



## **Desarrollo De Un Firewall De Bajo Costo Y Alto Rendimiento Utilizando Hardware Genérico**

David Alejos Omedas

Ciclo Superior de Administración de Sistemas Informáticos en Redes

IES Medina Ahazara

06/2023



Esta obra está sujeta a una licencia de  
Reconocimiento - No Comercial - Sin Obra  
Derivada 3.0 España de Creative Commons

**Ficha Del Proyecto Final**

Título del trabajo:	Desarrollo de un firewall de bajo costo y alto rendimiento utilizando hardware genérico
Nombre del autor:	David Alejos Omedas
Fecha de entrega (mm/aaaa):	06/2023
Área del Trabajo Final:	Redes
Ciclo Grado Superior:	Administración de Sistemas Informáticos en Red
Resumen del Trabajo (máximo 250 palabras):	
<p>El proyecto consiste en convertir un PC en un router OPNsense virtualizado utilizando Proxmox. Esto permitirá cubrir las necesidades de red de una empresa sin invertir grandes sumas en hardware. Para demostrar las capacidades del dispositivo se diseñará una red para una empresa ficticia con dos VLAN.</p> <p>Entre las funciones de seguridad que realizará el dispositivo se encuentran el bloqueo de conexiones IP maliciosas, el bloqueo de publicidad a nivel de red, DNS local y servidor DHCP para la asignación de direcciones IP estáticas.</p> <p>Además, se añadirán servicios adicionales para demostrar la versatilidad del sistema frente a dispositivos comerciales. Estos servicios incluyen un sitio web WordPress, una wiki para la documentación de procesos y el desarrollo de un portal web personalizado.</p> <p>Una vez implementado el sistema se realizarán pruebas de rendimiento y consumo para comprobar que el sistema es viable.</p>	

## Índice

Ficha Del Proyecto Final .....	3
Lista de imágenes .....	7
Introducción .....	11
Contexto y justificación del Proyecto.....	11
Objetivos del Proyecto .....	11
Propuesta de solución.....	12
Análisis descriptivo.....	13
Análisis de requisitos .....	14
Requisitos de Hardware .....	14
Requisitos de Software .....	14
Requisitos de Red .....	15
Requisitos de Escalabilidad .....	16
Requisitos Humanos.....	16
Temporalización .....	16
Identificación de tareas.....	16
Secuenciación .....	19
Memoria técnica .....	20
Planificación de la red.....	20
Adquisición de materiales.....	21
Ordenador.....	21
Tarjeta de red.....	21
Switch.....	22
Instalación del sistema .....	22
Instalación de tarjeta de red adicional .....	22
Instalación de Proxmox .....	23

DESARROLLO DE UN FIREWALL AVANZADO	5
Configuración inicial de Proxmox .....	23
Creación de máquina KVM para OPNsense .....	24
Instalación de OPNsense .....	25
Configuración inicial de OPNsense .....	27
Desactivación de usuario root .....	29
Optimización de la máquina KVM.....	31
Segmentación de la red mediante VLAN.....	33
Configuración del switch .....	33
Configuración de la VLAN en OPNsense.....	35
Configuración del servidor DHCP .....	36
Configuración del servidor dedicado a la red VLAN1.....	37
Configuración del servidor DHCP de la red VLAN2.....	37
Acceso externo .....	38
Configuración de NAT .....	38
Bloqueo y seguridad.....	39
Bloqueo de tráfico malicioso mediante listas IP.....	40
Reglas de firewall.....	43
Bloqueo de publicidad y webs maliciosas.....	44
Bloqueo de dominios por DNS .....	48
Otros .....	49
DNS local .....	49
Servicios de red adicionales: BookStack.....	50
Servicios de red adicionales: Wordpress .....	53
Servicios de red adicionales: Servidor Apache .....	54
Desarrollo de la página de inicio a medida.....	56
Seguimiento y control.....	60
Instantáneas.....	60
Evaluación del rendimiento.....	60

DESARROLLO DE UN FIREWALL AVANZADO	6
Livebox Fibra Sagemcom F@st 5656 .....	61
HP Prodesk 8500T (OPNsense) .....	61
Evaluación del consumo eléctrico .....	61
Livebox Fibra Sagemcom F@st 5656 .....	61
HP Prodesk 8500T .....	62
Estudio presupuestario .....	63
Costes del Proyecto .....	63
Conclusiones.....	63
Análisis DAFO.....	65
Debilidades .....	65
Amenazas .....	65
Fortalezas.....	66
Oportunidades .....	66
Ampliaciones futuras .....	67
Escalabilidad.....	67
Glosario .....	68
Trabajos citados.....	70
Anexos .....	71
Habilitación del acceso por consola.....	71

## Lista de imágenes

Ilustración 1 - HP Prodesk 600 G4.....	21
Ilustración 2 - TP-Link Adaptador UE300 USB .....	22
Ilustración 3 – Switch gestionable GS308E.....	22
Ilustración 4 - Instalación de tarjeta de red externa .....	22
Captura 1 – Configuración de las interfaces de red en Proxmox .....	24
Captura 2 – Carga de la ISO de instalación de OPNsense en Proxmox .....	24
Captura 3 – Configuración de Hardware de la KVM .....	25
Captura 4 – Asistente de configuración de OPNsense .....	25
Captura 5 - Confirmación de la asignación de las interfaces de red .....	26
Captura 6 – Bienvenida a OPNsense en modo liveCD .....	26
Captura 7 – Selección de disco de destino .....	26
Captura 8 – Finalización del proceso de instalación.....	27
Captura 9 – Portal de autenticación a la versión Web de OPNsense.....	27
Captura 10 – Asistente de configuración inicial.....	28
Captura 11 – Configuración básica .....	28
Captura 12 – Configuración del servidor ntp .....	28
Captura 13 – Configuración de la interfaz wan en modo DHCP .....	29
Captura 14 – Opciones de seguridad para la WAN .....	29
Captura 15 – Configuración de la red LAN .....	29
Captura 16 – Creación de usuario .....	30
Captura 17 – Asignación de usuario al grupo administrador .....	30
Captura 18 – Deshabilitación de cuenta de usuario.....	30
Captura 19 – Listado de usuarios .....	31
Captura 20 – Plugin Quemu Agent habilitado .....	31

DESARROLLO DE UN FIREWALL AVANZADO	8
Captura 21 – Configuración de Quemu Agent en la máquina KVM de proxmox .....	31
Captura 22 – Configuración de parámetros optimizables .....	32
Captura 23 – Desactivación de puntero de tablet en la máquina KVM .....	32
Captura 24 – Desactivación de offloading por hardware en OPNsense .....	32
Captura 25 – Estado y versión del sistema .....	33
Captura 26 – Actualización del sistema .....	33
Captura 27 – Interfaz de configuración de VLAN 802.1Q en el switch NETGEAR .....	34
Captura 28 - Configuración de tipo de puertos para la VLAN 1.....	34
Captura 29 - Captura 30 - Configuración de tipo de puertos para la VLAN 1 .....	34
Captura 31 – Asignación VLANs a los puertos físicos .....	35
Captura 32 – Listado de VLANs en OPNsense .....	35
Captura 33 – Asignación de interfaces.....	36
Captura 34 – Configuración de la Interfaz virtual .....	36
Captura 35 – Configuración del servidor DHCP para la red LAN .....	37
Captura 36 – Mapeos DHCP estáticos .....	38
Captura 37 – Comprobación del servidor DHCP desde un cliente .....	38
Captura 38 – Configuración de regla NAT para dar acceso a un servidor.....	39
Captura 39 – Listado de reglas NAT activas .....	39
Captura 40 – Comprobación de la regla NAT .....	39
Captura 41 – Creación de un alias para el firewall .....	41
Captura 42 – Listado de alias configurados en el firewall .....	41
Captura 43 – Configuración de regla de bloqueo en el firewall .....	42
Captura 44 – Ping a IP bloqueada.....	42
Captura 45 – Registro del firewall.....	42
Captura 46 – Regla para impedir el tráfico de un equipo a otro.....	43
Captura 47 – Intento de Ping a un equipo bloqueado por el firewall .....	43
Captura 48 – Conexiones rechazadas por el firewall .....	44
Captura 49 – Regla para dar acceso a internet a la VLAN2 .....	44



DESARROLLO DE UN FIREWALL AVANZADO	9
Captura 50 – Complemento activo .....	45
Captura 51 – Habitación de ADGUAD en OPNsense.....	45
Captura 52 – Configuración DNS en el servidor DHCP.....	46
Captura 53 – Configuración de interfaz web de ADGUARD.....	46
Captura 54 - Configuración de interfaz de escucha para ADGUARD .....	46
Captura 55 – Panel de estadísticas de ADGUAD .....	47
Captura 56 – Listas de bloqueo por defecto.....	47
Captura 57 – Añadir listas de bloqueo .....	47
Captura 58 – Listas especializadas en bloquear malware y phishing.....	48
Captura 59 – Bloqueo de dominios por DNS.....	49
Captura 60 – Bloqueo de servicios por DNS.....	49
Captura 61 – Reescritura de dominios para uso en local.....	50
Captura 62 – Lista de plantillas de contenedores descargadas en Proxmox.....	50
Captura 63 – Creación del contenedor para bookStack.....	51
Captura 64 – Configuración de la red del contenedor en la VLAN 2.....	51
Captura 65 – Configuración del dominio local en el asistente de instalación .....	51
Captura 66 – Asignación de IP al dominio local en el servidor DNS.....	52
Captura 67 – Resumen del asistente de instalación.....	52
Captura 68 – Panel de inicio de BookStack .....	52
Captura 69 – Configuración de contenedor para Wordpress .....	53
Captura 70 – Reescritura de DNS a nivel local .....	53
Captura 71 – Página de administración de Wordpress .....	54
Captura 72 – Panel de control del contenedor Turnkey LAMP .....	55
Captura 73 – Creación de un host virtual de Apache .....	55
Captura 74 – Administrador de archivos de Webmin.....	55
Captura 75 – Página de inicio a medida.....	56
Captura 76 – Creación de una instantanea .....	60
Captura 77 – Test de velocidad y latencia conectado al router de la operadora .....	61

DESARROLLO DE UN FIREWALL AVANZADO	10
Captura 78 - Test de velocidad y latencia conectado al router OPNsense .....	61
Captura 79 – Tipo de Shell asignada al usuario .....	71
Captura 80 – Permitir sudo .....	71
Captura 81 – Habilitar SSH.....	71
Gráfico 2 -Diagrama de Gantt .....	19
Gráfico 1 – Esquema de la red.....	20
Gráfico 3 - Gráficas del consumo instantaneo y acumulado en 24h .....	62
Gráfico 4 - Gráficas del consumo instantaneo y acumulado en 24h.....	62

## **Introducción**

### **Contexto y justificación del Proyecto**

Los dispositivos empresariales de marcas establecidas tienen un precio superior al que están dispuestas a pagar muchas pequeñas y medianas empresas, a pesar de que ofrecen funciones de las que se podrían beneficiar. Por ello podría resultar útil crear un dispositivo de enrutamiento y cortafuegos con capacidades similares a dichos dispositivos y que a su vez sea más versátil y económico, permitiendo ampliar sus capacidades según vayan creciendo las necesidades de la empresa.

Actualmente las pequeñas y medianas empresas utilizan hardware que ofrecen pocas funcionalidades o recurren a hardware más avanzado de segunda mano pero que ya se encuentra anticuado, por lo que un dispositivo versátil y económico que ofrezca las funcionalidades que necesitan podría resultarles atractivo.

### **Objetivos del Proyecto**

El objetivo principal es proporcionar a la empresa una solución de red versátil, escalable, y económica que no requiera invertir en hardware adicional durante un largo periodo de tiempo y se pueda ejecutar desde un único dispositivo físico. Algunos de los objetivos específicos del proyecto son:

- Usar hardware de PC para crear el router / firewall.
- Explorar las distintas funciones que ofrecen los sistemas operativos firewall.
- El rendimiento y consumo energético debe ser igual o mejor que un router comercial de precio similar.

- Filtrado de publicidad a nivel de red.
- Filtrado de amenazas mediante lista negra.
- Separar los servidores locales en una VLAN distinta.
- Implementar el sistema mediante virtualización, de forma que permita añadir servicios de red adicionales según las necesidades del usuario, además del resto de ventajas que pueda aportar la virtualización como el soporte de snapshots.
- Ofrecer otros servicios en la red desde el mismo dispositivo que puedan resultar de utilidad a una empresa y que no se puedan ofrecer directamente desde el sistema operativo de firewall.

### **Propuesta de solución**

Este proyecto propone aprovechar un ordenador que la empresa ya no esté utilizando o bien comprar uno para crear un router/ firewall que cubra sus necesidades; a la vez que pueda escalar su funcionalidad con el crecimiento de la empresa sin necesidad de inversión adicional en hardware.

Se propone crear el dispositivo basándose en el sistema operativo libre OPNsense, que gestionará las funciones principales de la red. Para facilitar futuras expansiones en funcionalidad, además de dar soporte a snapshots, se va a ejecutar sobre Proxmox, un sistema operativo de virtualización a nivel de kernel que es muy eficiente en el uso de recursos hardware disponibles.

Todo ello será ejecutado en un PC cuyo único requisito es que tenga potencia de procesamiento suficiente para ejecutar OPNsense sobre Proxmox y que disponga de dos tarjetas de red Gigabit Ethernet. La potencia del PC elegido dependerá de las necesidades de la empresa y lo que esté dispuesta a gastar.

## **Análisis descriptivo**

La parte esencial del proyecto consiste en convertir un mini PC en un router/ firewall utilizando OPNsense y virtualizarlo mediante Proxmox.

OPNsense es una distribución de firewall de código abierto basada en FreeBSD que ofrece una amplia gama de servicios de seguridad para proteger redes contra ciberataques. Con características como control de aplicaciones y filtrado web, es una herramienta invaluable para los administradores de redes. Además, su facilidad de instalación y compatibilidad con servidores físicos y virtuales lo convierten en una opción atractiva.

Por otro lado, Proxmox es una plataforma de virtualización de código abierto basada en Debian que permite gestionar fácilmente máquinas virtuales, clústeres de alta disponibilidad y herramientas de recuperación desde su interfaz web.

Está comprobado que OPNsense funciona bien en máquinas KVM bajo Proxmox, por lo que se utilizará esta combinación de software para permitir la máxima flexibilidad de configuración al proyecto.

En términos de arquitectura de red, el router dividirá la red en dos VLAN: una para los usuarios de la red (empleados) y otra para los servidores de la empresa. Los servidores podrán estar tanto en equipos físicos independientes como virtualizados en el propio dispositivo.

Las funcionalidades principales que se implementarán serán:

- Router / Firewall de red con filtrado mediante lista negra de IP.
- Servidor DHCP en cada una de las VLAN con asignaciones estáticas.
- Servidor DNS local, con filtrado mediante listas negras de dominios.
- Snapshots del SO OPNsense para recuperación del sistema.

Otras funcionalidades adicionales que se incluirán a modo de ejemplo de las funcionalidades que puede llegar a ofrecer son:

- Servidor de Wordpress accesible desde el exterior mediante redireccionamiento NAT.
- Servidor BookStack de tipo Wiki, que permitirá a la empresa documentar de forma organizada sus procesos.
- Portal de inicio personalizado para la red local, que contendrá enlaces a los diferentes servicios de la red local para un fácil acceso.

### **Análisis de requisitos**

A continuación se identificarán y describirán los diversos elementos necesarios para el desarrollo e implementación exitosa del proyecto.

#### ***Requisitos de Hardware***

- Un ordenador que cumpla con los requisitos mínimos de Proxmox y OPNsense.
- Suficiente capacidad de almacenamiento para las máquinas virtuales y los servicios adicionales a implementar.
- Suficiente memoria RAM para soportar el funcionamiento de las máquinas virtuales y el enrutamiento de tráfico.
- Una segunda tarjeta de red para el PC ya sea interna o externa, en caso de que no la tenga.
- Un Switch compatible con el protocolo 802.1q

#### ***Requisitos de Software***

- La última versión estable de Proxmox, que será instalada directamente en el PC para virtualizar tanto el router como el resto de las máquinas virtuales y contenedores.

- La última versión estable de OPNsense, configurada como el router/firewall principal de la red.
- Un contenedor de Proxmox con WordPress instalado para poder alojar el sitio web de la empresa.
- Un contenedor de Proxmox con BookStack instalado para proporcionar una wiki donde la empresa pueda organizar y documentar sus procesos.
- Un servidor web en un contenedor de Proxmox para alojar la página de inicio personalizada que contendrá enlaces a los servicios de la red local.

### ***Requisitos de Red***

- Configuración de dos VLAN, una para los usuarios de la red y otra para los servidores de la empresa.
- Configuración del redireccionamiento NAT en OPNsense para permitir el acceso al sitio web de la empresa desde el exterior.
- Configuración de funciones de seguridad en OPNsense, como el uso de listas negras para bloquear conexiones IP maliciosas y bloqueo de publicidad mediante la extensión de servidor DNS ADGUARD HOME.
- Configuración de reescritura de DNS en ADGUARD HOME para facilitar el acceso a los servidores locales sin necesidad de recordar las direcciones IP de cada equipo.
- Asignación de direcciones IP estáticas en el servidor DHCP de OPNsense para algunos de los servidores.

***Requisitos de Escalabilidad***

- Capacidad de agregar nuevas máquinas virtuales: El proyecto debe permitir la fácil adición de nuevas máquinas virtuales en Proxmox para implementar servicios adicionales a medida que la empresa los necesite.
- Capacidad de escalabilidad de recursos: El hardware utilizado debe tener suficiente capacidad para soportar el crecimiento de la red y la carga adicional de servicios sin comprometer el rendimiento.

***Requisitos Humanos***

- Se requiere de una persona con conocimientos en redes y sistemas operativos para implementar el proyecto, así como conocimientos en desarrollo web para crear la página de inicio según los requisitos que imponga el cliente.

**Temporalización****Identificación de tareas**

Se han identificado las siguientes tareas a realizar para completar el desarrollo del proyecto.

- Análisis y definición de requisitos: Incluye identificar los requisitos hardware, software y red necesarios, además de determinar de los objetivos y funcionalidades necesarias.
- Selección y adquisición del hardware: Incluye adquirir un PC compatible con Proxmox y OPNsense y verificar que funciona adecuadamente.
- Planificación de la red: Consistirá en planificar la distribución tanto física como lógica de la red.
- Instalación e interconexión física de los dispositivos.



- Desarrollo del portal web que servirá de página de inicio o directorio de los servicios de la red.
- Instalación y configuración del software en el dispositivo:
  - Instalación de Proxmox: Descargar la última versión estable de Proxmox e instalarlo en el PC escogido.
  - Realizar una configuración básica de Proxmox.
  - Creación de una máquina virtual KVM para OPNsense.
  - Instalación de OPNsense.
  - Realizar una configuración básica de OPNsense.
  - Desactivación del usuario root en OPNsense.
  - Optimización de la máquina KVM para el correcto funcionamiento de OPNsense.
  - Segmentación de la red en VLAN: Establecer y configurar las VLAN necesarias para separar la red de usuarios y la red de servidores, configurando las reglas de enrutamiento y seguridad necesarias.
  - Configuración del servidor DHCP para que asignen las configuraciones correctas según las especificaciones del proyecto.
  - Configuración del redireccionamiento NAT para permitir el acceso externo a la máquina que sirve la web hecha en WordPress.
  - Configuración del bloqueo de tráfico mediante listas negras de IP.
  - Definición de las reglas de firewall que puedan ser necesarias para satisfacer las necesidades de la empresa.
  - Configuración del bloqueo de publicidad mediante DNS.
  - Bloqueo de los dominios que requiera el cliente.
  - Configuración de la reescritura DNS en el servidor DNS para facilitar el acceso a los recursos de la red.

- Instalación y configuración de Wiki basada en BookStack.
  - Instalación y configuración de servidor web con WordPress.
  - Instalación y configuración de servidor apache que alojará la página de inicio.
- Evaluación del sistema para verificar el rendimiento y consumo del dispositivo
- Documentación de las configuraciones y procedimientos realizados durante la implementación.
- Capacitación al personal de la empresa sobre el funcionamiento y mantenimiento del sistema.

Secuenciación

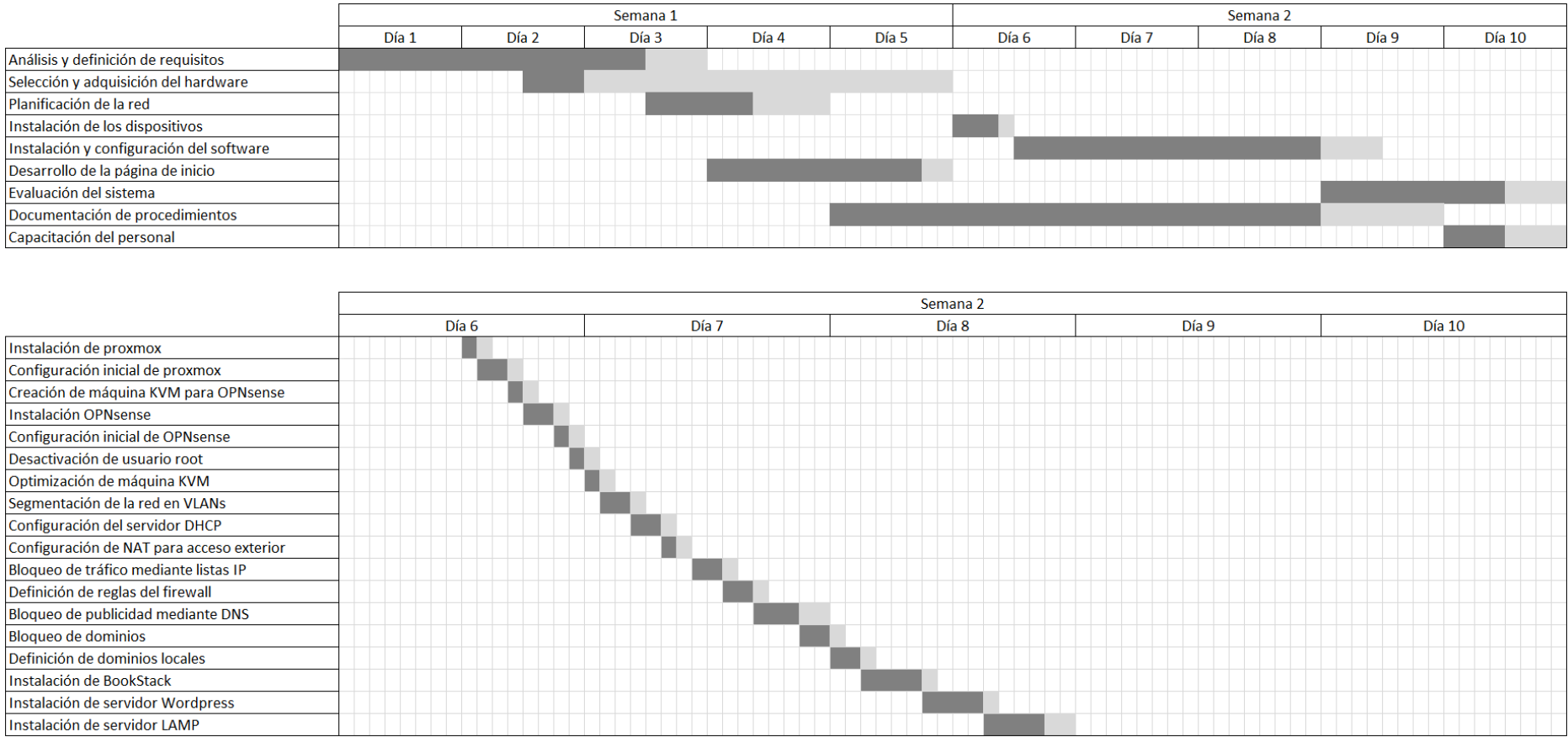


Gráfico 1 -Diagrama de Gantt

## Memoria técnica

### Planificación de la red

La red consistirá en dos VLAN gestionadas por el router principal. En la VLAN 1 se encuentran los clientes de la red local, los cuales obtendrán la configuración IP a través del servidor DHCP de la red.

En la VLAN 2 se encuentran los servidores Apaches, WordPress y BookStack. En la red física puede haber más servidores, que se tendrán que conectar a la VLAN 2 mediante un Switch 802.1q correctamente configurado.

El ordenador tendrá dos tarjetas de red, una de ellas conectada al router de la operadora, haciendo la función de interfaz WAN y la otra al switch, haciendo la fusión de interfaz LAN, por la que circulará el tráfico de las dos VLAN.

El esquema de la red será el siguiente:

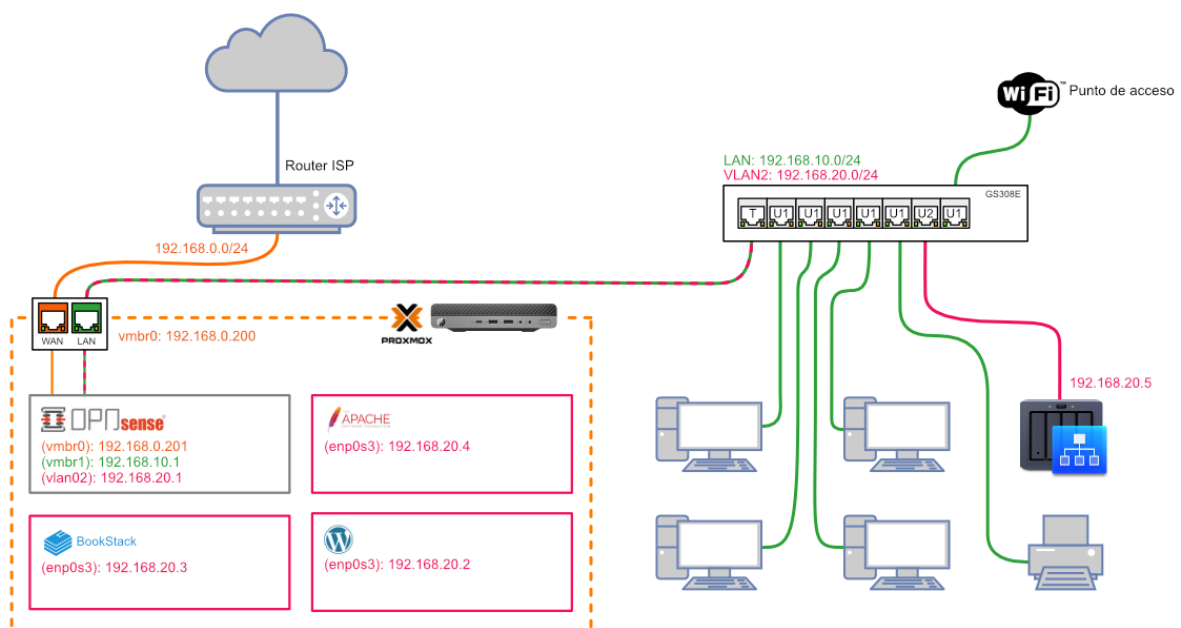


Gráfico 2 – Esquema de la red

Las direcciones IP en la red serán las siguientes:

VLAN1:	192.168.10.0/24
VLAN2:	192.169.20.0/24
<hr/>	
Proxmox:	192.168.10.200
OPNsense:	192.168.10.1
	192.168.20.1
Srv. DNS:	192.168.10.1
Wordpress:	192.168.20.2
BookStack:	192.168.20.3
Apache:	192.168.20.4

### Adquisición de materiales

El hardware escogido dependerá en cada caso de las necesidades de la empresa y de si se puede reutilizar algo de lo que ya tenga en propiedad. Para la realización práctica de este proyecto se ha escogido el siguiente equipo:

#### **Ordenador**

HP ProDesk 600 G4, miniordenador con 16GB de ram, 256GB de disco sólido y procesador i5 8500T en formato de 1L.



*Ilustración 1 - HP Prodesk 600 G4*

#### **Tarjeta de red**

Dado que el PC escogido sólo dispone de una tarjeta de red y no es posible añadir otra internamente, se ha escogido la tarjeta de red TP-Link UE300 con conexión USB 3.2 compatible con Gigabit Ethernet.



*Ilustración 2 - TP-Link Adaptador UE300 USB*

## **Switch**

Se ha escogido un Netgear gestionable GS308E Gigabit Ethernet de 8 puertos, ya que es compatible con el protocolo 802.1q necesario si se van a utilizar VLANs en la red.

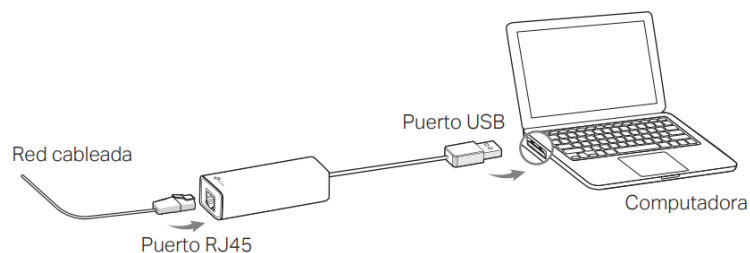


*Ilustración 3 – Switch gestionable GS308E*

## **Instalación del sistema**

### ***Instalación de tarjeta de red adicional***

La instalación de la tarjeta de red USB es Plug & Play y es reconocida directamente por Proxmox sin necesidad de drivers adicionales.



*Ilustración 4 - Instalación de tarjeta de red externa*

### ***Instalación de Proxmox***

En primer lugar instalaremos la plataforma de virtualización sobre la que correrá el sistema operativo de firewall (OPNsense) y el resto de los servicios.

Descargamos la última versión de Proxmox 7.4 de su web oficial y cargamos la ISO en un pendrive de arranque configurado con YUMI o similar

```
https://proxmox.com/en/downloads  
https://www.pendrivelinux.com/yumi-multiboot-usb-creator/
```

Arrancamos el equipo desde el pendrive. Para el modelo escogido, la tecla para seleccionar el dispositivo de arranque es F9, mientras que la de acceso a la BIOS es F10.

Una vez arrancado desde el pendrive seguimos el asistente de instalación, introduciendo los siguientes datos cuando nos los solicite:

```
Contraseña: asir23  
Host Name: pve.home  
IP: 192.168.0.200  
Puerta de enlace: 192.168.0.1  
Servidor DNS: 192.168.0.1
```

### ***Configuración inicial de Proxmox***

**Configuración de repositorios:** El repositorio que viene configurado por defecto en Proxmox es el “pve-enterprise” el cual no sirve sin una suscripción de pago activa. Para poder actualizar el sistema de forma gratuita hay que cambiarlo por el repositorio “No-Subscription” en la sección pve > Updates > Repositories

**Configuración de hardware de red:** Hay que asegurarse de que ambas tarjetas de red son reconocidas por el sistema y están correctamente configuradas. Durante la instalación de Proxmox sólo se configuró una tarjeta de red, por lo que será necesario configurar la segunda añadiendo un nuevo “Linux Bridge” desde la sección pve > System > Network con IP 192.168.10.200/24

Create ▾	Revert	Edit	Remove	Apply Configuration				
Name ↑	Type	Ac...	Au...	VL...	Ports/Slaves	B...	CIDR	Gateway
eno1	Network Device	Yes	No	No				
enx30de4b5e27fc	Network Device	Yes	No	No				
vmbr0	Linux Bridge	Yes	Yes	Yes	enx30de4b5e27fc		192.168.0.200/24	192.168.0.1
vmbr1	Linux Bridge	Yes	Yes	Yes	eno1		192.168.10.200/24	

Captura 1 – Configuración de las interfaces de red en Proxmox

Creación de máquina KVM para OPNsense

Una vez configurado Proxmox pasamos a crear la máquina KVM que ejecutará OPNsense. Lo primero es conocer los requisitos mínimos de instalación (Requisitos mínimos, s.f.) (Virtualizacion, s.f.) para poder configurarla correctamente.

CPU: 2 núcleos a 1 GHz RAM: 1 GB
-------------------------------------

Subimos la ISO de OPNsense al almacenamiento del nodo de Proxmox, que podemos descargar de su web oficial.

<a href="https://opnsense.org/download/">https://opnsense.org/download/</a>
---

Storage 'local' on node 'pve'					Help
Summary	Upload	Download from URL	Remove	Search: Name, Format	
Backups					
ISO Images	Name	Date	Format	Size	
CT Templates	OPNsense-23.1-OpenSSL-dvd-amd64.iso	2023-05-07 20:19:34	iso	1.64 GB	
Permissions	pSense-CE-2.6.0-RELEASE-amd64.iso	2023-05-07 20:19:56	iso	767.46 MB	

Captura 2 – Carga de la ISO de instalación de OPNsense en Proxmox

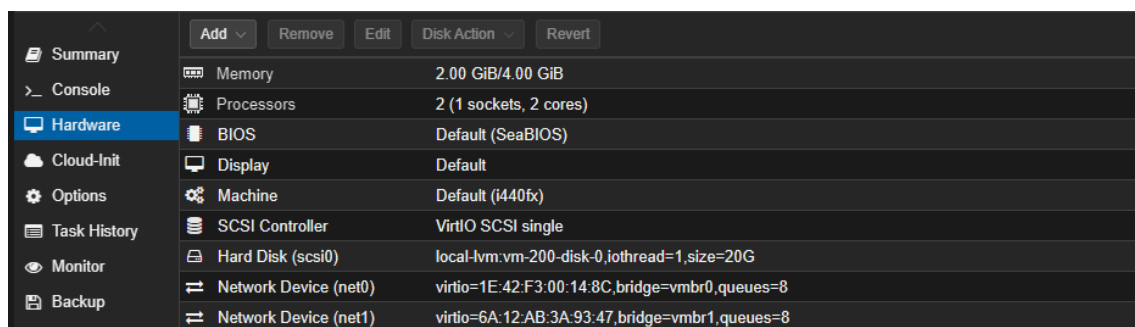
Ahora hay que crear una máquina KVM (Ahmed, 2014, pág. 303)con los siguientes datos:

ID: 200 Nombre: OPNsense ISO: OPNsense.iso Disco: 20GB, IO Thread Cores: 2 Memoria: 4096MB Sin interfaz de red
--



Una vez creada, seleccionamos la máquina KVM y vamos a configuración de hardware para terminar de configurar las tarjetas de red. Añadimos las dos interfaces de red que ha detectado Proxmox (Linux Bridges) como tarjetas de red tipo VirtIO con la siguiente configuración:

```
Bridge: vmbr0, vmbr1
Firewall: no
Model: virtio
Multiqueue: 8
```



Captura 3 – Configuración de Hardware de la KVM

## Instalación de OPNsense

Iniciamos el sistema desde la imagen ISO, lo que cargará el asistente de configuración de OPNsense. Nos pregunta si deseamos configurar LAGs (Agregación de links) y VLANs. Le decimos que no.

```
Press any key to start the manual interface assignment: 4
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

Captura 4 – Asistente de configuración de OPNsense

Nos presenta un listado con las interfaces de red detectadas y nos pregunta cuál de ellas queremos definir como WAN y cual como LAN. Seleccionamos vtneto como WAN configurada mediante DHCP, ya que es la que está conectada a la salida del router del operador. Seleccionamos vtnet1 como interfaz LAN.

```
The interfaces will be assigned as follows:  
WAN -> vtnet0  
LAN -> vtnet1  
Do you want to proceed? [y/N]:
```

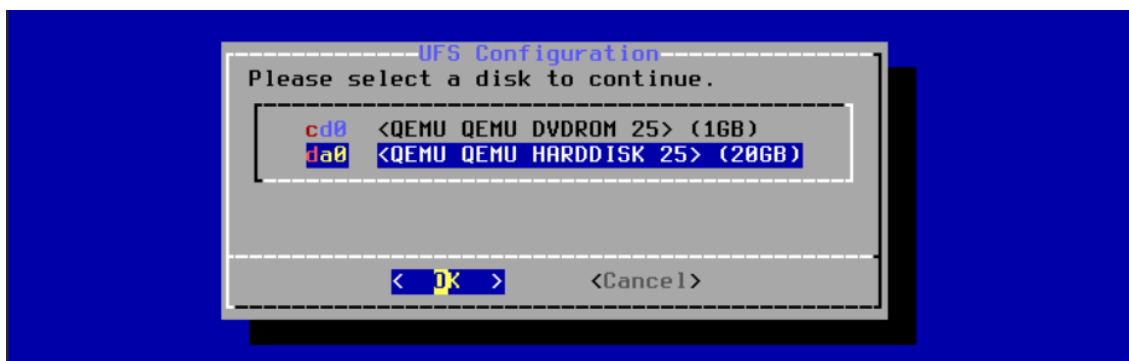
*Captura 5 - Confirmación de la asignación de las interfaces de red*

Una vez configurado nos presenta un resumen con los datos de acceso y la opción de continuar como LiveCD o instalar el sistema en el disco interno. Iniciamos sesión con el usuario installer y password opnsense para que comience el proceso.

```
Welcome! OPNsense is running in live mode from install media. Please  
login as 'root' to continue in live mode, or as 'installer' to start the  
installation. Use the default or previously-imported root password for  
both accounts. Remote login via SSH is also enabled.  
  
FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)  
login:
```

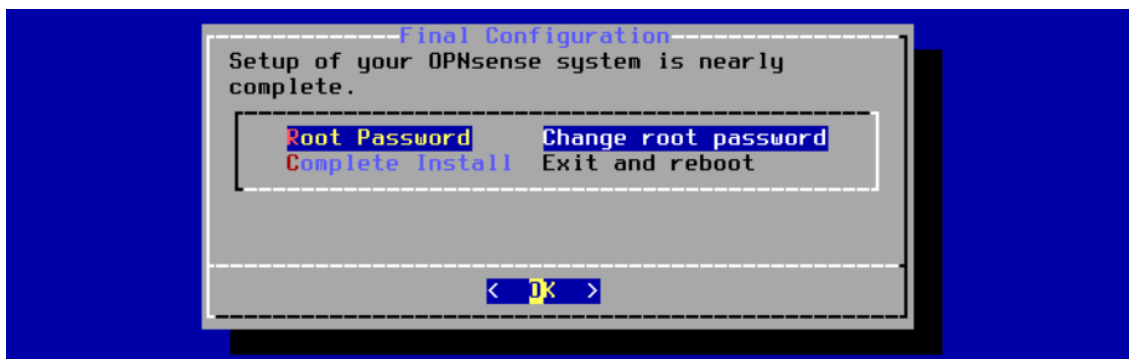
*Captura 6 - Bienvenida a OPNsense en modo liveCD*

Seleccionamos un sistema de ficheros para el disco. En nuestro caso UFS. Seleccionamos el disco de instalación y confirmamos la operación:



*Captura 7 - Selección de disco de destino*

Cuando termine nos da la opción de cambiar la contraseña de root por una más segura. Podemos completar la instalación directamente, ya que desactivaremos el usuario root más adelante como medida de seguridad.

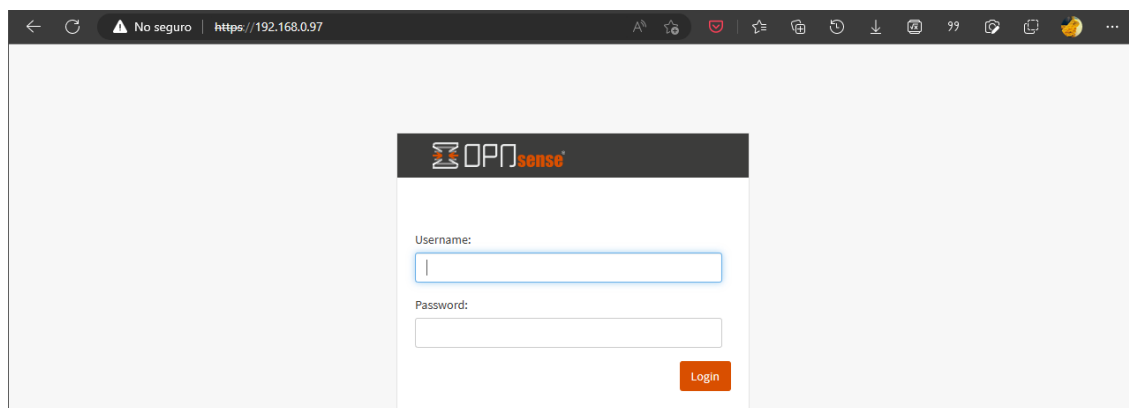


*Captura 8 – Fianlización del proceso de instalación*

A partir de este momento podemos eliminar la imagen ISO de la máquina virtual y continuar la configuración desde el navegador accediendo a la IP mostrada por consola.

### ***Configuración inicial de OPNsense***

Cuando accedemos a OPNsense vía navegador web, nos mostrará un formulario de acceso donde tendremos que poner el usuario y contraseña. Si no lo cambiamos en el paso anterior, el usuario será root y la contraseña OPNsense.



*Captura 9 – Portal de autenticación a la versión Web de OPNsense*

Para completar la configuración básica, nos podemos ayudar del asistente de configuración al que podemos acceder en System > Wizard

**System: Wizard: General Setup**

This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Next

*Captura 10 – Asistente de configuracion inicial*

Seguimos el asistente con el fin de configurar los siguientes parámetros:

DNS Primario: 208.67.222.222  
DNS Secundario 208.27.220.220  
Timezone: Europe/Madrid  
WAN: DHCP  
Dirección IP (LAN): 192.168.10.1/24

**Información General:** En la primera página establecemos principalmente el nombre del host y las direcciones de los servidores DNS primario y secundario, así como el lenguaje del sistema

Servidor DNS Primario:	<input type="text" value="208.67.222.222"/>
Servidor DNS Secundario:	<input type="text" value="208.67.220.220"/>

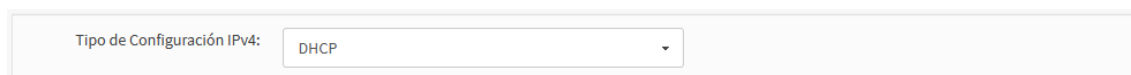
*Captura 11 – Configuración básica*

**Información Servidor de Tiempo:** Aquí podemos dejar los servidores por defecto o definir unos personalizados, así como establecer la zona horaria.

Nombre de host de servidor de tiempo:	<input type="text" value="0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2...."/>
Introduzca el nombre de host (FQDN) del servidor de tiempo.	
Zona Horaria:	<input type="text" value="Europe/Madrid"/>

*Captura 12 – Configuración del servidor ntp*

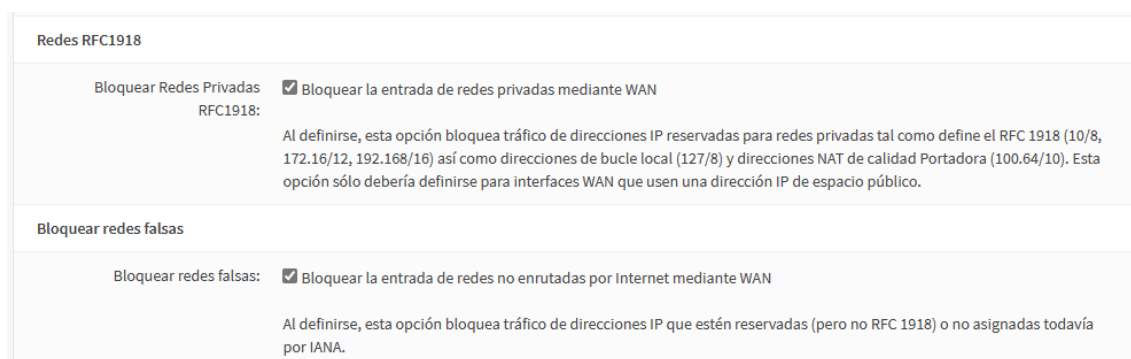
**Configurar Interfaz WAN:** La interfaz WAN la podemos dejar configurada en DHCP, de forma que sea el router del operador el que le asigne la configuración de red.



Tipo de Configuración IPv4: DHCP

*Captura 13 – Configuración de la interfaz wan en modo DHCP*

Por motivos de seguridad dejaremos marcadas las dos últimas casillas, que bloquearán el tráfico proveniente de redes privadas externas.



Redes RFC1918

Bloquear Redes Privadas RFC1918: ☒ Bloquear la entrada de redes privadas mediante WAN

Al definirse, esta opción bloquea tráfico de direcciones IP reservadas para redes privadas tal como define el RFC 1918 (10/8, 172.16/12, 192.168/16) así como direcciones de bucle local (127/8) y direcciones NAT de calidad Portadora (100.64/10). Esta opción sólo debería definirse para interfaces WAN que usen una dirección IP de espacio público.

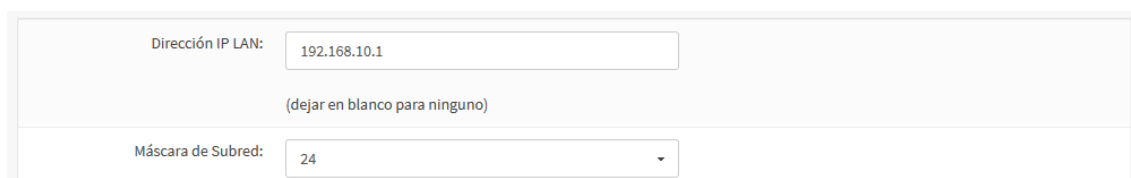
Bloquear redes falsas

Bloquear redes falsas: ☒ Bloquear la entrada de redes no enrutadas por Internet mediante WAN

Al definirse, esta opción bloquea tráfico de direcciones IP que estén reservadas (pero no RFC 1918) o no asignadas todavía por IANA.

*Captura 14 – Opciones de seguridad para la WAN*

**Configurar interfaz LAN:** Establecemos la dirección IP que tendrá OPNsense en la red local, así como la máscara de subred, que define el tamaño de la red.



Dirección IP LAN: 192.168.10.1

(dejar en blanco para ninguno)

Máscara de Subred: 24

*Captura 15 – Configuración de la red LAN*

**Cambio de contraseña de root:** Opcionalmente podemos cambiar la contraseña del usuario root antes de terminar el asistente. Como vamos a desactivar el usuario root, no será necesario cambiar nada.

### ***Desactivación de usuario root***

Por motivos de seguridad, vamos a sustituir el usuario root por un usuario administrador con un nombre de usuario menos obvio. Para ello vamos a Sistema >

Acceso > Usuarios y pulsamos el botón [+] para añadir un usuario nuevo (Camargo, 2022, pág. 113).

Nombre de usuario: opn\_admin  
Contraseña: asir23  
Grupo: admins

The screenshot shows a user creation form with the following fields and options:

- Nombre de usuario:** A text input field containing "opn\_admin".
- Contraseña:** Two password input fields, both containing "asir23". The second field is labeled "(confirmación)".
- ☐ Genere una contraseña codificada para evitar el inicio de sesión en la base de datos local para este usuario.

*Captura 16 – Creación de usuario*

The screenshot shows the "Membresías de Grupos" (Group Memberships) section. It features two lists of groups:

- No Miembro de:** An empty list box.
- Miembro de:** A list box containing the group "admins".

Between the two lists are two arrows: a right-pointing arrow (→) and a left-pointing arrow (←), used to move groups between the lists.

*Captura 17 – Asignación de usuario al grupo administrador*









Cerramos sesión de root e iniciamos sesión con el nuevo usuario. Volvemos al administrador de usuarios y editamos el usuario root para deshabilitarlo.

The screenshot shows the configuration for the "root" user. The fields are as follows:

- Definido por:** SYSTEM
- Deshabilitado:** A checkbox that is checked (☑).
- Nombre de usuario:** A text input field containing "root".

*Captura 18 – Deshabilitación de cuenta de usuario*

Una vez guardado debería quedar así en la lista de usuarios. De esta forma un usuario malintencionado tendrá más difícil iniciar sesión, ya que el nombre de usuario no es el que viene por defecto.

Nombre de usuario	Nombre completo	Grupos	
 opn_admin	Administrador	admins	 
 root	System Administrator	admins	
 Administrador de Sistema  Usuario Deshabilitado  Usuario Normal			

Captura 19 – Listado de usuarios

Optimización de la máquina KVM

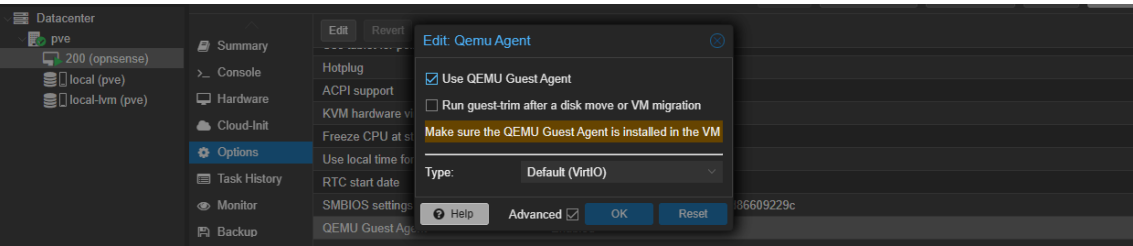
Podemos mejorar el rendimiento de la máquina virtual activando una serie de parámetros tanto en el propio OPNsense como el Proxmox.

**Qemu-guest-agent:** Lo primero que podemos hacer es habilitar el agente para máquinas virtuales QEMU. Es un plugin que se puede activar en Sistema > Firmware > Complementos

Estado	Ajustes	Registro de cambios	Actualizaciones	Complementos	Paquetes
Nombre		Versión	Tamaño	Repository	Comentar
os-qemu-guest-agent (instalado)		1.2	19.0KiB	OPNsense	QEMU Guest Agent for OPNsense
os-acme-client		3.17	714KiB	OPNsense	ACME Client

Captura 20 – Plugin Qemu Agenta habilitado

Ahora nos vamos a Proxmox y activamos “Qemu Guest Agent” en las opciones de la máquina virtual. Una vez activado, reiniciamos la máquina virtual.



Captura 21 – Configuración de Qemu Agent en la máquina KVM de proxmox

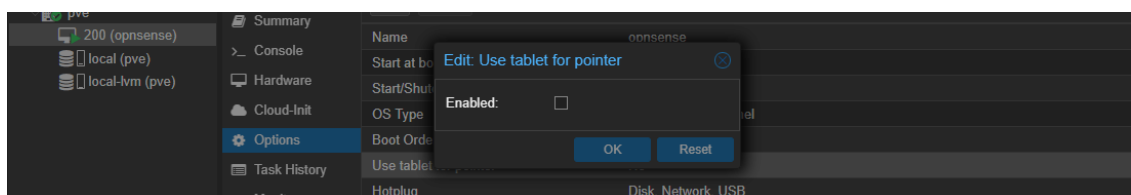
Si se ha activado correctamente, ahora debería aparecer una nueva entrada llamada “QEMU Guest Agent” en el menú “Servicios” de OPNsense.

Si al iniciar el sistema, el servicio QEMU Guest Agent no se inicia automáticamente, es posible que el parámetro `virtio_console_load` esté desactivado. Lo podemos activar en Sistema > Ajustes > Parámetros Optimizables (Qemu Guest Agent, s.f.)

Parámetro Ajustable	<input type="text" value="virtio_console_load"/>
Descripción	<input type="text"/>
Valor	<input type="text" value="YES"/>

*Captura 22 – Configuración de parámetros optimizables*

**Desactivar «Use tablet for pointer»:** Desactivando este parámetro en las opciones de la máquina KVM, es posible ganar algo de rendimiento en la CPU (`good_tips_for_opnsense`, s.f.)



*Captura 23 – Desactivación de puntero de tablet en la máquina KVM*

**Desactivar hardware offloading en OPNsense:** En Interfaces > Ajustes es conveniente comprobar que Hardware CRC, Hardware TSO y Hardware LRO están deshabilitados, ya que las interfaces VirtIO pueden causar problemas si estos parámetros se encuentran activados.

Interfaces de Red	
Hardware CRC	<input checked="" type="checkbox"/> Desactivar el hardware de descarga de suma de comprobación
Hardware TSO	<input checked="" type="checkbox"/> Desactivar hardware de descarga de segmentación TCP
Hardware LRO	<input checked="" type="checkbox"/> Deshabilitar la descarga de gran recepción por hardware

*Captura 24 – Desactivación de offloading por hardware en OPNsense*

**Actualización del sistema:** Para un correcto funcionamiento es conveniente mantener el sistema operativo actualizado. Podemos forzar una actualización desde el



menú Sistema > Firmware > Estado pulsando en el botón «Comprobar actualizaciones del sistema».

Estado	Ajustes	Registro de cambios	Actualizaciones	Complementos	Paquetes
Escribir	opnsense				
Versión	23.1.7_3				
Architecture	amd64				
Commit	b084e7458				
Mirror	<a href="https://pkg.opnsense.org/FreeBSD:13:amd64/23.1">https://pkg.opnsense.org/FreeBSD:13:amd64/23.1</a>				
Repositories	OPNsense				
Updated on	Sun May 14 14:44:44 CEST 2023				
Checked on	N/A				
<div><div> Comprobar actualizaciones</div><div> Run an audit ▼</div></div>					

Captura 25 – Estado y versión del sistema

Estado	Ajustes	Registro de cambios	Actualizaciones	Complementos	Paquetes
<pre> [23/31] Fetching mpd5-5.9_16.pkg: ..... done [24/31] Fetching php81-ldap-8.1.19.pkg: ..... done [25/31] Fetching php81-xml-8.1.19.pkg: ... done [26/31] Fetching php81-pdo-8.1.19.pkg: ..... done [27/31] Fetching php81-curl-8.1.19.pkg: ..... done [28/31] Fetching php81-mbstring-8.1.19.pkg: ..... done [29/31] Fetching qemu-guest-agent-8.0.0.pkg: ..... done [30/31] Fetching opnsense-23.1.8.pkg: ..... done [31/31] Fetching php81-gettext-8.1.19.pkg: . done Checking integrity... done (0 conflicting)           </pre>					

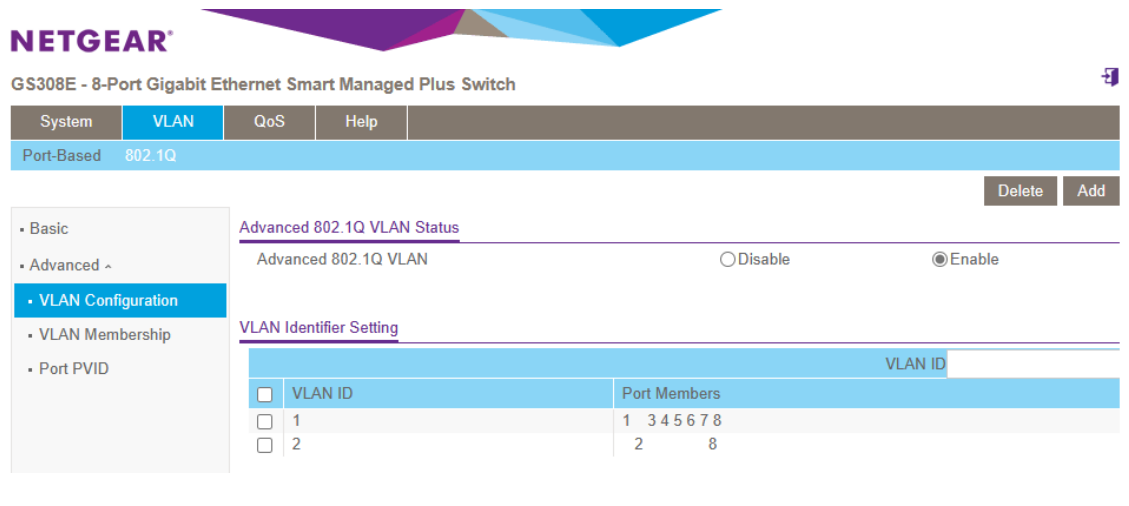
Captura 26 – Actualización del sistema

## Segmentación de la red mediante VLAN

Vamos a segmentar la red en dos mediante VLAN. La red por defecto (VLAN 1) para los dispositivos de los usuarios y la VLAN 2 dos para los servidores. Necesitaremos realizar configuraciones tanto en el switch como en el router.

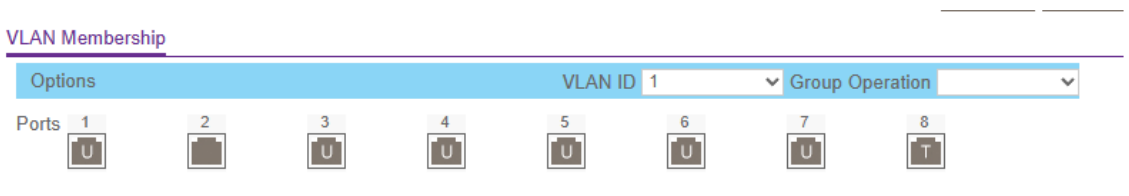
### Configuración del switch

En el Switch configuraremos como se van a distribuir los distintos puertos Ethernet y sus características. Accedemos a la interfaz de gestión y creamos la VLAN 2



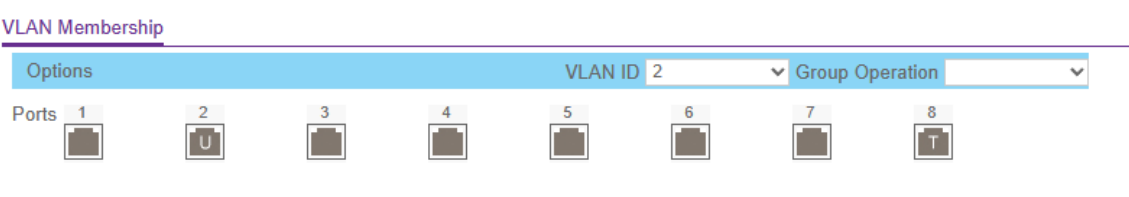
Captura 27 – Interfaz de configuración de VLAN 802.1Q en el switch NETGEAR

En la configuración de la VLAN1 quitamos el puerto 2 y marcamos el puerto 8 como troncal.



Captura 28 - Configuración de tipo de puertos para la VLAN 1

En la configuración de la VLAN2, dejamos todos los puertos sin marcar excepto el 2 que lo macamos como untagged y el 8 que lo marcamos como troncal



Captura 29 - Captura 30 - Configuración de tipo de puertos para la VLAN 1

Por último, en la configuración de los puertos marcamos el puerto 2 como perteneciente a la VLAN 2 para que el tráfico sin marcar que pase por ahí se considere tráfico perteneciente a la VLAN 2..

PVID Configuration

<input type="checkbox"/>	Port	PVID
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	2
<input type="checkbox"/>	3	1
<input type="checkbox"/>	4	1
<input type="checkbox"/>	5	1
<input type="checkbox"/>	6	1
<input type="checkbox"/>	7	1
<input type="checkbox"/>	8	1

Captura 31 – Asignación VLANs a los puertos físicos

Configuración de la VLAN en OPNsense

Es en el router donde se crean y configuran las VLAN. Crearemos una única VLAN destinada a separar los servidores del resto de la red empresarial.

**Creación de la VLAN:** Para configurar una VLAN en OPNsense primero hay que definirla. Para ello vamos a Interfaces > Otros > VLAN y pulsamos el botón «+»

Crearemos una VLAN con los siguientes datos:

Parent: vtnet1 [LAN]  
Etiqueta: 2  
Prioridad: 0

<input type="checkbox"/>	Device	Parent	Etiqueta	PCP	Descripción	Comandos
<input type="checkbox"/>	vlan02 [OPT2]	vtnet1 (6a:12:ab:3a:93:47) ...	2	Mejor Esfuerzo (0, por defe...	vlan2	<div><div></div><div></div><div></div></div>

Captura 32 – Listado de VLANs en OPNsense

**Asignar una VLAN a un puerto de red:** En Interfaces > Asignaciones asignamos la nueva interfaz (Camargo, 2022, pág. 92) que se ha creado a uno de los puertos físicos del ordenador. En nuestro caso lo asignaremos al puerto vlano2 vlan2 que se encuentra vinculado a la interfaz vtnet1

Interfaz (ID ⓘ)	Puerto de red	
<u>LAN</u> (lan)	vtnet1 (6a:12:ab:3a:93:47) ▼	
<u>OPT2</u> (opt2)	vlan02 vlan2 (Parent: vtnet1, Tag: 2) ▼	
<u>WAN</u> (wan)	vtnet0 (1e:42:f3:00:14:8c) ▼	
<b>Guardar</b>		

*Captura 33 – Asignación de interfaces*

**Activación de la interfaz:** Finalmente, buscamos la nueva interfaz que aparecerá en el menú Interfaces y entraremos para terminar de configurarla. Marcamos la casilla de Habilitar y asignamos una IP estática a la interfaz. La red de los servidores será la 192.168.20.0/24 por lo que le asignaremos la 192.168.20.1

ⓘ Tipo de Configuración IPv4	IPv4 Estática ▼
ⓘ Tipo de Configuración IPv6	Ninguno ▼

Configuración Estática IPv4	
ⓘ Dirección IPv4	192.168.20.1 24 ▲
ⓘ Puerta de Enlace de Subida IPv4	Auto-detectar ▼ +

*Captura 34 – Configuración de la Interfaz virtual*

En este punto la VLAN está creada y configurada, aunque aún faltan algunas configuraciones que se completarán en los apartados dedicados al DHCP y al firewall.

## Configuración del servidor DHCP

El servidor DHCP es un servicio de red fundamental que se puede encontrar en prácticamente todos los router comerciales. Su principal función es asignar de manera automática direcciones IP y configuraciones de red a los dispositivos que se conectan a la red sobre la que tiene autoridad.

En OPNsense se puede configurar desde el menú Servicios > DHCPv4 > [LAN] (Manual de DHCP, s.f.).

**Configuración del servidor dedicado a la red VLAN1**

La red LAN será configurada con los siguientes parámetros:

Rango:	192.168.10.10 – 192.168.10.245
DNS Srv:	192.168.10.1
Puerta de enlace:	192.168.10.1

The screenshot shows the configuration interface for the DHCP server for VLAN1. It consists of three main sections:

- Rango (Range):** A section with a label 'Rango' and two input fields. The first field is labeled 'de' (from) and contains the value '192.168.10.10'. The second field is labeled 'hacia' (to) and contains the value '192.168.10.245'.
- Servidores DNS (DNS Servers):** A section with a label 'Servidores DNS' and a single input field containing the value '192.168.10.1'.
- Puerta de Enlace (Gateway):** A section with a label 'Puerta de Enlace' and a single input field containing the value '192.168.10.1'.



*Captura 35 – Configuración del servidor DHCP para la red LAN*

**Configuración del servidor DHCP de la red VLAN2**

El servidor DHCP para la VLAN2 se configura igual que el de la red LAN, aunque con los parámetros descritos a continuación. El servidor DNS será el mismo en las dos redes.

Rango:	192.168.20.10 – 192.168.20.200
DNS Srv:	192.168.10.1
Puerta de enlace:	192.168.20.1

Como esta red está dedicada a servidores, es interesante asignar IP estática a cada uno de los equipos. Podemos añadir asignaciones de IP estáticas a equipos conocidos pulsando en el símbolo «+» al final de la página de configuración del servidor DHCP, aunque una opción más cómoda es ir al apartado Servicios > DHCPv4 > Arrendamientos y hacer estático el equipo deseado si ya se ha conectado a la red. Esto se consigue pulsando en el símbolo «+» que aparece al su lado.

Mapeos DHCP Estáticos para esta interfaz.					
ARP Estática	Dirección MAC	Dirección IP	Nombre host	Descripción	+
	90:2b:34	192.168.20.2	DESKTOP-V9L		 

*Captura 36 – Mapeos DHCP estáticos*

Como se puede observar, cuando el equipo con la MAC definida en las tablas se conecta a la red, el servidor DHCP le asigna la configuración IP asociada.

```

Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . : localdomain
Vínculo: dirección IPv6 local. . . : fe80::8b47:93b8:cce7:8eda%10
Dirección IPv4. . . . . : 192.168.20.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.20.1

```

*Captura 37 – Comprobación del servidor DHCP desde un cliente*

## Acceso externo

Una de las formas de dar acceso a un equipo de la red local desde el exterior es la traducción de direcciones de red o NAT (Camargo, 2022, pág. 182), que usaremos para que se pueda acceder al servidor apache de la máquina con IP 192.168.20.2 por el puerto 8080.

## Configuración de NAT

En Cortafuegos > NAT > Redirección de puerto creamos una nueva regla que tenga como objetivo la IP 192.168.20.2 y el puerto 80, para un rango de puertos de un único puerto (8080) y con destino la dirección de la WAN (192.168.0.201)

Destino

WAN dirección

Rango de puertos destino

de:

para:

(otro)

(otro)

8080

8080

IP objetivo de redirección

Host único o Red

192.168.20.2

Puerto de Redirección Objetivo

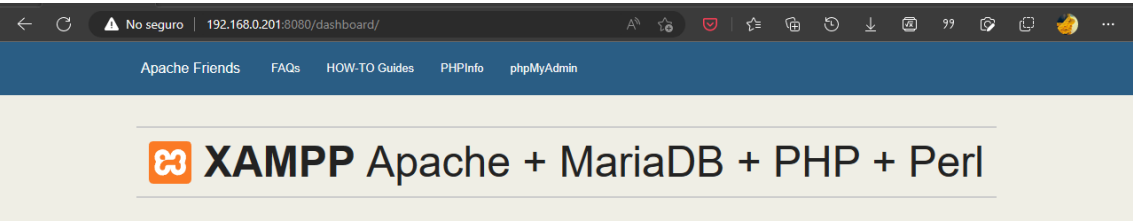
HTTP

Captura 38 – Configuración de regla NAT para dar acceso a un servidor

Origen					Destino		NAT							
<input type="checkbox"/>	Interfaz	Proto	Dirección	Puertos	Dirección	Puertos	IP	Puertos	Descripción					
	LAN	TCP	*	*	Dirección LAN	22, 80, 443	*	*	Regla Anti-Bloqueo					
<input type="checkbox"/>	 WAN	TCP	*	*	WAN dirección	8080	192.168.20.2	80 (HTTP)						
	Regla habilitada				No redireccionar				Regla vinculada					
	Regla deshabilitada				Deshabilitado no redirigir				Regla enlazada deshabilitada					
	Alias (clic para ver/editar)													

Captura 39 – Listado de reglas NAT activas

Si accedemos a la dirección 192.168.0.201:8080 desde el navegador de un equipo conectado al router de la operadora (exterior de la red), cargará la web alojada en el servidor apache.



Captura 40 – Comprobación de la regla NAT

Bloqueo y seguridad

Una de las funciones principales de un router/firewall es controlar que sólo se realizan conexiones legítimas. Para este proyecto nos vamos a centrar en bloquear conexiones conocidas por ser malignas, evitar en la medida de lo posible la publicidad al navegar por la web y el bloqueo de webs vetadas por la empresa.

***Bloqueo de tráfico malicioso mediante listas IP***

Bloquear IPs es una forma simple y efectiva de prevenir que se realicen conexiones con direcciones que son conocidas por ser maliciosas. De esta forma si un equipo se ve comprometido, el malware no será capaz de comunicarse con el atacante.

Bloquear IPs a mano sería una tarea impracticable, por lo que es útil recurrir al uso de listas creadas por la comunidad o por organizaciones que se dedican a recopilar este tipo de IPs y bloquearlas en conjunto.

**Crear un alias para las listas de bloqueo externas:** Gracias a los alias es posible utilizar listas de bloqueo externas para utilizar en las reglas de firewall. El primer paso es crear un alias para la lista de bloqueo y seleccionar como tipo "URL Table (IPs)". Es útil crear un alias separado para cada tipo de lista de bloqueo, ya que nos permitirá tener más control sobre el intervalo de actualización estado de activación de cada uno de ellos (IP blocklists, s.f.). Las listas de bloqueo son ficheros de texto plano que podemos obtener de diversas fuentes. En nuestro caso utilizaremos las del proyecto Spamhouse:

```
https://www.spamhaus.org/drop/drop.txt  
https://www.spamhaus.org/drop/edrop.txt  
https://www.spamhaus.org/drop/droptv6.txt
```

Creamos un alias en Cortafuegos > aliasess pulsando el botón «+» y rellenamos los datos que nos pida. En «Escribir» seleccionamos «Tabla URL» y ponemos la lista de URLs de las listas de bloqueo escogidas.



Habilitado

☒

Nombre

Baneados

Escribir

Tabla URL (IPs)

Categories

malware

Refresh Frequency

Días

0

Horas

12.00

Contenido

https://www.spamhaus.org/drop/drop.txt

https://www.spamhaus.org/drop/edrop.txt

https://www.spamhaus.org/drop/dropv6.txt

Limpiar todo

Copy

Paste

Estadísticas




☒

Descripción

Spamhouse

Captura 41 – Creación de un alias para el firewall

Si le damos a la lista un nombre en mayúscula aparecerá por encima del resto de listas creadas por OPNsense.

<input type="checkbox"/>	Habilit...	Nombre	Escribir	Descrip...	Contenido	Loaded#	Actualiz...	Comandos
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Baneados	Tabla URL (IPs)	Spamhouse	https://ww...	1335	2023-05-29...	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	bogons	Externa (avanzado)	bogon net...		10		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Baneados	Externa (avanzado)	Baneados		70		

Captura 42 – Listado de alias configurados en el firewall

**Crear reglas de bloqueo en el firewall:** Como queremos bloquear completamente las IP contenidas en el Alias que acabamos de crear podemos crear una regla flotante, lo que quiere decir que no está vinculada a ninguna de las interfaces de red y se aplicará a todas.

Creamos una regla flotante tipo «Bloquear» para las interfaces WAN y LAN que filtre cualquier protocolo. Como destino seleccionamos el alias «Baneados» y activamos el registro de paquetes.



Reglas de firewall

En una empresa puede darse el caso de que se quiera que uno o varios equipos de la red no sean capaces de establecer conexión con otros equipos de otra red de la empresa. Por ejemplo, impedir que uno de los ordenadores se conecte al servidor de datos.

Las reglas de firewall pueden servir para este propósito. Como prueba vamos a crear una regla que impida todo el tráfico saliente de uno de los PC de la red LAN (192.168.10.10) que tenga como destino el servidor Proxmox (192.168.0.200) situado en el lado WAN de OPNsense.

Para ello crearemos una regla LAN con origen en 192.168.10.10/32 y destino 192.168.0.200/32 de tipo «Bloquear» y la situamos por encima de las reglas que vienen predefinidas.

<input type="checkbox"/>				IPv4 *	192.168.10.10	*	192.168.0.200	*	*	*				
<input type="checkbox"/>				IPv4 *	LAN red	*	*	*	*	*	Default allow LAN to any rule			
<input type="checkbox"/>				IPv6 *	LAN red	*	*	*	*	*	Default allow LAN IPv6 to any rule			

Captura 46 – Regla para impedir el tráfico de un equipo a otro

Si ahora intentamos hacer ping desde el PC al servidor veremos como el Firewall está bloqueando la conexión.

```
sojel ~ 23:48 ping 192.168.0.200

Haciendo ping a 192.168.0.200 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

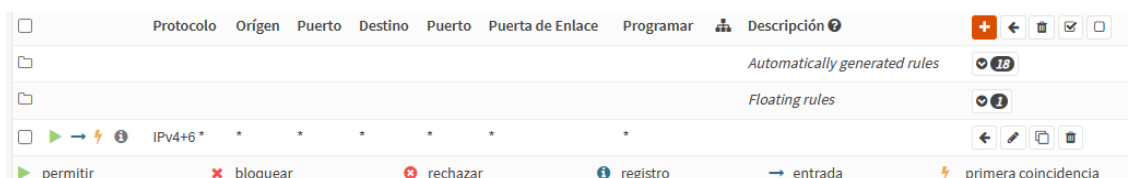
Estadísticas de ping para 192.168.0.200:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),
```

Captura 47 – Intento de Ping a un equipo bloqueado por el firewall

Interfaz	Tiempo	Origen	Destino	Proto	Etiqueta	
lan	→ 2023-05-29T23:50:56	192.168.10.10	192.168.0.200	icmp		
wan	← 2023-05-29T23:50:52	fe80::1c42:f3ff:fe00:148c	fe80::628d:26ff:fe31:1583	ipv6-icmp	IPv6 RFC4890 requirements (ICMP)	
wan	→ 2023-05-29T23:50:52	fe80::628d:26ff:fe31:1583	fe80::1c42:f3ff:fe00:148c	ipv6-icmp	IPv6 RFC4890 requirements (ICMP)	
lan	→ 2023-05-29T23:50:51	192.168.10.10	192.168.0.200	icmp		
lan	→ 2023-05-29T23:50:46	192.168.10.10	192.168.0.200	icmp		
lan	→ 2023-05-29T23:50:41	192.168.10.10	192.168.0.200	icmp		
wan	← 2023-05-29T23:50:37	192.168.0.200:58855	192.168.10.10:7443	tcp	Initiating outgoing from Firewall host itself (source ip)	

*Captura 48 – Conexiones rechazadas por el firewall*

**Dar acceso a internet a los equipos de la VLAN2:** Como queremos que los equipos conectados a la VLAN2 tengan acceso a internet, hay que crear una regla que permita todo el tráfico IPv4 desde cualquier origen y a cualquier destino. Una vez creada la regla los equipos conectados a esa red tendrán conectividad a internet.

*Captura 49 – Regla para dar acceso a internet a la VLAN2*

### ***Bloqueo de publicidad y webs maliciosas***

Una forma muy eficiente de bloquear la publicidad de las páginas web y proteger a los empleados de intentos de phishing y otro software malintencionado es bloquear las conexiones antes de que ocurran en el navegador del usuario. De esta forma se incrementa de forma notable el rendimiento de los navegadores, ya que reduce enormemente la cantidad de conexiones que tienen que realizar por cada web a la que acceden. Si esto lo combinamos con extensiones de navegador que terminen de bloquear lo que pueda haber pasado el filtro DNS (código javascript destinado a mostrar anuncios y popups) los usuarios de la red podrán tener una experiencia de navegación mucho más satisfactoria y rápida.

Existen listas mantenidas por la comunidad de urls conocidas por servir anuncios, malware y phishing, las cuales podemos cargar en un servidor DNS con el fin de bloquearlas.

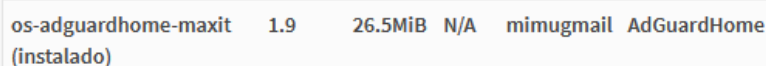
Aunque es posible añadir dichas listas al servidor nativo de OPNsense (Unbound DNS), el complemento ADGUARD es mejor opción, ya que permite gestionarlas de forma más sencilla a la vez que ofrece detalladas estadísticas de uso.



**Instalación del repositorio:** Para la instalación del complemento es necesario instalar el repositorio en el que se encuentra mediante consola de comandos. Para poder acceder a la consola hay que cambiar las configuraciones descritas en el apartado o, ya que el acceso se encuentra desactivado por defecto.

Lo podemos instalar ejecutando los siguientes comandos:

```
sudo fetch -o /usr/local/etc/pkg/repos/mimugmail.conf  
pkg update
```

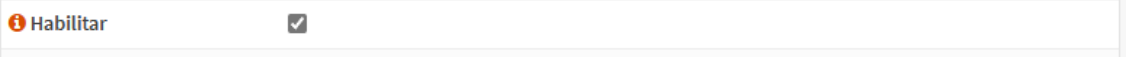
**Instalación del complemento:** Si se ha instalado correctamente el repositorio, ahora debería aparecer el complemento os-ADGUARDhome-maxit en la lista que se muestra en el apartado sistema > firmware > complementos




os-adguardhome-maxit (instalado)	1.9	26.5MiB	N/A	mimugmail	AdGuardHome	 
-------------------------------------	-----	---------	-----	-----------	-------------	---

*Captura 50 – Complemento activo*

Lo activamos en servicios > ADGUARDhome > General



 Habilitar ☒

*Captura 51 – Habitación de ADGUAD en OPNsense*

**Desactivación del servidor DNS nativo:** Antes de continuar es conveniente dejar libre el puerto 53 desactivando el servicio Unbound DNS, ya que ADGUARD intentará hacer uso de él. Se puede desactivar en Servicios > Unbound DNS > General desmarcando la casilla «Habilitar Unbound»

**Configuración del servidor DHCP:** Para que los clientes que se conecten a la red no tengan que realizar ninguna configuración adicional, cambiaremos la dirección del servidor DNS primario configurado en el servidor DHCP de OPNsense por la de ADGUARD, que coincide con la IP del propio OPNsense.



*Captura 52 – Configuración DNS en el servidor DHCP*

**Configuración inicial de ADGUARD:** Nos conectamos a la IP de OPNsense desde el navegador por el puerto 3000. Se abrirá el asistente de configuración. En la interfaz de administración ponemos la red interna, para evitar accesos desde el exterior y dejamos el puerto 3000 que viene por defecto.



*Captura 53 – Configuración de interfaz web de ADGUARD*

Configuraremos el servidor DNS para que sólo escuche las peticiones realizadas desde la red interna por el puerto 53.



*Captura 54 - Configuración de interfaz de escucha para ADGUARD*

Por último nos pide que configuremos un usuario par el acceso al panel de control web.

```
usuario: agh_admin
contraseña: asir2023
```

Una vez iniciemos sesión, nos mostrará un resumen con todas las estadísticas uso.



Captura 55 – Panel de estadísticas de ADGUARD

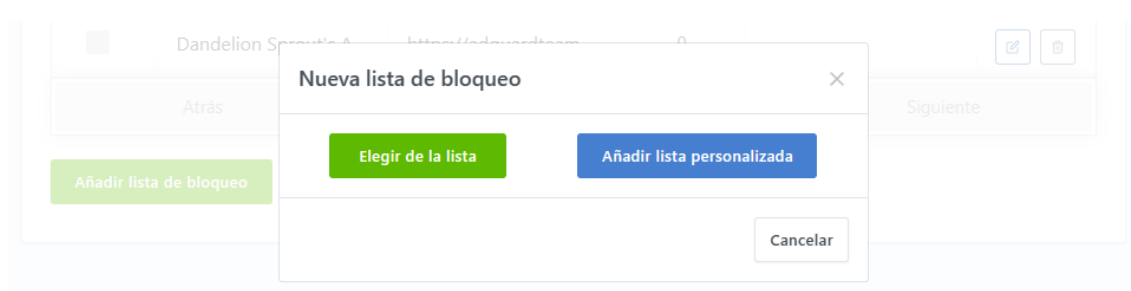
**Listas de bloqueo de publicidad:** Por defecto ADGUARD viene con dos listas configuradas, aunque sólo una de ellas se encuentra activa. Podemos activar las dos y añadir más pulsando el botón «Añadir lista de bloqueo»

AdGuard Home entiende las reglas básicas de bloqueo y la sintaxis de los archivos hosts.

Habilitado	Nombre	URL de la lista	Número de r...	Última actualización	Acciones
<input checked="" type="checkbox"/>	AdGuard DNS filter	https://adguardteam....	53.870	29 de mayo de 2023,...	
<input checked="" type="checkbox"/>	AdAway Default Bloc...	https://adguardteam....	6550	29 de mayo de 2023,...	

Captura 56 – Listas de bloqueo por defecto

Si las listas que vienen configuradas por defecto se nos quedan cortas siempre podemos recurrir a listas mantenidas por terceros pulsando en «Añadir lista personalizada» y poniendo la URL de la lista a insertar.



Captura 57 – Añadir listas de bloqueo

Un buen recurso donde empezar a buscar nuevas listas es «The Big Blocklist Collection» en el siguiente enlace:

<https://firebog.net/>

**Listas de bloqueo de webs maliciosas:** Si queremos que ADGUARD bloquee las webs conocidas por tener malware, podemos añadir las listas predefinidas en Filtros > Listas de bloqueo DNS > Añadir lista de bloqueo > Elegir de la lista y hacer scroll hasta el final, donde encontraremos la sección seguridad.



*Captura 58 – Listas especializadas en bloquear malware y phishing*

### ***Bloqueo de dominios por DNS***

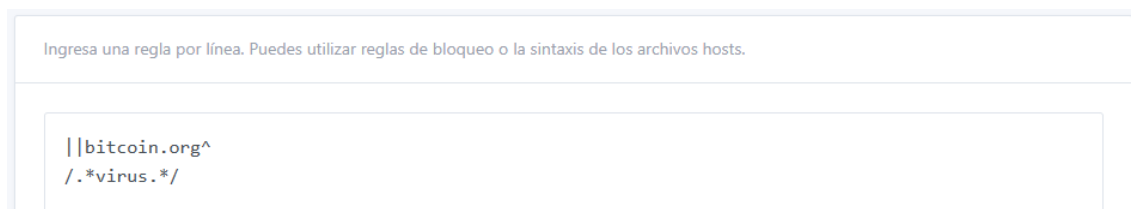
El bloqueo de webs es una funcionalidad importante para muchas empresas. OPNsense ofrece varias formas de conseguir este objetivo, desde configurar un proxy caché transparente hasta filtrado por DNS.

El proxy transparente es la forma más segura de evitar que los usuarios se salten el bloqueo a la vez que permite bloquear por tipo de contenido, como ejecutables o ficheros comprimidos. Si embargo hoy en día es cada vez más común que el tráfico sea encriptado, lo que dificulta la configuración en modo transparente a la vez que puede dar problemas en muchas webs.

Por ello vamos a configurar el bloqueo de webs con el mismo método que hemos usado para bloquear la publicidad, aunque sólo permita bloqueo a nivel de dominio.

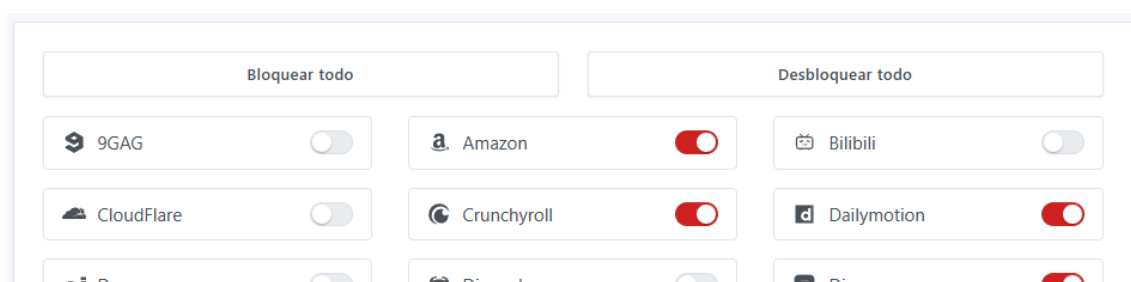
En el menú Filtros > Reglas de filtrado personalizado de ADGUARD podemos definir las reglas que queramos. Por ejemplo, bloquearemos el dominio y subdominios de bitcoin.com y cualquier dominio que contenga la palabra “virus”





*Captura 59 – Bloqueo de dominios por DNS*

Para bloquear servicios más conocidos, el menú Filtros > Servicios bloqueados permite bloquear una serie de servicios predefinidos de forma sencilla.



*Captura 60 – Bloqueo de servicios por DNS*

## Otros

### ***DNS local***

En una organización puede ser útil asignar una serie nombres de dominio a las IPs locales de ciertos equipos de la red para facilitar el acceso a los servicios que ofrecen. Esto se puede conseguir mediante la reescritura de DNS, disponible tanto desde el propio OPNsense en el apartado Servicios > Unbound DNS > Sobrescribir o desde ADGUARD en flitros > Reescritura DNS. Como estamos utilizando ADGUARD como servidor DNS, usaremos este último.



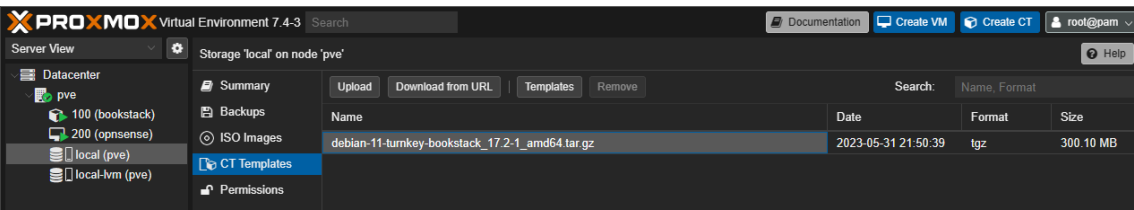
Captura 61 – Reescritura de dominios para uso en local

**Servicios de red adicionales: BookStack**

La principal ventaja de utilizar OPNsense dentro de Proxmox, es que este último permite añadir otros servicios a la red de forma fácil y rápida haciendo uso del hardware ya existente.

Vamos a suponer que la empresa necesita una plataforma tipo wiki para documentar de forma centralizada sus procesos, tareas e información interna de la empresa.

Nos valdremos de los contenedores predefinidos que incluye Proxmox (Ahmed, 2014, pág. 370). En Datacenter > pve > local (pve) > CT Templates descargamos la plantilla turnkey-bookstack para instalar una instancia de BookStack.



Captura 62 – Lista de plantillas de contenedores descargadas en Proxmox

Ahora creamos un nuevo contenedor de nombre bookstack y contraseña asir23 basado en la plantilla que acabamos de descargar.

Node:	pve	Resource Pool:	
CT ID:	101	Password:	*****
Hostname:	bookstack	Confirm password:	*****
Unprivileged container:	<input checked="" type="checkbox"/>	SSH public key:	

*Captura 63 – Creación del contenedor para bookStack*

Le asignamos 8GB de disco, 1 cores y 1024MB de RAM. La memoria SWAP la ponemos a 0 para evitar reducir la vida del SSD del anfitrión. En la configuración de red le asignamos la interfaz puente vmbr1, con la etiqueta VLAN 2 y dirección IP 192.168.20.3/24.

Name:	enp0s3	IPv4:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC address:	auto	IPv4/CIDR:	192.168.20.3/24
Bridge:	vmbr1	Gateway (IPv4):	192.168.20.1
VLAN Tag:	2	IPv6:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> SLAAC

*Captura 64 – Configuración de la red del contenedor en la VLAN 2*

Una vez creado accedemos por consola con el usuario root y la contraseña asir23 para iniciar un asistente de configuración donde nos pedirá la contraseña del administrador (Asir2023) de Bookstack y a continuación un correo ([admin@bookstack.local](mailto:admin@bookstack.local)) que hará las funciones de nombre de usuario.

En el siguiente paso nos pide un dominio para el servicio. La dirección que pongamos aquí la tendremos que configurar en la reescritura de DNS de nuestro servidor DNS.

Enter schema and domain to use for BookStack.
<input type="text" value="https://bookstack.local"/>

*Captura 65 – Configuración del dominio local en el asistente de instalación*

Reescrituras DNS

Permite configurar fácilmente la respuesta DNS personalizada para un nombre de dominio específico.

Dominio	Respuesta	Acciones
opnsense.local	192.168.10.1	
proxmox.local	192.168.0.200	
bookstack.local	192.168.20.3	

Captura 66 – Asignación de IP al dominio local en el servidor DNS

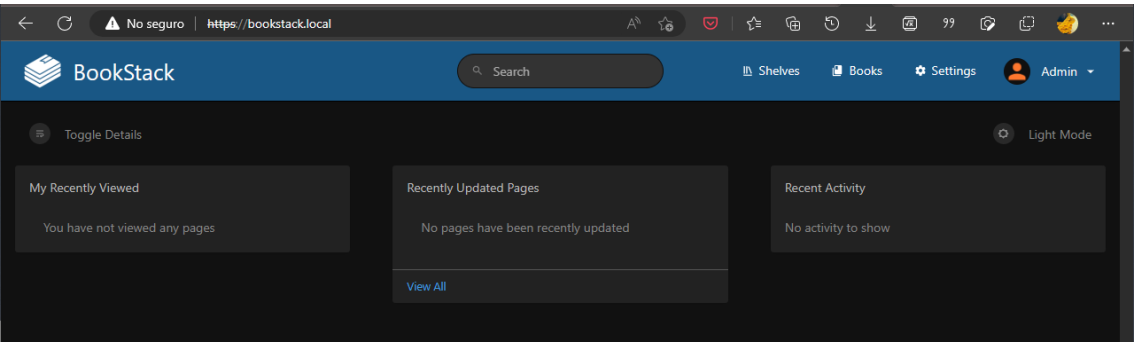
Los siguientes pasos los podemos saltar, por lo que continuamos hasta finalizar el asistente.

```
BOOKSTACK appliance services

Web:      http://192.168.20.3
          https://192.168.20.3
Web shell: https://192.168.20.3:12320
Webmin:   https://192.168.20.3:12321
Adminer:  https://192.168.20.3:12322
SSH/SFTP: root@192.168.20.3 (port 22)
```

Captura 67 – Resumen del asistente de instalación

Probamos a acceder desde un equipo de la red e iniciamos sesión con las credenciales que acabamos de configurar. Si todo ha ido bien, cargará la página principal de BookStack.



Captura 68 – Panel de inicio de BookStack

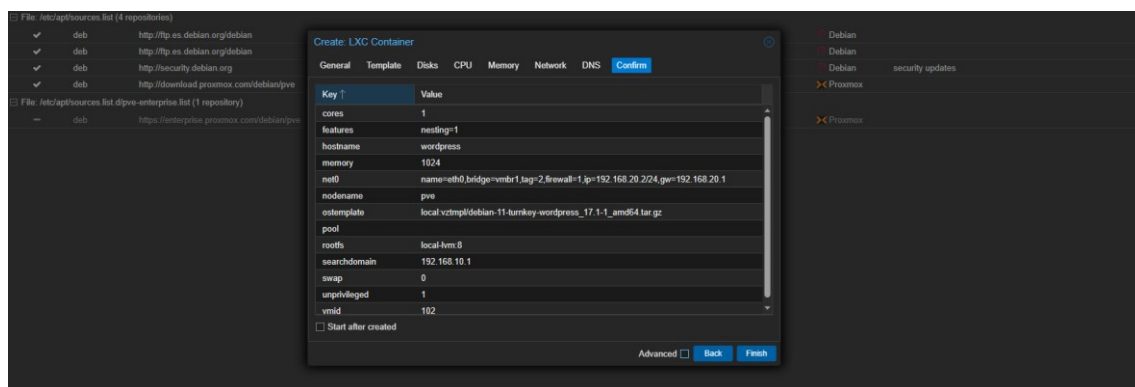
**Servicios de red adicionales: Wordpress**

De la misma manera, podemos instalar un servidor apache con Wordpress. Descargamos la plantilla turnkey-wordpress y procedemos a crear un contenedor a partir de ella con los siguientes datos:

```

usuario CT:      root
contraseña CT:   asir23
Plantilla:       debian-11-turnkey-wordpress_17.1-1_amd64.tar.gz
Disco:           8GB
Núcleos CPU:     1
Memoria:         1GB
Swap:            0MB
Bridge:          vmbr1
VLAN Tag:        2
IP:              192.168.20.2/24
Gateway:         192.168.20.1
DNS:             192.168.10.1

```



*Captura 69 – Configuración de contenedor para Wordpress*


Ahora toca instalar y configurar Wordpress. Usaremos los siguientes datos:

```

usuario CT:      admin@wordpress.local
contraseña CT:   Asir2023#

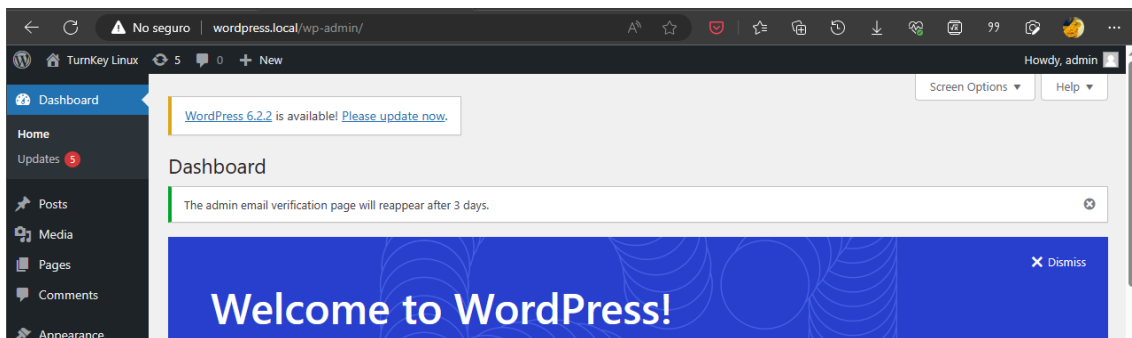
```

Configuraremos en la reescritura de DNS el dominio wordpress.local para que apunte a la dirección del contenedor:

wordpress.local	192.168.20.2	
-----------------	--------------	---

*Captura 70 – Reescritura de DNS a nivel local*

Si accedemos desde el navegador se abrirá la página de Wordpress, pudiendo acceder al panel de administración con el usuario y contraseña configurados.



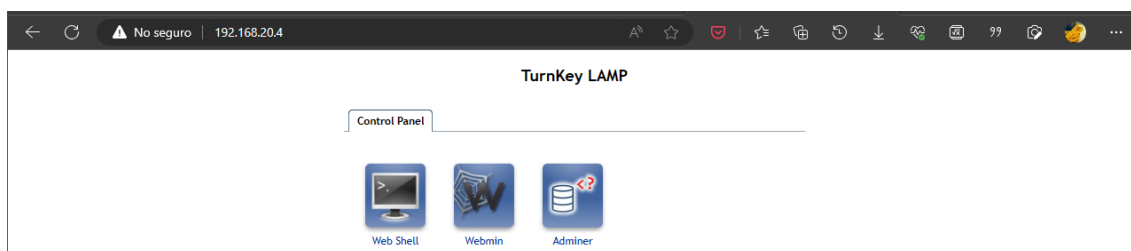
*Captura 71 – Página de administración de Wordpress*

### ***Servicios de red adicionales: Servidor Apache***

Para alojar una página de inicio con enlaces a todos los servicios crearemos un servidor apache virtual. Empezamos creando un servidor lamp con ayuda de las plantillas de contenedores que incluye Proxmox, igual que hemos hecho para los anteriores servicios. Los datos para la configuración son los siguientes:

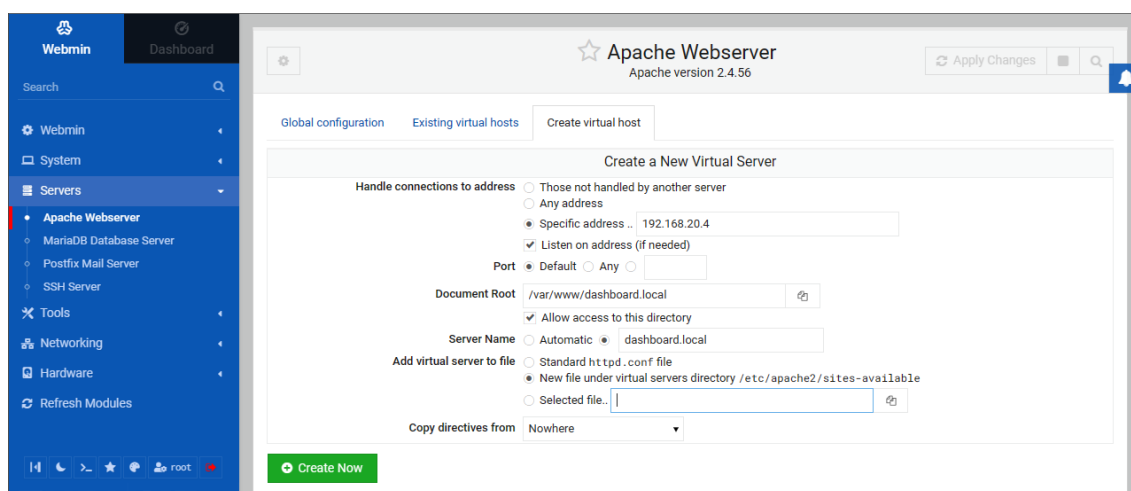
```
usuario CT:      root
contraseña CT:   asir23
Plantilla:       debian-11-turnkey-lamp_17.1-1_amd64.tar.gz
Disco:           8GB
Núcleos CPU:     1
Memoria:         1GB
Swap:            0MB
Bridge:          vmbr1
VLAN Tag:        2
IP:              192.168.20.4/24
Gateway:         192.168.20.1
DNS:             192.168.10.1
Password Tk:     Asir2023#
```

Una vez instalado, accedemos a la ip del servidor desde el navegador y se abrirá la interfaz de webmin. Necesitamos crear y configurar el servidor virtual de apache donde alojar la web.



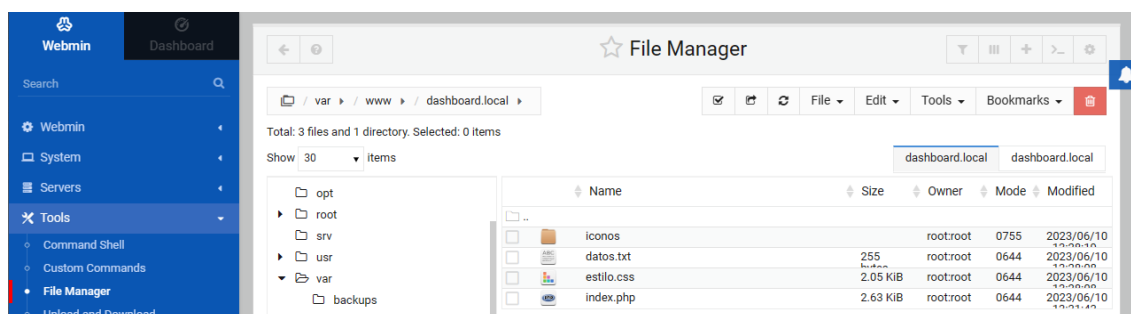
Captura 72 – Panel de control del contenedor Turnkey LAMP

Abrimos webmin y vamos a servers > Apache Webserver para crear un nuevo host virtual con los datos que se ven en la imagen.



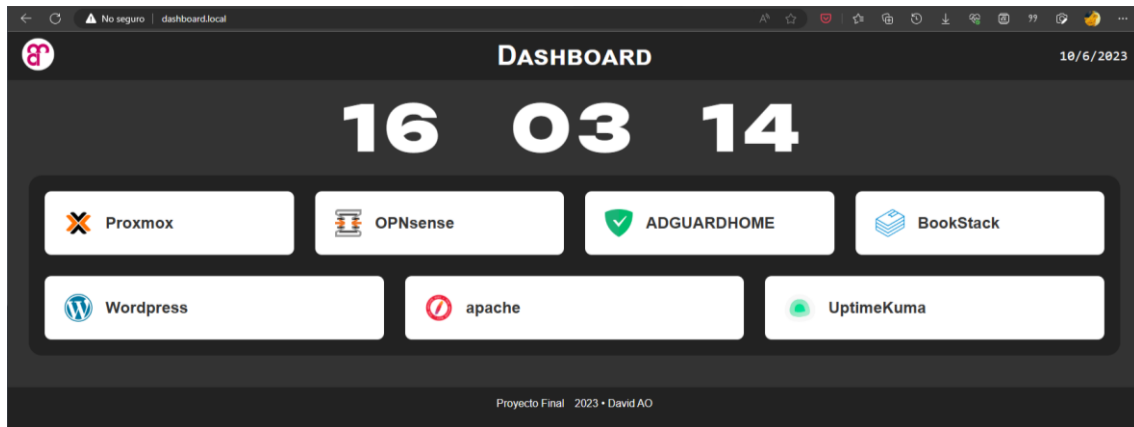
Captura 73 – Creación de un host virtual de Apache

Una vez configurado y activo, vamos al gestor de ficheros de webmin para subimos los ficheros que forman la página de inicio. El código php que forma en la página de inicio se puede ver en la sección Desarrollo de la página de inicio a medida.



Captura 74 – Administrador de archivos de Webmin

Cuando entremos desde el navegador nos mostrará una página con enlaces a todos los servicios disponibles en la red interna.



*Captura 75 – Página de inicio a medida*

## Desarrollo de la página de inicio a medida

Puede ser útil para la empresa disponer de una web interna corporativa con enlaces a los distintos servicios de la red para un rápido acceso a los mismos.

La página de inicio que se va a desarrollar mostrará enlaces en forma de cuadrícula de los servicios que la compañía decida, tanto servicios de la red interna como enlaces a recursos web que puedan resultar de utilidad a los trabajadores.

Para facilitar la modificación de los enlaces mostrados, se van a listar en un fichero .txt dentro del servidor. Un servicio por línea, con nombre y url separados por punto y coma de la siguiente forma:

```
Proxmox;https://proxmox.local:8006
OPNsense;https://192.168.10.1
ADGUARDHOME;http://192.168.10.1
BookStack;http://bookstack.local
Wordpress;http://wordpress.local/wp-admin
apache;https://dashboard.local:12321/
UptimeKuma;http://uptimekuma.local:3001
```

El código PHP leerá el fichero e insertará los enlaces en el código HTML de forma dinámica. Además se mostrará la fecha y la hora actuales mediante javascript.

```
<!DOCTYPE html>
<html lang="en">
  <?php
    $filename = "datos.txt";
```



```

$file = @fopen($filename, 'r');

if ($file) {
    $array = explode("\n", fread($file, filesize($filename)));
}

foreach ($array as $clave=>$linea) {
    $array[$clave] = explode(";", $linea);
}

?>
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<!-- ===== ESTILOS ===== -->
<link rel="stylesheet"
href="https://fonts.googleapis.com/css?family=Crimson+Text|Work+Sans:40
0,700">
-->
<link rel="stylesheet" href="./estilo.css">
<!-- ===== OTROS ===== -->
<title>Dashboard</title>
<script type="text/javascript">
    window.addEventListener('DOMContentLoaded', () => {
        setInterval(tiempo, 1000);
        function tiempo() {
            tiempo = new Date();
            fecha = tiempo.toLocaleDateString();
            horas = tiempo.getHours();
            minutos = tiempo.getMinutes();
            segundos = tiempo.getSeconds();
            document.getElementById("fecha").innerHTML = fecha;
            document.getElementById("hora").innerHTML = ("0" + horas).slice(-2);
            document.getElementById("minuto").innerHTML = ("0" +
minutos).slice(-2);
            document.getElementById("segundo").innerHTML = ("0" +
segundos).slice(-2);
        }
    });
</script>
</head>
<body>

<header>
<div class="hlogo">

</div>
<div>
<h1>Dashboard</h1>
</div>
<div class="fechahora">
<div id="fecha"></div>
</div>
</header>
<div class="hora">
<div id="hora"></div>
<div id="minuto"></div>
<div id="segundo"></div>
</div>
<div id="cont_dinamico">
<?php foreach($array as $linea): ?>
<a class="servicio" href="<?=$linea[1]; ?>">

<h2 class="nombre"><?=$linea[0]; ?></h2>
</a>

```

```

        <?php endforeach; ?>
    </div>
    <footer>
        <p>Proyecto Final</p>
        <p>2023 &#8226; David A0</p>
    </footer>
</body>
</html>

```

Por último, la hoja de estilos CSS para darle un estilo visualmente atractivo:

```

@import url('https://fonts.googleapis.com/css2?family=Unbounded:wght@900&display=swap');

body {
    background-color: #333;
    font-family: Arial, Helvetica, sans-serif;
    color: #fff;
    margin: 0px;
}

header {
    height: 3.5em;
    background-color: #222;
    display: flex;
    align-items: center;
    flex-wrap: nowrap;
    justify-content: space-between;
    padding: 0 1em;
    font-size: 1.3rem;
}

header .hlogo {
    width: 10em;
    display: block;
}

header img {
    width: 50px;
}

header .fechahora {
    width: 10em;
    text-align: right;
    font-family: monospace;
}

header h1 {
    border-left: 50px;
    font-variant: small-caps;
    text-align: center;
}

.hora {
    width: 100%;
    font-family: Unbounded;
    height: 1.5em;
    display: flex;
    align-items: center;
    justify-content: center;
    padding: 0 20%;
    font-size: 6rem;
    font-weight: 900;
    text-align: center;
    gap: 5rem;
}

.hora div {

```

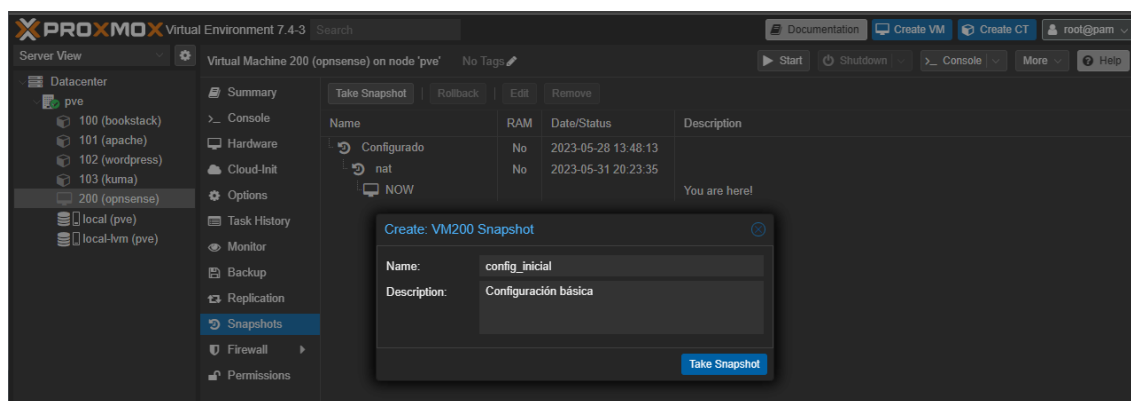
```
width:2em;
letter-spacing: 0.1em;
}
#cont_dinamico {
display:flex;
background-color: #222;
margin: 0 2rem;
border-radius: 20px;
padding: 0.5em;
flex-wrap: wrap;
align-content: flex-start;
position: relative;
}
#cont_dinamico .servicio {
flex: 20em;
flex-wrap: nowrap;
height: 3.5em;
margin: 1em;
background-color: #fff;
padding: 20px;
border-radius: 10px;
vertical-align: middle;
padding-left: 30px;
display:flex;
color:#333;
text-decoration: none;
align-items: center;
}
#cont_dinamico .logo {
height: 75%;
}
#cont_dinamico .nombre {
display: inline-block;
vertical-align: middle;
margin-left: 20px;
}
footer {
background:#222;
margin-top: 3rem;
display:flex;
align-items: center;
flex-wrap: nowrap;
justify-content: center;
box-shadow: 0 50vh 0 50vh #222;
gap:1rem;
}
footer p {
display:block;
}
```

## Seguimiento y control

### Instantáneas

Una vez se ha configurado todo el sistema y comprobado que todo funciona correctamente, se harán instantáneas de cada una de las máquinas virtuales para poder revertir la configuración a una que se sabe que funciona en caso de que algo falle.

Se pueden hacer instantáneas desde Proxmox en la sección Snapshots de cada una de las máquinas.



*Captura 76 – Creación de una instantanea*

### Evaluación del rendimiento

El dispositivo no sería de utilidad si empeorase el rendimiento de la red de forma significativa. Por ello se han hecho pruebas de velocidad con y sin OPNsense entre el ordenador y el router del operador.

**Livebox Fibra Sagemcom F@st 5656**

FECHA / HORA	PING ms	DESCARGA Mbps	SUBIDA Mbps	DISTANCIA km	UBICACIÓN / SERVIDOR	PROVEEDOR
05/28/2023 2:42 PM	18 31 21	592.77	628.40	~ 150	Sevilla Orange Servidores adicionales utilizados para la prueba de descarga	Orange

*Captura 77 – Test de velocidad y latencia conectado al router de la operadora***HP Prodesk 8500T (OPNsense)**

FECHA / HORA	PING ms	DESCARGA Mbps	SUBIDA Mbps	DISTANCIA km	UBICACIÓN / SERVIDOR	PROVEEDOR
05/28/2023 2:40 PM	19 32 22	590.33	629.87	~ 150	Sevilla Orange Servidores adicionales utilizados para la prueba de descarga	Orange

*Captura 78 - Test de velocidad y latencia conectado al router OPNsense*

Como se puede apreciar en las pruebas, la diferencia de rendimiento tanto en velocidad como en latencia no es significativa.

**Evaluación del consumo eléctrico**

Otro aspecto a tener en cuenta es el consumo eléctrico, ya que se trata de un dispositivo que estará conectado 24h al día durante años. Si el consumo fuese muy elevado podría incrementar demasiado el coste de operación haciendo más atractivas otras alternativas comerciales de menor consumo.

Durante el año 2022 el precio medio del kWh fue de 0.19€ (Precio medio de la electricidad en 2022, s.f.), lo que nos permitirá calcular el coste económico que supone tener el router conectado durante todo el año.

**Livebox Fibra Sagemcom F@st 5656**

Se ha puesto un medidor de consumo en el enchufe de alimentación del router y se le ha dado un uso normal durante 24h. Los resultados son los siguientes:

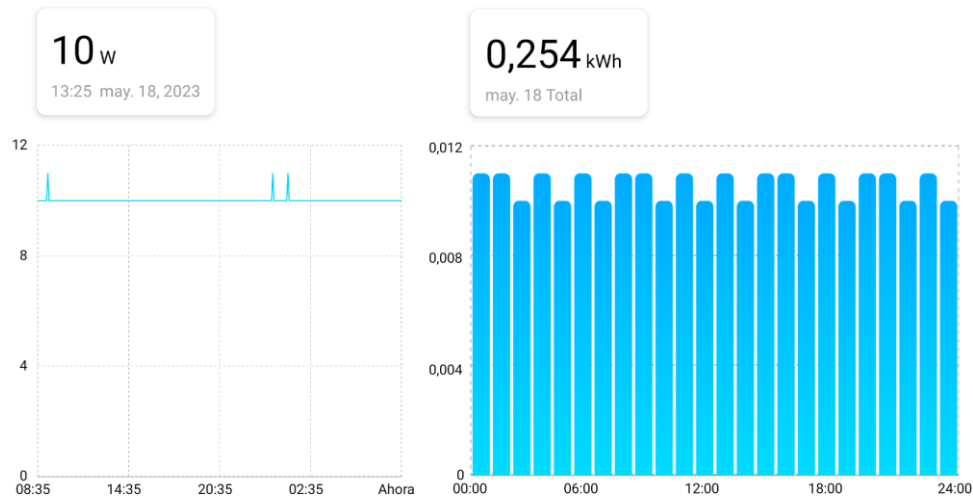


Gráfico 3 - Gráficas del consumo instantáneo y acumulado en 24h

Coste anual en 2022 utilizando un el router suministrado por la operadora de internet Orange:

$$0.254 \text{ kwh/d} * 365 \text{ d} * 0.19 \text{ €/kwh} = 17.62 \text{ €}$$

### **HP Prodesk 8500T**

Se ha puesto un medidor de consumo en el enchufe de alimentación del pc y se le ha dado un uso normal como router durante 24h. Los resultados son los siguientes:

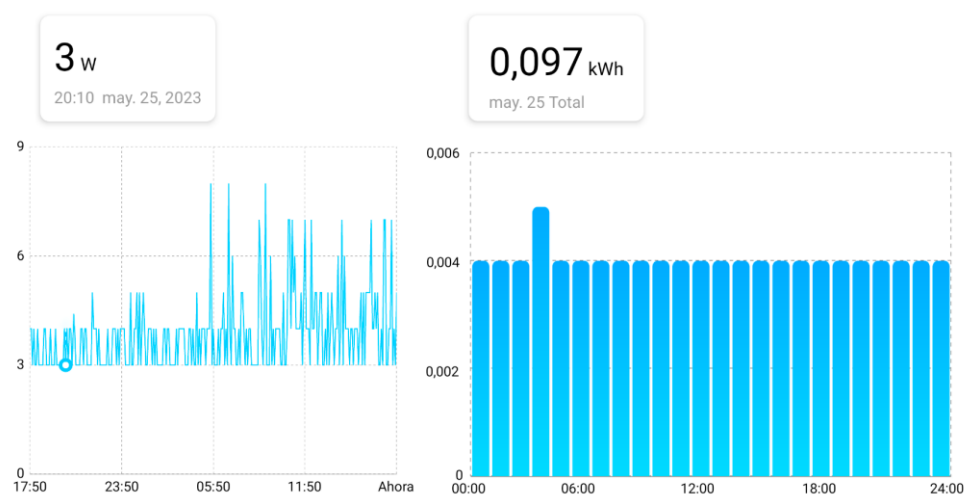


Gráfico 4 - Gráficas del consumo instantáneo y acumulado en 24h

Coste anual adicional en 2022 utilizando un el miniordenador haciendo funciones de router y firewalls avanzados.

$$0.097 \text{ kwh/d} * 365 \text{ d} * 0.19 \text{ €/kwh} = 6.73 \text{ €}$$

### Estudio presupuestario

#### Costes del Proyecto

El coste del proyecto variará en función de las necesidades de cada empresa. Para el caso mostrado en este proyecto el coste en dispositivos físicos ha sido el siguiente:

HP PRODESK 600 G4 – 8600T 16GB RAM	200€
Trajeta de red USB TP-Linl	12,99€
Switch gestionable Netgear GS308E	16.52€
TOTAL	229,51€

Además hay que tener en cuenta el tiempo invertido en instalar y configurar todo el sistema para una persona, por lo que hay que añadir el salario a jornada completa de un trabajador cualificado durante dos semanas.

### Conclusiones

Durante el proyecto se ha logrado convertir con éxito un mini PC en un router OPNsense, virtualizado mediante Proxmox, proporcionando además servicios de red adicionales dentro del mismo dispositivo.

La división de la red en dos VLAN, una para los usuarios y otra para los servidores, permite mantener una separación lógica y mejora la seguridad de la red. Además, mediante la configuración del firewall para que haga uso de listas negras, se

han implementado medidas eficientes para bloquear conexiones no deseadas y proteger la red.

Mediante redirección de puertos NAT se ha permitido que el servidor de WordPress, que está ubicado en la VLAN 2, sea accesible desde el exterior, ahorrando a la empresa los costes de hosting que le supondría alojar una web en una empresa externa.

La implementación de ADGUARD HOME ha mejorado la experiencia de navegación de los empleados, proporcionando un entorno más limpio, rápido y seguro para los usuarios.

La implementación de BookStack en el mismo router ha facilitado la gestión de documentación interna de la empresa sin incurrir en costes adicionales.

Se ha mejorado la usabilidad y la experiencia de los usuarios de la red al registrar dominios locales en el servidor DNS local, en lugar de que recordar la IP de los distintos servicios de la red. Esto ha sido mejorado aún más mediante la implementación de una página de inicio que permite acceder a los servicios recordando únicamente una dirección web.

Se ha comprobado que no supone un incremento significativo en el coste de la factura eléctrica respecto a un router comercial.

En general, se ha demostrado que utilizando tecnologías de código abierto y virtualización es posible crear un entorno de red completo en un solo equipo físico, con capacidad de dar servicio a una pequeña empresa.

El proyecto ha logrado alcanzar los objetivos principales y cumplir con la mayoría de las metas establecidas. Sin embargo, al realizar un análisis crítico del



seguimiento de la planificación y la metodología utilizada, se pueden identificar áreas de mejora y desafíos encontrados durante el proceso como pueden ser:

- Una mejor definición de los objetivos, ya que durante el desarrollo de proyecto han surgido nuevas ideas para incorporar que han retrasado la ejecución de este.
- Una mejor planificación del sistema a implementar, considerando los recursos materiales disponibles.

## **Análisis DAFO**

### ***Debilidades***

**Complejidad técnica:** La virtualización y configuración de servicios adicionales en el router a la hora de expandir las funcionalidades del dispositivo pueden requerir conocimientos técnicos y planificación adecuados, lo que puede ser una barrera para algunos usuarios sin experiencia.

**Dependencia de un único equipo:** Al utilizar un solo equipo físico para virtualizar el router y los servicios adicionales, existe un riesgo de fallo del hardware, lo que podría afectar a toda la red y los servicios asociados.

### ***Amenazas***

**Riesgo de seguridad:** Aunque OPNsense ofrece funciones de seguridad avanzadas, es importante mantenerse actualizado con las últimas actualizaciones y parches de seguridad para mitigar posibles vulnerabilidades.

**Dependencia de un solo proveedor:** Al utilizar OPNsense y Proxmox, el proyecto está sujeto a la disponibilidad y soporte continuo de las plataformas, lo que puede representar un riesgo en caso de cambios o falta de actualizaciones.

### ***Fortalezas***

**Versatilidad:** La virtualización con Proxmox permite agregar servicios adicionales y mejorar la flexibilidad de la red de forma rápida y económica al no requerir hardware adicional.

**Seguridad mejorada:** El uso de OPNsense como router proporciona funciones avanzadas de seguridad, como el uso de listas negras, bloqueo de publicidad y firewall avanzado, lo que ayuda a proteger la red de conexiones maliciosas y mejorar la experiencia de navegación.

**Recuperación ante problemas:** La capacidad de realizar snapshots en Proxmox ofrece una ventaja significativa al permitir revertir a un estado anterior en caso de problemas, lo que facilita la recuperación de la red y minimiza el tiempo de inactividad.

**Eficiencia energética:** El mini PC utilizado como router consume menos energía que un router comercial y al utilizar la virtualización se optimiza aún más la eficiencia en el uso de recursos, lo que ayuda a reducir los costos a la vez que tiene un menor impacto ambiental.

### ***Oportunidades***

**Flexibilidad en la expansión de servicios:** Al utilizar la virtualización, puedes agregar fácilmente nuevos servicios a la red en el futuro sin necesidad de invertir en hardware adicional, lo que brinda oportunidades de crecimiento y adaptación a las necesidades cambiantes de la empresa.

**Continuidad del servicio:** La posibilidad de realizar snapshots y configurar un clúster de alta disponibilidad ofrece una oportunidad para garantizar la continuidad del servicio en caso de fallos.

### **Ampliaciones futuras**

Algunos de los servicios que no se han podido configurar por falta de recursos o tiempo han sido:

- Servidor proxy caché transparente con reglas de bloqueo de ficheros potencialmente peligrosos (.exe, .bat, etc).
- Antivirus de red basado en ClamAV.
- Detección de intrusiones basado en Suricata.
- Configuración de portal cautivo para red de invitados con limitación de ancho de banda.
- Servidor OpenVPN con autenticación en dos factores.
- Visualización avanzada de datos y estadísticas con elastic y grafana
- Clúster de alta disponibilidad en Proxmox o OPNsense.

### **Escalabilidad**

El sistema permite escalar varias de sus características de forma sencilla. Añadiendo más dispositivos físicos y uniéndolos en un clúster de alta disponibilidad es posible incrementar de forma significativa la fiabilidad del sistema.

Además, al tratarse de un PC convencional, permite ampliar de forma rápida y sencilla la memoria RAM y el espacio de disco duro a diferencia de los router convencionales que no permiten ampliar estas características.

## Glosario

**ADGUARD:** Es una herramienta de bloqueo de anuncios y filtrado de contenido utilizada para bloquear anuncios en aplicaciones y navegadores web, además de proporcionar funciones de seguridad y privacidad.

**DNS (Sistema de Nombres de Dominio):** Es un sistema utilizado en Internet que traduce los nombres de dominio legibles por humanos en direcciones IP numéricas que las computadoras pueden entender.

**Firewall:** Es un sistema de seguridad de red que controla y filtra el tráfico de red basado en reglas predefinidas. Su objetivo es proteger la red y los dispositivos de amenazas externas y no autorizadas.

**IP (Protocolo de Internet):** Es un protocolo de comunicación utilizado para identificar y ubicar dispositivos en una red. Cada dispositivo en una red IP tiene una dirección IP única.

**KVM (Kernel-based Virtual Machine):** Es un software de virtualización que permite ejecutar múltiples sistemas operativos como máquinas virtuales en un único host físico.

**LiveCD:** Es una forma de distribución de software en la que el sistema operativo se ejecuta directamente desde un CD o una unidad USB sin necesidad de instalación en el disco duro de una computadora.

**NAT (Traducción de Direcciones de Red):** Es una técnica utilizada en redes de computadoras para traducir direcciones IP privadas en direcciones IP públicas, permitiendo que varios dispositivos se conecten a Internet utilizando una única dirección IP pública.

**OPNsense:** Es una distribución de software libre basada en FreeBSD que funciona como un firewall y enrutador de código abierto. Proporciona funciones de seguridad y administración de redes.

**Proxmox:** Es una plataforma de virtualización de código abierto que permite la creación y administración de máquinas virtuales y contenedores. También incluye características de alta disponibilidad y migración en vivo.

**Puerta de enlace:** También conocida como gateway, es un dispositivo que actúa como punto de entrada o salida para una red. Conecta redes diferentes y permite el enrutamiento de datos entre ellas.

**Router:** Es un dispositivo de red que se utiliza para conectar múltiples redes y enrutar el tráfico de datos entre ellas. Permite la conexión a Internet y el enrutamiento de datos entre diferentes redes.

**Switch:** Es un dispositivo de red que conecta varios dispositivos en una red local. Permite el envío de datos entre los dispositivos conectados mediante el uso de direcciones MAC.

**Tarjeta de red:** También conocida como adaptador de red, es un dispositivo de hardware que permite la conexión de una computadora a una red. Proporciona una interfaz para la comunicación de datos a través de la red.

**VLAN (Red de Área Local Virtual):** Es una técnica de virtualización de redes que permite segmentar una red física en múltiples redes virtuales, lo que proporciona aislamiento y seguridad mejorada.

**Webmin:** Es una interfaz web basada en navegador que permite la administración y configuración de sistemas basados en Unix, como servidores Linux.

Proporciona una forma fácil de administrar varios servicios y configuraciones a través de una interfaz gráfica.

### Trabajos citados

*Acceso SSH.* (s.f.). Recuperado el 21 de 05 de 2023, de reddit.com:

[https://www.reddit.com/r/opnsense/comments/nfox60/cant\\_access\\_the\\_firewall\\_via\\_console\\_and\\_ssh/](https://www.reddit.com/r/opnsense/comments/nfox60/cant_access_the_firewall_via_console_and_ssh/)

Ahmed, W. (2014). *Mastering Proxmox*. Birmingham: Packt>.

Camargo, J. C. (2022). *OPNsense Beginner to Professional*. Birmingham: Packt>.

*good\_tips\_for\_opnsense.* (s.f.). Recuperado el 20 de 05 de 2023, de reddit.com:

[https://www.reddit.com/r/OPNsenseFirewall/comments/q7wme0/good\\_tips\\_for\\_opnsense\\_under\\_proxmox/](https://www.reddit.com/r/OPNsenseFirewall/comments/q7wme0/good_tips_for_opnsense_under_proxmox/)

*IP blocklists.* (s.f.). Recuperado el 17 de 05 de 2023, de allthingstech.ch:

<https://www.allthingstech.ch/using-opnsense-and-ip-blocklists-to-block-malicious-traffic>

*Manual de DHCP.* (s.f.). Recuperado el 2 de 05 de 2023, de docs.opnsense.org:

<https://docs.opnsense.org/manual/dhcp.html>

*Precio medio de la electricidad en 2022.* (s.f.). Recuperado el 26 de 05 de 2023, de

es.statista.com: <https://es.statista.com/estadisticas/993787/precio-medio-final-de-la-electricidad-en-espana/>

*Qemu Guest Agent.* (s.f.). Recuperado el 23 de 05 de 2023, de forum.opnsense.org:

[https://forum.opnsense.org/index.php?topic=23284.msg110753&utm\\_source=pocket\\_saves](https://forum.opnsense.org/index.php?topic=23284.msg110753&utm_source=pocket_saves)

*Requisitos mínimos.* (s.f.). Recuperado el 1 de 02 de 2023, de docs.opnsense.org:

<https://docs.opnsense.org/manual/hardware.html>

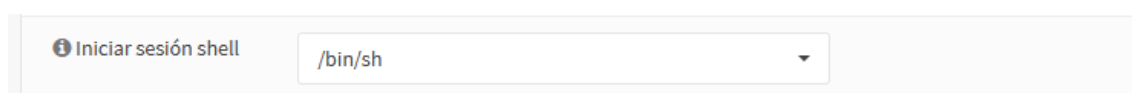
Virtualizacion. (s.f.). Recuperado el 14 de 05 de 2023, de docs.opnsense.org:

<https://docs.opnsense.org/manual/virtuals.html#kvm>

## Anexos

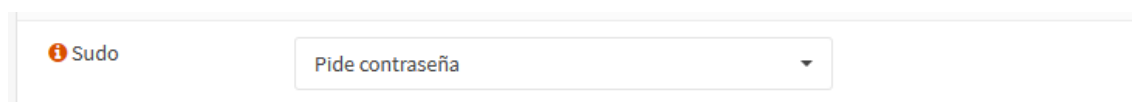
### Habilitación del acceso por consola

Por defecto el acceso por consola y SSH está deshabilitado y hay que cambiar algunas configuraciones en el sistema si se desea hacer uso de él. Lo primero es dar permiso al usuario para iniciar sesión por Shell en Sistema > Acceso > Usuarios, o bien volver a habilitar de forma temporal el usuario root (Acceso SSH, s.f.).



Captura 79 – Tipo de Shell asignada al usuario

En Sistema > Ajustes > Administración tendremos que configurar Sudo para que pida la contraseña y habilitar el acceso por ssh.



Captura 80 – Permitir sudo



Captura 81 – Habilitar SSH

Es recomendable volver a deshabilitar el acceso una vez se terminen de hacer las tareas que lo requerían.