ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

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

EDISON FERNANDO RUIZ ANDINO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA.

RIOBAMBA – ECUADOR

Junio 2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** titulado 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, de responsabilidad del señor Edison Fernando Ruiz Andino, ha sido minuciosamente revisado y se autoriza su presentación.

Ing. Luis Eduardo Hidalgo Almeida; Ph, D.
PRESIDENTE

Firmado electrónicamente por:
LUIS EDUARDO HIDALGO ALMEIDA

Ing. Jacqueline Elizabeth Ponce Pinos; Mag.
DIRECTORA

Firmado electrónicamente por:
JACQUELINE ELIZABETH PONCE PINOS

Ing. Jairo Rene Jácome Tinoco; Mag.
MIEMBRO

Firmado electrónicamente por:
JAIRO RENE JACOME

Ing. Paulina Sofía Valle Oñate; Mag.
MIEMBRO

Firmado electrónicamente por:
PAULINA SOFIA VALLE

Riobamba, agosto 2022

DERECHOS INTELECTUALES

Yo, Edison Fernando Ruiz Andino, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
EDISON
FERNANDO RUIZ
ANDINO

EDISON FERNANDO RUIZ ANDINO

No. Cédula:060361002-3

DECLARACIÓN DE AUTENTICIDAD

Yo, Edison Fernando Ruiz Andino, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Firmado electrónicamente por:
EDISON FERNANDO RUIZ ANDINO

Edison Fernando Ruiz Andino

No. Cédula: 060361002-3

DEDICATORIA

Para todas las personas que creyeron en mí y con confiaron plenamente en que llagaría a feliz término con este reto de superación intelectual, a todos ustedes les expreso mi infinito amor por haber estado presentes en momentos difíciles.

Edison Ruiz

AGRADECIMIENTO

A todos los amigos que no tuvieron el reparo de ayudar y aportaron con sus conocimientos para completar este trabajo de titulación.

Edison Ruiz

TABLA DE CONTENIDO

Páginas

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue evaluar las condiciones de seguridad que tienen las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba dentro de su red LAN, mediante encuestas aplicadas a sesenta y cuatro de ellas, las cuales, en su gran mayoría no cuentan con elementos de seguridad, se encuentran conectadas al servidor ISP o proveedor de internet de manera directa, esto probablemente se debe al elevado costo en licenciamiento del Firewall. Se valoró el funcionamiento del Firewall PfSense de software libre, al cual se le aplicó diferentes pruebas utilizando Kali Linux 2021.2 y sus herramientas como nmap junto con NESSUS, web EICAR para identificar el nivel de seguridad que tiene el Firewall. Las pruebas fueron ejecutadas al Antivirus, Sistema de detección de intrusos (IDS), Sistema de prevención de intrusos (IPS), Proxy, se ejecutó un escaneo de vulnerabilidades y puertos con ayuda de web de EICAR Test para descargar archivos maliciosos. Las configuraciones del Firewall PfSense fueron aplicadas de acuerdo con los manuales de Netgate Doc obtenido de la página oficial, todos los módulos de seguridad trabajaron en conjunto sin ningún problema. Para la comprobación de la hipótesis se aplicó Chi-Cuadrado con un nivel de confianza de 0.05. Los indicadores fueron la Probabilidad de Amenaza versus la Magnitud del Daño, los cuales fueron valorados con una escala del uno al cuatro, siendo cuatro el nivel más alto de Probabilidad de Amenaza y Magnitud del Daño, para encontrar el valor final se estos dos se multiplicaron dando como resultado el nivel de Riesgo, mismo que fue valorado y comparado con la siguiente escala: si el resultado se encuentra entre 1 y 6 el riesgo es bajo, entre 8 y 9 riesgo medio, entre 12 y 16 riesgo alto. De acuerdo con los resultados obtenidos, implementar el Firewall PfSense reduce significativamente la Probabilidad de Amenaza y Magnitud del Daño, se concluye que, el uso del Firewall PfSense mejora la seguridad, integridad y confidencialidad de la información que tiene la compañía limita, se recomienda el uso de este software dentro de la red LAN de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba u otras entidades que necesiten fortalecer la seguridad informática.

Palabras clave: <VULNERABILIDADES>, <SEGURIDAD>, <CONFIDENCIALIDAD>, <INTEGRIDAD>, <PROBALIDAD DE RIESGO>, <MAGNITUD DE DAÑO>, <SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)>, <SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)>, <WEB EICAR>, <MÉTODO PROPUESTO>.

ABSTRACT

The objective of the research was to evaluate the security conditions that the Limited Liability Companies of the city of Riobamba have within their LAN network through surveys applied to sixty-four of them, most of which do not have security elements, they are connected to the ISP server or internet provider directly, this is probably due to the high cost in Firewall licensing. Likewise, the performance of the free software PfSense Firewall was evaluated, to which different tests were applied using Kali Linux 2021.2 and its tools such as nmap together with NESSUS, web EICAR to identify the security level of the Firewall. Tests were run on the Antivirus, IDS, IPS, Proxy, a vulnerability and port scan was run with the help of web EICAR Test to download malicious files. PfSense Firewall configurations were applied according to Netgate Doc manuals obtained from the official website, all security modules worked together without any problem. For hypothesis testing, Chi-Square was applied with a confidence level of 0.05. The indicators were the Probability of Threat versus the Magnitude of Damage, which were valued with a scale from one to four, being four the highest level of Probability of Threat and Magnitude of Damage, to find the final value these two were multiplied giving as a result the level of Risk, which was valued and compared with the following scale: if the result is between 1 and 6 the risk is low, between 8 and 9 medium risk, between 12 and 16 high risk. According to the results obtained we can say that, implementing the PfSense Firewall significantly reduces the Probability of Threat and Magnitude of Damage, we can conclude that, the use of the PfSense Firewall improves the security, integrity and confidentiality of the information that the company has limits, we recommend the use of this software within the LAN network of the Limited Liability Companies of the City of Riobamba or other entities that need to strengthen computer security.

Keywords: <VULNERABILITIES>, <SECURITY>, <CONFIDENTIALITY>, <INTEGRITY>, <PROBALITY OF RISK>, <MAGNITUDE OF DAMAGE>, <INTRUDER DETECTION SYSTEM [IDS]>, <INTRUDER PREVENTION SYSTEM [IPS]>, <WEB EICAR>, <PROPOSED METHOD>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Planteamiento del Problema

1.1.1. Situación Problemática

En el mundo actual, tan interconectado a través de internet, impulsado por la tecnológica, evolución e innovación y el creciente número de dispositivos conectados, hace que la web cada vez se vuelve más compleja y vulnerable, las compañías en su gran mayoría no tienen un control interno de la información, se limitan a tener conectados todos los equipos al enrutador que provee él IPS de su localidad. En este entorno, los incidentes de seguridad y ciberataques se incrementan exponencialmente.

Los sistemas y aplicaciones web son el blanco más frecuente de ataques. Por lo cual, la seguridad informática o ciberseguridad es crítica para salvaguardar la información como activo de alto valor de las Compañías, Empresas, Pymes. Es importante destacar que la seguridad interna de la información y dispositivos conectados a la red es crítica, tomando en cuenta que en la actualidad hay muchas personas que están laborando en la modalidad de teletrabajo, manejando así información delicada de la organización.

Los dispositivos IoT tienen una gran capacidad para recibir instrucciones desde internet, permitiendo que los usuarios ejecuten ordenes controlando así equipos electrónicos, sin embargo, estas funcionalidades no son perfectas abriendo una ventana a los posibles atacantes, dejando entrar a personas sin ser invitadas.

Pero, adquirir un dispositivo especializado para proteger la información es demasiado costoso, incluso algunas empresas y Pymes no lo tienen, existen otras opciones para solventar esto, contamos

con software libre que puede ayudar al aseguramiento de la información, de esta manera se disminuyen los costos y las personas pueden utilizarlos sin ninguna restricción.

El firewall es un equipo que permite el filtrado de tráfico entre dos redes o entre un quipo y una red, permitiendo o rechazando la información dependiendo de las reglas establecidas, el primer requerimiento se centra en la seguridad perimetral de la red manteniendo un primer nivel de protección frente a amenazas que provengan del exterior de la red.

1.1.2. Formulación del problema

¿Cómo aportará la evaluación del firewall de frontera PfSense en la protección de la confidencialidad, integridad y disponibilidad de información de las Compañías de Responsabilidad Limitada de Riobamba?

1.1.3. Preguntas directrices o específicas de la investigación

¿Cuáles son las vulnerabilidades más conocidas y explotadas en una red?

¿Cuáles son los aspectos que se deben considerar para proteger una red?

¿Qué normas y/o estándares aportan para conseguir una red segura?

¿Cómo configurar un firewall de frontera para mejorar la seguridad de la red?

1.2. Justificación de la investigación

1.2.1. Justificación Teórica

Una red insegura es un riesgo potencial que afecta a la Confidencialidad, Integridad y Disponibilidad de la información como bien intangible de las Empresas cuya pérdida, robo o sabotaje puede tener consecuencias desastrosas. Basado en esta problemática de la seguridad inherente de la información y sistemas informáticos, se han creado normas y estándares internacionales para concientizar sobre la importancia de tener un firewall de frontera y proporcionar guías, para la mitigación de vulnerabilidades que pueden presentar una red.

En el ámbito de las telecomunicaciones, un firewall (cortafuegos) es un dispositivo o sistema capaz de cifrar, limitar o decodificar el tráfico de comunicaciones entre un ordenador, o una red local, y el

resto de internet, con el objetivo de impedir que sistemas o usuarios no autorizados tengan acceso, una plataforma robusta para el control de accesos y protección de los servicios informáticos garantiza un correcto aprovechamiento de la infraestructura y garantiza la integridad y confidencialidad de la información.

Desde los primeros ataques de seguridad masivos, hasta la actualidad, los ciberataques se han ido perfeccionado y la protección digital se ha tenido que adaptar a técnicas maliciosas como por ejemplo el malware, o el phishing. Un firewall de seguridad permite protección de ataques de denegación de servicios, seguridad ante intrusión, accesos seguros desde equipos externos, filtrado con antivirus y antispam, detección de ataques de intrusos IPS e IDS, filtrado de contenidos, cortafuegos y sistemas de monitorización.

1.2.2. Justificación Práctica

Para validar el método propuesto se utilizarán dos (2) escenarios:

- El primero será la infraestructura de red simulada en forma general para la conexión directa al internet mediante un enrutador propiedad del ISP, al cual se conectan todos los dispositivos IoT del domicilio.
- El segundo escenario es una variante al cual se conectará el Firewall Pf Sense después del enrutador entregado por el ISP, al Firewall se le arán las configuraciones para seccionar la red WiFi para distribuir la conexión interna y usuarios externos o DMZ, control de ancho de banda, tiempo de uso del recurso, control de tráfico, IPS, IDS, control de virus.

Se pretende entonces verificar el nivel de seguridad que existe en estas dos infraestructuras mediante herramientas de detección de vulnerabilidades como: Nmap, Whireshak, Metaesploit, entre otros; y evaluar los resultados obtenidos.

Se deberá observar que el escenario dos (método propuesto) presenta menos riesgo de vulnerabilidad, al menos de los ataques más conocidos, al aplicar configuraciones de aseguramiento de entrada y salida de información.

1.2.3. Justificación Metodológica

La investigación dará a conocer la importancia de la seguridad informática dentro de una infraestructura de red local implementada en empresas, se implementará un firewall para controlar la entrada y salida de información, esto permitirá tener mayor control del tráfico de red.

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Evaluar el firewall de frontera free PfSense para proteger la confidencialidad, integridad y disponibilidad de la información de Compañías De Responsabilidad Limitada en Riobamba año 2021.

1.3.2. Objetivos Específicos

- Diagnosticar la seguridad actual de la red interna con la que cuentan las Compañías de Responsabilidad Limitada de Riobamba, mediante encuestas aplicadas para detectar vulnerabilidades con la finalidad de garantizar el Plan de Continuidad del Negocio.
- Diseñar un escenario de prueba de infraestructura de red general basado en las necesidades de las Compañías de Responsabilidad Limitada de Riobamba, utilizando Network Notepad con la finalidad de mejorar la seguridad y acceso a la información.
- Virtualizar la implementación de infraestructura de red propuesta con PfSense, garantizando el acceso de manera segura a los recursos informáticos e información de las Compañías de Responsabilidad Limitada de Riobamba.
- Evaluar los resultados obtenidos del escenario de prueba y compararlos con el diseño actual de red de las Compañías de Responsabilidad Limitada de Riobamba para analizar los beneficios obtenidos al implementar el firewall PfSense.

1.4. Hipótesis

La evaluación del firewall de frontera free PfSense mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba.

CAPÍTULO II

2. MARCO DE REFERENCIA

2.1. Antecedentes del problema

Con la finalidad de legitimar y lograr una buena comprensión de este estudio a todos los lectores, se han revisado varios trabajos de investigación similares de lo cuales se ha encontrado temas que defienden y sirven de referencia para desarrollar esta investigación.

2.1.1. Análisis de metodologías propuestas para mejorar la seguridad en la red interna de una empresa.

- "PFSENSE y RASPBERRY al rescate de la seguridad en hogares y Pymes Colombianas (Pérez, 2014), propone utilizar el software PFSENSE basado en Free BSD como una solución de seguridad perimetral teniendo en un inicio funcionalidades básicas y el posterior incremento de paquetes (VPN, abtivirus, IDS/IPS, proxy server, radius server y portales cautivos) para el fortalecimiento del núcleo; **pero es muy general y no se centra en la utilización de otros paquetes que ayudarían a mejorar la seguridad.**
- "Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS" (Marín, Patiño, & Acevedo, 2020), presenta un sistema para mejorar la seguridad perimetral de una microempresa, en la cual incluye una VPN, firewall, IDS, a este sistema se aplicaron pruebas de técnicas de penetración mediante Kali del sistema operativo Linux; **no contempla el uso del IPS, DNS server, radius y portales cautivos.**
- "Securing Wireless Network Using pfSense Captive Portal with Radius Authentication – A Case Study at UMaT" (Larbi, Asante, & Danso, 2016), presentan una propuesta de acceso a la red utilizando portal cautivo con autenticación radius para mejorar la seguridad de acceso a redes inalámbricas en la University of Mines and Technology utilizando PFSENSE; **se enfoca en las redes inalámbricas que son las más utilizadas.**

2.2. Bases teóricas

2.2.1. Arquitectura de una Red Empresarial

1. Arquitectura de Red Perimetral

(Hernández, 2016) Describe la arquitectura de red perimetral como un sistema que abarca diferentes esquemas en el cual es posible configurar soluciones de perímetro, por ejemplo, Firewalls, UTM, NGFW para cumplir con los estándares de seguridad requeridos.

2. Red de borde

Se encuentra en la periferia de la red interna y tiene comunicación al exterior por medio de un router y este a su vez deberá conectarse a un cortafuegos configurado de tal manera que filtre el tráfico de entrada y salida (Méndez, 2017).

3. Redes internas

Formada por un grupo de computadores o servidores internos al cual tiene acceso los usuarios para solicitar información de acuerdo con las actividades que realizan, un ejemplo sería un servidor SQL, Proxy, Web. (Mendez, 2017).

4. Red perimetral

Funciona como un puente de comunicación entre la red interna y redes exteriores brindando seguridad en caso de que usuarios no autorizados intenten acceder a la red interna encontrándose primero con una DMZ(Baca, 2016).

2.2.2. Amenazas Informáticas

(Tarazona T, 2007) Define una categorización básica que une las amenazas de acuerdo a sus similitudes que tiene en común: Errores humanos, defectos del procesamiento de información, catástrofes naturales y acciones malintencionadas de los usuarios, se puede listar las amenazas más comunes:

a) Alteración de la Información

b) Ataques de Fuerza Bruta

c) Denegación de Servicios (DDoS)

d) Desastres Naturales

e) Divulgación de Información

f) Espionaje

g) Fraudes basados en el uso de computadores

h) Robo de Información

i) Sabotaje, vandalismo

j) Suplantación de identidad

k) Uso no autorizado de Sistemas Informáticos

l) Virus informáticos o código malicioso

2.2.3. Firewall

Un firewall puede estar constituido por hardware, software o la combinación de los dos elementos, este dispositivo es la primera barrera de protección que deben pasar los paquetes en una red, puede aceptar o denegar el acceso de información dentro o fuera de la red, cada uno de los paquetes es analizado y toma la decisión adecuada. (Cisco, s.f.).

Utilizando reglas de filtrado un firewall permite o rechaza el acceso de un paquete, es una parte importante para la seguridad de la red interna. Es una pared que se encuentra entre el router del ISP y la red interna del domicilio, se puede implementar utilizando software, hardware o ambos, el objetivo de este es proteger la información ante posibles ataques informáticos por parte de personas u organizaciones mal intencionadas.

2.2.4. PfSense

PfSense es un software de código abierto diseñado sobre el núcleo Linux y específicamente FreeBSD, está implementado de tal manera que funciona como un firewall al cual le pueden incluir varios paquetes extras para mejorar su funcionamiento por esta razón es altamente manipulable, su configuración es muy intuitiva al tener una interfaz gráfica a la cual se accede por medio del navegador web, utiliza pocos recursos del hardware. (pfSense, s.f.).

1. Balanceo de Carga

Implementado el balanceo de carga podemos evitar que los servidores WEB, DNS y otros dejen de funcionar en caso de tener varios accesos simultáneos a estos servicios distribuyendo de manera equitativa las solicitudes de información a estos servidores. (pfsense, s.f.).

2. Enrutamiento estático

PfSense tiene instalado por defecto un servidor DHCP que proporciona direcciones IP a cada uno de los equipos que se conectan a la red (DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, 2016).

3. Portal Cautivo

El portal cautivo impide el acceso de personas no autorizadas a la red mediante una validación que se hace a través de un portal web al cual se redirecciona al usuario cuando desee ingresar a consumir los recursos de red. (pfsense, s.f.).

4. Servidor VPN

El modo VPN crea una comunicación en forma de túnel uniendo al usuario con el servidor evitado una posible fuga de información, esta comunicación se encuentra encriptada (pfsense, s.f.).

5. Servidor DNS y reenviador de cache DNS

Un servidor DNS es una lista de direcciones IP y nombres de dominios de páginas web o recursos de la res interna, compara el dominio con la IP y establece la comunicación entre el usuario y el servicios que desea consumir. (pfsense, s.f.).

6. Servidor DHCP

El servidor DHCP asigna direcciones IP de manera aleatoria a cada uno de los dispositivos que se conecten a la red interna permitiendo el ingreso y salida de la información, esto también aplica a las VLANs que se tenga asignado dentro de la red. (pfsense, s.f.)

7. Tabla de estado

La tabla de estado guardar reportes de cada una de las conexiones de esta manera se puede hacer un seguimiento detallado de los recursos que se encuentran consumiendo los usuarios de la red. (pfsense, s.f.).

2.2.5. Políticas del Firewall

(Microsoft, 2016) Describe que, dentro del firewall se deben establecer reglas de seguridad que permitan filtrar la entrada y salida de datos en la red interna o virtual, la información deberá pasar por un puerto específico de acuerdo al tipo de información que está consumiendo el usuario, tomando en cuenta que para cada tipo de tráfico existe un puerto que recibe la información, tomando esto en cuenta todos los demás puertos deberán estar cerrados, se deberá contar con el esquema de la red para poder estables reglas de manera más fácil y poderlas manipular de mejor manera de acuerdo al incremento de la red.

Tabla 1-2: Políticas predeterminadas del Cortafuegos.

Nombre de la Política	Nivel de Seguridad	Configuración del Cliente	Excepciones	Uso Recomendado
Acceso total	Bajo	Activar cortafuegos	Ninguna	Utilícela para permitir a los clientes un acceso a la red sin restricciones
Cisco Trust Agent for Cisco NAC	Bajo	Activar cortafuegos	Permitir el tráfico UDP entrante y saliente a través del puerto 21862	Utilícela cuando los clientes tienen una instalación del agente Cisco Trust Agent (CTA)
Puertos de comunicación para Trend Micro Control Manager	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP/UDP entrante y saliente a través de los puertos 80 y 10319	Utilícela cuando los clientes tienen una instalación del agente MCP

Consola de ScanMail for Microsoft Exchange	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 16372	Utilice esta opción cuando los clientes necesiten acceder a la consola de ScanMail
Consola de InterScan Messaging Security Suite (IMSS)	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 80	Utilícela cuando los clientes necesitan acceder a la consola de IMSS

Fuente: Trend Micro
Realizado por: Edison Ruiz

2.2.6. Redes de Computadoras

Grupo de equipos informáticos que se encuentran interconectados entre ellos, la forma de comunicación depende del medio o el canal de transmisión, estos pueden ser alámbrico, se refiere al canal de transmisión por medio de cables que pueden ser UTP, coaxial, fibra óptica y los medios inalámbricos son redes wifi, satélite y enlaces de microonda. (ANDREW S., 2009).

(Salcedo, 2017) Define a las redes de acuerdo con sus estándares de comunicación, se puede tener el estándar del modelo OSI que trabaja con siete capas para lograr la comunicación entre los dispositivos de la red y el protocolo TCP/IP que es más utilizado dentro de la nube de internet.

1. Estándares de redes:

a) IEEE 802.3, estándar para Ethernet
b) IEEE 802.5, estándar para Token Ring
c) IEEE 802.11, estándar para Wi-Fi
d) IEEE 802.15, estándar para Bluetooth

2. Protocolos de Redes:

(Cisco -CCNA, s.f.) Define el protocolo de red como una serie de estándares que se deben respetar para establecer la comunicación entre los equipos informáticos que se encuentran conectados a le red.

2.2.7. Seguridad Perimetral

(Sánchez, 2013) Define a la seguridad perimetral como algo esencial y primordial dentro de una red, estos elementos conjugan el software y hardware como mecanismos de protección básicos que puedan detectar la presencia de posibles personas no autorizadas, dependiendo del campo de aplicación los dispositivos de seguridad perimetral pueden variar y pueden estar constituidos por radares, cámaras de seguridad, IDS, IPS, bloqueos de microonda.

Las zonas seguridad pueden ser dividas de acuerdo a su nivel dentro de una red:

a) DMZ (Zona desmilitarizada)
b) Red interna
c) Red Externa

En este punto la red corporativa de cualquier universidad se conecta con la red púbica, por tal razón es importante reforzar las medidas de seguridad.

2.2.8. Vulnerabilidades de Red

(Cisco - CCNA, s.f.) Propone que la vulnerabilidad es una falencia dentro de todo el protocolo de seguridad y puede ser aprovechado por personas internas o externas para ingresar de manera no autorizada a la red.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Introducción

En esta sección se determinó los procedimientos y/o técnicas a utiliza para determinar el método más apropiado para disminuir los posibles riesgos potenciales de seguridad dentro de la red interna de las compañías de responsabilidad limitada de la ciudad de Riobamba así como el escenario de estudio, adicionalmente se verifico los instrumentos a utilizar.

Para este trabajo de investigación, la observación fua la herramienta más importante al momento de detectar las vulnerabilidades más críticas que se presentaron sobre el escenario, se clasificó la investigación.

3.2. Tipo y diseño de la Investigación

3.2.1. Tipo de Investigación

La investigación es considerada del tipo descriptiva y aplicado, ya que se utilizará el conocimiento adquirido producto de la investigación para realizar un estudio comparativo de las vulnerabilidades detectadas dentro de la red interna de las compañías de responsabilidad limitada de la ciudad de Riobamba con el antes y el después de la utilización del aseguramiento de la red perimetral utilizando el firewall PfSense con la finalidad de disminuir los potenciales riesgos de seguridad.

3.2.2. Diseño de la Investigación

El diseño de la presente investigación es de tipo cuasi-experimental, se establecerá una serie de pruebas estandarizadas a la infraestructura dentro de un ambiente controlado basado en la ingeniería del caos para descubrir fallas, para obtener valores cuantificables se utilizara software para análisis de vulnerabilidades sobre dos prototipos implementados que serán probados en ambientes controlados, se verificará antes y después de aplicar el firewall PfSense.

3.3. Métodos de Investigación

Para esta investigación se utilizará los siguientes métodos:

- El Método Científico ya que se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables; consta de las siguientes etapas:
  - Planteamiento del problema: Se basa en consulta de bibliografía científica, investigaciones realizadas en el país.
  - Formulación de la hipótesis.
  - Levantamiento de la información: Se ejecutarán pruebas de penetración en un amiente controlado.
  - Análisis e interpretación de resultados: Se analizarán los resultados obtenidos de las pruebas realizadas.
  - Comprobación de la hipótesis: Se determina si la con la implementación del firewall de frontera se mejorar el nivel de seguridad de las Compañías de Responsabilidad Limitada.
  - Difusión de resultados.
- El Método Analítico se aplica durante la etapa de análisis donde se recopiló la información, para proyectar lo que se va a realizar y como se va realizar la investigación
- Método Experimental porque se basa en pruebas realizadas en escenarios de laboratorio, en las que se observa los elementos más importantes del objeto de estudio que se investiga para obtener una captación de los fenómenos a primera vista.

3.4. Fuentes de Información

3.4.1. Primarias

- Pruebas
- Observación de resultados

3.4.2. Secundarias

- Trabajos de investigación nacional e internacional.
- Tesis desarrolladas relacionadas con el tema de investigación.
- Artículos científicos en base de datos de bibliotecas virtuales.

- Libros especializados en la biblioteca y electrónicos.
- Sitios web oficiales y blogs de especialistas.
- Revistas indexadas y no indexadas publicadas.
- Revistas electrónicas.
- Diccionarios especializados.
- Compañías de Responsabilidad Limitada de Riobamba

3.5. Técnicas de recolección de datos primarios y secundarios

Las técnicas que se utilizaron para la recolección de datos de la investigación fueron:

Las técnicas que serán utilizadas en la presente investigación son:

- Recopilación de información: permite obtener información esencial del objeto de estudio de la investigación para su desarrollo, utilizando todas las fuentes.
- Encuestas: permite recoger información sobre la situación inicial de las compañías de responsabilidad limitada de Riobamba.
- Observación: Permite determinar los resultados de las pruebas realizadas en las simulaciones bajo un amiente controlado.
- Análisis: determina los resultados de la investigación.
- Pruebas: ejecuta los experimentos en los escenarios de pruebas en un amiente controlado.

3.6. Planteamiento de la Hipótesis

3.6.1. Hipótesis General

La evaluación del firewall de frontera free PfSense mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba.

3.6.2. Identificación de variables

- **Variable Independiente:** Políticas de seguridad del firewall de frontera.
- **Variable Dependiente:** Nivel de seguridad de la red interna de las Compañías de Responsabilidad Limitada.

3.6.3. Operacionalización de Variables

- **Operacionalización Conceptual de Variables**

Tabla 1-3: Operacionalización conceptual de variables

Variable	Tipo	Concepto
Políticas de seguridad del firewall de frontera.	Independiente	Conjunto de políticas aplicadas al firewall de frontera PfSense.
Nivel de seguridad de la red interna de las Compañías de Responsabilidad Limitada.	Dependiente	Disminución de riesgos potenciales de la red interna de las Compañías de Responsabilidad Limitada.

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

- **Operacionalización Metodológica de Variables**

Tabla 2-3: Operacionalización de Metodología de Variables

Hipótesis	Variables	Indicadores	Técnica	Instrumento
La evaluación del firewall de frontera free PfSense mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba.	**Independiente** Políticas de seguridad del firewall de frontera. **Dependiente** Nivel de seguridad de la red interna de las Compañías de Responsabilidad Limitada	Normas Políticas Controles Vulnerabilidades detectadas	Observación Encuesta Observación Pruebas con software	Políticas de seguridad implementadas dentro del Firewall Herramientas para detección de vulnerabilidades

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

3.7. Población y Muestra

3.7.1. Población

La población será de 531 Compañías de Responsabilidad Limitada de la ciudad de Riobamba (Superintendencia de Compañías, s. f.), información tomada de la Superintendencia de Compañías.

3.7.2. Selección de la Muestra

Para determinar la muestra se tomó en consideración las 531 Compañías de Responsabilidad Limitada de la ciudad de Riobamba (Superintendencia de Compañías, s. f.), el muestreo se realizará con un nivel de confianza del 95%, dando un total de 64 Compañías a las cuales se aplicará una encuesta para determinar el estado de su seguridad, los resultados se valoraran para determinar las políticas de seguridad a implementar dentro del firewall de frontera PfSense que será implementado en máquina virtual para realizar pruebas de vulnerabilidades.

Tabla 3-3: Vulnerabilidades a evaluar

Nº	Vulnerabilidades
1	Puertos abiertos
2	DMZ
3	IPS
4	IDS
5	Acceso a red WiFi
6	Exposición de datos sensibles
7	Acceso y denegación de acceso

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

3.8. Procedimientos Generales

Para recolectar la información se usará la información proporcionada por los encargados del manejo de la red interna de las Compañías de Responsabilidad Limitada de la ciudad de Riobamba, con la finalidad de verificar si utilizan un firewall de frontera, cuáles son las políticas implementadas en el este dispositivo para mitigar las posibles irrupciones de usuarios no autorizados a la red y controles de acceso a la información.

Tabla 4-3 Técnicas para la demostración de la hipótesis

Variables	Indicadores	Técnicas
INDEPENDIENTE	Normas Políticas Controles	Pruebas al Sistema
DEPENDIENTE	Vulnerabilidades detectadas	Observación Pruebas con software

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

3.9. Instrumentos de recolección de datos primarios

En la tabla que se presenta a continuación se detallan los instrumentos o herramientas empleados para la recolección de datos:

Tabla 5-3. Instrumentos de recolección de datos

Instrumentos	Descripción
Kali Linux	Distribución basada en Debian GNU7Linux diseñada para auditoria
Otros	**Navegadores web:** Firefox **Sniffing:** Wireshark, Ettercap **Escaneo y detección de vulnerabilidades:** Nessus, nmap **Explotación de vulnerabilidades:** nmap **Denegación de Servicios:** Synflood **Observación:** Ficha de observación

Fuente: Investigación
Realizado por: Ruiz Edison, 2021

3.10. Instrumentos para procesar datos recopilados

Entre los instrumentos para procesar los datos tenemos:

- **Excel.-** Para el tratamiento de los datos, nos ayudará en la realización de gráficos, diagramas, etc.; prepara la información para un análisis posterior
- **SPSS.-** Realiza un análisis estadístico de datos y servirá para graficar la distribución.

3.11. Ambiente de pruebas

3.11.1. Hardware y software utilizado

Se utilizará la versión más actual y con soporte de PfSense 2.5.2 que se encuentra en la URL: https://www.pfsense.org/download/, con la cual se implementará el Firewall de frontera y se realizarán las configuraciones necesarias de acuerdo con el análisis inicial para una adecuada seguridad y óptimo rendimiento de la red interna.

Para la implementación de las políticas de seguridad se tomará en cuenta configuraciones estándar de acuerdo con las investigaciones realizadas como por ejemplo cerrar puertos no utilizados, DMZ, IDS, IPS, validación de usuarios para acceso a la red.

Tabla 6-3. Hardware utilizado para pruebas

Cantidad	Equipo	Marca	Modelo	Especificaciones	Observaciones
1	Portátil	DELL	INSPIRON 5567	INTEL CORE i7 2.2 GHZ, 16 GB en RAM	Equipo personal para el desarrollo del prototipo y el proyecto de tesis
1	portátil	DELL	INSPIRON N4050	INTEL CORE i5 2.2GHZ, 6GB en RAM	Equipo personal sobre el cual se implementara el Firewall de frontera PfSense.

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

Tabla 7-3 Software utilizado para pruebas

Nombre	Descripción	Observaciones
PfSense 2.5.2	Firewall de Frontera	Software utilizado para implementar políticas de seguridad.
Kali Linux 2021.2	Sistema Operativo para Pentesting	Software utilizado para realizar pruebas de penetración.
VMWare Workstation 10	Simulador para máquinas virtuales	Software sobre el cual se instalara el Firewall PfSense 2.5.2

Fuente: Ruiz Edison, 2021
Realizado por: Ruiz Edison, 2021

3.11.2. Prototipos de prueba

- Creación de clientes: Los clientes se simularán en máquinas virtuales con ayuda del software VMware 15.5 Pro que permite crear máquinas virtuales en el cual estará instalado el servidor PfSense 2.5.2
-

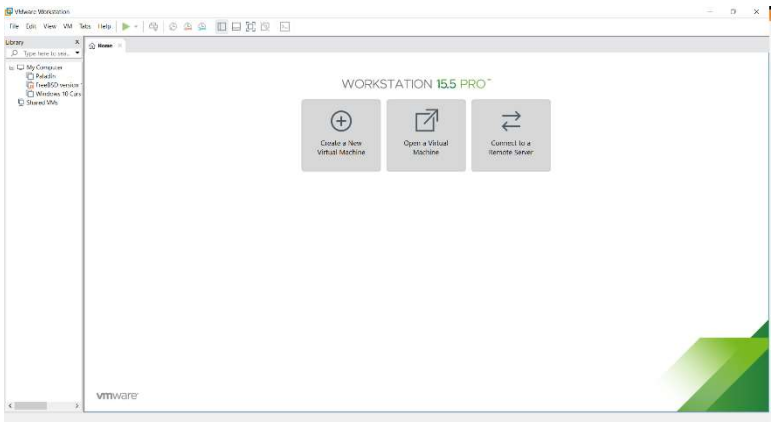


Figura 1-3. Interfaz de VMware Workstation
Fuente: Autor

Las máquinas virtuales para los clientes dispones de un procesador dedicado con un núcleo, un tamaño de memoria RAN virtual de 1GB, tamaño de disco variable que aumenta su tamaño de acuerdo con las necesidades, se debe tomar en cuenta que este consumo merma la memoria RAN del anfitrión y su tarjeta de red virtual, los usuarios contaran con un Sistema Operativo Windows 10 Home.

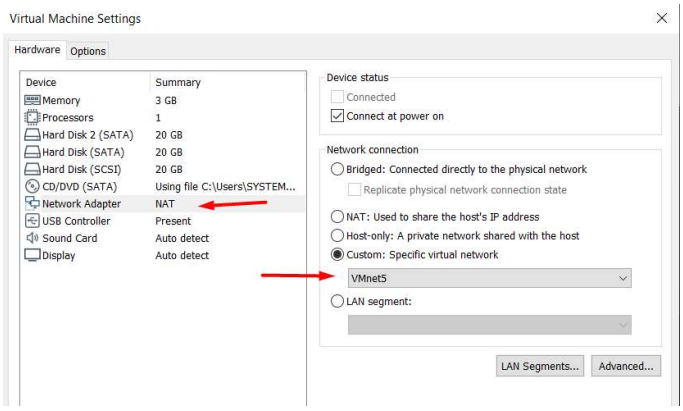


Figura 2-3. Edición del tipo de red
Fuente: Autor

- Creación del Servidor PfSense
- Diseño de la red interna

- Configuración de los dispositivos de red
- Servicio Squid: Proxy transparente para el control de páginas web
- DMZ
- Servidor DHCP
- Implementación de políticas en PfSense
- Control de acceso

3.12. Selección de la metodología

Al no existir un sistema 100% seguro, en este caso un aseguramiento completo utilizando un Firewall de frontera, no se descartará ninguna propuesta de seguridad existente, todas las medidas que se puedan tomar para evitar los posibles riesgos de seguridad se consideraran para mermar el posible acceso de usuarios no autorizados a la red, de esta manera se volverá más difícil la tarea de quien intente vulnerar la seguridad de la red.

3.12.1. Metodología seleccionada

El método o guía que se utilizará para aplicar las políticas de seguridad se basan en la descripción de 24 políticas básicas para seguridad perimetral (Gutierrez, 2018), la cual se basa en cinco dominios con un total de 24 políticas de seguridad.

- Arquitectura: Definir zonas de seguridad para controlar el acceso a redes
- Acceso: Se debe negar todo, excepto
- Administración y Gestión: Se debe tener un diagrama actualizado de la red
- Acceso VPN
- Navegación en internet

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Presentación de resultados

En esta sección se realizará una discusión de los resultados, donde se interpretará los resultados obtenidos en la investigación y su relación con los objetivos y la hipótesis.

En base a los resultados obtenidos, se observará que muchos de las Compañías de Responsabilidad Limitada de la ciudad de Riobamba no cuentan con un Firewall de frontera para proteger la red interna y en los casos que tienen seguridad perimetral solo cuentan con bloqueo de páginas web de acuerdo con el horario de trabajo, es decir tienen bloqueado el acceso a redes sociales u otras páginas que no son necesarias para desarrollar su trabajo diario.

4.2. Identificación de información

La identificación de activos es muy importante al permitir ejecutar con precisión el alcance de la investigación, permite valorar los activos con veracidad e identificar las posibles amenazas que podrían ser explotadas por personas internas o externas. Se presentarán los resultados de la encuesta aplicada a cada una de las 64 Compañías de Responsabilidad Limitada de la cuidad de Riobamba.

Figura 3-4. Encuesta aplicada a las Compañías de Responsabilidad Limitada Riobamba
Fuente: Autor

4.3. Tabulación de resultados de la encuesta

Se presentarán los resultados obtenidos de la encuesta realizada a las 64 Compañías de Responsabilidad Limitada de la ciudad de Riobamba, de acuerdo con este diagnóstico se realizará la propuesta para mejorar la seguridad. Cada una de las preguntas fue elaborada tomando en consideración parámetros básicos de aseguramiento de información.

Debemos tomaran en cuenta que la mayor parte de compañías no cuenta con un departamento informático para dar soporte, en algunos casos se encuentran conectados de manera directa al enrutador de su proveedor de internet.

4.3.1. Resultados de la encuesta.

- ¿Utiliza un Firewall de frontera o perimetral para seguridad de la red interna de la Compañía?

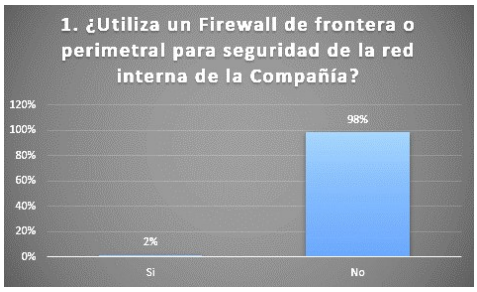


Gráfico 1-4. Resultado de la encuesta pregunta 1
Fuente: Autor

Resultado: El 98% de las Compañías de Responsabilidad Limitada no tienen un Firewall para proteger su red interna, se conectan directamente al enrutador del proveedor de internet (ISP), solo el 2% utiliza este elemento por seguridad.

- ¿Qué tipo de firewall utiliza?

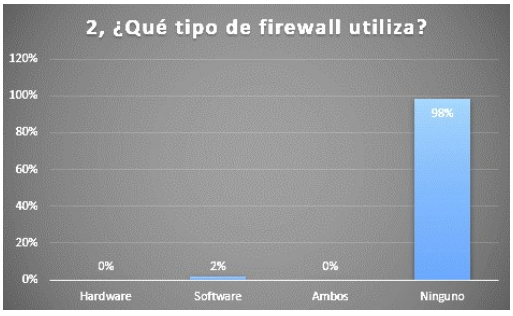


Gráfico 2-4. Resultado de la encuesta pregunta 2
Fuente: Autor

Resultado: 2% de las Compañías de Responsabilidad Limitada tiene software que haces las funciones de Firewall, el 98% no utiliza un Firewall para asegurar la red interna.

- El firewall que utiliza es:

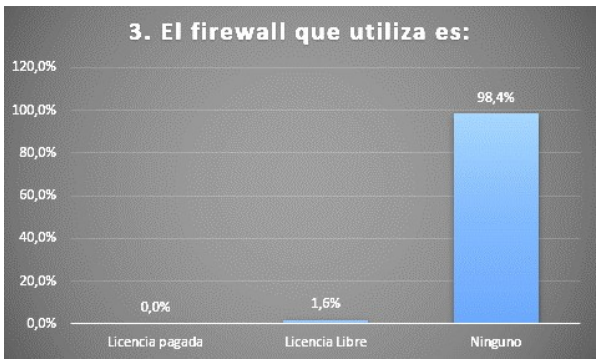


Gráfico 3-4. Resultado de la encuesta pregunta 3
Fuente: Autor

Resultado: El 1.6% de las Compañías de Responsabilidad Limitada utiliza un Firewall de Licencia Libre, no paga por el uso, el 98.4% no utiliza.

- Las configuraciones del firewall son

Gráfico 4-4. Resultado de la encuesta pregunta 4
Fuente: Autor

Resultado: El 2% de las Compañías de Responsabilidad Limitada configura el equipo de acuerdo con los requerimientos de la empresa y el 98% no utiliza un Firewall.

- Tiene control de acceso de usuarios

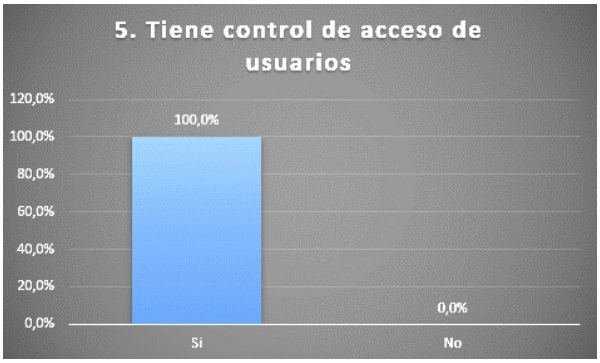


Gráfico 5-4. Resultado de la encuesta pregunta 5
Fuente: Autor

Resultado: EL 100% de las Compañías de Responsabilidad Limitada cuenta con un control de usuarios dentro de su red.

- Para el control de acceso utiliza:

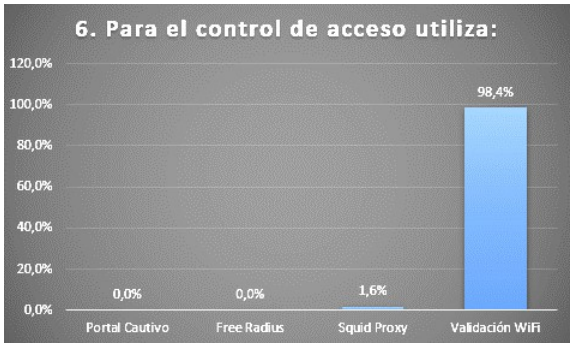


Gráfico 6-4. Resultado de la encuesta pregunta 6
Fuente: Autor

Resultado: El 98.4% de las Compañías de Responsabilidad Limitada tiene un control por medio de validación de red WiFi, 1.6% utiliza el Squid Proxy invisible.

- Tiene implementado una DMZ (zona desmilitarizada) para usuarios externos

Gráfico 7-4. Resultado de la encuesta pregunta 7
Fuente: Autor

Resultado: El 100% de las Compañías de Responsabilidad Limitada no utiliza una DMZ, todos los usuarios se conectan a una misma red.

- Tiene implementado un IPS (sistema de prevención de intrusos)

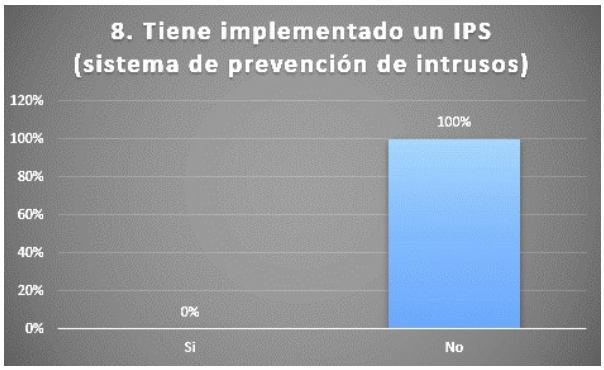


Gráfico 8-4. Resultado de la encuesta pregunta 8
Fuente: Autor

Resultado: El 100% de las Compañías de Responsabilidad Limitada no utiliza un sistema de prevención de intrusos en la red.

- Tiene implementado un IDS (sistema de detección de intrusos)

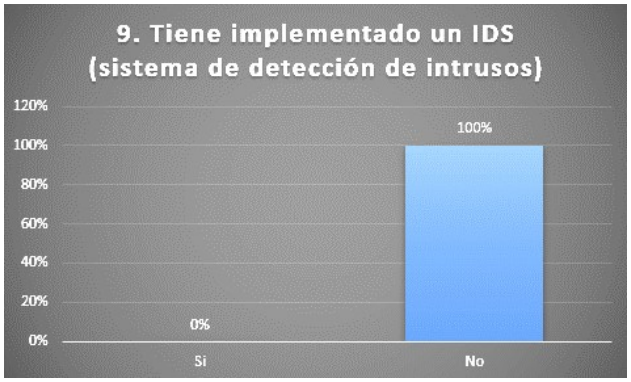


Gráfico 9-4. Resultado de la encuesta pregunta 9
Fuente: Autor

Respuesta: El 100% de las Compañías de Responsabilidad Limitada no cuenta con un Sistema de Detección de Intrusos.

- Tiene implementado VLans para separar las áreas de la Compañía

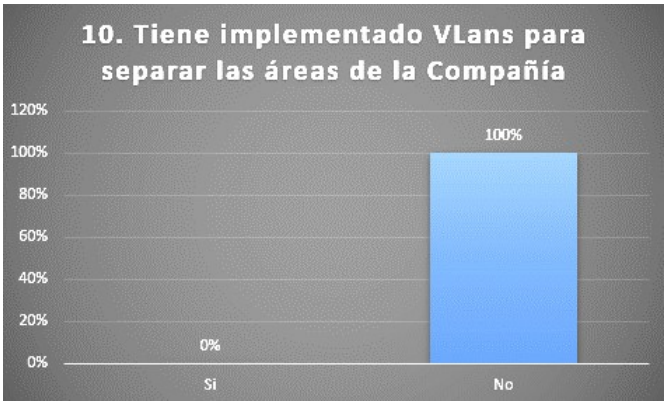


Gráfico 10-4. Resultado de la encuesta pregunta 10
Fuente: Autor

Respuesta: El 100% de las Compañías de Responsabilidad Limitada no cuenta con Redes Virtuales Locales.

- El antivirus que utiliza dentro de su empresa tiene:

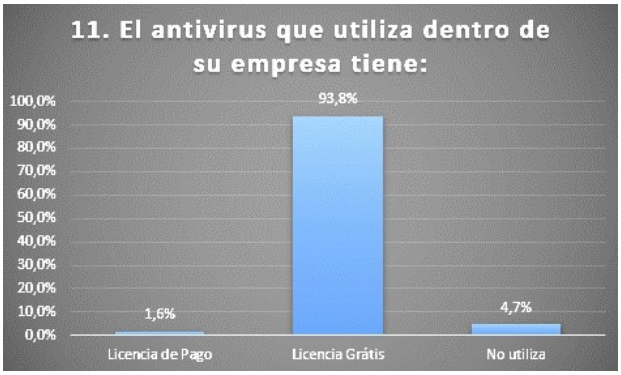


Gráfico 11-4. Resultado de la encuesta pregunta 11
Fuente: Autor

Resultado: El 93.8% de las Compañías de Responsabilidad Limitada utilizan antivirus de licencia libre para sus equipos de cómputo, un 4.7% no utiliza ningún tipo de antivirus y solo el 1.6% paga la licencia por tener protección en sus equipos de cómputo personales.

- Cuando un empleado es desvinculado de la Compañía

Gráfico 12-4. Resultado de la encuesta pregunta 12
Fuente: Autor

Resultado: El 95.3% de las Compañías de Responsabilidad Limitada no realiza ninguna acción cuando desvinculan a un empleado o trabajador, un 1.6% cierran todas las cuentas relacionadas con la compañía y cambian las claves de acceso a los dispositivos digitales, 1.6% cambia las claves de acceso a los dispositivos digitales, el 1.6% respalda la información y formatea el computador que utilizaba.

- Estaría dispuesto a utilizar un Firewall de frontera de Licencia gratuita que se ajuste a los requerimientos antes mencionados

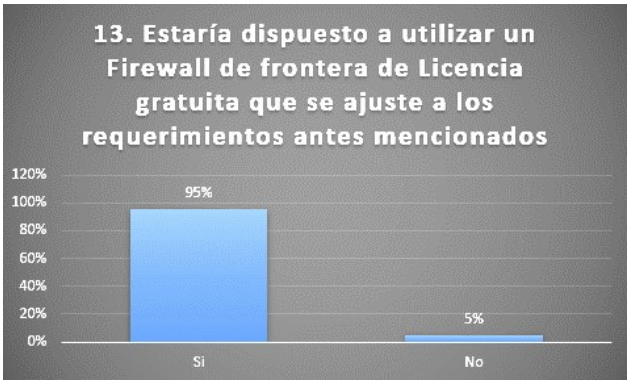


Gráfico 13-4. Resultado de la encuesta pregunta 13
Fuente: Autor

Resultado: El 95% de las Compañías de Responsabilidad Limitada estaría dispuesto a utilizar un Firewall de licencia gratuita para mejorar la seguridad de la red, el 5% no cree necesario el utilizar este elemento de protección.

- **Resumen de resultados antes de utilizar el Firewall PfSense**

Tabla 8-4: Resumen de resultados de Encuesta-Antes de utilizar el Firewall PfSense

Nº	Preguntas	Frecuencias				Total
1	¿Utiliza un Firewall de frontera o perimetral para seguridad de la red interna de la Compañía?	SI		NO		
		1		63		64
2	¿Qué tipo de firewall utiliza?	Hardware	Software	Ambos	Ninguno	
		0	1	0	63	64
3	El firewall que utiliza es:	Licencia de Pago	Licencia Libre	Ninguno		
		0	1	63		64
4	Las configuraciones del firewall son	Por defecto	Implementadas	Ninguno		
		0	1	63		64

5	Tiene control de acceso de usuarios	SI		NO		
		64		0		64
6	Para el control de acceso utiliza:	Portal Cautivo	Free Radius	Squid Proxy	Validación WiFi	
		0	0	1	63	64
7	Tiene implementado una DMZ (zona desmilitarizada) para usuarios externos	SI		NO		
		0		64		64
8	Tiene implementado un IPS (sistema de prevención de intrusos)	SI		NO		
		0		64		64
9	Tiene implementado un IDS (sistema de detección de intrusos)	SI		NO		
		0		64		64
10	Tiene implementado VLans para separar las áreas de la Compañía	SI		NO		
		0		64		64
11	El antivirus que utiliza dentro de su empresa tiene:	Licencia de Pago	Licencia Gratis	No utiliza		
		1	60	3		64
12	Cuando un empleado es desvinculado de la Compañía	Cierra todas las cuentas relacionadas con la Compañía	Cambia las claves de acceso a los dispositivos digitales	Respalda la información y formatea el computador que utilizaba	No realiza ninguna acción	
		1	1	1	61	64
13	Estaría dispuesto a utilizar un Firewall de frontera de Licencia gratuita que se ajuste a los requerimientos antes mencionados	SI		NO		
		61		3		64

Fuente: Resultados Encuesta

Realizado por: Edison Ruiz

4.4. Evaluación del Firewall

Analizando la encuesta realizada a las Compañías de Responsabilidad Limitada podemos darnos cuenta de que la mayoría de ellas se encuentra conectada al internet exponiendo toda su información y exponiendo sus aplicaciones a diferentes tipos de ataques, estos pueden ser ejecutados a través de malware, spyware, accesos no autorizados y diversas variaciones de amenazas externas o internas.

En la mayoría de los casos no se implementa ninguna solución para mitigar las vulnerabilidades por el costo que representa el licenciamiento de este software, una de las alternativas para costear un sistema de protección o firewall es el uso de sistemas Open-Source, al tener en el mercado una gran variedad de sistemas nos centraremos en evaluar el Free PfSense y valorar su ajuste a las necesidades de las Compañías de Responsabilidad Limitada.

4.4.1. Entorno de Pruebas

La virtualización facilita el tener varios equipos corriendo en un mismo recurso físico, dentro de un computador podemos correr servidores y computadores con diferentes sistemas operativos y todos ellos interconectados al mismo tiempo, en este caso, la limitación dependerá del computador físico en el cual está corriendo la virtualización, por tal razón se consideró un equipo que soporte el consumo de recursos.

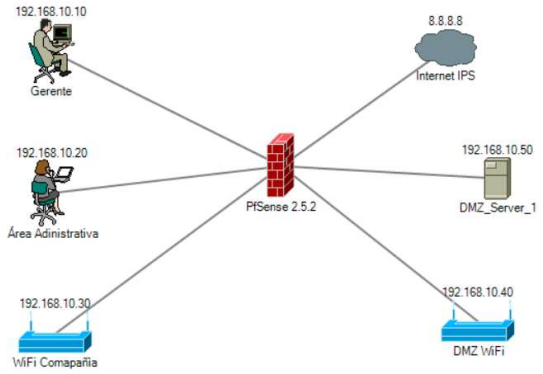


Figura 4-4. Diseñe de la red de pruebas elaborado en Network Notepad
Fuente: Autor

En la figura 17 se muestra la topología de red que vamos a utilizar dentro del entorno de pruebas, en la cual están configuradas las redes WAN, LAN y DMZ, dentro de la red LAN se encuentra una VM con sistema operativo Ubuntu Desktop y la DMZ cuenta con Ubuntu Server, el tráfico proveniente de la red WAN hacia la red LAN y DNZ será filtrado por el firewall PfSense, para realizar los ataques se utilizó un VM con sistema operativo Kali Linux con el cual se hará el escaneo de puertos y vulnerabilidades, dentro de la red LAN se hará la descarga de archivos infectados y el uso de herramientas web EICAR Test.

Para la valoración del firewall se instalaron las características valoradas en la encuesta, Servidor DHCP, Antivirus, IDS/IPS, Servidor Proxy, todos estos elementos fueron configurados en el PfSense después de su instalación siguiendo las recomendaciones del manual Netgate Docs.

Para la máquina del atacante se utilizó el sistema operativo Kali Linux 2021.2, para el escaneo de puertos se utilizó la herramienta Nmap. Se utilizó la herramienta Nessus para escanear vulnerabilidades del PfSense y servidor web, el cual tiene sistema operativo Ubuntu Server 20.04 LTS dentro de este se encuentra corriendo Apache Server versión 2.4.41 y está conectado a la DMZ.

Tabla 9-4: Configuración de las Máquinas virtuales y PfSense

Máquinas Virtuales	**Configuración**
PfSense Community Editión versión 2.5.2	4 Gb de memoria RAN 2 procesadores 1 partición de 40 Gb 3 adaptadores de red
Kali Linux versión 2021.2	2 Gb de memoria RAN 1 procesadores 1 partición de 20 Gb 1 adaptadores de red
Ubuntu Server versión 20.04.1 LTS	1 Gb de memoria RAN 1 procesadores 1 partición de 10 Gb 1 adaptadores de red
Ubuntu Desktop versión 20.04.2	1.5 Gb de memoria RAN 1 procesadores 1 partición de 10 Gb 1 adaptadores de red

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz, 2021

4.4.2. Servicios del firewall PfSense

Los servicios que ofrece el firewall PfSense se detallan a continuación, esto ayudará a tener una mejor idea de los recursos que podemos utilizar para proteger la red interna de las Compañías de Responsabilidad Limitada.

Tabla 10-4: Servicios del firewall PfSense

Servicios	**PfSense Community Edition versión 2.5.2**
Servidor DNS	SI
Servidor DHCP	SI
VPN (Ipsec y Open VPN)	SI
Balanceo de carga NAT	SI
Tabla de estado	SI
Proxy	SI
Enrutamiento	SI
IP virtuales	SI
Portal Cautivo	SI
Filtrado web	SI
IPS	SI
IDS	SI
AntiSpam	SI
Antivirus	SI
Antiphishing	NO
Servidor PPPoE	SI
Control de usuarios	SI
Servidor SNMP	NO
Spyware	SI

Fuente: Netgate Docs, 2021

Realizado por: Edison Ruiz

4.4.3. Detección de vulnerabilidades con la herramienta Nessus

Se realizó un escaneo avanzado con la herramienta Nessus la cual valora las vulnerabilidades con la siguiente escala enumeradas de mayor a menor grado de peligrosidad; Critical, High, Medium, Low, Info, en algunos casos detalla las posibles soluciones de la vulnerabilidad encontrada, después de terminado el escaneo tenemos el siguiente resultado.

Tabla 11-4: Resultados de escaneo avanzado vulnerabilidades direccionado a los hosts con Nessus

Firewall	Vulnerabilidades
PfSense Community Edition versión 2.5.2	13 del tipo informativo

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz, 2021

Vulnerabilidades del tipo informativo se encuentran en la escala más baja de la herramienta Nessus, se detalla los puertos escaneados del Pfsense.

Tabla 12-4: Resultados del escaneo web de vulnerabilidades direccionado a los hosts con Nessus

Firewall	Vulnerabilidades
PfSense Community Edition versión 2.5.2	17 del tipo informativo

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz, 2021

Vulnerabilidades del tipo informativo se encuentran en la escala más baja de la herramienta Nessus, se detalla los puertos escaneados del Pfsense.

4.4.4. Escaneo de puertos con nmap

El escaneo con la herramienta nmap se realizó desde la máquina virtual Kali Linux 2021.2 la cual incluye en su instalación, la prueba se aplicó a los equipos de la red incluido el firewall PfSense, para la prueba se utilizó el comando; nmap -sS-SV-PN-P 1-65535-r-w ipDestino, cada parámetro realiza la siguiente prueba:

- sS: Envía un paquete SYN para abrir una conexión real y marca el puerto como abierto si recibe un SYN/ACK, y cerrado al recibir un ICMP unreachable error o ninguna respuesta
- SV: Escaneo del servicio que está corriendo en el puerto.
- PN: Fuerza el escaneo
- p 1-65535 comprueba todos los puertos.
- r: comprueba los puertos de forma consecutiva.
- w: Muestra toda la información en pantalla.

Tabla 13-4: Resultados del escaneo de puertos con nmap

Firewall	Puerto	Estado	Servicio	Versión
PfSense Community Edition versión 2.5.2	80	Abierto	http	Apache httpd 2.4.41

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz

Al cerrar todos los puertos a acepción del 80 para mantener comunicación con el servidor la red se vuelve menos vulnerable, el PfSense brinda una mejora en la protección.

4.4.5. Prueba de archivos maliciosos con EICAR Test.

La prueba se realizó con la herramienta EICAR Test para poner a prueba el funcionamiento del antivirus del PfSense el cual trabajo con ClamAV este paquete está incluido en Squid Guard, con esto verificaremos si el firewall es capaz de detectar un archivo con contenido malicioso.

Tabla 14-4: Resultados del EICAR Test

Archivos de prueba	Resultado del PfSense Community Edition Versión 2.5.2
eicar.com	Bloqueado
eicar.com.txt	Bloqueado
eicar_com.zip	Bloqueado
eicarcom2.zip	Bloqueado

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz

Todas las pruebas tuvieron resultados favorables, los archivos con contenido malicioso fueron bloqueados, con esta prueba se asume que el firewall puede detectar este tipo de archivos aumentando la seguridad de la red y de los equipos.

4.4.6. Tipo de licencia que utiliza el Firewall PfSense

PfSense es una distribución Open Source, por esta razón cuenta con varios paquetes de libre acceso que permiten controlar diferentes ámbitos de seguridad y permiten expandir fácilmente las

funcionalidades del software sin comprometer su desempeño dentro de una Empresa, está basado en Free BSD para el uso del Router y Firewall.

Las Compañías CIA LTDA podrán acceder a este software sin ninguna restricción y pago, los requerimientos mínimos para la instalación y funcionamiento del Firewall son:

- Procesador 600Mhz (mas es mejor) de 64Bits.
- 512Mb RAM (mas es mejor)
- 4Gb disco (mas es mejor)
- 2 tarjetas de red (mínimo WAN y LAN)
- Puerto USB o DVD para instalación del ISO.
- Conectividad a internet.

4.5. Análisis de riesgo entre de la evaluación de las Compañías y la evaluación del PfSense

Un ataque informático es cuando la amenaza se convirtió en realidad, cuando el evento se realizó, pero no se determina si el atacante tuvo éxito o no, los datos e información fueron perjudicados perdiendo su confidencialidad, integridad y disponibilidad. Para estimar la probabilidad de amenaza que tienen las empresas se valoró cada una de las preguntas de acuerdo con la siguiente escala.

Tabla 15-4: Valoración de vulnerabilidades

Clasificación por Gravedad	Nivel	Conocimiento del Atacante
Insignificante	1	Alto
Bajo	2	Medio - Alto
Mediana	3	Ninguno - Medio
Alta	4	Ninguno, ejecutar la herramienta

Fuente: Gestión de riesgo en la seguridad informática, 2021

Realizado por: Edison Ruiz

Para obtener el resultado aplicaremos la fórmula matemática Riesgo = Probabilidad de Amenaza x Magnitud del daño, si el resultado se encuentra entre 1 y 6 el riesgo es bajo, entre 8 y 9 riesgo medio, entre 12 y 16 riesgo alto.

Tabla 16-4: Valoración de riesgo de las Empresas sin módulos de protección.

Empresa sin módulos de protección	Probabilidad de Amenaza	Magnitud de Daño	Resultado	Riesgo
Firewall	4	4	16	Alto
IDS	4	4	16	Alto
IPS	4	4	16	Alto
DMZ	4	4	16	Alto
Antivirus	2	4	8	Medio

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz

Sin módulos de protección las empresas se encuentran total mente expuestas a los atacantes y como consecuencia su información no será confidencial, integra y no estaría disponible.

Tabla 17-4: Valoración de riesgo de las Empresas con módulos de protección.

Empresa con módulos de protección	Probabilidad de Amenaza	Magnitud de Daño	Resultado	Riesgo
Firewall	2	2	4	Bajo
IDS	2	1	2	Bajo
IPS	2	1	2	Bajo
DMZ	2	3	6	Bajo
Antivirus	2	2	4	Bajo

Fuente: Edison Ruiz, 2021

Realizado por: Edison Ruiz

4.5.1. Análisis e interpretación de resultados

El nivel de riesgo al implementar los módulos de protección que brinda el PfSense disminuyó de Alto a Bajo, por lo cual es recomendable que las Empresas de Responsabilidad Limitada de la Ciudad de Riobamba lo utilicen dentro de su red LAN.

4.6. Comparativa de vulnerabilidades antes y después de la valoración del firewall PfSense.

Tabla 18-4: Frecuencias observadas (fo), comparativa de riesgos antes y después de la evaluación del firewall PfSense

Riesgos	Frecuencias		Total
	Antes	Después	
Alto	4	0	4
Medio	1	0	1
Bajo	0	5	5
Total	**5**	**5**	**10**

Fuente: Encuestas aplicas a Empresas y Evaluación del Firewall PfSense

Realizado por: Edison Ruiz

- Para medir la reducción de riegos de las Empresas de Responsabilidad Limitada con la evaluación del firewall de frontera PfSense se determina que el 100% de riesgo alto y medio se redujo a un riego bajo.

4.7. Comprobación estadística de la hipótesis

Para la comprobación de la hipótesis general se aplicó estadística inferencial aplicando **Chi-Cuadrado (X^2)**. Después de analizar y valorar la probabilidad de amenaza y magnitud del daño se determinó la siguiente hipótesis nula Ho y la alternativa H1:

- La **Hipótesis Nula (Ho)** "La evaluación del firewall de frontera free PfSense no mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba." con un nivel de significancia del 5% en la prueba de Chi Cuadrado X^2.
- La **Hipótesis Alternativa (H1)** "La evaluación del firewall de frontera free PfSense si mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba." con un nivel de significancia del 5% en la prueba de Chi Cuadrado X^2.

Para comprobar la hipótesis se aplicó encuestas a 64 Empresas de Responsabilidad Limitada de la Ciudad de Riobamba y se evaluó el Firewall PfSense utilizando herramientas disponibles dentro del sistema operativo Kali Linux 2021.2 y Nessus.

La tabla de frecuencias esperadas (fe) la calculamos con la fórmula:

$$f_e = \frac{\boldsymbol{Total\ columna\ x\ Total\ fila}}{\boldsymbol{Suma\ total}}$$

$$f_{e1,1} = \frac{5x4}{10} = 2$$

$$f_{e1,2} = \frac{5x4}{10} = 2$$

$$f_{e2,1} = \frac{5x1}{10} = 0.5$$

$$f_{e2,2} = \frac{5x5}{10} = 0.5$$

$$f_{e3,1} = \frac{5x5}{10} = 2.5$$

$$f_{e3,2} = \frac{5x5}{10} = 2.5$$

Tabla 19-4: Frecuencia de valores esperados

Riesgos	**Frecuencias**		**Total**
	Antes	**Después**	
Alto	2	2	4
Medio	0.5	0.5	1
Bajo	2.5	2.5	5
Total	**5**	**5**	**10**

Fuente: Encuestas aplicas a Empresas y Evaluación del Firewall PfSense

Realizado por: Edison Ruiz

Con las tablas de valores observados y valores esperados calculamos el valor de Chi Cuadrado X^2 con la siguiente ecuación:

$$\boldsymbol{X^2 calculado} = \sum_{i=1}^{r}\sum_{j=1}^{k} \frac{\left(f_{o_{ij}} - f_{e_{ij}}\right)^2}{f_{e_{ij}}}$$

Dónde:

$\boldsymbol{f_{o_{ij}}}$**:** son las frecuencias observados y número de riesgos observados en la fila i columna j

$\boldsymbol{f_{e_{ij}}}$**:** son las frecuencias esperadas y número de riesgos esperados correspondientes a cada fila i columna j

$$\boldsymbol{X^2 calculado} = \frac{\left(\boldsymbol{f_{o_{11}}} - \boldsymbol{f_{e_{11}}}\right)^2}{\boldsymbol{f_{e_{11}}}} + \frac{\left(\boldsymbol{f_{o_{22}}} - \boldsymbol{f_{e_{22}}}\right)^2}{\boldsymbol{f_{e_{22}}}} + \cdots + \frac{\left(\boldsymbol{f_{o_{rk}}} - \boldsymbol{f_{e_{rk}}}\right)^2}{\boldsymbol{f_{e_{rk}}}}$$

$$X^2 calculado = \frac{(4-2)^2}{2} + \frac{(0-2)^2}{2} + \frac{(1-0.5)^2}{0.5} + \frac{(0-0.5)^2}{0.5} + \frac{(0-2.5)^2}{2.5} + \frac{(5-2.5)^2}{2.5}$$

$$X^2 calculado = 2 + 2 + 0.5 + 0.5 + 2.5 + 2.5$$

$$\boldsymbol{X^2 calculado = 10}$$

Encontramos los grados de libertad (n) utilizando la fórmula:

$$\boldsymbol{n = (número\ de\ filas - 1)x(número\ de\ columnas - 1)}$$

Para el caso tenemos una matriz de 2x3

$$\boldsymbol{n = (2-1)x(3-1)}$$

$$\boldsymbol{n = 2\ grados\ de\ libertad}$$

Para poder demostrar la hipótesis tomamos el valor del 5% como nivel de significancia o el error que se puede cometer al rechazar o aceptar la H_0 y H_1, debemos observar en la tabla para verificar el valor y compara con el resultado de X^2 calculado.

El valor encontrado en la tabla (ANEXO A.) de valores para Chi Cuadrado con 2 grados de libertad y un nivel de significancia de 0.05 es **X^2tabla=5.991**.

4.7.1. Criterio de decisión

Los resultados obtenidos X^2 calculado y X^2 tabla deben ser comparados tomando en cuenta las siguientes condiciones:

Se acepta H_0 cuando X^2 calculado <= X^2 tabla, de no ser el caso de rechaza la H_0 y se acepta H_1

Valor de X^2 calculado de la investigación = 10

Valor de X^2 tabla = 5.991

Valorando el criterio de discusión obtenemos:

$$X^2 calculado = 10 > X^2 tabla = 5.991$$

Al no cumplirse la condición podemos rechazar la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1)

Queda demostrado que:

H_1:" La evaluación del firewall de frontera free PfSense si mejorara la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada en Riobamba."

La comprobación de la hipótesis por el método del X^2 permite afirmar que el uso del Firewall PfSense mejorar la confidencialidad, integridad y disponibilidad de la información de las Compañías de Responsabilidad Limitada de la ciudad de Riobamba mitigando la posibilidad de ataques y daños de la información que manejan dentro de su red LAN interna.

CAPÍTULO V

5. PROPUESTA;

Las Empresas de Responsabilidad Limitada de la Ciudad de Riobamba cuentan con un capital de inicio de actividades de 400 dólares americanos para el inicio de sus actividades, al ser un capital mínimo no consideran la seguridad informática como una necesidad y los altos costos de implementación de módulos de prevención limitan el uso de estos.

Al contar con una alternativa de software libre como el firewall PfSense sin costo de uso y que permite tener varios módulos de protección funcionando en un computador de bajas prestaciones como se detalla en el capítulo anterior las Empresas de Responsabilidad Limitada de la Ciudad de Riobamba podrá contar con está seguridad dentro de su red interna LAN

5.1. Instalación del Firewall PfSense.

Para la instalación se deben seguir los pasos especificados en la página de descarga del producto

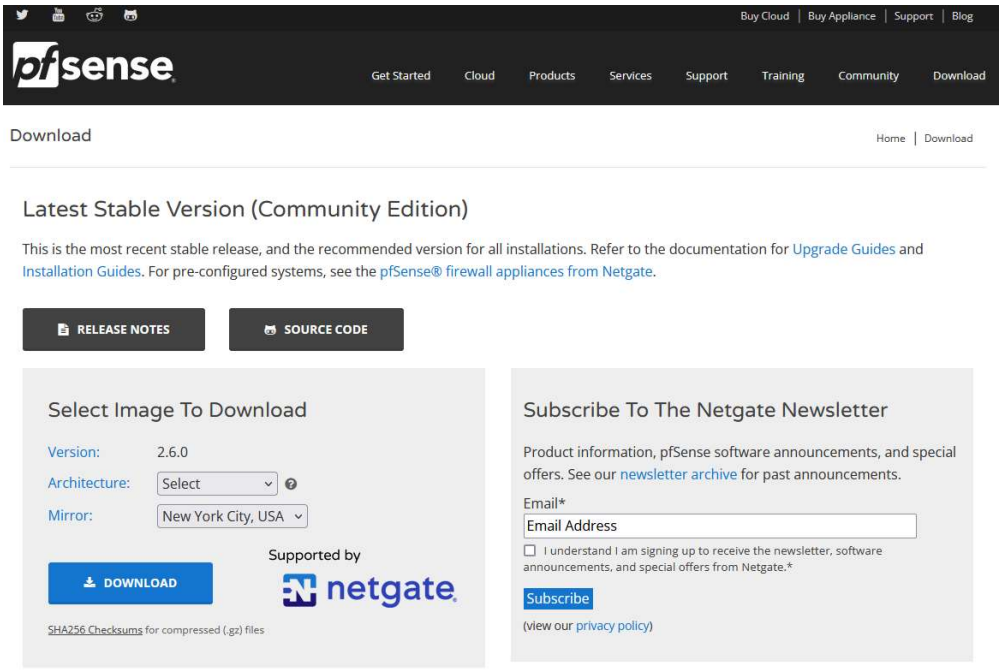


Figura 5-5. Página de descarga de PfSense
Fuente: www.pfsense.org

La última versión disponible para la descarga es 2.6.0 se debe seleccionar la arquitectura, como se va a trabajar en un computador reciclado para hacer las pruebas se seleccionó la arquitectura AMD64(64-bits), tipo de instalador USB Memstick Installer, Console VGA, Mirror New York City, USA, se creó una USB Booteable con el programa Rufus 2.6.818

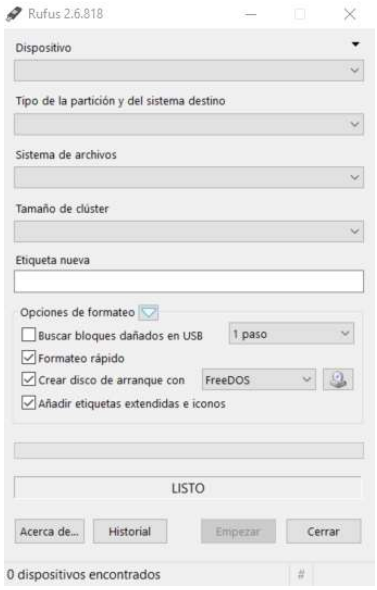


Figura 6-5. Programa Rufus 2.6.818
Fuente: Rufus.ie/es

Iniciamos el computador desde la unidad USB creada, al cargar el sistema nos encontramos con una pantalla de bienvenida de PfSense con un menú donde seleccionaremos la opción 1 y comenzará a aparecer las ventanas de configuración del software.

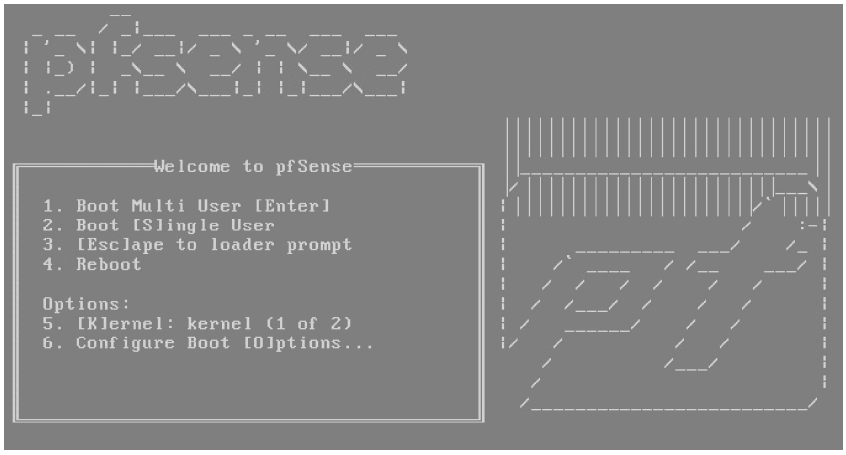


Figura 7-5. Pantalla de Bienvenida
Fuente: Autor

En las siguientes ventanas de configuración se debe seleccionar el idioma, tipo de partición dependiendo del tipo de computador puede ser UEFI o UFS, verificar está característica en la BIOS del equipo para evitar errores en el primer arranque del Firewall PfSense, al final configuraremos las VLans y las direcciones IP y mascara de red para cada una de las interfaces WAN y LAN.

Para ingresar al panel de control del Firewall PfSense lo hacemos desde un navegador web y escribimos la dirección de IP de la red LAN, el nombre usuario es **admin** y la contraseña por defecto es **pfsense** que deberá ser cambiada para evitar intromisión de personas no autorizadas al panel de control.

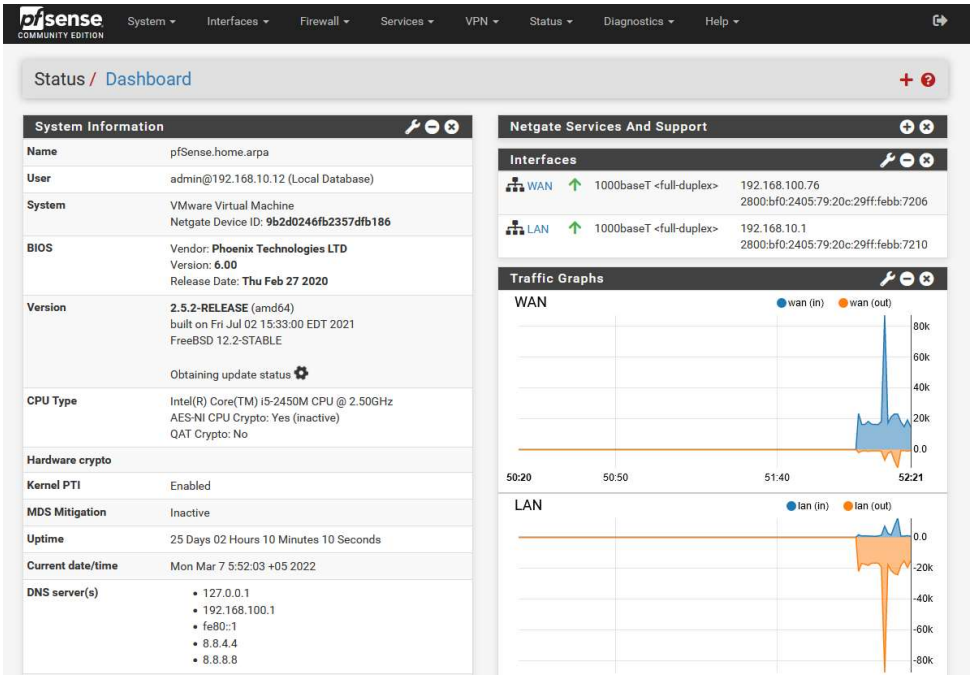


Figura 8-5. Panel de Control o Dashboard del PfSense
Fuente: Autor

5.2. Configuración de los módulos de seguridad.

Los módulos de protección deben ser configurados de acuerdo a los manuales de uso de Netgate Doc que se puede descargar de su página oficial, los complementos deben estar parametrizados de manera correcta o de lo contrario no funcionaran.

5.2.1. Manejo de puertos, reglas del Firewall

Las reglas que implementamos en el Firewall permitirán dividir o segmentar de manera correcta la red interna de las Compañías CIA LTDA al permitir o denegar el tráfico de los diferentes puertos de comunicación de las diferentes interfaces de comunicación tanto de la LAN como de la WAN, en el

apartado **Firewall/Rules** tenemos diferentes pestañas para la configuración, en este caso se tomará en cuenta tres interfaces, WAN, LAN y DMZ.

El Firewall después de iniciar su funcionamiento bloquea automáticamente todos los puertos de comunicación como protección, por esa razón no se podrá acceder al panel de control por la red WAN, los usuarios que externos a la red que quieran ingresar de manera no autorizada no lograran acceder teniendo así un nivel de protección.

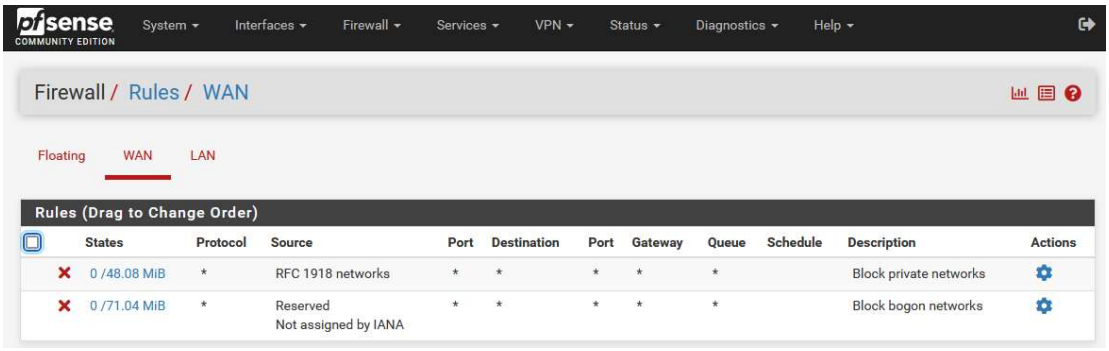


Figura 9-5. Reglas de la red WAN del PfSense
Fuente: Autor

La red LAN tiene reglas predefinidas que ayudan a no bloquearnos a nosotros mismo para poder acceder a las configuraciones del Panel de Control, tenemos permiso para ingresar desde cualquier equipo que este dentro de la red LAN con IPV4 o IPV6, se debe tomar en cuenta que las reglas se verifican de arriba hacia abajo por esa razón si en la parte superior bloqueamos todo nos quedamos sin conexión.

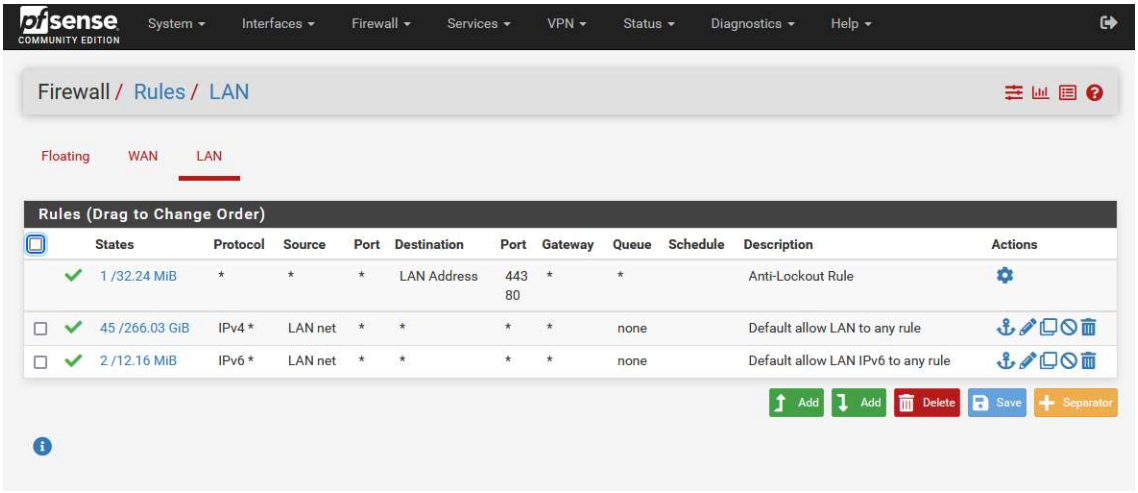


Figura 10-5. Reglas de la Red LAN del PfSense
Fuente: Autor

- **Manejo de Aliases**

Los Aliases nos ayudan a agrupar un conjunto de direcciones IP y Puertos de comunicación lo que facilita el bloquear varias direcciones IP con una misma regla sin necesidad de crear reglas para cada uno de los equipos que tenemos dentro de la red LAN, en el apartado Firewall / Aliases podemos añadir varias direcciones IP y Puertos, en la sección URL podemos direccionar a un archivo de texto para descarga de manera rápida cientos de direcciones IP, Puertos y Redes dentro del PfSense.

Figura 11-5. Manejo de Aliases en PfSense
Fuente: Autor

Creado el Aliases nos dirigimos a la sección Firewall y podemos cargarla en origen y/o destino, así los reconocerá de manera automática y se listará los Aliases que inicien con la misma letra, y si vamos a configurar puertos de comunicación nos dirigimos a la sección de puertos de origen y/o destino y de igual manera los reconocerá.

Por seguridad de la red interna se cerrarán todos los puertos de comunicación a excepción del 80, 8080 y 443 que se necesitan para acceder a páginas web HTTP y HTTPS para verificar el estado de los puertos se realizó un escaneo con Nmap de Kali Linux dando un resultado favorable

Figura 12-5. Escaneo de Puertos al PfSense con Nmap
Fuente: Autor

5.2.2. Control de acceso a usuarios

En PfSense podemos implementar tres formas de validar usuarios dentro de la red interna LAN, los mismos serán puestos a prueba para verificar su funcionamiento dentro de un entorno controlado, cada uno de ellos puede ser implementado de acuerdo con las necesidades.

- **Squid Proxy**

Nos ayuda a controlar el ancho de banda para que el servicio de internet no se sature dentro de la empresa tomando en cuenta el incremento de aplicaciones web, video llamadas, telefonía IP y otros recursos que consumen internet dentro de la LAN, está aplicación es la más utilizada puede funcionar de manera independiente dentro de un sistema operativo o en este caso bajo el PfSense.

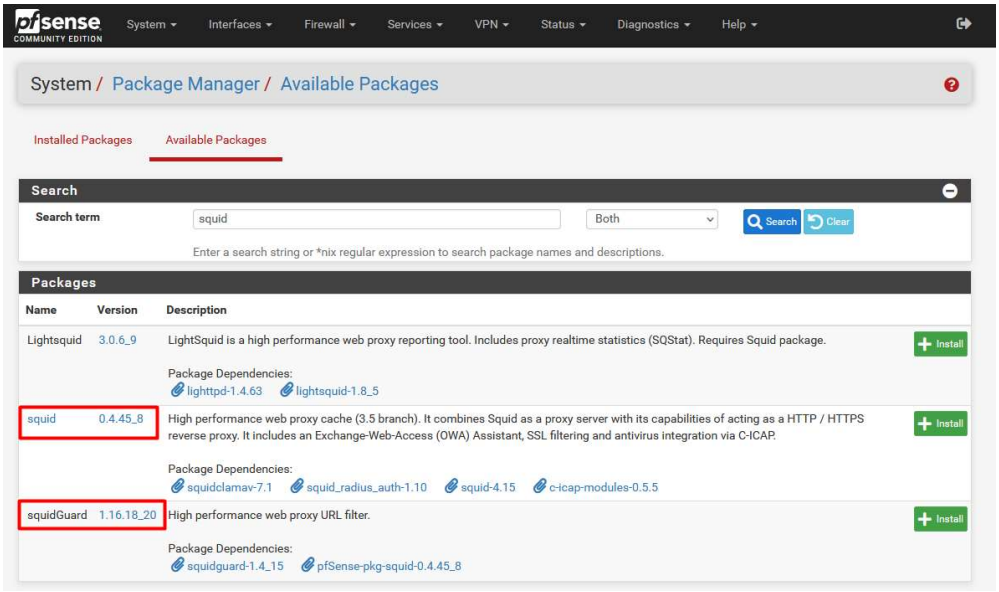


Figura 13-5. Instalación del paquete Squid y Squid Guard en PfSense
Fuente: Autor

Para obtener el paquete nos dirigimos a System / Package / Available Packages e instalamos los paquetes Squid y SquidGuard como se muestra en la figura 24, después de la instalación comenzamos la configuración del recurso tomando en cuenta que las configuraciones por defecto son las optimas para el funcionamiento, al final levantamos el servicio, podemos verificar que se encuentra corriendo en la sección Status / Services del panel de control

Figura 14-5. Squid Proxy Server Service Running en PfSense
Fuente: Autor

De esta manera se tiene un control de acceso a los recursos de cada usuario que se encuentra dentro de la red LAN, se puede restringir el acceso a diferentes tipos de páginas web como, por ejemplo: redes sociales, juegos, pornografía, y otros. Así se tendrá menor consumo de los recursos y menor riesgo de acceder a contenido web con virus evitando daños en equipos de cómputo.

Figura 15-5. Prueba de Squid Proxy en PfSense
Fuente: Autor

Se configuró Squid Proxy de modo transparente para evitar configuraciones adicionales en cada uno de los terminales que se tendrán dentro de la Compañía CIA LTDA y se bloqueó la página web www.youtube.com, como se muestra en la figura 26 impide el acceso y nos presenta un mensaje de Acceso Denegado, se comprueba el correcto funcionamiento de la aplicación.

- **Portal Cautivo**

El portal cautivo vigila el tráfico HTTP y hace que los usuarios de la red LAN pasen por una validación de credenciales nombre de usuario y contraseña para tener salida al internet desde su terminal, se puede controlar el tiempo de uso y ancho de banda, este servicio puede ser implementado en aeropuertos, centros de negocios, hoteles, proveedores de internet inalámbrico y para el caso de estudio en pequeñas y mediana empresas.

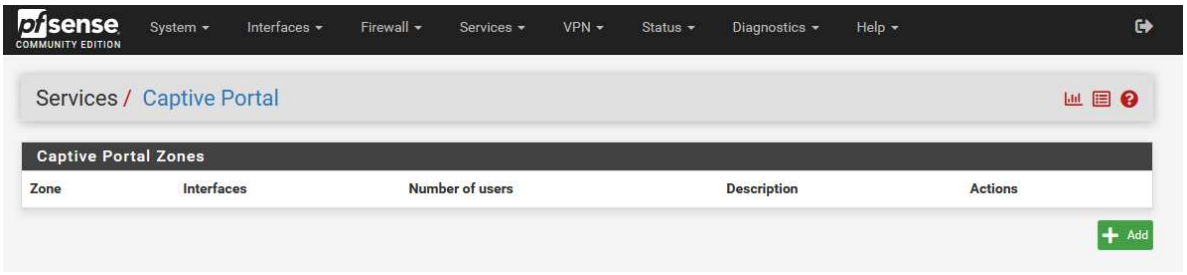


Figura 16-5. Servicio de Portal Cautivo del PfSense
Fuente: Autor

Configuramos el portal cautivo tomando en cuenta que esto se va a aplicar a la red LAN a la cual se van a conectar todos los usuarios de red, una de las ventajas es que no necesitamos generar una página de validación el PfSense nos da una plantilla que podemos utilizar para el ingreso de credenciales del usuario que desea tener acceso a los recursos de la red.

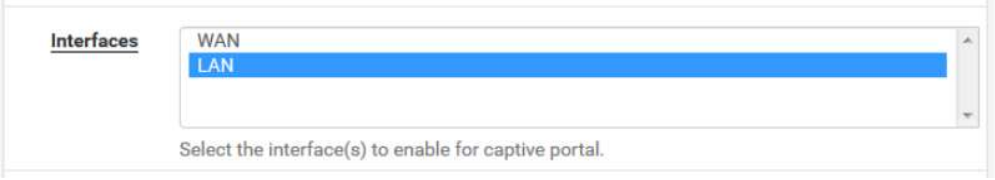


Figura 17-5. Interfaces para aplicar la validación con Portal Cautivo
Fuente: Autor

Para finalizar la configuración debemos agregar los usuarios de la red LAN y agregarles a un grupo de usuarios donde se limitará el ancho de bando y uso del internet. Se realizaron las pruebas de validación y visualizó la plantilla predeterminada del PfSense para ingresar las credenciales de validación.

Figura 18-5. Pantalla de validación predefinida del PfSense
Fuente: Autor

Al completar la validación tenemos acceso a internet dentro de la red LAN, funciona de manera correcta, todos los usuarios registrados tienen disponible el recurso.

- **Free Radius**

Radius frecuentemente usan diferentes protocolos de autenticación PAP, CHAP Y EAP. Una de las características es permitir controlar sesiones donde se registra el comienzo y final de la validación esto sería lo más importante, también se tiene otros parámetros, es de libre utilización y se encuentra disponible el paquete para PfSense y dispone de una interfaz gráfica para su configuración sin necesidad de modificar archivos de texto.

Figura 19-5. Esquema de funcionamiento de un servidor RADIUS
Fuente: Redes Zone, 2021

Los usuarios se conectarán directamente al AP, la principal ventaja de tener Free Radius es el evitar que los posibles atacantes suplante la identidad del AP y evita que los usuarios de red envíen credenciales al tener un usuario, contraseña para la validación y tener un certificado CA para verificar que la red WiFi a la que nos estamos conectando es legítima.

Al igual que los otros paquetes primero lo debemos instalar desde System / Package Manager / Available Packages, lo encontramos con el nombre de freeradius3 la versión a instalar y probar será 0.15.7_33 que soporta MySQL, PostgreSQL, LDAP, Kerberos como base de datos de información.

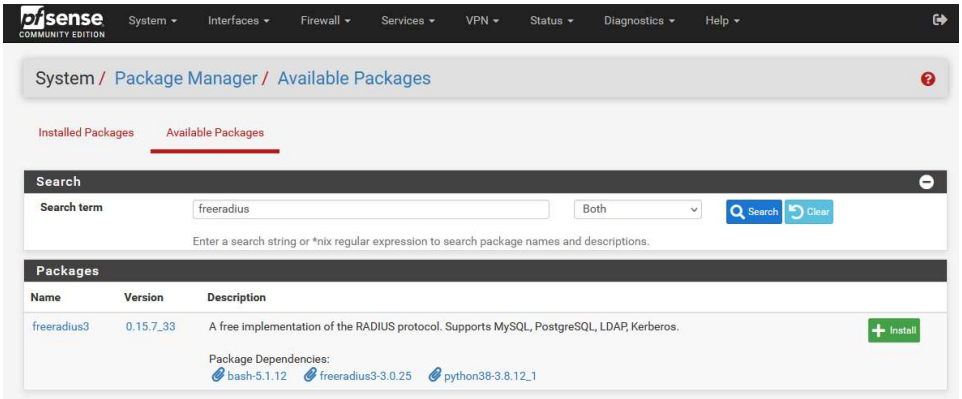


Figura 20-5. Instalación de freeradius3 en PfSense
Fuente: Autor

Al configurar Free Radius en la sección de servicios del PfSense mediante la interfaz gráfica encontraremos varios parámetros a tomar en cuenta para su correcto funcionamiento dependiendo de lo que se dispone dentro de la red LAN, estos elementos se detallan a continuación:

Users: Se define el nombre de usuario y contraseña que se a utilizar para la validación e ingreso a través de WiFi y otros parámetros avanzados.

MACs: Se establece el funcionamiento de Radius al encontrar una MAC específica proporcionara la misma dirección IP, VLAN, limita el ancho de banda, tiempo de uso del recurso y otras configuraciones.

Interfaces: Se detalla la interfaz física y lógica donde escuchará el servidor Radius y los puertos de escucha del protocolo UDP.

Settings: Se tiene configuraciones globales del servidor e incluye el registro de usuarios.

EAP: Parámetros globales del protocolo EAP

SQL y LDAP: Configuraciones para integrar base de datos.

Figura 21-5. Panel de configuración de Free Radius de PfSense
Fuente: Autor

5.2.3. Acceso a usuarios externos

Este tipo de accesos son utilizados cuando la empresa tiene servidores web, SMTP, DNS y otros a los cuales deben ingresar personas externas a la institución, por está razón se debe separar las redes para que no exista vulnerabilidades que puedan aprovechar los atacantes.

- **DMZ**

Una Zona Desmilitarizada se utiliza para acceso a servicios públicos protegiendo la red interna, es considerada una red menos segura, cumple el objetivo de aislar las redes cada una será independiente de la otra, pero bajo la supervisión del PfSense.

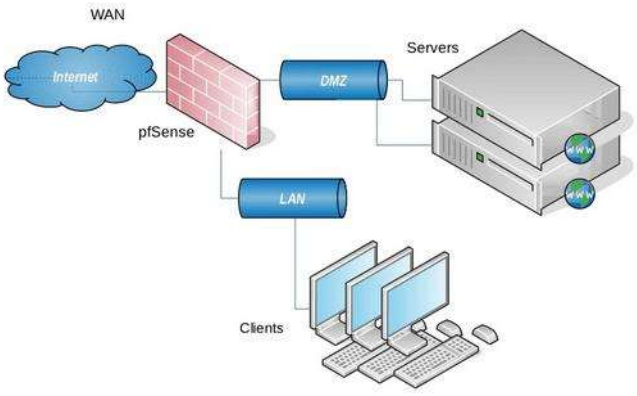


Figura 22-5. Diagrama de la DMZ
Fuente: Rubicon Communications LLC (Netgate), 2022

Se debe agregar una interfaz nueva en el apartado Interfaces / Interface Assignments dentro del panel de control, se debe tomar en cuenta que el computador donde se encuentra instalado el PfSense deberá tener otra tarjeta de

red adicional para manejar está interfaz, por defecto se crea con el nombre de OPT1 a la cual debemos cambiar el nombre a DMZ.

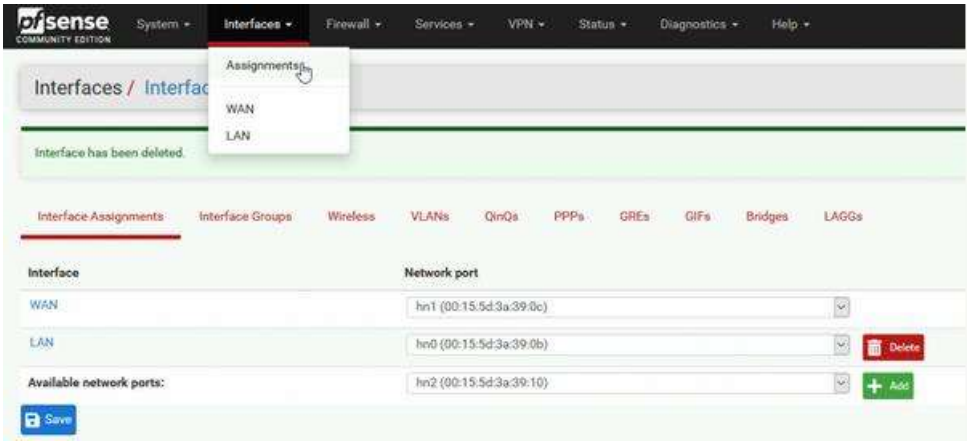


Figura 23-5. Adición de una nueva interfaz
Fuente: Autor

Al igual que las otras interfaces que maneja el PfSense deberemos establecer reglas para poder tener comunicación con el exterior es decir que los usuarios externos tengan la posibilidad de acceder a los servidores web, correo u otros que disponga la Compañía.

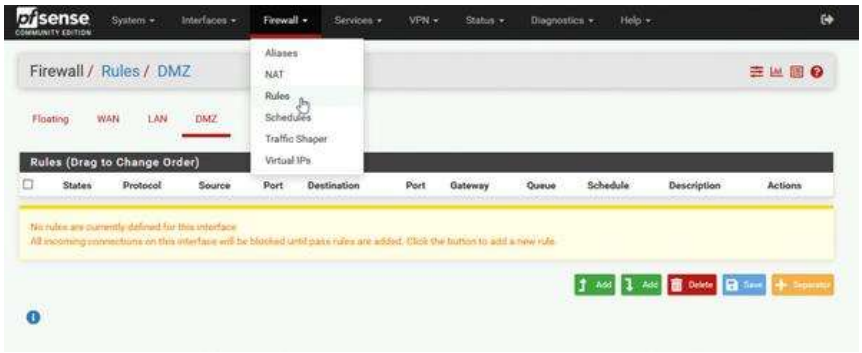


Figura 24-5. Asignación de reglas a la DMZ
Fuente: Autor

La red LAN no tiene restricciones para acceder a la DMZ donde se encuentran los servidores, pero desde la DMZ a la LAN no se puede acceder por seguridad tomando en cuenta que los usuarios externos van a estar navegando por los servidores que tiene la empresa.

5.2.4. Sistema de prevención y detección de intrusos IPS / IDS

Pfsense a más de disponer de un potente Firewall que disminuye o bloquea los ataques DoS y DDoS posee dos paquetes que ayudan a la prevención y detección de intrusos como el Snort y Suricata, los mismo que podremos instalar desde Package Manager del panel de control.

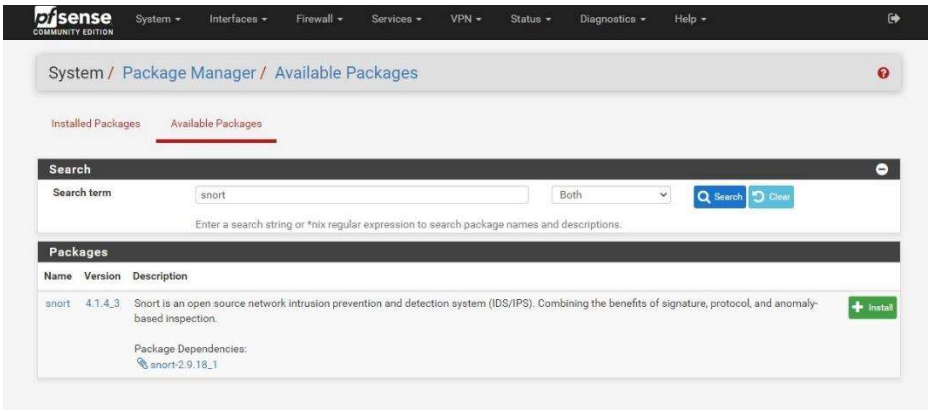


Figura 25-5. Instalación del Paquete Snort 4.1.5_1
Fuente: Autor

Las pruebas se realizaron con el paquete Snort al igual que los demás aplicativos o complementos del PfSense es gratuita, para que funcione debemos registrarnos en la página www.snort.org, debemos crear una cuenta para tener acceso a las reglas para filtrar los paquetes, muy importante generar el Oinkcode necesario para configurar el paquete.

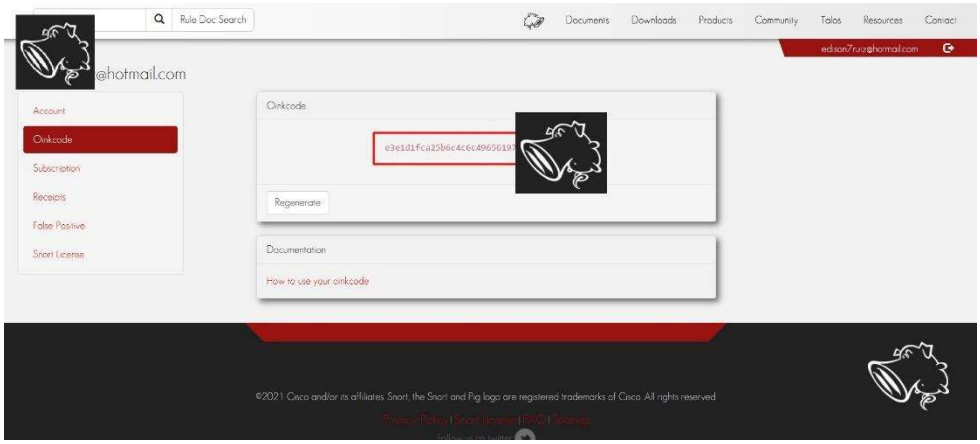


Figura 26-5. Oinkcode de Snort
Fuente: Autor

Para cada una de las direcciones IP que pasan por el Firewall genera un código único para identificarlo GID:SID, con ese código podemos generar reglas de bloque para que no exista trafico para esas direcciones, antes de poner a trabajar el Snort debemos tener claro los paquetes que se van a bloquear y habilitar lo necesario para trabajar, por defecto cierra todo lo que se encuentra en las reglas.

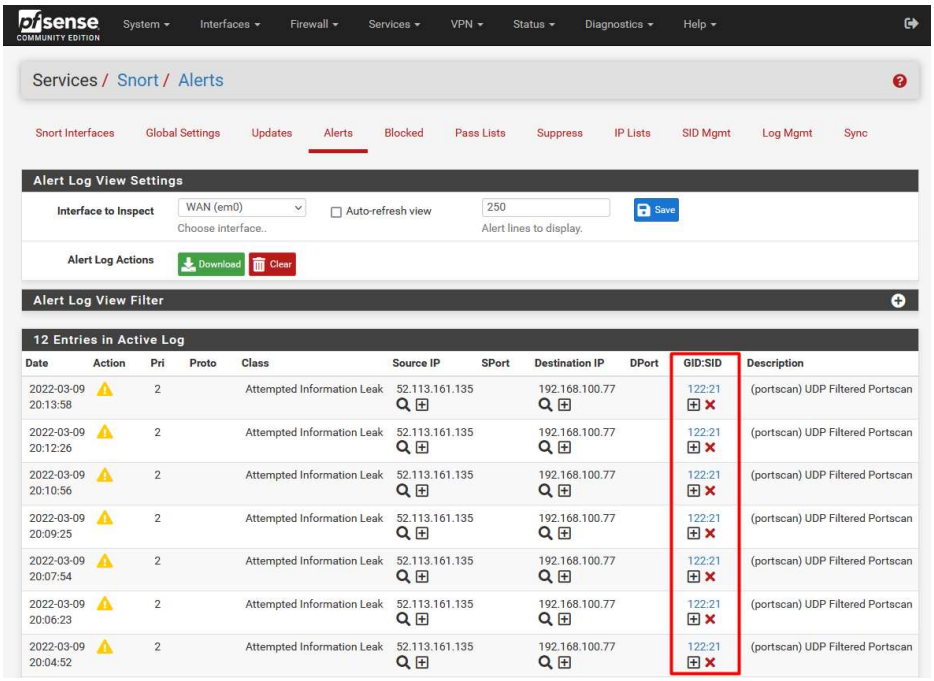


Figura 27-5. Alertas del Snort
Fuente: Autor

Snort puede funcionar en todas las interfaces que tiene configurado el PfSense, para cada una podemos establecer reglas diferentes para controlar el flujo de paquetes. Si queremos utilizar reglas Snort OpenAppID la descargamos de su página oficial al ser de acceso libre las actualizaciones se general entre 15 a 20 días después de salidas las de pago.

5.2.5. VLANs

La red Virtual LAN o VLANs tiene la función de separar el tráfico de diferentes redes aumentando la seguridad dentro de una red LAN, PfSense permite crear varias VLANs y cada una puede tener varios niveles de permisos, accesos a recursos, de está manera cada una de las áreas que tiene la Compañía puede tener su propia red virtual.

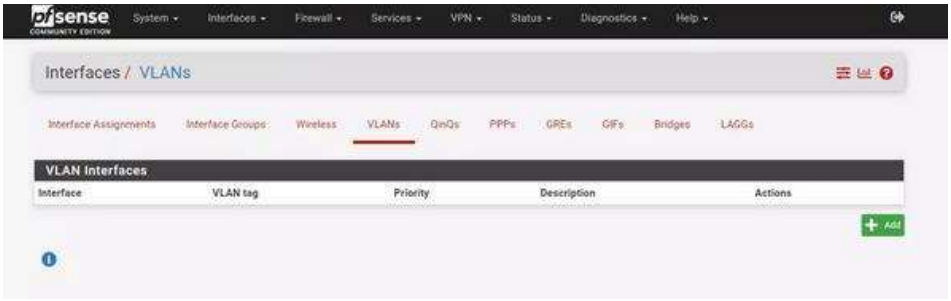


Figura 28-5. Adicionar una VLAN en PfSense
Fuente: Autor

Por defecto no tenemos ninguna VLAN creada, la VLAN1es para administración de la red LAN y podemos configurar cualquier de ellas y crear las necesarias para satisfacer las necesidades de la Compañía, para adicionar una debemos dar click en Add del panel de control.

Figura 29-5. Parámetros de configuración VLANs
Fuente: Autor

Los parámetros de configuración que debemos tomar en cuenta para una correcta configuración de las VLANs son:

- Parent Interface: Asignamos el puerto a la LAN
- VLAN Tag: Asignar el VLAN ID que corresponde al switch.
- VLAN Priority: Se puede dejar vacio.
- Description: Nombre de la VLAN.

Siempre se debe anclar todas las VLANS a la interfaz LAN, termina la adición se desplegarán todas con el nombre por defecto OPT1, OPT2, etc. Cada VLAN es independiente o invisible para las otras, de esta manera se aumenta la seguridad restringiendo el acceso de usuarios a otras áreas y recursos.

5.2.6. Antivirus ClamAV

Squid Proxy Server tiene un paquete ClamAV antivirus que ayuda con la detección de posibles amenazas antes de descargar archivos del internet, como los demás paquetes es de acceso gratuito y de fácil configuración, para activarlo nos dirigimos a Navigate to Services / Squid Proxy Server / Antivirus del panel de control.

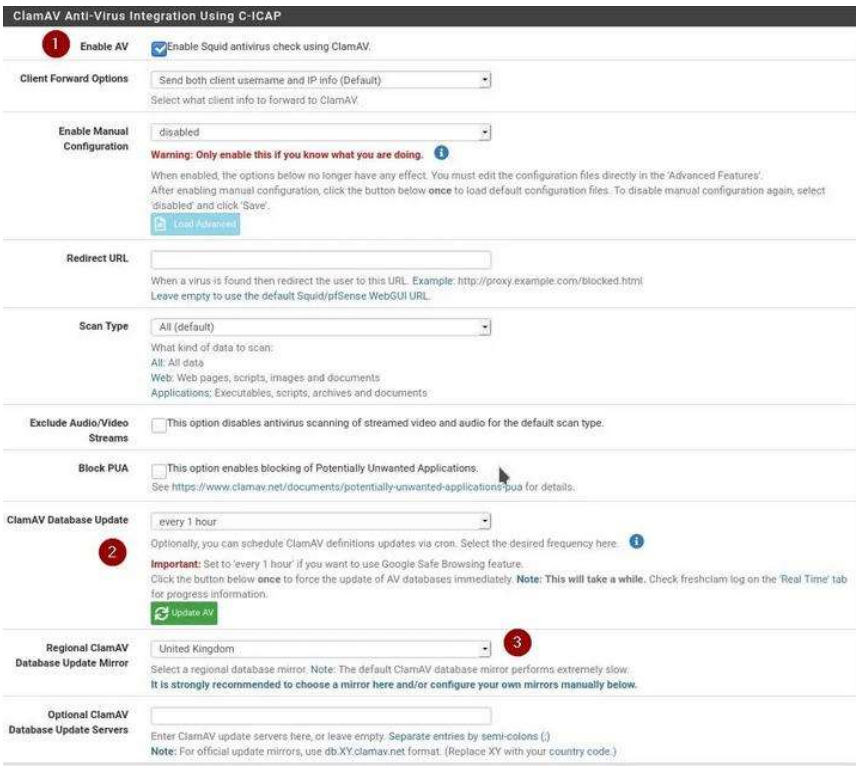


Figura 30-5. Activación de antivirus ClamAV
Fuente: Autor

Para que el antivirus funcione es necesario reiniciar el Firewall PfSense, debemos actualizar la base de datos del ClamAV, nos dirigimos a Services / Squid Proxy Server / Antivirus del panel de control, verificamos que el servicio c-icap este corriendo.

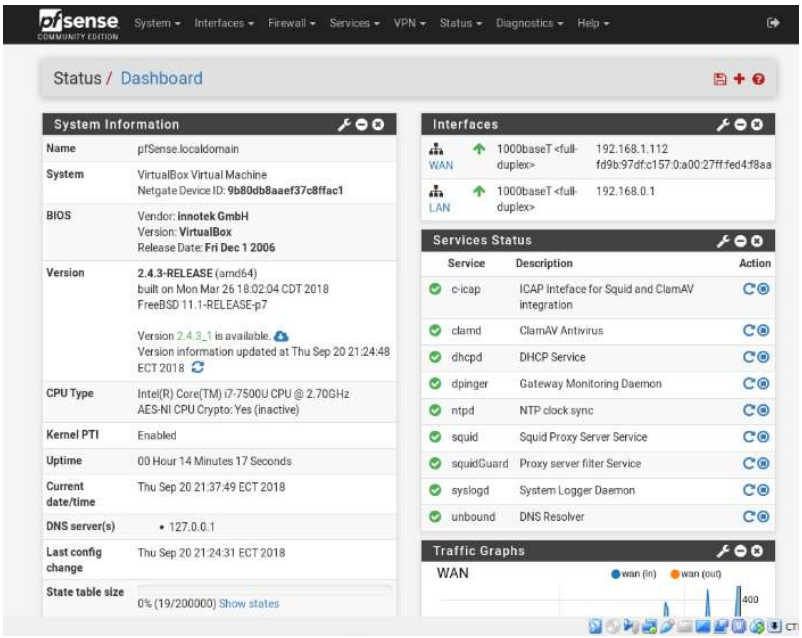


Figura 31-5. Servicio c-icap corriendo
Fuente: Autor

Para probar el funcionamiento del ClamAV antivrus ingresamos a la página https://www.eicar.org que tiene alojado archivos con diferentes extensiones infectados para probar la detección de virus, las pruebas se hicieron con malware en la URL encontramos los siguientes paquetes: eicar.com, eicar.com.txt, eicar.com.zip, eicarcom2.zip, se probó con todos, el resultado fue favorable, ClamAv detecto todos los archivos generando un bloqueo de descargar.

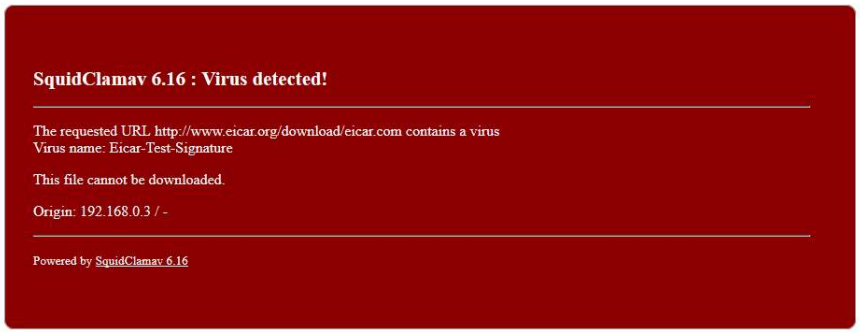


Figura. 32-5. Detección de ClamAV
Fuente. Autor

CONCLUSIONES

- Para el diagnostico de seguridad actual de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba se aplicaron 64 encuestas de un universo de 531 de acuerdo al registro de la Superintendencia de Compañías, como resultado se obtuvo que la mayoría de ellas no cuenta con un Firewall de protección o algún otro elemento de seguridad que proteja la red interna LAN, dejando total mente expuesta su información y equipos de cómputo al estar conectados directamente al ISP o proveedor de internet, se debe tomar en cuenta que este tipo de Empresas no superan los $400 como base de su constitución, debido a eso el licenciamiento de este tipo de seguridad es inaccesible.
- El diseño de la infraestructura de red LAN es simple pero cumple con la función de ubicar el Firewall PfSense después del router de internet entregado por el ISP o proveedor de internet, la nueva infraestructura de red divide cada una de las zonas que se tienen dentro de la Compañías de Responsabilidad Limitada de la Ciudad de Riobamba, están definidas las áreas de la LAN en la cual se conectaran todos los usuarios y tendrán acceso al internet después de una validación contra el Proxy y la DMZ donde se podrán conectar todos los usuarios externos e internos de la red, pero los usuarios externos no podrán acceder a la red interna.
- La virtualización se realizó con el software VMWare dentro del cual se crearon varios equipos para ejecutar las pruebas, dentro de la red interna el Sistema Operativo Ubuntu Linux para descargar archivos infectados, con Sistema Operativo Kali Linux se hicieron las pruebas de vulnerabilidades, al igual con el software NESSUS y web EICAR Test para la descarga de archivos infectados, todas estas pruebas fueron ejecutadas para verificar las vulnerabilidades del Firewall PfSense, se logró recopilar la información necesaria para los cálculos de comprobación de hipótesis.
- Al evaluar los resultados obtenidos de la encesta podemos verificar que la mayoría de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba no cuenta con un Firewall o módulos de seguridad dentro de su red LAN, por lo tanto, el Riesgo de sufrir un ataque es Alto. La evaluación del PfSense demostró que se puede disminuir el Riesgo de sufrir ataques dentro de la red LAN, todos los módulos de seguridad que ofrece este software pueden convivir sin ningún problema. Aplicado Chi-Cuadrado se pudo demostrar la hipótesis alternativa H1 con un nivel de significancia del 5%.

RECOMENDACIONES

- Debemos tomar en cuenta que el mismo resultado se puede esperar en la Pymes y los Hogares, se encuentran totalmente expuestos a potenciales Riesgos por esta razón se debería considerar el utilizar este tipo de Firewall para proteger la red interna y disminuir la probabilidad de ataque y daños en la información.
- Utilizar el diseño de red LAN para tener una mejor distribución de los equipos, el esquema es sencillo, pero cumple con su función, a futuro en las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba también se podría implementar el uso de VLANs para fortalecer aún más la seguridad de la información.
- Para correr las pruebas se debería utilizar software libre, con esto se facilita el uso de licencias, las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba al usar software libre podrían mejorar su nivel de seguridad debido a que en el internet se encuentran más cantidad de virus para el sistema operativo Linux, esto se deberá evaluar de acuerdo con el Negocio de cada una de ellas.
- El uso de este tipo de software mejora significativamente el nivel de seguridad de seguridad de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba, también se lo podría aplicar a las Pymes, Micro Pymes y dentro de los hogares, se debe tomar en cuenta que PfSense no es la único Firewall de licencia libre.

GLOSARIO

Autenticación: Es el proceso de verificación de la identidad o localización de un usuario, servicio o aplicación. La autenticación se realiza utilizando al menos uno de tres mecanismos: "algo que tienes", "algo que sé "o" algo que es". La aplicación puede autenticar y proporcionar diferentes servicios basados en la ubicación, método de acceso, el tiempo de permanencia y los hábitos de uso de la aplicación web.

Autorización: La determinación de los recursos que un usuario, un servicio o aplicación tienen como permisos de acceso. Recursos accesibles que pueden ser URL, archivos, directorios, bases de datos, servlets, caminos de ejecución.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Configuración del sistema: Conjunto de controles que ayuda a asegurar que los componentes de infraestructura que brindan soporte al software fueron desplegados de manera segura.

Control de Acceso: Un conjunto de controles que permiten o niegan el acceso a un recurso de un usuario o entidad dado.

Escáner de vulnerabilidades: Aplicación que permite comprobar si un sistema es vulnerable a un conjunto de deficiencias de seguridad.

Escáner de vulnerabilidades: Aplicación que permite comprobar si un sistema es vulnerable a un conjunto de deficiencias de seguridad.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Gestión de Archivos: Conjunto de controles que cubren la interacción entre el código y otro sistema de archivos.

Impacto: Medida del efecto negativo en el negocio que resulta de la ocurrencia de un evento indeseado; pudiendo ser el resultado la explotación de una vulnerabilidad.

Integridad: los datos reflejen la realidad y que correspondan con lo que debe ser y no ha sido modificadas indebidamente.

Mitigar: Pasos tomados para reducir la severidad de una vulnerabilidad. Estos pueden incluir remover una vulnerabilidad, hacer una vulnerabilidad más difícil de explotar, o reducir el impacto negativo de una explotación exitosa.

NMAP: Programa de código abierto que abierto que sirve para efectuar rastreo de puertos TCP y UDP. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Protección de datos: Conjunto de controles que ayudan a asegurar que el software maneja de forma segura el almacenamiento de la información.

Requerimiento de Seguridad: Conjunto de requerimientos funcionales y de diseño que ayudan a asegurar que el software se construye y despliega de forma segura.

Sistema: Término genérico que cubre sistemas operativos, servidores web, frameworks de aplicaciones e infraestructura relacionada.

Validación de entrada: Conjunto de controles que verifican que las propiedades de los datos ingresados coinciden con las esperadas por la aplicación, incluyendo tipos, largos, rangos, conjuntos de caracteres aceptados excluyendo caracteres peligrosos conocidos.

Vulnerabilidad: Debilidad en un sistema que lo hace susceptible a ataque o daño.

BIBLIOGRAFÍA

[1]. ANDREW S. , T. (03 de 01 de 2009). redes-de-computadoras-tanenbaum-4ta-edicion-espanol. Obtenido de juliorestrepo.wordpress.: https://juliorestrepo.files.wordpress.com/2010/08/redes-decomputadoras-tanenbaum-4ta-edicion-espanol.pdf

[2]. Cisco - CCNA. (s.f.). Introducción a las redes. Obtenido de Tipos de vulnerabilidades: n https://staticcourse-assets.s3.amazonaws.com/ITN6/es/index.html#11.2.1.3.

[3]. Cisco. (s.f.). ¿Qué es un ataque DDoS? Obtenido de https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

[4]. Cisco. (s.f.). ¿Qué es un cortafuegos? Obtenido de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[5]. Claranet. (09 de 08 de 2012). Claranet. Obtenido de ¿Qué tipos de servidores hay?: https://www.claranet.es/about/news/que-tipos-de-servidores-hay.html

[6]. DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, S. L. (2016). ALICIA - Acceso libre a información Científica para la innovación. Obtenido de 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 Amazonía Peruana, Iquitos-2016.

[7]. FreeBSD. (13 de 11 de 2013). FreeBSD. Obtenido de Acerca de FreeBSD: https://www.freebsd.org/es/about.html

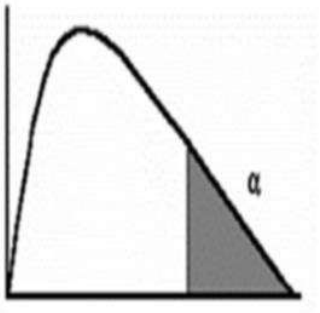
[8]. Guitierrez, F. (25 de Febrero de 2011). Modelado de amenazas. Obtenido de Amenazas: http://seguridadenlanube.blogspot.pe/2011/02/el-modelado-de-amenazas-de seguridades.html.

[9]. pfsense. (s.f.). Descripción general de pfSense. Obtenido de pfsense: https://www.pfsense.org/aboutpfsense/

[10]. Superintendencia de Compañías. (s.f.). Directorio de Compañías. Obtenido de Superintendencia de Compañías: https://www.supercias.gob.ec/portalscvs/

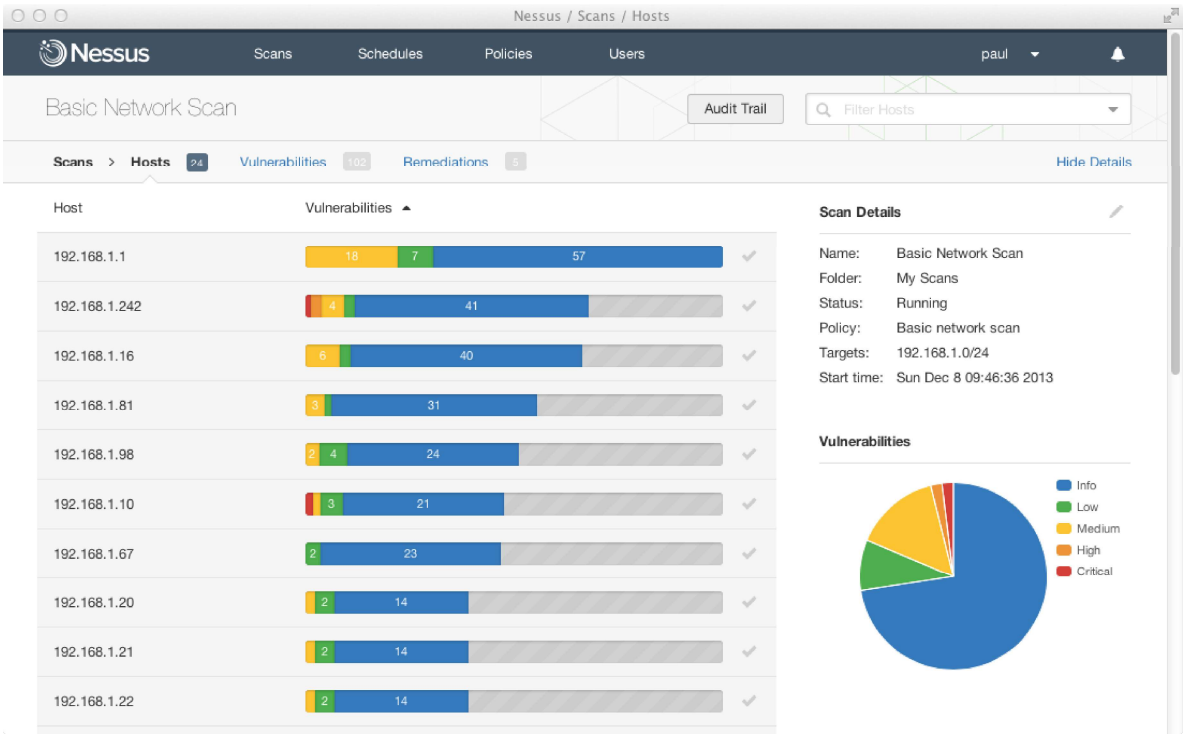
ANEXOS

ANEXO A. TABLA DE CHI-CUADRADO PARA VERIFICAR VALORES Y DEMOSTRAR HIPÓTESIS

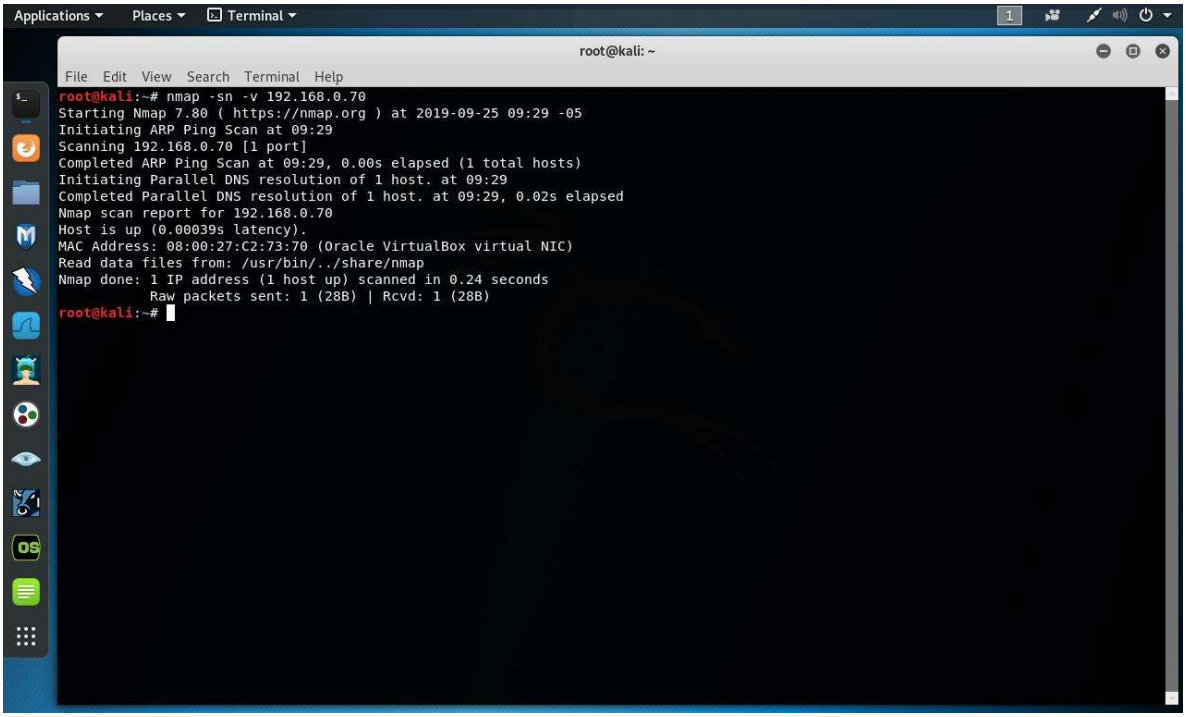


Grados de libertad	α=.995	α=.99	α=.975	α=.95	α=.90	α=.10	α=.05	α=.025	α=.01	α=.005
1	0.0000	0.0002	0.0010	0.0039	0.0158	2.7055	3.8415	5.0239	6.6349	7.8794
2	0.0100	0.0201	0.0506	0.1026	0.2107	4.6052	5.9915	7.3778	9.2103	10.597
3	0.0717	0.1148	0.2158	0.3518	0.5844	6.2514	7.8147	9.3484	11.345	12.838
4	0.2070	0.2971	0.4844	0.7107	1.0636	7.7794	9.4877	11.143	13.277	14.860
5	0.4117	0.5543	0.8312	1.1455	1.6103	9.2364	11.070	12.833	15.086	16.750
6	0.6757	0.8721	1.2373	1.6354	2.2041	10.645	12.592	14.449	16.812	18.548
7	0.9893	1.2390	1.6899	2.1673	2.8331	12.017	14.067	16.013	18.475	20.278
8	1.3444	1.6465	2.1797	2.7326	3.4895	13.362	15.507	17.535	20.090	21.955
9	1.7349	2.0879	2.7004	3.3251	4.1682	14.684	16.919	19.023	21.666	23.589

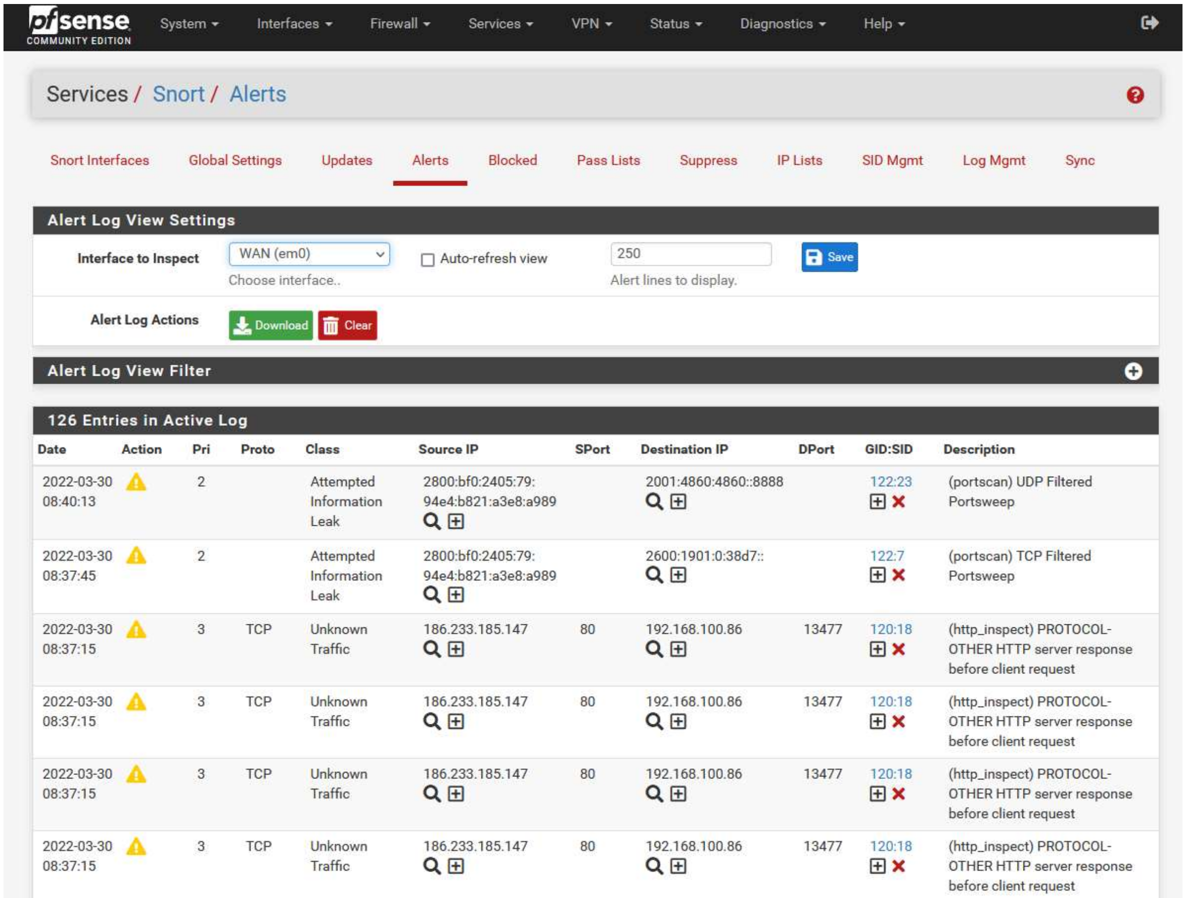
ANEXO B. HERRAMIENTA NESSUS



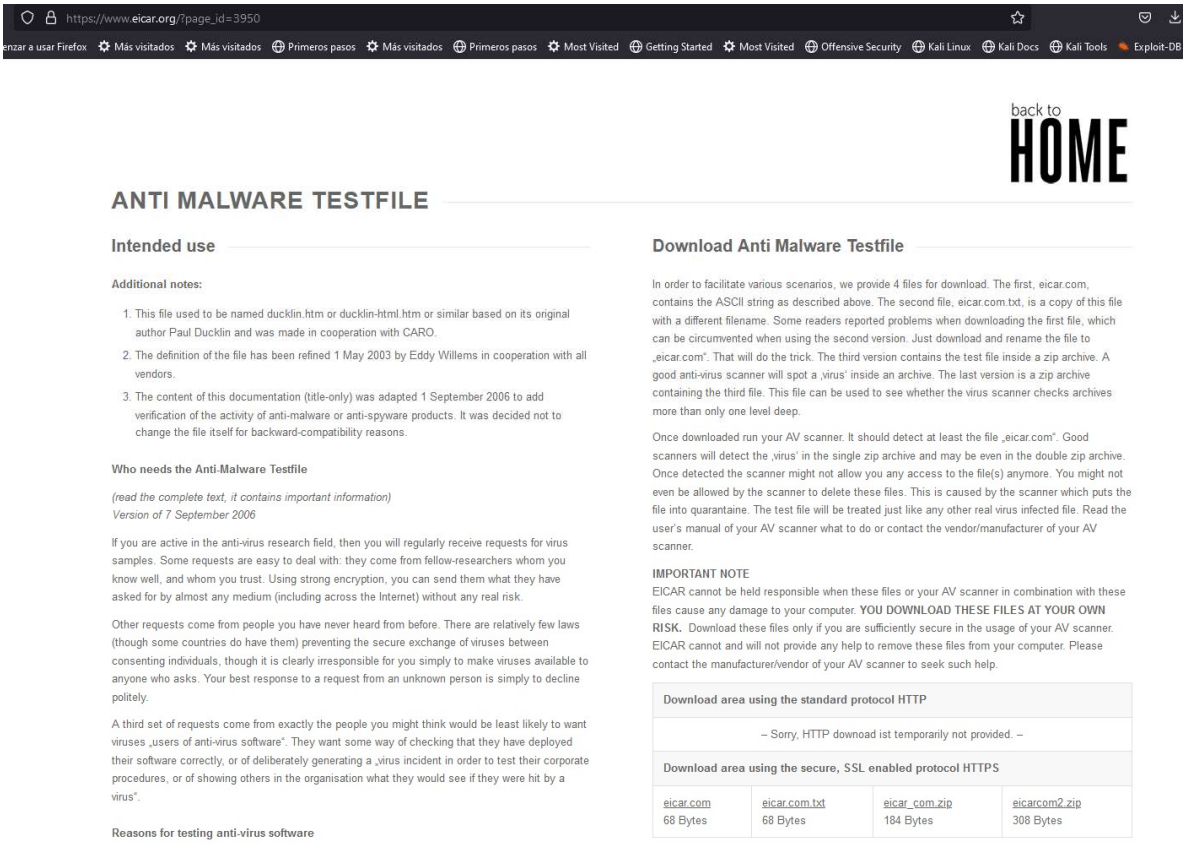
ANEXO C. HERRAMIENTA NMAP



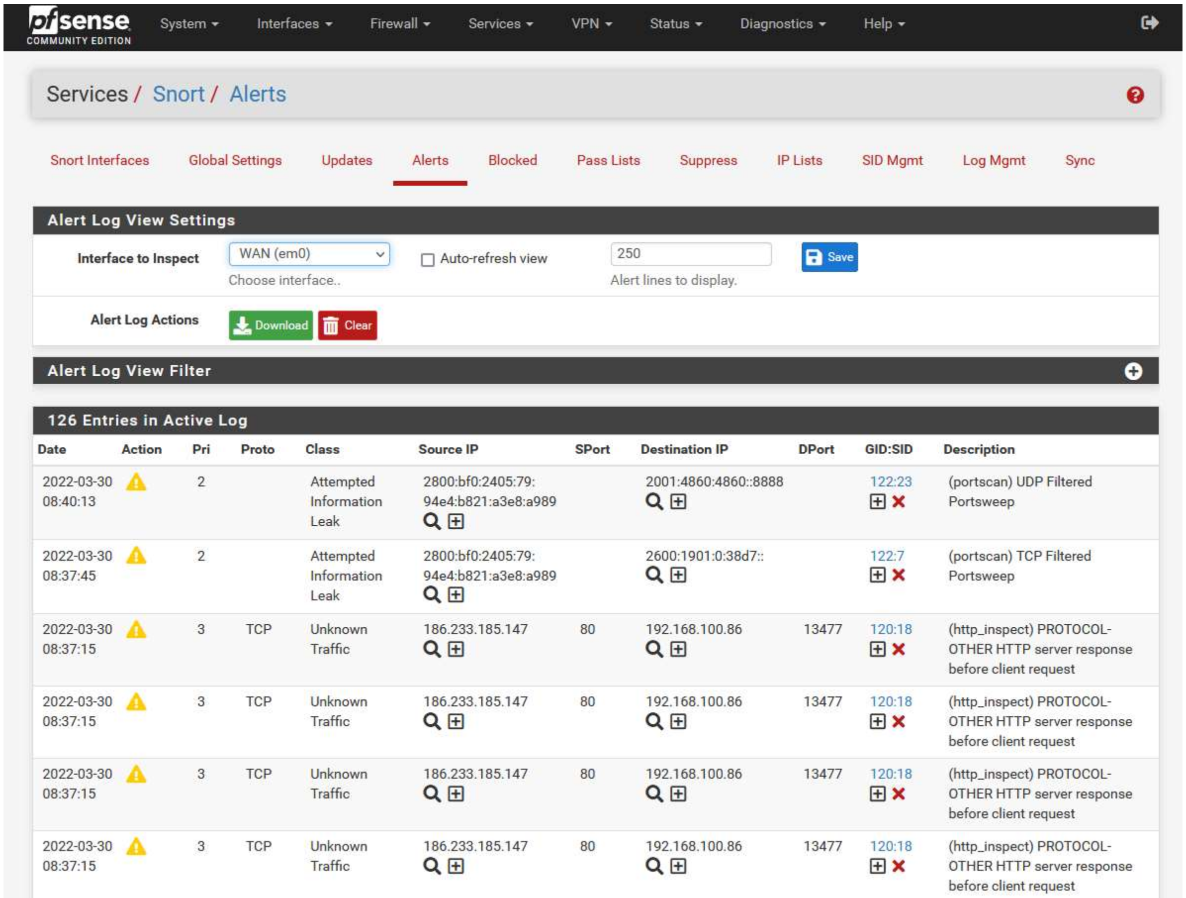
ANEXO D. ALERTAS DEL SNORT



ANEXO E. WEB EICAR TEST



ANEXO F. PÁGINA OFICIAL DEL SNORT



espoch | Dirección de Bibliotecas y Recursos del Aprendizaje

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 05 / 08 / 2022

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Edison Fernando Ruiz Andino*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Seguridad Telemática*
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

Firmado electrónicamente por:
LUIS ALBERTO CAMINOS VARGAS

UNIDAD DE PROCESOS TÉCNICOS DBRA ESPOCH

0083-DBRA-UPT-IPEC-2022

Re: Traducción del resumen de Tesis-Maestria

JORGE SANTIAGO SANTAMARIA SERRANO <santiago.santamaria@espoch.edu.ec>
29/7/2022 14:27

Para: Centro de Idiomas; Edison Fernando Ruiz Andino

ABSTRACT-signed.pdf
24,26 KB

God bless you. Wish you luck

De: Centro de Idiomas <idiomas@espoch.edu.ec>
Enviado: jueves, 28 de julio de 2022 04:11 p. m.
Para: JORGE SANTIAGO SANTAMARIA SERRANO <santiago.santamaria@espoch.edu.ec>
Asunto: RV: Traducción del resumen de Tesis-Maestria

Saludos cordiales,
Favor realizar la siguiente traducción y enviar al mail del estudiante con copia al mail: idiomas@espoch.edu.ec
Atentamente,

Centro de Idiomas
"Saber para ser"

De: Edison Fernando Ruiz Andino <edison.ruiz@espoch.edu.ec>
Enviado: jueves, 28 de julio de 2022 16:04
Para: Centro de Idiomas <idiomas@espoch.edu.ec>
Cc: Edison Ruiz Andino <edison7ruiz@hotmail.com>
Asunto: Traducción del resumen de Tesis-Maestria

Estimados compañeros del Centro de idiomas, después de la revisión de mi resumen de tesis por parte de biblioteca, procedo a enviar a ustedes el documento para el trámite pertinente, para lo cual adjunto el resumen en formato Word y comprobante de pago.