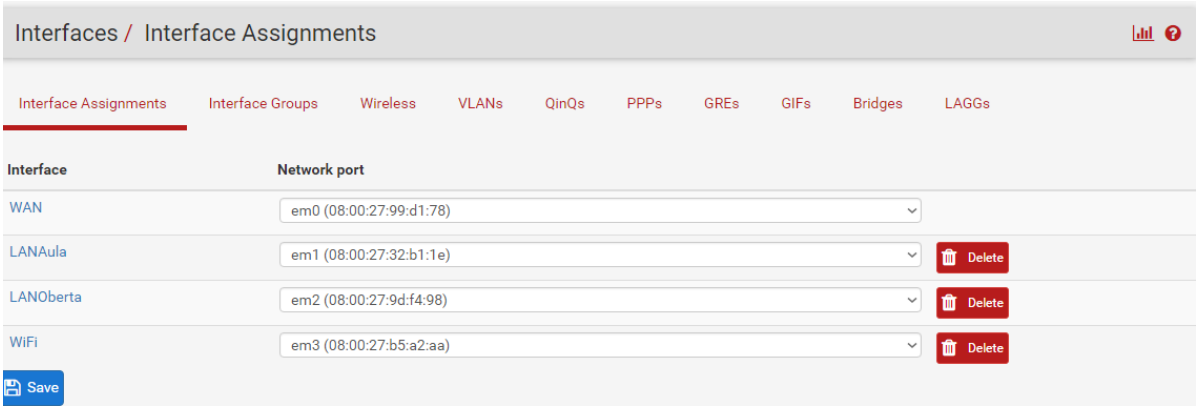
Access Denied.

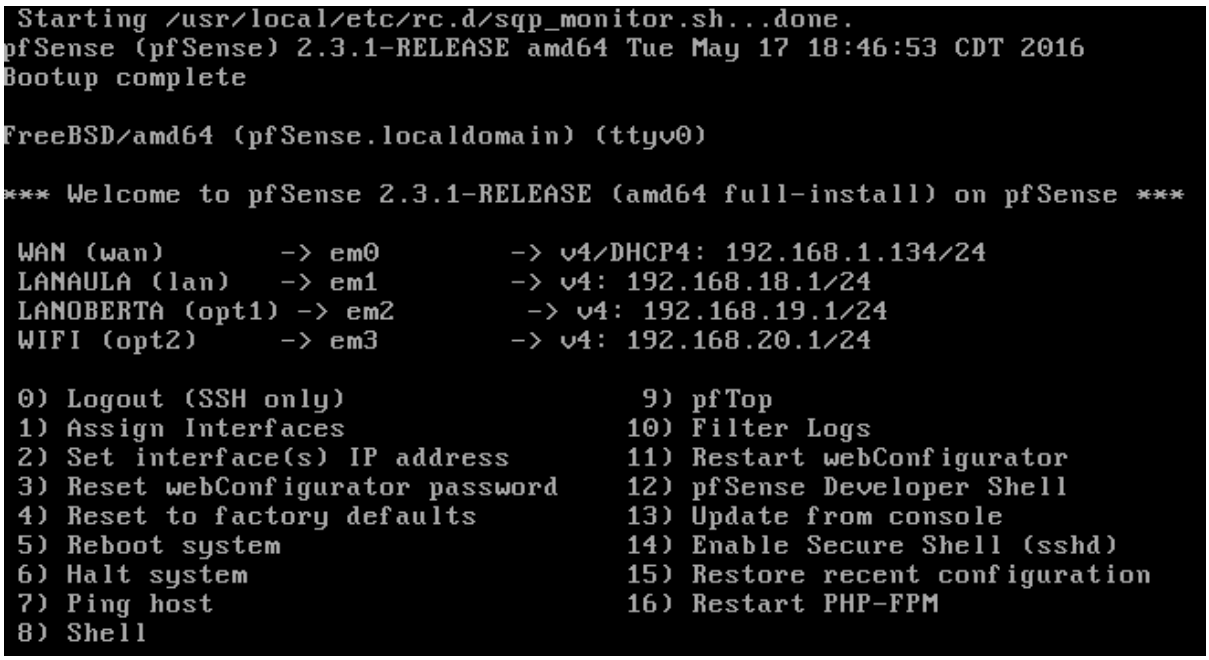
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is cpique@elpuig.xeill.net.

5.6.1. Asignación de Interfaces

Una vez realizadas algunas pruebas, añadimos dos interfaces más, la que teníamos ahora como LAN pasará a llamarse LanAula, y tendremos dos nuevas llamadas LanOberta y WiFi, la primera sin las restricciones del Aula, y la segunda para quien acceda mediante WiFi.





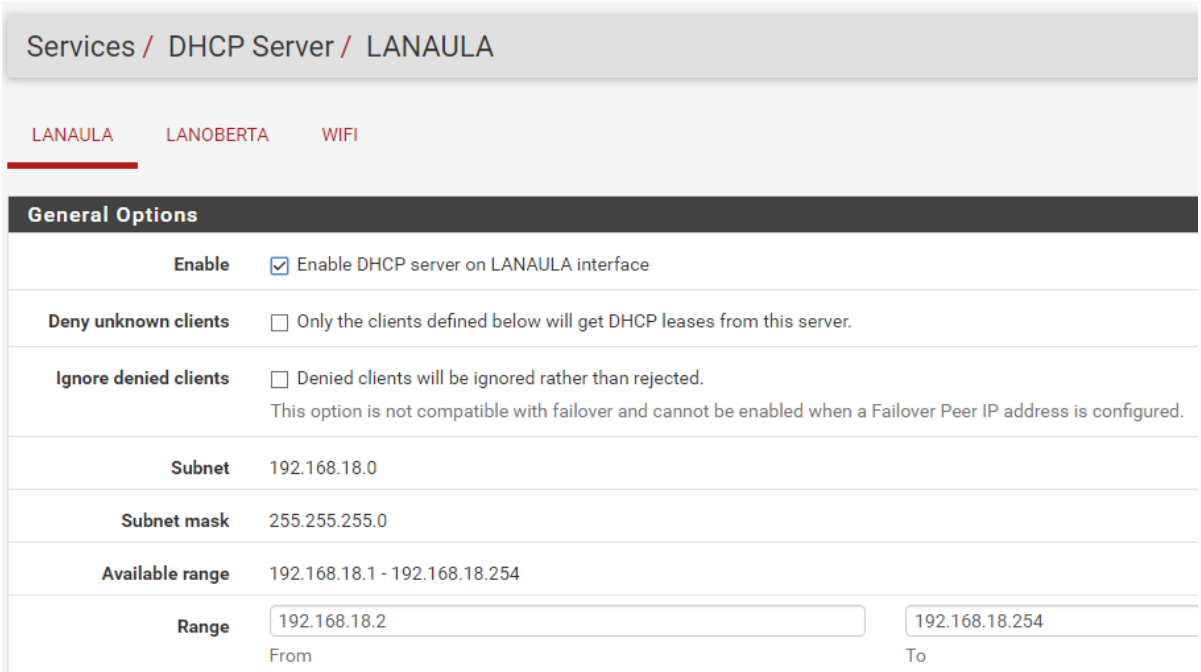
5.6.2. Activar el servicio DHCP

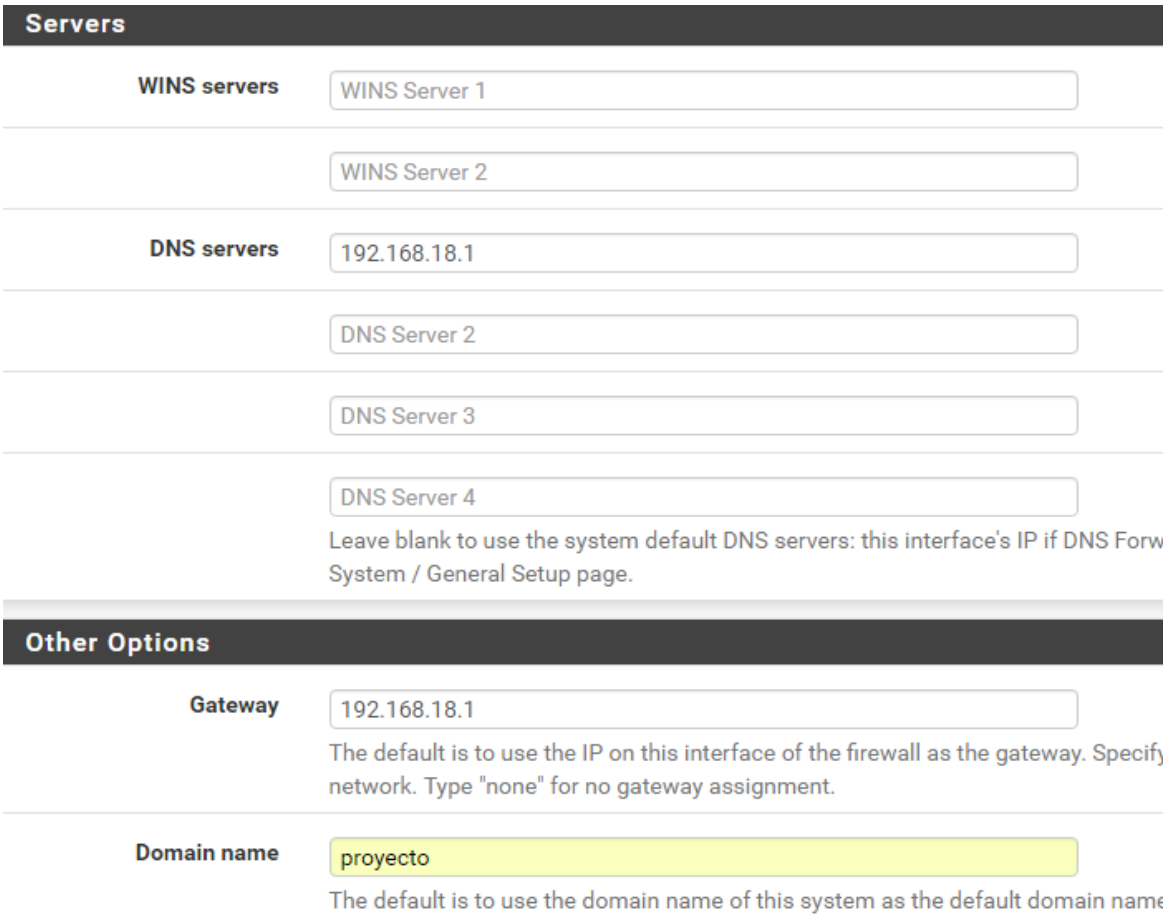
Servicio DHCP (Dynamic Host Configuration Protocol)

Es un servidor que usa un protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

Emplearemos DHCP en la interfaz LANAula, de esta manera el equipo se conectará automáticamente sin tener que asignarle la IP de forma manual.

Hay que activar la casilla “Enable DHCP server on LAN interface” desde “Services/DHCP Server”, asignar el rango de ips que el servidor otorgará y guardar los cambios.




Servers
WINS servers
WINS Server 1
WINS Server 2
DNS servers
192.168.18.1
DNS Server 2
DNS Server 3
DNS Server 4
Leave blank to use the system default DNS servers: this interface's IP if DNS Forw
System / General Setup page.
Other Options
Gateway
192.168.18.1
The default is to use the IP on this interface of the firewall as the gateway. Specify
network. Type "none" for no gateway assignment.
Domain name
proyecto
The default is to use the domain name of this system as the default domain name

5.6.3. Activar el servicio DNS

DNS (Domain Name Server):

Es una tecnología basada en una base de datos que sirve para **resolver nombres** en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder.

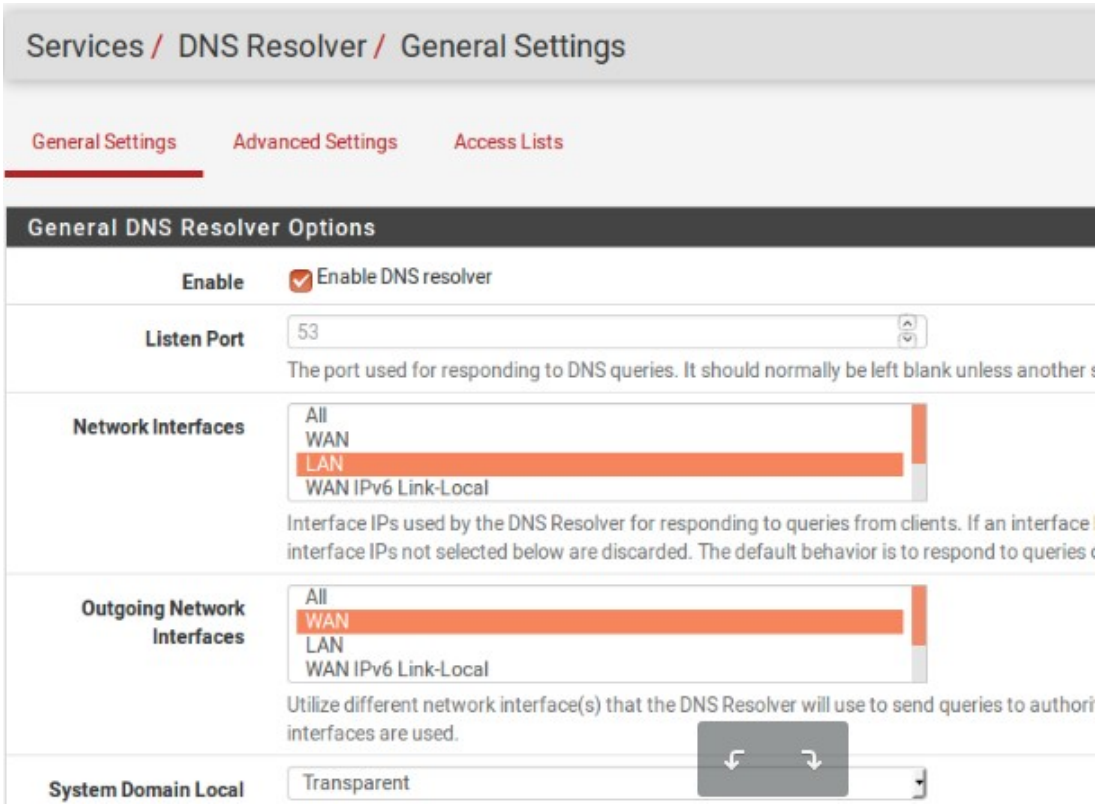
Cuando un ordenador está conectado a una red (ya sea Internet o una red casera) tiene asignada una dirección IP. Si estamos en una red con pocos ordenadores, es fácil tener memorizadas las direcciones IP de cada uno de los ordenadores y así acceder a ellos pero ¿qué ocurre si hay miles de millones de dispositivos y cada uno tiene una IP diferente? Pues que se haría imposible, por eso existen los dominios y las DNS para traducirlos.

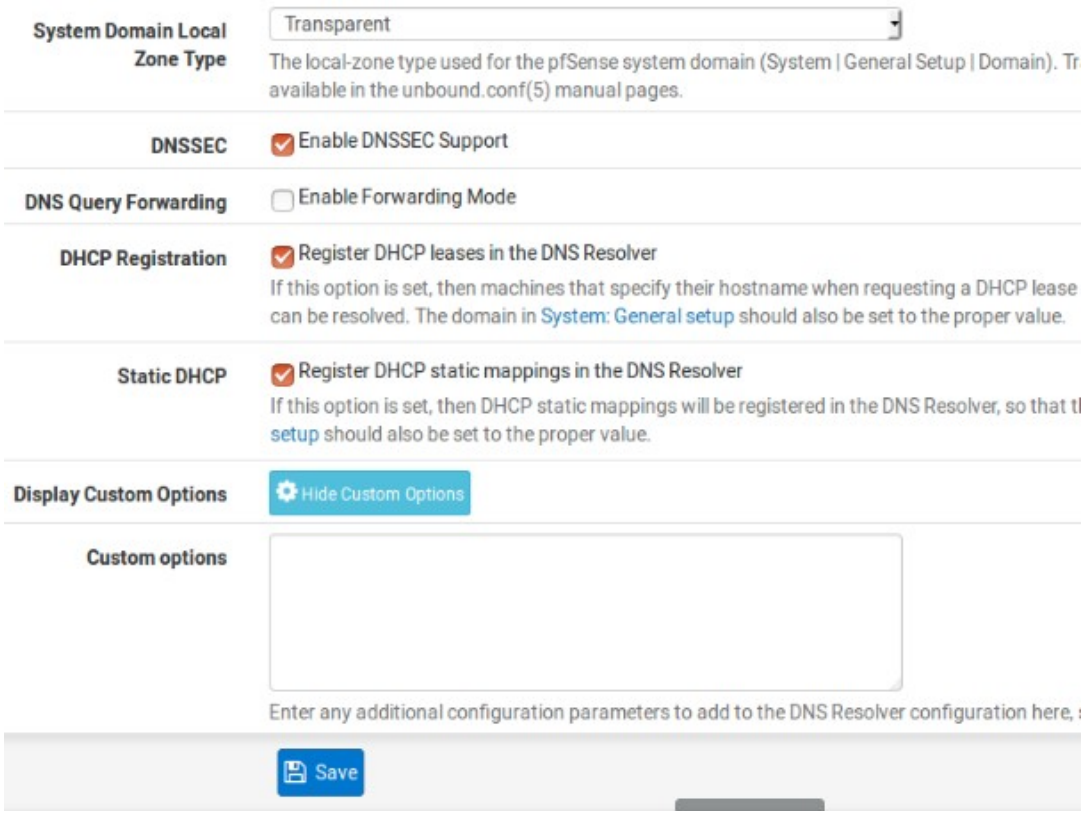
Por lo tanto, el DNS es un sistema que sirve para traducir los nombres en la red, y está compuesto por tres partes con funciones bien diferenciadas.

- **Cliente DNS**: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.
- **Servidor DNS**: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión.
- **Zonas de autoridad**: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org).

Desde “Services/DNS Resolver/General Settings” y activamos el DNS que incorpora pfSense, además le diremos que haga las asignaciones que realice el DHCP de pfSense.

Al emplear el DHCP de pfSense, las máquinas verán el cortafuegos como su servidor de nombres y su puerta de enlace.

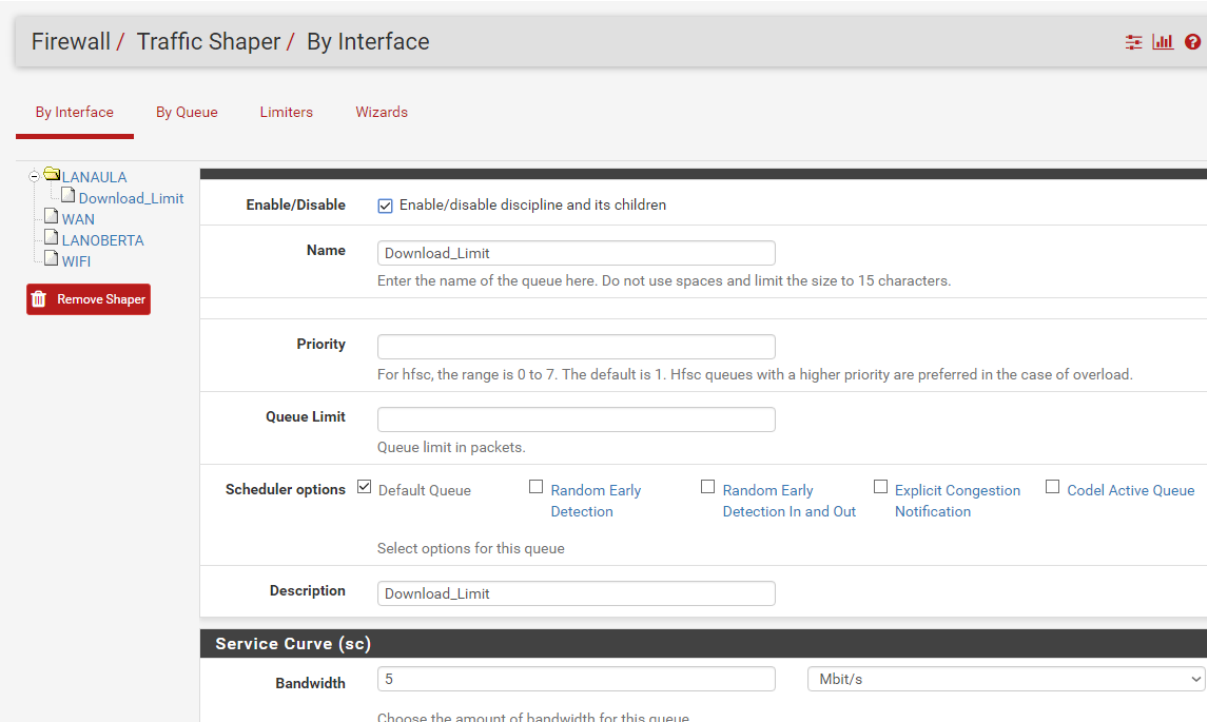




5.6.4. Limitación del ancho de banda de forma manual

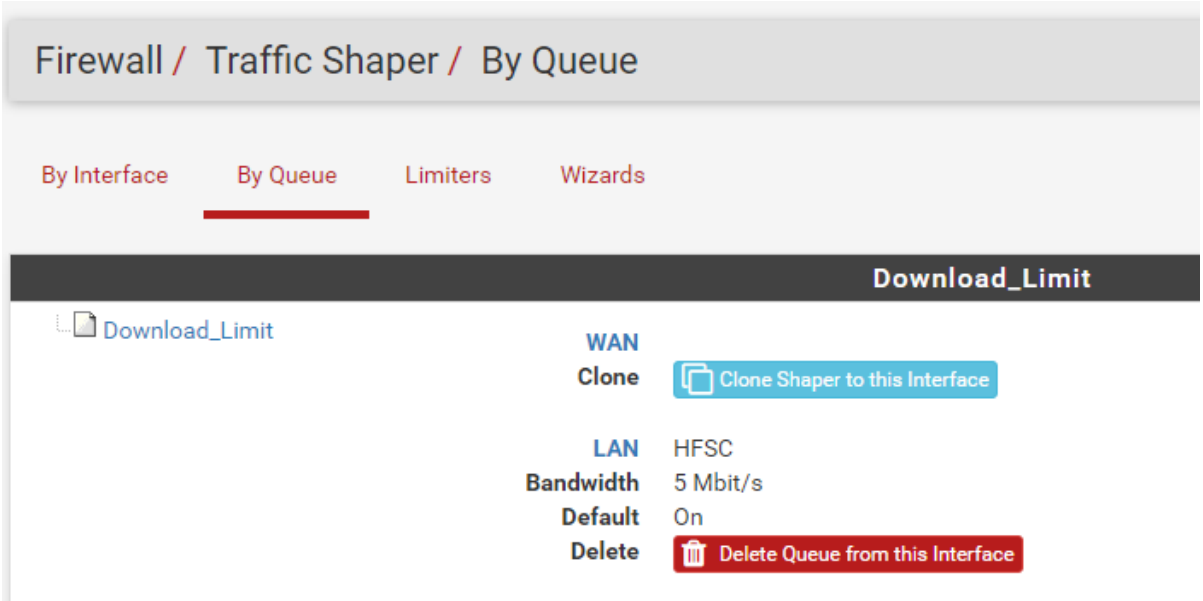
Para no saturar el ancho de banda del centro, crearemos unas restricciones para limitar el ancho de banda dentro de una red. En este caso vamos a hacer la prueba de limitarlo a 5 MB/s de forma general.

Para crear la regla, en nuestra máquina pfSense tendremos que ir a “Firewall/Traffic Shaper” y en “By Interface/LAN” configuraremos una restricción llamada Download_Limit donde el ancho de banda estará limitado a 5 MB/s, pulsaremos en LAN, pondremos la restricción y salvamos, acto seguido se pulsará en añadir cola o bien al salvar se añadirá automáticamente.



También desde aquí, se puede configurar el ancho de banda mínimo y máximo por cada cola.

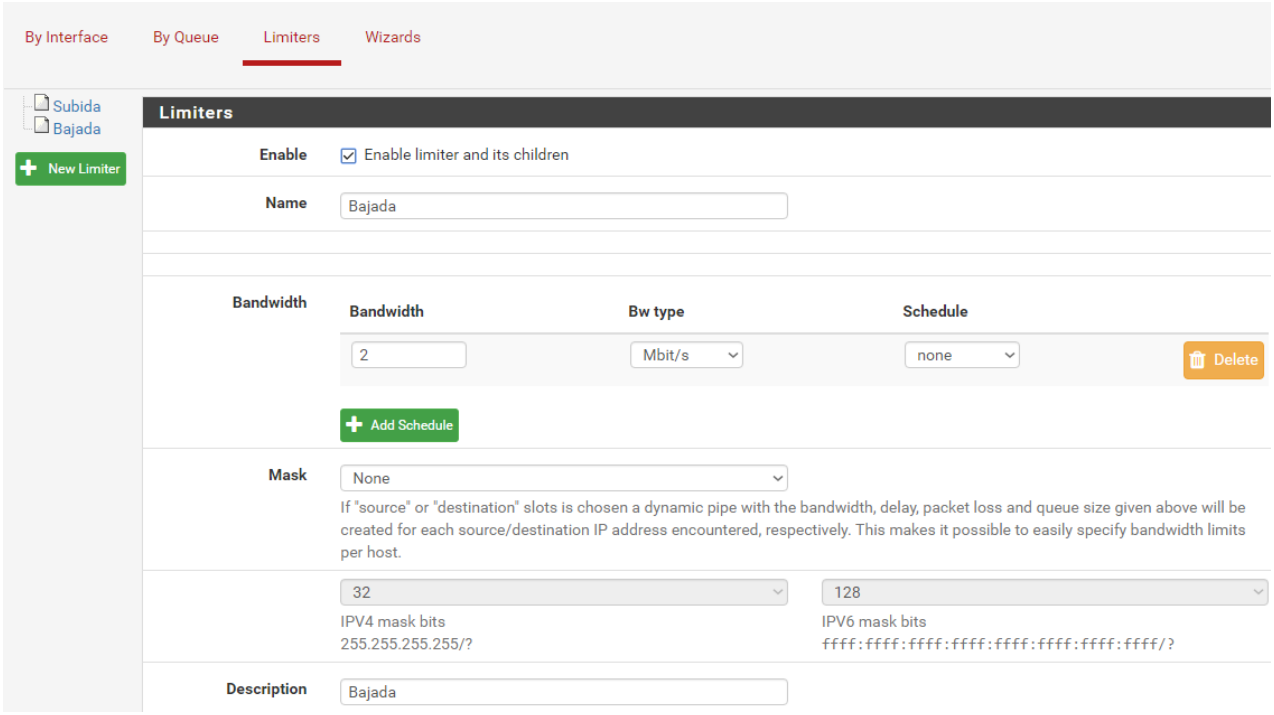
En By Queue nos mostrará si hay colas configuradas en el sistema:

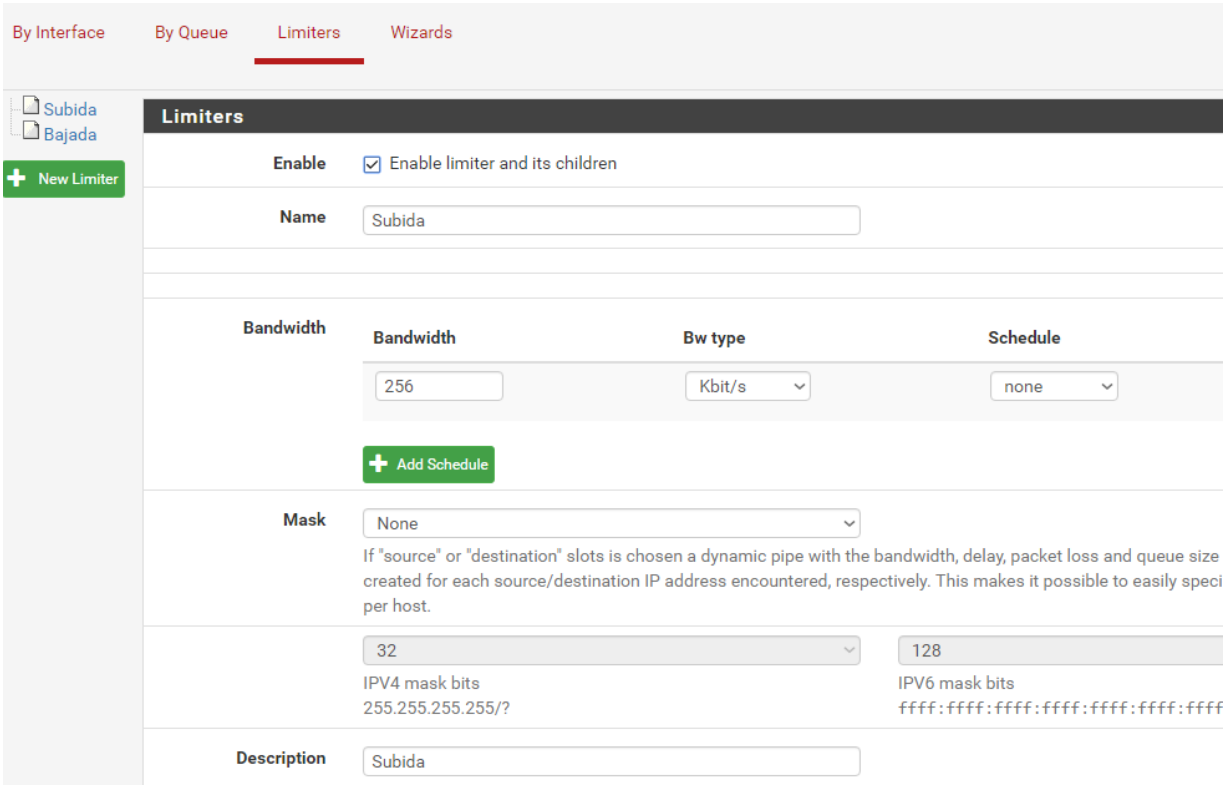


También se pueden crear Limiters, que servirán para limitar tanto la subida como la bajada, ya de forma más particular y como complemento al límite general que tenemos establecido en 5MB/s.

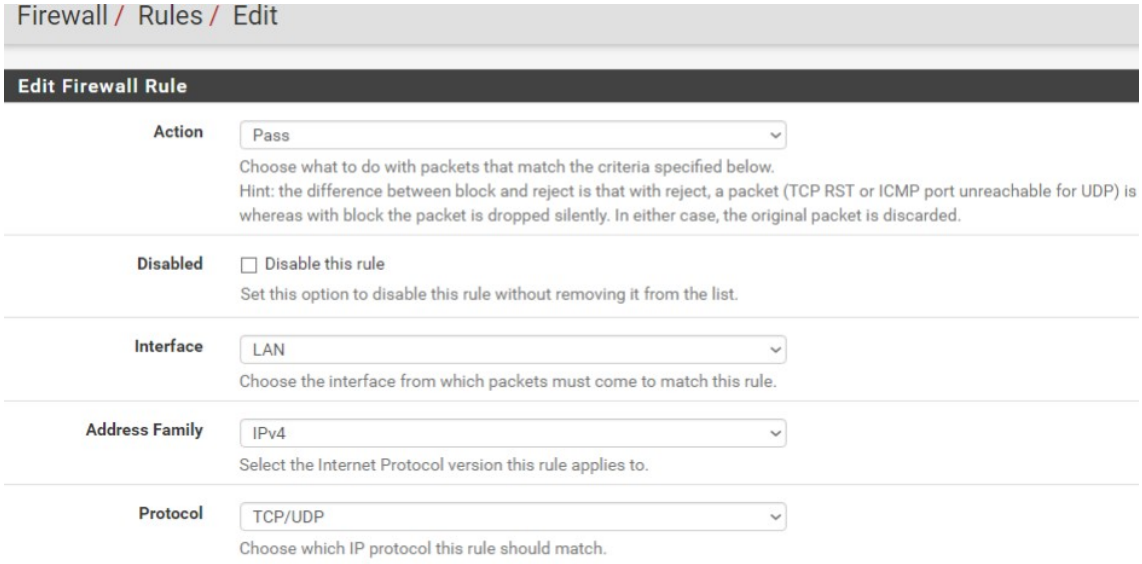
En Limiters pulsaremos en New Limiter y crearemos el límite de la cola de descargas.

Creamos un límite de 2 MB/s de bajada y 256Kb/s de subida, por ejemplo:

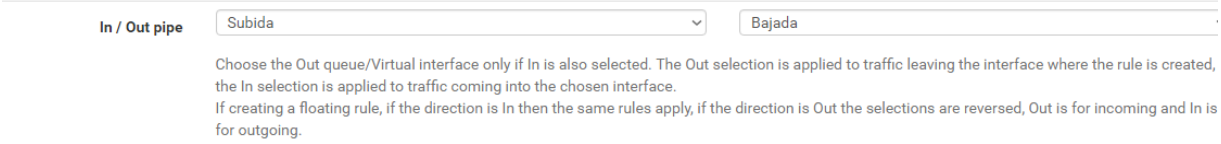




Y pulsaremos en salvar. Acto seguido tendremos que ir a Firewall/Rules y crear una nueva regla para aplicar dichos límites en la interfaz que creamos conveniente.



En In/Out pipe seleccionamos nuestros dos limiters personalizados de Subida/Bajada y salvamos.



Una vez aplicado el límite, haremos la prueba con un medidor de velocidad para comprobar si se han establecido tal como los habíamos configurado:

Podemos observar que se ha respetado tanto el límite de bajada de 2MB/s como el de subida de 256Kb/s.

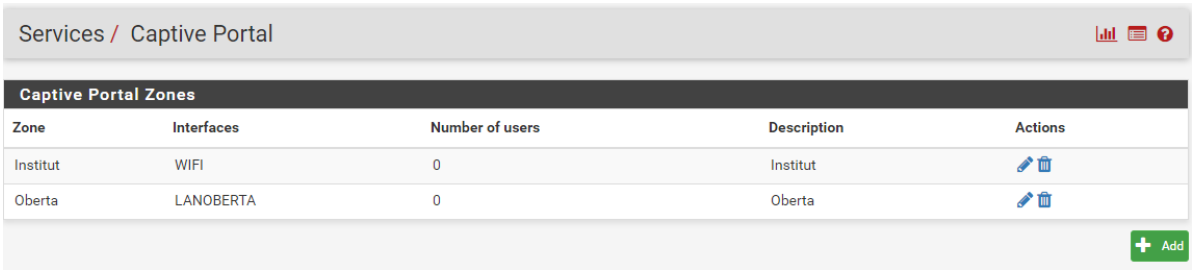
5.6.5. Portal Cautivo

Un **portal cautivo** es un programa o máquina de una red informática que fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

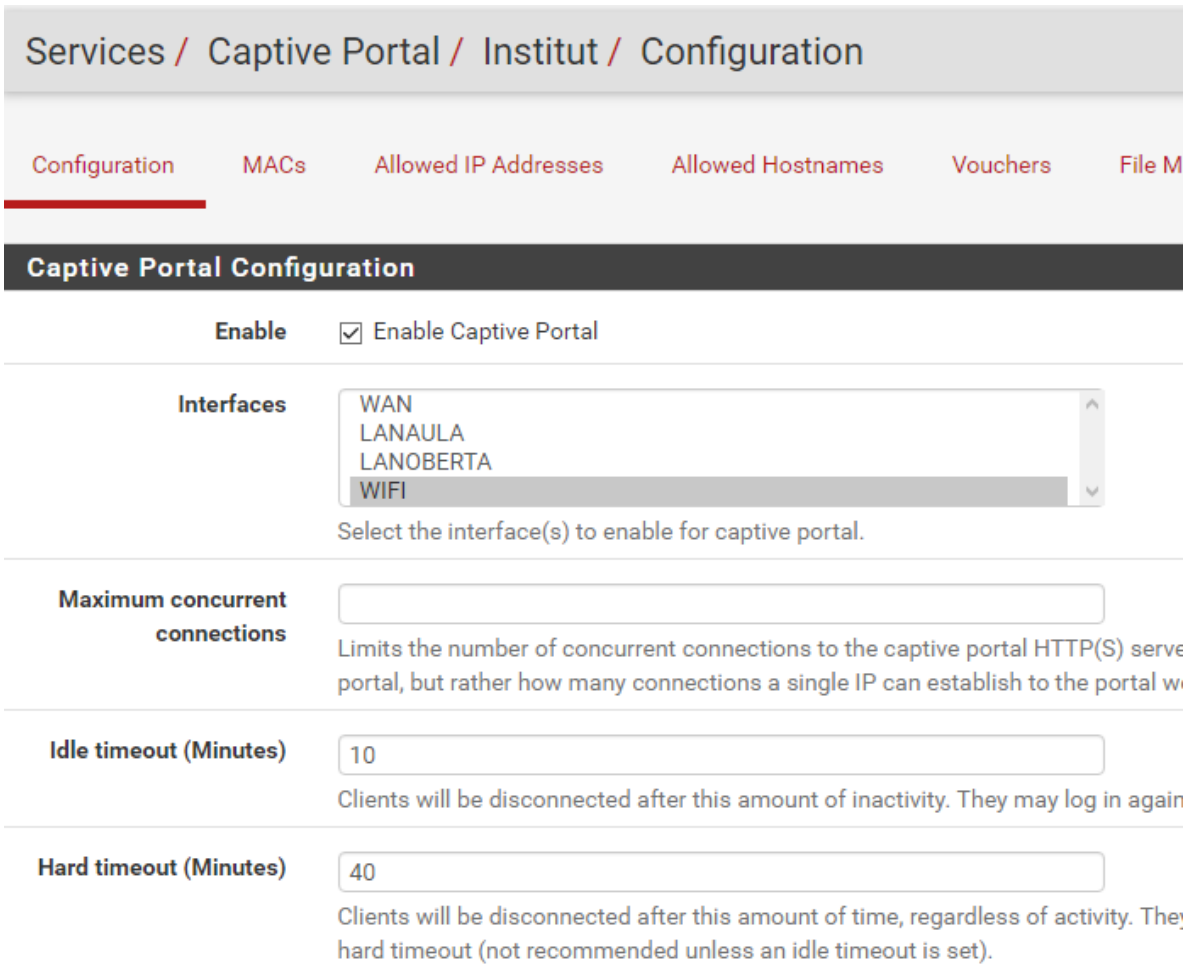
El programa intercepta el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente.

Se usan sobre todo en redes inalámbricas abiertas, donde interesa mostrar un mensaje de bienvenida a los usuarios, y para informar de las condiciones del acceso, también puede requerir un usuario y contraseña para poder acceder.

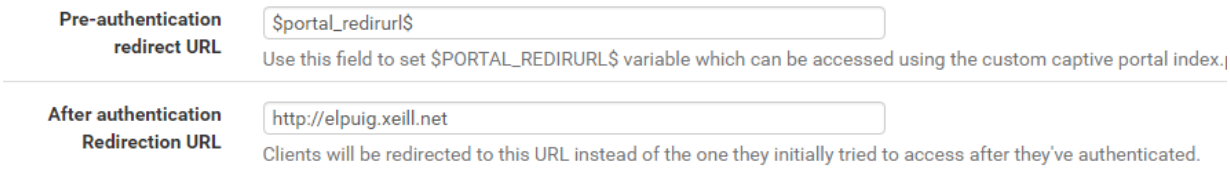
Para nuestro proyecto, en Services/Captive Portal crearemos un portal con autenticación para LanOberta y uno sin autenticación para WiFi, de esta manera veremos como funcionan ambos.

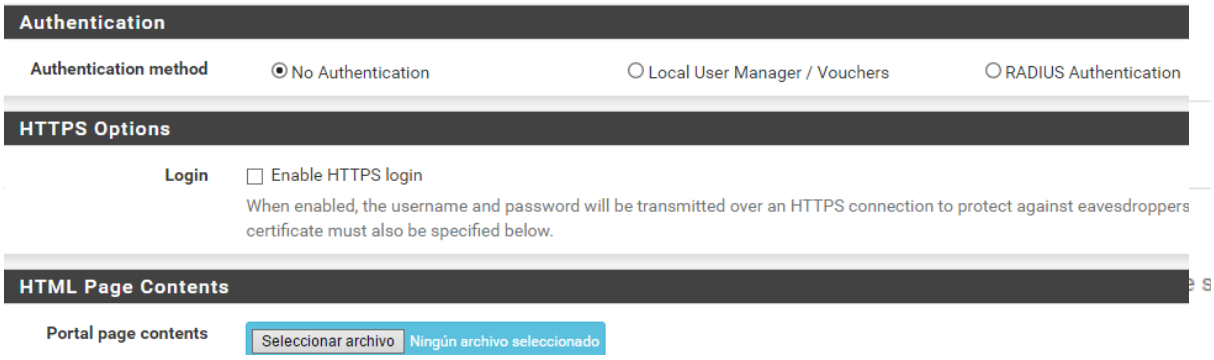


Primero configuraremos un portal cautivo para la interfaz WiFI sin autenticación alguna, el cual nos desconecte a los 40 minutos de uso o después de 10 minutos de inactividad.



Desde aquí también se puede establecer un límite de velocidad para esa interfaz si lo consideramos oportuno. Para que funcione habrá que cargar una web html donde nos indique que estamos bajo un portal teniendo que aceptar antes de poder utilizar la conexión y nos redireccione a la web del centro una vez aceptado. Por lo que tenemos escribir la palabra $portal_rediurl$ para que funcione conjuntamente con nuestra web html.

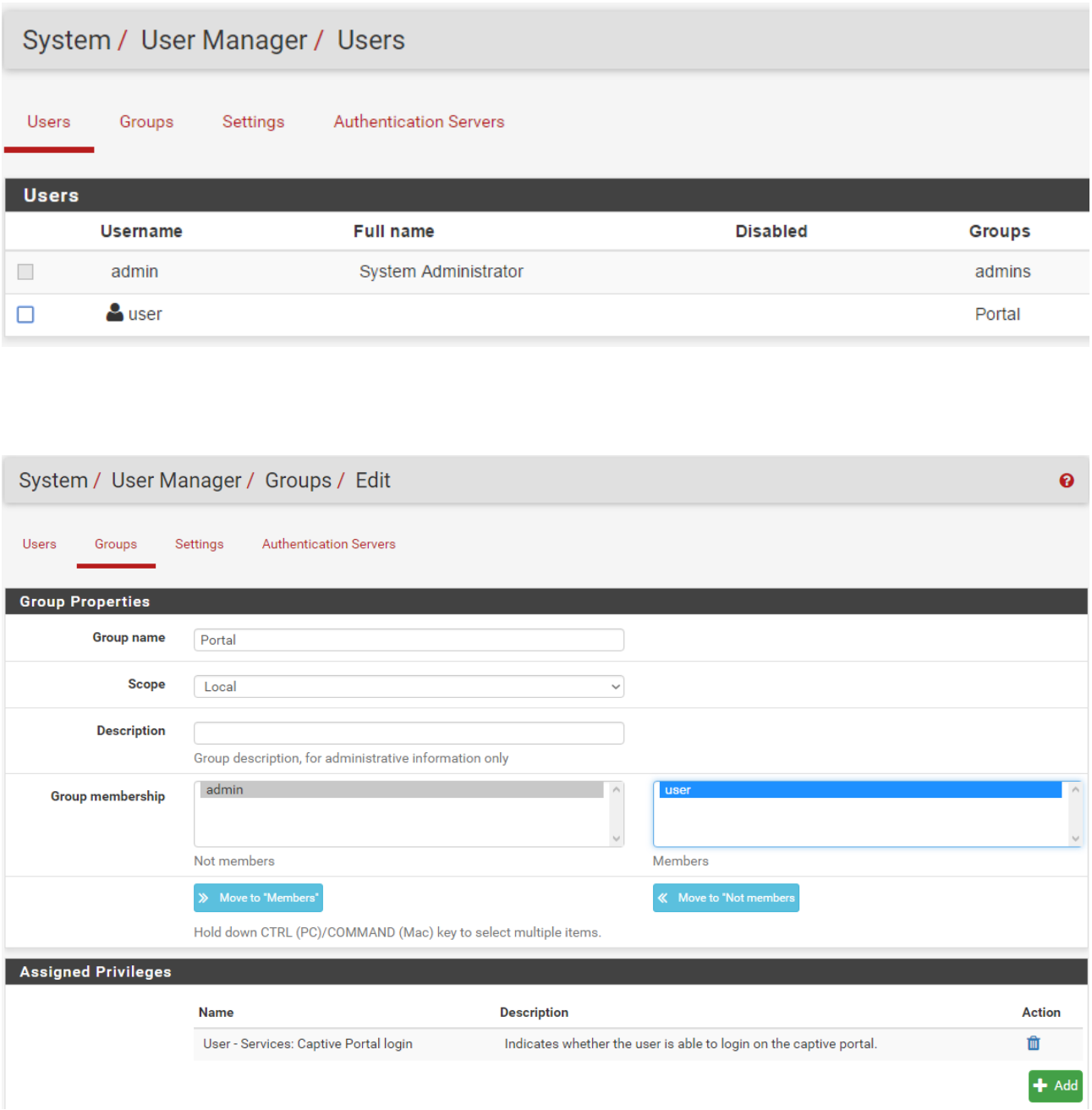




De esta manera al intentar acceder a Internet desde la interfaz WiFi, nos deberá saltar la siguiente pantalla de validación, hasta que no pulsemos el botón de aceptar, no debería tener acceso para poder navegar.

Una vez comprobado el sistema de portal sin autenticar, vamos a configurar para la interfaz LanOberta uno que necesite un usuario y contraseña para su validación.

Antes de entrar a configurar el portal, tenemos que crear el usuario previamente, desde “System/User Manager” crearemos un usuario llamado user de contraseña user para hacer la prueba. Después de crearlo hay que entrar en el apartado Groups y asignarle privilegios para que pueda utilizar el servicio de portal cautivo, tal como muestran las siguientes capturas.


System / User Manager / Users
Users
Groups
Settings
Authentication Servers
Users
Username
Full name
Disabled
Groups
admin
System Administrator
admins
user
Portal
System / User Manager / Groups / Edit
Users
Groups
Settings
Authentication Servers
Group Properties
Group name
Portal
Scope
Local
Description
Group description, for administrative information only
Group membership
admin
user
Not members
Members
Move to "Members"
Move to "Not members"
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Assigned Privileges
Name
Description
Action
User - Services: Captive Portal login
Indicates whether the user is able to login on the captive portal.
Add

Después de crear el usuario, los pasos para activar el portal cautivo son exactamente los mismos que en el caso anterior, pero esta vez eligiendo la interfaz LanOberta, y como método de autenticación activar la opción de usuario local, habrá que cargar igual una página web html donde nos permita acceder mediante un usuario y contraseña, a diferencia del método sin autenticar que era simplemente pulsando en aceptar.

Una vez creado y activado, al acceder mediante la interfaz LanOberta, nos debería aparecer la siguiente pantalla, en la que deberíamos ingresar el usuario y contraseña creados previamente, para poder tener acceso a Internet.

5.6.6. Configuración mediante asistente (Wizard)

Con este asistente, se puede configurar una interfaz o varias de una manera sencilla, desde la que podremos configurar diversos apartados como el ancho de banda y múltiples tipos de prioridades, ya sea para juegos, voz IP o p2p. Para acceder al asistente tenemos que ir a “Firewall/Traffic Shaper/Wizards”, para después elegir si queremos una configuración global o individual.

Cuando se inicia el asistente, nos preguntará sobre que interfaz o interfaces queremos que actúe, lo primero que nos pide configurar es el límite de ancho de banda y un apartado llamado Local y WAN Interface en modo HFSC, PRIQ o CBQ.

HFSC: Hierarchical Fair Service Curve

Es la opción por defecto de pfSense, tiene una jerarquía de colas y tráfico en tiempo real. Es la vamos a utilizar.

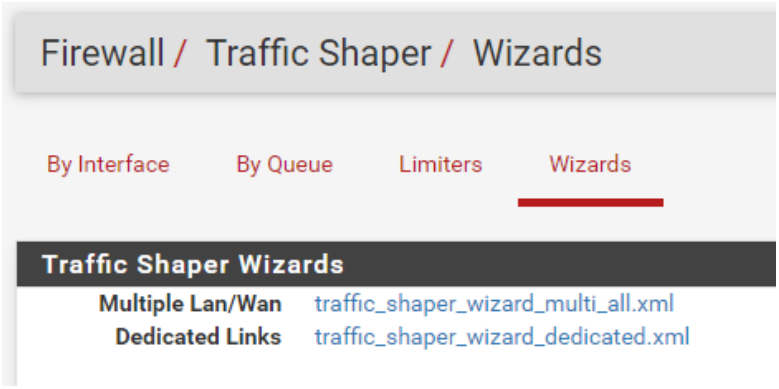
PRIQ: Priority Queueing

La cola de prioridad es la forma más simple de limitar el tráfico, también bastante eficaz. Se lleva a cabo la prioridad solamente del tráfico, sin tener en cuenta el ancho de banda.

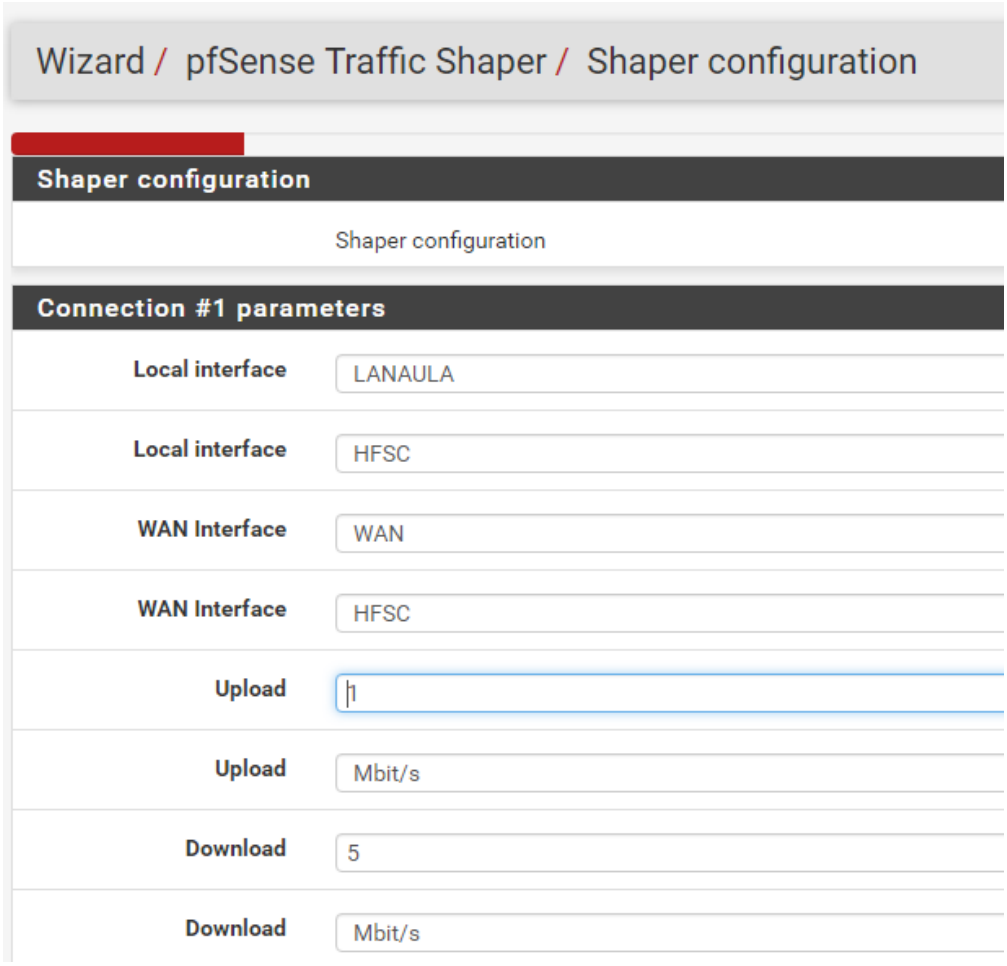
CBQ: Class Based Queueing

Funciona de la misma manera que PRIQ, sin embargo, en lugar de procesar todos los paquetes de la clase, procesará todos los paquetes hasta alcanzar el límite del ancho de banda.

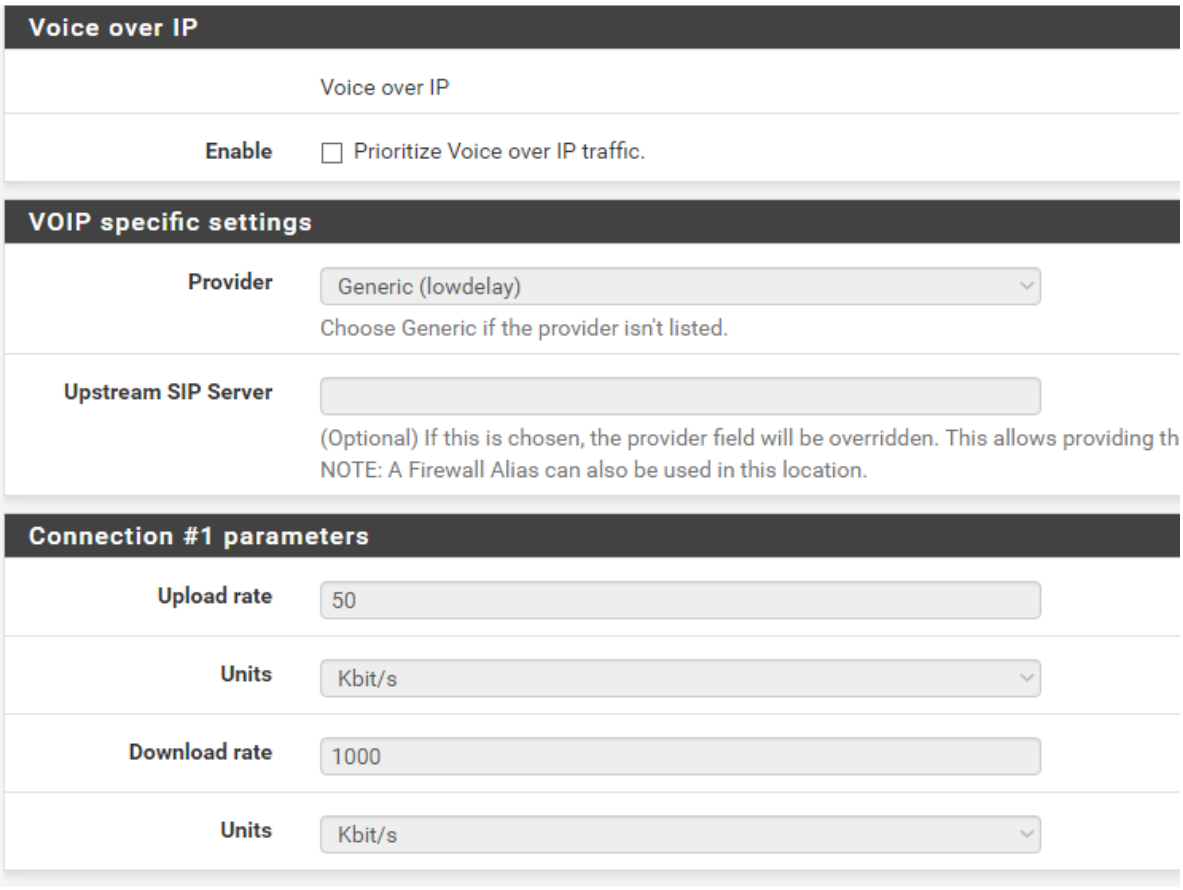
Desde aquí seleccionamos si queremos que se active en una o varias interfaces.



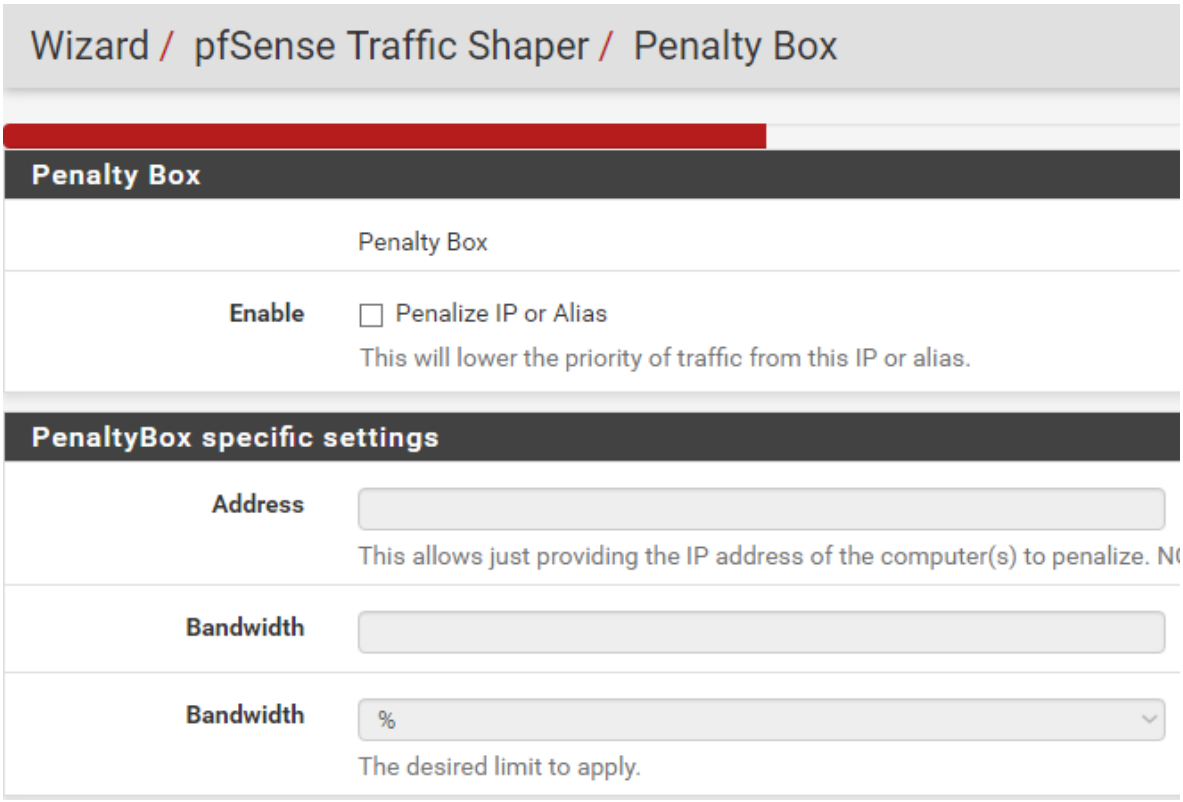
Como he comentado anteriormente, aquí seleccionamos la interfaz, el tipo de funcionamiento de las colas y el límite del ancho de banda.



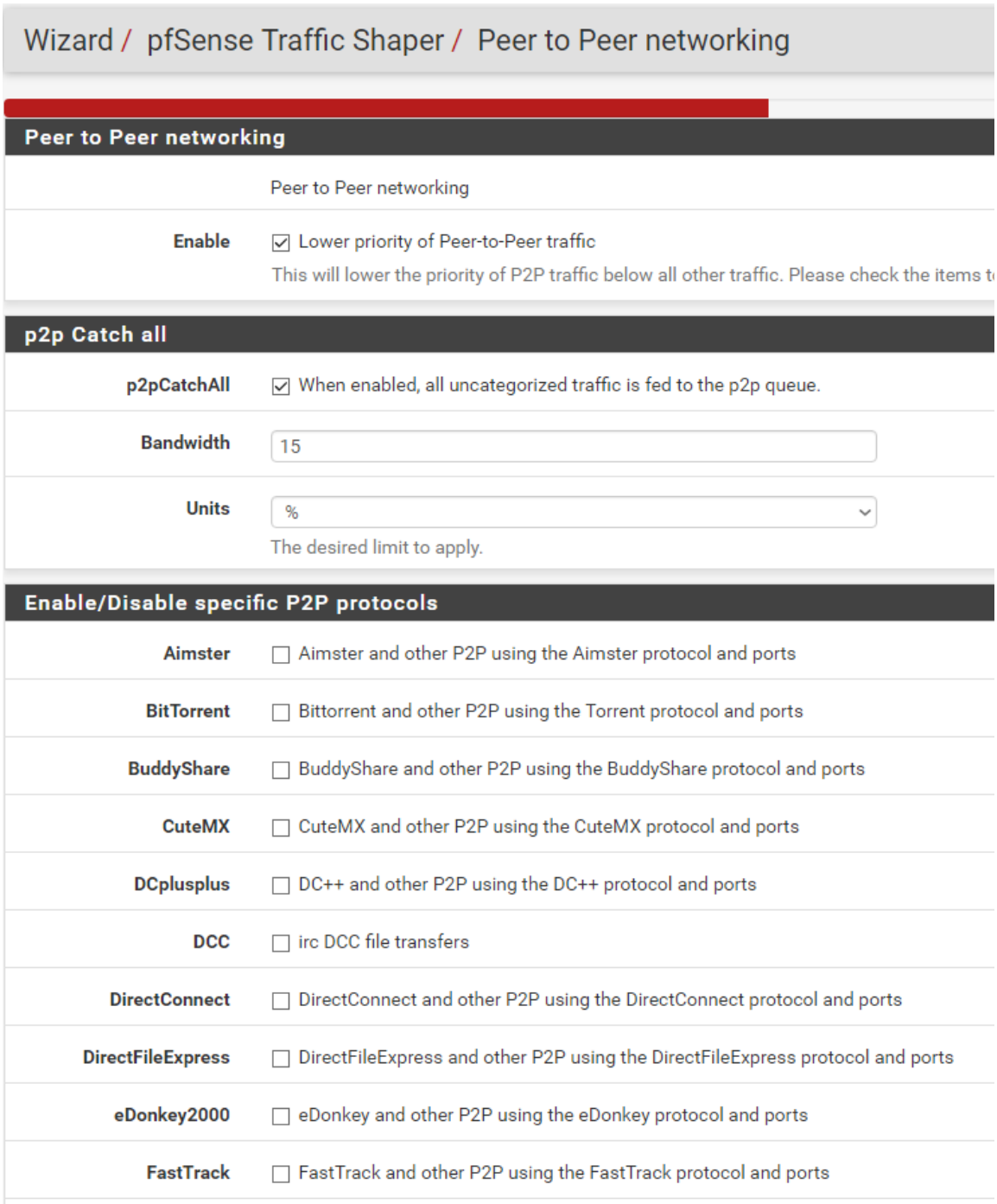
En este nuevo apartado nos aparece si queremos activar la prioridad al tráfico de Voz IP cuando sea necesario. También se puede establecer un límite para asignar a esta característica, por defecto la he dejado sin activar y se habilitará en la interfaz WiFi.



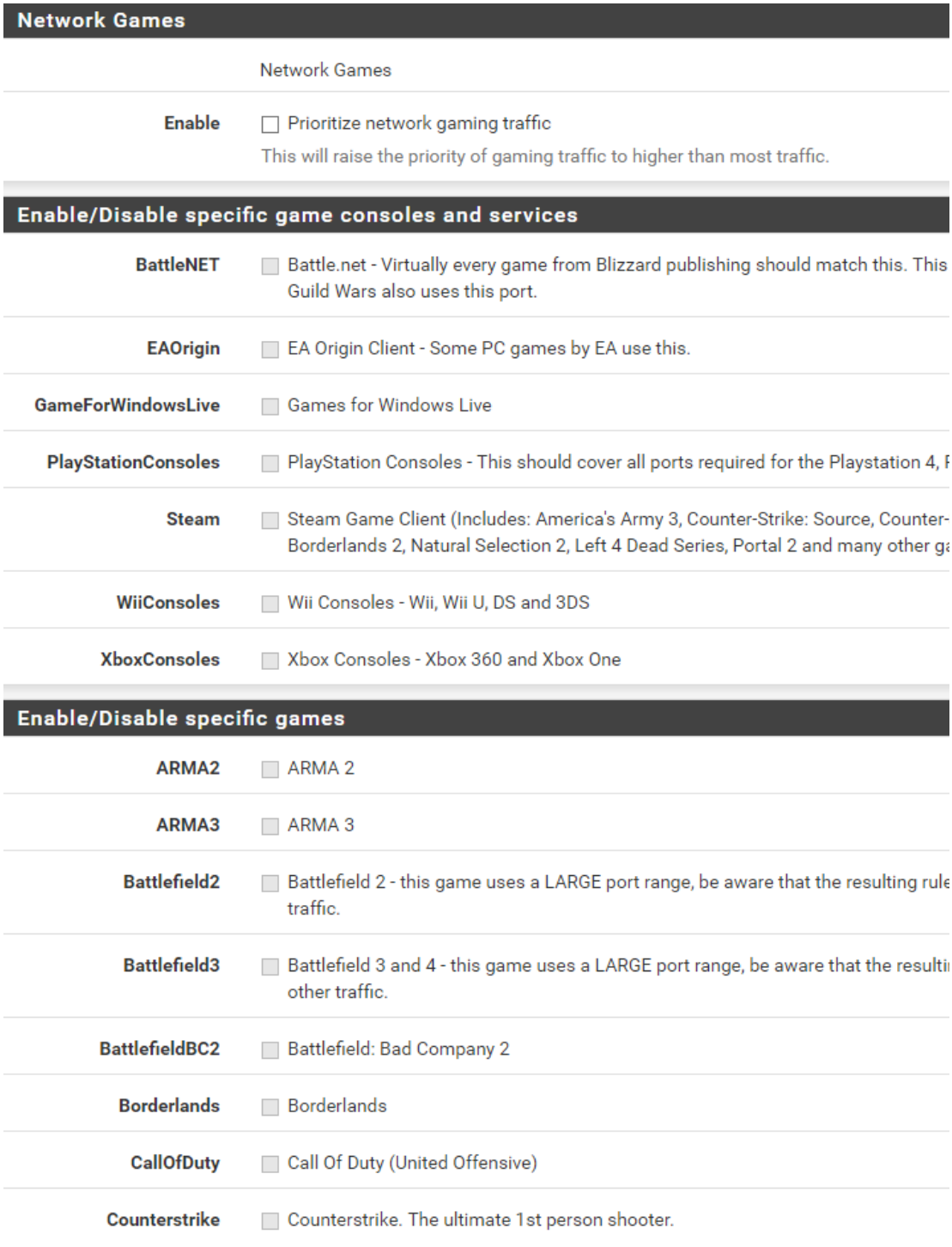
Desde penalty box, podemos establecer una limitación de ancho de banda a una IP concreta, en este caso no vamos a activar la opción, ya que en principio no queremos limitar el ancho de banda a una sola IP.



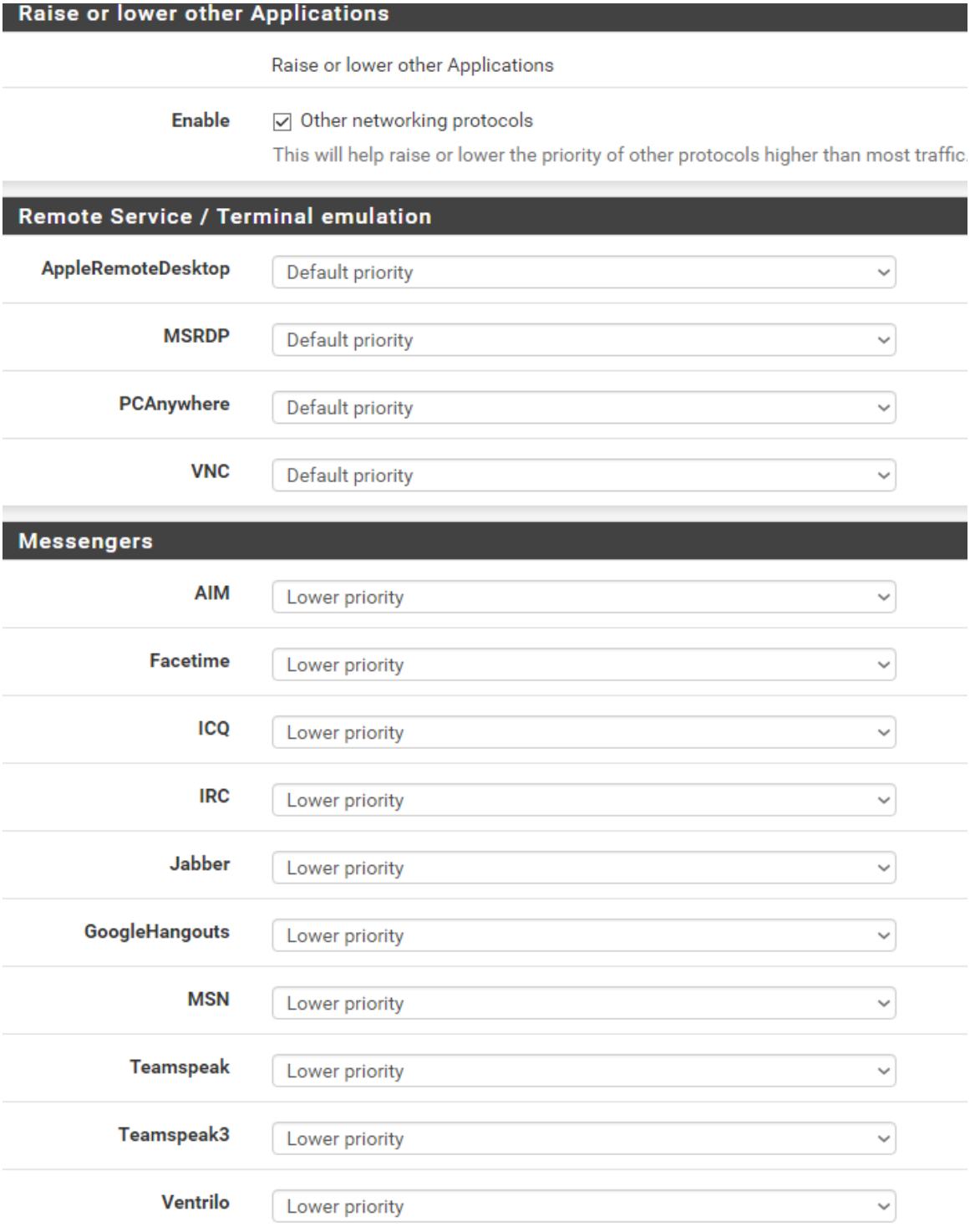
El siguiente paso es bastante interesante, ya que nos permite regular el tráfico de las redes Peer to Peer, es decir, limitar el software de descargas de intercambio de ficheros, ideal si no queremos saturar el ancho de banda con varios usuarios descargando. Tanto en WiFi como en LanAula la tendremos activa, en Oberta no será necesario.



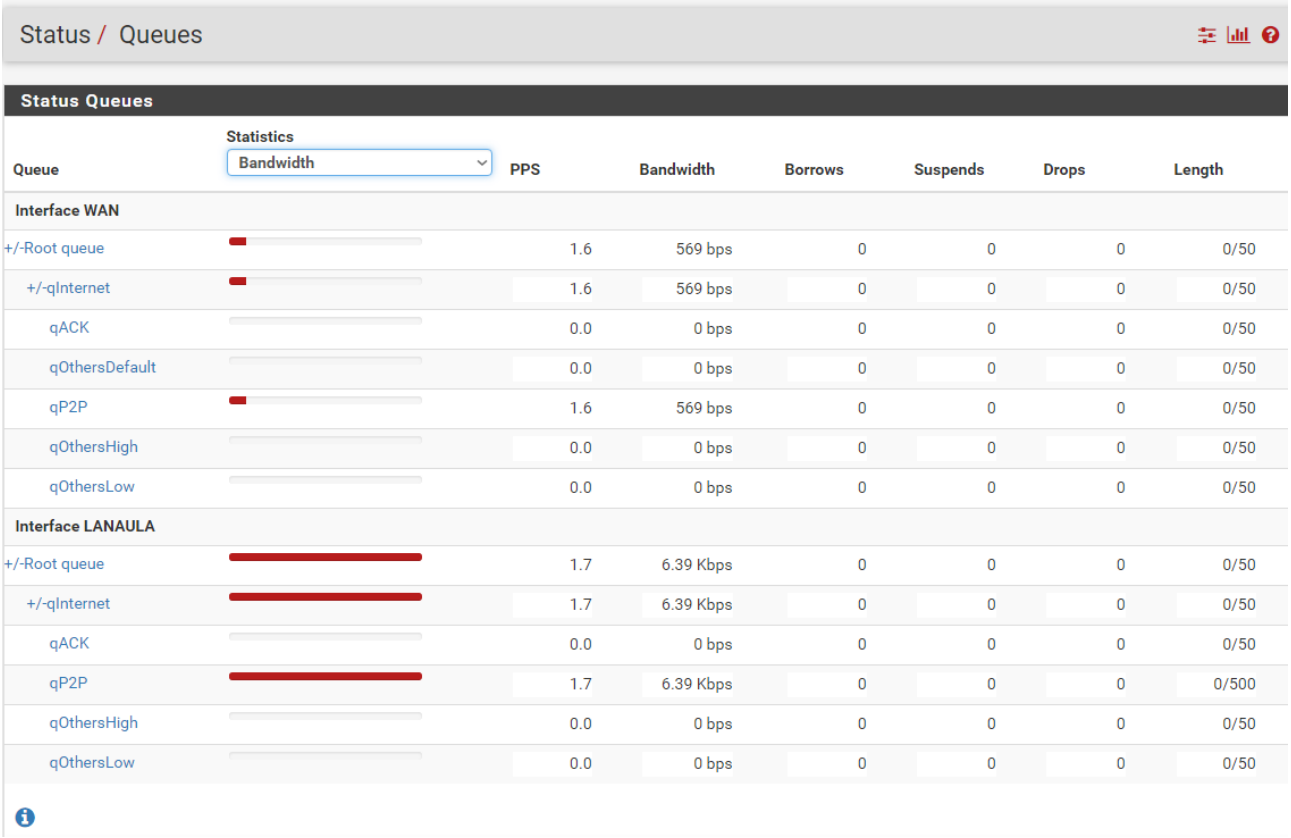
Para el que esté interesado en el juego online, puede activar estas opciones para que cuando quiera jugar, pueda hacerlo con el menor lag/latencia posible, para que en caso de uso masivo de la red, el juego online tenga prioridad sobre el resto. Nos dejará activar o no diferentes plataformas de juego, ya sean de PC o consolas, la dejaremos desactivada ya que no es una red pensada para el juego online.



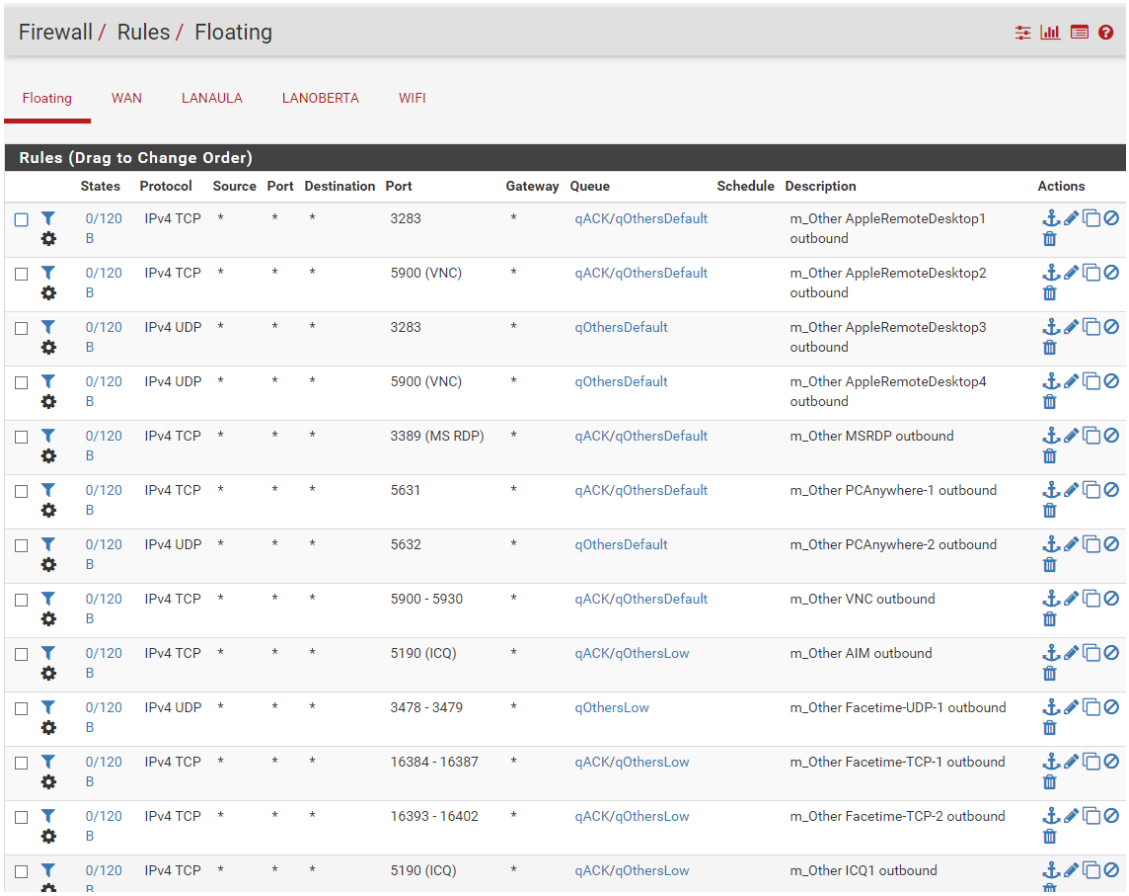
La última opción del asistente, es la prioridad de los diferentes servicios que podrán ser utilizados en Internet, dependiendo para donde vaya destinada la configuración nos interesará darle prioridad a un servicio u a otro. Entre ellas tenemos aplicaciones de mensajería, servicios remotos y VPN, web, correo, cliente de juegos, etc. Para cada tipo de interfaz sería necesario adecuarla a su principal uso, por ejemplo en la de un Aula debería tener una prioridad baja la mensajería instantánea o clientes de juegos.



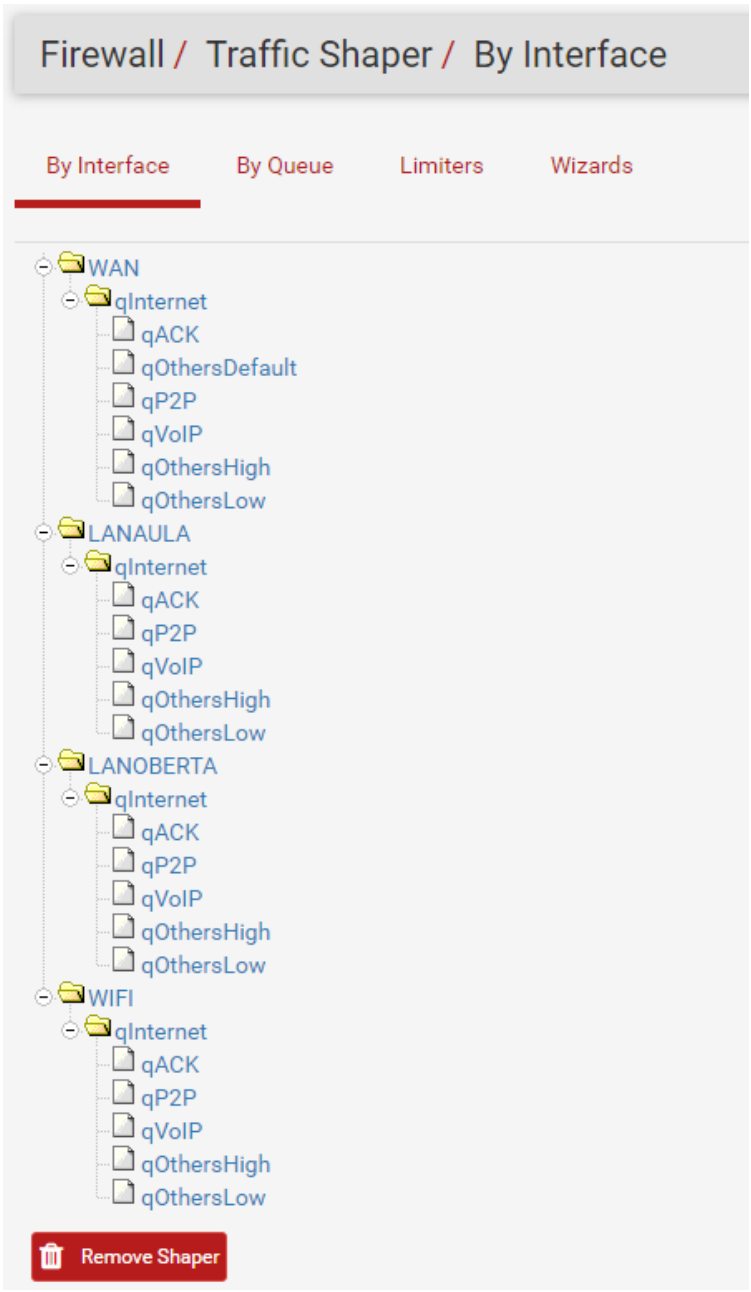
Con la configuración del asistente finalizada, desde “Status/Queues” se puede observar una pequeña monitorización de los diferentes servicios configurados para cada interfaz.



Los perfiles del asistente se pueden modificar a posteriori desde “Firewall/Rules/Floating”, pudiendo modificar uno a uno cada parámetro de forma más personalizada, tal como vemos en la siguiente imagen.



Una vez configurado se mostrará una imagen tal que así:



5.6.7. Snort

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DdoS, finger, FTP, ataques web, CGI, Nmap, etc.

La colocación de Snort en nuestra red puede realizarse según el tráfico quieren vigilar: paquetes que entran, paquetes salientes, dentro del firewall o fuera del mismo.

Realizaremos su instalación desde “System Packages” y lo activaremos.

5.6.8. OpenVPN

OpenVPN es un cliente/servidor VPN tanto para equipos GNU/Linux como para Windows.

Sirve para conectarnos a Internet de una manera segura desde cualquier red ya sea cableada o WiFi, con cifrado o sin cifrar. Todo el tráfico irá cifrado a través de un Túnel desde el AP que nos conectamos hasta nuestra casa y desde allí saldrá a Internet. Lo malo es que debes tener una buena velocidad de subida, ya que de eso dependerá en mayor medida tu velocidad de bajada.

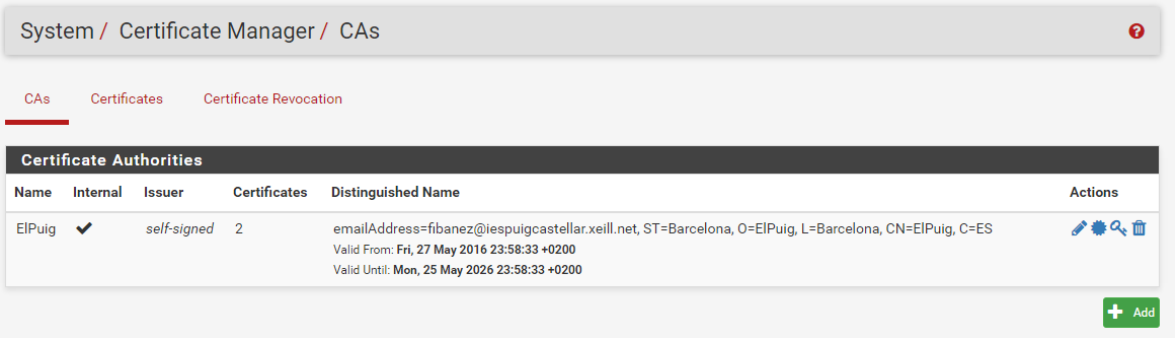
También sirve en caso de no redirigir el tráfico, para poder acceder a los recursos compartidos que tengamos configurados como tal. Tenemos dos tipos de configuración llamados TUN Y TAP.

TUN: El controlador TUN emula un dispositivo punto a punto, es utilizado para crear túneles virtuales operando con el protocolo IP. Las máquinas que queden detrás de cada uno de los extremos del enlace pertenecerán a subredes diferentes.

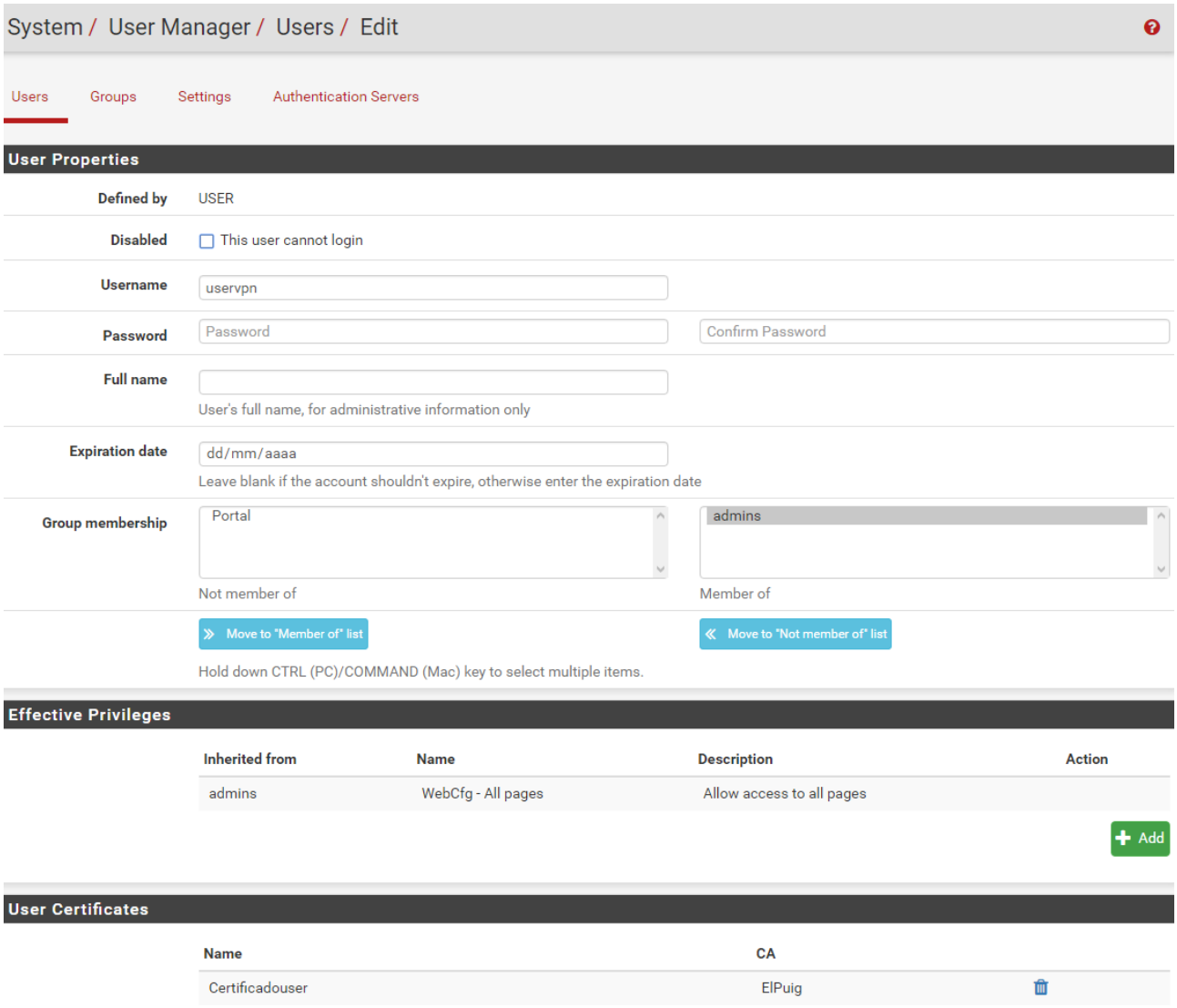
TAP: Simula una interfaz de red Ethernet, más comúnmente conocido como modo puente o bridge, estos túneles virtuales encapsulan directamente paquetes Ethernet. Las máquinas situadas detrás de cada uno de los extremos del enlace pueden operar como parte de la misma subred. El modo de funcionamiento puente es particularmente útil para enlazar usuarios remotos, ya que éstos pueden conectarse a un mismo servidor y virtualmente formar parte de la red principal.

5.6.9. Configuración de OpenVPN

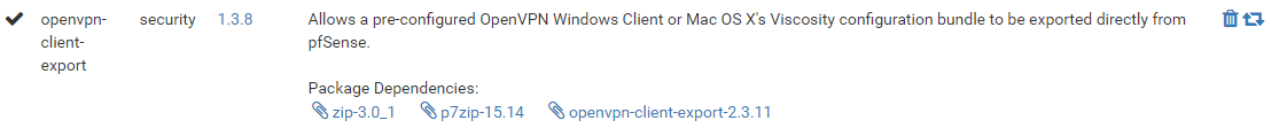
Para empezar, habrá que generar un certificado (le llamaremos ElPuig) que posteriormente será usado para conectar con nuestro OpenVPN a través de un cliente y el software que utilizaremos. Desde “System/Certificate Manager/CAs” haremos el proceso, rellenaremos los datos que nos piden y finalizaremos el asistente.



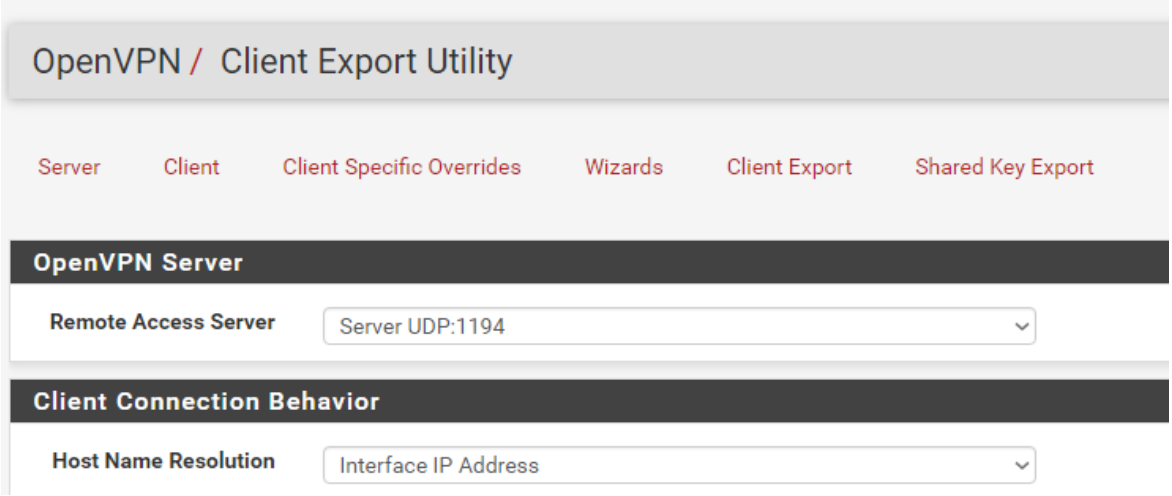
Ahora es turno de crear un usuario, que será el que conectará a través de nuestra conexión. Lo haremos desde “System/User Manager/Users”. Crearemos un usuario llamado uservpn que forme parte del grupo admins y le cargaremos el certificado “ElPuig” creado anteriormente.

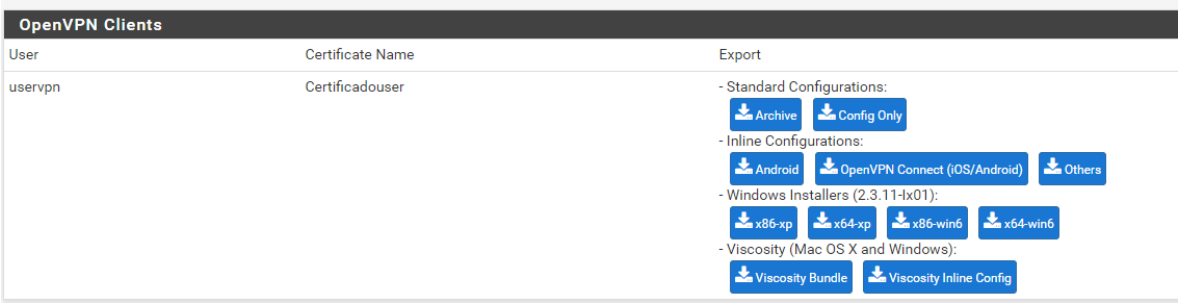


Después de crear el certificado y el usuario, habrá que instalar el siguiente paquete en caso de no estar ya instalado: Openvpn-Client-Export, desde el administrador de paquetes de pfSense.



Cuando tengamos todo listo después de instalar el client-export, haremos uso de esta herramienta para exportar nuestra configuración completa, que podrá ser importada o instalada a nuestro cliente VPN. Después iremos a la web de OpenVPN y descargaremos e instalaremos la aplicación en nuestro ordenador o en la máquina que vamos a necesitar conectar, ya que a través de esa aplicación, podremos conectarnos.



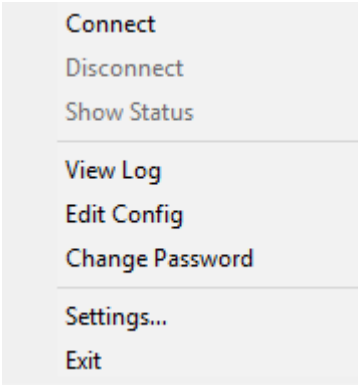


Descargaremos el instalador para que al ejecutar lo configure de forma automática, o el archivo con la configuración para poner manualmente dentro del directorio de la aplicación OpenVPN.

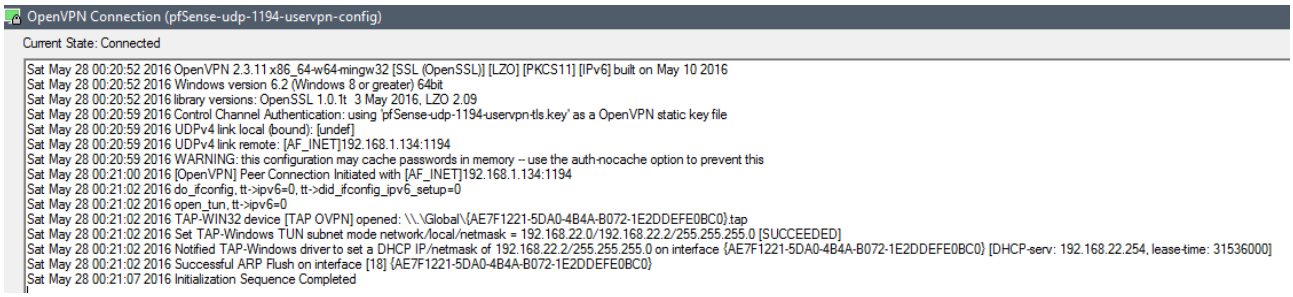
El fichero con extensión .ovpn tendrá esta configuración que será aplicada en nuestro cliente:

```
dev tun
persist-tun
persist-key
cipher AES-256-CBC
auth SHA1
tls-client
client
resolv-retry infinite
remote 192.168.1.134 1194 udp
lport 0
auth-user-pass
pkcs12 pfSense-udp-1194-uservpn.p12
tls-auth pfSense-udp-1194-uservpn-tls.key 1
ns-cert-type server
```

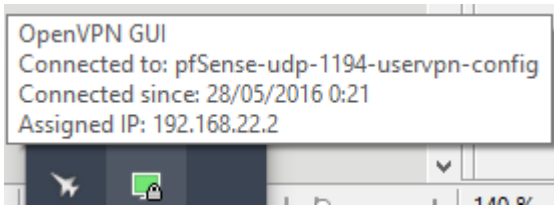
Se podrá configurar desde “Edit Config” y para conectarnos habrá que pulsar en Connect.



Si todos los pasos se han realizado correctamente, cuando hagamos la conexión nos mostrará una pantalla como la siguiente, donde se verá el proceso que lleva a cabo hasta conectar nuestro cliente de la red .1 con la máquina de la red .22, utilizando una configuración TUN para estas subredes.



El icono de OpenVPN nos indicará que se ha conectado de forma satisfactoria:



Por lo que ahora tenemos acceso a esta red de forma segura, cifrada a través del túnel. Con esta última prueba, daremos por concluido el proyecto del cortafuegos pfSense.

6. Conclusiones

Este proyecto ha sido fruto de las necesidades de ver como funciona un cortafuegos, entender las diferentes funciones que posee, e intentar llevarlas a cabo en una red informática.

Se ha empezado haciendo un estudio de la parte de teoría, explicando los diferentes conceptos que existen y que nos podemos encontrar a la hora de planificar el funcionamiento de un cortafuegos, para ello optamos por una distribución libre de código abierto como es pfSense.

Una vez instalado, nos hemos adentrado a ver las diferentes funciones que nos ofrece, desde limitar el ancho de banda y bloquear o permitir el tráfico, hasta poder crear un portal cautivo para que las conexiones se realicen mediante un usuario y contraseña.

Hemos empezado prácticamente desde cero, ya que personalmente no había configurado nunca un cortafuegos, por lo que todo lo que se ha ido aprendiendo ha sido bastante interesante y puede ser una ayuda en un futuro.

Se ha intentado seguir la planificación como estaba prevista, y considero que se ha seguido la línea que se había marcado. Al ir por libre configurando y viendo como funcionaba todo, hay partes que no se han conseguido implementar como nos hubiese gustado, no se ha podido profundizar en los protocolos o el DMZ, el portal Radius fallaba, así que finalmente se hizo con usuarios locales, y el cliente OpenVPN se ha probado bajo un cliente Windows al hacer las pruebas en casa.

En su conjunto ha merecido la pena iniciar este proyecto, ya que era un tema interesante y necesario. Al final considero que ha faltado tiempo, pero todo lo aprendido siempre es positivo.

7. Glosario

FreeBSD: Distribución de software libre

pfSense: cortafuegos basado en FreeBSD

DHCP: Protocolo de configuración dinámica de host (*Dynamic Host Control Protocol*)

DNS: Servidor de nombres de dominio (*Domain Name Server*)

DMZ: Zona desmilitarizada (*Demilitarized Zone*)

EULA: Contrato de licencia del usuario final (*EndUserLicense Agreement*)

GPL: Licencia pública general (*General Public License*)

HTTP: Protocolo de transferencia de hipertexto (*HyperText Transfer Protocol*)

NFS: Sistema de ficheros en red (*Network File System*)

PC: Ordenador personal (*Personal Computer*)

TCP/IP: Protocolo de control de transmisión/Protocolo de Internet (*Transmission ControlProtocol/Internet Protocol*)

IDS: Sistema de detección de intrusiones.

QoS: Calidad de servicio (*Quality of Service*)

Backdoor: Puerta trasera

DdoS: Ataque a un sistema (*Distributed Denial of Service*)

8. Bibliografía

https://es.wikipedia.org/

https://forum.pfsense.org/index.php

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

http://www.maestrosdelweb.com/snort/

https://openvpn.net

http://www.linux-party.com/index.php/

9. Anexo

En este apartado habría que incorporar el punto 5 del proyecto, que no es más que la instalación y configuración de la máquina virtual y el cortafuegos paso a paso con todas las funciones que he se han utilizado.