UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

REPORTE FINAL DE ESTADÍA

Cid Olmedo José Guadalupe

Implementación del firewall pfSense+ en la infraestructura de red de la UTCV

EDUCACIÓN SECRETARÍA DE EDUCACIÓN PÚBLICA
UTP COORDINACIÓN GENERAL DE UNIVERSIDADES TECNOLÓGICAS Y POLITÉCNICAS
VERACRUZ GOBIERNO DEL ESTADO
SEV Secretaría de Educación
DET Dirección de Educación Tecnológica del Estado de Veracruz
SEMSyS Subsecretaría de Educación Media Superior y Superior

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

Técnico Superior Universitario en Tecnologías de la Información Área Infraestructura de Redes Digitales

“Implementación del firewall pfSense+ en la infraestructura de red de la UTCV”

REPORTE FINAL DE ESTADÍA

QUE PARA OBTENER EL GRADO ACADÉMICO DE:

TÉCNICO SUPERIOR UNIVERSITARIO EN TECNOLOGÍAS DE LA INFORMACION ÁREA INFRAESTRUCTURA DE REDES DIGITALES

José Guadalupe Cid Olmedo

ASESOR ACADÉMICO: PhD. Luis Rolando Guarneros Nolasco

ASESOR INDUSTRIAL: ISC. Michel Orozco Carrera

CUITLÁHUAC, VER. AGOSTO, 2023

Agradecimientos

En primer lugar, quiero agradecer a Dios por permitirme cumplir con una meta más en mi vida personal y académica gozando de salud y bienestar.

Gracias a mi madre Hortencia Olmedo Pérez por su apoyo, disciplina y cariño incondicional durante esta etapa en mi vida, por siempre buscar darme lo mejor siempre para cumplir cada una de mis metas, y por enseñarme que, aunque la vida te tire, siempre te puedes levantar.

A mi padre José Gerardo Polonio Cid Hernández por darme su cariño y apoyo, por su amor, valores que me inculcó. Le agradezco por enseñarme que no importa de donde vengas porque siempre puedes lograr lo que te propongas y que dios en un gran apoyo siempre que lo necesites.

Gracias a mi hermano Luis Ángel Cid Olmedo por estar conmigo cuando mis padres no podían, por cuidarme cuando estaba en una etapa temprana de mi vida, por apoyarme cuando lo necesitaba y por brindarme si cariño de hermano.

Finalmente, gracias a mi novia Aleyda Denisse Juárez Flores, por su amor, apoyo y comprensión en los buenos y malos momentos, por estar conmigo a pesar de las dificultades y sobre todo por brindarme una palabra de aliento cuando lo necesitaba.

Resumen

Este proyecto surge como respuesta a la necesidad de mejorar la seguridad, gestionar el tráfico de datos y gestionar el acceso a sitios web en la infraestructura de red de la institución de la UTCV, en Cuitláhuac, Ver. La propuesta consistió en implementar el firewall pfSense+ para garantizar un acceso seguro y controlado a los recursos en línea. Mediante la metodología PPDIOO, se analizaron requerimientos, se configuró el firewall, se establecieron políticas de filtrado web, se limitaron anchos de banda y se crearon reglas entre VLANS. Los resultados fueron notables: la red se volvió más segura y eficiente, beneficiando a alumnos, docentes, administrativos y el área de rectoría. La experiencia de navegación mejoró y el rendimiento general de la red se optimizó. Este proyecto brindó una solución efectiva para fortalecer la seguridad y optimizar el tráfico de datos en la red educativa de la UTCV, generando un entorno de trabajo y estudio más seguro y productivo para la comunidad educativa.

Palabras clave: firewall, pfSense+, VLAN, VLANS.

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

Índice

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

Índice de figuras

Índice de tablas

CAPÍTULO I. INTRODUCCIÓN

1. Introducción

Durante la era digital, donde la información fluye constantemente a través de la red, la protección de los datos y la salvaguarda de la privacidad se convierten en aspectos fundamentales para el desarrollo y funcionamiento adecuado de cualquier institución. La presencia de múltiples dispositivos conectados y la constante interacción con recursos en línea exponen a las redes educativas a diversas amenazas y vulnerabilidades, lo que implica la necesidad de contar con un robusto sistema de seguridad.

La “Implementación del firewall pfSense+ dentro de la infraestructura de red de la UTCV” busca solventar la necesidad de fortalecer la seguridad y el control del tráfico de datos en su entorno educativo y sitios web de la red. La creciente dependencia de la tecnología en el ámbito educativo ha impulsado la necesidad de adoptar soluciones avanzadas que aseguren una navegación segura y protegida para docentes, alumnos, personal administrativo, personal del área de rectoría e invitados de la institución.

Esta investigación se enfoca en detallar los pasos llevados a cabo para configurar el firewall pfSense+ haciendo uso de la metodología PPDIOO para tener el control de cada actividad requerida a lo largo de la implementación; con la finalidad poseer un firewall óptimo y personalizado para la UTCV, tomando en consideración las necesidades específicas de los usuarios y las políticas de la institución.

El presente trabajo se estructura en cuatro capítulos secuenciales. En primer lugar, la "Introducción" la cual se enfoca en una investigación científica sobre el objeto de estudio, considerando antecedentes relevantes que ayuden a reconocer el proyecto. El segundo capítulo, la "Metodología", se centra en los pasos a seguir para la implementación del proyecto, basándose en los alcances, objetivos y haciendo uso de instrumentos de investigación para establecer los entregables de cada fase. El tercer capítulo, "Desarrollo del proyecto", integra las actividades siguiendo la metodología

PPDIOO, proporcionando un análisis detallado de lo realizado en cada fase durante la implementación. Por último, en el cuarto capítulo "Resultados y Conclusiones", presenta las contribuciones obtenidas a través de una recapitulación de todo lo abordado en el desarrollo del proyecto.

1.1 Estado del arte

Las redes inalámbricas en la actualidad tienen un papel fundamental tanto en las universidades como en diversos entornos. En el caso específico de las instituciones académicas, la importancia de las redes inalámbricas radica en la capacidad de brindar constante conectividad, accesible para estudiantes, profesores y personal administrativo en todo el campus. El presente proyecto se centra en el "Implementación del firewall pfSense+ dentro de la infraestructura de red de la UTCV", implementando un firewall de código abierto. En esta sección se presentan diversos trabajos relacionados con la implementación de una red inalámbrica, sistemas operativos de virtualización e implementación de firewall dentro de una infraestructura de red.

El trabajo de (Cuéllar et al., 2020) titulado "Firewall a nivel de software en la empresa de vigilancia y seguridad privada Timanco LTDA" consistió en la implementación de un firewall a nivel de software el cual garantiza la seguridad de su red interna y protección a sus clientes. Para realizarlo, se comenzó por identificar la problemática la cual era que la empresa no contaba con un firewall que permitiera restringir el acceso de usuarios que no estuvieran autorizados, lo cual acabaría por permitir el contenido potencialmente malicioso que provenía de internet. También, era necesario prevenir que se accediera a sitios que no estuvieran dentro de las funciones laborales de la empresa. Para esto, se planteó una propuesta de solución que partió de un análisis de registro de eventos y recolección de información utilizando el método de análisis de registro de eventos y recolección de información con el personal del área de Tecnología Informática de la empresa, en donde se esperó recuperar la mayor cantidad de información relacionada con el aprovechamiento de vulnerabilidades e historial de sucesos. Los resultados de este proyecto se centraron en la implementación adecuada del firewall permitiendo demostrar el buen funcionamiento de este al evitar conexiones no seguras y no autorizadas.

El proyecto de (Lescay et al., 2019) se enfocó en el diseño de una estrategia de superación para la adquisición de conocimientos teórico-prácticos sobre Proxmox y pfSense. Además, se aplicaron métodos teóricos, empíricos y estadísticos para realizar el estudio exploratorio en 43 informáticos y administradores de redes. El proyecto tuvo como objetivo que los administradores de redes implementarán de manera eficaz el sistema Proxmox y el firewall pfSense dentro de las instituciones de salud de Santiago de Cuba, lo que permitió la estandarización de los servidores y servicios en las unidades de salud del territorio, en función del acceso a internet por parte de los profesionales. Como resultado de todo esto, el proyecto permitió crear una comunidad entre los administradores de redes que comenzaron a utilizar Proxmox y pfSense en las instituciones de salud.

El trabajo de (Lio, 2022) titulado “Virtualización con Proxmox VE como alternativa de infraestructura en instituciones de Salud” se enfocó en que, en una institución de Cuba se tiene el acceso limitado a recursos y tecnologías lo que genera un problema al momento de disponer de una infraestructura funcional para sus instituciones. Además, se da a conocer que, aunque en los centros de atención sanitaria disponibles, la tecnología informática y de comunicaciones (TIC) es accesible, es muy difícil para las instituciones disponer de tecnologías y equipos adecuados. Con base en lo anterior (Lio, 2022) propuso la implementación de técnicas de virtualización, tales como Proxmox VE como posible alternativa de solución para mejorar la eficiencia y sostenibilidad de los sistemas informáticos en el sector de la salud; asimismo, se buscó información para definir los criterios a seguir en la implementación. Al final, se logró la primera instalación después de seguir varias recomendaciones y guías. La virtualización con Proxmox VE trajo beneficios para las instituciones de salud, tales como la fácil administración, posibilidad de una gestión centralizada, la monitorización al aportar sencillez en aspectos como realizar actualizaciones, una mayor disponibilidad, una mayor fiabilidad y permitió una fácil recuperación ante desastres.

El trabajo de (Espín, 2022) cuyo título es “Diseño e implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad” consistió en la implementación de un firewall de nueva generación diseñado e implementado con herramientas de código abierto para proteger las redes del Instituto Superior Tecnológico Libertad contra diferentes tipos de ataques. El trabajo contempló la implementación de un firewall que no solo es capaz de analizar el tráfico y bloquear puertos, sino que también puede identificar el tipo de tráfico generado por las aplicaciones, que representa una ventaja ofrecida por un firewall de nueva generación, además, en el proyecto se utilizaron herramientas de código abierto y gratuitas, tales como VMware ESXI v6.7, Proxmox, Zentyal v4.0, OPNSense v21.7, PfSense v2. Lo anterior ayudó a que la institución destinara un presupuesto fuerte para su despliegue. Finalmente, la implementación de firewall de nueva generación permitió mejorar el rendimiento de la red institucional, obteniendo mejores tiempos de respuesta en la transmisión de datos. Además, se pudo garantizar el acceso a recursos compartidos como impresoras, unidades de red y scanners en todo momento sin perjudicar la productividad del personal. También, hubo una mejora en los accesos a recursos en internet gracias a la optimización del uso del ancho de banda debido a las políticas y perfiles de navegación configuradas en el NGFW.

El trabajo de (Bastidas, 2023) titulado “Reingeniería de la infraestructura de red de datos física y lógica del Gobierno Autónomo Descentralizado Municipal Santa Elena” se enfocó en la mejora de la infraestructura de red de datos del Gobierno Autónomo Descentralizado Municipal Santa Elena. En este se describe que los ciberdelincuentes actualmente utilizan diversas técnicas de ataque para lograr sus objetivos malintencionados, por ejemplo, el del malware Point of Sale que afectó a empresas como Target, Home Depot y UPS en 2014, en donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de los usuarios. Por lo anterior, se optó por optimizar la estructura física y lógica de la red para garantizar una comunicación más eficiente, confiable y segura.

En este proyecto se utilizó la metodología Top-Down Network Design para ayudar a identificar requisitos técnicos, así como seleccionar las tecnologías adecuadas y optimización en el diseño de la red, esta metodología tuvo como resultado una planificación adecuada y una implementación efectiva de las medidas de seguridad para proteger la red contra posibles ataques informáticos. Como conclusión (Bastidas, 2023) culminó con un resultado positivo, ya que se logró implementar pfSense+ como solución adecuada, flexible y asequible para una infraestructura de red eficiente. Al identificar y analizar los problemas de la red con la que se contaba, se logró desarrollar un diseño mejorado que abordaba eficazmente las limitaciones que existían. La configuración de las políticas de seguridad a través del Firewall PfSense resultó fundamental para garantizar la protección de los sistemas y datos críticos de la organización. La instalación del firewall pfSense en la plataforma de virtualización VMWARE permitió obtener sistemas compatibles que desempeñan las mismas funciones que un firewall físico, además de optimizar el uso de los recursos de hardware disponible.

Autor	Título del trabajo	Problema que resuelve	Resultados obtenidos	Tecnologías utilizadas	Costo
Jhoin Ferney Cuéllar Diaz, Roberto Duran Fierro, Jorge Leonardo Gaita Roldan	Firewall a nivel de software en la empresa de vigilancia y seguridad privada Timanco LTDA	La red de comunicaciones interna de la empresa de Vigilancia y Seguridad Privada Timanco Ltda. Carecía de seguridad por la falta de un firewall	Al implementar el firewall se aseguró el buen funcionamiento de este, evitando conexiones no seguras y no autorizadas	**Únicamente se indica descripción general*** Equipo Servidor Instalación y configuración inicial Capacitación de la herramienta para el personal a cargo Fotocopias, impresiones, papelería general pfSense	$ 35,255.20
Michel Lescay Arias, Luis Alberto Montoya Acosta, Lisbet Estrada Ladoy, Gertrudis Torre de la Vega, Lucía Graciela Barrera Yero	Estrategia de superación para la utilización de Proxmox y pfSense en las instituciones de salud	En la provincia de Santiago de Cuba, existen insuficiencias en la implementación de servicios de red por parte de los administradores de red e informáticos	Al llevar a cabo este proyecto los administradores de redes lograron implementar Proxmox y pfSense dentro de las instituciones de salud de Santiago de Cuba	Proxmox pfSense	N/A
Ing. Borys Lio Alonso	Virtualización con Proxmox VE como alternativa de	El acceso a recursos y tecnologías en Cuba es muy	Con Proxmox como técnica de virtualización fue muy útil	Proxmox	N/A

	infraestructura en instituciones de Salud	limitado y es un problema disponer de infraestructura funcional para las instituciones de salud	implementar sistemas en el sector salud, permitiendo habilitar la infraestructura y servicios de gran estabilidad y escalabilidad sin inversiones.		
Diego Omar Espín Corrales	Diseño e implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad	Ataques como phishing y malware, pueden ser originados por un usuario final o un cliente que abrió un correo o un mensaje a través de una red social	Se logró proteger las redes del Instituto Superior Tecnológico Libertad contra diferentes tipos de ataques gracias a la implementación del firewall y el conjunto de softwares que se utilizaron	**Únicamente se indica descripción general*** **Hardware:** 2 Servidores **Software:** VMware ESXI v6.7 Proxmox Zentyal v4.0 OPNSense v21.7 pfSense v2 Snort OpenVPN	N/A
Ismael Joaquín Bastidas Orrala	Reingeniería de la infraestructura de red de datos física y lógica del gobierno autónomo descentralizado municipal Santa Elena	Las ineficiencias en la comunicación dentro de la red, la falta de seguridad y dificultades en la gestión de la red	La identificación y análisis de problemas permitió desarrollar un diseño mejorado y la configuración de políticas de seguridad en el firewall pfSense garantizó la	**Se menciona que los dispositivos a utilizar son los que la institución provee*** Organizador de cables Switches Patch Panel Patch Cord Jack RJ-45 pfSense	N/A ***Se menciona que generará y ahorrará costos, pero no los indica***

			protección de sistemas y datos críticos, por otro lado, la instalación en la plataforma de virtualización VMWARE optimizó el uso de recursos de hardware, obteniendo sistemas compatibles con funciones de un firewall físico.	Routers Conmutadores KVM de montaje en rack de 8 puertos Conversor de medios WDM VMware Diagrams.net	

Tabla 1.1. Comparativa de proyectos
Fuente: Elaboración propia

1.2 Descripción del problema

El uso de redes inalámbricas se ha vuelto cada vez más frecuente en la actualidad. En el año 2021 según el estudio de (Galeano, 2023) se registró que los usuarios con acceso a internet rondaron los 4.660 millones de personas, es decir, el 59.5% de la población para un año después alcanzar los 4,950 millones de personas, lo que representaba al 62.5% de la población mundial, los resultados anteriores representan la importancia de contar con acceso a internet para realizar diversas actividades. Con el avance de la tecnología, los dispositivos móviles y demás dispositivos junto con las aplicaciones basadas en la nube, han convertido a las redes inalámbricas en una necesidad para las personas y las organizaciones, sin embargo, el crecimiento de las redes inalámbricas ha aumentado la necesidad de implementar firewalls a nivel software para proteger la red. Estos firewalls proporcionan una capa adicional de

seguridad al filtrar el tráfico de red y controlar el acceso a los recursos evitando así posibles amenazas.

La red inalámbrica de la UTCV presenta una serie de problemas técnicos y de conectividad que están teniendo un impacto significativo en el acceso a Internet de los usuarios. Una de las principales deficiencias es la falta de un firewall adecuado en el entorno de red. La ausencia de esta medida de seguridad expone la información de los usuarios a diversos riesgos, como ciberataques, accesos no autorizados, fuga de información sensitiva e interrupción de los servicios, entre otros. Esta vulnerabilidad pone en peligro la integridad y la confidencialidad de los datos de los usuarios, lo que es especialmente preocupante en un entorno académico donde se manejan información sensible y de investigación.

Además, los recursos disponibles en la red existente resultan insuficientes para satisfacer las crecientes demandas de conectividad de la comunidad universitaria. La conexión a Internet puede ser lenta e inestable, lo que dificulta el acceso a recursos en línea, la realización de actividades académicas y de investigación, así como la comunicación en tiempo real con otros usuarios. Esta limitación en la conectividad afecta negativamente la productividad y el rendimiento de la comunidad universitaria.

La implementación del firewall pfSense+ se propone como una posible solución del problema detectado. Para llevar a cabo esta solución, será necesario configurar y adaptar el firewall pfSense+ de acuerdo con los requisitos de seguridad específicos de la UTCV.

1.3 Objetivos

1.3.1 Objetivo general

Configurar e implementar el firewall pfSense+ en la infraestructura de red de la Universidad Tecnológica del Centro de Veracruz (UTCV), para mejorar la seguridad de la red y protegerla ante diversos ataques.

1.3.2 Objetivos específicos

- Analizar la infraestructura de la red de la UTCV para identificar las vulnerabilidades en términos de seguridad y establecer los requisitos de configuración del firewall pfSense+.
- Realizar el diseño lógico y físico de la red de la UTCV, teniendo en cuenta los requisitos de seguridad establecidos para asegurar una implementación adecuada y eficiente.
- Realizar pruebas del funcionamiento del firewall pfSense+ para verificar su funcionalidad, detectar posibles vulnerabilidades y asegurar que se cumplan los estándares de seguridad establecidos por la UTCV.
- Establecer un monitoreo para del firewall pfSense+ para supervisar el tráfico de red, detectar y responder de manera óptima a posibles amenazas, garantizando así la disponibilidad y confidencialidad de los recursos de información en la infraestructura de la UTCV.
- Capacitar al personal de TI de la UTCV en el uso y administración del firewall pfSense+, brindando los conocimientos necesarios para mantener y actualizar adecuadamente las políticas de seguridad, así como para responder y solucionar incidentes de seguridad de manera eficiente.

1.4 Definición de variables

En esta sección se definirán las variables las cuales formaron parte del proyecto para dar solución a la problemática presentada. (Hernández, 2014:138) argumenta y define que, “una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse.” En este sentido se describen las variables presentes en el proyecto.

1.4.1 Variables según su relación con otras variables

En la investigación, se pueden identificar distintos tipos de variables cuya clasificación se determina en función de su relación con otras variables. Incluso, eventualmente es posible que un elemento sea considerado de un tipo de variable de estudio y pertenezca a otro tipo en un estudio diferente, dependiendo de las circunstancias de la investigación.

1.4.1.1 Variables dependientes

- Cobertura de red inalámbrica
- Velocidad de conexión
- Estabilidad de la red

1.4.1.2 Variables independientes

- Configuración de la red
- Medidas de seguridad
- Capacitación de usuarios

1.5 Hipótesis

Al configurar el firewall pfSense+ en la red inalámbrica de la UTCV implementando medidas de seguridad y proporcionando capacitación a los usuarios, se logrará mejorar la cobertura de esta, aumentando la velocidad de conexión, garantizando la estabilidad de la red y mejorando la conectividad para el desarrollo de las actividades académicas y administrativas en una red segura dentro de la institución.

1.6 Justificación del proyecto

En un mundo cada vez más conectado, la seguridad de las infraestructuras de redes se ha vuelto una preocupación primordial. Las organizaciones, especialmente las instituciones educativas deben garantizar la protección de la integridad de la información que fluye a través de sus redes. Según el trabajo de (Nicolini, 2020), indica que, “la inversión en educación en México no es ni debe considerarse como un gasto para el país”. Por el contrario, fortalecer el sistema educativo se traduce en el crecimiento tanto social como económico, lo cual contribuye al desarrollo general de la nación. Tomando en cuenta lo anteriormente descrito, la Universidad Tecnológica del Centro de Veracruz al ser parte integral del sector universitario desempeña un papel crucial en la economía del país debido a los ingresos generados en el ámbito educativo, tomando como punto de partida los servicios tecnológicos con el propósito de colaborar en el desarrollo socio-económico de la región, brindando educación continua favoreciendo los sectores productivo y educativo, hasta la incubadora de empresas y bolsa de trabajo.

El proyecto titulado “Implementación del firewall pfSense+ en de la infraestructura de red de la UTCV” surge como respuesta a la necesidad de tener un control sobre los dispositivos que se conectan a la red de la institución y reforzar la seguridad de la red de la UTCV para proteger la información sensitiva de la institución y de los colaboradores de esta. Con esto se pretende garantizar la integridad de la información de quienes forman parte de la institución y garantizar la integridad de los dispositivos que conforman la red. Asimismo, se evaluará la infraestructura existente, la configuración del firewall pfSense+ y las pruebas de monitoreo continuo. Durante la implementación, es importante considerar posibles complicaciones, tales como la compatibilidad entre sistemas y dispositivos existentes, la capacitación del personal e interrupciones en la operatividad de la red. El desarrollo del proyecto se realiza utilizando la metodología PPDIOO basada en un ciclo de vida para el diseño e implementación de redes. Esto brindará un mayor control en todas las actividades del proyecto, permitiendo un avance eficiente, adaptable a cambios y errores.

El proyecto en curso traerá múltiples beneficios, entre los cuales destaca el fortalecimiento de la seguridad de la infraestructura de red de la UTCV. Esta mejora en la seguridad no solo beneficia a estudiantes, sino que también impacta de manera directa en los usuarios del campus Cuitláhuac de la UTCV, como lo son profesores y personal administrativo al contar con un entorno más seguro y protegido contra ciberataques. Por último, la implementación del firewall pfSense+ contribuirá a una navegación en la red más segura y protegida, mejorando así la experiencia de los usuarios al utilizar los recursos tecnológicos de la institución y como principal beneficiado de la solución propuesta serán los usuarios de la UTCV campus Cuitláhuac por las razones antes mencionadas.

1.7 Alcances y Limitaciones

1.7.1 Alcances

La realización del proyecto en la Universidad Tecnológica del Centro de Veracruz tiene como alcance la configuración e implementación de un firewall de código abierto denominado pfSense+ dentro de la red inalámbrica únicamente en el campus Cuitláhuac ubicado en la localidad de Dos Caminos. Se llevará a cabo la implementación de este firewall con el propósito de fortalecer la seguridad de la red inalámbrica del campus, protegiendo los datos y garantizando un entorno seguro para estudiantes, profesores y personal administrativo.

Lo anterior se realizará utilizando la metodología “PPDIOO” en un tiempo estimado de cuatro meses (mayo-agosto, 2023). Cabe mencionar que se elaborará un reporte técnico donde se especificará lo realizado a lo largo el proyecto en la institución.

1.7.2 Limitaciones

- **Falta de equipamiento**

  La disponibilidad de hardware o software necesario para la implementación del firewall pfSense+, actualmente no se cuenta con los dispositivos físicos para implementar lo de manera óptima. Esto podría afectar la capacidad de llevar a cabo el proyecto correctamente.

- **Infraestructura de red**

  La infraestructura de red actual, no cuenta con los dispositivos adecuados para implementar el firewall pfSense+ además de la falta de espacio para la instalación del servidor en el área final en donde se quedará.

- **Interferencias y obstáculos físicos**

  La presencia de interferencias electromagnéticas, obstáculos físicos o limitaciones geográficas dentro del campus de la UTCV puede afectar la calidad y alcance de la conectividad inalámbrica.

- **Incompatibilidad de sistema**

  El firewall al ser instalado en un servidor con una versión diferente a la que se implementó en un escenario anterior pude ocasionar problema de incompatibilidad debido a que no es común realizar un donwgrade a una infraestructura de red.

1.8 Universidad Tecnológica del Centro de Veracruz

1.8.1 Historia

El modelo educativo de las universidades tecnológicas en México surgió en 1991 como resultado de estudios comparativos realizados por la Secretaría de Educación Pública (SEP) desde los años setenta. Este modelo se basó en los esquemas de enseñanza de países como Estados Unidos, Canadá, Alemania, Japón y Francia. La Universidad Tecnológica del Centro de Veracruz fue creada el 9 de noviembre de 2004 como una institución pública de educación superior descentralizada del Gobierno del

Estado. Inició sus actividades el 3 de enero de 2005 con la primera generación de estudiantes en el nivel de Técnico Superior Universitario.

Con el tiempo, la demanda de ingreso a esta universidad ha aumentado significativamente. En el ciclo escolar 2018-2019, la matrícula alcanzó los 5,915 estudiantes, lo cual representa un incremento considerable en comparación con los 199 estudiantes iniciales. La universidad ofrece una amplia gama de programas educativos, incluyendo 20 programas de nivel Técnico Superior Universitario y 10 programas de Licenciatura e Ingeniería para aquellos que desean continuar sus estudios. Referente a las instalaciones, la universidad ha experimentado diversas inauguraciones a lo largo de los años. En 2006 se inauguró la primera etapa de construcción, que incluyó el Edificio de Docencia Aula 1 y el Laboratorio Pesado de Alimentos. En años posteriores se inauguraron el Centro de Información Bibliográfica (CIBI) en 2008, el Edificio de Docencia Aula 2 en 2009 y el Laboratorio Pesado de Mantenimiento Industrial en 2012.

La Universidad Tecnológica del Centro de Veracruz forma parte del sistema de Universidades Tecnológicas en México. Fue establecida en 2004 y ha experimentado un notable crecimiento en su matrícula. Ofrece una amplia variedad de programas educativos y cuenta con modernas instalaciones en diferentes campus para el desarrollo de sus actividades académicas.

1.8.2 Misión

Formar profesionistas responsables, creativos y competentes a nivel nacional e internacional, mediante una educación tecnológica, científica e integral, basada en procesos, certificados y acreditados, asegurando el cumplimiento de la Nueva Escuela Mexicana, a fin de impactar positivamente en la sociedad.

1.8.3 Visión

Ser considerada una institución referente en el marco nacional e internacional a través de su calidad educativa y de servicios, con un enfoque sustentable, coadyuvando al fortalecimiento de una sociedad incluyente.

1.8.4 Valores

- Lealtad
- Honestidad
- Responsabilidad
- Trabajo en Equipo
- Igualdad
- Cuidado del Medio Ambiente

1.8.5 Procesos que realizan en la empresa

- **Servicios tecnológicos**

  Con el propósito de coadyuvar en el desarrollo socioeconómico de la región, la UTCV oferta servicios tecnológicos y de capacitación a las empresas y personas emprendedoras en distintas áreas.

- **Educación continua**

  A través del Departamento de Educación Continua, la UTCV ofrece los sectores productivo y educativo, así como a las y los egresados, servicios de capacitación o actualización, con la finalidad de incrementar su productividad laboral. Asimismo, también se encarga de proporcionar servicios de consultoría, asistencia técnica y transferencia del modelo.

- **Incubadora de empresas**

  Con la finalidad de satisfacer las necesidades del ecosistema emprendedor, se cuenta con un modelo de incubación certificado por el Instituto Nacional del Emprendedor (INADEM), avalando las acciones que se realizan en materia de emprendimiento. Este centro pertenece a la Red de Incubadoras de las

Universidades Tecnológicas y Politécnicas (RISUTyP), Red VeracruzIncuba, y la Red Iberoamericana de Incubadoras de Base Tecnológica (RETEI).

- **Estadías profesionales**

  La Universidad Tecnológica del Centro de Veracruz implementa el programa Estadía para que los estudiantes apliquen sus conocimientos en empresas reales. Durante trece a quince semanas, los alumnos llevan a cabo un proyecto a tiempo completo bajo la supervisión de un asesor académico y un asesor industrial. Al finalizar, deben presentar un informe aprobado por sus tutores y el jefe del programa educativo para obtener su título. Las Estadías se llevan a cabo de enero a abril para nivel Ingeniería o Licenciatura, y de mayo a agosto para nivel TSU. Este programa promueve la experiencia práctica y fortalece la formación de los estudiantes.

- **Bolsa de trabajo**

  La Universidad Tecnológica del Centro de Veracruz brinda un servicio a sus egresados y empleadores de empresas tanto locales como nacionales. A través de este servicio, la universidad busca mantener una conexión duradera con sus graduados y con las empresas más destacadas del país. El objetivo principal es fomentar la inserción laboral y crear oportunidades de empleo para los estudiantes de diversas disciplinas en la universidad. La UTCV se compromete a promover la colocación laboral y facilitar el acceso a trabajos significativos para sus estudiantes.

CAPÍTULO II. METODOLOGÍA

2.1 Descripción de la metodología

El empleo de una metodología en la investigación y gestión de proyectos se refiere a la forma en que un investigador planifica o diseña de manera sistemática un estudio para poder asegurar la obtención de resultados válidos y confiables que cumplan con las metas y objetivos establecidos en un período de tiempo específico (Ortega, 2021). La realización del proyecto en desarrollo va de la mano con el uso de la metodología PPDIOO (Preparar, Planear, Diseñar, Implementar, Operar y Optimizar) desarrollada por Cisco Systems para la administración e implementación de redes. El modelo PPDIOO se caracteriza por su flexibilidad al ser una combinación de diferentes modelos, integrando lo más favorable de cada uno en un solo enfoque. Estas cualidades son las que hacen que este modelo sea apropiado para la gestión e implementación de redes, ofreciendo una gran versatilidad y adaptabilidad a las necesidades específicas de cada proyecto:

- Es secuencial porque separa claramente diferentes etapas durante el ciclo de vida.
- Es iterativo porque se realimenta continuamente una de otra, generando una flexibilidad y tolerancia a fallos por cada etapa.
- Incorpora, la comodidad de la estructuración en bloques de las tareas a realizar por cada etapa, debido a que cada una de las seis etapas corresponde a un panorama diferente.
- La representación cíclica indica la necesidad de realizar dichas tareas de un modo continuo, logrando un funcionamiento recíproco entre las etapas o fases.

Etapa	Instrumento	Objetivo
Preparar	Observación no estructurada	Realizar el primer análisis de observación simple, reconociendo el fenómeno sobre el cual no se cuenta con referencias previas.
	Investigación documental	Analizar, interpretar y comparar información sobre el objeto de estudio a partir de un cúmulo de fuentes documentales.
Planear	Checklist	Con base en una investigación documental, establecer una observación estructurada y elaborar un checklist para realizar mejoras y ajustes en la propuesta inicial, considerando los hallazgos y resultados de la revisión de literatura.
Implementar	Focus group	Obtener retroalimentación y recomendaciones por medio de un instrumento de investigación cualitativa aplicado a los usuarios finales con el propósito de evaluar su percepción sobre la implementación de pfSense+ en la infraestructura de red de la UTCV durante la etapa de implementación del proyecto.
Operar	Checklist	Obtener información de la red tras la fase de implementación, con ello comparar el antes y después de la implementación del firewall, detectar y dar seguimiento a errores, generando datos y estadísticas cuantitativas.

Tabla 2.1. Instrumentos de investigación
Fuente: Elaboración propia

2.2 Ventajas

PPDIOO es una metodología que cuenta con una serie de prácticas diseñadas para facilitar la evolución de la red, permitiendo que se convierta en un sistema capaz de respaldar eficientemente la gestión empresarial. Dentro de sus múltiples ventajas se encuentran:

- Acelerar su estrategia entregando soluciones a tiempo, dentro del presupuesto, a través de una metodología consistente y comprobada.
- Optimizar la gestión del proyecto.
- Facilitar la administración y brindar flexibilidad a los cambios.
- Mejorar la disponibilidad, estabilidad, seguridad y escalabilidad de la red mediante la planificación, el diseño, el mantenimiento y la optimización del sistema.
- Brindar una tolerancia a los fallos y cambios.
- Retroalimentar y optimizar de errores.
- Administrar la creciente complejidad de su red, garantizando procedimientos de instalación, mantenimiento y recomendaciones consistentes.

2.3 Fases o etapas de la metodología

La metodología PPDIOO, creada por Cisco, representa el proceso completo de diseño e implementación de una red, compuesto por seis fases identificadas por las iniciales de cada una: Preparar, Planear, Diseñar, Implementar, Operar y Optimizar.

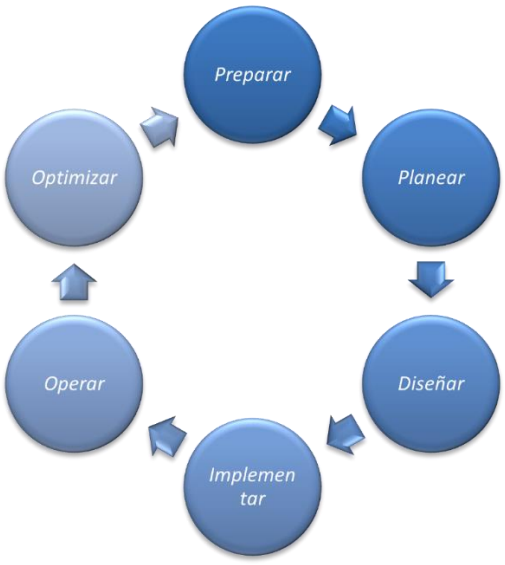


Fig. 2.1. Ciclo de vida de la metodología PPDIOO
Fuente: Elaboración propia

Este enfoque garantiza la optimización del rendimiento de la red a lo largo de su ciclo de vida (Morales Chapman & Torres Leiva, 2021). Las fases de la metodología PPDIOO se dividen en las siguientes:

- **Preparar (Prepare):** La primera fase de la metodología se enfoca en la preparación, en la cual se hará el primer reconocimiento y evaluación de la problemática a través de un primer acercamiento con el sistema actual para evaluar de los recursos actuales del sistema e identificar sus principales características y deficiencias.
- **Planear (Plan):** Una vez completada la fase de preparación y después de haber recabado la información gracias al primer acercamiento a la problemática; se procede con la segunda etapa de la metodología que es la planeación, en la cual se realizará la identificación de los requerimientos y una evaluación detallada del sistema así como de los recursos actuales de la red ayudados de un análisis previo sobre las deficiencias detectadas, de manera que se implemente un plan adecuado y seguro que esté cumpliendo con cada punto a solucionar.
- **Diseñar (Design):** Esta etapa de la metodología se hará el desarrollo del diseño lógico y físico de la solución propuesta, esto se hará basándose en los requerimientos y características evaluadas en las fases anteriores.
- **Implementar (Implement):** La etapa de implementación juega un papel crucial dentro de la metodología, ya que es en esta fase donde se lleva a cabo la puesta en práctica de la solución definida al inicio del proyecto. En esta etapa se integran las fases anteriores y se realiza la ejecución siguiendo los diseños previamente elaborados.
- **Operar (Operate):** Después de haber pasado la etapa de la implementación, la siguiente etapa es la encargada de llevar a cabo que actividades que se enfoquen en el análisis, monitoreo y administración del funcionamiento de la red, identificando problemas o fallos que surjan en que proyecto.

- **Optimizar (Optimize):** La última etapa de esta metodología hace referencia a la optimización en la cual se dará solución a los fallos detectados en la fase anterior. Es permitido realizar ajustes y mejoras en el diseño para incrementar el desempeño, resolver problemas con dispositivos y optimizar la red en general.

CAPÍTULO III. DESARROLLO DEL PROYECTO

En el desarrollo de este proyecto, se lleva a cabo una serie de procesos y acciones que se enlazan con una metodología bien definida, con el propósito de alcanzar los objetivos y metas de manera óptima y exitosa. En el presente capítulo, se detalla el desarrollo del proyecto siguiendo las etapas de la metodología PPDIOO y se mencionan las actividades necesarias para la generación de los entregables a través del uso de instrumentos de investigación a lo largo del proyecto.

3.1 Fase 1: Preparar

Al llegar a las instalaciones de la institución educativa UTCV en Cuitláhuac, Veracruz, se realizó un análisis detallado de la problemática, considerando la descripción proporcionada por el ISC. Michel Orozco Carrera. Esta descripción abordó el propósito y la importancia de abordar la solución a la problemática. Desde el primer acercamiento, se procede con la fase de preparación, realizando actividades para identificar y evaluar la situación problemática de manera minuciosa.

Las evidencias generadas en esta fase son las siguientes:

Reporte de estudio de campo del firewall existente (pfSense+)

La realización del estudio de campo ha habilitado la adquisición de datos concretos, lo que a su vez ha posibilitado el análisis de los fenómenos en un entorno auténtico. Inicialmente, se procedió a llevar a cabo el estudio de campo, centrando la atención en aspectos específicos previamente definidos:

- Era la primera aproximación al contexto de la problemática.
- Existía un manual derivado de un proyecto previo, dado que el proyecto actual es una continuación de dicho trabajo anterior.

A pesar de disponer de un conocimiento preliminar sobre la problemática, se optó por la recopilación de información a través de la observación no estructurada (Anexo A).

Mediante este enfoque, se lograron obtener detalles significativos en relación con el problema, identificando los siguientes aspectos:

Fecha	**3 de mayo del 2023**
Objetivo	Implementar el firewall pfSense+ en la infraestructura de red de la UTCV.
Observador	José Guadalupe Cid Olmedo.
Lugar	Universidad Tecnológica del Centro de Veracruz, Veracruz.
En la institución educativa de la UTCV ubicada en Cuitláhuac, Ver, el firewall actual el cual es el encargado de controlar el tráfico de la red en la UTCV es deficiente, debido a que, no se tiene bien configurado el firewall y, por lo tanto, se enfrenta problemas de conectividad, lo que expone a los usuarios a riesgos de ciberataques y fuga de información sensible.	
Resultados del estudio	Durante el proceso de investigación de la problemática, se obtuvieron los siguientes puntos: • Una VLAN debe ser agregada y otra debe ser separada del segmento de red actual. • El ancho de banda en las VLANS no está correctamente limitado. • Red congestionada. • Bloqueo poco eficiente a sitios web específicos.

Tabla 3.1. Reporte de estudio de campo
Fuente: Elaboración propia

Creación de copias de seguridad del firewall existente (pfSense+).

Esta fase resulta de suma importancia, ya que garantiza tanto la seguridad como la continuidad ininterrumpida del sistema. Las copias de seguridad, en este contexto, cumplen una función esencial al proporcionar un respaldo de las configuraciones actuales y los datos críticos.

En el apartado "Diagnostics" situado dentro del panel de navegación del firewall pfSense+, se ejecuta un procedimiento particular. Este procedimiento, denominado "Backup & Restore" se realiza con el propósito específico de llevar a cabo las correspondientes copias de seguridad (Fig. 3.1).

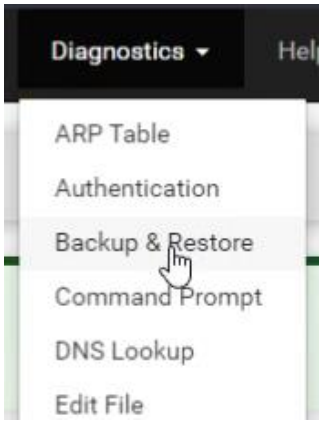


Fig. 3.1. Panel: Backup & Restore pfSense+
Fuente: Elaboración propia

Creación de la copia de seguridad.

Existen múltiples áreas sobre las cuales realizar copias de seguridad específicas, las cuales son:

- **All**: Esta alternativa ejecuta una copia íntegra de respaldo de todas las áreas señaladas a continuación. Resulta útil si se tiene la intención de poseer una copia absoluta y exhaustiva de la totalidad de la configuración de pfSense+.

- **Aliases**: Este realiza una copia de los alias, estos son conjuntos de direcciones IP o nombres de host que pueden ser utilizados en múltiples secciones de la configuración del firewall. Estos alias simplifican la administración de las reglas del firewall, dado que es posible referirse a un alias en lugar de enumerar todas las direcciones IP de manera individual.
- **Captive Portal**: El portal cautivo es una característica que restringe el acceso a Internet hasta que los usuarios autentiquen su conexión. La configuración del portal cautivo puede ser respaldada con el objetivo de asegurar la restauración precisa de las restricciones y las páginas de autenticación.
- **Captive Portal Vouchers**: Los códigos de acceso (vouchers) son generados por el portal cautivo para otorgar a los usuarios un acceso limitado a la red. El respaldo de estos códigos es esencial para mantener un registro de las credenciales generadas y permitir su restitución.
- **Dashboard Widgets**: El panel de control de pfSense+ incluye widgets y elementos visuales que suministran información y estadísticas acerca del estado del sistema y la red. El respaldo de esta configuración garantiza la persistencia de las preferencias y el diseño personalizado.
- **DNS Forwarder**: El servidor DNS Forwarder redirige las solicitudes DNS desde los dispositivos de la red hacia servidores DNS externos. La realización de un respaldo de esta configuración asegura que las peticiones DNS sigan siendo gestionadas adecuadamente.
- **DNS Resolver**: El servicio de resolución de DNS (DNS Resolver) aborda internamente las peticiones DNS y provee capacidades avanzadas de filtrado y protección. El respaldo de esta configuración conserva las reglas de resolución y filtrado.
- **DNS Server**: pfSense+ puede operar como un servidor DNS interno para resolver registros DNS locales. La salvaguardia de esta configuración garantiza la adecuada restauración de los registros locales y las zonas DNS.

- **DHCPv6 Server**: El servidor DHCPv6 asigna direcciones IPv6 a dispositivos en la red. Al respaldar esta configuración, se asegura la correcta restitución de la asignación de direcciones IPv6.
- **Firewall Rules**: Las reglas del cortafuegos controlan el tráfico permitido y bloqueado en la red. La realización de respaldos de estas reglas asegura el mantenimiento coherente de las políticas de seguridad.
- **Interfaces**: Las interfaces de red definen cómo pfSense+ interactúa con las redes. El respaldo de esta configuración es fundamental para preservar la conectividad y la configuración de red.
- **IPSEC**: IPsec permite conexiones VPN seguras entre redes. El respaldo de esta configuración asegura que las conexiones VPN sean restituidas de manera adecuada.
- **NAT**: Las reglas de traducción de direcciones de red posibilitan la comunicación entre redes internas y externas. Salvaguardar estas reglas es esencial para mantener la funcionalidad de la red.
- **Package Manager**: El respaldo de la información de configuración sobre los paquetes (extensiones) instalados en pfSense+ garantiza la restauración correcta de los paquetes adicionales.
- **RRD Data**: RRD almacena datos empleados para generar gráficos y estadísticas sobre el sistema y la red. El respaldo de estos datos asegura que las estadísticas puedan ser recuperadas.
- **Scheduled Tasks**: Las tareas programadas automatizan acciones en pfSense+. El respaldo de estas tareas mantiene la automatización y el mantenimiento planificado.
- **Syslog**: El sistema de registro (syslog) registra eventos y actividades del sistema. La salvaguardia de esta configuración asegura un registro de eventos en caso de problemas.

- **System**: La configuración del sistema incluye detalles como la zona horaria, la contraseña del usuario administrador y el nombre del host. El respaldo de esta configuración conserva la coherencia del sistema.
- **SNMP Server**: El servidor SNMP permite la supervisión y gestión remota del dispositivo. El respaldo de esta configuración mantiene la capacidad de supervisión.
- **VLANS**: Las VLAN son redes virtuales creadas dentro de una red física. El respaldo de la configuración de VLAN asegura la segmentación y la conectividad adecuadas.

Dada la migración del servidor antiguo al nuevo, la opción "All" fue seleccionada para respaldar nuestra configuración. Esto asegura que todas las áreas y aspectos de pfSense+ sean respaldados y posteriormente restaurados en el nuevo servidor. Esta elección se hizo con el propósito de garantizar una transición sin complicaciones y una continuidad operativa efectiva en el nuevo entorno, damos clic en “Download configuration as XML” (Fig. 3.2) lo que nos da como resultado un archivo de configuración .xml para su posterior importación (Fig. 3.3).

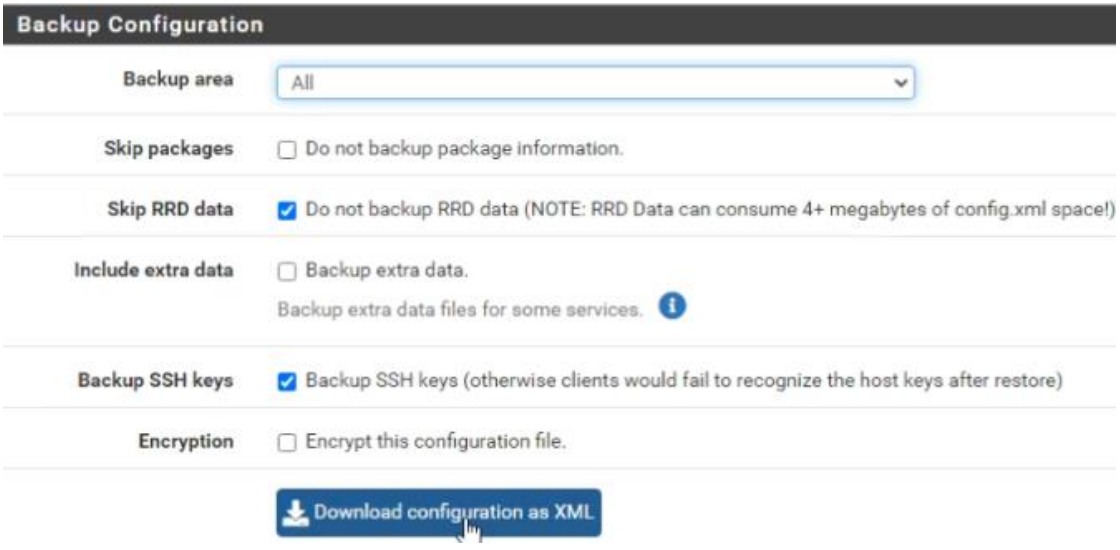


Fig. 3.2. Backup configuration
Fuente: Elaboración propia

Fig. 3.3. Archivo de configuración XML de pfSense+
Fuente: Elaboración propia

Restauración de copias de seguridad.

Para importar la copia de seguridad proveniente del firewall pfSense+, se ha seguido un proceso específico.

1. En primera instancia, se ha accedido a la sección detallada en el apartado "Diagnostics" del panel de navegación del firewall pfSense+ y luego a "Backup & Restore" (Fig. 3.4).

2. Una vez en esta sección, se ha desplazado la pantalla hacia abajo, donde se ha localizado la opción correspondiente “Restore area”.

3. Una vez ahí, se ha mantenido la configuración predeterminada como "All," con el objetivo de restaurar todas las configuraciones previamente establecidas en el firewall.

4. Por último, se ingresa al apartado "Seleccionar un archivo," dentro del cual se ha escogido la copia de seguridad .xml más reciente.

Fig. 3.4. Restore Backup Panel
Fuente: Elaboración propia

3.2 Fase 2: Planear

En el transcurso de esta fase, se lleva a cabo la determinación de los entregables. Este proceso facilita la identificación de los componentes, exigencias y tareas que conformarán la ejecución del proyecto, en conjunto con la introducción de una alternativa de solución.

Las evidencias generadas en esta fase son las siguientes:

Cronograma de actividades.

La organización del tiempo adquiere relevancia con el propósito de anticipar diversas actividades y acciones implementadas en la evolución del proyecto. En consecuencia, se elabora un cronograma de actividades, que abarcó un lapso de 15 semanas. En dicho cronograma, se incorporan las actividades a efectuar, así como su correspondiente duración. (Anexo B).

Análisis de requerimientos.

Apoyándose en los datos reunidos en el informe del estudio de campo y tras la identificación de la problemática presente en la infraestructura de la UTCV, se

procedió a establecer los requisitos indispensables para la formulación de la propuesta de resolución.

- Configuración adecuada del Firewall.
- Implementación de VLANS.
- Limitación de ancho de banda en las VLANS.
- Filtrado de contenido.
- Actualización regular.
- Contingencia y Respuesta a Incidentes.

3.3 Fase 3: Diseñar

De acuerdo con los datos recabados en el informe del estudio de campo y tomando en consideración los requisitos evaluados en las etapas precedentes, se emprende la elaboración de los diseños de red correspondientes. Estos diseños fueron adaptados a las necesidades particulares del proyecto. Al mismo tiempo, una tabla de direccionamiento se crea con la finalidad de segmentar las VLANS pendientes en ambas situaciones. Cabe resaltar que este proceso se realizará con una cuidadosa atención a los alcances, limitaciones y recursos disponibles, sirviendo como marco de referencia.

Las evidencias generadas en esta fase son las siguientes:

Diseño lógico de la red actualizado.

Se ha establecido una dirección IPv4 principal en el rango de 172.x.x.x como base de la arquitectura. Para la asignación dinámica de direcciones IP a los dispositivos finales, se ha adoptado el protocolo DHCP (Protocolo de Configuración Dinámica de Hosts), lo que agrega un nivel adicional de flexibilidad y automatización a la red. Una representación visual de esta estructura se presenta en el diagrama correspondiente, donde las VLANS se plasman con claridad, acompañadas de sus respectivos direccionamientos, nomenclaturas e identificadores. Esta herramienta gráfica no solo

facilita la comprensión de la disposición de la red, sino que también sirve como referencia para la gestión, el mantenimiento y las futuras expansiones

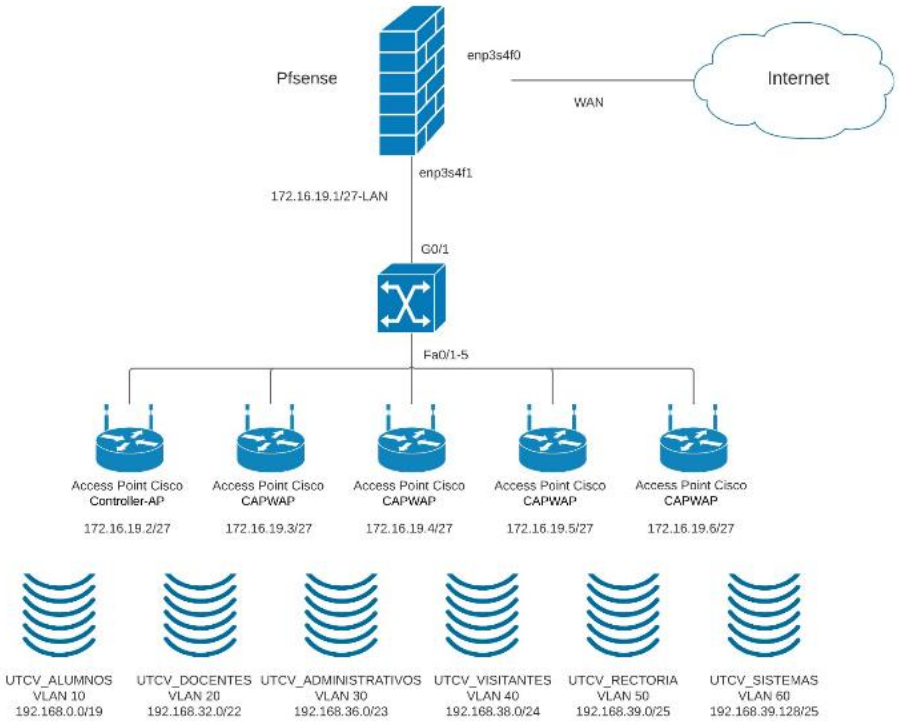


Fig. 3.5. Diseño lógico de la red
Fuente: Elaboración propia

Diseño físico de la red actualizado.

El diseño físico de la red ofrece una representación visual precisa de los aspectos detallados relacionados con las conexiones físicas requeridas para interconectar los dispositivos. Se puede observar que se sitúa al firewall de manera directa antes del switch y dentro del servidor. Este posicionamiento es consecuente con el hecho de que pfSense+ se encuentra alojado en un contenedor Docker dentro del servidor Proxmox, el cual ha sido empleado en el contexto de este proyecto. El diseño físico de la red de la institución de la UTCV, conformado por:

- Un servidor ProLiant ML350 G6 con el sistema operativo Proxmox 6.4.

- Un Switch Catalyst 3560 de capa 3 que se encargó de las configuraciones para la red LAN para que los Access Point lograran tener conexión.
- 5 Access Point Aironet 1815i de Cisco.

Ver Anexo C para más detalles de los dispositivos utilizados.

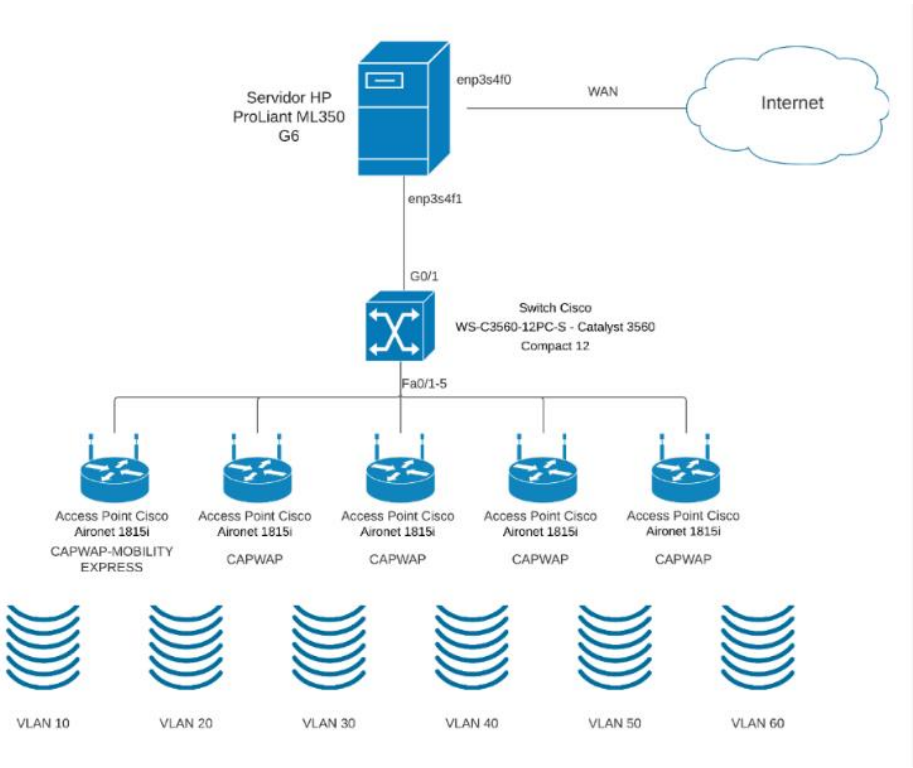


Fig. 3.6. Diseño físico de la red
Fuente: Elaboración propia

Tabla de direccionamiento con las interfaces en pfSense+.

La elaboración de una tabla de direccionamiento de red ha resultado ser de vital importancia, dado que esta tabla posee un control detallado sobre la asignación de direcciones IP y la configuración de cada VLAN. Esta acción se revela como un componente esencial para potenciar el rendimiento, la administración y la seguridad de la infraestructura de red. Dentro de la mencionada tabla de direccionamiento de red, se observa la implementación de un proceso de subnetting que permite la

segmentación de la red con el propósito de lograr una administración eficiente. Cada VLAN fue diseñada de tal manera que pueda alojar una cantidad adecuada de hosts, es decir, los dispositivos conectados, en conformidad con los requisitos específicos de cada área.

Cada asignación de direcciones IP en las distintas VLANS fue meticulosamente escogida con el propósito de optimizar la utilización de las direcciones disponibles y satisfacer los requisitos de los diversos grupos de usuarios presentes en la red. La delimitación de las redes se realizó de la siguiente manera:

- La VLAN de Alumnos está diseñada para acoger hasta 8190 hosts, de los cuales 8188 son utilizables. Esta configuración permite acomodar a la totalidad de estudiantes de la institución UTCV, gracias a la abundancia de direcciones disponibles.
- La VLAN de Docentes tiene capacidad para un gran número de profesores, ofreciendo 1022 hosts en total, de los cuales 1020 pueden utilizarse. Esta disposición garantiza que los docentes puedan llevar a cabo sus clases en el aula y tengan acceso a Internet según sea necesario.
- La VLAN de Administrativos está dimensionada para un número menor de hosts, totalizando 510, de los cuales 508 están disponibles para uso. Esta limitación se ajusta a las necesidades del personal administrativo de la institución, considerando su menor cantidad en comparación con docentes y estudiantes, lo que evita el derroche de direcciones IP.
- La VLAN de Visitantes ofrece una capacidad de 254 hosts, de los cuales 252 pueden usarse. Esta VLAN se concibió para eventos dentro de la institución que requieran acceso a Internet para los visitantes.
- La VLAN de Rectoría está creada con 128 hosts en total, de los cuales 126 están disponibles. Surgió inicialmente para asegurar una conexión estable en su propio segmento.

- Finalmente, la VLAN para el área de sistemas es implementada debido a la falta de una VLAN específica para este sector. Esta VLAN cuenta con 128 hosts en total, de los cuales 126 pueden utilizarse, lo que permite a este departamento operar en su propio entorno aislado de la red principal.

VLAN	Tamaño	Dirección	Mask	Dir. Mask	Rango	Broadcast
Alumnos	8190	192.168.0.0	/19	255.255.224.0	192.168.0.1-192.168.31.254	192.168.31.255
Docentes	1022	192.168.32.0	/22	255.255.252.0	192.168.32.1-192.168.35.254	192.168.35.255
Administrativos	510	192.168.36.0	/23	255.255.254.0	192.168.36.1-192.168.37.254	192.168.37.255
Visitantes	254	192.168.38.0	/24	255.255.255.0	192.168.38.1-192.168.38.254	192.168.38.255
Rectoría	128	192.168.39.0	/25	255.255.255.128	192.168.39.1-192.168.39.126	192.168.39.127
Sistemas	128	192.168.39.128	/25	255.255.255.128	192.168.39.129-192.168.39.254	192.168.39.255

Tabla 3.2. Tabla de direccionamiento
Fuente: Elaboración propia

3.4 Fase 4: Implementar

La configuración y despliegue adecuado del firewall pfSense+ en la infraestructura de red de la UTCV adquiere una importancia crucial en aras de asegurar la salvaguardia de los recursos y datos de la institución. Esta implementación contribuye significativamente a la optimización de la eficiencia y productividad de la red en su conjunto. Las evidencias generadas en esta fase son las siguientes:

Actualizar firewall pfSense+.

Al llevar a cabo la implementación de la actualización, se muestra ante el usuario el panel correspondiente al proceso de actualización del firewall pfSense+. Esta interfaz gráfica proporciona información en tiempo real acerca del sistema pfSense+ que abarca tanto la posibilidad de realizar actualizaciones continuas hacia las versiones

más recientes. En lo que respecta al procedimiento de actualización específico del firewall pfSense+, este es un proceso compuesto por las siguientes etapas:

1. **Verificación de la versión actual**: En la categoría del panel de configuración designada como "Current Base System", se muestra la edición instalada actual del sistema pfSense+, la cual en esta ocasión es la 23.05.

2. **Comprobación de actualizaciones**: Esta parte confiere la habilidad de establecer una conexión con los servidores de pfSense+ al panel de actualización para constatar la existencia de nuevas ediciones, actualizaciones de seguridad y correcciones. En el transcurso de este procedimiento, se verifica que la edición más reciente disponible es la 23.05.1.

3. **Selección de la actualización**: En nuestro caso específico, se elige actualizar a la versión más nueva y estable, particularmente la "Latest Stable Version (23.05.1)", esto se refleja en la sección "Branch".

4. **Descarga e instalación**: Una vez que se ha elegido la actualización y se ha generado una copia de seguridad correspondiente, se lleva a cabo la obtención de los archivos necesarios y después se realiza la instalación de la nueva edición. Todos estos pasos se ejecutan al hacer clic en el botón "Confirmar" (Fig. 3.7).

5. **Reinicio y verificación**: Una vez que se ha completado el proceso de descarga e instalación, se procede a reiniciar el firewall para implementar las modificaciones efectuadas. Tras finalizar este reinicio, en el panel de actualización de pfSense+, se puede observar que la edición más nueva y estable se ha instalado con éxito (Fig. 3.8).

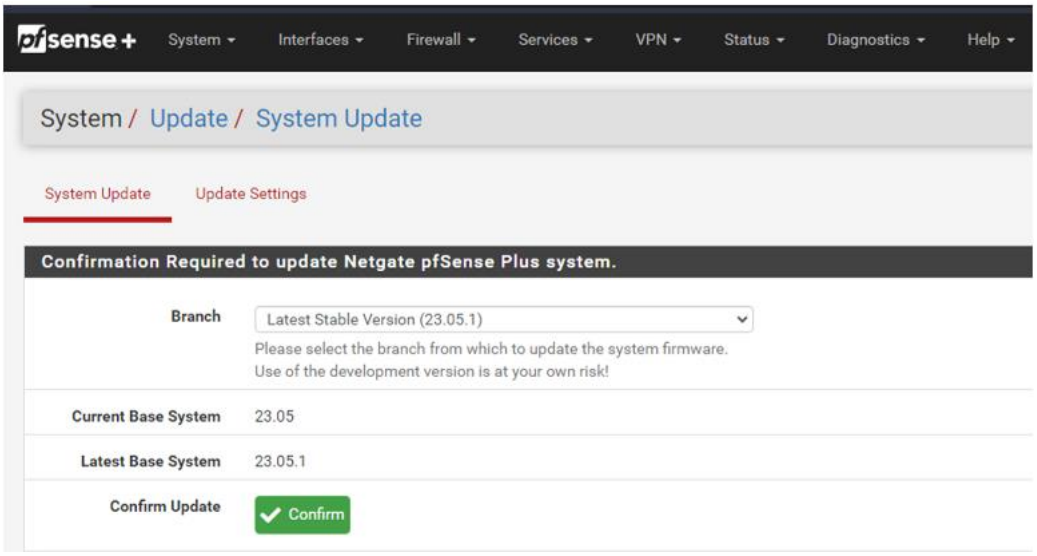


Fig. 3.7. Panel de actualización de pfSense+
Fuente: Elaboración propia

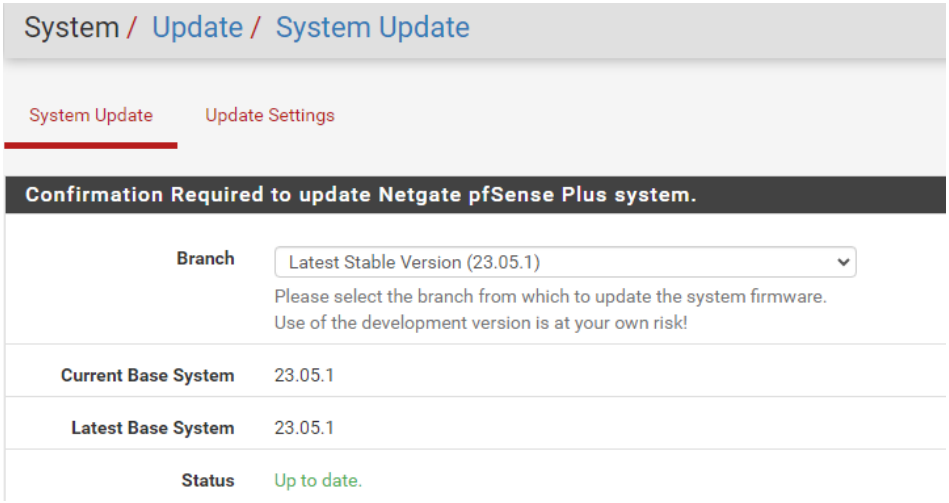


Fig. 3.8. Versión actualizada de pfSense+
Fuente: Elaboración propia

Crear interfaces VLAN en pfSense+.

La segmentación correcta de una red es crucial para su correcto funcionamiento, por ello, la creación de las VLANS faltantes, Rectoría y Sistemas es necesario, al hacer esto se separarán los dispositivos y usuarios en grupos lógicos según su área o función en la institución de la UTCV. Esto minimiza la superficie para posibles ataques

y limita la propagación de amenazas, protegiendo los datos sensibles y los recursos. Es importante mencionar que ya se contaba con las interfaces configuradas de las VLANS Alumnos, Docentes, Administrativos y Visitantes, por lo que únicamente se agregan las interfaces faltantes.

En cuanto al proceso de la creación y configuración de las interfaces VLANS faltantes dentro del firewall pfSense+ se lleva a cabo de la siguiente manera:

1. Antes de iniciar la creación de las VLANS, se contaban con 4 interfaces configuradas: UTCV_ALUMNOS, UTCV_DOCENTES, UTCV_ADMINISTRATIVOS y VLAN_VISITANTES (Tabla 3.3).

2. Se procede a crear las VLANS. En el panel de configuración de VLANS en pfSense+ selecciona la interfaz correspondiente que en nuestro caso es VLAN 50. Se selecciona el adaptador vtnet1, correspondiente a LAN, para asegurar el acceso a internet. La VLAN de Rectoría se designa con la etiqueta VLAN 50, dado que las VLANS 10, 20, 30 y 40 están en uso. También se añade una breve descripción para identificación. Mencionando que el estándar 802.1Q es una especificación que aplican en todas las interfaces VLAN que trabaja dentro del marco de trabajo IEEE 802.1 que se refiere a la segmentación de redes mediante etiquetas VLAN, en este caso de la 1 a la 4094 (Fig. 3.9).

3. Para el caso de la VLAN de Sistemas se realiza el mismo proceso que para la VLAN de Rectoría, eligiendo la VLAN 60 como etiqueta en este caso.

4. Posteriormente a la creación de las interfaces, dentro del panel de configuración de pfSense+ en la sección de “Interfaces / VLAN50 (vtnet1.50)” correspondiente a la VLAN de Rectoría, la descripción correspondiente a la VLAN se introduce, y la configuración IPv4 se mantiene en modo estático. La

casilla "Enable interface" se activa para permitir el funcionamiento de la interfaz (Fig. 3.10).

5. La dirección IP que se aplica corresponde con el direccionamiento definido en la tabla de direccionamiento previamente definido. En la misma configuración de la interfaz vtnet1.50, se asigna la dirección IPv4 192.168.39.1/25 (Fig. 3.11).

6. Para la VLAN 60 en la sección de “Interfaces / VLAN60 (vtnet1.60)” que corresponde a Sistemas, se aplica una configuración similar que la VLAN50, la descripción adecuada a la VLAN y la configuración IPv4 se mantiene en modo estático. La casilla "Enable interface" también permanece activa para permitir el funcionamiento de la interfaz.

7. Para colocar su IP se aplica la que corresponde según el direccionamiento generado previamente, en la configuración de la interfaz vtnet1.60 se asigna la dirección IPv4 192.168.39.129/25.

8. Las configuraciones de las interfaces se ven resumidas en la tabla 3.4.

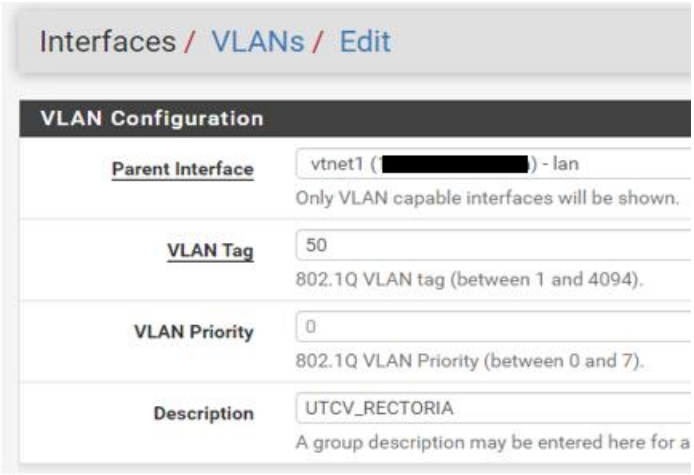


Fig. 3.9. Configuración de interfaz VLAN Rectoría
Fuente: Elaboración propia

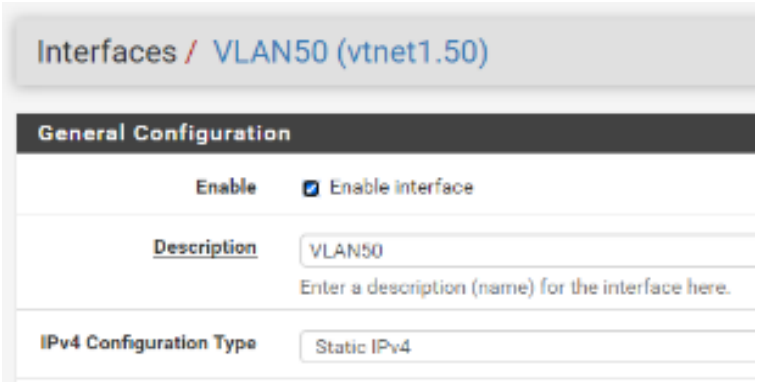


Fig. 3.10. Interfaz VLAN50
Fuente: Elaboración propia

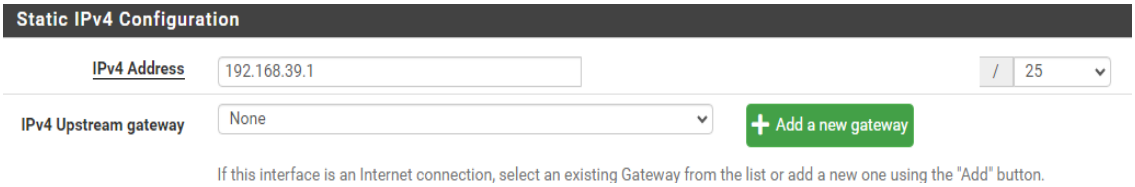


Fig. 3.11. IPv4 configuración VLAN50
Fuente: Elaboración propia

Interfaces VLANS		
Parent Inteface	VLAN Tag	Drescription
vtnet1 – lan	10	UTCV_ALUMNOS
vtnet1 – lan	20	UTCV_DOCENTES
vtnet1 – lan	30	UTCV_ADMINISTRATIVOS
vtnet1 – lan	40	VLAN_VISITANTES

Tabla 3.3. Interfaces VLANS
Fuente: Elaboración propia

Description	IPv4 Configuration Type	IPv4 Address	IPv4 Upstream gateway
VLAN10	Static IPv4	192.168.0.1	None
VLAN20	Static IPv4	192.168.32.1	None
VLAN30	Static IPv4	192.168.36.1	None
VLAN40	Static IPv4	192.168.38.1	None
VLAN50	Static IPv4	192.168.39.1	None
VLAN60	Static IPv4	192.168.39.129	None

Tabla 3.4. Configuración IPv4 Interfaces VLAN
Fuente: Elaboración propia

Configuración de VLANS en DHCP Server.

1. En el panel de configuración de pfSense+, en la sección "Services / DHCP Server", se realiza la configuración del direccionamiento correspondiente a las VLANS (Fig. 3.12).

2. Los WINS servers (Windows Internet Naming Service) que son servidores específicos de redes Windows que facilitan la conexión entre estos dispositivos y los DNS servers (Domain Name System) que permiten la navegación y la comunicación entre dispositivos, se mantienen sin configuración en todas las interfaces desde VLAN10 hasta VLAN60, incluida la interfaz LAN. Esto se hace con la finalidad de aplicar el bloqueo de sitios web. La omisión de servidores

DNS evita que los usuarios accedan a sitios bloqueados, pero aún posean acceso a internet (Fig. 3.13).

3. En todas las interfaces, desde VLAN10 hasta VLAN60, incluida la interfaz LAN, se opta por habilitar la casilla "Enable DHCP server". Esto activa el protocolo DHCP en estas interfaces (Fig. 3.14).

4. Dentro cada interfaz de VLAN se observan configuraciones no modificables, “subred, máscara de subred y el rango total disponible”. El rango de direcciones que se requiere abarcar se modifica de acuerdo al uso de cada VLAN. Para Alumnos y Rectoría, el rango de direcciones se modifica para mejorar la seguridad y la administración de la red, así como para el uso de direcciones IP que no se distribuyeran para pruebas o testeos de la red (Tabla 3.5).

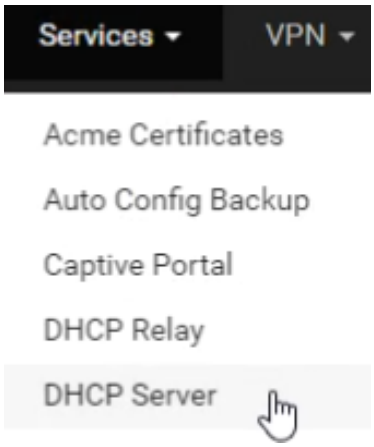


Fig. 3.12. Apartado DHCP Server
Fuente: Elaboración propia

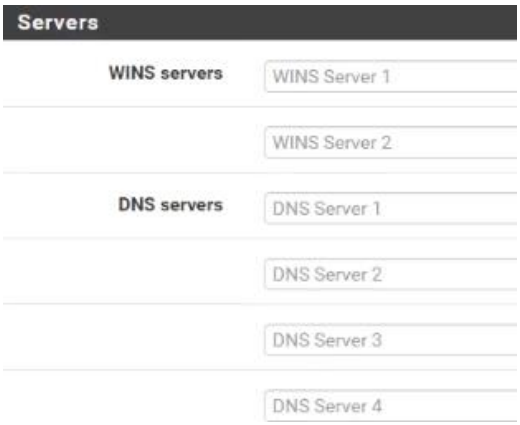


Fig. 3.13. DNS Servers
Fuente: Elaboración propia

Fig. 3.14. DHCP activo en interfaz VLAN10
Fuente: Elaboración propia

VLAN	Subnet	Subnet mask	Available range	Range
Alumnos	192.168.0.0	255.255.224.0	192.168.0.1-192.168.31.254	From 192.168.0.106 To 192.168.31.254
Docentes	192.168.32.0	255.255.252.0	192.168.32.1-192.168.35.254	From 192.168.32.2 To 192.168.35.254
Administrativos	192.168.36.0	255.255.254.0	192.168.36.1-192.168.37.254	From 192.168.36.2 To 192.168.37.254
Visitantes	192.168.38.0	255.255.255.0	192.168.38.1-192.168.38.254	From 192.168.38.2 To 192.168.38.254
Rectoría	192.168.39.0	255.255.255.128	192.168.39.1-192.168.39.126	From 192.168.39.5 To 192.168.39.120
Sistemas	192.168.39.128	255.255.255.128	192.168.39.129-192.168.39.254	From 192.168.39.133 To 192.168.39.250

Tabla 3.5. Rango DHCP interfaces
Fuente: Elaboración propia

Configuración del portal cautivo de las VLANS en pfSense+.

En pfSense+, se configura un portal cautivo para las VLANS, estableciendo un punto de acceso controlado que exige autenticación para el acceso a la red. El proceso para realizar esto es el siguiente:

1. Una vez que se ha establecido la configuración DHCP para cada VLAN, el siguiente paso consiste en acceder a la sección denominada "Services / Captive Portal" del panel de configuración de pfSense+ (Fig. 3.15).

2. Al acceder a la sección "Services / Captive Portal / Add Zone", se lleva a cabo la creación de una zona destinada al área de rectoría. Esta zona recibe el nombre de "UTCV_RECTORIA". Directamente bajo esta denominación, se suministra una breve descripción con el propósito de identificar de manera clara y precisa dicha zona (Fig. 3.16).

3. Tras completar la creación del portal, se procede a modificar su configuración empleando el botón de edición correspondiente (Fig. 3.17).

4. Una vez dentro de la configuración del portal, se realizan modificaciones en varias secciones. Se ajusta la descripción, se especifica la interfaz a la que está relacionado y se establece un límite máximo de conexiones simultáneas, limitado a 4 para el área de rectoría (Fig. 18).

5. Después de haber finalizado las configuraciones iniciales, se procede a marcar la opción que activa una pestaña emergente en los navegadores, redirigiendo a la página de la UTCV (http://www.utcv.edu.mx). Adicionalmente, se opta por el tipo de inicio de sesión "Multiple". Esta elección permite que un usuario pueda iniciar sesión desde múltiples ubicaciones o dispositivos de forma simultánea (Fig. 3.19).

6. Con relación al servidor de autenticación configurado para la VLAN de rectoría, se emplea un enfoque específico. Aquí se opta por utilizar un servidor con el nombre idéntico al de la VLAN. Este servidor es implementado como un contenedor Docker, alojado en el servidor Proxmox. Cabe destacar que el servidor Proxmox forma parte de la infraestructura de red (Fig. 3.20).

7. En la sección del panel de configuración de la sección anterior, se visualiza la casilla "Enable Captive Portal", la cual se ha activado en todos los portales. Esto incluye tanto los portales ya existentes como el portal recién creado para rectoría. Esta acción se ha realizado con el propósito de asegurar el funcionamiento adecuado de todos los portales cautivos (Fig. 3.21).

Se emplearon configuraciones específicas para cada portal cautivo, las cuales se detallan a continuación:

Portal Cautivo de Alumnos

- Descripción: PORTAL CAUTIVO VLAN_ALUMNOS.
- Interface: VLAN10.
- Número máximo de conexiones: 2 conexiones.
- Se desconecta: Cada 5 minutos de inactividad.
- Current user logins: Last login.
- Autentication Server: ALUMNOS.

Portal Cautivo de Docentes

- Descripción: PORTAL CAUTIVO VLAN_DOCENTES.
- Interface: VLAN20.
- Número máximo de conexiones: 4 conexiones.
- Se desconecta: Cada 25 minutos de inactividad.
- Current user logins: Last login.

- Autentication Server: DOCENTES.

Portal Cautivo de Administrativos

- Descripción: PORTAL CAUTIVO VLAN_ADMINISTRATIVOS.
- Interface: VLAN30.
- Número máximo de conexiones: 4 conexiones.
- Se desconecta: Cada 25 minutos de inactividad.
- Current user logins: Last login.
- Autentication Server: ADMINISTRATIVOS.

.

Portal Cautivo de Visitantes

- Descripción: PORTAL CAUTIVO VLAN_VISITANTES.
- Interface: VLAN40.
- Número máximo de conexiones: 2 conexiones.
- Se desconecta: Cada 20 minutos de inactividad.
- Current user logins: Last login.
- Autentication Server: Local Database, ya que funciona con un sistema de tokens que se generan dentro del propio pfSense+

8. Se presentan los portales cautivos en estado activo y completamente listos para su utilización. (Fig. 3.22).

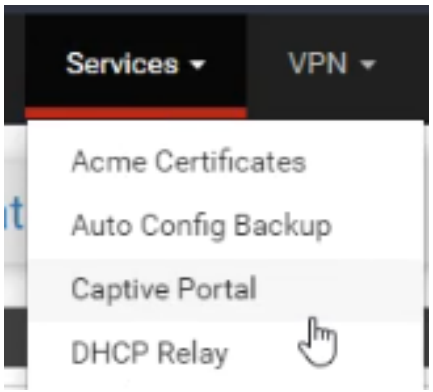


Fig. 3.15. Sección de portal cautivo
Fuente: Elaboración propia

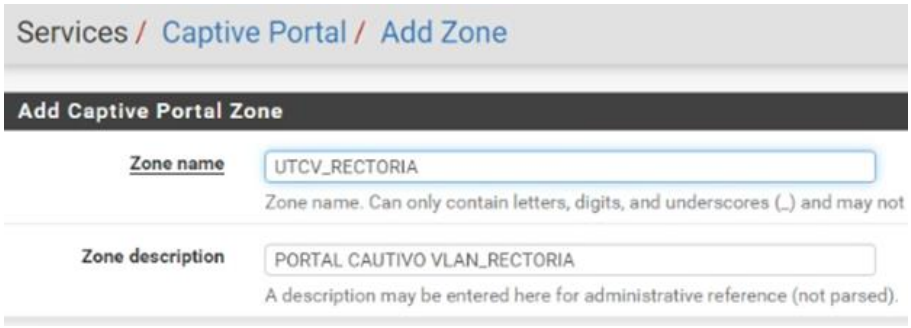


Fig. 3.16. Creación de portal cautivo Rectoría
Fuente: Elaboración propia

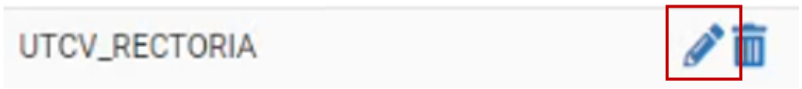


Fig. 3.17. Botón edición portal rectoría
Fuente: Elaboración propia

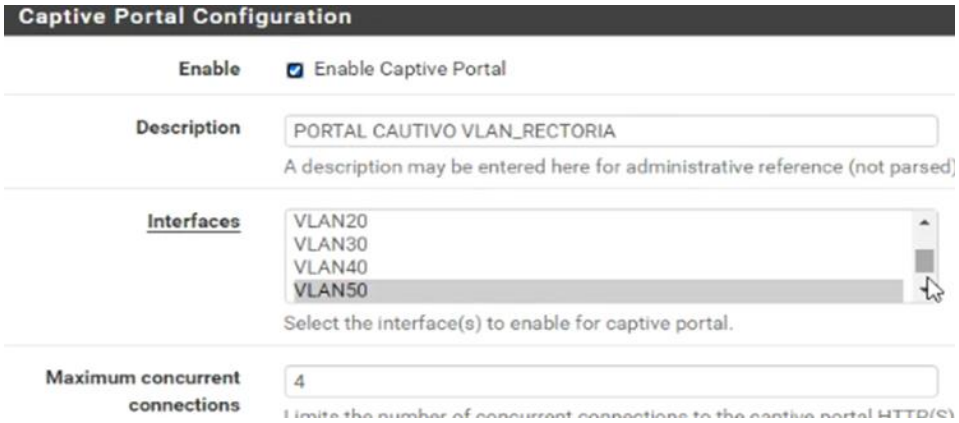


Fig. 3.18. Edición portal rectoría
Fuente: Elaboración propia

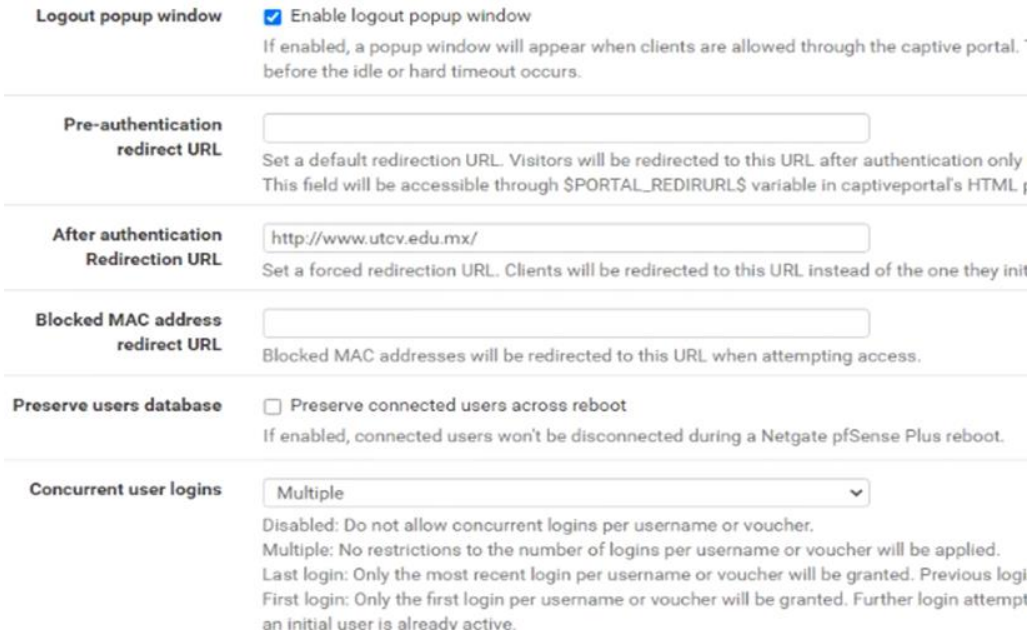


Fig. 3.19. Edición portal rectoría continuación
Fuente: Elaboración propia

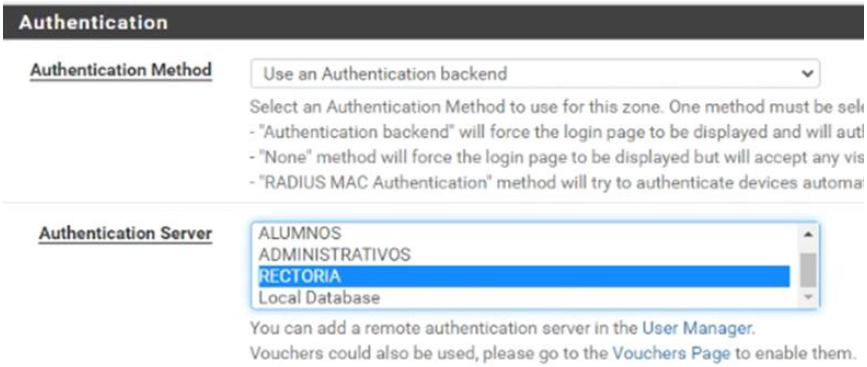


Fig. 3.20. Servidor de autenticación de rectoría
Fuente: Elaboración propia

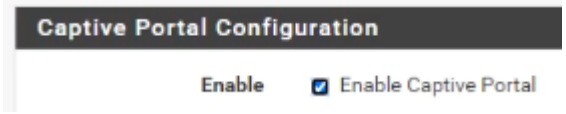


Fig. 3.21. Casilla de portal cautivo activo
Fuente: Elaboración propia

Fig. 3.22. Portales Cautivos Activos
Fuente: Elaboración propia

Personalizar portal cautivo de VLANS en pfSense+.

Dentro del entorno de pfSense+, se realiza la tarea de personalizar el portal cautivo dirigido a las VLANS. Esta adaptación involucra ajustes específicos que reflejan la identidad y los requerimientos de la red, con el propósito de optimizar la autenticación y el acceso de los usuarios de manera más efectiva.

1. En la casilla "Enable Custom captive portal login page", ubicada dentro de la configuración del "Services / Captive Portal", se permite la personalización de la página de inicio de sesión en los portales. Esta opción se activa en todos los portales, tanto los previamente creados como el portal recién establecido para rectoría. Esta acción garantiza la posibilidad de emplear páginas .html personalizadas en los portales (Fig. 3.23-24).

2. Para implementar una página personalizada en el portal cautivo, se realiza el proceso de importación de una página en formato .html. Esta página se obtiene

de uno de los portales ya existentes. Se modifica en el código HTML, ajustando la dirección IP y el nombre de la VLAN al que la página hacía referencia. Estos cambios brindan el correcto funcionamiento de la página.html (Fig. 3.25-27).

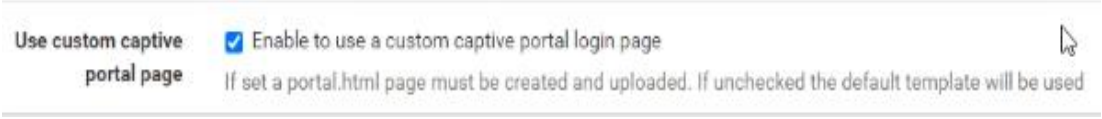


Fig. 3.23. Casilla de portal cautivo personalizado activa
Fuente: Elaboración propia

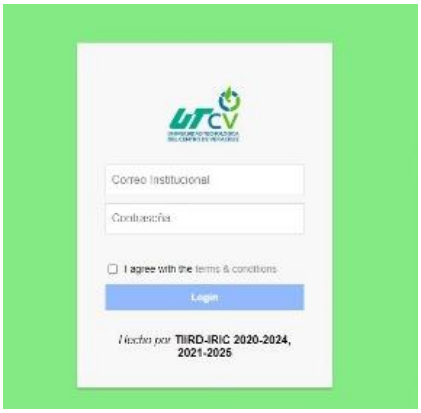


Fig. 3.24. Portal cautivo personalizado
Fuente: Elaboración propia

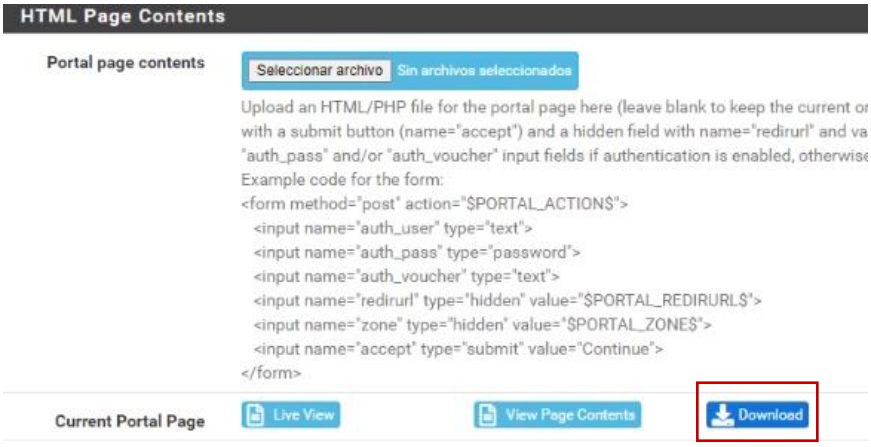


Fig. 3.25. Descargar portal cautivo
Fuente: Elaboración propia

Fig. 3.26. Archivo HTML de portal cautivo
Fuente: Elaboración propia

Fig. 3.27. Importar portal cautivo
Fuente: Elaboración propia

Implementar políticas de filtrado web específicas en el firewall pfSense+.

En la configuración del firewall pfSense+, se emplean políticas de filtrado web específicas para regular el acceso y la seguridad en la red. Mediante reglas detalladas, se controla el tráfico de internet según protocolos, direcciones IP, puertos y opciones de filtrado avanzadas, logrando así una navegación en línea eficiente y segura.

1. Para la configuración del filtrado web, dentro del panel de configuración de pfSense+, en la sección “Services” se procede a acceder a la opción "SquidGuard Proxy Filter" (Fig. 3.28).

2. Dentro del apartado, se activa únicamente la casilla "Enable SSL filtering" para bloquear el contenido con certificado HTTPS (Fig. 3.29).

3. Luego, en la sección "Services", se procede a acceder a la opción "SquidGuard Proxy Filter" (Fig. 3.30).

4. En la sección correspondiente a las Blacklist, se incluye una extensa lista de sitios web de diversas categorías para facilitar el filtrado de sitios web no deseados. Esta lista se proporciona como un enlace para descarga (Fig. 3.31).

5. En la sección de creación de listas personalizadas, se establecen enlaces a sitios web organizados por categorías para ampliar la cobertura de sitios web bloqueados. Se asigna un mensaje de "redirección" para cuando se bloquee un sitio web perteneciente a alguna de estas listas personalizadas (Fig. 3.32).

6. Después de crear las listas personalizadas, se procede a la creación de cuatro grupos de listas de control de acceso (ACL) con nombres como VLAN10_ALUMNOS, VLAN20_DOCENTES, VLAN30_ADMIN y VLAN40_INVITADOS. Estos grupos se establecen en la sección "Groups ACL" para administrar y aplicar restricciones específicas para los usuarios de cada VLAN (Fig. 3.33).

7. Se configura la ACL para la VLAN10_ALUMNOS y se define el rango de direcciones IP para el filtrado de contenido en la Figura 3.57. El rango de direcciones IP definido es 192.168.0.1-192.168.31.254, correspondiente a la VLAN de Alumnos. Se considera que por defecto las categorías no denegadas son permitidas por SquidGuard (Fig. 3.34).

8. Para la VLAN10_ALUMNOS. Los sitios web bloqueados incluyen categorías como Apuestas, Cine/Películas, Compras, Adultos, Redes Sociales, Streaming, OnlyFans, Anuncios, Contenido violento, Audio y Vídeo, Chats, Citas, Venta de sustancias nocivas, Financias, Anime y VPN's (Fig. 3.35-37).

9. Se configura la ACL para VLAN20_DOCENTES y se define el rango de direcciones IP en la Figura 3.65. El rango de direcciones IP definido es 192.168.32.2-192.168.35.254, correspondiente a la VLAN de docentes.

10. Para la VLAN20_DOCENTES. Los sitios web bloqueados incluyen categorías como Adultos, Contenido Sexual, OnlyFans, Contenido violento y warez (Software Pirata). Las categorías no denegadas se consideran permitidas por defecto por SquidGuard.

11. Se configura la ACL para VLAN30_ADMIN y se define el rango de direcciones IP en la Figura 3.65. El rango de direcciones IP definido es 192.168.36.2-192.168.37.254.

12. Para la VLAN40_ADMIN. Los sitios web bloqueados incluyen categorías como Adultos, Contenido Sexual, OnlyFans, Contenido violento y warez (Software Pirata). Las categorías no denegadas se consideran permitidas por defecto por SquidGuard.

13. Se configura la ACL para VLAN40_INVITADOS y se define el rango de direcciones IP en la Figura 3.69. El rango de direcciones IP definido es 192.168.38.2-192.168.38.254, correspondiente a la VLAN total de Invitados.

14. Para la VLAN40_INVITADOS. Los sitios web bloqueados incluyen categorías como Adultos, Contenido Sexual, OnlyFans, Contenido violento y warez (Software Pirata). Las categorías no denegadas se consideran permitidas por defecto por SquidGuard.

Fig. 3.28. Opción Squid Proxy Server
Fuente: Elaboración propia

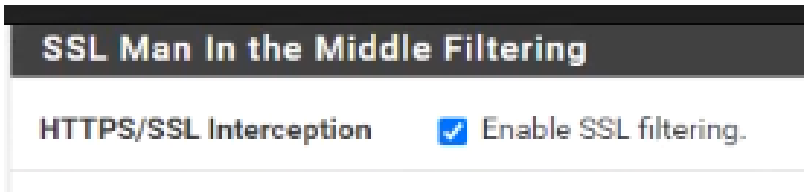


Fig. 3.29. Enable SSL filtering
Fuente: Elaboración propia

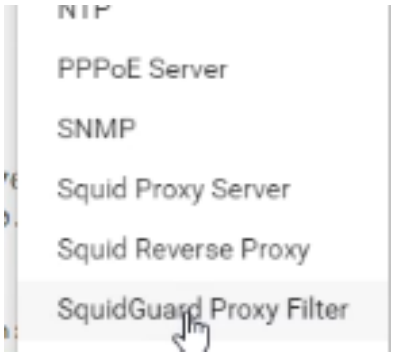


Fig. 3.30. Opción SquidGuard Proxy Filter
Fuente: Elaboración propia

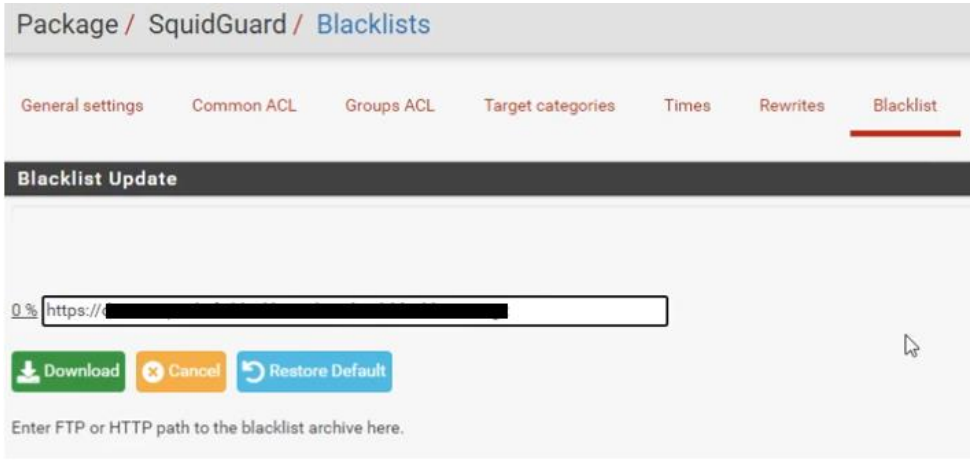


Fig. 3.31. Blacklist Update
Fuente: Elaboración propia

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XML

Name	Redirect	Description
Permit		Permite el acceso al sitio http de utcv.
Apuestas_Block	Acceso Denegado: Apuestas!	Bloqueo de páginas de apuestas
Cine_Block	Acceso Denegado: Cine, etc!	Bloqueo paginas para ver videos_peliculas_series_partidos
Compras_Block	Acceso Denegado: Paginas Compras!	Bloqueo de páginas de compras
Hentai_Block	Acceso Denegado: Hentai!	Bloqueo de páginas Hentai
Contenido_Sexual	Acceso Denegado: Contenido Sexual!	Bloqueo de contenido sexual
RedSocial_Block	Acceso Denegado: Redes Sociales!	Bloqueo de redes sociales
Streaming_Block	Acceso Denegado: Streaming!	Bloqueo de páginas de streaming
Only_Block	Acceso Denegado: Onlyfans_etc!	Bloqueo de Onlyfans_etc

Fig. 3.32. Blacklist personalizadas
Fuente: Elaboración propia

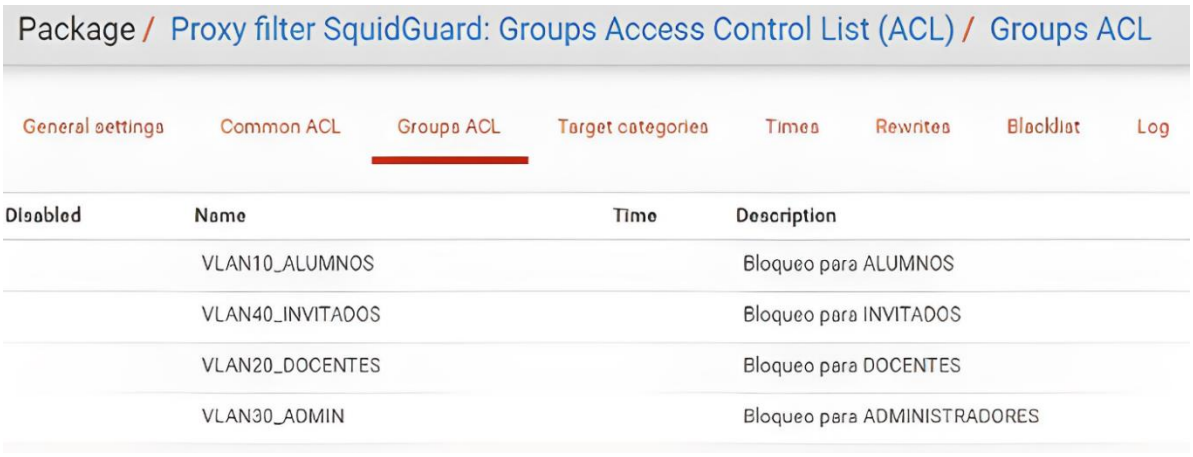


Fig. 3.33. Groups ACL creados
Fuente: Elaboración propia

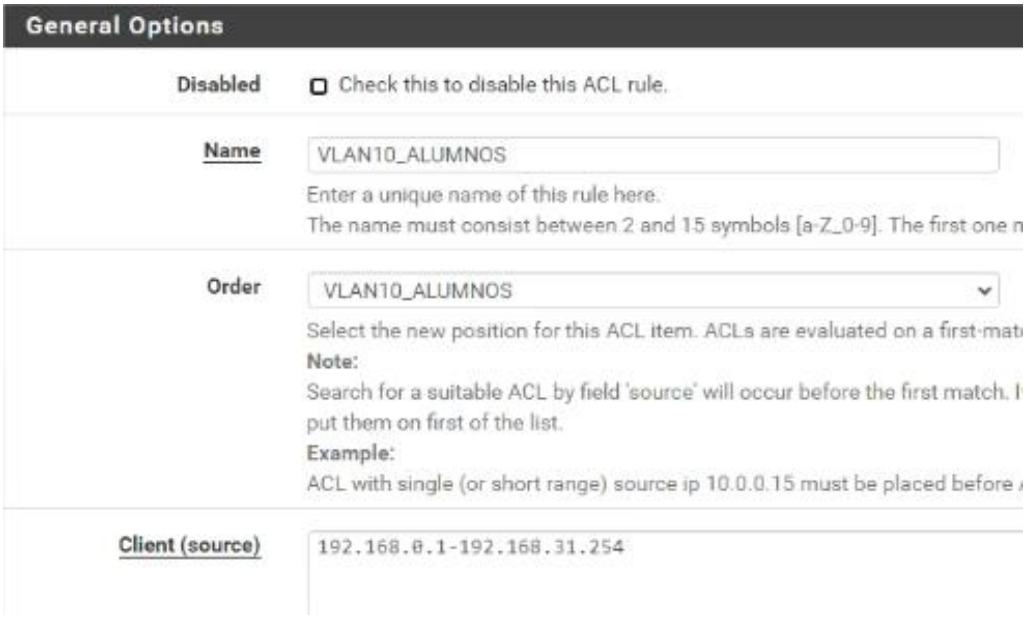


Fig. 3.34. Configuración ACL Alumnos
Fuente: Elaboración propia

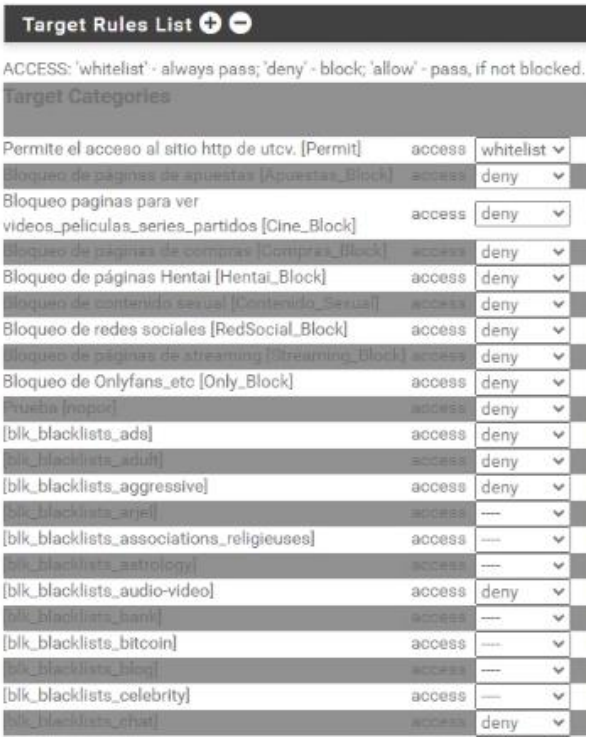


Fig. 3.35. Target list Alumnos Pt.1
Fuente: Elaboración propia

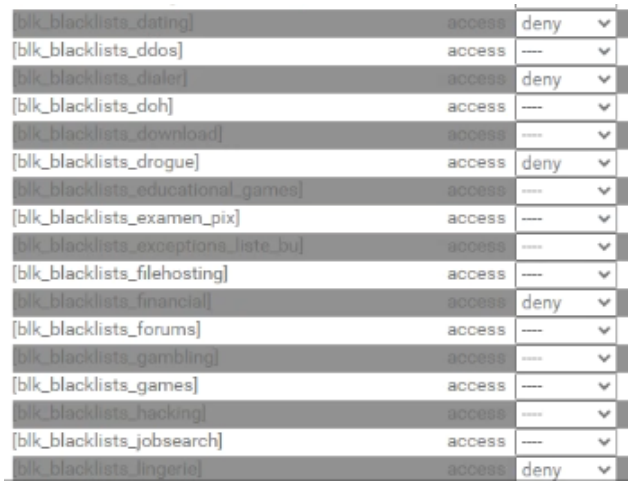


Fig. 3.36. Target list Alumnos Pt.2
Fuente: Elaboración propia

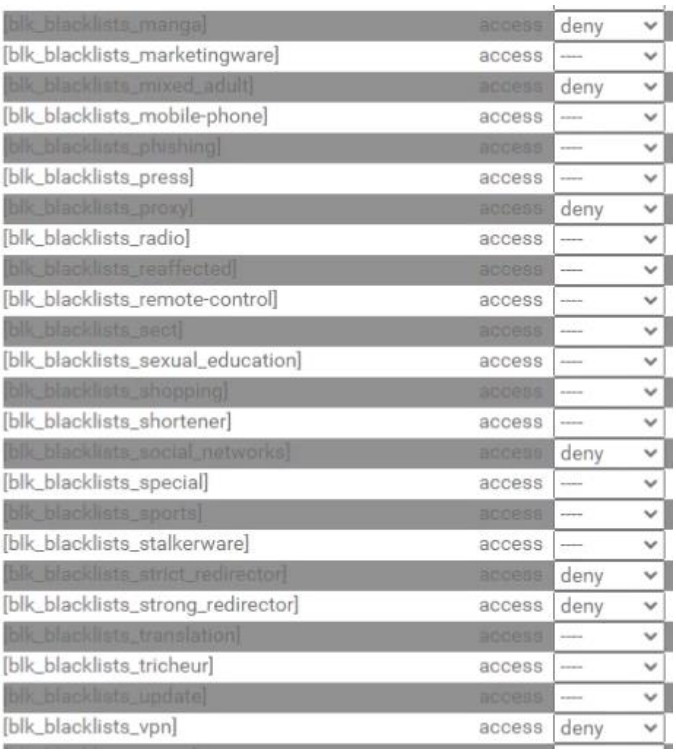


Fig. 3.37. Target list Alumnos Pt.3
Fuente: Elaboración propia

Implementar reglas para el tráfico de red en el firewall pfSense+.

En la sección "Firewall / Alias" del panel de configuración de pfSense+, se configuran Alias para mejorar el control de bloqueo en las reglas entre VLANS. Los Alias facilitan la gestión al agrupar direcciones IP, puertos o redes. Esto optimiza la regulación del tráfico entre VLANS, mejorando la seguridad y el rendimiento de la red. El proceso para la implementación de las reglas es el siguiente:

1. En la sección "Firewall / Alias / IP " del panel de configuración de pfSense+, se presentan los alias que se utilizaron. Sin embargo, las reglas que se aplicaron en realidad correspondieron al alias "ADMINISTRACIÓN". Esta medida se realiza con el propósito de evitar el acceso entre las distintas VLANS,

manteniendo así un nivel adecuado de seguridad y aislamiento entre las redes (Fig. 3.38).

2. El alias "ADMINISTRACIÓN" se configura para denegar el acceso a los sitios de administración de las VLANS 10, 20, 30, 40, 50 y 60. También se negó el acceso al sitio web de configuración de los Access Point que formaban parte de la infraestructura de red. El acceso al sitio web de Proxmox fue bloqueado mediante este alias en las VLANS correspondientes, mientras que el sitio web del firewall pfSense+ no se bloquea, debido a que el propio firewall evita ser negado a sí mismo. Sin embargo, se implementó una contraseña segura para garantizar la protección del firewall (Fig. 3.39).

3. En la interfaz VLAN10 se implementan las siguientes reglas (Fig. 3.40):
   - Una regla permitiendo la comunicación con el DNS local para el bloqueo de sitios web definidos en la lista de destino de esta VLAN.
   - Reglas para denegar toda comunicación con el resto de las VLANS, debido a que se trata de una red de Alumnos.
   - Se bloquea el acceso a sitios de administración utilizando el alias del mismo nombre.
   - Se permite el resto del tráfico para mantener la funcionalidad de la interfaz.

4. En la interfaz VLAN20 se implementan las siguientes reglas (Fig. 3.41):
   - Una regla permitiendo la comunicación con el DNS local para el bloqueo de sitios web definidos en la lista de destino de esta VLAN.
   - Bloqueo al acceso a sitios de administración usando el alias del mismo nombre.
   - Se permite el resto del tráfico para mantener la funcionalidad de la interfaz.
   - Se crearon reglas para denegar toda comunicación con el resto de las VLANS, aunque permanecieron inactivas debido a políticas institucionales.

5. En la interfaz VLAN30 se implementan las siguientes reglas (Fig. 3.42):
   - Una regla permitiendo la comunicación con el DNS local para el bloqueo de sitios web definidos en la lista de destino de esta VLAN.
   - Bloqueo al acceso a sitios de administración utilizando el alias del mismo nombre.
   - Se permite el resto del tráfico para mantener la funcionalidad de la interfaz.
   - Se crearon reglas para denegar toda comunicación con el resto de las VLANS, aunque permanecieron inactivas debido a políticas institucionales.

6. En la interfaz VLAN40 se implementan las siguientes reglas (Fig. 3.43):
   - Una regla permitiendo la comunicación con el DNS local para el bloqueo de sitios web definidos en la lista de destino de esta VLAN.
   - Bloqueo al acceso a sitios de administración usando el alias del mismo nombre.
   - Se permite el resto del tráfico para mantener la funcionalidad de la interfaz.
   - Se crearon reglas para denegar toda comunicación con las otras VLANS, ya que los invitados no necesitaban acceso a otras VLANS.

7. Para la interfaz de rectoría no se aplican reglas debido a que las políticas de la institución no requieren restringir el acceso desde esta VLAN (Fig. 3.44).

8. En el caso de la VLAN de sistemas no se aplican las reglas de igual manera que en la interfaz de rectoría debido a que en esta VLAN se encuentran los encargados del mantenimiento del firewall pfSense+ (Fig. 3.45).

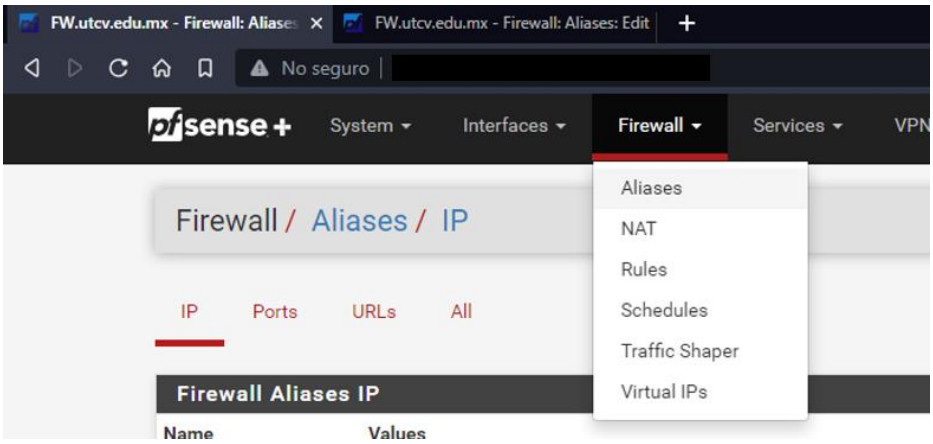


Fig. 3.38. Firewall/Alias Sección
Fuente: Elaboración propia

Fig. 3.39. Firewall Alias IP
Fuente: Elaboración propia

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN40 VLAN50 VLAN60

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✓ 64/26.72 MiB	IPv4 TCP/UDP	VLAN10 net	*	VLAN10 address	53 (DNS)	*	none		VLAN10 DNS LOCAL
☐	✗ 0/0 B	IPv4+6 *	VLAN10 net	*	VLAN60 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN60
☐	✗ 0/392 B	IPv4+6 *	VLAN10 net	*	VLAN50 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN50
☐	✗ 0/0 B	IPv4+6 *	VLAN10 net	*	VLAN40 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN40
☐	✗ 0/11 KiB	IPv4+6 *	VLAN10 net	*	VLAN30 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN30
☐	✗ 0/495 B	IPv4+6 *	VLAN10 net	*	VLAN20 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN20
☐	✗ 0/735 KiB	IPv4 *	*	*	ADMINISTRACION	*	*	none		
☐	✓ 131/7.70 GiB	IPv4 *	*	*	*	*	*	none		

Fig. 3.40. Reglas en interfaz VLAN10
Fuente: Elaboración propia

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN40 VLAN50 VLAN60

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✓ 7/2.30 MiB	IPv4 TCP/UDP	VLAN20 net	*	VLAN20 address	53 (DNS)	*	none		VLAN20 DNS LOCAL
☐	✗ 0/0 B	IPv4+6 *	VLAN20 net	*	VLAN60 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN60
☐	✗ 0/0 B	IPv4+6 *	VLAN20 net	*	VLAN50 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN50
☐	✗ 0/0 B	IPv4+6 *	VLAN20 net	*	VLAN40 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN40
☐	✗ 0/0 B	IPv4+6 *	VLAN20 net	*	VLAN30 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN30
☐	✗ 0/0 B	IPv4+6 *	VLAN20 net	*	VLAN10 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN10
☐	✗ 0/109 KiB	IPv4 *	*	*	ADMINISTRACION	*	*	none		Deniega el acceso a sitios de administración
☐	✓ 36/1.35 GiB	IPv4 *	*	*	*	*	*	none		Permite todo

Fig. 3.41. Reglas en interfaz VLAN20
Fuente: Elaboración propia

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN40 VLAN50 VLAN60

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	1/5.56 MiB	IPv4 TCP/UDP	VLAN30 net	*	VLAN30 address	53 (DNS)	*	none		VLAN30 DNS LOCAL
✗	0/0 B	IPv4+6 *	VLAN30 net	*	VLAN60 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN60
✗	0/0 B	IPv4+6 *	VLAN30 net	*	VLAN50 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN50
✗	0/0 B	IPv4+6 *	VLAN30 net	*	VLAN40 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN40
✗	0/0 B	IPv4+6 *	VLAN30 net	*	VLAN20 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN20
✗	0/0 B	IPv4+6 *	VLAN30 net	*	VLAN10 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN10
✗	0/136 KiB	IPv4 *	*	*	ADMINISTRACION	*	*	none		Deniega el acceso a sitios de administración
✓	25/1.93 GiB	IPv4 *	*	*	*	*	*	none		Permitir todo
✓	0/0 B	IPv4 TCP	VLAN30 net	*	VLAN30 address	53 (DNS)	*	none		Permite únicamente DNS

Fig. 3.42. Reglas en interfaz VLAN30
Fuente: Elaboración propia

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN40 VLAN50 VLAN60

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	0/1.30 MiB	IPv4 TCP/UDP	VLAN40 net	*	VLAN40 address	53 (DNS)	*	none		VLAN40 DNS LOCAL
✗	0/0 B	IPv4+6 *	VLAN40 net	*	VLAN60 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN60
✗	0/0 B	IPv4+6 *	VLAN40 net	*	VLAN50 net	*	*	none		BLOQUEO DE COMUNICACION CON VLAN50
✗	0/0 B	IPv4 *	VLAN40 net	*	LAN net	*	*	none		Bloquea trafico hacía LAN_NET
✗	0/0 B	IPv4+6 *	VLAN40 net	*	VLAN10 net	*	*	none		Bloquea trafico hacía UTCV_ALUMNOS
✗	0/0 B	IPv4+6 *	VLAN40 net	*	VLAN20 net	*	*	none		Bloquea trafico hacía UTCV_DOCENTES
✗	0/0 B	IPv4+6 *	VLAN40 net	*	VLAN30 net	*	*	none		Bloquea trafico hacía UTCV_ADMINISTRATIVOS
✗	0/54 KiB	IPv4 *	*	*	ADMINISTRACION	*	*	none		Deniega el acceso a sitios de administración
✗	0/0 B	IPv4 ICMP any	VLAN40 net	*	*	*	*	none		Bloquear el ping hacia cualquier red
✓	0/36 KiB	IPv4 *	*	*	*	*	*	none		Permitir todo

Fig. 3.43. Reglas en interfaz VLAN40
Fuente: Elaboración propia

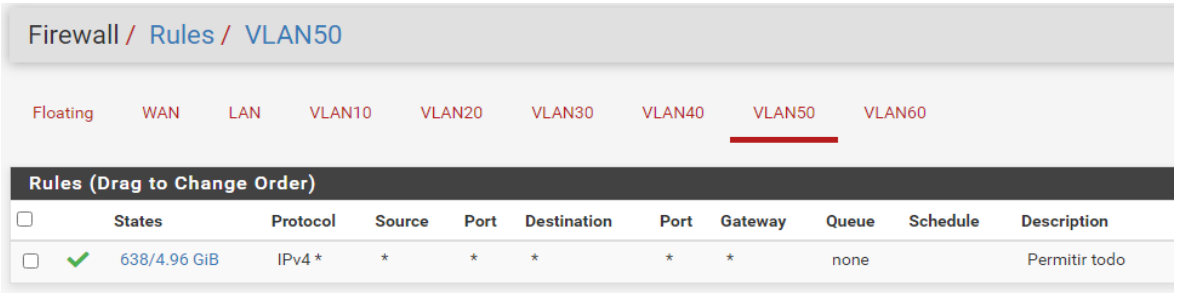


Fig. 3.44. Reglas en interfaz VLAN50
Fuente: Elaboración propia

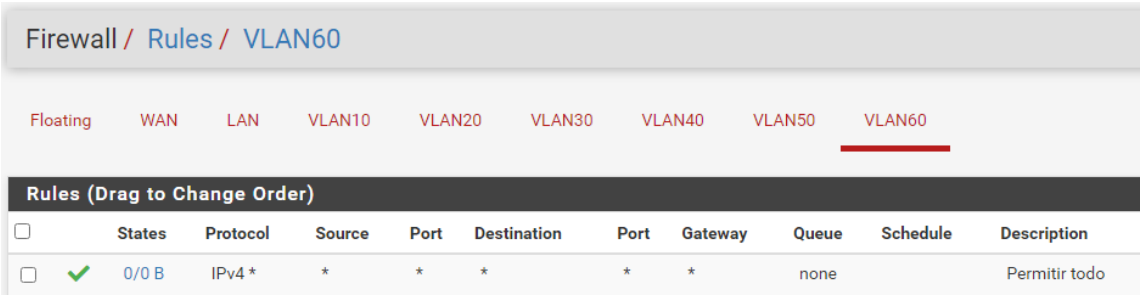


Fig. 3.45. Reglas en interfaz VLAN60
Fuente: Elaboración propia

Limitar anchos de banda en las VLANS dentro del firewall pfSense+.

Una de las políticas por las que se optó para el manejo de la red fue limitar el ancho de banda, para lo cual se realizaron las siguientes configuraciones:

VLAN	Subida (Kbit/s)	Bajada (Kbit/s)
Alumnos	4000	4000
Docentes	10240	10240
Administrativos	12288	12288
Visitantes	Ilimitado	Ilimitado
Rectoría	Ilimitado	Ilimitado

Tabla 3.6. Tabla de anchos de banda
Fuente: Elaboración propia

- El ancho de banda designado para la red de Docentes, el cual resulta suficiente para que los docentes realizaran sus labores e investigaciones para sus alumnos en clase.
- El ancho de banda designado para la red de Administrativos, el cual resulta ser excelente para que el área administrativa de la UTCV pueda realizar sus labores diarias.
- El ancho de banda en el caso de la red de Visitantes y Rectoría es sin límite, esto porque así es delimitado por parte de la institución, ya que se requiere autorización por parte de esta.

3.5 Fase 5: Operar

Durante la fase de operación se realiza un análisis del funcionamiento del firewall pfSense+, evaluando su rendimiento (consumo de recursos) y verificando la efectividad de las políticas de seguridad implementadas y filtrado de sitios web. Esto permitió asegurar que el firewall operara de manera óptima.

Las evidencias generadas en esta fase son las siguientes:

Análisis del funcionamiento del firewall pfSense+.

Se realizaron pruebas en la red inalámbrica para comprobar en funcionamiento del firewall pfSense+ en la infraestructura de red.

1. Bloqueo de sitios web definidos: Gracias a la implementación de nuestro sistema de seguridad, hemos logrado bloquear con éxito sitios web no permitidos. Este logro es resultado de nuestro enfoque en la seguridad en línea y demuestra nuestra capacidad para mantener un entorno seguro y productivo (Fig. 3.46).

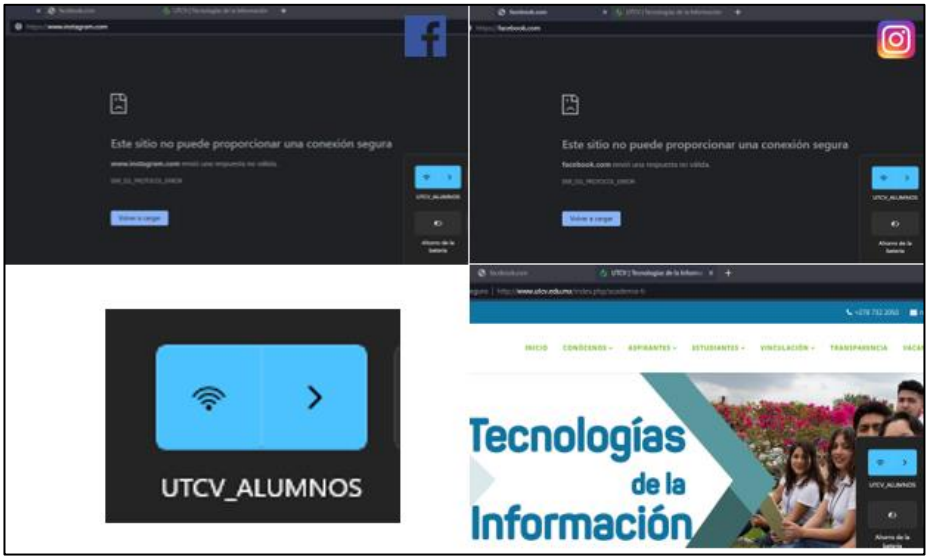


Fig. 3.46. Sitios web bloqueados SquidGuard
Fuente: Elaboración propia

2. Ancho de banda de acuerdo a lo limitado: En este caso no se aprovechó el ancho de banda que se le asignó a cada VLAN debido a que el paquete de internet con el que cuenta la escuela no fue suficiente para cubrir las necesidades de los alumnos y personal de la institución de la UTCV (Fig. 3.47).

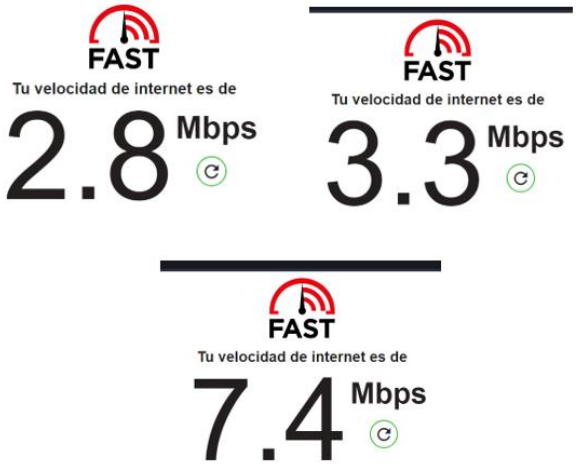


Fig. 3.47. Ancho de banda limitado
Fuente: Elaboración propia

3. Prueba de acceso a la página de administración de Proxmox dentro de la red de Alumnos, la cual está con el acceso denegado de acuerdo a la regla de negar el acceso a sitios web de administración y otra prueba de acceso desde la red de Sistemas hacia la página de administración de Proxmox y el resultado fue el correcto en ambos casos (Fig. 3.48-49).

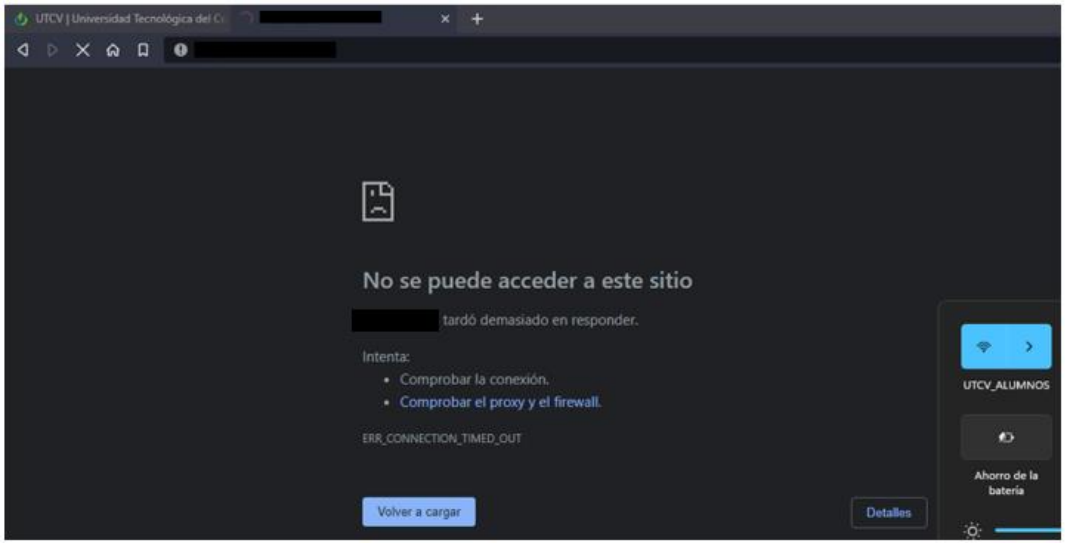


Fig. 3.48. Reglas entre VLANS en funcionamiento
Fuente: Elaboración propia

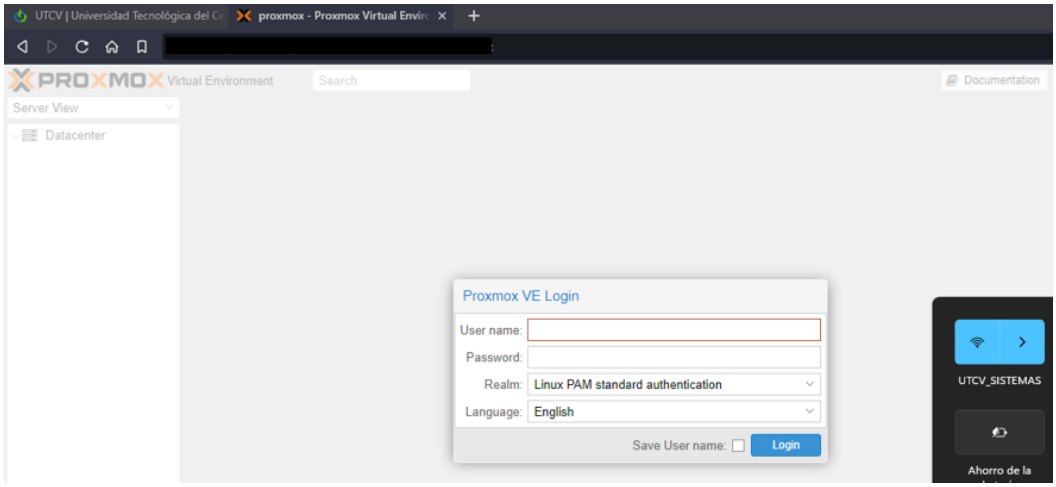


Fig. 3.49. Reglas entre VLANS en funcionamiento 2
Fuente: Elaboración propia

El análisis y pruebas realizadas arrojaron resultados positivos, las interfaces creadas y portales cautivos funcionan en conjunto correctamente, el acceso a sitios web no productivos está controlado, el ancho de banda de la red inalámbrica está definido y cada VLAN consume lo indispensable para no saturar la red y por último las reglas entre las VLANS permiten tener un control de la red misma sobre accesos no deseados entre las mismas.

3.6 Fase 6: Optimizar

A pesar de la exitosa implementación del firewall pfSense+ en la infraestructura de red de la UTCV, Cuitláhuac, Ver., se han identificado ciertos aspectos que requieren atención y mejoras para optimizar aún más el rendimiento y la seguridad de la red.

Se recomienda aumentar la capacidad del plan de internet, ya que uno de los principales problemas que se han identificado es la limitada capacidad del plan de internet con el que cuenta la institución. La gran cantidad de usuarios que hacen uso de la red educativa puede generar congestión y ralentizar el acceso a los recursos en línea, afectando la experiencia de navegación y el desempeño de las actividades académicas. Se sugiere que la institución realice una revisión del plan de internet actual y considere la posibilidad de contratar un plan de mayor capacidad, acorde con la cantidad de usuarios y las necesidades de conectividad de la comunidad educativa.

Otra de las recomendaciones es la implementación de reglas en las VLANS que no se pudieron implementar para mejorar el control y la gestión del tráfico de datos en la red. Se recomienda ampliamente implementar dichas reglas para optimizar en tráfico de la red, como el empleo del QoS (Calidad de Servicio), para priorizar ciertos tipos de tráfico, como el de aplicaciones educativas y herramientas de comunicación, sobre otros tipos de tráfico menos prioritarios. Esto permitirá asegurar que los recursos más relevantes para el ámbito académico tengan un acceso más rápido y confiable, incluso en situaciones de alta demanda de la red.

CAPÍTULO IV. RESULTADOS Y CONCLUSIONES

La fase final de este y cualquier proyecto obliga a recapitular en general un todo lo que se realizó a lo largo de su desarrollo. Es así que durante el apartado de las conclusiones se presentan los aportes que se realizaron mediante la investigación, apoyándose en los resultados que se alcanzaron.

4.1 Resultados

El enfoque principal de la implementación del firewall pfSense+ en la infraestructura de red de la institución educativa UTCV, tuvo el propósito de fortalecer la seguridad y el control del tráfico de datos en su entorno de red educativo. Para lograr este objetivo, se llevaron a cabo diferentes procesos que se alinearon con los objetivos específicos establecidos, los cuales fueron proporcionales a cumplir el objetivo general planteado, los resultados del proyecto se muestran a continuación:

En primer lugar, se logró la creación de una VLAN específica para el área de rectoría. Esta acción permitió separar de manera efectiva el tráfico de red de esta área administrativa, dando un nivel adicional de aislamiento y protección. La implementación de esta VLAN resultó en una mejor organización y control de las actividades del área de rectoría, optimizando la eficiencia en el manejo de su infraestructura de red.

La segmentación de la red del área de sistemas en una VLAN propia, alejándola de la red local (LAN) en donde se encontraba originalmente. Esta decisión se basó en prácticas recomendadas de seguridad, ya que la red de sistemas suele ser un objetivo de alto riesgo para posibles ciberataques. Al ubicarla en una VLAN separada, se redujo la superficie de ataque y se brindó un nivel adicional de protección a esta área vital para el funcionamiento de la institución.

En relación con las políticas de filtrado web, se logró con éxito el bloqueo de sitios web definidos según las políticas establecidas por la institución. La implementación de listas negras específicas permitió restringir el acceso a sitios no productivos,

protegiendo así a los usuarios de contenido inapropiado y reduciendo la posibilidad de amenazas de seguridad. Además, la configuración del firewall pfSense+ para utilizar un servidor de autenticación personalizado facilitó el control de los portales cautivos y proporcionó una experiencia segura y personalizada para cada de usuario.

Una mejora significativa en el rendimiento de la red se alcanzó mediante la limitación de los anchos de banda para cada VLAN. La asignación adecuada de recursos aseguró que cada área de la institución tuviera acceso a la cantidad necesaria de ancho de banda, evitando la saturación y optimizando el rendimiento general de la red. Como resultado, se observó una reducción en los tiempos de respuesta y una mayor estabilidad en el tráfico de datos, lo que contribuyó a una experiencia de usuario más satisfactoria.

Finalmente, se crearon reglas entre las VLANS para limitar el acceso entre ellas, con el objetivo de evitar la fuga de información confidencial y mantener la privacidad y seguridad de cada área de la institución. La configuración de las reglas garantizó que solo el tráfico autorizado pudiera fluir entre las VLANS, aunque por políticas de la institución no en todas las interfaces se lograron aplicar dichas reglas, aun así se brindó una capa adicional de protección y control de la información en las VLANS que si se lograron aplicar dichas reglas.

4.2 Conclusiones

La importancia de implementar un firewall dentro de una infraestructura de red, como es el caso del firewall pfSense+ en la infraestructura de red de la UTCV, Cuitláhuac, Ver., ha demostrado ser de vital importancia para fortalecer la seguridad y el control del tráfico de datos. A lo largo de este proyecto, se han identificado diversos aspectos relevantes que enfatizan la necesidad de contar con un firewall y los conocimientos fundamentales para llevar a cabo su configuración y gestión de manera efectiva, lo que permitió llegar a la conclusión de que la presencia de un firewall en la infraestructura de red es esencial para proteger la información confidencial y salvaguardar la privacidad de los usuarios. La implementación de un firewall brinda

una capa adicional de seguridad contra posibles amenazas y ciberataques, asegurando así la integridad y disponibilidad de los recursos de la red.

La implementación del firewall pfSense+ en la UTCV ha tenido un impacto positivo en la institución al mejorar la seguridad y el rendimiento de la red. La creación de VLANS específicas para áreas específicas y la limitación de anchos de banda han optimizado el tráfico de datos y asegurado un funcionamiento más eficiente en toda la infraestructura de red, de igual manera me permitió adquirir un conjunto de conocimientos en el área de servidores y seguridad de redes. La comprensión de conceptos como VLANS, políticas de filtrado web, control de anchos de banda y reglas de acceso entre redes, resultaron fundamentales para el diseño e implementación exitosa del firewall pfSense+.

Por último, podemos decir que se cumplió la hipótesis planteada al inicio del proyecto, demostrando que la implementación del firewall pfSense+ en la infraestructura de red de la UTCV sería una solución efectiva y adecuada para fortalecer la seguridad y control del tráfico de datos.

Referencias

Aguirre, M. F. (2021, septiembre 14). ¿Qué son los entregables de un proyecto? Ejemplos prácticos. appvizer.es. https://www.appvizer.es/revista/organizacion-planificacion/gestion-proyectos/entregables-de-un-proyecto

Alonso, B. L. (2022). Virtualización con Proxmox VE como alternativa de infraestructura en instituciones de Salud.

Arias, M. L., Acosta, L. A. M., & Ladoy, L. E. (2019.). Estrategia de superación para la utilización de proxmox y pfSense en las instituciones de salud.

Bastidas Orrala, I. J. (2023). Reingeniería de la infraestructura de red de datos física y lógica del Gobierno Autónomo Descentralizado Municipal Santa Elena. [BachelorThesis, La Libertad: Universidad Estatal Península de Santa Elena, 2023.]. https://repositorio.upse.edu.ec/handle/46000/9259

Diaz, J. F. C., Fierro, R. D., & Roldan, J. L. G. (2020). Firewall a nivel de Software en la empresa de vigilancia y seguridad privada Timanco LTDA.

Espin Corrales, D. O. (2022). Diseño e Implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad [BachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/23007

Galeano, S. (2023, enero 26). El número de usuarios de internet en el mundo crece un 1,9% y alcanza los 5.160 millones (2023). Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce. https://marketing4ecommerce.net/usuarios-de-internet-mundo/

Llanes, R. P., & Alonso, R. R. (2020). Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. Revista Cubana de Ciencias Informáticas, 14(1). https://www.redalyc.org/journal/3783/378365895002/html/

Morales Chapman, J. A., & Torres Leiva, N. (2021). Implementación de una red privada virtual basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C. Repositorio Institucional - UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/74675

Ortega, C. (2021). ¿Qué es la metodología de la investigación? QuestionPro. https://www.questionpro.com/blog/es/metodologia-de-la-investigacion/

Ortega, C. (2021). Investigación mixta. Qué es y tipos que existen. QuestionPro. https://www.questionpro.com/blog/es/investigacion-mixta/

Parra, A. (2020). Cuáles son los tipos de variables en una investigación. QuestionPro. https://www.questionpro.com/blog/es/tipos-de-variables-en-una-investigacion/

Piarpuezán López, J. A., & Riascos Ortiz, D. A. (2021). Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020 [Thesis, UPEC]. http://www.repositorio.upec.edu.ec/handle/123456789/1288

Pimazzoni, D. R. N. (2020). El financiamiento de la educación pública en México / The financing of public education in Mexico. ARTSEDUCA, 25, Article 25. https://www.e-revistes.uji.es/index.php/artseduca/article/view/4277

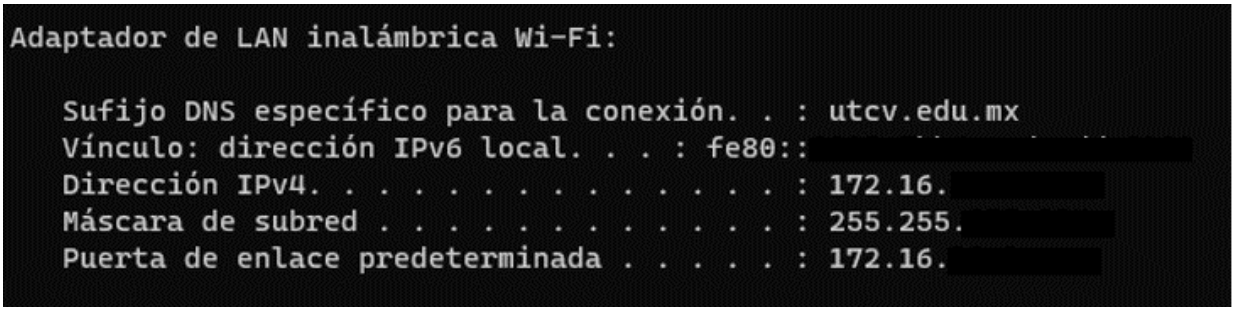
Sampieri, R. H. (2010). Metodología de la Investigación (Sexta ed.). Ciudad de México: Mc Graw Hill.

Zubirán, P. de la L., Zubirán, M. A. de la L., & García, A. de la L. (2022). Los instrumentos de la investigación científica. Hacia una plataforma teórica que clarifique y gratifique. Horizonte de la Ciencia, 12(22), 189-202. https://www.redalyc.org/journal/5709/570969250014/html/

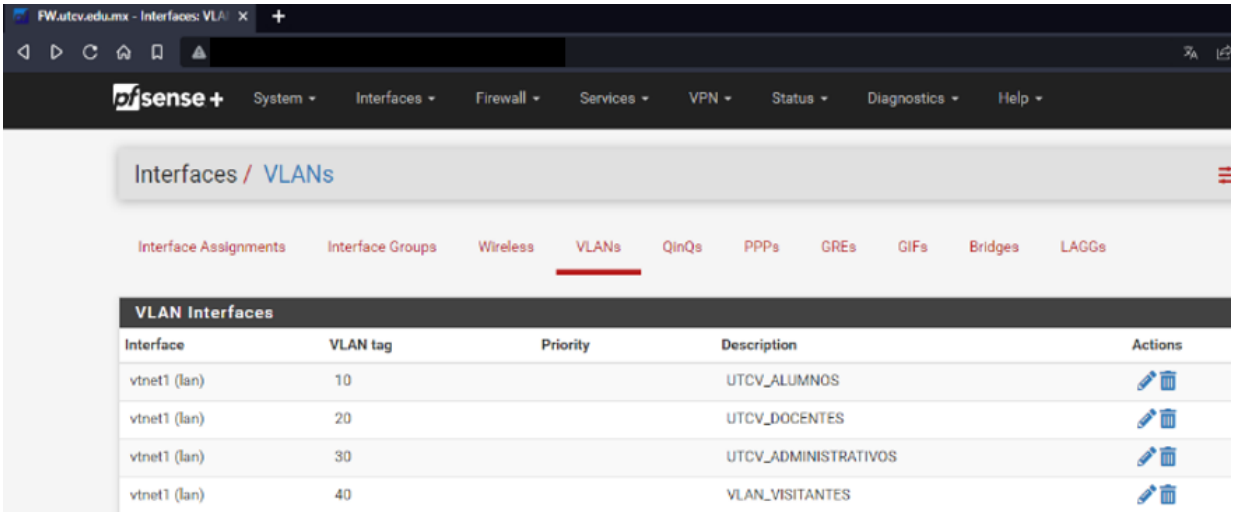
Anexos

Anexo A. Observación no estructurada

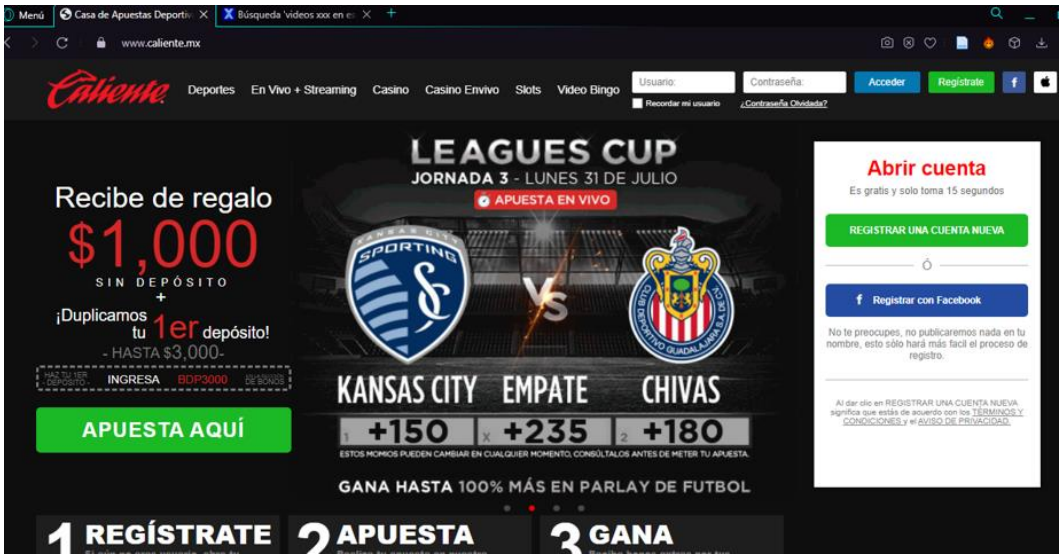
- Red de sistemas está sobre la LAN.
- Red de sistemas no separada del segmento de red.
- Direcciones IP de la LAN dadas por la red de sistemas actual.



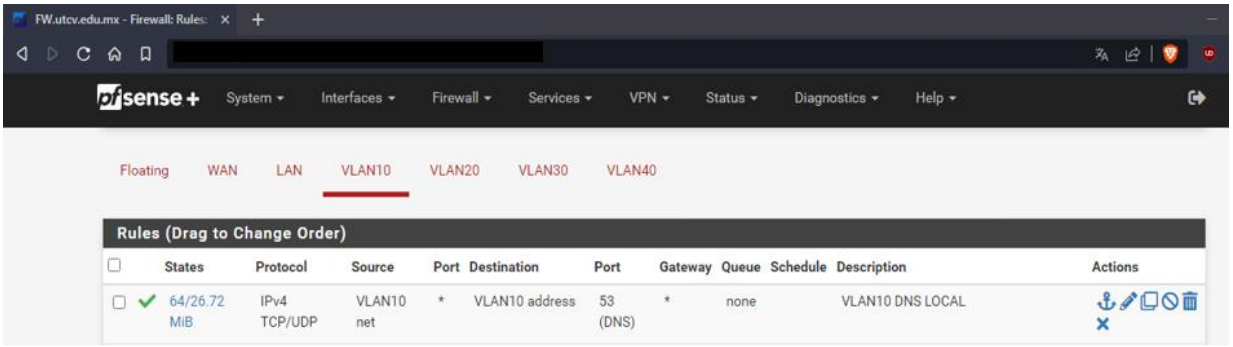
- Inexistencia de VLAN de rectoría.

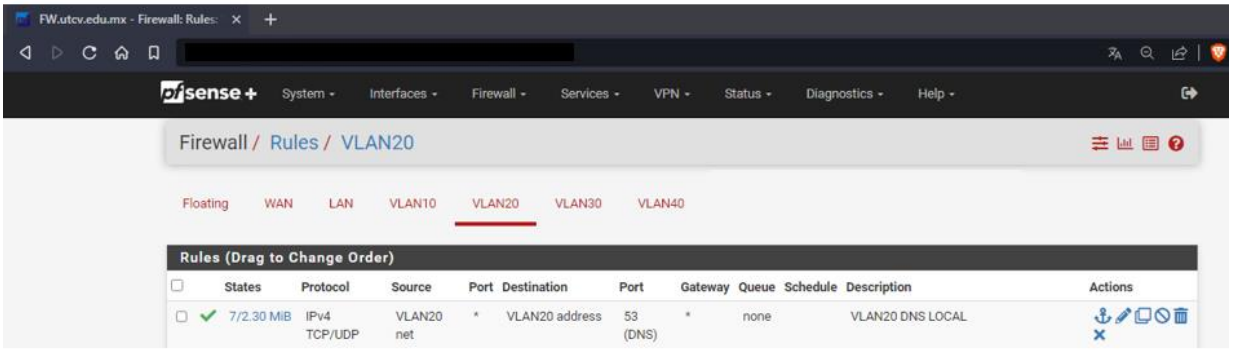


- Filtrado de contenido poco eficiente o nulo.



- Reglas inexistentes entre VLANS.
- Solo se permite, pero no se deniega tráfico de algún tipo.
- Cualquier VLAN puede acceder a las demás.





Anexo B. Cronograma de actividades

Actividad	Inicio de la actividad	Duración de la actividad	Inicio real	Duración real	Porcentaje completado	Semanas														
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Fase de Preparación																				
Reconocimiento de la problemática y mejora de la misma	1	1	1	1	100%															
Reporte de estudio de campo del firewall existente (PfSense+)	1	1	1	1	100%															
Creación de copias de seguridad del firewall existente (PfSense+)	1	1	1	1	100%															
Fase de Planeación																				
Realizar un análisis de requerimientos	2	1	2	1	100%															
Fase de Diseño																				
Diseño lógico	2	1	2	1	100%															
Diseño físico	2	1	2	1	100%															
Tabla de direccionamiento con las interfaces en PfSense+	3	1	3	2	100%															
Fase de Implementación																				
Actualizar firewall PfSense+	4	1	4	1	100%															
Crear VLANS faltantes dentro del firewall PfSense+	4	1	4	1	100%															
Implementar políticas de filtrado web específicas en el firewall PfSense+	5	2	5	3	100%															
Implementar reglas para el tráfico de red en el firewall PfSense+	6	2	6	2	100%															
Limitar anchos de banda en las VLANS dentro del firewall PfSense+	7	2	7	3	100%															
Fase de Operación																				
Análisis del funcionamiento del firewall PfSense+	12	2	12	2	100%															
Listado de errores detectados	14	1	14	1	100%															
Fase de Optimización																				
Informe de corrección de errores	15	1	15	1	100%															
Reporte técnico	15	1	15	1	100%															
Cierre de estadía	15	1	15	1	100%															

Anexo C. Tabla de dispositivos y características

Dispositivo	Nombre	Características
	Cisco - WS-C3560-12PC-S - Catalyst 3560 Compact 12 Switch POE.	✓ Capacidad duplex, ✓ Conmutación Layer 3, conmutación Layer 2, auto-sensor por dispositivo, Encaminamiento. ✓ IP, soporte de DHCP. ✓ Alimentación mediante Ethernet (PoE), negociación automática. ✓ Concentración de enlaces, soporte VLAN. ✓ Señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico.
	Servidor HP ProLiant ML350 G6, en el cual montamos el firewall pfSense.	✓ Procesador Intel Xeon E5645 (2.40GHz, 12MB, 6 núcleos, 80 Watts). ✓ Corriente: 750 Watts, Hot Plug ✓ 32 GB RAM ✓ 1 x HP HH SATA DVD-ROM ✓ Interfaz del HDD Serial Attached SCSI (SAS) ✓ 2 disco Duro Hp 900-gb ✓ Controlador de Red

		✓ 1 x NC362i, 1 GbE de 2 puertos ✓ Controlador de Almacenamiento ✓ Smart Array P410i/256MB
	5 puntos de acceso Aironet 1815i de Cisco	✓ Proporciona conectividad 802.11ac Wave 2 con el doble de velocidad de 802.11ac.

Anexo D. Checklist

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ	Implementación del firewall pfSense+ dentro de la infraestructura de red de la UTCV			
	Lista de verificación		Versión 1.0	
Proceso: Finalización del proyecto		Prácticante: José Guadalupe Cid Olmedo		
Universidad Tecnológica del Centro de Veracruz, Cuitláhuac, Veracruz.				
Detectar el antes y después de la implementación del proyecto en la institución de la Universidad Tecnológica del Centro de Veracruz.				
Pruebas	**Antes**		**Después**	
	X	☑	X	☑
VLAN para el área de rectoría	X			☑
Área de sistemas separada de la LAN en una VLAN	X			☑
Bloqueo sitios web configurado de manera eficiente	X			☑
Límites de ancho de banda por VLAN adecuados		☑		☑
Reglas de firewall adecuadas entre las VLAN	X			☑
Contraseñas robustas implementadas	X			☑