Revista MINERVA

Plataforma digital de la revista: https://minerva.sic.ues.du.sv

DOI: 10.5377/revminerva.v6i2.17089

Nota Técnica | Technical Report

Integración de servicios de ciberseguridad y enrutamiento usando software libre basado en pfSense

Integration of cybersecurity and routing services using free software based on pfSense

Josue Daniel Osorto-Rivera[1]

Oscar Rene Miranda Urbina[1]

Carlos Osmin Pocasangre Jimenez[1]

Correspondencia:
MU17001@ues.edu.sv

Presentado: *30 de enero de 2023*
Aceptado: *6 de junio de 2023*

1 Escuela de Ingeniería Eléctrica, Facultad de Ingeniería y Arquitectura, Universidad de El Salvador

RESUMEN

La implementación de medidas de ciberseguridad, para cualquier lugar que requiera una conexión a Internet, es cada vez más importante, convirtiéndose no solo en un extra para los usuarios sino en una necesidad. El desconocimiento de cómo funcionan los ataques cibernéticos es la principal vulnerabilidad ante estos, por lo que la ciberseguridad se convierte en una prioridad. La implementación de redes privadas en Internet es una alternativa para aquellos proyectos que necesitan compartir datos entre conexiones remotas. Implementar una de estas redes puede ser más simple de lo que parece, ya que comprender lo que realmente son, facilita la protección de los datos de los usuarios contra ataques cibernéticos. En este artículo científico se encontrará la implementación de una red privada a través de Internet pública en el Laboratorio de Telemática de la Escuela de Ingeniería Eléctrica de la UES.

Palabras claves: Red privada virtual, firewalls, pfSense, ciberseguridad.

ABSTRACT

The implementation of cybersecurity measures for any place that requires an Internet connection is increasingly important, becoming not only an extra for users, but a necessity. Ignorance of how cyberattacks work is the main vulnerability to these, so cybersecurity becomes a priority. Therefore, the implementation of private networks on the internet is an alternative for those projects that need to share data between remote connections. Implementing one of these networks can be simpler than it seems, since understanding what they really are makes it easier to protect users from cyberattacks. In this scientific article, the implementation of a private network through the public internet in the telematics laboratory of the school of electrical engineering at UES will be found.

Keywords: Virtual private network, firewalls, pfSense, cybersecurity.

INTRODUCCIÓN

La vulnerabilidad de un usuario en Internet no siempre es clara para gran parte de la población mundial. Esta realidad es inminente y sobre todo peligrosa. En 2007, el ataque conocido como WannaCry infectó más de 230,000 computadoras en 150 países, en equipos con sistema operativo Windows, resultando en pérdidas de más de USD 4 mil millones (Latto, 2020).

La ciberseguridad es la práctica de proteger sistemas, redes y programas, de ataques digitales. Estos ataques generalmente tienen como objetivo acceder, modificar o destruir información confidencial; extorsionar a los usuarios o interrumpir la continuidad del negocio (CISCO, 2022a; Michalec et al., 2023).

En el pasado, no había forma de leer a través de un papel, la única forma de interceptar un mensaje era literalmente haciéndolo, pero el mundo ha cambiado más en los últimos años que en toda la historia. La comunicación se ha vuelto instantánea y versátil, ya no es necesario viajar a Japón para hablar con japoneses, ir a un restaurante para pedir comida, o incluso llamar para hacerlo, ya no es necesario ir al banco para abrir una cuenta de ahorros, etc. Sin embargo, como suele suceder, la sociedad decide tomar atajos, y hoy en día, mucha información personal y confidencial se utiliza no solo en las actividades cotidianas de una persona, sino también por grandes corporaciones para realizar gran parte de su información y finanzas. Por esta misma razón, los mayores expertos en tecnología del mundo han filtrado información de cientos de miles de personas atacando a países de primer mundo y con una fuerte cultura de ciberseguridad integrada en su día a día.

Por esta razón, se ha decidido abordar el tema desde la implementación de VPN en routers integrados. En 2020, la razón de ataque más relevante en los Estados Unidos fue el robo o el compromiso de credenciales (IBM, 2021). La formación en estos temas, para la población en general, es necesaria porque en la historia reciente y futura, dichos ataques siempre serán una amenaza.

DESARROLLO

pfSense es un software basado en FreeBSD (sistema operativo de código abierto para computadoras) que incluye varias funciones que facilitan su uso como firewall y enrutador (Zientara, 2018). El objetivo de este software es utilizar sus funciones para crear una conexión segura utilizando VPN y firewalls para establecer y mantener un tráfico de información seguro. Entre las principales funciones de pfSense se encuentra el firewall, la traducción de direcciones de red (NAT), un proceso mediante el cual una o más direcciones locales se traducen en direcciones globales y viceversa (KeepCoding, 2022), el servidor DHCP y la VPN.

VPN

Es una red privada que crea una conexión de red entre dispositivos en Internet (Amazon Web Services, 2023). En este punto, muchas empresas se han dedicado a crear un amplio mercado de servicios VPN. Según nuevas pruebas e investigaciones (Migliano, 2023), los proveedores comerciales se especializan según el uso que el cliente le dará a la red privada, lo que significa que los proveedores no se pueden clasificar de “peor a mejor” sino, del tipo de cliente al que proveen, por ejemplo: VPN con bajo presupuesto; VPN para streaming; VPN para privacidad; etc. Por esta razón, se ha seleccionado al proveedor de VPN NordVPN.

Pero ¿exactamente, por qué usar una VPN? Según la documentación oficial del proveedor ExpressVPN, la encriptación VPN oculta la dirección IP y mezcla el tráfico de los usuarios. También encripta el tráfico del usuario al servidor. NordVPN utiliza el algoritmo de

cifrado AES-256-GCM (NordVPN, 2023). Esto muestra que no se trata solo de una red privada de servidores, estos servidores implementan medidas de seguridad. El último aspecto, pero no menos importante para decidir qué VPN usar, es que según una reciente investigación (Jones, 2023), el puerto TCP coincide con el puerto más adecuado para el área de trabajo que se implementará. Además, la fiabilidad del tráfico TCP es mayor que la del tráfico UDP.

Hardware

Al ser pfSense® un software, se necesita hardware para instalarlo o se pueden utilizar máquinas virtuales para simularlo (VirtualBox, VMware Workstation, etc.). En esta investigación, se utilizó la mini PC PROTECTLI modelo FW4B-0-4-32, que tiene 32 GB de memoria interna y 4 GB de RAM. Netgate ofrece dispositivos más económicos, como el modelo SG-1100, entre otros.

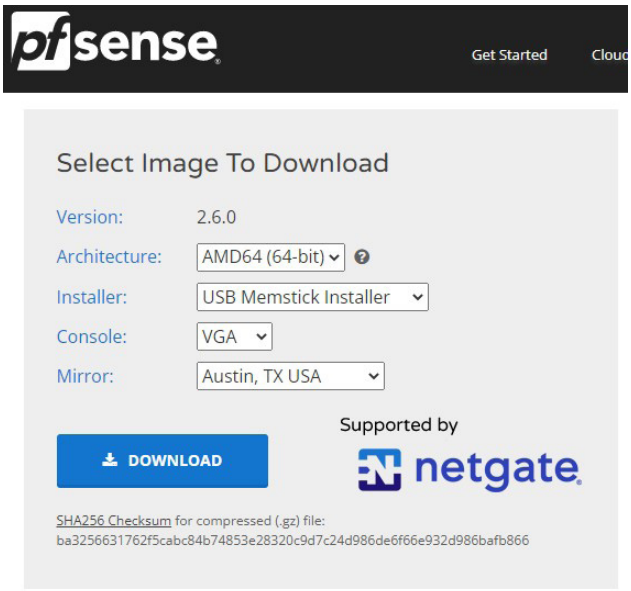
El proceso de instalación del software pfSense es similar al de cualquier sistema operativo. Se debe determinar si el software se descarga como imagen ISO o como instalador USB y luego cargarlo en un dispositivo de almacenamiento con opción USB, formateada y configurada con soporte de arranque. La Figura 1 muestra la configuración para cargar el instalador en un almacenamiento con puerto USB.

Una vez descargada la imagen de pfSense, se debe formatear y configurar un almacenamiento con opción USB y con soporte de arranque activo. Existen varios programas que cumplen esta función. En este caso, se utiliza el programa Rufus versión 3.20 para configurar la imagen de pfSense con opción de arranque, como se muestra en la Figura 2.

Debido a que la mini PC cuenta con puertos HDMI, RJ45 y USB, se recomienda conectar el almacenamiento USB a la mini PC y luego utilizar un monitor y un teclado para configurar el software de pfSense. Así mismo es importante tener en cuenta la configuración

Figura 1

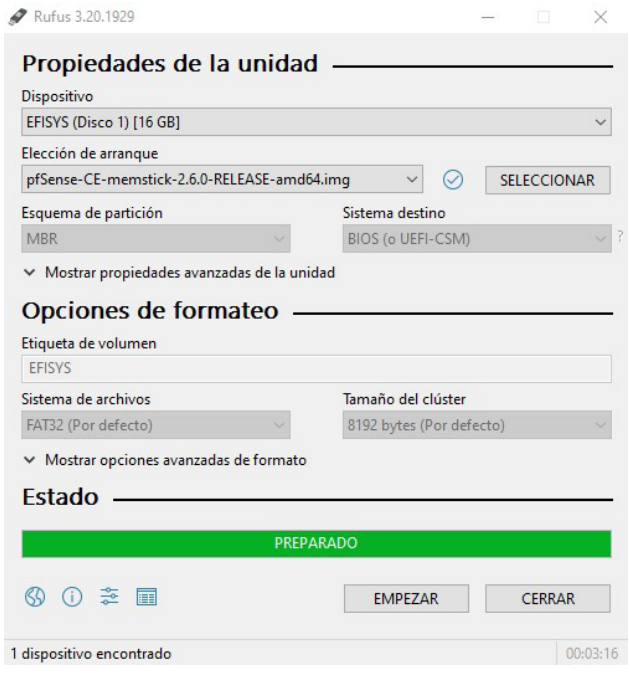
Panel de descarga de pfSense



Nota. Imagen ilustrativa capturada en la interfaz web de pfSense pfsense.org/download.

Figura 2

Ventana de Rufus para la configuración del dispositivo de almacenamiento.



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

recomendada por el programa instalador de pfSense. Una vez que el software de pfSense esté en funcionamiento, se puede utilizar el modelo FW4B de la mini PC, que cuenta con cuatro puertos de red (WAN, LAN, OPT1 y OPT2), también se sugiere utilizar el puerto WAN para conectar el proveedor de Internet contratado y el puerto LAN para conectar un Switch Cisco en el que se pueden conectar varios dispositivos dentro de la red privada configurada en pfSense.

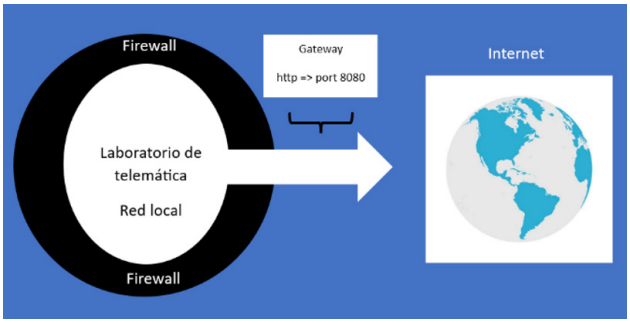
Diagramas de implementación

La estructura de ciberseguridad utilizada por algunas organizaciones se basa en la configuración de un firewall que aísla el contacto directo entre la red local y el internet, un solo puerto de salida para monitorear el tráfico entrante y saliente. Para el caso de aplicación en el Laboratorio de Telemática de la Escuela de Ingeniería Eléctrica en la Universidad de El Salvador es igual, la Figura 3 identifica el estado del Laboratorio previo a nuestra intervención. En caso de que un usuario acceda a internet no cuenta con ninguna VPN salvo que exista una instalada en el dispositivo conectado que usualmente es el software que las compañías de VPN proporcionan.

En la Figura 4 se observa el diagrama con el router con VPN incorporado. El router con VPN incorporada se instalará en el puerto permitido

Figura 3

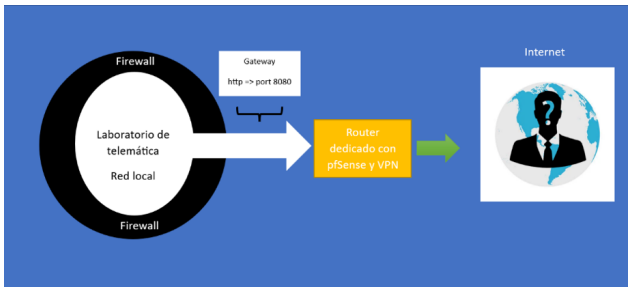
Diagrama de estado inicial de laboratorio.



Nota. Imagen ilustrativa capturada en Microsoft Word

Figura 4

Diagrama de estado final de laboratorio con router ya incorporado



Nota. Imagen ilustrativa capturada en Microsoft Word

por el firewall de la red local (este puerto depende de la organización), de esta forma, si un usuario dentro de la red local quisiera acceder a internet puede hacerlo de manera segura a través de la VPN incorporada en el router sin necesidad de instalar un software.

Configuración de pfSense

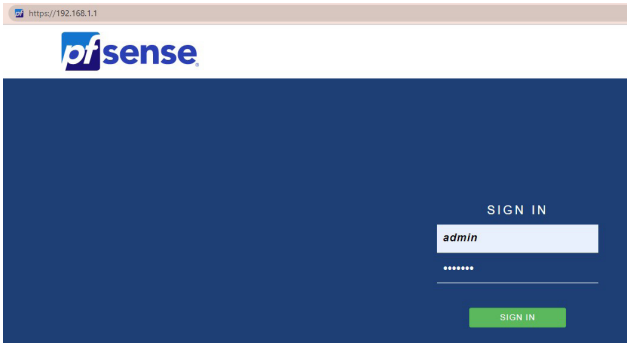
Para configurar pfSense, es importante tener en cuenta que el puerto LAN al que se conecta la PC brinda una dirección IP diferente a la proporcionada por el proveedor de Internet. Para acceder a la interfaz web de pfSense, es necesario buscar la dirección IP que se le asigna a la PC en uso mediante el servicio DHCP. En caso de utilizar Linux, se puede usar el comando “ip address”. Si se utiliza Windows, existen diferentes formas de solicitar esta información, como la terminal del sistema con el comando “ipconfig” o accediendo a las configuraciones de red en la sección de propiedades de red.

El software pfSense cuenta con una configuración de red predeterminada que utiliza la dirección *IP 192.168.1.0* y el gateway para acceder a la interfaz web en 192.168.1.1. Las credenciales predeterminadas para el nombre de usuario y la contraseña son “admin” y “pfense”, respectivamente (Figura 5).

Al entrar en la interfaz web de pfSense se despliega una configuración inicial la cual se deja por defecto, debido a que lo que se

Figura 5

Interfaz web para autenticación de pfSense



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

pretende es tener una red privada ya que una red pública contiene direcciones IP a las cuales se puede acceder directamente desde internet, y las redes privadas permiten conectarse de forma segura a otros dispositivos dentro de la misma red. En la opción de interfaces dentro de la interfaz web se modifica la interfaz LAN modificando la dirección IPv4, que trae por defecto (192.168.1.1), por una dirección privada, existe una basta cantidad de redes privadas por lo que la dirección seleccionada puede cambiar según sea el caso. En este caso se ha tomado la dirección 172.16.0.1 con máscara 24 tal como se observa en la Figura 6.

Después de realizar la configuración inicial de pfSense, es recomendable cambiar la contraseña predeterminada para mayor seguridad. Una vez finalizadas y aplicadas todas las configuraciones, es necesario actualizar la página e introducir la nueva dirección IP asignada a la red privada. Si se cambian las credenciales de acceso, es importante tener en cuenta que los cambios ya están aplicados.

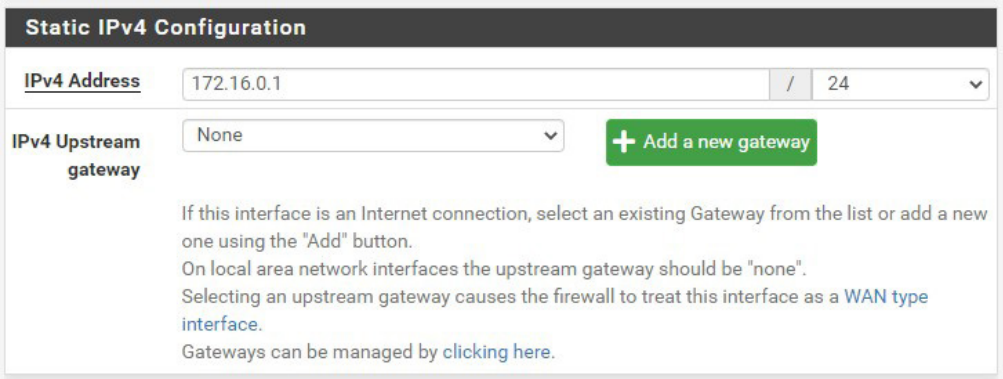
Para verificar si pfSense ha realizado los cambios correctamente, se pueden utilizar los comandos mencionados anteriormente para obtener y visualizar las configuraciones de red en el ordenador. Si no se visualizan los cambios en Linux, se puede utilizar el comando "sudo dhclient -r", mientras que en Windows se puede utilizar el comando "ipconfig /release" en la terminal del sistema. Estos comandos liberan y renuevan la dirección IP en ambos sistemas operativos, y los cambios en la configuración de red se aplicarán después de realizar esta operación.

Firewall

La importancia de migrar a un firewall en las empresas es mejorar la postura de seguridad con las capacidades más recientes para la protección de la red unificada y la microsegmentación de cargas de trabajo (CISCO, 2022b). El tablero principal de pfSense brinda información de sistema, interfaces, unidades de memoria, etc. Además, puede brindar información adicional como estado de

Figura 6

Configuración de red privada en interfaz LAN



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

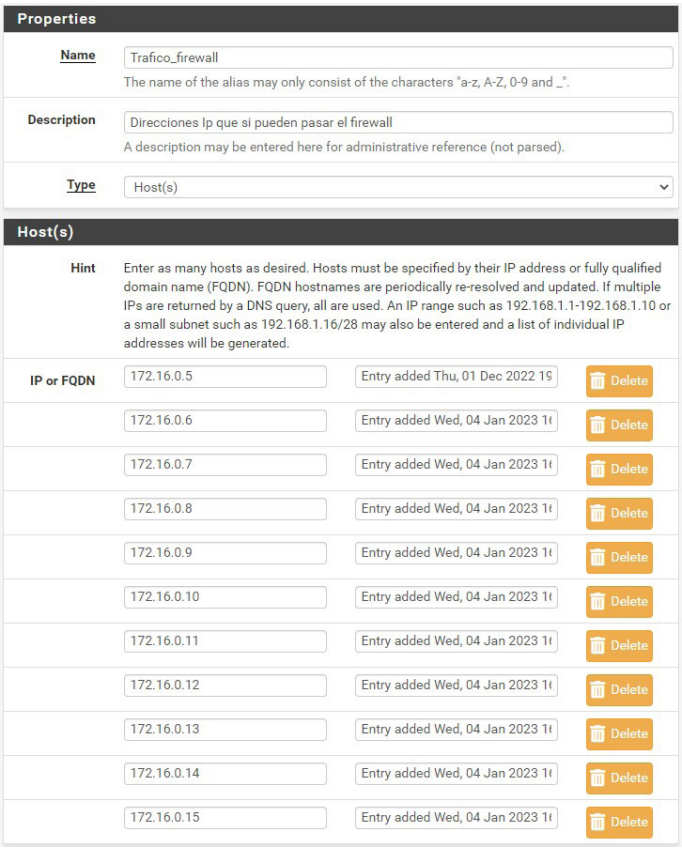
servicios, estado de portal cautivo, estado de firewall, información de VPN, entre otros. Todas estas opciones están disponibles desde el apartado de widgets. En este punto ya se tiene configurada la red privada y se tiene el firewall brindado por pfSense con sus configuraciones por defecto. Existen casos en los que se necesita brindar acceso en los firewalls a ciertas direcciones IP de la red, esto es posible haciendo uso de la opción "aliases" dentro de la configuración del firewall, el cual se basa en agrupar según sea necesario las direcciones IP ahorrando escritura al configurar las reglas del firewall. En este caso se da acceso a un rango desde 172.16.0.5 hasta 172.16.0.15, dentro de la opción de Aliases se le asigna el nombre al grupo de direcciones IP, una descripción y se agregan las direcciones pertenecientes al grupo tal como se observa en la Figura 7.

Una vez que se ha configurado el grupo de direcciones IP, es posible establecer las reglas del firewall con mayor facilidad. Dado que estas reglas se aplican a la red privada, al configurarlas se debe seleccionar la interfaz LAN. En primer lugar, se pueden observar las reglas predeterminadas que pfSense aplica al firewall (y que no se pueden modificar). Luego, se agrega una nueva regla en la que se asigna el grupo de direcciones IP que utiliza el gateway configurado con la conexión VPN para acceder a Internet. Además, se debe proporcionar una descripción y guardar la regla, como se muestra en la Figura 8.

Al configurar la regla, se debe tener en cuenta la opción "Action", que determina el comportamiento de la regla en el firewall. Es posible especificar, si se permite el acceso, se bloquea o se rechazan las direcciones IP. El

Figura 7

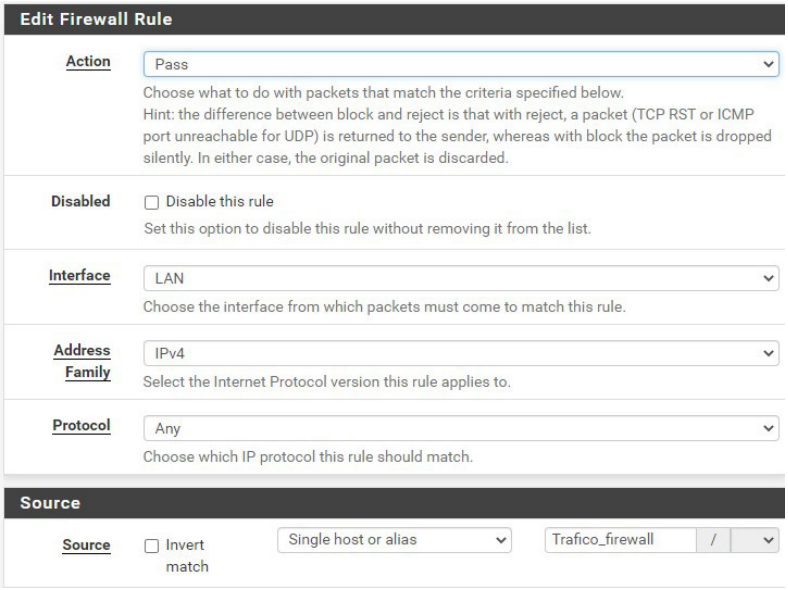
Configuración de Aliases



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Figura 8

Configuración de reglas dentro de firewall



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

protocolo predeterminado en la configuración es TCP, pero se puede cambiar a cualquier otro protocolo. Luego, en las opciones avanzadas,

se debe modificar el gateway del puerto WAN y asignar el gateway configurado al servicio de la VPN. Así, se asegura que el grupo de direcciones IP tenga acceso a Internet a través de la conexión VPN establecida. Una vez que la sección del firewall está configurada y funcionando correctamente, es necesario configurar la VPN a través de la cual el tráfico de la red pasará. Una VPN es una red privada virtual que permite al usuario asegurar la actividad de la red de manera que solo sea conocida por el proveedor y el usuario. En términos simples, funciona de manera similar a una red privada doméstica, lo que significa que la información y los archivos compartidos a través de una encriptación VPN son seguros y se mantienen separados del resto de Internet.

Mercado VPN

A este punto, muchas empresas se han dedicado a crear un amplio mercado de servicios VPN. Los proveedores comerciales se especializan según el uso que el cliente le dará a la red, esto conlleva que los proveedores no se pueden clasificar de “menor a peor” sino, del tipo de cliente al que provee ej. VPN con bajo presupuesto, VPN para streaming, VPN para privacidad, etc.

Acorde a la documentación oficial de pfSense este es compatible con varios proveedores de VPN vistos en esta tabla. El primer proveedor puesto a prueba fue PIA VPN. La especialidad de este proveedor es la privacidad, los servicios Torrent está limitado y está disponible en 84 países. Al instalar este proveedor en el router se obtuvieron problemas de desconexión impredecibles y latencia muy alta. Se entiende que es por la misma naturaleza de la aplicación de este proveedor.

Como segunda y definitiva opción el proveedor NordVPN fue utilizado, aunque su especialidad es la velocidad para los propósitos de este estudio era suficiente, además que la estabilidad que brinda NordVPN en comparación con PIA VPN en este router utilizando pfsense es considerable.

Otro inconveniente mayor es que muchos proveedores de VPN no tienen flexibilidad en los puertos proporcionados a un usuario para usar su red. Estos puertos son específicos para cada protocolo de red.

Para la instalación de este proveedor en pfSense será necesario conocer que es y cómo funciona el algoritmo de encriptación. Es el nombre del algoritmo de encriptación. AES es un estándar de cifrado utilizado, recomendado y aprobado por la agencia de seguridad nacional de los Estados Unidos (NSA), es utilizado para asegurar la comunicación clasificada como TOP SECRET.

De acuerdo con la documentación oficial de NordVPN, Si alguien utilizara un ataque de fuerza bruta (que implica verificar todas las posibles combinaciones de teclas), necesitaría juntas todos los recursos computacionales que la humanidad dispone y utilizar todo el tiempo que el universo lleva existiendo, y aun así posiblemente no tener éxito.

Configuración de VPN

Una red doméstica se gestiona a través de un router local, mientras que una VPN (red privada virtual) se gestiona de forma virtual. Para poder utilizar una VPN, tanto el cliente como el proveedor deben gestionar un software que permita a las máquinas comunicarse entre sí y garantizar el cifrado de la VPN. En la mayoría de los casos, el proveedor es controlado a través de un servidor de acceso remoto o RAS (remote access server), que permite verificar la información transmitida a través de varios tipos de protocolos y procesos de tunelización. El túnel VPN es una conexión encriptada entre el usuario, el cliente y el servidor. La tunelización garantiza que la información esté encapsulada de manera que no se pueda interceptar, alterar o vigilar. Esto se logra mediante el envío de la dirección IP del servidor anfitrión a través del cual se ejecuta la encriptación VPN en lugar de la dirección IP del usuario, lo que garantiza el anonimato total.

Entre los protocolos utilizados en el proceso de tunelización, se encuentran el Protocolo de Túnel Punto a Punto (PPTP), el protocolo de Túnel de Capa 2 (L2TP), el protocolo de Túnel de Socket Seguro (SSTP) y el protocolo de OpenVPN. Este último es utilizado por pfSense y consta de una aplicación de software de código abierto que utiliza conexiones punto a punto, que a su vez utilizan tanto SSL como TLS para el intercambio de claves. A diferencia del protocolo L2TP, el protocolo de OpenVPN puede ejecutarse a través de puertos UDP o TCP, lo que permite eludir los firewalls.

La configuración de la VPN se realiza a través del software pfSense utilizando la configuración de OpenVPN. Para ello, se ha seleccionado el proveedor NordVPN y se ha elegido el servidor recomendado por parte de NordVPN para obtener los protocolos disponibles para el servidor. En este caso, se ha utilizado el protocolo TCP con puerto 443.

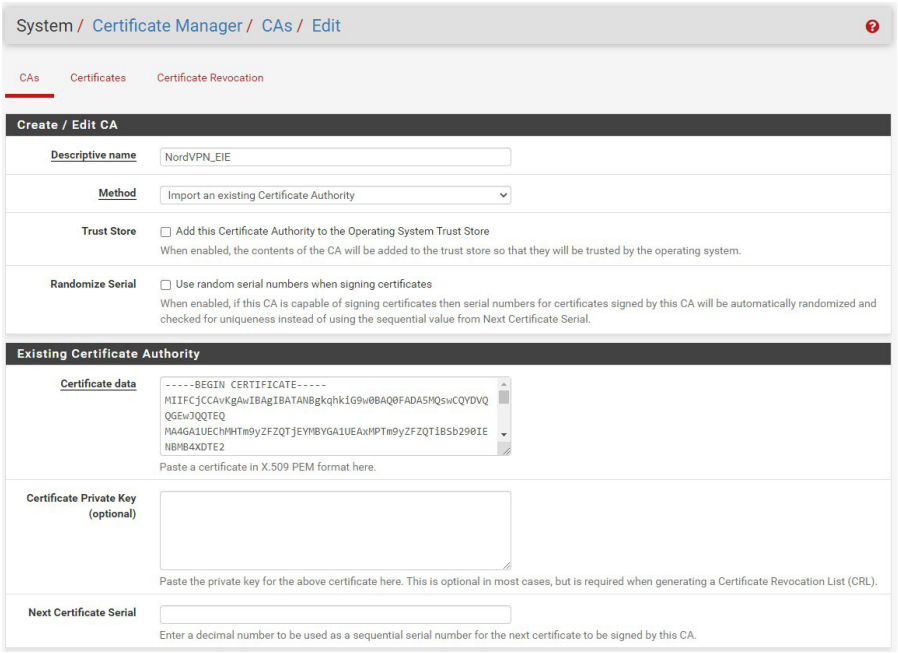
Para configurar la VPN, se debe introducir el certificado del protocolo TCP para el servidor en EUA. Cada servidor posee un certificado diferente y se puede observar cómo hacerlo en la Figura 9 de la configuración del sistema.

Luego se procede a configurar el cliente de la VPN en la sección de OpenVPN. Se selecciona el modo del servidor “Peer to Peer (SSL/TLS)” y se elige el protocolo que se utilizará para la configuración. En este caso, se selecciona el protocolo TCP para direcciones IPV4 y se utiliza el puerto por el cual se tiene la conexión del proveedor de internet (WAN). En esta configuración, es necesario especificar la autenticación del usuario por parte del proveedor de la VPN. Esta información se puede obtener dentro del sitio web del proveedor.

Luego, se procede a configurar los valores del proveedor criptográfico, donde se establecen los algoritmos y paquetes de cifrado, los valores de nombres de identidad, los valores del almacén de claves de cifrado y los valores de la entidad emisora de certificados (CA). Estos

Figura 9

Configuración de certificado de VPN



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

valores se configuran según el protocolo TCP obtenido por parte del proveedor de la VPN.

Dentro de las opciones avanzadas de la configuración del cliente, se encuentra el apartado de creación del puerto virtual. En este apartado, se establece la opción única para direcciones IPV4.

Posteriormente, en el apartado de interfaces, se pueden observar dos interfaces configuradas por defecto (WAN y LAN). Es necesario crear y habilitar la interfaz para la VPN. En este caso, se le ha asignado el nombre del proveedor “NordVPN”, como se puede ver en la Figura 10.

Una vez seleccionadas las opciones adecuadas de configuración desde la interfaz web de pfSense, se procede a habilitar la función de “DNS resolver” en la sección de “servicios-DNS resolver”. Esta función se encarga de convertir nombres de dominios en direcciones IP. En las configuraciones, se debe seleccionar la opción de interfaces de salida y el certificado SSL/TLS.

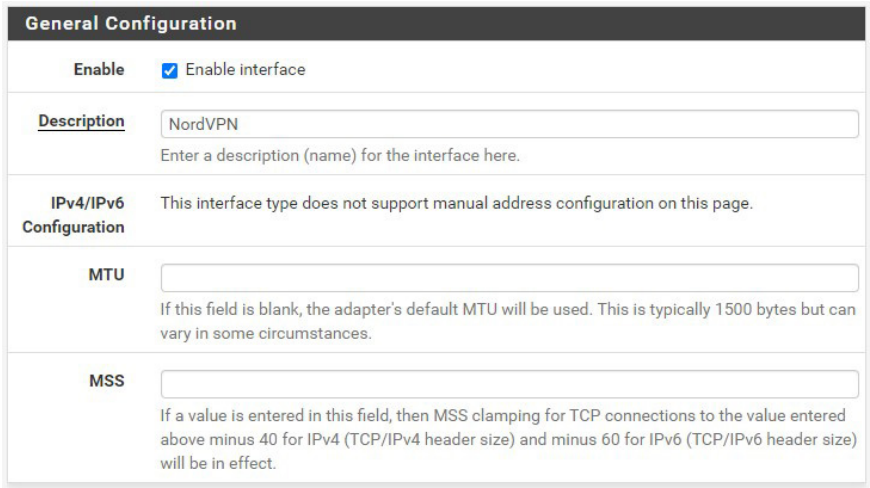
En la sección de interfaces de salida, se debe especificar la interfaz de salida previamente configurada y nombrada como “ NordVPN”. De esta manera, el servidor DNS utilizará únicamente la interfaz de la VPN para enviar consultas a servidores autorizados y recibir respuestas. Esta opción trae de manera predeterminada el uso de todas las interfaces disponibles, por lo que es importante establecer la interfaz correcta para garantizar el buen funcionamiento de la VPN.

En la sección del certificado SSL/TLS, se debe seleccionar el certificado denominado “*Web Configurator default*”. Si este certificado no está disponible por defecto, se debe realizar una configuración similar a la que se muestra en la Figura 11. Este certificado es necesario para garantizar la seguridad de la conexión VPN mediante el cifrado SSL/TLS.

Uno de los objetivos principales del uso de un proveedor de VPN es garantizar el anonimato al generar tráfico hacia internet. Para lograr esto, es necesario habilitar la opción de identidad oculta dentro de las opciones avanzadas

Figura 10

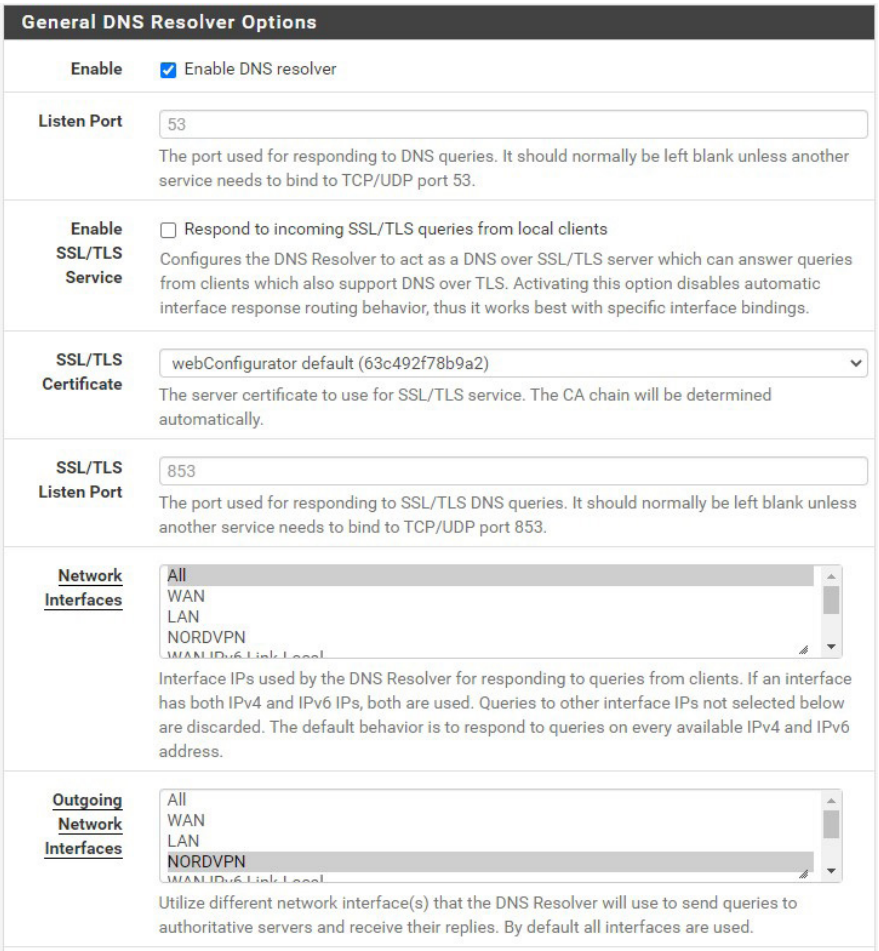
Configuración general de pfSense



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Figura 11

Opciones generales del servicio DNS resolver



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

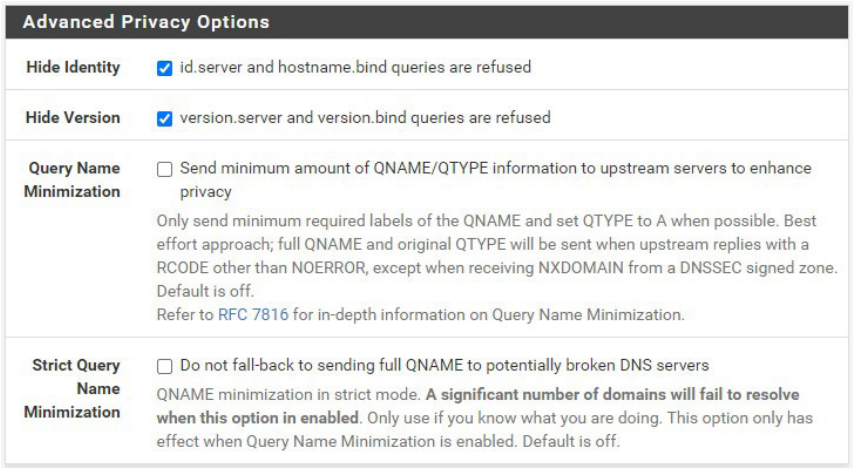
del servicio DNS resolver. Además, se debe seleccionar la versión adecuada, tal como se muestra en la Figura 12. De esta manera, se podrá garantizar que la identidad del usuario permanezca oculta y protegida durante la navegación en línea.

Una vez finalizada la configuración de la VPN, se deben configurar las reglas necesarias para habilitar la traducción de direcciones de red. Para hacer esto, se debe acceder al apartado de firewall y seleccionar NAT. Luego, se debe elegir el modo de NAT saliente o "outbound NAT mode" y seleccionar la opción de modo manual de generación de reglas.

En este punto, se deben dejar las reglas en la opción para ser generadas por defecto y agregar una nueva para identificar la red privada. Es importante especificar que la regla será de tipo IPV4 en el apartado "address family" y seleccionar la opción "any" en la sección de protocolo, tal como se muestra en la Figura 13.

Figura 12

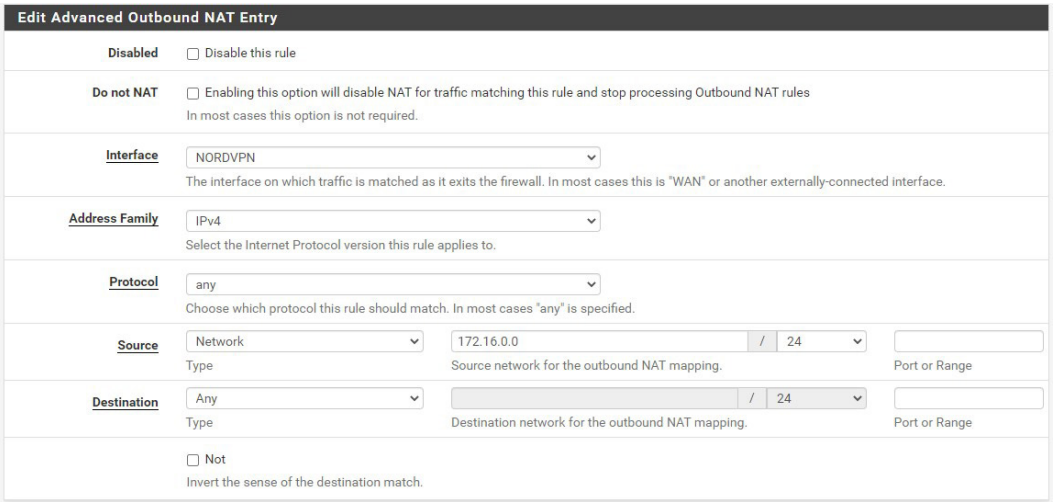
Opciones de privacidad avanzadas



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Figura 13

Edición avanzada de opciones de trafico de salida NAT en PfSense



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Como último paso, se deben configurar los servidores en pfSense. En este caso, el proveedor ofrece dos servidores DNS: server 1 (103.86.96.100) y server 2 (103.86.99.100). Esta configuración se puede modificar en el apartado de sistema y desde la sección de ajustes generales.

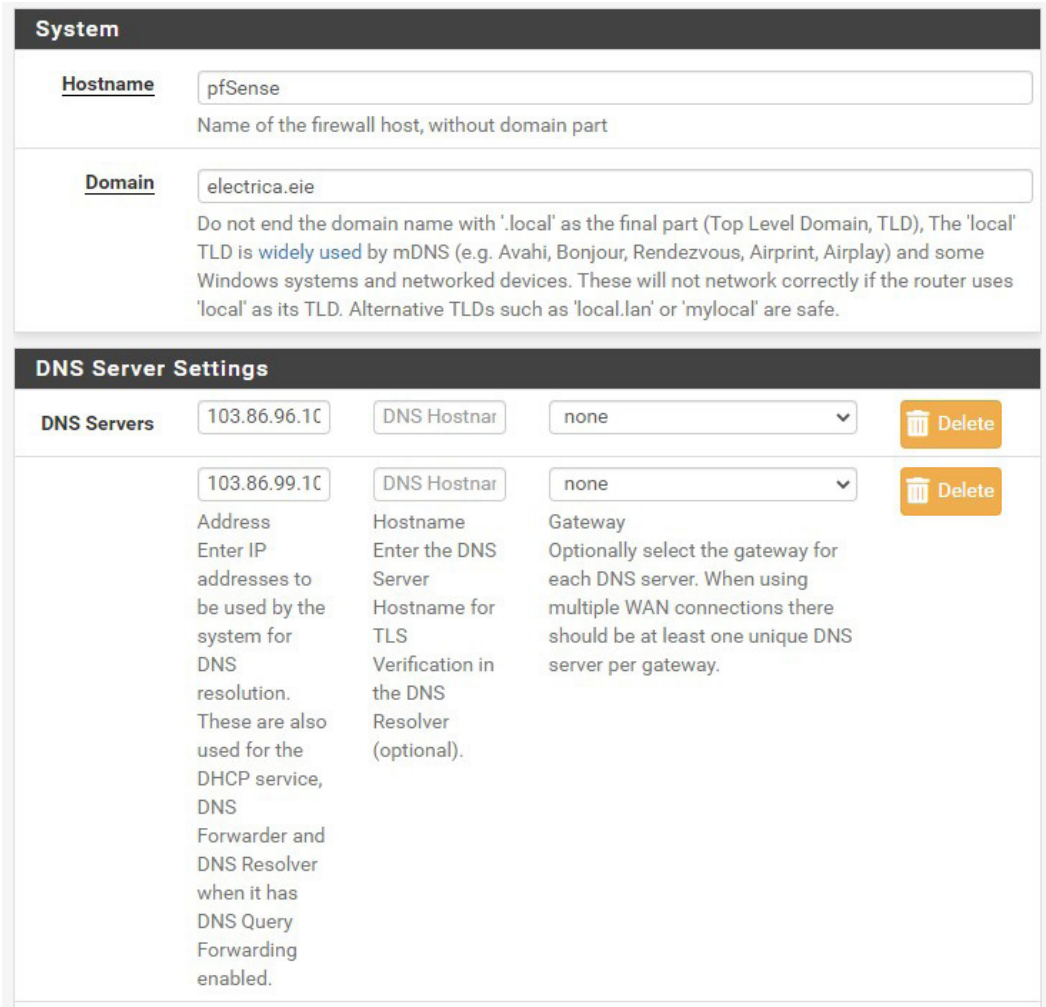
En la Figura 14 se pueden observar los cambios ya realizados. Además, se ha modificado el nombre de dominio por "eléctrica.eie". Es importante tener en cuenta que este nombre puede variar, pero es esencial respetar que no se debe terminar un dominio en ".local".

Después de completar esta última operación, se habrá configurado un sistema completo que encripta el tráfico a través de VPN, lo que proporciona protección para la información del usuario. Todo esto se ha llevado a cabo utilizando el software pfSense.

Como se ha mencionado anteriormente, existen diversas herramientas para monitorear el funcionamiento de todos los elementos de la VPN. En el caso del cliente de la VPN, se puede acceder al estado del cliente, el cual proporciona información sobre la dirección local, la dirección virtual y la dirección del host mediante la cual se accede a internet. Como se puede

Figura 14

Configuración de servidores DNS de NordVPN



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

observar en la Figura 15, el servidor se encuentra activo (up) y ha proporcionado una dirección IP de host remota: 37.120.157.19, utilizando el puerto 443.

Servicios de ciberseguridad por enrutamiento versus aplicaciones VPN

En el mercado existen numerosas opciones de VPN. La razón por la cual se utiliza el enrutamiento es para asegurar la protección de datos en laboratorios de investigación. En los laboratorios privados, la seguridad de los datos es fundamental, pero también se debe considerar la portabilidad de la implementación y la ciberseguridad por enrutamiento en caso de que se necesite migrar el laboratorio a otra ubicación geográfica. Por esta razón, es posible que esta aplicación no sea viable en situaciones donde se necesite proteger los datos de un gran número de usuarios.

Cuando el cliente está activo y conectado al servidor del proveedor de VPN, y las compuertas están activas y sin reportes de pérdida de información tal como se observa en la Figura 16, se tiene un sistema seguro en el que el tráfico de información viaja de manera encapsulada a través de los túneles encriptados por medio del servidor de VPN. Además, se cuenta con un franqueo del firewall que brinda una red privada segura. En la Figura 17, se puede

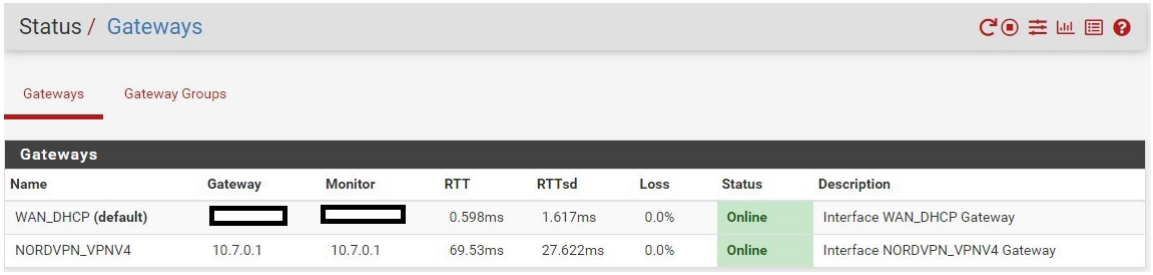
Figura 15

Estadísticas del estado del cliente y del proveedor VPN

Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Figura 16

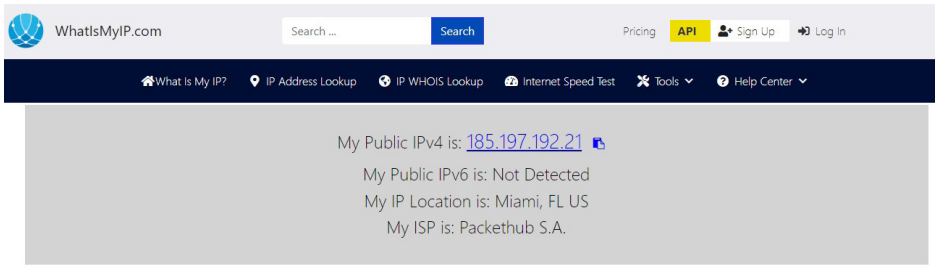
Estado de los gateways



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

Figura 17

Prueba de dirección IP a través de VPN



Nota. Imagen ilustrativa capturada en la interfaz web de PfSense.

observar que la dirección IP de salida a internet es: 185.197.192.21, la cual se localiza en Miami, Florida, Estados Unidos. De esta manera, se logra ocultar por completo la identidad de la dirección IP local.

CONCLUSIONES

Al momento de plantearse la instalación de un router con el servicio de VPN integrado, deben tomarse en cuenta las medidas de ciberseguridad tomadas previamente por el host. Si esto no es tomado en cuenta pueden encontrarse puntos de comunicación interrumpida como podría ser un firewall que permita solo acceder mediante puertos específicos que no coincidan con los puertos proporcionados por el proveedor de la VPN. En su mayoría, estos proveedores trabajan de manera tal, que su infraestructura está determinada y no pueden cambiar el puerto que proporcionan, esto también se debe a medidas de ciberseguridad.

Aunque pfSense es un software basado en un sistema operativo de código abierto, este por sí solo tiene acceso a muchas medidas de ciberseguridad para ser implementadas, sin embargo, para acceder a un mejor beneficio de este router es necesario contratar los servicios de un proveedor de una VPN y es muy importante entender que, aunque estas dos tecnologías se unan y sean compatibles, el sistema de versionado y actualización es completamente independiente uno del otro. Por esto se recomienda que, si se decide implementar un sistema con estos dos elementos en mente, se debe estar pendiente de la documentación en cada actualización por parte de ambas comunidades.

REFERENCIAS

Amazon Web Services. (2023). *¿Qué es una VPN? - Explicación de las redes privadas virtuales - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/vpn/

CISCO. (2022a). ¿Qué es la ciberseguridad? *Cisco*. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

CISCO. (2022b). *¿Qué es un firewall? - Cisco*. https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

IBM. (2021). *¿Qué es un ataque cibernético? | IBM*. https://www.ibm.com/mx-es/topics/cyber-attack

Jones, J. P. (2023). *UDP o TCP: ¿en qué se diferencian y cuál deberías usar?* https://www.top10vpn.com/es/guias/udp-vs-tcp/

KeepCoding. (2022). ¿Qué es NAT? | KeepCoding Bootcamps. *KeepCoding Tech School*. https://keepcoding.io/blog/que-es-nat/

Latto, N. (2020). ¿Qué es WannaCry? https://www.avast.com/es-es/c-wannacry

Michalec, O., Shreeve, B., & Rashid, A. (2023). Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems. *Energy Research & Social Science*, *106*, 103327. https://doi.org/10.1016/j.erss.2023.103327

Migliano, S. (2023). *Las 10 mejores VPN del 2023 calificadas por expertos en VPN*. https://www.top10vpn.com/es/mejor-vpn/

NordVPN. (2023). *Cifrado VPN de última generación*. https://nordvpn.com/es/features/next-generation-encryption/

Zientara, D. (2018). *Mastering pfSense: Manage, secure, and monitor your on-premise and cloud network with pfSense 2.4, 2nd Edition*. Packt Publishing Ltd.