

Proyecto Fin de Ciclo ASIR



Red Segura-Pymes
pfSense (Firewall)

Administración de Sistemas Informáticos en Red

Tutor: Álvaro Manzano Rueda

Antonio G. Tenorio Gañán 2º ASIR

<https://github.com/Antonio-Gabino>

Licencia Creative Commons: CC BY-NCSA

Fecha de entrega: 09/06/2025

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Agradecimientos

Quisiera dedicar unas palabras de agradecimiento a todas las personas que me han acompañado y apoyado durante esta etapa formativa, haciendo posible que este proyecto, y el camino recorrido hasta llegar a él, haya sido una experiencia profundamente enriquecedora y motivadora.

En primer lugar, a mi **mujer** y a mi **hijo**, por su paciencia, su amor incondicional y su comprensión durante todos estos meses de estudio y esfuerzo. Gracias por estar siempre a mi lado, incluso en los momentos más difíciles. Sin vuestro apoyo, nada de esto habría sido posible.

Agradezco sinceramente a todo el **profesorado**, tanto al actual como al que ya no está, por su dedicación, paciencia y compromiso constante. Cada uno ha contribuido de manera significativa no solo a mi formación académica, sino también a mi crecimiento personal.

Quiero hacer una mención especial a **Rosario, Juan José, Gabriel, Alberto, Soraya, José Antonio y José Luis Boa**, quienes han estado presentes en muchos momentos clave, brindándome su ayuda, explicaciones, consejos y palabras de ánimo cuando más lo necesitaba.

Extiendo también este agradecimiento a **jefatura de estudios** y al resto del profesorado en general, por facilitarme el acceso a recursos y espacios de estudio, y por haberme abierto en numerosas ocasiones la biblioteca, un gesto que me ha permitido preparar adecuadamente mis tareas y exámenes en un entorno tranquilo y apropiado.

Por último, gracias a mis **compañeros y compañeras de estudio**, con quienes he compartido dudas, aprendizajes, esfuerzos y también momentos de alegría que han hecho que esta etapa haya sido mucho más amena y llevadera.

Quisiera dedicar también unas palabras en memoria de mi padre, **Antonio Tenorio Méndez**, que en vida siempre tuvo un deseo claro: que me formara, que estudiara y trabajara, pero, sobre todo, que **nunca dejara de aprender**. Fue una gran persona, un referente de cariño y principios, que nos quiso profundamente y que sigue presente en cada paso que doy. Este logro también es para él.

A todos/as, **gracias de corazón**.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Índice

1. Introducción.....	6
1.1 Objetivos del proyecto.....	6
1.2 Justificación y relevancia del proyecto.....	7
1.3 Metodología de trabajo.....	8
1.4 Estructura del documento.....	9
2. Análisis de Requisitos.....	9
2.1 Entorno de desarrollo o implantación.....	10
2.2 Requisitos funcionales y técnicos.....	10
2.3 Requisitos de seguridad.....	11
2.4 Requisitos de hardware y software.....	11
2.5 Restricciones y consideraciones específicas.....	12
3. Diseño de la Infraestructura.....	12
3.1 Arquitectura de red.....	13
3.2 Selección de tecnologías y servicios.....	14
3.3 Diseño lógico y físico de la red.....	15
3.4 Planificación de servidores y servicios.....	17
4. Implementación y Configuración VM.....	18
4.1 Descarga e instalación de VirtualBox (versión 7.1.8).....	18
4.2 Instalación de VM pfSense (Firewall).....	21
4.2.1 Configuración de VM pfSense (Firewall).....	30
4.3 Instalación de VM Debian 12 (Servidor Web).....	42
4.4 Instalación y configuración Apache2 (Servidor Web).....	52
4.5 Crear un sitio web en Apache.....	54
4.6 Instalación y configuración del Nginx (Servidor Web).....	55
4.7 Instalación de VM Debian 12 (cliente1).....	57
4.8 Configuración de servicios principales.....	59
4.8.1 Servicio SSH (Secure Shell).....	59
4.8.2 Servicio SFTP (FTP Secure).....	60
4.8.3 DHCP Configuración automática de IPs en clientes.....	65
4.8.4 Instalar y configurar servidor DNS.....	70
4.9 Integración de servicios y pruebas de funcionamiento.....	74

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

4.9.1	Pruebas de conectividad básica.	74
4.9.2	Verificación de reglas de pfSense (Firewall).	76
3.10	Automatización de tareas y scripts.	80
3.10.1	Script 1. Copia de seguridad de archivos importantes (Servidor Web)....	80
3.10.2	Script 2. Monitoreo de los servicios Apache2 y Nginx.	82
3.10.3	Script 3. Actualización del S.O. Debian 12.	83
5.	Administración y Monitorización.	84
5.1	Gestión de usuari@s y permisos.	84
5.2	Herramientas de monitorización y alertas.	86
5.3	Mantenimiento preventivo y correctivo.	89
5.4	Políticas de backup y recuperación.	90
6.	Seguridad Informática.	91
6.1	Configuración de reglas de pfSense (Firewall)....	91
6.1.1	Regla 1. Conexión del equipo anfitrión a pfSense.	91
6.1.2	Regla 2. Ping del equipo anfitrión a pfSense.....	95
6.1.3	Regla 3. Bloquear acceso SSH cliente1 al Servidor Web.....	96
6.1.4	Regla 4. DHCP Bloqueo de clientes desconocidos.	98
6.1.5	Regla 5. Activar reserva IP - MAC mediante DHCP.....	101
6.1.6	Regla 6. Permitir tráfico DMZ a WAN.....	102
6.1.7	Regla 7. Bloquear tráfico DMZ a LAN.....	103
6.1.8	Regla 8. Permitir tráfico cliente2 LAN a DMZ.....	105
6.1.9	Regla 9. Permitir tráfico LAN (HTTP) a DMZ.....	106
6.1.10	Regla 10. Permitir tráfico LAN (HTTPS) a DMZ.....	107
6.1.11	Regla 11. Bloquear resto de tráfico de LAN a DMZ.....	108
6.1.12	Regla 12. Permitir tráfico LAN a WAN.	109
6.1.13	Regla 13. Permitir tráfico WAN a DMZ (HTTP).	110
6.1.14	Regla 14. Permitir tráfico WAN a DMZ (HTTPS).	111
6.1.15	Regla 15. Bloquear resto de tráfico WAN a DMZ.	111
7.	Documentación Técnica.	112
7.1	Manuales de instalación y configuración.....	112
7.2	Tareas Comunes del Administrador.	113
7.3	Esquemas y diagramas de la infraestructura.	115

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

8. Conclusiones y Futuras Mejoras.....	117
8.1 Resumen del proyecto y valoración de los resultados obtenidos.....	117
8.2 Dificultades encontradas y soluciones aplicadas.	117
8.3 Posibles ampliaciones y mejoras futuras.	120
8.3.1 Incorporación de una Zona Desmilitarizada (DMZ).	121
8.3.2 Incorporación de un cliente2 Windows.	122
8.4 Propuesta de solución comercial: BIOS Security Box (BSB).	124
8.5 Aprendizaje personal y profesional.	125
9. Webgrafía.....	127
9.1 Fuentes utilizadas.....	127
9.1.1 Páginas webs y vídeos.	127
9.1.2 Tutoriales y descarga de ficheros de instalación.	127

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

1. Introducción.

En un entorno cada vez más digitalizado, la seguridad de las redes informáticas se ha convertido en un aspecto crucial incluso para las pequeñas empresas. La protección frente a amenazas externas e internas, el control del tráfico y la correcta segmentación de la red son elementos clave para garantizar la disponibilidad, integridad y confidencialidad de los datos y servicios.

Este proyecto tiene como finalidad el diseño e implementación de una red interna segura para una pequeña empresa, utilizando herramientas de software libre. Para ello, se ha creado una infraestructura virtual compuesta por tres elementos fundamentales:

- Un cortafuego **pfSense**, encargado de gestionar el tráfico de red y aplicar políticas de seguridad.
- Un **servidor web** que integra **Apache** y **Nginx** para simular un entorno de producción real con balanceo de carga o proxy inverso.
- Un **cliente** que representa el equipo de un empleado, utilizado para probar la conectividad y el acceso controlado a los servicios del servidor.

Este proyecto se desarrolla en un entorno virtualizado mediante Virtual Box, lo que permite simular de forma realista las condiciones de una red empresarial en un entorno controlado. Gracias a esta configuración, podemos realizar pruebas, simulaciones y evaluaciones de seguridad sin poner en riesgo sistemas reales.

1.1 Objetivos del proyecto.

El principal objetivo de este proyecto es **demostrar cómo implementar una red segura en el entorno de una pequeña empresa**, utilizando herramientas de código abierto y buenas prácticas de administración de sistemas. Para ello, se diseña e implementa una red interna compuesta por tres elementos clave: un cortafuego pfSense, un servidor web y un cliente.

Los objetivos específicos que se pretenden lograr con esta implementación son los siguientes:

- **Diseñar e implementar un entorno de red segmentado y seguro** que nos permita controlar y filtrar el tráfico de forma eficiente mediante el uso de un firewall pfSense.
- **Configurar y desplegar un servidor web funcional** que utilice Apache y Nginx en paralelo, simulando un entorno real de producción con balanceo o proxy inverso.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- **Simular el acceso de un empleado** a través de un cliente conectado a la red interna, validando la conectividad, seguridad y el acceso controlado a los recursos del servidor.
- **Aplicar políticas de seguridad en el cortafuego pfSense**, tales como reglas de acceso, NAT, redirecciones de puertos y bloqueo de tráfico no deseado.
- **Comprobar la eficacia del sistema frente a posibles amenazas internas o externas**, evaluando el comportamiento del firewall ante diferentes escenarios.
- **Fomentar el uso de soluciones libres** como alternativas viables y profesionales para pequeñas y medianas empresas (Pymes).

1.2 Justificación y relevancia del proyecto.

Hoy en día, incluso las pequeñas empresas dependen en gran medida de las redes informáticas para su funcionamiento diario. Esto hace que proteger los sistemas y la información sea algo fundamental. A pesar de ello, muchas pequeñas y medianas empresas no cuentan con recursos suficientes para implementar soluciones de seguridad costosas o complejas.

Este proyecto se justifica porque ofrece una solución viable, segura y económica para proteger una red interna, utilizando software libre y herramientas accesibles como pfSense. Este cortafuego permite controlar el tráfico de red, definir reglas de acceso, proteger los servicios internos y evitar posibles ataques desde el exterior. Además, **su uso no requiere licencias de pago**, lo que lo convierte en una opción muy atractiva para empresas con presupuestos limitados.

La instalación de un servidor web con Apache y Nginx en paralelo permite simular un entorno real de trabajo, en el que se pueden aplicar configuraciones habituales como el uso de un proxy inverso o balanceo de carga. También se incluye un cliente que representa el equipo de un empleado, para verificar que puede acceder a los servicios internos de forma segura y controlada.

La relevancia del proyecto radica en que, como estudiantes, nos permite aplicar conocimientos prácticos sobre redes, seguridad y administración de sistemas en un caso realista. Además, fomenta el uso de tecnologías libres, que son cada vez más utilizadas en el ámbito profesional. Este tipo de proyectos ayuda a desarrollar competencias muy valoradas en el sector, como la planificación de infraestructuras seguras, la configuración de servicios, y la capacidad de resolver problemas técnicos.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

En resumen, este trabajo no solo muestra cómo proteger una red interna de forma efectiva, sino que también nos prepara como estudiantes, a enfrentarnos a situaciones reales en el futuro laboral.

1.3 Metodología de trabajo.

Para llevar a cabo este proyecto se ha seguido una metodología práctica y estructurada, basada en el desarrollo paso a paso de cada uno de los componentes que forman parte de la red. El enfoque adoptado ha sido principalmente experimental, con el objetivo de diseñar, configurar y comprobar el funcionamiento de una red segura en un entorno controlado.

El trabajo se ha dividido en varias fases:

1. **Planificación del proyecto:** En primer lugar, se definió el objetivo general y se diseñó la arquitectura de red que se iba a implementar. Se decidió trabajar con tres máquinas virtuales: una para el **cortafuego pfSense**, otra para el **servidor web** (con **Apache** y **Nginx**), y una tercera para el **cliente**.
2. **Instalación del entorno:** Se instalaron y configuraron las máquinas virtuales necesarias, utilizando un entorno de virtualización como **VirtualBox**. Se establecieron las interfaces de red para permitir la comunicación entre las máquinas.
3. **Configuración del cortafuego pfSense:** Se configuró pfSense como puerta de enlace de la red, aplicando reglas de firewall para controlar el tráfico. También se realizaron tareas como la asignación de IPs, configuración de NAT y redirección de puertos, todo ello enfocado a garantizar la seguridad de la red interna.
4. **Despliegue del servidor web:** En esta fase se instaló Apache y Nginx en el servidor, configurándolos para que trabajaran juntos, mediante un esquema de proxy inverso o balanceo de carga. Se utilizó la página web de prueba de Apache para comprobar el acceso desde el cliente1.
5. **Configuración y prueba del cliente:** Se configuró la máquina cliente1 para que pudiera conectarse a través del firewall y acceder correctamente al servidor web. Se realizaron pruebas para validar la conectividad, el acceso seguro y el cumplimiento de las reglas definidas en pfSense.
6. **Verificación y documentación:** Finalmente, se realizaron distintas pruebas de funcionamiento y de seguridad para comprobar que la red se comportaría como se

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

esperaba. Todos los pasos fueron documentados con capturas de pantalla, explicaciones detalladas y justificaciones técnicas.

Esta metodología me ha permitido avanzar de forma ordenada, detectar posibles errores durante la implementación y proponer soluciones. Además, facilita la comprensión del proceso completo y sirve como guía para futuras implementaciones similares en entornos reales.

1.4 Estructura del documento.

Este trabajo se organiza en los siguientes apartados:

1. **Introducción:** Presenta el contexto, objetivos y metodología del proyecto.
2. **Análisis de Requisitos:** Define los requisitos técnicos, funcionales y de seguridad necesarios.
3. **Diseño de la Infraestructura:** Describe la arquitectura lógica y física del sistema.
4. **Implementación y Configuración:** Detalla el proceso técnico de instalación para desplegar la red y los servicios.
5. **Administración y Monitorización:** Explica las tareas de gestión y seguimiento del sistema.
6. **Seguridad Informática:** Presenta las medidas adoptadas para proteger la red y los servicios.
7. **Documentación Técnica:** Recoge configuraciones, comandos y pruebas realizadas.
8. **Conclusiones y Futuras Mejoras:** Reflexiona sobre los resultados y posibles mejoras del proyecto.
9. **Webgrafía:** Enumera las fuentes consultadas.
10. **Presentación del Trabajo:** Describe brevemente la herramienta pfSense y su relevancia en el proyecto.

Esta estructura nos permite una lectura clara y lógica del contenido, facilitando la comprensión del proceso seguido y de las decisiones tomadas durante el desarrollo del proyecto.

2. Análisis de Requisitos.

En este apartado se presenta el estudio de las necesidades técnicas y funcionales que justifican el desarrollo de la infraestructura de red propuesta en este trabajo. Su finalidad es proporcionar

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

una base clara y estructurada que oriente el diseño e implementación del sistema, garantizando que se ajusta a los requerimientos reales y prácticos de una pequeña empresa.

2.1 Entorno de desarrollo o implantación.

El proyecto se lleva a cabo en un entorno virtualizado, lo que permite simular una red real en condiciones controladas. Para ello, se utiliza **VirtualBox** como plataforma de virtualización, donde se crean las tres máquinas (VM) necesarias para la infraestructura: un cortafuego con **pfSense**, un servidor web con **Apache** y **Nginx**, y un **cliente** que simula el equipo de un empleado. Todas las máquinas están conectadas a una red interna definida en VirtualBox, con acceso a Internet controlado, lo que favorece un escenario seguro y reproducible para pruebas y demostraciones.

2.2 Requisitos funcionales y técnicos.

Para el correcto funcionamiento de la infraestructura, hemos implementado los siguientes servicios y funcionalidades:

- Seguridad de red básica mediante un firewall pfSense que controle el tráfico interno y externo.
- Definición de reglas de cortafuegos que permitan solo el tráfico necesario y bloquen accesos no deseados.
- Acceso al servidor web restringido exclusivamente a dispositivos conectados a la red LAN y equipos que se conectan desde Internet WAN.
- Implementación de un servidor web con doble motor: Apache para la gestión de contenido dinámico y Nginx como proxy inverso o para servir contenido estático.
- Capacidad de registrar y monitorizar el tráfico desde pfSense para análisis y auditorías.
- El sistema debe permitir la navegación interna del cliente hacia el servidor web DMZ y hacia el exterior Internet WAN de forma segura.
- Se debe permitir el acceso web (puertos 80 y 443) desde el cliente hacia el servidor web.
- El firewall pfSense debe poder registrar y monitorizar todo el tráfico que pasa a través de él, permitiendo el análisis posterior.
- La combinación Apache + Nginx debe estar operativa para servir contenido web estático y dinámico con eficiencia.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- El sistema debe ser replicable en un entorno virtualizado accesible (como VirtualBox o Proxmox).

2.3 Requisitos de seguridad.

- Las máquinas tienen acceso a Internet, pero desde la WAN no se puede acceder a los clientes, desde la DMZ sí se puede acceder a Internet y viceversa, pero desde la DMZ no se puede acceder a la LAN, sí desde la LAN a la DMZ.
- Se deben establecer reglas de firewall para prevenir ataques internos y limitar accesos no autorizados.
- El servidor web deberá estar protegido contra escaneos y accesos indeseados.

2.4 Requisitos de hardware y software.

Para ejecutar este proyecto de forma adecuada en un entorno virtualizado, se establecen los siguientes requisitos:

Hardware

- **CPU:** Procesador con soporte para virtualización (Intel VT-x o AMD-V), para la instalación de pfSense se recomienda 1 CPU y se asignan 2 núcleos (Cores).
- **RAM:** 6 GB mínimo, se asignan (2 GB para pfSense, 3 GB para el servidor web, 2 GB para los clientes Linux y 4 GB para el cliente Windows).
- **Almacenamiento:** Entre 30 GB y 50 GB por máquina virtual aproximadamente.
- **Tarjeta de red:** Adaptadores de red configurables para redes internas y externas en VirtualBox.

Software

- **Plataforma de virtualización:** VirtualBox (versión estable 7.1.8 actual).
- **Sistema operativo para el firewall:** pfSense (versión estable 2.7.2 actual).
- Sistema operativo para el servidor web y cliente: Debian GNU/Linux (versión estable 12.10.0 actual).
- **Servidores web:** Apache 2.4.63 y Nginx 1.26.3 (versiones estables actuales).

Estos requisitos aseguran el correcto funcionamiento del entorno virtualizado, sin comprometer el rendimiento ni la estabilidad durante las pruebas y simulaciones.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

2.5 Restricciones y consideraciones específicas.

Durante el desarrollo del proyecto deberemos tener en cuenta algunas limitaciones y condiciones especiales que influyen en el diseño y la implementación.

- El acceso a Internet está restringido dentro de la red interna, no así en la DMZ.
- El entorno virtualizado limita el rendimiento frente a una implementación en hardware físico, por lo que se deben ajustar los recursos.
- La configuración debe estar documentada y ser replicable, lo que impone una disciplina estricta en la toma de decisiones técnicas.
- En la medida de lo posible, no se permitirá el uso de software privativo o de pago, en línea con los principios de soluciones libres para Pymes, a no ser que sea estrictamente necesario.
- Se prioriza la facilidad de mantenimiento y la simplicidad en la configuración, dado que el proyecto está orientado a pequeñas empresas con conocimientos técnicos limitados.

Estas consideraciones aseguran que el proyecto se mantenga realista, viable y alineado con su objetivo formativo y profesional.

3. Diseño de la Infraestructura.

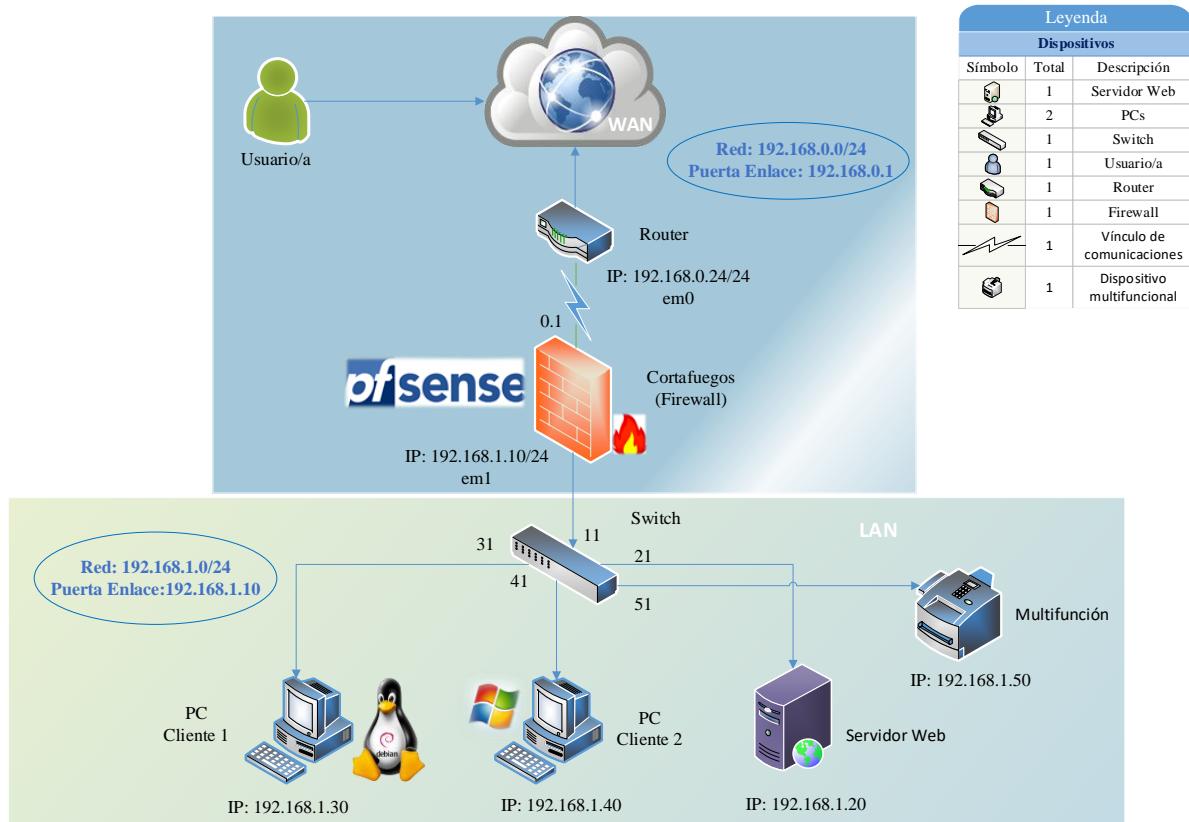
El diseño de la infraestructura es un aspecto clave para asegurar que la red cumpla con los requisitos de seguridad, rendimiento y facilidad de gestión. En este apartado se detalla cómo se ha planificado la red del proyecto, incluyendo la arquitectura general, la elección de tecnologías, los diagramas lógico y físico, y la distribución de servicios. Se describe detalladamente la infraestructura de red diseñada para este trabajo, abarcando la arquitectura general, la selección de tecnologías utilizadas, los esquemas lógico y físico, y la planificación de servidores y servicios. El diseño está orientado a garantizar la seguridad, eficiencia y facilidad de administración dentro de una pequeña empresa, aplicando buenas prácticas y herramientas de software libre.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo		Proyecto de Administración de sistemas informáticos en red.	

3.1 Arquitectura de red.

La red ha sido diseñada para simular el entorno de una pequeña empresa, con una estructura segmentada y funciones bien definidas para cada componente. Se compone de tres elementos principales:

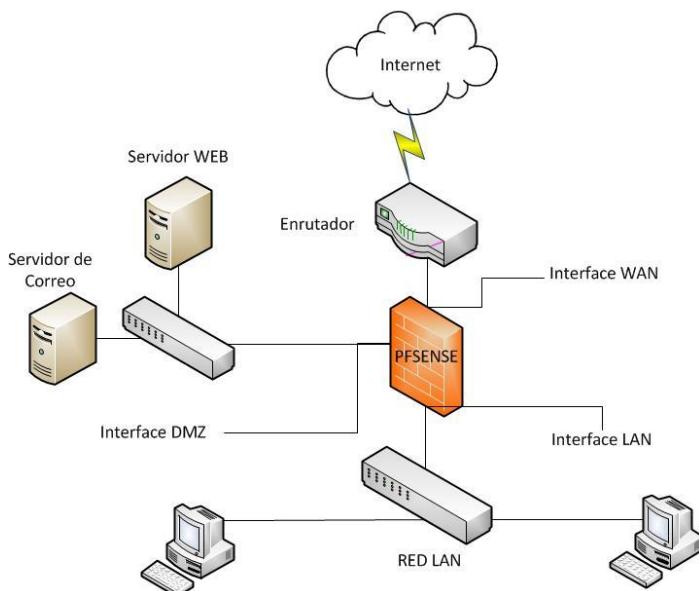
- **Firewall (pfSense):** Actúa como la puerta de enlace entre la red interna y el exterior. Controla el tráfico, aplica políticas de seguridad, realiza NAT (traducción de direcciones de red) y redireccionamiento de puertos, y permite o bloquea conexiones según las reglas establecidas.
- **Servidor Web (Apache + Nginx):** Ejecuta Apache para gestionar contenido dinámico (como páginas PHP) y Nginx como proxy inverso o balanceador de carga para distribuir solicitudes y servir contenido estático. Esta combinación simula un entorno real de producción con balanceo de carga.
- **Cliente (Estación de Trabajo):** Representa un equipo típico de un empleado. Se utiliza para acceder a los servicios del servidor y comprobar el funcionamiento de las reglas de seguridad.



	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Todos los equipos están conectados mediante una red LAN interna en un entorno de virtualización (VirtualBox), con direcciones IP estáticas para facilitar la configuración. La topología de red es en **estrella**, lo que permite una gestión centralizada y eficiente.

El entorno virtualizado con VirtualBox aísla la red interna, sin acceso directo desde Internet a dicha red, permitiendo realizar pruebas en un entorno controlado y seguro.



3.2 Selección de tecnologías y servicios.

La elección de tecnologías se basa en criterios de eficiencia, seguridad, coste y disponibilidad.

A continuación, se justifica la selección:

- **pfSense:** Es una solución de cortafuegos de código abierto, ampliamente adoptada por empresas pequeñas y medianas. Ofrece funciones avanzadas como reglas personalizadas, NAT, VPN, DHCP y registro del tráfico. Su interfaz gráfica permite una configuración sencilla sin sacrificar potencia o versatilidad. Se seleccionó por ser gratuito, robusto y con una interfaz intuitiva, permitiendo aplicar reglas de firewall, NAT y realizar monitoreo del tráfico, además de utilizarla la empresa donde realizo las prácticas ofreciéndosela a sus clientes a través de un dispositivo el cual lleva incorporado éste protocolo de seguridad.
- **Apache y Nginx:** Se emplean conjuntamente para simular un entorno web completo. Apache gestiona las peticiones dinámicas (PHP, bases de datos), mientras que Nginx actúa como proxy inverso o balanceador de carga, optimizando el rendimiento. Esta

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

combinación refleja una configuración moderna, donde Apache maneja el contenido dinámico y Nginx distribuye el tráfico y sirve contenido estático de forma eficiente.

- **Debian GNU/Linux:** Sistema operativo base para el servidor web y el cliente, elegido por su estabilidad, seguridad y filosofía de software libre. Su soporte comunitario y actualizaciones regulares lo hacen ideal para entornos empresariales.
- **VirtualBox:** Se utiliza para crear un entorno de pruebas seguro, portable y reproducible. Permite simular una red real con mínimo coste en recursos y sin necesidad de hardware adicional, ideal para laboratorios y entornos de desarrollo.
- **Red interna virtual:** Aísla la red del exterior, ofreciendo un entorno seguro y controlado para las pruebas.

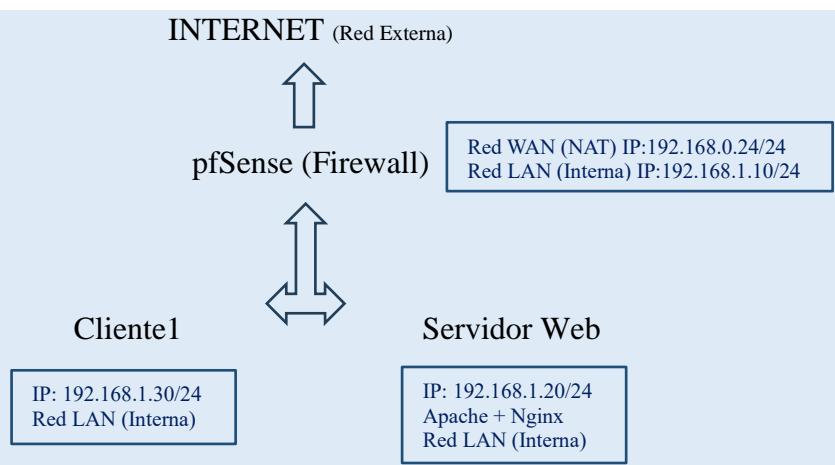
Estas herramientas, combinadas, ofrecen una solución profesional y escalable, adecuada para el contexto de una Pyme que busca garantizar seguridad sin recurrir a soluciones privativas o costosas. La elección se basa en su disponibilidad, facilidad de uso, fiabilidad y fidelidad al entorno de una pequeña empresa.

3.3 Diseño lógico y físico de la red.

Se han elaborado dos tipos de diseños para representar la infraestructura:

Diseño Lógico

El diagrama lógico muestra cómo se comunican los distintos dispositivos.



- **Cliente y Servidor:** Ambos están en la misma red interna.
- **Tráfico:** Todo el tráfico pasa por pfSense, permitiendo aplicar políticas de seguridad y cómo se segmentan a nivel de red.
- **Red WAN:** Utilizada por pfSense para acceso a Internet.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

- **Red LAN:** Conecta a los clientes y al servidor web.
- **Firewall pfSense:** Posee dos interfaces de red: una WAN conectada al exterior (Internet simulado) y una LAN que conecta al resto de dispositivos.
- **Política de Seguridad:** Permite únicamente el tráfico esencial entre cliente y servidor, denegando todo el tráfico no autorizado.

Diseño Físico

El diagrama físico representa cómo están organizadas las máquinas en VirtualBox.

- **VM1:** pfSense (2 interfaces: Adaptador puente externa + LAN interna).
 - WAN: 192.168.0.24/24
 - LAN: 192.168.1.10/24
- **VM2:** Servidor Web (1 interfaz: LAN interna).
 - LAN: 192.168.1.20/24
- **VM3:** Cliente (1 interfaz: LAN interna).
 - LAN: 192.168.1.30/24

Describiendo la disposición de los equipos y su conexión en el entorno virtualizado. Todas las máquinas están alojadas en VirtualBox, con recursos asignados de forma equilibrada.

- **pfSense:**
 - 2 núcleos de CPU
 - 2 GB de RAM
 - 30 GB de disco
- **Servidor Web:**
 - 2 núcleos de CPU
 - 3 GB de RAM
 - 30 GB de disco
- **Clientes:**
 - 2 núcleo de CPU
 - 2 GB de RAM
 - 30 GB de disco

Estas máquinas están conectadas a dos redes virtuales internas: una LAN interna común para cliente y servidor, y una WAN exclusiva de pfSense para Internet. Este diseño permite

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

reproducir una arquitectura empresarial básica, facilita la gestión y proporciona un entorno seguro para pruebas.

PfSense puede actuar como **router** y **firewall** entre el mundo exterior y la red local.

3.4 Planificación de servidores y servicios.

Cada equipo en la red cumple una función específica:

pfSense

- **Gestión de Direcciones IP:** Puede actuar como servidor DHCP.
- **Reglas de Firewall y NAT:** Aplica reglas de firewall y realiza NAT.
- **Registro y Monitoreo:** Registra eventos y tráfico de red.
- **Ampliación:** Puede ampliarse con herramientas de monitorización como **ntopng**.

Servidor Web

- **Apache:** Ejecuta aplicaciones dinámicas (PHP).
- **Nginx:** Actúa como proxy inverso y balanceador de carga.
- **Configuración de Sitios Virtuales:** Se configuran sitios virtuales accesibles desde el cliente.

Cliente

- **Acceso al Servidor:** Accede al servidor mediante navegador web.
- **Herramientas de Red:** Utiliza herramientas como ping, **traceroute** o **curl** para pruebas de conectividad.
- **Verificación de Políticas de Seguridad:** Verifica que las políticas de seguridad funcionan correctamente.

Asignación de Funciones

Dispositivo	Funciones Principales
pfSense	<ul style="list-style-type: none"> - Cortafuegos. - Servidor DHCP para la red LAN. - Aplica reglas de firewall, realiza NAT y redirección. - Registro de eventos y monitoreo del tráfico de red. - Puede ampliarse con herramientas como ntopng.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Dispositivo	Funciones Principales
Servidor Web	<ul style="list-style-type: none"> - Servicio web HTTP/HTTPS. - Apache ejecuta contenido y aplicaciones dinámicas (PHP). - Nginx actúa como proxy inverso y balanceador de carga. - Hosting de páginas de prueba. - Se configuran sitios virtuales accesibles desde el cliente.
Cliente	<ul style="list-style-type: none"> - Simula un usuario interno, verificando que las políticas de seguridad funcionan correctamente. - Acceso a contenido web mediante un navegador. - Pruebas de conectividad y seguridad con herramientas de red como ping, traceroute o curl.

Esta planificación asegura que los roles estén bien definidos y permite escalar o modificar fácilmente los servicios si fuese necesario.

4. Implementación y Configuración VM.

En este apartado se describe el proceso de instalación y configuración de los sistemas operativos y servicios que forman parte de la infraestructura del proyecto. Se detalla cómo se llevó a cabo la implementación dentro de un entorno virtualizado, utilizando **VirtualBox** como herramienta principal. Esto permite una puesta en marcha segura y controlada. Además, se incluyen las pruebas realizadas para validar el correcto funcionamiento de cada componente, así como scripts para automatizar tareas básicas. También se presentan capturas de pantalla para evidenciar el proceso y los resultados obtenidos. Los sistemas operativos utilizados son **pfSense**, **Debian GNU/Linux** y **Windows**.

4.1 Descarga e instalación de VirtualBox (versión 7.1.8).

Antes de comenzar con la instalación de los sistemas operativos, es necesario disponer de un entorno de virtualización. Para este proyecto utilizamos **Oracle VM VirtualBox**, una herramienta gratuita y multiplataforma que permite crear máquinas virtuales fácilmente.

1. Accedemos al sitio oficial de VirtualBox para realizar la descarga gratuita.

<https://www.virtualbox.org>

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

virtualbox.org/wiki/Downloads

Hogar Descargar Documentación Comunidad Search

Descargar VirtualBox

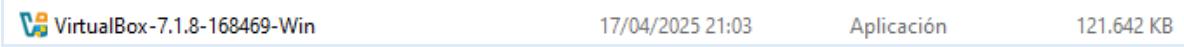
El paquete de extensiones de VirtualBox está disponible para uso personal y educativo en esta página bajo la licencia PUEL. También está disponible bajo términos comerciales o empresariales. Al descargarlo, acepta los términos y condiciones de la licencia correspondiente.



2. Seleccionamos el S.O. del equipo anfitrión (Windows, macOS o Linux).

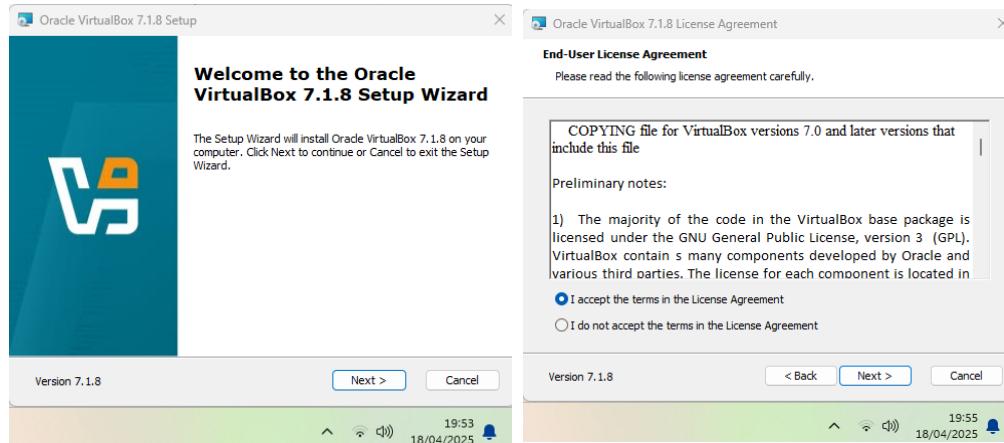
- Por ejemplo, si se utiliza **Windows**, hacer clic en “Hosts de Windows”, si se utiliza **Linux** hacer clic en “Distribuciones de Linux” y si se utiliza **Mac** hacer clic en “Hosts macOS/Apple Silicon”.

3. Descargamos el instalador y ejecutamos el archivo.



- Seguimos el asistente de instalación:

- Aceptamos los términos de licencia.
- Seleccionamos los componentes por defecto.
- Permitimos la instalación de controladores de red y USB cuando lo solicite.



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

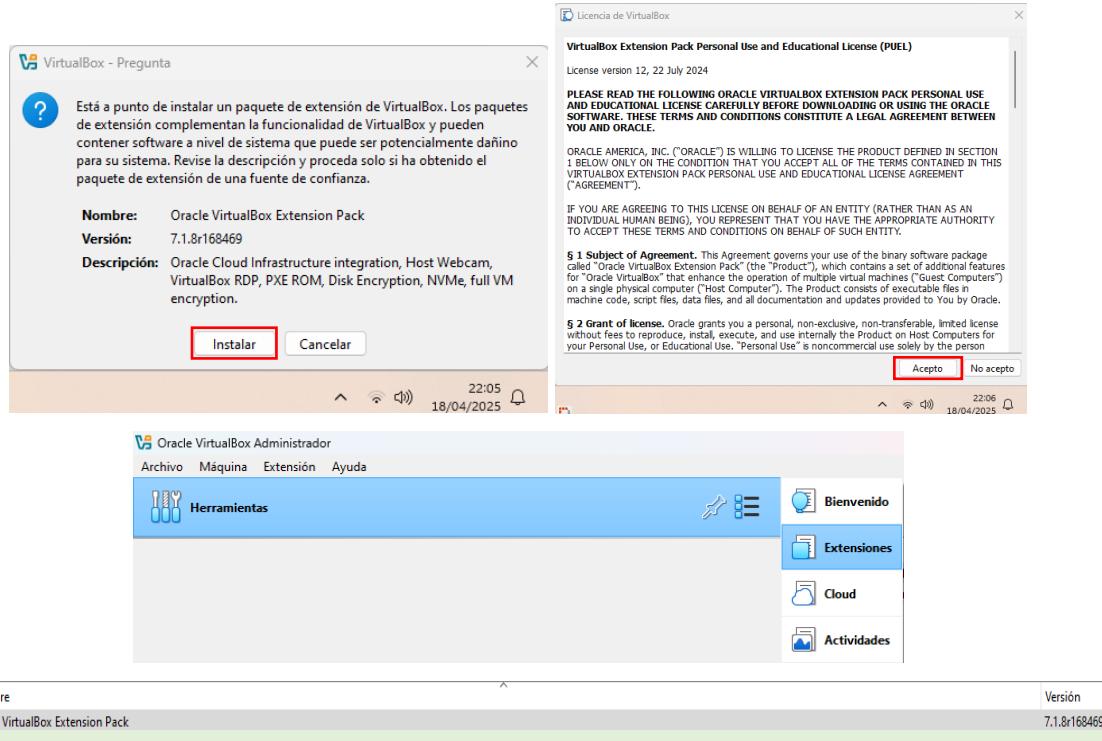


4. Instalamos el Extensión Pack (opcional pero recomendable):

 Oracle_VirtualBox_Extension_Pack-7.1.8	17/04/2025 21:09	VirtualBox Extensi...	22,436 KB
--	------------------	-----------------------	-----------

- Añade compatibilidad con dispositivos USB 2.0 y 3.0, escritorio remoto y cifrado de discos.
- Una vez descargado, hacemos doble clic en el archivo y aceptamos los términos de su instalación.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------



5. Reiniciamos el equipo si lo solicita el instalador.

- Enlace a video demostrativo de la instalación de VirtualBox:

<https://www.youtube.com/watch?v=3EpWqt8q9sA&t=6s>

4.2 Instalación de VM pfSense (Firewall).

Se puede descargar gratuitamente desde su sitio oficial: <https://www.pfsense.org/download/>

Recomendándose, descargar la versión de arquitectura AMD64 (64 bits) con instalador ISO.

The screenshot shows the product page for the "INSTALADOR DE NETGATE" (pfSense Installer ISO) on the Netgate website. The page includes the following details:

- INSTALADOR DE NETGATE**
- \$0.00**
- Envío calculado al finalizar la compra.
- Paga con el tiempo por pedidos superiores a 35,00 \$ con [shop](#). Más información.
- Los clientes que utilizan cuentas de Shippo Pay pueden experimentar una demora de 1 a 2 días en el procesamiento del pedido.
- Imagen de instalación: AMD64 ISO IPMI/Máquinas virtuales.
- Cantidad: 1
- AÑADIR A LA CESTA**
- ENCUENTRA UN SOCIO**

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

shop.netgate.com/cart

netgate

TODOS LOS PRODUCTOS PRODUCTOS PFSENSE+ PRODUCTOS TNSR+ ACCESORIOS+ APOYO+ MÁS+

CARRO DE LA COMPRA

Instalador Netgate AMD64 ISO (Máquinas virtuales)

Subtotal \$0.00

Impuestos y envío calculados al finalizar la compra

Los certificados de exención de impuestos o de renta deben enviarlos a sales@netgate.com antes de finalizar la compra para obtener el beneficio de exención de impuestos. No podemos reembolsar el impuesto sobre las ventas una vez finalizada la compra.

CARRITO VACÍO ACTUALIZAR CARRITO VERIFICAR

netgate

TODOS LOS PRODUCTOS PRODUCTOS PFSENSE+ PRODUCTOS TNSR+ ACCESORIOS+ APOYO+ CAPACITACIÓN

ACceso

smr.gabino@gmail.com

.....

¿Olvidaste tu contraseña?

INICIAR SESIÓN

o Volver a la tienda

Iniciar sesión de socio

atxfiles.netgate.com/mirror/downloads/

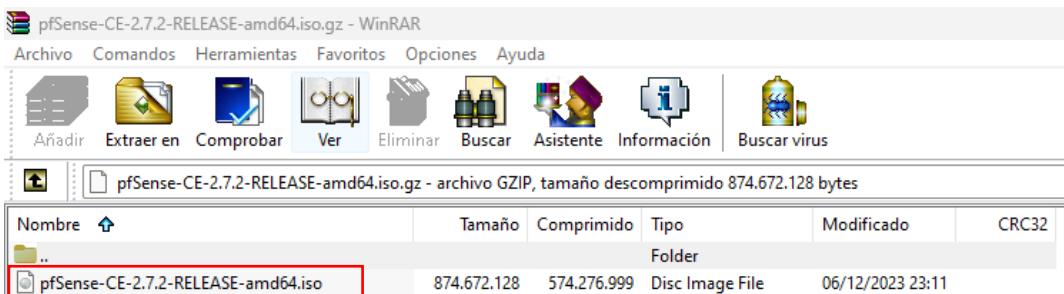
Index of /mirror/downloads/

..	old/		
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz		06-Jun-2024 19:18	-
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256		31-Jan-2022 20:31	437073513
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz		31-Jan-2022 20:32	114
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256		29-Jun-2023 20:11	495733706
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz		29-Jun-2023 20:11	114
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz.sha256		17-Nov-2023 00:47	574639430
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz		17-Nov-2023 00:47	114
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.sha256		08-Dec-2023 18:27	574277009
pfSense-CE-memstick-2.6.0-RELEASE-amd64.img.gz		08-Dec-2023 18:27	114
		31-Jan-2022 20:40	438161574

- ✓ Verificamos la integridad mediante el hash SHA256 (opcional, pero recomendado).
1. Descomprimimos el archivo para acceder a la imagen ISO de pfSense.



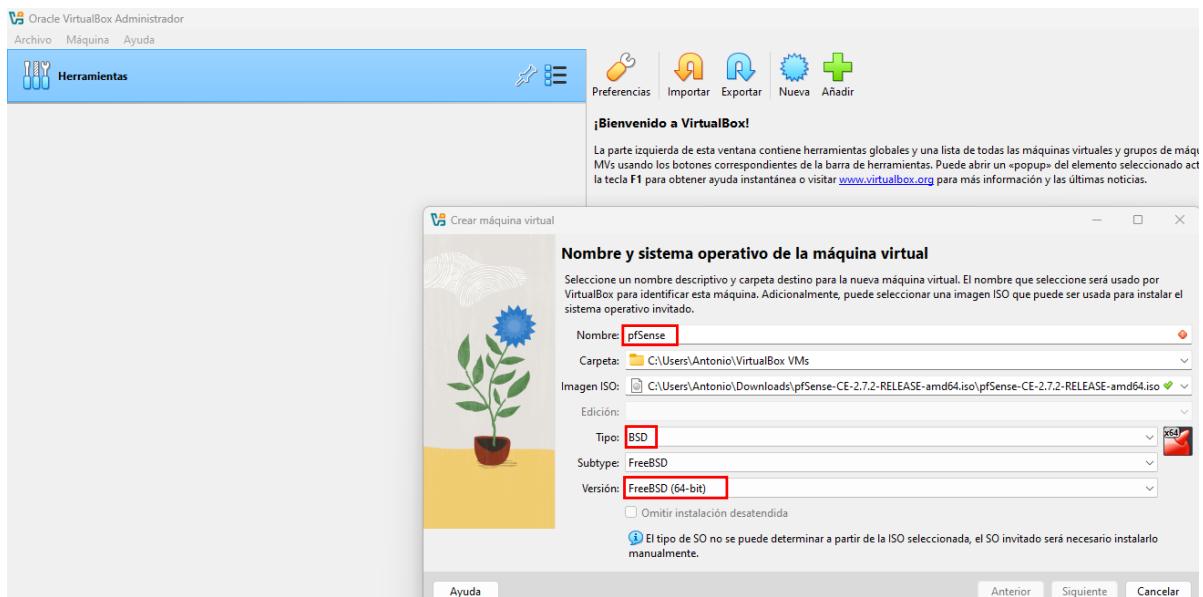
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



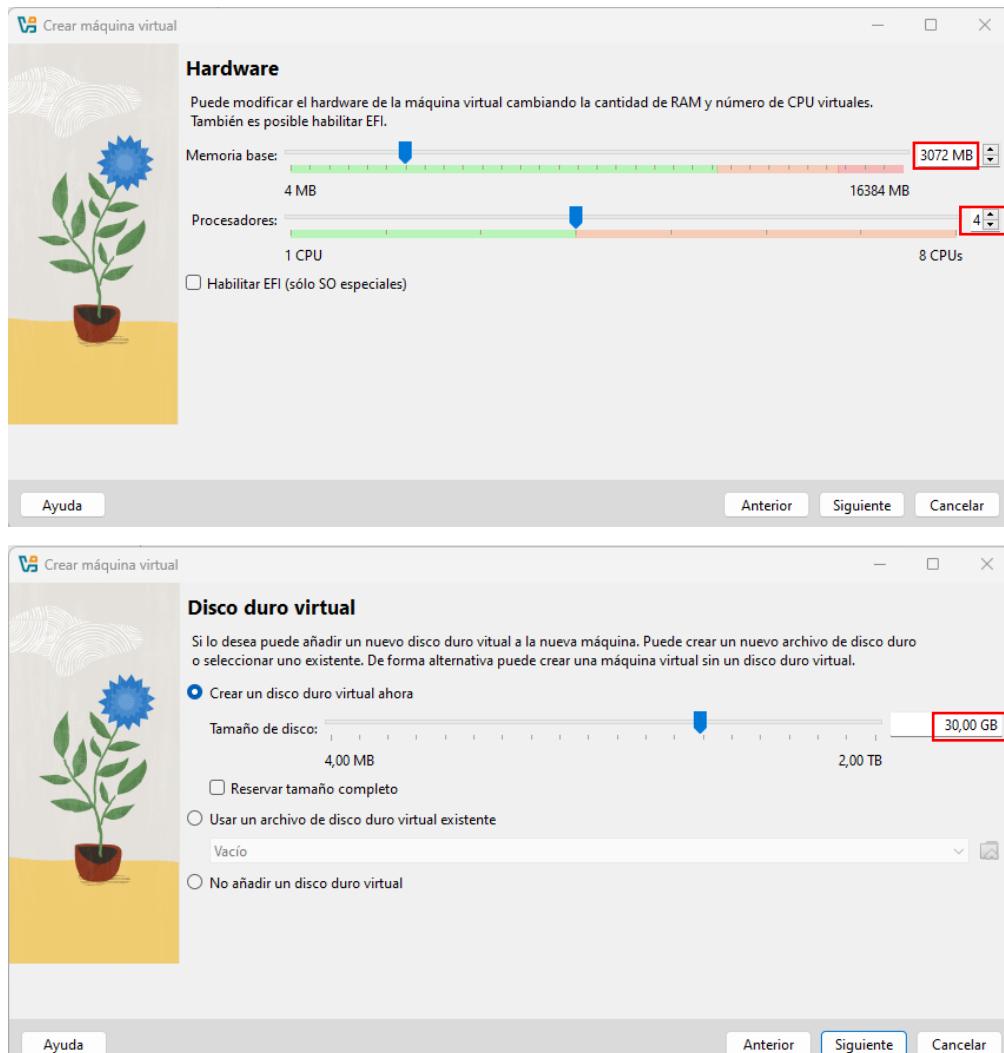
- ✓ Encima del fichero, botón derecho extraer en la carpeta que especifiquemos.



- Abierto VirtualBox, creamos la máquina virtual haciendo clic en el menú del lado derecho llamado “caja de herramientas” - “Nueva”.
- Nombre: **pfSense**.
 - Imagen ISO: **pfSense-CE-2.7.2-RELEASE-amd64.iso**
 - Tipo: **BSD**.
 - Versión: **FreeBSD (64-bit)**.
 - RAM: **3072 MB** o más.
 - Procesadores: **4 CPU**.
 - Disco duro: **30 GB** (tipo VDI, reservado dinámicamente).
 - Añadir **2 adaptadores de red**:
 - Adaptador 1 (WAN): modo **Adaptador puente**.
 - Adaptador 2 (LAN): modo **Red interna** “miredlan”

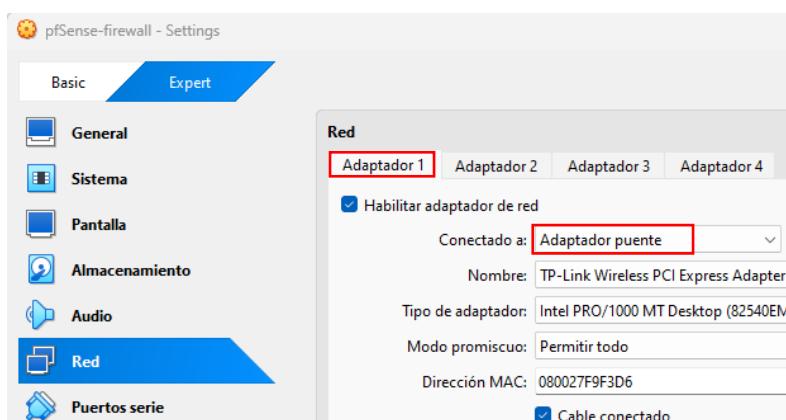


	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo		Proyecto de Administración de sistemas informáticos en red.	



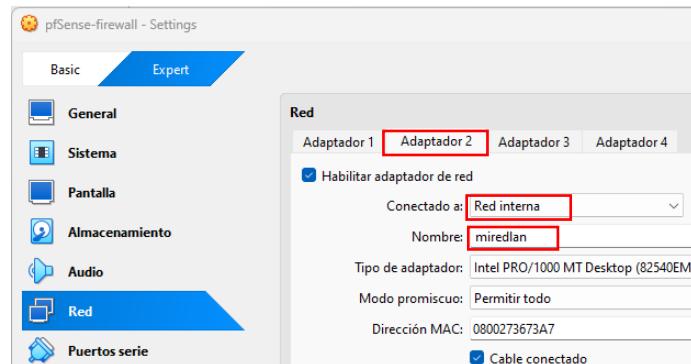
3. Creada la VM pfSense, configuramos las dos interfaces de red WAN y LAN.

Accedemos al icono “Configuración” que está en el menú superior, abriéndose el siguiente cuadro de diálogo donde elegiremos el modo “experto”, seleccionando el primer “Adaptador 1” de red (interfaz-Adaptador puente).

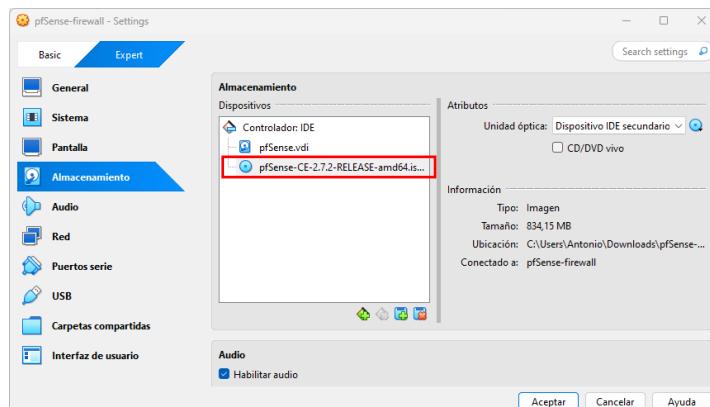


	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

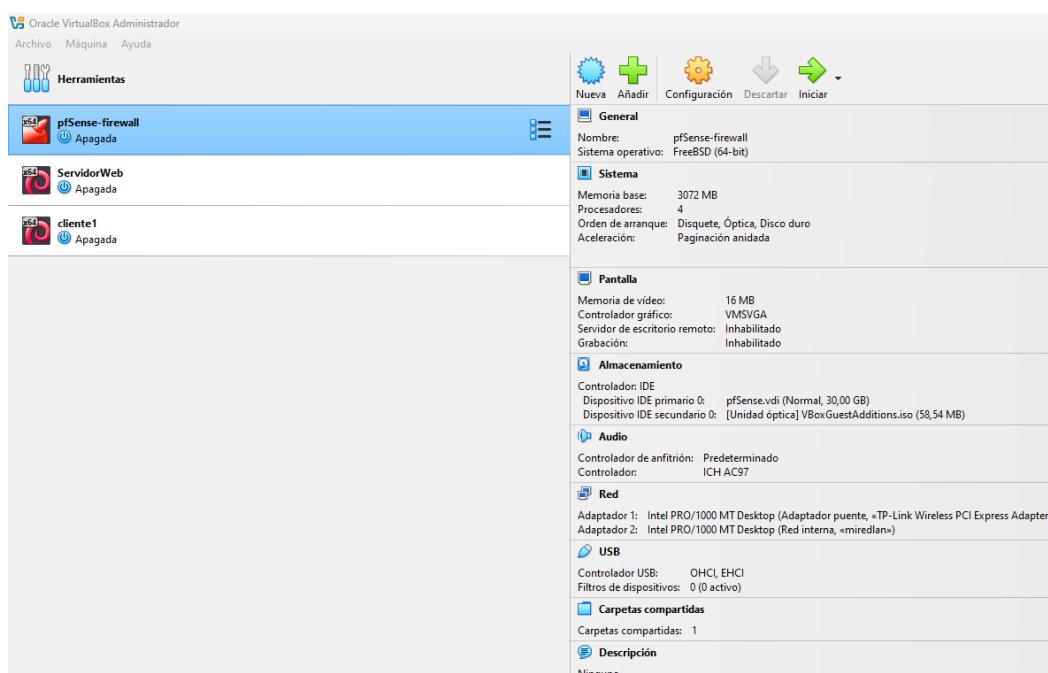
Hacemos clic en el “Adaptador 2” y elegimos Red interna (interfaz-LAN) “miredlan”.



4. Nos desplazamos al menú “Almacenamiento” para montar la imagen ISO de pfSense, la seleccionamos e iniciamos la instalación.



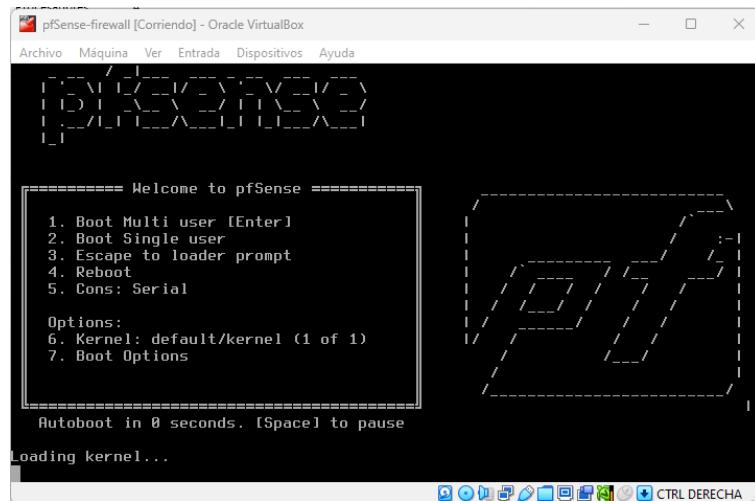
5. Resumen de la configuración de la máquina virtual pfSense.



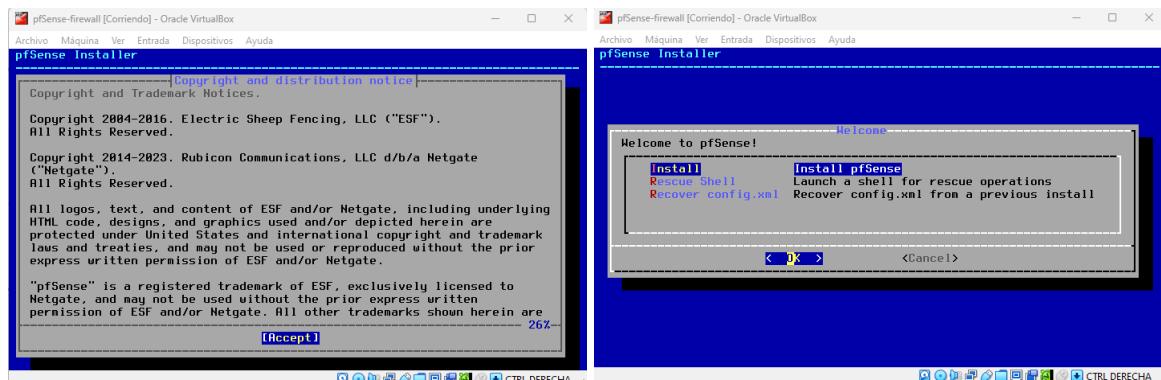
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

6. Arrancamos la máquina virtual pfSense, para proceder con la instalación y configuración, una vez descargada la imagen ISO y configurado los adaptadores de red 1 y 2.

Nos vamos al menú “caja de herramientas” y hacemos clic en “Iniciar” para que arranque nuestra VM.



7. El proceso de instalación es sencillo, se nos abre el instalador para que realicemos su instalación y configuración, le damos a “Aceptar” y a “OK”.



8. Por defecto nos realiza la instalación del teclado en el idioma “español”.
9. Elegimos el tipo de partición de archivos, en este caso “Auto (ZFS)”.

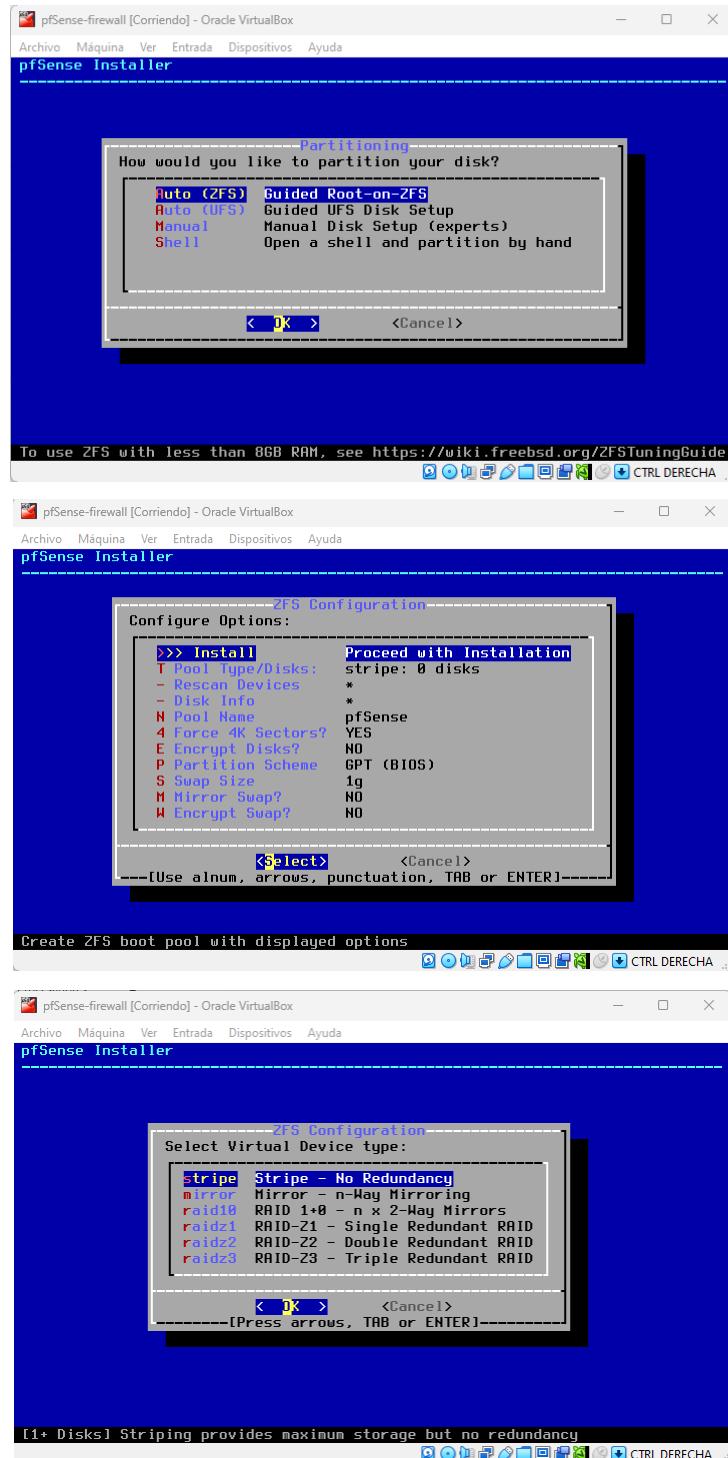
¿Qué es ZFS?

En pfSense, la opción "Auto (ZFS)" utiliza el sistema de archivos ZFS para el almacenamiento de datos del sistema, incluyendo configuraciones y registros. Desarrollado por Sun Microsystems y ahora propiedad de Oracle, ofrece características avanzadas como integridad de datos, redundancia y creación de instantáneas, agrupar dispositivos de almacenamiento en

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

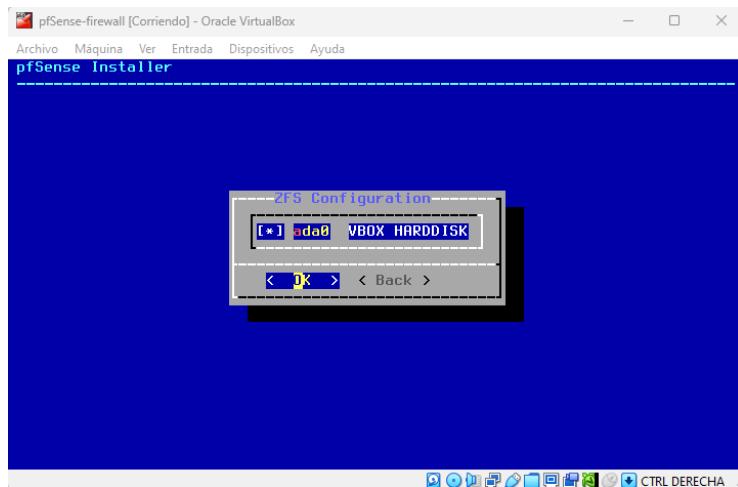
"Pools" escalables, soporta snapshots para recuperación de datos y replicación para mayor seguridad y disponibilidad.

Damos a "Intro o Enter" varias veces.



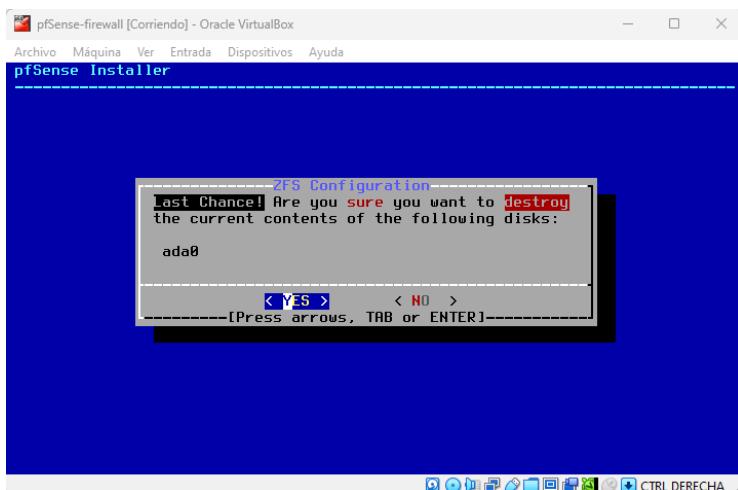
Damos a la "tecla espacio" para que se ponga el asterisco y presionamos "Intro o Enter".

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

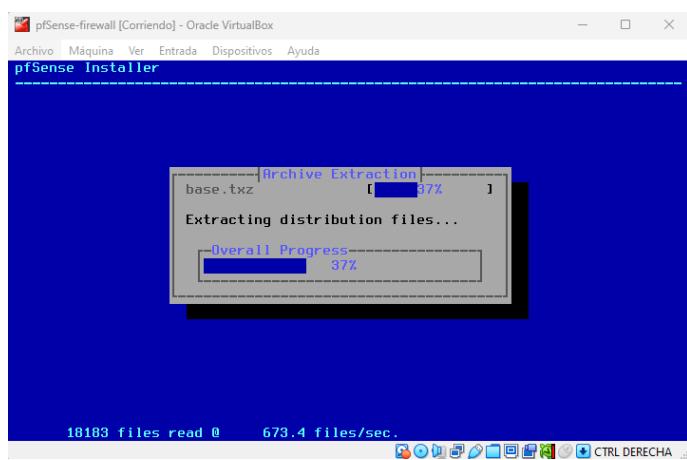


10. ¿Está seguro de que desea destruir (escribir) el contenido actual de los siguientes discos: **ada0**

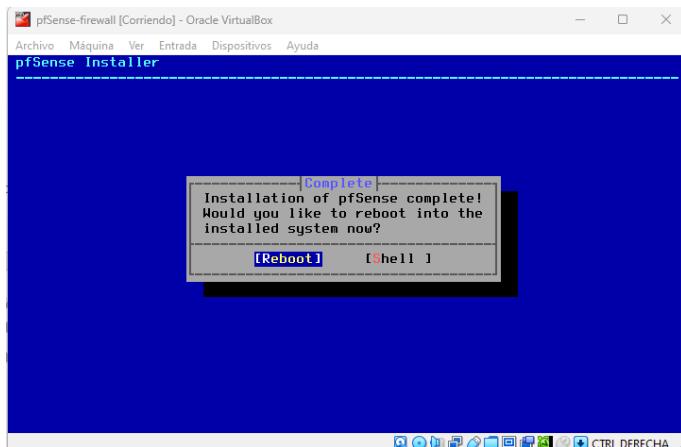
Por defecto aparece en NO, con la tecla “flecha” cambiamos a la posición YES.



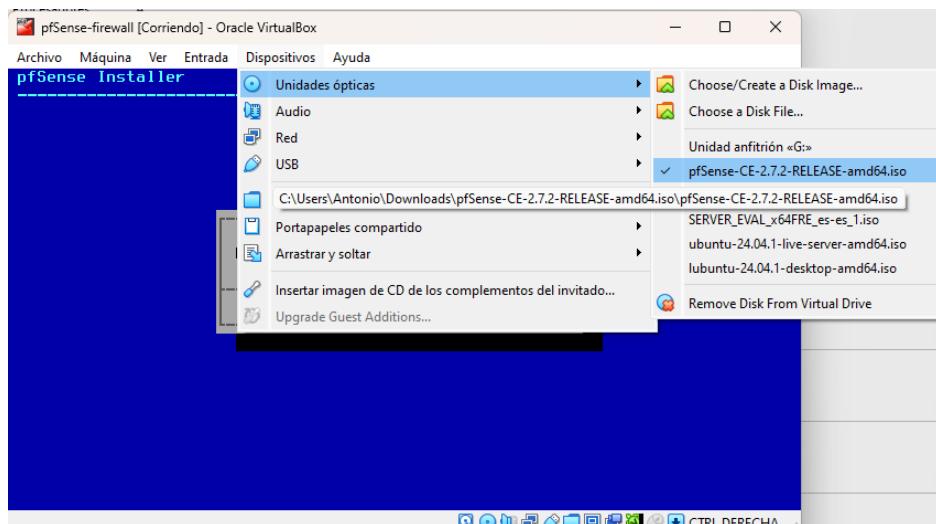
11. Copiándose los archivos en el almacenamiento y finalizando la instalación.



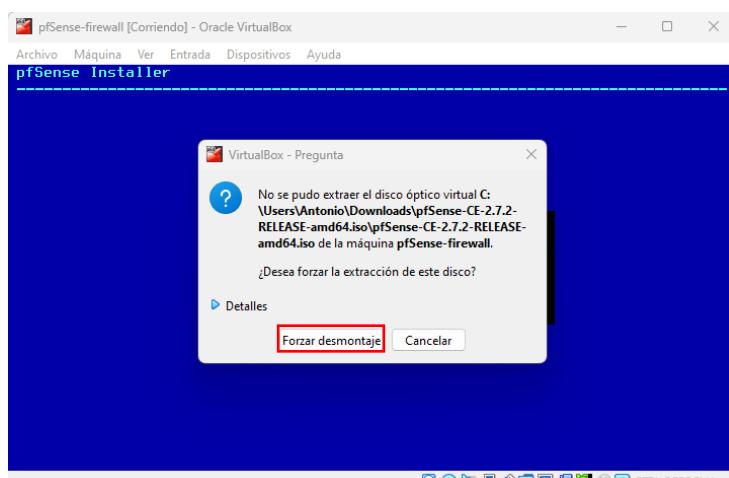
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------



12. Reiniciamos pfSense, para ello antes de reiniciar retiramos la imagen ISO que tenemos en la unidad virtual CD, yéndonos al menú “Dispositivos” “Unidades ópticas” y desmarcamos la imagen.

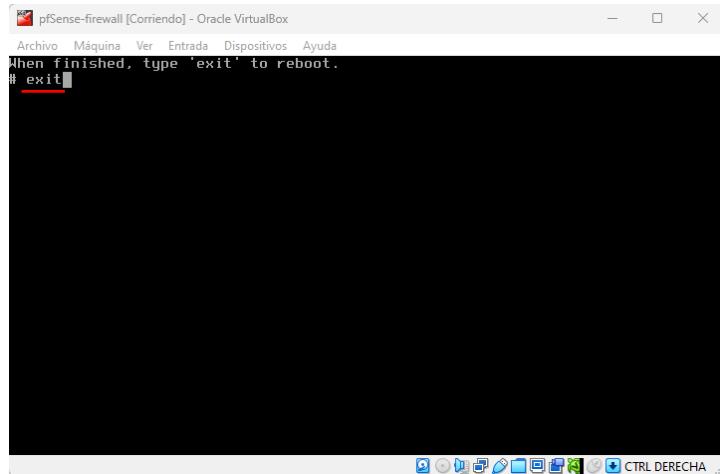


13. Forzamos el desmontaje de la imagen, pulsando en la pestaña “Forzar desmontaje”.

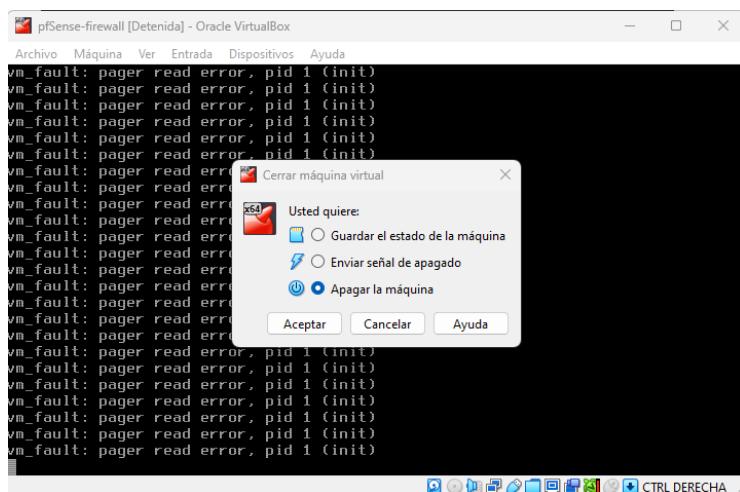


	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

14. Presionamos “Intro o Enter” para hacer el reinicio y escribimos “exit” para reiniciar.



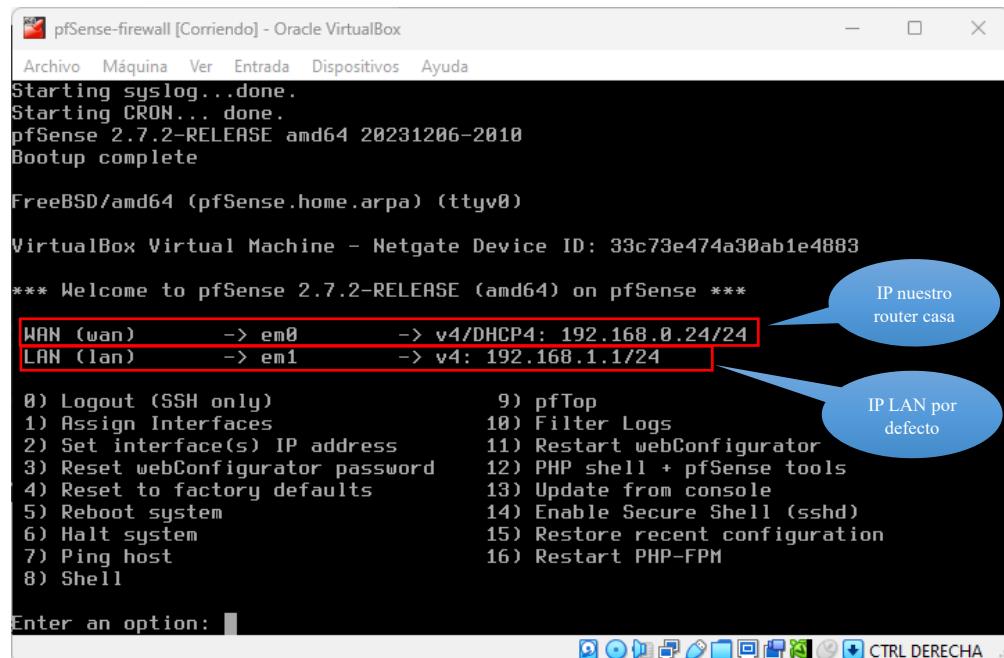
15. Nos puede dar un error como este, forzamos el cierre de la máquina dándole a cerrar, y después seleccionamos “Apagar la máquina”, parando la VM.



4.2.1 Configuración de VM pfSense (Firewall).

1. Iniciamos la VM, y una vez que finaliza de cargar, nos muestra el menú principal con los valores por defecto de fábrica, mostrándonos distintas opciones numeradas que podemos seleccionar utilizando la línea de comandos, en caso de querer realizar cambios. En nuestro caso cambiaremos la IP 192.168.1.1/24 (puerta de enlace) por una configurada manualmente por nosotros **192.168.1.10/24**.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 33c73e474a30ab1e4883

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.24/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

En la opción **1)** podemos asignar interfaces.

Ejemplo:

- La interfaz **em0** será nuestra **WAN** la interfaz **em1** será la **LAN**, etc.

En la opción **2)** podemos configurar direcciones IP.

En la opción **3)** podemos restear la contraseña de la interfaz gráfica accediendo a través del navegador web.

En la opción **4)** podemos resetear a valores de fábrica.

En la opción **5)** podemos reiniciar el sistema.

En la opción **6)** podemos apagar el sistema.

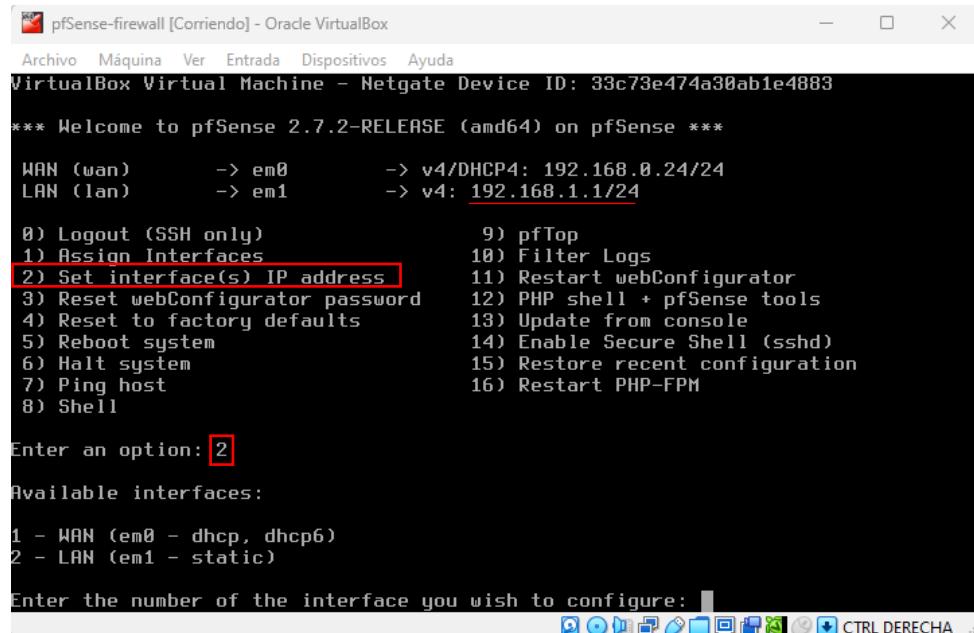
En la opción **7)** podemos hacer un ping, y así, podemos seguir en las siguientes opciones y hacer más cosas como restaurar la configuración del navegador web.

- Se puede ver que la interfaz WAN, está asignando la dirección IP de nuestro router, el cual tiene activado el DHCP, y la interfaz LAN nos muestra por defecto una IP.

2. Configuramos la **IP LAN** para asignar una nueva IP **192.168.1.10/24**.

Elegimos la **opción 2)**

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	



```

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.24/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: 2

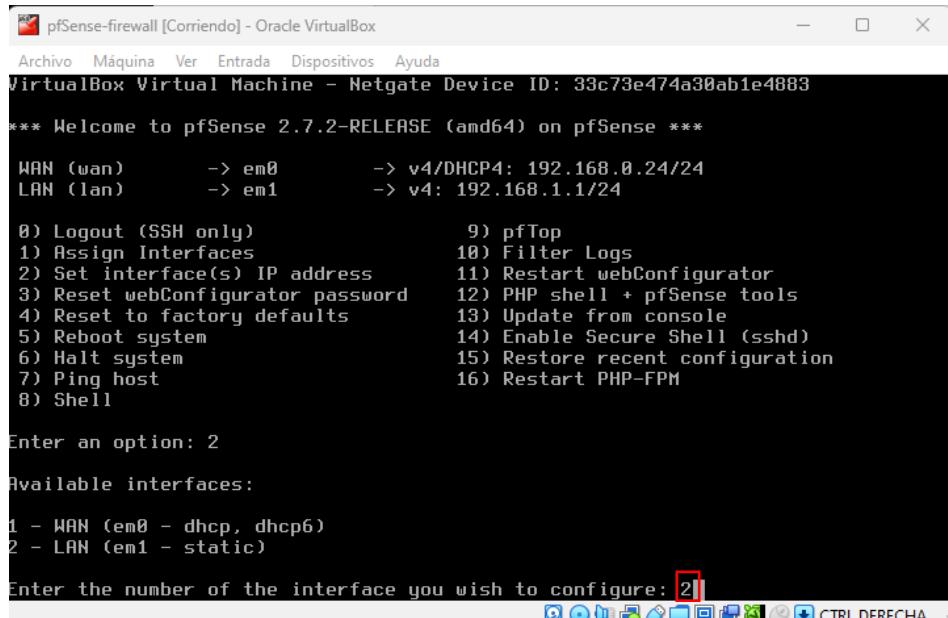
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

```

3. Introducimos el número 2 de la interfaz LAN que es, la que queremos configurar.



```

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.24/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: 2

Available interfaces:

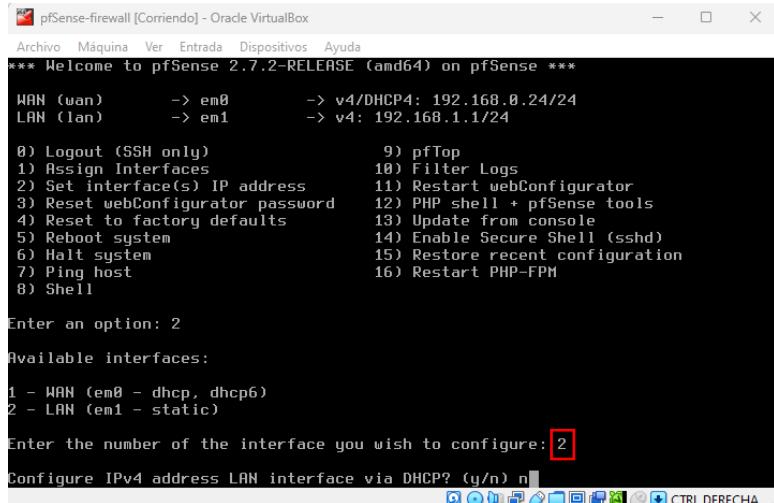
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

```

4. Pregunta si queremos configurar la nueva dirección IP activando el DHCP y le decimos que NO, porque la IP la usaremos en nuestra red interna, así, que nos interesa que sea estática.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.24/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

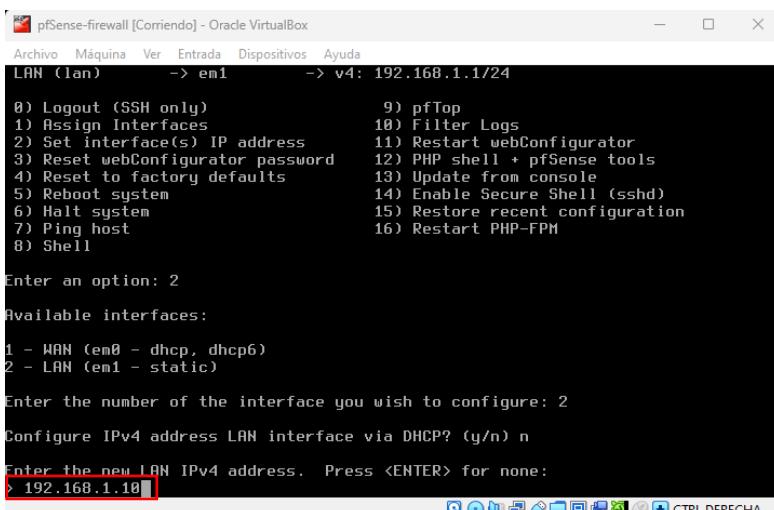
Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n

```

5. Introducimos la nueva dirección IP LAN que queremos establecer.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

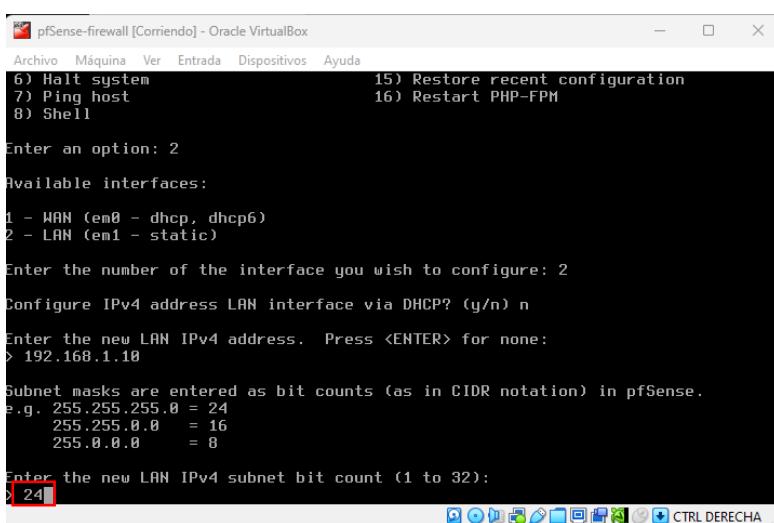
Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

```

6. Pregunta cuál será la máscara de subred.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
6) Halt system                 15) Restore recent configuration
7) Ping host                    16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

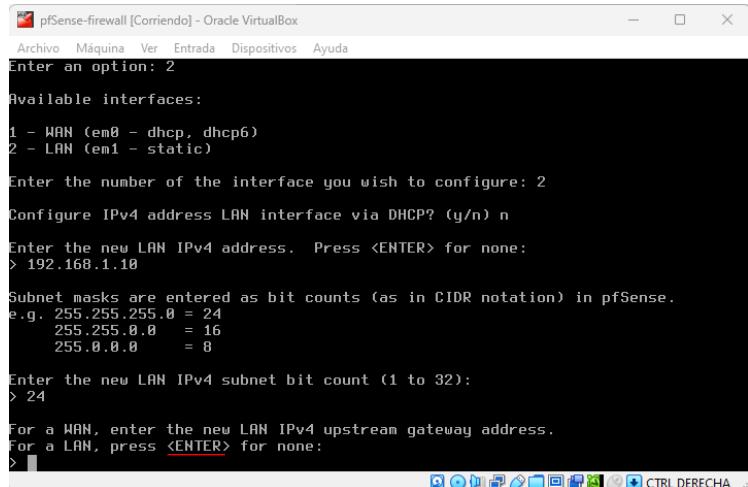
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

```

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

7. Pregunta si es para una red LAN, presionamos “Enter”.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

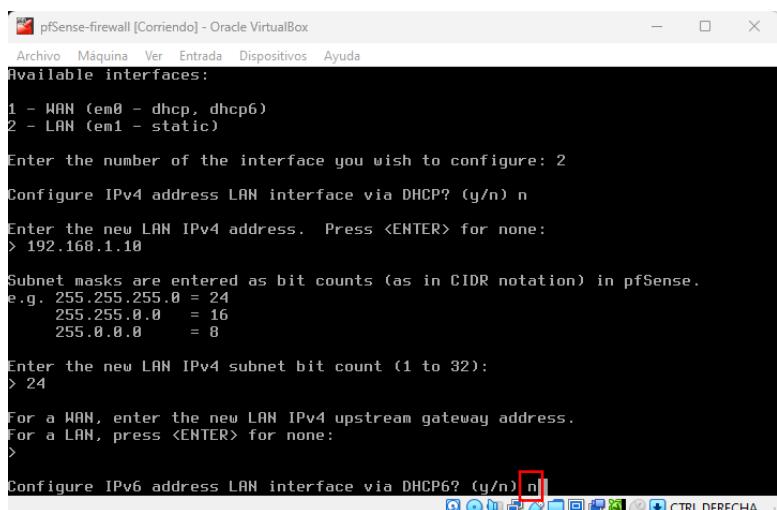
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

```

8. Pregunta si queremos configurar IPv6 a través del DHCP6, decimos que NO.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

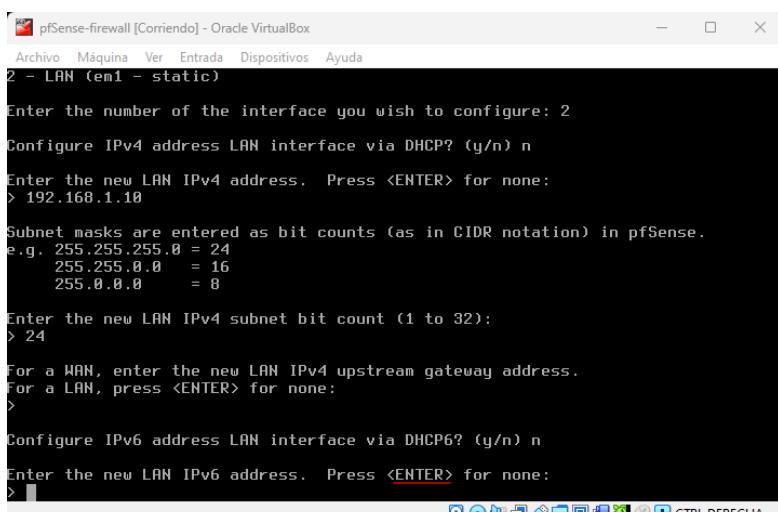
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

```

9. Pregunta si queremos asignar IPv6 de forma estática, presionamos “Enter”.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

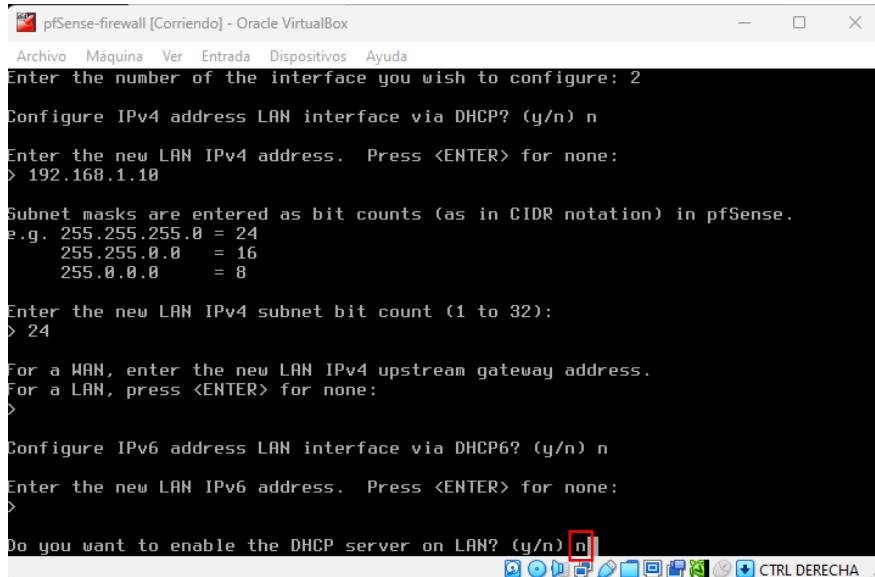
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

10. Pregunta si queremos configurar un servidor con DHCP en la LAN, decimos que **NO**.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

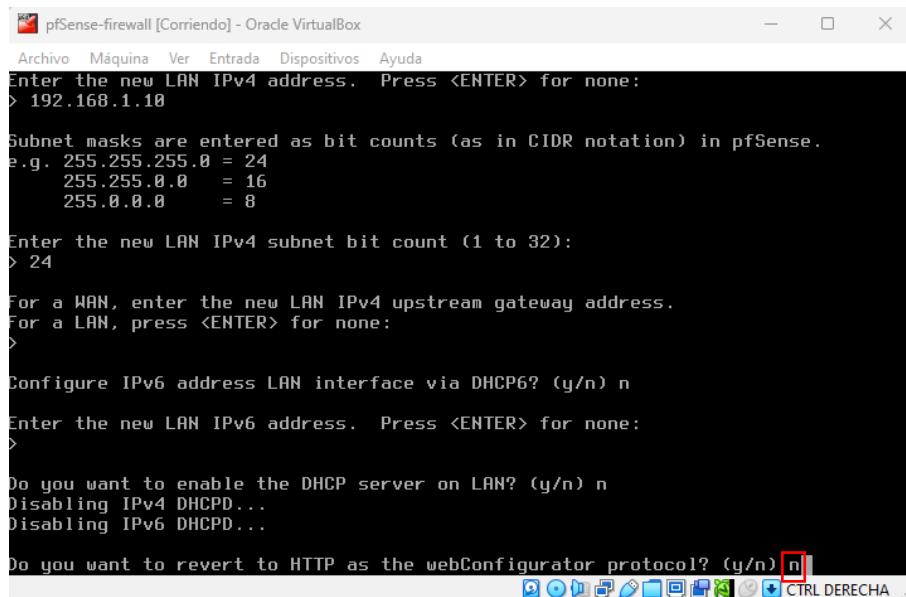
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

```

11. Pregunta si queremos utilizar HTTP para la configuración a través del navegador web, decimos que **NO**, porque queremos acceder a través de HTTPS.



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

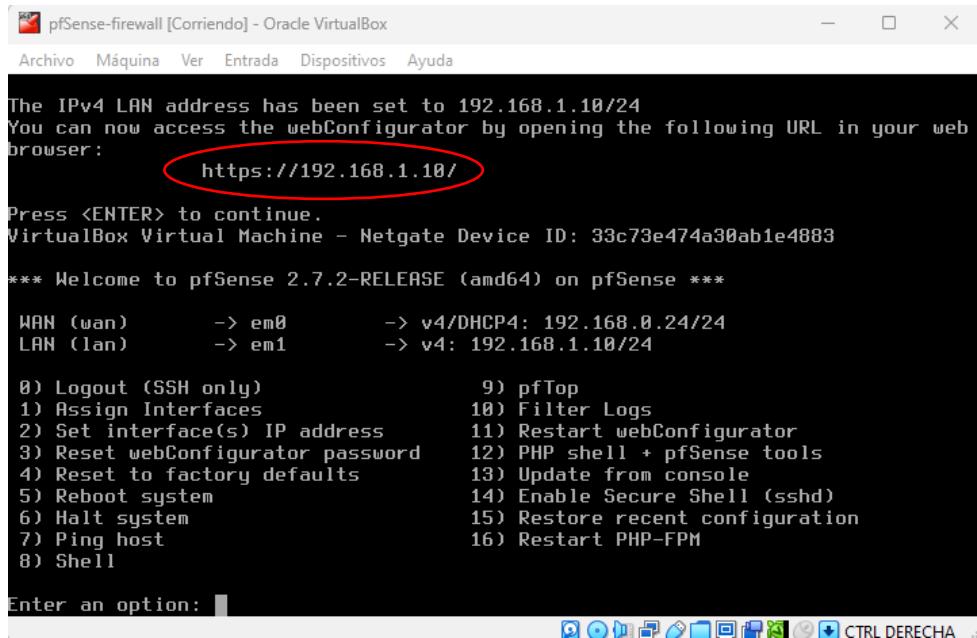
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

```

12. Finalmente aceptamos los cambios presionando “Enter”, estableciéndose el cambio a la IP LAN que hemos configurado, pudiendo acceder a través del navegador a pfSense con un cliente siempre que el equipo estuviera conectado a la interfaz LAN.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	



```

pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

The IPv4 LAN address has been set to 192.168.1.10/24
You can now access the webConfigurator by opening the following URL in your web
brouser:
    https://192.168.1.10/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 33c73e474a30ab1e4883

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.24/24
LAN (lan)      -> em1      -> v4: 192.168.1.10/24

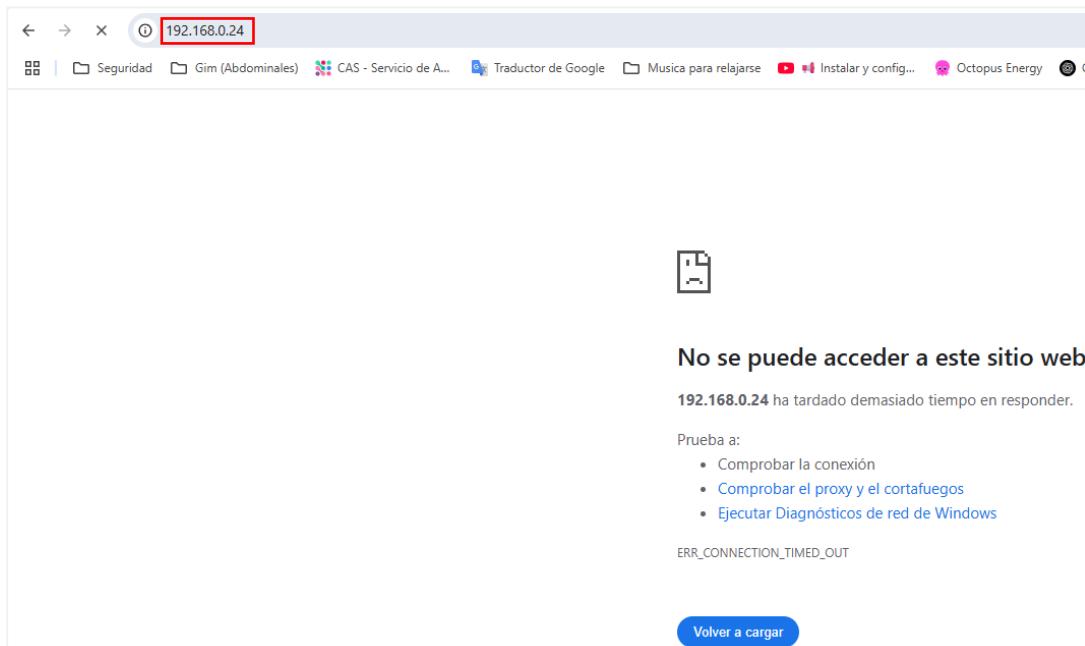
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable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

Enter an option: ■

```

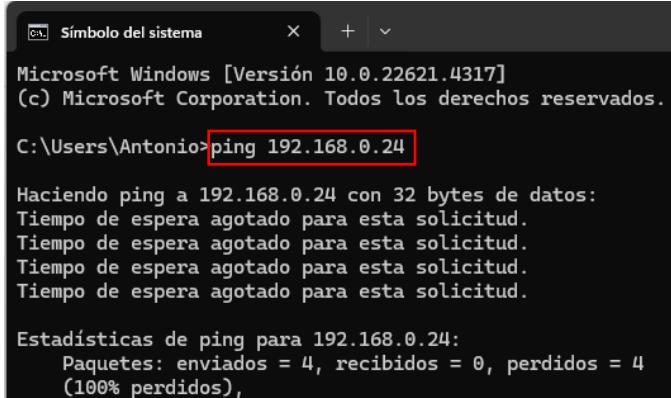
13. Realizamos una prueba para que se pueda ver, que no se puede acceder desde el navegador de nuestro equipo anfitrión Windows 11 a pfSense porque tiene bloqueado el puerto desde la WAN y no deja pasar ninguna petición que venga desde Internet como medida de seguridad.

▪ <https://192.168.0.24>



14. Hacemos un ping desde “Símbolo de sistema” desde el anfitrión y vemos que tampoco responde porque hay reglas que están bloqueando el acceso.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



```

Símbolo del sistema
Microsoft Windows [Versión 10.0.22621.4317]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Antonio>ping 192.168.0.24

Haciendo ping a 192.168.0.24 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.24:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),
  
```

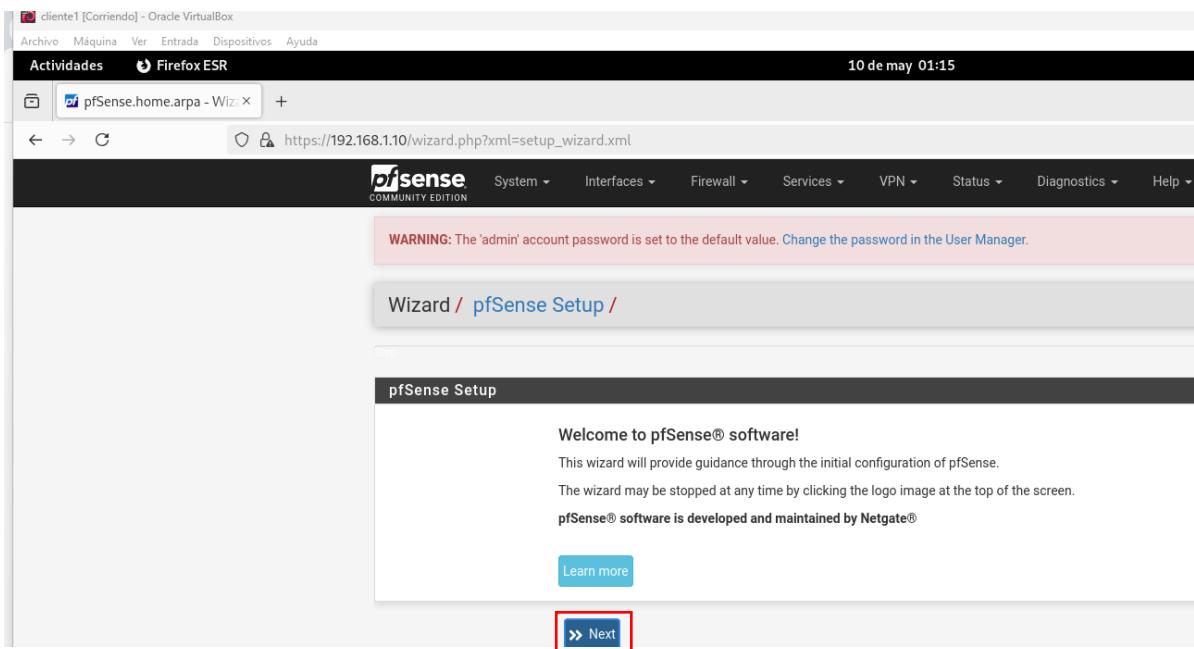
15. Podemos deshabilitar pfSense (firewall) a través de la Shell (**opción 8**), ejecutando el comando.

- pfctl -d (Deshabilitar el firewall).
- pfctl -e (Habilitar el firewall).

Y ahora sí podríamos acceder desde el navegador del equipo anfitrión y configurar pfSense, pero nosotros lo configuraremos desde el cliente1, más adelante realizaremos cambios y haremos pruebas.

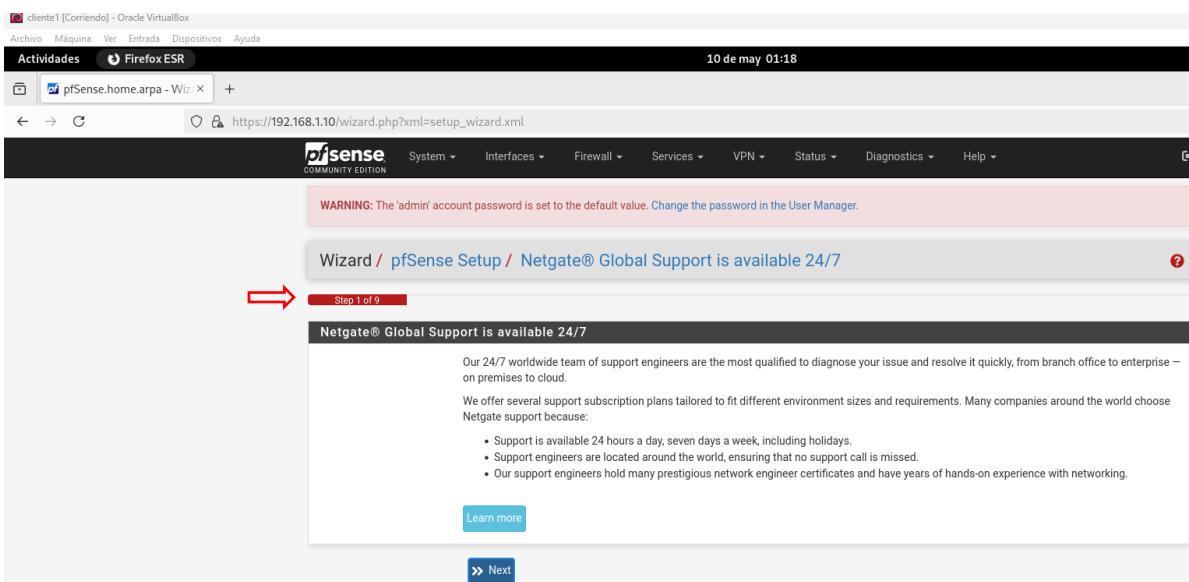
4.1.1.1 Configuración inicial del panel de administración (firewall pfSense).

1. Comenzamos con la bienvenida, pulsamos en “Next”.



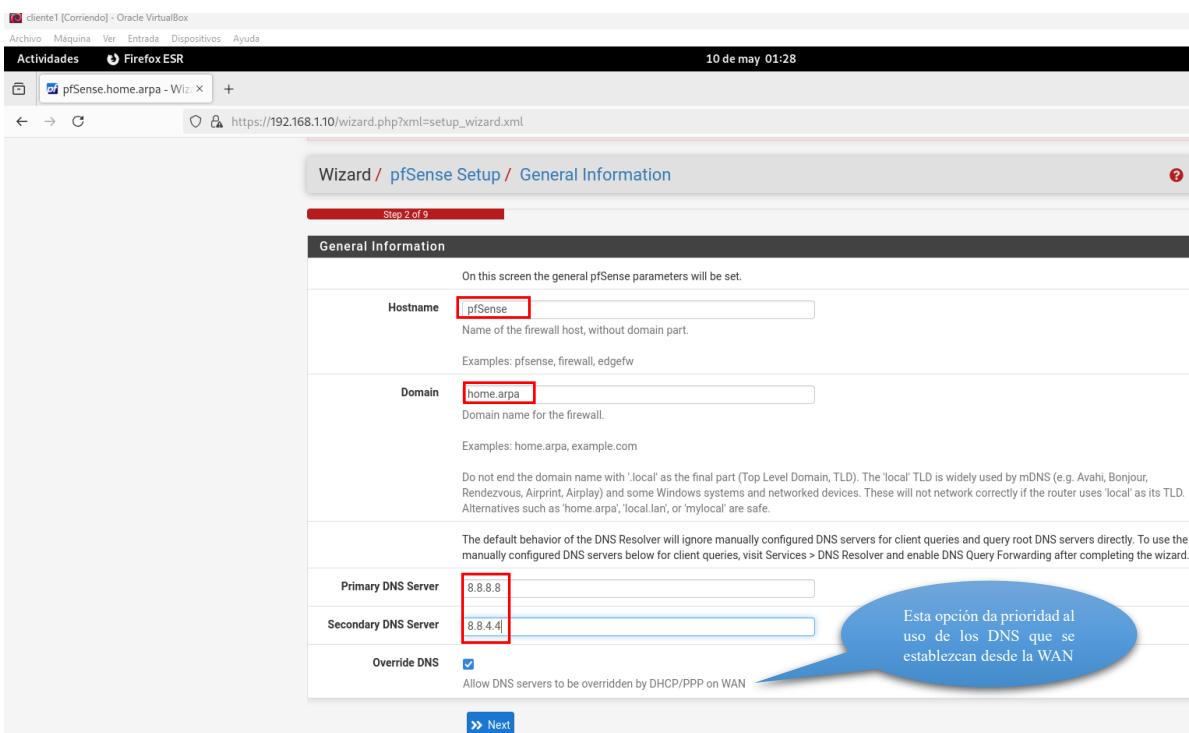
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

2. Podemos ver que son 9 pasos los que tendremos que configurar con los datos oportunos, en cada una de las ventanas que nos vayan saliendo.



The screenshot shows the first step of the pfSense setup wizard. The title bar says 'Wizard / pfSense Setup / Netgate® Global Support is available 24/7'. Below it, a progress bar indicates 'Step 1 of 9'. The main content area discusses Netgate support, mentioning 24/7 availability and various support plans. It includes a 'Learn more' button and a 'Next' button at the bottom.

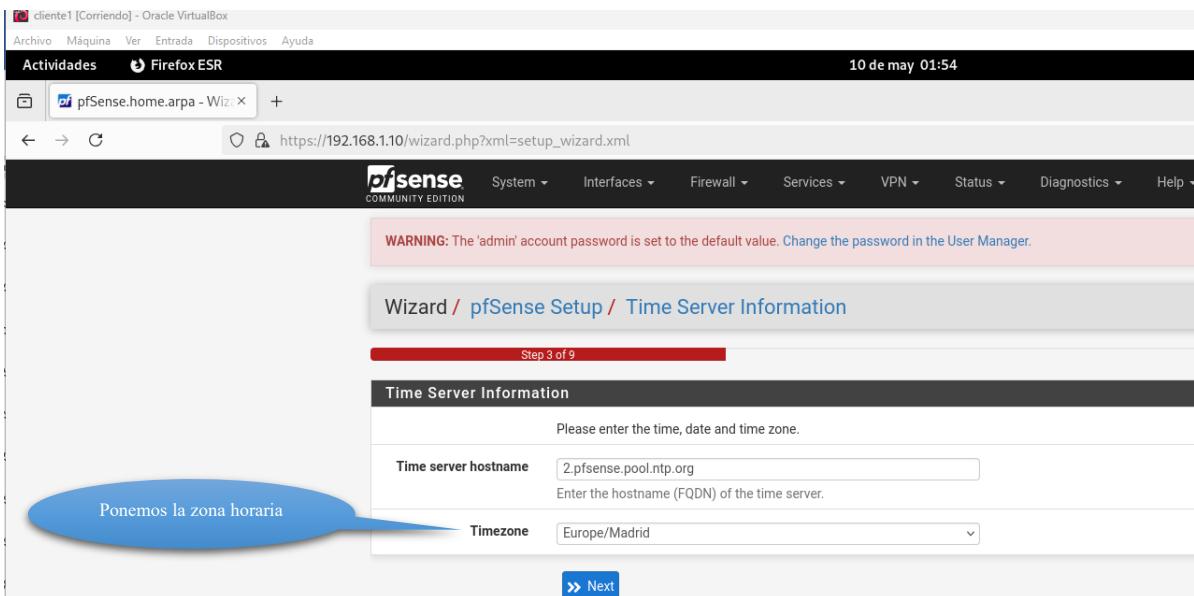
3. Ponemos el nombre “pfSense”, dejamos el dominio por defecto “home.arpa” y ponemos los DNS primario 8.8.8.8 y secundario 8.8.4.4 de Google.



The screenshot shows the second step of the pfSense setup wizard, titled 'General Information'. It asks for the host name ('Hostname') and domain ('Domain'), both set to 'pfSense' and 'home.arpa' respectively. Under 'Primary DNS Server', the IP '8.8.8.8' is entered, and under 'Secondary DNS Server', the IP '8.8.4.4' is entered. A blue callout bubble points to the 'Override DNS' checkbox with the text: 'Esta opción da prioridad al uso de los DNS que se establezcan desde la WAN'.

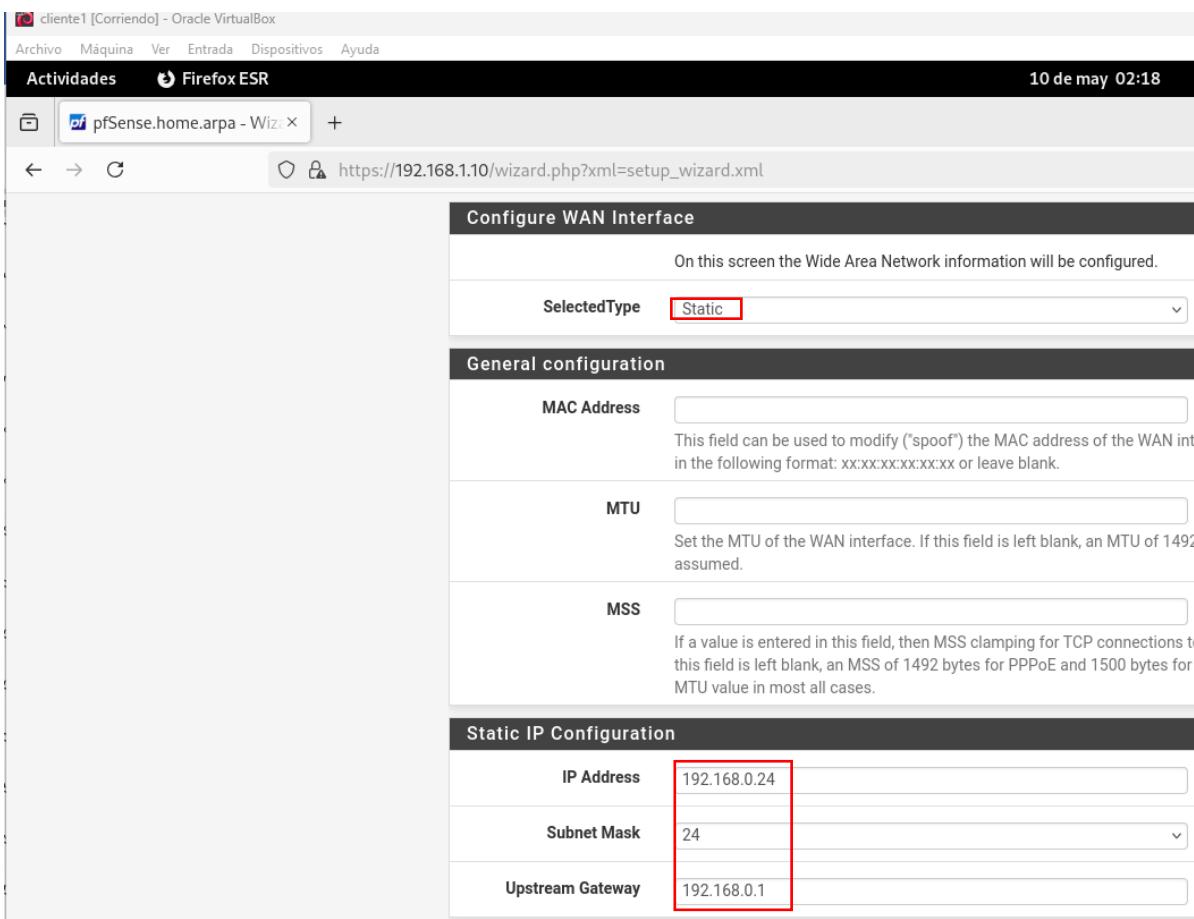
4. Esta ventana la dejamos como viene por defecto, no tocamos el servidor del tiempo.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



Ponemos la zona horaria

5. En la siguiente ventana configuraremos pfSense para que tenga una “IP estática” 192.168.0.24/24, y la puerta de enlace 192.168.0.1/24, deshabilitamos las dos casillas para que las redes privadas puedan entrar a través de la WAN.



Static IP Configuration	
IP Address	192.168.0.24
Subnet Mask	24
Upstream Gateway	192.168.0.1

	Dpto. Informática	Ciclo Módulo	CFGs de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

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

>> Next

6. Dejamos por defecto la red LAN y su máscara, la configuraremos anteriormente.

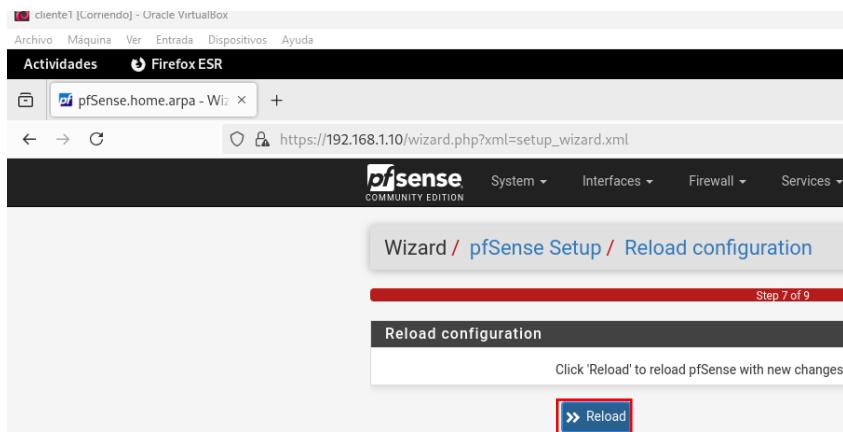
The screenshot shows the pfSense setup wizard at Step 5 of 9, titled "Configure LAN Interface". It displays the configuration for the Local Area Network. The "LAN IP Address" field contains "192.168.1.10" and the "Subnet Mask" dropdown is set to "24". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Management screen." A "Next" button is visible at the bottom right.

7. Configuramos la contraseña del administrador “Admin”.

The screenshot shows the pfSense setup wizard at Step 6 of 9, titled "Set Admin WebGUI Password". It asks for the admin password to be set. Both the "Admin Password" and "Admin Password AGAIN" fields contain the password "123456". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Management screen." A "Next" button is visible at the bottom right.

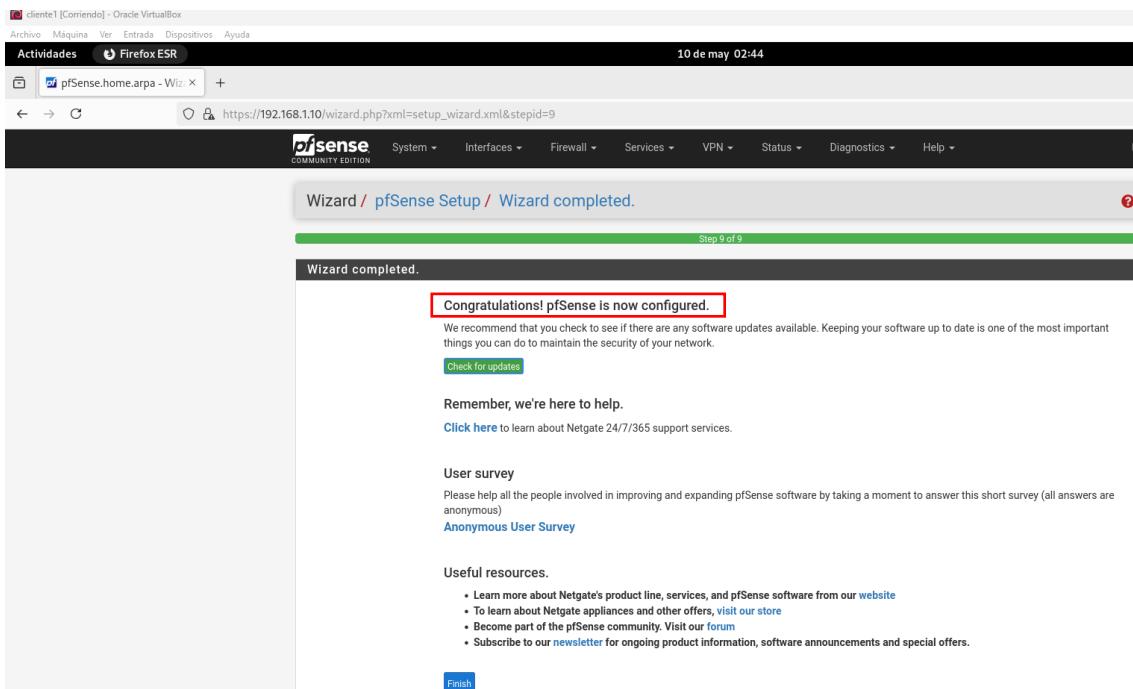
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

8. Recargamos para guardar los cambios.



The screenshot shows a Firefox browser window titled "cliente1 [Corriendo] - Oracle VirtualBox". The address bar shows "https://192.168.1.10/wizard.php?xml=setup_wizard.xml". The main content is the pfSense Setup Wizard, Step 7 of 9, titled "Reload configuration". It says "Click 'Reload' to reload pfSense with new changes." and features a prominent red "» Reload" button.

9. PfSense está configurado.



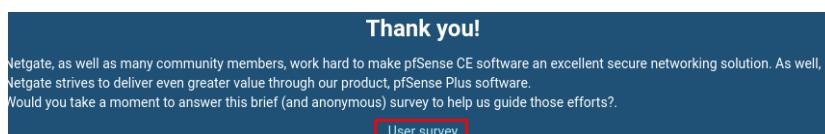
The screenshot shows a Firefox browser window titled "cliente1 [Corriendo] - Oracle VirtualBox". The address bar shows "https://192.168.1.10/wizard.php?xml=setup_wizard.xml&stepid=9". The main content is the pfSense Setup Wizard, Step 9 of 9, titled "Wizard completed.". It displays a message: "Congratulations! pfSense is now configured." followed by a note: "We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network." There is also a "Check for updates" button. Other sections include "User survey", "Useful resources", and a "Finish" button.

10. Aceptamos los términos y condiciones, no antes de leerlo.



The screenshot shows the "Copyright and Trademark Notices" page of the pfSense software. It contains legal disclaimers and notices from 2004-2016 and 2014-2025. It includes information about Netgate's product line, services, and pfSense software, as well as trademarks for pfSense, Netgate, and other companies like Electric Sheep Fencing and Rubicon Communications. It also mentions the Apache 2.0 license for the software.

11. Para finalizar nos pregunta si queremos participar en una breve encuesta.

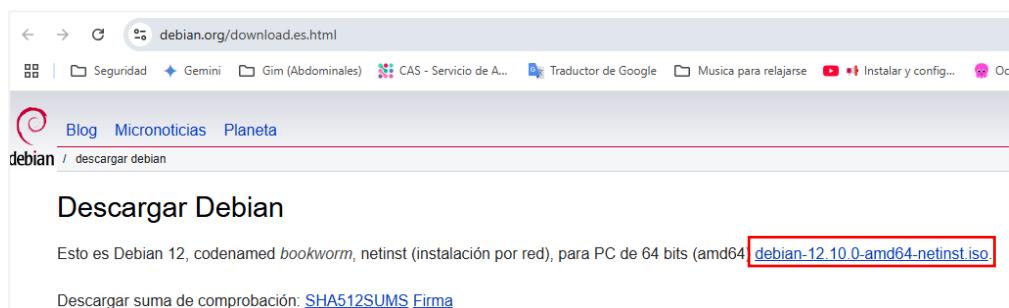


The screenshot shows a survey participation prompt. It features a "Thank you!" message, a brief description of Netgate's efforts to make pfSense a secure networking solution, and a call-to-action: "Would you take a moment to answer this brief (and anonymous) survey to help us guide those efforts?". A red "User survey" button is highlighted at the bottom.

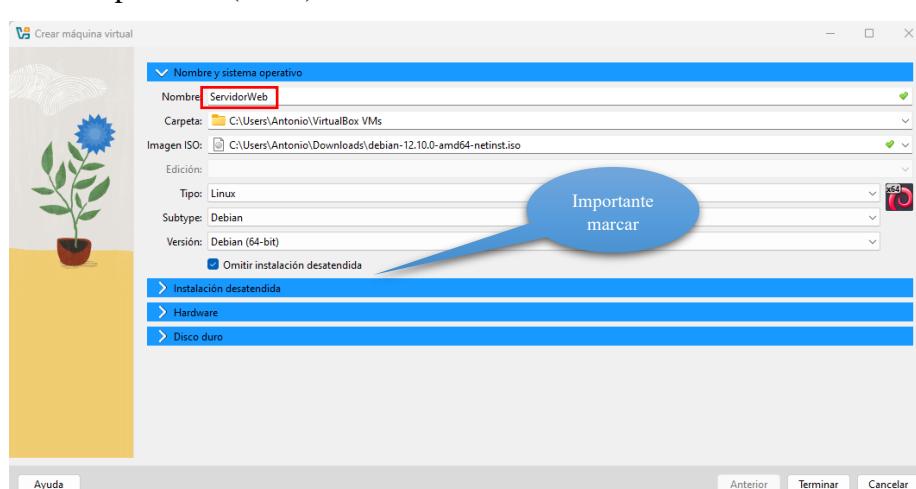
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

4.3 Instalación de VM Debian 12 (Servidor Web).

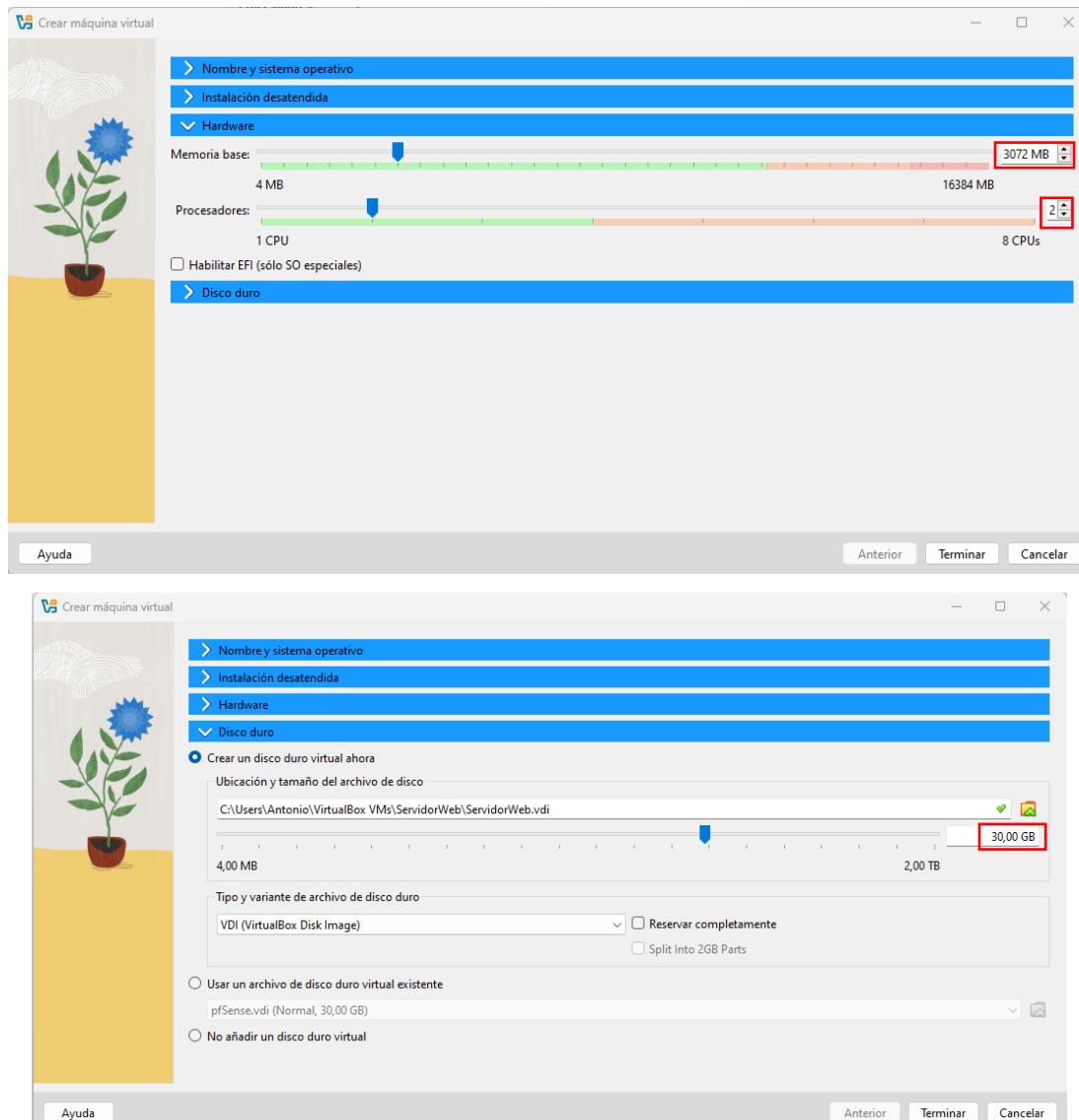
Sistema operativo utilizado tanto en el servidor web como en el cliente. Su estabilidad y seguridad lo hacen ideal para este tipo de entorno. Su descarga gratuita, está disponible en <https://www.debian.org/distrib/netinst.en.html> o <https://www.debian.org/download.es.html> seleccionando la versión estable de AMD64 (64 bits).



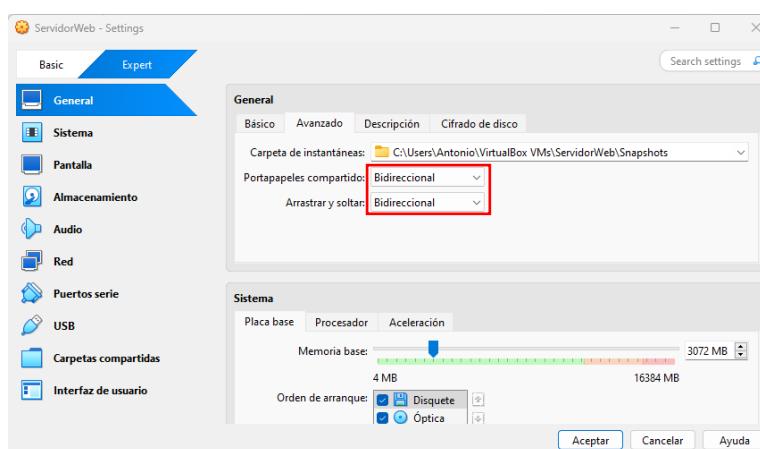
1. Creamos la máquina virtual haciendo clic en el menú del lado derecho llamado “caja de herramientas” - “Nueva”. 
- Nombre: **ServidorWeb**.
- Imagen ISO: **debian-12.10.0-amd64-netinst.iso**
- Tipo: **Linux**.
- Versión: **Debian (64-bit)**.
- RAM: **3072 MB** o más.
- Procesadores: **2 CPU**.
- Disco duro: **30 GB** (tipo VDI, reservado dinámicamente).
- Añadimos un adaptador de red:
 - Adaptador 1 (LAN): modo **Red interna** “miredlan”.



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

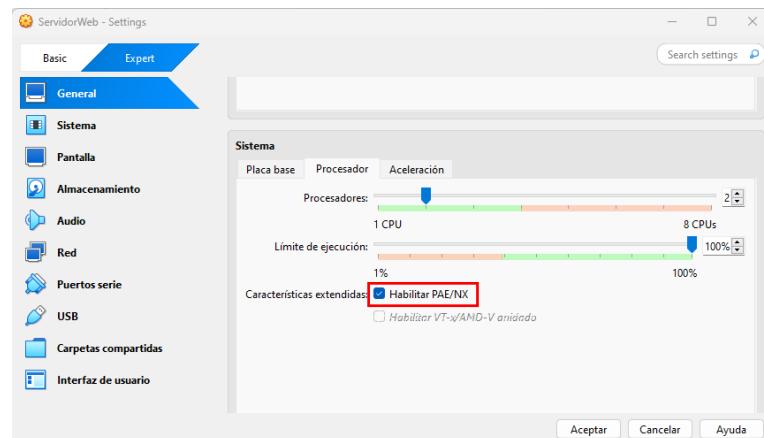


2. Configuramos algunos parámetros más en el menú “Configuración”.

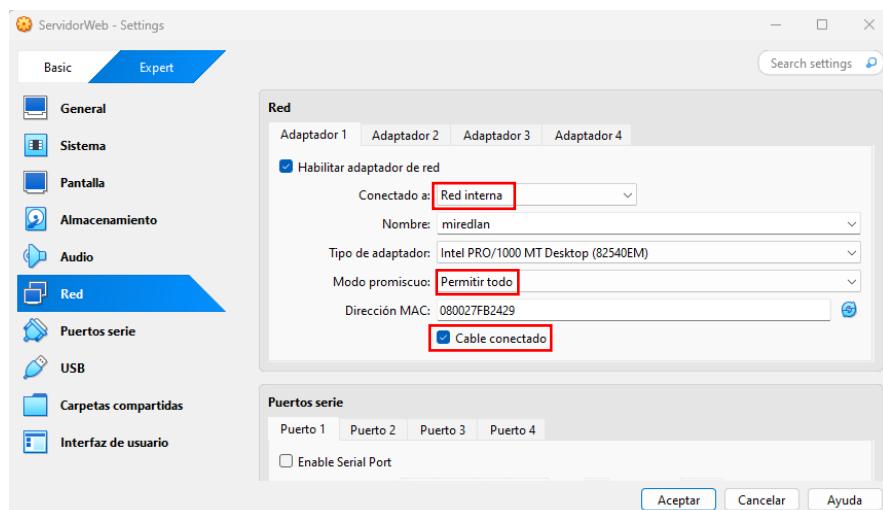


	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

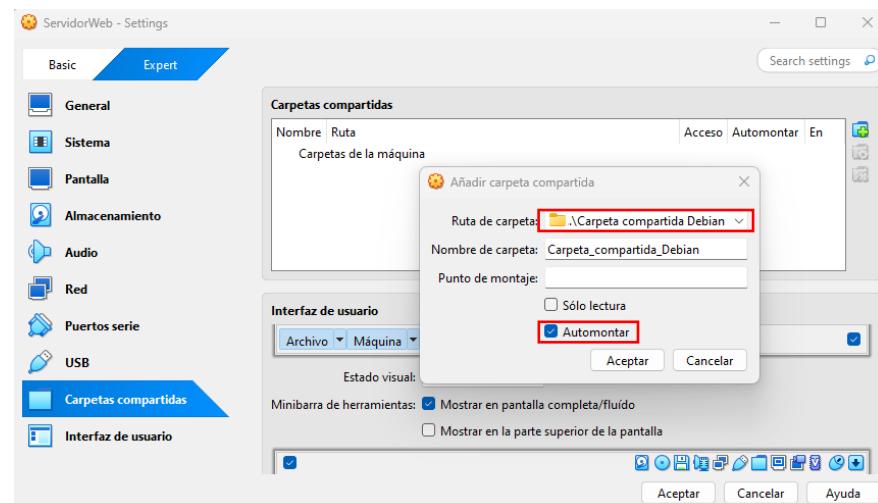
3. Marcamos la opción PAE/NX, la cual nos permitirá que una CPU de 32 bits pueda acceder a más de 4 GB de memoria RAM.



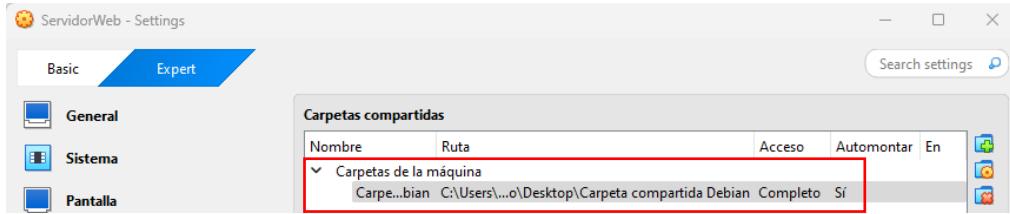
4. Configuramos y elegimos el “Adaptador 1” como Red interna “miredlan”.



5. Configuramos una carpeta compartida por si nos hiciera falta más adelante.



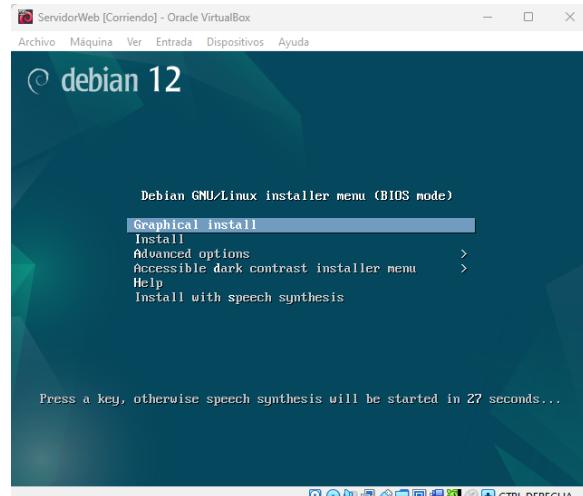
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------



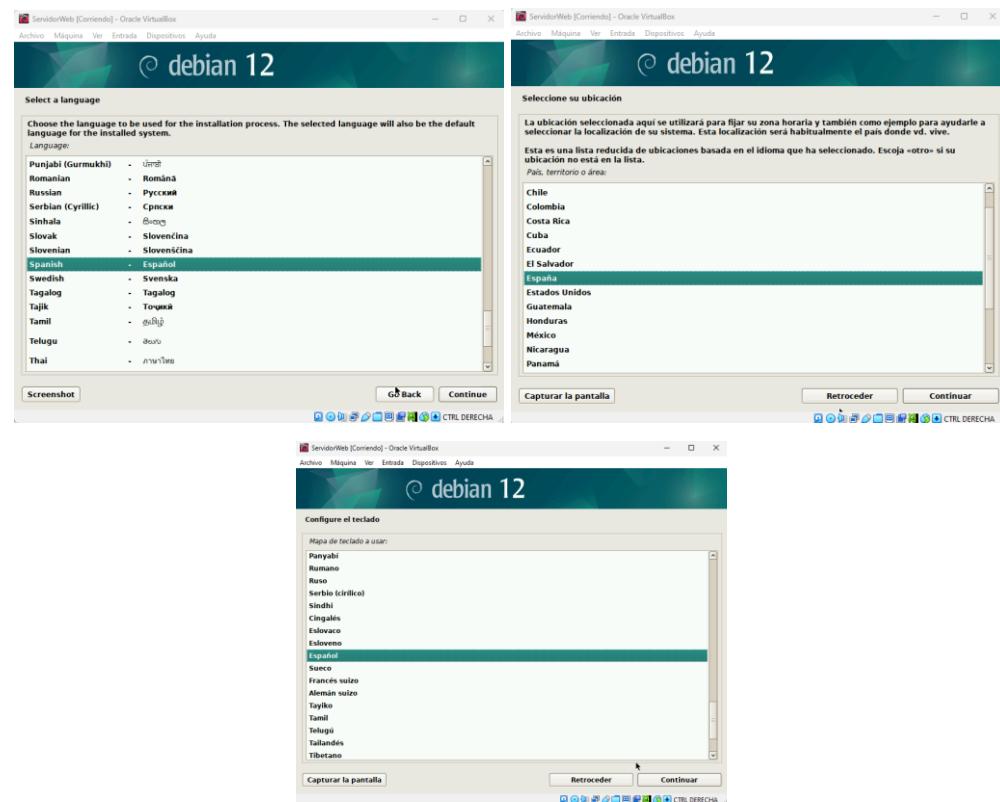
6. Damos al menú “Mostrar” para que se inicie la máquina virtual, y empieze a cargar el sistema operativo



que se inicie la máquina virtual, y empieze a cargar el sistema operativo

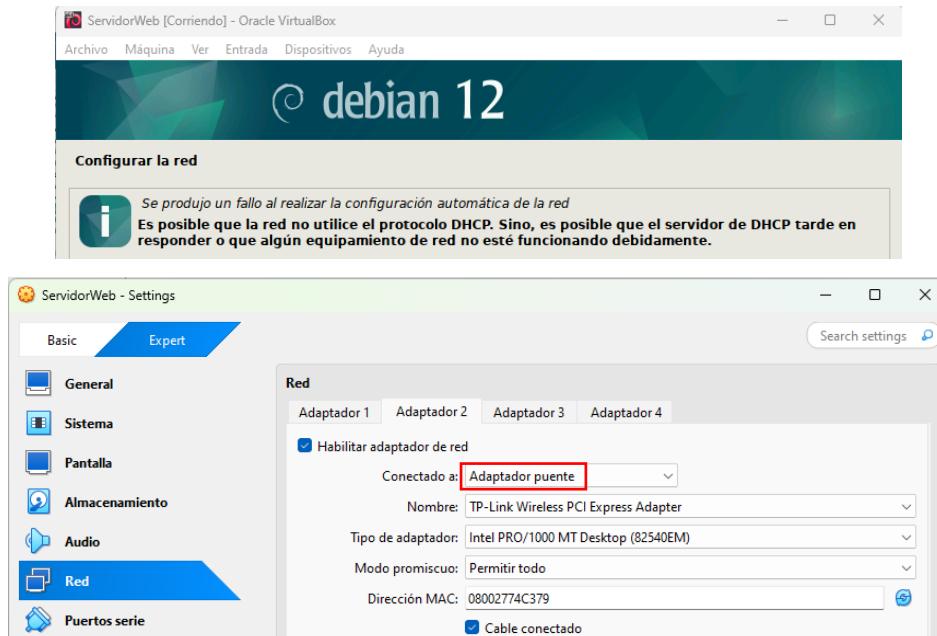


7. Elegimos el idioma del sistema operativo.



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

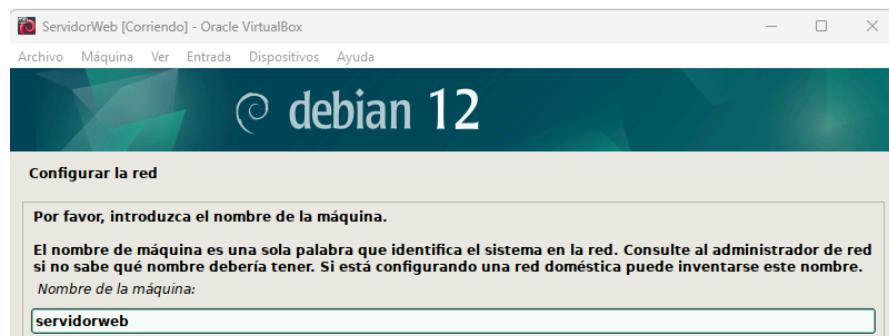
8. Nos avisa que no tenemos habilitado el DHCP, porque hemos seleccionado el adaptador de red interna “miredlan”, así que configuraremos un segundo “**Adaptador 2**” de red como “Adaptador puente” para que tengamos conexión a Internet y así, se actualicen los paquetes de Debian durante la instalación.



9. Seleccionamos el adaptador primario que nos va a dar acceso a Internet.

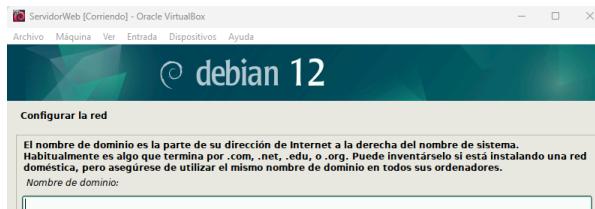


10. Damos un nombre a la máquina “servidorweb”.

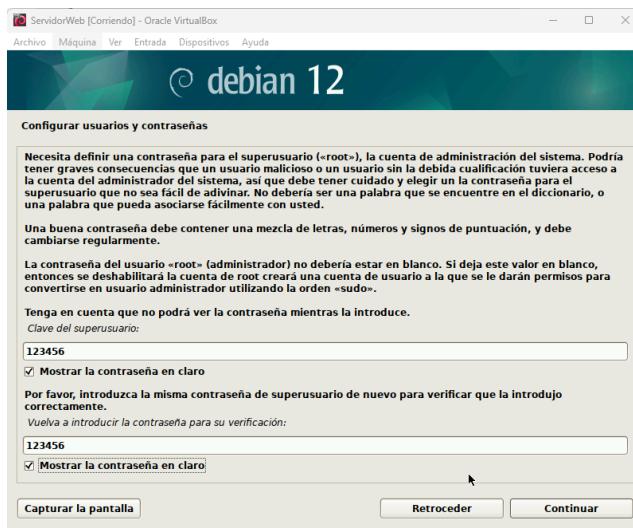


	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

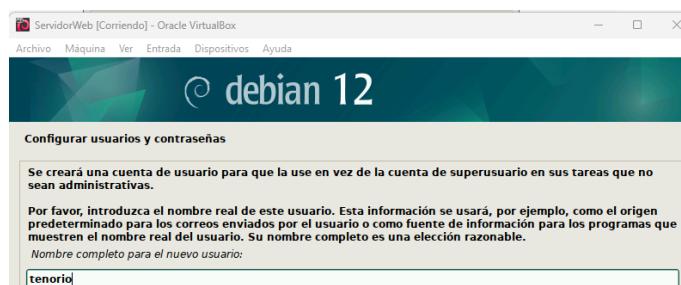
11. El nombre de dominio lo dejamos en blanco.



12. Configuramos una contraseña para el superusuario **root** (administrador del sistema).



13. Creamos la cuenta de usuario con el nombre “tenorio” para tareas comunes.

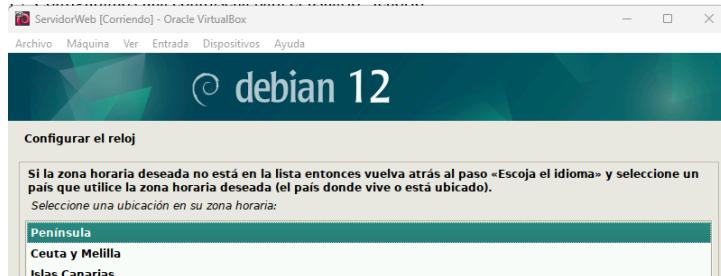


14. Configuramos una contraseña para el usuario “tenorio”, siempre teniendo en cuenta que estamos en un entorno de laboratorio, fuera de este, habría que poner una contraseña robusta.

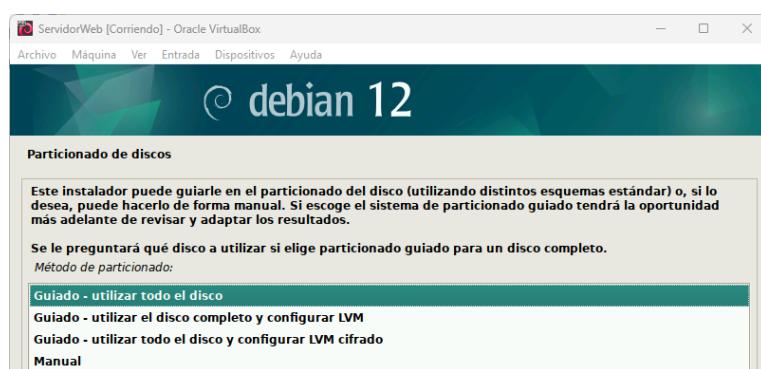


	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

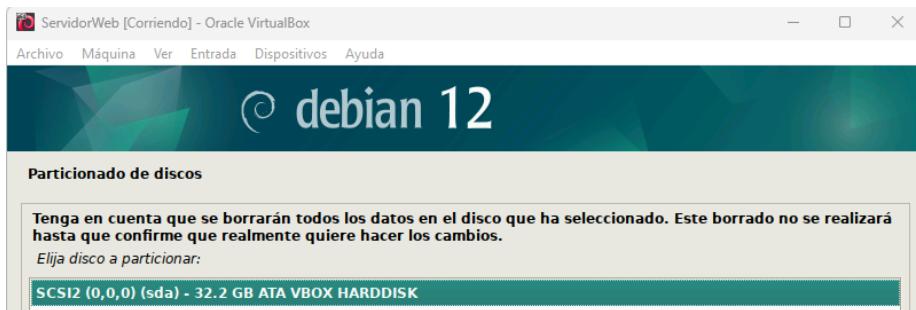
15. Configuramos el reloj con la zona horaria.



16. Dejamos por defecto la configuración del particionado del disco.



17. Elegimos el disco (sda) por defecto.

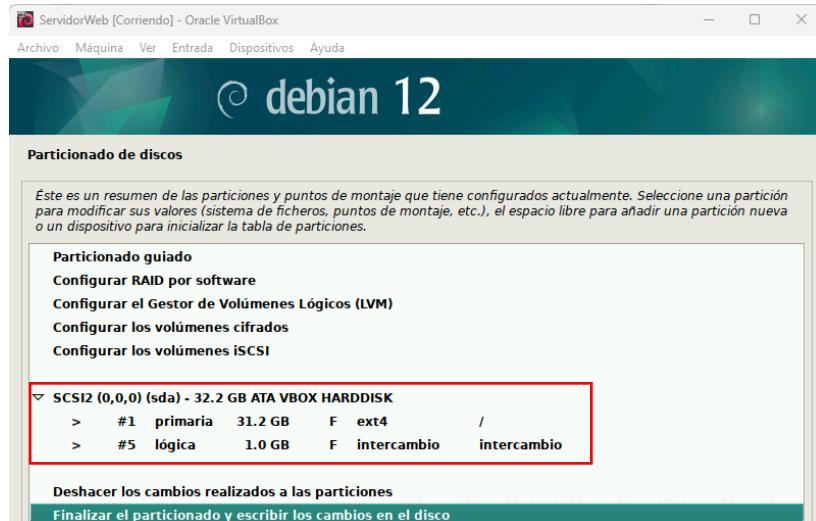


18. Dejamos por defecto todos los ficheros en una partición.

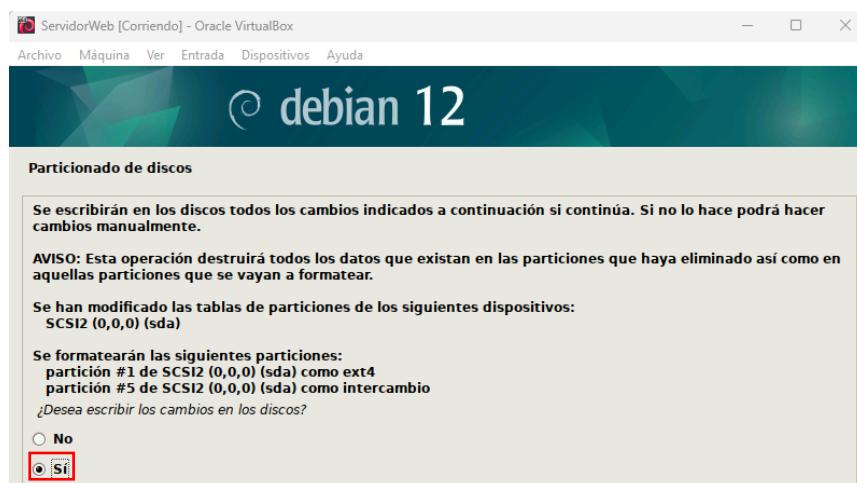


	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

19. Resumen del particionado que va a hacer el propio sistema por defecto.



20. Decimos que **SI**, que queremos que se guarden los cambios en el disco.

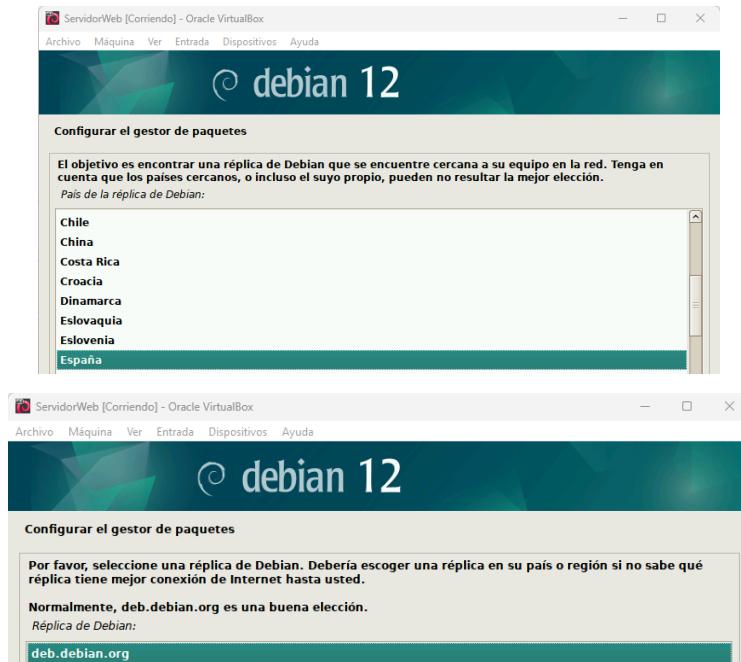


21. Decimos que **NO** queremos analizar medios de instalación adicionales.

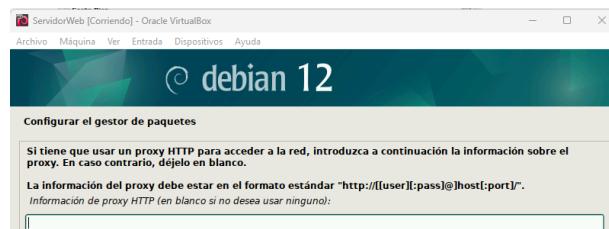


	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

22. Configuramos el gestor de paquetes que buscará una réplica de Debian en España.



23. Dejamos la configuración del proxy HTTP por defecto en blanco.

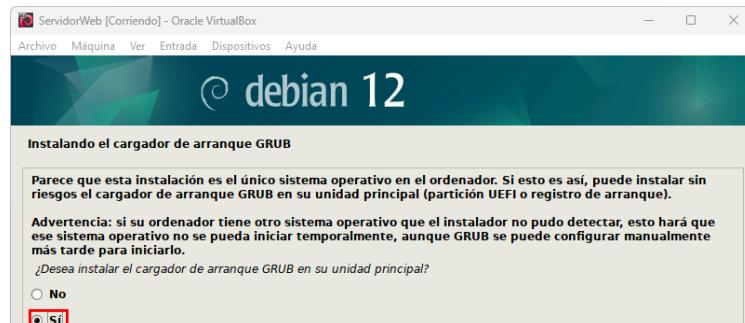


24. Dejamos por defecto la propuesta de instalación de programas de entorno de escritorio que nos aconseja el sistema.

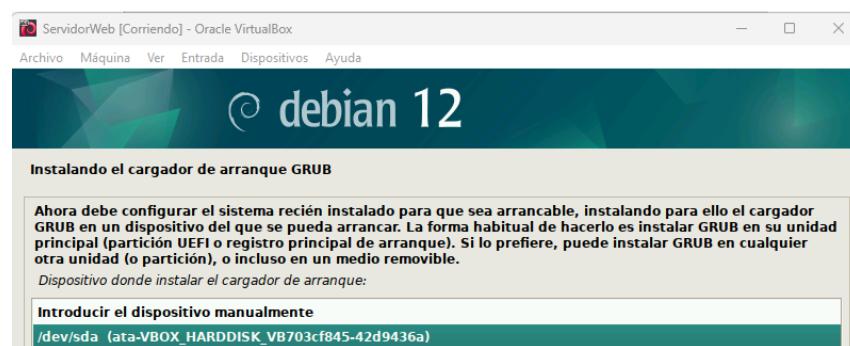


	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

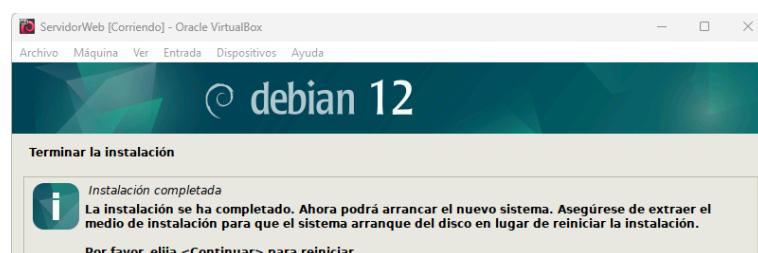
25. Decimos que **SI** a la instalación del cargador de arranque GRUB.



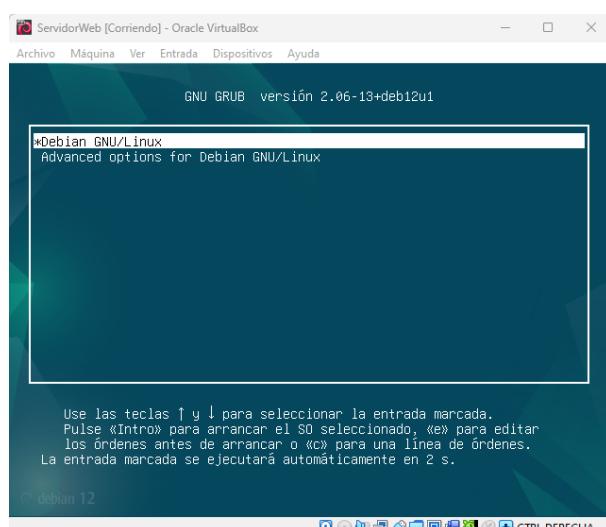
26. Configuramos el sistema para que sea arrancable.



27. Finalizamos la instalación.

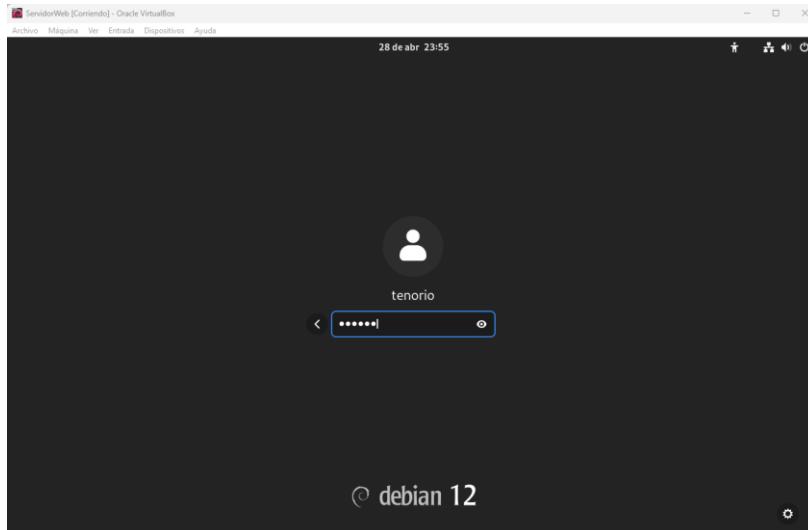


28. Comienza el inicio del sistema, cargando el gestor de arranque **GRUB**.



	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

29. Iniciamos sesión correctamente con el usuario **tenorio**.



4.4 Instalación y configuración Apache2 (Servidor Web).

1. Arrancamos la VM “ServidorWeb” y accedemos al S.O. con el usuario “tenorio”.

Antes de comenzar con la instalación de Apache2, accedemos a la terminal como superusuario “root”, y configuramos el archivo “sudoers” e incluimos al usuario “tenorio” para que tenga privilegios de “sudo”, con el comando.

- visudo

```
30 de abr 23:23
tenorio@servidorweb: ~
GNU nano 7.2          /etc/sudoers.tmp *

# Ditto for GPG agent
Defaults: %sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
tenorio ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

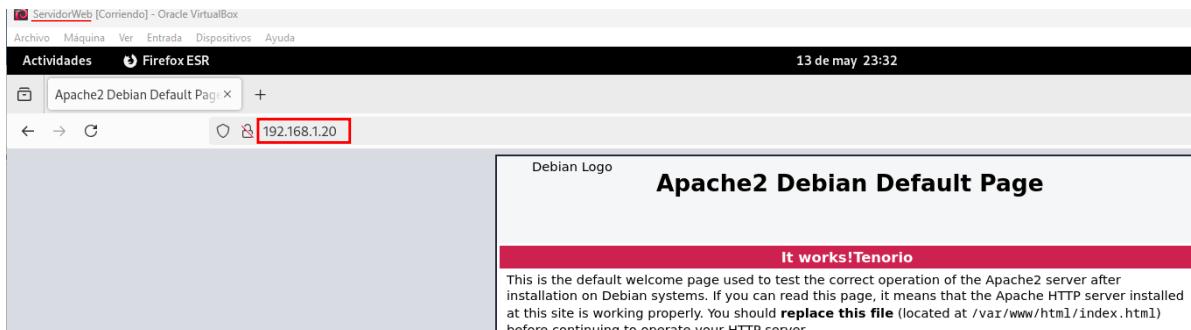
# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d

Nombre del fichero a escribir: /etc/sudoers.tmp
^G Ayuda      M-D Formato DOS  M-A Añadir      M-B Respaldar fichero
^C Cancelar   M-W Formato Mac  M-P Anteponer  ^T Navegar
```

2. Abrimos la terminal y con los siguientes comandos, actualizamos la lista de paquetes disponibles.
 - sudo apt update
 - sudo apt upgrade -y
3. El paquete del servidor web Apache2 está incluido por defecto en el repositorio de Debian, y será el encargado de gestionar las peticiones web, lo instalamos con el comando.
 - sudo apt install apache2 -y

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

4. Una vez instalado, comprobamos que está funcionando correctamente escribiendo en el navegador “Firefox” la dirección IP del servidor 192.168.1.20 apareciendo la página de bienvenida de Apache.



5. Configuramos Apache2 para que se inicie automáticamente al arrancar el sistema y verificamos el servicio con los comandos.

- sudo systemctl enable apache2
- sudo systemctl status apache2

6. Para configurar Nginx como proxy inverso para Apache2 en Debian 12, es necesario cambiar el puerto por defecto de Apache2 del 80 al 8080, ya que Nginx utilizará el puerto 80 por defecto. Esto se hace editando el archivo de configuración de puertos con el comando.

- sudo nano /etc/apache2/ports.conf

Buscamos donde pone “Listen 80” y lo sustituimos por “Listen 127.0.0.1:8080”.

```

1 de may 00:13
tenorio@servidorweb:~          1 de may 00:13
GNU nano 7.2          /etc/apache2/ports.conf *
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

#Listen 80
Listen 127.0.0.1:8080

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

Comentamos la línea
y creamos debajo
una nueva

Ctrl+O (para guardar los cambios)
Ctrl+X (para salir)

Nombre del fichero a escribir: /etc/apache2/ports.conf
^G Ayuda      M-D Formato DOS   M-A Añadir   M-B Respaldar fichero
^C Cancelar   M-M Formato Mac   M-P Anteponer ^T Navegar

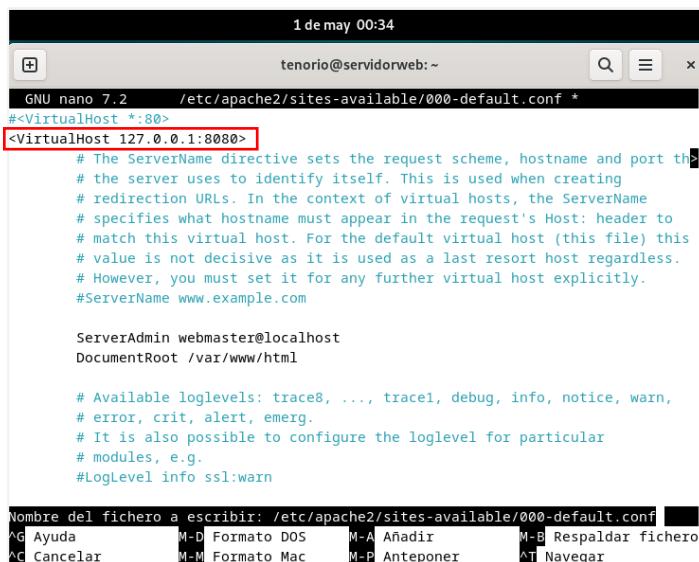
```

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

7. A continuación, editamos el archivo de configuración del host virtual por defecto de Apache2 y cambiamos el puerto por defecto.

- sudo nano /etc/apache2/sites-available/000-default.conf
- sudo nano /etc/apache2/sites-enabled/000-default.conf

Buscamos la siguiente línea <VirtualHost *:80> y la sustituimos por <VirtualHost 127.0.0.1:8080>.



```

1 de may 00:34
tenorio@servidorweb:~ 
GNU nano 7.2      /etc/apache2/sites-available/000-default.conf *
#<VirtualHost *:80>
<VirtualHost 127.0.0.1:8080>
# The ServerName directive sets the request scheme, hostname and port th>
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

Nombre del fichero a escribir: /etc/apache2/sites-available/000-default.conf
^G Ayuda      M-D Formato DOS   M-A Añadir      M-B Respalidar fichero
^C Cancelar   M-M Formato Mac   M-P Anteponer   ^T Navegar

```

8. Reiniciamos el servicio Apache2 para aplicar los cambios con el comando.

- sudo systemctl restart apache2

9. Apache2 está iniciado y escuchando en el puerto 8080, podemos comprobarlo ejecutando el comando.

- sudo ss -antpl | grep apache2



```

1 de may 00:49
tenorio@servidorweb:~$ sudo ss -antpl | grep apache2
LISTEN 0      511      127.0.0.1:8080      0.0.0.0:*      users:(("apache2",pid=4585,fd=3),("apache2",pid=4584,fd=3),("apache2",pid=4583,fd=3))
tenorio@servidorweb:~$ 

```

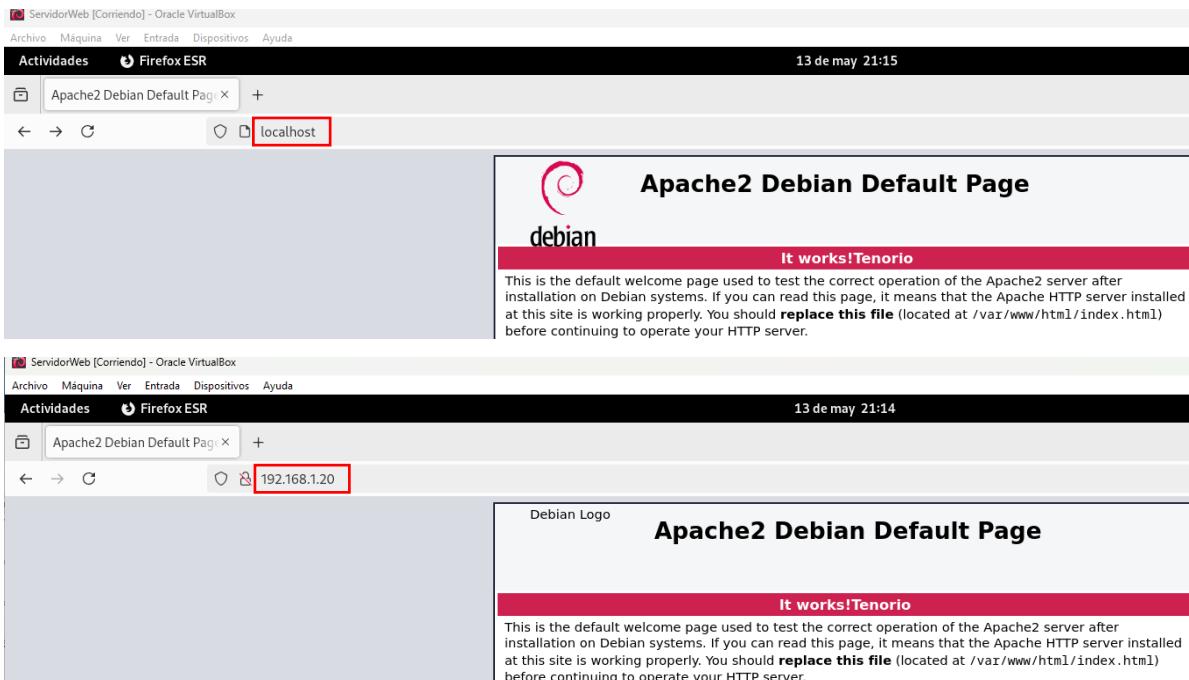
4.5 Crear un sitio web en Apache.

1. Editamos el archivo HTML que tiene por defecto Apache2, ejecutando el comando.

- sudo nano /var/www/html/index.html

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

2. Realizada las configuraciones anteriores en el servidor web Apache2, toca probarlo utilizando la URL <http://localhost> o <http://192.168.1.20>, si todo va bien, obtendremos la página de prueba de Apache2, servida a través del puerto 8080.



4.6 Instalación y configuración del Nginx (Servidor Web).

- Instalamos el paquete Nginx que actuará como servidor frontal (proxy inverso), recibiendo las peticiones y pasándoselas a Apache2 ejecutando el comando.
 - `sudo apt install nginx -y`
- Iniciamos el servicio Nginx y lo habilitamos para que se inicie al reiniciar el sistema ejecutando el comando.
 - `sudo systemctl start nginx`
 - `sudo systemctl enable nginx`

```
5 de may 20:11
tenorio@servidorweb:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-05-05 20:02:38 CEST; 7min ago
```

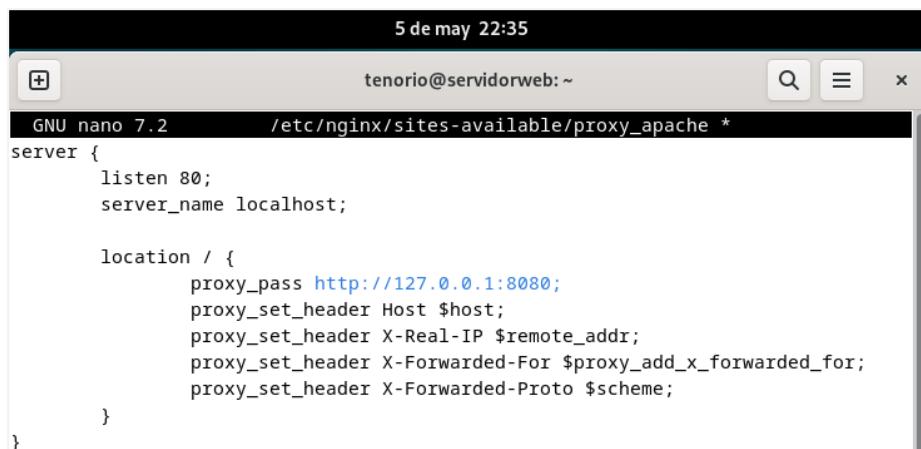
- Configuramos Nginx como proxy inverso para reenviar todas las peticiones que lleguen por el puerto **80** al puerto **8080** del servidor web Apache2, y creamos un nuevo archivo de configuración en el directorio “sites-available” de host virtual Nginx.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- sudo nano /etc/nginx/sites-available/proxy_apache
4. Añadimos las siguientes líneas de configuración necesaria para que Nginx actúe como proxy inverso para Apache2.

```
server {
    listen 80;
    server_name localhost;

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host; Establece el encabezado X-Real-IP con la dirección IP del cliente que se conecta directamente a Nginx.
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
} Agrega la dirección IP del cliente original al encabezado X-Forwarded-For.
Establece el encabezado X-Forwarded-Proto con el protocolo original (http o https) utilizado en la solicitud del cliente.
```



```
5 de may 22:35
tenorio@servidorweb:~$ nano /etc/nginx/sites-available/proxy_apache
GNU nano 7.2          /etc/nginx/sites-available/proxy_apache *
server {
    listen 80;
    server_name localhost;

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

5. Comprobamos si Nginx tiene algún error de sintaxis ejecutando el comando.

- nginx -t

```
tenorio@servidorweb:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

6. Habilitamos el host virtual creando un enlace simbólico en el directorio “sites-enabled” que apunte al archivo de configuración en “sites-available”, ejecutando el comando.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

- sudo ln -s /etc/nginx/sites-available/proxy_apache /etc/nginx/sites-enabled/
7. Podemos eliminar el archivo por defecto (opcional), nosotros no lo haremos.
- sudo rm /etc/nginx/sites-enabled/default
8. Reiniciamos el servicio Nginx para aplicar los cambios, ejecutando el comando.
- sudo systemctl restart nginx
9. Comprobamos el estado de Nginx ejecutando el comando.
- sudo systemctl status nginx

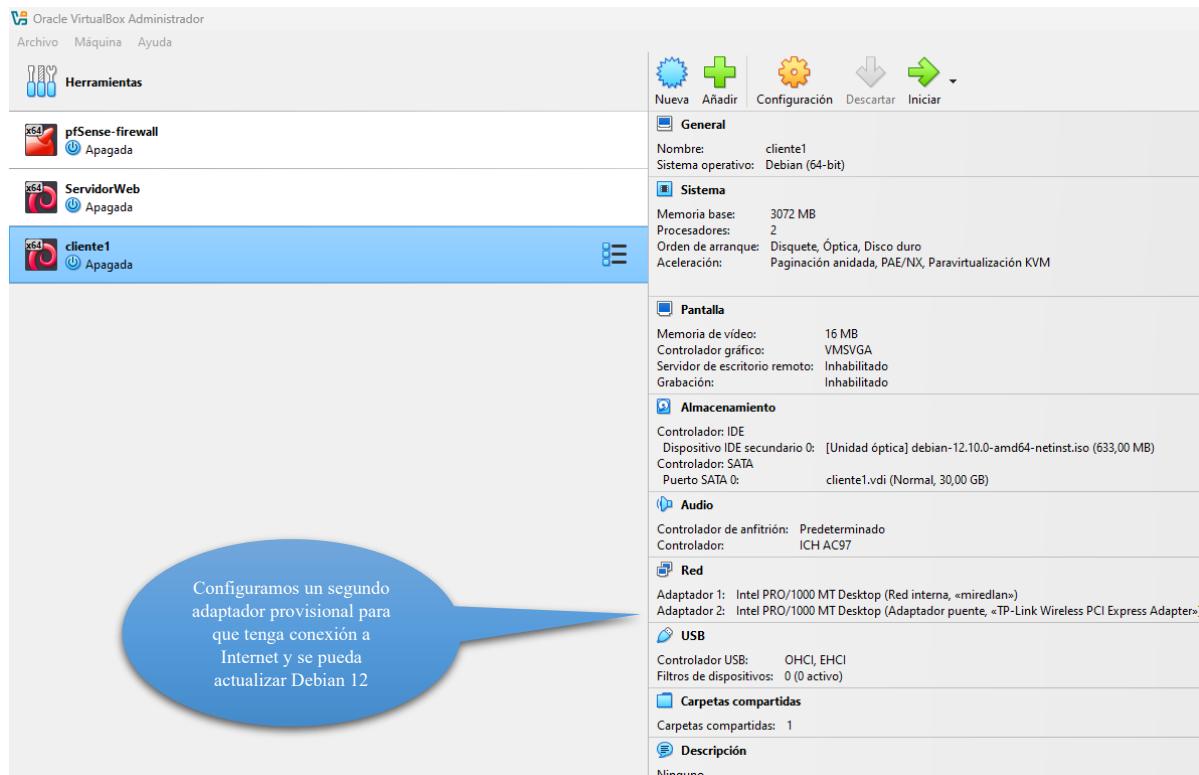
4.7 Instalación de VM Debian 12 (cliente1).

Por su estabilidad y seguridad, hemos utilizado el sistema operativo Debian/Linux, de descarga gratuita, está disponible en <https://www.debian.org/distrib/netinst.en.html> o <https://www.debian.org/download.es.html> seleccionando la versión estable AMD64 (64 bits).

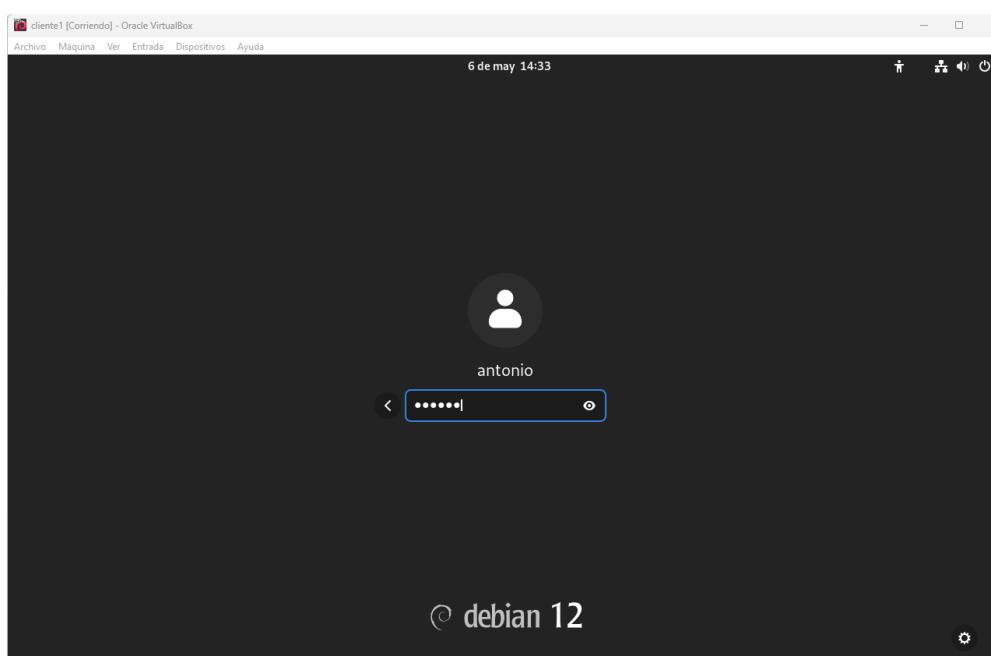


1. Creamos la máquina virtual haciendo clic en el menú del lado derecho llamado “caja de herramientas” - “Nueva”.
- 
- Nombre: **cliente1**.
 - Imagen ISO: **debian-12.10.0-amd64-netinst.iso**
 - Tipo: **Linux**.
 - Versión: **Debian (64-bit)**.
 - RAM: **3072 MB** o más.
 - Procesadores: **2 CPU**.
 - Disco duro: **30 GB** (tipo VDI, reservado dinámicamente).
 - Añadir un adaptador de red:
 - Adaptador 1 (LAN): modo **Red interna** “miredlan”.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



2. Siguiendo los pasos realizados en la configuración anterior del “servidor web”, damos al menú “Mostrar-Iniciar”  para que se inicie la máquina virtual, y empiece a cargar el sistema operativo Debian 12.
3. Finalizada la instalación, iniciamos sesión correctamente con el usuario **antonio**.



 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

4.8 Configuración de servicios principales.

Realizaremos la instalación y configuración básica de los servicios SSH, SFTP y DNS, tanto en el **cliente1** como en el **servidor web**, dentro de la red interna (LAN). Estos servicios, nos permitirán la administración remota, la transferencia de archivos y la resolución de nombres, respectivamente. Además, instalamos en pfSense el servicio DHCP Server para que realice la asignación automática de IPs en los clientes.

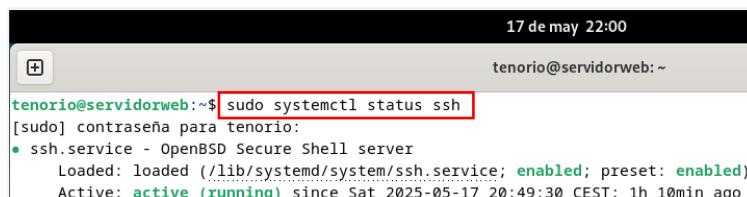
4.8.1 Servicio SSH (Secure Shell).

El objetivo de SSH es permitir el acceso remoto seguro al servidor web desde el cliente1 y permitirnos como administrador gestionar el servidor y otros dispositivos desde lejos encriptando las conexiones.

1. Comenzamos realizando la instalación en el servidor web, para ello abrimos la terminal, actualizamos el S.O. Debian 12 e instalamos **SSH** con los comandos.
 - sudo apt update
 - sudo apt install openssh-server

Una vez instalado verificamos el estado del servicio con el comando.

- sudo systemctl status ssh (Nos pedirá la contraseña del usuario/a)



```
17 de may 22:00
tenorio@servidorweb:~$ sudo systemctl status ssh
[sudo] contraseña para tenorio:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-05-17 20:49:30 CEST; 1h 10min ago
    Docs: man:sshd(8)
```

2. Vamos a permitir conexiones SSH solo desde la red LAN editando el archivo de configuración ejecutando el comando.

- sudo nano /etc/ssh/sshd_config

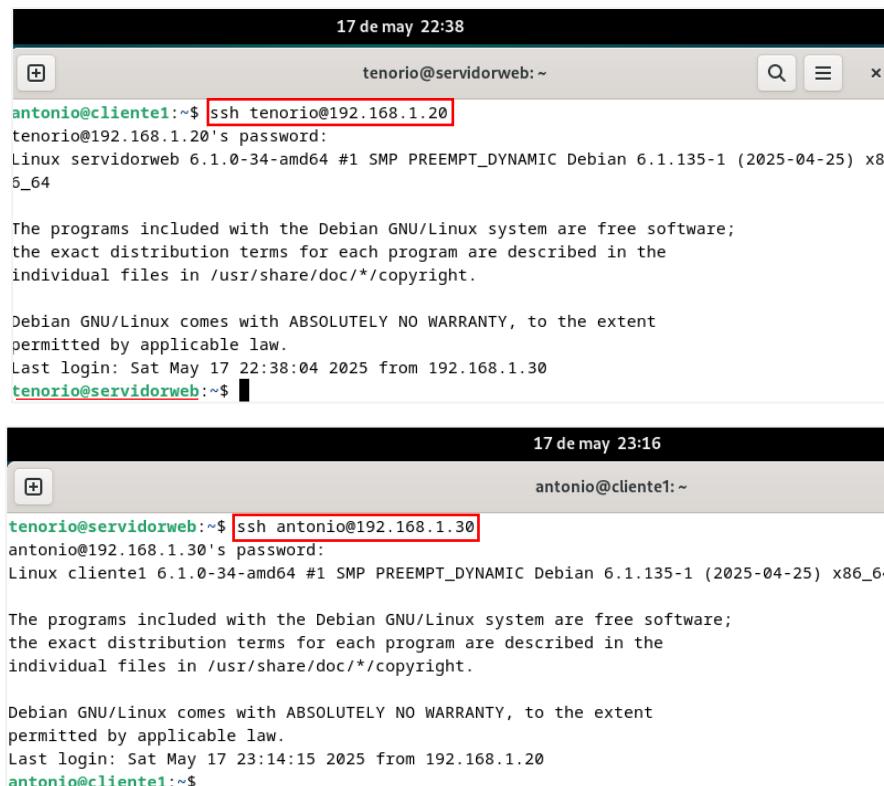


```
2 de jun 01:39
tenorio@servidorweb:~$ nano /etc/ssh/sshd_config
GNU nano 7.2
Include /etc/ssh/sshd_config.d/*.conf
Port 22
#AddressFamily any
ListenAddress 0.0.0.0
#ListenAddress 192.168.1.20
ListenAddress ::

2 de jun 01:41
tenorio@servidorweb:~$ cat /etc/ssh/sshd_config
#Port 22
#AddressFamily any
#ListenAddress 192.168.1.20
ListenAddress ::
```

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

3. Reiniciamos el servicio con el comando.
 - sudo systemctl restart ssh
4. Realizamos la instalación en el cliente1 ejecutando el comando.
 - sudo apt install openssh-client
5. Comprobamos que accedemos correctamente desde el cliente1 al servidor y viceversa.



The image shows two terminal windows side-by-side. Both are running on a Debian 6.1.135-1 system (x86_64). The top window (client1) has a title bar '17 de may 22:38' and shows the command: `antonio@cliente1:~$ ssh tenorio@192.168.1.20`. It asks for the password and displays the server's information: 'Linux servidorweb 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64'. It also shows the standard Debian GNU/Linux copyright notice and the last login information. The bottom window (servidorweb) has a title bar '17 de may 23:16' and shows the command: `tenorio@servidorweb:~$ ssh antonio@192.168.1.30`. It asks for the password and displays the client1's information: 'Linux cliente1 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64'. It also shows the standard Debian GNU/Linux copyright notice and the last login information.

4.8.2 Servicio SFTP (FTP Secure).

Para permitir la transferencia segura de archivos entre los equipos de la red interna, he optado por implementar FTPS (FTP Secure) en el servidor web en lugar del protocolo FTP tradicional, porque éste último transmite datos y credenciales en texto plano, mientras que FTPS añade una capa de seguridad mediante cifrado TLS/SSL, protegiendo así la confidencialidad e integridad de la información durante la transmisión.

1. Comenzamos la instalación ejecutando los comandos.
 - sudo apt update y sudo apt upgrade -y
 - sudo apt install vsftpd

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

2. Realizamos una copia de seguridad del fichero original, por si tenemos que restablecerlo, en caso de algún fallo, ejecutando el comando.
 - sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original
 3. Creamos un certificado autofirmado SSL/TLS para pruebas ejecutando el comando.
 - sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

Nos solicitará los datos del país (ES), provincia (Sevilla), localidad (Tomares), nombre de la empresa (Bios), unidad organizativa (Informática), nombre del servidor web (ServidorWeb), email (smr.gabino@gmail.com).

4. Editamos el archivo de configuración **vsftpd** para usar FTPS ejecutando el comando.

- sudo nano /etc/vsftpd.conf

Habilitar FTP y usuarios locales.

```
listen_ipv6=YES  
anonymous_enable=NO  
local_enable=YES  
write_enable=YES
```

```
18 de may 15:45
tenorio@servidorweb:~  
+  
GNU nano 7.2  
# addresses) then you must run two copies of vsftpd with two configuration  
# files.  
listen_ipv6=YES  
#  
# Allow anonymous FTP? (Disabled by default).  
anonymous_enable=NO  
#  
# Uncomment this to allow local users to log in.  
local_enable=YES  
#  
# Uncomment this to enable any form of FTP write command.  
write_enable=YES
```

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Seguridad básica.

chroot_local_user=YES

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd.chroot_list

Activar SSL/TLS.

ssl_enable=YES

allow_anon_ssl=NO

force_local_data_ssl=YES

force_local_logins_ssl=YES

ssl_tlsv1=YES

ssl_tlsv2=NO

ssl_tlsv3=NO

require_ssl_reuse=NO

ssl_ciphers=HIGH

rsa_cert_file=/etc/ssl/private/vsftpd.pem

rsa_private_key_file=/etc/ssl/private/vsftpd.pem

```
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
```

```
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
```

Opcional: restringir el acceso pasivo (configura según tu firewall).

pasv_enable=YES

pasv_min_port=40000

pasv_max_port=50000

Comentario técnico.¹

¹ **Nota técnica:** Aunque en el entorno actual cliente y servidor están ubicados en la misma red LAN, y por tanto el tráfico FTPS no atraviesa el cortafuego pfSense, se ha establecido un rango fijo de puertos pasivos (40000:50000) como medida preventiva. Esta configuración permitirá, en futuras fases del proyecto, trasladar el servidor a una zona DMZ controlada por pfSense sin necesidad de modificar la configuración del servicio FTPS. En ese contexto, bastaría con abrir dicho rango y el puerto 21 en el cortafuegos para habilitar conexiones seguras desde el exterior, mejorando la seguridad y escalabilidad de la infraestructura.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

```
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#ssl_enable=NO
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
# Opcional: restringir el acceso pasivo (configuramos según nuestro firewall, en un futuro nos permitirá conexiones FTPS de forma segura)
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000
```

5. Reiniciamos el servicio y comprobamos el estado ejecutando los comandos.

- sudo service vsftpd restart
- sudo service vsftpd status

6. Creamos un usuario de prueba

Daniel ejecutando el comando.

```
tenorio@servidorweb:~$ sudo adduser ftpsdaniel
Añadiendo el usuario `ftpsdaniel' ...
Añadiendo el nuevo grupo `ftpsdaniel' (1001) ...
```

- sudo adduser ftpsdaniel

7. Comprobamos que el cortafuego esté activo en el servidor web y en el cliente1, además que tenga los puertos activados o abiertos, ejecutando los comandos.

- sudo ufw enable
- sudo ufw status

```
antonio@cliente1:~$ sudo ufw status
Status: inactive
antonio@cliente1:~$ sudo ufw enable
Firewall is active and enabled on system startup
antonio@cliente1:~$ sudo ufw status
Status: active
antonio@cliente1:~$
```

8. Abrimos los puertos necesarios y establecemos un rango fijo de puertos pasivos, ejecutando los comandos.

- sudo ufw allow 20/tcp
- sudo ufw allow 21/tcp
- sudo ufw allow 990/tcp
- sudo ufw allow 40000:50000/tcp

```
antonio@cliente1:~$ sudo ufw allow 20/tcp
Rule added
Rule added (v6)
antonio@cliente1:~$ sudo ufw allow 21/tcp
Rule added
Rule added (v6)
antonio@cliente1:~$ sudo ufw allow 990/tcp
Rule added
Rule added (v6)
antonio@cliente1:~$ sudo ufw allow 40000:50000/tcp
Rule added
Rule added (v6)
```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

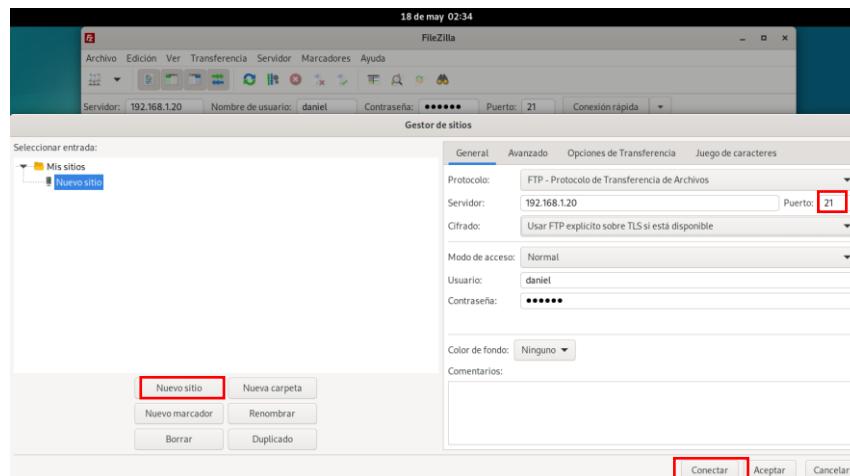
9. Como nuestra VM es un cliente Linux, instalamos “FileZilla 3.63.0” en el **cliente1** ejecutando el comando.

- `sudo apt install filezilla -y`

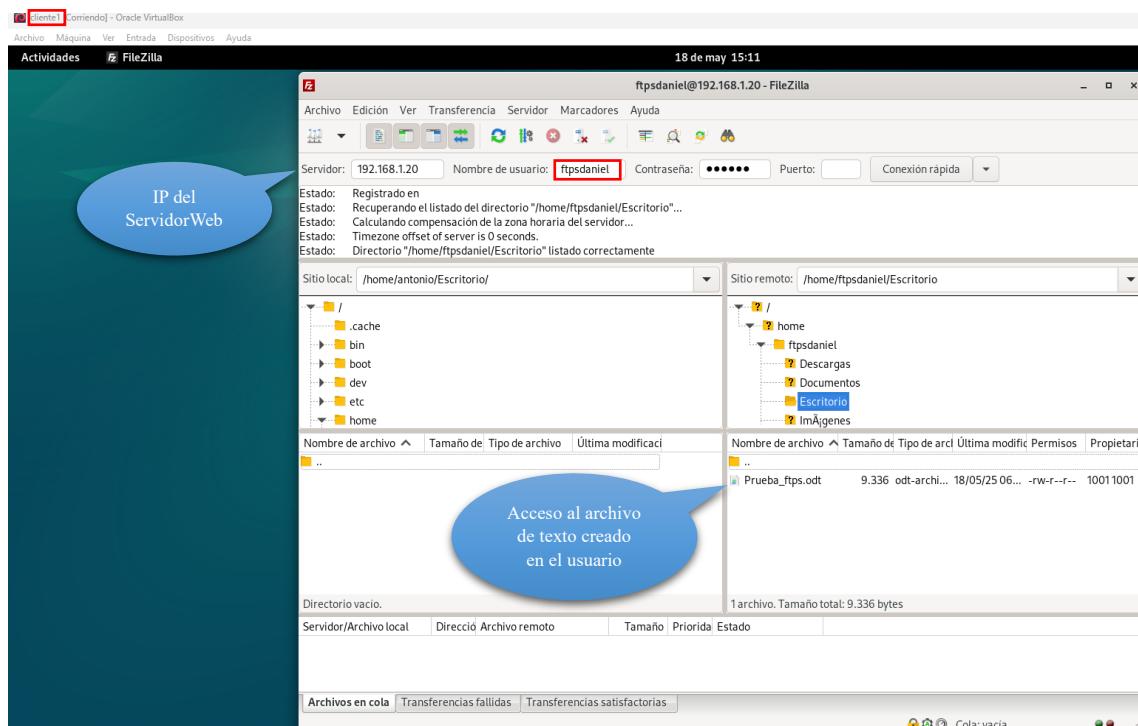


En Windows podríamos usar FileZilla o este otro cliente WinSCP.

10. Abrimos FileZilla, menú “Archivo”, “Gestor de sitios”, “Nuevo sitio”, cumplimentamos los datos y elegimos el protocolo adecuado (FTP sobre TLS explícito, o SFTP), puerto 21 ó 22.

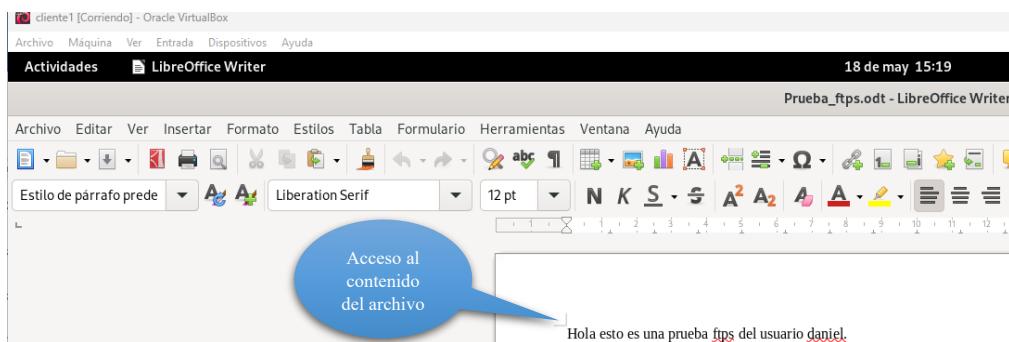


Comprobamos la conexión FTPS desde FileZilla con el usuario **ftpsdaniel** desde el cliente1.



The screenshot shows the Oracle VM VirtualBox interface with the 'cliente1' machine running. The IP address '192.168.1.20' is highlighted in a blue speech bubble. In the foreground, the FileZilla application window is open, showing a successful connection to the server. The local directory is set to '/home/antonio/Escritorio/' and the remote directory is set to '/home/ftpsdaniel/Escritorio'. A file named 'Prueba_ftps.odt' is listed in the remote directory. A blue speech bubble points to this file with the text 'Acceso al archivo de texto creado en el usuario'.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	



Comprobamos desde la terminal, que todo es correcto.

```
antonio@cliente1:~$ sftp ftpsdaniel@192.168.1.20
ftpsdaniel@192.168.1.20's password:
Connected to 192.168.1.20.
sftp> cd /home/ftpsdaniel/Escritorio/
sftp> ls
Prueba_ftps.odt
sftp>
```

Directorio usuario
ftpsdaniel, podemos
ver el fichero

4.8.3 DHCP Configuración automática de IPs en clientes.

La configuración del DHCP Server en pfSense (Firewall) que vamos a realizar, permitirá a los clientes obtener una dirección IP de manera automática de un pool de IPs establecido. El servidor recibe las peticiones de los clientes y este les asigna una dirección IP disponible.

Es importante tener en cuenta que para configurar el servidor DHCP en una interfaz, esta debe tener una dirección IP estática.

Esquema de cómo funciona un DHCP.



1. Configuramos en el equipo cliente Windows el servidor DHCP en nuestro firewall pfSense. Abrimos el panel de administración del cortafuego y comprobamos que nuestras interfaces LAN y DMZ sean estáticas.
2. Nos vamos al menú “Services”, “DHCP Server” y por defecto nos muestra las dos interfaces que pueden configurarse LAN y DMZ.

<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
---------------------------------	---

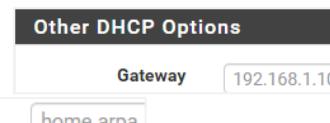
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

3. Comenzamos con la interfaz LAN, marcamos la opción “enable”, asignamos un rango desde la 100 a la 199.



4. Ponemos los Servidores DNS públicos de Cloudflare 1.0.0.1-1.1.1.1

5. Dejamos por defecto la puerta de enlace 192.168.1.10 para que los clientes puedan tener acceso a Internet.



6. Dejamos el nombre de dominio por defecto.

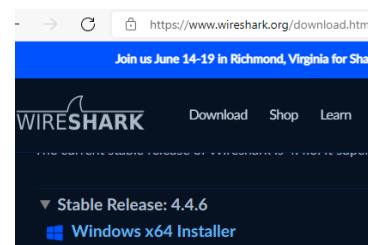


7. Hacemos lo mismo en la interfaz DMZ, marcamos la opción “enable”, y asignamos el mismo rango, los mismos DNS Servers.



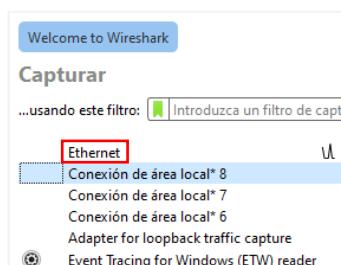
8. Dejamos por defecto la puerta de enlace 192.168.2.10

9. Descargamos la aplicación **Wireshark** que nos va a permitir capturar paquetes y analizar el contenido entre el cliente Windows y pfSense.



Es una herramienta que nos permite ir al nivel del paquete y poder ver cuál es el contenido en cada una de las capas del modelo OSI y de esa forma obtener información adicional para resolver problemas en nuestra red.

10. Abrimos la aplicación Wireshark y elegimos nuestra interfaz Ethernet.



LA PILA OSI



11. Realizamos un filtro por “dhcp” y vemos que ahora mismo no se están mandando mensajes por dhcp, para comprobarlo deshabilitamos la tarjeta de red que está en “estática” a que obtenga las IPs de forma dinámica a través del dhcp.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

Properties: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP: 192.168.1.40

Máscara de subred: 255.255.255.0

Puerta de enlace predeterminada: 192.168.1.10

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 8.8.8.8

Servidor DNS alternativo: 8.8.4.4

Capturing from Ethernet

File Edit View Capture Analyze Statistics Telephone Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
334	36.180852	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction
347	37.216107	192.168.1.10	192.168.1.100	DHCP	342	DHCP Offer - Transaction
348	37.217972	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction
349	37.228517	192.168.1.10	192.168.1.100	DHCP	342	DHCP ACK - Transaction

1. Mensaje **Discover** va IP 0.0.0.0 a 255.255.255.255 broadcast nivel capa 2 buscando el servidor pfSense.

2. pfSense **Offer** con la propuesta de la IP 192.168.1.100 por pfSense.

3. El cliente Windows manda mensaje **Request**

4. Finalmente, el servidor pfSense manda el mensaje de **Ack** confirmando la dirección IP propuesta.

Frame 334: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{57...}

Ethernet II Src: PCSSystemtec_3b:33:31 (08:00:27:3b:33:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff) Dirección MAC destino

Source: PCSSystemtec_3b:33:31 (08:00:27:3b:33:31) Dirección MAC origen de nuestra interfaz red virtual cliente Windows.

Type: IPv4 (0x0800)

[Stream index: 2]

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67 Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión : home.arpa

Descripción : Intel(R) PRO/1000 MT Desktop Adapter

Dirección física : 08-00-27-3B-33-31

Capturing from Ethernet

File Edit View Capture Analyze Statistics Telephone Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
334	36.180852	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction
347	37.216107	192.168.1.10	192.168.1.100	DHCP	342	DHCP Offer - Transaction
348	37.217972	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction
349	37.228517	192.168.1.10	192.168.1.100	DHCP	342	DHCP ACK - Transaction

LAN Interface (lan, em1)

Status up ↑

MAC Address 08:00:27:36:73:a7

IPv4 Address 192.168.1.10

Frame 347: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{57...}

Ethernet II Src: PCSSystemtec_36:73:a7 (08:00:27:36:73:a7), Dst: PCSSystemtec_3b:33:31 (08:00:27:3b:33:31)

Destination PCSSystemtec_3b:33:31 (08:00:27:3b:33:31) Dirección MAC de nuestra interfaz red virtual es el destino.

Source: PCSSystemtec_36:73:a7 (08:00:27:36:73:a7) Dirección MAC origen de la interfaz pfSense.

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.100

User Datagram Protocol, Src Port: 67, Dst Port: 68

Dynamic Host Configuration Protocol (Offer)

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

Capturando desde Ethernet

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
334	36.180852	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction
347	37.216107	192.168.1.10	192.168.1.100	DHCP	342	DHCP Offer - Transaction
348	37.217972	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction
349	37.228517	192.168.1.10	192.168.1.100	DHCP	342	DHCP ACK - Transaction

Aquí la dirección origen sigue siendo MAC Windows, pero el destino sigue siendo broadcast.

> Frame 348: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{5...}
 > Ethernet II, Src: PCSSystemtec_3b:33:31 (08:00:27:3b:33:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 > Source: PCSSystemtec_3b:33:31 (08:00:27:3b:33:31)
 > Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
 > User Datagram Protocol, Src Port: 68, Dst Port: 67
 > Dynamic Host Configuration Protocol (Request)

Aquí todavía no se ha asignado la IP a la VM Windows porque necesita que el servidor pfSense mande el mensaje de ACK.

Capturando desde Ethernet

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
334	36.180852	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction
347	37.216107	192.168.1.10	192.168.1.100	DHCP	342	DHCP Offer - Transaction
348	37.217972	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction
349	37.228517	192.168.1.10	192.168.1.100	DHCP	342	DHCP ACK - Transaction
16559	3636.631666	192.168.1.100	192.168.1.100			Organizar Deshabilitar este
16560	3636.650239	192.168.1.10	192.168.1.100			Ethernet Red Intel(R) PRO/1000 MT

Estado de Ethernet

Detalles de la conexión de red

Detalles de la conexión de red:

Propiedad	Valor
Sufijo DNS específico p...	home.apa
Descripción	Intel(R) PRO/1000 MT Desktop Adap...
Dirección física	08-00-27-3b-33-31
Habilitado para DHCP	SI
Dirección IPv4	192.168.1.100
Máscara de subred IPv4	255.255.255.0
Concesión obtenida	viernes, 30 de mayo de 2025 15:05:00
La concesión expira	viernes, 30 de mayo de 2025 18:05:00
Puerta de enlace predet...	192.168.1.10
Servidor DHCP IPv4	192.168.1.10
Servidores DNS IPv4	1.0.0.1 1.1.1.1

Finalmente vemos que se ha asignado la IP a la VM Windows.

Finalmente vemos que se ha asignado la IP a la VM Windows.

12. Comprobamos que el servidor DHCP asigne bien a los clientes las IPs, abrimos el cliente Debian 12 que tiene la interfaz **enp0s3** en estática IP 192.168.1.30 y la cambiamos, comprobando que una vez actualizada la interfaz, que nos asigne bien la IP dentro del rango que configuramos de la 100 a la 199.

13. Para ver información de la puerta de enlace ejecutamos el comando.

- ip route

```
30 de may 16:44
antonio@cliente1: ~
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noq
t qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host noprefixroute
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu :
  link/ether 08:00:27:0f:ab:14 brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.101/24 brd 192.168.1.255 scope
    
```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

```

30 de may 16:50
antonio@cliente1:~$ ip route
default via 192.168.0.1 dev enp0s8 proto dhcp src 192.168.0.102 metric 101
default via 192.168.1.10 dev enp0s3 proto dhcp src 192.168.1.101 metric 102
192.168.0.0/24 dev enp0s8 proto kernel scope link src 192.168.0.102 metric 101
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.101 metric 102

30 de may 20:33
tenorio@servidorweb:~$ ip route
default via 192.168.2.10 dev enp0s3 proto dhcp src 192.168.2.100 metric 100
default via 192.168.0.1 dev enp0s8 proto dhcp src 192.168.0.101 metric 101
192.168.0.0/24 dev enp0s8 proto kernel scope link src 192.168.0.101 metric 101
192.168.2.0/24 dev enp0s3 proto kernel scope link src 192.168.2.100 metric 100

```

Vemos que nos muestra como puerta de enlace la IP de pfSense (Firewall).

14. Podemos ver información sobre las dos IP que pfSense nos ha asignado yéndonos al panel de administración “Status”, “DHCP Leases”. Vemos también las direcciones usadas de los “Pools” que hemos configurado.

Leases							
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
✓ ↑	192.168.1.100	08:00:27:3b:33:31	DESKTOP-R8BIO1B		2025/05/30 18:44:02	2025/05/30 20:44:02	 
✓ ↑	192.168.2.100	08:00:27:fb:24:29	servidorweb		2025/05/30 18:15:34	2025/05/30 20:15:34	 
Lease Utilization							
Interface	Pool Start	Pool End	Used	Capacity	Utilization		
LAN	192.168.1.100	192.168.1.199	1	100	1% of 100		
DMZ	192.168.2.100	192.168.2.199	1	100	1% of 100		

15. Ahora vamos a reservar una dirección IP para nuestro servidor web haciendo clic en la cruz azul “Add static mapping”, no debe estar en nuestro rango 192.168.2.100-192.168.2.199. Asignaremos la IP **192.168.2.20** y el DHCP la asignará teniendo en cuenta la dirección MAC, ya que no queremos que nuestro servidor web esté cambiando de dirección IP regularmente.

Static DHCP Mapping on DMZ															
DHCP Backend	ISC DHCP														
MAC Address	08:00:27:fb:24:29 MAC address of the client host														
Client Identifier	An optional identifier														
IP Address	192.168.2.20														
<table border="1"> <tr> <td>Hostname</td> <td>servidorweb Name of the client host</td> </tr> <tr> <td>Description</td> <td>Servidor Web en DMZ</td> </tr> <tr> <td colspan="2"> <table border="1"> <tr> <td>DNS Servers</td> <td>1.0.0.1 1.1.1.1</td> </tr> </table> </td> </tr> <tr> <td>Other DHCP Options</td> <td> <table border="1"> <tr> <td>Gateway</td> <td>192.168.2.10 The default is to use the correct gateway</td> </tr> <tr> <td>Domain Name</td> <td>home.arpa</td> </tr> </table> </td> </tr> </table>		Hostname	servidorweb Name of the client host	Description	Servidor Web en DMZ	<table border="1"> <tr> <td>DNS Servers</td> <td>1.0.0.1 1.1.1.1</td> </tr> </table>		DNS Servers	1.0.0.1 1.1.1.1	Other DHCP Options	<table border="1"> <tr> <td>Gateway</td> <td>192.168.2.10 The default is to use the correct gateway</td> </tr> <tr> <td>Domain Name</td> <td>home.arpa</td> </tr> </table>	Gateway	192.168.2.10 The default is to use the correct gateway	Domain Name	home.arpa
Hostname	servidorweb Name of the client host														
Description	Servidor Web en DMZ														
<table border="1"> <tr> <td>DNS Servers</td> <td>1.0.0.1 1.1.1.1</td> </tr> </table>		DNS Servers	1.0.0.1 1.1.1.1												
DNS Servers	1.0.0.1 1.1.1.1														
Other DHCP Options	<table border="1"> <tr> <td>Gateway</td> <td>192.168.2.10 The default is to use the correct gateway</td> </tr> <tr> <td>Domain Name</td> <td>home.arpa</td> </tr> </table>	Gateway	192.168.2.10 The default is to use the correct gateway	Domain Name	home.arpa										
Gateway	192.168.2.10 The default is to use the correct gateway														
Domain Name	home.arpa														

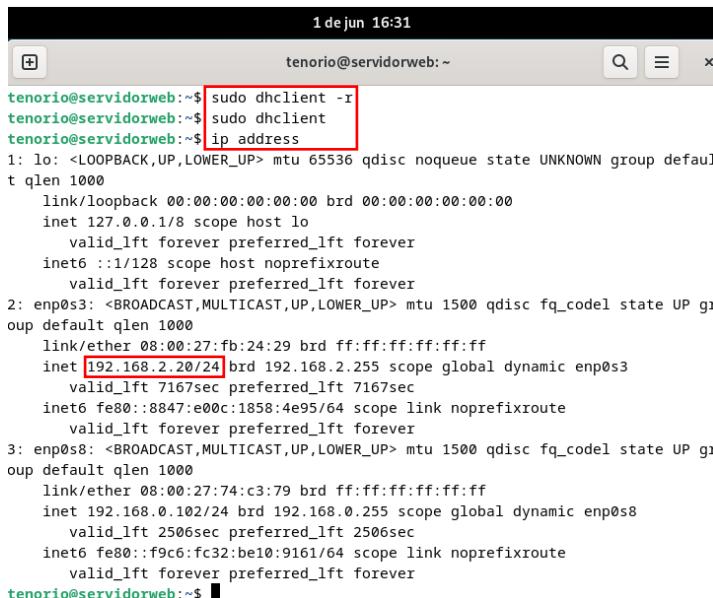
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

16. Podemos ver cómo se ha realizado la reserva correctamente.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:fb:24:29	192.168.2.20	servidorweb	Servidor Web en DMZ
+ Add Static Mapping				

17. Vamos a nuestro servidor web y actualizamos la dirección IP, para que se actualice a la nueva IP 192.168.2.20, ejecutamos los comandos.

- sudo dhclient -r (Le pedimos al cliente DHCP que libere (release) la dirección IP actual que ha sido asignada a la interfaz de red).
- sudo dhclient (Solicitamos una nueva dirección IP al servidor DHCP).
- ip address



```

1 de jun 16:31
tenorio@servidorweb:~$ sudo dhclient -r
tenorio@servidorweb:~$ sudo dhclient
tenorio@servidorweb:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fb:24:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.20/24 brd 192.168.2.255 scope global dynamic enp0s3
        valid_lft 7167sec preferred_lft 7167sec
        inet6 fe80::8847:e00c:1858:4e95/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:74:c3:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global dynamic enp0s8
        valid_lft 2506sec preferred_lft 2506sec
        inet6 fe80::f9c6:fc32:be10:9161/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
tenorio@servidorweb:~$ 

```

4.8.4 Instalar y configurar servidor DNS.

Tener un **servidor DNS interno** en el servidor web, nos va a permitir que se puedan resolver nombres de dominio personalizados (`www.atenoriopfsense.local`) dentro de nuestra red, para que los clientes no tengan que usar direcciones IP.

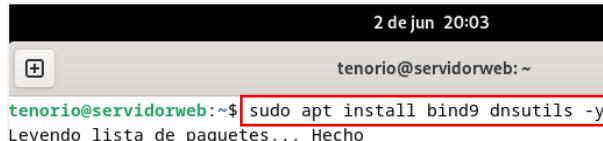
- ❖ **La zona de búsqueda directa** traduce nombres de dominio en direcciones IP.
- ❖ **La zona de búsqueda inversa** traduce direcciones IP en nombres de dominio.

1. Actualizamos los repositorios ejecutando los comandos.

- sudo apt update
- sudo apt upgrade -y

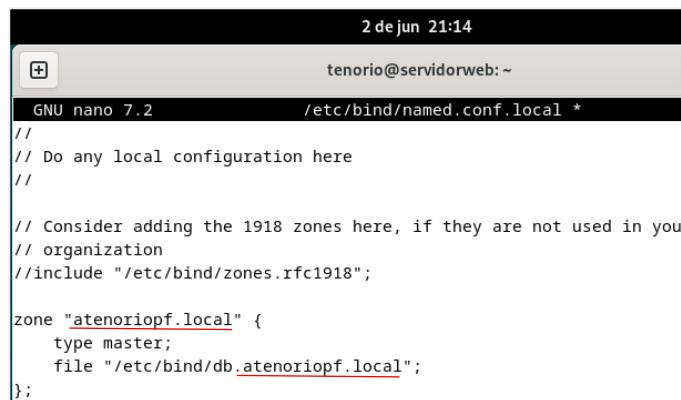
 Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	---------------------	---	-----------------------------------

2. Instalamos el paquete bind9 y herramientas para comprobarlo desde el terminal del servidor web ejecutando el comando.
- sudo apt install bind9 dnsutils -y



```
2 de jun 20:03
tenorio@servidorweb:~$ sudo apt install bind9 dnsutils -y
Leyendo lista de paquetes... Hecho
```

3. Configuramos la zona DNS editando el archivo de configuración principal **named.conf.local**, creando una nueva zona con nuestro dominio “**atenoriopf.local**”.



```
2 de jun 21:14
tenorio@servidorweb:~$ 
GNU nano 7.2          /etc/bind/named.conf.local *
// 
// Do any local configuration here
//

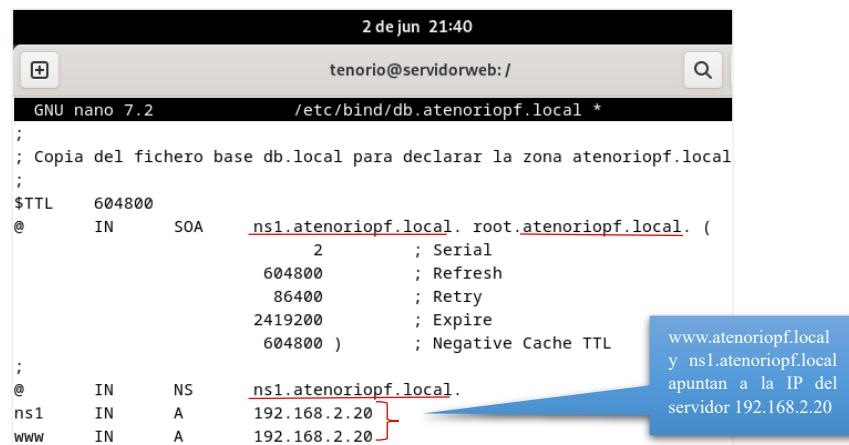
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "atenoriopf.local" {
    type master;
    file "/etc/bind/db.atenoriopf.local";
};
```

4. Creamos el archivo de zona copiando el archivo base **db.local**, ejecutando el comando.

- sudo cp /etc/bind/db.local /etc/bind/db.atenoriopf.local

5. Editamos el fichero **db.atenoriopf.local** modificando su contenido por nuestro dominio.



```
2 de jun 21:40
tenorio@servidorweb:/
GNU nano 7.2          /etc/bind/db.atenoriopf.local *
;
; Copia del fichero base db.local para declarar la zona atenoriopf.local
;
$TTL    604800
@      IN      SOA     ns1.atenoriopf.local. root.atenoriopf.local. (
                          2           ; Serial
                          604800      ; Refresh
                          86400       ; Retry
                          2419200     ; Expire
                          604800 )    ; Negative Cache TTL
;
@      IN      NS      ns1.atenoriopf.local.
ns1   IN      A       192.168.2.20
www  IN      A       192.168.2.20
```

www.atenoriopf.local
y ns1.atenoriopf.local
apuntan a la IP del
servidor 192.168.2.20

6. Verificamos que no tengamos errores en el fichero ejecutando el comando.

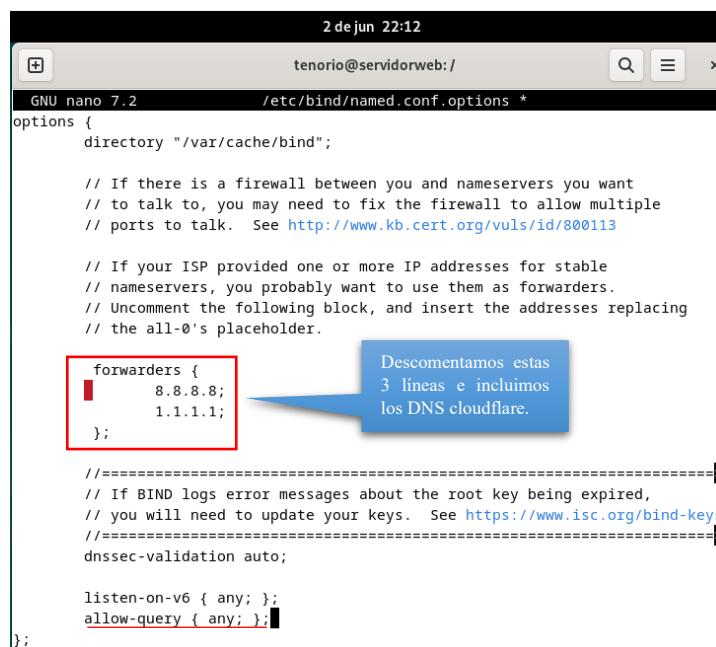
- sudo named-checkconf

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

7. Los siguiente sería configurar el fichero **named.conf.options** ejecutando el comando.

- sudo nano /etc/bind/named.conf.options

Tenemos que configurar este fichero porque el servidor DNS solo resuelve **nombres locales** (www.atenoriopf.local). Pero si un cliente quiere acceder a google.com, ese nombre debe ser **reenviado a un servidor externo**, (DNS de Google 8.8.8.8 y 1.1.1.1, de Cloudflare), como respaldo.



```
2 de jun 22:12
tenorio@servidorweb: /etc/bind/named.conf.options *
GNU nano 7.2
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

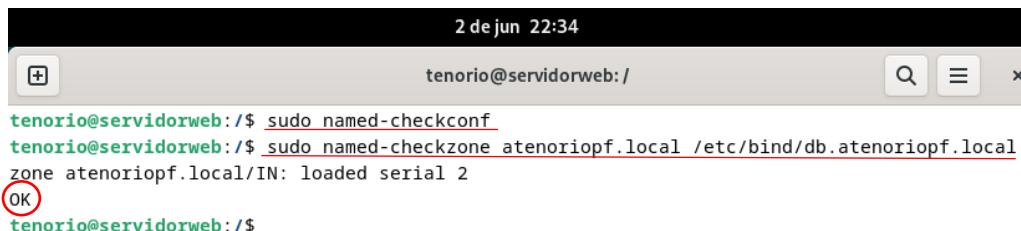
    forwarders {
        8.8.8.8;
        1.1.1.1;
    };
}

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

listen-on-v6 { any; };
allow-query { any; };
};
```

8. Verificamos que el fichero no tenga errores y que la zona esté OK ejecutando los comandos.

- sudo named-checkconf
- sudo named-checkzone atenoriopf.local /etc/bind/db.atenoriopf.local



```
2 de jun 22:34
tenorio@servidorweb:/$ sudo named-checkconf
tenorio@servidorweb:/$ sudo named-checkzone atenoriopf.local /etc/bind/db.atenoriopf.local
zone atenoriopf.local/IN: loaded serial 2
OK
tenorio@servidorweb:/$
```

9. Reiniciamos los servicios DNS ejecutando el comando.

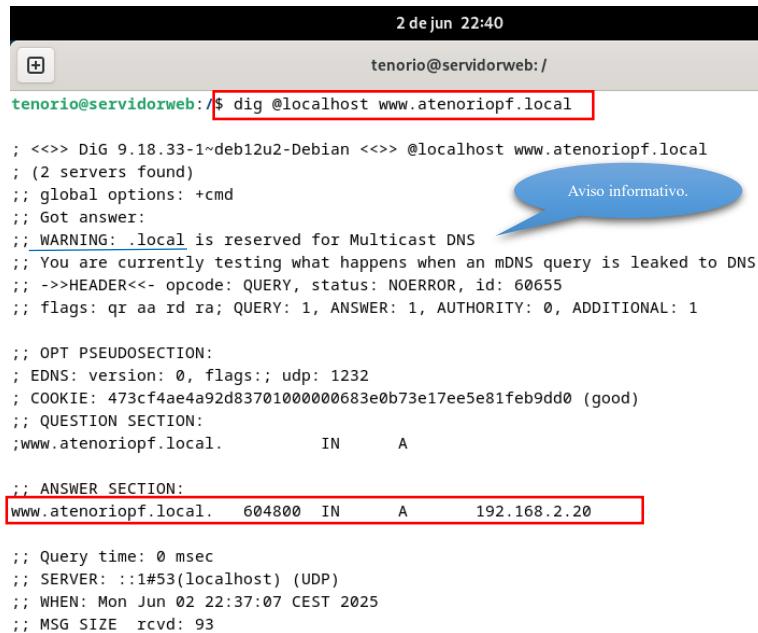
- sudo systemctl restart bind9

10. Comprobamos que funciona desde el mismo servidor ejecutando el comando.

- dig @localhost www.atenoriopf.local

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

Vemos que responde perfectamente y que se ha realizado la configuración correctamente.



```

2 de jun 22:40
tenorio@servidorweb:/
tenorio@servidorweb:~$ dig @localhost www.atenoriopf.local
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @localhost www.atenoriopf.local
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 60655
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 473cf4ae4a92d83701000000683e0b73e17ee5e81feb9dd0 (good)
;; QUESTION SECTION:
;www.atenoriopf.local.      IN      A

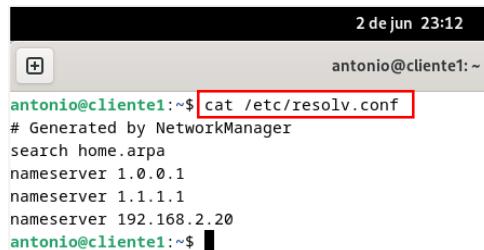
;; ANSWER SECTION:
www.atenoriopf.local.  604800  IN      A      192.168.2.20

;; Query time: 0 msec
;; SERVER: ::1#53(locahost) (UDP)
;; WHEN: Mon Jun 02 22:37:07 CEST 2025
;; MSG SIZE rcvd: 93

```

11. Comprobamos desde un equipo de la red cliente1 (LAN) poniendo como DNS el servidor donde tenemos BIND9.

Ahora sí, el cliente1 **está utilizando correctamente el servidor DNS local (192.168.2.20)** junto con los servidores de Cloudflare (1.0.0.1 y 1.1.1.1). Esto significa que **puede resolver tanto nombres locales como externos**.



```

2 de jun 23:12
antonio@cliente1:~
antonio@cliente1:~$ cat /etc/resolv.conf
# Generated by NetworkManager
search home.arpa
nameserver 1.0.0.1
nameserver 1.1.1.1
nameserver 192.168.2.20
antonio@cliente1:~$ 

```

12. Vamos a cambiar el dominio “home.arpa” y el nombre del servidor para que no nos muestre más la IP de la red externa 192.168.0.1 y sólo nos muestre la del servidor DNS 192.168.2.20, editando el fichero /etc/resolv.conf ejecutando el comando.

- sudo nano /etc/resolv.conf



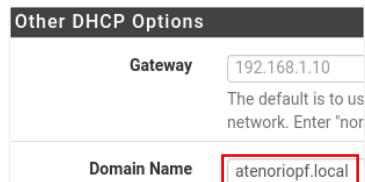
```

2 de jun 23:31
tenorio@servidorweb:/
GNU nano 7.2                               /etc/resolv.conf *
# Generated by NetworkManager
search atenoriopf.local
nameserver 1.0.0.1
nameserver 1.1.1.1
nameserver 192.168.2.20

```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

13. Realizamos el cambio también en pfSense, tanto en la interfaz LAN como en la DMZ. Abrimos el panel de administración menú “Services”, “DHCP Server”, casilla “Domain Name”.

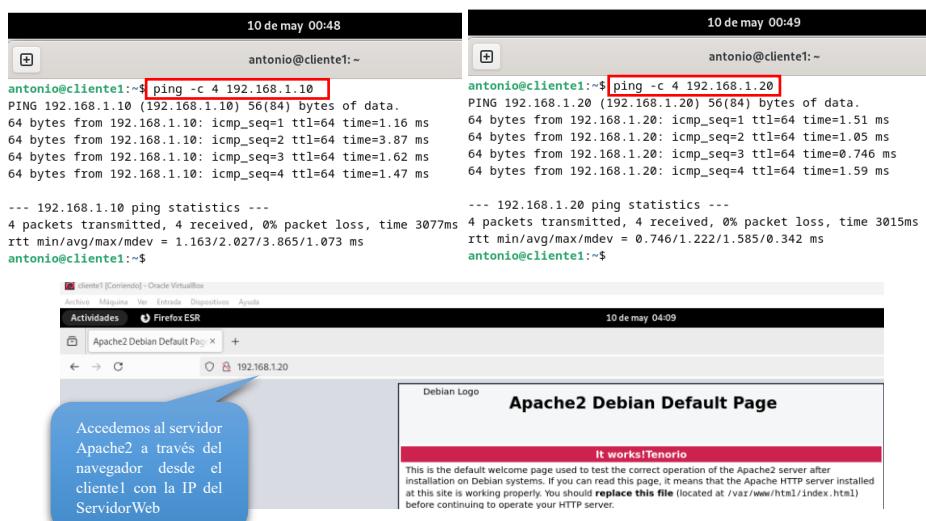


```
2 de jun 23:44
antonio@cliente1:~$ cat /etc/resolv.conf
# Generated by NetworkManager
search atenoriopf.local
nameserver 192.168.2.20
antonio@cliente1:~$
```

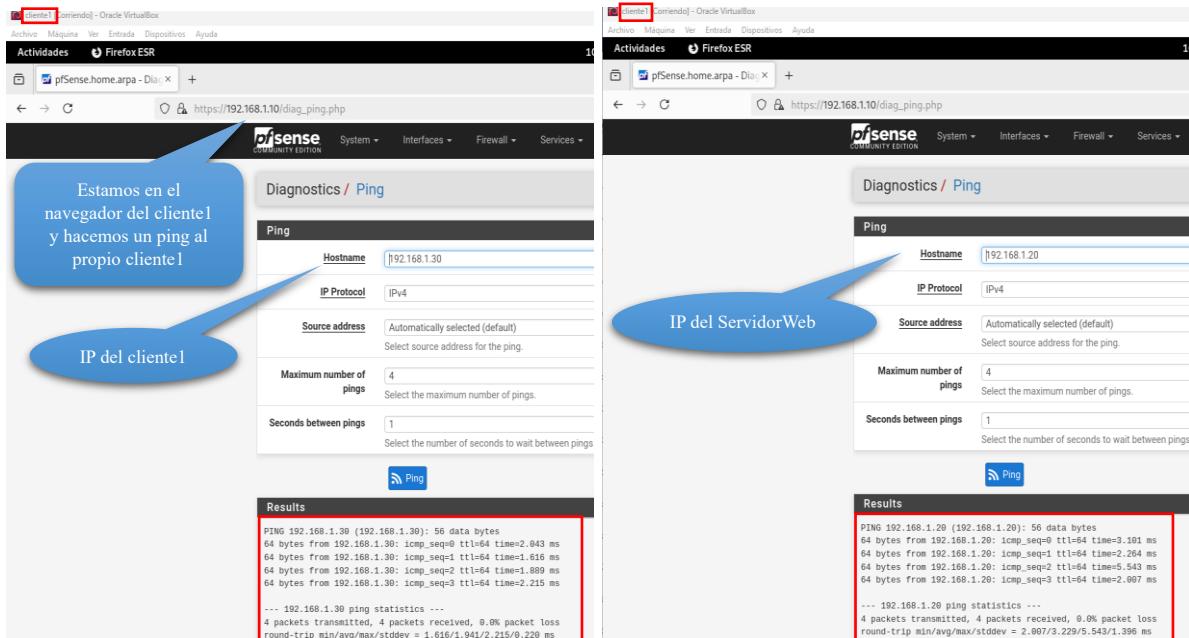
4.9 Integración de servicios y pruebas de funcionamiento.

4.9.1 Pruebas de conectividad básica.

- ✓ Verificamos que todas las máquinas se comunican entre sí, ejecutando el comando **ping** y a través de un **navegador web** (Firefox).
- Desde el cliente1. **192.168.1.30**
 - ping 192.168.1.10 (pfSense) y viceversa.
 - ping 192.168.1.20 (ServidorWeb) y desde (pfSense).



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



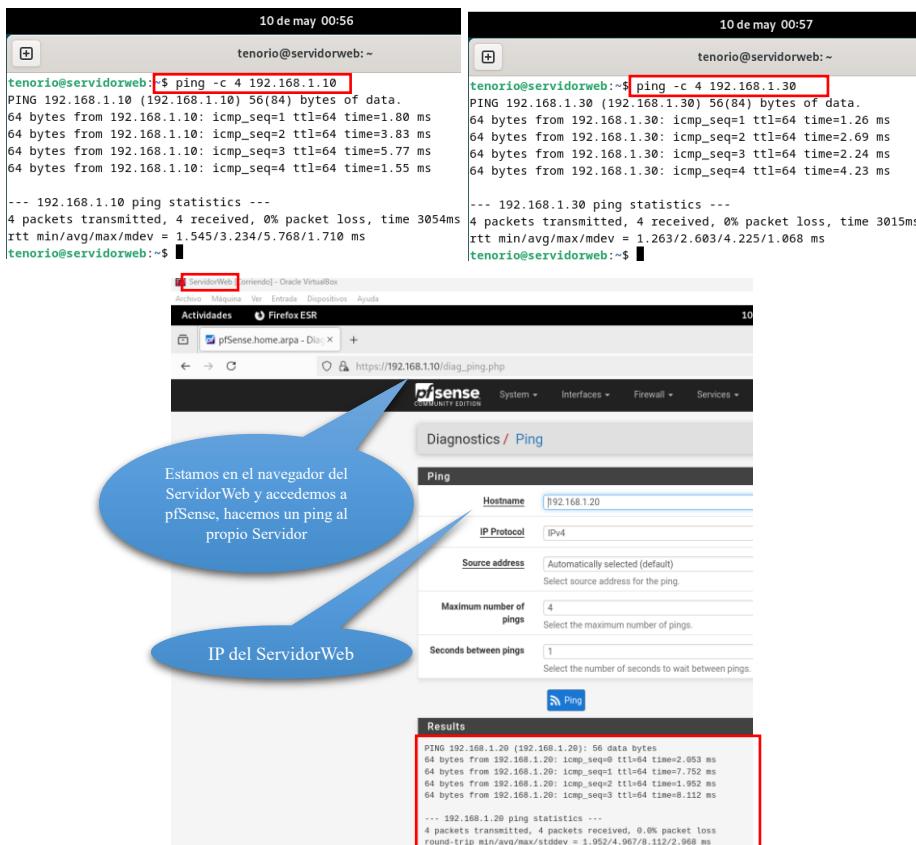
Estamos en el navegador del cliente1 y hacemos un ping al propio cliente1

IP del cliente1

IP del ServidorWeb

- Desde el servidor web 192.168.1.20

- ping 192.168.1.10 (pfSense).
- ping 192.168.1.30 (cliente1) y desde (pfSense).
- ping 192.168.1.20 desde (pfSense) al (ServidorWeb).



10 de may 00:56

tenorio@servidorweb:~\$ ping -c 4 192.168.1.10

PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=1.80 ms

64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=3.83 ms

64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=5.77 ms

64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=1.55 ms

--- 192.168.1.10 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3054ms

rtt min/avg/max/mdev = 1.545/3.234/5.768/1.710 ms

tenorio@servidorweb:~\$

10 de may 00:57

tenorio@servidorweb:~\$ ping -c 4 192.168.1.30

PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.

64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=1.26 ms

64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=2.69 ms

64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=2.24 ms

64 bytes from 192.168.1.30: icmp_seq=4 ttl=64 time=4.23 ms

--- 192.168.1.30 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3015ms

rtt min/avg/max/mdev = 1.263/2.603/4.225/1.068 ms

tenorio@servidorweb:~\$

10 de may 00:57

Actividades Firefox ESR

https://192.168.1.10/diag_ping.php

Diagnostics / Ping

Ping

Hostname: 192.168.1.20

IP Protocol: IPv4

Source address: Automatically selected (default)

Maximum number of pings: 4

Seconds between pings: 1

Ping

Results

PING 192.168.1.20 (192.168.1.20) 56 data bytes

64 bytes from 192.168.1.20: icmp_seq=0 ttl=64 time=2.081 ms

64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=2.264 ms

64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=5.543 ms

64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=2.097 ms

--- 192.168.1.20 ping statistics ---

4 packets transmitted, 4 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 2.007/3.229/5.543/1.396 ms

Results

PING 192.168.1.20 (192.168.1.20) 56 data bytes

64 bytes from 192.168.1.20: icmp_seq=0 ttl=64 time=2.053 ms

64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=7.752 ms

64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=1.952 ms

64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=8.112 ms

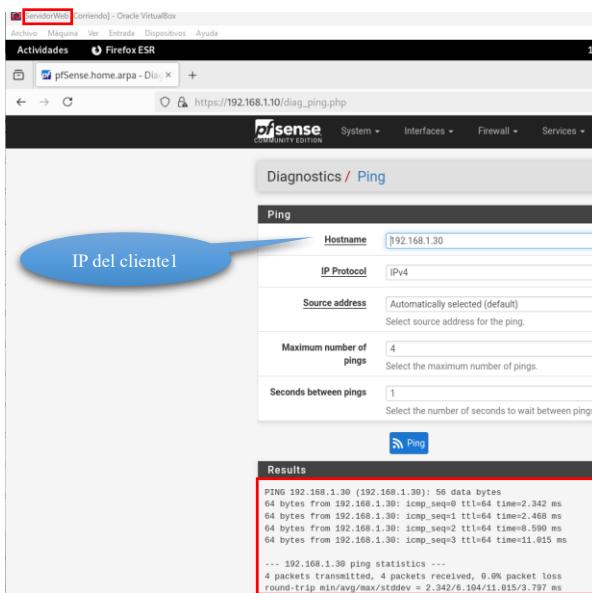
--- 192.168.1.20 ping statistics ---

4 packets transmitted, 4 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 1.952/4.067/8.112/2.968 ms

IP del ServidorWeb

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



4.9.2 Verificación de reglas de pfSense (Firewall).

- Para comprobar cuáles son las reglas que se han establecido por defecto en la instalación de pfSense, desde el cliente1 accedemos con el usuario **atenorio** al panel de administración, menú “Firewall” “Rules”, para ver las reglas establecidas por defecto.

The screenshot shows the pfSense web interface with the URL `https://192.168.1.10/firewall_rules.php?f=lan`. The 'Firewall / Rules / LAN' page is displayed. The 'Rules' tab is selected. The table below shows the configuration of three default rules:

Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
*	*	443	*	*		Anti-Lockout Rule	
*	*	*	*	*	none	Default allow LAN to any rule	
*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

- ✓ La primera regla (Anti-Lockout Rule) asegura que el administrador, siempre pueda acceder a la interfaz de administración web de pfSense desde tu red LAN.
- ✓ Las segunda y tercera reglas (Default allow LAN to any rule) son reglas permisivas que permiten que los dispositivos dentro de tu red LAN se comuniquen con cualquier destino a través de IPv4 e IPv6 respectivamente. Estas son reglas comunes en una configuración básica para proporcionar acceso a internet desde la red local (LAN).

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

2. Para explorar la red y evaluar su seguridad, vamos a utilizar **Nmap**, que es una herramienta gratuita, que nos permite descubrir qué dispositivos están conectados a una red, qué servicios ofrecen, qué sistemas operativos usan y qué cortafuegos están activos. Aunque es muy útil para auditorías de seguridad, también ayuda a los administradores de redes en tareas diarias como inventariar dispositivos, planificar actualizaciones y monitorear el tiempo de actividad de los equipos.

- Instalamos nmap en el **cliente1** ejecutando el comando.

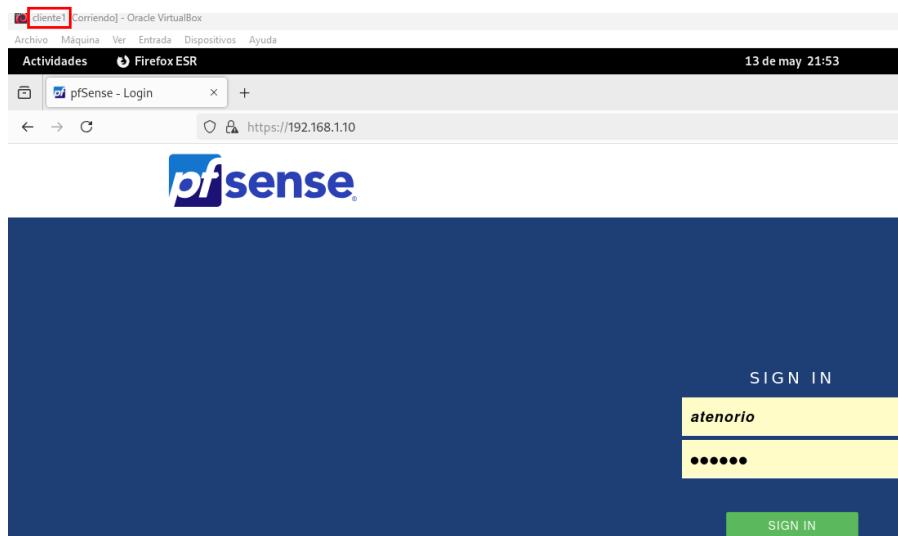
- sudo apt install nmap.

- Ejecutamos un escaneo de puertos con nmap en la dirección IP 192.168.1.20, y nos muestra como resultado, que el puerto 80 TCP está abierto y el servicio que se está ejecutando en él es HTTP, sugiriéndonos que el servidor web está activo en esa dirección IP.

```
12 de may 21:30
antonio@cliente1:~$ nmap 192.168.1.20
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-12 21:18 CEST
Nmap scan report for 192.168.1.20
Host is up (0.0031s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
```

- Intentamos acceder a pfSense desde el cliente1 (<http://192.168.1.10>) y vemos que **no** tiene el acceso bloqueado.



	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

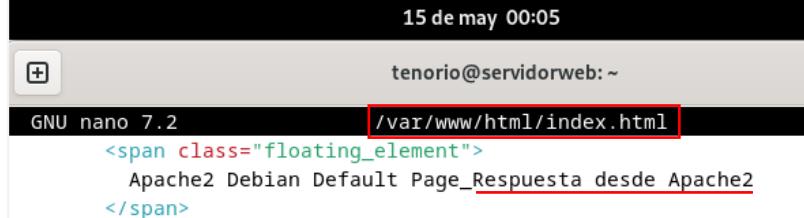
- Ejecutamos un escaneo de puertos con nmap en la dirección IP 192.168.1.10, y nos muestra como resultado, que están abierto los puertos **TCP 53** que se asocia comúnmente con el servicio de nombres de dominio (DNS), **80** que se asocia con el protocolo de transferencia de hipertexto (HTTP), que es la base de la World Wide Web y **443** que se asocia con HTTP sobre TLS/SSL (HTTPS), que es la versión segura de HTTP, sugiriéndonos que el servidor web está activo en esa dirección IP. La mayoría de los otros puertos TCP comunes fueron filtrados, por nuestro firewall. La línea **Not shown: 997 filtered tcp ports (no-response)** indica que el firewall está haciendo su trabajo al no responder a las peticiones en la mayoría de los puertos, protegiendo así la red interna.

```
antonio@cliente1:~$ nmap 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-13 21:55 CEST
Nmap scan report for 192.168.1.10
Host is up (0.0064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.48 seconds
```

3. Comprobamos si el **balanceo/proxy inverso Apache2/Nginx** funciona correctamente.

- En el servidor web abrimos el archivo “index.html” que contiene la página principal ejecutando el comando.
 - sudo nano /var/www/html/index.html
- Editamos una parte del fichero poniendo <Respuesta desde Apache2>, guardamos y cerramos con los comandos ctrl+O y ctrl+X.



```
15 de may 00:05
tenorio@servidorweb: ~
GNU nano 7.2          /var/www/html/index.html
<span class="floating_element">
  Apache2 Debian Default Page_Respuesta desde Apache2
</span>
```

- En Nginx hacemos lo mismo editamos una parte del fichero “index.html” poniendo <Respuesta desde Nginx> ejecutando el comando.
 - sudo nano /usr/share/nginx/html/index.html

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

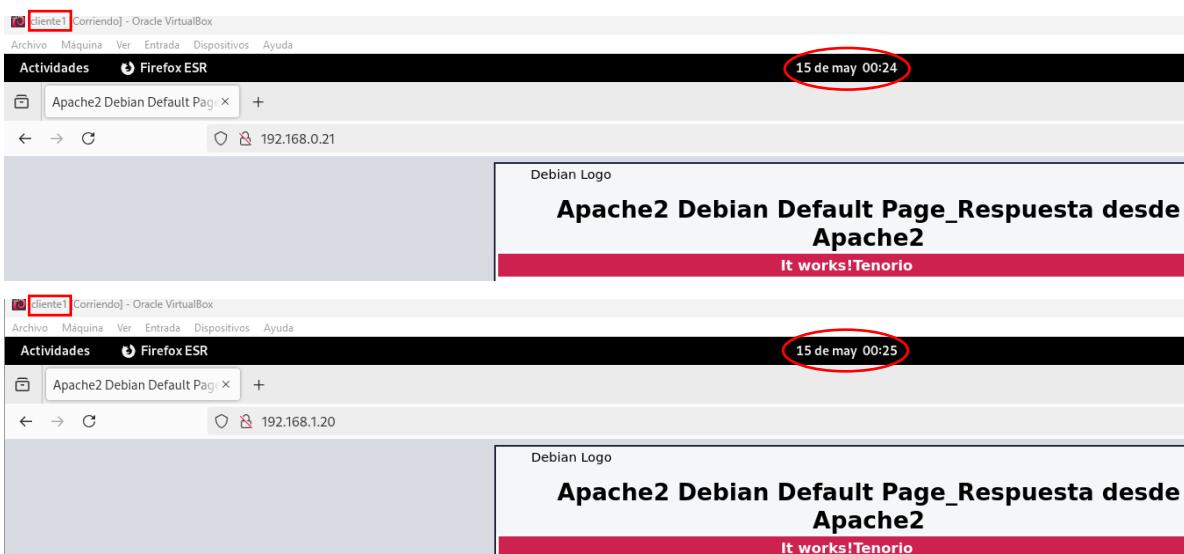
15 de may 00:07

```

+          tenorio@servidorweb: ~
GNU nano 7.2      /usr/share/nginx/html/index.html
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!_Respuesta desde Nginx</h1>

```

- Como Nginx está haciendo de proxy inverso hacia Apache2, vemos el contenido que nos sirve Apache2, así que solo veremos “Respuesta desde Apache2”.
- Realizamos la comprobación abriendo el navegador desde el cliente1 y poniendo en su barra de dirección la IP del servidor web <http://192.168.0.21> externa, recargamos varias veces para ver si cambia el mensaje y como usamos proxy inverso a un único Apache2, siempre veremos la misma respuesta <Respuesta de Apache2>, funcionando correctamente la configuración de nuestro proxy inverso.



The screenshot displays two client machines, 'cliente1' and 'cliente2', both running Oracle VirtualBox. Each client has a Firefox ESR browser window open to the IP address 192.168.0.21. The timestamp in the top right corner of each browser window is circled in red, showing '15 de may 00:24' for cliente1 and '15 de may 00:25' for cliente2. Both browser windows show the same Apache2 Default Page: 'Apache2 Debian Default Page_Respuesta desde Apache2' and 'It works!Tenorio'. This visualizes how the proxy setup ensures both clients receive the same response from the single Apache2 server.

- También podemos comprobarlo desde la consola ejecutando el comando **curl** una vez instalado en Debian 12.

- curl <http://192.168.0.21>

15 de may 00:27

```

+          antonio@cliente1: ~
ent"/>
<span class="floating_element">
Apache2 Debian Default Page_Respuesta desde Apache2

```

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

3.10 Automatización de tareas y scripts.

La automatización de tareas es esencial para mejorar la eficiencia y reducir errores en la administración de sistemas de nuestra empresa, por ello se plantean algunos scripts básicos que pueden ser útiles en el entorno de nuestro proyecto.

3.10.1 Script 1. Copia de seguridad de archivos importantes (Servidor Web).

Este script realiza una copia de seguridad del contenido del directorio **/var/www/html** y lo guarda en un archivo comprimido dentro del directorio **/copia**. El nombre del archivo de copia de seguridad “**copia_fecha.tar.gz**” incluye la fecha actual para facilitar su identificación y asegura que el directorio de destino exista antes de realizar la copia de seguridad con el comando **mkdir -p**.



```

20 de may 21:32
tenorio@servidorweb: /usr/local/bin
GNU nano 7.2           copia_ficheros_html_original.sh *
#!/bin/bash

# Directorio de origen y destino.
dir_original="/var/www/html"
copia_dir="/copia"

# Nombre del archivo de copia de seguridad.
copia_fichero="copia_$(date +%d%m%Y).tar.gz"

# Creamos el directorio de copia de seguridad si no existe.
mkdir -p $copia_dir

# Realizamos la copia de seguridad comprimida.
tar -czf $copia_dir/$copia_fichero $dir_original

# Mensaje de confirmación
echo "La copia de seguridad se ha realizado exitosamente: $copia_dir/$copia_fichero"

```

Un lugar apropiado para guardar nuestros scripts de administración del sistema es el directorio **/usr/local/bin/**. Este directorio suele estar en el PATH del sistema, lo que nos permite ejecutar el script desde cualquier ubicación sin necesidad de especificar la ruta completa, por lo que movemos el script a este directorio con el comando.

- sudo mv /home/tenorio/Documentos/copia_ficheros_html_original.sh /usr/local/bin/

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

19 de may 22:45

```
tenorio@servidorweb:~$ sudo mv /home/tenorio/Documentos/copia_ficheros_html_original.sh /usr/local/bin/
[sudo] contraseña para tenorio:
tenorio@servidorweb:~$ cd /usr/local/bin/
tenorio@servidorweb:/usr/local/bin$ ls
copia_ficheros_html_original.sh
tenorio@servidorweb:/usr/local/bin$ sudo nano copia_ficheros_html_original.sh
tenorio@servidorweb:/usr/local/bin$
```

Script guardado en el directorio especificado

Damos permiso de ejecución al script ejecutando el comando.

- `sudo chmod +x /usr/local/bin/copia_ficheros_html_original.sh`

Ejecutamos el script, realizando este la copia de seguridad satisfactoriamente.

19 de may 23:30

```
tenorio@servidorweb:/copia
tenorio@servidorweb:/usr/local/bin$ sudo ./copia_ficheros_html_original.sh
tar: Eliminando la '/' inicial de los nombres
La copia de seguridad se ha realizado exitosamente: /copia/copia_19052025.tar.gz
tenorio@servidorweb:/usr/local/bin$ ls
copia_ficheros_html_original.sh
tenorio@servidorweb:/usr/local/bin$ cd /var/www/html/
tenorio@servidorweb:/var/www/html$ ls
index.html index.nginx-debian.html
```

Script tiene permiso de ejecución, cambiando de color

Directorio donde están los ficheros originales Apache y Nginx

19 de may 23:30

```
tenorio@servidorweb:/copia
tenorio@servidorweb:/var/www/html$ cd /copia/
tenorio@servidorweb:/copia$ ls
copia_19052025.tar.gz
tenorio@servidorweb:/copia$
```

Ahora vamos a programar la ejecución del script de `copia_ficheros_html_original.sh` todos los días a las 22:00 usando **cron**.

Abrimos la terminal, nos salimos del directorio `/copia` y editamos el archivo “**crontab**” del usuario **tenorio** ejecutando el comando.

- `crontab -e`

Nos pide que elijamos un editor **nano**, para abrir el fichero.

21 de may 00:24

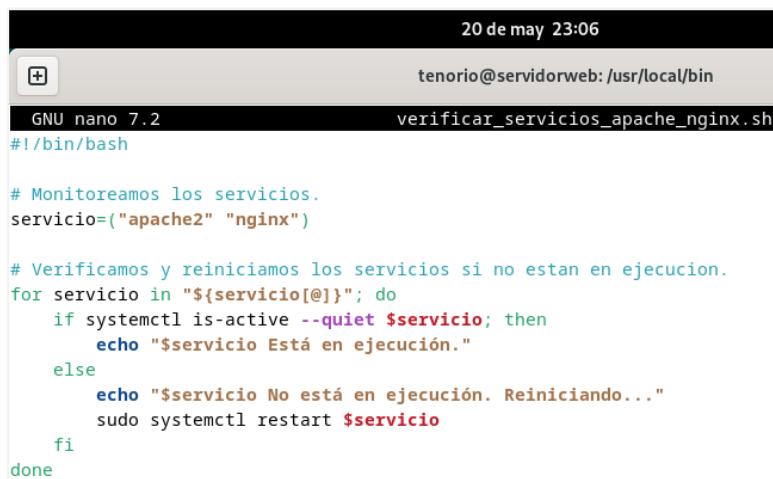
```
tenorio@servidorweb:/
GNU nano 7.2
/tmp/crontab.k8EXi0/crontab *
#
#   m   h   dom   mon   dow      command
# minuto hora dia_mes mes dia_semana ruta_fichero
0 22 * * * /usr/local/bin/copia_ficheros_html_original.sh
# El script de copia de seguridad de nuestros ficheros importantes del Servidor Web,
# se ejecutarán automáticamente todos los días a las 22:00 h.
```

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

3.10.2 Script 2. Monitoreo de los servicios Apache2 y Nginx.

Este script verifica si los servicios Apache2 y Nginx están en ejecución y si no lo están, los reinicia si es necesario.

Nos colocamos en el directorio anterior **/usr/local/bin** donde suele estar el PATH del sistema, lo que nos permitirá ejecutar el script desde cualquier ubicación sin necesidad de especificar la ruta completa y guardamos el script.



```

20 de may 23:06
tenorio@servidorweb:/usr/local/bin
GNU nano 7.2           verificar_servicios_apache_nginx.sh

#!/bin/bash

# Monitreamos los servicios.
servicio=("apache2" "nginx")

# Verificamos y reiniciamos los servicios si no están en ejecución.
for servicio in "${servicio[@]}"; do
    if systemctl is-active --quiet $servicio; then
        echo "$servicio Está en ejecución."
    else
        echo "$servicio No está en ejecución. Reiniciando..."
        sudo systemctl restart $servicio
    fi
done

```

Damos permiso de ejecución al script ejecutando el comando.

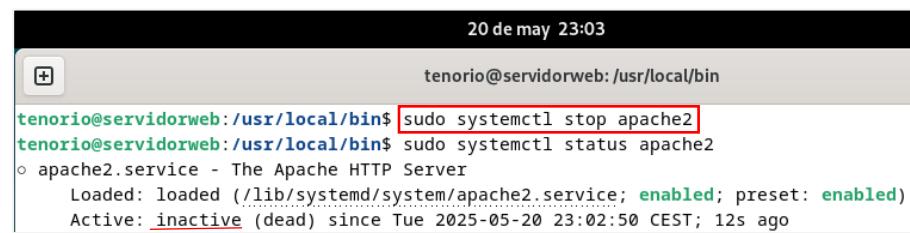
- sudo chmod +x /usr/local/bin/verificar_servicios_apache_nginx.sh

```

tenorio@servidorweb:/usr/local/bin$ sudo chmod +x /usr/local/bin/verificar_servicios_apache_nginx.sh
tenorio@servidorweb:/usr/local/bin$ ls
copia_ficheros_html_original.sh  verificar_servicios_apache_nginx.sh
tenorio@servidorweb:/usr/local/bin$ 

```

Antes de ejecutar el script comprobamos como están los servicios de Apache2 y Nginx, porque los tenemos activados, paramos el servicio de Apache2 para ejecutar el script y ver si funciona correctamente.



```

20 de may 23:03
tenorio@servidorweb:/usr/local/bin
tenorio@servidorweb:/usr/local/bin$ sudo systemctl stop apache2
tenorio@servidorweb:/usr/local/bin$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: inactive (dead) since Tue 2025-05-20 23:02:50 CEST; 12s ago

```

```

tenorio@servidorweb:/usr/local/bin$ sudo ./verificar_servicios_apache_nginx.sh
apache2 No está en ejecución. Reiniciando...
nginx Está en ejecución.
tenorio@servidorweb:/usr/local/bin$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Tue 2025-05-20 23:07:41 CEST; 11s ago

```

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

3.10.3 Script 3. Actualización del S.O. Debian 12.

Este script actualiza el sistema operativo y los paquetes instalados.

Nos colocamos en el directorio anterior **/usr/local/bin/** y guardamos el script.

```
20 de may 23:24
tenorio@servidorweb:/usr/local/bin
GNU nano 7.2           actualizar_sistema.sh
#!/bin/bash

# Actualizamos el S.O.y su lista de paquetes
sudo apt update

# Actualizamos los paquetes instalados a las nuevas versiones.
sudo apt upgrade -y

# Borramos los paquetes innecesarios.
sudo apt autoremove -y

# Mensaje de confirmación.
echo "Actualización del sistema completada."
```

Damos permiso de ejecución al script ejecutando el comando.

- sudo chmod +x /usr/local/bin/actualizar_sistema.sh

```
tenorio@servidorweb:/usr/local/bin$ sudo nano actualizar_sistema.sh
tenorio@servidorweb:/usr/local/bin$ sudo chmod +x actualizar_sistema.sh
tenorio@servidorweb:/usr/local/bin$ ls
actualizar_sistema.sh copia_ficheros_html_original.sh verificar_servicios_apache_nginx.sh
tenorio@servidorweb:/usr/local/bin$
```

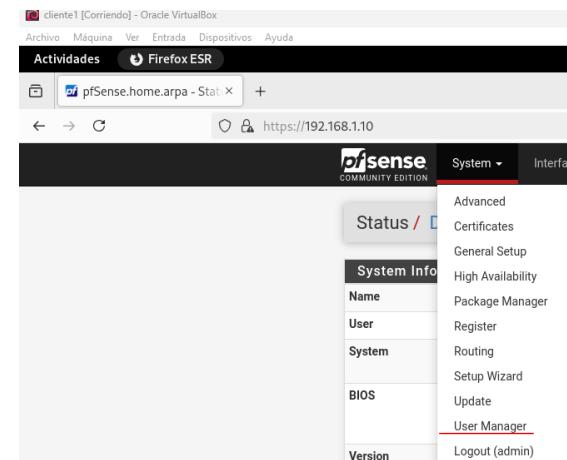
```
20 de may 23:34
tenorio@servidorweb:/usr/local/bin
tenorio@servidorweb:/usr/local/bin$ sudo ./actualizar_sistema.sh
Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Des:3 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Descargados 103 kB en 2s (46,4 kB/s)
```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

5. Administración y Monitorización.

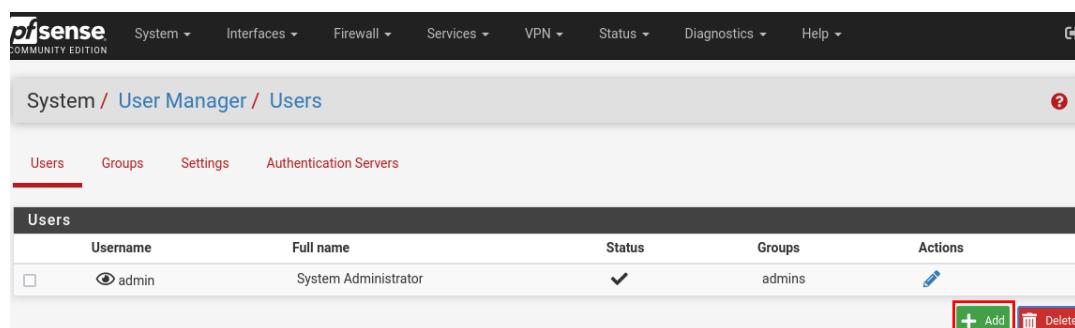
5.1 Gestión de usuari@s y permisos.

- Como medida de seguridad lo primero que haremos será crear nuestro usuario/a para que no estemos accediendo con la cuenta del administrador, para ello nos vamos al menú “System” “User manager”.



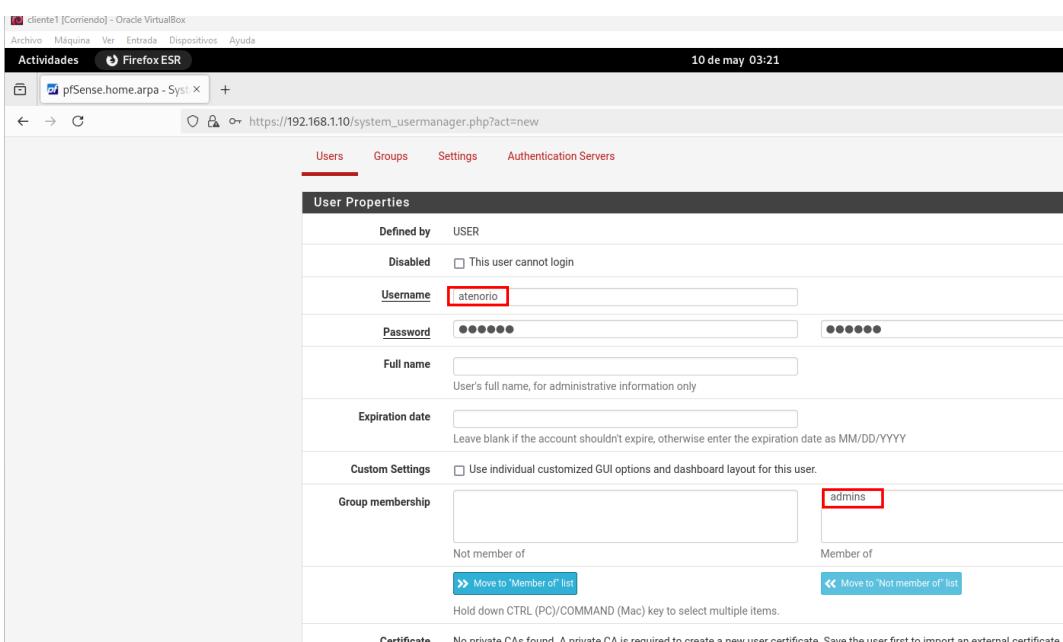
The screenshot shows the pfSense web interface. In the top navigation bar, "System" is selected. Under "System", "User Manager" is highlighted. The main content area displays a sidebar with various system management options like Advanced, Certificates, and General Setup, and a main panel for "System Info" which includes sections for Name, User, System, BIOS, and Version.

- Añadimos un nuevo usuario/a haciendo clic en “Add”.



The screenshot shows the "User Manager / Users" page. The "Users" tab is selected. A table lists one user: "admin" (System Administrator). At the bottom right, there are "Add" and "Delete" buttons, with the "Add" button being highlighted with a green box and a red border.

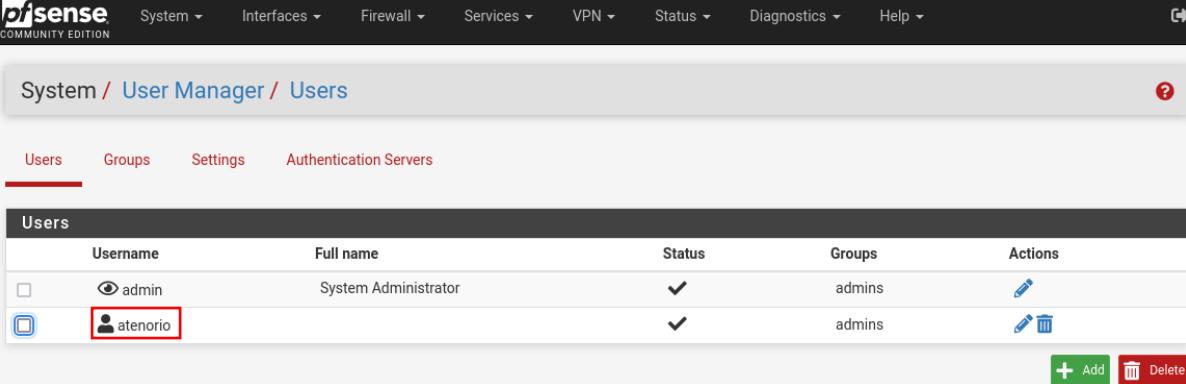
- Configuramos una contraseña y ponemos que pertenece al grupo “admins”.



The screenshot shows the "User Properties" configuration page for a new user. The "Defined by" field is set to "USER". The "Username" field contains "atenorio". The "Password" field has several dots. The "Group membership" field contains "admins", which is highlighted with a red box. The "Member of" field is empty.

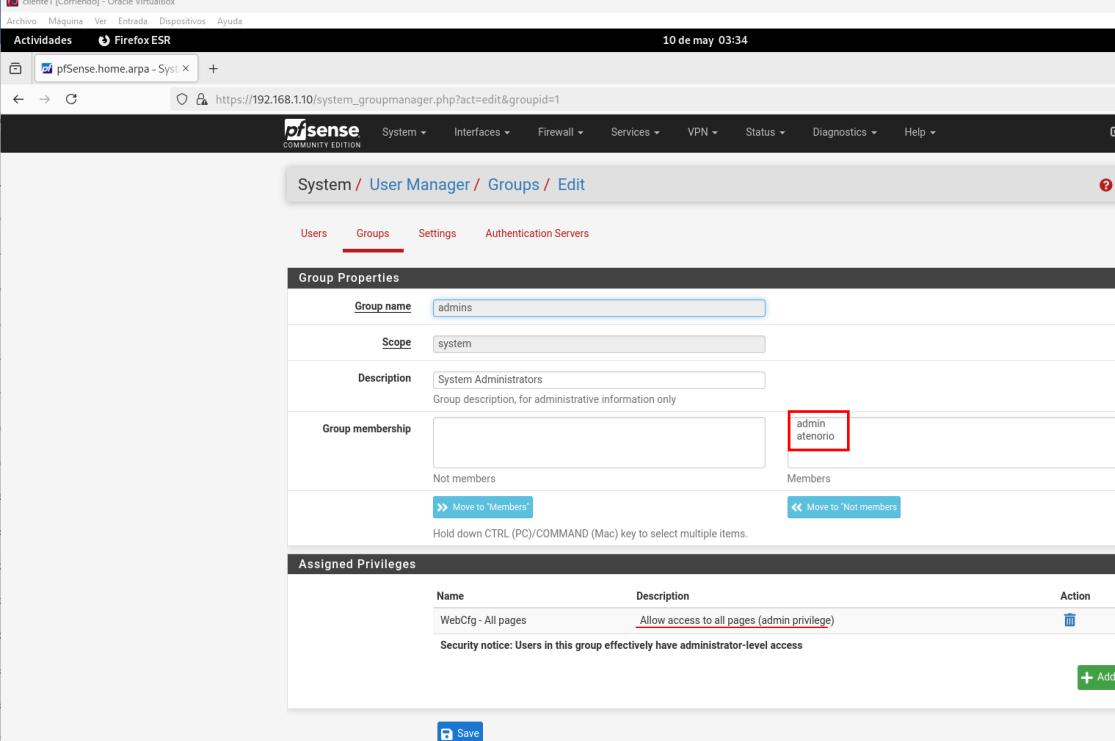
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

4. Ya está añadido el usuario **atenorio** como administrador.



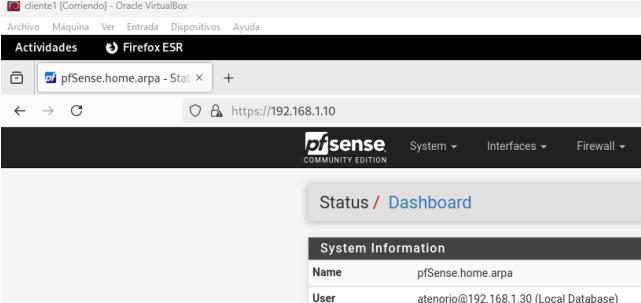
The screenshot shows the pfSense User Manager interface. At the top, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Users' tab is selected. Below it is a table with columns: Username, Full name, Status, Groups, and Actions. Two users are listed: 'admin' (System Administrator) and 'atenorio' (User). Both users have their status checked and belong to the 'admins' group. The 'Actions' column for each user includes edit and delete icons. At the bottom right of the table, there are 'Add' and 'Delete' buttons.

5. En el menú “Groups” podemos ver que el grupo “admins” tiene dos usuarios **admin** y **atenorio** con todos los privilegios.



The screenshot shows the pfSense Group Manager interface. At the top, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Groups' tab is selected. Below it is a 'Group Properties' section for the 'admins' group. The 'Group name' is 'admins', 'Scope' is 'system', and 'Description' is 'System Administrators'. Under 'Group membership', there are two users: 'admin' and 'atenorio', both of which are highlighted with a red box. There are 'Move to Members' and 'Move to Not members' buttons. Below this is an 'Assigned Privileges' table with one entry: 'WebCfg - All pages' with a description 'Allow access to all pages (admin privilege)'. A note says 'Security notice: Users in this group effectively have administrator-level access'. At the bottom right, there is a 'Save' button.

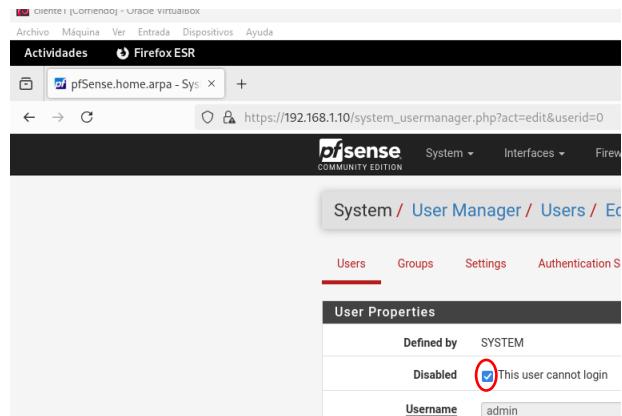
6. Salimos de pfSense y accedemos con el usuario **atenorio**.



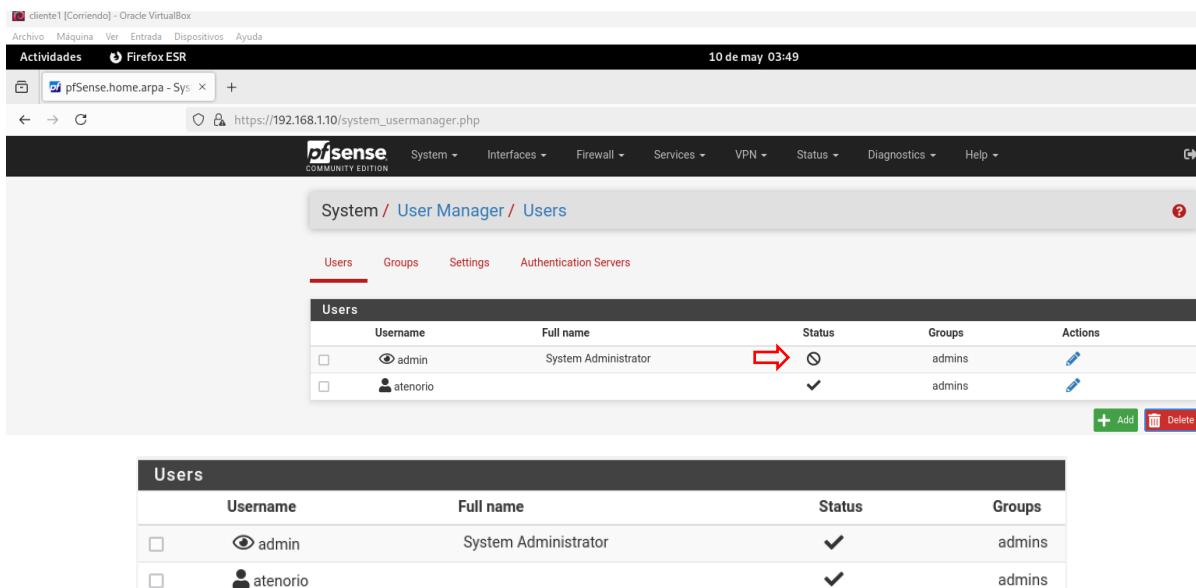
The screenshot shows the pfSense Status / Dashboard interface. At the top, there are tabs for 'Status' and 'Dashboard'. Below it is a 'System Information' table with two rows: 'Name' (pfSense.home.arpa) and 'User' (atenorio@192.168.1.30 (Local Database)).

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

7. Para dar mayor seguridad a la hora de administrar pfSense podríamos deshabilitar a “admin”, habilitando la casilla “Este usuario/a no puede iniciar sesión”. Como estamos en un entorno de prácticas no lo voy a deshabilitar.



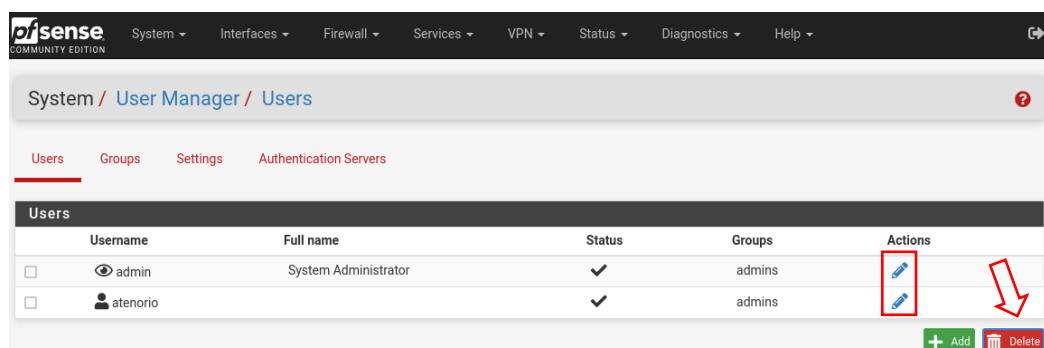
The screenshot shows the pfSense User Manager interface. In the 'User Properties' section, the 'Disabled' checkbox is checked, indicating that the user cannot log in. A red circle highlights this checkbox.



The screenshot shows the pfSense User Manager interface. The 'Users' list page is displayed, showing two users: 'admin' and 'atentorio'. The 'admin' user is selected. A red arrow points to the 'Delete' button in the 'Actions' column of the 'admin' row.

Users					
Username	Full name	Status	Groups	Actions	
admin	System Administrator	✗	admins		
atentorio		✓	admins		

8. De igual manera podríamos actualizar o eliminar usuarios/as de forma fácil, haciendo clic en la casilla “Delete” y en el “Lápiz”.



The screenshot shows the pfSense User Manager interface. The 'Users' list page is displayed, showing two users: 'admin' and 'atentorio'. The 'admin' user is selected. A red box highlights the 'Edit' icon in the 'Actions' column of the 'admin' row. A red arrow points from this 'Edit' icon to the 'Delete' button in the bottom right corner of the page.

Users					
Username	Full name	Status	Groups	Actions	
admin	System Administrator	✗	admins		
atentorio		✓	admins		

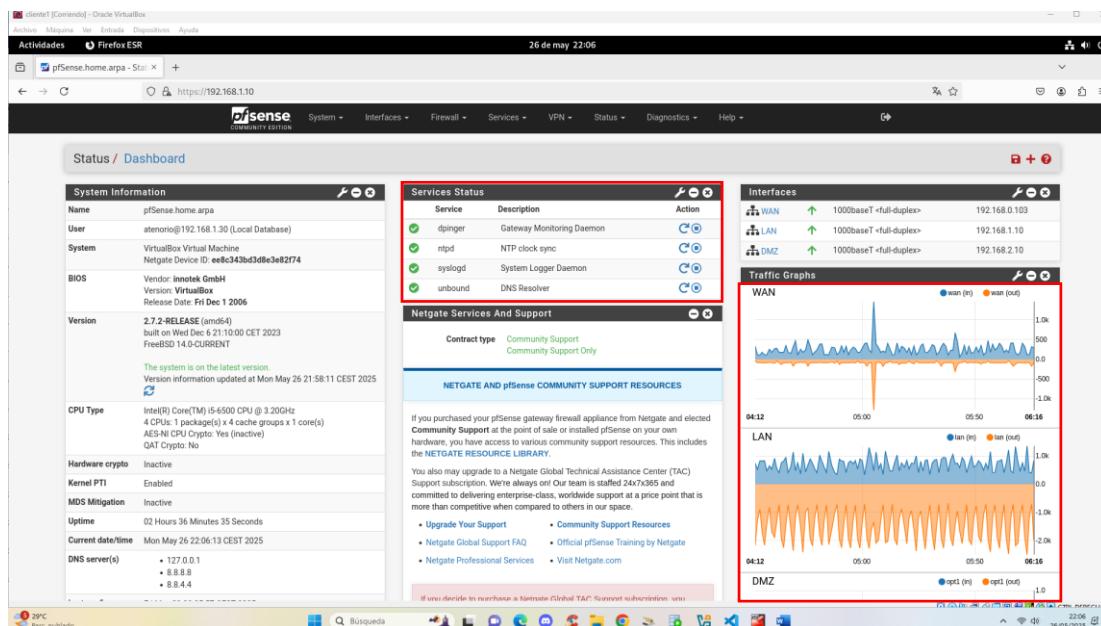
5.2 Herramientas de monitorización y alertas.

La monitorización y las alertas son esenciales para mantener el sistema en buen estado y responder rápidamente a cualquier problema.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Monitorización

El **dashboard de pfSense**, proporciona una visión general del estado del sistema, incluyendo el uso de CPU, memoria y tráfico de red. Para acceder, iniciamos sesión en la interfaz web y abrimos el panel de administración, se muestra por defecto el dashboard o bien desde el menú “Status”, “Dashboard”. También podemos personalizarlo, arrastrando y soltando widgets para mostrar información que nos interese, en nuestro caso hemos puesto dos cuadros uno con el gráfico de tráfico de red de la LAN y WAN y un cuadro con el estado de los servicios fundamentales para el funcionamiento y la gestión de redes y sistemas.

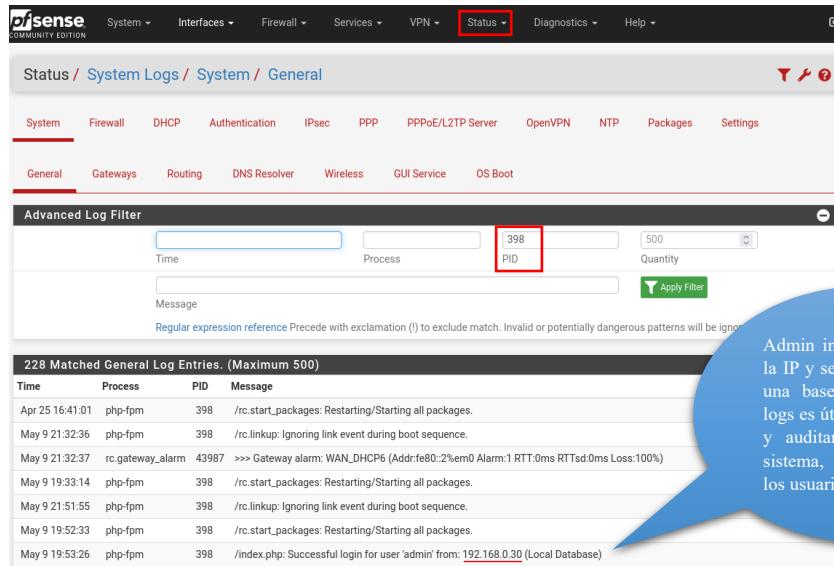


Resumen

- **dping:** Monitorea la conectividad de red a través de gateways.
- **ntpd:** Sincroniza el reloj del sistema con servidores de tiempo.
- **syslogd:** Recopila y registra mensajes de log del sistema y aplicaciones.
- **unbound:** Proporciona resolución de nombres de dominio de manera segura y eficiente.

Podemos utilizar los **logs y reportes** del sistema y generar informes para analizar el tráfico y detectar anomalías, accediendo al menú “Status”, “System Logs”, “Log filter” y hacer un filtro por número identificador del proceso PID.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------



The screenshot shows the pfSense system logs interface. A blue callout bubble points to a specific log entry:

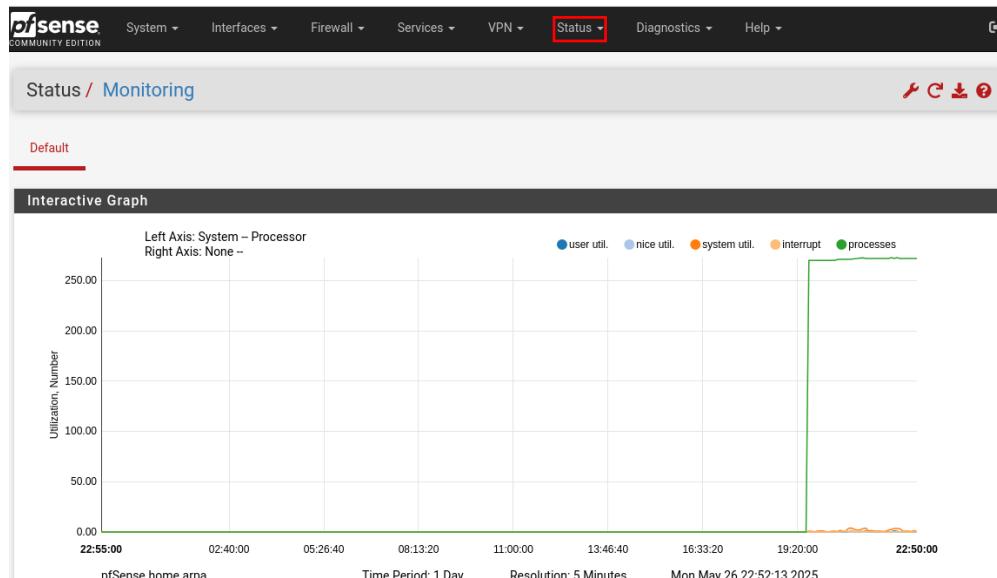
```

228 Matched General Log Entries. (Maximum 500)
Time          Process    PID   Message
Apr 25 16:41:01 php-fpm    398   /rc.start_packages: Restarting/Starting all packages.
May 9 21:32:36 php-fpm    398   /rc.linkup: Ignoring link event during boot sequence.
May 9 21:32:37 rc.gateway_alarm 43987 >> Gateway alarm: WAN_DHCPS (Addr:fe80::2%em0 Alarm:1 RTT:0ms RTTsd:0ms Loss:100%)
May 9 19:33:14 php-fpm    398   /rc.start_packages: Restarting/Starting all packages.
May 9 21:51:55 php-fpm    398   /rc.linkup: Ignoring link event during boot sequence.
May 9 19:52:33 php-fpm    398   /rc.start_packages: Restarting/Starting all packages.
May 9 19:53:26 php-fpm    398   /index.php: Successful login for user 'admin' from: 192.168.0.30 (Local Database)

```

Admin inicia sesión desde la IP y se autentica usando una base de datos local, lo que es útil para monitorear y auditar los accesos al sistema, asegurando sólo los usuarios autorizados.

Para generar informes gráficos sobre el tráfico y el uso de recursos, podemos hacerlo desde el menú “Status”, “Monitoring”.

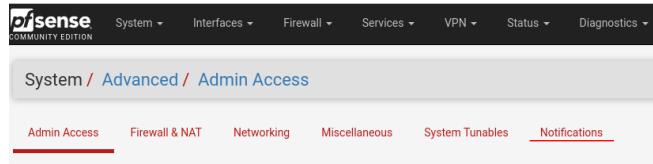


Podemos configurar SNMP para integrar pfSense con herramientas de monitorización externas como **Nagios**, **Zabbix** o **Grafana**, desde el menú “Service”, “SNMP” y recibir alertas.

Alertas

También podemos establecer alertas por correo electrónico para notificar sobre eventos críticos, desde el menú “System”, “Advanced”, “Notifications”.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	



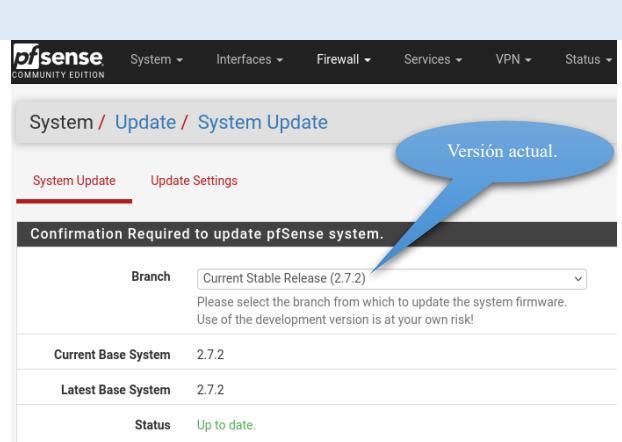
Configurar通知 en el panel de administración para eventos importantes, desde el mismo lugar accediendo a “Admin Access”, además de integrar pfSense con sistemas de gestión de eventos para una respuesta más rápida a incidentes utilizando herramientas como **Syslog-ng** o **Graylog** para centralizar los logs y las alertas.

5.3 Mantenimiento preventivo y correctivo.

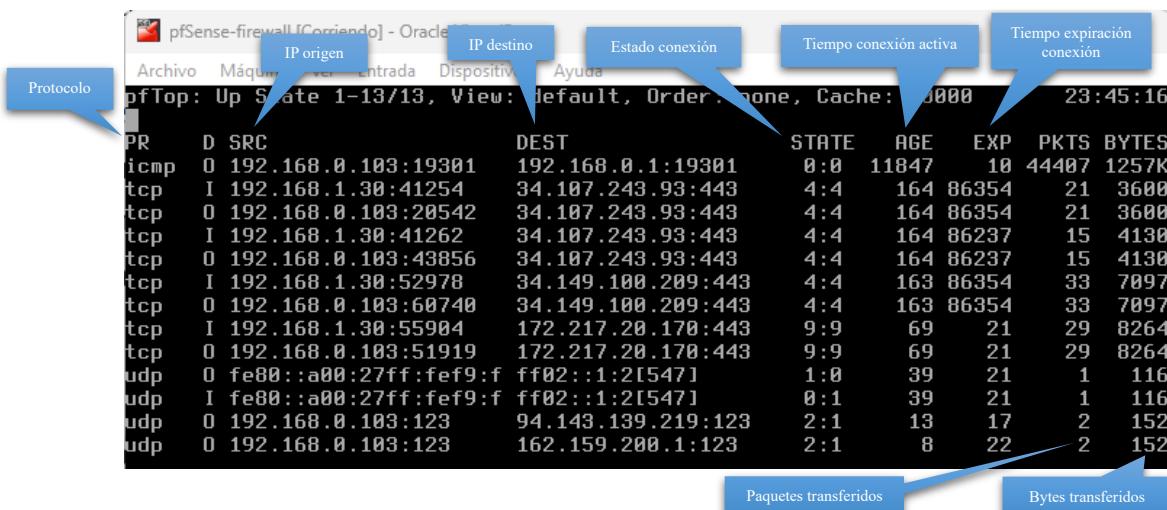
Es esencial para evitar fallos y corregir problemas rápidamente.

Preventivo

Debemos realizar **actualizaciones** regulares para mantener el sistema y los paquetes actualizados, corregir vulnerabilidades y mejorar el rendimiento, desde el menú “System”, “Update”, “Check for Updates” para que nos busque actualizaciones.



Revisar regularmente los **logs** del sistema para detectar y corregir problemas potenciales, así como realizar **pruebas de rendimiento** periódicas para identificar cuellos de botella y optimizar el sistema con herramientas como **pfTop** que monitorizan el rendimiento en tiempo real, a través de la terminal de pfSense.



	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

Correctivo

Establecer un **procedimiento claro** para responder a incidentes y corregir problemas rápidamente, documentando los pasos a seguir en caso de un incidente.

Realizar un **análisis de las causas desde la raíz** para identificar los problemas desde el origen y evitar que se repitan, utilizando técnicas como el diagrama de causa y efecto Ishikawa (espina de pescado) herramienta visual para identificarlos.

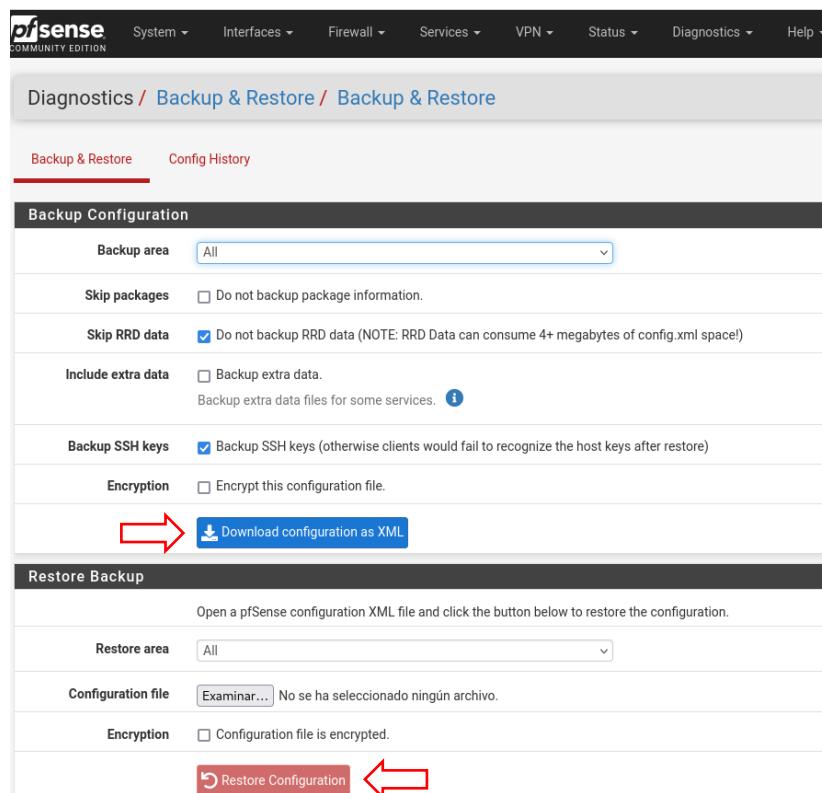
Documentamos todos los problemas y soluciones para futuras referencias, manteniendo si es posible un registro detallado de incidentes, con la descripción del problema y los pasos tomados para solucionarlos.

5.4 Políticas de backup y recuperación.

Estas políticas son esenciales para proteger los datos y garantizar la continuidad de la empresa.

Backup

Descargamos copias de seguridad regulares de la configuración y los datos críticos, desde el menú “Diagnostics”, “Backup & Restore”, y hacemos clic en el cuadro azul “Download configuration as XML”. También podemos restaurar la configuración a través de nuestras copias de seguridad descargadas.



 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

También es una buena práctica, **almacenar las copias de seguridad** en un lugar seguro, preferiblemente fuera de pfSense, en la nube o dispositivos externos y utilizar scripts y herramientas para **automatizar** el proceso de backup como hemos realizado con el servidor web, realizando la copia de los index.html.

Recuperación

Es conveniente desarrollar un **plan de recuperación** ante desastres que documente los pasos a seguir en caso de una falla crítica, incluyendo procedimientos para restaurar la configuración y los datos desde las copias de seguridad, realizar **pruebas de recuperación** periódicas y simulación de fallas y prácticas de recuperación de datos, para garantizar que los backups sean válidos y que el proceso de recuperación funcione correctamente.

No olvidarnos de hacer un **manual de recuperación** ante desastres bien detallado y con contactos de emergencia, por si necesitáramos ayuda de algún administrador/a con más experiencia.

6. Seguridad Informática.

6.1 Configuración de reglas de pfSense (Firewall).

Antes de realizar la configuración de las reglas, detallamos un resumen de la red actual.

Red Actual

LAN (interna): 192.168.1.0/24 <ul style="list-style-type: none"> • <i>pfSense (LAN):</i> 192.168.1.10 • <i>Servidor web:</i> 192.168.1.20 <ul style="list-style-type: none"> • <i>Cliente1:</i> 192.168.1.30 	WAN (externa): 192.168.0.0/24 <ul style="list-style-type: none"> • <i>pfSense (WAN):</i> 192.168.0.24 • <i>Servidor web:</i> 192.168.0.21 <ul style="list-style-type: none"> • <i>Cliente1:</i> 192.168.0.23
---	---

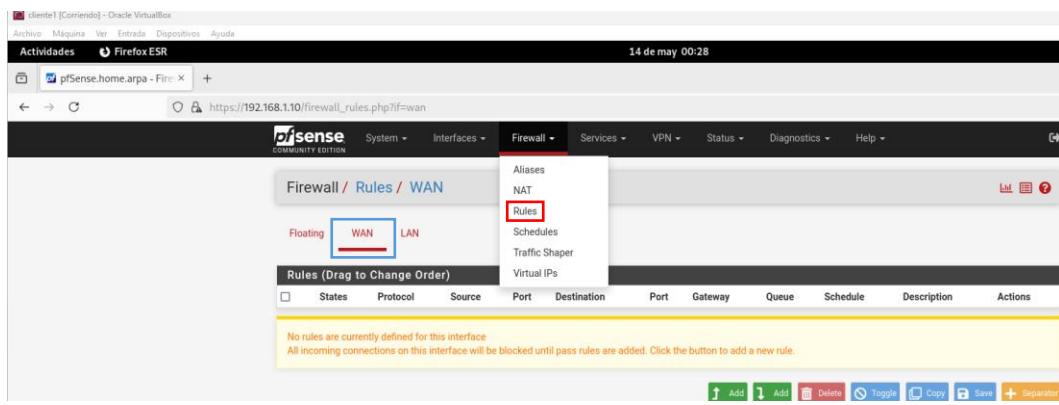
6.1.1 Regla 1. Conexión del equipo anfitrión a pfSense.

Desde el cliente1 vamos a agregar una regla para que podamos conectarnos desde el equipo anfitrión Windows 11 al servidor pfSense a través de la red WAN por el puerto HTTPS 443, sólo como prueba, porque lo lógico sería que el administrador se conectara desde la red local LAN², bien desde el servidor web o cualquiera de los equipos de la red interna e hiciera las tareas de configuración desde un entorno seguro.

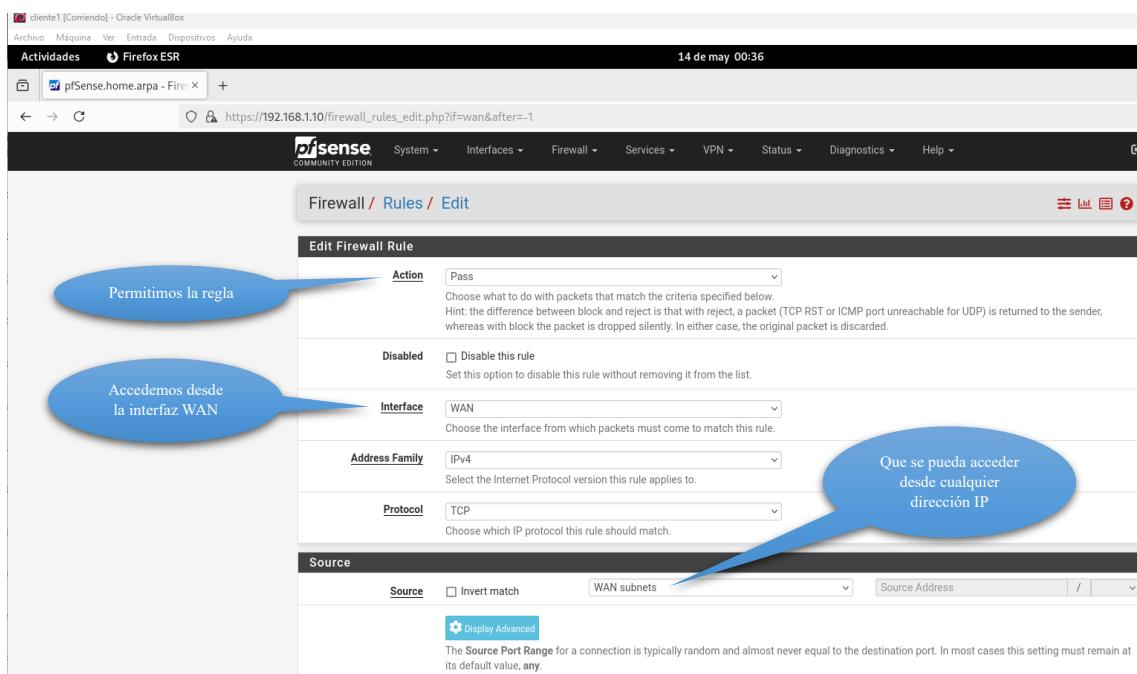
² Por seguridad la configuración del cortafuegos (pfSense) se debe hacer por la red LAN siempre.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

- Nos vamos al panel de administración menú “Firewall” “Rules” “WAN” y hacemos clic en “Add”.



The screenshot shows the pfSense Firewall Rules WAN interface. The 'Rules' tab is selected. A blue callout points to the 'Add' button at the bottom right of the interface.



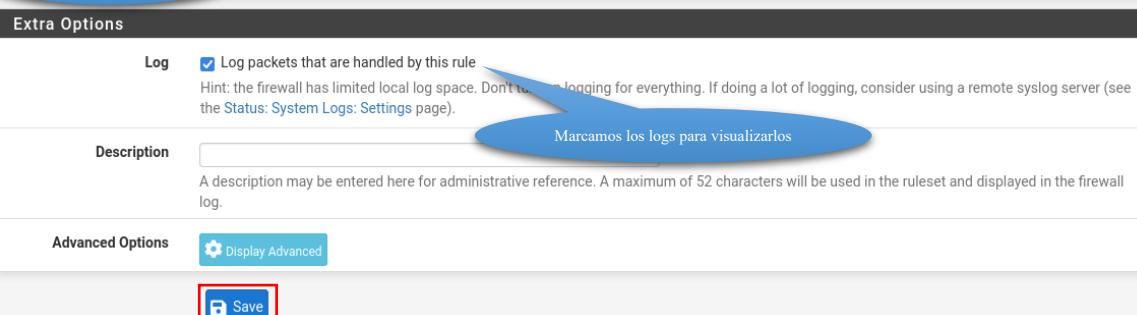
The screenshot shows the 'Edit Firewall Rule' configuration page. Annotations explain the parameters:

- Permitimos la regla (We allow the rule)
- Accedemos desde la interfaz WAN (Access from the WAN interface)
- Que se pueda acceder desde cualquier dirección IP (That it can be accessed from any IP address)



The screenshot shows the 'Destination' section of the rule configuration. Annotations explain:

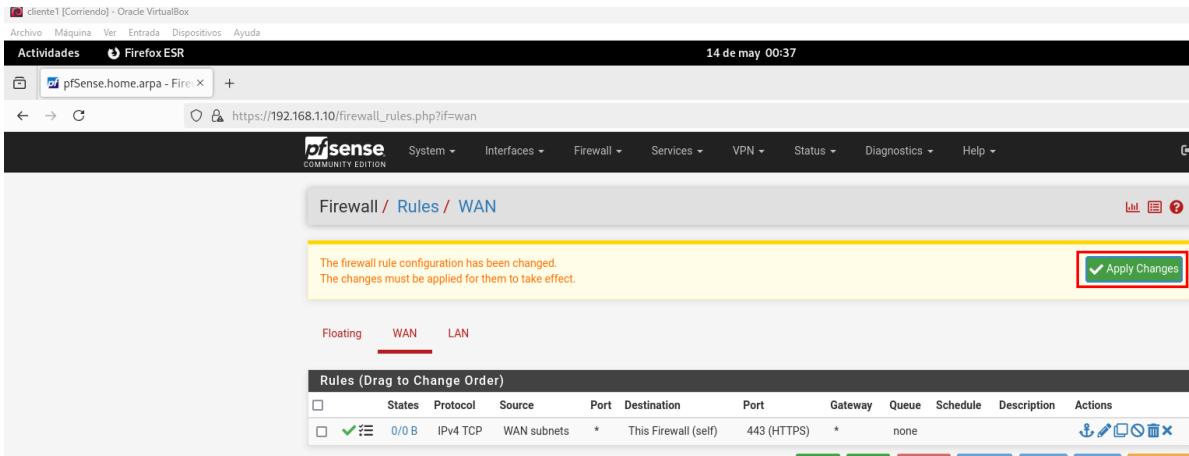
- Agregamos una regla (We add a rule)
- El destino nuestro Firewall (The destination is our Firewall)

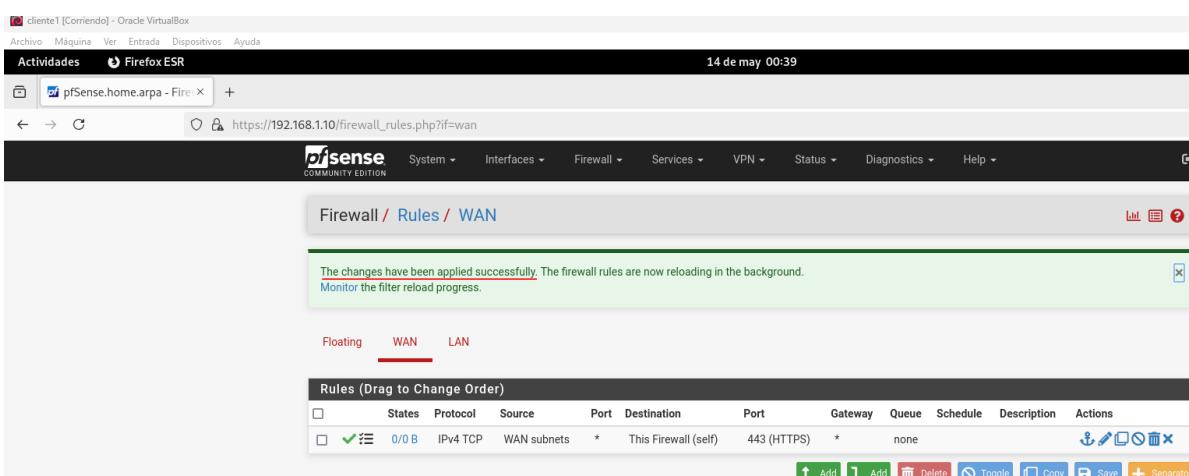


The screenshot shows the 'Extra Options' section of the rule configuration. Annotations explain:

- Marcamos los logs para visualizarlos (We mark the logs to view them)
- Save button highlighted (Save button highlighted)

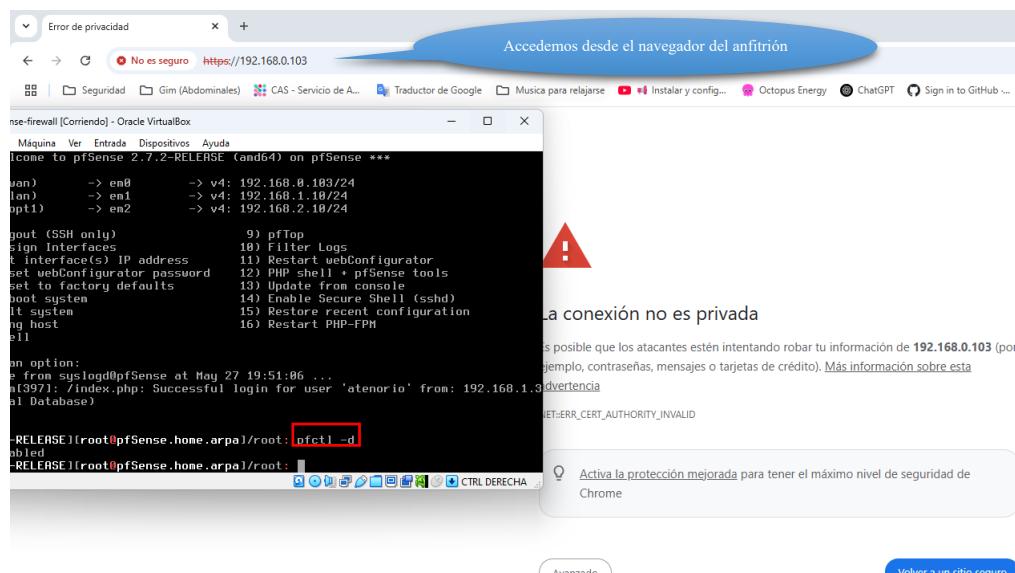
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	-----------------------------------	---	-----------------------------------





- Nos vamos al menú principal de pfSense y pulsamos la opción 8 para entrar en la Shell, una vez dentro ejecutamos el comando.

- `pfctl -d` (deshabilitamos pfSense para que nos permita acceder a su interfaz).



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

Desde el equipo anfitrión hemos podido acceder al panel de administración de pfSense con la IP que nos da salida a Internet desde el Firewall.

The screenshot shows the pfSense Status / Dashboard. It includes sections for System Information (IP: 192.168.1.10, User: atenorio), Netgate Services And Support (Community Support), and Interfaces (WAN, LAN, DMZ). The Traffic Graphs section shows WAN, LAN, and DMZ traffic over time.

Aquí podemos ver los movimientos de paquetes que ha habido, al haberlos conectado a través del anfitrión a pfSense.

The screenshot shows the Firewall / Rules / WAN configuration page. It displays a table of rules and a "Rules (Drag to Change)" sidebar. A tooltip provides details about the selected rule: Tracking ID: 1747175864, evaluations: 1.52K, packets: 2.29K, bytes: 1.08 MB, states: 1, state creations: 8.

```
pfSense-firewall [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
DMZ (opt1) -> em2 -> v4: 192.168.2.10/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option:
message from syslogd@pfSense at May 27 19:51:06 ...
php-fpm[397]: /index.php: Successful login for user 'atenorio' from: 192.168.1.3
0 (Local Database)
8

[2.7.2-RELEASE]root@pfSense.home.arpal/root: pfctl -d
of disabled
[2.7.2-RELEASE]root@pfSense.home.arpal/root:
Message from syslogd@pfSense at May 27 20:08:54 ...
php-fpm[397]: /index.php: Successful login for user 'atenorio' from: 192.168.0.1
00 (Local Database)
```

En el menú de pfSense nos aparece un mensaje de conexión satisfactoria desde el equipo anfitrión.

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::757d:ecaf:27f7:9473%7
Dirección IPv4. . . . . : 192.168.0.100
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.0.1
```

IP equipo anfitrión

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

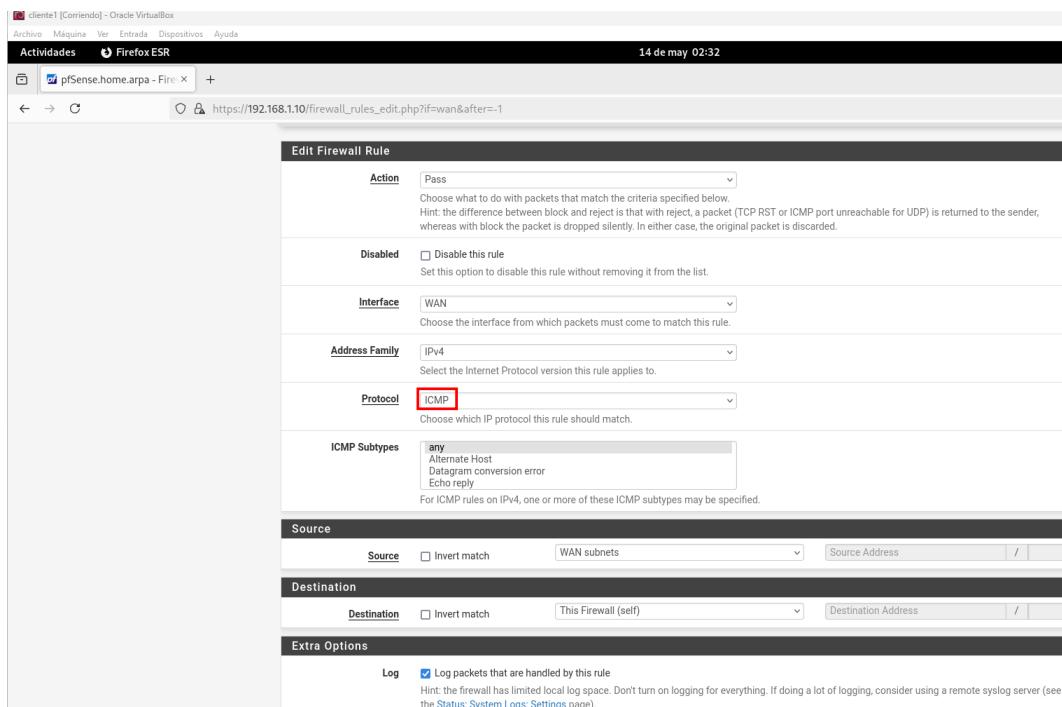
- Finalizada la configuración anterior volvemos a activar pfSense (Firewall) ejecutando el comando.

- `pfctl -e`

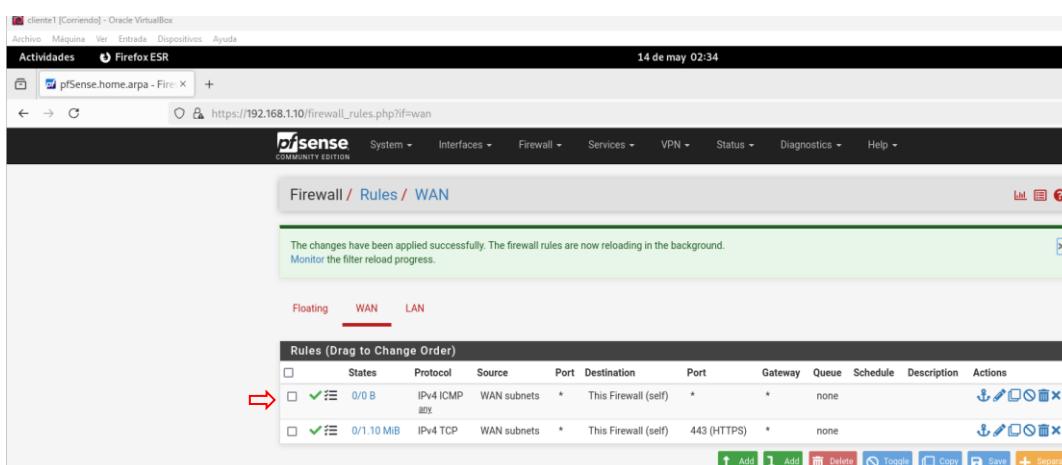
```
B: Command not found.
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -e
of enabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: █
```

6.1.2 Regla 2. Ping del equipo anfitrión a pfSense.

Creamos otra regla que nos permita realizar un ping desde el equipo anfitrión al firewall, porque ahora mismo no existe, es por ello, que la comunicación entre ambos equipos está bloqueada, utilizando el protocolo ICMP.



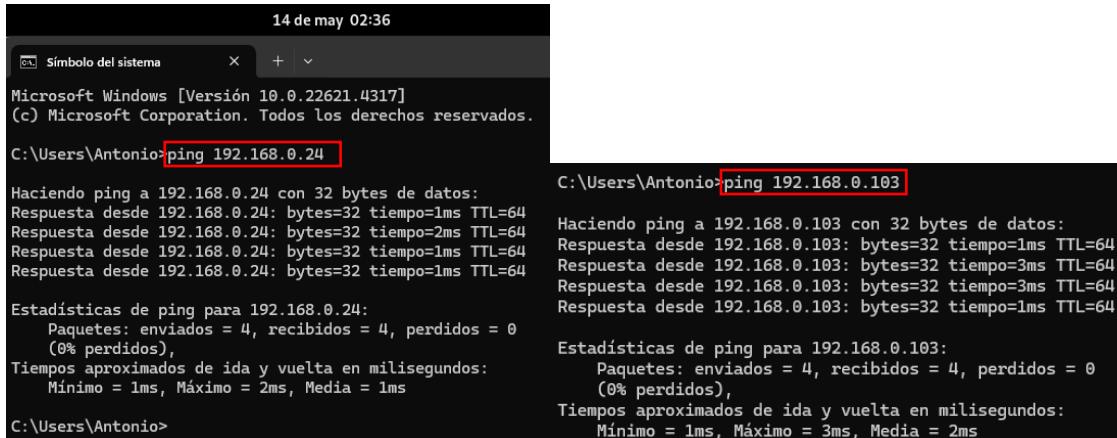
The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Protocol' field is set to 'ICMP'. Under 'ICMP Subtypes', 'Echo reply' is selected. In the 'Source' section, 'WAN subnets' is specified. In the 'Destination' section, 'This Firewall (self)' is selected. The 'Log' checkbox is checked. The 'Action' dropdown is set to 'Pass'.



The screenshot shows the 'Firewall / Rules / WAN' list. A red arrow points to the newly created rule, which has an '0/0 B' state and an '0/1.10 MiB' rate limit. The rule allows ICMP traffic from 'WAN subnets' to 'This Firewall (self)' on port 443 (HTTPS). The 'Actions' column shows icons for edit, delete, toggle, copy, save, and separator.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

- Realizamos un ping a la IP del firewall 192.168.0.24 y ahora sí obtenemos respuesta³.



```

14 de may 02:36

Símbolo del sistema x + v
Microsoft Windows [Versión 10.0.22621.4317]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Antonio>ping 192.168.0.24

Haciendo ping a 192.168.0.24 con 32 bytes de datos:
Respuesta desde 192.168.0.24: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.24: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.0.24: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.24: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.0.24:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Antonio>

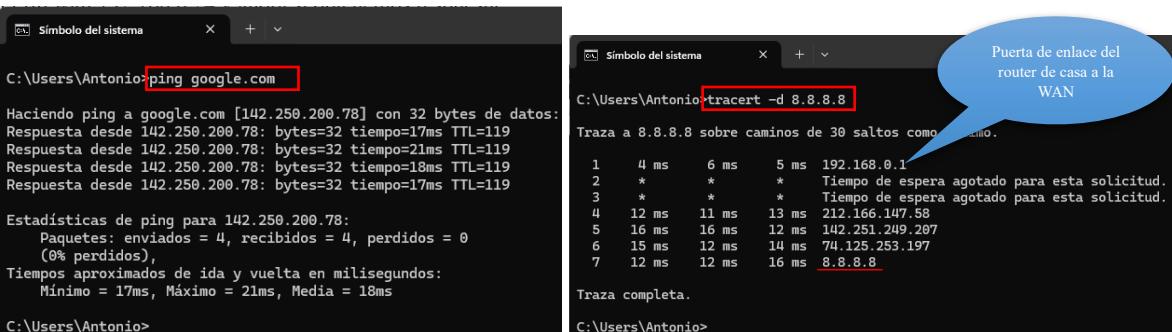
C:\Users\Antonio>ping 192.168.0.103

Haciendo ping a 192.168.0.103 con 32 bytes de datos:
Respuesta desde 192.168.0.103: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.103: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.103: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.103: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.0.103:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 3ms, Media = 2ms

```

Realizamos un ping a Google.com y ejecutamos el comando tracert, obteniendo respuesta.



```

Símbolo del sistema x + v
C:\Users\Antonio>ping google.com

Haciendo ping a google.com [142.250.200.78] con 32 bytes de datos:
Respuesta desde 142.250.200.78: bytes=32 tiempo=17ms TTL=119
Respuesta desde 142.250.200.78: bytes=32 tiempo=21ms TTL=119
Respuesta desde 142.250.200.78: bytes=32 tiempo=18ms TTL=119
Respuesta desde 142.250.200.78: bytes=32 tiempo=17ms TTL=119

Estadísticas de ping para 142.250.200.78:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 17ms, Máximo = 21ms, Media = 18ms

C:\Users\Antonio>

C:\Users\Antonio>tracert -d 8.8.8.8
Traza a 8.8.8.8 sobre caminos de 30 saltos como el primero.
 1   4 ms    6 ms    5 ms  192.168.0.1
 2   *         *         *   Tiempo de espera agotado para esta solicitud.
 3   *         *         *   Tiempo de espera agotado para esta solicitud.
 4   12 ms   11 ms   13 ms  212.166.147.58
 5   16 ms   16 ms   12 ms  142.251.249.287
 6   15 ms   12 ms   14 ms  74.125.253.197
 7   12 ms   12 ms   16 ms  8.8.8.8

Traza completa.

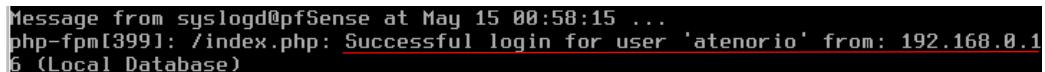
C:\Users\Antonio>

```

6.1.3 Regla 3. Bloquear acceso SSH cliente1 al Servidor Web.

La siguiente regla, la crearemos como administrador desde el equipo anfitrión Windows 11, puesto a que a través de la WAN tenemos acceso a la interfaz web de pfSense.

- En el menú de pfSense nos vuelve aparecer un mensaje de conexión satisfactoria desde el equipo anfitrión.



```

Message from syslogd@pfSense at May 15 00:58:15 ...
php-fpm[399]: /index.php: Successful login for user 'atenorio' from: 192.168.0.1
6 (Local Database)

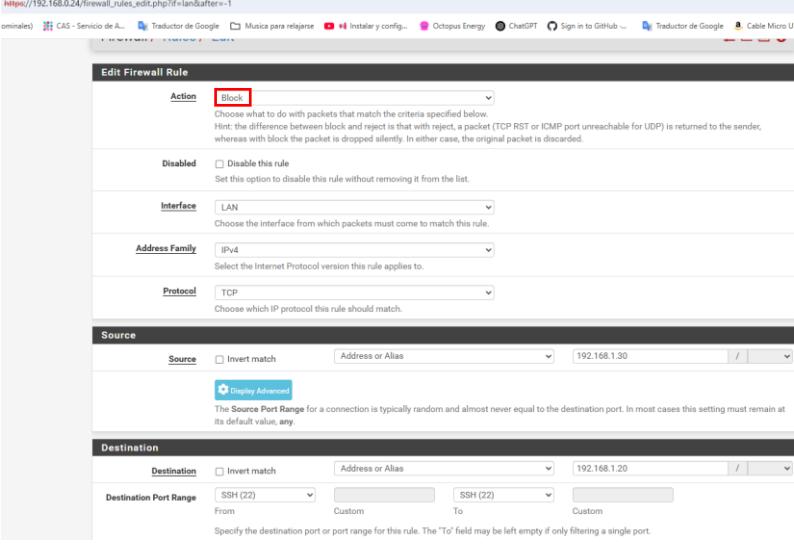
```

- En la barra de direcciones del navegador Firefox ponemos la IP WAN que nos facilita pfSense 192.168.0.24 y accedemos al panel de administración, menú “Firewall” “Rules” “WAN” y hacemos clic en “Add”.

³ En algún momento se puede observar que la IP WAN cambia porque desde el operador de red Vodafone ha sido cambiada, aunque a veces utilizo esta como estática 192.168.0.24 que fue la configuración inicial.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

https://192.168.0.24/firewall_rules.edit.php?if=lan&after=-1



Action: Block

Disabled: Disable this rule

Interface: LAN

Address Family: IPv4

Protocol: TCP

Source: Source: 392.168.1.30

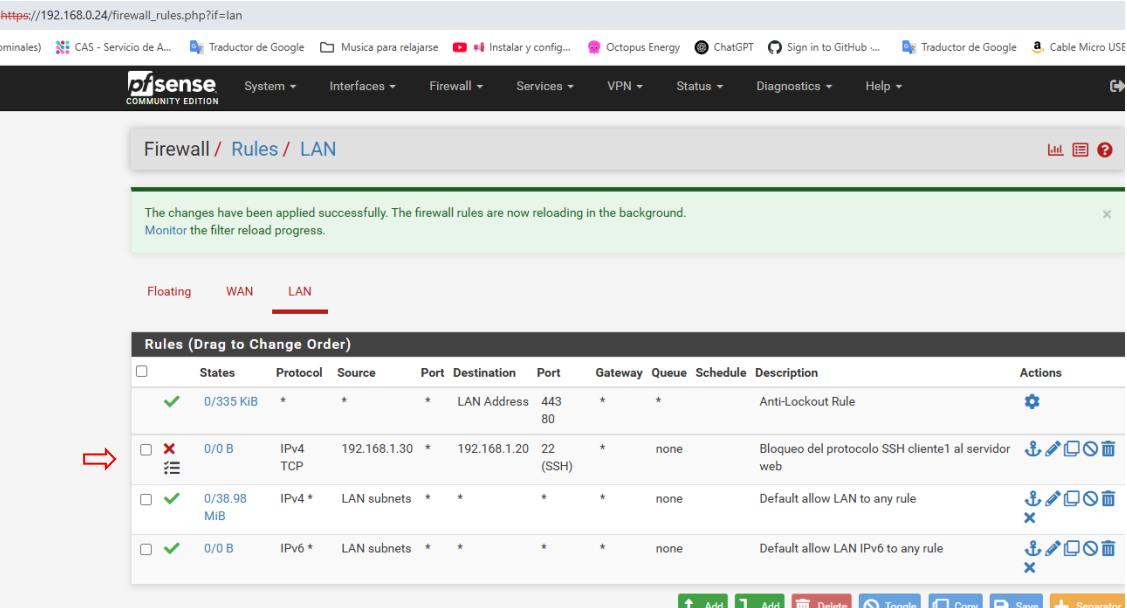
Destination: Destination: 392.168.1.20
Destination Port Range: SSH (22) From: Custom To: Custom

Extra Options:

- Log:** Log packets that are handled by this rule
- Description:** Bloqueo del protocolo SSH cliente1 al servidor web
- Advanced Options:** [Display Advanced](#)

Save

https://192.168.0.24/firewall_rules.php?if=lan



The changes have been applied successfully. The firewall rules are now reloading in the background.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/335 Kib	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	Edit
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.1.30	*	192.168.1.20	22 (SSH)	*	none		Bloqueo del protocolo SSH cliente1 al servidor web	Edit Delete Copy Save
<input type="checkbox"/>	0/38.98 MiB	IPv4	*	*	LAN subnets	*	*	*		Default allow LAN to any rule	Edit Delete Copy Save
<input type="checkbox"/>	0/0 B	IPv6	*	*	LAN subnets	*	*	*		Default allow LAN IPv6 to any rule	Edit Delete Copy Save

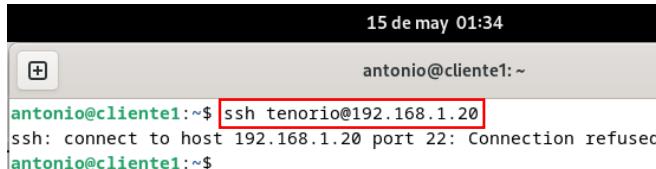
Add **Up** **Down** **Delete** **Toggle** **Copy** **Save** **+ Separator**

- Antes de realizar la comprobación, instalamos ssh en el servidor web y en el cliente1, ejecutando el siguiente comando en la terminal de ambos equipos.

- sudo apt install openssh-server
- sudo apt install openssh-client

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

- Para comprobar que funciona, abrimos la terminal en el cliente1 y ejecutamos el comando.
 - ssh atenorio@192.168.1.20
- Nos muestra un mensaje comunicándonos que el acceso a SSH fue rechazado, bloqueando correctamente el puerto 22 del servidor web.



```
15 de may 01:34
antonio@cliente1: ~
antonio@cliente1:~$ ssh tenorio@192.168.1.20
ssh: connect to host 192.168.1.20 port 22: Connection refused
antonio@cliente1:~$
```

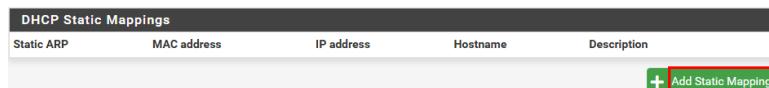
6.1.4 Regla 4. DHCP Bloqueo de clientes desconocidos.

La opción "**Deny Unknown Clients**" en pfSense es una configuración del servidor DHCP que mejora la seguridad de la red. Al activarla, el servidor DHCP solo asigna direcciones IP a dispositivos cuyas direcciones MAC están registradas en una lista previamente en pfSense y que este ha comprobado antes de enviar el mensaje de Offer. Esto significa que sólo los dispositivos con una IP reservada y configurada de manera estática recibirán una dirección IP, evitando que dispositivos no autorizados accedan a la red automáticamente. Esta medida ayuda a controlar y limitar el acceso a la red, asegurando que solo los dispositivos conocidos puedan conectarse.

- Vamos a proteger nuestro servidor DHCP para que no entregue direcciones IP a clientes desconocidos.
- Necesitamos las direcciones MAC de los equipos a los que les vamos a permitir el acceso, por lo que abrimos la terminal del **cliente2** Windows 10 y ejecutamos el comando.

▪ ipconfig /all Dirección física. : 08-00-27-3B-33-31

- Abrimos el panel de administración de pfSense y nos vamos al menú “Services”, “DHCP Server”, al final del todo “DHCP Static Mappings” y añadimos una nueva entrada “Add”.



- Vamos a reservar una IP para la MAC del equipo cliente2.

Static DHCP Mapping on LAN		Static DHCP Mapping on LAN		Other DHCP Options	
Static ARP	MAC address	Static ARP	MAC address	Hostname	Description
DHCP Backend	ISC DHCP	DHCP Backend	ISC DHCP	cliente2-windows	Name of the client host with
MAC Address	08:00:27:3B:33:31	MAC Address	08:00:27:3B:33:31	Description	PC cliente2-windows 10
				Other DHCP Options Gateway: 192.168.1.10 <small>The default is to the correct gate</small> Domain Name: home.arpa	

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- Ya tenemos reservada la IP para el cliente2.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:3b:33:31	192.168.1.40	cliente2-windows	PC cliente2-windows 10

- Renovamos la IP de este equipo cliente2 ejecutando los comandos.

- ipconfig /release (libera la ip actual).
- ipconfig /renew (solicita una nueva ip).

- Obtenemos la IP que hemos reservado para este equipo.

```
Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión . . . : home.arpa
  Vínculo: dirección IPv6 local . . . : fe80::14eb:6356:1a53:a026%8
  Dirección IPv4 . . . . . : 192.168.1.40
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 192.168.1.10
```

- Anteriormente era esta. **Dirección IPv4. : 192.168.1.100(Preferido)**
- Repetimos el proceso con el **cliente1** Debian 12, para ver todas las direcciones MAC de las interfaces podemos ejecutar el comando.

- ip link show

```
31 de may 03:08
antonio@cliente1:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
  link/ether 08:00:27:0f:ab:14 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
  link/ether 08:00:27:b4:de:ee brd ff:ff:ff:ff:ff:ff
```

- Vamos a reservar una IP para la MAC del equipo cliente1.

Static DHCP Mapping on LAN		Other DHCP Options							
DHCP Backend	ISC DHCP	Hostname	1.0.0.1						
MAC Address	08:00:27:0f:ab:14	IP Address	192.168.1.30						
		Description	PC cliente1-debian 12						
		DNS Servers	1.1.1.1						
Other DHCP Options <table border="1"> <tr> <td>Gateway</td> <td>192.168.1.10</td> </tr> <tr> <td colspan="2">The default is t the correct gat</td> </tr> <tr> <td>Domain Name</td> <td>home.arpa</td> </tr> </table>				Gateway	192.168.1.10	The default is t the correct gat		Domain Name	home.arpa
Gateway	192.168.1.10								
The default is t the correct gat									
Domain Name	home.arpa								

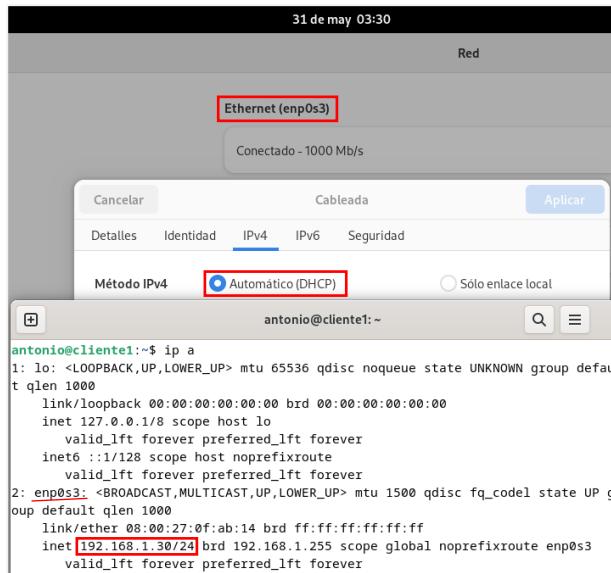
- Ya tenemos reservada la IP para el cliente1.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:0f:ab:14	192.168.1.30	cliente1-debian	PC cliente1-debian 12
	08:00:27:3b:33:31	192.168.1.40	cliente2-windows	PC cliente2-windows 10

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

- Reiniciamos el servicio de red en el equipo cliente1 ejecutando el comando.

- sudo systemctl restart systemd-networkd

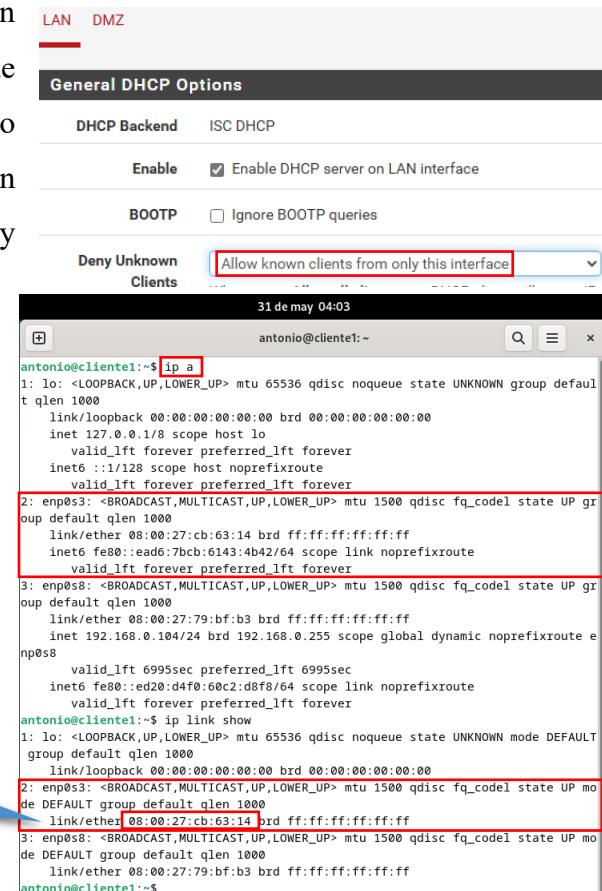


- Una vez que tenemos la dirección MAC agregadas a la tabla o lista inferior, le decimos al servidor pfSense que si recibe una petición para asignar una dirección IP de una MAC que no está en esta tabla, se va a denegar, que no ofrezca direcciones IPs a MAC que no estén en esta tabla, utilizando la opción “Deny Unknown Clients”, “Allow known clients from only this interface”.

- El servidor DHCP únicamente va a asignar direcciones IP de forma dinámica a las direcciones MAC que hay en la tabla inferior.

- Comprobamos con un cliente3⁴ Windows 10 que hemos creado, nos debe dar un error porque la dirección MAC de este equipo no está en la lista.

Aquí está la dirección MAC, podemos ver que no genera IP, porque no está configurada la MAC.



⁴ En esta captura se puede apreciar que pone cliente1, pero es el cliente3, cloné la máquina y no le quité el nombre, ya está actualizado.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

- De esta forma protegemos nuestra red de entregar direcciones IPs dinámicas a clientes que nosotros no conocemos.

6.1.5 Regla 5. Activar reserva IP - MAC mediante DHCP.

El Protocolo de Configuración Dinámica de Host (DHCP) será el único método permitido para incorporar entradas de manera dinámica a la tabla de Protocolo de Resolución de Direcciones (ARP). De este modo, si existen clientes que no están registrados en la lista de dispositivos conocidos y están utilizando una dirección IP estática, no tendrán autorización para acceder a Internet ni a otras redes.

ARP Table					
Interface	IP Address	MAC Address	Hostname	Status	Link Type
WAN	192.168.0.104	08:00:27:79:bf:b3		Expires in 335 seconds	ethernet
WAN	192.168.0.1	e8:1b:69:5f:de:2b		Expires in 1190 seconds	ethernet
WAN	192.168.0.103	08:00:27:f9:f3:d6		Permanent	ethernet
LAN	192.168.1.115	08:00:27:cb:63:14		Expires in 324 seconds	ethernet
DMZ	192.168.2.10	08:00:27:08:28:15		Permanent	ethernet
LAN	192.168.1.30	08:00:27:0f:ab:14	cliente1-debian	Expires in 1118 seconds	ethernet
LAN	192.168.1.10	08:00:27:36:73:a7	pfSense.home.arpa	Permanent	ethernet
DMZ	192.168.2.50	08:00:27:fb:24:29	servidorweb	Expires in 739 seconds	ethernet

- Aquí podemos ver la tabla de mapeo entre las IP, interfaces y direcciones MAC donde el cliente3 se ha conectado. El cliente3 configuró una IP de forma estática y queremos que no se agregue a la tabla ARP como ha ocurrido, la MAC está activa y por eso ha podido acceder a Internet. Queremos que no se permita y que sólo DHCP permita esas entradas.

- No vamos a “Services”, “DHCP Server”, “Other DHCP Options” y marcamos la casilla.

Static ARP **Enable Static ARP entries**
 Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.

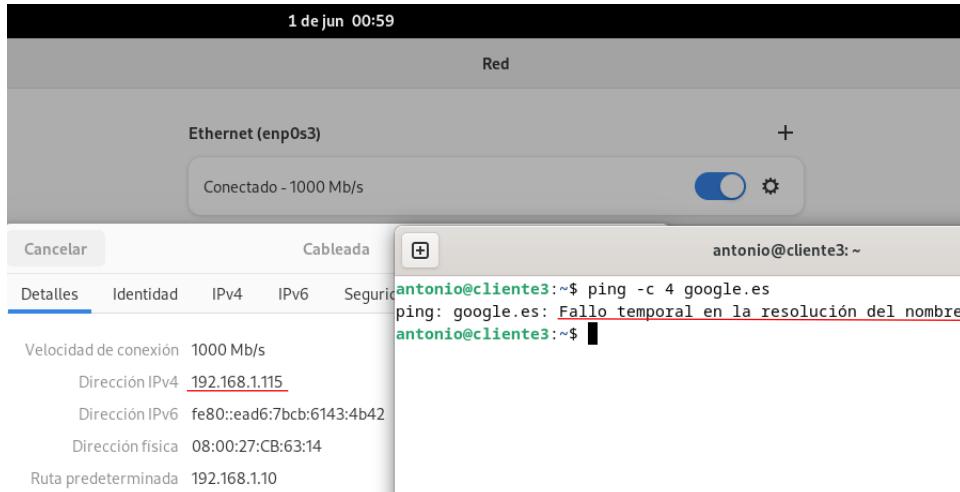
Restringir la comunicación con el firewall únicamente a los hosts listados en asignaciones estáticas que contienen direcciones IP y MAC. Ningún otro host podrá comunicarse con el firewall en esta interfaz. Este comportamiento se aplica incluso cuando el servidor DHCP está deshabilitado.

- Para comprobarlo nos vamos al menú “Diagnostics”, “ARP Table” y observamos que ya no está la IP que configuramos de forma estática en el cliente3.

ARP Table					
Interface	IP Address	MAC Address	Hostname	Status	Link Type
WAN	192.168.0.1	e8:1b:69:5f:de:2b		Expires in 1197 seconds	ethernet
WAN	192.168.0.103	08:00:27:f9:f3:d6		Permanent	ethernet
DMZ	192.168.2.10	08:00:27:08:28:15		Permanent	ethernet
LAN	192.168.1.30	08:00:27:0f:ab:14	cliente1-debian	Expires in 1168 seconds	ethernet
LAN	192.168.1.10	08:00:27:36:73:a7	pfSense.home.arpa	Permanent	ethernet

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

- Podemos apreciar que el equipo cliente3 ya no tiene acceso a Internet.



- Si vamos al cliente1 y hacemos un ping a Google, vemos que sí tiene conexión a Internet.

```
antonio@cliente1:~$ ping -c 4 google.es
PING google.es (142.250.200.67) 56(84) bytes of data.
64 bytes from mad07s24-in-f3.1e100.net (142.250.200.67): icmp_seq=1 ttl=119 time=49.2 ms
64 bytes from mad07s24-in-f3.1e100.net (142.250.200.67): icmp_seq=4 ttl=119 time=44.1 ms

--- google.es ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 3027ms
rtt min/avg/max/mdev = 44.074/46.620/49.166/2.546 ms
antonio@cliente1:~$
```

- Colocamos una IP estática al cliente1 y vemos que ya no tiene comunicación con Internet, estamos obligando a todos los equipos a que utilicen una IP dinámica, siendo DHCP quien genere la entrada en la tabla ARP. El cliente1 ya no tiene permiso para crear una entrada en la tabla ARP.

- Hemos agregado una capa más de seguridad a nuestra configuración DHCP.

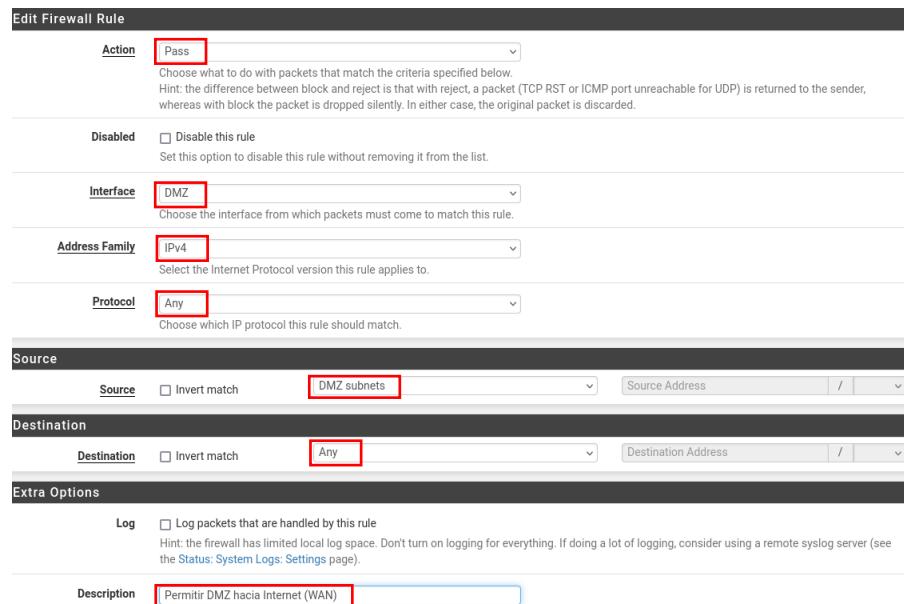
```
antonio@cliente1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 0.0.0.0 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0f:ab:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.118/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::7488:2463:b2af:6f57/64 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:de:ee brd ff:ff:ff:ff:ff:ff
antonio@cliente1:~$ ping -c 4 google.es
ping: google.es: Falló temporal en la resolución del nombre
antonio@cliente1:~$
```

6.1.6 Regla 6. Permitir tráfico DMZ a WAN.

Vamos a permitir y configurar la generación de tráfico desde la DMZ hacia la interfaz 192.168.2.10 dando salida a Internet (WAN).

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

- Configuramos la regla 1 de “permitir”, teniendo en cuenta que cuando creamos la regla de bloqueo, esta debe quedar por encima.



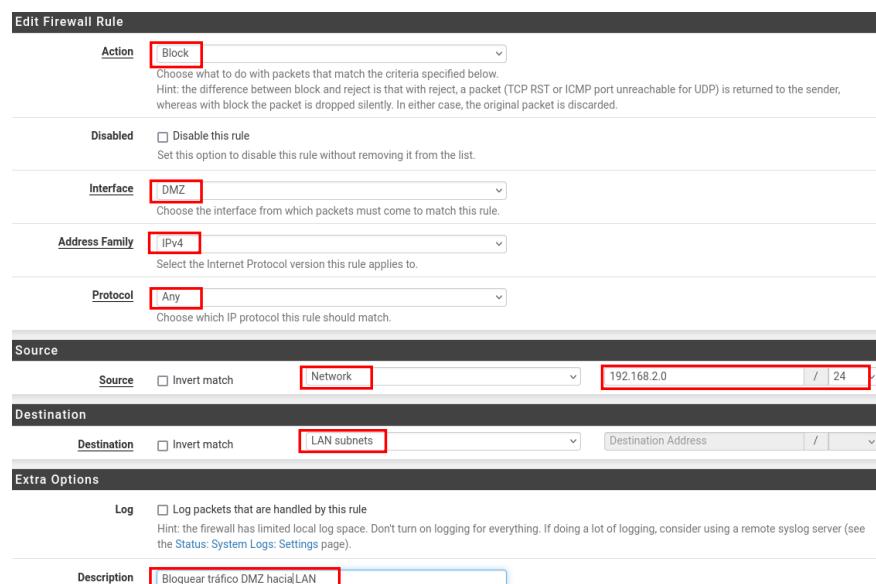
The screenshot shows the 'Edit Firewall Rule' configuration window. The 'Action' dropdown is set to 'Pass'. Other settings include 'Disabled' (unchecked), 'Interface' set to 'DMZ', 'Address Family' set to 'IPv4', and 'Protocol' set to 'Any'. In the 'Source' section, 'Destination' is set to 'Any'. Under 'Extra Options', 'Log' is unchecked. The 'Description' field contains 'Permitir DMZ hacia Internet (WAN)'.

El orden se ha establecido evaluando que regla es más específica y vemos que es la que va hacia la LAN que tiene una única dirección de destino 192.168.1.0/24, mientras que Internet son todas las direcciones IPs.

6.1.7 Regla 7. Bloquear tráfico DMZ a LAN.

Vamos a bloquear cualquier tráfico que vaya desde la DMZ hacia la LAN.

- Desde el cliente1, abrimos el panel de administración de pfSense, menú “Firewall”, “Rules”, “DMZ”.



The screenshot shows the 'Edit Firewall Rule' configuration window. The 'Action' dropdown is set to 'Block'. Other settings include 'Disabled' (unchecked), 'Interface' set to 'DMZ', 'Address Family' set to 'IPv4', and 'Protocol' set to 'Any'. In the 'Source' section, 'Destination' is set to 'LAN subnets'. Under 'Extra Options', 'Log' is unchecked. The 'Description' field contains 'Bloquear tráfico DMZ hacia LAN'.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

- Comprobamos el orden de las reglas establecido.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/3 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✗	0/0 B	IPv4 *	192.168.2.0/24	*	LAN subnets	*	*	none		Bloquear tráfico DMZ hacia LAN	
✓	0/0 B	IPv4 *	DMZ subnets	*	*	*	*	none		Permitir DMZ hacia Internet (WAN)	

- Realizamos la comprobación yéndonos al servidor web que está en la zona DMZ y hacemos un ping hacia la interfaz 192.168.2.10 configurada en el firewall DMZ, obtenemos respuesta.

```

1 de jun 14:51
tenorio@servidorweb:~$ ping -c 4 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=2.90 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=1.64 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=1.49 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=64 time=3.21 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.488/2.308/3.207/0.753 ms
tenorio@servidorweb:~$ ping -c 4 google.es
PING google.es (142.250.184.3) 56(84) bytes of data.
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp_seq=1 ttl=118 time=
34.3 ms
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp_seq=2 ttl=118 time=
31.9 ms
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp_seq=4 ttl=118 time=
32.2 ms

--- google.es ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3019ms
rtt min/avg/max/mdev = 31.904/32.806/34.308/1.069 ms
tenorio@servidorweb:~$ 

```

- Si hacemos un ping a una dirección LAN por ejemplo cliente1 IP 192.168.1.30, comprobamos que no está permitido.

```

1 de jun 14:55
tenorio@servidorweb:~$ ping -c 4 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.

--- 192.168.1.30 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3071ms
tenorio@servidorweb:~$ 

```

- Desde la LAN hacia la DMZ, el cliente1 si tiene permiso para enviar paquetes al servidor web.

```

1 de jun 14:58
antonio@cliente1:~$ ping -c 4 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=1.66 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=1.33 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=64 time=1.22 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 1.220/1.408/1.657/0.161 ms
antonio@cliente1:~$ 

```

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-------------------------------

6.1.8 Regla 8. Permitir tráfico cliente2 LAN a DMZ.

Vamos a dar permiso al cliente2 IP 192.168.1.40, para que a través del protocolo puerto TCP 22 que corresponde a SSH, se conecte al servidor web y pueda hacer configuraciones.

- Nos vamos al panel de administración de pfSense, menú “Firewall”, “Rules”, “LAN”.

Edit Firewall Rule

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.40
<input type="checkbox"/> Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.			
Destination			
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.2.20
Destination Port Range	SSH (22)	From	To
<input type="checkbox"/> Custom		<input type="checkbox"/> Custom	
Description	Permitir cliente2 SSH hacia Servidor Web		

- Comprobamos que la regla se ha establecido correctamente.

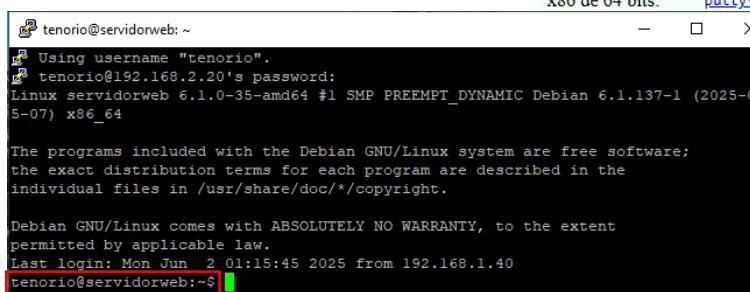
Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/645 KiB	*	*	*	LAN Address	443 80 22	*	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.1.40	*	192.168.2.20	22 (SSH)	*	none	Permitir cliente2 SSH hacia Servidor Web	
<input type="checkbox"/>	✓	1/580 KiB	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

- Para comprobar que el cliente2 se conecte por SSH, nos descargamos la aplicación PuTTY.



	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

- Nos descargamos el instalador haciendo clic en

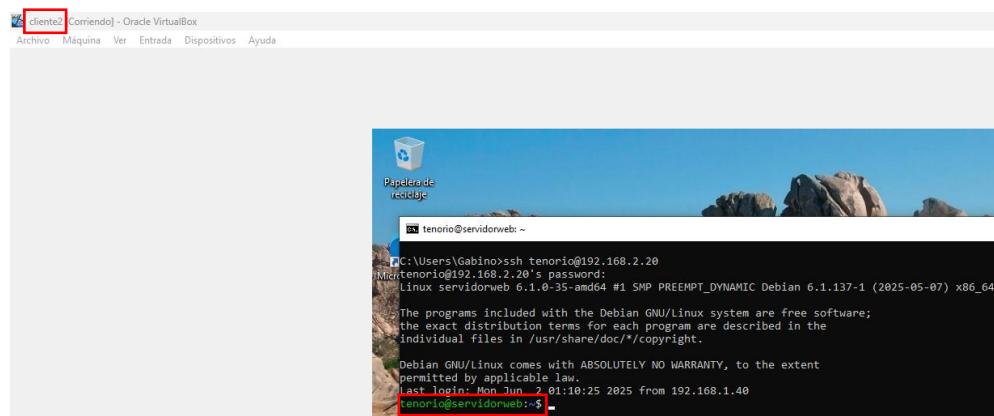


```
tenorio@servidorweb: ~
Using username "tenorio".
tenorio@192.168.2.20's password:
Linux servidorweb 6.1.0-35- amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 2 01:15:45 2025 from 192.168.1.40
tenorio@servidorweb:~$
```

- Comprobamos por terminal el éxito de la conexión.



6.1.9 Regla 9. Permitir tráfico LAN (HTTP) a DMZ.

Vamos a permitir que todos los equipos que están en la LAN puedan acceder a través del puerto HTTP y HTTPS al servidor web que está en la zona DMZ.

Edit Firewall Rule	
Action	Pass
Choose what to do with packets that match the criteria specified below.	
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	TCP
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match <input type="button" value="LAN subnets"/>
<input type="checkbox"/> Display Advanced	
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.	
Destination	
Destination	<input type="checkbox"/> Invert match <input type="button" value="Address or Alias"/>
Destination Port Range	HTTP (80)
From	Custom
To	Custom

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

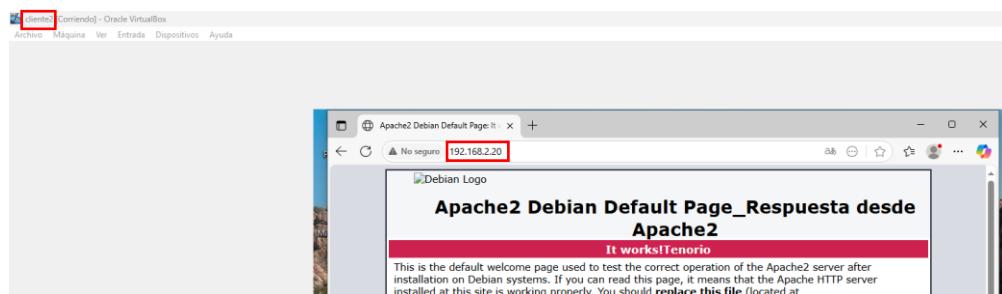
Description

- Ponemos la regla debajo de la que hemos creado anteriormente SSH.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓ 1/748 KIB	*	*	*	LAN Address	443 80 22	*	*	*	Anti-Lockout Rule
✓ 0/0 B	IPv4 TCP	192.168.1.40	*	192.168.2.20	22 (SSH)	*	none	*	Permitir cliente2 SSH hacia Servidor Web
✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.2.20	80 (HTTP)	*	none	*	Permitir LAN a HTTP Servidor Web DMZ
✓ 0/590 KIB	IPv4	*	LAN subnets	*	*	*	none	*	Default allow LAN to any rule
✓ 0/0 B	IPv6	*	LAN subnets	*	*	*	none	*	Default allow LAN IPv6 to any rule

Buttons at the bottom: Add, Delete, Toggle, Copy, Save, Separator.

- Comprobamos desde el cliente2 que el acceso al servidor web en la zona DMZ sea permitido, y como se aprecia nos muestra la página de Apache2.



- Comprobamos también desde el cliente1 y accedemos correctamente.



6.1.10 Regla 10. Permitir tráfico LAN (HTTPS) a DMZ.

Vamos a crear la regla parecida a la anterior para HTTPS.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

Edit Firewall Rule

Action	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="Pass"/> <p>Choose what to do with packets that match the criteria specified below.</p> <p>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="LAN"/> <p>Choose the interface from which packets must come to match this rule.</p>
Address Family	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="IPv4"/> <p>Select the Internet Protocol version this rule applies to.</p>
Protocol	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="TCP"/> <p>Choose which IP protocol this rule should match.</p>

Source					
Source	<input type="checkbox"/> Invert match	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="LAN subnets"/>	Source Address /		
<input type="button" value="Display Advanced"/> <p>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</p>					

Destination					
Destination	<input type="checkbox"/> Invert match	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="Address or Alias"/>	192.168.2.20 /		
Destination Port Range	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="HTTPS (443)"/>	From	Custom	To	Custom
Description <input style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="Permitir LAN a HTTPS Servidor Web DMZ"/>					

- Igual que antes ponemos la regla debajo de la que hemos creado anteriormente HTTP.

Floating	WAN	LAN	DMZ							<input checked="" style="border: 1px solid red; padding: 2px; margin-bottom: 5px;" type="button" value="Apply Changes"/>		
Rules (Drag to Change Order)												
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/819 KIB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	<input type="button" value=""/>	
<input checked="" type="checkbox"/>	0/0 B ≡	IPv4 TCP	192.168.1.40	*	192.168.2.20	22 (SSH)	*	none		Permitir cliente2 SSH hacia Servidor Web	<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value="X"/>	
<input checked="" type="checkbox"/>	0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	80 (HTTP)	*	none		Permitir LAN a HTTP Servidor Web DMZ	<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value="X"/>	
<input checked="" type="checkbox"/>	0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	443 (HTTPS)	*	none		Permitir LAN a HTTPS Servidor Web DMZ	<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value="X"/>	
<input checked="" type="checkbox"/>	5/745 KIB	IPv4	*	*	LAN subnets	*	*	none		Default allow LAN to any rule	<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value="X"/>	
<input checked="" type="checkbox"/>	0/0 B ≡	IPv6	*	*	LAN subnets	*	*	none		Default allow LAN IPv6 to any rule	<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/> <input type="button" value="X"/>	

6.1.11 Regla 11. Bloquear resto de tráfico de LAN a DMZ.

Ahora vamos a crear una regla de bloqueo para ponerla debajo de las dos anteriores, para que los clientes desde la LAN no puedan acceder nada más que a través de los puertos 80 y 443 solamente, el resto bloqueado.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
--	----------------------	---------------------	---	-----------------------------------

Edit Firewall Rule

Action	Block		
Choose what to do with packets that match the criteria specified below.			
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	Any		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	LAN subnets	Source Address
Destination			
Destination	<input type="checkbox"/> Invert match	DMZ subnets	Destination Address
Extra Options			
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		
Description	Bloquear resto tráfico LAN a DMZ (Solo permite 80 y 443)		

- Colocamos la regla de bloqueo debajo de las dos reglas que permiten el tráfico desde la LAN sólo a los puertos 80 HTTP y 443 HTTPS.

Floating	WAN	LAN	DMZ																																																																																								
Rules (Drag to Change Order)																																																																																											
<table border="1"> <thead> <tr> <th>States</th><th>Protocol</th><th>Source</th><th>Port</th><th>Destination</th><th>Port</th><th>Gateway</th><th>Queue</th><th>Schedule</th><th>Description</th><th>Actions</th></tr> </thead> <tbody> <tr> <td>✓ 1/901 KiB</td><td>*</td><td>*</td><td>*</td><td>LAN Address</td><td>443 80 22</td><td>*</td><td>*</td><td>*</td><td>Anti-Lockout Rule</td><td></td></tr> <tr> <td>✓ 0/0 B ≡</td><td>IPv4 TCP</td><td>192.168.1.40</td><td>*</td><td>192.168.2.20</td><td>22 (SSH)</td><td>*</td><td>none</td><td></td><td>Permitir cliente2 SSH hacia Servidor Web</td><td></td></tr> <tr> <td>✓ 0/0 B ≡</td><td>IPv4 TCP</td><td>LAN subnets</td><td>*</td><td>192.168.2.20</td><td>80 (HTTP)</td><td>*</td><td>none</td><td></td><td>Permitir LAN a HTTP Servidor Web DMZ</td><td></td></tr> <tr> <td>✓ 0/0 B ≡</td><td>IPv4 TCP</td><td>LAN subnets</td><td>*</td><td>192.168.2.20</td><td>443 (HTTPS)</td><td>*</td><td>none</td><td></td><td>Permitir LAN a HTTPS Servidor Web DMZ</td><td></td></tr> <tr> <td>✗ 0/0 B ≡</td><td>IPv4 *KiB</td><td>LAN subnets</td><td>*</td><td>DMZ subnets</td><td>*</td><td>*</td><td>none</td><td></td><td>Bloquear resto tráfico LAN a DMZ (Solo permite 80 y 443)</td><td></td></tr> <tr> <td>✓ 0/759 KiB</td><td>IPv4 *KiB</td><td>LAN subnets</td><td>*</td><td>*</td><td>*</td><td>*</td><td>none</td><td></td><td>Default allow LAN to any rule</td><td></td></tr> <tr> <td>✓ 0/0 B</td><td>IPv6 *KiB</td><td>LAN subnets</td><td>*</td><td>*</td><td>*</td><td>*</td><td>none</td><td></td><td>Default allow LAN IPv6 to any rule</td><td></td></tr> </tbody> </table>				States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	✓ 1/901 KiB	*	*	*	LAN Address	443 80 22	*	*	*	Anti-Lockout Rule		✓ 0/0 B ≡	IPv4 TCP	192.168.1.40	*	192.168.2.20	22 (SSH)	*	none		Permitir cliente2 SSH hacia Servidor Web		✓ 0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	80 (HTTP)	*	none		Permitir LAN a HTTP Servidor Web DMZ		✓ 0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	443 (HTTPS)	*	none		Permitir LAN a HTTPS Servidor Web DMZ		✗ 0/0 B ≡	IPv4 *KiB	LAN subnets	*	DMZ subnets	*	*	none		Bloquear resto tráfico LAN a DMZ (Solo permite 80 y 443)		✓ 0/759 KiB	IPv4 *KiB	LAN subnets	*	*	*	*	none		Default allow LAN to any rule		✓ 0/0 B	IPv6 *KiB	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions																																																																																	
✓ 1/901 KiB	*	*	*	LAN Address	443 80 22	*	*	*	Anti-Lockout Rule																																																																																		
✓ 0/0 B ≡	IPv4 TCP	192.168.1.40	*	192.168.2.20	22 (SSH)	*	none		Permitir cliente2 SSH hacia Servidor Web																																																																																		
✓ 0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	80 (HTTP)	*	none		Permitir LAN a HTTP Servidor Web DMZ																																																																																		
✓ 0/0 B ≡	IPv4 TCP	LAN subnets	*	192.168.2.20	443 (HTTPS)	*	none		Permitir LAN a HTTPS Servidor Web DMZ																																																																																		
✗ 0/0 B ≡	IPv4 *KiB	LAN subnets	*	DMZ subnets	*	*	none		Bloquear resto tráfico LAN a DMZ (Solo permite 80 y 443)																																																																																		
✓ 0/759 KiB	IPv4 *KiB	LAN subnets	*	*	*	*	none		Default allow LAN to any rule																																																																																		
✓ 0/0 B	IPv6 *KiB	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule																																																																																		
<div style="text-align: right;"> </div>																																																																																											

6.1.12 Regla 12. Permitir tráfico LAN a WAN.

Esta regla ya viene establecida por defecto por pfSense, permitiendo el tráfico del cualquier equipo desde la LAN a la WAN por IPv4 e IPv6.

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/759 KIB	IPv4 *	LAN subnets	*	*	*	*	none	<u>Default allow LAN to any rule</u>	 
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	<u>Default allow LAN IPv6 to any rule</u>	 

6.1.13 Regla 13. Permitir tráfico WAN a DMZ (HTTP).

Vamos a permitir que los usuarios puedan acceder desde la WAN Internet hacia la DMZ a través de los puertos 80 HTTP y 443 HTTPS al Servidor Web.

Podemos permitir que los usuarios accedan al servidor web o a toda la red DMZ, sólo deberíamos cambiar la opción “Destination”, “DMZ subnets o Address or Alias”.

Destination

<u>Destination</u>	<input type="checkbox"/> Invert match	<input type="text" value="Address or Alias"/>
--------------------	---------------------------------------	---

- Realizamos la configuración accediendo al panel de administración de pfSense.

Edit Firewall Rule

<u>Action</u>	<input type="text" value="Pass"/>
Choose what to do with packets that match the criteria specified below.	
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
<u>Disabled</u>	<input type="checkbox"/> Disable this rule
Set this option to disable this rule without removing it from the list.	
<u>Interface</u>	<input type="text" value="WAN"/>
Choose the interface from which packets must come to match this rule.	
<u>Address Family</u>	<input type="text" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
<u>Protocol</u>	<input type="text" value="TCP"/>
Choose which IP protocol this rule should match.	

Source

<u>Source</u>	<input type="checkbox"/> Invert match	<input type="text" value="Any"/>	<input type="text" value="Source Address"/> / <input type="text"/>
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.			

Destination

<u>Destination</u>	<input type="checkbox"/> Invert match	<input type="text" value="Address or Alias"/>	<input type="text" value="192.168.2.20"/> / <input type="text"/>
<u>Destination Port Range</u>	<input type="text" value="HTTP (80)"/> From <input type="text" value="Custom"/>	<input type="text" value="HTTP (80)"/> To <input type="text" value="Custom"/>	

Extra Options

<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. C the Status: System Logs: Settings page .	
<u>Description</u>	<input type="text" value="Permitir de WAN a DMZ Servidor Web HTTP"/>

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

6.1.14 Regla 14. Permitir tráfico WAN a DMZ (HTTPS).

Vamos a crear la regla parecida a la anterior para HTTPS.

Edit Firewall Rule

Action Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule Set this option to disable this rule without removing it from the list.

Interface Choose the interface from which packets must come to match this rule.

Address Family Select the Internet Protocol version this rule applies to.

Protocol Choose which IP protocol this rule should match.

Source

Source Invert match Source Address /

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match 192.168.2.20 /

Destination Port Range From Custom To Custom

Extra Options

Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Do the Status: System Logs: Settings page.

Description

6.1.15 Regla 15. Bloquear resto de tráfico WAN a DMZ.

Vamos a bloquear el resto de tráfico que no venga por el puerto 80 HTTP y 443 HTTPS, aunque de forma automática se va a bloquear porque sólo estamos permitiendo los puertos anteriores, como estadística podemos ver cuántos paquetes han sido descartados.

	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

Edit Firewall Rule

Action	<input style="border: 1px solid red; padding: 2px; margin-bottom: 5px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="Block"/> <p>Choose what to do with packets that match the criteria specified below.</p> <p>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input style="border: 1px solid red; padding: 2px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="WAN"/> <p>Choose the interface from which packets must come to match this rule.</p>
Address Family	<input style="border: 1px solid red; padding: 2px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="IPv4"/> <p>Select the Internet Protocol version this rule applies to.</p>
Protocol	<input style="border: 1px solid red; padding: 2px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="Any"/> <p>Choose which IP protocol this rule should match.</p>
Source	
Source	<input type="checkbox"/> Invert match <input style="border: 1px solid red; padding: 2px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="Any"/> Source Address /
Destination	
Destination	<input type="checkbox"/> Invert match <input style="border: 1px solid red; padding: 2px; width: 100px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: center; outline: none;" type="button" value="Any"/> Destination Address /
Extra Options	
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).</p>
Description	<input style="border: 1px solid red; width: 600px; height: 25px; font-size: 10px; font-weight: bold; border-radius: 5px; background-color: white; color: black; text-decoration: none; text-align: left; outline: none;" type="text" value="Bloquear resto tráfico WAN a DMZ (Solo permite 80 y 443)"/>

7. Documentación Técnica.

7.1 Manuales de instalación y configuración.

- Documentación oficial PFSENSE.
<https://docs.netgate.com/pfsense/en/latest/>
- Manual instalación y configuración de pfSense.
<https://clockworkcomputerip.blogspot.com/2024/12/pfsense-instalacion.html>
- Configurar pfSense (firewall).
<https://www.redeszone.net/tutoriales/seuridad/pfsense-firewall-profesional-configuration/#388954-principales-caracteristicas>
- Guía Debian 12 GNU/Linux de instalación.
<https://www.debian.org/releases/stable/armel/install.es.pdf>
- El manual del administrador de Debian.
<https://debian-handbook.info/browse/es-ES/stable/sect.installation-steps.html>

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

- Manual de configuración para el servidor OpenSSH en Linux.
<https://seguridad.cicese.mx/dutic/80/Servidor-OpenSSH-en-Linux:-Manual-de- configuraci%C3%B3n-para-m%C3%A1xima-seguridad>

7.2 Tareas Comunes del Administrador.

Como administradores de sistemas es fundamental que nos aseguremos que la infraestructura tecnológica de la empresa funcione de manera segura y eficiente. En este proyecto, se destacan las siguientes tareas operativas como esenciales para una gestión adecuada del entorno.

1. Configuración de Redes.

- Establecer y supervisar las conexiones de red en pfSense para asegurar la comunicación entre las zonas LAN, WAN y DMZ.
- Definir rutas estáticas y ajustar el enrutamiento para mejorar el flujo de tráfico entre los diferentes segmentos de red.

2. Mantenimiento del Cortafuegos.

- Crear y revisar regularmente las reglas del firewall en pfSense para gestionar el tráfico de entrada y salida según las políticas de seguridad.
- Monitorear los registros de tráfico para identificar intentos de acceso no autorizados o actividades sospechosas.

3. Administración de Servicios Web.

- Configurar y gestionar servidores Apache y Nginx, asegurando su correcta integración y asignación de puertos.
- Vigilar el rendimiento de los servicios web y tomar medidas correctivas en caso de fallos o lentitud.

4. Gestión del Servidor FTP y SSH.

- Configurar y probar el servicio `vsftpd` para permitir transferencias seguras mediante FTPS.
- Corregir errores en el archivo de configuración `vsftpd.conf` y abrir puertos en el cortafuegos local (UFW) para permitir conexiones de clientes.
- Configurar el servicio SSH para permitir acceso remoto seguro al servidor, asegurando que solo usuarios autorizados puedan conectarse mediante autenticación basada en claves o contraseñas seguras.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- Supervisar y gestionar las claves SSH para garantizar que solo los usuarios autorizados tengan acceso al servidor.

5. Control de Usuarios y Permisos.

- Crear usuarios en los diferentes sistemas (pfSense, servidor web, FTP), aplicando políticas de contraseñas seguras y asignando los permisos necesarios.
- Supervisar los accesos y modificar credenciales en caso de sospechas de brechas de seguridad.

6. Monitoreo y Análisis de Logs.

- Revisar los registros de eventos del sistema y servicios (logs de pfSense, Apache, Nginx, FTP, etc.) para detectar errores, accesos fallidos o patrones de ataque.
- Automatizar alertas ante eventos críticos mediante herramientas de monitoreo o scripts personalizados.

7. Actualizaciones y Copias de Seguridad.

- Aplicar actualizaciones periódicas del sistema operativo y servicios para corregir vulnerabilidades.
- Programar copias de seguridad de configuraciones y datos críticos, especialmente en pfSense y en el servidor web.

8. Gestión del Ancho de Banda.

- Configurar políticas de limitación o prioridad de ancho de banda en pfSense para garantizar un uso equilibrado de la red entre los distintos servicios y usuarios.

9. Alta Disponibilidad y Redundancia.

- Planificar sistemas de respaldo para pfSense (CARP, failover) y servicios web, asegurando la continuidad del servicio ante posibles fallos.

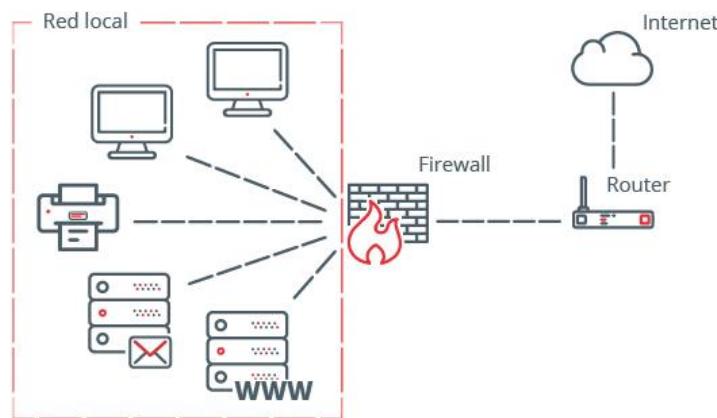
10. Documentación y Registro de Cambios.

- Registrar detalladamente cada cambio de configuración, instalación o intervención realizada en la red o los servicios, para facilitar futuras auditorías o procesos de mantenimiento.

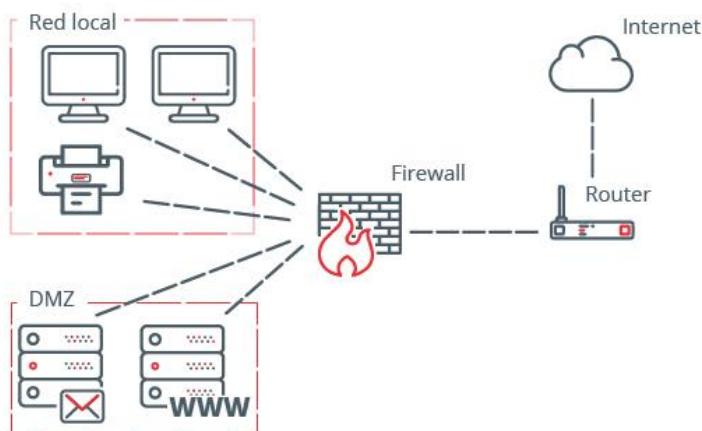
 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

7.3 Esquemas y diagramas de la infraestructura.

En la siguiente imagen se muestra un diagrama de la red de nuestra empresa en sus comienzos, la cual cuenta con un cortafuegos (firewall) pfSense, que filtrará el tráfico de red entrante y saliente por medio de una serie de reglas, las cuales permitirán su paso o las rechazarán.

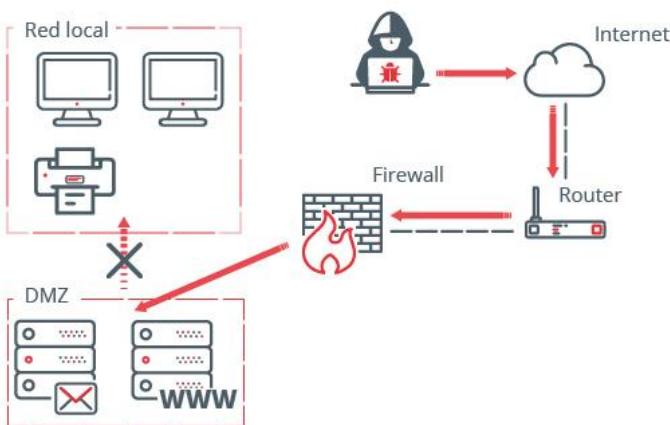


Una zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de la organización, mostrando un ejemplo de nuestra red local con una DMZ.



Por lo general, una DMZ permitirá las conexiones procedentes tanto de Internet, como de la red local de la empresa donde están los equipos de los trabajadores, pero **las conexiones que van desde la DMZ a la red local, no están permitidas**. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad. Si un ciberdelincuente comprometiera un servidor de la zona desmilitarizada, tendría muchos más complicado acceder a la red local de nuestra organización, ya que las conexiones procedentes de la DMZ se encontrarían bloqueadas.

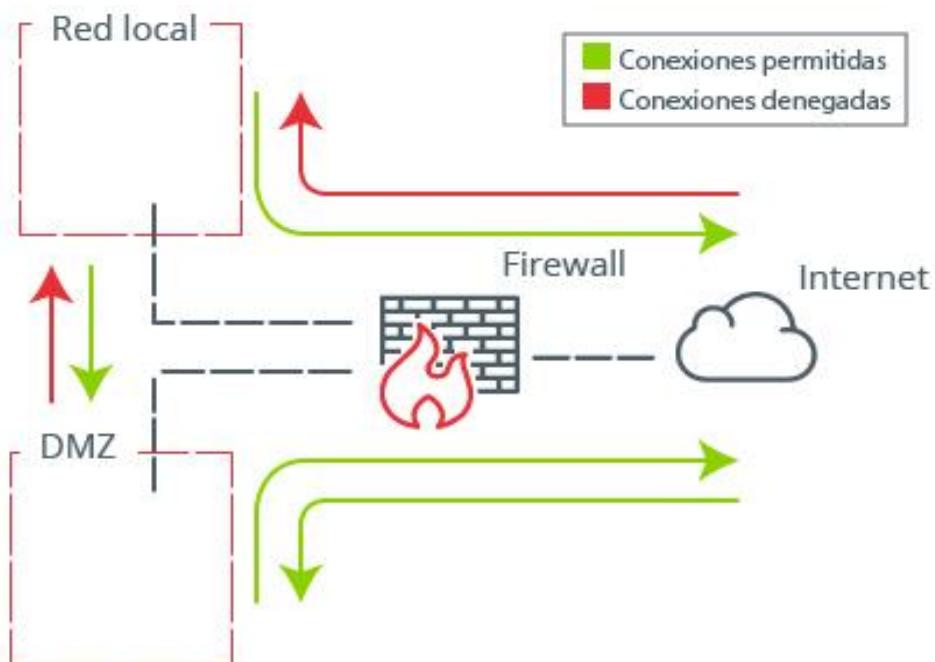
	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo		Proyecto de Administración de sistemas informáticos en red.	



A continuación, se muestra una tabla con el tipo de conexiones recomendables que permitirían o denegarían el firewall dependiendo de su origen y destino.

Configuración básica de un firewall con DMZ

Origen	Destino	Política
Internet	DMZ	Permitido
DMZ	Internet	Permitido
Internet	LAN	Denegado
DMZ	LAN	Denegado
LAN	DMZ	Permitido
LAN	Internet	Permitido



	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

8. Conclusiones y Futuras Mejoras.

8.1 Resumen del proyecto y valoración de los resultados obtenidos.

Este proyecto ha consistido en el diseño e implementación de una red interna segura para una pequeña empresa, utilizando entornos virtualizados con VirtualBox. La infraestructura implementada se basa en tres componentes principales: un cortafuego configurado con pfSense, un servidor web combinado con Apache + Nginx, y dos clientes representando el acceso de dos empleados a los servicios internos de la empresa.

Durante el desarrollo se ha logrado establecer una red funcional, organizada y protegida, en la que se aplican buenas prácticas de seguridad, tales como el filtrado del tráfico, la segmentación de la red y la administración centralizada del acceso. La elección de pfSense como cortafuegos ha demostrado ser acertada por su flexibilidad, capacidad de personalización y amplia gama de herramientas integradas. Del mismo modo, la combinación de Apache y Nginx ha aportado versatilidad, rendimiento y eficiencia al servicio web ofrecido. Los resultados obtenidos han sido satisfactorios, permitiendo comprobar la eficacia de la infraestructura propuesta en un entorno controlado, y validando así su viabilidad para entornos reales de pequeñas empresas.

8.2 Dificultades encontradas y soluciones aplicadas.

Durante el desarrollo del proyecto me he encontrado con diversos obstáculos técnicos que requirieron análisis y resolución. Entre ellos destacan los siguientes:

- **Problema de reinicio pfSense.**

Cuando terminamos la instalación del S.O. de pfSense, tenemos que forzar el cierre de la máquina dándole a cerrar, y después seleccionamos “Apagar la máquina”, parando la VM, porque el procedimiento habitual no realiza el reboot, cuando ponemos exit.
Pag. 28

- **Problemas de enrutamiento y conectividad entre las máquinas virtuales.**

En las fases iniciales fue necesario ajustar la configuración de las interfaces de red en VirtualBox, definiendo correctamente los adaptadores internos y en Adaptador puente para permitir la comunicación entre LAN, WAN y clientes.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- **Configuración del cortafuego pfSense.**

Debido a su amplio conjunto de opciones, fue necesario realizar varias pruebas y ver muchos vídeos para aplicar correctamente las reglas de filtrado, NAT y ruteo. Para ello, he tenido que recurrir a la documentación oficial, páginas web, tutoriales, manuales y foros de soporte comunitario entre otros.

- **Integración de Apache y Nginx.**

Configurar ambos servidores en un mismo entorno requirió definir adecuadamente los archivos de configuración y puertos, y establecer su papel como servidor proxy inverso y servidor de aplicaciones respectivamente.

- **Errores en la configuración del servidor FTP seguro (vsftpd).**

Al establecer la conexión desde el cliente1 al servidor mediante el protocolo FTPS, se encontraron fallos relacionados con el puerto 22 (utilizado por SSH en lugar de FTPS) y configuraciones incorrectas en el archivo vsftpd.conf. Se detectaron errores de escritura, espacios innecesarios y parámetros mal colocados que impedían el correcto funcionamiento del servicio. La solución consistió en revisar cuidadosamente el archivo, validar los parámetros utilizados y consultar la documentación oficial, además de realizar pruebas hasta dar con la solución.

- **Restricciones del cortafuego UFW.**

Fue necesario abrir manualmente los puertos correspondientes para permitir el tráfico de FTPS y otros servicios. Inicialmente, el cortafuego bloqueaba las conexiones entrantes, lo cual impedía la comunicación entre cliente y servidor. Esto se solucionó configurando adecuadamente las reglas de UFW para permitir el tráfico en los puertos utilizados.

- **Error en script de monitorización por variable mal escrita.**

Durante la creación de un script de monitorización para verificar el estado de un servicio, el script no funcionaba correctamente. Tras revisar varias veces la lógica, observé que el problema era una variable mal escrita: la palabra “servicio” aparecía como “sevicio”, omitiendo la letra “r”.

Corregí la variable con la ortografía correcta y el script comenzó a ejecutarse correctamente. Este error verificó la importancia de validar la sintaxis cuidadosamente y de usar herramientas de depuración o ejecución paso a paso.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- **Error de red en la DMZ.**

Durante la configuración del servidor web en la DMZ, al activar el DHCP, la máquina me asignaba una IP de la red **192.168.1.0/24** (LAN) en vez de la **192.168.2.0/24** (DMZ).

Observe revisando, que la máquina virtual estaba conectada por error a la red interna “miredlan” asignada a la **LAN**, en lugar de la red correspondiente a la **DMZ**.

Corregí el adaptador de red en VirtualBox, asignando al servidor la red interna correcta “DMZ”. Al apagar la interfaz y volverla a encender se actualiza la IP, el servidor recibiendo la dirección IP adecuada dentro del rango (100-199) **192.168.2.0/24**. Este fallo me ha hecho ver la importancia de asignar correctamente las redes virtuales cuando uno está trabajando con múltiples subredes y cortafuegos.

- **Error al asignar IP estática en pfSense.**

Durante la asignación de una dirección IP estática al servidor web desde pfSense, se produjo un error al introducir sin darme cuenta una dirección perteneciente a la subred **LAN** (192.168.1.0/24) en lugar de la subred **DMZ** (192.168.2.0/24). El error se produjo al crear la reserva DHCP estática pfSense mostró un aviso indicando que la IP configurada no pertenecía al rango válido de la subred seleccionada. Al revisar el aviso, me di cuenta del error y cambié la asignación de la reserva estática a la interfaz **DMZ**, introduciendo de nuevo los mismos datos con la IP **192.168.2.50**. Esta vez, pfSense aceptó la configuración correctamente. Volvemos a poner de manifiesto la importancia de comprobar cuidadosamente la interfaz asociada al rango DHCP cuando estamos trabajando con múltiples subredes y direcciones IP fijas en entornos segmentados.

- Durante la configuración del servidor, se encontraron y resolvieron varios problemas para asegurar su correcto funcionamiento.

Uno de los problemas detectados fue un **error de sintaxis** en el nuevo archivo de configuración de Nginx, ubicado en **/etc/nginx/sites-available/proxy_apache**. Este error impedía que Nginx se iniciara correctamente, afectando la capacidad del servidor para gestionar las solicitudes de proxy hacia Apache. Al revisar el archivo, se encontró que había espacios no perceptibles a simple vista. Después de corregir este error, se

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

probó la configuración y se reinició Nginx, lo que solucionó el problema y restauró su funcionalidad.

- Otro problema encontrado fue en el **archivo de configuración de SSH**, **/etc/ssh/sshd_config**. Se descubrió que una línea necesaria para permitir el inicio de sesión con contraseña estaba desactivada (comentada), lo que impedía esta forma de autenticación. Además, otra línea tenía un valor incorrecto, configurado como “no” cuando debería haber sido “yes”. Estos errores impedían que el cliente2 se conectara al servidor mediante SSH. Para resolver este problema, se activó la línea necesaria y se corrigió el valor a yes. Luego, se reinició el servicio SSH para aplicar los cambios, permitiendo así que los usuarios pudieran conectarse sin problemas.

Estas dificultades fueron superadas mediante un proceso continuo de prueba y error, apoyado por la documentación técnica, recursos en línea y el uso de comandos de diagnóstico para verificar la conectividad y el estado de los servicios.

8.3 Posibles ampliaciones y mejoras futuras.

A partir de los resultados obtenidos, se proponen varias líneas de mejora que podrían implementarse en futuras versiones de la infraestructura para aumentar su robustez, escalabilidad y funcionalidad:

- **Incorporación de una zona desmilitarizada (DMZ).**
Para incrementar la seguridad, se sugiere implementar una DMZ en la que se aloje el servidor web. Esto permitiría aislar los servicios públicos del resto de la red interna, minimizando los riesgos en caso de ataques desde el exterior.
- **Despliegue de un sistema IDS/IPS (Detección y Prevención de Intrusiones).**
Herramientas como **Snort** o **Suricata** pueden integrarse en pfSense para analizar el tráfico en tiempo real, detectar amenazas y responder ante actividades sospechosas.
- **Implementación de una VPN.**
La instalación de una VPN permitiría el acceso remoto seguro de empleados o administradores, protegiendo las comunicaciones mediante cifrado y autenticación.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

- **Mejora del rendimiento mediante alta disponibilidad.**

Para entornos críticos, sería recomendable aplicar configuraciones de alta disponibilidad (HA) que garanticen el acceso continuo a los servicios, incluso ante fallos de hardware o software.

8.3.1 Incorporación de una Zona Desmilitarizada (DMZ).

La incorporación de una Zona Desmilitarizada (DMZ) es una estrategia clave para mejorar la seguridad de la red al aislar los servicios que están expuestos a Internet del resto de la red interna. La red DMZ servirá como zona intermedia entre la red interna (LAN) y la red externa (WAN), mejorando así la seguridad de la infraestructura.

El objetivo es crear una DMZ para alojar el servidor web y aislarlo de la red interna, permitiéndonos que, si el servidor web se viera comprometido, los atacantes no tuvieran acceso directo a la red LAN, además podríamos mejorar el control de acceso implementando reglas de firewall para controlar el tráfico entre la DMZ, la red interna y la red externa.

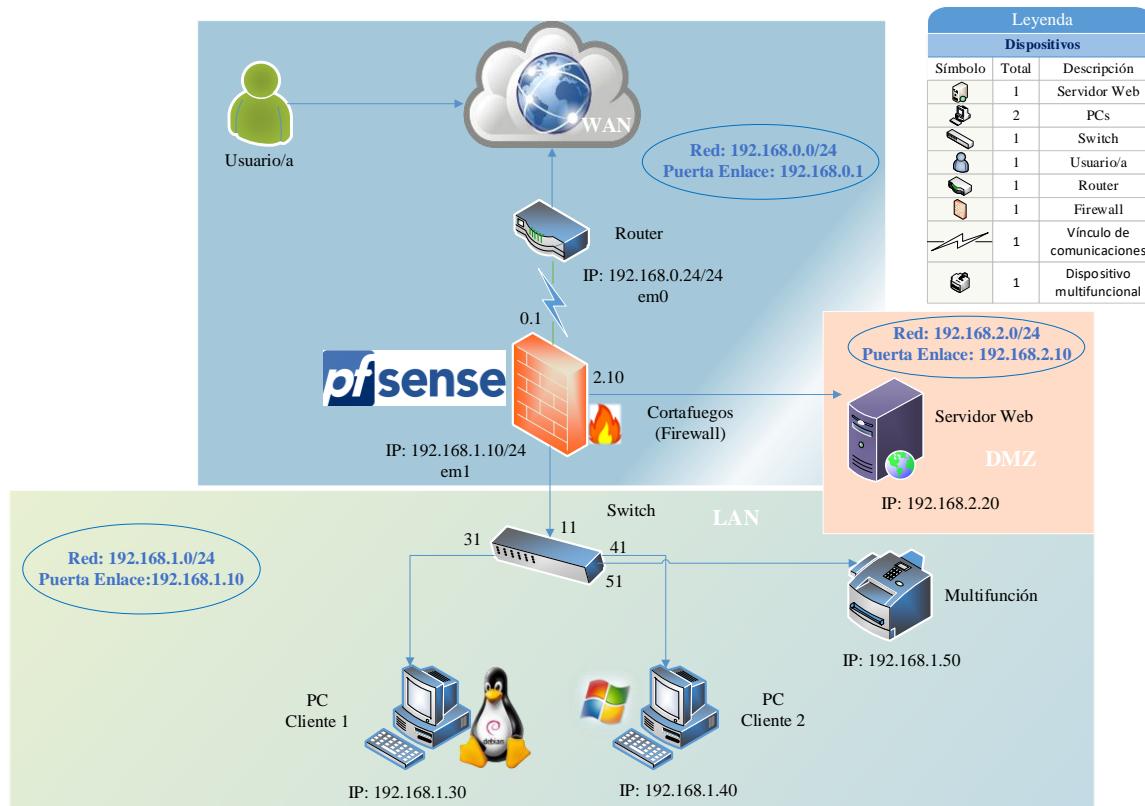
1. Planificación de la red.

- Red Interna (LAN): 192.168.1.0/24
- DMZ: 192.168.2.0/24
- Red Externa (WAN): Conectada a Internet (192.168.0.0/24)

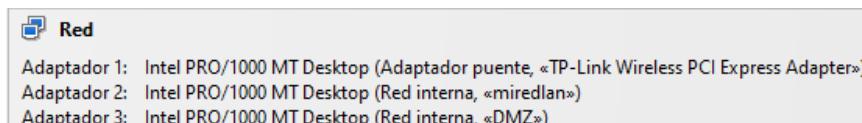
Definimos una nueva subred para la DMZ asignando las siguientes IPs.

- IP del servidor web (dentro de la DMZ): 192.168.2.20/24
- IP de la interfaz DMZ en pfSense: 192.168.2.10/24

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo		Proyecto de Administración de sistemas informáticos en red.	



- Configuramos un nuevo adaptador de red en la VM pfSense, accediendo al menú “Configuración”, “Red”, “Adaptador 3” y lo habilitamos, le damos un nombre a nuestra red interna DMZ.



- Creamos una nueva interfaz en pfSense accediendo a la interfaz web (panel de administración), desde el navegador del anfitrión.

Interfaces		
WAN	1000baseT <full-duplex>	192.168.0.24
LAN	1000baseT <full-duplex>	192.168.1.10
DMZ	1000baseT <full-duplex>	192.168.2.10

8.3.2 Incorporación de un cliente2 Windows.

Realizamos la instalación de un cliente Windows 10 en nuestra red LAN, por varias razones, compatibilidad de software, el soporte de hardware, dispositivos periféricicos, las preferencias del usuario/a, la integración con otros sistemas o servicios, las necesidades de pruebas y

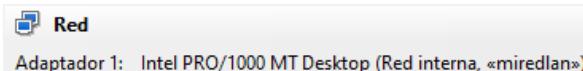
	Dpto. Informática	Ciclo Módulo	CFGS de Administración de Sistemas Informáticos en Red Proyecto de Administración de sistemas informáticos en red.	PROGRAMACIÓN DIDÁCTICA
---	----------------------	---------------------	---	-----------------------------------

desarrollo, el soporte técnico y la utilización en entornos educativos por la familiaridad de las personas con este S.O.

1. Descargamos la iso del sistema operativo de la página oficial de Windows y creamos una nueva VM con los recursos necesarios.



2. Habilitamos el adaptador 1 y lo conectamos en “Red interna”, “miredlan”.

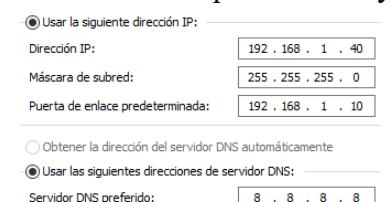


3. Configuramos una dirección IP **192.168.1.30** que esté dentro de nuestra red LAN 192.168.1.0/24. Accedemos al ícono de la barra de tareas clic derecho “Configuración de red e Internet” en “Configuración de red avanzada”, “Cambiar opciones del adaptador”, nos aparece nuestra interfaz de red Ethernet, doble clic “Propiedades” y configuraremos una IP estática y ponemos como puerta de enlace la IP de pfSense (Firewall) 192.168.1.10.



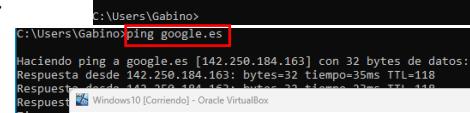
4. Para comprobar la conectividad entre el cliente Windows y pfSense, ponemos en el buscador **cmd** y abrimos “Símbolo de sistema”, ejecutamos el comando obteniendo respuesta.

- ping 192.168.1.10

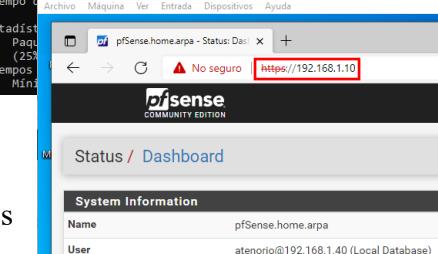


5. Ejecutando el comando siguiente, vemos que también tenemos salida a Internet a través del cortafuego.

- ping google.es



6. Accediendo al navegador Edge y poniendo en su barra de direcciones la IP 192.168.1.10 de pfSense accedemos al panel de administración del Firewall.



7. Podemos realizar una consulta de paquetes ejecutando el comando.

- tracert -d 8.8.8.8

 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

```
C:\Users\Gabinio

```

IP de pfSense y
puerta de enlace del
router de casa WAN

Resto direcciones IPs de
internet y terminamos en
google

8. Instalamos las Guest Additions para mejorar funcionalidades y rendimiento, nos vamos al menú superior “Dispositivos”, “Insertar imagen de CD de los complementos del invitado”, en la parte inferior hacemos doble clic en la carpeta amarilla en la parte izquierda submenú “Este equipo”, doble clic sobre el icono VirtualBox, seguimos el asistente de instalación hasta que finalice y reiniciamos Windows, una vez reiniciado la instalación se completó con éxito.



8.4 Propuesta de solución comercial: BIOS Security Box (BSB).

Como propuesta de evolución del sistema, planteo el desarrollo y comercialización de un dispositivo integral de seguridad bajo el nombre **BIOS Security Box (BSB)**, una solución diseñada por la empresa **Bios Technology Solutions S.L.U.** basada en pfSense y orientada a pequeñas empresas, centros educativos y organismos públicos.



 Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
	Módulo	Proyecto de Administración de sistemas informáticos en red.	

La BSB se presenta como un **firewall de nueva generación**, combinando hardware y software en un único dispositivo que centraliza todas las funcionalidades necesarias para proteger una red corporativa, entre ellas:

- Cortafuegos avanzados con sistema de filtrado de contenidos.
- Análisis antivirus en tiempo real del tráfico de red.
- Balanceo y gestión del ancho de banda entre diferentes líneas (fibra óptica, ADSL, radioenlaces...).
- Tecnología proxy para ahorrar ancho de banda y optimizar el tráfico repetitivo.
- Control de usuarios y contenidos desde cualquier ubicación.
- Sistema de detección y prevención de intrusiones (IDS/IPS).
- Soporte para configuración en alta disponibilidad.
- Portal cautivo para mejorar el control de acceso a Internet.

Al integrar todas estas funcionalidades en un solo equipo, **la BSB reduce significativamente los costes frente a soluciones independientes**, al mismo tiempo que ofrece una administración centralizada y accesible.



Esta solución se alinea con las tendencias actuales de seguridad y podría suponer una evolución lógica del presente proyecto, permitiendo su implementación real en entornos empresariales sin necesidad de conocimientos técnicos avanzados por parte del usuario final.

Enlace a descarga de documentación promocional.

<https://bios-ts.es/home/bios-security-box/>

8.5 Aprendizaje personal y profesional.

La realización de este proyecto ha supuesto para mí una experiencia enriquecedora e inolvidable tanto a nivel personal como profesional. A lo largo del desarrollo he consolidado

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

y ampliado conocimientos claves en administración de redes, seguridad informática, virtualización de sistemas y servicios de red, permitiendo aplicar de forma práctica lo aprendido durante el ciclo formativo de Administración de Sistemas Informáticos en Red (ASIR).

Uno de los aprendizajes más destacados ha sido la planificación e implementación de una red segura y funcional, integrando elementos como el cortafuego pfSense, servidores web (Apache y Nginx), control de acceso y gestión de tráfico. Este proceso ha requerido una comprensión detallada del funcionamiento de los protocolos de red, de las políticas de seguridad, y de la necesidad de segmentar adecuadamente la red interna para proteger los activos críticos de la empresa (hardware y software).

Asimismo, se han reforzado competencias en resolución de problemas técnicos, como los errores de configuración en servicios como vsftpd, fallos de conexión por puertos bloqueados, o scripts que no funcionaban correctamente por errores de sintaxis. Estos desafíos han fomentado una actitud proactiva, paciente y metódica para analizar errores, consultar documentación oficial y aplicar soluciones eficaces.

También ha sido clave la mejora de habilidades en el uso de herramientas de administración y monitorización, y en la aplicación de buenas prácticas de seguridad como la creación de reglas de cortafuegos, gestión de servicios críticos, y posibles futuras implementaciones de IDS/IPS y VPN.

Desde una perspectiva profesional, este proyecto ha permitido experimentar un entorno de trabajo similar al real, donde es necesario no solo tener conocimientos técnicos, sino también saber documentar cada proceso, tomar decisiones justificadas y prever futuras ampliaciones o mejoras. Todo ello ha contribuido a fortalecer la capacidad de análisis, organización y comunicación técnica, aspectos fundamentales en el ejercicio profesional como administrador de sistemas.

En definitiva, el proyecto ha representado una oportunidad para madurar como técnico, afianzar la vocación en el ámbito de la ciberseguridad y adquirir una visión más integral de las infraestructuras de red en entornos empresariales.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

9. Webgrafía.

9.1 Fuentes utilizadas.

9.1.1 Páginas webs y vídeos.

- Instalar pfSense en ZFS.
<https://dcseguridad.es/pfsense-en-zfs-y-ampliar-swap-el-mejor-sistema-de-archivos/>
- Información sobre la descarga de medios de instalación pfSense.
<https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html>
- Curso pfSense.
<https://www.youtube.com/@WilmerAlmazan>
- Debian entornos gráficos Linux.
<https://www.youtube.com/watch?v=7X8l71eNt20&t=10s>
- Diferencias entre Apache y Nginx.
<https://marketersgroup.es/diferencias-entre-apache-y-nginx/>
- Cómo utilizar el comando ping para la solución de problemas de red.
<https://blog.invigate.com/es/comando-ping>
- Protocolo Secure Shell (SSH).
<https://www.cloudflare.com/es-es/learning/access-management/what-is-ssh/>
- Protocolo SFTP.
<https://www.arsys.es/blog/sftp>
- Configurar servidor FTP en Linux.
<https://www.youtube.com/watch?v=okeWIOZBroA&t=170s>
- Configurar DNS en Debian 12.
https://www.youtube.com/watch?v=xk_h3MV684M&t=20s
- DMZ.
<https://www.incibe.es/empresas/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>

9.1.2 Tutoriales y descarga de ficheros de instalación.

- Tutorial de instalación de Debian 2019.
<https://blog.redigit.es/tutorial-de-instalacion-para-debian/>
- Instalar Apache con Nginx como proxy inverso.

	Dpto. Informática	Ciclo	CFGS de Administración de Sistemas Informáticos en Red	PROGRAMACIÓN DIDÁCTICA
		Módulo	Proyecto de Administración de sistemas informáticos en red.	

<https://howtoforge.es/como-instalar-apache-con-nginx-como-proxy-inverso-en-ubuntu-22-04/>

- Descargar e instalar VirtualBox en Windows.
<https://www.youtube.com/watch?v=3EpWqt8q9sA&t=6s> (vídeo ilustrativo).
- Descarga_pfSense 2.7.2 (Versión utilizada gratuita).
<https://www.pfsense.org/download/>
- Descarga_Debian 12.10.0
<https://www.debian.org/download.es.html>
<https://www.debian.org/distrib/netinst.en.html>
- Descarga_VirtualBox 7.1.6
<https://www.oracle.com/es/virtualization/technologies/vm/downloads/virtualbox-downloads.html>
- Descarga_Apache 2.4.63
<https://httpd.apache.org/download.cgi>
- Descarga_Nginx 1.26.3
<https://nginx.org/en/download.html>
- Tutoriales: Guía completa sobre WordPress.
<https://www.hostinger.com/mx/tutoriales/>
- Guía de nmap (Mapeador de redes).
<https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/>
- Blog informático relacionado con la enseñanza en los Ciclos Formativos.
<https://clockworkcomputerip.blogspot.com/>