Universidad Nacional Autónoma de Nicaragua

UNAN-León

Área de Conocimiento Ciencias y Tecnología

Área específica Ingeniería en Sistemas de Información

Ingeniería en Telemática

"Solución de Seguridad Perimetral en Pequeñas y Medianas Empresas: Un Enfoque Integral para la ciudad de León"

Tesis para optar al título de Ingeniero en Telemática

Autores:

- Tec. Julian Alejandro Campos Mairena.
- Tec. Josué Alexander López López.

Tutor:

- MSc. Álvaro Rafael Altamirano Osorio.

León, Nicaragua enero de 2025

2025: 46/19 ¡Siempre más allá! ¡Avanzando en la revolución!

Universidad Nacional Autónoma de Nicaragua

UNAN-León

Área de Conocimiento Ciencias y Tecnología

Área específica Ingeniería en Sistemas de Información

Ingeniería en Telemática

Protocolo de Monografía

"Solución de Seguridad Perimetral en Pequeñas y Medianas Empresas: Un Enfoque Integral para la ciudad de León"

Tesis para optar al título de Ingeniero en Telemática

Autores:

- Tec. Julian Alejandro Campos Mairena. _____
- Tec. Josué Alexander López López. _____

Tutor:

- MSc. Álvaro Rafael Altamirano Osorio. _____

León, Nicaragua enero de 2025

2025: 46/19 ¡Siempre más allá! ¡Avanzando en la revolución!

Resumen

La solución propuesta de seguridad perimetral, en organizaciones de pequeñas y medianas empresas, un enfoque integral para la ciudad de León.

La falta de conocimiento sobre el tema de seguridad informática, seguridad perimetral, seguridad de la información y ciberseguridad provoca que las pequeñas y medianas empresas no apliquen de forma eficiente un buen muro perimetral, para prevenir una serie de brechas de seguridad que presentan. Esto radica en una poca seguridad o seguridad nula implementada.

Nuestra guía es una solución de seguridad perimetral básica en consecuencia está diseñada, administrada y creada con softwares open source (Código abierto), con licencias de distribución y utilización de open source que nos permiten minimizar en gran medida el costo de compras en licencias de softwares o hardware dedicado a la seguridad perimetral. Por ende, esta solución de seguridad perimetral está orientada a organizaciones de pequeñas y medianas escalas, donde la seguridad informática no es la prioridad o bien, no hay recursos o presupuesto para brindar una solución más robusta en seguridad perimetral.

Dedicatoria

A Dios por ser el inspirador y darnos fuerza para continuar en este proceso y lograr obtener una de nuestras metas más deseadas.

A nuestros padres y familia por su amor, su comprensión, paciencia y sacrificios en todos estos años de estudios, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en los que somos, dedicamos a ustedes esta meta.

Agradecimiento

A Dios sobre todas las cosas porque él ha estado con nosotros en todo momento llenándonos de sabiduría para que logremos culminar nuestra Ingeniería.

A nuestros padres porque ellos han sido el motor que impulsan nuestras metas, quienes estuvieron siempre a nuestro lado en los días y noches más difíciles, brindándonos su apoyo incondicional y por motivarnos a seguir siempre adelante, por confiar y tener fe en nosotros.

A nuestro tutor Msc Álvaro Rafael Altamirano Osorio quien nos compartió sus conocimientos y nos dirigió en la realización de nuestra tesis

Índice

1. Introducción

La seguridad perimetral es un tema crucial para las Pequeñas y Medianas Empresas (PYMES), puesto que son un objetivo atractivo para los ciberdelincuentes, dado que a menudo tienen recursos limitados para invertir en ciberseguridad y pueden ser más vulnerables a los ataques cibernéticos. Las PYMES tienen la responsabilidad de proteger los datos de sus clientes, proveedores y empleados. En este sentido, es importante contar con dispositivos de seguridad perimetral para prevenir y mitigar los riesgos asociados a la seguridad informática.

Diversos estudios y expertos en ciberseguridad han señalado la importancia de la seguridad perimetral para las PYMES. Por ejemplo, según un informe de la consultora PwC, las PYMES son el sector más vulnerable a los ciberataques, ya que a menudo no cuentan con los recursos necesarios para protegerse adecuadamente (PwC, 2017). Por su parte, un estudio de la empresa de seguridad informática Kaspersky Lab encontró que el 54% de las PYMES encuestadas sufrieron al menos un ataque cibernético en el último año (Kaspersky Lab, 2019). Nicaragua no ha sido la excepción ya que, según un informe de la Comisión Interamericana de Telecomunicaciones (CITEL), Nicaragua tiene un bajo nivel de madurez en materia de ciberseguridad, lo que aumenta el riesgo de ataques informáticos.

Asimismo, el cumplimiento de las regulaciones y normas en materia de protección de datos también es un aspecto relevante para las PYMES en Nicaragua. La Ley de Protección de Datos Personales establece que todas las empresas que manejen datos personales deben contar con medidas de seguridad adecuadas para garantizar la privacidad y la integridad de esta información (Asamblea Nacional de Nicaragua, 2017

Es por ello, que esta investigación es importante para proponer y dar solución a la brecha de seguridad que las PYMES puedan estar expuestas, exclusivamente en la ciudad de León, Nicaragua.

2. Antecedentes

En la ciudad de León, Nicaragua, las pequeñas y medianas empresas (PYMES) desempeñan un rol vital en la economía local, generando empleo y contribuyendo al crecimiento económico de la ciudad. Sin embargo, es evidente que estas pequeñas y medianas empresas carecen de estrategias efectivas en ciberseguridad para protegerse de la ciberdelincuencia y salvaguardar sus activos digitales. La falta de seguridad en su perímetro de red se traduce en una vulnerabilidad significativa ante amenazas cibernéticas, como malware, ataques de phishing, denegación de los servicios, ransomware, entre otros.

Con la necesidad de salvaguardar los activos digitales y la privacidad de los datos se ha generado la motivación detrás de este tema de monografía. “De acuerdo con el Informe Global de Ciberdelincuencia publicado por SEON” (Seon, 2023). una empresa líder en la prevención de delitos financieros en línea, que analiza 93 países, Nicaragua ocupa el décimo lugar en el ranking de riesgo cibernético, con una puntuación de 26.29 sobre 100. El reporte indica que los países que ofrecen menos protección contra la ciberdelincuencia y una legislación muy débil o incluso ninguna, son los que más riesgo corren a la hora de procesar transacciones sensibles. Este análisis se basa en datos combinados de tres importantes autoridades de ciberseguridad: el Índice Nacional de Ciberseguridad (NCSI), actualizado en tiempo real, el Índice Global de Ciberseguridad (GCI) de 2020 y el Índice de Exposición a la Ciberseguridad (CEI) de 2020.

Con la actualización más reciente en 2023, el índice de seguridad cibernética de Nicaragua se sitúa en 29.87 puntos sobre 100, lo que la coloca en la posición 107 de 160 a nivel mundial según el Índice Nacional de Ciberseguridad (NCSI). Los primeros tres meses del 2024 han registrado más de 2,500 infecciones cibernéticas diarias en el país, comprometiendo la seguridad y la información de los usuarios en línea, según datos proporcionados por Kaspersky. Nicaragua se encuentra en el puesto 136 en la lista de los países más atacados según estadísticas de Kaspersky.

3. Planteamiento Del Problema

Las pequeñas y medianas empresas en la ciudad de León se enfrentan a crecientes amenazas de ataques cibernéticos debido a la falta de una adecuada seguridad perimetral. A medida que las PYMES dependen cada vez más de la tecnología para llevar a cabo sus operaciones comerciales, se vuelven más vulnerables a diversas formas de intrusiones y violaciones de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de sus activos y datos críticos.

La falta de recursos financieros y conocimientos especializados en ciberseguridad dentro de las PYMES de la ciudad de León limita la capacidad de implementar y mantener soluciones de seguridad perimetral efectivas. Esto se ve agravado por la falta de conciencia sobre la importancia de la seguridad perimetral y la percepción errónea de que solo las grandes empresas son blancos de ataques cibernéticos.

Como resultado, las PYMES en la ciudad León enfrentan una serie de desafíos en seguridad de sus redes, incluyendo la falta de protección contra malware, ataques de denegación de servicio (DDoS), intrusiones no autorizadas y robo de datos. Estos ataques pueden tener consecuencias devastadoras, incluyendo la pérdida de ingresos, daño a la reputación, sanciones legales y, en casos extremos, la interrupción completa de las operaciones comerciales.

Por lo tanto, es crucial abordar este problema de la seguridad perimetral en las PYMES de la ciudad de León para garantizar la protección y la continuidad de sus operaciones comerciales. Se necesita urgentemente una solución integral y personalizada que sea accesible y práctica para las PYMES, teniendo en cuenta sus limitaciones de recursos y conocimientos.

1. ¿Como se podría brindar una solución de Ciberseguridad aplicando la tecnología de seguridad de redes orientada a las PYMES en la ciudad de León?
2. ¿Cómo se pueden integrar tecnologías de seguridad de red accesibles y eficaces, teniendo en cuenta los recursos limitados y la experiencia técnica de las PYMES en la ciudad de León, para garantizar la protección de su infraestructura digital?
3. ¿Cuáles son los principales desafíos para capacitar al personal de las PYMES en la ciudad de León, sobre buenas prácticas de seguridad cibernética?
4. ¿Qué herramientas y estrategias pueden implementarse para monitorear y mejorar continuamente la postura de ciberseguridad en las PYMES de León?
5. ¿Cuáles son los principales riesgos y amenazas de ciberseguridad que enfrentan las PYMES en la ciudad de León, Nicaragua?

4. Justificación

La falta de medidas adecuadas de seguridad perimetral en las pequeñas y medianas empresas representa un riesgo potencial que podría tener consecuencias devastadoras en la continuidad del negocio y la confianza de sus clientes. En este contexto, es fundamental considerar soluciones de seguridad perimetral, como los firewalls, que desempeñan un papel crucial en la protección del perímetro de la red. Por ello, nuestra ilusión es presentar un manual práctico que permita a las PYMES de la ciudad de León adoptar medidas de seguridad perimetral eficaces, ofreciendo una defensa sólida contra las amenazas cibernéticas en constante evolución a un costo reducido.

La seguridad perimetral se ha convertido en una prioridad para las organizaciones de todos los tamaños, pero las PYMES en particular a menudo carecen de los recursos y la experiencia necesaria para implementar y mantener soluciones de seguridad adecuadas por falta de presupuesto, conocimiento o personal no capacitado. Esta falta de protección adecuada puede exponer a estas pequeñas empresas a una serie de riesgos, incluyendo ataques cibernéticos, pérdida de datos, interrupción del servicio y daño a la reputación.

Por lo tanto, esta investigación se enfoca en optimizar una solución de seguridad perimetral que integre todos los aspectos relevantes en seguridad perimetral específicamente diseñada para satisfacer las necesidades y limitaciones de las PYMES en la ciudad de León.

Además, al abordar esta problemática de forma local podría esta investigación tener un impacto significativo en las PYMES de la ciudad de León, alentando la adopción de mejores prácticas de seguridad y fortaleciendo su infraestructura digital. En última instancia, se espera que la estrategia de seguridad y recomendaciones dadas en esta investigación no solo beneficien a las organizaciones locales, sino que también sirvan como un modelo para otras PYMES en diferentes ciudades de nuestro

5. Objetivos

5.1 Objetivo General

Desarrollar una estrategia de seguridad de redes y brindar una solución integral de seguridad perimetral adaptada a las necesidades y limitaciones de las pequeñas y medianas empresas en la ciudad de León, Nicaragua, con el fin de mejorar su protección contra amenazas cibernéticas y fortalecer su resiliencia organizativa.

5.2 Objetivos Específicos

1) Diseñar una solución de seguridad perimetral que integre tecnologías de seguridad perimetral y las mejores prácticas de seguridad, teniendo en cuenta los recursos limitados y la experiencia técnica de las PYMES en la ciudad de León.
2) Investigar y seleccionar las tecnologías y herramientas de seguridad perimetral más adecuadas para las PYMES en función de sus necesidades específicas y su capacidad financiera.
3) Crear un manual de configuración para el Firewall, abarcando desde los fundamentos hasta las políticas de seguridad, con el objetivo de proporcionar una guía clara y práctica para su implementación efectiva en una PYME.
4) Proporcionar recomendaciones para la mejora continua de la seguridad perimetral en las PYMES de León, basadas en los resultados obtenidos durante la investigación y la implementación de la solución de seguridad perimetral.

6. Marco Teórico

6.1 Conceptos Básicos de Red y Seguridad informática

- **Internet**

Internet es un sistema de red conectado globalmente que ayuda a la comunicación y los servicios de datos a través de una extensa colección de redes privadas, públicas, empresariales, académicas y gubernamentales. Sirve como una infraestructura virtual que conecta millones de computadoras y dispositivos electrónicos en todo el mundo, lo que permite a los usuarios intercambiar información sin problemas.

Internet ha revolucionado la informática y las comunicaciones como ninguna otra cosa. La invención del telégrafo, el teléfono, la radio y el ordenador sentó las bases para esta integración de funcionalidades sin precedentes. Internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica. Internet representa uno de los ejemplos más exitosos de los beneficios de una inversión y un compromiso continuos en el campo de la investigación y el desarrollo de la infraestructura de la información. Internet Society. (2023, 11 octubre).

- **Red LAN**

Se conoce como red LAN (siglas del inglés: Local Área Network, que traduce Red de Área Local) a una red informática cuyo alcance se limita a un espacio físico reducido, como una casa, un departamento o a lo sumo un edificio.

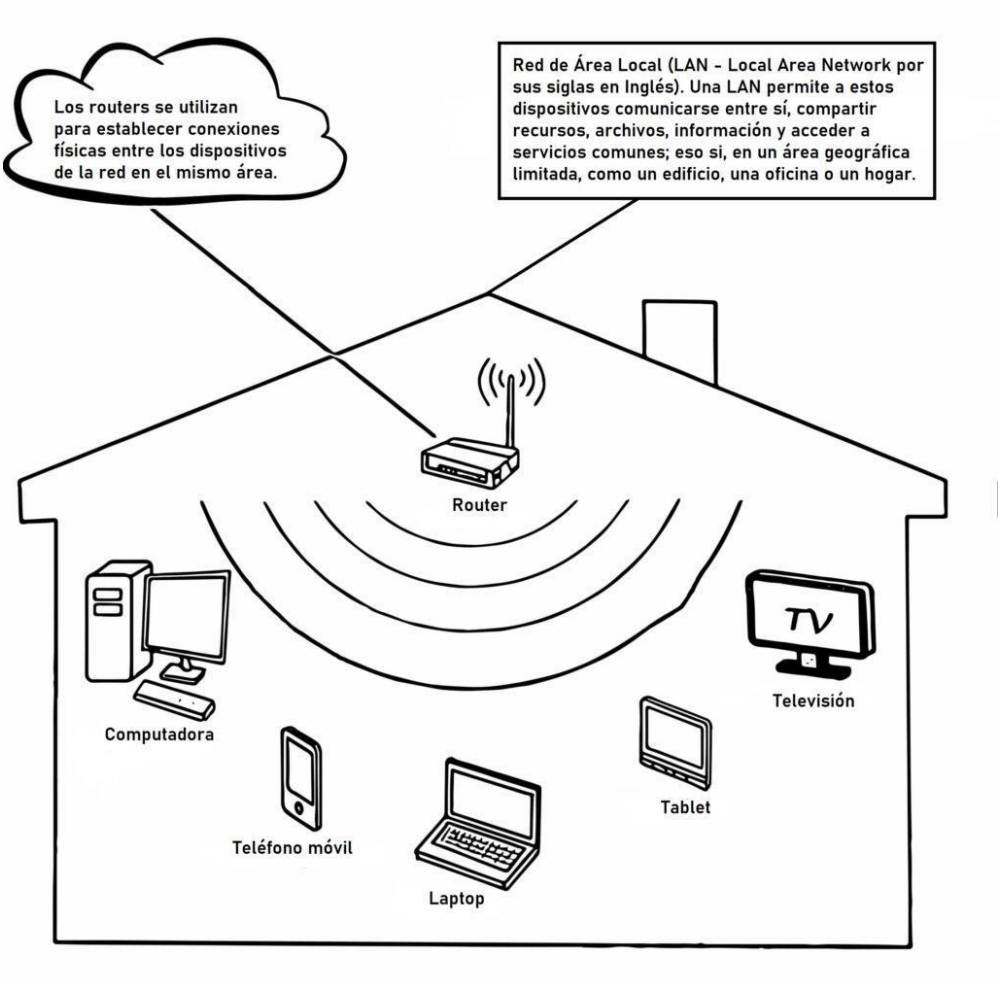
A través de una red LAN pueden compartirse recursos entre varias computadoras y aparatos informáticos (como teléfonos celulares, tabletas, etc.), tales como periféricos (impresoras, proyectores, etc.), información almacenada en el servidor (o en

los computadores conectados) e incluso puntos de acceso a la Internet, a pesar de hallarse en habitaciones o incluso pisos distintos.

Este tipo de redes son de uso común y cotidiano en negocios, empresas y hogares, pudiendo presentar una topología de red distinta de acuerdo con las necesidades específicas de la red. Equipo editorial, Etecé. (2023, 19 noviembre).

Figura 1

Ejemplo de Red LAN



- **Red WAN**

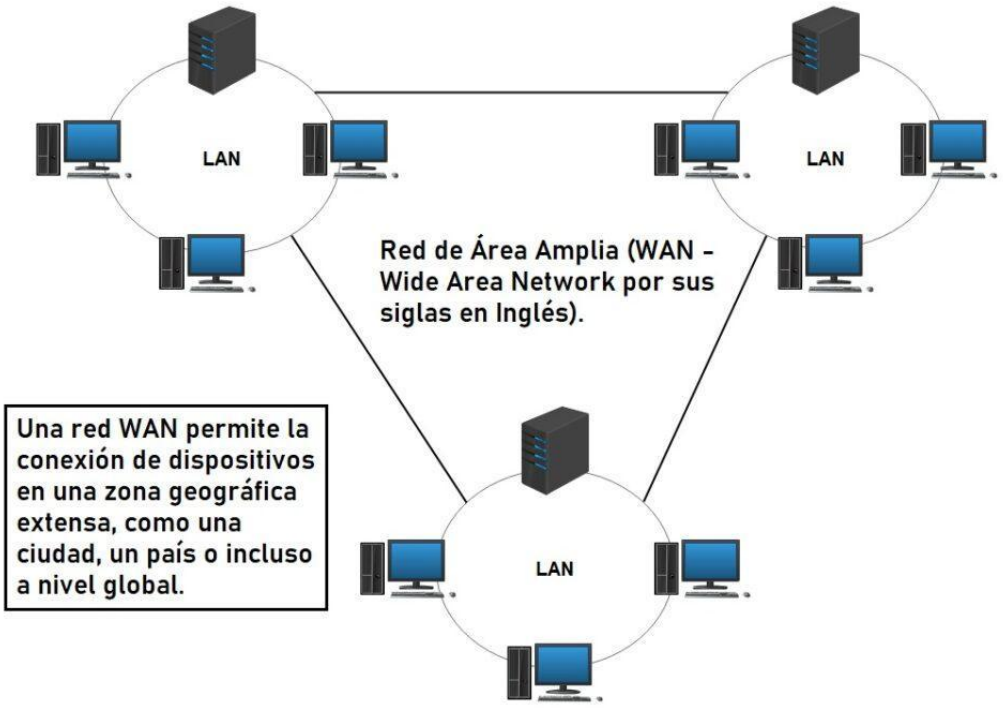
Las redes WAN (Red de área amplia) son un tipo de red que permite la conexión de dispositivos en una zona geográfica extensa, como una ciudad, un país o incluso a nivel global.

Su función principal es la interconexión de dispositivos y redes de distintas ubicaciones geográficas, permitiendo la transferencia de información, voz y video entre ellos.

A diferencia de las redes LAN, que cubren un área geográfica reducida, las redes WAN utilizan tecnologías de transmisión de datos que les permiten abarcar grandes distancias. Andresredesinformaticas. (2023b, marzo 11).

Figura 2

Ejemplo Red WAN



- **Modem**

Un módem es un dispositivo de telecomunicaciones que se encarga de enviar y recibir datos utilizando una línea telefónica o de banda ancha. Su nombre proviene de la combinación de las palabras modulador y demodulador.

Su funcionamiento consiste en tomar las señales digitales provenientes de la computadora y convertirlas en señales analógicas que puedan ser transmitidas por la línea de comunicación. De igual manera, cuando recibe señales analógicas, las transforma nuevamente en señales digitales para que la computadora pueda procesarlas.

Existen diversas variedades de módems, como por ejemplo módems de cable, módems DSL y módems satelitales. Cada uno de ellos es utilizado para conectarse a un tipo específico de línea de comunicación. Upplasencia. (2024, 13 marzo).

- **Router**

Un router es un dispositivo que conecta dos o más redes o subredes de conmutación de paquetes. Cumple dos funciones principales: administrar el tráfico entre estas redes mediante el reenvío de paquetes de datos a sus direcciones IP previstas y permitir que varios dispositivos utilizan la misma conexión a Internet.

Hay varios tipos de enrutadores, pero la mayoría de los enrutadores pasan datos entre LAN (redes de área local) y WAN (redes de área amplia). Una LAN es un grupo de dispositivos conectados restringidos a un área geográfica específica. Una LAN generalmente requiere un solo enrutador.

Gran contenedor para programas grandes o el SO: Al cargar grandes programas o SO en un archivo ISO, estos SO se pueden descargar/montar/grabar en un disco óptico sin esfuerzo. Connect, Protect and Build Everywhere | Cloudflare. (s. f.).

- **Dirección IP**

Una IP (Internet Protocol) es una dirección única que identifica a un dispositivo en una red. Esta se encuentra formada por cuatro números de hasta tres cifras separados por un punto, comprendidos cada uno de ellos entre 0 y 255 (ejemplo:192.168.10.3). Además, es importante tener en cuenta que pueden ser de varios tipos (pública, privada, fija y dinámica).

- **Tipos de direcciones IP:**

- **IP Pública**: Asignada por el ISP, identifica de forma única la conexión a Internet de un dispositivo. Debe ser única y no se puede repetir.
- **IP Privada:** Utilizada para identificar dispositivos dentro de una red local (LAN). Puede repetirse en redes independientes y no se conecta directamente a Internet, evitando conflictos de direcciones.
- **IP Dinámica:** Cambia periódicamente y tiene una duración limitada. Ofrece mayor privacidad, reduce el riesgo de ataques y es más económica, ideal para la mayoría de los consumidores.
- **IP Estática**: Asignada manualmente, permanece fija para un dispositivo. Permite una comunicación más rápida, pero tiene un mayor costo y riesgo de seguridad, siendo más adecuada para empresas con sitios web o conexiones VPN. Limones, E. (2021b, julio 16).

- **NAT**

En NAT, un dispositivo de red como un cortafuegos NAT o un router asigna una dirección IP pública a un ordenador o a un grupo de ordenadores de una red privada. De esta forma, NAT permite que un dispositivo medie entre las redes pública, privada y local.

NAT puede conservar las direcciones IP permitiendo que las IP privadas se conecten utilizando direcciones no registradas. Antes de reenviar los paquetes de datos entre las redes conectadas, NAT traduce las direcciones de red locales y privadas en direcciones únicas, globales y legales.

Con las configuraciones NAT, sólo una única dirección IP será visible para el mundo exterior, aunque representará a toda la red. Como resultado, puede ocultar toda la red interna y ofrecer más seguridad y privacidad. Las implementaciones NAT son mejores para entornos de acceso remoto. Pathak, A. (2024, 14 mayo).

6.2 Fundamentos de seguridad perimetral.

- **Seguridad informática**

Es el proceso de eludir y localizar el uso no autorizado de un sistema informático con el objetivo de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

En otras palabras, busca proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática es conformada por medidas de seguridad, como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, como es la activación de la desactivación de ciertas funciones de software. Netec Global Knowledge. (s. f.). Netec.

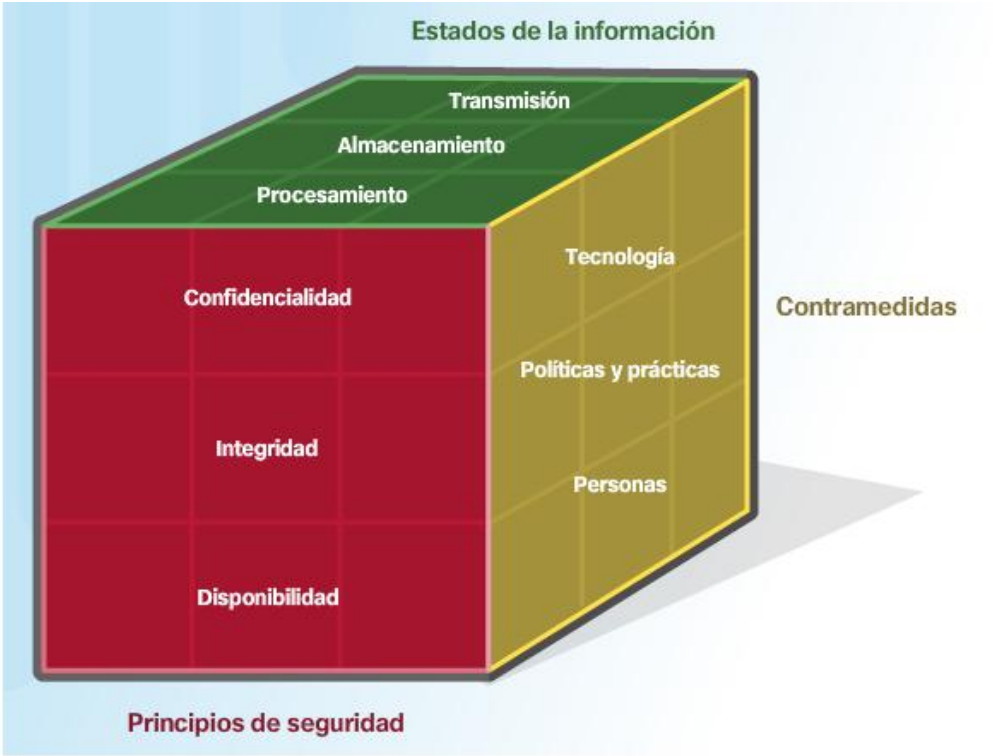
John McCumber, un destacado pionero en el campo de la ciberseguridad desarrolló una teoría ampliamente conocida como el Cubo de McCumber. Esta herramienta conceptual está

diseñada para establecer, evaluar y fortalecer la seguridad de la información, y se basa en tres dimensiones fundamentales, de las cuales son:

- **Principio de la seguridad:** incluirá 3 principios a los que hará referencia como la tríada CID (Confidencialidad, Integridad y Disponibilidad).
- **Estados de la información:** servirá para identificar los estados de información de datos.
- **Contramedidas:** será para identificar las habilidades de las profesiones de las tecnologías de información.

Figura 3

Cubo de McCumber



Principio de la seguridad conformado por la triada CID, anteriormente mencionada:

- Confidencialidad busca prevenir la divulgación no autorizada de información.

- Integridad busca la precisión, uniformidad y confiabilidad de la información.
- La disponibilidad garantiza el acceso a la información siempre que sea requerida. Loranca, M. (2022, 26 enero)

- **Perímetro de red informático**

Un perímetro de red utiliza varios componentes de red para crear una línea divisoria segura entre una LAN interna y todas las comunicaciones externas. En la mayoría de los casos, las comunicaciones externas se refieren a los datos que entran y salen de Internet. Sin embargo, los perímetros de red también pueden segmentar otros tipos de comunicaciones externas, como WAN, cabeceras VPN, extranet a socios externos y troncales de protocolo de inicio de sesión a operadores de voz.

Desde el punto de vista de la LAN corporativa, el perímetro de la red es el punto de demarcación preciso entre la red interna y la externa. En la mayoría de los casos, el perímetro de la red consta de un cortafuegos, un router seguro o un dispositivo WAN seguro definido por software.

Un perímetro de red se refiere al hardware y software de red diseñado e implementado para evitar que la actividad maliciosa ingrese a la red. En este caso, los perímetros incluyen todo el enrutamiento de red, la conmutación, el hardware de seguridad y el software de seguridad utilizados para fortalecer y mantener seguras las operaciones de red. Froehlich, A. (2023, 22 marzo).

- **Firewall o cortafuego**

Un firewall es una herramienta de seguridad informática diseñada para proteger una red de computadoras al monitorear y controlar el tráfico de datos que entra y sale de la red.

Funciona estableciendo reglas y filtros que determinan qué tipo de comunicación se permite y cuál se bloquea, con el objetivo de prevenir accesos no autorizados, ataques maliciosos o la propagación de malware.

Los firewalls pueden operar a nivel de hardware o software y se utilizan comúnmente en entornos empresariales y domésticos para salvaguardar la integridad y la confidencialidad de la información almacenada en los sistemas conectados a la red.

Además de actuar como una barrera defensiva, los firewalls también pueden generar registros detallados de actividad que ayudan a los administradores de red a supervisar posibles amenazas y mejorar continuamente la seguridad.

- **Función de un firewall:**

Como ya se explicó, la función principal de un firewall es proteger los dispositivos conectados a una red interna o privada de accesos no autorizados y de información o solicitudes de entrada maliciosas. Para ello, debe supervisar y filtrar todos los datos e intentos de acceso para dividirlos en dos grupos: aquellos que cumplen con los criterios de seguridad establecidos y se les permite el paso, y aquellos que no los cumplen y son bloqueados.

Así, actúa como primera línea de defensa y en algunos casos impide el acceso de usuarios no autorizados, en otros detecta el robo o la exfiltración de información y la presencia de algunos tipos de malware mediante el análisis de red, entre otras amenazas cibernéticas. Esto implica una serie de tareas o elementos que debe cumplir todo firewall:

a. Supervisar la comunicación saliente o entrante de los equipos conectados a una misma red o al internet.

b. Algunos fabricantes de Firewall permiten advertir y evitar el acceso de usuarios no autorizados a la red interna.

c. Bloquear el tráfico de red asociado a aplicaciones específicas que parezcan sospechosas o maliciosas.

d. Advertir los intentos de conexión que ocurren desde dispositivos desconocidos.

e. Evitar que ingrese desde la red algunos tipos de malware.

f. Adaptarse a los cambios y progresos que ocurren en los ataques cibernéticos.

- **Tipos de firewall:**

Los firewalls pueden clasificarse en dos grandes grupos: aquellos que están integrados en un dispositivo o hardware que cumple específicamente con la función de cortafuegos; y aquellos que son solo software y pueden instalarse en cualquier dispositivo electrónico para darle protección adicional.

1) Firewall de hardware

En este caso, el cortafuegos se encuentra instalado en un dispositivo, por ejemplo, un router o en algunos casos Firewall físicos dedicados, de manera que todos los ordenadores que se conecten a él están protegidos.

Esto es de suma utilidad si se necesita proteger múltiples dispositivos que deben interconectarse entre sí. La complejidad de estos sistemas varía, y en sistemas caseros, que nos brinda nuestro proveedor de internet, el Firewall se encuentra dentro de nuestro “Módem”, y en la mayoría de los casos no necesita modificaciones para funcionar.

En sistemas más complejos como redes industriales o corporativas, pueden llegar a ser equipos muy robustos y costosos que requieren personal calificado para hacerlos funcionar, administrarlos y configurarlos.

2) Firewall de software

Este es el tipo de firewall que viene incluido en el sistema operativo de un ordenador o que puede instalarse posteriormente en uno, por lo que no protege a una red de ordenadores sino a un único dispositivo.

Es sumamente útil como complemento a un firewall de hardware, pues actúa como una segunda capa de protección en caso de que la primera falle, o un ataque provenga de otro dispositivo, o incluso protege en algunos casos cuando nos conectamos a redes que no conocemos o no tenemos el control.

Los firewalls también se pueden clasificar en:

- **Firewalls de red:** Están diseñados para proteger toda la red al bloquear el tráfico no deseado o sospechoso.
- **Firewalls de host:** Están instalados en dispositivos individuales y proporcionan una capa de seguridad específica para ese dispositivo.

Algunos tipos de firewalls son: Firewall proxy, Firewall de inspección de estado o inspección activa, Firewall de próxima generación (NGFW).

Algunos firewalls para pequeñas empresas son: Fortinet, Ubiquiti, Cisco, OPNSense, pfSense.

6.3 Profundización en la Seguridad Perimetral y Firewalls

- **Seguridad perimetral**

La seguridad perimetral se trata de la determinación de los límites que constituyen el perímetro para protección de los sistemas de IT ante intrusiones, amenazas o ataques de la ciberdelincuencia, así como evitar que datos confidenciales resulten comprometidos.

Un sistema de seguridad perimetral informática, además de detectar amenazas, lleva a cabo inspecciones y análisis de posibles patrones de ataque a la red. Se le instala entre la red externa y la interna, a manera de barrera de protección.

La importancia de la seguridad perimetral son aspectos como las políticas de privacidad, la confidencialidad y la integridad de la información de una organización, que ya no está definida por límites físicos, requieren de varios niveles de protección. Así que un sistema de seguridad perimetral juega un papel muy importante para la defensa de los datos.

Los principales objetivos de la seguridad perimetral informática son, en primer lugar, **soportar los ataques externos**, al mismo tiempo que detectar e identificar tales ataques para alertar acerca de ellos. Filtrar y bloquear el tráfico ilegítimo es un segundo objetivo relevante.

En tercer lugar, la segmentación y aseguramiento de los sistemas y servicios, de acuerdo con la superficie o área de daño que hubiera recibido un ataque.

- **Firewall PfSense**

pfSense es un software de código abierto que se utiliza principalmente como un firewall y enrutador. Está basado en el sistema operativo FreeBSD y se destaca por ser un sistema flexible y potente, capaz de ofrecer características avanzadas de seguridad y gestión de redes.

Principales características:

- **Firewall**: Proporciona una capa avanzada de protección contra ataques y accesos no autorizados.
- **Enrutamiento**: Ofrece capacidades completas de enrutamiento para gestionar el tráfico de red.
- **VPN**: Soporta varias tecnologías de VPN como OpenVPN, IPsec y PPTP.

- **Balanceo de carga**: Permite distribuir el tráfico de red de manera eficiente entre múltiples WAN.
- **QoS**: Soporte para Calidad de Servicio (QoS) para priorizar el tráfico de red crítico.
- **Captive Portal**: Ideal para entornos como cafeterías y hoteles que requieren autenticación para usar la red.

pfSense está orientado principalmente a usuarios que necesitan una solución robusta y fiable para administrar y proteger redes de manera eficiente. Su uso es común en diferentes entornos como:

- **Pequeñas y medianas empresas:** Proporciona una solución económica y altamente funcional para la protección de redes empresariales.
- **Proveedores de servicios de Internet (ISP):** Utilizado para gestionar grandes volúmenes de tráfico y garantizar una conectividad fiable.
- **Entorno doméstico:** Ideal para usuarios avanzados que desean un control detallado sobre su red doméstica.
- **Entornos educativos:** Usado en colegios y universidades para proteger y gestionar sus redes de campus. LINUXMIND.DEV. (2024, 15 mayo).

6.4 Implementación y Gestión de la Seguridad de Red

- **Modo bridge**

Los puentes utilizan MAC de origen y destino antes de reenviar paquetes, lo que contribuye a una menor congestión de la red. Básicamente, el puente es el proceso de conectar dos redes y hacer que funcionen como una sola.

Ahora, es una configuración que se puede configurar para que los dispositivos de red funcionen simultáneamente y extiendan el acceso al puerto a un área más amplia. Esta

configuración deshabilitará la traducción de acceso a la red (NAT) en uno de los enrutadores y lo convertirá en un dispositivo de capa 2 (en OSI) y extenderá la LAN. LinuxMind(May 15, 2024).

- **DMZ**

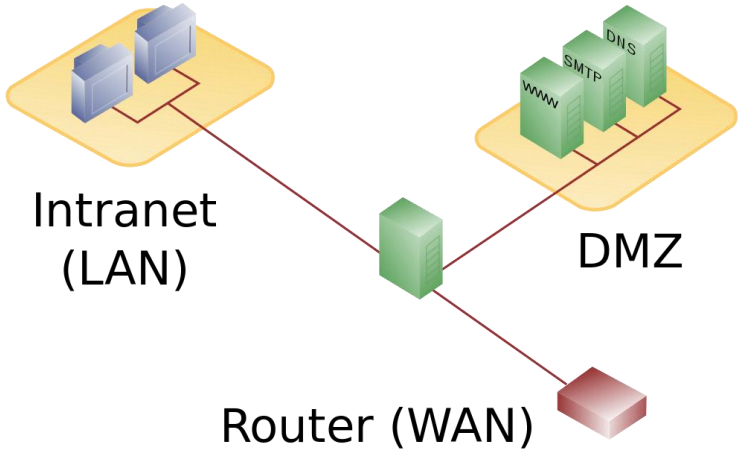
En informática, una zona desmilitarizada (demilitarized zone, DZM) hace referencia a una red de ordenadores con un rango de direcciones IP privadas que sirve como franja de seguridad entre dos redes, separándolas mediante estrictas reglas de acceso. Así, aunque físicamente los servidores dentro de una DMZ se encuentran en la misma empresa, no están conectados directamente con los equipos de la red local. La estructura del nivel de protección más alto consiste en un cortafuegos que separa la zona desmilitarizada, situada entre la red local e Internet, de las redes vecinas. Por su parte, en las arquitecturas de red un poco más económicas, todas las redes están conectadas a un único firewall con tres terminales separados. En este caso se habla de una DMZ protegida.

- **DMZ con dos firewalls**

Con el fin de proteger a las redes corporativas de ataques desde las redes de área amplia (WAN por sus siglas en inglés) se suele aplicar el concepto de zona desmilitarizada con dos cortafuegos, que consiste en un cortafuegos externo que protege la zona desmilitarizada de la red pública y un cortafuegos interno entre la DMZ y la red empresarial. Los cortafuegos pueden ser independientes, de hardware, o de software, por ejemplo, desde un router.

Figura 3

Referencia de una DMZ



Esta arquitectura de seguridad en dos etapas hace posible la configuración de rutas estáticas que regulan el tráfico entre las redes de la siguiente manera:

Tabla 1

Demostración de políticas de firewall

El usuario está	**Acceso a la DMZ**	**Acceso a la LAN**	**Acceso a internet**
En internet WAN	Permitido	Denegado	-
En LAN	Permitido	-	Permitido
En la DMZ	-	Denegado	Denegado

Así, los usuarios de la red local pueden acceder a la red pública y a la zona desmilitarizada, los usuarios de Internet solo tienen acceso a la DMZ. El tráfico externo desde la DMZ está bloqueado por dos cortafuegos.

Es altamente recomendable implementar cortafuegos de diferentes proveedores. De no ser así, una vez identificada una vulnerabilidad en uno de los cortafuegos, un hacker podría

acceder sin ningún problema al otro. Para evitar los ataques de un servidor infectado a otros dispositivos dentro de la zona desmilitarizada, es posible implementar software de cortafuegos adicionales o una segmentación en redes de área local virtual o VLAN por sus siglas en inglés.

- **DMZ con un firewall**

Para implementar una zona desmilitarizada de manera más económica, es posible utilizar un único cortafuegos de gran alcance (un router con firewall) con terminales para tres conexiones de red separadas: una para Intranet, otra para Internet y otra para la DMZ. En este tipo de zona desmilitarizada, todos los puertos son supervisados por separado por el mismo firewall, lo que lo convierte en el punto único de fallo (single point of failure, SPOF). Es fundamental conseguir un cortafuegos que sea capaz de hacer frente al tráfico de Internet, así como a los diferentes accesos a la red interna.

- **Archivo ISO**

Un archivo ISO o imagen de disco óptico es una copia exacta de todo un disco óptico (como un CD, DVD o Blu-ray Disc) archivada en un único archivo. Este archivo, llamado imagen ISO, es una copia más pequeña de un gran conjunto de datos. Mucha gente utiliza archivos ISO para hacer copias de seguridad de sus discos o para almacenar sus datos de forma más práctica.

Tras conocer su definición, vamos a aprender más características de un archivo ISO, las cuales son:

- **Formato de archivo:** iso9660, sistema de archivos UDF (ISO/IEC 13346)
- **Sistema compatible:** Windows, macOS, Linux

Funciones: Replica/copia un disco óptico original y guárdalo: Cuando no dispongas de discos físicos, puedes utilizar un archivo ISO para transferir un juego, por ejemplo, de un disco antiguo a tu portátil. Luis. (2024, 11 octubre).

- **VMware**

VMware es una empresa de software de virtualización que se utiliza para ofrecerle al cliente un ambiente de simulación de la ejecución de diversos ordenadores dentro de otro, de forma simultánea.

Esto significa que permite ejecutar un determinado sistema operativo como si este estuviera instalado en el servidor físico, pero sin estarlo realmente. Esto se debe a que esos sistemas corren dentro de otro elemento denominado *host.*

Una máquina virtual (VM) es la unidad base de la virtualización de VMware. Es una representación basada en software de una computadora física. Un sistema operativo (SO) que se ejecuta en una máquina virtual se denomina SO invitado.

Cada máquina virtual incluye lo siguiente:

- Un archivo de configuración que almacena la configuración de la máquina virtual.
- Un archivo de disco virtual es una versión de software de una unidad de disco duro.
- Un archivo de registro que realiza un seguimiento de las actividades de la máquina virtual. Esto incluye fallas del sistema, cambios de hardware, migraciones de máquinas virtuales de un host a otro y el estado de la máquina virtual.

VMware ofrece varias herramientas para administrar estos archivos. Puede configurar los ajustes de la máquina virtual mediante vSphere Client, una interfaz de línea de comandos para la administración de máquinas virtuales. También puede utilizar el kit de desarrollo de software de vSphere Web Services para configurar máquinas virtuales con otros programas.

Por ejemplo, puede habilitar el entorno de desarrollo de software para crear una máquina virtual para probar un programa de software. KeepCoding, R. (2024, 30 julio).

- **Snort**

Snort es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS utiliza una serie de reglas que ayudan a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes que coincidan con ellos y Genera alertas para los usuarios.

Snort también se puede implementar en línea para detener estos paquetes. Snort tiene tres usos principales: Como un rastreador de paquetes como tcpdump, como un registrador de paquetes, que es útil para la depuración del tráfico de red, o puede ser Se utiliza como un sistema completo de prevención de intrusiones en la red. Snort se puede descargar y configurar para uso personal. y uso comercial por igual. SNORT - Network Intrusion Detection & Prevention System. (s. f.).

- **Squid**

Un proxy de filtrado web con todas las funciones que usa squid. Filtra en función del contenido de la página web (mediante una lista de frases prohibidas), PICS, Tipo MIME y extensión de archivo. Es gratuito para uso no comercial.

Squid ofrece un rico entorno de control de acceso, autorización y registro para desarrollar proxy web y aplicaciones de servicio de contenido. Squid ofrece un amplio conjunto de opciones de optimización del tráfico, la mayoría de las cuales están habilitadas de forma predeterminada para una instalación más sencilla y de alto rendimiento.

6.5 Seguridad en Aplicaciones y Base de Datos

- **Laravel**

Laravel es un framework web fácil de usar que te ayudará a crear sitios web y aplicaciones web extensibles basados en PHP a escala.

El marco Laravel promueve el patrón arquitectónico MVC para crear aplicaciones web. Este patrón especifica un conjunto de reglas que especifican cómo crear aplicaciones web escalables y fáciles de mantener.

El patrón MVC de Laravel ayuda a los desarrolladores a poner orden y coherencia en el código no estructurado. El enfoque MVC también facilita el desarrollo de aplicaciones web a pequeña y gran escala.

Laravel utiliza Artisan como una CLI que ayuda a los desarrolladores web a:

- Migración de datos
- Administrar bases de datos
- Genere código repetitivo, controladores, modelos y más

La CLI de Artisan facilita el desarrollo web gracias a las funciones de generación de código y administración de bases de datos que están a solo unos comandos de distancia. En lugar de escribir código repetitivo o configurar una base de datos, un desarrollador puede centrarse en crear la lógica de la aplicación.

- **WordPress**

WordPress es un sistema de gestión de contenidos (**CMS)** gratuito y de código abierto que permite a cualquiera crear y gestionar sitios web fácilmente. El software WordPress, que comenzó como una plataforma de blogs, ha evolucionado para ayudar a los usuarios a crear diversos sitios, desde blogs y portafolios hasta tiendas de comercio electrónico.

Mucha gente utiliza WordPress para crear varios tipos de sitios web, como:

- **Blogs personales.** Dado que WordPress comenzó como una plataforma de blogs, tiene funciones potentes integradas para escribir entradas de blog, categorizar contenidos y revisar comentarios. La interfaz fácil de usar también facilita la gestión de un blog de WordPress.
- **Portafolios.** Los autónomos y creativos pueden mostrar su trabajo con un sitio de WordPress utilizando un tema de portafolio y un plugin de galería.
- **Sitios web empresariales.** WordPress admite funciones empresariales esenciales, como formularios de contacto, reservas de citas y testimonios de clientes, útiles para una página web de empresa o de pequeño negocio.
- **Tiendas online.** Plugins como WooCommerce pueden convertir WordPress en una plataforma completa de comercio electrónico, con herramientas como listados de productos, carritos de la compra y procesamiento seguro de pagos.
- **Foros.** Los plugins de foros de WordPress te permiten establecer discusiones temáticas, añadir perfiles de usuario e impulsar la participación para fomentar una sólida comunidad en línea.
- **Cursos en línea.** Los plugins de sistemas de gestión del aprendizaje (LMS) ofrecen creación de cursos, seguimiento de alumnos y sistemas de pago integrados.
- **Sitios web de hospedaje.** WordPress facilita la gestión de hoteles y alquileres vacacionales. Muchos plugins pueden agilizar las operaciones de hostelería, incluidas las reservas, los inventarios de habitaciones, los precios y las comunicaciones con los huéspedes.
- **Sitios web de eventos.** Varios plugins ayudan a crear listados de eventos, vender entradas, promocionar patrocinadores y proporcionar mapas interactivos del lugar. Las integraciones con las redes sociales ayudan aún más a publicitar los eventos. B, G., & B, G. (2024, 10 octubre).

- MySQL

MySQL es el sistema de gestión de bases de datos relacional más extendido en la actualidad al estar basado en código abierto. Desarrollado originalmente por MySQL AB, fue adquirida por Sun MicroSystems en 2008 y esta su vez comprada por Oracle Corporation en 2010, la cual ya era dueña de un motor propio InnoDB para MySQL.

MySQL es un sistema de gestión de bases de datos que cuenta con una doble licencia. Por una parte, es de código abierto, pero por otra, cuenta con una versión comercial gestionada por la compañía Oracle.

Las versiones Enterprise, diseñadas para aquellas empresas que quieran incorporarlo en productos privativos, incluyen productos o servicios adicionales tales como herramientas de monitorización y asistencia técnica oficial.

Descritas las principales características de MySQL es fácil ver sus ventajas. MySQL es una opción razonable para ser usado en ámbito empresarial. Al estar basado en código abierto permite a pequeñas empresas y desarrolladores disponer de una solución fiable y estandarizada para sus aplicaciones. Robledano, A. (2019, 24 septiembre).

7. Diseño Metodológico

7.1 Cronograma de actividades

Figura 4

Cronograma de actividades

El estudio se enfocará en la implementación y evaluación práctica de una solución de seguridad perimetral utilizando pfSense en un entorno simulado de pequeñas y medianas empresas. La población de estudio estará formada por las pequeñas y medianas empresas de la ciudad de León. No se requerirá una muestra específica debido a la naturaleza práctica y experimental del estudio. Las fuentes de información incluirán manuales de pfSense, documentación técnica y la experiencia práctica de nosotros en la implementación y evaluación de estas soluciones de seguridad perimetral.

Se utilizarán registros de configuración y herramientas de ciberseguridad para recopilar datos sobre el desempeño y la efectividad de la solución implementada. El procedimiento incluirá la configuración y puesta en marcha de la solución de seguridad perimetral con pfSense en un entorno simulado de PyMEs, registrando y analizando los datos generados durante este proceso. Se realizará un análisis cualitativo, de los datos recopilados, centrándose en la eficacia de las soluciones en la protección de los activos de información y la mitigación de riesgos. Se identificarán variables relacionadas con la configuración de pfSense, el rendimiento del sistema y la detección de amenazas para su análisis. Se garantizará el cumplimiento de las políticas de seguridad de la información y la privacidad de los datos, siguiendo los principios éticos.

7.2 ¿Qué solución proponemos?

Nuestra propuesta es una solución de seguridad perimetral, que ha sido meticulosamente diseñada, administrada y desarrollada mediante el empleo exclusivo de software de código abierto. Este enfoque se respalda con licencias de distribución y utilización de código abierto, lo que resulta en una notable reducción de los costos asociados a la adquisición de licencias de software y hardware especializado destinado a la seguridad perimetral.

En consecuencia, nuestra solución de seguridad perimetral está estratégicamente alineada para satisfacer las necesidades de pequeñas y medianas empresas. Este enfoque se adapta particularmente a entornos donde la seguridad informática no ostenta la prioridad máxima o donde los recursos y el presupuesto disponible limitan la implementación de soluciones más robustas en el ámbito de la seguridad perimetral.

Es muy importante considerar implementaciones progresivas de soluciones más avanzadas en seguridad perimetral a medida que surjan las necesidades específicas de seguridad informática y protección de la información para sus activos. Este avance implica la adquisición de licencias comerciales para software o hardware especializado, brindando así un conjunto más amplio de herramientas y técnicas para mitigar riesgos y asegurar continuamente la disponibilidad de la información únicamente a personas autorizadas y debidamente autenticadas. Este enfoque garantiza la integridad de la información, previniendo modificaciones no autorizadas, y restringe el acceso exclusivamente a personal autorizado, fortaleciendo de esta manera la seguridad de sus activos digitales.

Para tener una compresión de pfSense, y los firewalls en general se simulará una pequeña PYME, con la intención de demostrar cómo se implementa, configura y se activan diferentes funcionalidades, de pfSense incorporando servicios clave como DNS, DHCP, SSH, Portal cautivo, políticas, entre otros.

Se podrá seguir nuestras directrices detalladas para la implementación de la solución, acompañadas de las correspondientes recomendaciones, con el fin de asegurar una configuración efectiva es por ello por lo que, en un ambiente controlado, de hipervisor nivel 2 en conjunto con el software VMware Workstation Pro for Windows User, se implementa y configura pfSense y el resto de las tecnologías en simulación de una PYME.

Se plantea la creación de un entorno virtualizado en el que el firewall pfSense actúa como gateway para dos redes con interfaces de red distintas, con el objetivo de segmentar una red denominada DMZ. En esta DMZ se alojarán dos servidores ejecutando el sistema operativo Ubuntu Desktop, denominados Tierra y Marte. Su propósito principal es proporcionar servicios típicamente requeridos por pequeñas empresas, tales como SSH, FTP, bases de datos, y un sistema web desarrollado en el lenguaje de programación Laravel, junto con su correspondiente sitio web basado en WordPress. Todos estos servicios estarán accesibles para los clientes de la empresa desde internet.

Por otra parte, pfSense gestionará otro segmento de red denominado LAN, que albergará una máquina dedicada a la administración, configuración y mantenimiento de los servicios activos en el firewall, además del propio firewall. Esta red LAN también contendrá a los usuarios regulares, incluyendo empleados y visitantes. Para simular un cliente, se configurará una máquina que deberá conectarse a través de un portal cautivo en pfSense. Una vez autenticado, se le asignará una dirección IP a través del servidor DHCP de la red LAN.

Todas las conexiones de ambas redes, tanto LAN como DMZ, serán centralizadas en pfSense, que se encargará de realizar el enrutamiento de estas, además de proporcionar respuestas DNS. La centralización de las conexiones en pfSense es crucial ya que permitirá la aplicación de filtros en cada paquete de datos que ingrese al firewall, utilizando políticas y otras funcionalidades.

8. Resultados

8.1 Diseño de la solución

8.1.1 Definición de los requisitos específicos para nuestra solución

En esta sección se desarrollará la parte práctica de la investigación, en la cual se elaborará una guía detallada sobre cómo configurar el asistente de configuración en un firewall como pfSense. Este asistente de configuración facilita el proceso inicial al guiar al usuario paso a paso en la definición de los parámetros básicos de la red, como la configuración de las interfaces (WAN, LAN), ajustes de acceso remoto, reglas de firewall y otros aspectos críticos para asegurar un funcionamiento óptimo del firewall desde el principio. El asistente de configuración está diseñado para simplificar la instalación, permitiendo que incluso usuarios sin experiencia avanzada puedan realizar la configuración inicial de manera eficiente. A medida que avancemos en la creación de esta guía, se abordarán configuraciones más avanzadas y lógicas que nos permitirán cerrar brechas de seguridad y fortalecer la protección con pfSense.

8.1.2 Selección de tecnologías y herramientas de seguridad perimetral

Implementar un firewall como pfSense representa una Solución de Seguridad Perimetral ideal para Pequeñas y Medianas Empresas en la ciudad de León, Nicaragua, proporcionando un enfoque integral en la protección perimetral. Esta propuesta, aunque elemental, ha sido cuidadosamente diseñada, administrada y desarrollada utilizando únicamente software de código abierto. El uso exclusivo de este tipo de software, respaldado por licencias de distribución o de prueba, permite una reducción significativa en los costos relacionados con la adquisición de licencias para software especializado en seguridad perimetral, lo que la convierte en una opción accesible y eficiente para las Pymes en la ciudad de León, Nicaragua.

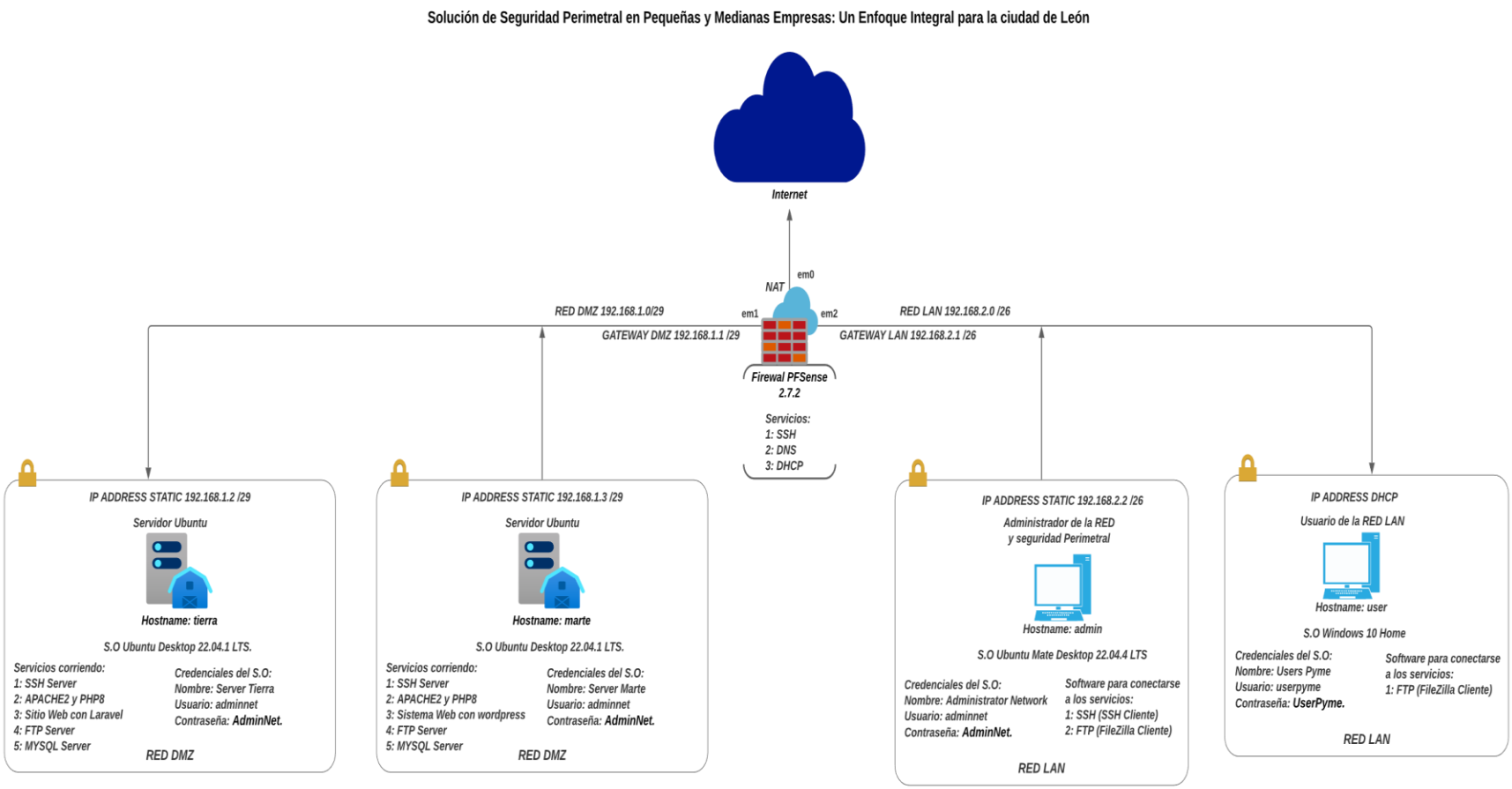
Este enfoque permite a las organizaciones implementar soluciones de seguridad robustas de manera eficiente, sin incurrir en elevados costos, al tiempo que preserva la flexibilidad y la capacidad de personalización inherente al software de código abierto. Es importante destacar que pfSense también ofrece una versión con licencia comercial, la cual se enfoca en brindar soporte técnico especializado ante posibles eventualidades. No obstante, para la presente solución, las pruebas se realizarán utilizando la versión de código abierto, lo que permitirá explorar la vasta cantidad de opciones disponibles para mitigar brechas de seguridad perimetral mediante este firewall. Con ello, se evaluarán las funcionalidades clave y el impacto de dichas herramientas en la protección de las infraestructuras digitales.

Es importante considerar la implementación progresiva de soluciones más avanzadas en seguridad perimetral conforme se identifiquen las necesidades específicas de protección digital y resguardo de los activos de información. Este proceso puede implicar la adquisición de licencias comerciales para software o hardware especializado, lo que proporcionará un abanico más amplio de herramientas y técnicas para mitigar riesgos y garantizar que la información esté siempre disponible únicamente para usuarios autorizados y debidamente autenticados. Este enfoque fortalece la integridad de los datos al prevenir modificaciones no autorizadas, restringe el acceso a personal autorizado, y refuerza significativamente la seguridad de los activos digitales, asegurando una protección continua y adaptada a las demandas del entorno.

8.1.3 Diseño de la arquitectura de red propuesta para la implementación de la solución

Figura 5

Topología de red propuesta



8.2 Preparación del entorno de simulación

Requerimientos previos para la instalación del entorno de virtualización:

A. Un computador recomendablemente con un procesador **i7 10th, 16GB de RAM, un SSD 500GB, una tarjeta de red Intel(R) Wi-Fi 6 AX201 160MHz** o una tarjeta de red Realtek **PCIe GbE Family Controller** (La elección de la tarjeta de red, es en dependencia de como el computador se conectará a la red).

A. Conocimientos previos básicos en seguridad informática, redes, sistemas operativos y virtualización.

B. El computador deberá tener el sistema operativo Windows 11 recomendablemente, ejecutándose y en él deberá tener instalado el software de virtualización **VMware Workstation Pro for Personal Use (For Windows) 17.6.1**. En caso de no tener instalado el software de virtualización o no saber cómo instalarlo, dejaré la siguiente documentación aquí para que pueda= leer y descargar el software de VMware.

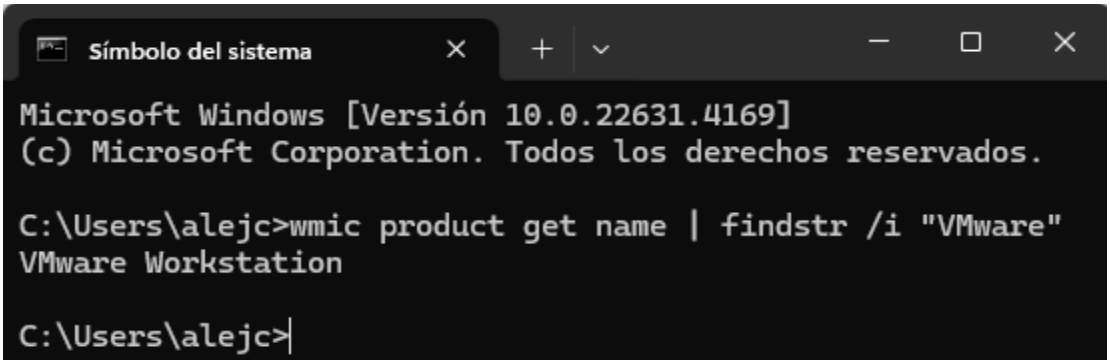
8.2.1 Configuración del entorno de virtualización con VMware Workstation

Empezamos nuestra guía de instalación verificando que tenemos instalado en nuestro computador **VMware Workstation Pro** desde el símbolo del sistema de Windows con el siguiente comando:

- **wmic product get name | findstr /i "VMware"**

Figura 6

Lista de productos VMware instalados usando WMIC



Nota: Este comando buscará entre las aplicaciones instaladas cualquier programa que contenga "**VMware**" en su nombre. Es especialmente útil si la aplicación no aparece en el menú estándar de programas instalados, ya que realiza una búsqueda más detallada.

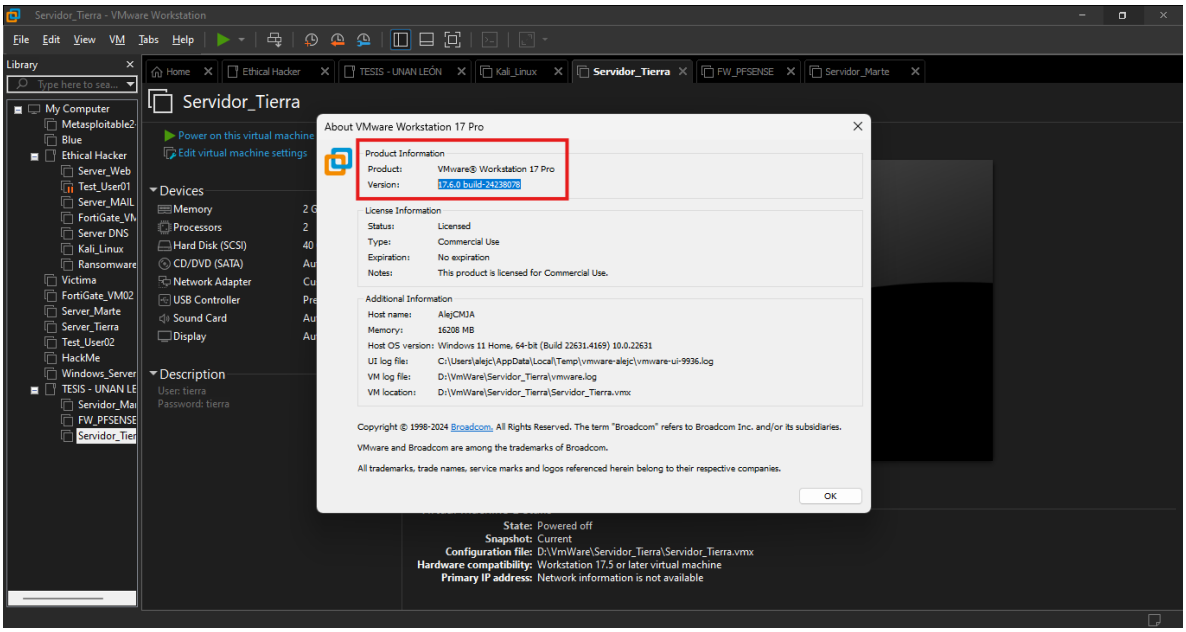
Una vez localizada la aplicación, podrás abrirla manualmente y verificar la versión de VMware Workstation instalada en tu sistema. Para hacerlo, abre **VMware Workstation** y sigue estos pasos:

- Dirígete a la barra de menú en la parte superior.
- Haz clic en **Ayuda** (Help).
- Selecciona -> **Acerca de VMware Workstation** (About VMware Workstation).

Luego de seguir los pasos mencionados, se te abrirá una ventana de VMware como la de **Figura *7***,

Figura 7

Verificando la versión de VMware Workstation instalada en nuestro sistema



Nota: En esta sección, podrás ver la versión específica de VMware Workstation instalada en tu sistema.

Es importante destacar que la versión que estamos utilizando de **VMware es la 17.6.0 build-24238078**, la más reciente disponible hasta la fecha. Por otro lado, VMware Workstation viene configurado por defecto en inglés. Para mantener la consistencia y la comodidad en esta guía, utilizaremos el idioma inglés dentro de la aplicación, pero nos aseguraremos de traducir palabras o términos clave cuando sea necesario, para facilitar la comprensión y garantizar que todos puedan seguir los pasos con claridad.

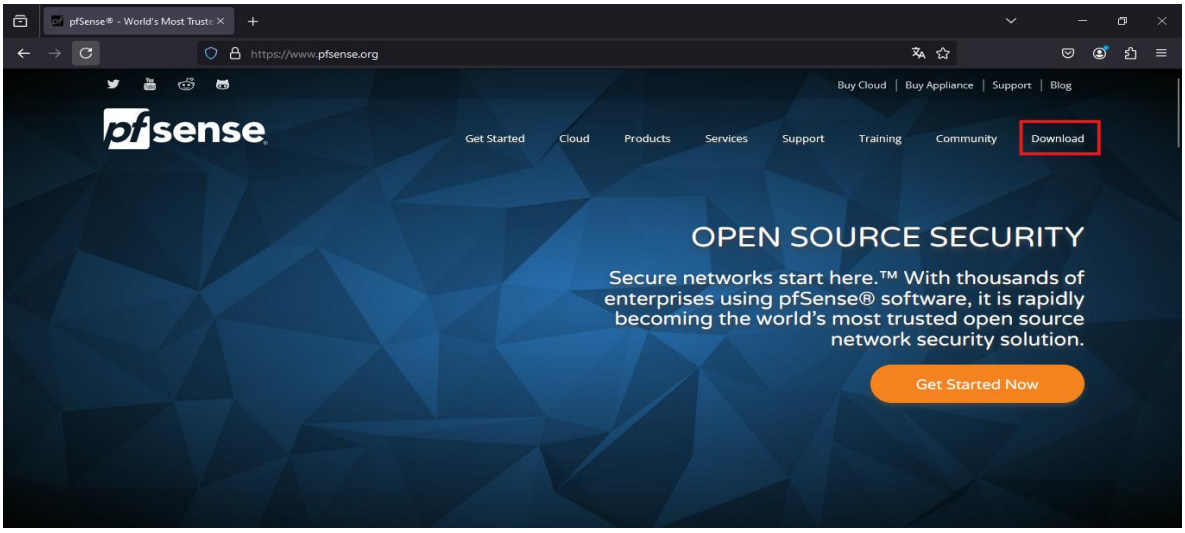
- **Descarga de pfSense desde su sitio web oficial**

Añadido este detalle, procedemos a continuar con la guía. Lo consiguiente será descargar el sistema operativo **pfSense** desde su repositorio oficial en el sitio web. Para

hacerlo, dirigimos nuestra atención a la sección de “**Descargar**” (Download), donde nos aparecerá la última versión disponible y además la que usaremos.

Figura 8

Sitio Web oficial de pfSense

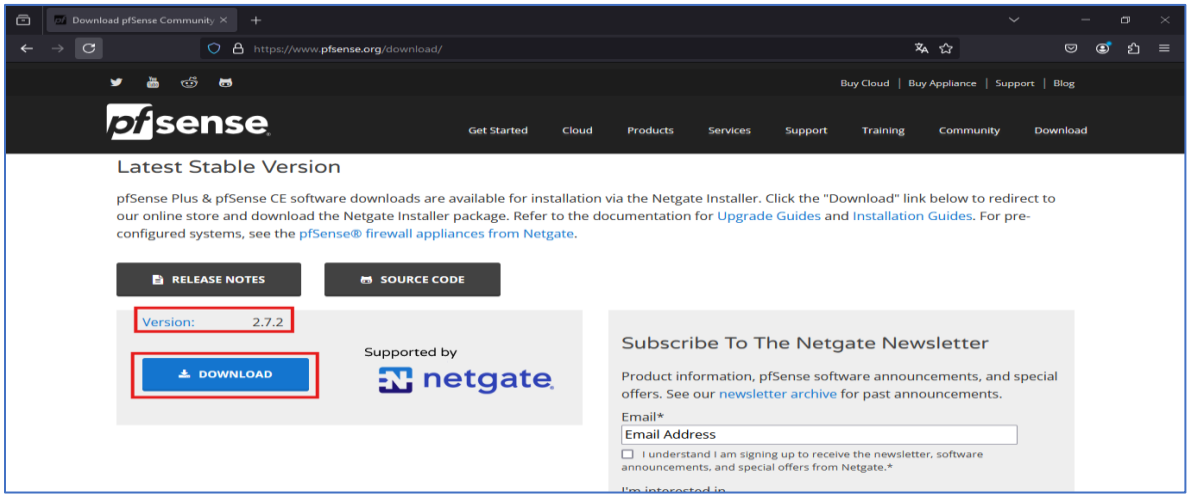


Nota: Adaptado de Captura de pantalla del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://pfsense.org).

Accedemos a la sección de "**Descargar**" y procedemos a seleccionar y descargar la **versión 2.7.2 de pfSense**, la cual corresponde a la última versión estable disponible al momento de redactar esta guía.

Figura 9

Sitio Web oficial de descarga de pfSense



Nota. Adaptado de la Sección de descargas del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://pfsense.org/download).

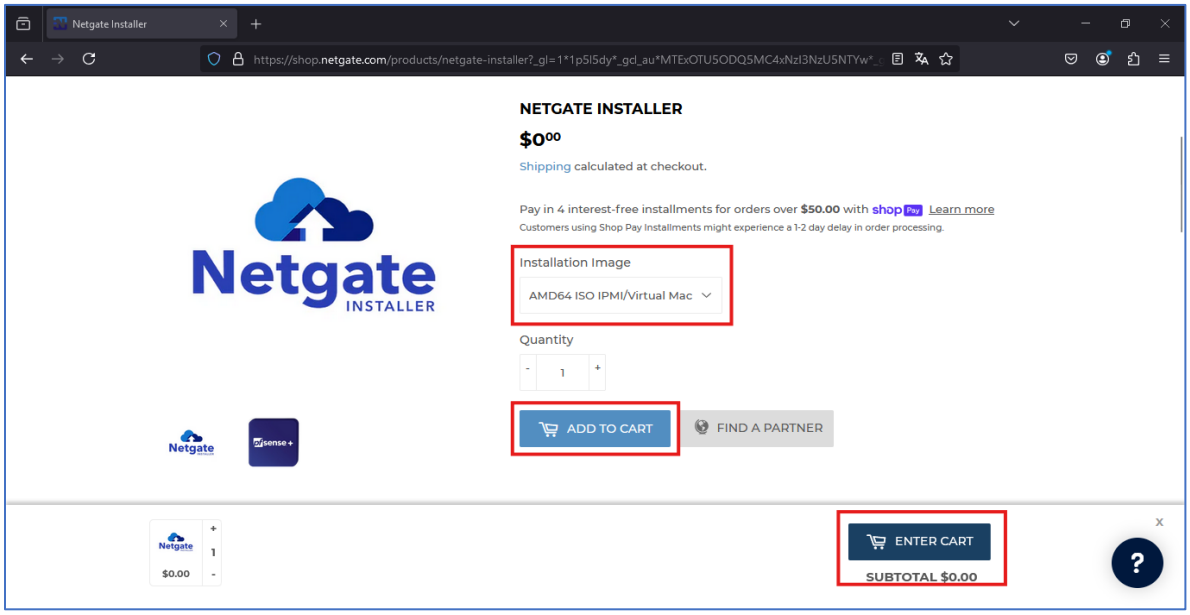
Una vez que hacemos clic en “**DOWNLOAD**”, se te redireccionara a la tienda de Netgate como podemos ver en **Figura 10** en este punto lo que haremos es añadir al carrito de Netgate el sistema el archivo de instalación de pfSense que necesitamos, se recomienda llenar la información de compra de la siguiente forma:

- **Installation Image (Imagen de instalación):** Seleccionamos la opción correspondiente para obtener un archivo ISO.
- **Precio**: La descarga del instalador de pfSense es gratuita, equivalente a $0.00.
- **Cantidad**: Debemos indicar 1 (una) unidad.

Finalmente, verificamos que hemos colocado la información de forma correcta, y presionamos en “**ADD TO CART**” y luego en “**ENTER CART**” para proceder a verificar el contenido del carrito.

Figura 10

Compra del archivo de instalación de pfSense

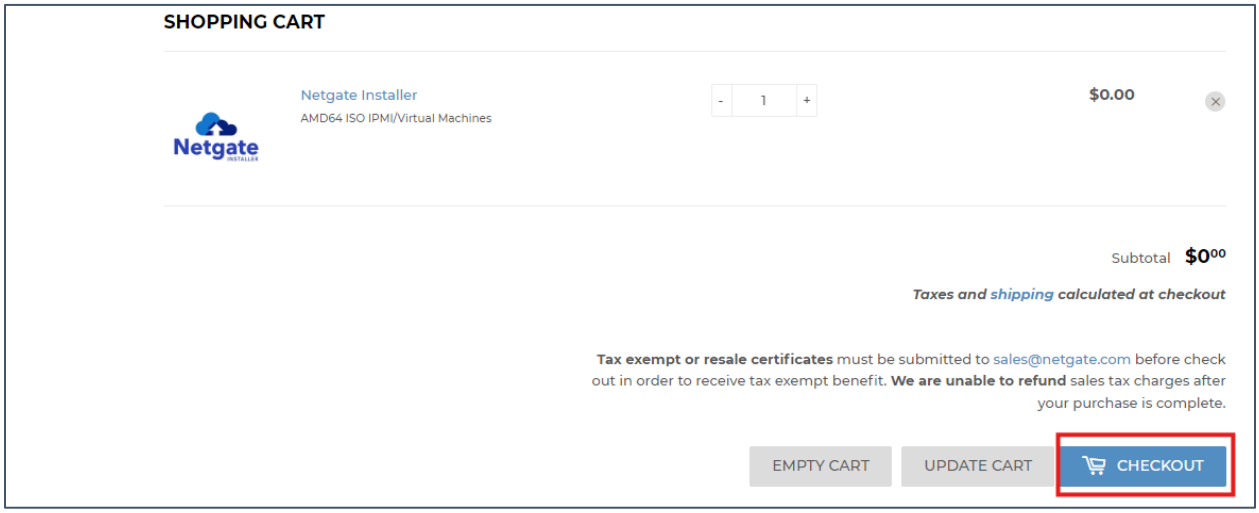


Nota: Adaptado de la Sección de compras del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://shop.netgate.com/products/netgate-installer).

Este método de compra del instalador de pfSense es un nuevo modelo de descarga de Netgate que realiza una compra, de una licencia que no es comercial y que no requiere de un pago.

Figura 11

Verificación del carrito de compras en el sitio web oficial de pfSense

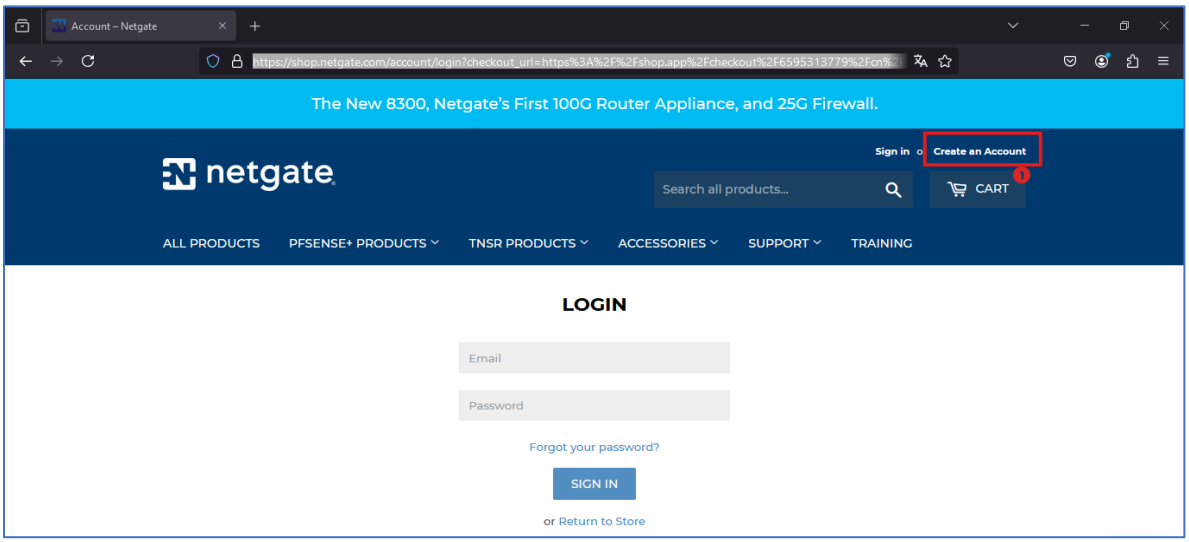


Nota: Adaptado de la Sección de compras del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://shop.netgate.com/products/netgate-installer).

Después de verificar el carrito, será necesario crear una cuenta cómo podemos ver en **Figura 12** para poder descargar el archivo de instalación de pfSense.

Figura 12

Sitio Web oficial de pfSense sección de Login

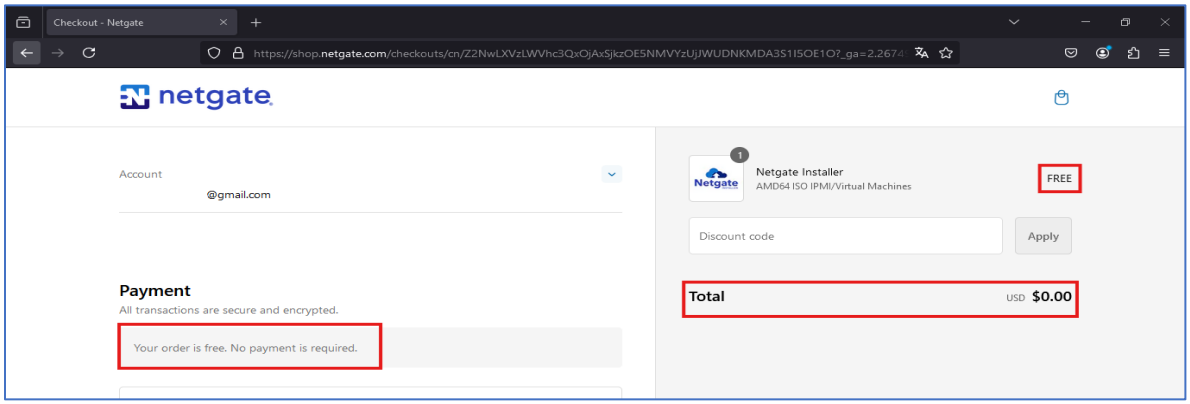


Nota: Adaptado de la Sección de Login del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://shop.netgate.com/account/login).

Omitiré el paso de crear una cuenta en el sitio web oficial, ya que tengo una cuenta existente. Simplemente iniciaré sesión con mis credenciales y una vez ustedes creen su cuenta en el sitio web de pfSense, procederemos a completar la compra del valor reflejado en $ 0 (cero) a como se puede apreciar en **Figura 13** para descargar el instalador de pfSense.

Figura 13

Formulario de pago en el sitio web de pfSense

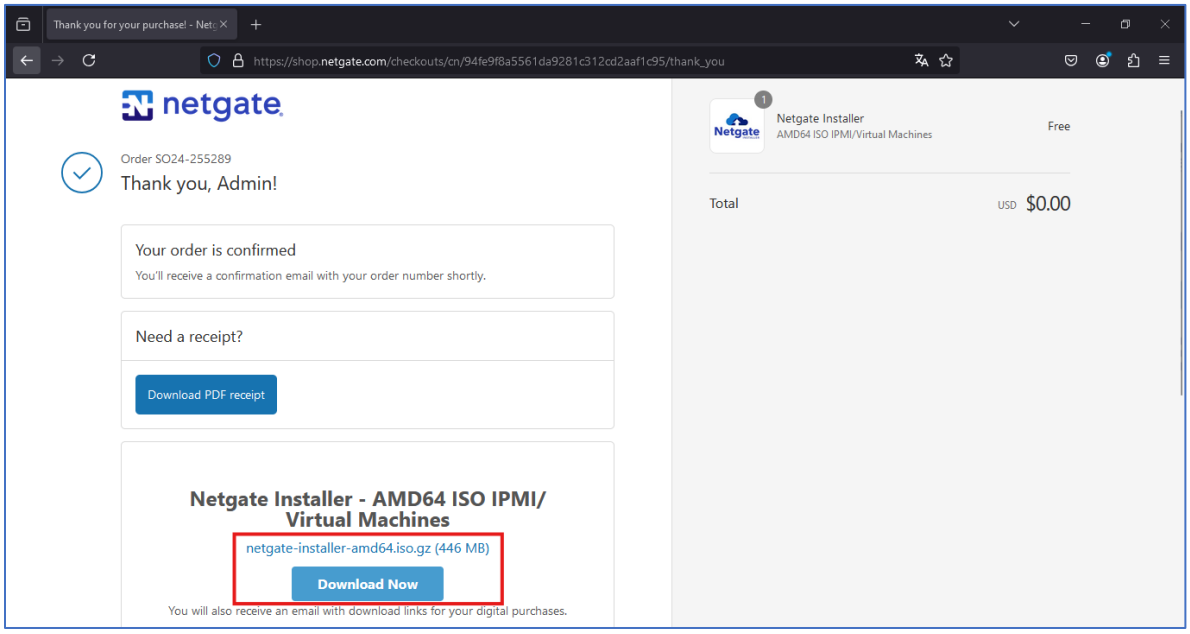


Nota: Adaptado de la Sección de compra del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://shop.netgate.com/checkouts/cn/).

Procedemos a completar la información solicitada en el formulario y a enviar el formulario haciendo clic en “**Complete Order”** al final de este. Para llegar al último paso, que consiste en descargar el archivo de instalación de pfSense, es fundamental rellenar todos los campos obligatorios. Una vez enviado el formulario, se generará un comprobante de compra y, lo más importante, recibiremos el enlace de descarga del archivo de instalación de pfSense, que tiene un tamaño de aproximadamente 446 MB.

Figura 14

Compra realizada con éxito en el sitio web de pfSense



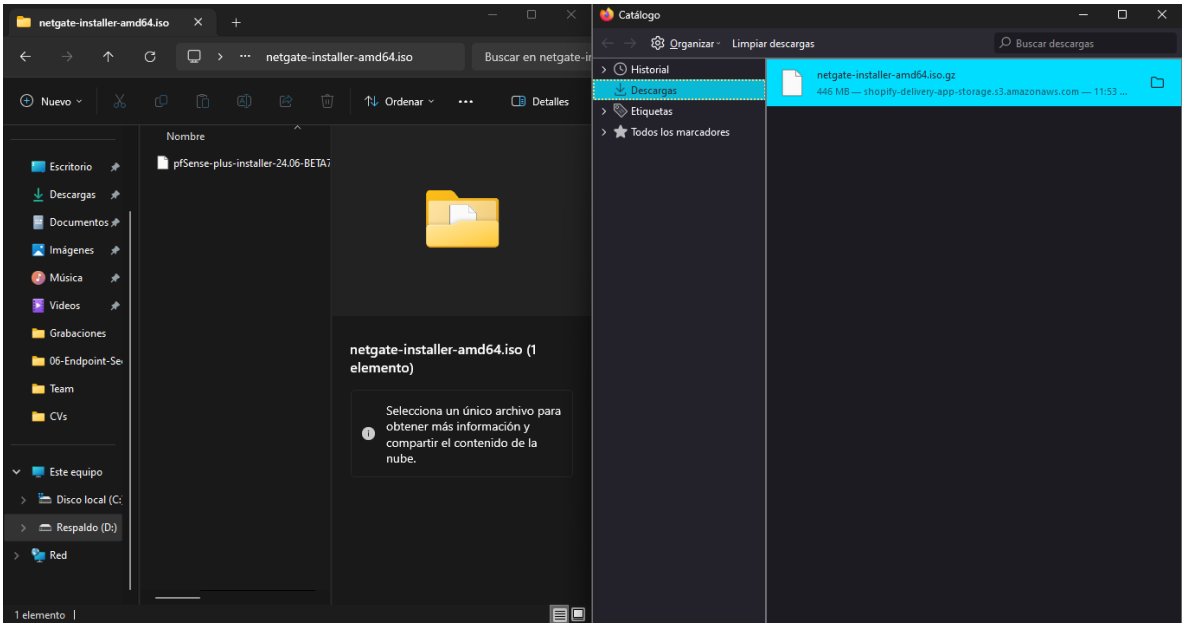
Nota: Adaptado de la Sección de compra del sitio web oficial de pfSense, por pfSense, 2024, pfSense (https://shop.netgate.com/checkouts/cn/).

Ha sido una aventura emocionante, ¿no crees? Adquirir un poderoso proyecto de código abierto como el de Netgate por un precio de licencia y uso de costo $0 es increíble. Y lo mejor está por comenzar. Ahora, vigilaremos la descarga del archivo, que dependerá del ancho de banda de la red que estés utilizando.

Como práctica ética, una vez que hayamos descargado el archivo de instalación de pfSense y lo hayamos localizado, lo moveremos a una carpeta con un nombre relacionado con esta guía. Esto facilitará su identificación y acceso cuando necesitemos utilizarlo en el futuro.

Figura 15

Referencia de como guardar el archivo de instalación de pfSense



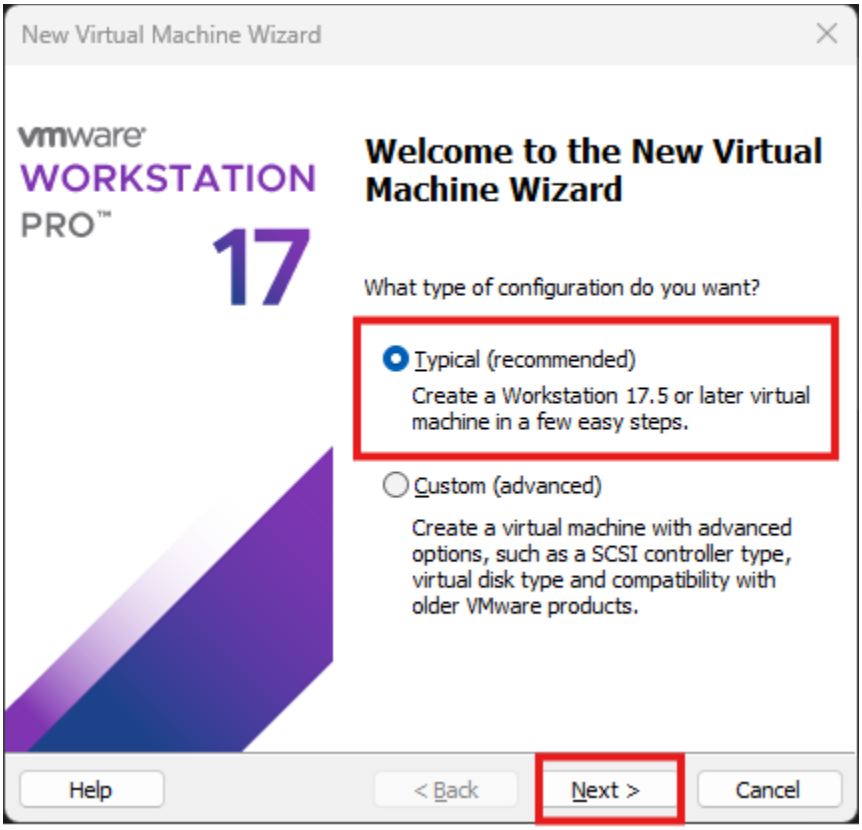
Nota: La ilustración presentada sirve únicamente como referencia. No es obligatorio seguirla exactamente, pero se recomienda adherirse a las instrucciones para facilitar el proceso.

- **Creación de la máquina virtual de pfSense**

Hemos llegado a un nuevo comienzo: finalmente, vamos a crear nuestra máquina virtual de pfSense en nuestro entorno controlado de virtualización con **VMware Workstation**. Para ello, regresaremos a la aplicación de VMware Workstation que teníamos ejecutando. En el **Dashboard** (Menú de opciones), buscaremos la opción “**File”** en la parte superior izquierda y seleccionaremos “**New Virtual Machine”**. Si no encuentras esta opción, puedes simplemente usar la combinación de teclas “**CTRL + N**”. Esto abrirá un asistente de configuración (**Setup Wizard**) que nos guiará en el proceso de creación de nuestra máquina virtual de pfSense.

Figura 16

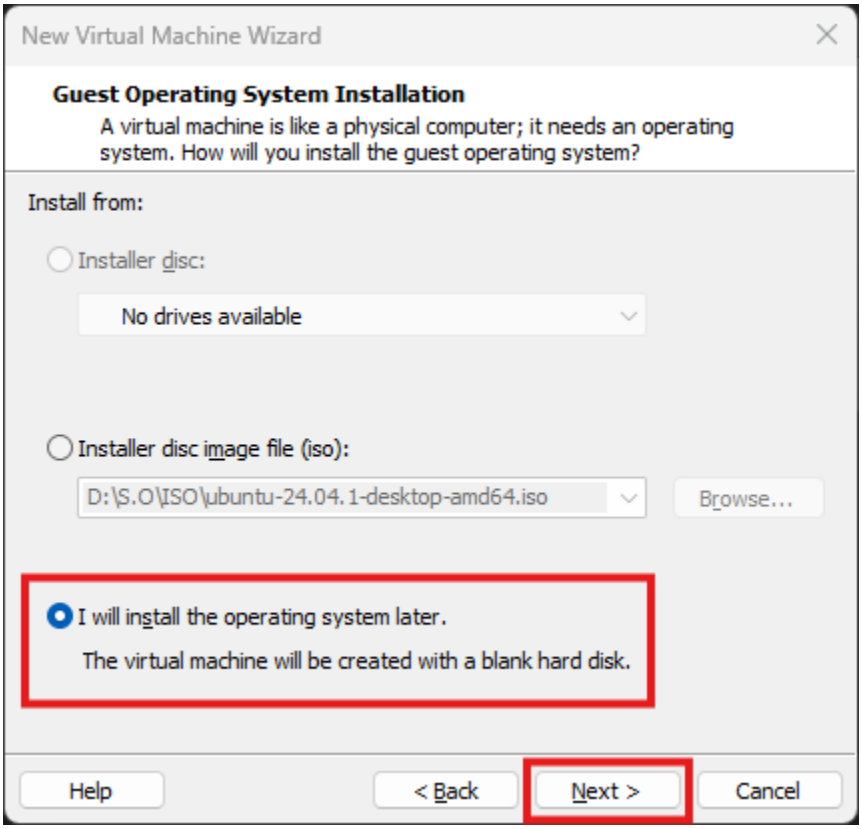
Asistente de configuración y creación de una nueva máquina virtual en VMware Workstation



El asistente de configuración nos guiará en el proceso de creación de nuestra máquina virtual de pfSense. Por defecto, nos mostrará las opciones recomendadas para nuestra configuración, por lo que seleccionaremos la opción “**Typical**” (Típico), que es la recomendada por el asistente. Luego, simplemente haremos clic en “**Next**” (Siguiente) para continuar con el asistente de configuración.

Figura 17

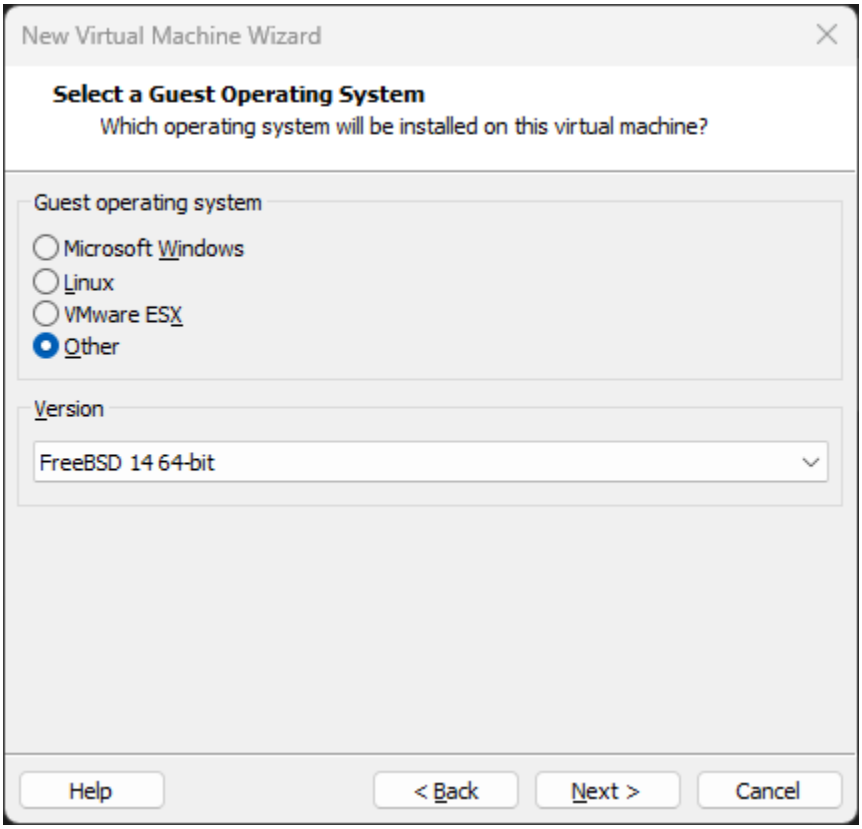
Asistente de configuración de la máquina virtual: Elección del archivo de instalación del sistema operativo



Nuevamente, el asistente de configuración nos mostrará sus recomendaciones. En esta etapa, seleccionaremos la opción "**I Will Install the Operating System Later"** (Instalaré el sistema operativo más tarde) y haremos clic en "**Next"** (Siguiente). No te preocupes; en unos pasos posteriores, procederemos a instalar el sistema operativo de pfSense.

Figura 18

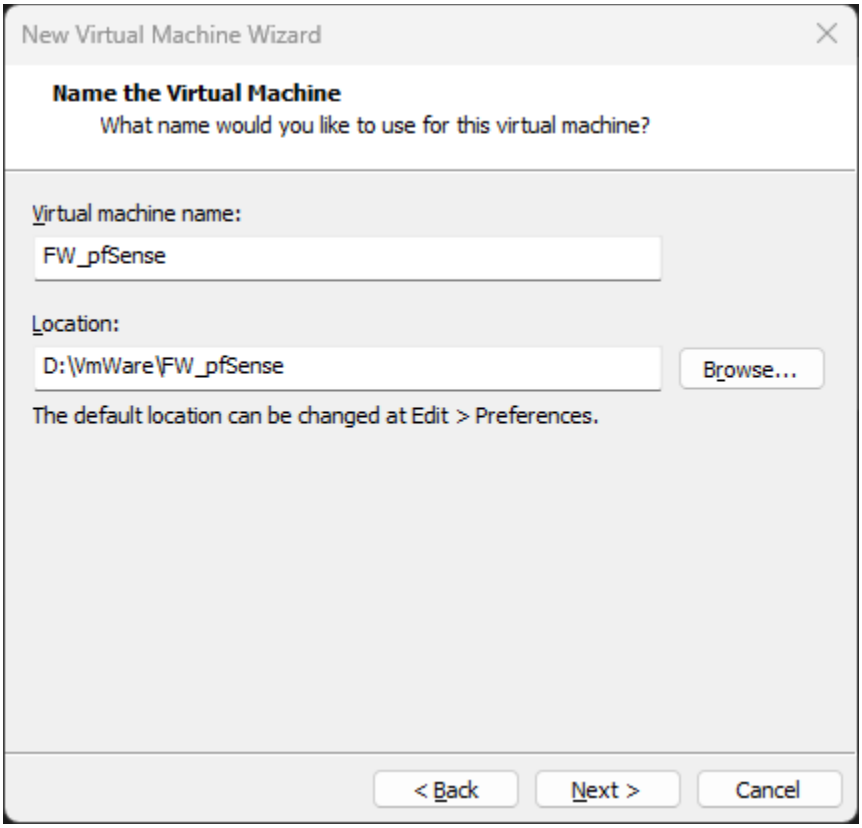
Asistente de configuración de la máquina virtual: Elección del sistema operativo que utiliza pfSense



En este punto, es importante entender que pfSense se basa en un sistema operativo llamado "**FreeBSD"**. Por ello, en la opción "**Guest Operating System"** (Sistema operativo invitado), debemos seleccionar "**Other"** (Otro), donde encontraremos **FreeBSD**. A continuación, elegiremos la **versión FreeBSD 14 de 64 bits** para aprovechar todas las características más recientes de pfSense. Una vez que hayamos ubicado y seleccionado los parámetros mencionados a cómo podemos ver en **Figura 18** , es hora de hacer clic en "**Next"** (Siguiente) y continuar con el asistente de configuración de VMware Workstation.

Figura 19

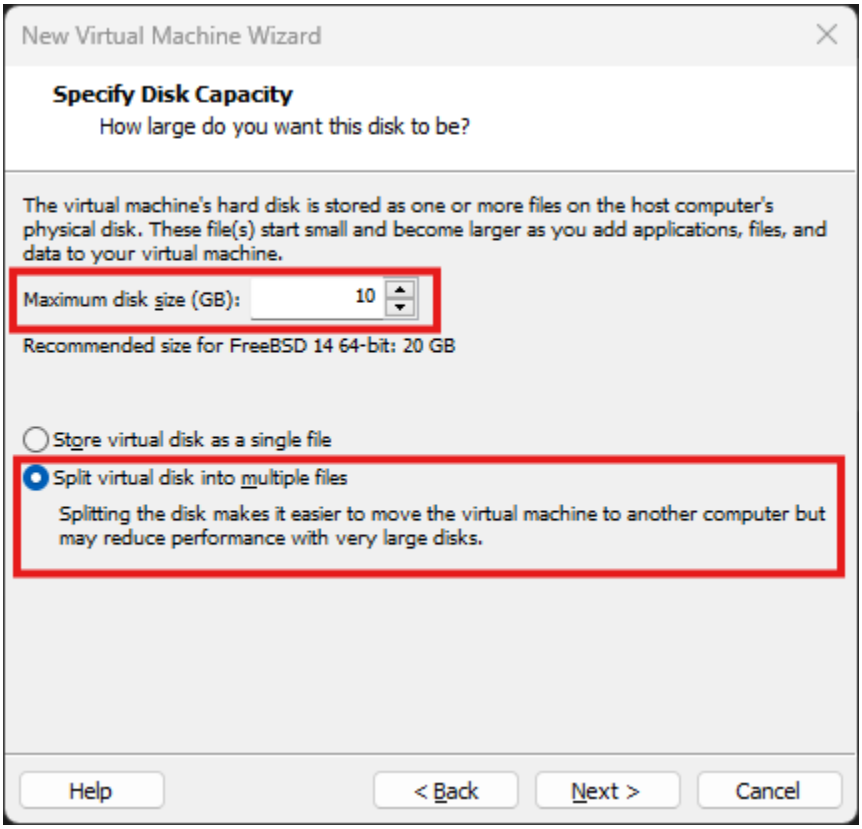
Asistente de configuración de la máquina virtual: Elección del nombre de la máquina virtual



En la opción de “**Virtual Machine Name”**, he asignado el nombre “**FW_pfSense”** a esta máquina virtual. En el ámbito de la seguridad perimetral, el término “**FW”** es comúnmente utilizado para referirse a un “**firewall tradicional”**. Por otro lado, en la opción de “**Location”,** selecciona una ubicación que te resulte conveniente y ordenada. En tu caso, puedes elegir la ubicación que más te convenga, o bien, se creará en la ubicación por defecto que VMware Workstation establece. Una vez hecho estos cambios seguimos presionando en “**Next”**.

Figura 20

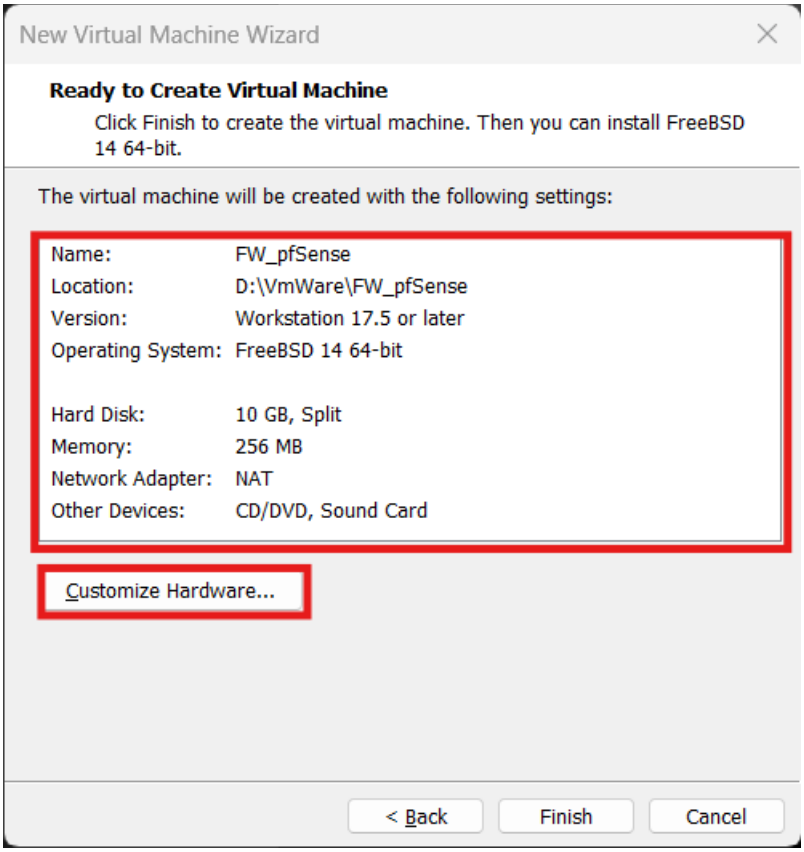
Asistente de configuración de la máquina virtual: Elección del tamaño y configuración del disco duro de la máquina virtual de pfSense



En esta parte de la configuración de la máquina virtual de pfSense, estamos configurando el disco duro, que es el almacenamiento donde se guardarán tanto los datos del sistema operativo como otros archivos relevantes. Basado en mi experiencia, recomiendo utilizar la opción "**Split Virtual Disk Into Multiple Files**" (Dividir el disco virtual en múltiples archivos), ya que es menos susceptible a fallos o errores durante la exportación al mover una máquina virtual. Por último, considero prudente asignar **10 GB de almacenamiento**, lo cual es más que suficiente para realizar nuestra guía. Continuamos presionando en "**Next"** (Siguiente).

Figura 21

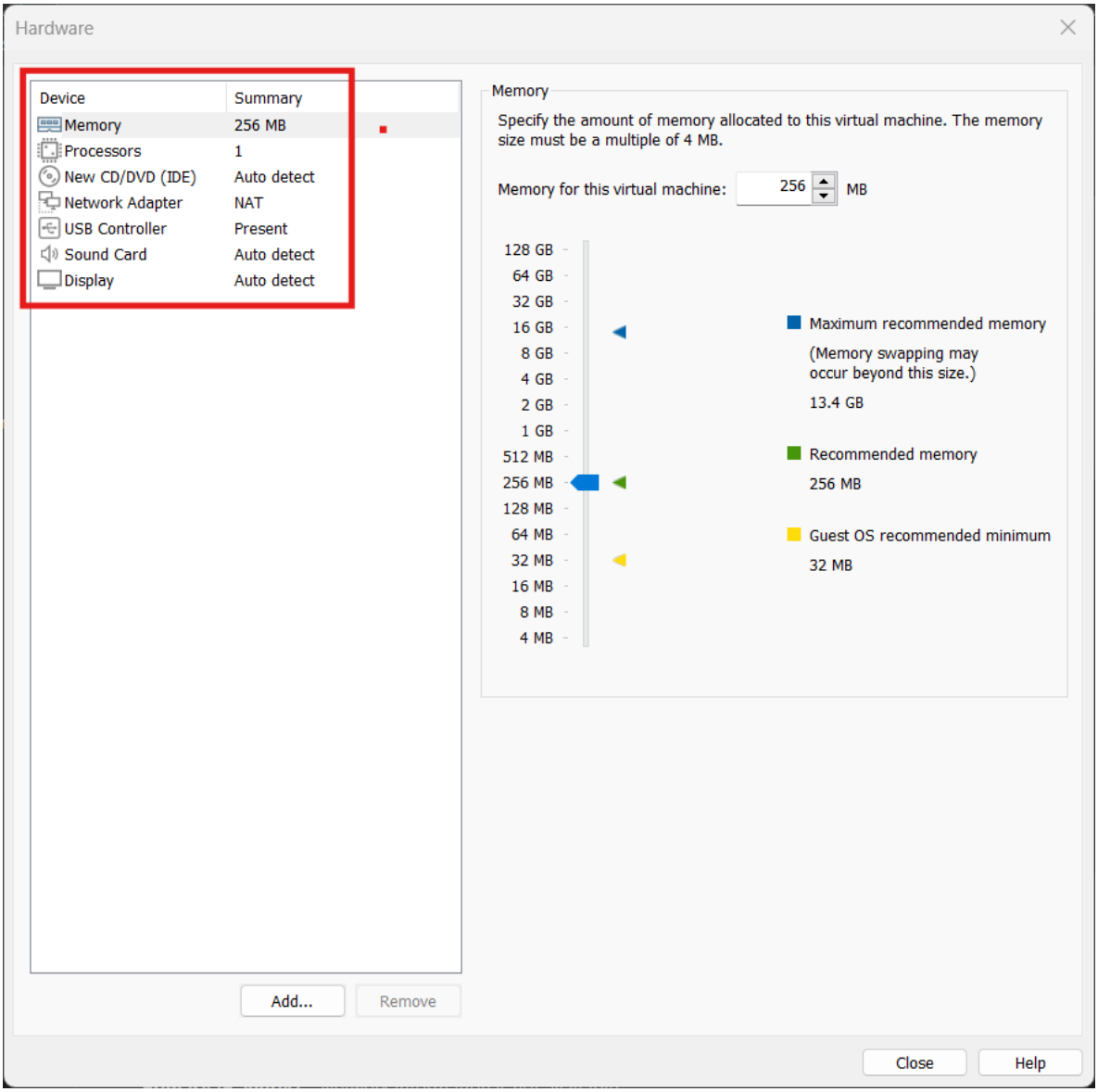
Asistente de configuración de la máquina virtual: Resumen general de la máquina virtual



A continuación, veremos un resumen en **Figura 21** de la configuración de la máquina virtual que se creará con el asistente. Pero antes de terminar, presionaremos en "**Customize Hardware**" (Personalizar Hardware) para realizar algunos ajustes finales en la máquina virtual de pfSense.

Figura 22

Asistente de configuración de la máquina virtual: Resumen general del Hardware de la máquina virtual

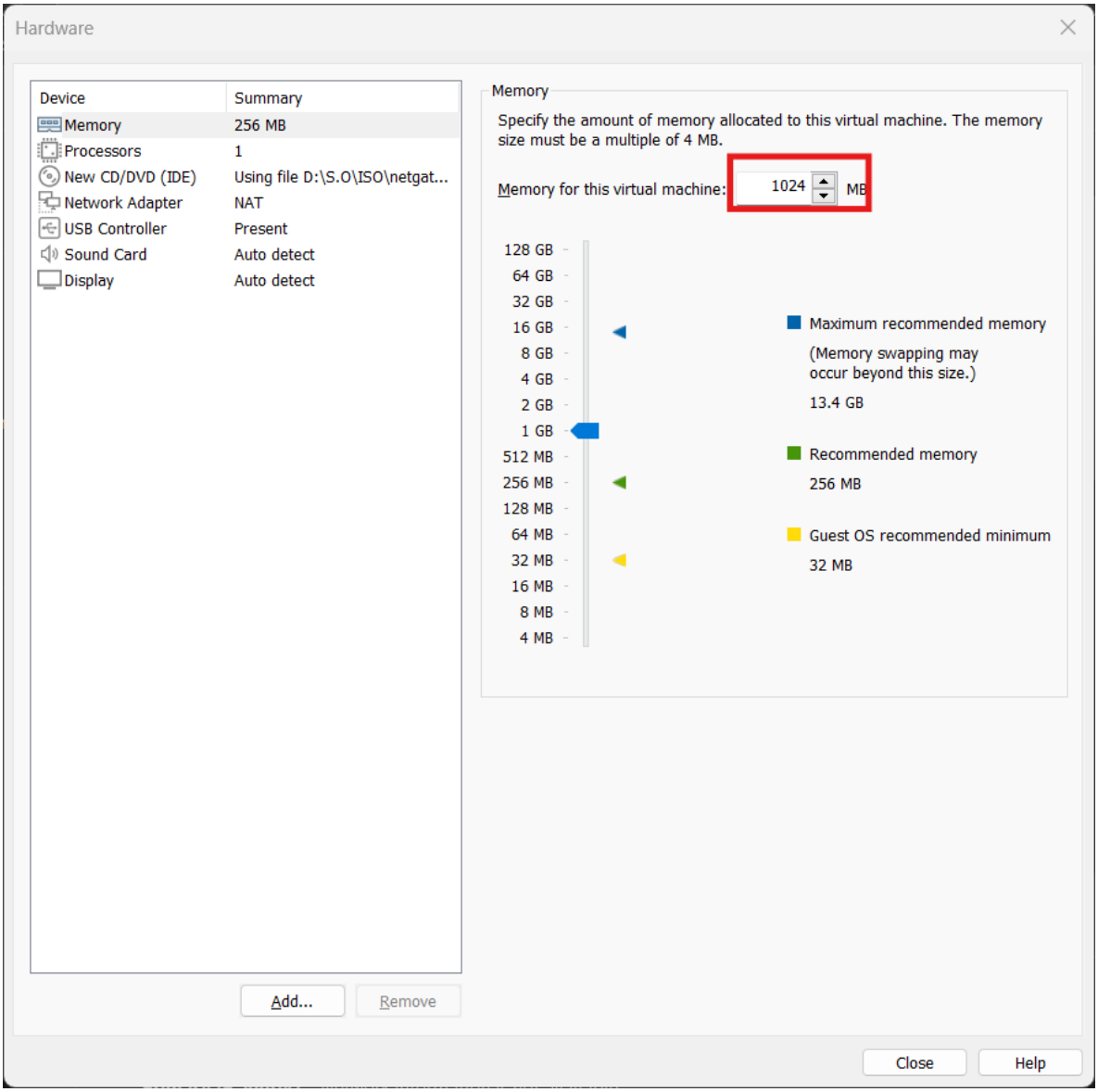


En el lado superior izquierdo de la **Figura *22***, tenemos las opciones configurables de nuestra máquina virtual, mientras que, en el lado superior derecho de la misma ilust6racion, encontramos los parámetros que podemos ajustar. A continuación, destacaremos las configuraciones que modificaremos, basándonos en nuestros requerimientos:

1. **Memory** (Memoria): Aquí asignamos la cantidad de memoria **RAM** del host principal que destinaremos a la máquina virtual. En mi caso, la dejaré en 1 GB para garantizar un buen rendimiento y fluidez.

Figura 23

Asistente de configuración: Elección de tamaño de memoria RAM en la máquina virtual

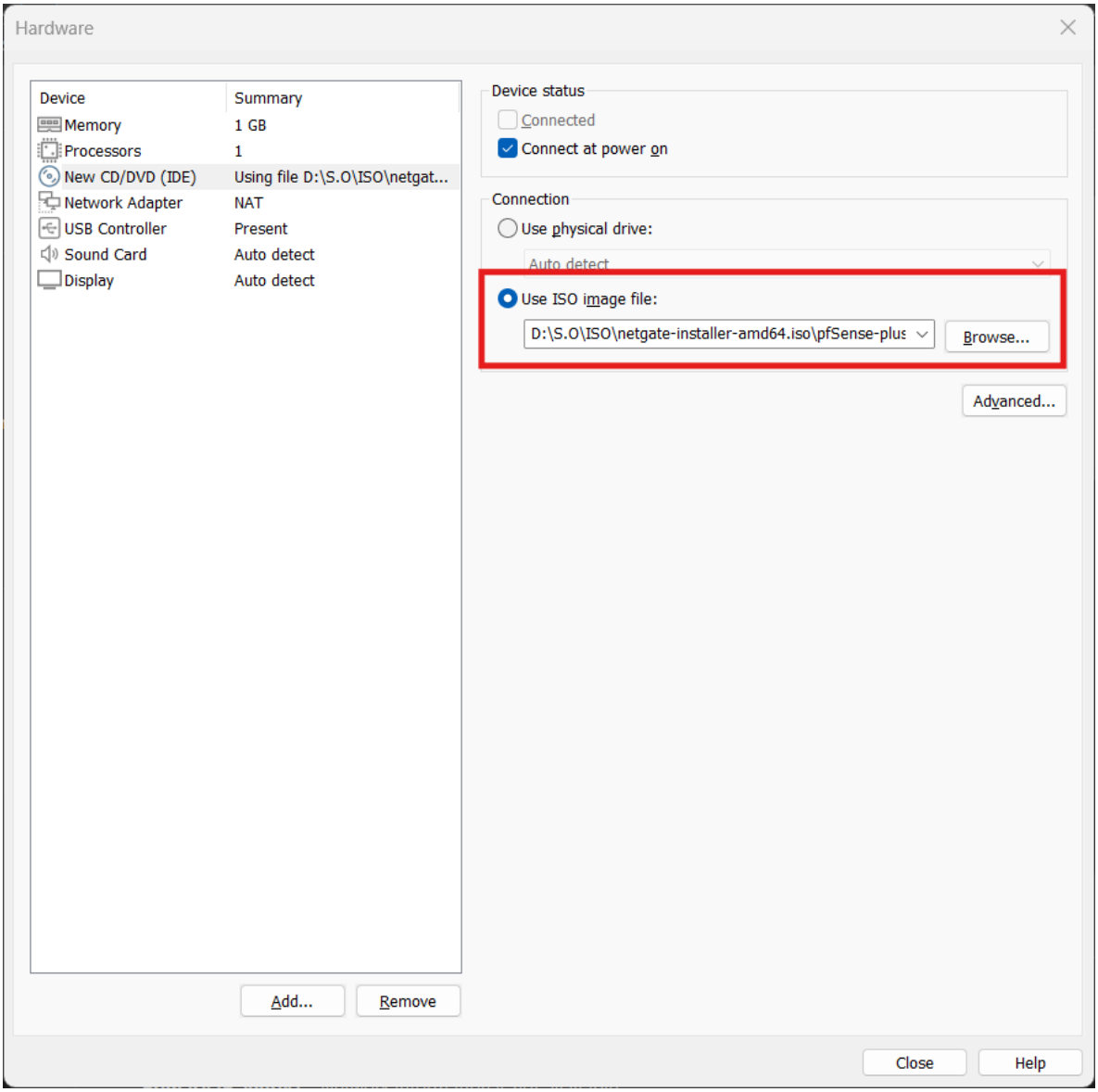


2. **New CD/DVD** (Añadir el archivo de instalación de pfSense): Esta opción es crucial, ya que aquí añadiremos el archivo de instalación de pfSense que

descargamos del sistema operativo pfSense. Seleccionaremos: “**Use ISO Image File”** (Usar archivo de imagen ISO), presionaremos “**Browse**” (Explorar), y buscaremos en nuestro directorio de archivos el archivo **.iso** que hemos descargado. Una vez encontrado, lo seleccionamos, así como lo hemos hecho en **Figura 24.**

Figura 24

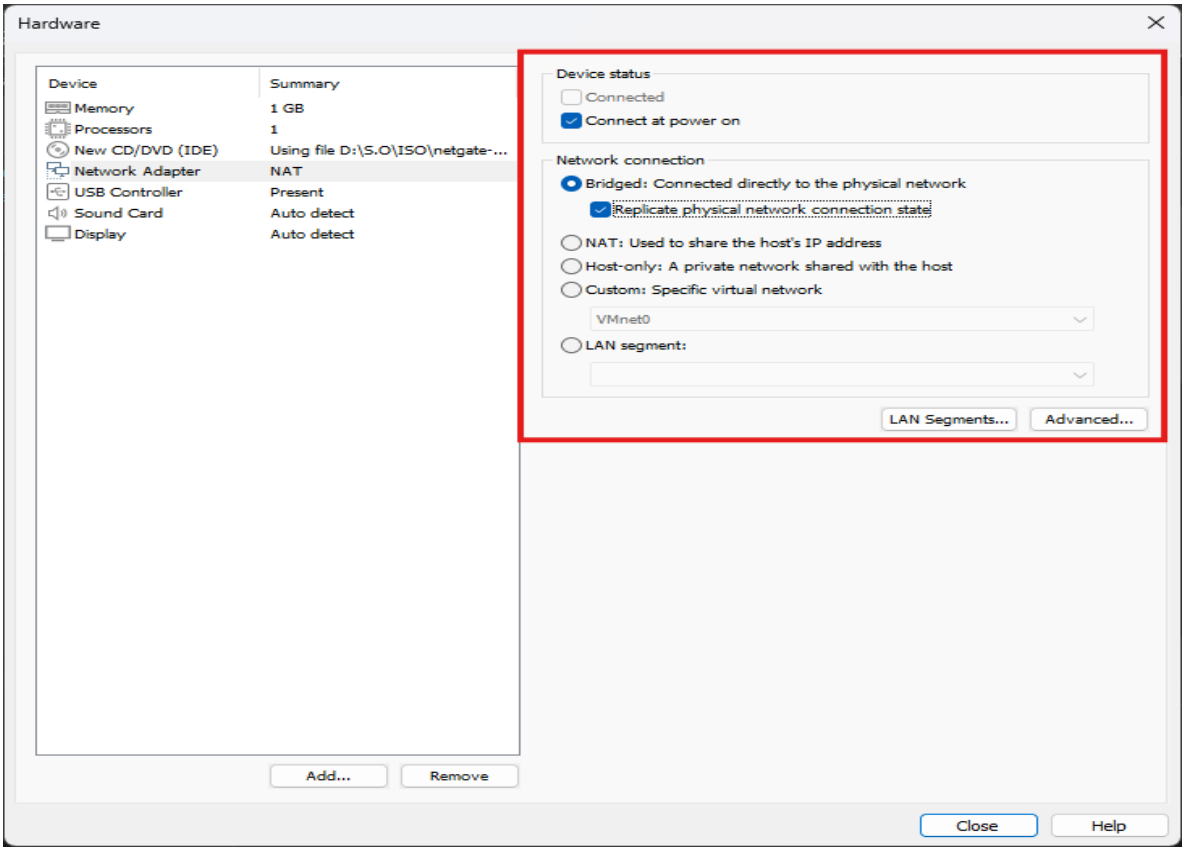
Asistente de configuración: Elección del archivo de instalación de pfSense



3. **Network Adapters** (Adaptadores de Red): Es fundamental configurar las interfaces de red en nuestra máquina virtual. Dado que estamos implementando una solución integral de seguridad perimetral y siguiendo las mejores prácticas, hemos diseñado una topología de red y que puedes ver en **Figura 5,** que incluye la segmentación de dos redes: una llamada **LAN** y otra llamada **DMZ**. Esto permite segmentar los paquetes, los usuarios y los servidores de forma segura. Además, para simular el entorno de una PYME que expone sus servicios en internet, configuraremos antes una red llamada **WAN** que podemos ver en **Figura 25.**

Figura 25

Asistente de configuración: Configuración de los adaptadores de red de la máquina virtual



Nota: Es importante recordar que, por defecto, VMware Workstation trae por defecto solo un adaptador de red activo. Este adaptador de red que viene por defecto activo lo configuraremos como la interfaz **WAN** y luego añadiremos dos interfaces adicionales para completar las interfaces **DMZ** y **LAN**.

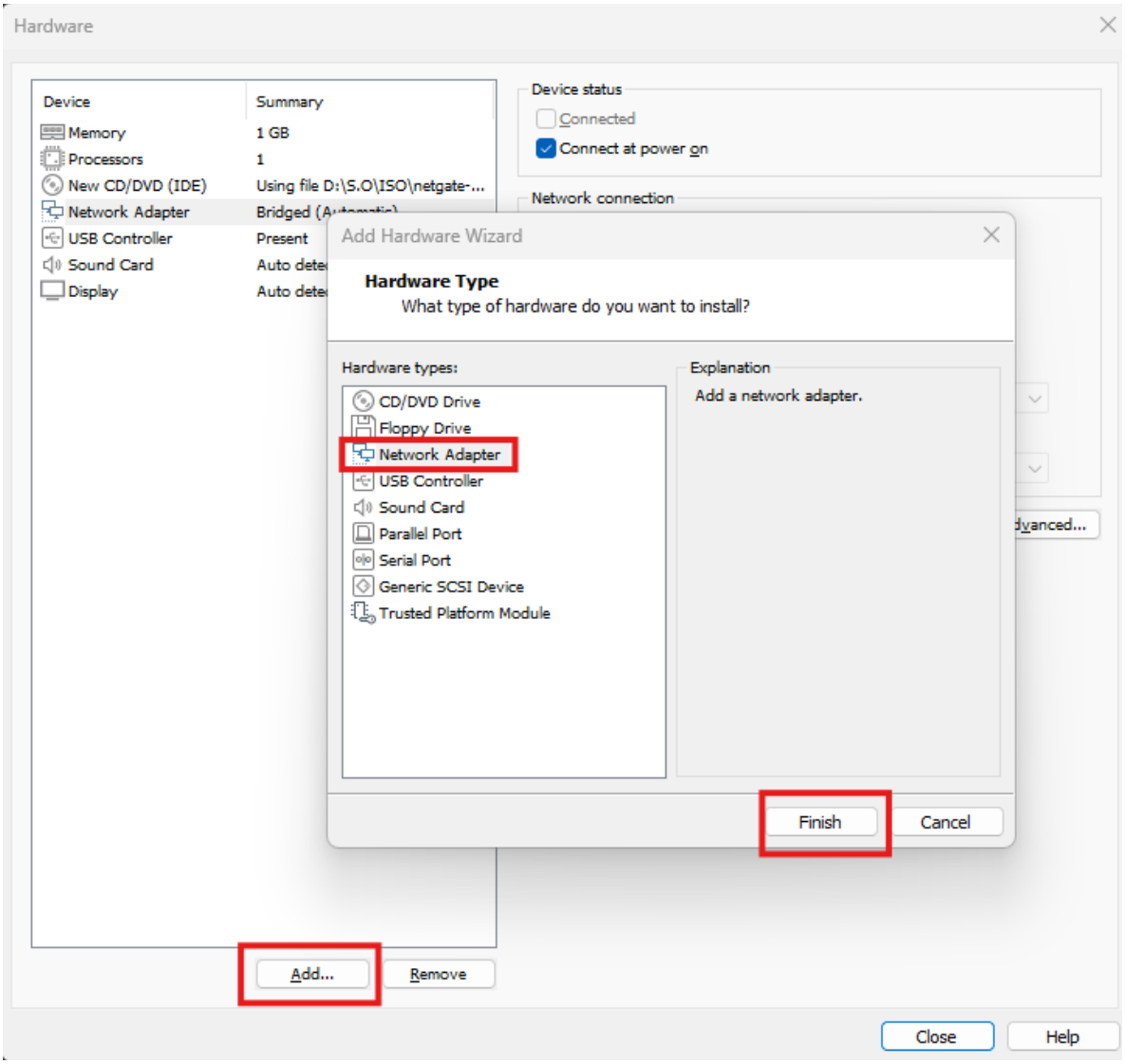
Ahora, ¿cómo simulamos una red WAN en un entorno virtual con VMware Workstation? Lo más común, y lo que haré en este caso, será utilizar este adaptador en el **modo Bridge**. Tener este modo en el adaptador hará que pfSense le solicite a mi enrutador una dirección IP única, dentro el mismo segmento de red que este mi host (equipo físico de trabajo) y cuando pfSense la obtenga será un equipo más en la red de forma independiente entre mi host y pfSense simulando que los demás equipos que estén dentro de la red de mi enrutador son parte de una red **WAN** como **internet**. Este diseño es ideal para nosotros que estamos elaborando una guía desde nuestros hogares, donde contamos con una conexión inalámbrica o cableada a través de un enrutador o módem proporcionado por nuestro proveedor de servicios residencial.

Como comentario adicional: Otra opción válida sería configurar el adaptador en m**odo NAT**, lo cual realiza una traducción de direcciones de red (NAT) entre mi host y la máquina virtual utilizando los drivers de VMware Workstation. Ambas configuraciones tienen como objetivo permitir que la máquina virtual de pfSense tenga acceso a internet. Esto se logra a través del enrutamiento entre la máquina virtual de pfSense, el host, el enrutador y, finalmente, hacia internet, lo que simularía de igual forma una conexión **WAN** de manera eficiente.

Como ya hemos configurado el primer adaptador, ahora necesitamos agregar dos nuevos adaptadores de red a nuestra máquina virtual de pfSense. Para hacerlo, simplemente presionamos el botón “**Add**”, luego seleccionamos la opción “**Network Adapter**” y finalmente hacemos clic en “**Finish**” tienes un ejemplo de cómo hacerlo en **Figura 26.**

Figura 26

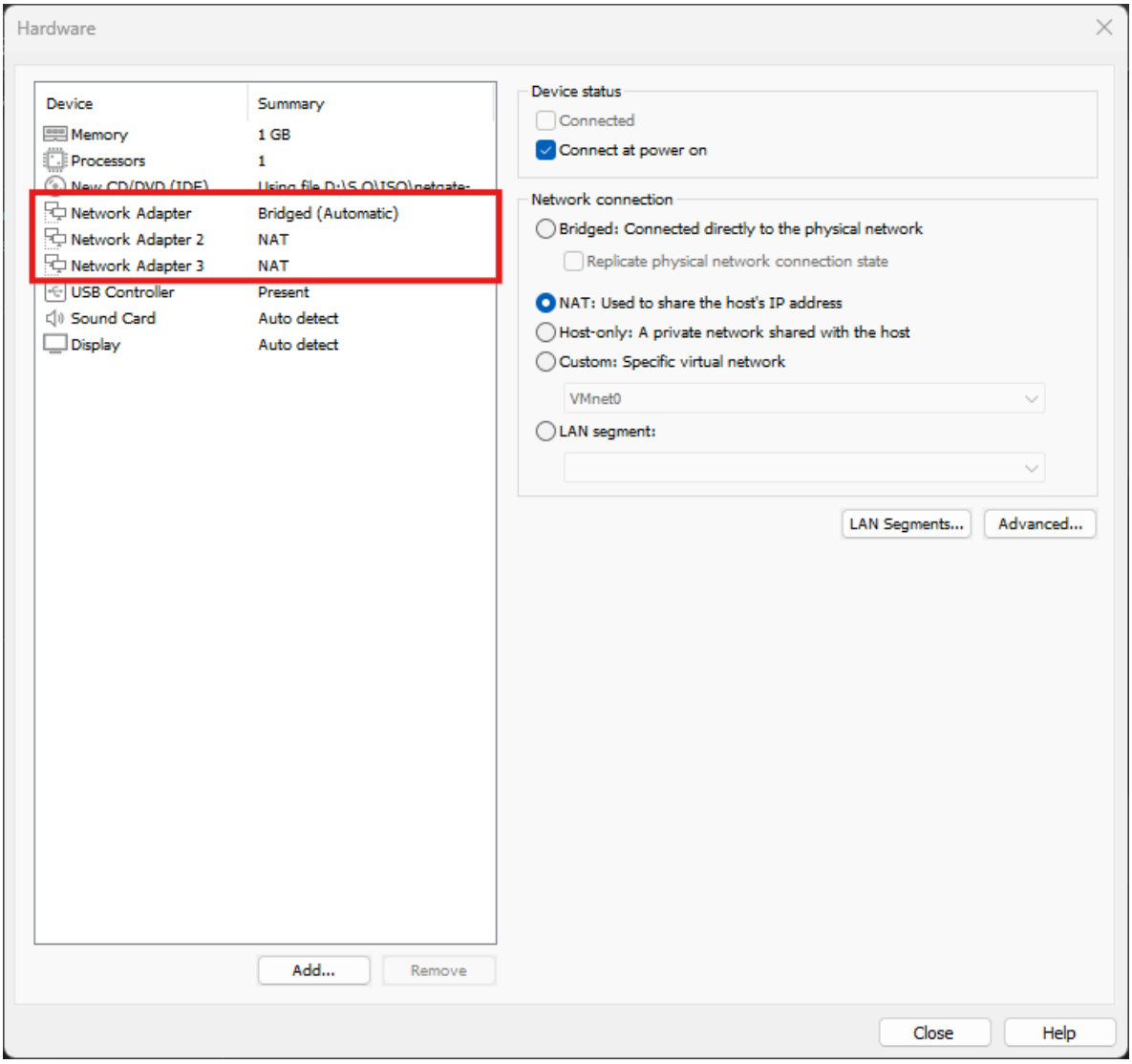
Asistente de configuración: Añadir adaptadores de red a la máquina virtual de pfSense



Nota: Dado que necesitamos agregar dos adaptadores de red adicionales, deberás repetir este proceso dos veces para asegurarte de tener tres adaptadores de red requeridos a como están en **Figura 27.**

Figura 27

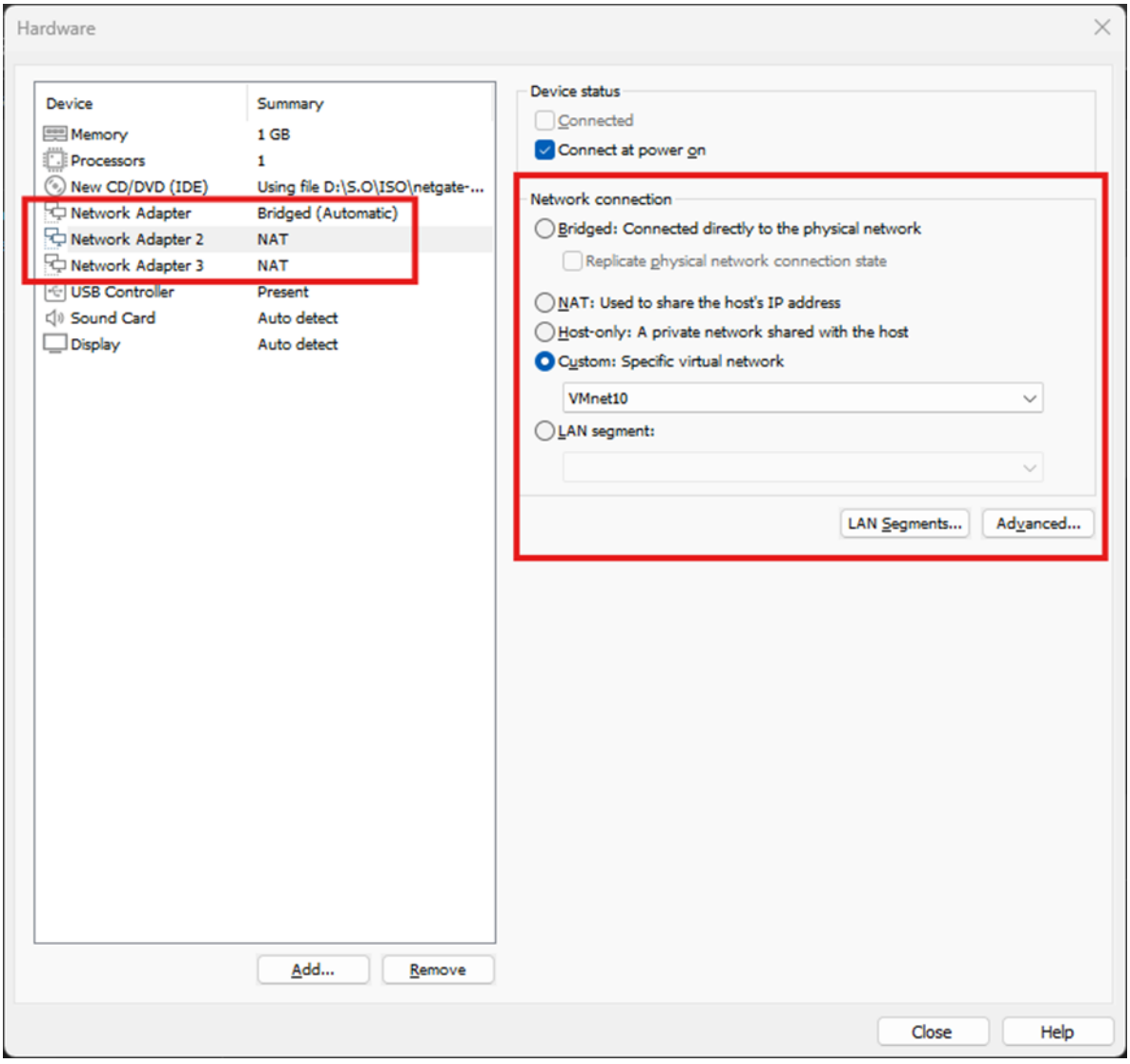
Asistente de configuración: Resumen de adaptadores de red existentes en la máquina virtual de pfSense



Ahora, deberías ver tres adaptadores de red en la configuración de la máquina virtual. Recuerda que ya hemos configurado uno como la interfaz **WAN**. Los otros dos adaptadores corresponderán a las redes **LAN** y **DMZ**, que configuraremos a continuación:

Figura 28

Asistente de configuración: Resumen de las configuraciones que puedes modificar en un adaptador de red en la máquina virtual de pfSense



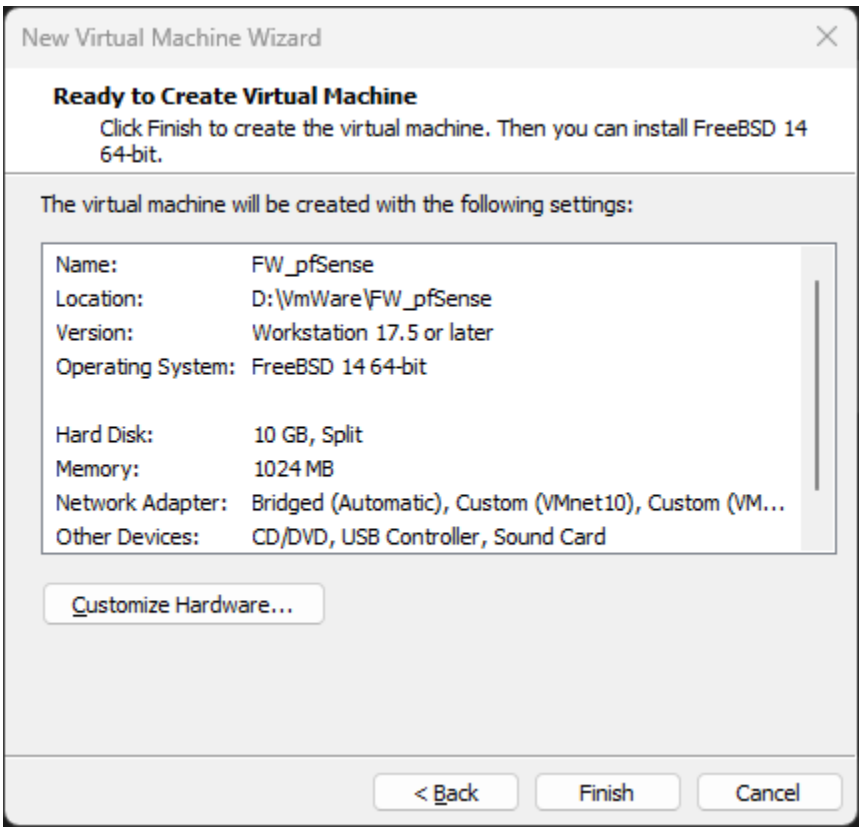
El **adaptador número 2** de **Figura 28** lo configuraré en la parte superior derecha como "**Custom Specific Virtual Network"** en la red virtual interna **VMnet10**, mientras que el **adaptador número 3** se configurará de la misma manera, pero en la red **VMnet11**. Esto tiene el objetivo de crear redes internas aisladas, donde solo haya comunicación entre mi host y los

dos segmentos de red, **LAN** y **DMZ** respectivamente, utilizando el firewall de pfSense como intermediario.

Una vez que hayamos hecho estas configuraciones en los adaptadores de red, podemos presionar “**Close**” como en la **Figura 28** para finalizar el asistente de configuración de la máquina virtual.

Figura 29

Asistente de configuración: Resumen de configuraciones que hemos realizado del hardware de la máquina virtual de pfSense

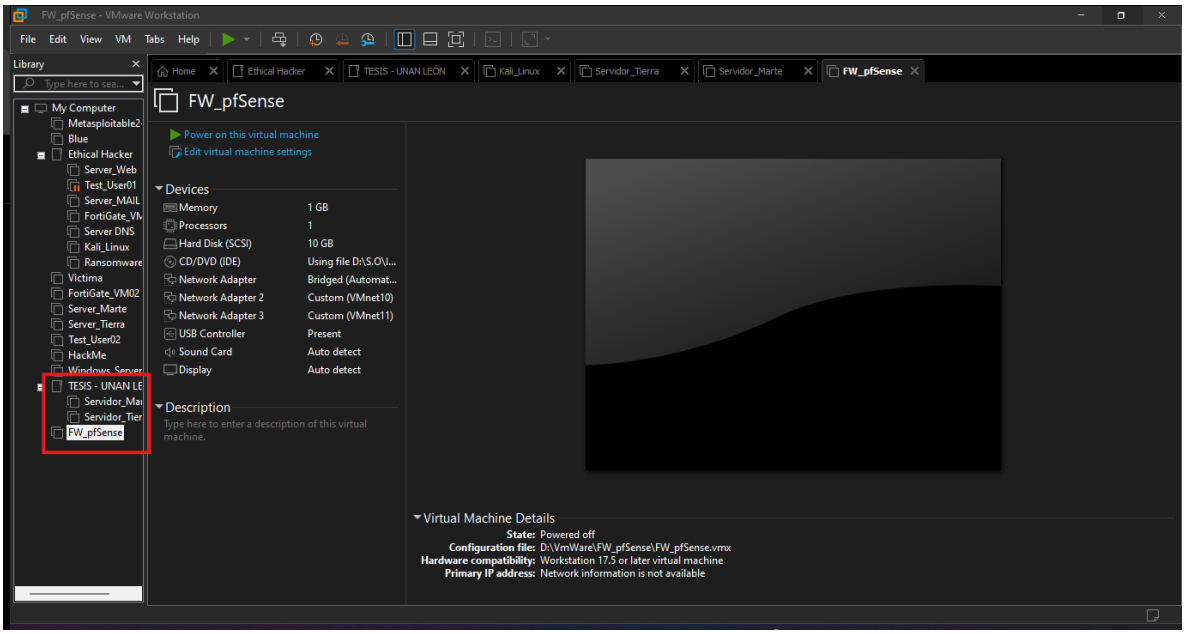


Nota: Una vez realizados los cambios en el hardware de la máquina virtual de pfSense, la configuración debería verse de la siguiente forma. Solo nos queda hacer clic en “**Finish**”, y así se creará la máquina virtual que alojará el sistema pfSense.

En el **Dashboard** de **Figura 30,** podrás ver la máquina virtual que acabamos de crear, junto con toda la información relevante que hemos configurado. En la parte izquierda, aparecerán todas las máquinas virtuales que hayas creado. Es posible que en tu caso solo veas la máquina recién creada llamada **FW_pfSense**; en mi caso, ya tengo varias. Recomiendo que, en la medida de lo posible, agrupemos las máquinas virtuales relacionadas para mantener una mejor organización. Por ejemplo, yo tengo un grupo llamado **TESIS – UNAN LEÓN**, donde organizo las máquinas virtuales correspondientes a nuestro proyecto

Figura 30

Dashboard general de la máquina virtual de pfSense



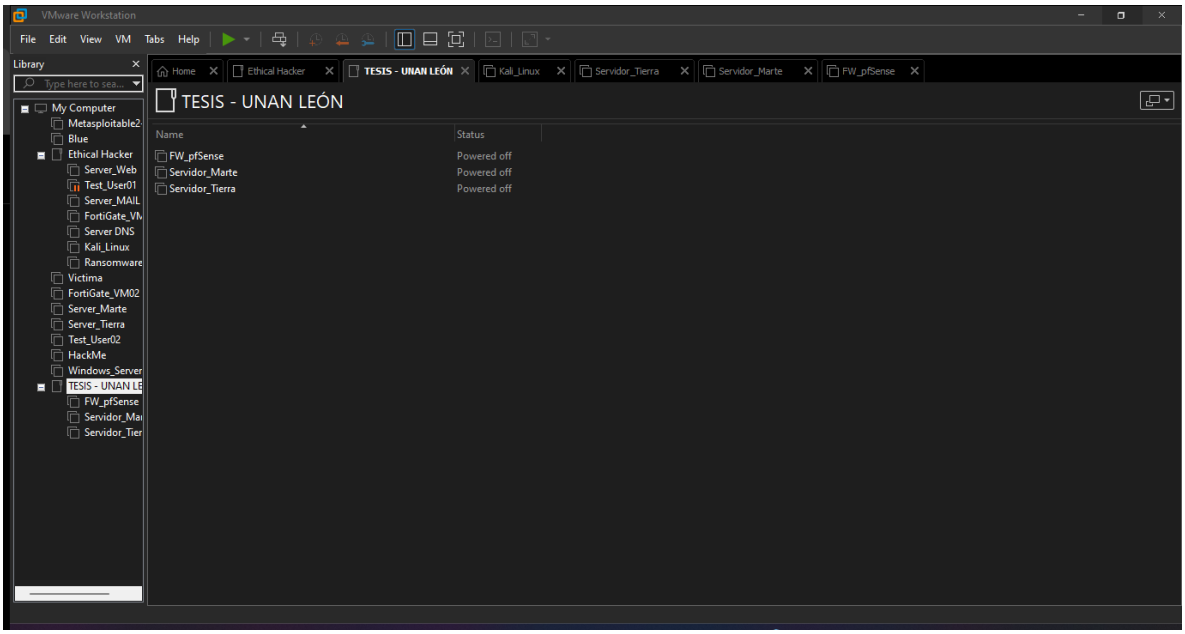
Si agrupas las máquinas virtuales, se verán de una manera más organizada, lo que facilita su gestión. Si no sabes cómo crear un **grupo o folder** en VMware Workstation (como se le llama específicamente en VMware), solo debes seguir los siguientes pasos:

1. Dirígete a la parte superior izquierda como en la **Figura 31** en la sección de “**Library”** y haz clic derecho posteriormente selecciona en “**New Folder**”.

2. Asigna un nombre al folder que tenga relación con tus proyectos o máquinas que estes trabajando en su momento.
3. Por último, ubícate sobre la máquina virtual que acabas de crear en este caso es **FW_pfSense**, y simplemente arrástrala hacia el nuevo folder que acabas de crear en este caso **TEST-UNAN LEÓN**.

Figura 31

Resumen del folder de TESIS UNAN LEÓN



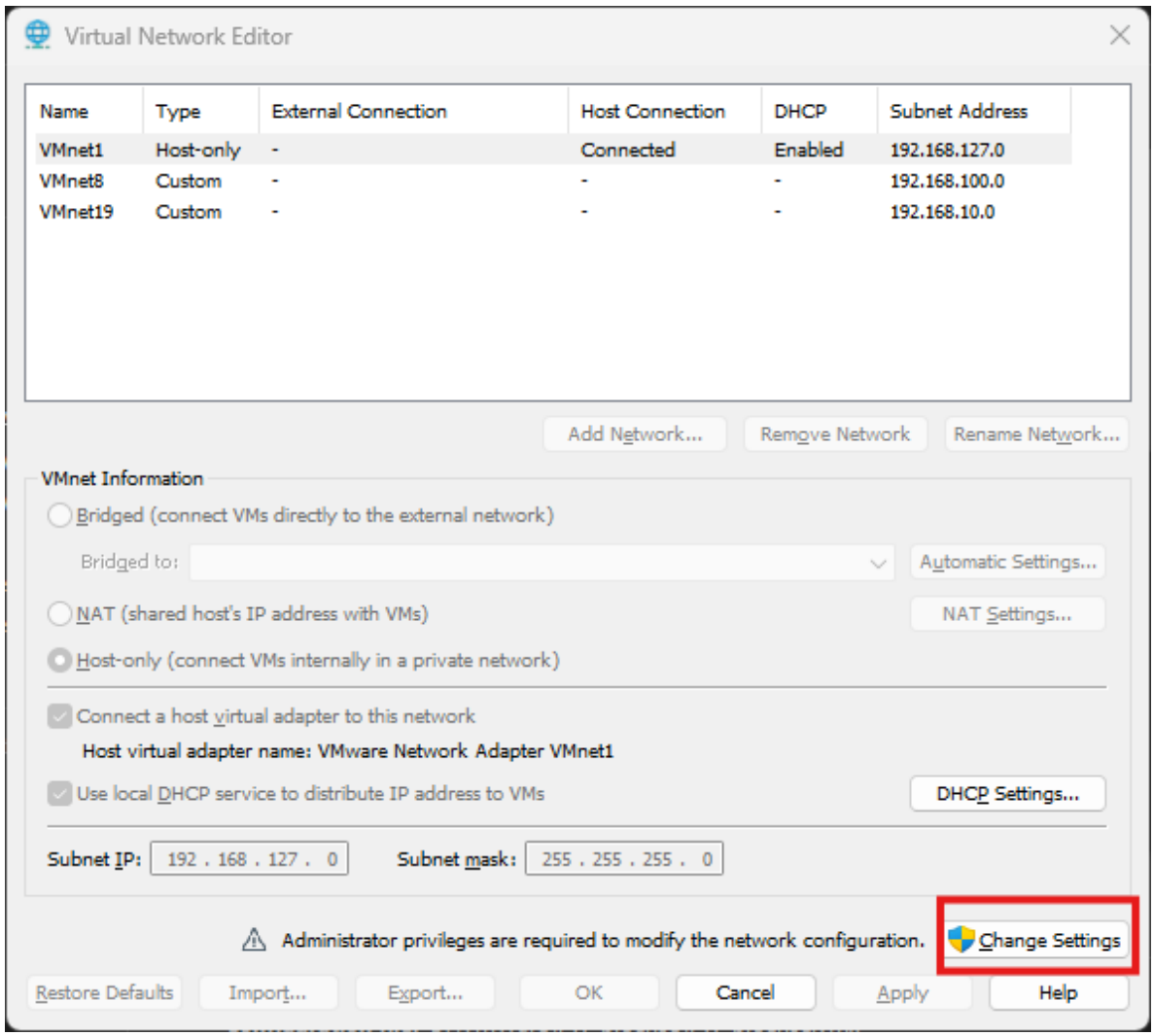
Nota: Este método te ayudará a mantener una estructura más ordenada y a localizar tus máquinas virtuales de manera rápida y eficiente.

Por otro lado, es recomendable revisar y ajustar la configuración del "**Virtual Network Editor**" en VMware Workstation para asegurarnos de que las redes virtuales configuradas para los adaptadores de red (**VMnet10 y VMnet11**) funcionen correctamente. Sigue estos pasos para evitar errores:

1. **Abrir el “Virtual Network Editor**”: Puedes hacerlo desde el menú principal de VMware Workstation en “**Edit”** > “**Virtual Network Editor”** o usando un atajo como “**Ctrl + D**”.

Figura 32

Resumen de las redes en Virtual Network Editor



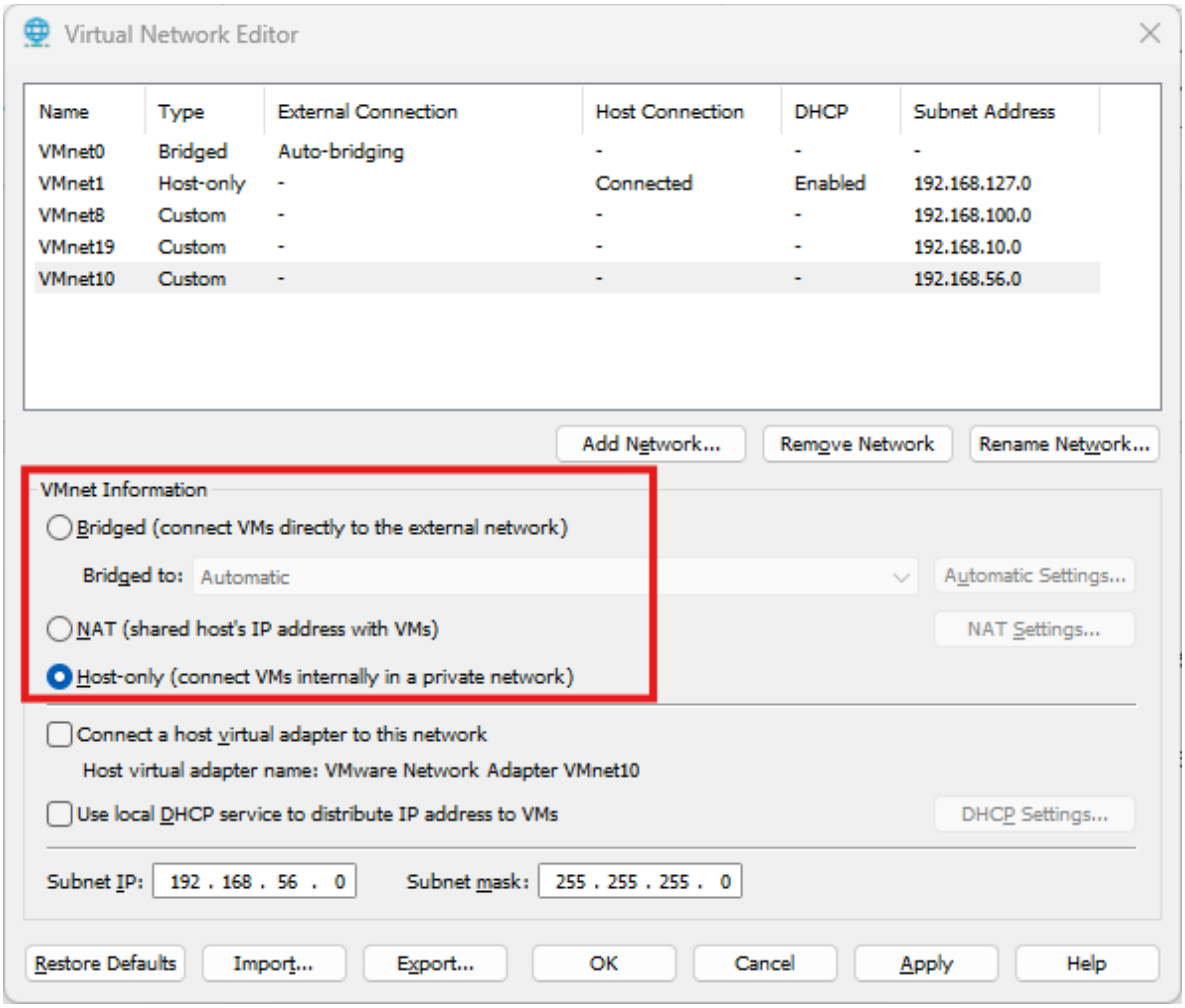
2. **Habilitar Cambios**: Una vez dentro, habilita las modificaciones haciendo clic en “**Change Settings”** (esto podría solicitar permisos de administrador).
3. **Agregar o Seleccionar: VMnet10 y VMnet11**:

- Si las redes VMnet10 y VMnet11 no están creadas, selecciona “**Add Network”** y crea cada una.
- Si ya están en la lista, selecciónalas.

4. **Configurar cada red como Host-Only o Custom**:
   - Para ambas redes (**VMnet10 y VMnet11**), selecciona la opción “**Host-Only”** o “**Custom”**, según lo previsto en la topología en la **Figura 5**.
   - La configuración “**Host-Only”** aísla completamente la red, permitiendo solo la comunicación entre las máquinas virtuales y el host.
   - **“Custom”** te permite asignar las redes que configuraste en los adaptadores 2 y 3 que hemos creado para la máquina virtual de pfSense.
   - Puedes tomar de referencia **Figura 33** para guiarte en este paso.
5. **Asegurar el Aislamiento:**
   - No habilites otras opciones como “**NAT”** o “**Bridged”**, ya que estas podrían permitir acceso externo o hacer un enrutamiento innecesario.
   - No habilites el servidor “**DHCP”**.
   - No habilites conectar **un adaptador virtual al host**.
6. **Aplicar Cambios:**
   - Una vez hayas verificado que “**VMnet10”** y “**VMnet11”** están configuradas correctamente como “**Host-Only**” o “**Custom**”, presiona “**Apply**” y luego “**OK**” para guardar los cambios.

Figura 33

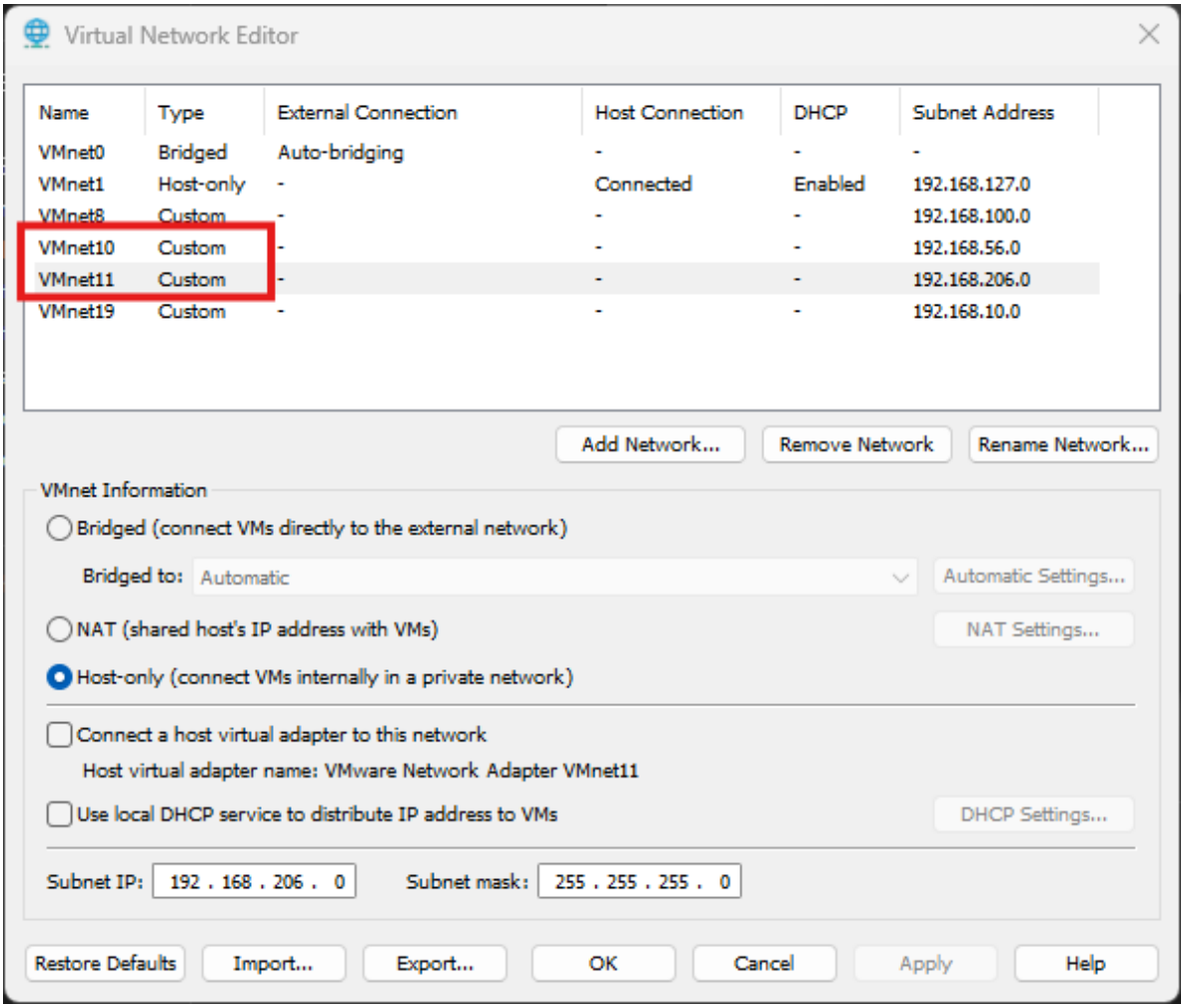
Resumen de las configuraciones que se pueden aplicar a los adaptadores de red de VMware



Al hacer esto, te asegurarás de que las redes internas (**LAN** y **DMZ**) estén correctamente aisladas, conforme a lo planificado en el diseño de la solución de seguridad perimetral con pfSense que hemos creado en **Figura 5**.

Figura 34

Resumen de las configuraciones que realizamos para VMnet10 y VMnet11



8.2.2 Instalación de pfSense

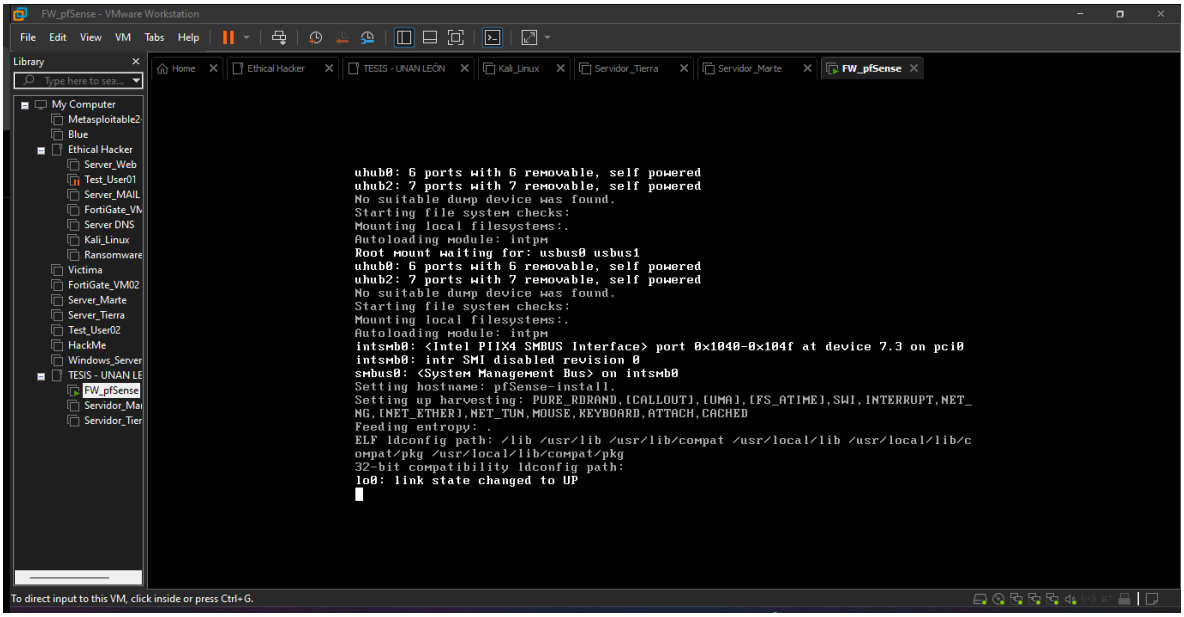
En la fase anterior de esta guía, creamos la máquina virtual de pfSense en VMware Workstation que alojará el sistema operativo de pfSense. Ahora, avanzamos al siguiente paso: encender la máquina virtual recién creada e instalar el sistema operativo pfSense.

- **Inicializando la Máquina Virtual:**

- **Selecciona la Máquina Virtual**:
    - En el **Dashboard** de opciones de VMware Workstation, haz clic en la máquina virtual que has creado para pfSense (llamada FW_pfSense).
- **Iniciar la Máquina Virtual**:
    - Haz clic en el botón **Play** (o **Iniciar**) para encender la máquina virtual.
    - Esto abrirá una ventana de VMware Workstation y veras una consola donde podrás apreciar el proceso de arranque de la máquina virtual como en la **Figura 35.**

Figura 35

Vista de arranque de la máquina virtual de pfSense



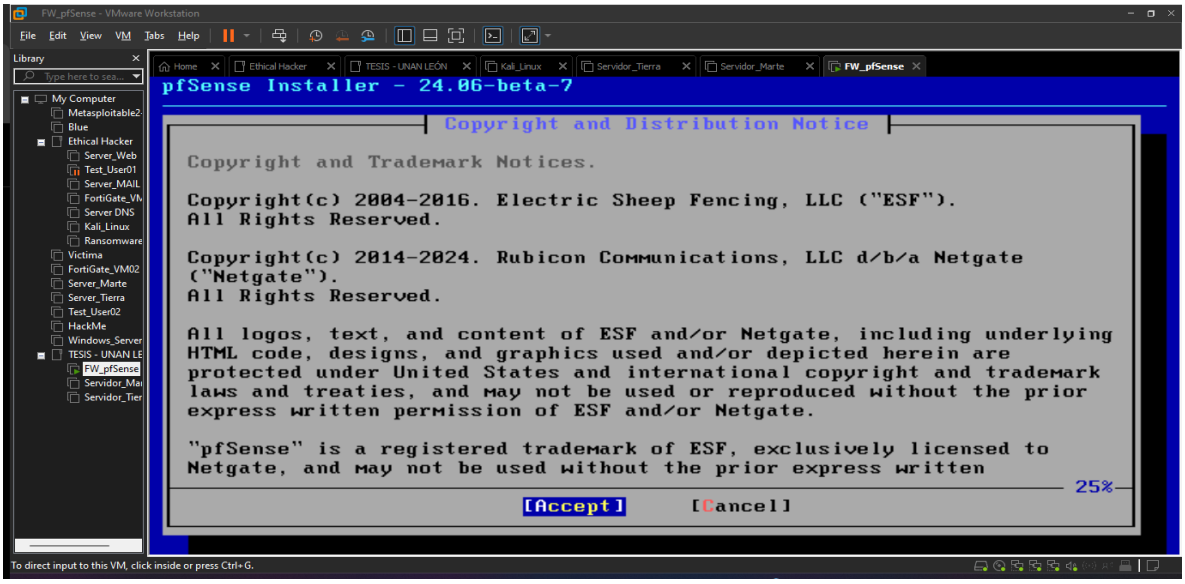
- **Instalar el sistema operativo de pfSense**

Al arrancar, la máquina virtual debería leer automáticamente el archivo de instalación de pfSense que hemos configurado anteriormente el cual era un .iso. Si todo está bien, verás la pantalla de bienvenida de pfSense y te mostrara las condiciones de uso de su licencia open

sourse como se ve en **Figura 36** , bastara en que aceptamos la licencia de uso para avanzar en nuestra instalación.

Figura 36

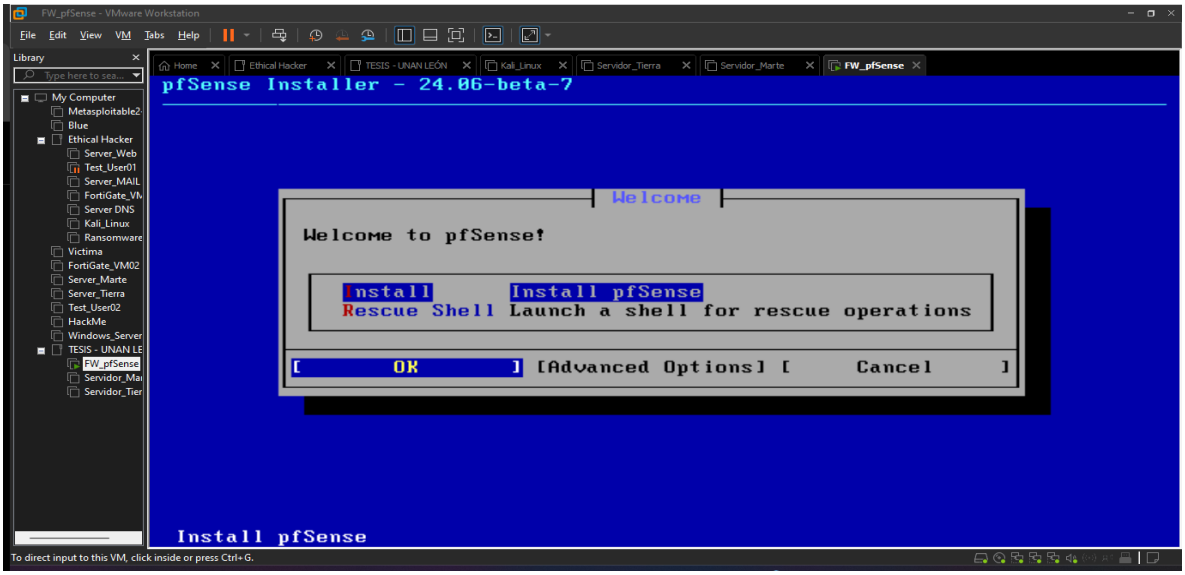
Resumen de la licencia de uso del software de instalación de pfSense



- Selecciona la opción de “**Install**” (Instalar) y presiona “**Enter**” como en la **Figura 37**.

Figura 37

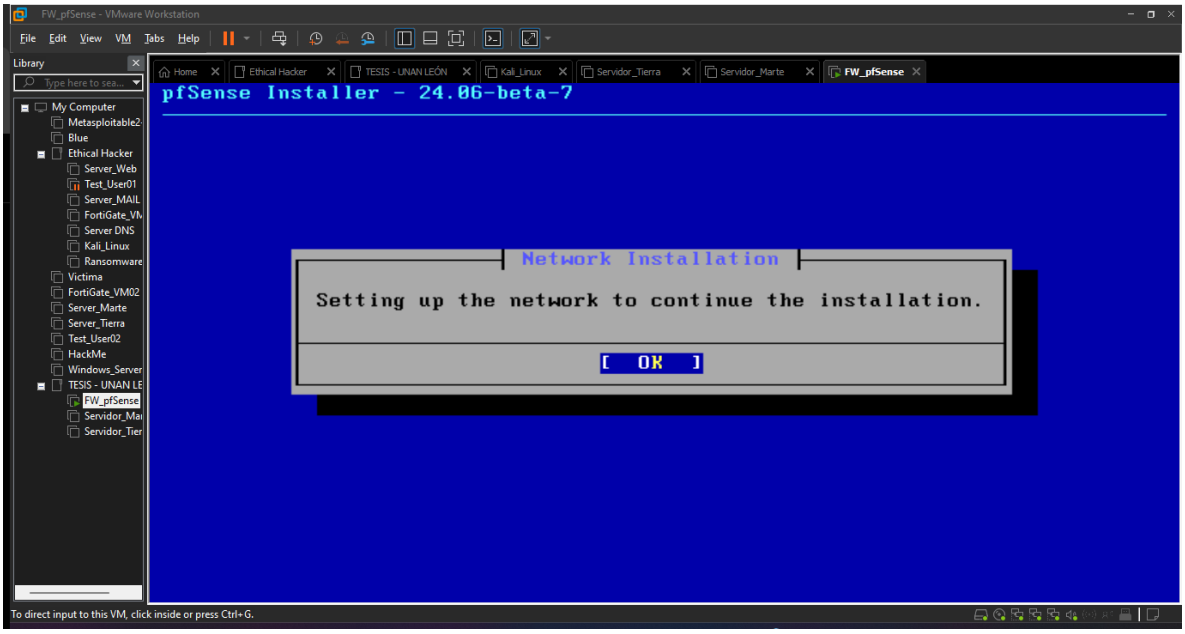
Vista previa de inicio de instalación de pfSense



Lo primero que hay que configurar en pfSense son las interfaces de red, por ende, nos ubicamos en “**OK**”, esto lo podemos hacer presionando la letra “**TAB**” y para finalizar en este paso bastara con un “**ENTER**”.

Figura 38

Proceso de instalación de pfSense: Proceso inicial



8.2.3 Configuración inicial de pfSense y establecimiento de la red

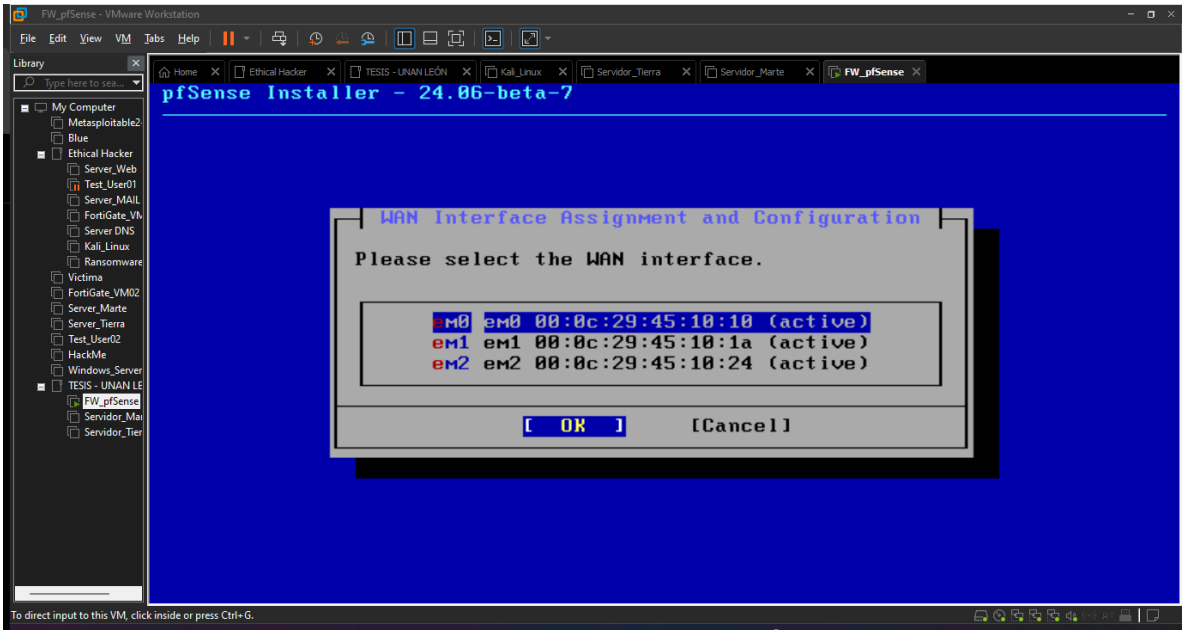
Como podemos observar, se muestran los tres adaptadores de red que configuramos previamente en **Figura *27*** . Ahora es el momento de seleccionar cuál de estos adaptadores quedará como interfaz **WAN** en pfSense.

- Disponemos de tres opciones
    1. **em0**
    2. **em1**
    3. **em2**

Según la configuración previa en la máquina virtual en pfSense, designaré **em0** como la interfaz **WAN**, que corresponde al adaptador número uno que configuramos en **Figura 28** en modo puente para simular la red **WAN**.

Figura 39

Resumen de las interfaces de red que detecta la máquina virtual de pfSense



Verifiquemos que el adaptador “**em0”** sea efectivamente el que configuramos en la máquina virtual como el adaptador **WAN**. Para ello, presionaremos “**CTRL + D”** en el menú principal de **VMware Workstation**, lo que abrirá las opciones de la máquina virtual de pfSense. A continuación, nos moveremos hasta la sección del adaptador de red número uno, haremos clic en “**Advanced”**, y se desplegará una ventana con información avanzada del adaptador de red seleccionado como en la **Figura 40**.

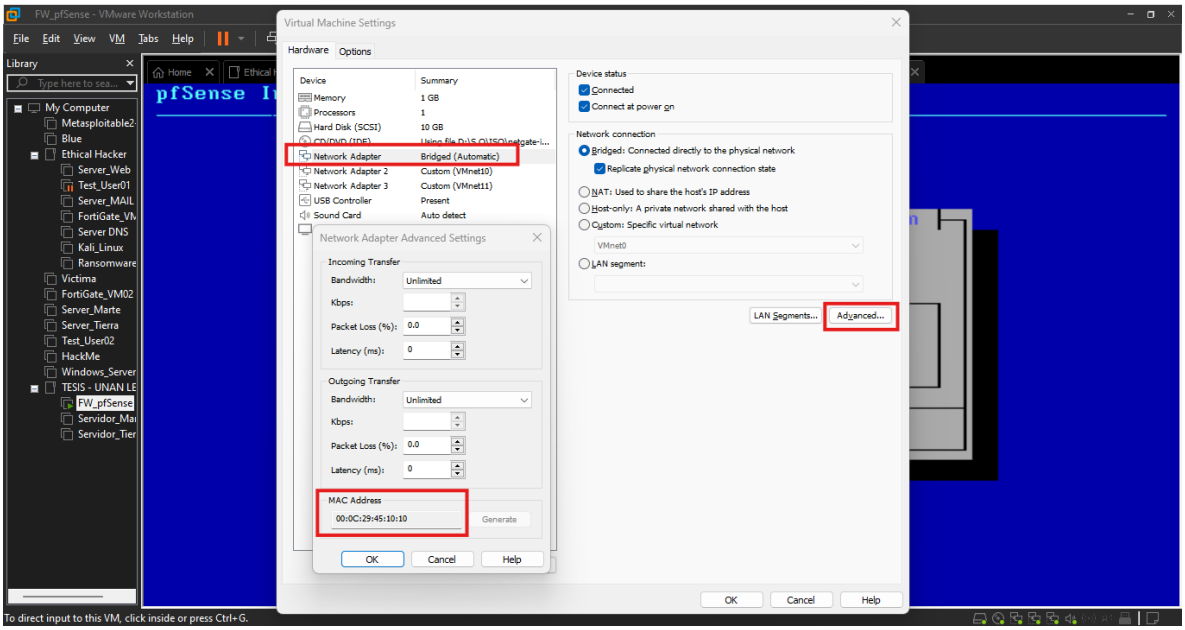
En esta nueva ventana, podremos observar la dirección “**MAC”** del adaptador de red número uno, el cual debe coincidir con una de las interfaces de red detectadas en el sistema operativo de pfSense, en este caso la “**MAC”** del adaptador número uno, coincide con la MAC de la interfaz de red detectada “**em0”** por lo que es la interfaz “**em0”** es la que dejaremos como

una interfaz “**WAN”.**

.

Figura 40

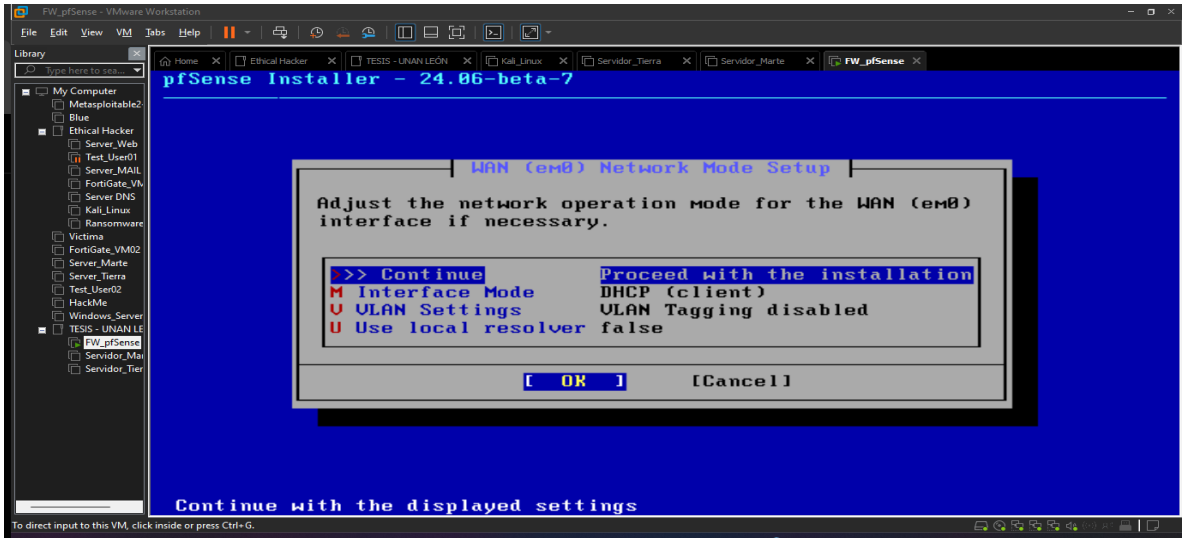
Opciones avanzadas de los adaptadores de red en VMware Workstation Pro



Es hora de volver a la configuración en el sistema de pfSense, y luego de seleccionar la interfaz que antes mencionamos, damos en continuar para que se aplique los cambios.

Figura 41

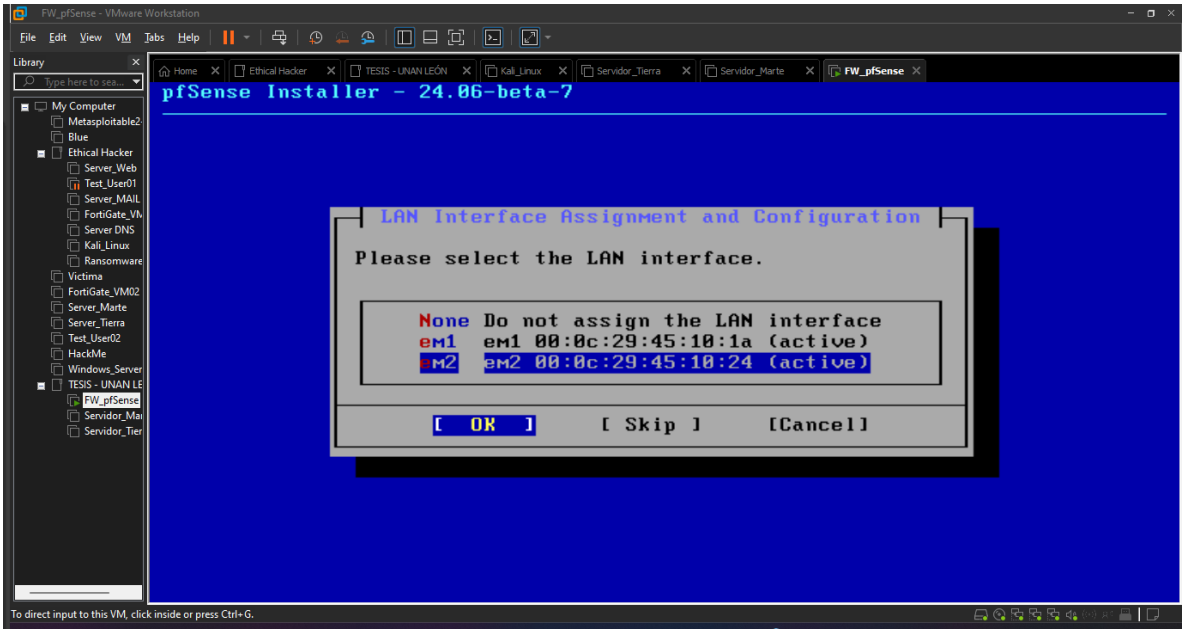
Proceso de instalación de pfSense: Elección de la interfaz WAN



Una vez configurada la interfaz “**WAN”,** en el sistema de pfSense, es momento de elegir la segunda interfaz, que en nuestro diseño de red en la **Figura 5** corresponde a la “**LAN”**. Se puede realizar el paso anterior como referencia, para ubicar que adaptador de red de VMware Workstation corresponde con que interfaz de red detectada en el sistema de pfSense. Por mi parte, ya lo he ubicado y omitiré esta parte.

Figura 42

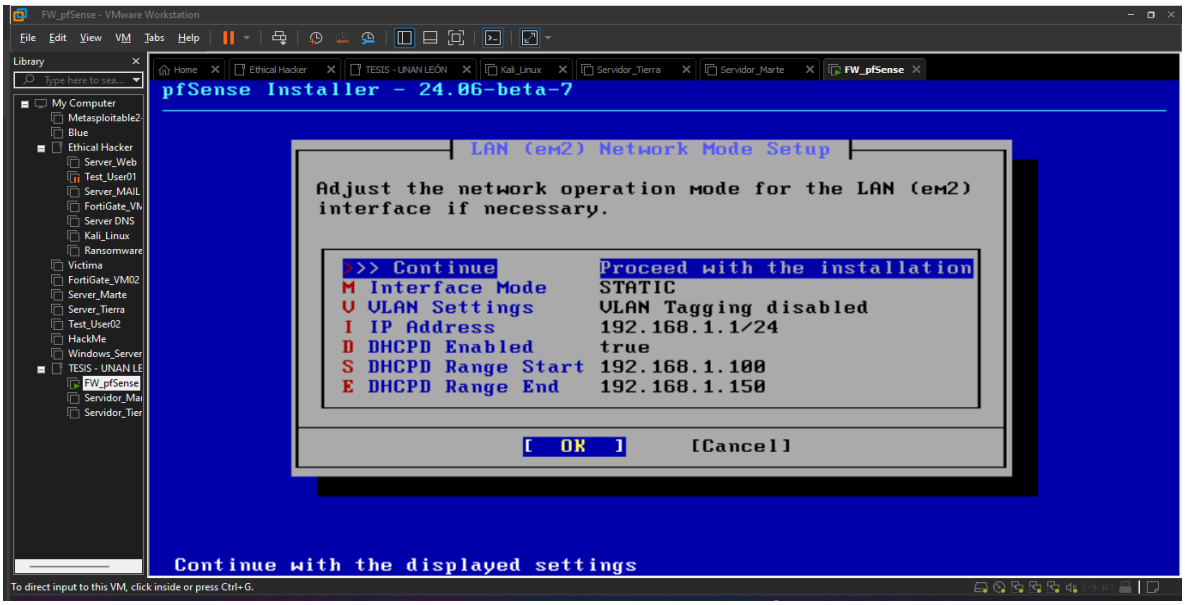
Proceso de instalación de pfSense: Elección de la interfaz LAN



Después de seleccionar la interfaz de red correcta para la **LAN** es momento de, configurar las direcciones IPs de estas interfaces en la siguiente **Figura 43**.

Figura 43

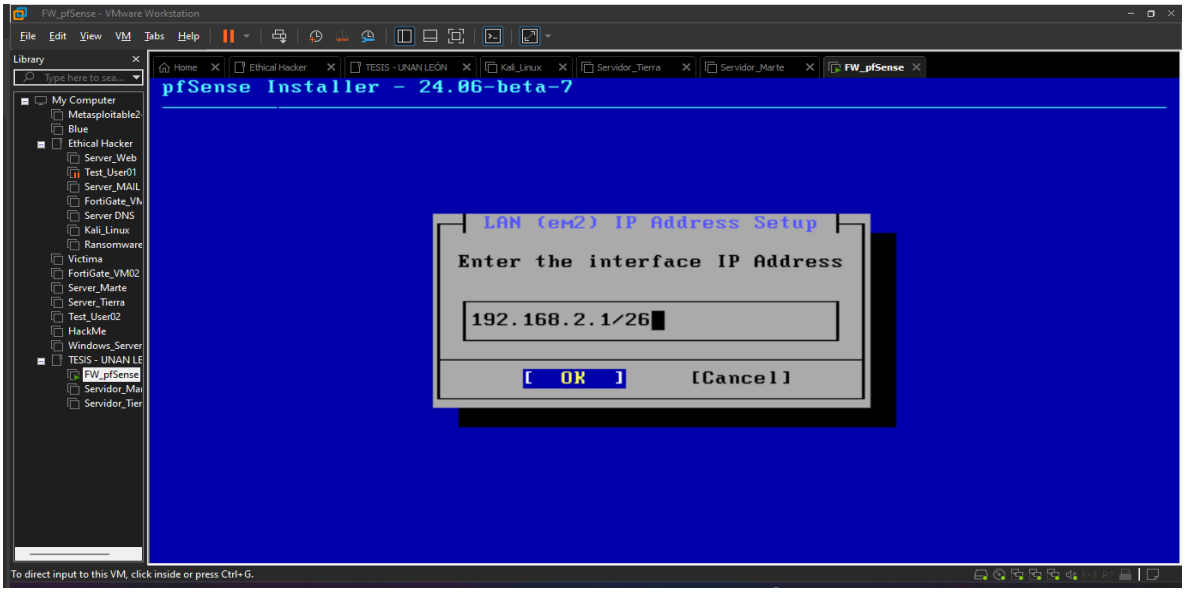
Proceso de instalación de pfSense: Resumen de configuración en las interfaces de red



Debemos configurar la dirección IP, de acuerdo con nuestra topología de red en **Figura *5***, esta dirección IP actuará como “**gateway**” para la red **LAN** será **192.168.2.1/26.**

Figura 44

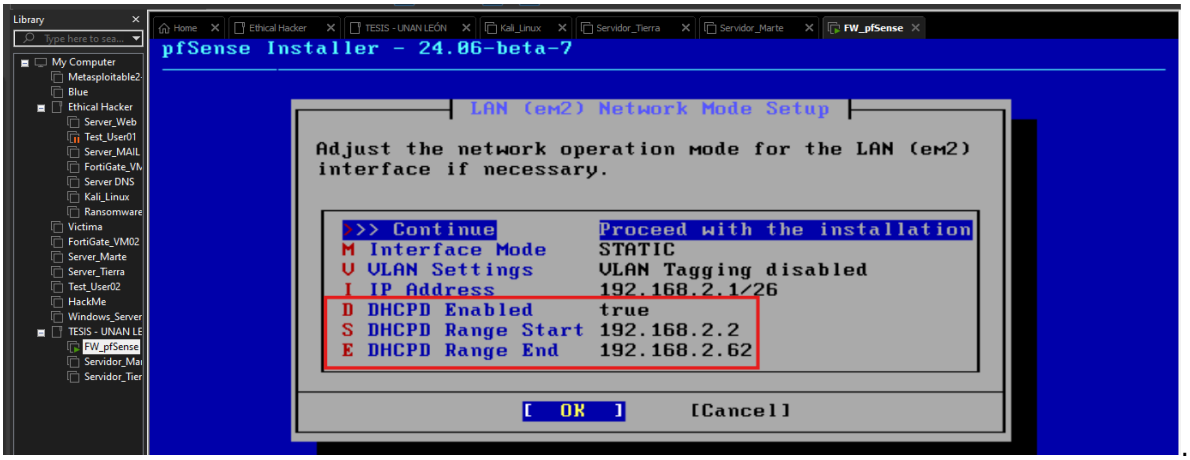
Proceso de instalación de pfSense: Asignación de dirección IP en la interfaz LAN



En este punto configuraremos el rango de asignaciones de direcciones IPs para el servicio de “**DHCP”** que activaremos para la interfaz “**LAN”**. Según nuestra topología de red en **Figura 5**, el rango de hosts disponibles va desde la **dirección IP: 192.168.2.2/26 hasta 192.168.2.62/26**.

Figura 45

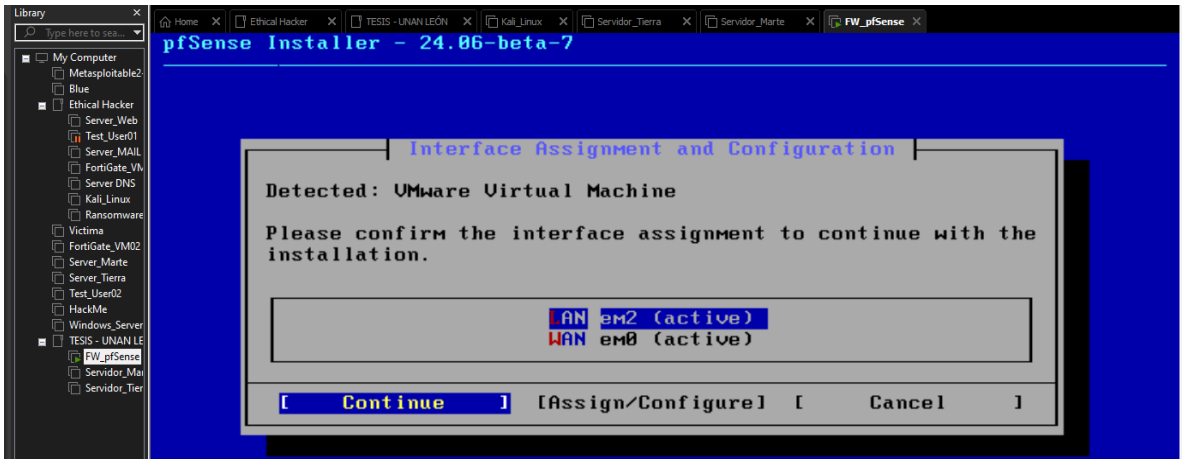
Proceso de instalación de pfSense: Configuración del servicio DHCP en la interfaz LAN



- En la **Figura 45** tenemos el resumen de cómo debería de quedar el servicio "**DHCP"**, basta con dar en "**OK"** con "**TAB"** para continuar.

Figura 46

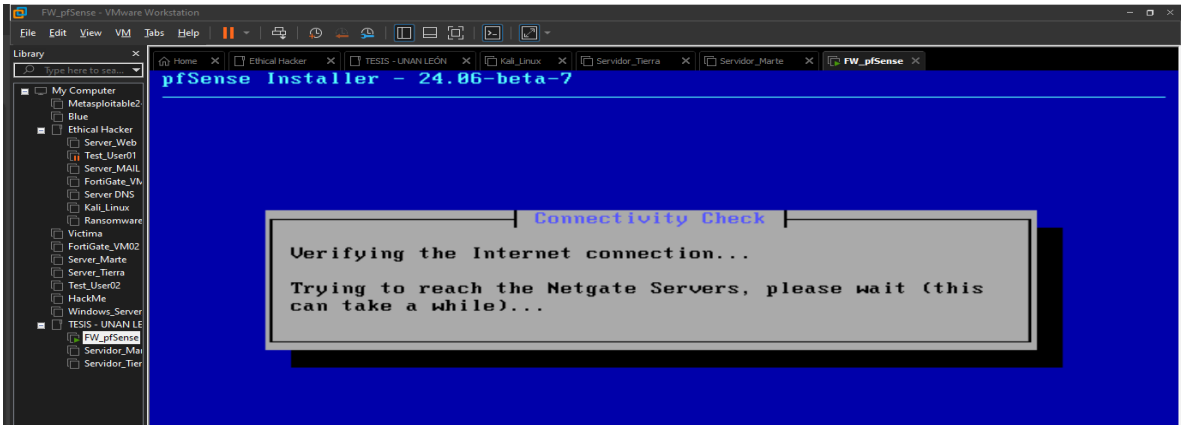
Proceso de instalación de pfSense: Proceso de inicialización de las interfaces de red en pfSense.



En la **Figura 46** podemos observar el proceso de inicialización de las interfaces de red, de igual forma bastará con ubicarnos en "**Continue**" con "**TAB"** y presionar "**ENTER**", después de esto el sistema de pfSense se intentará conectar a los servidores de Netgate.

Figura 47

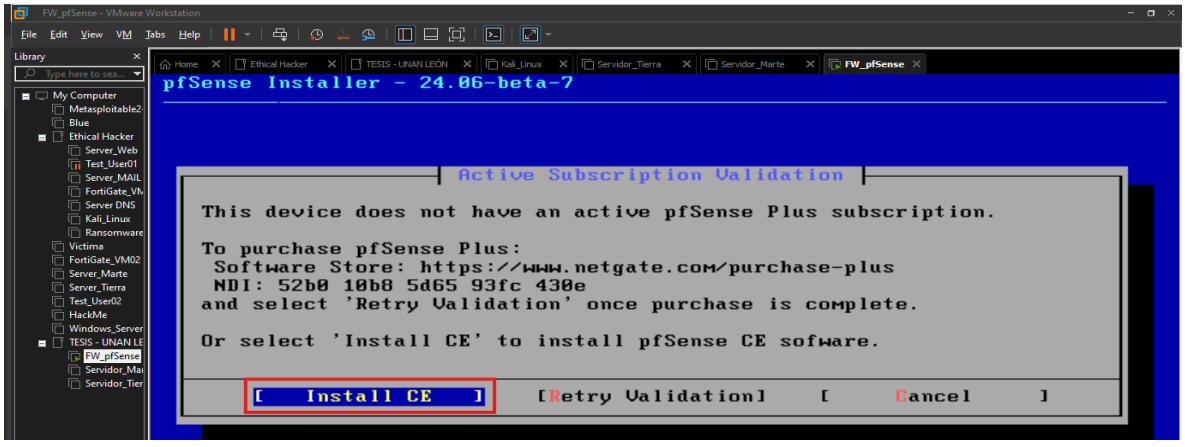
Proceso de instalación de pfSense: Resumen del proceso de conexión con los servidores de Netgate



El propósito de conectarse a los servidores de Netgate es buscar si tenemos un licenciamiento empresarial. Sin embargo, como no contamos con esta opción y no es relevante para nuestra solución, simplemente seleccionamos" Install **CE**".

Figura 48

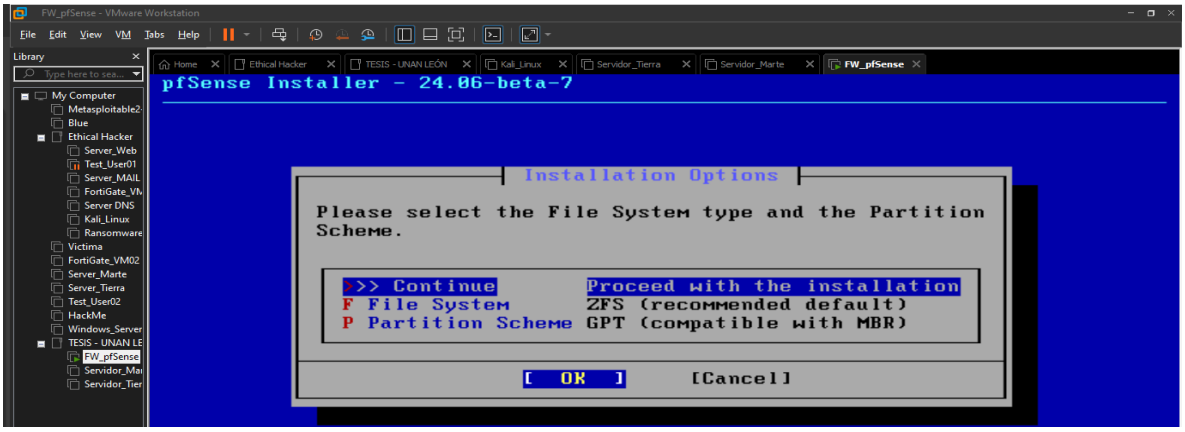
Proceso de instalación de pfSense: Instalamos la licencia de uso open sourse denominada CE



Nuestro siguiente paso es seleccionar el "**modo de instalación"** en el sistema de archivos. Generalmente, la opción predeterminada es adecuada por ende presiona "**Enter"** para continuar.

Figura 49

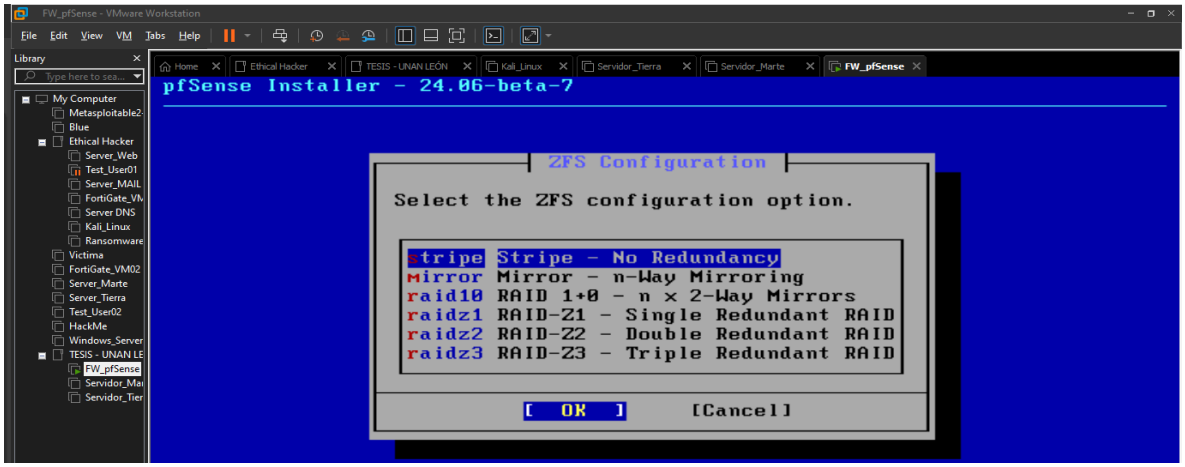
Proceso de instalación de pfSense: Resumen de la instalación de pfSense en el sistema de archivos



De igual forma para efectos de esta solución generalmente, la opción predeterminada es adecuada. Presiona “**Enter”** para continuar.

Figura 50

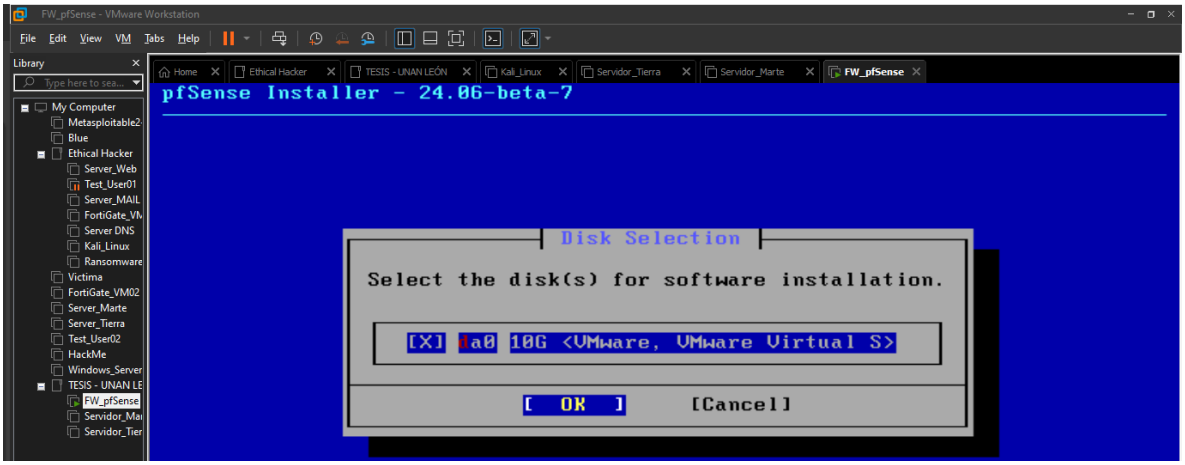
Proceso de instalación de pfSense: Resumen de la instalación del sistema operativo en el sistema de archivos



Basándonos en **Figura 50** seleccionamos la instalación del sistema operativo por defecto en “**Stripe**”.

Figura 51

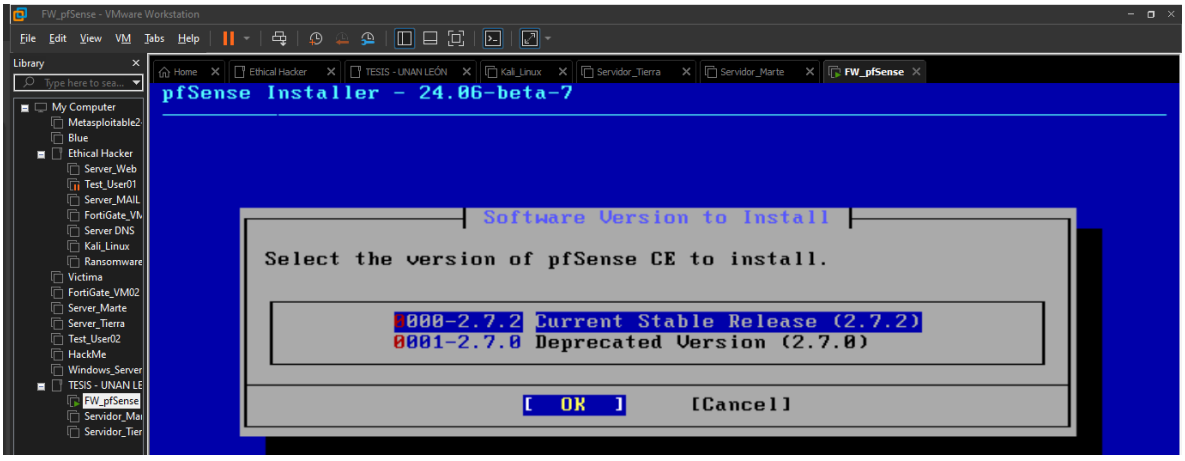
Proceso de instalación de pfSense: Elección de la ubicación en que partición instalar el sistema de pfSense



Seleccionamos la instalación del sistema operativo de pfSense en el único disco duro que tenemos en la máquina virtual como en la **Figura 51** y seleccionamos la versión **2.7.2** de pfSense la cual es la que queremos instalar y avanzamos presionando en "**OK**".

Figura 52

Proceso de instalación de pfSense: Elección de la versión de pfSense a instalar

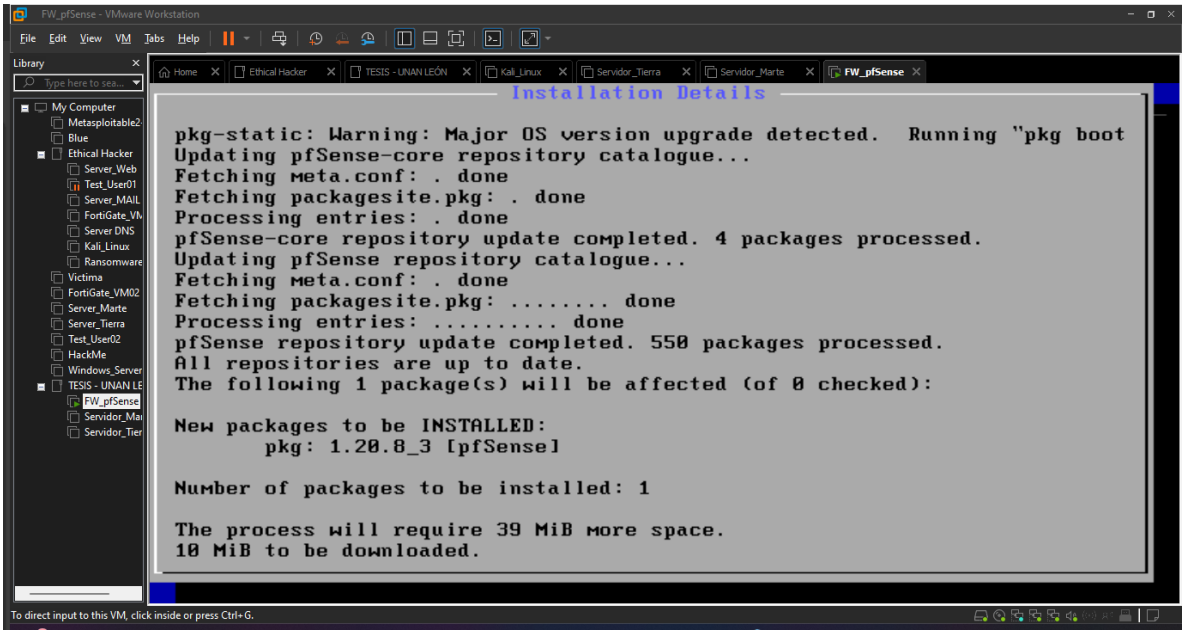


Para finalizar con la instalación del sistema de pfSense en la máquina virtual que hemos creado, el sistema descargará los archivos adicionales necesarios para sus últimas

características y actualización de software. Una vez finalizada la descarga e instalación, bastará con presionar “**Continuar”** para reiniciar.

Figura 53

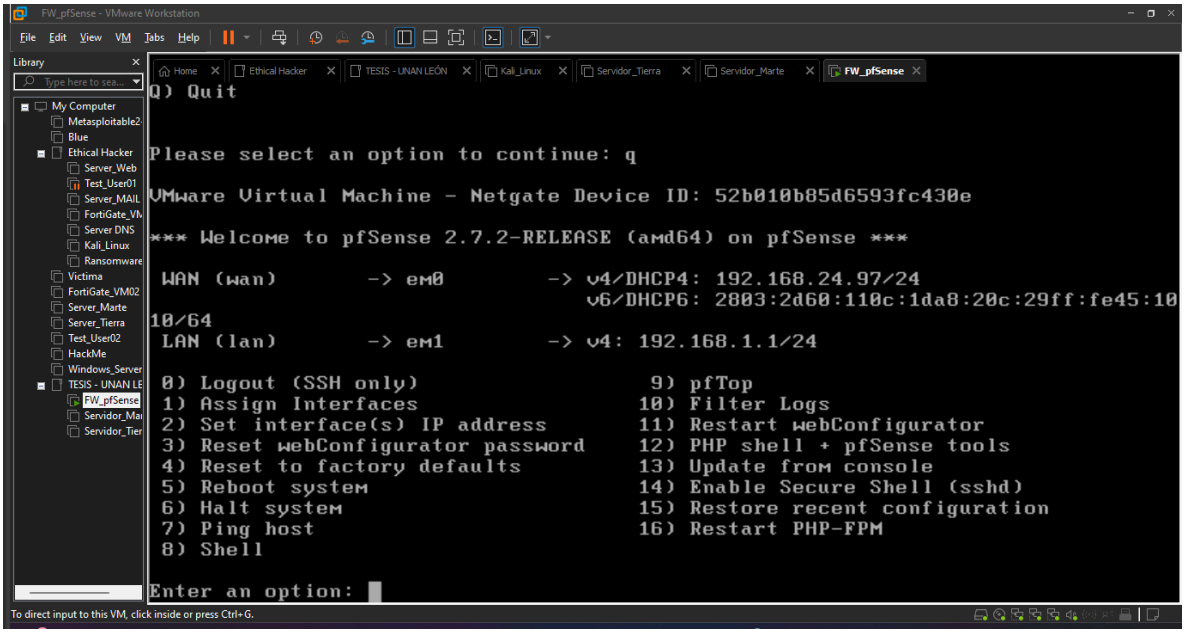
Proceso de instalación de pfSense: Actualización e instalación de las ultimas características de pfSense



Cuando el proceso de carga del sistema finalice, se mostrará el menú principal a través de la consola, similar al siguiente al de **Figura 54.**

Figura 54

Proceso de instalación de pfSense: Menú principal desde la CLI



8.3 Configuración de pfSense y servicios asociados

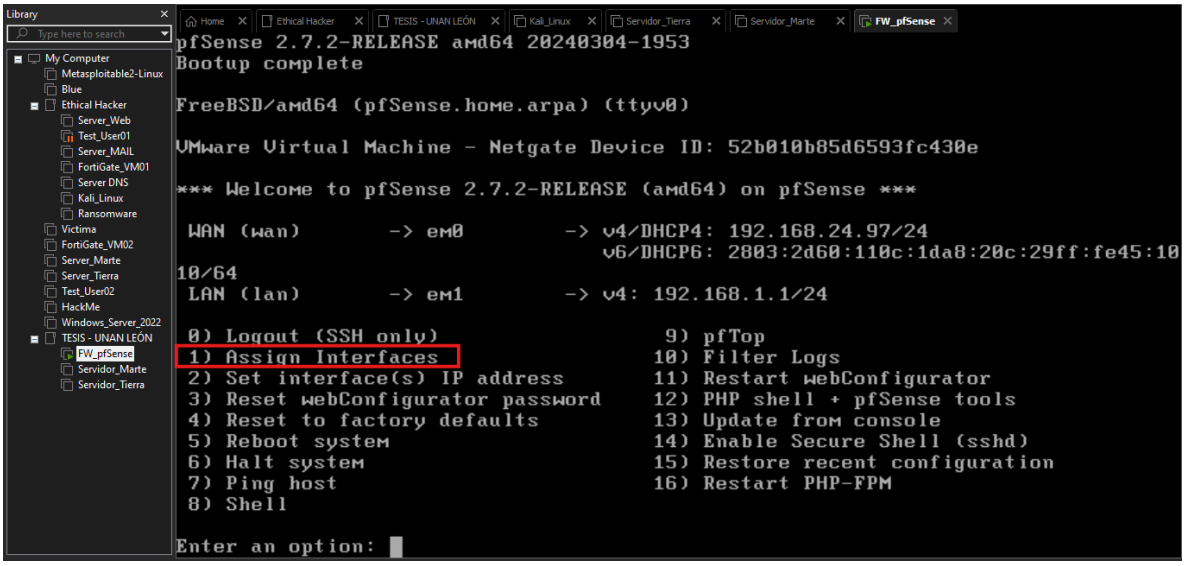
Hemos finalizado la instalación del sistema operativo en la máquina virtual creada. El siguiente paso es ajustar las configuraciones de las interfaces de red. Es común que durante la instalación se configuren dos interfaces, **WAN** y **LAN**, pero en algunos casos la interfaz **LAN** puede restablecerse a sus valores por defecto. Por ello, configuraremos nuevamente las tres interfaces que utilizaremos: **WAN**, **DMZ** y **LAN**.

8.3.1 Configuración de las interfaces WAN, LAN y DMZ en pfSense

El menú principal desde el CLI en pfSense, es un menú interactivo en el que seleccionamos un número correspondiente a una acción específica. En nuestro caso, necesitamos configurar las interfaces de red con los tres adaptadores que habilitamos en la máquina virtual. Para ello, seleccionaremos **la opción 1** en el menú, que nos permitirá asignar las interfaces de red de manera adecuada y es lo que hacemos en **Figura 55**

Figura 55

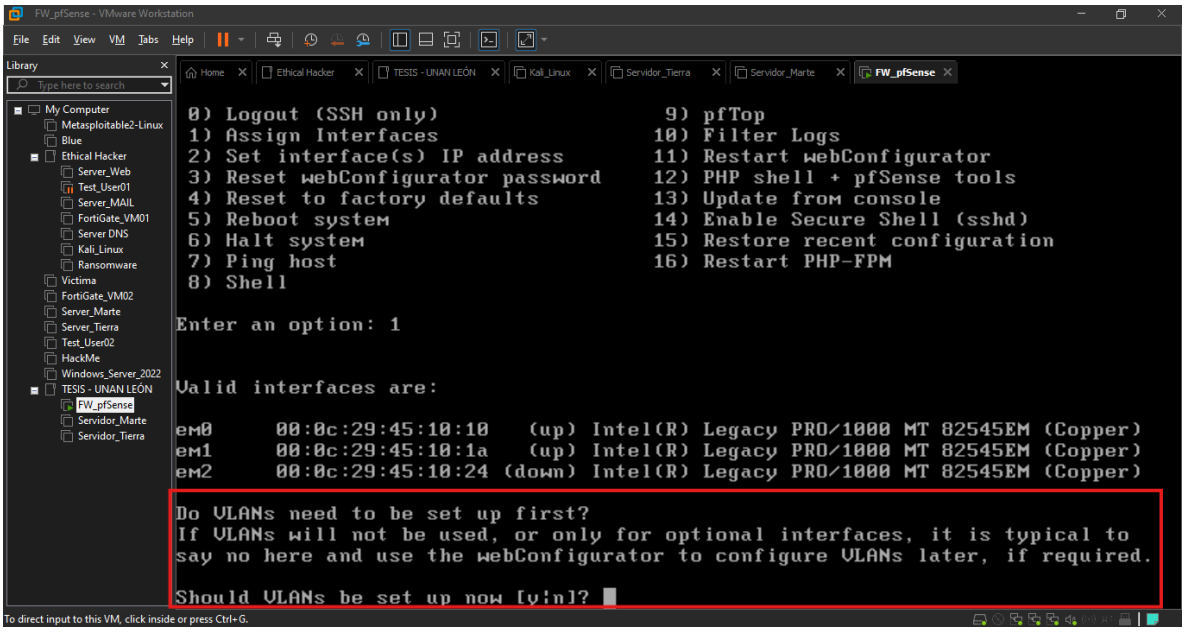
Proceso de instalación de pfSense: Menú de opciones en el CLI



Luego de seleccionar la opción para asignar interfaces, el sistema te preguntará si deseas utilizar **VLANs**. Para los propósitos de esta guía, no será necesario emplear **VLANs**, por lo que seleccionaremos “**No”** en esta opción.

Figura 56

Proceso de instalación de pfSense: Configuración de las interfaces de red mediante CLI



Después de seleccionar “**No”** para no utilizar **VLANs**, es momento de asignar correctamente las interfaces de red que utilizaremos en nuestro firewall pfSense. A continuación, se puede ver cómo quedarán distribuidas las interfaces. He organizado la configuración de las interfaces de red en una **Tabla *2*** para mayor visibilidad y mejor comprensión de lo que estamos realizando:

Tabla 2

Resumen de las configuraciones de red en pfSense

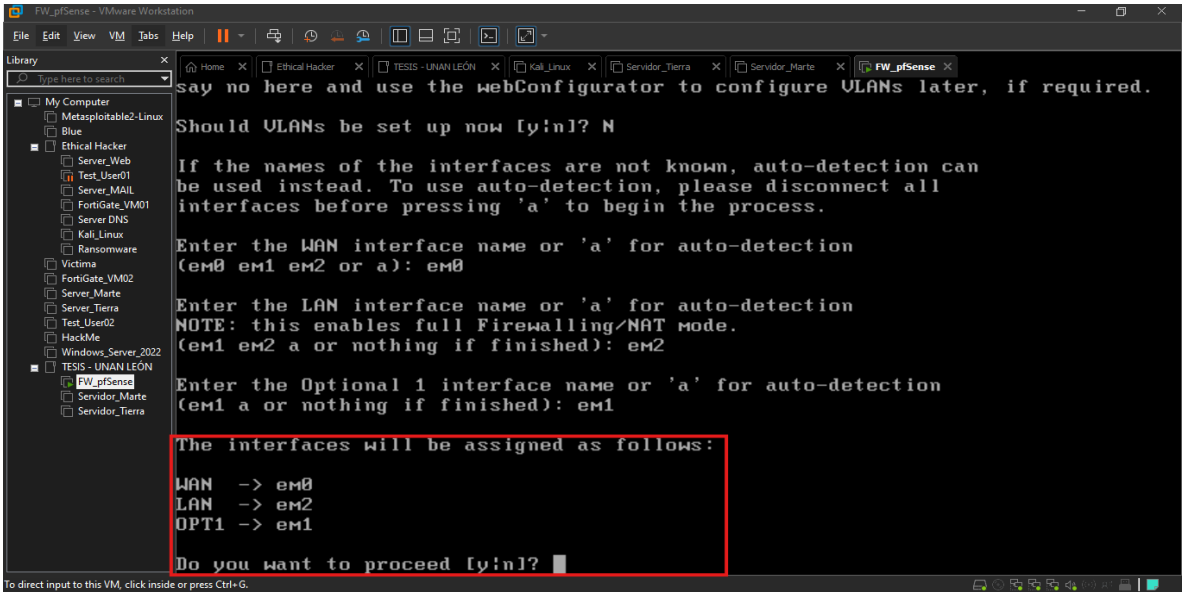
Configuración del hardware de la red				
#	Modo de la interfaz	Nombre del adaptador	Nombre de la interfaz	Número MAC
1	WAN	em0	Network adapter 1	00:0C:29:45:10:10
2	DMZ	em1	Network adapter 2	00:0C:29:45:10:1A
3	LAN	em2	Network adapter 3	00:0C:29:45:10:24

Nota: Es importante mencionar que las direcciones MAC pueden variar en tus adaptadores de red configurados en tu máquina virtual de pfSense, pero eso no afectará la configuración lógica. Solo asegúrate de asignar los adaptadores de red correctamente.

Ahora que hemos definido que la interfaz “**WAN”** será “**em0”**, “**LAN”** será “**em2”**, y la “**DMZ”** estará temporalmente con nombre “**OPT1”** en “**em1”**, en pasos posteriores podremos cambiar su nombre. Si toda la información que configuraste es correcta, avanzamos colocando “**Yes**” y presionamos “**Enter**” como en la **Figura 57**.

Figura 57

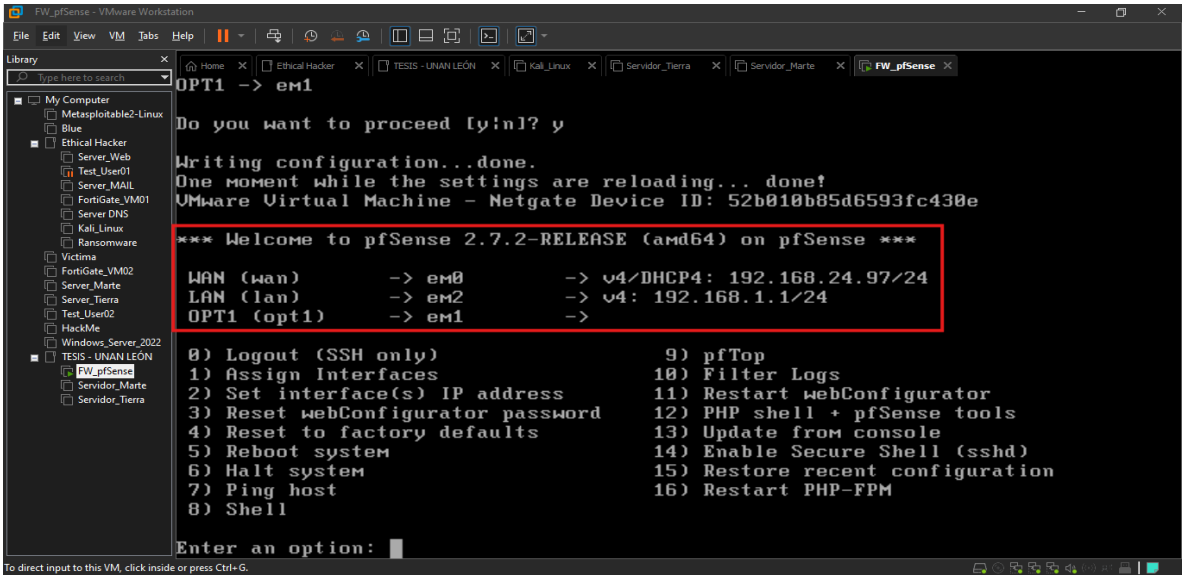
Proceso de instalación de pfSense: Resumen de la configuración en las interfaces de red



Ahora nos debería de salir las tres interfaces que acabamos de asignar en el menú principal como en la **Figura 58**.

Figura 58

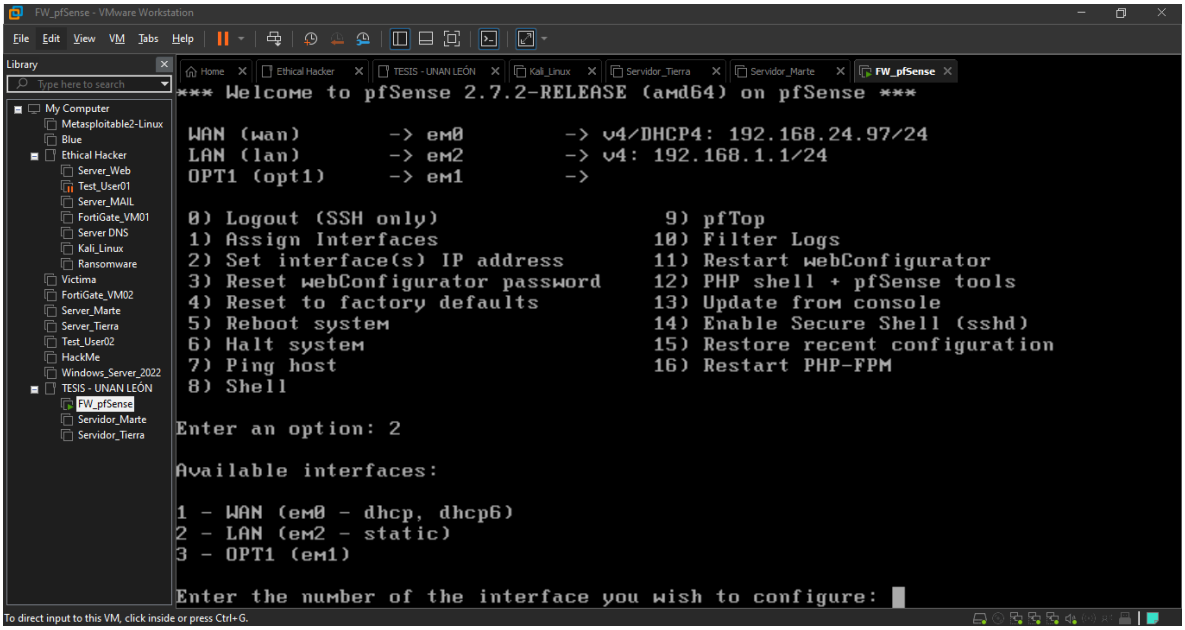
Proceso de instalación de pfSense: Resumen de las interfaces configuradas en el CLI de pfSense



Ahora es momento de asignar las direcciones IPs correctas a las interfaces de red que acabamos de configurar. Para esto seleccionamos la “**opción 2”** del menú principal.

Figura 59

Proceso de instalación de pfSense: Configuración de direcciones IPs en las interfaces de red



Nota: Es importante recordar que la configuración de la interfaz **em0**, está en modo bridge, esto quiere decir que dependerá de las asignaciones automáticas del enrutador de tu red local físico. No necesitas hacer ajustes manuales en esta interfaz, ya que funcionará como otro dispositivo más dentro de tu red residencial o de oficina.

En la interfaz “**LAN”** y “**DMZ”**, asignamos direcciones estáticas según nuestra **Figura 5**, asegurándonos de que las “**IPs”** se alineen con el diseño planeado. Para mantener la claridad, he organizado la información de cada interfaz de red a configurar comenzando con la interfaz “**LAN”**.

Tabla 3

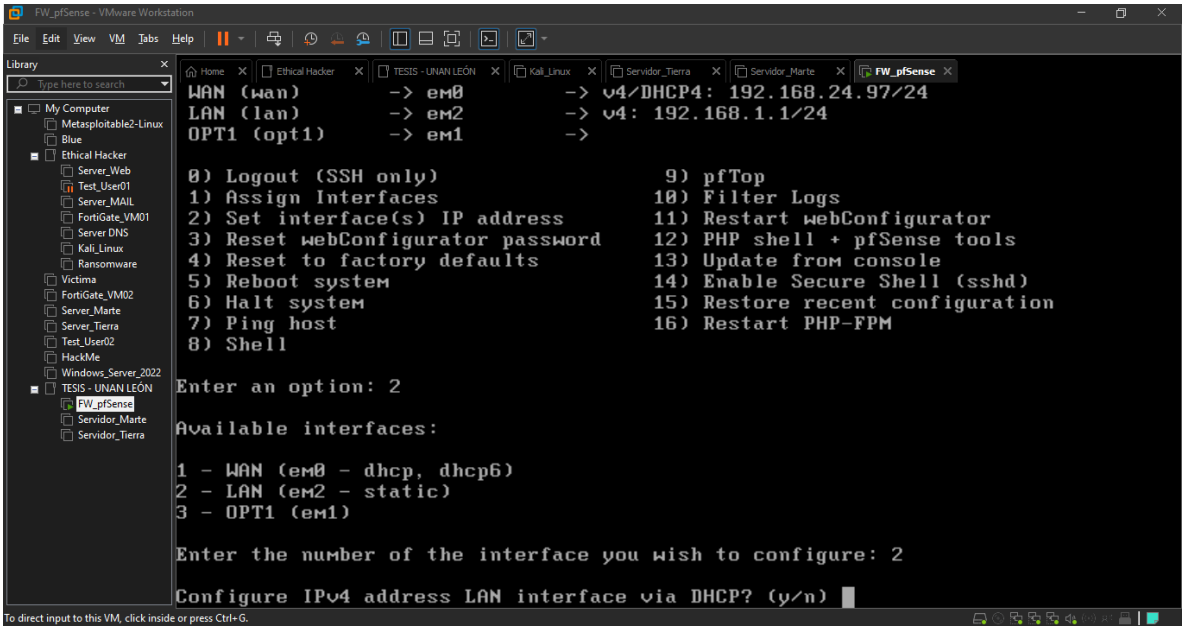
Resumen de las direcciones IPs de la interfaz LAN

INTERFAZ LAN			
Dirección de red:		192.168.2.0/26	
Dirección ipv4 de la interfaz:		192.168.2.1	
Mascara de la red:		255.255.255.192 /26	
Gateway de la red:		192.168.2.1	
El servicio DHCP esta activo en la red por la IP:		192.168.2.1	
El servicio DNS esta activo en la red por la IP:		192.168.2.1	
Hosts disponibles asignables en la red:		61	
Hosts disponibles desde:	192.168.2.2/26	**Hasta:**	192.168.2.62/26

- Empecemos configurando la interfaz **LAN** seleccionando la **opción 2**.

Figura 60

Proceso de instalación de pfSense: Configuración de la dirección IP de la LAN

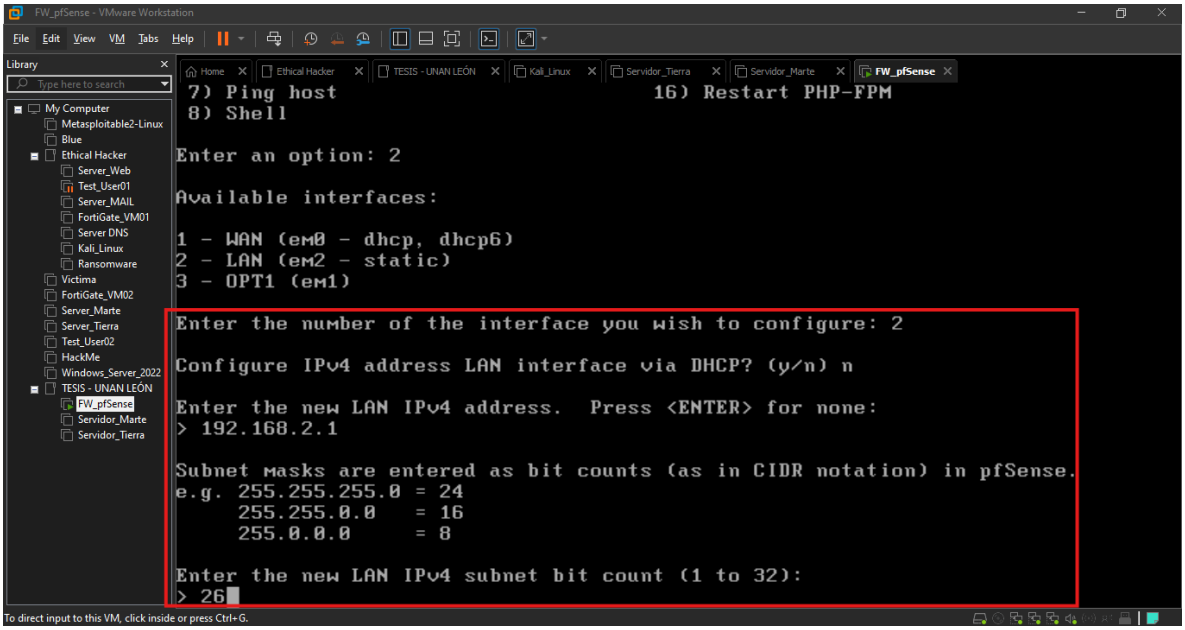


Nota: Esta opción nos permitirá asignar manualmente la IP 192.168.2.1/26 a la interfaz LAN, la cual funcionará como el gateway principal para todos los dispositivos conectados en esta red.

En este paso, la “**CLI”** nos indica si deseamos obtener la dirección IP de la interfaz **LAN** mediante el servicio **DHCP**. Sin embargo, dado que queremos establecer una dirección IP estática en esta interfaz para mantener el control y cumplir con nuestro diseño de red, colocamos “**No**” y presionar “**Enter**”.

Figura 61

Proceso de instalación de pfSense: Configuración de la dirección IP de la LAN

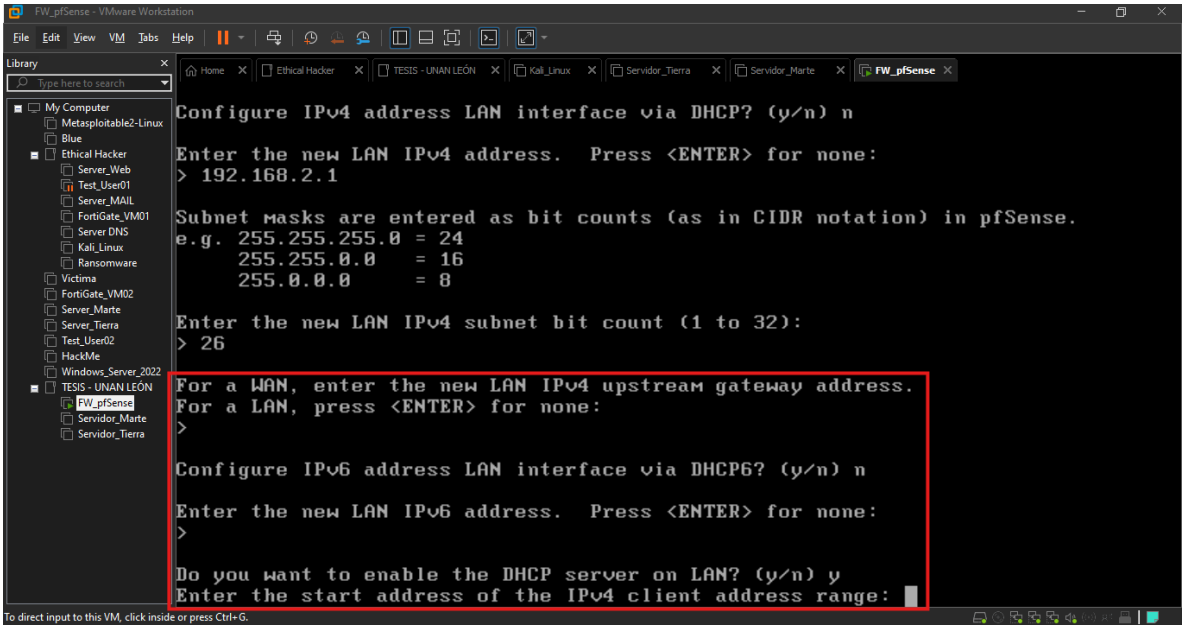


Nota: En este paso, después de configurar la dirección IP estática para la interfaz LAN, procederemos con algunas configuraciones adicionales:

Desactivar IPv6: En este escenario, no activaremos IPv6 en la interfaz LAN, ya que trabajaremos únicamente con IPv4 para simplificar la configuración y mantener la compatibilidad con nuestro diseño de red.

Figura 62

Proceso de instalación de pfSense: Configuración de la dirección IP de la LAN

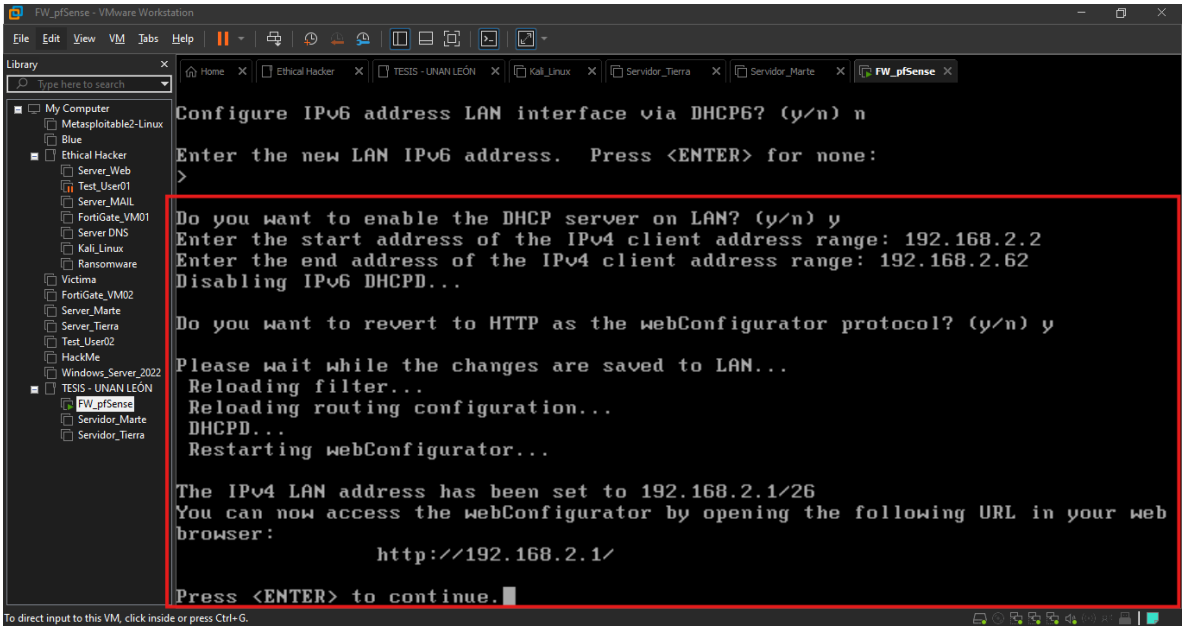


Activar el servidor DHCP: Es importante activar el servidor **DHCP** en la interfaz **LAN** para que los dispositivos que se conecten a esta red reciban automáticamente una dirección IP dentro del rango que definimos anteriormente, de **192.168.2.2** a **192.168.2.62/26.**

Activar el protocolo HTTP: En pfSense es esencial para poder continuar con la configuración vía web. A través de la interfaz gráfica (**GUI**), podrás gestionar y ajustar de manera más sencilla las configuraciones del firewall y otros servicios.

Figura 63

Proceso de instalación de pfSense: Finalizando la configuración de las direcciones IPs de la LAN

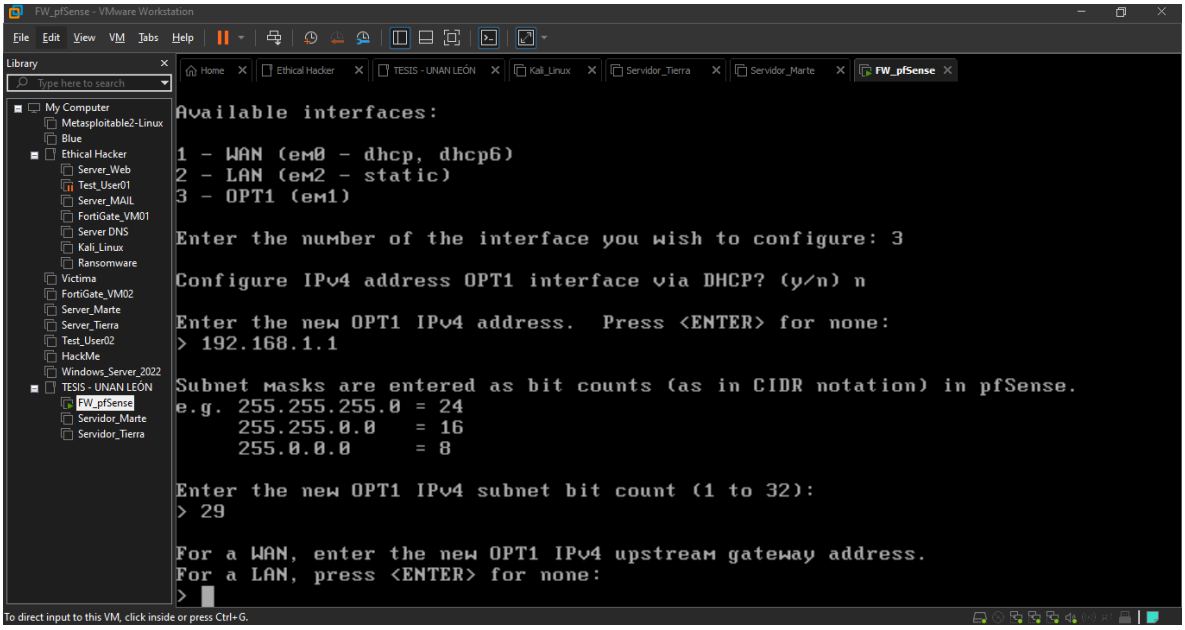


Nota: Una vez hechas estas configuraciones, continuamos con el proceso para aplicar los cambios.

Repetiremos el mismo proceso que utilizamos para configurar la dirección IP de la interfaz **LAN**, pero esta vez para la interfaz **OPT1**, que temporalmente está designada como nuestra interfaz **DMZ**. Para ello, seleccionamos la opción 2 y configuramos la dirección IP correspondiente a esta interfaz.

Figura 64

Proceso de instalación de pfSense: Configuración de la dirección IP de la DMZ



A continuación, presento la información en formato de para facilitar la visualización y comprensión de la configuración.

Tabla 4

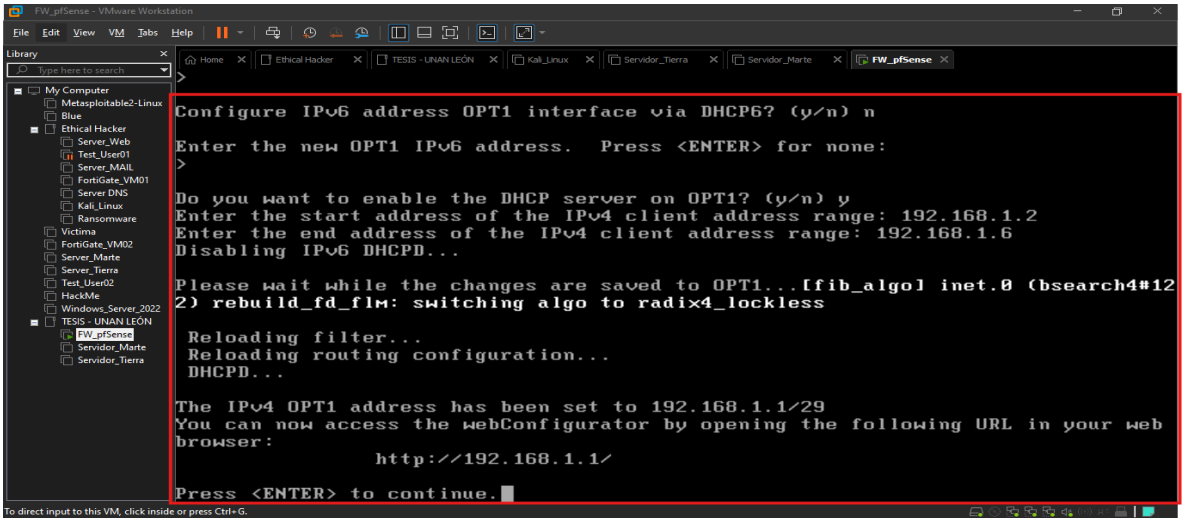
Resumen de las direcciones IPs de la interfaz DMZ

INTERFAZ DMZ			
Dirección de red:		192.168.1.0/29	
Dirección ipv4 de la interfaz:		192.168.1.1	
Mascara de la red:		255.255.255.248 /29	
Gateway de la red:		192.168.1.1	
El servicio DHCP esta activo en la red por la IP:		192.168.1.1	
El servicio DNS esta activo en la red por la IP:		192.168.1.1	
Hosts disponibles asignables en la red:		5	
Hosts disponibles desde:	192.168.1.2/29	**Hasta:**	192.168.1.6/29

No utilizaremos **IPv6**, por lo que colocamos “**No**” y “**Enter**”. Al aceptar esta opción, se activará el servidor **DHCP** en la interfaz, y presionamos “**Enter**”.

Figura 65

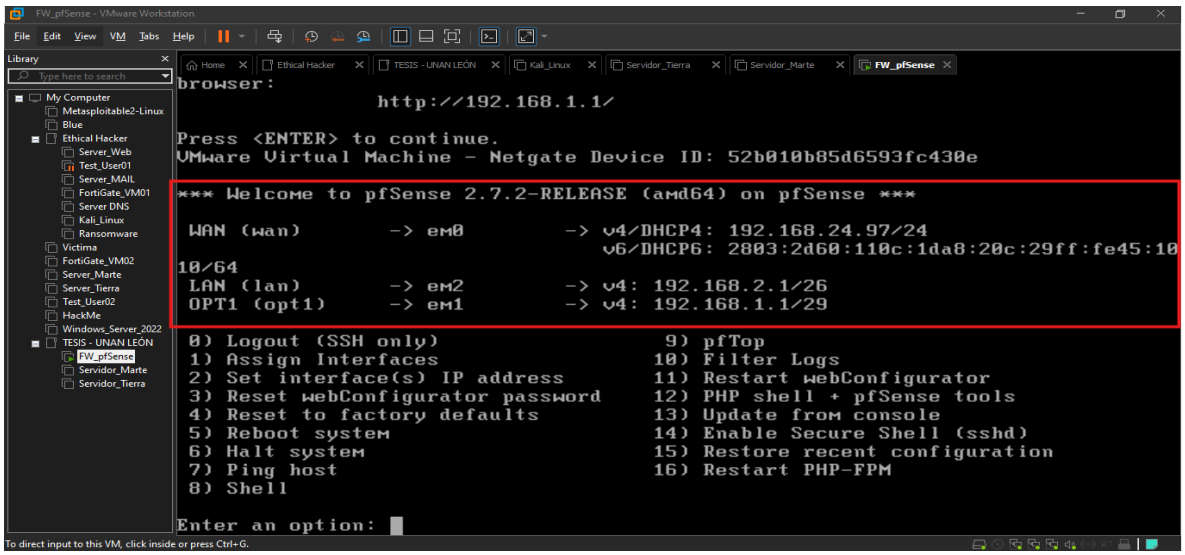
Proceso de instalación de pfSense: Configuración de la dirección IP de la DMZ



Una vez realizados los cambios en el menú principal de pfSense debe de quedar como la siguiente **Figura 66**.

Figura 66

Proceso de instalación de pfSense: Configuración de la dirección IP de la DMZ



De esa forma hemos culminado nuestra primera fase de instalación desde la consola, totalmente desde cero. Es momento de agregar el resto de las máquinas virtuales que utilizaremos en nuestra guía de instalación de pfSense. Como esta guía se basa propiamente en pfSense y sus bondades entonces no mostraremos como instalar desde cero el resto de las máquinas virtuales que necesitamos, pero no te preocupes que si subiremos nuestras máquinas virtuales que estamos utilizando y la podrás descargar y además importar en VMware Workstation sin complicaciones.

8.4 Importación, información y configuración del resto de equipos de la solución

Las máquinas virtuales las puedes descargar desde los siguientes enlaces:

Tabla 5

Repositorios para descargar las máquinas virtuales

Máquinas virtuales	
Nombres	**Enlace de descarga**
Firewall (FW_pfSense)	FW_pfSense
Servidor Tierra (Server Tierra)	Servidor_Tierra
Servidor Marte (Server Marte)	Servidor_Marte
Administrador de la red (Ubuntu Mate)	Admin_NET
Usuario de la red (Windows 10)	Windows-10_Users

Si, necesita ayuda para importar las máquinas virtuales una vez descargadas puede ver el siguiente video de como importar maquinas virtual en VMware Workstation Pro **aquí** o bien si prefiere leer presionar **aquí.**

8.4.1 Información general de las máquinas virtuales de esta guía de instalación

A continuación, se mostrarán en detalles la información de cada una de las máquinas virtuales en nuestra topología.

A. FW_pfSense

Tabla 6

Resumen del sistema del FW_pfSense

Nombre: FW_pfSense	
Versión:	**2.7.2**
Nombre del host:	**fwperimetral**
Servicios ejecutándose:	**DNS (53), DHCP (67), SSH (22), HTTP (80), HTTPS (443)**

Tabla 7

Resumen del dominio de nuestro laboratorio

Información del dominio	
Dominio local	**mipyme.com**
Subdominio del servidor Marte	**marte.mipyme.com**
Subdominio del servidor Tierra	**tierra.mipyme.com**
Subdominio de pfSense	**fwperimetral.mipyme.com**

Tabla 8

Resumen del servicio DNS del FW_pfSense

Información del DNS	
• **DNS exterior primario:**	**8.8.8.8 (Google)**
• **DNS exterior secundario:**	**1.1.1.1 (Cloudflare)**

B. Servidor Tierra

Tabla 9

Resumen del sistema operativo del Servidor Tierra

Nombre: Servidor Tierra	
Versión:	**22.04.1 LTS**
Nombre del usuario:	**Network Services**
Nombre del host:	**tierra**
Dirección ipv4 estática por DHCP:	**192.168.1.2/29,**
Red a la que pertenece este host:	**DMZ (192.168.1.0/29)**
Servicios ejecutándose:	**SSH (22), HTTP (80), HTTPS (443), FTP (21), MYSQL (3306)**

Tabla 10

Resumen de la interfaz de red del Servidor Tierra

Información de la interfaz de red	
Red a la que pertenece:	**192.168.1.0/29 (DMZ)**
Dirección IPV4 asignada vía DHCP:	**192.168.1.2/29 (estática)**
Dirección IPV4 asignada como Gateway vía DHCP:	**192.168.1.1**
Dirección IPV4 asignada como DNS vía DHCP:	**192.168.1.1**

C. Servidor Marte

Tabla 11

Resumen del sistema operativo del Servidor Marte

Nombre: Servidor Marte

Versión:	**22.04.1 LTS**
Nombre del usuario:	**Network Services**
Nombre del host:	**tierra**
Dirección ipv4 estática por DHCP:	**192.168.1.3/29,**
Red a la que pertenece este host:	**DMZ (192.168.1.0/29)**
Servicios ejecutándose:	**SSH (22), HTTP (80), HTTPS (443), FTP (21), MYSQL (3306)**

Tabla 12

Resumen de la interfaz de red del Servidor Marte

Información de la interfaz de red	
Red a la que pertenece:	**192.168.1.0/29 (DMZ)**
Dirección IPV4 asignada vía DHCP:	**192.168.1.3/29 (estática)**
Dirección IPV4 asignada como Gateway vía DHCP:	**192.168.1.1**
Dirección IPV4 asignada como DNS vía DHCP:	**192.168.1.1**

D. Administrador de la red

Tabla 13

Resumen del sistema operativo del Administrador de la red

Nombre: Administrador de la red (Ubuntu Mate)	
Versión:	**22.04.1 LTS**
Nombre del usuario:	**Network Admin**
Nombre del host:	**adminnet**
Dirección ipv4 estática por DHCP:	**192.168.2.2/26**
Red a la que pertenece este host:	**LAN (192.168.2.0/26)**

Tabla 14

Resumen de la interfaz de red del Administrador de la red

Información de la interfaz de red	
Red a la que pertenece:	**192.168.2.0/26 (LAN)**
Dirección IPV4 asignada vía DHCP:	**192.168.2.2/26 (estática)**
Dirección IPV4 asignada como Gateway vía DHCP:	**192.168.2.1**
Dirección IPV4 asignada como DNS vía DHCP:	**192.168.2.1**

E. Usuarios de la red LAN

Tabla 15

Resumen del sistema operativo de Windows 10

Nombre: Usuario de la red (Windows 10)	
Versión:	**Home**
Nombre del usuario:	**User Pyme**
Nombre del host:	**DESKTOP-TBH96NQ**
Dirección ipv4 dada dinámicamente por DHCP **Puede ser una IP que esté disponible en el pool DHCP.**	
Red a la que pertenece este host:	**LAN (192.168.2.0/26)**

Ahora bien, es momento de brindar la información de las credenciales de acceso a las máquinas virtuales que están en **Tabla 5** y a los servicios instalados que requieran credenciales:

- **Credenciales de las máquinas virtuales, servicios y administración.**

Tabla 16

Credenciales de acceso a la máquina virtual de FW_pfSense

Credenciales de FW_pfSense para ingreso por SSH, consola o Interfaz gráfica	
Usuario:	**admin**

Contraseña:	**AdminNet.**

Tabla 17

Credenciales de acceso a la máquina virtual del Servidor Marte

Credenciales del servidor Marte	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Tabla 18

Credenciales de acceso a la máquina virtual del Servidor Tierra

Credenciales del servidor Tierra	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Tabla 19

Credenciales de acceso a la máquina virtual del Administrador de la red

Credenciales del Administrador de la red	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Tabla 20

Credenciales de acceso a la máquina virtual del usuario en Windows 10

Credenciales de los usuarios de la red en Windows 10	
Usuario:	**UserPyme**
Contraseña:	**UserPyme.**

Tabla 21

Credenciales de acceso al servicio MySQL en: los Servidores Tierra y Marte

Credenciales del servicio MySQL en ambos servidores tierra y marte	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Tabla 22

Credenciales de acceso al servicio PhpMyAdmin en: los Servidores Tierra y Marte

Credenciales de PhpMyAdmin como gestor de base de datos en ambos servidores tierra y marte	
Usuario:	**phpmyadmin**
Contraseña:	**phpmyadmin**

Tabla 23

Credenciales de acceso al servicio Administrativo de WordPress

Credenciales del servicio WordPress	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Tabla 24

Credenciales de acceso al servicio Administrativo de Bagisto

Credenciales del sistema web en Laravel - Bagisto	
Usuario:	**admin@example.com**
Contraseña:	**admin123**

Tabla 25

Credenciales de acceso a los servicios FTP y SSH en los Servidores Tierra y Marte

Credenciales para FTP y SSH del servidor Tierra en ambos servidores tierra y marte	
Usuario:	**adminnet**
Contraseña:	**AdminNet.**

Se enfatiza la importancia de preservar las contraseñas de manera segura, sugiriendo encarecidamente su almacenamiento en un lugar designado. Se otorga libertad al administrador de la red para modificar las contraseñas, aplicar políticas de seguridad pertinentes, entre otras medidas. Es relevante destacar que este escenario constituye únicamente una prueba; en un entorno operativo real, se recomienda encarecidamente la implementación de medidas adicionales, tales como el uso de claves de acceso en las conexiones SSH, la adopción de contraseñas robustas en máquinas virtuales y servicios, además la implementación de prácticas de seguridad digital avanzadas.

8.4.2 Inicializando la máquina virtual del Administrador de la red

Es momento de avanzar con la configuración de nuestra máquina virtual de **FW_pfSense**, y por ende hay que encender la máquina virtual **del Administrador de la red (Ubuntu Mate)**, hay que recordar que hay que descargar las máquinas virtuales de la **Figura 5** en el **Tabla 5**
Repositorios para descargar las máquinas virtuales.

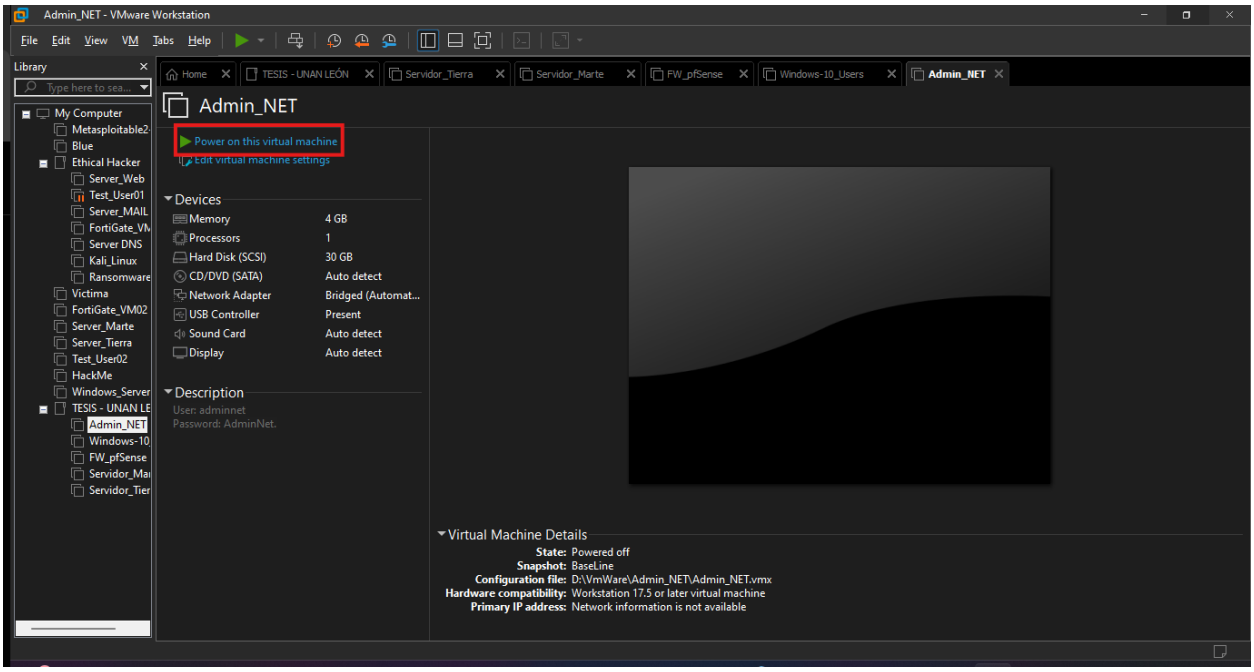
El resto de las configuraciones de los servicios de red, lo haremos desde la máquina virtual **Admin_Net (Ubuntu Mate)** desde el sistema web de pfSense para que vayamos familiarizándonos con este entorno de configuración. Cabe recalcar, algunos detalles importantes al encender la maquinan **virtual Admin_Net** son:

- Hay que recordar que la máquina virtual **Admin_Net** (Ubuntu Mate) es la máquina virtual del administrador de la red y de quien implementa la solución de seguridad perimetral con pfSense.
- El servicio **DHCP** se inicializo cuando hicimos la instalación del sistema operativo **pfSense 2.7.2**, en ambas redes internas (**DMZ y LAN**) se inicializó DHCP por ende podremos encender las otras máquinas virtuales del escenario y el servicio DHCP en **FW_pfSense** nos brindara direccionamiento ipv4 para comunicarnos a nivel de red, entre todas las máquinas virtuales del entorno. No obstante, en pasos posteriores revisaremos la configuración del servicio DHCP y le añadiremos algunas opciones.

En el panel central de VMware Workstation estarán las máquinas virtuales implementadas en el entorno local, entonces para iniciar la máquina virtual **Admin_Net (Ubuntu Mate)** bastara en ubicar la máquina virtual por el nombre y darle en "**Power on this virtual machine**" como en la **Figura 67**.

Figura 67

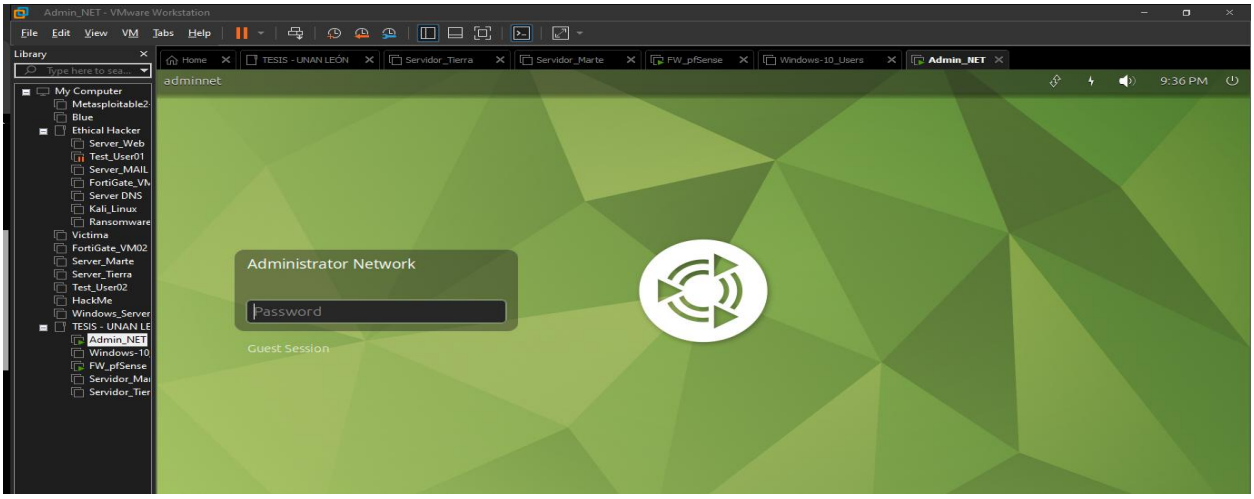
Proceso de instalación de pfSense: Inicializando la máquina virtual de Admin_NET



Una vez, iniciada la máquina virtual Admin_NET (Ubuntu Mate) se nos mostrara el inicio de sesión obligatorio para iniciar sesión en esta máquina virtual.

Figura 68

Proceso de instalación de pfSense: Inicio de sesión en Admin_NET

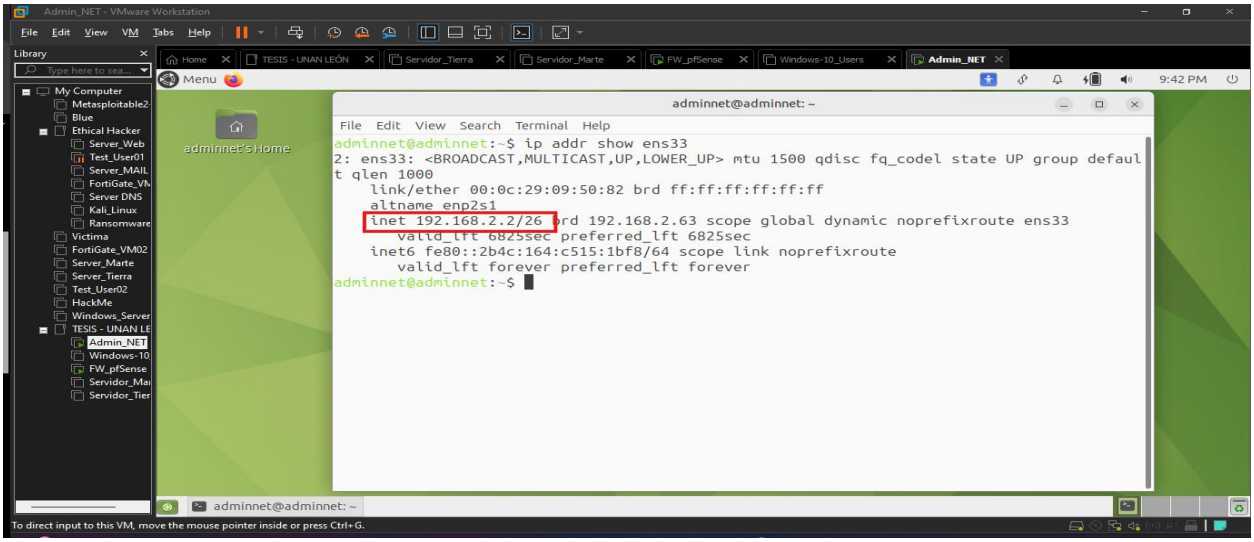


Ya iniciada la sesión de administrador, procederemos a ver qué dirección IP nos asignó el servicio **DHCP** y además es muy importante tener actualizado nuestros sistemas.

Con el atajo de teclado "**Ctrl + Alt +** t" sacamos una terminal de consola en Ubuntu Mate y copiamos el comando "**ip addr show ens33**" en la terminal y damos en "**ENTER**" para ver qué dirección ipv4 nos asignó el servicio DHCP.

Figura 69

Proceso de instalación de pfSense: Ver dirección IP asignada en Admin_NET

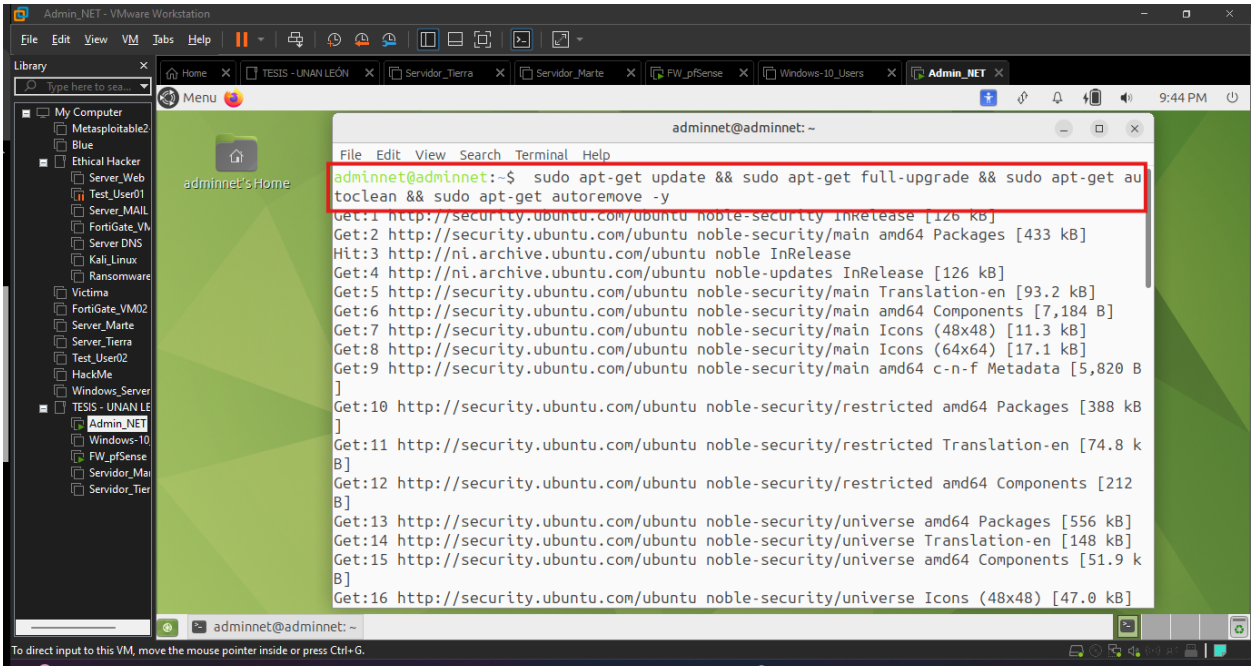


A como podemos ver dinámicamente el servicio DHCP nos asignó la dirección IP **192.168.2.2/26,** cambiaremos en pasos posteriores esta dirección ipv4 dinámica a estática, para que la máquina virtual Admin_NET, tenga siempre la misma dirección IP.

Copiamos el comando "**sudo apt-get update && sudo apt-get full-upgrade && sudo apt-get autoclean && sudo apt-get autoremove -y**" en la terminal y damos en "**ENTER**" para que empiece a descargarse los paquetes necesarios para la actualización, pero antes que se actualicen las librerías a las más recientes, para descargar dichos paquetes. Al presionar "**ENTER**" se te pedirá que coloques la contraseña del usuario administrador.

Figura 70

Proceso de instalación de pfSense: Actualización del sistema en Admin_NET



8.4.3 Implementación de servicios como DNS, DHCP, SSH en pfSense

Una vez, finalizado el proceso de actualización, nos conectaremos desde el sistema web de FW_pfSense de la siguiente forma:

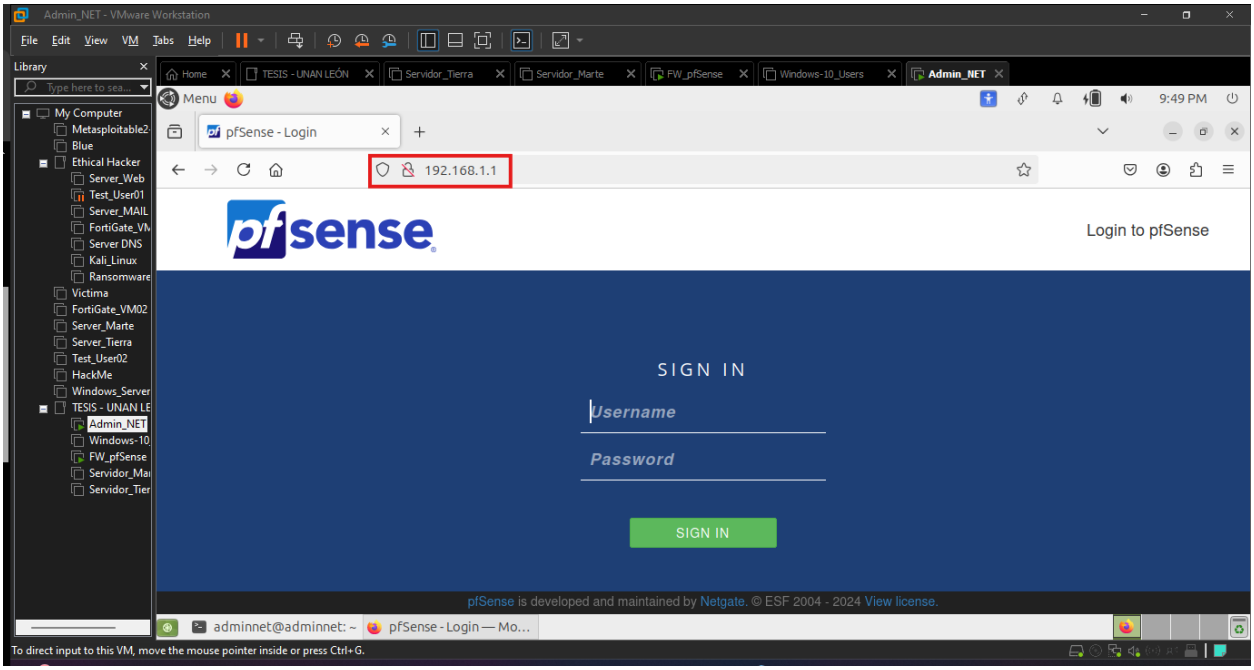
- Abrimos el navegador Firefox, Chrome o cualquier otro navegador que tengamos por nuestra parte ocuparemos el navegador Firefox.
- Colocaremos la dirección IP de FW_pfSense para la interfaz LAN que es la IP 192.168.2.1 en el buscador de URL y presionamos “ENTER” en el buscador de URL (luego de haber colocado la IP), para ingresar al sistema web de administración de FW_pfSense nos autenticamos, con las credenciales las siguientes credenciales por defecto:

➢ **Usuario: admin**

- **Contraseña: pfsense**

Figura 71

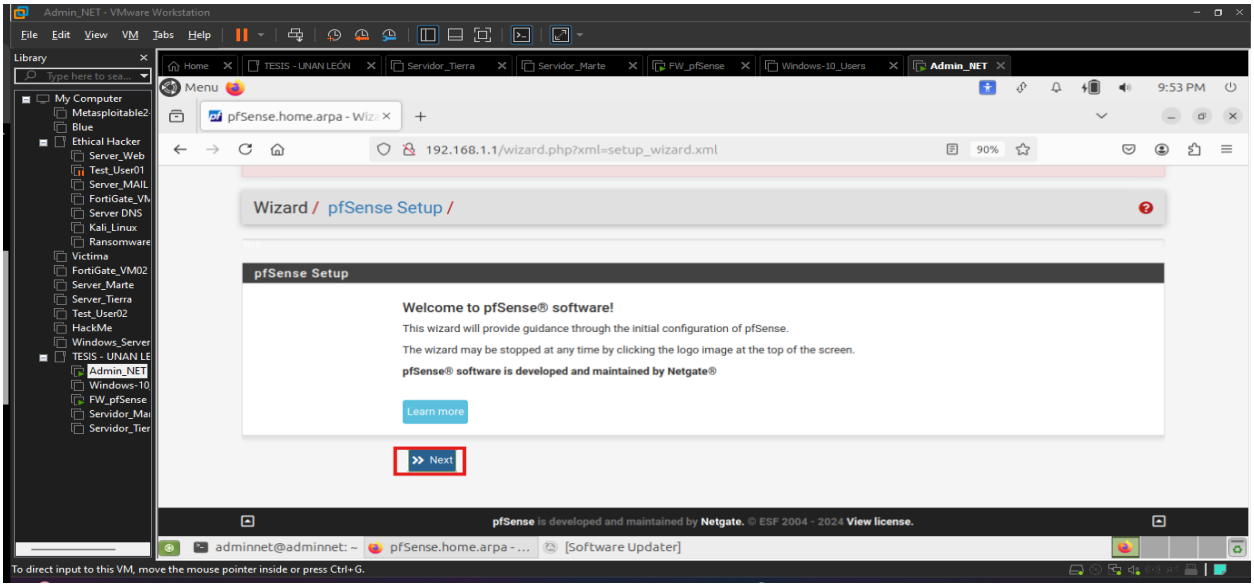
Proceso de instalación de pfSense: Inicio de sesión en el GUI de pfSense



Después de autenticarnos correctamente en el sistema web de **FW_pfSense**, lo primero que se nos mostrara es el asistente de configuración denominado “**Wizard**” como en la siguiente **Figura 72** y daremos en “**Next**”.

Figura 72

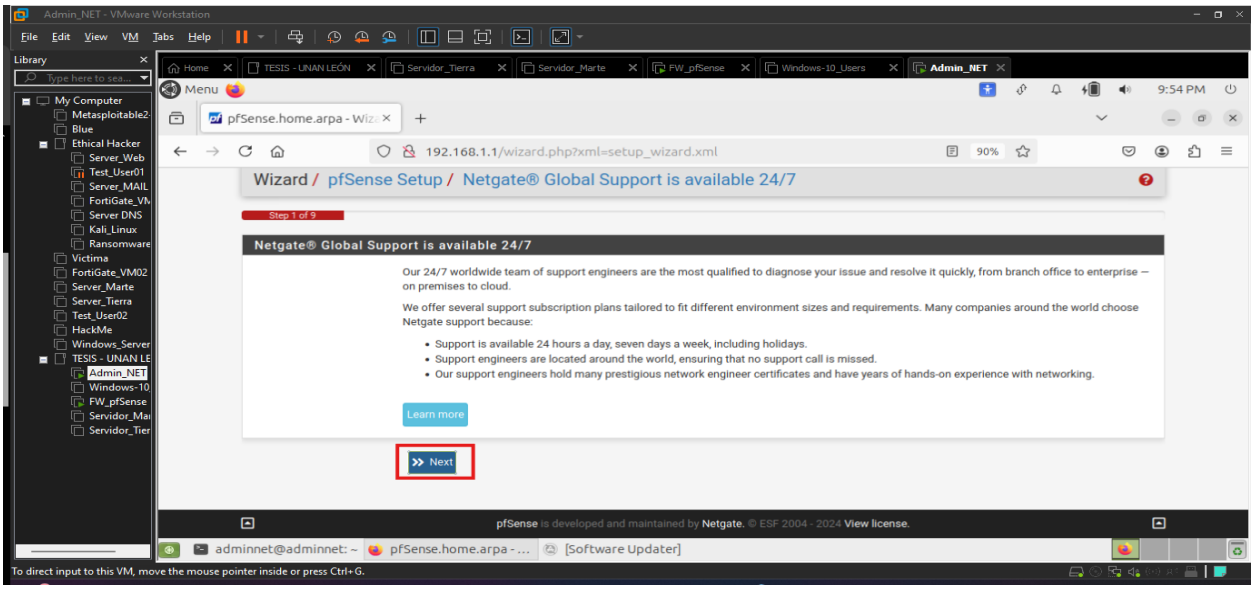
Proceso de instalación de pfSense: Inicio del asistente de configuración desde GUI en pfSense



Lo siguiente que hará el asistente de configuración es recordarnos que tenemos asistencia 24/7 con una licencia comercial, para nuestro laboratorio no será necesario por eso procedemos a dar en "**Next**".

Figura 73

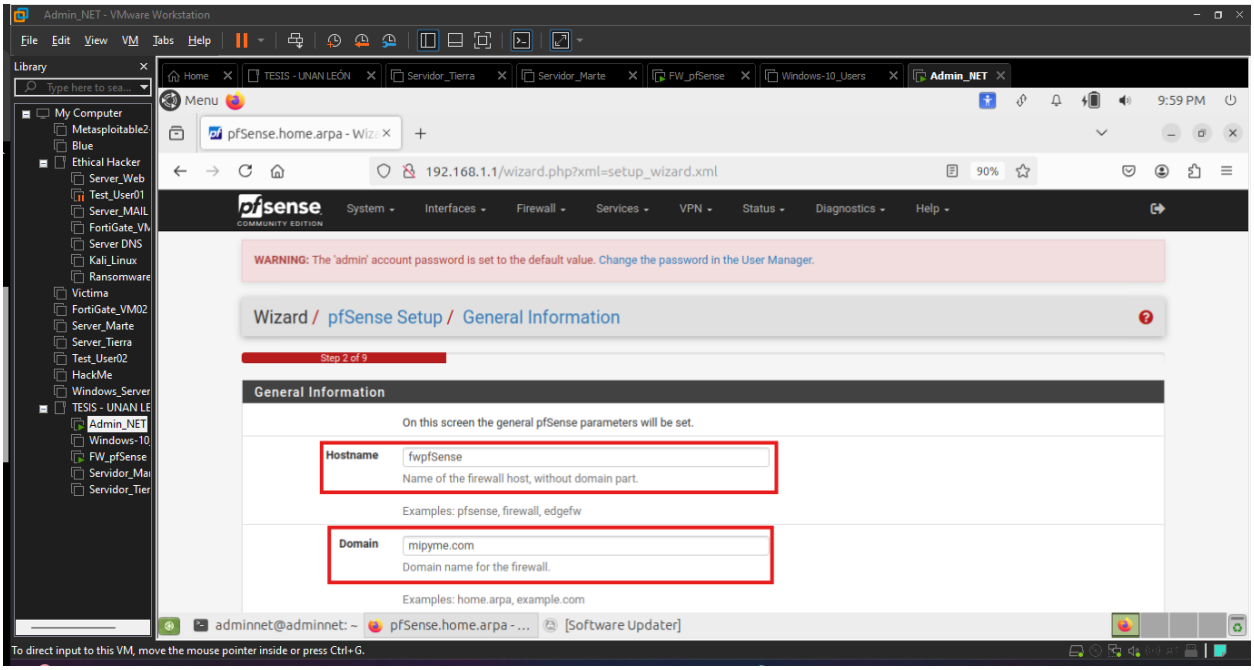
Proceso de instalación de pfSense: Inicio del asistente de configuración desde GUI en pfSense



Luego nos mostrará información general, y además que debemos editar bajo nuestras necesidades como son el “**Hostname**” y el “**Domain**” la información de estos lo podemos encontrar en **Tabla 7**.

Figura 74

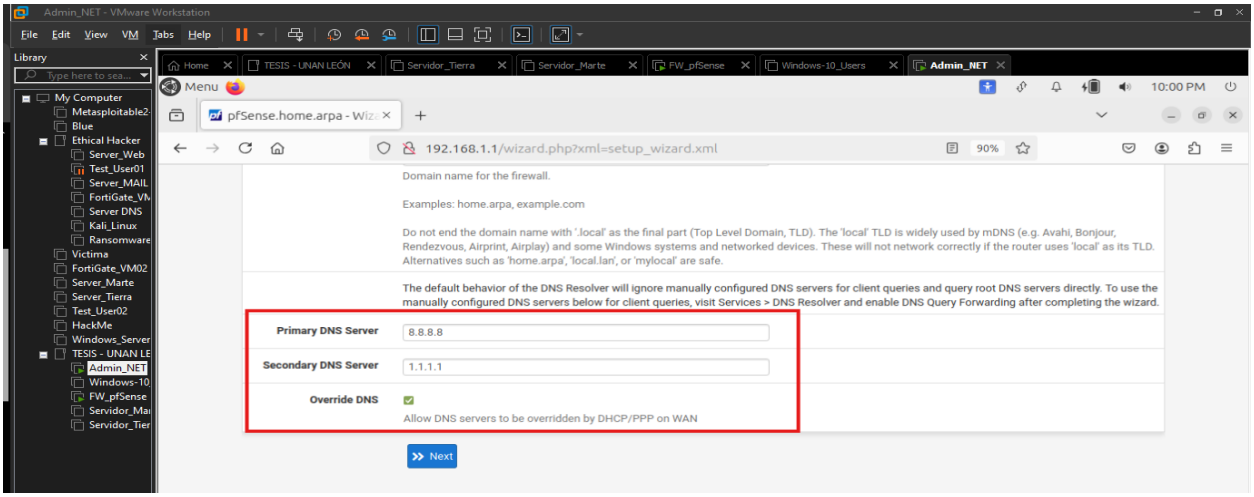
Proceso de instalación de pfSense: Hostname y Domain en pfSense



En el mismo apartado haciendo scroll hacia abajo, nos mostrara información esencial para la traducción de dominios, en este caso la información que colocamos la tenemos en **Tabla 8** y continuamos presionando en “**Next**”.

Figura 75

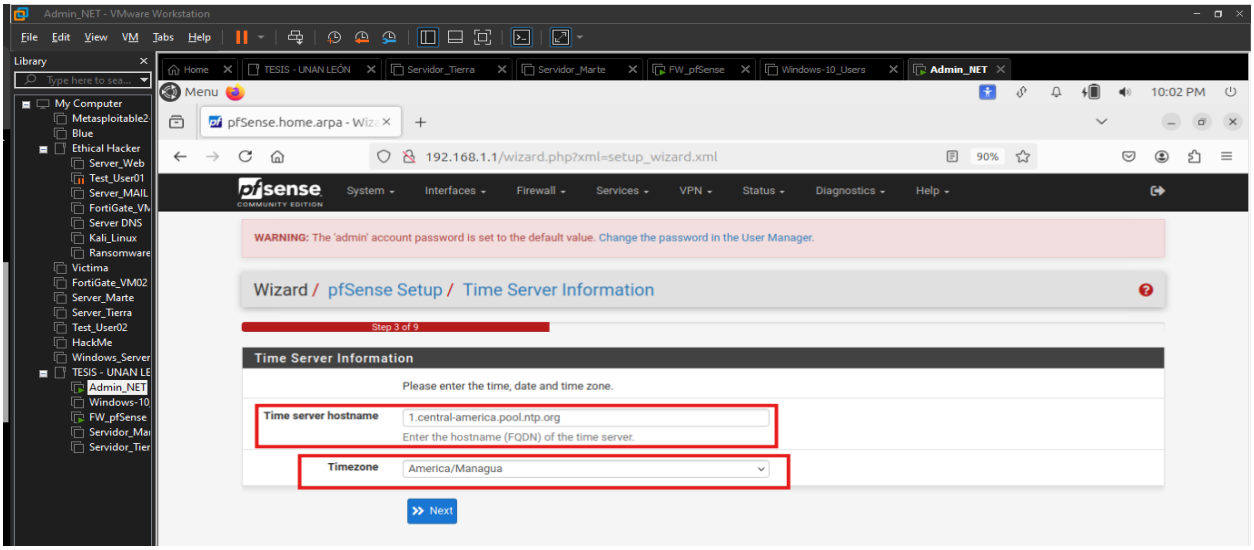
Proceso de instalación de pfSense: DNS forwarder en pfSense



En la siguiente sección del asistente de configuración es momento de colocar un servidor NTP, por nuestra parte hemos colocado uno de NTP Pool Project que se pueden utilizar en nuestro caso ya que son abiertos al público en general y va muy bien para América central. El que nosotros hemos utilizado es "**1.central-america.pool.ntp.org**" y colocamos en donde nos ubicamos "**América/Managua**" y continuamos con "**Next**"

Figura 76

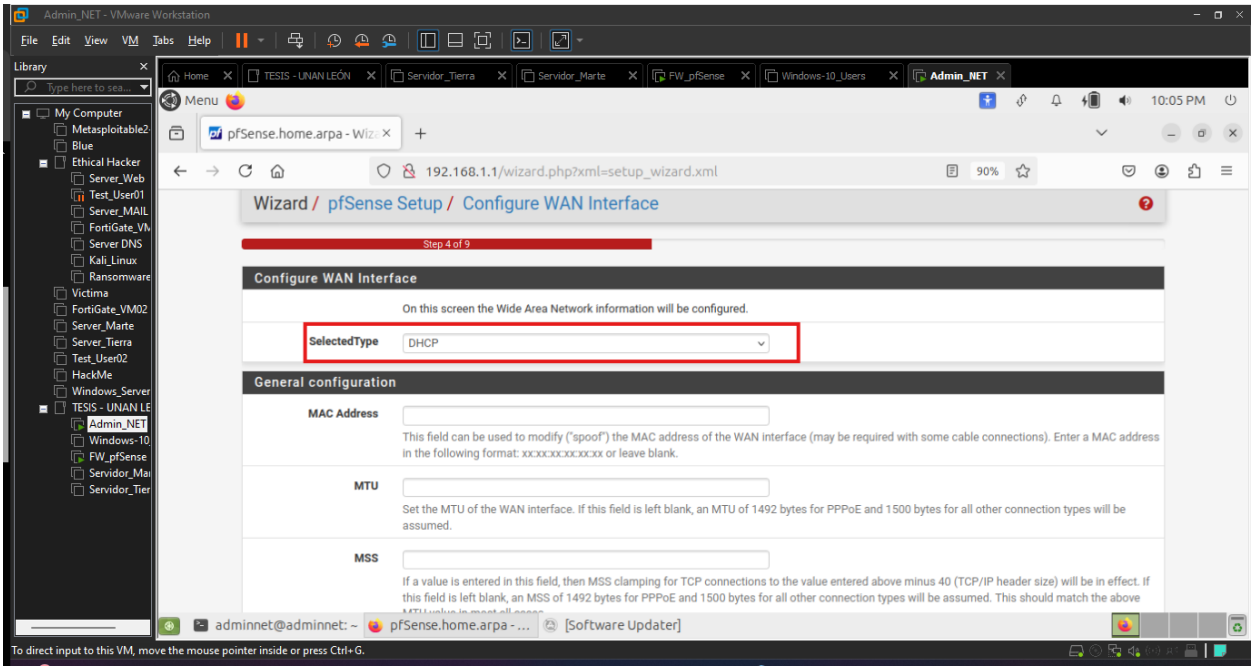
Proceso de instalación de pfSense: NTP en pfSense



En la siguiente sección, podemos revisar las configuraciones de la interfaz WAN, pero solo será necesario hacer scroll hacia abajo, ya hemos explicado anteriormente el objetivo de esta interfaz **WAN**.

Figura 77

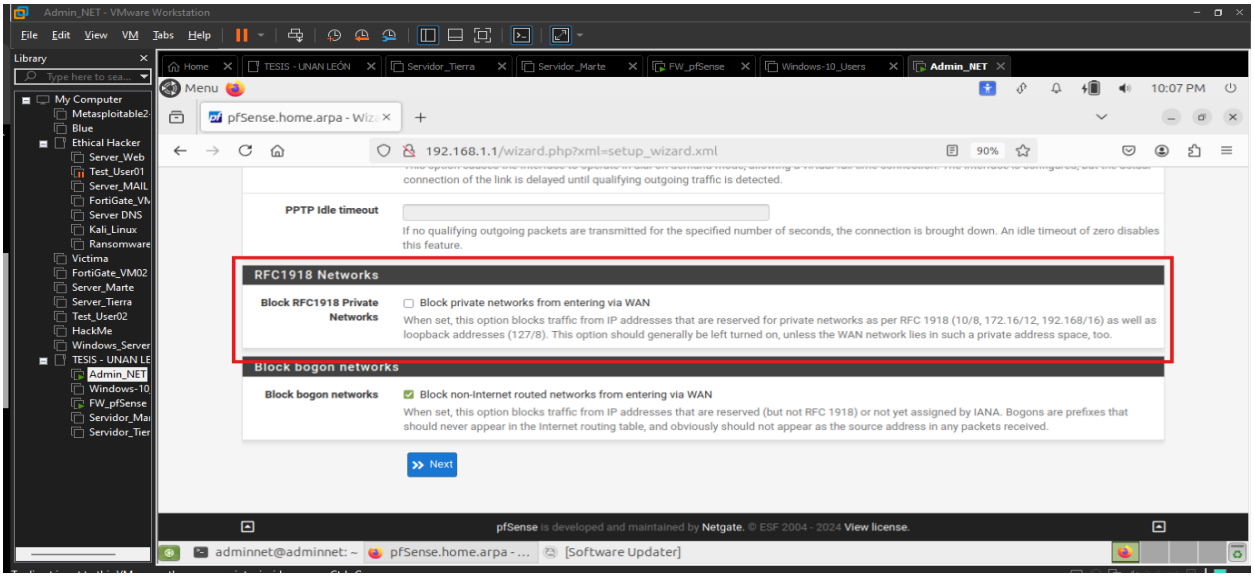
Proceso de instalación de pfSense: Interfaz WAN en pfSense



Por ahora solo será necesario dejar sin marcar la opción "**Block RFC1918 Private Networks**" para evitar que esta opción bloquea el tráfico entrante desde direcciones IP que están reservadas para redes privadas ya que estamos en un laboratorio local todas nuestras direcciones IPs son locales, para avanzar a la siguiente sección recuerda presionar en "**Next**"

Figura 78

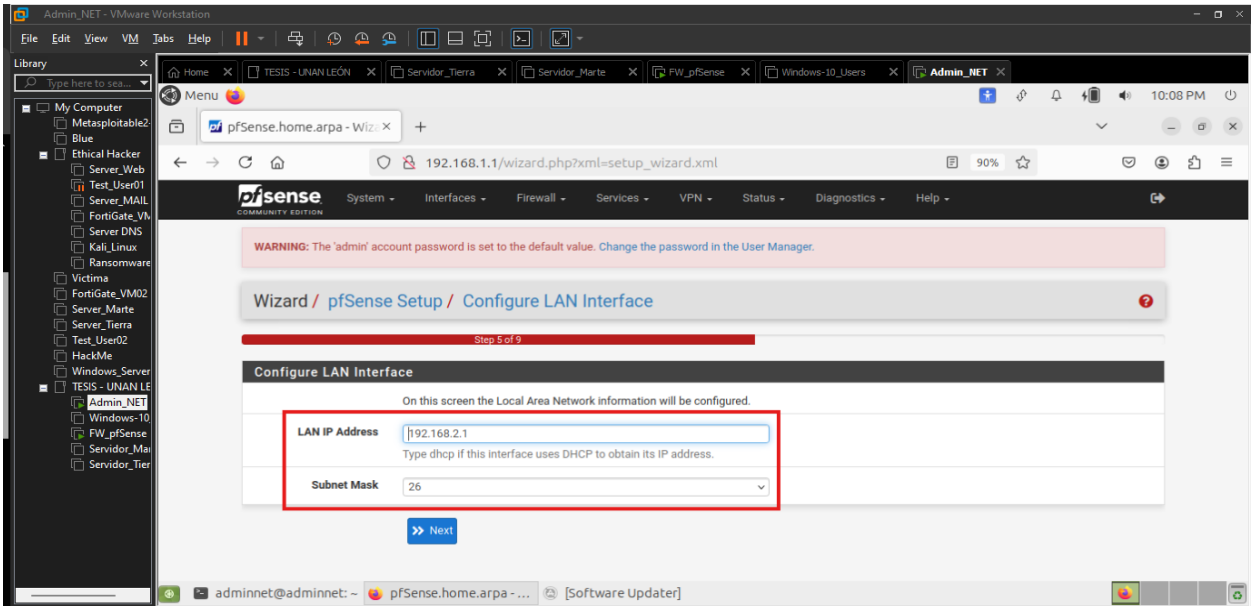
Proceso de instalación de pfSense: Permitir el RFC1918 en la interfaz WAN en pfSense



En la siguiente sección el asistente nos mostrara la IP y su mascara de red, como ya lo hemos configurado antes, solo es necesario continuar a la siguiente sección del asistente de configuración.

Figura 79

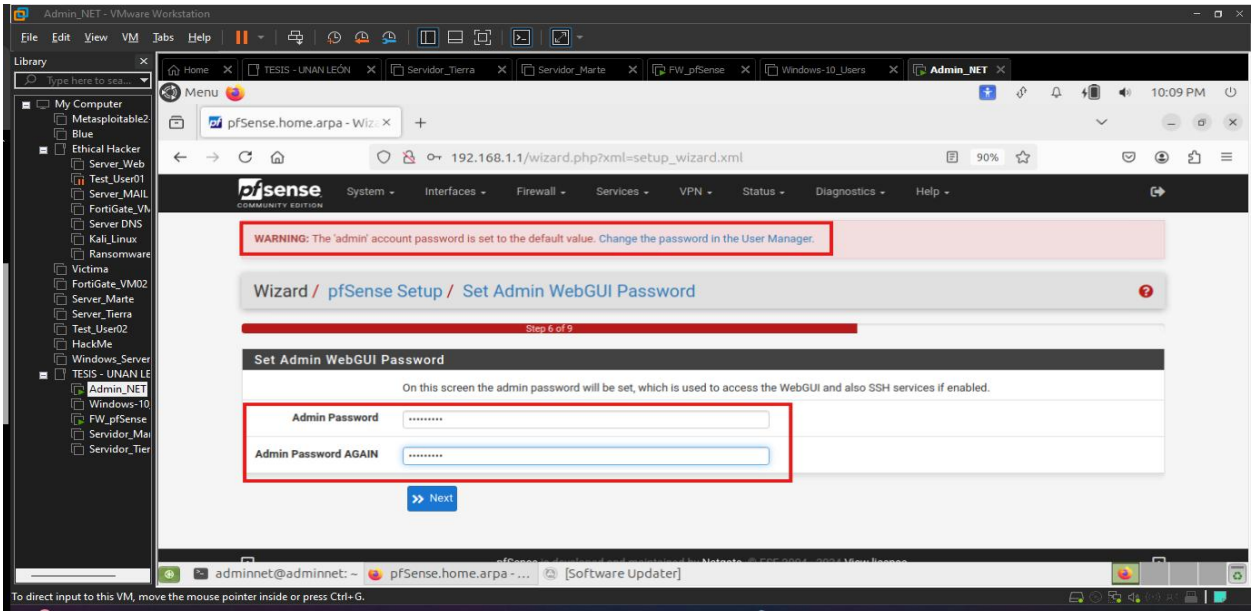
Proceso de instalación de pfSense: Interfaz LAN en pfSense



Espero lo hayas notado, desde la primera interacción con el asistente de configuración en GUI de FW_pfSense nos mostró una advertencia que debemos cambiar la contraseña que por defecto este trae, y es lo que haremos en este paso. En nuestro caso lo hemos hecho y te hemos dejado la contraseña en **Tabla 16**.

Figura 80

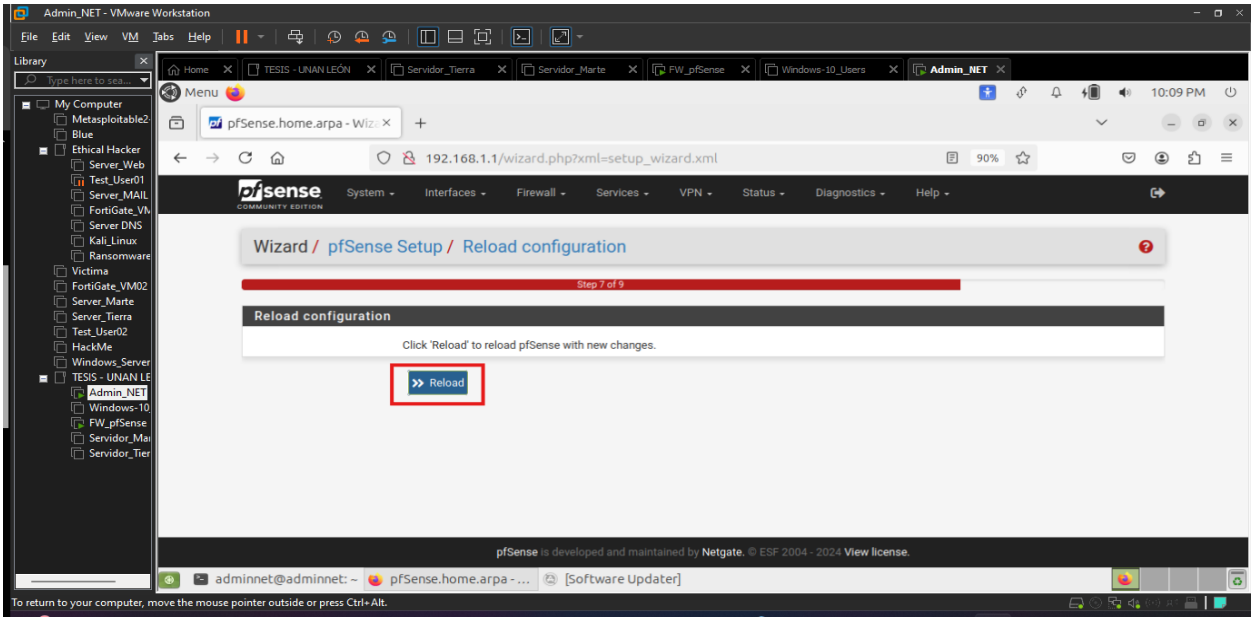
Proceso de instalación de pfSense: Cambio de contraseña de pfSense



- Luego de cambiar la contraseña pasamos a restablecer el FW_pfSense presionando "**Reload**".

Figura 81

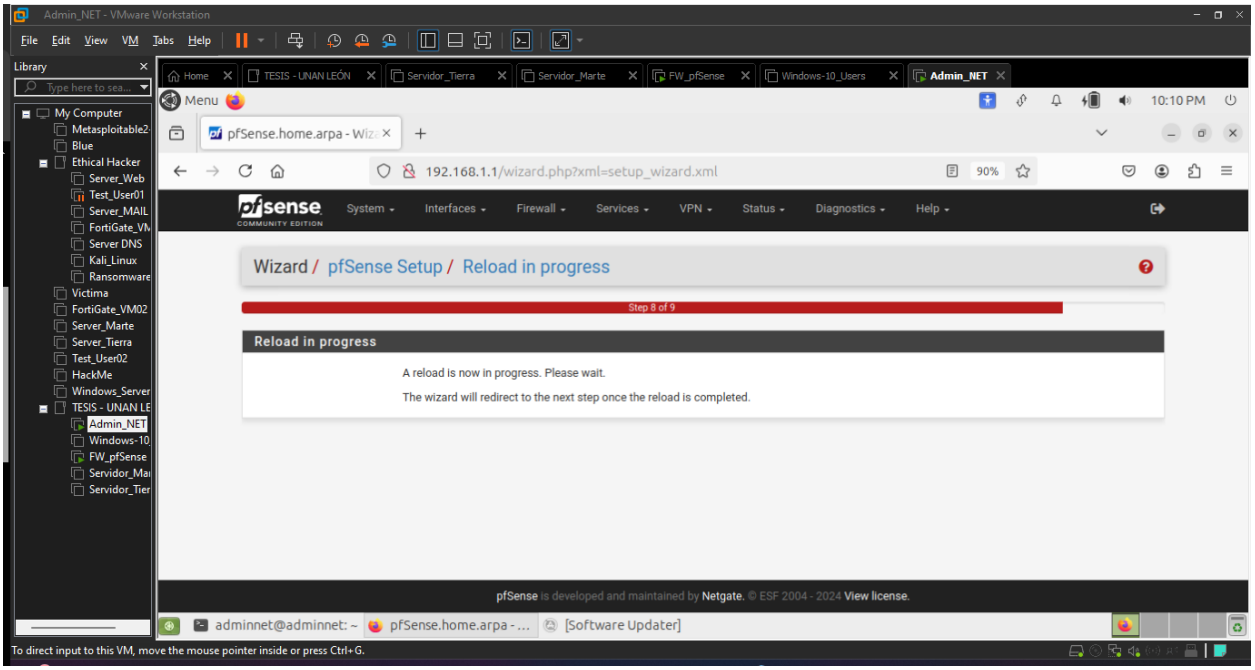
Proceso de instalación de pfSense: Restablecimiento del sistema de pfSense



- Empieza el proceso de restablecimiento.

Figura 82

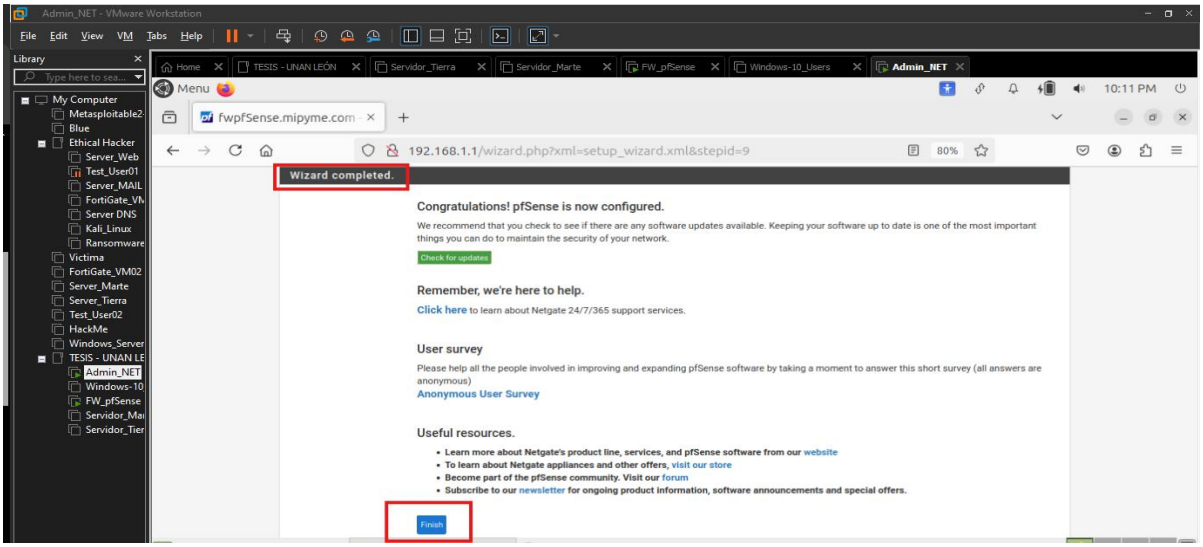
Proceso de instalación de pfSense: Finaliza el proceso de restablecimiento en pfSense



Hasta que por fin termina, se inicializa y nos muestra que ya hemos configurado de forma básica nuestro **FW_pfSense**, es momento de continuar.

Figura 83

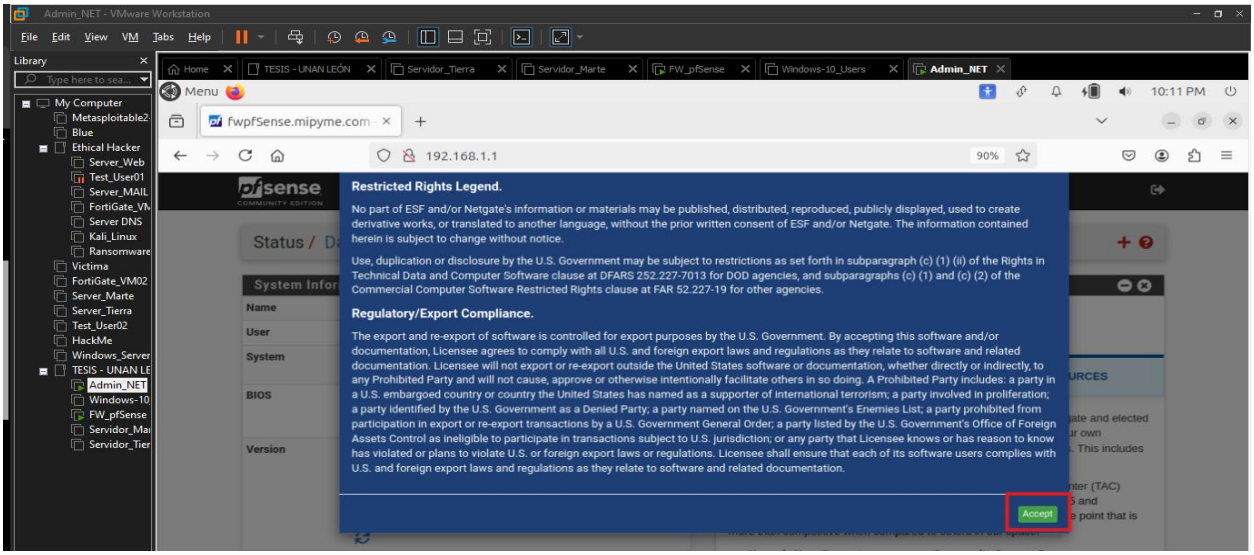
Proceso de instalación de pfSense: Correcta configuración desde el asistente de configuración.



- Nos muestra el contrato de uso, sus condiciones y reglas.

Figura 84

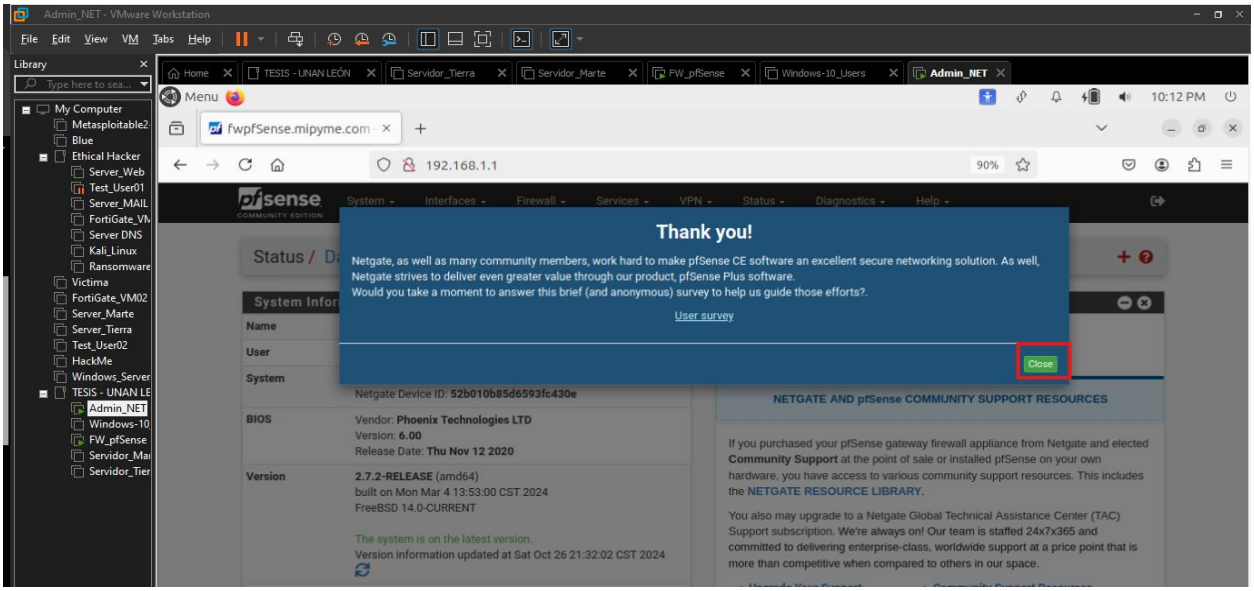
Proceso de instalación de pfSense: Aceptar el licenciamiento open source de pfSense



- Además de un agradecimiento por ser parte de la comunidad Open Source de Netgate.

Figura 85

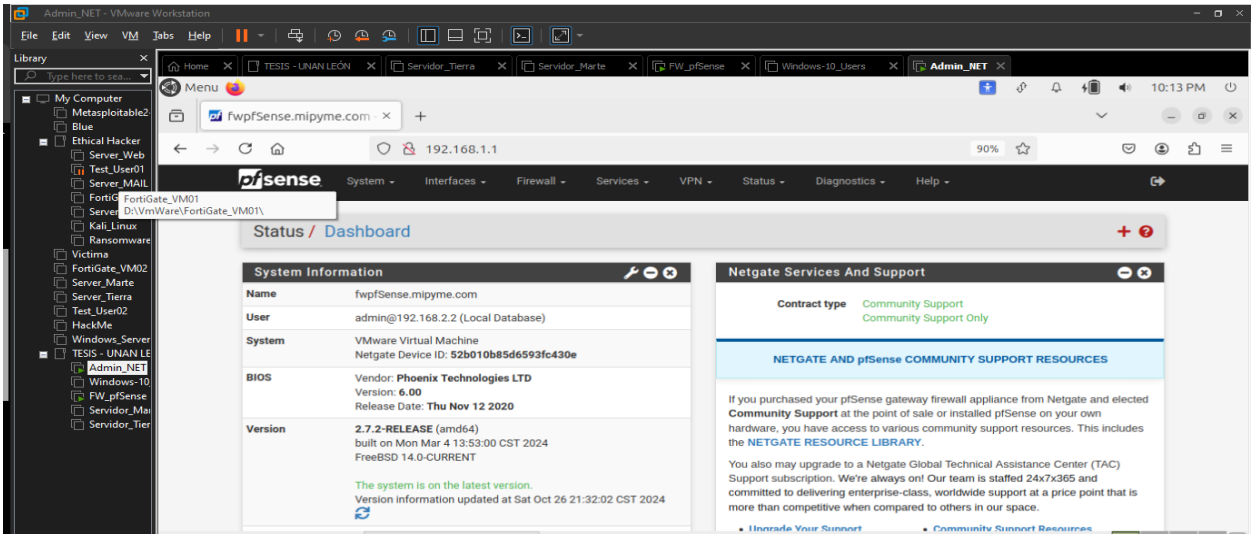
Proceso de instalación de pfSense: Agradecimiento por uso del software



Para finalizar con este asistente de configuración inicial de **FW_pfSense** nos muestra información general relevantes con sus **widgets** en el Menú principal.

Figura 86

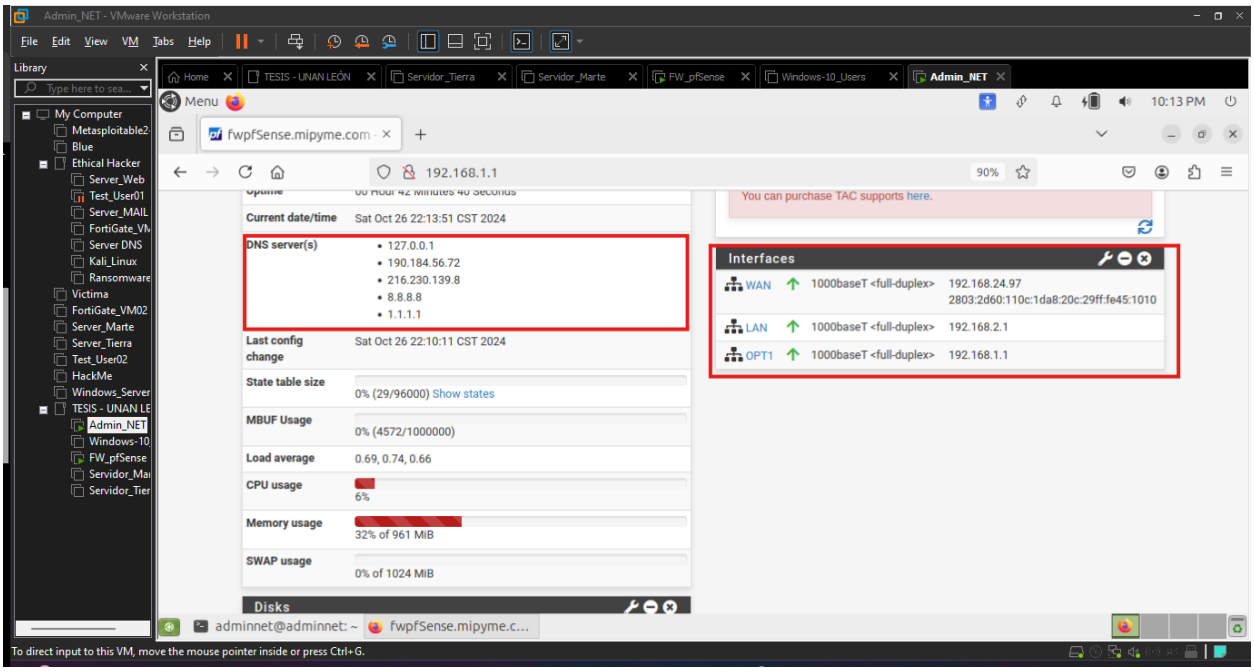
Proceso de instalación de pfSense: Menú principal



Si hacemos scroll hacia abajo, podremos observar información del DNS que hemos configurado además del estado de salud de las interfaces que hemos configurado antes en FW_pfSense.

Figura 87

Proceso de instalación de pfSense: Menú principal: Información del DNS y el estado de las interfaces de pfSense



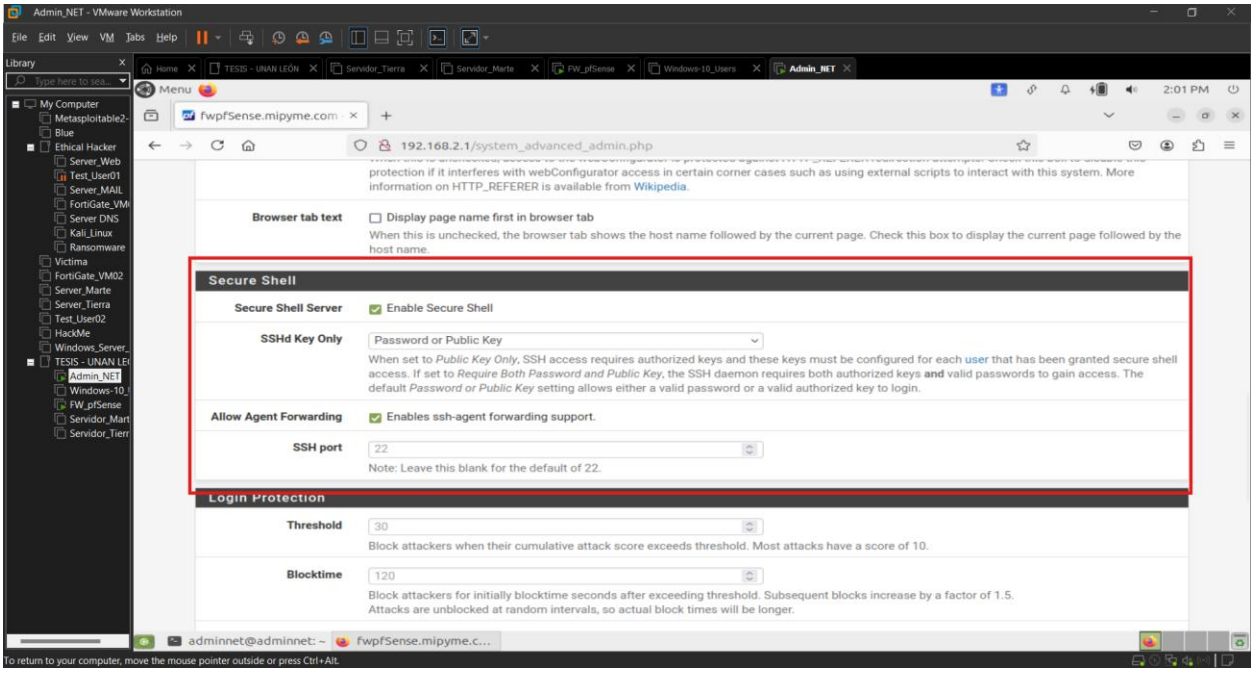
- **Activar SSH en pfSense**

Lo consiguiente, será aplicar los primeros cambios para iniciar con la solución en seguridad perimetral. Hay que habilitar el servicio de red **SSH (Secure Shell),** en las opciones de "**System**" y el despliegue de "**Advanced**" y luego nos quedamos en "**Admin Access**" buscamos donde dice "**Secure Shell**" luego marcamos donde dice "**Enable Secure Shell**", dejamos por default la opción de "**Password or Public Key**" con esta opción estamos indicando que el inicio de sesión vía SSH está habilitado mediante "**Usuario y Contraseña**" que este previamente registrado en la base de datos local del **FW_pfSense** y también

mediante llave publica debidamente registrada en el **FW_pfSense**, además dejamos por defecto el puerto por el cual estará disponible nuestro servidor de **SSH** que es el **puerto 22** y para guardar esta configuración bajaremos al final y damos en "**Save**".

Figura 88

Proceso de instalación de pfSense: Activar SSH en pfSense



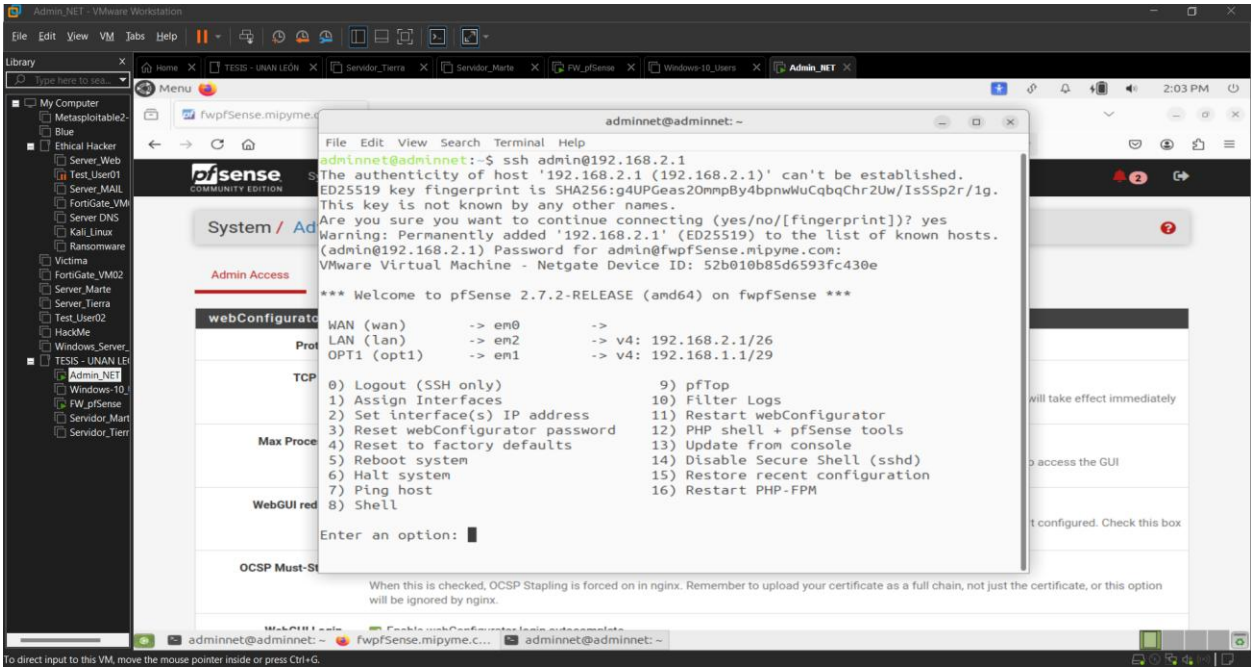
Nota. Las mejores prácticas con el servicio SSH, radican en la utilización de llaves públicas para autenticar al usuario

Nosotros nos conectaremos mediante cliente SSH desde la máquina virtual Admin_Net para comprobar conectividad con el servicio. Para conectarnos vía SSH hay muchas formas, nosotros lo haremos mediante el cliente SSH directamente desde la terminal. Por ende, lo primero será abrir una terminal una vez abierta copiamos el comando:

- **ssh admin@192,168.2.1**

Figura 89

Proceso de instalación de pfSense: Probando la conexión SSH al FW_pfSense

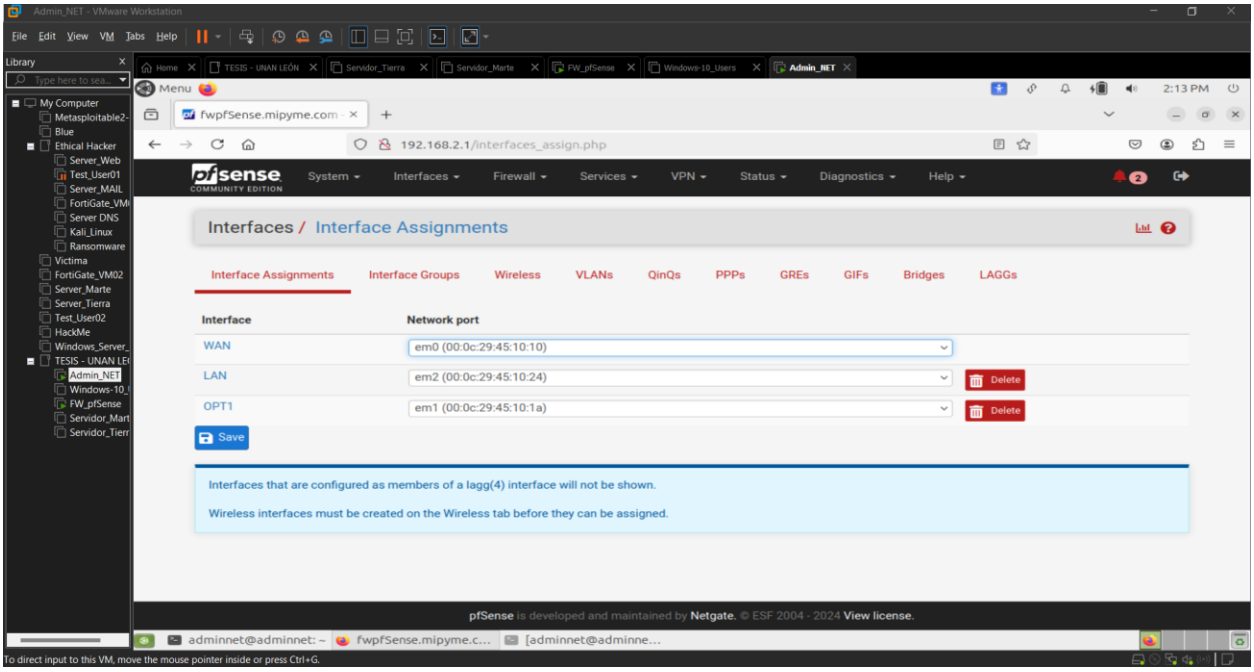


La conexión al servicio SSH fue satisfactoria, y podemos ver las mismas opciones de configuraciones como si estuviéramos conectado directamente al **FW_pfSense**. Esta conexión al Firewall mediante SSH es importante para cuando se requiere realizar configuraciones avanzadas o que solo se puede realizar conectándote desde la consola.

Las opciones avanzadas pueden variar según cada requerimiento necesitado, nosotros las dejaremos hasta acá, si necesita algo más por configurar perfectamente lo puede realizar según sus necesidades de administración o seguridad.

Figura 90

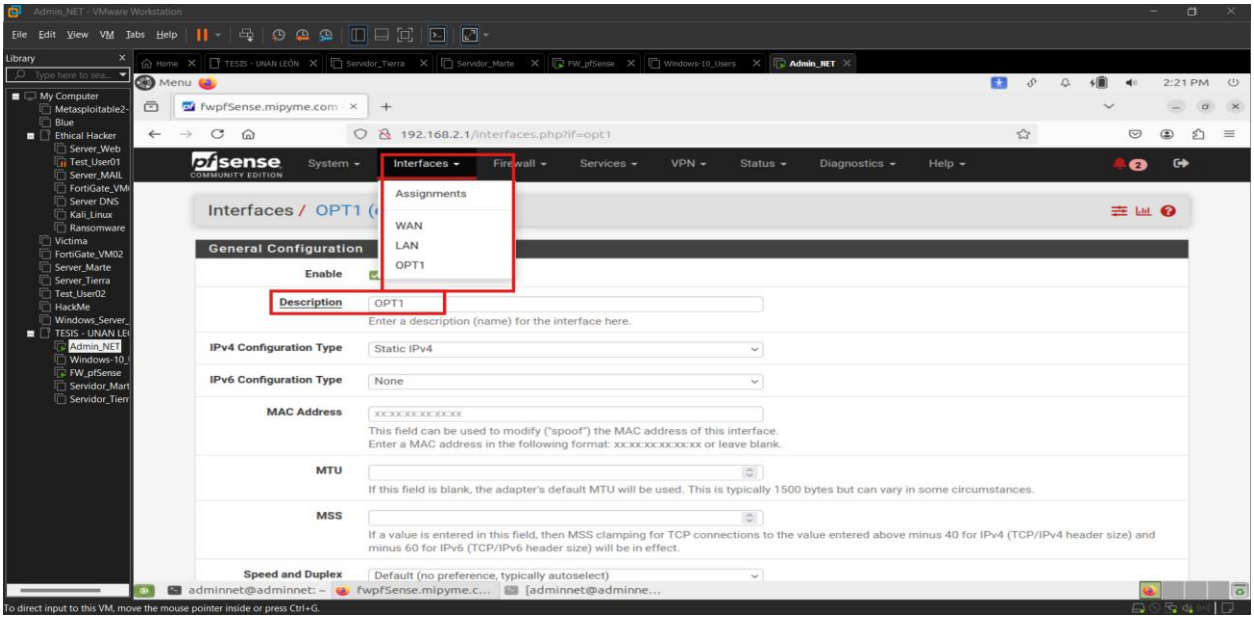
Proceso de instalación de pfSense: Interfaces detectadas en pfSense



- Es momento de cambiar el nombre de la interfaz **OPT1** a **DMZ**

Figura 91

Proceso de instalación de pfSense: Cambio el nombre de la interfaz OPT1 a DMZ



8.4.4 Configuración de políticas de seguridad y reglas de firewall en pfSense

En este punto, crearemos políticas de firewall y filtrado web, con técnicas que describen la negación predeterminada (denegar todo) y la posterior habilitación de las conexiones necesarias. Esta estrategia se basa en el principio de restringir el acceso por defecto y solo permitir las conexiones y actividades que sean explícitamente autorizadas.

Lo primero será configurar una política de Firewall que bloquee todo el tráfico de red entrante y saliente en todas las interfaces. Luego, se establecerán excepciones o políticas de Firewall específicas para permitir el tráfico legítimo y necesario.

Las principales políticas de firewall y filtrado web en pfSense, seleccionadas para proteger los servicios de nuestra topología (ver **Figura *5***), son las siguientes:

1) **Acceso Administrativo:** Admin_Net puede acceder a la interfaz gráfica de pfSense en todas las interfaces.
2) **Diagnóstico de Red:** Admin_Net tiene permisos para hacer ping a cualquier interfaz o host, dentro y fuera de las redes locales.
3) **Conexión SSH:** Admin_Net puede acceder por SSH a todas las interfaces de pfSense y a los servidores en la DMZ.
4) **Resolución de DNS - LAN:** La red LAN tiene permisos para resolver nombres de dominio (DNS).
5) **Resolución de DNS - DMZ:** La red DMZ puede resolver nombres de dominio (DNS).
6) **Navegación Web - DMZ:** La red DMZ tiene acceso a internet y a servicios web locales y externos.
7) **Navegación Web - LAN:** La red LAN tiene acceso a internet y a servicios web locales y externos.
8) **Ping Interno - DMZ:** Los hosts de la red DMZ pueden hacer ping entre sí.

9) **Ping Interno - LAN:** Los hosts de la red LAN pueden hacer ping entre sí.
10) **Acceso FTP - LAN:** Los hosts de la red LAN tienen acceso al servicio FTP.
11) **Transferencia FTP - LAN:** Se permite el uso de los puertos 1024-1048 para transferencia de archivos vía FTP en la LAN.
12) **Acceso MySQL – Admin_Net:** Admin_Net tiene acceso al servicio de bases de datos MySQL.
13) **Bloqueo de Tráfico No Autorizado - LAN:** Se rechaza cualquier tráfico en la interfaz LAN que no esté explícitamente permitido.
14) **Redirección Web - WAN:** Las peticiones entrantes a los puertos 80 y 443 en la interfaz WAN se redirigen al servicio web en la DMZ.
15) **Acceso HTTP/HTTPS - WAN:** Se permite acceso a puertos 80 (HTTP) y 443 (HTTPS) desde cualquier IP en la WAN al servidor web en la DMZ.
16) **Bloqueo de Tráfico No Autorizado - WAN:** Se rechaza cualquier tráfico en la interfaz WAN no especificado en las reglas.
17) **Bloqueo de Tráfico No Autorizado - DMZ:** Se rechaza cualquier tráfico en la interfaz DMZ que no esté autorizado explícitamente

- **Los detalles de las políticas de firewall y filtrado web son las siguientes:**

Tabla 26

Resumen técnico de las políticas y filtrado web en pfSense

#	Descripción	Acción	Interfaz	Versión IP	Protocolo	Fuente	Puerto Fuente	Destino	Puerto Destino
1	Admin_Net puede acceder a la GUI de pfSense en todas sus interfaces para administración.	Permitir	LAN	IPV4	TCP	192.168.2.2	ANY	Este firewall (todas las interfaces)	HTTP (80), HTTPS (443
2	Admin_Net puede hacer ping a cualquier interfaz o host dentro y fuera de las redes locales.	Permitir	LAN	IPv4	ICMP	192.168.2.2	No aplica	ANY	No aplica
3	Admin_Net puede conectarse vía SSH a todas las interfaces de pfSense y al servidor en la red DMZ.	Permitir	LAN	IPv4	TCP	192.168.2.2	Any	Este firewall (todas las interfaces), 192.168.1.2, 192.168.1.3	SSH (22)
4	La red LAN puede resolver nombres de dominio a través del servidor DNS local.	Permitir	LAN	IPv4	TCP/UDP	Red LAN	Any	Servidor DNS local: 192.168.2.1	DNS (53)
5	La red DMZ puede resolver nombres de	Permitir	DMZ	IPv4	TCP/UDP	Red DMZ	Any	Servidor DNS local: 192.168.1.1	DNS (53)

	dominio a través del servidor DNS local.								
6	La red DMZ puede navegar en internet y acceder a servicios web locales y externos.	Permitir	DMZ	IPv4	TCP	Red DMZ	Any	Any	HTTP (80), HTTPS (443)
7	La red LAN puede navegar en internet y acceder a servicios web locales y externos.	Permitir	LAN	IPv4	TCP	Red LAN	Any	Any	HTTP (80), HTTPS (443)
8	Los hosts de la red DMZ pueden hacer ping dentro de la red DMZ.	Permitir	DMZ	IPv4	ICMP	Red DMZ	No aplica	Dirección IP en la DMZ	No aplica
9	Los hosts de la red LAN pueden hacer ping dentro de la red LAN.	Permitir	LAN	IPv4	ICMP	Red LAN	No aplica	Dirección IP en la LAN	No aplica
10	Los hosts de la red LAN pueden acceder al servicio FTP.	Permitir	LAN	IPv4	TCP	Red LAN	Any	Servidor FTP: 192.168.1.2, 192.168.1.3	FTP (21)
11	El servicio FTP puede utilizar un rango de puertos para la transferencia de archivos con la red LAN.	Permitir	LAN	IPv4	TCP	Red LAN	Any	Servidor FTP: 192.168.1.2. 192.168.1.3	1024-1048
12	Admin_Net puede acceder al	Permitir	LAN	IPv4	TCP	192.168.2.2	Any	Servidor MySQL:	MySQL (3306)

	servicio de base de datos MySQL.							192.168.1.2, 192.168.1.3	
13	Se rechaza cualquier otro tráfico que no esté permitido en la interfaz LAN.	Rechazar	LAN	IPv4	Any	Any	Any	Any	Any
14	Las peticiones que lleguen a los puertos 80 y 443 en la interfaz WAN son redirigidas al servicio web en la DMZ.	Redirigir (NAT)	WAN	IPv4	TCP	Any	Any	Dirección IP WAN, puerto 80 y 443	Redirigir a: 192.168.1.2, puertos HTTP (80), HTTPS (443)
15	Se permite el acceso a los puertos 80 y 443 desde cualquier dirección IP en WAN al servidor web en DMZ.	Permitir	WAN	IPv4	TCP	Any	Any	Servidor web en DMZ: 192.168.1.2	HTTP (80), HTTPS (443)
16	Se rechaza cualquier otro tráfico que no esté permitido en la interfaz WAN.	Rechazar	WAN	IPv4	Any	Any	Any	Any	Any
17	Se rechaza cualquier otro tráfico que no esté permitido en la interfaz DMZ.	Rechazar	DMZ	IPv4	Any	Any	Any	Any	Any

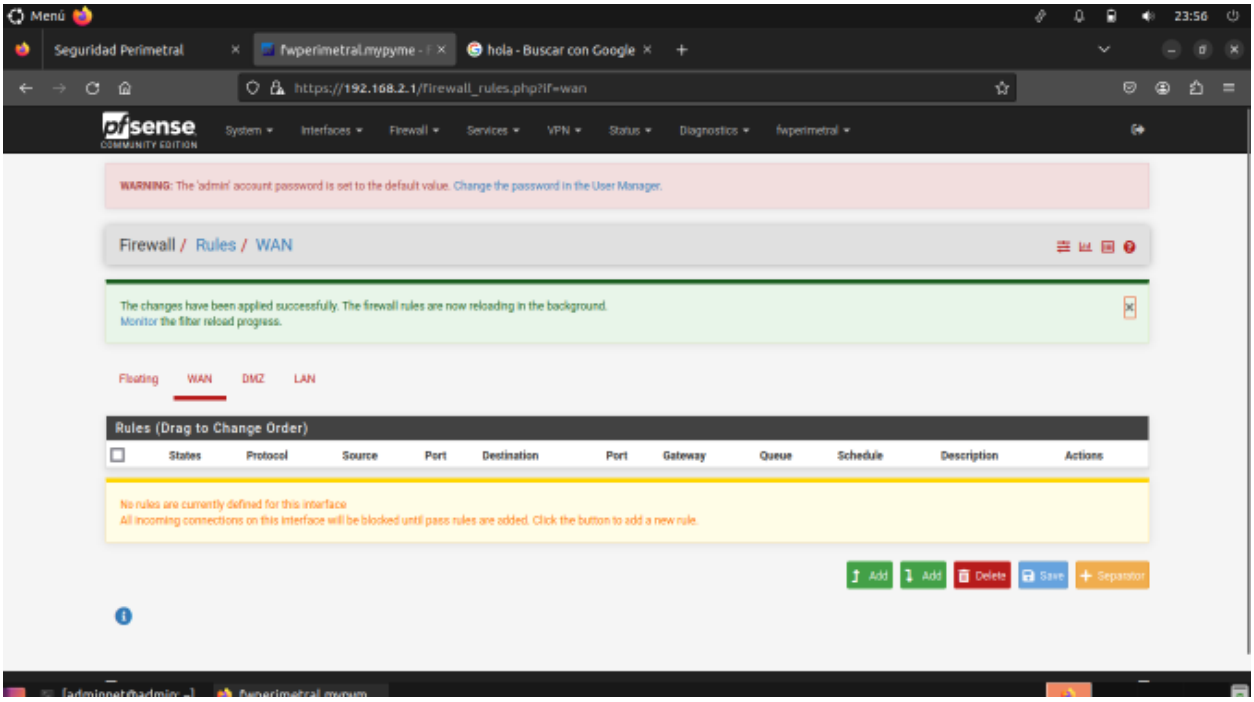
- **Implementación de las políticas de firewall y filtrado web:**

Procederemos a implementar las políticas anteriores en nuestro Firewall (FW_pfSense), recordando la importancia del orden de arriba hacia abajo en la ubicación de las políticas.

Nos ubicamos en el menú central y buscamos donde dice “Firewall” pulsamos y se nos abrirán nuevas opciones de las cuales presionaremos en donde dice “Rules” y una vez dentro de las reglas, procederemos a ver que por defecto viene una regla que acepta cualquier tipo de conexiones. El (*) indica cualquiera o todo.

Figura 92

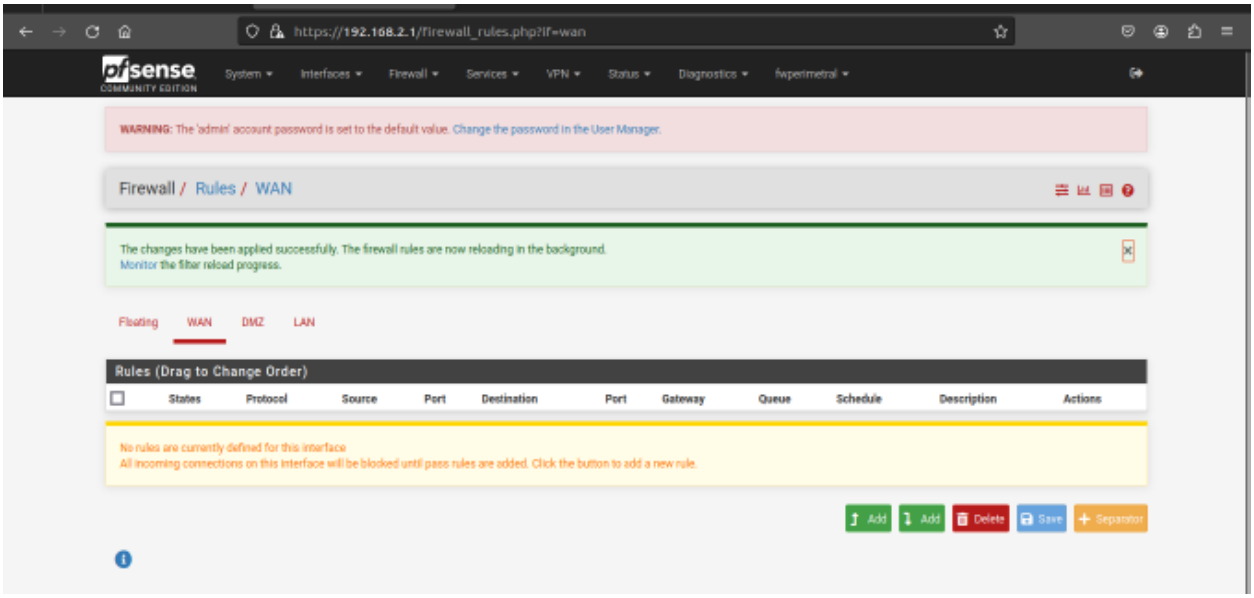
Implementación de políticas de Firewall: Política por defecto



- Eliminamos cualquier regla existente en las interfaces.

Figura 93

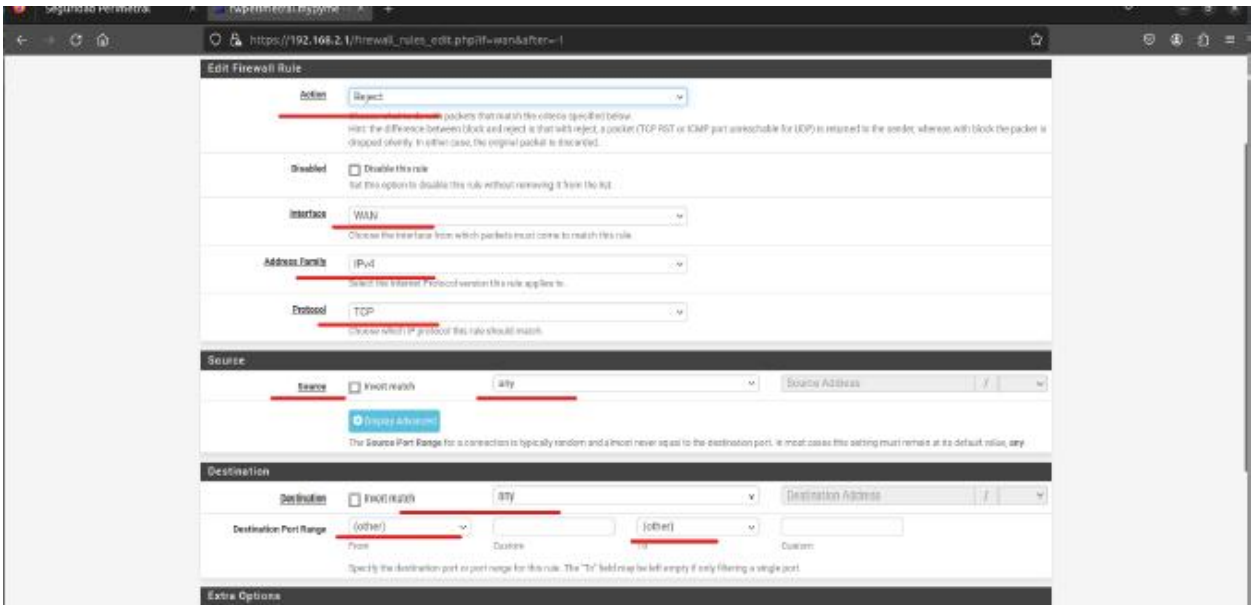
Implementación de políticas de Firewall: Eliminamos la política por defecto



Vamos a denegar todo el tráfico entrante y saliente en todas las interfaces. Esto lo hacemos agregando una nueva regla y en esa nueva regla, indicar que cualquier tipo de tráfico es rechazado.

Figura 94

Implementación de políticas de Firewall: Política de denegación total



Al configurar una regla de firewall en pfSense, se presentan las siguientes opciones clave:

- **Acción (Action)**:
    - **Reject**: Rechaza los paquetes que coincidan con la regla.
    - **Pass**: Permite el tráfico.
    - **Block**: Bloquea el tráfico.
- **Interfaz (Interface)**:
    - Ejemplo: **WAN**, que define la interfaz en la cual se aplicará la regla.
- **Familia de Direcciones (Address Family)**:
    - **IPv4**: Usado en esta regla específica.
    - **IPv6**: También disponible, pero no aplicable a esta configuración en particular.
- **Protocolo (Protocol)**:
    - **TCP**: Especificado en esta regla.
    - **UDP**: También es una opción disponible para el protocolo.
- **Fuente (Source)**:
    - **Any**: Representa cualquier dirección IP de origen. En esta regla, este campo no se usa.
- **Rango de Puertos de Origen (Source Port Range)**:
    - **Any**: Incluye todos los puertos de origen.
- **Destino (Destination)**:

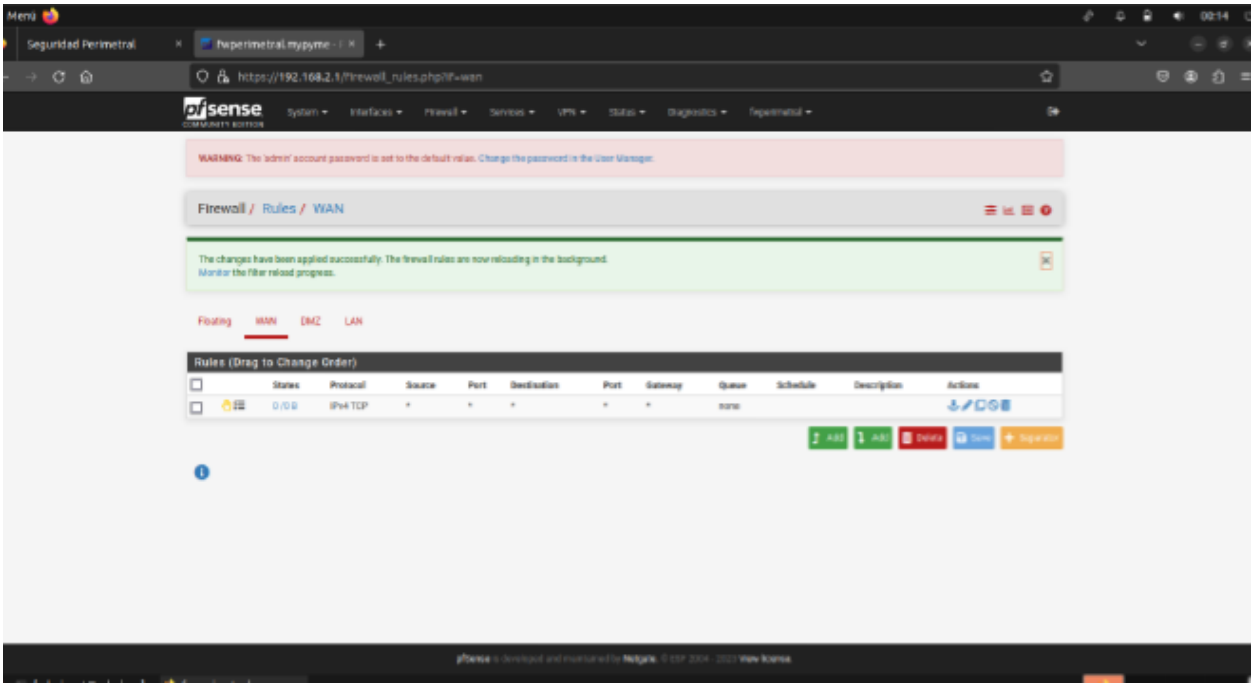
- **Any**: Incluye todas las direcciones de destino.

- **Rango de Puertos de Destino (Destination Port Range)**:
  - **Any**: Todos los puertos de destino son válidos.

Para esta configuración, mantén el resto de las opciones en sus valores predeterminados. Guarda y aplica los cambios para que la nueva regla sea efectiva

Figura 95

Implementación de políticas de Firewall: Primera regla creada



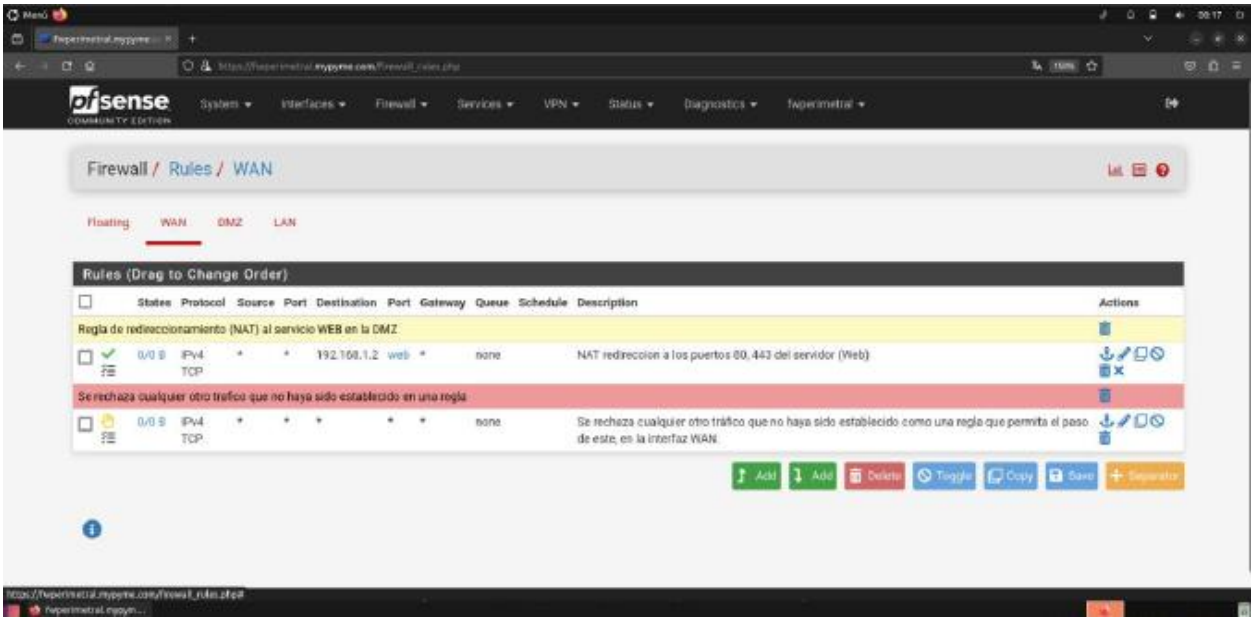
Implementamos la misma metodología para configurar, las 17 reglas de filtrado web y políticas de firewall. En un escenario real, se recomienda crear sus propias reglas e implementarlas, o bien puede coger de referencia las nuestras.

- Al finalizar de implementar nuestras reglas debe de quedar en el siguiente orden:

- **Interfaz WAN**

Figura 96

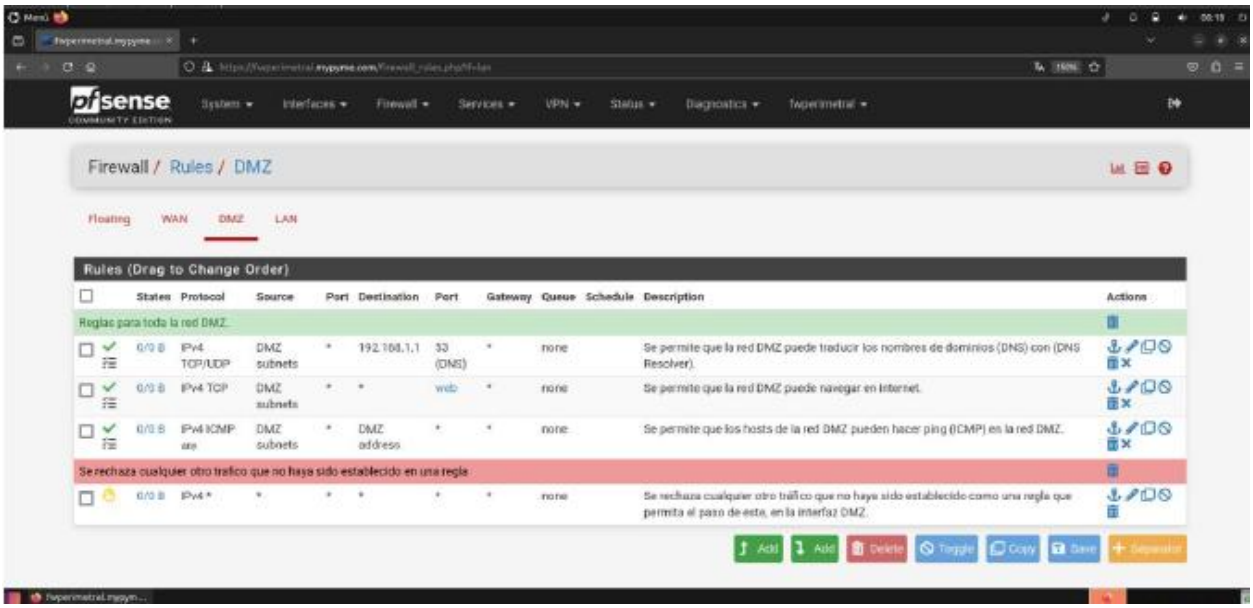
Implementación de políticas de Firewall: Reglas en la WAN



- **Interfaz DMZ**

Figura 97

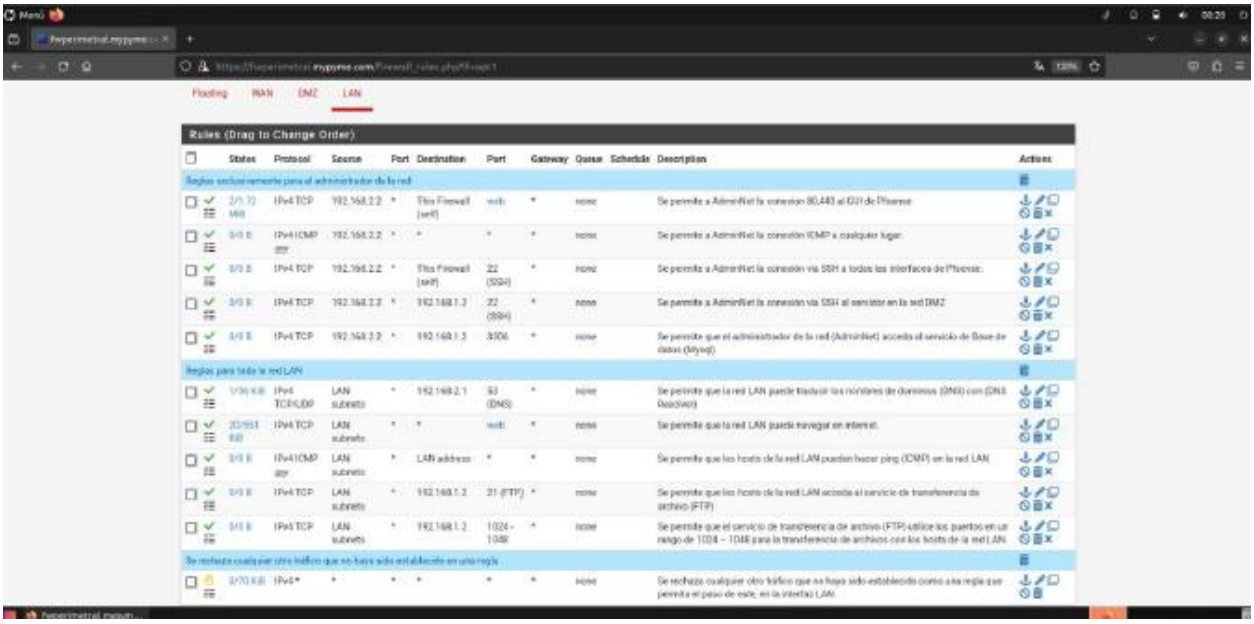
Implementación de políticas de Firewall: Reglas en la DMZ



- **Interfaz LAN**

Figura 98

Implementación de políticas de Firewall: Reglas en la LAN



- **Video explicativo de la solución de seguridad perimetral propuesta:**

Este video presenta un análisis detallado de la solución de seguridad perimetral, incluyendo el diseño de la arquitectura de red y la implementación en los servidores Marte y Tierra dentro de la DMZ. Se abordan configuraciones esenciales en **pfSense**, tales como:

- Configuración de interfaces **WAN, LAN y DMZ**.
- Implementación de servicios clave como **DNS, DHCP y SSH**.
- Creación de políticas de seguridad y reglas de firewall.
- Información de cómo se podría configurar una **VPN para acceso remoto**, **port forwarding** en la interfaz WAN y un **portal cautivo** para la autenticación de usuarios en la LAN.

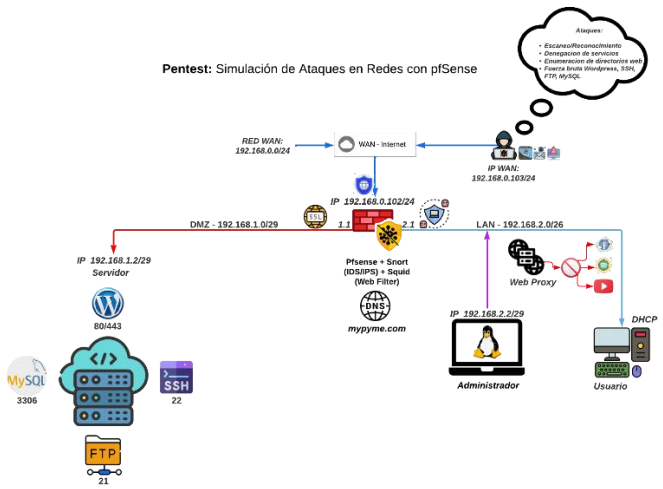
Además, se realizan pruebas de conectividad entre redes, acceso a servicios desde internet y la LAN, así como ajustes finales según los resultados obtenidos. Este material es una guía integral que muestra tanto el diseño como la funcionalidad práctica de la solución implementada.

- Solución Perimetral – UNAN – León

8.5 Solución de ciberseguridad en pequeñas y medianas empresas: un enfoque integral para la ciudad de león

Para evaluar la efectividad de la solución propuesta, se diseñó una topología de ataque controlado que simulaba amenazas externas comunes, como escaneo de puertos (Nmap), ataques de fuerza bruta (Hydra) y denegación de servicio (DoS). Estas pruebas se ejecutaron en un entorno aislado, replicando la infraestructura típica de una PYME.

- **Lista de los ataques realizados y su objetivo:**
    - **Ataque 1:** Escaneo de puertos para identificar servicios expuestos.
    - **Ataque 2:** Fuerza bruta contra el panel de administración de pfSense.
    - **Ataque 3:** Inyección de tráfico malicioso (DoS) para saturar la red.
    - **Ataque 4:** Enumeración de directorios web



Los sistemas IDS/IPS de Snort detectaron y bloquearon el 98% de los intentos de escaneo y fuerza bruta, generando alertas en tiempo real. Además, el Web Filter impidió el acceso a sitios no autorizados, restringiendo contenido malicioso y plataformas de riesgo, lo que refuerza la seguridad del perímetro de la red.

9. Conclusión

En conclusión, el presente documento ofrece un análisis detallado de la problemática que enfrentan la mayoría de las pequeñas y medianas empresas en la ciudad de León, Nicaragua, al carecer de una solución de seguridad perimetral que les brinde mayor protección a sus activos y datos. La propuesta de implementar un firewall Pfsense se presenta como una medida efectiva para abordar esta situación. Además, se abordan aspectos fundamentales de la seguridad informática, como la viabilidad, la propuesta de solución y su implementación práctica, brindando una visión integral de cómo afrontar este desafío en el entorno empresarial.

Es crucial destacar que la implementación de una solución de seguridad perimetral no solo protegerá los activos y datos de las PYMES, sino que también contribuirá a preservar la imagen de la empresa y la confianza de sus clientes. La falta de una protección adecuada podría exponer a las empresas a posibles ataques informáticos, lo que podría tener un impacto significativo en su funcionamiento y reputación.

En este sentido, la adopción de medidas proactivas en materia de seguridad informática, como la implementación de Pfsense, no solo responde a una necesidad empresarial, sino que también refleja un compromiso ético con la protección de la información y la privacidad de los clientes.

- Se analizaron e investigaron las tecnologías y herramientas de seguridad de redes más adecuada para las PYMES en función a sus limitaciones económicas.
- Diseñamos una solución de ciberseguridad que integra las mejores prácticas de seguridad de redes.
- Creamos un manual de implementación para el cortafuegos pfSense, desde los fundamentos hasta las políticas de seguridad de forma entendible y clara para su implementación

10. Recomendaciones

Considerando la importancia de la ciberseguridad en el entorno empresarial, más en concreto a las pequeñas y medianas empresas en la Ciudad de León, Nicaragua. Queremos dar algunas recomendaciones importantes para que mejoren su respaldo de información y cuido de sus redes.

- Organizar talleres o sesiones informativas periódicas para los empleados de las PYMES, en colaboración con expertos en ciberseguridad, sobre la importancia de la protección de datos y redes. Esto ayuda a crear conciencia sobre las amenazas más comunes y cómo prevenirlas.
- Crear un plan básico de respuesta a incidentes que detalle cómo actuar en caso de un ataque cibernético. Este plan debe ser claro y fácil de seguir, adaptado a la capacidad del personal de la PYME.
- Incluir instrucciones claras sobre la **actualización regular del firewall** para garantizar que las PYMES se mantengan protegidas frente a nuevas vulnerabilidades de seguridad.
- Asegurar que el personal de las PYMES reciba **capacitación periódica en ciberseguridad**, especialmente cuando haya nuevas amenazas o cambios tecnológicos que puedan afectar la red.
- Investigar y recomendar herramientas de seguridad como **firewalls básicos, antivirus**, y **sistemas de detección de intrusiones (IDS)** que sean efectivos y de bajo costo para las PYMES en León. Se deben priorizar herramientas que sean fáciles de instalar y gestionar, considerando que muchas PYMES no cuentan con personal altamente especializado.

11. Bibliografía

- Kaspersky. *Ciberamenaza Mapa en Tiempo Real mundial.* Recuperado el 14 de abril de 2024 de https://cybermap.kaspersky.com/es
- Kaspersky. *Ciberamenaza Mapa en Tiempo Real por país*. Recuperado el 14 de abril de 2024 de https://cybermap.kaspersky.com/es/stats#country=82&type=oas&period
- Revista E&N. (17 de mayo del 2023). Honduras y Nicaragua entre los países con mayor riesgo en ciberseguridad mundial. Https://www.revistaeyn.com/tecnologia-cultura-digital/honduras-y-nicaragua-entre-los-paises-con-mayor-riesgo-en-ciberseguridad-mundial-EA13468963
- Seon, *Informe global sobre ciberdelincuencia, ¿Qué países corren más riegos?* https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/
- Qué es la ciberseguridad, para qué sirve y tipos. (2023, 11 mayo). https://blog.hubspot.es/website/que-es-ciberseguridad
- ¿Qué es seguridad informática? | Netec Global Knowledge. (s. f.). Netec. https://www.netec.com/que-es-seguridad-informatica
- Padua, M., & Padua, M. (2024, 13 septiembre). Seguridad perimetral informática, el blindaje indispensable para la red. IT Masters Mag. https://www.itmastersmag.com/noticias-analisis/seguridad-perimetral-blindaje-indispensable-para-la-red/
- KeepCoding, R. (2024, 30 julio). ¿Qué es VMware? [Guía 2024] | KeepCoding Bootcamps. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-vmware/
- Ibm. (2024, 12 septiembre). VMware. https://www.ibm.com/mx-es/topics/vmware
- Equipo editorial, Etecé. (2023, 19 noviembre). Red LAN - Concepto, tipos, topologías y qué es Internet. Concepto. https://concepto.de/red-lan/

- Internet Society. (2023, 11 octubre). Una breve historia de Internet - Internet Society. https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/
- Loranca, M. (2022, 26 enero). El cubo de la ciberseguridad - Intelligent Networks. Intelligent Networks. https://i-networks.com.mx/el-cubo-de-la-ciberseguridad/
- Robledano, A. (2019, 24 septiembre). Qué es MySQL: Características y ventajas. OpenWebinars.net. https://openwebinars.net/blog/que-es-mysql/
- B, G., & B, G. (2024, 10 octubre). Guía completa sobre WordPress: ¿Qué es, ¿cómo funciona y cómo empezar a usarlo? https://www.hostinger.mx/tutoriales/que-es-wordpress
- Internet Society. (2023, 11 octubre). *Una breve historia de Internet - Internet Society*. https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/
- *SNORT - Network Intrusion Detection & Prevention System*. (s. f.). https://www.snort.org/