UACM

Universidad Autónoma de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Implementación de seguridad perimetral con un firewall virtualizado de código abierto para micro, pequeñas y medianas empresas

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADOS EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A N

ESMERALDA ELIZABETH CHAVEZ CRUZ

BRIAN SALDAÑA GUTIÉRREZ

D I R E C T O R

MTRO. JOEL YAZBEK BUENDÍA GÓMEZ

Ciudad de México, mayo de 2025.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Honorable Jurado

- Dr. Luis Angel Alarcón Ramos
- Dr. Marco Antonio González Silva
- Dr. Josiane Jaime Rodríguez Suárez

Nada humano me es ajeno

Quiero comenzar expresando mi más profundo agradecimiento a mi querida Universidad Autónoma de la Ciudad de México. Gracias por brindarme la oportunidad de hacer realidad esta meta por concluir mis estudios. Agradezco haber formado parte de esta institución y haber vivido este camino lleno de aprendizajes, desafíos y logros, donde cada meta alcanzada fue posible gracias al acompañamiento y las herramientas que me brindaron.

Gracias por permitirme vivir experiencias que marcaron mi vida y por los lazos que construí con amigos y compañeros que estuvieron a mi lado durante esta travesía. En especial, quiero agradecer a Brian Saldaña, cuya dedicación y responsabilidad fueron una inspiración constante para mí. Tu apoyo desde el momento en que te conocí, fue clave en mi vida; fuiste un pilar fundamental, y por ello, siempre estaré agradecida.

A mis padres, les estaré eternamente agradecida. Gracias por velar siempre por mi bienestar y brindarme un apoyo incondicional, motivados únicamente por su deseo de verme feliz y realizada. Me enseñaron valores esenciales: a ser responsable, a esforzarme, a querer superarme y, sobre todo, a amar. Todo lo que soy se lo debo, en gran medida, a ustedes. Gracias por tanto.

También quiero extender un sincero reconocimiento y agradecimiento a mi director de tesis, Mtro. Yazbek Joel Buendía. Gracias por su invaluable apoyo, por abrirnos las puertas del laboratorio, por su paciencia, por guiarnos con generosidad y compartirnos sus conocimientos. Gracias por regalarnos parte de su tiempo para acompañarnos en esta meta que iniciamos hace algun tiempo. Es un profesor ejemplar, y siempre llevaré conmigo lo aprendido de usted.

Finalmente, agradezco profundamente a mis lectores: Dr. Luis Ángel Alarcón Ramos, Dr. Marco Antonio González Silva y Dr. Josiane Jaime Rodríguez Suárez. Gracias por aceptar ser parte de este proyecto que Brian y yo emprendimos con ilusión y compromiso. Agradezco su tiempo, sus recomendaciones y su disposición para compartirnos sus conocimientos. Su colaboración fue fundamental para la culminación de este trabajo.

Elizabeth Chavez

Resumen

Este trabajo propone la migración de un sistema de seguridad perimetral mediante la virtualización de un firewall en el laboratorio de redes de telecomunicaciones del plantel San Lorenzo Tezonco, perteneciente a la Universidad Autónoma de la Ciudad de México. El objetivo es mejorar la seguridad perimetral de la red, agregando reglas que ayuden a controlar el tráfico de datos hacia y desde la red interna. Esta propuesta es adaptable a micro, pequeñas y medianas empresas, aunque se debe considerar que la arquitectura y los recursos de cada red pueden variar, por lo que su implementación puede requerir ajustes específicos. Además, como parte de esta propuesta, se incluyeron cámaras de videovigilancia para reforzar la seguridad física de la red, junto con servicios adicionales como telefonía IP, una zona desmilitarizada (DMZ) y WiFi, que son de utilidad para las actividades del laboratorio. También se crearon VLANs para mejorar la administracioń de la red y facilitar la creación de reglas en el firewall.

El primer paso fue la instalación del software de virtualización Proxmox en el servidor, permitiendo la creacioń de las máquinas virtuales necesarias. Tras completar la instalación y configuración de Proxmox, se procedió a la creación de las máquinas virtuales. En la primera de ellas, se instaló Pfsense, que actuaría como firewall. Luego de su instalación, se configuraron las interfaces correspondientes a WAN, LAN, DMZ, WLAN y ASTERISK, con reglas específicas para controlar el flujo de tráfico, permitiendo, denegando o redirigiendo el tráfico según las necesidades. Una vez finalizadas las configuraciones, se crearon las máquinas virtuales para los servicios adicionales y las configuraciones necesarias para el correcto funcionamiento de la red.

Al concluir, Pfsense demostró ser efectivo en la gestión de la seguridad perimetral, configurando diferentes interfaces con reglas específicas para controlar el tráfico de red, lo cual fue validado mediante pruebas de trafico, como pings entre interfaces. Proxmox facilitó el monitoreo y la administración de recursos, proporcionando información detallada sobre el uso de CPU, memoria y tráfico. Además, se implementaron servicios adicionales como un servidor web con Apache y Joomla, así como un sistema de llamadas VoIP con Asterisk, que funcionaron correctamente en las pruebas. Finalmente, la red se organizó utilizando VLANs, lo que mejoró la seguridad y la gestión al restringir el acceso a los usuarios generales solo a Internet, mientras que los administradores tienen acceso completo.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1. Antecedentes

Información publicada por Kaspersky daily en 2020, menciona que los ciberataques van más dirigidos a empresas que a usuarios, en este ámbito, Brasil encabeza la lista con 55.25 %, seguido de México con 22.81 %, Colombia 10.20 %, Perú 4.22 %, Chile con 3.27 % y Argentina con 3.25 % [1]. Además, tras la pandemia causada por el Covid-19 varias empresas optaron por el trabajo a distancia, pero más del 50 % de los empleados que trabajan de forma remota, reportan una falta de medidas de ciberseguridad para realizar sus actividades [2]. Adicional a estas cifras en el 2020 ESET security reportó que el 59 % de las empresas en México presentó al menos un incidente de seguridad de la información [2]. Con base en estos datos, se puede concluir que las medidas de seguridad implementadas por las empresas parecen no ser las óptimas.

Una encuesta realizada en 2019 por el Instituto Federal de Telecomunicaciones reveló que el 88 % de las medianas, el 73 % de las pequeñas y el 60 % de las microempresas consideran que la ciberseguridad es muy importante. Sin embargo, la misma encuesta mostró que el 71 % de las micro, el 57 % de las pequeñas y el 43 % de las medianas empresas no cuentan con personal encargado para gestionar esa área [3].

Con base en los datos obtenidos de diversas fuentes, se plantea un enfoque de concientización sobre las vulnerabilidades que enfrentan las compañias, especialmente las micro, pequeñas y medianas empresas (MiPyMes) en México. Para ellas, se desarrolla una propuesta de seguridad perimetral, buscando la migración, actualización o implementación de un firewall hacia un ambiente virtual con el proposito de ahorrar en recursos de hadware y mejorando las reglas de tráfico desde y hacia la red de la MiPyMe.

1.2. Hipótesis

Con la implementacion de un firewall de código abierto y un dispositivo que permita la creación de entornos de virtualización basados en software libre, se podrá llevar a cabo la migración, actualización o implementación en las medidas de seguridad perimentral en el Laboratorio de Redes de Computadoras del plantel San Lorenzo Tezonco. Esta iniciativa también puede ser replicada por las MiPyMes de México, ayudándolas a adoptar soluciones de seguridad perimetral y, de esta forma, reducir la brecha de seguridad que enfrenta el país.

1.3. Planteamiento del problema

Las medidas de seguridad de entre el 70 % y 80 % de las medianas empresas se basa en la instalación de antivirus, programas autorizados solo por el administrador, cambio frecuente de contraseñas, restringir el acceso a páginas web y acceso a información a usuarios específicos, esto según datos obtenidos por el IFT en el 2019 [3]. Además, en el 62 % de las empresas, el responsable de la seguridad es el encargado de sistemas y en un 35 % el encargado de soporte técnico. Pero el problema en muchas de estas empresas radica en evitar los costos que conlleva invertir en seguridad, y creer que por el tamaño de la empresa es poco probable que puedan ser víctimas de algún ataque [3].

Como ejemplo, se tiene el Laboratorio de Redes de Computadoras del plantel San Lorenzo Tezonco, ubicado en la alcaldía Iztapalapa, este laboratorio brinda servicio a los estudiantes y profesores de la carrera de Ingeniería en sistemas electrónicos y telecomunicaciones (ISET), de la Universidad Autónoma de la Ciudad de México (UACM), como tal no se trata de una MiPyMe, pero esta red cumple con las características en tamaño y servicio de una. Actualmente hay un Firewall de código abierto implementado dentro de un CPU con pocos recursos y que no se encuentra en uso. En los últimos años, este laboratorio no ha sufrido modificaciones en las reglas implementadas dentro del Firewall y no han sido monitoreadas o actualizadas para que puedan estar en óptimas condiciones, esto causa una brecha de seguridad para esta instalación, la cual resguarda información de alumnos y profesores de la carrera.

1.4. Justificación

Con base a la investigación previamente realizada, las MiPyMes de México están dentro de los primeros lugares de latinoamérica en sufrir ciberataques, muchas empresas no son conscientes de lo grave que es esta situación, por lo que no se preocupan por implementar medidas de seguridad para no verse muy afectados. Ante estas amenazas, diversas son las causas que provocan esta situación, pero uno de los más importantes son los costos que puede implicar una implementación.

De esta manera, se vuelve importante buscar herramientas y métodos de seguridad que permitan disminuir esta brecha en las MiPyMes Mexicanas, el crecimiento de las redes y el acercamiento a internet, provocan un riesgo latente que debe ser reducido. Además, ser víctima de ataques conlleva una infinidad de problemas, desde pérdidas monetarias, pérdidas de clientes, no brindar un buen servicio, dar una mala imagen de la empresa y que incluso podría derivar en el cierre de la misma.

1.5. Beneficios esperados

Con el uso de métodos y herramientas de seguridad perimetral e instalación de todo el software de código abierto en un solo servidor, se busca reducir en recursos de hardware, debido a que esta implementación no involucra equipo adicional, más allá del servidor. Se añade un software de virtualización que nos permita interconectar todos los servicios requeridos. Además, de agregar recursos que cumplan con las necesidades de cualquier MiPyMe, porque puede que ya tengan alguna implementación de seguridad, deseando tener un esquema de solución para cada situación.

1.6. Delimitar el problema

Este proyecto propone una solución de seguridad perimetral para MiPyMes, utilizando un firewall de software libre para gestionar el tráfico de datos de la red privada, tanto hacia como desde internet. Con el objetivo de optimizar recursos de hardware, el firewall se instalará en una máquina virtual alojada en Proxmox. Además, se implementarán VLANs a través de un switch, lo que permitirá segmentar la red y evitar que cualquier equipo tenga acceso a computadoras con información sensible.

Asimismo, se creará un servidor web en la zona desmilitarizada (DMZ) de manera virtual. En otra máquina virtual se instalará el software Asterisk que va a permitir hacer y recibir llamadas a través de internet. También se configurará un servidor adicional, igualmente virtualizado en Proxmox, encargado de gestionar las cámaras de seguridad. Por último, pensando en el crecimiento en el uso de equipos inalámbricos se agregará el servicio de WiFi a esta propuesta..

Todo esto se llevará a cabo en el Laboratorio de Redes de Computadoras de la UACM San Lorenzo Tezonco. Una vez simulada la red de la empresa, y probando el funcionamiento del sistema de seguridad, podrá ser implementada en alguna micro, pequeña o mediana empresa.

1.7. Objetivos

Objetivo general: Implementar, actualizar o migrar un sitema de seguridad perimetral con un Firewall de código abierto para la red interna de MiPyMes, utilizando entornos de virtualización.

1.7.1. Objetivos específicos

1. Investigar sobre problemas de seguridad informática en empresas y MiPyMes a nivel mundial, continental y en México; también investigar posibles soluciones a la brecha de seguridad en empresas y MiPyMes mexicanas.

2. Desarrollar un diagrama de red, con los servicios que se agregarán a la propuesta de la red para una MiPyMe.

3. Investigar y buscar Firewall de código abierto para probar y poder seleccionar uno que cumpla con las condiciones predefinidas para su implementación en una MiPyMe.

4. Instalar y configurar el entorno de virtualización Proxmox.

5. Crear, instalar y configurar el servidor web, utilizando Joomla como sistema de gestión de contenidos (CMS), el cual formará parte de la DMZ.

6. Crear, instalar y configurar un servidor para una central telefónica, utilizando el software Asterisk para agregar servicios de VoIP.

7. Programar las cámaras a implementar; crear, instalar y configurar un servidor para ZoneMinder, que es un software que permite gestionar cámaras.

8. Configurar un equipo AP, para agregar servicio de WiFi, y que en éste puedan conectarse cámaras de forma inalámbrica, y usuarios.

Capítulo 2

Fundamentos teóricos

2.1. Antecedentes

2.1.1. Modelos de comunicaciones

En primer lugar, es importante saber qué es un modelo de comunicaciones, ya que, es a partir de la necesidad de evolucionar la forma en cómo se comunica el ser humano, que empieza a surgir la invención de nuevas tecnologías para comunicarse. Además, de este modo se puede tener conocimiento sobre las partes que intervienen y que se buscan proteger cuando se produce un mensaje. Entonces, cuando se habla de alguna teoría de la comunicación, la de Claude Shannon es la más aceptada. El Prof. Galeano, interpreta que Shannon, la define como un "proceso de transferencia de información", que se puede dar de forma lineal y unidireccional. Esta teoría aplica a cualquier mensaje y se representa en cinco partes como se muestra en la figura 2.1: fuente, transmisor, canal, receptor, donde además se le añade una fuente de ruido, esto porque siempre habrá alguna perturbación a la hora de enviar cualquier información, por el medio que sea [4].

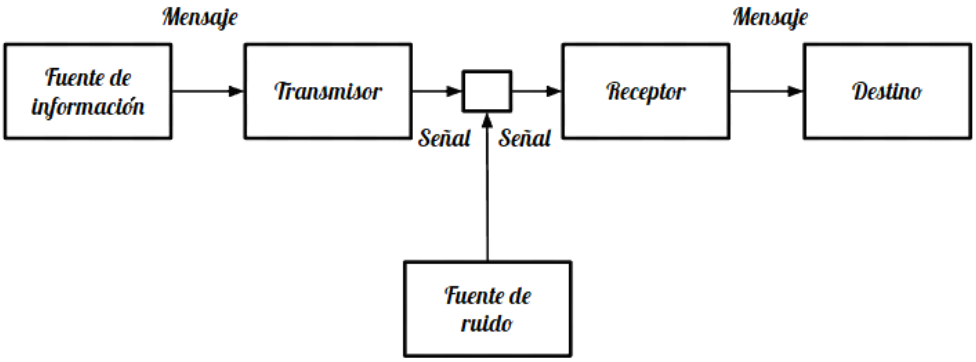

Figura 2.1: Modelo de comunicación

2.1.2. Redes de computadoras

La necesidad del ser humano por mejorar la manera en que se comunica, dio paso al desarrollo de nuevas tecnologías, como el teléfono, la radio, la televisión, etc. Esta evolución en el modo de comunicación, forma parte clave del nacimiento de las redes de computadoras, como se muestra en la figura 2.2, son un conjunto de equipos que nos permite intercambiar información a través de un medio de transmisión, ya sea un medio guiado (fibra óptica, coaxial, par trenzado, etc.) o no guiado, que de una u otra forma se encuentran conectados entre si. (microondas, infrarrojos, satélites, etc.) [5].

En la actualidad, el uso de estas redes se ha convertido en una actividad diaria en la vida de millones de personas, para su uso personal o empresarial, esto es porque se permite guardar, recibir y difundir cantidades exorbitantes de información, además de brindar servicios que pueden llegar a ser de suma importancia, como lo son cuentas bancarias o informació personal. Por esta razón empieza a volverse una prioridad poder resguardar y mantener seguras estas redes de cualquier peligro latente.

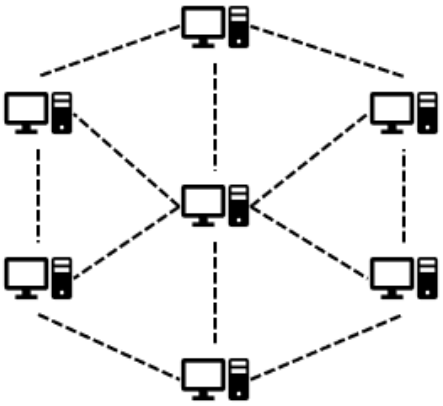

Figura 2.2: Red de computadoras

Tipos de redes de computadoras

Para poder brindar un esquema de solución adecuado a cada red, es importante tener en cuenta ciertos aspectos, como su tamaño, estructura física, y la manera en que se comunican los equipos. De acuerdo con estas variantes se brindarán distintas soluciones [5].

Redes de computadoras según su tamaño.

Red de área personal (PAN): Este tipo de red es comúnmente pequeña y se utiliza principalmente para la comunicación entre dispositivos personales. Un ejemplo claro de este tipo de redes son todo tipo de computadoras que están conectadas a un monitor, teclado, mouse e impresora. La conexión se puede dar por medio de cables o de forma inalámbrica como se observa en la figura 2.3 [5].

Figura 2.3: PAN

Red de área local (LAN): Por lo general este tipo de redes son de propiedad privada, pueden operar dentro de un edificio, oficina, casa o fábrica. Todos los equipos que se encuentran dentro de la red, podrán compartir recursos e intercambiar información.

La comunicación dentro de una LAN también se puede dar de forma inalámbrica como se muestra en la figura 2.4, a este tipo de red se le denomina Wireless local area network o WLAN. Esta se rige por el estándar IEEE 802.11, también conocido como WiFi. En la mayoría de los casos, los equipos dentro de esta red se comunican con un dispositivo denominado AP (Access Point), el cual permite transmitir paquetes entre los equipos [5].

Figura 2.4: WLAN

Red de área metropolitana (MAN): Este tipo de redes cubren una ciudad, es decir, un área geográfica más extensa a comparación de una PAN y una LAN. Se iniciaron a partir de la instalación de antenas comunitarias, para las áreas con mala recepción de televisión inalámbrica. En la actualidad una MAN como la que se observa en la figura 2.5 puede proveer servicios de internet y televisión [5].

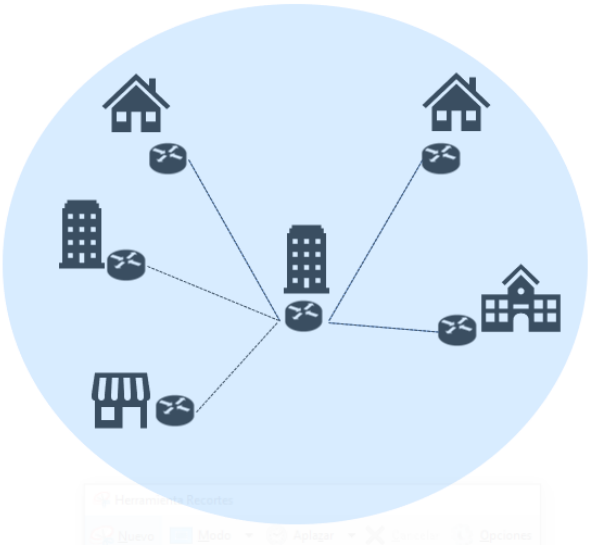

Figura 2.5: MAN

Red de área amplia (WAN): Esta red abarca un área muy grande, como un país o continente como se puede ver en la figura 2.6. Ayuda a interconectar redes, por ejemplo, conectar redes LAN de alguna organización mundial que no estén en una misma ubicación física, otro ejemplo claro es el Internet [5].

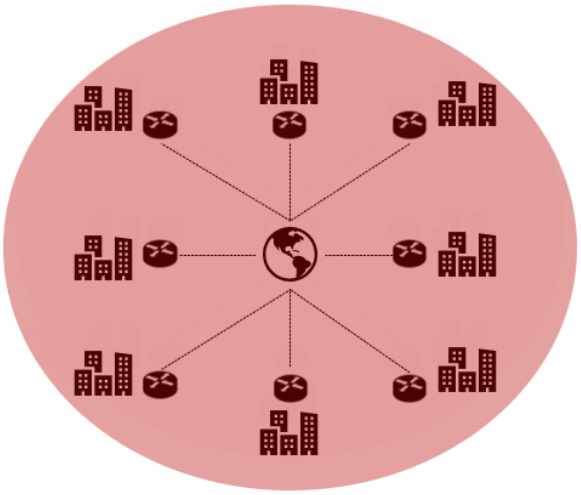

Figura 2.6: WAN

Redes de computadoras según su topología física (mapa físico).

Topología en bus: Es utilizada para redes pequeñas, todos los equipos se conectan a un solo segmento de red a través de un cable como se puede ver en la figura 2.7. Los equipos se pueden comunicar mediante un Transceiver, esto permite retirar un equipo sin que sea detenido el funcionamiento de la red [6].

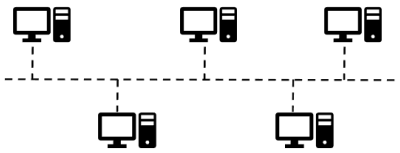

Figura 2.7: Topología en bus

Topología en anillo: Los dispositivos dentro de esta red se conectan de manera adyacente, formando un anillo como se puede observar en la figura 2.8, la información pasa de equipo en equipo hasta que llega a su destino. Si uno de estos es interrumpido por algún fallo, toda la red deja de funcionar. Este problema se puede solucionar, aplicando un cableado redundante, o con relés que permitan saltar el equipo que tiene el fallo [6].

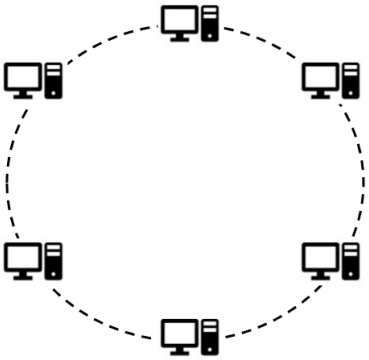

Figura 2.8: Topología en anillo

Topología en estrella: Esta es la estructura más antigua y clásica. Como se puede observar en la figura 2.9 en esta topología los equipos son conectados a un ordenador central, formado por conmutador, toda comunicación pasa siempre por él [6].

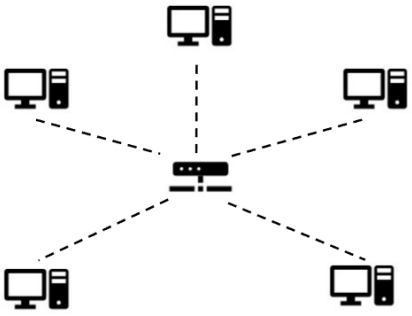

Figura 2.9: Topología en estrella

Topología en malla: Como se puede ver en la figura 2.10 todos los dispositivos están conectados entre sí, creando una conexión punto a punto entre todos los dispositivos que están dentro de la red. Se crean enlaces dedicados, donde el flujo de datos se da sólo entre los dispositivos que interconectan. Esta topología proporciona una mayor tolerancia a fallos y fiabilidad [6].

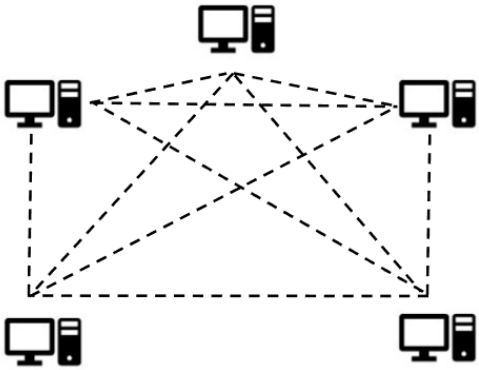

Figura 2.10: Topología en malla

Redes de computadoras según su tipo de enlace

Enlaces de difusión multipunto: En este tipo de difusión todos los dispositivos que están en la red comparten el canal de comunicación, se divide en:

Broadcast: La difusión del mensaje se da de forma masiva a través de la red, como se muestra en la figura 2.11. Para realizar la transmisión no es necesario conocer las direcciones de cada uno de los equipos [6].

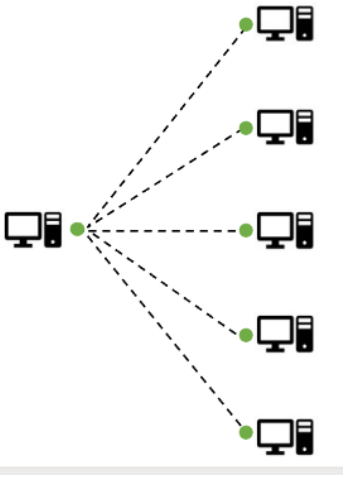

Figura 2.11: Broadcast

Multicast: El mensaje se envía a un conjunto de equipos. El envío del paquete con una dirección multicast se ve limitado a la subred, en la figura 2.12 los puntos verdes indican los equipos con los que habrá comunicación, mientras que los puntos rojos representan aquellos con los que no la habrá [6].

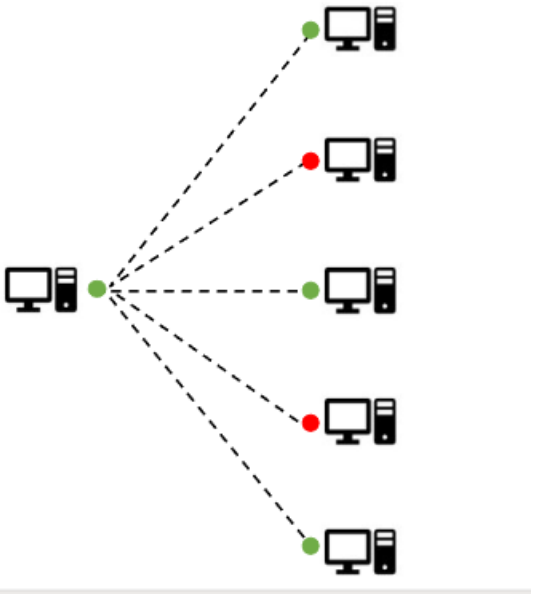

Figura 2.12: Multicast

Unicast: Esta comunicación se da entre dos máquinas como se muestra en la figura 2.13, yendo de un origen a un destino dentro de una red, es posible que el paquete pase por una o más máquinas intermedias [6].

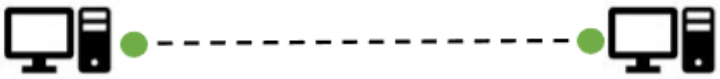

Figura 2.13: Unicast

2.1.3. Información.

No se puede dejar de lado este término, ya que, desde una perspectiva empresarial es un recurso necesario y de gran valor. Implica un proceso de interpretación, pues generalmente cualquier persona o empresa está constantemente recibiendo datos, pero solo aquellos que aporten algún conocimiento de importancia, serán denominados como información. Por esta razón, es importante que esta sea captada a tiempo y en la cantidad precisa [7].

2.1.4. Modelo OSI.

El modelo OSI divide la comunicación en siete capas, como se muestra en la figura 2.14. Este modelo surgió debido al crecimiento de las redes y a la necesidad de estandarizar las tecnologías de comunicación, permitiendo la interoperabilidad a nivel global, sin importar el país, fabricante o idioma. Un claro ejemplo de esta estandarización es Internet. El modelo establece una serie de protocolos que garantizan una comunicación eficiente y coherente. Además, proporciona una estructura clara para entender cómo se transmiten los datos y qué elementos deben ser protegidos en cada capa [8].

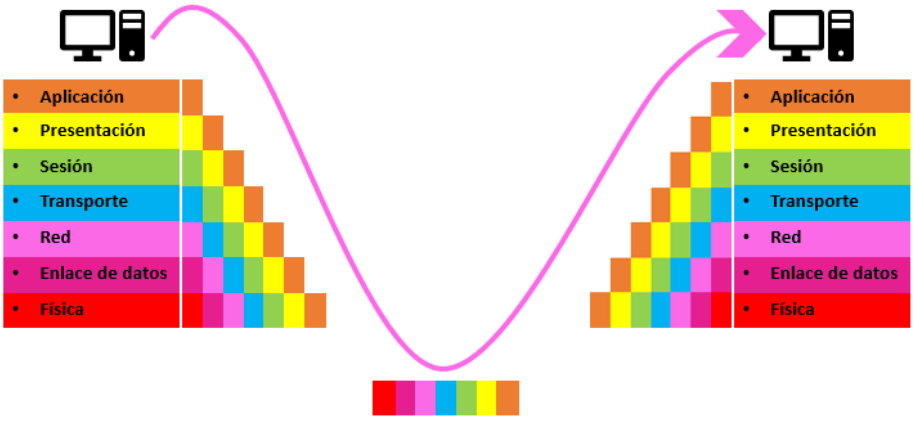

Figura 2.14: Modelo OSI

Capas del modelo OSI.

Física

La capa física se encarga de la transmisión de bits (0 y 1), a través de los circuitos de comunicación. El propósito general de esta capa es definir las reglas para garantizar que cuando una PC origen envíe un bit en 1, a una PC de destino, está reciba un 1 y no un 0 [8].

Enlace de datos

La capa de enlace de datos se encarga de enviar los mensajes al dispositivo adecuado en una LAN, para eso va a utilizar direcciones de hardware (MAC) y convertirá los mensajes de la capa de red en bits, para que la capa física los transmita, también incluye la detección de errores para asegurar la entrega segura de los datos [8].

La dirección MAC (Media Access Control) es un identificador único asignado a un dispositivo físico dentro de una red. Está compuesta por 6 bytes o 48 bits y se expresa en formato hexadecimal. Esta dirección es utilizada para identificar de manera exclusiva a un dispositivo dentro de la red local (LAN). Un ejemplo de una dirección MAC es el siguiente:

A0:D5:00:AC:11

Subcapa LLC(Control De Enlace Lógico): Se encarga de la comunicación entre las capas superiores y el software de red, toma los datos del protocolo de la red, y agrega información de control para ayudar a entregar el paquete al nodo de destino. Se Puede considerar como el controlador de la Tarjeta de interfaz de red (NIC) [8].

Subcapa MAC(Control de acceso al medio): Se encarga de direccionar el mensaje utilizando la dirección física MAC que permite que una trama se envíe al equipo de destino y de detectar los errores [8].

Red

La capa de red se va a encargar de gestionar el direccionamiento lógico y la entrega de paquetes de datos entre dispositivos en redes diferentes. Se encarga de decidir la ruta que los datos deben seguir para llegar a su destino, asegurando que los paquetes se transmitan de manera eficiente entre redes conectadas.

En la capa de red se utilizan dos tipos de paquetes:

- Paquetes de datos: Se utilizan para transportar datos de usuario a través de la red de internet, utilizando el protocolo IP.

- Paquetes de actualización de rutas: se utiliza para actualizar los routers vecinos sobre las redes conectadas. Los protocolos que envían paquetes de actualización de ruta, se denominan protocolos de enrutamiento. Los más comunes son: RIP, RIPv2, EIGRP y OSPF [8].

Transporte

Esta capa se va a encargar de la manera en cómo se va a realizar la transferencia de datos de un host a otro, se encargará de brindar una entrega segura o no, es decir, puede ser sin conexión u orientada a una conexión, dependiendo del protocolo en uso.

- UDP (User Data Protocol) sin conexión, este protocolo no garantiza la entrega de datos debido a que los paquetes o datagramas se pueden perder, duplicar o entregar erróneamente, tampoco recupera paquetes perdidos o corruptos; sin embargo, es rápido. La unidad de datos de protocolo en UDP son los datagramas.

- TCP (Transmission Control Protocol) antes de que un host de origen comience a enviar paquetes o segmentos, se establece una conexión previa. La unidad de datos de protocolo en TCP son los segmentos [8].

Sesión

Esta capa se va a encargar de administrar la comunicación, es decir va a permitir que se establezca o se cierre la comunicación con una aplicación. También se encarga de cómo será la comunicación entre los dispositivos ofreciendo tres maneras distintas: modo simplex, Half-Duplex y full-dúplex [8].

Presentación

Esta capa se asegura de que la información enviada a la capa de aplicación de un sistema sea legible por la capa de aplicación del otro sistema, para esto procesa la información realizando tres funciones principales:

1. Cifrado.
2. Codificación y conversión de datos o servicios (traducción).
3. Compresión [8].

Aplicación

Es la capa donde los programas de aplicación API (Application Programming Interfaces) interactúan directamente con el sistema operativo para proveer los servicios de red como la transferencia de archivos, emulación de terminal, mensajería, etc [8].

Sin embargo, existe un modelo reducido de 4 capas llamado TCP/IP, que es acorde a este proyecto, ya que no necesitamos indagar tanto en las capas de aplicación, presentación, sesión, y la capa fiísica. En la figura 2.15, se observa una comparativa de estos 2 modelos.

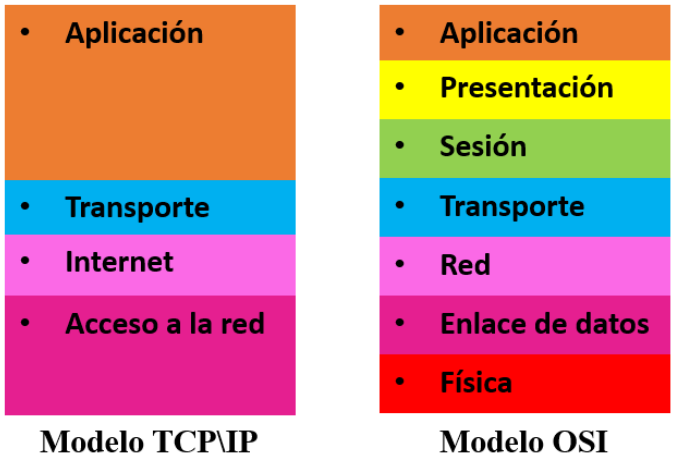

Figura 2.15: Modelo TCP/IP VS OSI

2.1.5. Network Address Translation (NAT)

Un router NAT permite que múltiples dispositivos en una red privada utilicen una única dirección IP pública para comunicarse con el exterior. Esto ayuda a conservar direcciones IP públicas ya que estas son limitadas, y también proporciona una capa de seguridad al ocultar las direcciones IP de la red privada [9].

Por ejemplo, en la figura 2.16 el equipo con IP privada 192.168.1.2 hace una petición hacia un servidor en internet con IP pública 128.119.20.189, cuando esta petición pasa por el router con NAT, la dirección IP de origen se traduce a la dirección pública del router NAT, en este caso es la IP 138.76.29.7. Esta es la dirección que se presenta al servidor en la WAN (Wide Area Network), ocultando la dirección IP privada.

Cuando el servidor con IP 128.119.20.189 responde a la petición enviada, la respuesta se envía a la dirección pública del router NAT . El router NAT recibe la respuesta y consulta su tabla de NAT, que mantiene un registro de las conexiones activas, para identificar a qué dispositivo interno debe reenviar el paquete. El router NAT traduce nuevamente la

dirección IP de destino, pasando de la IP pública a la IP privada del dispositivo que inició la comunicación [9].

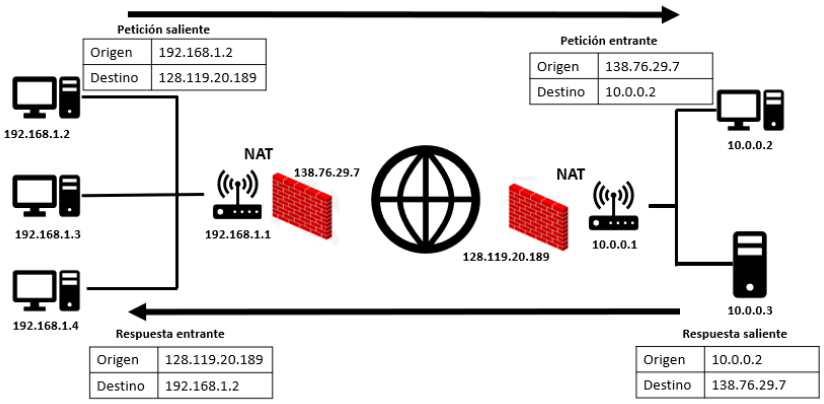

Figura 2.16: NAT

2.1.6. Domain Name System (DNS)

Cuando un dispositivo se conecta a una red, se le asigna una dirección IP. Si se está en una red con pocos ordenadores, es fácil tener memorizadas las direcciones IP de cada uno y así acceder a ellos, pero en el caso de internet existen millones de dispositivos y cada uno tiene una IP diferente, entonces, esto hace imposible conocer todas las direcciones que existen, para resolver este problema se utiliza DNS [5].

En la figura 2.17 se ilustra el proceso básico de una consulta DNS y la posterior conexión a un servidor web:

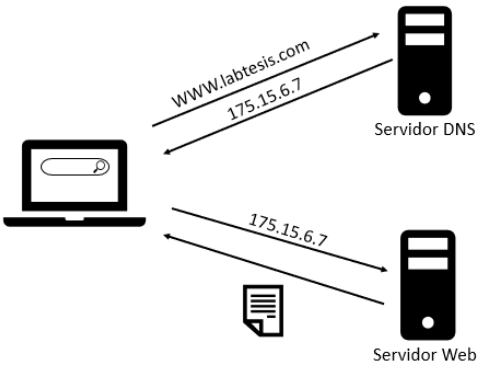

Figura 2.17: DNS

El usuario ingresa al dominio www.labtesis.com en su navegador, la solicitud se envía primero al servidor DNS, que se encarga de resolver el dominio en una dirección IP. En este

caso, el dominio www.labtesis.com se traduce a la dirección IP 175.15.6.7. Una vez que el navegador del usuario recibe la dirección IP, este se conecta al servidor web correspondiente a la IP 175.15.6.7. Por último, el servidor web responde enviando el contenido del sitio solicitado al usuario.

2.2. Marco teórico

2.2.1. Seguridad

Este término evoca miles de definiciones, debido a la gran cantidad de ramas que abarca, tomando la definición dada por Romero y otros, en su libro publicado en 2018 se dice que es, "una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien" [10], además, mencionan que la seguridad busca la manera de evitar o prevenir cualquier riesgo. En conclusión, se puede decir que la seguridad es la ausencia de riesgos, por esta razón mencionan que este término involucra cuatro acciones:

1. Prevención del riesgo.
2. Transferir el riesgo.
3. Mitigar el riesgo.
4. Aceptar el riesgo.

Clasificación de la seguridad

Dada la gran cantidad de áreas que abarca la seguridad, va a existir una lista muy extensa de clasificaciones para este término, causa de esto se pondrán algunos de los ejemplos más conocidos:

- Seguridad ciudadana.
- Seguridad nacional.
- Seguridad informática.
- Seguridad social.
- Bioseguridad.
- Seguridad laboral.
- Seguridad vial.
- Seguridad jurídica.

Seguridad informática

Urbina en su libro del 2016 menciona que, la seguridad informática, es una disciplina que conlleva políticas y normas, ya sean internas o externas, con el fin de proteger la integridad y privacidad de la información que se encuentre almacenada en un sistema informático, de esta forma busca minimizar cualquier riesgo físico o lógico a los que está expuesta [8].

Seguridad perimetral

La seguridad perimetral es una rama de estudio dentro de la seguridad informática, ya que, de acuerdo con Postigo, esta se va a encargar de las máquinas y dispositivos que se encuentran entre la red interna (sistema informático) y el lugar donde se interactúa con otras redes, controlando de esta manera la información que sale del interior y los posibles ataques que entren del exterior.

Existen distintos métodos que van a permitir asegurar el perímetro de un sistema informático, por ejemplo los Firewalls, las redes privadas virtuales (VPN), los sistemas de detección de intrusos (IDS), sistemas de gestión y control de acceso e identidad [11].

2.2.2. Código abierto

Es sustancial hablar sobre los software de código abierto, término que estará muy presente debido a que se hará uso de programas de este tipo. Estos están desarrollados y mantenidos mediante una colaboración abierta, además, permiten a los usuarios acceder a su código fuente para que cualquiera lo pueda usar, examinar y redistribuir como le convenga. Por lo anteriormente mencionado, este tipo de software tienen ciertas cualidades que, influyeron en la decisión de hacer uso de ellos, algunas de estas ventajas son:

1. Acceso al código fuente para cualquier programador.

2. Control para solucionar o corregir errores.

3. Se puede adaptar a las necesidades individuales, a otros productos y también acepta la interacción con otros sistemas y herramientas.

4. No tiene costo por adquisición.

5. Existen comunidades en línea, que brindan soluciones de mantenimiento y soporte, también existen empresas que ofrecen ayuda gratuita en línea.

6. Permite desarrollar nuevos productos sin empezar de cero.

7. Permite una alta interoperabilidad entre sistemas [12].

2.2.3. Firewall

En la actualidad, cada vez es mayor el uso de equipos de comunicación y sin duda la gran mayoría de personas o empresas que hacen uso de estas herramientas, buscan estar conectadas siempre a internet, sin embargo, el mantenerse conectados involucra aceptar el exponerse a riesgos que pueden estar presentes en esta red tan grande. Actualmente no existe una manera que pueda acabar con estos riesgos y amenazas, lo único que queda por hacer es disminuirlos con herramientas de seguridad, como por ejemplo, la implementación de un Firewall, que es la propuesta que se da en este trabajo para limitar daños que puedan causar ciertos ataques informáticos [8].

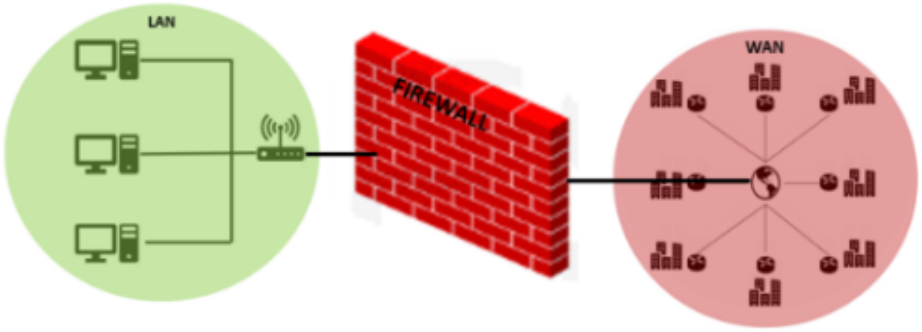

Figura 2.18: Firewall

Un Firewall va a estar ubicado en medio de dos redes como se muestra en la figura 2.18, el cual será útil para brindar protección a una red confiable de una que no lo es, en muchos de los casos la no confiable es internet. Este elemento puede ser en software o hardware, cuya principal función será la de proteger la red de accesos no autorizados, ayudará a monitorear el tráfico que entra y sale, creando advertencias de posibles ataques o irregularidades que pongan en riesgo la información valiosa. Cabe señalar que siempre existirá algún hueco, porque un Firewall no es inteligente, por lo que se verá limitado a la configuración del administrador [13].

En el mercado hay muchas opciones para cubrir necesidades tanto de presupuesto, sistema operativo, como de complejidad. En la tabla 2.1, se pueden ver algunos Firewalls

basados en software y la comparación con algunas funciones extras que pudiesen llegar a ser un diferenciador para saber cuál elegir, porque al final cualquiera que se elija debe de ser configurado para brindar seguridad.

Algunos podrían preferir algo para Windows donde ya venga todo integrado y su interfaz sea fácil e intuitiva, en la tabla, estos serían Comodo y ZoneAlarm, donde pudiesen incluir una versión de paga con más características. OPNSense, IPFire, Smoothwall, Pfsense, son opciones Open-Source, basadas en Linux, donde se tiene la opción de poder configurarlos con las características que mejor se acomoden, y no quedarse con las que vienen integradas, además, algo que no aparece en la tabla 1, son los pocos recursos que puede llegar a consumir un Firewall basado en Linux.

Estos últimos, al ser tan "versátiles", sus interfaces pueden no llegar a ser intuitivas y se pueden complicar, es ahí donde la comunidad juega un papel importante, porque si se tiene algún problema o duda al usarlo, por ejemplo, en el caso de Smoothwall, los problemas se tendrán que resolver por cuenta propia, porque la comunidad aún es pequeña [14], por otro lado, la comunidad de PfSense es demasiado grande, y puede que alguien ya haya encontrado solución al problema. Otros 2 Firewall para probar son Shorewall y UFW, donde el primero es ideal para Ubuntu, y según algunas páginas de internet no es muy complejo y es fácil de usar. El segundo está dirigido para GNU/Linux, donde destaca su soporte para múltiples ISP.

Firewall	IDS	VPN	Antivirus	Captura de paquetes	Acceso Remoto	IPv6
OPNSense	Sí	Sí	Sí	Sí	SSH, WEB	Sí
IPFire	Sí	Sí	Sí	Sí	SSH, WEB	Sí
Smoothwall	Sí	Sí	Sin información	Integrado	SSH, WEB	No
PfSense	Sí	Sí	Sí	Sí	SSH, WEB	Sí
ZoneAlarm	Sí	Sí	Sí	Integrado	Sin información	Sí
Comodo	Integrado	Sí	Integrado	Integrado	Sí	Sí

Tabla 2.1: Características de algunos Firewall de software

DMZ (Desmilitarized zone)

Con el Firewall se busca mantener la red segura, agregando reglas para que los datos de confianza estén dentro de la red y los inseguros fuera de ella. Aun así, no se puede cortar toda la comunicación con el mundo exterior, por esta razón, se pueden agregar ciertos arreglos, como incorporar una DMZ (demilitarized zone), colocando una máquina, la cual se va a ubicar fuera del perímetro de seguridad de la red, esta se va a encargar de ofrecer servicios de carácter público, así las computadoras que se encuentran en el exterior de la red corporativa se podrán comunicar con ella para navegar, ya sea por la página web de la empresa o por el servicio que se esté brindando, sin entrar en la red segura, de igual forma la red segura se podrá comunicar con la DMZ como se muestra en la figura 2.19. [5]

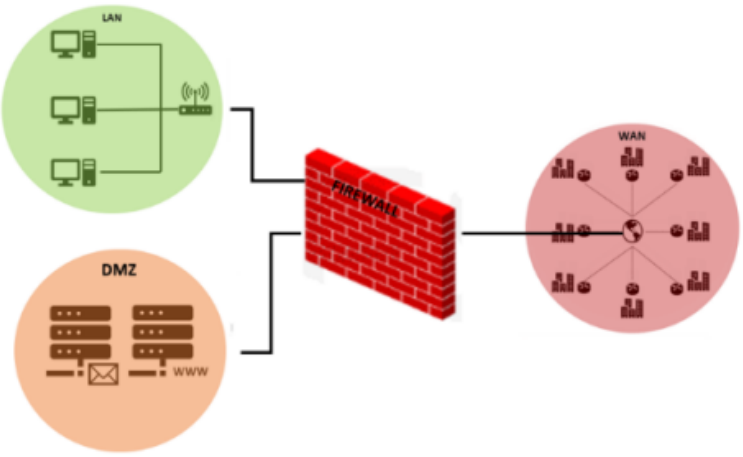

Figura 2.19: DMZ

2.2.4. Router

Los routers son una parte importante en este trabajo, este dispositivo de capa tres permite dirigir y enviar los datos de la red a través de diferentes tipos de paquetes de datos, eligiendo la ruta que deben seguir. También permite conectar los equipos a redes de área local e Internet, donde se desarrollan la mayoría de las actividades comerciales más importantes. Sin un router como el que se muestra en la figura 2.20, no se podría acceder a Internet, lo que lo hace tan importante para la creación de redes.

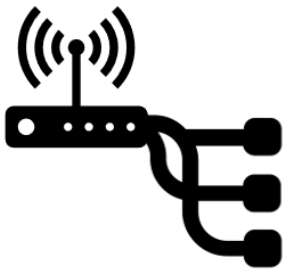

Figura 2.20: Router

Como parte complementaria, para la propuesta de implementación de este trabajo, se agregaron servicios que puedan cubrir ciertas necesidades que se puedan presentar dentro de una MiPyMe (Micro, Pequeña y Mediana empresa)

2.2.5. VoIP (Voice Over Internet Protocol)

Actualmente la telefonía IP ha tenido una presencia cada vez mayor en la sociedad, pero son las redes corporativas las que están optando por tener más provecho sobre esta, esto debido a que los servicios pueden extenderse sobre una misma red como se muestra en la figura 2.21, además cuando una empresa cuenta con varias sedes estas se pueden interconectar sin que se establezcan circuitos dedicados que tienden a ser muy caros. En conclusión, este servicio ayuda a reducir costos en llamadas y equipos, además, se puede agregar más servicios, se aprovecha mejor los recursos, y se reducen costos por mantenimiento, implementación y operaciones [15].

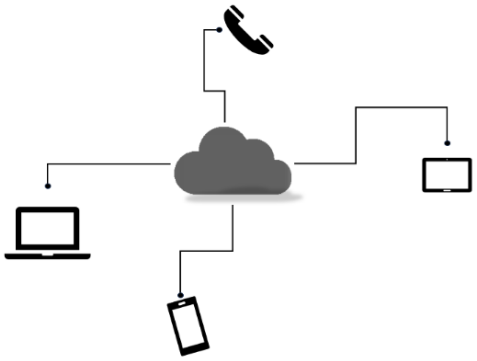

Figura 2.21: VoIP

2.2.6. Asterisk

Para la propuesta de implementación de VoIP, se hará uso de Asterisk que es un software libre que proporciona las funciones de una central telefónica. Las razones por las que se decide implementar este software son: permite la integración con la telefonía analógica, soporta cualquier protocolo estándar, puede personalizarse según las necesidades, es sencillo de usar, cuenta con los componentes necesarios para la escalabilidad y es un sistema de comunicación potente [16].

2.2.7. Proxmox

En la búsqueda de dar una mejor propuesta para este proyecto, se decide utilizar Proxmox para virtualizar ciertas partes o equipos de la red que se desean implementar. La decisión de utilizar este software se da a partir de los beneficios que ofrece, además de ofrecer una solución más completa y que pueda cubrir las necesidades que se puedan presentar en la red de cualquier Micro, Pequeña y Mediana empresa (MiPyMe). Para empezar, es necesario explicar qué es Proxmox y mencionar algunos de los beneficios que lo hacen una buena propuesta a implementar.

Proxmox es un sistema que permite virtualizar servidores o computadoras para poder instalar máquinas virtuales o contenedores, este se puede instalar en un equipo con pocos recursos, teniendo como requerimientos mínimos: CPU: 64 bits (Intel EMT o AMD6), RAM: 1 GB y Disco duro: 8 GB [17]. Tiene una estructura escalable, es decir, permite ir navegando cuántas computadoras o servidores se desee y dentro de ellas ir ejecutando diferentes tipos de máquinas. Tiene alta disponibilidad, permite hacer respaldos de forma automatizada e interconectar servidores [17].

Aunque Proxmox presenta ciertas limitaciones, como su capacidad de escalabilidad dependiente de la infraestructura, y en comparación con VMware, otro software de virtualización cuyas actualizaciones son más frecuentes y ofrece mayor capacidad de personalización, sigue siendo una excelente opción en términos de costo-beneficio para una MiPyME, ya que Proxmox es de código abierto y gratuito, mientras que VMware requiere una licencia de pago [18].

2.2.8. Switch

Los switches trabajan dentro de la capa de enlace de datos, se encargan del correcto envío de los paquetes, conocidos como tramas. Para realizar el envío de las tramas hacen uso de la tabla MAC, la cual proporciona los datos de la interfaz que le corresponde a cada dirección MAC de algún equipo físico.
En un principio, los equipos dentro de una red no tienen noción de cuál es la topología de la red. Cuando un equipo quiera enviar información a otro, la máquina de origen creará una trama, donde colocara en la cabecera la dirección MAC de origen y de destino, en el momento en que el switch recibe la trama logra captar la MAC del equipo de origen y a que interfaz del switch corresponde, posteriormente hace el envío de la trama hacia todas las interfaces, hasta localizar la MAC de destino, de esta manera se va llenando la tabla CAM [19].

2.2.9. Open vSwitch (OVS)

En último lugar como complemento para realizar el envió correcto de los paquetes dentro del entorno virtual se tiene Open vSwitch, este es un conmutador virtual de código abierto, donde su principio funcional es similar al de un switch físico. También admite la distribución a través de múltiples servidores físicos [20].

La instalación de Open vSwitch va a permitir conectar la parte virtual con la parte física para que la red esté interconectada, ya que estará conformada tanto por máquinas virtuales como físicas, este switch permitirá crear puentes que conecten los puertos físicos con los puertos virtuales y se realice la conmutación de los paquetes.

Capítulo 3

Desarrollo

3.1. Enfoque metodológico

En este trabajo se realizan pruebas a diversos firewalls de código abierto para compararlos entre sí y recabar los datos necesarios que faciliten su análisis frente a la documentación existente de los fabricantes y foros especializados. A través de estas pruebas, se obtienen los datos requeridos para evaluar, según criterios establecidos, qué software ofrece el mejor desempeño. Se busca que el firewall cumpla con características como fácil implementación, buen rendimiento, interfaz amigable, facilidad de uso, bajos requerimientos y amplia disponibilidad de información. Esto permite seleccionar el software más adecuado para satisfacer las necesidades de las MiPyMEs. Una vez elegido el firewall, se procede con su implementación, ofreciendo así una propuesta factible y rentable para estas empresas

3.2. Método de recolección de datos

Para obtener los datos necesarios y dar solución a la problemática planteada, se realiza un plan que ayude a lograr el objetivo de este trabajo, el cual consiste en una alternativa económica, de fácil uso y adaptable para MiPyMes. Se lleva a cabo la recolección de datos mediante encuestas, entrevistas, informes y reportes realizados por organizaciones expertas en el tema. Dicha propuesta se lleva a cabo en un entorno muy similar a una MiPyMe, en este caso se utiliza como referencia el Laboratorio de Redes de Computadoras del Plantel San Lorenzo Tezonco, de la Universidad Autónoma de la Ciudad de México.

Mediante el uso de un software de virtualización, se realiza la comparativa de los Firewall para tener en cuenta cual cumple con una fácil implementación, buen rendimiento, interfaz amigable, fácil uso, pocos requerimientos de instalación y basta información en foros, estos resultados se muestran en tablas comparativas.

3.3. Diagrama de la red

En las siguientes figuras se muestran los diagramas de la red implementada en el laboratorio de redes de telecomunicaciones del planten San Lorenzo Tezonco, en la figura 3.1 se observa el entorno físico, donde, hay un servidor en el cual se tiene instalado Proxmox; a las interfaces físicas del servidor se conectan los siguientes equipos:

1. Dispositivo Access Point de la marca Linksys de doble banda. A este se tienen conectadas via inalámbrica por la banda 2.4G dos cámaras ESP32-CAM.

2. Switch extreme que conecta con dos VLAN. Para la red local, donde se conectaran los equipos de los trabajadores de la MiPyMe y la red de administración, donde solo se podrán conectar personal autorizado.

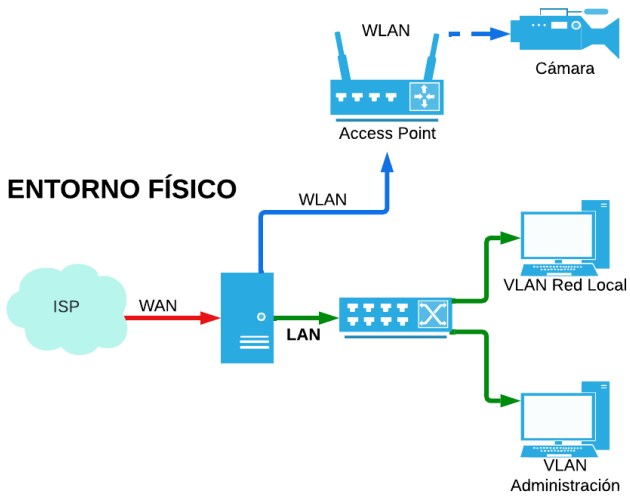

Figura 3.1: Entorno Físico

La figura 3.2 muestra el diagrama del entorno virtual de la red, donde se crearon 8 máquinas virtuales, a continuación se muestra un listado de las máquinas creadas y sus especificaciones:

1. Máquina virtual 100: tiene instalado Pfsense, al cual se le asigno una memoria RAM de 2 GB, un disco de 32 GB , un procesador con 2 sockets y 2 cores, y tiene agregados cinco puertos virtuales.

2. Máquina virtual 102: tiene instalado Ubuntu server 22.04, aqui se aloja el servidor web, cuenta con un memoria RAM de 4GB, un disco de 32 GB, un procesador con 2 sockets y 2 cores, y cuenta con un solo puerto de red virtual.

3. Máquina virtual 103: se tiene instalado Ubuntu server 22.04, aqui se tiene instalado Asterisk para dar el servicio de VoIP, cuenta con una memoria RAM de 2 GB, un disco duro de 32 GB, un procesador con un socket y un core, y tiene sólo un puerto de red virtual.

4. Máquina virtual 104: tiene instalado Ubuntu server 22.04, aqui se tiene instalado ZoneMinder para dar poder gestionar las cámaras de videovigilancia, cuenta con una memoria RAM de 2 GB, un disco duro de 64 GB, un procesador con dos sockets y dos cores, y tiene sólo un puerto de red virtual.

5. Máquina virtual 105: tiene instalado un sistema operativo Ubuntu desktop, aquí se tiene acceso a Pfsense para su administración, cuenta una memoria RAM de 4 GB, un disco de 32 GB, un procesador con 2 sockets y 2 cores y cuenta con un solo puerto de red virtual.

6. Máquina virtual 106: tiene instalado un sistema operativo Ubuntu desktop, aquí descargamos el software Zoiper que nos permite realizar llamadas, cuenta con una memoria RAM de 4 GB, un disco duro de 32 GB, un procesador con 2 socket y 2 core y cuenta con un sólo puerto virtual.

7. Máquina virtual 107: tiene instalado un sistema operativo Ubuntu desktop, al igual que en la máquina 106 tiene descargado el software Zoiper para realizar llamadas entre estos dos equipos, cuenta con una memoria RAM de 4 GB, un disco duro de 32 GB, un procesador con 2 socket y 2 core y cuenta con un solo puerto de red virtual.

8. Máquina virtual 108: tiene instalado un sistema operativo Ubuntu desktop, al igual que en la máquina 106 tiene instalado un sistema operativo Ubuntu desktop, aquí se tiene acceso a ZoneMinder para su administración, cuenta una memoria RAM de 4 GB, un disco de 32 GB, un procesador con 2 sockets y 2 cores y cuenta con un solo puerto virtual.

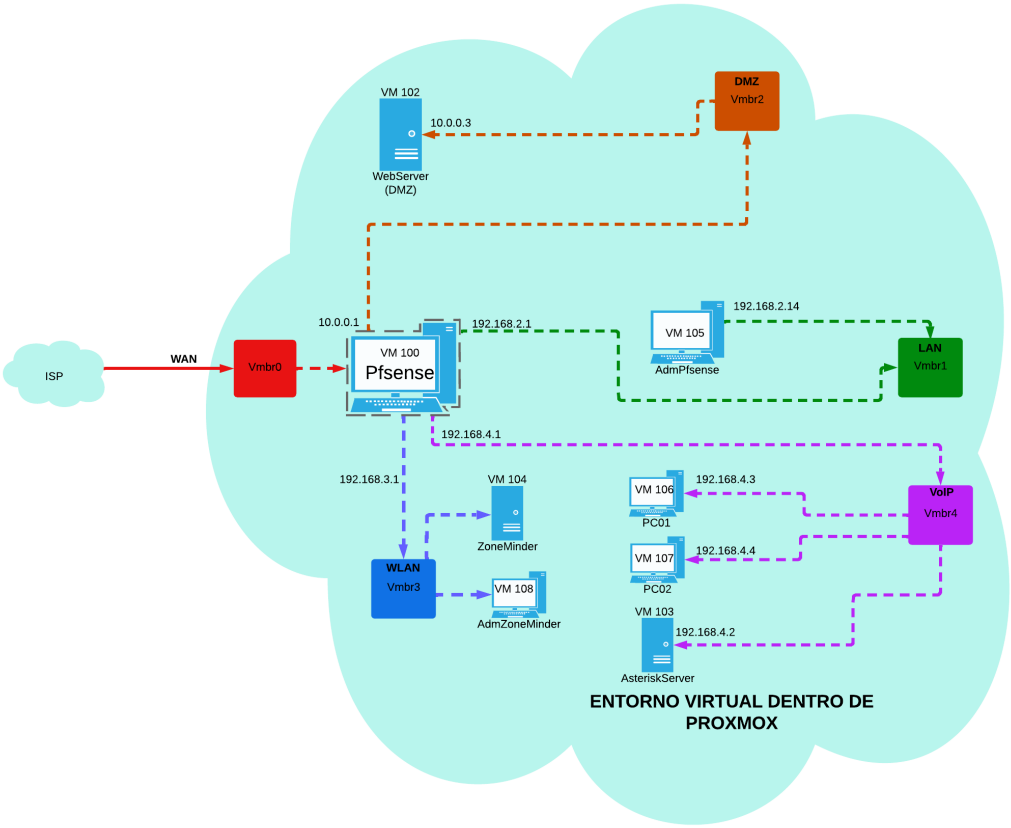

Figura 3.2: Entorno Virtual

En el siguiente subtema se muestra el proceso para la implementación de Proxmox, software de virtualización instalado en el servidor para unificar todo lo mostrado en la figura 3.2 y formar el entorno virtual.

3.4. Proxmox

3.4.1. Instalación

Como parte de la búsqueda de una mejor solución para realizar la implementación del Firewall, se propone agregar Proxmox. Este virtualizador permite reducir la necesidad de implementar más equipos físicos y facilita la optimización de recursos, contribuyendo a un uso más eficiente de la infraestructura existentes.

Para la instalación de Proxmox se utiliza un servidor físico, de la marca supermicro el cual cuenta con una memoria RAM de 16 GB y un disco duro de 500 GB. Se descarga la imagen ISO desde la página oficial de Proxmox para realizar la instalación, en este caso

se guarda dentro de una memoria, la cual se conecta por un puerto USB al equipo, para posteriormente proceder a arrancar el servidor.

Cuando se enciende se muestra una primera pantalla para dar inicio a la instalación, y una más para los acuerdos de licencia. Se llena la información sobre: el País, la zona horaria y el idioma del teclado. A continuación, se elige la contraseña para el usuario root para identificarse y se llenan los siguientes campos: FQDN, Dirección IP, Máscara y Servidor DNS.

Una vez terminado, sólo queda reiniciar el servidor. Al reiniciar la máquina se tiene que identificar con el usuario root y la contraseña que se le dió en la instalación. También muestra la dirección del servidor web con el que se puede conectar desde un navegador para poder hacer las configuraciones desde una interfaz web más amigable.

Debido a que el equipo no estaba conectado a la red, se le asignó una dirección IP fuera del rango de direcciones, lo cual provocó que no se tuviéra acceso a la interfaz web de Proxmox. Para solucionar esto, se tuvo que cambiar la dirección IP del servidor, lo cual se realizó entrando al archivo de interfaces usando el siguiente comando:

```
-nano /etc/network/interfaces
```

Dentro del archivo, se modificó la dirección IP, colocando una que estuviera dentro del rango, está quedo como se muestra en la figura 3.3

```
iface vmbr0 inet static
        address 192.168.1.65/24
        gateway 192.168.1.254
        bridge-ports eno1
        bridge-stp off
        bridge-fd 0
```

Figura 3.3: Cambio de dirección IP de Proxmox

Posteriormente, se reinicia el servidor con el siguiente comando:

```
- reboot
```

Una vez realizados estos pasos se logra acceder a la interfaz web de Proxmox, como se muestra en la figura 3.4.

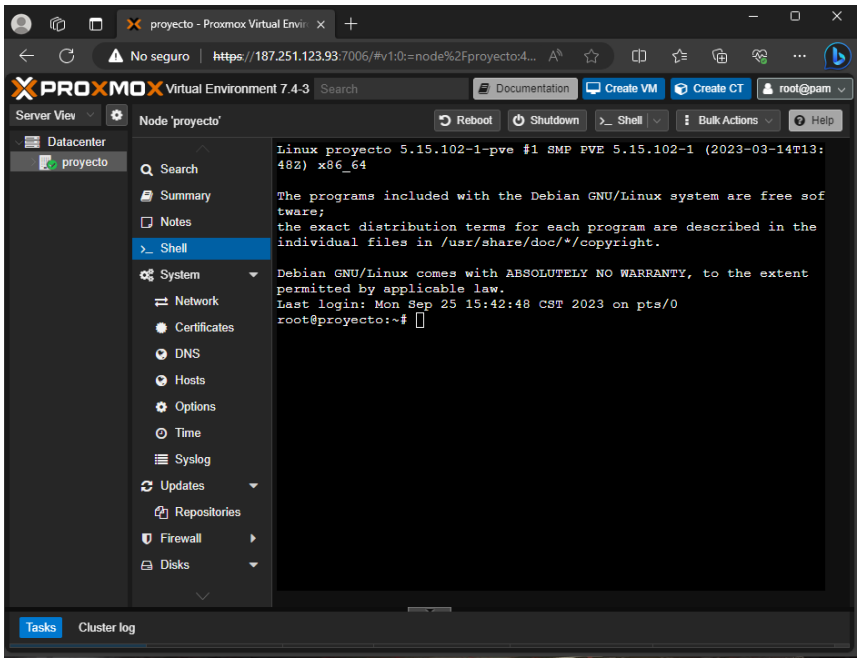

Figura 3.4: Interfaz web de Proxmox

Al ser un entorno virtual es necesario tener interfaces virtuales, esto ayuda a que las máquinas creadas dentro de Proxmox se puedan conectar con otras máquinas, ya sean dentro del mismo entorno virtual o con equipos físicos que estén conectados directamente al servidor. Por defecto Proxmox no permite crear dichas interfaces, por lo tanto, es necesaria la instalación de Open vSwitch, este proceso es descrito a continuación

3.4.2. Configuraciones

Instalación de OpenvSwitch

Antes de realizar la instalación del Firewall y demás servicios, se instaló Open vSwitch que es un conmutador virtual que va ayudar a crear puentes entre las máquinas virtuales y el servidor físico.

Para instalar OpenvSwitch, en primer lugar, se realiza una actualización de los paquetes, utilizando el comando:

- `apt-get update`

Posteriormente se procede a instalar Open vSwitch, para esto se ejecuta el comando:

- `apt install openvswitch-switch`

Terminada la instalación y configuraciones en Proxmox, se puede empezar con la creación de máquinas virtuales, siendo la primera de ellas el Firewall que se seleccionó, a continuación se muestra el proceso que se llevo a cabo para esta selección e implementación.

3.5. Firewall

3.5.1. Pruebas y selección

Como parte de las listas de pruebas, se realiza la instalación de distintos Firewall de código abierto, con los requerimientos mínimos en RAM y Disco duro. Se utilizo VirtualBox para crear distintas máquinas virtuales, y poder comparar el software. Los Firewall en los cuales se realizaron pruebas son: Pfsense, Smoothwall, IPFire, OPNSense, Endian e IPCop. En la tabla 3.1 se muestra los requerimientos mínimos para cada uno de los Firewall. Para su comparación, se tomaron en cuenta las características que se muestran en la tabla 3.2. Estas son de las más comunes para que cumplan con un buen desempeño.

Firewall	RAM	Disco
Pfsense	1 GB	8 GB
Smoothwall	128 MB	2 GB
IPFire	1 GB	4 GB
OPNSense	2 GB	4 GB
Endian	512 MB	8 GB
IPCop	512 MB	6 GB

Tabla 3.1: Requerimientos mínimos de los Firewall

Características	Pfsense	Smoothwall	IPfire	OPNSense	Endian	IPCop
Funciones de routing y firewall avanzado	Si	Si	Si	Si	Si	Si
NAT	Si	Si	Si	Si	Si	Si
Balanceador de carga	Si	No	Sin información	Si	Si	No
Dispone de cliente/servidor VPN con Ipsec y OPpenVPN	Si	No	Si	Si	Si	Si
Monitorización avanzada de la actividad de red mediante logs y gráficos	Si	Si	Si	Si	Si	Si
Servidor DNS	Si	Si	Si	Si	Si	Si
DNS dinámico y portales cautivos	Si	Si	Sin información	Si	Sin informacioń	Si
Servicios DHCP y DHCP Relay	Si	Si	Si	Si	Si	Si
Posibilidad de instalar software adicionales	Si	No	Si	Si	No	Si
Bloqueo de tráfico SPAM	Si	No	Si	Si	Si	Sin información
Bloque de potenciales eventos de phishing y virus	Si	Si	Sin información	Si	Si	Sin información
Bloqueo de anuncios tipo Adblocker	Si	Si	Si	Si	Si	Si
Portal restricto	Si	Sin información	Sin información	Sin información	Sin información	No
Monitor completo de tráfico web	Si	Si	No	Si	Si	Si

Tabla 3.2: Características comunes de los Firewall

Además, se consideran ciertos factores clave para la selección del firewall, basados en criterios previamente establecidos y en la experiencia de instalación y configuración de cada uno de los Software. Los elementos evaluados incluyen: interfaz intuitiva, disponibilidad de información, facilidad de instalación, facilidad de configuración y posibilidad de agregar extensiones. A cada firewall se le asigna una puntuación de 0 a 100 para cada criterio. En la tabla 3.3 se muestran las calificaciones asignadas a cada software.

Firewall	**Interfaz intuitiva**	**Información**	**Fácil Instalación**	**Configuraciones**	**Agregar extensiones**
Pfsense	100	100	100	100	100
IPFire	100	80	100	90	80
OPNSense	100	80	100	80	80
Endian	100	80	100	80	80
IPCop	100	80	100	80	80

Tabla 3.3: Consideraciones para la selección del Firewall

La instalación de Smoothwall no se logró realizar, a causa de la poca información existente para lograr resolver el problema que se presentaba, por esta razón, se decide dejar fuera de la tabla a este Firewall y por lo mismo descartarlo.

Para el caso de Pfsense, se tiene una muy buena experiencia en cuanto a instalación, información y facilidad al momento de realizar todas las configuraciones deseadas, además, cuenta con todas las herramientas que son más comunes en un Firewall, por todas las características que poseé Pfsense, se opta implementar este software en esta propuesta.

3.5.2. Instalación de Pfsense

Dados los resultados de la comparativa entre los distintos Firewalls evaluados, se concluye que el software Pfsense es la opción apropiada para cubrir las necesidades de una MiPyMe, por lo tanto este será el software utilizado en este trabajo.

Para realizar su implementación, en primer lugar, se debe descargar su imagen iso, esto se realiza entrando a la página oficial, en el apartado download. La figura 3.5 muestra la versión, arquitectura, tipo de instalación y espejo seleccionados para descargar Pfsense.

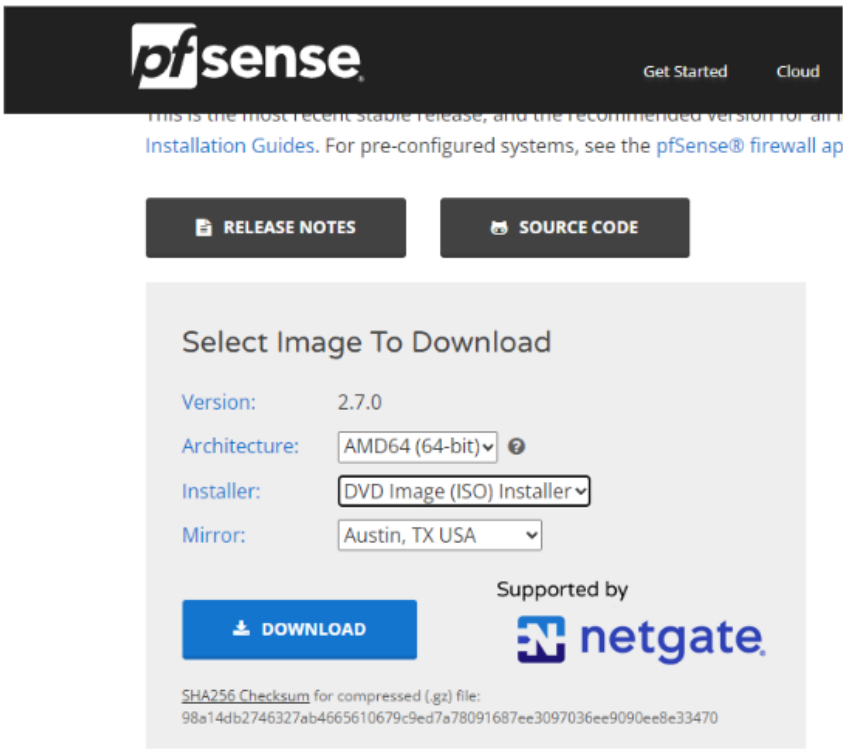

Figura 3.5: Descarga de Pfsense

Una vez descargada la imagen ISO, se debe cargar dentro de Proxmox, para esto se debe acceder al nodo que se creó, en este caso se llama “proyecto”, se abre la pestaña “local(proyecto)”, donde aparece el recuadro de “ISO Images”, ahí se selecciona “Upload” y se agrega la imagen ISO. La figura 3.6 muestra la ubicación de la imagen ISO de Pfsense dentro de Proxmox.

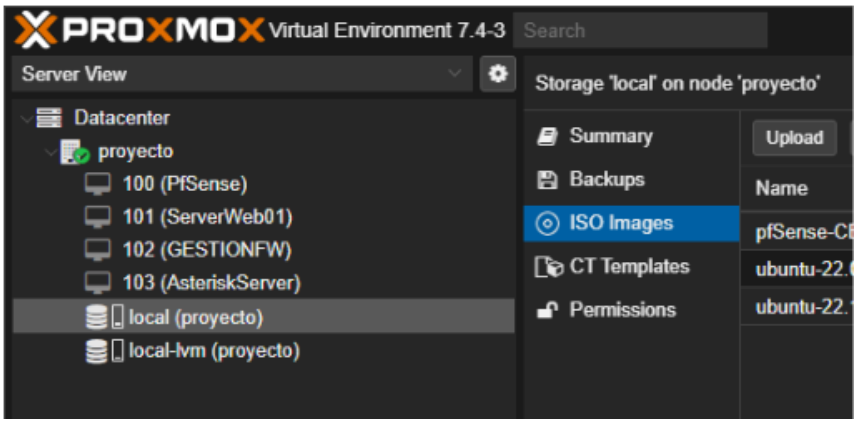

Figura 3.6: Imagen ISO de Pfesense

Ya que se cargó la imagen ISO, se puede realizar la instalación de Pfsense, para esto se crea una VM (Virtual Machine) seleccionando el icono de Create VM como se muestra en la figura 3.7.

Figura 3.7: Icono para crear una VM

Como primer paso, se selecciona el nombre para la máquina, en este caso se llama Pfsense como se muestra en la figura 3.8.

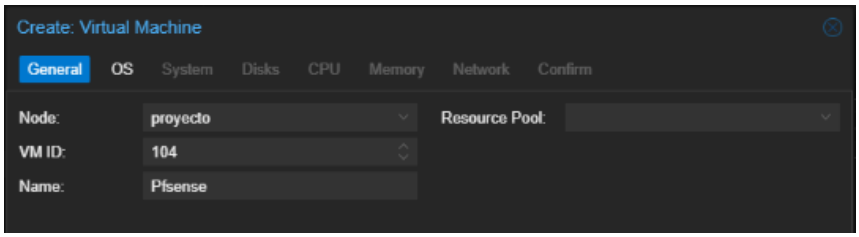

Figura 3.8: Nombre de la VM

Posteriormente, se agrega el ISO en el apartado de "OS" que ya se encuentra cargado como se observa en la figura 3.9.

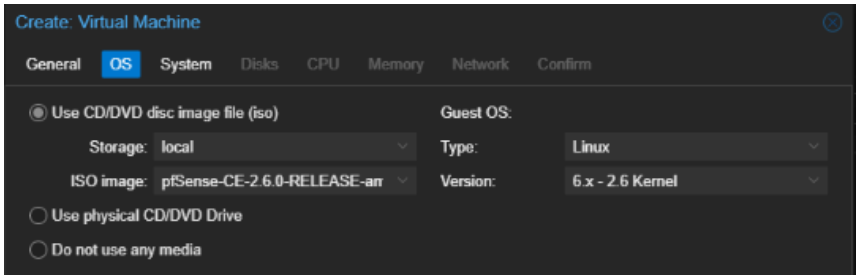

Figura 3.9: OS de Pfsense

En la parte de System se selecciona "VirtiO SCSI" en el controlador (SCSI Controller), lo demás se deja por defecto como se muestra en la figura 3.10.

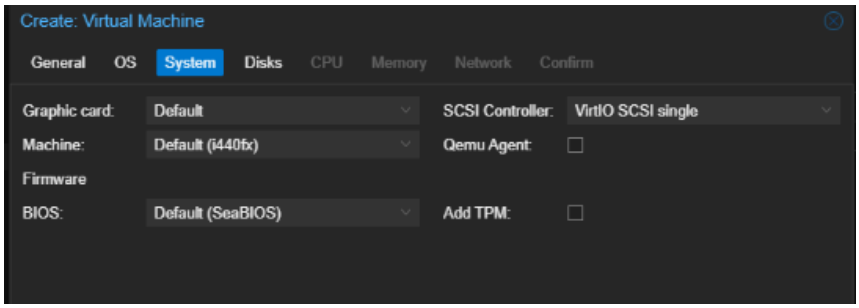

Figura 3.10: System de Pfsense

Se asigna un disco duro de 32 GB y en caché se deja por defecto como se puede ver en la figura 3.11.

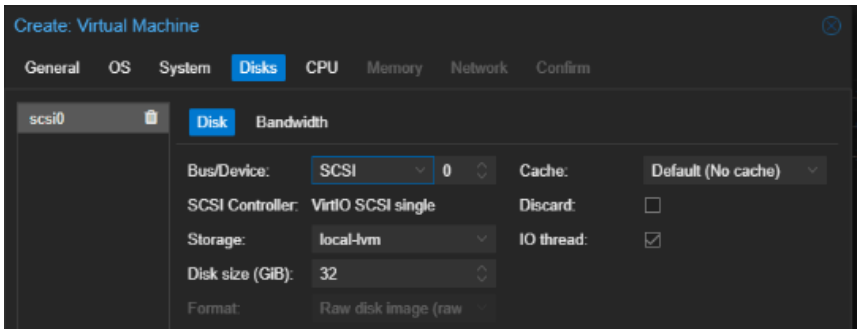

Figura 3.11: Disk de Pfsense

En CPU se agregan 2 Cores y 2 sockets como se obeserva en la figura 3.12.

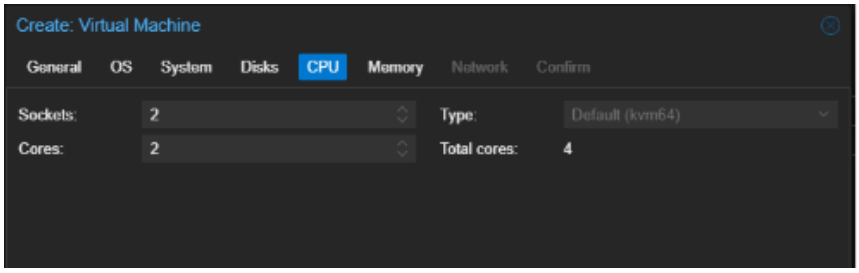

Figura 3.12: CPU de Pfsense

Se agrega una memoria RAM de 2GB como se observa en la figura 3.13, la cual se puede cambiar en un futuro.

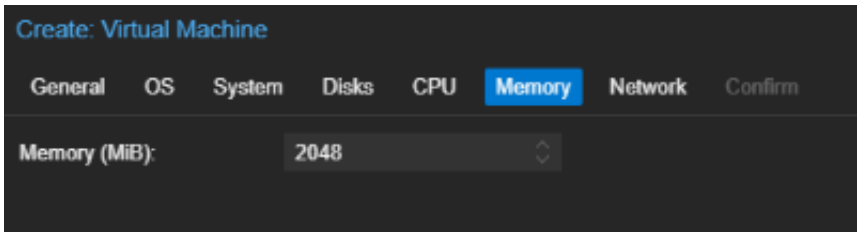

Figura 3.13: Memory de Pfsense

En los ajustes de la red, se selecciona el puerto virtual “vmbr0” como se observa en la figura 3.14, este está en bridge con la tarjeta de red que conecta hacia el ISP del laboratorio.

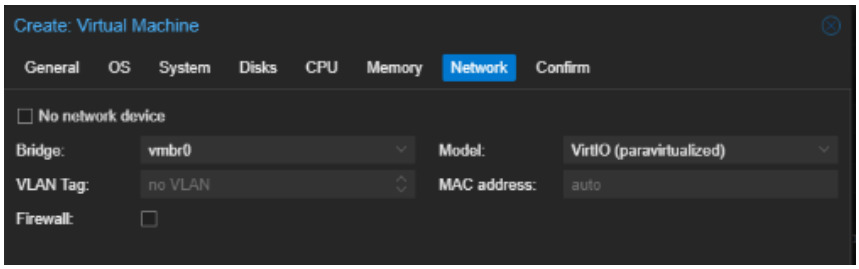

Figura 3.14: Network de Pfsense

Finalmente se confirma la configuración como se observa en la figuar 3.15 y sólo queda esperar por la creación de la máquina virtual.

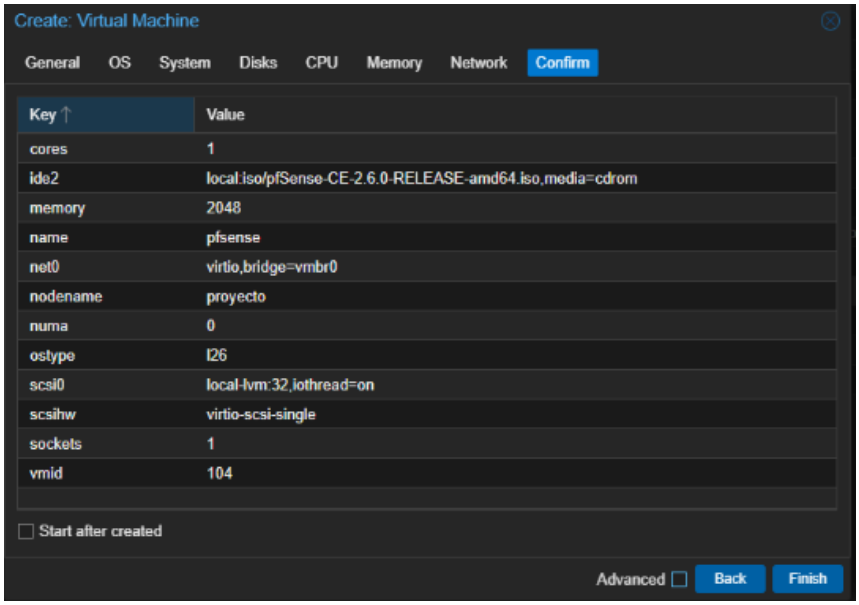

Figura 3.15: Configuración final de Pfsense

Una vez creada la máquina virtual, se selecciona en “Start Now”, para empezar con la instalación como se observa figura 3.16.

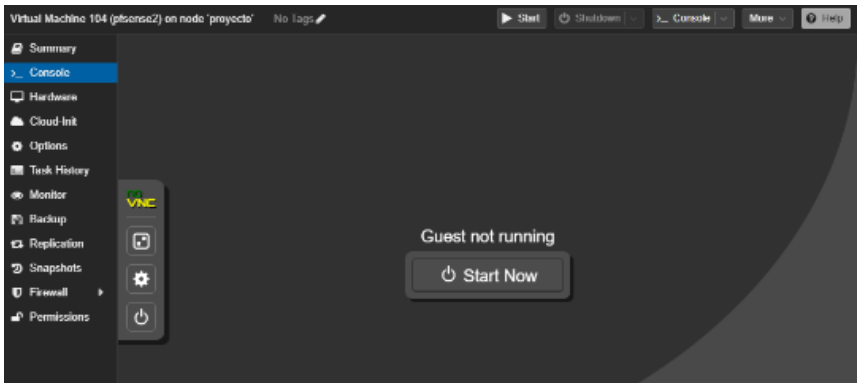

Figura 3.16: Inicio de la VM

Cuando termina la instalación, se crea una interfaz virtual de Pfsense denominada "vnet0", esta interfaz está en bridge con vmbr0 de Proxmox y la cual está en bridge con la interfaz física de red del servidor que se conecta a la WAN del laboratorio, con una IP asignada por DHCP. Esta conexión se encarga de brindar conexión de internet a pfsense como se muestra en la figura 3.17.

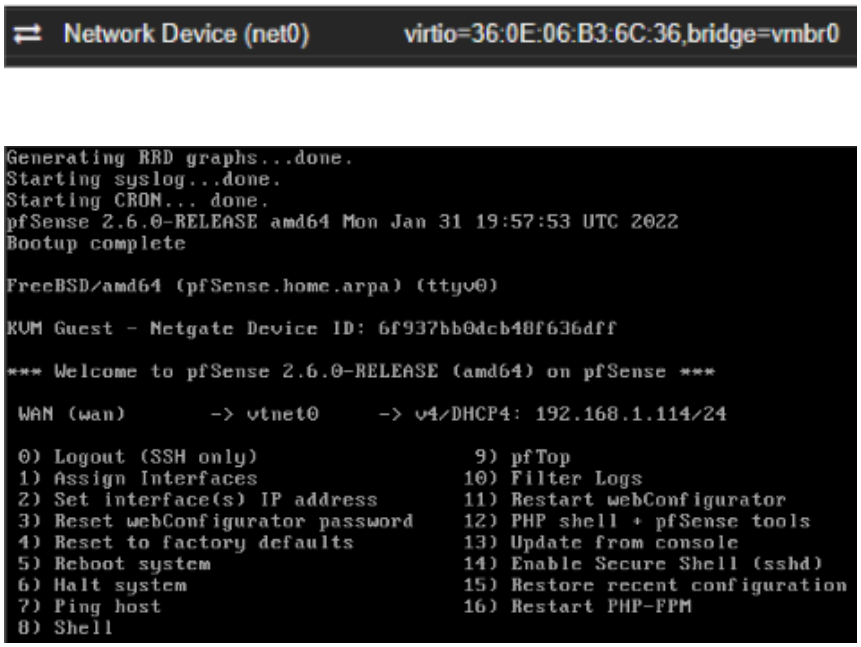

Figura 3.17: Conexión hacia la WAN en Pfsense

Después de que se haya terminado la instalación se podrá acceder a la interfaz web para poder realizar las configuraciones del Firewall. Es importante tener bien identificados los puertos virtuales debido a que algunos están en puente con un puerto físico y si estos llegan a estar mal conectados causaría problemas en las redes respecto a la conexión y configuraciones que se realizan a cada una de ellas.

3.5.3. Configuraciones de Pfsense

Asignación de redes

Las primeras configuraciones realizadas en Pfsense son la asignación de redes, para realizarlo, en primer lugar, se deben agregar más interfaces de red, para hacerlo se dirige a la pestaña Hardware, se selecciona la opción "Add" y posteriormente "Network Device", como se muestra en la figura 3.18

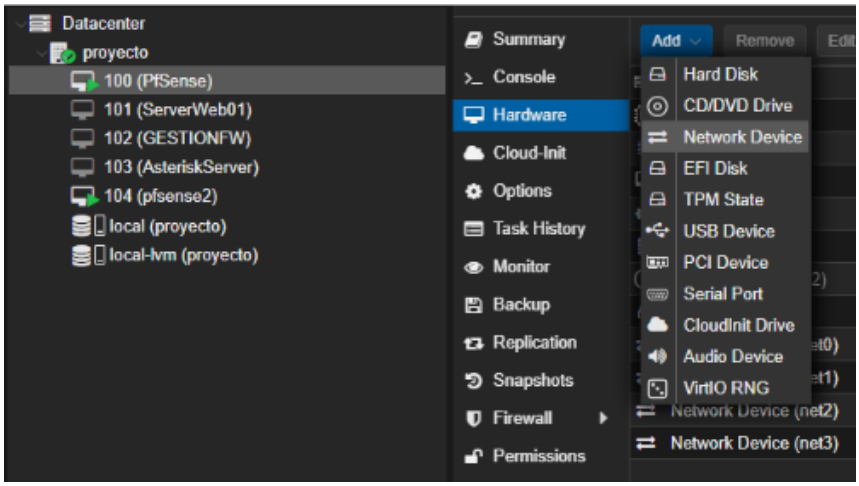

Figura 3.18: Añadir interfaces

Se abrirá la ventana que se muestra en la figura 3.19, aquí se selecciona con qué interfaz se conectará Pfsense en bridge hacia Proxmox y se quita el Firewall, para no tener problemas de conexión.

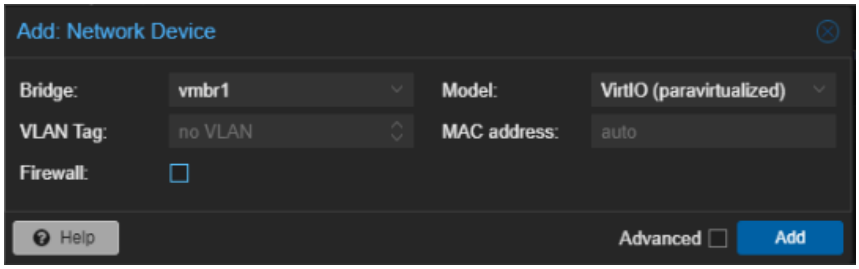

Figura 3.19: Bridge de Pfsense hacia Proxmox

La figura 3.20, muestra todas las interfaces que son agregadas en Pfsense, donde, "net0" estará conectada a la red WAN, "net1" se conectará a la red LAN, "net2" con la red WLAN, "net3" con la DMZ y "net4" con ASTERISK.

Figura 3.20: Interfaces habilitadas

Una vez que se agregaron las interfaces de red en la VM, se ingresa en ellas y se realiza la asignación de cada interfaz hacia la red que pertenecerá, existen dos formas de realizarlo, una es por medio de la interfaz web y la otra es desde la consola de línea de comandos de Pfsense.

La asignación de estas interfaces se realizan dentro de la consola de Pfsense, para esto se selecciona la opción 1, que indica "Assign Interfaces", como se muestra en la figura 3.21.

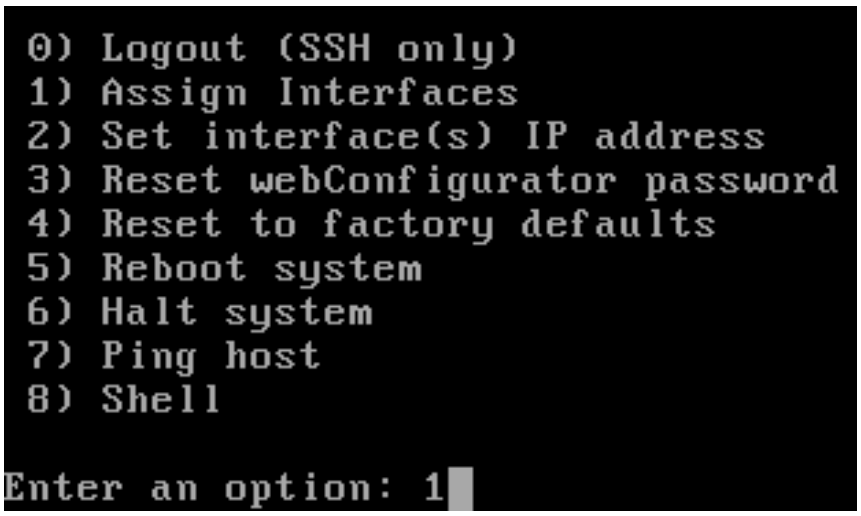

Figura 3.21: Asignación de interfaces

Una vez seleccionada la opción 1, preguta si se quiere agregar una VLAN, en este caso se indica que no con la letra "n", como se muestra en la figura 3.22.

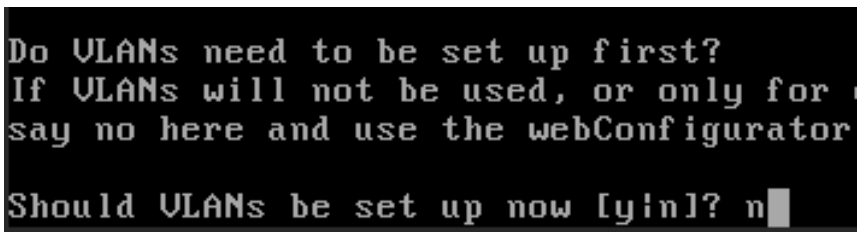

Figura 3.22: Agregar VLAN

En la figura 3.23, se muestra la asignación de todas las interfaces. Primero, pide que se introduzca el nombre de la interfaz que corresponda a la red WAN, en este caso es la interfaz "vtnet0" la que corresponde a esta red, después, para la red LAN, corresponde la interfaz "vtnet1", para la WLAN corresponde "vtnet2" y para la DMZ "vtnet3". Finalmente, preguntara si se desea proceder, con la letra "y" se indica que sí.

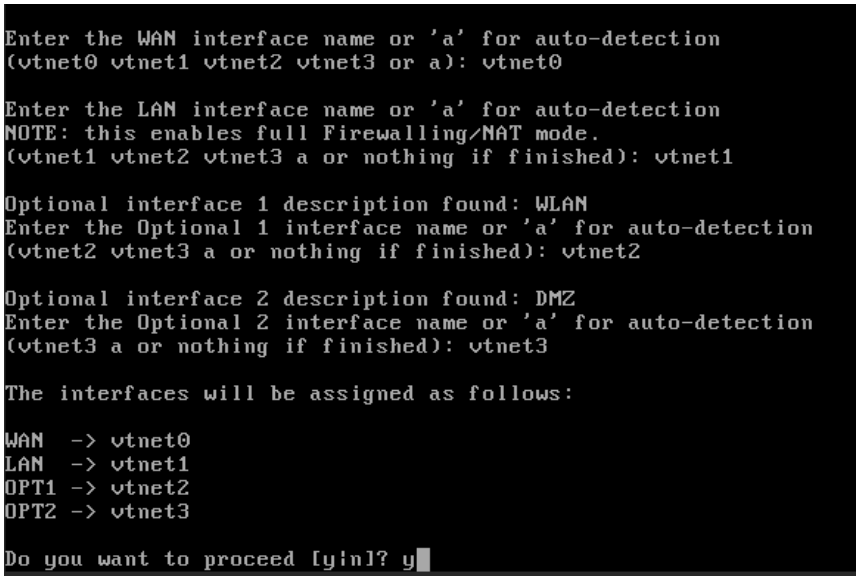

Figura 3.23: Interfaces agregadas a Pfsense

Configuración de reglas

Para poder asegurar la red, se necesita tener reglas en PfSense. Las reglas van a indicar la manera en como es gestionado el tráfico de red. Estas van a generar un conjunto de condiciones que se deben cumplir en la conexión y una acción para permitir o bloquear el tráfico. Si el Firewall encuentra paquetes de tráfico que coincidan con las condiciones de las reglas, este realiza la acción que este asociada.

Para la asignación de reglas en esta red, se va a limitar el acceso de las redes creadas en el Firewall, esto quiere decir que, la DMZ en donde se encuentra la página web, no debe tener comunicación con el Firewall, ni la red WAN; pero el Firewall si puede tener comunicación con las redes LAN que se crearon y que en un futuro se puedan crear. Esto se hace para evitar que cualquiera pueda entrar y editar las configuraciones del Firewall, si alguien lo hace, se deja expuesta toda la información que se quiere proteger, es por eso que es indispensable esta parte.

Este tipo de regla podría verse aún más estricta, ya que, solo se esta limitando la comunicación entre las redes, también se podría restringir el acceso a ciertas páginas web, y así evitar la descarga de archivos no deseados, o caer en estafas, todo esto con el fin de tener un mejor control del tráfico de datos tanto de entrada como de salida. Todo esto va

a depender de las necesidades que tenga la empresa.

La asignación de las reglas se realizan desde la interfaz web de Pfsense que se observa en la figura 3.24, se accede desde una máquina conectada a la LAN, en el browser se coloca la dirección IP asignada a la interfaz LAN, para acceder a Pfsense solicitara que se coloque el usuario y contraseña.

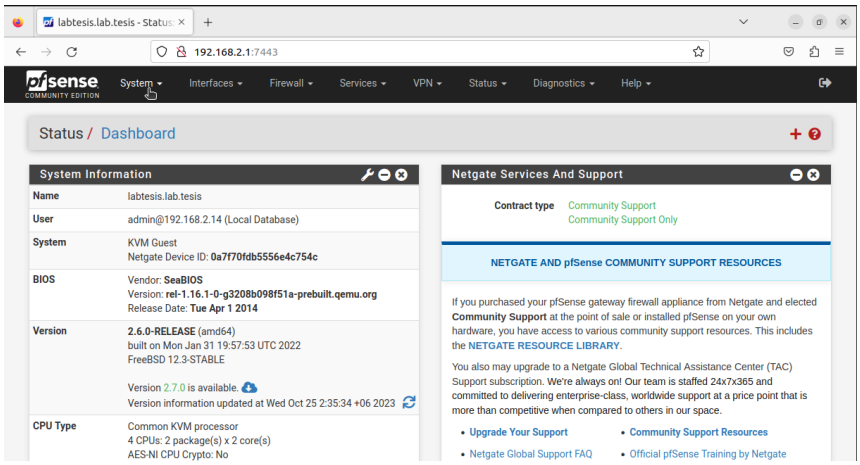

Figura 3.24: Interfaz web

Dentro de la interfaz web en la pestaña de Firewall, se selecciona la opción de “Rules”, como se muestra en la figura 3.25

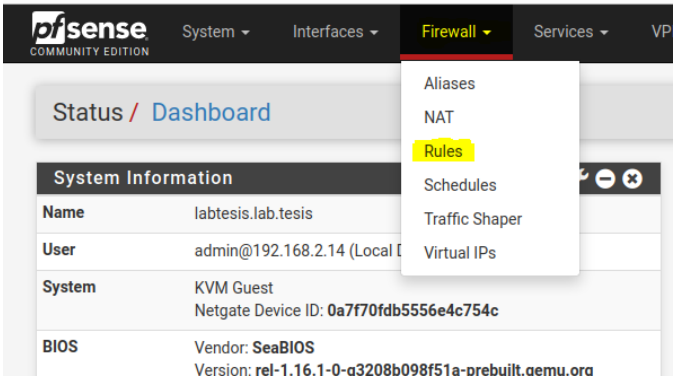

Figura 3.25: Acceder a las reglas

En la figura 3.26 se muestra la ventana en donde se encuentra la configuración de las reglas para cada interfaz asignada en Pfsense.

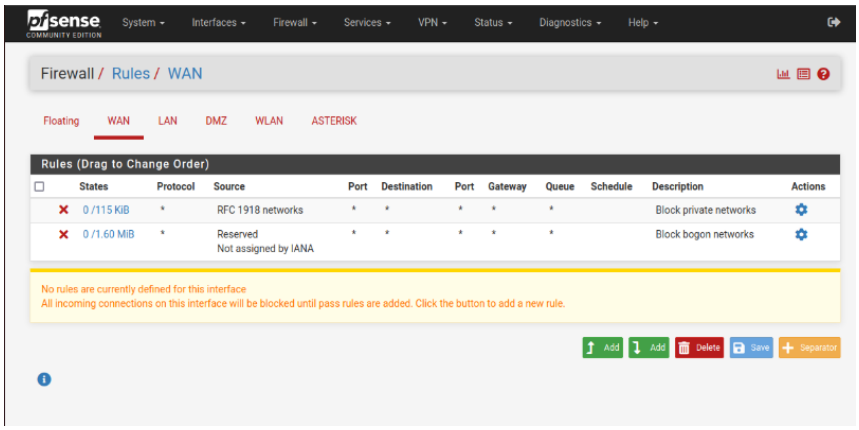

Figura 3.26: Reglas

Con estas reglas se logra tener control del tráfico en las distintas redes conectadas a Pfsense, a la LAN se le da acceso para poder tener flujo hacia todas las redes, estas mismas reglas se aplican en las redes WLAN y ASTERISK, debido a se le asigno el mismo tipo de comunicación. Para la WAN se bloquea el acceso, esto para evitar la filtracion de tráfico no deseado y por último la DMZ, se le bloquea el tráfico hacia las redes LAN, WLAN y ASTERISK, esta zona se busca que solo reciba tráfico proveniente de la red WAN, debido a que esta destinado a funcionar como servidor web.

3.6. Cámaras

3.6.1. Programación de la cámara ESP32-CAM

Para incrementar la seguridad en la MiPyMe se implementa el uso de cámaras de seguridad, para esto se utiliza ESP32-CAM, que es una tarjeta de desarrollo basado en el microcontrolador ESP32-S que trae incorporada una cámara OV2640 que permite hacer streaming de video, esta se conecta a la red por medio de WiFi [21].

Para utilizar esta placa se debe programar desde la PC, con ayuda del softaware arduino IDE. Antes de empezar es necesario instalar el controlador CH340 que va a permitir programar y establecer comunicación USB-Serial [21].

Para iniciar con la programación de la cámara dentro del software arduino IDE se abre la pestaña File y se selecciona la opción de “preferences”, posteriormente “Aditional board manager”, ahí se agrega el url: “https://dl.espressif.com/dl/package_esp32_index.json” y dar click en OK, como se muestra en la figura 3.27.

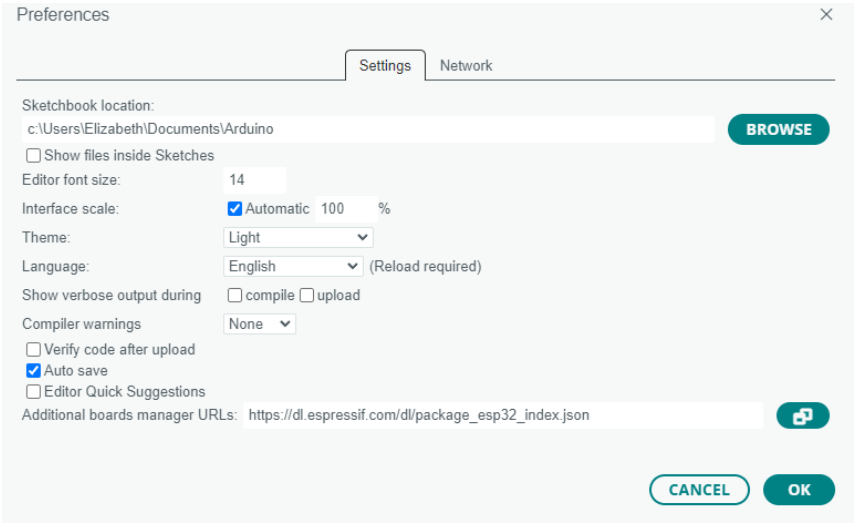

Figura 3.27: URL para descargar la placa de esp32

En la pestaña de "Tools", se selecciona "boards" y posteriormente "boards manager", se abrirá una pestaña y dentro se busca la placa esp32 by Espressif Systems y posteriormente se instalan como se muestra en la figura 3.28.

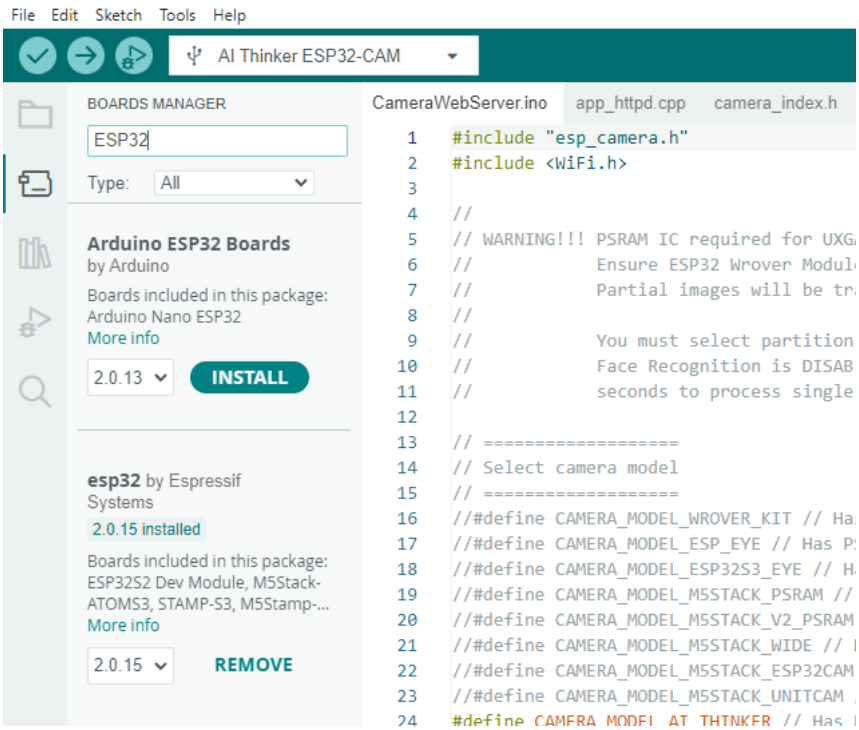

Figura 3.28: Descarga de placa esp32 en Arduino

Nuevamente en la pestaña de "Tools" y después a la opción "board", se despliegan 3 opciones de la cual se seleciona "esp32" y se busca la placa "AI Thinker ESP32 CAM" como se muestra en la figura 3.29

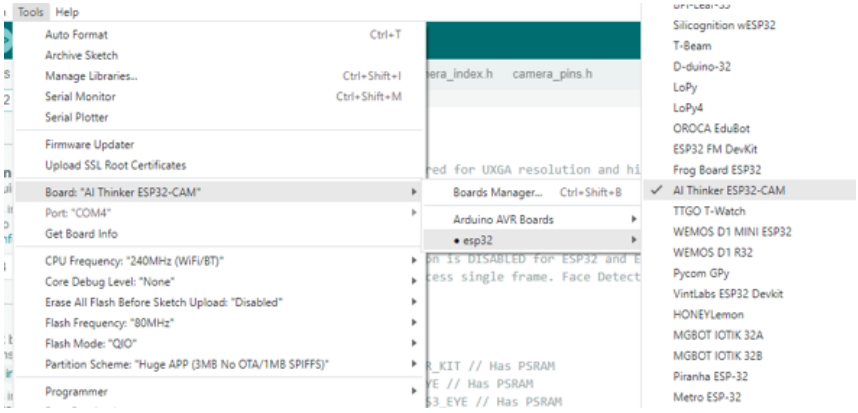

Figura 3.29: Selección de la placa AI Thinker ESP32 CAM

Ahora ya se puede conectar la placa a la PC, para comprobar que se conecto y que la PC lo esta reconociendo, en la pestaña "Tools", del menú desplegable se selecciona "Port", como se muestra en la figura 3.30 sólo se muestra una opción ya que es el único dispositivo conectado a la PC.

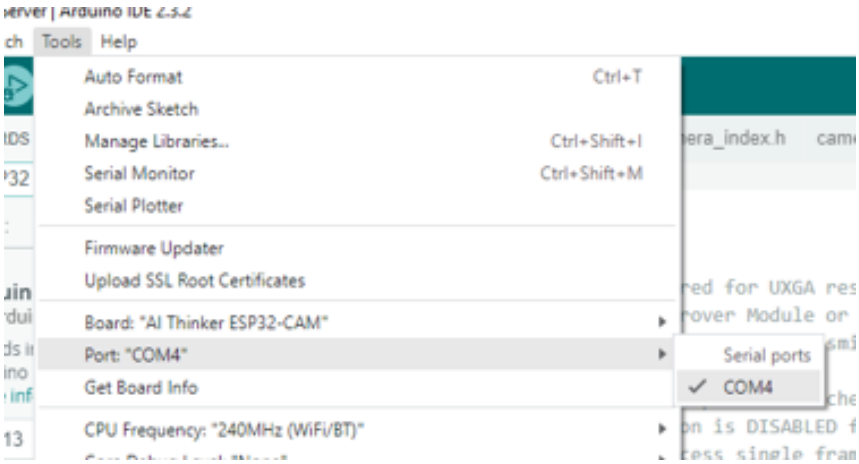

Figura 3.30: Selección del puerto

Se inserta una plantilla para programar la placa,en la pestaña "File" y después a "examples", se seleciona ESP32 y de las opciones mostradas se selecciona "camera" como se muestra en la figura 3.31.

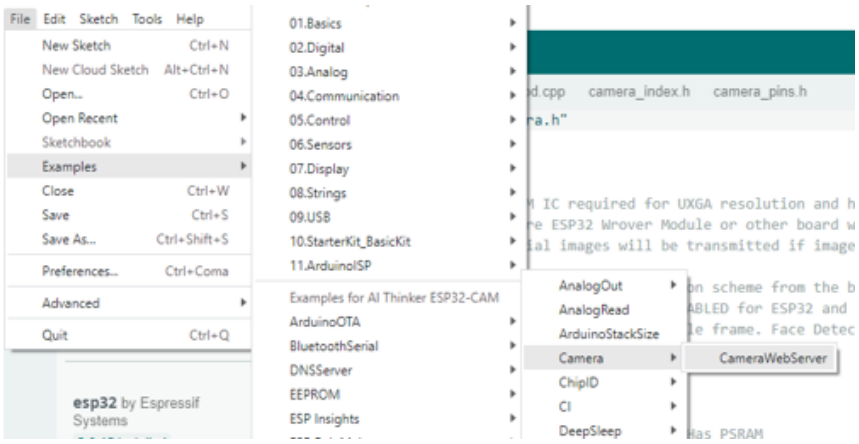

Figura 3.31: Insertar código de ejemplo para programar la cámara

Antes de cargar el ejemplo de "CamaraWebServer" se modifica la linea de código `CAMERA_MODEL_WROVER_KIT` y descomentar la línea de código `CAMERA_MODEL_AI_THINKER` como se muestra en la figura 3.32.

```
// ==================
//#define CAMERA_MODEL_WROVER_KIT // Has PSRAM
//#define CAMERA_MODEL_ESP_EYE // Has PSRAM
//#define CAMERA_MODEL_ESP32S3_EYE // Has PSRAM
//#define CAMERA_MODEL_M5STACK_PSRAM // Has PSRAM
//#define CAMERA_MODEL_M5STACK_V2_PSRAM // M5Camera version B H
//#define CAMERA_MODEL_M5STACK_WIDE // Has PSRAM
//#define CAMERA_MODEL_M5STACK_ESP32CAM // No PSRAM
//#define CAMERA_MODEL_M5STACK_UNITCAM // No PSRAM
#define CAMERA_MODEL_AI_THINKER // Has PSRAM
//#define CAMERA_MODEL_TTGO_T_JOURNAL // No PSRAM
//#define CAMERA_MODEL_XIAO_ESP32S3 // Has PSRAM
// ** Espressif Internal Boards **
//#define CAMERA_MODEL_ESP32_CAM_BOARD
```

Figura 3.32: lineas de código para definir la cámara

Como se muestra en la figura 3.33 se conecta a una red WiFi la placa, en las siguientes líneas de código colocar el nombre y contraseña de la red WiFi.

```
#include "camera_pins.h"
const char* ssid = "----";
const char* password = "----";
```

Figura 3.33: Lineas para conectar a WiFi

Antes de programar la placa se debe poner en modo de programación, para hacerlo se debe mantener presionado el botón de FLASH después presionar una vez el botón de RESET sin dejar de presionar FLASH y por último dejar de oprimir FLASH. La figura 3.34 muestra los botones que se deben oprimir.

Figura 3.34: Placa ESP32-CAM

Ya cargado el código, se abre el monitor serie y se cambia la velocidad de baudios a 115200, después se presiona el botón de RESET a la placa y se espera a que se conecte a la red WiFi. ya que se conecte se imprimirá una dirección IP como se muestra en la figura 3.35

Figura 3.35: IP para acceder al video

Con esto ya se puede abrir un navegador web, e ingresar la dirección IP, se debe estar conectado a la misma red WiFi. Para ver la cámara dar clic en START STREAM como se muestra en la Figura 3.36

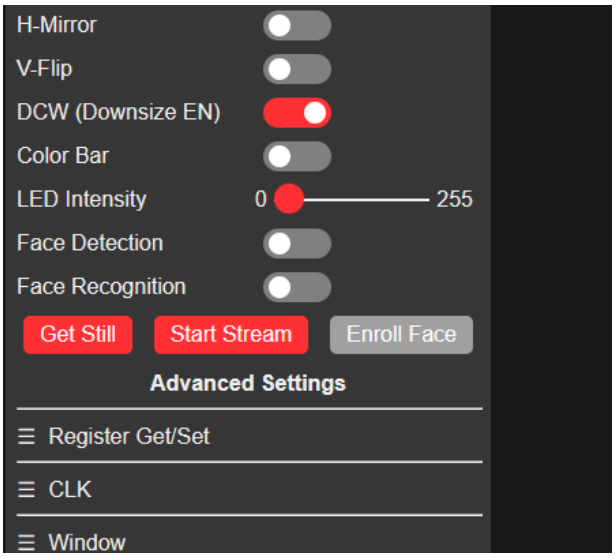

Figura 3.36: Iniciar la cámara

3.6.2. Instalación de ZoneMinder

Como medida de seguridad, se realiza la instalación de una cámara que pueda colocarse en alguna zona estratégica para monitorear las instalaciones de la MiPyMe, dicho monitoreo se puede realizar con ayuda de ZoneMinder, el cual permite guardar las grabaciones, apagar la cámara, prender la cámara, entre otras.

El software se instala en un servidor Ubuntu mediante la creación de una máquina virtual (VM) en Proxmox. Para ello, se asigna un nombre a la máquina, denominada "ZoneMinder", y se carga el ISO de Ubuntu Server previamente disponible. En el apartado de "System", se dejan los parámetros predeterminados; se asigna un disco duro de 64 GB, 2 núcleos y 2 sockets de CPU, así como 2 GB de memoria RAM. Para la configuración de red, se selecciona el puerto virtual vmbr5, el cual está en modo bridge con PfSense y forma parte de la red de cámaras, además de estar conectado en bridge con la interfaz física eno5. Finalmente, se confirma la configuración y se espera a que se complete la creación de la VM, como se muestra en la figura 3.37.

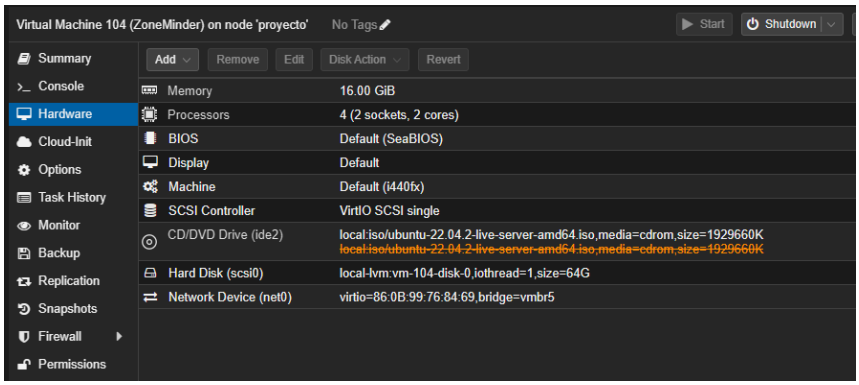

Figura 3.37: Hadware ZoneMinder

Terminada la instalación del SO, se ingresa al servidor con sus respectivas credenciales, para posteriormente realizar una actualización del sistema utilizando el comando:

```
- apt update -y
```

Para ejecutar ZoneMinder se necesita de un servidor web Apache, PHP y MySQL, por lo tanto, primero se configura el servidor LAMP completo en el sistema, con el comando:

```
- apt install apache2 mysql-server php
```

Posteriormente se habilitan los servicios:

```
- systemctl enable -now apache2 mysql
```

Con el siguiente comando se puede ver el estatus de los servidores

```
- systemctl status apache2 mysql -no-pager -l
```

En la figura 3.38 se puede observar el Software de ZoneMinder

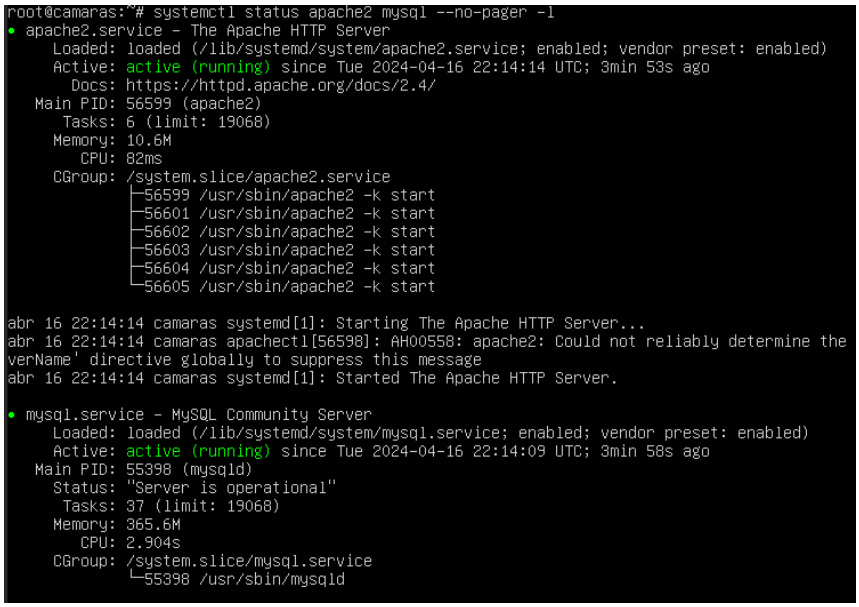

Figura 3.38: Software ZoneMinder

ZoneMinder está disponible para instalarse usando el administrador de paquetes APT y el repositorio base de Ubuntu, por lo tanto se puede ejecutar un único comando para obtener dicho repositorio

- `sudo add-apt-repository ppa:iconnor/zoneminder-1.36`

Una vez agregado el repositorio, se ejecuta el comando de actualización del sistema

- `apt update && apt upgrade`

Ahora se procede a instalar ZoneMinder.

- `apt install zoneminder`

El siguiente paso es configurar MySQL, primero se elimina el siguiente archivo

- `rm /etc/mysql/my.cnf`

Posteriormente se hace copia del siguiente archivo

- `cp /etc/mysql/mysql.conf.d/mysqld.cnf /etc/mysql/my.cnf`

Se Accede al siguiente archivo para editarlo

```
- nano /etc/mysql/my.cnf
```

Al final del archivo se agrega la siguiente línea

```
- sql_mode = NO_ENGINE_SUBSTITUTION
```

Para guardar el archivo se presiona "Ctrl+O", presionando la tecla Enter y luego salir presionando "Ctrl+X".

Los siguientes comandos permiten que el usuario de Apache tenga acceso a los archivos de ZoneMinder para que pueda manejar las peticiones de los usuarios y enviar los archivos asociados a la aplicación.

```
- chmod 740 /etc/zm/zm.conf
```

```
- chown root:www-data /etc/zm/zm.conf
```

```
- chown -R www-data:www-data /usr/share/zoneminder/
```

Se habilitan los módulos de Apache:

```
- a2enmod cgi rewrite expires headers
```

Se habilita el archivo de configuración del host virtual ZoneMinder:

```
- a2enconf zoneminder
```

Se establece la fecha y zona horaria en el archivo PHP.ini

```
- nano /etc/php/*/apache2/php.ini
```

Para encontrar el área desde donde se puede configurar la zona horaria, se presiona "Ctrl + w", se escribe Date y luego se presiona la tecla "Enter". Una vez localizada el área se agrega la zona horaria, en este caso se coloca la de Mexico_City como se observa en la figura 3.39.

```
[Date]
; Defines the default timezone used by the date functions
; https://php.net/date.timezone
date.timezone = America/Mexico_City
```

Figura 3.39: Zona horaria

Con los siguientes comandos se inicia y habilita el servicio del sistema ZoneMinder:

- `systemctl enable zoneminder`

- `systemctl start zoneminder`

Además, se debe recargar el servicio Apache para aplicar los cambios que se han realizado

- `systemctl reload apache2`

Para acceder a la interfaz web de ZoneMinder, se abre un navegador que pueda acceder a la dirección IP del servidor donde esta instalado el software. La primera vez que se ingresa muestra los términos de privacidad, en la parte inferior derecha se presiona en Apply como se observa en la figura 3.40.

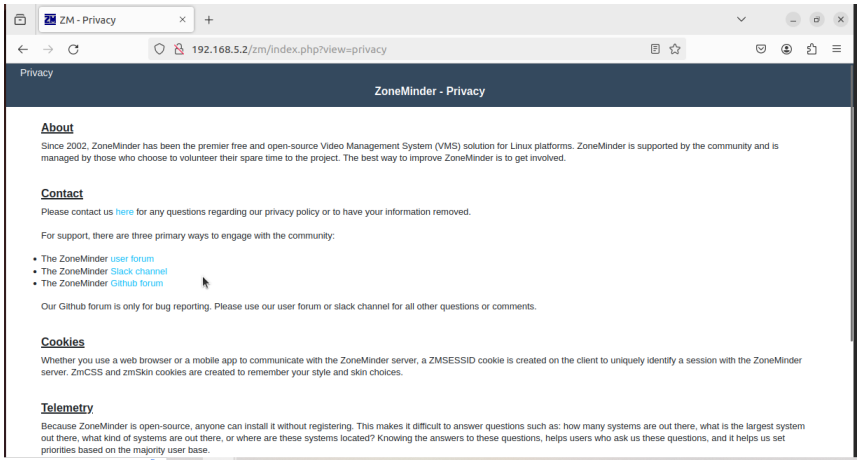

Figura 3.40: Acceso web ZoneMinder

Finalmente como se observa en la figura 3.41 se puede ver la pantalla de inicio de la interfaz web de ZoneMinder.

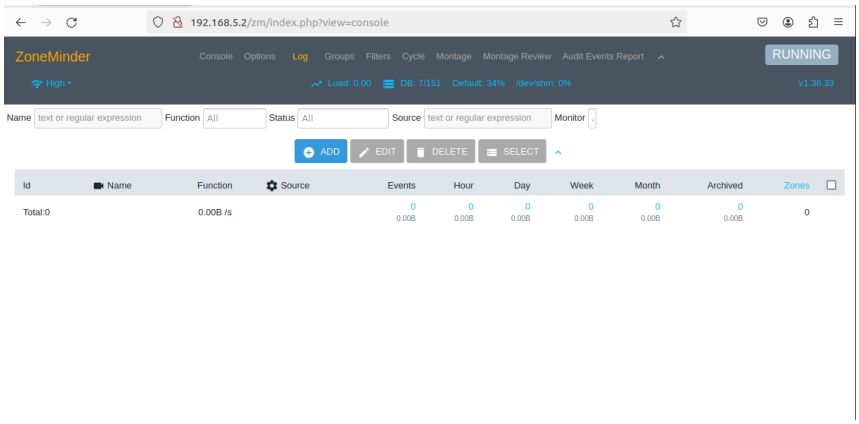

Figura 3.41: Pantalla inicio ZoneMinder

Para agregar las cámaras a ZoneMinder, primeramente, hay que asegurarse de que no se encuentren iniciadas como se observa en la figura 3.42, para saber esto, se dirige a la dirección IP de una de las cámaras (192.168.3.6), en la parte inferior se observan 3 botones, uno de ellos dice "start stream", eso significa que no está iniciada, si por alguna razón se llega a ver "stop stream" eso significa que esta iniciada.

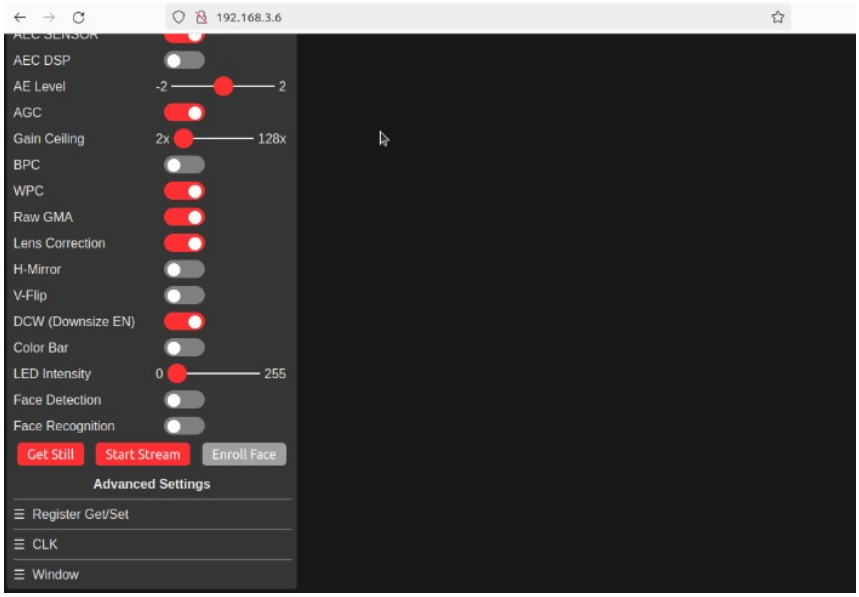

Figura 3.42: Cámara no iniciada

En la página web de ZoneMinder como se observa en la figura 3.41, se da clic en el botón "ADD", abre una pantalla nueva, donde del lado izquierdo se observan varías opciones, primero se selecciona "General", se le asigna el nombre de la cámara que se va a agregar, en este caso se nombró "CAM6" como se muestra en la figura 3.43.

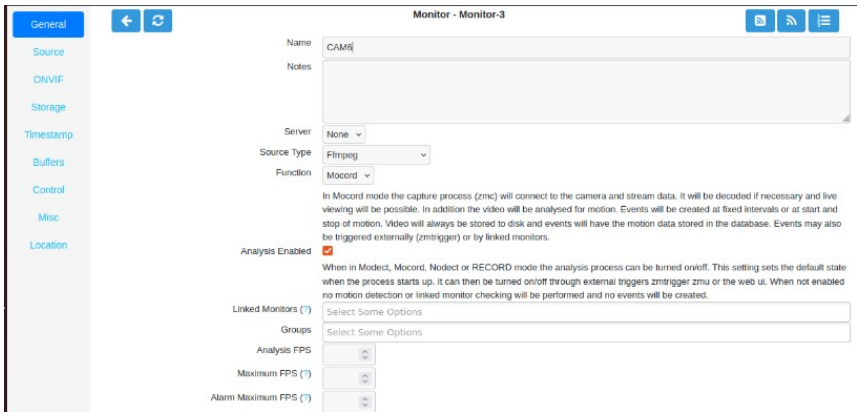

Figura 3.43: Página web de ZoneMinder para configurar las cámaras

Para agregar la cámara se accede a la opción de "Source", dentro se agrega la IP en la parte de "Source Path", también se agrega la resolución (640X480) y en "Method" se selecciona el protocolo de transporte TCP como se observa en la figura 3.44.

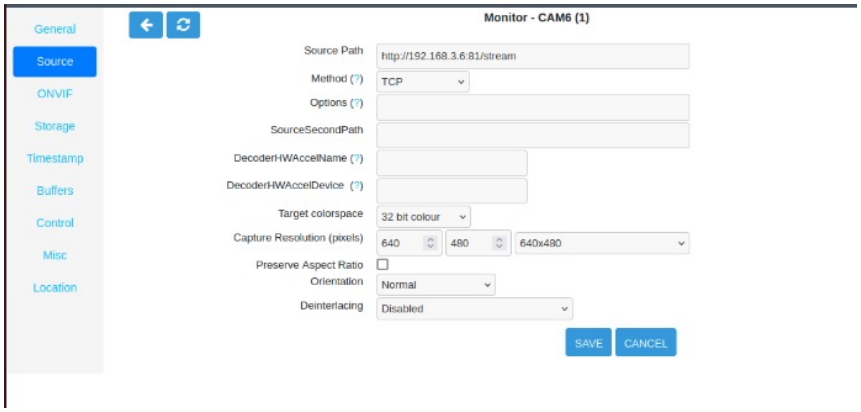

Figura 3.44: Opción para nombrar cámara

Se guardan estas configuraciones apretando el botón "SAVE", para la segunda cámara se realizan los mismos pasos, agregando la IP correspondiente.

Un servicio que se le añadió a esta propuesta, es la implementación de un servidor web para la MiPyMe, si ya se cuenta con una página se pueda adaptar a este proyecto, a continuación se muestra el desarrollo para la instalación y configuración.

3.7. Servidor Web

3.7.1. Instalación

Como servidor se selecciona un Ubuntu server 22.04 LTS. Para realizar la instalación del sistema operativo, en primer lugar se crea una VM en Proxmox, posteriormente, se

selecciona un nombre para la máquina, se agrega el ISO de Ubuntu Server que ya se tiene cargado en el apartado "System", se deja todo por defecto, se le asigna un disco duro de 32GB, en CPU se agregan 2 Cores y 2 sockets, se agrega una memoria RAM de 4 GB. Para la parte de red, se selecciona el puerto virtual vmbr4, que esta en bridge con Pfsense y forma parte de la DMZ. Finalmente se confirma la configuración para crear la VM.

3.7.2. Configuraciones

Instalación de Joomla

Para gestionar el contenido en la página web se instala Joomla, este se utiliza para publicar aplicaciones y sitios web en línea. Está escrito en PHP y suele estar configurado para utilizar bases de datos MySQL/MariaDB.

Lo primero que se realiza para su instalación es comprobar que el servidor este actualizado, para esto se ejecutaron los siguientes comandos:

- `sudo apt-get update`

- `sudo apt-get upgrade`

Para que joomla funcione se requiere de un servidor web, por lo tanto se decide instalar LAMP, el cual consta de varias tecnologías de software diferentes, servidor web Apache, servidor de bases de datos MySQL y la última versión de PHP con otras extensiones. Para instalar LAMP se utiliza el siguiente comando:

- `apt install apache2 mysql-server php8.1 libapache2-mod-php8.1 php8.1-dev php8.1-bcmath php8.1-intl php8.1-soap php8.1-zip php8.1-curl php8.1-mbstring php8.1-mysql php8.1-gd php8.1-xml unzip -y`

Se debe crear una base de datos y un usuario joomla, para que se pueda almacenar el contenido de la web. Para esto primero, se debe conectar a MySQL con el siguiente comando:

- `mysql`

Una vez conectado, se crea una base de datos y un usuario con los siguientes comandos:

- `mysql>CREATE DATABASE joomladb;`

- `mysql>CREATE USER 'labtesis'@'localhost' IDENTIFIED BY 'SM5306';`

Posteriormente, se le concede todos los privilegios a la base de datos de Joomla con el siguiente comando:

```
- mysql>GRANT ALL ON joomladb.* TO 'labtesis'@'localhost';
```

Se vacía la tabla de privilegios y salir de MySQL:

```
- mysql>FLUSH PRIVILEGES;
```

```
- mysql>EXIT;
```

Una vez que se realizaron todos los pasos anteriores, se puede instalar Joomla:

```
- wget https:/downloads.joomla.org/cms/joomla4/4-1-2/Joomla_4-1-2-Stable-
Full_Package.zip
```

Completada la descarga, se descomprime el archivo descargado:

```
- unzip Joomla_4-1-2-Stable-Full_Package.zip -d /var/www/html/joomla
```

A continuación, se debe cambiar la propiedad y permisos de Joomla:

```
-chown -R www-data:www-data /var/www/html/joomla/ - chmod -R 755 /var/
www/html/joomla/
```

Se debe crear un archivo de configuración del host virtual de Apache para Joomla. para su creación se utiliza el siguiente comando:

```
- nano /etc/apache2/sites-available/joomla.conf
```

Dentro del archivo, se agregan las siguientes líneas que se muestran en la figura 3.45:

```
<VirtualHost *:80>

ServerAdmin webmaster@your-domain.com

ServerName joomla.example.com
DocumentRoot /var/www/html/joomla

<Directory /var/www/html/joomla/>
        Options FollowSymlinks
        AllowOverride All
        Require all granted
</Directory>

ErrorLog ${APACHE_LOG_DIR}/example.com_error.log
CustomLog ${APACHE_LOG_DIR}/example.com_access.log combined

</VirtualHost>
```

Figura 3.45: Archivo de configuración del host virtual de Apache para Joomla

Se guarda y cierra los cambios dentro del archivo, luego se activa el host virtual de Joomla:

```
- a2ensite joomla.conf
```

Una vez terminados todos los pasos anteriores, se puede acceder a la instalación web de Joomla. Para esto nos dirigimos al navegador y utilizando la dirección 10.0.0.3/joomla se puede acceder al instalador como se muestra en la figura 3.46

Figura 3.46: Instalador web de Joomla

Se llena la información respectiva y se da clic en Configurar datos de acceso. Aparece

la siguiente página:

Se proporciona un nombre, usuario, contraseña y dirección de correo electrónico,una vez llenada la información se da clic en Configurar la conexión a la base de datos. Surge la siguiente página que se muestra en la figura 3.47:

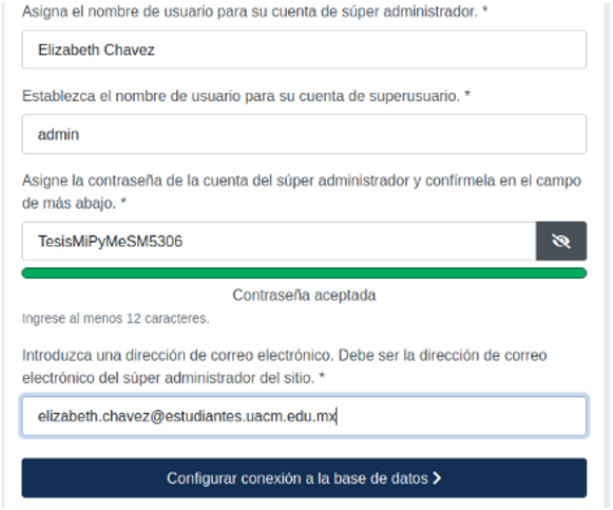

Figura 3.47: Datos de inicio de sesión en Joomla

Como se muestra en la figura 3.48 se proporciona el nombre de la base de datos, el nombre de usuario de la base de datos, el host, la contraseña, y se da clic en el botón Instalar Joomla.

Figura 3.48: Configuraciones de la base de datos

En esta instalación existieron problemas cuando se intentó acceder a la página para poder comenzar a realizar las configuraciones en Joomla, aparecía un error, este se daba porque la cantidad de espacio en memoria y disco que se le dío a la máquina virtual eran muy pequeños para los requisitos que utiliza este programa. Ya entrando a Joomla, solicita un registro de usuario y contraseña, así como registrar la base de datos previamente creada en la instalación como se muestra en la figura 3.49, siendo este otro error, ya que no estaba coincidiendo el registro.

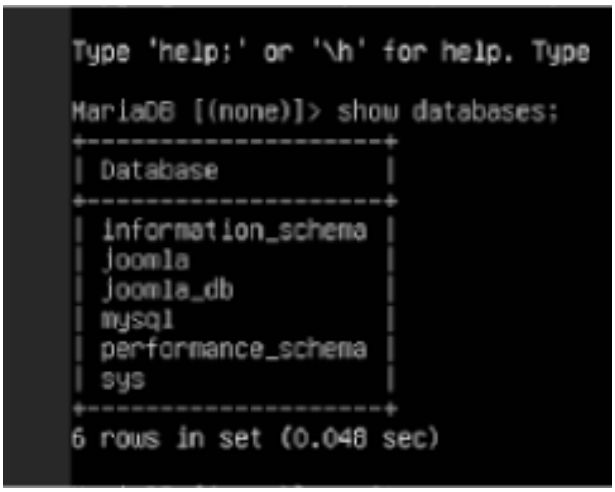

Figura 3.49: Base de datos Joomla

Para acceder al servidor desde otra red, que es el objetivo, se utiliza el redireccionamiento de puertos como se muestra en la figura 3.50, se redirige el tráfico entrante desde la WAN hacia el servidor, esto porque todo el tráfico de la WAN está entrando por la interfaz de Pfsense que tiene una dirección IP que no es la del servidor, se le asigna el puerto 80 que es el que corresponde a HTTP que es el protocolo que se utiliza para cargar la página web.

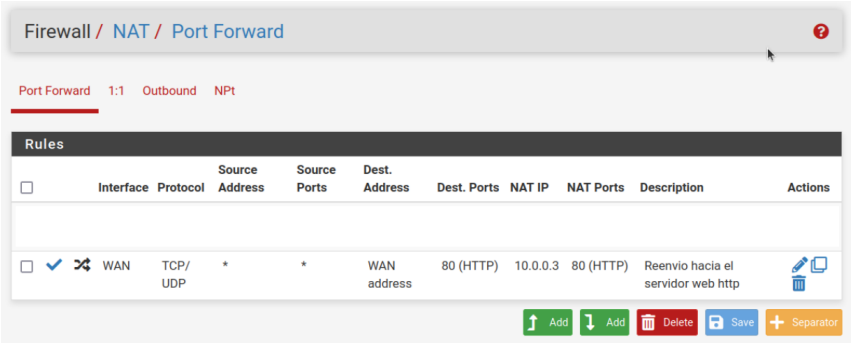

Figura 3.50: NAT para la DMZ

Aún con lo anterior no se lograba tener acceso al servidor, esto causado porque estaban activadas las opciones de Block private networks and loopback addresses y Block bogon network que se muetsran en la figura 3.51, lo que hacen estas opciones es bloquear el tráfico.

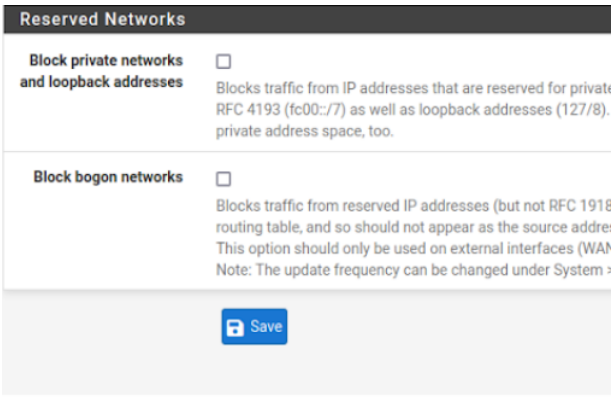

Figura 3.51: Bloqueos de Pfsense

Con el fin de que la MiPyMe pueda contar con una comunicación interna de voz por internet, se le agrega un servidor Asterisk que brinde el servicio de VoIP, dicha instalación se detalla a continuación.

3.8. Servidor Asterisk

3.8.1. Instalación

Para la instalación de Asterisk, se creó una VM en Proxmox con un servidor Ubuntu 22.04, lo primero a realizar es actualizar el servidor con el comando:

```
- apt-get-update
```

Una vez que se realizó la actualización, se procede a la instalación, para esto se ejecuta el comando:

```
- apt-get install asterisk
```

Con el comando:

```
-asterisk -V
```

Se puede ver que versión que se descargo en el servidor, como se puede ver en la figura 3.52.

Figura 3.52: Versión instalada de Asterisk

Para confirmar que el servicio de Asterisk este activo se ejecuta el comando:

- `service asterisk status`

En la figura 3.53 se puede observar que el servicio esta activado.

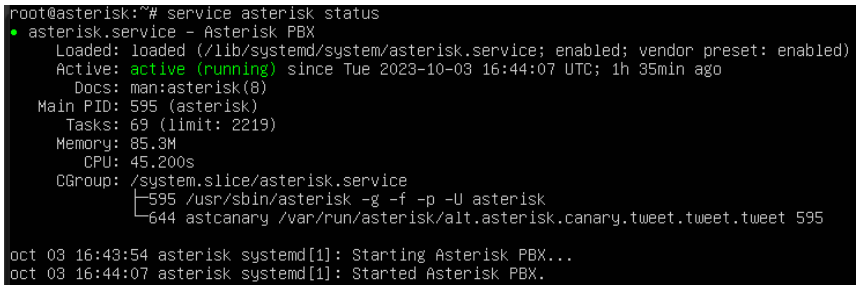

Figura 3.53: Asterisk servicio

3.8.2. Configuraciones

Idioma

Asterisk cuenta con idioma por defecto en inglés, la configuración al español es opcional, para este trabajo se agrega esta configuración por comodidad. Para realizar esto, se ejecuta el comando:

- `apt-get install asterisk.promp-es asterisk-core-sounds-es asterisk-core-sounds-es-gsm asterisk-core-sounds-es-wav asterisk-core-sounds-es-g722`

Con el comando:

- `dpkg -l asterisk*`

Se puede ver los paquetes instalados y así comprobar que se hayan instalado correctamente, en la figura 3.54 se muestran los paquetes instalados.

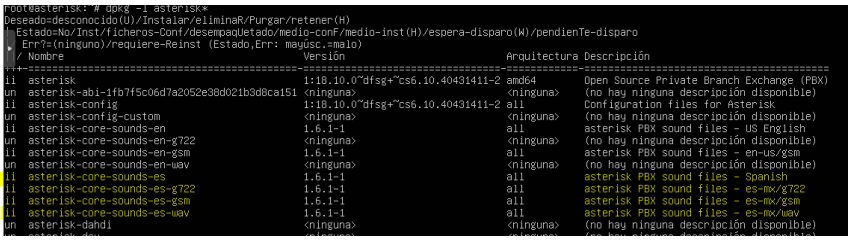

Figura 3.54: Paquetes para idioma en español

Usuarios

Para la configuración de Asterisk, se crean dos usuarios (pc01 y pc02), se entra al archivo sip.conf, con el comando:

- `vi`

Se Ingresa al archivo para agregar los usuarios. Para esto se ejecuta el comando:

- `vi /etc/asterisk/sip.conf`

Una vez dentro, en la parte final del archivo se agrega la información que se muestra en la figura 3.55.

```
[usuario](!)
Type=friend
host=dynamic
context=redesplus

;Extension 101
[ext101](usuario)
username=pc01
secret=s1234
;port=5061

;Extension 102
[ext102](usuario)
username=pc02
secret=s1234
port=5061
```

Figura 3.55: Usuarios agregados

En la figura anterior, se muestra el tipo de usuarios con type=friend esto define que el usuario con esa extensión puede enviar y recibir llamadas. Con host=dynamic se define que el equipo con cualquier IP se podrá registrar como usuario. Entre corchetes se define la extensión,[ext101] y [ext102], lo que se encuentra entre paréntesis esta llamando los parámetros de configuración que se encuentran en las líneas de arriba, (usuario). Se

define el nombre del usuario con username=usuario, con secret=contraseña se define una contraseña para la extensión, esto es necesario para conectar terminales.

Una vez realizadas estas configuraciones, se hace un reload para actualizarlas, con el comando:

```
-service asterisk reload
```

Para confirmar que se hayan agregado los usuarios correctamente, se entra a la consola de Asterisk con el comando:

```
-astersik -rvvv
```

Una vez dentro de la consola, se ejecuta el comando:

```
-sip show users
```

En la figura 3.56, se muestra la información de los usuarios creados.

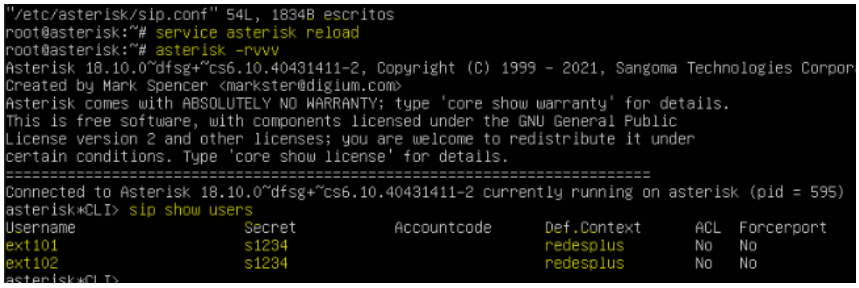

Figura 3.56: Información de los usuarios

El comando:

```
- sip show peers
```

Como se puede observar en la figura 3.57, muestra las extensiones y usuarios, en este caso el host se muestra como unspecified, es decir, no esta especificado aún, porque todavia no hay nadie conectado, en cuanto alguien se conecte, mostrara la dirección IP de ese host.

Figura 3.57: Información de host

Conectando los usuarios

Para conectar los usuarios, se hace uso del software Zoiper, este se instala en dos máquinas virtuales con Ubuntu 20.10 (pc01 y pc02). Estas configuraciones se realizan de la misma forma en ambas máquinas con sus respectivas extensiones.

Una vez que se descargo Zoiper, lo primero que se realiza es seleccionar la pestaña de settings, dentro se elige la opción de create a new account, como se muestra en la figura 3.58.

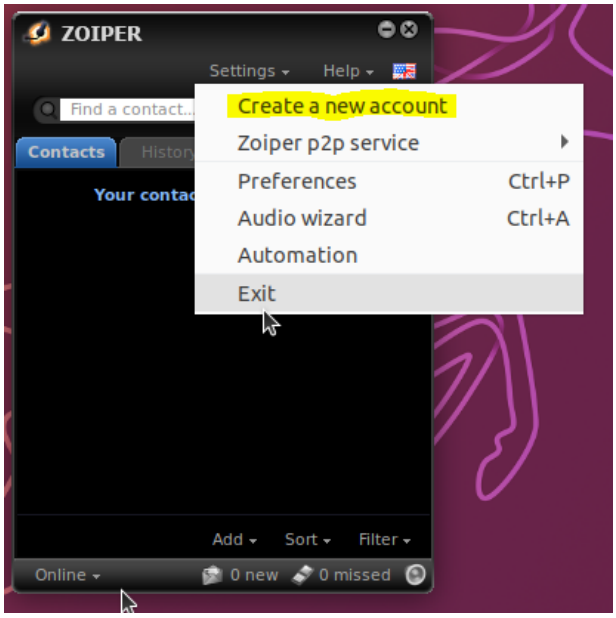

Figura 3.58: Crear cuenta en Zoiper

Se abre una nueva ventana, para elegir el tipo de cuenta, se selecciona la opción de SIP como se muestra en la figura 3.59).

Figura 3.59: Tipo de cuenta

En la siguiente ventana, se agrega el usuario, contraseña e IP del servidor como se muestra en la figura 3.60.

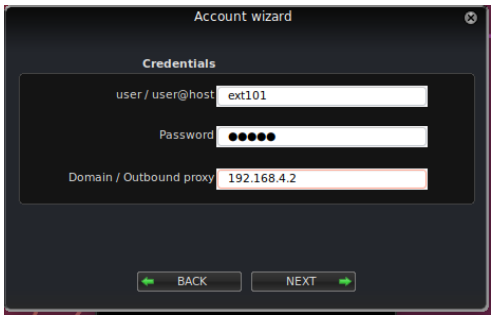

Figura 3.60: Crear credenciales

Finalmente, como se muestra en la igura 3.61 aparecerá el nombre completo de la cuenta y se finaliza.

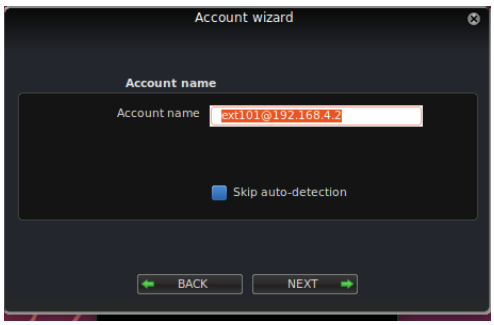

Figura 3.61: Nombre completo de la cuenta

Accediendo al servidor de Asterisk, se notifica que se ha registrado el usuario y la dirección IP del host donde se encuentra como se observa en la figura 3.62)

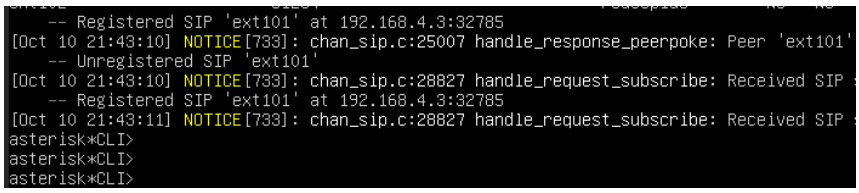

Figura 3.62: Registro del usuario

Una vez registrados los usuarios, lo que sigue es configurar el archivo extensions.conf, este va a definir la forma en que se comportaran las llamadas entrantes y salientes del sistema.

Con el comando nano, se accede al archivo extensions.conf, para configurar el plan de las llamadas como se observa en la figura 3.63.

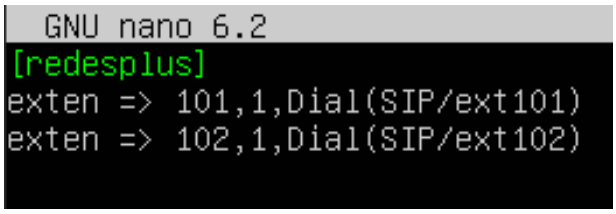

Figura 3.63: Plan de las llamadas

Para que se puedan aplicar las configuraciones, se ejecuta el comando:

```
-dialplan reload
```

Con todas estas configuraciones ya se podrá realizar llamadas entre los usuarios.

Para el servicio de WiFi se agrega un modem que permita conectar equipos inalámbricos a la red, este se debe configurar en modo puente para que se pueda administrar con Pfsense; esta configuración se muestra a continuación.

3.9. Access Point

Para realizar la configuración del Access Point, se utiliza un router linksys wrt 1900 ac, se formatea el dispositivo, para posteriormente acceder desde un navegador web a la dirección IP “192.168.1.”, o escribir “https://myrouter.local”, se ingresa la contraseña predeterminada del AP, que es “admin” para iniciar sesión. Una vez que se ingreso, pide asignarle un nombre y contraseña a cada banda como se observa en la figura 3.64.

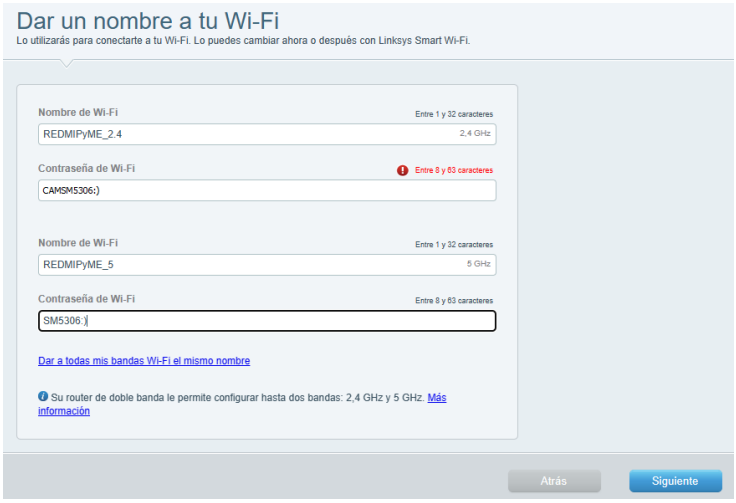

Figura 3.64: Asignación de nombre y contraseña a cada banda

Posteriormente pide crear una contraseña para el router, esto va a permitir acceder a

las configuraciones del Access Point como se muestra en la figura 3.65.

Figura 3.65: Asignación de nombre del router

Es importante mencionar que el Access Point opera en modo puente para que la red WiFi sea gestionada por el firewall PfSense. Además, la banda de 2.4 GHz se mantiene oculta, ya que en ella se conectan las cámaras, y se desea restringir el acceso a estas a los usuarios de la red WiFi.

3.10. Switch

El propósito del uso de un switch es conectar una mayor cantidad de dispositivos a la red, ya que el servidor por sí solo no es suficiente para conectar todos los dispositivos que utiliza una MiPyMe. Además se pueden crear VLAN para que se pueda segmentar la red.

En este caso, la red que se está implementando se divide en 2 VLAN, la primera es la red local, a la que se pueden conectar los equipos de los empleados de la MiPyMe, la segunda VLAN es de administración, a esta únicamente tendrán acceso los administradores de la red. Estas VLANs tienen el identificador 24 y 10, respectivamente.

Para crear las VLAN mencionadas anteriormente, se debe ingresar a las configuraciones del switch por medio de un cable de consola e ingresando las credenciales para tener acceso, una vez que se logra la conexión se ingresan los comando para la creación de las VLAN, ejecutando los siguiente comandos:

```
 - create vlan Red_Admin tag 10

- create vlan Red_Lan tag 24
```

Para asociarlos a las interfaces, se colocan los siguiente comandos:

- `configure Red_Admin add ports 1, 2 untagged`

- `configure Red_Lan add ports 3, 4, 5, 6, 7 untagged`

Para que Pfsense pueda administrar las VLANs creadas en el switch, es necesario crearlas también en el Firewall. Se crean en la sección de Interfaces, y después en VLANs, se observa un botón de "Add", en cual se dan de alta los IDVlan 10 y 24. En la figura 3.66 se observa la configuración para la VLAN 24, colocando la interface por la cual se va a conectar, en este caso es la LAN, su prioridad, ID y una descripción. En la figura 3.67), se muestra la configuración de la VLAN 10.

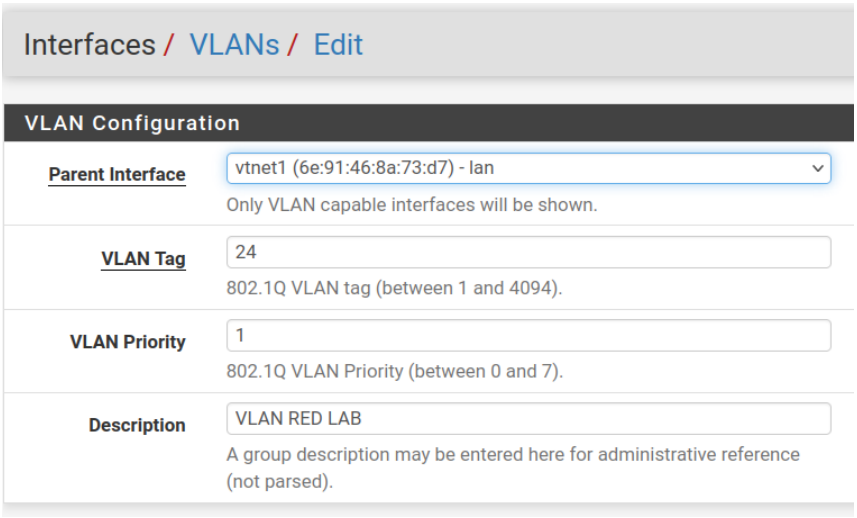

Figura 3.66: Creación VLAN 24

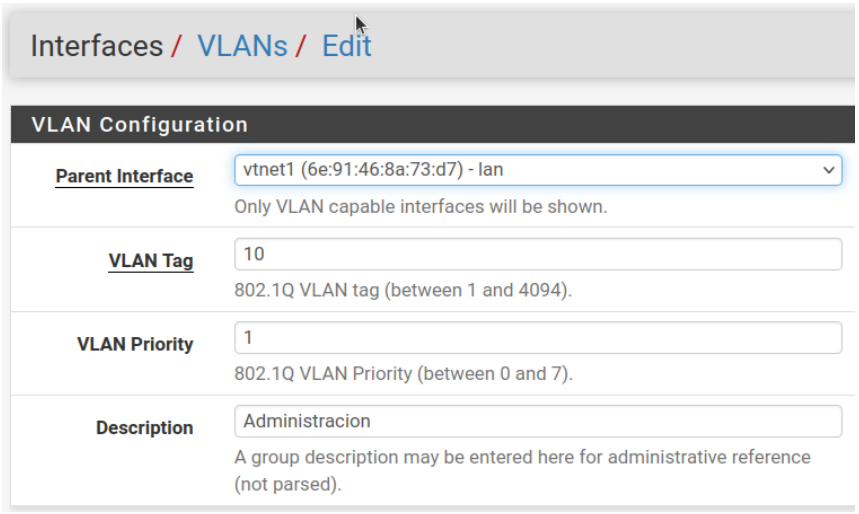

Figura 3.67: Creación VLAN 10

Con la creación de las VLAN se permite una escalabilidad en la red, esto pensando en que pueda existir un crecimiento en la MiPyMe. Una vez creadas las VLANs en el swtich, se necesita ocupar una interfaz diferente, la cual va a ser en donde se conecte el servidor, y donde se creará la troncal. El crear este enlace permitirá el paso de datos de las VLANs sobre un mismo cable. Para esto, se van a etiquetar las VLAN 10 y 24 en el switch. Las VLAN etiquetadas permiten que los puertos de acceso del conmutador manejen más de una VLAN y separe el tráfico [22]. Por eso es importante, etiquetar las VLANs tanto en el switch, como en el Firewall. Los siguientes comandos muestran cómo se etiquetan las vlans creadas en una interfaz diferentes, esto para poder crear la troncal.

- configure vlan Red_Admin add port 24 tagged

- configure vlan Red_Lan add port 24 tagged

Capítulo 4

Análisis de resultados

A continuación se muestran los resultados obtenido de la implementación de esta propuesta de seguridad, se realizan pruebas para confirmar su funcionalidad, esto con el fin de comprobar que se haya realizado la instalación de forma correcta.

4.1. Pfsense

La instalación de PfSense permite ofrecer el servicio de un firewall de forma gratuita, con una amplia variedad de configuraciones disponibles. A continuación, se describen algunos de los elementos que se pueden visualizar en el menú principal o dashboard.

En la figura 4.1, se muestra información del sistema, cosas relevantes que se pueden observar en esta sección es la versión instalada, el vendor, cantidad de memoria usada, porcentaje de CPU usado. Estos últimos indicadores son útiles para evaluar el rendimiento y llevar un monitoreo continuo del firewall.

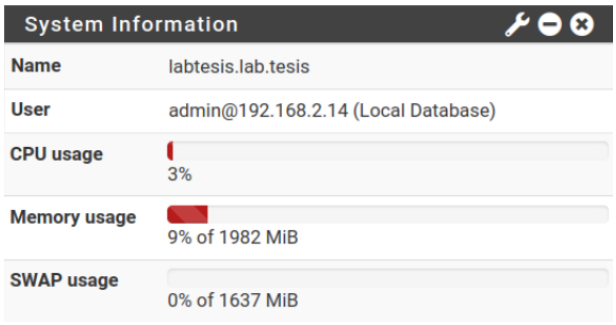

Figura 4.1: Información del sistema

En la figura 4.2, se observan todas las interfaces que fueron agregadas en el Firewall.

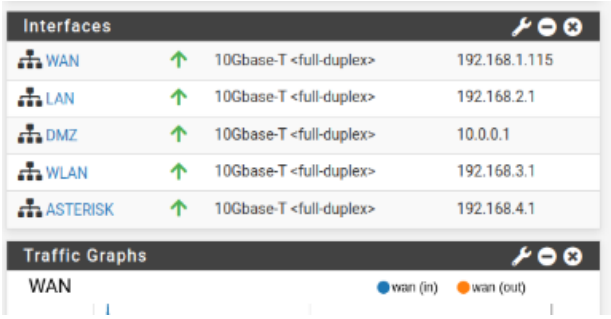

Figura 4.2: Interfaces

En la figura 4.3 se muestran gráficos que proporcionan información sobre el tráfico en cada interfaz de red conectada a PfSense. Estos gráficos ofrecen una visión del estado y uso de la red, permitiendo una administración eficiente y una respuesta rápida a posibles problemas.

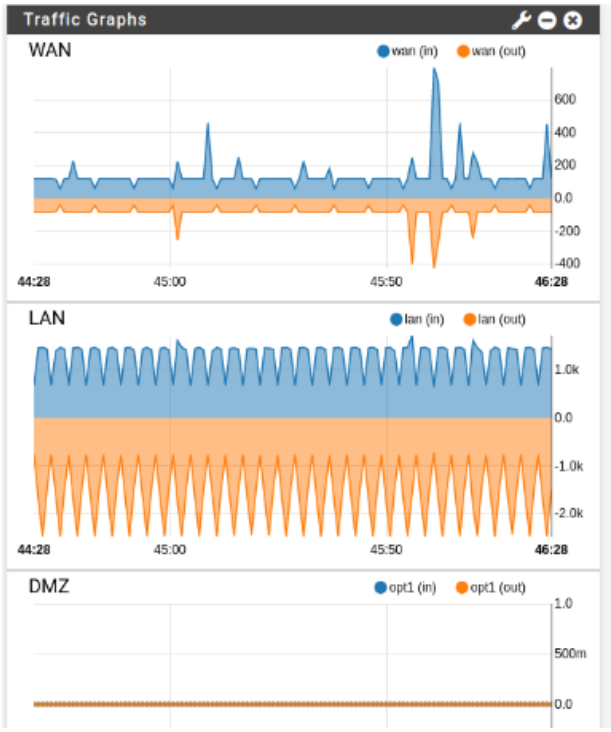

Figura 4.3: Gráficos del tráfico

En las figuras anteriores se muestra información, que permitirá llevar a cabo un análisis de los recursos utilizados, gráficas del tráfico y demás elementos que npermiten realizar un monitoreo de la red. Este menú puede ser configurado, permitiendo agregar widgets como el de estado real de las interfaces de red, el de OpenVPN e IPsec, logs del Firewall y muchos otros más, se puede adaptar a las necesidades de la red, para que pueda ser observado todo a la vez.

Pfsense también cuenta con una gran cantidad de Opciones para su configuración, que son de gran ayuda al momento de administrar la seguridad de la red, en la tabla 4.1 se muestran las funciones que permite configurar Pfsense y que antes de este trabajo no estaban implementadas o actualizadas. Es importante destacar que, aunque la funcionalidad de VPN no se implementa en este trabajo, se considera una línea de desarrollo futuro para mejorar la propuesta presentada.

Sección	Utilidad
System	Se encuentran todos los elementos que están directamente relacionados con la administración del Firewall.
Interfaces	Permite habilitar y asignar las interfaces que se conectarán al Firewall, también muestra las que ya están habilitadas y realizar configuraciones
Firewall	Permite configurar todas las reglas para el Firewall
Services	Se encuentran disponibles todos los servicios que tiene por defecto Pfsense
VPN	Permite crear VPN, este software soporta la mayoría de los protocolos de VPN
Status	Permite ver el estado global de Firewall y sus servicios
Diagnostics	Contiene varias herramientas que permiten ver información para realizar troubleshooting

Tabla 4.1: Funciones a ocupar de PFsense

Finalmente, se encuentran las reglas, que son fundamentales, ya que determinan si se permite o niega el acceso a la red. Cada interfaz tiene sus propias reglas. Las siguientes figuras muestran los resultados de estas configuraciones.

La figura 4.4 muestra las reglas en la WAN, esta configurada para que permita conexiones entrantes HTTP y HTTPS hacia el servidor web, mientras que el resto del tráfico que no se ajuste a esas reglas es bloqueado por defecto. Esto proporciona acceso controlado desde la red externa (WAN) a ciertos servicios en la red interna, manteniendo la seguridad al restringir otros tipos de tráfico.

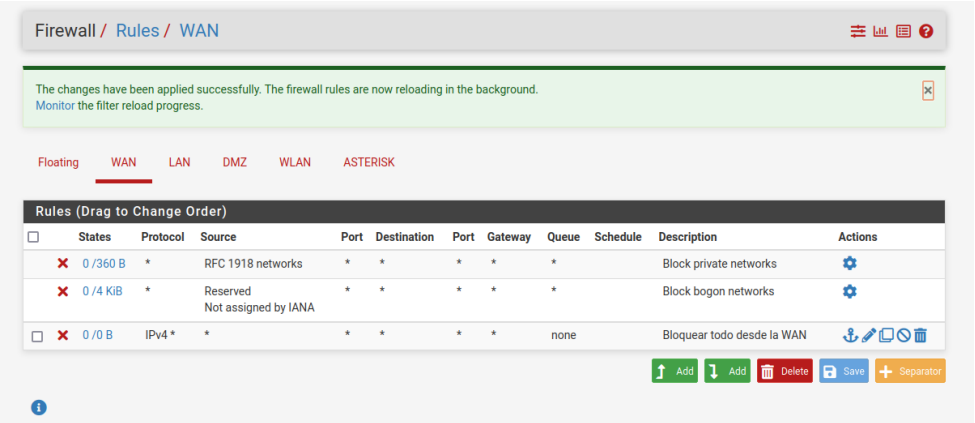

Figura 4.4: Reglas en WAN

La figura 4.5 se muestran las reglas que se aplican en la red LAN. Su configuración evita el bloqueo accidental del administrador al acceder al firewall desde la red LAN y permite tráfico hacia la dirección LAN del firewall en el puerto 7443. Estas reglas aseguran el acceso del administrador, y permiten el tráfico necesario para que los dispositivos dentro de la LAN se comuniquen sin restricciones.

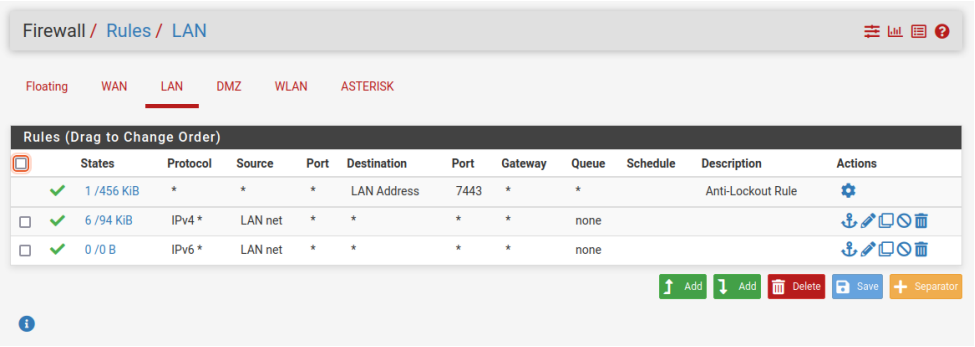

Figura 4.5: Reglas en LAN

La figura 4.6 muestra las reglas en la DMZ, esta configuración segmenta la DMZ de otras redes internas (LAN, ASTERISK y WLAN), mientras que permite el acceso desde cualquier red hacia la DMZ y desde la DMZ hacia Internet. Esto proporciona un aislamiento efectivo, protegiendo la red interna al permitir únicamente el tráfico necesario hacia y desde la DMZ.

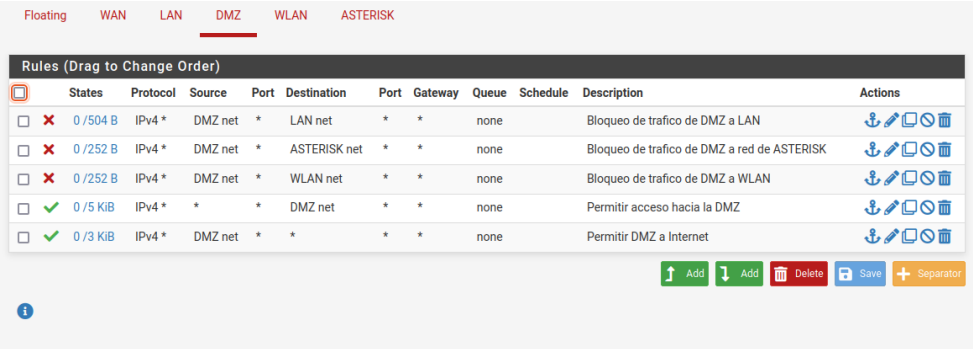

Figura 4.6: Reglas en DMZ

La figura 4.7 muestra las reglas en la WLAN, estas reglas permiten el tráfico necesario para que los dispositivos dentro de la WLAN se comuniquen sin restricciones.

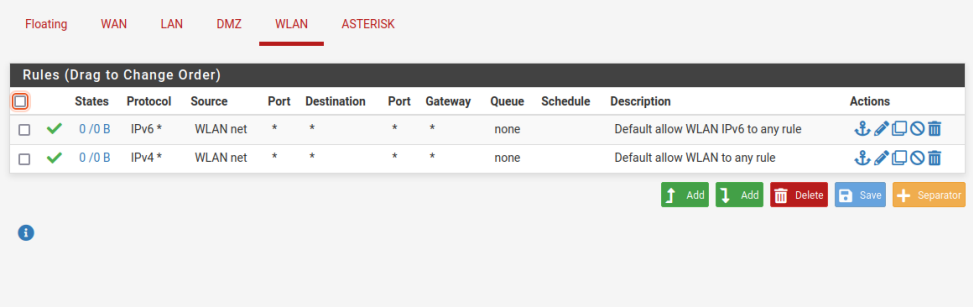

Figura 4.7: Reglas en WLAN

La figura 4.8 muestra las reglas en ASTERISK estas reglas permiten el tráfico necesario para que los dispositivos dentro de la red se comuniquen sin restricciones.

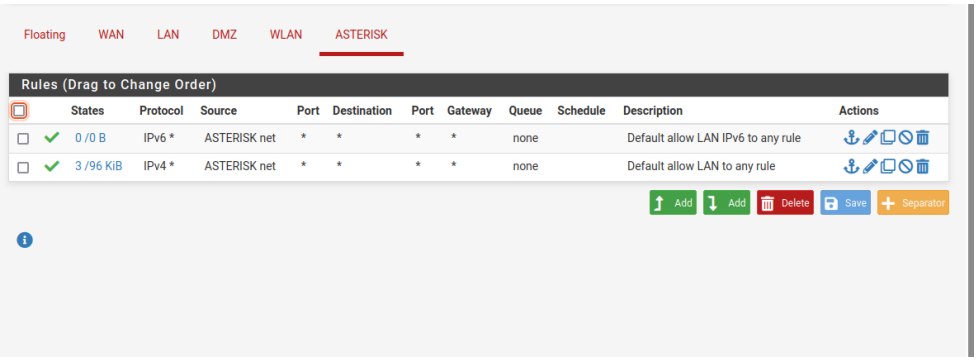

Figura 4.8: Reglas en ASTERISK

En las siguientes figuras se muestran las pruebas de flujo de tráfico realizadas mediante el envio de pings desde las distintas interfaces, para comprobar que las reglas se están aplicando correctamente.

La figura 4.9 muestra el flujo desde la LAN hacia la DMZ, realizado por el envío de pings

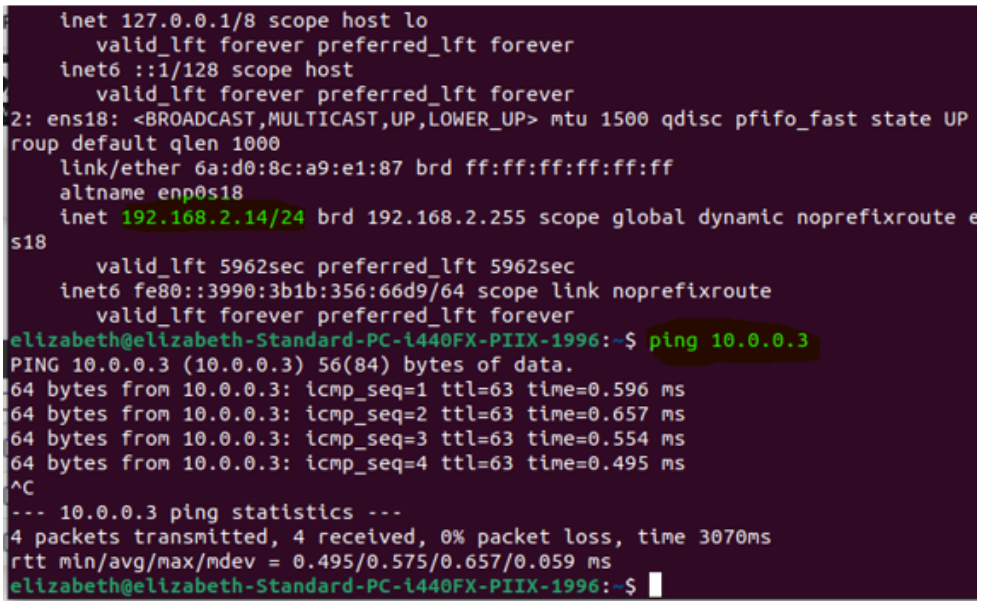

Figura 4.9: Ping desde la LAN hacia la DMZ

La figura 4.10 muestra el flujo desde la DMZ hacia distintas interfaces de la LAN, realizado por el envío de pings.

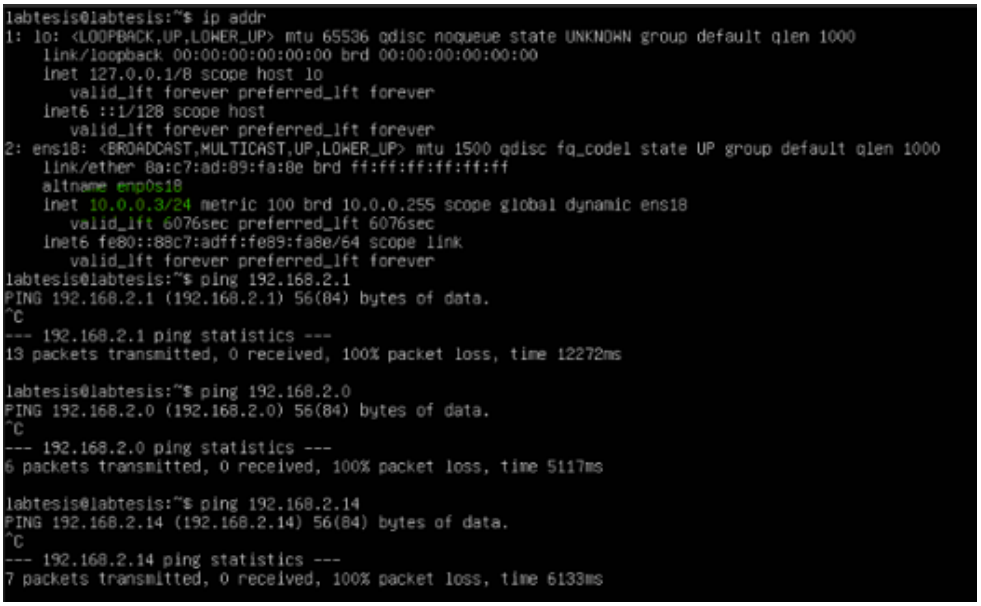

Figura 4.10: Ping desde la DMZ hacia la LAN

La figura 4.11 muestra el flujo desde la DMZ hacia la interfaz de ASTERISK, realizado por el envío de pings.

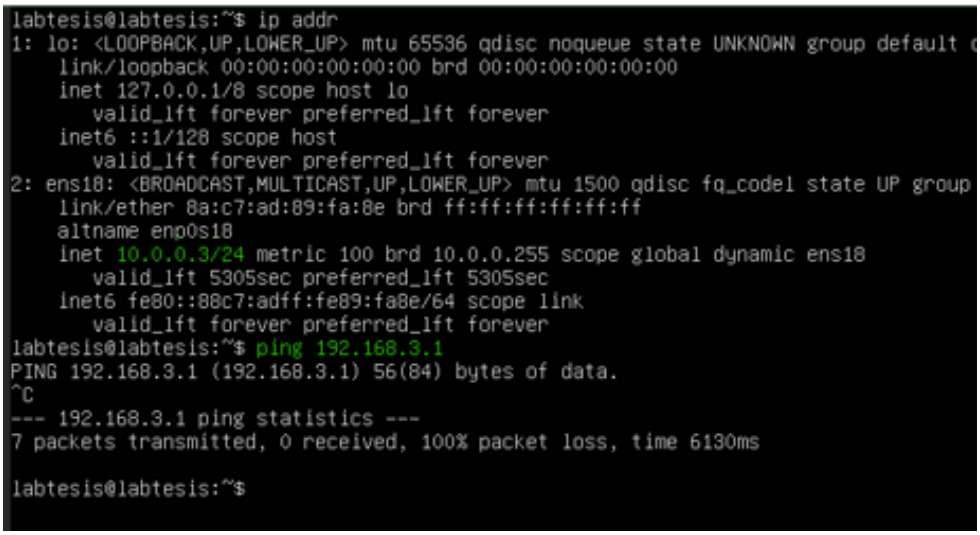

Figura 4.11: Ping desde la DMZ hacia la WLAN

La figura 4.12 muestra el flujo desde la DMZ hacia la interfaz de ASTERISK, realizado por el envío de pings.

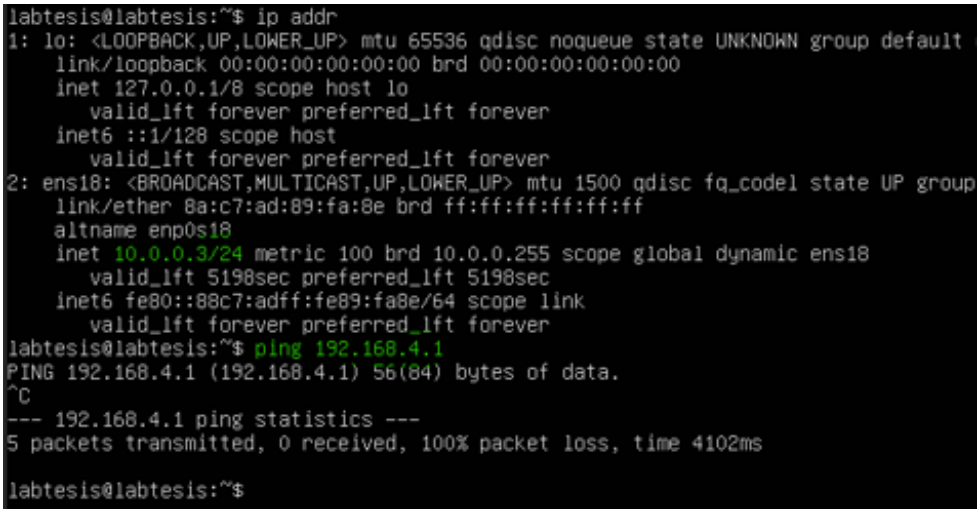

Figura 4.12: Ping desde la DMZ hacia ASTERISK

La figura 4.13 muestra el Flujo desde un equipos conectado a red ASTERISK hacia la DMZ, realizado por el envío de pings.

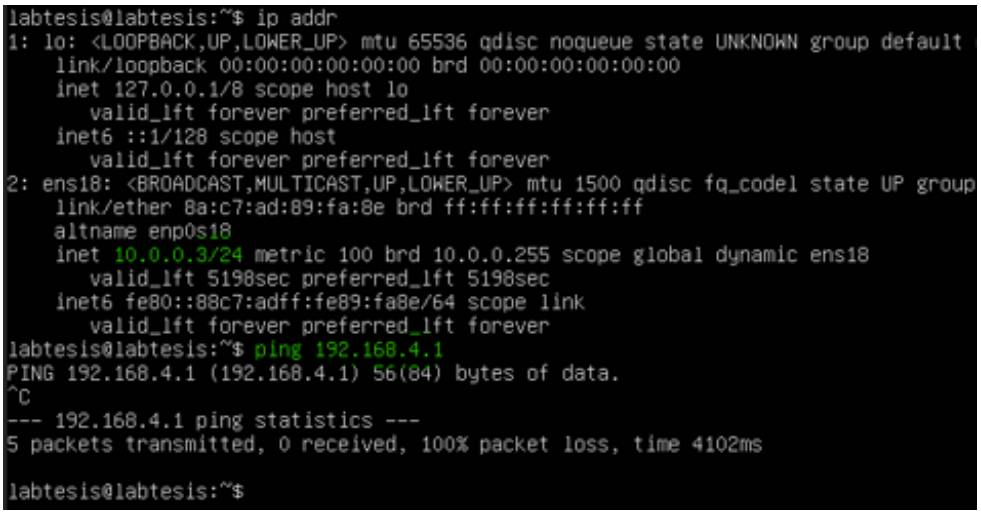

Figura 4.13: Ping desde ASTERISK hacia la DMZ

4.2. Proxmox

Finalizada toda la instalación de Proxmox, desde la interfaz web se pueden ver todas las máquinas virtuales creadas para la configuración de la red, como se puede observar en la figura 4.14

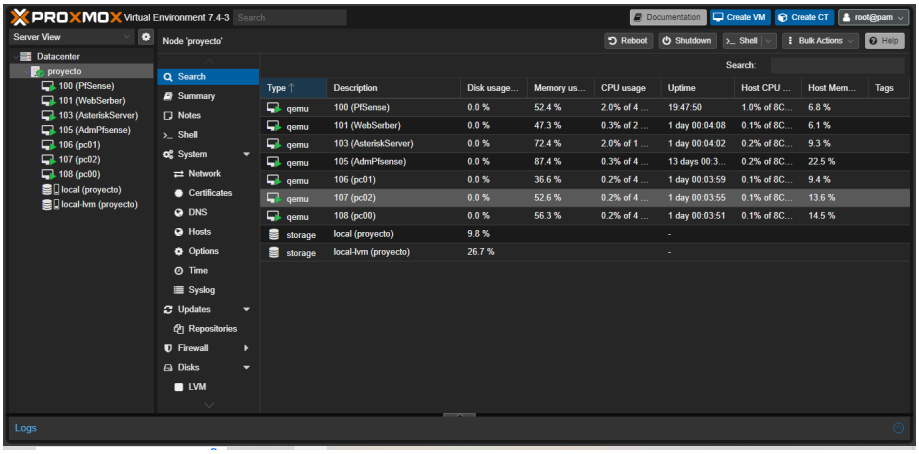

Figura 4.14: Máquinas creadas en Proxmox

Además, se pueden observar todas las interfaces físicas y virtuales existentes y se muestra su estado, es decir, si estas están activas o no.

En la figura 4.15, se puede ver a qué red corresponde cada interfaz y a qué interfaz física está conectada cada interfaz virtual.

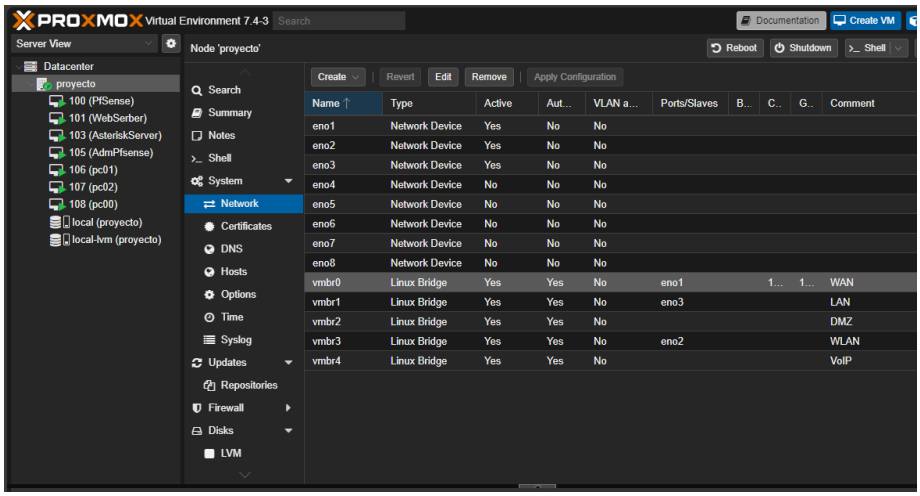

Figura 4.15: Interfaces totales

También, Proxmox cuenta con gráficos e información sobre el cpu, memoria, tráfico en la red y tiempo de actividad.

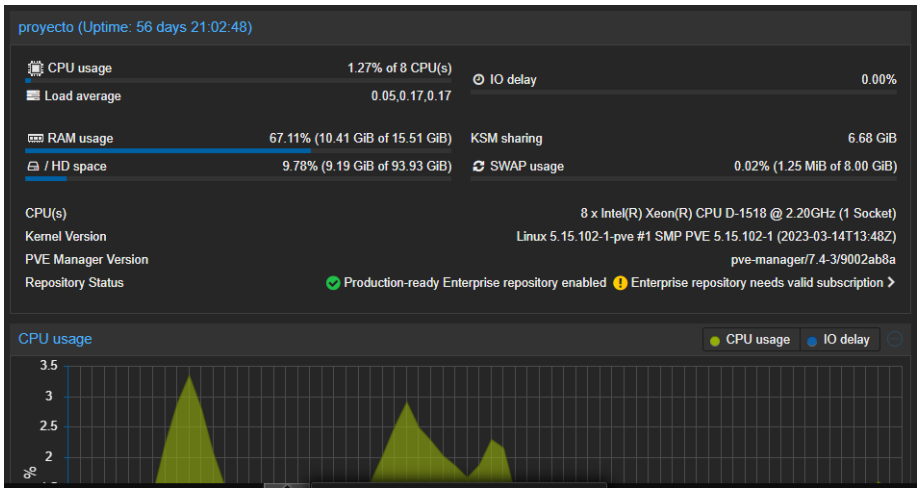

Figura 4.16: Resumen de Proxmox

Esta información es muy importante para llevar a cabo un monitoreo del estado en que se encuentra el servidor con Proxmox.

4.3. Servidor

Con la instalación de APACHE que se muestra en la figura 4.17, se permite utilizar la DMZ como un servidor web, el cual puede servir como plataforma para blogs, sitios de comercio electrónico y todo tipo de aplicaciones web que deseé tener ahí la empresa.

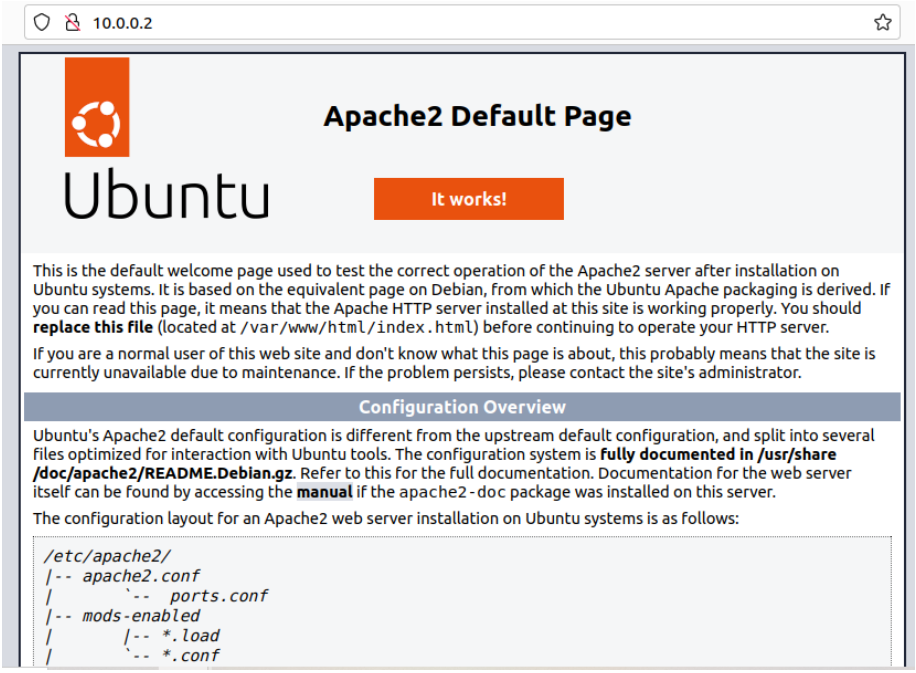

Figura 4.17: APACHE

Adicionalmente, como se observa en la figura 4.18 se instaló Joomla que es una herramienta que permite gestionar con mucha facilidad un sitio web, ayuda a que se realice con rapidez y sin tener muchos conocimientos técnicos.

Figura 4.18: Joomla

Para administrar la página web con Joomla se creo un usuario con su respectiva contraseña para poder acceder, en la figura 4.19 se muestra la interfaz para acceder con las credenciales a Joomla.

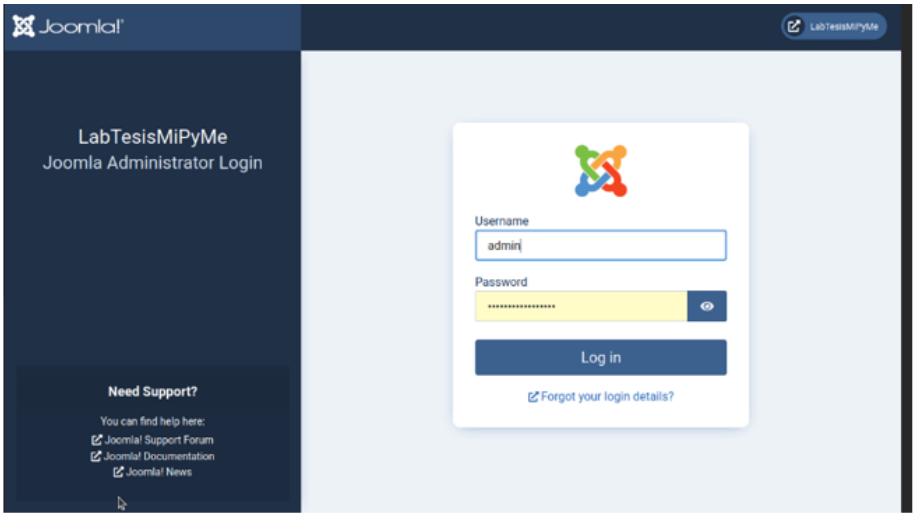

Figura 4.19: Acceso a Joomla

Una vez dentro de Joomla se pueden iniciar con la administración de la página web, esta se deja sin realizar cambios como se puede ver en la figura 4.20

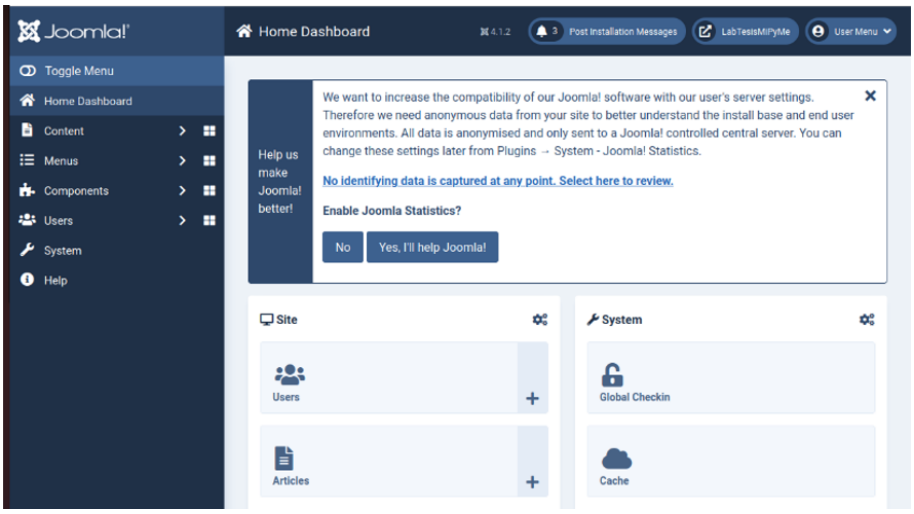

Figura 4.20: Inicio Joomla

4.4. Asterisk

Con Asterisk se está adicionando el servicio de VoIP a este proyecto, este software permitirá gestionar llamadas. Cuenta con un contestador automático programable. Permite la

distribución de llamadas entrantes y salientes. También se puede escalar el total de líneas y extensiones.

Para comprobar su buen funcionamiento se realizó una llamada entre dos extensiones creadas, como se muestra en la figura 4.21

Figura 4.21: Llamada en ASTERISK

4.5. Switch

El tener la opción de expandir la red es importante en este tipo de empresas, porque en cualquier momento pueden crecer. La opción de configurar un switch es precisamente el poder conectar más equipos. En este caso se colocó una VLAN de usuarios con el identificador 24, en donde se pueden agregar 5 equipos extra, y un identificador 10 para administración, figura 4.22. Mediante reglas creadas en PfSense, los que se conecten a la VLAN 24, no pueden acceder a otras secciones de la red, simplemente se les está dando acceso a internet. Asimismo, se tienen 2 interfaces para uso administrativo, quien se conecte a la VLAN 10, la cual fue asignada en las interfaces 1 y 2, y si conoce las credenciales, puede tener acceso a las demás secciones de la red.

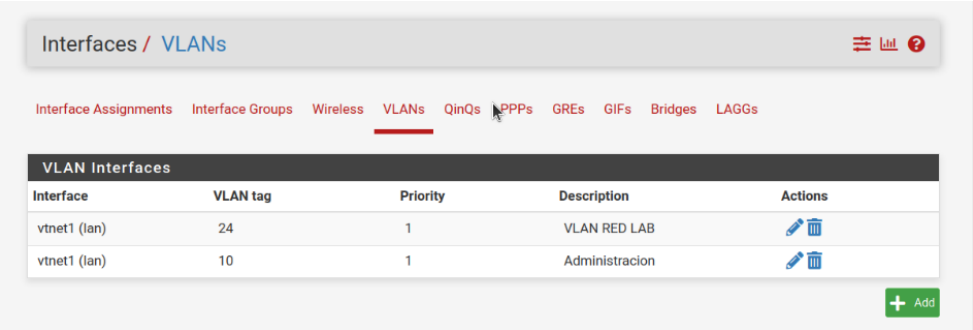

Figura 4.22: VLANs en PfSense

Al agregar este switch, también se tiene una mejor organización, porque no es necesario estar conectándose al servidor cada vez que se requiera monitorear o realizar algún cambio; desde la red de administrador se puede hacer. Y las reglas mencionadas, para que solo los administradores puedan tener acceso al Firewall se muestran en la figura 4.23 , y para la Red LAN en la Figura 4.24

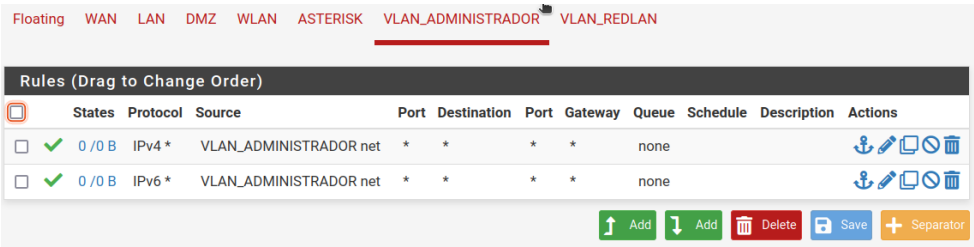

Figura 4.23: Reglas en las VLANs para administrador

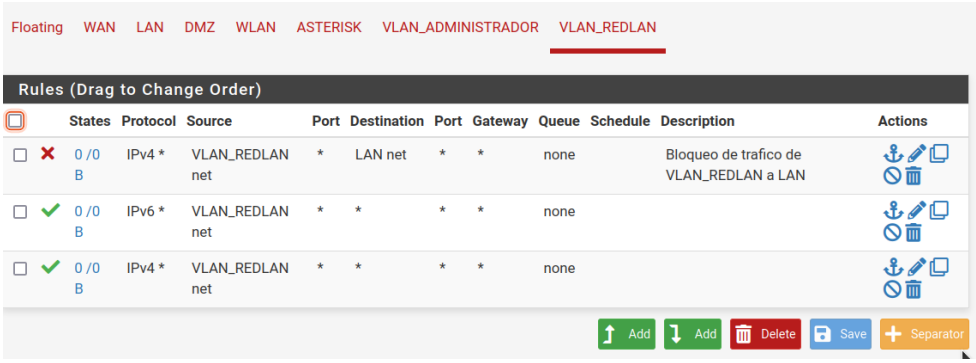

Figura 4.24: Reglas en las VLANs para la LAN

Capítulo 5

Trabajos futuros

A partir de esta implementación se enumeran algunos campos o vias de crecimiento para realizar a partir del presente trabajo, algunos de estos son:

- Integración de sistemas de detección de intrusos (IDS) e Integración de sistema de prevención de intrusos (IPS)

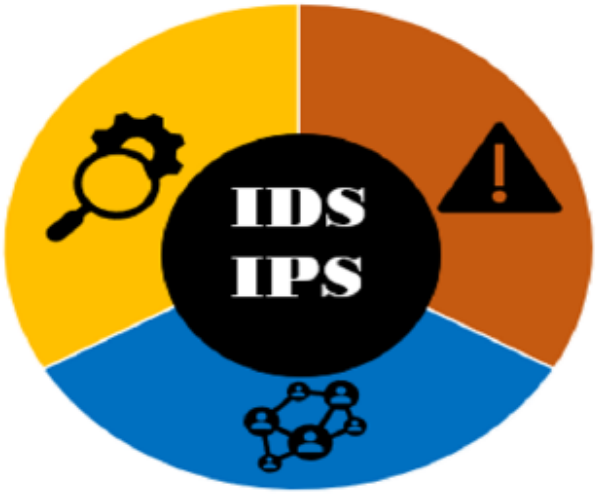

Figura 5.1: IDS & IPS

- Integración de soluciones de acceso remoto seguro con una VPN

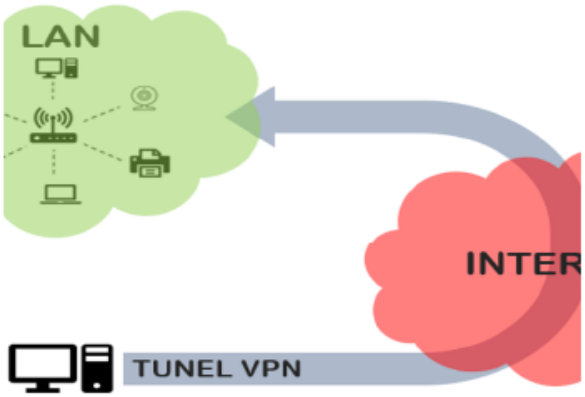

Figura 5.2: VPN

- Integración de Seguridad perimetral de varios niveles

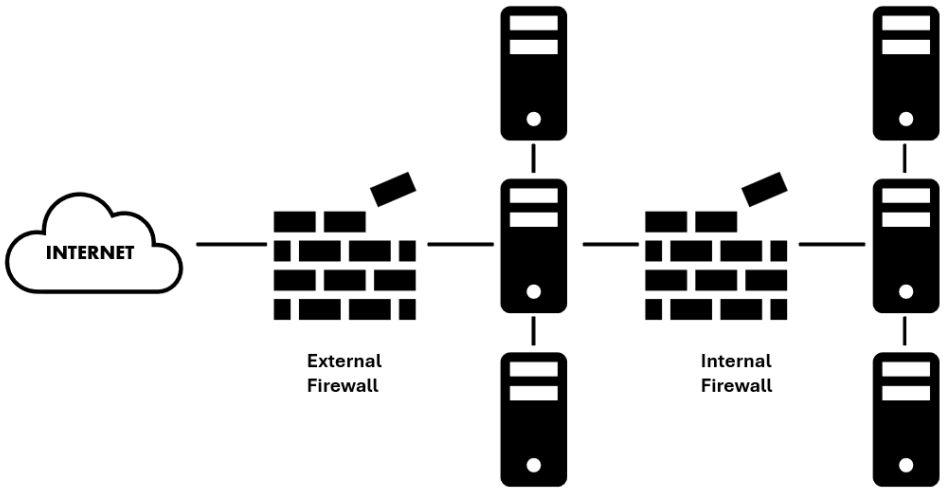

Figura 5.3: Seguridad perimetral de varios niveles

Estas propuestas buscan ampliar y fortalecer la seguridad perimetral en micro, pequeñas y medianas empresas, asegurando una protección integral y adaptada a las necesidades específicas de cada organización.

Capítulo 6

Conclusiones

Esmeralda Elizabeth Chavez Cruz

Con el desarrollo de este trabajo se logra comprender que la brecha de seguridad en las MiPyMes representa un gran desafío, ya que factores como la falta de recursos y conocimiento en seguridad informática afectan en su desarrollo, por esta razón este tipo de empresas se ven muy vulneradas. Para buscar que esta brecha se pueda disminuir, es necesario que se empiecen a adoptar medidas de seguridad que se puedan implementar. Se puede esmpezar por pequeñas acciones que ayuden a que el riesgo de sufrir ataques disminuya.

Una solución son los Firewall de código abierto, a comparación de soluciones propietarias, estos son una respuesta efectiva y viable para las MiPyMes. Con Pfsense se permite implementar medidas de seguridad sin que conlleve costos de licenciamientos, también, gracias a que es de código abierto puede ser personalizado según las necesidades que se tengan. Aunque, cabe destacar que es importante que se cuente con personal capacitado para gestionar y mantener el sistema, para que se garantice su configuración y actualización adecuada.

Con la virtualización de redes en las MiPyMes se tiene un estrategia beneficiosa, con esto se puede reducir sus costos de hardware, ya que se disminuye la necesidad de equipos físicos y su mantenimiento. Con ProxMox se puede utilizar de forma eficiente los recursos existentes, ayudando a que exista una reducción de espacio físico para los equipos de la red y también se puede tener una gestión y monitoreo centralizado. Por último, va a permitir una mayor agilidad y rapidez en la implementación de aplicaciones y servicios, como por ejemplo agregar servicios de voz, de servidor web, cámaras, etc.

Finalmente, todos los conocimientos adquiridos durante la formación universitaria fueron de gran ayuda para adquirir habilidades en áreas como, fundamentos de redes y seguridad informática. Estas bases permitieron entender e identificar errores, diseñar la red, configurar la red e implementar toda esta propuesta. Sin todos estos conocimientos, el

desarrollo de este trabajo hubiera sido imposible y mucho menos su ejecución.

Brian Saldaña Guitierrez

Lo que se propone en este proyecto es un complemento a lo que ya se tiene en cualquier red de alguna empresa en crecimiento, e incluso que apenas esta empezando, es una opción que plantea el reducir gastos para acercarse a tener una red segura, y poder tener una mejor administración de la misma, así como darle forma a lo ya establecido. Es decir, si en un pequeño call center no tiene ningún tipo de ciberseguridad, pero ya cuentan con una infraestructura de red ya establecida, esta propuesta se puede adaptar sin necesidad de realizar cambios muy drásticos.

Con esto, además, se esta entrando en un entorno al cual muchas empresas están apuntando, que es el entorno de virtualización, más empresas están optando por tener un Firewall de forma virtualizada, y aquí se esta mostrando un entorno virtualizado de código abierto, tratando de darla un enfoque más accesible a las MiPyMes. Este proyecto se colocó, de forma funcional en un laboratorio de la UACM San Lorenzo Tezonco, que cumple con los criterios de una peque{na empresa, y sin duda podría implementarse en alguna tienda, barbería, o hasta en locales que se encuentren en peque{nas plazas.

El juntar un Firewall y Asterisk, y de esta forma poder crear redes LAN, DMZ, canales voz, administrar cámaras de seguridad, redes WiFi, en un solo servidor PROXMOX, permite que se pueda crecer hasta donde la empresa lo necesite, o reducirse si así es el caso, de una forma sencilla y transparente. Teniendo en cuenta que se utilizó software OpenSourse, nos permitió probar varios Firewall para poder seleccionar uno que estuviera completo y fácil de usar, en donde si se tiene algún problema se pueda encontrar la solución, o aclarar alguna duda, dentro de algún foro en internet.

Bibliografía

[1] D. H, "Empresas, principal objetivo de ciberataques en américa latina," 2020. [Online]. Available: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

[2] ESET, "Eset security report latam 2020," 2020. [Online]. Available: https://empresas.eset-la.com/novedad/eset-security-report-2020

[3] IFT, "Cuarta encuesta 2019 usuarios de servicios de telecomunicaciones micro, pequeñas y medianas empresas," 2019. [Online]. Available: https://www.efdeportes.com/efd179/modelos-teoricos-de-la-comunicacion.htm

[4] G. E.C., "Modelos de comunicación," 2013. [Online]. Available: https://www.efdeportes.com/efd179/modelos-teoricos-de-la-comunicacion.htm

[5] A. S. and T. D. J., *Redes de computadoras*. Pearson, 2012.

[6] P. Gil., J. Pomares, and F. Candelas, *Redes y Transmisión de Datos*. TextosDocentes, 2010.

[7] R. L. Alcamí, B. F. Julián, A. P. Denia, and L. M. Cháfer, *Introducción a la gestión de sistemas de información en las empresas*. Sapientia, 2021.

[8] G. Baca Urbina, *Introducción a la seguridad informática*. Patria, 2016.

[9] K. Kurose and J. F. Ross, *REDES DE COMPUTADORAS: UN ENFOQUE DESCENDENTE*. Pearson, 2017.

[10] R. Castro, F. Moran, V. Navarrete, A. Cruzzaty, P. Anzules, A. Mero, M. Quimiz, C. Merino, and Martha, *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Alicante, 2018.

[11] A. P. Palacios, *Seguridad informática*. Paraninfo, 2020.

[12] Valio, "Ventajas y desventajas del código abierto," 2022. [Online]. Available: https://es.linkedin.com/pulse/ventajas-y-desventajas-del-c%C3%B3digo-abierto-valio-spa

[13] Callegari, *Firewall / Cortafuegos*, 2008.

[14] smoothwall.org, "Smoothwall solutions?" [Online]. Available: https://smoothwall.org/about.html#accordion01-i

[15] J. A. Carballar, *VoIP La telefonia de internet.* Thomson, 2008.

[16] M. IP, "Qué es asterisk y cómo funciona: características, servicios y por qué lo necesitas," 2018. [Online]. Available: https://www.masip.es/blog/que-es-asterisk/

[17] PROXMOX, "Proxmox." [Online]. Available: https://www.proxmox.com/en/proxmox-virtual-environment/requirements

[18] Tecnozero, "Tecnozero." [Online]. Available: https://www.tecnozero.com/vmware/proxmox-vs-vmware/

[19] A. Ernesto, *REDES CISCO. Guía de estudio para la certificacion CCNA Routing y Switching.* RaMa, 2020.

[20] openvswitch.org, "Production quality, multilayer open virtual switch," 2016. [Online]. Available: https://www.openvswitch.org/

[21] U. Electronics, "Unit electronics." [Online]. Available: https://uelectronics.com/producto/esp32-38-pines-esp-wroom-32/?srsltid=AfmBOor_xmDt6-WWtRFTj2TmQREUjZ9AjAIbPHe8cHgsxpq8Jon3jtDD

[22] K. Kinzer, "Untagged vs. tagged vlan: What's the difference?" 2022. [Online]. Available: https://jumpcloud.com/blog/untagged-vs-tagged-vlan