UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE TELECOMUNICACIONES

DISEÑO DE FRONTERA DE RED EN SOFTWARE LIBRE PARA LA EMPRESA ABSORPELSA BAJO LA METODOLOGÍA Y ARQUITECTURA DE SEGURIDAD CISCO SAFE.

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Telecomunicaciones

AUTORES: DARWIN ALBERTO AVALOS SÁNCHEZ
ANDY SANTIAGO GUANOCHANGA GALLO

TUTOR: JUAN CARLOS DOMÍNGUEZ AYALA

Quito, Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

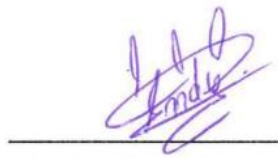
Nosotros, Darwin Alberto Avalos Sánchez documento de identificación N° 1722301817 y Andy Santiago Guanochanga Gallo con documento de identificación N° 1727027060; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro La Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 07 de septiembre del año 2022.

Atentamente,

Darwin Alberto Avalos Sánchez
1722301817



Andy Santiago Guanochanga Gallo
1727027060

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

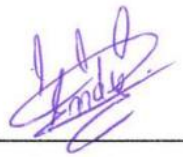
Nosotros, Darwin Alberto Avalos Sánchez con documento de identificación N° 1722301817 y Andy Santiago Guanochanga Gallo con documento de identificación N° 1727027060, expresamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico "Diseño de frontera de red en software libre para la empresa Absorpelsa bajo la metodología y arquitectura de seguridad Cisco Safe.", el cual ha sido desarrollado para optar por el título de: Ingenieros en Telecomunicaciones en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 07 de septiembre del año 2022.

Atentamente,

Darwin Alberto Avalos Sánchez
1722301817



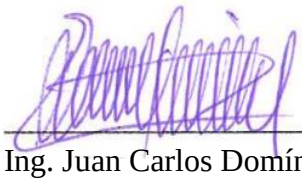
Andy Santiago Guanochanga Gallo
1727027060

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Carlos Domínguez Ayala con documento de identificación N° 1713195590, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO DE FRONTERA DE RED EN SOFTWARE LIBRE PARA LA EMPRESA ABSORPELSA BAJO LA METODOLOGÍA Y ARQUITECTURA DE SEGURIDAD CISCO SAFE. realizado por Darwin Alberto Ávalos Sánchez con documento de identificación N° 1722301817 y Andy Santiago Guanochanga Gallo con documento de identificación N° 1727027060, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 07 de septiembre del año 2022.

Atentamente,



Ing. Juan Carlos Domínguez Ayala, MSc
1713195590

DEDICATORIA

Dedico este proyecto de titulación a mis padres, Luis y Fanny, que siempre me apoyaron y creyeron en mí, acompañándome en mi jornada de crecimiento educativo, personal y profesional, sin importar las circunstancias o limitantes a lo largo del camino. También a todas las personas a lo largo de este viaje me brindaron su aporte, amistad, conocimiento y sobre todo me compartieron enseñanzas de vida que me llevaré por siempre. Afrontando juntos las experiencias agridulces pero enriquecedoras del día a día y estando en el momento y lugar correcto cuando más lo necesitaba.

Darwin Alberto Avalos Sánchez

Dedico este proyecto principalmente a mi madre que con tanto esfuerzo ha estado en los momentos más difíciles de mi vida, brindando fortaleza en cada paso que doy, el apoyo incondicional que supo sacarme de los momentos más difíciles y a mi abuela que con su alegría hace que cada reto se torne sencillo.

Andy Santiago Guanochanga Gallo

AGRADECIMIENTOS

A mis padres, que en cada etapa de mi vida me han manifestado su amor, entrega, sabiduría y apoyo incondicional, a mis buenos amigos y conocidos, incondicionales con aquel aliento de impulso, para lograr cosas más importantes y grandes cada instante que se tiene la oportunidad de empezar de nuevo, aprendiendo de los errores y experiencias pasadas, para tratar de ser cada día, un mejor profesional, amigo y ser humano.

A la Universidad Politécnica Salesiana, a los docentes y colaboradores que la conforman, por proporcióname las herramientas, conocimientos, técnicas y capacitación necesaria para afrontar la vida laboral y profesional.

A mi tutor, el Ing. Juan Carlos Domínguez, por ofrecer y compartir sus conocimientos y experiencias, para concluir con éxito el presente trabajo.

Darwin Alberto Avalos Sánchez

A mi madre, hermano y amigos que sin su confianza esto no lo hubiese logrado. A la Universidad Politécnica Salesiana que con sus maestros impartieron conocimientos que ahora son útiles para la vida profesional, de la misma forma a mi tutor de tesis Ing. Juan Carlos Domínguez, por conllevar este trabajo y tener paciencia en la enseñanza.

Andy Santiago Guanochanga Gallo

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

SIGLAS & ACRÓNIMOS

TI & TO: Tecnologías de la Información & Tecnología Operativa

PPDIOO: Planificación, Preparación, Diseño, Implementación, Operación, Optimización

VoIP: (Voice over Internet Protocol), Voz sobre IP

PIN: (Places in Network), Lugares en la red

QoS: (Quality of service), Calidad de servicio

MINTEL: Ministerio de Telecomunicaciones y de la Sociedad de la Información.

LATAM: Latinoamérica

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones

ISTR: Informe Anual de Seguridad de SYMANTEC

GCI: Global Cybersecurity Index

PYMES: Pequeñas Y Medianas Empresas

OSI: El modelo de interconexión de sistemas abiertos

TCP-IP: Protocolo de control de transmisión/Protocolo de Internet

PAN: Red de Área Personal

WAN: Red de Área Amplia

LAN: Red de Área Local

WLAN: Red de Área Local Inalámbrica

NAT: Traducción de direcciones

DNS: Sistema de Nombres de Dominio

VPN: Red Privada Virtual

DMZ: Zona Desmilitarizada

NGFW: Firewall de Nueva Generación

RESUMEN

El panorama de seguridad informática se encuentra en constante evolución desde mediados del siglo XX, esto se debe en gran parte, a los agigantados avances en las redes de computadores y el internet. El aumento de la capacidad informática, digitalización, y telecomunicaciones; mientras que el costo y consumo energético de los dispositivos disminuye, desencadenó en el surgimiento de nuevas tecnologías e introdujo conceptos en el ámbito empresarial de las tecnologías de la información y operativa. Hoy en día es inevitable vivir sin estos avances, y de alguna forma u otra la información personal y empresarial forma parte de estos sistemas, lo cual presenta un desafío continuo en la correspondiente ciencia de la ciberseguridad y diseño de redes.

El presente proyecto adopta como referencia el diseño de una red de frontera en software libre basándose en la arquitectura y metodología de desarrollo Cisco SAFE, se compone de seis capítulos, donde se obtuvo como producto final la simulación de una red convergente que se ajusta a los requisitos de seguridad, escalabilidad, alta disponibilidad y QoS.

La empresa Absorpelsa (Papeles Absorbentes S.A), se dedica a la fabricación y venta de papeles absorbentes de uso personal y limpieza, cartones grises, cartones (test Liner y liner Pad) y laminados naturales. El propósito del diseño de la red de frontera es contribuir, optimizar y repotenciar la infraestructura física y lógica, al emplear software de firewall open source PfSense, para garantizar la seguridad de la información a partir de la configuración de políticas de NGFW. Se aplicaron metodologías complementarias PPDIOO & Top-Down para el diseño del prototipo de red que aportaron un proceso sistemático para cada uno de los módulos de los que se distribuyó la red de la empresa.

Por último, se simuló la topología de frontera en programas especializados donde se verificó, optimizó y se documentó los resultados incorporando la implementación de proyectos de cableado estructurado y telefonía IP (VoIP); por último, se evalúa la factibilidad económica de este proyecto técnico.

Palabras Clave: Software libre, metodologías, escalabilidad, firewall NGFW, arquitecturas de red, Cisco SAFE.

ABSTRACT

The IT security landscape has been constantly developing since the middle of the 20th century, due in large part to the rapid advances in computer networks and the Internet. The increase in computing capacity, digitization, and telecommunications while the cost and energy consumption of devices decreased, triggered the emergence of modern technologies, and introduced concepts in the business field of information and operational technologies. Today, it is inevitable to live without these advances, and in one way or another, personal and business information is part of these systems, which presents a continuous challenge in the corresponding science of cybersecurity and network design.

The present project adopts as reference the design of a frontier network in free software based on the architecture and method of Cisco SAFE development, composed of six chapters, where the final product was obtained as the simulation of a converged network that meets the requirements of security, scalability, high availability and QoS. The company Absorpelsa S.A. is dedicated to manufacturing and selling absorbent papers for personal use and cleaning, gray cardboard, cardboard (test liner and liner Pad), and natural laminates. The purpose of the border network design is to contribute, optimize and enhance the physical and logical infrastructure, using PfSense open-source firewall software, to ensure the security of information from the configuration of NGFW policies. Complementary methodologies PPDIOO & Top-Down were applied to design the network prototype that supplied a systematic process for each of the modules in which the company's network was distributed.

Finally, the border topology was simulated in specialized programs where the results were verified, optimized, and documented, incorporating the implementation of structured cabling and IP telephony (VoIP) projects; finally, the economic feasibility of this technical project is evaluated.

Keywords: Free software, methodologies, scalability, NGFW firewall, network architectures, Cisco SAFE.

INTRODUCCIÓN

Actualmente en los entornos empresariales de las industrias de automatización, procesos y manufacturera. Las TI & TO convergen para establecer lo que se entiende como la industria 4.0. El presente Proyecto aborda seis capítulos del diseño de la red de frontera en software libre para la empresa Absorpelsa, en base de las mejores prácticas, fases metodológicas, herramientas y políticas; considerando las guías referenciales Cisco SAFE y se encuentra enfocado en el desarrollo de un entorno de red convergente que cumpla con las necesidades y requerimientos actuales y futuros de esta empresa manufacturera, de forma conjunta al configurar el appliance firewall open source para proveer de la seguridad, integridad, autenticidad, confidencialidad y alta disponibilidad de la información en todos los lugares de la red (PIN).

Para cumplir con los objetivos planteados a lo largo de este proyecto, se evalúa la situación inicial de red, se deducen las oportunidades, riesgos y desafíos que se encuentran.

La estructura del documento se compone de la siguiente manera:

En el capítulo uno se analizará la motivación del proyecto técnico, el planteamiento, formulación y justificación del problema de estudio, los objetivos y por último se describirá las metodologías a utilizarse en el proyecto. En el capítulo dos se detallará el marco conceptual, el cual contiene, conceptos técnicos acerca de las tecnologías de la información que comprende (redes computadores, metodologías de diseño de redes, modelos, protocolos de comunicación y topologías de red, dispositivos de NGFW)

El capítulo tres dará a conocer la situación inicial a partir del planteamiento de la situación geográfica, descripción de red actual, problemas detectados; requerimientos además del análisis de desafíos, oportunidades y pilares de apoyo para su etapa de diseño.

En el capítulo cuatro se elabora la propuesta del diseño de red de borde y seguridad perimetral, estableciendo la metodología empresarial SAFE y sus soluciones de diseño y simulación de topología física & lógica; mediante módulos, dimensionamiento de tráfico, redundancia, propuesta de (QoS) y distribución del equipo activo.

El capítulo cinco se elabora el análisis de costos de implementación y factibilidad económica. Últimamente, el capítulo seis desarrolla las conclusiones, recomendaciones consecuentes y trabajos futuros del proyecto técnico realizado.

CAPÍTULO 1
ANTECEDENTES

En este capítulo se analizará el planteamiento del problema, formulación de la justificación, se detallarán los objetivos y se describirá la metodología utilizada (elementos metodológicos, métodos y técnicas de investigación y las unidades de análisis). Además, se empleará como base de estudio: La visión general, guías de arquitecturas y diseños referenciales, a su vez recursos relacionados con el modelo de seguridad Cisco SAFE.

1.1 Antecedentes.

En la actualidad vivimos en un mundo que se encuentra cada día más digitalizado e interconectado, las TI cumplen un rol importante en las industrias del entretenimiento, información, telecomunicaciones, procesos de producción y manufacturera, entre muchas otras. Estas incorporan como parte sus tecnologías los procesos antes mencionados. La empresa Absorpelsa no es la excepción, pero evidencia puntos críticos a considerar, la ausencia de una robusta, adecuada y bien definida arquitectura de red, la falta de un servidor de seguridad óptimo; una ineficiente segmentación del cableado estructurado y puntos de conectividad inalámbrica. Esto limita su capacidad productiva, administrativa y sobre todo tecnológica; de modo que limita nuevas oportunidades de expansión, simplificación de procesos, ahorro tiempo y esfuerzo.

Bajo estos planteamientos se observa los potenciales riesgos, amenazas y vulnerabilidades, considerando que uno de los principales activos de las PYMES y grandes empresas es la información relacionada con sus procesos comerciales y operativos.

Otro de los problemas emergentes a considerar para la protección de estos activos, es la necesidad de software especializado, que por lo general incurre en costos de propiedad y licenciamiento, por esta razón el impacto de las tecnologías “open source” han sido relevantes desde sus inicios en la industria del software y en la sociedad en su conjunto, a fin de contar con algunos de sus principales beneficios, como son el menor o nulo costo, mejor rendimiento; sistema de apoyo y actualizaciones.

Como solución a la problemática en cuestión, se propone la simulación de red bajo la aproximación del diseño de la metodología y arquitectura modular Cisco SAFE, en software de código abierto para el appliance del firewall de nueva generación; esto se desarrolla de manera descentralizada. Al emprender un conjunto de fases metodológicas y actividades correspondientes a las guías y diseños empresariales publicados por Cisco, en consecuencia, se busca garantizar buenas prácticas de desarrollo y gestión de todos los lugares de red (PIN), entre otros puntos importantes especificados a lo largo del documento.

1.2 Formulación del problema

¿Cuáles serán los resultados, impacto y beneficios obtenidos a partir del rediseño y repotenciación de la infraestructura de red en hardware y software open source bajo el diseño de la metodología/arquitectura Cisco SAFE?

1.3 Importancia y Alcances.

La seguridad informática se ha transformado en una de las vitales preocupaciones de las instituciones, organizaciones y empresas. Ante amenazas en el entorno de red, de origen externo o interno, se vislumbra la necesidad intrínseca de reestructurar y repotenciar la infraestructura de hardware y software. Debido al gran incremento de incidentes de seguridad que existen en los gobiernos y empresas alrededor del globo, bajo diferentes tipos de ataques de la naturaleza de amenazas como lo son: la interrupción, interceptación, modificación y fabricación de la información.

Las estadísticas del informe de seguridad informática en LATAM y el mundo, además de tres investigaciones; el estudio global de (COMPARITECH, 2018), (ISTR, 2017) & (GCI, 2021). (*Informe de Seguridad Informática En Latam y El Mundo - Hacknoid*,.) Presentaron en sus informes los resultados en base a métricas y criterios de análisis relacionados con múltiples tipos de vulnerabilidades en la red de 60 y 157 países respectivamente, entonces resulta que, la región en su conjunto de naciones se posicionó como las menos ciberseguras en el ranking.

El pionero estudio de la Escuela Clark de la Universidad de Maryland, sostiene que cada 39 segundos hay un ciberataque, como promedio (*Hackers Attack Every 39 Seconds | 2017-02-10 | Security Magazine*, .) lo cual es alarmante cuando menos. De acuerdo con la

información proporcionada por el MINTEL Ecuador Ocupa Sexto Lugar En La Región, Según Índice de Ciberseguridad (Ministerio de Telecomunicaciones y de La Sociedad de La Información, 2017.) de 19 países de América Latina, está claro que existe una extensa cantidad de recursos y fuentes de empresas multinacionales de ciberseguridad como Kaspersky y ESET que sostienen la misma problemática.

Por esta razón, el presente proyecto técnico traerá consigo la protección de estos activos y servicios esenciales, bajo un marco que garantice un entorno de red interoperable; escalable, ciberseguro, etc. Lo cual contribuye como parte del proceso de transformación digital e incorporación de los fundamentos de la industria 4.0 dentro de la empresa.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar la red de frontera en software libre para la empresa ABSORPELSA bajo la metodología y arquitectura de seguridad Cisco SAFE.

1.4.2 Objetivos Específicos

- Definir la línea base de la infraestructura de la empresa ABSORPELSA para determinar la situación actual y condiciones de red.
- Diseñar la red de frontera basados en la arquitectura cisco SAFE del módulo de acceso a internet con características y parámetros que garanticen la resiliencia de la red
- Simular un prototipo de frontera con software para verificar las características de la nueva red diseñada.
- Evaluar la factibilidad económica del proyecto con el objeto de una posible implementación a futuro.

1.5 Metodología.

Para la realización del presente proyecto se tomó como metodología de investigación los siguientes elementos metodológicos, métodos y técnicas de investigación que se describen a continuación, los cuales permitieron verificar el cumplimiento de los

objetivos y actividades correspondientes al diseño de la red de frontera, cumpliendo con las recomendaciones de la documentación de la metodología/arquitectura cisco SAFE facilitando la abstracción de los resultados.

1.5.1 Elementos Metodológicos

- **Paradigma de investigación:** Positivista.
- **Tipo de Investigación:** Cuantitativa & Cualitativa.
- **Alcance:** Correlacional.

1.5.2 Métodos y técnicas de investigación

- **Método de Análisis. –** Se emprendió con la identificación de cada una de las acciones que llevaran a cabo con respecto a comparativa de características, funcionales, configuraciones, de los dispositivos de red, analizando las variables de análisis involucradas en los diferentes apartados.
- **Método de Síntesis. –** Se realizó un proceso de fundamentación para el desarrollo de la hipótesis fundada, tras un proceso de revisión y análisis de las metodologías/diseños referenciales de SAFE.
- **Método Experimental. –** Se lo aplicó por medio de las pruebas y simulaciones del prototipo de la red de frontera en software libre dentro del software especializado al reflejar la comparativa entre resultados deseados y obtenidos.
- **Método Inductivo. –** Permitió establecer relaciones entre las investigaciones anteriores para formular la línea base de la red en función de la realidad, puntos, parámetros, y características actuales de la empresa, y las acciones inmediatas y futuras que se puedan llegar a emprender.
- **Método Comparativo. –** Este método permitió comparar los datos obtenidos a partir del análisis del comportamiento y resultados esperados de la red bajo determinada topología física / lógica conexa con los conceptos especificados en el marco teórico.

1.5.3 Unidades de Análisis

Se considera como análisis general la red de datos en hardware y software de la empresa ABSORPELSA de la provincia de Pichincha cuidad de Quito, entre los cuales se puede mencionar la velocidad de conexión de internet, ancho de banda, transferencia de datos, capacidad de almacenamiento total, ocupado, disponible, entre otros apartados relacionados con los parámetros mínimos de QoS y análisis de factibilidad económica.

CAPÍTULO 2
MARCO CONCEPTUAL

En este capítulo se presenta el marco conceptual, el cual se compone de los conceptos técnicos que aglomera las tecnologías de la información y de cada uno de los elementos que componen la infraestructura de la red como: (redes computadores, modelos de comunicación, topologías de red, dispositivos de networking, firewall, calidad de servicio) a su vez el análisis de las metodologías PPDIOO y Módulos del Diseño Empresarial de Borde de Internet bajo las guías referenciales SAFE.

2.1 Metodología de diseño de Redes

Las metodologías de diseño de redes a través constante experimentación acumulada en su búsqueda de soluciones en los diversos ambientes de red, emplea métodos analíticos y tecnológicos con el objetivo de cumplir con los requerimientos determinados para su diseño de la red. Lo cual se consigue a partir de un conjunto de procedimientos flexibles, sistemáticos y estructurados, que ajusten a los objetivos planteados.

2.1.1 Metodología PPPDIO & Top-Down

Las metodologías empleadas en el proyecto técnico del diseño de red en software libre para la empresa Absorpelsa fueron seleccionadas en base a las metodologías empresariales ofrecidas por Cisco, considerando principalmente el modelo de seguridad para redes empresariales SAFE de Cisco además de incluir el establecimiento de excelentes prácticas de seguridad para la configuración de equipos, establecimiento de contraseñas y control de accesos a la red.

La metodología PPDIOO permite establecer el ciclo de vida de la red a partir del establecimiento de 6 fases detalladas en sus iniciales: (Preparación, Planificación Diseño, Implementación, Operación y Optimización) cada una se encarga de cumplir una función específica y mantienen una relación con su fase previa y siguiente.(*PPDIOO Stages > Cisco's PPDIOO Network Cycle | Cisco Press,* .)

La figura 2.1 representa gráficamente el diagrama de ciclos de la fase de vida de la red de esta metodología.

Figura 2.1 Fases Ciclo de Vida Metodología de diseño de red PPDIOO

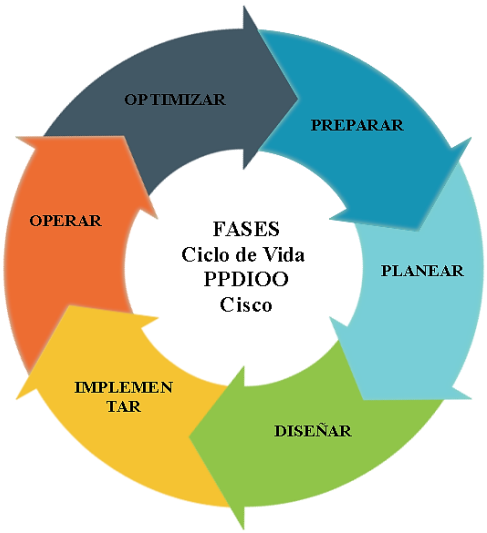


Diagrama de ciclos correspondiente a las seis fases del ciclo de vida de la metodología PPDIOO.
Elaborado por: Darwin Avalos y Andy Guanochanga. Fuente: Cisco SAFE

Las metodologías Top-Down, Botton-Up forman parte de dos enfoques de diseño de la red, cada una con sus desafíos, pros y contras; parten desde determinada capa del modelo OSI. La Tabla 2.1 establece las características, ventajas y desventajas de las metodologías Top-Down (de arriba hacia abajo) vs Botton-Up (de abajo hacia arriba), para seleccionar entre las direcciones de diseño que mejor adecue a los objetivos, requerimientos y necesidades de la empresa.(*Differences of Top-Down vs. Bottom-Up Approaches*, .)

Tabla 2.1 Tabla comparativa metodologías Top-Down vs Botton-Up.

Características,Ventajas & Desventajas	
Top-Down	**Bottom-Up**
Comienza desde la parte superior del modelo OSI Capa 7 (Aplicación)	Comienza desde la parte inferior del modelo OSI Capa 1 (Física)
Comienza estableciendo lo que necesita la organización	Es generalmente rápida en su configuración a comparacion de su contraparte
Provee de una imagen del panorama general tanto al cliente como al diseñador de la red	Aprovecha la experiencia previa
Las operaciones se modifican y completan según la dirigencia superior	Puede mejorar la infraestructura de networking dentro de la organización
Consume una cantidad de tiempo considerado	Pueden perderse algunos requerimientos de la organización en su diseño
Toma más tiempo durante su configuración	Alta probabilidad de fallo

Tabla comparativa de características, ventajas y desventajas de las metodologías Top-Down vs Botton-Up.
Elaborado por: Darwin Avalos y Andy Guanochanga. Fuente:()

La siguiente Figura 2.2 se encarga de indicar las cuatro fases correspondientes con la metodología Top-Down en su proceso de diseño y actividades correspondientes.

Figura 2.2 Fases Principales del diseño de la Metodología Top-Down

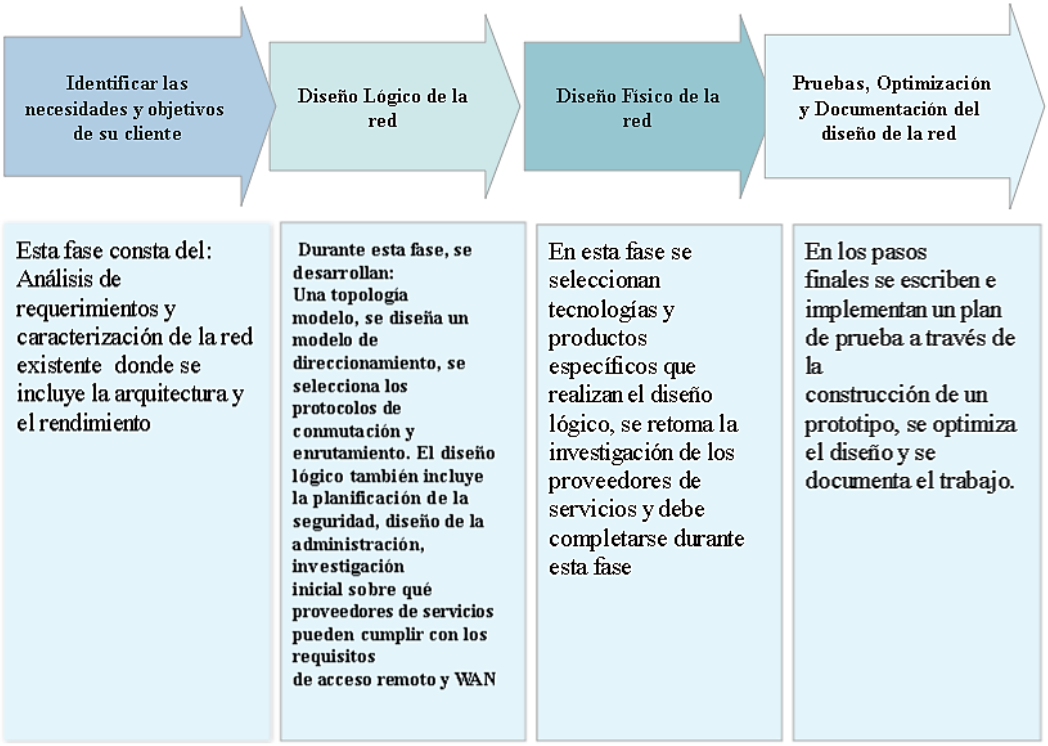


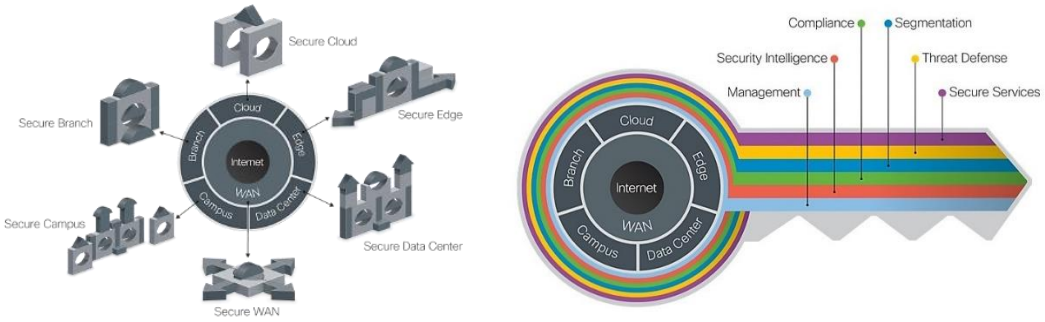
Diagrama de fases principales de proceso de la metodología de diseño de red Top-Down. Elaborado por: Darwin Avalos y Andy Guanochanga. Fuente: (Oppenheimer, s.f).

2.2 Modelo y Método de seguridad SAFE

SAFE es un modelo y método de seguridad utilizado para asegurar la continuidad del negocio. Se centra en las amenazas y mejores prácticas para su mitigación. Usando un modelo de referencia de seguridad, los desafíos de asegurar las funciones comerciales actuales se simplifican en un enfoque de bloques de construcción. El modelo incorpora mejores prácticas de seguridad actuales, arquitectura, discusiones y diseños probados en laboratorio. Los diseños validados por Cisco de SAFE abordan principios críticos de defensa en profundidad, modularidad, flexibilidad, disponibilidad y resiliencia de servicio cumplimiento de normativas, eficiencia operativa, implementación auditable y colaboración global. (*Cisco SAFE Reference Guide SAFE Overview Executive Summary*, p. 4) Algunas de las principales características de este modelo empresarial se centran en proveer diferentes módulos especializados denominados Secure Cloud, Edge, Data Center, WAN, Campus, Branch; que en función del modelo arquitectónico organizacional

consideran los requisitos de industrias específicas, sus objetivos, ver Figura 2.3 arquitectura modular de adecuación a su propuesta diseño de ambientes de red empresarial, la llave de Cisco simplifica el proceso de entendimiento de los módulos y dominios involucrados.

Figura 2.3 Módulos lugares en la red de acuerdo con la Key de Cisco SAFE



Módulos PIN lugares en la red de acuerdo con la Key de Cisco SAFE, Fuente: (Cisco SAFE,2014)

2.2.1 Módulos de diseño empresarial Cisco

Entre los principales módulos que conforman la arquitectura empresarial de Cisco el módulo Enterprise Edge conformado por SP Edge y el Internet Access, Remote Access & VPN, WAN Site-to-Site VPN, encargados de brindar conectividad entre el ISP y los demás módulos por métodos propios de cada submódulo; sobresalen entre los más importantes con los que se encuentran estructurados dentro de una arquitectura empresarial. Debido a que es donde la red, establece la conexión la red de área extensa, la internet. Necesario para acceder a diferentes servicios FTP, DNS, SMTP; HTTP, aplicaciones y sitios web orientados al usuario en cuestión.(SAFE Overview Guide, 2018)

El módulo de Campus contiene a nivel de infraestructura, una composición de dispositivos conectados formados de muchas LANs segmentadas generalmente se delimitan a un área geográfica fija o abarcan diferentes departamentos de un área empresarial.

El módulo empresarial remoto llega a subdividirse en Enterprise Branch, Data Center, Teleworkers son los encargados de proveer servicios de terminación de acceso remoto para aplicaciones como VPNs, teletrabajo al garantizar la interconexión con diferentes sucursales o ISPs externos.

2.3 Redes de computadores

Con el avance inmensurable de las TICs se requiere que los dispositivos puedan recolectar, almacenar, transportar y procesar datos. Las redes de computadoras son un conjunto de dispositivos autónomos (es decir con CPU y memoria) separados pero interconectados a través de un mecanismo para compartir recursos, hardware o software entre los usuarios que se encuentren en la red. Cada computadora se denomina host. Para la conexión se puede realizar mediante los medios de transmisión: cableado coaxial, UTP, fibra óptica o inalámbricamente como microondas, bluetooth, infrarrojo o satélites de comunicaciones.

El sistema de redes es escalable es decir se adapta a los requerimientos computacionales, tienen mayor flexibilidad en cuanto al aumento o disminución de equipos, permiten que los recursos se encuentren disponibles y accesibles para los usuarios. Todas estas características se rigen a protocolos y estándares internacionales.

Según las necesidades de cada compañía la aplicación de las redes de computadoras puede tener distintos criterios como la transmisión de datos, tamaño y topología.

2.3.1 Transmisión de datos

- **Redes punto a punto. –** Conexión directa entre dos sistemas, enlace entre terminal y el ordenador o entre pares de computadoras. No se requiere direccionamiento para la transmisión de datos ya que existe un solo canal no compartido.
- **Redes multipunto. –** También denominado redes de broadcast (radiodifusión) es un enlace simultaneo entre computadoras o un computador central y varios nodos en donde se requiere un direccionamiento para distinguir el destinatario.

2.3.2 Tipos de redes de acuerdo con el tamaño

- **PAN. –** Una red de área personal, permite al usuario interactuar con dispositivos en un rango corto, típicamente 10 metros. Una laptop, una impresora, equipos de audio y video se interconectan entre sí a través de cableado físico o por vía inalámbrica (WPAN) centralizando el control en una sola persona.
- **LAN. –** Las redes de área local se basan en conexiones en entornos pequeños como de oficina, hogar o empresas con una cantidad mínima de computadores. Comparten recursos por un medio físico (cable UTP) el cual no debe exceder una distancia de 100 metros. como estándar desde el punto de los servidores, router o switch a los usuarios.

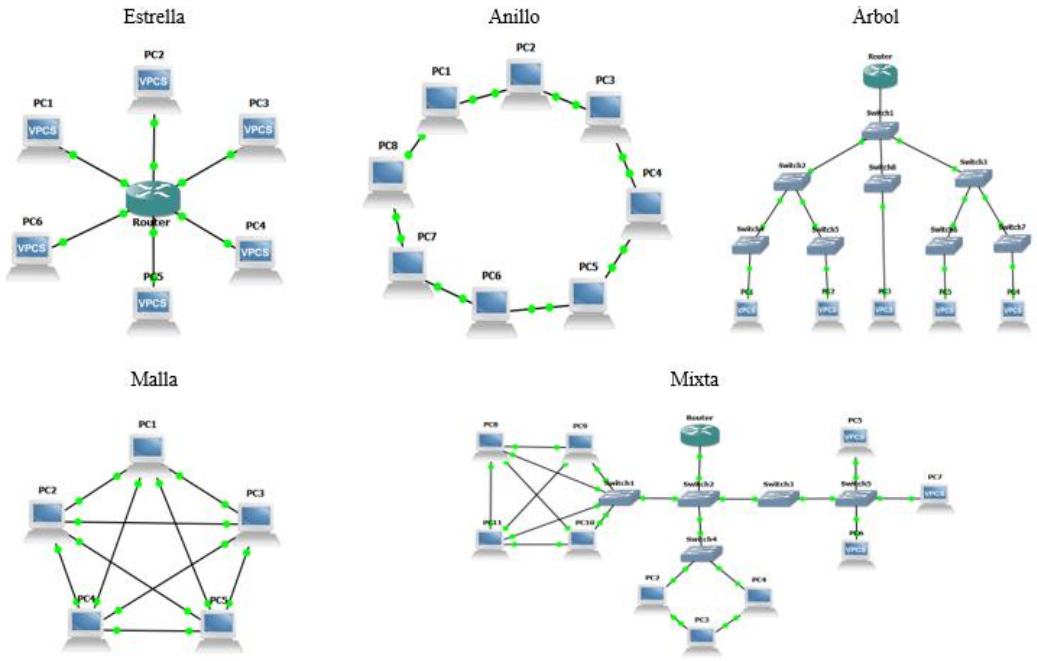
- **WAN. –** Una red de área extendida facilita la comunicación en áreas con mayor extensión geográfica. Para acceder a este servicio se requiere de un proveedor debido a que se enlazan con una central nacional o internacional a través de cableado de cobre o fibra óptica denominada bucle local o "última milla".
- **MAN. –** La red de área metropolitana comunica nodos remotos como si fueran una red LAN permitiendo así la conexión por fibra óptica alquilados por proveedores de internet (ISP) entre ciudades, pueblos o cualquier zona metropolitana.

2.3.3 Tipos de topología de red

- **Estrella. –** Los dispositivos van conectados a un componente principal, switch, en donde el control de tráfico se centraliza. Cada PC es independiente, al presentarse un problema de red no afecta a los demás dispositivos, y la detección de este se facilita. La funcionalidad cae estrictamente en el switch central requiriendo así más capacidad en el software como ancho de banda, puertos lógicos, velocidad de navegación, memoria, etc., en caso de no cumplir con las necesidades de la arquitectura genera en ocasiones un cuello de botella para la entrada y salida en los nodos.
- **Anillo. –** Se caracteriza por conectar los dispositivos en un anillo físico en forma bidireccional cerrado, para que la información circule se debe transferir la información a los nodos adyacentes. Esta arquitectura es muy sólida por lo que varias veces entra en problemas con los usuarios, pero al tener gran cantidad de repetidores en cada nodo ralentiza la velocidad en la red. Provee de acceso equitativo para todos los equipos y la falla de uno altera en su totalidad la conexión.
- **Árbol. –** Desde un nodo central se ramifican conexiones hacia los nodos. Los dispositivos de las distintas ramas se tornan los principales de manera análoga similar a la topología en estrella por lo que debe duplicar y enlazar las líneas adyacentes. La información de la red es en jerarquía.
- **Malla. –** Cada nodo tienen conexión directa (física) con los demás nodos, creando una conexión redundante, es decir que si un enlace tiene problemas en la red la información sigue circulando por varias rutas en la red sin incidentes. Este tipo de topología es muy confiable, pero a su vez es una de las más costosas.
- **Mixta. –** Cuando en una arquitectura se demanda un aumento de dispositivos, requerimientos específicos o seguridad la red debe ser modificada creando topologías mixtas. Son aquellas que unen topologías de estrella, anillo, malla, árbol, etc., combinando las ventajas de cada una, pero con una complejidad en la configuración.

En una topología hibrida, al fallar un equipo no debe afectar la circulación de la información. (O & P, 2012)

Figura 2.4 Tipos de Topología de Red.



Tipos de topologías lógicas de red: estrella, anillo, árbol, malla, mixta. Elaborado por: Darwin Avalos y Andy Guanochanga.

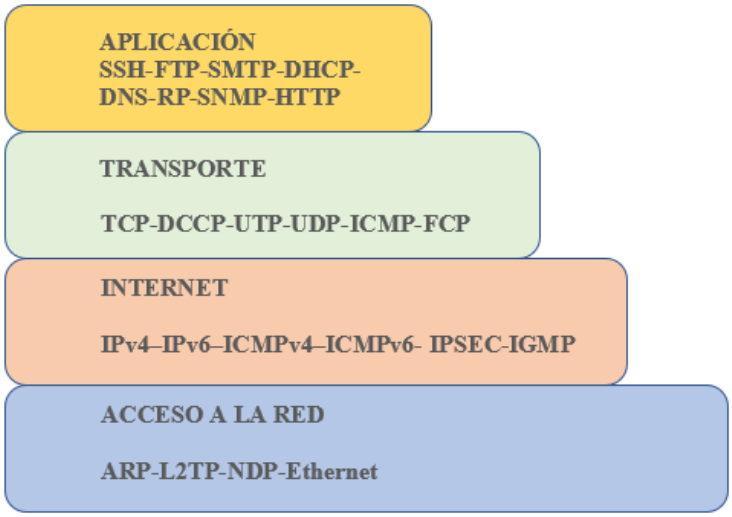
2.4 Modelos y Protocolos en procesos de transmisión de información.

El intercambio de información entre dispositivos se requiere de procedimientos complejos como protocolos para que exista comunicación. Estas normas de diálogo se realizan de manera jerárquica y subdivide cada tarea en capas. Los protocolos permiten la comunicación eficaz identificando el emisor y el receptor, el idioma y la gramática en común, velocidad de entrega y recepción, requerimientos de confirmación o acuse de recibo, codificación y encapsulamiento de mensajes. La unión de distintos protocolos conforma suites y estándares para trabajar de forma conjunta y brindar servicios de comunicación en la red. TCP-IP y OSI son ejemplos de estándares abiertos y disponibles para que se pueda implementar tanto en hardware como software. (Cisco, 2019)

2.4.1 Modelo TCP-IP

El Protocolo para el Control de Transmisión / Protocolo de Internet está compuesto por 4 capas con funciones y aspectos específicos brindando un servicio a la capa superior. (McGraw-Hill, 2012)

Figura 2.5 Modelo de Protocolo TCP-IP | Servicios dentro de Capa



Capas del Protocolo para el Control de Transmisión / Protocolo de Internet: aplicación, transporte internet, acceso a la red. Elaborado por: Darwin Avalos y Andy Guanochanga.

- **Capa de Aplicación**. - Esta comprendida por procesos y aplicaciones que permiten interactuar y transmitir datos con la capa inferior, Capa de Transporte. Tiene servicios para el correo electrónico, transferencia de archivos y conexión remota. (UNIVERSIDAD DE COLIMA, 2019)
- **Capa de Transporte**. - Distintos protocolos como TCP permiten la conexión de un extremo al otro con la capacidad de detectar errores y corregirlos. Para reducir la cantidad de información de la cabecera se encarga UDP y así gana rapidez en la transmisión de datos.

  En esta capa se requiere conexión entre los hosts y se negocia el intercambio en tres segmentos de datos: host A envía un segmento de sincronización (SYN) al host B con un identificador numérico, el host B ubica el host A y responde con un segmento de confirmación (ACK) para iniciar la transmisión de datos. Al recibir el host A esta confirmación, este envía nuevamente al host B un ACK con la primera trama de datos e inicia la transmisión.
- **Capa de Internet**. - El protocolo IP es quien interactúa con las capas superiores, cuenta con varias versiones debido al aumento de equipos en la red. IPv4 al tener

un número limitado de host se ve la necesidad de implementación de IPv6, ya que tiene mayor cantidad de hosts para el direccionamiento. Un paquete accede a la capa de red y se propaga con formato de datagrama, consulta la dirección de origen y destino, posteriormente envía los datos de un equipo al otro.

- **Capa de Acceso a la Red**. – Este nivel es donde se encapsula los datagramas del protocolo IP para ser transmitida en tramas por la red Ethernet, de la misma forma se asocia las direcciones de cada equipo (IP física) con los adaptadores de red (NIC). (UNIVERSIDAD DE COLIMA, 2019)

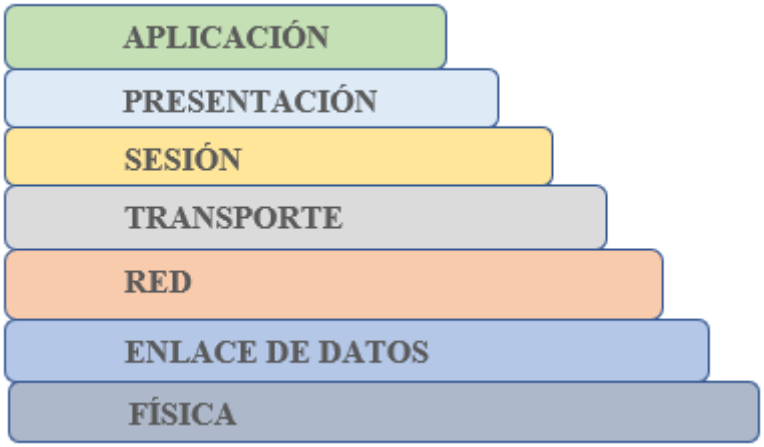
2.4.2 Modelo OSI

El Protocolo de Interconexión de Sistema Abierto ver Figura 2.6, es un conjunto de estándares que de acuerdo con el nivel de capa aseguran la interoperabilidad y compatibilidad entre los equipos en la red. Este modelo divide la comunicación en capas, permite la comunicación de hardware y software de distintos fabricantes, las configuraciones de una capa no afectan a las demás por lo que la comunicación se torna rápida.(Osi, 1984)

- **Capa de Aplicación**. – La capa más próxima al usuario, proporciona los servicios de red a las aplicaciones como hojas de cálculo, terminales bancarias y procesamiento de texto, etc. Establece disponibilidad, comunicación, sincroniza la compatibilidad semántica y recupera errores para la integridad de datos.
- **Capa de Presentación**. – Traduce los formatos de los datos en uno en común y garantiza el entendimiento de la capa de aplicación de un equipo con la de otro.
- **Capa de Sesión**. – Ofrece una eficiente transferencia de datos, clase de servicio y un registro de problemas de las capas inferiores (presentación, aplicación), a la vez establece y finaliza la sesión entre los hosts de la red que se comunican.
- **Capa de Transporte**. – Segmenta los datos que van a transmitirse desde el host emisor y los reensambla como una corriente de datos en el host receptor. Esta capa proporciona confiabilidad en el transporte y establece una conexión fiable manteniendo una calidad de servicio al usuario.
- **Capa de Red**. – Selecciona la mejor ruta para que la información llegue al host destino atravesando distintos sistemas intermedios (subredes).

- **Capa de Enlace de Datos**. – Provee el tránsito de datos a través de un enlace físico, a la vez direcciona y entrega de manera ordenada las tramas controlando así los errores y el flujo de la red.
- **Capa Física**. – Relaciona especificaciones mecánicas, eléctricas y funcionales para mantener un enlace físico con los dispositivos finales. Características como el voltaje, velocidad y distancias de transmisión física, conectores y otras propiedades semejantes son definidos en esta capa.(Osi, 1984)

Figura 2.6 Capas Modelo OSI



Capas del Protocolo de Interconexión de Sistema Abierto: aplicación, presentación, sesión, transporte, red, enlace de datos, física. Elaborado por: Darwin Avalos y Andy Guanochanga.

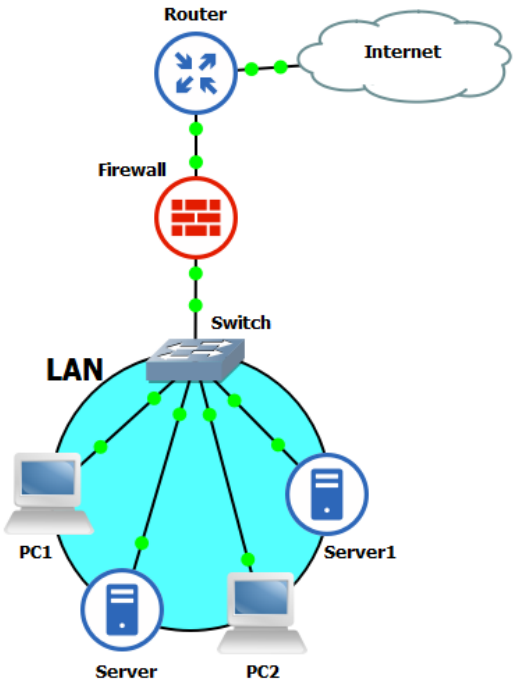
2.5 Firewalls & NGFW

Las compañías cada vez automatizan, documentan y gestionan sus actividades en una red local. Al tener varios servicios en nube o en servidores físicos asume riegos de hacking, accesos no autorizados desde el exterior o solo buscan perjudicar a la entidad; es por esta razón que, la implementación de un sistema que garantice la defensa de todos los elementos de la red interna como información, hardware y software es necesaria.

Los firewalls o cortafuegos son herramientas para la seguridad entre la red privada y el internet administrando todos los accesos posibles de entrada y salida, lo cual al encontrar un intruso rechaza la petición y bloquea el acceso a la red interna o por el contrario acepta y tiene ingreso para navegar. Para que cumpla su función se requiere que todo el tráfico atraviese por el mismo para inspeccionar todos los paquetes. Se puede administrar niveles de confianza para que ciertos usuarios puedan acceder a recursos que el administrador disponga.(Sampaio & Bernardino, 2017)

La nueva generación de firewall (Next Generation Firewall, NGFW) utilizan filtrados para la aceptación de paquetes tanto dinámicos como estáticos, soporta VPN y así garantiza las conexiones desde el Internet y la red interna. La diferencia entre un firewall normal y los NGFW es que filtra de acuerdo con las aplicaciones, tiene capacidad de bloquear programas malignos, incorporan antivirus y herramientas que ayudan a proteger la red.(Esparza Morocho, 2013)

Figura 2.7 Firewall de frontera



Firewall de frontera, filtrado de paquetes entre Internet y la red LAN. Elaborado por: Darwin Avalos y Andy Guanochanga.

Existen firewalls licenciados, se requiere de un partner para implementarlos por lo que el costo económico dependerá de los servicios que requiera la red interna o gratuitos (Open-Source) que pueden ser configurados por el departamento encargado de las TICs de la compañía. (¿Qué Es Un next Generation Firewall ,2014 .)

2.5.1 Firewalls Open-Source

El código abierto o software libre permite a pequeñas y medianas empresas (Pyme) adquirir servicios gratuitos con acceso al código fuente para que los usuarios puedan configurar, buscar bugs en el código y obtener el mayor rendimiento. Cada firewall Open Source contempla distintas formas de bloquear paquetes o permite instalar aplicaciones que ayudan a la seguridad perimetral, por lo que son viables para la

implementación, algunos de los más usados son Lire, SmoothWall con una interfaz amigable, OPN Sense y PfSense basados FreeBSD, entre otros. (Cuenca, 2016)

2.5.2 PfSense

Es un firewall de código abierto que se encarga de la seguridad del tráfico en la red de frontera de las Pyme garantizando la protección de información con pocos recursos de CPU. Cuenta con módulos y aplicaciones que administran los paquetes que entran y salen de la red interna hacia el Internet impidiendo que usuarios no autorizados filtren datos o modifiquen accesos de la red a su conveniencia.

Para la instalación de PfSense no requiere de hardware costoso, es necesario un servidor o un ordenador con mínimo de dos tarjetas de red para la WAN y LAN, memoria RAM de acuerdo con las necesidades internas y de las aplicaciones que se instalaran. Las actualizaciones de este firewall son frecuentes y al ser un software con código abierto el soporte puede atribuirse a distintos desarrolladores.

Dentro de sus principales funciones por defecto constituyen el Firewall, Network Address Translation (NAT), Servidores (DNS, PPPoE, DHCP, VPN [Opt: IPsec, Open VPN y en PPTP]); creación DMZ (Zona Militar Desmilitarizada), Balanceo de carga multi-WAN, Portal cautivo, Wi-Fi AP, destacando su capacidad backup gestión rápida. (*SEAQ - Expertos En Pfsense Para Colombia - Open Source,* .)

CAPÍTULO 3
SITUACIÓN INICIAL

En el presente capítulo se determina la situación inicial a partir del planteamiento de la situación geográfica, descripción de red actual, problemas de diagnóstico y pronóstico detectados; requerimientos además del análisis de desafíos, brechas, oportunidades y pilares de apoyo para su etapa de diseño.

3.1 Situación geográfica

Como parte del proceso de la definición de la línea base de la infraestructura se establece los datos geográficos de la empresa ABSORPELSA S.A. Figura 3.1. Ubicada al sur de la ciudad de Quito, en la Av. Pedro Vicente Maldonado S26-183 y, Quito 170139. Los principales límites al Norte la Industria Omega C.A, Sur Escuela Fiscal Francisco Javier Salazar, Este Supermercado AKI y Oeste Quebrada el Conde; cuenta con un área del terreno 2424.4475 m^2 el cual se compone de áreas: administrativas (gerencia general, administrativo financiero, talento humano, contabilidad, sistemas, tesorería, compras y ventas) y de producción (Tissue, Alta Densidad, laboratorio de calidad, bodega de repuestos y materia prima, mantenimiento, bodega de despacho, mercadeo y seguridad industrial).Revisar diagrama estructural departamentos, Anexo 1.

Figura 3.1 Fachada empresa propuesta de desarrollo proyecto técnico

Vista principal de empresa Absorpelsa. Fuente: (Absorpelsa,2022)

3.2 Descripción de Red Actual

El Data center ubicado en el área de sistemas del departamento administrativo provee de la conectividad a las demás áreas mencionadas en la situación geográfica, a través de 6

Racks tipo pared (7 UR) distribuidos con equipos de networking adicionales; el área principal del centro de datos de la empresa consta de una infraestructura de dispositivos de networking y redes posicionadas en dos racks de suelo de (45 UR); la red de la empresa Absorpelsa consta de un diseño topológico en forma de árbol.

El levantamiento de la información de los dispositivos activos en la red previo-propuesta del proyecto revisar en la Tabla 3.1, Figura 3.2 y Anexo 10.

Tabla 3.1 Dispositivos Activos en la red actual de la empresa Absorpelsa.

Dispositivos & Función	Marca & Modelo	N° de Puertos & Capa	Versión -Stds
Switch Core	Cisco Business -250 Series	24 | Capa 3	3.1.1.7
Switch	Cisco Business -350 Series	24 | Capa 2	3.1.1.7
Switch	Cisco Catalyst - 2960 Series	8 | Capa 2	15.2(7)E5
Switch	HP - J9561A	24 | Capa 2	Unk
Switch	Cisco Catalyst - 2960 Series	8 | Capa 2	15.2(7)E5
Switch	Cisco Catalyst - 2960 Series	8 | Capa 2	15.2(7)E5
Router Provider	HP - A-MSR 900 JF8124	4 | Capa 3	Unk
Trancievers	10/100Mbps Multi-mode Multimedia Converter - MC100CM	1. 100M SC/UPC port 2. 100M RJ45 port (Auto MDI/MDIX) | Capa 1	IEEE 802.3, IEEE 802.3u, IEEE 802.3x
MikroTik Firewall	MikroTik - RouterOs RB951G-2HND	5 | Capa 3 & 4	6.49.6
Clouds Storage	Western Digital Corp-HJ937D & TYPOLE	1 | Capa 1	Unk

Tabla en detalle de dispositivos activos en la infraestructura de red actual. Elaborado por: Darwin Avalos y Andy Guanochanga.

En relación con el direccionamiento de la red solo emplean la versión IPv4, va a parte de la red 192.168.1.0/24, de esta manera se proveía del despacho de direcciones a los diferentes dispositivos que componían la red LAN por medio del DHCP. Las configuraciones de IPs de los servidores a partir de la red 10.10.10.0/24 se observa en la Tabla 3.2.

En primera instancia el proyecto de cableado estructurado remitir al Anexo 1,2,3; inició casi de forma simultánea con las actividades iniciales del desarrollo del proyecto técnico, por lo cual se lo considero incluir como parte del proyecto interdisciplinario.

Al emplear el software Advanced Ip Scanner se realizó el barrido completo de los dispositivos conectados a la red, incluyendo los equipos activos e inactivos, ver Anexo 4, con el propósito de saber la cantidad de dispositivos que pertenecen al dominio de la empresa y diferenciarlos entre el resto de los dispositivos.

Tabla 3.2 Segmentación IPv4 Servidores de la Empresa.

SERVIDOR FÍSICO	SERVIDOR VIRTUAL	SERVICIOS	IP
SRVDOM		DNS/ DHCP/ ACTIVE DIRECTORY	10.10.10.1
SRVEXC2016		CORREO ELECTRÓNICO E-MAIL EMPRESARIAL	10.10.10.3
SRVABS	SRVAC	SISTEMA CONTABLE/ SQL SERVER/ HYPER V	10.10.10.7
	SRVWSUS	ACTUALIZACIONES MICROSOFT	10.10.10.14
	SRVTERMINAL		10.10.10.18
SRVSTORAGE		ALMACENAMIENTO / IMPRESORAS	10.10.10.15
SRVMBA3		VMWARE	10.10.10.17
	ANTISPAM	ANTISPAM	10.10.10.21
SRVBCK	BACKUP	RESPALDOS DE SEGURIDAD	10.10.10.32

Tabla de segmentos VLAN red actual. Elaborado por: Darwin Avalos y Andy Guanochanga.

Figura 3.2 Distribución equipos de networking Data Center

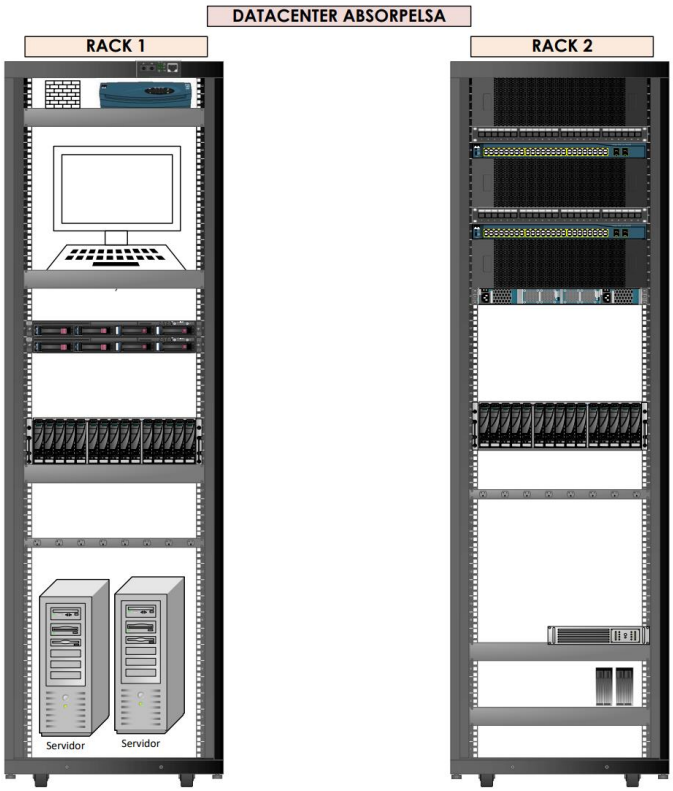


Diagrama en Visio distribución de infraestructura red actual de equipos. Elaborado por: Darwin Avalos y Andy Guanochanga.

En relación con las especificaciones de hardware con las que cuentan los dispositivos como Pc y laptops en la empresa el almacenamiento es de 500GB para el usuario promedio con un porcentaje de alrededor del 53 %, 240GB para el 37% y 1TB en el 10%. La memoria RAM en estos dispositivos está entre 3 y 4GB. Las especificaciones de los

dispositivos que cumplen las funciones de servidores en la red de la empresa observar en la Tabla 3.3.

Tabla 3.3 Tabla especificaciones hardware de servidores de la empresa.

SERVIDOR FÍSICO	SO	MODELO DEL SISTEMA	VERSION	RAM	MEMORIA DISPONIBLE	PROCESADOR
SRVDOM	Microsoft Windows Server 2016 Std.	HP Z400 WORKSTATION	10.0.14393 compilacion 14393	8 GB	439 gb de 465 gb	Procesador Intel(R) Xeon(R) CPU W3520 @ 2.67GHz, 2661 Mhz, 4 procesadores principales, 4 procesadores lógicos
SRVEXC2016	Microsoft Windows Server 2016 Std.	ProLiant DL380 G5	HP P56,2008/01/24	20GB	C:224 gb de 136gb D: 262 gb de 465gb F:350gb de 1.81 TB	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz, 2000 Mhz, 4 procesadores principales, 4 procesadores lógicos
SRVABS	Microsoft Windows Server 2012 R2 Std.	ProLiant DL380 G5	HP P56,2015/08/16	27 GB	C: 16.6gb de 136 gb D: 43.7gb de 465 gb E:107 gb de 558 gb G: 480 gb de 558 gb I92 gb de de 558gb C: 120 gb de 148gb	Intel64 Family 6 Moderl 23 Stepping 6 GenuineIntel 2000 Mhz
SRVSTORAGE	Microsoft Windows Server 2016 Std.	Virtual Machine	American Megatrends Inc. 090006, 2012/05/23	4 GB	D:20.2 gb de 249 gb	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz, 2000 Mhz, 2 procesadores principales, 2 procesadores lógicos
SRVMBA3 & SRVBCK	Microsoft Windows Server 2016 Std.	ProLiant DL360 Gen9	HP P89, 2016/09/13	32GB	C:66.6 gb de 278 gb	Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz, 2197 Mhz, 10 procesadores principales, 20 procesadores lógicos

Tabla en detalle de dispositivos servidores activos en la infraestructura. Elaborado por: Darwin Avalos y Andy Guanochanga.

La mejora del rendimiento y políticas seguridad de los módulos o zonas de red de la empresa se han configurado a lo largo del siguiente capítulo la VLANs en el Switch de Core y Appliance NGWF, las configuraciones de las listas de control de acceso ACLs, bloqueo de páginas web, puertos y comunicación InterVLAN, etc.

La Tabla 3.4 se encarga de presentar los tipos de dispositivos finales, puntos de red, puntos de acceso la red; presentes y disponibles en las diferentes áreas de la que conforma la empresa.

Tabla 3.4 Tabla especificaciones de puntos de red y conectividad.

Área de Trabajo	Puntos de Red	PCs	Laptops	Impresoras	Biométricos	Wireless	Puntos libres
Exteriores (Garita & Bodega Despacho)	2	0	0	0	1	0	1
Planta Baja (Administración)	15	2	8	1	1	1	2
Planta Baja (Seguridad Industrial)	8	1	6	1	0	0	0
Planta Alta (Gerencia & Financiero)	4	0	3	0	0	1	0
Plata Alta (Contabilidad & Sala de Reuniones)	6	0	4	0	0	1	1
Plata Alta (Mantenimiento)	24	2	4	1	0	1	16
Laboratorio & Materia Prima	8	3	1		0	1	3
Mercadeo & Bodega Repuestos	8	1	0	0	0	1	6
Tissue (Administración)	10	1	4	0	1	1	3
Total:	85	10	30	3	3	7	32

Tabla en detalle de tipo dispositivos finales activos, puntos de red, puntos de acceso; presentes y disponibles. Elaborado por: Darwin Avalos y Andy Guanochanga.

3.3 Diagnóstico & Pronóstico de problemas detectados.

El proceso de análisis de la red en su situación inicial, el diagnóstico y pronóstico de los problemas encontrados en el lugar de estudio, donde se va a enfocar la propuesta de diseño del proyecto, toma en consideración el eje central, sus objetivos, la orientación

empresarial, los procesos involucrados en cada una de sus etapas y los puntos críticos de riesgo de Absorpelsa S.A, con lo cual, se llegó a determinar lo expuesto en los siguientes subapartados.

3.3.1 Diagnóstico de Problemas en la red.

En la empresa Absorpelsa S.A debido a su infraestructura topológica actual (física y lógica) de red y datos, además de las políticas de seguridad que manejan, se llega a evidenciar importantes falencias en su funcionamiento y estabilidad entre las que se pueden destacar.

- El diseño de red empresarial no contempla un sistema fiable acorde con las necesidades actuales de la empresa en relación con la seguridad, arquitectura y escalabilidad.
- La arquitectura presente es plana y no considera el control de acceso a usuarios externos o invitados.
- Los recursos de hardware del firewall actual en la empresa Mikrotik no consideran la escalabilidad de la red, esto se debe al incremento de dispositivos adicionales como teléfonos IP y el incremento de los Access Point.
- Es indispensable configurar políticas de calidad de servicio para la priorización del tráfico en el flujo entrada y salida de la red de acuerdo con el nivel de requerimientos de las aplicaciones.
- No se ha establecido un conjunto de componentes para los dispositivos de red de frontera.
- En necesario aplicar nuevas políticas de seguridad preventivas como: bloqueo de tráfico en específico, puertos, control de listas de acceso, y filtrado de contenido.
- Se debe establecer prioridades el ancho de banda en base al Bw provisto por el ISP para ofrecer a los usuarios una navegación y conexión a internet estable.
- La UPS no cuenta con suficiente potencial eléctrico para garantizar la alimentación continua los equipos TI.
- La distribución de las GPO del dominio de la red actual no se encuentran correctamente delimitadas y configuradas acorde a la jerarquía de tipos de usuario que conforma la red.
- Máquinas ajenas al entorno empresarial pueden ingresar a la red sin autorización, provocando excesivo broadcast, y evidenciando potenciales brechas de seguridad de la información ante amenazas de programas malignos.

- Usuarios sin restricción de accesos pueden ingresar de forma inalámbrica y acceder a los servidores.
- Poca seguridad en la red inalámbrica, la cual puede ser violada por cualquier persona con conocimientos mínimos de informática.
- Las políticas de contraseñas no cumplen con parámetros de seguridad en relación con su composición de números, caracteres especiales, mayúsculas y minúsculas.
- Existen APs que son añadidos a conveniencia del usuario sin previa notificación al administrador de la red.
- Los switches ocupados en ciertos departamentos en la arquitectura de la red no son administrables y sin suficiente capacidad de abastecimiento para los dispositivos finales.
- Las contraseñas dentro del Active Directory no se renuevan periódicamente para los usuarios.
- No cuentan con el licenciamiento oficial en diversas aplicaciones que usan para sus procesos y áreas de trabajo.
- El cableado estructural limita las capacidades de velocidad en transmisión de dato en la red.
- El servidor encargado del antispam no se encuentra actualizado y no tiene la renovación de licencia.
- Ciertos equipos no cuentan con las especificaciones necesarias en CPU, RAM para su correcto funcionamiento.
- Falta de capacitación en la concientización de diferentes y peligrosos ataques como phishing, ransomware, etc.

3.3.2 Pronóstico de Problemas de la red.

- Dado que se prevé la expansión de la empresa se avecina el incremento de usuarios; lo cual acarrea, en aumentar equipos TI, conexiones, puntos de acceso, entre otros. Lo que desencadena en problemas de estabilidad al no contar con una infraestructura que soporte dicho aumento, los problemas inmediatos se relacionan con la disminución de la velocidad de conexión de internet, control de la seguridad informática de los datos,
- Al ser una topología que, en su arquitectura, presenta limitaciones en su rendimiento, configuración y mantenimiento, además que si el dispositivo de

mayor jerarquía o nivel falla, los que le siguen también presentaran complicaciones.

- De acuerdo con las características del dispositivo que trabaja como firewall, el consumo de estos recursos físicos va a aumentar constantemente, a medida que se incorporan dispositivos adicionales; lo cual genera una sobrecarga de la capacidad de rendimiento de la CPU, que puede elevar la temperatura en un sobrecalentamiento y a su vez, generar desfases en el sistema; como última consecuencia terminar en fallos electrónicos.
- Al no instituir pilares de QoS no se llega a cumplir los requerimientos de Bw en los departamentos, donde es indispensable cumplir con requisitos de ancho de banda estándar necesarios para la navegación, uso de servicios y aplicaciones web.
- Al no establecer de forma adecuada los nuevos segmentos de infraestructura de la red, no es posible configurar políticas de control de acceso adecuadas al bloque del cual forman parte.
- No tener el balanceo de carga y distribución de ancho de banda, termina en un tráfico de red entrante desproporcional entre varios destinos, lo cual no cumpliría con el apartado alta disponibilidad de servicios a través de redes de datos.
- Al no haber un control del ingreso de equipos y conexiones, aumenta la inseguridad en relación confidencialidad de los usuarios que conforman la red de área local.
- No contar con contraseñas robustas y de renovación mensual por lo mínimo, para los dispositivos de enrutamiento, finales y puntos de acceso inalámbrico; eleva latentemente las posibilidades de accesos indeseados por intrusos con motivaciones negativas y perjudiciales.
- Sin tener la posibilidad de administrar los dispositivos de capa 2 & 3, es difícil establecer parámetros de QoS y VLANs con una configuración alta de políticas de seguridad.
- En caso de usar software modificado, desactualizado o sin mantenimiento, aumenta las brechas de seguridad, al posiblemente tener archivos maliciosos que se insertan o ejecutan desde algún apartado oculto a simple vista durante su proceso de instalación o parche.

- Un medio de transmisión que no soporte un elevado ancho de banda afecta el factor velocidad/distancia, lo cual se refleja en un rendimiento bajo dentro de los servicios aplicativos de la empresa.
- A pesar de tener la topología y políticas de seguridad más sofisticadas, los métodos de vulneración de seguridad también se aprovechan de un minucioso análisis y herramientas, los cuales, se aprovechan de técnicas como la ingeniería social, suplantación de identidad, etc. El saber identificar las principales características de estos tipos de ataques si bien es una tarea menos complicada para el administrador de los sistemas TI, la responsabilidad no puede recaer solamente sobre ellos, lo cual puede estar fuera de su control al tener que estar a cargo de una creciente cantidad de usuarios que conformen la red.

3.3.3 Análisis Integral de Requerimientos de Red Actual-Futura

El análisis de los problemas, requerimientos, brechas y pilares de apoyo encontradas a partir del diagnóstico y pronóstico, al establecer la línea base de la situación inicial, en complemento con simulaciones elaboradas en Packet Tracer, GNS3 para el establecimiento de segmentación y distribución de red IPv4, también al discurrir los requerimientos de ancho de banda, tráfico de aplicaciones, parámetros mínimos calidad de servicios indispensables y políticas de configuración.

Las siguientes ideas son de principal consideración al emprender soluciones que capaces de optimizar y corregir los problemas detectados:

- El proyecto de cableado estructurado abarca alrededor del 85 % de los puntos de red de los que compone la red, cubrir con el otro 15% es importante para poder modificar de conectividad de equipos alrededor del ambiente de red empresarial.
- Se debe considerar el ancho de banda por parte del ISP debe ser incrementado y considerar la incorporación de un segundo ISP garantizar la redundancia de la conectividad al Internet y alta disponibilidad de los servicios de aplicativos.
- Es necesario delimitar y actualizar los usuarios que conforman el dominio de red y dispositivos que la componen, realizando un papel específico de control e identificación; alrededor de 45 personas componen el dominio, útil al identificar posibles ingresos o conexiones indeseadas de usuarios externos.
- La reconfiguración de los dispositivos involucrados en la nueva arquitectura a efectuar en la red, en su segmentación de red e interconexión lógica y física.

- El manejo de los requisitos de la QoS debe considerar la información recomendada para las diferentes aplicaciones de servicios, y evaluación necesidad del usuario.
- El remplazo de las funcionalidades y configuraciones del dispositivo encargado de las funciones Firewall Mikrotik por el Appliance de la propuesta se debe efectuar bajo las premisas de rediseño de los demás apartados.

CAPÍTULO 4
PROPUESTA DEL DISEÑO DE LA RED DE BORDE

En el capítulo cuatro se elabora la propuesta del diseño de red de borde y seguridad perimetral, estableciendo la metodología empresarial SAFE y sus soluciones de diseño y simulación de topología física & lógica; mediante la aproximación de módulos empresariales, dimensionamiento de tráfico de aplicaciones, redundancia, propuesta de (QoS) y distribución del equipo activo, además de los resultados de configuración y simulación del prototipo propuesto.

4.1 Diseño de la Solución

De acuerdo con las metodologías de desarrollo de redes ya establecidas en el marco teórico y en continuidad con el ciclo de vida del diseño de las metodologías Top-Down, PPDDIO y Cisco SAFE para el proyecto técnico se adecuan a la realidad empresarial. Al establecer una correlación entre las primeras metodologías se simplifica las etapas de desarrollo del proyecto en tres fases que agrupan en pares las fases de la Figura 4.1; las actividades correspondientes se cubrirán a lo largo del capítulo.(Safe_wp1, 2000.)

Al partir desde la capa superior del modelo OSI de acuerdo con el diseño de la metodología Top-Down en la Figura 4.1, resulta como la metodología adecuada para el diseño considerando los puntos planteados antes, capaz de proporcionar una arquitectura que satisfaga los requerimientos actuales y se encuentre lo suficientemente bien estructurada para considerar futuras implementaciones. Para el diseño de la topología de red propuesta como prototipo del proyecto, se aplica las metodologías PPDIOO, Top-Down, de forma conjunta con el modelo y método de seguridad empresarial Cisco SAFE.

Figura 4.1 Capas del Modelo OSI para aplicación metodología Top-Down.

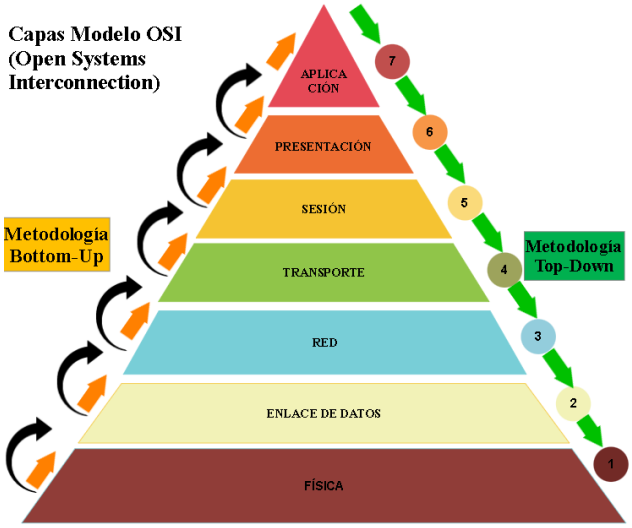


Diagrama de pirámide correspondiente a las capas del modelo OSI para proceso de diseño Top-Down. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.2 Selección del NGFW y Servidor de virtualización

Entre las opciones de NGFW Open Source considerados dentro de la comparativa se tomó en cuenta los Appliances PfSense, ClearOS e IPFire, por medio la asignación puntaciones en un rango de 0: [Insatisfactorio], 5: [Poco satisfactorio] y 10: [Extremadamente satisfactorio], de acuerdo con las funciones/características indagadas de las fuentes respectivas.

Tabla 4.1 Tabla comparativa de características selección de Appliance open-source

	pfSense	ClearOS	IpFire
Costo	10	0	0
Balance Wan y Failover	10	10	10
Alta Disponibilidad	0	10	10
Routing	10	10	10
Firewall	10	10	10
Filtrado Web	10	10	10
AP Inalámbrico	10	0	10
Antispam	0	10	10
Antivirus	10	10	10
Portal Cutivo	10	0	10
Servidor DHCP	10	10	10
Servidor Open VPN	10	10	10
Cliente Open VPN	10	10	10
Servidor DNS	10	10	10
IPsec VPN	10	10	10
Servidor Radius	10	10	10
Servidor PPTP	10	10	0
Servidor SSH	10	10	10
Servidor Web	10	10	0
Servidor File	10	10	10
Servidor SMTP	0	10	0
Servidor VoIP	10	0	10
TOTAL	**190**	180	180

Tabla comparativa de Appliances NGFW. Elaborado por: Darwin Avalos y Andy Guanochanga.

A partir de los resultados comparados en la Tabla 4.1 destaca PfSense con un puntaje de 190/220, por lo cual se lo adopta como firewall NGFW de software libre en el diseño del prototipo de red frontera, al cumplir con las características, funciones y capacidades necesarias en la red de la empresa.

Al escoger el servidor encargado de virtualizar el firewall perimetral se considera los requerimientos en base de las especificaciones mínimas para ambientes de red de baja escala ver Tabla 4.2 y Anexo 5 detalla la comparativa entre los parámetros de las opciones indagadas. En pro de satisfacer las necesidades actuales y futuras de la red; por medio del análisis comparativo de dos potenciales dispositivos de servidor que destacan por sobrepasar en sus características.

Tabla 4.2 Especificaciones mínimas del servidor de virtualización PfSense

Nº	Requisitos Mínimos de Instalación
1	CPU compatible con amd64 (x86-64) de 64 bits
2	Frecuencia del Procesador superior 600Mhz
3	Memoria superior 1 GB de RAM
4	Unidad de disco superior a 8 GB (SSD, HDD, etc.)
5	Compatibilidad para una o más tarjetas de interfaz de red.
6	Unidad USB de arranque o unidad óptica de alta capacidad (DVD o BD) para la instalación inicial
7	Conectividad a internet

Tabla de requisitos mínimos para instalación del Appliance PfSense. Elaborado por: Darwin Avalos y Andy Guanochanga. Fuente: (Netgate Docs.)

Tabla 4.3 Tabla de Puntos de Selección de Servidor para PfSense.

Modelo / Características	Cisco UCS C220 M4	HPE ProLiant DL 160 Gen10	DELL EMC PowerEdge R740
Conexiones de Red	0	10	10
Factor Forma	10	10	10
Procesador	5	10	10
RAM	10	10	10
Ranuras de Memoria	0	10	10
Ranuras de Expansión	5	5	10
Disco Duro	5	10	5
Alimentación	5	10	5
Precio	0	10	5
TOTAL	40	**85**	75

Tabla puntuaciones, comparativa para servidor de almacenamiento del Appliance PfSense. Elaborado por: Darwin Avalos y Andy Guanochanga.

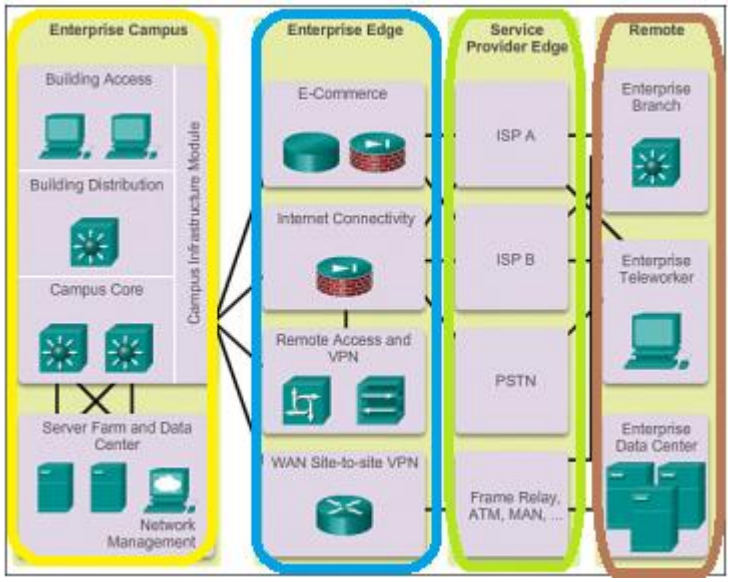
4.3 Diseño Prototipo de red frontera

Los equipos que conforman determinadas áreas o módulos funcionales en la arquitectura modular de SAFE se encuentran establecidos con la premisa de integración de las capas, manteniendo el nivel jerárquico, para presentar alta redundancia, convergencia, velocidad en redes empresariales grandes y escalables. Bajo la guía de una aportación académica previa(Cahueñas & Lizarzabaru,2019), se ajusta los planteamientos o toma de decisiones en función de la propp

Un ejemplo de este tipo de arquitectura se presenta en la Figura, que al trasladarse prototipo del proyecto considera cada módulo con una zona propuesta en el modelo de la Figura, al hacer un match del color encerrado en los bloques de ambas figuras, la zona desmilitarizada de la red no se contempla dentro esta asociación, pero se la plantea más adelante.

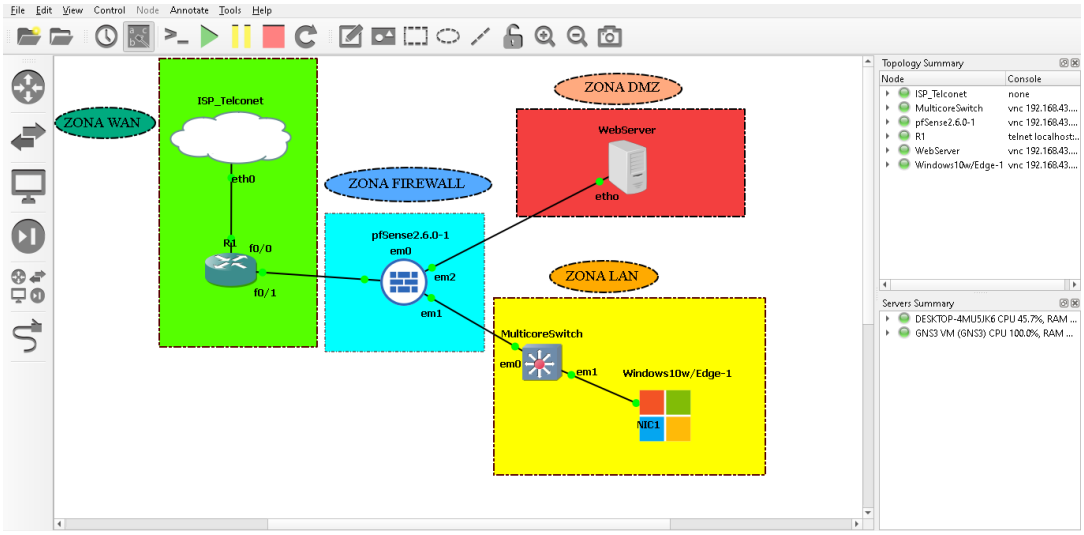
El prototipo de red frontera se observa en la Figura considera el posicionamiento de los equipos en el área del Data center de la planta baja. Está compuesto por 4 Zonas, la zona (WAN, FIREWALL, DMZ y LAN); cada una establece una serie de políticas de firewall en función de los segmentos de la red de los que forman parte orientadas permitir y bloquear determinado tráfico de aplicaciones y servicios.

Figura 4.2 Arquitectura Modular Cisco Enterprise.



Arquitectura empresarial modular, Fuente: (Cisco,2014)

Figura 4.3 Diseño prototipo de red de frontera.

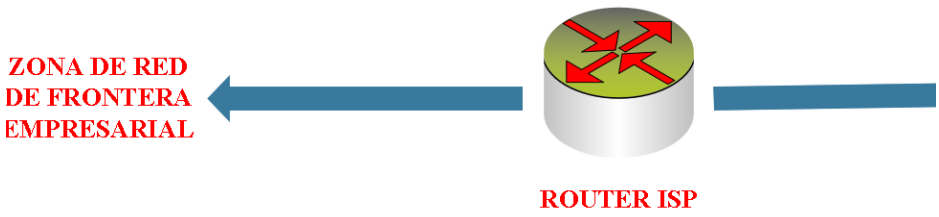


Prototipo de red de Frontera GNS3. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.3.1 Zona WAN

Service Provider Edge, en relación con el ejemplo de arquitectura empresarial se vincula en primer lugar con el módulo Enterprise Edge, al ser responsable de la distribución de conectividad a Internet provista por el ISP, para que el resto de los módulos puedan establecer conexiones entre ellos y ejecutar sus aplicaciones. El diseño del módulo WAN, ver en la Figura 4.4.

Figura 4.4 Diseño Módulo Zona WAN Módulo Conectividad con la Internet.

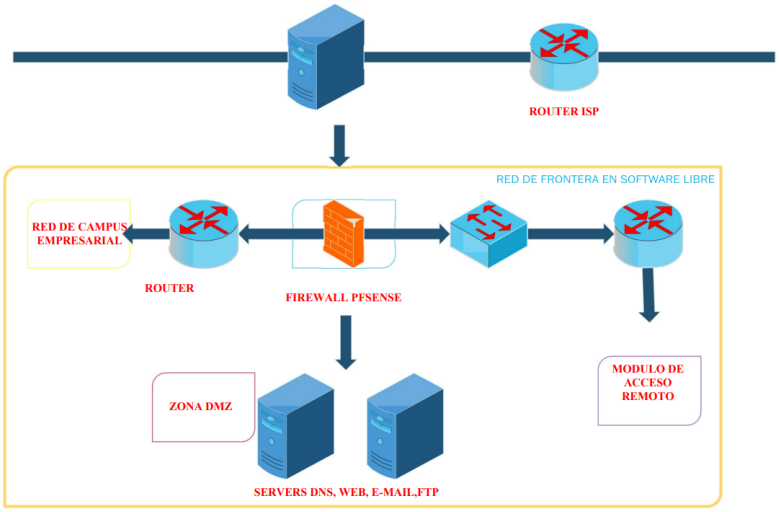


Diseño de módulo Zona WAN/Módulo Conectividad con la Internet. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.3.2 Zona Firewall

Enterprise Edge o red de borde empresarial, en el diseño se aplica submódulo de conectividad internet destaca al ser módulo en que se configuran especialmente los parámetros de forma que, al proveer de conexión, incorpore aspectos de seguridad y funcionalidades propias del NGFW seleccionado previamente, para lograr un desempeño óptimo para todos los departamentos y usuarios de la red. El módulo dentro del cual el Appliance cumplirá la función software de red de frontera se observa en la Figura.

Figura 4.5 Diseño Módulo Zona Edge/Módulo de Frontera de la Red



Diseño de módulo de Frontera de Red Empresarial. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.3.3 Zona DMZ

Gran parte del tiempo no se puede tener control del tráfico de red que puede atravesar por la red LAN al acceder a redes o sitios que no son de completa confianza, bajo la idea de que algunos de los principales servicios, recursos o aplicaciones, así como servidores DNS, e-mail, entre otros, de cualquier empresa están alojados en la internet pública sin distinción de organización. Al ser una prioridad el agregar la mayor cantidad de capas de seguridad posibles se configura esta subred entre la red privada; en relación con las demás zonas se establecen las relaciones, de la siguiente forma:

WAN → DMZ: Permite el tráfico necesario para el uso de los recursos y aplicaciones que manejen la empresa.

LAN → DMZ: Establece una serie de políticas para el acceso de determinados recursos mediante la configuración de reglas.

DMZ → LAN: Las políticas para el acceso cuentan con reglas que no permiten esta comunicación para la mayoría de tráfico que se genera dado que los que no se considera segmentos de red con sus políticas distintivas y mas robustas una que otra.

EDGE → DMZ: Son configurados parámetros menos restrictivos a comparación de los establecidos en la LAN para que la frontera actúe como puente entre las zonas WAN y DMZ.

4.3.4 Zona LAN

Enterprise Campus, conforma la capa de núcleo, distribución y acceso para el nivel 3 de empresas grandes y en nivel 2 en redes empresariales de mediana escala al establecer un

modelo de núcleo colapsado, al combinar las capas de distribución en una, para reducir el equipamiento necesario para la infraestructura de red. El cual se comunica con el módulo Enterprise Edge, de forma que se requiere configurar una serie de políticas que permitan determinados tipos de tráfico a los diferentes puntos de red que conforme este módulo. Las dos propuestas de nivel de red diseñadas, remitir en los Anexos 7 y 8 respectivamente. Es importante puntualizar que, si bien la reducción de costos es un punto clave en el diseño de una red, al buscar garantizar resiliencia, escalabilidad y manejabilidad los modelos de núcleo colapsado no pueden llegar a cumplir con dichos requerimientos por sí solos.

4.4 Tráfico sobre aplicaciones y calidad de servicio

4.4.1 Tráfico de aplicaciones

Debido a que la empresa manufacturera funcionara de forma ininterrumpida en su proceso de producción, dado la jornada laboral de los demás colaboradores, es áreas de trabajo requieren de conectividad continua las 9 horas al día.

Por otra parte, de los 207 puntos de red se proyecta que sean utilizados un total de 104 host y se asume que a los puntos de acceso se conecten un total 55 usuarios para el uso de aplicaciones web dando un total de 168 usuarios conectados, de acuerdo con la ecuación 3.1 se procede a realizar resolución de la formula. Ecuación 3.2 el Ta previsto en 5 años con una tasa de crecimiento del 5% anual.

$$T_A = [(usuarios * \text{Navegación}(Mb)] * horas \qquad \text{Ec. (1)}$$

$$T_A = (159\, usuarios * Mb) * 9\, horas = 1431\, Mb$$

$$AB = \frac{T_A}{9\, horas} * \frac{8\, bites}{1\, byte} * \frac{1\, hora}{3600\, segundos}$$

$$AB = \frac{1431\, Mb}{9\, horas} * \frac{8\, bites}{1\, byte} * \frac{1\, hora}{3600\, segundos} = 0{,}3534\, bps$$

$$T_p = AB + (AB * 5\, años * 5\%)$$

$$T_{Ap} = 0{,}3534\, bps + (0{,}3534\, bps * 5 * 0{,}05) = 1.2369\, bps \qquad \text{Ec. (2)}$$

4.4.2 Tráfico de aplicaciones e-mail y conectividad al internet

Para el respectivo cálculo del tráfico del acceso a Internet y e-mail se parte del tamaño promedio estimado del tamaño de una página web 3398 Kb; y se estima que cada usuario tenga acceso a 18 sitios por hora. Manteniendo la consideración del crecimiento de tasa anual del 5% por 5 años.

$$T_i = número\ de\ sitios * tamaño\ de\ página\ (Kb)$$

$$T_i = 18\ sitios * 3398\ kb = 61164 \frac{Kbytes}{hora}\ por\ cada\ usuario$$

$$AB = \frac{61164\ kbytes}{1\ hora} * \frac{8\ bites}{1\ byte} * \frac{1\ hora}{3600\ segundos} * \frac{1000}{1\ KB}$$

$$AB = 135{,}92\ kbps\ por\ cada\ usuario$$

$$T_{ti} = Nùmero\ de\ usuarios * AB$$

$$T_{ti} = 159 * 135{,}92\ kbps = 21{,}61\ Mbps$$

$$T_{tp} = 21{,}61\ Mbps + (21{,}61\ Mbps * 5 * 0{,}05) = 27{,}01\ Mbps$$

Para el uso de correo electrónico por parte del personal que conforman la plantilla empresarial de la empresa Absorpelsa se proyecta el envío de 35 correos y cada usuario genere un flujo de 0,1 Mbps. Estimación crecimiento al 5% por año.

$$T_C = número\ de\ correos * flujo\ estimado$$

$$T_C = 35 * 0{,}1\ Mbps = 3{,}5\ Mbps$$

$$T_{Cp} = 3{,}5\ Mbps + (3\ kbps * 5 * 0{,}05) = 4{,}25\ Mbps$$

4.4.3 Tráfico de aplicaciones para telefonía de VoIP

En este bloque se realizan los cálculos necesarios para la telefonía de voz sobre IP considerando los parámetros de intensidad de tráfico instantáneo, volumen de tráfico y el periodo de observación.

$$\boldsymbol{A} = \frac{V}{T}$$

Donde:

A: Intensidad de Tráfico en

Erlangs

V: Volumen de Tráfico

T: Periodo de Observación

A partir de estimaciones del volumen diario de tráfico durante las actividades laborales en el horario de 9 am a 12 pm para la estimación del dimensionamiento de los requerimientos de la telefonía IP, considera una cantidad aproximada de 118 llamadas, con un tiempo de 16714 segundos y que cada una tiene un promedio de.

$$t' = \frac{tiempo * nùmero\ de\ llamadas}{nùmero\ total\ de\ llamadas}$$

$$t' = \frac{16714\ seg * 1\ llamada}{118\ llamadas} = 141{,}64\ seg$$

$$t' = \frac{141{,}64\ seg}{3600\ seg} * 1\ hora$$

$$t' = 0{,}039\ horas$$

Al establecer el volumen de tráfico se toma en cuenta la multiplicación entre el número de llamadas y la cantidad de tiempo en horas cuyo resultado es de 4,6 Erlangs:

$$A = \frac{V}{1\ hora}$$

$$A = \frac{4{,}6\ Erlangs}{1\ hora} = 4{,}6\ Erlangs$$

$$AB_V = 158kbps$$

Para el dimensionamiento del ancho de banda de voz requerida para el CFCSB se ha seleccionado el códec G.729A, por su capacidad de compresión de paquetes de audio digital y se ha utilizado la herramienta online Erlangs and VoIP Bandwidth Calculator (Erlang Bandwidth Calculator, 2022),ver Anexo 12. Para el cálculo del Ancho de Banda mínimo que requiere la empresa se obtuvo al realizar la sumatoria de los resultados obtenidos anteriormente obteniendo un aproximado de 83,69 $Mbps$.

4.4.4 Calidad de Servicio y Redundancia

Independiente de la red el exigir garantías sólidas de desempeño se debe considerar como uno de los principales requisitos en el diseño de estas arquitecturas, cuatro aspectos importantes son claves que no deben pasar desapercibidas estas son: las aplicaciones que necesitan, cómo regular el tráfico que ingresa, cómo reservar recursos en los dispositivos de capa 2 y 3 para la asegurar el adecuado desempeño, poder soportar el incremento de tráfico de forma segura.

De acuerdo con la realidad de la empresa y en respuesta a los cuatro aspectos se tiene que las aplicaciones principales en las que se requieren de QoS giran en torno al sistema de gestión empresarial Odoo que agrupa un conjunto de submódulos para la gestión de los procesos involucrados en esta industria, además de las aplicaciones comunes de cualquier otra empresa como el servicio de nombres de dominio, directorio, página web, telefonía

etc. La Tabla 4.4 y Tabla 4.5 determinan los niveles de requerimientos y características de tráfico QoS por aplicaciones que se consideraron.(Tanenbaum & Wetherall, 2012)
El aspecto de redundancia se puede llegar a dar por cubierto al contar con dos ISP distintos o dos enlaces diferentes del mismo proveedor que garanticen la conectividad al Internet 24/7, a su vez en los servidores, al tener aplicaciones considerablemente esenciales el tener un servidor espejo que ejecute los mismos servicios en caso de fallas es un punto destable, pero no considerado dentro del proyecto.

Tabla 4.4 Niveles de requerimientos QoS por Aplicación.

Aplicaciòn	Ancho de Banda	Retardo	Variación de Retardo	Pérdida
Correo electrònico	Bajo	Bajo	Baja	Media
Compartir archivos	Alto	Bajo	Baja	Media
Acceso a Web	Medio	Medio	Baja	Media
Inicio de sesiòn remoto	Bajo	Medio	Media	Media
Audio bajo demanda	Bajo	Bajo	Alta	Baja
Video bajo demanda	Alto	Bajo	Alta	Baja
Telefonìa	Bajo	Alto	Alta	Baja
Videoconferencias	Alto	Alto	Alta	Baja

Tabla Niveles de Requerimientos de calidad de servicio por Aplicación. Fuente (Redes de Computadoras, Tanenbaum & Wetherall, 2012)

Tabla 4.5 Tabla parámetros QoS de acuerdo con las aplicaciones .

Tràfico	Retraso	Jitter	Pérdida	Ancho de Banda
Voz	≤ 150 ms	≤ 30 ms	≤ 1%	30 - 128 kbps
Video	≤ 200 - 400 ms	≤ 30 - 50 ms	≤ 0.1 - 1%	384 kbps - 20 Mbps

Características de tráfico retraso pérdida, jitter, ancho de banda y latencia aplicaciones. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.5 Diseño topológico de la Red de Frontera

En esta etapa se delimita los apartados de la segmentación IPv4, bajo las directrices de políticas de seguridad que se establecerán

4.5.1 Direccionamiento IPV4

En relación con la segmentación de red IPv4 el direccionamiento de la red general va a partir de la red 192.168.1.0 /24, de esta manera, las VLANs fueron establecidas de la siguiente forma: Datos (VLAN 10), Móviles (VLAN 20), Visitas (VLAN 30), Cámaras

(VLAN 40); Voz (VLAN 50) y Servidores (VLAN 60), de próximo, es necesario configurar la comunicación InterVLAN de los segmentos establecidos en la Tabla 4.8.

Tabla 4.6 Segmentación VLANs.

VLANs ID	Red	Slash MSK	MSK
VLAN 10	Datos	/25	255.255.255.128
VLAN 20	Móviles	/24	255.255.255.0
VLAN 30	Visitas	/27	255.255.255.224
VLAN 40	Cámaras	/28	255.255.255.240
VLAN 50	Voz	/29	255.255.255.248
VLAN 60	Servidores	/28	255.255.255.240

Tabla de asignación segmentos VLAN. Elaborado por: Darwin Avalos y Andy Guanochanga.

4.6 Instalación y Configuración del Firewall de Frontera PfSense

El proceso de instalación y configuración comprende la descarga de los recursos necesarios para la virtualización del Appliance, y las acciones posteriores del levantamiento de la configuración inicial.

4.6.1 Descarga, instalación y configuraciones iniciales

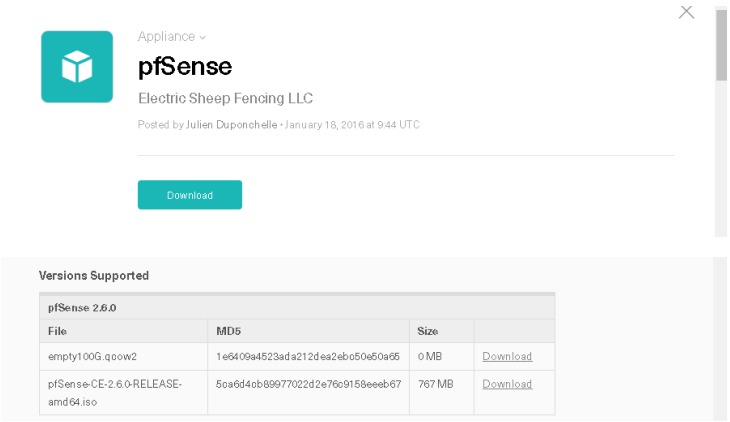
Dependiendo del método de virtualización o instalación del Appliance, para el prototipo de red es indispensable descargar los recursos de la imagen ISO de la página oficial de PfSense la Figura indica los parámetros de la ISO descargada, el seleccionar el hipervisor de virtualización, en este caso VMware Workstation Pro.

El otro método de descarga del Appliance para su virtualización dentro del simulador de red GNS3 emplea dos archivos necesarios para su incorporación dentro del apartado añadir templates. Antes se debe cumplir con un requerimiento previo relacionado a la instalación del GNS3 VM Server en el hipervisor, dentro del cual se guardará toda la información y archivos de los Appliance que se vayan a añadir.

Figura 4.6 Características de ISO de descarga del Appliance NGFW

Descarga del ISO Appliance página of. Fuente: (PfSense,2022)

Figura 4.7 Marketplace Descarga de Appliance



GNS3 Marketplace Descarga de Appliance, Fuente: (GNS3,2022)

La virtualización del Appliance por facilidad, se realizó utilizando el método dos, que, en uso de dos máquinas virtuales, la primer VM encargada de almacenar y correr la ISO del Appliance PfSense y la segunda con sistema operativo Windows 10 instalado para las pruebas y configuraciones mediante la interfaz de administración web. Las configuraciones iniciales dentro de la interfaz web remitir al Anexo

4.6.2 Características de PfSense incorporadas dentro del prototipo de Red.

Entre el abanico de configuraciones y funcionalidades que provee el servidor de firewall de nueva generación con una orientación hacia la mitigación de vulnerabilidades los módulos y zonas de red a partir de la delimitación del tráfico en las interfaces, puertos, VLANs, bajo el mapeo de políticas direcciones de origen, destino, permitiendo o denegando del flujo para determinas aplicaciones o servicios.

4.6.3 Configuración de las listas de acceso ACLs Y PFBlocker NG

En la configuración de PfSense partió de la propuesta de red LAN 192.168.1.0 la cual desglosa redes virtuales VLAN'S para Datos 192.168.10.0/25, Móviles 192.168.20.0/24, Visitas 192.168.30.0/27, Cámaras 192.168.40.0/28, Voz 192.168.50.0/29 y Servidores 192.168.60.0/28, los cuales compartirán un puerto troncal que filtra los paquetes de salida en base a los puertos TCP/IP, de la misma forma la navegación es bloqueada por un appliance PFBlocker que impide acceso a distintas páginas web que no son de uso empresarial, y limitan la productividad de los colaboradores.

Como parte de las políticas de seguridad, se configura listas de control de acceso (Acls) las cuales permiten el tráfico de los protocolos de tráfico delimitados en las Tablas 4.7, 4.8 y 4.9, establecen las configuraciones para el control del tráfico bajo determina aplicación o servicio que emplea un puerto determinado y sigue un flujo, previamente señalado; remitir a (Anexos 13,14,15) para verificación, simulación y resultados.

Tabla 4.7 Tabla de listas de control de acceso ACLs N.

Interfaz	Origen	Destino	Puertos	Estados	Descripción
WAN	186.3.59.104/29	any	80.443.587	Paso	Recursos Estimados
	any		any	Bloqueo	Bloqueo
LAN	192.168.1.0	any	80,443,20-21,22,53,68,69,123,110,143,1433	Paso	Recursos Estimados
	any		any	Bloqueo	Bloqueo
DMZ	192.168.60.0	192.168.1.0	any	Bloqueo	Bloqueo
	any	any		Paso	Paso

Tabla de listas de control de acceso PfSense. Elaborado por: Darwin Avalos y Andy Guanochanga.

Tabla 4.8 Listas de Filtrado InterVLAN.

Interfaz	Origen	Destino	Puertos	Estados	Descripción
VLAN 10	192.168.10.0/25	192.168.10.5/25	20-21,53,69	Paso	Gateway
		192.168.20.0/24	Any	Bloqueo	No permitir
		192.168.30.0/27	20-21,69	Paso	Compartir Archivos
		192.168.40.0/29	Any	Bloqueo	Archivo
		192.168.50.0/26	5004,5060-5061-4569	Paso	Telefonia
		192.168.60.0/28	101,110,143,1433,68	Paso	Servicios
VLAN 20	192.168.20.0/24	192.168.20.5/25	20-21,69	Paso	Gateway
		192.168.10.0/24	Any	Bloqueo	Bloqueo
		192.168.30.0/27			
		192.168.40.0/29			
		192.168.50.0/26			
		192.168.60.0/28			
VLAN 30	192.168.30.0/27	192.168.30.5/25	20-21,53,69	Paso	Archivo
		192.168.10.0/24	Any	Bloqueo	No permitir
		192.168.20.0/24			
		192.168.40.0/29			
		192.168.50.0/26			
		192.168.60.0/28			
VLAN 40	192.168.40.0/29	192.168.40.5/29	80-8080	Paso	Gateway
		192.168.10.0/24	21	Paso	Compartir Archivos
		192.168.20.0/24		Bloqueo	No permitir
		192.168.30.0/27			
		192.168.50.0/26			
		192.168.60.0/28			
VLAN 50	192.168.50.0/26	192.168.50.5/26	5004,5060-5061,4569	Paso	Gateway
		192.168.10.0/24	Any		Compartir Archivos
		192.168.20.0/24		Bloqueo	No permitir
		192.168.30.0/27			
		192.168.40.0/29			
		192.168.60.0/28			
VLAN 60	192.168.60.0/28	192.168.60.5/28	80,443,20-21,53,67,69,123,33433,110,143,1433	Paso	Gateway
		192.168.10.0/24	Any	Bloqueo	No permitir
		192.168.20.0/24			
		192.168.30.0/27			
		192.168.40.0/29			
		192.168.50.0/26			

Tabla de asignación de segmentos intercomunicación VLAN. Elaborado por: Darwin Avalos y Andy Guanochanga.

Tabla 4.9 Tabla de Filtrado de Puertos para VLANs.

Interfaz	Origen	Destino	Puertos	Estados	Descripción
VLAN 10	any	192.168.10.0/25	80,443,20-21,53,68,69,123,110,143,1433	Permitir	Recursos Estimados
VLAN 20	any	192.168.20.0/24	80,443,20-21,69,123	Permitir	Recursos Estimados
VLAN 30	any	192.168.30.0/27	80,443,20-21,69,123	Permitir	Recursos Estimados
VLAN 40	any	192.168.40.0/29	80-8080	Permitir	Recursos Estimados
VLAN 50	any	192.168.50.0/26	5004,5060-5061-4569	Permitir	Recursos Estimados
VLAN 60	any	192.168.60.0/28	80,443,20-21,53,67,69,123,110,143,1433	Permitir	Recursos Estimados

Tabla de asignación segmentos VLAN. Elaborado por: Darwin Avalos y Andy Guanochanga.

CAPÍTULO 5
ANÁLISIS DE COSTOS

En el presente capítulo se va a establecer los costos de implementación de la propuesta de diseño de la red de frontera en software libre, considerando la inversión inicial, costos de capital y costos de operación al calcular las fórmulas relacionadas con como el VAN & TIR; útiles en la definición de la rentabilidad y factibilidad económica.

5.1 Factibilidad y Rentabilidad económica

En el apartado de (ver, Anexos) se presenta las especificaciones de hardware para el servidor en donde se implementaría el firewall open source de seguridad perimetral PFSENSE, entre otros dispositivos adicionales para repotenciar la infraestructura de red de la empresa, incluyendo cotizaciones de algunos de estos.

5.1.1 Costos de Capital (CAPEX)

La Tabla 5.1 consta de todos los equipos considerados para esta propuesta de implementación de la red de frontera, donde se obtienen valores estimados del equipamiento necesario en base a cotizaciones por parte de los distribuidores, y consultas en tiendas de comercio electrónico (Proformas, ver Anexos 3,5,6,11).

Tabla 5.1 Tabla Costos de Capital lista de dispositivos.

Proyecto de diseño de Red de Frontera en Software Libre para la empresa Absorplesa				
Nº ÍTEM	**DISPOSITIVO**	**CANTIDAD**	**VALOR UNITARIO**	**VALOR TOTAL Icl. IVA**
1	Puntos de accesoWifi Tp-Link	7	87,6	665
3	Switch Capa 3 de Alta disponibilidad	1	439,12	499
4	Servidor HPE ProLiant DL 160 Gen10	1	50764	5755
5	Telefonos VoIP (1 Central Telefonica+ 24Teléfonos configurados)	25	2996	3356
7	Proyecto de Cableado Estructurado(2 Switch Capa3+Cableado CAT 6A)	1	10500	11760
*	**VALOR TOTAL:**		$	**22035**

Tabla en detalle de dispositivos necesarios en el costo de capital CAPEX para Absorpelsa. Elaborado por: Darwin Avalos y Andy Guanochanga.

5.1.2 Costos de Operación (OPEX)

Los costos operacionales de la propuesta del diseño se obtuvieron a partir de las consideraciones que se prevé, para el desarrollo en variables de mano de obra y gastos

operacionales del proyecto compuesto por los parámetros especificados en el conjunto de la Tabla 5.2.

Tabla 5.2 Parámetros de Costos de Operación & Mano de Obra

COLABORADOR	DÍAS/MESES	HORAS LABORALES DIARIAS	COSTO POR HORA	COSTO TOTA
Guanochanga Andy	5	5	$11	$255
Avalos Darwin	5	5	$11	$255
OPEX TOTAL				**$510**

EGRESOS	VALOR MES A MES
Plan de Interner de 80 Mbps	$77,20
Gastos Operativos	$150
OPEX TOTAL	**$217,20**

Parámetros de Costos de mano de obra y costos operativos. Elaborado por: Darwin Avalos y Andy Guanochanga.

Al determinar el costo de la mano de obra que, durante el transcurso de tiempo estimado de 5 meses asciende al valor de $ 2550, se termina añadiendo un costo adicional al valor obtenido dentro del apartado del CAPEX, por ende, el valor de la inversión va a alcanzar la suma de $24. 585.El valor de inversión total disminuye en función que se completó el pago del proyecto de cableado estructurado CAT 6A, ver Anexo 11, deduciendo dicho valor del resultado obtenido de la Tabla 5.2.

Los gastos operacionales previstos durante el proceso del proyecto ya en operación, el valor es de $ 1.086. La Tabla 5.3 presenta el nivel de ahorro que aporta la propuesta simulada del prototipo de red de borde, considerando el deslinde de proveedores externos de telefonía fija y la contratación de planes móviles para los colaboradores de la industria.

Tabla 5.3 Detalles de Ahorro Propuesta de diseño.

CONCEPTO	CANTIDAD	COSTO			COSTO MENSUAL
Llamadas Internas y Externas		**ASIGANACION MESUAL(USD)**	**COSTO MINUTO(USD**	**DURACIÓN APOX.(min)**	242,38
	650	18,13	0,046	7,5	
Plan Moviles celulares y Ahorro Llamadas móviles externas	50,00	21,5	112		1187,00
NFGW Dedicado	1	225 al Año			18,75
Valor TOTAL de Ahorro				$	**1448,13**

Tabla en detalle de conceptos de ahorro por implementación de propuesta de diseño de red de borde y telefonía IP. Elaborado por: Darwin Avalos y Andy Guanochanga.

5.1.3 Recuperación de la inversión y análisis del TIR y el VAN

Ya definidos los egresos como el ahorro del proyecto, es posible realizar el flujo efectivo. Es pertinente considerar que el proyecto de cableado estructurado sus valores ya fueron finiquitados hace tres meses, por tanto, se descuenta dicho valor de la inversión total. La Tabla 5. 4 detalla del flujo neto en delimitación de tiempo trimestral con una depreciación del 10% del costo general de la inversión inicial del proyecto.

Tabla 5.4 Flujo Neto Efectivo.

PERIODO	0	1er Trimestre	2do Trimestre	3er Trimestre	4to Trimestre	5to Trimestre	6to Trimestre
INGRESOS POR AHORRO		4344,39	4344,39	4344,39	4344,39	4344,39	4344,39
GASTOS OPERATIVOS		651,60	651,60	651,60	651,60	651,60	651,60
DEPRECIACIÓN		320,63	320,63	320,63	320,63	320,63	320,63
UTILIDAD		3372,17	3372,17	3372,17	3372,17	3372,17	3372,17
INVERSIÓN	-12825,00						
DEPRECIACIÓN		320,63	320,63	320,63	320,63	320,63	320,63
FLUJO	-12825	3692,79	3692,79	3692,79	3692,79	3692,79	3692,79
FLUJO ACUMULADO	-12825	-9132,21	-5439,42	-1746,63	1946,16	5638,95	9331,74

Resultados		
TASA DE INTERES	15%	
TIR	0,18	
VAN	13.975,30 €	
VAN USD	14.208.832	$

Tabla en detalle del flujo neto efectivo del proyecto. Elaborado por: Darwin Avalos y Andy Guanochanga.

De acuerdo con el criterio de análisis de pertinencia del proyecto, si el valor actual neto VAN o VPN, es mayor que cero es viable caso contrario ser lo debe rechazar y da que el TIR es el porcentaje de beneficio o pérdida que se puede obtener de una inversión, al obtener un valor de 0,18. El proyecto es aceptable, ya que su rentabilidad es mayor que la rentabilidad mínima requerida o coste de oportunidad.

CAPÍTULO 6
CONCLUSIONES

Al definir la línea base de la empresa en cuestión en el apartado de la situación inicial, se adquirió información mediante un proceso sistemático y enriquecedor orientado a entender las variables, características, limitantes y requerimientos actuales; se estableció como norma indispensable y primordial para proyecto de diseño de arquitectura empresarial. Aportando un panorama general de la realidad actual y los escenarios futuros de la red a la empresa Absorpelsa, que se consideraron en el diseño propuesto, para garantizar una arquitectura modular integral capaz de satisfacer aspectos de conectividad, escalabilidad resiliencia y seguridad.

La visión general, guías de arquitecturas, diseños referenciales, a su vez, recursos relacionados con el modelo empresarial Cisco SAFE proporcionaron una aproximación de los procedimientos, equipamiento y recomendaciones empleadas en diseño de los módulos de frontera, conectividad con internet y campus empresarial entendiendo que las aplicaciones, servicios y usuarios son el objetivo en la adecuación de los componentes necesarios que aseguraron la resiliencia del ambiente de red empresarial.

La simulación del prototipo de red de seguridad perimetral, considero la segmentación IPv4 adecuada, en función del número de host necesarios, el establecimiento de la configuración de las características seleccionadas como parte de las políticas de seguridad, se configuró las características de listas de control de acceso (ACLs), PFBlocker para establecer un filtrado de acceso a las páginas de Instagram, Facebook y YouTube, lo cual en un ambiente laboral solo generaría distracción y baja productividad; Filtrado de puertos y comunicaciones InterVLAN, que permitieron el paso y bloqueo de tráfico de los protocolos más comunes dentro de las aplicaciones manejan o no como empresa. Destacando que para contar con una red resiliente se requiere de un ancho de banda del ISP superior a los 100 Mbs de velocidad simétrica, y configuración de políticas adicionales de distribución de ancho de banda, y acceso remoto dentro del NGFW.

Como parte de las actividades establecidas en el Anexo 9, el desarrollo del cronograma para el cumplimiento del proyecto de grado se evidenció en el Anexo 10, donde se destacó la labor del cumplimiento de los objetivos y actividades relacionadas con la propuesta de

red para la empresa; destacando la funcionalidad de administración y potencia de configuración en la capacidad de incorporar servicios agregados más adelante.

El proyecto resulta ser viable al recuperar la inversión total en el cuarto trimestre (año), al considerar los beneficios relacionados con los aspectos tecnológicos, de procesos de sistemas de gestión, comunicación y distribución conectividad de internet. Las fórmulas de la tasa interna de retorno y valor actual neto arrojan valores positivos en la rentabilidad del proyecto. Reflejando que el ahorro en telefonía fija de proveedores externos y planes móviles celulares, se convierten en ingresos importantes a lo largo de su tiempo de vida.

RECOMENDACIONES

En la realización de trabajos futuros se recomienda efectuar más configuraciones dentro del Appliance PfSense orientado a la mitigación de las vulnerabilidades, complementando con configuración de políticas de seguridad elaboradas dentro de las funcionalidades disponibles del mismo, entre las cuales se puede proponer el bloqueo de usuarios, balanceo de carga, algoritmo de colas, configuración de Hotspot, certificados de conexión VPN.

Explorar el uso de herramientas tecnológicas externas para el análisis de vulnerabilidades en tipo de archivos, URLs y control de procesos & subprocesos dentro de los sistemas operativos, que pueden afectar a los dispositivos finales, y expandirse de forma inadvertida, por tanto, desarrollar a partir de un análisis cibernético forense, o de pruebas de penetración, en pro de conocer que políticas adicionales son idóneas para incluir al prototipo de red borde en software libre.

Continuar con el diseño del módulo empresarial de Acceso VPN y teletrabajo, a medida que, las necesidades se incrementen y sean pertinentes de diseñar e implementar; bajo la aproximación de los módulos del modelo cisco SAFE, considerando las directrices de equipamiento, configuración, políticas, entre otras consideraciones provistas por los documentos oficiales del módulo en específico. Determinar configuraciones adiciones en los switches de capa 3 y Routers relación con la calidad de servicio mediante comandos de consola.

Documentar un instrumento técnico y formal de las políticas de seguridad información, control de acceso de para los usuarios, responsabilidades individuales y grupales, mitigaciones de vulnerabilidades, procedimientos de control y análisis de eventos de seguridad. También el establecer procedimientos del monitoreo del desempeño configuraciones actuales, procesos de repotenciación de infraestructura que especifiquen, donde se priore la actualización de estos informes en un plazo estimado.

REFERENCIAS

¿ Qué es un next generation firewall ? (2014).

Cisco. (2019). Capítulo 3 : Protocolos y comunicación de red. *CCNA Routing y Switching*, 4–14. https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp3.pdf

Cisco SAFE Reference Guide SAFE Overview Executive Summary. (.).

Cuenca, J. M. (2016). Firewall O Cortafuegos. *Universidad Nacional de Loja*, *February*, 1–5. https://www.researchgate.net/publication/295256426

Differences of Top-Down vs. Bottom-Up Approaches. (.). Recuperado Junio 17, 2022, de https://www.investopedia.com/articles/investing/030116/topdown-vs-bottomup.asp

Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad – Ministerio de Telecomunicaciones y de la Sociedad de la Información. (.). Recuperado Mayo 23, 2022, de https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/#search

Erlang bandwidth calculator - Free tools de Westbay Engineers. (.). Recuperado Julio 10, 2022, de https://www.erlang.com/calculator/eipb/

Esparza Morocho, J. P. (2013). *Implementacion de un firewall sobre plataformas Linux*. 138. https://bibdigital.epn.edu.ec/bitstream/15000/6056/1/CD-4785.pdf

Fernando, J., Maliza, C., Andrés, J., & Toro, L. (.). *UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CARRERA: INGENIERÍA ELECTRÓNICA Trabajo de titulación previo a la obtención del título de: INGENIEROS ELECTRÓNICOS TEMA: DISEÑO DE LA RED DE FRONTERA PARA EL CENTRO DE FORMACIÓN CONTINUA SAN BARTOLO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA*.

Hackers Attack Every 39 Seconds | 2017-02-10 | Security Magazine. (.). Recuperado May 23, 2022, de https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Informe de seguridad informática en Latam y el mundo - Hacknoid. (.). Recuperado May 23, 2022, de https://www.hacknoid.com/hacknoid/informe-seguridad-informatica-en-latam-y-el-mundo/

McGraw-Hill. (2012). Protocolo TCP/IP. *May 25, 2012*, 24. http://assets.mheducation.es/bcv/guide/capitulo/8448199766.pdf

O, D. G., & P, C. R. (2012). *Topología Mixta*.

Osi, E. (1984). El modelo OSI - análisis de la red en capas. *Unicen*, *2*, 1–11.

PPDIOO Stages > Cisco's PPDIOO Network Cycle | Cisco Press. (.). Recuperado July 2, 2022, de https://www.ciscopress.com/articles/article.asp?p=1697888&seqNum=2

SAFE Overview Guide Threats, Capabilities, and the Security Reference Architecture SAFE Overview Guide Threats, Capabilities, and the Security Reference Architecture | Contents. (2018).

safe_wp1. (2000).

Sampaio, D., & Bernardino, J. (2017). Evaluation of firewall open source software. *WEBIST 2017 - Proceedings of the 13th International Conference on Web Information Systems and Technologies*, *Webist*, 356–362. https://doi.org/10.5220/0006361203560362

SEAQ - Expertos en Pfsense para Colombia - Open Source. (.). Recuperado Julio 6, 2022, de https://www.seaq.co/pfsense.html

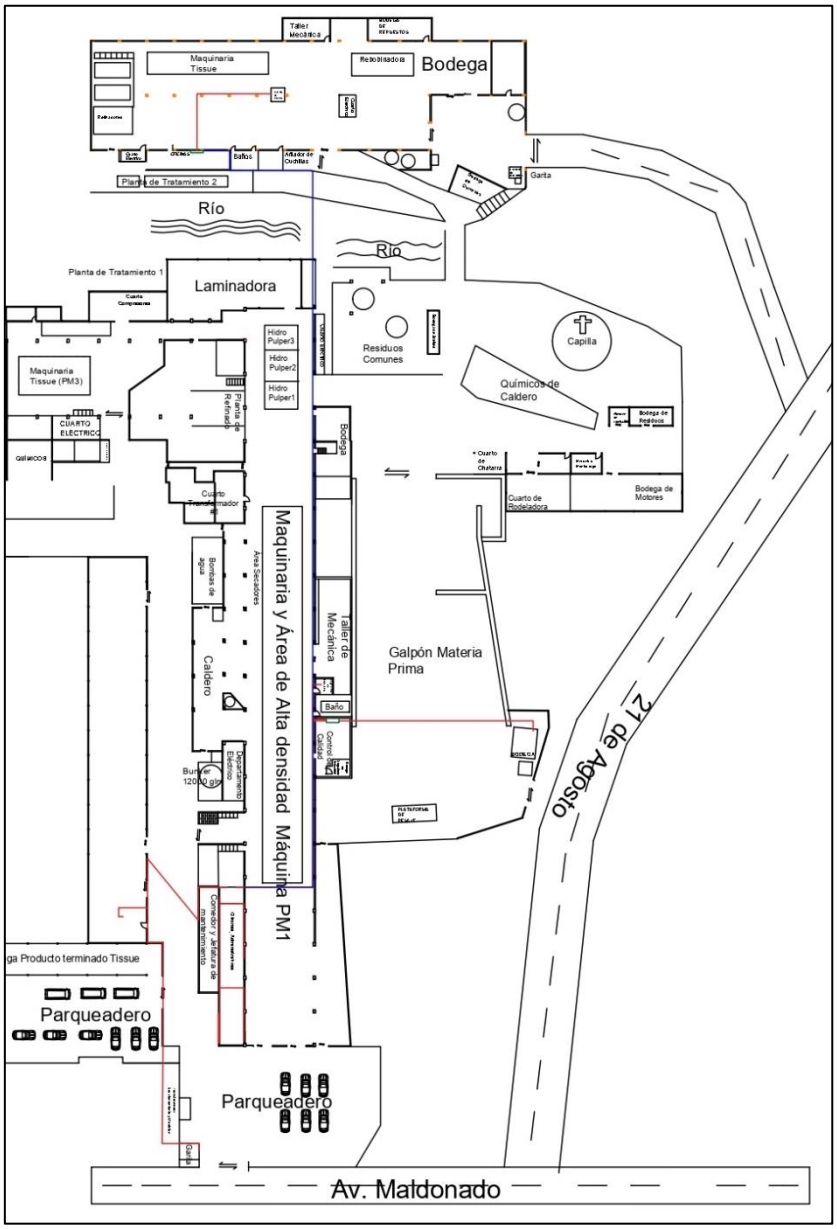
Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras*. Pearson Educación.

UNIVERSIDAD DE COLIMA. (2019). Modelo Tcp/ Ip. *Mexico*, 1–5.

ANEXOS

Anexo 1

Diagrama de Completo de Área Empresarial e Interconexión del Proyecto del Cableado Estructurado para la infraestructura red Absorpelsa AutoCAD



Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 2

Características de Equipamiento empleado en Interconexión del Proyecto del Cableado Estructurado y Proforma Bigexpert.

CANTIDAD	MARCA	SERIE	DESCRIPCION
1	CISCO	FOC2602YPYU	Switch 24 puertos CBS250-24T-4G. Inlcuye : Smartnet 36 meses y configuración
1	CISCO	CN19KPF06Z	Switch 24 puertos CBS350-24T-4G. Inlcuye : Smartnet 36 meses y configuración
50	SIEMON	NO DETALLADO	JACK ZMAX CAT 6A F/UTP BLANCO 45 GRADOS Z6A-45- Número de parte : S02B Z6A-45- S02B
50	SIEMON	NO DETALLADO	JACK ZMAX CAT 6A F/UTP NEGRO Número de parte : Z6AS01B
6	SIEMON	NO DETALLADO	PATCH PANEL 6A/7A MODULAR PLANO 24 PTOS Número de parte : TMPNLZ- 24-01
50	SIEMON	NO DETALLADO	PATCH CORD CAT 6A BLIND 3FT AZUL Número de parte : ZM6AS03- 06B
50	SIEMON	NO DETALLADO	PATCH CORD CAT 6A BLIND 7FT AZUL Número de parte : ZM6AS07-06B
50	SIEMON	NO DETALLADO	FACEPLATE 1 PUERTO BLANCO Número de parte : MX-FP-S- 01-02B
	SIEMON	NO DETALLADO	CABLE F/UTP CAT6A LS0H Número de parte : 9A6L4-A5
1	SIEMON	220307-O-LA19889	GARANTIA DE 25 AÑOS, OTORGADA POR SIEMON

Anexo 3

Interconexión del Proyecto del Cableado Estructurado 6A Inversión Total Proforma Bigexpert.

INGENIERIA Y SOLUCIONES TECNOLOGICAS BIGEXPERT CIA LTDA

BIGEXPERT CIA LTDA

Matriz: QUITO, YANÉZ PINZON N26-56 EDIFICIO FRAGO LOCAL 2
Establecimiento: QUITO, YANÉZ PINZON N26-56 EDIFICIO FRAGO LOCAL 2

OBLIGADO A LLEVAR CONTABILIDAD: SI

R.U.C.: 1792516145001
FACTURA
No. 001-999-000000525
NÚMERO DE AUTORIZACIÓN
2101202201179251614500120019990000005251234567811
AMBIENTE: PRODUCCIÓN
EMISIÓN: Normal
CLAVE DE ACCESO

Nombre: PAPELES ABSORVENTES ABSORPELSA S.A
Identificación: 1791353455001
Fecha Emisión: 21/01/2022

Código	Cantidad	Descripción	Precio Unitario	Desc.	Precio Total
P001	1.000000	CABLEADO ESTRUCTURADO MARCA SIEMON CAT 6 A	10500.000000	0.00	10500.00
D001	1.000000	INCLUYE:	0.000000	0.00	0.00
D001	48.000000	PUNTOS CABLEADO ESTRUCTURADO CAT6A	0.000000	0.00	0.00
D001	1.000000	Servicio reubicación de enlace de fibra óptica	0.000000	0.00	0.00
D001	2.000000	SWITCH CISCO 24 Puertos ADMINISTRABLE CAPA 3	0.000000	0.00	0.00
D001	2.000000	Smart Net , CON-SNT-CBS3504G	0.000000	0.00	0.00

Información Adicional	
Dirección:	Av. Maldonado S 26 -183 Y 21 de Agosto
Teléfono:	2671 900
Email:	rcamacho@absorpelsa.com.ec,
Contribuyente	Contribuyente Régimen RIMPE

Información Formas de Pago		
Forma Pago	Valor	Plazo (días)
OTROS CON UTILIZACION SISTEMA FINANCIERO	11760.00	0

SUBTOTAL IVA 12%	10500.00
SUBTOTAL IVA 0%	0.00
EXENTO	0.00
SUBTOTAL SIN IMPUESTOS	10500.00
TOTAL DESCUENTO	0.00
ICE	0.00
IVA 12%	1260.00
PROPINA	0.00
TOTAL	11760.00

Anexo 4

Escaneo Completo Advanced Ip Scanner IPv4 Ad Equipos Activos e Inactivos Red Empresarial.

Estado	Nombre	IP	Fabricante	Dirección MAC
Activado	192.168.10.1	192.168.10.1		20:CF:AE:28:3E:08
Activado	192.168.10.12	192.168.10.12	Cisco-Linksys, LLC	C8:B3:73:2C:36:59
Inactivo	192.168.10.125	192.168.10.125		D8:B0:53:1C:B1:CB
Activado	192.168.10.126	192.168.10.126	QPCOM INC.	88:A5:BD:20:61:08
Activado	192.168.10.2	192.168.10.2		CC:ED:4D:03:4D:4B
Inactivo	192.168.10.45	192.168.10.45	Hewlett Packard	E4:E7:49:0C:88:72
Activado	192.168.10.5	192.168.10.5	Routerboard.com	E4:8D:8C:8C:88:85
Inactivo	192.168.10.57	192.168.10.57	LG Electronics (Mobile Communications)	A8:B8:6E:2E:60:5F
Inactivo	192.168.10.59	192.168.10.59	Samsung Electronics Co.,Ltd	A4:6C:F1:D3:E5:EA
Inactivo	192.168.10.61	192.168.10.61		28:CD:C4:46:07:23
Activado	192.168.10.7	192.168.10.7	Cisco Systems, Inc	10:BD:18:34:33:41
Activado	192.168.10.8	192.168.10.8	Cisco Systems, Inc	D4:A0:2A:72:1B:C1
Activado	192.168.10.9	192.168.10.9	Cisco Systems, Inc	00:1C:0E:FC:EC:41
Activado	192.168.10.90	192.168.10.90	Samsung Electronics Co.,Ltd	A8:51:5B:CF:70:39
Activado	192.168.10.91	192.168.10.91		10:82:D7:CC:8F:E7
Activado	BODEGA	192.168.10.67	Elitegroup Computer Systems Co.,Ltd.	C0:3F:D5:62:57:81
Activado	CAGUIRRELPT	192.168.10.109		A8:93:4A:8E:C3:E9
Inactivo	CAGUIRRELPT.incasa.local	192.168.10.33		00:E8:00:32:01:22
Inactivo	DESKTOP-6048635	192.168.10.36	Dell Inc.	EC:F4:BB:83:E4:BF
Inactivo	DESKTOP-7QBVA4L	192.168.10.113	LCFC(HeFei) Electronics Technology Co., Ltd.	28:D2:44:A7:37:B5
Inactivo	DESKTOP-GGS9MTK	192.168.10.115		E4:54:E8:46:CE:C7
Inactivo	DESKTOP-MGARJ60	192.168.10.60	Intel Corporate	60:6C:66:8F:14:93
Inactivo	DESKTOP-PRAJQI4	192.168.10.119	Pixelworks, Inc.	00:08:18:08:30:27
Inactivo	DOCAMPO	192.168.10.30		4C:79:6E:BD:5B:69
Inactivo	ELECTRICO.incasa.local	192.168.10.32	Merlin Systems, Inc.	00:03:17:0C:0E:10
Inactivo	ELECTRICO.incasa.local	192.168.10.39		90:CC:DF:D3:F8:24
Inactivo	FREINOSO	192.168.10.65		A4:97:B1:4C:C5:2D
Inactivo	Helpdesk1	192.168.10.118		30:D0:42:0F:1F:A2
Activado	INCADM	192.168.10.62	Hewlett Packard	D4:C9:EF:7B:AF:8D

Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 5

Especificaciones de Comparativa de Servidor para Appliance de Virtualización.

Modelo / Características	HPE ProLiant DL 160 Gen10	Cisco UCS C220 M4	DELL EMC PowerEdge R740
Disco Duro	120 GB/ 16GB RDIMM	1 TB/ 16 GB RDIMM	1.6 TB/ 32 GB RDIMM
Procesador	Procesador Silver 4116	Intel Xeon E5-2600 v4	Intel Xeon de 2da Generación
Max Memoria	RDIMM 256 GB	Cisco 64 G SAS Modular RAID	3 TG DIMM DDR4
Raid Software	HPE Smart Array S100i SR Gen 10 SW RAID	Cisco 12 G SAS Modular RAID	PERC H330, H730P, H740p, RAID de Software
Max Interno	9.6 TB	64 GB (x2)	240 GB
Fuente de Poder	HPEE 500W Flex Slot	770 W (CA) 0 1050 W (CC)	Titanium 750 W Platinium 495 W 750 W, 1100 W 1600 W y 2000 W
Interfaces	Video, Puerto de red, HPE iLO Remote Management, Network Port, Front Ilo Service Port, Micro SD, Slot, USB3.0	2 puerto i 350, Gbenth, PXE boot, DB 15VGA conector , RJ45 serial port, USB 3.0 (x2), KVM, VIC, CNA, HBA	4 x 1 GE 0 2 x 10 GE + 2x I GEo4x 10 GE o 2 x 25 GE Video, 2 x USB 2.0 USB 3,0 disponible IDRAC dedicada Tarieta de video VGA
SO	Windows Swerver (2016/2022), Vmware, (U1/U2/U3), Red Hat Enterprise Linux, SUSE Linux Enterprise Server	Linux RHEL (6.5/6.6/6.7/7.0/7.2/SLES) VMware	Canonical, Ubuntu LTS Citrix XenServer Microsoft Windows Server con Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VM ware ESXi
Gráficos	Modos de Video de 32 bpp 16MB de Memoria de Video	Matrox G200e video/controlador	Matrox G200eW3,16MB Video
Chasis	4LFF 8SFF	M4 LFF M4 SFF	SFF
Ventiladores	3 Estándar	6	6
Factor Forma	1 U Rack	1 U Rack	2 U Rack
Slots	3 Slots PCIe 3.0	2 Slots PCIe Riser	8 Gen3
Batería Reemplazable	Si	Si	Si
Precio	5.843,47	6.6878,40	5.790,63

Anexo 6

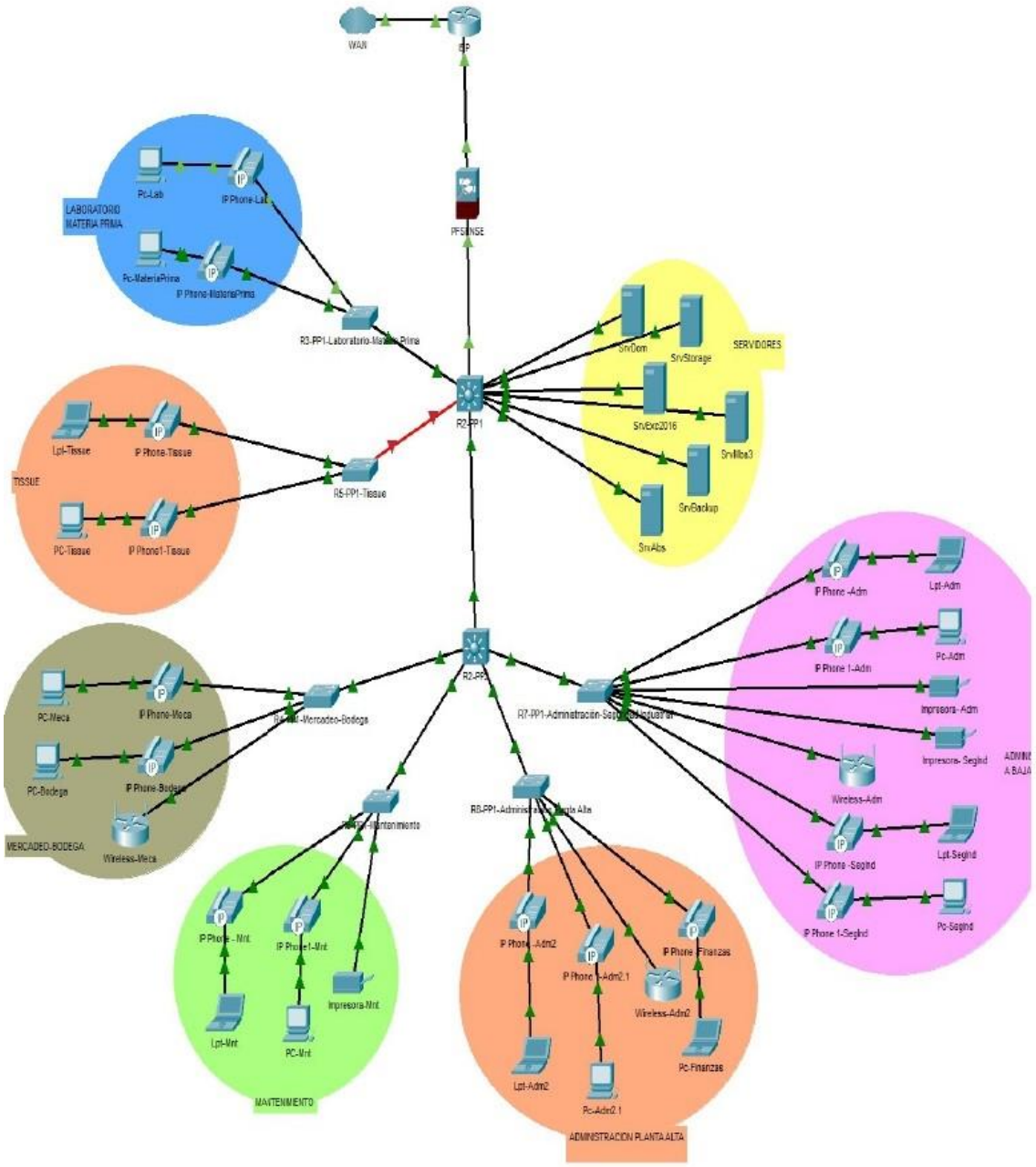
Especificaciones de Comparativas de Switch Capa 3 & Router Característica de Alta disponibilidad.

Modelo Parámetros	Cisco Business 350 CBS350-24FP-4X	Cisco Business 250 CBS250-24PP-4G	Cisco Business CBS250-24FP-4G	TP-LINK T3700G-28TQ	Switch Aruba 2930F
Puertos y Ranuras I/O	24 puertos 10/100/1000 + 4 x SFP+ de 10 GE; 24 puertos PoE con balance de potencia total de 370 W, PoE, PoE+	24 puertos Gbps 10/100/1000 PoE+ 195W + 4 puertos gigabit SFP rackeable	24 puertos 10/100/1000 + 4 x 1G SFP; 24 puertos PoE con 382 W de presupuesto de potencia total, PoE, PoE+	24 puertos 10/100/1000 Mbps (Negociación automática/Auto MDI/MDIX); 4 ranuras Combo SFP 100/1000Mbps; 4 Ranuras de hasta 10G SFP (2 ranuras fijadas y 2 opcionales); 1 puerto de consola	24 puertos RJ-45 con detección automática 10/100/1000 (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T); Dúplex: 10BASE-T/100BASE-TX: semi o completo; 1000BASE-T: solo completo; 4 puertos SFP+ 1/10 GbE; sin PHY
Enrutamiento	Routing IPv4; Routing IPv6; Interfaz de capa 3;Routing entre dominios sin clase (CIDR); Enrutamiento basado en directivas (PBR); Servidor DHCP; Retransmisión DHCP en capa 3; Retransmisión de protocolo de datagramas de usuario (UDP)	Routing IPv4; Routing IPv6; Interfaz de capa 3; Routing entre dominios sin clase (CIDR); Retransmisión de protocolo de configuración dinámica de host (DHCP) en capa 3; Retransmisión de protocolo de datagramas de usuario (UDP).	Routing IPv4; Routing IPv6; Interfaz de capa 3;Routing entre dominios sin clase (CIDR); Enrutamiento basado en directivas (PBR); Servidor DHCP; Retransmisión DHCP en capa 3; Retransmisión de protocolo de datagramas de usuario (UDP)	Reenvío IP a velocidad de cable; Enrutamiento estático; RIP v1, v2; OSPF v2; ECMP; PIM-SM / PIM-DM / IGMP; Servidor DHCP / Relé; Proxy ARP; VRRP	Servidor DHCP; enrutamiento IP estático; ECMP (Equal-Cost Multi-Path Routing; RIPv1, RIPv2 y RIPng; OSPF (Open Shortest Path First) OSPFv2 y OSPFv3.
Seguridad	Protocolo Secure Shell (SSH); Capa de sockets seguros (SSL); IEEE 802.1X (función de Autenticador); Autenticación web; Protección de la unidad de datos de protocolo puente (BPDU) STP; Protección de raíz de STP; Protección de bucle invertido de STP; Detección de DHCP; Protección de IP de origen (IPSG); Inspección ARP dinámica (DAI); Enlace de puertos IP/Mac (IPMB); Secure Core Technology (SCT); Datos confidenciales seguros (SSD); VLAN privada; Perímetro de VLAN privada; Perímetro de VLAN privada (PVE) con aislamiento de capa 2 y comunidad VLAN; RADIUS/TACACS+; Administración de RADIUS; Prevención de denegación de servicio (DoS); Diversos niveles de privilegio para usuarios en CLI; Listas de control de acceso (ACL).	Capa de sockets seguros (SSL); Protocolo Secure Shell (SSH); IEEE 802.1X (función de autenticador); Protección de bucle invertido de STP; Secure Core Technology (SCT); Datos confidenciales seguros (SSD); Prevención de denegación de servicio (DoS); Listas de control de acceso (ACL).	Listas de control de acceso (ACL); IEEE 802.1X (función de autenticador); RADIUS, TACACS+; Filtrado de dirección MAC; Protección DoS; Prevención de ataque de DoS Protección de la unidad de datos de protocolo puente (BPDU) STP; Protección frente a bucle de árbol de extensión; Protocolo Secure Shell (SSH); Capa de sockets seguros (SSL).	Encuadre IP-MAC-Port-VID; Autenticación basada en puerto IEEE 802.1X/ MAC, Radio, VLAN Invitado; Defensa DoS; Inspección dinámica ARP (DAI); SSH v1/v2; SSL v2/v3/TLSv1;Seguridad Portuaria;Broadcast/Multicast/control de tormentas unicast desconocido	ACL; Firewall; AAA;Radius; HWTACAS;ARP;ICMP;URF;CPCAR; Black List
Rendimiento	128 Gbps	128 Gbps	75 Mbps	128 Gbps	128 Gbps
Factor Forma	1 U de Rack	1 U de Rack	1 U de Rack	1 U de Rack	1 U de Rack
Consumo de energía	46,60 W	46,60 W	39,5 W	47 W	46.60 W
Precio	**499,00**	475,6	240,86	2.000,00	2.174,00

Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 7

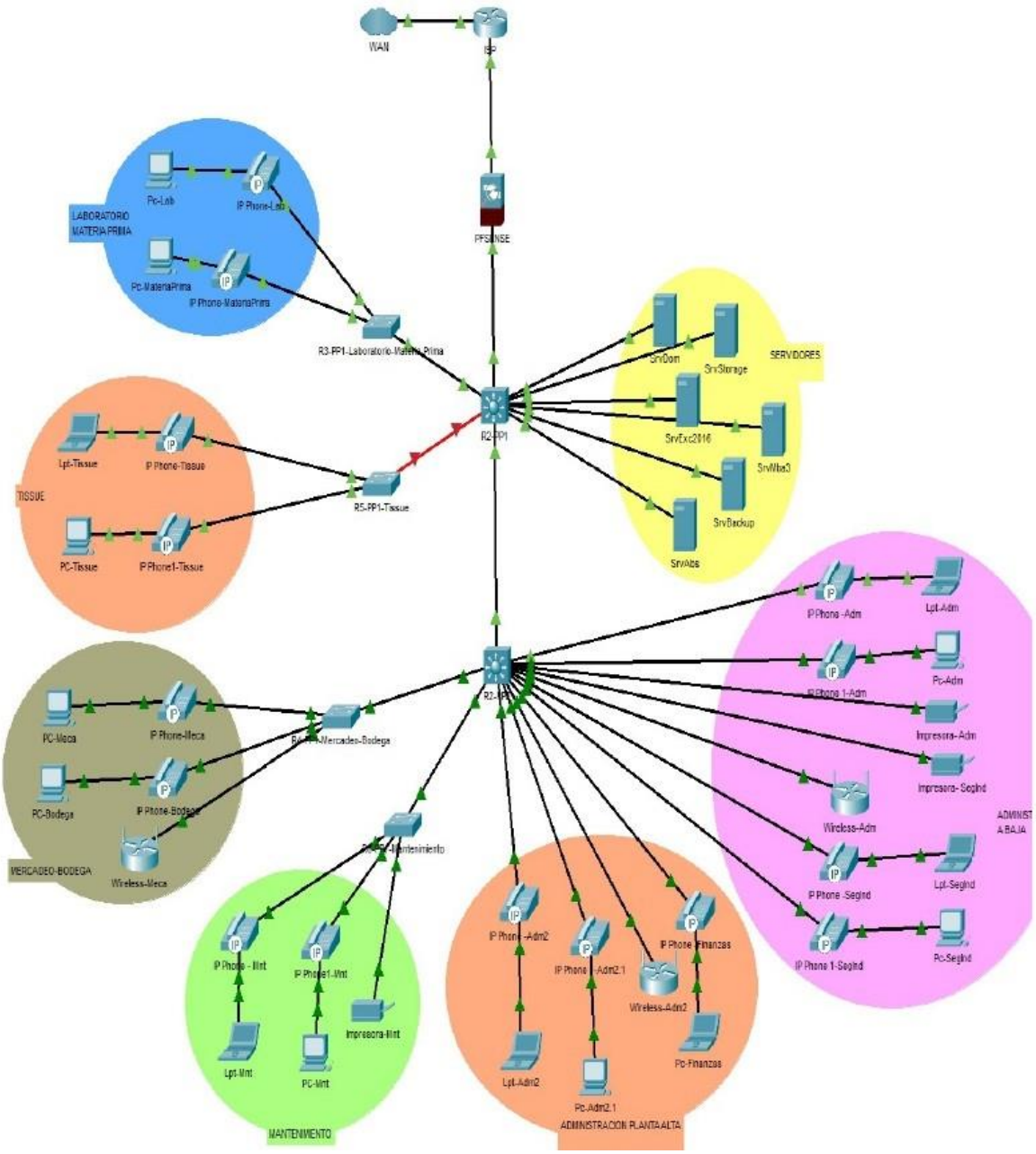
Topología del módulo de red de CAMPUS LAN de Nivel 3



Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 8

Topología del módulo de red de CAMPUS LAN de Nivel 2 Núcleo Colapsado



Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 9

Cronograma de Actividades Proyecto Técnico.

Meses	MARZO				ABRIL				MAYO				JUNIO				JULIO			
Número de semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Actividades																				
Objetivo Especifico 1																				
Compilar un inventario de hardware, software y configuración.																				
Verifique que SNMP MIB se admita en el router																				
Consultar y registrar objetos MIB del SNMP específicos del router.																				
Analizar datos para determinar umbrales.																				
Monitoreo del umbral de prueba & Solución de problemas inmediatos.																				
Objetivo Especifico 2																				
Direccionamiento IPV4																				
Diseño de Topología Lógica de la Red de Frontera																				
Diseño de Topología Física de la Red de Frontera																				
Seguridad de la red de frontera.																				
Objetivo Especifico 3																				
Simulación de la red de borde.																				
Comprobación de conectividad.																				
Análisis del tráfico de la red.																				
Objetivo Especifico 4																				
Determinar la inversión inicial																				
Determinar el precio del servicio, costos directos e indirectos																				
Calcular los parámetros de viabilidad del proyecto (VAN y TIR) para tener una estimación de su repercusión económica																				
Objetivo Especifico 5																				
Elaborar el documento del proyecto en base de los resultados obtenidos.																				
Revisar y corregir el borrador del articulo por parte del tutor.																				
Entregar el articulo académico final.																				
Tutorías																				

Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 10

Conjunto de E Actividades Realizadas a lo largo de la ejecución del Cronograma de Actividades

Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 11

Proyecto de Telefonía VoIP Proforma Bigexpert.

Dirección: Yánez Pinzón N26-56, edificio Frago Pb Local 2
Telf: +593 2 5149606/ +593 995889187 / +593 984696537
email : ventas@bigexpert.com.ec www.bigexpert.com.ec
RUC: 1792516145001

PROFORMA No. 2021-0000535

Quito, 30 AGOSTO 2021

Señores :	ABSORPELSA		
Dirección :	AV. MALDONADO S26-13 Y 21 AGOSTO		
RUC:			
Proyecto :	TELEFONIA IP UCM 6302 Y TELEFONOS A GIGABIT		
Atención :	ROIJAN PEREZ		
Correo :	rperez@absorpelsa.com.ec	Teléfono :	0987581193

ITEM	CANT.	DESCRIPCION	V.UNITARIO	V. TOTAL
1	1	SISTEMA DE TELEFONIA IP - GRANDSTREAM.	$ 1.414,00	$ 1.414,00
		INCLUYE:		
1.1	1	CENTRAL TELEFONICA GANDSTREAM UCM 6302		
1.2	1	GARANTIA EXTENDIDA GRANDSTREAM UCM 6302 3 AÑOS		
1.3	1	SERVICIOS DE CONFIGURACIÓN EN SITIO : * Configuración extensiones y usuarios * Troncales analógicas * Plan de marcación * Rutas entrantes y salientes * Grupos de timbrado * Grupos de captura * Salas de conferencia (audio) * IVR		
2		TELÉFONOS. INCLUYE CONFIGURACIÓN		
2.1	22	TELEFONO EMPRESARIAL GRANDSTREAM GRP 2603	$ 59,53	$ 1.309,66
2.2	1	TELÉFONO OPERADORA GRANDSTREAM GRANDSTREAM GRP2615	$ 150,61	$ 150,61
2.3	1	MODULO DE EXTENSIONES PARA TELÉFONOS DE OPERADORA GRANDSTREAM GBX20	$ 122,29	$ 122,29
			SUBTOTAL	$ 2.996,56
			12% IVA	$ 359,59
			TOTAL	$ 3.356,15

Forma de pago: 50 % con la orden de compra
25 % crédito 30 días
25 % crédito 60 días.

Validez de la oferta: 45 días

Tiempo de entrega: 5 DÍAS LABORABLES.

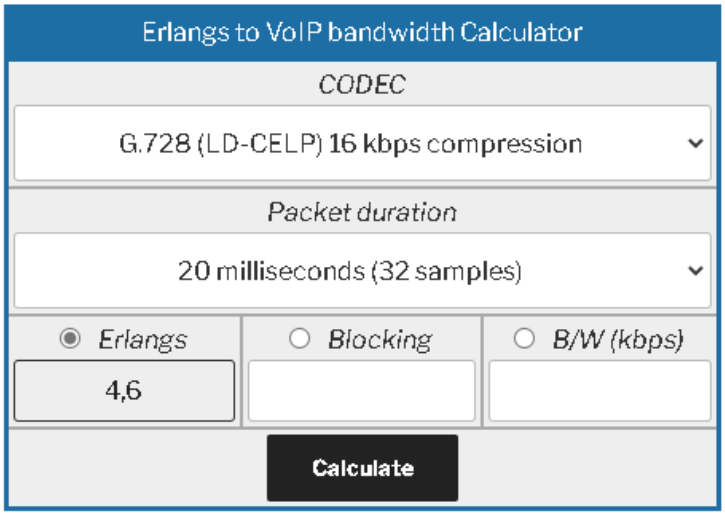
Nota: No incluye bienes y servicios no especificados en este documento
El cliente entregará las lineas telefónicas probadas y funcionando, pachadas en un patch panel en el mismo rack donde se instalará la central telefónica.

Confidencialidad: La información de este documento es de carácter confidencial y no puede ser divulgada a terceros.

Ing. Jacquelinne Huilcamaigua MSC.
BigExpert Cia. Ltda

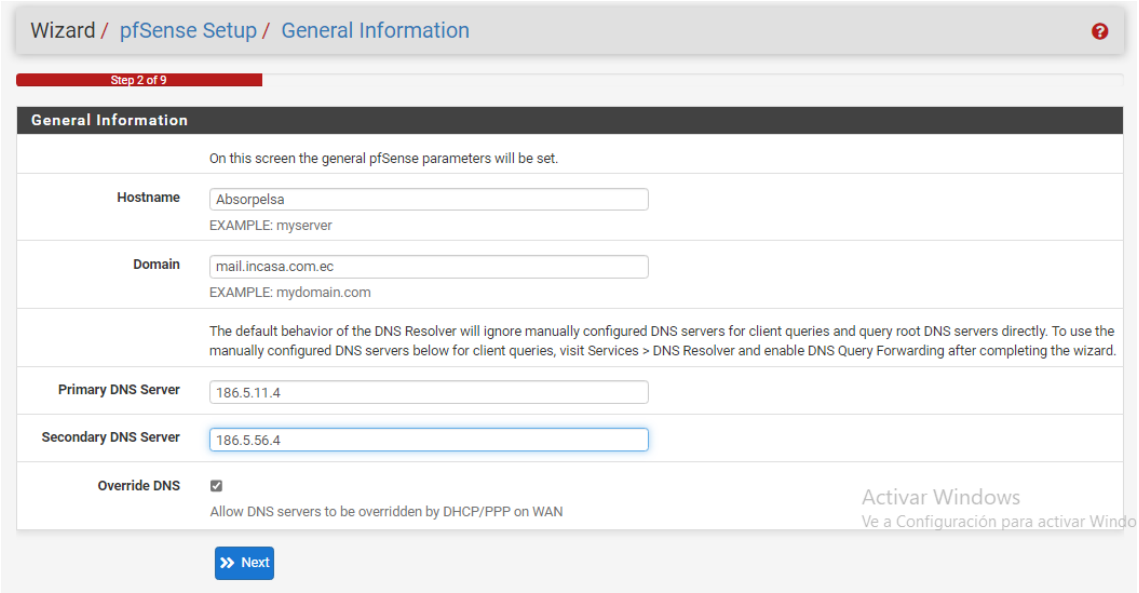
Anexo 12

Calculator Earlangs to VoIP bandwidth

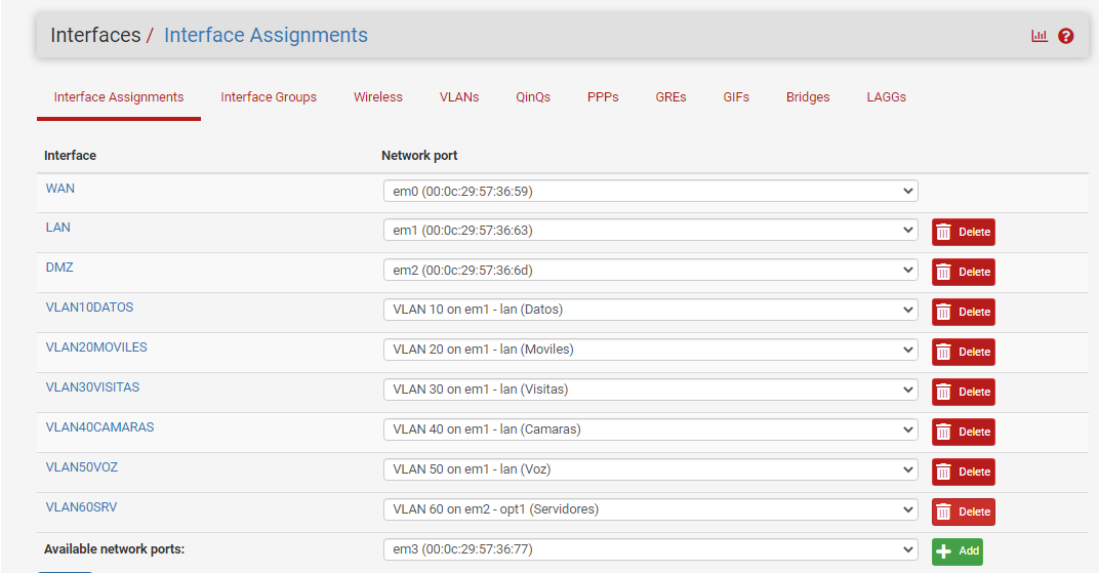


Anexo 13

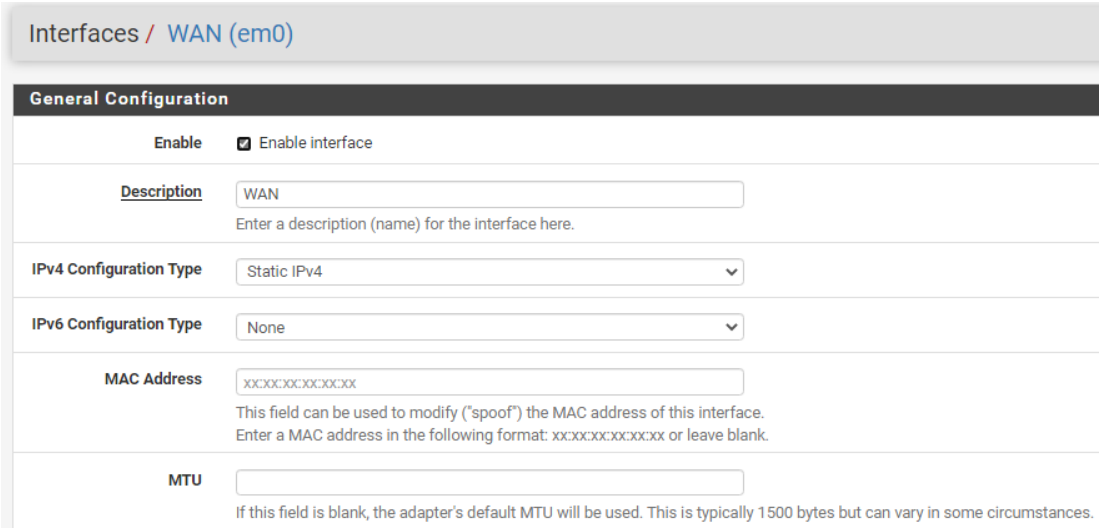
Configuración Inicial del Firewall de Nueva Generación PfSense



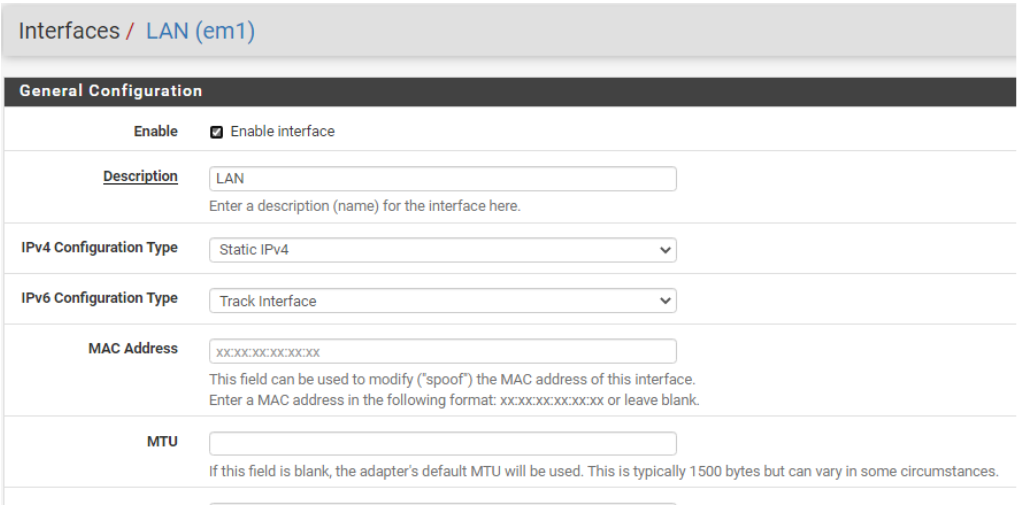
NGFW PfSense WAN, LAN y VLANs

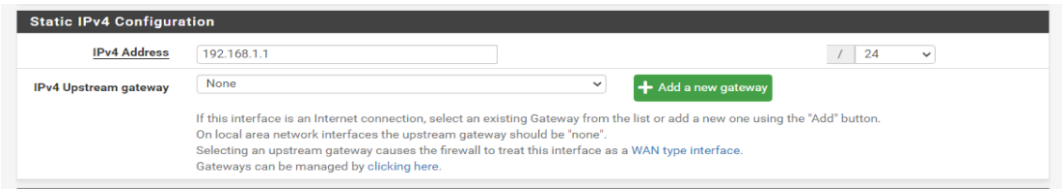


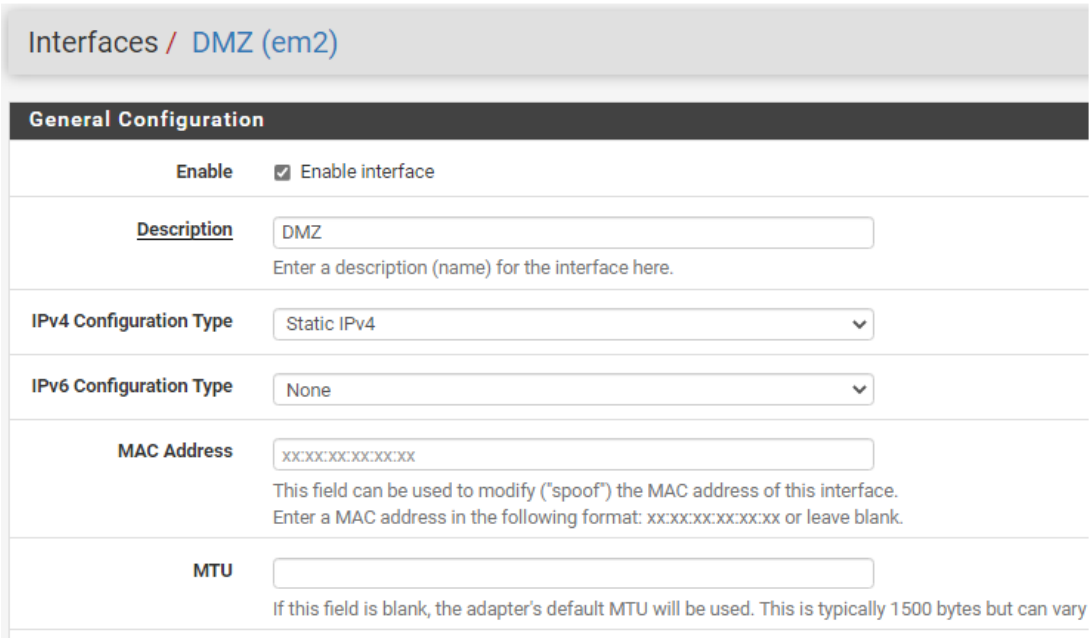
Elaborado por: Darwin Avalos y Andy Guanochanga



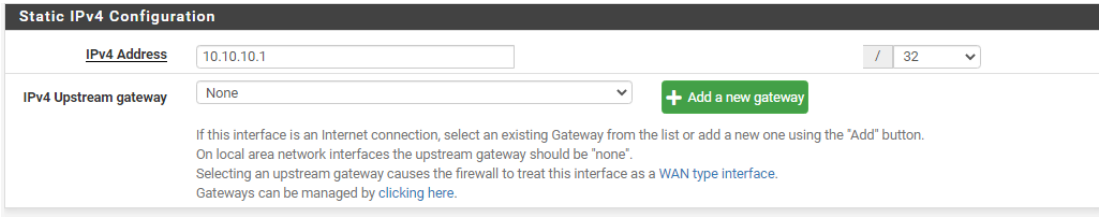
Elaborado por: Darwin Avalos y Andy Guanochanga



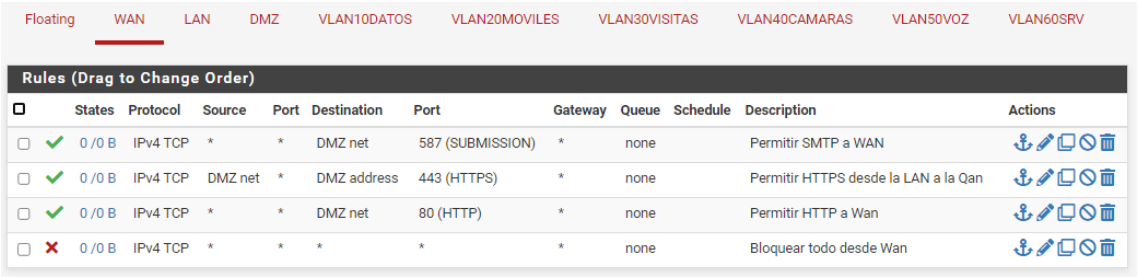




Elaborado por: Darwin Avalos y Andy Guanochanga

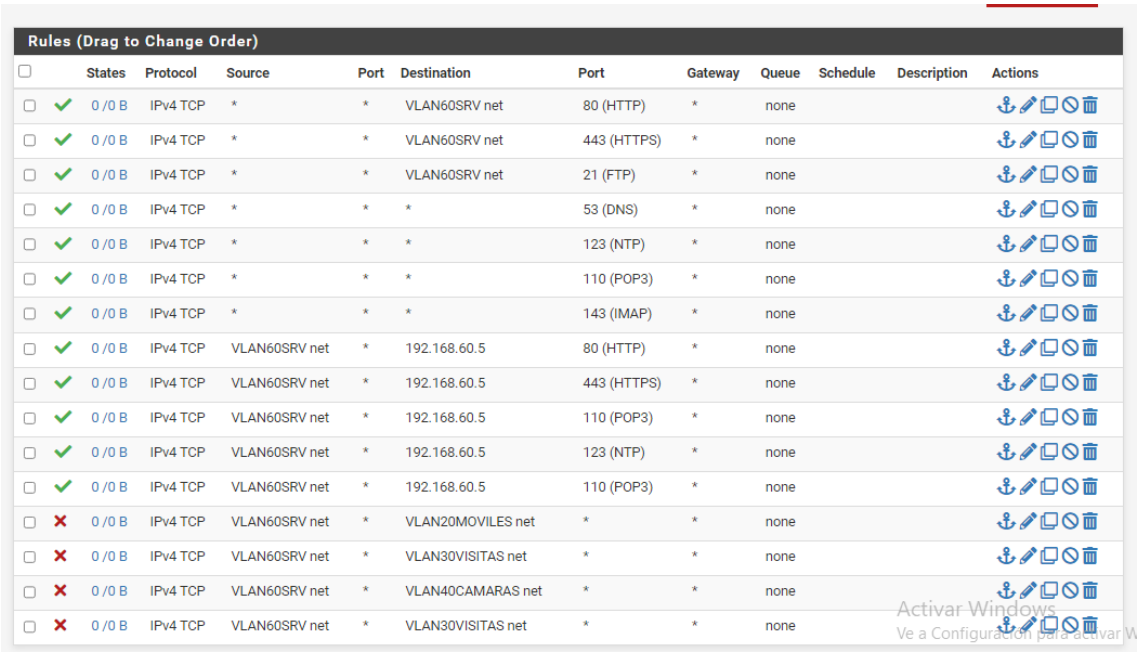


Reglas WAN

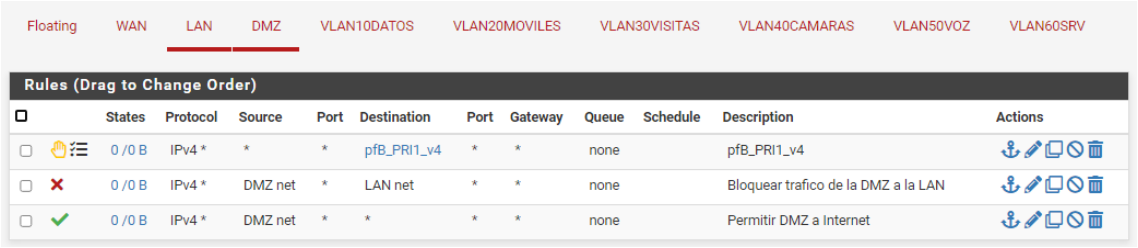


Elaborado por: Darwin Avalos y Andy Guanochanga

Reglas LAN



Reglas DMZ



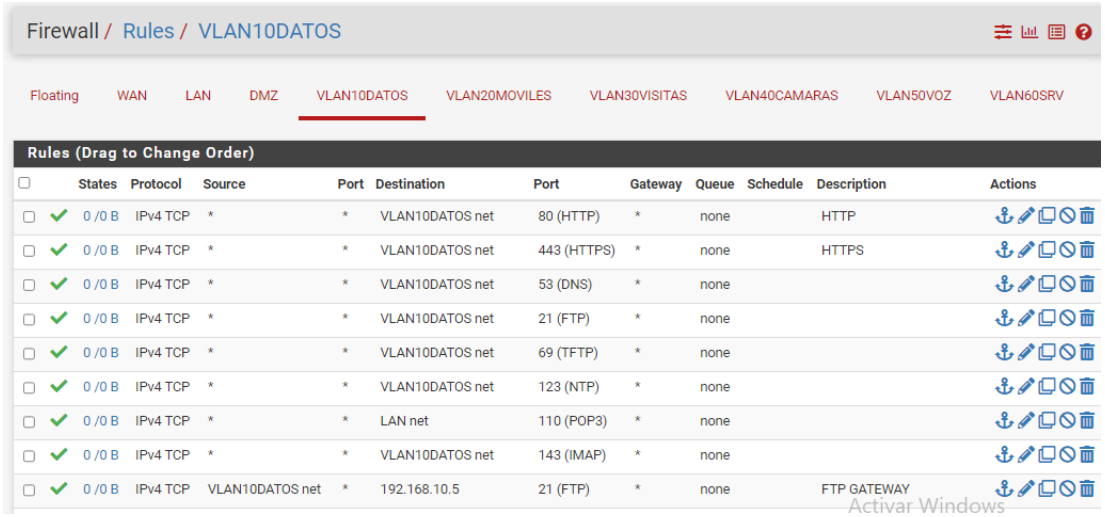
Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4	
	0 /0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Bloquear trafico de la DMZ a la LAN	
	0 /0 B	IPv4 *	DMZ net	*	*	*	*	none		Permitir DMZ a Internet	

Elaborado por: Darwin Avalos y Andy Guanochanga

Reglas VLAN10



Firewall / Rules / VLAN10DATOS

Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	80 (HTTP)	*	none		HTTP	
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	443 (HTTPS)	*	none		HTTPS	
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	53 (DNS)	*	none			
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	21 (FTP)	*	none			
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	69 (TFTP)	*	none			
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	123 (NTP)	*	none			
	0 /0 B	IPv4 TCP	*	*	LAN net	110 (POP3)	*	none			
	0 /0 B	IPv4 TCP	*	*	VLAN10DATOS net	143 (IMAP)	*	none			
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	192.168.10.5	21 (FTP)	*	none		FTP GATEWAY	

	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	192.168.10.5	21 (FTP)	*	none		FTP GATEWAY	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	192.168.10.5	53 (DNS)	*	none		DNS	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	192.168.10.5	69 (TFTP)	*	none		TFTP	
	0 /0 B	IPv4 *	VLAN10DATOS net	*	VLAN20MOVILES net	*	*	none		Bloqueo vlan10 a vlan20	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN30VISITAS net	21 (FTP)	*	none		VLAN10 A VLAN30	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN30VISITAS net	69 (TFTP)	*	none		VLAN10 A VLAN30 TFTP	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN40CAMARAS net	*	*	none		Bloqueo vlan10 a vlan40	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN50VOZ net	5004 (RTP)	*	none		vlan10 a vlan50	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN50VOZ net	5060 (SIP)	*	none		vlan10 a vlan50 SIP	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN50VOZ net	4569	*	none		vlan10 a vlan50 iax	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN60SRV net	110 (POP3)	*	none		vlan10 a vlansrv	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN60SRV net	143 (IMAP)	*	none		vlan10 a vlansrv	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN60SRV net	1433	*	none		vlan10 a vlansrv	
	0 /0 B	IPv4 TCP	VLAN10DATOS net	*	VLAN60SRV net	68	*	none		vlan10 a vlansrv	

Reglas VLAN20

Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 TCP	*	*	VLAN20MOVILES net	80 (HTTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN20MOVILES net	443 (HTTPS)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN20MOVILES net	21 (FTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN20MOVILES net	69 (TFTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN20MOVILES net	123 (NTP)	*	none			
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	192.168.20.5	21 (FTP)	*	none		Gateway	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	192.168.20.5	69 (TFTP)	*	none		vlan20 a gateway	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	VLAN10DATOS net	*	*	none		bloqueo vlan20 a vlan10	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	VLAN30VISITAS net	*	*	none		bloqueo vlan20 a vlan30	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	VLAN40CAMARAS net	*	*	none		bloqueo vlan20 a vlan40	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	VLAN50VOZ net	*	*	none		bloqueo vlan20 a vlan50	
0 /0 B	IPv4 TCP	VLAN20MOVILES net	*	VLAN60SRV net	*	*	none		bloqueo vlan20 a vlan60	

Elaborado por: Darwin Avalos y Andy Guanochanga

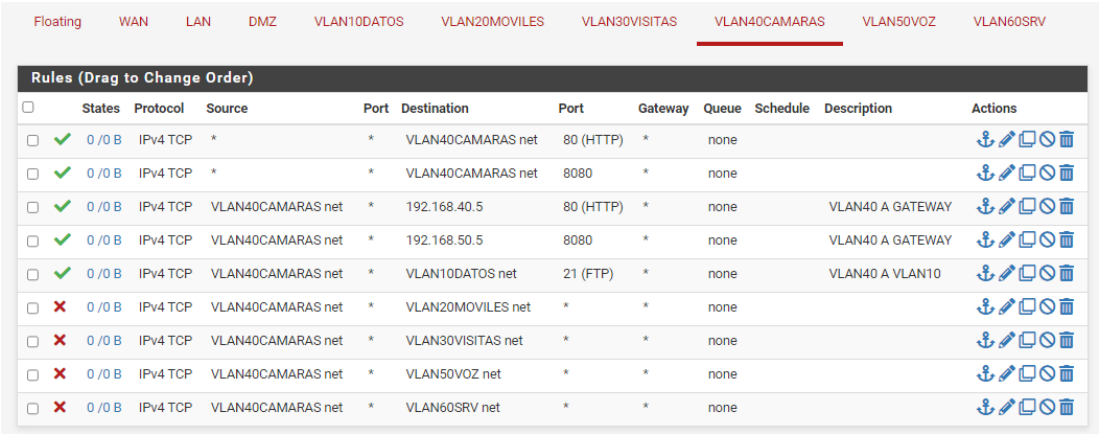
Reglas VLAN30

Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 TCP	*	*	VLAN30VISITAS net	80 (HTTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN30VISITAS net	443 (HTTPS)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN30VISITAS net	21 (FTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN30VISITAS net	69 (TFTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN30VISITAS net	123 (NTP)	*	none			
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	192.168.30.5	21 (FTP)	*	none		vlan30 a gateway	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	192.168.30.5	53 (DNS)	*	none		vlan30 a gateway	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	192.168.30.5	69 (TFTP)	*	none		vlan30 a gateway	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	VLAN10DATOS net	*	*	none		Bloqueo vlan30 a vlan10	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	VLAN20MOVILES net	*	*	none		Bloqueo vlan30 a vlan20	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	VLAN40CAMARAS net	*	*	none		Bloqueo vlan30 a vlan40	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	VLAN50VOZ net	*	*	none		Bloqueo vlan30 a vlan50	
0 /0 B	IPv4 TCP	VLAN30VISITAS net	*	VLAN60SRV net	*	*	none		Bloqueo vlan30 a vlan60	

Reglas VLAN40



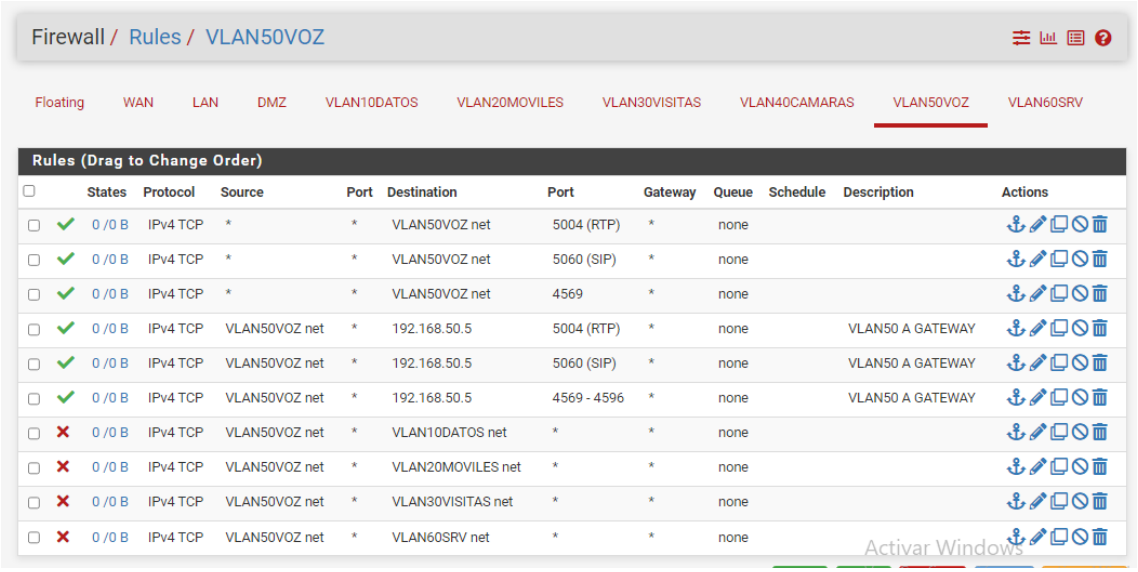
Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 TCP	*	*	VLAN40CAMARAS net	80 (HTTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN40CAMARAS net	8080	*	none			
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	192.168.40.5	80 (HTTP)	*	none		VLAN40 A GATEWAY	
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	192.168.50.5	8080	*	none		VLAN40 A GATEWAY	
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	VLAN10DATOS net	21 (FTP)	*	none		VLAN40 A VLAN10	
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	VLAN20MOVILES net	*	*	none			
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	VLAN30VISITAS net	*	*	none			
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	VLAN50VOZ net	*	*	none			
0 /0 B	IPv4 TCP	VLAN40CAMARAS net	*	VLAN60SRV net	*	*	none			

Elaborado por: Darwin Avalos y Andy Guanochanga

Reglas VLAN50



Firewall / Rules / VLAN50VOZ

Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 TCP	*	*	VLAN50VOZ net	5004 (RTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN50VOZ net	5060 (SIP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN50VOZ net	4569	*	none			
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	192.168.50.5	5004 (RTP)	*	none		VLAN50 A GATEWAY	
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	192.168.50.5	5060 (SIP)	*	none		VLAN50 A GATEWAY	
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	192.168.50.5	4569 - 4596	*	none		VLAN50 A GATEWAY	
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	VLAN10DATOS net	*	*	none			
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	VLAN20MOVILES net	*	*	none			
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	VLAN30VISITAS net	*	*	none			
0 /0 B	IPv4 TCP	VLAN50VOZ net	*	VLAN60SRV net	*	*	none			

Reglas VLAN60

Floating | WAN | LAN | DMZ | VLAN10DATOS | VLAN20MOVILES | VLAN30VISITAS | VLAN40CAMARAS | VLAN50VOZ | VLAN60SRV

Rules (Drag to Change Order)

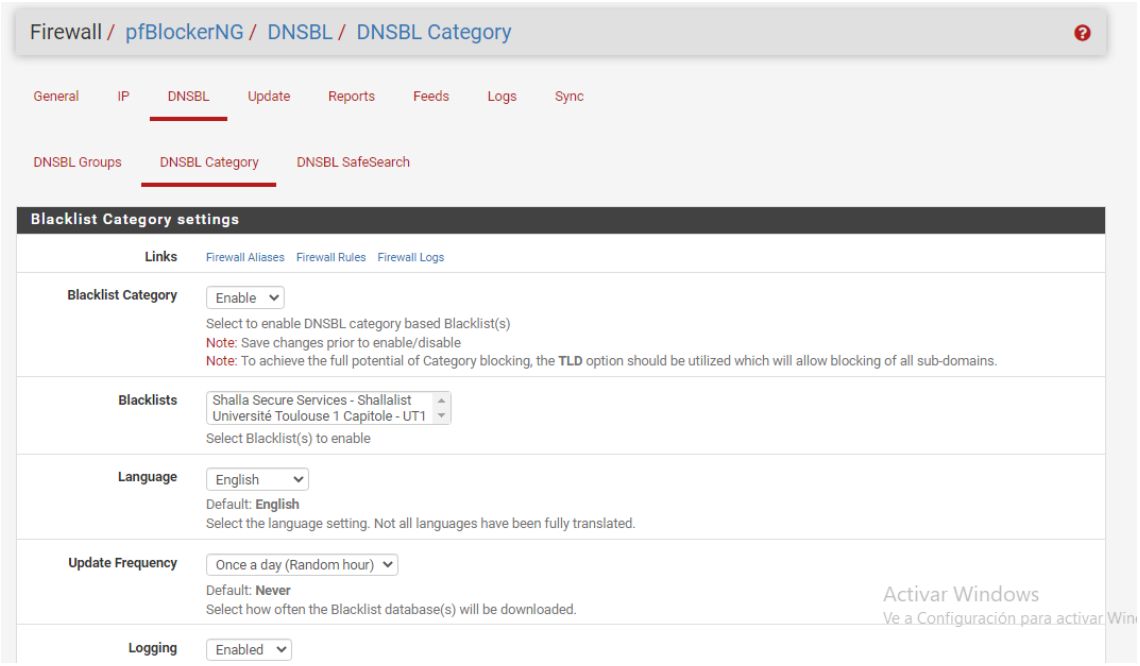
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 TCP	*	*	VLAN60SRV net	80 (HTTP)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN60SRV net	443 (HTTPS)	*	none			
0 /0 B	IPv4 TCP	*	*	VLAN60SRV net	21 (FTP)	*	none			
0 /0 B	IPv4 TCP	*	*	*	53 (DNS)	*	none			
0 /0 B	IPv4 TCP	*	*	*	123 (NTP)	*	none			
0 /0 B	IPv4 TCP	*	*	*	110 (POP3)	*	none			
0 /0 B	IPv4 TCP	*	*	*	143 (IMAP)	*	none			
0 /0 B	IPv4 TCP	VLAN60SRV net	*	192.168.60.5	80 (HTTP)	*	none			

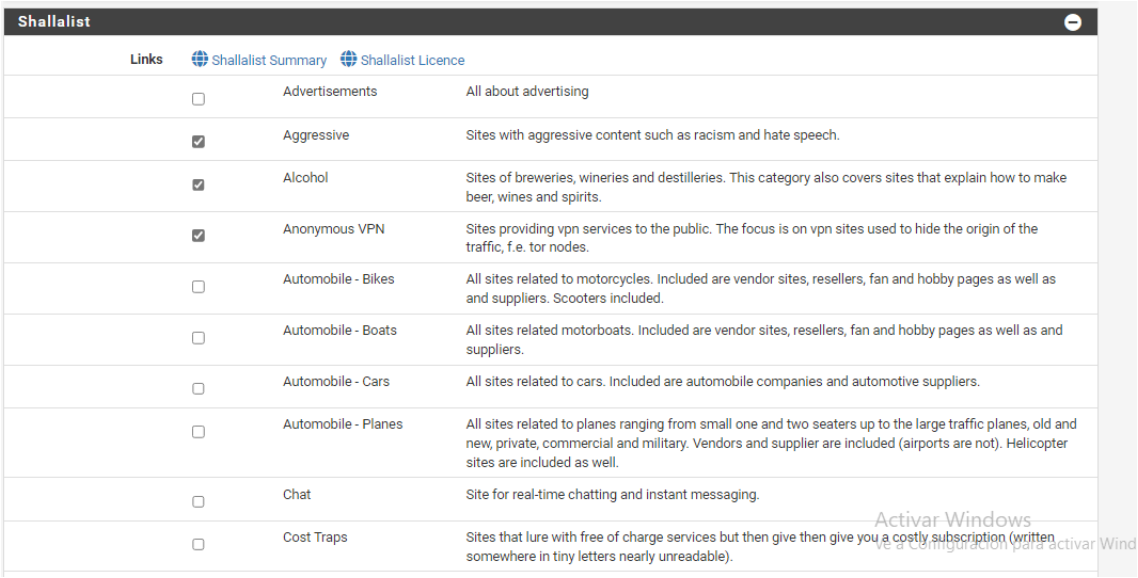
☐	✓	0 /0 B	IPv4 TCP	VLAN60SRV net	*	192.168.60.5	443 (HTTPS)	*	none	
☐	✓	0 /0 B	IPv4 TCP	VLAN60SRV net	*	192.168.60.5	110 (POP3)	*	none	
☐	✓	0 /0 B	IPv4 TCP	VLAN60SRV net	*	192.168.60.5	123 (NTP)	*	none	
☐	✓	0 /0 B	IPv4 TCP	VLAN60SRV net	*	192.168.60.5	110 (POP3)	*	none	
☐	✗	0 /0 B	IPv4 TCP	VLAN60SRV net	*	VLAN20MOVILES net	*	*	none	
☐	✗	0 /0 B	IPv4 TCP	VLAN60SRV net	*	VLAN30VISITAS net	*	*	none	
☐	✗	0 /0 B	IPv4 TCP	VLAN60SRV net	*	VLAN40CAMARAS net	*	*	none	
☐	✗	0 /0 B	IPv4 TCP	VLAN60SRV net	*	VLAN30VISITAS net	*	*	none	

Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 14

Configuración del PfBlocker (Instagram, Facebook, YouTube)



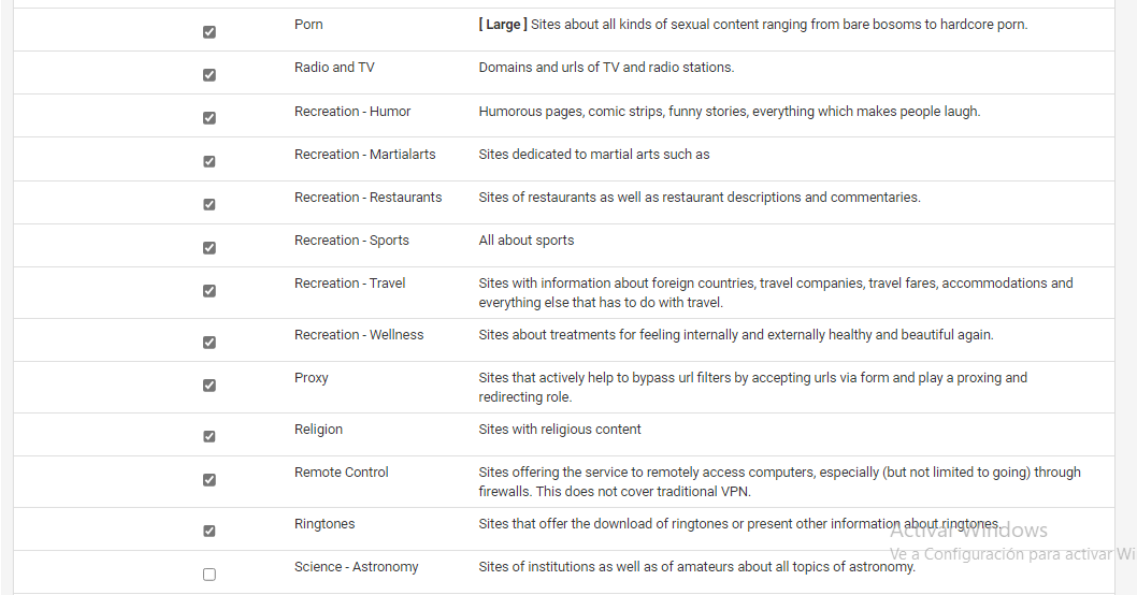


Shallalist

Links: Shallalist Summary | Shallalist Licence

☐	Advertisements	All about advertising
☑	Aggressive	Sites with aggressive content such as racism and hate speech.
☑	Alcohol	Sites of breweries, wineries and destilleries. This category also covers sites that explain how to make beer, wines and spirits.
☑	Anonymous VPN	Sites providing vpn services to the public. The focus is on vpn sites used to hide the origin of the traffic, f.e. tor nodes.
☐	Automobile - Bikes	All sites related to motorcycles. Included are vendor sites, resellers, fan and hobby pages as well as and suppliers. Scooters included.
☐	Automobile - Boats	All sites related motorboats. Included are vendor sites, resellers, fan and hobby pages as well as and suppliers.
☐	Automobile - Cars	All sites related to cars. Included are automobile companies and automotive suppliers.
☐	Automobile - Planes	All sites related to planes ranging from small one and two seaters up to the large traffic planes, old and new, private, commercial and military. Vendors and supplier are included (airports are not). Helicopter sites are included as well.
☐	Chat	Site for real-time chatting and instant messaging.
☐	Cost Traps	Sites that lure with free of charge services but then give then give you a costly subscription (written somewhere in tiny letters nearly unreadable).

Elaborado por: Darwin Avalos y Andy Guanochanga



☑	Porn	**[Large]** Sites about all kinds of sexual content ranging from bare bosoms to hardcore porn.
☑	Radio and TV	Domains and urls of TV and radio stations.
☑	Recreation - Humor	Humorous pages, comic strips, funny stories, everything which makes people laugh.
☑	Recreation - Martialarts	Sites dedicated to martial arts such as
☑	Recreation - Restaurants	Sites of restaurants as well as restaurant descriptions and commentaries.
☑	Recreation - Sports	All about sports
☑	Recreation - Travel	Sites with information about foreign countries, travel companies, travel fares, accommodations and everything else that has to do with travel.
☑	Recreation - Wellness	Sites about treatments for feeling internally and externally healthy and beautiful again.
☑	Proxy	Sites that actively help to bypass url filters by accepting urls via form and play a proxing and redirecting role.
☑	Religion	Sites with religious content
☑	Remote Control	Sites offering the service to remotely access computers, especially (but not limited to going) through firewalls. This does not cover traditional VPN.
☑	Ringtones	Sites that offer the download of ringtones or present other information about ringtones.
☐	Science - Astronomy	Sites of institutions as well as of amateurs about all topics of astronomy.

☐	Shopping	Sites offering online shopping and price comparisons.
☑	Social Networking	Sites bringing people together (social networking) be it for friendship or for business.
☐	Spyware	Sites that try to actively install software or lure the user in doing so in order to spy the surfing behaviour (or worse). The home calling sites where the collected information is sent, are listed too.
☐	Tracker	Sites keeping an eye on where you surf and what you do in a passive manner. Covers web bugs, counters and other tracking mechanisms in web pages that do not interfere with the local computer yet collect information about the surfing person for later analysis.
☐	Update Sites	List to allow necessary downloads from vendors.
☐	URL shortener	Sites offering short links for URLs.
☑	Violence	Sites about killing and harming people. Covers anything about brutality and beastiality.
☐	Warez	Collection of sites offering programs to break licence keys, licence keys themselves, cracked software and other copyrighted material.
☐	Weapons	Sites offering all kinds of weapons or accessories for weapons
☐	Webmail	Sites that offer web-based email services.
☐	Web Phone	Sites that enable user to phone via the Internet. Any site where users can voice-chat with each other.
☑	Web Radio	Sites that offer listening to music and radio live streams.
☑	Web TV	Sites offering TV streams via Internet.

Enable All Disable All

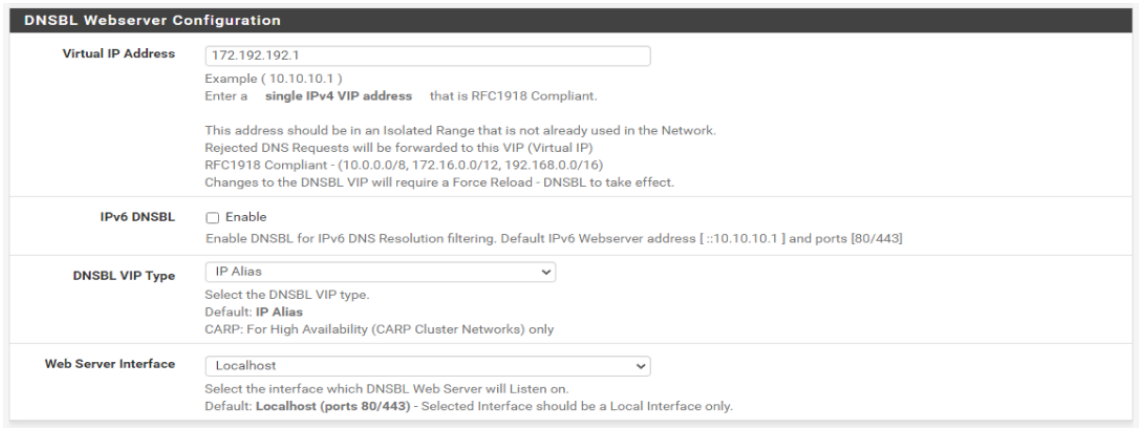
Elaborado por: Darwin Avalos y Andy Guanochanga

pfBlockerNG

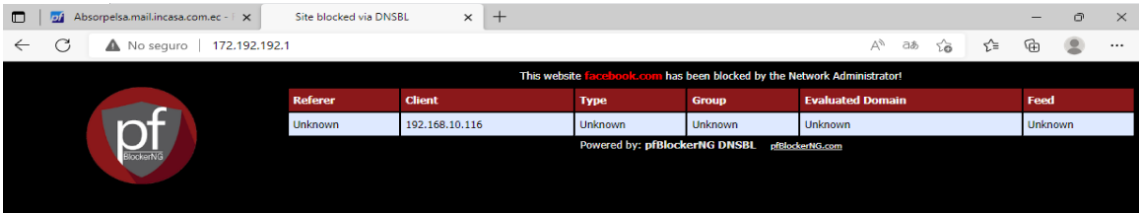
MaxMind:

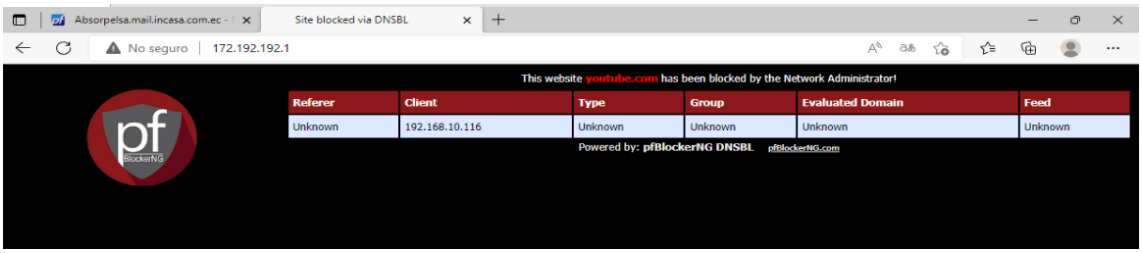
IP	0	0	0	0
DNSBL	35	343	10.20	46

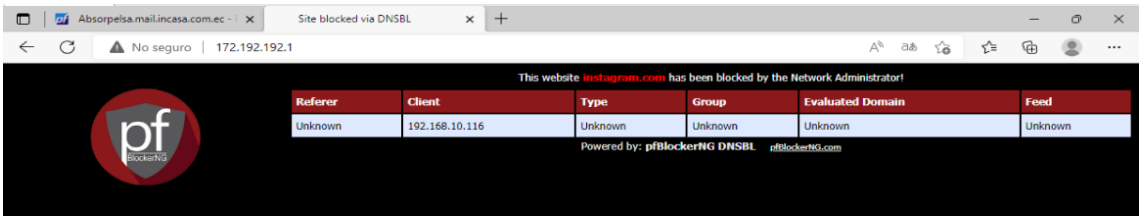
Alias	Count	Packets	Updated	
pfB_PRI1_v4	17,635	0	Jul 14 05:55:15	(1)
DNSBL_ADs_Basic	145,549	35	Jul 14 06:50:11	
DNSBL_UT1	679	0	Jul 14 06:50:10	



Elaborado por: Darwin Avalos y Andy Guanochanga







Elaborado por: Darwin Avalos y Andy Guanochanga

Anexo 15

Comprobación de conectividad hacia la LAN Simulación del Prototipo

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : incasa.local
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.10.116
   Máscara de subred . . . . . . . . . . . . : 255.255.255.128
   Puerta de enlace predeterminada . . . . . : 192.168.10.5

C:\Users\pasantesist>ping 186.3.59.110

Haciendo ping a 186.3.59.110 con 32 bytes de datos:
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 186.3.59.110:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\pasantesist>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : incasa.local
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.30.22
   Máscara de subred . . . . . . . . . . . . : 255.255.255.224
   Puerta de enlace predeterminada . . . . . : 192.168.30.5

C:\Users\pasantesist>ping 186.3.59.110

Haciendo ping a 186.3.59.110 con 32 bytes de datos:
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 186.3.59.110:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\pasantesist>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : incasa.local
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.60.10
   Máscara de subred . . . . . . . . . . . . : 255.255.255.240
   Puerta de enlace predeterminada . . . . . : 192.168.60.5

C:\Users\pasantesist>ping 186.3.59.110

Haciendo ping a 186.3.59.110 con 32 bytes de datos:
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo=272ms TTL=64
Respuesta desde 186.3.59.110: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 186.3.59.110:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 272ms, Media = 68ms
```

Elaborado por: Darwin Avalos y Andy Guanochanga