UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE COMPUTACIÓN

“Implementación de un Sistema de Seguridad en la empresa CERPIBIENES Utilizando pfSense”

Trabajo de titulación previo a la obtención del

Título de Ingeniero en Ciencias de la Computación

AUTOR: Miguel Alejandro Cervantes Zea

TUTOR: Mora Saltos Nelson Msc

Guayaquil, junio del 2025

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, **Miguel Alejandro Cervantes Zea** con documento de identificación N.° **0931076269**, manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 10 de julio del 2025

Atentamente,

Miguel Alejandro Cervantes Zea
C.I.: 0931076269

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Miguel Alejandro Cervantes Zea, con documento de identificación N.° 0931076269, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto técnico: "**Implementación de un Sistema de Seguridad en la empresa CERPIBIENES Utilizando pfSense**", el cual ha sido desarrollado para optar por el título de: Ingeniero en Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 10 de Julio del 2025

Atentamente,

Miguel Alejandro Cervantes Zea
C.I.: 0931076269

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, **Nelson Salomon Mora Saltos** con documento de identificación N.° **0909257800**, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el proyecto técnico: **Implementación de un Sistema de Seguridad en la empresa CERPIBIENES Utilizando pfSense**, realizado por **Miguel Alejandro Cervantes Zea** con documento de identificación N.° **0931076269**, obteniendo como resultado final el trabajo de titulación bajo la opción **PROYECTO TÉCNICO** que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 10 de Julio del 2025

Atentamente,

Nelson Salomon Mora Saltos
C.I.: **0909257800**

DEDICATORIA

Dedico este logro, de manera especial, a mi familia. A mi padre, Ubaldo Cervantes, por sus valiosas enseñanzas, su ejemplo de seguir adelante y por educarme con principios que han guiado mi formación personal y profesional. A mi madre, Katherina Zea, por su constante apoyo, su ayuda y su incondicional acompañamiento, elementos fundamentales en cada etapa de mi vida. A ambos, expreso mi más profundo agradecimiento y amor por todo lo que han hecho de mí.

También lo dedico a la CEO de la empresa CERPIBIENES, Alicia Cervantes, quien amablemente se tomó el tiempo de escuchar mi propuesta y mostrar interés en el proyecto. Su apertura, disposición y confianza fueron elementos clave para que este trabajo pudiera ponerse en marcha. Le agradezco profundamente su apoyo y la oportunidad brindada para colaborar con su empresa.

Miguel Alejandro Cervantes Zea

AGRADECIMIENTOS

Mi mayor agradecimiento a mis padres Ubaldo Cervantes y Katherina Zea por su atencion y esfuerzo, Con su apoyo en cada instante de mi existencia Gracias por su cariño, enseñanza, compañía y respaldo incondicional; han sido mi guía en los momentos más oscuros.

Deseo manifestar mi más genuino agradecimiento hacia la compañía CERPIBIENES por brindarme la posibilidad de llevar a cabo este proyecto. Su apoyo y disposición fueron fundamentales para el logro efectivo de este proyecto, y quiero expresar mi profundo agradecimiento por el espacio y los recursos que me permitieron crecer profesionalmente durante todo el proceso.

Finalmente deseo agradecer a mis docentes con los que colabore en el transcurso de mi carrera, les agradezco por proveer sus enseñanzas y sus experiencias, cada aporte ha sido fundamental para alcanzar esta meta.

Miguel Alejandro Cervantes Zea

RESUMEN

Hoy en día, tanto hogares como pequeñas empresas dependen en gran medida del uso de dispositivos vinculados a Internet, como computadoras y celulares, para sus operaciones diarias.

El empleo diario de dispositivos vinculados a internet ha cambiado profundamente la manera en que nos comunicamos y llevamos a cabo nuestras actividades comerciales. Sin embargo, esta omnipresencia digital también ha puesto de manifiesto una vulnerabilidad crítica: muchas redes operan con defensas inadecuadas o inexistentes en el peor de los casos.

La falta de sistemas de protección actualizados, como firewalls robustos o detectores de intrusiones, deja a estas redes expuestas a un sinfín de ciberataques. Este hecho destaca lo importante que se vuelve contar con soluciones de seguridad más sofisticadas y confiables en un entorno digital que evoluciona rápidamente.

Tras analizar esta problemática, se identificó la urgente la necesidad de una solución de seguridad que fuera no solo accesible, sino también altamente efectiva para proteger nuestra red frente a posibles ciberataques. Con ese objetivo en mente, utilizar el sistema operativo pfSense, instalado en dispositivos Netgate.

Esta combinación está diseñada para fortalecer significativamente la seguridad de la red en la empresa Cerpibienes, ofreciendo una defensa sólida y adaptable ante el creciente número de amenazas en el entorno digital. Gracias a esta implementación, se podrá reforzar la infraestructura de Networking, protegiendo los activos de la empresa y asegurando la continuidad de las operaciones.

ABSTRACT

Today, both households and small businesses heavily rely on systems connected to the internet, such as computers or cellphones, for their daily operations.

The daily use of these devices has profoundly changed how we communicate and conduct our business activities. However, this digital omnipresence has also highlighted a critical vulnerability: many networks operate with inadequate, or at worst, nonexistent defenses.

The lack of updated protection systems, such as robust firewalls or intrusion detectors, leaves these networks exposed to countless cyberattacks. This fact underscores the importance of having more sophisticated and reliable security solutions in a rapidly evolving digital environment.

After analyzing this problem, an urgent need was identified for a security solution that was not only accessible but also highly effective in protecting our network against potential cyberattacks. With that goal in mind, the pfSense operating system will be used, installed on Netgate devices.

This combination is designed to significantly strengthen the network security at the company Cerpibienes, offering a solid and adaptable defense against the growing number of threats in the digital environment. Thanks to this implementation, the networking infrastructure can be reinforced, protecting company assets and ensuring the continuity of operations.

Tabla de contenido

Índice de Figuras

1. INTRODUCCIÓN

En la actualidad, tanto hogares como empresas dependen en gran parte de dispositivos vinculador a Internet, como computadoras y celulares. Sin embargo, la mayoría de las redes no cuentan con las medidas de seguridad necesarias para una navegación segura, lo que las convierte en objetivos susceptibles a ataques cibernéticos a través de la red. Estas fallas pueden venir de routers con sistemas operativos obsoletos, el cual es lamentablemente el más común, o la falta de sistemas firewall avanzados que ayuden al control de tráfico entrante y saliente de la red. Por ello, es necesario buscar soluciones económicas y efectivas que permitan la mejorará de la seguridad en red, como los dispositivos Netgate con pfSense, cuya implementación será aplicada en la empresa CERPIBIENES.

PfSense es un sistema operativo basado en FreeBSD el cual se distingue significativamente de sus contrapartes comerciales, como Fortinet o Check Point, en su código abierto, gracias a este los usuarios tienen la capacidad de examinar el sistema a fondo, lo que permite comprender con precisión cómo funciona el sistema, cómo se gestionan los datos y qué cambios se han implementado, desde las nuevas características implementadas al sistema, hasta posibles errores que se encuentren dentro de estos cambios que puedan llegar a comprometer el sistema, este nivel de transparencia lo hace una opción ideal para organizaciones que se encuentren empezando su funcionamiento y deseen una solución fuerte para su seguridad en línea, a un precio accesible.

2. PLANTEAMIENTO DEL PROBLEMA

2.1. Antecedentes

Los routers proporcionados por nuestros proveedores de servicios de Internet (ISP), pueden llegar a presentar múltiples vulnerabilidades que los presentan como blancos atractivos para ciber atacantes. En 2021 se identificaron 506 vulnerabilidades en routers domésticos, de las cuales 87 fueron clasificadas como críticas. Lo más preocupante es que muchas de estas vulnerabilidades siguen sin ser corregidas por parte de los fabricantes. Estas fallas pueden permitir a los atacantes realizar diversas acciones maliciosas, como interceptar datos, redirigir el tráfico a sitios fraudulentos o incluso tomar el control total del dispositivo (Kaspersky, 2022).

2.2. Planteamiento del Problema

Aunque la conectividad digital y el acceso a servicios en línea ha crecido rápidamente, la protección de las redes usadas en hogares y empresas de pequeña escala continúa siendo una preocupación crítica. Muchos de estos entornos operan con equipos de red que no tienen configuraciones de seguridad avanzadas y que no reciben actualizaciones regulares, lo que aumenta su vulnerabilidad a ciberataques (González, 2025).

La falta de inversión en soluciones de ciberseguridad por parte de dichas empresas, la cual puede venir por desconocimiento o limitaciones presupuestarias, agrava aún más esta problemática. Los routers convencionales, frecuentemente configurados con valores predeterminados y de fácil acceso, representan un punto de entrada vulnerable que puede comprometer toda la red interna. Esta problemática pone en peligro la seguridad y privacidad de los datos sensibles corporativos, afectando la continuidad operativa del negocio. Ante esta realidad, es fundamental implementar una solución eficiente y asequible que permita elevar el nivel de seguridad en la empresa (Kaspersky, 2022).

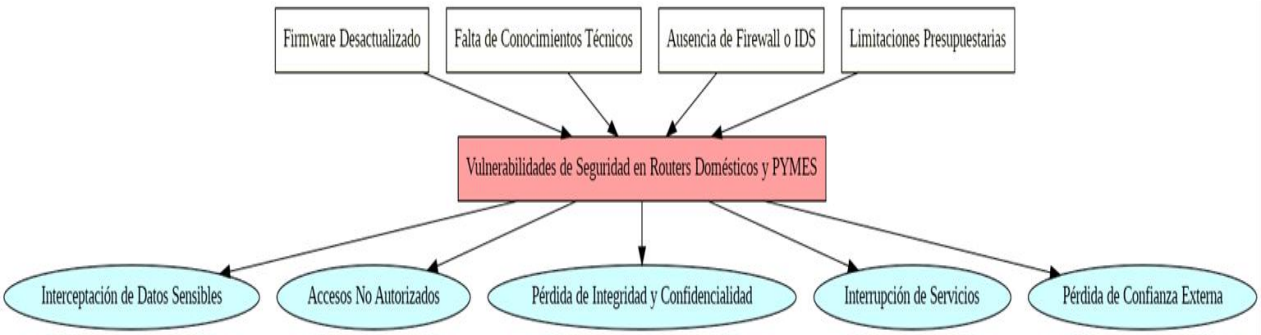
En este contexto, se propone la implementación del sistema pfSense instalado en dispositivos Netgate, una alternativa basada en el sistema operativo de FreeBSD, el cual es de código abierto, este sistema ofrece funcionalidades de red avanzadas como firewall, detección de intrusiones y control de acceso. Su adopción representa una oportunidad viable para fortalecer la seguridad de red en la empresa CERPIBIENES, sin comprometer la sostenibilidad económica del proyecto (Carmona, Interconexión de redes de forma segura mediante cortafuegos pfSense, 2024).

2.3. Árbol del Problema

Causas y Consecuencias de la falta de seguridad en routers domésticos

Imagen 1

Causas y Consecuencias de la falta de seguridad en routers domesticos



Fuente: Mapa Conceptual hecho por el autor

2.4. Importancia y Alcances

La empresa “CERPIBIENES”, al igual que muchas pequeñas organizaciones, enfrenta un gran desafío: no tiene una infraestructura de red que le brinde la protección necesaria contra las amenazas informáticas actuales, como los ataques DDoS. Esta circunstancia amenaza la continuidad de sus operaciones, la integridad de la información y la credibilidad ante sus clientes.

Por eso, es fundamental que fortalezcan la seguridad de su red. Implementar un sistema de seguridad perimetral, como el que ofrece pfSense, junto con herramientas como Snort y pfBlockerNG, permitirá a la empresa administrar el flujo de datos de red de manera más agil, detectar accesos sospechosos y bloquear amenazas externas de forma automatizada (Castillo, 2024). La implementación de este sistema contribuirá a:

- Reducir el tráfico malicioso y los accesos no autorizados.
- Asegurar que solo los empleados e invitados legítimos puedan acceder a la red de la empresa.
- Asegurar la disponibilidad continua de los servicios de la empresa.
- Minimizar los riesgos de pérdida de datos sensibles.

- Proveer al personal técnico con herramientas para monitorear y reaccionar ante incidentes en tiempo real.

Este proyecto se centra en mejorar la infraestructura local de red de CERPIBIENES, aumentando su seguridad sin necesidad de recurrir a soluciones costosas. Además, sentará las bases para futuras expansiones o mejoras.

2.5. Justificación

Hoy en día, muchas pequeñas empresas como "CERPIBIENES" dependen de una red informática básica para llevar a cabo sus operaciones, pero a menudo carecen de firewalls avanzados que les ayuden a protegerse de las amenazas digitales, que son cada vez más dañinas. Esta falta de protección puede resultar en filtrado de información de clientes o empleados, interrupciones en el servicio de red y daños a la reputación de la organización (Briceño, 2021).

El presente proyecto propone una solución en el uso del sistema operativo pfSense, una herramienta de código abierto que permite gestionar el tráfico de red, establecer reglas de seguridad y detectar posibles amenazas mediante módulos especializados. Su implementación está respaldada por una justificación técnica y económica sólida, ya que ofrece un alto nivel de protección sin necesidad de realizar grandes inversiones.

Asimismo, al incorporar herramientas como Snort para identificar intrusiones y pfBlockerNG para el filtrado de IPs y dominios malintencionados, se potencia notablemente la seguridad sin comprometer la estabilidad de la infraestructura de la red. Estas soluciones asimismo promueven la formación interna de los empleados, al incluirlos en la administración directa del sistema (Tigrero, 2025).

2.6. Delimitación

El proyecto de seguridad informática está enfocado exclusivamente en la infraestructura de la red de la empresa CERPIBIENES, considerando únicamente la instalación, configuración y evaluación del sistema pfSense.

La solución se implementará en un dispositivo Netgate, el cual asumirá el rol de router principal tras colocar el equipo del ISP en modo puente. Se configurarán reglas de firewall, módulos de detección de intrusos y listas de bloqueo automatizadas. Además, se realizarán

evaluaciones de vulnerabilidades a través del uso de la herramienta Nessus para validar la efectividad del sistema sobre el router (Mena, 2025).

El proyecto no contempla la protección de dispositivos finales en áreas fuera del alcance de la red, las cuales podrían ser solventadas con el uso de un antivirus. El enfoque principal es la protección del perímetro de red para mitigar accesos no autorizados.

El sistema permanecerá funcional mientras el equipo Netgate esté operativo y correctamente configurado, el cual será administrado por personal técnico designado por la empresa.

2.7. Delimitación Espacial

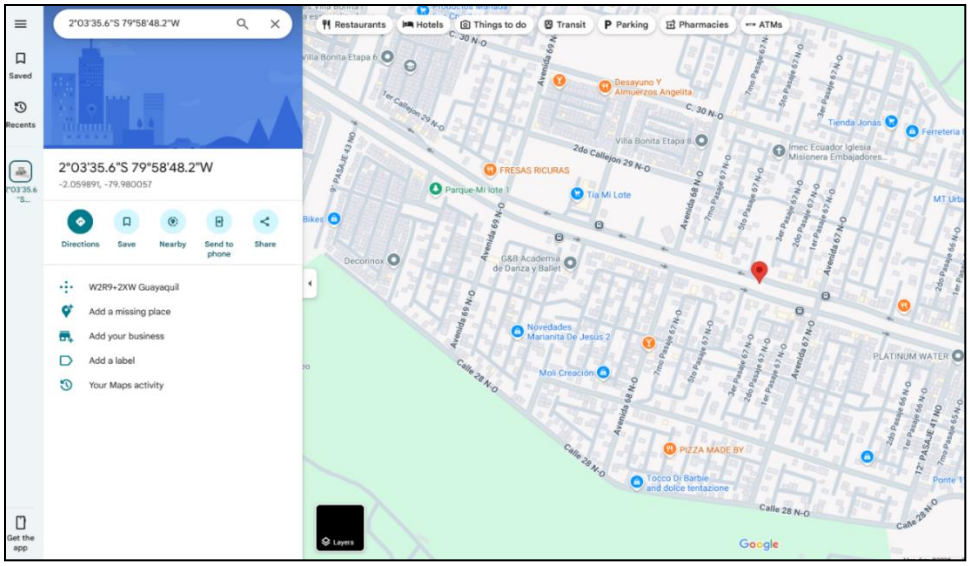
Imagen 2

Foto de la Empresa

Fuente: Foto Tomada por el Autor

Imagen 3

Ubicación de la empresa en Google Maps



Fuente: Google Maps

2.8. Delimitación Temporal

El proyecto técnico se puso en marcha en febrero del 2025 y se llevó a cabo de manera continua hasta su finalización en julio del 2025.

2.9. Grupo objetivo (beneficiario)

Los beneficiarios del presente proyecto son los siguientes:

- **Empresa:**

La empresa CERPIBIENES se beneficiará directamente al contar con una infraestructura de red más segura y controlada, lo que permitirá proteger sus recursos digitales y operaciones internas frente a accesos no autorizados o amenazas externas.

- **Gerencia:**

La gerencia podrá contar con reportes y alertas que le permitan monitorear eventos de seguridad, identificar intentos de intrusión y tomar decisiones informadas sobre la gestión tecnológica de la empresa.

- **Persona técnica:**

El equipo encargado de las tecnologías de la información tendrá a su disposición las herramientas pfSense, Snort y pfBlockerNG, con interfaces gráficas y configuraciones que les permitirán administrar reglas de firewall, listas de bloqueo, y registros de eventos en tiempo real.

- **Administrador del sistema:**

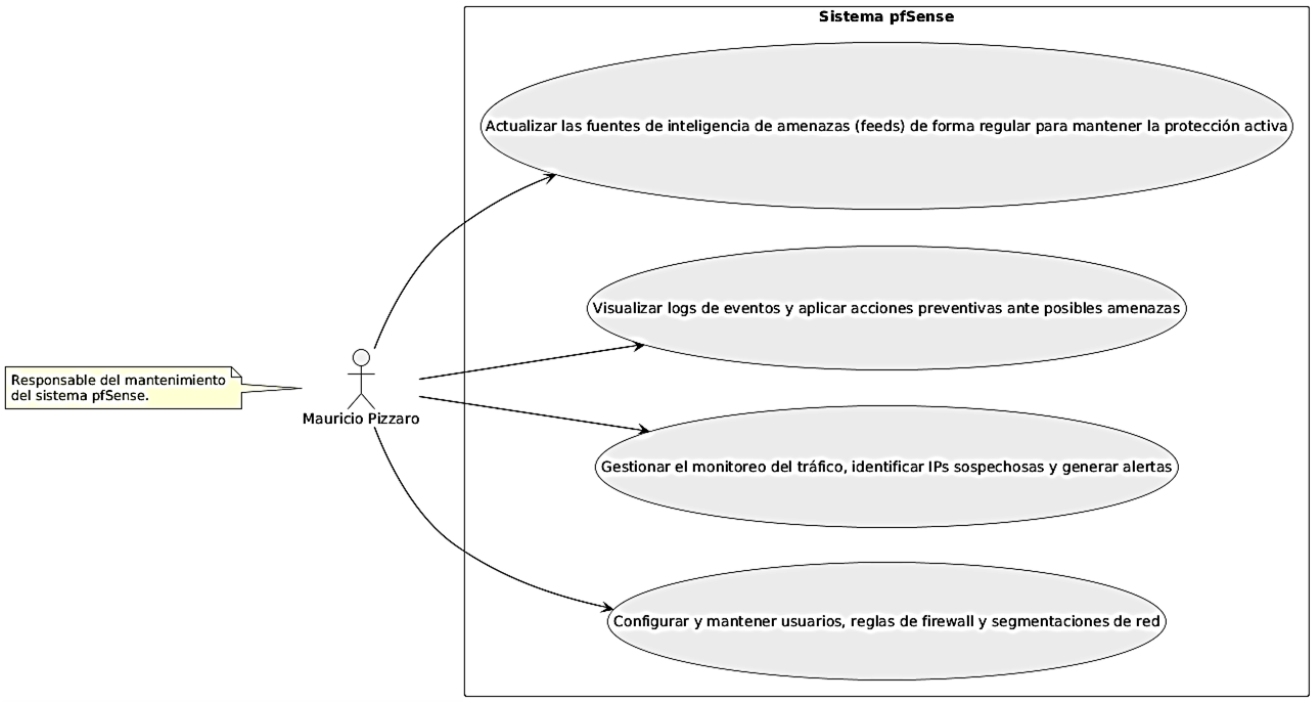
El responsable designado por la empresa es el empleado, Mauricio Pizarro, quien contará con un entorno de gestión centralizada que le permitirá:

  - Configurar y mantener usuarios, reglas de firewall y segmentaciones de red.
  - Gestionar el monitoreo del tráfico, identificar IPs sospechosas y generar alertas.
  - Visualizar logs de eventos y aplicar acciones preventivas ante posibles amenazas.
  - Actualizar las fuentes de inteligencia de amenazas (feeds) de forma regular para mantener la protección activa.

Este conjunto de beneficios está orientado a fortalecer el entorno operativo de la empresa, mejorando su nivel de protección digital y permitiendo una administración técnica autónoma, organizada y efectiva.

Imagen 4

Administrador del sistema en la empresa



Fuente: UML hecho por el autor

3. OBJETIVOS

3.1. Objetivo General

Implementar una solución de seguridad en la infraestructura de red de la empresa CERPIBIENES utilizando un appliance Netgate SG-1100 con pfSense instalado, para mitigar vulnerabilidades y mejorar la protección frente a amenazas cibernéticas.

3.2. Objetivos Específicos

- Configurar el router que el proveedor de servicios de Internet (ISP) dio a la empresa Cerpibienes, en modo puente (bridge mode) a través de su interfaz web, con el fin de que

el appliance Netgate actúe como el router principal y asuma el control total de la red empresarial. Esta configuración permitirá que todo el tráfico de red pase directamente por PfSense.

- Implementar los módulos Snort y pfBlockerNG dentro del entorno pfSense, con el objetivo de habilitar capacidades avanzadas de detección y prevención de intrusiones, así como el bloqueo automatizado de direcciones IP y dominios maliciosos. Esta integración refuerza la seguridad perimetral de la red mediante mecanismos proactivos de filtrado y monitoreo del tráfico.
- Evaluar la efectividad del sistema PfSense implementado mediante la ejecución de pruebas de penetración utilizando la distribución Kali Linux, complementadas con un análisis comparativo de las alertas generadas y los accesos bloqueados, tanto antes como después de la instalación del dispositivo y las configuraciones. Esta evaluación permitirá medir el impacto de las medidas adoptadas y validar su capacidad de defensa frente a posibles amenazas.

3.3. Objetivos de Seguridad

El primer objetivo de este proyecto consiste en reducir al mínimo el tráfico malicioso que pueda comprometer la integridad de red de la empresa CERPIBIENES, garantizando que únicamente el tráfico legítimo tenga permiso para ingresar o salir del sistema. Este control es fundamental para preservar la integridad y disponibilidad de los recursos de red, asegurando una conexión estable y segura que no interfiera con el desarrollo normal de las actividades del personal.

Para alcanzar este objetivo, se implementará feeds(listas) de amenazas basadas a nivel de IP o DNS, que se actualicen constantemente, permitiendo el bloqueo de IPs maliciosas que intenten ingresar al sistema, bloqueando efectivamente los accesos no autorizados al sistema de red (Cavazos, 2021).

Además, se empleará la aplicación Snort dentro del entorno pfSense para la detección de tráfico malicioso, configurándola para que emita alertas cada vez que identifique actividades sospechosas o potencialmente peligrosas (Eduardovych, 2024).

Como parte de las pruebas finales, se utilizarán herramientas especializadas en Nessus, con el propósito de identificar vulnerabilidades existentes tanto en el router provisto por la ISP como en el appliance pfSense.

3.4. Aportaciones

Todas las organizaciones necesitan de la protección sus datos, desde la privacidad del personal hasta información crítica como contratos y proyectos, pero no todas ellas cuentan con el presupuesto necesario para implementar soluciones que puedan solventar esta necesidad (Quezada, Aguilar, & Marroquín, 2023).

Es por eso por lo que la empresa CERPIBIENES, la cual es una empresa pequeña y con un presupuesto limitado, opto por implementa el sistema operativo de código abierto conocido como PfSense, debido a que este nos da una solución de seguridad en red por un presupuesto accesible, el cual no cuenta con una problemática que muchos proyectos de código abierto tienen, la cual es la falta de soporte técnico que se nos puede ser proveído por las organizaciones que aprovechan el proyecto.

Hay una gran cantidad de documentación disponible en línea, esto gracias a su existencia como software de código abierto**,** , la cual resultara de gran utilidad en caso de ser necesaria una auditoria al código en caso de presentarse algún problema en el sistema, esta también nos ayudara a la formación del equipo encargado de la administración y mantenimiento del firewall.

4. MARCO TEÓRICO

4.1. ¿Qué es pfSense?

PfSense es un sistema operativo de código abierto basado en el sistema operativo FreeBSD de la familia Unix, diseñada específicamente para funciones de firewall y routing. Desarrollado por la empresa Netgate, pfSense combina la estabilidad de Unix con la flexibilidad de un sistema de código abierto, lo que permite su auditoría, personalización y adaptación a distintas infraestructuras de red (Romero, 2023).

Una de sus principales fortalezas radica en su transparencia, ya que, al tratarse de software libre, los administradores tienen acceso directo al código fuente, facilitando auditorias aplicadas por comunidades y empresas. Esta transparencia la diferencia de soluciones propietarias como Fortinet o Checkpoint. (Carmona, 2024).

En cuanto a sus requisitos técnicos, pfSense es liviano y escalable: puede funcionar correctamente con 1 GB de RAM, 8 GB de almacenamiento, una CPU de dos núcleos y al menos dos interfaces de red RJ45 para la configuración básica de LAN y WAN

4.2. Diseño Teórico del Sistema

El diseño de red propuesto contempla dos segmentos diferenciados y protegidos: la red WAN, que representa la conexión hacia el exterior (Internet), y la red LAN, orientada a la administración interna. El tráfico será gestionado y protegido por pfSense, complementado por herramientas adicionales como Snort y pfBlockerNG.

WAN (Wide Area Network): Punto de entrada y salida hacia Internet, puede estar expuesta a amenazas como DDoS. Este segmento será supervisado por módulos de seguridad que analicen y filtren el tráfico (Toala, Segovia, & Zúñiga, 2022).

LAN (Local Area Network): Dedicada a la gestión interna de la red. Utilizará técnicas de NAT (Network Address Translation) para evitar que los dispositivos internos sean directamente accesibles desde el exterior. Servirá también como canal de administración de toda la red (Mejía, Ortiz, Ramos, & Moscoso, 2022).

DHCP: Dynamic Host Configuration Protocol, en acrónimo conocido como DHCP, protocolo de red que permite que los dispositivos conectados a esta reciban una IP de manera automática (Lomelí, Duarte, & Gutiérrez, 2025).

WLAN: Wireless Local Area Network, en acrónimo conocido como WLAN, permite la interconexión de dispositivos a través de ondas de radio, necesaria para dispositivos que solo puedan conectarse de forma inalámbrica, como los celulares (Tomala, 2023).

4.3. Requerimientos de Hardware

Para la implementación del sistema se requerirán los siguientes componentes:

Switch no gestionable: A falta de necesidad para VLANs por parte de la empresa, se optará por un switch no gestionable

Router como punto de acceso (AP): Permitirá conexión Wi-Fi para móviles y visitantes, en caso de ser necesario, podra actuar como router de respaldo.

4.4. Snort

Snort es un sistema de detección y prevención de intrusiones (IDS/IPS) desarrollado por Cisco, ampliamente utilizado para el análisis profundo de paquetes de red y detección de patrones maliciosos. Su integración con pfSense permite detectar amenazas como escaneos de puertos, ataques de denegación de servicio y tráfico no autorizado (Mazacon, 2022).

Una ventaja significativa de Snort es su capacidad de operar en modo pasivo (solo detección) o modo activo (detección y bloqueo). Su arquitectura modular y las actualizaciones periódicas de sus reglas lo convierten en una herramienta altamente adaptable a distintos entornos de red.

4.5. pfBlockerNG

pfBlockerNG es un paquete adicional de pfSense que permite bloquear conexiones entrantes o salientes en función de listas negras de IP y dominios maliciosos, conocidas como feeds. Estas listas pueden actualizarse automáticamente y filtrarse por regiones geográficas (GeoIP) o categorías de amenazas (Ferrer, 2023).

Además de mejorar la seguridad perimetral, pfBlockerNG permite aplicar políticas de navegación para usuarios internos, restringiendo el acceso a sitios no deseados y proporcionando estadísticas de uso que facilitan la toma de decisiones en ciberseguridad.

4.6. Nessus

Nessus es una herramienta de análisis de vulnerabilidades desarrollada por la empresa Tenable, ampliamente reconocida por su precisión, cobertura y facilidad de uso. Permite realizar escaneos de seguridad automatizados sobre redes, servidores, dispositivos IoT y aplicaciones, detectando configuraciones erróneas, parches faltantes y vulnerabilidades conocidas (Santos & Córdoba, 2024).

Nessus utiliza una base de datos actualizada de más de 75,000 plugins, lo que le permite identificar desde vulnerabilidades críticas hasta configuraciones débiles que podrían ser explotadas por atacantes.

En el presente proyecto, Nessus será utilizado para evaluar el estado de seguridad de la red antes, utilizando el router proveido por la ISP de la empresa y después de la implementación de pfSense, usando el appliance Netgate, permitiendo así medir la efectividad de las soluciones aplicadas.

5. METODOLOGÍA

Se hará uso de una metodología experimental para la comprobación del funcionamiento del proyecto. A través de esta se podrán controlar y parchar las fallas de seguridad que se lleguen a presentar dentro de la configuración de red de la empresa.

Como primer paso se ha conseguido un appliance netgate, el dispositivo que cumplirá las funciones de router, al ser un router no necesita alto uso de cpu, disco duro ni ram, con 8gb de almacenamiento, 1gb de ram y un cpu de 2 núcleos es más que suficiente para hacer las labores del router y firewall, este se encontrará conectado directamente al router de la empresa, el cual será modificado internamente para actuar como modem únicamente, esto debido a que es un router-modem y no un router modem separados.

En un segundo paso se realizarán las comprobaciones de que el resto del hardware necesario (router-punto de acceso y switch) se encuentra en buen estado y operativo. A continuación, se procederá a conectar y configurar los equipos en la estructura de red de la empresa, en la cual testearemos diversos computadores y celulares en los cuales haremos pruebas de navegación, descarga y carga de la red para asegurarnos de que esta sea estable y funcional.

Como tercer y último paso se utilizará herramientas de ciberseguridad dentro de la distribución de Linux para ciberseguridad conocida como “Kali-Linux” para asegurar la seguridad dentro de la red, en las cuales se incluirán:

Nmap: Usada para el reconocimiento y escaneo de puertos de la red expuestos para poder bloquearlos (Colque, 2021).

Netcat: Revisar el estado de los puertos para confirmar que no estén expuestos (Martínez, 2023).

Wireshark: Capturar tráfico desde las interfaces de red de la empresa para después hacer las configuraciones necesarias para evitar su captura (Paucar & Tipán, 2022).

5.1. Arquitectura de la red

5.1.1. Descripción de la arquitectura

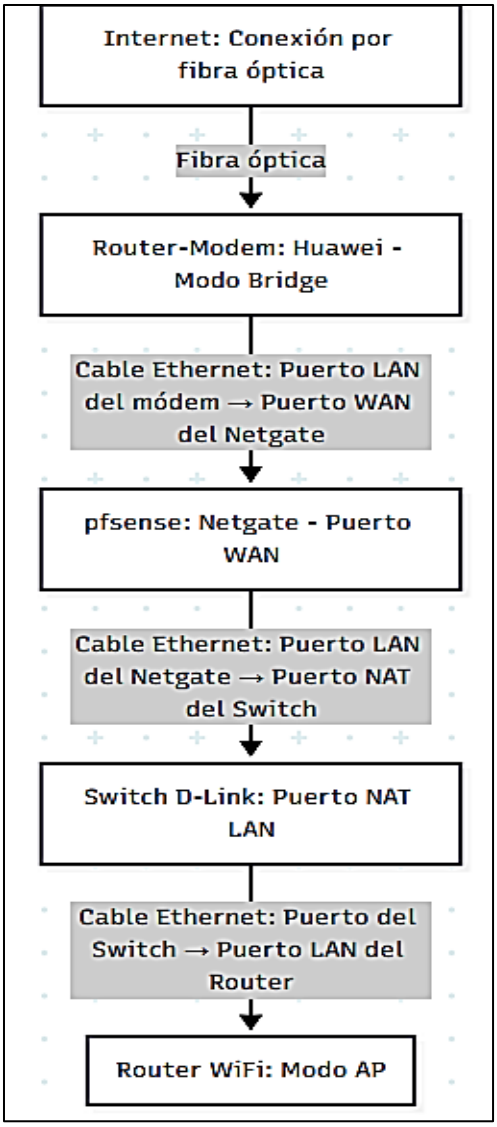
Se distinguen dos casos: un diseño teórico y luego el diseño real en el que se basa este proyecto.

Para el diseño de la red se tendrá en cuenta que la arquitectura sea escalable, es decir que se pueda expandir según las necesidades de la empresa, además de dar el mayor rendimiento. Este diseño va a tener una parte central, que va a ser nuestro router-firewall pfSense, siguiendo un modelo de seguridad en red.

Diagrama de flujo #1

Imagen 5

Diseño de la red



Fuente: UML hecho por el autor

5.1.2. Diseño real

Tomando en cuenta el diseño teórico y basándose en él, se pasará a dar forma al diseño real donde se explicará a fondo que dispositivos hardware utilizamos y de qué forma los conectaremos entre sí, además de cualquier tipo de limitación que lleguemos a encontrar.

En la empresa CERPIBIENES se ha hablado y han dejado claro que por el momento necesitan al menos 100 equipos conectados a internet, con la posibilidad de incrementarlos de ser necesario.

Para llevarlo a cabo, se configuro dentro del Appliance la posibilidad de usar IPs desde la ip 192.168.137.100 hasta la 192.168.137.254, el cual es lo máximo permitido por el rango de direcciones disponibles dentro de la subred 192.168.137.0/24, que tiene una máscara de subred 255.255.255.0.

Esta configuración nos permite el uso de 154 direcciones utilizables, con las direcciones 2-99 reservadas para dispositivos que necesiten una IP estática, de ejemplo una impresora o un NAS (Network Attached Storage), para la ejecución del proyecto, el Router-AP se le dará la IP 192.168.137.2.

La dirección 192.168.137.1 es la dirección desde donde nosotros configuraremos el appliance/firewall para las necesidades de la empresa.

Imagen 6

Imagen del router dentro de la empresa

Fuente: Foto Tomada por el autor

5.1.3. Como podremos configurarlo en nuestro router principal

Debemos comprender primero que tipo de router tenemos, y las tecnologías que funcionan dentro de el

Existen 2 tipos de routers proveídos por nuestras ISP (Internet Service Provider), los 4 en 1 y los 5 en 1, ejemplificado con imágenes:

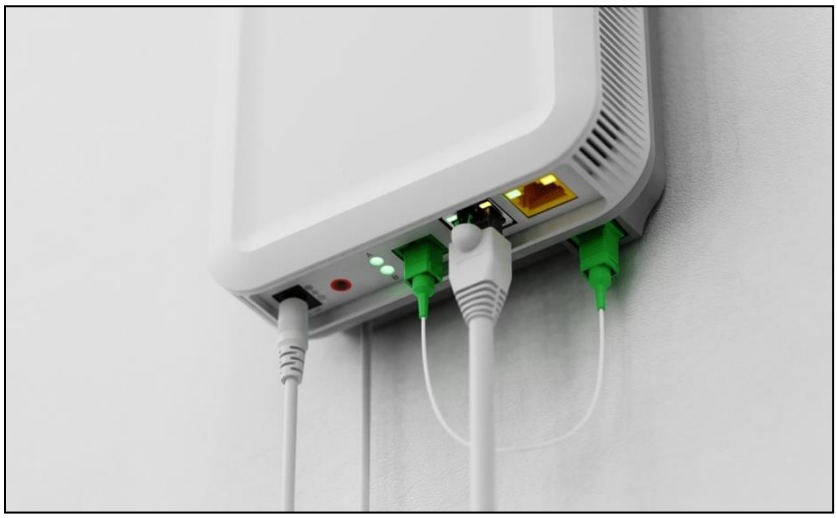
Imagen 7

Routers 4 en 1 (router, firewall, Access point y switch)

Fuente: Foto de referencia de google

Imagen 8

Routers 5 en 1 (modem,router, firewall, Access point y switch)



Fuente: Foto de referencia de google

La diferencia principal es que el router 5 en 1, se encuentra conectado directamente a la fibra que la ISP coloco en el hogar donde se encuentre alojado, mientras que el router 4 en 1 necesita de un modem dedicado para poder conectarse al internet del local, y eso incluye una ventaja por que podríamos reusar el router 4 en 1 únicamente como Access point, pero esto no se podría hacer en los router 5 en 1, el cual solo podría ser usado como modem.

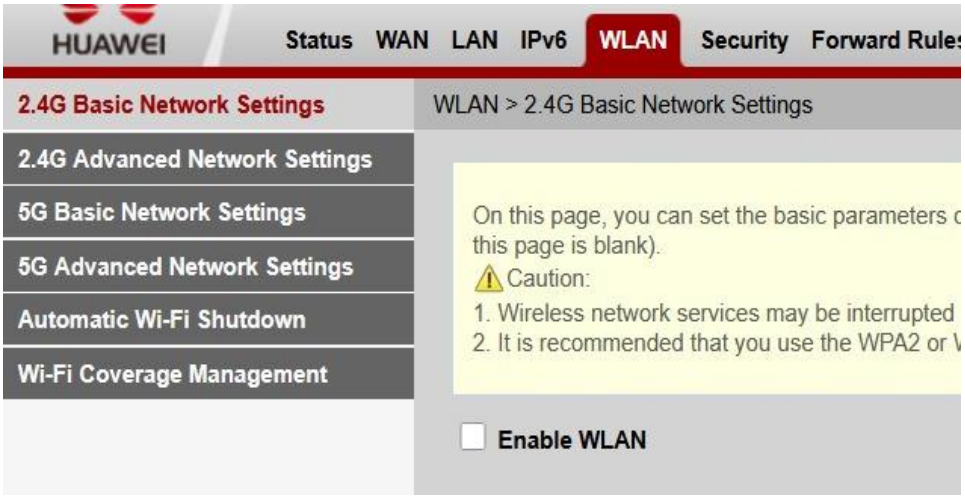
Para poder usar el appliance como router principal necesitaremos hacer unas cuantas configuraciones dentro del router 5 en 1 para desactivar sus funciones de router y que funcione únicamente como modem.

Al realizar estas configuraciones podemos llegar a perder acceso a la interfaz gráfica, por lo que necesitaremos conectarnos vía ethernet al router.

Lo primero que debemos hacer es deshabilitar las WLAN, tanto la 2,4 como la 5G, para que no interfieran con las nuevas WLAN que crearemos dentro del nuevo AP.

Imagen 9

Desactivación de las WLAN dentro del router del ISP.

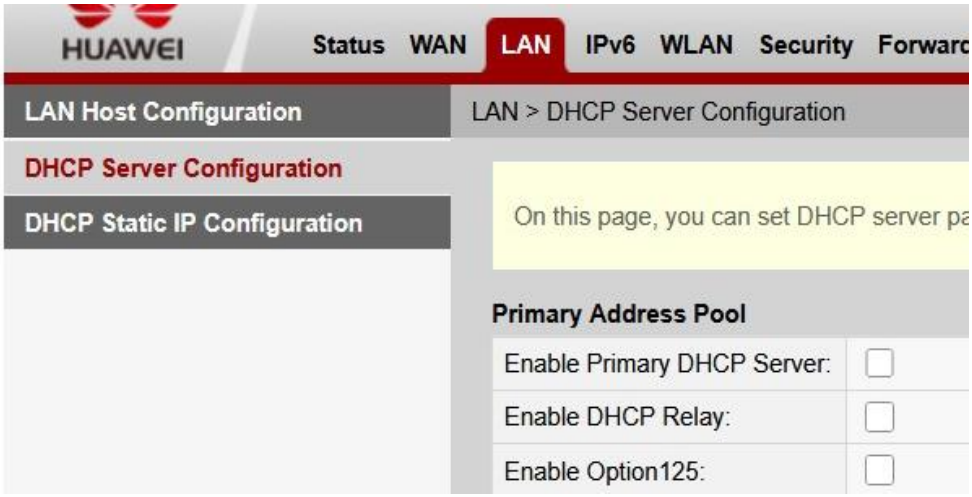


Fuente: Hecho por el autor

Después nos encargaremos de desactivar las funciones DHCP del router para evitar que asigne una IP privada al router PfSense, lo que podría generar conflicto al momento de asignar IPs, y en el peor de los casos, perdidas de conexión.

Imagen 10

Desactivación de DHCP en el router del ISP

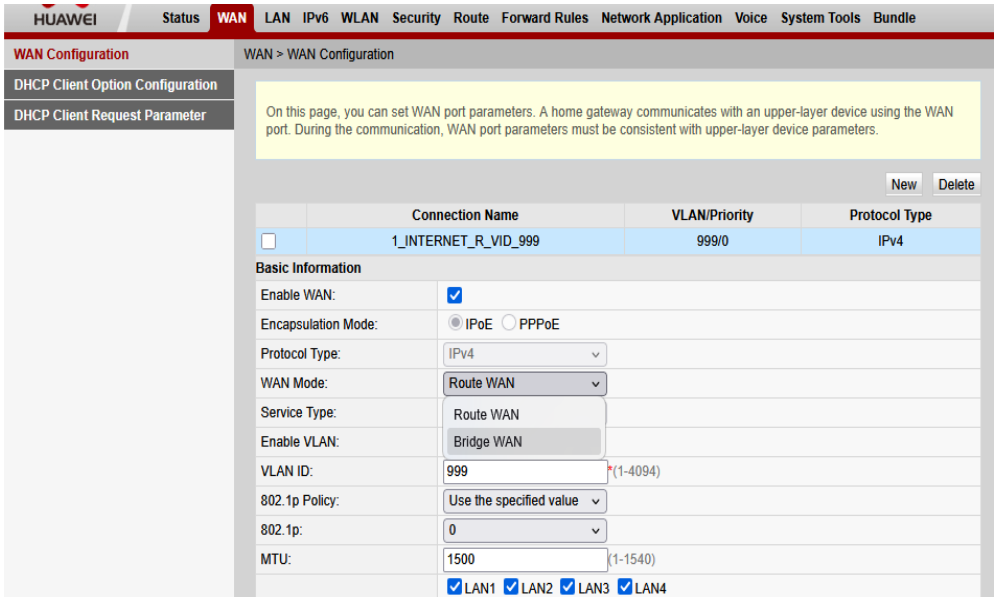


Fuente: Hecho por el autor

Y lo más importante, entrar en la configuración de la WAN y configurar el router en modo puente, para que actúe como un puente o modem de fibra para proveer de internet no enrutado al appliance con PfSense.

Imagen 11

Cambio a modo puente del router del ISP

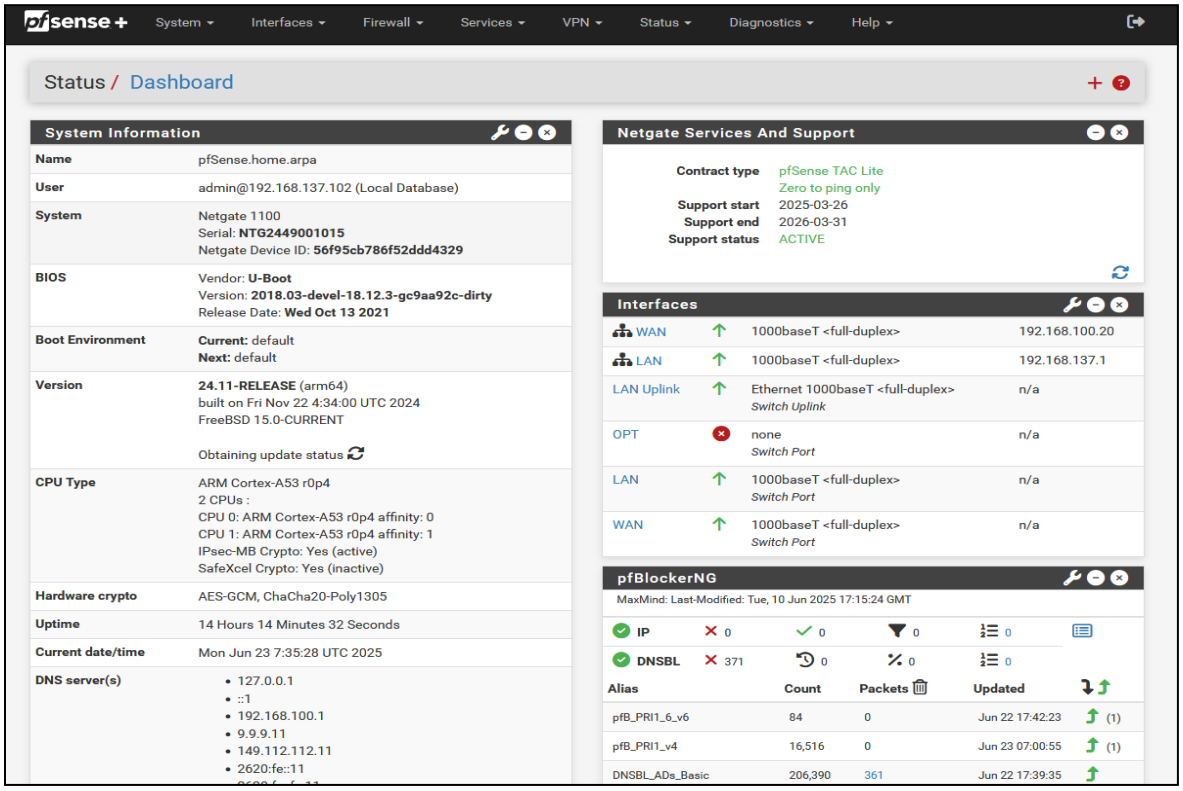


Fuente: Hecho por el autor

Como resultado PfSense debería tomar control como router, firewall y servidor DHCP, sin interferencias del router principal.

Imagen 12

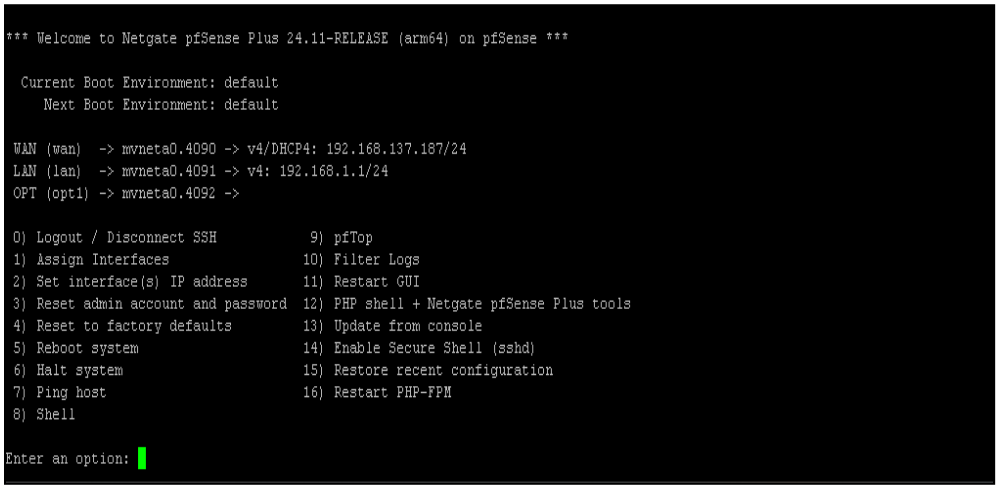
Interfaz de PfSense



Fuente: Hecho por el autor.

Imagen 13

CLI de PfSense (obtenidos a través de una conexión por consola en la aplicación Putty)



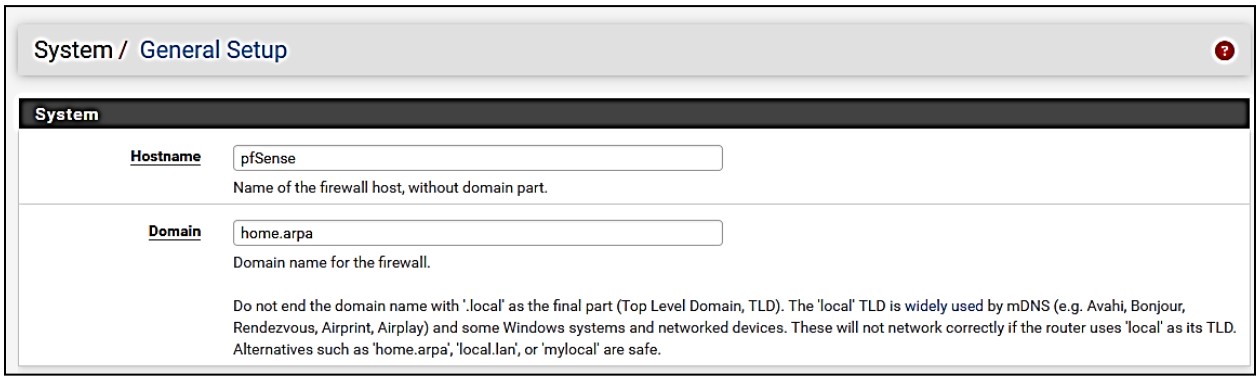
Fuente: Hecho por el autor.

5.1.4. General Setup

Se encarga de la configuración de algunos servicios como el nombre del host, el dominio, los servidores DNS, la zona de tiempo y el idioma del sistema. Se usarán las configuraciones predeterminadas “pfsense” para el hostname y dominio como “home. arpa” (esto podrá ser cambiado en caso de que la empresa desee adquirir su propio dominio) quedando dicha configuración reflejada de la siguiente forma:

Imagen 14

General Set-up en la interfaz de PfSense

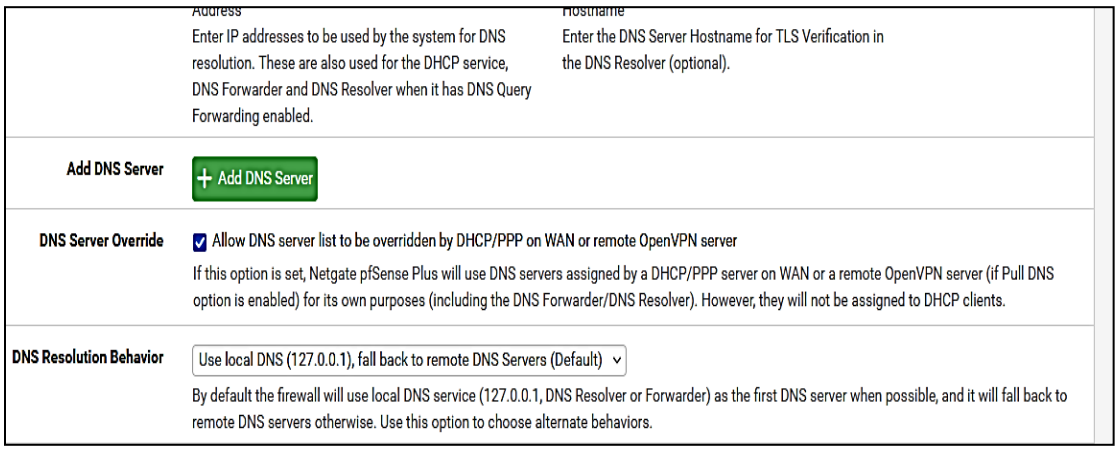


Fuente: Hecho por el autor.

Para el DNS se usarán los DNS proveídos por PfBlocker con un fallback a los servidores de la ISP de la empresa en caso de tener problemas, en la siguiente captura se mostrará un servidor DNS de prueba, fácilmente reemplazable en caso de ser requerido

Imagen 15

Configuracion del DNS



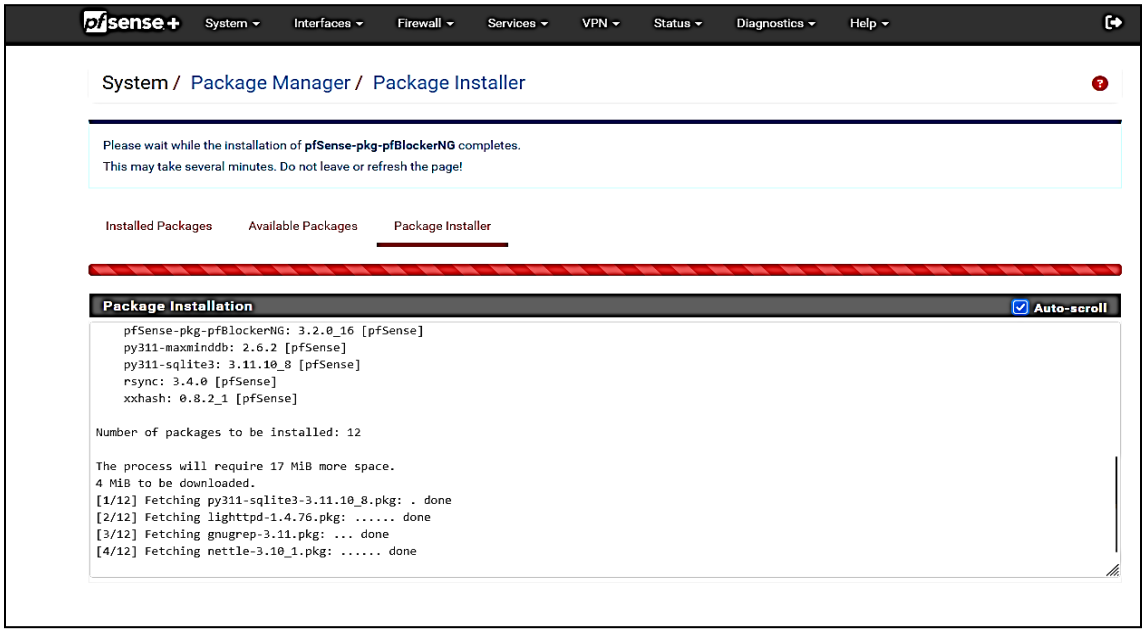
Fuente: Hecho por el autor.

5.1.5. Package Manager

Package Manager es el gestor de paquetes o módulos que tenemos instalados y también los que se encuentran disponibles para su instalación, desde aquí instalaremos PfBlocker y Snort.

Imagen 16

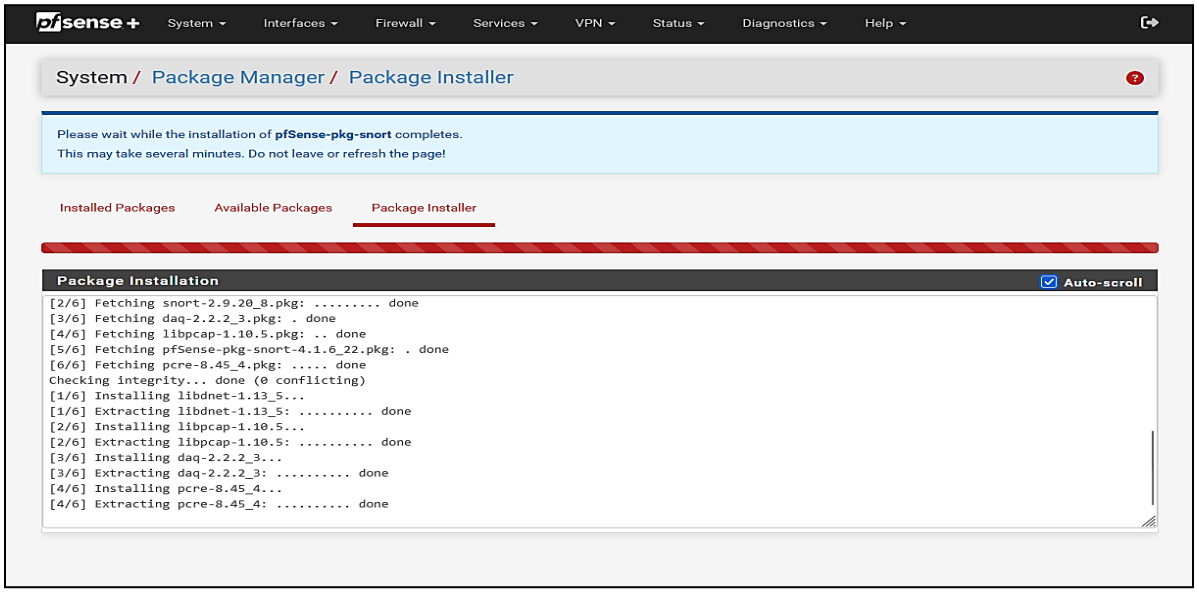
Instalacion de Pfblocker en PfSense



Fuente: Hecho por el autor.

Imagen 17

Instalación de Snort en PfSense



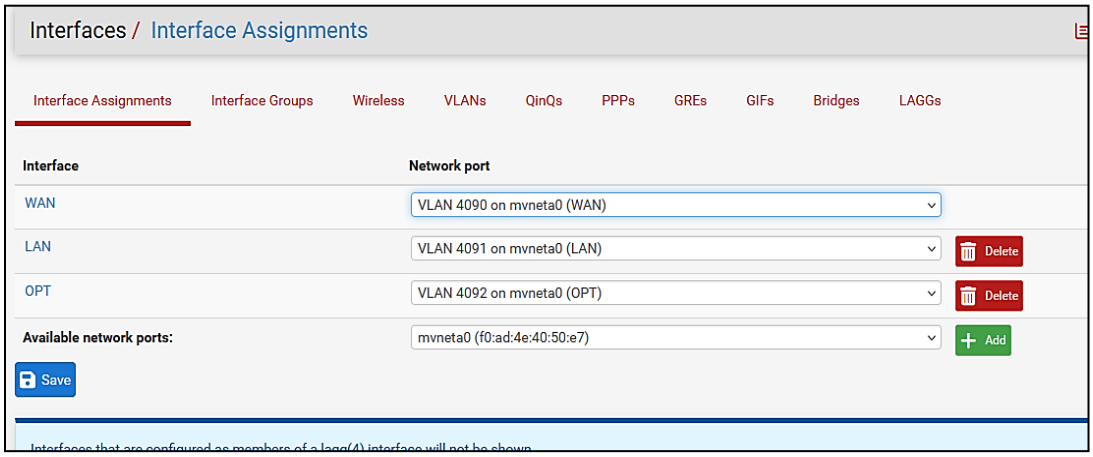
Fuente: Hecho por el autor.

5.1.6. Interfaces

Define el apartado de puertos LAN y WAN, define cual será el puerto que recibirá el internet del modem y cuál será el puerto que permiten conectar dispositivos internos de la red local de la empresa.

Imagen 18

Asignacion de las interfaces en PfSense



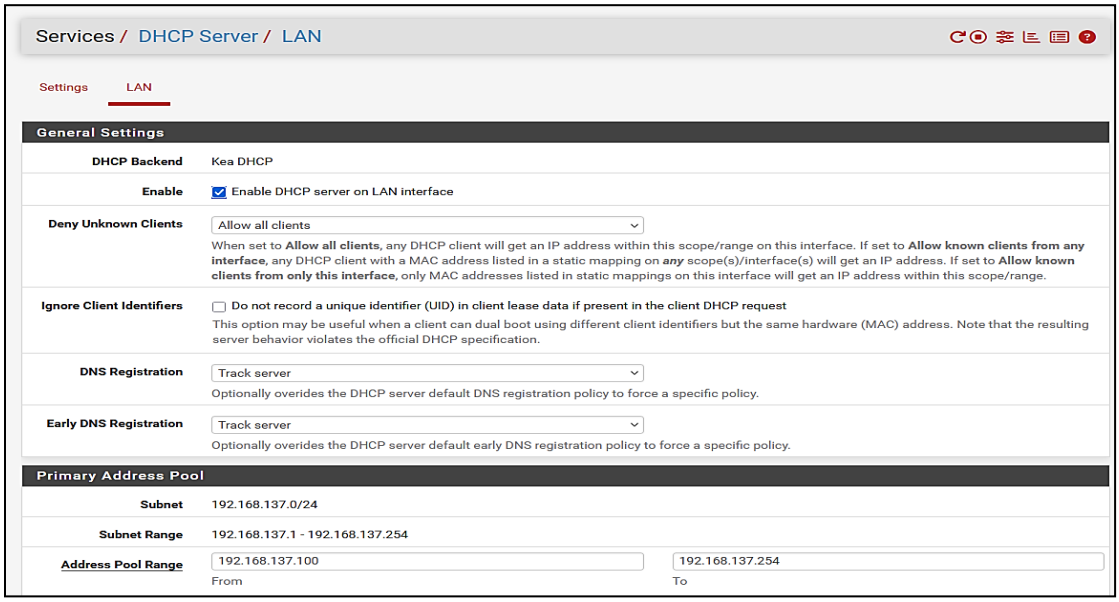
Fuente: Hecho por el autor.

5.1.7. Services

En este apartado se detalla la configuración de los servicios integrados por defecto en pfSense, así como los módulos adicionales instalados mediante el gestor de paquetes. Para este proyecto se tendrán en cuenta los servicios como Snort, DHCP Server y el servidor DNS (donde configuraremos la cantidad de IPs que el sistema puede dar a los dispositivos que se conecten).

Imagen 19

Servicio de LAN en PfSense



Fuente: Hecho por el autor.

5.1.8. PfBlocker

PfBlocker es un paquete de gestión el cual mejora la seguridad proveida por el firewall a través de filtrado de IP basado en listas negras de IPs y dominios. Permite controlar el acceso y el tráfico saliente a la red de la empresa (Flames, 2023).

Ofrece tres funciones principales:

- **IP Blocking:** Se encarga de gestionar las listas de reputación de IPs maliciosas (bogons, spamhaus, emerging threats, etc.), creando reglas de firewall que bloquean el tráfico entrante/saliente de esos rangos (Zhang, Wang, & Liew, 2022).
- **DNSBL (DNS Blacklist):** Implementa un servidor DNS local que intercepta solicitudes DNS hacia dominios maliciosos, de publicidad o rastreo, y responde con direcciones falsas (como 10.10.10.1), bloqueando así el acceso (Rochina, 2021).
- **GeoIP Filtering:** Permite bloquear o permitir tráfico según el país o región de origen (ideal para restringir accesos innecesarios desde ubicaciones geográficas no relacionadas con la

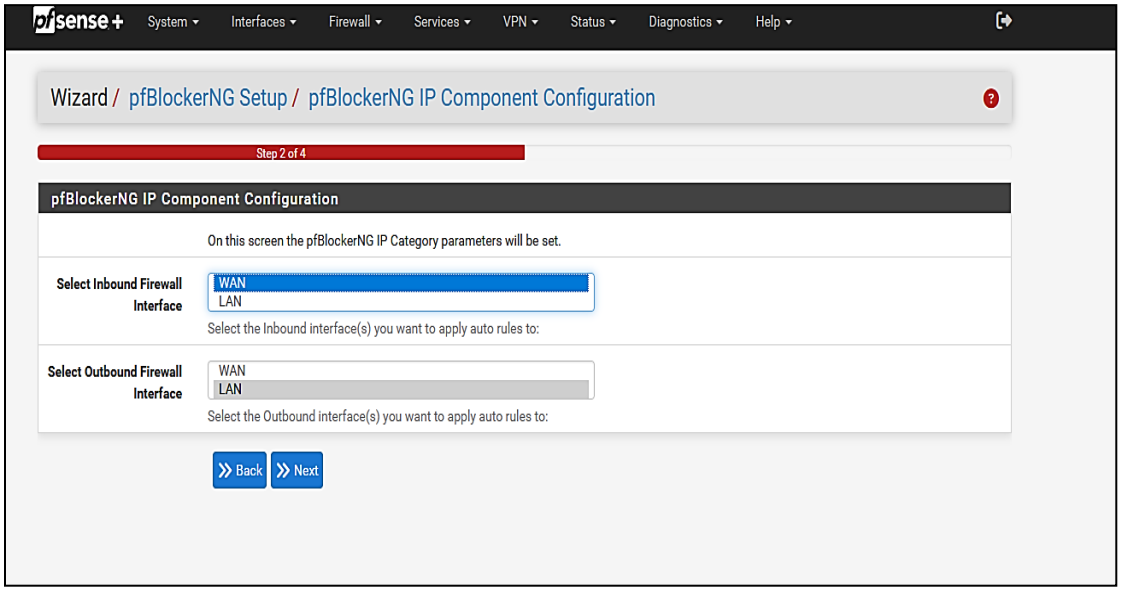
operación de la red, aunque fácilmente puede ser retirado en caso de que la empresa llegue a moverse a aquellos países) (Fainchtein, 2023).

Se configura cual será la interfaz que rechazará el tráfico entrante, la WAN, y cual rechazará el tráfico saliente, la LAN.

Asigncion de las interfaces de entrada y salida (WAN y LAN) dentro de PfBlocker

Imagen 20

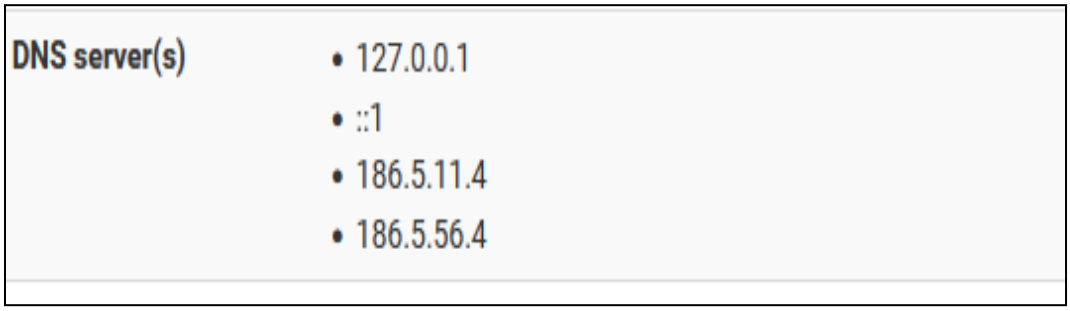
Asignacion de las interfaces de entrada y salida (WAN y LAN) dentro de PfBlocker



Fuente: Hecho por el autor.

Imagen 21

Confirmación que el DNS de PfBlocker funcione dentro de PfSense

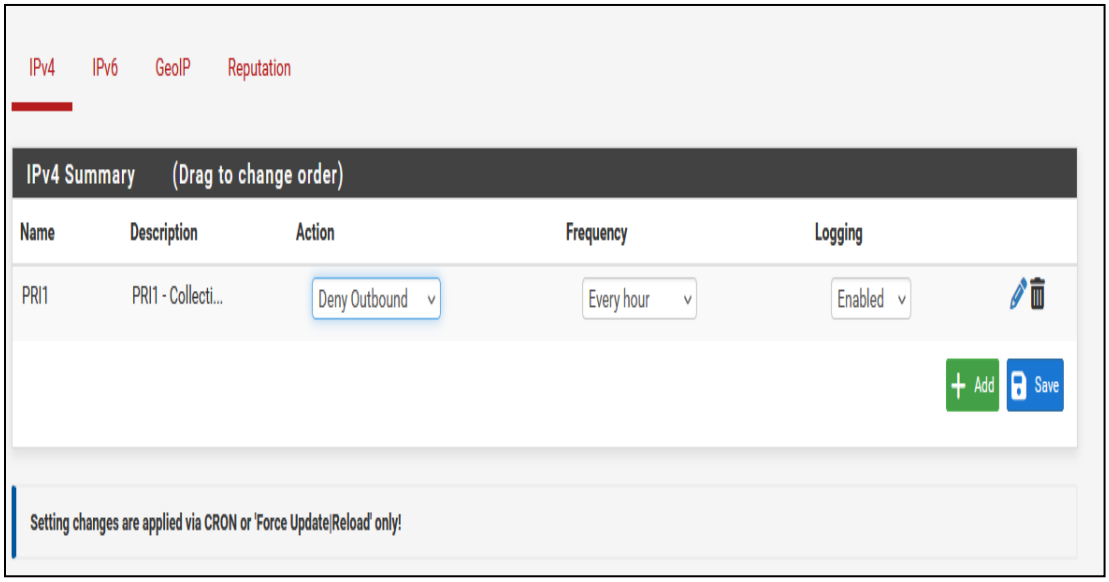


Fuente: Hecho por el autor.

En la siguiente captura se muestra una lista de ejemplo, generada por PfSense como medio de configuración para el resto de las listas, esta solo es para poder configurar listas IPV4.

Imagen 22

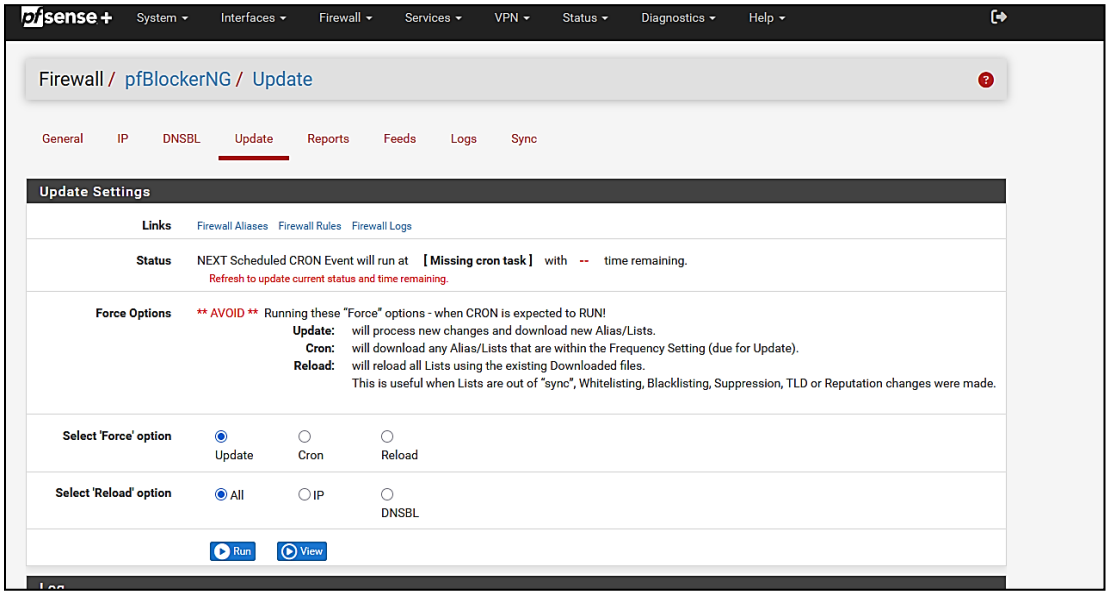
Añadir listas de bloqueo dentro del sistema



Fuente: Hecho por el autor.

Imagen 23

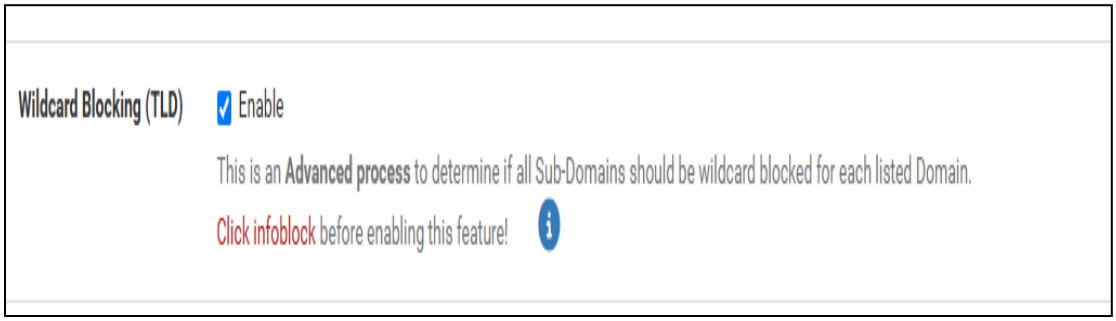
Actualizar las listas de bloqueo para que el sistema funcione



Fuente: Hecho por el autor.

Imagen 24

Bloqueo de los subdominios de las IPs maliciosas del sistema

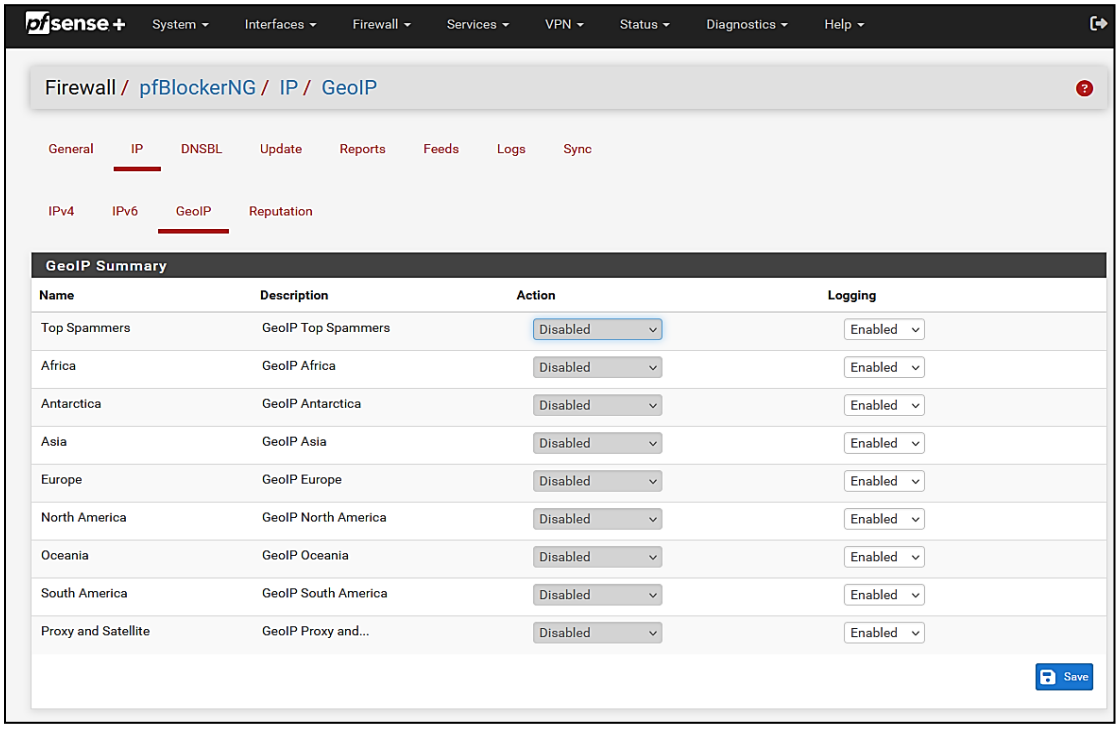


Fuente: Hecho por el autor.

Aquí se muestra el bloqueo basado en IP, más conocido como GeoIP, solo será configurado "Top Spammers" a orden de la empresa, deberemos ponerlo en la configuración "Deny Both" para que el tráfico no deseado no entre ni salga al internet.

Imagen 25

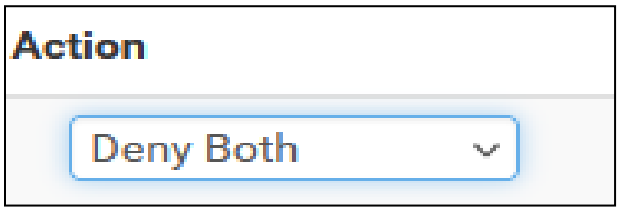
Bloqueo de IPS basado en Region



Fuente: Hecho por el autor.

Imagen 26

Denegando el acceso de las IPS Spammers



Fuente: Hecho por el autor.

Para confirmar que el sistema bloquee se usó una de las tantas ips bloqueadas por el pfblocker, en este caso 247realmedia.com

Imagen 27

IP seleccionada para empezar la prueba

Fuente: Hecho por el autor.

Se usará el comando dig @192.168.137.1 A 247realmedia.com

dig (Domain Information Groper) es una herramienta de línea de comandos en sistemas basados en UNIX que se usa para hacer consultas DNS. Lo que permitirá verificar qué direcciones IP están asociadas a nombres de dominio y cómo se resuelven (Álvarez, 2024).

Si obtenemos una ip que no sea 10.10.10.1 significa que el sitio no está bloqueado

Imagen 28

Prueba de la IP sin PfBlocker

```
Rafa@Rafa ~ % dig @192.168.137.1 A analytics.163.com

; <<>> DiG 9.10.6 <<>> @192.168.137.1 A analytics.163.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42230
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1432
;; QUESTION SECTION:
;analytics.163.com.             IN      A

;; ANSWER SECTION:
analytics.163.com.      475     IN      A       59.111.239.33

;; Query time: 8 msec
;; SERVER: 192.168.137.1#53(192.168.137.1)
;; WHEN: Tue Jun 17 10:37:47 -05 2025
;; MSG SIZE  rcvd: 62
```

Fuente: Hecho por el autor.

Imagen 29

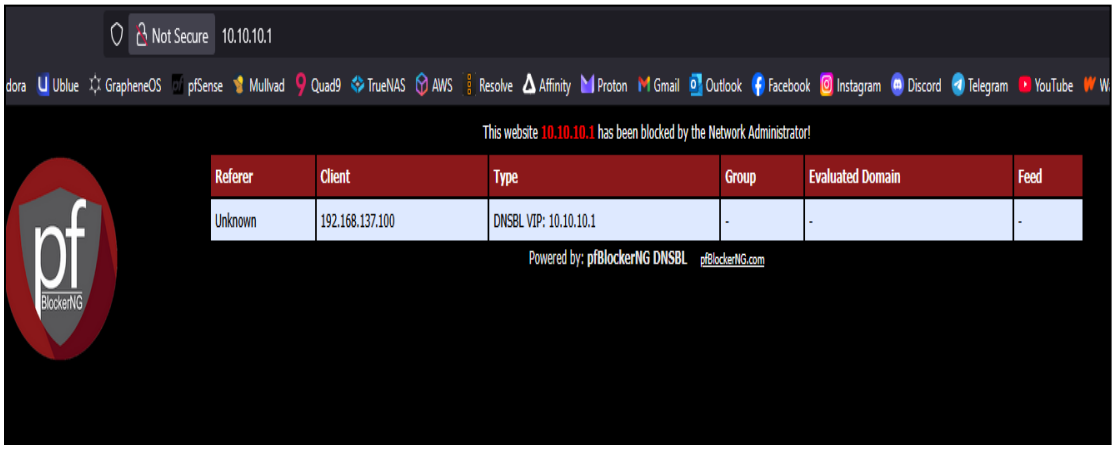
Prueba de la IP con PfBlocker

```
Rafa@Rafa ~ % dig @192.168.137.1 A analytics.163.com

; <<>> DiG 9.10.6 <<>> @192.168.137.1 A analytics.163.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50224
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1432
;; QUESTION SECTION:
;analytics.163.com.             IN      A

;; ANSWER SECTION:
analytics.163.com.      60      IN      A       10.10.10.1

;; Query time: 5 msec
;; SERVER: 192.168.137.1#53(192.168.137.1)
;; WHEN: Tue Jun 17 10:41:10 -05 2025
;; MSG SIZE  rcvd: 62
```

Fuente: Hecho por el autor.

Imagen 30

Prueba de la IP en un navegador

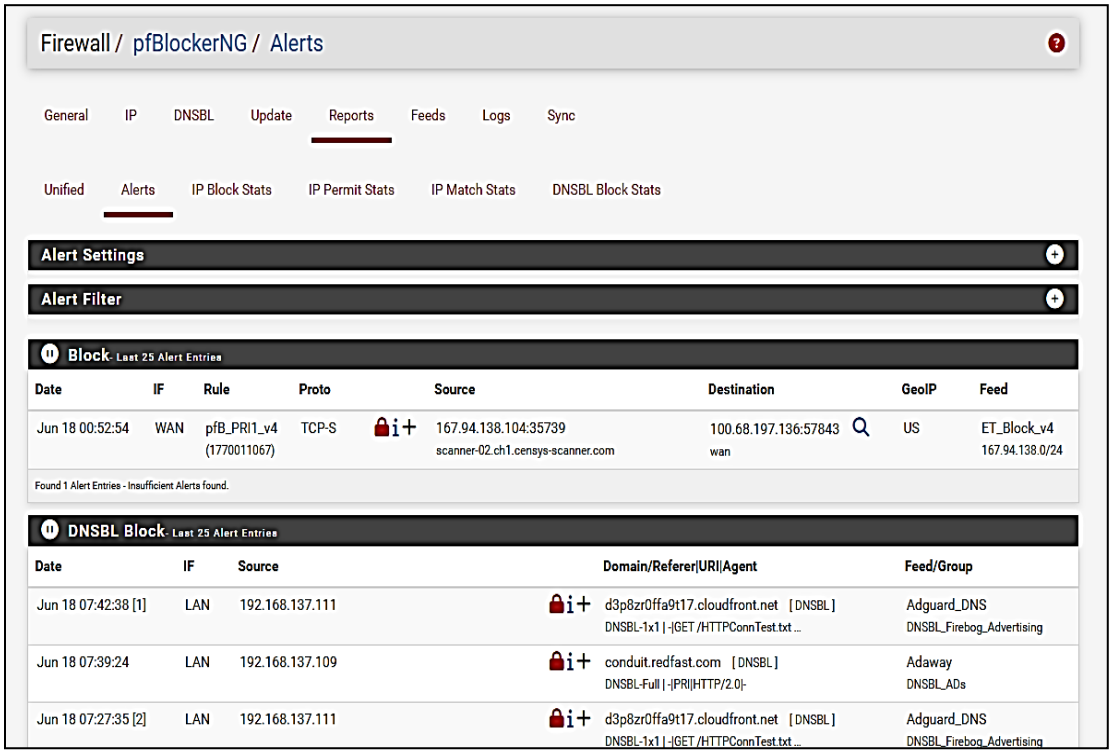


Fuente: Hecho por el autor.

Además, también nos brindara con un grupo de alertas que nos daran a conocer si algunas de las IPs dentro de las blacklist traten de entrar al sistema de red.

Imagen 31

Alertas dentro de PfBlocker



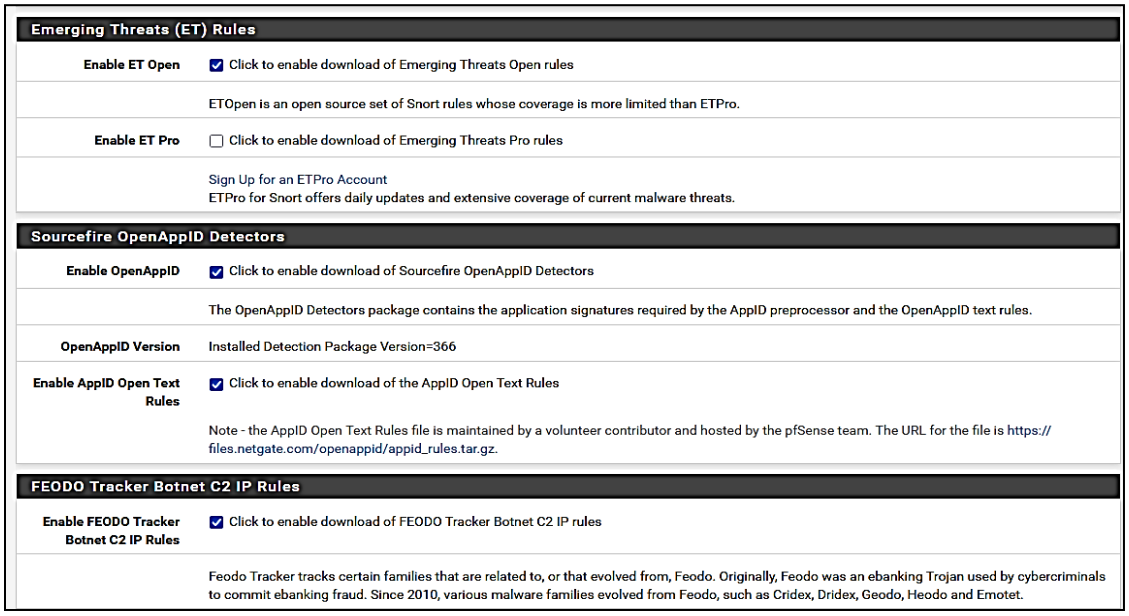
Fuente: Hecho por el autor.

5.1.9. Snort

Snort es un sistema de detección de intrusos (IDS, por sus siglas en inglés) que permite identificar actividades sospechosas, anomalías y posibles amenazas en la red. Se trata de una herramienta gratuita y de código abierto, actualmente mantenida por Cisco, que la ofrece sin costo, aunque cobra por servicios de soporte técnico y acceso anticipado a las reglas de detección que se encuentren en estado beta, no recomendable si se desea tener un servicio estable (Pérez, 2021).

Imagen 32

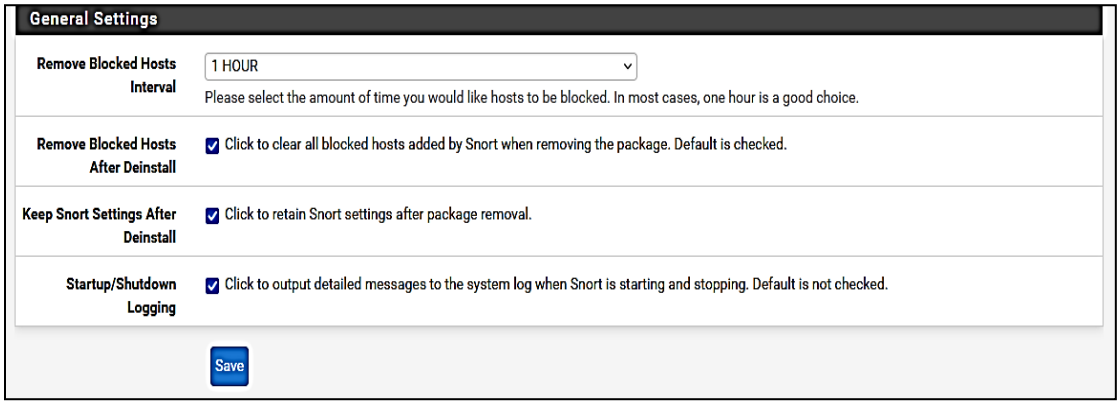
Activamos todas las reglas necesarias para Snort



Fuente: Hecho por el autor.

Imagen 33

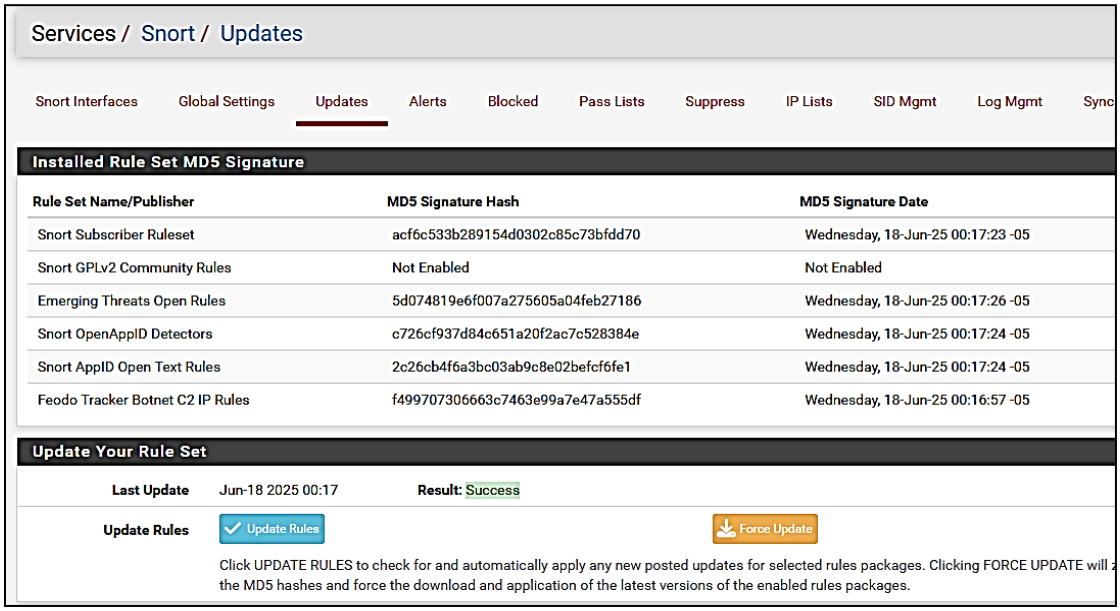
Configuramos las reglas para desconectar dispositivos que se encuentren mandando o recibiendo tráfico malicioso en el sistema



Fuente: Hecho por el autor.

Imagen 34

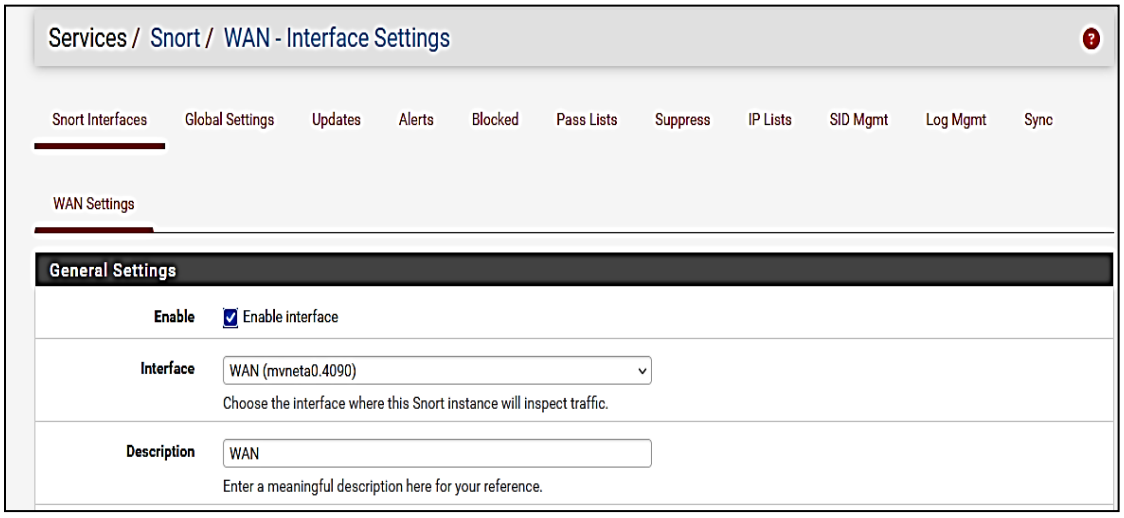
Actualizamos las reglas de Snort para mantener las reglas actualizadas y estables



Fuente: Hecho por el autor.

Imagen 35

Activamos el servicio SNORT al completo dentro de la WAN del sistema



Fuente: Hecho por el autor.

5.1.10. Switch

Para la interconexión de dispositivos mediante red cableada, se utilizará un switch D-Link, específicamente el modelo DGS-1008A, un equipo no gestionable (unmanaged) (Blanchet, Pérez, & Facchini, 2021). Este switch permitirá conectar directamente al sistema aquellos dispositivos que necesiten acceso por Ethernet, tales como puntos de acceso inalámbricos (Access Points), impresoras de red

Imagen 36

Switch D-Link que se usara en el proyecto

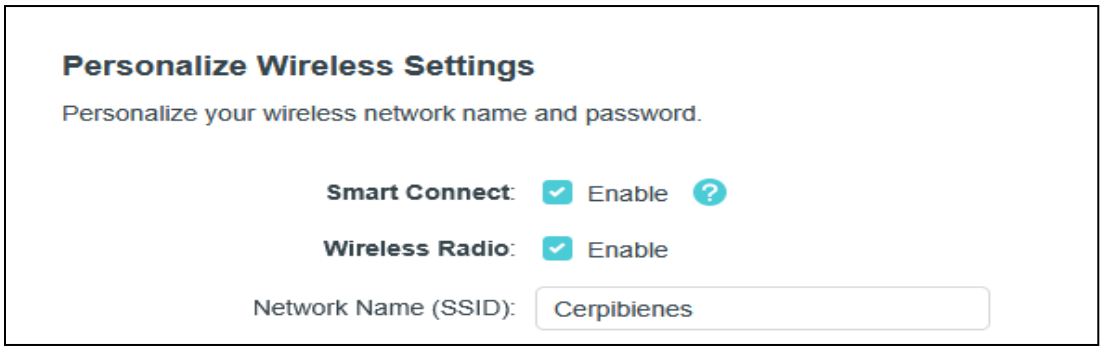
Fuente: Hecho por el autor.

5.1.11. Router Access-Point

Para proporcionar conectividad inalámbrica dentro de la infraestructura de red, se utilizará un router TP-Link AX1500 configurado en modo Access Point. Este dispositivo será responsable de ofrecer acceso Wi-Fi a los usuarios y equipos que no estén conectados por cable Ethernet.

Imagen 37

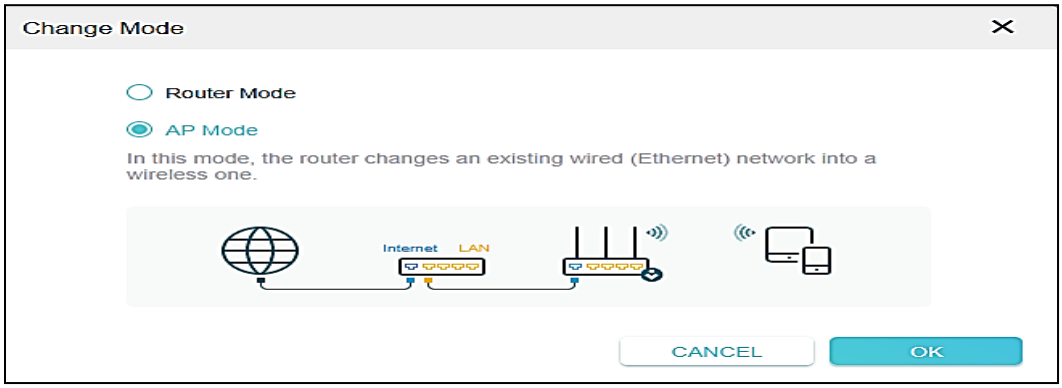
Configuración de las WLAN en el Router-AP



Fuente: Hecho por el autor.

Imagen 38

Cambio al modo AP dentro del Router TP-Link



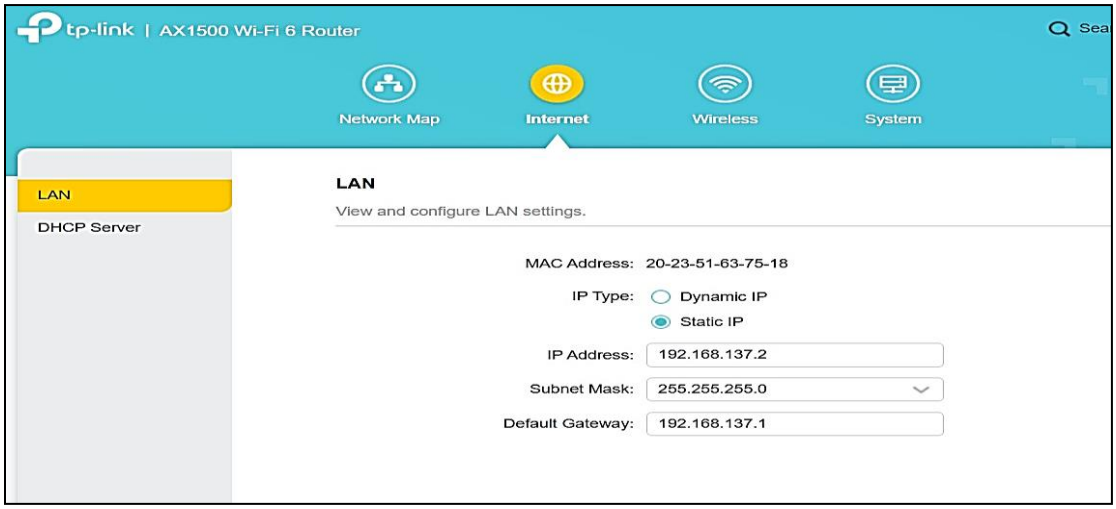
Fuente: Captura tomada por el autor.

La configuración inicial se realizará accediendo a la interfaz web de administración, disponible por defecto en la dirección IP 192.168.0.1. Desde dicha interfaz, se procederá a cambiar el modo de funcionamiento del Access Point, desactivando así funciones como el servidor DHCP y el enrutamiento NAT, que serán gestionadas exclusivamente por el firewall pfSense.

Además de que se le asignara una IP estática dentro de las IPs que dejamos reservadas en el sistema PfSense, la 192.168.137.2

Imagen 39

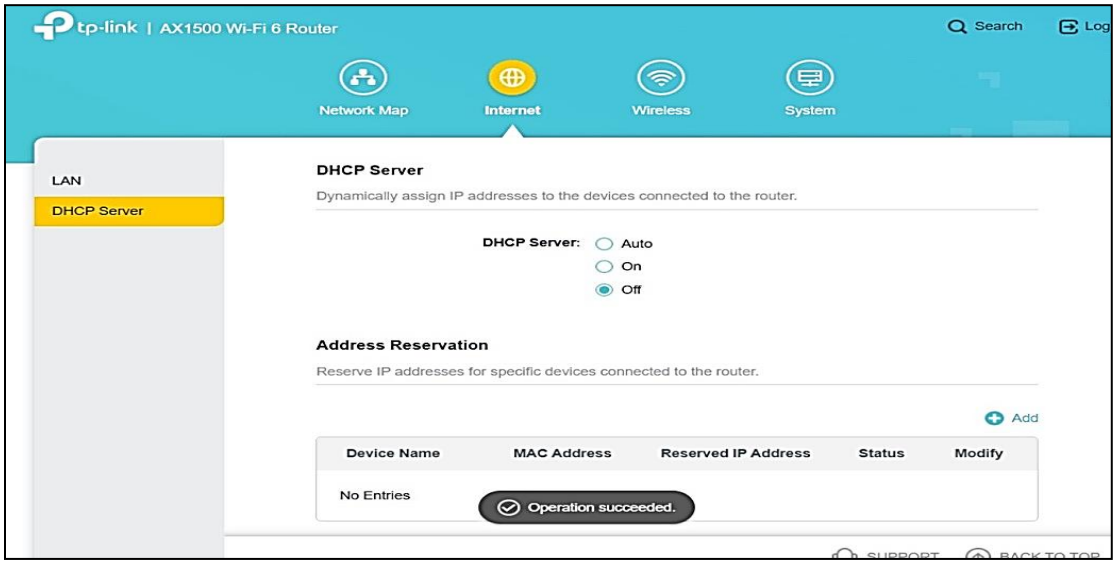
Configuración de la IP-Estática dentro del Router-AP



Fuente: Captura tomada por el autor.

Imagen 40

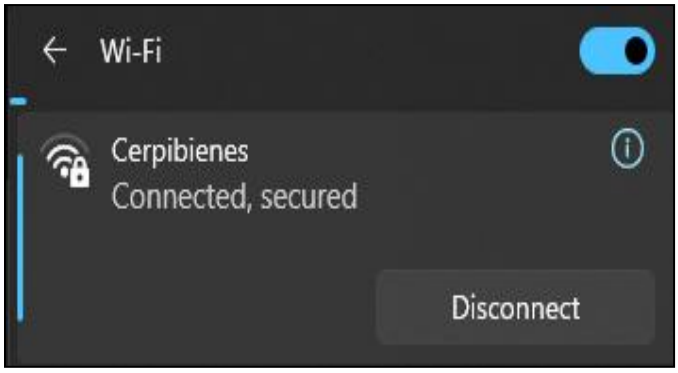
Desactivación del servidor DHCP del AP para que no de problemas de doble-NAT



Fuente: Captura tomada por el autor.

Imagen 41

Conexión inalámbrica de prueba para comprobar que el servicio funcione



Fuente: Desarrollado por el autor.

5.2. Análisis de vulnerabilidades con NESSUS

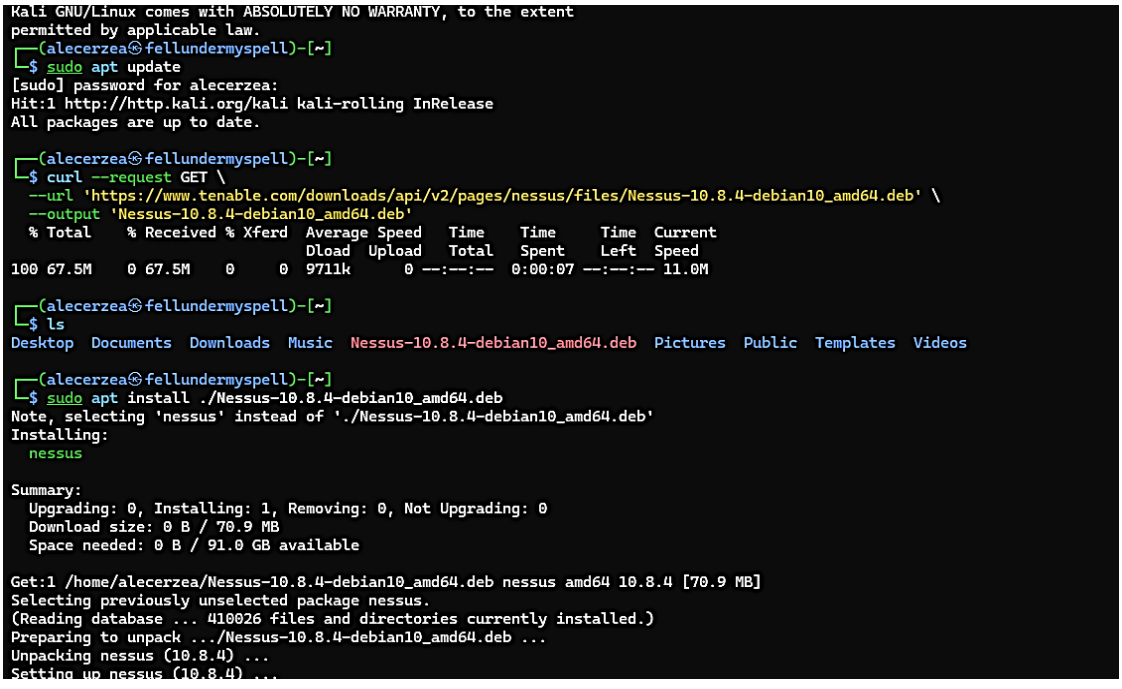
Para llevar a cabo un análisis de vulnerabilidades en la red, se utilizará la herramienta **Nessus**, una de las aplicaciones más reconocidas en el ámbito de la ciberseguridad por su capacidad para detectar fallos de configuración, puertos abiertos, servicios inseguros y otras debilidades explotables en sistemas y dispositivos de red.

Nessus será instalado dentro de una máquina virtual con Kali Linux, la cual se ejecutará en modo puente (bridge mode**)**. Esta configuración permite que la máquina virtual se comporte como un equipo más dentro de la red local, obteniendo una dirección IP directamente del servidor DHCP gestionado por pfSense.

Gracias a esta conexión directa, Nessus podrá interactuar con todos los dispositivos de la red de forma transparente, realizando escaneos completos y obteniendo resultados precisos. Esta integración facilita la detección temprana de amenazas y permite evaluar el nivel de seguridad de la infraestructura antes de su puesta en producción.

Imagen 42

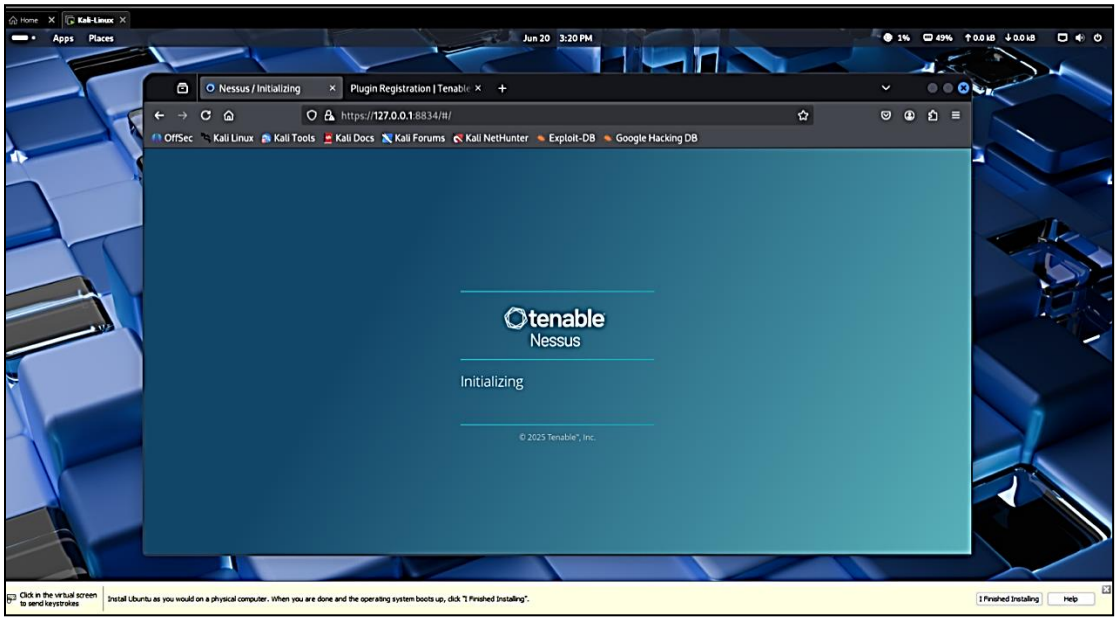
Instalación del paquete de Nessus en Kali-linux para empezar a escanear vulnerabilidades



Fuente: Captura tomada por el autor.

Imagen 43

Interfaz gráfica de Nessus en Kali-Linux



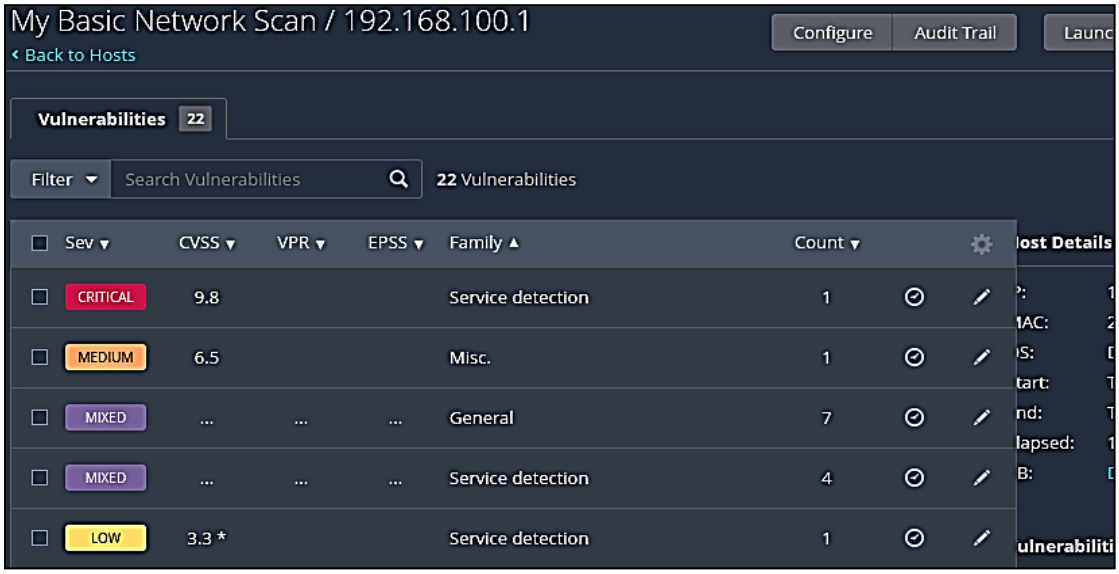
Fuente: Captura tomada por el autor.

Una vez dentro de la interfaz gráfica, iniciaremos el análisis de la red utilizando los hostnames o IPs, comparando el comportamiento entre el router anterior de la empresa y el nuevo router basado en PfSense.

Este es un escáner de vulnerabilidades ejecutado utilizando el router anterior de la empresa. Como se puede observar, se ha detectado una vulnerabilidad crítica: una falla de seguridad relacionada con los protocolos SSL 2.0 y 3.0. Esta vulnerabilidad podría permitir a un atacante interceptar y robar información mediante un ataque de tipo man-in-the-middle dentro del sistema. No es posible resolver esta vulnerabilidad desde el propio router, ya que dejó de recibir actualizaciones desde el año 2022.

Imagen 44

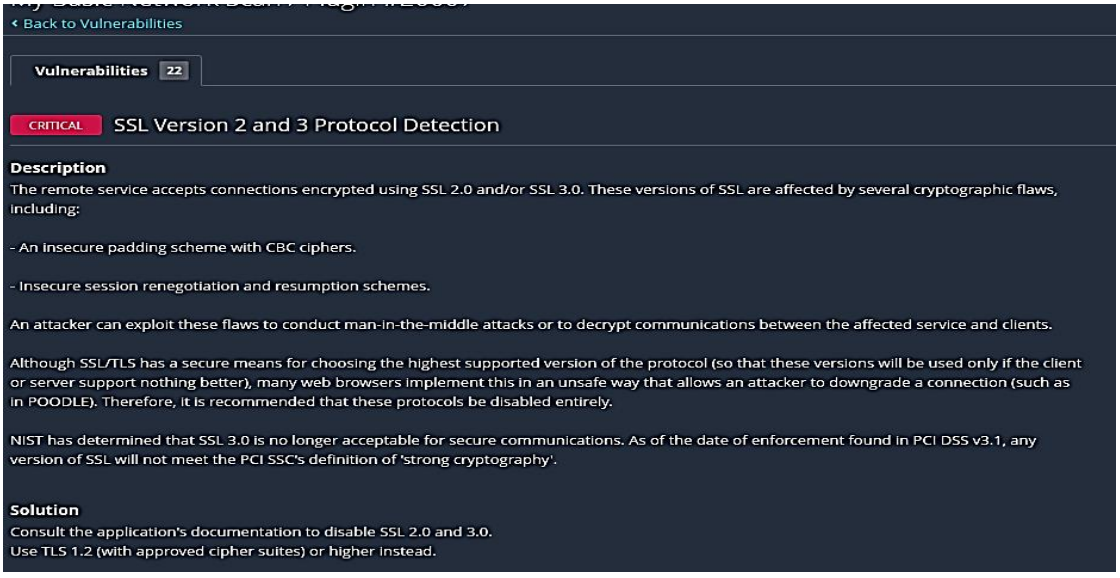
Escáner de vulnerabilidades en el router proveído por la ISP de la empresa



Fuente: Captura tomada por el autor.

Imagen 45

Explicación de la vulnerabilidad critica encontrada en el router de la empresa

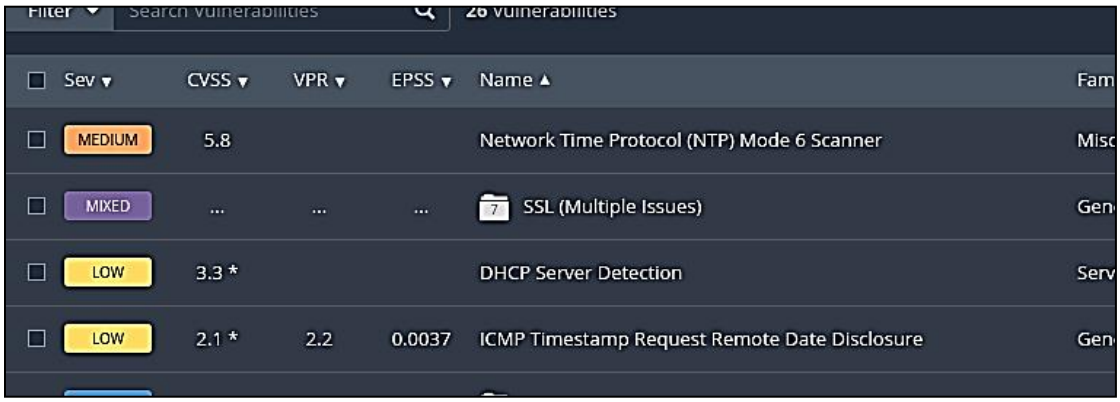


Fuente: Captura tomada por el autor.

Al realizar un escaneo de red en PfSense, se detectó una menor cantidad de vulnerabilidades en comparación con el router anterior. Además, las alertas identificadas no corresponden a vulnerabilidades reales, sino a falsos positivos. Un ejemplo de ello es la detección del servicio DHCP como una vulnerabilidad menor, cuando en realidad este servicio es esencial para permitir la conexión inalámbrica o el servicio ICMP, que nos sincroniza la hora con nuestro país.

Imagen 46

Escaneo de vulnerabilidades en el router PfSense



Fuente: Captura tomada por el autor.

5.3. Explicación de cómo funciona un ataque MAN-IN-THE-MIDDLE y DDoS

Un ataque Man-in-the-Middle sucede cuando atacante se posiciona en medio de una comunicación entre dos partes, en este caso el usuario y el router, y logra interceptar, alterar o falsificar la información que se intercambia sin que las partes logren detectarlo. Esto es posible en redes wifi vulnerabilidades en las conexiones que usan SSL 2.0 o SSL 3.0, las cuales tienen fallos en la forma en que manejan el cifrado por bloques (CBC). En redes Wi-Fi que presenten estas fallas, un atacante puede descifrar poco a poco datos sensibles, como contraseñas, cookies o tokens de sesión, poniendo en riesgo tanto la confidencialidad como la autenticidad de la comunicación (Pérez F. , 2023).

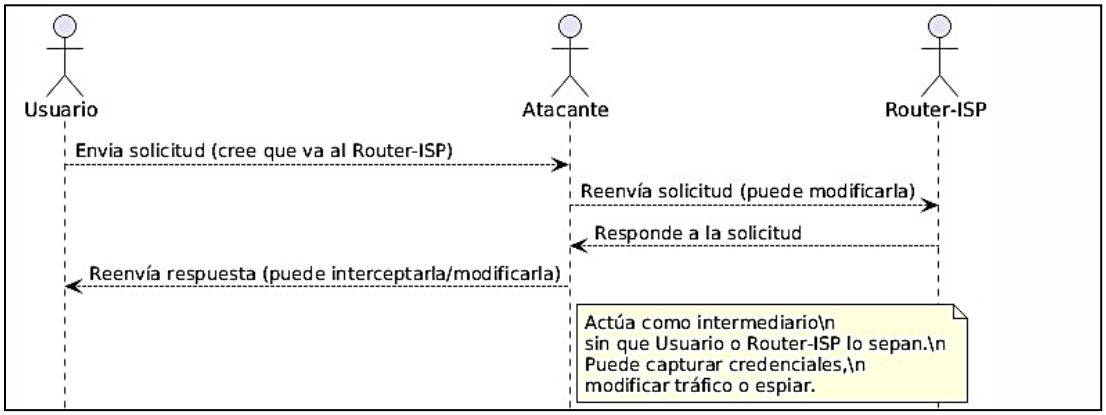
Por otro lado, un ataque de Denegación de Servicio Distribuida (DDoS) es una estrategia maliciosa diseñada para interrumpir el tráfico normal hacia un servidor, servicio o red específicos, saturando su infraestructura con una gran cantidad de datos desde Internet. El principal objetivo de un ataque DDoS es hacer que el sitio web o el servicio atacado se vuelva inaccesible para sus usuarios legítimos (Cloudflare, s.f.; Gcore, s.f.). La clave del éxito en un ataque DDoS radica en aprovechar múltiples sistemas comprometidos que generan el tráfico de ataque. Estos sistemas, que pueden variar desde computadoras personales hasta dispositivos conectados en el Internet de las Cosas (IoT), son infectados con malware y se transforman en 'bots' o 'zombies'. Cuando un atacante controla un conjunto de estos bots, se habla de una botnet, que gestiona el volumen de tráfico malicioso de manera coordinada.

5.3.1. Diagrama de secuencia 1:

Explicación de un ataque Man-in-the-middle

Imagen 47

Explicación de un ataque Man-in-the-middle



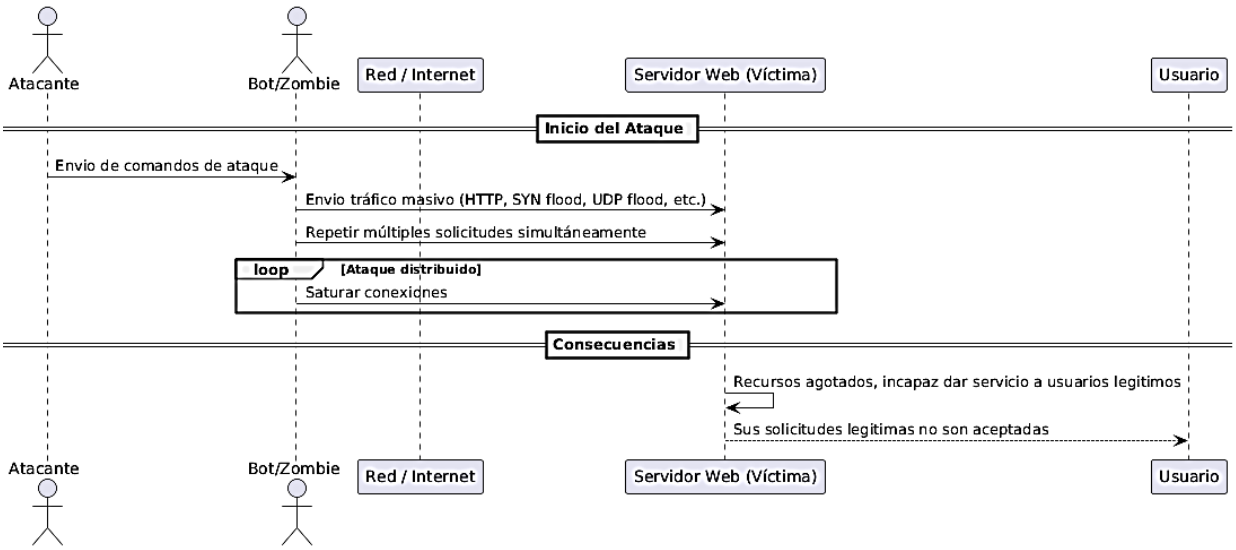
Fuente: UML Hecho por el autor.

5.3.2. Diagrama de secuencia 2:

Explicación de un ataque DDoS

Imagen 48

Explicación de un Ataque DDoS



Fuente: Captura tomada por el autor.

¿Como nos protegería PfSense?

Cuando un usuario intente establecer una conexión a través de la red, pfSense analiza en tiempo real todo el tráfico entrante y saliente, verificando que sea legítimo según las reglas predeterminadas por Snort. Si un atacante tratara de iniciar un ataque Man-in-the-Middle, pfSense podrá detectar esos patrones sospechosos y redirigir ese tráfico a Snort para un análisis más profundo. Gracias a sus reglas, Snort bloqueara la actividad maliciosa. Con la respuesta de Snort, pfSense bloqueara automáticamente la conexión del atacante, rechazando cualquier tráfico no autorizado y garantizando que solo la comunicación del usuario autorizado siga activa. Esta integración permite detectar y responder a amenazas en tiempo real, protegiendo la integridad de las comunicaciones mediante el bloqueo de la dirección IP del atacante, expulsándolo de la red (Andino, 2022).

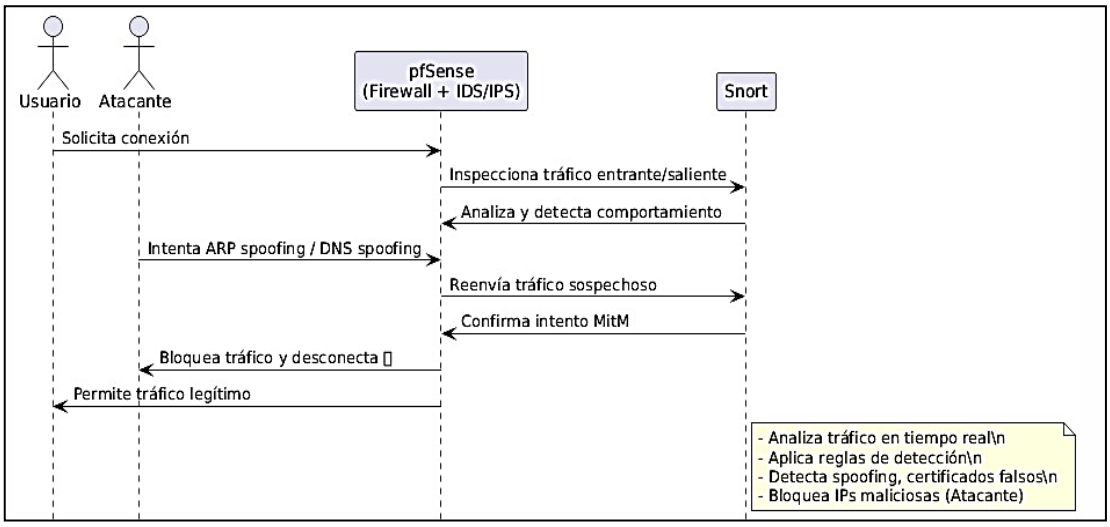
Para la defensa contra ataques de denegación de servicio, se usaría la aplicación PfBLocker, recientemente instalada en el sistema, esta nos protege la red mediante el bloqueo de direcciones IP maliciosas conocidas. Para ello, se apoya en extensas bases de datos de inteligencia de amenazas que se actualizan continuamente, incluyendo millones de direcciones IP vinculadas a actividades perjudiciales. Esto significa que, si una IP forma parte de una botnet empleada en ataques DDoS o ha sido identificada repetidamente como fuente de amenazas, PfBlockerNG la bloqueará automáticamente en el perímetro de nuestra red. Esta acción temprana es fundamental para reducir significativamente la cantidad de tráfico malicioso que llega a nuestro firewall principal, ayudando a prevenir la saturación de ancho de banda y recursos por ataques DDoS. Además, al bloquear las IPs de los centros de control y comando de malware, añadimos una capa adicional de protección contra ciertos tipos de ataques Man-in-the-Middle y actividades de exfiltración de datos.

5.3.3. Diagrama de secuencia 3:

Explicación de como PfSense evitaría un ataque Man-in-the-middle

Imagen 49

Evito de un Ataque Man-in-the-middle



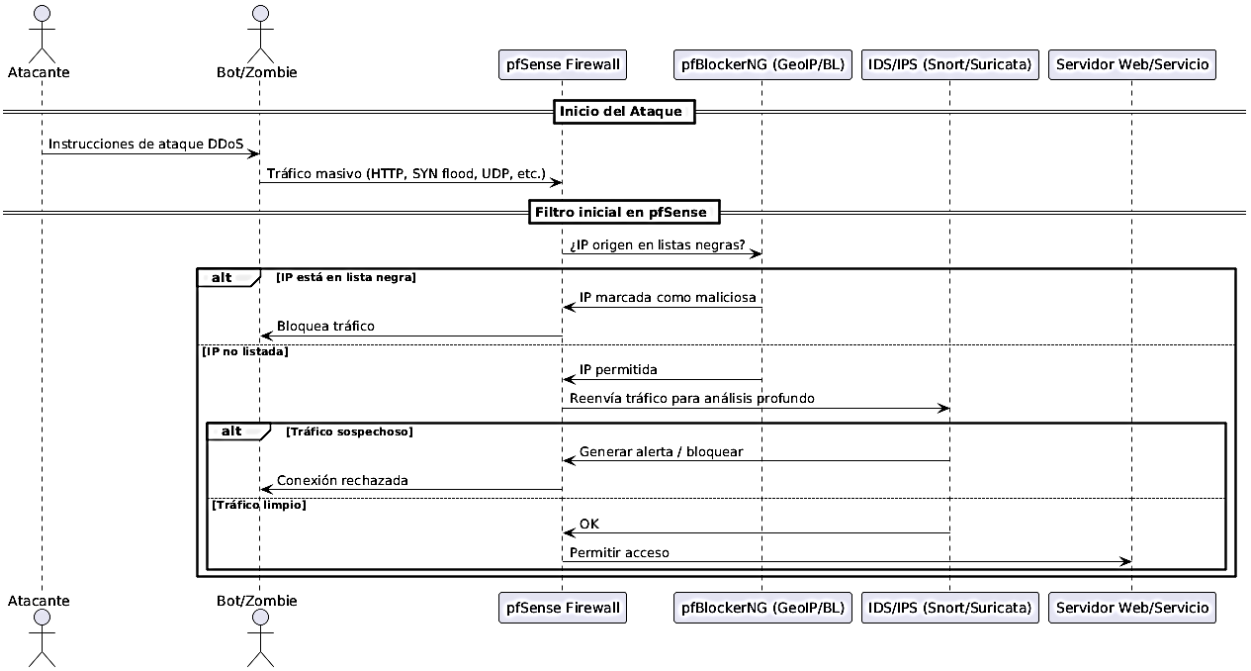
Fuente: UML Hecho por el autor.

5.3.4. Diagrama de secuencia 4:

Explicación de como PfSense evitaría un ataque DDoS

Imagen 50

Evito de un Ataque DDoS



Fuente: UML Hecho por el autor.

5.4. Comparativo de PfSense entre Fortinet y CheckPoint

Mapa Conceptual 1:

Comparativo entre Firewalls con PfSense, Fortinet, Checkpoint

Imagen 51

Comparativa de firewalls

Fuente: Mapa Conceptual Hecho por el autor.

6. CONCLUSIÓNES Y RECOMENDACIONES

La seguridad de red es una necesidad que, hasta hace poco tiempo, no era algo de fácil acceso a empresas que contaran con presupuestos limitados. En el mundo en el que vivimos donde las amenazas cibernéticas crecen a cada momento, es necesario implementar soluciones de seguridad eficientes sin incurrir en gastos elevados. La propuesta de utilizar dispositivos Netgate con pfSense demuestra que es factible contar con un firewall profesional, con funciones avanzadas como filtrado de paquetes, detección de intrusos y control de acceso, sin necesidad de grandes inversiones. Gracias a su carácter de código abierto y su enfoque modular, pfSense se posiciona como una herramienta robusta y accesible que permite a pequeñas empresas como CERPIBIENES fortalecer significativamente su seguridad informática sin comprometer su viabilidad económica. Esta solución representa un paso firme hacia una infraestructura de red más segura, escalable y sostenible.

Unas recomendaciones que puedo dar a futuro para empresas que deseen implementar el sistema PfSense a futuro, la primera será el uso de un router y modem separados, esto no solo simplifica la configuración, sino que reduce parte del presupuesto necesario, pues el router separado puede ser reusado como punto de acceso para conexiones inalámbricas dentro de la empresa, quitando la necesidad de un punto de acceso externo.

7. REFERENCIAS BIBLIOGRÀFICAS

Álvarez, R. (2024). PentesTool.

Andino, E. (2022). Evaluación del Firewall de Frontera Free Pfsense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba año 2021.

Blanchet, R., Pérez, S., & Facchini, H. (2021). Estudio y simulación de redes definidas por software y automatización de red.

Briceño, E. (2021). Seguridad de la información.

Carmona, J. (2024). Interconexión de redes de forma segura mediante cortafuegos pfSense.

Castillo, J. (2024). Integración de soluciones de ciberseguridad en software libre para la protección de las pymes aplicado para la Fundación de Atención al Discapacitado.

Cavazos, A. (2021). Inteligencia de seguridad y analítica nacional (ISA): método para el análisis y la investigación del panorama de ciberataques en México mediante el uso inteligencia de amenazas y ciencia de datos.

Colque, M. (2021). NMAP COMO UNA HERRAMIENTA PARA LA SEGURIDAD DE REDES. REVISTA CIENTÍFICA: CIENCIA Y TECNOLOGÍA INFORMÁTICA, , 2(2), 22-25.

Eduardovych, B. (2024). Diseño e implementación de un sistema integrado de monitorización de eventos de seguridad.

Fainchtein, R. (2023). No Sieve is Good Enough: Examining the Creation, Enforcement and Evasion of Geofilters.

Ferrer, C. (2023). Firewall DNS Como herramienta para la protección de los menores de edad en el ámbito escolar y familiar.

Flames, J. (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.

González, J. (2025). Ciberseguridad industrial.

Kaspersky. (2022). 87 critical vulnerabilities discovered in routers in 2021. Kaspersky.

Lomelí, G., Duarte, V., & Gutiérrez, J. (2025). Optimización dinámica del rango de direcciones IP mediante el análisis del protocolo DHCP y un algoritmo adaptativo basado en software libre. ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica, 14(1), C1-19.

Martínez, G. (2023). Análisis técnico comparativo de herramientas de escaneo de puertos de redes de telecomunicaciones.

Mazacon, M. (2022). Análisis comparativo sobre las herramientas de Seguridad Informática Open Source: Nessus y Snort.

Mejía, M., Ortiz, C., Ramos, W., & Moscoso, L. (2022). Gestión del tráfico de red en la calidad de servicio “QoS” WAN en Tambopata-Perú 2021. Revista de ciencias sociales, 28(2), 300-318.

Mena, I. (2025). Optimización de la Seguridad Informática en Infraestructuras de Redes Corporativas.

Paucar, L., & Tipán, A. (2022). Ensamble de un adaptador inalámbrico para el desarrollo del software sniffer en una red LoRaWAN y análisis con Wireshark.

Pérez, A. (2021). Evaluación de sistemas de detección de amenazas: Snort y Suricata.

Pérez, F. (2023). Análisis de los ciberataques. El ataque Man-In-The-Middle y el SSLstrip.

Quezada, O., Aguilar, D., & Marroquín, E. (2023). Guía para la evaluación de la ciberseguridad en instituciones privadas.

Rochina, C. (2021). Diseño y evaluación de una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

Romero, G. (2023). Análisis comparativo de las herramientas Open Source Brazilfw y Pfsense, en los aspectos de seguridad en entornos de red .

Santos, J., & Córdoba, C. (2024). Análisis de Vulnerabilidades en un Entorno de Red Virtual: Implementación de Nessus como Herramienta de Evaluación. Revista de Ciencias de Seguridad y Defensa, 9(03), 13-13.

Tigrero, D. (2025). Monitoreo de red inteligente usando IDS y dispositivos de edge computing.

Toala, B., Segovia, E., & Zúñiga, K. (2022). LAS REDES WAN Y SU IMPORTANCIA PARA LOS ORDENADORES: LAS REDES WAN Y SU IMPORTANCIA PARA LOS ORDENADORES. UNESUM-Ciencias. Revista Científica Multidisciplinaria, 6(1), 1-14.

Tomala, R. (2023). Implementación de una infraestructura de red mediante redes LAN y WLAN, empleando equipos de redes, para la optimización de la red de la Institución Educativa Ancón.

Zhang, L., Wang, T., & Liew, S. (2022). Speeding up block propagation in Bitcoin network: Uncoded and coded designs. Computer Networks, 206, 108791.

Cloudflare. (s.f.). *What is a distributed denial-of-service (DDoS) attack?*