UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

"PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL INFORMÁTICO DE UN CENTRO DE DATOS DE UNA INSTITUCIÓN MUNICIPAL".

AUTOR

Bacilio Espinoza, Edison Rodolfo

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Lídice Haz López, Msi.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. Jose Sanchez A. Msc.
DIRECTOR DE LA CARRERA

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Lídice Haz López, Msia.
TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Y. Msia
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

Ing. Marjorie Coronel S. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por BACILIO ESPINOZA EDISON RODOLFO, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 06 días del mes de diciembre del año 2023

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. HAZ LÓPEZ LÍDICE, MSI.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **BACILIO ESPINOZA EDISON RODOLFO**

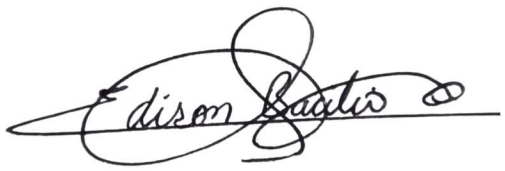
DECLARO QUE:

El trabajo de Titulación, "Propuesta de un sistema de seguridad perimetral informático de un centro de datos de una institución municipal" previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La libertad, a los 06 días del mes de diciembre del año 2023

EL AUTOR



Edison Rodolfo Bacilio Espinoza

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado (Propuesta de un sistema de seguridad perimetral informático de un centro de datos de una institución municipal), presentado por el estudiante, BACILIO ESPINOZA EDISON RODOLFO fue enviado al Sistema Anti-plagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. HAZ LÓPEZ LÍDICE, MSI.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

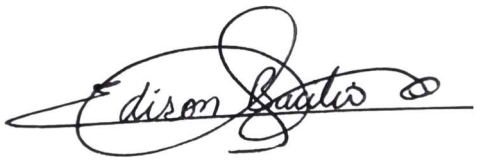
Yo, **BACILIO ESPINOZA EDISON RODOLFO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 06 días del mes de diciembre del año 2023

EL AUTOR



Bacilio Espinoza Edison Rodolfo

AGRADECIMIENTO

Quiero en primer elevar mi corazón en gratitud a Dios, la fuente de toda gracia y amor, por guiar mis pasos en este viaje de tesis. Tu sabiduría infinita y tu amor incondicional me han sostenido en los momentos de desafío y me han inspirado a alcanzar mis metas académicas.

A mi familia, por su amor incondicional, apoyo emocional y paciencia a lo largo de esta travesía académica. Sin su apoyo, esta tesis no habría sido posible.

A mis amigos y compañeros de clase, quienes me brindaron ánimo, aliento y momentos de distracción cuando más los necesitaba. Gracias por ser parte importante de esta importante etapa.

Agradezco a mis profesores por compartir su conocimiento y por inspirarme a seguir explorando mi campo de estudio.

Por último, pero no menos importante quiero expresar mi profundo agradecimiento a la Ing. Haz Lídice López por su orientación, apoyo constante y sabiduría durante todo el proceso de investigación. Su dedicación y experiencia fueron fundamentales para el éxito de este proyecto.

Edison Rodolfo, Bacilio Espinoza

DEDICATORIA

Este trabajo va dedicado de manera especial a mis padres, quienes me han brindado amor incondicional, orientación y oportunidades invaluables a lo largo de mi vida. Todo lo que he logrado se debe a su sacrificio y apoyo constante.

A mis queridos hermanos, cuya presencia y amistad han sido un regalo invaluable en mi vida. Juntos hemos compartido risas, desafíos y triunfos, y su respaldo ha sido inquebrantable.

A mi familia extendida, quienes han estado presentes en cada paso de mi camino, brindando su apoyo y cariño sin condiciones. Vuestra unidad y amor son un faro de fortaleza y comprensión.

A mis amigos más cercanos, quienes han sido mi red de apoyo inquebrantable. Vuestra amistad ha iluminado mi camino y ha hecho que este viaje sea significativo y memorable.

Edison Rodolfo, Bacilio Espinoza

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto de titulación “Propuesta de un sistema de seguridad perimetral informático de un centro de datos de una institución municipal”, tiene la finalidad de dar una propuesta de seguridad perimetral restructurando la arquitectura de red de una institución municipal, luego de la recolección de información y estudio de vulnerabilidades se pudo denotar la falta de seguridad hacia los sistemas informáticos teniendo problemas para brindar un buen servicio a sus habitantes.

En el presente trabajo se utilizó método científico de recolección de información como la entrevista y observación en donde se pudo reconocer la actual arquitectura de red que cuenta la institución, siendo este muy básico para brindar una seguridad adecuada, para llevar adelante este trabajo se planteó utilizar la metodología para el diseño de redes Top-Dow el cual se adaptó para el desarrollo de este.

El resultado del proyecto de titulación es una nueva arquitectura de red virtualizada que va a simular la estructura rediseñada de la institución, estableciendo reglas de seguridad.

Palabras claves: Seguridad perimetral, Firewall, Arquitectura de red

ABSTRACT

The present degree project "Proposal for a computer perimeter security system for a data center of a municipal institution", has the purpose of providing a proposal for perimeter security by restructuring the network architecture of a municipal institution, after the collection of information and study of vulnerabilities, it was possible to denote the lack of security towards computer systems having problems providing a good service to its inhabitants.

In this work, a scientific method of collecting information was used, such as interview and observation, where it was possible to recognize the current network architecture that the institution has, this being very basic to provide adequate security. To carry out this work, it was proposed to use the methodology for the design of Top-Dow networks which was adapted for its development.

The result of the degree project is a new virtualized network architecture that will simulate the redesigned structure of the institution, establishing security rules.

Keywords: Perimeter security, Firewall, Network architecture

INTRODUCCIÓN

Los gobiernos municipales son instituciones del estado de Ecuador que ofrecen servicios de distinta indoles a la comunidad que se especifica en la fase recolección de información, pero si bien es cierto muchas veces estas instituciones enfrentan grandes problemas de seguridad. La propuesta de un rediseño de red permitirá frenar alguno de los problemas de seguridad que afrontan estas instituciones estableciendo reglas de seguridad que lleven a proteger los datos que esta empresa maneja, la nueva arquitectura de red nos ayudara a segmentara los diferentes departamentos restringiendo y dando privilegios a usuarios según sus necesidades, esto llevara a cubrir la mayoría de las falencias que se enfrentan estas instituciones.

Este trabajo para su ejecución se ha dividido en 3 capítulos:

Capítulo I: En este capítulo, se abordan los antecedentes que condujeron a la formulación de la propuesta. Se comienza por recopilar información sobre un estudio de las problemáticas actuales que pueden afrontar estas instituciones y se proporciona una descripción detallada del proyecto. Se especifica la metodología y las herramientas que se utilizarán y se presentan los objetivos que se deben cumplir, junto con su justificación. Además, se delimita el alcance de la propuesta planteada.

Capítulo II: En este segundo capítulo, se aborda el marco conceptual, donde se definen los conceptos clave relacionados con la investigación. Se presta especial atención a la comprensión de sus significados. En el marco teórico, se recopilan ideas, teorías fundamentales y factores investigativos que son esenciales para el estudio. Estos elementos se explican en detalle y se proporcionan referencias relevantes. La metodología de investigación se basa en técnicas de recolección de datos, como entrevistas y observación en un establecimiento para poder plantear el problema, esto brindara información precisa y útil para el desarrollo de la propuesta.

Capítulo III: En este tercer capítulo, una vez que se han obtenido los requerimientos del proyecto, se procede a llevar a cabo las etapas de la metodología Top-Down. Estas etapas incluyen la recopilación de información, el análisis de requerimientos, la evaluación de opciones comerciales y la presentación de un modelo propuesto para su implementación. El capítulo culmina con conclusiones y recomendaciones específicas derivadas del proyecto.

CAPITULO I. FUNDAMENTACIÓN

1.1 Antecedentes

Actualmente las empresas llevan datos en forma digital, teniendo estructuras tecnológicas donde se almacena estos, por eso es una prioridad proteger estos a posibles ataques. De acuerdo con cifras de la firma Fortinet, se producen 545000 intentos de intrusión en las redes cada minuto y se neutralizan más de 140000 programas de programa maligno cada 60 segundos en el mundo. En un informe revelador llamado Global Cibersecutiry Index de la ITU (International Communication Union), Ecuador se ubica en el puesto 9 de América y en el 65 a nivel mundial con respecto a materia de ciberseguridad [1].

Las entidades municipales son empresas del estado que la mayoría de veces constan de un Centro de Datos que está bajo el cargo de un departamento de sistemas, la estructura de su red con las que cuentan estas instituciones son muy antiguas ya que no se han ido actualizando con el paso de la tecnología, considerando que estas instituciones son empresas medianas se puede decir que cuenta con una cantidad aproximada de 200 usuarios que están conectados a la red y también fuera de esta se proveen la red a otros lugares por medio de antenas.

El centro de datos por lo general se encuentra dentro de la institución y puede estar conformado por un Router principal que nos da acceso a la red y a la vez este puede compartir red para las otras extensiones, tomare como ejemplo un municipio en el que consta de 5 servidores, de Correo, Web, Proxy, Base de datos, Almacenamiento, también consta con telefonía IP y cámaras de vigilancia, puede tener gran cantidad de Switches que repartan la red a los diferentes departamentos de un municipio como alcaldía, vicealcaldia, desarrolló comunitario, coactiva, salud ocupacional, comunicación, talento humano, obras públicas, catastro, jurídico, turismo y comunicación (Ver anexo 1).

Esta institución municipal tiene una segmentación por IP que del switch principal reparte a otros switch en cascada y da red a los diferentes departamentos, siendo esta una red plana donde todos los usuarios tanto administrativos como finales están conectados en la misma red, desde ahora describiendo este escenario se puede evidenciar fallos en la red, los usuarios pueden presentar problemas como es quedarse sin red pero no por el

proveedor sino que las maquinas están infectadas con virus, siendo una falencia la falta de políticas en el firewall que no permitan la entrada de estos.

Por estos problemas se puede evidenciar que la infección de malware puede afectar en la producción diaria de los empleados de la institución municipal, pueden dejar a estos servidores con varias horas sin el servicio, hasta solucionar el problema, esto a su vez causa molestias a los usuarios que acuden a esta institución a realizar sus trámites. Si bien es cierto esta puede a llegar a ser una simple infección de un usuario en una máquina se puede propagar rápidamente a las otras máquinas ya que todas se encuentra en el mismo sector sin una adecuada segmentación.

La empresa tiene firewalls que llegan a proteger la red de ataques y amenazas, pero este no es lo suficiente seguro ya que no suelen ser adecuadamente dimensionadas, llegando a vulnerar estos mediante explotaciones a vulnerabilidades, la data en este escenario es vulnerable a robo o falsificación de información sumamente sensible, esto se puede dar porque otras personas ajenas a la institución o los mismos usuarios tienen información de algunos procesos o credenciales que no deberían conocer y pueden hacer mal uso de esta si ningún control ni monitoreo.

Existen varios estudios en cuanto a la seguridad de un centro de datos, en el trabajo de Carlos Manuel Fabuel Díaz de Madrid implemento un sistema de seguridad perimetral, pero haciendo un análisis a las principales fabricantes de equipos para establecer esta seguridad configurando el equipo, en ciertas empresas se tiene que buscar una mejor alternativa ya que son equipos tecnológicos de un costo que no es bajo [2].

En el trabajo de Kenny Esleyther Ruiz Vieira y Wilson Delgado Ramos de Perú se hizo una Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, en el cual implementaron seguridad perimetral en ámbito de software con los requerimientos perimetral DMZ, se utilizó PFSense que es un software libre que permite solucionar inconvenientes de seguridad sin tener que gastar en un equipo físico [3].

El proyecto de José Vicente Núñez Noboa de la ciudad de guayaquil donde realizo un diseño e implementación de seguridad perimetral para la infraestructura de la empresa FASAKO S.A. usando herramientas Open Source se implementó herramientas como lo es el firewall Router pfSense, el IDS e IPS Snort, el acceso remoto Open VPN, el servicio

de monitoreo Ntopng y un formador de tráfico de red, siendo el estudio de este es bastante completo y se tomara referencia de este para nuestro trabajo [4].

Por el escenario antes mencionado en cuanto a problemas presentes de seguridad se ha planteado una solución para reducir los riesgos de ataques e infecciones en una red municipal que puedan afectar a los datos que se encuentran alojados y al funcionamiento normal de la red, el presente trabajo se plantea una solución de seguridad perimetral a través de implementar un firewall de software libre, que pueda verificar que nuestra red está protegida a posibles ataques que proteja la información que entra y sale de la red, siendo esta de vital importancia y vale tener en cuenta la seguridad perimetral de estas instituciones ya que existe sensible y muy importante información.

Descripción del proyecto

En los gobiernos municipales se manejan datos de gran importancia al ser una institución gubernamental, esto lleva a que sea vulnerables a ataques informáticos con el objetivo de robar esta información. Pero no solo de personas ajenas a la institución representan un riesgo, los mismos usuarios que están en la red ponen en riesgo el centro de datos, por la falta de control en la navegación que pueden llegar a infectar la red.

Se va a proponer un sistema de seguridad perimetral informático, que se trata de la primera línea de defensa en un centro de datos, que se va a encargar de proteger los sistemas y dispositivos en tiempo real de la red tratando de evitar el acceso de usuarios no identificados o sin autorización tanto de redes internas o externas [5].

La seguridad perimetral informática tiene como objetivo cumplir cuatro pilares fundamentales que son: [5]

- Soportar ataques que sean externos a la red
- Monitorizar la red para detectar los ataques recibidos y dar reporte de estos.
- Aislar y segmentar los sistemas o servicios referente a los ataques recibidos.
- Filtrar y bloquear el tráfico no permitido en la red

El presente proyecto describirá las características a implementar en un sistema de seguridad perimetral de acuerdo con el análisis y estudio de un centro de datos de una institución municipal, esto llevara a que la investigación sea de tipo descriptiva, siendo

no experimental, va a llevar a cabo el levantamiento de información, su análisis, planeación y diseño de este, aplicando los parámetros de una seguridad perimetral [6].

Para poder cumplir con todo lo antes mencionado este proyecto se va a dividir en fases que van a partir del modelo par de diseño de redes Top-Dow que cuenta con 6 fases, analizar Requerimientos, desarrollar diseño lógico, desarrollar diseño físico, probar, optimizar y documentar diseño, implementar y probar red, monitorear y optimizar red [7].

Se va a ser uso de cuatro fases para este proyecto como se realizó en el trabajo de José Vicente Núñez Noboa con su tema de Diseño e implementación de seguridad perimetral para la infraestructura de la inmobiliaria FASAKO S.A. usando herramientas open source por esto al igual en ese proyecto se va a implementar cuatro fases [4].

A continuación, se va a describir las cuatro fases en la que se ha divido el proyecto:

Fase 1: Levantamiento de información:

- Estudio de la arquitectura presente en la red.
- Equipos presentes en la actual infraestructura de la red.
- Análisis del actual estado de la red.

Fase 2: Análisis de requerimientos:

- Identificar los activos críticos.
- Evaluar las amenazas potenciales.
- Definir los requisitos de seguridad.
- Evaluar restricciones y regulaciones.
- Documentar los requerimientos

Fase 3: Evaluación comercial:

- Soluciones UTM.
- Evaluación Técnica.
- Soluciones por Hardware.
- Soluciones por Software.

Fase 4: Propuesta del modelo a implementar:

- Rediseño de infraestructura.
- Sistema de firewall y programas a implementar.

- Sistema de detección de intrusos.
- Análisis solución de implementación.

Para poder llevar a cabo cada el estudio actual de la red es necesario usar herramientas para su análisis, que son catalogadas como herramientas de Ethical hacking ya que se va a ser uso de ellas para una auditoria autorizada de la red.

- Nslookup: El mandato NSLOOKUP se utiliza para consultar servidores de nombres para poder localizar información sobre los nodos de red [8].
- Nmap: Es una fuente gratuita y abierta utilidad para el descubrimiento de redes y la auditoría de seguridad [9].
- Whois: Es un conjunto de instrucciones comúnmente empleados para acceder a bases de datos que contienen información sobre usuarios registrados o sucesores de un recurso en Internet, como un nombre de dominio, un rango de direcciones IP o un sistema autónomo [10].
- Netcraft: Esta proporciona análisis sobre la participación en el mercado de servidores y servicios de alojamiento web, lo que implica la identificación del tipo de servidor web y sistema operativo utilizado [11].
- Nmap: La herramienta de red más completa para administradores y usuarios. Monitoriza redes y equipos y permite detectar vulnerabilidades antes de que sean aprovechadas por atacantes para entrar sin autorización a nuestros equipos [12].
- Shodan: Esta es una herramienta de busque da por direcciones IP, esta nos permite recopilar información de los dispositivos o servicios que ese encuentran en la red, esta herramienta en línea permite identificar los sistemas que se ejecutan y poder detectar posibles vulnerabilidades [13].

Este proyecto en relación con la seguridad del centro de datos y su infraestructura en cuanto a la seguridad perimetral en una empresa contribuirá a la línea de investigación Tecnologías y Gestión de la Información, debido a que la propuesta está relacionada con temas de infraestructura y seguridad de las tecnologías de la información, virtualización y seguridad de la información que permitan generar información indispensable para la toma de decisiones en la empresa [14].

1.3 Objetivos del proyecto

Objetivo general

Diseño de un sistema de seguridad perimetral para una institución municipal mediante el uso de herramientas open source que contribuyan con la administración de la seguridad del centro de datos, basados en el diagnóstico y diseño de la red.

Objetivos específicos

1. Realizar un análisis comparativo del software de seguridad perimetral mediante una matriz de evaluación de características.
2. Determinar el estado actual de la red para la identificación de las vulnerabilidades existentes en el centro de datos.
3. Rediseñar el esquema de la red aplicando el sistema de seguridad perimetral del centro de datos de la institución municipal.
4. Implementar un laboratorio de pruebas mediante el uso de máquinas virtuales para evaluar las políticas de seguridad de la red propuesta.

1.4 Justificación del Proyecto

El cambio a una economía digital ha aumentado con esto la dependencia de las empresas en los sistemas de TI en cuanto al ámbito de seguridad los cambios se han vuelto altamente cambiantes y en constante evolución para estar a la vanguarda en protección, el cambio que las empresas necesitan es ir más allá del enfoque tradicional de detectar y solucionar problemas, la estrategia de seguridad más eficaz es para prevenir y analizar posibles amenazas [15].

En la mañana del 16 de abril del 2022, la infraestructura tecnológica de la Dirección Metropolitana de Informática (DMI) del Municipio de Quito, fue objeto de un ciberataque. El origen fue un malware (software hostil intrusivo, virus informático) de tipo Ransomware, como consecuencia se afectaron los servicios automatizados con los cuales la municipalidad atiende a la ciudadanía [16].

Como se puede verificar en Ecuador no estamos acentos de estos ataques que afectan a las instituciones del estado, si bien esto se puede llegar a mitigar con un buen control del ataque es mejor tener una barrera que ayude a cubrir estos ataques en caso de que se den, sin necesidad de estar buscando soluciones al momento del ataque.

Al momento de realizar este proyecto existen proxys dentro de estas instituciones que controla el tráfico de red, pero no es del todo segura, ya que la red se encuentra infectada y existen varias infecciones no localizadas, es cierto que la mayoría de las instituciones pueden seguir trabajando con una normalidad aceptable pero no es seguro que los datos que se encentran en estas instituciones no estén protegidos y que personas no autorizadas puedan tener accesos que no deberían tener.

Por esto se plantea un sistema de seguridad perimetral que va a ser la primera barrera de seguridad de cara al internet, ayudando a controlar la entrada y salida de usuarios al sistema, poder monitorizar el sistema para ver su estado actual es una necesidad para poder tener el control total de este. El diseño es una propuesta que se va a plantear sobre el sistema que actualmente está empleado no pretende ser 100% seguro porque nunca se puede proteger algo al máximo, pero si pretende ayudar a mitigar y controlar la mayoría de estos problemas.

En relación con la propuesta del sistema se pretende proveer una solución con un sistema de código abierto que ayuda al ahorro de costo para estas instituciones, porque es cierto que existen equipos que hacen este trabajo sin mucha necesidad del ser humano, pero a su vez su costo es muy elevado y lo que se pretende es dar una solución que ayude y no tenga costos excesivos de implementación.

El presente proyecto está direccionado al plan nacional de desarrollo, haciendo énfasis en el eje 2, el cual detalla lo siguiente:

Eje 2: Economía al servicio de la sociedad [17].

Objetivo 5: Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [17].

Política 5.6: Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [17].

1.5 Alcance del Proyecto

Tomando como principal guía el objetivo general que menciona el diseño de un sistema de seguridad perimetral para una institución municipal mediante el uso de herramientas

open source que contribuyan con la administración de la seguridad del centro de datos, basados en el diagnóstico y diseño de la red; se procede a realizar dicho objetivo mediante un levantamiento de información de la infraestructura de una institución municipal. Cabe recalcar que el alcance de este proyecto tiene la finalidad desarrollar un sistema de seguridad perimetral ayudando a minimizar los problemas de inseguridad que existen y verificamos mediante el levantamiento de una red virtualizada, llegando a realizar una propuesta mas no se los va a implementar en un ámbito real.

Fase 1: Levantamiento de información y pruebas:

En este apartado se va a levantar información del estado actual en la que se encuentran estas instituciones, pero si bien es cierto se va a levantar información solo dentro de la institución principal, ya que como se mencionó antes existen más infraestructuras anexadas a estas de las cuales no se va a incluir en el actual proyecto.

Fase 2: Análisis de requerimientos:

En el análisis de los requerimientos se va a realizar un estudio a la red y al centro de datos, buscando fallos o vulnerabilidades, se va a hacer un análisis de para poder localizar fallas que estén afectando al centro de datos, esto con el fin de identificar problemas y plantear los requerimientos que necesita el sistema.

Fase 3: Evaluación comercial:

Se va a realizar un estudio de los posibles equipos de hardware y de sistemas de software que ayudan a implementar un sistema de seguridad perimetral y se va a proporcionar las características y costos de estos para dar a conocer el precio de su implementación.

Fase 4: Propuesta del modelo a implementar:

Luego de saber cómo es el sistema y cómo funciona, se analiza los problemas, verificar los requerimientos del sistema y la evaluación comercial se va a llegar a proponer un sistema que se acople a las necesidades de estas instituciones municipales, pero va a ser más un estudio y una simulación, mas no es un escenario real, sino que será propuesto de acuerdo con toda la información levantada.

CAPITULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 Marco Conceptual

2.1.1 Infraestructura de sistemas

La infraestructura del sistema incluye servidores, estaciones de trabajo, portátiles, dispositivos móviles y dispositivos de red cubiertos por el reglamento anterior equipo de sistemas de información de la organización. Las mayores amenazas para el equipo son físicas: daño por incendio, inundación y tormenta otros desastres. En la mayoría de los casos, lo mejor es luchar contra ellos. las amenazas son una adecuada planificación de recuperación ante desastres y Continuidad del negocio. El propósito de las principales amenazas planteadas por Internet son los programas que se ejecutan en estas máquinas y los datos almacenado en ellos [18].

2.1.2 Plataformas de Hardware

En el renglón de computadoras existe una amplia gama de plataformas de hardware y servidor, que varía en función de la tecnología y características utilizadas. Es importante tener armonía y compatibilidad entre plataformas plataforma de hardware y software porque de ella dependerá la estabilidad se implementan características y servicios [19].

2.1.3 Plataformas de Sistemas Operativos

Sistema operativo escalable, compatible, seguro, fiable y asequible es el primer requisito para TI. Hay muchas posibilidades y varían de unas a otra arquitectura en la que se quieren implementar diferentes servicios, o función. Cada plataforma tiene mecanismos de seguridad incorporados una línea de base que se puede aumentar para mejorar la seguridad.

2.1.4 Arquitectura de una red empresarial

Microsoft Corporation define la arquitectura de red corporativa en su sitio web, como regla general, hay tres zonas:

Red fronteriza: Esta red está conectada directamente a Internet a través de un enrutador que debe proporcionar nivel inicial de protección como un filtro de tráfico de red básico

el enrutador transmite datos a través de la red perimetral a través del servidor protección perimetral [20].

Red periférica: Esta red, comúnmente conocida como DMZ (red de zona desmilitarizada) o red un punto final que conecta a los usuarios a un servidor web u otro servicio. Y el servidor web luego se conecta a la intranet a través de cortafuegos interno [21].

Intranet: La intranet está conectada a servidores internos como servidores SQL y usuarios internos [20].

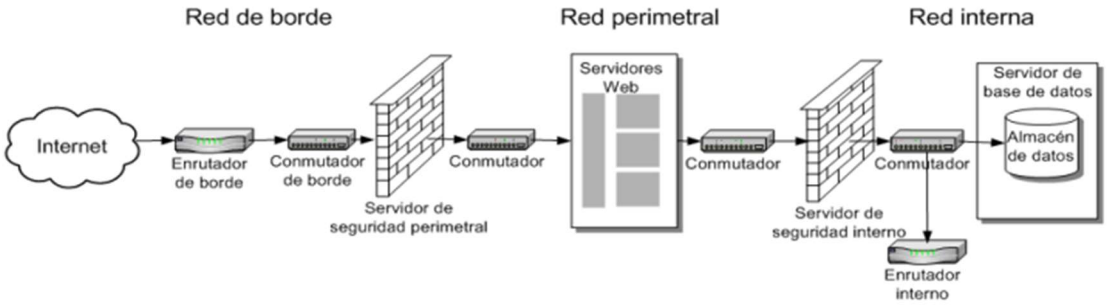


Fig. 1 Arquitectura de Red Empresarial.

Un servidor seguro es un equipo que se utiliza para administrar el creciente tráfico IP entre dos redes. Los dispositivos de cortafuegos normalmente se ejecutan en L3 (capa 3) del modelo OSI, aunque algunos modelos pueden funcionar a un nivel superior. Como regla general, los cortafuegos tienen las siguientes ventajas [22]:

- Protege los servidores internos contra ataques a la red
- Se aplican políticas de uso y acceso a la web.
- Supervisa el tráfico y genere alertas cuando se detecten patrones sospechosos

Debe enfatizarse que los firewalls están limitados a ciertos tipos de amenazas. Los cortafuegos deben implementarse como parte del sistema de seguridad de una organización. El cortafuegos examina los paquetes IP entrantes y bloquea aquellos que considera intrusos. Algunos bloqueos se pueden realizar reconociendo de antemano que algunos paquetes no son válidos y otros configurando un firewall para bloquearlos. TCP/IP se desarrolló hace muchos años sin ninguna preocupación por la seguridad o la piratería y tiene muchos defectos. Un firewall externo puede tener un ancho de banda más

limitado que un firewall interno porque el tráfico entrante está más restringido porque en realidad es un servidor web u otros servicios especiales [22].

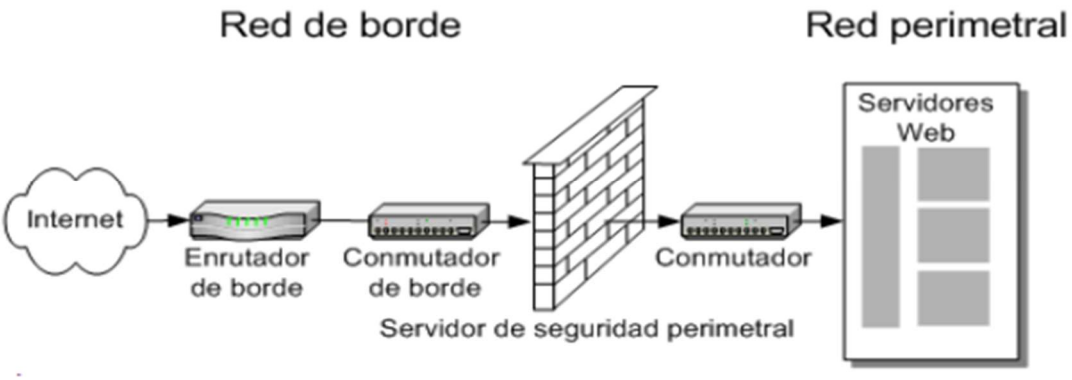


Fig. 2 Servidor de seguridad único con componentes redundantes.

2.1.5 Seguridad perimetral

La seguridad perimetral representa un concepto en evolución que implica la amalgama de componentes y sistemas, tanto electrónicos como mecánicos, con el fin de salvaguardar los límites físicos, detectar posibles intentos de intrusión y/o disuadir a intrusos en instalaciones altamente sensibles. Dentro de estos sistemas, destacan elementos como radares tácticos, sensores de video, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, así como concertinas, entre otros [23]. Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra 16 óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de soporte (auto soportados, soportados, enterrados, detección visual, etc.) [23].

Describir qué aspectos de la protección del perímetro incluyen, escalabilidad requerida, tolerancia a fallas, eficiencia, seguridad y garantía de gestión de seguridad. Entre las regiones con diferentes niveles de seguridad de redes corporativas, tenemos:

- intranet
- red externa
- DMZ (Zona Desmilitarizada)

Actualmente, la red corporativa de cualquier universidad está conectada a la red pública, por ello, es importante reforzar las medidas de seguridad [23].

2.1.6 Firewall

Un cortafuegos es un componente de seguridad de red que supervisa la circulación de datos entrante y saliente, tomando decisiones sobre permitir o bloquear tráfico específico en base a un conjunto predefinido de reglas de seguridad. Durante más de un cuarto de siglo, los cortafuegos han desempeñado un papel fundamental como primera línea de defensa en la seguridad de redes. Establecen una barrera entre las redes internas seguras y controladas, que pueden considerarse de confianza, y las redes externas no confiables, como Internet. Es importante señalar que un cortafuegos puede adoptar la forma de hardware, software o una combinación de ambos [24].

Esencialmente, actúan como una barrera entre la red interna que contiene información confidencial y confiable de amenazas externas como Internet, es decir, protegen las computadoras personales, los servidores o las computadoras conectadas a la red del acceso no autorizado pueden robar información privada y confidencial e incluso sabotear su la red. Como puede ver, cuantas más comprobaciones tenga en cuenta el cortafuegos, más precisas serán las reglas se vuelve más complejo. Deben manejarse con el mayor cuidado posible dar lugar al rechazo, la negación o, en este caso, la omisión [24].

Pero, en general, ¿cuáles son los pros y los contras de un firewall? [25]

Ventajas

- Configuración del circuito de seguridad de la red.
- Control de acceso mejorado a todos los paquetes de datos entrantes y salientes.
- Optimizar el tráfico de red [25].

Desventajas

- Requiere un conocimiento completo de las redes de datos.
- Pueden ser muy difíciles.
- Si no se configuran correctamente, pueden causar problemas con los servicios proporcionados por la red [25].

2.1.7 Reglas de un Servidor de seguridad

Microsoft Corporation en su página nos dice que nuestro servidor de seguridad perimetral necesitará que se realicen las siguientes reglas, ya sea de forma establecida o a través de una configuración [26]:

- Bloquee los paquetes entrantes que parezcan tener una dirección IP de origen interna o provengan de una red externa.
- Bloquee los paquetes salientes que requieran una dirección IP de fuente pública (el tráfico solo debe provenir de servidores bastión).
- Resolver consultas y respuestas DNS basadas en UDP desde la resolución de nombres DNS a servidores DNS de Internet.
- Permitir consultas y respuestas de DNS basadas en UDP desde servidores DNS de Internet para publicidad de DNS.
- Permite que los clientes UDP externos consulten y respondan anuncios de DNS.
- Permitir consultas y respuestas de DNS basadas en TCP desde servidores DNS en Internet a anuncios de DNS.
- Permitir que el correo saliente del servidor SMTP se envíe a Internet.
- Permitir el correo entrante desde Internet al servidor bastión SMTP para el correo entrante.
- Permitir tráfico proxy desde servidores proxy de Internet.
- Permitir que las respuestas de proxy de Internet se enruten a servidores proxy perimetrales [26].

2.1.8 Vulnerabilidad

La vulnerabilidad compone un factor que pone en peligro la seguridad de un sistema, habitualmente se cree que una vulnerabilidad es un punto débil de un sistema, la vulnerabilidad informática es un elemento de un sistema informático que puede ser explotado por un atacante para violar la seguridad. Las vulnerabilidades se consideran internas al sistema, por lo que es trabajo de los administradores y usuarios detectarlas, evaluarlas y mitigarlas. Los atacantes pueden explotar las vulnerabilidades de seguridad que son el resultado de una programación negligente, fallas en el diseño del sistema e incluso limitaciones tecnológicas [27].

Podemos clasificarlos de la siguiente manera.

- Física.
- Natural.
- Hardware.
- Software.
- Red.
- Factor humano.

En este proyecto se va a investigar en base a las vulnerabilidades de la red, las redes pueden llegar a ser sistemas muy vulnerables debido a que son muchas computadoras conectadas entre sí para compartir recursos, las cuales pueden atacar a toda la red invadiendo la red por primera vez en una de las computadoras. y luego ampliar para el resto [28]. En la red, la prioridad es enviar información, por lo que cualquier vulnerabilidad está directamente relacionada con la posibilidad de interceptación de información por parte de personas no autorizadas y errores en la disponibilidad del servicio. Gracias a estas dos vulnerabilidades, las redes se convierten en una colección de vulnerabilidades de hardware, software, físicas e incluso naturales [28].

2.1.9 Políticas de Seguridad y su Desarrollo

La política de seguridad define lo que se debe proteger en el sistema informático mientras que los procedimientos de seguridad describen cómo lograr cierta seguridad. La Política de Privacidad se desarrolla en los siguientes pasos [29]:

1) Identificar y evaluar activos: qué activos necesitan ser protegidos y cómo proteger la empresa para prosperar.
2) Identificar amenazas: ¿cuáles son los posibles problemas de seguridad? Considere la posibilidad de brechas de seguridad y las posibles consecuencias si ocurren. Estas amenazas son externas o internas [29]:
    - Amenazas externas: provienen del exterior de la organización, como virus, gusanos, caballos de Troya, esfuerzos de piratas informáticos, represalias de exempleados o espionaje industrial.
    - Amenazas internas: las amenazas provienen del interior de la empresa y pueden ser muy costosas porque los atacantes obtienen acceso y comprenden mejor dónde se almacena la información sensible y confidencial. Las amenazas

internas también incluyen el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que los empleados pueden causar al enviar y ver material ofensivo a través de Internet.

3) Evaluación de riesgos. Esta puede ser una de las partes más difíciles de crear una política de privacidad. Debe calcular la probabilidad de ciertos eventos y determinar qué evento es más probable que cause el mayor daño. El costo puede ser más que dinero: el valor debe ser en términos de pérdida de datos, privacidad, responsabilidad, atención pública no deseada, pérdida de confianza del cliente o del inversor y el costo de remediar las violaciones de seguridad [29].
4) División de responsabilidades: elegir un equipo de desarrollo ayudará a identificar amenazas potenciales en todas las áreas de la empresa. La solución ideal sería un representante de cada departamento de la empresa. Los miembros principales del equipo serán el Administrador de la Red, el Asesor Legal, el Gerente Senior y representantes del Departamento de Recursos Humanos y Asuntos Públicos [30].
5) Establecer política de privacidad: cree una política que apunte a documentos relacionados; especificaciones y procedimientos, normas y contratos de trabajo. Estos documentos deben incluir detalles de la plataforma informática, los antecedentes tecnológicos, las responsabilidades del usuario y la estructura organizativa [30].
6) Implementar la política de la empresa. La política elegida debe definir claramente las responsabilidades de seguridad e identificar quién posee qué sistemas y datos. También puede pedir a todos los empleados que firmen el formulario; Si está firmado, debe indicarse claramente [31].
7) Administración de programas de seguridad: establecer procedimientos internos para implementar y hacer cumplir estos requisitos [29].

2.2 Marco Teórico

2.2.1 Importancia de políticas de seguridad Informática.

La importancia de las políticas de seguridad informática radica en la necesidad de proteger la información crítica y los sistemas tecnológicos en un entorno cada vez más digital y conectado. Aquí tienes algunas razones clave para la importancia de estas

políticas. protección de datos sensibles, cumplimiento legal y regulaciones, protección contra amenazas cibernéticas, disponibilidad de sistemas y servicios, protección de la reputación, optimización de recursos, crecimiento y competitividad. Las pequeñas y medianas empresas enfrentan el problema de las vulnerabilidades informáticas en sus operaciones diarias, lo que puede dañar su funcionamiento a largo plazo [32].

Estas vulnerabilidades se pueden abordar mediante políticas de seguridad informática basadas en la norma ISO 27001. La falta de seguridad informática puede resultar en la pérdida o alteración de datos, ataques cibernéticos y daños a la reputación empresarial. Implementar políticas de seguridad informática según ISO 27001 es esencial para garantizar la gestión segura de la información y evitar pérdidas económicas. Estas políticas incluyen principios clave como confidencialidad, integridad y disponibilidad de datos. Se puede utilizar el modelo PDCA para involucrar a todo el personal en la implementación de estas políticas a lo largo de un período de 6 meses a 1 año. Las amenazas informáticas pueden tener diversos impactos, y las vulnerabilidades pueden surgir de diversas fuentes, incluyendo factores humanos, naturales, físicos y de software [32].

2.2.2 Análisis y técnicas de seguridad en redes de informática basado en Open Source.

En cuanto a la seguridad informática en las redes, es un tema sumamente importante, pero es un tema complicado ejecutar, porque se cuenta con licencias y herramientas de software que no son económicas, siendo esto un problema para las pequeñas y medianas empresas. Visto este problema surgen soluciones como los softwares Open Source que al igual ayudan a la detección y prevención de intrusos con un alto nivel de seguridad con características eficientes; por lo tanto, poseen el mismo grado de efectividad que un software licenciado, pero a su vez su implementación suele ser más complicada. Suricata es un software de detección y prevención de intrusos (IDS/IPS) que analiza el tráfico con una amplia base de datos actualizada [33].

Estas herramientas presentan varias características resaltantes que los posicionan como una excelente alternativa de código abierto basado en un conjunto de reglas y características que los posicionan en un buen puesto en cuanto a seguridad [33].

2.2.3 Vulnerabilidades en los sistemas informáticos

Los sistemas informáticos se enfrentan a una serie de amenazas y ciberataques. Es crucial identificar y analizar las vulnerabilidades de seguridad en estos sistemas para protegerlos de manera efectiva [34]. Los atacantes pueden aprovechar estas debilidades para comprometer la seguridad de un sistema informático. Estas vulnerabilidades pueden utilizarse para obtener acceso no autorizado a los sistemas, alterar o destruir datos, o llevar a cabo ataques de denegación de servicio. Existen numerosas herramientas y técnicas disponibles para llevar a cabo este tipo de análisis [34].

El avance tecnológico impulsado por Internet y sus diversas aplicaciones ha dado lugar a una generación que se enfrenta constantemente a nuevos desafíos, desarrollando habilidades y actitudes relacionadas con la tecnología digital. Sin embargo, junto con estos avances, han surgido amenazas en diversas formas que son cada vez más difíciles de detectar, lo que compromete la seguridad de aquellos usuarios que no cuentan con la capacitación necesaria para identificar, mitigar o evitar estas amenazas en un entorno potencialmente peligroso. En muchos casos, estas amenazas pueden tener un impacto significativo en la vida humana y causar daños considerables [35].

2.3 Metodología del proyecto

2.3.1 Metodología de Investigación

La metodología de la investigación busca mostrar los elementos para la búsqueda, recolección e interpretación de la información lo cual se vuelve importante para realizar el siguiente proyecto [36].

Para el presente trabajo se realizará investigación diagnostica se refiere a la investigación que comprende la recolección de datos para probar hipótesis o responder a preguntas concernientes a la situación de estudio [37]. Por esta razón la investigación diagnostica tiene la finalidad de conocer más acerca la infraestructura y la funcionalidad del sistema. Para saber también cómo se maneja un centro de datos de estas instituciones, se va a tomar en cuenta una institución municipal donde para recolectar información se usarán métodos de recolección de datos, en este caso se usará la entrevista para poder conocer el estado actual de la seguridad una de estas instituciones.

A su vez también se desarrollará la metodología de investigación exploratoria que consiste en examinar un tema o problema de investigación poco estudiado, del cual se tienen dudas o no se ha abordado antes [38]. Dada que es una investigación poco estudiada y no existen investigaciones referentes acerca de la ejecución de un sistema de seguridad perimetral en instituciones municipales. Sé realizará un estudio bibliográfico y finalmente la se propondrá un sistema de seguridad que se acople a las necesidades específicas de la mayoría de estas instituciones.

Variables

En el presente trabajo se propone una variable cuantitativa la cual tiene como prioridad comprobar el estado actual de protección de cómo se encuentra el centro de datos de la institución mediante el levantamiento de información y del uso de herramientas de análisis de vulnerabilidad, estoo permita tomar las medidas necesarias que ayude a la protección de datos de la entidad municipal y poder reducir las vulnerabilidades presentes.

La Variable: Aplicación de reglas de seguridad Perimetral Informático que contribuya en la seguridad al centro de datos.

2.3.2 Técnicas e instrumentos de recolección de datos

La entrevista se realizará a un trabajar municipal siendo su cargo en esos momentos como jefe de departamento de Sistemas, (Anexo 1) y los resultados serán proporcionados en este documento para conocimiento y ayuda del proyecto. Se llevará a cabo dentro de los horarios laborables, y disposición del jefe del departamento, también mediante observación, se verificará el estado en que se encuentran los equipos y sus localizaciones (Anexo 2). De esta entrevista se puede destacar que se obtuvo información valiosa de una estructura actual y de cómo se encuentra la seguridad de este municipio, y se obtuvo como resultados esta información.

Año de Existencia: Según la respuesta del entrevistado, las instalaciones de la data center de la institución existen desde el año 2014. Esto proporciona una línea de tiempo importante para comprender la infraestructura actual y su posible evolución.

Sistema de Seguridad: El entrevistado menciona que existen dos barreras de protección en cuanto a seguridad de los datos. Esto sugiere que la institución ha tomado medidas

para proteger la data center, aunque no se proporcionan detalles específicos sobre estas barreras.

Niveles de Seguridad: Se menciona la existencia de un proxy que asegura la navegación. Sin embargo, no se proporcionan detalles sobre otros niveles de seguridad que puedan estar implementados en la data center.

Equipos y Software: Se informa que Telconet provee un equipo de Fortinet que plantea políticas de seguridad. Esto sugiere la presencia de un sistema de seguridad de hardware. También se mencionan diferentes tipos de servidores y se indica que existen al menos 5 servidores en la infraestructura.

Estructura de la Red: Se proporciona una descripción básica de cómo está estructurada la red, desde el ISP hasta los switches que distribuyen la red a los diferentes departamentos. Esta información es esencial para comprender la topología de la red.

Número de Usuarios: El entrevistado informa que actualmente hay más de 200 usuarios conectados a la red. Esta cifra es importante para comprender la carga de usuarios en la infraestructura.

Provisión de Red: Se menciona que la infraestructura de la red también proporciona conectividad a otros lugares, como el Registro de la Propiedad, el taller y la Matriculación Vehicular. Esto amplía la comprensión de la utilidad de la infraestructura.

Departamentos Abastecidos: Se enumeran los departamentos que se benefician de la infraestructura de la red. Esta información es importante para identificar los puntos de acceso y las áreas críticas en la institución.

Cantidad de Equipos: Se proporciona información sobre la cantidad de equipos en la red, incluyendo servidores y computadoras. Esta información es relevante para evaluar el tamaño de la infraestructura.

Ataques y Malware: El entrevistado indica que la falta de seguridad ha resultado en problemas con malware en la red, lo que ha afectado la producción de los empleados. Esta información destaca la importancia de abordar los problemas de seguridad existentes.

Esta entrevista y la observación proporciona una visión inicial de la infraestructura de un centro de datos de una institución municipal y los desafíos de seguridad que enfrenta.

Será importante utilizar esta información como base para un estudio más detallado de seguridad y para proponer soluciones que aborden los problemas de malware y mejoren la seguridad de la institución.

2.3.3 Metodología de desarrollo

El uso de la metodología top-down ayuda a pensar el problema y empezar con un diseño inicial de cómo debería resolverse, para que esta estructura ayude en la implementación de la solución final, cada fase busca recolectar información para seguir con la siguiente, si bien es cierto tienen una baja interacción que buscan ser lo más independiente posible [39].

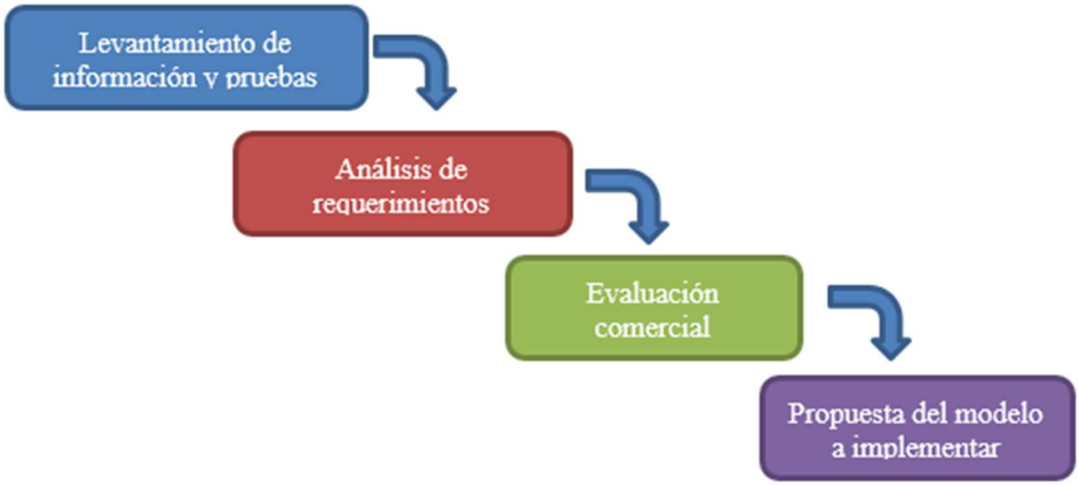


Fig. 3 Ciclo de metodología Top Down

Se va a dividir en cuatro fases que se mencionan a continuación:

Fase 1: Levantamiento de información y pruebas:

Resulta necesario examinar, supervisar e identificar los vínculos que conectan las distintas oficinas dentro de estas instituciones. Además, es necesario elaborar un esquema integral de la red LAN para determinar la disposición de los equipos activos de conmutación, conectados a través del cableado estructurado, con las estaciones de trabajo y los puertos utilizados para la conexión a Internet.

Fase 2: Análisis de requerimientos:

En la etapa de evaluación de requisitos, se procederá a identificar los activos críticos actuales de la empresa. A partir de esto, se analizarán las posibles amenazas que podrían comprometer el centro de datos de las instituciones municipales. También se llevará a cabo la identificación de los requisitos necesarios para establecer una seguridad acorde con las recomendaciones de un sistema de seguridad perimetral.

Fase 3: Evaluación comercial:

Para poder llegar a implementar un sistema de seguridad perimetral se va a levantar información de sistemas existentes de seguridad perimetral, tanto en costos de adquisición y también en el costo de implementación, para así poder tomar la mejor decisión.

Fase 4: Propuesta del modelo a implementar.

La definición para llegar un modelo de las políticas de seguridad que serán aplicadas sobre los componentes que conforman la solución de seguridad perimetral: firewall externo, proxy de navegación, son etapas de todo el proceso de implementación de la solución de seguridad completa que se va a aplicar de acuerdo con la información levantada.

CAPITULO 3. PROPUESTA

3.1. Fase 1: Levantamiento de información.

Esta fase comprende la recolección de datos de la infraestructura actual de una red de un municipio, para esto es necesario analizar, monitorear e identificar los enlaces que interconectan las oficinas con las que cuenta la empresa, se necesita identificar el esquema general de la red LAN para determinar la ubicación de los equipos, activos de conmutación a los que estarán conectados por medio del cableado con las estaciones de trabajo y los puertos que estos utilizan para la salida hacia el internet, lo que nos permitirá encontrar posibles fallas que se puedan afectar a la seguridad del sistema, a continuación se muestran de manera detallada toda la información recabada.

Servicios que ofrece una institución municipal.

La infraestructura del municipio está adaptada para ofrecer varios servicios a los usuarios en la siguiente tabla se va a detallar:

Servicio	Descripción
Servidor Web	La institución cuenta con páginas web que se encuentran alojada en servidores físicos el área de sistemas en la segunda planta, pero este se encuentra virtualizado.
Servidor de bases de Datos	La institución cuenta con equipos destinados precisamente a la base de datos de la institución donde solo se encuentra los datos de aplicaciones que la institución usa para ofrecer servicios a los usuarios.
Video vigilancia	La institución cuenta con muy pocas cámaras de seguridad no se ha planteado un circuito en el edificio principal, pero si en el taller se cuenta con unas cámaras que se monitorizan desde el centro de sistemas.

Impresoras IP	La institución cuenta con equipos de impresión ubicados en varios departamentos, cada equipo tiene su dirección IP asignada que se encuentra configurado en la red
Impresoras IP	También se cuenta con telefonía interna para comunicarse con cada departamento, cada departamento cuenta con un teléfono IP.
Correo	La institución cuenta con el servicio de correo este se Zimbra y cada trabajador se le provee un correo institucional para fines de trabajo.
Conexión cableada	Servicio dirigido a cada departamento, cada departamento cuenta con varias conexiones cableadas donde se pueden conectar, cabe recalcar que se le asigna una IP estática a cada equipo que se conecte.
Wifi	Conexión inalámbrica en departamentos que sea necesario, para conferencia o invitados especiales.

Tabla 1 Servicios de red

Datos de la situación actual del centro de datos.

Debido a que estamos hablando de una infraestructura de un municipio que se estima que es una red que ofrece asistencia a 200 trabajadores, que a su vez estos ofrecen los servicios mencionados a la comunidad de todo el sector donde se encuentra el establecimiento.

La infraestructura física del municipio puede contar con varios departamentos, entre los que podemos encontrar la alcaldía, obras públicas, turismo, gestión de riesgo, talento humano, concejales, bodega, comunicación, secretaria, terrenos, coactiva, secretaria, policía municipal, bienestar social, tesorería y el departamento de sistemas que es donde puede estar alojado el centro de datos de la institución, cada departamento cuenta con equipos para que cubran las necesidades de cada uno de esto, ciertos departamentos cuentan con impresoras y telefonía IP.

Componente	Modelo/Marca
Servidores	Modelo: HP 1650 Storage
	Modelo: ProLiant DL 380 G9
	Modelo: ProLiant DL 560 G8
	Modelo: ProLiant DL 380 G7 (x2)
	Modelo: ProLiant DL 380 G10 (x2)
Equipos de Comunicación Switch	Modelo: Cisco Catalyst 2960-X Series (x3)
	Modelo: HPE OfficeConnect 1920 Series (JG926A)
Red Cableada	
Topología	Tipo Estrella según ANSI/TIA/EIA-568-B
Cables	Cableado horizontal y vertical
Puntos de Red	
Departamento de Sistemas	1 punto de red
Bienestar Social	1 punto de red
Alcaldía	1 punto de red
Computadoras de Escritorio	120 computadoras de escritorio de varias marcas
Data Center	
Sistema UPS	Garantiza el funcionamiento de los servidores en caso de pérdida de energía.

Tabla 2 Equipos existentes en la red.

El acceso físico al área de data center por lo general se encuentra en un departamento adecuado para este, restringiendo la entrada a personal no autorizado, el personal como trabajadores del departamento de sistemas, ayudante y pasantes de la misma área con previa solicitud de acceso autorizada por el director del departamento de sistemas pueden ingresar.

El departamento de sistemas maneja un segmento de red LAN con direccionamiento IP en el rango 172.XXX.XXX.XXX a 172.XXX.XXX.XXX manejado por un servicio de DHCP tanto para la red cableada como para la inalámbrica, además dispone de una IP pública 186.X.X.X en la cual se encuentra alojada el portal web de la institución, trabaja con un servidor controlador de dominio (sistemas.local), un servidor proxy, un servidor de correo, un servidor de archivos, estos servidores se encuentran virtualizados mediante un servidor Zential donde se encuentran 2 Host, en el host 1 se encuentra el dominio los servidores y el host 2 un servidod NAS donde están los servidores virtuales. Además, cuenta con un enlace de Internet, con ancho de banda de 20 Mbps cuyo proveedor ISP es Telconet.

Para la obtención de vulnerabilidades en red se realizó un experimento que siguió un diseño claro con pasos específicos, desde la instalación del sistema operativo hasta el uso de diversas herramientas para obtener información detallada y buscar vulnerabilidades que se detallan en el (Anexo 3).

Herramienta	**Resultados Obtenidos**
nslookup	Dirección IP pública: 186.X.X.X
whois	Información del propietario, responsable, dirección, país, teléfono y correo electrónico relacionados con la dirección IP.
Netcraft	Tipo de servidor web y sistema operativo detectados en el sitio.
nmap	Puertos abiertos: 80, 113, 443, 2000 y 5060.
Shodan	Vulnerabilidades identificadas en los puertos 22, 25, 80, 443, 465, 993, 995 y 7071.

Tabla 3 Vulnerabilidades actuales de la red detectadas.

Mediante es escaneo de red en si se pudo evidenciar que la red de la institución cuenta con los siguientes puertos abiertos.

Puerto	Protocolo	IP
22	TCP	xxx.gob.ec
25	TCP	xxx.gob.ec
80	TCP	xxx.gob.ec
443	TCP	xxx.gob.ec
465	TCP	xxx.gob.ec
993	TCP	xxx.gob.ec
995	TCP	xxx.gob.ec
7071	TCP	xxx.gob.ec

Tabla 4 Puertos abiertos

Arquitectura actual de la red

La red de la unidad educativa cuenta con una topología de red basada topología estrella, esta topología esta desarrollada de forma básica, el punto central se encuentra en el cuarto de redes, de la cual parten cada uno de los diferentes puntos de acceso hacia los diferentes departamentos.

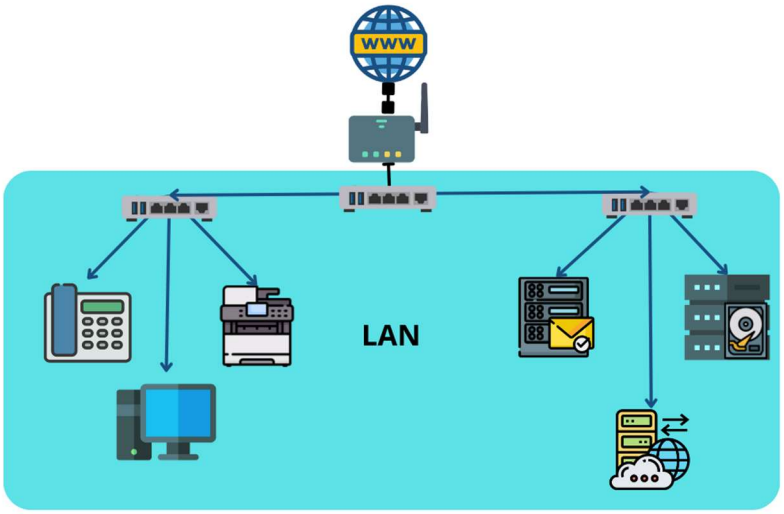


Fig. 4 Estado actual de la arquitectura de la red

3.2 Fase 2: Análisis de requerimientos.

En esta fase se va a detallar los requerimientos que se va a describir todo los requisitos que el centro de datos del municipio de la institución municipal, y se va plantear todos los requisitos que se propuso de acuerdo al alcance de nuestro proyecto, para que exista un buen funcionamiento en beneficio de los trabajades de la empresa y esto lleve también al beneficio de los usuario finales que se sirven de los servicios del municipio, a continuación se va a detallar cada uno de los servicios que se plantea implementar de acuerdo con la recolección de datos y manifestado por el cliente.

Requerimientos de red.

La solución propuesta busca proteger la red de una institución municipal contra los ataques provenientes de internet, al tiempo que optimiza el uso del servicio de internet y brinda visibilidad y control del tráfico entrante y saliente. A continuación, se detallan los principales requisitos de seguridad y funcionalidades que se desean obtener:

- Protección contra ataques desde internet: La solución debe contar con medidas de seguridad efectivas para mitigar los ataques cibernéticos, como firewalls de última generación, sistemas de detección y prevención de intrusiones (IDS/IPS), filtrado de contenido malicioso y protección contra malware.
- Control granular de acceso a Internet: Se requiere la capacidad de gestionar y controlar el acceso de los usuarios a sitios web y protocolos específicos. Esto permite establecer políticas de seguridad personalizadas y restringir el acceso a contenido inapropiado o potencialmente peligroso.

Requerimientos de administración y gestión

Los requerimientos de administración y gestión para la implementación de la solución de seguridad perimetral son los siguientes:

1. Gestión de la solución:
    - Definir grupos, roles y responsabilidades para la administración lógica de los componentes de la solución.

- Registrar y auditar los cambios realizados en la política de seguridad, incluyendo la creación o modificación de reglas.

2. Reglas generales para el control de acceso:
    - Todo acceso desde internet debe ser realizado a través de un medio seguro y encriptado.
    - Bloquear todo tráfico entrante y saliente no declarado como permitido.
    - Implementar una DMZ para filtrar y analizar el tráfico y prohibir el acceso directo desde la red de usuarios hacia internet.
    - Utilizar NAT para enmascarar todo el tráfico saliente desde la red interna hacia internet.
3. Reglas de asignación por usuario:
    - Identificar a todos los usuarios con un único usuario antes de brindarles acceso a los sistemas desde internet.
    - Implementar autenticación para todos los usuarios a través de una base de datos de un servidor LDAP o Active Directory.
    - Permitir el acceso compartido remoto con el proveedor de seguridad para soporte técnico y monitoreo del equipo.
    - Establecer requisitos de contraseñas, como longitud mínima de 9 caracteres, caracteres numéricos y alfanuméricos, y prohibición de reutilizar contraseñas recientes.
4. Política de evaluación constante de la seguridad:
    - Mantener actualizados los dispositivos dedicados a la seguridad perimetral con la última versión de firmware.
    - Realizar pruebas de penetración al menos una vez al año y después de cada modificación en la red.
    - Utilizar sistemas de detección de intrusos para monitorear el tráfico de la red y alertar sobre eventos sospechosos.
    - Mantener actualizados los detectores de intrusos.

- Realizar escaneos de vulnerabilidades externos e internos de forma regular y después de implementar nuevos sistemas o cambios en la topología de la red o el firewall.

Requerimientos técnicos

Los requerimientos técnicos de la solución de seguridad perimetral son los siguientes:

- Capacidad de configuración de enlace de respaldo en el firewall perimetral: El firewall perimetral debe tener la capacidad de utilizar un enlace de respaldo en caso de falla del enlace principal, asegurando la disponibilidad y continuidad de la conexión a internet.
- Aplicación de filtro de paquetes dinámico en los firewalls: Los firewalls deben ser capaces de analizar y filtrar los paquetes de red en tiempo real, aplicando reglas de seguridad para permitir o bloquear el tráfico de acuerdo con las políticas establecidas.
- Bloqueo de ataques de negación de servicio: Los firewalls deben contar con mecanismos de detección y bloqueo de ataques de denegación de servicio (DoS) que puedan afectar la disponibilidad y rendimiento de la red.
- Capacidad de detección de ataques o intentos de intrusión: Los firewalls deben ser capaces de detectar y bloquear los intentos de intrusión o ataques maliciosos provenientes de internet, garantizando la seguridad de la red.

Además, se especifican requerimientos específicos para cada elemento de seguridad:

Firewall Perimetral:

- Capacidad de dominar distintos protocolos de enrutamiento (OSPF).
- Control de flujo y ancho de banda.
- Prevención de intrusos, filtro de contenido y antivirus embebido.
- Manejo de múltiples enlaces hacia internet.

Control de acceso a Internet:

- Control de acceso por HTTP, HTTPS y a nivel de inspección SSL.

- Políticas por usuarios y grupos de usuarios.
- Filtro de protocolos de Internet.
- Filtrado de direcciones y dominios en internet.
- Control de aplicativos y categorías de páginas web.
- Perfil de control de aplicación.

Control de correos electrónicos:

- Lista negra para denegar dominios específicos.

Monitoreo y reportes personalizados:

- Monitoreo 24/7 del tráfico y servicios en los equipos de seguridad.
- Visualización en tiempo real de eventos en la red.

Generación automática de reportes personalizados en formato PDF y envío a la bandeja de entrada del administrador de red.

3.3 Fase 3: Evaluación comercial.

Se tomo en cuenta un par de criterios para poder elegir cual sería la mejor solución en cuanto al sistema de seguridad perimetral:

Evaluación Tecnológica

Esta parte va a tomar en cuenta si la solución cumple con los requerimientos planteados por la empresa.

Selección de fabricantes

Existen diversas marcas que se centran en la seguridad perimetral de la red informática para satisfacer las necesidades de los usuarios, como Palo Alto, Juniper, Cisco, Checkpoint, Fortinet, entre otras, es crucial identificar cuál proporciona el mejor servicio. La competencia entre estas marcas es intensa, y la elección de la solución más confiable implica comprender su desempeño relativo.

Para evaluar estas tecnologías emergentes, muchas empresas recurren a entidades especializadas, y una de las más reconocidas y confiables es Gartner. Esta firma estadounidense de investigación en tecnologías de la información se dedica a comparar

empresas en función de su historial, evolución en el mercado, servicios ofrecidos, estabilidad, y cumplimiento de los requisitos de los usuarios. Valiosa información al respecto se encuentra disponible en su página web.

El cuadrante mágico de Gartner.

Las empresas dentro se posicionan en el Cuadrante Mágico de acuerdo con su desempeño. Dentro de este existen cuatro áreas de las cuales se va a mencionar su descripción:

- Líderes: Empresas consolidadas con productos probados, ejecución eficiente y recursos para mantener el liderazgo.
- Desafiadores: Proveedores con visión integral, impulsando innovación, pero careciendo de la escala de los líderes.
- Jugadores de Nicho: Enfocados en segmentos específicos con ejecución limitada y soluciones especializadas.
- Visionarios: Empresas con visión atractiva, desarrollando ejecución y demostrando capacidad para obtener resultados.

De la investigación realizada por Gartner en el año 2022, se va a mostrar el cuadrante de mágico proporcionado por esta empresa en la siguiente imagen.

Figure 1: Magic Quadrant for Network Firewalls

Fig. 5 Cuadro mágico Gartner

(Fuente: Gartner)

Como se puede observar en la imagen en este estudio se ha nombrado a varios proveedores que entre los lideres tenemos los siguientes:

Empresa	**Administración y Protección**	**Valor**	**Generalidades**
Fortinet	Alto	Intermedio	Amplio portafolio de productos de seguridad y gestión centralizada.
Palo Alto Networks	Alto	Alto	Enfoque en prevención de amenazas avanzadas y seguridad de aplicaciones.
Check Point	Alto	Alto	Amplia experiencia en seguridad de red y prevención de amenazas.

Tabla 5 Listado de equipos de Firewall

Para este trabajo de investigación vamos a tomar en comparativa los 3 lideres según el cuadro mágico de Gartner y vamos a revisar las funcionalidades con los que cada uno cuenta.

Funcionalidades	**Fortinet**	**Palo Alto Networks**	**Check Point**
Firewall	✔ (Firewall de próxima generación)	✔ (Firewall de próxima generación)	✔ (Firewall de próxima generación)
Prevención de amenazas avanzadas	✔ (Análisis de comportamiento, inteligencia de amenazas)	✔ (Análisis de comportamiento, inteligencia de amenazas)	✔ (Análisis de comportamiento, inteligencia de amenazas)

Control de aplicaciones	✔ (Control y visibilidad de aplicaciones)	✔ (Control y visibilidad de aplicaciones)	✔ (Control y visibilidad de aplicaciones)
Seguridad en la nube	✔ (Seguridad en la nube)	✔ (Seguridad en la nube)	✔ (Seguridad en la nube)
VPN	✔	✔	✔
Gestión unificada de amenazas	✔	✔	✔
Protección contra malware	✔	✔	✔
Seguridad de correo electrónico	✔	✔	✔
Análisis de registros y reportes	✔	✔	✔

Tabla 6 Funcionalidades de equipos de Firewall

Otro punto para considerar dentro del análisis para la elección del mejor equipo también llega a ser los costos de estos para que se puedan implementar si bien es cierto en la primera tabla nos dice que Fortinet tiene un costo intermedio en cuento a sus contrincantes, en la siguiente tabla se va a poner costos referenciales sacados de páginas de ventas de cada uno ya que no existe una sola página para los tres.

Equipo	**Fortinet FortiGate 600F**	**Palo Alto Networks PA-3410**	**Check Point 6900**
Costo Referencial	$ 18,423.00	$ 50,858.49	$ 44,766.99

Costo Referencial de Licencia Anual	$ 7,577.17	$ 19,084.91	$ 18,020.00
Costo de Instalación y Configuración			$ 25,00/hora 8 horas
Costo Referencial de Mantenimiento Anual			$ 25,00/hora 4 horas
Costo Referencial de Capacitación			$ 25,00/hora 8 horas
Total	$ 26,500.17	$ 70,443.4	$ 63,286.99

Tabla 7 Precios

Fortinet como solución de paga.

Fortinet es una sólida opción como solución final de seguridad cibernética debido a sus numerosos beneficios y capacidades. Al elegir Fortinet, podemos obtener una solución completa que abarque desde firewalls de próxima generación hasta protección de ataques y seguridad en la nube.

Comparación de herramientas de código abierto.

Al igual que las herramientas de paga se ha planteado reconocibles opciones en cuanto a código abierto, en el siguiente cuadro se va a comparar entre las herramientas gratuitas comparando sus características.

Funcionalidades	**PfSense**	**OPNsense**	**IPFire**
Tipo de solución	Firewall, enrutador	Firewall, enrutador	Firewall, enrutador
Enfoque	Código abierto	Código abierto	Código abierto
Interfaz gráfica de usuario	WebGUI	WebGUI	WebGUI

Facilidad de uso	Interfaz intuitiva	Interfaz intuitiva	Interfaz intuitiva
Características de seguridad	Firewall de próxima generación, VPN, IDS/IPS, filtrado web, balanceo de carga, failover, entre otros	Firewall de próxima generación, VPN, IDS/IPS, filtrado web, balanceo de carga, QoS, entre otros	Firewall de próxima generación, VPN, filtrado web, QoS, IDS/IPS, entre otros
Rendimiento	Alto rendimiento	Alto rendimiento	Buen rendimiento
Licenciamiento	Licencia BSD	Licencia BSD	Licencia GPL
Soporte técnico	Comunidad de usuarios, soporte comercial disponible	Comunidad de usuarios, soporte comercial disponible	Comunidad de usuarios, soporte comercial disponible
Actualizaciones y seguridad	Actualizaciones regulares, correcciones de seguridad	Actualizaciones regulares, correcciones de seguridad	Actualizaciones regulares, correcciones de seguridad
Integración con otros sistemas	API disponible	API disponible	API disponible
Personalización	Altamente personalizable	Altamente personalizable	Personalizable
Compatibilidad hardware	Amplia gama de hardware soportado	Amplia gama de hardware soportado	Amplia gama de hardware soportado

Tabla 8 Software de código abierto

Ahora vamos a hacer al igual que los anteriores cuadros un cuadro comparativo con algunas de las funcionalidades que estas soluciones ofrecen.

Funcionalidades	pfSense	OPNsense	IPFire
Firewall	✓	✓	✓
Enrutador	✓	✓	✓
VPN	✓	✓	✓
IDS/IPS	✓	✓	✓
Filtrado Web	✓	✓	✓
Balanceo de carga	✓	✓	✗
QoS	✓	✓	✓
Failover	✓	✓	✓
Alta disponibilidad	✓	✓	✗
Control de ancho de banda	✓	✓	✗
Filtrado de contenido	✓	✓	✗
Protección contra malware	✓	✓	✓
Filtrado de correo no deseado	✓	✓	✗
Virtualización	✓	✗	✗
Portal Cautivo	✓	✗	✗
Autenticación de usuarios	✓	✓	✗

Registro de eventos	✔	✔	✔
Integración con servicios cloud	✔	✘	✘

Tabla 9 Comparación de Funciones de Software de código abierto.

Como podemos observar el que más opciones nos ofrece y es más completo es Pfsense, si bien es cierto esta solución no es tan completa como Fortigate pero si buscamos algo que no nos cueste y podamos implementar algo de seguridad en el centro de datos del municipio tenemos que decantarnos por este, pero como se plantea en esta solución es más recomendable Fortigate por la seguridad que ofrece como recalcamos a continuación.

Puntos de Comparación	**Fortinet**	**pfSense**
Enfoque	Solución comercial	Solución de código abierto
Facilidad de uso	Interfaz intuitiva y amigable	Requiere conocimientos técnicos
Características de seguridad	Amplia gama de funciones de seguridad, prevención de amenazas, control de aplicaciones, protección de endpoints, SD-WAN, seguridad en la nube, entre otras	Firewall de filtrado de paquetes, VPN, equilibrio de carga, enrutamiento y NAT, entre otros
Rendimiento	Alto rendimiento en la mayoría de sus dispositivos, especialmente en los modelos empresariales	Rendimiento puede variar según el hardware en el que se implemente
Licenciamiento	Basado en modelos de licencias con características y capacidades diferenciadas	Licencia de código abierto bajo la Licencia BSD

Soporte técnico	Ofrece soporte técnico comercial con diferentes niveles de servicio	Comunidad de usuarios y foros en línea, soporte comercial disponible con algunas opciones
Actualizaciones y seguridad	Actualizaciones regulares de firmware y base de datos de amenazas	Actualizaciones de código abierto y correcciones de seguridad comunitarias, con seguimiento activo por parte de la comunidad
Escalabilidad	Escalabilidad para satisfacer las necesidades de redes de diferentes tamaños	Escalabilidad, pero requiere hardware y conocimientos adecuados para manejar cargas más grandes
Integración con otros sistemas	Ofrece integración con sistemas de terceros y soluciones de seguridad adicionales	Requiere configuración manual para integrarse con sistemas de terceros

Tabla 10 Matriz de evaluación de características de software de seguridad perimetral.

Pfsense como solución Open Source.

pfSense es una solución de firewall de código abierto y una plataforma de enrutamiento que se basa en el sistema operativo FreeBSD. Es una distribución de software libre que está diseñada para proporcionar funciones avanzadas de seguridad de red y enrutamiento, lo que la hace popular como una solución de firewall de código abierto para empresas y entornos de red de diferentes tamaños.

Algunas de las características clave de pfSense como solución Open Source incluyen:

Firewall de próxima generación: pfSense ofrece un potente firewall que permite filtrar y bloquear el tráfico no deseado, lo que protege la red de amenazas externas.

VPN (Redes Privadas Virtuales): pfSense admite diferentes tipos de VPN, como IPSec, OpenVPN y L2TP, lo que permite conexiones seguras y cifradas entre diferentes ubicaciones o usuarios remotos.

Control de tráfico y aplicaciones: Permite controlar y priorizar el tráfico de red y aplicaciones, lo que garantiza un uso eficiente de los recursos de red y una experiencia de usuario mejorada.

Filtro web: pfSense puede bloquear el acceso a sitios web no deseados o potencialmente peligrosos, lo que mejora la seguridad y la productividad en la red.

Balanceo de carga y alta disponibilidad: Proporciona funciones para distribuir el tráfico de red entre varios enlaces de Internet y asegurar la continuidad del servicio mediante alta disponibilidad y tolerancia a fallos.

Seguridad basada en reglas: Permite definir reglas de seguridad específicas para el tráfico de entrada y salida, lo que brinda un mayor control sobre la seguridad de la red.

Soporte para paquetes adicionales: pfSense es altamente extensible y admite la instalación de paquetes adicionales para agregar funcionalidades adicionales según las necesidades específicas de cada organización.

Como solución de código abierto, pfSense tiene una comunidad activa de usuarios y desarrolladores que contribuyen con actualizaciones y mejoras continuas. Esto garantiza que la plataforma esté actualizada y segura, y que se mantenga al día con las últimas tendencias y tecnologías de seguridad de red.

3.4 Fase 4: Propuesta del modelo a implementar.

El diseño de la propuesta que se recomida es reutilizando equipos que ya están en la arquitectura de la red, sino que en esta ocasión se va a ser la implementación de un equipo de firewall como lo es PfSense esto con el fin de implementar reglas de seguridad perimetral (ver Figura).

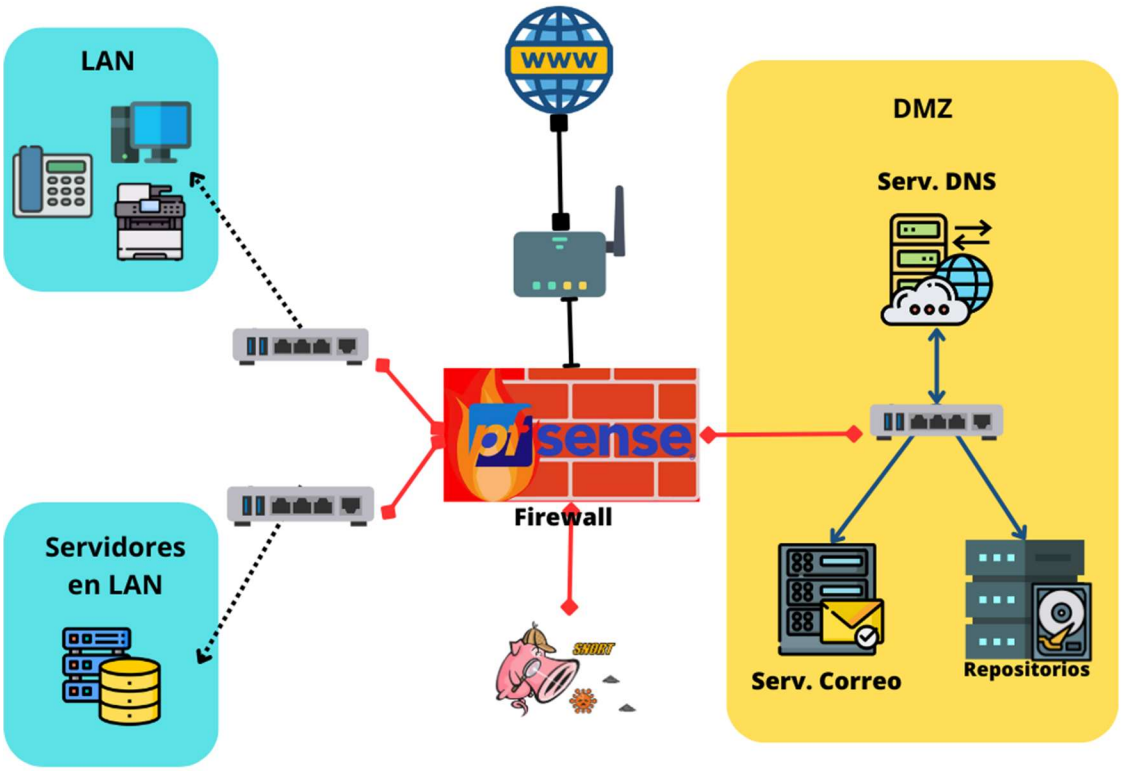


Fig. 6 Arquitectura propuesta de Seguridad Perimetral de Red

Para poder simular la red del municipio vamos a implementar una simulación de esta red mediante un entrono virtual controlado en la Tabla podemos identificar el esquema de direccionamiento de IP's para las redes LAN y WAN de la maquina anfitrión y la red del entorno virtualizado, lo que permite el funcionamiento de la arquitectura propuesta.

Direccionamiento IP de la Arquitectura de Seguridad Perimetral de Red simulada.

Equipo	**DIRECCIONAMIENTO DE INTERFACES**		
	ETH0	ETH1	VIRTUAL
	RED WAN (Internet)	RED LAN	RED DMZ
Maquina Administrador	X	192.168.5.100	X
Firewall PFSENSE	DHCP	192.168.5.100	10.10.40.1

Servidor Web	X	X	10.10.40.20
Repositorios	X	X	10.10.40.50
DNS	X	X	10.10.40.40
Servidor Correo GW	X	X	10.10.40.30
Controlador de Dominio	X	192.168.5.5	X
Servidor de Correo	X	192.168.5.7	X
Base de Datos	X	192.168.5.8	X

Tabla 11 Direccionamiento IP de Arquitectura simulada.

Reglas por aplicar para cubrir vulnerabilidades y requerimientos.

Protección contra ataques desde Internet:

Requerimiento	Descripción
Firewall:	Configurar reglas de firewall para bloquear tráfico no deseado en los puertos identificados (22, 25, 80, 443, 465, 993, 995, 7071).
	Implementar reglas de bloqueo específicas para IPs maliciosas identificadas a través de servicios como Shodan.
IDS/IPS:	Utilizar paquetes de IDS/IPS en pfSense para detectar y prevenir ataques.

Tabla 12 Direccionamiento IP de Arquitectura simulada.

Control granular de acceso a Internet:

Requerimiento	Descripción
Proxy Web:	Implementar un proxy web transparente para un control más granular del acceso a sitios web.

	Configurar reglas de filtrado web para restringir el acceso a contenido inapropiado o peligroso.

Tabla 13 Reglas de acceso a internet.

Requerimientos de administración y gestión:

Requerimiento	Descripción
Gestión de la solución:	Establecer roles y responsabilidades para la administración de pfSense.
	Implementar un sistema de registro y auditoría para cambios en la política de seguridad.

Tabla 14 Reglas de administración.

Requerimientos técnicos:

Requerimiento	Descripción
Firewall Perimetral:	Configurar pfSense con las reglas necesarias para el control de flujo, NAT, y filtrado de contenido.
	Implementar reglas de prevención de intrusiones y antivirus embebido.
Control de Acceso a Internet:	Utilizar pfSense para controlar el acceso a Internet basado en horarios, categorías de páginas web y aplicativos.
	Implementar listas negras para denegar dominios específicos.
Control de Correos Electrónicos:	Configurar inspección de correo para detectar ataques y spam.
	Implementar detección de virus en archivos adjuntos.
Monitoreo y Reportes:	Configurar monitoreo 24/7 y generación automática de reportes personalizados.

Tabla 15 Requerimientos Técnicos.

WAN (Wide Area Network):	
1.1	Mantener al menos dos proveedores de servicios de Internet (ISP) para redundancia y alta disponibilidad.
1.2	Colocar un firewall perimetral (pfSense) entre la red interna y la conexión a Internet.
1.3	Configurar reglas para protección contra ataques y filtrado de tráfico no deseado.

Tabla 16 Reglas para WAN.

LAN (Local Area Network):	
1.	Implementar un proxy web transparente para un control más granular del acceso a sitios web.
2.	Configurar reglas de filtrado web para restringir el acceso a contenido inapropiado o peligroso.
3.	Implementar un proxy web transparente para un control más granular del acceso a sitios web.

Tabla 17 Reglas para LAN.

DMZ (Demilitarized Zone):	
3.1	Colocar la DMZ entre el firewall perimetral y la LAN interna para aislar servicios públicos.
3.2	Colocar servidores web y servicios públicos en la DMZ para limitar el acceso directo desde Internet a la LAN interna.
3.3	Establecer reglas específicas para el tráfico entre la DMZ y la LAN interna.

Tabla 18 Reglas DMZ.

Gestión y Monitoreo:	
5.1	Configurar una estación de administración conectada a la LAN para gestionar los dispositivos de red.
5.2	Implementar herramientas de monitoreo para supervisar el tráfico en tiempo real y generar alertas ante eventos sospechosos.

Tabla 19 Reglas de gestión y monitoreo.

Consideraciones de Seguridad:	
6.1	Realizar actualizaciones periódicas de firmware y software en todos los dispositivos de red.
6.2	Implementar autenticación fuerte para el acceso a dispositivos de red y servicios críticos.
6.3	Definir y aplicar políticas de seguridad claras para el control de acceso, filtrado de contenido y gestión de contraseñas.
6.4	Desarrollar un plan de respuesta a incidentes para abordar rápidamente cualquier problema de seguridad.

Tabla 20 Reglas a considerar.

3.5 Resultados obtenidos.

3.5.1 Diagrama de red simulado en GNS3.

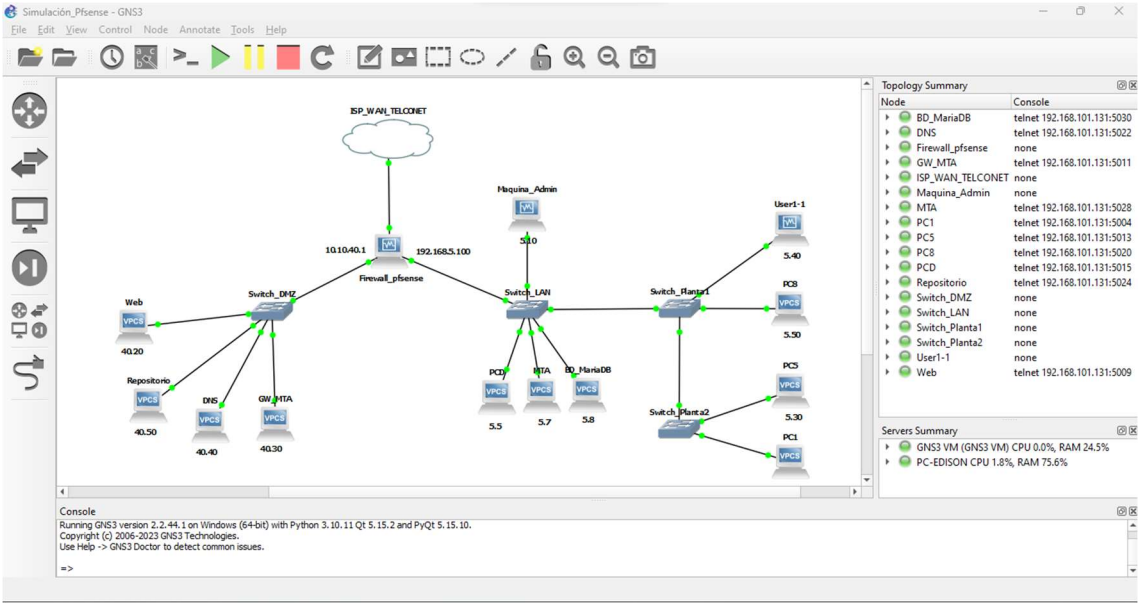


Fig. 7 Red simulada en GNS3 y Virtual box.

3.5.2 Reporte de vulnerabilidades de la red actual.

HACKING ETICO			
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA INSTITUCION			
DATOS DE LUGAR			
Lugar		Salinas	
No. Prueba:		A-01	
DATOS DEL EXPERIMENTO			
Pagina:		www.xxxxxx.gob.ec	
DETALLES DEL EXPERIMENTO			
Objetivo del experimento :	Levantar información de vulnerabilidades	Fase:	Adquisición de evidencia
Nivel complejidad prueba:	fácil	Tiempo ejecución:	30 minutos
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP Realteck 8821CE Wireless	Virtualización:	Kali Linux
Software:	nslookup whois	Redes:	wifi domestica

	Netcraft		
	iplocation		
	nmap		
	Shodam		
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
nslookup	SI	IP publica:	186.x.xx.xx
whois	SI	información del propietario:	ID del propietario, responsable, dirección, país, teléfono, correo electrónico
Netcraft	SI	detección servidor:	Tipo de servidor web y sistema operativo
nmap	SI	reconocimiento de redes y puertos	Puertos abiertos 80/113/443/2000/5060
Shodam	SI	vulnerabilidades:	Puertos abiertos 22/25/80/443/465/993/995/7071
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1.Instalacion de sistema operativo kali linux 2. Abrir consola usar nslookup con la url a escanear 3.Usar comando Whois con la ip para obtener más datos 4.Abrir en el navegador Netcraft y poner la ip 5. En la consola de kali ejecutar nmap y poner ip 6. En el navegador buscar shodan y buscar vulnerabilidades con la ip.			Anexo 3. Recolección de datos y búsqueda de vulnerabilidades.
Conclusiones:			
El análisis de los datos revela que la institución tiene potenciales vulnerabilidades en varios aspectos, desde la exposición de puertos hasta posibles problemas en la configuración de servicios. La información recopilada puede ser crucial para la mejora de la seguridad y la implementación de medidas correctivas.			

Tabla 21 Reporte de vulnerabilidades.

3.5.2 Reporte de implementación del sistema de seguridad perimetral propuesto.

Reporte de implementación del sistema de seguridad perimetral propuesto			
Reglas aplicadas en simulación.			
DATOS DE LUGAR			
Lugar		Salinas	
No. Prueba:		A-02	
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Levantar laboratorio virtual en gns3	Fase:	Propuesta del modelo a implementar
Nivel complejidad prueba:	medio	Tiempo ejecución:	12 horas
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP Realteck 8821CE Wireless	Virtualización:	GNS3
Software:	Pfsense	Redes:	wifi domestica
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Pfsense	SI	IP:	192.168.3.181
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Instalación y Configuración de pfSense. 2. Definición de Reglas en pfSense para WAN, LAN, DMZ. 3. Instalación y Configuración de SNORT. 4. Instalación de Paquetes Squid, SquidGuard y Lightsquid. 5. Configuración del Servidor Proxy Squid. 6. Configuración de Logs en Squid. 7. Control de Lista de Accesos (ACL). 8. Configuración de Grupos ACL en SquidGuard. 9. Pruebas y Monitoreo. 10. Evaluación de la Efectividad.			Anexo 4. Instalación y configuración de las herramientas de seguridad perimetral.
Conclusiones:			

El análisis de los datos revela que la implementación de reglas en pfSense ha sido efectiva en la protección contra vulnerabilidades, bloqueando el tráfico no deseado en los puertos identificados. La configuración de reglas en pfSense demuestra ser una medida crucial para mejorar la seguridad del sistema.

Tabla 22 Reglas aplicadas en simulación.

Conclusiones

La implementación de una herramienta de código abierto como pfSense ha evidenciado ayudar a la protección de sistemas informáticos, junto con SNORT, Squid y Lightsquid ha fortalecido significativamente la seguridad perimetral de ese ejemplo. La configuración de reglas específicas en pfSense permite un control detallado del tráfico, garantizando la protección contra posibles amenazas externas.

La integración de SNORT agrega una capa adicional de seguridad, detectando e impidiendo intrusiones en tiempo real. Además, Squid y Lightsquid ofrecen un control granular sobre el acceso a Internet, mejorando la productividad y filtrando contenido no deseado.

La combinación de estas herramientas proporciona una defensa contra vulnerabilidades potenciales a posibles ataques desde el exterior, pero también proporciona seguridad de los activos dentro de la institución limitando el acceso a usuarios a direcciones restringidas, contribuyendo a la seguridad dentro y fuera de la institución.

Recomendaciones

Se sugiere realizar auditorías periódicas de seguridad para evaluar la efectividad de las reglas implementadas y ajustarlas según sea necesario. Además, es crucial mantener actualizadas todas las herramientas y reglas de seguridad para hacer frente a las amenazas emergentes.

Se sugiere al igual implementar un plan de respuesta a incidentes que ayuden a mitigar posibles problemas de seguridad en el tiempo más corto posible, también se recomienda realizar simulacros periódicos esto ayudará a garantizar una respuesta efectiva en caso de violaciones de seguridad.

Además, se recomienda capacitar al personal sobre prácticas de seguridad cibernética y concientizar sobre posibles riesgos que se pueden encontrar en la red, esto ayudara a fortalecer la postura de seguridad global de la red de la institución.

REFERENCIAS

[1] S. T. R. M. T. Flavio Morales, «Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información,» *risti,* nº E27, p. 554, 2019.

[2] C. M. F. DÍAZ, «IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL,» Madrid, 2013.

[3] W. DELGADO RAMOS y K. RUIZ VIEIRA, «Implementación de una solución de seguridad perimetral Open Source en La Red,» CHICLAYO, 2018.

[4] J. V. N. Noboa, «Diseño e implementación de seguridad perimetral para la infraestructura de la inmobiliaria FASAKO S.A usando herramientas open source,» Guayaquil, 2017.

[5] La universidad del Intertnet, «Seguridad perimetral informática: objetivos y plataformas recomendables,» 30 07 2020. [En línea]. Available: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/.

[6] A. M. Proceso, «Cómo hacer un Diseño de Investigación,» de *Metodológico en la Investigación*, 2010, p. 58.

[7] E. Hernández, «DISEÑO DE UNA INFRAESTRUCTURA DE RED VOIP PARA LA UNIVERSIDAD DE CARTAGENA UTILIZANDO TOPDOWN,» Cartagena, 2015.

[8] IBM, «Mandato NSLOOKUP,» *IBM OMEGAMON for Networks on z/OS,* 2021.

[9] nmap, «Nmap.org,» 2022. [En línea]. Available: https://nmap.org/.

[10] Y. F. Tarqui Mita, «FOOTPRINTING,» *Revista de Información, Tecnología y Sociedad,* p. 41, 2013.

[11] V. J. R. Diego, E-branding: posiciona tu marca en la Red, Netbiblo, 2008.

[12] J. López, «Análisis de redes con Nmap 5,» *Todo Linux: la revista mensual para entusiastas de GNU/Linux ,* nº 109, pp. 39-42, 2009.

[13] A. Robles Camporro, «Procesos automáticos de ataques de fuerza bruta a dispositivos IoT en SHODAN.,» Universidad de Oviedo, 2023.

[14] UPSE, «REGLAMENTO DE INESTIGACION SISTEMA Y TELECOMUNICACIONES,» 16 marzo 2019. [En línea]. Available: https://www.upse.edu.ec/secretariageneral/images/archivospdfsecretaria/4.REGLAMENTOS/1.%20NORMATIVAS%20ACAD%C3%89MICAS/REGLAMENTO_2019/RCS-SE-16-03-2019_REGLAMENTO_DEL_CENTRO_DE_INVESTIGACION_DE_SISTEMA_Y_TELECOMUNICACION.pdf. [Último acceso: 24 noviembre 2022].

[15] a. networks, «Seguridad perimetral en la empresa,» 17 abril 2017. [En línea]. Available: https://www.adaptixnetworks.com/seguridad-perimetral-empresa/. [Último acceso: 16 diciembre 2022].

[16] www.quitoinforma.gob.ec, «Quito Informa,» 26 abril 2022. [En línea]. [Último acceso: 16 diciembre 2022].

[17] C. N. D. PLANIFICACIÓN, «PLAN NACIONAL DE DESARROLLO 2021, 2025,» 2021.

[18] S. Figueroa, A. Rodríguez, O. Bone y G. Saltos, «La seguridad informática y la seguridad de la información.,» *Polo del conocimiento,* vol. 2, nº 12, pp. 145-155, 2018.

[19] C. Gustavo, «Plataformas de hardware,» Scientia, Soluciones Informaticas, 10 12 2012. [En línea]. Available: https://www.programandoamedianoche.com/2012/12/plataformas-de-hardware/.

[20] L. Mendez, «Redes Empresariales,» Blog de Cisco Latinoamérica, 17 02 2017. [En línea]. Available: https://gblogs.cisco.com/la/en-leobardo-quieres-incrementar-la-eficiencia-en-tu-negocio-domina-tu-borde-de-red/.

[21] G. Baca, Introduccion a la seguridad informática, Mexico D.F.: Grupo editorial Patria, 2016.

[22] Moving-IT, «¿Qué es un firewall o cortafuegos? Tipos de Firewall y funciones. UTM y NGFW.,» 26 enero 2018. [En línea]. Available: https://www.moving-it.net/que-es-un-firewall/.

[23] V. Sánchez, «Elementos básicos de la seguridad perimetral,» Wordpress, 11 enero 2013. [En línea]. Available: https://vicentesanchez90.files.wordpress.com/2013/01/elementos-basicos-de-la-seguridad-perimetral.pdf.

[24] Cisco Systems, Inc., «¿Qué es un cortafuegos?,» [En línea]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

[25] J. Arenas, «Firewalls,» *Controlando el Acceso a la Red,* 2010.

[26] Microsoft, «Configuración de las directivas de seguridad,» 2023.

[27] M. Catro, Introducción a la seguridad informática y el análisis de vulnerabilidades., 3Ciencias, 2018.

[28] P. Lopez, Seguridad Informatica, Editex, 2010.

[29] C. A. D. CLAVIJO, « Políticas de seguridad informática.,» *Entramado,* vol. 2, nº 1, pp. 86-92, 2006.

[30] W. VEGA VELASCO, «Políticas y seguridad de la información.,» *Fides et Ratio-Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia,* vol. 2, nº 2, pp. 63-69, 2008.

[31] G. LÓPEZ y D. LÁZARO, «Sistema de Auditoría de las Políticas de Seguridad Informática del Centro de Ideoinformática.,» *Universidad de las Ciencias Informáticas..*

[32] A. C. L. CASA, «Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador.,» *Ciencias de la Ingeniería y Aplicadas,* vol. 5, nº 2, pp. 82-98, 2021.

[33] M. J. FARRO CACHAY, «Análisis y técnicas de seguridad en redes de informática basado en Open Source, una revisión de la literatura científica en los últimos 5 años.,» Universidad Privada del Norte, 2020.

[34] J. C. e. a. CUEVAS, «Análisis de Vulnerabilidades de Sistemas Web en desarrollo y en producción.,» XX Workshop de Investigadores en Ciencias de la Computación , 2018.

[35] J. M. DIAZ, « Risks and Vulnerabilities of the Denial of Service Distributed on the Internet of Things.,» *Rev. Bioetica & Derecho,* vol. 46, p. 85, 2019.

[36] V. A. PhD, «Metologias de la investigacion,» 2010, pp. 1-5.

[37] L. R. Gay, «Educational Research Neu Jersey,» Estados Unidos, Prentice Hall Inc, 1996.

[38] D. C. F. C. y. D. M. d. P. B. L. D. R. Hernandez Sampieri, «Metodología de la Investigación,» Mexico, Mc Graw Hill, 2014.

[39] J. C. Saavedra, «[Infografía] Metodología Top-Down para el Diseño de Redes,» 2022 06 2022. [En línea]. Available: http://juancarlossaavedra.me/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/. [Último acceso: 16 diciembre 2022].

ANEXOS

ANEXO 1: FORMATO DE ENTREVISTA.

Universidad Estatal Península de Santa Elena

Santa Elena – La Libertad

2023

Entrevista para el proyecto de Titulación

"Propuesta de un sistema de seguridad perimetral informático de un centro de datos de una institución municipal".

Objetivo: Recoger la información necesaria para estudio de seguridad de la data center.

Institución: Gobierno Autónomo Municipal Descentralizado.

Entrevistado: Ing. David Tóala

Cargo: Gerente del departamento de sistemas.

1. **¿Desde qué año existen las instalaciones de la data center de esta institución?**
   Las instalaciones actuales en cuanto en infraestructura del centro de datos existen desde el año 2014

2. **¿Existe actualmente un sistema de seguridad implementado?**
   Se cuenta con dos barreras de protección en cuanto a seguridad de los datos.

3. **¿Qué niveles de seguridad se manejan?**
   Existe un proxy que asegura la navegación.

4. **¿Se usa algún sistema de software o hardware en la institución?**
   Telconet nos provee de un equipo de Fortinet que plantea políticas de seguridad.

5. **¿Qué tipos de servidores existen?**
   Tenemos 5 servidores de correo, web, base de datos y proxys.

6. **¿Cómo está estructurada la red?**
   Tenemos al ISP, después tenemos el Proxy, seguimos con la base de datos y Dominio, de ahí encontramos los switches que reparten la red a los diferentes departamentos

7. **¿Cuántos usuarios existen conectados a la red?**
   Actualmente se cuenta con más de 200 usuarios conectados a la Red.

8. **¿Proporciona red algún otro lado?**

Tenemos antenas que proveen de red al Registro de la propiedad, al taller y a la Matriculación Vehicular

9. **¿A que departamentos abastece de red la infraestructura del municipio?**
   En este edificio se provee de red a departamentos como de alcaldía, vicealcalde, desarrolló comunitario, coactiva, salud ocupacional, comunicación, talento humano, obras públicas, catastro, jurídico, turismo y comunicación

10. **¿La red actualmente está libre de malware?**
    No, actualmente tenemos problemas con malwares que afectan a la conexión y también se encuentra con problemas el servidor de correo.

11. **¿Afecta en la producción diaria la falta de seguridad?**
    Muchas veces se ve estancado la producción de los empleados por infecciones en sus máquinas.

12. **¿Han existido ataques a la data center?**
    Al no poder tener una monitorización no podemos verificar si han existido ataques.

ANEXO 2: FORMATO DE FICHA DE OBSERVACIÓN.

Universidad Estatal Península de Santa Elena

Santa Elena – La Libertad

2023

Formato ficha de observación para el proyecto de Titulación

"Propuesta de un sistema de seguridad perimetral informático de un centro de datos de una institución municipal".

Institución: Gobierno Autónomo Municipal Descentralizado.

Lugar: Santa Elena

Tipo de observación: Directa

Periodo sujeto a revisión: 24 horas

Objetivo: Exploración de estado actual de la institución referente a seguridad informática.

Causas: Falta de implementación de medidas de seguridad informáticas, firewall con sus respectivas políticas de seguridad, llevando un buen control de la red para tener una buena prestación de servicios.

Efectos: La institución cuenta con varias vulnerabilidades de seguridad que puede llevar a perdida de información y presentar problema a la hora de brindar sus servicios a los ciudadanos.

Recomendaciones:

Correctivas:

Proponer un sistema de seguridad perimetral de una adecuada arquitectura de red que lleve a mejorar la seguridad de la entidad a través de herramientas de firewall que permitan controlar la seguridad de la institución.

Preventiva:

Presentar reglas de seguridad que ayuden a mejorar la seguridad de la institución para poder prevenir la perdida de información o los posibles ataques de personas ajenas a la institución de estas.

ANEXO 3: RECOLECCIÓN DE INFORMACIÓN Y BÚSQUEDA DE VULNERABILIDADES.

Para esta recolección de información se van a usar varias herramientas, empezamos con Kali Linux siendo uno de los más reconocidos, este sistema operativo se instaló en una máquina virtual en la herramienta de virtual box con una memoria de 4096 MB, a partir de estas y otras herramientas se va a analizar varias vulnerabilidades.

Fig. 8 Maquina Kali Linux en Virtual box.

En el sistema de Kali Linux en la consola ingresamos el comando nslookup [opción], como opción ingresamos la web (www.xxxxx.gob.ec) es 186.X.X.X como se muestra en la figura.

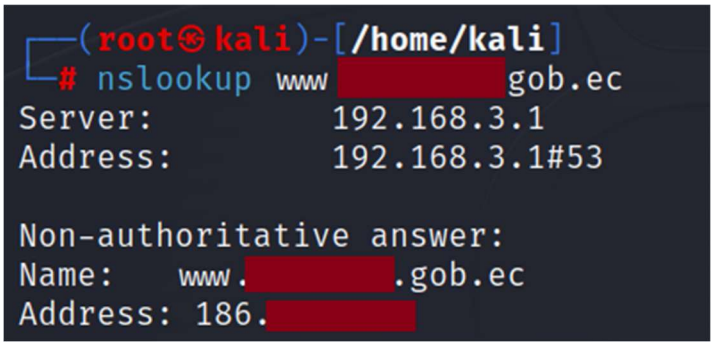


Fig. 9 Ejecución comando nslookup.

Whois es otro comando que proporciona más información del dominio, desde la consola ejecutamos el comando whois con la IP que obtuvimos en el anterior paso y como observamos obtuvimos datos como ID del propietario, nombre del propietario, dirección del país, teléfono, correo electrónico, etc.

```
┌──(root㉿kali)-[/home/kali]
└─# whois 186.[redacted]
% IP Client: 186.66.50.133

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2023-11-27 13:51:19 (-03 -03:00)
```

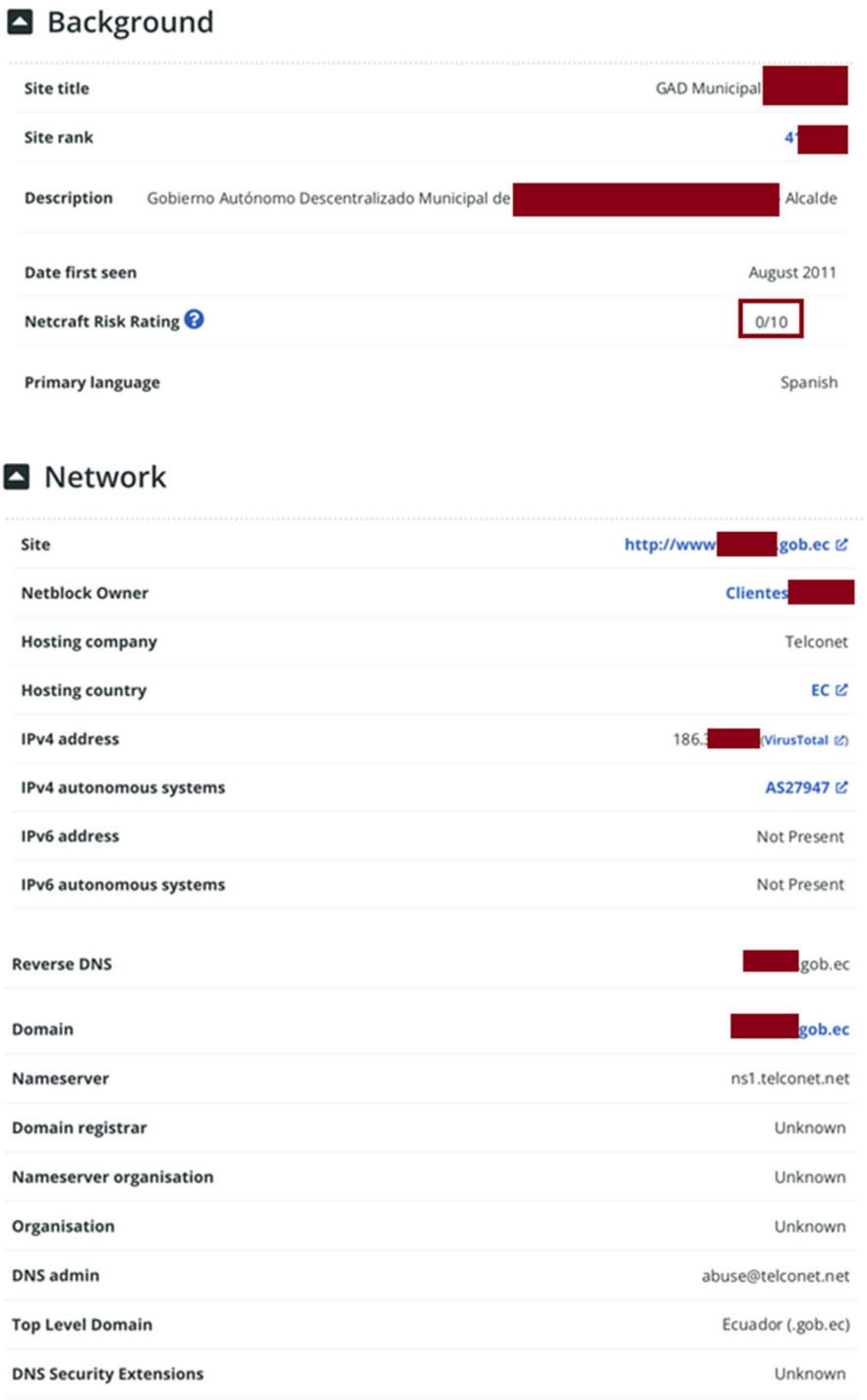
```
inetnum:     186.[redacted]/25
status:      reallocated
aut-num:     N/A
owner:       Clientes[redacted]
ownerid:     EC-CLSA1-LACNIC
responsible: Tomislav Topic
address:     Kennedy Norte Mz. 109 Solar 21, 5, Piso 3
address:     5934 - Guayaquil - GY
country:     EC
phone:       +593 4 2680555 [101]
owner-c:     SEL
tech-c:      SEL
abuse-c:     SEL
created:     20100423
changed:     20100423
inetnum-up:  186.3.64.0/18
```

```
nic-hdl:     SEL
person:      Carlos Montero
e-mail:      networking@telconet.ec
address:     Kennedy Norte MZ, 109, Solar 21
address:     59342 - Guayaquil -
country:     EC
phone:       +593  46020650 [5011]
created:     20021004
changed:     20230724

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Fig. 10 Ejecución comando Whois.

También tenemos a Netcraft que es un sitio web donde se proporciona más datos sobre el dominio, información del servidor y del sistema operativo donde se ejecuta.



Background

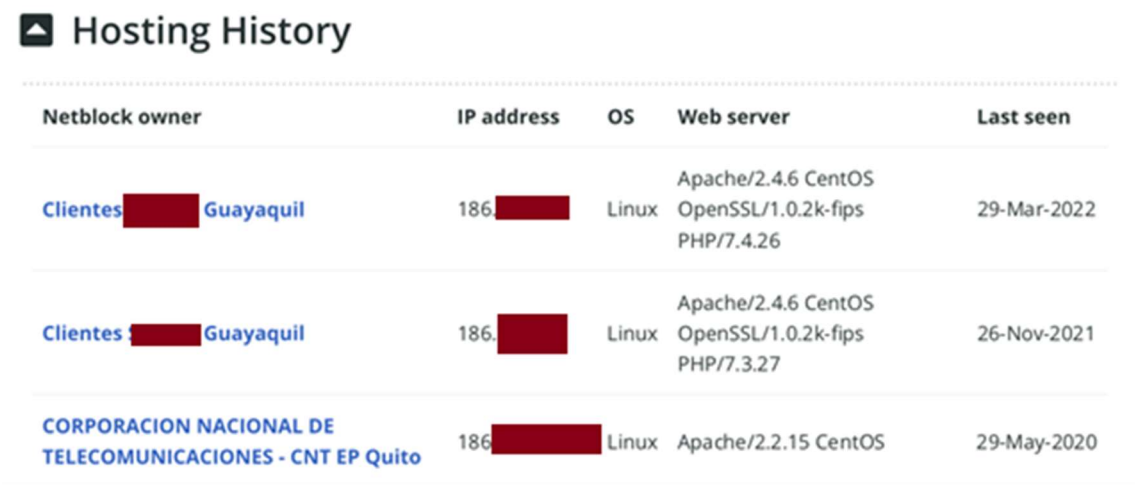
Site title	GAD Municipal [redacted]
Site rank	4[redacted]
Description	Gobierno Autónomo Descentralizado Municipal de [redacted] Alcalde
Date first seen	August 2011
Netcraft Risk Rating	0/10
Primary language	Spanish

Network

Site	http://www[redacted]gob.ec
Netblock Owner	Clientes[redacted]
Hosting company	Telconet
Hosting country	EC
IPv4 address	186.[redacted] (VirusTotal)
IPv4 autonomous systems	AS27947
IPv6 address	Not Present
IPv6 autonomous systems	Not Present
Reverse DNS	[redacted]gob.ec
Domain	[redacted]gob.ec
Nameserver	ns1.telconet.net
Domain registrar	Unknown
Nameserver organisation	Unknown
Organisation	Unknown
DNS admin	abuse@telconet.net
Top Level Domain	Ecuador (.gob.ec)
DNS Security Extensions	Unknown

Fig. 11 Resultados de la herramienta Netcraft.
(Fuente: Netcraft)

También podemos observar el historial del hospedaje, el sistema operativo donde se ejecuta y como también el web server del dominio, como se ve en la siguiente imagen.



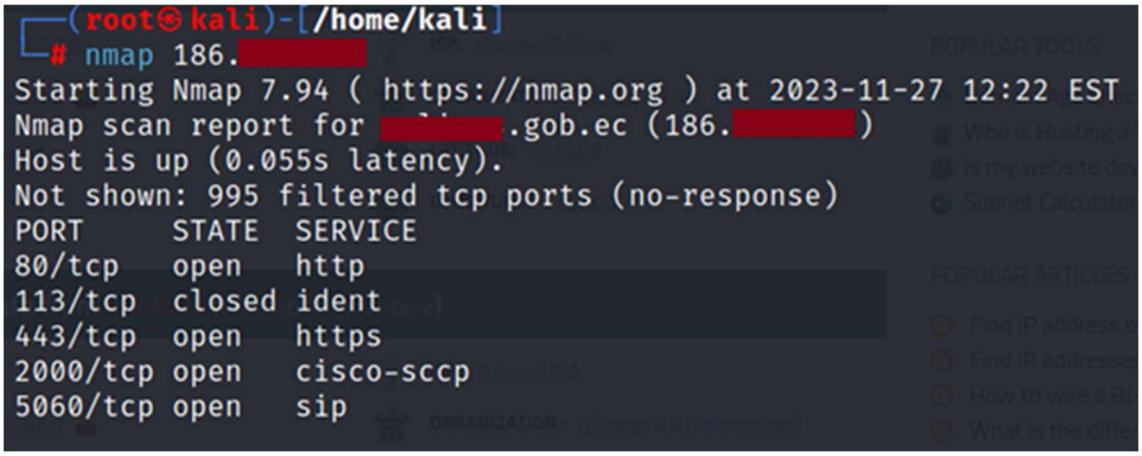
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Clientes [redacted] Guayaquil	186.[redacted]	Linux	Apache/2.4.6 CentOS OpenSSL/1.0.2k-fips PHP/7.4.26	29-Mar-2022
Clientes [redacted] Guayaquil	186.[redacted]	Linux	Apache/2.4.6 CentOS OpenSSL/1.0.2k-fips PHP/7.3.27	26-Nov-2021
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	186[redacted]	Linux	Apache/2.2.15 CentOS	29-May-2020

Fig. 12 Resultados del historial del hosting.

(Fuente: Netcraft)

Se tiene también la herramienta nmap que es para el escaneo de vulnerabilidades, que se orienta al reconocimiento de redes y los puertos abiertos en esto, con el comando nmap hace un escaneo a 1000 puertos que entre los más comunes tenemos a TCP, UDP, ICMP, entre otros.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 186.[redacted]
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-27 12:22 EST
Nmap scan report for [redacted].gob.ec (186.[redacted])
Host is up (0.055s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
2000/tcp open   cisco-sccp
5060/tcp open   sip
```

Fig. 13 Ejecución comando nmap.

Se realizo un escaneo de vulnerabilidad con la herramienta Shodan al ser un escaneo sin utilizar fuerza bruta a la IP pública del municipio donde nos arrojaron varias vulnerabilidades, y así mismo mostro los puertos abiertos de esta institución.

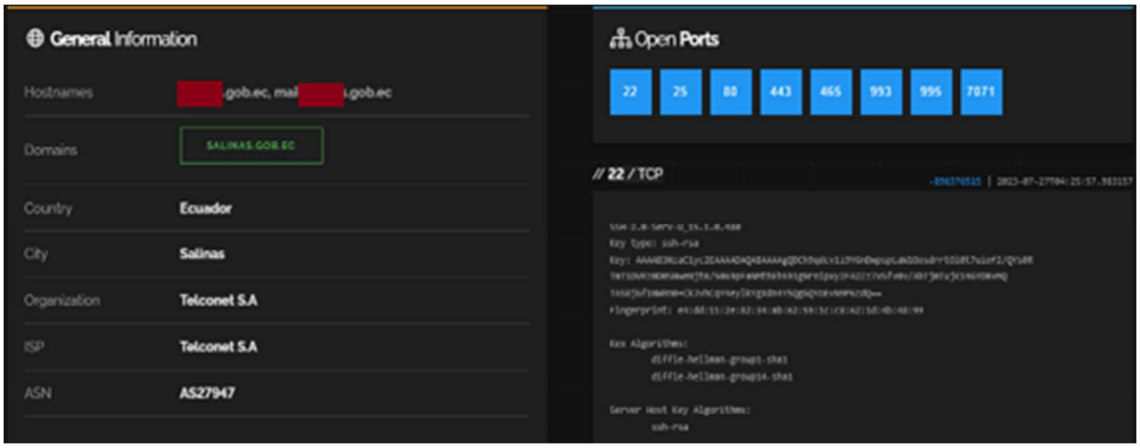


Fig. 14 Análisis red externa

(Fuente:Shoodam)

Podemos ver que se encuentra abiertos puertos como el 7071 que es donde se encuentra la cuenta de administrador de Zimbra.

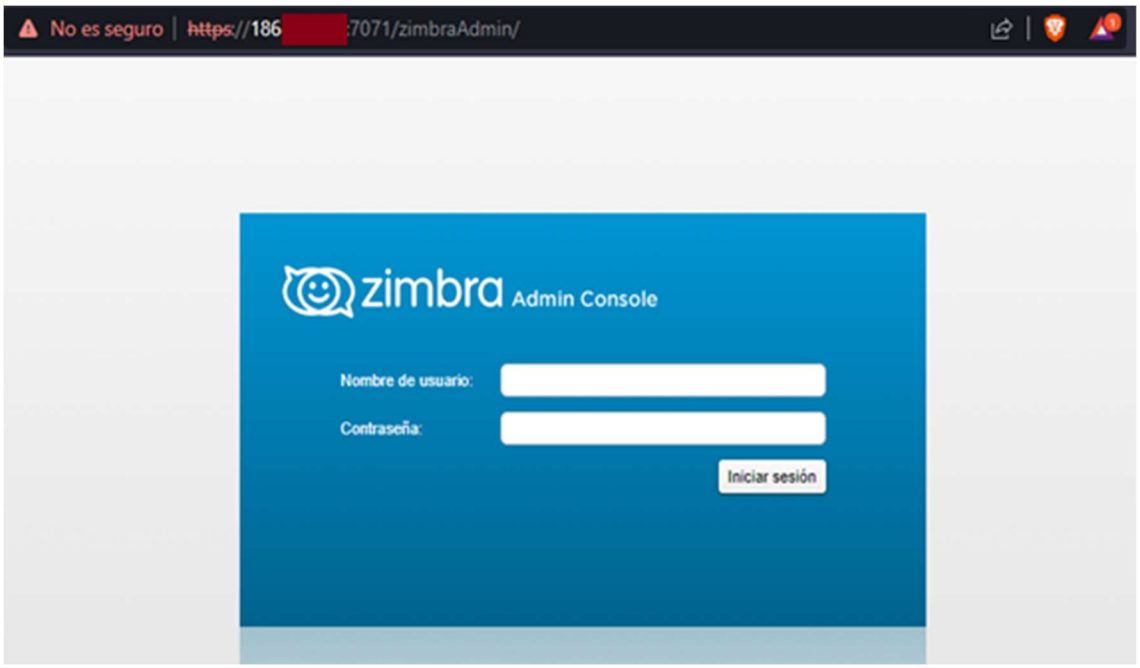


Fig. 15 Consola Admin Zimbra

(Fuente: página web institución)

Así mismo se encontró abierto el puerto 22 de protocolo SSH de red destinado principalmente a la conexión con máquinas a las que accedemos por la línea de comandos. En otras palabras, con SSH podemos conectarnos con servidores, usando la red Internet como vía para las comunicaciones, pero sino está en uso es un peligro latente a los servidores de la institución.

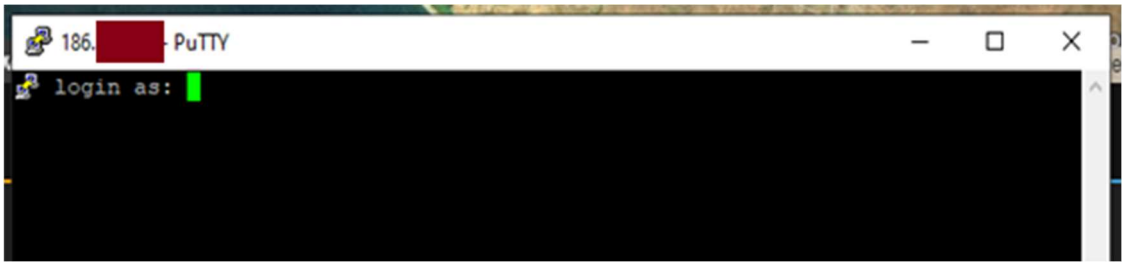


Fig. 16 Conexión exitosa SSH

(Fuente: Putty)

ANEXO 4: INSTALACIÓN Y CONFIGURACIÓN DE LAS HERRAMIENTAS DE SEGURIDAD PERIMETRAL

Instalación y Configuración de PFSense (Firewall) Este sistema de cortafuegos está basado en FreeBSD que presenta diversas características y es de código abierto, aunque es la versión gratuita, es una de las mejores herramientas de Firewall que existen. En la Figura 17, se muestra la configuración de las interfaces que manejará pfsense dentro de la arquitectura como se planteó en la imagen.

Fig. 17 Interfaz configuradas en Firewall PfSense

En la Figura 17, se enseña la información general, las interfaces, gateways, y alguno que otro registro dentro del Firewall. Así como también podemos observar las interfaces que creamos en línea de comando en el sistema de Pfsense.

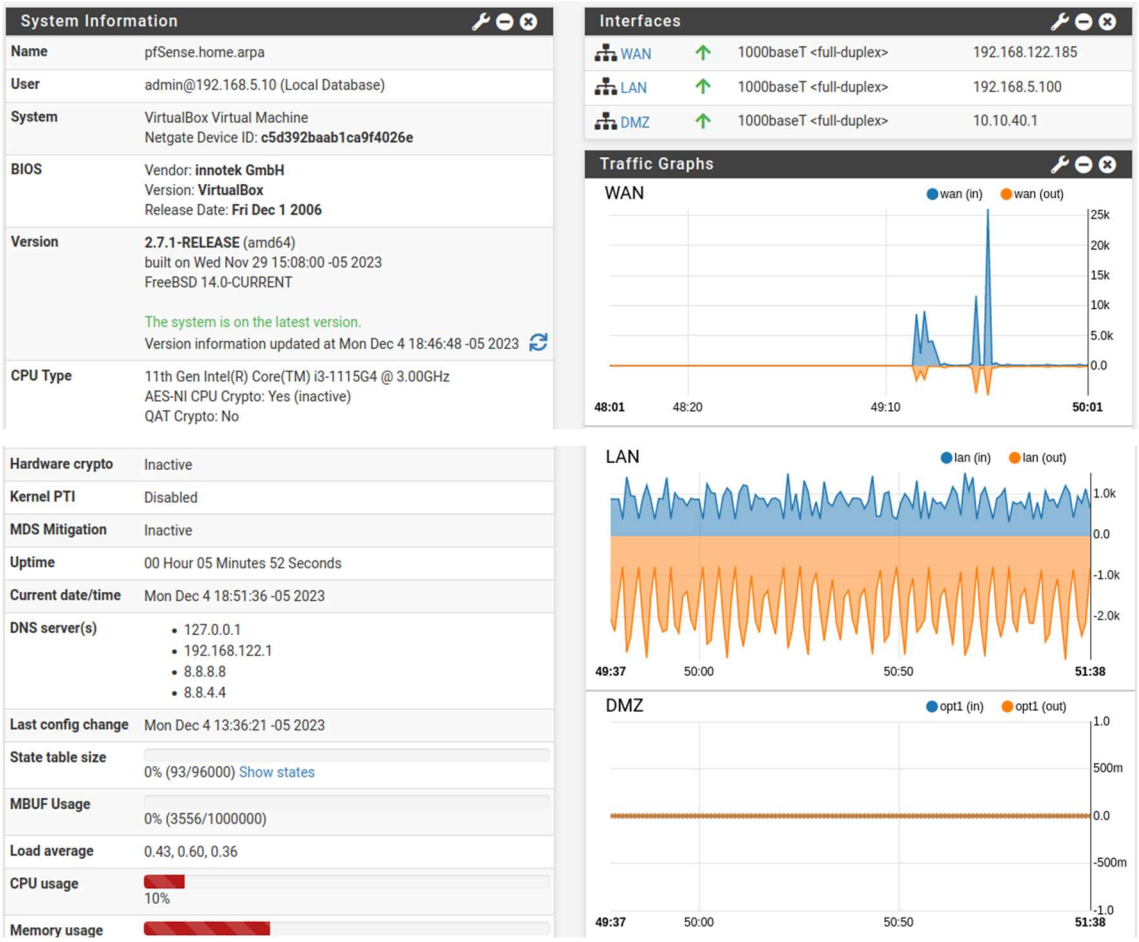


Fig. 18 Interfaz de PfSense

Mediante el panel de administración se configuran las interfaces de las redes agregadas, y se definen reglas de filtrado para cada una de estas (ver Figura 18, Figura 19 y Figura 20).

Definición de Reglas para WAN – PFSense

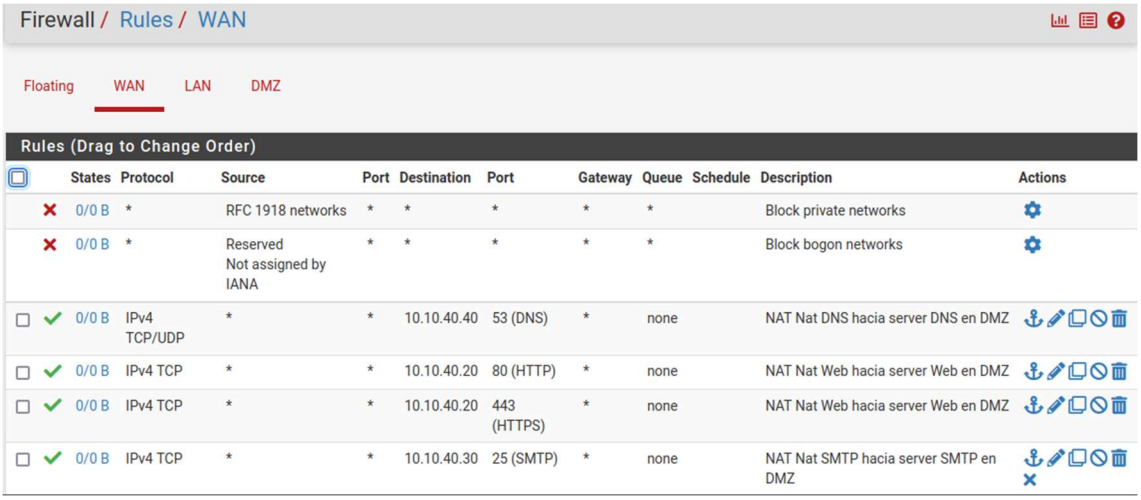
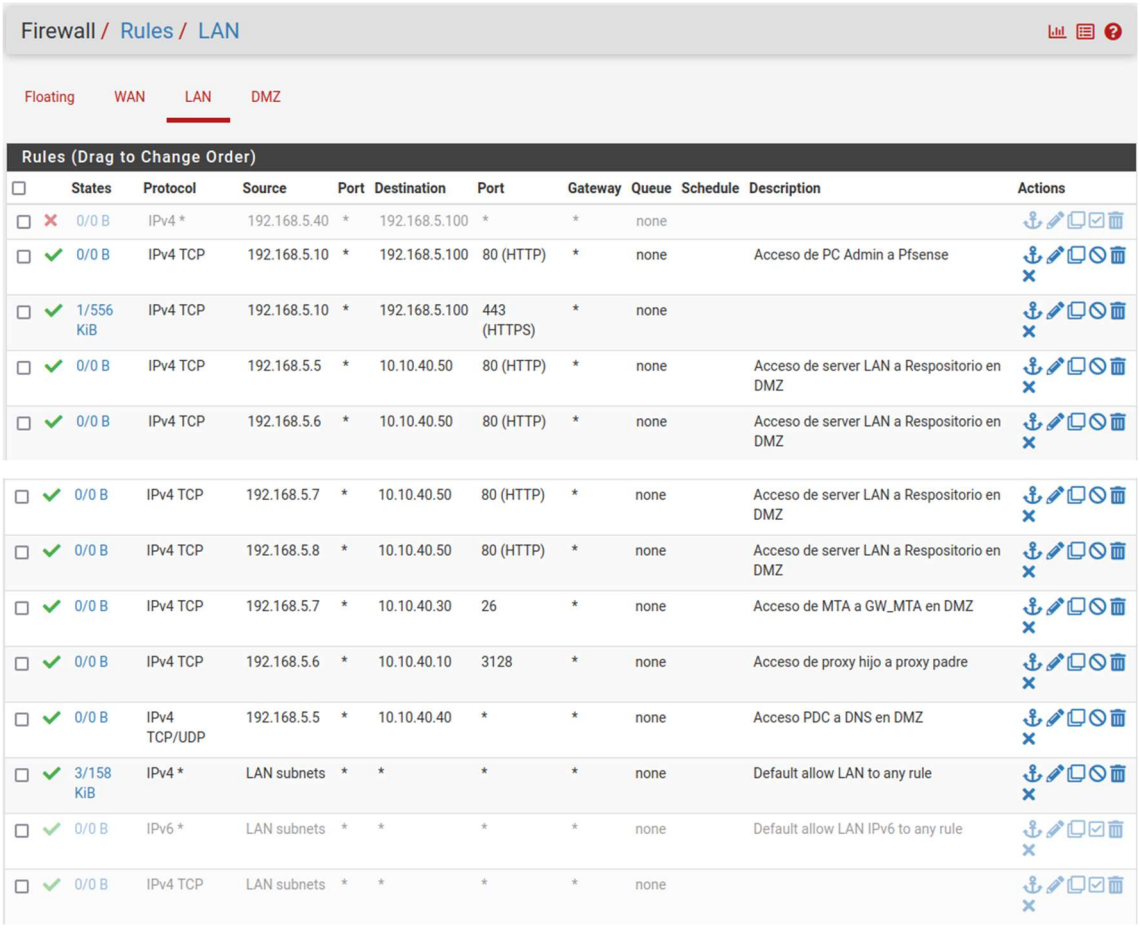


Fig. 19 Reglas para WAN

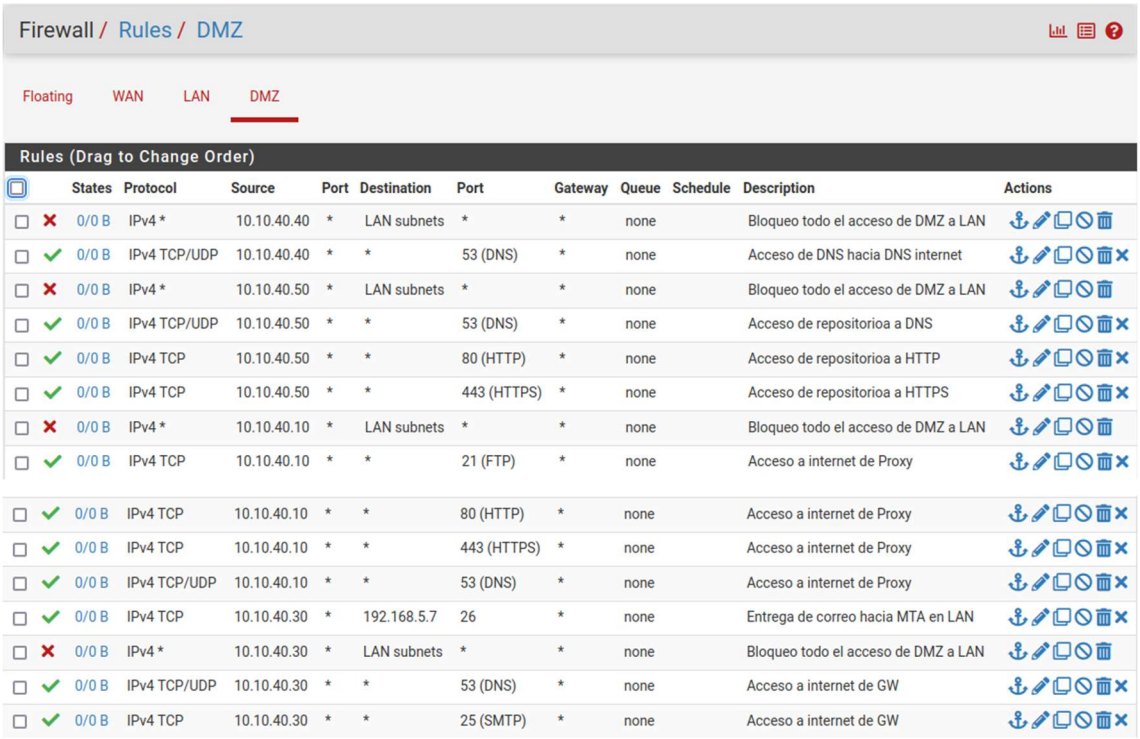
Definición de Reglas para LAN – PFSense



States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	192.168.5.40	*	192.168.5.100	*	*	none			
0/0 B	IPv4 TCP	192.168.5.10	*	192.168.5.100	80 (HTTP)	*	none		Acceso de PC Admin a Pfsense	
1/556 KiB	IPv4 TCP	192.168.5.10	*	192.168.5.100	443 (HTTPS)	*	none			
0/0 B	IPv4 TCP	192.168.5.5	*	10.10.40.50	80 (HTTP)	*	none		Acceso de server LAN a Respositorio en DMZ	
0/0 B	IPv4 TCP	192.168.5.6	*	10.10.40.50	80 (HTTP)	*	none		Acceso de server LAN a Respositorio en DMZ	
0/0 B	IPv4 TCP	192.168.5.7	*	10.10.40.50	80 (HTTP)	*	none		Acceso de server LAN a Respositorio en DMZ	
0/0 B	IPv4 TCP	192.168.5.8	*	10.10.40.50	80 (HTTP)	*	none		Acceso de server LAN a Respositorio en DMZ	
0/0 B	IPv4 TCP	192.168.5.7	*	10.10.40.30	26	*	none		Acceso de MTA a GW_MTA en DMZ	
0/0 B	IPv4 TCP	192.168.5.6	*	10.10.40.10	3128	*	none		Acceso de proxy hijo a proxy padre	
0/0 B	IPv4 TCP/UDP	192.168.5.5	*	10.10.40.40	*	*	none		Acceso PDC a DNS en DMZ	
3/158 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
0/0 B	IPv4 TCP	LAN subnets	*	*	*	*	none			

Fig. 20 Reglas para LAN

Definición de Reglas para DMZ – PFSense



	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/0 B	IPv4 *	10.10.40.40	*	LAN subnets	*	*	none		Bloqueo todo el acceso de DMZ a LAN	
✓	0/0 B	IPv4 TCP/UDP	10.10.40.40	*	*	53 (DNS)	*	none		Acceso de DNS hacia DNS internet	
✗	0/0 B	IPv4 *	10.10.40.50	*	LAN subnets	*	*	none		Bloqueo todo el acceso de DMZ a LAN	
✓	0/0 B	IPv4 TCP/UDP	10.10.40.50	*	*	53 (DNS)	*	none		Acceso de repositorioa a DNS	
✓	0/0 B	IPv4 TCP	10.10.40.50	*	*	80 (HTTP)	*	none		Acceso de repositorioa a HTTP	
✓	0/0 B	IPv4 TCP	10.10.40.50	*	*	443 (HTTPS)	*	none		Acceso de repositorioa a HTTPS	
✗	0/0 B	IPv4 *	10.10.40.10	*	LAN subnets	*	*	none		Bloqueo todo el acceso de DMZ a LAN	
✓	0/0 B	IPv4 TCP	10.10.40.10	*	*	21 (FTP)	*	none		Acceso a internet de Proxy	
✓	0/0 B	IPv4 TCP	10.10.40.10	*	*	80 (HTTP)	*	none		Acceso a internet de Proxy	
✓	0/0 B	IPv4 TCP	10.10.40.10	*	*	443 (HTTPS)	*	none		Acceso a internet de Proxy	
✓	0/0 B	IPv4 TCP/UDP	10.10.40.10	*	*	53 (DNS)	*	none		Acceso a internet de Proxy	
✓	0/0 B	IPv4 TCP	10.10.40.30	*	192.168.5.7	26	*	none		Entrega de correo hacia MTA en LAN	
✗	0/0 B	IPv4 *	10.10.40.30	*	LAN subnets	*	*	none		Bloqueo todo el acceso de DMZ a LAN	
✓	0/0 B	IPv4 TCP/UDP	10.10.40.30	*	*	53 (DNS)	*	none		Acceso a internet de GW	
✓	0/0 B	IPv4 TCP	10.10.40.30	*	*	25 (SMTP)	*	none		Acceso a internet de GW	

Fig. 21 Reglas para DMZ

Instalación y Configuración de SNORT

No solo nos podemos nos podemos quedar con las funciones básicas que nos ofrece Pfsense, ya que este facilita la instalación de los distintos paquetes que nos van a ayudar a llevar un contro de la seguridad del sistema, como primera herramienta tenemos el paquete de detección y prevención de intrusos SNORT, dentro de Administrador de paquetes del firewall, buscamos al IPS y seleccionamos la opción de instalar. (ver Figura 21 y Figura 22)

Administrador de paquetes – Selección de SNORT

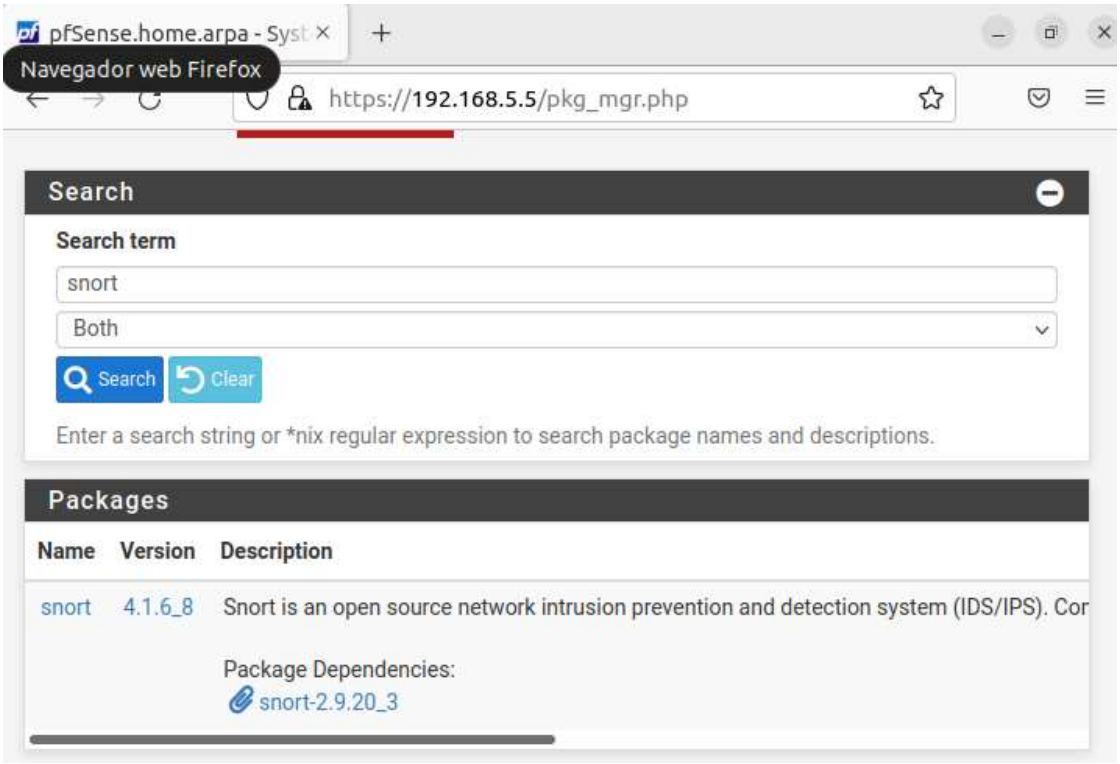


Fig. 22 Fichero para la instalación de Snort

Instalación Completada – SNORT

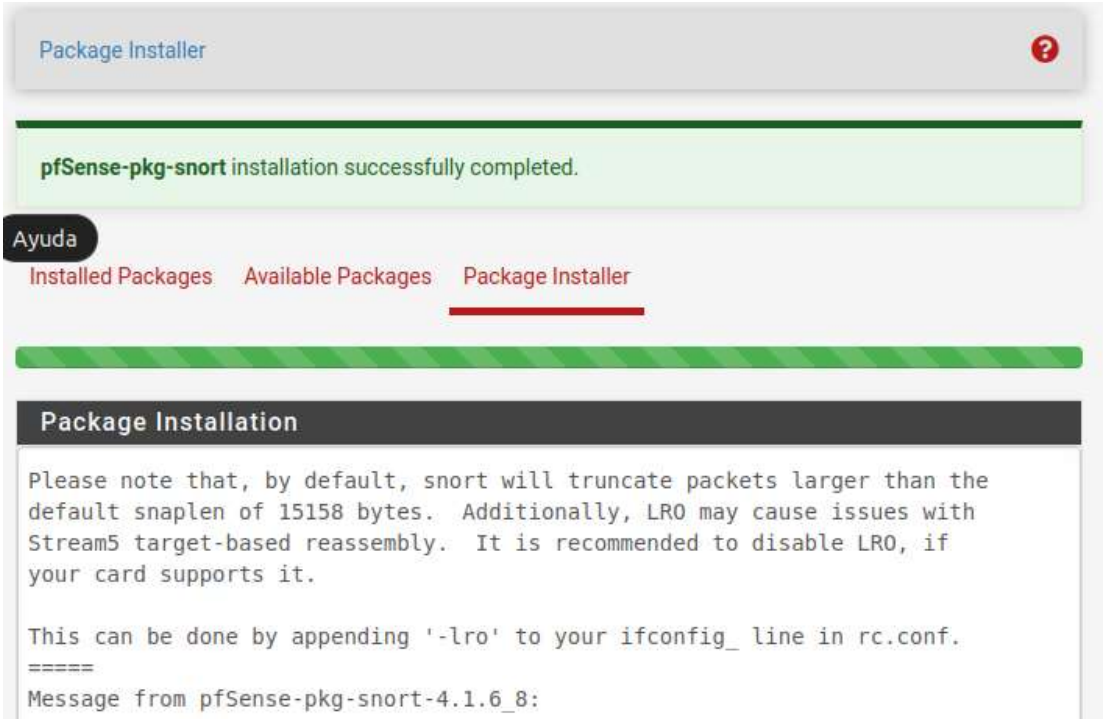


Fig. 23 Instalación completa de Snort

Para descargar las reglas que SNORT proporciona, fue necesario crearse una cuenta en el sitio oficial de este IPS, y generar el OINKCODE, que nos posibilita la descarga de esta regla como muestra la imagen 24.

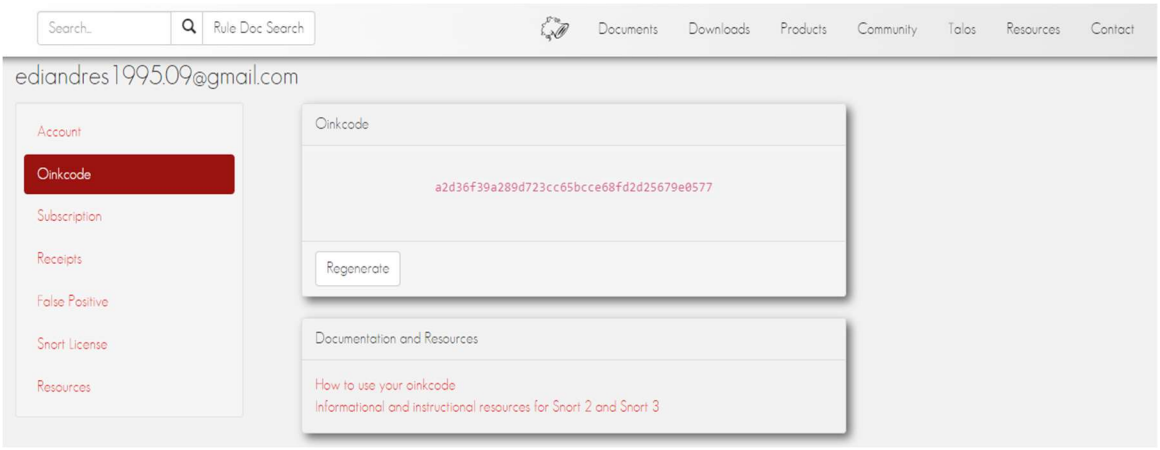


Fig. 24 Obtención de OINKCODE

Configuración Globales – SNORT

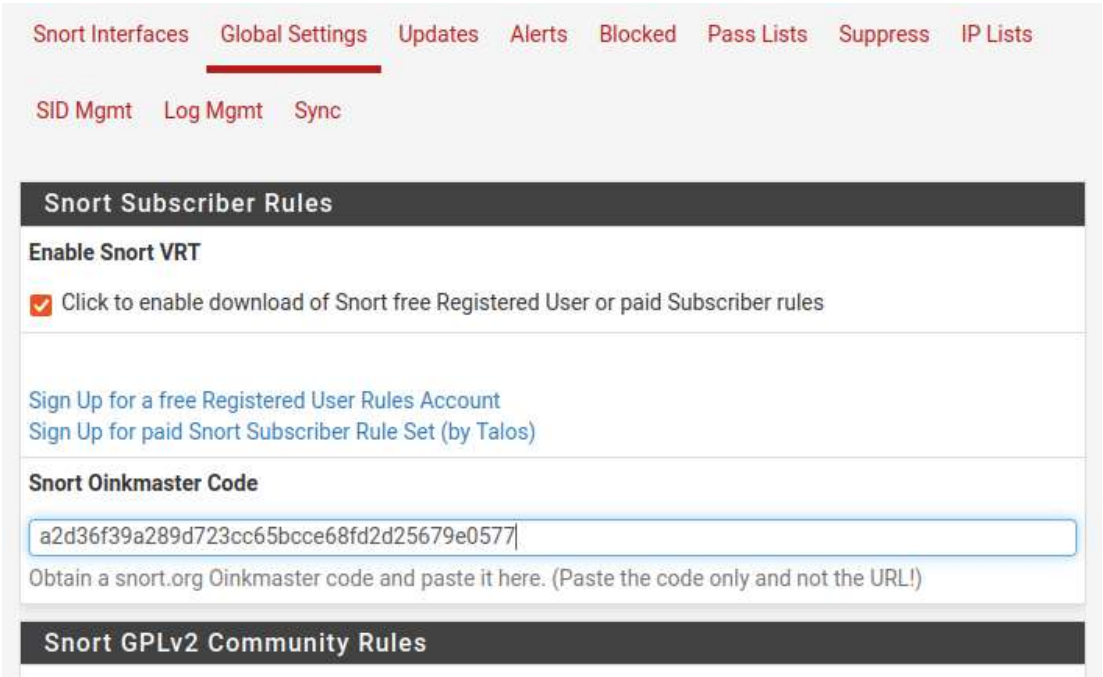


Fig. 25 Configuración Globales de Snort

Instalación Completa de Reglas – SNORT

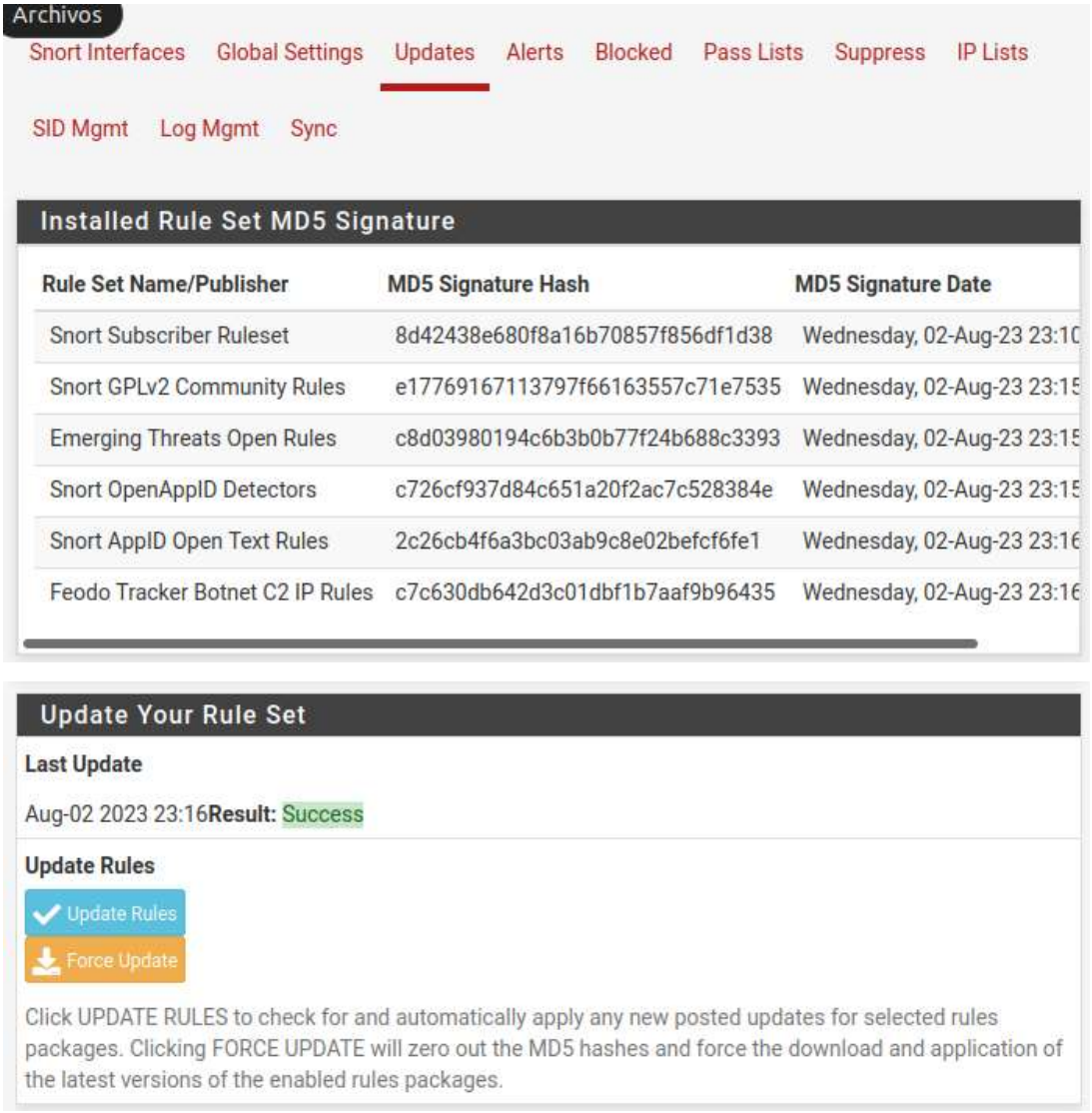


Fig. 26 Instalación de reglas Snort

En la Figura 26, podemos ver las reglas definidas para las interfaces WAN y LAN de la Arquitectura mediante SNORT.

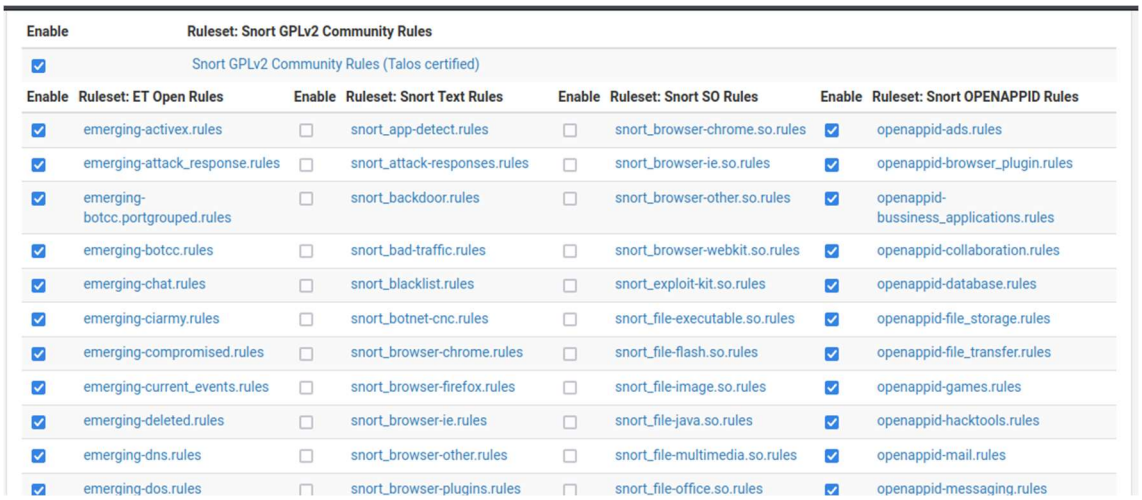


Fig. 27 Implementación de reglas Snort

Una vez configuradas las reglas es necesario habilitar el servicio de snort en cada interfaz como se muestra a continuación.

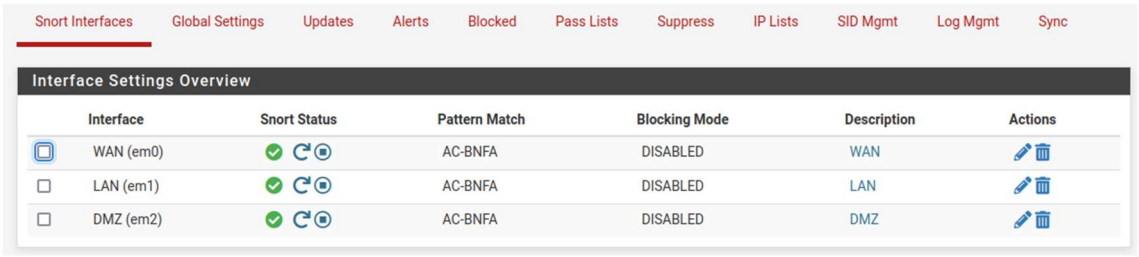


Fig. 28 Estado de las interfacez.

En Snort existen dos modos de configuración en alerta y bloqueo, en este proyecto esta configurado como alerta para ver el tráfico existente en las interfaces y habilitar el bloqueo de acuerdo de las necesidades de la empresa, ya que si se activa sin saber cada una de las reglas que existen se podría perder el acceso a la red.

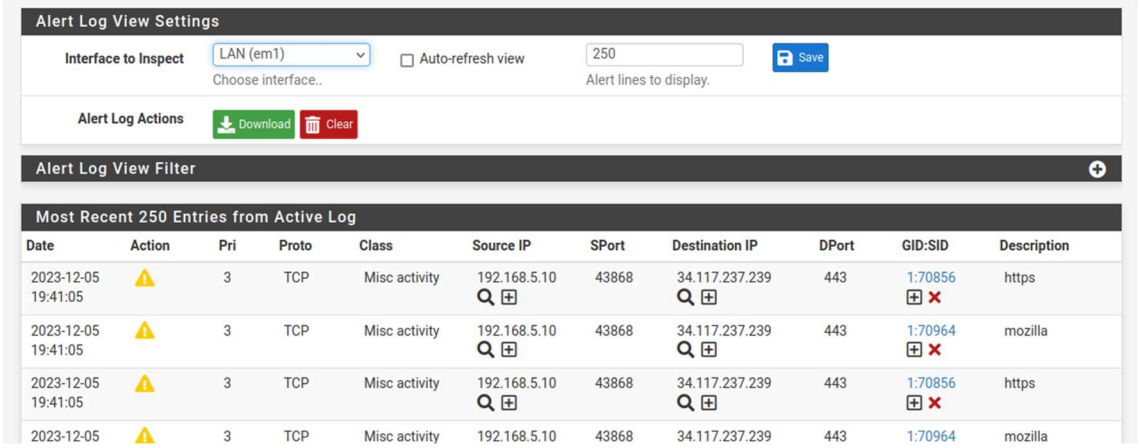


Fig. 29 Alertas de navegación en Snort

Así como tenemos Snort también contamos con Paquetes Squid que nos van a ayudar en varias reglas de seguridad del sistema como se va a presentar a continuación. En la figura 27 se aprecia la instalación en INstalled Packages de los 3 paquetes comenzando con Squid, SquidGuard y Lightsquid.

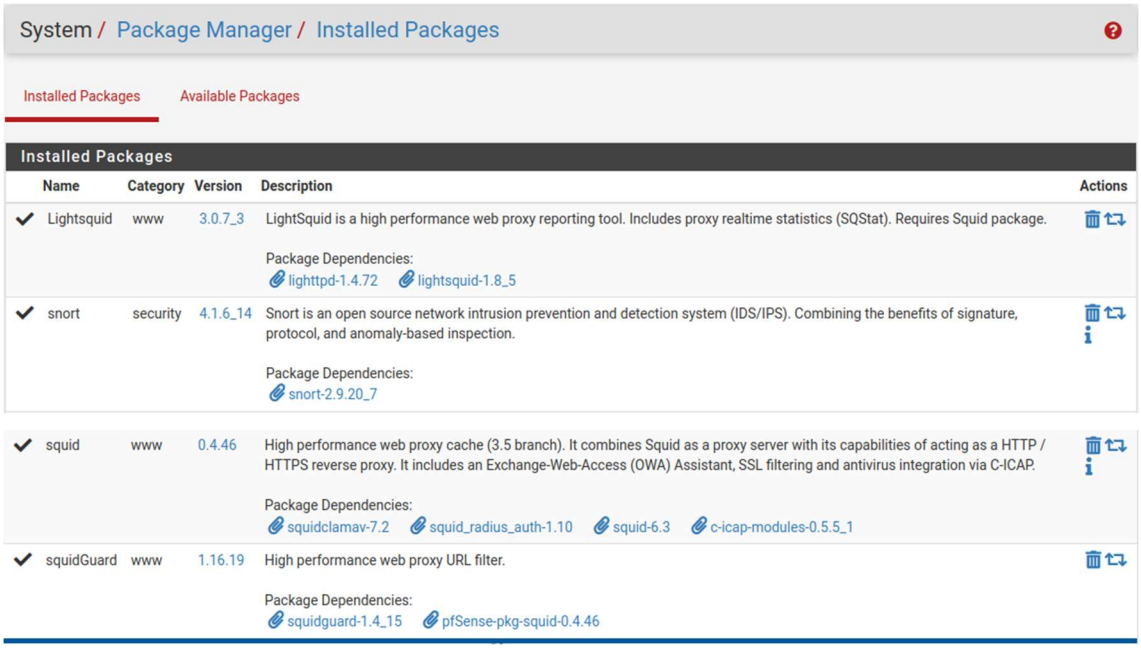


Fig. 30 Instalación de paquetes Squid, SquidGuard y Lightsquid.

Configuración de Servidor Proxy

En la figura 27 se configura las políticas de reemplazo, distinguiendo las diferencias y usos de políticas de reemplazo lo más factible es usar el HEAP-LFUDA, el reemplazo o la funcionalidad de esta política entrara cuando este a más de 90% y menos de 95%.

HEAP-LFUDA: Es una variante de la política de reemplazo LFU (Leasrt Frecuently Used), integra un contador dentro de la caché que clasifica a las webs por tiempo eliminando las más antiguas, a las páginas más usadas se les clasifica por tiempo indefinido

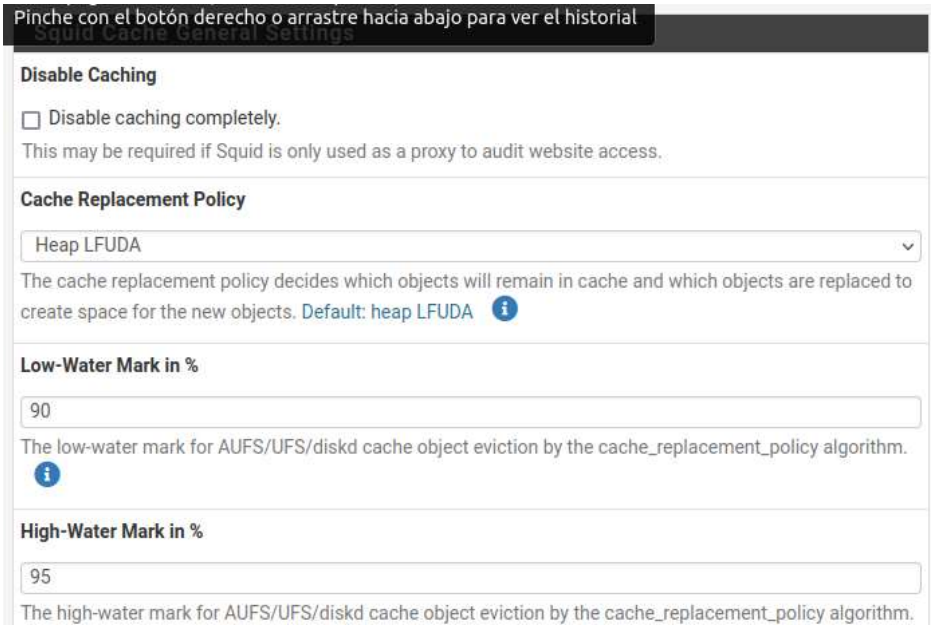


Fig. 31 Configuración de política de reemplazo.

Configuración de Cache

Para la configuración de caché es necesario tener en cuenta la capacidad de hardware en la que está instalado el sistema.

El máximo tamaño que debe tener una web o un archivo para guardarse en el web proxy por defecto pone 4 megabytes. En el caso del sistema de la Oficina Departamental de Estadística de Junín se asigna un tamaño de 10000 Mb o 10Gb guardando los archivos en formato ufs, la ubicación en /var/squid/cache con un tamaño mínimo de 0 kilobytes hasta 4 megabytes como se aprecia en la figura 29.

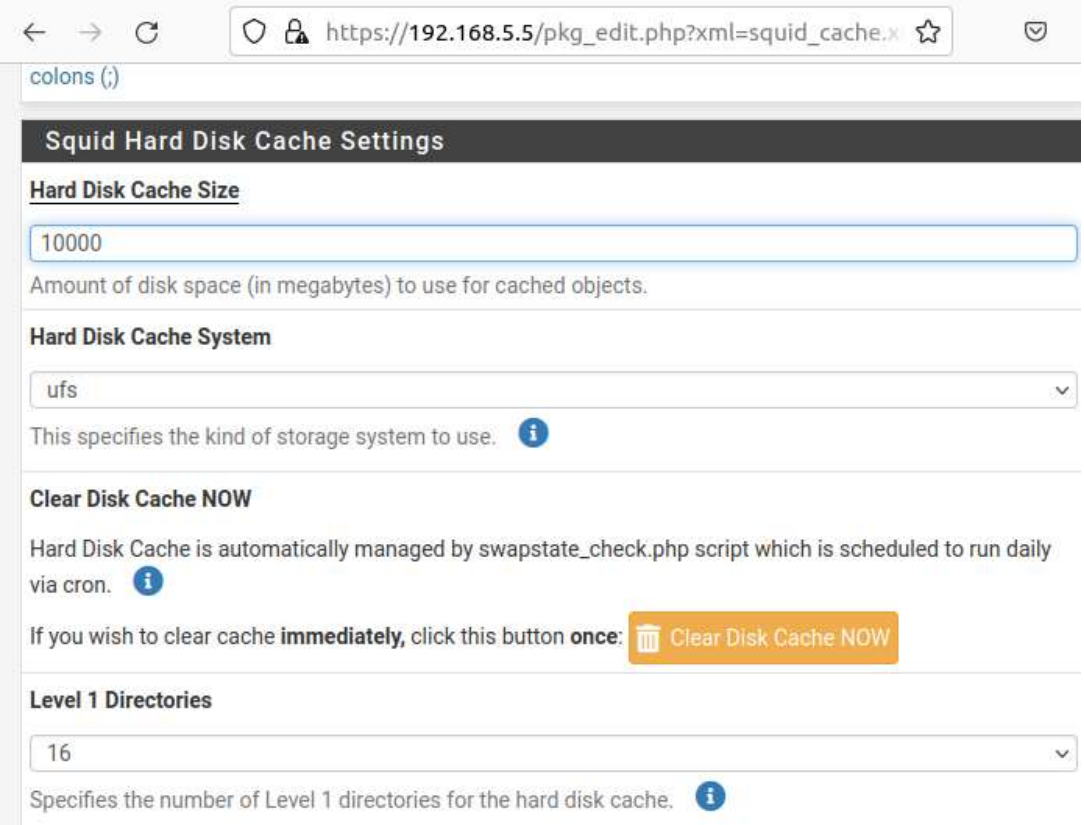


Fig. 32 Configuración de la cache Fuente.

Reglas generales

En Services se da click a Squid Proxy Server, donde se da check al Enable Squid Proxy para habilitar, en el proxy Interface se selecciona la LAN y loopback para mayor precisión del servidor proxy, se usa el puerto por defecto del squid 3128 que sirve para asignar un protocolo.

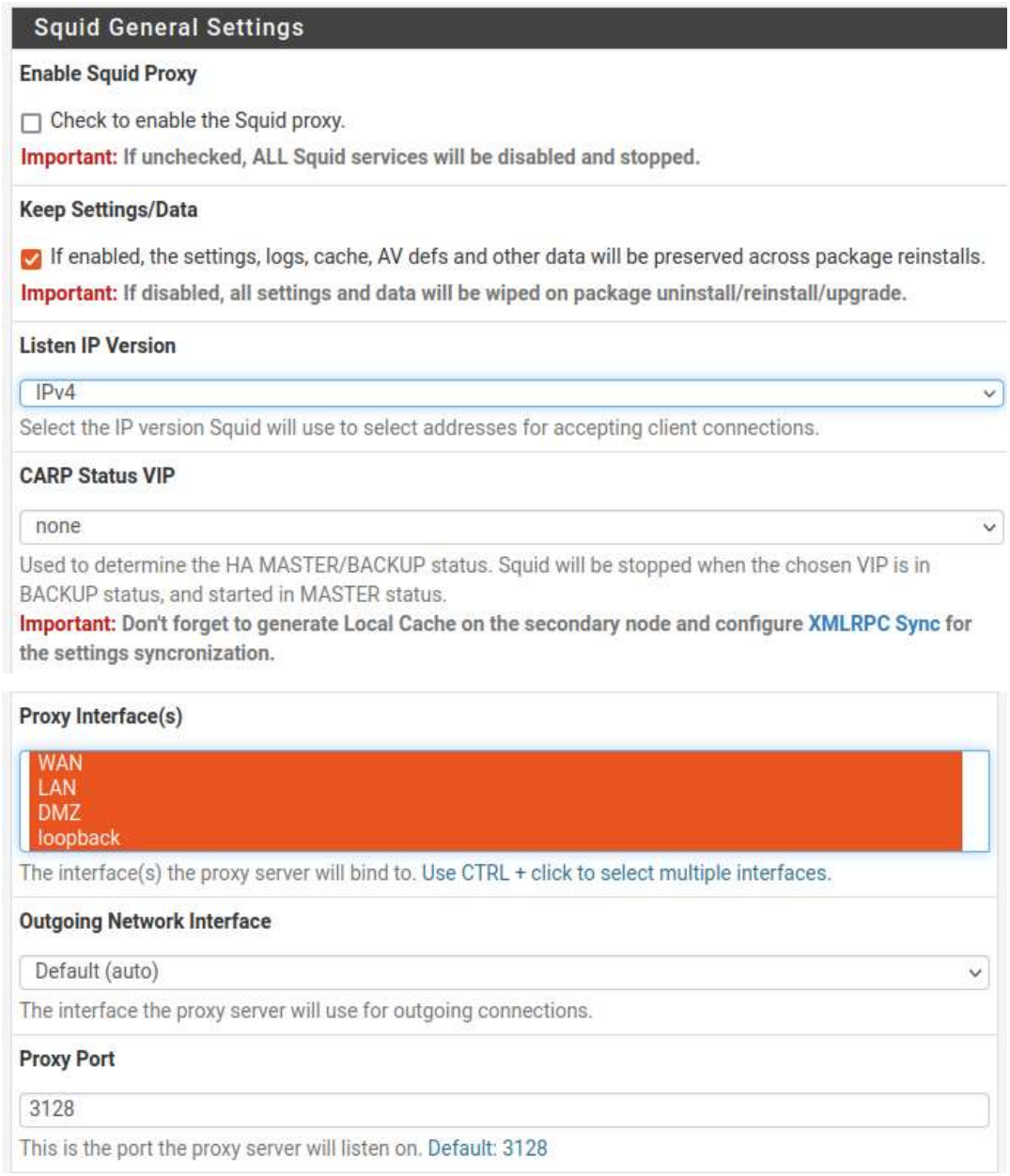


Fig. 33 Configuración del servidor proxy.

Configuración de Logs

Para la configuración de Logs se habilita en general el Enable Access Logging se usa la ruta por defecto del log var/squid/logs.En la figura 29 se realiza las configuraciones y también el Rotate Logs que señala los logs de navegación serán guardados y rotados cada 5 día para que el espacio de memoria no termine llenándose, para finalizar se habilita la opción Log Pages Denied by Squidguard que enlaza los datos almacenados con Squid.

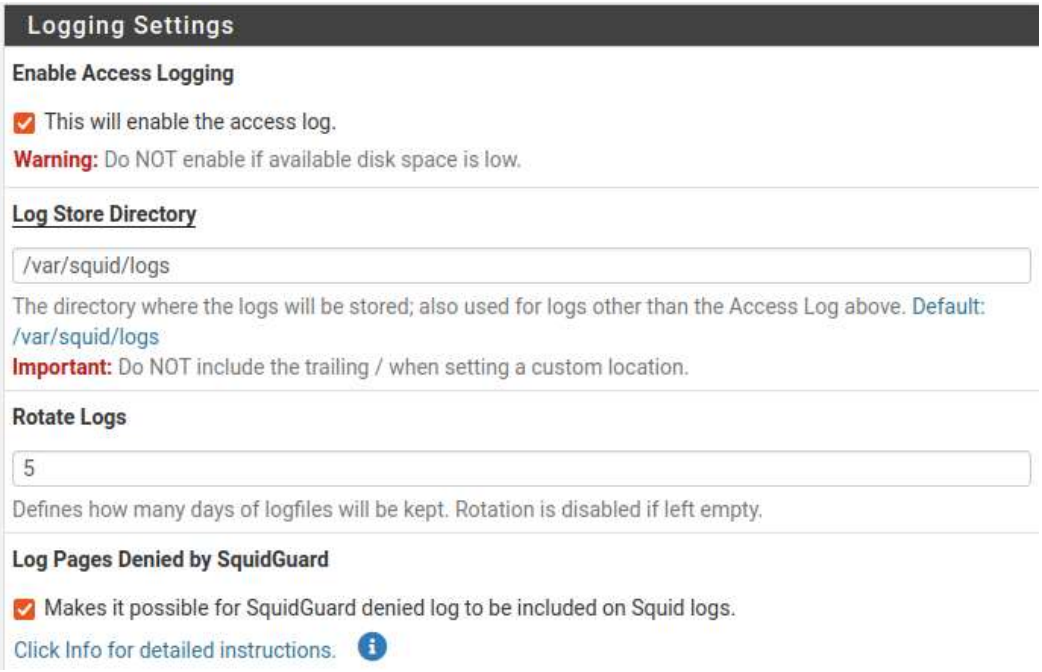


Fig. 34 Habilitación de Logs.

Configuración de notificaciones.

Toda la información puede ser dirigida a un correo para poder ver las alertas o puntos críticos, también automatiza el uso de información. En la siguiente figura se aprecia que el Visible Hostname, en el Adminitrators Email se agrega el correo del administrador de red ediandres1995.09@gmail.com donde le van a llegar alertas de los eventos que ocurran en el firewall.

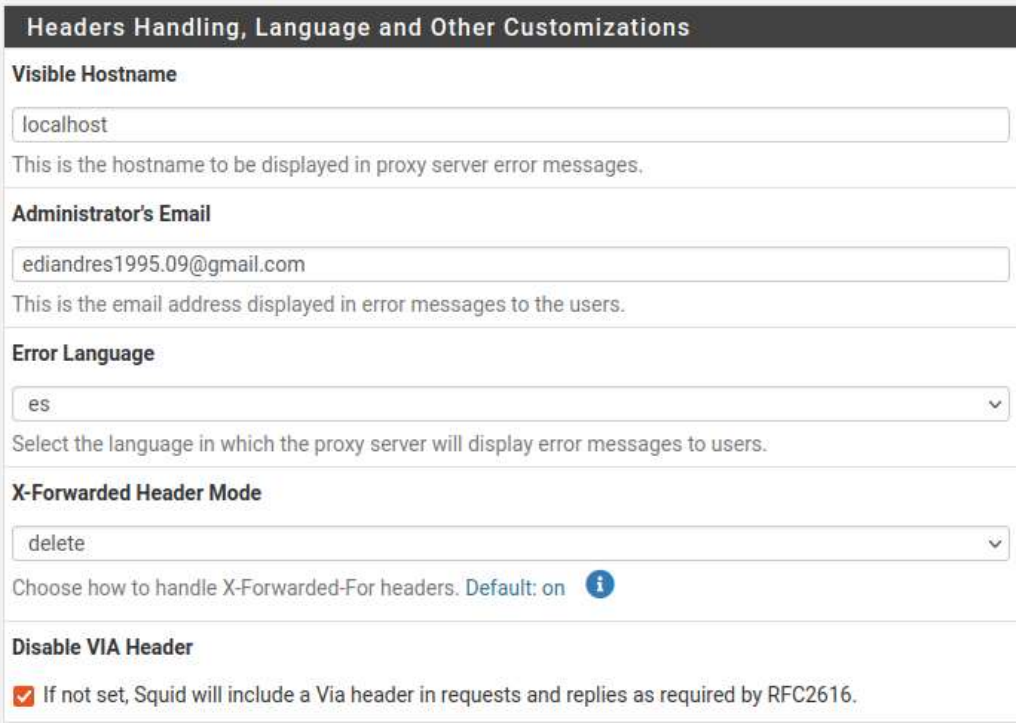


Fig. 35 Configuración de notificaciones.

Control de lista de accesos

La seguridad será manejada con la configuración de ACL (Access Control List), en el web proxy configurado se implementa el ACL que se usa para filtrar y administrar el acceso a páginas generalmente navegadas como Youtube, Facebook, páginas que contengan virus o de ocio que consumen bando de ancha.

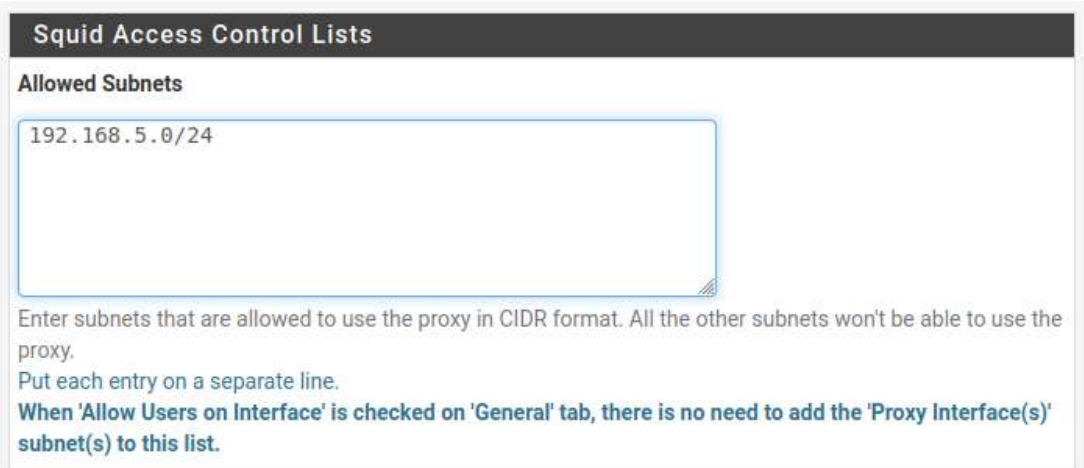


Fig. 36 Autorización de control de lista de acceso a la red interna.

En la figura 32 se dirige a la pestaña de blaklist donde se hace uso del siguiente link http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz el cual contiene carpetas con URLs conocidas, después se da click en Download.

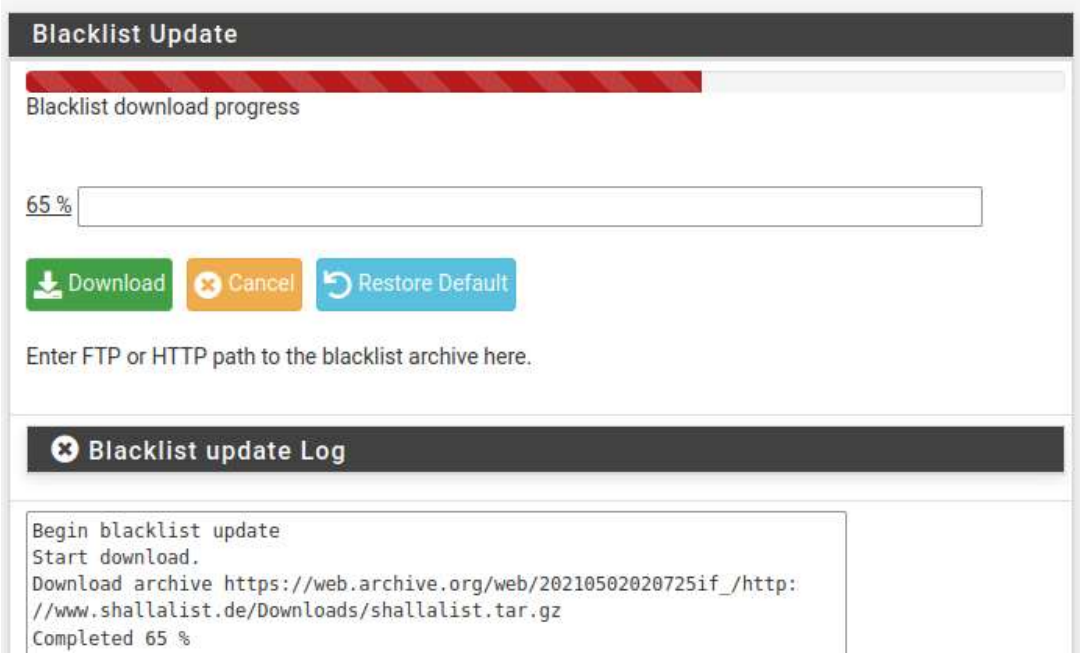


Fig. 37 Descarga de Blacklist.

Common ACL: En Target Rules List se carga las carpetas que contienen las URLs descargadas en la BlackList, en la figura 33 se selecciona el tipo de acceso entre denegar pasar a lista blanca o simplemente no realizar ninguna acción, en el capítulo uno se evaluó el tráfico de red tomando como guía se seleccionará las carpetas para denegar el tráfico.

Fig. 38 Denegación de páginas.

Groups ACL

En esta parte se configura los grupos se realiza la siguiente configuración.

- Disabled: Si se activa el check, la regla queda inactiva, se deja sin check.
- Name: Perfil 01.
- Order: Sin orden.
- Client (source): Agregar todas las IP's que tengan autorización para el uso de perfil 1.
- Target Rules: Se despliega la lista y se hace Deny: alcohol, anonvpn, chat, hacking, hobby_games-misc, hobby_gamesonline, movies, music, porn, radiotv, remotecontrol, ringtones, spyware, tracker, updatesites, webradio, webtv.
- WhiteList: YouTube, descargas_office.
- Default access [all]: allow.
- Log: Habilitar check.

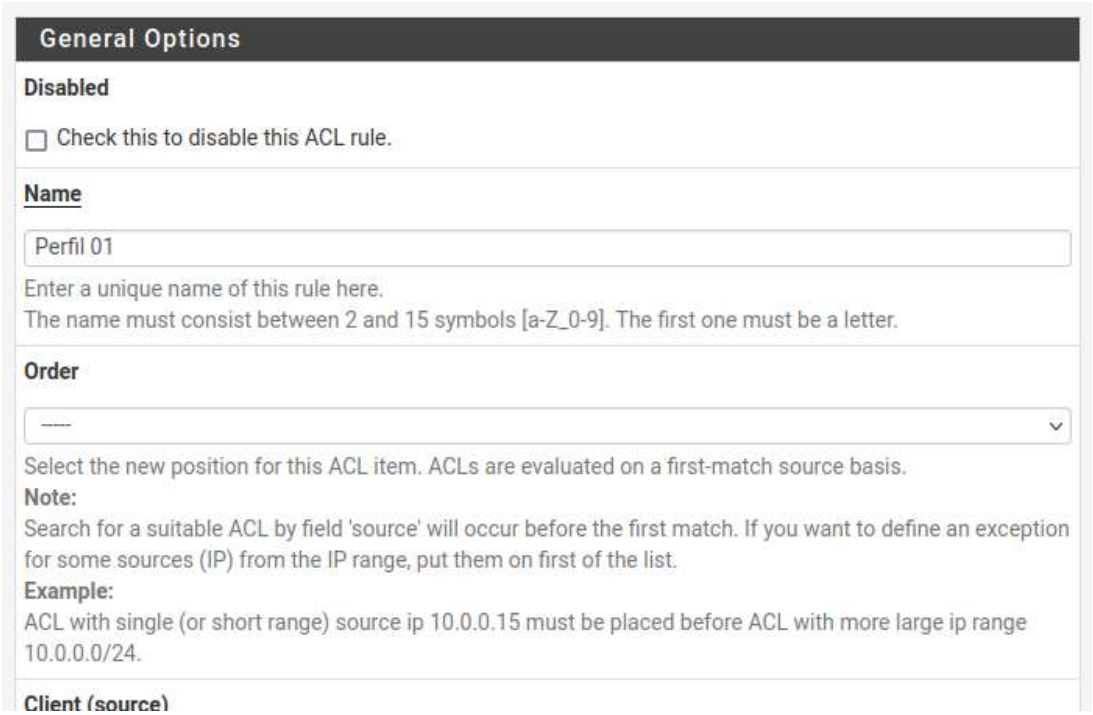


Fig. 39 Creación de grupo Perfil 01.

Fig. 40 Bloqueo de IP de LAN a Firewall.

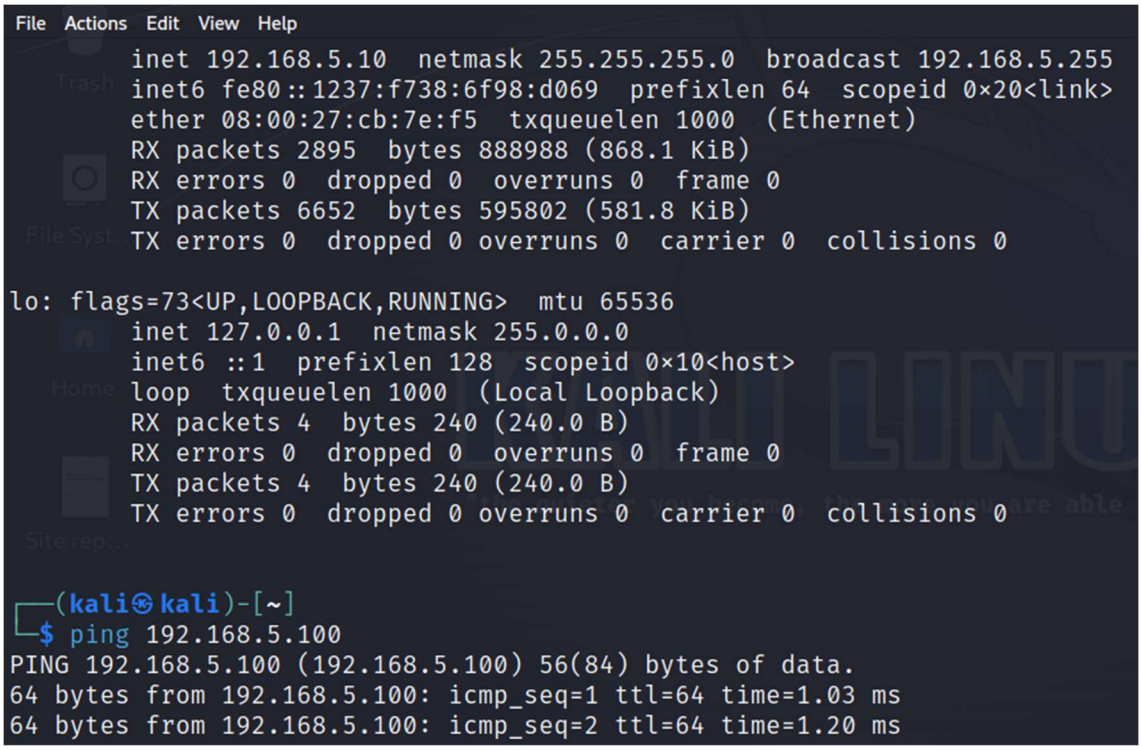


Fig. 41 Acceso de Admin de IP de LAN a Firewall.

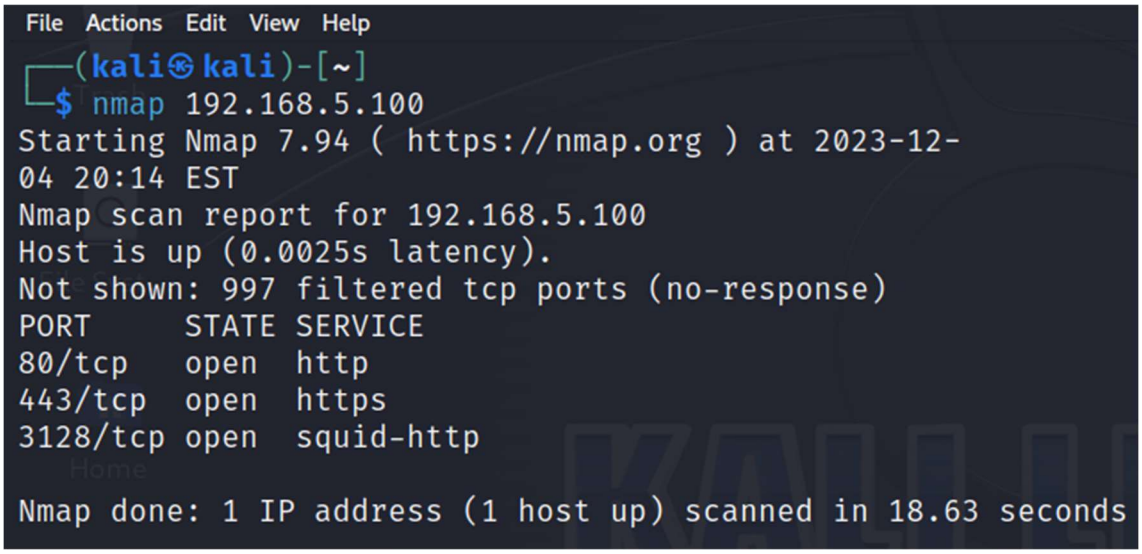


Fig. 42 Nmap a LAN.

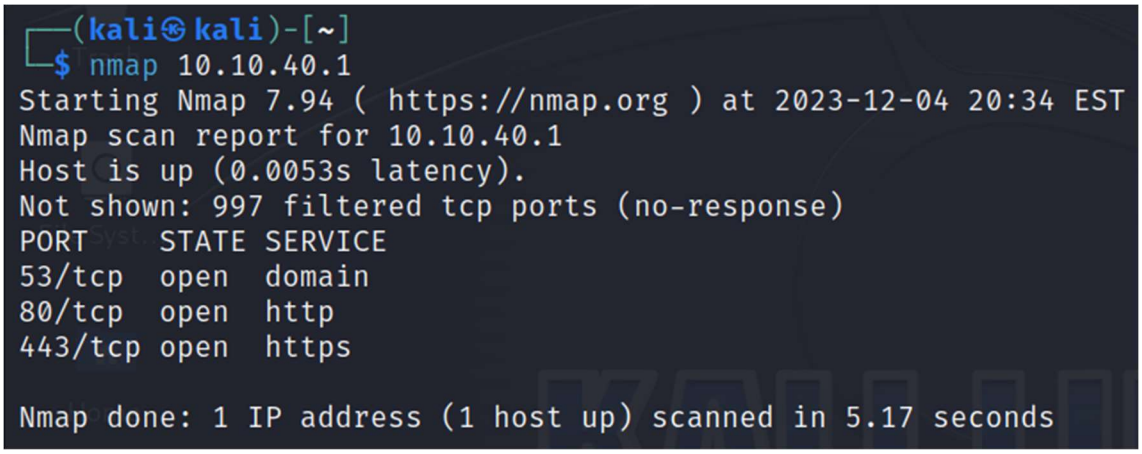


Fig. 43 Nmap a DMZ.

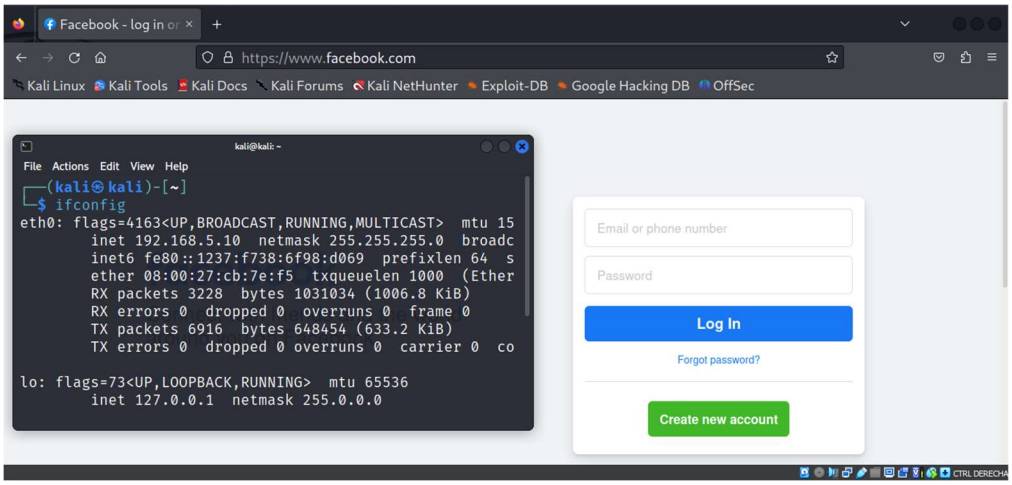


Fig. 44 Acceso de usuarios con privilegios a internet.

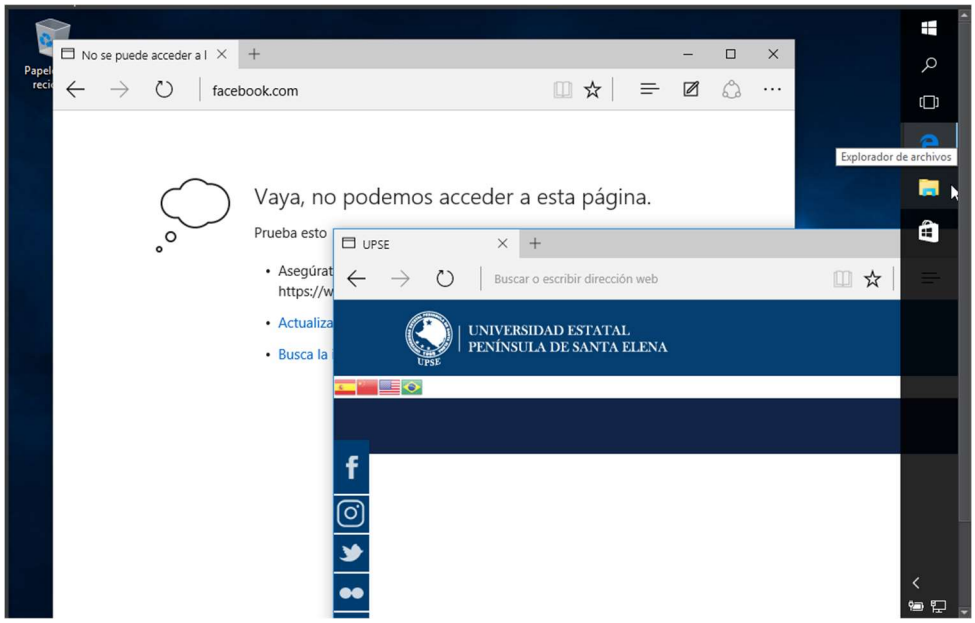


Fig. 45 Acceso limitado de páginas de internet a usuarios