UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

"MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS UTILIZANDO UN FIREWALL DE SOFTWARE LIBRE CON PFSENSE EN LAS EMPRESAS DE REVISIONES TÉCNICAS DE LA CIUDAD DE TACNA EN EL AÑO 2021"

PARA OPTAR:

TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. MÁXIMO FABRIZZIO ESPINOZA PECHE

TACNA - PERÚ

2022

UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

"MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS UTILIZANDO UN FIREWALL DE SOFTWARE LIBRE CON PFSENSE EN LAS EMPRESAS DE REVISIONES TÉCNICAS DE LA CIUDAD DE TACNA EN EL AÑO 2021"

Tesis sustentada y aprobada el 18 de noviembre de 2022; estando el jurado calificador integrado por:

PRESIDENTE	**:**	**Mag. JOSÉ MARCIAL SUMARRIVA BUSTINZA**
SECRETARIO	**:**	**Ing. ALFREDO ESTEBAN CALIZAYA CRUZ**
VOCAL	**:**	**Mag. MARCO ANTONIO SEBASTIÁN COLOMA YUNGANINA**
ASESOR	**:**	**Ing. MARKO JESUS POLO CAMACHO**

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Maximo Fabrizzio Espinoza Peche, en calidad de bachiller de la escuela profesional de ingeniería electrónica de la facultad de Ingeniería de la Universidad Privada de Tacna, identificado con DNI 70674058 declaro bajo juramento que:

1. Soy autor de la tesis titulada: *"Mitigación de vulnerabilidades informáticas utilizando un firewall de software libre con pfSense en las empresas de revisiones técnicas de la ciudad de Tacna en el año 2021"* la misma que presento para optar el título profesional de *ingeniero electrónico.*
2. La tesis no ha sido plagiada ni total ni parcialmente, habiéndose respetado las normas internacionales de citas y referencias para las fuentes consultadas.
3. La tesis presentada no atenta contra los derechos de terceros.
4. La tesis no ha sido publicada ni presentada anteriormente para obtener algún grado académico o título profesional.
5. Los datos presentados en los resultados son reales, no hay sido falsificados, ni duplicados, ni copiados.

Por lo expuesto, mediante la presente asumo frente a *La Universidad* cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido de la tesis, así como por los derechos sobre la obra.

En consecuencia, mediante hago responsable, frente a *La Universidad* y a terceros, de cualquier daño que pudiera ocasionar, por el incumplimiento de lo declarado o que pudiera encontrar como causa del trabajo presentado, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las encontrasen causa en el contenido de la tesis.

De identificarse fraude, piratería, plagio, falsificación o que la obra haya sido publicada anteriormente; asumo las consecuencias y sanciones que mi acción se deriven, sometiéndome a la normativa vigente de la Universidad Privada de Tacna.

Tacna, 18 de noviembre del 2022

MAXIMO FABRIZZIO ESPINOZA PECHE
70674058

DEDICATORIA

A mis padres Maximo y Julia y a mi pequeña hermana Florencia, por acompañarme a lo largo de mi vida brindándome los consejos para cada día ser mejor y superarme a mí mismo.

A mi abuelo Máximo, quien me dejó tanto conocimiento histórico del país, de mi ciudad y de mi familia y que me vigila desde el cielo.

AGRADECIMIENTOS

A mi entrenador de atletismo, Sr. Eduardo Ojeda, por ser una gran padre, maestro, consejero y amigo, dándome las lecciones de vida necesarias para alcanzar mis objetivos.

A mi asesor de tesis, ingeniero electrónico Marko Polo, un gran profesional que supo guiarme por cada etapa de este proyecto. Y al ingeniero electrónico Renatto Montesinos, intachable profesional y amigo que me brindó las pautas y recomendaciones iniciales de este proyecto.

A Melanny, el apoyo en esta etapa de mi vida, por su cariño y palabras de aliento para poder llegar a ser un profesional que me ayudaron a mantenerme enfocado en mis metas, gracias por darme ese empujón que siempre necesité.

A mis compañeros de carrera, que juntos vivimos momentos inolvidables dentro y fuera de las aulas y compartimos algunas experiencias de muchas que nos espera el camino.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Objetivo: Diseñar, elaborar y ejecutar un hardware de mitigación de vulnerabilidades cibernéticas, Firewall, utilizando el software de código abierto pfSense de compilación Linux, con materiales tecnológicos dentro de la misma empresa de revisiones técnicas y así, optimizar los recursos de la misma para brindar una capa adicional de seguridad en lo que respecta a las tecnologías de la información. **Método:** Se realizó el diseño experimental de la presente tesis cual fue ejecutado en tiempo real en una copia del servidor principal de la revisión técnica, utilizándose dominios y puertos específicos para poder funcionar a manera de espejo. **Resultados:** la obtención de datos luego de implementar el firewall en la arquitectura de la red y realizar simulaciones de ataques cibernéticos como phishing y man-in-the-middle, fue exitosa para la mitigación de estos ataques, enviando alertas (logs) al administrador cuando se presentaba alguno de estos casos. **Conclusiones:** la implementación de un Firewall en una pequeña y/o mediana empresa en la actualidad es de vital importancia frente al auge de la era digital que evoluciona a paso acelerado en el Perú, junto también con los actores maliciosos que surgen por ello.

Palabras Clave: Mitigación, Vulnerabilidad, Firewall, pfSense, Linux, empresa, revisión técnica, dominios, puertos, ataques cibernéticos, phishing, alertas (logs).

ABSTRACT

Objective: Plan, design and elaborate a cybernetics vulnerabilities mitigation hardware, Firewall, using a free code software as pfSense with Linux compilation, using technological materials found inside the technical revision center so then optimize the resources of the center giving itself an additional information technologies security layer. **Method:** the experimental design whose was made for this project was executed on real time using a backup of the technical revision center main server, domains and specific open ports were used for making it work as a mirror server. **Results:** data obtention after implementing the Firewall in the LAN architecture and making hacking simulations to itself as phishing and man-in-the-middle, was successfully mitigated against these attacks, sending logs to the I.T. administrator when an alert was prompted. **Conclusions:** Nowadays, Firewall implementation in a small and medium company it's of vital importance facing the quick rise of digital era in Peru, along with the growing of malicious cybernetics actors.

Key Words: mitigation, vulnerabilities, firewall, pfSense, Linux, Company, Technical Revision Center, Domains, Ports, cybernetics attacks, phishing, logs.

INTRODUCCIÓN

A finales del año 2019, la enfermedad conocida como coronavirus (COVID-19 – Corona-Virus-Disease-2019) causado por el virus SARS-CoV-2, alertó a la población mundial y es declarado pandemia por la OMS el 11 de marzo del año 2020. A raíz de esto, la mayoría de los países afectados optaron por medidas sanitarias específicas para mitigar el avance de la enfermedad, en especial, la cuarentena obligatoria (*Lockdown*).

En el Perú, se tuvo que apresurar el salto al uso de tecnologías digitales sin distinción de rublo, para evitar el contacto físico entre personas al momento del intercambio de servicios o bienes. Esto dio origen a la implementación de manera casi obligatoria de la tele-educación, la tele-medicina, y el tele-trabajo en la mayoría de las empresas privadas y públicas, para evitar que, tanto su personal como los clientes, sean afectados por esta enfermedad y cuidar a los trabajadores que se encuentren dentro de la población con comorbilidades y con vejez.

La rapidez con la cual se dio este salto tecnológico fue un reto para la mayoría de las instituciones y empresas que, en su momento, minimizaron el hecho de tener una infraestructura de red electrónica de datos digitales correctamente diseñada, puesto que contaban con dispositivos de red (o de acceso) desfasados para el uso remoto y/o contaban con una red empresarial que no es debidamente escalable. Es a razón de esta deficiencia estructural digital en la mayoría de las empresas, como también la carencia de políticas de seguridad informática que permite que personajes con fines maliciosos encuentren una vulnerabilidad informática que les permite robar, ocultar y/o eliminar información sensible de la empresa empleando una variedad de ataques cibernéticos.

Una reducida cantidad de empresas aplican una política de seguridad informática teniendo en cuenta estas amenazas, lo cual conlleva a la implementación de equipos de seguridad informática como Firewalls, *IPS*, *IDS* e inclusive el propio servicio de antivirus en ordenadores para así reducir o eliminar estas vulnerabilidades que se puedan presentar.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

La carga informática de datos digitales con la cual tienen que lidiar todos los sectores económicos y sociales es muy alta a comparación de años anteriores. Actualmente, el nivel básico de seguridad informática con la que cuenta la mayoría de hogares, sectores profesionales y entornos empresariales de la ciudad de Tacna, tienen políticas de seguridad que, al encontrarse desfasadas, los vuelven blancos fáciles contra los actores maliciosos.

El internet se ha convertido en una necesidad primordial para el inicio y desarrollo de actividades de todo tipo de negocio. Acceder a los recursos de la gran red para poder gestionar una entrega, obtener información específica o corroborar datos con un servidor de autenticación, es más común al día de hoy que en otros años.

Las pequeñas empresas de revisiones técnicas de la ciudad de Tacna representan mi caso de estudio. Donde el testimonio y la experiencia vivida por aquellas empresas de este tipo frente a ataques cibernéticos compone la base de la formulación de un método que mitigue la vulnerabilidad que en algún momento padecieron, procediendo a reforzar su estructura de red como la seguridad informática de esta.

1.2. Formulación del problema

¿Las empresas de revisiones técnicas se encuentran protegidas frente a vulnerabilidades informáticas que afecten significativamente en la confidencialidad y monetización de sus bases de datos?

1.3. Justificación del problema

En la actualidad, la rapidez con la que se implementó mejoras digitales y tecnológicas con la que la mayoría de países más desarrollados puedan sobrellevar la temida pandemia del COVID-19 y adaptarse al empleo y uso de plataformas digitales, creó una brecha informática para aquellas personas y empresas que carecían de conocimientos sobre la seguridad de las tecnologías de la información.

A raíz de esto, el alarmante incremento de los crímenes cibernéticos contra personas naturales y personas jurídicas en el Perú permiten distinguir con claridad

cuáles son las necesidades que estas requieren satisfacer para mejorar su seguridad informática; como también mejorar su estructura electrónica de datos digitales.

En los centros de inspección técnica vehicular, se busca la disponibilidad, integridad y confiabilidad de los datos procesados en todo momento, desde el inicio de apertura hasta la entrega del certificado de revisión técnica.

Es por eso que, el diseño de Firewall que implementaré en este tipo de empresa, logrará que tenga la robustez necesaria en políticas de ciber-seguridad para así poder mitigar alguna vulnerabilidad que se encuentre presente.

1.4. Objetivos

1.4.1. Objetivo General

Desarrollar e implementar un firewall basado en el sistema operativo de software libre pfSense, que mitigue la vulnerabilidad informática de las empresas de revisiones técnicas en la ciudad de Tacna, año 2021.

1.4.2. Objetivos Específicos

a) Identificar las diferentes amenazas informáticas que afecten la operatividad de las empresas de revisiones técnicas en Tacna
b) Implementar políticas de seguridad informática que reduzcan su vulnerabilidad
c) Instalar y configurar el firewall con pfSense, que permita detectar las amenazas informáticas

1.5. Hipótesis

Se desarrollará e implementará un Firewall que mitigará las vulnerabilidades que se presenten en una empresa de revisiones técnicas de Tacna.

a) La identificación a tiempo de las amenazas informáticas mitigará las vulnerabilidades que puedan existir frente a estas en la empresa de revisiones técnicas.
b) La implementación de políticas de seguridad informática permitirá reducir el riesgo de presentarse vulnerabilidades en la empresa de revisiones técnicas.
c) La instalación y configuración del Firewall con pfSense, permitirá a la detección de amenazas informáticas.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes del estudio

Ruiz y Delgado (2018) realizaron un trabajo titulado “Implementación de una solución de seguridad perimetral Open Source en La Red telemática de la Universidad Nacional Pedro Ruiz Gallo” en el cual presentó una solución de seguridad perimétrica de código libre cubriendo unos requerimientos de red perimetral DMZ utilizando el software de pfSense. Aplicó configuraciones que permiten realizar trabajos de monitoreo, bloqueo y restricciones de tráfico web para proteger datos de la institución.

El trabajo realizado por Oliveira (2016) titulado “Efecto de la implementación del sistema pfSense en la seguridad perimetral lógica en los servicios de la red troncal de la universidad Nacional de la amazonia Peruana, Iquitos” en el cual configuró de forma remota un firewall lógico implementado con FreeBSD desde la ciudad de Lima para poder realizar pruebas con respecto a la evolución de las amenazas informáticas y la fiabilidad y protección de datos que brindaría este sistema de seguridad para la universidad Nacional de la amazonia Peruana.

Zapata (2012) proyecto titulado “Estudio de las técnicas de control de acceso a internet y su aplicación en la red de datos del colegio Corina Parral de la ciudad de Chimbo” en la cual concluye que ningún firewall puede defenderse de manera automática contra cada nueva amenaza que surge, este firewall debe mantenerse actualizado constantemente contra las amenazas que surgen día a día.

2.2. Bases teóricas

2.2.1. Redes de computadoras

Una red de computadoras es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro tipo de transporte de datos. (*Gorgona, n.d*).

Se llama así a la interconexión de computadoras para compartir información, recursos y servicios. Éstas utilizan protocolos de red y un conjunto de reglas y procedimientos que deben respetarse para el envío y recepción de datos en la red y así asegurar que la información llegue a su destino.

Estas se pueden clasificar de varias formas:

- Por su extensión las redes pueden ser:
    - Área de red personal (PAN)
    - Área de red Local (LAN)
    - Área de red metropolitana (MAN)
    - Área de red amplia (WAN)
- Por topología:
    - Red de anillo
    - Red de bus
    - Red de bus-estrella
    - Red de estrella

2.2.2. Mitigación

Se trata de un proceso que reduce esencialmente la probabilidad de que una vulnerabilidad sea explotada (Tori, 2020).

Es una forma de ganar tiempo mientras que la organización espera que se lace la tecnología adecuada o se encuentre el momento apropiado para programar un tiempo de inactividad en el sistema, International Business Machines (IBM,2021).

Mitigar, en el campo digital, es la acción que toma la persona encargada del área de ciberseguridad de una empresa para poder evitar un ataque informático y también, contrarrestarlo para evitar una reincidencia.

2.2.3. Vulnerabilidades Informáticas

Vulnerabilidad es la debilidad que tiene un sistema y puede ser aprovechada para comprometer su seguridad de datos por una persona malintencionada (Fortinet, 2020).

Las vulnerabilidades informáticas son aquellas deficiencias en el diseño de la seguridad de un software, un equipo informático como también en una red de área local o amplia de una compañía, estas detallan los diferentes puntos por donde el atacante pudiera ingresar al sistema y obtener datos del mismo.

2.2.4. Servidor

En el campo de la informática y las telecomunicaciones, servidor se entiende por un equipo informático que forma parte de una red y provee servicios a otros equipos. Algunos de estos servidores pueden ser:

- Servidor de impresiones
- Servidor de correo.
- Servidor de acceso remoto.
- Servidor de base de datos.
- Servidor de seguridad.

2.2.5. Amenazas informáticas

Un intruso que logra obtener un acceso modificando software o explotando vulnerabilidad de software en una determinada red privada se denomina actor de amenaza (Cisco, 2019).

Estas pueden ser agrupadas en cuatro grandes categorías: factores humanos (accidental, errores), fallas en los sistemas de procesamiento de la información, desastres naturales y actos maliciosos, algunas de estas amenazas son:

- Virus informático o código malicioso
- Robo de información
- Suplantación de identidad
- Denegación de servicios
- Ataques de fuerza bruta
- Entre otros

2.2.6. Firewall

Un sistema de firewall se localiza entre la red privada y el internet, este equipo refuerza la regla de acceso de seguridad controlando los enlaces establecida entre dos o más redes (Senthilkmar y Muthukumar, 2020).

Es un dispositivo electrónico que previene el ingreso del flujo de tráfico no deseado hacia una organización. Es resistente contra ataques de red, todo el tráfico de red fluye a través de él y mejoran las políticas de seguridad de una empresa.

Algunos enrutadores modernos poseen propiedades de firewall en su sistema operativo, lo que hace que empresas con políticas de seguridad menos estrictas opten por no utilizar un hardware especifico de firewall, pero quedando vulnerables ante ataques elaborados de penetración de tecnologías de la información.

2.2.7. Implementación de la tecnología de Firewall en una empresa

- **Red de borde - OUTSIDE**

Es la red directa que brinda acceso al internet brindado por el ISP, aquí es donde se origina el tráfico unstrusted (no confiable) y este no tiene acceso a la red interna de la empresa.

- **Red perimetral - DMZ**

Permite la conexión entre usuarios de redes externas a servidores que se encuentren en la red interna basados en políticas de seguridad asignadas de acuerdo al tipo de tráfico inspeccionado.

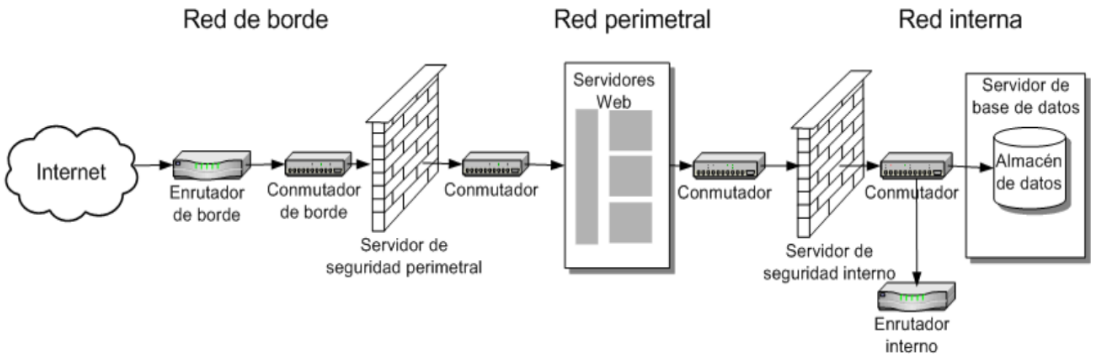
- **Red interna - INSIDE**

Es la red donde se encuentra el conjunto de servidores privados que brindan servicios a los usuarios internos de la red, aquí se origina el tráfico trusted (confiable) que es inspeccionado y permitido de acceder a la red de borde, y el intercambio de tráfico es asociado como trusted y es permitido.

La arquitectura de una red empresarial debidamente organizada es representada por la figura 1, utilizando su red de borde para las comunicaciones con el exterior, la red perimetral para el acceso externo controlado y la red interna con la base de datos principal (véase figura 1).

Figura 1

Ejemplo de una arquitectura de red informática segmentada por tres etapas.



Nota. representación gráfica obtenida por TechNet, España, 2019, del sitio web https://www.microsoft.com/spain/technet/recursos/articulos/secmod156.mspx

2.2.8. pfSense

Es una distribución libre de cortafuegos de red, basado en el sistema operativo FreeBSD con un kernel personalizado que incluye paquetes de software de terceros para funcionalidades adicionales. Incluye una interfaz web para la configuración de todos sus componentes.

- Hardware: puede utilizarse un hardware especifico requerido por Netgate ® o virtualizarlo en un hardware que se adecue a las especificaciones necesarias por usuario.
- Cloud: Provee protección cortafuegos a través de la nube, lo que lo hace muy confiable para regiones aisladas.

La funcionalidad de pfSense contiene:

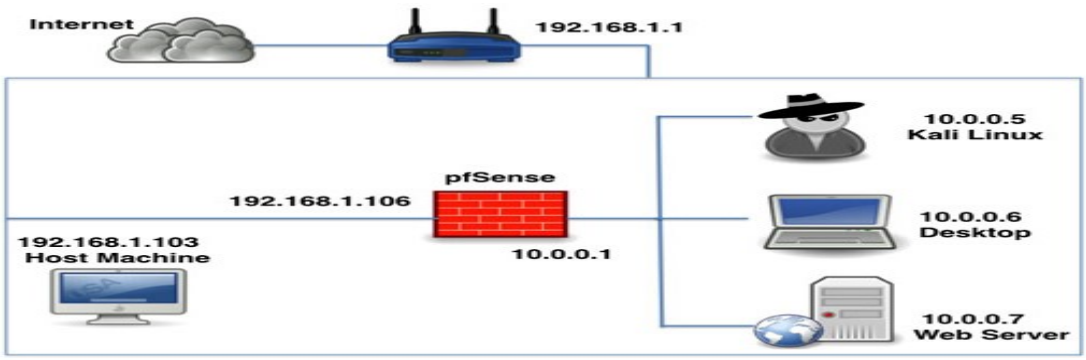
- *Firewall*, configurado como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a parte de una dirección ya sea de red o de host de origen y destino.
- *Servidor VPN*, usando protocolos de tunneling como IPSec, PPTP, entre otros.
- *Servidor de Balanceo de carga,* característica usada en servidores web, de correo y dns. Provee estabilidad y redundancia en el envío de tráfico a través del enlace WAN.
- *Portal Cautivo*, fuerza la autenticación de usuarios redirigiéndolos a una página de autenticación.
- *Tabla de estado,* guarda el estado de las conexiones abiertas en una tabla.
- *Servidor DNS.*

- *Servidor DHCP*, además de poder implementar VLANs.
- *Servidor PPPoE*, usado para la autenticación de usuarios para ingresar a internet.
- *Enrutamiento estático,* función de router y nat.
- *Redundancia,* permite configurar dos o más cortafuegos a través del protocolo CARP (Common Adress Redundacy Protocol)
- *Reportes y monitoreo.*

La representación lógica de una implementación de firewall en un entorno de red como la figura 2, muestra el funcionamiento de un firewall PfSense dentro de un entorno real donde tenemos un servidor web, un router y una máquina de host. (Véase figura 2).

Figura 2

Representación lógica de los equipos de red utilizando pfSense



Nota. Representación lógica por Inforsec institute, Internet, 2015, del sitio web https://resources.infosecinstitute.com/topic/setting-pentest-lab-pfsense-virtualbox/ , Srinivas.

2.2.9. Revisiones Técnicas en el Perú (C.I.T.V.)

En los centros de inspección técnica vehicular (C.I.T.V.) se evalúa, verifica y certifica el buen funcionamiento y mantenimiento de los vehículos, así como el cumplimiento de las condiciones y requisitos técnicos establecidos en la normativa nacional, con el objeto de garantizar la seguridad del transporte y tránsito terrestre, y las condiciones ambientales saludables.

Estos centros se ubican por región y operan de acuerdo a decretos supremos y normas que establezca el estado.

La sensibilidad de los datos informáticos que manejan es de carácter muy alto, ya que transportan la información vehicular completa del tipo de vehiculo que haya pasado su revisión técnica en el centro de inspección (por ejemplo: carrocerías M1, M2, N1, N2, L3, L5, entre otros). Como también información de los dueños de los vehículos que hayan pasado la revisión técnica (SOAT, tarjeta de propiedad, licencias de conducir, DNIs, entre otros).

Un centro de inspección técnica vehicular deberá tener una entrada despejada y señalizada por donde será la salida y entrada de vehiculo, la figura 3 representa la revisión técnica C.I.T.V. ANTARQUI S.A.C., de la ciudad de Tacna, donde vehículos pasan su revisión para obtener un certificado de revisión técnica aprobatoria o desaprobatoria (véase figura 3).

Figura 3

Frontis de un centro de inspección técnica vehicular en la ciudad de Tacna

Nota. Fotografía tomada por Maximo Espinoza, Tacna, 2021.

2.2.10. Protocolos de red

Estos definen el formato y conjunto de reglas para intercambiar mensajes entre dispositivos de red. Cada protocolo tiene su propia función, formato y reglas de comunicación:

- **Protocolos de comunicaciones de red**

  Permiten la comunicación entre dos o más dispositivos. Las familias de tecnología Ethernet tienen una variedad de protocolos como IP (Internet Protocol), TCP (Protocolo de control de transmisión), HTTP (Protocolo de transferencia de hipertexto) entre otros.

- **Protocolos de seguridad de red**

  Protegen los datos para proporcionar autenticación, integridad de los datos y cifrado de datos. Entre ellos están el SSH (Secure Shell), SSL (Secure Sockets Layer) y TLS (Transport Layer Security).

- **Protocolos de routing (Enrutamiento)**

  Permiten a los routers intercambiar información de ruta, comparar y seleccionar la mejor ruta de destino. Entre ellos están OSPF (*Open Shortest Path First*) y BGP (*Border Gateway Protocol).*

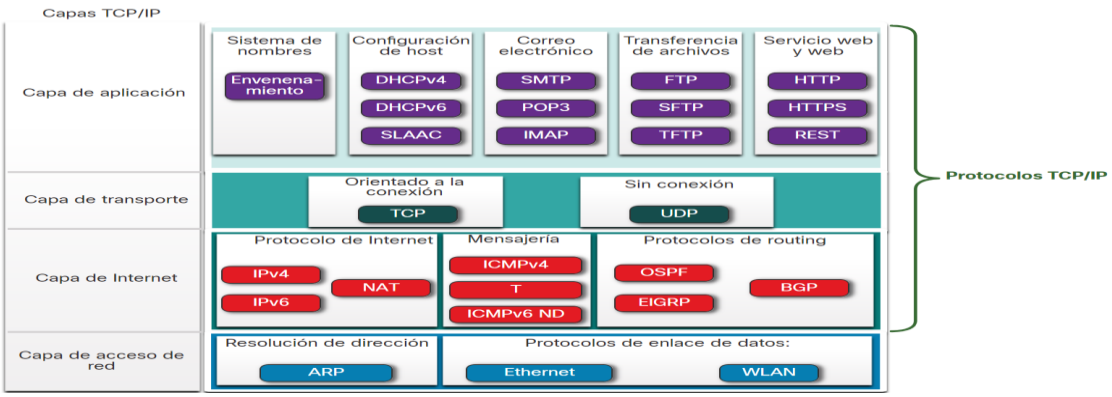
- **Protocolos de detección de servicios**

  Se utilizan para la detección automática de dispositivos o servicios. Entre ellos están DHCP (*Dynamic Host Configuration Protocol*) y DNS (*Domain Name Services*)

La suite de protocolos TCP/IP, representada por la figura 4, es un primordial conocimiento a saber ya que debería conocerse a detalle en que capa del modelo OSI estará el protocolo que buscamos proteger para la elaboración de las reglas de entrada y salida del Firewall. (Véase Figura 4).

Figura 4

Suites de protocolos TCP/IP y de comunicación.



Nota. Imagen obtenida por Cisco Academy – Introduction to networks, 2020, Cisco Netacad.

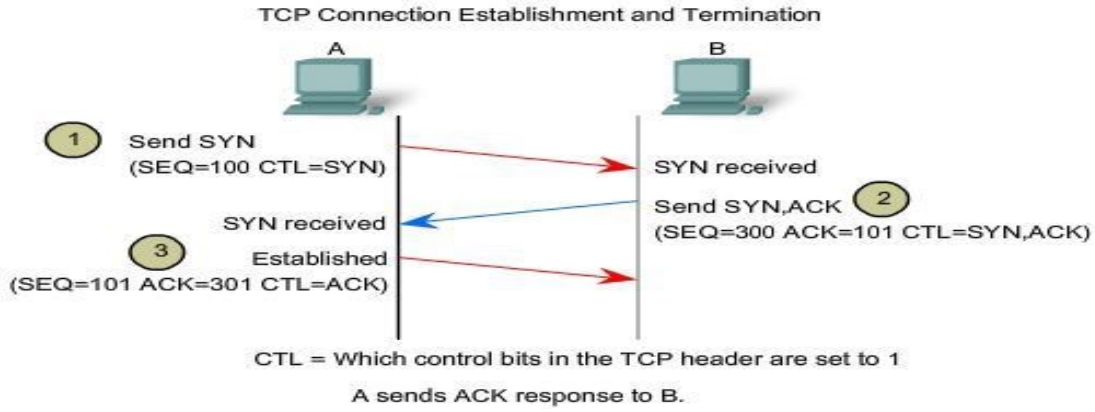
2.2.11. Protocolo SMB (Server Message Block)

Este es un protocolo cliente-servidor que controla el acceso a archivos y directorios enteros, como también a recursos de red como impresoras, interfaces entre otro. Se comunica a través de protocolo IP utilizando three-way handshake antes de establecer una conexión definitiva. Normalmente utiliza el puerto TCP 445.

El three-way handshake, representada por el diagrama de establecimiento y terminación TCP en la figura 5, permite reconocer cuando y que equipos establecen una conversación, pudiendo reconocer los protocolos que estos intercambiarán (véase figura 4).

Figura 5

El Three-Way Handshake



Nota. Representación gráfica obtenida por Cisco TCO-Establish and Terminate the connection, 2020, Cisco learning network.

Las versiones de SMB son representadas en la figura 6, donde se indica la versión del sistema operativo que soporta cada versión de SMB y las funciones adicionales que se agregaron al transcurrir los años (véase figura 6).

Figura 6

Versiones de SMB en el S.O. Windows.

Versión SMB	Soportada desde	Nuevas funciones
CIFS	Windows NT 4.0	Comunicación a través de la interfaz NetBIOS
SMB 1.0	Windows 2000	Conexión directa a través de TCP
SMB 2.0	Windows Vista, Windows Server 2008, Samba 3.5	Varias mejoras de rendimiento, firma de mensajes mejorada, función de caché para las propiedades de archivo
SMB 2.1	Windows 7, Windows Server 2008 R2	Mecanismos de bloqueo
SMB 3.0	Windows 8, Windows Server 2012,Samba 4.0	Conexiones multicanal, cifrado de extremo a extremo, acceso a almacenamiento remoto
SMB 3.0.2	Windows 8.1,Windows Server 2012 R2	
SMB 3.1.1	Windows 10, Windows Server 2016, Samba 4.3	Prueba de integridad, cifrado AES-128 con Galois/Counter Mode (GCM)

Nota. por Digital Guide Ionos - SMB (Server Message Block): definición, funciones y áreas de aplicación ,2020, Know How.

2.2.12. Ciberataques más frecuentes en el Perú

Revista de la página web Andina.pe, que explica los diferentes intentos de ciberataques más frecuentes del Perú hasta agosto del 2020 (Andina.pe, 2020).

- ***SSH.Connection.Brute.Force*** consta de varias solicitudes de inicio de sesión, lanzadas a una velocidad de aproximadamente 200 veces en 10 segundos.
- ***SMB.Login.Brute.Force*** genera al menos 500 inicios de sesión en un minuto, lo que indica un posible ataque de fuerza bruta en los sistemas operativos Microsoft Windows.
- ***W32/Bancos.CFR!tr*** está clasificado como un troyano. Sus actividades comúnmente incluyen establecer conexiones de acceso remoto, capturar la entrada del teclado, recopilar información del sistema, descargar / cargar archivos, colocar otro malware en el sistema infectado, realizar ataques de denegación de servicio (DoS) y ejecutar / finalizar procesos.
- ***W32/Tibs.PACKED!tr*** está clasificado como un troyano, un tipo de malware que realiza actividades sin el conocimiento del usuario. Por ejemplo, el establecimiento de conexiones de acceso remoto, capturar la entrada del teclado, recopilar información del sistema, descargar / cargar archivos, colocar otro malware en el sistema infectado, realizar ataques de denegación de servicio (DoS) y ejecutar / finalizar procesos.
- ***W32/Generic_PUA_MC.FXK*** se clasifica como un infector de archivos. Un infector de archivos es un tipo de malware que tiene la capacidad de propagarse al adjuntar su código a otros programas o archivos.

2.3. Definición de términos

2.3.1. Actor malicioso

Se llama así a las personas con conocimientos avanzados de computación que buscan obtener, vender, descubrir, entre otros, de una empresa o persona en específico. Estos pueden ser Hackers (Blancos, grises o negros), Ciber-criminales, hacktivistas, hackers apoyados por estados, entre otros (Cisco, 2020).

2.3.2. Activo (informático)

Información digital de valor sensible de la empresa que puede contener datos que no deben ser expuestos (Cisco, 2020).

2.3.3. Exploit (explotación)

Se llama así cuando el actor malicioso aprovecha una vulnerabilidad y la "explota" para obtener el fin deseado mediante un software, hardware e incluso vulnerabilidad humana (Cisco, 2020).

2.3.4. ISP - Proveedor de servicios de internet

Es la compañía que proporciona las conexiones y el soporte informático para poder acceder a internet (Cisco, 2020).

2.3.5. IDS – Sistema de detección de intrusos

Es utilizado para analizar la detección de intrusos en la red, basado en sensores virtuales que permiten el monitoreo constante de la red (Cisco, 2020).

2.3.6. IPS -Sistema de prevención de intrusos

Este permite establecer reglas donde compara firmas de los programas que se utilicen a nivel de capa 7, y así corroborar la autenticidad de los protocolos de red que pasen a través de él (FTP, SMTP, entre otros) para luego descartar paquetes considerados como amenazas o permitir el tráfico (Cisco, 2020).

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Diseño de la investigación

El diseño de la presente tesis se encuentra dentro de la línea de investigación de Telecomunicaciones, de la escuela profesiones de ingeniería electrónica.

El tipo de investigación de la presente tesis es aplicada, se busca aplicar los conocimientos adquiridos para brindar una solución tecnológica directa a los problemas presentes en los centros de inspecciones técnicas vehiculares.

El nivel de la presente tesis es aplicativo, donde la finalidad de la tesis es solucionar un problema tecnológico de mi población.

3.2. Acciones y actividades

El diseño del firewall con pfSense se realizó con un reconocimiento completo de la estructura de red informática, tanto en hardware como en software, de las empresas de revisiones técnicas donde se aplicará.

El ensamblaje de este Firewall se realizó utilizando componentes tecnológicos de la propia empresa de revisiones técnicas, donde se buscó optimizar los recursos a utilizar realizando trabajos de soldadura electrónica en partes necesarias.

Realizado el ensamblado, se instaló y configuro el sistema operativo dentro del equipo donde ira el software de pfSense, usando una virtualización de máquina para poder tener una mayor versatilidad al momento de modificar y hacer pruebas de reconocimiento como también las pruebas de seguridad.

3.3. Materiales y/o instrumentos

Se utilizó los siguientes recursos para la elaboración de la presente tesis:

- El instituto nacional de estadística del Perú (INEI), para poder visualizar las estadísticas del incremento sobre el uso de internet en hogares y empresas, más aun, en este periodo 2019-2021, donde se atraviesa la pandemia del Sars-Cov2 (covid-19).
- Biblioteca de la Universidad Privada de Tacna, obtención de referencias a tesis presentadas por egresados de la carrera de ingeniería electrónica.

- *Cisco,* gran fuente de información sobre todo respecto a conceptos, diseño de redes empresariales y tipos de ataques informáticos.
- *Cisco NetAcademy,* cursos especifico de ingeniería de las telecomunicaciones informáticas.
- *FORTINET,* empresa dedicada a la seguridad de red con amplia aplicación a nivel mundial, contiene un amplio glosario de los problemas de ciberseguridad que se actualiza todos los días.

3.4. Población y/o muestra de estudio

- *Universo*; son todas las instituciones y empresas de la ciudad de Tacna que funcionen bajo políticas informáticas para ejercer su comercio bajo las estrictas medidas de prevención dadas por el virus SARS-CoV-2
- *Población*; son las empresas privadas de Revisiones Técnicas que trabajan junto con el Ministerio de Transportes y Telecomunicaciones para la emisión de certificados de revisiones técnicas vehiculares de manera semestral o anual a vehículos automotores que brinden servicio público (transporte de personas o mercancías) o sean de uso particular.
- *Muestra*; la cantidad de veces que mi población haya sufrido un ataque informático y también clasificar por muestra el tipo de ataque que fueron y si fue exitoso, teniendo en cuenta los activos que fueron afectados.

3.5. Operacionalización de variables

3.5.1. Variable independiente:

- Firewall de software libre - pfSense

3.5.2. Variable dependiente:

- La seguridad informática de la red.
- La arquitectura informática de la red.

3.6. Procesamiento y análisis de datos

En el desarrollo de mi tesis, utilice una técnica de procesamiento propia para determinar en donde, como y cuando aplicar mi software de mitigación de vulnerabilidades.

Los pasos que determine utilizar son los siguientes:

- Determinar y delimitar el tema de tesis, revisar las referencias de proyectos de tesis que hayan utilizado parecida metodología, tema de estudio y marco teórico.
- Determinar el ambiente donde se aplicará este proyecto de tesis para saber qué tipo de información es la que debemos proteger; para la ejecución de este proyecto, se aplicara en un Centro de Inspección Técnica Vehicular de la ciudad de Tacna en el año 2021.
- Adecuar el hardware necesario para la correcta virtualización del software pfSense, donde se creará las reglas de acceso, administración de la red y filtros necesarios para el proyecto de tesis.
- Aplicar las acciones necesarias para reconocer las carencias electrónicas de tecnologías de la información que se presenten en el determinado objeto de estudio.
- Realización de pruebas y corrección de complicaciones que se presenten al momento de agregar un dispositivo a una red que puede o no ser escalable.
- Con los datos obtenidos posterior a la implementación del dispositivo de seguridad, realizar la comparación del antes y después para así poder corroborar la eficiencia del dispositivo en el ámbito del objeto de estudio.

CAPÍTULO IV: RESULTADOS

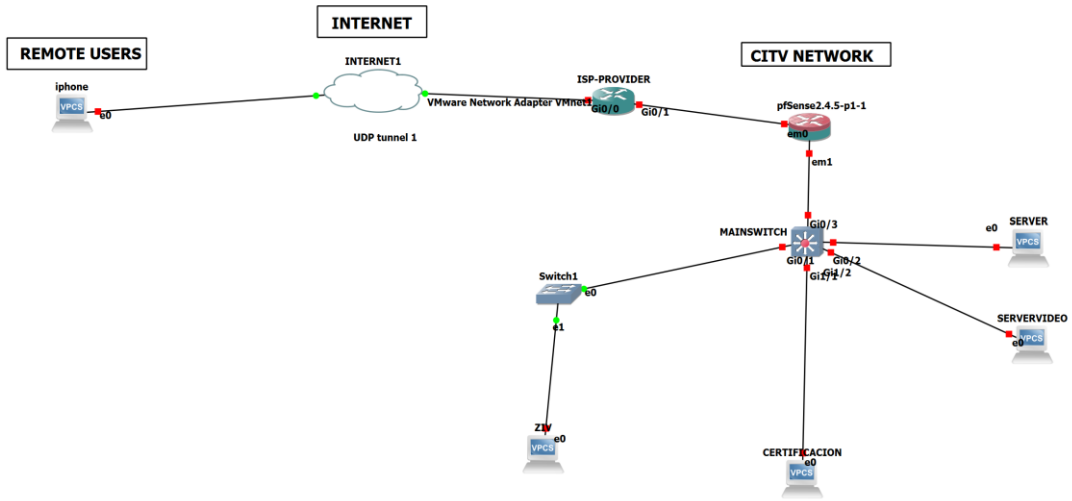
4.1. Diseño en ingeniería

La red de área local donde se aplicará este proyecto es de única segmentación, debido a que la cantidad de dispositivos no es excesiva. Se utilizará el firewall para hacer esta segmentación entre el ISP y la LAN de la empresa teniendo en cuenta el impacto en la red que este genere.

El diagrama lógico representa la implementación del firewall basado en pfsense dentro de una red de área local de una revisión técnica de la ciudad de Tacna, además, el uso de los usuarios remotos a través del internet que serían filtrados por el firewall (véase figura 7).

Figura 7

Diagrama lógico simplificado de la implementación del firewall pfSense en la LAN de una CITV



Nota. Diseño realizado por Maximo Espinoza –GNS3, 2022.

4.2. Diseño de red de las empresas de revisiones técnicas

Para el funcionamiento de una empresa de revisiones técnicas, es necesario realizar un correcto cableado estructurado, teniendo en principal consideración las estaciones de la zona de inspección vehicular, las cuales estarán conectadas a las máquinas

industriales para la realización de pruebas a los vehículos, quienes captarán los resultados de estas a través de protocolos RS232, ETHERNET, UART y USB.

Estas estaciones de trabajo deberán poder subir los resultados obtenidos por cada una de las maquinas hacia un servidor local, guardando la información por cada placa del vehiculo que paso inspección. Esta carga de datos se realizará a través del protocolo Ethernet y SMB estableciendo el Three-Way Handshake.

A groso modo, la maquinaria utilizada para una empresa de revisión técnica que opere con una línea de inspección tipo mixta o combinada es:

- Frenómetro de rodillos.
- Banco de prueba de suspensiones.
- Analizador de holguras.
- Alineador de ruedas.
- Analizador de gases.
- Analizador de opacidad.
- Sonómetro.
- Reflectómetro.
- Luxómetro con regloscopio.
- Medidor de profundidad de neumático (Profundímetro).
- Torre de inflado.
- Distanciómetro o guincha de medición
- Captador de RPM

Como representación de una zona de inspección técnica vehicular tipo mixta, en la figura 8, se muestra una parte de la zona de inspección técnica vehicular, con los técnicos mecánicos - eléctricos y automotrices utilizando un luxómetro con regloscopio para medir las luces del vehiculo, para que luego este pueda pasar a la prueba del Frenometro de rodillos (véase figura 8).

Figura 8

Zona de Inspección Técnica Vehicular - ZIV

Nota. Imagen tomada por Maximo Espinoza –JPCH INVERSIONES EIRL, 2022.

Las estaciones de trabajo (hardware) en la línea de inspección técnica vehicular deberán contar con lo siguiente, no de una marca en específico, pero si con las características técnicas necesarias para el funcionamiento:

- Ordenador tipo torre con tarjeta madre con puertos tipo PCI o PCIe.
- Monitor LCD.
- Lectora de tarjetas SD.
- Cámara fotográfica.
- Cámara filmadora.
- Cámara Web.
- Teclado y mouse.

Como representación de terminal de trabajo de la zona de inspección técnica vehicular, en la figura 9, se aprecia el monitor, analizador de gases, analizador de opacidad, captador de RPM, pistola de temperatura y ordenador (véase figura 9).

Figura 9

Estación de trabajo en la Zona de Inspección Técnica Vehicular - ZIV

Nota. Fotografía tomada por Maximo Espinoza –JPCH INVERSIONES EIRL, 2022.

Seguidamente, se encuentra el área administrativa, tesorería, certificación y corroboración de datos documentarios y el DATACENTER.

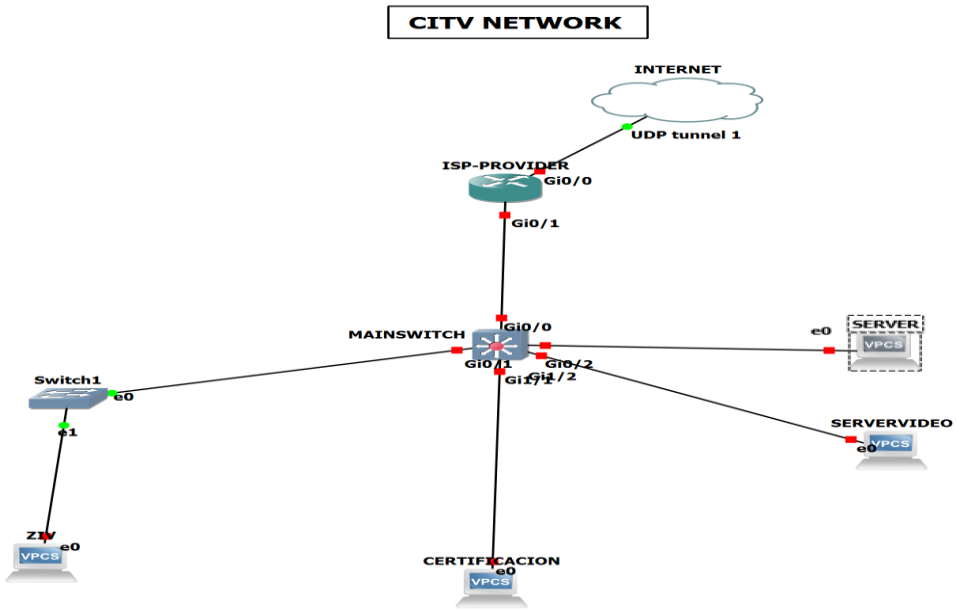
El cableado estructurado de la empresa se realizó de la siguiente manera:

- Cable UTP cat5e de la marca NEXXT.
- Switch L2 Administrable TEG-240WS de la marca Trendnet.
- Switch L2 no Administrable marca SATRA.
- Antena Ubiquiti modelo PB M5-400.
- Router Mikrotik provisto por el ISP.
- Router/modem TP-Link modelo TL0MR6400 respaldo para asegurar la conectividad continua a internet.
- Servidor de datos de las inspecciones técnicas.
- Servidor de video de cámaras de circuito cerrado

La estructura de red de la empresa de revisión técnicas donde implementare el uso de mi firewall es representada utilizando un software de simulación (GNS3), como en la figura 10 (véase figura 10).

Figura 10

Diagrama lógico resumido de la LAN



Nota. Diagrama elaborado por *Maximo Espinoza –GNS3*, 2022.

4.3. Parámetros de diseño para la implementación de un Firewall

Luego del reconocimiento de todos los dispositivos electrónicos y de red del centro de inspección técnica vehicular, se aprecia que la jerarquía de la LAN es un modelo de dos niveles, esto debido a que las capas de distribución y núcleo se encuentran en una sola y la estabilidad de la red no es extensa por la cantidad de usuarios conectados.

En el ámbito digital de la empresa, el activo que se debe proteger es el archivo digital de inspección técnica vehicular de todos aquellos vehículos que han pasado una revisión técnica.

La implementación de un Firewall siguiendo una topología tipo estrella extendida no tendrá un impacto significativo en el rendimiento de la red, por lo tanto, no se verá afectada la comunicación que existe con el Ministerio de Transportes y Comunicaciones para la sincronización de datos con el Centro de inspección Técnica Vehicular.

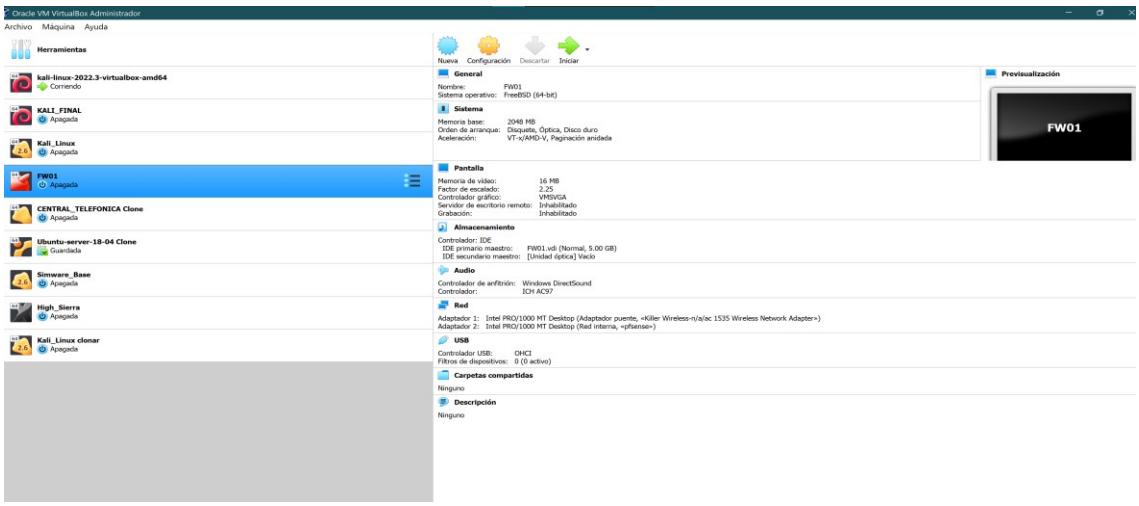
4.4. Software pfSense

La instalación del software de pfSense se realizó en una máquina virtual utilizando la aplicación de VirtualBox en un ordenador con el sistema operativo Windows 10 Pro de 64 bits.

Dando así una mejor versatilidad al momento de realizar las configuraciones y pruebas en este firewall, permitiendo la rápida administración del mismo como también realizar un respaldo de configuración rápido para así ser llevado a un nuevo hardware más potente si se requiere aumentar las políticas de seguridad. (Vease Figura 11)

Figura 11

Aplicación de VirtualBox con Máquina virtual de pfSense

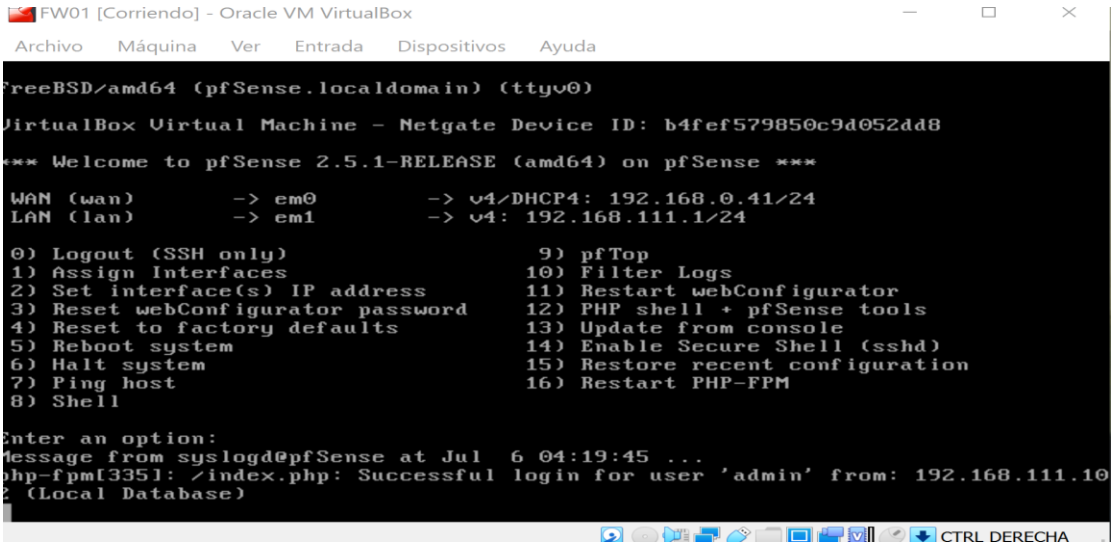


Nota. Captura de pantalla *por Maximo Espinoza – VirtualBox, 2022.*

Una vez realizada la configuración inicial e instalación del software de pfSense, se define las interfaces físicas que serán utilizadas para la red WAN y la red LAN.a través de la interfaz de código dentro del software de mitigación de vulnerabilidades de pfsense (véase figura 12).

Figura 12

Ventana principal de configuración de pfSense

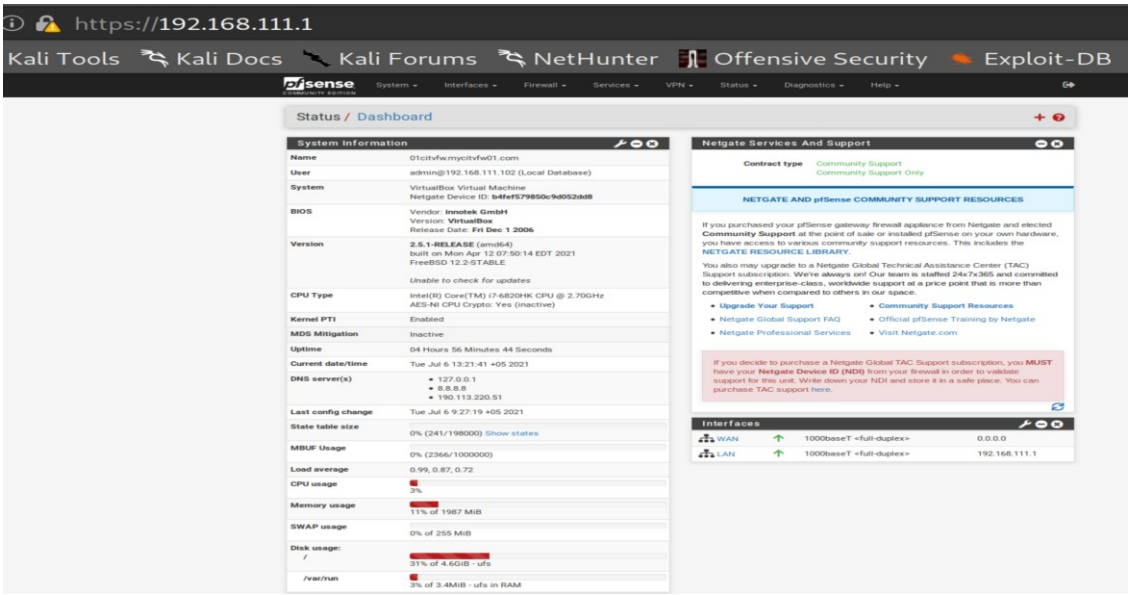


Nota. Captura de pantalla *por Maximo Espinoza – VirtualBox, 2022.*

Utilizando un ordenador dentro de la red LAN de pfSense (red interna), accedemos a la interfaz web del firewall para realizar las configuraciones correspondientes. Se utilizará las credenciales por defecto dentro del manual de instalación de pfSense® (véase figura 13).

Figura 13

Dashboard de pfSense



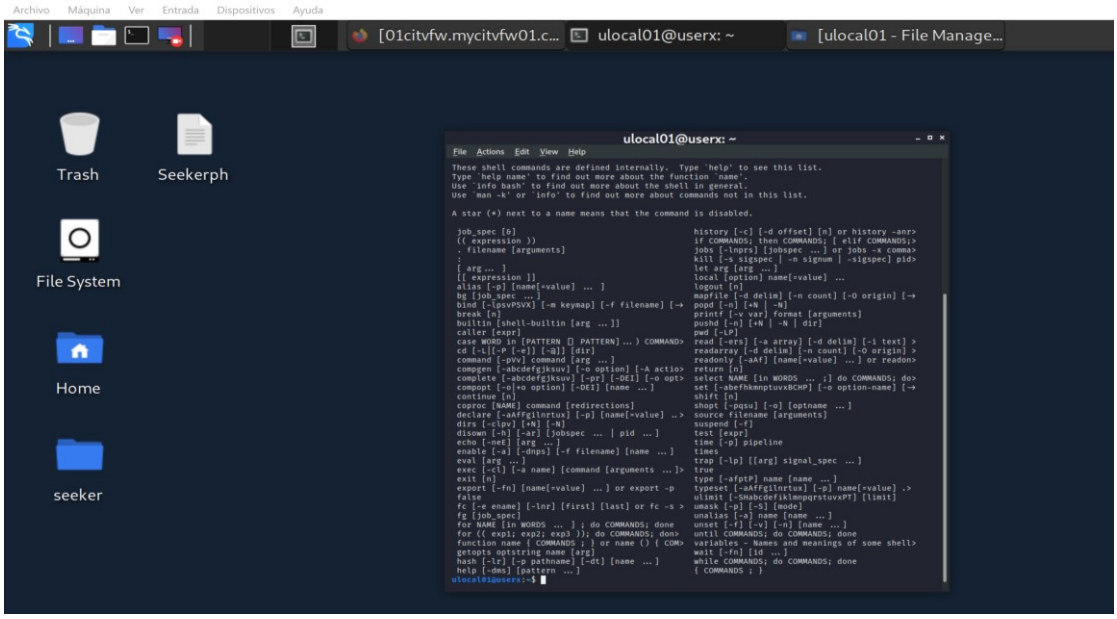
Nota. web Gui del firewall de *pfSense*, *por Maximo Espinoza – VirtualBox, 2022.*

4.5. Pruebas de penetración

Para realizar las pruebas correspondientes contra la eficacia del diseño y configuración del firewall con pfSense, se hace uso del sistema operativo Kali Linux (véase figura 14).

Figura 14

Ventana de inicio de Kali Linux

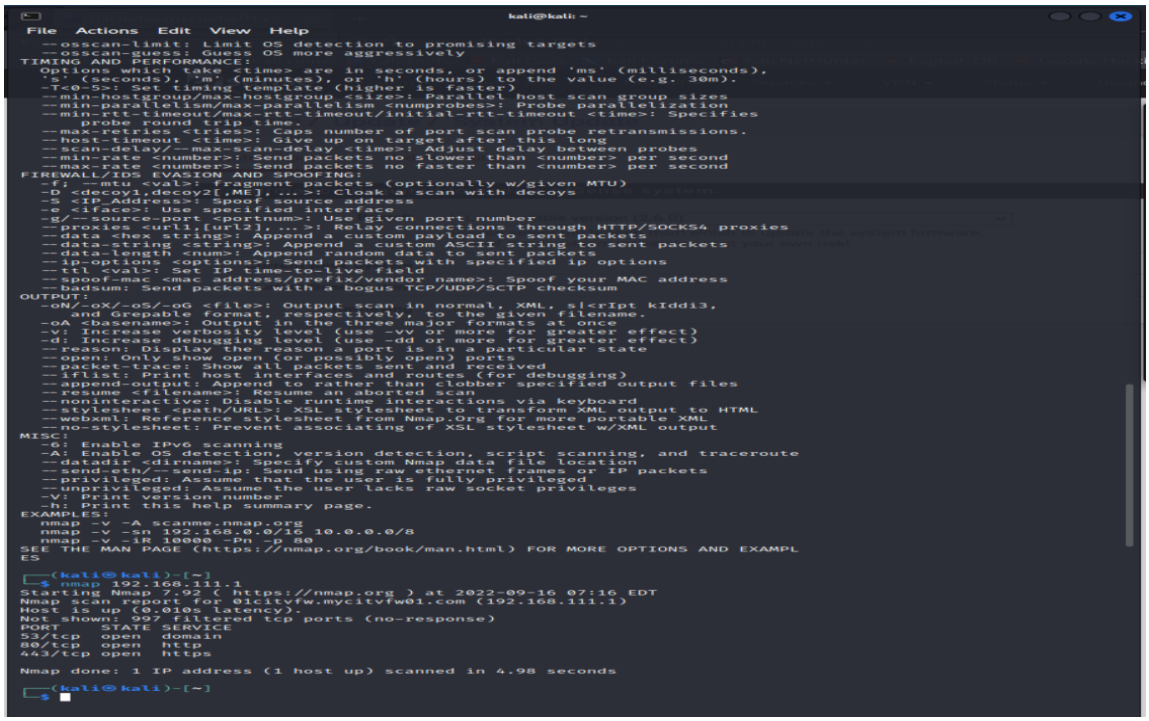


Nota. Captura de pantalla de Kali Linux, *por Maximo Espinoza – Kali Linux, 2022.*

De acuerdo a la prueba que haremos al Firewall de pfSense, colocaremos nuestro ordenador Kali Linux desde la red LAN (interna) o desde la red WAN (externa), haciendo uso de las herramientas de prueba de penetración de la misma basados en línea de código o a través de interfaz gráfica. Se utilizará el software de escaneos de puertos de nmap (Véase Figura 15) y el software de fuerza bruta de xhydra (Véase Figura 16)

Figura 15

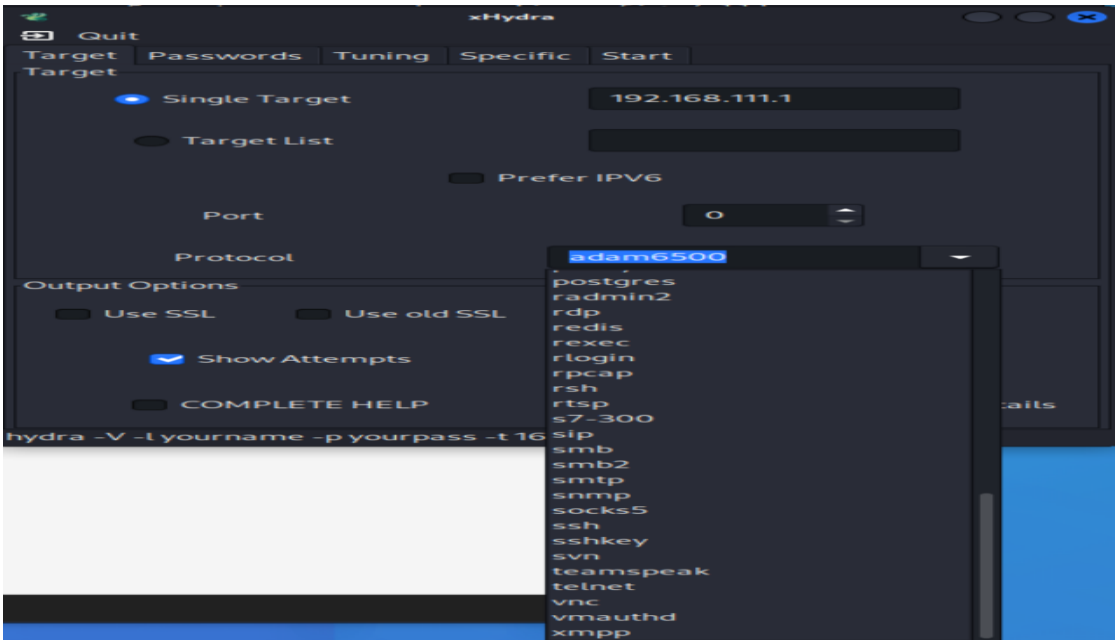
Ventana de aplicación nmap



Nota. nmap para buscar vulnerabilidades, *por Maximo Espinoza – Kali Linux, 2022.*

Figura 16

Ventana gráfica de aplicación xHydra



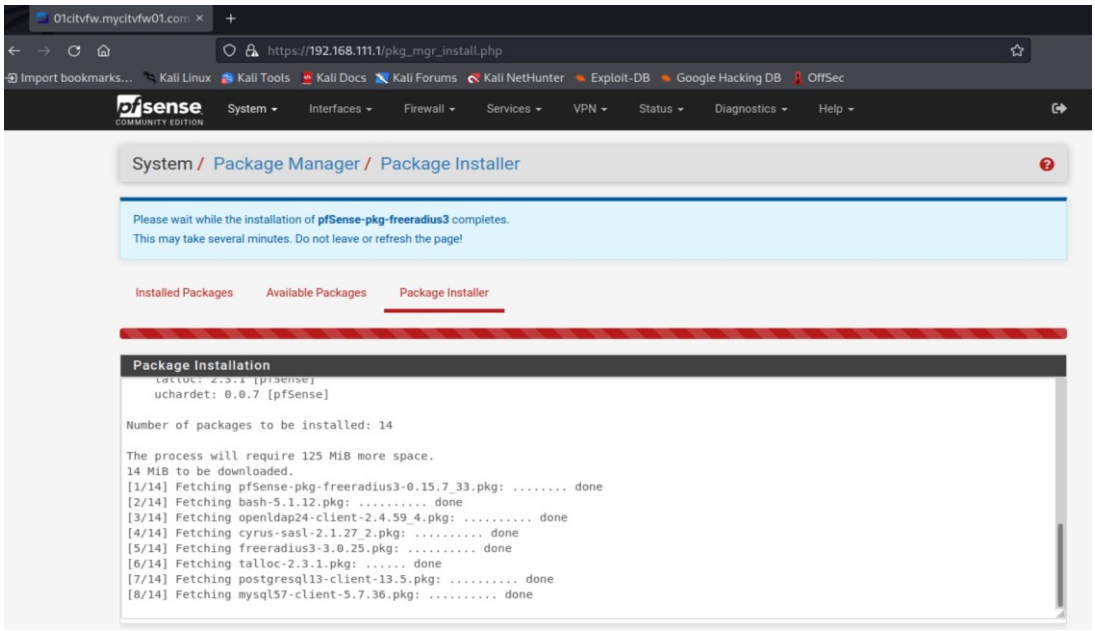
Nota. xHydra para prueba de seguridad de contraseñas a través de fuerza bruta, *por Maximo Espinoza – Kali Linux, 2022.*

Realizadas la prueba de penetración y descubrimiento de vulnerabilidades que existan en nuestro Firewall, procedemos con la instalación de paquetes basados en las necesidades encontradas por la empresa de revisiones técnicas. Estos paquetes pueden incluir mejoras adicionales a la funcionalidad de firewall que ya posee pfSense como la adición de un servidor de autenticación, autorización y contabilidad como RADIUS usando freeRadius, también tunelización VPN utilizando IPSec u Open VPN (véase figura 17).

Cabe resaltar que, al instalar mayor cantidad de paquetes y brindar más funcionalidades al Firewall de pfSense, se verá afectada la memoria RAM de la misma, el uso del microprocesador asignado y el espacio de almacenamiento del firewall.

Figura 17

Web GUI de instalación de paquetes en pfSense



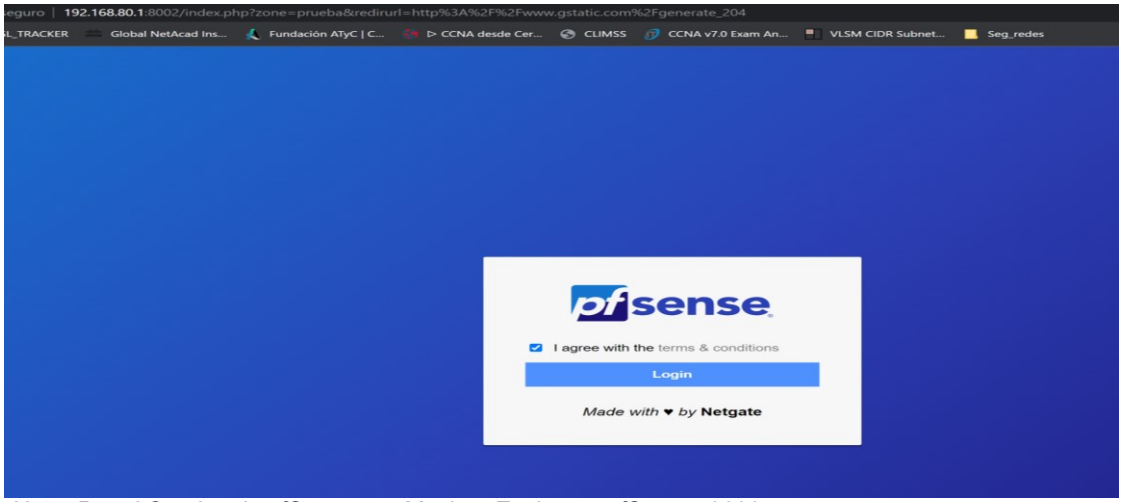
Nota. freeRadius dentro del firewall de pfSense, *por Maximo Espinoza – Kali Linux, 2022.*

Configuración de seguridad de acceso a la red mediante terminal utilizando un portal cautivo dentro del mismo Firewall pfSense (véase figuras 18 y 20).

Este servicio de portal cautivo brinda un mejor monitoreo por terminal (Dir. IP) del tráfico de datos que se da de subida y de bajada, además de brindar un login personalizable con términos y condiciones por cada autenticación de usuario.

Figura 18

Web GUI de acceso a navegación por internet usando portal cautivo.

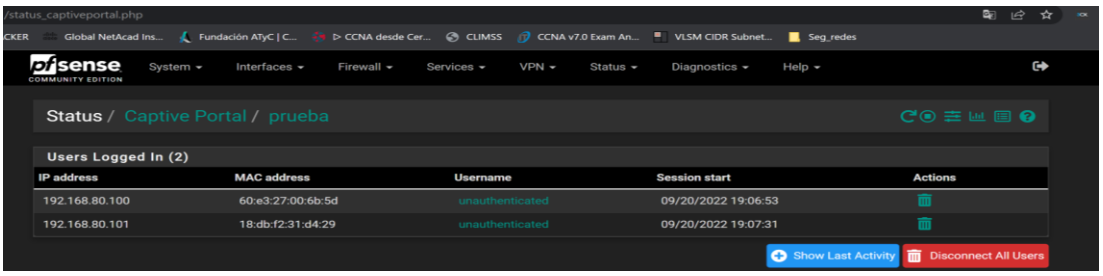


Nota. Portal Cautivo de pfSense por Maximo Espinoza, pfSense, 2022.

Además, provee una autenticación con un servidor de usuarios dentro del Firewall o también a través de un servidor de AAA como Radius. Esto mostrara sus direcciones IP y MAC a través de la página de Status (véase figuras 19 y 20).

Figura 19

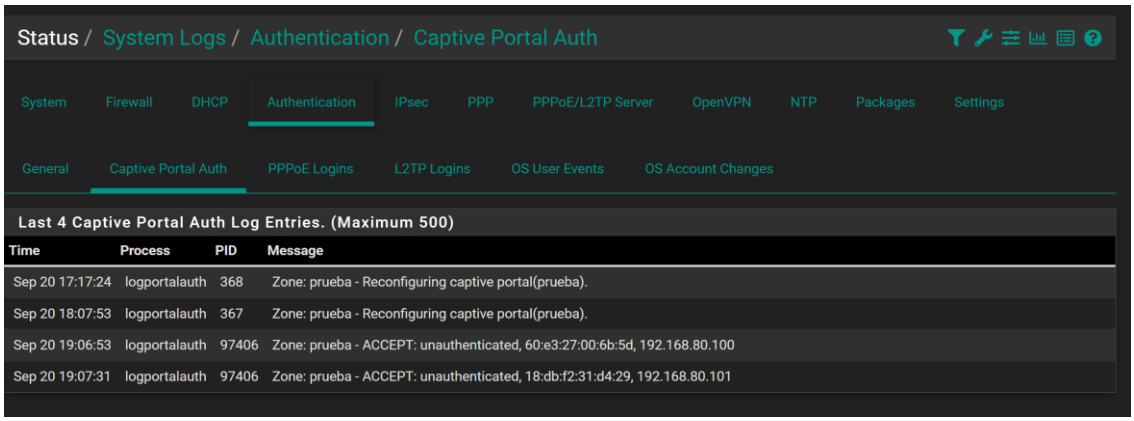
Terminales con sesión iniciada usando portal cautivo.



Nota. Captive Portal por Maximo Espinoza, pfSense, 2022.

Figura 20

Log de autenticaciones



Nota. Entradas Log del portal cautivo, detalladas por PID (process identifier), *por Maximo Espinoza – pfSense, 2022.*

Figura 21

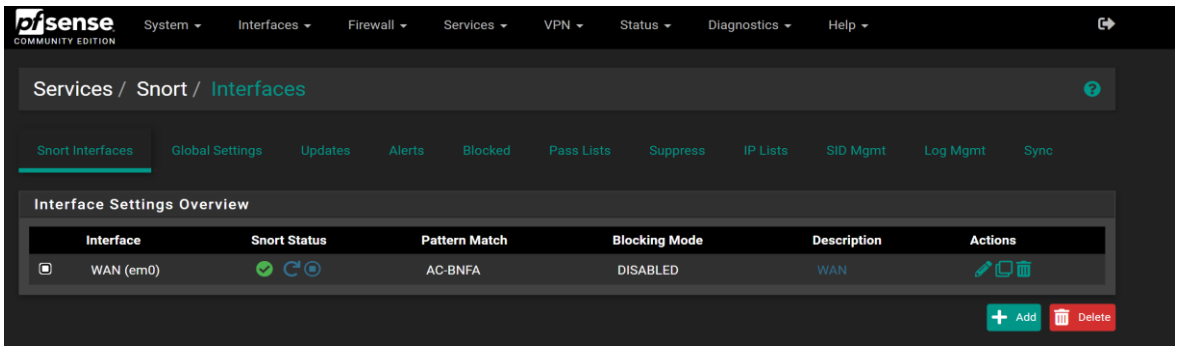
Acceso a página web de una Revisión Técnica

Nota. Navegación por aplicativo web luego de autenticación mediante portal cautivo y/o Radius Server, *por Maximo Espinoza – Google Chrome, 2022.*

Configuración del servicio SNORT, que asigna la funcionabilidad de IDS e IPS al Firewall de pfSense, basándose en comparaciones de firmas y reglas utilizando la base de datos del Snort.org y también de Solarwinds.com (véase figuras 22 y 23).

Figura 22

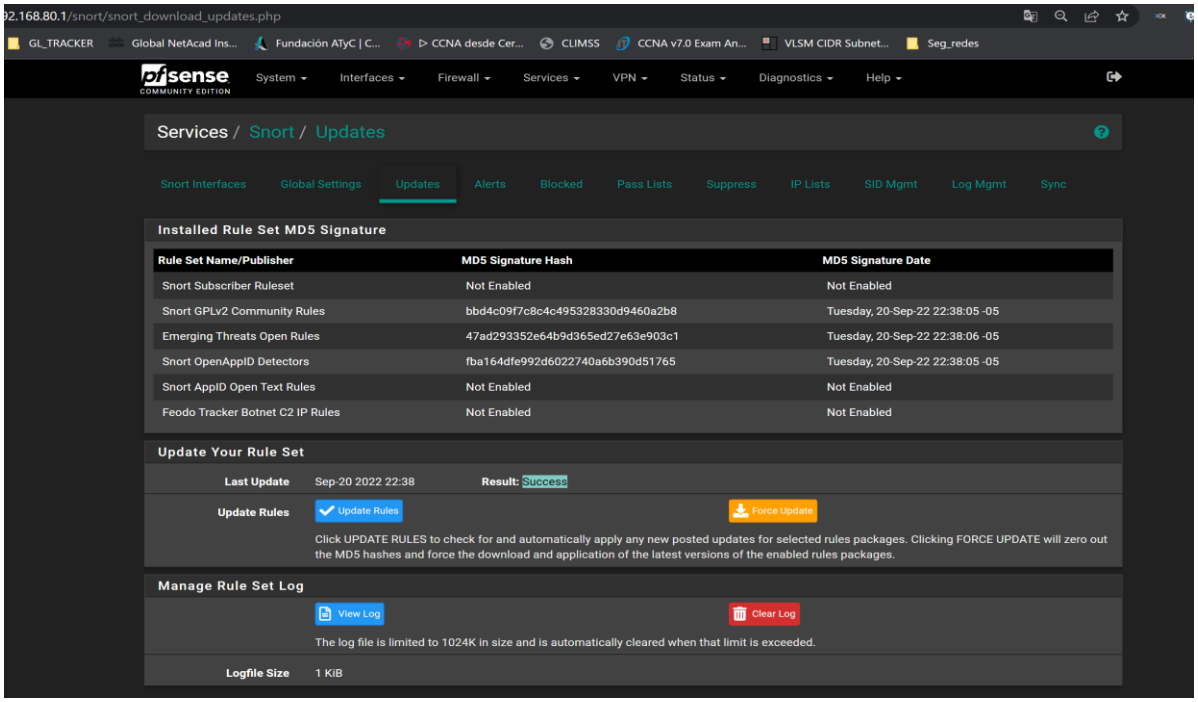
Servicio de Snort



Nota. Selección de interfaz para asignar donde SNORT realizara el monitoreo y la función de IPS y/o IDS, *por Maximo Espinoza – pfSense, 2022.*

Figura 23

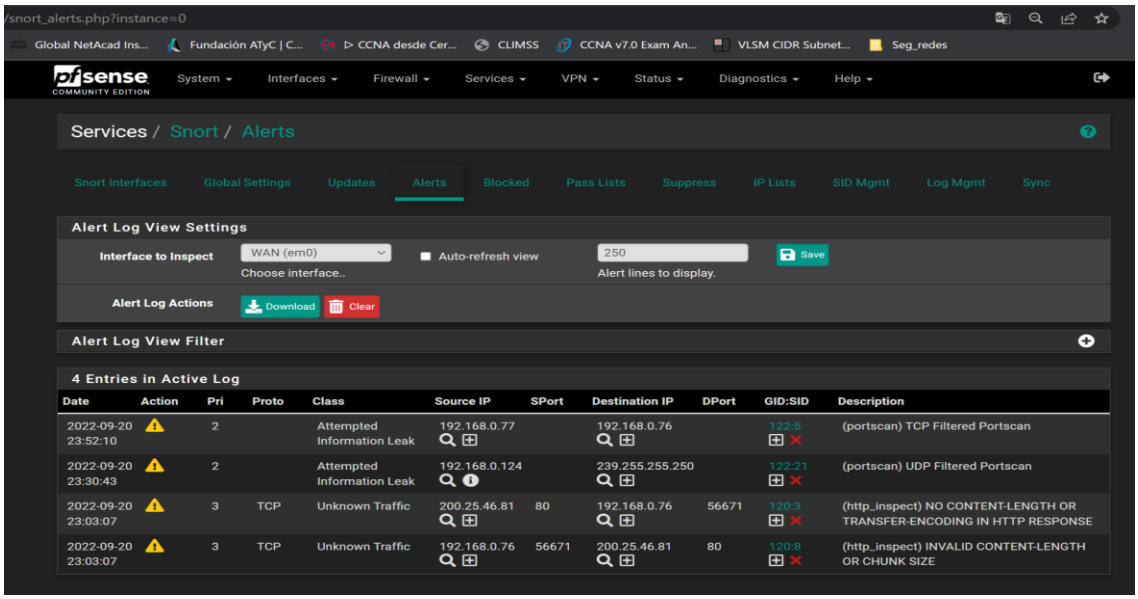
Actualización de suscripción y registro de firmas y reglas de SNORT



Nota. Actualización (automática luego) de firmas y paquetes de reglas de acuerdo a la suscripción elegida por el administrador, *por Maximo Espinoza – pfSense, 2022.*

Figura 24

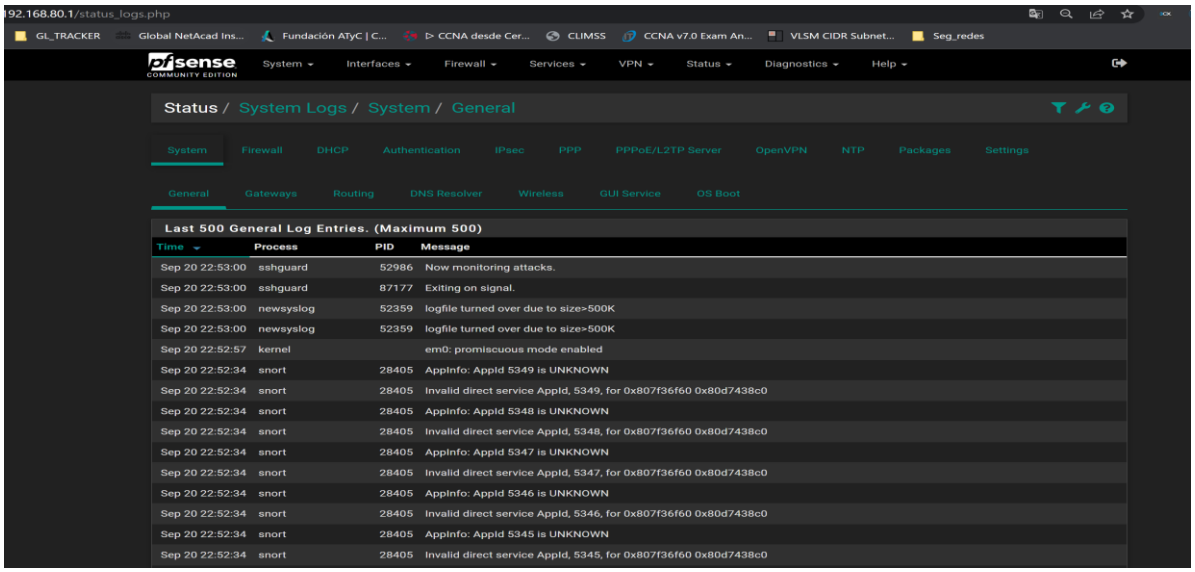
Alertas de Ataques de Snort



Nota. Alertas de ataques generadas por SNORT a través de la interfaz WAN (desde internet hacia la red privada), *por Maximo Espinoza – pfSense, 2022.*

Figura 25

Log general del sistema pfSense

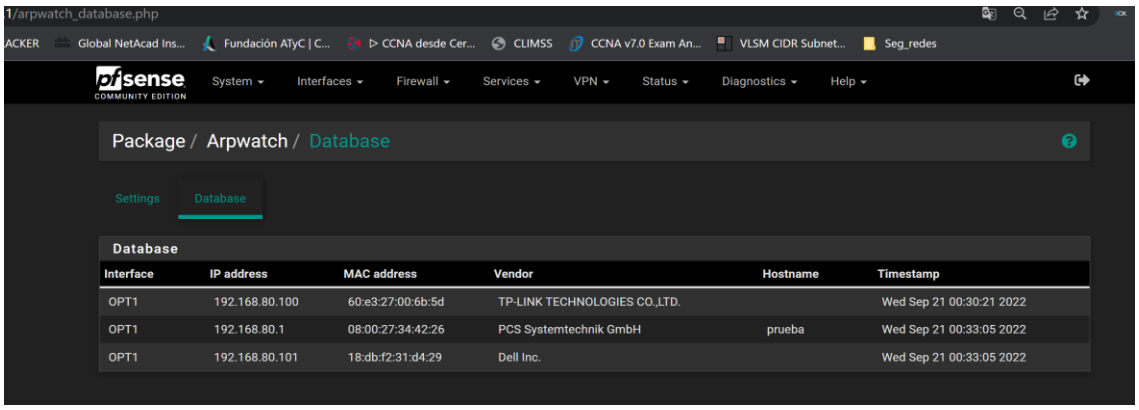


Nota. Log o reporte general del sistema de Firewall de pfSense, identificados por PID (identificación de procesos) *por Maximo Espinoza – pfSense, 2022.*

Por último, configuración de ArpWatch, que permitirá descubrir que dispositivos agregan a la base de datos de pfSense mediante la capa de enlace de datos, también se podrá limitar la cantidad de paquetes que se envíe a través de cada uno de estos clientes para evitar ataques internos (véase figura 26).

Figura 26

Base de datos Arpwatch



Nota. Base de datos de equipos registrados por arpwatch por Maximo Espinoza – pfSense, 2022.

CONCLUSIONES

Mediante el diseño y la implementación de un Firewall utilizando el software de sistema operativo libre de pfSense en las empresas de revisiones técnicas, que incluye el diseño de red, escalabilidad e impacto en el rendimiento, permitió una sustancial mejora en la seguridad informática de la misma, integrando seguridad en la capa de aplicación, transporte, red y enlace de datos como también el monitoreo constante del tráfico de datos, permitiendo así una mejor auditoria de la información que entra y sale de la empresa.

Se logró mitigar las vulnerabilidades a las cuales estuvo expuesta la empresa de revisión técnica, además de permitir una rápida respuesta de mitigación frente a una amenaza presentada desde la empresa como también de manera externa.

A través de técnicas de seguridad informática, se logró reforzar y asegurar la base de datos que poseen las empresas de revisión técnica, creando redundancia y también acceso seguro de manera externa e interna de la empresa.

RECOMENDACIONES

De acuerdo con el desarrollo que la empresa tenga en el ámbito económico, es posible implementar a futuro dispositivos adicionales contra la mitigación de vulnerabilidades como un sistema de detección de intrusiones (IDS) como también un sistema de prevención de intrusiones (IPS); estos dispositivos adicionales al firewall implementado crearían una red casi impenetrable ante cualquier ataque cibernético.

Brindar capacitaciones a todo el personal del centro de inspección técnica vehicular sobre las políticas de seguridad informática de la empresa, para así evitar una amenaza interna inadvertida.

Realizar una auditoría cada quincenal o mensual sobre el estado del firewall, a modo de evitar que este se encuentre desactualizado frente a nuevas amenazas que puedan surgir con el pasar del tiempo.

REFERENCIAS BIBLIOGRÁFICAS

Alfaro Rodríguez, C. H. (2012, s.f.). Metodología de investigación científica aplicado a la ingeniería.

https://unac.edu.pe/documentos/organizacion/vri/cdcitra/Informes_Finales_Investigacion/IF_ABRIL_2012/IF_ALFARO%20RODRIGUEZ_FIEE.pdf

FORTINET, (2021). Estadísticas de ataques cibernéticos reportados en Latinoamérica, especialmente PERU por Fortinet. https://www.fortinetthreatinsiderlat.com/en/Q32020/PE/html/trends#trends_position

pfSense (2021.) Página Web principal de pfSense

https://www.pfsense.org/

Cisco (2021) Pagina de Soporte de tecnología de Cisco.

https://www.cisco.com/c/es_mx/tech/index.html

Redacción Gestión, (2020, agosto 17) Los cinco ciberataques más frecuentes en el Perú.

https://gestion.pe/tecnologia/los-cinco-ciberataques-mas-frecuentes-en-el-peru-hackers-noticia/

Observatorio Nacional de Política Criminal - INDAGA (2020, diciembre) Diagnostico Situacional Multisectorial sobre la ciberdelincuencia en el Perú.

https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA.pdf

Ruiz Viera, K.E., Delgado Ramos, W. (2018) Implementación de una solución de seguridad perimetral Open Source en La Red telemática de la Universidad Nacional Pedro Ruiz Gallo [Tesis para titulación – Universidad de Lambayeque]

https://repositorio.udl.edu.pe/handle/UDL/122

Lancho Gonzales, A. (2017). Sistema Cortafuegos de Alta Disponibilidad con PfSense [Proyecto de fin de grado, Universidad Politécnica de Madrid].

http://oa.upm.es/49677/1/TFG_ALVARO_LANCHO_GONZALEZ.pdf

Da Silva De Oliveira, R. G. (2016) Efecto de la implementación del sistema pfSense en la seguridad perimetral lógica en los servicios de la red troncal de la universidad Nacional de la amazonia peruana, Iquitos [Tesis de titulación – Universidad Nacional de la Amazonia Peruana]

http://repositorio.ups.edu.pe/handle/UPS/10

FORTINET (2022), mapa de amenazas en tiempo real brindada por fortiguard

https://threatmap.fortiguard.com/

FORTINET (2022), glosario de ciberseguridad brindada por Fortinet sobre los últimos tipos de ataques cibernéticos.

https://www.fortinet.com/lat/resources/cyberglossary

Manual de inspecciones técnicas del Perú R.D. N. 11581-2008-MTC-15, 2008,

https://www.sutran.gob.pe/wp-content/uploads/2020/06/Manual-de-inspecciones-t%C3%A9cnicas-vehiculares-tabla-de-interpretaci%C3%B3n-de-defecto-de-inspecciones-t%C3%A9cnicas-vehiculares.pdf

Analuisa Zapata, R. A. (2012), Estudio de las técnicas de control de acceso a internet y su aplicación en la red de datos del colegio Corina Parral de la ciudad de Chimbo [Tesis para titulación – Escuela superior politécnica de Chimborazo]

Portal web de La División de Investigación de Delitos de alta Tecnología de la Policía nacional del Perú – PNP, 2022,

https://www.policia.gob.pe/

Luis Gorgona S. Teoría de Redes de computadoras.

https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf

Tori Sitcawich (2020) – Vulnerability Remediation vs Mitigation: What´s the difference?

https://www.rapid7.com/blog/post/2020/09/14/vulnerability-remediation-vs-mitigation-whats-the-difference/

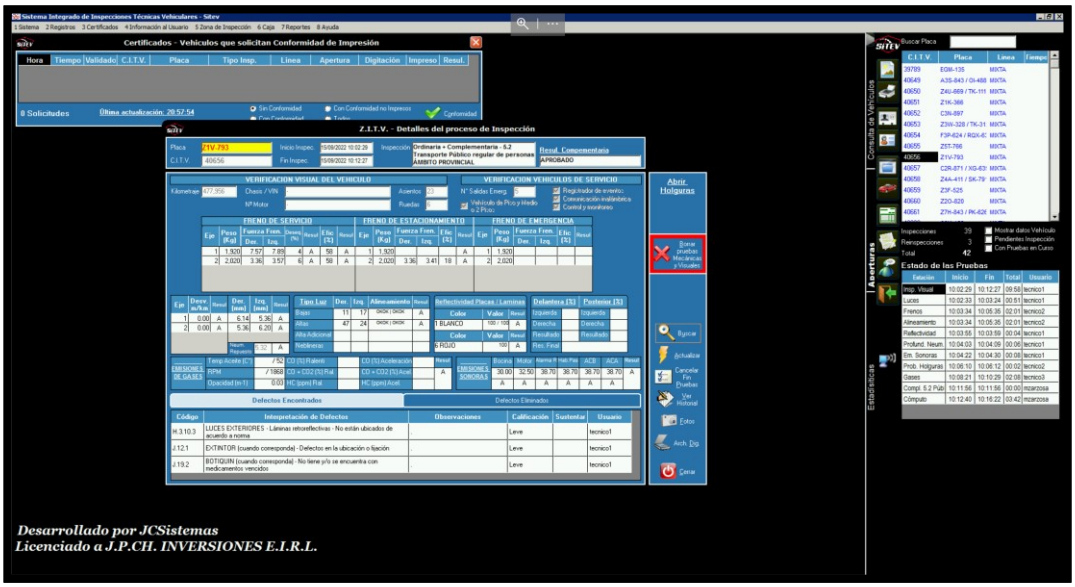
ANEXOS

Anexo 1. Tabla de ciberdelitos obtenida de la DIVINDAT – PNP

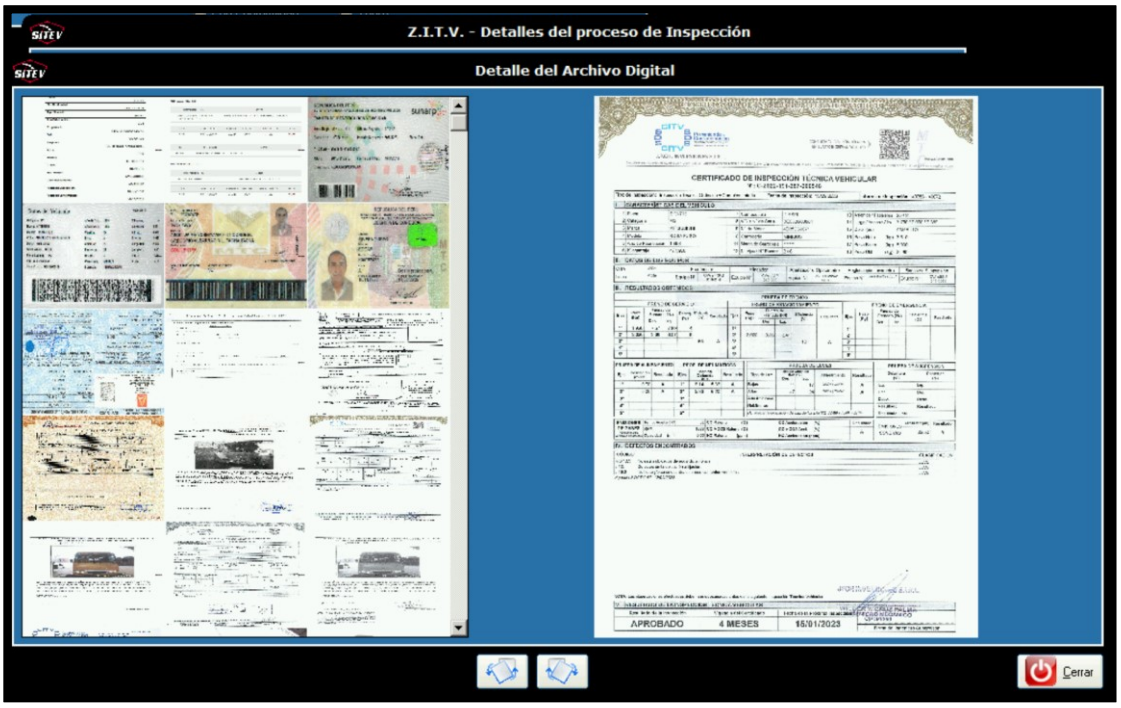
Tipo de ciberdelito	Actoresidentificados	
	Perfiles del ciberdelincuente	Perfiles de las víctimas
Abuso de mecanismos y dispositivos informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Personas jurídicas.
Contra datos y sistemas informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Contra la fe pública	▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Empresas.
Contra la indemnidad y libertad sexual	▪ Profesionales de la educación. ▪ Personas con diagnóstico clínico de malestar psicológico. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Niños, niñas y adolescentes vulnerables.
Contra el patrimonio y fraude informático	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Otros cometidos mediante el uso de TIC	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.

Fuente: DIVINDAT – DIRINCRI PNP / Elaboración: DIVINDAT – DIRINCRI PNP

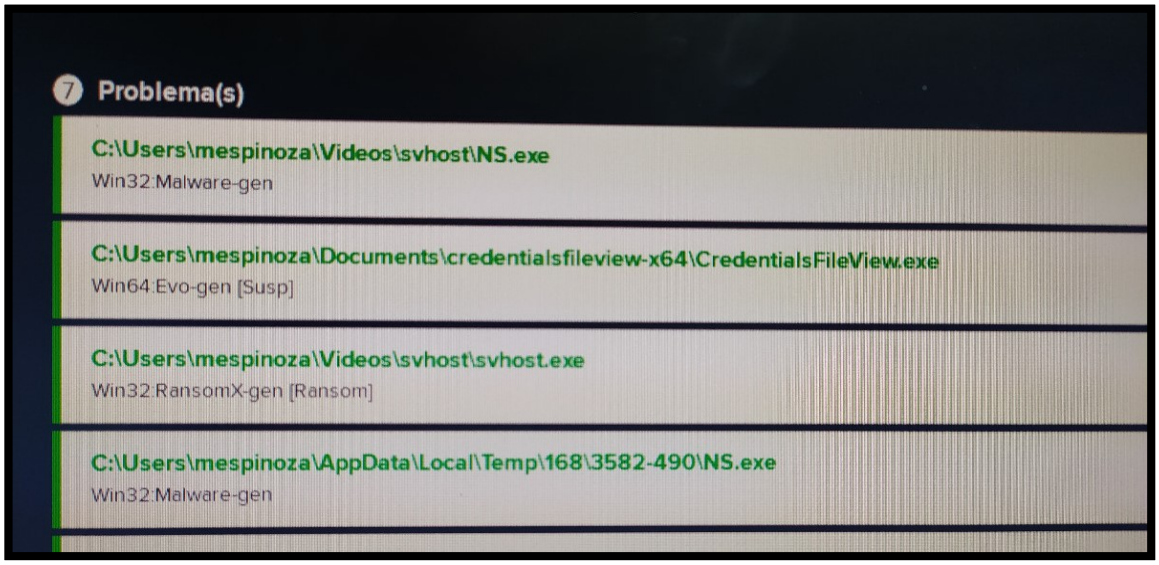
Anexo 2. Cuadro de resultados obtenidos del programa de revisiones técnicas sitev



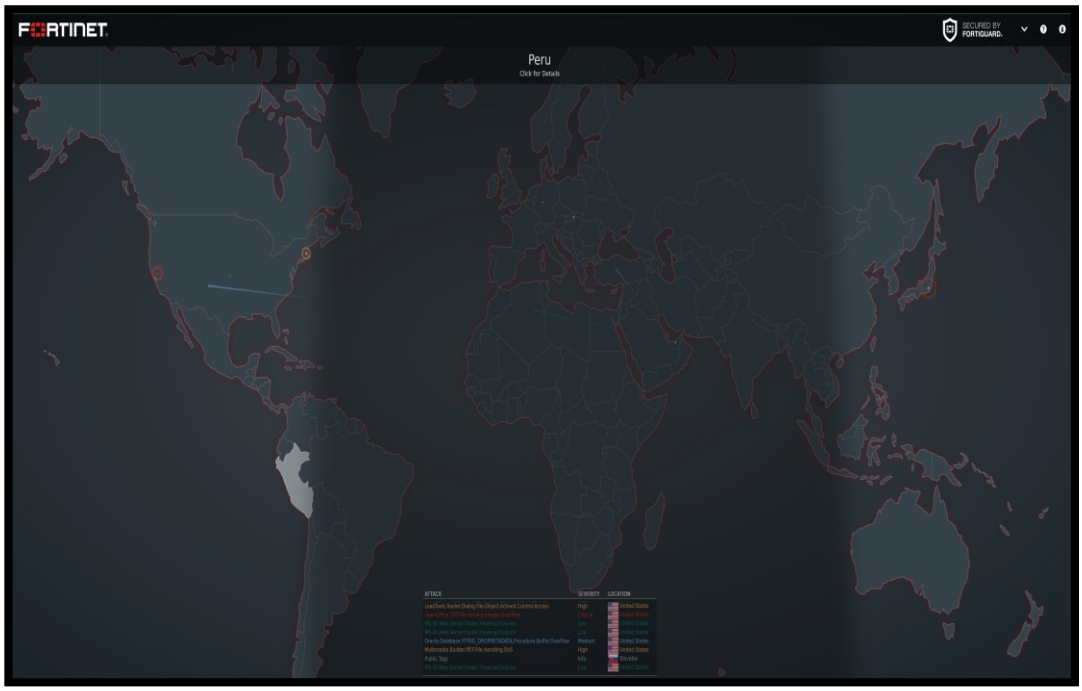
Anexo 3. Representación de archivo digital de un vehiculo



Anexo 4. Ataques informáticos mitigados por pfSense

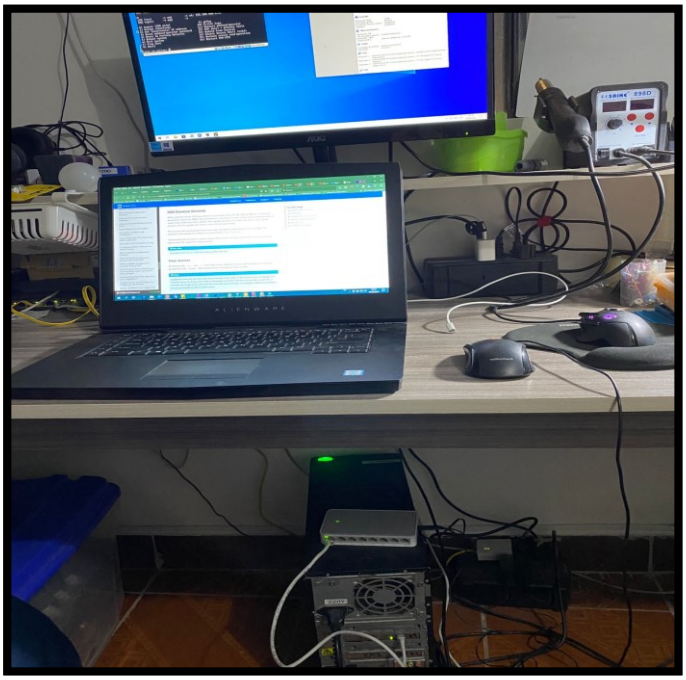


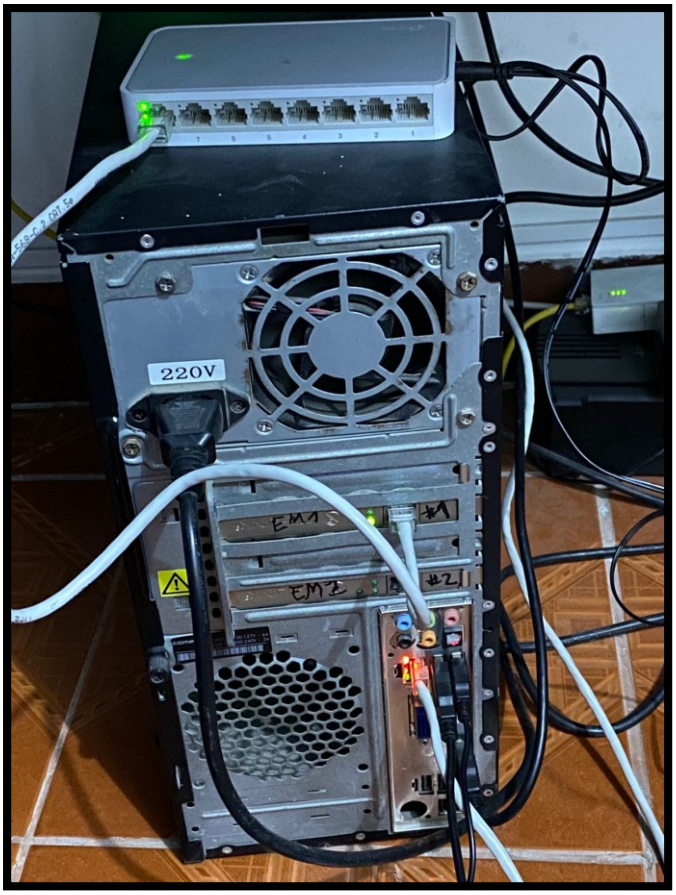
Anexo 5. Mapa de ataques en tiempo real de Fortinet



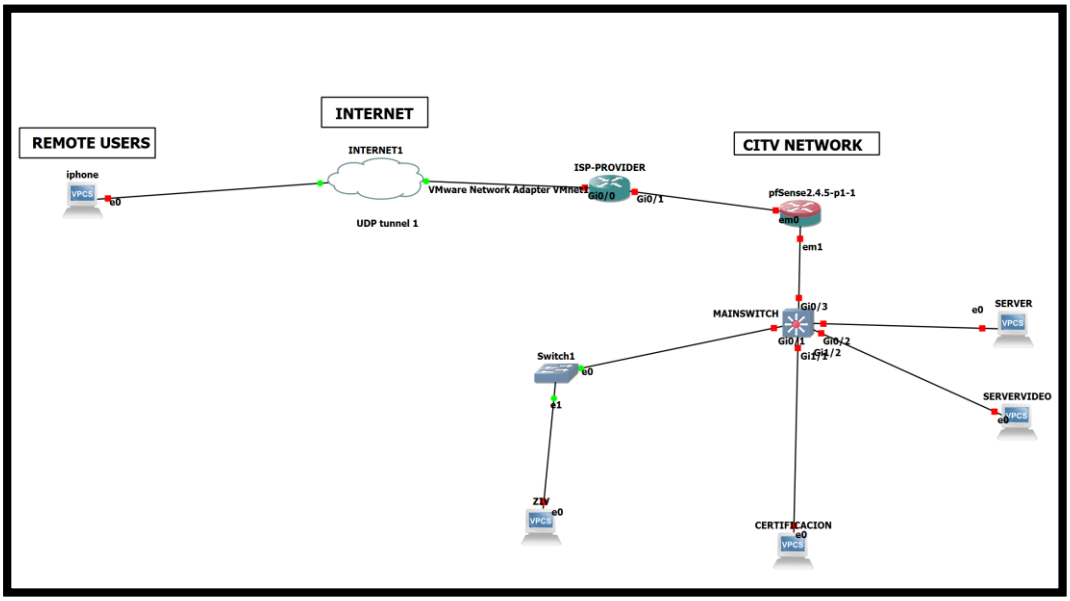
Anexo 6. Servidor de datos de revisiones técnicas

Anexo 7. Hardware utilizado para pfSense

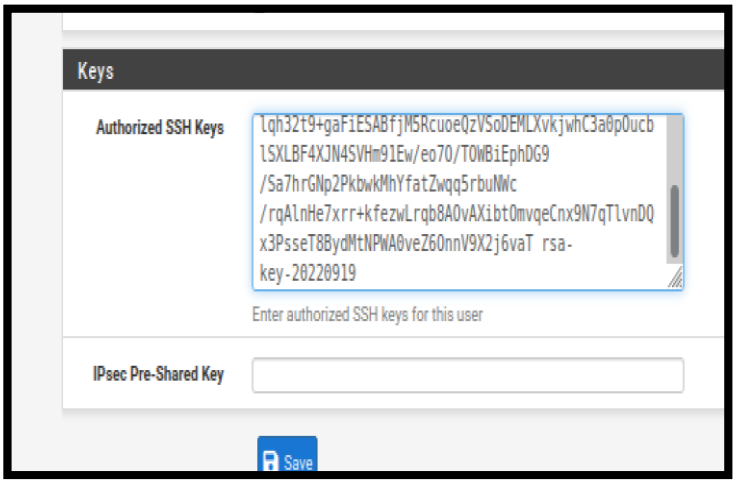


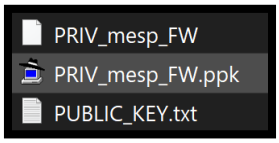


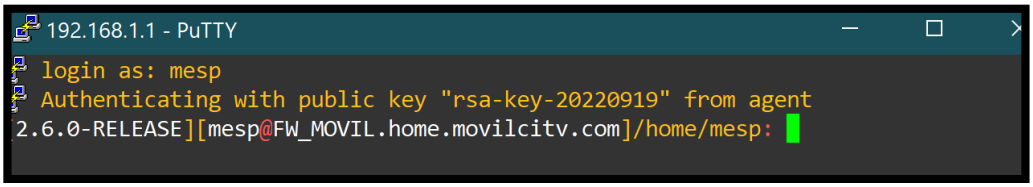
Anexo 8. Diagrama lógico final



Anexo 9. Autenticación SHH con llave pública y privada







Anexo 10. Matriz de consistencia

Hipótesis	Objetivos	Campo de Aplicación	Variables	Indicadores	Métodos
Se desarrollará e implementará un Firewall que mitigará las vulnerabilidades que se presenten en una empresa de revisiones técnicas de Tacna.	Desarrollar e implementar un firewall basado en el sistema operativo de software libre pfSense, que mitigue la vulnerabilidad informática de las empresas de revisiones técnicas en la ciudad de Tacna, año 2021.	Empresas que trabajen con activos de información sensible y de constante autenticación que necesiten una mejora de seguridad informática.	Firewall de software Libre	-Vulnerabilidades. -Activos.	El método de la investigación es aplicado .
La identificación a tiempo de las amenazas informáticas mitigara las vulnerabilidades que puedan existir frente a estas en la empresa de revisiones técnicas.	Identificar las diferentes amenazas informáticas que afecten la operatividad de las empresas de revisiones técnicas en Tacna.	Servidores, bases de datos y sesiones de usuarios.	Software de reconocimiento	-Amenazas	
La implementación de políticas de seguridad informática permitirá reducir el riesgo de presentarse vulnerabilidades en la empresa de revisiones técnicas.	Implementar políticas de seguridad informática que reduzcan su vulnerabilidad.	Empleados Administradores	Políticas de seguridad informática	-Políticas de seguridad	
La instalación y configuración del Firewall con pfSense, permitirá a la detección de amenazas informáticas.	Instalar y configurar el firewall con pfSense, que permita detectar las amenazas informáticas.	Firewall	Detección de amenazas	-Firewall con pfSense	