UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

IMPLEMENTACIÓN DE APLICACIONES DE SEGURIDAD MEDIANTE USO DE SWITCHING AND ROUTING

PRESENTADO POR:

JOSUE DANIEL OSORTO RIVERA

OSCAR RENE MIRANDA URBINA

PARA OPTAR AL TITULO DE:

INGENIERO ELECTRICISTA

CIUDAD UNIVERSITARIA, JUNIO 2023

UNIVERSIDAD DE EL SALVADOR

RECTOR :

MSC. ROGER ARMANDO ARIAS ALVARADO

SECRETARIA GENERAL :

ING. FRANCISCO ANTONIO ALARCON SANDOVAL

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO :

PhD. EDGAR ARMANDO PEÑA FIGUEROA

SECRETARIO :

ING. JULIO ALBERTO PORTILLO

ESCUELA DE INGENIERIA ELECTRICA

DIRECTOR INTERINO :

ING. WERNER DAVID MELENDEZ VALLE

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO ELECTRICISTA

Titulo :

IMPLEMENTACIÓN DE APLICACIONES DE SEGURIDAD MEDIANTE USO DE SWITCHING AND ROUTING

Presentado por :

JOSUE DANIEL OSORTO RIVERA

OSCAR RENE MIRANDA URBINA

Trabajo de Graduación Aprobado por:

Docente Asesor :

PhD. CARLOS OSMIN POCASANGRE JIMENEZ

San Salvador, junio 2023

Trabajo de Graduación Aprobado por:

Docente Asesor :

PhD. CARLOS OSMIN POCASANGRE JIMENEZ

NOTA Y DEFENSA FINAL

En esta fecha, miércoles 22 de febrero de 2023, en la Sala de Lectura de la Escuela de Ingeniería Eléctrica, a las 5:00 p.m. horas, en presencia de las siguientes autoridades de la Escuela de Ingeniería Eléctrica de la Universidad de El Salvador:

1. Ing. Werner David Meléndez Valle
   Director Interino
   Firma

2. MSc. José Wilber Calderón Urrutia
   Secretario
   Firma

Y, con el Honorable Jurado de Evaluación integrado por las personas siguientes:

- DR. CARLOS OSMIN POCASANGRE JIMENEZ
  (Docente Asesor)
  Firma

- ING. WERNER DAVID MELENDEZ VALLE
  Firma

- DR. CARLOS EUGENIOMARTINEZ CRUZ
  Firma

Se efectuó la defensa final reglamentaria del Trabajo de Graduación:

IMPLEMENTACIÓN DE APLICACIONES DE SEGURIDAD MEDIANTE USO DE SWITCHING AND ROUTING

A cargo de los Bachilleres:

- OSORTO RIVERA JOSUE DANIEL

- MIRANDA URBINA OSCAR RENÉ

Habiendo obtenido en el presente Trabajo una nota promedio de la defensa final: 8.1

(Ocho punto Uno)

AGRADECIMIENTOS

Queridos padres, quiero tomar esta oportunidad para expresarles mi más profundo agradecimiento por su apoyo incondicional y amor durante todo el proceso de realización de mi tesis. Su presencia constante y palabras de aliento han sido fundamentales para que logre culminar este importante proyecto en mi vida.

En especial, me gustaría resaltar el papel extraordinario de mi madre. Tu presencia y dedicación incansable han sido un pilar fundamental en cada paso que he dado. Tus palabras de aliento y paciencia han sido un bálsamo que me ha dado fuerzas para continuar incluso en los momentos más difíciles. Tu amor incondicional me ha motivado a dar lo mejor de mí en cada etapa de este proceso y no tengo palabras suficientes para agradecerte por ello.

También quiero expresar mi gratitud hacia el ingeniero Carlos Pocasangre, mi asesor en este proyecto. Gracias a su amplio conocimiento y experiencia, he podido contar con una guía invaluable. Sus consejos y retroalimentación constructiva han sido fundamentales para mejorar mi trabajo y llevarlo a un nivel superior. Siempre estuvo dispuesto a escuchar mis dudas y brindarme orientación, lo cual valoro enormemente.

Además, quiero agradecer al ingeniero Werner Meléndez por su valiosa contribución en esta tesis. Su conocimiento especializado y perspectivas únicas han enriquecido mi investigación y me han dado una visión más amplia del tema y estoy muy agradecido por su tiempo y esfuerzo invertidos en mi proyecto.

Por último, pero no menos importante, quiero extender mi agradecimiento a la secretaria Reina Vides. Su amabilidad, eficiencia y atención a los detalles han sido de gran ayuda en el proceso de

presentación y documentación de mi tesis. Su disposición para ayudar y su profesionalismo han hecho que todo el proceso sea más llevadero y sin contratiempos.

No tengo palabras suficientes para expresar cuánto significa para mí contar con su apoyo y guía durante todo este tiempo. Han sido mi fuerza impulsora y mi mayor inspiración. Gracias por creer en mí y por alentarme a alcanzar mis metas. Este logro no habría sido posible sin su amor, sacrificio y confianza en mí.

Con todo mi aprecio y gratitud,

Josue Daniel Osorto Rivera

AGRADECIMIENTOS

A mi madre Blanca Elena de Miranda, a mi padre Oscar Rene Miranda Flores. No existe un manual de cómo ser unos buenos padres, pero ellos deberían escribir uno. Supieron hacerme sentir apoyado y querido en todo momento en mis decisiones. Gracias por dedicarme y regalarme lo más valioso de sus vidas, su tiempo. A mi difunta abuela, que en el momento más adecuado dirigió hacia mí unas palabras que cambiaron el rumbo de mis pensamientos. Este título está dedicado a ustedes.

A mis hermanas, que cuando necesite su apoyo siempre estuvieron presentes para brindarlo. Su apoyo a sido decisivo en este título y en la persona que soy hoy en día.

A mi tía Ana María Isabel Urbina, como una segunda madre que siempre me apoyo con buena voluntad y amor. Gracias por, sin ninguna obligación, estar siempre ahí.

A mis amigos y compañeros de universidad, con los que lidiamos muchos obstáculos para llegar hasta este punto.

A nuestro docente asesor, que nos brindó de la orientación adecuada para realizar este documento.

Oscar Rene Miranda Urbina

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO TECNICO

Firewall: Un firewall es un sistema de seguridad que controla y monitorea el tráfico de red, permitiendo o bloqueando el acceso a recursos basado en reglas predefinidas. Ayuda a proteger la red de amenazas externas y evita accesos no autorizados.

VPN (Red Privada Virtual): Una VPN es una tecnología que permite crear una conexión segura y encriptada a través de una red pública, como Internet. Proporciona a los usuarios remotos un acceso seguro a la red privada de la universidad, como si estuvieran físicamente presentes en la ubicación de la red.

PfSense: Es un software de código abierto basado en FreeBSD que se utiliza para crear dispositivos de seguridad y enrutamiento. pfSense ofrece un conjunto de herramientas y servicios para configurar y administrar firewalls, routers y VPNs, y es ampliamente utilizado en entornos de red de empresas y organizaciones.

WAN (Wide Area Network): Es la red de área amplia que conecta la red privada de la universidad con otras redes o Internet. En el contexto de pfSense, se refiere a la interfaz de red que conecta el firewall o router a la red externa.

LAN (Local Area Network): Es la red de área local que comprende los dispositivos y sistemas dentro de la red privada de la universidad. En el contexto de pfSense, se refiere a la interfaz de red que conecta el firewall o router a los dispositivos y sistemas internos.

NAT (Network Address Translation): Es una técnica que permite mapear direcciones IP entre redes diferentes. Se utiliza para traducir las direcciones IP privadas de los dispositivos internos a direcciones IP públicas, y viceversa, para permitir la comunicación entre la red privada y la red externa.

Port Forwarding (Redirección de Puertos): Es un mecanismo que permite redirigir el tráfico de red desde un puerto específico en la red externa hacia un dispositivo o servidor específico en la red interna. Se utiliza para permitir el acceso remoto a servicios internos, como servidores web o de correo electrónico.

VPN Site-to-Site: Es una configuración de VPN que permite conectar dos redes privadas separadas, como diferentes campus universitarios, a través de Internet. Esta configuración establece una conexión segura y encriptada entre los dos sitios, permitiendo el acceso seguro a los recursos de red de ambas ubicaciones.

VPN Remote Access: Es una configuración de VPN que permite a los usuarios remotos establecer una conexión segura con la red privada de la universidad desde ubicaciones externas. Los usuarios pueden acceder a los recursos de red internos de manera segura como si estuvieran físicamente presentes en el campus.

VPN Client: Es el software o la aplicación instalada en el dispositivo de un usuario remoto para establecer una conexión VPN con la red privada de la universidad. El cliente VPN autentica al usuario y cifra el tráfico de datos para garantizar la privacidad y la seguridad durante la comunicación.

INTRODUCCION

La vulnerabilidad de un usuario en la internet suele no estar del todo clara para mucha de la población mundial, esta realidad es inminente y sobre todo peligrosa. En 2007 el ataque conocido como WannaCry infecto más de 230,000 PC en 150 países a computadoras con el sistema operativo Windows (IBM, 2022), teniendo un costo en pérdidas por más de 4000 millones USD. La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio. 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 volvió instantánea y versátil, ya no es necesario viajar a japón para hablar con japoneses, ir a un restaurante para pedir comida, ni siquiera llamar por teléfono para esto, ya no hay que ir al banco para abrir una cuenta de ahorros, etc., pero, como suele pasar, la sociedad decide tomar atajos, y hoy en día, mucha información personal y confidencial es usada no solo en las actividades cotidianas de una persona, sino, también por grandes corporaciones para llevar a cabo mucha de su información y finanzas, por esta misma razón los expertos en tecnología más grandes del mundo han filtrado información de cientos de miles de personas atacando a países primermundistas y con mucha cultura de ciberseguridad integrada en su día a día. Por esa razón, hemos decidido abordar el tema desde la implementación de vpn en routers integrados. En 2020, la razón de ataque más relevante en USA fue el robo o el compromiso de credenciales, por esto, la educación en estos temas a la población en general es necesaria porque en la historia reciente y futura, estos ataques serán siempre una amenaza.

OBJETIVOS

OBJETIVO GENERAL

- Configurar un hardware utilizando PfSense aplicando sus funcionalidades de firewall y VPN para intensificar la seguridad de la navegación dentro y fuera de la red por un usuario conectado en el laboratorio de telemática de la escuela de ingeniería eléctrica en la Universidad de El Salvador.

OBJETIVOS ESPECIFICOS

- Especificar las reglas de configuración de un firewall
- Realizar la incorporación del router dedicado dentro de la infraestructura ya existente en el laboratorio de telemática de la escuela de ingeniería de la Universidad de El Salvador
- Incorporar los servicios de una VPN en un enrutador
- Incorporar los algoritmos de encriptación dentro del enrutador dedicado

ALCANCES

- Se analizará la arquitectura de red que posee en la actualidad la Universidad de El Salvador y se adaptará la implementación de una VPN y un Firewall utilizando hardware administrado por el programa pfSense. Se definirán los requisitos de hardware y software necesarios para implementar estas soluciones.
- Se realizará un estudio detallado de la infraestructura de red de la universidad, incluyendo la topología de red, los dispositivos de red utilizados y los sistemas de seguridad actuales.
- Se procederá a la adquisición del hardware compatible con el programa pfSense y se llevará a cabo su configuración de acuerdo con los requerimientos de la red de la universidad.
- Se configurará una VPN utilizando el hardware administrado por pfSense, con el objetivo de establecer conexiones seguras entre los diferentes usuarios de la escuela de ingeniería eléctrica.
- Se configurará y desplegará un Firewall utilizando el hardware administrado por pfSense para controlar el tráfico de red entrante y saliente, aplicar políticas de seguridad, detectar y prevenir posibles intrusiones y proteger la red contra programa maligno y otras amenazas.
- Se elaborará un informe detallado que documente todo el proceso de implementación, incluyendo la configuración de la VPN y el Firewall en el hardware administrado por pfSense, las políticas de seguridad aplicadas y las recomendaciones para mantener y mejorar la seguridad de la red a largo plazo.

ANTECEDENTES

La ciberseguridad en los últimos años es la rama más demandada por las empresas y del interés al público general. Los ataques cibernéticos más grandes de la historia han muchos millones de dólares a empresas multimillonarias, en algunos casos la contraseña de cientos de miles de cuentas ha sido expuestas gracias a eso.

Actualmente las empresas implementan ciberseguridad con hardware y software. En su mayoría la navegación por internet se hace mediante el uso de redes privadas virtuales VPN. La evolución de las VPN durante los últimos años ha sido al punto que hoy en día se consideran necesarias para realizar trámites clasificados por la internet. Las VPN se clasifican por especialidades como streaming, videojuegos, seguridad, wifi publico etc.

PLANTEAMIENTO DEL PROBLEMA

En el laboratorio de telemática ubicado en la escuela de ingeniería eléctrica de la Universidad de El Salvador existe una vulnerabilidad ante ataques cibernéticos al visitarse sitios no seguros, esto debido que no se cuenta con la implementación adecuada de VPN. El anonimato puede marcar la diferencia entre ser el foco de un pirata informático o no. Navegar sobre sitios no seguros mediante una IP falsa es la forma más segura de hacerlo.

JUSTIFICACION

En 2024, se cumplirán 50 años de lo que está registrado en muchos libros como la primera compra en internet. En 1974 un hombre compro una pizza por internet en estados unidos, en 1992 existían ya 1 millón de computadoras conectadas en esta red, para 1996 ya eran 10 millones. En 2022 existe un aproximado de 12,000 millones de dispositivos conectados en esta gran red. La principal diferencia es que hoy en día ya no solo se compran pizzas por internet, la delicadez de información que se maneja es valiosa. Ya no hablamos solo de tramites sencillos como comprar una pizza a diario se realizan transferencias bancarias, firmas digitales, migraciones de bases de datos, blockchain, incluso trámites legales, entre otros. En menos de lo que pensamos nuestra información más importante recaerá totalmente en la red, y se debe concientizar a futuros profesionales en ingeniería y a la población en general sobre este tema.

CAPITULO 1: FUNDAMENTOS DE LAS REDES DE COMPUTADORAS

1.1 DEFINICIÓN DE RED DE COMPUTADORAS

Una red de computadoras es un grupo de computadoras interconectadas entre si las cuales comparten informacion y recursos. Esta conexión se puede realizar de diferentes maneras, ya sea cable de cobre, fibra optica, rayos infrarrojos o microondas. De entre los diferentes recursos y la informcion que se puede compartir estan los siguientes:

- Archivos
- Aplicaciones
- Impresoras
- Correo electrónico

Las redes de computadoras ofrecen muchas ventajas. Sin ellas todos los envios de la informacion tendrian que hacerse de forma anual, por medio de diskettes o CDs. Esto seria un proceso lento. Con las redes no solo se puede intercambiar informacion a nivel local, sino que tambien a grandes distancias incluso mundiales y de forma instantanea.

1.1.1 CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS

El mundo de las redes de computadoras es muy complejo, por lo que es necesario clasificarlas para facilitar su estudio, ya que existen muchos tipos de redes. Las redes pueden ser clasificadas en cuanto a cobertura, topología y propiedad.

Cobertura:

La clasificación de redes en cuanto a cobertura se refiere a la extensión que tiene una red dentro de un área geográfica. Utilizando este criterio, las redes de computadoras se pueden clasificar de acuerdo con la tabla 1.1.

Tabla 1.1: Clasificación de las redes según cobertura

Distancia entre procesadores	Procesadores ubicados en el mismo	Clasificación
1 m	Metro cuadrado	Red de área personal (PAN)
10 m	Cuarto	Red de área local (LAN)
100 m	Edificio	
1 km	Campus	Red de área campus (CAN)
10 km	Ciudad	Red de área metropolitana (MAN)
100 km	País	Red de área amplia (WAN)
1000 km	Continente	
10000 km	Planeta	Internet

Sin embargo, esencialmente las redes pueden clasificarse simplemente como redes de área local (que abarcan desde un cuarto hasta un campus) y redes de área amplia (que abarcan distancias mayores a un campus hasta abarcar todo el planeta). Resulta más práctico clasificarlas con estas 2 distinciones para identificar las tecnologías y los dispositivos de redes.

Red de Área Local (LAN):

Es aquella red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad pequeña.

Las redes LAN tienen las siguientes características:

- Operan dentro de una zona geográfica limitada
- Permiten a los usuarios acceder a medios de gran ancho de banda
- Proporcionan conectividad de tiempo completo a los servicios locales
- Conectan físicamente dispositivos adyacentes

Las principales tecnologías LAN son las siguientes:

- Ethernet
- Token Ring
- FDDI

Siendo la tecnología Ethernet la más popular y las más difundidas de entre todas ellas.

Una red LAN puede intercomunicarse por medio de un cableado que transmita señales punto a punto; O bien, por medio de una zona de influencia de un punto de acceso (Access point) inalámbrico. La velocidad que se puede alcanzar en este tipo de red abarca desde los 100 Mbps hasta los 40,000 Gbps según el tipo de cable y conexión que se desee utilizar.

Tabla 1.2: Categorías de cables ethernet

CATEGORÍA	VELOCIDAD	FRECUENCIA	VELOCIDAD DE DESCARGA
ETHERNET CAT 5	100 Mbps	100 MHz	15,5 MB/s
ETHERNET CAT 5E	1.000 Mbps	100 MHz	150,5 MB/s
ETHERNET CAT 6	1.000 Mbps	250 MHz	150,5 MB/s
ETHERNET CAT 6A	10.000 Mbps	500 MHz	1.250 MB/s ó 1,25 GB/s
ETHERNET CAT 7	10.000 Mbps	600 MHz	1,25 GB/s
ETHERNET CAT 7A	10.000 Mbps	1.000 MHz	1,25 GB/s
ETHERNET CAT 8	40.000 Mbps	2.000 MHz	5 GB/s

En la tabla 1.2 se pueden observar los principales datos de cada una de las categorías de cable ethernet que se puedan encontrar. La velocidad determina la velocidad máxima soportada por el cable. Existen ocasiones en las que diferentes categorías soportan la misma velocidad, pero esto no significa que sean iguales, ya que hay otros parámetros como la frecuencia para tener en cuenta.

La frecuencia define la potencia de la red, suele establecer su anchura y el rango de pérdida de datos a lo largo del cable. Cuanto más largo sea un cable de red, más potencia se irá perdiendo. Por ejemplo, un cable de 1 m normalmente ofrecerá un mayor pico de velocidad que uno de 3 m, aunque la diferencia la establece la frecuencia.

De entre los diferentes aspectos que se deben tener en cuenta a la hora de elegir un cable según la función que se vaya a utilizar hay que tener en cuenta el apantallamiento electromagnético de los hilos de cobre que hay en su interior. Este apantallamiento es un blindaje que protege los cables por debajo de la cubierta de plástico, éste ayuda a la estabilidad y calidad de las velocidades de transmisión. Sin embargo, no son vitales para las instalaciones eléctricas, esto debido a que los apantallamientos se centran más en las instalaciones con fuentes electromagnéticas, como transformadores o algunos motores, y a nivel doméstico no suelen ser necesarios.

De entre los tipos de apantallamiento más utilizados se tienen los siguientes:

- UTP
- FTP
- STP
- SFTP

Red de Área Amplia (WAN): es aquella red que está formada por la interconexión de varias redes LAN. Una red WAN abarca una gran área geográfica de varios kilómetros. Este tipo de redes

son utilizadas cuando los usuarios de red necesitan acceder a los recursos de otra red. Hoy esto ocurre por ejemplo cuando las oficinas administrativas de una compañía necesitan utilizar recursos de red que se encuentran en alguna de sus diferentes instalaciones a varios kilómetros de distancia.

Las redes WAN tienen las siguientes características:

- La transmisión de datos se realiza generalmente por cable, fibra óptica o satélites
- Permiten que los usuarios mantengan comunicación en tiempo real entre sí
- Proporciona acceso a los recursos remotos de una LAN
- Es un sistema de interconexión de equipos informáticos en espacios geográficos dispersos, por consiguiente, se extiende por grandes cantidades de kilómetros

Las principales tecnologías de una red WAN son:

- Módems
- Red digital de servicios integrados (RDSI)
- Red óptica síncrona (SONET)
- Frame Relay
- Portadoras T1, E1, etc

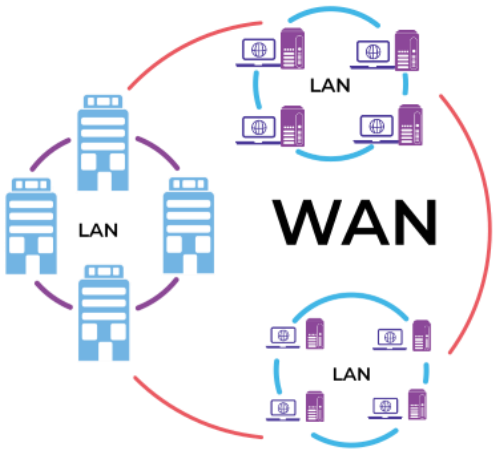

Figura 1. 1 Redes LAN conectadas a una red WAN

En la figura 1.1 se pueden observar distintas redes LAN conectadas a una WAN que pueden utilizar diferentes tecnologías.

Topología:

La topología de una red se define como un mapa físico o lógico de una red para intercambiar datos, este mapa es la forma en la que está diseñada la red. Existen cuatro tipos de red básicos de las cuales se desprenden varias combinaciones.

Estas es topología son:

Red tipo bus: En esta topología se utiliza un cable o serie de cables como eje central al cual se conectan todas las computadoras. En este conductor se efectúan todas las comunicaciones entre las computadoras, este tipo de red se utiliza principalmente cuando no son muchas las computadoras a conectar.

Red tipo estrella: Este tipo de red se caracteriza por tener un núcleo del cual se desprenden las líneas hacia varias terminales. Este tipo de topología fue de las primeras en utilizarse en el mundo de las computadoras, es útil cuando se tiene una computadora central muy potente rodeada de

máquinas de menor potencia. Esta topología es la más común porque es la que más utilizan las redes ethernet.

Red tipo anillo: este tipo de topología de red utiliza un bus como eje central para conectar todos los equipos, sin embargo, dicho bus forma un anillo. Esta topología es utilizada con mayor frecuencia en redes Token Ring y FDDI además de que es favorecida por los principales proveedores de acceso a internet.

Red tipo malla: en esta topología, todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de tipo maya suelen implementarse solamente en redes WAN.

Red tipo híbrido: la topología híbrida es una red que utiliza combinaciones de las 4 topologías mencionadas anteriormente.

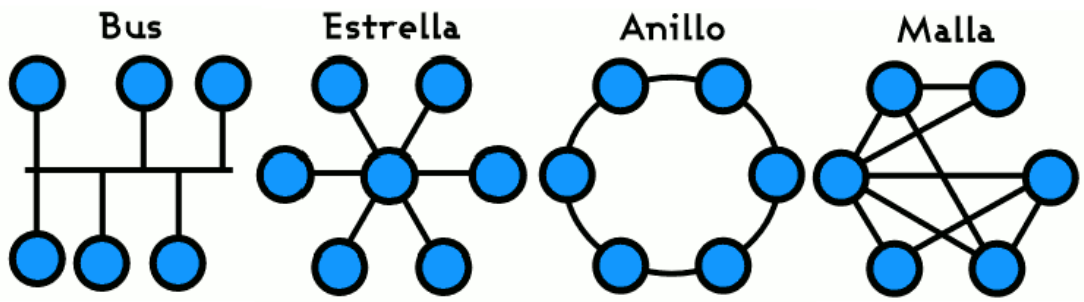

Figura 1. 2 Topologías de red

En la figura 1.2 se pueden observar las topologías de red explicadas anteriormente donde la primera es la red tipo bus, la segunda es la red tipo estrella, la tercera es la red tipo anillo y la cuarta es la red tipo malla.

Propiedad:

La clasificación de las redes en cuanto a propiedad se refiere a la forma de administración de la red. Así pues, las redes de computadoras se pueden clasificar de la siguiente forma:

Redes Privadas: Una red privada conecta un número controlado de ordenadores y suele ser local a los dispositivos físicos. Esta red está completamente separada de la red pública por lo que los datos que se mueven a través de esta red privada no están en la naturaleza por lo que no son visibles para nadie fuera de la red privada y es intocable por cualquier medio público mientras está en tránsito. Como estos datos se envían a través de una red separada, no es necesario cifrarlo mientras están en tránsito. Los datos están protegidos en base al acceso extremadamente limitado.

Características de las redes privadas:

- Es una red administrada y operada por una organización en particular.
- Casi siempre sus usuarios son los propios miembros o los empleados de la organización.
- El administrador de la red es quien puede incluir a nuevos usuarios si lo cree conveniente por una cuestión de privilegios.
- En esencia una red privada no usa los servicios de terceros para interconectarse.
- Una red privada puede solicitar los servicios de una red pública para interconectarse a través de enlaces.

Redes Públicas: Una red pública es un tipo de red en la que cualquier persona, es decir, el público en general tiene acceso y a través de ella puede conectarse a otras redes o internet. Esto contrasta con una red privada, donde se establecen restricciones y reglas de acceso para relegar el acceso a unos pocos seleccionados.

Características de las redes públicas:

- Son redes que brindan servicios de telecomunicación a cualquier usuario.
- Los usuarios se abonan mediante una suscripción o un pago aunque en algunos casos pueden ser gratuitas.
- Los usuarios también se pueden identificar como abonados por esa condición de suscripción.
- Quienes proveen a los usuarios del acceso a la red pública se conocen como proveedores de servicios de telecomunicaciones o PST.
- La red es pública no por una referencia a la privacidad de la información, sino porque está disponible el servicio para todos.
- Los proveedores de servicios de telecomunicaciones se deben acoger a las regulaciones o normativas de cada país, en términos de velar por la privacidad de sus usuarios.

1.2 COMPONENTES DE UNA RED DE COMPUTADORAS

Una red de computadoras consta de varios equipos necesarios para el correcto funcionamiento de la red. De entre los diferentes componentes de una red se pueden encontrar los dispositivos de red y el cableado de los dispositivos de red.

1.2.1 DISPOSITIVOS DE INTERCONEXIÓN DE RED

Estos dispositivos son los que conectan a los dispositivos terminales de red para formar la red y controlar el flujo de información, Estos dispositivos son el enrutador, el conmutador y el concentrador.

El concentrador o hub hoy es un dispositivo que conecta varios cables de red que llegan desde computadoras cliente a la red. Existen concentradores de diferentes tamaños en los cuales se puede

conectar desde 2 computadoras hasta más de 60 equipos. La información que llega al nodo de un hub es retransmitida a todos los demás nodos conectados en este equipo, lo que puede afectar el desempeño de una red. En la figura 1.3 se muestra gráficamente la función de un concentrador.

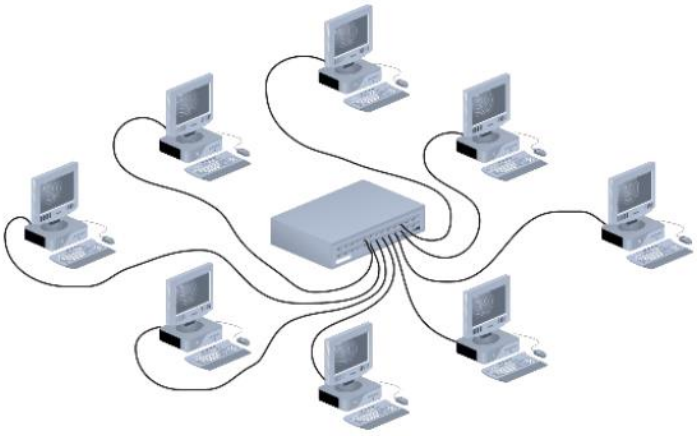

Figura 1. 3 Función del Hub dentro de la red

El conmutador o switch tal como se muestra en la figura 1.4 es un dispositivo que conmuta de forma dinámica sus distintos puertos para crear las conexiones. Un switch es un equipo semejante a un hub con la diferencia de que todas las conexiones de red tienen su propio dominio de colisión, esto hace que cada conexión de red sea privada, lo cual incrementa el desempeño de una red.

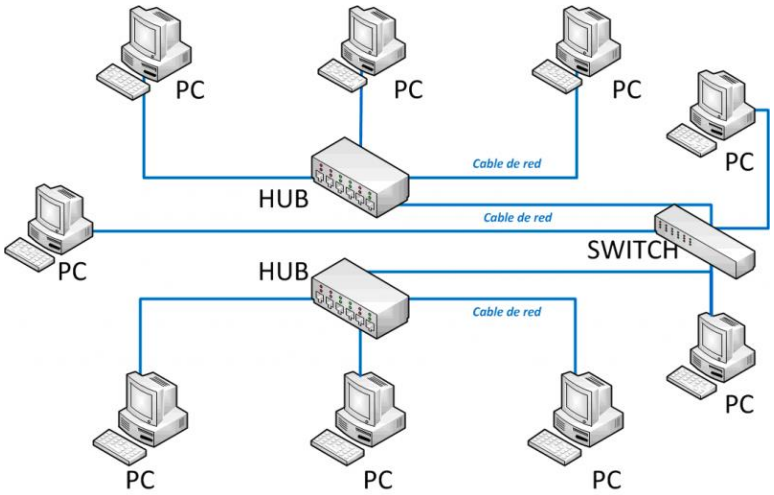

Figura 1. 4 Integración de Hub y switch en una misma red

Posteriormente se tiene el enrutador o router el cual es un equipo que direcciona los paquetes de datos de una red a otra. Las 2 redes se conectan al router usando sus propios cableados y tipos de conexión. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red. Para que un router funcione de manera correcta, necesita ser programado lo que se puede realizar conectando una PC a una terminal del router y utilizando algún software de terminal o programa en modo gráfico según sea el modelo del router.

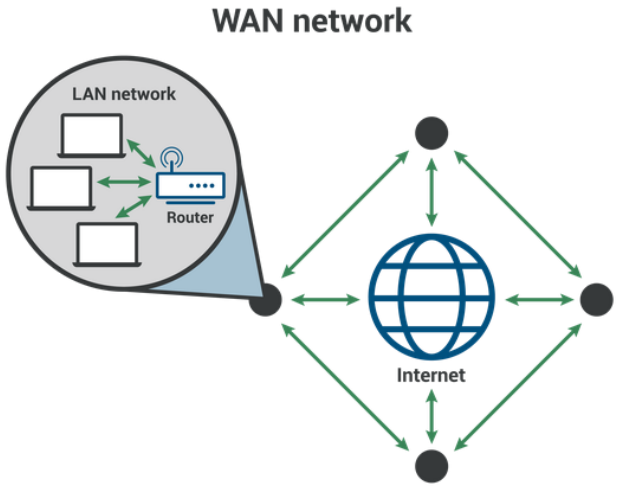

Figura 1. 5 Diagrama de red con router brindando servicio de internet

1.2.2 CABLEADO DE DISPOSITIVOS DE RED

Éste se refiere al medio físico que se usa para conectar entre sí las estaciones de trabajo de los usuarios junto con otros dispositivos o nodos de la red para lograr un intercambio de información, la elección del sistema de cableado depende de varios factores tales como el tipo de ambiente donde se va a instalar, el tipo de equipo por conectar, la aplicación y requerimientos además de la capacid ad económica.

En la actualidad se utilizan tres tipos principalmente de cables para instalar redes de computadoras, se utiliza el par trenzado y el cable coaxial como las dos opciones alámbricas y fibra óptica como tercera opción de tipo óptico. Para el primer cable mencionado es el medio de transmisión más utilizado actualmente, se trata de cuatro pares de 2 conductores de cobre forrados con plástico, torcidos entre sí y protegidos con una cubierta de plástico. De las clases más convencionales de par trenzado se tiene el UTP y el STP. Para el caso de la fibra óptica esta consiste en un núcleo central muy delgado de vidrio con alto índice de refracción de la luz el cual posee alrededor de su núcleo un revestimiento de vidrio, pero con un índice de refracción más bajo que protege el núcleo de la contaminación. La fibra óptica posee un ancho de banda muy grande y poca pérdida de señal por lo que hace que sean ideales para transmitir un gran volumen de datos y a grandes distancias, la desventaja que éste posee en la actualidad es que su instalación es muy costosa.

1.3 MODELO DE ARQUITECTURA DEL PROTOCOLO TCP/IP

El modelo OSI describe las comunicaciones de red ideales con una familia de protocolos. TCP/IP no se corresponde directamente con este modelo. TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas.

Tabla 1.3 Pila de protocolo TCP/IP

Ref. OSI Nº de capa	Equivalente de capa OSI	Capa TCP/IP	Ejemplos de protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

La tabla 3 muestra las capas de protocolo TCP/IP y los equivalentes del modelo OSI. También se muestran ejemplos de los protocolos disponibles en cada nivel de la pila del protocolo TCP/IP. Cada sistema que participa en una transacción de comunicación ejecuta una única implementación de la pila del protocolo.

Capa de red física

La capa de red física especifica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe los estándares de hardware como IEEE 802.3, la especificación del medio de red Ethernet, y RS-232, la especificación para los conectores estándar.

Capa de vínculo de datos

La capa de vínculo de datos identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. La capa de vínculo de datos proporciona también control de errores y estructuras. Algunos ejemplos de protocolos de capa de vínculo de datos son las estructuras Ethernet IEEE 802.2 y Protocolo punto a punto (PPP).

Capa de internet

La capa de Internet, también conocida como capa de red o capa IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

Protocolo IP

El protocolo IP y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

- Direcciones IP: Las convenciones de direcciones IP forman parte del protocolo IP.
- Comunicaciones de host a host: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
- Formato de paquetes: El protocolo IP agrupa paquetes en unidades conocidas como datagramas.
- Fragmentación: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

Protocolo ARP

El protocolo de resolución de direcciones (ARP) se encuentra conceptualmente entre el vínculo de datos y las capas de Internet. ARP ayuda al protocolo IP a dirigir los datagramas al sistema receptor adecuado asignando direcciones Ethernet (de 48 bits de longitud) a direcciones IP conocidas (de 32 bits de longitud).

Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red. ICMP registra:

- Paquetes soltados: Paquetes que llegan demasiado rápido para poder procesarse.
- Fallo de conectividad: No se puede alcanzar un sistema de destino.
- Redirección: Redirige un sistema de envío para utilizar otro enrutador.

Capa de transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como transmisión de punto a punto. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

Protocolo TCP

TCP permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. Este protocolo TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

- Punto de partida, que abre la conexión.
- Transmisión completa en orden de bytes.
- Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

TCP confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción. Por tanto, el protocolo TCP se considera un protocolo fiable orientado a la conexión.

1.4 ACCESO REMOTO Y CONEXIONES WAN

Antes de que la VPN fueran tomadas como opción para el acceso remoto, era común que una corporación instalara módems desde los cuales el usuario remoto hacía una llamada para estar en conexión con la red corporativa. En redes donde no hay muchos usuarios remotos se pueden agregar solo uno o dos módems a una computadora configurada como servidor de acceso remoto (RAS, Remote Access Server). El acceso remoto utilizado de esta manera resulta ser costoso y requiere de un gran soporte por parte de las empresas. Frecuentemente, los usuarios se encuentran muy alejados de las oficinas centrales de las compañías y tienen que realizar llamadas de largas

distancias o llamada 0-800. Esto resulta ser especialmente costoso si las llamadas son internacionales y si los trabajadores requieren estar conectados durante un tiempo prolongado.

Conexiones WAN

Existen diversas tecnologías o conexiones para poder unir diferentes redes LAN y crear una red WAN. Un enlace WAN puede ser conmutado o dedicado. Por conmutado se entiende que es aquel que no está disponible todo el tiempo, la conexión se establece solo cuando es necesaria. Un ejemplo de esto es una conexión de acceso telefónico a redes a través de un módem. Por otra parte, un enlace dedicado es aquel donde la conexión siempre estará disponible, incluso cuando no se esté utilizando. Las conexiones WAN se pueden clasificar de la siguiente manera:

- Servicios de conmutación de circuitos
- Servicios de conmutación de paquetes
- Servicios de conmutación de celdas
- Servicios digitales dedicados
- Servicios de marcación, cable e inalámbricos

CAPITULO 2: DEFINICIÓN DE RED PRIVAD A VIRTUAL (VPN)

Una red privada virtual es una red privada que utiliza la infraestructura de una red pública para poder transmitir información, una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos (Amazon Web Services, 2022). La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. Un usuario de una red virtual no será capaz de detectar la red física, el solo podrá ver la red virtual.

Desde la perspectiva del usuario la VPN es una conexión punto a punto entre el equipo (Cliente VPN) y el servidor de la organización (Servidor VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado. Esta estructura se puede apreciar de mejor manera en la figura 2.1.

Figura 2. 1 VPN como red virtual

De los conceptos de red privada y red virtual se tiene el concepto de red privada virtual, debido al hecho de ser una red privada que utiliza una red pública, la seguridad de una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones, en una red pública como internet existen muchos programas y personas que están dispuestas a robar información. Debido a esto es que las VPN deben de poseer

excelentes mecanismos de autenticación y de encriptación en la información para que este viaje a través de una red pública.

Los componentes básicos de una VPN son los siguientes:

- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de transito
- Cliente VPN

2.1 CLASIFICACIÓN DE LAS VPN

- VPN de acceso remoto: Este modelo consiste en que los usuarios se conectan desde un sitio remoto y se utiliza internet como un vínculo de acceso y después de ser autenticados se puede decir que el nivel de acceso que poseen es como el de una red local.
- VPN punto a punto: En este modelo la arquitectura a seguir es la de conectar los nodos remotos con la matriz o punto central. El servidor VPN debe detener un vínculo permanente con internet y debe de aceptarlas conexiones provenientes de los sitios y establecer el llamado túnel VPN; mientras que los puntos externos deben de utilizar los servicios de su proveedor local de internet por medio de banda ancha, a este fenómeno también se le conoce como tuneleo (tunneling).
- VPN interna: esta opción tiene las mismas cualidades de una VPN tradicional, la única diferencia es que en lugar de utilizar internet como medio de acceso utiliza la red local del edificio donde se encuentra, con lo cual su nivel de seguridad es mayor que cualquier red Wi-Fi.

- VPN basada en firewall: Este tipo de VPN aprovecha los mecanismos de seguridad del servidor de seguridad, incluyendo la restricción del acceso a la red interna, realiza la traducción de direcciones, satisfaciendo los requerimientos de autenticación. La mayoría de los firewalls comerciales también optimizan el núcleo del sistema operativo al despojar a los servicios innecesarios o peligrosos, proporcionando seguridad adicional para el servidor VPN. La desventaja de este tipo de tecnología es poder optimizar su desempeño de manera eficiente sin mermar las aplicaciones del sistema operativo.
- VPN basado en software: Este tipo de VPN hoy es ideal en casos donde ambos extremos de la VPN no están controlados por la misma organización o cuando diferentes firewall y enrutadores se implementan dentro de la misma.

2.2 ARQUITECTURAS DE LAS VPNS

Dentro de las posibles arquitecturas que encontramos en las VPN se pueden mencionar las siguientes:

- Proporcionada por un servidor de Internet: El proveedor de Internet puede instalar en su oficina un dispositivo que se encargará de la creación del túnel para la organización.
- Basadas en firewalls: De la misma forma en que las VPN trabajan en los niveles más bajos del modelo OSI, el firewall actuará de la misma forma.
- Basadas en Caja Negra: Básicamente es un dispositivo con software de cifrado. No provee seguridad en la organización, pero si en los datos. Para suplir esta carencia se pueden utilizar un firewall en serie o paralelo al dispositivo de VPN.
- Basadas en Enrutadores: Puede ser en este caso que el software de cifrado se añada al enrutador ya existente o bien que se utilice una salida exclusiva de otro proveedor.

- Basadas en acceso remoto: El cliente tiene software por el cual se conecta al servidor de VPN de la corporación a través de un túnel cifrado.
- Basadas en software: Por lo general se utiliza de un cliente a un servidor de VPN que está instalado en alguna estación de trabajo. Es necesario tener procesos de administración de claves y un emisor de certificados.

2.3 PROTOCOLOS

Algunos de las tecnologías y protocolos usados para habilitar las VPNs sitio-a-sitio incluyen:

- IPSec: Consiste en un conjunto de protocolos diseñados para proteger el tráfico del IP entre puertas de enlace seguras. Mientras este transita entre redes intermedias.
- GRE: Puede ser usado para construir túneles y transportar tráfico multiprotocolo entre dispositivos CE en una VPN. GRE tiene una pequeña o ninguna seguridad, pero los túneles GRE pueden ser protegidos usando IPSec.
- Draft Martini (cualquier transporte sobre MPLS [AToM]): El trasporte de datos tipo Draft Martini habilita un trasporte de datos del tipo punto-a-punto de protocolos del tipo Frame Relay, ATM, Ethernet, Ethernet VLAN (802.1 Q), HDLC (High-Level Data Link Control) y tráfico PPP sobre MPLS.
- L2TPv3: permite el transporte punto-a-punto de protocolos tales como Frame Relay, ATM, Ethernet, Ethernet VLAN, HDLC, y tráfico PPP sobre IP.
- MPLS LSPs: Una LSP es una ruta a través de una LSR (Label Switch Routers) en una red MPLS. Los paquetes son entregados en base a etiquetas agregadas al paquete. LSP puede ser señalizado usando TDP (Tag Distribution Protocol), LDP (Label Distribution Protocol), o RSVP (Resource Reservation Protocol).

También se requieren otros protocolos y tecnologías para permitir el acceso remoto, tales como:

- L2F (Layer Two Forwarding): L2F es un protocolo propietario de Cisco que fue diseñado para permitir encapsulamiento de tramas PPP (o SLIP [Serial Line Interface Protocol]) entre un sistema NAS y un dispositivo de puerta de enlace VPN ubicado en un sitio central. Los usuarios de acceso remoto conectados a un sistema NAS, y las tramas PPP de los usuarios de acceso remoto son entonces encapsulados sobre la red hacia la puerta de enlace VPN de origen y destino.
- PPTP (Point-to-Point Tunneling Protocol): PPTP es un protocolo que fue desarrollado por un grupo de empresas, incluyendo Microsoft, 3Com, y Ascend Communications. Como L2F, PPTP permite el encapsulamiento de tramas PPP de clientes de acceso remoto entre sistemas NAS y una VPN gateway. Los paquetes encapsulados PPP llevados sobre túneles PPTP son usualmente protegidos usando MPPE (Microsoft Pointto-Point Encryption).
- L2TPv2/L2TPv3 (Layer 2 Tunneling Protocol versions 2 and 3): L2TP es una norma de la IETF (Internet Engineering Task Force) que combina las mejores cualidades de L2F y PPTP. En un ambiente de acceso remoto, L2TP permite tanto encapsulamiento de las tramas PPP de los clientes de acceso remoto a través de sistemas NAS a una puerta de enlace VPN como encapsulamiento de tramas PPP directamente desde el cliente de acceso remoto al concentrador/puerta de enlace VPN. L2TP tiene una seguridad intrínseca limitada por lo cual los túneles L2TP son usualmente protegidos con IPSec.
- IPSec: Así como se habilitan VPNs sitio-a-sitio, IPSec también puede ser usado para asegurar tráfico de datos a través de túneles entre usuarios tanto de acceso remoto como usuarios móviles y un concentrador o puerta de enlace VPN.

- SSL (Secure Sockets Layer): es un protocolo de seguridad que originalmente fue desarrollado por Netscape Communications (SSL versiones 1, 2, y 3), y provee de acceso remoto seguro para usuarios móviles y usuarios. Puede estar limitado funcionalmente (comparado con L2F, PPTP, L2TPv2, o IPSec) si son desplegadas VPNs clientless con SSL de acceso remoto.
- TLS (Transport Layer Security): Es un estándar IETF muy similar a SSLv3.

Una ventaja es que no se requiere ningún tipo de software adicional porque SSL es incluido en cualquier navegador Web.

2.4 CONEXIONES Y SEGURIDAD EN LAS VPN

La conectividad que las VPNs puedan tener estará en función de qué tipo de políticas de seguridad se implementen y las respectivas herramientas que se utilicen para lograrlo. Será importante tomar en cuenta las ventajas y desventajas que cada opción pueda ofrecer a fin de poder elegir aquella de acuerdo con los requerimientos que sean necesarios.

Una VPN sin seguridad deja de ser privada, la cual es uno de los principales objetivos de esta. La seguridad en las VPNs se describe con tres aspectos:

- Privacidad (Confidencialidad): los datos transmitidos sólo deberán estar disponibles para el receptor autorizado.
- Confiabilidad (Integridad): la información transmitida no deberá cambiar entre el receptor y el emisor.
- Disponibilidad: la información trasferida deberá estar disponible cuando sea necesaria.

Todas estas metas deberán lograrse usando software confiable, hardware, IPS's y políticas de seguridad.

Una política de seguridad define las responsabilidades, procedimientos estandarizados, y los controles de daños además de los escenarios de recuperación que se prepararán para la peor situación posible.

Entendiendo que el daño máximo posible y el costo de la recuperación de la peor catástrofe posible pueden dar una idea de cuánto esfuerzo deberá gastarse en la seguridad. La seguridad en las VPNs se logrará protegiendo el tráfico con modernos y fuertes métodos de cifrado, técnicas de autenticación segura y firewalls controlando el tráfico que se genera desde y hacia el túnel. Cifrar el tráfico no es suficiente, hay grandes diferencias en términos de seguridad dependiendo del método que se implemente.

2.5 CERTIFICADOS Y AUTENTICACIÓN DE UNA VPN

Existen otros métodos para asegurar las comunicaciones entre los puntos involucrados, como es el uso de SSL/TSL. Estas capas usan el cifrado asimétrico, el cuál funciona de manera distinta que el cifrado simétrico. Para este caso, ambos puntos de comunicación tienen dos llaves cada uno: una pública y otra privada. La llave pública es la que se maneja sobre las comunicaciones, con la cual se cifra la información. Y sólo aquel que posea el otro par de las llaves, en este caso la llave privada, podrá descifrar los datos.

La autenticación de usuarios es un mecanismo implementado en las VPNs en el punto de acceso de estas, el cual es usado para garantizar que solo las personas que se autentican pueden acceder a la red y a sus recursos. Los esquemas que se pueden implementar individualmente o en combinación con otros incluyen los siguientes:

Identificación de usuario y clave de acceso (Login ID y password): Este esquema usa la autenticación basada en la identificación del usuario y la clave de acceso basada en el sistema para verificar la identidad del usuario que accede al nodo VPN.

Clave de acceso secreta: En este esquema el usuario inicia la clave secreta seleccionando una palabra clave secreta y un número entero, n. Este número entero denota el número de veces que una función hash (actualmente MD4) será aplicada a la clave misma. El resultado es almacenado en el servidor correspondiente. Cuando los usuarios intenten acceder al sistema, el servidor llevará a cabo el procedimiento de autenticación. El software que el usuario usa para intentar la conexión solicitará la palabra clave, aplicará n-1 iteraciones de la función hash a la palabra clave, y se la enviará al servidor.

El servidor aplicará la función hash a esta respuesta, si el resultado obtenido es el mismo que el valor almacenado anteriormente, la autenticación fue exitosa. El usuario es entonces autorizado a ingresar al sistema.

RADIUS: Es un protocolo de seguridad de Internet que está fuertemente basado en el modelo cliente/servidor, donde la máquina que ingresa a la red es el cliente y el servidor RADIUS, en el punto de acceso, autentica al cliente. Generalmente los servidores RADIUS autentican al usuario usando una lista de nombres de usuario y claves de acceso que mantienen internamente. RADIUS puede también actuar como un cliente para autenticar usuarios de los sistemas operativos, tales como UNIX, NT y NetWare. Adicionalmente, los servidores RADIUS pueden actuar como clientes para otros servidores RADIUS. Para asegurar aún más la información durante las transacciones entre los clientes y los servidores RADIUS esta puede ser cifrada usando mecanismos de autenticación, tales como el protocolo de autenticación de claves (Password Authenticaction

Protocol PAP) y el protocolo de autenticación por aviso mutuo (CHAP Challenge Handshake Authentication Protocol)

Como este nombre lo sugiere, el esquema implementa la autenticación dual para verificar las credenciales del usuario. Combina el uso de un token y de una clave de acceso. Durante el proceso de autenticación, un dispositivo electrónico sirve como token y como identificador único, tales como el número personal de identificación (PIN Personal Identification Number) que es usado como la clave de acceso.

Control de acceso: Después de que los usuarios se han autenticado exitosamente, estos ganan acceso a los recursos permitidos, servicios de red y aplicaciones localizadas en la misma. Esto puede ser un problema de seguridad porque el usuario, incluso el que ya está autenticado, puede encontrarse con la información almacenada en varios dispositivos, sabiéndolo o no.

Los permisos de control de accesos son una parte integral del propio control. Los problemas de seguridad pueden ser manejados otorgando privilegios limitados a los usuarios. Por ejemplo, la información puede ser salvaguardada permitiendo a los usuarios no privilegiados sólo permisos de lectura de cierta información. Sólo los usuarios autorizados y el administrador deben de tener los privilegios para escribir, modificar o borrar información.

El control de accesos está basado en la identificación del usuario. Aunque otros parámetros, tales como la dirección IP de origen y la de destino, los puertos, y grupos, juegan un papel importante en el esquema tradicional de control de accesos.

Los mecanismos modernos y avanzados de control de accesos se basan en otros parámetros tales como el tiempo, día, aplicaciones, servicios, métodos de autenticación, URLs, y mecanismos de cifrado.

Cifrado de Información

El cifrado de información o la criptografía es uno de los componentes más importantes de la seguridad de las VPNs y juega un papel primordial en la seguridad de la información durante su tránsito por las redes. Es el mecanismo de convertir la información a un formato ilegible, conocido como texto cifrado, así los intentos desautorizados de acceder a la información se pueden prevenir mientras la información es transmitida a través de un medio inseguro.

El cifrado de información previene inconvenientes como:

- Interceptación de la información y su lectura.
- Modificación de la información y su robo detectable.
- Fabricación de información.
- No-repudio de información.

Certificados Digitales

Un certificado digital es el equivalente electrónico de una identificación y es usado para identificar a una entidad única durante la transmisión. Además de establecer la identidad del dueño, los certificados digitales también eliminan las oportunidades de suplantaciones, reduciendo la oportunidad de la fabricación de información, y adicionalmente previenen efectivamente el rechazo de pertenencia de la información.

Un certificado digital consiste en información que ayuda a validar al emisor e incluye la siguiente información:

- El número de serie del certificado
- La fecha de finalización del certificado

- La firma digital del certificado de autorización (CA)
- La llave pública del propietario (PKI)

Durante la transacción, el emisor debe de enviar su certificado digital durante la transmisión con un mensaje cifrado para autenticarse a sí mismo. Como en el caso de las llaves públicas, la llave pública CA es ampliamente publicada y disponible a todo el mundo.

Sistema de distribución de certificados (CDS Certificate Distribution System)

El sistema de distribución de certificados es un repositorio para los usuarios y las organizaciones, adicionalmente un CDS genera y almacena pares de llaves, firma llaves públicas después de validarlas y almacena y remueve las llaves perdidas y caducas.

2.6 APLICACIONES Y ADMINISTRACIÓN DE VPN

El hardware VPN es básicamente para servidores VPN, clientes VPN y otros dispositivos de hardware, tales como enrutadores VPN y concentradores.

Servidores VPN

Generalmente, los servidores VPN son hardware dedicado corriendo software de servidores. Dependiendo de los requerimientos de la organización, puede haber uno o más servidores VPN. Como los servidores VPN deben de proveer servicio a los clientes remotos y locales, estos están siempre operativos y listos para las peticiones.

Las principales funciones de los servidores VPN incluyen las siguientes:

- Escuchar peticiones de conexión VPN.
- Negociar parámetros y requerimientos de conexión, tales como los mecanismos de cifrado y autenticación.

- Autenticación y autorización de clientes VPN.
- Aceptar información del cliente o la petición de reenvío de información del cliente.
- Actuar como el punto final del túnel VPN y la conexión. El otro punto de conexión se provee por las peticiones del usuario a la conexión VPN.

Clientes VPN

Los clientes VPN son máquinas locales o remotas que inicializan la conexión VPN a un servidor VPN y se introducen a la red remota después de haberse autenticado en el extremo de esta. Después de un acceso exitoso pueden comunicarse mutuamente el servidor VPN y el cliente. Generalmente un cliente VPN es basado en software.

Aunque también puede ser un dispositivo de hardware dedicado. Un enrutador VPN basado en hardware con capacidades de conexión en demanda que se comunica con otro dispositivo VPN es un ejemplo de hardware dedicado. Con el incremento de una plantilla de trabajo móvil, muchos usuarios (clientes VPN) pueden tener perfiles de roaming. Estos usuarios pudieran haber usado una VPN para comunicarse con la Intranet del corporativo como, por ejemplo:

- Usuarios móviles con laptops, palmtops, y notebooks los cuales usan redes públicas para conectarse con la Intranet de la organización accediendo a los correos y otros recursos de la Intranet.
- Administradores remotos los cuales usan las redes intermedias, tales como la Internet, para conectarse a una red remota para administrar, monitorear, diagnosticar, o configurar servicios y dispositivos.

Enrutadores VPN, Concentradores, y gateways

En el caso de la configuración de una VPN pequeña, el servidor VPN puede tomar una ruta para conectarse. Generalmente, un enrutador es el último extremo de una red privada a menos que esté detrás de un firewall. El papel de un enrutador VPN es hacer accesible las partes remotas de una Intranet. Por lo cual, los enrutadores son responsables de hallar posibles rutas hacia la red de destino y de escoger la ruta más corta del conjunto de rutas, como en el caso de las redes tradicionales.

Aunque los enrutadores tradicionales pueden ser usados en las VPNs, los expertos recomiendan usar enrutadores especialmente optimizados para las VPNs. Estos enrutadores, adicionalmente al enrutamiento, proveen seguridad, escalabilidad, y calidad de servicio (QoS) en la forma de redundancia en las rutas.

Para mantener a una VPN en óptimo estado de trabajo y con un rendimiento adecuado, deberán cuidarse algunos aspectos importantes. Debe recordarse que el desempeño de una VPN depende en gran medida del desempeño de los servidores VPN y de la infraestructura que se utilice. Se deberá revisar el desempeño de los servidores cuando menos una vez a la semana, para evitar cualquier imprevisto que baje el desempeño. Es recomendable tener bitácoras detalladas de cada actividad relacionada con la VPN. Adicionalmente se deberán transferir dichas bitácoras a otra máquina para que en caso de que un intruso gane acceso este no pueda alterarlas.

2.7 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 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. (Jones, J. P., 2022)

La tabla mostrada es los anexos de este documento es una comparación de los proveedores VPN comerciales más demandados, clasificados según velocidad, precio, países disponibles, etc. (Migliano, S, 2023).

Acorde a la documentación oficial de pfsense este es compatible con varios proveedores de VPN vistos en esta tabla (pfSense. Netgate, 2022). 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 naturaliza 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. (NordVPN, 2022).

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. (ExpressVPN, 2022).

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 le universo lleva existiendo, y aun así posiblemente no tener éxito.

CAPITULO 3: FIREWALL

3.1 INTRODUCCIÓN A FIREWALL

Los primeros dispositivos de firewall (o "cortafuegos") aparecieron a mediados de la década de 1980. Desde los primeros firewalls que implementaron filtros de paquetes simples y rudimentarios hasta los dispositivos actuales que pueden analizar simultáneamente la actividad en varias capas de una red, la tecnología ha evolucionado enormemente para crear herramientas más sofisticadas y seguras.

La popularización de Internet ha creado una serie de problemas de seguridad y, según todos los expertos, esta preocupación por la seguridad inherente a las redes hoy en día es el principal obstáculo para una actividad exitosa en el campo del comercio electrónico. Los cortafuegos se han convertido, por tanto, en dispositivos imprescindibles en la arquitectura de cualquier red informática que tenga acceso a Internet.

3.2 SEGURIDAD EN TCP/IP

A pesar de que la familia de protocolos TCP/IP fue desarrollada inicialmente para el Departamento de Defensa de los Estados Unidos, existen en ella un número considerable de graves problemas de seguridad que son inherentes al protocolo e independientes del nivel de corrección de cualquier implementación.

El hecho de que un host confíe en algo tan vulnerable como la dirección IP que viene escrita en un paquete como única autenticación de la procedencia de dichos datos, los casi inexistentes mecanismos de autenticación asociados a los protocolos de enrutamiento o la falta de mecanismos que garanticen la confidencialidad y la integridad de los datos que viajan a través de una red son

claros ejemplos de ello. Algunos de estos problemas pueden ser solventados mediante el uso de un cortafuegos.

Los cortafuegos, junto con los antivirus, constituyen hoy en día la herramienta de seguridad más efectiva y ampliamente extendida a nivel corporativo (y crece poco a poco a nivel doméstico gracias a la proliferación de cortafuegos personales) y se revela como el único mecanismo de seguridad verdaderamente efectivo para protegernos de estas vulnerabilidades intrínsecas al protocolo TCP/IP.

Los principales riesgos de una organización con salida a Internet son los mismos que debemos tener en cuenta a la hora de proteger un sistema cualquiera: confidencialidad, integridad y disponibilidad. Los siguientes son los ataque más frecuentes y populares que vulneran estos principios:

- Sniffers
- Suplantación de IP o Spoofing
- Ataques de contraseñas
- Control de salida ilegal información sensible desde una fuente interna
- Ataques de Hombre en el medio (o man-in-the-middle attacks)
- Ataques de Denegación de Servicio, Denial of Service o ataques DoS
- Ataques a nivel de aplicación para explotar vulnerabilidades conocidas
- Caballos de Troya (Trojan Horses), Virus y otros códigos maliciosos

El nivel de protección que puede proporcionar un firewall varía mucho según sus necesidades. Por ejemplo, imaginemos que solo necesitamos enviar y recibir correos electrónicos, un cortafuegos nos protege eficazmente de ataques que no tienen como objetivo este servicio.

Los cortafuegos generalmente se configuran para protegernos de cualquier intento de acceso. Autenticación no autorizada o incorrecta de fuera a dentro de la red o viceversa. Pero más allá de eso, una de las cosas más importantes a considerar es su firewall. Proporciona un único punto de entrada inevitable a la red donde se pueden centralizar las mediciones seguridad y pruebas para ello.

Son tres las principales amenazas sobre las cuales un cortafuegos no puede protegernos.

Las dos primeras son evidentes, un cortafuegos no puede protegernos contra amenazas que no pasan a través de él. Como decíamos en el punto anterior, el cortafuegos debe de ser el punto único e ineludible de acceso a nuestra red. Si esto no es así su efectividad es sólo parcial. Tampoco pueden protegernos, generalmente, contra amenazas que proceden del interior de nuestra red. Un empleado malicioso, un troyano o algunos tipos de virus pueden usar mecanismos válidos 'desde dentro' para realizar acciones maliciosas.

Por último, los cortafuegos no pueden protegernos contra clientes o servicios que admitimos como válidos pero que son vulnerables. Tampoco puede protegernos contra mecanismos de tunneling sobre HTTP, SMTP u otros protocolos. No son muy efectivos, a pesar de que algunos fabricantes así lo anuncian, contra los virus. Los cortafuegos no pueden ni deben sustituir otros mecanismos de seguridad que reconozcan la naturaleza y efectos de los datos y aplicaciones que se estén manejando y actúen en consecuencia.

3.3 TIPOS, TECNOLOGÍAS Y GENERALIDADES

Los cortafuegos son dispositivos o sistemas que controlan el flujo de tráfico entre dos o más redes empleando ciertas políticas de seguridad. Básicamente son dispositivos cuya funcionalidad se limita a permitir o bloquear el tráfico entre dos redes en base a una serie de reglas. Su complejidad reside en las reglas que admiten y en como realizan la toma de decisiones en base a dichas reglas.

La tecnología utilizada en los cortafuegos se ha convertido en una industria especializada por lo que en la actualidad hay muchos dispositivos diferentes que realizan esta función de diferentes maneras. Una manera conveniente y fácil de comparar las ventajas de cada plataforma es observar las capas del modelo OSI mostrado en la figura 3.1, con las que interactúa el cortafuegos.

La clasificación conceptual más simple divide los cortafuegos en dos tipos:

- Cortafuegos a nivel de red (trabajan en las capas 2, 3 y/o 4)
- Cortafuegos a nivel de aplicación (trabajan en las capas 5, 6 y/o 7)

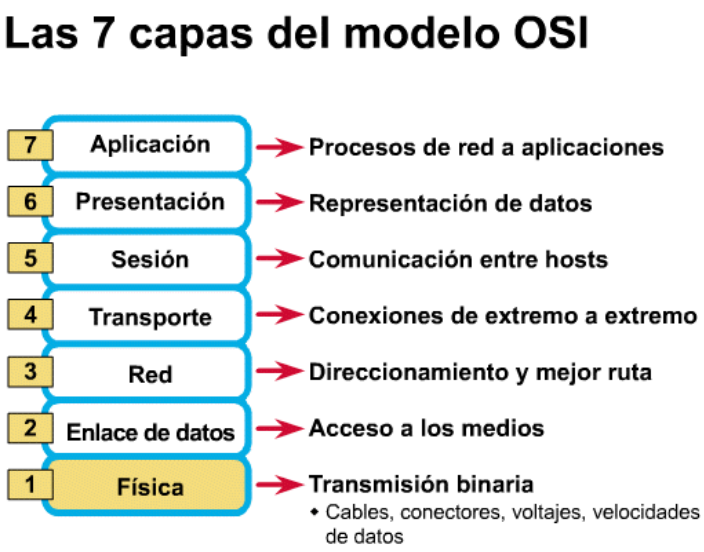

Figura 3. 1 Modelo OSI

Como regla general, se puede afirmar que cuanto más bajas sean las capas en las que el cortafuegos trabaja, su evaluación será más rápida y transparente pero su capacidad de acción ante ataques complejos es menor.

3.4 TIPOS DE FIREWALL

Cortafuegos de filtrado de paquetes

Se ocupa de tomar decisiones de procesamiento basadas en direcciones de red, puertos o protocolos**.** En general, son muy rápidos porque no hay mucha lógica detrás de las decisiones que toman. No hacen ninguna inspección interna del tráfico, ni tampoco almacenan ninguna información del estado. Deben abrirse los puertos manualmente para todo el tráfico que fluirá a través del firewall. Un hecho, que, sumado a las limitaciones de este sistema, hace que se considere uno de los tipos de cortafuegos menos seguros.

Esto se debe a que reenviará cualquier tráfico que fluya en un puerto aprobado y, por lo tanto, podría enviarse tráfico malicioso, porque, siempre que esté en un puerto aceptable, no se bloqueará.

Puerta de enlace a nivel de circuito

Una puerta de enlace de nivel de circuito opera en la capa de transporte de los modelos de referencia de Internet o OSI y, como su nombre indica, implementa el filtrado a nivel de circuito en lugar del filtrado a nivel de paquete. Este firewall comprueba la validez de las conexiones (es decir, circuitos) en la capa de transporte (generalmente conexiones TCP) contra una tabla de conexiones permitidas, antes de que se pueda abrir una sesión e intercambiar datos.

Las reglas que definen una sesión válida prescriben y, una vez que se permite una sesión, no se realizan más verificaciones, ni siquiera a nivel de paquetes individuales.

Entre las desventajas de las puertas de enlace a nivel de circuito se encuentran la ausencia de filtrado de contenido y el requisito de modificaciones de software relacionadas con la función de transporte.

Firewall de inspección con estado

Este es uno de los tipos de firewall capaces de realizar un seguimiento del estado de la conexión. Los puertos se pueden abrir y cerrar dinámicamente si es necesario para completar una transacción. Por ejemplo, cuando se realiza una conexión a un servidor utilizando HTTP, el servidor iniciará una nueva conexión al sistema en un puerto aleatorio. Un firewall de inspección con estado abrirá automáticamente un puerto para esta conexión de retorno.

Habitualmente, se consideran más seguros que los de filtrado de paquetes, ya que procesan los datos de la capa de aplicación y, por ese motivo, pueden profundizar en la transacción para comprender lo que está sucediendo.

Puerta de enlace de nivel de aplicación (también conocido como firewall proxy)

Este tipo de firewalls operan en la capa de aplicación del modelo OSI, filtrando el acceso según las definiciones de la aplicación. Se considera como uno de los firewalls más seguros disponibles, debido a su capacidad para inspeccionar paquetes y garantizar que se ajusten a las especificaciones de la aplicación. Dada la cantidad de información que se procesa, los firewalls de la puerta de enlace de aplicaciones pueden ser un poco más lentos.

Firewall de próxima generación

Un cortafuegos de próxima generación ofrece un filtrado de paquetes básico o una toma de decisiones basada en proxy dentro de las capas 3 y 4 del modelo OSI disponible dentro de los firewalls tradicionales y con estado (Cisco, Cortafuegos, 2022). Sin embargo, amplía su protección

al tomar también decisiones en la capa de aplicación (es decir, la capa 7). Las características que definen a este novedoso cortafuegos son la identificación y control de aplicaciones, autenticación basada en el usuario, protección contra programas malignos, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación.

Las empresas que deseen una protección completa que les blinde contra las amenazas, no deberían conformarse con ninguno de los tipos de firewall previos al de próxima generación, a no ser que opten por una combinación de ellos que les garantice la eficacia deseada. En un entorno en el que la ciberseguridad es vital (Cisco, 2022).

3.5 TRANSLACIÓN DE DIRECCIONES (NAT)

El valor añadido frente a los cortafuegos actuales son los servicios adicionales que ofrece ya que facilitan la tarea de asegurar y administrar la red. Se trata de servicios en algunos casos hechos a medida y en otros habituales de otros dispositivos pero que, en cualquier caso, representan un punto importante a la hora de decidirnos por una u otra implementación.

El servicio NAT (Network Address Translation) resuelve dos problemas principales:

En primer lugar, son herramientas muy útiles. Eficaz para ocultar la dirección de red real de su red interna. En segundo lugar, y debido a la reducción del espacio de direcciones IP disponibles, muchas organizaciones usan NAT para permitir la salida a Internet de sus equipos de la red interna con un mínimo de direcciones legalmente válidas.

Existen tres estrategias diferentes a la hora de implementar NAT:

- Translación de Direcciones de Red Estática: En este esquema de NAT cada sistema interno de la red privada tiene su propia dirección IP exterior. Con este sistema se logra esconder el esquema interno de nuestra red, pero no la reducción de direcciones IP válidas de acceso

al exterior. Los cortafuegos que incluyen esta característica usan para ello una simple tabla de correspondencia entre unas direcciones y otras.

- Translación de Direcciones de Red Oculta: Con este esquema todos los sistemas de la red interna comparten la misma dirección IP externa. Reviste dos importantes inconvenientes: es imposible poner a disposición de los usuarios externos ningún recurso de la red interna, y obliga al Cortafuegos a usar su propia dirección externa como sustituta de la dirección de todos los equipos que protege, con lo cual implícitamente estamos revelando la dirección de este y lo hacemos susceptible de ser atacado directamente, además de restarle flexibilidad al sistema.
- Translación de Puertos: El sistema de translación de puertos (PAT) resuelve los dos problemas vistos en el esquema anterior, convirtiéndolo en la mejor forma de implementar NAT. En primer lugar, no es necesario usar la dirección externa del Cortafuegos, sino que podemos crear otra dirección virtual para este propósito. En segundo lugar, es posible hacer accesibles recursos internos a los usuarios del exterior. El cortafuegos usa el puerto del cliente para identificar cada conexión entrante y construye a tal efecto una tabla de traslaciones como la mostrada a continuación:

  La translación de puertos se realiza de forma secuencial en algunos sistemas (como el de la tabla del ejemplo anterior) y aleatoria, dentro de un rango de puertos válidos, en otros. Se trata, de los tres esquemas vistos, del más conveniente, flexible, seguro y por tanto el más ampliamente usado en la actualidad.

3.6 REDES PRIVADAS VIRTUALES (VPN)

Uno de los servicios adicionales más valorados de los Cortafuegos actuales es la posibilidad d construcción de Redes privadas Virtuales (VPN o Virtual Private Networks) que permiten extender a las comunicaciones externas la seguridad del interior de nuestra red.

Una VPN se construye en la cúspide de la pila de protocolos ya existentes en la red usando protocolos adicionales y fuertes cifrados y mecanismos de control de integridad, sustitución o repetición de la información transmitida.

Existen diferentes formas de construir una VPN. Quizás la forma más lógica y comúnmente usada es utilizar para ello el estándar IPSec., consistente en una porción de las características de seguridad de IPv6 separadas y portadas para ser usadas en IPv4. Otras opciones son el estándar propuesto por Microsoft llamado PPTP (Point to Point Tunneling Protocol) o L2TP (Layer 2 Tunneling Protocol), propuesto por la IETF (Internet Engineering Task Force).

El motivo por el que se coloca el servidor de VPN en el cortafuegos es evidente: colocarlo detrás de él haría que el tráfico cifrado entrante y saliente generado por el servidor VPN no pudiese ser inspeccionado totalmente y hubiera que obviar funciones como las de autenticación, logging, escaneo de virus etc. sobre todo este tráfico. Colocando el servidor VPN detrás del cortafuegos lo hacemos vulnerable a ataques directos, el principal problema de las VPN es el elevado coste de recursos que supone el cifrado completo de las comunicaciones lo cual reduce considerablemente el ancho de banda efectivo que somos capaces de tratar. Una solución para mitigar este problema es usar una tarjeta cifradora por hardware, las cuales suelen reducir en aproximadamente un 50% el tiempo necesario en realizar la encriptación.

Funciones de inspección y autenticación

La función de inspección de contenido es uno de los servicios adicionales más interesantes que ofrecen los Cortafuegos a nivel de aplicación por lo que para realizar una inspección de contenidos en el tráfico HTTP y SMTP se incluyen los siguientes elementos:

- Applets de Java
- Código ActiveX, JavaScript o CGI
- Inspección de virus (binarios y de macro)
- Inspección del contenido de ciertos formatos (.zip, .doc, .xls, .ppt, etc.)
- Bloqueo de contenidos en base a URLs, direcciones IP y/o palabras clave
- Bloqueo de comandos específicos de determinadas aplicaciones

Otro servicio básico en los cortafuegos a nivel de aplicación es la autenticación de usuarios que en los dispositivos a nivel de red debe limitarse a la dirección IP de procedencia de la petición, con el consiguiente riesgo de suplantación, mientras que en estos pueden habilitarse servicios clásicos de combinación login y password.

CAPITULO 4: HARDWARE E IMPLEMENTACION

4.1 SISTEMAS DE ENRUTAMIENTO

4.1.1 ENRUTAMIENTO

El enrutamiento de red es el proceso de seleccionar una ruta a través de una o más redes. Los principios de enrutamiento se pueden aplicar a cualquier tipo de red, desde redes telefónicas hasta transporte público. En una red de conmutación de paquetes, como Internet, el enrutamiento es la ruta que toman los paquetes del Protocolo de Internet (IP) desde el origen hasta el destino. Estas decisiones de enrutamiento en Internet las toma un hardware de red especializado llamado enrutadores.

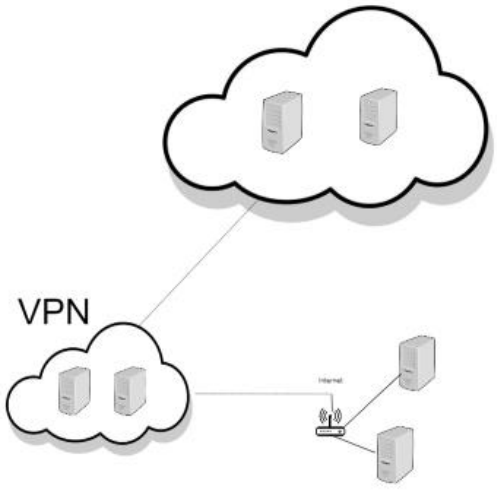

Figura 4. 1 Diagrama de implementación

4.1.2 EL ENRUTADOR

Un enrutador es una pieza de hardware de red responsable de reenviar paquetes de datos a sus destinos. Un enrutador conecta dos o más redes IP o subredes y envía paquetes de datos entre ellas según sea necesario. Los enrutadores se utilizan en hogares y oficinas para crear conexiones de red de área local. Los enrutadores más potentes funcionan en cualquier parte de Internet y ayudan a que los paquetes de datos lleguen a sus destinos.

Para esta instancia se utiliza la mini PC PROTECTLI modelo FW4B-0-4-32 el cual cuenta con 32GB de memoria interna y una memoria RAM de 4 GB

4.2 VPN Y ENRUTADOR

¿Qué es un router VPN?

En términos sencillos, es cuando se ejecuta una VPN en un router, cifrando de forma efectiva los datos de todos los dispositivos conectados a tu red: el cifrado de datos en toda la red con solo un dispositivo que tenga una VPN. Aparte de eso, un router VPN también puede referirse a un router especialmente hecho para alojar una VPN (porque no todos los routers tienen la opción de ejecutar una VPN).

Al ser Pfsense un software, se necesita hacer uso de un hardware para poder instalarlo, o hacer uso de máquinas virtuales para simularlo (VM VirtualBox, VMware Workstation, etc.).

El proceso de instalación del software Pfsense es similar a cualquier sistema operativo, se debe tener establecido si el software se descargara como imagen ISO o como instalador USB y posteriormente descargarlo en una USB formateada y configurada como soporte de arranque, en la figura 4.2 se muestra la configuración de descarga como instalador USB.

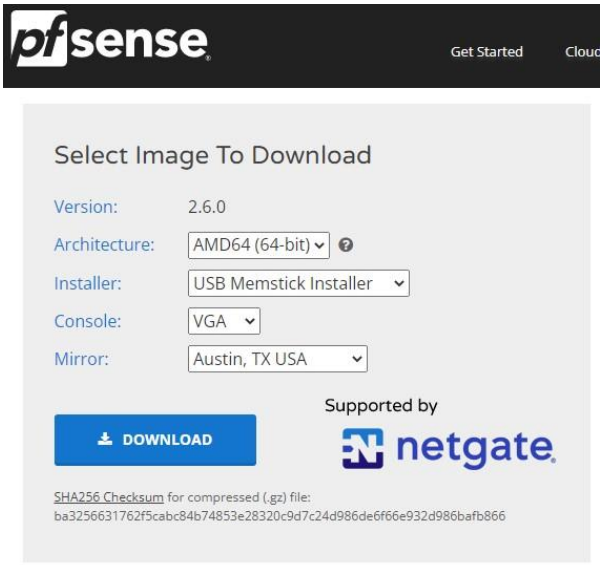

Figura 4. 2 configuración de descarga de Pfsense

Al momento de tener descargada la imagen de Pfsense, se necesita formatear y configurar una USB como soporte de arranque. Existen diversos programas que cumplen con esta función, en este caso se utiliza el programa Rufus en su versión 3.20 para configurar la imagen de Pfsense como opción de formateo de USB tal como se observa en la figura 4.3.

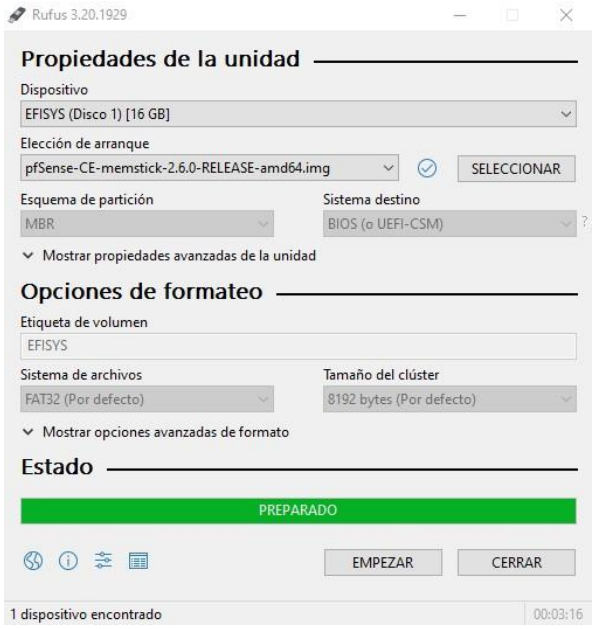

Figura 4. 3 Configuración de Rufus para USB como motor de arranque

Posteriormente se conecta la USB en la mini PC para poder realizar la configuración del software de Pfsense, para esto se utilizó un monitor y teclado debido a que la mini Pc cuenta con puertos HDMI, puertos RJ45 y puertos USB. Se configura Pfsense con la configuración recomendada que se brinda en el instalador.

Al tener el software Pfsense corriendo, el modelo FW4B utilizado como mini Pc cuenta con 4 puertos de red (WAN, LAN, OPT1 y OPT2) de los cuales se hará uso del puerto WAN al cual se conecta el proveedor de internet que se tenga contratado y el puerto LAN se conecta a un Cisco Switch para poder conectar varios dispositivos dentro de la red privada que se va a configurar posteriormente en Pfsense.

4.2 DIAGRAMAS DE IMPLEMENTACION

La ciberseguridad de muchas organizaciones se basa en gran parte en la configuración de un firewall que aísla el contacto directo entre la red local y la internet, un solo puerto de salida para monitorear el tráfico entrante y saliente. La figura 4.4 identifica el estado el laboratorio previo a nuestra intervención. Para el caso de aplicación en el laboratorio de telemática de la escuela de ingeniería eléctrica en la universidad de El Salvador es igual. 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.

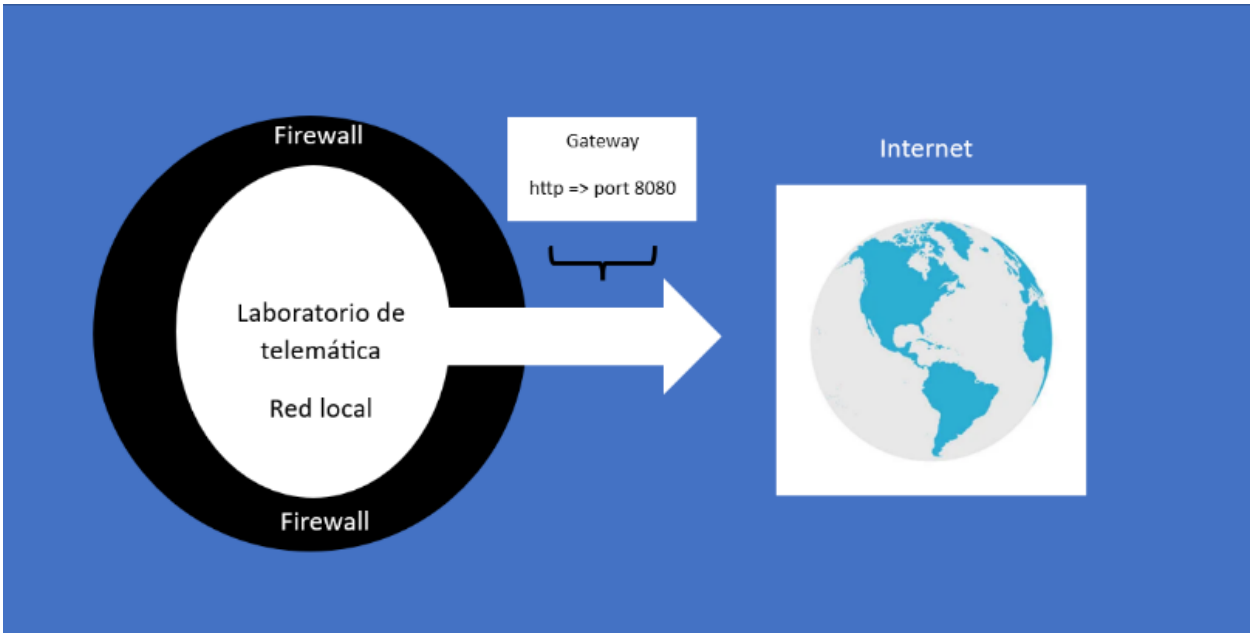

Figura 4. 4 Diagrama de estructura de ciberseguridad

En la figura 4.5 se observa el diagrama con el router con VPN incorporado. El router con VPN incorporada se instalará en el puerto permitido 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.

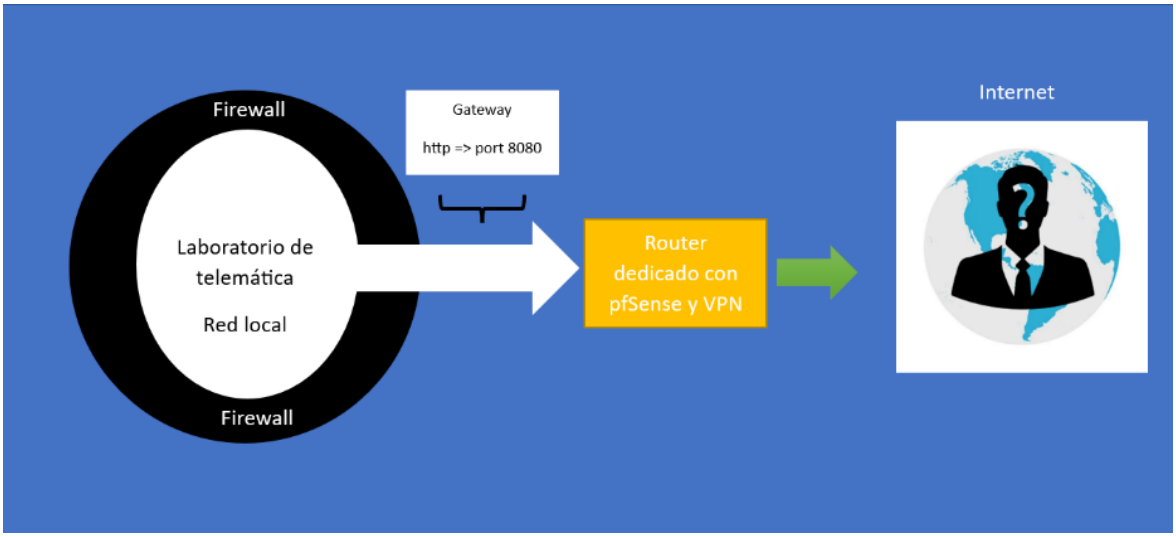

Figura 4. 5 Diagrama de implementación del router dedicado a la estructura existente

4.3 CONFIGURACION DE PFSENSE

Se debe tomar en cuenta que el puerto LAN al que se encuentra conectada la PC brinda una dirección ip diferente a la de nuestro proveedor de internet, por lo que para poder acceder a la interfaz web de Pfsense se debe buscar la dirección ip que se le asigna a la PC en uso por medio del protocolo de DHCP. En caso de estar utilizando Linux, el comando a utilizar es "ip address", en caso de estar utilizando Windows existen diferentes formas de solicitar esta información, ya sea utilizando la terminal del sistema y utilizando el comando "ipconfig" o accediendo a las configuraciones de red en la sección de propiedades de red. Pfsense cuenta con una configuración de red por defecto la cual tiene una dirección 192.168.1.0 por lo que el gateway para acceder en el navegador web es 192.168.1.1. Las credenciales por defecto que tiene configuradas Pfsense para nombre de usuario es "admin" y la contraseña es "pfsense".

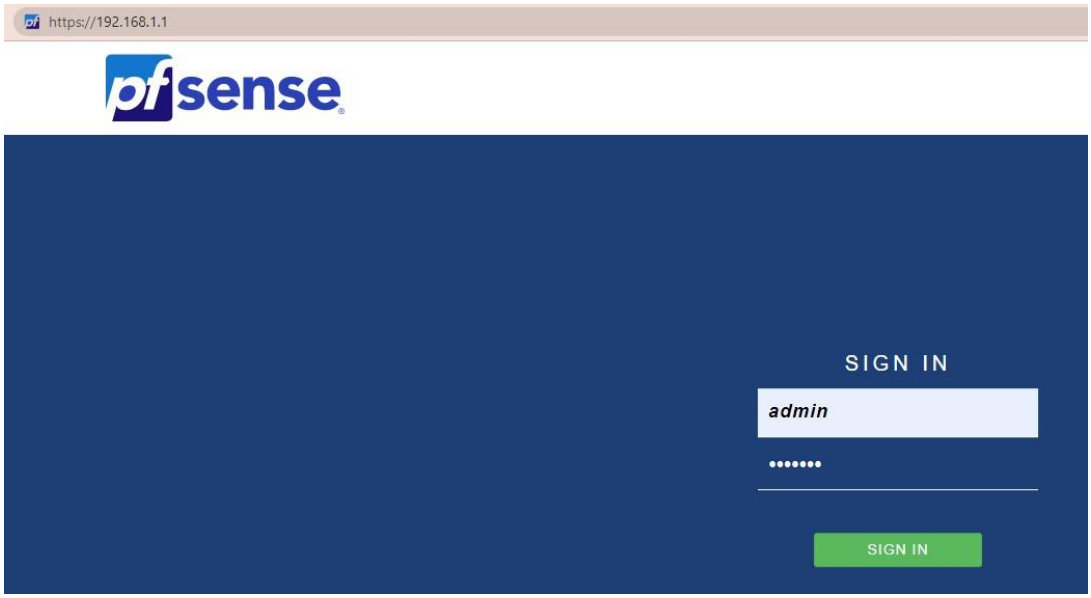

Figura 4. 6 interfaz web de pfsense

Al entrar en la interfaz web de Pfsense tal como se observa en la figura 4.6, se despliega una configuración inicial la cual se deja por defecto, debido a que lo que se 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 permite 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 mascara 24 tal como se observa en la Figura 4.7.

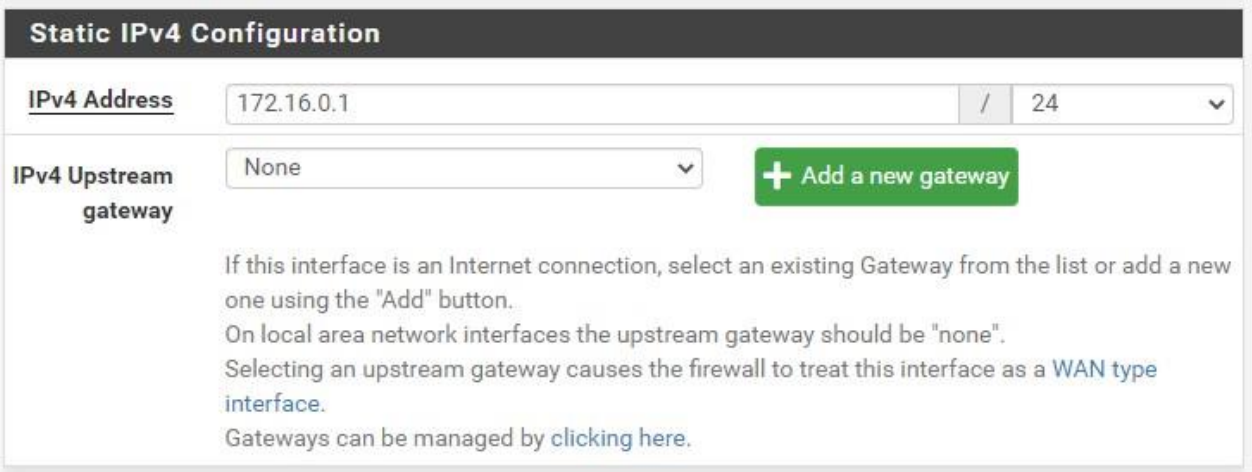

Figura 4. 7 Configuración de red privada en interfaz LAN

Posteriormente se puede configurar una contraseña diferente a la que trae el software Pfsense por defecto, al momento que tengamos estas configuraciones finalizadas y aplicadas tenemos que refrescar la página e introducir la nueva dirección ip que se ha configurado para la red privada, además en caso de cambiar las configuraciones de las credenciales de acceso se debe tomar en cuenta ya que estos cambios ya están aplicados. Una de las maneras para revisar si el software Pfsense ha realizado los cambios de manera correcta es nuevamente utilizar los comandos especificados anteriormente y poder así obtener y visualizar las configuraciones de red que se tienen en el ordenador. En caso de no visualizar los cambios se utiliza en Linux el comando “sudo

dhclient -r" y en caso de estar utilizando Windows desde la terminal del sistema utilizando el comando "ipconfig /release". Estos comandos se utilizan para liberar y renovar la dirección ip en ambos sistemas operativos, posteriormente los cambios en la configuración de red estarían aplicados.

4.4 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. El tablero principal de Pfsense brinda información de sistema, interfaces, unidades de memoria, etc. además puede brindar información adicional como estado de 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 necesitan 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 4.8.

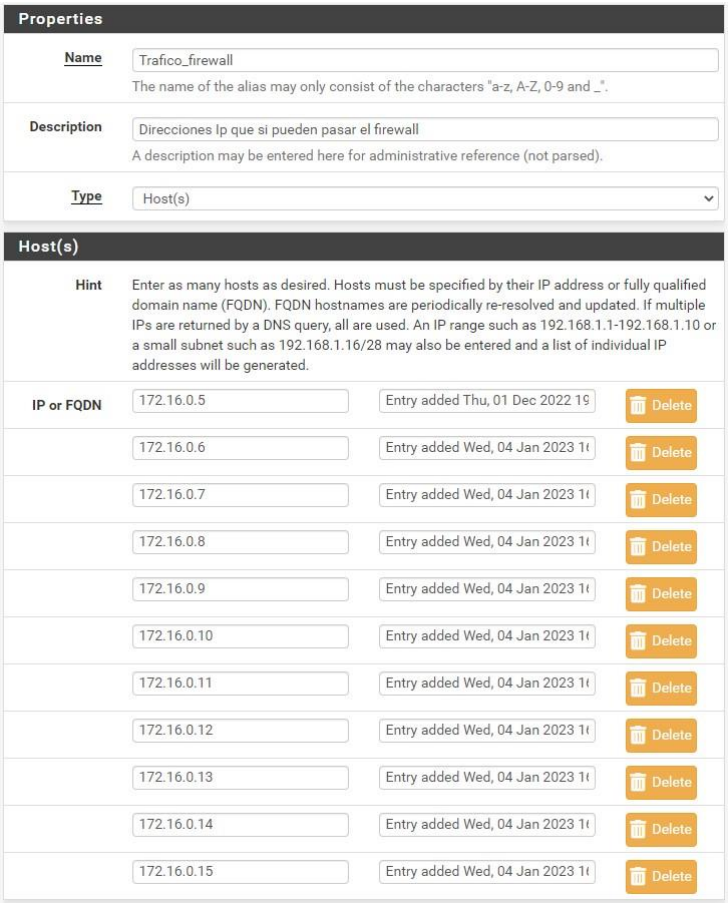

Figura 4. 8 Configuración de Aliases

Teniendo configurado el grupo de direcciones ip, es posible configurar las reglas del firewall con mayor facilidad. Debido a que es la red privada a la que se le aplican las reglas, al entrar a las configuraciones de reglas para el firewall se selecciona la interfaz LAN para realizar las configuraciones. En primera instancia se pueden observar las reglas por defecto que Pfsense aplica al firewall (no se modifican), se agrega una regla donde se asigna el grupo de direcciones ip las cuales utilizan el gateway configurado con la conexión VPN para poder llegar a internet, se le asigna una descripción y se guarda tal como se observa en la Figura 4.9. Dentro de las configuraciones se tiene la opción "Action", esta opción dicta el comportamiento de la regla dentro del firewall ya que se especifica si se deja pasar, se bloquea o se rechaza las direcciones ip. El protocolo por defecto que trae la configuración es TCP, se cambia a la configuración de cualquier

protocolo y posteriormente en opciones avanzadas se modifica la gateway de WAN a la gateway configurada con el servicio de la VPN.

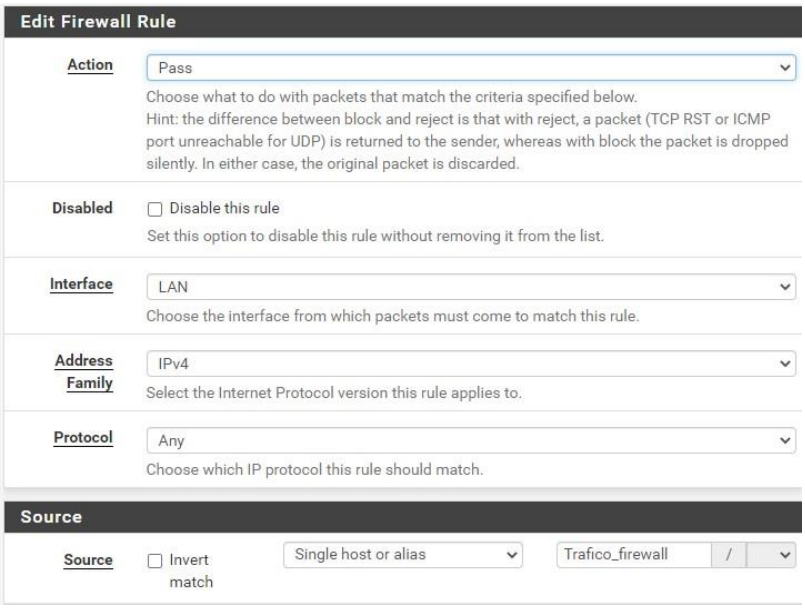

Figura 4. 9 Configuración de reglas dentro de firewall

Teniendo la sección referente al firewall de manera funcional, queda la configuración de la VPN por donde pasaría el tráfico de la red. Una VPN es una red privada virtual que le permite al usuario asegurar la actividad de la red de manera que solo sea conocida por parte del proveedor y el mismo usuario, superficialmente funciona de la misma manera que una red privada domestica por lo que la información y los archivos que se comparten a través de una encriptación VPN son seguros y se mantienen separados del resto de internet.

4.5 CONFIGURACION DE VPN

Una red domestica se maneja a través de un router local mientras que una VPN (red privada virtual) se maneja de forma virtual, para poder utilizar una VPN el cliente y el proveedor deben instalar un software que permita a las maquinas comunicarse entre sí y al mismo tiempo garantiza el cifrado de la VPN. El proveedor es controlado en la mayoría de los casos a través de un servidor de acceso remoto o RAS (remote access server) y 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 estará encapsulada de manera que no se podrá interceptar, alterar o incluso vigilar su actividad, esto gracias a que envía 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.

De entre los protocolos utilizados en el proceso de canalización se tiene el protocolo de túnel punto a punto (PPTP), protocolo de túnel de capa 2 (L2TP), protocolo de túnel de sockets seguros (SSTP) y el protocolo de OpenVPN la cual se utiliza por parte de pfsense y consta de una aplicación de software de código abierto que utiliza conexiones punto a punto que utiliza tanto SSL como TLS para el intercambio de claves. Este protocolo de OpenVPN a diferencia del protocolo L2TP puede ejecutarse a través de puertos UDP o TCP, lo que permite eludir firewalls.La VPN se configura a través del software pfsense utilizando la configuración de OpenVPN, para esto se ha seleccionado el proveedor NordVPN y se elige el servidor recomendado por parte de NordVPN para poder obtener los protocolos disponibles para el servidor, en este caso se utiliza el protocolo TCP con puerto 443. Para configurar la VPN, en la configuración del sistema se introduce el certificado del protocolo TCP para el servidor de EUA (cada servidor posee un certificado diferente) tal como se observa en la Figura 4.10.

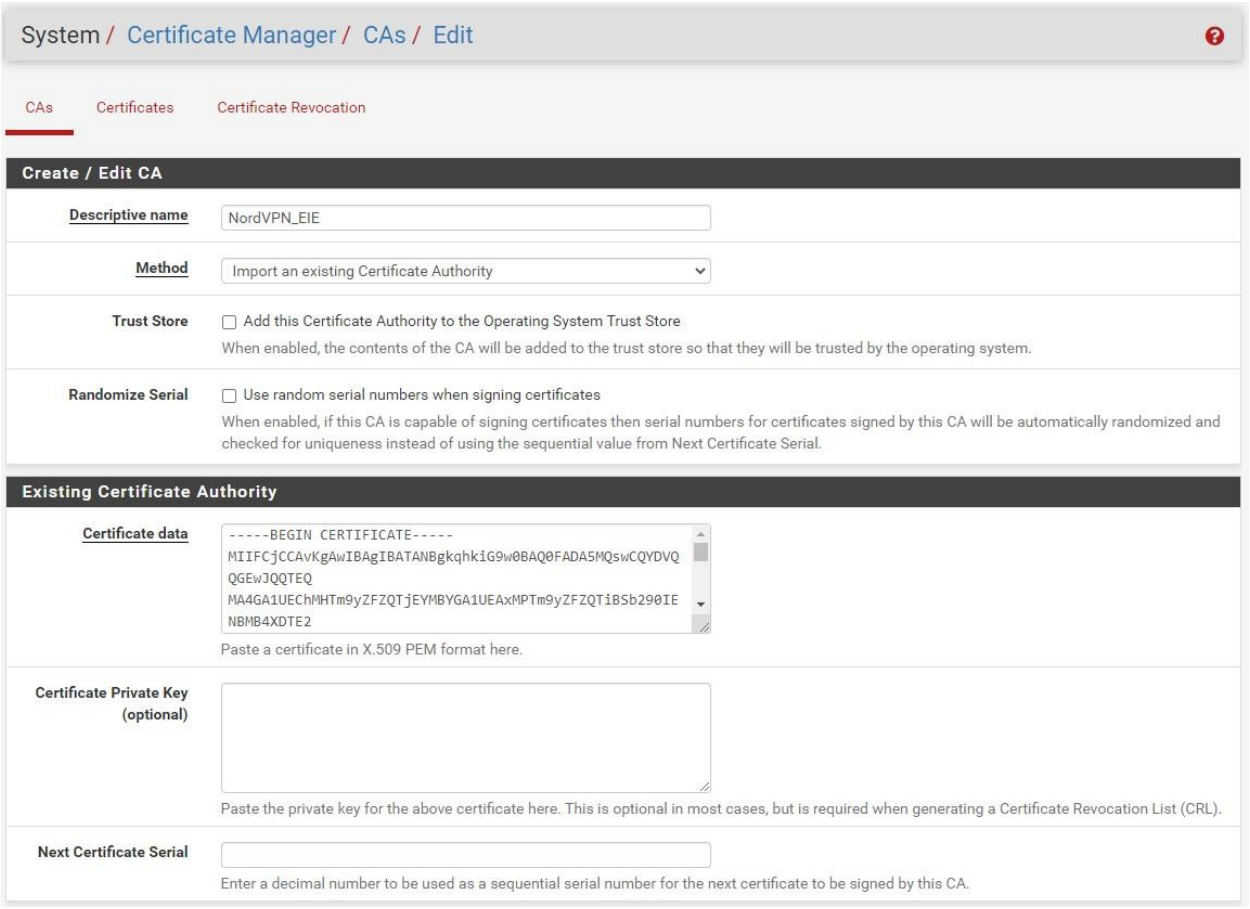

Figura 4. 10 Configuración de certificado de VPN

Posteriormente se configura el cliente de la VPN en el apartado de OpenVPN, se selecciona el modo del servidor "Peer to Peer (SSL/TLS)" y se selecciona el protocolo que se utilizara para la configuración, para este caso se selecciona el protocolo TCP para direcciones IPV4 y sale por el puerto al cual se tiene la conexión del proveedor de internet (WAN). En esta configuración se debe especificar la autentificación de usuario por parte del proveedor de la VPN. Esta información se obtiene dentro del sitio del proveedor. Posteriormente se configuran los valores del proveedor criptográfico donde se establecen los algoritmos y paquetes de cifrado, valores de nombres de identidad, valores del almacén de claves de cifrado y los valores de la entidad emisora de certificados (CA). Estos valores son configurados según el protocolo TCP obtenido por parte del proveedor de la VPN.

Dentro de las opciones avanzadas de la configuración del cliente se tiene el apartado de la creación del puerto virtual, en este apartado se establece la opción única para direcciones IPV4. Posteriormente en el apartado de interfaces, inicialmente se tienen dos interfaces configuradas por defecto (WAN y LAN). Se debe crear y habilitar la interfaz para la VPN, la cual en este caso se le asigno el nombre del proveedor "NordVPN" tal como se observa en la figura 4.11.

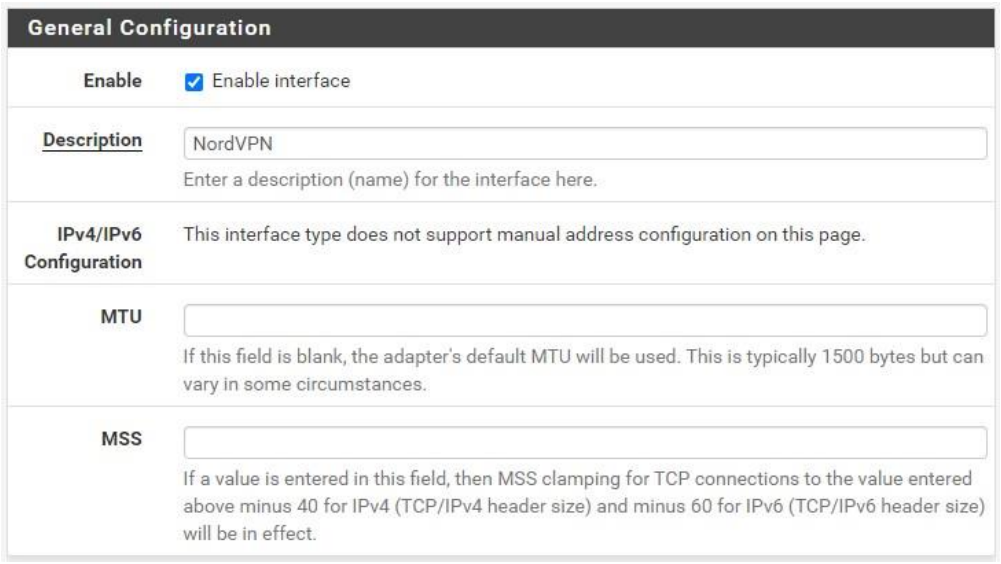

Figura 4. 11 Configuración de interfaz para el uso de la VPN

Teniendo la interfaz configurada, en el apartado de servicios-DNS resolver donde se habilita para cumplir su función como convertidor de nombre de dominios a direcciones ip. Dentro de las configuraciones se tiene la opción de interfaces de salida y el certificado SSL/TLS, en la sección de interfaces de salida se debe colocar como única interfaz de salida la que fue configurada previamente y que se le dio el nombre en este caso como "NORDVPN". Esto para que el servidor DNS utilice únicamente la interfaz de la VPN para enviar consultas a servidores autorizados y recibir a su misma vez sus respuestas. Esta opción trae de manera predeterminada el uso de todas las interfaces disponibles. En la sección del certificado SSL/TLS se coloca el denominado "Web Configurator default, en caso no este por defecto similar a la figura 4.12.

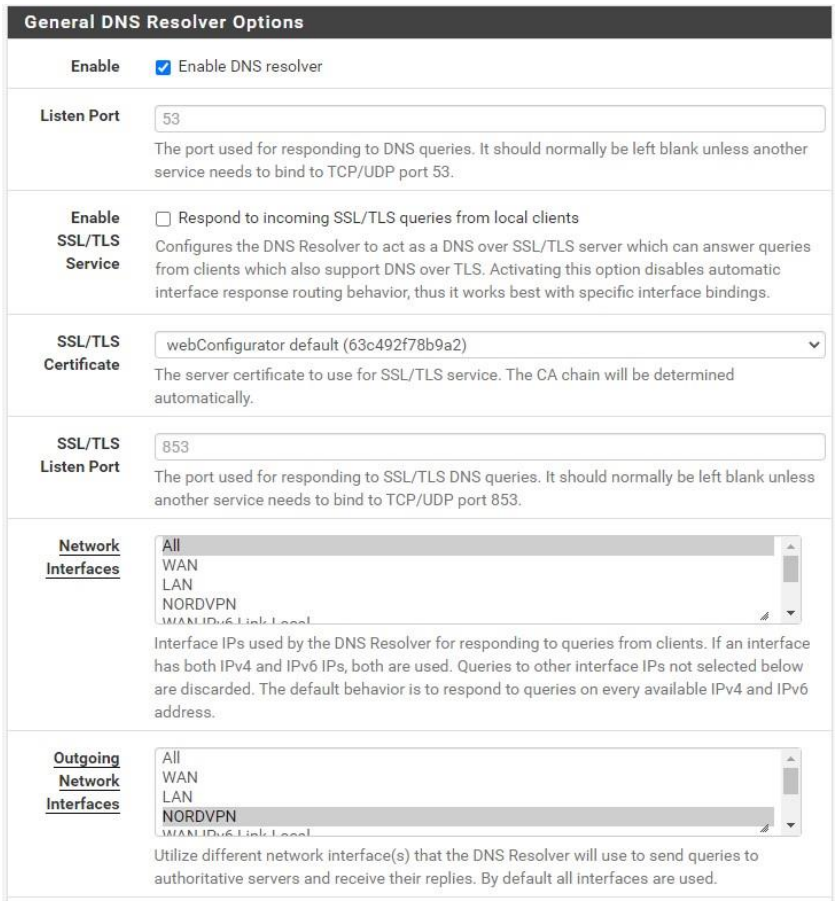

Figura 4. 12 Configuración de general de DNS resolver

Uno de los fines del uso del proveedor de VPN es brindar anonimato al momento de generar tráfico hacia internet por lo que se debe habilitar dentro de las opciones avanzadas del servicio DNS resolver la opción de identidad oculta y a su vez la versión tal como se observa en la figura 4.13.

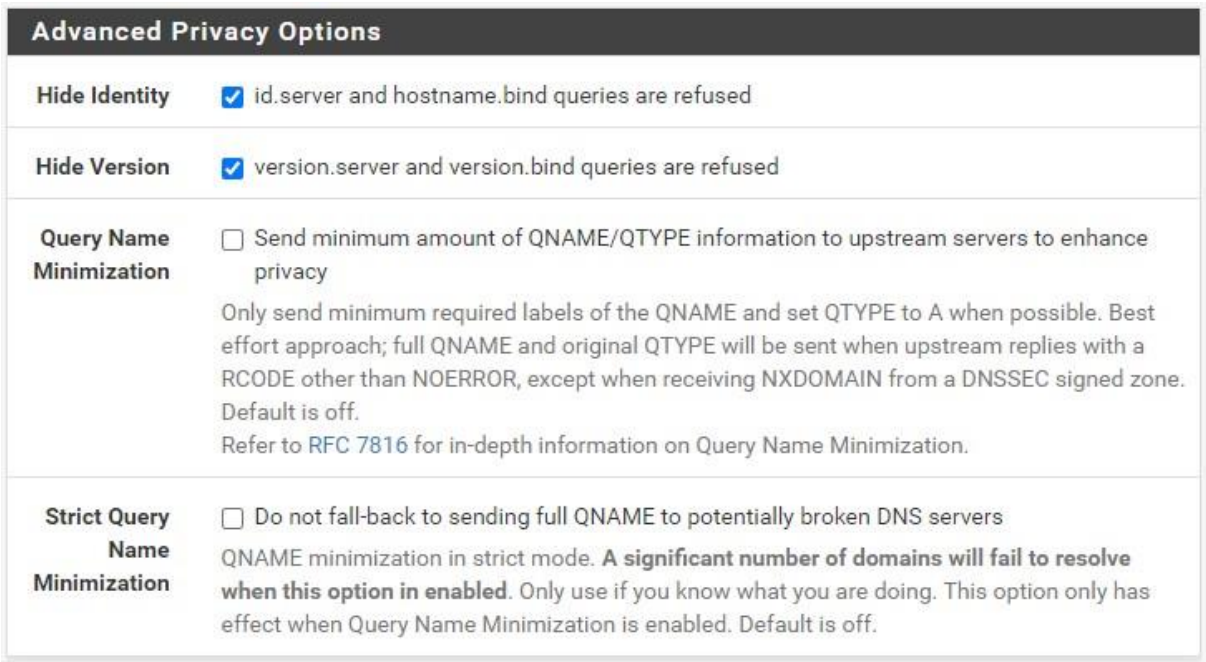

Figura 4. 13 Configuración de DNS resolver para identidad oculta

Teniendo la configuración de la VPN finalizada se configuran las reglas necesarias para poder habilitar la traducción de direcciones de la red, dentro del apartado firewall se selecciona NAT y el modo de NAT saliente o "outbound NAT mode" se selecciona la opción el modo manual de

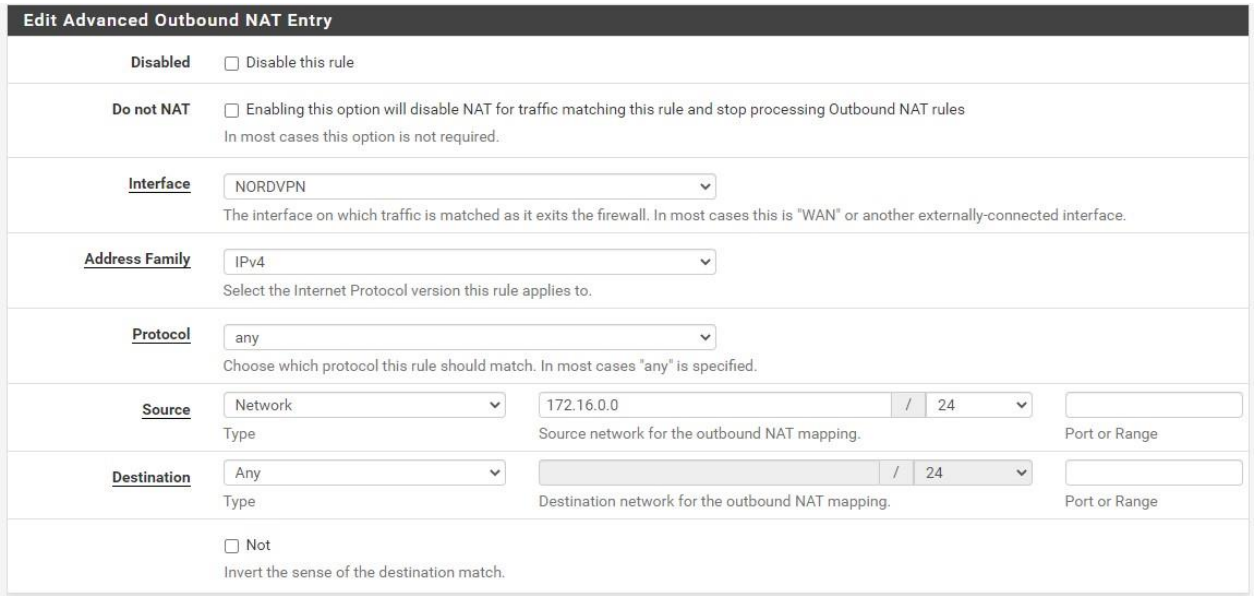

Figura 4. 14 Configuración de NAT para la red privada

generación de reglas. Posteriormente se deja tal cual están las reglas generadas por defecto y se agrega una regla para poder identificar la red privada especificando que serán de tipo IPV4 en el apartado “address family” y se especifica en la sección de protocolo la opción “any” tal como se observa en la figura 4.14.

Como ultima configuración se deben configurar los servidores en pfsense, en este caso el proveedor brinda los servidores DNS que son server 1(103.86.96.100) y server 2 (103.86.99.100). Esta configuración se modifica en el apartado de sistema en la sección de ajustes generales. En la figura 4.15 se observan los cambios ya realizados, además en el nombre de dominio se ha modificado por “eléctrica.eie”, este nombre puede variar. Únicamente es necesario respetar que no se debe terminar un dominio en “. local”.

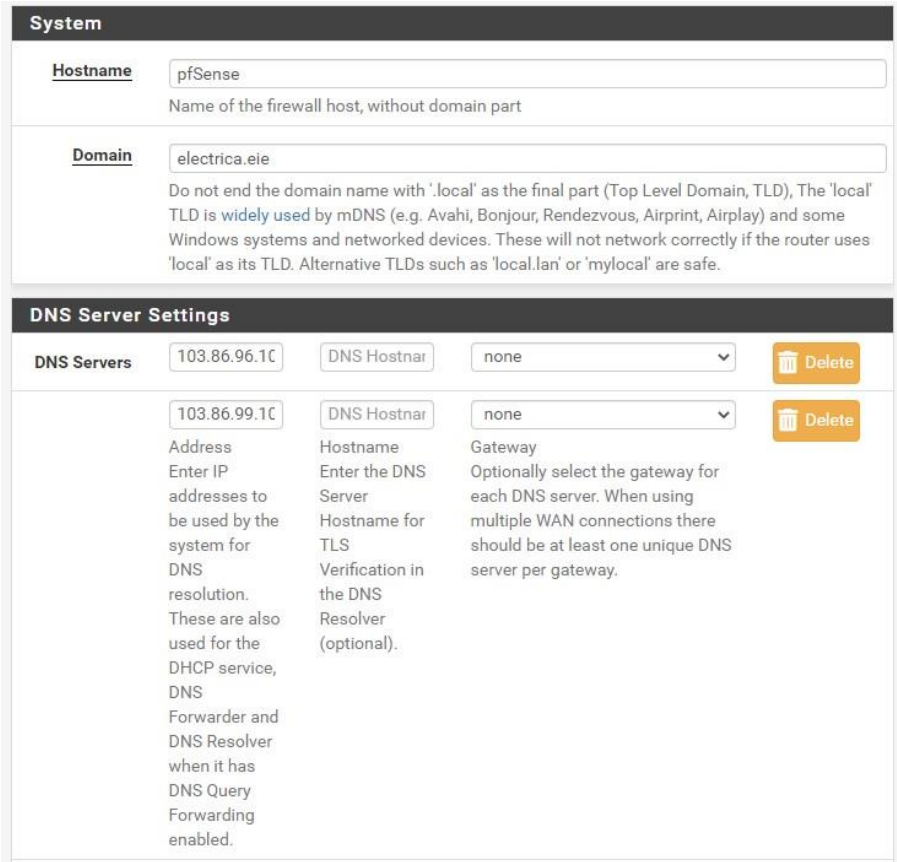

Figura 4. 15 Configuración de servidores DNS de NordVPN

Al terminar esta última configuración, se tiene configurado un sistema completo en el cual se encripta el tráfico mediante VPN lo que protege la información del usuario. Todo esto configurado haciendo uso del software Pfsense. Tal como se ha especificado inicialmente existen diferentes herramientas mediante las cuales se puede monitorear el funcionamiento de todos los elementos de la VPN.

En el caso del cliente, en el caso del cliente de la VPN se tiene su estado el cual brinda la dirección local, la dirección virtual y la dirección que brinda el host mediante la cual se sale a internet. Tal como se observa en la Figura 4.16 el servidor esta activo (up) y ha dado una dirección de host remota de 37.120.157.19 utilizando el puerto 443.

Client Instance Statistics

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
NordVPN TCP4	up	Fri Jan 20 3:54:47 2023	[redacted]	10.7.3.6	37.120.157.19:443	46.89 MiB	606.49 MiB	

Figura 4. 16 Estado de cliente de proveedor VPN

4.6 RESULTADOS DE IMPLEMENTACION

Teniendo el cliente de la VPN activo, se debe revisar el estado de las compuertas de salida (gateways) para comprobar que no exista perdida de datos, al observar la figura 4.17 se tiene que tanto la gateway WAN y NORDVPN están activas y no presentan perdidas.

Status / Gateways

Gateways | Gateway Groups

Gateways

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
WAN_DHCP **(default)**	[redacted]	[redacted]	0.598ms	1.617ms	0.0%	Online	Interface WAN_DHCP Gateway
NORDVPN_VPNV4	10.7.0.1	10.7.0.1	69.53ms	27.622ms	0.0%	Online	Interface NORDVPN_VPNV4 Gateway

Figura 4. 17Estado de gateways

Por lo que al estar el cliente activo y conectado al servidor del proveedor de VPN además las gateways se encuentran activas y sin reportes de pérdidas de información, se tiene un sistema mediante el cual el tráfico de información viaja de manera encapsulada a través de los túneles encriptados por medio del servidor de la VPN y además se tiene un franqueo de firewall lo que brinda una red privada segura. En la figura 4.18 se puede observar que la ip con la que se sale a internet es 185.197.192.21 la cual tiene una localización en Miami, FL Estados Unidos. Ocultando por completo la identidad de la ip local.

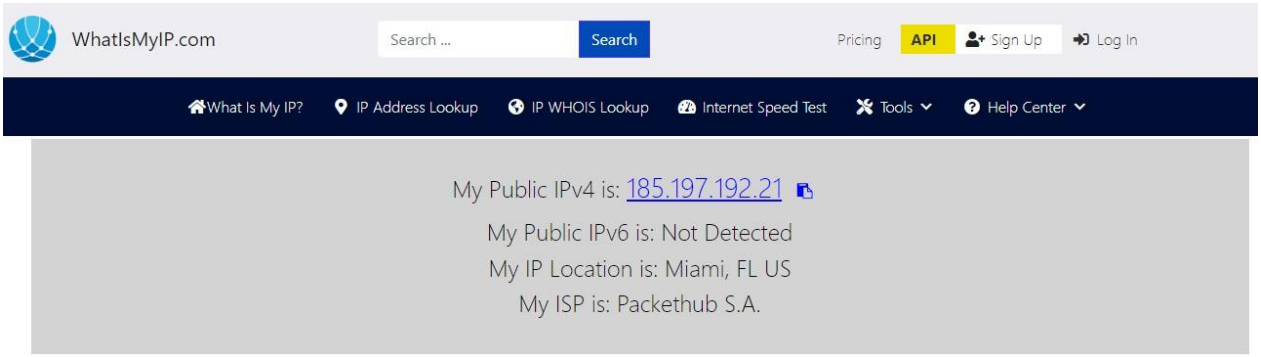

Figura 4. 18 Prueba de dirección IP a través de VPN

CONCLUSIONES

La mayoría de los proveedores VPN son empresas con una estructura de servidores definida y administrada con políticas de acceso bastante limitadas, una política común es que el puerto que brindan para acceder a su red está definido y es compartido por todos sus usuarios, entonces, cuando se diseña una instalación de un router con una VPN integrada, deben tomarse en cuenta estas políticas para evitar puntos de comunicación interrumpida.

La solución implementada ofrece escalabilidad y flexibilidad para adaptarse a las necesidades cambiantes de la universidad. pfSense y el hardware compatible permiten expandir la infraestructura de seguridad de acuerdo con el crecimiento de la red y la demanda de recursos, proporcionando una base sólida para futuras mejoras y expansiones.

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 beneficio más grande 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 junten 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, se debe estar pendiente de la documentación en cada actualización por parte de ambas comunidades.

La implementación de un Firewall ha permitido controlar y monitorear el tráfico de red, bloqueando los accesos no autorizados y evitando posibles amenazas externas. Esto ha fortalecido la seguridad de la red privada de la universidad, protegiéndola contra ataques cibernéticos y mitigando los riesgos de filtración de datos.

BIBLIOGRAFIAS

- Amazon Web Services. (s.f.). ¿Qué es una VPN? Amazon Web Services. Recuperado el 20 de septiembre de 2022, de https://aws.amazon.com/es/what-is/vpn/

● Cisco. (s.f.). ¿Qué es la ciberseguridad? Cisco. Recuperado el 14 de noviembre de 2022, de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

● Cisco. (s.f.). Cortafuegos. Cisco Secure Firewall. Recuperado el 17 de noviembre de 2022, de https://www.cloud.cisco.com/site/mx/es/products/security/firewalls/index.html

● ExpressVPN. (s.f.). ¿Qué es la encriptación de VPN (y cómo funciona)? ExpressVPN. Recuperado el 20 de noviembre de 2022, de https://www.expressvpn.com/es/what-is-vpn/vpn-encryption

● IBM. (s.f.). Ataques cibernéticos. IBM. Recuperado el 21 de nocirmbre de 2022, de https://www.ibm.com/cl-es/topics/cyber-attack

● Jones, J. P. (2023, 19 enero). UDP vs TCP: ¿cuál es la mejor opción para VPN? Top10VPN. Recuperado el 8 de noviembre de 2022, de https://www.top10vpn.com/es/guias/udp-vs-tcp/

● Latto, N. (2021, 05 de agosto). ¿Qué es WannaCry? Avast. Recuperado el 22 de nocimebre, de 2022, de https://www.avast.com/es-es/c-wannacry

● Migliano, S. (2023, 11 de enero). Las 10 mejores VPN del 2023. Top10VPN. Recuperado el 25 de noviembre de 2022, de https://www.top10vpn.com/es/mejor-vpn/

● Netgate. (s.f.). pfSense. Netgate. Recuperado el 22 de noviembre de 2022, de https://docs.netgate.com/pfsense/en/latest/

● NordVPN. Encriptación de próxima generación: ¿qué es y cómo funciona? NordVPN. Recuperado el 28 de noviembre de 2022, de https://nordvpn.com/es/features/next-

generation-encryption/

https://www.ibm.com/cl-es/topics/cyber-attack

ANEXOS

	ExpressVPN	NordVPN	PIA VPN	Surfshark	IPVanish	CyberGhost
Clasificación						
Mejor para	Streaming y Juegos Online	Velocidad	Privacidad	Valor	Fire TV Stick	Prueba gratis
Calificación de velocidad	9.2	9.5	9.3	8.6	9.1	8.8
Torrent	Ilimitado	Restringido	Ilimitado	Ilimitado	Ilimitado	Restringido
Paises	94	59	84	65	51	90
Servidor	3000	5.613	17 193	3200	2000	9.769
Política de registro	Datos de servidor anónimos	Sin registros	Sin registros	Datos de servidor anónimos	Sin registros	Datos de servido anónimos
Pago mensual	12,95 $	11,95 $	11,95 $	12,95 $	10,99 $	12,99 $
Prueba gratis	7 días (solo móvil)	7 días (solo Android)	X	7 días (solo móvil)	X	1, 3 y 7 días

Anexo 1: Tabla comparativa de proveedores VPN