UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ABRIL 2022 - SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

" HERRAMIENTAS FIREWALL BASADAS EN TECNOLOGÍAS OPENSOURCE."

EGRESADO:

ALEXIS TONNY CAICEDO VEINTIMILLA

TUTOR:

JOSÉ TEODORO MEJÍA VITERI

AÑO 2022

RESUMEN.

Con la explosión de Internet y el ingenio de los piratas informáticos, la seguridad se ha convertido en un problema complejo en donde requiere una solución de seguridad bien pensada para manejar la situación en las organizaciones.

Este estudio de caso se encuentra desarrollado está bajo la sublínea de investigación de la carrera de Ingeniería en Sistemas: "Redes y tecnologías inteligentes de software y hardware"; por lo tanto, el presente caso de estudio tiene como finalidad el estudio de las Herramientas Firewall Basadas En Tecnologías Opensource.

La seguridad de la red controla las medidas de seguridad que sirven para proteger la privacidad, la integridad y la disponibilidad de una red local dentro de una organización. Estos dispositivos continúan evolucionando, pero gran parte de la información básica está fácilmente disponible y se necesita un poco de esfuerzo para eliminar a los atacantes de su red.

La evaluación de los firewalls se realizó mediante un método cuantitativo en un ambiente con tráfico de red simulado y se utilizaron métricas como ancho de banda, jitter y tasa de pérdida de paquetes de red, por lo que el método e indicadores antes mencionados son ampliamente utilizados para evaluar el desempeño de los firewalls

Los cortafuegos de software libre pueden ser una alternativa útil en lo que respecta a la seguridad de la red, por lo que en este estudio de caso se analizó cuatro distribuciones de Linux diseñadas específicamente para brindar este servicio las cuales poseen como característica común y operan mediante los módulos de filtrado.

PALABRAS CLAVES: seguridad, firewall, cortafuegos, software, open source, servicio, red.

ABSTRACT.

With the explosion of the Internet and the ingenuity of hackers, security has become a complex issue that requires a well-thought-out security solution to handle the situation in organizations.

This case study is developed under the research subline of the Systems Engineering career: "Intelligent software and hardware networks and technologies"; therefore, the purpose of this case study is to study the Firewall Tools Based on Opensource Technologies.

Network security controls the security measures that serve to protect the privacy, integrity, and availability of a local network within an organization. These devices continue to evolve, but much of the basic information is readily available and it takes some effort to remove attackers from your network.

The evaluation of the firewalls was carried out using a quantitative method in an environment with simulated network traffic and metrics such as bandwidth, jitter and network packet loss rate were used, so the aforementioned method and indicators are widely used. to evaluate the performance of firewalls

Free software firewalls can be a useful alternative when it comes to network security, so in this case study four Linux distributions designed specifically to provide this service were analyzed, which have as a common feature and operate through filter modules.

KEYWORDS: security, firewall, firewalls, software, open source, service, network.

INTRODUCCION.

Con la explosión de Internet y el ingenio de los piratas informáticos, la seguridad se ha convertido en un problema complejo en donde requiere una solución de seguridad bien pensada para manejar la situación en las organizaciones. Una solución de seguridad debe ser capaz de manejar las amenazas de seguridad por lo cual deben de ser lo suficientemente flexible como para adaptarse a los cambios tecnológicos de la actualidad.

La seguridad de la información es uno de los aspectos más importantes en una entidad, empresa u organización, lo cual garantiza la disponibilidad, integridad y confidencialidad de la información. Esto se logra mediante la implementación de un conjunto de controles que se seleccionan a través de un proceso de gestión de riesgos y se gestionan desde un sistema de seguridad de la información.

La gestión de seguridad tiene como objetivo garantizar la protección de la información en las redes y sus instalaciones de procesamiento. Para administrar la seguridad, existen sistemas como los firewalls que pueden inspeccionar los paquetes de red entrantes o salientes a nivel de aplicación y controlar, permitir o denegar el tráfico de red.

Los Administradores de sistemas para evitar estas vulnerabilidades en donde utilizan varias herramientas como IDS, proxies, firewalls que proporcionan información valiosa para saber qué está pasando en una red en un momento dado, deben ser analizados simultáneamente y posteriormente.

Además, pueden aplicar controles de seguridad para garantizar la protección de los servicios conectados contra el acceso no autorizado, un firewall es el principal escudo protector de una red para comprobar y permitir/denegar tanto el tráfico entrante o saliente.

Configurado de manera adecuada, nuestra red podrá funcionar con una mejor seguridad debido al control que se realiza, y, por supuesto, estará segura ante tráfico sospechoso.

En este trabajo se realizó un análisis cuantitativo de las funcionalidades de seguridad, los rendimientos de red y el consumo de recursos de hardware de los principales firewalls basados en software libre existentes hasta el momento evaluando mediante el método experimental, en donde se obtendrá una actualizada información la misma que permitirá llegar a recopilar información mediante la técnica de las encuestas.

La Facultad de Administración, Finanzas e Informática, fija la siguiente línea para el "Desarrollo de Sistemas de Información, Comunicación y Emprendimientos Empresariales y Tecnológicos", Este estudio de caso se encuentra desarrollado está bajo la sublínea de investigación de la carrera de Ingeniería en Sistemas: "Redes y tecnologías inteligentes de software y hardware"; por lo tanto, el presente caso de estudio tiene como finalidad el estudio de las Herramientas Firewall Basadas En Tecnologías Opensource.

DESARROLLO.

La seguridad de la red controla las medidas de seguridad que sirven para proteger la privacidad, la integridad y la disponibilidad de una red local dentro de una organización. Estos dispositivos continúan evolucionando, pero gran parte de la información básica está fácilmente disponible y se necesita un poco de esfuerzo para eliminar a los atacantes de su red. Es peligroso suponer que hoy en día las herramientas actuales son suficientes para mantener a los atacantes fuera de la red. Un hacker siempre encontrará una manera de manipular la información con el fin de hacer daño a la entidad o víctimas. (Marqués, 2020)

La información es importante para lograr los objetivos en las organizaciones, que se considera el activo más importante. Por lo tanto, está sujeto a diversas amenazas, como robo, fraude, fraude, divulgación, destrucción y muchas otras cosas.

El uso del Internet en la actualidad es tan indispensable para la operatividad de las empresas, por lo tanto, sus sistemas de información están expuestos a diferentes tipos de ataques o vulnerabilidades lo cuales pueden ser ejecutados a través de malware, spyware, accesos no autorizados, robos de contraseñas y amenazas externas e internas. (Nieto, 2020)

La Gestión Unificada de Amenazas existe para minimizar el riesgo de las existentes. Son dispositivos de seguridad con combinaciones de hardware, software y tecnologías de red cuyo objetivo principal es realizar múltiples funciones de seguridad. (Carlos Camacho, 2021)

- Evaluar las Herramientas de Firewall Basadas en Tecnologías Opensource en la actualidad para la gestión de seguridad empresarial.

Por lo tanto, sus objetivos específicos son:

- Analizar el marco teórico referencial e identificar los resultados.
- Realizar una evaluación cuantitativa en algunos sistemas de firewall de código abierto y la efectividad con respecto a la solución propuesta.
- Evaluar, validar, verificar e interpretar los resultados efectivos.

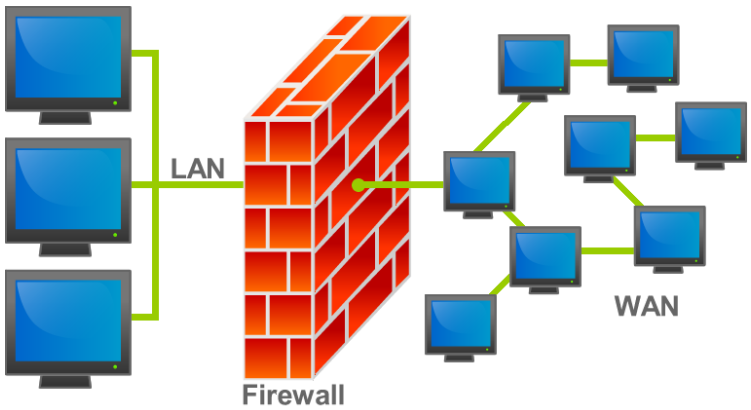


Imagen 1 ¿Que es Firewall o Cortafuegos?

Obtenido de: https://www.tec-innova.mx/que-es-un-firewall/

Un firewall o cortafuegos, es una herramienta cuya función es proteger a la red privada, de intrusiones o ataques de otras redes, bloqueándoles la accesibilidad. Es un software o una combinación de ambos que filtra el tráfico entrante y saliente entre dos o más redes de comunicaciones entre 2 o más puntos, y está diseñado para la protección de redes privadas del acceso no autorizado y no verificado en una conexión a internet. (UpperSolutions, 2022)

Los firewalls permiten la configuración de reglas para alinear el tráfico de las comunicaciones de acuerdo a las necesidades de las organizaciones que los implementen.

El termino Firewall surge en el año 1980 después de la aparición de internet con el objetivo de proteger los datos e información de los usuarios. Las empresas querían que los usuarios manejaran sus computadores con conexión a internet sigan aumentando progresivamente, en esa época fueron los routers o enrutadores separaban a las redes de las otras para que trabajen independientemente.

A fines de la década de 1980, la comunidad de Internet sufrió problemas de seguridad causados por algunos usuarios. Clifford Stoll descubrió cómo manipular el sistema de espionaje alemán. Otro ataque fue el gusano Morris, el primer ataque a gran escala a la seguridad de Internet que afectó a seis mil servidores y la primera violación a la Ley de Abuso y Fraude Informático, afectando alrededor del 10% de las computadoras conectadas. Hay miles de puertas de enlace, cada una con su propia función. Se dice que los puertos permitidos para comunicarse están abiertos, mientras que los puertos no permitidos están cerrados. Los parámetros del cortafuegos son predeterminados automáticamente por la propia computadora, pero el usuario puede cambiarlos y definirlos. (Huawei, 2019)

Un firewall es necesario para proteger su red de ataques cibernéticos, pero tener un firewall no necesariamente asegura su negocio. Es importante configurarlo y operarlo correctamente. La funcionalidad de estas herramientas de firewall generalmente se encuentra en un puerto entre dos redes. Entre la red pública y la red privada, los datos pueden entrar o salir de la red si el tráfico cumple con las reglas configuradas en los firewalls. Si no sigue las reglas configuradas en los firewalls, la información se bloquea antes de llegar al destino. El filtrado de contenido permite a los administradores bloquear fácilmente ciertos tipos de contenido web sin tener que filtrar manualmente cada URL. Los sitios web inapropiados y los sitios de redes sociales se bloquean rápida y fácilmente. (InternationallT, 2021)

Muchas empresas, compran herramientas específicas para monitoreos de firewall, pero este no es el mejor enfoque que se da actualmente. El mejor enfoque es tener una solución integral de monitoreo de red que proporcione monitoreo de firewall en el contexto de la red de su empresa y muestre todos los recursos rastreados en un solo lugar.

Un firewall gestiona la manera de proteger nuestra información y por ende puede realizar otras funciones.

Entre las cuales se detallan a continuación:

- Verificar el número de conexiones de un punto e interrumpir la conexión de los puertos que están en espera o escuchando sin previa autorización o si no han notificado dicha acción.
- Filtro los paquetes de datos según su origen, número de puerto y destino.

Los firewalls pueden clasificarse en:

Firewall de Hardware: Son dispositivos que se colocan en el router y la conexión a internet de manera apartada. En la actualidad en los routers ya vienen incorporados, y se caracterizan por tener una buena protección contra posibles ataques como virus, troyanos, etc.

Firewall de Software: Estas herramientas se dividen en 2 tipos los cuales son gratuitos y pagados.

En la actualidad existen varios tipos de firewall que son:

Firewall Proxi.	**Stateful inspection Firewall.**
Son sistemas de seguridad de red, que además realiza la gestión de elegir qué tráfico está permitido y cuál no, además utilizan una tecnología para analizar en profundidad los paquetes de datos en busca de señales de un ataque.	Estos tipos permiten bloquear el tráfico según el estado, el puerto y los criterios de protocolo. Seguimiento de la actividad desde el momento en que se abre una llamada hasta que se cierra. El filtrado se realiza de acuerdo con las restricciones especificadas por el operador.
Firewall para la gestión Unificada de Amenazas (UTM).	**Firewall de última generación.**
Se centra en la sencillez y su fácil uso. Contiene otros servicios adicionales como la gestión de nube y la prevención de intrusiones y antivirus,	Al permitir más funciones que un simple filtro, un firewall avanzado proporciona: La detección y control de aplicaciones para bloquear aplicaciones potencialmente amenazantes.

Tabla 1 Tipos de Herramientas de Firewall

Elaborado por: Alexis Caicedo Veintimilla

Una computadora conectada a Internet tiene más probabilidades de verse afectada por virus y ataques cibernéticos. En este caso, los usuarios deben contar con un escudo protector que proteja la computadora y los archivos importantes de cualquier virus, malware o elemento dañino que pueda infectar el dispositivo, existen actualmente, los cortafuegos o firewall que son utilizados principalmente por individuos y organizaciones

que se puede instalar en la combinación deseada de hardware y software de la computadora. (Adalberto Iriarte Solís, 2018)

Entre las ventajas y desventajas del firewall se señala las siguientes:

Ventajas	Desventajas
Brindar protección contra elementos nocivos: Los firewalls están diseñados para proteger la computadora de virus, malware y otros códigos maliciosos. Y si la computadora tiene protección de firewall, el usuario puede ejecutar la tarea de oficina de manera segura.	**Orientado a los costos**: un firewall también tiene varias desventajas para sus usuarios, y el factor costo es uno de ellos. Comprar un firewall puede ser costoso para las organizaciones porque tienen que pagarlo.
El proceso de instalación es relativamente fácil: Si no tiene conocimientos técnicos, también se puede instalar firewalls en su computadora, no es necesario el asesoramiento profesional., actualmente la mayoría de los sistemas operativos modernos, como Windows 11, 10, Windows 8 y 7, ya tienen firewalls preinstalados.	**Puede obstaculizar algunas actividades organizativas:** Un firewall bloquea el acceso a varios sitios que contienen malware o virus. Esto puede estar bien para sus usuarios, pero las empresas más grandes a menudo se meten en problemas por ello.
El análisis del tráfico: Es uno de los principales beneficios de un firewall, o viceversa la mayoría de las amenazas Donde es el tráfico virtualizado.	**Puede disminuir el nivel de rendimiento:** Basados en aplicaciones de seguridad que se ejecutan en segundo plano en la computadora.

Ayuda a mantener la privacidad de alto nivel: Un usuario espera total privacidad cuando se conecta, pero puede sufrir en algunos escenarios inesperados. Entonces, si usa los firewalls en este caso, se asegurará de mantener su privacidad en un alto nivel.	**Aun así, pueden ocurrir algunos ataques de piratería:** Los firewalls son eficaces contra los troyanos simples y sus tipos. Por lo tanto, otros tipos de malware pueden infectar su dispositivo informático.
Detener los ataques de los piratas informáticos: Los piratas informáticos realizan actividades ilegales al obtener acceso no autorizado a las computadoras de personas como nosotros y llegar a obtener acceso a datos confidenciales, como detalles de tarjetas de crédito., etc.	**Necesita un mantenimiento cuidado:** Aunque las pequeñas empresas de hoy están felices de pagar por los cortafuegos para sus dispositivos informáticos. Pero para las empresas muy grandes, es necesario contar con un equipo dedicado de profesionales de TI que puedan mantenerse al día con todo el trabajo de mantenimiento del firewall.

Tabla 2 Ventajas y Desventajas de las Herramientas de Firewall.

Elaborado por: Alexis Caicedo Veintimilla

El termino Opensource se refiere a al código de un programa que se distribuye libremente (incluso de manera gratuita) y que puede ser usado y modificado por los usuarios sin ninguna restricción. Una buena analogía sería, por ejemplo, la de una receta.

Aunque Open Source y Software Libre están ligados, estos no tienen por qué ser gratuitos y estaríamos hablando de software privativo y no privativo. Y en este sentido el software comercial también se puede llegar a considerar libre. (Fernandez, 2022)

La FSF (Free Software Foundation) establece cuatro libertades esenciales para los usuarios y por debajo de ellas se encuentra la capacidad de crear software de una forma diferente entre ellas son las siguientes;

1. Libertad para usar el software como desee para cualquier propósito.
2. Libertad para explorar el uso del software y modificarlo a voluntad. Entonces necesitas acceder al código fuente.
3. Libertad de distribución de ejemplares.
4. Libertad para proporcionar versiones modificadas a terceros.

Los programas de código abierto permiten a los usuarios corporativos e individuales administrar de manera eficiente todas las funciones importantes de la red. En definitiva, puede contar con soluciones que configuran de forma permanente funciones de enrutamiento y redes en general, como DHCP y DNS. Volviendo a la discusión sobre la seguridad, estos programas de código abierto tienen muchas características que les permiten agregar un escudo de protección más amplio: firewalls, antivirus, servicios antispam y filtros web. (Hat, 2019)

Con el método investigativo cuantitativo agregando el deductivo lo cual permitió el desarrollo del presente caso se tomó referencias de varios autores de fuentes bibliográficas en donde se lleva a cabo la consulta y recopilación de herramientas Firewall basadas en tecnologías OpenSource.

Basado en los lineamientos se llegó a utilizar técnicas e instrumentos como las encuestas, las cuales se manejaron mediante Formularios de Google drive haciéndole llegar a personas cercanas y compañeros con el fin de recolectar información a ser analizada para tomar en cuenta los conocimientos de las personas sobre herramientas de Firewall.

Llevando a cabo la evaluación de los firewalls, donde se realizó mediante un método cuantitativo en un ambiente con tráfico de red simulado y se utilizaron métricas como ancho de banda, jitter y tasa de pérdida de paquetes de red, por lo que el método e indicadores antes mencionados son ampliamente utilizados para evaluar el desempeño de los firewalls. . .

Para seleccionar las herramientas de firewall se analizó toda la información existente en Internet, se identificaron las soluciones basadas en código abierto con las licencias de uso libre más estudiadas.

Nombre del Firewall	**Versión disponible**	**Sistema Operativo**	**Requerimientos mínimos de hardware**		
			CPU	**RAM (MB)**	**HDD**
pfSense / Netgate	2.5.2	FreeBSD	64-bit amd64 (x86-64)	1024	80 GB
Endian / Endian SRL	3.3.2	Red Hat	Dual core (x86-64) 1 GHz	2048	8 GB
VyOS / The VyOS Project	1.2.8	Debian	64-bit amd64 (x86-64) Dual core 1 Ghz	512	2 GB
IPCop / Dafos Training	2.1.9	LFS	CPU i486	64	512 MB
Zentyal / Gesforeda, S.L.	7.0	Ubuntu	64-bit amd64 (x86-64) Dual core 2 GHz	1024	80 GB
ClearOS / ClearFoundation	7.9.1	CentOS	CPU 64-bit	1024	10 GB
OPNsense / Deciso B.V.	21.7.1	FreeBSD	64-bit amd64 (x86-64) Dual core 1 Ghz	2048	2 GB

Tabla 3 Herramientas de Firewall Open Source

Elaborado por: Alexis Caicedo Veintimilla.

Nombre del Firewall	**Ventajas**	**Desventajas**
pfSense / Netgate	• Soporte Comercial y de Comunidad. • Extensa lista de Módulos y Funcionalidades • Disponible en modalidad Cloud, Virtual Appliance, Hardware y Software	• Dificulta la automatización. • Soporte con el fabricante únicamente disponible en inglés. • Pobre sistema de reporte

Endian / Endian SRL	• Servidor que controla tráfico de salida de la red • Control de sitios en donde los usuarios no tienen conocimientos.	• La configuración en modo consola tiene un largo periodo de aprendizaje y está basado en ficheros
VyOS / The VyOS Project	• Incluye todas las herramientas y controladores para virtuales de VMware. • La imagen OVA se puede descargar desde el sitio de descarga estándar	• Solo se ejecuta en sistemas amd64 estándar
IPCop / Dafos Training	• IPCop ofrece mucha más información sobre la configuración de nuestra LAN y sobre el funcionamiento de la misma • Desempeña tanto como servidor de seguridad, brindando mucha información sobre el tráfico de nuestra red.	• La Actualizaciones de IPCop son pocas y distantes.
Zentyal / Gesforeda, S.L.	• Permite unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet.	• Ofrece suscripciones de soporte opcionales.
ClearOS / ClearFoundation	• Funciona muy cómodamente desde la terminal • Instalación, es bastante sencilla y toma alrededor de 10 minutos	• Sus versiones son gratuitas por parte de la «comunidad»
OPNsense / Deciso B.V.	• Incluye varias características de gama alta como el balanceo de carga, alta disponibilidad y portal cautivo.	• Proporciona un amplio conjunto de ofertas comerciales con los beneficios de fuentes abiertas y verificables combinados con una simple licencia BSD.

Tabla 4 Ventajas y Desventajas de las Herramientas de Firewall Open Source.

Elaborado por: Alexis Caicedo Veintimilla

La herramienta IPCop requiere de pocos recursos de un computador para su funcionamiento, fueron excluidos del análisis porque actualmente carecen de soporte técnico por parte de sus fabricantes, sus últimas actualizaciones fueron liberadas en 2019 y 2021 respectivamente, situación que puede vulnerar su desempeño ante ataques informáticos y comprometer la seguridad de las redes de datos.

Con el análisis respectivo se determinó que FreeBSD ofrece los mejores indicadores de rendimiento para la gestión de redes con respecto a otras distribuciones de Linux. Sin embargo, los hallazgos obtenidos en la presente investigación demostraron

que los índices de rendimiento de red y consumo de CPU y RAM de los firewalls pfSense y OPNsense, ambos basados en FreeBSD, fueron superados por ClearOS, solución basada en CentOS. Demostraron que los cortafuegos basados en software libre son resistentes a varios ataques cibernéticos y tienen un rendimiento de red similar al de los cortafuegos basados en hardware.

pfSense tiene las principales características de seguridad que tienen IPCop y Zentyal. ClearOS brinda un mejor rendimiento de red que las soluciones IPCop, Endian y Fedora 21 contra ataques DoS.

En este trabajo se analizaron las funcionalidades de seguridad y los rendimientos de varios cortafuegos o firewall basados en software libre. En el análisis realizado no se comprobó el comportamiento de las soluciones abordadas ante ataques informáticos, ni su desempeño respecto a soluciones privativas, estas carencias constituyen limitaciones de la presente investigación.

Sin embargo, se determinó que los resultados obtenidos evidenciaron que la totalidad de los cortafuegos analizados poseen numerosas funcionalidades orientadas a incrementar la seguridad de las redes de datos, no obstante, pfSense carece de un filtro para asegurar la mensajería electrónica y VyOS requiere de herramientas ajenas a su núcleo de instalación para implementar filtros de correo, antivirus y detección/prevención de intrusiones. En contraposición a los resultados obtenidos por Sampaio & Bernardino (2017), en relación a las funcionalidades de seguridad que poseen ambas soluciones en su núcleo básico de instalación, hallazgo que demuestra el desarrollo y nivel de madurez alcanzado por este cortafuego se concordancia con los resultados se identificó que ClearOS constituye una solución integral para garantizar la seguridad de las redes de datos, además, este cortafuegos evidenció un rendimiento de red satisfactorio y un consumo de recursos de hardware inferior al resto de las herramientas estudiadas.

Los resultados y las limitaciones de este estudio constituyen una base para investigaciones futuras relacionadas con el despliegue y la efectividad de cortafuegos basados en software libre. Como líneas de trabajo futuro se propone comparar el desempeño de las herramientas abordados en esta investigación respecto a soluciones propietarias y firewalls basados en hardware, así como analizar sus comportamientos ante diferentes ataques informáticos.

CONCLUSIONES

Los cortafuegos de software libre pueden ser una alternativa útil en lo que respecta a la seguridad de la red, por lo que en este estudio de caso se analizó cuatro distribuciones de Linux diseñadas específicamente para brindar este servicio las cuales poseen como característica común y operan mediante los módulos de filtrado.

El estudio permitió identificar que las soluciones analizadas ofrecen un conjunto de funciones que posibilitan mejorar la seguridad de las redes de datos, es claro que Endian, Gentall, PFSense, VoIP, IPFire y ClearOS tienen mejor rendimiento de red que OPNsense. En general, ClearOS mostró excelentes índices de uso de CPU y memoria RAM, lo que mostró su alta eficiencia en el almacenamiento de redes de datos y el mejor uso de los recursos de hardware.

Los resultados obtenidos en este trabajo sustentan la toma de decisiones sobre el uso de herramientas de ciberseguridad en las redes digitales de las organizaciones a través de casos de estudio donde se demostró la potencialidad de implementar un sistema Open-Source y sus beneficios donde se planea realizar la implementación en un entorno de pruebas real, con el propósito de validar los resultados obtenidos en este entorno de pruebas.

BIBLIOGRAFÍA.

Adalberto Iriarte Solís, P. V. (2018). Evaluacion de Firewall basados en softwares libres. *Pistas educativas*.

Carlos Camacho, D. N. (2021). Análisis comparativo de Gestión Unificada de Amenazas (UTM) de codigo abierto paa fortalecer la seguridad de la imformacion. *Revista de Ciencias de serguridad y defensa*.

Corrales, D. E. (2022). Diseño e Implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad.

Fernandez, L. (2022). Los mejores Firewall open-source para proteger tu red. *Redes Zone*.

Hat, R. (2019). ¿Qué es el open source?

Huawei. (2019). Un vistazo por la historia de los Firewalls de Huawei.

InternationallT. (2021). ¿Qué es el Monitoreo de Firewall?

Marqués, F. L. (2020). Qué es la seguridad en Internet y cómo garantizarla. *Clinic Cloud*.

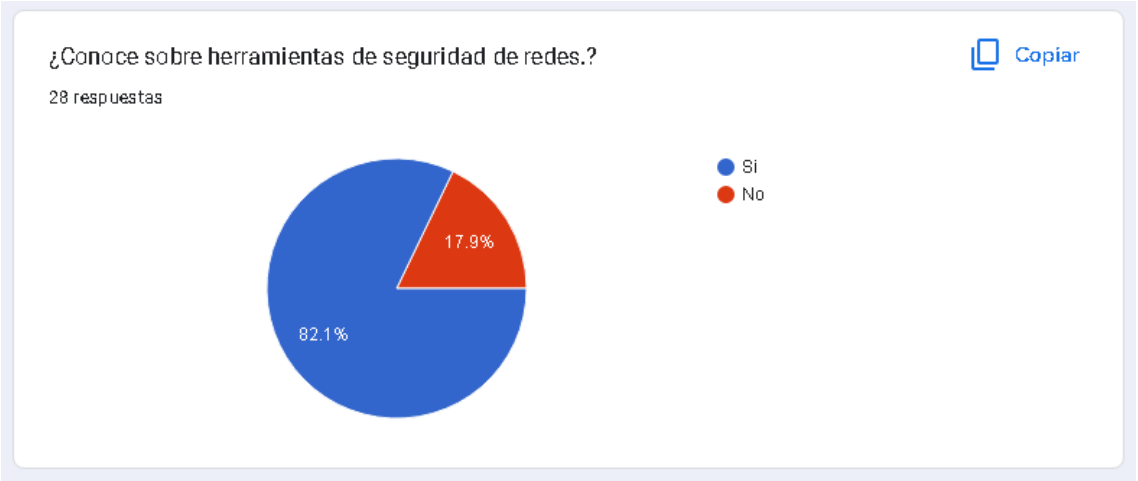
Nieto, A. (2020). Seguridad en la red, prioridad para las empresas, una gran oportunidad para el canal. *En lad Red, prioridad para las empresas.*

Salaguste, G. (2022). Secured and fault tolerant infrastructure: Implementation of an open source web application firewall.

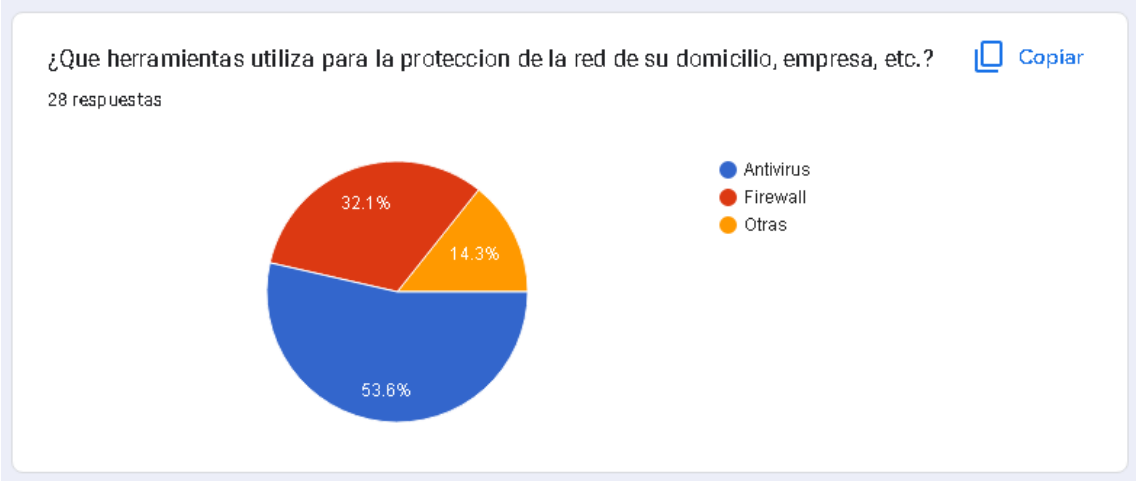
Singh, J. (2018). Impact of paranoia levels on the effectiveness of the modsecurity web application firewall. . *1st International Conference on Data Intelligence and Security (ICDIS)*.

UpperSolutions. (8 de Marzo de 2022). *QUE ES UN FIREWALL O CORTAFUEGOS Y PARA QUE SIRVE*. Obtenido de UpperSolutions: https://uppersolutions.es/que-es-un-firewall-o-cortafuegos-y-para-que-sirve/

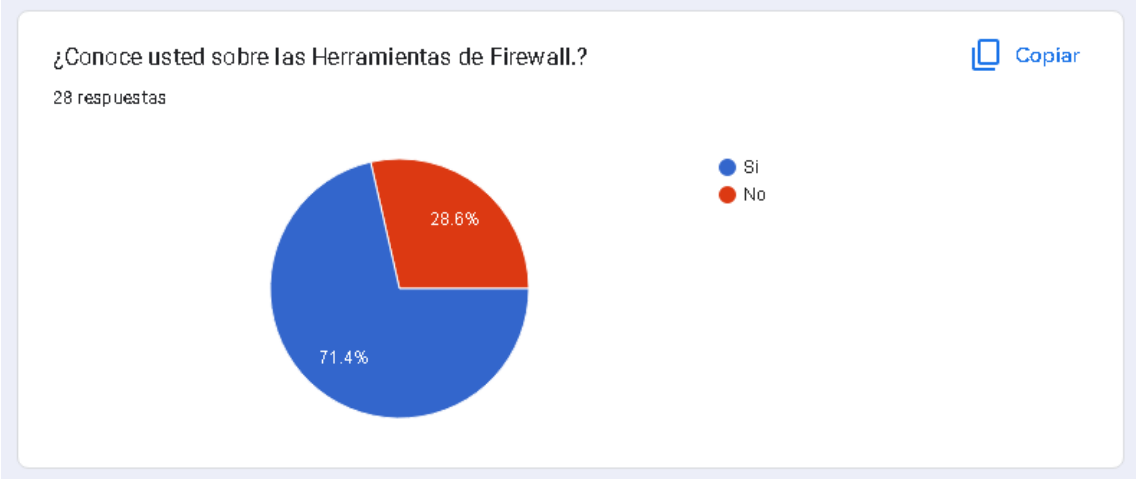
ANEXOS



Análisis: Con la encuesta de manera virtual, que se llevó el 82.1% de las personas conocen sobre herramientas de seguridad de las redes mientras que el 17.9% desconoce.



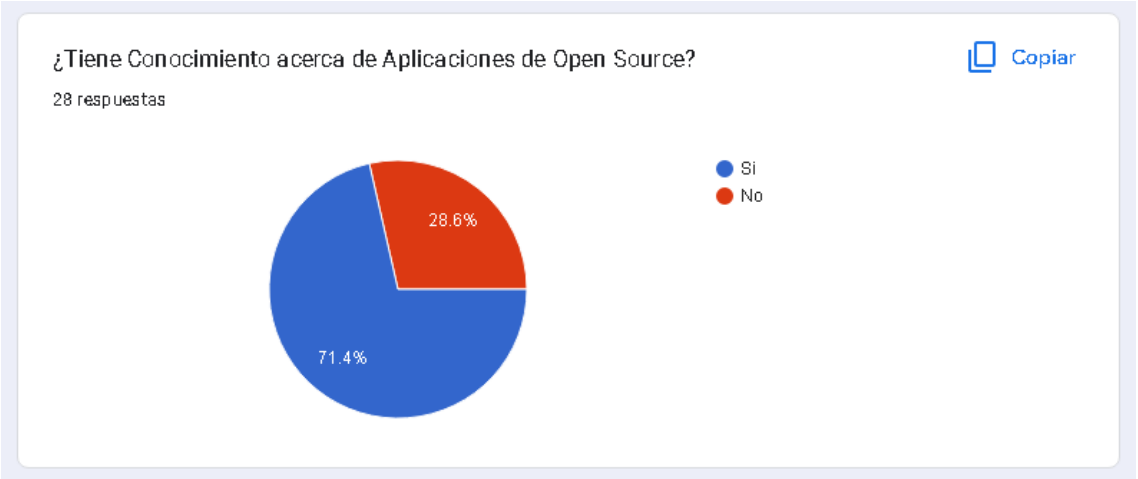
Análisis: El 53.6% utilizan antivirus como métodos de seguridad, el 32.1% Firewall y otras herramientas el 14.3%, El antivirus tiene funciones de control de redes y protección de la misma y como es de costumbre todos los usuarios piden instalar esta herramienta al adquirir un equipo, y el resto conocen acerca de los firewalls por lo que hacen su control de las redes de manera independientes para ahorrar recursos del computador.



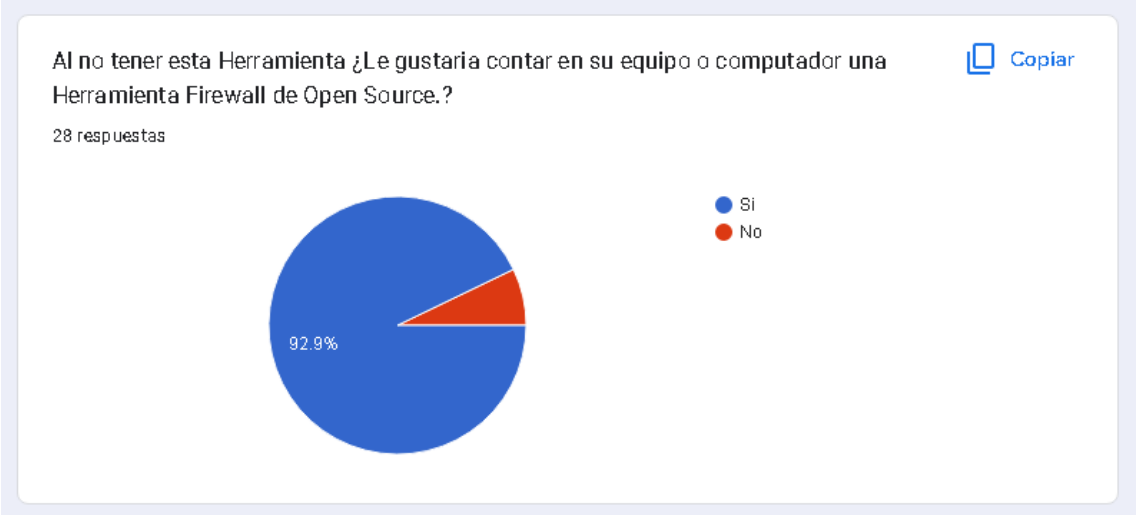
Análisis: El 71.4% conocen de las herramientas, como se menciono en la pregunta anterior es por ahorrar recursos del computador, mientras que el 28.6% desconoce sobre las herramientas mencionadas.

Análisis: El 67.9% conoce acerca del firewall que tiene su equipo , era de esperar ya que Windows trae por defecto y puede ser manipulado por parte del propietario, mientras que el 32.1% desconoce totalmente, puede ser que lo tengan pero no están tan familiarizados con estas herramientas.

Análisis: El 100% de las personas encuestadas esta de acuerdo en optar con estas herramientas para controlar el tráfico de red en sus equipos en el hogar u las empresas.



Análisis: El 71.4% conoce acerca de aplicaciones de Open source , y el 26.6% no tiene total conocimiento acerca de este término pero si han de manipular ciertas aplicaciones.



Análisis: Según el 92.9% desearía contar con dicha herramienta en su equipo ya que son de fácil acceso y sencillas de gestionar.