UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS

IMPLEMENTACIÓN DE FIREWALL PARA EL CONTROL DE SERVICIO DE INTERNET EN LA FILIAL CHANCHAMAYO DE LA UNIVERSIDAD PERUANA LOS ANDES

Autor:

JOAQUIN CAJAHUARINGA JHON CARLOS

Línea de Investigación Institucional:

NUEVAS TECNOLOGÍAS Y PROCESOS

Para optar el título profesional de:

Ingeniero de Sistemas y Computación

HUANCAYO – PERÚ

2020

_____

DR. HENRY GEORGE MAQUERA QUISPE

ASESOR METODOLÓGICO

_____

DR. JOHN FREDY ROJAS BUJAICO

ASESOR TEMÁTICO

DEDICATORIA

Esta investigación está dedicada para mi familia, en especial para mi madre Angelica Victoria Cajahuaringa Tomas y padre Miguel Enrique Joaquin Aleluya que con sus constantes enseñanzas y su ayuda incondicional hoy puedo ser un profesional de bien. A mis hermanos Edgar, Luis y Pamela a quienes les debo mis mejores momentos de la infancia quienes hasta ahora me siguen apoyando en todo, a mis amigos con quienes pasé muy buenos momentos mientras duro la vida universitaria y a los que conocí en el trabajo con quienes ahora comparto sabiduría, agradezco a mis docentes universitarios que me enseñaron lo necesario para afrontar un trabajo en forma correcta.

Bach. Jhon Carlos Joaquin Cajahuaringa

HOJA DE CONFORMIDAD DE LOS JURADOS

DR. CASIO AURELIO TORRES LÓPEZ
PRESIDENTE

……
JURADO

……
JURADO

……
JURADO

MG. MIGUEL ANGEL CARLOS CANALES
SECRETARIO DOCENTE

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La problemática fue el uso desmedido del servicio de internet dentro de la filial Chanchamayo que ocasionó lentitud en la transmisión de información, perdida de paquetes de información y quejas de los trabajadores administrativos. El objetivo de la tesis fue implementar un Firewall para controlar el uso del internet, gestionando los accesos de acuerdo al uso o labor de cada personal administrativo. De igual manera, en los laboratorios de cómputo se controló el servicio de Internet de acuerdo las demandas tecnológicas que cada curso desarrollado por el docente. Asimismo, el servicio de Internet es controlado en horarios en los que los laboratorios no se encuentren en horario de clases con el fin de no saturar los servicio relacionados con la red de computadoras interna. Se realizó una verificación funcional de los dispositivos de red que se encuentran bajo la administración de la Universidad con el fin de implementar una solución tecnológica a través de la metodología Top Down. Al finalizar la tesis los sistemas de información llegaron a un nivel de funcionamiento aceptable.

Palabras Clave: Firewall, CentOS, Shorewall, Squid, Top Down, UPLA

ABSTRACT

The problem was the excessive use of the internet service within the Chanchamayo subsidiary, which caused slowness in the transmission of information, loss of information packages and complaints from administrative workers. The objective of the thesis was to implement a Firewall to control the use of the internet, managing the access according to the use or work of each administrative staff. Similarly, in the computer labs, the Internet service was controlled according to the technological demands that each course developed by the teacher. Likewise, the Internet service is controlled at times when the laboratories are not during class hours in order not to saturate the services related to the internal computer network. A functional verification of the network devices that are under the administration of the University was carried out in order to implement a technological solution through the Top Down methodology. At the end of the thesis, the information systems reached an acceptable level of operation.

Keywords: Firewall, CentOS, Shorewall, Squid, Top Down, UPLA

INTRODUCCIÓN

Actualmente las empresas están en constante competencia intentando ofrecer el mejor servicio y la mejor calidad en sus operaciones, una de las herramientas que más se utiliza para alcanzar la calidad en el servicio son las tecnologías de la información y como estamos en una era donde no somos ajenos a los avances tecnológicos y las empresas empiezan a invertir en el sector tecnológico, las soluciones tecnológicas son la mejor opción para mejorar en muchas áreas.

Las empresas dedicadas al sector educación además de dar una buena formación a los estudiantes, también buscan que sus sistemas y su servicio de internet funcione correctamente ya que del servicio de internet depende sus páginas publicadas, sistemas web, sistemas de información, sistemas de matrícula y entre otros sistemas; con esa premisa un Firewall puede ofrecer un control del servicio de internet de forma correcta, delimitando el ancho de banda según sea necesario, bloqueando páginas web que no sean de uso necesario por cada usuario, proteger tu red interna de intrusiones por parte de hackers con el bloqueo de puertos y la verificación entre IP y MAC.

Se ha utilizado la metodología Top-Down porque se ajusta a las necesidades de la solución, porque al dividir el problema principal en pequeños problemas podre tener una visión más precisa y solucionar cada pequeño problemas de la manera más óptima, dicho esto la metodología me permitirá crear reglas en el firewall para cada problema y al finalizar el proyecto tendré todas las reglas necesarias para obtener el objetivo final de la tesis que es Mejorar el Servicio de Internet en la Filial Chanchamayo de la Universidad Peruana los Andes.

La presente investigación se dividió en cinco capítulos, a continuación, detallo el contenido de cada capítulo:

Capítulo I: “Problema de la Investigación”, describe a la organización, se detalla el problema de la organización, los objetivos y la justificación.

Capitulo II: “Marco Teórico”, describe la teoría necesaria para entender la investigación, también se considera los antecedentes que se usaron como guía y finalmente las bases teóricas para sustentar la investigación, también se define la hipotesis general con sus hipotesis específicas.

Capitulo III: “Metodología”, describe la solución de la problemática planteada en la investigación y también se detalla los pasos de la metodología Top Down Network Design.

Capitulo IV: “Resultados”, es aquí donde se realiza el desarrollo de la solución con la metodología seleccionada (Top Down Network Design) con la identificación de los requerimientos, su especificación de los mismos y finalizando con la validación.

Capítulo V: “Discusión de resultados”, es aquí donde se discute los resultados con las tesis de referencia.

Finalmente se culmina con las conclusiones, recomendaciones y los anexos.

Bach. Joaquin Cajahuaringa Jhon Carlos

CAPITULO I

1.1. PLANTEAMIENTO DEL PROBLEMA

En la filial Chanchamayo de la Universidad Peruana los Andes existen usuarios administrativos y laboratorios de cómputo que utilizan los estudiantes de la filial, es muy común que en el momento que los estudiantes hacen uso de los equipos de cómputo visiten páginas de redes sociales, videos en la diferentes paginas existentes, así como también la utilización de juegos, por otro lado el personal administrativo suele realizar descargas de todo tipo y la vistas a páginas web que no corresponden a su labor.

Ambos casos se definen como mal uso del servicio de internet contratado por la Universidad. Otro problema que trae es la queja de los docentes que mencionan que el internet es deficiente con la cantidad de equipos instalados y por consecuencia no pueden realizar sus clases de forma correcta, también el personal administrativo que labora en la filial suele quejarse que los sistemas de información no responden de forma correcta y que por ese motivo en épocas de matrícula se extienden colas de estudiantes por horas.

Todo lo descrito anteriormente trae como consecuencia la perdida de paquetes, lentitud en la red con latencias de respuestas muy altas que hacen que los sistemas de información trabajen de forma ineficiente, y que en los laboratorios de cómputo el internet sea tan lento que hasta el docente no pueda realizar su clase como lo tiene planeado.

Toda la problemática descrita es por el mal uso que le dan los mismos usuarios al servicio de internet contratado por la universidad, para obtener pruebas de la problemática descrita se realizó un análisis a la red y se habilito una bitácora de quejas por tres meses en horas punta, se promedió los valores obtenidos en cada mes de prueba obteniendo los siguientes resultados (Anexo 1: para visualizar las pruebas de cada día):

Mes uno:

Tabla 1. Promedio Mes Uno

Mes Uno	Latencia	470.2
	Quejas	5.9
	Paquetes Perdidos	34.9

Autoría Propia

Mes dos

Tabla 2. Promedio Mes Dos

Mes Dos	Latencia	467.5
	Quejas	5.7
	Paquetes Perdidos	34

Autoría Propia

Mes tres

Tabla 3. Promedio Mes Tres

Mes Tres	Latencia	463
	Quejas	5.6
	Paquetes Perdidos	33.3

Autoría Propia

Para realizar las pruebas de tiempo de respuesta se utilizó el comando “ping” hacia el DNS de Google y el resultado obtenido es el siguiente:

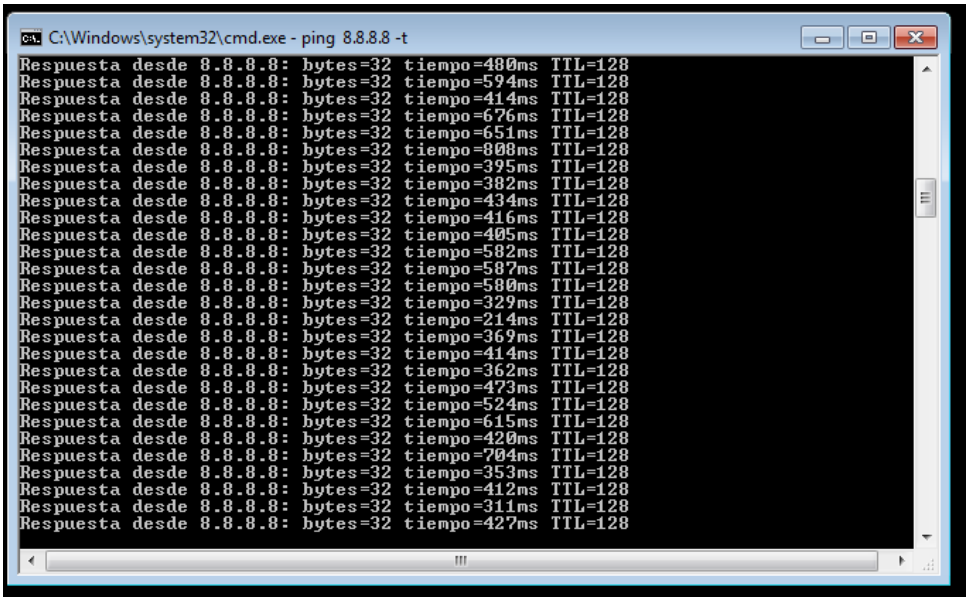

Figura 1. Pruebas de tiempo de respuesta, Autoría Propia

Para contar la cantidad de paquetes perdidos se utilizó un Sniffer llamado “Wireshark”, esta herramienta realiza el conteo de todos los paquetes que comunican la red hacia internet y también los paquetes que intercambian cada equipo conectado, el resultado obtenido fue:

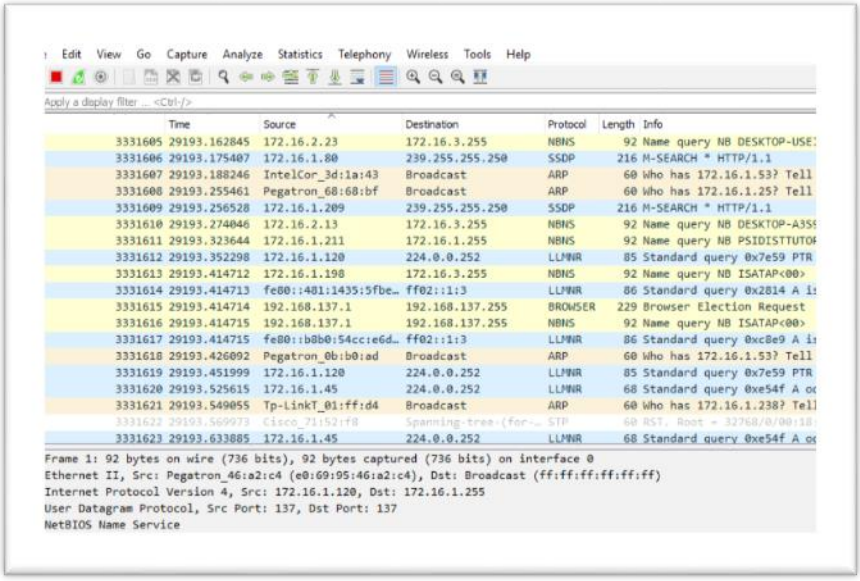

Figura 2. Conteo de paquetes con Wireshark, Autoría Propia

1.2. FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA

1.2.1. Problema General

¿De qué manera el firewall permite mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes?

1.2.2. Problemas Específicos

a. ¿De qué manera el firewall permite optimizar la identificación de protocolos más usados en la red interna de la Filial Chanchamayo de la Universidad Peruana los Andes?
b. ¿De qué manera el firewall permite mejorar el control de accesos a la red interna de la Filial Chanchamayo de la Universidad Peruana los Andes?
c. ¿De qué manera el firewall permite agilizar el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes?

1.3. JUSTIFICACIÓN

1.3.1. Practica o Social

Al finalizar la implementación del Firewall el servicio de internet será administrados de forma correcta y se beneficiaran los trabajadores administrativos, docentes y estudiantes de la Filial Chanchamayo

1.3.2. Científica o Teórica

La presente investigación detallara la instalación del SHOREWALL y SQUID, las funciones que realizan estos programas son muy eficientes para el control de los servicios de internet.

1.3.3. Metodológica

Con ayuda de la metodología Top Down Network Design se detallará un problema principal del cual se subdividirán para poder analizar cada sub problema y crear reglas direccionadas al uso con cada usuario final. Al dividir el problema es posible asignar los subproblemas a diferentes personas con lo que se puede llegar a solucionar el problema de forma más rápida y eficiente.

1.4. DELIMITACIONES

1.4.1. Delimitación Espacial

La tesis se delimito únicamente en la Filial Chanchamayo de la Universidad Peruana los Andes

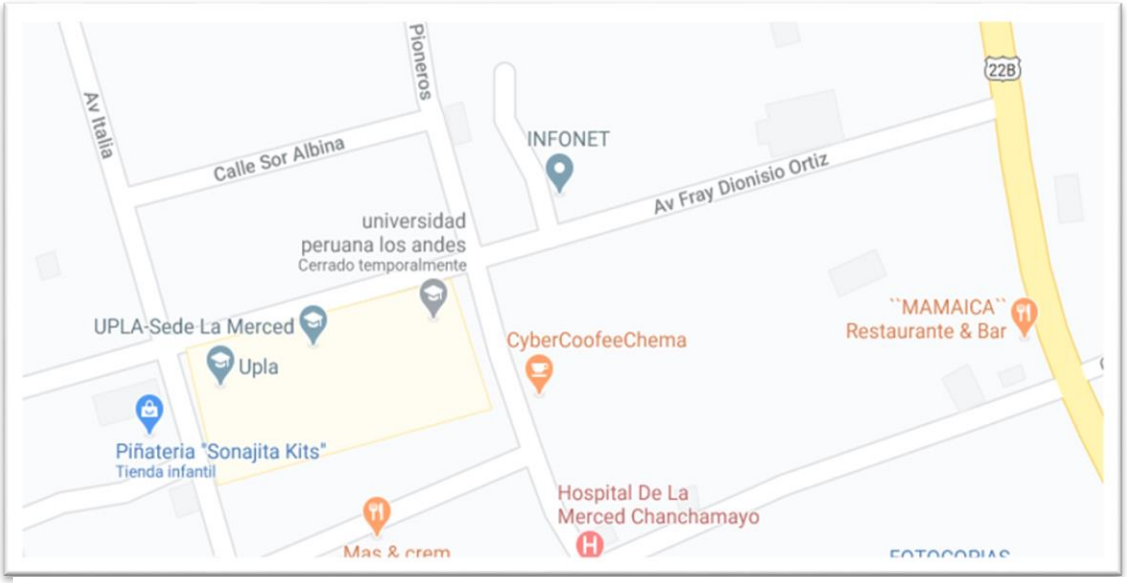

Figura 3: Croquis Filial Chanchamayo UPLA, Autoría: Google

1.4.2. Delimitación Temporal

El tiempo que se necesitó para culminar la tesis fue de doce semanas, en las cuales se realizó el análisis, implementación y pruebas de funcionalidad del Firewall.

1.4.3. Delimitación Económica

Esta tesis fue financiada por la universidad Peruana los Andes con el Hardware necesario, los materiales y servicios fueron financiados por mi persona. Detallo los recursos necesarios para implementar el firewall.

Tabla 4. Tabla de Recursos

Tipo	Categoría	Recurso	Descripción	Monto
Recursos Disponibles	Hardware	Equipo	Servidor	S/ .000.00
	Software	Software	Shorewall	S/ .000.00
		Software	Squid	S/. 000.00
Recursos Necesario	Materiales	Papel	Hojas de Impresión	S/. 250.00
	Servicios	Pasajes	Viaje a la Filial las veces necesarias	S/. 500.00
		Energía	Para el funcionamiento de los equipos	S/. 200.00
		Alimentación	Alimentos en los Viajes	S/. 600.00
			Total:	S/. 1550.00

Autoría propia

1.5. LIMITACIONES

la principal limitación que se tuvo en la tesis fue la baja colaboración de los usuarios finales al recabar la información, posiblemente por el miedo a ser controlados y monitoreados en cada acción que realicen al navegar por internet.

Al ser un Firewall implementado con Software Libre y que ya se contaba con un servidor que proporciono la Universidad no se tuvo problemas económicos.

1.6. OBJETIVOS

1.6.1. Objetivo General

Implementar un Firewall mediante la metodología Top Down Network Design para mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes.

1.6.2. Objetivos Específicos

a. Identificar los protocolos más usados mediante la metodología top Down Network Design para mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes.
b. Implementar reglas para habilitar protocolos mediante la metodología Top Down Network Design para mejorar el control de accesos a la red interna en la Filial Chanchamayo de la Universidad Peruana los Andes.
c. Realizar pruebas de funcionalidad mediante la metodología Top Down Network Design para agilizar el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes.

CAPITULO II

2.1. ANTECEDENTES

2.1.1. Antecedentes Nacionales

Para sustentar la investigación, se revisó algunos trabajos realizados que tienen relación con la investigación:

Tesis (1): Sus conclusiones son:

a. Se verifico que existía vulnerabilidad de acceso en el puerto 22, configurado por defecto en el protocolo SSH, por lo tanto, se plantea usar el puerto 25622 que es un puerto de UNIX no registrado formalmente. De esta manera para un hacker no será fácil rastrear el puerto de conexión.
b. Se desarrolló un diseño de acuerdo a las políticas de seguridad de la empresa Conexión Linux SAC, donde solo Gerencia y Administrador de red tienen acceso al servidor master. Mientras que en los medios de accesibilidad se usó el protocolo SSH con un puerto específico para minimizar la vulnerabilidad, como también el bloqueo del protocolo ICMP hacia la WAN.
c. Se logró integrar al algoritmo del firewall el bloqueo del broadcast innecesario, bloqueo de protocolo IPV6, como también reglas predeterminadas por el firewall, para garantizar el tráfico limpio. Mientras para asegurar la integridad de los paquetes de datos se

realizó dos reglas: duras y blandas, esto con la finalidad de garantizar el funcionamiento de la red.

Tesis (2): Los autores concluyen en:

a. Mediante la implementación del Firewall TMG Forefront se espera minimizar los riesgos de ataques de malware y spam para toda la red de datos de la clínica Aliada.
b. Mediante la implementación del Firewall TMG Forefront se espera mejorar la gestión de políticas de seguridad bajo la ISO 27001 (Seguridad de la Información) la cual nos facilitaría un estándar en la aplicación de políticas a los usuarios de la red de datos de la Clínica Aliada.
c. Mediante la implementación del Firewall TMG Forefront se obtendrá un servicio de internet optimizado y veloz, estas mejoras se verán reflejadas al entrar el firewall a producción.
d. La evaluación financiera del proyecto estima que nuestro cliente la Clínica Aliada se verá beneficiado en su gestión de seguridad produciendo un trabajo más eficaz de sus colaboradores y mejorando su Calidad de Servicio en todas las áreas de la empresa.

Tesis (3): Concluyen en:

a. Se identificó el sistema FreeBSD versión 6.3 que brindaba la seguridad perimetral lógica en los servicios de la red troncal de la Universidad Nacional de la Amazonía Peruana.
b. Se pudo determinar la existencia de vulnerabilidades en cada uno de los doce servicios durante el funcionamiento de la red perimetral existente. Se produjo vulnerabilidades con un promedio de 104.6 vulnerabilidades por servicio, siendo el mayor número registrado de eventos no autorizados 426 y el mínimo de 14.

c. Se implementó y configuró el sistema PfSense para la gestión de la seguridad perimetral lógica, tal como consta en el Acta de Instalación.
d. Se pudo determinar la existencia de vulnerabilidades en cada uno de los doce servicios durante el funcionamiento de la red perimetral existente y su gestión con PfSense. Se produjo vulnerabilidades con un promedio de 3.3 vulnerabilidades por servicio, siendo el mayor número registrado de eventos no autorizados 7 y el mínimo de 1.

2.1.2. Antecedentes Internacionales

Tesis (4): El Investigador concluye con:

a. Teniendo en cuenta las encuestas realizadas tanto a nivel de usuarios como a nivel técnico podemos denotar que la red si presenta inconvenientes como el ofrecer servicios sobre todo en horas pico, a su vez hay una gran aceptación de la propuesta puesto que con este nuevo diseño tendremos varios beneficios como lo es la Escalabilidad, Redundancia y el Mantenimiento de la misma. Esto me permitiría de una manera muy práctica realizar la planificación para una posible expansión. Si en algún momento uno de los switches Core que es base del modelo jerárquico llegase a fallar siempre estará el otro como un respaldo para mantener a la red en funcionamiento, es decir proporcionando el servicio a los usuarios. Por otro lado, mantenerla no sería costoso puesto que es modular y escalable. En este nuevo diseño los protocolos a utilizarse serán el Spanning Tree, Vlan y Caps. El uso de Cable de Categoría 6 permitiría una ampliación del ancho de banda que actualmente tiene el Cable que usamos, es decir el de Categoría 5E, además de una mejora en el rendimiento de la

transmisión. Por lo tanto, se decidió cambiar a cable de categoría 6, porque esto significaría menos retransmisiones de pérdida o corrupción de paquetes de datos en determinadas condiciones, que se traduce en una mayor fiabilidad de las redes de categoría 6 en comparación a la categoría 5e.

Tesis (5): Sus conclusiones son:

a. La puesta en marcha del modelo de gestión de supervisión y monitoreo de la infraestructura de la red de datos en la UCLA, brinda un conjunto de beneficios que se traducen en aspectos claves para el óptimo desempeño de la red, pues el uso de la herramienta Zabbix, permitió la integración del modelo de gestión de red SNMP usado en la Universidad con el planteado en este trabajo.
b. Adicionalmente, esta herramienta de monitoreo ofrece una vista general de la infraestructura a los especialistas adscritos al Departamento de Redes de Datos RedUCLA, proporcionando así la posibilidad de predecir eventos, identificar fallas y 116 generar soluciones en menores tiempos; aunado a lo anterior, Zabbix incluye la opción de automatizar tareas como la concerniente al inventario de equipos; manejo de estadísticas, generación de reportes y gráficas, entre otras.

Tesis (6): El investigador Concluye:

a. El sistema planteado reúne los requisitos de ser un sistema de uso simple desde el punto de vista del usuario, pero reúne la complejidad suficiente dentro de sus procesos internos, para ser una solución lo suficientemente segura. Todos los procesos adicionales que se realizarán dentro del sistema de seguridad, son totalmente transparentes para el usuario, es decir el usuario no se

percatará que dentro del sistema se realizan verificaciones adicionales de seguridad.

b. Iptables es una herramienta flexible, aun cuando su entendimiento conlleva algo de complejidad; una vez comprendida su filosofía de funcionamiento, la herramienta se vuelve muy versátil y permite realizar implementaciones modulares.
c. Se dispondrá de mayor seguridad al emplear herramientas de software abierto y de libre acceso, ya que al haber más personas que lo utilizan y lo revisan, ayudarán a encontrar posibles errores o fallas de seguridad que podrían afectar el funcionamiento del sistema.

2.2. MARCO CONCEPTUAL

2.2.1. MAC ADDRESS

Según Joan Carles la Mac Address o dirección Mac es un identificador único de 48 bits para identificar a los dispositivos de red, por ejemplo, las tarjetas de red Ethernet, tarjetas de red wifi o inalámbricas, Switch de red, routers, impresoras, etc.

2.2.2. DIRECCION IP

Según Alonso Nuria Olivia la dirección ip es un número que identifica de manera lógica y jerárquica a un interfaz de red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, laptop, teléfonos inteligentes) que utilicen el protocolo ip (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

2.2.3. FIREWALL

En informática, un Firewall (Cortafuego traducción al español) es la parte de un sistema informático o una red informática que está diseñada

para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Funciona como una barrera entre internet u otras redes públicas y nuestra red interna.

Para ello un firewall cuenta con reglas predefinidas que son:

- Autorizar una conexión (Allow)
- Bloquear una conexión (Deny)
- Re direccionar un pedido de conexión sin avisar al emisor (Drop)

Estas reglas permiten colocar un método de filtración que depende de las políticas de seguridad de cada organización, estas se distinguen por:

- Permitir únicamente las comunicaciones autorizadas.
- Impedir cualquier comunicación que fue prohibida.

El primer método es más seguro, pero requiere de una definición de reglas precisas según las necesidades de comunicación de la organización.

Tipos de Firewall

Esencialmente existen dos tipos de Firewall, se implementan según la infraestructura de datos o el tamaño de la red.

- Firewall por Software (como gratuitas o de pago)
  Se caracterizan por:
  - Contar con un sistema operativo y normalmente son para uso personal
  - Se integran fácilmente con otros productos de seguridad
  - Se puede instalar en un equipo (Hardware) con la finalidad de obtener una mejor administración y mayor seguridad.
- Firewall por Hardware (mediante la utilización de dispositivos)
  Es el que viene instalado en los routers que se utilizan para acceder a internet. La mayoría de routers vienen con un firewall instalados. También existen dispositivos Firewall por separado que son mucho más robustos, ofreciendo mayor seguridad, pero

se debe de entender que su instalación y configuración no es tan sencilla.

2.2.4. INTERNET

Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial.

2.2.5. PROTOCOLOS DE RED

Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores, es una convención que controla o permite la conexión, comunicación y transferencia de datos entre dos puntos finales.

2.2.6. WIRESHARK

Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

2.2.7. MODELO TCP/IP

Es usado para comunicaciones en redes y como en todo protocolo describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red, TCP/IP provee de conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Tiene las siguientes capas de red:

d. Capa 1 o capa de acceso medio: acceso al medio, asimilable a la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.
e. Capa 2 o capa de internet: internet, asimilable a la capa 3 (red) del modelo OSI.
f. Capa 3 o capa de transporte: transporte, asimilable a la capa 4 (transporte) del modelo OSI.
g. Capa 4 o capa de aplicación: aplicación, asimilable a las capas 5 (sesión), 6(presentación y 7(aplicación) del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI.

2.2.8. RED LAN

Es una red informática cuyo alcance se limita a un espacio físico, como sería una oficina, casa, departamentos o los ambientes de una empresa. Comparte la información entere varios recursos informáticos como puede ser: celulares, pc, laptops, etc. También a periféricos (scanner, impresoras, etc.), comunica los servidores con el resto de la red de la empresa u organización facilitando el acceso a internet sin importar la habitación donde se encuentre o el piso en una institución.

este recurso es común en los hogares, negocios y empresas con la variación en la topología de red que se implementa de acuerdo a la necesidad del hogar, negocio u empresa.

2.2.9. TOPOLOGÍA DE RED

Se dividen en:

- Red en Bus: es cuando un solo cable comunica a todos los equipos permitiendo la transmisión de datos en línea recta, es una solución sencilla pero muy susceptible a daños y por consecuencia la interrupción del servicio.

- Red Estrella: Cuando todos los equipos se conectan a un servidor central y este administra los recursos y asigna la dirección ip según se solicite.
- Red en Anillo: es una conexión unidireccional entre los equipos informáticos, en este caso la transmisión se interrumpe solo en el nivel que exista el fallo.
- Red Mixta: esta topología combina los modelos anteriores

2.2.10. TARJETA DE INTERFAZ DE RED

También llamada placa de red, es una tarjeta destinada a ser colocada en la placa madre de un computador para que la maquina se sume a la red y empieza a compartir sus recursos como son la impresora, documentos, conexión a internet, etc.

Fundamentalmente su función es la transmisión y recepción de datos o información. Realiza una tarea llamada buffering, termino con que se define a una tarea de almacenar información para que los datos posteriormente se puedan transmitir por medio de los respectivos cables.

2.2.11. TIPOS DE REDES

Generalmente se clasifican por su alcance geográfico por el cual refleja su volumen de datos, a continuación, se detalla algunas:

- Redes LAN (Redes de Área Local). Se ubican en sitios concretos y específicos con poco alcance como en una casa, oficinas, y hasta un edificio.
- Redes MAN (Redes de Área Metropolitana). Su alcance es mayor al de local, pero no es internacional, un ejemplo muy simple sería el campus universitario que tienen sedes en distintos lugares.

- Redes WAN (Redes de Área Amplia). Redes que traspasan regiones geográficas, pueden ser nacionales y hasta internacionales. Es también conicidad como la Internet.

2.2.12. ROUTER

También es conocido como enrutador, permite la interconexión entre subredes direccionando los paquetes de datos a la dirección indicada. Es decir, consigue el mejor camino para que los paquetes sean transportados de forma adecuada analizando la información de origen y destino. Se lleva a cabo por dos procesos:

- Reenvió de paquetes: recibe paquetes y lo envía al punto de salida adecuado según determine la tabla de encaminamiento que es un documento electrónico donde se detalla las rutas de los nodos de red.
- Encaminamiento de paquetes: determina la ruta del paquete desde el emisor hasta el receptor.

2.2.13. PROTOCOLOS DE RED

Es una capa de mediación que establece una serie de acuerdos para poder intercambiar datos regulando las condiciones del transporte, el direccionamiento, enrutamiento y controlar las posibles fallas. Significa que para que dos equipos se comuniquen entre si deben de utilizar los mismos protocolos de red, en tal manera que concuerdan las mismas condiciones para la transmisión.

2.2.14. CABLE DE RED

Es un cordón que contiene 8 conductores los cuales están aislados, este cordón está dentro de una envoltura que garantiza resistencia y flexibilidad. Se denomina cable de red al elemento físico que permite la

conectividad entre dos equipos, puede ser de forma directa o por medio de un Router o Switch.

2.2.15. SWITCH DE RED

Es un dispositivo que permite conectar varios equipos dentro de una red como son computadoras, impresoras, cámaras, scanner, etc. Su funcionamiento es simple, un equipo manda un mensaje y el Switch retransmite por la salida en la que está su objetivo para esta tarea el Switch utiliza la dirección física de la tarjeta de red (MAC). Tradicionalmente un pulso de luz indica bit 1 y cuando no está la luz indica bit 0.

2.2.16. FIBRA ÓPTICA

En simples palabras la fibra óptica es la manipulación controlada de la luz con terminaciones especiales y en placas que hacen posible la transmisión de información. Está compuesto por Núcleo, manto, recubrimiento, tensores y chaqueta. Esta tecnología no sufre de interferencias que se ocasionan por los cambios de tensión, temperatura, ni perdidas en función a la distancia. Ofrece un nivel de seguridad más alto entre todos los medios de conexión y alcanza una velocidad superior a los 40Tbps.

2.2.17. METODOLOGÍA TOP DOWN NETWORK DESIGN

La metodología seleccionada para esta tesis es Top Down, es una metodología que se centraliza en reuniones, aplicaciones y observación de datos previamente para su elección de enrutadores, conmutadores y todo tipo de medios operacionales en sus capas menores. Además,

ayudara a diseñar redes que cumplan con los objetivos del negocio y técnicas del cliente. Se divide en cuatro fases:

- Fase uno

  Identificando objetivos y necesidades del cliente

  Se inició el análisis de objetivos y restricciones empresariales con sus requisitos técnicos, lo cual tiene como tarea entender las metas del negocio del cliente en su red actual y el nuevo diseño. Aquí se tiene que analizar el negocio para su diseño de redes, identificación de software y hardware de la red del cliente, políticas y normas que se implantaran el desarrollo de la red, finalmente el presupuesto para el trabajo.

  Identificación de las necesidades

  Proporciona técnicas para analizar los objetivos técnicos de un usuario para un desconocido diseño, analiza los objetivos técnicos del cliente que se adapten a las necesidades de los mismos. En sus fines técnicos esta la escalabilidad, rendimiento de la red, disponibilidad, seguridad, adaptabilidad, manejabilidad y usabilidad.

  Análisis de Objetivos Técnicos y Compensaciones

  Se determina el alcance de la red considerando el crecimiento de la universidad. La disponibilidad es la continuidad del servicio es decir que la universidad cuente con internet en todas que se use el laboratorio de cómputo y las horas de trabajo de los trabajadores administrativos.

  Caracterización de la red existente

  Parte importante para examinar la red actual que tiene la Filial Chanchamayo con la finalidad de realizar un rediseño de la red

para mejorar la conectividad y administración los equipos agregándoles seguridad en la navegación.

- Fase dos

  Diseño de red lógico

  En esta fase se diseña la topología de red, el modelo de direccionamiento y nombramiento, se seleccionará los protocolos para los dispositivos de interconexión. Este mismo incluye la seguridad y administración de la red.

- Fase tres

  Diseño físico de la red

  Se diseña la estructura física de la red, es fundamental para estructurar todas las conexiones físicas de la red a implementar en el proyecto.

  Seleccionamos el tipo de Switch, Router, Servidores, Equipos, etc. Necesarios para la implementación del Firewall.

- Fase cuatro

  Prueba, optimización y documentación

  Como cada sistema es diferente, la selección de métodos y herramientas de prueba requiere de precisión y un completo entendimiento del sistema a ser evaluado.

2.2.18. CALIDAD DEL SERVICIO DE INTERNET

Es el rendimiento promedio de una red computadoras, específicamente vistos por los usuarios finales de una red.

Se puede medir la calidad de servicio por la tasa de errores, ancho de banda, rendimiento, disponibilidad, retrasos en la transmisión, etc. Es la habilidad de suministrar diferentes prioridades a distintas aplicaciones,

usuarios o datos. Ejemplo, el ancho de banda asignado se puede garantizar en un porcentaje. La garantía es importante si la capacidad de la red es insuficiente, especialmente para la transmisión multimedia en tiempo real como es voz sobre IP, juegos en línea y IP-TV ya que siempre requieren de un ancho de banda específico para que no sufra retrasos en la transmisión.

La calidad de servicios a menudo es usada para medir la calidad porque refiere a un mejor rendimiento, bajas latencias y poca probabilidad de errores.

2.3. DEFINICIÓN DE TÉRMINOS

2.3.1. LATENCIA

Es el tiempo que demora en transmitir un paquete dentro de la red, la latencia influye en el tiempo de carga de una página web.

2.3.2. HORAS PUNTA

Son las horas entre las 10 y 11 de la mañana de lunes a viernes, se le llama así por la cantidad de usuarios que se tiene en el momento y es propicia para realizar las pruebas.

2.3.3. BITÁCORA

Cuaderno de registro donde el personal administrativo describe las quejas y se habilita durante las horas punta mientras se realiza las pruebas a la red interna.

2.3.4. ANCHO DE BANDA

Es la capacidad de transmisión que tiene una conexión y es importante porque determina calidad y velocidad de una red. Se mide por la

cantidad de datos o información que puede transportar entre dos puntos de red en un determinado tiempo.

2.3.5. LABORATORIO DE COMPUTO

Es un ambiente con el objetivo de que los docentes y estudiantes compartan información o experiencia de aprendizaje con el fin de gestionar proyectos educativos con ayuda de las tecnologías digitales.

2.3.6. CONTROL DE ACCESOS

Se refiere a los permisos que cada usuario final tendrá acceso hacia el internet, por ejemplo, no todos los usuarios tendrán acceso a redes sociales y páginas de reproducción de videos solo aquellos a los que laboren con dichas páginas.

2.4. HIPOTESIS

2.4.1. HIPOTESIS GENERAL

La implementación de un FIREWALL mediante la metodología Top Down Network Design permite mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes.

2.4.2. HIPOTESIS ESPECIFICAS

a. La utilización de la herramienta Wireshark mediante el análisis de tráfico permite identificar los protocolos más utilizados por los usuarios finales en la Filial Chanchamayo de la Universidad Peruana los Andes.
b. La implementación de reglas mediante la metodología Top Down Network Design permite mejorar el control de accesos según la

necesidad del usuario final en la Filial Chanchamayo de la Universidad Peruana los Andes.

c. La realización de pruebas de funcionalidad permite el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes.

2.5. VARIABLES

2.5.1. Definición conceptual de la variable

a. Variable Independiente

Implementación del Firewall

La idea básica es que el firewall bloquee todo el tráfico entrante a menos que exista una regla implícita o el retorno de un tráfico solicitado desde la red interna. (Fernando Illescas, Cisco)

b. Variable Dependiente

Calidad del servicio de internet

Con las nuevas estrategias surgidas en internet, se configuran nuevas necesidades que no deben olvidar la focalización principal hacia el cliente y la Calidad en el servicio. Con el objetivo de permitir una mejor gestión y control del riesgo, proporcionando mayor seguridad y confianza a los usuarios de la red. (Mar Álvarez Reygoza, Articulo)

2.5.2. Definición operacional de las Variables

Tabla 5. Definición Operacional de las Variables

Variable	Definición	Dimensión	Indicadores
Variable Independiente Implementación de un Firewall	Construcción de políticas técnica de seguridad a través de un	Tecnología	Número de Aplicaciones no Académicas

	dispositivo de red	Políticas	Número de reglas habilitadas Número de pruebas satisfactorias
Variable Dependiente Calidad de servicio de internet en la filial	Rendimiento promedio visto por los usuarios de red	Servicio	Latencia Número de quejas Número de paquetes perdidos

Autoría Propia

2.5.3. Operacionalización de las Variables

Tabla 6. Operacionalización de las Variables

Conceptualización	Dimensiones	Ítems	Fuentes	Instrumentos
Número de Aplicaciones no Académicas	Tecnología	El uso de las aplicaciones no académicas	Propias	Wireshark
Número de Reglas Habilitadas	Políticas	La implementación de reglas para mejorar la calidad del servicio de internet	Propias	Shorewall Squid
Número de Pruebas Satisfactorias	Políticas	Realizar pruebas para comprobar el correcto funcionamiento del Firewall	Propias	Pruebas de concurrencia Prueba de estrés
Latencia	Servicio	Mejorar el tiempo de respuesta	Propias	Consola de Windows

				Wireshark
Número de quejas	Servicio	Disminuir el número de quejas	Usuarios Finales	Bitácora
Número de paquetes perdidos	Servicio	Estabilizar el tráfico de los paquetes	Propias	Consola de Windows Wireshark

Autoría Propia

CAPÍTULO III
METODOLOGÍA

3.1. MÉTODO DE INVESTIGACIÓN

En la presente investigación se usó el método científico, se define como los procedimientos que sigue cada ciencia para hallar, sistematizar y explicar las verdades que le son propias, es un procedimiento para el acotamiento de un sector objetivo, es decir que delimita como interesantes y dignas de investigarse solo algunas cualidades muy definidas del ser y del comportamiento de los entes.

3.2. TIPO DE INVESTIGACIÓN

Se aplicó la Investigación Aplicada o tecnología que se define como las que se desarrollan con la finalidad de resolver problemas de la practica social o productiva; buscar, descubrir o validar los métodos, técnicas o materiales que optimicen los procesos, sus hipotesis se demuestran en términos de eficaz o ineficaz.

3.3. NIVEL DE INVESTIGACIÓN

El nivel de investigación fue Explicativa porque no solo se explicó o describió el problema de mi investigación, sino se determinó las causas del problema. La investigación explicativa se basa en establecer el porqué de un problema o fenómeno, también busca establecer las distintas causas de un problema,

comportamiento o procesos. Finalmente se logra la comprensión o entendimiento del problema planteado.

3.4. DISEÑO DE INVESTIGACIÓN

Se utilizó el diseño pre-experimental, estos diseños van dirigida a la evaluación, control y supervisión de una sola variable, motivo por el cual el estudio resulta sumamente sucinto y concreto, por no decir que el mismo se reduce a un solo grupo.

3.5. POBLACIÓN Y MUESTRA

Mi población estuvo compuesta por todos los protocolos de red tales como son: ssh, ftp, http, sftp, telnet, smtp, ntp, pop3, tcp, udp. Elegí estos protocolos porque son los más usados por los usuarios finales. Esta información fue obtenida después de realizar un escaneo a la red interna de la universidad con la herramienta Sniffer Wireshark, en una hora punta se llegó a la población total de 1500000 paquetes transmitidos.

Mi muestra será dirigida, se tomó esa decisión por la cantidad de paquetes que se obtiene al realizar el escaneo a la red interna. Serán los protocolos http, https, ftp porque son los protocolos más usados por los usuarios finales en la Filial Chanchamayo de la Universidad Peruana los Andes. Que en la misma hora punta se obtuvo que la muestra llega a los 175000 paquetes transmitidos.

3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Análisis de Correlaciones: Esta técnica sirve para analizar datos estadísticos, sirve para determinar si existe una relación entre dos variables cuantitativas diferentes y cuan fuerte es la relación entre las mismas.

Análisis de Regresión: es otra técnica de análisis de datos estadísticos que sirve para investigar la relación entre diferentes variables, se utiliza cuando una de las variables (variable independiente) afecta al comportamiento de otra (variable dependiente).

3.7. PROCESAMIENTO DE LA INFORMACIÓN

Por el tipo de mi investigación procesare la información de forma Cuantitativa, ya que manejo datos numéricos.

3.8. TÉCNICA Y ANÁLISIS DE DATOS

Se realizará un análisis de correlaciones porque me permite determinar la relación entre variables cuantitativas y también la relación entre ellas, se utiliza en la investigación porque se tiene variables que tienen una evolución similar.

CAPITULO IV
RESULTADOS

4.1. FASE I: IDENTIFICAR LAS NECESIDADES Y OBJETIVOS DEL CLIENTE

Se identifica los objetivos del negocio, los requisitos del cliente, también se verifica la red actual existente verificando el Hardware y el rendimiento de los mismos.

4.1.1. Identificación de las Necesidades

Visión institucional de la Universidad Peruana los Andes

Ser una Universidad líder y competitiva en la formación profesional, investigación y responsabilidad social comprometida con el desarrollo de la sociedad.

Misión institucional de la Universidad Peruana los Andes

La Universidad Peruana los Andes es una organización académica, dedicada a la formación profesional integral, la investigación y fomento de la cultura para el desarrollo sostenible de la sociedad.

Política de Calidad de la Universidad Peruana los Andes

La Universidad Peruana los Andes, garantiza un servicio educativo de calidad, promoviendo la mejora continua en los procesos de enseñanza-aprendizaje, investigación y responsabilidad social universitaria, a través de la autoevaluación, licenciamiento y acreditación de los programas de estudios de la Universidad para formar profesionales competentes y comprometidos con el desarrollo de la sociedad.

Objetivos de la Universidad Peruana los Andes

d. Mejorar la calidad educativa en beneficio de la población estudiantil.
e. Mejorar los servicios de Wifi de los estudiantes y Docentes dentro del Campus Universitario.
f. Disminuir la cantidad de quejas de los administrativos por el servicio de internet.
g. Mejorar el uso del servicio de internet, que sea utilizado de la forma correcta según la necesidad de los administrativos, docentes y estudiantes.

4.1.2. Análisis de Objetivos Técnicos y Compensación

Escalabilidad

Detalla el alcance de la red y también se considera el crecimiento de la red interna, se tiene en cuenta el crecimiento que tiene la universidad y las posibilidades del aumento del personal administrativo como también la creación de nuevos laboratorios de cómputo.

Disponibilidad

Actualmente se tiene un pequeño registro de cortes en el servicio de internet, se mejorará el servicio para que no existan caídas y se cuente con el servicio dentro del horario de labores de los administrativos, también cuando los estudiantes tengan clases en los laboratorios de cómputo y finalmente para el uso de la plana docente de la filial dentro de su horario de clases en laboratorio y con ese objetivo se dividirá la red interna de la siguiente manera.

- **Zona "USR"**

  Estos usuarios serán los más controlados, solo se les dará acceso exclusivo a las páginas webs necesarias para que realicen su trabajo de forma normal. El Firewall verificara que la Dirección MAC y el IP pertenezcan al equipo registrado y si es así brindara el servicio de internet al usuario.

- **Usuarios "VIP"**

  Estos usuarios serán los que no tengan restricciones en la navegación, pero si se guardan los registros de su navegación en un archivo Log dentro del Firewall. El Firewall Verificara que la dirección MAC y el IP pertenezcan al equipo registrados y si es así brindara el servicio de internet.

- **Usuarios "Lab01"**

  En este grupo se encuentran todas las IPs del laboratorio de cómputo uno, en las horas que no se tenga clases de Tics el internet será restringido, pero se liberara para las clases. El

Firewall Verificara que la dirección MAC y el IP pertenezcan al equipo registrados y si es así brindara el servicio de internet.

- **Usuarios “Lab02”**

  En este grupo se encuentran todas las IPs del laboratorio de cómputo dos, en las horas que no se tenga clases de Tics el internet será restringido, pero se liberara para las clases. El Firewall Verificara que la dirección MAC y el IP pertenezcan al equipo registrados y si es así brindara el servicio de internet.

- **Zona “Wifi”**

  Esta zona está separada de los usuarios. Esta zona no tendrá un control por parte del Firewall, porque no se guardará un historial de navegación. Esa zona será controlada por un equipo Mikrotik quien determinará los usuarios y contraseñas para acceder a la red Wifi de la universidad y el ancho de banda asignado.

- **Zona “DMZ”**

  Esta zona está separada para el servidor de monitoreo de la Filial y a la vez sirve para la exportación de marcaciones de los docentes hacia el Sistema Digital de Control de Asistencia Docente (SIDCAD), esta zona tendrá internet libre sin limitaciones.

4.1.3. Características de la red

En la siguiente figura se detalla la forma en la cual viene trabajando la Filial Chanchamayo, se trata únicamente de la red interna de la Filial no la Red empresarial de la Universidad Peruana los Andes.

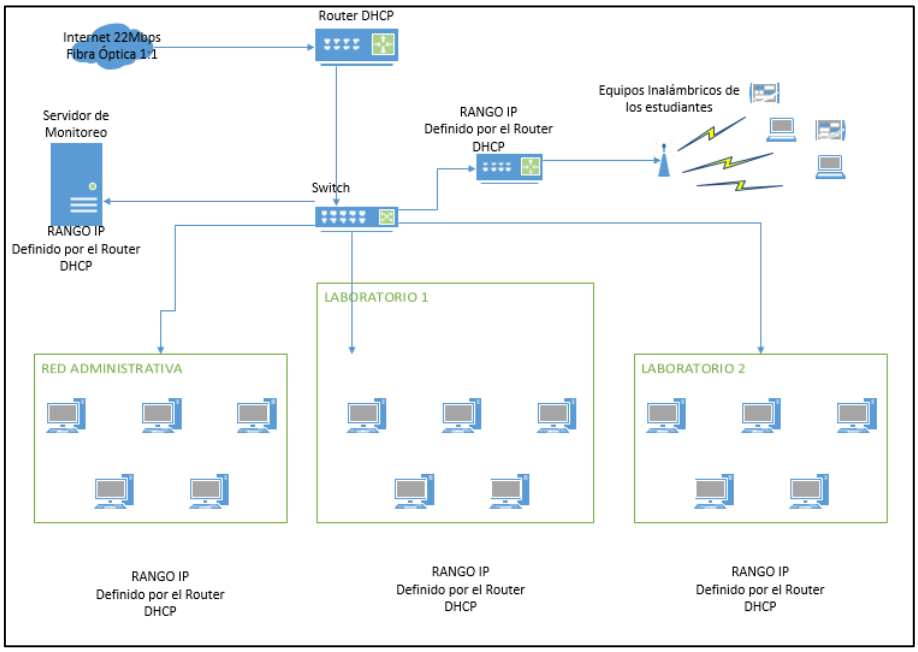

Figura 4. Red Interna de la Filial Chanchamayo, Autoría Propia

Se puede observar que la red no tiene ningún tipo de control, cada usuario puede hacer el uso del internet en forma libre sin limitar el ancho de banda. Esto trae problemas al momento de realizar sus labores el personal administrativo.

4.1.4. Descripción de la Problemática

Se realizó la verificación en la infraestructura de red la Universidad Peruana los Andes – Filial Chanchamayo, se identificó lentitud en el servicio, perdida de paquetes de datos y latencia alta generando demoras en el tiempo de respuesta, en consecuencia, quejas y molestias por parte del personal administrativo, docente y estudiantes. A continuación, se detalla en la tabla N° 7.

DESCRIPCIÓN DE LA PROBLEMÁTICA EN LA FILIAL

Tabla 7. Descripción de la Problemática

Problemas	**Latencia muy alta:** ✓ La respuesta de los sistemas de información es muy lenta, perjudicando el trabajo del personal administrativo que labora en la Filial ✓ Los estudiantes se quejan que en los laboratorios de cómputo la velocidad del internet es insuficiente, esto causa mala reputación de la universidad y por consecuencia no se matriculan muchas personas a los procesos de admisión. ✓ Los Docentes de la Filial suelen quejarse que no realizan de forma correcta sus clases de Tecnologías de la Información, porque es demasiado lento la velocidad de respuesta de las páginas web, también tienen problemas al ver el historial de su asistencia porque la página de la universidad no responde correctamente al solicitar los reportes. **Perdida de Paquetes** ✓ Al aplicar un Sniffer a la red interna de la Universidad se puede apreciar un Ping de respuesta demasiado alto y por consecuencia la perdida de paquetes, esto es porque el ancho de banda del internet está siendo utilizado de forma incorrecta al realizar descargas, ver videos en las diferentes páginas web existentes, juegos en línea y entre otros problemas que se pudo observar.
	Para el personal Administrativo: ➢ El personal administrativo requiere que el internet sea lo más estable posible para poder realizar sus labores normales como son matricula de estudiantes, reporte de notas, cobros de los estudiantes de la filial, reportes de tomas de daciones y también para el correcto funcionamiento del sistema de control de Asistencia Docente.

Necesidad	➢ Páginas web bloqueadas de acuerdo al trabajo que tenga asignado cada personal, esto ayudara a reducir el tráfico interno de la red. Para los Estudiantes: ➢ El estudiante de la Filial necesita que el internet funcione de acuerdo a la asignatura que realice en el laboratorio de cómputo, la velocidad debe ser igual para cada equipo y las páginas web estén habilitadas según la necesidad de la asignatura; de esta forma el estudiante podrá realizar sus clases de forma correcta y también podrá visualizar sus notas dentro de los laboratorios de la universidad y en el proceso de matrícula online poder matricularse sin ningún inconveniente. Para los Docentes: ➢ Los docentes de la filial necesitan que los laboratorios funcionen de forma correcta para realizar sus clases, verificar sus avances en la ejecución, verificar su asistencia en el sistema de Asistencia Docente (SIDCAD) y también poder buscar información para poder realizar sus investigaciones.

Autoría Propia

Para alcanzar el objetivo de mejorar la calidad de servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes dividiré los problemas, estas divisiones ayudaran a visualizar mejor el problema y de esta manera obtener mejores resultados.

Problema de Personal Administrativo

El personal administrativo sufre constantemente de caídas del servicio de internet y se debe al mal uso del mismo en los demás actores como son los estudiantes y hasta personal docente. El personal administrativo su queja constantemente que no funcionan los reportes académicos de los sistemas de la universidad y por ese motivo no pueden realizar sus labores de forma correcta.

Requisitos:

- Es necesario contar con el apoyo del personal administrativo para que me facilite la información acerca de sus labores y los inconvenientes que tiene al momento de laborar.

- Aplicare un Sniffer para monitorear la red y ver que puertos, protocolos y páginas web son las que más utilizan.

Se muestra a continuación el diagrama de red que tiene el personal administrativo actualmente:

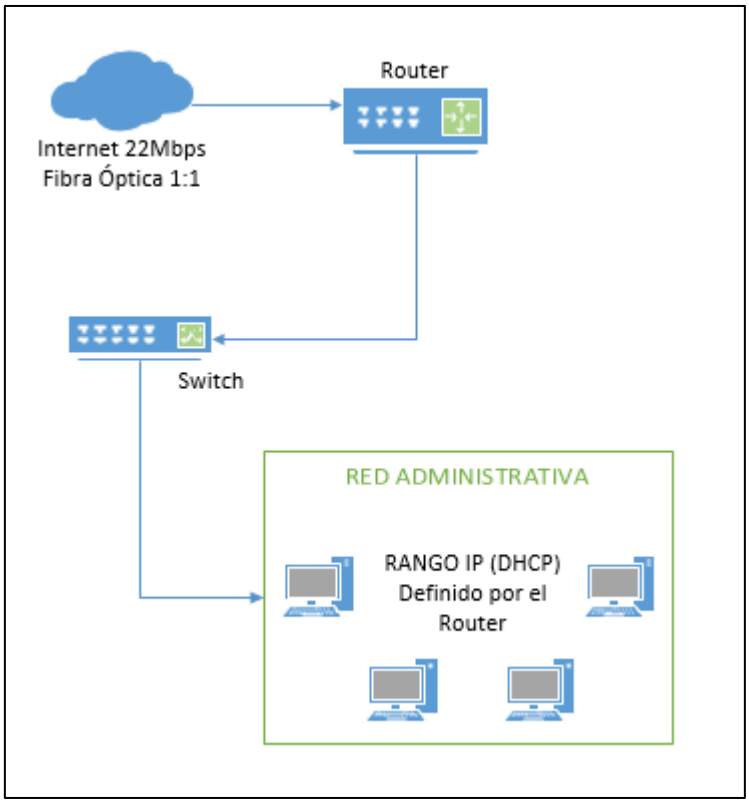

Figura 5. Diagrama de Red del personal Administrativo, Autoría Propia

En el diagrama se aprecia que no existe control alguno sobre el uso del servicio de internet, porque es prácticamente una conexión directa

desde el Router hacia los equipos del personal administrativo. No se tiene ningún registro de la navegación realizada por cada personal.

Problemas del Personal Docente

El personal docente para dictar sus clases necesita que la línea de internet esté funcionando correctamente en los laboratorios de cómputo en los horarios de Tics, también detalla que es necesario para verificar su marcación de asistencia en el Sistema de control de asistencia docente proporcionado por la universidad.

Requisitos:

- El docente tiene que brindar los horarios de clases que se le asigne para habilitar la navegación libre pero controlada en los laboratorios de cómputo.

- Controlar la Velocidad de Internet para el correcto uso del Ancho de Banda, así podemos controlar que en los dos laboratorios de cómputo funcione el internet en forma correcta.

A continuación, se muestra el diagrama de red de los laboratorios que actualmente se trabaja:

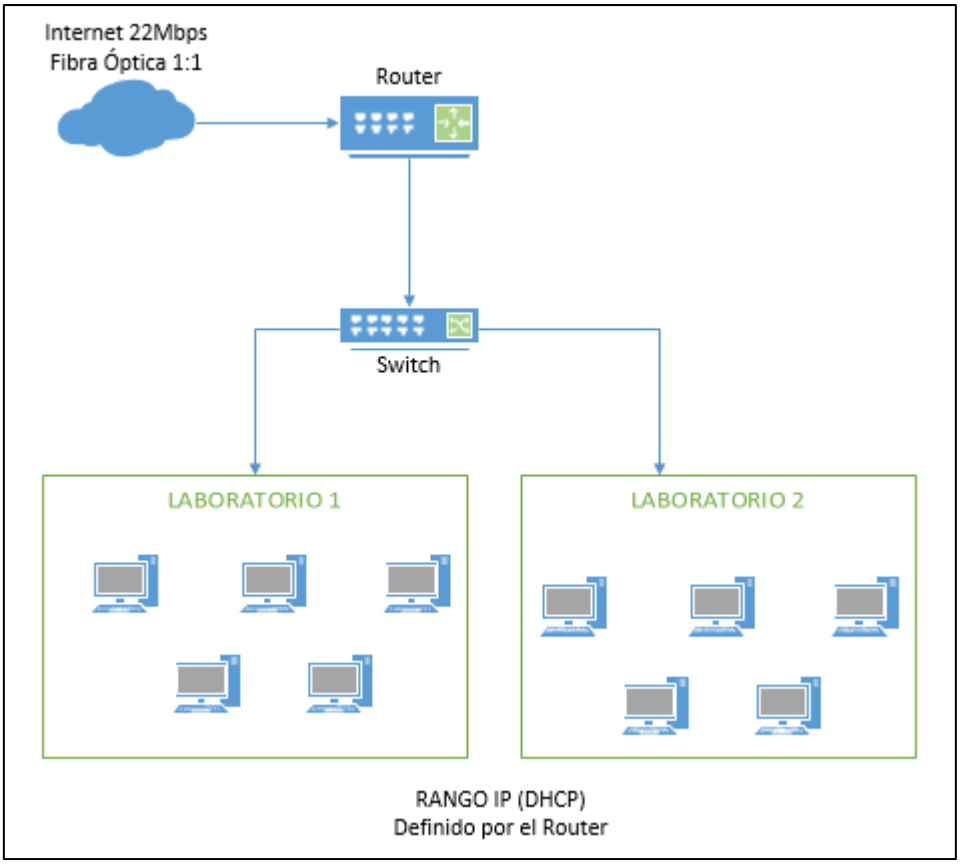

Figura 6. Diagrama de Red de Laboratorios, Autoría Propia

En el diagrama detalla que los equipos de cómputo no tienen ningún control, los estudiantes navegan, descargan y hasta juegan en cualquier página. Por el mal uso que hace algunos estudiantes se perjudica a todos los demás y hasta el docente no puede realizar sus clases con normalidad.

Problemas de los Estudiantes

En la filial se les facilita a los estudiantes un acceso a la red Wifi con sus usuario y contraseñas que se les detalla en la intranet, los estudiantes se quejan constantemente que no pueden ni siquiera acceder a los servicios de la universidad desde la red Wifi, también no

pueden realizar ningún tipo de búsqueda en varios momentos del día y que normalmente suele ser lenta la velocidad que se les brinda.

A continuación, se detalla cómo se encuentra la Red Wifi Actualmente:

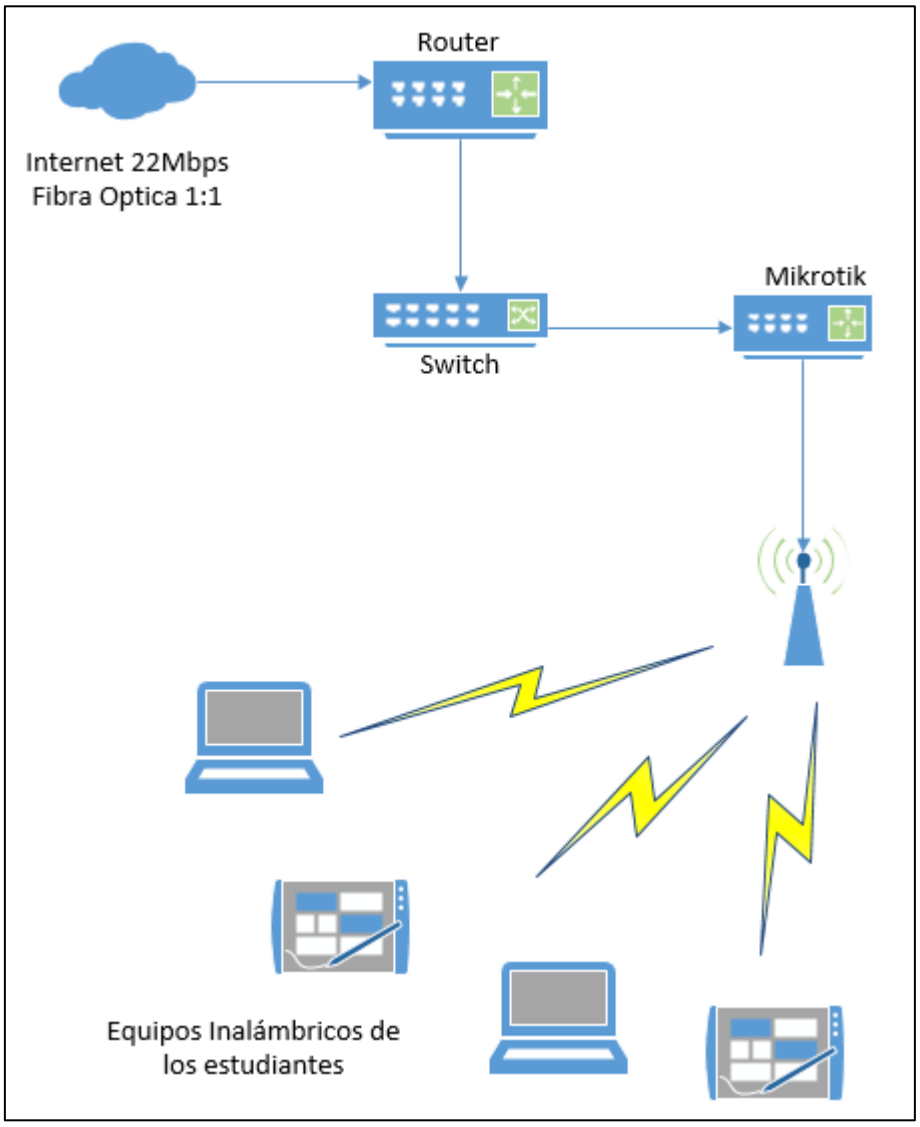

Figura 7. Diagrama de Red de la Red Wifi, Autoría Propia

Se aprecia que la conexión al equipo Mikrotik es en forma directa desde el Switch, es decir como una conexión directa desde el Router. Cuando muchos estudiantes ingresan a la red wifi suelen saturar la red total, se señala que cada estudiante tiene un plan de datos de 2GB por mes,

pero al no tener control sobre el ancho de banda asignado para el Wifi en las primeras semanas el servicio suele ser muy lento.

Problemas con el Servidor

La filial cuenta con un servidor por el cual se comunica el sistema de Asistencia Docente, este Servidor es de vital importancia ya que sin este los docentes no podrían verificar sus marcaciones diarias ni tampoco se tendría acceso al cliente de monitoreo de la red interna de la Filial.

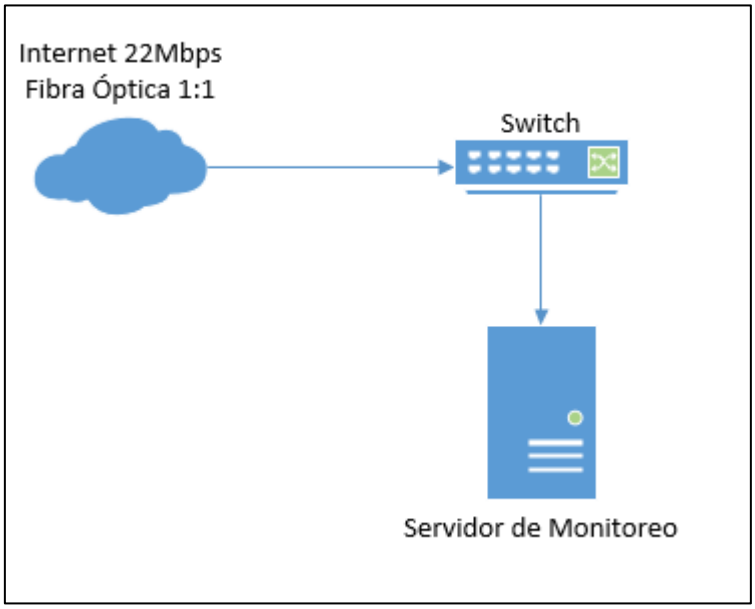

Figura 8. Diagrama de Red de los Servidores, Autoría Propia

Se puede apreciar que el servicio de internet de la misma manera llega directamente desde el Switch, esto ocasiona que no se pueda conectar correctamente al servidor a exportar las marcaciones de los docentes para el sistema de asistencia, también es muy lenta la transferencia de información.

4.2. FASE II: DISEÑO DE RED LÓGICO

4.2.1. Diseño de la topología de red

En la siguiente figura se detalla el funcionamiento del Firewall, la distribución IPs a detalle de toda la red que ahora será administrada. También se detalla la cantidad de tarjetas de Red que tiene el servidor que alberga al Firewall para que funcione correctamente, y por último se aprecia los equipos necesarios en la red interna de la universidad.

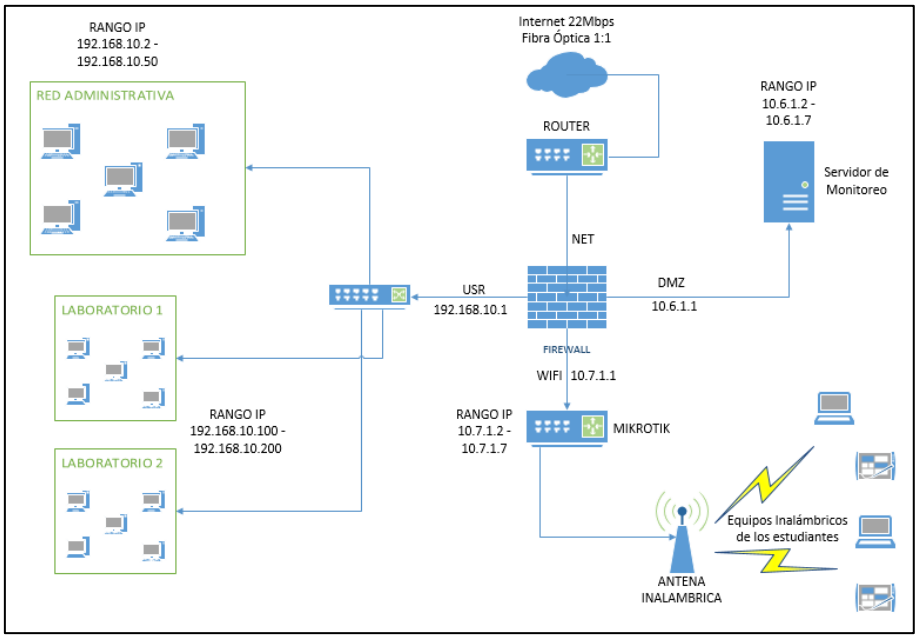

Figura 9. Diagrama de Red Lógico, Autoría Propia.

4.2.2. Protocolos de Red

Son conjuntos de normas que sirven para guiar una conducta o acción. Sirven para intercambiar paquetes de un equipo hacia una red de ordenadores es decir que para que dos ordenadores se comuniquen deben de utilizar los mismos protocolos de red. Existen muchos protocolos porque no es lo mismo interconectar dos equipos de cómputo a conectar el equipo a internet. Estos son los protocolos de red que se tienen en cuenta en esta investigación:

- IP (Protocolo de Internet)

- ARP (Protocolo de resolución de direcciones)
- TCP (Protocolo de control de transmisión)
- UDP (Protocolo de datagrama de usuario)
- HTTP (Protocolo de transferencia de hipertexto)

4.2.3. Estrategias para administrar la red

h. Conocer lo Básico

Aquí es donde se verifico los equipos que ya cuenta la universidad y cuáles son los que faltan por ejemplo en la universidad ya se cuenta con un Switch en cada laboratorio, Router con acceso a internet, dos servidores uno con el cliente de monitoreo y el otro para la instalación del Firewall, también se cuenta con un equipo Mikrotik para el control de accesos a la red Wifi con sus respectivas antenas en el Campus.

i. Elegir el Modelo de Implementación

En este caso la Red interna de la Filial Chanchamayo ya fue definida y se encuentra en operación, ahora para la investigación se debe ubicar el Firewall dentro de la red para que pueda administrar la Red en general.

j. Determinar las reglas de control en el Firewall

Según cada problema que se tiene en la red interna de la Filial Chanchamayo se creara una regla específica para bloquear páginas, controlar los accesos al servidor donde se aloja el cliente de monitoreo

4.3. FASE III: DISEÑO FÍSICO DE REDES

4.3.1. Selección de Dispositivos

Servidor para el Firewall

- CPU: E31220 3.10Ghz
- Arquitectura: 32bit, 64bit
- HDD: 1Tb
- RAM: 2Gb

Servidor para el Cliente de monitoreo

- CPU: E3-1245 v5 3.50Ghz
- Arquitectura: 32bit, 64bit
- HDD: 2 Tb
- RAM: 15 Gb

Equipo Mikrotik

- CPU: TLR4-00980CG-10CE
- Modelo: CCR1009-8G-1S
- RAM: 1Gb
- SO: Router OS
- HDD: 128 Mb

Switch (3 unidades)

- Marca: TPI-Link
- Cantidad de puertos: 48
- Capacidad de Computación: 96Gb/s
- Modelo: TL-SG1048

Distribución de equipos en el Gabinete de Red

En la figura se puede apreciar la distribución de los equipos dentro del Gabinete de Red, también se puede observar las conexiones que se

tiene dentro del Gabinete de Red y también el Punto de red que sale hacia el equipo Mikrotik que se encuentra en otra oficina dentro del Campus Universitario.

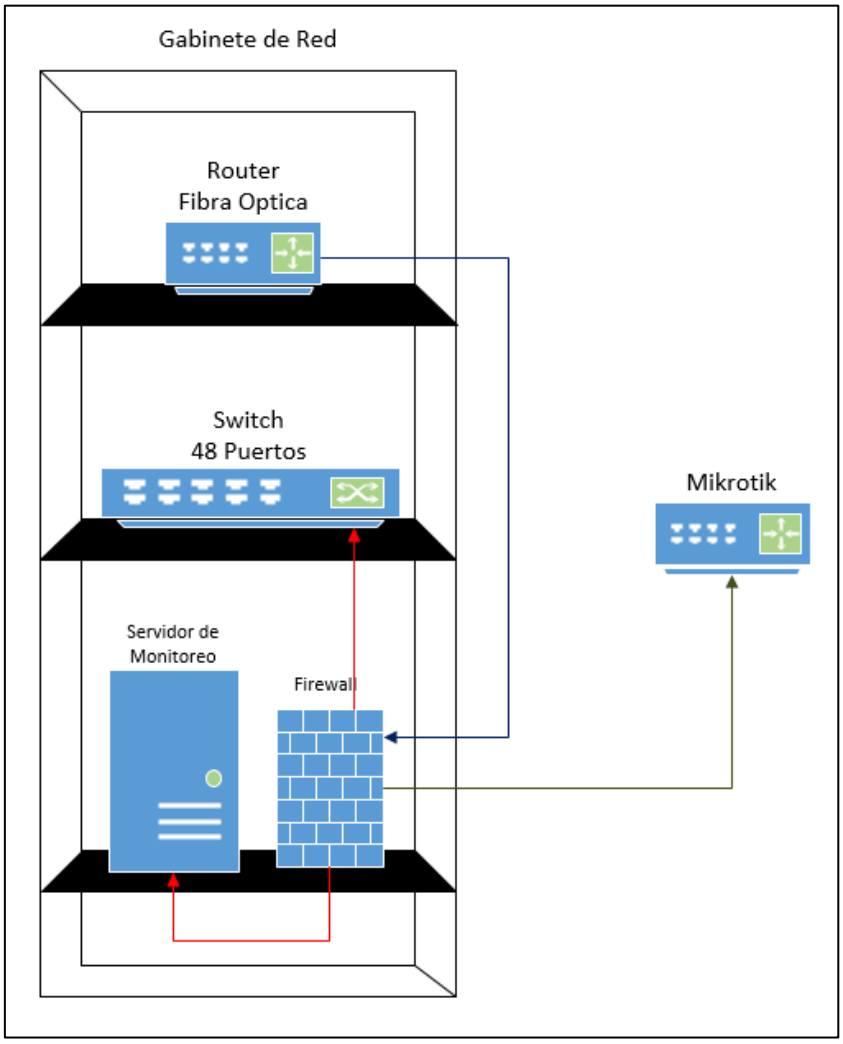

Figura 10. Distribución de Equipos, Autoría Propia

4.4. FASE IV: PRUEBA, OPTIMIZACIÓN Y DOCUMENTACIÓN DEL DISEÑO

En esta fase se detalla la construcción del Firewall desde la instalación del sistema Operativo en el Servidor, configuración de las tarjetas inalámbricas, Instalación del Shorewall, Instalación del Squid.

4.4.1. Instalación del Sistema Operativo CentOS 7 Minimal

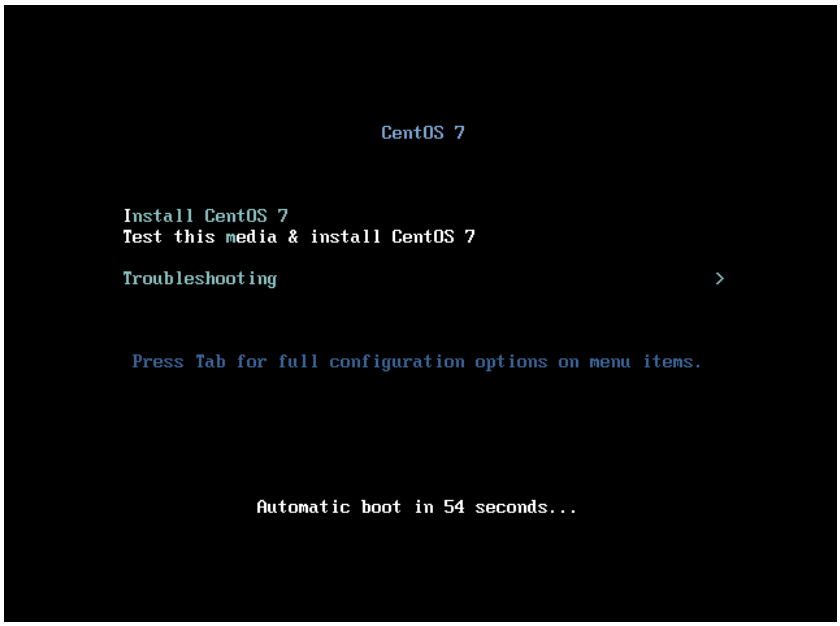

Figura 11. Inicio de Instalación, Auditoria Propia

Inicio de Instalación del S.O. CentOS 7 Minimal, una de las características del S.O. Minimal es el manejo por consola únicamente.

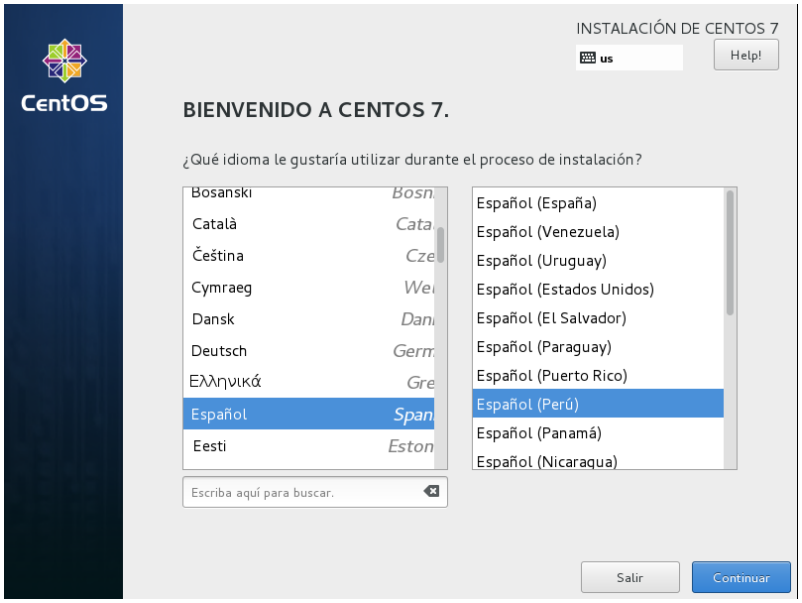

Figura 12. Selección de Idioma, Autoría Propia

Seleccionamos el Idioma con el cual vamos a instalar el S.O. CentOS 7 Minimal.

Figura 13. Selección de Disco, Autoría Propia

Seleccionamos el Disco Duro donde se instalará el S.O. CentOS 7 Minimal.

Figura 14. Creación de Usuario, Autoría Propia

Creamos una contraseña para el Usuario ROOT, consideremos que el Usuario ROOT es el usuario supremo en los Sistemas Operativos LINUX, no es necesario la creación de un usuario Adicional. Esperamos a que termine el proceso de instalación y reiniciamos el equipo.

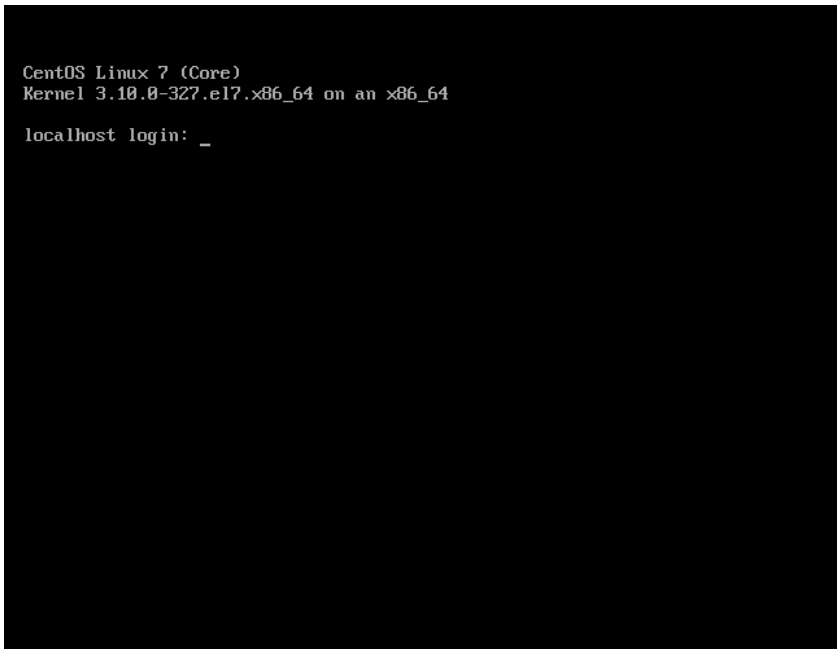

Figura 15. Pantalla de Inicio, Autoría Propia

Al terminar la Instalación nos sale esta pantalla, colocamos el usuario por defecto “ROOT” y la contraseña que asignamos al momento de la instalación.

4.4.2. Configuración del Firewall

Se ejecuta el siguiente comando:

/etc/sysconfig/network-scripts/

En la dirección se observa lo siguiente:

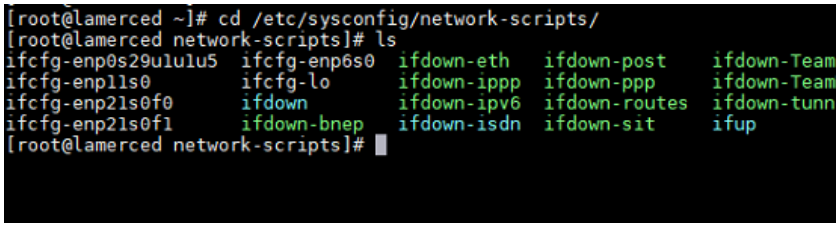

Figura 16. Lista de Interfaces de Red, Autoria Propia

Lo que se necesita en este directorio es identificar las tarjetas de red físicas del servidor, en este caso son 4 que se utilizaran de la siguiente manera:

- Ifcfg-enp6s0 -> Esta tarjeta se conectará a internet directamente del Router.

- Ifcfg-enp11s0 -> Esta tarjeta de red será para el grupo de red del personal administrativo y los laboratorios de computo.

- Ifcfg-eno21s0f0 -> Esta tarjeta de red será para el servidor de monitoreo.

- Ifcfg-eno21s0f1 -> esta tarjeta de red será para el servicio de Wifi del campus Universitario.

En esta ocasión se utilizó una configuración con IPv4 para lo cual editaremos primero la tarjeta de red que se conectara a internet, es decir la tarjeta identificada como “Ifcfg-enp6s0”. Colocamos el siguiente comando para ingresar a la edición:

Nano ifcfg-enp6s0

Al colocar el comando nos mostrara las siguientes opciones de configuración, lo configuración necesaria esta resaltado de rojo. Recomiendo eliminar o comentar las demás líneas para evitar cualquier problema futuro en la configuración de la red. Un comentario se realiza con el símbolo “#”.

TYPE=Ethernet

PROXY_METHOD=none

BROWSER_ONLY=no

BOOTPROTO=static

DEFROUTE=yes

IPV4_FAILURE_FATAL=no

IPV6INIT=yes

IPV6_AUTOCONF=yes

NAME=enp6s0

UUID=c7052bbb-9fc6-4152-a3fa-9d3d75652bc9

DEVICE=enp6s0

ONBOOT=yes

IPADDR=X.X.X.X

NETMASK=255.255.255.X

GATEWAY=X.X.X.X

DNS1=x.x.x.x

DNS2=y.y.y.y

Con la explicación realizada paso a configurar la interfaz de red “Ifcfg-enp6s0” de la siguiente manera (por motivos de seguridad no se muestra la “ip” publica que tiene la universidad):

```
TYPE=Ethernet
#PROXY_METHOD=none
#BROWSER_ONLY=no
BOOTPROTO=static
#DEFROUTE=yes
#IPV4_FAILURE_FATAL=no
#IPV6INIT=yes
#IPV6_AUTOCONF=yes
#IPV6_DEFROUTE=yes
#IPV6_FAILURE_FATAL=no
#IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp6s0
UUID=6ad86449-829a-45f0-be16-054049300762
DEVICE=enp6s0
ONBOOT=yes
IPADDR=[redacted]
NETMASK=255.255.255.248
GATEWAY=[redacted]
DNS1=[redacted]
DNS2=1.1.1.1
```

Figura 17. Configuración de Interfaz de Red - Internet, Autoría Propia

Ahora la configuración de la interfaz “Ifcfg-enp11s0”, Red de usuarios y laboratorios.

```
TYPE=Ethernet
#PROXY_METHOD=none
#BROWSER_ONLY=no
BOOTPROTO=static
#DEFROUTE=yes
#IPV4_FAILURE_FATAL=no
#IPV6INIT=yes
#IPV6_AUTOCONF=yes
#IPV6_DEFROUTE=yes
#IPV6_FAILURE_FATAL=no
#IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp11s0
#UUID=7a7aa933-5e7d-467e-8684-fe40aa28efd7
DEVICE=enp11s0
ONBOOT=yes
IPADDR=192.168.10.1
NETMASK=255.255.255.0
```

Figura 18. Configuración de Interfaz de Red - administrativos y laboratorios, Autoría Propia

Seguimos con la configuración de la interfaz “Ifcfg-eno21s0f0”, Red del servidor de monitoreo.

```
TYPE=Ethernet
#PROXY_METHOD=none
#BROWSER_ONLY=no
BOOTPROTO=static
#DEFROUTE=yes
#IPV4_FAILURE_FATAL=no
#IPV6INIT=yes
#IPV6_AUTOCONF=yes
#IPV6_DEFROUTE=yes
#IPV6_FAILURE_FATAL=no
#IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp21s0f0
#UUID=7a7aa933-5e7d-467e-8684-fe40aa28efd7
DEVICE=enp21s0f0
ONBOOT=yes
IPADDR=10.6.1.1
NETMASK=255.255.255.248
```

Figura 19. Configuración de Interfaz de Red - Servidores, Autoría Propia

Por último, la interfaz de red “Ifcfg-eno21s0f1”, Red Wifi.

```
TYPE=Ethernet
#PROXY_METHOD=none
#BROWSER_ONLY=no
BOOTPROTO=static
#DEFROUTE=yes
#IPV4_FAILURE_FATAL=no
#IPV6INIT=yes
#IPV6_AUTOCONF=yes
#IPV6_DEFROUTE=yes
#IPV6_FAILURE_FATAL=no
#IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp21s0f1
#UUID=7a7aa933-5e7d-467e-8684-fe40aa28efd7
DEVICE=enp21s0f1
ONBOOT=yes
IPADDR=10.7.1.1
NETMASK=255.255.255.248
```

Figura 20. Configuración de Interfaz de Red - Wifi, Autoría Propia

Ahora que ya concluimos con la configuración de las tarjetas de red actualizaremos el Sistema Operativo con el siguiente comando:

Yum update -y

cuando termine de descargar todos los archivos, se actualizará el sistema y procedemos a reiniciar el servidor con el siguiente comando:

reboot

Cuando inicie el sistema nos volvemos a identificar con el usuario y clave, antes de continuar con la instalación del Shorewall y Squid, debemos detener y desactivar el servicio del firewall que viene por defecto en el Sistema operativo, y para ellos utilizamos los siguientes comandos:

systemctl stop firewalld

systemctl disable firewalld

El primero comando detiene el firewall y el segundo evita que el firewall se inicie junto con el sistema operativo.

También se debe desactivar el SELINUX con el siguiente comando:

nano /etc/sysconfig/selinux

mostrará el siguiente contenido, la línea resaltada de rojo debe ser configura de esa manera, lo demás se deja por defecto. Y reiniciamos el Sistema Operativo.

 # This file controls the state of SELinux on the system.

 # SELINUX= can take one of these three values:

 # enforcing - SELinux security policy is enforced.

 # permissive - SELinux prints warnings instead of enforcing.

 # disabled - No SELinux policy is loaded.

SELINUX=disabled

 # SELINUXTYPE= can take one of three two values:

 # targeted - Targeted processes are protected,

 # minimum - Modification of targeted policy. Only selected processes are protected.

 # mls - Multi Level Security protection.

SELINUXTYPE=targeted

Instalación del servicio SHOREWALL

Para poder descargar los RPMs para la instalación del Shorewall instalaremos WGET con el siguiente comando:

yum install wget

cuando termine de instalar utilizaremos el WGET para obtener la última versión del firewall Shorewall, estos repositorios se encuentran en la siguiente dirección:

http://www.invoca.ch/pub/packages/shorewall/RPMS/ils-7/noarch/

En ese directorio debemos encontrar los repositorios Core y Base del Shorewall, tienen la siguiente estructura:

shorewall-5.x.x.x-x.el7.noreach.rpm

shorewall-core-5.x.x.x-x.el7.noreach.rpm

Para descargar los archivos necesarios para el Shorewall ingresamos los siguientes comandos:

Wget http://www.invoca.ch/pub/packages/shorewall/RPMS/ils-7/noarch/shorewall-5.X.X.X-X.el7.noarch.rpm

wget http://www.invoca.ch/pub/packages/shorewall/RPMS/ils-7/noarch/shorewall-core-5.X.X.X-X.el7.noarch.rpm

Los RPMs se descargarán en el directorio que nos encontrábamos al momento de ejecutar el comando, y para instalarlos utilizamos los siguientes comandos en ese mismo orden:

yum install –y shorewall-core-5.X.X.X-X.el7.noarch.rpm

yum install –y shorewall-5.X.X.X-X.el7.noarch.rpm

Una vez culminada la instalación podremos encontrar el siguiente directorio

cd /etc/Shorewall

En ese directorio encontraremos todos los archivos necesarios para configurar las reglas, las zonas, las políticas y entre otros necesarios para el correcto funcionamiento del Firewall Shorewall.

Los archivos que son necesarios configurar en esta solución son:

Tabla 8. Archivos de Configuración Shorewall

shorewall.conf	Archivo principal de configuración del Firewall, parámetros generales del comportamiento del firewall.
hosts	Se establecen quienes pertenecen a cada zona creada.
interfaces	Se establecen las interfaces físicas y las zonas principales a las que pertenecerán dichas interfaces, así mismo aquí se establece si se definirá la filtración a través de la dirección MAC.
maclist	En caso de que se habilite la filtración a través de las direcciones MAC.
	Se definen si las zonas aceptaran IPV4 o IPV6, así mismo también se define si se establecerán

zones	sub zonas de las zonas principales establecidas en el archivo interfaces.
policy	Se Definen los accesos o bloqueos de manera general entre las zonas y subzonas existentes en el firewall.
snat	En este archivo se realiza la comunicación entre las tarjetas de red, se especifica si la interfaz que nos provee internet tendrá comunicación con la interfaz que se comunica con la red de usuarios o servidores, así como la comunicación también entre estos dos últimos.
rules	En este archivo se define los accesos y re direccionamientos que ejecutara el firewall de acuerdo como los definamos.

Autoría Propia

Se empezó configurando el archivo “shorewall.conf” con el comando:

nano shorewall.conf

En el archivo buscamos las siguientes líneas y deberían estar de la siguiente manera:

STARTUP_ENABLED=Yes

IP_FORWARDING=On

Cuando se termine de configurar toda la parte inicial del Firewall Shorewall reiniciamos el sistema operativo.

Ahora que inicia el sistema operativo se procede a configurar el archivo “interfaces” de la siguiente manera:

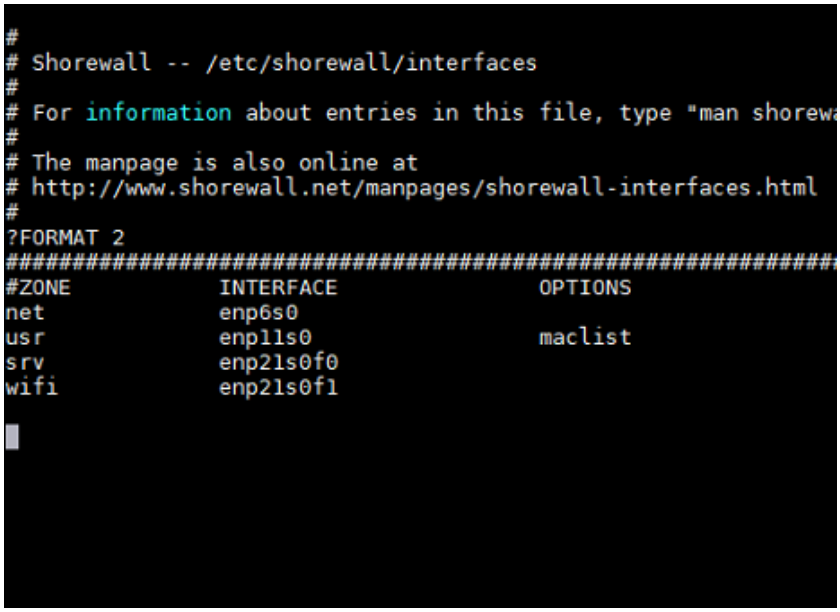

Figura 21. Interfaces - Shorewall, Autoría Propia

Se define los nombres de las zonas y con qué interfaces trabajara cada una, también se aprecia que la zona “usr” tiene como opción “maclist” esto obliga a realizar una filtración por medio de la MAC.

Una vez definida las interfaces procedemos a configurar el archivo “zones” de la siguiente manera:

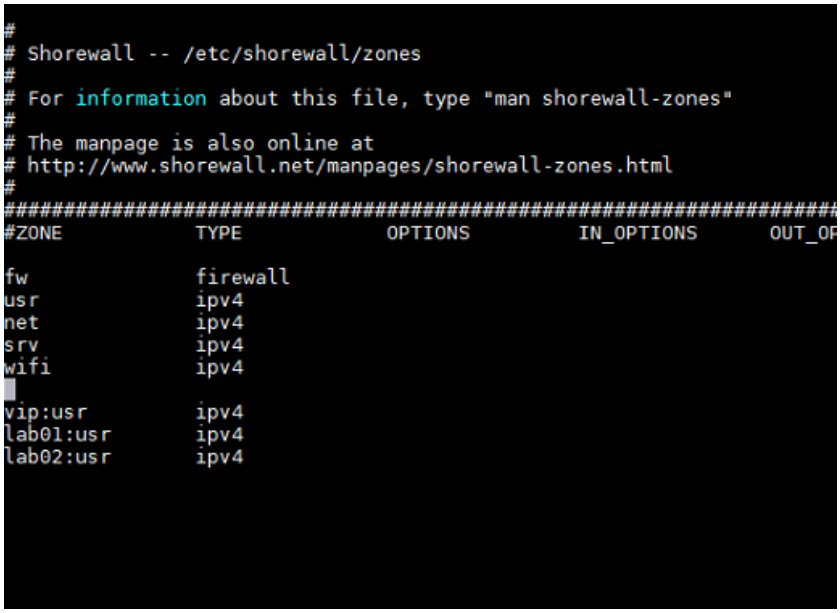

Figura 22. Zones - Shorewall, Autoría Propia

Se coloca el nombre de las zonas y también creamos sub zonas con el objetivo de ordenar los IPs para los administrativos y los laboratorios de cómputo. También se puede ver que en el tipo de red colocamos la IPv4.

Ahora modificaremos el archivo “maclist”, aquí se autoriza mediante la MAC a todos los equipos que tendrán acceso al servicio de internet en la Filial.

Configuración para los trabajadores administrativos en nivel “USUARIO”

```
# Shorewall -- /etc/shorewall/maclist
#
# For information about entries in this file, type "man shorewall-maclist"
#
# For additional information, see http://shorewall.net/MAC_Validation.html
#
#############################################################################
#DISPOSITION    INTERFACE              MAC                    ADDRESSES

################################## USUARIOS ###################################
ACCEPT          enp1ls0                C8:5B:76:FE:B7:F9      192.168.10.2 #ADMINISTRADOR S
ACCEPT          enp1ls0                44:8A:5B:8A:2E:AD      192.168.10.3 #MARCADOR DE ADMINISTRAT
ACCEPT          enp1ls0                f8:1a:67:7f:1d:7f      192.168.10.4 #DPTO ACADEMICO
ACCEPT          enp1ls0                84:c9:b2:7d:54:a8      192.168.10.5 #DPTO ACADEMICO
ACCEPT          enp1ls0                38:D5:47:0F:BA:CF      192.168.10.6 #DPTO DE SERVICIO SOCIAL

ACCEPT          enp1ls0                E0:CB:4E:8B:D5:DD      192.168.10.7

ACCEPT          enp1ls0                44:8a:5b:8a:28:90      192.168.10.8 #SECRETARIA DEL DIRECTOR

ACCEPT          enp1ls0                50:3E:AA:B2:BB:65      192.168.10.9 # ASISTENTE DPTO. ACADEM
ACCEPT          enp1ls0                44:8a:5b:8a:29:19      192.168.10.10 # SECRETARIA ACADEMICA
ACCEPT          enp1ls0                98:40:BB:49:8E:2D      192.168.10.11 # LAPTOP TEMPORAL DOCENT
ACCEPT          enp1ls0                0C:9D:92:78:DA:39      192.168.10.12 #BIBLIOTECA
ACCEPT          enp1ls0                0C:9D:92:78:CC:10      192.168.10.13 #BIBLIOTECA
ACCEPT          enp1ls0                90:FB:A6:3A:28:0F      192.168.10.14 #BIBLIOTECA
ACCEPT          enp1ls0                E0:CB:4E:8C:8A:C0      192.168.10.15 #BIBLIOTECA
ACCEPT          enp1ls0                90:FB:A6:3A:28:5F      192.168.10.16 #SALA DOCENTE NUMERO 1
```

Figura 23. Maclist usr - Shorewall, Autoría Propia

Configuración para los trabajadores administrativos en nivel “VIP”

```
################################### VIP #######################################

ACCEPT          enp1ls0                44:8a:5b:8a:2c:40      192.168.10.17 #JEFE DPTO ACADEMIC
ACCEPT          enp1ls0                F8:CA:B8:17:5B:CC      192.168.10.18 #ING JULIO PIZARRO
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.19
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.20
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.21
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.22
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.23
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.24
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.25
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.26
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.27
#ACCEPT         enp1ls0                xx:xx:xx:xx:xx:xx      192.168.10.28
```

Figura 24. Maclist vip - Shorewall, Autoría Propia

Configuración para los Laboratorios de cómputo número uno.

```
############################ LABORATORIO 1 ####################################

ACCEPT          enp1ls0         E0:D5:5E:AA:56:00               192.168.10.100  #PC1
ACCEPT          enp1ls0         E0:D5:5E:AC:7B:60               192.168.10.101  #PC2
ACCEPT          enp1ls0         E0:D5:5E:AC:84:74               192.168.10.102  #PC3
ACCEPT          enp1ls0         E0:D5:5E:AB:8B:4B               192.168.10.103  #PC4
ACCEPT          enp1ls0         E0:D5:5E:AB:7B:2B               192.168.10.104  #PC5
ACCEPT          enp1ls0         E0:D5:5E:AB:7B:47               192.168.10.105  #PC6
ACCEPT          enp1ls0         E0:D5:5E:AB:76:54               192.168.10.106  #PC7
ACCEPT          enp1ls0         E0:D5:5E:AC:A0:0A               192.168.10.107  #PC8
ACCEPT          enp1ls0         E0:D5:5E:AC:DC:FE               192.168.10.108  #PC9
ACCEPT          enp1ls0         E0:D5:5E:AB:99:6C               192.168.10.109  #PC10
ACCEPT          enp1ls0         E0:D5:5E:AB:86:81               192.168.10.110  #PC11
ACCEPT          enp1ls0         E0:D5:5E:AC:A0:13               192.168.10.111  #PC12
ACCEPT          enp1ls0         E0:D5:5E:AB:7A:73               192.168.10.112  #PC13
ACCEPT          enp1ls0         E0:D5:5E:AA:FB:8E               192.168.10.113  #PC14
ACCEPT          enp1ls0         E0:D5:5E:AB:4D:0C               192.168.10.114  #PC15
ACCEPT          enp1ls0         E0:D5:5E:AA:FB:A1               192.168.10.115  #PC16
ACCEPT          enp1ls0         E0:D5:5E:AC:69:3E               192.168.10.116  #PC17
ACCEPT          enp1ls0         E0:D5:5E:AC:64:83               192.168.10.117  #PC18
ACCEPT          enp1ls0         E0:D5:5E:AC:7A:D0               192.168.10.118  #PC19
ACCEPT          enp1ls0         E0:D5:5E:AC:7B:43               192.168.10.119  #PC20
ACCEPT          enp1ls0         E0:D5:5E:AA:56:10               192.168.10.120  #PC21
ACCEPT          enp1ls0         E0:D5:5E:AC:76:A1               192.168.10.121  #PC22
ACCEPT          enp1ls0         E0:D5:5E:AB:50:1E               192.168.10.122  #PC23
ACCEPT          enp1ls0         E0:D5:5E:AA:56:03               192.168.10.123  #PC24
ACCEPT          enp1ls0         E0:D5:5E:AC:62:52               192.168.10.124  #PC25
ACCEPT          enp1ls0         E0:D5:5E:AB:7A:78               192.168.10.125  #PC26
ACCEPT          enp1ls0         E0:D5:5E:AC:7B:44               192.168.10.126  #PC27
ACCEPT          enp1ls0         E0:D5:5E:AC:75:C5               192.168.10.127  #PC28
ACCEPT          enp1ls0         E0:D5:5E:AC:7A:CC               192.168.10.128  #PC29
ACCEPT          enp1ls0         E0:D5:5E:AC:79:63               192.168.10.129  #PC30
ACCEPT          enp1ls0         44:8A:5B:8A:2D:24               192.168.10.130  #PC Docente
```

Figura 25. Maclist lab01 - Shorewall, Autoría Propia

Configuración para los Laboratorios de cómputo número dos

```
############################ LABORATORIO 2 ####################################

ACCEPT          enp1ls0         E0:D5:5E:AC:81:05               192.168.10.141  #PC1
ACCEPT          enp1ls0         E0:D5:5E:AB:B8:44               192.168.10.142  #PC2
ACCEPT          enp1ls0         E0:D5:5E:AB:7B:62               192.168.10.143  #PC3
ACCEPT          enp1ls0         E0:D5:5E:AC:67:48               192.168.10.144  #PC4
ACCEPT          enp1ls0         E0:D5:5E:AC:A4:F7               192.168.10.145  #PC5
ACCEPT          enp1ls0         E0:D5:5E:AC:A0:48               192.168.10.146  #PC6
ACCEPT          enp1ls0         E0:D5:5E:AB:8B:20               192.168.10.147  #PC7
ACCEPT          enp1ls0         E0:D5:5E:AB:8B:12               192.168.10.148  #PC8
ACCEPT          enp1ls0         E0:D5:5E:62:63:B8               192.168.10.149  #PC9
ACCEPT          enp1ls0         E0:D5:5E:62:63:AF               192.168.10.150  #PC10
ACCEPT          enp1ls0         E0:D5:5E:6D:9E:4C               192.168.10.151  #PC11
ACCEPT          enp1ls0         E0:D5:5E:6D:9E:57               192.168.10.152  #PC12
ACCEPT          enp1ls0         E0:D5:5E:AB:8A:E7               192.168.10.153  #PC13
ACCEPT          enp1ls0         E0:D5:5E:AB:06:BE               192.168.10.154  #PC14
ACCEPT          enp1ls0         E0:D5:5E:AA:3A:34               192.168.10.155  #PC15
ACCEPT          enp1ls0         E0:D5:5E:AA:55:F0               192.168.10.156  #PC16
ACCEPT          enp1ls0         E0:D5:5E:AC:84:60               192.168.10.157  #PC17
ACCEPT          enp1ls0         E0:D5:5E:AC:82:99               192.168.10.158  #PC18
ACCEPT          enp1ls0         E0:D5:5E:AC:67:02               192.168.10.159  #PC19
ACCEPT          enp1ls0         E0:D5:5E:AC:81:0E               192.168.10.160  #PC20
ACCEPT          enp1ls0         E0:D5:5E:A5:E8:19               192.168.10.161  #PC21
ACCEPT          enp1ls0         E0:D5:5E:AC:7A:E9               192.168.10.162  #PC22
ACCEPT          enp1ls0         E0:D5:5E:AB:50:34               192.168.10.163  #PC23
ACCEPT          enp1ls0         E0:D5:5E:AB:3E:27               192.168.10.164  #PC24
ACCEPT          enp1ls0         E0:D5:5E:AA:C8:CB               192.168.10.165  #PC25
ACCEPT          enp1ls0         E0:D5:5E:A7:17:43               192.168.10.166  #Pc26
ACCEPT          enp1ls0         E0:D5:5E:AB:7B:5B               192.168.10.167  #PC27
ACCEPT          enp1ls0         E0:D5:5E:AB:8A:CF               192.168.10.168  #PC28
ACCEPT          enp1ls0         E0:D5:5E:AB:B8:73               192.168.10.169  #PC29
ACCEPT          enp1ls0         E0:D5:5E:AB:8B:4D               192.168.10.170  #PC30
ACCEPT          enp1ls0         E0:D5:5E:AB:8A:FD               192.168.10.171  #PC31
ACCEPT          enp1ls0         E0:D5:5E:AB:8B:0D               192.168.10.172  #PC32
ACCEPT          enp1ls0         E0:D5:5E:AB:50:24               192.168.10.173  #PC33
ACCEPT          enp1ls0         E0:D5:5E:AB:7B:2C               192.168.10.174  #PC34
ACCEPT          enp1ls0         E0:D5:5E:AC:84:95               192.168.10.175  #PC35
ACCEPT          enp1ls0         44:8A:5B:8A:29:0F               192.168.10.176  #PC Docente
```

Figura 26. Maclist lab02 - Shorewall, Autoría Propia

En esta configuración se aprecia que la columna tres y cuatro son las que varían son donde van la dirección MAC y el IP respectivamente, en la columna dos se coloca la interfaz de red del servidor a través por la cual el cliente se conectara.

Ahora toca configurar el archivo “hosts”, acá definiremos las IP que pertenecerán a las sub zonas creadas de la siguiente manera:

```
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-hosts.html
#
###############################################################################
#ZONE           HOSTS                           OPTIONS

vip     enp1ls0:192.168.10.17
vip     enp1ls0:192.168.10.18
vip     enp1ls0:192.168.10.19
vip     enp1ls0:192.168.10.20
vip     enp1ls0:192.168.10.21
vip     enp1ls0:192.168.10.22
vip     enp1ls0:192.168.10.23
vip     enp1ls0:192.168.10.24
vip     enp1ls0:192.168.10.25
vip     enp1ls0:192.168.10.26
vip     enp1ls0:192.168.10.27
vip     enp1ls0:192.168.10.28
```

Figura 27. Host Vip - Shorewall, Autoría Propia

```
lab01   enp1ls0:192.168.10.100
lab01   enp1ls0:192.168.10.101
lab01   enp1ls0:192.168.10.102
lab01   enp1ls0:192.168.10.103
lab01   enp1ls0:192.168.10.104
lab01   enp1ls0:192.168.10.105
lab01   enp1ls0:192.168.10.106
lab01   enp1ls0:192.168.10.107
lab01   enp1ls0:192.168.10.108
lab01   enp1ls0:192.168.10.109
lab01   enp1ls0:192.168.10.110
lab01   enp1ls0:192.168.10.111
lab01   enp1ls0:192.168.10.112
lab01   enp1ls0:192.168.10.113
lab01   enp1ls0:192.168.10.114
lab01   enp1ls0:192.168.10.115
lab01   enp1ls0:192.168.10.116
lab01   enp1ls0:192.168.10.117
lab01   enp1ls0:192.168.10.118
lab01   enp1ls0:192.168.10.119
lab01   enp1ls0:192.168.10.120
lab01   enp1ls0:192.168.10.121
lab01   enp1ls0:192.168.10.122
lab01   enp1ls0:192.168.10.123
lab01   enp1ls0:192.168.10.124
lab01   enp1ls0:192.168.10.125
lab01   enp1ls0:192.168.10.126
```

Figura 28. Host lab01 - Shorewall, Autoría Propia

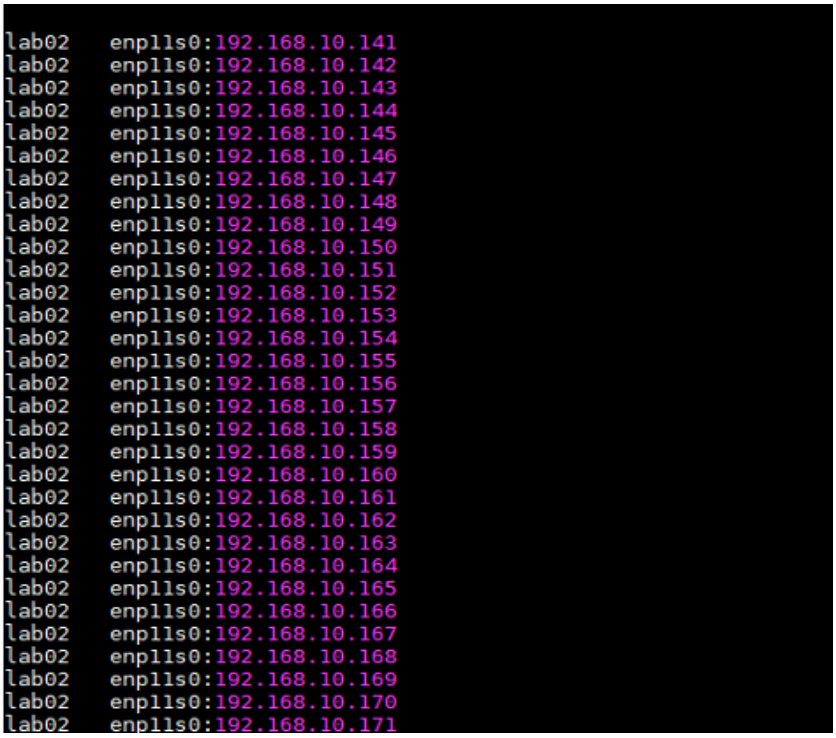

Figura 29. Host lab02 - Shorewall, Autoría Propia

Como se aprecia en los gráficos primero se coloca la sub zona luego se coloca la interfaz de red por donde ingresará la conexión del cliente y seguido de los dos puntos se coloca la IP del usuario que será parte de esa zona.

Ahora debemos configurar el archivo “policy”, definiremos los bloqueos o accesos por cada zona y sub zona que creamos de la siguiente manera:

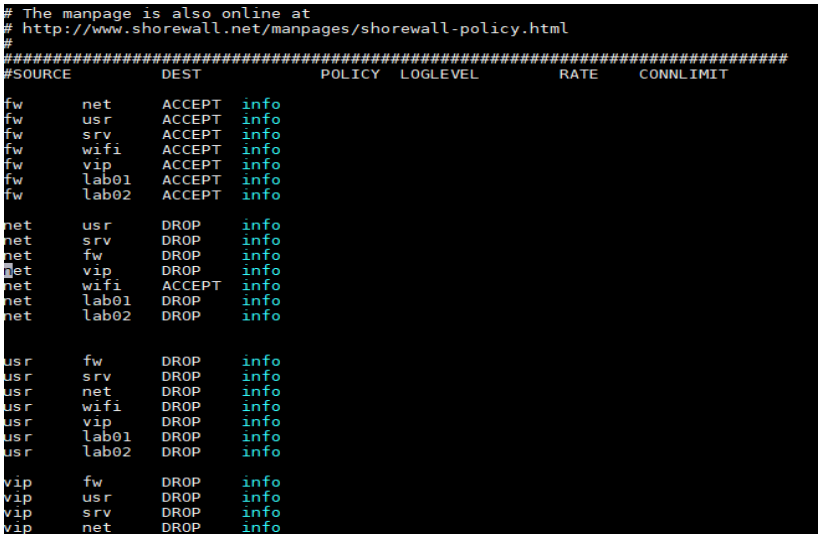

Figura 30. Policy - Shorewall, Autoría Propia

La sintaxis correcta para establecer las políticas es que en la primera columna es la zona de origen, la segunda columna es la zona destino, en la tercera columna se define si se bloquea (DROP) o se acepta (ACCEPT) la comunicación entre las zonas, en la cuarta columna se colca “info” para que se registre sus actividades en los Logs. Todas las zonas y sub zonas deben estar declaradas con sus respectivos bloqueos o accesos, en caso contrario el Firewall mostrara un error al momento de iniciar.

Ahora se configuro el archivo “snat” de la siguiente manera:

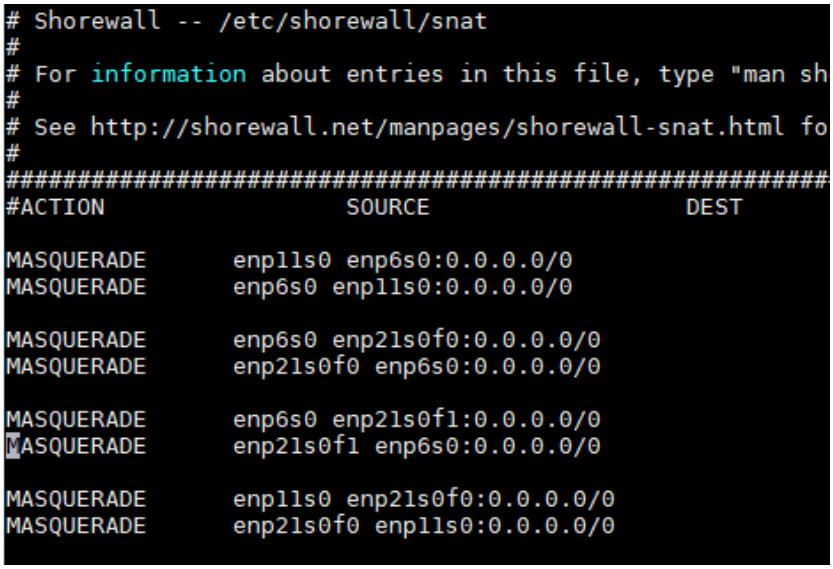

Figura 31. Snat - Shorewall, Autoría Propia

La sintaxis correcta para establecer el “snat” es primero colocar MASQUERADE seguido de las interfaces que queremos comunicar entre sí, luego se coloca el IP por el cual queremos que se comunique, en este caso utilizamos el comodín 0.0.0.0/0.

Por último, se definió las reglas, esta es la parte más importante del Shorewall Firewall ya que aquí es donde definiremos las reglas de accesos y los redireccionamientos que se ejecutara.

El Shorewall Firewall fue configurado de la siguiente manera:

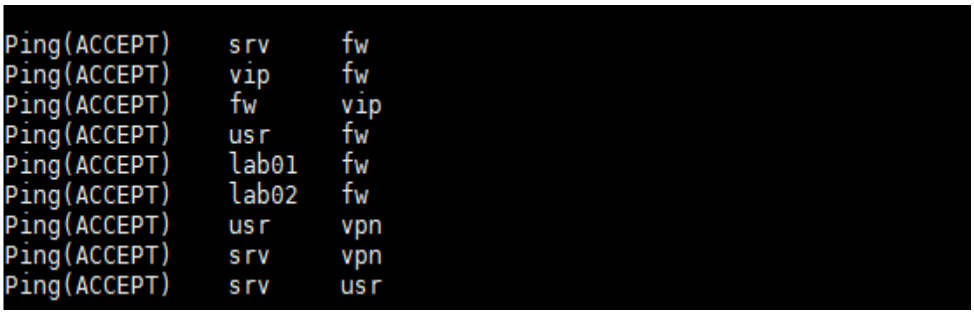

Figura 32. Rules Ping - Shorewall, Autoría Propia

Se autoriza el ping a las zonas y sub zonas según la necesidad, esto sirve para probar la conectividad entre las distintas zonas y también comprobar si llegan hasta el Shorewall Firewall.

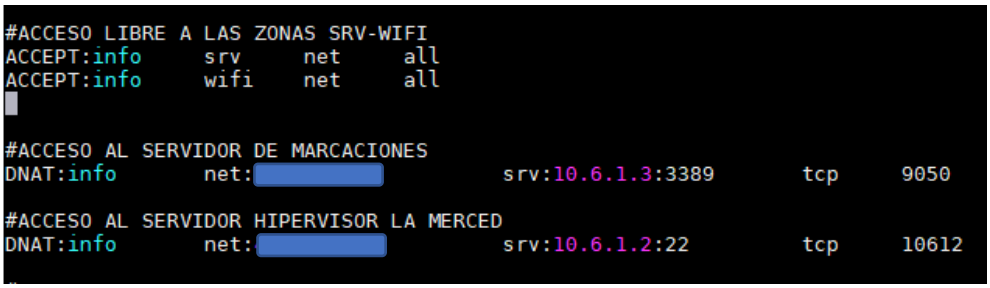

Figura 33. Rules acceso - Shorewall, Autoría Propia

Según el análisis el Wifi y los servidores deben de contar con internet libre, en las líneas tres y cuatro se lee que las zonas “wifi” y “srv” se conecten hacia la “net” en forma total.

Ahora también debemos tener acceso al servidor de marcaciones para exportar las marcaciones de los docentes y así actualizar el Sistema de Control Asistencia Docente, ahora conectarnos al hipervisor es de suma importancia para controlar el tráfico de la red interna de la filial. En las líneas siguientes se detalla que por medio de un direccionamiento la “net” (se detalla el único “ip” publico que puede ingresar) se conecte a la zona de servidores (se detalla a que “ip” específicamente debe ingresar) por medio del puerto 3389, 22(Puertos de escritorio remoto y ssh respectivamente) enmascarado con un puerto cualquiera. En la imagen no se muestra el “ip” publico de la universidad por motivos de seguridad.

```
#ACEPTAR INGRESO POR SSH AL FIREWALL DESDE LA NET
ACCEPT:info     net:[redacted]      fw      tcp     22
ACCEPT:info     srv             fw      tcp     22

#ACCESO AL SQUID
ACCEPT  usr     fw      tcp     3128
ACCEPT  vip     fw      tcp     3128
ACCEPT  lab01   fw      tcp     3128
ACCEPT  lab02   fw      tcp     3128
```

Figura 34. Rules acceso 2 - Shorewall, Autoría Propia

En las primeras tres líneas se configura el acceso por “ssh” al firewall, esto es para poder ingresar al firewall desde la sede central de la universidad (también se define la “ip” publica especifica que puede ingresar) y también se configura que se ingrese al firewall desde la zona de servidores y por último en la parte que dice “ACCESO AL SQUID” se coloca las zonas que tendrán control para el bloqueo de páginas, control de ancho de banda y el bloqueo de puertos por medio del puerto 3128.

4.4.3. Configuración del proxy Squid

Una vez terminada la configuración del Firewall Shorewall, se continua con la instalación del proxy Squid.

Descargamos el código fuente de la compilación del Squid con el siguiente comando:

wget http://www.squid-cache.org/Versions/v4/squid-4.X.tar.gz

Culminada la descarga lo descomprimimos con el siguiente comando:

tar -xvzf squid-4.3.tar.gz

Ahora para poder configurar correctamente el Proxy Squid necesitamos instalar el “gcc” con el siguiente comando:

yum install wget gcc gcc-c++ make perl –y

Con el archivo del Squid descomprimido nos dirigimos al directorio “Squid-4.x” y dentro de del directorio existe un archivo llamado “configure”, para ejecutar y configurar el archivo ejecutamos el siguiente comando:

./configure --enable-inline --enable-removal-policies=lru,heap --enable-poll --enable-delay-pools --enable-cache-digest --enable-snmp --enable-htcp --enable-carp --enable-select --enable-large-files --enable-underscores --enable-icap-client --with-filedescriptors=372925 --enable-arp-acl --with-maxfd=372925 --enable-basic-auth-helper=NCSA --enable-storeio=aufs --enable-async-io --enable-ltdl-convenience

Una vez termine de configurarse los parámetros colocamos los siguientes comandos:

make all

make install

Cuando termine de configurar el Squid, encontraremos los archivos del Squid en el directorio:

cd /usr/local/Squid/etc

Ahora se configura el archivo principal que administra el comportamiento del servicio Squid Proxy, el archivo tiene el nombre de “squid.conf” aquí definiremos los siguientes parámetros:

- Definición de IP y puerto de acceso de los clientes
- Definición de las listas IP, control de acceso y control de dominios.

- Definición del control de ancho de banda

Definición de IP y Puerto de acceso a clientes

```
#DEFINICION DEL PUERTO PROXY
http_port 192.168.10.1:3128
```

Figura 35. Puerto - Squid, Autoría Propia

Esta IP y puerto es configurada en opciones de internet de un equipo con Sistema Operativo Windows 10 de la siguiente manera:

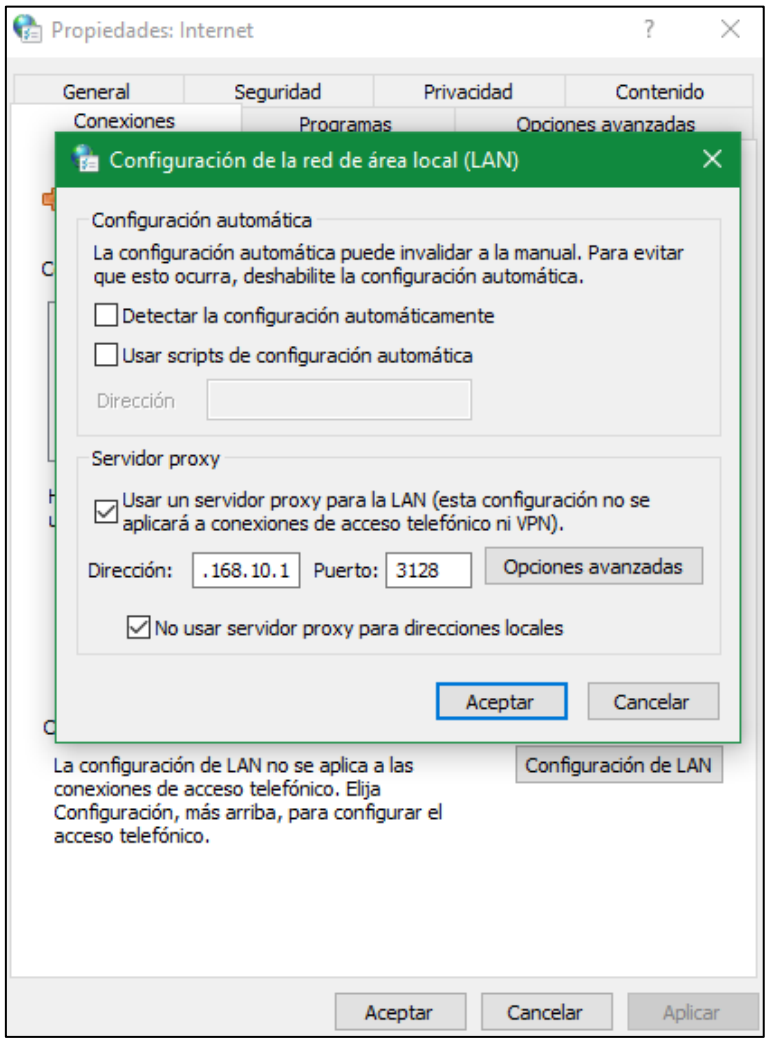

Figura 36. Ejemplo Puerto - Squid, Autoría Propia

Todo equipo que ingrese a la red interna de la Filial Chanchamayo debe de tener esta configuración en el proxy para que pueda acceder a internet, esto ayuda a guardar el registro de actividades de cada usuario en el “LOG” del Squid.

Definición de las listas IP, control de acceso y control de dominios

```
#############################################################################
############################## LISTA DE IPS ##################################
#############################################################################

acl ips_usuarios src "/usr/local/squid/etc/lista_ips/usr"
acl ips_vip src "/usr/local/squid/etc/lista_ips/vip"
acl ips_laboratorio-1 src "/usr/local/squid/etc/lista_ips/laboratorio-1"
acl ips_laboratorio-2 src "/usr/local/squid/etc/lista_ips/laboratorio-2"

#############################################################################
#####################  LISTA CONTROL DE ACCESO ##############################
#############################################################################

acl lista_blanca_puertos port "/usr/local/squid/etc/lista_control/puertos"
acl lista_negra_palabras url_regex -i "/usr/local/squid/etc/lista_control/palabras"
acl lista_negra_extensiones urlpath_regex "/usr/local/squid/etc/lista_control/extensiones"

#############################################################################
#####################  LISTA CONTROL DE DOMINIOS ############################
#############################################################################

acl dominio_winupdate dstdomain .windowsupdate.com
acl dominio_winupdate dstdomain .microsoft.com

acl dominios_autorizados dstdomain "/usr/local/squid/etc/lista_dominios/autorizados"
acl dominios_global dstdomain "/usr/local/squid/etc/lista_dominios/global"
acl dominios_bloqueo_general dstdomain "/usr/local/squid/etc/lista_dominios/general"
acl dominios_multimedia dstdomain "/usr/local/squid/etc/lista_dominios/multimedia"
acl dominios_juegos dstdomain "/usr/local/squid/etc/lista_dominios/juegos"
acl dominios_juegos_online dstdomain "/usr/local/squid/etc/lista_dominios/juegos_online"
acl dominios_porno dstdomain "/usr/local/squid/etc/lista_dominios/porno"
acl dominios_proxy dstdomain "/usr/local/squid/etc/lista_dominios/proxy"
acl dominios_filehostings dstdomain "/usr/local/squid/etc/lista_dominios/filehostings"
acl dominios_info dstdomain "/usr/local/squid/etc/lista_dominios/info"
```

Figura 37. Definición de listas- Squid, Autoría Propia

Listas IP

Separamos las IP que serán asignadas para realizar un control diferente a cada tipo de usuario de la siguiente manera: Lista de IPs de la sub zona “usr”

Figura 38. Lista IP usr - Squid, Autoría Propia

Lista de IPs de la sub zona “vip”

Figura 39. Lista IP vip - Squid, Autoría Propia

Lista de IPs de la sub zona “laboratorio-1”

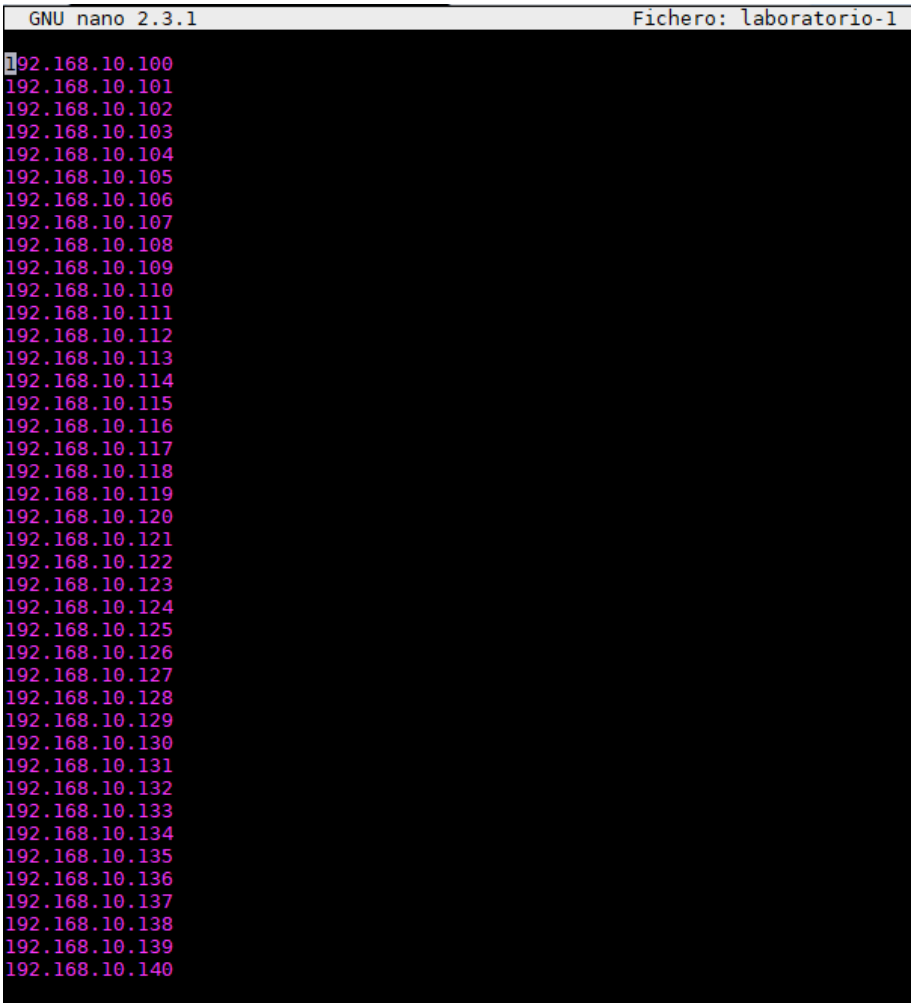

Figura 40. Lista IP lab01 - Squid, Autoría Propia

Lista de IPs de la sub zona “laboratorio-2”

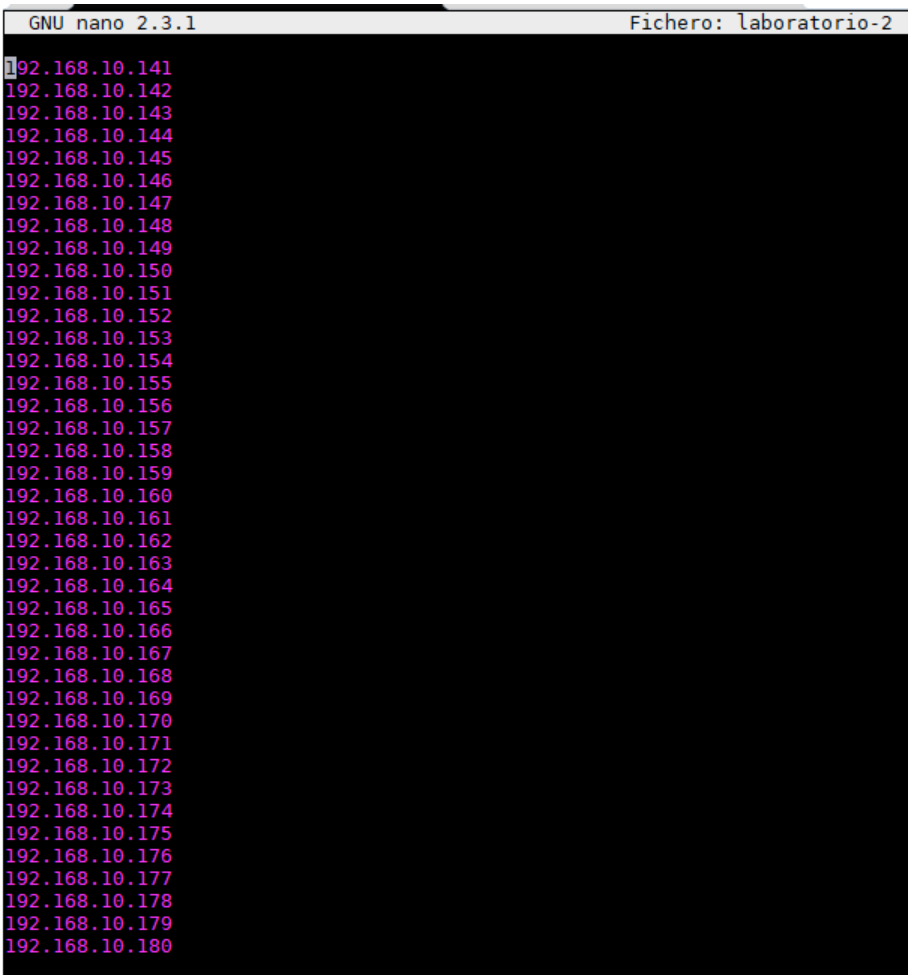

Figura 41. Lista IP lab02 - Squid, Autoría Propia

Culminada la separación de IPs procedemos a crear las listas de control de acceso:

Lista de palabras bloqueadas:

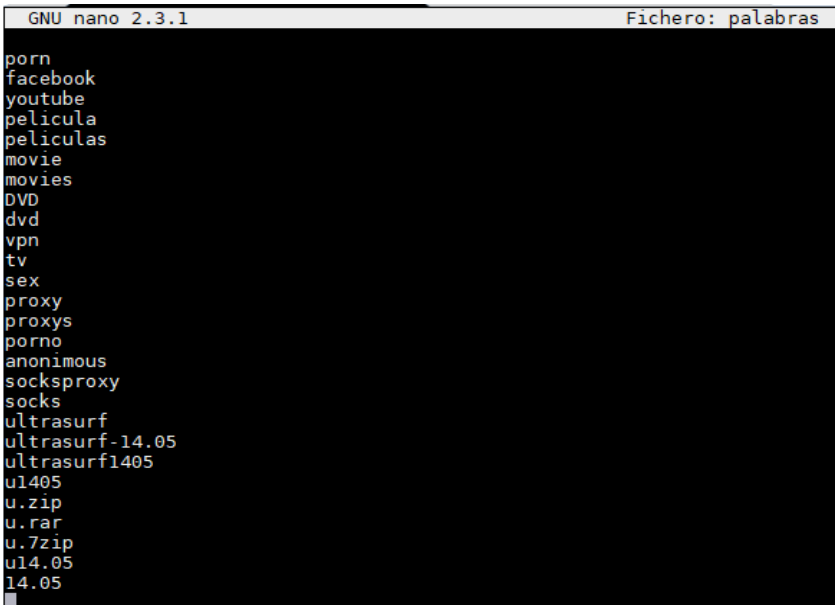

Figura 42. Lista Palabras - Squid, Autoría Propia

Lista de extensiones bloqueadas

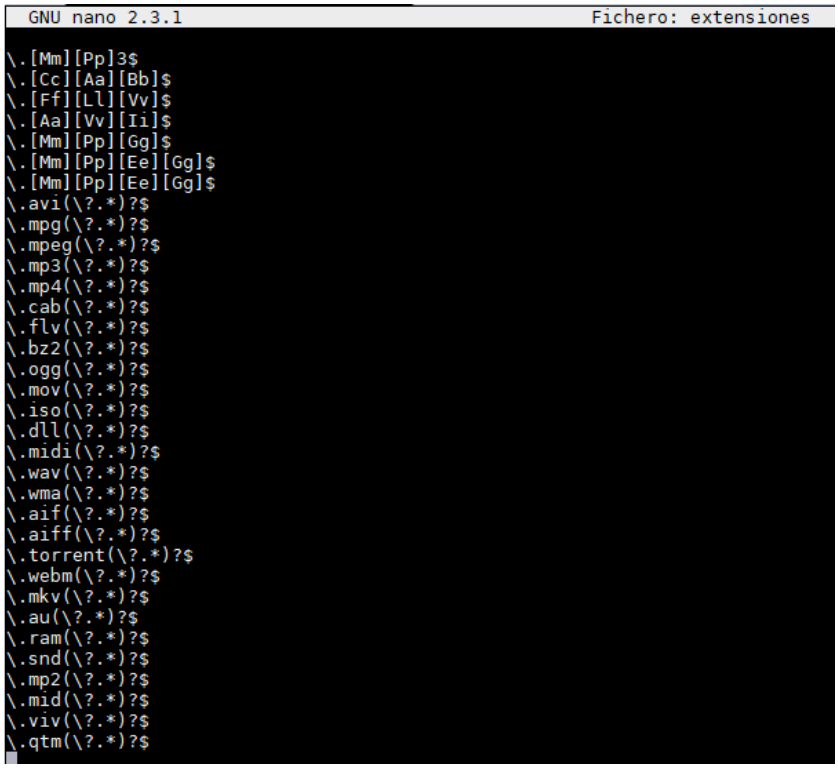

Figura 43. Lista Extensiones - Squid, Autoría Propia

Lista de puertos permitidos:

Figura 44. Lista Puertos - Squid, Autoría Propia

De la misma manera en que se realizó las listas de puertos, extensiones y palabras se crean listas de dominios autorizados, dominios generales, dominios multimedia, dominios de juegos online, dominios de páginas pornográficas, dominios de proxy, dominios globales, dominios de descargas para posteriormente ir denegando los accesos según el nivel de usuario.

A continuación, se muestra cómo se realiza concede y se bloquea según las listas creadas:

```
#############################################################################
#################### DEFINICION DE REGLAS DE ACCESO Y BLOQUEO ################
#############################################################################

#DENEGACION DE WINDOWS UPDATE
http_access deny dominio_winupdate

#ACCESO SIN RESTRICIONES A USUARIOS VIP
http_access allow ips_vip

#ACEPTAR A LOS DOMINIOS A LOS AUTORIZADOS
http_access allow dominios_autorizados ips_laboratorio-1
http_access allow dominios_autorizados ips_laboratorio-2
http_access allow dominios_autorizados ips_usuarios

#DENEGACION A LOS PUERTOS QUE NO ESTEN ESPECIFICADOS EN lista_blanca_puertos
http_access deny !lista_blanca_puertos ips_laboratorio-1
http_access deny !lista_blanca_puertos ips_laboratorio-2
http_access deny !lista_blanca_puertos ips_usuarios

#DENEGACION A LAS PALABRAS ESPECIFICADAS EN lista_negra_palabras
http_access deny lista_negra_palabras ips_laboratorio-1
http_access deny lista_negra_palabras ips_laboratorio-2
http_access deny lista_negra_palabras ips_usuarios

#DENEGACION A LAS PALABRAS ESPECIFICADAS EN lista_negra_extensiones
http_access deny lista_negra_extensiones ips_laboratorio-1
http_access deny lista_negra_extensiones ips_laboratorio-2
http_access deny lista_negra_extensiones ips_usuarios

#DENEGACION A LAS PALABRAS ESPECIFICADAS EN dominios_bloqueo_general
http_access deny dominios_bloqueo_general ips_laboratorio-1
http_access deny dominios_bloqueo_general ips_laboratorio-2
http_access deny dominios_bloqueo_general ips_usuarios

#DENEGACION A LAS PALBRAS ESPECIFICADAS EN dominios_global
http_access deny dominios_global ips_laboratorio-1
http_access deny dominios_global ips_laboratorio-2
http_access deny dominios_global ips_usuarios
```

Figura 45. Definición de Reglas - Squid, Autoría Propia

En la figura se muestra a detalle que los usuarios “vip” contaran con acceso a internet libre pero controlado y los demás usuarios que se encuentran en las sub zonas “usr, laboratorio-1, laboratorio-2” tienen restricciones según las listas creadas con anterioridad y también se controla las páginas que puede acceder según detalla la lista de dominios autorizados.

Ahora limitaremos el ancho de banda, como tenemos cuatro sub zonas de usuarios se separa en cuatro clases de usuarios de la misma manera, en siguiente cuadro se detalla la velocidad asignada a cada uno.

Tabla 9. Definición de Ancho de Banda

Sub Zona	Velocidad Asignada
VIP	350 kbps
USR	250 kbps
LABORATORIO-1	250 kbps
LABORATORIO-2	250 kbps

Autoría Propia

En el Squid con el siguiente código se limita la velocidad según el cuadro:

```
#####################################################################
################ DEFINICION DE CUOTAS DE ANCHO DE BANDA ##############
#####################################################################

#DEFINICION DE LOS GRUPOS PARA SEGMENTACION DE ANCHO DE BANDA
delay_pools 4

#CUOTA DE 350kbps/s PARA EL GRUPO LISTA DE ips_vip
delay_class 1 2
delay_parameters 1 -1/-1 750000/-1500000
delay_access 1 allow ips_vip

#CUOTA DE 250kbps/s PARA EL GRUPO LISTA DE ips_usuarios
delay_class 2 2
delay_parameters 2 -1/-1 500000/1000000
delay_access 2 allow ips_usuarios

#CUOTA DE 250kbps/s PARA EL GRUPO LISTA DE ips_laboratorio-1
delay_class 3 2
delay_parameters 3 -1/-1 500000/1000000
delay_access 3 allow ips_laboratorio-1

#CUOTA DE 250kbps/s PARA EL GRUPO LISTA DE ips_laboratorio-2
delay_class 4 2
delay_parameters 4 -1/-1 500000/1000000
delay_access 4 allow ips_laboratorio-2
```

Figura 46. Definición de Ancho de Banda - Squid, Autoría Propia

Ahora se habilita el internet libre a los laboratorios en los horarios de TICs para que los docentes puedan realizar sus clases, de la siguiente manera programada en el Squid:

```
#############################################################################
######################### LIBERAR LABORATORIOS ##############################
#############################################################################

#LABORATORIO 1
acl Lab1-Lunes  time M 12:15-14:30
acl Lab1-Jueves time H 7:45-10:00
acl Lab1-Viernes time F 16:45-21:00

#LABORATORIO 2
acl Lab2-Lunes1 time M 7:45-10:00
acl Lab2-Lunes2 time M 16:00-18:15
acl Lab2-Viernes time F 16:45-19:00

#LABORATORIO 1
http_access allow Lab1-Lunes ips_laboratorio-1
http_access allow Lab1-Jueves ips_laboratorio-1
http_access allow Lab1-Viernes ips_laboratorio-1

#LABORATORIO 2
http_access allow Lab2-Lunes1 ips_laboratorio-2
http_access allow Lab2-Lunes2 ips_laboratorio-2
http_access allow Lab2-Viernes ips_laboratorio-2
```

Figura 47. Horarios Docente - Squid, Autoría Propia

En la figura primero se detalla el horario en el cual el docente tiene clases de TICs en la semana, luego se habilita el acceso a internet libre a las IPs de los laboratorios en el horario previamente detallado.

Con todas las configuraciones realizadas el Firewall empieza a funcionar correctamente, en la parte de anexos se muestra capturas del funcionamiento del firewall y también la preparación del Firewall en forma Física.

CAPITULO V
DISCUSIÓN DE RESULTADOS

5.1. PRUEBA DEL SISTEMA

Como resultado de la implementación de Firewall para el control de servicios de internet en la filial Chanchamayo mediante la metodología Top-Down se obtiene los siguientes resultados:

5.1.1. Evaluación de resultados (Antes y Después)

Antes de implementar el firewall se tenía quejas por parte del personal administrativo, también constante pérdida de paquetes y una latencia muy alta y todo eso por el mal uso del servicio de internet, ahora que ya está implementado el Firewall se realizó la misma prueba en la misma hora punta en cada día con el objetivo de comparar las cantidades de quejas, Paquetes perdidos y Latencia del Antes y Después; se obtuvo los siguientes resultados:

Mes uno:

Tabla 10. Promedio Mes Uno Después de la Implementación

Mes Uno	Latencia	49.05
	Quejas	0
	Paquetes Perdidos	0.15

Autoría Propia

Mes dos:

Tabla 11. Promedio Mes Dos Después de la Implementación

Mes Dos	Latencia	49.55
	Quejas	0
	Paquetes Perdidos	0.25

Autoría Propia

Mes tres:

Tabla 12. Promedio Mes Tres Después de la Implementación

Mes Tres	Latencia	52.35
	Quejas	0
	Paquetes Perdidos	0.4

Autoría Propia

Para validar las hipotesis de la tesis se realizó la prueba de Kolmogorov-Smirnov de dos muestras con ayuda del Software IBM SPSS Statistics y se obtuvo los siguientes resultados.

Tabla 13. Prueba Kolmogorov-Smirnov

Estadísticos de prueba				
		Tiempo_Respuesta	Quejas	Paquetes_Perdidos
Máximas diferencias extremas	Absoluto	1,000	1,000	1,000
	Positivo	,000	,000	,000

	Negativo	-1,000	-1,000	-1,000
Z de Kolmogorov-Smirnov		5,477	5,477	5,477
Sig. asintótica(bilateral)		,000	,000	,000
a. Variable de agrupación: Pruebas				

Autoría Propia

Se puede observar que en los tres indicadores el nivel de significación en menor a 0.05, lo que significa que la distribución no es normal.

Como son variables dependientes y en la prueba de normalidad como resultado fue no normal se aplica una prueba de rangos con signo de Wilcoxon y se consiguieron los siguientes resultados.

Tabla 14. Prueba Wilcoxon - Rangos

Rangos				
		N	Rango promedio	Suma de rangos
Latencia_D - Latencia_A	Rangos negativos	60[a]	30,50	1830,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	60		
Quejas_D - Quejas_A	Rangos negativos	60[d]	30,50	1830,00
	Rangos positivos	0[e]	,00	,00
	Empates	0[f]		
	Total	60		

Paquetes_D - Paquetes_A	Rangos negativos	60[g]	30,50	1830,00
	Rangos positivos	0[h]	,00	,00
	Empates	0[i]		
	Total	60		
a. Latencia_D < Latencia_A				
b. Latencia_D > Latencia_A				
c. Latencia_D = Latencia_A				
d. Quejas_D < Quejas_A				
e. Quejas_D > Quejas_A				
f. Quejas_D = Quejas_A				
g. Paquetes_D < Paquetes_A				
h. Paquetes_D > Paquetes_A				
i. Paquetes_D = Paquetes_A				

Autoría Propia

Hipotesis Especificas:

Indicador: Latencia

H0: La utilización de la herramienta Wireshark mediante el análisis de tráfico permite identificar los protocolos más utilizados por los usuarios finales.

H1: La utilización de la herramienta Wireshark mediante el análisis de tráfico no permite identificar los protocolos más utilizados por los usuarios finales.

Indicador: Número de Quejas

H0: La implementación de reglas mediante la metodología Top Down Network Design permite habilitar los protocolos necesarios de acuerdo a la necesidad del usuario final.

H1: La implementación de reglas mediante la metodología Top Down Network Design no permite habilitar los protocolos necesarios de acuerdo a la necesidad del usuario final.

Indicador: Paquetes Perdidos

H0: La realización de pruebas de funcionalidad permite comprobar el correcto funcionamiento del firewall.

H1: La realización de pruebas de funcionalidad no permite comprobar el correcto funcionamiento del firewall.

Tabla 15. Prueba Wilcoxon - Estadístico

Estadísticos de prueba			
	Latencia_D - Latencia_A	Quejas_D - Quejas_A	Paquetes_D - Paquetes_A
Z	-6,736[b]	-6,768[b]	-6,742[b]
Sig. asintótica(bilateral)	,000	,000	,000
a. Prueba de rangos con signo de Wilcoxon			
b. Se basa en rangos positivos.			

Autoría Propia

Se concluyó que como el valor de p ((Sig. asintótica. (bilateral)) en los tres indicadores son menor a 0.05 rechazando la hipótesis nula y confirmando que la implementación de un Firewall mediante la metodología Top Down Network Design permite mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes.

5.2. DISCUSIÓN DE RESULTADOS

La tesis titulada APLICACIÓN DE UN FIREWALL CON IPTABLES EN LA EMPRESA CONEXIÓN LINUX SAC de la autoría de Joseph Frank Veliz Castañeda publicada por la UNIVERSIDAD NACIONAL HERMILIO VALDIZAN [1]

a. En la problemática de la tesis uno explica que tiene lentitud en la red LAN en la empresa Conexión Linux SAC en el caso de esta tesis también está presente el mismo problema y es porque en ambas tesis la red no está correctamente administrada.
b. La solución planteada en la tesis uno es un Firewall que controle la entrada, salida de paquetes y el bloque de puertos en esta tesis de la misma manera se implementó un firewall para controlar el uso del servicio de internet.
c. Finalmente, la tesis uno concluye en que había puertos vulnerables y según las políticas de seguridad de la empresa se diseñó la solución, en esta tesis se concluye que el firewall redujo en un 60% la lentitud de la red interna en la Filial Chanchamayo de la Universidad Peruana los Andes.

La tesis titulada IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA de la autoría de Castillo Palomino Renzo, Domínguez Chávez Miguel y Sulca Galarza Carlos publicada por la UNIVERSIDAD PERUANA DE LAS AMERICAS [2]

d. El investigador detalla existen vulnerabilidades en la red teniendo en cuenta la detección de ataques, en esta tesis también existe el riesgo de ataques externos a la red porque no se controla el acceso.

e. Implementa un firewall para que la clínica tenga seguridad perimetral y no exista intromisiones, en esta investigación de la misma manera se toma en cuenta la seguridad perimétrica de la red interna.

f. Finalmente concluye en que la seguridad es una tarea sumamente compleja y demandante, que se puede comparar con la conclusión de que se debe de manejar de forma correcta las tecnologías.

La tesis titulada EFECTO DE LA IMPLEMENTACIÓN DEL SISTEMA PFSENSE EN LA SEGURIDAD PERIMETRAL LÓGICA EN LOS SERVICIOS DE LA RED TRONCAL DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA de la autoría de Da Silva De Oliveira Diaz Renzo y silva Ledesma Jony publicada por la UNIVERSIDAD PRIVADA DE LA SELVA PERUANA [3]

a. Inicia detallando la existencia de un firewall lógico el cual era configurado remotamente, expresa la importancia de los datos académicos y la información personal de los usuarios hacen que sea necesaria la búsqueda de nuevas soluciones informáticas para resguardar la información de los servidores por ello implementa otro Firewall lógico (PfSense) buscando un efecto de cambio en la seguridad de la red que como indicador maneja el número de vulneraciones a la red perimetral, en la presente tesis no se toma indicador el número de vulnerabilidades porque está centrada más en la calidad del servicio de internet pero con esta misma solución desde el archivo “log” del “Shorewall” se puede encontrar el número de intentos de vulnerabilidad de la red interna de la Filial Chanchamayo.
b. Concluye comparando el antes y después de las vulnerabilidades en términos porcentuales consiguiendo un 91.83% de mejora, en esta tesis se podría comparar dicho valor con el número de quejas que se tiene que se reduce en 100%, porque después de la implementación el personal administrativo no presento queja alguna del servicio de internet.

La tesis titulada ESTUDIO DEL REDISEÑO DE LA RED Y ANALISIS COMPARATIVO DE SOFTWARE LIBRE DE ADMINISTRACION DE RED

APLICADAS AL CENTRO DE COMPUTO DE LA FACULTAD DE CIENCIAS ADMINISTRATIVAS de la autoría de Daniel Xavier Fiallo Moncayo publicada por la UNIVERSIDAD DE GUAYAQUIL [4]

a. Fiallo expresa que un gran problema para lograr un rediseño de una red exitoso son los limitados recursos financieros para llevar a cabo este proyecto. Este escenario es compartido en esta investigación por lo que se propuso una solución tecnológica basada en el uso de los activos bajo la administración del área de Tecnologías de Información de la organización, de manera que no se exija una inversión alta.
b. Concluye que a la empresa no le importa la herramienta a utilizar ni mucho menos la metodología; solamente ven la parte del costo y beneficio dejando a veces de lado un mejor sistema de reporteria. En esta tesis de la misma manera la casi nula inversión de la universidad se debe a que primero quieren ver si los resultados obtenidos son positivos y después de ahí recién invertir en mejorar, esta forma de trabajo de la universidad suele traer como consecuencia un funcionamiento básico pero que cumple con todos los requerimientos iniciales.

La tesis titulada IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SUPERVISÓN Y MONITOREO DE LA INFRAESTRUCTURA DE RED DE DATOS EN LA UNIVERSIDAD CENTROCCIDENTAL “LIZANDRO ALVARADO (UCLA)” de la autoría de Galindez Suarez Gloria publicada por la UNIVERSIDAD CENTROCCIDENTAL LIZANDRO ALVARADO [5]

a. Inicia con la afirmación de que las personas gastan más energía eléctrica con una conexión a internet deficiente y es porque se pasan más tiempo esperando que la pagina cargue que en realizar la tarea o investigación y lo realiza en zonas con conexión a internet deficiente, esta problemática es comparada con las quejas del personal administrativo que de la misma manera afirman que la velocidad deficiente trae como consecuencia retraso en sus labores diarias.

b. Concluye que reducir la velocidad de internet en las zonas donde los usuarios no utilizan de forma constante el internet y utilizarlas en las zonas donde los usuarios están en uso constante ayuda a mejorar la velocidad en un 66%.

La tesis titulada IMPLEMENTACIÓN DE UN FIREWALL SOBRE PLATAFORMA LINUX EN LA EMPRESA DE CONTABILIDAD ARMAS Y ASOCIADOS de la autoría de Juan Pablo Esparza Morocho publicada por la ESCUELA POLITECNICA NACIONAL DE ECUADOR [6]

a. Indica que la empresa tiene una conexión directa a internet sin restricciones y que se tiene el riesgo de sufrir intromisiones de virus y de ataques informáticos que ponen en riesgo la seguridad de la empresa, en esta tesis de la misma manera la universidad tenía a su personal administrativo con conexión directa a internet sin límites y traía como consecuencia lentitud en los sistemas de información de la universidad.
b. Concluye en que los procesos son transparentes para el usuario final, es decir que el usuario no se percatara que se realizan verificaciones de seguridad, en esta tesis de la misma manera el firewall guarda un registro de cada página web visitada por el personal administrativo y es totalmente transparente al usuario, el personal administrativo no tendrá idea de que toda su navegación será registrada así lo realice desde el modo incognito de cualquier navegador web.

CONCLUSIONES

1. Al identificar los protocolos más usados en la filial Chanchamayo mediante la metodología Top Down Network Design se mejoró la calidad del servicio de internet, con esta información se pudo determinar las páginas más visitadas por el personal administrativo.

2. Al implementar reglas para habilitar protocolos mediante la metodología Top Down Network Design se mejoró el control de accesos al servicio de internet en la Filial Chanchamayo, estas reglas definen las paginas necesarias a las que el personal administrativo y en los laboratorios de cómputo tendrán acceso.

3. Al realizar pruebas de funcionalidad al firewall mediante la metodología Top Down Network Design se evidencio la mejora de calidad del servicio de internet en la Filial Chanchamayo, en las pruebas realizadas se comprobó el bloqueo de páginas y el control de ancho de banda a cada usuario final.

4. Se evidencio que la implantación del firewall mediante la metodología Top Down Network Design en la Filial Chanchamayo de la Universidad Peruana los Andes, se agilizo el funcionamiento de los sistemas de información, redujo drásticamente las quejas y los paquetes perdidos son prácticamente nulos.

RECOMENDACIONES

1. Se recomienda utilizar el Firewall para seguir identificando protocolos usados por el personal administrativo y estudiantes en los laboratorios de cómputo con la finalidad de seguir bloqueando paginas no academias.

2. Se recomienda actualizar las reglas del Firewall constantemente de acuerdo a la necesidad del personal administrativo y los estudiantes de la Filial Chanchamayo.

3. Se recomienda realizar pruebas de control de ancho de banda a cada usuario de la filial Chanchamayo, con el objetivo de verificar el correcto acceso a las páginas web y a los sistemas de información de la Universidad.

4. Continuar la utilización del Firewall y darle mantenimiento adecuado para que las quejas y paquetes perdidos no aumenten y que los usuarios finales sigan trabajando con normalidad.

5. Contar con un proveedor de internet que garantice la disponibilidad del servicio las 24 horas, con la finalidad de que el servicio sea ininterrumpido y los usuarios finales no sean afectados.

REFERENCIAS BIBLIOGRÁFICAS

1. **Castañeda, Joseph Frank Veliz.** *Aplicación de un firewall con iptables en la empresa conexión linux sac.* s.l. : Universidad Nacional Hermilio Valdizan.

2. **Castillo Palomino, Renzo, Dominguez Chavez, Miguel y Sulca Galarza, Carlos.** *Implementación de un firewall TMG forefront para la seguridad .* s.l. : Universidad Peruana las Americas.

3. **Da Silva de Oliveira Diaz, Renzo y Silva Ledesma , Jony.** *Efecto de la implementación del sistema pfsense en la seguridad perimetral logica en los servicio de la red troncal de la universidad naciona de la amazonía peruana.* s.l. : Universidad Privada de la Selva Peruana.

4. **Moncayo, Daniel Xavier Fiallo.** *Estudio del rediseño de la red y el analisis comparativo de software libre de administración de red aplicadas al centro de computo de la facultad de ciencias administrativas.* s.l. : Universidad de Guayaquil.

5. **Suarez, Gloria Galindez.** *Implementación de un modelo de gestion de supervisión y monitoreo de la infraaestructura de la red de datos en la Universidad Centroccidental Lizandro Alvarado.* s.l. : Universidad Centroccidental Lisandro Alvarado.

6. **Morocho, Juan Pablo Esparza.** *Implementación de un Firewall sobre plataforma linux en la empresa de contabilidad armas y asociados.* s.l. : Escuela Politecnica Nacional de Ecuador.

7. **Guffabte, Naranjo Tania, Guffabte, Naranjo Fernando y Chavez, Hernandez Patricio.** *Investigación Cientifica.*

8. **Mallma, G Canto.** *Investigación Cientifica.* 2004.

9. **Arias, Frida G.** *EL PROYECTO DE INVESTIGACION.*

10. **Sampieri, Roberto Hernandez.** *METODOLOGIA DE LA INVESTIGACIÓN.*

ANEXOS

Anexo 1: Matriz de Consistencia

Tabla 16: Matriz de consistencia

TITULO	PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES
Implementación de un firewall para el control de servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes	**GENERAL:** ¿De qué manera el firewall permite mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes? **ESPECIFICOS:** ¿De qué manera el firewall permite optimizar la identificación de protocolos más usados en la red interna de la Filial Chanchamayo de la Universidad Peruana los Andes? ¿De qué manera el firewall permite mejorar el control de accesos a la red interna de la Filial Chanchamayo de la Universidad Peruana los Andes? ¿De qué manera el firewall permite agilizar el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes?	**GENERAL:** Implementar un Firewall mediante la metodología Top Down Network Design para mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes. **ESPECIFICOS:** Identificar los protocolos más usados mediante la metodología top Down Network Design para mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes. Implementar reglas para habilitar protocolos mediante la metodología Top Down Network Design para mejorar el control de accesos a la red interna de la Filial Chanchamayo de la Universidad Peruana los Andes. Realizar pruebas de funcionalidad mediante la metodología Top Down Network Design para agilizar el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes.	**GENERAL:** La implementación de un FIREWALL mediante la metodología Top Down Network Design permite mejorar la calidad del servicio de internet en la Filial Chanchamayo de la Universidad Peruana los Andes. **ESPECIFICOS:** La utilización de la herramienta Wireshark mediante el análisis de tráfico permite identificar los protocolos más utilizados por los usuarios finales en la Filial Chanchamayo de la Universidad Peruana los Andes. La implementación de reglas mediante la metodología Top Down Network Design permite mejorar el control de accesos según la necesidad del usuario final en la Filial Chanchamayo de la Universidad Peruana los Andes. La realización de pruebas de funcionalidad permite el correcto funcionamiento de los sistemas de información en la Filial Chanchamayo de la Universidad Peruana los Andes.	**VARIABLE INDEPENDIENTE** Implementación de un firewall. **VARIABLE DEPENDIENTE** Calidad del Servicio de Internet.

Anexo 2: Detalle de pruebas diarias a la Red Antes de la implementación del Firewall

Mes Número 01

Tabla 17: Pruebas Antes Mes 01

Mes 01	Día 1	Latencia	425ms
		Quejas	5
		Paquetes Perdidos	32
	Día 2	Latencia	526ms
		Quejas	6
		Paquetes Perdidos	35
	Día 3	Latencia	482ms
		Quejas	5
		Paquetes Perdidos	39
	Día 4	Latencia	524ms
		Quejas	4
		Paquetes Perdidos	38
	Día 5	Latencia	426ms
		Quejas	8
		Paquetes Perdidos	26
	Día 6	Latencia	489ms
		Quejas	8
		Paquetes Perdidos	42
	Día 7	Latencia	589ms
		Quejas	8
		Paquetes Perdidos	39
	Día 8	Latencia	389ms
		Quejas	4
		Paquetes Perdidos	25
	Día 9	Latencia	589ms
		Quejas	8
		Paquetes Perdidos	46
	Día 10	Latencia	489ms
		Quejas	6
		Paquetes Perdidos	38
	Día 11	Latencia	425ms
		Quejas	6
		Paquetes Perdidos	29
	Día 12	Latencia	506ms
		Quejas	7

Mes 01		Paquetes Perdidos	32
	Día 13	Latencia	398ms
		Quejas	4
		Paquetes Perdidos	27
	Día 14	Latencia	409ms
		Quejas	5
		Paquetes Perdidos	36
	Día 15	Latencia	528ms
		Quejas	8
		Paquetes Perdidos	45
	Día 16	Latencia	325ms
		Quejas	3
		Paquetes Perdidos	24
	Día 17	Latencia	469ms
		Quejas	6
		Paquetes Perdidos	41
	Día 18	Latencia	432ms
		Quejas	5
		Paquetes Perdidos	38
	Día 19	Latencia	395ms
		Quejas	4
		Paquetes Perdidos	21
	Día 20	Latencia	589ms
		Quejas	8
		Paquetes Perdidos	45

Autoría Propia

Mes Numero 2

Tabla 18: Pruebas Antes Mes 02

Mes 02	Día 1	Latencia	398ms
		Quejas	4
		Paquetes Perdidos	21
	Día 2	Latencia	501ms
		Quejas	5
		Paquetes Perdidos	31
	Día 3	Latencia	435ms
		Quejas	3
		Paquetes Perdidos	29

Mes 02	Día 4	Latencia	458ms
		Quejas	6
		Paquetes Perdidos	34
	Día 5	Latencia	528ms
		Quejas	8
		Paquetes Perdidos	35
	Día 6	Latencia	429ms
		Quejas	6
		Paquetes Perdidos	35
	Día 7	Latencia	524ms
		Quejas	6
		Paquetes Perdidos	34
	Día 8	Latencia	421ms
		Quejas	4
		Paquetes Perdidos	29
	Día 9	Latencia	485ms
		Quejas	7
		Paquetes Perdidos	38
	Día 10	Latencia	527ms
		Quejas	8
		Paquetes Perdidos	32
	Día 11	Latencia	428ms
		Quejas	6
		Paquetes Perdidos	34
	Día 12	Latencia	389ms
		Quejas	4
		Paquetes Perdidos	29
	Día 13	Latencia	629ms
		Quejas	8
		Paquetes Perdidos	45
	Día 14	Latencia	456ms
		Quejas	6
		Paquetes Perdidos	34
	Día 15	Latencia	489ms
		Quejas	7
		Paquetes Perdidos	38
	Día 16	Latencia	425ms
		Quejas	5
		Paquetes Perdidos	36

	Día 17	Latencia	459ms
		Quejas	5
		Paquetes Perdidos	40
	Día 18	Latencia	397ms
		Quejas	4
		Paquetes Perdidos	29
	Día 19	Latencia	487ms
		Quejas	5
		Paquetes Perdidos	39
	Día 20	Latencia	485
		Quejas	7
		Paquetes Perdidos	38

Autoría Propia

Mes Numero 03

Tabla 19: Pruebas Antes Mes 03

Mes 03	Día 1	Latencia	425ms
		Quejas	7
		Paquetes Perdidos	29
	Día 2	Latencia	489ms
		Quejas	6
		Paquetes Perdidos	27
	Día 3	Latencia	469ms
		Quejas	5
		Paquetes Perdidos	35
	Día 4	Latencia	387ms
		Quejas	4
		Paquetes Perdidos	28
	Día 5	Latencia	512ms
		Quejas	8
		Paquetes Perdidos	37
	Día 6	Latencia	378ms
		Quejas	4
		Paquetes Perdidos	29
	Día 7	Latencia	487ms
		Quejas	7
		Paquetes Perdidos	29
	Día 8	Latencia	528ms
		Quejas	6
		Paquetes Perdidos	38

Mes 03	Día 9	Latencia	524ms
		Quejas	8
		Paquetes Perdidos	29
	Día 10	Latencia	478ms
		Quejas	6
		Paquetes Perdidos	38
	Día 11	Latencia	456ms
		Quejas	5
		Paquetes Perdidos	36
	Día 12	Latencia	421ms
		Quejas	5
		Paquetes Perdidos	32
	Día 13	Latencia	587ms
		Quejas	6
		Paquetes Perdidos	39
	Día 14	Latencia	356ms
		Quejas	3
		Paquetes Perdidos	24
	Día 15	Latencia	521ms
		Quejas	7
		Paquetes Perdidos	34
	Día 16	Latencia	469ms
		Quejas	6
		Paquetes Perdidos	38
	Día 17	Latencia	416ms
		Quejas	4
		Paquetes Perdidos	34
	Día 18	Latencia	467ms
		Quejas	5
		Paquetes Perdidos	32
	Día 19	Latencia	501ms
		Quejas	6
		Paquetes Perdidos	46
	Día 20	Latencia	389ms
		Quejas	4
		Paquetes Perdidos	32

Autoría Propia

Anexo 3: Detalle de pruebas diarias a la Red Después de la implementación del Firewall

Mes Numero 01

Tabla 20: Pruebas Después Mes 01

Mes 01	Día 1	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 2	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	0
	Día 3	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 4	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 5	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	1
	Día 6	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	0
	Día 7	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 8	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	0
	Día 9	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	0
	Día 10	Latencia	50ms
		Quejas	0
		Paquetes Perdidos	0
	Día 11	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 12	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	0

Mes 01	Día 13	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 14	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	0
	Día 15	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 16	Latencia	50ms
		Quejas	0
		Paquetes Perdidos	1
	Día 17	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	0
	Día 18	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	0
	Día 19	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	0
	Día 20	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	1

Autoría Propia

Mes Numero 02

Tabla 21: Pruebas Después Mes 02

Mes 02	Día 1	Latencia	56ms
		Quejas	0
		Paquetes Perdidos	1
	Día 2	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 3	Latencia	54ms
		Quejas	0
		Paquetes Perdidos	0
	Día 4	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0

Mes 02	Día 5	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	1
	Día 6	Latencia	50ms
		Quejas	0
		Paquetes Perdidos	0
	Día 7	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 8	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	1
	Día 9	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	
	Día 10	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 11	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	1
	Día 12	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	1
	Día 13	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	0
	Día 14	Latencia	46ms
		Quejas	0
		Paquetes Perdidos	0
	Día 15	Latencia	50ms
		Quejas	0
		Paquetes Perdidos	0
	Día 16	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	0
	Día 17	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	1

Mes 02	Día 18	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	
	Día 19	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	
	Día 20	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	

Autoría Propia

Mes Numero 03

Tabla 22: Pruebas Después Mes 03

Mes 03	Día 1	Latencia	47ms
		Quejas	0
		Paquetes Perdidos	0
	Día 2	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	0
	Día 3	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	1
	Día 4	Latencia	56ms
		Quejas	0
		Paquetes Perdidos	1
	Día 5	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 6	Latencia	54ms
		Quejas	0
		Paquetes Perdidos	1
	Día 7	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	0
	Día 8	Latencia	50ms
		Quejas	0
		Paquetes Perdidos	0
	Día 9	Latencia	58ms
		Quejas	0
		Paquetes Perdidos	1

Mes 03	Día 10	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	0
	Día 11	Latencia	56ms
		Quejas	0
		Paquetes Perdidos	0
	Día 12	Latencia	52ms
		Quejas	0
		Paquetes Perdidos	0
	Día 13	Latencia	48ms
		Quejas	0
		Paquetes Perdidos	1
	Día 14	Latencia	54ms
		Quejas	0
		Paquetes Perdidos	1
	Día 15	Latencia	58ms
		Quejas	0
		Paquetes Perdidos	1
	Día 16	Latencia	56ms
		Quejas	0
		Paquetes Perdidos	0
	Día 17	Latencia	51ms
		Quejas	0
		Paquetes Perdidos	0
	Día 18	Latencia	53ms
		Quejas	0
		Paquetes Perdidos	0
	Día 19	Latencia	55ms
		Quejas	0
		Paquetes Perdidos	0
	Día 20	Latencia	49ms
		Quejas	0
		Paquetes Perdidos	1

Autoría Propia

Anexo 4: Validación de Instrumento de Investigación

VALIDEZ DEL INSTRUMENTO DE INVESTIGACION

JUICIO DE EXPERTO

TESIS: “Implementación de firewall para el control de servicio de internet en la filial Chanchamayo de la Universidad Peruana los Andes”

INVESTIGADOR: Bach. Jhon Carlos Joaquin Cajahuaringa

Señor especialista se le pide su colaboración para que luego de un análisis valide el instrumento de investigación utilizado marcando con un aspa el casillero que cree conveniente de acuerdo a su criterio y experiencia, indicando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

Experto 01:

Validación de instrumento de recolección de datos

Indicador: Latencia

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

Indicador: Número de Quejas

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento		X			
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

Indicador: Número de Paquetes Perdidos

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento		X			
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

RESULTADO DE VALORACION DE LOS INSTRUMENTOS: [ ]

Nombres y Apellidos Jowal Sigfrido Cabrera Padilla	DNI N° 21423306
Dirección Jr. Mandego Muñoz N°600 El Tambo	Teléfono/Celular 964256145
Título Profesional Ingeniero de Sistemas	

Grado Académico —
Mención —
Institución donde trabaja Universidad Peruana Los Andes

Fecha:.....

.....

DNI: 21423306

Experto 02:

Validación de instrumento de recolección de datos

Indicador: Latencia

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento		X			
Coherencia del instrumento		X			
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

Indicador: Número de Quejas

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento		X			
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento		X			

Indicador: Número de Paquetes Perdidos

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido		X			
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

RESULTADO DE VALORACION DE LOS INSTRUMENTOS: [ ]

Nombres y Apellidos	DNI N°
Henry George Maguiña Quispe	00447732
Dirección	Teléfono/Celular
Jr. Libertad 165 . Segundo piso	998017891
Título Profesional	
Ingeniero en Informática y Sistemas	

Grado Académico
Doctor
Mención
Ingeniería de Sistemas
Institución donde trabaja
Universidad Nacional del Centro del Perú

Fecha:.....

.....

DNI: 00447732

Experto 03:

Validación de instrumento de recolección de datos

Indicador: Latencia

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido	X				
Instrumento adecuado		X			
Pertinencia de uso del instrumento	X				

Indicador: Número de Quejas

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido		X			
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

Indicador: Número de Paquetes Perdidos

CRITERIOS	APRECIACIÓN CUALITATIVA				
	Muy Bueno	Bueno	Regular	Malo	Muy Malo
Suficiencia del instrumento	X				
Claridad del instrumento	X				
Coherencia del instrumento	X				
Relevancia del contenido	X				
Instrumento adecuado	X				
Pertinencia de uso del instrumento	X				

RESULTADO DE VALORACION DE LOS INSTRUMENTOS: [ ]

Nombres y Apellidos	DNI N°
José Luis Soto Medina.	47044972.
Dirección	Teléfono/Celular
Avenida La Linera # 222.- El Tambo.	963362730.
Título Profesional	
Ingeniero de Sistemas y Computación	

Grado Académico
—
Mención
—
Institución donde trabaja
Universidad Peruana Los Andes. – Oficina de Informática y sistemas

Fecha: 17-12-19.

.....

DNI: 47044972.

Anexo 5: Instrumentos de recolección de datos

Indicador: Latencia

Se utilizó la consola de Windows para obtener el tiempo de respuesta hacia el DNS de Google.

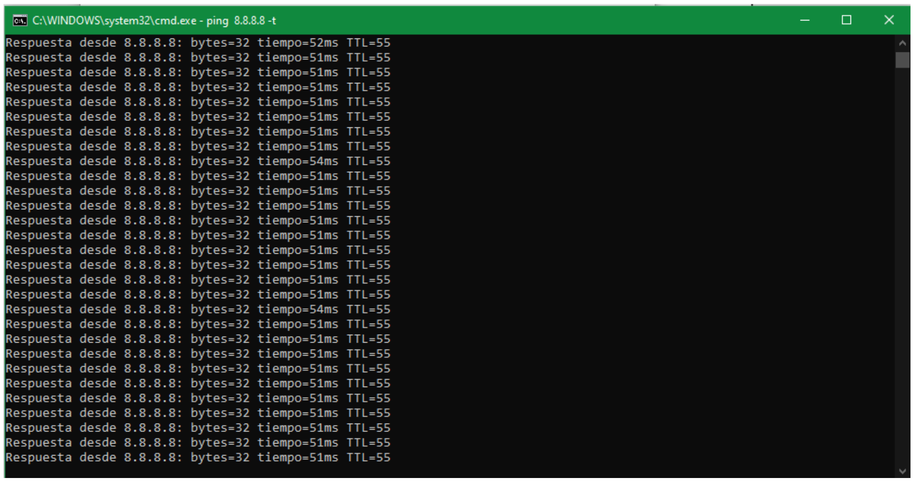

Figura 48. Consola de Windows, Autoría Propia

Indicador: Número de Quejas

Se utilizó una bitácora que se habilitaba en las pruebas donde el personal administrativo describía el motivo de la queja.

Figura 49. Bitácora, Autoría Propia

Indicador: Numero de Paquetes Perdidos

Se utilizó la herramienta Wireshark para realizar el conteo de paquetes perdidos.

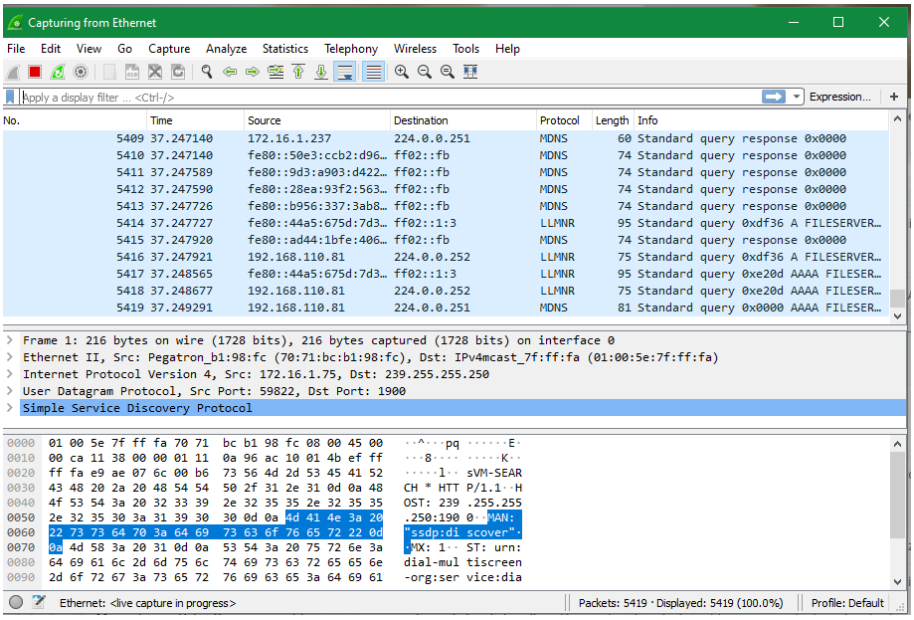

Figura 50. Wireshark, Autoría Propia

Anexo 6: Cronograma de Actividades

Tabla 23: Cronograma de Actividades

Actividades	Semanas							
	1-2	3-4	5	6	7	8-9	10-11	12
Determinar protocolos usados por la filial	X	X	X	X				
Determinar protocolos usados por Área	X	X	X	X				
Instalar y configurar el Sistema Operativo					X	X		
Instalar y configurar el Shorewall					X	X		
Instalar y configurar el Squid					X	X		
Crear reglas para habilitar protocolos						X	X	
Realizar pruebas de Funcionalidad						X	X	X

Anexo 7: Panel Fotográfico

Figura 51. Ordenamiento de Gabinete, Autoría Propia

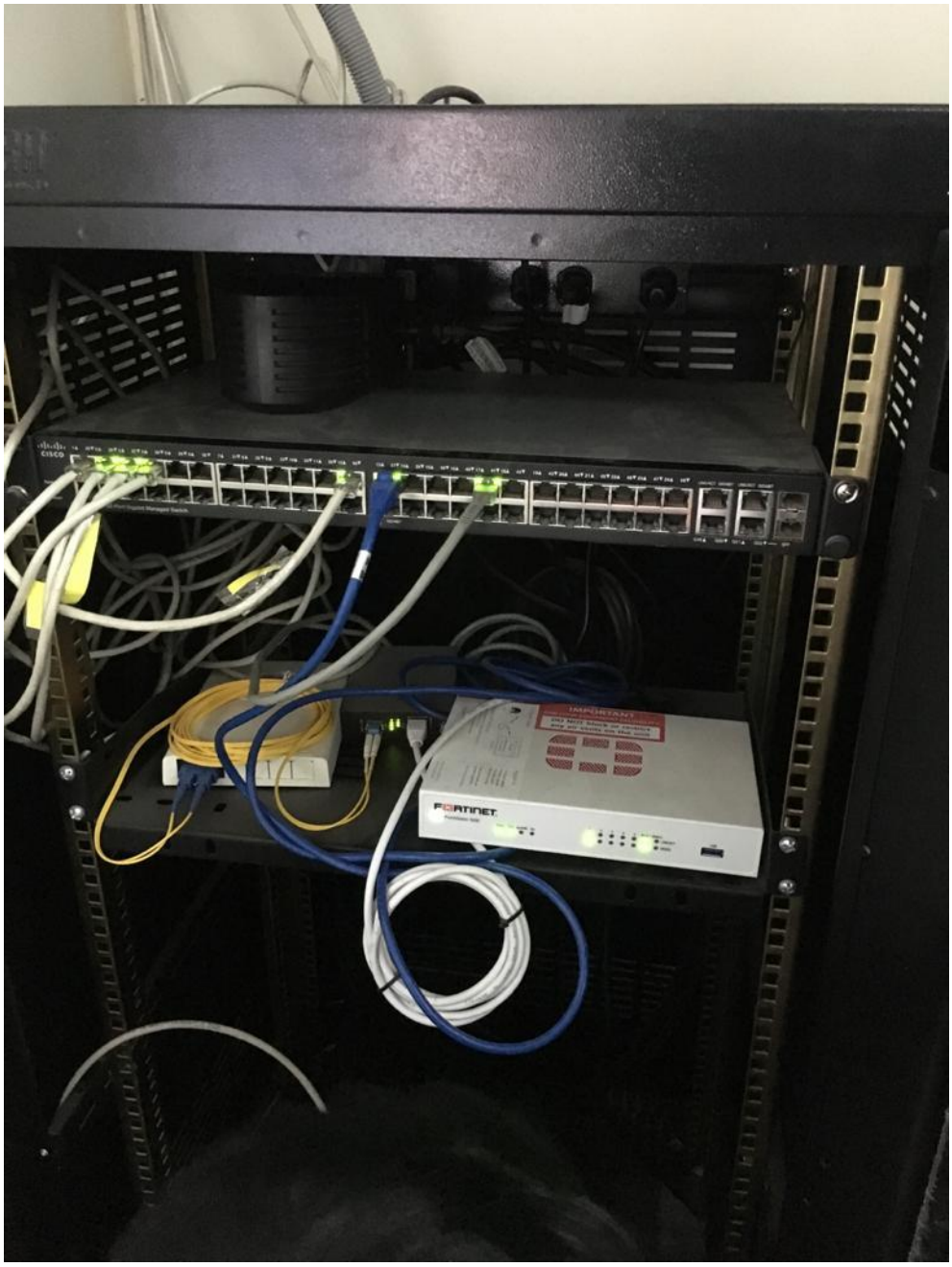

Figura 52. Gabinete de Red, Autoría Propia

Figura 53: Servidor y Firewall, Autoría Propia