ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE ALTERNATIVAS PARA LA IMPLEMENTACIÓN DE UN SISTEMA UNIFICADO DE SEGURIDAD INFORMÁTICA UTILIZANDO HARDWARE DE BAJO COSTO Y SOFTWARE LIBRE

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

JOHANN SEBASTIAN IÑAGUAZO VELEPUCHA

johann.inaguazo@epn.edu.ec

DIRECTOR: WILLIAMS FERNANDO FLORES CIFUENTES

fernando.flores@epn.edu.ec

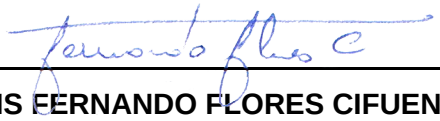
DMQ, septiembre 2022

CERTIFICACIONES

Yo, JOHANN SEBASTIAN IÑAGUAZO VELEPUCHA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

JOHANN SEBASTIAN IÑAGUAZO VELEPUCHA

Certifico que el presente trabajo de integración curricular fue desarrollado por JOHANN SEBASTIAN IÑAGUAZO VELEPUCHA, bajo mi supervisión.



WILLIAMS FERNANDO FLORES CIFUENTES

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JOHANN SEBASTIAN IÑAGUAZO VELEPUCHA

WILLIAMS FERNANDO FLORES CIFUENTES

DEDICATORIA

A mis padres, que han sido mi apoyo a lo largo de la carrera y que siempre han creído en mi para finalizar con éxito esta etapa académica. Especialmente a mi mamá, por ser mi fuente de inspiración para continuar superándome y para mostrarme que siempre se puede seguir adelante, incluso en los peores momentos.

A mis hermanas, que con su ejemplo han podido demostrarme que con esfuerzo todo es posible y que siempre vendrán días mejores.

A mis amigos, por siempre darme ánimos para continuar.

AGRADECIMIENTO

A Dios, por brindarme oportunidades incluso cuando no las he podido aprovechar todas. Aunque parezca que no estoy pendiente de ti, siempre te tengo en mente y te estoy agradecido, por cuidar a mi familia y amigos, y ser un faro de esperanza para la mayor parte del mundo.

A mi madre, mi primera maestra y ejemplo personificado de lo que es ser un ángel, con ella todo es mejor y este mundo tiene un brillo indescriptible. Por acompañarme y apoyarme durante toda la carrera, en mis desvelos y momentos de quiebre, y también en mis momentos de felicidad. La palabra “gracias” se queda corta contigo.

A mi padre, mi inventor favorito, artista e ingeniero con algo mejor que un título; aunque no lo diga muy seguido, eres una de las personas más importantes para mí, por creer que podía lograrlo y espero que así sea.

A mi director, por tenerme paciencia y apoyarme en la realización de este trabajo. Me encuentro muy agradecido con usted.

Finalmente, agradezco a la Escuela Politécnica Nacional y a todos aquellos que la conforman o conformaron, por nutrirme con su conocimiento, por exigirme y por ponerme retos. A todos aquellos que conocí durante mi estadía allí y con quienes compartimos gratos momentos. A todos y todas, gracias por todo.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

La seguridad informática es un tema de mucha importancia en la actualidad, más con el crecimiento de la tecnología de una manera exponencial cada día, la necesidad de estar conectados a los servicios que brinda el Internet ha desencadenado que las personas se conecten a la gran red desde múltiples dispositivos, especialmente desde sus organizaciones; para garantizar su seguridad, es de suma importancia disponer de una serie de mecanismos que brinden soluciones de seguridad informática. Los proveedores especializados en el área disponen de soluciones muy acordes a lo que una organización necesita, ofreciendo equipos del tipo Gestores Unificados de Amenazas (UTM); sin embargo, oficinas u organizaciones pequeñas o en crecimiento no disponen de los recursos suficientes para contratar dichas soluciones.

Este trabajo busca ser un estudio de alternativas de Sistemas Unificados de Seguridad Informática basadas en software libre y hardware de bajo costo, que sirva como una guía para considerar las opciones existentes que puedan adecuarse a sus recursos. Además, presentar conceptos que resultan fundamentales para el entendimiento del funcionamiento del equipo de seguridad informática. El estudio ofrece analizar cuatro opciones de sistemas que han ganado popularidad y reducir el número de opciones a 2, por medio de un análisis de los servicios que incorporan y la factibilidad que tienen de trabajar con equipos de tamaño reducido o computadores de bajo costo. Al final se opta por trabajar con los sistemas OPNsense y Endian, que son sistemas especializados en dicho campo.

PALABRAS CLAVE: Seguridad Informática, Sistema Unificado, Hardware de bajo costo, UTM, OPNsense, Endian.

ABSTRACT

Computer security is a very important issue today due to the exponential growth of technology every day. The need to be connected to Internet services has caused users to connect to the web from multiple devices, including from within their organizations. To guarantee security, it is important to have mechanisms that offer computer security solutions. There are providers specialized in information technology that have appropriate solutions according to the needs of an organization, these solutions are called Unified Threat Management; however, small or growing offices or organizations do not have the resources to purchase such solutions.

This work seeks to be a study of alternatives for Unified Information Security Systems based on free software and low-cost hardware, which serves as a guide to consider the existing options that may be adequate for your resources. In addition, present concepts that are essential for understanding the operation of computer security equipment. The study offers to analyze four system options that have gained popularity. To reduce them to two options, through an analysis of the services they incorporate and the feasibility of working with small-sized equipment or low-cost computers. Finally, it chooses to work with the OPNsense and Endian systems, which are specialized systems in the area of computer security.

KEYWORDS: Computer Security, Unified System, low-cost hardware, OPNsense, Endian.

1 INTRODUCCIÓN

La seguridad informática, si bien es un tema bastante discutido en la actualidad, algunas veces resulta ser el menos relevante; esta problemática se evidencia comúnmente en ambientes de hogares o en organizaciones pequeñas con recursos limitados; que, al no estar correctamente informados, descuidan este aspecto de suma importancia.

La basta información acerca del software y del hardware requerido, encontrada en foros web o semejantes, sólo hacen que sea más difícil la toma de decisiones en cuanto a encontrar soluciones que se adapten a los recursos disponibles de las organizaciones.

Los sistemas que engloban servicios dedicados a la seguridad informática, también llamados equipos de Gestión Unificada de Amenazas (Unified Threat Management, UTM), son sistemas robustos que vienen incluidos en equipos con hardware dedicado, pertenecientes a proveedores especializados en seguridad informática. Si bien estas soluciones son las más recomendadas, resulta poco accesible cuando se considera el presupuesto del que disponen organizaciones de mucho menor tamaño.

En el mercado web existen Gestores Unificados de Amenazas que son presentados mediante varias ediciones, algunas gratuitas pero incompletas; sin embargo, es difícil conocer en un primer vistazo aquellos servicios a los que se puede acceder sin límites y cuáles de ellos deben ser adquiridos por un costo adicional.

El estudio presentado tiene como objetivo mostrar alternativas de seguridad, es decir, sistemas que poseen un adecuado conjunto de servicios o herramientas básicas que hagan frente a las amenazas que comúnmente se puedan encontrar en una red; a este conjunto de herramientas se lo ha denominado Sistema Unificado de Seguridad Informática.

En estos días, cualquier computador puede ser utilizado para instalar un sistema, no obstante, a fin de garantizar su correcto funcionamiento respecto al rol de hacer frente a la seguridad en una red, es importante disponer de opciones que presenten alternativas a la disponibilidad del conjunto de servicios de seguridad a implementar.

Respecto a la propuesta de equipos físicos que puedan implementar dichos servicios, en un principio se consideran computadores de placa única o de espacio reducido que a simple vista pueden ser los más adecuados, sin embargo, es necesario analizar su viabilidad respecto a los requerimientos mínimos y recomendados de los sistemas en cuestión. El trabajo considera ser una guía para la toma de decisión respecto a alternativas de seguridad informática, junto con el equipamiento necesario, que puedan ser implementadas en ambientes con costes limitados.

1.1 OBJETIVO GENERAL

Analizar alternativas de software y hardware para la implementación de un Sistema Unificado de Seguridad Informática.

1.2 OBJETIVOS ESPECÍFICOS

1. Definir los conceptos relacionados para la implementación de un Sistema Unificado de Seguridad Informática.
2. Identificar y analizar soluciones de software libre y/o de código abierto que puedan afrontar las amenazas más comunes en una red.
3. Elaborar un análisis acerca del hardware de bajo costo necesario para la implementación de los Sistemas Unificados.
4. Desarrollar una comparación de la información obtenida con el fin de presentar 2 alternativas que incluyan los servicios de seguridad básicos y las soluciones de hardware que más se adapten al caso de estudio.

1.3 ALCANCE

El presente trabajo tiene como objetivo encontrar alternativas para la implementación de un Sistema Unificado de Seguridad Informática, por lo tanto, se empezará por definir los conceptos relacionados a un Sistema Unificado y los servicios de seguridad informática básicos que debe implementar el sistema con el objetivo de mitigar en cierto nivel el riesgo de un posible ataque informático.

Continuando con el trabajo, se definirán soluciones de software libre y/o de código abierto de Sistemas Unificados y se describirá una a una las características que poseen, haciendo énfasis en los servicios o herramientas básicas requeridas dentro del contexto de Seguridad Informática. Las soluciones de software se probarán en ambientes de virtualización con el fin de encontrar y extraer aquellas características comunes y realizar una comparación.

Dada la necesidad de equipos que reúnan el hardware requerido para la implementación de los sistemas, se analizará la viabilidad de utilizar equipos de bajo costo, por ejemplo: computadores de placa única tipo Intel NUC, Raspberry Pi, etc. Con ello se garantizará el funcionamiento de los equipos respecto a las alternativas.

Finalmente, con las posibles soluciones identificadas, se presentarán 2 alternativas de Sistemas Unificados de Seguridad Informática junto con el hardware necesario.

1.4 MARCO TEÓRICO

1.4.1 SEGURIDAD INFORMÁTICA

Partiendo de la etimología del término, seguridad en calidad de seguro es todo aquello que se encuentra libre de riesgo y, por otro lado, informática se refiere al manejo automático de la información por medio de equipos computarizados; por lo tanto, cuando se habla de ambos términos en conjunto, se refiere a controlar el riesgo que puede existir en uno o un conjunto de equipos de cómputo.

En un margen más amplio, no se debe confundir con el término Seguridad de la Información, el cual no se centra únicamente en el campo de la informática sino en todo medio que disponga de información; por otro lado, la Seguridad Informática se encarga de asegurar la información que es transmitida y almacenada, por medio de técnicas que garanticen la autenticidad, confidencialidad, integridad y disponibilidad de la misma. [1, pp. 13,14]; estos llamados pilares se ven definidos en la Figura 1.1. de acuerdo con [2].

Figura 1.1. Pilares de la Seguridad Informática

Otro término que resulta muy novedoso en estos días es el de Ciberseguridad y puede existir una confusión entre este y los términos previamente revisados, sin embargo, la diferencia más importante entre la ciberseguridad y la seguridad informática radica en que esta última, por lo general es defensiva [3]. A pesar de lo que se pueda encontrar

comúnmente en textos o información en la web, es importante enfatizar que la Seguridad de la información engloba a los otros dos términos. Es común encontrar que otros autores se refieren a ambos como sinónimos, sin embargo, tienen sus diferencias [4] como se lo mencionó anteriormente.

1.4.2 SISTEMA UNIFICADO DE SEGURIDAD INFORMÁTICA

La idea de disponer de un sistema centralizado que implemente un conjunto de servicios de seguridad básicos para tener la mejor defensa en una red de computadores lleva a definir el término Sistema unificado de seguridad informática o también conocido en otros medios como Gestión unificada de amenazas (UTM del inglés Unified Threat Management), es decir, una solución de seguridad que ofrezca múltiples funciones en un equipo centralizado de la red. Estos equipos deben incluir servicios de: firewall, prevención y detección de intrusos, red privada virtual (VPN), servidor proxy, gestores de ancho de banda, etc [5].

La mayoría de los sistemas UTM se encuentran diseñados para ser implementados sobre hardware dedicado, ahorrándose el trabajo de instalar la mayoría de las herramientas o un sistema operativo desde cero sin tener los conocimientos necesarios, sin embargo, existen soluciones alternativas que pueden ser instaladas en equipos que solamente dispongan del hardware mínimo para su funcionamiento.

1.4.3 SEGURIDAD POR CAPAS

En la actualidad, la gran variedad de amenazas existentes que pueden afectar a una red informática hace que sea necesario poseer una serie de mecanismos ofensivos para minimizar el impacto que esto cause en la red. El concepto de seguridad por capas o (DiD del inglés Defense in depth) comprende lo anteriormente mencionado, la protección de una red de ordenadores ante amenazas externas utilizando estrategias defensivas que pueden reducir significativamente los riesgos que dicha amenaza pueda causar en la infraestructura física y lógica de la organización [6, p. 2].

Basada en el modelo militar de implementar múltiples barreras para frenar el ataque de un enemigo y así otorgar el tiempo necesario a fin de planificar una medida ofensiva, la seguridad por capas busca bloquear o frenar las amenazas para impedir que los usuarios y la información que manejan se vea comprometida [7]. La Figura 1.2. basada en [8], presenta la información de las capas básicas que debería tener una infraestructura de red y las funciones que cumplen.

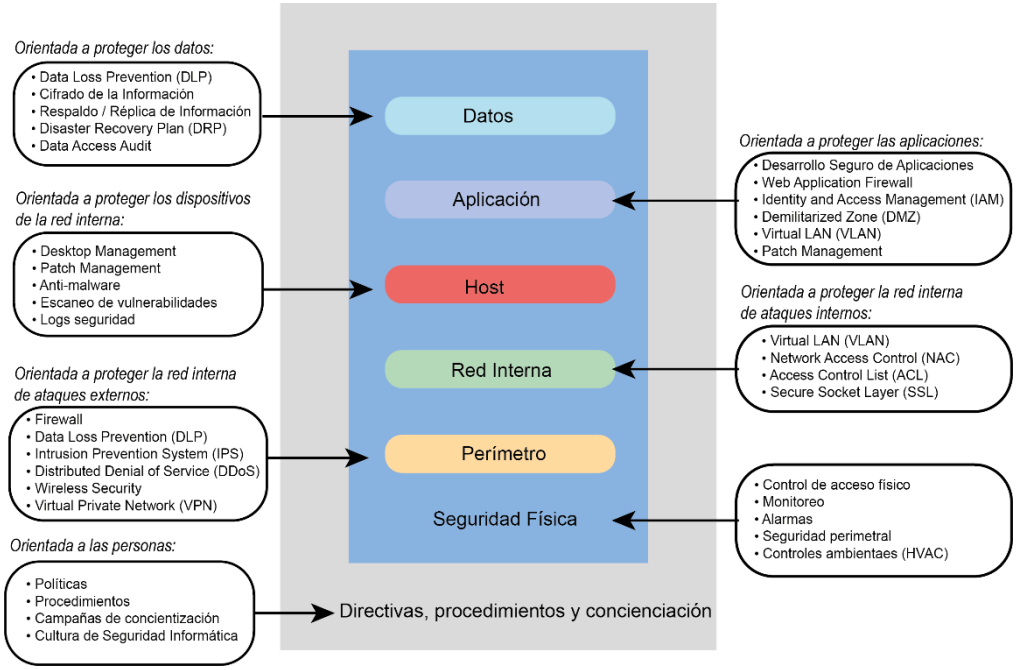


Figura 1.2. Esquema de seguridad por capas

Como uno de los elementos de importancia se tiene al usuario, que debe estar al tanto de las directivas y procedimientos que la organización haya definido respecto al área tecnológica, de igual forma, debe estar consciente de que un mal manejo de los medios informáticos puede generar una brecha de seguridad y comprometer a su equipo o la red de computadores en general.

La Seguridad Física es la encargada de controlar a los administradores que tienen acceso a la infraestructura de red, utilizando equipos de monitoreo, control biométrico y todos aquellos equipos físicos que sean necesarios para administrar los accesos y restringir totalmente a usuarios no autorizados.

El perímetro y la red interna se encargan de aquellos equipos que se encuentran entre la conexión lógica exterior y la red interna de computadores de la organización, por lo tanto, es necesario disponer de uno o varios equipos que ofrezcan los servicios que se muestran en la Figura 1.2. principalmente el firewall, que es la primera barrera exterior de la red interna. Con ello, se garantiza que equipos finales de usuario, así como servidores, se encuentren seguros antes agentes externos.

Por último, los equipos que manejan información importante deben disponer de un grupo de elementos y servicios que eviten el robo de información por causa de un agente interno o externo en caso de vulnerar las anteriores capas. Con todo lo descrito anteriormente, en teoría, se puede disponer de una red segura.

1.4.4 SERVICIOS DE SEGURIDAD

Con el objetivo de hacer frente a seguridad en una red, ya sea por factores maliciosos externos o internos como se lo mencionó en el literal anterior, a continuación, se detalla más a fondo el conjunto de servicios de seguridad básicos que se necesitan para mitigar en algo los riesgos o amenazas que se puedan encontrar en una red de computadores.

1.4.4.1 Firewall

Traducido al español como Cortafuegos, como referencia a un muro o un medio que evita la propagación de fuego, tiene como función la protección contra ingresos externos hacia los equipos computacionales que pertenecen a una red y que se encuentra en constante comunicación con el internet.

Principalmente se pueden encontrar de dos tipos, aquellos que trabajan sobre hardware dedicado y aquellos que pueden ser instalado en cualquier equipo informático que cumpla con las características de hardware necesarias, este servicio de firewall puede ser instalado como un servicio en el computador en cuestión; un ejemplo de firewall por software es aquel que se encuentra instalado por defecto en un sistema operativo [9, p. 204].

Un firewall puede ser usado para bloquear el acceso que puede provenir de agentes externos o aplicaciones específicas que intenten ingresar a una red específica y al mismo tiempo, permitir el acceso a aquella información de interés para la empresa.

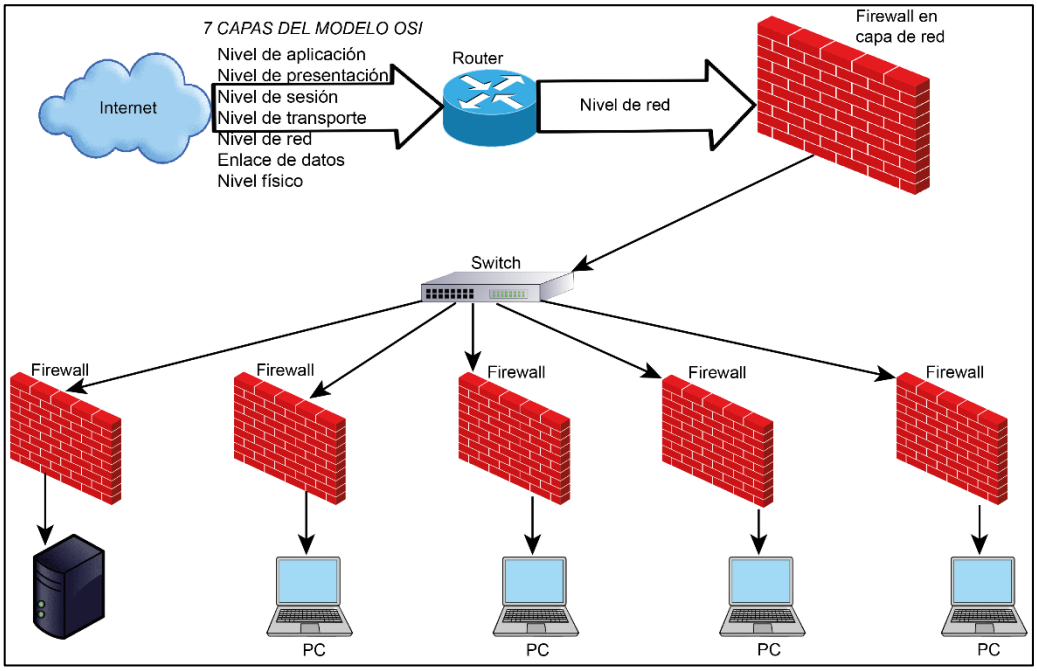


Figura 1.3. Firewall en una red local frente a Internet

La posición lógica de un Firewall es entre un Router y un Switch tal como se muestra en la Figura 1.3. y también, entre los equipos y el Switch, físicamente esto se consigue conectando el firewall a la red interna y configurando la red para que la salida sea mediante este dispositivo; con respecto al firewall de los equipos, corresponde a aquellos mediante software sobre un sistema operativo de usuario final. Es posible que el Router o un Switch de tipo administrable dispongan de estos servicios por defecto y no sea necesario la intervención de un equipo adicional.

1.4.4.2 Antivirus

Cuando se habla de amenazas externas que puedan ejecutarse desde cualquier equipo dentro de la red, resulta conveniente hablar de una solución antivirus, el cual protege al usuario, actuando sobre el sistema operativo en el cual se encuentre instalado y accediendo a toda la información contenida en busca de algún agente infeccioso; debido a que frecuentemente se desarrollan nuevos virus por parte de los atacantes, resulta necesario que el antivirus descargue información actualizada de las nuevas amenazas. Archivos adjuntos en correos electrónicos, programas descargados de fuentes no oficiales, programas o libros piratas descargados, son factores suficientes para resaltar la importancia de un antivirus, una recomendación a lo antes mencionado es no abrir aquello de lo cual no se conoce su procedencia, y aunque esto se cumpla, resulta probable que un usuario accidentalmente envíe un archivo de contenido malicioso [9, p. 177].

Un antivirus garantiza la protección de archivos o programas con el contenido malicioso desconocido por el usuario, sin embargo, es necesario mencionar que existen varias prestaciones por parte de cada proveedor y se debe elegir aquella que más se adecúe a las necesidades de los usuarios.

1.4.4.3 Amenazas en una red

Los datos que se manejan en una red resultan de gran interés por parte de los atacantes cibernéticos, las amenazas más comunes que se pueden encontrar son:

Virus, worms o gusanos, troyanos, phishing o suplantación de identidad, ataques del día cero, ataques de denegación de servicio, entre otros.

1.4.4.3.1 Ransomware

Software de carácter malicioso que se encarga de secuestrar la información de los usuarios para luego pedir una especie de rescate, es decir, un pago para poder recuperar la información afectada. La información del equipo es encriptada localmente y la información original es enviada a un a un servidor externo.

Es uno de los ataques que ha ganado popularidad en los últimos tiempos con el cual los cibercriminales extorsionan a usuarios y organizaciones. Hay usuarios que han pagado por el rescate, sin embargo, no siempre la información secuestrada es devuelta. La falta de un software antivirus es una de las formas más generales que usa para colarse en los equipos [2].

1.4.4.3.2 Phishing

También conocido como suplantación de identidad, es un ataque que se especializa en obtener información confidencial del atacado, su objetivo es la información de carácter financiero, es decir, cuentas bancarias o aquellas aplicaciones que manejan la temática de acceso a pagos. Su forma de actuar, un correo que es enviado a los usuarios con enlaces o archivos adjuntos de dudosa procedencia, que en la mayoría de los casos posee información parecida a un correo legítimo [2].

1.4.4.3.3 Spyware

Software malicioso que se ejecuta sin que el usuario conozca de su existencia al ejecutarse en segundo plano, su objetivo consiste en espiar y acceder a la información de los usuarios, una de las formas de instalarse es por medio de aplicaciones de fuentes no oficiales y que ocultan una segunda aplicación, en este caso el spyware [2].

1.4.4.3.4 Troyanos

Si se conoce la procedencia de su nombre es fácilmente entendible cómo actúa, en resumen, es un virus que se camufla en software con apariencia legítimo. Busca realizar estragos en el equipo atacado por medio de acciones no autorizadas, tales como, la eliminación de datos, bloqueos de sistema, modificaciones de ficheros, tomar control no autorizado del equipo, entre otras [2].

1.4.4.4 Sistemas de detección o prevención de intrusiones

Un Sistema de detección de Intrusos (del acrónimo en inglés IDS, Intrusion Detection System) se encarga de detectar todos aquellos accesos que no sean autorizados por el administrador de red hacia los computadores o a la red como tal, su forma de funcionamiento se basa en los analizadores de paquetes, es decir, la red es monitoreada para obtener información acerca de las intrusiones [9, pp. 155-156].

Un IDS monitorea el tráfico entrante y es comparado con una base de datos conformada con ataques que ya son conocidos, cuando actúa emite una alerta hacia el administrador de red quien puede tomar una medida ofensiva al respecto. Cuando se habla de accesos no autorizados, se refiere a ataques que pueden ser realizados por usuarios

malintencionados o aquellos que se realizan por medio de herramientas automatizadas para ese fin. Es necesario recordar que un IDS no trata de mitigar la intrusión por decisión propia, cualidad que si pertenece a un IPS [10].

Un Sistema de prevención de Intrusos (del acrónimo en inglés IPS, Intruder Prevention System) evita que intrusiones no deseadas o dañinas afecten a un equipo informático o una red de computadores. El sistema está diseñado para vigilar y detectar anomalías que transitan en una red, es posible que tenga cierta autonomía, tomando decisiones respecto al control de acceso de acuerdo con el contenido que circula en la red [9, p. 180].

Por medio de políticas de seguridad del tráfico monitoreado en tiempo real el sistema es capaz de identificar y de ser necesario, detener el ataque de cualquier actividad del tipo maliciosa, incluso, sin necesitar la ayuda del administrador de red. Por lo tanto, un IPS es capaz de proteger a los equipos y a la red antes de que suceda una intrusión, eliminando y combatiendo cualquier amenaza externa detectada [10].

1.4.4.5 Servidor Proxy

De acuerdo con [9, pp. 216-217], un proxy no es más que un firewall basado en tráfico HTTP de capa 7, lo cual permite a un computador tener acceso a redes externas o Internet de forma controlada. Un proxy es un intermediario, alguien que actúa a nombre de otro dispositivo, un computador no interactúa directamente con el internet, sino que es el servidor proxy el que se conecta directamente y el equipo informático conectado a él.

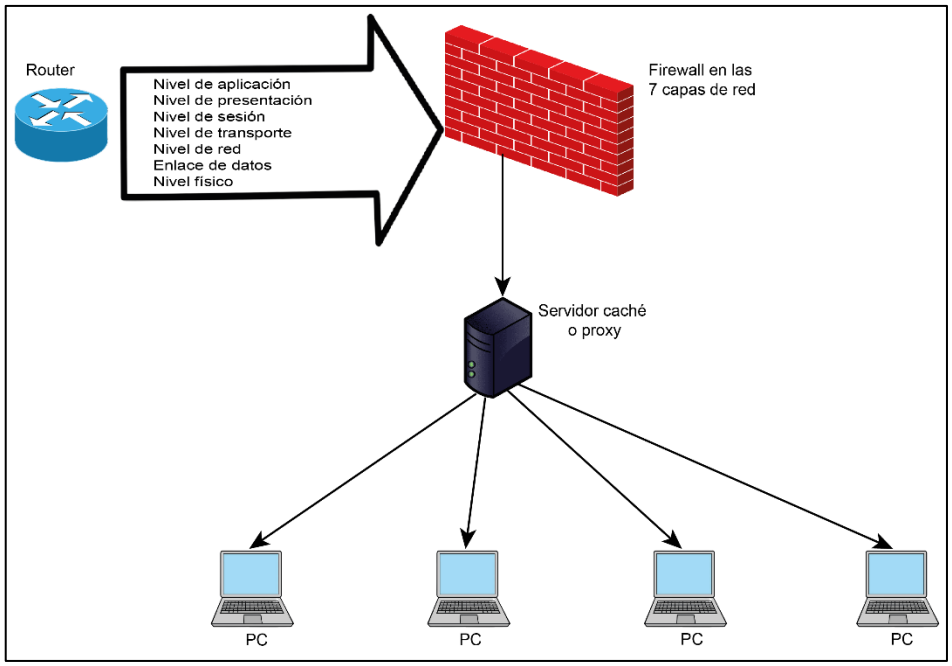


Figura 1.4. Servidor Proxy en una red

Uno de los trabajos extra que se deben realizar en todos los computadores para que se tenga conexión a internet por medio de un Proxy, es configurar todos los equipos de la red para que utilicen el servidor. Un servidor caché también puede actuar como firewall y al contrario de un proxy, no requiere ser configurado en todos los equipos [9, p. 217].

1.4.4.6 Gestor de ancho de banda

Gestionar el ancho de banda, ya sea para los recursos de red internos o para la salida externa, es muy importante y el uso en exceso del mismo puede comprometer al rendimiento y afectar los servicios necesarios de la organización, lo cual puede llevar a la inactividad de la red [11]. La importancia de utilizar un gestor de ancho de banda en la red radica en que se puede saber con exactitud qué servicios o usuarios están haciendo uso desmedido de la red, y de ser necesario, controlar esa conexión.

En el mercado existen múltiples softwares gratuitos y de pago que poseen soluciones de acuerdo con los requerimientos de las organizaciones, más adelante se entrará en detalle al respecto.

1.4.4.7 Red privada virtual

La necesidad de trabajar remotamente en una red organizacional o de hogar es la forma más común de ejemplificar el uso de una Red privada virtual (del acrónimo en inglés VPN, Virtual Private Network), con ella uno o más equipos informáticos pueden conectarse a una red privada, de una empresa, por ejemplo, utilizando Internet. Estas redes privadas virtuales pueden usarse de otras formas también útiles, esto se explicará más adelante [12].

Cuando un dispositivo utiliza una VPN, no se sigue el camino tradicional de comunicación de salida directa al internet, sino que primero tiene que pasar por un servidor VPN para establecer esa comunicación. Esto hace que la conexión sea más segura dado que la información se transmite cifrada por este túnel VPN.

Anteriormente se mencionaron aplicaciones adicionales de una VPN, las cuales se listan a continuación [12]:

- En redes públicas que no garantizan su seguridad, dado que carecen de algún tipo de verificación y el dispositivo puede quedar expuesto.
- Conectarse a una red privada de otro país para acceder a contenidos exclusivos: información censurada en un país, aplicaciones, videojuegos, tiendas en línea, etc.
- Permitir soporte técnico remoto a algún colaborador de la misma organización de manera segura.

1.4.5 SOFTWARE LIBRE

Es aquel encargado de respetar la libertad de los usuarios y su comunidad, mencionado en [13], su significado radica en la libertad que tienen los usuarios para ejecutar, compartir, modificar y mejorar el software. Esto adquiere sentido cuando se analiza su término en inglés *free software* que si lo traduce puede significar libertar o gratuidad. No debe ser confundido con el software de tipo código abierto (Open Source) que, si bien comparten ciertos puntos, maneja una filosofía diferente [13]. La diferencia más común es que el código abierto se encuentra sujeto a términos de licencia que el usuario debe respetar.

1.4.6 HARDWARE DE BAJO COSTO

Al hablar de hardware de bajo costo, se pueden incluir equipos ensamblados con componentes de diferentes fabricantes que no necesariamente se encuentran bajo una marca en específico, sin embargo, también existe la opción de utilizar mini PCs, que debido a sus dimensiones reducidas han adquirido popularidad al poseer todo lo que un computador comúnmente necesita.

Uno de los fabricantes de estos dispositivos es Intel, el cual mediante su línea de equipos NUC o Siguiente Unidad de Computación (del inglés Next Unit of Computing) ha logrado distribuir equipos que incorporan soluciones completas a equipos informáticos [14]. Estos equipos son pequeños, por lo general no vienen con disco duro por defecto, pero soportan dispositivos de almacenamiento de 2.5”, aquellos que normalmente son utilizados por computadores personales.

Otros equipos que han adquirido popularidad en los últimos tiempos son los computadores de placa única conocidos como Raspberry PI, estos incorporan su propio sistema operativo de tipo Linux y como almacenamiento la posibilidad de utilizar una tarjeta microSD. Los equipos se muestran en la Figura 1.5.

Figura 1.5. Intel NUC (izquierda) y Raspberry Pi (derecha)

2 METODOLOGÍA

El desarrollo metodológico del presente componente corresponde a un trabajo del tipo descriptivo [15, p. 113], que busca analizar el conjunto de servicios de seguridad básicos de los Sistemas Unificados de Seguridad Informática; con ello se pretende identificar sus características más comunes centrándose en su funcionamiento y relevancia dentro del contexto del trabajo.

En un primer filtro, se seleccionarán sistemas encontrados en foros web actualizados y así se tomará en cuenta a aquellos que en un primer vistazo cumplan con lo que se busca estudiar. Cada sistema será probado en un ambiente sencillo de virtualización con características de hardware limitado, semejantes a los requerimientos mínimos demandados.

La técnica de recolección de datos a utilizar se compone de dos puntos clave: la información obtenida de la virtualización y la revisión documental [16, p. 47], es decir, la documentación oficial existente en la web de cada sistema, además de la lista de hardware requerido; con esto, se espera sintetizar toda la información relevante para obtener datos que permitan realizar una posterior comparación y así llegar al objetivo deseado.

Finalmente, con la información obtenida se pretende elaborar un formato tipo lista de verificación por cada sistema, que englobe parámetros relevantes comunes, permitiendo un posterior análisis comparativo. Con base en los resultados obtenidos, se presentarán las 2 alternativas de Sistemas Unificados de Seguridad Informática junto con el hardware que sea necesario.

2.1 SISTEMAS PARA EL ESTUDIO

De acuerdo con las listas encontradas en [17] y [18], se han elegido aquellas opciones más acordes para ser estudiadas a lo largo del trabajo; sistemas que en primera instancia cumplen con el conjunto de servicios de seguridad básicos, ediciones community [19] para ser probadas en un ambiente de virtualización y documentación web debidamente estructurada.

Los sistemas que se listan disponen en su documentación apartados específicos referentes al hardware básico necesario, formas de instalación, configuración inicial y servicios base con su respectivo tutorial. Así mismo, dada la popularidad que tienen en el campo de servicios para redes, poco a poco su comunidad ha ido creciendo para aportar constantes actualizaciones y nuevas funcionalidades.

2.1.1 OPNSENSE

Es un proyecto de código abierto desarrollado a partir de FreeBSD, un sistema operativo utilizado para funcionalidades de red avanzadas, seguridad y almacenamiento, popular en servidores y plataformas embebidas [20]. Incluye gran cantidad de características que algunos UTM comerciales ofrecen, lo que lo hace una alternativa importante en el campo de la Seguridad Informática [21].

Ofrece múltiples servicios entre los cuales destacan: firewall, monitoreo de tráfico, VPN, IDS, etc. OPNsense puede encontrarse preinstalado en equipos de hardware dedicado ofertado por la empresa Deciso, desde equipos para uso simple hasta más complejos con alta disponibilidad.

2.1.2 PFSENSE

Distribución personalizada a partir de FreeBSD, nace en el 2004 como una bifurcación de m0n0wall, otro sistema de código abierto disponible inicialmente para plataformas embebidas. En un inicio pensado solamente para ofrecer los servicios de firewall y enrutador, sin embargo, a través del tiempo ha ido evolucionando hasta implementar más funcionalidades.

Actualmente se lo presenta como un sistema gratuito de código abierto, orientado a dispositivos de tipo hogar u oficinas pequeñas, incluso con ediciones para servidores de gran tamaño, con servicios para la administración de la seguridad en una red. No es necesario tener un conocimiento en FreeBSD para desarrollar o usar el software en cuestión [22].

2.1.3 CLEAROS

Sistema operativo basado en CentOS que puede ser ejecutado sobre hardware dedicado, así como en ambientes virtuales para un hogar o una oficina, contiene servicios orientados a los ambientes de TI; siendo estos: Gateway, servidor de archivos, soluciones de firewall, entre otras [23]. Ofrece soluciones para trabajar fácilmente con servidores que no sean ClearOS, mejorando así la interoperabilidad entre sistemas diferentes.

2.1.4 ENDIAN

Catalogado como un Gestor Unificado de Amenazas (UTM) de distribución GNU/Linux, es un software de código abierto con una interfaz web simple que incorpora servicios de firewall, VPN, seguridad para correo y web, entre otros. Es un software que también puede ser implementado en hardware dedicado [24].

2.2 REQUERIMIENTOS DE HARDWARE

La información ha sido extraída desde la documentación web de cada sistema para elaborar dos tablas comparativas, que abarcan a los cuatro sistemas a estudiar, las tablas incluyen información sobre los requerimientos mínimos y recomendados [25], [26], [27], [28] y [29].

Detallando la información presentada en la Tabla 2.1. los sistemas pueden ser implementados en un computador básico que contenga lo que se incluye en la lista, siendo la unidad lectora de CD/DVD opcional en caso de que no se lo utilice como medio de instalación. Por otro lado, los puertos USB son necesarios para conectar los periféricos de entrada, sin embargo, esto sólo es necesario para instalar el sistema operativo, luego la administración se la realizará remotamente por medio de la red.

El monitor es indispensable para la instalación del sistema operativo y para la configuración básica de red, luego la configuración se la puede realizar ingresando por medios remotos. En caso de que el equipo se conecte únicamente a la red local, no existe inconveniente en utilizar una sola interfaz de red.

Tabla 2.1. Requerimientos mínimos de los sistemas

	OPNsense	**pfSense**	**ClearOs**	**Endian**
RAM	2GB	512 MB	1 GB	2 GB
HDD/SSD	4 GB	4 GB	10 GB	8 GB
Procesador	Dual-core 1 GHz	amd64 (x86-64) de 64 bits	CPU 64 bits	(x86_64) 1 GHz
USB	Uso de periféricos y medios de instalación			
CD/DVD-ROM	Sólo si se utiliza como medio de instalación			
Interfaces de red	1	1	1	1
Monitor	Sólo durante la instalación y configuración inicial			

La Tabla 2.2. muestra los requerimientos necesarios que cada desarrollador solicita para que el sistema garantice el funcionamiento óptimo. En el caso de que el equipo cumpla con el rol de enrutador, se necesitarán al menos 2 interfaces de red, una para LAN y otra para WAN.

Adicionalmente, algunos sistemas también ofrecen servicios para una interfaz inalámbrica, esto no es necesario en un principio, pero también puede ser implementado. Más adelante,

se buscarán al menos dos alternativas de equipos que reúnan las características del hardware necesario mostrado en las tablas, para ser analizadas y estudiadas.

Tabla 2.2. Requerimientos recomendados de los sistemas

	OPNsense	**pfSense**	**ClearOs**	**Endian**
RAM	8 GB	1 GB	4 GB	4 GB
HDD/SSD	120 GB	8 GB	20 GB	20 GB
Procesador	CPU multinúcleo de 1,5 GHz	amd64 (x86-64) 64 bits	Dual-Core 64 bits	Dual-core 2 GHz
USB	Uso de periféricos y medios de instalación			
CD/DVD-ROM	Solo si se utiliza como medio de instalación			
Interfaces de red	2 o más	2 o más	1 o más	1 o más
Monitor	Sólo durante la instalación y configuración inicial			

2.3 AMBIENTE DE VIRTUALIZACIÓN

Cumpliendo con los requerimientos mínimos necesarios para ejecutar los sistemas, con las imágenes descargadas desde las webs oficiales de cada proveedor, se probarán cada uno de los sistemas unificados en un ambiente de virtualización.

Todas las máquinas han sido creadas con las características mostradas en la Figura 2.1., el adaptador de red es del tipo Puente (en inglés, Bridged) para que pertenezca a la misma red del computador anfitrión. Es necesario mencionar los sistemas OPNsense y pfSense, en su configuración inicial tratan de identificar al menos dos interfaces de red correspondientes a WAN y LAN, sin embargo, esto se puede omitir.

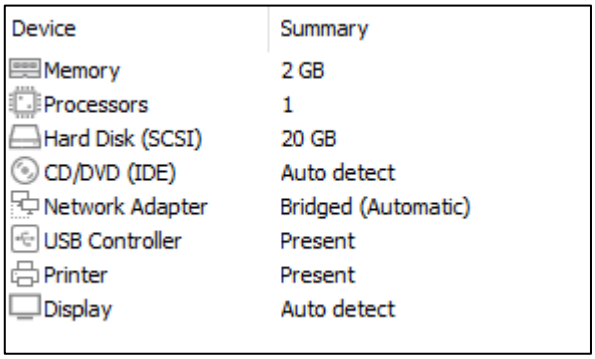


Figura 2.1. Características de hardware del ambiente de virtualización

2.3.1 INSTALACIÓN

En todos los casos, las imágenes ISO para la instalación han sido descargadas desde la página de cada desarrollador, las cuales pueden ser instaladas desde medios CD-ROM/DVD-ROM o desde dispositivos de almacenamiento USB. Las ediciones correspondientes son del tipo community, es decir, ediciones de distribución gratuita que tienen ciertas limitaciones o que no ofrecen todos los servicios disponibles, sin embargo, dichas funcionalidades pueden ser añadidas por usuarios con los conocimientos suficientes para realizarlo.

2.3.1.1 OPNsense

Una vez elegida como opción de arranque el sistema a instalar a través de medios USB o CD/DVD, el asistente de preparación para la instalación comenzará automáticamente. Después de unos minutos se le pedirá al usuario que ingrese las credenciales para poder acceder a la pantalla de instalación, siendo estas: el usuario <installer> con la contraseña <opnsense> de acuerdo con [30].

Cuando se ingresa a la pantalla principal de instalación, se presentarán algunas pantallas secuenciales de configuración y preparación para la instalación:

1. Sección de distribución de idioma de teclado.
2. Modo de instalación y particionamiento.
3. Asignación de nueva contraseña para el usuario <root>.
4. Progreso de Instalación.
5. Pantalla de instalación finalizada y opción de reiniciar.

La Figura 2.2. presenta las pantallas antes mencionadas correspondientes a los literales 2 y 4.

Figura 2.2. Pantallas de instalación de OPNsense

2.3.1.2 PfSense

La instalación de pfSense es bastante similar en el estilo gráfico a OPNsense, con pantallas secuencias, no obstante, se presentan algunas diferencias [31].

1. La pantalla inicial es un acuerdo de licencia con los términos por parte de pfSense.
2. Pantalla de bienvenida incluye una orden para instalar o realizar operaciones de recuperación del sistema por Interfaz de línea de comandos (del acrónimo en inglés CLI, Command-Line Interface) para usuarios avanzados.
3. Pantalla de selección de distribución de teclado.
4. Selección del sistema de archivos y tipo de particionamiento.
5. Pantalla de progreso de instalación.
6. Al finalizar la instalación se pregunta al usuario si desea realizar modificaciones adicionales utilizando la CLI.
7. Pantalla de finalización de instalación y reinicio.

La Figura 2.3. muestra las pantallas correspondientes a los literales 2 y 4.

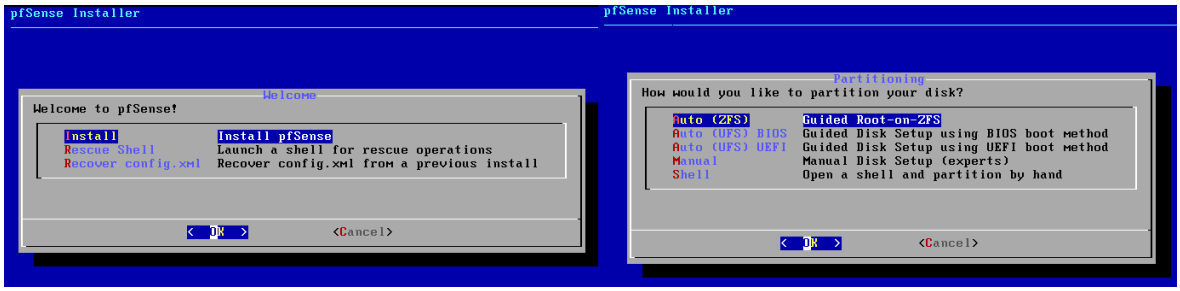


Figura 2.3. Pantallas de instalación de pfSense

2.3.1.3 ClearOS

Algunas consideraciones por parte del desarrollador son que, si se va a realizar la instalación en un ambiente virtualizado, tranquilamente se lo puede realizar con requerimientos mínimos de RAM de 1GB y HDD de 5GB, recursos suficientes de los que se dispone de acuerdo a la Figura 2.1.

ClearOS en su pantalla de arranque incluye las opciones de:

- Instalar el sistema como tal.
- Instalar el sistema en un ambiente de prueba.
- Realizar una corrección de errores.

Si se decide continuar con la instalación normal, se pueden apreciar las siguientes pantallas con un modo gráfico.

Como primera pantalla se tiene la de selección de distribución de teclado. Luego se muestra la pantalla de Configuración de instalación que corresponde con exactitud a la misma utilizada en sistemas Linux CentOS para servidores, que a su vez se basan en GNU/Linux Red Hat, por consiguiente, en caso de tener experiencia instalando sistemas de este tipo, la interfaz resultará bastante intuitiva. Estas dos pantallas mencionadas se muestran en la Figura 2.4.

Figura 2.4. Pantallas de instalación de ClearOS

Las configuraciones principales para tomar en cuenta son:

1. Fecha y Hora (zona horaria).
2. Origen de instalación (medio de instalación del sistema).
3. Selección de software (elementos adicionales a ser instalados).
4. Destino de Instalación.
5. Red y nombre de equipo.

Siendo el punto 4 no opcional. Es necesario elegir el destino de la instalación, es decir, la ubicación en la que se realizará la instalación y el tipo de partición, en caso de tener suficiente experiencia en estos temas. Así mismo, se recomienda asignar una contraseña para el usuario <root>, estas credenciales serán necesarias para ingresar al servidor.

De preferencia se puede configurar la red para poder acceder luego por interfaz web, sin embargo, en caso de no realizarlo, posteriormente se lo puede realizar sin problema alguno [32].

Una vez finalizada la instalación se le mencionará al usuario que reinicie el equipo y que retire el medio de instalación para evitar que vuelva a arrancar la pantalla de instalación accidentalmente.

2.3.1.4 Endian

Las pantallas de instalación de Endian, al igual que en OPNsense y pfSense, aparecen de manera secuencial de la siguiente forma:

1. Selección de idioma: inglés (por defecto), alemán e italiano.
2. Pantalla de bienvenida con confirmación para proseguir con la instalación.
3. Confirmación de particionamiento en HDD con advertencia de borrado de datos en ese medio de almacenamiento.
4. Progreso de instalación.
5. Habilitación de puerto de consola utilizando una interfaz serial.
6. Configuración de IP para la parte LAN.
7. Progreso de post-instalación.
8. Pantalla de finalización de instalación con información relevante para ingresar por medio de un navegador web.

Detallando un poco el literal 6, en Endian se maneja el concepto de Zonas: Red (WAN), Green (LAN), Orange (DMZ) y Blue (WIRELESS), por lo tanto, la dirección IP que se solicita al usuario en ese literal, corresponde al de la red LAN mediante la cual se puede acceder remotamente [33].

La Figura 2.5. muestra las pantallas correspondientes a los literales 2, 3 y 6.

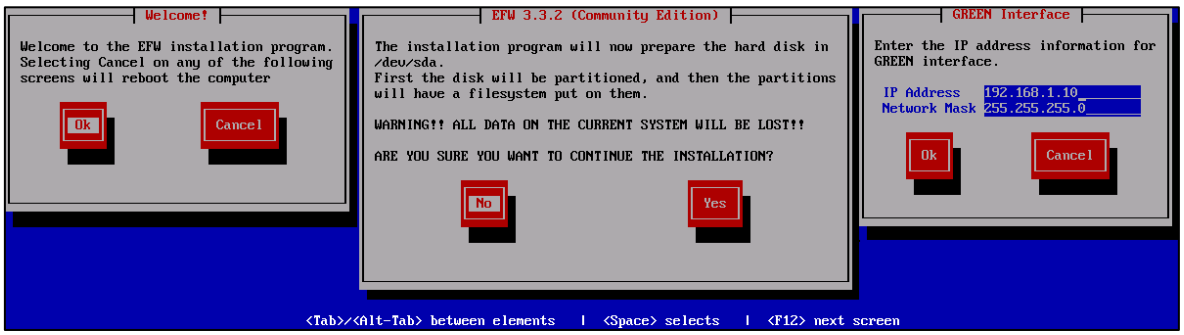


Figura 2.5. Pantallas principales de instalación de Endian

Al finalizar con la instalación, se mostrará una pantalla con la dirección IP configurada seguida del puerto por defecto, 80 para http y 10443 para https, mediante los cuales se puede ingresar a la interfaz web.

2.3.2 PRIMER USO Y CONFIGURACIONES

Después de completar la instalación de los sistemas operativos, es momento de iniciar cada sistema por primera vez y dar un breve vistazo a las configuraciones iniciales, observando con atención el alcance de sus opciones básicas a nivel de servidor y a nivel de interfaz web.

2.3.2.1 OPNsense

La pantalla de bienvenida muestra información de las interfaces WAN y LAN, nombre del dominio y una línea de comandos para ingresar con las credenciales necesarias, en este caso: usuario <root> con la contraseña <opnsense> [30]. La Figura 2.6. presenta el menú principal de configuración después de ingresar las credenciales correctamente.

Unos de los puntos de interés en este menú, es el de poder actualizar el sistema de dos formas distintas:

1. Ingresando la opción 8) Shell y escrbiendo “opnsense-update”.
2. Ingresando directamente a la opción 12) Update from console.

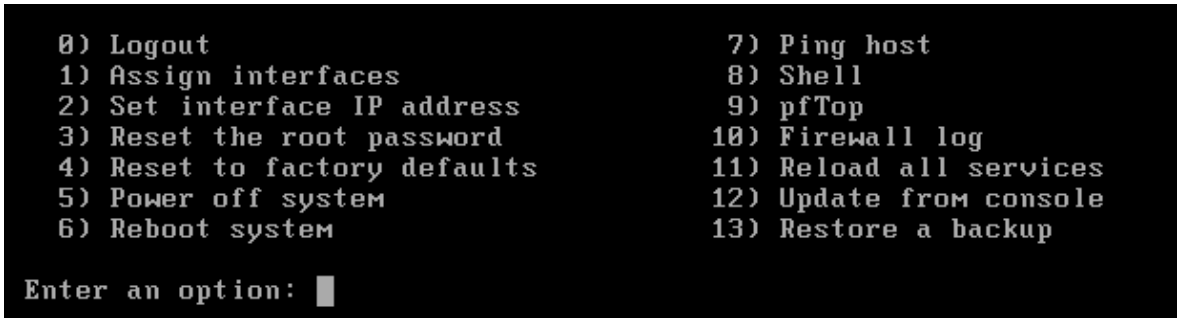


Figura 2.6. Menú de consola de OPNsense

Se procede a configurar los adaptadores de red reconocidos y así ingresar mediante interfaz web al resto de configuraciones posteriormente. Las interfaces de red por defecto son dos: LAN y WAN, para lo cual en la máquina virtual se añade otro adaptador de red, esto con fines de pruebas. Ingresando la opción 2 y siguiendo el asistente, se configurará la dirección IP 192.168.1.11 en la interfaz LAN, con lo cual se puede ingresar a la configuración web desde cualquier navegador. Adicionalmente, se piden otros datos de entrada como la opción de utilizar un servidor DHCP o cambiar el protocolo https a http, entre otros.

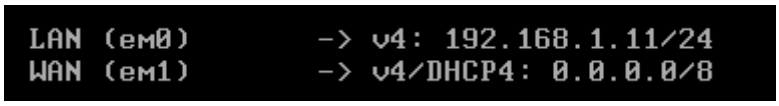


Figura 2.7. Interfaces de red de OPNsense

Ingresando a la dirección IP configurada y utilizando las credenciales previamente mencionadas, se le recibirá al usuario con un asistente de configuración, el cual es una especie de guía para la configuración inicial. El asistente permite la configuración de idioma, DNS, zona horaria, configuración de interfaces WAN y LAN, actualización de la contraseña de usuario root, entre otras.

Figura 2.8. Interfaz web principal de OPNsense

La Figura 2.8. muestra la pantalla web principal después de haber finalizado el asistente de configuración inicial. Los elementos que componen esta pantalla son:

En la parte izquierda se encuentra situado el Área de menús, con elementos clasificados por niveles de categoría y niveles de funciones o funcionalidades, siendo algunos de ellos desplegables, por ejemplo, la categoría Lobby y una de sus funciones contenidas, el Panel de control o panel de resumen. Haciendo clic en el logo de OPNsense, se redirige al Dashboard o panel de resumen, en el cual se encuentran los widgets, información respecto a la licencia, al sistema, etc.

También se puede hacer uso del cuadro de búsqueda para acceder a lugares existentes que no pueden ser encontrados a simple vista. Cuando se ingresa a alguna función, se pueden encontrar los formularios de configuraciones [34].

2.3.2.2 PfSense

Por defecto se tienen algunas configuraciones iniciales [35]:

- Interfaz WAN como cliente DHCP para IPv4 e IPv6.
- Interfaces LAN con una dirección IPv4 estática igual a 192.168.1.1/24.
- Todas las conexiones de entrada a la WAN se encuentran bloqueadas por defecto en el firewall.
- Todas las conexiones salientes desde la LAN se encuentran permitidas.
- NAT sobre tráfico saliente IPv4 de la WAN desde la subred LAN.
- SSH deshabilitado.

Por otro lado, la pantalla principal mostrado en Figura 2.9. dispone de elementos similares a los vistos en el sistema anterior, sin embargo, se puede notar que se tiene un mayor número de opciones a la elección del usuario. Al ingresar a la opción 2 se puede configurar las interfaces WAN y LAN, siendo la dirección IP 192.168.1.12 la escogida para la interfaz LAN.

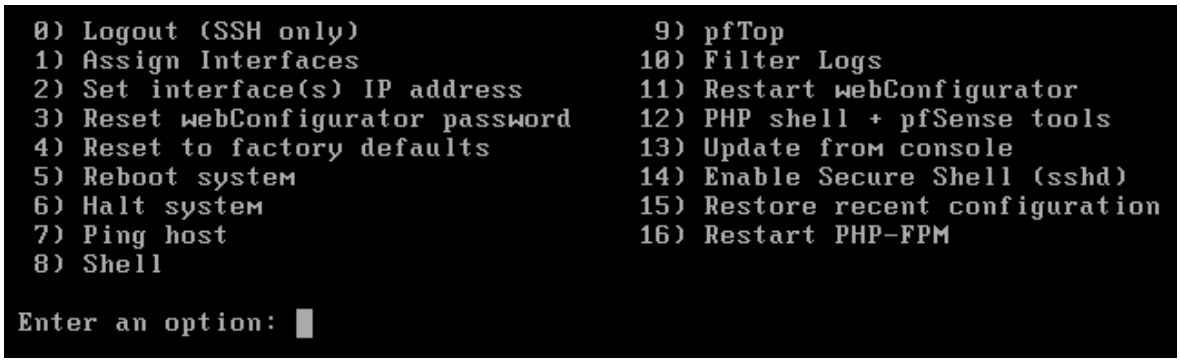


Figura 2.9. Menú principal de configuración de pfSense

Siguiendo el asistente de configuración se pueden asignar direcciones IP para ambas interfaces, habilitar el servidor DHCP, entre otros. Con esto se habilitará el acceso web al sistema y ya se podrá acceder mediante un navegador web.

Una vez iniciada sesión con las credenciales <admin> y la contraseña <pfsense> [36], se tiene acceso a un primer vistazo de la interfaz web de pfsense, de igual forma, se presenta un asistente que ayudará con las configuraciones básicas. Información general como nombre de equipo, configuración de zona horario y NTP, DNS, interfaces LAN y WAN, son configuraciones realizables desde el asistente.

La Figura 2.10. muestra la interfaz web principal, una vez finalizado el asistente de configuración inicial, aquí se pueden encontrar el área de menús en la parte principal y en

caso de hacer clic sobre el logo de pfSense, se puede visualizar el panel de resumen del servidor.

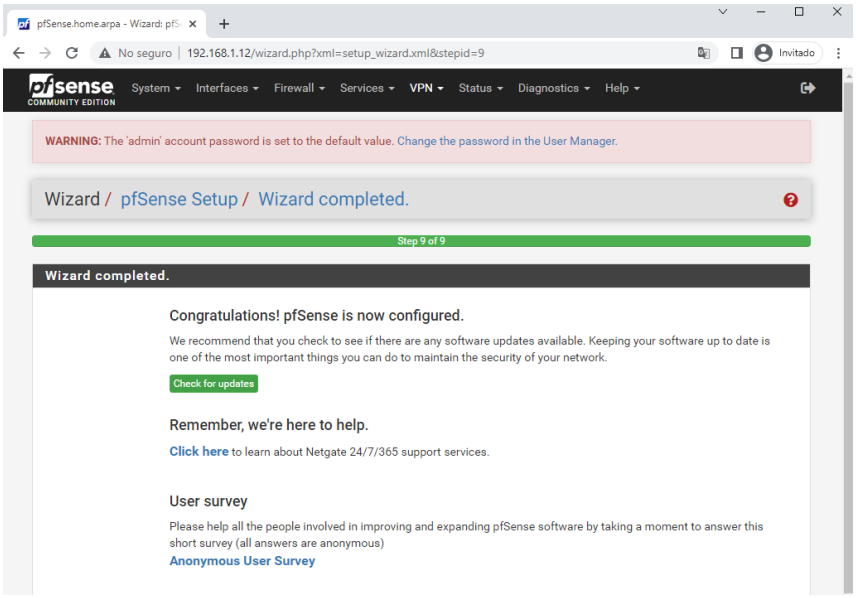


Figura 2.10. Interfaz web principal de pfSense

2.3.2.3 ClearOs

La pantalla inicial que se muestra en el servidor, a diferencia de los sistemas anteriores, tiene una interfaz gráfica, desde la cual es posible acceder a la mayoría de las configuraciones de red, además cuenta con un acceso al modo CLI para realizar cualquier configuración por medio de línea de comandos. Este equipo tiene la dirección 192.168.1.13 y se accede mediante el puerto 82. Las credenciales de ingreso corresponden a aquellas escogidas durante la parte de instalación, en este caso son usuario <root> y la contraseña configurada durante la instalación <1234>.

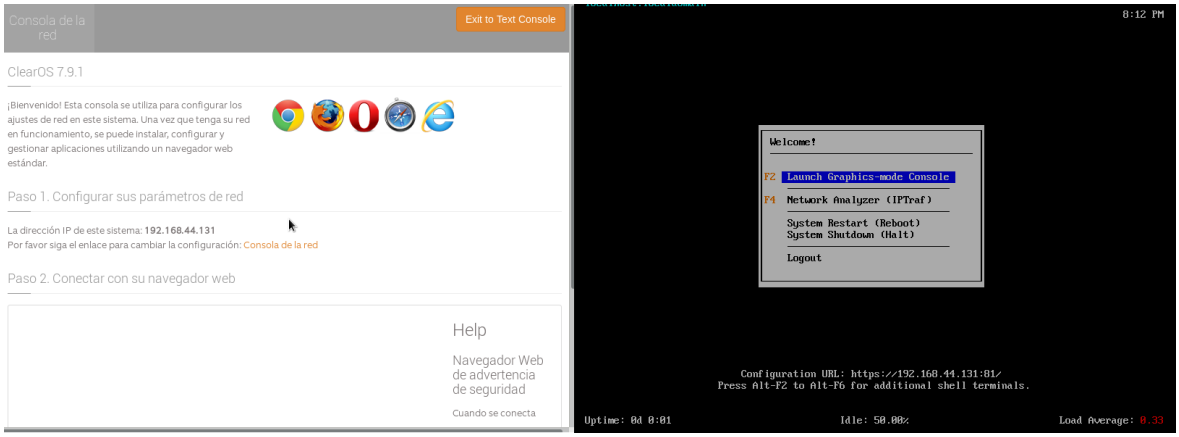


Figura 2.11. Pantallas principales desde el servidor de ClearOS

Después de ingresar al modo web desde un navegador, se accederá a un asistente en el cual se puede escoger el modo de red (servidor público, modo puerta de enlace, modo servidor privado), interfaces de red, servidores DNS, ediciones (Community, Home y Bussines), sistema de registro (no se puede omitir, es necesario crear una cuenta y por medio de esta se accede al Market), Al registrar el equipo se ha seleccionado un tamaño de personal igual a 10 personas, el software tiene una vigencia de 2 años. Antes de finalizar el asistente, es obligatorio descargar y actualizar el sistema, este proceso puede tomar varios minutos. Entre ellas se encuentran: el servidor dhcp, administrador de cuentas, dashboard, hora y fecha y ajustes generales.

El dashboard es totalmente personalizable y por defecto se tienen los servicios de firewall, servidores DHCP, DNS y SSH. Si se requiere de algo adicional se lo puede buscar e instalar desde el Market.

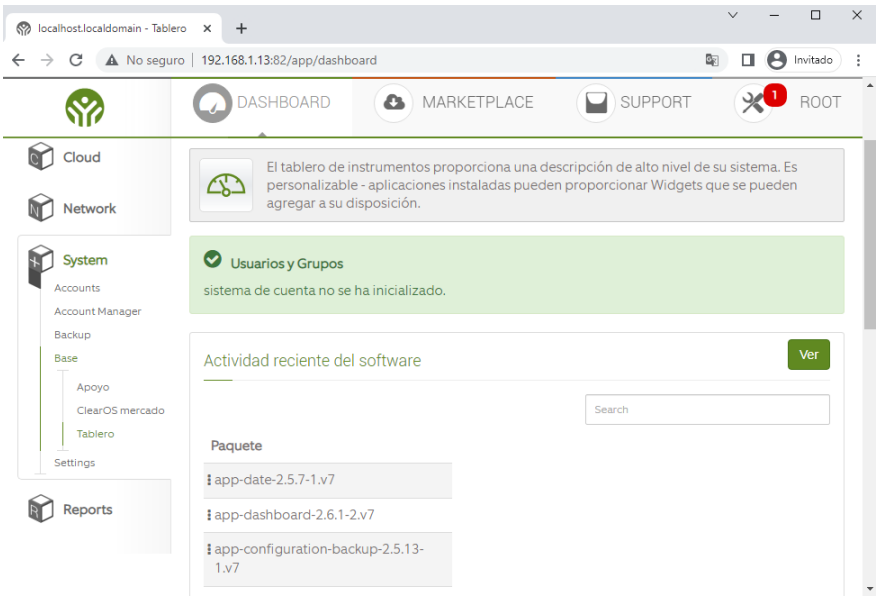


Figura 2.12. Interfaz web principal de ClearOS

La Figura 2.12. muestra la pantalla principal, en la cual los servicios se listan en la parte izquierda y en la parte superior se tiene acceso al panel de resumen y al Market. Algunos controles pueden personalizarse para ser añadidos a la pantalla principal. En la parte superior derecha, se listan notificaciones pendientes.

2.3.2.4 Endian

En la pantalla principal se puede visualizar una interfaz del tipo línea de comandos con la zona GREEN perteneciente a la red LAN, desde esta pantalla se pueden realizar cambios de credenciales y de configuraciones de red. La contraseña por defecto es <endian>, cuando se ingrese por primera vez se pedirá crear una contraseña de mínimo 8 caracteres

para conectarse remotamente por SSH, para este caso se escogerá la contraseña “Endian2022”.

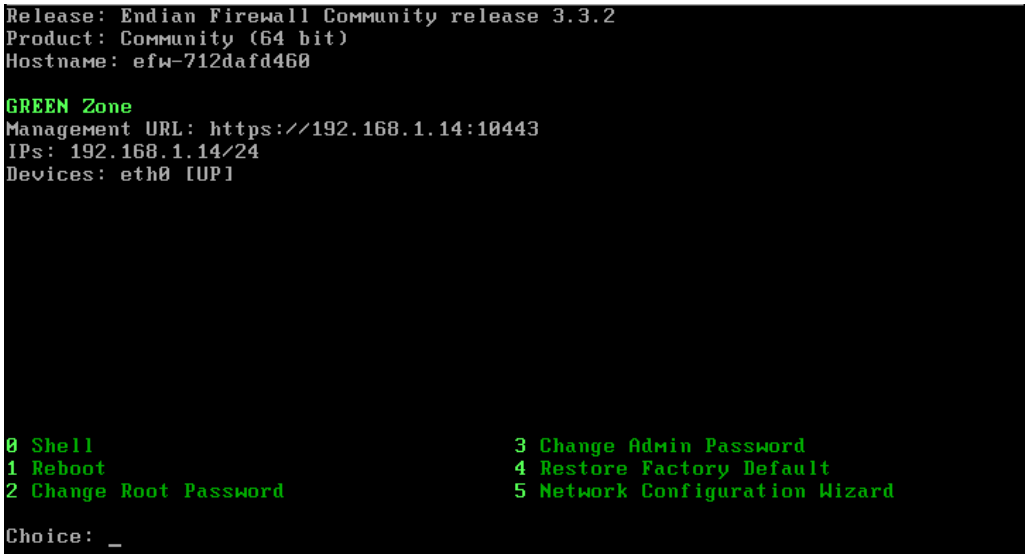


Figura 2.13. Pantalla principal en servidor de Endian

El asistente de configuración de red permite explorar las diferentes zonas para asignar las interfaces de red que se dispongan, así como sus direcciones IP, servidor DNS, etc. Al ingresar a la dirección IP 192.168.1.14 desde un navegador web, se pedirá al usuario que se registre para recibir actualizaciones gratuitas. Las credenciales para ingresar son “admin” y la contraseña “Endian2022” añadida anteriormente, mostrando así el dashboard. Los servicios que se incluyen son: firewall, proxy, vpn, ssh, servidor dhcp, etc.

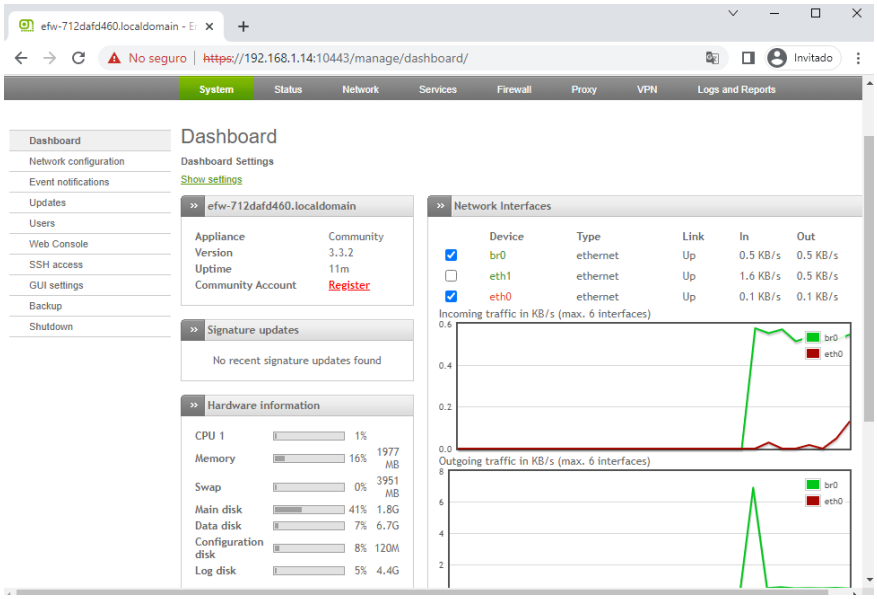


Figura 2.14. Interfaz web principal de Endian

2.4 SERVICIOS DE SEGURIDAD BÁSICOS

De la información revisada en el punto 1.4.3, se pueden analizar aquellos servicios que son fundamentales de acuerdo con la Arquitectura de seguridad por capas y estudiarlos respecto a cada sistema. Del perímetro y la red interna, principalmente se escogen los servicios de firewall, IDS e IPS, proxy y VPN. Sin embargo, también se añadirán aquellos servicios que resulten de interés dentro de los objetivos del trabajo.

2.4.1 OPNSENSE

2.4.1.1 Generalidades

En su pantalla principal OPNsense presenta un panel de control, también llamado dashboard o panel de resumen, del cual se pueden obtener datos respecto al nombre, la versión, actualizaciones disponibles, uso de los recursos del equipo, estado de los servicios, resumen de interfaces. Además, se incluye un área de menús con categorías y funcionalidades, en ellas se encuentran los servicios que se van a analizar a continuación.

2.4.1.2 Firewall

En el área de menús de se tienen los diferentes servicios que pueden ser configurados de acuerdo con lo que el usuario necesite (Figura 2.15.), una de sus categorías a revisar es la de Firewall, en ella se encuentran las funcionalidades comunes que se detallan a continuación [37]:

- Aliases (alias): listas de redes, equipos o puertos, utilizados para una mejor administración y uso de reglas.
- Categories (categorías): útil para el mantenimiento de grupos de reglas de mayor tamaño.
- Groups (grupos): orientado a la administración de interfaces, estás pueden combinarse y formar grupos.
- NAT (Network Address Translation): el conocido protocolo con el fin de traducir las direcciones de red es utilizado para compartir una dirección IP externa entre todos los dispositivos que conformen una red interna, es decir, separar las redes WAN y LAN. Necesario para que un equipo tenga salida a Internet.
- Rules (reglas): conjunto de reglas para permitir o denegar el tráfico desde alguna red hacia redes específicas.
- Shaper (conformado de tráfico): controla el tráfico de una red con el fin de garantizar su rendimiento, con la posibilidad de limitar el ancho de banda y retrasar paquetes de datos que cumplen con algún criterio en específico.

- Log Files (archivos de registro): proporciona información adicional a los problemas o acontecimientos que se presentan con el funcionamiento del firewall.

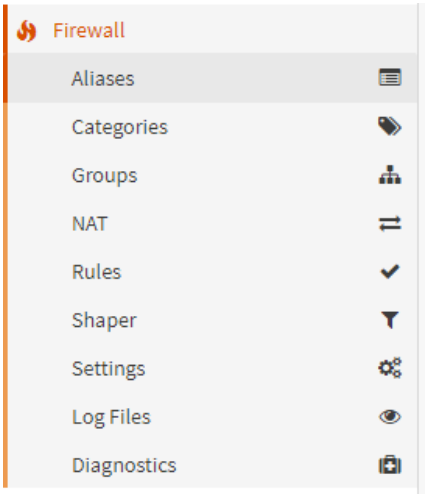


Figura 2.15. Lista de funciones de la categoría Firewall en OPNsense

La configuración de comunicación entre la red LAN y WAN por medio de NAT y las reglas que definen la comunicación interna hacia la externa, pero no viceversa, ya vienen por defecto como se muestra en la Figura 2.16.

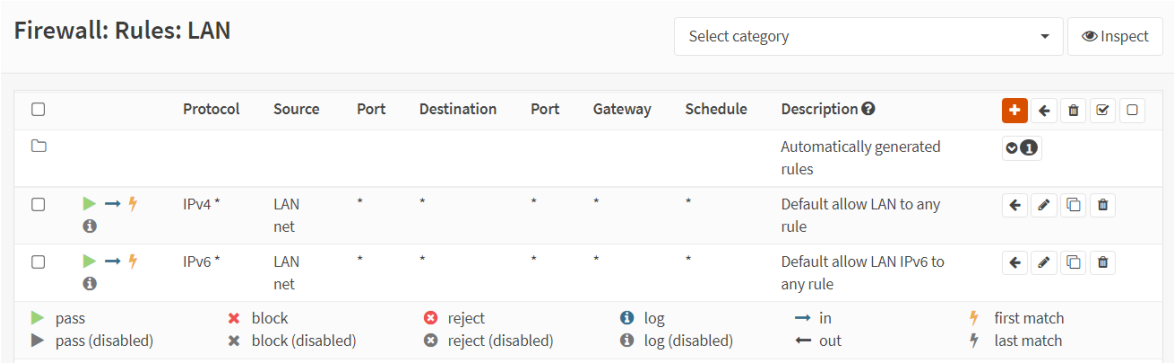


Figura 2.16. Reglas LAN de Firewall de OPNsense

Es necesario hacer énfasis en que los puntos de interés en este apartado son los de NAT, rules y traffic shaping, siendo las dos últimas las primordiales para administrar el tráfico que circula en la red por medio del firewall.

2.4.1.3 IDS e IPS

Se lo puede encontrar en la categoría Servicios. Detección de intrusiones está basado en Suricata, un software de código abierto encargado del análisis de red y la detección de amenazas [38]; además, en OPNsense, el servicio utiliza Netmap, para mejorar el

rendimiento y utilización del procesador. Es importante mencionar que Suricata funciona como un IDS e IPS, es decir, incluye ambas funcionalidades [39].

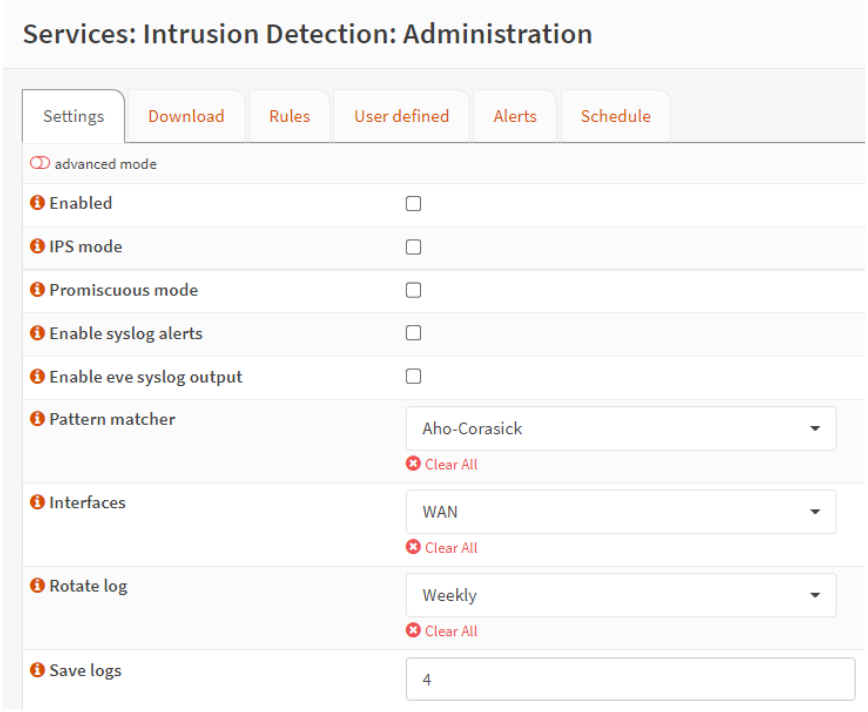


Figura 2.17. Pantalla principal de Administración de IDS/IPS de OPNsense

La Figura 2.17. muestra la pantalla de Administración del IDS/IPS, adicional a esta opción, se tienen políticas y archivos de registro. Sin embargo, la explicación se centrará en la pantalla principal de administración. El servicio puede configurarse sobre distintas interfaces, por lo que es importante definir cuál utilizar, cabe mencionar que cuando se utilizan direcciones IPv4 esto va de la mano con el protocolo NAT, es decir, si se requiere capturar tráfico de la interfaz WAN, sólo se visualizará aquel que parte después de la traducción realizada por NAT; así, es posible que no se tenga una alerta desde el equipo en cuestión sino directamente desde el firewall.

2.4.1.4 Servidor Proxy

Este se encuentra ubicado en la Categoría Servicios, dispone de cuatro opciones en su interior (**Figura 2.18**.):

- Administración: aquí se incluyen las opciones generales, como habilitar el servidor proxy y el uso personalizado de páginas de error, además de las que vienen por defecto.
- Logs de caché, acceso y almacenamiento.

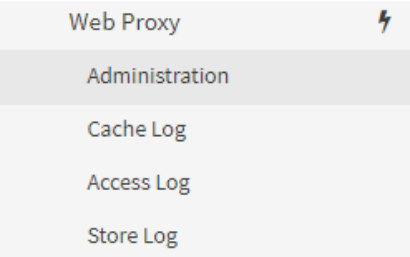


Figura 2.18. Menú de Web Proxy en OPNsense

2.4.1.5 VPN

Como servicio de VPN, OPNsense utiliza OpenVPN, que admite conexiones entre organizaciones o usuarios que se conectan remotamente. Adicionalmente, se ofrecen tecnologías como Ipsec, encargada de brindar mayor seguridad cuando se utilizan VPNs [40].

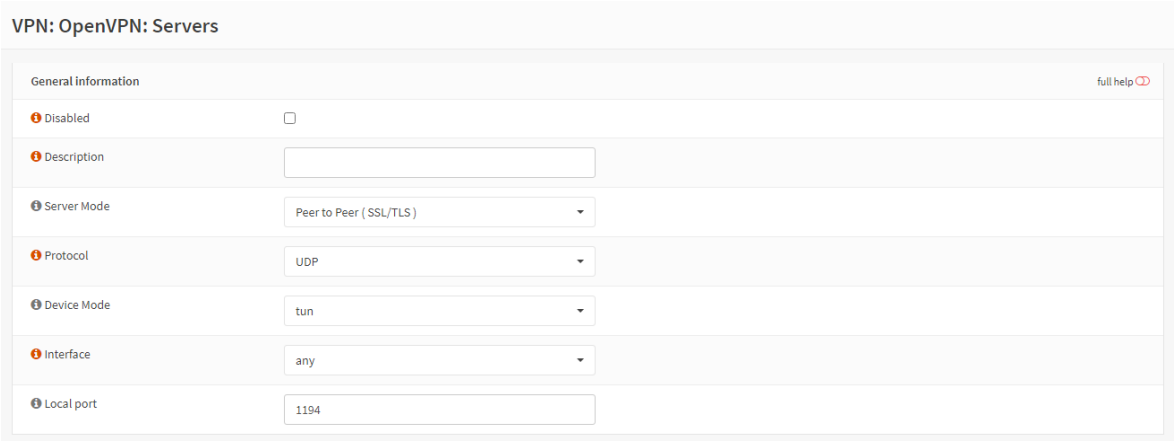


Figura 2.19. Pantalla de configuración de VPN en OPNsense

2.4.1.6 Herramientas adicionales

2.4.1.6.1 Informes

OPNsense ofrece la posibilidad de recopilar información acerca del estado del sistema como tal. De la información recolectada de datos primarios como: paquetes, calidad, sistema y tráfico, se puede generar cuadros de estadísticas que muestran información acerca de la salud del sistema, esto incluido en la categoría Reporting [41].

2.4.1.6.2 Usuarios

Mediante el administrador de usuarios, ubicado en la categoría System, funcionalidad Access, permite controlar el acceso que tienen los usuarios nuevos o aquellos que deberían tener un rol limitado [42].

2.4.1.6.3 Portal cautivo

Ubicado dentro de la categoría Services, permite forzar la autenticación para acceder a la red. Esto utilizado en redes inalámbricas como capa adicional de seguridad para el acceso a internet [43]

2.4.2 PFSENSE

2.4.2.1 Generalidades

La pantalla de bienvenida incluye datos del usuario autentificado, nombre de equipo, características generales de hardware, usos de los recursos del equipo, tipo de licencia del sistema, estado de las interfaces, etc. En la parte superior se tienen los menús que engloban los varios servicios que presenta pfSense.

2.4.2.2 Firewall

De acuerdo con la Figura 2.20. se pueden listar las funcionalidades que posee pfSense en su categoría Firewall, no se entrará en detalle de cada una dado que coincide en su mayoría con las ya presentadas en OPNsense. Como punto de interés se tiene una nueva funcionalidad, Virtual IPs; de acuerdo con [44] pfSense permite el uso de varias direcciones IP que trabajan junto con NAT o servicios locales, utilizando estás IP virtuales.

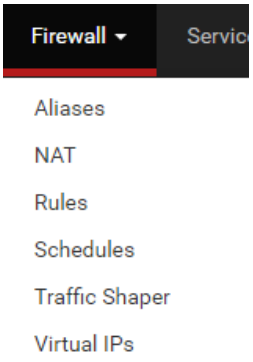


Figura 2.20. Menú Firewall en pfSense

La pantalla principal de configuración de reglas, al igual que OPNsense viene con reglas por defecto. Algo a mencionar es que la funcionalidad de Traffic Shaper incluye un asistente para ayudar con la configuración necesaria como se muestra en la Figura 2.21.

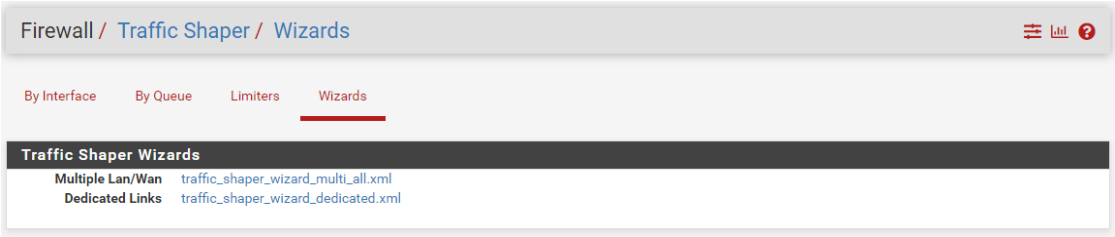


Figura 2.21. Funcionalidad de asistente de Traffic Shaper en pfSense

2.4.2.3 VPN

Pfsense ofrece el uso de OpenVPN, de IPSec y L2TP VPN. Una particularidad es que para la creación de un servicio VPN por medio de OpenVPN, se ofrece la posibilidad de utilizar un asistente. De acuerdo con la documentación de pfSense, se recomienda usar IPSec junto con L2TP VPN, dado que este último no posee las suficientes seguridades en la transferencia de la información.

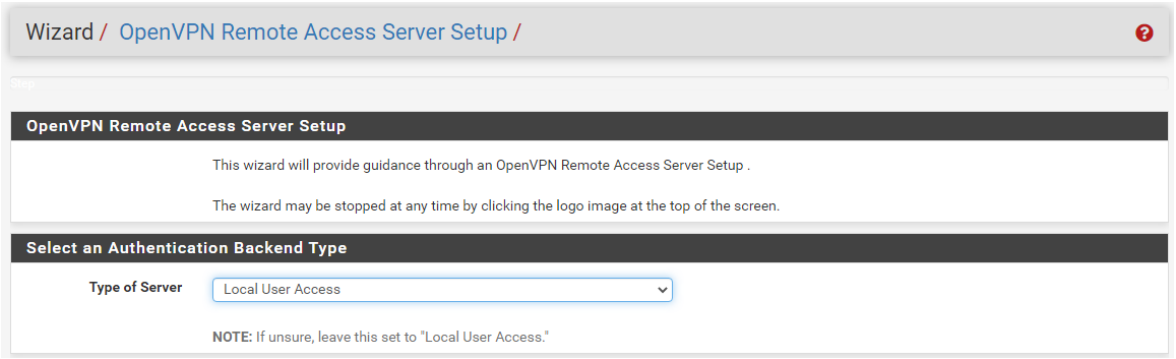


Figura 2.22. Asistente de configuración de VPN con OpenVPN en pfSense

2.4.2.4 Herramientas adicionales

2.4.2.4.1 SNMP (Simple Network Management Protocol)

Utilizado para el monitoreo remoto del equipo que implementa el servicio, el protocolo simple de administración de red permite consultar información del dispositivo administrado para obtener datos generales de: tráfico de red, información general del sistema, uso de procesador, memoria y almacenamiento [45].

2.4.2.4.2 Package Manager

Por medio del administrador de paquetes, se puede obtener información de funcionalidades instaladas o aquellas que pueden ser añadidas adicionalmente, es decir, que pfSense no trae por defecto. Al instalar se puede visualizar una ventana informativa de línea de comandos con el estado de la instalación.

2.4.3 CLEAROS

2.4.3.1 Generalidades

El panel de resumen por defecto de ClearOS no incluye ningún widget, tampoco muestra información general del sistema o de los recursos del sistema, sin embargo, se lo puede personalizar para que más se adecúe a lo que requiera el usuario. Como parte del menú de opciones izquierdo, incluye 4 categorías principales:

- Cloud: aquí se incluyen actualizaciones a nivel general.
- Network: configuración de servicios de Firewall y servidores DNS, DHCP y SSH.
- System: administrador de cuentas, respaldos de sistema, tienda de aplicaciones y tablero resumen.
- Reports: registros exportables del historial de acontecimientos en el servidor.

2.4.3.2 Firewall

La pantalla de administración del firewall que tiene por defecto ClearOS se basa en permitir o bloquear las conexiones entrantes, creando reglas a nivel de Servicio, puertos o un rango de puertos (Figura 2.23.),

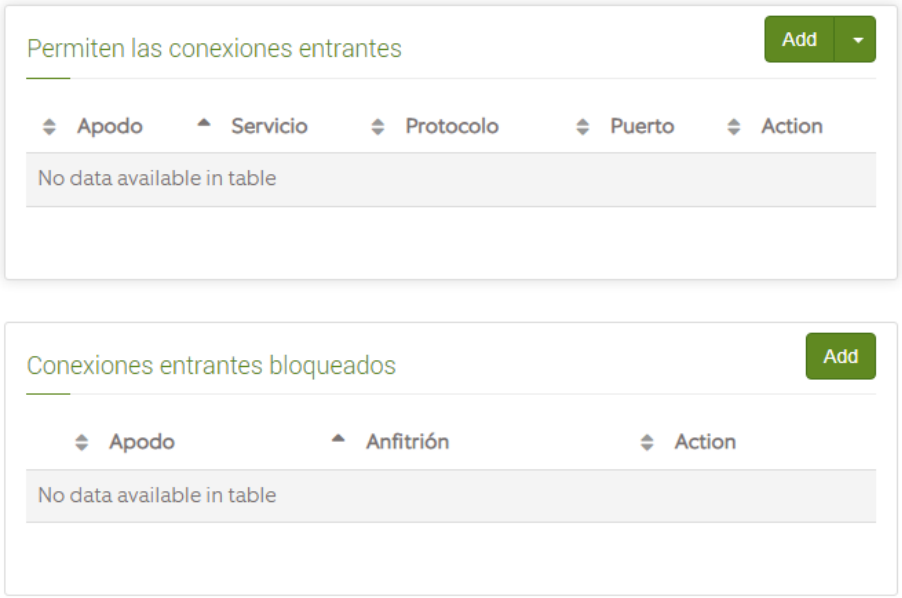


Figura 2.23. Pantalla de configuración de Firewall de ClearOS

2.4.3.3 Herramientas adicionales

2.4.3.3.1 Tienda de aplicaciones

ClearOS ofrece la posibilidad de añadir módulos de servicios de las 4 categorías antes mencionadas, por medio de su propia tienda de aplicaciones, aquí se pueden encontrar servicios gratuitos o también de paga (Figura 2.24.).

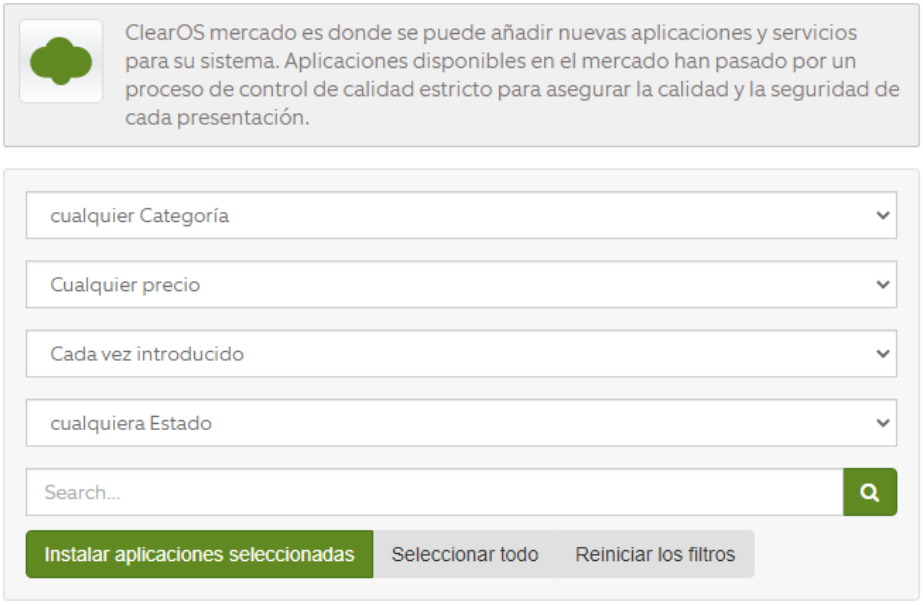


Figura 2.24. Tienda de aplicaciones de ClearOS

2.4.4 ENDIAN

2.4.4.1 Generalidades

La pantalla principal incluye el control principal con información relevante del uso de hardware, estado de interfaces y control de tráfico, estado de servicios, etc. Su área de menús se encuentra en la parte superior y a medida que se selecciona alguno, se muestran diferentes pantallas con más opciones.

2.4.4.2 Firewall

En Endian se incluyen funcionalidades para configurar NAT, tráfico saliente, entre zonas, tráfico VPN y diagramas de Firewall; imágenes que muestran el tipo de tráfico interceptado [46], al ingresar a cada funcionalidad se despliegan más configuraciones como se muestra en la Figura 2.25.

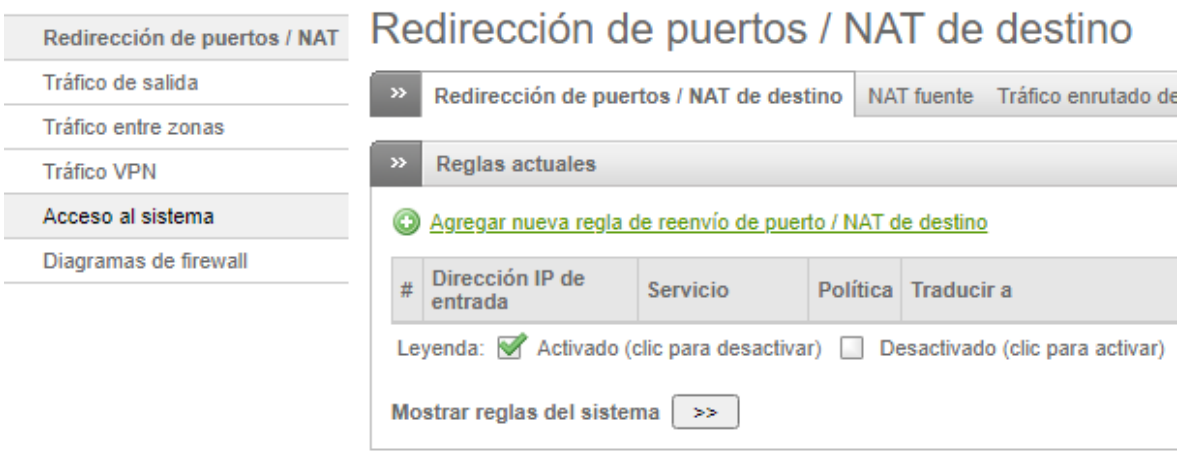


Figura 2.25. Funcionalidades del menú Firewall en Endian

2.4.4.3 IPS

Endian incluye los servicios de detección y prevención de intrusos, llamado Snort, software de código abierto que usa una serie de reglas para controlar la actividad maliciosa de la red, también, puede generar alertas para informar al usuario [47]. Las reglas se pueden obtener directamente de Endian o también por medio de un archivo que contenga reglas personalizadas [48].

Figura 2.26. Pantalla de configuración de IPS en Endian

2.4.4.4 Proxy

El servidor proxy incluye configuraciones para múltiples servicios, como se visualiza:

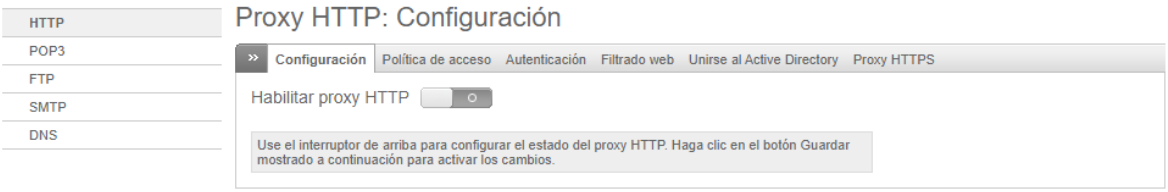


Figura 2.27. Pantalla de configuración de proxy en Endian

La Figura 2.27. muestra las opciones que el servidor proxy de Endian trae por defecto, siendo posible utilizar un proxy no solo para el protocolo HTTP, sino para POP3, FT, SMTP y DNS.

2.4.4.5 VPN

Admite la creación de redes virtuales utilizando el protocolo IPSec, compatible para clientes que ejecuten Microsoft Windows, Linux y MacOS. Dentro del menú se tiene el apartado para configurar un servidor VPN por medio de OpenVPN, un cliente, túneles VPN de conexiones L2TP utilizando IPSec, entre otros.

Figura 2.28. Pantalla de configuración de Servidor OpenVPN en Endian

2.4.4.6 Herramientas adicionales

2.4.4.6.1 Antivirus

El motor antivirus que trae por defecto es ClamAV, que puede usarse para escanear amenazas como virus y malware,

2.4.4.6.2 Monitoreo de tráfico

Se lo realiza con la herramienta ntopng, una vez que se habilita la opción aparecerá el vínculo a la interfaz de configuración i administración; se puede analizar el tráfico por computador, interfaz de redes locales [48].

2.5 HARDWARE NECESARIO

De acuerdo con lo ya mencionado en el apartado 2.2 REQUERIMIENTOS DE HARDWARE, se hará especial énfasis en los requerimientos mínimos del hardware necesario, por lo tanto, a continuación, se propone analizar dos alternativas de computadores de placa única.

2.5.1 INTEL NUC KIT NUC6CAYH

Tabla 2.3. Características de Intel NUC NUC6CAYH

Sistemas operativos soportados	Windows 10/11 64-bits
Procesador	Intel Celeron J4005 2.7GHz
Cantidad de núcleos	2
Memoria RAM	8 GB
Almacenamiento	Soporta HDD 2.5” SATA de cualquier capacidad
Interfaz inalámbrica	Intel Wireless AC 9462 + Bluetooth
Puertos USB	6
Puertos HDMI	2
Interfaz de red	Realtek 8111H-CG
Precio según Intel	$141.78
Precio aproximado en el país	$235.00 [49]

Extrayendo información de la página web del fabricante [50], se pudo sintetizar la información relevante respecto a la NUC NUC6CAYH en la Tabla 2.3., considerado como un computador de placa única de bajo costo. Adicionalmente, se obtuvo información de mercados web locales para incluir el precio aproximado de costo en el país.

Como puntos importantes se debe mencionar que la NUC dispone solo de una interfaz de red, por lo que podría ser utilizada únicamente para las funciones básicas de los sistemas; además, el disco duro no viene incluido, por lo tanto, es necesario adquirirlo adicionalmente.

2.5.2 RASPBERRY PI 4

Tabla 2.4. Características de Raspberry PI 4

Sistemas operativos soportados	Linux / Raspberry Pi OS
Procesador	Broadcom BCM2711 Quad Core 1.5GHz
Cantidad de núcleos	4
Memoria RAM	4 GB
Almacenamiento	Ranura microSD
Interfaz inalámbrica	Isuzu 802.11ac
Puertos USB	4 (2 USB 3.0 Y 2 USB 2.0)
Puertos HDMI	2 puertos micro-HDMI

Interfaz de red	1 gigabit Ethernet
Precio según Raspberry	$75.00 precio en EE. UU.
Precio aproximado en el país	$235.00 [51]

La información sintetizada para formar la Tabla 2.4. se la obtuvo de [52]. Al igual que el anterior computador de placa única revisado, este dispone de una sola interfaz red por lo que se asemejaría a la compatibilidad limitada con los sistemas como se lo mencionó anteriormente. El precio aproximado en el país posee una gran diferencia con respecto a su costo en otros lugares del mundo.

2.6 ANALISIS COMPARATIVO

2.6.1 CRITERIOS DE COMPARACIÓN

Con base en los apartados 2.3.1 INSTALACIÓN y 2.3.2 PRIMER USO Y CONFIGURACIONES, se pueden extraer ciertos criterios de comparación para elaborar una parte de la tabla de lista de verificación, siendo algunas de ellas:

- Entorno de instalación fácil de seguir.
- Uso de documentación para iniciar la instalación.
- Configuración de interfaz de red como parte de la instalación.
- Interfaz gráfica en el lado del servidor.
- Soporte de Interfaz de línea de comandos (CLI) en el servidor.
- Configuración de red desde el menú principal en el servidor.
- Asistente de configuración en Interfaz Web.
- Conjunto de servicios de seguridad básicos incluidos.
- Capacidad de añadir servicios adicionales.
- Panel de resumen con información relevante.

Del apartado 2.4 SERVICIOS DE SEGURIDAD BÁSICOS se pueden incluir todos los servicios revisados como parte de la misma tabla de comparación como lista de verificación, así como servicios adicionales de interés. A continuación, se enlistan los servicios tomados en cuenta:

- Firewall
- NAT
- Traffic Shaper
- Virtual IP
- Servidor Proxy

- IDS/IPS
- VPN
- IPSec
- Portal Cautivo
- Antivirus
- Servidor DHCP
- VLAN
- Servidor SNMP
- Servicios de Wireless

2.6.2 LISTA DE VERIFICACIÓN

Con la información incluida en el punto anterior, se elaboró un formato comparativo del tipo lista de verificación para comparar los sistemas de acuerdo con sus cualidades generales y servicios que implementan (revisar la sección ANEXOS).

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 RESULTADOS

3.1.1 TABLA COMPARATIVA

A continuación, se incluye la tabla comparativa con los resultados obtenidos en el capítulo anterior, y posteriormente se detallarán más a fondo sus elementos y los criterios de selección de las 2 alternativas.

Tabla 3.1. Tabla comparativa de Sistemas Unificados de Seguridad Informática

Nº	Criterios de comparación	OPNsense	pfSense	ClearOS	Endian
1	Entorno de instalación fácil de seguir	✔	✔	✔	✔
2	No es necesario el uso de documentación para seguir la instalación		✔	✔	✔
3	Configuración de interfaz de red como parte de la instalación			✔	✔
4	Interfaz gráfica en el lado del servidor			✔	
5	Soporte de Interfaz por la línea de comandos (CLI) en el servidor	✔	✔	✔	✔
6	Configuración de red desde el menú principal en el servidor	✔	✔	✔	✔

7	Asistente de configuración en Interfaz web	✔	✔	✔	
8	Conjunto de servicios de seguridad básicos incluidos	✔	✔		✔
9	Capacidad para añadir servicios adicionales Capacidad para añadir servicios adicionales		✔	✔	
10	Panel de resumen con información relevante	✔	✔	✔	✔
	Total	6	8	9	7
11	Servicios:				
	Firewall	✔	✔	✔	✔
	NAT	✔	✔		✔
	Traffic Shaper	✔	✔		✔
	Virtual IP		✔		
	Servidor Proxy	✔			✔
	IDS/IPS	✔		✔	✔
	VPN	✔	✔		✔
	IPSec	✔	✔		✔
	Portal cautivo	✔	✔		
	Antivirus			✔	✔
	Servidor DHCP	✔	✔	✔	✔
	VLAN	✔			✔
	Servidor SNMP		✔		✔
	Wireless	✔	✔		✔
	Total	11	10	4	12

Después de analizar los resultados de los sistemas, se observa que OPNsense, pfSense y Endian, tuvieron gran cantidad de puntos a favor en la lista de verificación desarrollada. No obstante, antes de presentar las 2 alternativas se detallarán cada uno de los puntos que conforman la tabla comparativa para justificar la decisión final.

3.1.2 CRITERIOS DE COMPARACIÓN

1. Entorno de instalación fácil de seguir: todas las opciones de sistemas destacaron aquí, todos los ambientes de instalación fueron intuitivos, haciendo que no sea necesario tener conocimientos especializados para la configuración de puntos específicos; se podría decir que se necesita saber sobre cómo hacer las particiones con respecto al almacenamiento, sin embargo, el asistente es muy claro y se pueden realizar de forma automática todos sus pasos.

2. No es necesario el uso de documentación para seguir la instalación: este punto va de la mano con el punto 1 y se refiere a que fue necesario buscar las credenciales del sistema OPNsense para iniciar la instalación, en cambio, el resto de sistemas necesita de las credenciales únicamente para ingresar a la interfaz web. Sin embargo, ClearOS tiene la opción de crear la contraseña durante la instalación.

3. Configuración de interfaz de red como parte de la instalación: ClearOS y Endian tienen la posibilidad de configurar la interfaz de red local durante la instalación, esto simplifica el acceso inicial haciendo posible ingresar directamente a la interfaz Web.

4. Interfaz gráfica en el lado del servidor: esto puede resultar favorable para usuarios que prefieren una interfaz gráfica para configuraciones básicas, ClearOS ofrece esta experiencia dando la opción de iniciar sesión y acceder a configuraciones sencillas en modo gráfico.

5. Soporte de Interfaz por la línea de comandos (CLI) en el servidor: este punto es algo que comparten todos los sistemas, pues, a pesar de que ClearOS tiene un modo gráfico desde el servidor, también se puede utilizar la línea de comandos para usuarios que son más experimentados en el tema, favorablemente todos los sistemas soportan dicha cualidad.

6. Configuración de red desde el menú principal en el servidor: si bien algunos menús se presentan de forma simple para que el usuario con pocos conocimientos pueda realizar configuraciones simples, la configuración de red no es la excepción. En términos de menor a mayor grado de complejidad, en primer lugar se tiene a ClearOS con su modo gráfico como se explicó en el punto 3; luego, se tiene a OPNsense y pfSense, que disponen de un asistente para realizar las configuraciones omitiendo aquellas de lo que no se tiene un mayor conocimiento pero cumpliendo con el objetivo de al menos configurar una dirección IP por interfaz de red; y por último, se tiene a Endian, donde es necesario revisar la documentación para comprender el término de zonas que utiliza y elegir aquellas que se requiere.

7. Asistente de configuración en Interfaz web: al ingresar con las respectivas credenciales por medio de un navegador web a la dirección IP configurada en la parte LAN de cada sistema, se tiene una pantalla principal que guía al usuario por configuraciones básicas para obtener el funcionamiento convencional del equipo de red. Esto es algo que Endian no trae, pero sus competidores si, lo que resulta importante considerando que es de mucha ayuda al usuario sin mayores conocimientos en el área.

8. Conjunto de servicios de seguridad básicos incluidos: durante el primer uso se pudo evidenciar que el sistema más incompleto es ClearOS, que posee limitados servicios en cuanto a seguridad en el contexto del trabajo se refiere. El resto de sistemas contiene gran cantidad de servicios que resultan atractivos a simple vista.

9. Capacidad para añadir servicios adicionales: en el punto anterior se comentó que ClearOS es una alternativa incompleta, no obstante, al utilizar la tienda de aplicaciones esto cambia por completo, ya que allí se ofrecen aquellos servicios que el usuario puede requerir, los cuales se encuentran en presentaciones gratuitas y de paga. PfSense en sus características dispone de algo similar, un administrador de paquetes, que de igual forma sirve para añadir funcionalidades que no se encuentran por defecto.

10. Panel de resumen con información relevante: también conocido como dashboard, en él se tiene información importante sobre el uso de recursos y/o características del sistema en cuestión. Se puede decir que las 4 alternativas disponen de uno, sin embargo, la que deja mucho que desear es la de ClearOS que, si bien puede usarse para agregar diferentes controles instalados, no alcanza la utilidad de los 3 sistemas competidores.

11. Servicios: se puede decir que es la parte de mayor relevancia en el trabajo, puesto que se necesitan de los servicios base mencionados en capítulos anteriores que garanticen el buen desempeño de la seguridad en una red computacional. En este punto resulta claro cuáles de los 4 sistemas serán considerados para ser las 2 alternativas a proponer.

3.1.3 ELECCIÓN DE LAS 2 ALTERNATIVAS

De acuerdo con los resultados obtenidos a lo largo del trabajo se seleccionan los sistemas unificados OPNsense y Endian como alternativas a ser implementadas en hardware de bajo costo, por ser las más completas en lo que a servicios de seguridad informática respecta. Por otro lado, pfSense también contiene herramientas muy útiles y la posibilidad de seguir expandiéndose gracias a su administrador de paquetes y de que dispone de asistentes de configuración en algunos de sus servicios. Finalmente, ClearOS puede llegar a tener los servicios necesarios por medio de su tienda de aplicaciones, su interfaz gráfica web resulta bastante atractiva y simple, por lo que también resultaría como una buena alternativa por debajo de los otros sistemas estudiados.

3.2 CONCLUSIONES

La información disponible acerca de Servicios Unificados de Seguridad Informática es abundante en foros web, que presentan listas de selección de varios softwares que pueden cumplir con el objetivo de garantizar un nivel básico de seguridad informática, en el contexto del trabajo se lo llama así, sin embargo, también se lo conoce como UTM (Unified Threat Management), no obstante, no se debe confundir con soluciones limitadas a funcionar únicamente como firewalls o enrutadores, ya que estos no reúnen todo lo requerido. Una vez discriminado este factor, la documentación de cada sistema ayudó a obtener información importante para el trabajo.

Las alternativas estudiadas en su mayoría son de código abierto, utilizando versiones del tipo community para obtener su medio de instalación y así poder probarlas en un ambiente de virtualización, todas ellas reúnen gran cantidad de herramientas que pueden llegar a ser útiles si previamente el usuario se informa adecuadamente por medio de documentación o tutoriales especializados.

En el trabajo de integración se utilizó la jerarquía de servicios de la arquitectura de seguridad por capas para elegir los servicios que debían ser analizados, este modelo es muy informativo en lo que respecta a herramientas necesarias para garantizar la seguridad en una red, aun así, se hace énfasis en que el factor más importante en una organización es el usuario y la capacidad y responsabilidad que tiene para manejar los medios tecnológicos a su disposición.

La comparación realizada ayudó a definir las 2 alternativas más tentativas en lo que respecta a un sistema unificado de seguridad informática, siendo estas OPNsense y Endian; sin embargo, esta comparación se realizó con criterios orientados a su complejidad en instalación y funcionalidad, es decir, en criterios pasivos en lo que respecta a las herramientas que posee cada sistema. Se espera que este trabajo sirva como punto de partida para que las alternativas sean probadas de forma activa con mayor énfasis en pruebas de penetración o vulnerabilidades, orientadas a cada sistema.

Los computadores de placa única presentados cumplen con los requerimientos mínimos para que funcionen las alternativas, esto apegado en lo mayormente posible a utilizar hardware de bajo costo; estos equipos tienen como singularidad la limitación en lo que a hardware interno se refiere, es decir, no tienen la posibilidad de incluir internamente más de una tarjeta de red. Sin embargo, en el mercado existen tarjetas de red que pueden ser conectadas por USB que también son de bajo costo, corrigiendo así esta problemática.

Los equipos propuestos son considerados como hardware de bajo costo, sin embargo, en el país esos precios fluctúan, haciéndolos más costosos; además, de acuerdo con la documentación de cada desarrollador de los sistemas unificados revisados, estos proponen adquirir equipos dedicados que ya incorporan sus sistemas, equipos orientados a brindar de seguridad a hogares u oficinas pequeñas, sin embargo, no se comercializan en el país.

3.3 RECOMENDACIONES

Si bien pfSense y ClearOS no fueron elegidas como alternativas, puede resultar subjetivo descartarlas como tentativas de alternativas basadas en los criterios que presenta el trabajo en cuestión, por lo tanto, es necesario probarlas en ambientes que se asemejen a un ambiente real, con clientes y con varias interfaces de red.

Los equipos físicos para probar las alternativas pueden ser computadores de escritorio que reúnan los requerimientos mínimos de los sistemas, incluso siendo ventajoso el usar redundancia por hardware o por software para aportar una medida básica de contingencia en caso de que el disco principal del servidor tenga un fallo.

Se debe estudiar a detalle, el funcionamiento de los servicios que ofertan los sistemas unificados, esto con el fin de comprobar activamente cuál es la mejor alternativa frente a ataques maliciosos que la ciberseguridad tiene identificados.

A pesar de que una red de hogar o de oficina pequeña no disponga de la infraestructura necesaria de red, se debe ser cuidadoso con las medidas de seguridad en lo que a usuarios respecta, siempre que se trabaja con información es necesario regirse a políticas que aseguren la seguridad informática de la organización y de sus colaboradores.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] M. Romero, G. Figueroa , D. Vera, J. Álava, G. Parrales, C. Álava, Á. Murillo y M. Castillo, Introducción a la seguridad informática y el análisis de vulnerabilidades, Alicante: 3ciencias, 2018.

[2] «Ciberseguridad. Una guía completa del concepto, tipos, amenazas y estrategias,» infosecurity Mëxico, [En línea]. Available: https://www.infosecuritymexico.com/es/ciberseguridad.html. [Último acceso: Abril 2022].

[3] «Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información,» Lisa Institute, 03 marzo 2021. [En línea]. Available: https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion. [Último acceso: Abril 2022].

[4] «¿Ciberseguridad o Seguridad de la información? Aclarando la diferencia,» ESET, 16 junio 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/. [Último acceso: Abril 2022].

[5] «¿Qué es la gestión unificada de amenazas (UTM)?,» Kaspersky, [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/utm. [Último acceso: Abril 2022].

[6] T. McGuiness, «Defense in Depth,» *SANS Institute,* 2021.

[7] «La seguridad por capas de Defense in Depth (DiD),» SOFTTEK, 02 Septiembre 2021. [En línea]. Available: https://softtek.eu/tech-magazine/cybersecurity/la-seguridad-por-capas-de-defense-in-depth-did/. [Último acceso: Abril 2022].

[8] R. Rojas, «Qué es la seguridad por capas y cómo se compone,» icorp, 23 febrero 2021. [En línea]. Available: http://www.icorp.com.mx/blog/que-es-la-seguridad-por-capas-y-como-se-compone/. [Último acceso: Abril 2022].

[9] G. Baca Urbina, Introducción a la seguridad informática, Distrito Federal: Grupo Editorial Patria, 2016.

[10] INCIBE, «¿Qué son y para qué sirven los SIEM, IDS e IPS?,» INCIBE, 03 Septiembre 2020. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips. [Último acceso: Abril 2022].

[11] «Gestión del ancho de banda | Software de monitoreo de ancho de banda de red - ManageEngine NetFlow Analyzer,» Manageengine.com, [En línea]. Available: https://www.manageengine.com/latam/netflow/gestion-ancho-de-banda.html. [Último acceso: Mayo 2022].

[12] welivesecurity, «Qué es una VPN y cómo funciona,» ESET, 10 septiembre 2012. [En línea]. Available: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/. [Último acceso: Junio 2022].

[13] «¿Qué es el Software Libre? - Proyecto GNU - Free Software Foundation,» Gnu.org, [En línea]. Available: https://www.gnu.org/philosophy/free-sw.es.html. [Último acceso: Junio 2022].

[14] «Intel NUC: ¿Qué es y para qué sirve?,» GEEKNETIC, 2020. [En línea]. Available: https://www.geeknetic.es/Intel-NUC/que-es-y-para-que-sirve. [Último acceso: Junio 2022].

[15] C. Bernal, Metodología de la investigación, Bogotá: Pearson, 2010.

[16] X. Pastor y C. Caicedo, ¿Cómo elaborar un trabajo final de máster?, Barcelona: UOC, 2016.

[17] T. S. Dutta, «Top 10 Best Open Source Firewall to Protect Your Enterprise Network 2022,» 9 Agosto 2022. [En línea]. Available: https://cybersecuritynews.com/best-open-source-firewall/. [Último acceso: Julio 2022].

[18] C. BasuMallick, «Top 10 Linux Firewall Solutions in 2021,» spiceworks, 20 julio 2021. [En línea]. Available: https://www.spiceworks.com/it-security/network-security/articles/top-10-linux-firewall-solutions/. [Último acceso: Junio 2022].

[19] ZEOKAT, «Versión Community Edition de moda,» VOZIDEA.COM, 29 septiembre 2013. [En línea]. Available: https://www.vozidea.com/version-community-edition-de-moda. [Último acceso: Julio 2022].

[20] FreeBSD, «The FreeBSD Project,» FreeBSD Foundation, [En línea]. Available: https://www.freebsd.org/. [Último acceso: Julio 2022].

[21] OPNsense, «Welcome to documentation! - Introduction,» OPNsense, [En línea]. Available: https://docs.opnsense.org/intro.html. [Último acceso: Julio 2022].

[22] «pfSense Documentation - Introduction,» Netgate, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/general/index.html. [Último acceso: Julio 2022].

[23] «ClearOS User Guide,» ClearCenter, 2020. [En línea]. Available: https://documentation.clearos.com/index:userguide7. [Último acceso: Julio 2022].

[24] Endian, «Endian UTM 3.0 Reference Manual,» Endian Docs, 17 Diciembre 2019. [En línea]. Available: http://docs.endian.com/3.0/utm/index.html. [Último acceso: Julio 2022].

[25] OPNsense, «Hardware sizing & setup - Hardware requirements,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/hardware.html. [Último acceso: Agosto 2022].

[26] pfSense, «pfSense Hardware Requirements and Guidance,» pfSense, [En línea]. Available: https://www.pfsense.org/products/. [Último acceso: Agosto 2022].

[27] Netgate, «pfSense - Minimum Hardware Requirements,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/hardware/minimum-requirements.html. [Último acceso: Agosto 2022].

[28] ClearCenter, «System Requirements,» ClearCenter, 2020. [En línea]. Available: https://documentation.clearos.com/content:en_us:7_b_system_requirements. [Último acceso: Agosto 2022].

[29] Endian, «System Requirements,» Endian Docs, [En línea]. Available: https://www.endian.com/products/network-security/software/. [Último acceso: Agosto 2022].

[30] OPNsense, «Initial Installation & Configuration,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/install.html. [Último acceso: Agosto 2022].

[31] Netgate, «pfSense - Perform the Installation,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html. [Último acceso: Agosto 2022].

[32] ClearCenter, «Installation of ClearOS,» ClearCenter, 2020. [En línea]. Available: https://documentation.clearos.com/content:en_us:7_b_installation_wizard. [Último acceso: Agosto 2022].

[33] Endian, «Getting Started - The zones,» Endian Docs, [En línea]. Available: http://docs.endian.com/3.0/utm/first.html#the-zones. [Último acceso: Agosto 2022].

[34] OPNsense, «General User Interface,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/gui.html. [Último acceso: Agosto 2022].

[35] Netgate, «pfSense Software Default Configuration,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/install/install-pfsense.html. [Último acceso: Agosto 2022].

[36] Netgate, «Connecting to the GUI,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/config/index.html. [Último acceso: Agosto 2022].

[37] OPNsense, «Firewall,» OPNsense, [En línea]. Available: https://docs.opnsense.org/firewall.html. [Último acceso: Agosto 2022].

[38] Suricata, «Suricata is far more than an IDS/IPS,» Suricata, [En línea]. Available: https://suricata.io/. [Último acceso: Agosto 2022].

[39] OPNsense, «Intrusion Prevention System,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/ips.html. [Último acceso: Agosto 2022].

[40] OPNsense, «Virtual Private Networking,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/vpnet.html. [Último acceso: Agosto 2022].

[41] OPNsense, «Reporting,» OPNsense, [En línea]. Available: https://docs.opnsense.org/reporting.html. [Último acceso: Agosto 2022].

[42] OPNsense, «Access / User Management,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/users.html. [Último acceso: Agosto 2022].

[43] OPNsense, «Captive portal & GuestNET,» OPNsense, [En línea]. Available: https://docs.opnsense.org/manual/captiveportal.html. [Último acceso: Agosto 2022].

[44] Netgate, «pfSense - Firewall,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-addresses.html. [Último acceso: Agosto 2022].

[45] Netgate, «SNMP,» Netgate Docs, [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/services/snmp.html. [Último acceso: Agosto 2022].

[46] Endian, «Firewall menú,» Endian Docs, [En línea]. Available: http://docs.endian.com/3.0/utm/firewall.html. [Último acceso: Agosto 2022].

[47] «¿Qué es Snort?,» SNORT, [En línea]. Available: https://www.snort.org/. [Último acceso: 2022].

[48] Endian, «Services Menú,» Endian Docs, [En línea]. Available: http://docs.endian.com/3.0/utm/services.html. [Último acceso: Agosto 2022].

[49] M. Ecuador, «Mercadolibre - Intel NUC celeron J4005,» Mercadolibre, [En línea]. Available: https://listado.mercadolibre.com.ec/intel-nuc-celeron-j4005#D[A:intel%20nuc%20celeron%20j4005]. [Último acceso: Agosto 2022].

[50] Intel, «Kit Intel® NUC NUC7CJYH,» Intel Corporation, [En línea]. Available: https://ark.intel.com/content/www/es/es/ark/products/126135/intel-nuc-kit-nuc7cjyh.html. [Último acceso: Agosto 2022].

[51] M. Ecuador, «Mercadolibre - Raspberry Pi 4B de 4GB,» Mercadolibre, [En línea]. Available: https://articulo.mercadolibre.com.ec/MEC-516375748-raspberry-pi-4b-de-4-gigas-ram-made-in-uk-iot-15ghz-4k-_JM#position=1&search_layout=stack&type=item&tracking_id=1886feec-d735-4adb-9313-6cadb52b33bc. [Último acceso: Agosto 2022].

[52] R. Pi, «Raspberry Pi 4 Tech Specs,» Raspberry Pi, [En línea]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/?variant=raspberry-pi-4-model-b-8gb. [Último acceso: Agosto 2022].

5 ANEXOS

ANEXO I. Formato de lista para comparar sistemas unificados.

ANEXO I. Formato de lista para comparar sistemas unificados

Nº	Criterios de comparación	OPNsense	pfSense	ClearOS	Endian
1	Entorno de instalación fácil de seguir				
2	No es necesario el uso de documentación para seguir la instalación				
3	Configuración de interfaz de red como parte de la instalación				
4	Interfaz gráfica en el lado del servidor				
5	Soporte de Interfaz por la línea de comandos (CLI) en el servidor				
6	Configuración de red desde el menú principal en el servidor				
7	Asistente de configuración en Interfaz web				
8	Conjunto de servicios de seguridad básicos incluidos				
9	Capacidad para añadir servicios adicionales Capacidad para añadir servicios adicionales				
10	Panel de resumen con información relevante				
	Total				
11	Servicios:				
	Firewall				
	NAT				
	Traffic Shaper				
	Virtual IP				
	Servidor Proxy				
	IDS/IPS				
	VPN				
	IPSec				
	Portal cautivo				
	Antivirus				
	Servidor DHCP				
	VLAN				
	Servidor SNMP				
	Wireless				
	Total				