# FACULTAD DE CIENCIAS E INGENIERÍA
# ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA CON MENCIÓN EN TELECOMUNICACIONES

**TESIS**

**Para optar el título profesional de Ingeniero Electrónico con Mención en Telecomunicaciones**

Planificación de transición del Protocolo Ruckus Wireless al Protocolo pfSense para optimizar el servicio de red de datos de la Universidad de Ciencias y Humanidades

**PRESENTADO POR**

Coquis Flames, Jacqueline Mariel

**ASESOR**

Flor Cunza, Hugo

0000-0002-5337-7202

**Lima, Perú, 2023**

# INFORME DE ORIGINALIDAD ANTIPLAGIO TURNITIN

Mediante la presente, Yo:

1. Jacqueline Mariel Coquis Flames, identificada con CEXT 001974436

Somos egresados de la Escuela Profesional de Ingeniería Electrónica con mención en Telecomunicaciones del año 2023 – 01, y habiendo realizado[1] la___TESIS___ para optar el Título Profesional de [2]Ingeniero Electrónico con mención en Telecomunicaciones, se deja constancia que el trabajo de investigación fue sometido a la evaluación del Sistema Antiplagio Turnitin el 22 de noviembre de 2023, el cual ha generado el siguiente porcentaje de similitud de [3]: 16% (dieciséis por ciento)

En señal de conformidad con lo declarado, firmo el presente documento a los 24 días del mes de noviembre del año 2023.

| _____ | _____ | _____ |
|---|---|---|
| **Egresado 1** | **Egresado 2** | **Egresado 3** |

**Hugo Flor Cunza**
**Nombre del Asesor(a)**
**DNI 45283202**

[1] Especificar qué tipo de trabajo es: tesis (para optar el título), artículo (para optar el bachiller), etc.

[2] Indicar el titulo o grado académico: Licenciado o Bachiller en (Enfermería, Psicología …), Abogado, Ingeniero Ambiental, Químico Farmacéutico, Ingeniero Industrial, Contador Público …

[3] Se emite la presente declaración en virtud de lo dispuesto en el artículo 8°, numeral 8.2, tercer párrafo, del Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI, aprobado mediante Resolución de Consejo Directivo N° 033-2016-SUNEDU/CD, modificado por Resolución de Consejo Directivo N° 174-2019-SUNEDU/CD y Resolución de Consejo Directivo N° 084-2022-SUNEDU/CD.

# JACQUELINE MARIEL COQUIS FLAMES. TRABAJO FINAL

INFORME DE ORIGINALIDAD

| 16% | 16% | 2% | 5% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | repositorio.uch.edu.pe<br>Fuente de Internet | 4% |
| 2 | repositorio.upn.edu.pe<br>Fuente de Internet | 2% |
| 3 | Submitted to Universidad de Ciencias y Humanidades<br>Trabajo del estudiante | 2% |
| 4 | Submitted to Universidad Privada del Norte<br>Trabajo del estudiante | <1% |
| 5 | hdl.handle.net<br>Fuente de Internet | <1% |
| 6 | www.scribd.com<br>Fuente de Internet | <1% |
| 7 | idoc.pub<br>Fuente de Internet | <1% |
| 8 | www.coursehero.com<br>Fuente de Internet | <1% |
| 9 | qdoc.tips<br>Fuente de Internet | |

## Resumen

Actualmente, la ciberseguridad es un tema de gran interés, tanto para las grandes y pequeñas compañías como para los centros educativos, debido a que existen muchas maneras en las que el sistema de seguridad de una red pueda ser vulnerado. El presente trabajo tiene como contexto el campus de la Universidad de Ciencias y Humanidades, una universidad ubicada en Lima norte donde actualmente se tiene implementado el sistema de red de datos bajo los equipos y el software de Ruckus Wireless, al ser un software propietario, se deben realizar pagos regulares para mantener el sistema actualizado y protegido contra amenazas. En este sentido, el objetivo de la tesis es mejorar el servicio de red de datos mediante la planificación de transición del protocolo de software propietario al protocolo de software libre en la Universidad de Ciencias y Humanidades, donde la opción de software libre elegido es pfSense por ser robusto y altamente seguro. Asimismo, la metodología utilizada es la simulación por medio de máquinas virtuales en la plataforma de VirtualBox que permitirá configurar el sistema operativo de pfSense para luego comprobar las reglas establecidas a través de una simulación con pfSense instalado como servidor. Se logró realizar la simulación de manera efectiva y se logró comprobar el correcto funcionamiento de la configuración de pfSense por lo que se concluye que si es posible lograr una transición del protocolo Ruckus Wireless al protocolo pfSense de manera efectiva.


**Palabra clave:** Ciberseguridad, Seguridad de red, Software propietario, Software de codigo abierto, Dashboard.

**Abstract**

Currently, cybersecurity is a topic of great interest, both for large and small companies and for educational institutions, because there are many ways in which the security system of a network can be violated. The context of this work is the campus of the University of Sciences and Humanities, a university located in northern Lima where the data network system is currently implemented under the Ruckus Wireless equipment and software, as it is proprietary software, it is necessary to make regular payments to keep the system up to date and protected from threats. In this context, the objective of the thesis is to improve the data network service by planning the transition from the proprietary software protocol to the free software protocol at the University of Sciences and Humanities, where the free software option chosen is pfSense since it is robust and highly secure. Likewise, the methodology used is simulation through virtual machines on the VirtualBox platform that will allow configuring the pfSense operating system and then verifying the established rules through a simulation with pfSense installed as a server. The simulation was carried out effectively and the correct functioning of the pfSense configuration was verified, so it is concluded that it is possible to achieve a transition from the Ruckus Wireless protocol to the pfSense protocol effectively.

**Keywords:** Cybersecurity, Network Security, Proprietary Software, Open Source Software, Dashboard.

## Contenido

## Lista de Figuras

## Lista de Tablas

## Introducción

En la actualidad, la ciberseguridad es uno de los desafíos más importantes que enfrentan distintas instituciones y organizaciones, se debe procurar un sistema que no permita el acceso de atacantes que van en busca de información para su beneficio personal. En el año 2016 la Universidad de Calgary sufrió un ciberataque que paralizó varios de sus sistemas, esto fue hecho a través de un software malicioso que infectó varias máquinas, este incidente forzó a la universidad a pagar al atacante una suma de 20,000 dólares para asegurar varios sistemas importantes pudieran ser restablecidos y evitar que cualquier información personalpudiera ser divulgada, este incidente además de haber significado una pérdida de dinero también pasó a requerir un trabajo arduo por parte del personal de IT para asegurar la reparación de los daños ocasionados a las máquinas y aplicar los códigos necesario para desencriptar las máquinas afectadas. En este sentido, se puede apreciar cómo una red inalámbrica no segura puede causar consecuencias graves y llevar a representar grandes pérdidas de tiempo y dinero (CBC, 2016).

La Universidad de Ciencias y Humanidades es una universidad ubicada en Lima Norte, en Los Olivos, actualmente alberga una población total de 3507 estudiantes, y ofrece quince carreras diferentes; una parte importante e indispensable para el correcto funcionamiento de las instalaciones, tanto para los alumnos, el personal docente y administrativo es el óptimo estado de la red inalámbrica de Wi-Fi. La red Wi-Fi de una institución educativa debe estar asegurada contra amenazas de ciberataques debido a que de lo contrario se pone en riesgo la base de datos, la cual contiene información tanto de los estudiantes como del personal. En este sentido, la universidad debe contar con una topología de red inalámbrica apropiada para sus instalaciones que cumpla con los requerimientos necesarios para que la conexión a internet sea la más óptima y además garantice la protección de la información en la base de datos.

En la red inalámbrica de la Universidad de Ciencias y Humanidades, actualmente

se implementa un software propietario para garantizar la seguridad de la red. En este sentido, se ha procedido a buscar una opción de software de código abierto, que provea los protocolos de seguridad necesarios para la universidad y que permita el manejo de la red inalámbrica.

# CAPITULO I: PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

## 1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

### 1.1.1. Planteamiento y descripción del problema

Actualmente en la Universidad de Ciencias y Humanidades existe una red inalámbrica que conecta los distintos dispositivos en las instalaciones, dicha red está construida bajo el protocolo de software propietario de Ruckus Wireless, que es una compañía estadounidense adquirida y respaldada por Commscope que provee los equipos de hardware y software de tecnología diseñada para redes alámbricas e inalámbricas. De este modo, al adquirir el servicio de Ruckus Wireless, la Universidad de Ciencias y Humanidades ha recibido los equipos necesarios para hacer el despliegue de la red de datos y el software para gestionarla. Los equipos que se han adquirido son tres modelos de Access Point (Ruckus R500, Ruckus R310 y Ruckus T300) y un Zone Director el cual actúa como el centro del despliegue de la red ya que se encarga de manejar el funcionamiento de los Access Point de manera centralizada haciendo que se sincronicen automáticamente ajustando los niveles de potencia de transmisión y las asignaciones de canal de radio frecuencia.

Sin embargo, Ruckus Wireless también tiene un historial de vulnerabilidades en sus productos que afecta directamente a sus clientes. En 2019, un investigador de sistemas de seguridad, logro descubrir un numero de vulnerabilidades en la interface web para los routers Wi-Fi de Ruckus, las cuales fueron dadas a conocerse en el trigésimo sexto congreso “Chaos Communication Congress” llevado a cabo en Leipzig, Alemania en diciembre de 2019, en su investigación se descubrió la posibilidad de fuga de información y credenciales, omisión de autenticación, inyección de comandos,

recorrido de ruta, desbordamiento de pila y lectura/escritura de archivos arbitrarios, se analizaron 33 Access Point de Ruckus y se encontró que todos eran vulnerables. Dichos descubrimientos fueron reportados a Ruckus, quienes publicaron un aviso de seguridad el 24 de diciembre de 2019 (Commscope, 2019). Diez de estas vulnerabilidades fueron dadas números de identificación en la base de datos de vulnerabilidades y exposiciones comunes (CVE-2019-19834 a CVE-2019-19843) (CISA, 2020).

En 2023, nuevamente se han hallado puntos débiles en múltiples productos de Ruckus Wireless, motivo por el cual La Agencia de Ciberseguridad e Infraestructura (CISA) ha agregado estas vulnerabilidades a su “Catalogo de Vulnerabilidades Explotadas Conocidas”, indicando que el software de los Access Point de Ruckus Wireless contienen una vulnerabilidad en el componente de los servicios web, dichas fallas fueron registradas bajo el número CVE-2023-25717 de vulnerabilidades y exposiciones comunes (CISA, 2023). Si este componente web está habilitado en los Access Point, un atacante podría llevar a cabo una falsificación de solicitud entre sitios (CSRF) o una ejecución de código de manera remota (RCE), esto podría incluso afectar al Zone Director de Ruckus y panel de administrador en versión 10.4 y anteriores. Estas fallas de seguridad podrían afectar a miles de usuarios que hacen uso de los productos de la compañía ya que los dispositivos pueden ser accedidos de manera remota a través de internet dando un punto de inicio al atacante desde el cual podría ingresar al resto de la red corporativa si esta presenta más vulnerabilidades.

En ese sentido, es de gran importancia realizar una transición del protocolo de software propietario de Ruckus Wireless al protocolo de software libre de pfSense, debido a que la naturaleza transparente del software de código abierto puede potenciar la integridad y puede brindar un rendimiento mejorado debido a que al ser liberado para

una comunidad desarrolladora más grande permite mejoras sucesivas que se realizan de manera continua al software lo que también incrementa la sostenibilidad a largo plazo (Heron, Hanson y Ricketts, 2013).

### 1.1.2. Formulación del problema general

¿Cómo llevar a cabo la transición del protocolo de software propietario al protocolo de software libre para garantizar la mejora del servicio de red de datos de la Universidad de Ciencias y Humanidades?

### 1.1.3. Formulación de los problemas específicos

**P.E.1:** ¿Cuál es la situación actual del servicio de la red de datos de la Universidad de Ciencias y Humanidades?

**P.E.2:** ¿Cuál será la topología y la arquitectura de la red de datos de la Universidad de Ciencias y Humanidades?

**P.E.3:** ¿Cuál será el modelo de la red de datos para optimizar el servicio de red de datos de la Universidad de Ciencias y Humanidades?

**P.E.4:** ¿Cómo comprobar la efectividad del diseño planteado de red de datos para la Universidad de Ciencias y Humanidades?

## 1.2. DEFINICIÓN DE LOS OBJETIVOS DE LA INVESTIGACIÓN

### 1.2.1. Objetivo general

Diseñar y planificar el servicio de red de datos mediante el protocolo Ruckus Wireless al protocolo pfSense para optimizar la red inalámbrica de la Universidad de Ciencias y Humanidades.

### 1.2.2. Objetivos específicos

**O.E.1:** Determinar la situación actual de la red de datos de la Universidad de Ciencias y Humanidades.

**O.E.2:** Conocer la topología y la arquitectura de la red de datos de la Universidad de Ciencias y Humanidades.

**O.E.3:** Diseñar un modelo de red de datos para optimizar el servicio de la red de datos de la Universidad de Ciencias y Humanidades.

**O.E.4:** Simular la efectividad del diseño de la red de datos optimizada.

## 1.3. JUSTIFICACION DE LA INVESTIGACION

### 1.3.1. Justificación técnica.

El sistema de seguridad que se planteará, utilizará un software de códigoabierto y gratuito para proveer una alta seguridad al sistema de red inalámbrica de la Universidad de Ciencias y Humanidades, este software permitirá configurar un firewall para proteger el sistema de ataques y permitirá la configuración de routers a través de una gestión unificada contra amenazas para brindar un alto nivel de seguridad.

### 1.3.2. Justificación económica.

En la Universidad de Ciencias y Humanidades, actualmente, se utiliza unsistema de seguridad basado en un software propietario, Ruckus Networks, este software pertenece a la compañía CommScope y brinda soluciones de seguridad para redes de alto rendimiento, es un sistema de estructura de tipo empresarial que permite que el número de usuarios conectados a la red a través de

un solo equipo sea mayor sin comprometer el rendimiento de la misma ya que tiene más capacidad en cuanto a la concurrencia de dispositivos. Ruckus Networks solamente es compatible con los equipos de su misma marca, estos dispositivos son integrados a la red y el sistema permite gestionar múltiples enlaces. El sistema que se planteará en el presente trabajo estará basado en un software de código abierto, pfSense (Aggarwal, 2018), este tipo de sistema se podría implementar sin ningún costo de manera que se logre alcanzar un alto nivel de seguridad en las instalaciones de la universidad,de igual manera permite la configuración de firewall, router y manejo dela carga en la red de una manera sencilla.

### 1.3.3. Justificación social.

La Universidad de Ciencias y Humanidades actualmente cuenta con un sistema de seguridad de software propietario, el cual viene con un costo para poder ser utilizado, este sistema permite la implementación de lared inalámbrica en todo el campus. En este sentido, el proyecto que se planteará está basado en un software de código abierto, lo que permitirá que su implementación sea más económica y compatible con una más amplia variedad de hardware. Un alto nivel de seguridad es de vital importancia para garantizar que la base de datos y la información personal de los estudiantes y del personal docente y administrativo está completamente seguro.

## 1.4. ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN

### 1.4.1. Alcances

- Se desarrollará una propuesta de un modelo de red seguro para la red inalámbrica de la Universidad de Ciencias y Humanidades.
- El presente proyecto planea llegar a la propuesta de un diseño que pueda ser viable y escalable a un sistema más complejo.
- El sistema cumplirá con las necesidades de seguridad para la red de la Universidad de Ciencias y Humanidades y será desarrollado con un software de código abierto de manera que no tenga ningún costo.
- El sistema de seguridad de la red se podrá controlar mediante un Dashboard donde se podrá gestionar fácilmente cada aspecto de la red y se podrán visualizar los equipos y sus características.

### 1.4.2. Limitaciones

- El proyecto tendrá como límite geográfico el campus de la Universidad de Ciencias y Humanidades.
- El proyecto no empleará software propietario debido a los altos costos.
- El diseño de red debe ser de gestión centralizada de modo que sea más sencillo el manejo de los distintos aspectos de la red a nivel de toda la universidad.
- El diseño del sistema de seguridad en la red inalámbrica, al tratarse de un proyecto de tesis, está sujeto a un límite de tiempo para su culminación.

# CAPÍTULO II: FUNDAMENTO TEÓRICO

## 2.1. ANTECEDENTES DE LA INVESTIGACIÓN

### 2.1.1. Internacionales

Los autores Muntaka et al. (2021) basan su estudio en la Universidad de Kessben,la cual cuenta con muchos departamentos y secciones, donde varias computadoras están programadas para proveer el servicio a todo el campus, la demanda de muchos equipos y de estas computadoras como servidores incrementa con el crecimiento de la universidad y su desarrollo, en vista a esta problemática los autores proponen la implementación de un sistema integrado quesería la solución para minimizar gastos estructurales además de la ventaja que representa tener un sistema centralizado para la administración, el sistema también brindará un firewall robusto que servirá como mecanismo de defensa alos servicios completos, utilizando también un manejo de amenazas unificado (UTM) que pondría todas las soluciones de seguridad juntas. Se hace uso de un sistema operativo de código abierto llamado Nethserver, el firewall de Nethserver ha mejorado mucho con la implementación de inspección profunda de paquetes utilizando nDPI, el administrador puede fácilmente crear las reglas para el firewall donde puede dar o restringir el acceso de las PC a las páginas que se deseen. Luego de la implementación los autores concluyen que hay un uso efectivo del hardware disponible y que el sistema funciona sin problemas y que el acceso a la red también ha sido mejorado usando la funcionalidad UTM en Nethserver OS.

Según Sharma, Manuja, Puri y Kumar (2021), la asignación y gestión de ancho de banda es de gran importancia para asegurar la eficiencia del rendimiento de una red y que esto también representa uno de los problemas más resaltantes en las organizaciones en la

actualidad, los proveedores comerciales de este servicio en este campo son de alto costo en términos de tiempo y dinero. En vista a esta problemática los autores realizan el desarrollo de la personalización de una aplicación de código abierto la cual han dado el nombre de "RadSense" para dar un mejor rendimiento a una red de dos mil nodos. Han hecho uso de las aplicaciones de código abierto pfSense y Radius, tomando pfSense lo han instalado en un dispositivo que luego se conectó a la red de 2500 nodos, en la misma red han instalado y configurado el software de Free Radius en la máquina de pfSense, después de habilitar un portal cautivo se conectó la aplicación de Radius a una base de datos en MySQL. Los autores han hecho la implementación de RadSense para ayudar a los administradores de la red a tener un mejor manejo de los usuarios y de los servicios, demostrando una manera en la que se puede configurar el portal cautivo de pfSense y un servidor local de Radius para usuarios autentificados en una red alámbrica e inalámbrica y asegurar las credenciales de los usuarios. Los resultados mostraron que se logró la implementación de un sistema que ayudará a las organizaciones con el manejo de los recursos actuales y que con el mecanismo AAA de pfSense los administradores de la red pueden monitorear los recursos utilizados por los usuarios. Los autores concluyen que se logró integrar de manera efectiva pfSense, MySQL y Radius en una sola plataforma donde todo puede manejarse desde una aplicación llamada "RadSense" con sus propias características.

Tudosi, Graur, Balan y Potorac (2023) indican que el acenso en el número de crímenes cibernéticos está afectando a numerosas empresas a nivel mundial ya que no existe ninguna industria o negocio que tenga un máximo de protección en ese campo. Los daños que se producen pueden llegar a minimizarse siempre y

cuando se realice una revisión periódica del sistema, estas revisiones se llevan a cabo siguiendo un protocolo que incluye pruebas de penetración al sistema, escáneres de vulnerabilidad, y evaluaciones de la red. En este sentido, los autores mencionan que su estudio estará basado en resolver los problemas más comunes que se encuentran en un firewall de código abierto, haciendo uso de pfSense llevaron a cabo diversas pruebas para detectar puntos vulnerables para la red, las herramientas utilizadas para hacer la revisión de la red también se basaron en soluciones de código abierto como Kali Linux para llevar a cabo la revisión manual. Luego de realizar las pruebas e identificar los puntos débiles de la red los autores mencionan en su solución propuesta el implementar un analizador de protocolo de red como Wireshark que realice una inspección de los paquetes, como incluso de esta manera existes caminos alternativos para esquivar estas reglas establecidas en el sistema, los autores indican que la solución a esto se encuentra en las configuraciones personalizadas que se realizan en el firewall principal. Realizando estas configuraciones personalizadas se logra ocultar el firewall y protegerlo de escaneos de red, debido a esto, los autores resaltan que pfSense es una solución de firewall eficiente. En sus resultados, resaltan que todas las vulnerabilidades detectadas en la red pueden ser resueltas realizando las actualizaciones de software respetivas ya que las versiones más recientes proveen soluciones a problemas pasados. En sus conclusiones proponen el uso de otras herramientas de código abierto para detectar vulnerabilidades y mejorar eficiencia de pfSense.

### 2.1.2. Nacionales

Almidon (2019), indica que en la actualidad la tecnología ha avanzado rápidamente de manera que ha cambiado muchos

procesos y también los quehaceres de la vida diaria, en este sentido se presenta de la igual manera el peligro que acarrea este avance tecnológico el cual es el robo de información a organizaciones de toda clase incluyendo las intuiciones educativas. El estudio se centra en la Universidad Nacional de Huancavelica la cual tiene el ComplejoEducativo de Servicios Académicos donde se lleva a cabo la mayor parte del área administrativa. Los sistemas de información utilizados se basan en nivel WAN y nivel LAN. La red WAN presenta el problema de lentitud de acceso a las aplicaciones de la red, un 60% de los hosts pierden conectividad con la red de datos, reportes de perdida de datos en los sistemas de gestión documentaria, reportes del personal de soporte informático indicando que un 60% de los equipos han sido infectados con software maliciosos como virus o spyware. En vista de esta problemática el autor ha propuesto el diseño de un modelo de red basado en redes virtuales de área local para la protección de la información en la UniversidadNacional de Huancavelica, las VLAN permiten que se implementen políticas de acceso y seguridad para grupos de usuarios en particular lo que incrementa la seguridad. Luego de la implementación el estudio mostró que se redujo el tiempo de espera en las aplicaciones LAN de 77,35 a 15.79 ms promedio, mostró una disminución significativa de casos de pérdidas de datos de 1076 a 201, y redujo el porcentaje de acceso a servicios no autorizados de 88% a 9% para las redes a nivel LAN y de 89% a 2% a nivel de redes WAN, por este motivo el autor concluye que la implementación de redes virtuales de área local VLAN mejora la seguridad de la red de la Universidad Nacional de Huancavelica.

Asimismo, Pitancur (2019), señala que actualmente para proporcionar un sistema de red seguro en una organización como una empresa es necesario tomar en cuenta el aspecto de la

rentabilidad de la empresa ya que la implementación debe estar basada en el presupuesto disponible que se tenga para invertir con este propósito. El estudio se centra en la compañía Corporación Cayman S.A.C, que es una empresa dedicada al área de las motocicletas y maquinaria, la empresa ha crecido y ha movido su ubicación a un local más grande en Callao, por lo que el autor propone un diseño e implementación de una red de datos de seguridad perimetral basándose en un sistema ERP llamado Spring, igualmente se plantea implementar un Centro de Datos para la mejor organización de la información de manera que la red esté centralizada. Para la simulación del proyecto el autorutilizó un software llamado Opnet para realizar la topología de la red LAN. Luego de la implementación se pudieron obtener los resultados del Centro de Datos paraver el funcionamiento de la red, en los cuales se evidenció un retardo en la red de 85μs además de concluir que si se ha logrado centralizar la red de datos por loque se incrementa la confiabilidad y seguridad de la información lo cual también es reforzado con la instalación de un firewall, se comprobó el buen funcionamientodel sistema ERP Spring y la conexión con las demás sedes, y se logró restringir el acceso a internet de usuarios no autorizados.

Según Ayala (2022), su estudio se basa en la red inalámbrica del IESTP San Pedro, indica que dicha red no tiene ningún control de usuarios y que las páginas web no se encuentran restringidas. En vista a esta problemática, el autor propone realizar un análisis para determinar cómo afecta la implementación de un portal cautivo para administrar la seguridad de la información en la red inalámbrica. Se utilizó el instrumento Nessus y Packet Loss Test para la recolección de la información a ser tomada en cuenta para el análisis, tomó una población de 256 usuarios, una muestra de 154 usuarios y se

procesó la información con el software SPSS. Los resultados obtenidos mostraron una disminución de accesos a servicios no autorizados de 70.97%(Pre-test) a 3.99%, se logró de igual manera reducir el tiempo promedio de respuesta de navegación de 111.37 ms (Pre-test) a 68.45 ms, se redujo el porcentaje de pérdida de paquetes de 38.95% (Pre-test) a 4.64%, Se concluye finalmente que el portal cautivo mejoró notablemente la administración y seguridad de la red inalámbrica del IESTP San Pedro.

## 2.2. MARCO TEÓRICO

### 2.2.1. Protocolo

La palabra “Protocolo” abunda en la tecnocultura. Los protocolos son reglas convencionales y estándares que gobiernan las relaciones dentro de las redes de comunicación, con frecuencia estas relaciones vienen en la forma de una comunicación entre dos o más computadoras, pero la palabra “redes” puede referirse a cualquier sistema de interrelacionalidad, que podría ser biológico o informático, orgánico o inorgánico, técnico o natural. Un protocolo en redes de comunicación se define como un conjunto de reglas que aseguran que las conexiones funcionen, es un sistema para mantener la organización y el control. En un sentido más amplio, un protocolo es una tecnología que regula el flujo y dirige espacio en la red (Galloway y Thacker, 2004).

Un protocolo se refiere a una tecnología de organización y control que opera en redes distribuidas. Los protocolos existen en las redes de computadoras contemporáneas, pero también se aplican en una variedad de redes biológicas y bioinformáticas (Galloway, 2006).

### 2.2.2. Wide Area Network (WAN)

Una Red de Área Amplia en telecomunicaciones se define como una red que cubre un área extensa, dicha área puede ser metropolitana, regional o nacional (Zhang et al., 2011).

### 2.2.3. Local Area Network (LAN)

Una Red de Área Local consiste en un numero de terminales de computadora que están conectados a través de un servidor. Las redes de Área Local normalmente se utilizan en negocios, laboratorios y en el ámbito industrial donde los empleados deben comunicarse y compartir información estando todos en el mismo espacio o área (Braine y Yorozu, 1998).

### 2.2.4. Virtual Local Area Network (VLAN)

Las Redes Virtuales de Área Local son una tecnología que permite dividir una red física ya que el administrador puede hacer particiones en una red local para formar redes más pequeñas separadas e independientes (Mehdizadeha et al., 2017).

### 2.2.5. Redes Inalámbricas

Una red inalámbrica es un tipo de red en la que los dispositivos permanecen conectados a la red, pero sin necesidad de estar conectados físicamente a través de cables. Los puntos de acceso amplifican la señal de Wi-Fi de manera que los demás dispositivos puedan estar lejos de los routers pero aun estén conectados a la red (Cisco, 2023).

### 2.2.6. Seguridad de las VLAN

Las VLAN son capaces de proveer más seguridad a la arquitectura de la red ya que los administradores de la red pueden tener control sobre cada puerto, esto impide que un atacante conecte su

dispositivo a cualquier switch de la red y robe información sin ser detectado, el tráfico sensible que se origina de la compañía o empresa puede también ser controlado o restringido con el uso de redes virtuales de área local (Mehdizadeha et al., 2017).

Algunos de los ataques más comunes que se presentan en las Redes Virtuales de Área Local son:

- **Address Resolution Protocol (ARP) Spoofing.** ARP Spoofing es un método en el cual el atacante envía un mensaje de Protocolo de Resolución de Direcciones (ARP) falsificado. El propósito principal de este tipo de ataque es asociar la dirección MAC con la dirección IP de otro nodo, como el del default gateway, de manera que todos los mensajes que se envían a esa dirección IP en particular los recibe el atacante (Mehdizadeha et al., 2017).
- **LAN Hopping.** Un ataque de VLAN Hopping se realiza mediante el envío de paquetes con el código de identificación de la VLAN que se tiene como objetivo, ese código al ser revisado en la red permite el paso de los paquetes hacia la VLAN objetivo (Mehdizadeha et al., 2017).
- **MAC Flooding.** Es un método que se implementa para comprometer la seguridad de los switches de la red. En este ataque el atacante envía muchas direcciones MAC falsas con el propósito de saturar la memoria limitada en el switch que guarda la tabla de direcciones MAC. El tráfico se sobrepasa y queda expuesto debido a que el switch ya no puede mantener las direcciones de destino especificas en la memoria (Mehdizadeha et al., 2017).
- **Filtrado de Ingreso.** Es un método que se utiliza para asegurarse de que los paquetes entrantes provengan de las

redes que afirman su origen. Este método también puede ser utilizado como medida de protección contra ataques a la red (Mehdizadeha et al., 2017).

### 2.2.7. Calidad de Servicio (QoS)

El propósito principal de QoS es proveer un buen servicio en accesibilidad al usuario final. Para aplicar la calidad de servicio de una manera efectiva en una red el usuario debe poder alcanzar la infraestructura de red que contiene las aplicaciones (Azamuddin et al., 2020).

### 2.2.8. Lista de Control de Acceso (ACL)

Un firewall no detecta los nuevos ataques generados por un intruso, pero clasifica el tráfico basándose en las reglas de la Lista de Control de Acceso. Antes de procesar un paquete para enviarlo a su destino, el paquete debe ser analizado para revisar vulnerabilidades, un módulo de categorización de tráfico agrupa los paquetes indicando cuales se consideran vulnerables y no vulnerables (Ramprasath y Seethalakshmi, 2021).

### 2.2.9. FTP (File Transfer Protocol)

Un protocolo de transferencia de archivo (FTP) se utiliza para proteger el intercambio de información en una red, la mayoría de los FTP se basan en tres funciones criptográficas principales para proteger la información: cifrado de clave pública, firmas digitales e intercambio de claves (Villamora, Lim y Sebial, 2019).

### 2.2.10. TCP/IP (Transmission Control Protocol/ Internet Protocol)

Es un grupo de protocolos que permiten que un grupo de computadoras puedan comunicarse e intercambiar información en una red y en internet. Un protocolo es una secuencia de reglas que

le permiten a una computadora conectarse con otra. Las computadoras pueden conectarse a internet gracias a este protocolo (Villamora, Lim y Sebial, 2019).

### 2.2.11. Red de datos

Una red de datos es un sistema diseñado para transferir información entre varios dispositivos conectados entre sí a través de la conmutación de datos, líneas de transmisión y sistemas de control. (Bertsekas y Gallager, 2021).

### 2.2.12. Ruckus

Ruckus es un software de seguridad de redes alámbricas e inalámbricas para el diseño de redes con propósitos específicos para las compañías en las que se implementen, de igual manera, Ruckus también provee equipos de red que hacen uso de Internet de las cosas (IoT) para la implementación, es una marca propiedad de CommScope. Ruckus permite la implementación de redes de área local de alto rendimiento para interiores y exteriores (CommScope, 2022a).

### 2.2.13. Características de Ruckus.

Ruckus Wireless es un sistema de seguridad consistente, con baja taza de pérdida de paquetes y alto rendimiento. El portafolio de Ruckus Wireless tienedisponibilidad de puntos de acceso, switches y routers, además de ofrecer manejode servicios basados en la nube (CommScope, 2022a).

Actualmente en la Universidad de Ciencias y Humanidades se hace uso del Zone Director de Ruckus Wireless y tres tipos de Access Point de Ruckus Wireless diferentes:

- **Zone Director.** Se encarga de la conexión de dispositivos, controlando automáticamente las asignaciones de los canales y los niveles de las potencias de transmisión actuando como un sistema de control central para los puntos de acceso de Ruckus. Permite extender conexión Wireless en una red evitando la conexión via ethernet a cada Access Point. La licencia por el Zone Director de Ruckus Wireless es de $30.00 por Access Point y la licencia de soporte es de $450 por año. (CommScope, 2022b).

- **Ruckus r310.** Trabaja con el estándar 802.11ac, consta de una antena adaptativa Ruckus BeamFlex, usualmente se implementa en entornos empresariales, soporta unmáximo de 100 clientes por Access Point. Existen opciones de manejo de red de manera virtual o en la nube (CommScope, 2022c).

- **Ruckus r500.** Trabaja con el estándar 802.11ac, por lo que opera en la banda 5 GHz haciendo uso de OFDM, utiliza una antena adaptativa patentada y puede brindar una ganancia de hasta 4dB extras. Integra la tecnología BeamFlex que es desarrolladapor la misma compañía (CommScope, 2022d).

- **Ruckus t300.** Es un punto de acceso para exteriores que trabaja en banda dual 802.11.ac, su diseño y funcionalidad permite que sea implementos para utilizar en lugares donde el tráfico de información es grande como en centros comerciales o lugares públicos. (CommScope, 2022e).

### 2.2.14. Media Converter

Son dispositivos que hacen la conversión de medio para poder pasar

conexiones de fibra óptica a conexiones que sean apropiadas para los routers de la universidad. El modelo que se utiliza actualmente es el 3C-LINK 3C-W-1000-35-40, cuenta con cuatro puertos 10/100 y no es administrable (Nyein, Naing y Saldanha, 2009).

### 2.2.15. Switch

La universidad cuenta con varios modelos de Switch de distintas marcas en el despliegue de su red, los cuales son: el Switch 3Com 4800G, Dlink 1210 48G, Dlink 3120 48G, HP 1950-48G, HP 1920-48G, HP 1920-24G, HP 1910-24GB, HP 3150 48G y Aruba 1960, la mayoría son Switches administrables de capa 2 y capa 3 (Lu, Lai y Chang, 2022).

### 2.2.16. Servidor

La universidad también cuenta con tres modelos de servidores Hewlett Packard, HP Proliant G8, HP Proliant G9 y HP Proliant G7 los cuales se encargan de guardar la información de la red de datos (Alazab et al., 2021).

### 2.2.17. PfSense

Es un software de código abierto para seguridad de red a través de firewall y router que también permite tener un manejo de red unificado y hacer balance de carga. Puede ser utilizado a varios niveles, ya que es aplicado a redes domésticas y de igual manera puede ser implementado en una red empresarial, está basado en FreeBSD (PfSense, 2022).

### 2.2.18. Optical Networks

Optical Networks es una empresa con base en Perú que se especializa en el sector corporativo y empresarial, brindando

servicios de telecomunicaciones. De igual manera, realiza despliegue de fibra óptica y la cual es implementada en su Red Metropolitana de Alta Velocidad la cual tiene su capa central cubriendo las áreas de Lima y Callao que le permite brindar un alto nivel servicio (Win Empresas, 2023).

### 2.2.19. Win Empresas

Win Empresas es el nuevo nombre con el que sigue ejecutando sus funciones la empresa antes denominada Optical Networks, se centran en asistir a compañías en la transición digital de sus servicios, brindando soluciones de conectividad, Cloud Hibrido, ciberseguridad, gestión, servicios de Data Center, comunicaciones unificadas y tecnología corporativa (Win Empresas, 2023).

### 2.2.20. Fortinet

Fortinet es una empresa especializada en el área de ciberseguridad, encargada de proveer servicios de seguridad en tecnología operacional y tecnología de la información, estos servicios son brindados de igual manera para la protección de redes de cajeros automáticos en bancos. Fortinet, de la misma manera, ofrece el firewall FortiGate NGFW diseñado para brindar seguridad empresarial para protección contra amenazas (Fortinet, 2022).

### 2.2.21. La Red Científica Peruana

La Red Científica Peruana (RCP) es una asociación iniciada en 1991 encargada de la administración de los dominios en Perú. Las personas u organizaciones que poseen un dominio, lo solicitan por un espacio determinado de tiempo y luego de que este plazo es terminado deben renovar nuevamente su posesión del mismode

manera constante (RCP, 2022).

### 2.2.22. Dominio

Existen diferentes tipos de dominios ya que no todos funcionan de la misma manera, algunos dominios están reservados para sitios web específicos, conocer cada tipo es de gran importancia en el momento de la creación de una página webya que algunos poseen algunos aspectos especiales que se deben tomar en cuenta. La buena elección de un dominio también ayuda a mejorar la experiencia de los usuarios en el sitio y ayuda a promover de una mejor manera las marcas o las compañías. Cada sitio web es guardado en un servidor y es asignado una dirección IP (Internet Protocol), y cada una cuenta con un DNS (Domain Name System) que permite que cada dominio sea más fácil de buscar en el motor de búsqueda. (Mockapetris y Dunlap, 1988).

### 2.2.23. Tipos de dominios

- **Dominio de primer nivel (TLD).** Este representa el nivel de dominio más alto en la jerarquía del sistema de nombres de dominio (DNS), un dominio de primer nivel siempre aparece en la parte final de una dirección de página web, este tipo de dominio es administrado por la IANA (Internet Assigned Numbers Authority), la cual es una subdivisión de laICAAN, la cual se encarga de mantener un registro de las direcciones IP y de los identificadores que se utilizan según los estándares (Cazares, 2013)

- **Dominio de nivel superior de código de país (ccTLDs).** Este es un tipo de dominio especial cuyas extensiones son administradas por el país respectivo al que pertenecen y cubren esa área geográfica. (Yu, 2004)

- **Dominios genéricos de primer nivel (gTLDs).** Cubren un área temática y se dividen en dos tipos:

  a) **gTLDs no patrocinados:** Están sujetos a la ICAAN a un manejo centralizado y controlado.

  b) **gTLDs patrocinados:** Están sujetos a las restricciones y parámetros determinados por el patrocinador,de la misma manera la compañía u organismo está también bajo el del manejo deldominio. (Korczynski et al., 2018).

- **Dominio de segundo nivel (SLD).** Es el nombre que electivo que el cliente puede dar al dominio, es de libre elección y está por debajo del dominio del primer nivel en la jerarquía del sistema de nombres de dominio (ICANN, 2022a).

- **Dominio de tercer nivel.** Este tipo de dominio es opcional y se coloca en el lado izquierdo del dominio de segundo nivel por lo cual también es llamado un "subdominio", su objetivo eshacer referencia a secciones específicas de las páginas web (Cázarez, 2013).

### 2.2.24. DNS (Domain Name System)

El DNS es como un directorio telefónico para todas las páginas web de internet que está constituido por una red de servidores alrededor de todo el mundo. Los buscadores interactúan a través de

direcciones IP, el DNS se encarga de interpretar los nombres de dominio a direcciones IP para permitir que el buscador pueda cargar los recursos y la información en línea (Bishop, 2004).

### 2.2.25. ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN es la organización encargada del manejo y administración de los registros de DNS, es una organización sin fines de lucro, además lleva a cabo la tarea de ubicación de direcciones IP y manejo del sistema de servidores raíz, asegurando que todos los dominios tengan una dirección IP única y que los usuarios deinternet puedan hallar cada dominio a través de su nombre de dominio asignado que concuerde con su dirección IP válida. (ICANN, 2022b).

### 2.2.26. Web hosting

Web hosting es el proceso de compra de un espacio para albergar un sitio web en internet, ya que el contenido de la página, el código HTML, CSS y las imágenes deben ser guardadas en un servidor para que pueda ser visto en línea. En este sentido, todo este contenido debe ser subido desde una computadora local a un servidor web, los recursos del servidor como la memoria RAM, espacio de disco duro y ancho de banda son asignados al sitio web. Un servidor es una computadora que permite que los usuarios de internet de cualquier parte del mundo puedan conectarse a una página web. Una vez comprado el nombre de dominio, los archivos que contienen todo el contenido de la página web deben ser guardados en un servidor web el cual se encarga de hacer la conexión de estos archivos con el internet para poder ser vistos por los usuarios (Prodan y Ostermann, 2009).

### 2.2.27. Tipos de Web Hosting.

En la actualidad existen varios tipos diferentes de web hosting los cuales se han desarrollado para cubrir las necesidades de los diferentes tipos de sitios web

- **Web Hosting compartido.** Este tipo de web hosting es una buena opción para negocios pequeños o medianos que no esperan tener demasiado tráfico en su página web inicialmente. Hosting compartido ocurre cuando una página web es guardada en el mismo servidor que otras páginas web. (Canali, Balzarotti y Francillon, 2013).

- **VPS Hosting ("Virtual Private Server" o "Virtual Dedicated Service").** Este tipo de web hosting es como un punto medio entre hosting compartido y hosting dedicado ya que los clientes pueden ver un servidor virtual que parece ser dedicado solo a su página web cuando en realidad está brindando el servicio a otras páginas web de igual manera. (Telenyk et al., 2013).

- **Hosting dedicado.** Ocurre cuando una página web es alojada en un servidor dedicado, donde se proveen todos los servicios completos del servidor web, este tipo de hosting se utiliza principalmente en páginas web que manejan un gran número de usuarios y una gran cantidad de tráfico e información para que el servicio pueda ser óptimo. (Prodan y Ostermann, 2009).

- **Cloud hosting.** Cloud hosting permite el acceso a la información de una página web haciendo uso de la nube, este tipo de alojamiento provee una cantidad infinita de espacio para una cantidad ilimitada de dominios, esta opción también es de gran beneficio para compañías grandes ya que también permite tener un buen control y manejo de tráfico en la página web. (Molnar y Schechter, 2010).

### 2.2.28. Vulnerabilidad de una red

La seguridad de una red se logra a través del resguardo de la infraestructura subyacente de la red para evitar acceso no autorizado que pueda llevar a robo de información. La seguridad de una red debe estar aplicada en varias capas en el perímetro de la red y también de manera interna para que pueda ser lo más efectiva posible, como la protección de la red es aplicada en capas un usuario no autorizado no logra obtener accesos mientras que los usuarios pertenecientes a lared tienen las credenciales para acceder a los recursos de la red, sin embargo, la seguridad de red también busca evitar actividades no autorizadas dentro de la red incluso para los usuarios internos (Cisco, 2022a).

### 2.2.29. Tipos de seguridad de una red

- **Firewall.** Un firewall es un sistema de seguridad de redes que funciona restringiendo de manera selectiva y controlando el tráfico que entra y sale de una red privada. Su propósito es prevenir cualquier tipo de actividad no autorizada en la red ya sea proveniente de dentro o fuera de la misma. Un firewall hace selección de los paquetes de información con la finalidad de bloquear el ingreso de cualquier software malicioso e impedir el acceso de un atacante a la información de la red (Cisco, 2022a).

- **Sistema de prevención de intrusión (IPS).** Es un sistema que monitorea y hace un escáner del tráfico de la red de manera activa para bloquear cualquier ataque que pueda ser detectado, bloquean actividad maliciosa y de igual manera rastrean archivos de malware para evitar su propagación por la red (Cisco, 2022a).

- **Seguridad de la carga de trabajo.** Protege las aplicaciones y servicios cuya carga de trabajo en funcionamiento haceuso de los recursos de la nube u otros sistemas híbridos. Este tipo de cargas de trabajo tiene un área de ataque más amplio (Cisco, 2022a).

- **Seguridad netWORK.** Es un proyecto desarrollado por Cisco que tiene como objetivo unificar los controles de seguridad para las redes, cargas de trabajo y servicios basados en la nube, con el objetivo de simplificarlos (Cisco, 2022a).

- **SecureX.** Es una arquitectura desarrollada por Cisco basada en la nube que permite conectar los servicios de Cisco con la infraestructura de un cliente (Cisco, 2022a).

- **Segmentación de red.** Es una técnica de seguridad de la red donde una red principal es dividida en subredes más pequeñas con el objetivo de dar distintos controles de seguridad a cada subred (Cisco, 2022a).

- **VPN.** Una red privada virtual (VPN) es una herramienta de seguridad que permiteencriptar la información que entra y sale de red, permite ocultar la dirección IP y evita que la información pueda ser interceptada por un atacante (Cisco, 2022a).
- **Portal Cautivo.** Es una solución de Seguridad que monitorea el tráfico de la red forzando a los usuarios a ingresar a través la página web donde se presentan los procedimientos que deben seguir para poder conectarse a la red y tener acceso a internet (Ali et al., 2019).
- **Control de acceso.** Es una técnica de seguridad de red que establece que es necesario tener conocimiento completo de los usuarios pertenecientes a la red implementada, dela misma manera también se deben conocer todos los dispositivos incluidos en la red para poder aplicar políticas de privacidad correctamente (Cisco, 2022a).

- **Software Antivirus y Antimalware.** Los softwares maliciosos incluyen virus, worms, troyano, software de secuestro dedatos y spyware. Los programas utilizados para prevenir la entrada de estos archivos maliciosos al sistema deben realizar un monitoreo continuo de modo que se pueda detectar cualquier archivo sospechoso que haya logrado irrumpir para proceder a eliminarlo y reparar el daño que se haya podido ocasionar (Cisco, 2022a).

- **Seguridad de Aplicación.** Son las herramientas de hardware y software que se utilizan para proteger las aplicaciones principales con las cuales ópera alguna organización para cerrar brechas potenciales a la seguridad (Cisco, 2022a).

- **Análisis de comportamiento.** Son programas utilizados para detectar cualquier comportamiento anormal dentro del sistema. Al detectar estás amenazas a través de distintos indicadores que sugieren algún comportamiento sospechoso el programa soluciona rápidamente las amenazas (Cisco, 2022a).

- **Seguridad en la nube.** Es un grupo de tecnologías basadas en la nube que tienen como propósito el proteger las direcciones IP, aplicaciones y cualquier otra información sensible. Permite brindar una mejor seguridad a los datos e información que se guardan en la nube o aplicación importantes para el funcionamiento del sistema de una organización que opere basado en la nube (Cisco, 2022a).

- **Prevención de pérdida de información.** Las tecnologías de prevención de pérdida de información impiden que los usuarios de una red compartan, suban o descarguen información de manera no autorizada, incluso puede evitar la impresión de información sensible ya que una compañía debe asegurarse de que sus empleados no compartan información fuera del conocimiento de la compañía (Cisco, 2022a).

- **Seguridad de correo electrónico.** Entrada de correos electrónicos maliciosos son una de las preocupaciones principales a la hora de garantizar un buen sistema de seguridad. Las aplicaciones de seguridad de correo electrónico evitan la recepción de cadenas de correo electrónico sospechoso para prevenir la perdida de información (Cisco, 2022a).

- **Seguridad de red industrial.** Son un conjunto de técnicas y herramientas que permiten brindar seguridad en un ámbito industrial, a través del uso de sistemas de seguridad de OT para segmentar la red además de implementar herramientas de seguridad de IT para proteger los dispositivos OT (Cisco, 2022a).

- **Seguridad de dispositivo móvil.** Se refiere a todas las herramientas de seguridad aplicadas a dispositivos móviles, se aplican técnicas de ciberseguridad además de realizar la configuración de las conexiones para mantener la privacidad del tráfico de información de la red (Cisco, 2022a).

- **Manejo de evento y seguridad de la información.** Los softwares de manejo de evento y seguridad de la información consiguen la información necesaria para el personal de manera que puedan detectar amenazasy tengan la oportunidad de actuar rápidamente (Cisco, 2022a).

- **Seguridad Web.** Una solución de seguridad web permite controlar el uso que el personal de una organización hace de los servicios en línea, permite bloquear amenazas basadas en internet, y negar el acceso a sitios web maliciosos que representen una amenaza para la seguridad de los datos de la organización (Cisco, 2022a).

- **Seguridad inalámbrica.** Las redes inalámbricas no son tan seguras como las redes alámbricas. En este sentido, es de gran importancia adquirir productos diseñados específicamentepara la protección de redes inalámbricas para la seguridad de Wireless LANs (Cisco, 2022a)

### 2.2.30. Virtual Machine

Una máquina virtual o VM (Virtual Machine) es un recurso de computadora que utiliza software en lugar de una computadora física para ejecutar programas, sistemas operativos y herramientas. Las máquinas virtuales son ejecutadas en una computadora física y utiliza su propio sistema operativo, de modo que trabaja de forma separada de la computadora principal y de otras máquinas virtuales (Oracle, 2022).

Actualmente existen muchos programas de software para ejecutar máquinas virtuales, algunos de los más utilizados son los siguientes:

- **VirtualBox.** Es un software de código abierto que está disponible para utilizar en multiples plataformas y cuyo uso principal es como software de tecnología de simulación para la visualización y manejo de máquinas virtuales. Actualmente, VirtualBox pertenece a Oracle luego de haber sido comprado a la compañía Sun Microsystems, por lo que ahora lleva el nombre de Oracle VM VirtualBox (Oracle, 2023).

- **Citrix XenServer.** Es una plataforma de virtualización de servidores, XenServer hace uso del hipervisor Xen para la visualización, una vez instalado, permite instalar máquinas virtuales que pueden abrirse al mismo tiempo con un alto rendimiento (IBM, 2023).

- **QEMU.** Es un software de emulación y virtualización que hace uso de un traductor binario dinámico y permite la instalación de máquinas virtuales para su visualización y construcción de entornos virtuales diferentes ya que tiene la capacidad de ejecutar programas y aplicaciones sin modificar el sistema local, no cuenta con interfaz gráfica y se deben hacer las configuraciones desde una terminal, pero si permite instalar QEMU manager que permite ser usado como una en Windows (Gonzalez, 2022).
- **VMWare Workstation.** Es un programa de virtualización utilizado en tecnología de la información para instalar, construir y probar máquinas virtuales y dispositivos de red desde una laptop o PC permitiendo acceso a la nube y a aplicaciones de Windows (Choi, 2021).

### 2.2.31. Packet Tracer

Es una herramienta de simulación desarrollada por Cisco, permite la construcción de redes simples y complejas en un ambiente de simulación para evaluar distintos aspectos de la misma y tener una idea de cómo se llevaría a cabo su implementación. El uso de esta herramienta es de mucho beneficio sobretodo enla simulación de redes complejas o grandes ya que si se deseara implementarlas de manera física para evaluar el funcionamiento el costo podría ser un impedimento. (Cisco, 2022b).

### 2.2.32. Dashboard

Un Dashboard es una interfaz de usuario o página web en la que se brindan información de manera resumida, normalmente haciendo uso de gráficos y tablas de forma que la información pueda ser exhibida de manera sencilla y fácil de comprender. (Sarikaya et al., 2019)

## 2.3. MARCO METODOLÓGICO

### 2.3.1. Tipo de investigación

El tipo de investigación del presente proyecto de tesis está enfocado a la aplicación tecnológica. Debido a que se emplean diferentes herramientas para determinar un modelo seguro y optimizado de la red inalámbrica de la Universidadde Ciencias y Humanidades. En la cual, se tiene la finalidad de garantizar un alto nivel de seguridad en la red permitiendo que esta pueda brindar un servicio óptimo al personal administrativo y docente, y a cada estudiante. De este modo, se pretende reforzar la importancia de una buena seguridad en la red, sobretodo en una universidad, ya que el sistema cuenta con gran cantidad de información personal que debe ser resguardada de la mejor manera.

### 2.3.2. Metodología de la investigación

#### A. Contexto o escenario de la investigación

El sistema propuesto, se implementará en la Universidad de Ciencias y Humanidades ubicada en el distrito de Los Olivos. En la cual existen 5 facultades yen la cual se enseñan quince carreras para un total de 3507 estudiantes en toda launiversidad. Se escoge la Universidad de Ciencias y Humanidades debido al gran crecimiento que ha tenido la universidad en los últimos años, además de que se han agregado nuevas carreras a las facultades y el número de estudiantes y profesores también va en aumento por lo que es de vital importanciauna red inalámbrica eficiente que tenga un sistema de seguridad confiable para la protección de los datos, además de que el sistema propuesto debe ser de Software de código abierto para bajar los costos y permitir el uso de una mayor gama de equipos de distintas marcas.

## B. Muestra y participante

La mayoría de los estudios de investigación necesitan seleccionar una muestra, lo cual es crucial para delimitar el estudio. Esta muestra se escoge de una población más grande de objetos, personas, procesos, entre otros (Baltes y Ralph, 2022). En este sentido, para la presente tesis la información sobre la red de datos de la Universidad de Ciencias y Humanidades se obtendrá en el área de soporte técnico ya que allí es donde se tiene el conocimiento a más detalle del funcionamiento de la red actual de la universidad y de las áreas en la red que deben mejorarse para garantizar la protección de los datos. De igual manera, los objetos de estudio son el protocolo actual Ruckus Wireless y el protocolo al que se planifica la transición pfSense.

## C. Diseño o abordaje

El diseño propuesto está basado el software de PfSense, se utilizará una plataforma de máquina virtual inicialmente para la visualización de un Dashboard donde se muestren los equipos de la red de la universidad y donde se pueda implementar el software de seguridad con un firewall que permita el resguardo de la información, se deben visualizar cada uno de los equipos de manera que sea de fácil manejo. El sistema propuesto es un sistema que debe ser centralizado de manera que permita controlar cada una de las áreas de la red, las cuales estarán conectadas a un punto central desde el cual se realizará la administración de la misma, lo que también permite efectuar cambios fácilmente en caso de que sea necesario. De igual manera el Software de PfSense puede ser implementadocomo un servidor DHCP, un punto de acceso de Wi-fi, un servidor de DNS y un servidor VPN, permitiendo fortalecer la seguridad de la red.

### D. Procedimiento

Inicialmente se debe estudiar la red actual de la Universidad de Ciencias y Humanidades para tener claridad sobre el diseño de la red actual además de los equipos que se han utilizado para la implementación de la misma, una vez recopilada esa información, se debe proceder al diseño de la nueva red, seutilizará VirtualBox como una plataforma de software de visualización para la creación de las máquinas virtuales para la simulación de la red. Se comenzará instalando pfSense en VirtualBox y creando una red interna de modo que se puedan agregar más máquinas virtuales a esa red, se debe configurar DHCP en PfSense para que este pueda asignar las direcciones IP a las demás máquinas virtuales pertenecientes a la red de manera automática, luego debe verificarse quecada una de las máquinas virtuales haya sido asignada una dirección IP y que se ha logrado la conexión a la red de manera efectiva. Desde cada una de las máquinas virtuales asociadas a la red interna se puede ingresar a la plataforma de PfSense a través del buscador, se debe ingresar un nombre de usuario y contraseña que permite el acceso al Dashboard donde se visualizará toda la red y los equipos que la conforman. De este modo se podrá comprobar el correcto funcionamiento de la red diseñada y de los protocolos de seguridad antes de realizar la implementación de la misma de manera física en la Universidad de Ciencias y Humanidades.

## 2.4. MARCO LEGAL

El Decreto Legislativo que Aprueba la Ley de Gobierno Digital señala la importancia de la claridad respecto a las definiciones básicas en servicios digitales, los cuales son importantes para una adecuada gobernanza en

este ámbito. Además de cubrir los temas de identidad digital, interoperabilidad y arquitectura digital, también abarca el aspecto de seguridad digital y de datos, el cual es de suma importancia en las organizaciones y empresas que trabajan en el sector tecnológico.

Por otro lado, en el Artículo 1 de la Ley N° 29733, Ley de Protección de Datos Personales, explica que el objetivo principal de esta ley es el de hacer cumplir el derecho fundamental expuesto en el artículo 2 numeral 6 de la Construcción Política del Perú, donde abarca la importancia de la protección de datos y la responsabilidad que tienen las entidades de servicios informáticos de evitar suministrar información que pueda representar una brecha a la privacidad del ciudadano tomando en mayor consideración los datos sensibles. En esta ley

también se exponen en el Título I los principios rectores correspondientes como lo son:

- El principio de legalidad donde indica que todo el manejo de datos debe ser realizado en conformidad con las leyes establecidas.
- Principio de consentimiento, que establece que el titular de los datos debe dar su permiso para el uso y el procesamiento de los mismos.
- Principio de finalidad, que indica que los datos recopilados deben tener una finalidad para la cual se solicitan, y que los mismos deben ser utilizados para esa sola finalidad informada al titular de los datos.
- Principio de proporcionalidad, ya que la información y datos solicitados deben tener la proporción necesaria para el fin al cual se han de aplicar.
- Principio de seguridad, indica que las entidades públicas y privadas que hagan uso de datos personales están bajo la responsabilidad de brindar todos los medios necesarios para garantizar la seguridad y el buen tratamiento de los mismos.

- Principio de disposición de recurso, que establece que el titular de los datos tiene derecho a realizar reclamos en caso de considerar que su privacidad ha sido vulnerada.
- Principio de nivel de protección adecuado, donde indica que de ser necesario el envío de datos al exterior del país, las entidades deben apegarse a lo establecido por esta ley y por las leyes regulatorias internacionales.
- Valor de los principios, establece que todas las partes involucradas en el tratamiento de los datos personales deben ajustarse a lo establecido en esta ley.

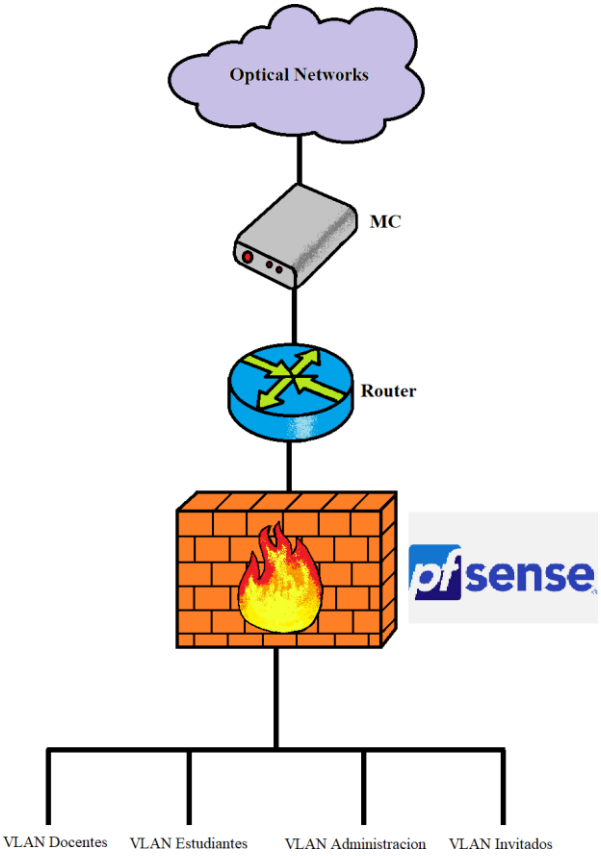
Del mismo modo, también se expone cómo la recopilación de datos debe tener una finalidad específica y que debe ser proporcional los datos solicitados con su finalidad, además de mencionar en el Artículo 9 que el titular de la base de datos ysu encargado deben brindar las condiciones necesarias y suficientes para que se garantice la completa seguridad de la información de los usuarios. De la misma manera, la Ley N°30096, Ley de Delitos Información, tiene como su objetivoprincipal la sanción del uso ilícito de los datos personales y la lucha contra la ciberdelincuencia. En el Proyecto de Ley 6544 se promueve la creación de un Centro Nacional de Ciberseguridad en el Perú (CENACI), cuyo objetivo principal será el de velar por el cumplimiento de las normas de ciberseguridad para luchar contra amenazas.

## 2.5. DIAGRAMA DE BLOQUES O ARQUITECTURA DEL SISTEMA

A continuación, se muestra la arquitectura del sistema, la cual se divide en distintos bloques. En el cual el firewall de PfSense es el componente principal y esel que brindará la seguridad a la red interna la cual se divide en cuatros redes locales virtuales para docentes, estudiantes, administración e invitados.

**Figura 1**

*Arquitectura propuesta de Red*




*Nota.* En la Figura 1 se visualiza la estructura propuesta de la red, donde se obtiene el servicio de internet a través de fibra ópticade Win Empresas, por lo que se requiere el uso de un MC (Media Converter) para hacer la conversión de cables y conectar seguidamente un router, el firewall de PfSense será programado para filtrar los distintos paquetes y adicionalmente se colocará un límite de ancho banda a los equipos para evitar sobrecargas. La red se dividirá en cuatro redes virtuales locales que serán paradocentes, estudiantes, administración e invitados. Se debe colocar un horario y ciertos límites a cada una de las VLANs y realizar la configuración necesaria dependiendo de la necesidad de losusuarios de cada red.

# CAPÍTULO III: DESARROLLO DE LA APLICACIÓN

## 3.1. DESARROLLO DEL OBJETIVO ESPECÍFICO 1

### 3.1.1. Datos de la organización

La Universidad de Ciencias y Humanidades es una institución de enseñanza superior que inició sus actividades el 16 de diciembre de 2006, ubicada en Av. Universitaria Norte Nº 5175, Los Olivos, Lima, 15304. Autorizada por el Consejo Nacional para la Autorización de funcionamiento de Universidades (CONAFU), logró obtener el licenciamiento por la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU) el 21 de noviembre de 2017 (SUNEDU, 2017). Actualmente, próxima a cumplir 17 años de vida institucional, alberga una población de 3507 estudiantes, y ofrece quince carreras diferentes. (Alcántara, 2017)

Desde su fundación, la Universidad de Ciencias y Humanidades procuró que la topología de red de datos pudiese ser escalable y permitiera realizar mejoras con el paso del tiempo. Inicialmente, hasta el año 2015 la Universidad de Ciencias y Humanidades hacía uso de una red de datos básica, donde los equipos implementados no estaban diseñados para un flujo grande de información o para un numero grande de usuarios ya que estos eran más de uso doméstico donde las formaciones de dispositivos estaban aisladas de un área a otra, al no contar con un sistema de control centralizado, las gestiones de configuración y permisos se realizaban en cada dispositivo individualmente, donde cada uno aplicaba sus propias políticas de seguridad. Sin embargo, ya había proyecciones de mejora, por lo que se siguieron haciendo cambios a la red de datos. La SUNEDU, al ser el organismo que se encarga de la supervisión del cumplimiento de las normas en establecimientos de educación superior, tiene como uno de los requerimientos para alcanzar el

licenciamiento el contar con acceso a internet en cada espacio, esto implica el ampliar el servicio de internet en conjunto. Durante este tiempo se consideraron varias marcas y productos potenciales para el despliegue de la red, entre los cuales estuvieron D-link en su gama Enterprise, Aruba Networking, Cisco y Ruckus Wireless como posibles opciones, se probaron productos de cada compañía para determinar su viabilidad evaluando sus características, costos y beneficios. Para el año 2017 la universidad ya contaba con dispositivos capaces de soportar una mayor cantidad de usuarios conectados y otro tipo de software para garantizar la seguridad de la red de datos, en este año, a partir del mes de mayo, también se implementó por primera vez Ruckus Wireless, por ser considerado como el que se ajustaba más a las necesidades de la universidad, a un precio asequible, y que permite la escalabilidad de la red. El uso de Ruckus implica realizar la compra de una licencia, la cual se paga una única vez, de allí en adelante, cada año se deben hacer los pagos necesarios para la compra de las actualizaciones en el software de Ruckus donde se garantice cubrir cualquier punto débil en seguridad del sistema, de no realizarse dicho pago anual aún se podrían hacer uso de los productos y del software pero no se contarían con las actualizaciones necesarias y la red quedaría vulnerable a ataques en puntos débiles. Desde el año 2017 hasta la actualidad no ha habido muchos cambios en términos de la topología de la red, sin embargo, se han realizado mejoras para aumentar la velocidad de transmisión de datos en el servicio de internet.

## 3.2. DESARROLLO DEL OBJETIVO ESPECIFICO 2

La Universidad de Ciencias y Humanidades ha ido haciendo cambios a su topología con el paso del tiempo de manera que la red pueda cubrir las necesidades de acuerdo al tráfico de datos del cuerpo

estudiantil, personal docente y administrativo en los tres edificios que conforman el campus. Inicialmente, desde la fundación de la universidad en el año 2006 hasta el 2015 los equipos eran de un uso doméstico; con el crecimiento de la universidad y con el propósito de recibir el licenciamiento hizo cambios a un nuevo modelo de red basado en los Access Point de Ruckus Wireless. Del mismo modo, también se hace uso de otros equipos como diferentes switches, servidores y Media Converters. Actualmente la universidad cuenta con 50 equipos de comunicación, de los cuales el 99% son switches administrables de capa 2 y capa 3. Los switches que se utilizan son:

- **3Com 4800G.** Tiene una potencia de 110 W y cuenta con conexiones de 24 puertos frontales de tres velocidades (10/100/1000 Mbps), de los cuales, cuatro son puertos combo de 100/1000 Mbps compartidos con SFP permitiéndole ser conectado con red de fibra óptica o de cobre lo que mejora la funcionalidad de conmutado a través de la red. De igual manera, tiene dos puertos en la parte de atrás para expansiones de 10 Gigabits (Tonitrus, 2023).
- **Dlink 1210 48G.** Un switch administrable de capa 2 que cuenta con 48 puertos de 10/100/1000 Mbps, 4 puertos combo de 100/1000 Mbps con SFP de velocidad dual y capacidad de conmutado de 104 Gbps (Dlink, 2023a).
- **Dlink 3120 48G.** Es un switch administrable de capa 2 y capa 3 con 48 puertos de los cuales 44 son de 10/100/1000 UTP y 4 son puertos combo de UTP/SFP, tiene fuente de alimentación redundante opcional y capacidad de conmutado de 136 Gbps (Dlink, 2023b).

De igual manera, se hace uso de cuatro modelos de switch HP, los cuales son:

- **HP 1910-24GB.** Es un switch administrable con 24 puertos de los cuales 20 son RJ-45 y son puertos de expansión 10/100/1000 Mbps que trabaja con una potencia de 12 W (Amazon, 2023a).
- **HP 1920-24G.** Es un switch administrable de capa 3 de 24 puertos RJ-45 10/100/1000 de los cuales 4 son puertos SFP de 1000 Mbps, potencia de 11,6 W y capacidad de conmutación de 56 Gbps (Amazon, 2023b).
- **HP 1920-48G.** Es un switch administrable de capa 2 y capa 3 de 48 puertos RJ-45 Ethernet, consumo de energía máximo de 481 W y que cuenta con una interface gráfica de usuario web que permite realizar las configuraciones y una terminal para ingresar comandos y capacidad de conmutación de 104 Gbps (Amazon, 2023c).
- **HP 1950-48G.** Es un switch con un total de 48 puertos RJ-45 de 10/100/1000, de los cuales dos son de SFP, tiene capacidad de conmutado de 176 Gbps con centro de administración inteligente y navegador web además de una interface de línea de comandos (HP, 2023).

Un switch administrable marca Aruba:

- **Aruba 1960.** Es un switch de capa 2 con gestión inteligente a través de aplicación móvil o plataforma web basada en la nube, con 48 puertos de los cuales 4 son SFP (Hewlett Packard Entreprise, 2023a).

  Del mismo modo, la universidad también cuenta con tres modelos de servidores HP

- **HP Proliant G7.** Servidor HP Gen7, procesador Intel Xeon, memoria RAM de 32GB y disco duro de 300 GB (Hewlett Packard Entreprise, 2023b).

- **HP proliant G8.** Es un servidor HP Gen8 de la serie ProLiant que cuenta con un procesador de 2.7 GHz, memoria RAM de 128 GB, disco duro de 300GB y chip Intel (Hewlett Packard Entreprise, 2023c).
- **HP Proliant G9**. Servidor HP Gen9 con procesador Intel Xeon, memoria RAM de 16GB y disco duro de 600GB (Hewlett Packard Entreprise, 2023d).

La universidad también utiliza un modelo de Media Converter:

- **3C-LiNK.** Es un dispositivo para hacer la conversión de conexión de fibra óptica a la conexión de router, el Media Converter es modelo 3C-W-1000-35-40 desarrollado por 3C-Link, tiene 4 puertos 10/100, permite escoger distintos módulos ópticos como fibra dual multi modo, fibra dual modo único y fibra única modo único, puede ser aplicado en redes para seguridad, monitoreo y cobertura inalámbrica, no es administrable (3C-LINK, 2023).

En el año 2020 se subieron todos los servicios a La Nube, con la compra de un espacio en La Nube de igual manera se provee el servicio de seguridad. Sin embargo, para el año 2021 el sistema llegó a detectar hasta 200 ataques por día, e incluso la página interna de la universidad se vio bloqueada en su momento, por ese motivo se decidió cerrar internacionalmente las entradas a la red y solo permitir el acceso a ciertos puertos de la red interna de manera que desde afuera de la red las entradas son limitadas para resguardar la seguridad, mientras que desde la red interna se dejó el acceso abierto a todas las fuentes de información necesarias a nivel internacional, este cambio permitió disminuir en gran cantidad el número de ataques a la red. El software de Ruckus no cuenta con un sistema de prevención de intrusiones (IPS) o sistema de detección

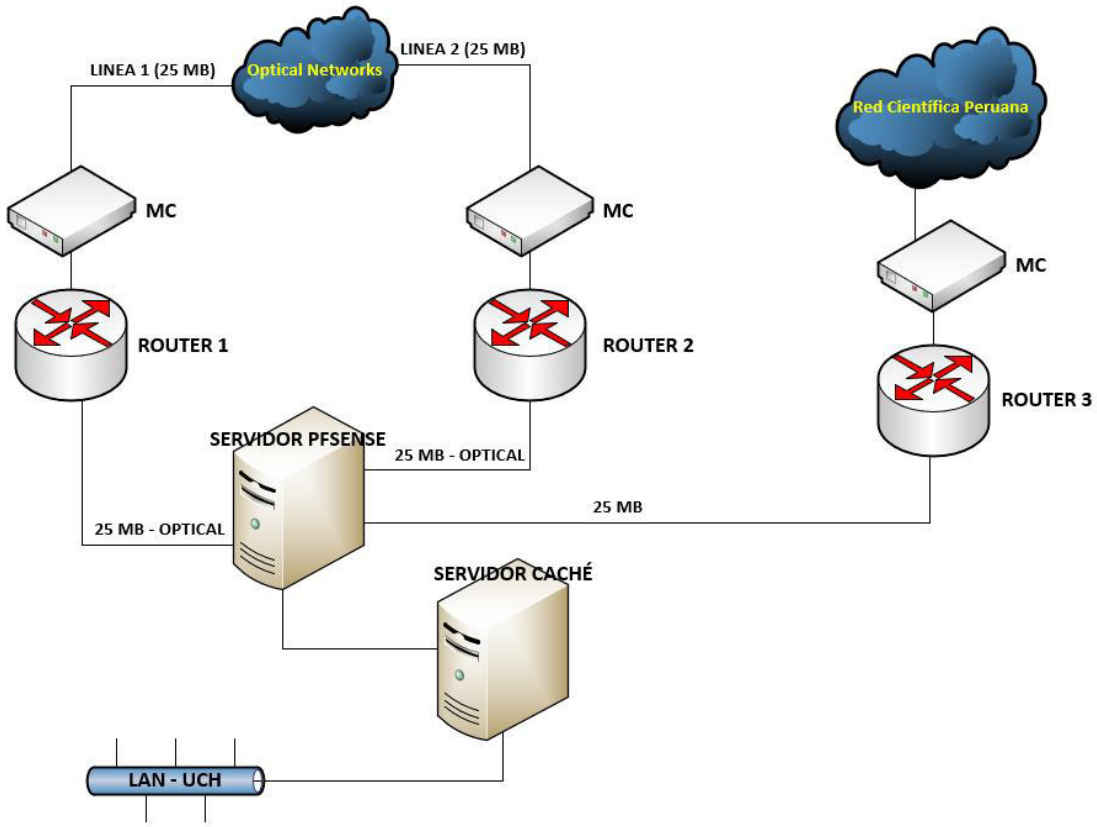
de intrusiones (IDS), por lo que el firewall de Fortinet, es el encargado de realizar el análisis del número de ataques al sistema en un periodo de tiempo especificado.

En cuanto al sistema eléctrico, la Universidad de Ciencias y Humanidades cuenta con una subestación que utiliza el servicio de la empresa “Luz del Sur” la cual se encarga de brindar media tensión para que la subestación brinde baja tensión de 220 V a las instalaciones de la universidad.

A continuación, se muestra en las siguientes figuras la evolución hasta la actualidad de la topología de la red de datos de la Universidad de Ciencias y Humanidades a nivel WAN y la red LAN actual.

**Figura 2**

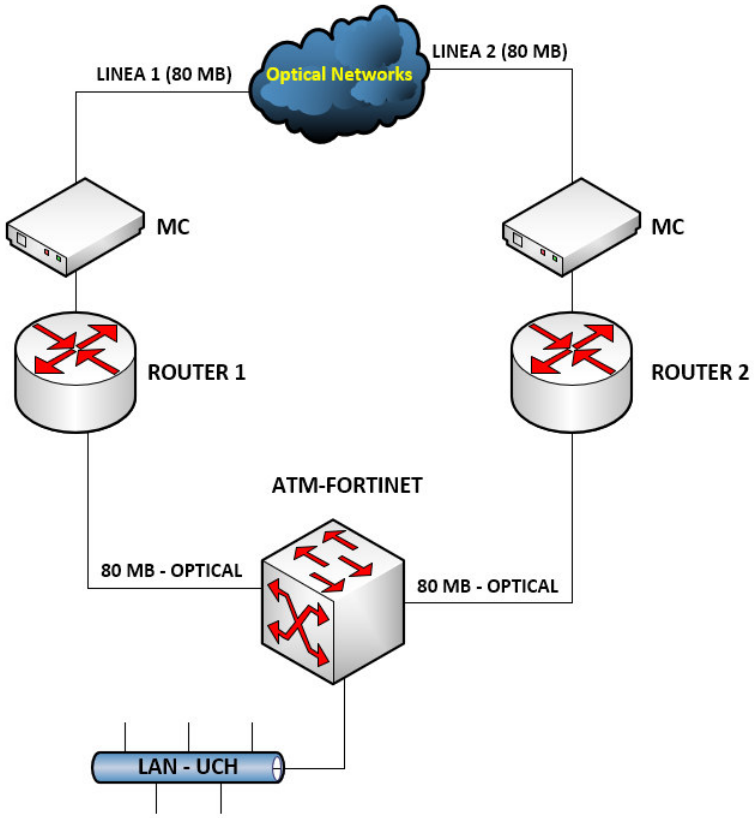
*Topología de la red WAN de la Universidad de Ciencias y Humanidades en 2015*




*Nota.* La Figura 2 muestra la red WAN de la Universidad de Ciencias y Humanidades en el año 2015, se puede ver en la parte superior los proveedores de servicio de internet, inicialmente se tenían dos, Optical Networks (actualmente Win Empresas) y la Red Científica Peruana. Luego se muestran tres MC (Media Converter) para llevar las conexiones a los tres routers que llegan a un servidor principal, que, en ese tiempo, hacía uso de pfSense para su gestión, en equipos de línea domestica que en lo posterior tuvieron que reemplazarse por unos que se ajustaran más a las necesidades de un campus universitario. Desde este servidor principal se llega a un servidor caché como protección adicional para la red LAN-UCH que se encuentra en la parte inferior de la figura.

**Figura 3**

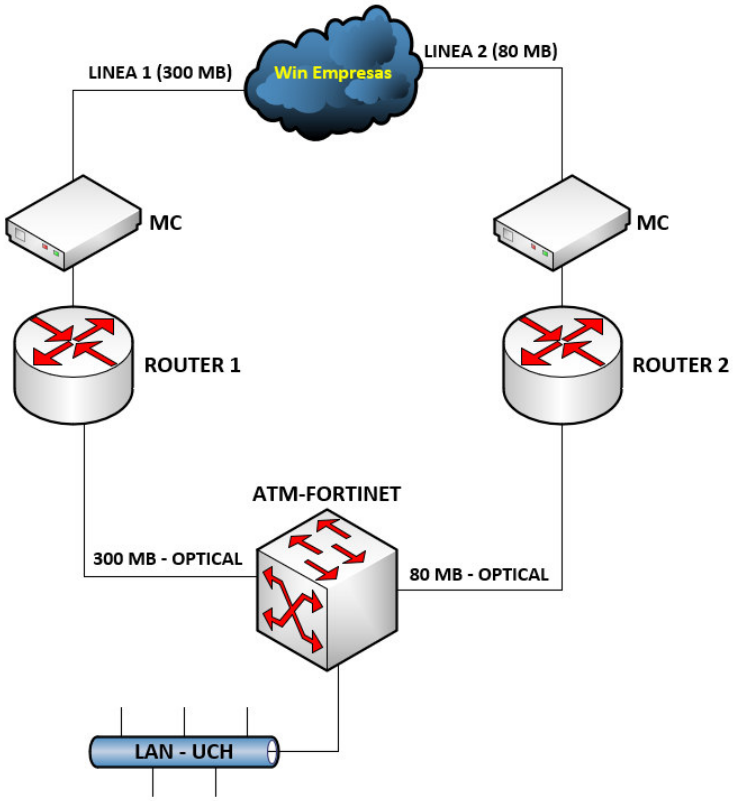
*Topología de la red WAN de la Universidad de Ciencias y Humanidades en 2017*




*Nota.* En la Figura 3 se muestran los cambios realizados a la red WAN desde la anterior en 2015 hasta 2017, donde aún se reciben los servicios de internet a través de fibra óptica de Optical Networks (actualmente Win Empresas) con una velocidad mejorada ahora de 80MB en ambas líneas, pero ya no se utiliza el servicio de la Red Científica Peruana, eliminando también un MC (Media Converter) y el Router 3, ahora solo contando con dos MC y sus respectivos routers cuya conexión llega hasta el router ethernet protegido por ATM-Fortinet, cuya única conexión es hacia la red LAN-UCH debido a que para el 2017 ya se había quitado el servidor caché.

**Figura 4**

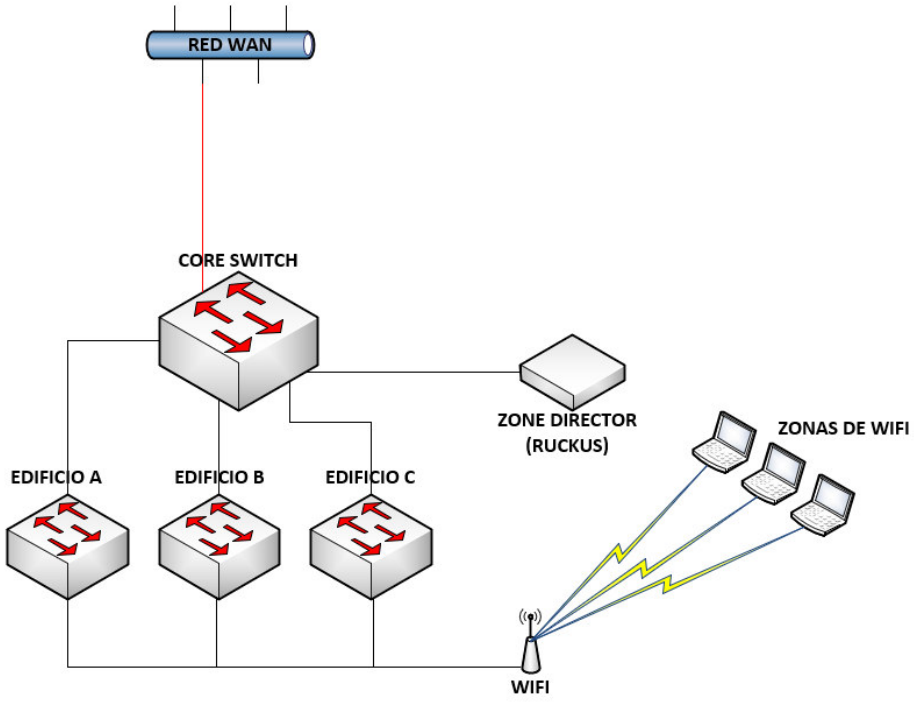
*Topología de la red WAN de la Universidad de Ciencias y Humanidades en 2023*




*Nota.* En la Figura 4 se muestra la red WAN actual para el año 2023, Optical Networks como proveedor de servicios de internet a través de fibra óptica cambió su nombre comercial a Win Empresas, 300MB en la línea 1 como línea principal y 80MB en la línea 2 que actúa como línea de contingencia, pero a grandes rasgos aún se mantiene la topología planteada de 2017.

**Figura 5**

*Topología de la red LAN de la Universidad de Ciencias y Humanidades en 2023*




*Nota.* En la Figura 5 se muestra la red LAN de la Universidad de Ciencia y Humanidades que se utiliza en la actualidad en el año 2023, en la parte superior de la figura se visualiza la red WAN, de la cual sale una conexión a un switch central denominado “Core Switch” desde el cual se realizan las conexiones hasta los switches principales en cada uno de los tres edificios del campus universitario, y desde estos se lleva el servicio hasta los demás switches distribuidos en cada edificio, la universidad cuenta con 50 switches en total desde los cuales se conectan los puntos de acceso que permiten el servicio de internet Wi-Fi que se visualiza en la parte inferior de la figura, este Wi-Fi permite acceso a internet a las distintas áreas de la Universidad. Se debe resaltar que al *Core Switch* también está conectado el “Zone Director” de Ruckus Wireless que funciona como sistema de control para los Access Point de la compañía.

El campus de la Universidad de Ciencias y Humanidades está compuesto por tres edificios, el edificio A, edificio B y edificio C:

- **Edificio A.** El edificio A es un edificio de 6 pisos, en el piso 1 se encuentra un switch de distribución que está conectado por enlace de fibra óptica al Data Center del edificio C que alimenta

a las oficinas administrativas del primer piso y a la biblioteca, todos los switches de acceso de este edificio se encuentran conectados a este switch de distribución por conexiones de cable de cobre, en el segundo piso cada una de las seis oficinas administrativas (Facultad de Ciencias de la Salud, Estudios Generales, Oficina de Psicopedagogía, Facultad de Ciencias e Ingeniería, Facultad de Humanidades y Ciencias Sociales y la Facultad de Ciencias Contables) cuenta con un switch de acceso de 24 puertos, en el piso 3 se encuentra un switch de acceso que alimenta las aulas del tercer y cuarto piso, en el piso 5 hay un switch de acceso que alimenta al quinto y sexto piso.

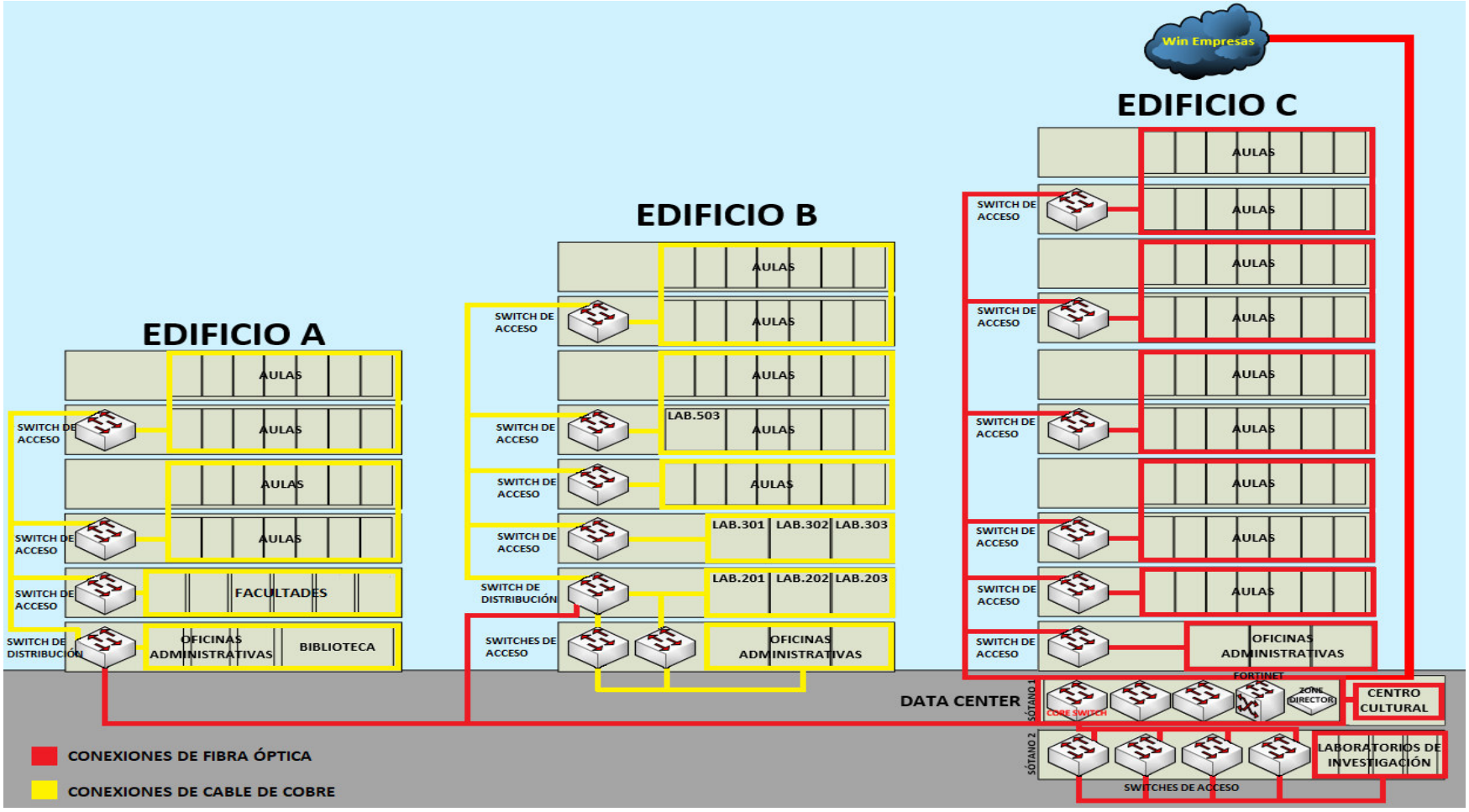
- **Edificio B.** Es un edificio de ocho pisos, en el piso 1 se encuentran dos switches para las oficinas administrativas, en el piso 2 se encuentra el switch de distribución de este edificio que se conecta por enlace de fibra óptica al Data Center del edificio C, en el piso 3 se encuentra un switch de acceso para los laboratorios 301, 302 y 303, en el piso 4 hay un switch de acceso para las aulas del cuarto piso, el piso 5 tiene un switch de acceso para el laboratorio 503 y para todas las aulas del quinto y sexto piso, en el piso 7 se encuentra un switch de acceso para todas las aulas del séptimo y octavo piso. En este edificio todos los switches son de 48 puertos.

- **Edificio C.** Es un edificio de dos sótanos y diez pisos, en el edificio C, en el sótano 1, se encuentra el Data Center donde se hallan todos los equipos principales en el despliegue de la red de datos, allí se ubica el router ethernet protegido por ATM-Fortinet, el Zone Director de Ruckus Wireless, tres switches que incluyen el Switch Core y una serie de servidores. Es a este Data Center donde llegan los servicios de fibra óptica de Win

Empresas que luego se distribuyen a los demás espacios de la universidad. El sótano 2 tiene cuatro switches que se conectan al Data Center para brindar servicios a los laboratorios de investigación. El piso 1 tiene switches de acceso con enlaces de fibra óptica para todos los ambientes y oficinas administrativas de este piso, en el piso 2 hay un switch de acceso para las aulas del segundo piso únicamente, en el piso 3 se encuentra un switch de acceso para las aulas del tercer y cuarto piso, en el piso 5 hay un switch de acceso que alimenta las aulas del quinto y sexto piso, el siguiente switch de acceso de encuentra en el piso 7 para las conexiones del séptimo y octavo piso, y el piso 9 tiene un switch de acceso para alimentar las aulas del noveno y décimo piso. La diferencia entre el edificio C y los otros dos edificios es que en el edificio C todos los enlaces son de fibra óptica estándar para 1000 Mbps.

**Figura 6**

*Distribución de switches en la Universidad de Ciencias y Humanidades en 2023*




*Nota.* En la Figura 6 se muestra la distribución de los switches en cada edificio del campus de la Universidad de Ciencias y Humanidades. Se han denotado los enlaces de fibra óptica en color rojo y los enlaces de cable de cobre en color amarillo.

## 3.3. DESARROLLO DEL OBJETIVO ESPECÍFICO 3

Procedimiento del diseño de red de datos para optimizar el servicio de la red de datos de la Universidad de Ciencias y Humanidades.

### 3.3.1. Configuración de máquinas virtuales en la plataforma de VirtualBox para crear la red interna “intnet”.

Inicialmente se debe instalar VirtualBox y descargar los archivos de instalación de cada uno de los sistemas operativos con los que se desea trabajar, estos sistemas operativos luego se instalan en VirtualBox y pasan a ser máquinas virtuales de manera que se pueden hacer modificaciones y configuraciones en ellas de manera independiente de la plataforma.

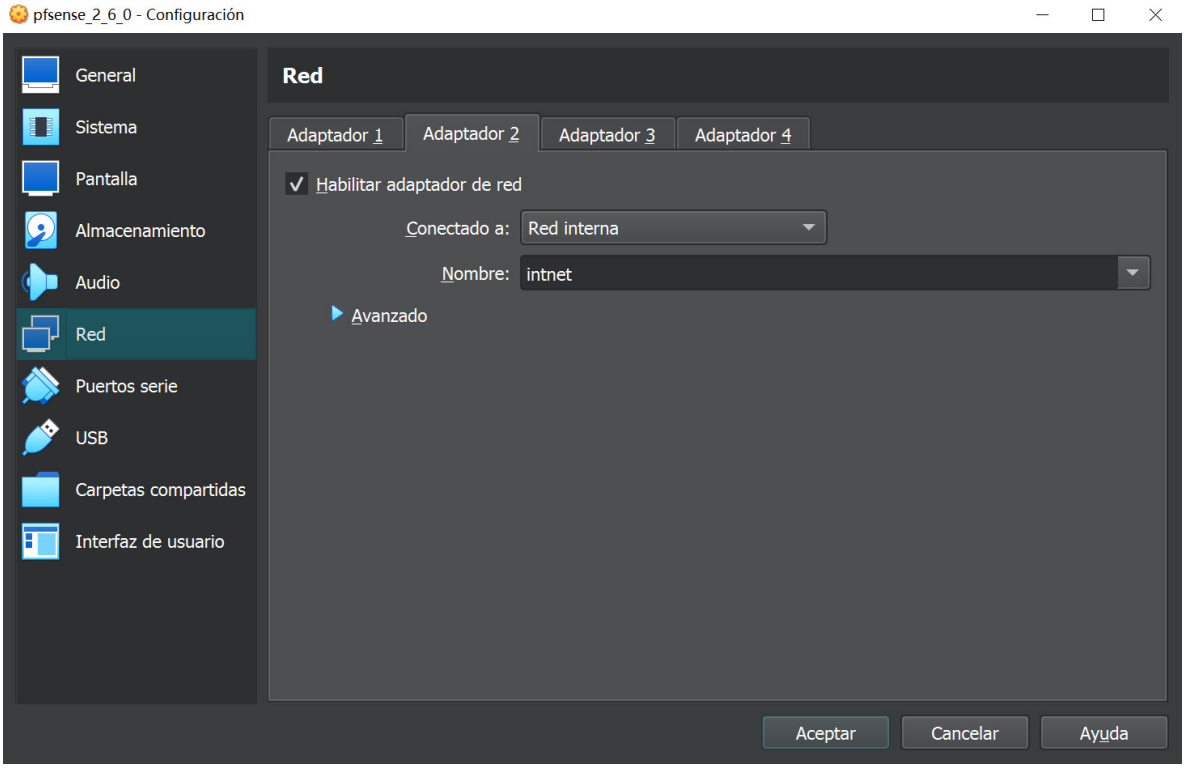
**Figura 7**

*Plataforma de VirtualBox*


*Nota.* En la Figura 7 se puede observar el entorno de VirtualBox, las máquinas virtuales, una vez instaladas, se muestran a la izquierda de la ventana y al seleccionar una se muestran las especificaciones. Se instaló pfSense y Windows 10 como las máquinas virtuales que inicialmente forman parte de la red interna.

**Figura 8**

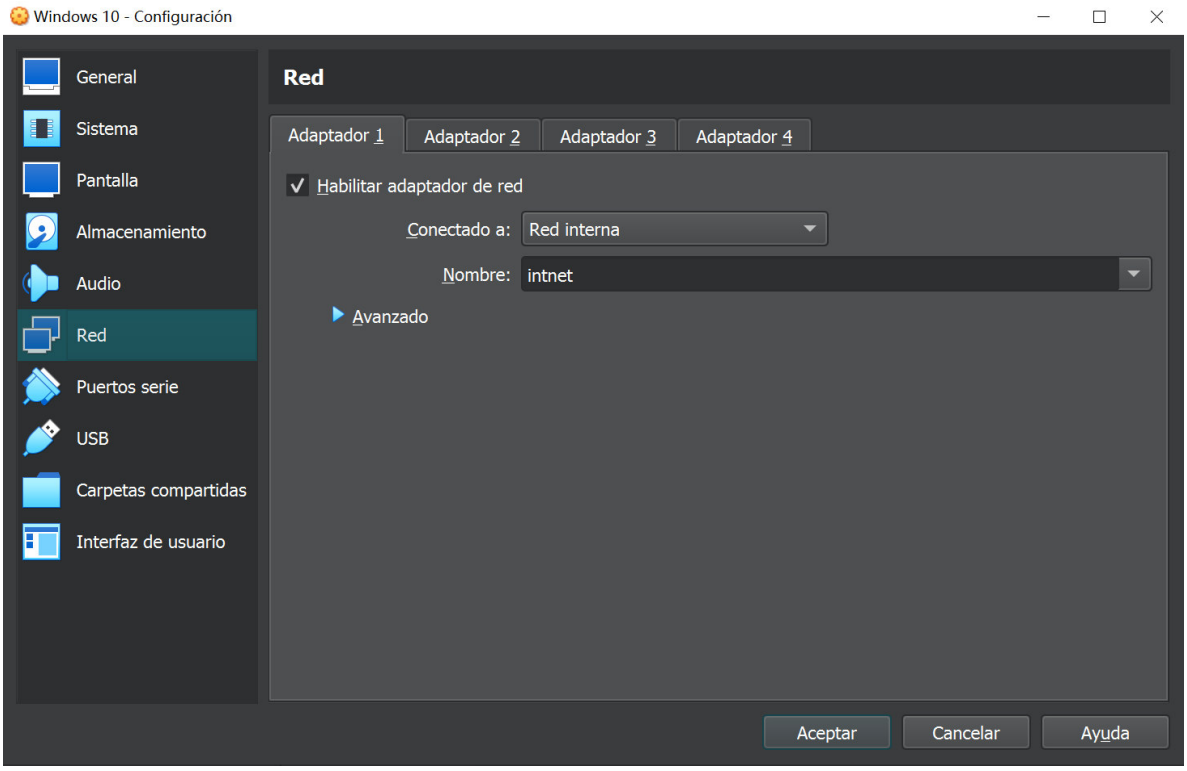
*Configuración de pfSense como parte de la red interna*




*Nota.* En la Figura 8 se muestra la configuración de la máquina virtual de pfSense para que forme parte de la red interna a la cual se la ha llamado “intnet”.

**Figura 9**

*Configuración de Windows 10 como parte de la red interna*



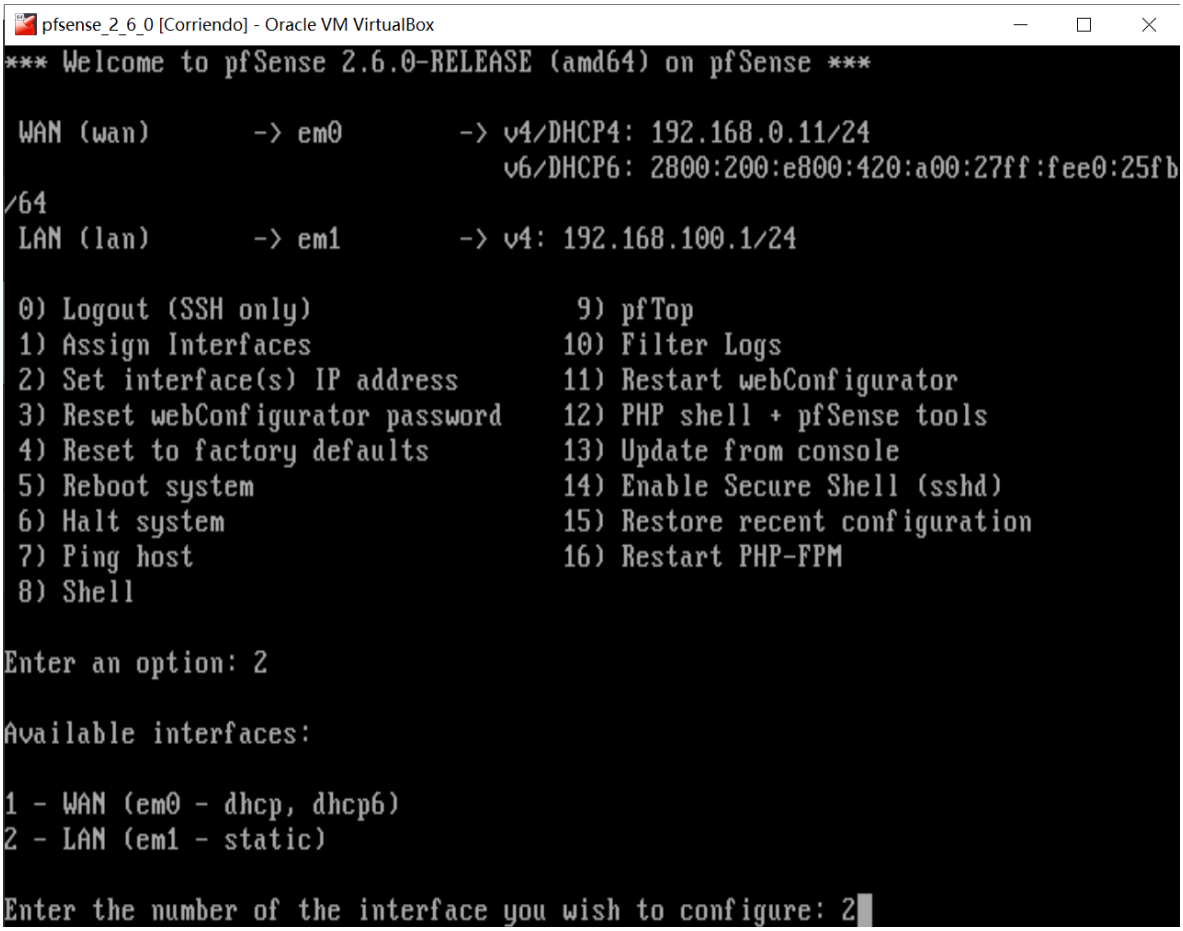

*Nota.* En la Figura 9 se muestra la configuración de la máquina virtual de Windows 10 para que forme parte de la red interna a la cual se la ha llamado “intnet”.

### 3.3.2. Configuración inicial de pfSense

Una vez instaladas las máquinas virtuales y configuradas como parte de la red interna “intnet” se debe entrar en la máquina virtual de pfSense para hacer las configuraciones iniciales como el cambio de las direcciones IP de la red y la asignación de direcciones IP a las demás máquinas virtuales a través de DHCP.

**Figura 10**

*Terminal de pfSense*



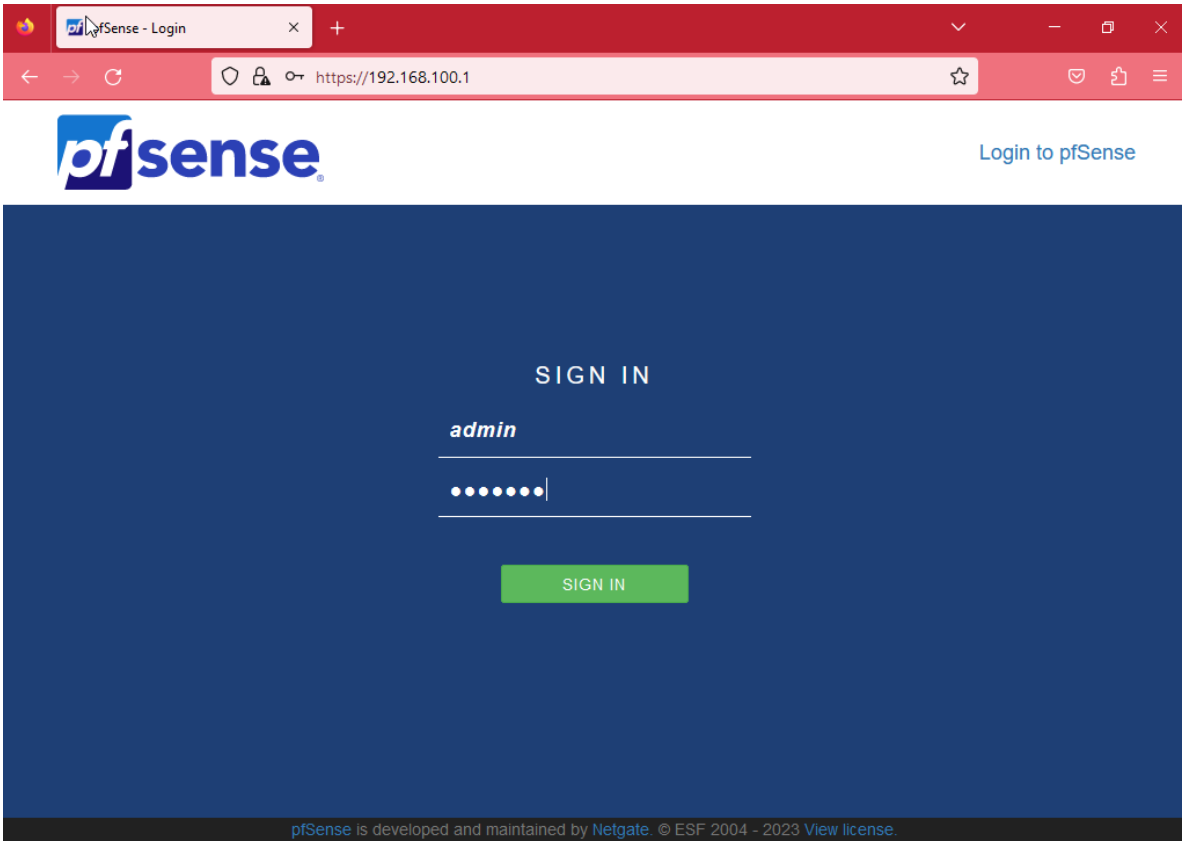

*Nota.* En la Figura 10 se puede ver la terminal de pfSense. Al abrir la máquina virtual de pfSense se espera a que cargue el programa y el sistema abre la terminal desde la cual se hacen muchas de las configuraciones de pfSense, se presentan dieciséis opciones iniciales, se elige la opción 2 para la configuración de direcciones IP para cambiar las direcciones IP de la red WAN y red LAN. También se configura DHCP desde la terminal para que pfSense asigne direcciones IP a las demás

máquinas virtuales que conforman la red interna “intnet”.

Una vez asignadas las direcciones IP, se puede ingresar a una de las máquinas virtuales pertenecientes a la red interna y se puede acceder a la plataforma en línea de pfSense a través del buscador, colocando la dirección IP asignada a la red LAN en la barra de búsqueda.

**Figura 11**

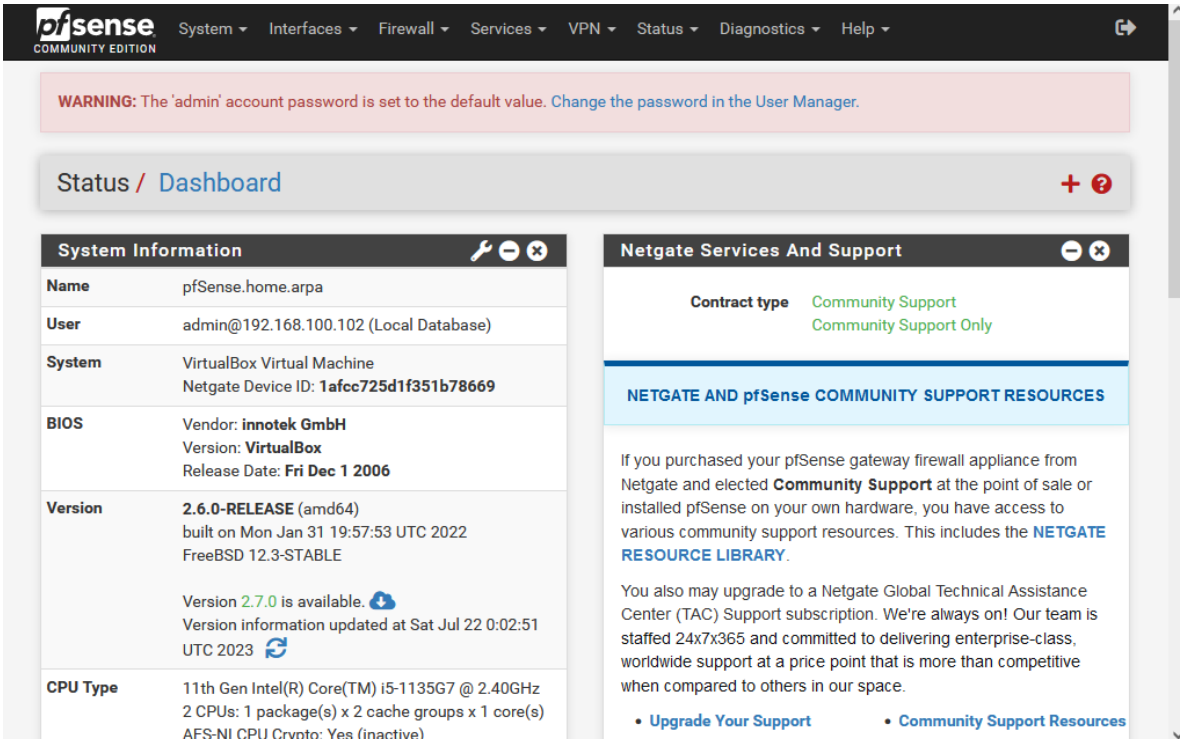
*Interface Gráfica de Usuario Online de pfSense*




*Nota.* En la Figura 11 se muestra la página de ingreso en línea de pfSense. Luego de realizar las configuraciones iniciales de pfSense desde la terminal, se puede ingresar a cualquiera de las máquinas virtuales que conforman la red interna “intnet” para ingresar a la plataforma Dashboard en línea de pfSense. En la Figura 12 se ha ingresado al buscador Mozilla Firefox desde la máquina virtual de Windows 10, se coloca la dirección IP de la red LAN en el buscador y luego se ingresan las credenciales, inicialmente el nombre de usuario es “admin” y la contraseña es “pfsense”, esto se puede cambiar para una contraseña más segura una vez dentro.

**Figura 12**

*Dashboard de pfSense*

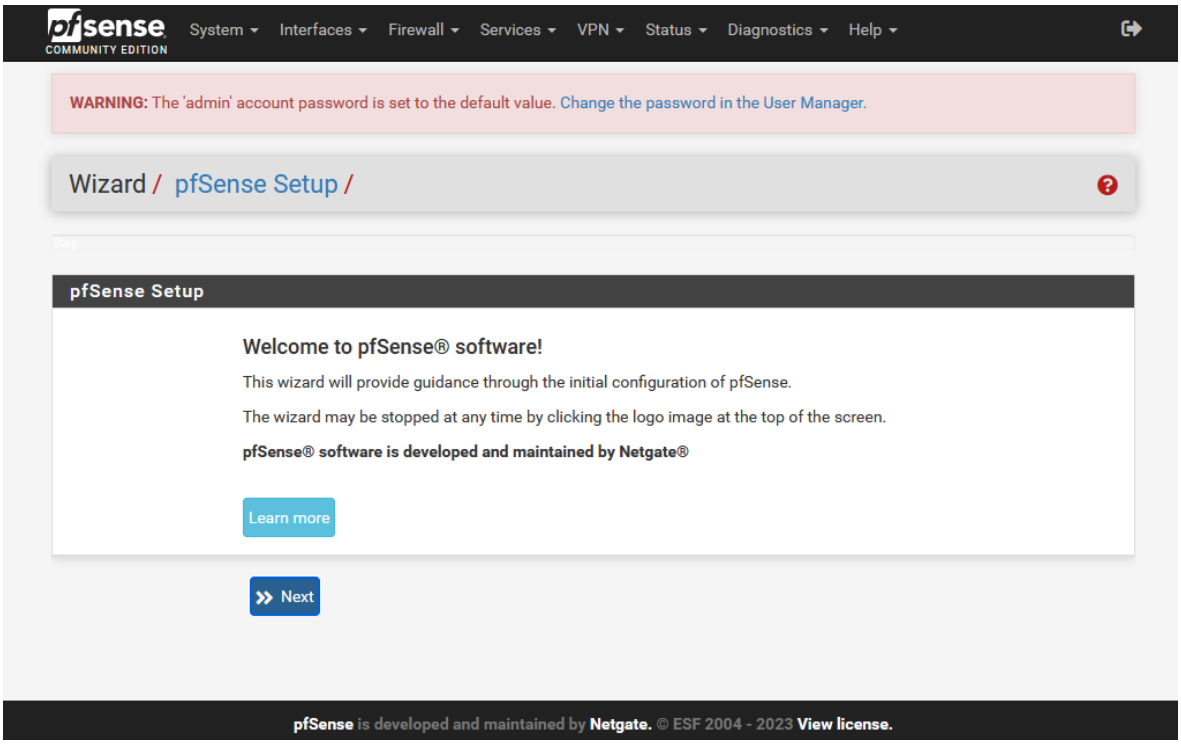



*Nota.* En la Figura 12 se muestra el Dashboard en línea de pfSense, desde el cual se realiza el manejo y administración de la red en forma centralizada, se pueden ver los detalles del funcionamiento de la red interna desde la página principal, estos detalles pueden ser configurados y se puede cambiar y personalizar según la necesidad de la red. En la parte superior se presentan las opciones (System, Interfaces, Firewall, Services, VPN, Status, Diagnostics y Help) con las que se puede hacer toda la configuración de pfSense.

Al ingresar a pfSense por primera vez se puede hacer la programación inicial siguiendo los pasos del Wizard de pfSense.

**Figura 13**

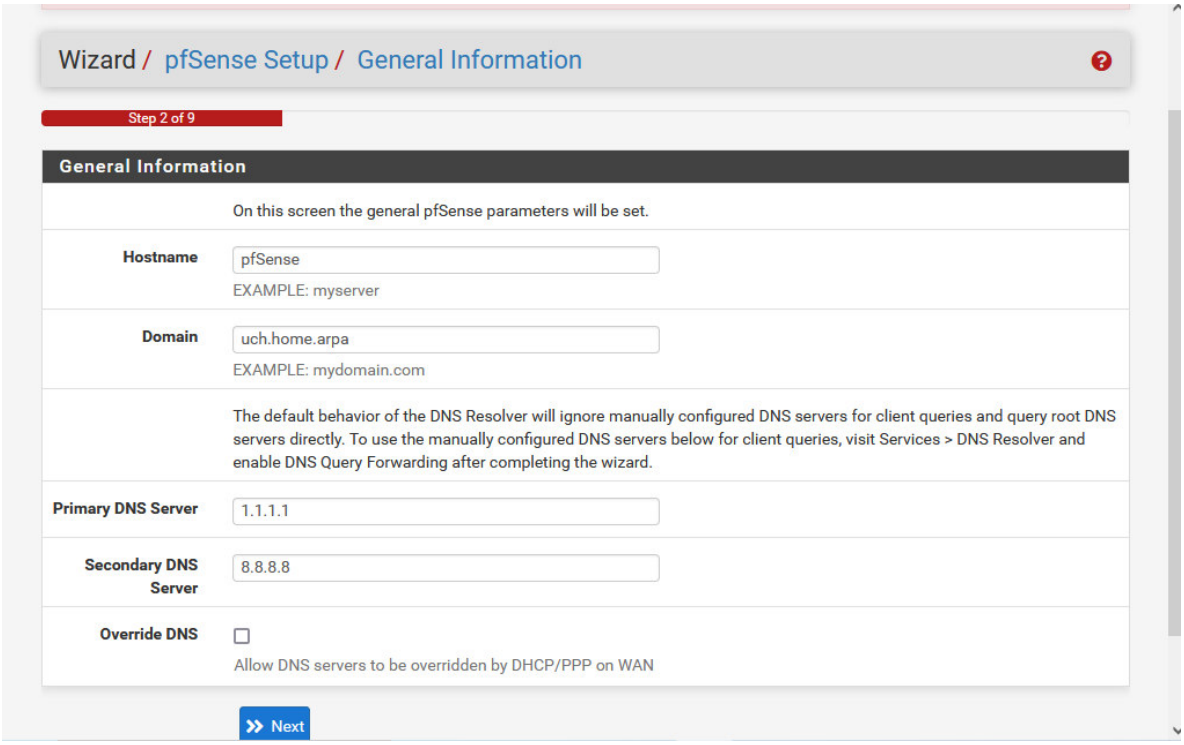
*Wizard de pfSense*




*Nota.* En la Figura 13 se muestra el Wizard de programación básica de pfSense, se siguen 9 pasos que completan la configuración básica.

**Figura 14**

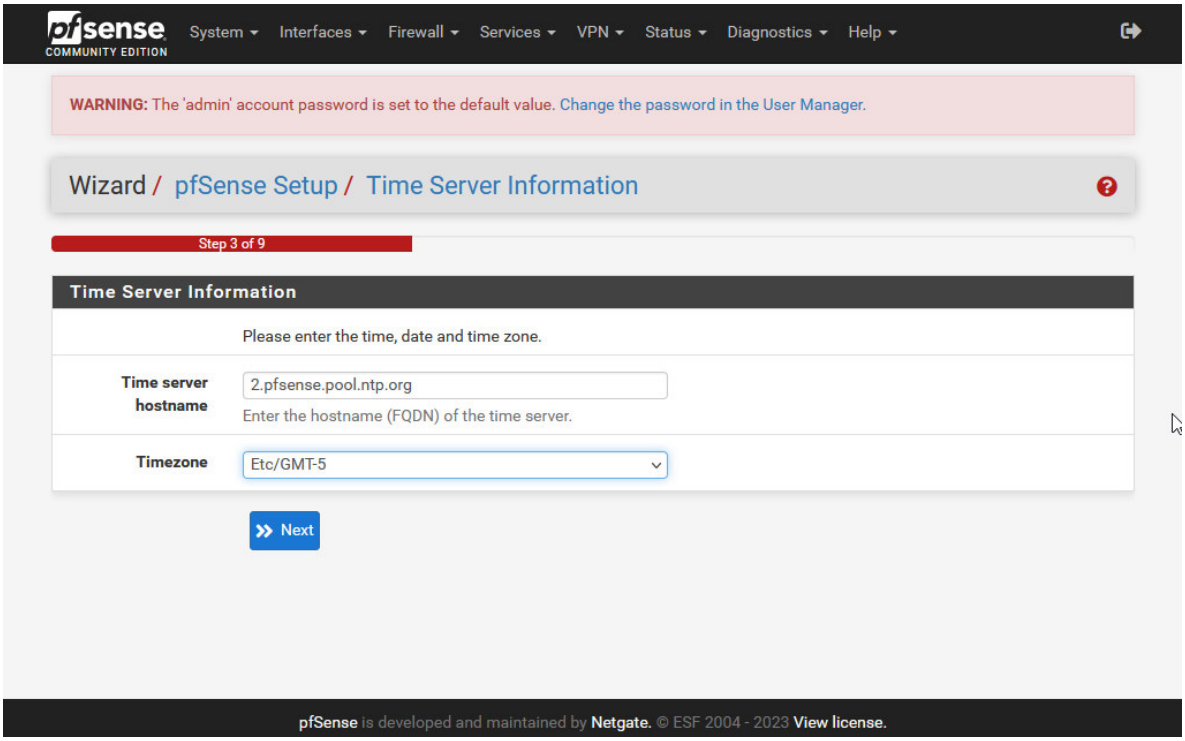
*Configuración de la información general desde el Wizard de pfSense*




*Nota.* En la Figura 14 se muestra la configuración de la información general desde la cual se elige el nombre de host (pfSense), el nombre de dominio (uch.home.arpa), el servidor primario de DNS (1.1.1.1 de Cloudflare) y el servidor secundario de DNS (8.8.8.8 de Google) que permiten mejorar el rendimiento, la velocidad del servicio y la privacidad.

**Figura 15**

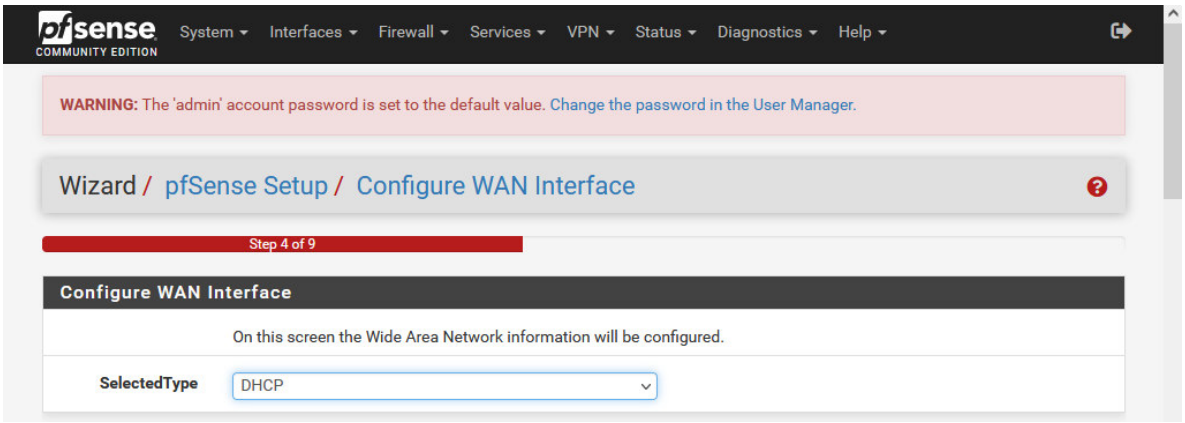
*Configuración de FQDN (Fully Qualified Domain Name) y la zona horaria*




*Nota.* En la Figura 15 se muestra el tercer paso de la configuración del Wizard de pfSense donde se escoge un FQDN (2.pfsense.pool.ntp.org) y la zona horaria (Etc/GMT-5).

**Figura 16**

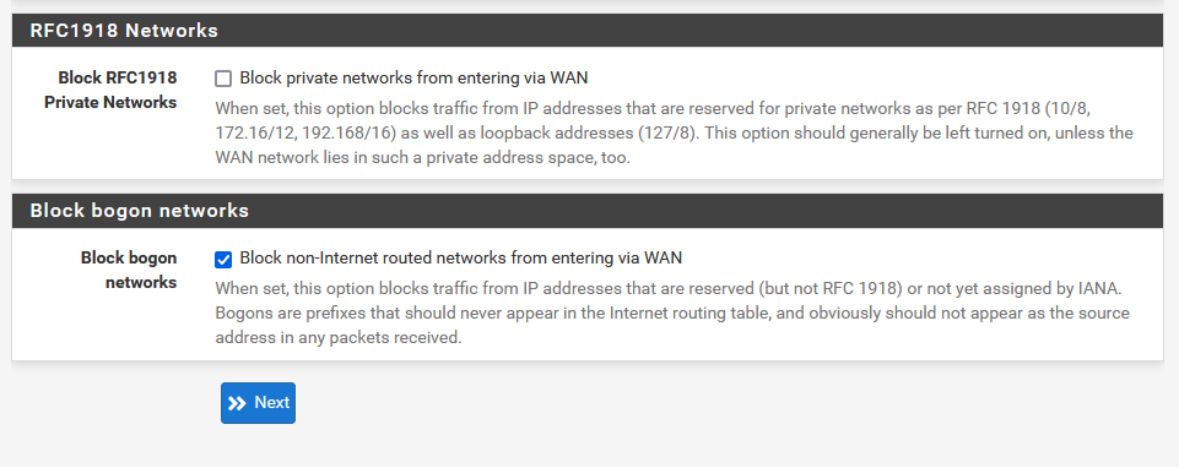
*Configuración de DHCP de la red WAN*




*Nota.* En la Figura 16 se muestra parte de la configuración de la red WAN, se elige el protocolo DHCP (Dynamic Host Configuration Protocol).

**Figura 17**

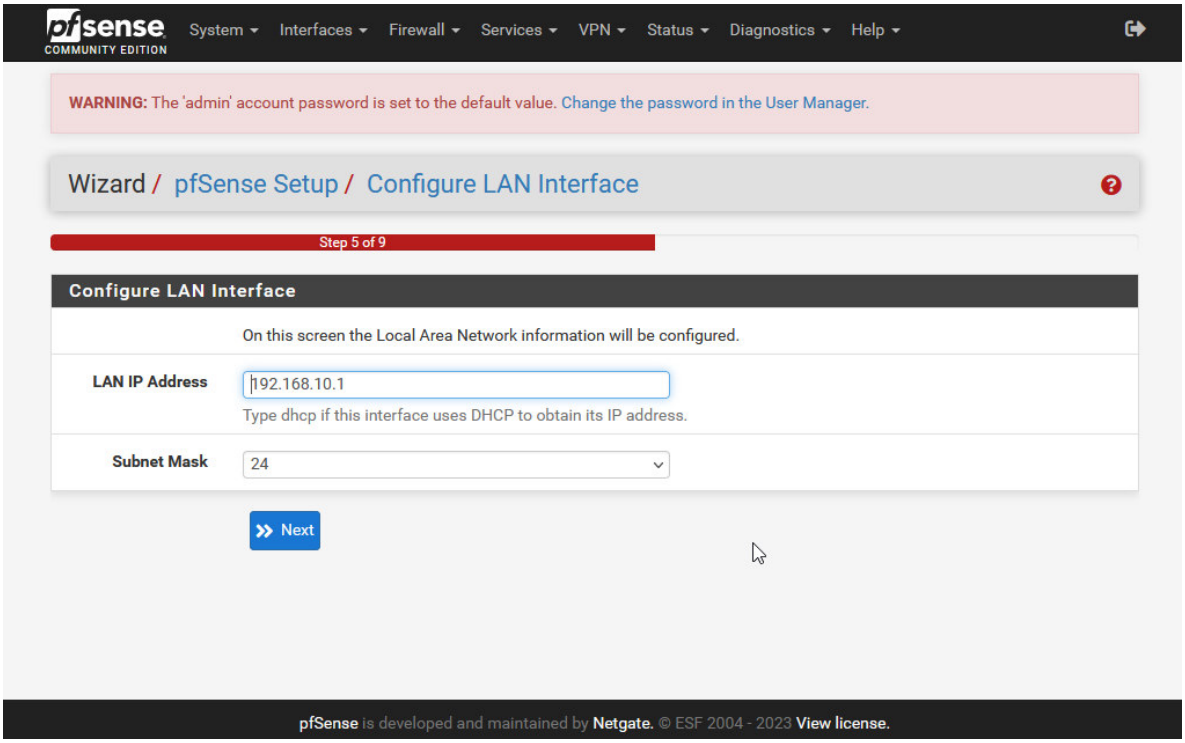
*Configuración para bloqueos de redes bogons de la red WAN*




*Nota.* En la Figura 17 se muestra la configuración para bloqueos de redes con direcciones IP falsas (redes bogons).

**Figura 18**

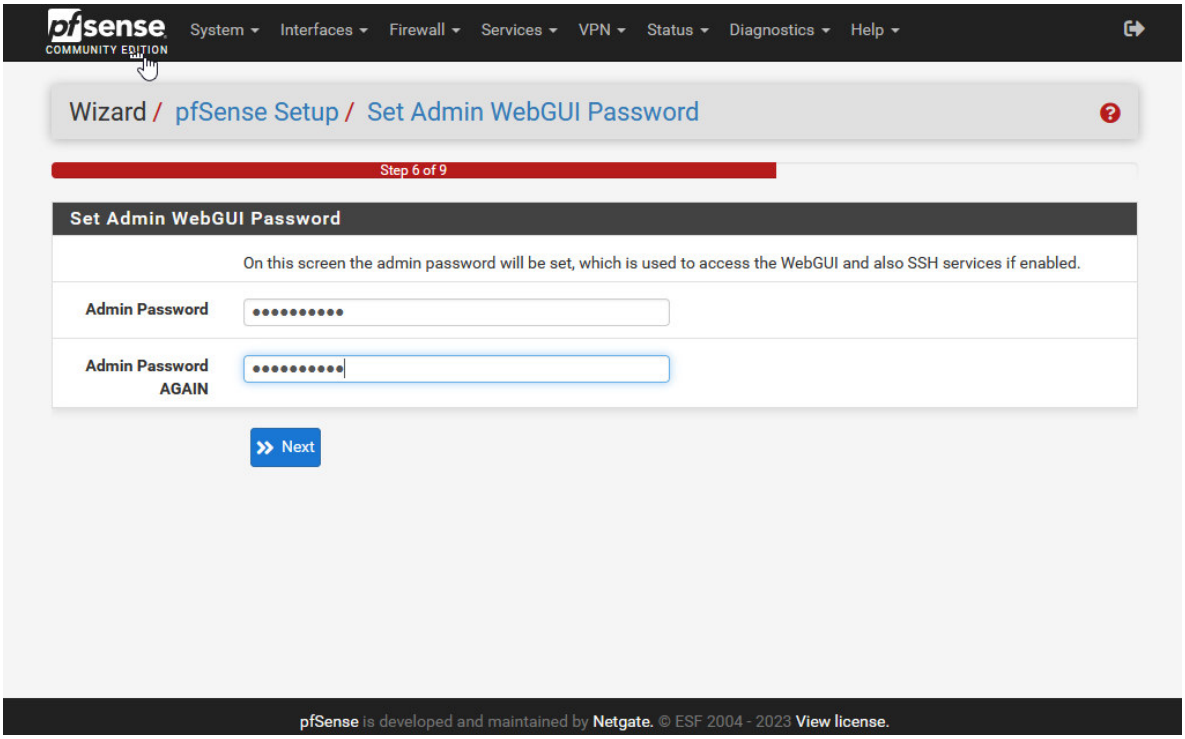
*Configuración de dirección IP de red LAN desde el Wizard.*




*Nota.* En la Figura 18 se muestra la configuración de dirección IP de la red LAN, aquí ya aparece automáticamente la que se había configurado desde la terminal (192.168.10.1/24) pero se puede configurar desde la interface gráfica de usuario en caso de no haberse hecho desde la terminal.

**Figura 19**

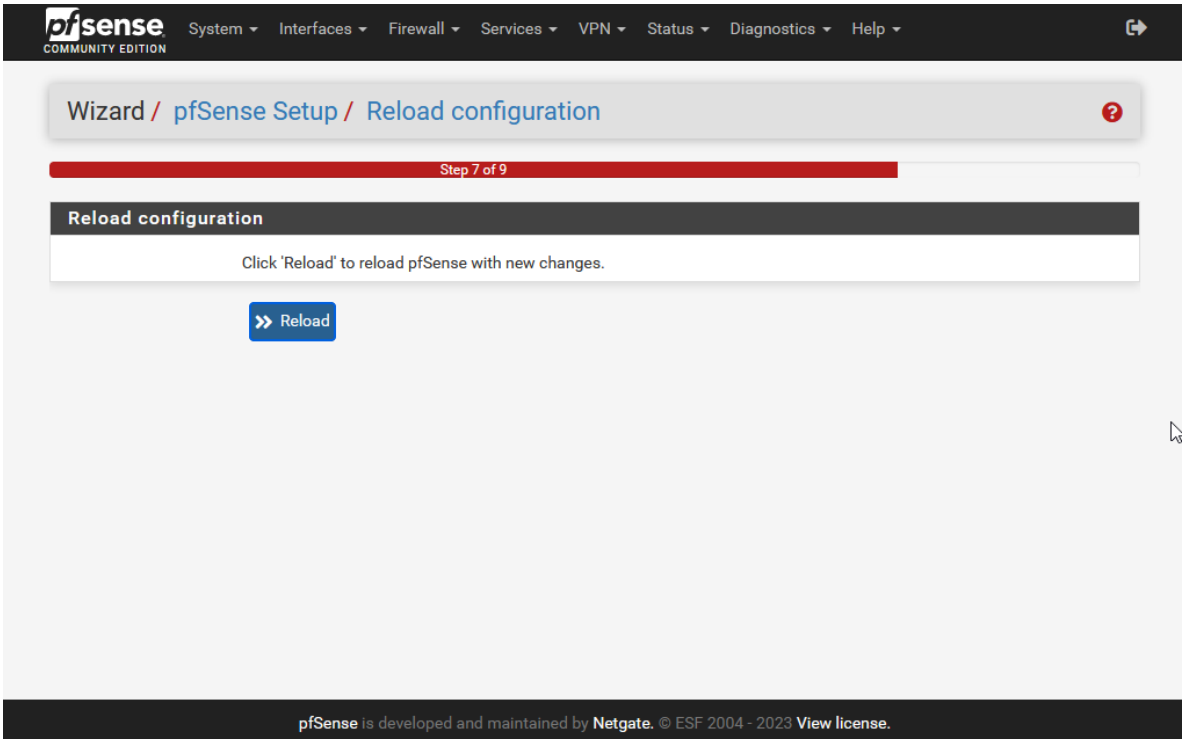
*Cambio a contraseña más segura*




*Nota.* En la Figura 19 se muestra el cambio a una contraseña más segura para el sistema.

**Figura 20**

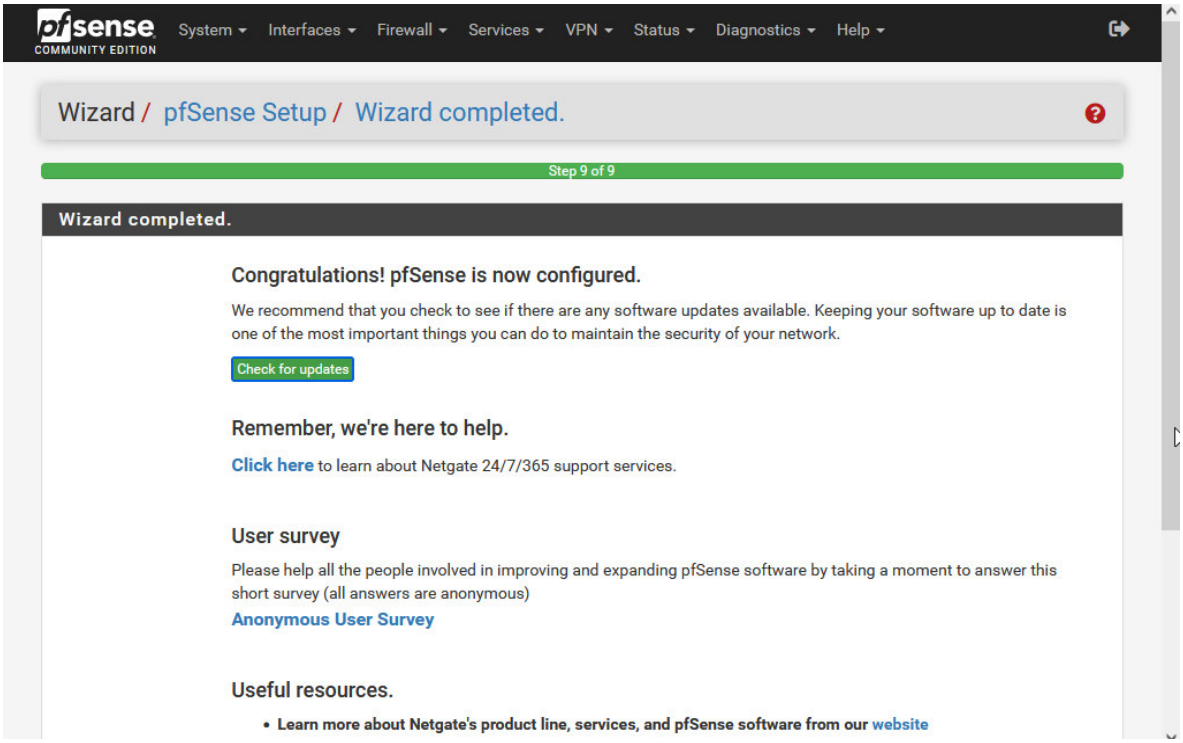
*Recarga de la página de pfSense*




*Nota.* En la Figura 20 se muestra el paso 7 donde se debe volver a cargar la página de pfSense para que se realicen los cambios configurados.

**Figura 21**

*Finalización de la configuración del Wizard*

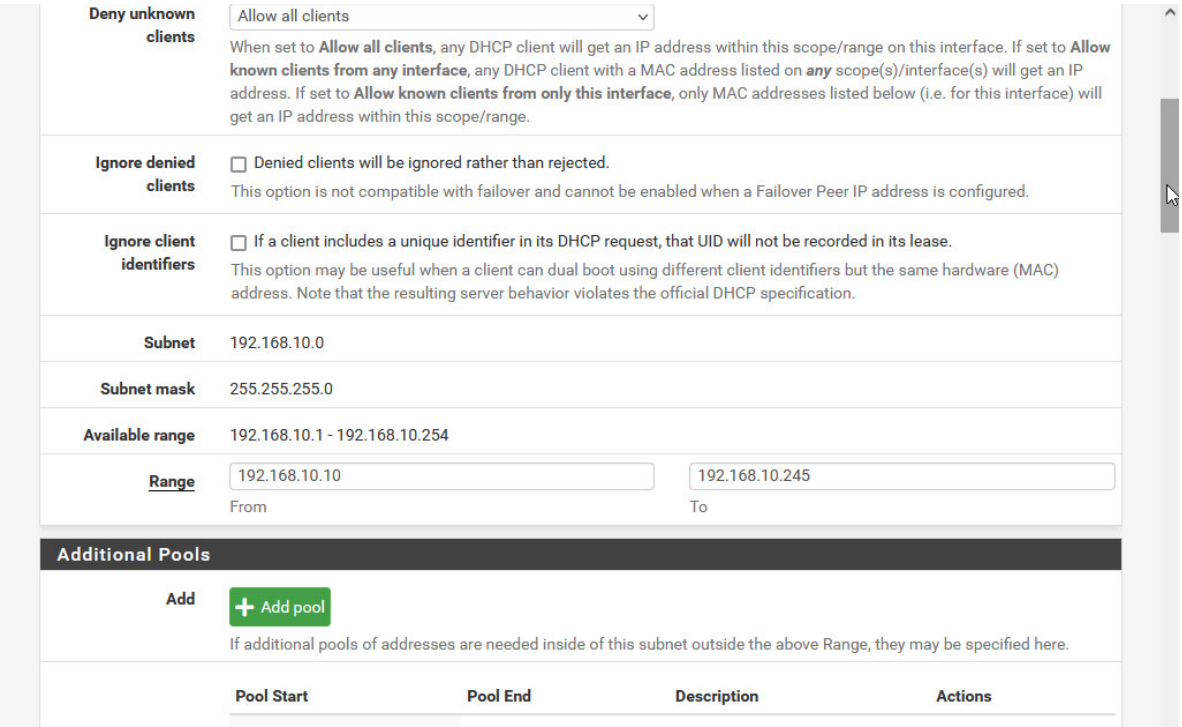



*Nota.* En la Figura 21 se muestra la finalización del proceso de configuración básica con el Wizard de pfSense.

Luego de terminar la configuración con el Wizard de pfSense se puede hacer la limitación del rango de direcciones IP elegibles en la pestaña de configuración.

**Figura 22**

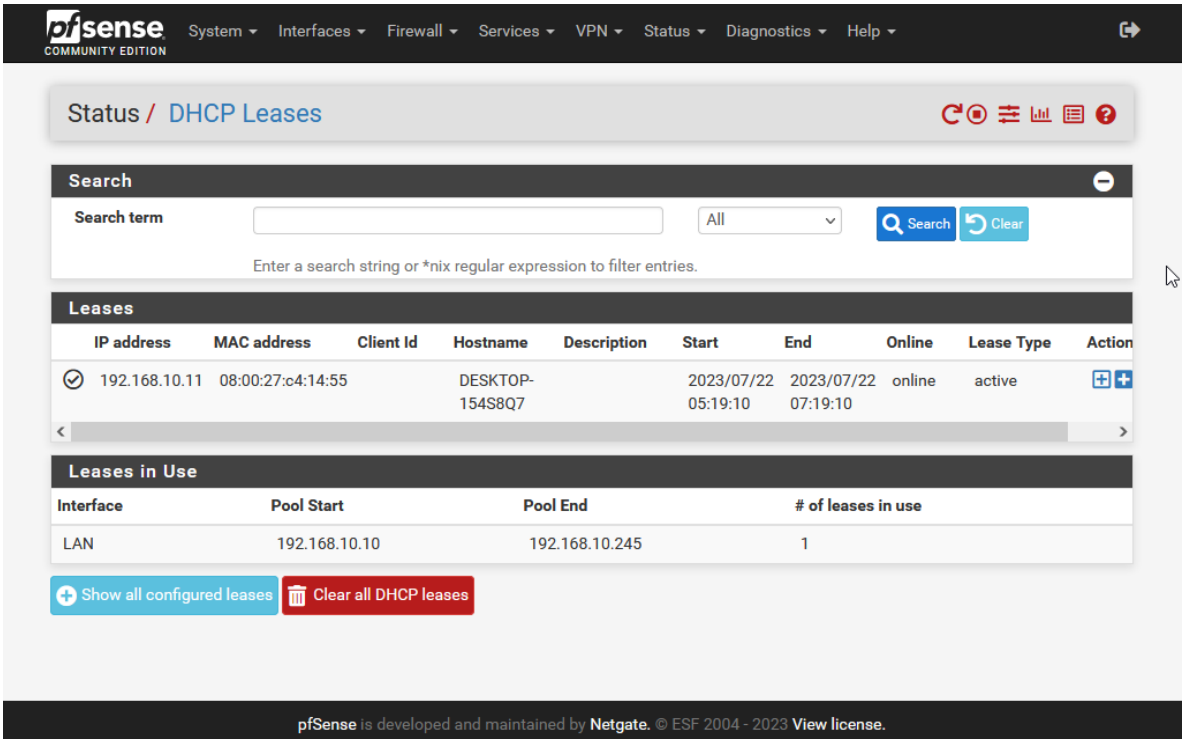
*Configuración de rango de direcciones IP*




*Nota.* En la Figura 22 se muestra el rango elegido para las direcciones IP en la red, desde la dirección 192.168.10.10 hasta la dirección 192.168.10.245.

**Figura 23**

*Muestra de pool de direcciones IP*



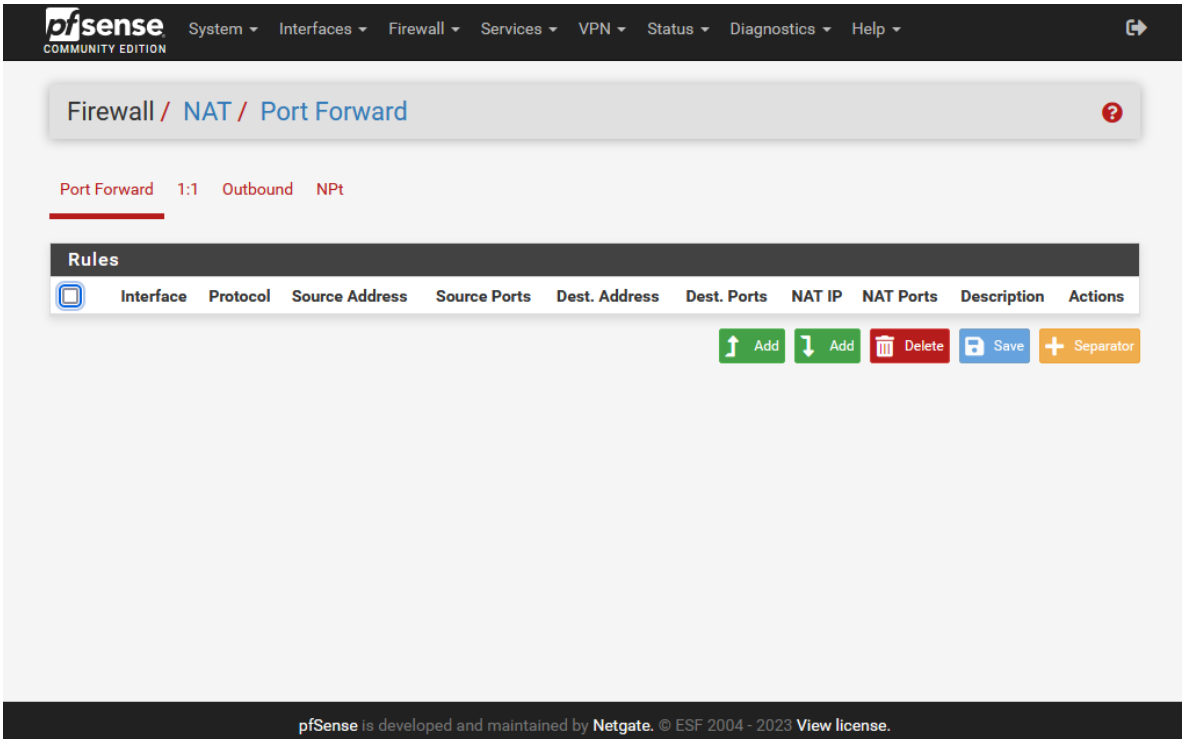

*Nota.* En la Figura 23 se muestra la configuración guardada del pool de direcciones IP en el rango elegido previamente.

### 3.3.3. Port Forwarding

Se deben abrir algunos puertos de la red para asegurar el acceso remoto a los servicios de la universidad.

**Figura 24**

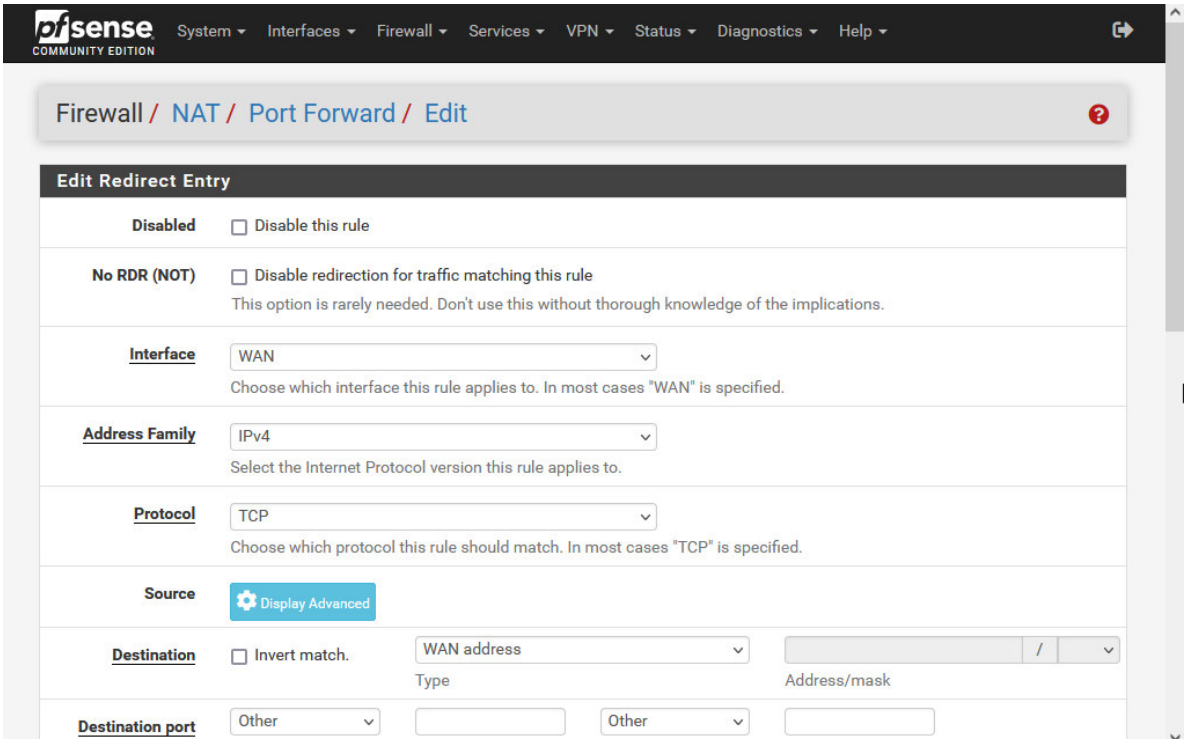
*Configuración de reenvío de puertos*




*Nota.* En la Figura 24 se muestra el camino de opciones que se debe seguir para acceder a la opción de configuración de reenvío de puertos (Port Forwarding).

**Figura 25**

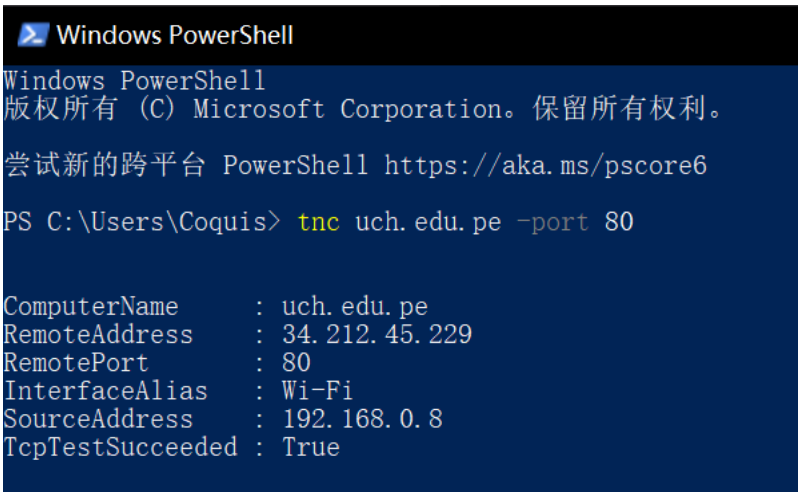
*Edición de configuración de reenvío de puertos*




*Nota.* En la Figura 25 se muestran la configuración inicial para el reenvío de puertos.

**Figura 26**

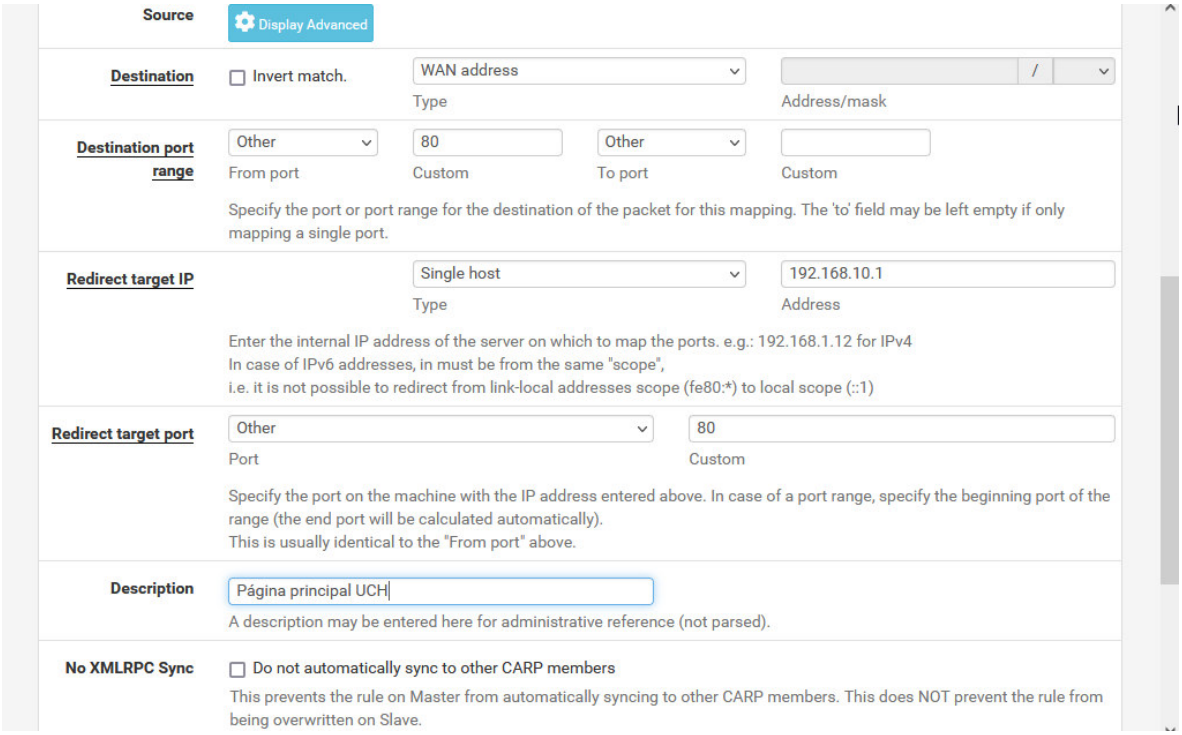
*Windows PowerShell para verificación de puertos*




*Nota.* En la Figura 26 se muestra el comando en Windows PowerShell para la verificación del puerto utilizado por una página en internet (puerto 80), este puerto luego debe abrirse desde la plataforma de pfSense para permitir el acceso al servicio de la página de la universidad desde fuera de la red.

**Figura 27**

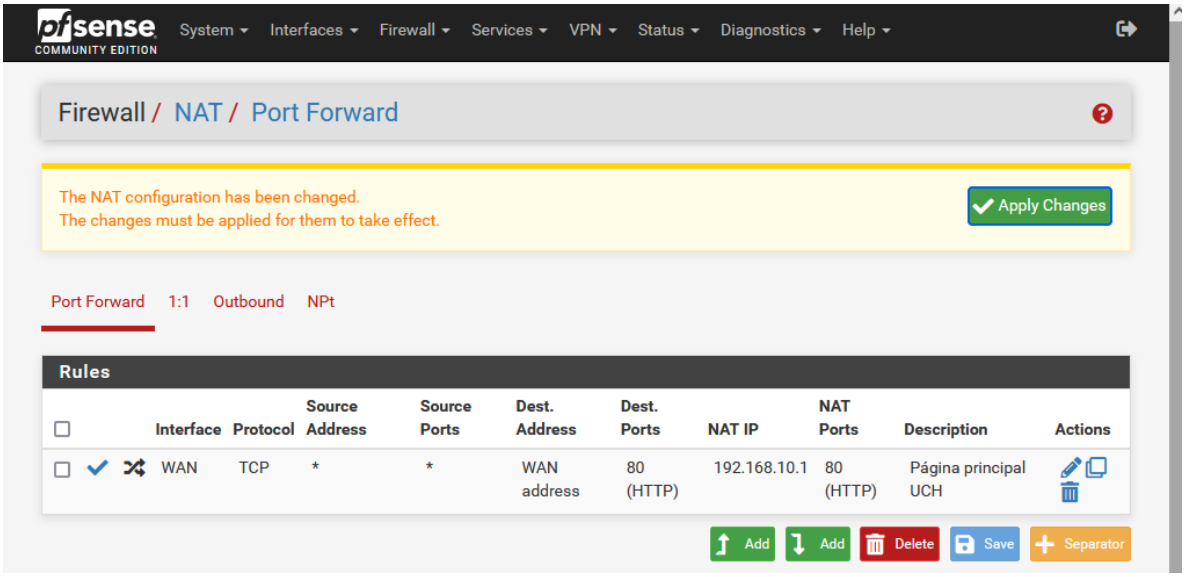
*Asignación del puerto que se desea abrir*




*Nota.* En la Figura 27 se muestra la configuración para abrir el puerto 80 en la red junto con su descripción (Página principal UCH), debido a que es el puerto utilizado por la página de la universidad en internet.

**Figura 28**

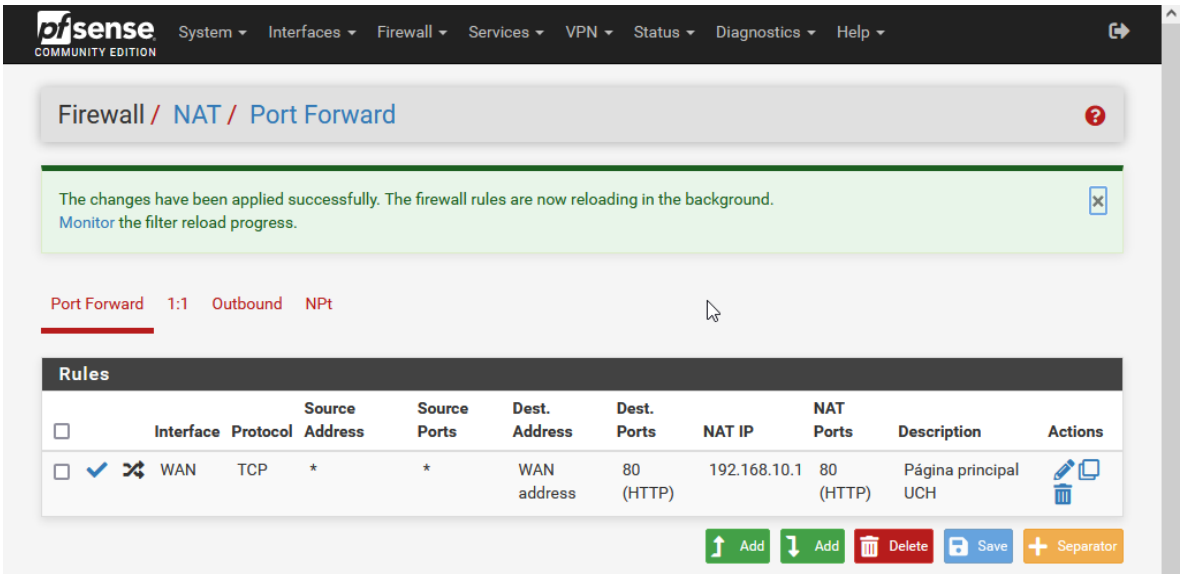
*Finalización de configuración de reenvío de puertos para el puerto 80*




*Nota.* En la Figura 28 se muestra la finalización de la configuración para abrir el puerto 80 en la red, se debe hacer clic en Apply Changes para guardar la configuración.

**Figura 29**

*Cambios de reenvío de puertos guardados de manera exitosa*



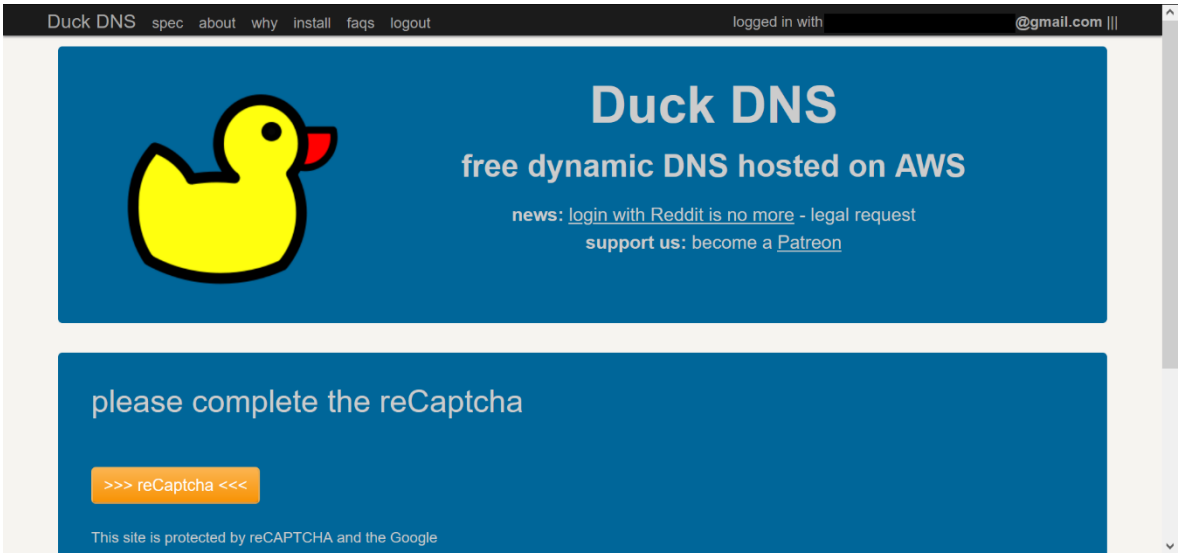

*Nota.* En la Figura 29 se muestra que luego de hacer clic en Apply Changes el sistema indica que los cambios han sido guardados de manera exitosa.

### 3.3.4. DNS dinámico

En esta sección se realiza la configuración del servicio de Dynamic DNS para la red, lo cual permite el manejo de direcciones IP al navegar en internet. Se debe elegir un proveedor para este servicio, para el presente trabajo se ha elegido el uso de Duck DNS que es un proveedor gratuito alojado en la Red Virtual Privada en La Nube (VPC) de Amazon (Duck DNS, 2023).

**Figura 30**

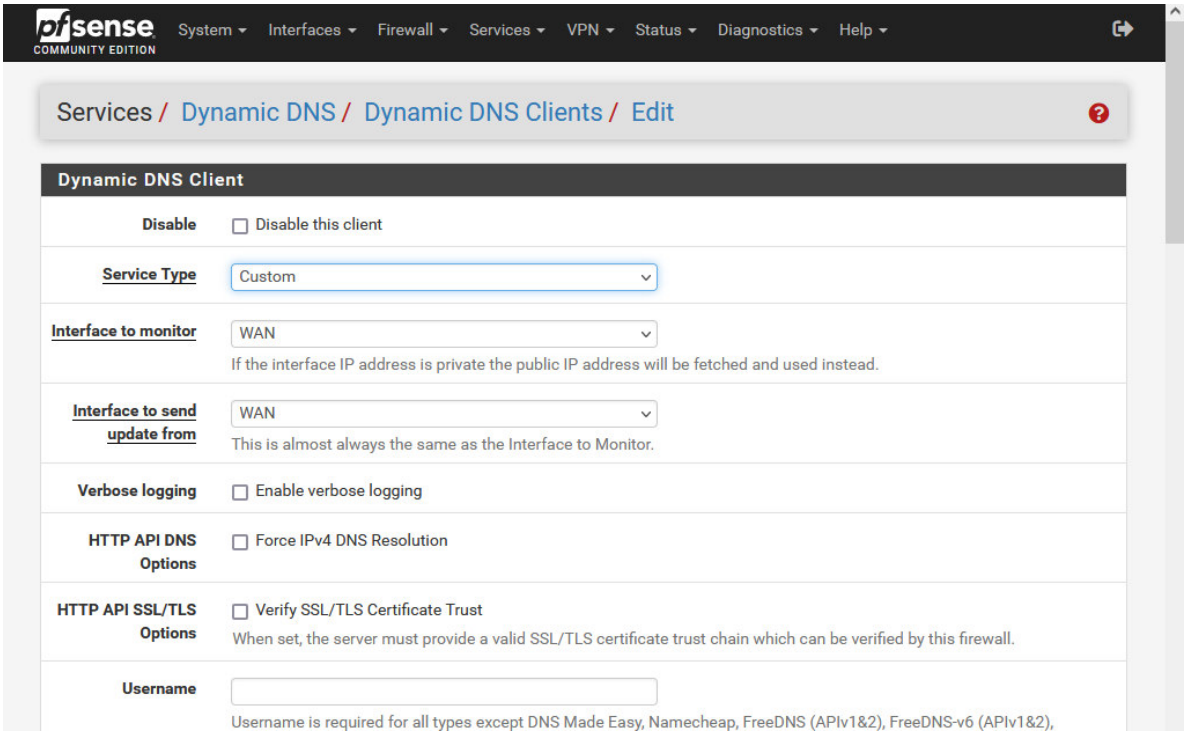
*Duck DNS*




*Nota.* En la Figura 30 se muestra el proveedor elegido para Dynamic DNS, Duck DNS, el cual brinda servicio gratuito para manejo de las direcciones IP en la red.

**Figura 31**

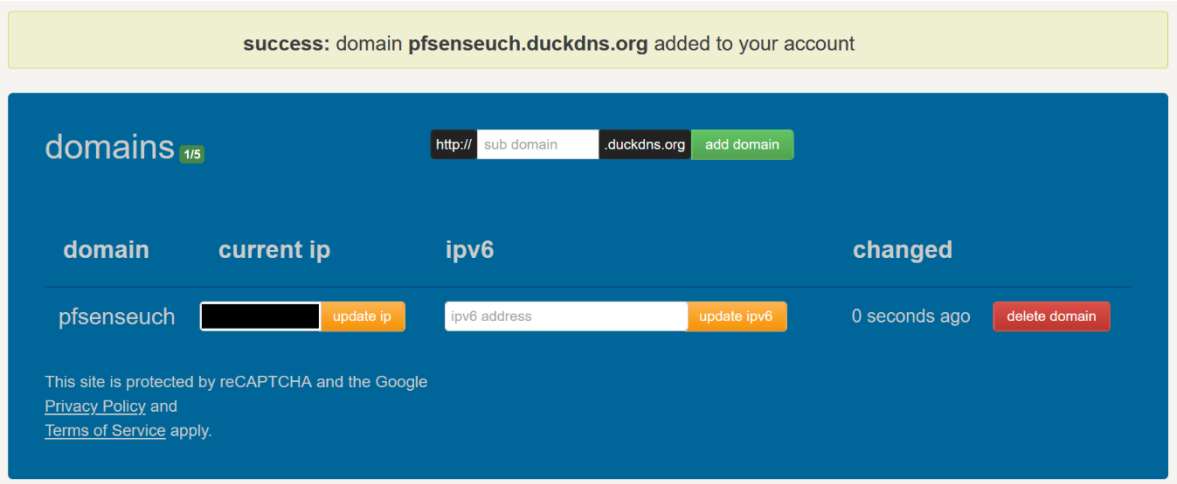
*Configuración en pfSense de Dynamic DNS*




*Nota.* En la Figura 31 se muestra la configuración de Dynamic DNS en la plataforma de pfSense, para Duck DNS se debe escoger la opción de Custom y red WAN.

**Figura 32**

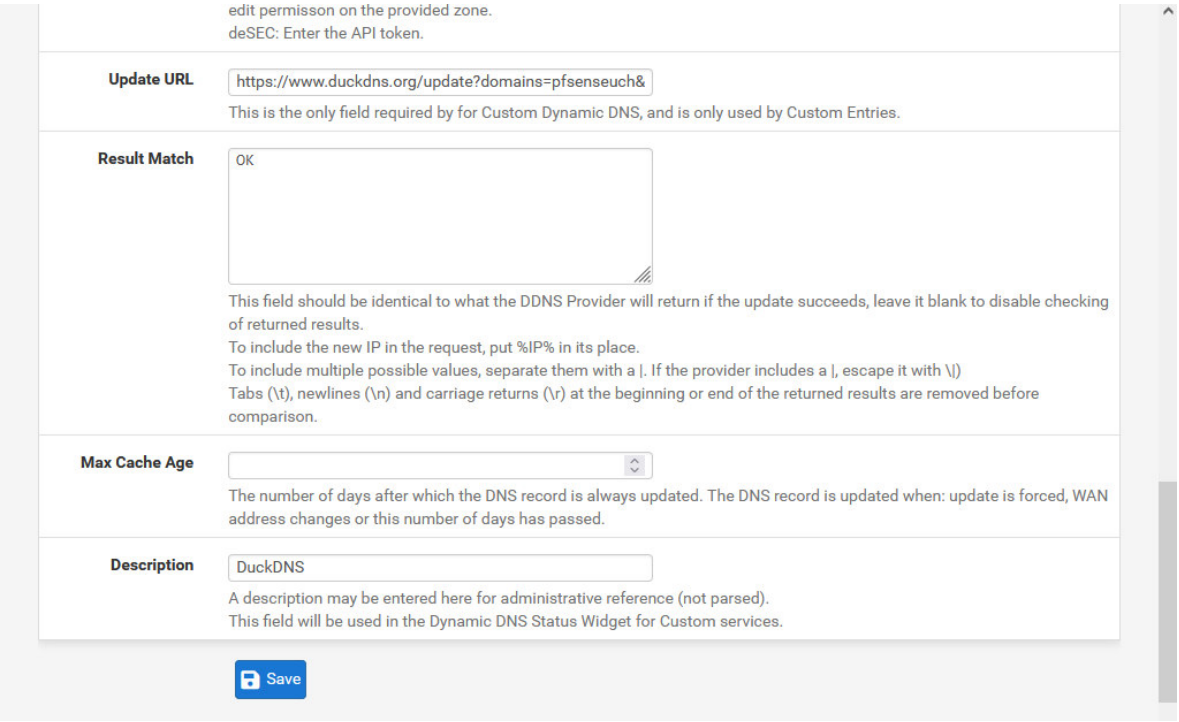
*Datos que deben ser ingresados en pfSense para configurar Duck DNS como proveedor del servicio*




*Nota.* En la Figura 32 se muestran los datos de dominio elegidos en la creación de la cuenta en la página de Duck DNS.

**Figura 33**

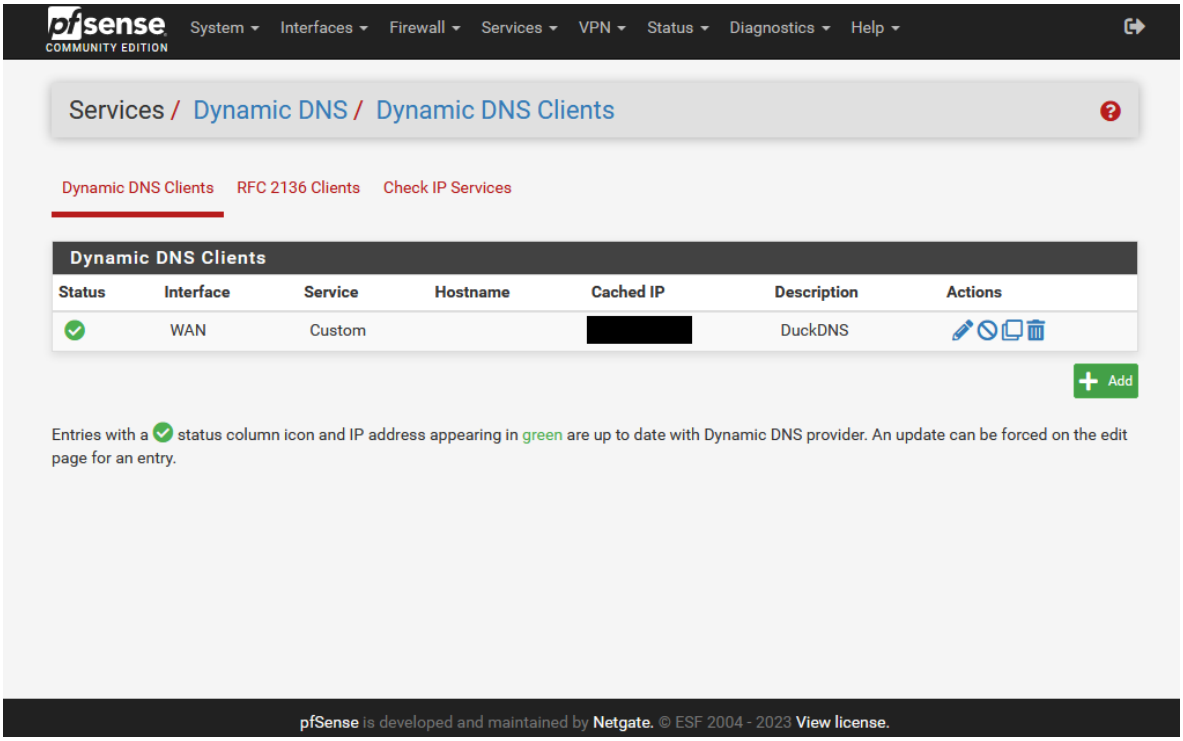
*Datos ingresados en la página de pfSense para configuración de Duck DNS como proveedor de Dynamic DNS*




*Nota.* En la Figura 33 se muestran los datos que restantes para la configuración de Duck DNS como proveedor de servicio de Dynamic DNS, se debe copiar y pegar un URL brindado por Duck DNS desde la página principal de la cuenta creada, el cual contiene el nombre de dominio elegido y un token único que permite la asignación del servicio. Colocar el resultado que debe coincidir con el elegido por Duck DNS y una descripción al final de la página, luego se guarda la configuración.

**Figura 34**

*Configuración de Dynamic DNS exitosa*



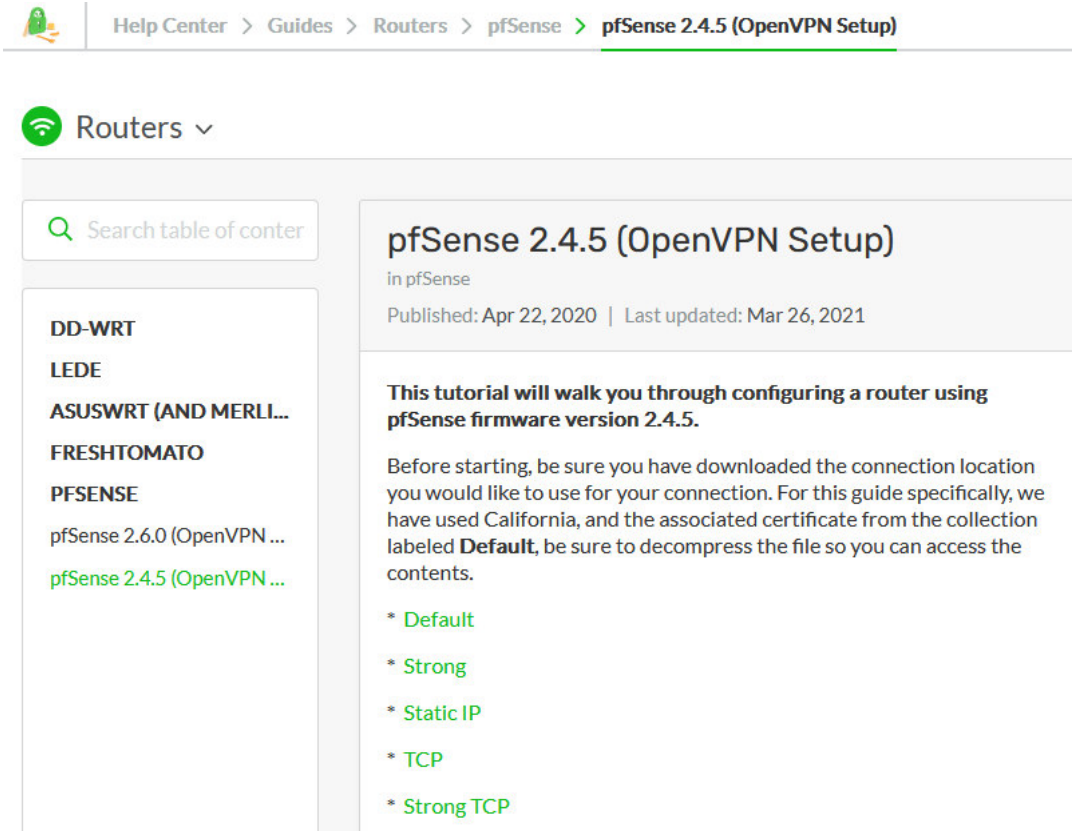

*Nota.* En la Figura 34 se muestra la confirmación de que el Dynamic DNS se configuro de manera correcta y se muestra el estado activo para el servicio con el proveedor elegido.

### 3.3.5. Virtual Private Network (VPN)

En este paso se configura una red privada virtual de modo que todo el tráfico de la red se redirija a un servidor remoto funcionando como un filtro que permite resguardar la información de manera más segura. El servicio de VPN que se ha utilizado para el presente trabajo es Private Internet Access, este es un servicio pago que brinda una alta seguridad y trabaja con pfSense (Private Internet Access, 2023).

**Figura 35**

*Página de Private Internet Access para configurar con pfSense*

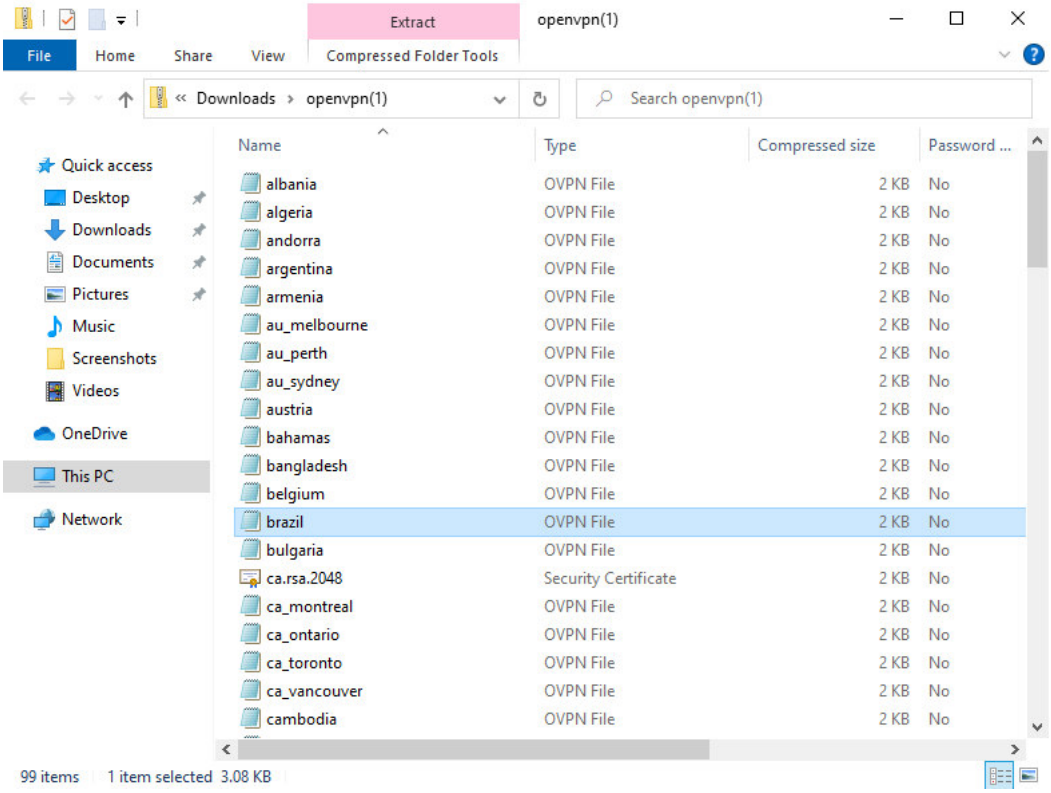



*Nota.* En la Figura 35 se muestra la página de Private Internet Access para hacer todas las configuraciones junto con pfSense. Lo primero que debe hacerse es la creación de una cuenta con Private Internet Access, al crearse una cuenta se pasa a recibir las credenciales que luego permiten vincular el servicio de VPN con pfSense. Estando en la página de Private Internet Access se debe abrir la pestaña que dice “Default” para que se descargue un archivo comprimido (.zip) que contiene

datos que se deben ingresar en la página de configuraciones de pfSense.

**Figura 36**

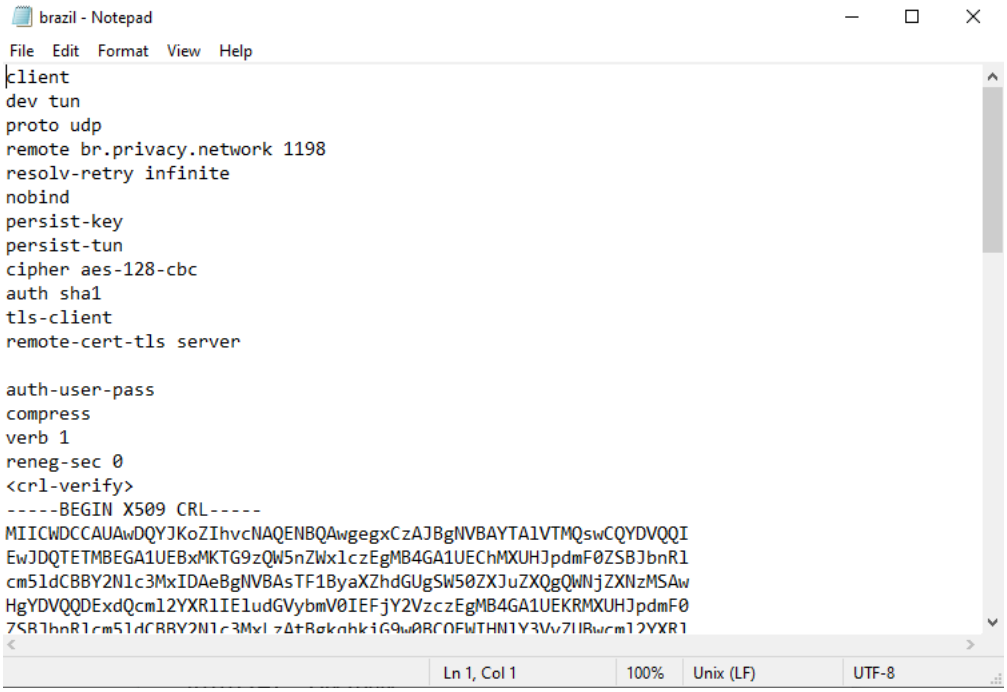
*Archivo comprimido al ser abierto*




*Nota.* En la Figura 36 se muestra el contenido del archivo comprimido descargado en la página de Private Internet Access. Se debe escoger el archivo de la ubicación geográfica más cercana, en el caso del presente trabajo se ha escogido Brasil.

**Figura 37**

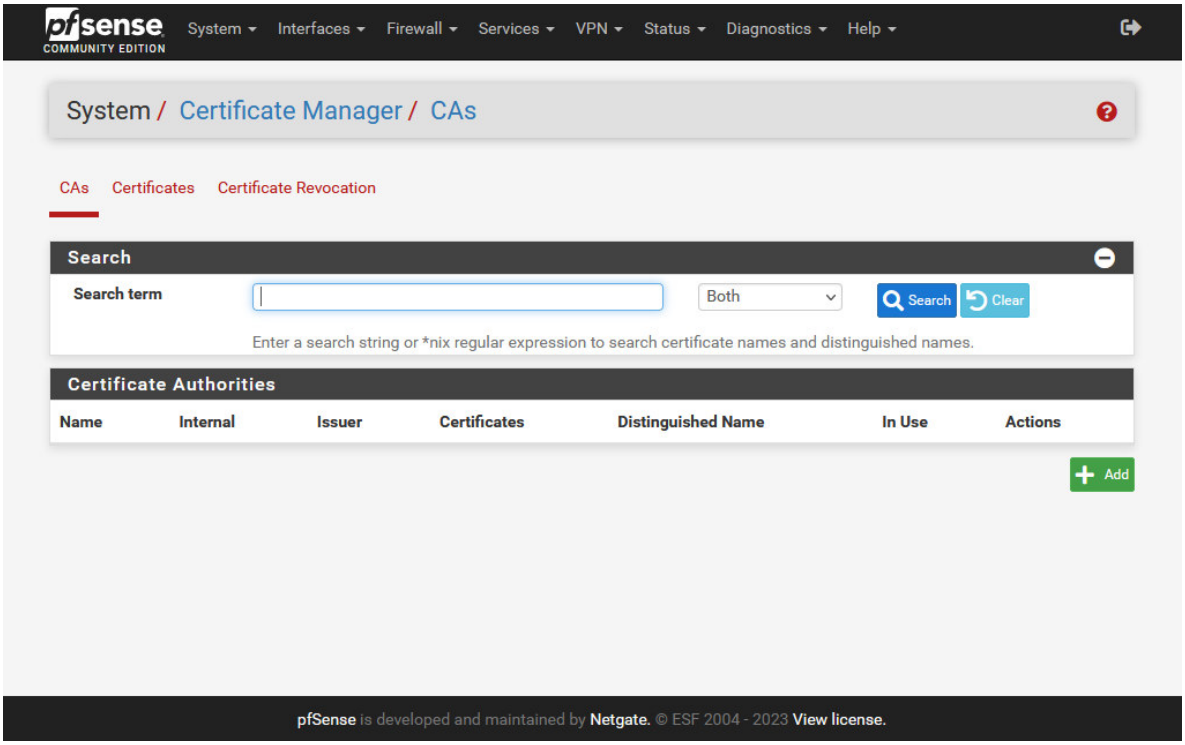
*Contenido del archivo de ubicación más cercana*




*Nota.* En la Figura 37 se muestra el contenido luego de haber abierto el archivo de Brasil, esta información luego debe ser ingresada en pfSense para lograr configurar la VPN.

**Figura 38**

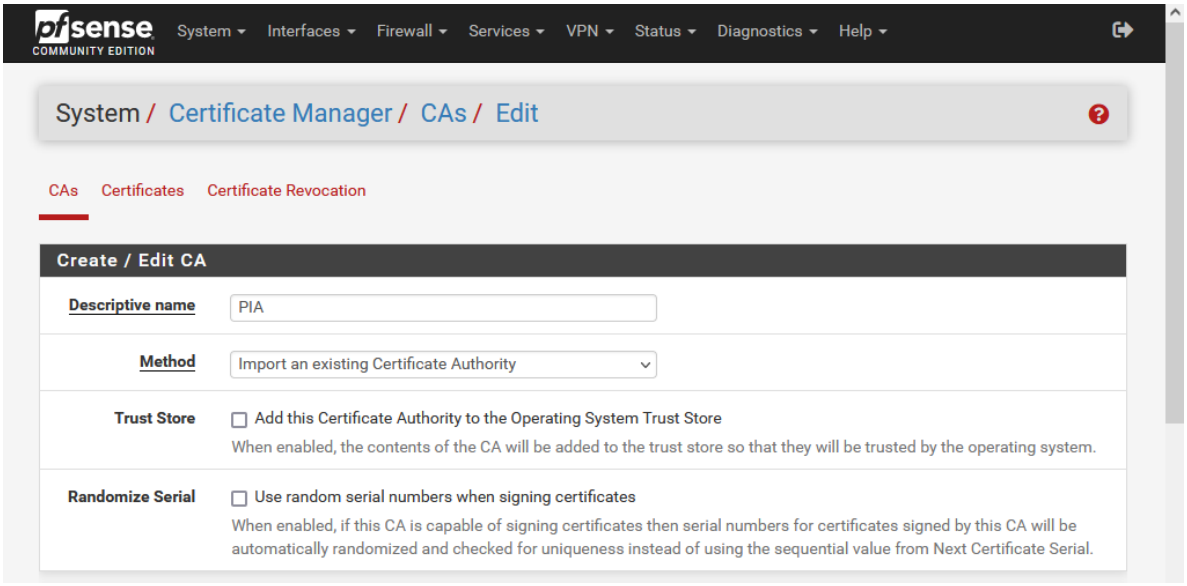
*Creación de "Certificate Authority (CA)" en pfSense*




*Nota.* En la Figura 38 se muestra el camino que se debe seguir para agregar la información del proveedor de servicios de VPN en pfSense. Al llegar a esta pestaña, se hace clic en "Add".

**Figura 39**

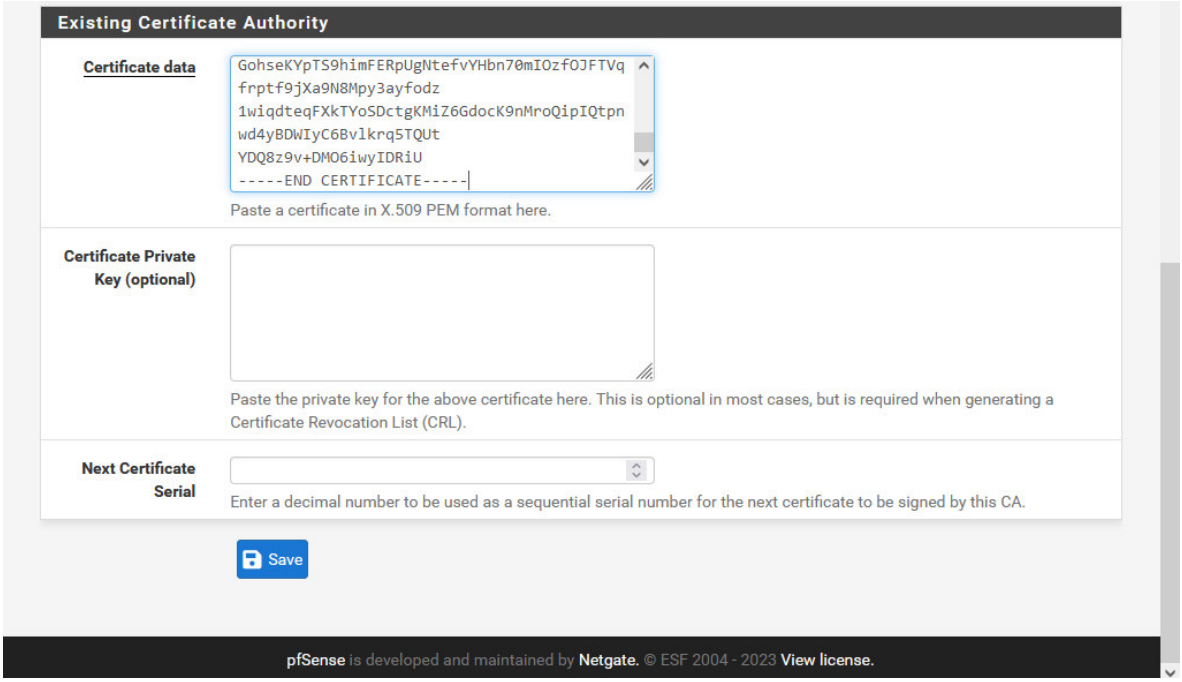
*Edición de información para creación de Autoridad Certificada*




*Nota.* En la Figura 39 se muestra la pestaña de configuración para editar y agregar la información necesaria para vincular Private Internet Access con pfSense. Primeramente, se le debe agregar un nombre descriptivo, en el caso del presente trabajo se ha colocado “PIA”, seguidamente se elige el método que permite importar una Autoridad Certificada existente.

**Figura 40**

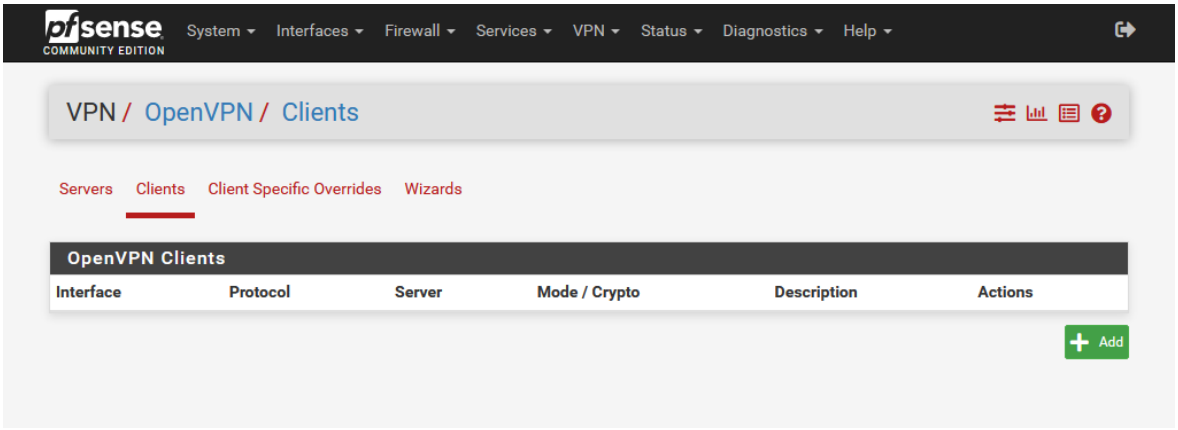
*Configuración de Autoridad Certificada en pfSense*




*Nota.* En la Figura 40 se muestra el llenado de la información para la Autoridad Certificada en pfSense, del archivo de la ubicación más cercana se debe copiar la parte que dice “Inicio de Certificado” hasta donde dice “Fin del Certificado” y se debe pegar en el campo que dice “Certificate data” en pfSense. Luego de esto, se hace clic en guardar.

**Figura 41**

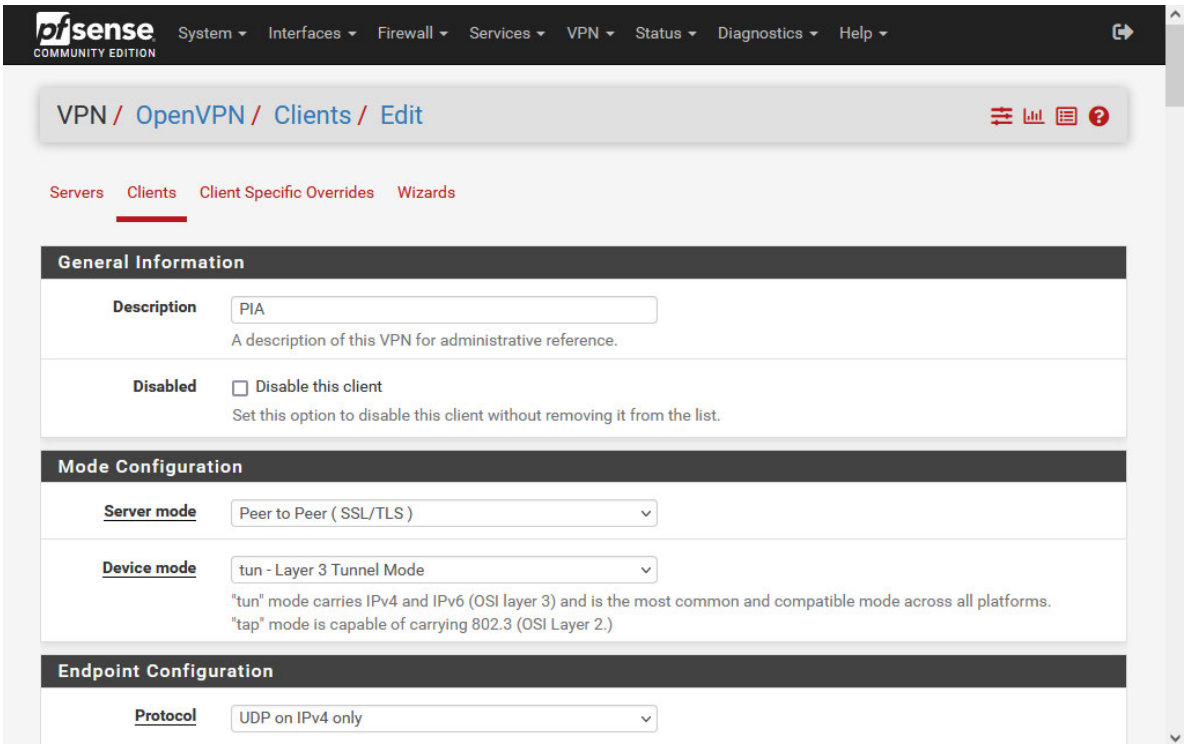
*Configuración de proveedor de servicios de VPN*




*Nota.* En la Figura 41 se muestra el camino que se debe seguir en la interface de pfSense para configurar el cliente de VPN. Al llegar a esta pestaña se debe hacer clic en “Add”.

**Figura 42**

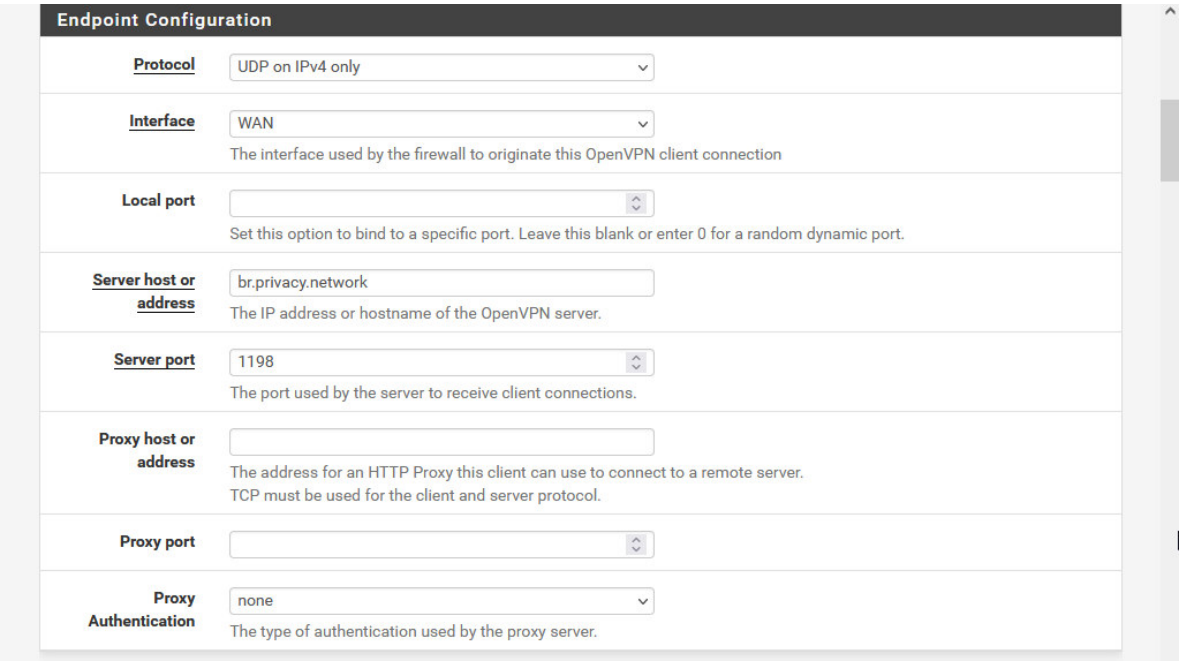
*Primeros campos para la creación de cliente de VPN*




*Nota.* En la Figura 42 se muestra el llenado de información necesaria para vincular la cuenta de Private Internet Access con pfSense. Primeramente, se coloca un nombre descriptivo (PIA), el modo del servidor, el modo del dispositivo y el protocolo.

**Figura 43**

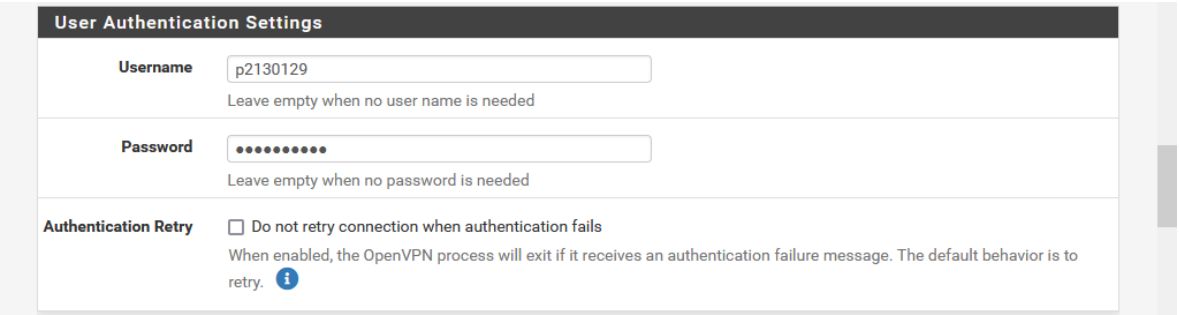
*Continuación de campos para la creación de cliente de VPN*




*Nota.* En la Figura 43 se muestra la continuación en cuanto a la creación del cliente de VPN donde se agrega la interface y el número de puerto (información que de igual manera aparece en el archivo de la ubicación más cercana).

**Figura 44**

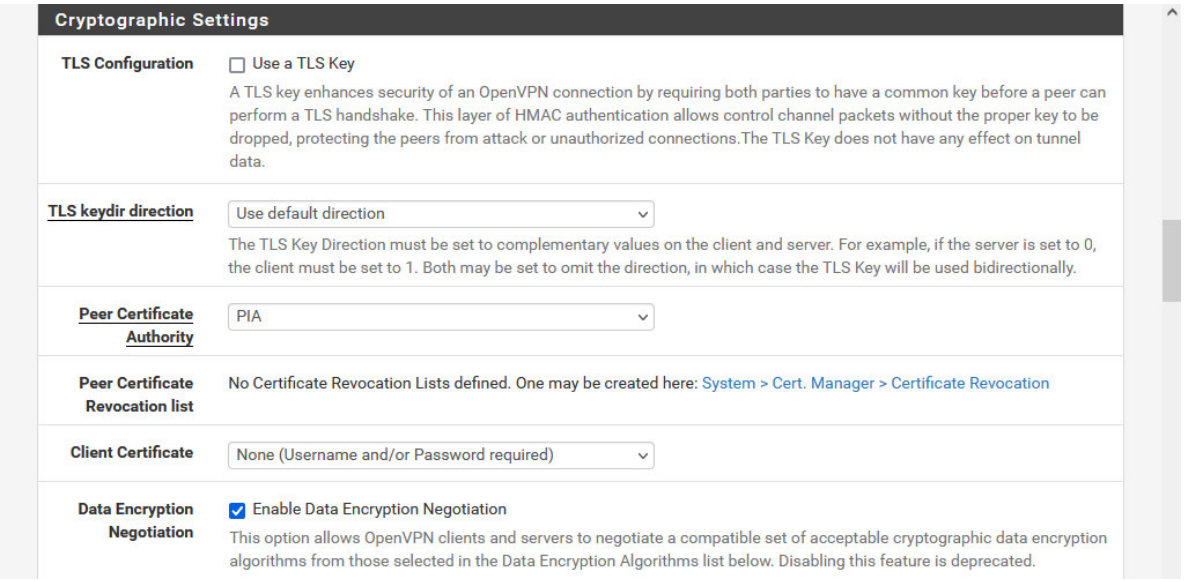
*Confirmación de credenciales para la creación de cliente de VPN*




*Nota.* En la Figura 44 se muestra la parte del llenado de la información para la creación de un cliente de VPN donde se debe ingresar el nombre de usuario y contraseña que provee Private Internet Access luego de la creación de una cuenta.

**Figura 45**

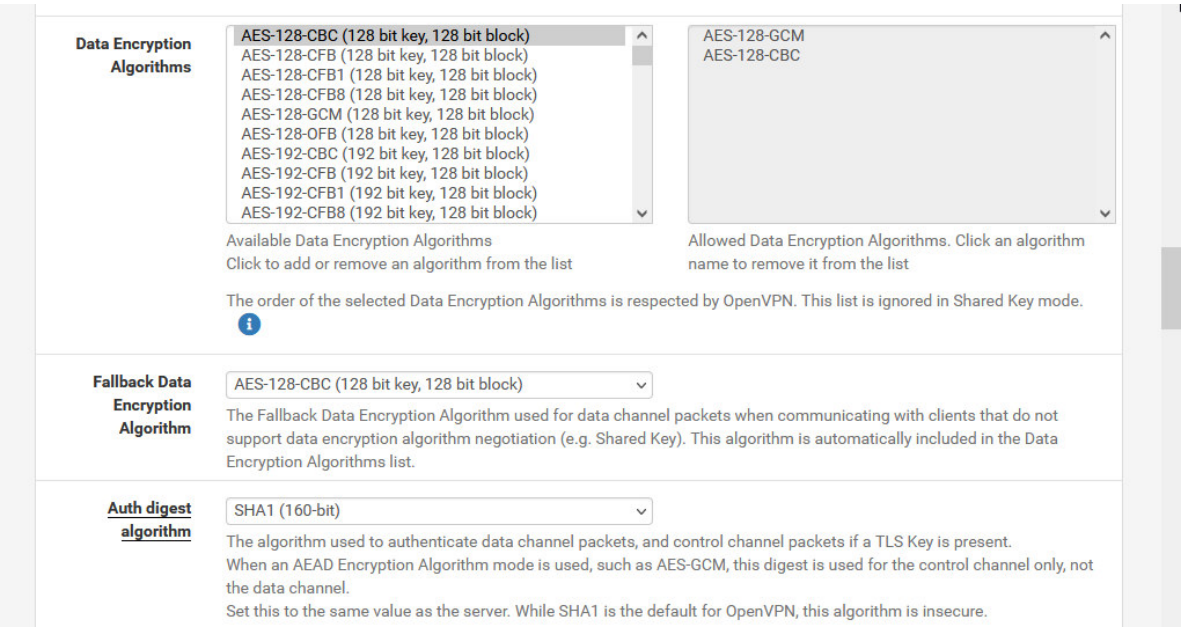
*Configuración de encriptado para la creación de cliente de VPN*




*Nota.* En la Figura 45 se muestra la parte del llenado de la información para la creación de un cliente de VPN donde se ingresa la Autoridad Certificada creada anteriormente (PIA).

**Figura 46**

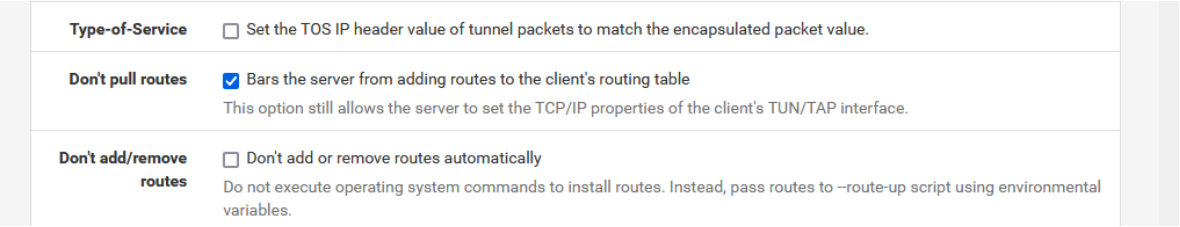
*Continuación de configuración de encriptado para la creación de cliente de VPN*




*Nota.* En la Figura 46 se muestran los algoritmos de cifrado de información elegidos, los cuales se encuentran de igual manera reflejados en el documento de la ubicación más cercana abierto anteriormente. Se escoge también un algoritmo de cifrado de datos alternativo y el algoritmo de resumen de autenticación.

**Figura 47**

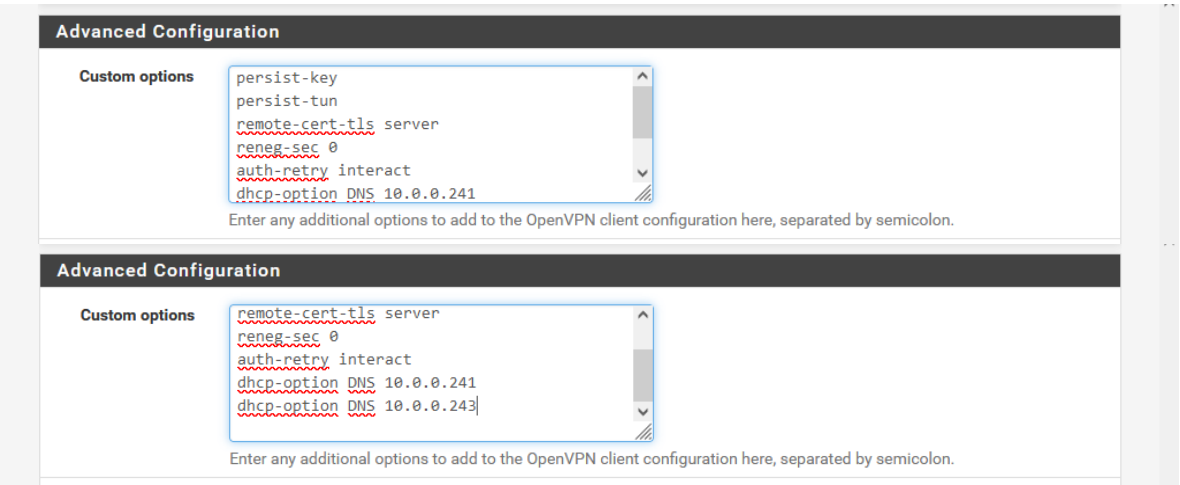
*Casilla de "Don't pull routes" para la creación de cliente de VPN*




*Nota.* En la Figura 47 se muestra la parte de la configuración para la creación de un cliente de VPN donde se marca la opción "Don't pull routes" que impide que el servidor agregue rutas a la tabla de enrutamiento del cliente.

**Figura 48**

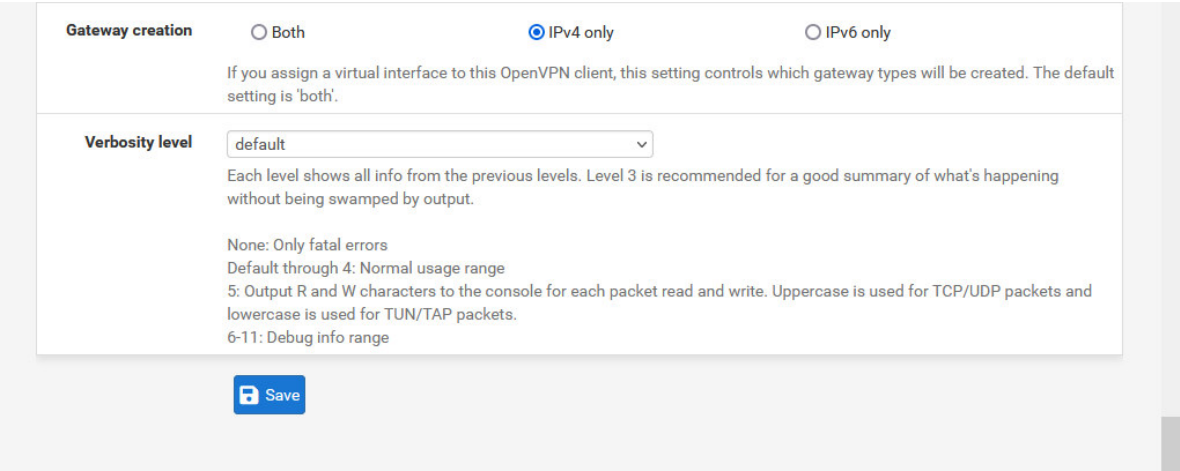
*Opciones personalizadas para la creación de cliente de VPN*




*Nota.* La Figura 48 es una comparación de dos imágenes que permiten ver la totalidad de las opciones personalizadas que se han agregado a la configuración para la creación de un cliente de VPN.

**Figura 49**

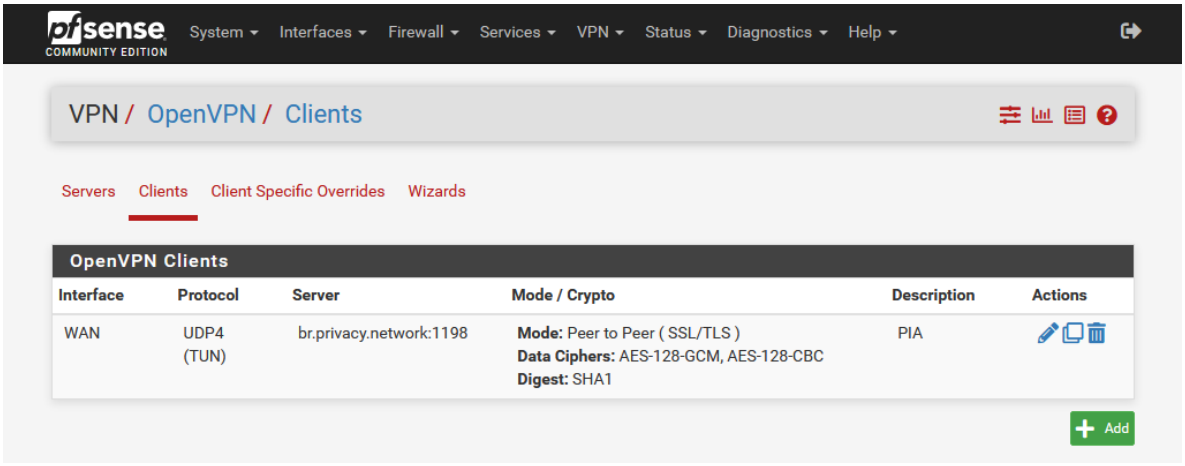
*Creación de Gateway para la creación de cliente de VPN*




*Nota.* En la Figura 49 se muestra la última parte de la configuración para la creación de un cliente de VPN, se debe marcar la creación del Gateway y se hace clic en guardar y se confirma para aplicar los cambios.

**Figura 50**

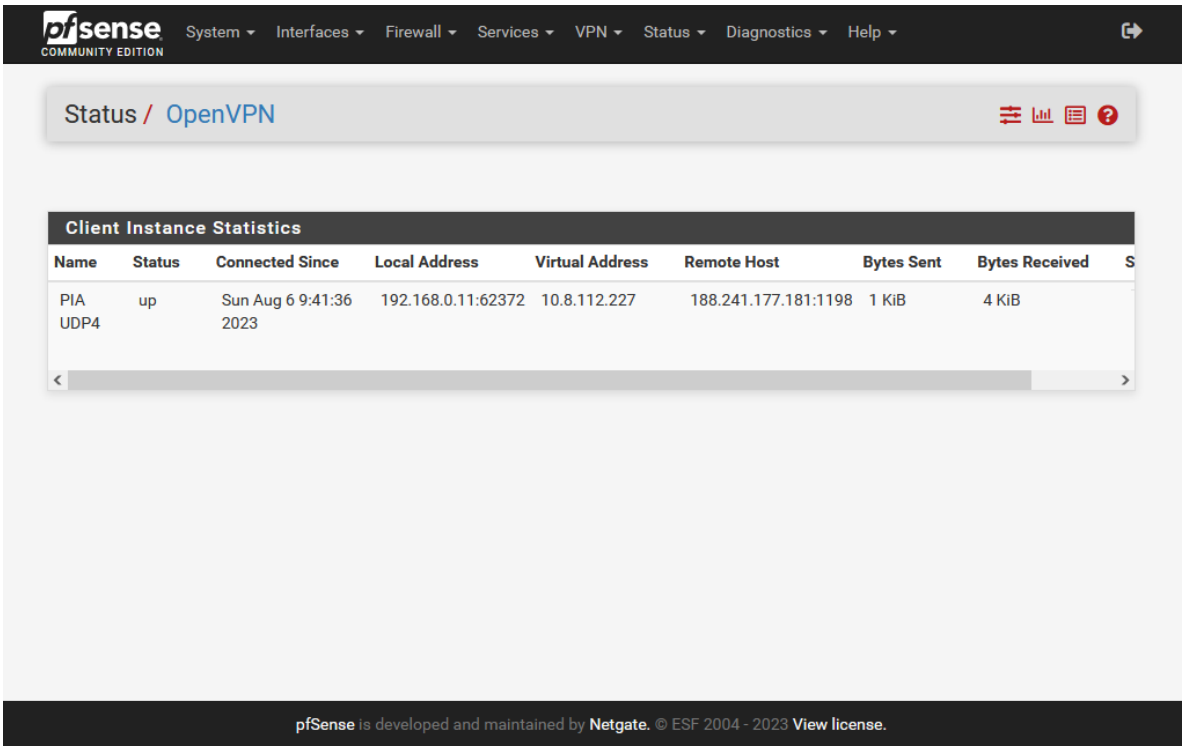
*Finalización de creación de un cliente de VPN*




*Nota.* En la Figura 50 se muestra la finalización de la creación del cliente de VPN.

**Figura 51**

*Confirmación del estado de la VPN*

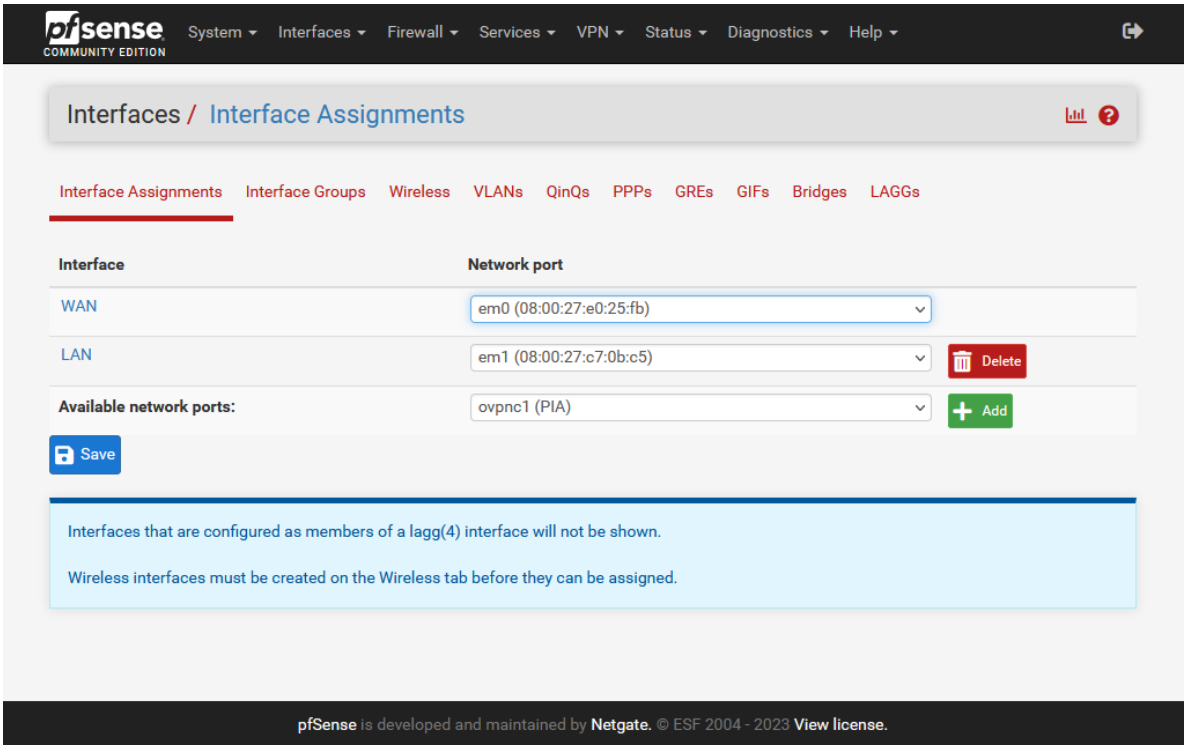



*Nota.* En la Figura 51 se muestra la manera para confirmar que la configuración de la VPN ha sido completada de la manera correcta, al ingresar en la pestaña de “Status” y “OpenVPN” se puede ver que en la columna de “Status” dice “up” indicando que está en funcionamiento, se muestra la

dirección IP de la red WAN y la del host remoto que es la que se mostrará al acceder a internet haciendo uso de la VPN.

**Figura 52**

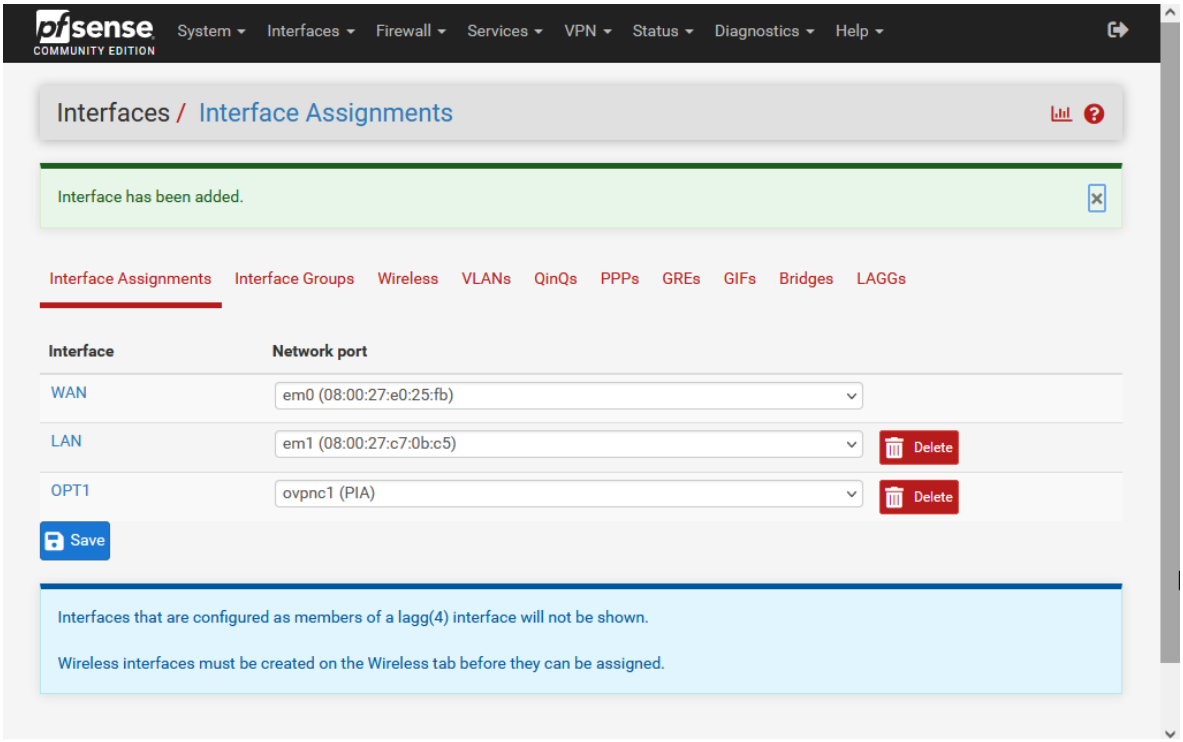
*Adición de interface PIA*




*Nota.* En la Figura 52 se muestra la asignación de interfaces desde donde se puede agregar la interface creada con la VPN. Se hace clic en “Add”.

**Figura 53**

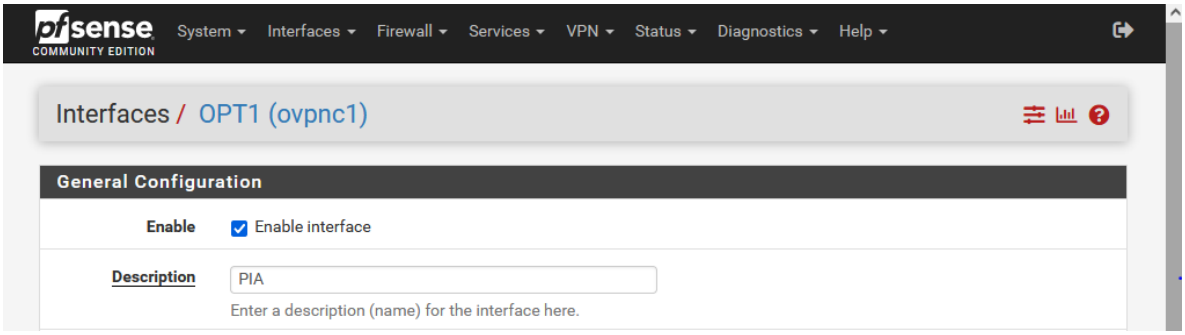
*Adición de interface PIA en tabla de intefaces de la red*




*Nota.* En la Figura 53 se muestra que luego de hacer clic en “Add”, se agrega PIA como nueva interface lo que permitirá ver su información en el dashboard. Es necesario hacer configuraciones para cambiar el nombre de la Interface y para habilitarla.

**Figura 54**

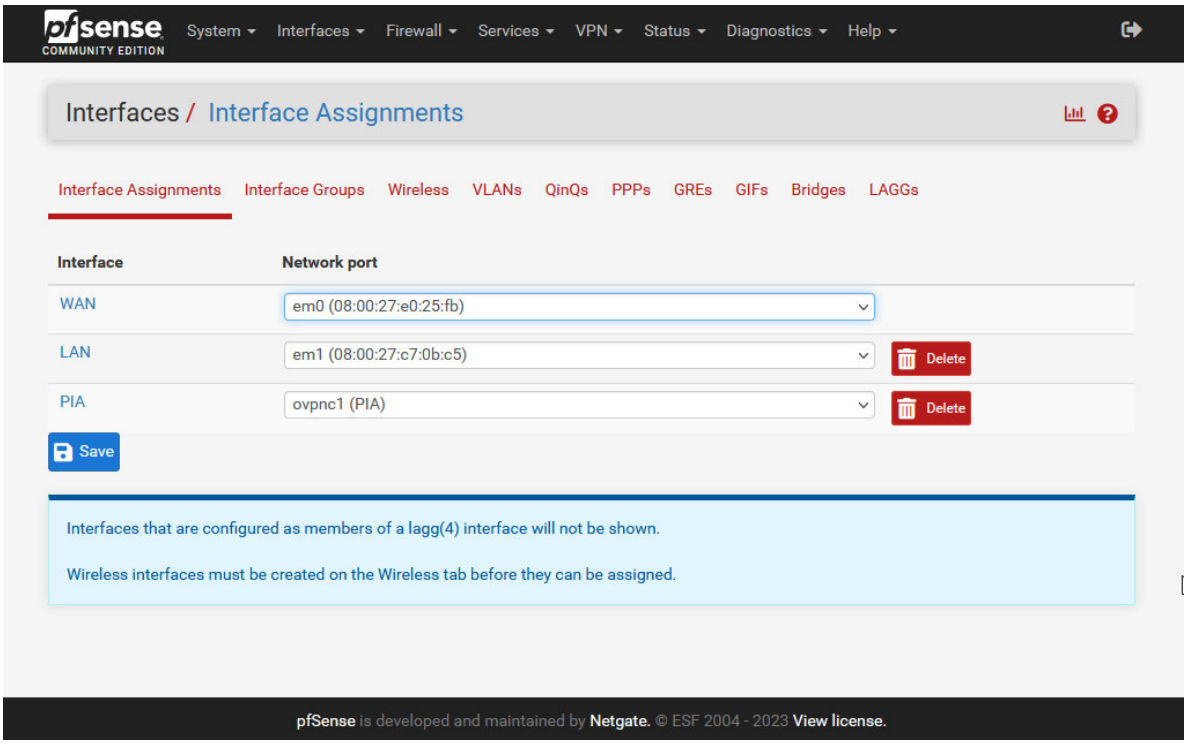
*Activación de interface PIA*




*Nota.* En la Figura 54 se muestra que luego de hacer clic sobre la interface PIA se abre la pestaña de configuración donde se debe marcar la casilla para habilitar la interface y se debe llenar el campo para asignarle un nombre descriptivo (PIA). Se debe hacer clic en guardar y se aplican los cambios.

**Figura 55**

*Finalización de configuración de interface PIA*



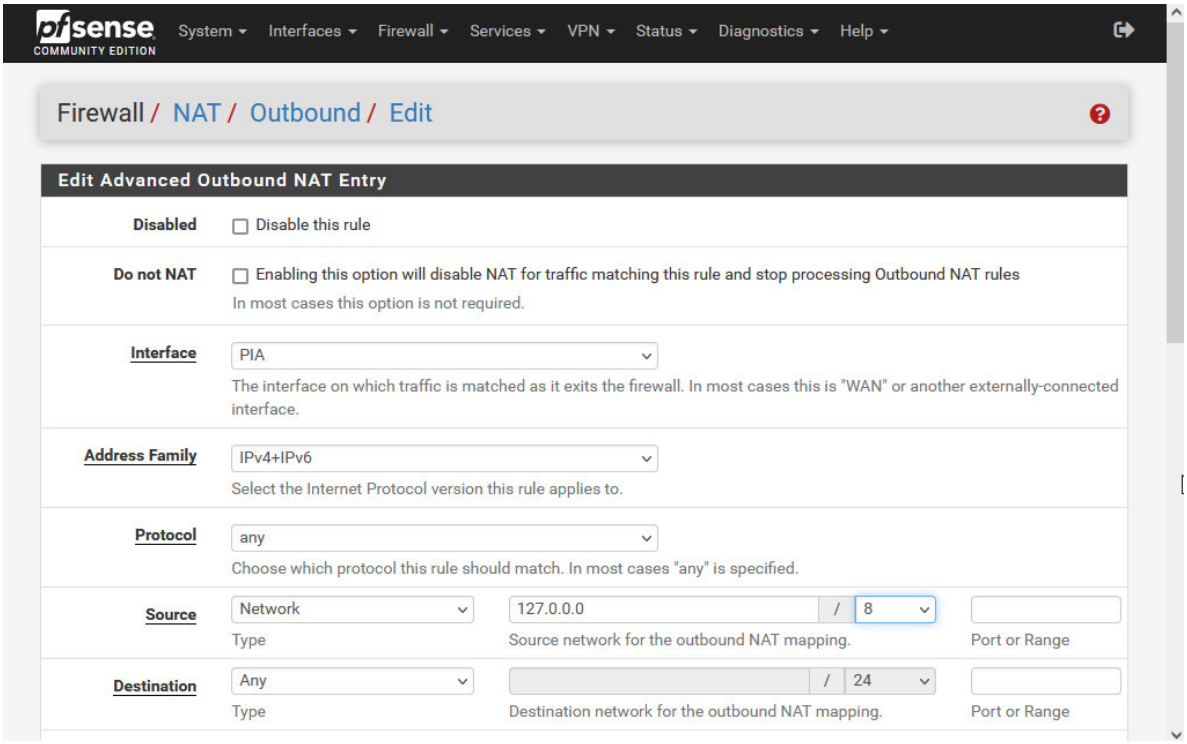

*Nota.* En la Figura 55 se muestra la finalización de la configuración de la interface PIA, se visualiza el cambio de nombre de interface efectuado y ya está habilitada.

### 3.3.6. NAT (Network Address Translation)

NAT es un proceso a través del cual se efectúa la traducción de una o más direcciones IP locales en una o más direcciones IP globales y viceversa, este proceso se realiza con la finalidad de permitir la conexión a internet del host local ya que para acceder a internet es necesaria una dirección IP pública. NAT normalmente opera en un enrutador o firewall (Srisuresh y Egevang, 2001).

**Figura 56**

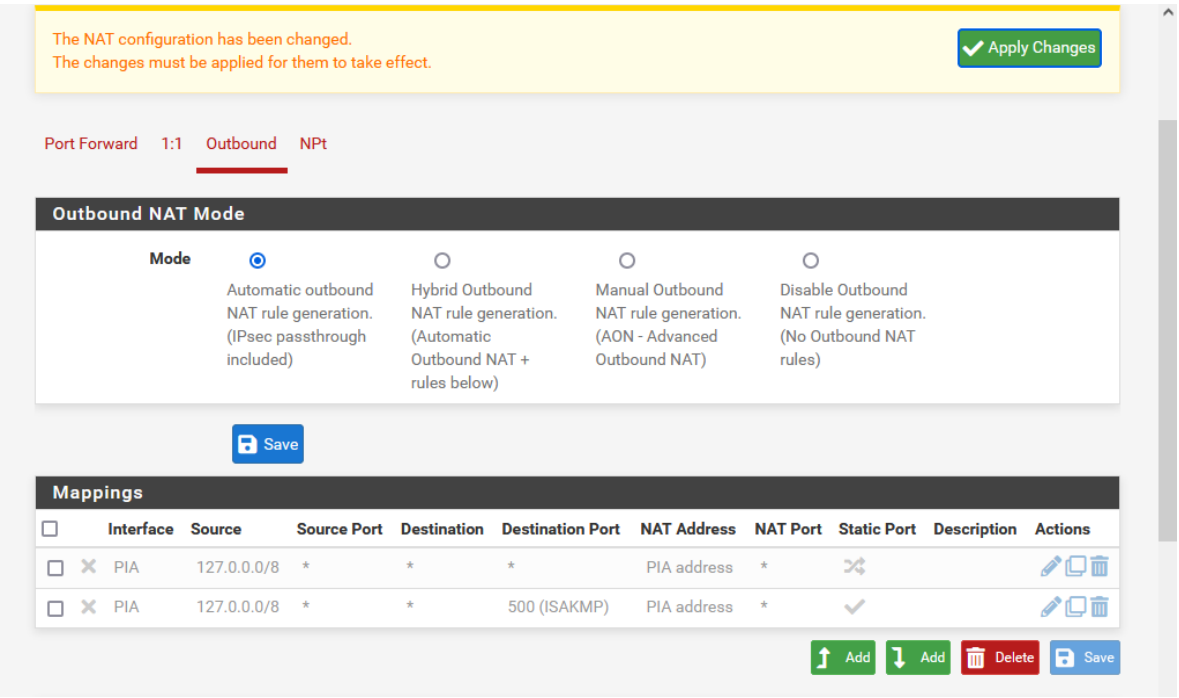
*Campos que deben llenarse para la primera regla de la configuración de NAT*




*Nota.* En la Figura 56 se muestra el camino para configurar NAT en el firewall de pfSense, inicialmente, se debe escoger la interface de la red que se desea utilizar (PIA), luego se escribe la fuente, en este caso se colocó la dirección de una red de un host local (127.0.0.0/8). Luego se hace clic en “Guardar”.

**Figura 57**

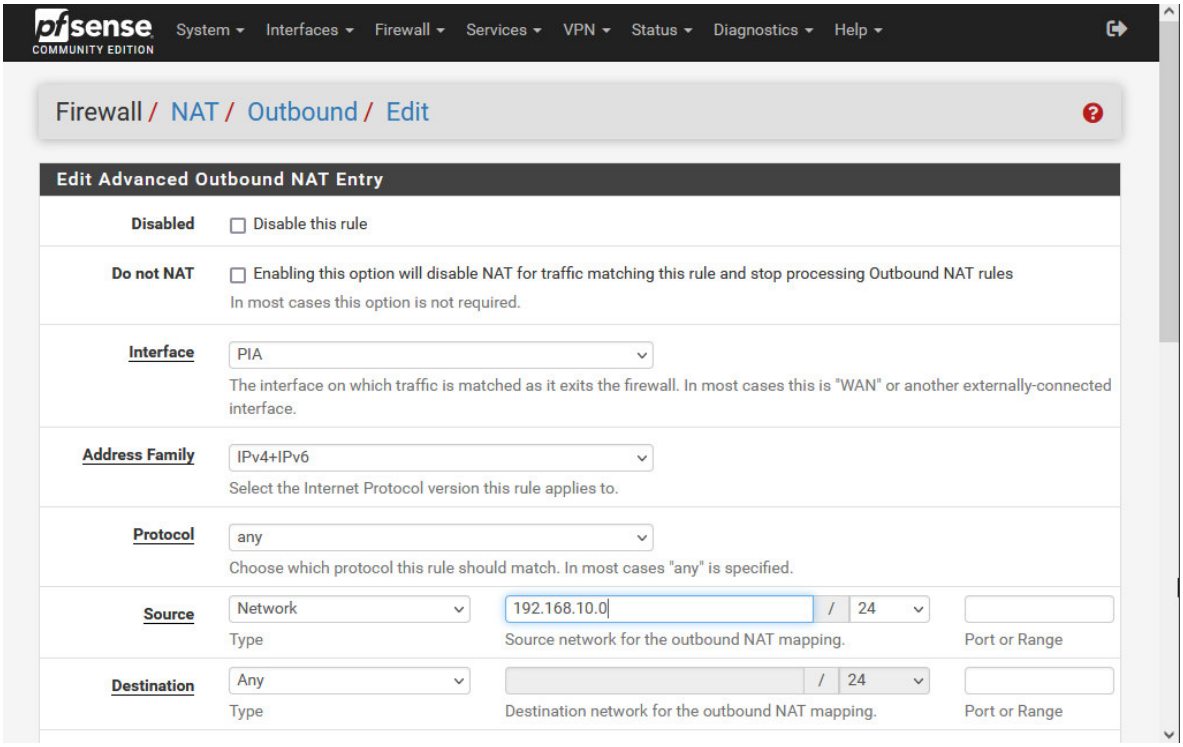
*Configuración de NAT*




*Nota.* En la Figura 57 se muestra la confirmación de NAT, se duplica la regla anterior y se agrega el puerto 500 como puerto de destino, este puerto es para tráfico de ISAKMP (Protocolo de administración de claves y asociación de seguridad de Internet).

**Figura 58**

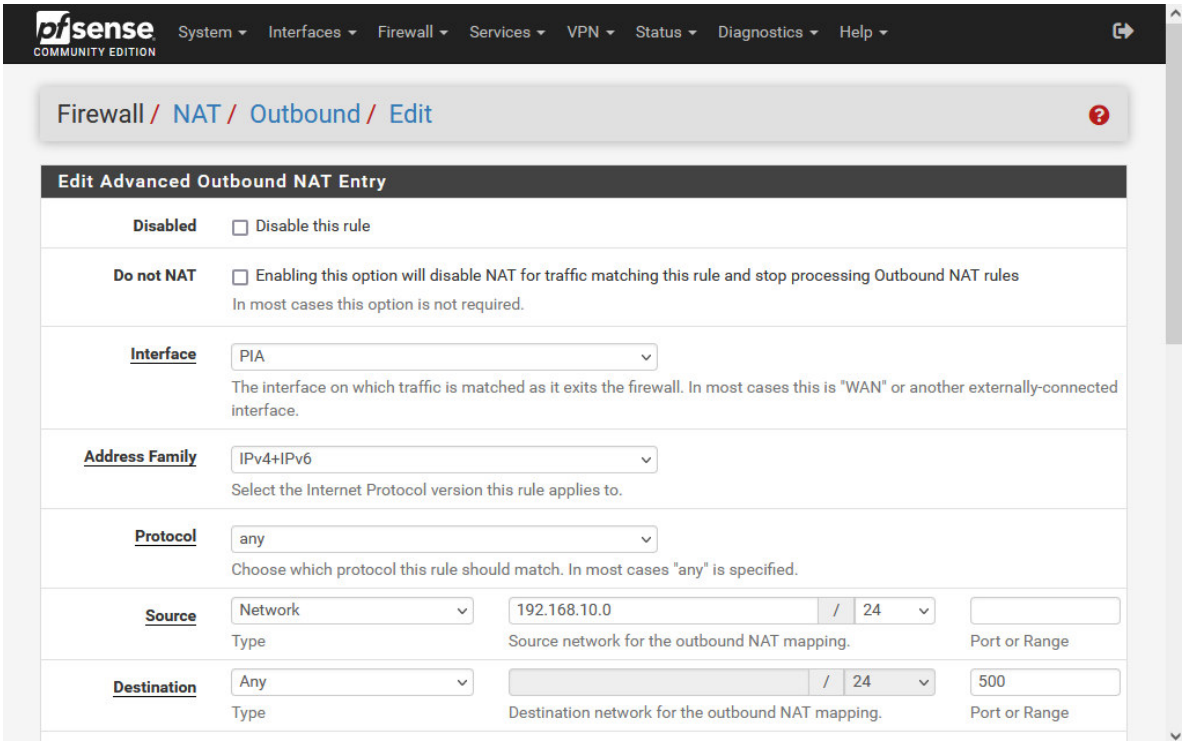
*Tercera regla para la configuración de NAT*




*Nota.* En la Figura 58 se muestra la configuración de la tercera regla de NAT, se coloca la dirección de la red fuente 192.168.10.0/24 y se hace clic en “Guardar”.

**Figura 59**

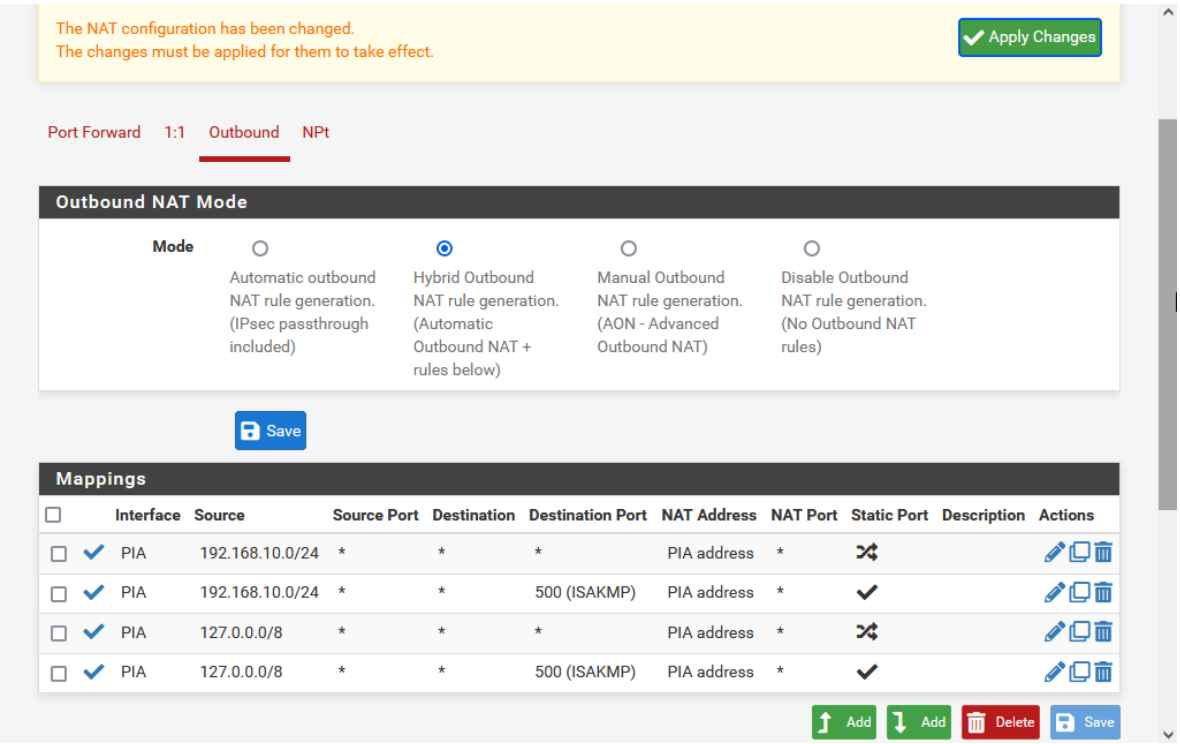
*Cuarta regla para la configuración de NAT*




*Nota.* En la Figura 59 se muestra la configuración de la cuarta regla para NAT, se duplica la regla anterior y se agrega el número de puerto en el destino (500).

**Figura 60**

*Finalización de la configuración de NAT*

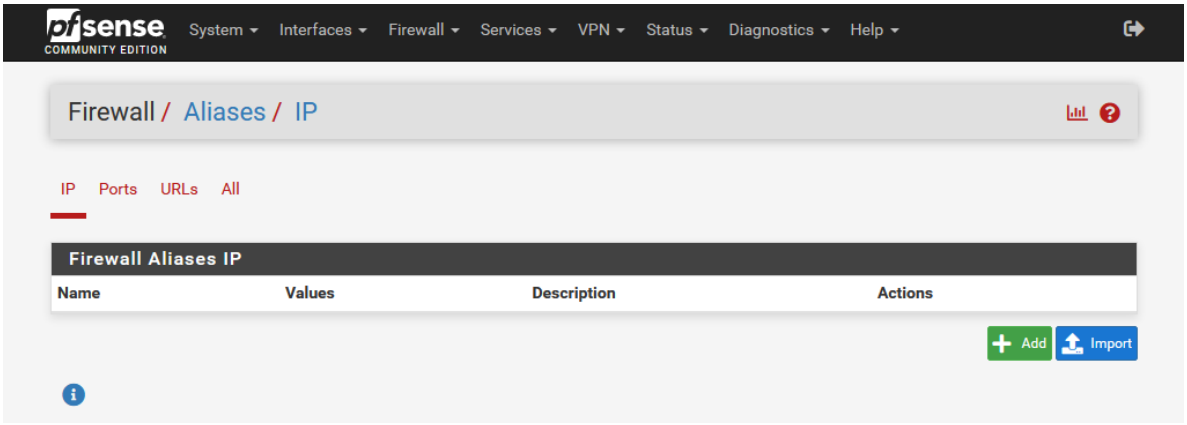



*Nota.* En la Figura 60 se muestra la tabla de Mappings con las cuatro reglas configuradas, se debe cambiar el modo de NAT a “Generación de reglas de NAT de salida hibrida” para que se puedan aplicar las reglas configuradas. Se hace clic en “Guardar”.

### 3.3.7. Reglas del Firewall

**Figura 61**

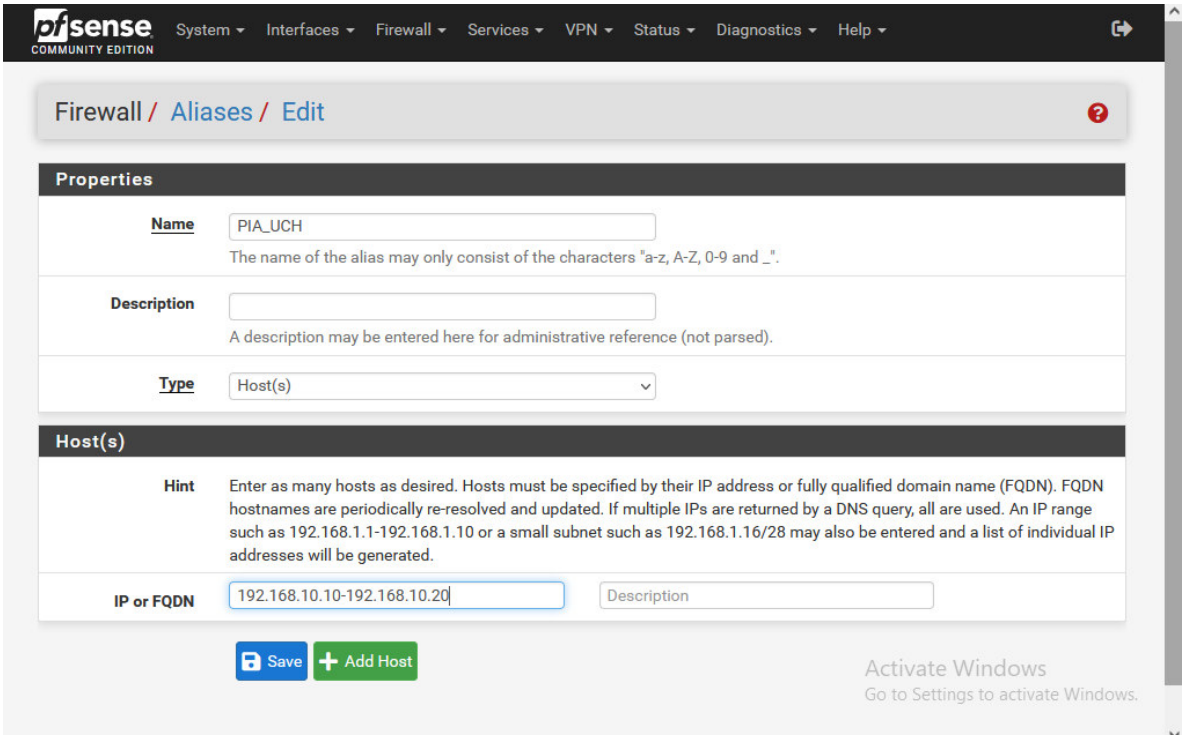
*Creación de un alias*




*Nota.* En la Figura 61 se muestra el inicio de la creación de un ailias, un alias es un grupo de direcciones IP al que se le da un nombre que luego permite referenciarlo en otras partes de la configuración. Se hace clic en “Add”.

**Figura 62**

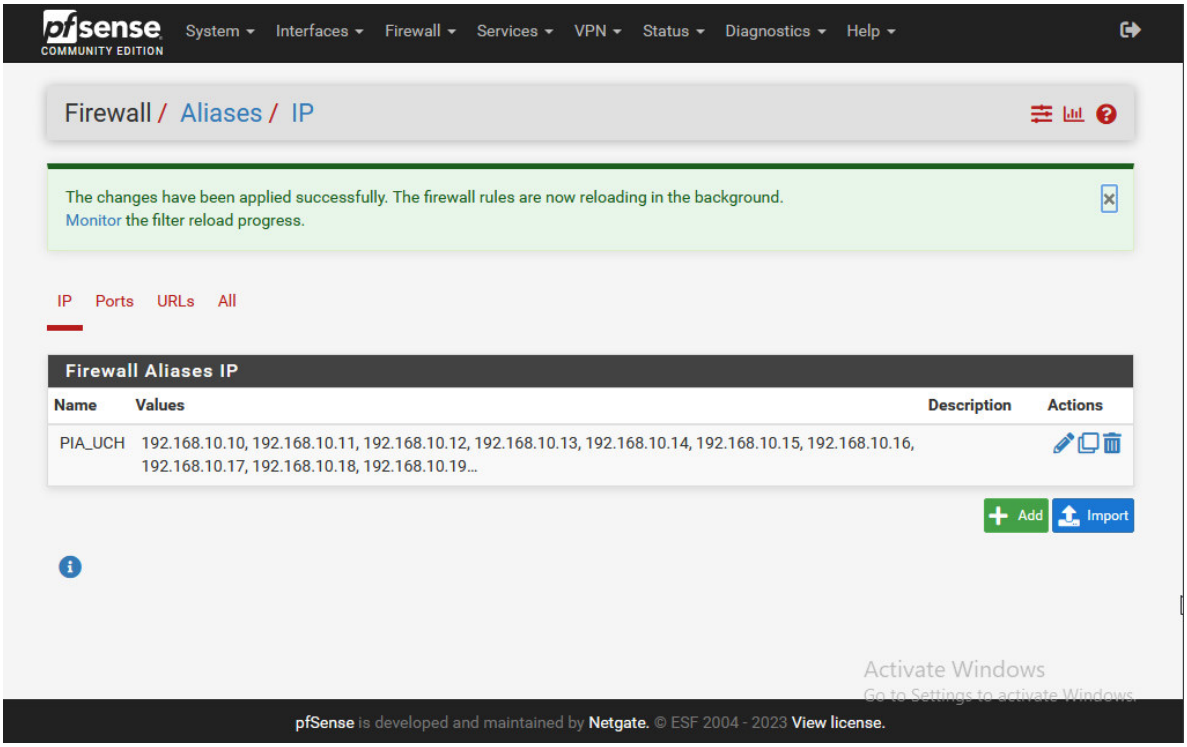
*Llenado de campos para la creación de un alias*




*Nota.* En la Figura 62 se muestran los campos que deben llenarse para la creación de un alias, se le coloca un nombre al grupo (PIA_UCH) y se coloca el rango de las direcciones IP que se desea colocar bajo este nombre (192.168.10.10-192.168.10.20). Se hace clic en “Guardar”.

**Figura 63**

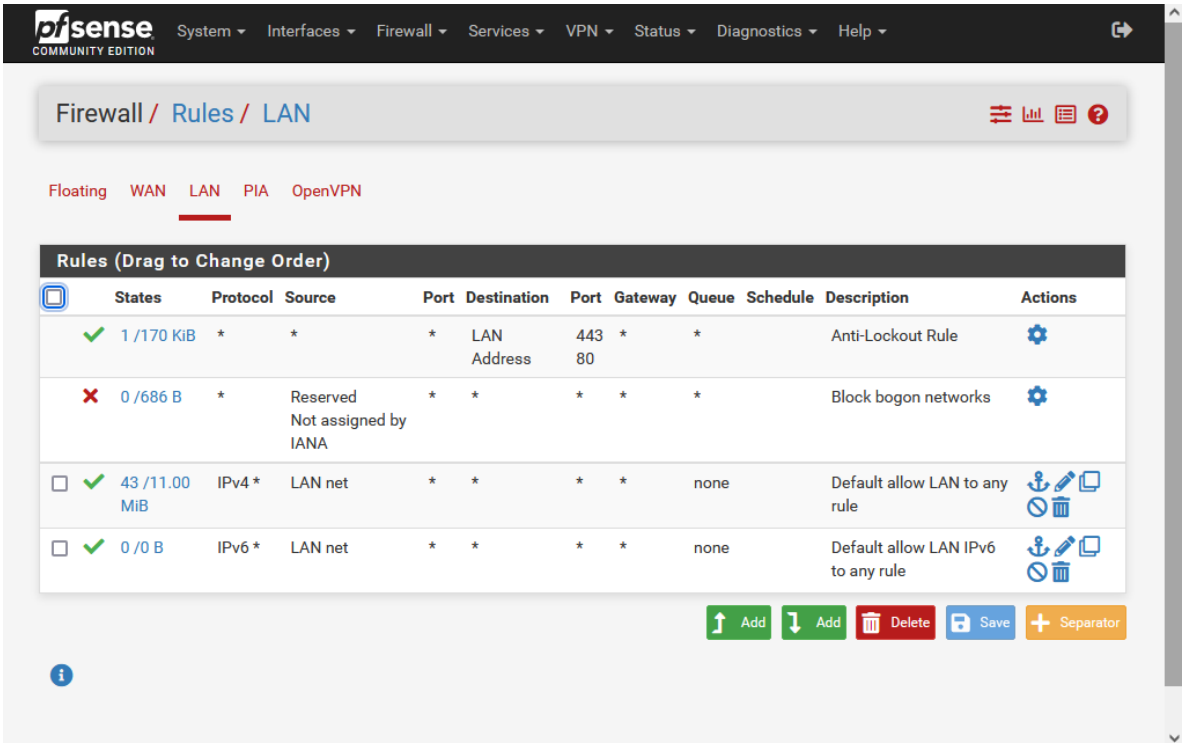
*Creación de alias realizado de manera exitosa*




*Nota.* En la Figura 63 se muestra la creación de manera exitosa de un grupo de direcciones IP bajo el alias “PIA_UCH”.

**Figura 64**

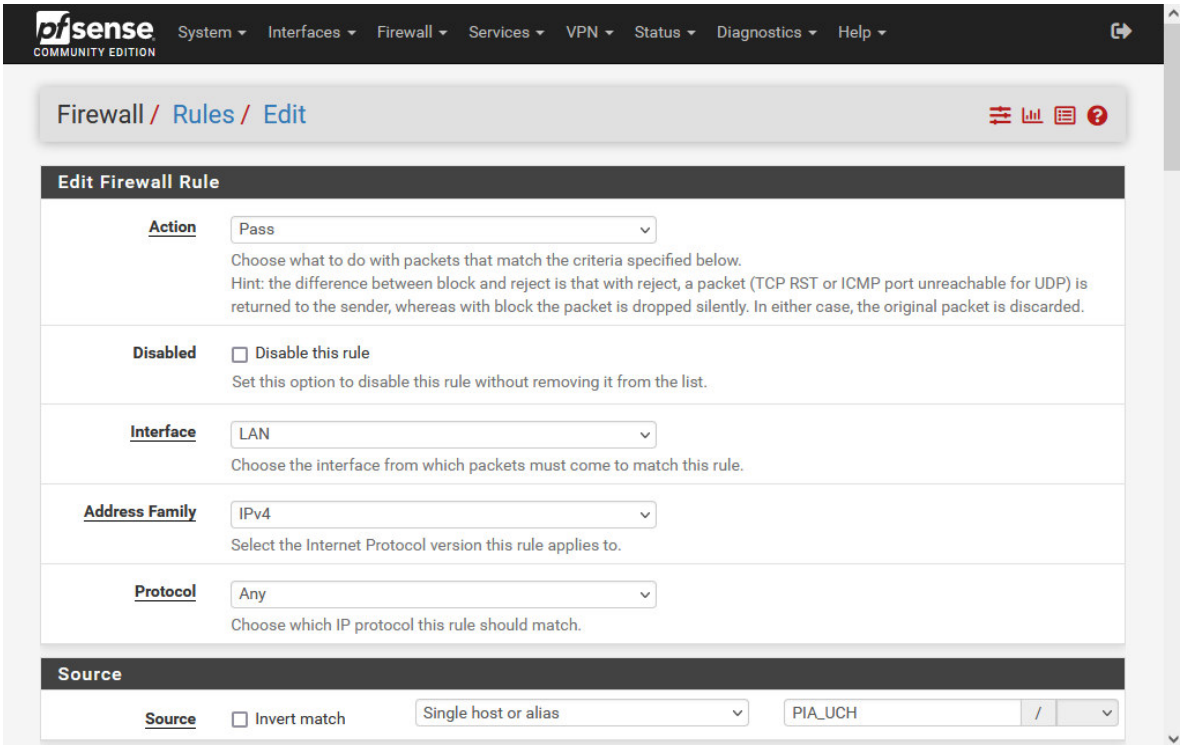
*Inicio de configuración de Firewall*




*Nota.* En la Figura 64 se muestra el camino para configurar las reglas del Firewall en la LAN.

**Figura 65**

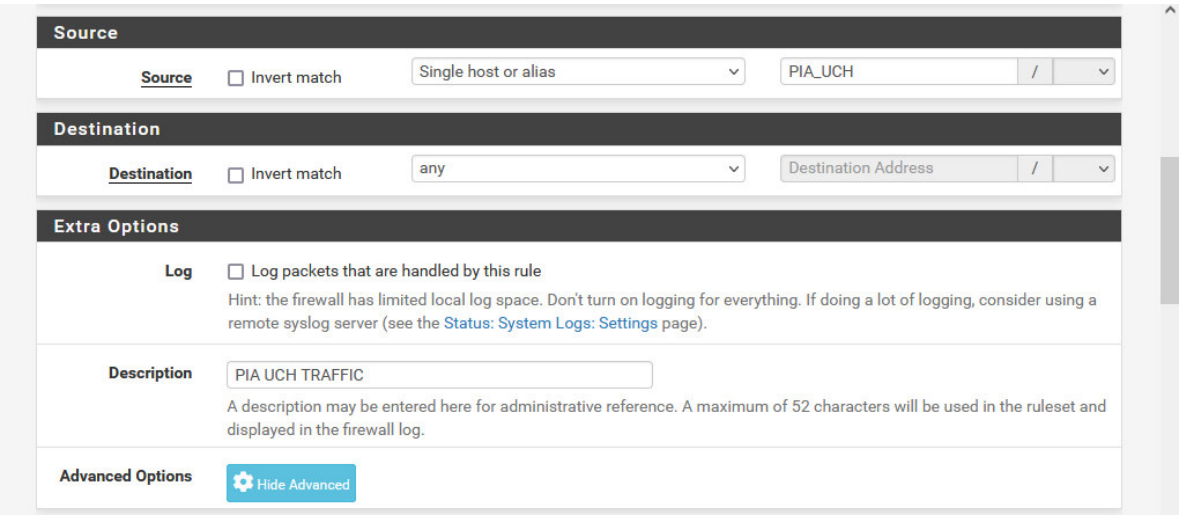
*Primeros campos para la edición de las reglas de Firewall*




*Nota.* En la Figura 65 se muestra la primera parte de los campos que se deben llenar para la configuración de las reglas del Firewall, se escoge la interface (LAN) y el protocolo (Any) para que pueda pasar todo tipo de tráfico de la red.

**Figura 66**

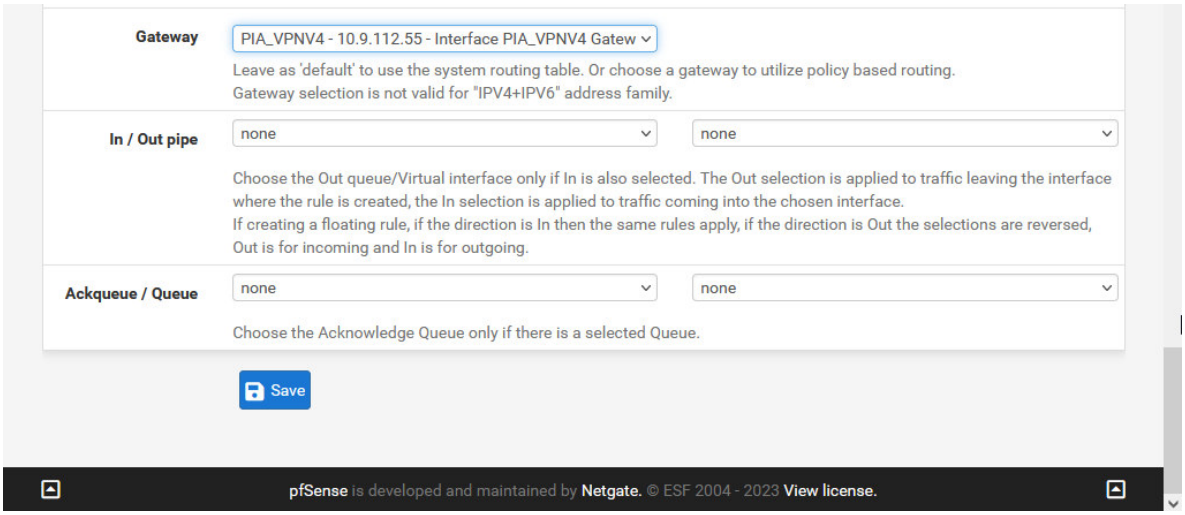
*Llenado de siguientes campos de edición de las reglas de Firewall*




*Nota.* En la Figura 66 se muestra la continuación de la configuración de las reglas del Firewall, en “Source” debe colocarse “single host or alias” para poder referenciar el alias que se había creado anteriormente (PIA_UCH). Se coloca una descripción indicando que ese será el tráfico que recibirán las direcciones IP que formen parte del grupo que está bajo el alias “PIA_UCH”.

**Figura 67**

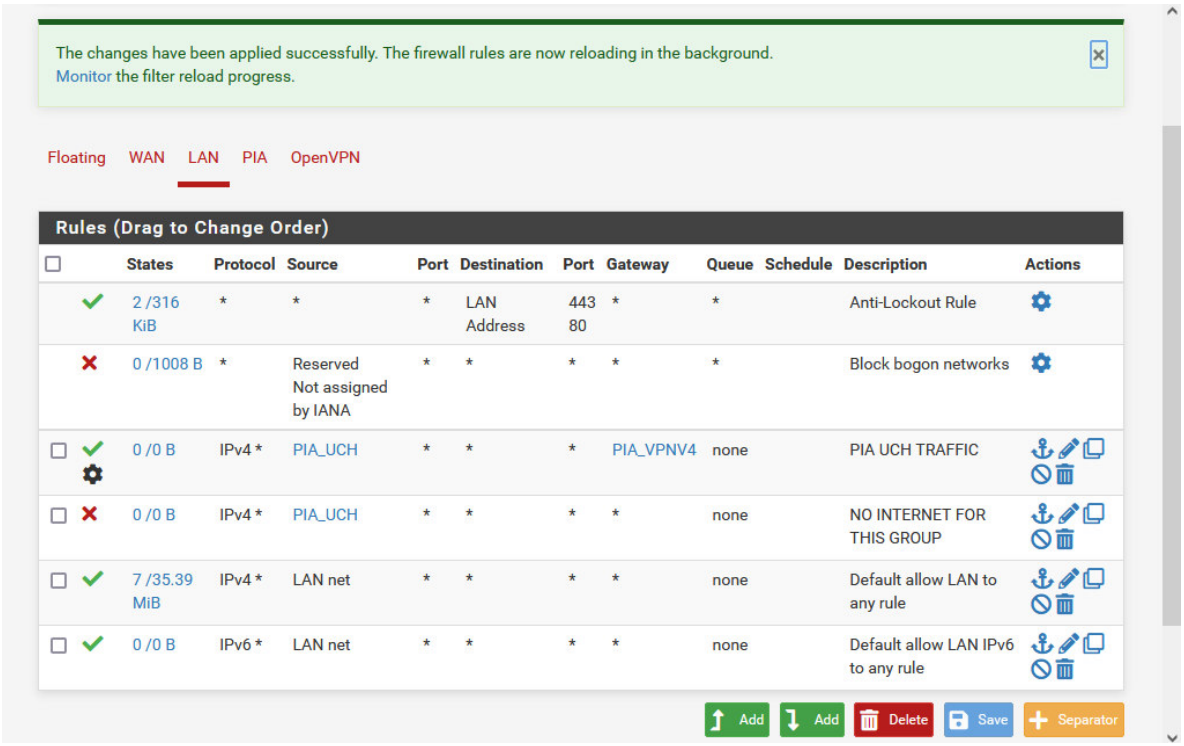
*Últimos campos de edición de las reglas de Firewall*




*Nota.* En la Figura 67 se muestra el llenado del resto de los campos para las reglas del Firewall. Se hace clic en “Guardar”.

**Figura 68**

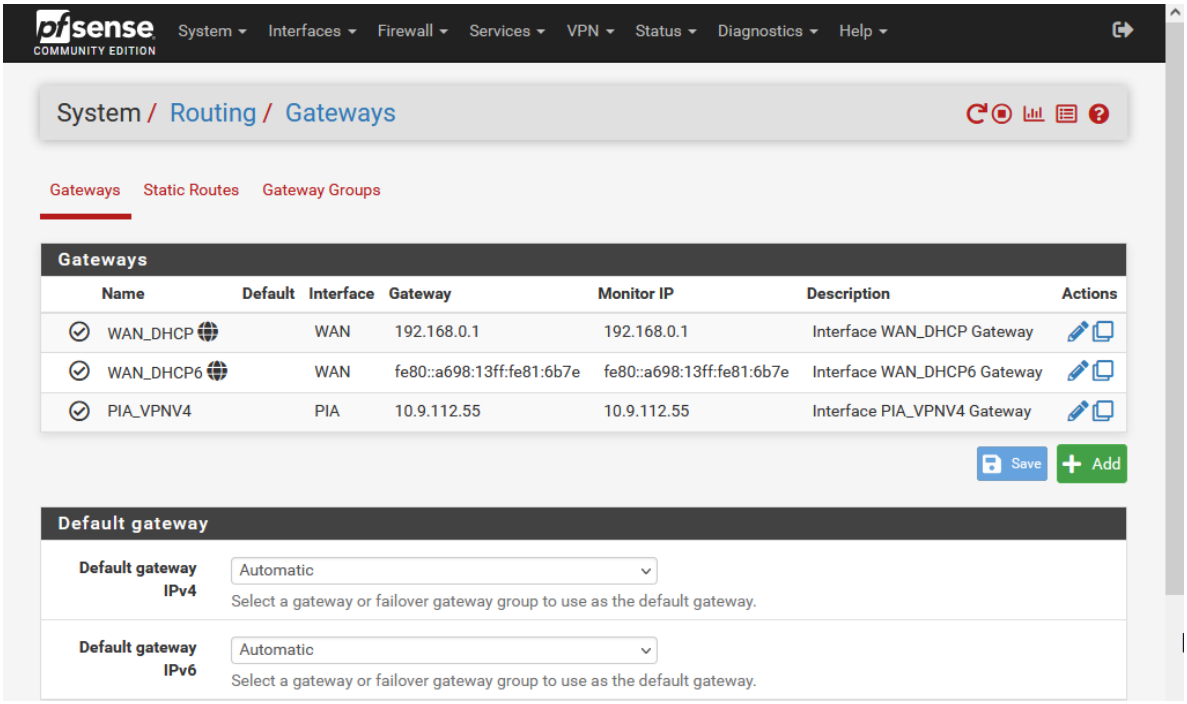
*Configuración de reglas de firewall guardada*




*Nota.* En la Figura 68 se muestra la tabla de reglas con dos nuevas reglas creadas para restringir el tráfico del grupo PIA_UCH.

**Figura 69**

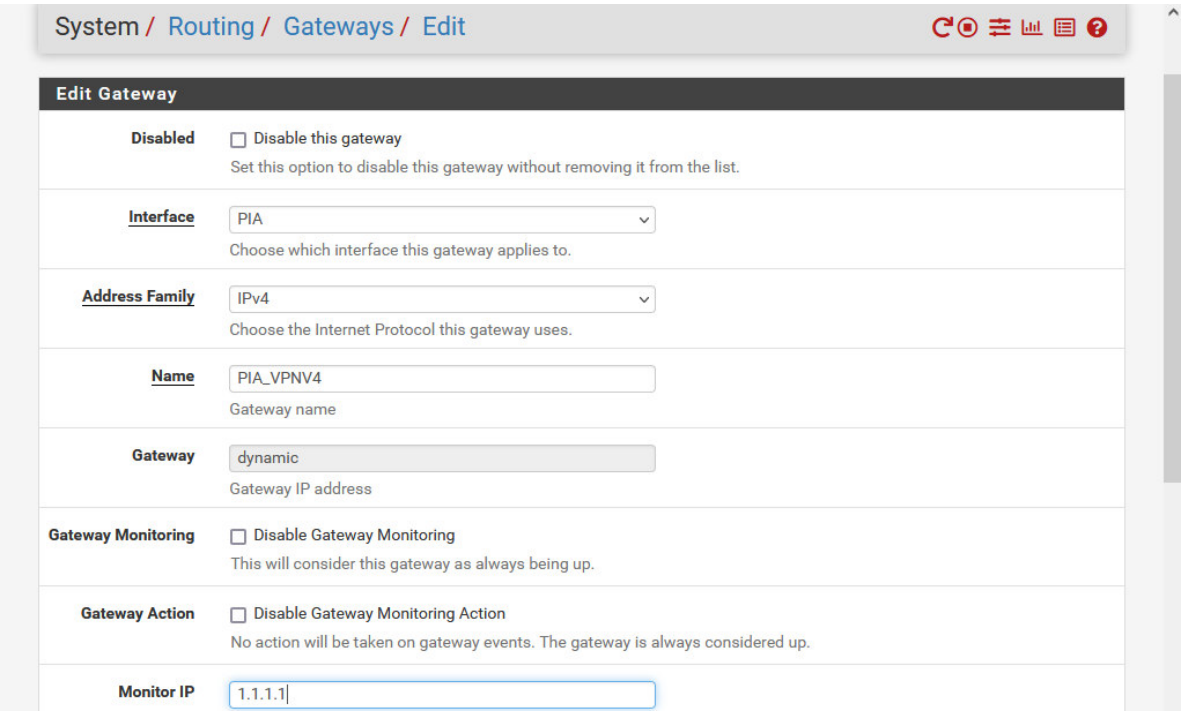
*Configuración de Gateway*




*Nota.* En la Figura 69 se muestra la configuración del Gateway PIA_VPNV4. Se hace clic en el “lápiz” para editar.

**Figura 70**

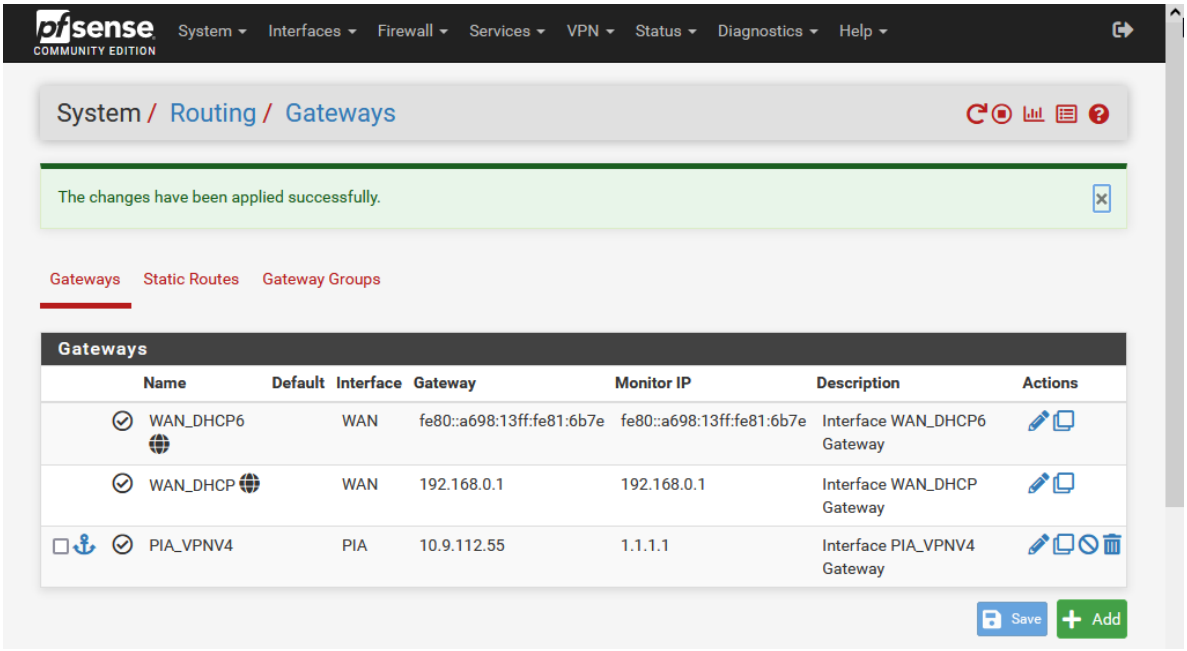
*Edición de la configuración de Gateway*




*Nota.* En la Figura 70 se muestra la edición de la configuración de Gateway donde se agrega una dirección IP de monitoreo (1.1.1.1), la cual es la dirección de Cloudflare.

**Figura 71**

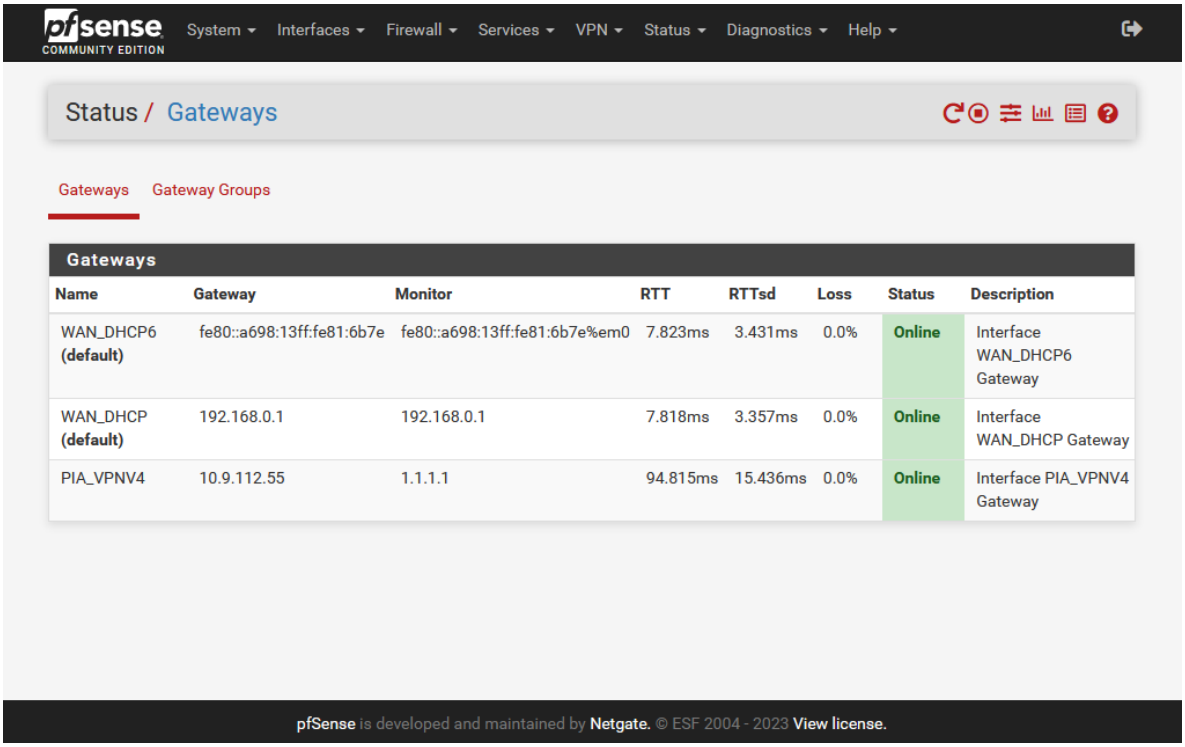
*Edición de configuración Gateway guardada*




*Nota.* En la Figura 71 se muestra la confirmación de que la configuración realizada en el Gateway ha sido guardada.

**Figura 72**

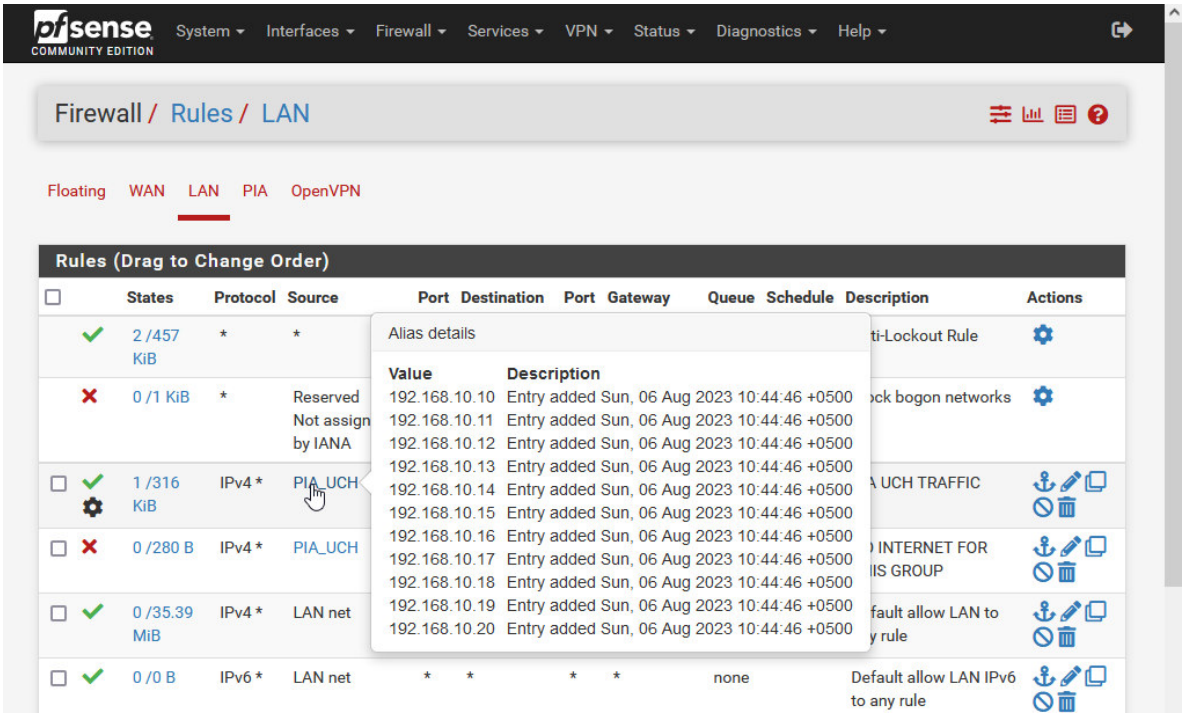
*Estado del Gateway modificado*




*Nota.* En la Figura 72 se muestra la confirmación de que la modificación en el Gateway se ha hecho correctamente, me muestra el estado “Online” y un 0.0% de perdida de paquetes.

**Figura 73**

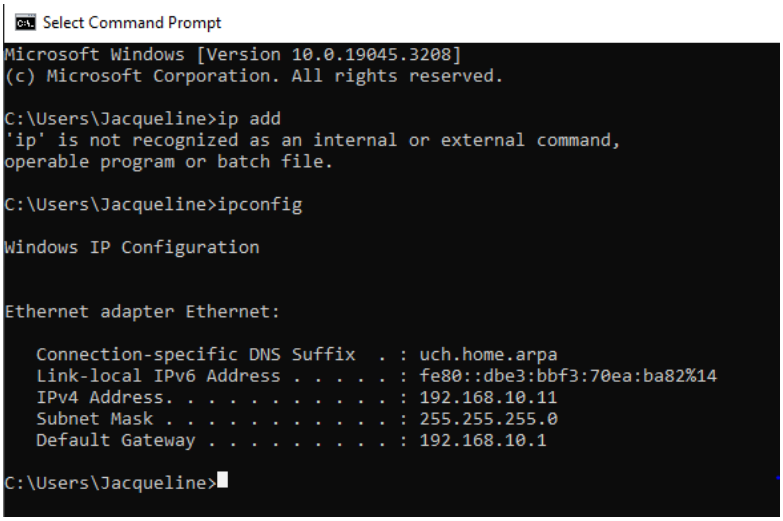
*Verificación de que el tráfico de la red está siendo a través de la VPN con las direcciones IP*




*Nota.* En la Figura 73 se muestra nuevamente la tabla de reglas creadas para el Firewall en la red LAN, se puede ver que en el grupo de direcciones IP bajo el alias de PIA_UCH se encuentra la dirección IP 192.168.10.11, la cual es la direcciones IP de la máquina virtual donde se están haciendo la configuración.

**Figura 74**

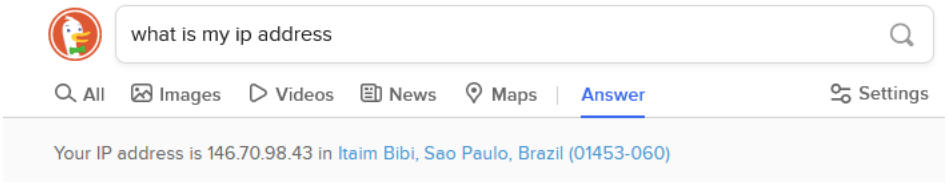
*Verificación de que el tráfico de la red está siendo a través de la VPN*




*Nota.* En la Figura 74 se muestra la confirmación de la dirección IP de la máquina virtual en la que se está trabajando, al colocar el comando “ipconfig” en el Command Prompt de Windows se puede ver que es la dirección IPv4 es la 192.168.10.11.

**Figura 75**

*Verificación de que el tráfico de la red está siendo a través de la VPN en el buscador*



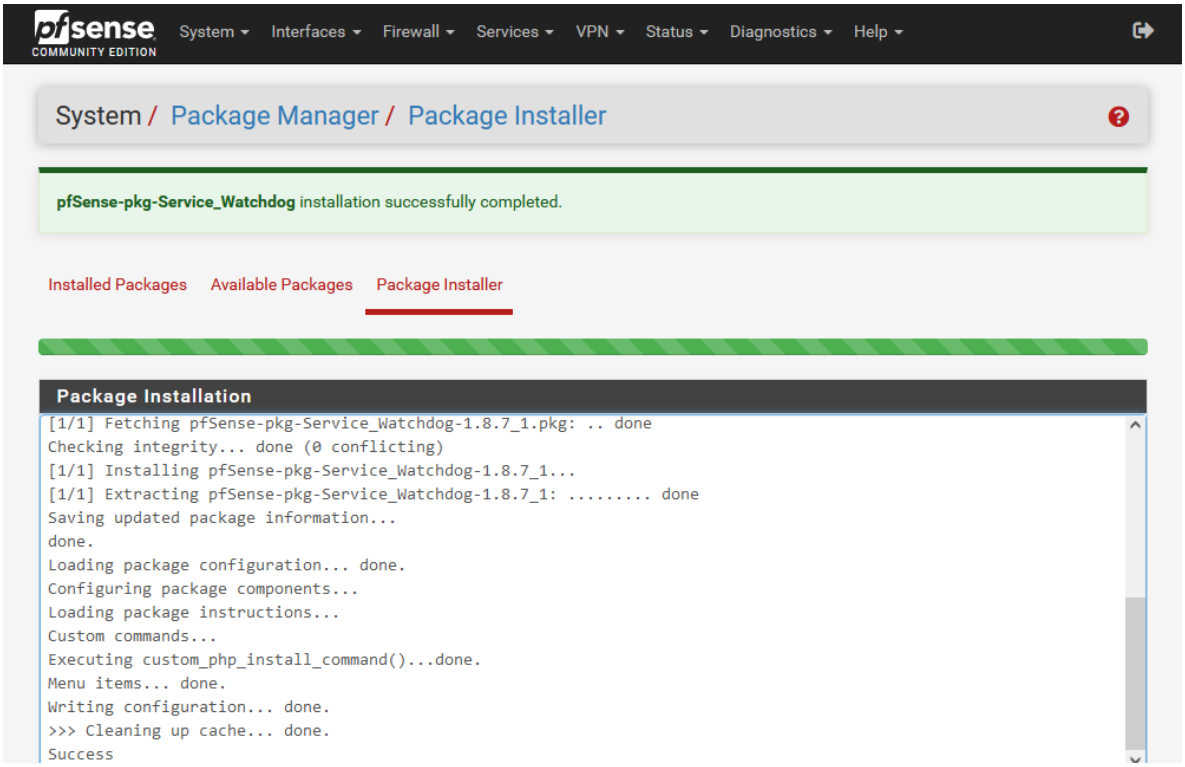

*Nota.* En la Figura 75 se muestra la búsqueda de la dirección IP de la máquina virtual realizada en DuckDuckGo donde se visualiza una dirección IP completamente diferente a la dirección IP real asignada a la máquina virtual, lo que confirma que la navegación en internet se está realizando a través de la VPN configurada.

### 3.3.8. Instalación de paquetes

En la configuración también se han instalado distintos paquetes que permitirán tener acceso a otros aspectos que mejoran la red de datos y la seguridad en la red como los sistemas de prevención y detección de intrusiones y un “Watchdog” que vigile que el servicio de VPN siempre esté en funcionamiento.

**Figura 76**

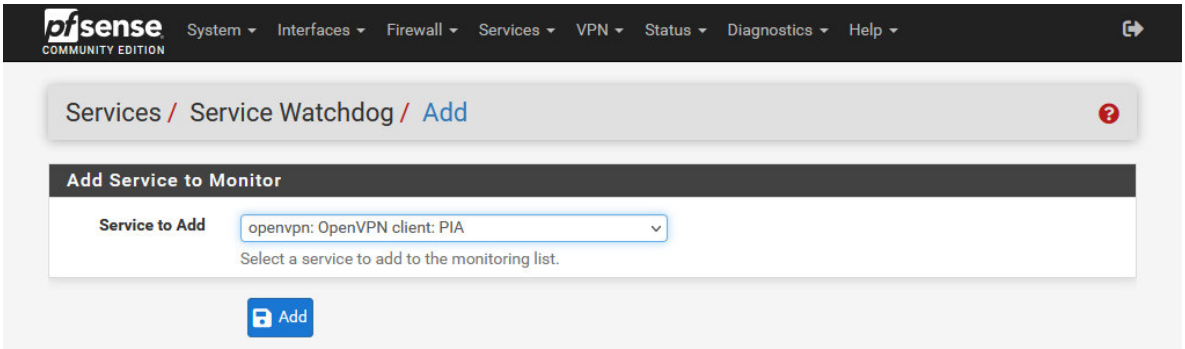
*Instalación de paquetes en pfSense*




*Nota.* En la Figura 76 se muestra la instalación de paquetes en pfSense. Se debe ir a la pestaña de “Sistema” y a “Package Manager” donde están las opciones de ver los paquetes instalados, los paquetes disponibles y el instalador de paquetes, en la pestaña de paquetes disponibles hay una gran cantidad de paquetes de los que se puede escoger e instalar de acuerdo a las necesidades de la red. Se escogió el paquete del “Service Watchdog” que se encarga de monitorear los servicios que se le indiquen, para que si por algún motivo alguno deja de funcionar repentinamente este “Watchdog” lo reinicia nuevamente asegurándose que siempre esté en funcionamiento.

**Figura 77**

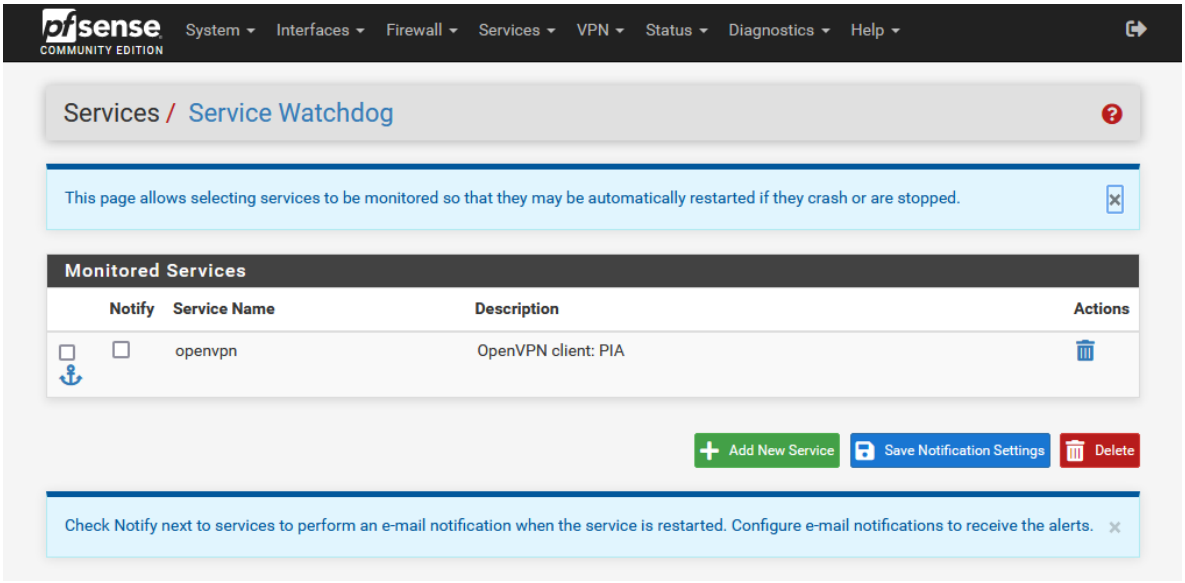
*Colocación de un servicio bajo la vigilancia del "Service Watchdog"*




*Nota.* En la Figura 77 se muestra que una vez instalado el paquete de "Service Watchdog" se puede colocar el servicio de VPN (Private Internet Access) bajo su vigilancia para que se asegure que siempre esté en funcionamiento.

**Figura 78**

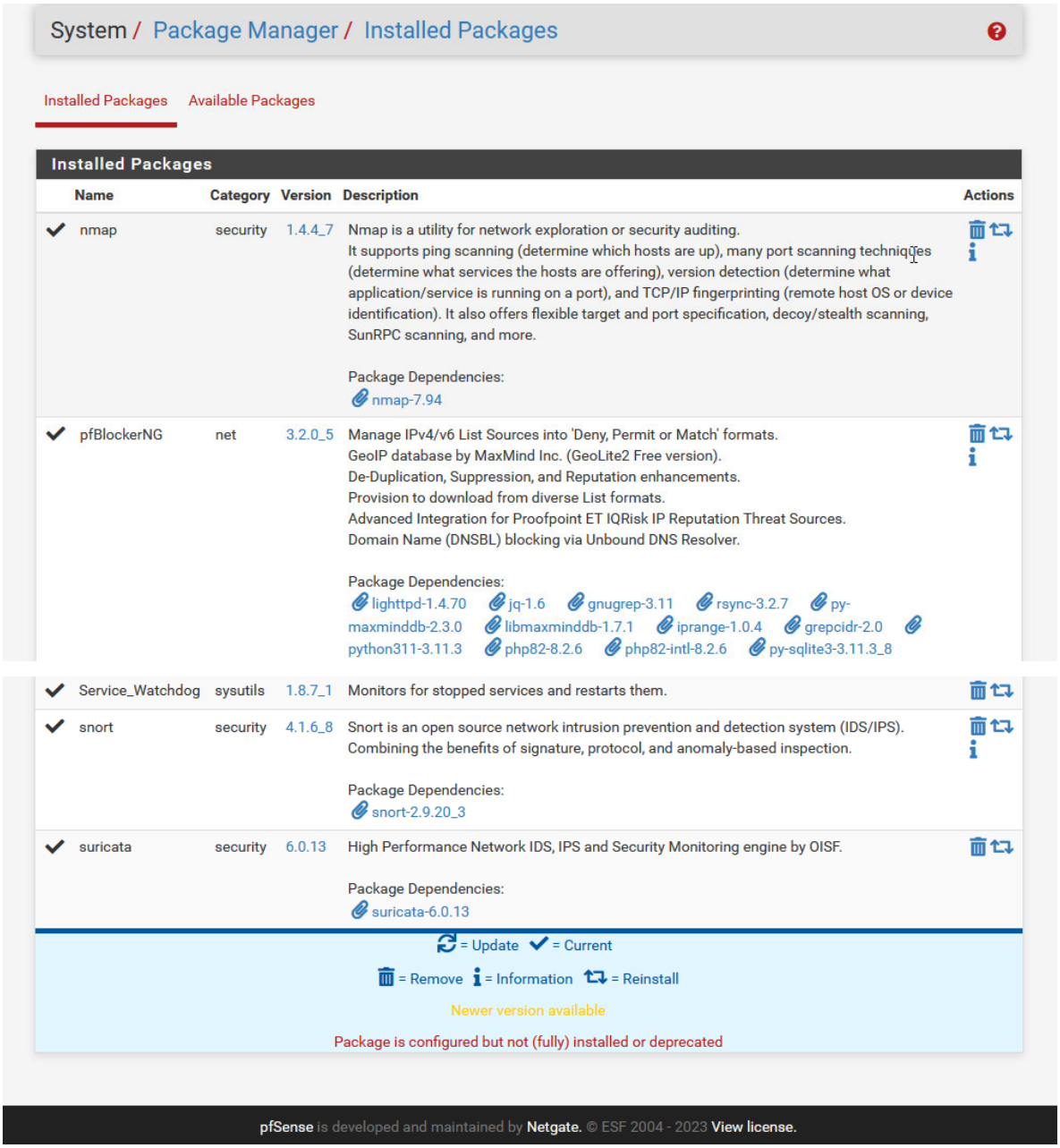
*VPN bajo supervisión del "Service Watchdog"*




*Nota.* En la Figura 78 se muestra que el servicio de VPN ya ha sido agregado de manera exitosa al cuidado de "Service Watchdog".

**Figura 79**

*Lista de paquetes instalados en pfSense*



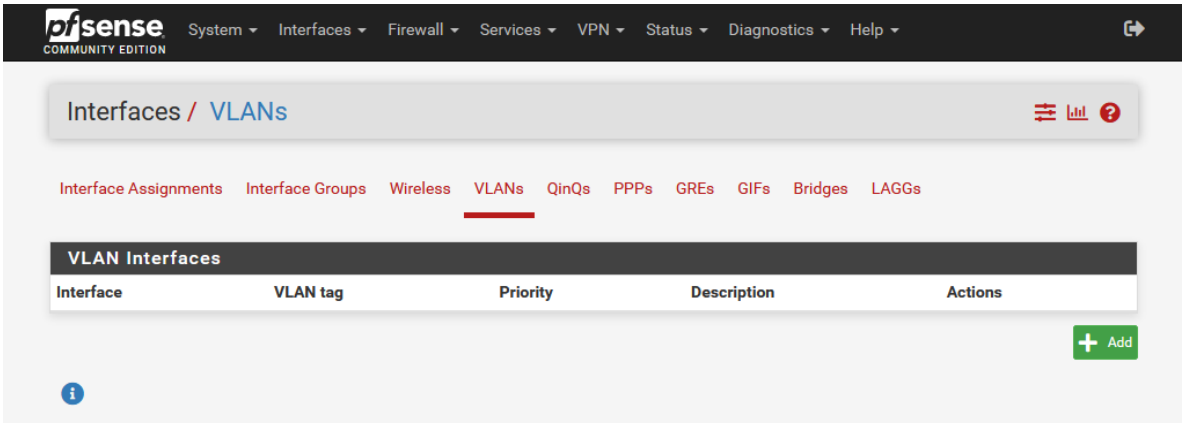

*Nota.* En la Figura 79 se muestran todos los paquetes que han sido instalados en pfSense.

### 3.3.9. Separación de la red en VLANs

En esta parte de la configuración se realiza la separación de la red LAN en cuatro VLANs (VLAN_Administración, VLAN_Docentes, VLAN_Estudiantes y VLAN_Invitados), que permitirá la creación de reglas individuales acordes a cada área y un mejor manejo del flujo de datos en la red.

**Figura 80**

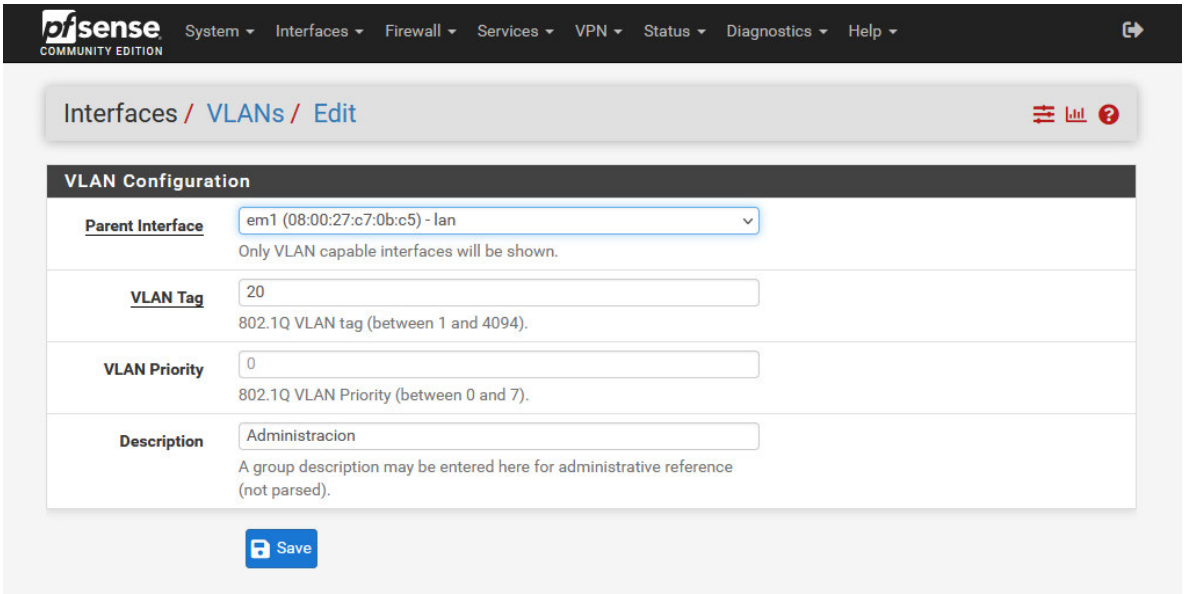
*Camino para la creación de las VLANs*




*Nota.* En la Figura 80 se muestra que al ir a la pestaña de “Interfaces” y “VLANs” se puede hacer clic en “Add” para la creación de nuevas VLANs.

**Figura 81**

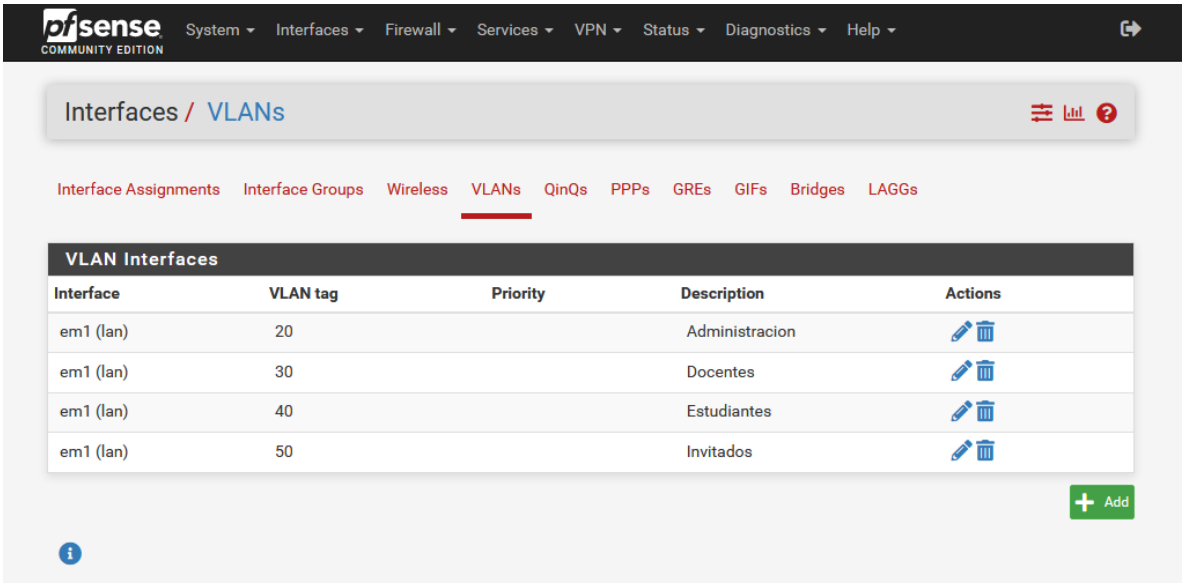
*Campos que deben ser llenados para la creación de una VLAN*




*Nota.* En la Figura 81 se muestran los campos que deben llenarse para la creación de una VLAN. Se debe escoger una Interface principal bajo la cual estará la VLAN, en este caso es la red LAN. Se debe escoger un “VLAN Tag”, este “Tag” funciona como una etiqueta para identificar la VLAN. Por último, se debe colocar una descripción, a esta primera VLAN será la VLAN para “Administración”. Este mismo proceso se siguió para las demás VLANs creadas, son cuatro en total para Administración, Docentes, Estudiantes e Invitados, los “Tags” escogidos son 20, 30, 40, 50 respectivamente, esto es para permitir que la red pueda ser escalable.

**Figura 82**

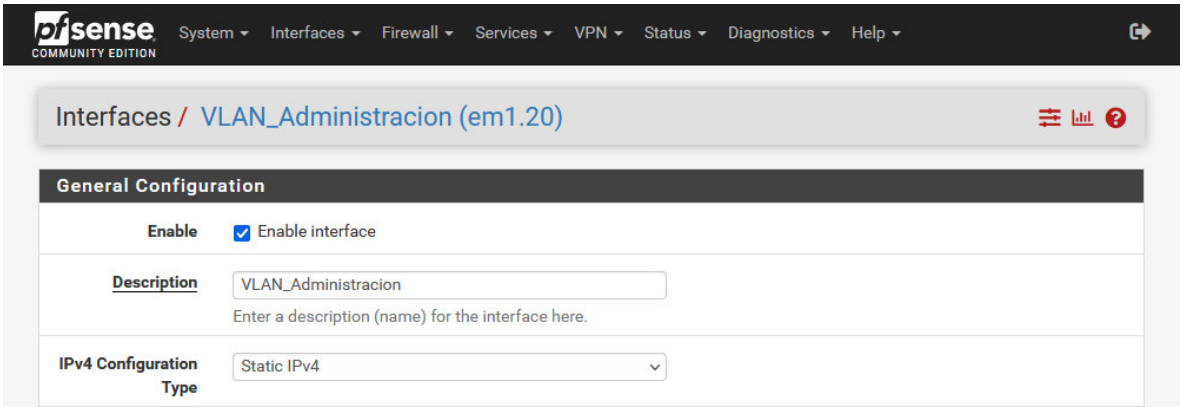
*Vista de VLANs creadas*




*Nota.* En la Figura 82 se muestran las VLANs luego de haber sido creadas.

**Figura 83**

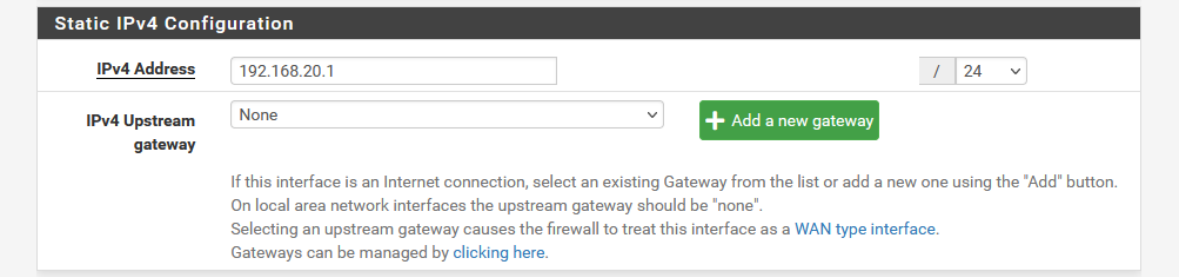
*Activación de cada VLAN creada*




*Nota.* En la Figura 83 se muestra la manera en la que cada VLAN puede ser activada, en la pestaña de “Interfaces” se escoge cada VLAN y se marca la casilla para habilitarlas, se coloca una descripción para cada una (VLAN_Administración, VLAN_Docentes, VLAN_Estudiantes, VLAN_Invitados) y la configuración de IPv4 (Estático).

**Figura 84**

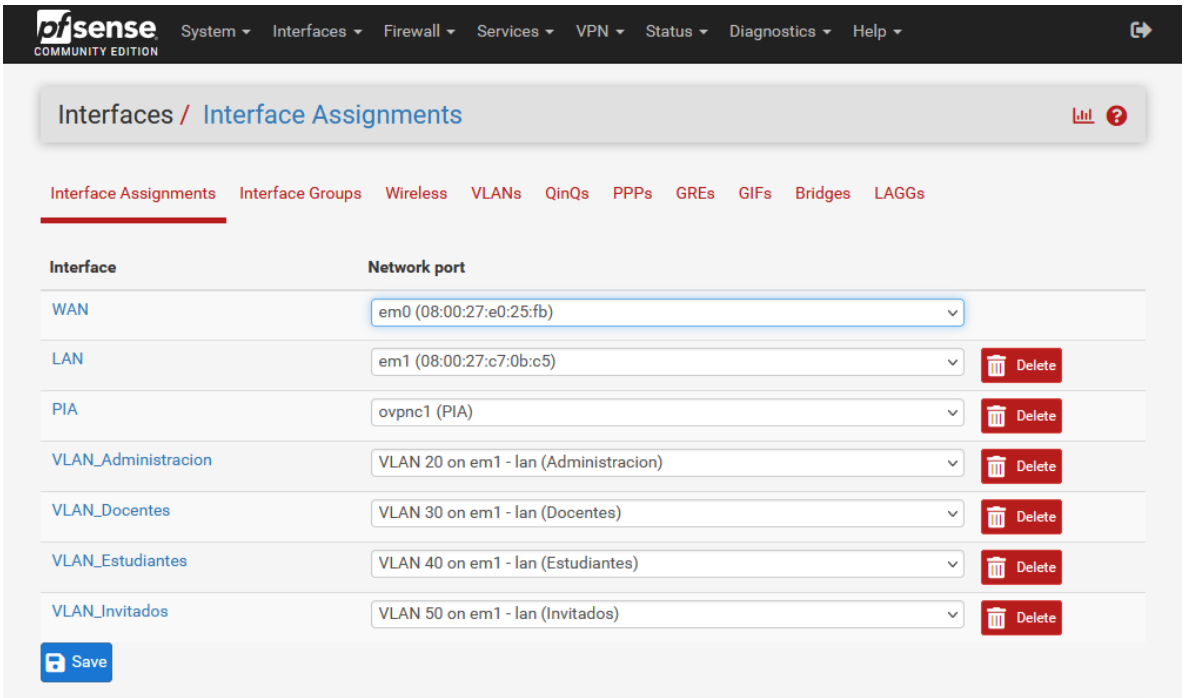
*Configuración de IPv4 estático*




*Nota.* En la Figura 84 se muestra la dirección de IPv4 estático que se configuró para la VLAN_Administración (192.168.20.1), el número 20 en el tercer octeto se escogió de esta manera para identificar a la VLAN de administración fácilmente debido a que ese es el número de "Tag" que se había escogido previamente para esta VLAN, las direcciones IP se escogieron y se configuraron de la misma manera para cada una de las VLANs restantes (192.168.30.1, 192.168.40.1, 192.168.50.1), de este modo, los dispositivos que estén en cada VLAN también serán más fáciles de identificar.

**Figura 85**

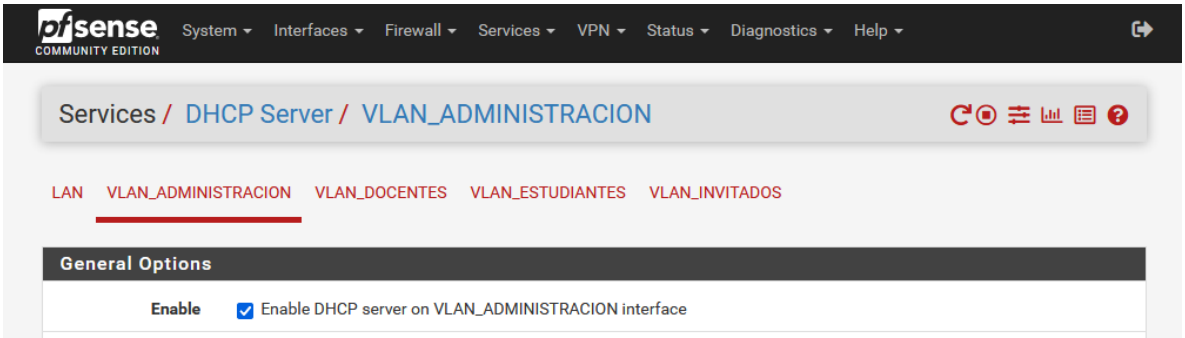
*Tabla de interfaces*




*Nota.* En la Figura 85 se muestra la tabla de interfaces en la red donde se muestran las VLANs luego de haber sido creadas y activadas.

**Figura 86**

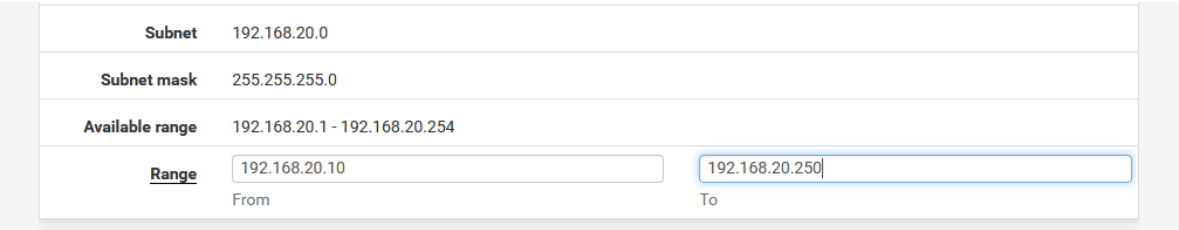
*Activación de DHCP en cada VLAN*




*Nota.* En la Figura 86 se muestra la casilla que debe marcarse para habilitar DHCP en cada VLAN.

**Figura 87**

*Configuración del rango de direcciones IP elegibles para el DHCP de cada VLAN*

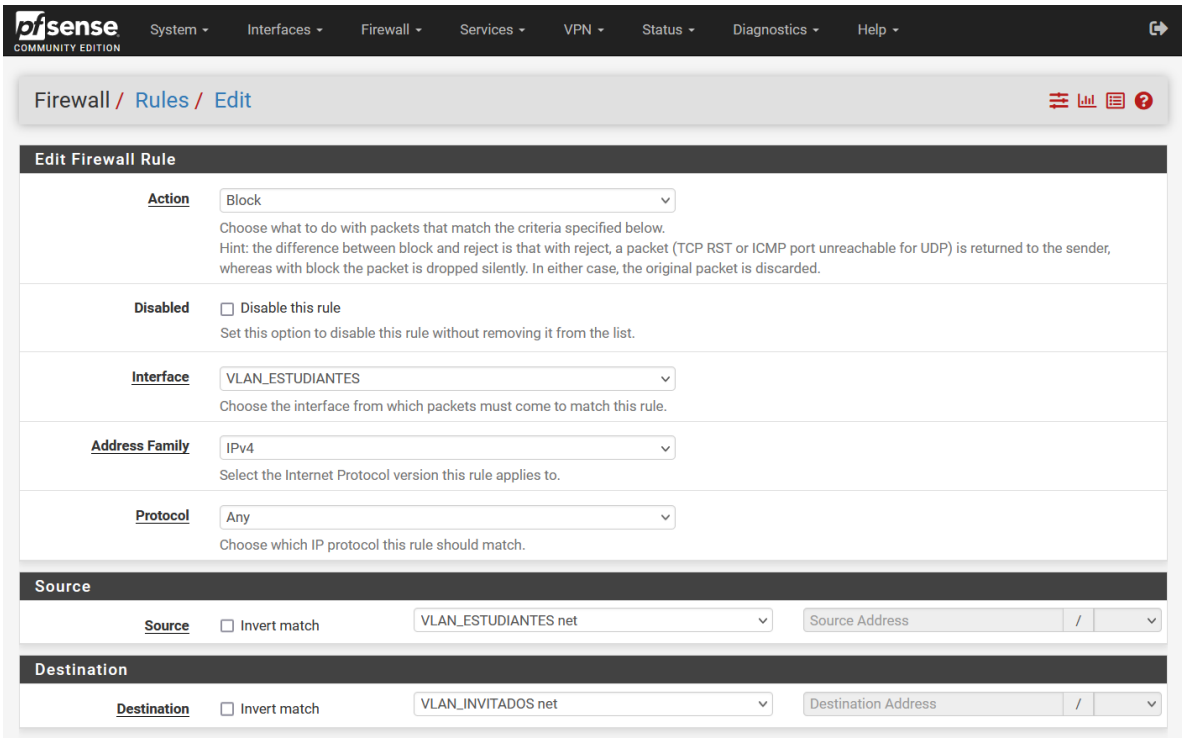



*Nota.* En la Figura 87 se muestra el rango de direcciones IP que se determinó para la VLAN de administración, de la misma manera también se configuró para las VLANs restantes.

### 3.3.10. Bloqueo de contenido en cada VLAN

**Figura 88**

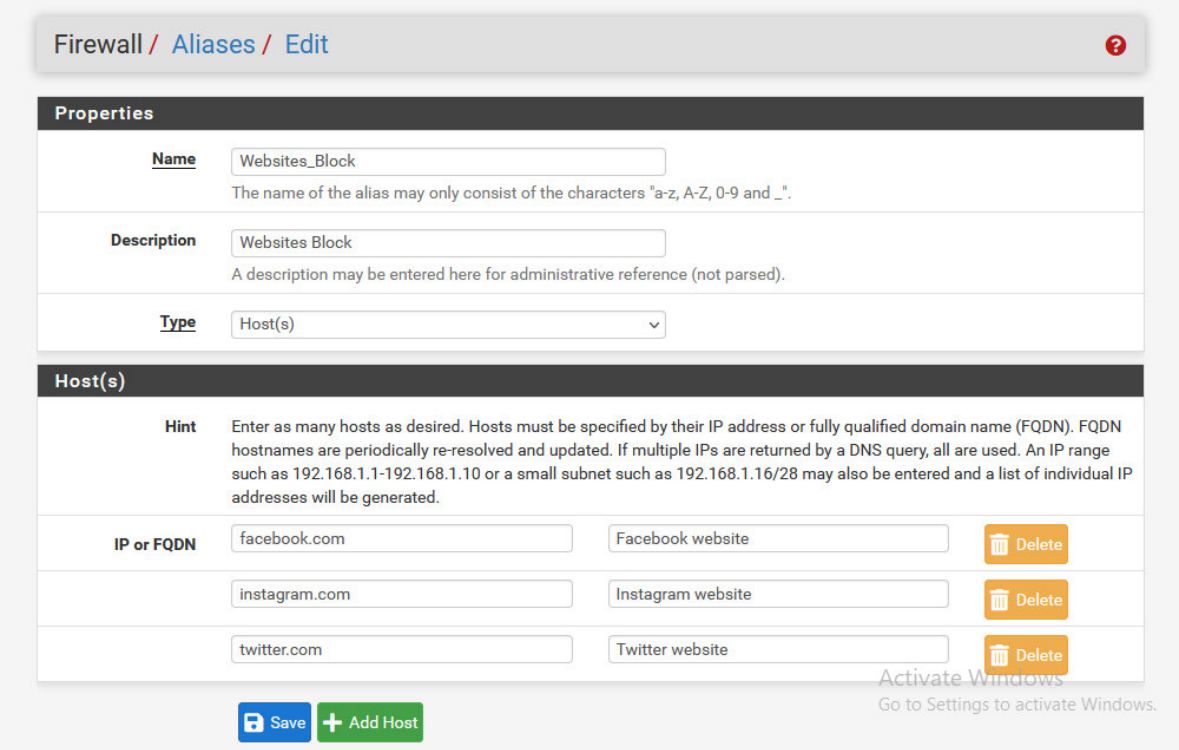
*Bloqueo de tráfico entres VLANs*




*Nota.* En la Figura 88 se muestra la creación de una regla de Firewall para bloquear el tráfico desde la VLAN_ESTUDIANTES a VLAN_INVITADOS, esto se hace con la finalidad de que las VLANs no puedan comunicarse entre ellas y exista una separación. De la misma manera también se bloqueó el tráfico entre las demás VLANs, la única VLAN a la que se le dio comunicación con todas las demás es la VLAN_Administración y las VLANs para docentes y estudiantes podrán comunicarse entre ellas.

**Figura 89**

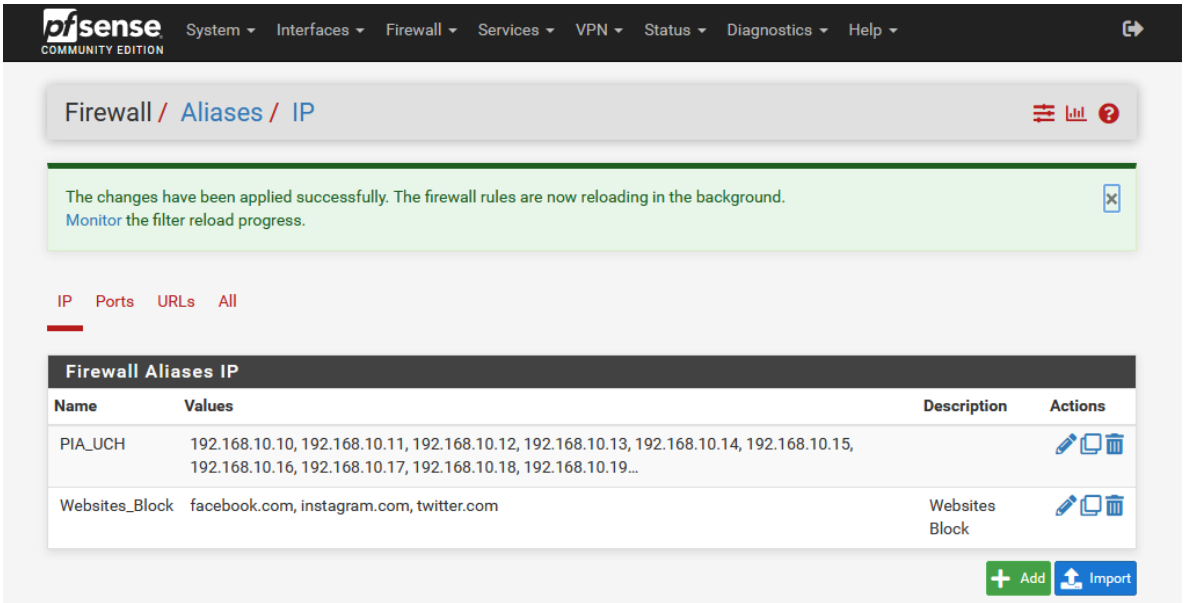
*Creación de alias para bloqueo de páginas web en las VLAN*




*Nota.* En la Figura 89 se muestra el llenado de campos para la creación de un alias para bloqueo de páginas web en las reglas de Firewall de las VLANs. Las tres páginas web que se han colocado bajo este alias son Facebook, Instagram y Twitter, se deben colocar en la sección de “IP o FQDN (Fully Qualified Domain Name)”.

**Figura 90**

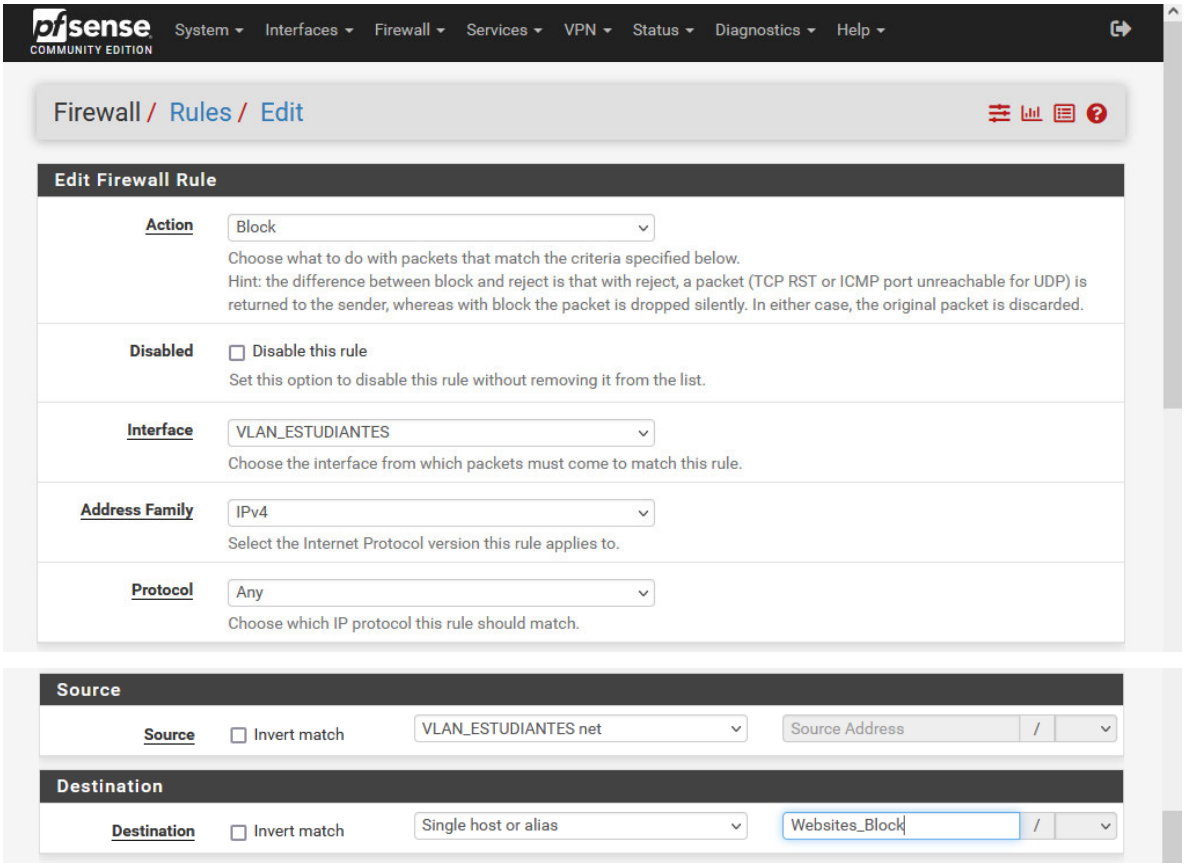
*Creación de alias realizado correctamente*




*Nota.* En la Figura 90 se muestra la tabla de alias creados donde se visualiza el nuevo alias de bloqueo de páginas web.

**Figura 91**

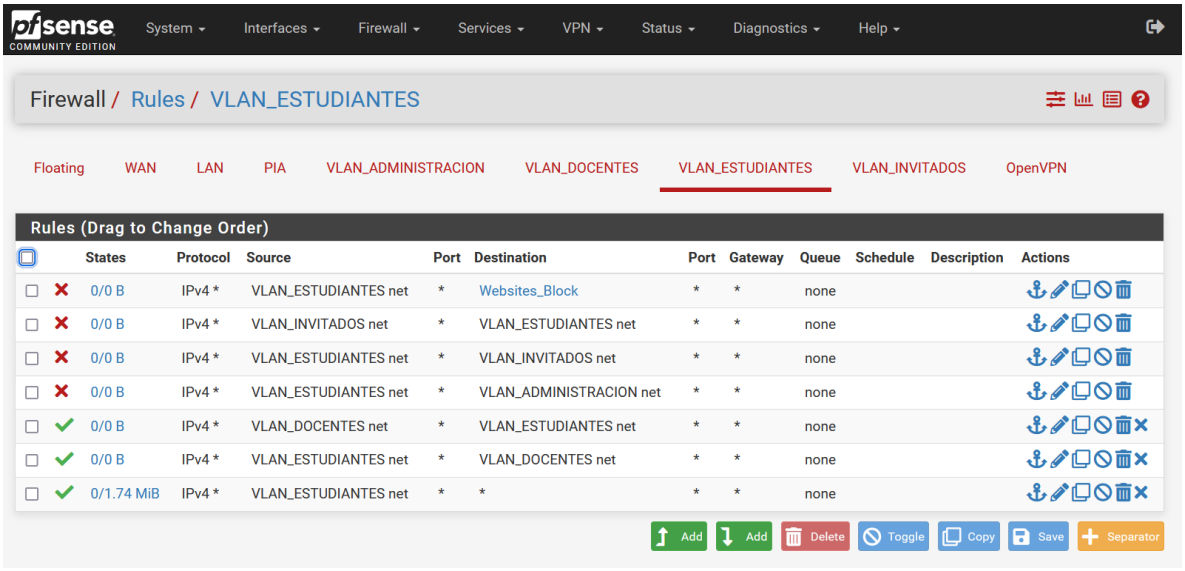
*Uso de alias creado para bloqueo de páginas web en la VLAN para estudiantes*




*Nota.* En la Figura 91 se muestra la creación de una regla de Firewall en la VLAN_Estudiantes para el bloqueo de las páginas web que se han colocado bajo el alias creado (Websites_Block).

**Figura 92**

*Tabla de reglas de Firewall en VLAN_Estudiantes*



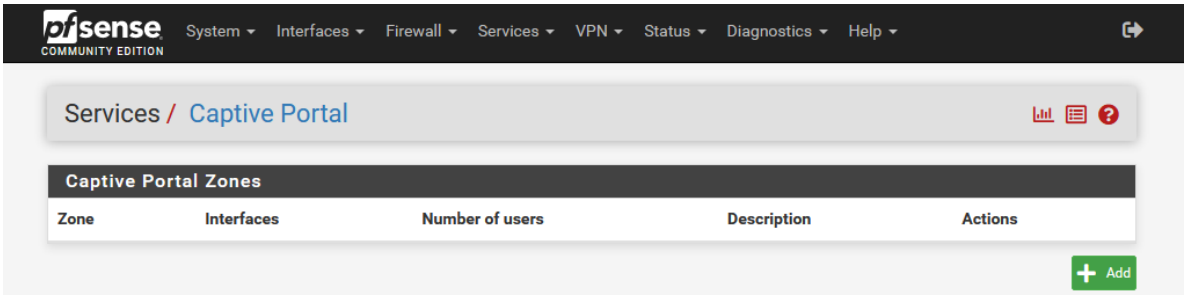

*Nota.* En la Figura 92 se muestra la tabla de reglas de Firewall en VLAN_Estudiantes donde se visualiza la nueva regla creada de boqueo de páginas web.

### 3.3.11. Creación de un portal cautivo

Este portal cautivo permitirá agregar más seguridad a la red debido a que cada usuario que desee acceder a la red debe ingresar un nombre de usuario y contraseña validos en la pestaña del portal cautivo para poder ingresar.

**Figura 93**

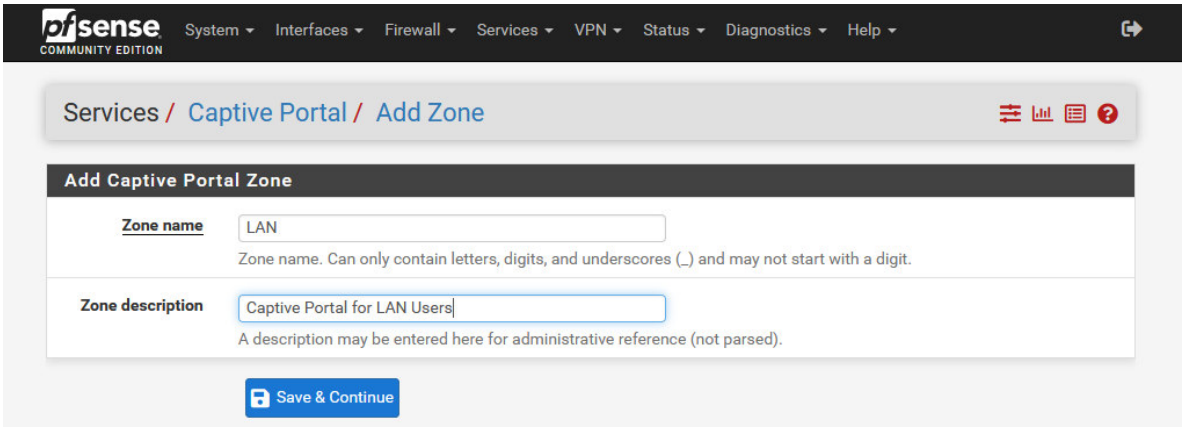
*Pestaña para crear un portal cautivo*




*Nota.* En la Figura 93 muestra la pestaña para la creación de un portal cautivo en pfSense. Se debe hacer clic en “Add”.

**Figura 94**

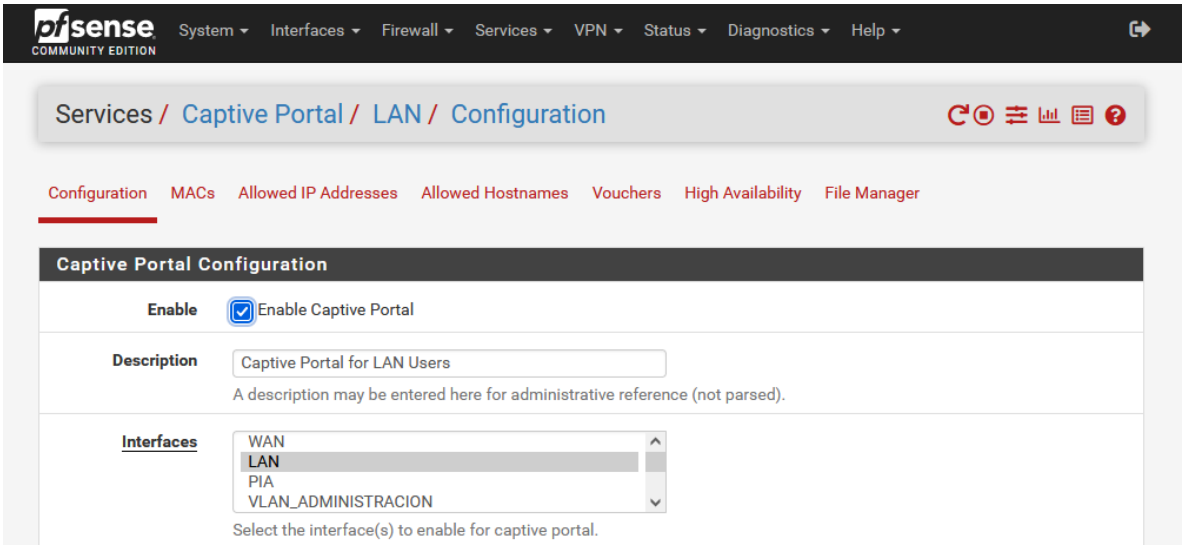
*Creación de zona para el portal cautivo*




*Nota.* En la Figura 94 se muestra la creación de la zona para el portal cautivo. La zona que se ha escogido para el portal cautivo es la red LAN, se debe colocar un nombre a la zona y una descripción.

**Figura 95**

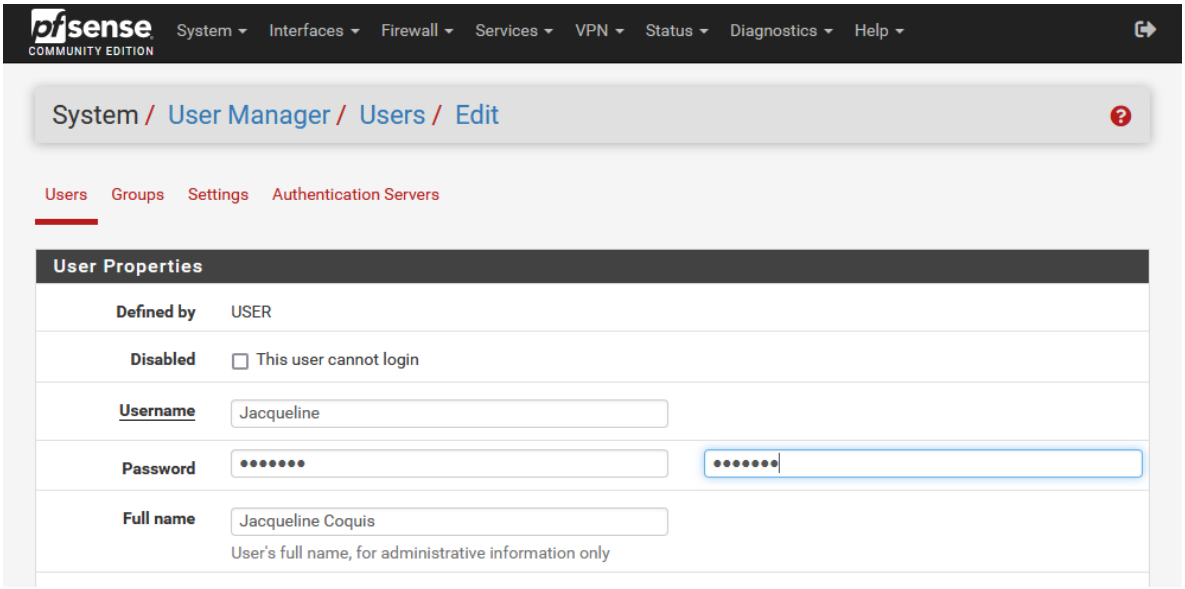
*Configuración de portal cautivo*




*Nota.* En la Figura 95 se muestra la configuración del portal cautivo, se marca la casilla para habilitarlo y se escoge la interface en la que estará operativo, en este caso se ha escogido la red LAN.

**Figura 96**

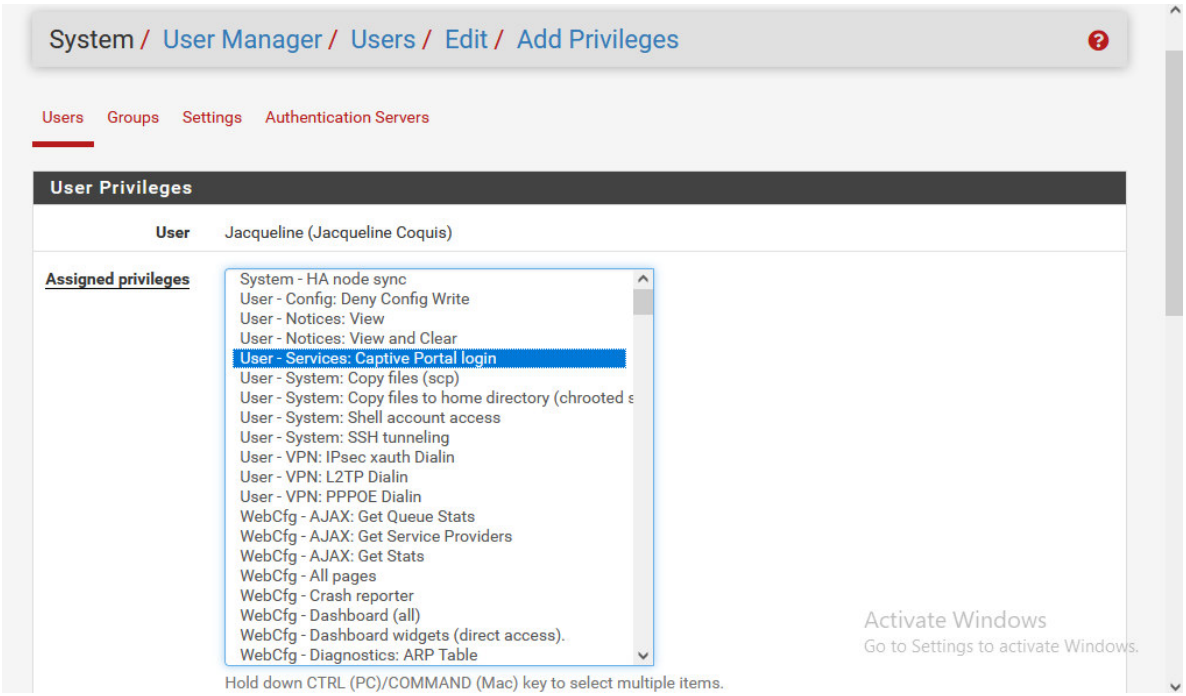
*Creación de usuario y credenciales para acceso a través del portal cautivo*




*Nota.* En la Figura 96 se muestra la creación de un usuario y contraseña para permitir el ingreso a través del portal cautivo.

**Figura 97**

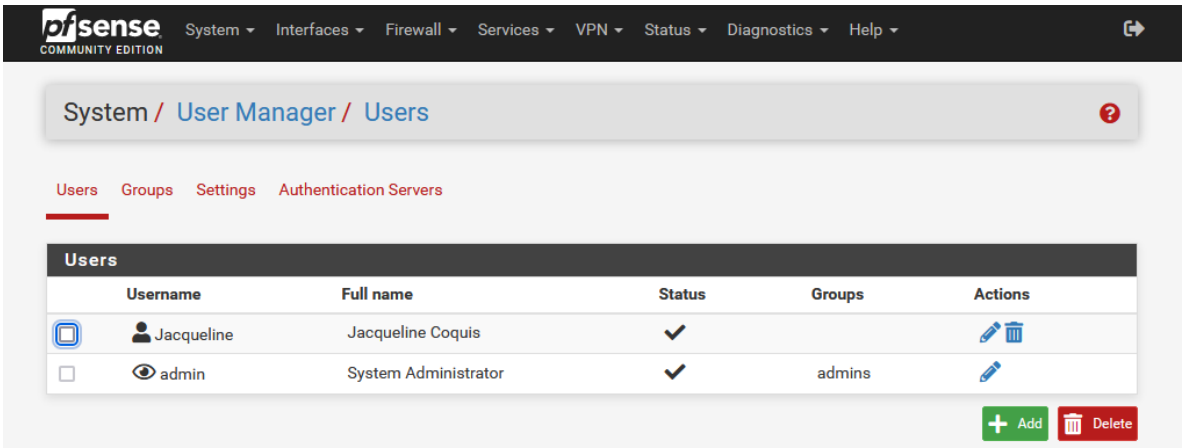
*Usuario con privilegio de acceso a portal cautivo*




*Nota.* En la Figura 97 se muestra la asignación de privilegios al usuario creado para permitir su acceso a través del portal cautivo.

**Figura 98**

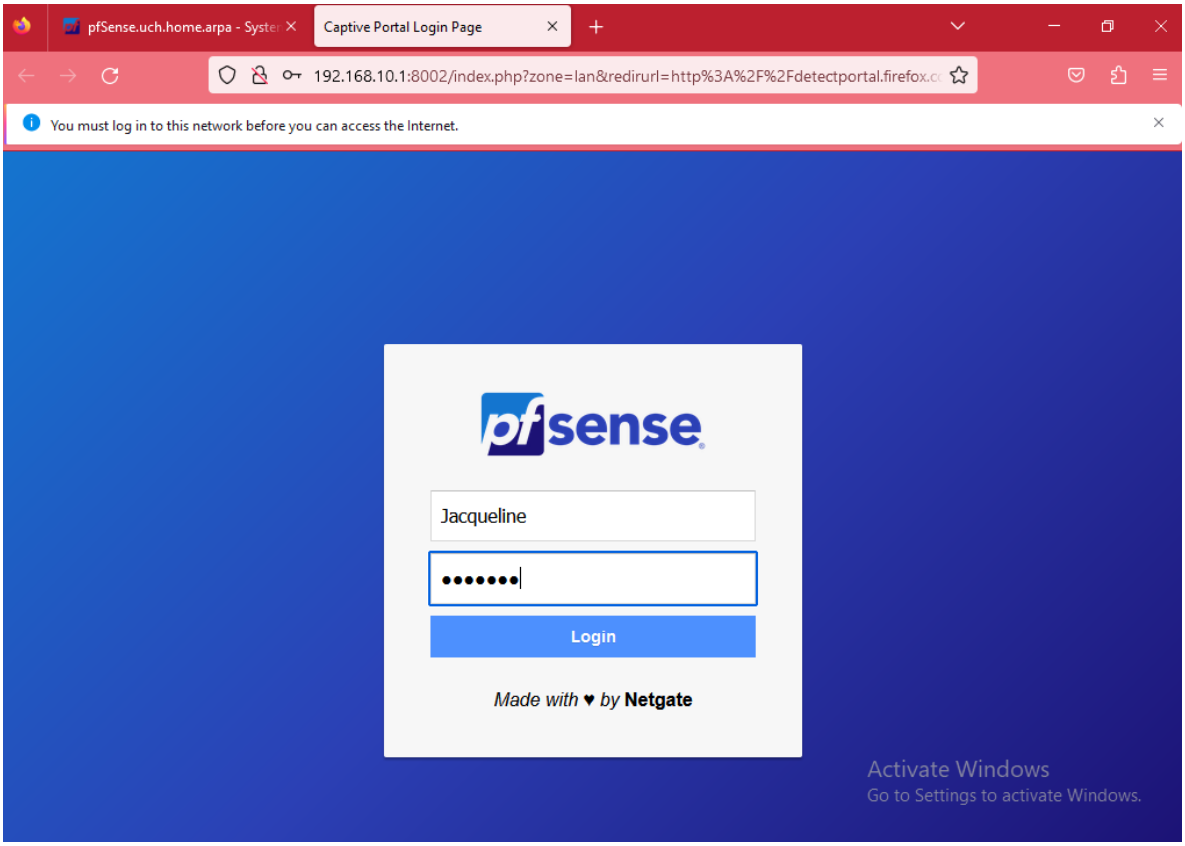
*Tabla de usuarios en pfSense*




*Nota.* En la Figura 98 se muestra la lista de usuarios en pfSense con el usuario creado.

**Figura 99**

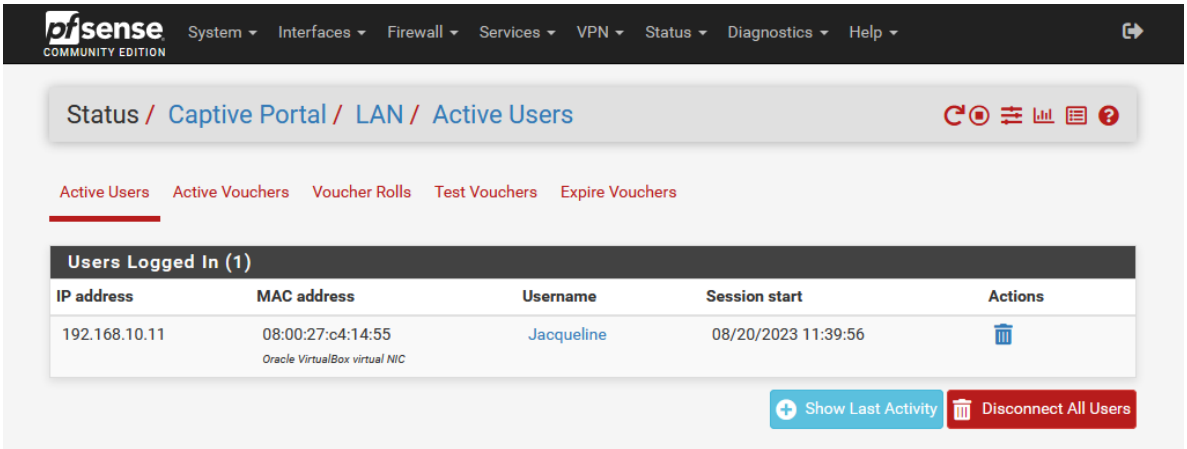
*Portal cautivo creado*




*Nota.* En la Figura 99 se muestra el portal cautivo creado, esta pestaña se abre al tratar de ingresar a internet, se debe colocar un nombre de usuario y una contraseña válidos para poder acceder a internet.

**Figura 100**

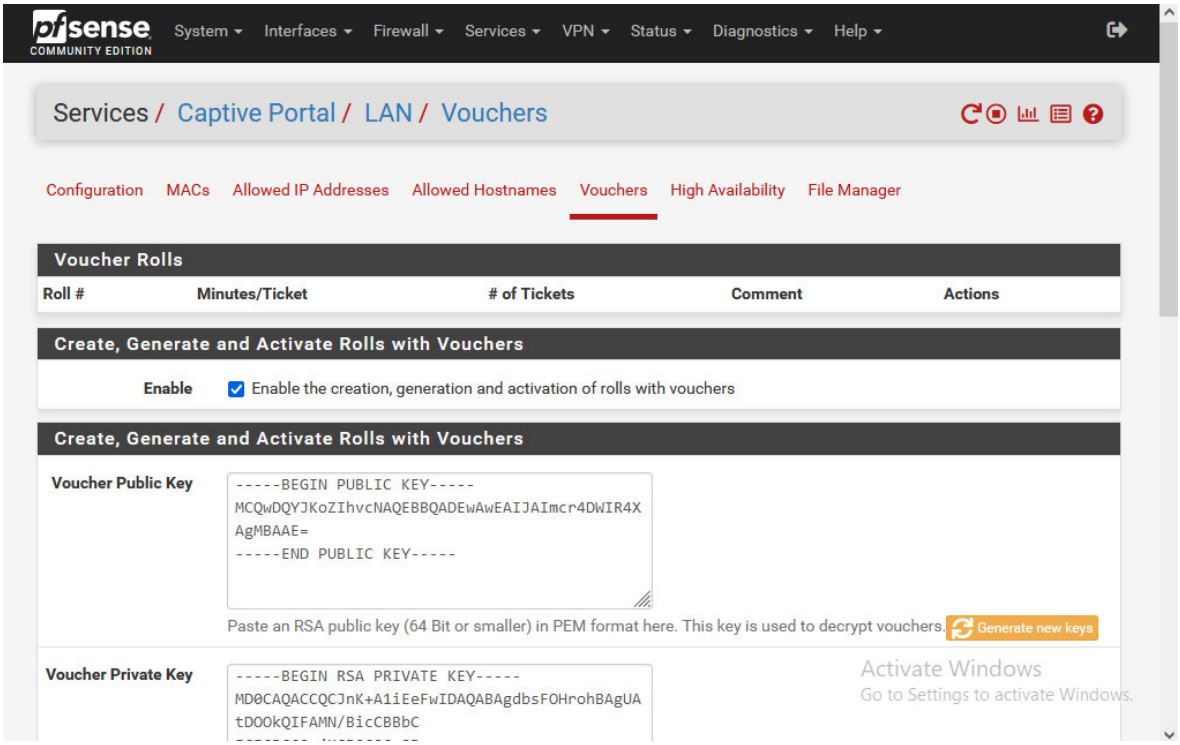
*Tabla de usuarios activos en pfSense*




*Nota.* En la Figura 100 se muestra la tabla de usuarios conectados a la red en pfSense luego de haber colocado las credenciales e ingresado a través del portal cautivo.

**Figura 101**

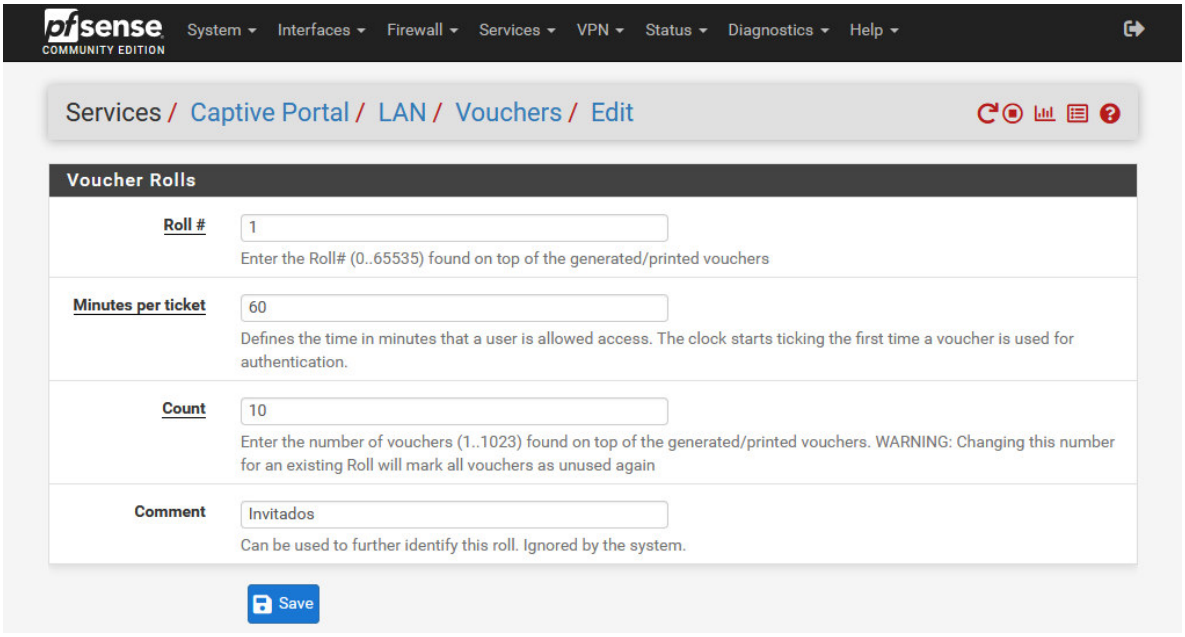
*Activación de creación de vouchers en pfSense*




*Nota.* En la Figura 101 se muestra la activación de la creación de vouchers para brindar acceso al portal cautivo para visitantes. Los vouchers son códigos que se generan para uso de una única vez que se pueden dar a visitantes para que tengan acceso a través del portal cautivo por tiempo limitado.

**Figura 102**

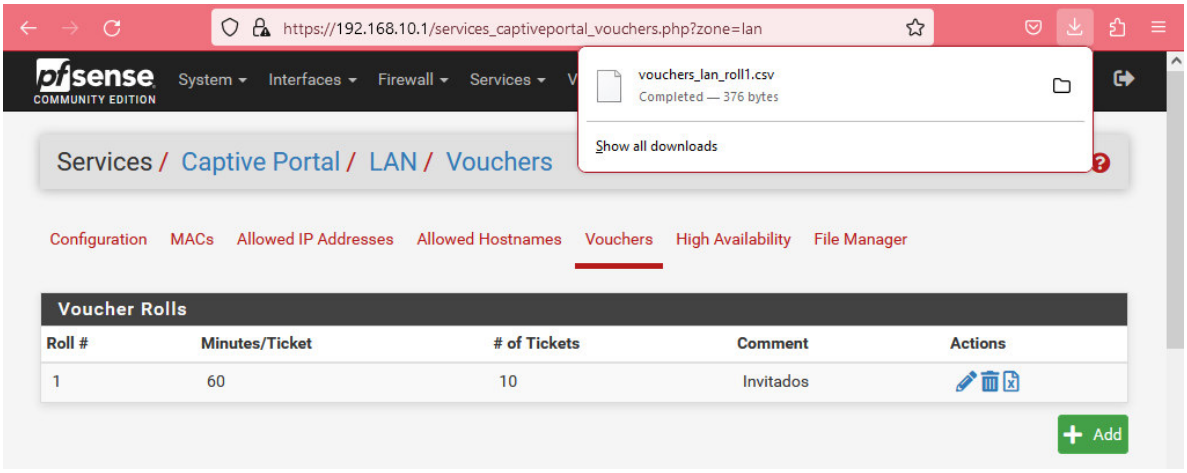
*Creación de vouchers*




*Nota.* En la Figura 102 se muestran los campos que deben llenarse para la creación de vouchers. En este ejemplo se crearon 10 vouchers con una duración de 60 minutos a cada uno para invitados.

**Figura 103**

*Descarga de documento con vouchers*




*Nota.* En la Figura 103 se muestra que luego de la creación de los vouchers se puede descargar el archivo con los códigos.

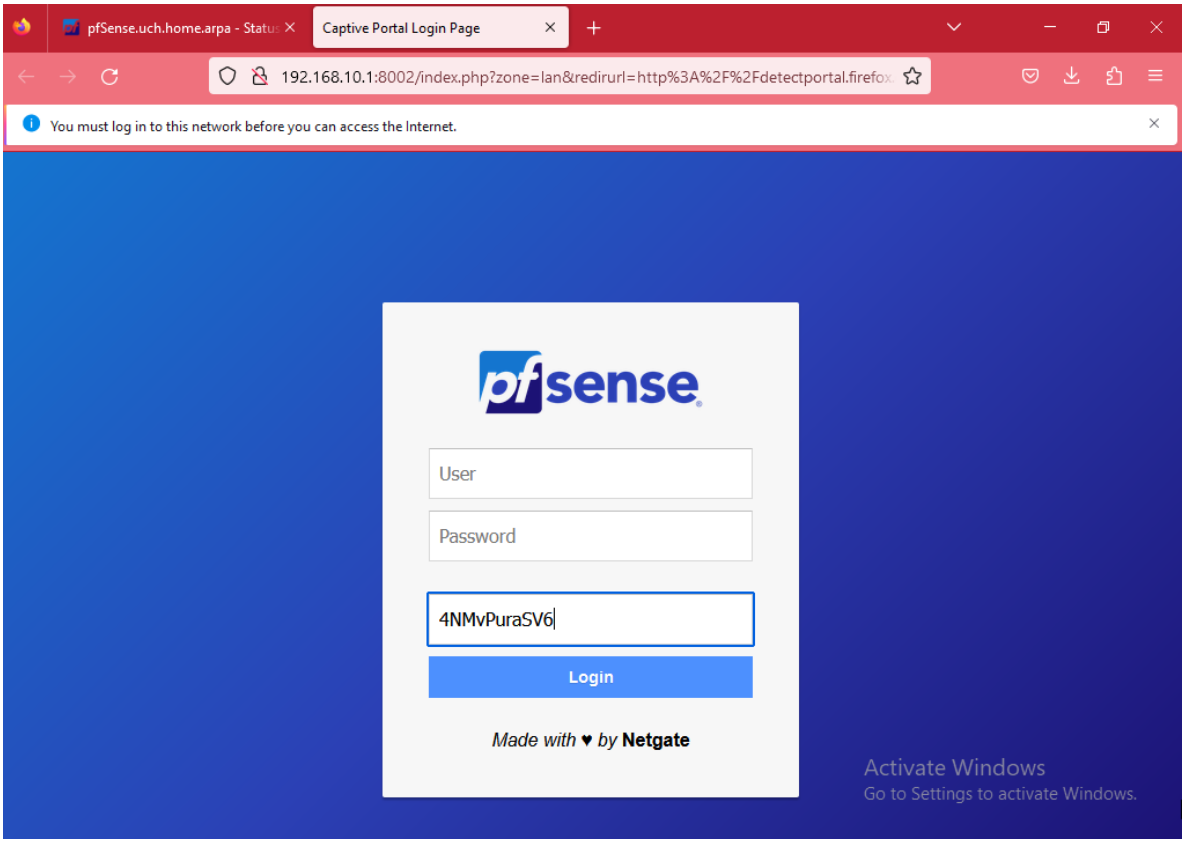
**Figura 104**

*Archivo descargado con los números de vouchers*


*Nota.* En la Figura 104 se muestra es archivo luego ser abierto con los códigos de los vouchers generados. Estos 10 códigos pueden ser dados a 10 visitantes para que tengan acceso por 60 minutos a la red a través del portal cautivo.

**Figura 105**

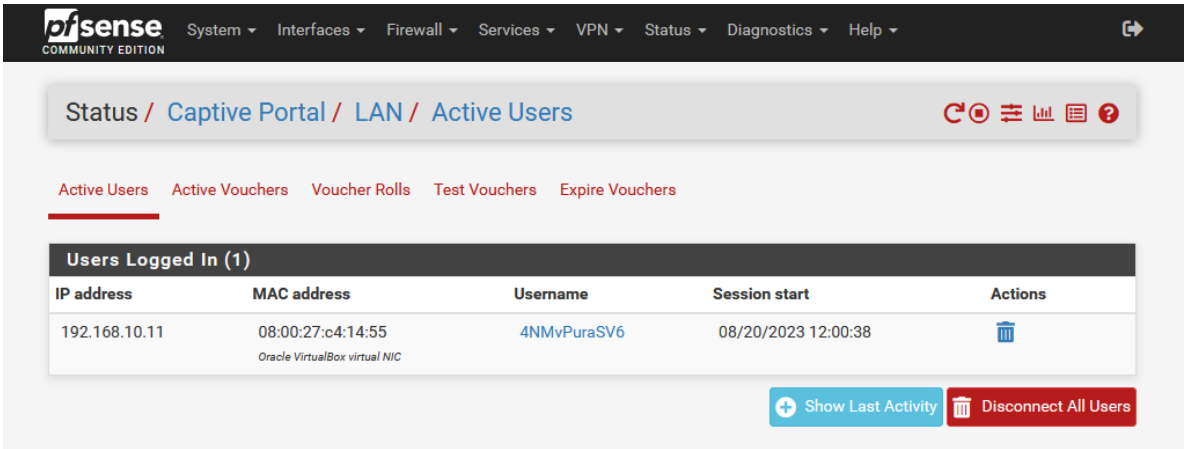
*Pestaña de portal cautivo con opción para ingresar con código de voucher*




*Nota.* En la Figura 105 se muestra la pestaña del portal cautivo para acceso a la red con la opción de ingresar con un código de voucher.

**Figura 106**

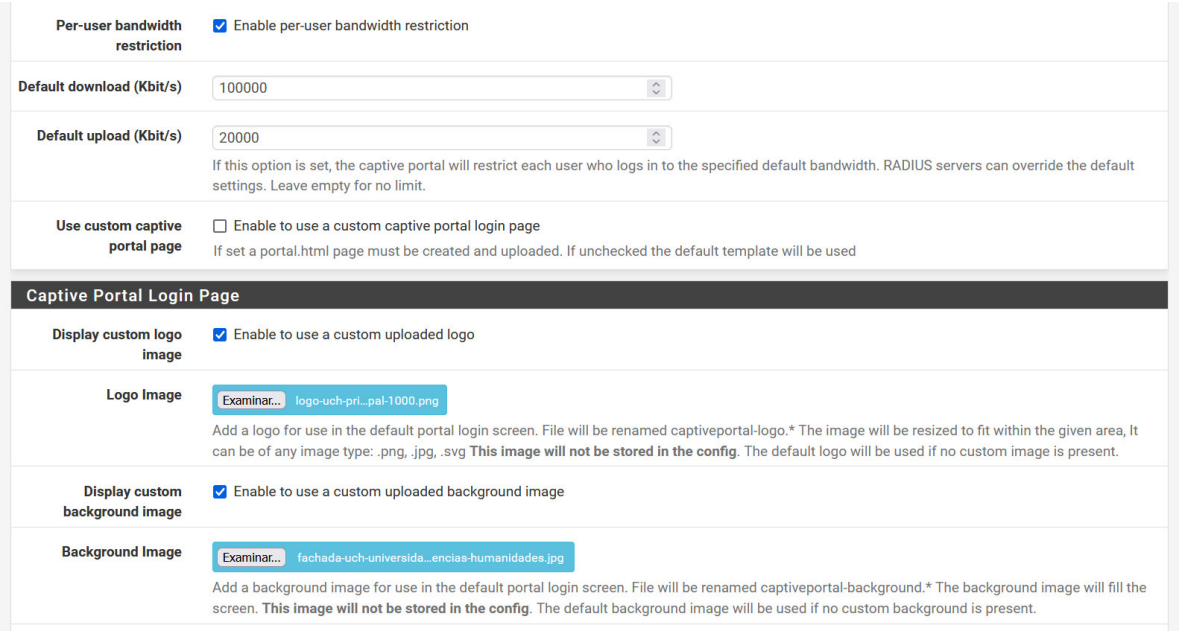
*Usuario activo en la red con código de voucher*




*Nota.* En la Figura 106 se muestra la tabla de usuarios activos en la red donde se visualiza el usuario que ha ingresado con el uso de un código de voucher.

**Figura 107**

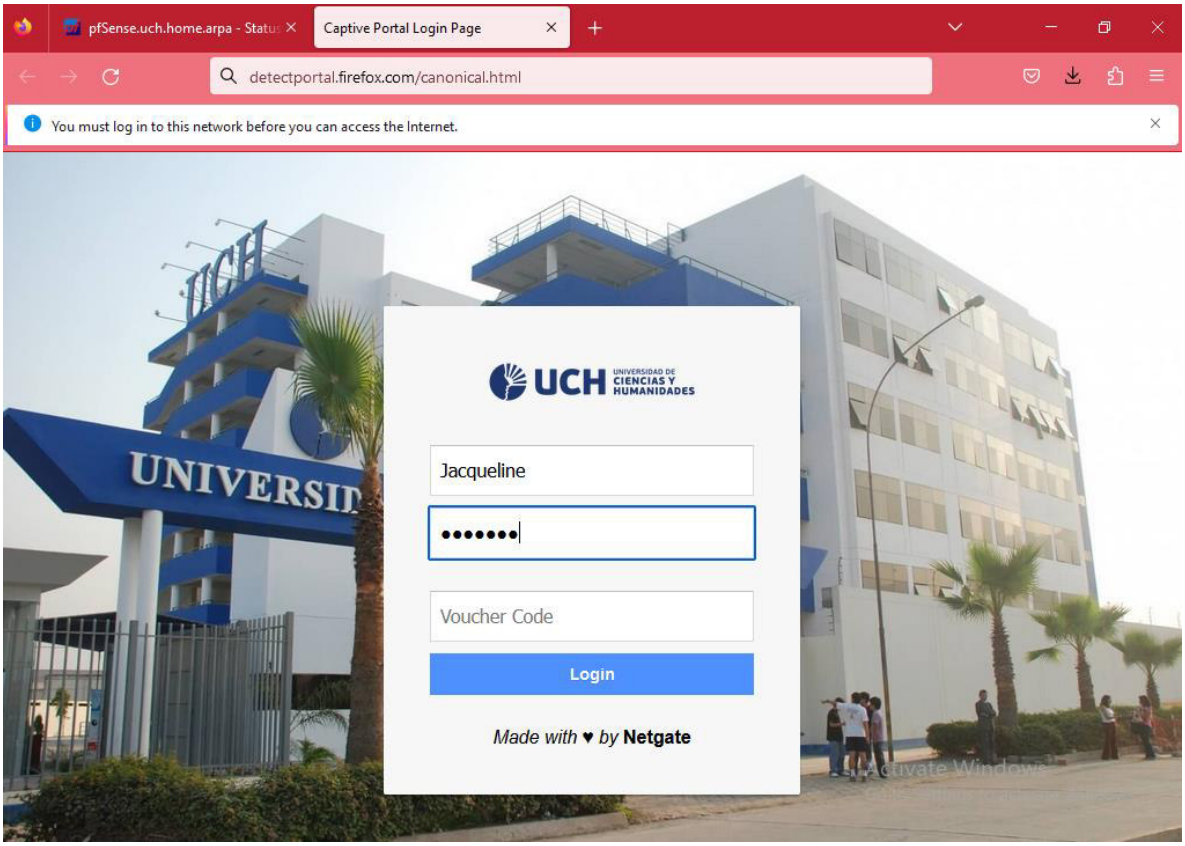
*Personalización del portal cautivo*




*Nota.* En la Figura 107 se muestra que en la configuración del portal cautivo se brinda la opción para colocar una restricción de ancho de banda que se configuró con 100 Mbps de velocidad de "Download" y 20 Mbps de "Upload". De igual manera, se brinda la opción para personalizarlo con un logo y una imagen de fondo. Se colocó el logo de la Universidad de Ciencias y Humanidades y una imagen de la universidad como fondo.

**Figura 108**

*Nueva imagen personalizada del portal cautivo*



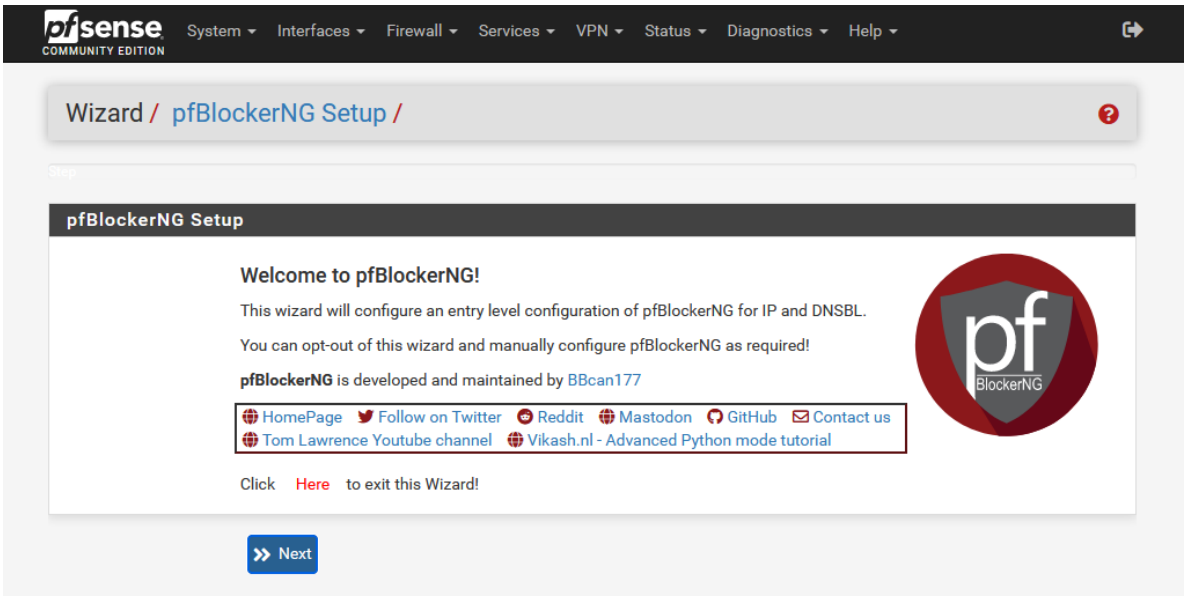

*Nota.* En la Figura 108 se muestra la nueva imagen del portal cautivo creado luego de la personalización con el logo de la Universidad de Ciencias y Humanidades y el fondo.

### 3.3.12. Configuración de pfBlockerNG

PfBlockerNG es un paquete de pfSense que permite bloquear las conexiones provenientes de otros países.

**Figura 109**

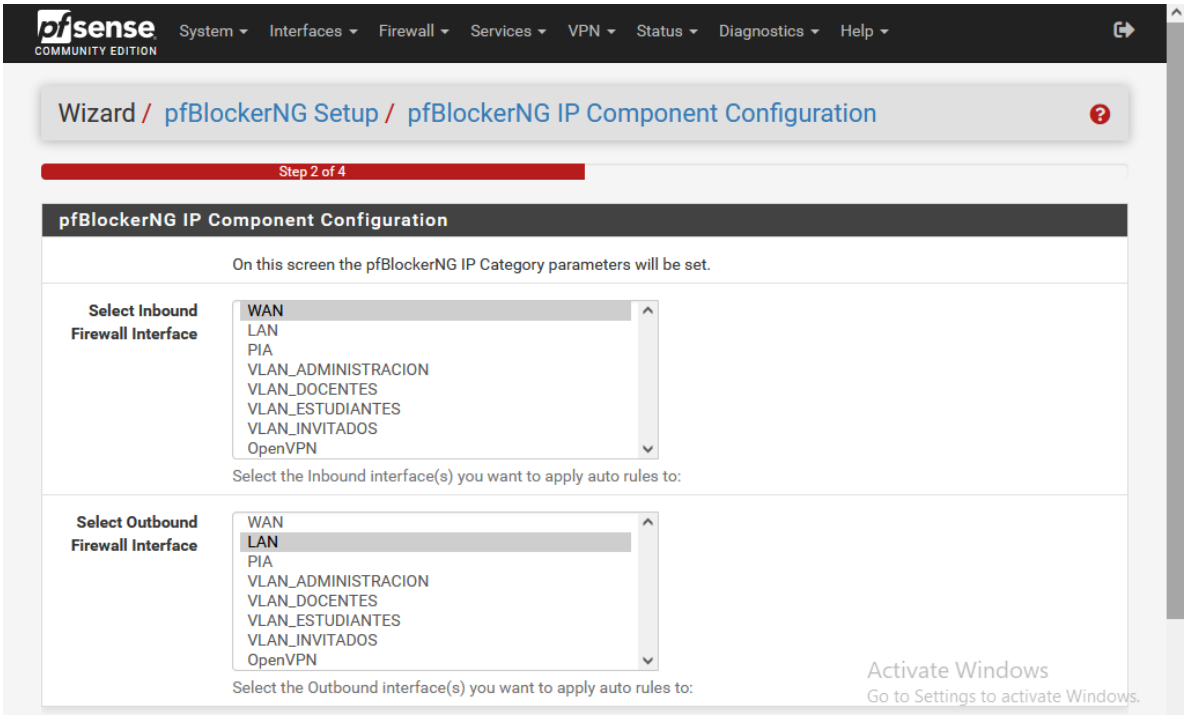
*Configuración de pfBlockerNG*




*Nota.* En la Figura 109 se muestra la configuración de pfBlockerNG. Se comienza con la configuración básica con el Wizard.

**Figura 110**

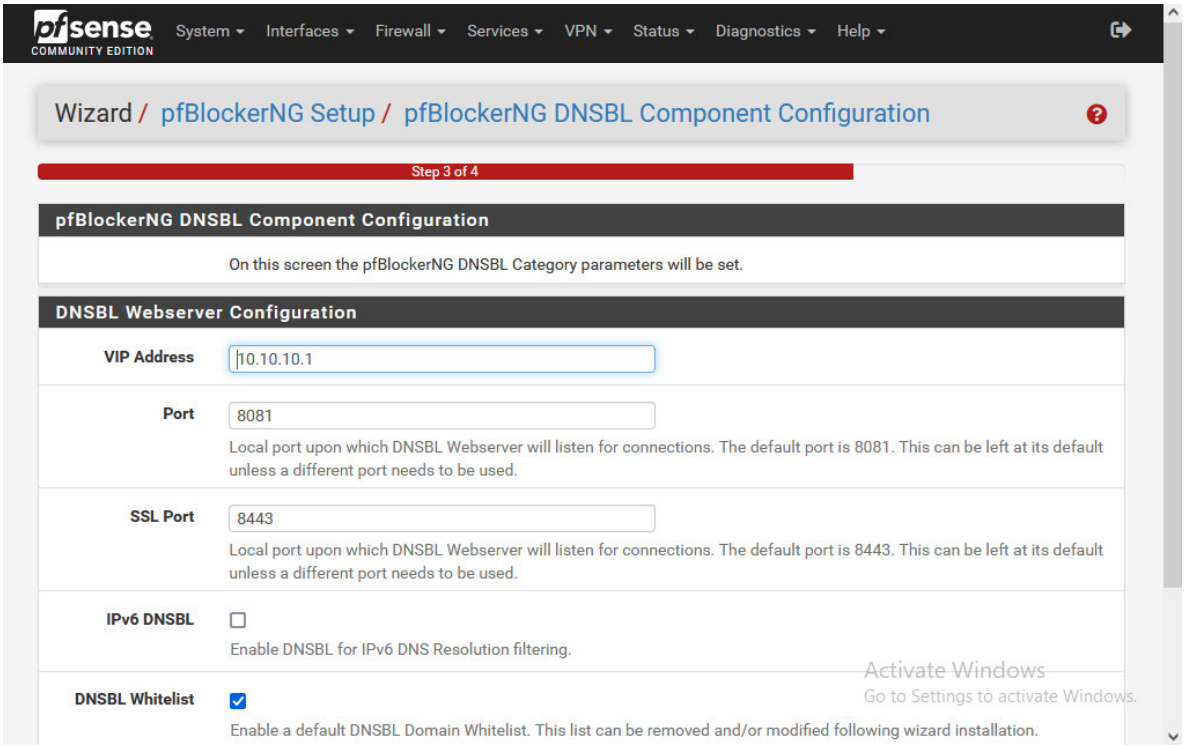
*Configuración de interfaces para pfBlockerNG*




*Nota.* En la Figura 110 se muestran los campos para ingresar las interfaces en pfBlockerNG.

**Figura 111**

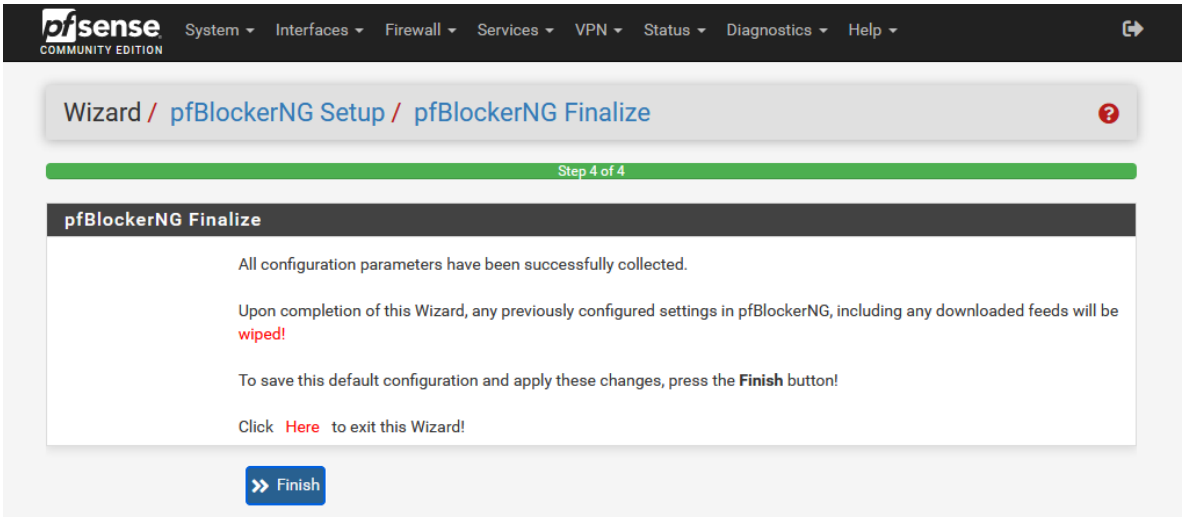
*Dirección VIP y puertos para pfBlockerNG*




*Nota.* En la Figura 111 se muestra la dirección VIP predeterminada para pfBlockerNG y los puertos predeterminados.

**Figura 112**

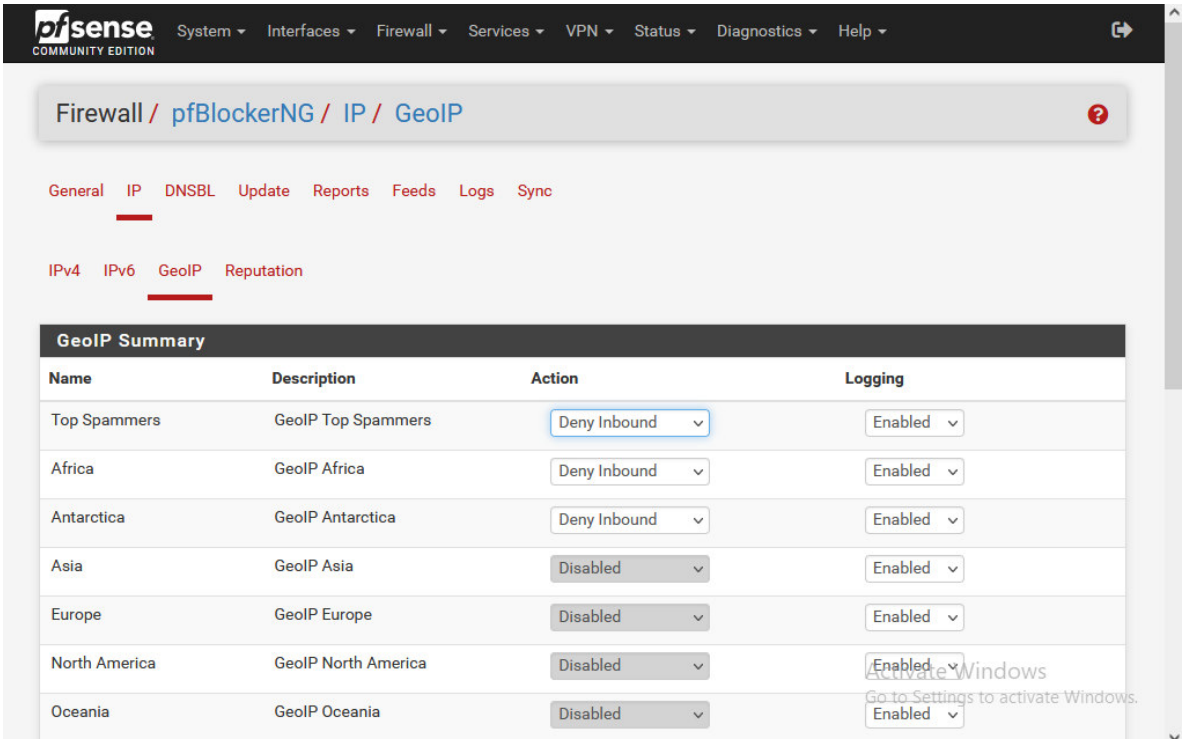
*Finalización de configuración básica de pfBlockerNG*




*Nota.* En la Figura 112 se muestra el último paso de la configuración básica de pfBlockerNG donde se debe presionar “Finish” para que las configuraciones tomen efecto.

**Figura 113**

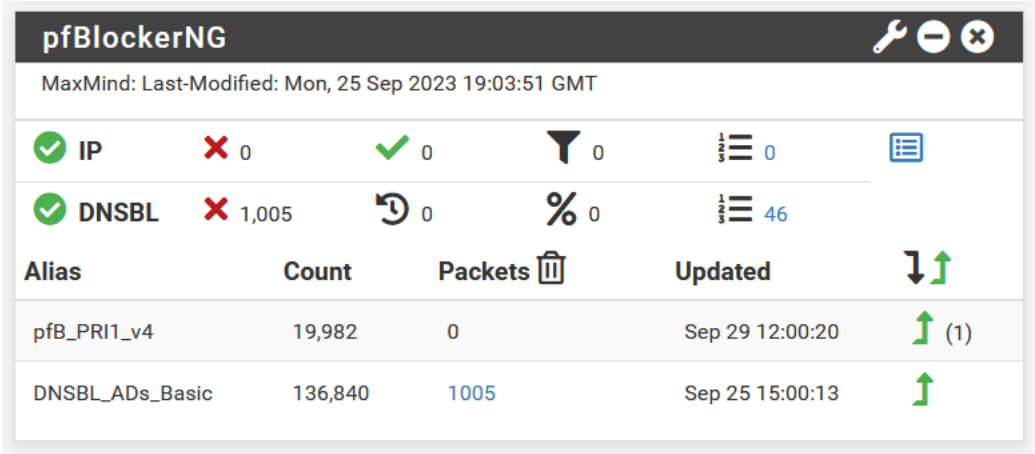
*Bloqueo de tráfico entrante internacional en pfBlockerNG*




*Nota.* En la Figura 113 se muestra la pestaña donde se puede bloquear el tráfico entrante internacional en pfBlockerNG.

**Figura 114**

*Widget de pfBlockerNG en el dashboard de pfSense*



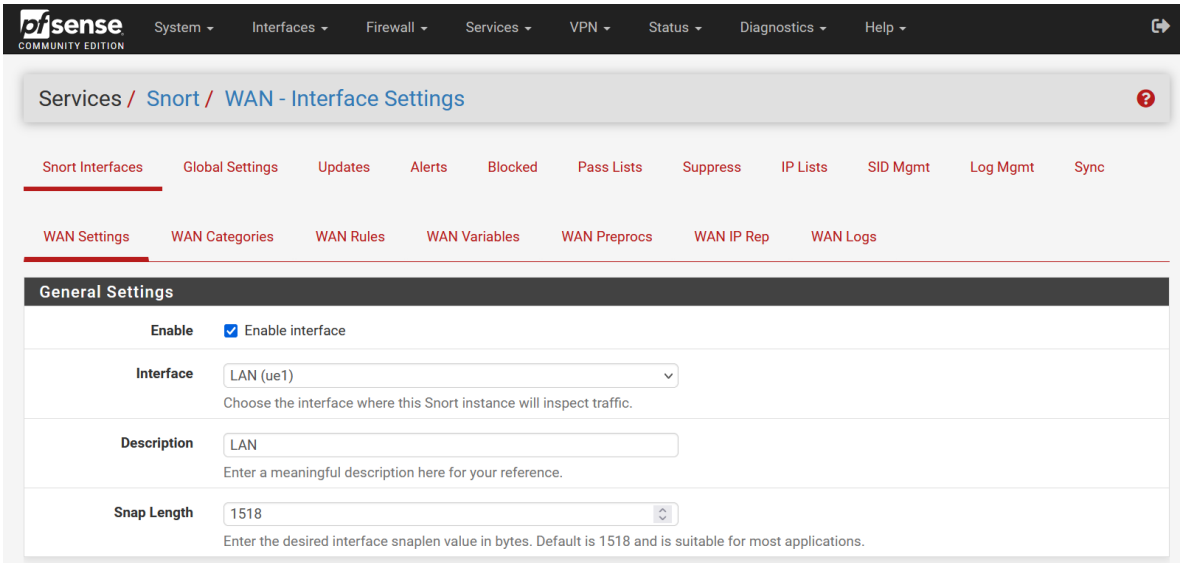

*Nota.* En la Figura 114 se muestra el widget de pfBlockerNG en el dashboard de pfSense donde se muestra el número de bloqueos.

### 3.3.13. Configuración de Snort

Snort es el sistema de prevención y detección de intrusiones que permitirá recibir alertas en caso de alguna amenaza a la red.

**Figura 115**

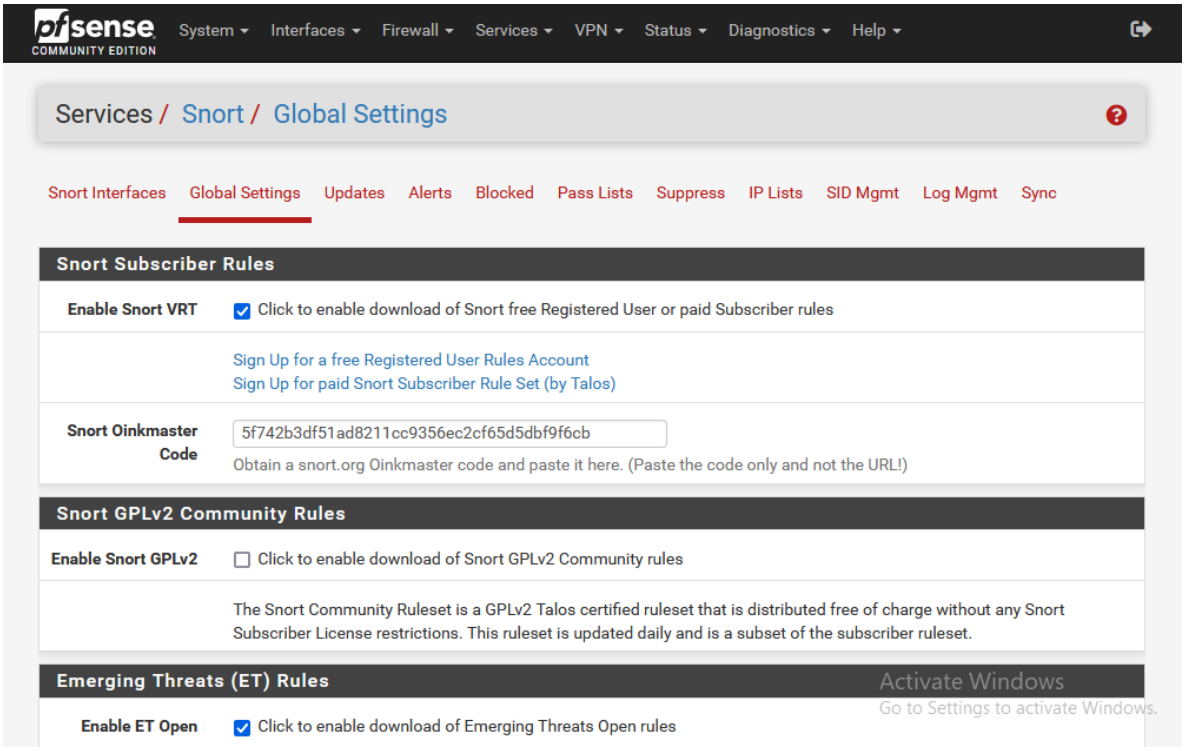
*Elección de interface para Snort*




*Nota.* En la Figura 115 se muestra la configuración de Snort, se escoge una interfaz en la que va a operar, en este caso es la red LAN.

**Figura 116**

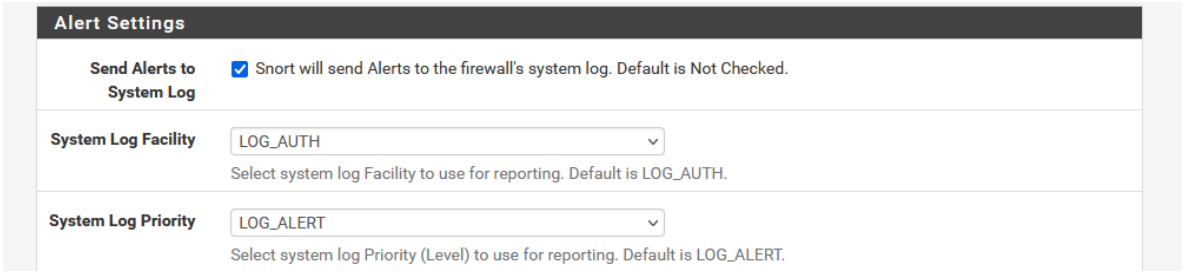
*Activación de Snort*




*Nota.* En la Figura 116 se muestra la activación de Snort. Se debe ingresar el “Oinkmaster Code” que se provee luego de haber creado una cuenta gratuita.

**Figura 117**

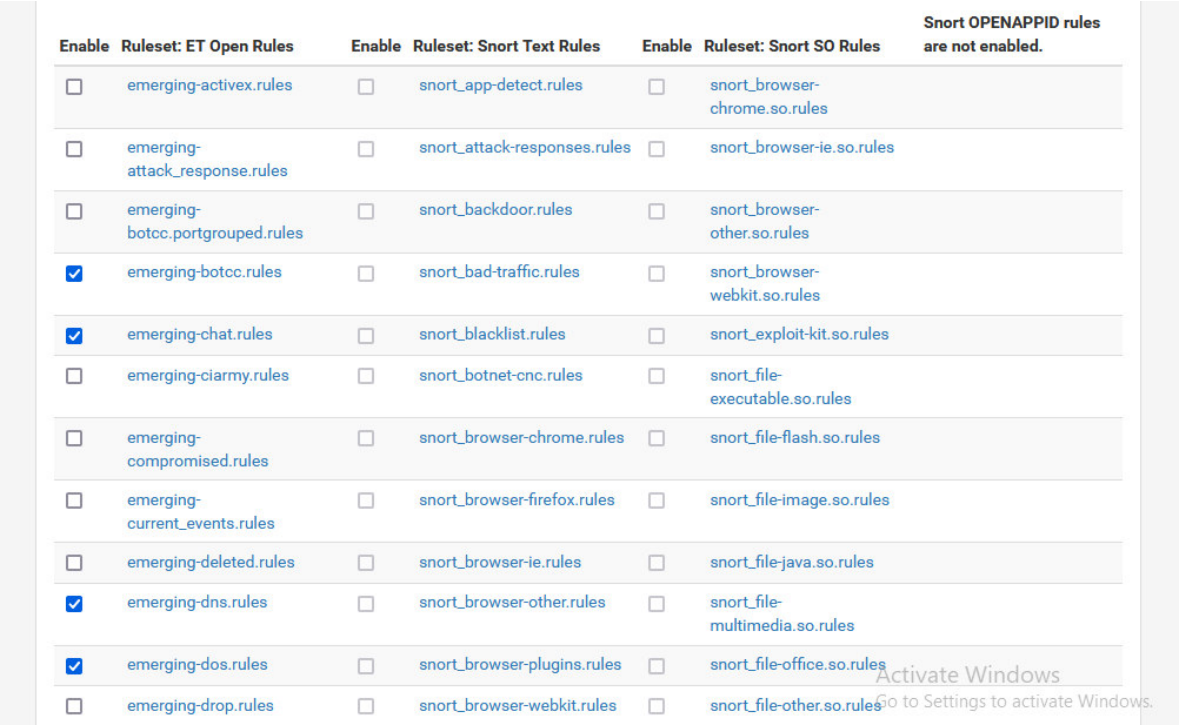
*Activación de enviado de alertas de parte de Snort*




*Nota.* En la Figura 117 se muestra la casilla que se debe marcar para que Snort envíe alertas al registro del sistema en caso que se detecte alguna intrusión.

**Figura 118**

*Configuración de reglas para Snort*



| Enable | Ruleset: ET Open Rules | Enable | Ruleset: Snort Text Rules | Enable | Ruleset: Snort SO Rules | Snort OPENAPPID rules are not enabled. |
|---|---|---|---|---|---|---|
| ☐ | emerging-activex.rules | ☐ | snort_app-detect.rules | ☐ | snort_browser-chrome.so.rules | |
| ☐ | emerging-attack_response.rules | ☐ | snort_attack-responses.rules | ☐ | snort_browser-ie.so.rules | |
| ☐ | emerging-botcc.portgrouped.rules | ☐ | snort_backdoor.rules | ☐ | snort_browser-other.so.rules | |
| ☑ | emerging-botcc.rules | ☐ | snort_bad-traffic.rules | ☐ | snort_browser-webkit.so.rules | |
| ☑ | emerging-chat.rules | ☐ | snort_blacklist.rules | ☐ | snort_exploit-kit.so.rules | |
| ☐ | emerging-ciarmy.rules | ☐ | snort_botnet-cnc.rules | ☐ | snort_file-executable.so.rules | |
| ☐ | emerging-compromised.rules | ☐ | snort_browser-chrome.rules | ☐ | snort_file-flash.so.rules | |
| ☐ | emerging-current_events.rules | ☐ | snort_browser-firefox.rules | ☐ | snort_file-image.so.rules | |
| ☐ | emerging-deleted.rules | ☐ | snort_browser-ie.rules | ☐ | snort_file-java.so.rules | |
| ☑ | emerging-dns.rules | ☐ | snort_browser-other.rules | ☐ | snort_file-multimedia.so.rules | |
| ☑ | emerging-dos.rules | ☐ | snort_browser-plugins.rules | ☐ | snort_file-office.so.rules | |
| ☐ | emerging-drop.rules | ☐ | snort_browser-webkit.rules | ☐ | snort_file-other.so.rules | |



*Nota.* En la Figura 118 se muestran las reglas para envío de alertas por los paquetes que coincidan con las reglas configuradas.

## 3.4. DESARROLLO DEL OBJETIVO ESPECIFICO 4

Procedimiento de simulación de la efectividad del diseño de la red de datos optimizada.

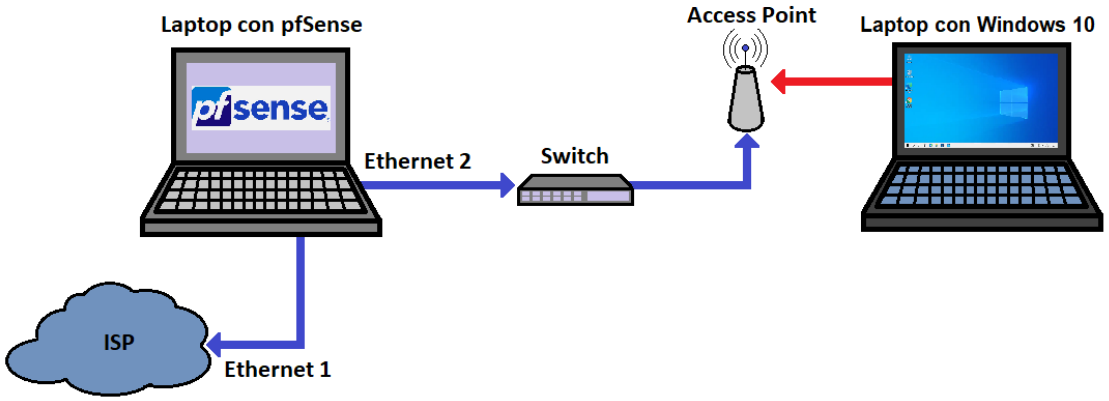
En el objetivo 4 se pasará a verificar el correcto funcionamiento de las reglas de firewall configuradas en pfSense, ya no se utilizará pfSense de manera virtualizada como máquina virtual en VirtualBox sino que se debe instalar pfSense como sistema operativo en una laptop que actuará como servidor y desde la cual se harán todas las conexiones para la simulación.

### 3.4.1. Elaboración de gráfico de simulación

Inicialmente debemos realizar un gráfico con todos los equipos que serán necesarios para realizar la simulación.

**Figura 119**

*Gráfico de la simulación*




*Nota.* En la Figura 119 se muestran los dispositivos que se utilizarán para la simulación y cómo serán conectados. El dispositivo principal es la laptop en donde se ha instalado pfSense como sistema operativo donde se encuentran todas las configuraciones de la red, esta laptop debe contar con dos puertos ethernet, un puerto se conecta al modem mediante el cual se recibe el servicio de internet del ISP (Internet Service Provider) y el otro puerto se debe conectar a un switch desde el cual se conecta el Access Point que permitirá que distintos dispositivos se conecten a la red a través

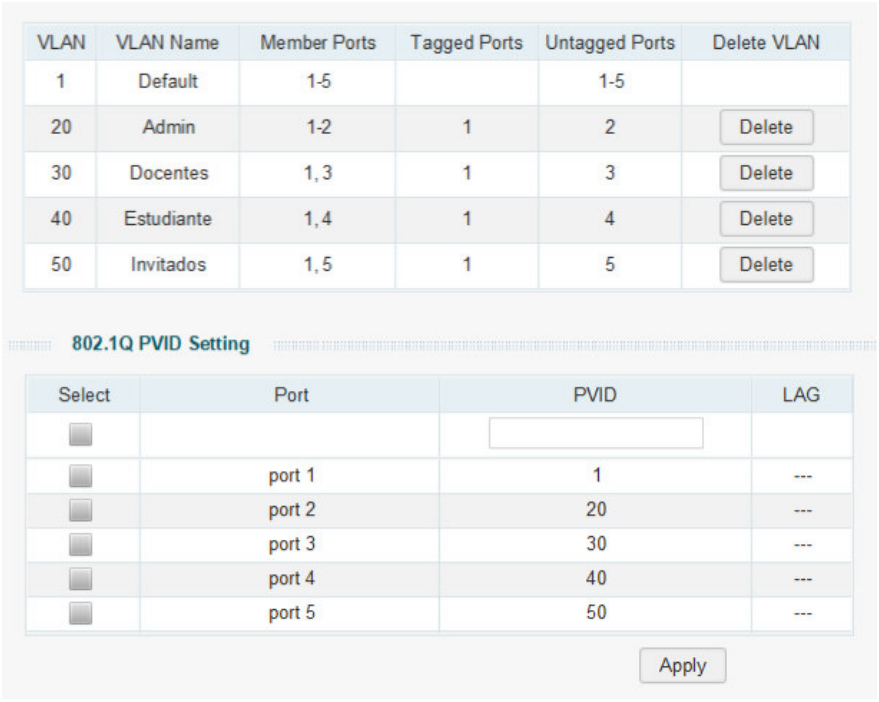
de pfSense. Para el presente trabajo se ha utilizado una laptop con Windows 10 para la verificación del correcto funcionamiento de las reglas establecidas en el firewall de pfSense; se realizarán pruebas de ping desde el Command Prompt de Windows 10 para verificar la conectividad.

### 3.4.2. Configuración del Switch

Antes de realizar las conexiones se debe configurar el switch que se va a utilizar, para el presente trabajo se ha utilizado el TP-LINK TL-SG105E de cinco puertos, el cual tiene la capacidad de ser configurado con las etiquetas de cada VLAN que se ha creado en pfSense.

**Figura 120**

*Configuración de switch en plataforma de TP-LINK*




*Nota.* En la figura 120 se muestra la configuración del switch realizada, se debe primeramente crear las VLANs con el protocolo 802.1Q en el switch, se escoge el puerto 1 como el puerto “uplink” por lo que debe estar “tagged” en cada VLAN, se les da nombres a cada una (Admin, Docentes, Estudiante e Invitados) y cada una debe tener el mismo PVID que se ha asignado en pfSense cuando se realizó la creación de las VLANs. Una vez creadas, se debe asignar cada PVID a un puerto en el switch, se asignó el puerto 2 a la VLAN 20, el puerto 3 a la VLAN 30, el puerto 4 a la VLAN 40 y el puerto 5 a la VLAN 50.

**Figura 121**

*Conexión de equipos*


*Nota.* En la Figura 121 se muestra la conexión realizada de los equipos para la simulación y las pruebas necesarias a la red para la comprobación de las reglas establecidas en el firewall de pfSense.

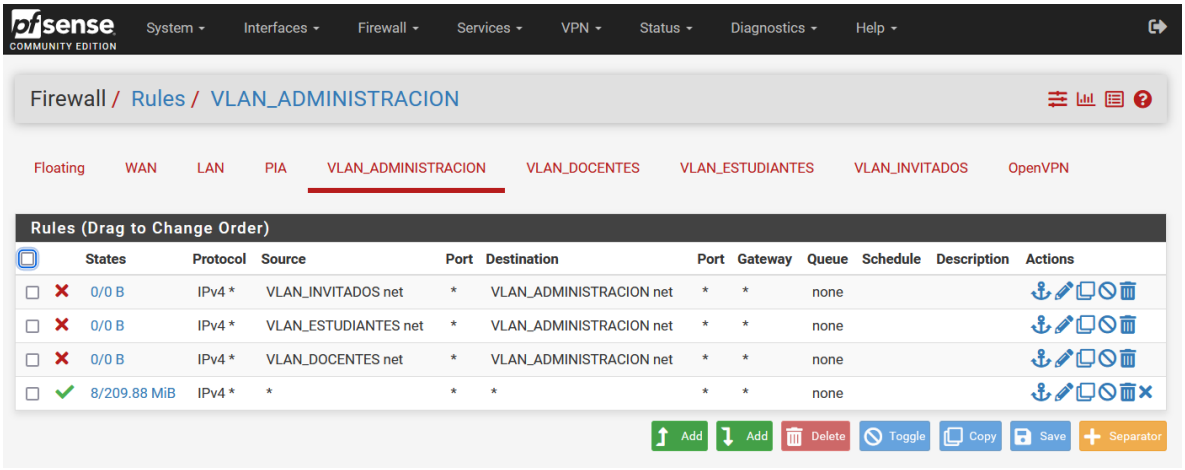
### 3.4.3. Verificación de reglas de firewall en las VLANs

Una vez configurado el switch, se realizan las conexiones de acuerdo al diagrama y se verifica el cumplimiento de las reglas del firewall de pfSense en cada VLAN. Para realizar las pruebas se conectó una laptop a cada puerto del switch para verificar cada VLAN.

- **VLAN 20 (Administración):** La VLAN 20 se configuró con la posibilidad de comunicarse con todas las demás VLANs sin restricción.

**Figura 122**

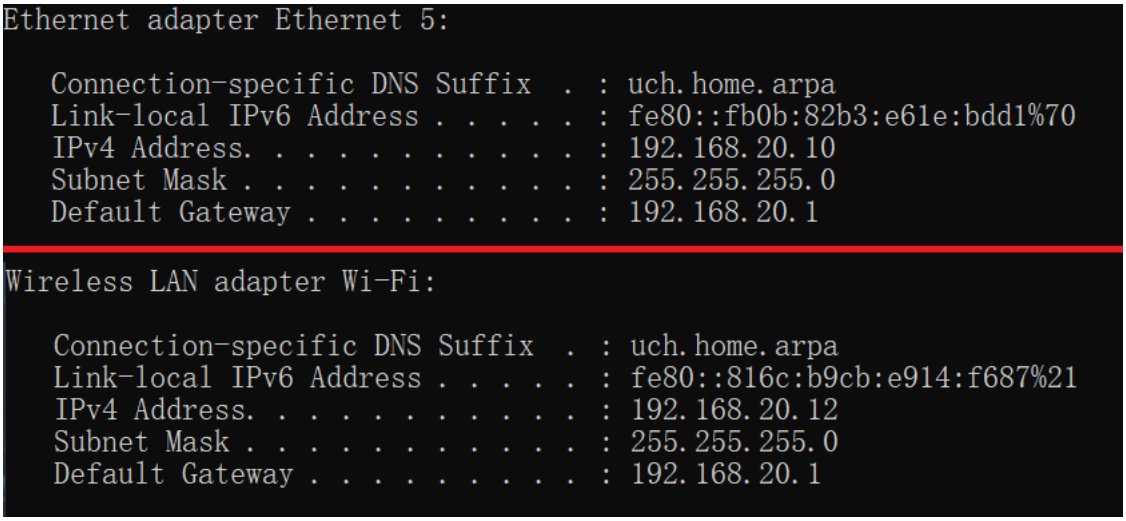
*Reglas de firewall establecidas para la VLAN 20*




*Nota.* En la Figura 122 se muestra la tabla de reglas de firewall para la VLAN 20.

**Figura 123**

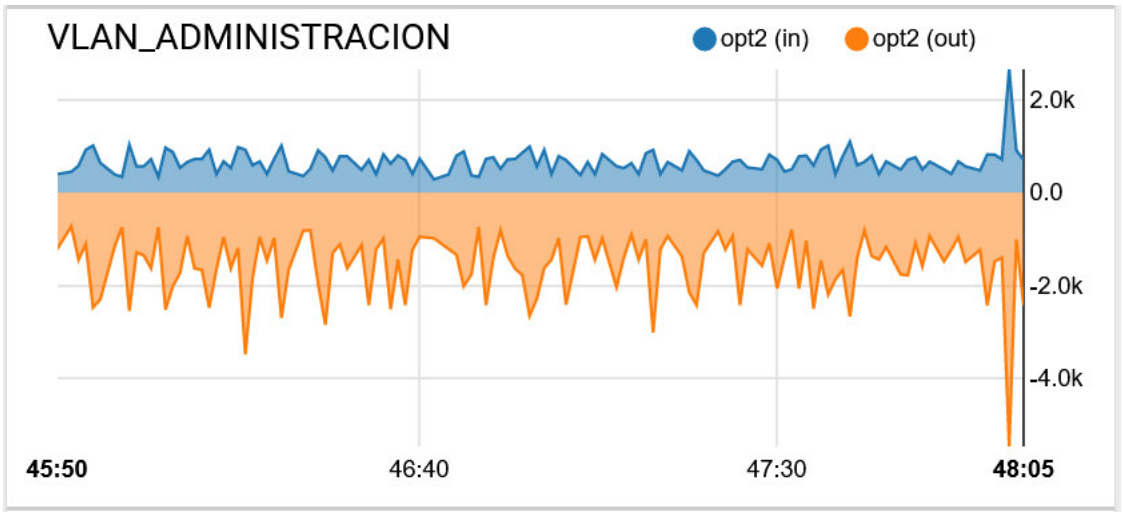
*Conexión a la VLAN 20*




*Nota.* En la Figura 123 se muestra la conexión de manera correcta al dominio creado de pfSense y con las direcciones IP del pool de DHCP creado en pfSense para la VLAN 20, 192.168.20.10 para la conexión a través de Ethernet directamente al switch y 192.168.20.12 para la conexión inalámbrica al Access Point. Se verifica la conexión a la VLAN 20 a través del puerto 2 del switch.

**Figura 124**

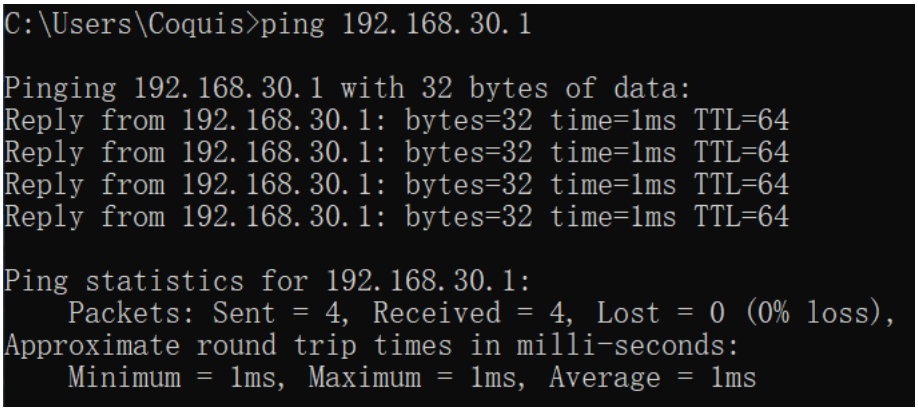
*Gráfica de tráfico de la VLAN 20 en pfSense*




*Nota.* En la Figura 124 se muestra la gráfica de trafico de la VLAN_ADMINISTRACION (VLAN 20) en el Dashboard de pfSense donde se comprueba el correcto flujo de datos en la VLAN 20.

**Figura 125**

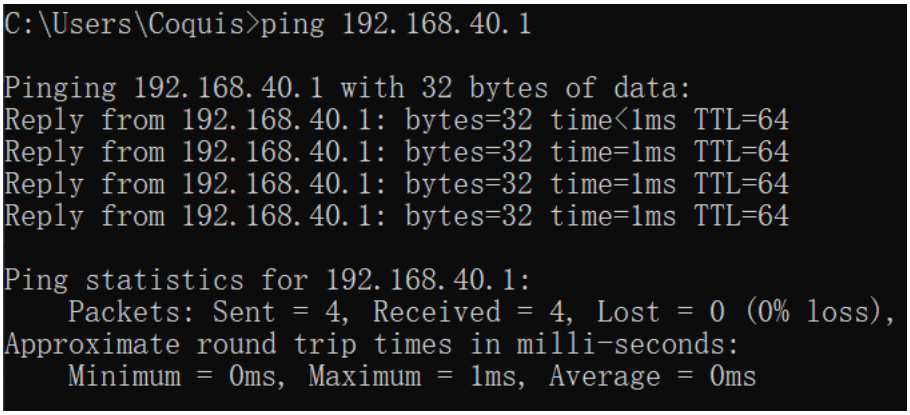
*Prueba de ping de la VLAN 20 a la VLAN 30 (Docentes)*




*Nota.* En la Figura 125 se muestra el resultado de la prueba al hacer ping desde la VLAN 20 a la VLAN 30 (VLAN_DOCENTES) donde se verifica que si hay conexión y se reciben todos los paquetes correctamente.

**Figura 126**

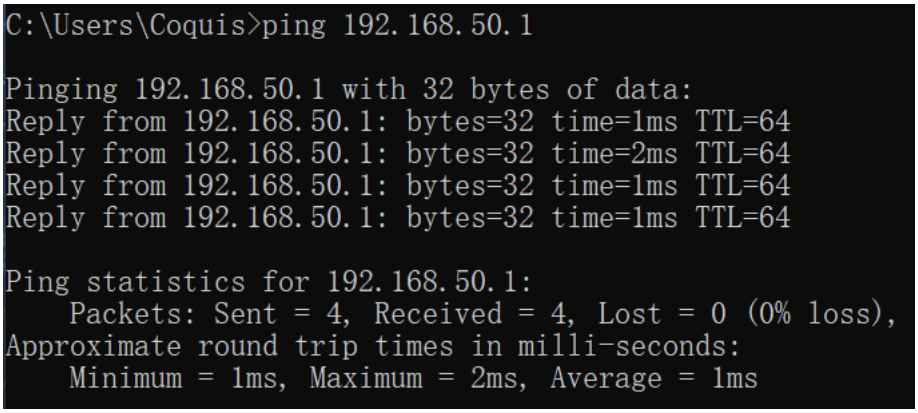
*Prueba de ping de la VLAN 20 a la VLAN 40 (Estudiantes)*




*Nota.* En la Figura 126 se muestra el resultado de la prueba al hacer ping desde la VLAN 20 a la VLAN 40 (VLAN_ESTUDIANTES) donde se verifica que si hay conexión y se reciben todos los paquetes correctamente.

**Figura 127**

*Prueba de ping de la VLAN 20 a la VLAN 50 (Invitados)*

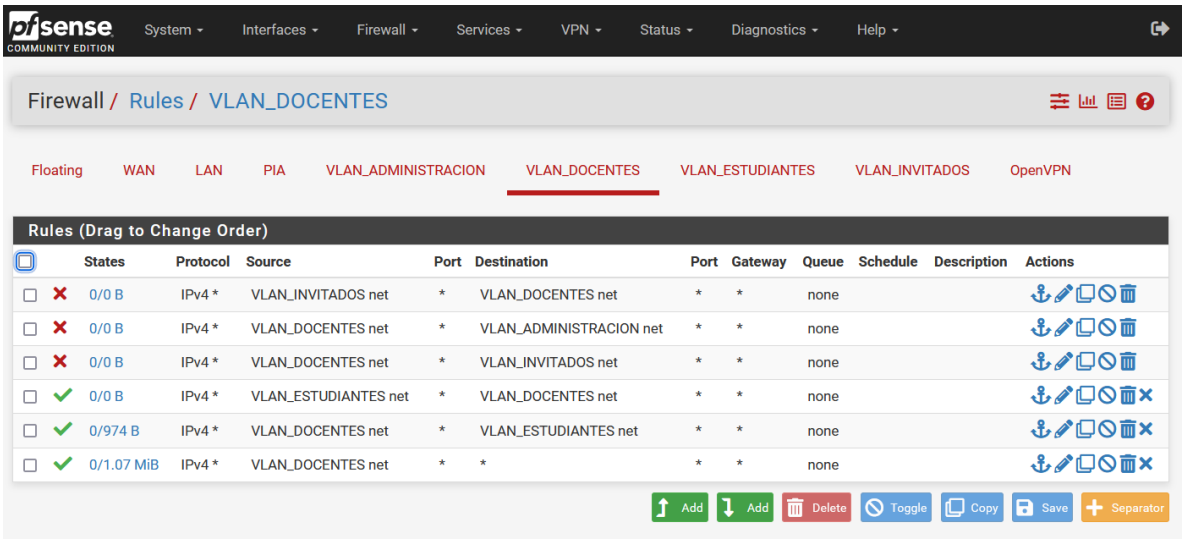



*Nota.* En la Figura 127 se muestra el resultado de la prueba al hacer ping desde la VLAN 20 a la VLAN 50 (VLAN_INVITADOS) donde se verifica que si hay conexión y se reciben todos los paquetes correctamente.

- **VLAN 30 (Docentes):** La VLAN 30 se configuró con la posibilidad de comunicarse únicamente con la VLAN 40 (Estudiantes), desde la VLAN_DOCENTES se bloqueó el tráfico hacia todas las demás VLANs.

**Figura 128**

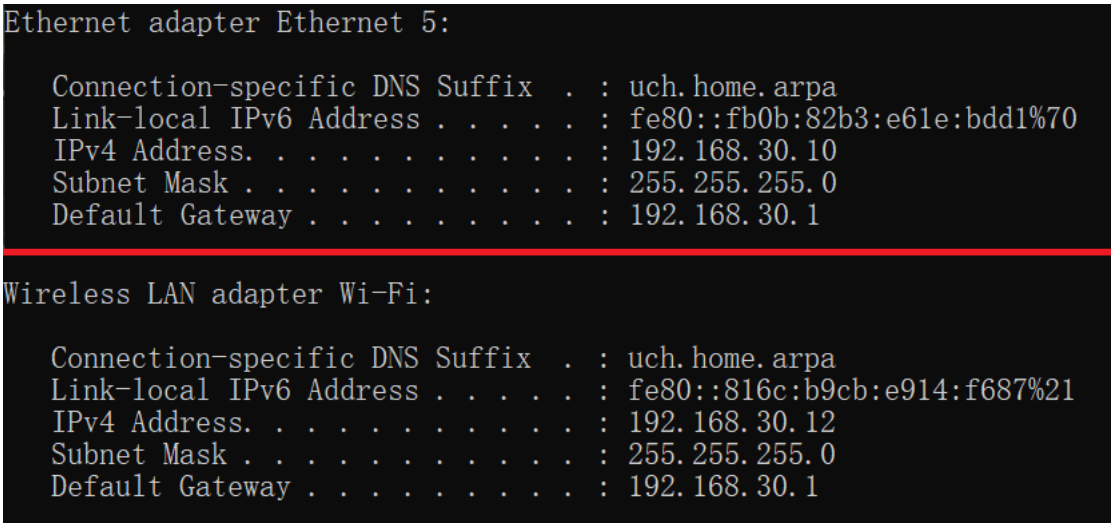
*Reglas de firewall establecidas para la VLAN 30*




*Nota.* En la Figura 128 se muestra la tabla de reglas de firewall para la VLAN 30

**Figura 129**

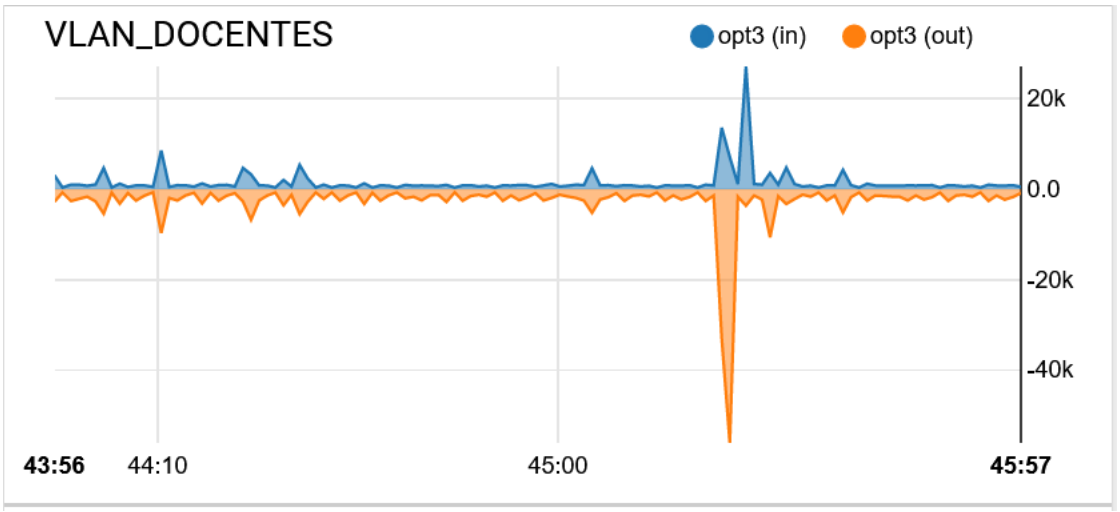
*Conexión a la VLAN 30*




*Nota.* En la Figura 129 se muestra la conexión de manera correcta al dominio creado de pfSense y con las direcciones IP del pool de DHCP creado en pfSense para la VLAN 30, 192.168.30.10 para la conexión a través de Ethernet directamente al switch y 192.168.30.12 para la conexión inalámbrica al Access Point. Se verifica la conexión a la VLAN 30 a través del puerto 3 del switch.

**Figura 130**

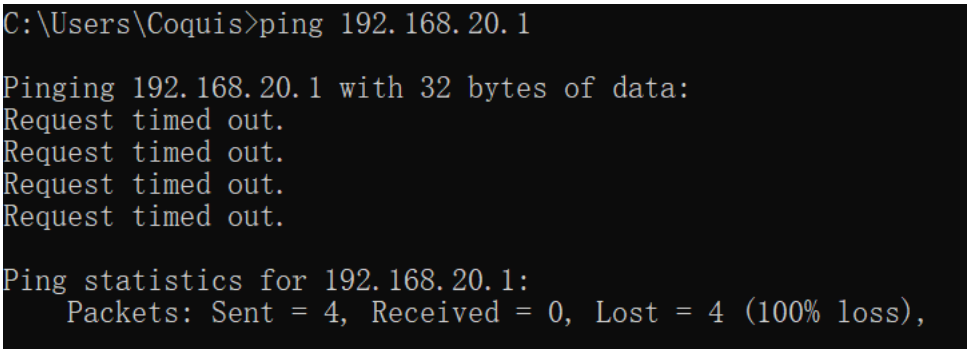
*Gráfica de tráfico de la VLAN 30 en pfSense*




*Nota.* En la Figura 130 se muestra la gráfica de trafico de la VLAN_DOCENTES (VLAN 30) en el Dashboard de pfSense donde se comprueba el correcto flujo de datos en la VLAN 30.

**Figura 131**

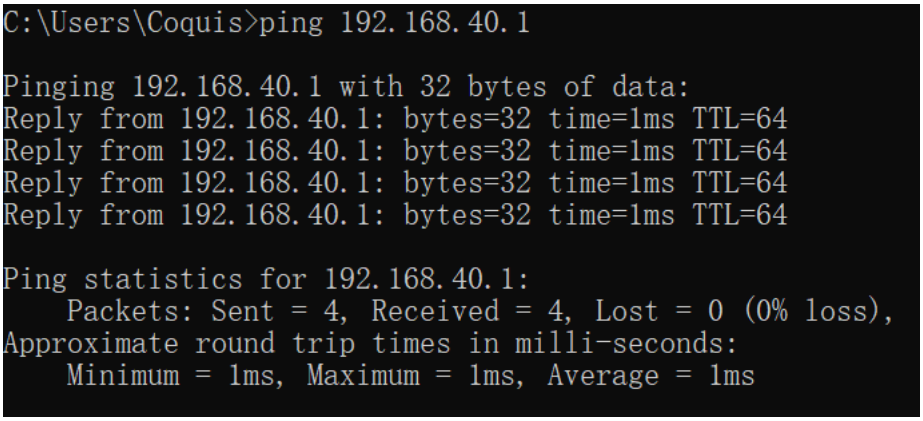
*Prueba de ping de la VLAN 30 a la VLAN 20 (Administración)*




*Nota.* En la Figura 131 se muestra el resultado de la prueba al hacer ping desde la VLAN 30 a la VLAN 20 (VLAN_ADMINISTRACION) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

**Figura 132**

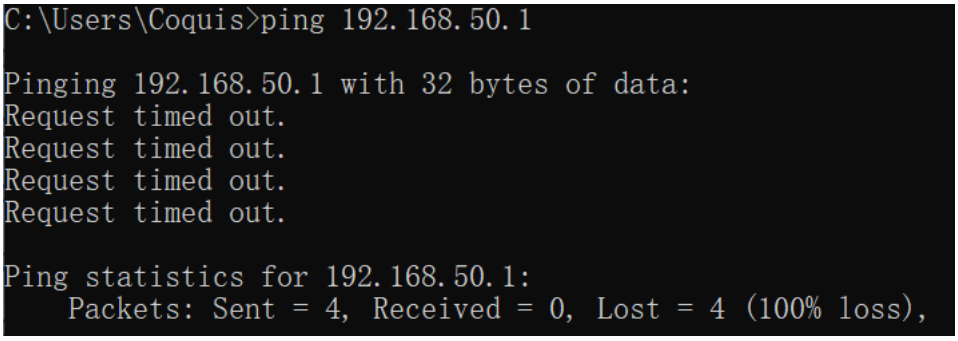
*Prueba de ping de la VLAN 30 a la VLAN 40 (Estudiantes)*




*Nota.* En la Figura 132 se muestra el resultado de la prueba al hacer ping desde la VLAN 30 a la VLAN 40 (VLAN_ESTUDIANTES) donde se verifica que sí hay conexión y se reciben todos los paquetes correctamente, de acuerdo con las reglas establecidas en el firewall de pfSense, debido a que esta es la única VLAN con la que se le ha permitido comunicación.

**Figura 133**

*Prueba de ping de la VLAN 30 a la VLAN 50 (Invitados)*

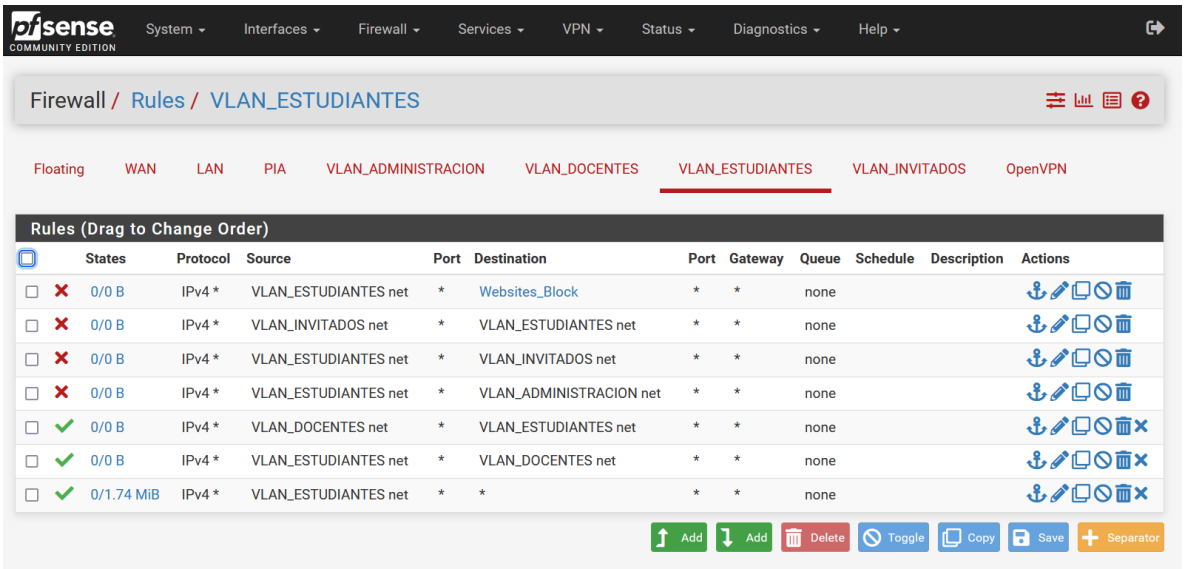



*Nota.* En la Figura 133 se muestra el resultado de la prueba al hacer ping desde la VLAN 30 a la VLAN 50 (VLAN_INVITADOS) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

- **VLAN 40 (Estudiantes):** La VLAN 40 se configuró con la posibilidad de comunicarse únicamente con la VLAN 30 (Docentes), desde la VLAN_ESTUDIANTES se bloqueó el tráfico hacia todas las demás VLANs.

**Figura 134**

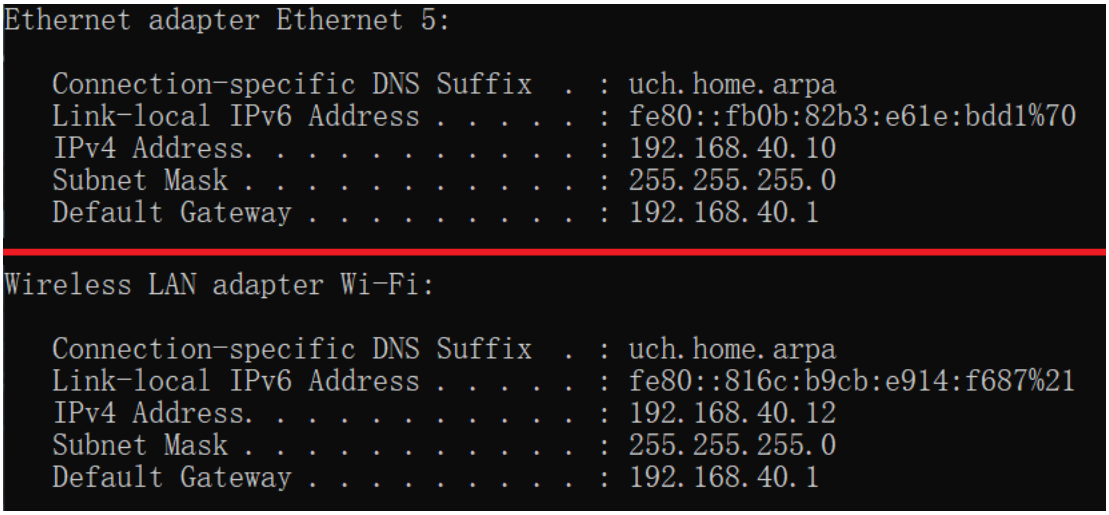
*Reglas de firewall establecidas para la VLAN 40*




*Nota.* En la Figura 134 se muestra la tabla de reglas de firewall para la VLAN 40

**Figura 135**

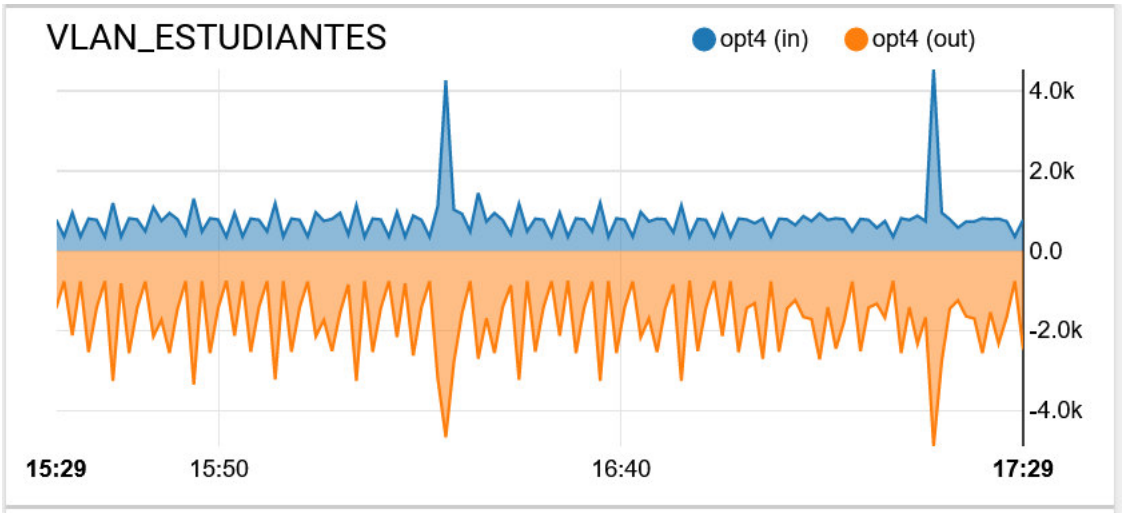
*Conexión a la VLAN 40*




*Nota.* En la Figura 135 se muestra la conexión de manera correcta al dominio creado de pfSense y con las direcciones IP del pool de DHCP creado en pfSense para la VLAN 40, 192.168.40.10 para la conexión a través de Ethernet directamente al switch y 192.168.40.12 para la conexión inalámbrica al Access Point. Se verifica la conexión a la VLAN 40 a través del puerto 4 del switch.

**Figura 136**

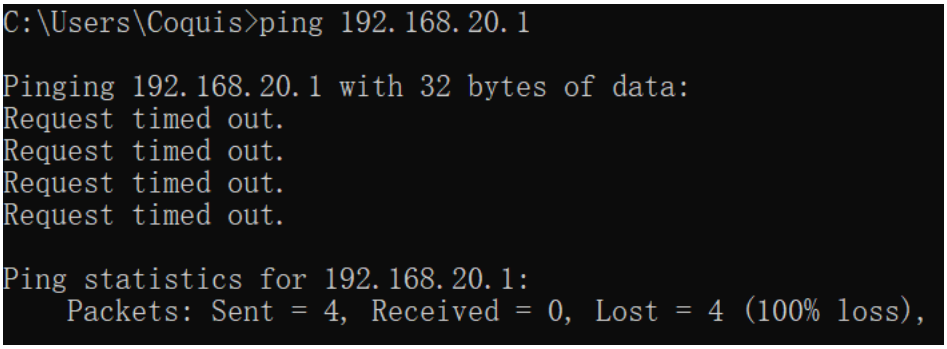
*Gráfica de tráfico de la VLAN 40 en pfSense*




*Nota.* En la Figura 136 se muestra la gráfica de trafico de la VLAN_ESTUDIANTES (VLAN 40) en el Dashboard de pfSense donde se comprueba el correcto flujo de datos en la VLAN 40.

**Figura 137**

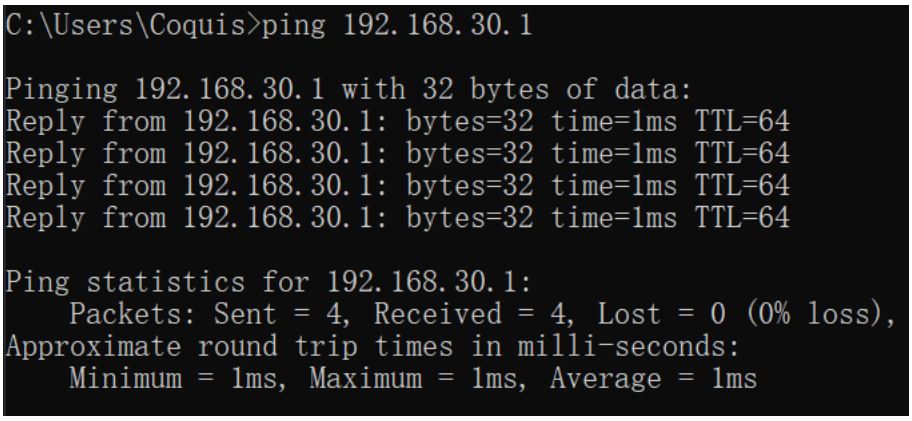
*Prueba de ping de la VLAN 40 a la VLAN 20 (Administración)*




*Nota.* En la Figura 137 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la VLAN 20 (VLAN_ADMINISTRACION) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

**Figura 138**

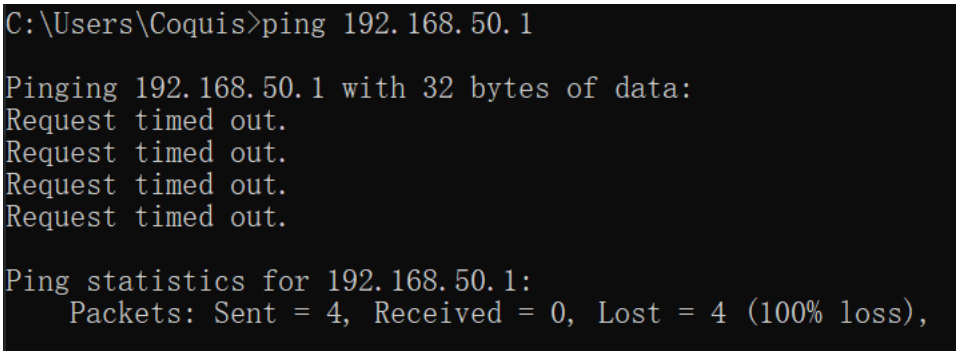
*Prueba de ping de la VLAN 40 a la VLAN 30 (Docentes)*




*Nota.* En la Figura 138 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la VLAN 30 (VLAN_DOCENTES) donde se verifica que sí hay conexión y se reciben todos los paquetes correctamente, de acuerdo con las reglas establecidas en el firewall de pfSense, debido a que esta es la única VLAN con la que se le ha permitido comunicación.

**Figura 139**

*Prueba de ping de la VLAN 40 a la VLAN 50 (Invitados)*




*Nota.* En la Figura 139 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la VLAN 50 (VLAN_INVITADOS) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

También se debe verificar que las páginas que se han bloqueado desde el firewall de pfSense para la VLAN_ESTUDIANTES no sean accesibles.

Primeramente, se debe verificar que existe conexión a internet, esto se realizó haciendo ping a la página del buscador de Google.

**Figura 140**

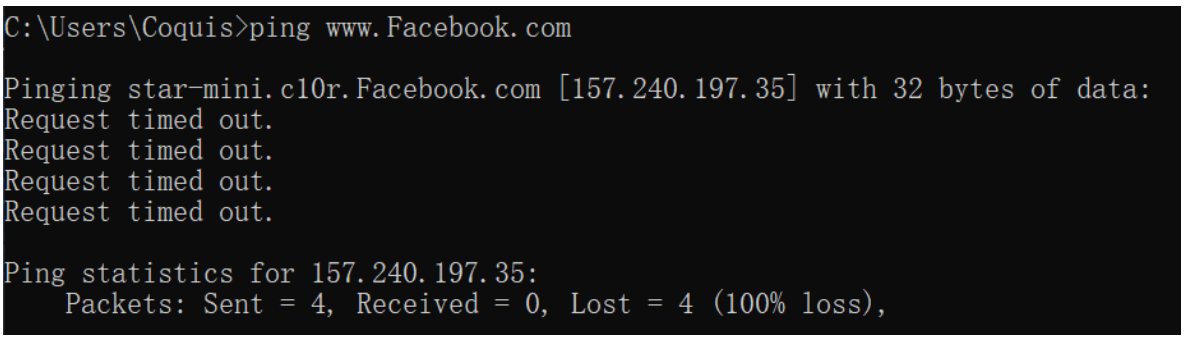
*Verificación de conexión a internet desde la VLAN 40*


*Nota.* En la Figura 140 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 al buscador www.Google.com donde se verifica que sí hay conexión y se reciben todos los paquetes correctamente de modo que se puede verificar que si hay conexión a internet.

Una vez que se ha comprobado la conexión a internet se puede pasar a verificar el bloqueo de las páginas indicadas en el firewall de pfSense (Facebook, Instagram y Twitter).

**Figura 141**

*Verificación bloqueo de Facebook para la VLAN 40*




*Nota.* En la Figura 141 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la página de Facebook (www.Facebook.com) donde se verifica que no hay conexión y que no es posible la conexión con esta página, de acuerdo con las reglas establecidas en el firewall de pfSense.

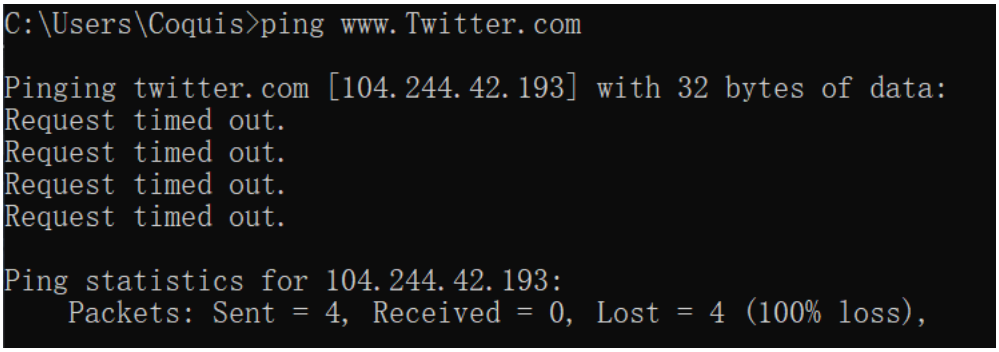
**Figura 142**

*Verificación bloqueo de Instagram para la VLAN 40*


*Nota.* En la Figura 142 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la página de Instagram (www.Instagram.com) donde se verifica que no hay conexión y que no es posible la conexión con esta página, de acuerdo con las reglas establecidas en el firewall de pfSense.

**Figura 143**

*Verificación bloqueo de Twitter para la VLAN 40*

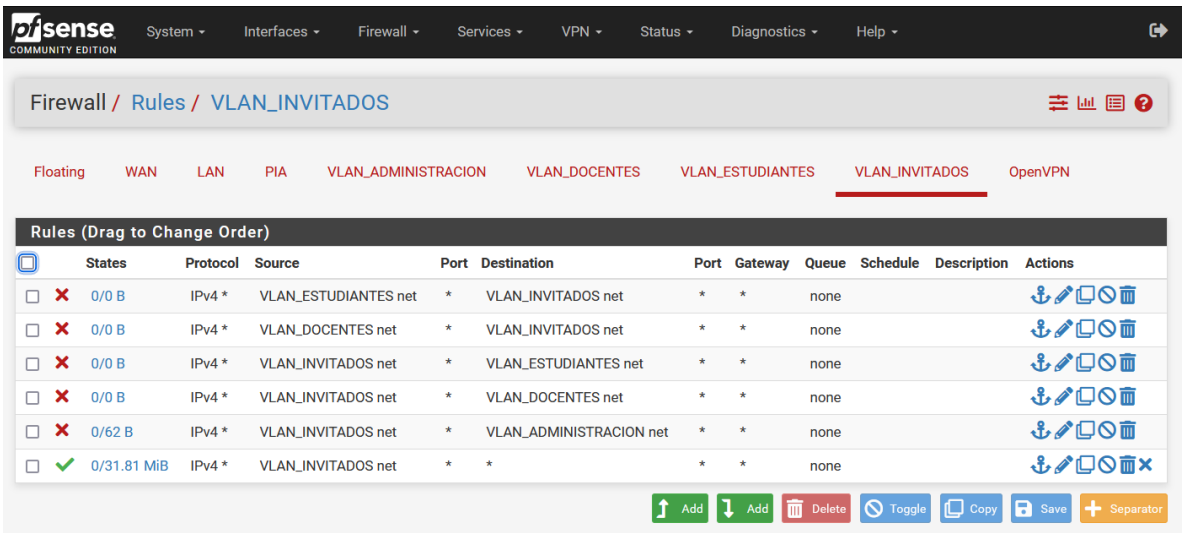



*Nota.* En la Figura 143 se muestra el resultado de la prueba al hacer ping desde la VLAN 40 a la página de Twitter (www.Twitter.com) donde se verifica que no hay conexión y que no es posible la conexión con esta página, de acuerdo con las reglas establecidas en el firewall de pfSense.

- **VLAN 50 (Invitados):** La VLAN 50 se configuró sin la posibilidad de comunicarse con ninguna de las demás VLANs, desde la VLAN_INVITADOS se bloqueó el tráfico hacia todas las demás VLANs.

**Figura 144**

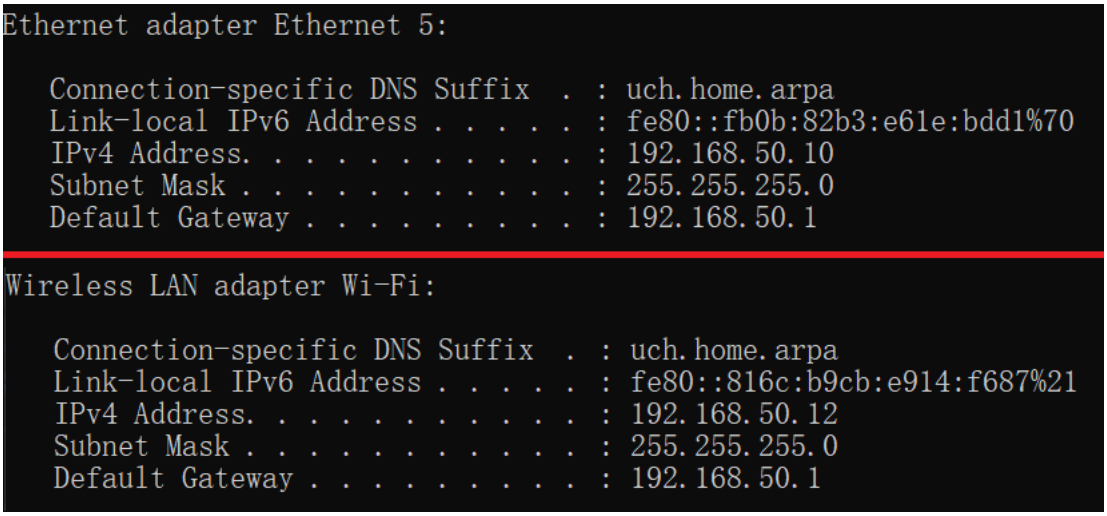
*Reglas de firewall establecidas para la VLAN 50*




*Nota.* En la Figura 144 se muestra la tabla de reglas de firewall para la VLAN 50

**Figura 145**

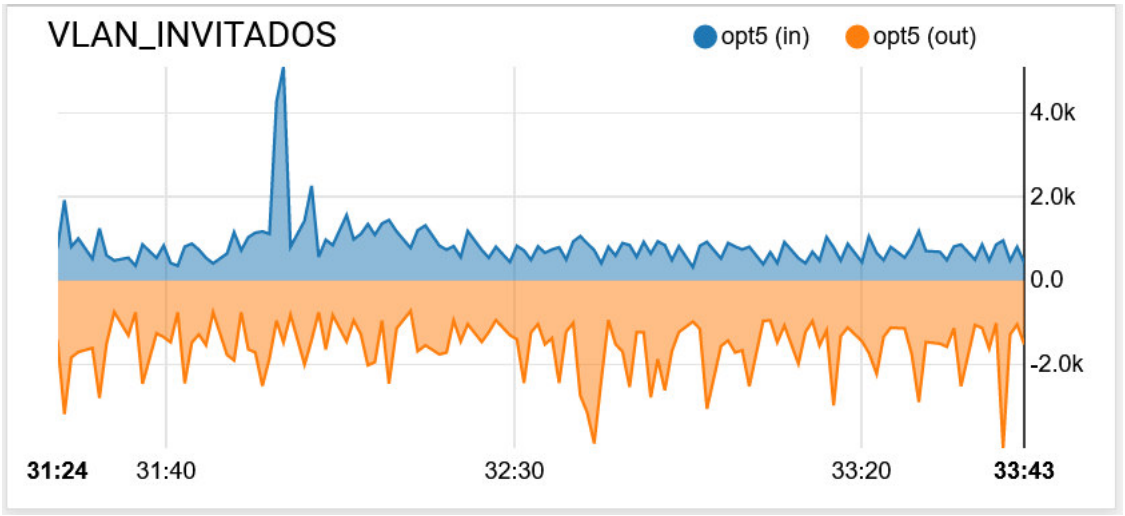
*Conexión a la VLAN 50*




*Nota.* En la Figura 145 se muestra la conexión de manera correcta al dominio creado de pfSense y con las direcciones IP del pool de DHCP creado en pfSense para la VLAN 50, 192.168.50.10 para la conexión a través de Ethernet directamente al switch y 192.168.50.12 para la conexión inalámbrica al Access Point. Se verifica la conexión a la VLAN 50 a través del puerto 5 del switch.

**Figura 146**

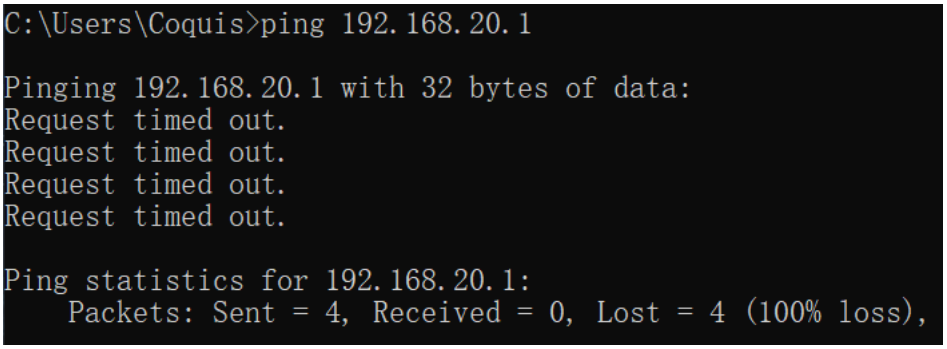
*Gráfica de tráfico de la VLAN 50 en pfSense*




*Nota.* En la Figura 146 se muestra la gráfica de trafico de la VLAN_INVITADOS (VLAN 50) en el Dashboard de pfSense donde se comprueba el correcto flujo de datos en la VLAN 50.

**Figura 147**

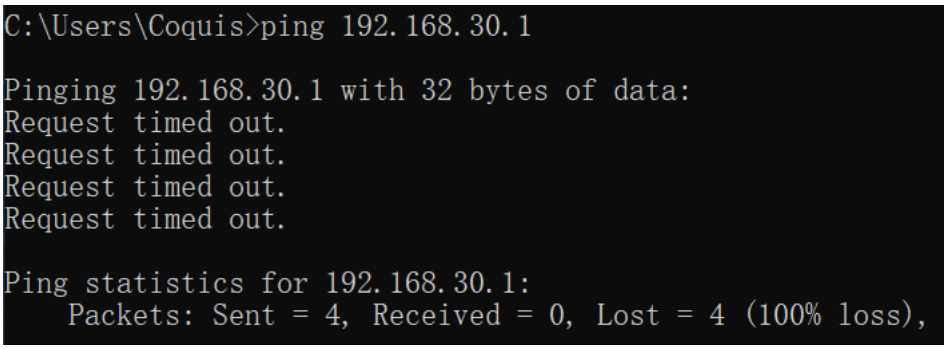
*Prueba de ping de la VLAN 50 a la VLAN 20 (Administración)*




*Nota.* En la Figura 147 se muestra el resultado de la prueba al hacer ping desde la VLAN 50 a la VLAN 20 (VLAN_ADMINISTRACION) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

**Figura 148**

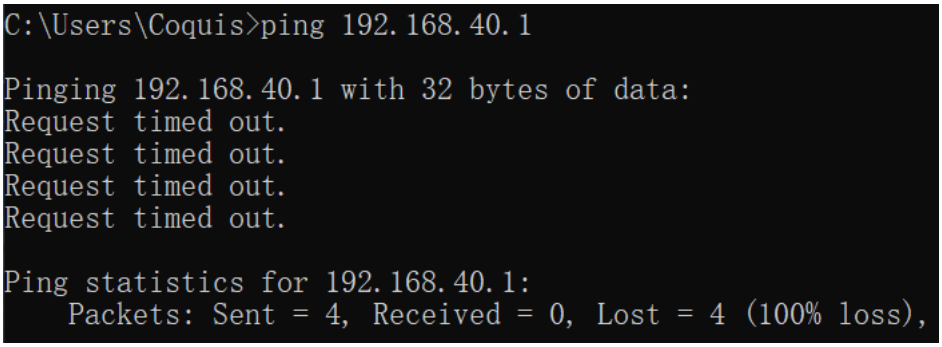
*Prueba de ping de la VLAN 50 a la VLAN 30 (Docentes)*




*Nota.* En la Figura 148 se muestra el resultado de la prueba al hacer ping desde la VLAN 50 a la VLAN 30 (VLAN_DOCENTES) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

**Figura 149**

*Prueba de ping de la VLAN 50 a la VLAN 40 (Estudiantes)*




*Nota.* En la Figura 149 se muestra el resultado de la prueba al hacer ping desde la VLAN 50 a la VLAN 40 (VLAN_ESTUDIANTES) donde se verifica que no hay comunicación en esa dirección, en concordancia con las reglas establecidas en el firewall de pfSense.

# CAPÍTULO IV: ANÁLISIS DE COSTO Y BENEFICIO

## 4.1. Análisis de costos

### 4.1.1. Recursos Humanos

Aquí se toma en cuenta en cuenta el costo de cada profesional en el proyecto. Durante el desarrollo del proyecto se necesitaron capacitaciones en algunos temas para poder completar todas las etapas de manera satisfactoria alcanzando los resultados buscados. A continuación, se da a conocer la tabla donde se indicarán los costos de forma detallada.

**Tabla 1**

*Gasto de recursos humanos del proyecto*

| CAPACITACION | TIEMPO | TARIFA POR MES | SUB TOTAL |
|---|---|---|---|
| Capacitación sobre VirtualBox | 1 MES | S/.750 | S/.750 |
| **TOTAL** | | | **S/. 750** |

*Nota.* En la Tabla 1, se dan a conocer los gastos por servicios de capacitación en distintos programas utilizados en el desarrollo del proyecto, tomando en cuenta que VirtualBox es la solución de software de virtualización que se ha elegido para el presente trabajo, es de gran importancia estar al tanto de todas las herramientas que este brinda para poder desarrollar la simulación del diseño de manera correcta y visualizar el funcionamiento para determinar su efectividad y viabilidad.

### 4.1.2. Recursos de Hardware

Aquí se toma en cuenta el costo que se genera por la compra de equipos de hardware para el desarrollo del proyecto, estas herramientas serán útiles para evitar los inconvenientes y disminuir el tiempo de desarrollo.

**Tabla 2**

*Gasto de recursos de Hardware del proyecto*

| | CANTIDAD | PRECIO POR UNIDAD | SUB TOTAL |
|---|---|---|---|
| **LAPTOP ASUS** | 1 | S/.3500 | S/.3500 |
| **USB Flash drive 128 MB** | 1 | S/.90 | S/.90 |
| **Access Point** | 1 | S/.100 | S/.100 |
| **TOTAL** | | | **S/3690** |

*Nota.* En la Tabla 2, se detallan los costos de los equipos que forman parte del hardware utilizado para el desarrollo del proyecto, se necesitó una laptop para hacer la instalación de los programas respectivos además de un USB Flash Drive para realizar la instalación de pfSense en el medio a través del cual se realizó la simulación con el Access Point del esquema de red propuesto.

### 4.1.3. Recursos de Software

Aquí se mencionan los programas que se han utilizado para el desarrollo del proyecto juntamente con el costo por cada uno seguido del costo total. En su mayoría, los productos de Software utilizados para el presente proyecto pueden ser adquiridos sin ningún costo, así como se detalla a continuación.

**Tabla 3**

*Gasto de recursos de Software del proyecto*

| | DESCRIPCIÓN | CANTIDAD | PRECIO POR UNIDAD | SUB TOTAL |
|---|---|---|---|---|
| **VirtualBox** | Licencia *free* | 1 | 0 | 0 |
| **pfSense** | Licencia *free* | 1 | 0 | 0 |

| | | | | |
|---|---|---|---|---|
| **Windows 10** | Licencia *free* | 1 | 0 | 0 |
| **Ubuntu** | Licencia *free* | 1 | 0 | 0 |
| **Private Internet Access** | VPN | 1 | S/.44.41 (un mes) | S/.44.41 |
| **TOTAL** | | | | **S/ 44.41** |

*Nota.* En la Tabla 3, se muestran los programas utilizados para la realización del proyecto, la mayoría de estos productos de software son libres, por este motivo no han representado un costo agregado al total. Unicamente se ha realizado el pago de $11.95(S/.44.41) por un mes de VPN (Private Internet Access).

### 4.1.4. Otros gastos

Aquí se toma en cuenta productos o servicios de costo variable que se han utilizado para el desarrollo del proyecto.

**Tabla 4**

*Gastos de costos variables*

| | **GASTO POR MES** | **MESES** | **SUB TOTAL** |
|---|---|---|---|
| **Servicio de Internet** | S/.80 | 6 MESES | S/.480 |
| **Transporte** | S/.24 | 6 MESES | S/.144 |
| **TOTAL** | | | **S/.624** |

*Nota.* En la Tabla 4, se detallan otros costos que han sido necesarios para poder concretar el presente proyecto en totalidad.

### 4.1.5. Costos de Desarrollo

El desarrollo del proyecto tiene un costo monetario que es el resultado de la suma de los costos de recursos humanos, hardware y software.

**Tabla 5**

*Gasto general de desarrollo del proyecto*

| Descripción de actividad | MONTO |
|---|---|
| **Total de Recursos Humanos** | S/.750 |
| **Total de Hardware** | S/.3690 |
| **Total de Software** | S/.44.45 |
| **Total de Costos Variables** | S/.624 |
| **TOTAL** | **S/. 5108.45** |

*Nota.* En la Tabla 5 se muestra el costo total para el desarrollo del proyecto.

## 4.2. Análisis de Beneficios

### 4.2.1. Beneficios tangibles

- pfSense, al ser un software libre, permite la reducción de costos de configuración de la red de datos para adquirir el programa inicial y también para las actualizaciones y paquetes adicionales ya que no tienen ningún costo.
- Permite escoger de una variedad más grande de hardware que se adapte a las especificaciones de la red y realizar cambios a voluntad sin depender de un solo proveedor.

### 4.2.2. Beneficios intangibles

- pfSense permite escoger entre un gran número protocolos de VPN que pueden ser configurados fácilmente desde la interfaz gráfica de usuario.
- Permite instalar paquetes adicionales de IDS y IPS que incrementan la seguridad en la red como Suricata o Snort.

## 4.3. ANÁLISIS DE SENSIBILIDAD

### 4.3.1. Desarrollo de flujo de caja

En la Tabla 6, se realiza el cálculo del flujo de caja de los primeros cuatro años, tomando en cuenta el gasto de recursos y la inversión inicial. Para el cálculo de los recursos de software se tomó en cuenta el precio por el plan de 3 años y tres meses que brinda Private Internet Access por $79.00 (S/.293.84), debido a que es el plan que se utilizaría a largo plazo.

**Tabla 6**

*Flujo de caja del proyecto*

| AÑOS | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| | BENEFICIO | | | |
| BENEFICIO CON PFSENSE | S/.1605,13 | S/.1605,13 | S/.1605,13 | S/.1605,13 |
| | EGRESOS | | | |
| INVERSIÓN INICIAL | S/. 5357.84 | | | |
| RECURSOS HUMANOS | S/.750 | | | |
| RECURSOS HARDWARE | S/.3690 | | | |
| RECURSOS DE SOFTWARE | S/.293.84 | | | S/.293.84 |
| GASTOS EXTRAS | S/.624 | | | |
| TOTAL DE EGRESO | S/. 5357.84 | S/.0 | S/.0 | S/.293.84 |
| SUMATORIA (BENEFICIO-EGRESO) | -3,752.71 | S/.1605,13 | S/.1605,13 | S/.1311.29 |
| GANANCIA | -3,752.71 | -2147.58 | -542.45 | S/. 768.84 |

*Nota.* En la Tabla 6 se muestra el flujo de caja del proyecto, y se aprecia que a partir del cuarto año desde haber realizado la inversión inicial se comienza a tener una ganancia.

### 4.3.2. Análisis de VAN

Se pasará a calcular el Valor Actual Neto (VAN) del desarrollo de la tesis, los valores que se utilizan para los siguientes cálculos se toman del flujo de caja realizado.

Información:

- Tiempo(t) = 4 años
- Inversión inicial ($I_o$) = S/.5357.84
- Tasa de interés (i) = 5%
  La fórmula para calcular el VAN es:

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{V_t}{(1+k)^n}$$

$$VAN = \text{ S/.92.13}$$

### 4.3.3. Análisis de TIR

Luego se calculará la Tasa de Interés de Retorno (TIR), este valor se calcula a partir del resultado obtenido de VAN.

$$VAN = \sum_{t=1}^{n} \frac{F_t}{(1+TIR)^t} - I = 0$$

Se debe conseguir la tasa de interés que haga que la VAN sea igual a cero.

La fórmula para el cálculo del análisis de TIR:

$$TIR = \frac{-I + \sum_{i=1}^{n} F_i}{\sum_{i=1}^{n} i * F_i}$$

Información:

- Tiempo(t) = 4 años
- Inversión inicial ($I_o$) = S/.5357.84
- Tasa de interés (i) =5%

Resultado:

TIR= 0.0576
TIR= 5.76%

### 4.3.4. Análisis de retorno de inversión (R.O.I.)

Esta cifra permite medir el rendimiento de una inversión para dar una idea de cuánta efectividad se tiene en base al monto que se desea invertir, el cálculo se realizó tomando en cuenta la ganancia que se espera recibir en un periodo de cuatro años desde la inversión inicial.

R.O.I. = 14.3%

Para calcular el R.O.I. se tomó en cuenta lo siguiente:

R.O.I. = (Ganancias – Inversión) /Inversión

## Conclusiones

- En primer lugar, se logró determinar la situación actual de la red de datos de la Universidad de Ciencias y Humanidades, donde se pudo mostrar el sistema que se utiliza actualmente a nivel de software y los equipos utilizados para el despliegue de la red.
- Además, se logró conocer la topología y la arquitectura de la red de datos de la Universidad de Ciencias y Humanidades, se presentaron las marcas de los equipos utilizados y sus especificaciones, también se mostró cómo está dado el despliegue de estos equipos en el campus de la universidad.
- De igual manera, se logró diseñar un modelo de red de datos para optimizar el servicio de la red de datos de la Universidad de Ciencias y Humanidades, se realizó la configuración de pfSense y se dividió la red en cuatro redes virtuales de área local para el personal administrativo, profesores, alumnos e invitados.
- Del mismo modo, se logró realizar la simulación de la efectividad del diseño de la red de datos optimizada con el uso de una laptop donde se instaló pfSense con las configuraciones realizadas en VirtualBox para simular el despliegue de la red diseñada.
- Finalmente, se concluye que si se logró diseñar y planificar la transición del protocolo Ruckus Wireless al protocolo pfSense para optimizar el servicio de red de datos de la Universidad de Ciencias y Humanidades. Con el protocolo pfSense se muestra un beneficio en el costo del sistema de la red, permite usar un número más amplio de marcas y productos de acuerdo con las necesidades de la red y permite mantener un alto nivel de seguridad.

## Recomendaciones

- En primer lugar, se recomienda hacer un seguimiento de las actualizaciones disponibles en el software de pfSense para mantener siempre un alto nivel de seguridad.

- En segundo lugar, se recomienda el uso de contraseñas de alta seguridad para acceder al sistema en el Dashboard de pfSense para mantener toda la información resguardada.

- Por último, se recomienda utilizar equipos de hardware diseñados para redes grandes que permiten más escalabilidad y proveen más seguridad a la red.

## Referencias


Aggarwal, M. (2018). *Network Security with pfSense: Architect, deploy, and operate enterprise-grade firewalls*. Packt Publishing Ltd. https://bit.ly/3N8emeV

Alazab, M., RM, S., M, P., Maddikunta, P., Gadekallu, T., y Pham, Q. V. (2021, octubre). Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics*, *18*(5), 3501-3509. http://doi.org/10.1109/TII.2021.3119038

Alcántara, J. (2017). *Diseño e implementación de aplicación multiplataforma móvil con funciones de encriptamiento y privacidad de datos orientada a la seguridad estuantil de la Universidad de Ciencias y Humanidades, distrito-Los Olivos 2014.* [Tesis de licenciatura, Universidad de Ciencias y Humanidades]. Repositorio Universidad de Ciencias y Humanidades. https://repositorio.uch.edu.pe/handle/20.500.12872/159

Ali, S., Osman, T., Mannan, M., y Youssef, A. (2019). On privacy risks of public wifi captive portals. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14* (pp. 80-98). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-31500-9_6

Almidón, C. (2019). *Redes virtuales locales (VLAN) en la seguridad de la información de la red de datos de la Universidad Nacional de Huancavelica.* [Tesis doctoral, Universidad Nacional del Centro del Perú]. Repositorio de la Universidad Nacional del Centro del Perú. https://repositorio.uncp.edu.pe/handle/20.500.12894/6693

Amazon (2023a). *HP ProCurve 1910 – 24 G Switch*. https://www.amazon.com/-

/es/ProCurve-1910-Switch-je006-ABA/dp/B003UL531W

Amazon (2023b). *Hewlett Packard Enterprise HPE OfficeConnect 1920S 24G 2SFP Switch*. https://www.amazon.com/-/es/Hewlett-Packard-Enterprise-OfficeConnect-Switch/dp/B06Y192XQ7

Amazon (2023c). *Hewlett Packard Enterprise 1920-48G-PoE+ Gigabit Ethernet (10/100/1000) Energía sobre Ethernet (PoE)*. https://www.amazon.es/Hewlett-Packard-Enterprise-1920-48G-PoE-Ethernet/dp/B00TWIAPDS

Aremu, A., Shahzad, A., y Hassan, S. (2018). Determinants of Enterprise Resource Planning adoption on organizations' performance among medium enterprises. *LogForum*, *14*(2). https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-1d1677a2-5ada-4c9e-8709-f45dc608b569

Ayala Bendezu, C. (2023). *Portal cautivo para administrar la seguridad de datos de la red inalambrica del IESTP San Pedro*. [Tesis de licenciatura, Universidad Peruana Los Andes]. Repositorio Institucional de la Universidad Peruana Los Andes. https://repositorio.upla.edu.pe/handle/20.500.12848/5441

Azamuddin, W., Hassan, R., Aman, A., Hasan, M., y Al-Khaleefa, A. (2020). Quality of service (Qos) management for local area network (LAN) using traffic policy technique to secure congestion. *Computers*, *9*(2), 39. https://doi.org/10.3390/computers9020039

Baltes, S., y Ralph, P. (2022). Sampling in software engineering research: A critical review and guidelines. *Empirical Software Engineering*, *27*(4), 94. https://link.springer.com/article/10.1007/s10664-021-10072-8

Bertsekas, D., y Gallager, R. (2021). *Data networks*. Athena Scientific. https://books.google.com.pe/books?hl=es&lr=&id=4-hFEAAAQBAJ&oi=fnd&pg=PR1&dq=data+network&ots=7TU5Mo2MjR&sig=eB9vglQwwQkHZnfOKoHBvrosSwY&redir_esc=y#v=onepage&q=data%20network&f=false

Bishop, M. (2004). Introduction to Computer Security. Pearson Education. http://www.uoitc.edu.iq/images/documents/informatics-institute/exam_materi als/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf

Boos, K., Liyanage, N., Ijaz, R., y Zhong, L. (2020). Theseus: an experiment in operating system structure and state management. In *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)* (pp. 1-19). https://www.usenix.org/conference/osdi20/presentation/boos

Braine, G., y Yorozu, M. (1998). Local area network (LAN) computers in ESL and EFL writing classes: Promises and realities. *JALT Journal*, *20*(2), 47-59. https://jalt-publications.org/files/pdf-article/jj-20.2-art3.pdf

Canali, D., Balzarotti, D., y Francillon, A. (2013, mayo). The role of web hosting providers in detecting compromised websites. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 177-188). https://dl.acm.org/doi/abs/10.1145/2488388.2488405

Carayon, P., y Hoonakker, P. (2019). Human factors and usability for health information technology: old and new challenges. *Yearbook of medical informatics*, *28*(01), 071-077. https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0039-1677907

Cázarez, E. [redcudimexico]. (13 de diciembre de 2013). Nuevos Nombres de

Dominio en Internet (Top-Level Domains) [Archivo de Vídeo]. Youtube. https://www.youtube.com/watch?v=kjNbPptklzI

CBC. (2016, junio 7) University of Calgary paid $20K in ransomware attack. https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979

Chilamkurthy, N., Pandey, O., Ghosh, A., Cenkeramaddi, L., y Dai, H. N. (2022). Low-power wide-area networks: A broad overview of its different aspects. *IEEE Access*. http://doi.org/10.1109/ACCESS.2022.3196182

Choi, B. (2021). Introduction to VMware Workstation. In *Introduction to Python Network Automation: The First Journey* (pp. 139-168). Berkeley, CA: Apress. https://link.springer.com/chapter/10.1007/978-1-4842-6806-3_4

Christou, O., Pitropakis, N., Papadopoulos, P., McKeown, S., y Buchanan, W. (2020). Phishing url detection through top-level domain analysis: A descriptive approach. *arXiv preprint arXiv:2005.06599*. https://doi.org/10.48550/arXiv.2005.06599

Cisco (2022a). *What is Network Security?* https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Cisco (2022b). *Cisco Packet Tracer*. https://www.netacad.com/es/courses/packet-tracer

Cisco (2023). *What is a Wi-Fi or wireless network vs. a wired network?* https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html

Commscope (2019). *Security Bulletins*. https://support.ruckuswireless.com/security_bulletins/299

CommScope (2022a). *Ruckus Networks Purpose-driven enterprise networks*. https://www.commscope.com/ruckus/

CommScope (2022b). *Overview of ZoneDirector*. https://docs.commscope.com/bundle/zd-10.3-userguide/page/GUID-79E709C8-B222-4E94-B945-257B8298B02C.html#:~:text=ZoneDirector%20provides%20unified%20AP%20configuration,connected%20and%20mesh%2Dconnected%20APs.

CommScope (2022c). *Ruckus R310*. https://webresources.ruckuswireless.com/datasheets/r310/ds-ruckus-r310-es.html

CommScope (2022d). *Ruckus R500*. https://www.commscope.com/globalassets/digizuite/901-731-ds-ruckus-r500-es.pdf

CommScope (2022e). *Ruckus t300*. https://support.ruckuswireless.com/products/64-ruckus-t300#sort=relevancy&f:@commonproducts=[T300]

Cybersecurity & Infrastructure Security Agency [CISA]. (2020). *Vulnerability Summary for the Week of January 20, 2020*. https://www.cisa.gov/news-events/bulletins/sb20-027

Cybersecurity & Infrastructure Security Agency [CISA]. (2023). *CISA Adds Seven*

*Known Exploited Vulnerabilities to Catalog*. https://www.cisa.gov/news-events/alerts/2023/05/12/cisa-adds-seven-known-exploited-vulnerabilities-catalog

Delgado Ramos, W., y Ruiz Vieira, K. E. (2018). *Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo*. [Tesis de licenciatura, Universidad de Lambayeque]. Base de datos Alicia https://alicia.concytec.gob.pe/vufind/Record/RUDL_012fbc94403191b73f8b2a96aea39000

Didmanidze, I., Beridze, Z., y Zaslavski, V. (2020, octubre). Analysis of wireless network security systems problems and those solutions. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 4, pp. 139-140). https://itconfdoc.nuwm.edu.ua/index.php/ITConf/article/view/143

Dixit, P., y Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, *39*, 100317. https://doi.org/10.1016/j.cosrev.2020.100317

Dlink (2023a). *Smart Managed Gigabit Switches DGS-1210 Series*. https://la.dlink.com/la/switches/dgs-1210-series/#Especificaciones

Dlink (2023b). *xStack L2 Managed Stackable Gigabit Switches DGS-3120 Series*. https://la.dlink.com/la/switches/dgs-3120-series/#Especificaciones

Duck DNS (2023). *Duck DNS free dynamic DNS hosted on AWS*. https://www.duckdns.org/

Feng, S., y Tesi, P. (2017). Resilient control under denial-of-service: Robust

design. *Automatica*, *79*, 42-51. https://doi.org/10.1016/j.automatica.2017.01.031

Fernández, G., y Xu, S. (2019, noviembre). A case study on using deep learning for network intrusion detection. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 1-6). IEEE. https://doi.org/10.1109/MILCOM47813.2019.9020824

Fortinet (2022). *Protecting the ATM network with Fortinet*. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-protecting-the-atm-network-with-fortinet.pdf

Galloway, A. (2006). Protocol. *Theory, Culture & Society*, *23*(2-3), 317-320. https://journals.sagepub.com/doi/abs/10.1177/0263276406023002 41?journalCode=tcsa

Galloway, A., y Thacker, E. (2004). Protocol, control, and networks. *Grey Room*, *17*(10), 6-29. https://direct.mit.edu/grey/article-abstract/doi/10.1162/1526381042464572/10432/Protocol-Control-and-Networks?redirectedFrom=PDF

Ghosh, A., Chakraborty, D., y Law, A. (2018). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology*, *3*(4), 208-218. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/trit.2018.1008

González Borrallo, A. (2022). *Co-Simulación Hardware/Software de SoPCs basados en FPGA usando QEMU y SystemC*. [Tesis de maestría, Universidad Politécnica de Madrid]. Archivo Digital UPM. https://oa.upm.es/71536/

Hewlett Packard Entreprise (2023a). *Conmutador Aruba Instant On 1960 48 G 40 p*

*Clase 4 8p Clase 6 PoE 2 XGT 2 SFP+ 600 W*. https://buy.hpe.com/es/es/networking/switches/fixed-port-web-managed-ethernet-switches/aruba-1900-switch-products/conmutador-aruba-instant-on-1960-48-g-40-p-clase-4-8p-clase-6-poe-2-xgt-2-sfp-600-w/p/jl809a?jumpid=i

Hewlett Packard Entreprise (2023b). *HPE ProLiant DL380 G7 Server – Overview*. https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c02215285

Hewlett Packard Entreprise (2023c). *Guía de usuario del servidor HP ProLiant DL380p Gen8*. https://support.hpe.com/hpesc/public/docDisplay?docId=c03235527&docLocale=es_ES

Hewlett Packard Entreprise (2023d). *Guía de usuario del servidor HPE ProLiant DL380 Gen9*. https://support.hpe.com/hpesc/public/docDisplay?docId=c04471511&docLocale=es_ES

Heron, M., Hanson, V. L., y Ricketts, I. (2013). Open source and accessibility: advantages and limitations. *Journal of interaction Science*, *1*(1), 1-10. https://journalofinteractionscience.springeropen.com/articles/10.1186/2194-0827-1-2

HP (2023). *HPE 1950-48G-2SFP+-2XGT-PoE+(370W) Switch*. https://www.hp.com/us-en/shop/pdp/hp-1950-48g-2sfp-2xgt-switch

Hsieh, K., Harlap, A., Vijaykumar, N., Konomis, D., Ganger, G., Gibbons, P., y Mutlu, O. (2017). Gaia: {Geo-Distributed} machine learning approaching {LAN} speeds. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)* (pp. 629-647).

https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/hsieh

Internet Corporation for Assigned Names and Numbers [ICANN]. (2022a). *Single-Character Second-Level Domain Name (SC SLD) AllocationFramework*. https://www.icann.org/resources/pages/proposed-scsld-allocation-framework-2008-06-13-en

Internet Corporation for Assigned Names and Numbers [ICANN]. (2022b). *What does ICAAN do?* https://www.icann.org/resources/pages/welcome-2012-02-25-en

International Business Machines [IBM] (2023). *¿Qué es Citrix XenServer?* https://cloud.ibm.com/docs/virtualization?topic=virtualization-what-is-citrix-xenserver&locale=es

Iliyasu, A., y Deng, H. (2019). Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks. *IEEE Access*, *8*, 118-126. https://ieeexplore.ieee.org/abstract/document/8941140

Karygiannis, T., y Owens, L. (2002). *Wireless Network Security:* US Department of Commerce, Technology Administration, National Institute of Standards and Technology.http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Knobloch, T., Illarionov, Y., Ducry, F., Schleich, C., Wachter, S., Watanabe, K., Taniguchi T., Mueller T., Waltl M., Lanza M., Vexler M., Luisier M. y Grasser, T. (2021). The performance limits of hexagonal boron nitride as an insulator for scaled CMOS devices based on two-dimensional materials. *Nature*

*Electronics*, *4*(2), 98-108. https://www.nature.com/articles/s41928-020-00529-x

Korczynski, M., Wullink, M., Tajalizadehkhoob, S., Moura, G., Noroozian, A., Bagley, D., y Hesselman, C. (2018, mayo). Cybercrime after the sunrise: A statistical analysis of DNS abuse in new gTLDs. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (pp. 609-623). https://doi.org/10.1145/3196494.3196548

Kuzlu, M., Fair, C., y Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*(1), 1-14. https://link.springer.com/article/10.1007/s43926-020-00001-4

Lee, J., Davari, H., Singh, J., y Pandhare, V. (2018). Industrial Artificial Intelligence for industry 4.0-based manufacturing systems. *Manufacturing letters*, *18*, 20-23. https://doi.org/10.1016/j.mfglet.2018.09.002

Ley de Delitos Informáticos (12 de febrero de 2021). Normas legales, N° 30096, Diario Oficial El Peruano. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Ley de Gobierno Digital (13 de septiembre de 2018). Normas legales, N° 1412, Diario Oficial El Peruano. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

Ley de Protección de Datos Personales (3 de julio de 2011). Normas legales, N° 29733, Diario Oficial El Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

Lu, P., Lai, M., y Chang, J. (2022). A Survey of High-Performance Interconnection Networks in High-Performance Computer Systems. *Electronics*, *11*(9), 1369. https://www.mdpi.com/2079-9292/11/9/1369

Mehdizadeh, A., Suinggi, K., Mohammadpoor, M., y Harun, H. (2017, diciembre). Virtual Local Area Network (VLAN): Segmentation and Security. In *The Third International Conference on Computing Technology and Information Management (ICCTIM2017)* (Vol. 78, p. 89). https://shorturl.at/iBCZ3

Mockapetris, P., y Dunlap, K. J. (1988, agosto). Development of the domain name system. In *Symposium proceedings on Communications architectures and protocols* (pp. 123-133). https://dl.acm.org/doi/abs/10.1145/52324.52338

Molnar, D., y Schechter, S. (2010, junio). Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In *WEIS* (Vol. 2010, pp.1-18). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=db9fb8fbc92b74d3d84e02240bf98064170ef23a

Mughal, A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *International Journal of Intelligent Automation and Computing*, *1*(1), 1-20. https://research.tensorgate.org/index.php/IJIAC/article/view/19

Muntaka, S., Muntaka, M., Osei-Wusu, F., y Adu-Boahen, N. (2021). An Integrated System Using Open source Nethserver OS; A Case Study of Kessben University College Local Area Network. *Muntaka, S., Muntaka, M., Osei-Wusu, F., & Adu-Boahen*, (2021), 427-439. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007696

Naagas, M., Mique Jr, E., Palaoag, T., y Dela Cruz, J. (2018). Defense-through-deception network security model: Securing university campus network from

DOS/DDOS attack. *Bulletin of Electrical Engineering and Informatics*, *7*(4), 593-600. https://doi.org/10.11591/eei.v7i4.1349

Ndia, J., Muketha, G., y Omieno, K. (2019). A survey of cascading style sheets complexity metrics. *International Journal of Software Engineering & Applications (IJSEA)*, *10*(3). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3405783

Neupane, K., Haddad, R., y Chen, L. (2018, abril). Next generation firewall for network security: a survey. In *SoutheastCon 2018* (pp. 1-6). IEEE. https://doi.org/10.1109/SECON.2018.8478973

Nyein, A., Naing, Z., y Saldanha, C. (2009). *Implementation of Media converter for Robust performance* (Doctoral dissertation, MERAL Portal). https://meral.edu.mm/records/2147

Oracle, 2022. *Virtual Machines (VMs).* https://www.oracle.com/cloud/compute/virtual-machines/

Oracle, 2023. *Oracle VM VirtualBox.* https://www.oracle.com/es/virtualization/virtualbox/

Patel, K., y Sharma, P. (2017). A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization. *IJARIIE*, *3*, 2395-4396. https://shorturl.at/zCLN5

PfSense. (2022). *Getting started*. https://www.pfsense.org/getting-started/

Pitancur, B. (2019). *Diseño e implementación de una red de datos y seguridad perimetral de la empresa Corporación Cayman S.A.C*. [Tesis de licenciatura,

Universidad Tecnológica del Perú] Repositorio Institucional de la Universidad Tecnológica del Perú. https://repositorio.utp.edu.pe/handle/20.500.12867/5933

Private Internet Access (2023). *Private Internet Access: #1 VPN For Digital Privacy.* https://www.privateinternetaccess.com/

Prodan, R., y Ostermann, S. (2009, octubre). A survey and taxonomy of infrastructure as a service and web hosting cloud providers. In *2009 10th IEEE/ACM International Conference on Grid Computing* (pp. 17-25). IEEE. https://doi.org/10.1109/GRID.2009.5353074

Proyecto de Ley 6544/2020-CR (2020). https://www.congreso.gob.pe/Docs/comisiones2020/DefensaNacional/files/dict%C3%A1menes/predictamen_6544_centro_nacional_de_seguridad_digital_(1).pdf

Ramprasath, J., y Seethalakshmi, V. (2021). Secure access of resources in software-defined networks using dynamic access control list. *International Journal of Communication Systems*, *34*(1), e4607. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4607

Resolución N.$^{0}$ 071-2017-SUNEDU/CD. Resolución que otorga la licencia institucional a la Universidad de Ciencias y Humanidades, para ofrecer el servicio educativo superior universitario. (21 de noviembre de 2017). https://intranet.sunedu.gob.pe/documentos/directorios/151/1588530-1.pdf

Red Científica Peruana [RCP]. (2022). *Red Científica Peruana*. http://www.rcp.net.pe/index.html

Sarikaya, A., Correll, M., Bartram, L., Tory, M., y Fisher, D. (2018). What do we talk about when we talk about dashboards? *IEEE transactions on visualization and computer graphics*, *25*(1), 682-692. https://doi.org/10.1109/TVCG.2018.2864903

Sarker, I., Furhad, M., y Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 1-18. https://link.springer.com/article/10.1007/s42979-021-00557-0

Shahzad, F. (2017). Modern and responsive mobile-enabled web applications. *Procedia Computer Science*, *110*, 410-415. https://www.sciencedirect.com/science/article/pii/S187705091731284X

Sharma, S., Manuja, M., Puri, D., y Kumar, A. (2021). Secure and Efficient Bandwidth Management for Local and Personal Area Networks Using Customized Open Source Application on a Commodity Hardware: RadSense—An Integration of pfSense Over Radius and MySQL. In *Innovations in Information and Communication Technologies (IICT-2020) Proceedings of International Conference on ICRIHE-2020, Delhi, India: IICT-2020* (pp. 379-386). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-66218-9_44

Somani, G., Gaur, M., Sanghi, D., Conti, M., y Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, *107*, 30-48. https://doi.org/10.1016/j.comcom.2017.03.010

Srisuresh P., y Egevang K. (2001). Traditional IP network address translator (Traditional NAT) [R]. https://www.rfc-editor.org/rfc/rfc3022.html

Subahi, A., Alotaibi, Y., Khalaf, O., y Ajesh, F. (2021). Packet Drop Battling Mechanism for Energy Aware Detection in Wireless Networks. *Computers, Materials & Continua*, *66*(2). https://doi.org/10.32604/cmc.2020.014094

Telenyk, S., Rolik, O., Bukasov, M., y Halushko, D. (2013). Models and methods of resource management for VPS hosting. *Czasopismo Techniczne*. http://psjd.icm.edu.pl/psjd/element/bwmeta1.element.ojs-nameId-6e3e8ea9-5a94-37a7-828b-e6cd5da23db6-year-2015-article-1742

Thomas, G. (2006). Incorporating media converters. *Contemporary Control Systems, Inc. the Extension*, *7*(6). https://www.ctrlink.com/pdf/Extv7n6.pdf

Tonitrus (2023). *HP - 3CRS48G-24-91 - 3Com Switch 4800G - Switch - 1.000 Mbps - 24-Port*. https://www.tonitrus.com/es/redes/accessories/others-4/10144397-014-hp-3crs48g-24-91-3com-switch-4800g-switch-1.000-mbps-24-port/

Tsakyridis, A., Alexoudi, T., Miliou, A., Pleros, N., y Vagionas, C. (2019). 10 Gb/s optical random access memory (RAM) cell. *Optics letters*, *44*(7), 1821-1824. https://doi.org/10.1364/OL.44.001821

Tudosi, A., Graur, A., Balan, D., y Potorac, A. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, *23*(5), 2683. https://doi.org/10.3390/s23052683

Villamora, V., Lim, M., y Sebial, A. (2019, febrero). Modern file transfer protocol using lossless compression, lattice-based encryption, and a data integrity hashing function. In *IOP Conference Series: Materials Science and Engineering* (Vol. 482, No. 1, p. 012050). IOP Publishing. https://doi.org/10.1088/1757-899X/482/1/012050

Wang, J. y Liu, X. (2011). "Computer network security of university and preventive strategy," *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, pp. 143-145. https://ieeexplore.ieee.org/document/6014237

Webster, P. (2019). Understanding the limitations of the ccTLD as a proxy for the national web: lessons from cross-border religion in the northern Irish web sphere. *The historical web and digital humanities: the case of national web domains*, 110-123. https://hcommons.org/deposits/item/hc:32631/

Wen, M., Ye, B., Basar, E., Li, Q., y Ji, F. (2017). Enhanced orthogonal frequency division multiplexing with index modulation. *IEEE Transactions on Wireless Communications*, *16*(7), 4786-4801. https://doi.org/10.1109/TWC.2017.2702618

Wijayanto, H., y Prabowo, I. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, *9*(3), 395-399. http://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/1021

Win Empresas. (2023). *¿Quiénes somos?* https://winempresas.pe/quienes-somos

Wollschlaeger, M., Sauter, T., y Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE industrial electronics magazine*, *11*(1), 17-27. https://ieeexplore.ieee.org/abstract/document/7883994

Yu, P. (2004). The origins of ccTLD policymaking. *Cardozo J. Int'l & Comp.L.*, *12*, 387. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjic12&div=18&id=&page=

Zaripova, D. (2021). Network security issues and effective protection against network attacks. *International Journal on Integrated Education*, *4*(2), 79-85. https://www.neliti.com/publications/344020/network-security-issues-and-effective-protection-against-network-attacks

Zhang, Y., Ansari, N., Wu, M., y Yu, H. (2011). On wide area network optimization. *IEEE Communications surveys & tutorials*, *14*(4), 1090-1113. https://doi.org/10.1109/SURV.2011.092311.00071

3C-LINK (2023). *10/100M 2FX+ 4TX fiber media converter (1SFP+ 1FX).* https://www.3c-link.com/html/2022/100MES_0811/224.html

## Glosario

**CBC:** Canadian Broadcasting Corporation (CBC, 2016).

**ccTLDs:** Country Code Top-Level Domain (Webster, 2019).

**CMOS:** Complementary metal-oxide semiconductor (Knobloch et al., 2021).

**CSS:** Cascading Style Sheets (Ndia, J., Muketha, G., y Omieno, K., 2019).

**DDOS:** Distributed Denial of Service (Somani, et al., 2017).

**DHCP:** Dynamic Host Configuration Protocol (Fernández y Xu, 2019).

**DiD:** Defense-in-depth (Mughal, 2018).

**DNS:** Domain Name System (Korczynski et al., 2018).

**DOS:** Denial of Service (Feng y Tesi, 2017).

**ERP:** Enterprise Resource Planning (Aremu, Shahzad y Hassan, 2018).

**gTLDs:** Generic Top-Level Domain (Korczynski et al., 2018).

**HTML:** Hypertext Markup Language (Shahzad, 2017).

**IANA:** Internet Assigned Numbers Authority (Iliyasu y Deng, 2019).

**ICAAN:** Internet Corporation for Assigned Names and Numbers (ICANN, 2022b).

**IoT:** Internet of Things (Ghosh, Chakraborty y Law, 2018).

**IP:** Internet Protocol (Mockapetris y Dunlap, 1988).

**IT:** Information Technology (Carayon y Hoonakker, 2019).

**LAN:** Local Area Network (Hsieh et al., 2017).

**MC:** Media Converter (Thomas, 2006).

**NGFW:** Next Generation Firewall (Neupane, Haddad y Chen, 2018).

**OFDM:** Orthogonal frequency-division multiplexing (Wen et al., 2017).

**OS:** Operating System (Boos et al., 2020).

**OT:** Operational Technology (Lee et al., 2018).

**RAM:** Random-access memory (Tsakyridis et al, 2019).

**RCP:** Red Científica Peruana (RCP, 2022).

**SLD:** Second Level Domain (ICANN, 2022a).

**TLD:** Top Level Domain (Christou et al., 2020).

**UTM:** Unified Thread Management (Muntaka et al., 2021).

**VLAN:** Virtual Local Area Network (Wollschlaeger, Sauter y Jasperneite, 2017).

**VPN:** Virtual Private Network (Cisco, 2022a).

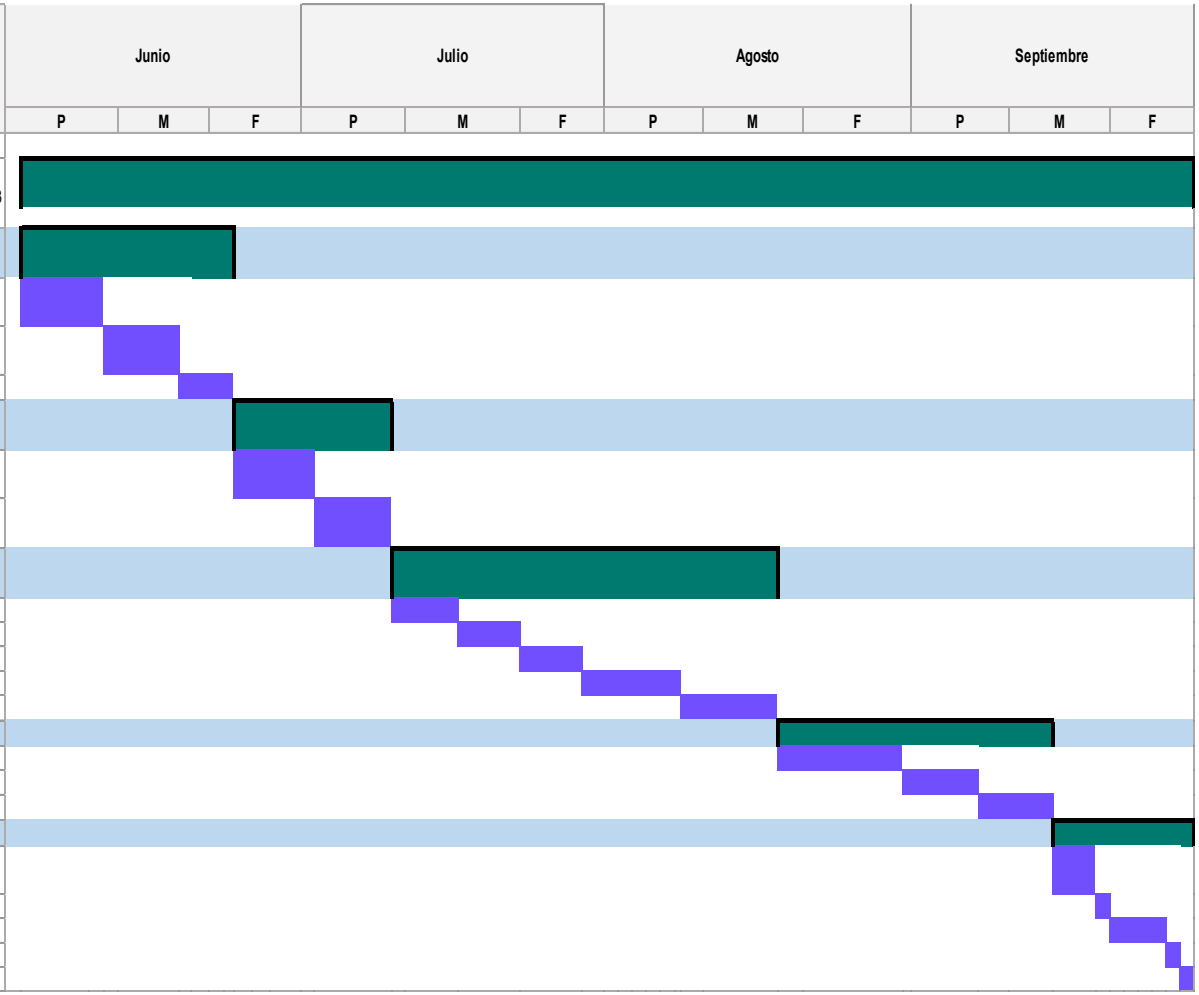
**VM:** Virtual Machine (Oracle, 2022).

**WAN:** Wide Area Network (Chilamkurthy et al., 2022).

# ANEXOS

## ANEXO A: Diagrama de Gantt

| Nombre de la tarea | Duración (dias) | Fecha de inicio | Fecha de finalización |
|---|---|---|---|
| **INICIO** | 0 | 02.06.2023 | 02.06.2023 |
| **PLANIFICACIÓN DE TRANSICIÓN DEL PROTOCOLO RUCKUS WIRELESS AL PROTOCOLO PFSENSE PARA OPTIMIZAR EL SERVICIO DE RED DE DATOS DE LA UNIVERSIDAD DE CIENCIAS Y HUMANIDADES** | 114 | 02.06.2023 | 23.09.2023 |
| **DETERMINAR LA SITUACIÓN ACTUAL DE LA RED DE DATOS EN LA UNIVERSIDAD DE CIENCIAS Y HUMANIDADES** | 18 | 02.06.2023 | 19.06.2023 |
| Buscar información histórica sobre la evolución de la red de datos en la Universidad de Ciencias y Humanidades | 8 | 02.06.2023 | 09.06.2023 |
| Buscar información sobre el software principal utilizado actualmente para la gestión de la red y el hardware implementado | 7 | 10.06.2023 | 16.06.2023 |
| Identificar características del software y hardware utilizado en la actualidad | 3 | 17.06.2023 | 19.06.2023 |
| **IDENTIFICAR LA TOPOLOGÍA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DE CIENCIAS Y HUMANIDADES** | 16 | 20.06.2023 | 05.07.2023 |
| Buscar información sobre la topología actual empleada para el despliegue de la red de datos e identificar sus elementos | 8 | 20.06.2023 | 27.06.2023 |
| Buscar información histórica sobre la evolución de la topología de la red de datos en la Universidad de Ciencias y Humanidades | 8 | 28.06.2023 | 05.07.2023 |
| **DISEÑAR UN MODELO DE RED DE DATOS PARA OPTIMIZAR EL SERVICIO DE LA RED DE DATOS DE LA UNIVERSIDAD DE CIENCIAS Y HUMANIDADES.** | 41 | 06.07.2023 | 15.08.2023 |
| Instalar y configurar VirtualBox | 7 | 06.07.2023 | 12.07.2023 |
| Instalar y realizar configuración inicial de pfSense | 7 | 13.07.2023 | 19.07.2023 |
| Instalar máquinas virtuales que conformarán la red interna | 7 | 20.07.2023 | 26.07.2023 |
| Configurar red interna con máquinas virtuales | 10 | 27.07.2023 | 05.08.2023 |
| Configurar de manera inicial pfSense en la terminal y en la plataforma web | 10 | 06.08.2023 | 15.08.2023 |
| **CONFIGURACIÓN DE PFSENSE** | 28 | 16.08.2023 | 12.09.2023 |
| Configurar de manera avanzada el Firewall de pfSense | 14 | 16.08.2023 | 29.08.2023 |
| Configurar de VPN | 7 | 30.08.2023 | 05.09.2023 |
| Configurar portal cautivo | 7 | 06.09.2023 | 12.09.2023 |
| **SIMULACIÓN DE MODELO DE RED DE DATOS PROPUESTO** | 11 | 13.09.2023 | 23.09.2023 |
| Determinar mejor dispositivo para realizar la instalación de pfSense con su configuración para las pruebas | 3 | 13.09.2023 | 15.09.2023 |
| Instalar pfSense en el dispositivo junto a su configuración | 1 | 16.09.2023 | 16.09.2023 |
| Simular la red diseñada | 5 | 17.09.2023 | 21.09.2023 |
| Determinar efectividad del diseño de red propuesto | 1 | 22.09.2023 | 22.09.2023 |
| Resultados de la simulación | 1 | 23.09.2023 | 23.09.2023 |



## ANEXO B: Matriz de consistencia

| PROBLEMÁTICA | PREGUNTA DE INVESTIGACIÓN | OBJETIVO GENERAL | PREGUNTA DE INVESTIGACIÓN | OBJETIVOS ESPECÍFICOS | ACCIONES | MARCO TEÓRICO | DESARROLLO | EVALUACIÓN | CONCLUSIONES | RECOMENDACIONES |
|---|---|---|---|---|---|---|---|---|---|---|
| En la Universidad de Ciencias y Humanidades existe una red inalámbrica que conecta los distintos dispositivos en las instalaciones, dicha red está construida bajo el protocolo de software propietario de Ruckus Wireless. Sin embargo, Ruckus Wireless también tiene un historial de vulnerabilidades en sus productos que afecta directamente a sus clientes. | ¿Cómo llevar a cabo la transición del protocolo de software propietario al protocolo de software libre pra garantizar la mejora del servicio de red de datos de la Universidad de Ciencias y Humanidades? | Diseñar y planificar el servicio de red de datos mediante el protocolo Ruckus Wireless al protocolo PFSense para optimizar la red inalámbrica de la Universidad de Ciencias y Humanidades. | ¿Cuál es la situación actual del servicio de la red de datos de la Universidad de Ciencias y Humanidades?<br><br>¿Cuál será la topología y la arquitectura la red de datos?<br><br>¿Cuál será el modelo de la red de datos para optimizar el servicio?<br><br>¿Cómo comprobar la efectividad del diseño planteado? | Determinar la situación actual de la red de datos de la Universidad de Ciencias y Humanidades.<br><br>Conocer la topología y la arquitectura de la red de datos de la Universidad de Ciencias y Humanidades.<br><br>Diseñar un modelo de red de datos para optimizar el servicio de la red de datos de la Universidad de Ciencias y Humanidades.<br><br>Simular la efectividad del diseño de la red de datos optimizada. | Establecer cómo es el servicio de red de datos en la Universidad de Ciencias y Humanidades.<br><br>Estudiar la topología de red de datos de la Universidad de Ciencias y Humanidades.<br><br>Realizar un modelo de red de datos.<br><br>Verificar la efectividad del diseño de la red. | Wide Area Network (WAN), Local Area Network (LAN), Virtual Local Area Network (VLAN), Redes Inalámbricas, Seguridad de las VLAN, Calidad de Servicio (QoS), Lista de Control de Acceso (ACL), FTP (File Transfer Protocol), TCP/IP (Transmission Control Protocol/ Internet Protocol), Red de datos, Ruckus, Características de Ruckus, Media Converter, Switch, Servidor, PfSense, Optical Networks, Win Empresas, Fortinet, La Red Científica Peruana, Dominio, Tipos de dominios, DNS (Domain Name System), ICANN (Internet Corporation for Assigned Names and Numbers), Web hosting, Tipos de Web Hosting, Vulnerabilidad de una red, Tipos de seguridad de una red, Virtual Machine, Packet Tracer, Dashboard. | Explicar la realidad actual.<br><br>Analizar los elementos de la red.<br><br>Diseño de la red de datos.<br><br>Validar el funcionamiento de la red. | Desarrollo de flujo de caja, Análisis de VAN, Análisis de TIR, Análisis de retorno de inversión (R.O.I.). | La Universidad de Ciencias y Humanidades actualmente utiliza un Zone Director en conjunto con los Access Point de Ruckus Wireless para el manejo de la red de datos y brindar conexión a cada espacio del campus universitario, del mismo modo hace uso de otros equipos como lo son Media Converters, Servidores y Switches. El cambio de Software propietario a Software libre permite una disminución en los costos además de permitir el uso e implementación de una cantidad más amplia de dispositivos sin depender de una única marca. | Se recomienda que la Universidad de Ciencias y Humanidades utilice Software libre que permite la disminución de los costos y la implementación de una cantidad mas grande de dispositivos de diferentes marcas, lo que brinda mas flexibilidad a la red de datos. |

## ANEXO C: Recibo por el pago del servicio de VPN de Private Internet Access

**RECEIPT**

PRIVATE INTERNET ACCESS, INC.
5555 DTC Parkway
Suite 360
Greenwood Village, CO 80111
United States

August 06, 2023
Order Number: PIA-NE9U7Y3
Payment method: Credit Card

| Details | Quantity | Unit Price | Sub-total |
|---|---|---|---|
| Private Internet Access 1 month plan | 1 | | USD $11.95 |

**TOTAL (USD): $11.95**