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

AUTORES:
JUAN FERNANDO CAHUEÑAS MALIZA
JONATHAN ANDRÉS LIZARZABURU TORO

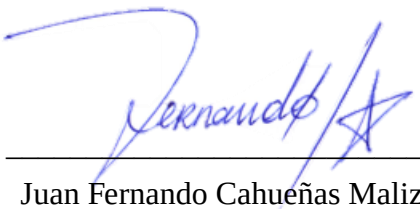
TUTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

Quito, agosto de 2019

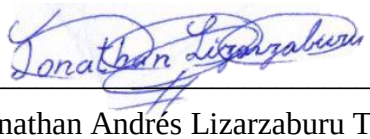
CESIÓN DE DERECHOS DE AUTOR

Nosotros, Juan Fernando Cahueñas Maliza y Jonathan Andrés Lizarzaburu Toro, con documentos de identificación N° 1804342259 y N° 0202100954 respectivamente, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: "DISEÑO DE LA RED DE FRONTERA PARA EL CENTRO DE FORMACIÓN CONTINUA SAN BARTOLO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA", mismo que ha sido desarrollado para optar por el título de Ingeniero Electrónico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservarnos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.



Juan Fernando Cahueñas Maliza
C.I. 1804342259



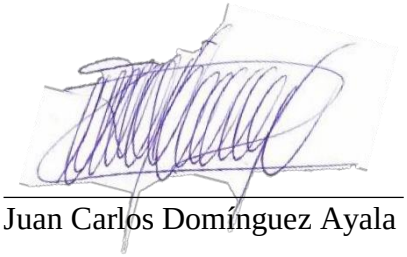
Jonathan Andrés Lizarzaburu Toro
C.I. 0202100954

Quito, agosto de 2019

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, "DISEÑO DE LA RED DE FRONTERA PARA EL CENTRO DE FORMACIÓN CONTINUA SAN BARTOLO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA" realizado por Juan Fernando Cahueñas Maliza y Jonathan Andrés Lizarzaburu Toro, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto de 2019.



Juan Carlos Domínguez Ayala
C.I: 1713195590

DEDICATORIA

Al Ente Supremo que ha colocado las oportunidades y a las personas indicadas en mi camino, quien ha abierto más de una ventana cuando la vida me ha cerrado una puerta.

A mi Madre Mery en el cielo, que puede ver desde lo alto una meta más que he cumplido y por el amor infinito que me da, aunque no esté a mi lado.

A mi Padre Rafael, quien pese a los percances que le ha puesto la vida me acompaña, me aconseja y me apoya incondicionalmente.

A mis tías Amparito, Nelly y Pamela por su cuidado, preocupación y apoyo.

A mis primos Santiago y Alexandra, que me han brindado su cariño y atención sin importar la distancia y que han visto en mi un ejemplo a seguir.

A mis amigos más cercanos que me han dado el empujón para confiar en mí mismo, en especial al Jonathan Lizarzaburu. ¡Gracias Bro!

Juan Fernando Cahueñas Maliza

DEDICATORIA

Quiero agradecer primero a Dios, por la oportunidad que me brindó para probarme a mí mismo y quien no me ha abandonado en ningún momento en este largo camino de aprendizaje y autosuperación.

A mi mamá y hermana, quienes me han dado el amor, cariño y paciencia, que han sido el apoyo en los buenos y malos momentos de mi vida y que se encuentran muy orgullosas de mí por este logro personal.

A Fernando Cahueñas; coautor del presente proyecto, gracias por el aliento y la paciencia.

Jonathan Andrés Lizarzaburu Toro

AGRADECIMIENTO

Extendemos nuestro profundo agradecimiento a la Universidad Politécnica Salesiana, y a cada uno de los docentes de la Carrera de Ingeniería Electrónica, quienes nos han impartido sus conocimientos con el propósito de ser profesionales que dejen el alto el nombre de la institución.

A nuestra familia por el cariño y apoyo incondicional, a nuestros amigos y compañeros quienes nos han extendido su ayuda y han sido soporte dentro y fuera de las aulas.

A nuestro tutor; Ingeniero Juan Carlos Domínguez, que con gran predisposición nos encaminó en esta última etapa de vida universitaria y nos ha preparado con su experiencia para el campo profesional.

A todos aquellos que; directa o indirectamente, nos brindaron su ayuda para hacer posible el desarrollo de este trabajo.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El Centro de Formación Continua San Bartolo (CFCSB); extensión Sur de la Universidad Politécnica Salesiana, de la ciudad de Quito, se dedica a la preparación y capacitación técnica de niños, niñas y adolescentes para que se integren a la sociedad aportando al mercado laboral.

El presente proyecto toma como referencia la red de campus de la institución, y se diseñó la infraestructura de frontera que asegura las comunicaciones y la conectividad hacia el exterior. En base a la Guía de Diseño Empresarial de Borde de Internet de Cisco se obtuvo una red de frontera convergente que se acopla con las necesidades y requerimientos de seguridad, alta disponibilidad, escalabilidad y calidad de servicio.

El propósito del diseño de red de borde es el de coadyuvar a la misión del centro optimizando la red de campus junto con aplicativos de software libre que permitan controlar el volumen de tráfico de voz, datos y video que se genera en las actividades diarias de la institución, la distribución eficiente del ancho de banda mejorará la experiencia de los usuarios y los mecanismos que aseguren una alta disponibilidad en cualquier momento.

Se aplicaron las metodologías PPDIOO de Cisco para el Diseño de Redes y Top-Down, que aportaron un proceso sistemático para el diseño de cada uno de los módulos que conforman la red de frontera para el centro.

Finalmente, se modeló la topología de frontera en programas especializados donde se verificó, optimizó y se documentó los resultados para una futura implementación.

ABSTRACT

The “Centro de Formación Continua San Bartolo” (CFCSB); a south extension of “Universidad Politécnica Salesiana”, of Quito city, is dedicated to the preparation and technical capacitation of children and teenagers, to ensure their integration into society contributing to the working market.

The current Project takes as a reference, the campus’ network of the institution, and the edge infrastructure has been designed to guarantee the communications and the outward connectivity. Based on the Cisco Internet Edge Guide, a convergent border infrastructure was obtained, which engages itself with security necessities and requirements, high availability, scalability, and a better-quality service for students, teachers, administrative staff and guest.

The perimeter network’s design was made with the purpose of contributing to the mission’s center, optimizing the campus’ network alongside open source apps which allow to control the amount of voice traffic, data and videos that are generated on daily activities inside the institution. The efficient distribution of the bandwidth will improve the user’s experience and the mechanisms that ensure that the network is always going to be available.

Cisco PPDIOO and Top-Down methodologies were applied, which provided a systematic process for the design of each one of the modules that form the border network for the center.

Finally, the topology of the border network was modeled with specialized programs and was also verified, optimized and the results were documented for future implementation.

INTRODUCCIÓN

El presente proyecto recoge en cuatro capítulos el desarrollo del diseño de la red de frontera para el CFCSB, en base a los lineamientos definidos en la Guía de Diseño Empresarial de Borde de Internet de Cisco junto con las Metodologías PPDIOO y Top-Down para el Diseño de Redes; proponiendo una infraestructura convergente, de alta disponibilidad y segura para el desarrollo de las actividades por parte de los estudiantes, docentes y personal administrativo.

Para alcanzar este objetivo, primero se ha considerado el diseño de la red interna elaborado por alumnos de la Universidad para el levantamiento de la línea base que brinde un panorama de las necesidades que no hayan sido consideradas en la primera propuesta.

En la segunda etapa se detalla el diseño de los módulos de conectividad a Internet, acceso remoto y VPN, módulo WAN junto con la propuesta de las topologías lógica, física y el direccionamiento IPv4/IPv6. Se realizó la selección tanto de equipos como la del Firewall de Siguiente Generación (NGFW) para satisfacer las necesidades de los usuarios de la red de la institución. Además, se desarrolló el análisis para el dimensionamiento del tráfico, la propuesta de mecanismos de calidad de servicio y seguridad que permitan un uso controlado de la red, optimizando los procesos para incrementar la productividad dentro del CFCSB.

En la tercera etapa del proyecto han sido verificados los resultados obtenidos en las fases previas, modelando el comportamiento del tráfico con el uso del software de simulación OPNET Modeler para obtener parámetros de Jitter, Throughput, Delay y Packet Loss dentro de los estándares permisibles de una red moderna.

En esta etapa también se muestran los resultados de la simulación de la topología realizada en el programa GNS3 y la virtualización de máquinas en VMware para la configuración de los equipos activos y del NGFW.

Seguidamente, se realizó el análisis costo-beneficio para verificar la viabilidad del proyecto, arrojando resultados positivos de la misma.

Finalmente, se documentaron las configuraciones, resultados y presupuestos con el fin de brindar las herramientas para la futura implementación de la red de frontera.

CAPÍTULO 1
ANTECEDENTES

1.1 Planteamiento del Problema

La UPS, en su aspiración de brindar educación y capacitación en distintas ramas técnicas y tecnológicas a jóvenes, niños y niñas; abrirá las puertas del CFCSB al sur de la capital para ofrecer valiosas oportunidades de formación y capacitación en áreas técnicas para ayudar a su incorporación idónea en el mercado laboral.

Actualmente el centro ya cuenta con el diseño de red de campus, mismo que fue desarrollado en un proyecto técnico por parte de alumnos de la Universidad Politécnica Salesiana; sin embargo, en este diseño no se contempló el estudio de la red perimetral y tampoco se realizaron las mediciones para verificar su comportamiento con un número elevado de usuarios. Por otra parte, no se definieron las zonas críticas que generan una alta carga de datos, lo que podría provocar una posible saturación de la red y un mal funcionamiento de esta.

La red de campus carece de los módulos para el acceso a Internet, acceso remoto y conexión WAN para la comunicación con el Campus Sur de la Universidad, además de que la red se encuentra vulnerable a amenazas internas y externas dada la inexistencia de firewalls, dispositivos de seguridad adaptables, sistemas de prevención y detección de intrusiones; tampoco se ha dimensionado un sistema de alimentación ininterrumpida para impedir que los dispositivos del rack principal sean afectados por problemas eléctricos.

1.2 Justificación del Problema

En el presente proyecto de tesis, propone el diseño de una nueva red de frontera en base a la Guía de Diseño Empresarial de Borde de Internet de Cisco para proveer de conectividad a Internet, sucursales remotas y usuarios móviles, proporcionando escalabilidad y flexibilidad a partir del diseño de la red de campus del CFCSB, el cual será un ambiente orientado para la acción educativa de los jóvenes, niños y niñas para su capacitación con el uso de recursos tecnológicos.

Al no existir un adecuado diseño de red definido con un nivel mínimo de seguridades se requiere una solución que brinde una conexión con mecanismos de calidad de servicio y seguridad en base a software libre que garanticen que el trabajo y la

operatividad de los procesos comunicacionales y administrativos del centro se cumplan con fluidez.

Los módulos que conforman la guía de diseño de Cisco brindan los servicios esenciales de redes y servidores de comercio electrónico, conectividad y zona perimetral (DMZ), acceso remoto, VPN y WAN basados en Internet y utilizados en ambientes de redes empresariales. De esta manera se plantea proveer seguridad en las conexiones entre usuarios hacia los servicios externos como Internet, datos, video, PSTN y a su vez lograr que la red de frontera actúe como la puerta de enlace del Centro de Formación Continua al resto del ciberespacio manteniendo una experiencia de navegación segura.

1.3 Objetivos

1.3.4 Objetivo General

Diseñar la red de frontera en el Centro de Formación Continua San Bartolo en base a la Guía de Diseño Empresarial de Borde de Internet de Cisco para proveer de conectividad a estudiantes, docentes, administrativos y visitantes.

1.3.5 Objetivos Específicos

- Establecer la línea base de la red perimetral para que sea determinado el estado actual de la red del Centro de Formación Continua San Bartolo.

- Diseñar los módulos de Acceso a Internet, Acceso Remoto y Conexión WAN en base al Diseño Empresarial de Borde de Internet de Cisco con los respectivos lineamientos para que sea asegurada la conectividad y la seguridad lógica.

- Evaluar los parámetros de Calidad de Servicio (QoS) de la red perimetral para que sea conocido el ancho de banda, pérdida de paquetes y latencia.

- Aplicar el análisis coste-beneficio para que sea determinada la factibilidad del diseño.

- Simular la red de borde del Centro de Formación Continua San Bartolo para

que sea comprobada la calidad de la red mediante los parámetros el Throughput, Retardo y Jitter.

1.4 Marco Conceptual

1.4.4 Metodología del Diseño

La propuesta de diseño de la red de frontera se la realizará en base a metodologías validadas por Cisco con el fin entregar al CFCSB una red que cumpla con las necesidades y requerimientos de funcionalidad, seguridad y de conectividad orientada a la formación teórica, técnica y práctica de sus alumnos.

1.4.5 Metodología PPDIOO

La metodología PPDIOO de Cisco adopta un ciclo de vida que se puntualiza en seis etapas, con el fin de reducir el costo total de propiedad, mejorar la disponibilidad de sus servicios, mejorar la calidad de la experiencia del usuario y reducir los gastos operativos. (Al-shawi, 2016)

1.4.6 Metodología Top-Down Network y Bottom-Up

Existen dos enfoques para el diseño de redes, los cuales brindan estrategias y soluciones para el desarrollo de nuevos productos. En la Tabla 1.1 se muestra un cuadro comparativo con las metodologías Top-Down y Bottom-Up para el nuevo diseño de la red de frontera.

Tabla 1.1 Comparación entre las Metodologías Top-Down y Bottom-Up

Top-Down	Bottom-Up
Los trabajos se alteran y se completan según la autoridad superior	Se centra en las aplicaciones que impulsan la necesidad de crear una red nueva o rediseñar una preexistente
Provee tanto a los diseñadores como al cliente de una perspectiva global del diseño deseado	Se empieza en la capa más baja del modelo OSI
Proporciona un diseño que es apropiado tanto para los requerimientos actuales como para un despliegue futuro	Da como resultado una red inapropiada para los servicios requeridos, usándose principalmente cuando se solicita una respuesta rápida

Determinación de la Metodología para el nuevo diseño de la red de frontera del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Como se puede observar, el diseño de redes con la Metodología Top-Down ofrece notables beneficios al ser comparada con su contraparte y se enfoca en la tecnología

necesaria y el posterior diseño partiendo desde la capa aplicación del modelo OSI. (Team Nuggets, 2016)

La metodología Top-Down se organiza en cuatro fases principales del diseño de red.

- **Identificar las necesidades y objetivos de su cliente:** Esta fase se cubre: Análisis de requerimientos y caracterización de la red existente donde se incluye la arquitectura y el rendimiento. (Oppenheimer, s.f)
- **Diseño Lógico de la red: Durante esta fase, se desarrollan:** Una topología modelo, se diseña un modelo de direccionamiento, se selecciona los protocolos de conmutación y enrutamiento. El diseño lógico también incluye la planificación de la seguridad, diseño de la administración, investigación inicial sobre qué proveedores de servicios pueden cumplir con los requisitos de acceso remoto y WAN. (Oppenheimer, s.f)
- **Diseño Físico de la red:** En esta fase se seleccionan tecnologías y productos específicos que realizan el diseño lógico, se retoma la investigación de los proveedores de servicios y debe completarse durante esta fase. (Oppenheimer, s.f)
- **Pruebas, Optimización y Documentación del diseño de la red:** En los pasos finales se escriben e implementan un plan de prueba a través de la construcción de un prototipo, se optimiza el diseño y se documenta el trabajo. (Oppenheimer, s.f).

1.4.7 Módulos del Diseño Empresarial de Borde de Internet de Cisco

El Perímetro o Borde de Internet es uno de los segmentos más importantes que forman parte de una Red Empresarial, ya que es donde la red corporativa se encuentra con la Internet pública. Cada vez que los usuarios de la red tienen acceso a servicios como correo electrónico, herramientas de colaboración o acceden a sitios web, los recursos de la red corporativa deben permanecer accesibles y seguros. (CISCO, 2015)

El Modelo Cisco de Distribución de Borde sigue un diseño modular de bloques que ofrece flexibilidad y personalización al momento de diseñar la red como se indica a continuación en la Figura 1.1.

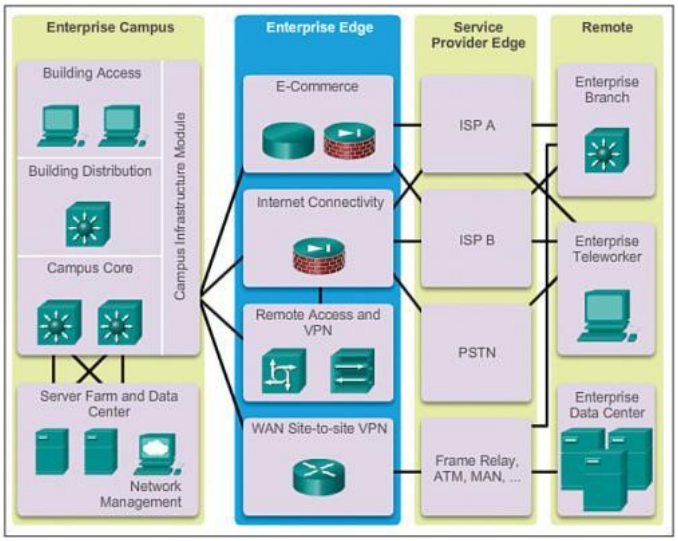
1.4.8 Módulo E-Commerce

Es aquel que permite a las empresas soportar aplicaciones de comercio electrónico a través de Internet. Incluyen servidores web, de aplicaciones y de bases de datos,

firewall y sistemas de prevención de intrusos en redes (IPS).

La nueva red de frontera del CFCSB no cuenta con el diseño de este módulo, debido a que la red tiene una orientación educativa y no comercial.

Figura 1.1 Modelo Cisco de Distribución de Borde



Módulos del Modelo Cisco de Distribución de Borde. Fuente: (Cisco Networking Academy, 2014)

1.4.9 Módulo de Conectividad a Internet

Este bloque permite un acceso seguro a Internet por parte de los usuarios corporativos a la vez que brindan servicios al público en general, como lo son: Servidores FTP, SMTP, DNS y HTTP. En este módulo se encuentran los firewalls que se encargan de asegurar la conexión a base a políticas e inspección de paquetes a nivel de aplicación.

Este módulo también acepta conexiones de Redes Privadas Virtuales (VPN) por parte de usuarios y sitios remotos, además de las conexiones provenientes de la red telefónica conmutada (PSTN), que previo a su autenticación se reenvían al Módulo VPN.

1.4.10 Módulo Acceso Remoto y VPN

Este módulo se encarga de proporcionar acceso corporativo a usuarios remotos en base a protocolos SSL, VPN o Easy VPN y que acceden a través del Módulo de Conectividad a Internet.

1.4.11 Módulo WAN

Las sucursales adoptan una salida a internet con la finalidad de proporcionar un enlace de respaldo redundante para la red WAN a través de dispositivos dedicados que se encargan de esta funcionalidad de copia de seguridad, de esta manera se asegura la

continuidad y disponibilidad de la empresa.

1.4.12 Enlace de Datos

Son los enlaces arrendados por aparte de un proveedor de servicios. A nivel de la ciudad de Quito las empresas que se encargan de brindar soluciones de conectividad y acceso a Internet son: CNT, Telconet, Celerity, etc.

1.4.13 Seguridad de la Red

La Seguridad de la Red abarca los mecanismos implementados; tanto en hardware como en software, para salvaguardad la integridad de los datos y de la propia red. Estos mecanismos se basan en protocolos, estándares, reglas y políticas que bloqueen o dificulten el software malicioso y reduzcan el riesgo de afectar a la infraestructura y/o a la información, los objetivos que se desean alcanzar al momento de ejecutar políticas de seguridad en una red son: Confidencialidad, Integridad, Autenticación, Disponibilidad y No Repudio.

Cabe mencionar que una protección absoluta es imposible de implementar, pero si se pueden alcanzar altos niveles de seguridad.

Los mecanismos de seguridad que serán incluidos en el diseño de la red de frontera de la institución son:

- Firewall
- Listas de Control de Acceso (ACL)
- Filtrado de Contenido (Listas Blancas y Listas Negras)
- Autenticación de usuarios remotos
- Segmentación de red

1.4.14 Firewall

Los Firewalls o Contrafuegos son los componentes más importantes del sistema, ya que estos proveen de seguridad a la información; también constituyen la primera línea de defensa contra los ataques de seguridad y se encuentran configurados con reglas o políticas que bloquean o aceptan determinado tráfico de red y por medio de la implementación de base de datos confiables es posible incrementar el nivel de seguridad que estos ofrecen.

Los tipos de Firewalls existentes son:

- Filtrado de paquetes
- Proxy a nivel circuito
- Proxy a nivel de aplicación
- Stateful Firewall
- UTM (Unifield Threat Management)
- NGFW (Next Generation Firewall)

1.4.15 Firewalls de Siguiente Generación (NGFW)

Los Firewalls de Siguiente Generación son la evolución de los Firewalls básicos, incluyen funcionalidades primarias, pero se adiciona la inspección de aplicación y demás características avanzadas. Los requisitos que debe cumplir un equipo de seguridad para ser definido como NGFW son:

- Contar con las capacidades de un firewall de primera generación.
- Contar con indicadores que muestren la capacidad de acción al momento de identificar las actividades de un programa maligno.
- Brindar una íntegra visibilidad de la red.
- Reducir el nivel de complejidad y de costes.
- Facilidad para integrarse e interactuar con soluciones de seguridad de terceros.
- Salvaguardar de la inversión.

1.4.16 Trafico de Red

Son los paquetes que circulan por una ruta para ingresar y salir de un sistema en flujos heterogéneos y consistentes para múltiples utilidades y aplicaciones. Se clasifican en:

- **Tráfico Elástico:** Aquel que puede ajustarse a los retardos o rendimientos de una red sin disminuir la calidad y requerimiento de las aplicaciones, por ejemplo: Conexión remota, correo electrónico, acceso web, gestión de red, transferencia de archivos.
- **Tráfico No Elástico:** Aquel que no puede adaptarse con facilidad a las variaciones de retardos o rendimientos de una red.

1.4.17 Calidad de Servicio

Calidad de servicio es aquella propiedad que debe ser incorporada en el diseño de una

red convergente con el objetivo de proporcionar los parámetros necesarios de Ancho de Banda, Rendimiento, Jitter, Pérdidas de Paquetes, Retardo y Latencia para que así se cubran las demandas sin degradar la experiencia de los usuarios finales. (ISO, 2019)

En el desarrollo del presente proyecto de tesis se aborda el análisis de los parámetros de QoS descritos en la Tabla 1.2.

Tabla 1.2 Parámetros para el Análisis

Parámetro	Descripción
Throughput (Rendimiento)	Especifica cuántos datos son transferidos a través de la red, se expresa en paquetes por segundo y es medio después de la transmisión de datos.
Jitter (Variación del retardo)	Expresa la variación que es experimentada entre dos retardos consecutivos al momento de la transmisión y el procesamiento de los datos, son causados cuando existe congestión en la red y pueden llegar a afectar seriamente a la calidad del flujo en paquetes de audio y video.
Delay (Retardo)	Es el tiempo que tarda en transmitirse un bit de origen a destino, es causado por errores en el envío de datos, distancia, procesamiento, enlaces, conectores, entre otros.
Packet Loss (Pérdida de Paquetes)	Se refiere a los paquetes que no han sido transmitidos exitosamente debido a la baja calidad del medio de transmisión, la congestión en una red, fallos de dispositivos o al sobre flujo del buffer afectando de manera directa al receptor.

Parámetros de Calidad de servicio a ser analizados. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

El tráfico de las redes modernas exige mayor cantidad de recursos debido al número de usuarios conectados como también el aumento de dispositivos que tienen acceso al Internet, por tal razón en la Tabla 1.3 se muestran los valores permisibles de acuerdo con la ITU G.144 y la RFC3393 para voz, video y datos.

Los datos que no sean voz o video pueden tener un comportamiento predecible y dependiendo del tipo de aplicación que se esté utilizando no son altos consumidores de recursos en una red.

Tabla 1.3 Requerimientos de Tráfico para Voz, Video y Datos

Tráfico	Delay	Jitter	LOSS	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
Datos	–	–	–	–

Requerimientos para la implementación de Calidad de Servicio en Voz, Video y Datos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

1.4.18 Políticas y Clases de Calidad de Servicio

Las políticas de calidad de servicio se basan en la revisión, clasificación y la posterior priorización de paquetes que circulan a través de una red en base a la cantidad de Ancho de Banda disponible. Para la definición de clases se deben organizar individualmente los flujos de tráfico que van desde Best-Effort hasta Reenvío Express según la distribución de la red. (Oracle, 2014)

La función de los mecanismos o algoritmos de encolamiento es de asegurar que los paquetes sean enviados de manera eficiente en orden de prioridad o tan rápido como sea posible, este proceso puede producir congestión ya que los datos no son enviados con la velocidad deseada y son colocados en colas para su futura transmisión viéndose reflejado su impacto en el ancho de banda, Jitter, pérdidas de paquetes y retardo.

Los mecanismos de encolamiento utilizados para la propuesta de Calidad de Servicio de la red de frontera se muestran en la Tabla 1.4.

Tabla 1.4 Mecanismos de Encolamiento

Encolamiento	Descripción
FIFO (First In First Out)	- Es el Sistema de encolamiento más básico utilizado - No requiere de clasificación o planeación - No puede alterar el orden en el que los paquetes se envían - Retrasa tramas cortas detrás de plazos más largos
PQ (Priority Queuing)	- Programa el tráfico de manera que las colas de prioridad más alta siempre obtienen el servicio - Se pueden establecer un número máximo de 4 colas, llamadas: alta, medio, normal y baja - Puede mejorar considerablemente la latencia de paquetes de alta prioridad - Retrasa tramas cortas detrás de plazos más largos
WFQ (Weighted Fair Queuing)	- Clasifica paquetes en flujos - El número de colas alcanza las 4096 por interfaz - Utiliza cualquier ancho de banda que está disponible para reenviar el tráfico de los flujos

Mecanismos de encolamiento para administrar y evitar congestión en la red. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

1.4.19 Niveles de Calidad de Servicio

Los niveles de Calidad de Servicio se refieren a las capacidades que tiene una red para realizar cierto servicio para un tráfico específico; para el desarrollo del proyecto serán analizados los siguientes: Best-Effort, Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ).

En la Tabla 1.5 se indican las ventajas y desventajas de cada nivel con el objetivo de elegir el que se apeguen a las necesidades y requerimientos del diseño.

Tabla 1.5 Ventajas y Desventajas de los Mecanismos de Calidad de Servicio

Mecanismo	Ventajas	Desventajas
Best-Effort	- No es necesario hacer algún cambio en la red - Aumento de la capacidad en los ISP	- Se sobredimensionan las capacidades - Retados mayores a 400 ms - Uso de diferentes técnicas para mitigar los efectos causados por pérdidas
IntServ (Integrated Services)	- Facilita que la red mantenga políticas de red integrada - La posibilidad de crear reglas de QoS para flujos discretos	- Todos los elementos deben mantener el estado e intercambiar mensajes de señalización por cada flujo - Se necesitan mensajes periódicos de refrescos para mantener la sesión, lo que aumenta el tráfico en la red
DiffServ (Differentiated Services)	- Sin reservación del canal - Reducción de la carga de la red - Se basa en el marcado de paquetes - No hay reserva de recursos por flujo - No distingue flujos individuales, clasifica los paquetes en categorías (según el ToS solicitado)	- En los servicios no hay reserva (no están garantizados) - Las garantías de QoS no son tan severas como en IntServ, pero en muchos casos se consideran suficientes.

Comparación de ventajas y desventajas entre los Mecanismos de Calidad de Servicio. Fuente: (Juca, 2016)

1.4.20 Ancho de Banda

Ancho de Banda es el conjunto de datos o recursos informáticos que son enviados a través de una conexión de red en un determinado tiempo.

La Comisión Federal de Comunicaciones (FCC); agencia reguladora de comunicaciones internacionales e interestatales a través de radio, televisión, cable y satélite a en los Estados Unidos, ha definido valores aproximados de Ancho de Banda para el desempeño adecuado de las aplicaciones utilizadas en una red, en base a la utilización típica del medio con varios dispositivos conectados.

En la siguiente tabla se muestra un listado de las aplicaciones y las velocidades necesarias para su adecuado desempeño.

Tabla 1.6 Ancho de Banda estimada por Aplicación

Actividad	Velocidad Mínima (Mbps)
Navegación General	1
Correo y Mensajería	0.1
Llamadas por Internet (VoIP)	Menor que 0.5
Redes Sociales	0.25
Llamada personal con Video Estándar	1.5
Descarga de Archivos	10
Backup	10

Velocidades aproximadas necesarias para la operación adecuada de cada aplicación. Fuente: (Federal Communications Commission, 2018)

1.4.21 Código Abierto (Open Source)

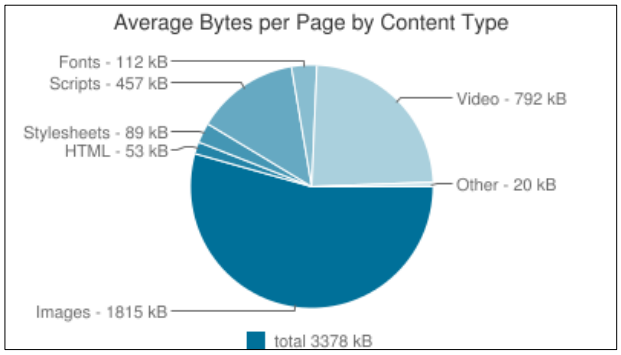
En el campo de las tecnologías, el Código Abierto es utilizado para la creación o levantamiento de proyectos, productos o iniciativas orientados a la comunidad de manera colaborativa que permita a los desarrolladores tener la posibilidad de modificar o compartir su diseño a partir de un código fuente al que cualquiera puede acceder, por mencionar a algunos de ellos: Proyecto GNU, Documentación Libre (FDL), Creative Commons, etc. Las características que brinda la herramienta Open Source son su flexibilidad, fiabilidad, seguridad y constante de desarrollo. (Khosrow-Pour, 2018)

1.4.22 Páginas Web

También llamada página digital o página electrónica, una página web es aquel documento que contienen texto, imágenes, video, sonido, enlaces, programas, etc. Y que forma parte de la red informática mundial y se despliegan navegadores de Internet.

Para el diseño del presente proyecto de tesis se ha considerado el tamaño promedio de una página web hasta el año 2017 para el desarrollo del análisis del ancho de banda mínimo necesario para el CFCSB.

Figura 1.2 Tamaño promedio de una página web



Tamaño promedio de una página web hasta el año 2017. Fuente: (Camarena, 2017)

1.4.23 Alta Disponibilidad y Redundancia

Los conceptos de alta disponibilidad y redundancia son parte de la capacidad que tiene una red para recuperarse de fallos causados por agentes internos o externos a niveles lógicos y físicos de la manera más rápida posible, para que sean minimizadas las afectaciones en el servicio. (Menéndez, 2016)

CAPÍTULO 2
SITUACIÓN INICIAL

2.1 Situación Geográfica

El CFCSB se encuentra ubicado al sur de la ciudad de Quito, en la calle Joaquín Gutiérrez y Teodoro Gómez de la Torre; está delimitado al norte por la Metalúrgica Ecuatoriana, al sur por Almacenera Almacopio S.A, al este por La Industria Harinera S.A y al oeste por el Conjunto Habitacional Jardín del Sur. Anteriormente en este predio funcionaba el Liceo del Sur.

El área del terreno es de aproximadamente 6882 m^2 y en él se encuentran dos edificios que serán utilizados como aulas de capacitación para ofrecer oportunidades de preparación y capacitación a los niños, niñas y adolescentes.

Figura 2.1 Fachada Principal de la institución

Vista de la entrada y fachada principal del CFCSB. Fuente: (Google Maps, 2019)

2.2 Descripción de la Red Actual

La red de campus se diseñó basándose con el modelo de Cisco de núcleo colapsado, cuenta con tres racks: El rack de piso (central) brinda conectividad a las dos plantas del edificio principal, y los racks de pared (secundarios) para el auditorio, los Talleres de la Escuela San Patricio (TESPA) y a la Unidad Educativa San Patricio (UESPA).

La propuesta de cableado estructurado contempló la utilización de cable par trenzado 6A.

Los equipos activos presentes en el diseño de la red se muestran en la Tabla 2.1 a continuación.

Tabla 2.1 Dispositivos activos en la red de campus

Dispositivo	Marca	Cantidad
Switch Layer 3 Catalyst 3850	Cisco	1
Switches US-48	Ubiquiti	6
Switches US-24	Ubiquiti	1
Unifi UAP-AC-PRO	Ubiquiti	27

Listado de equipos activos utilizados en la red de campus del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

El direccionamiento del diseño de red de campus partió de la red 172.16.0.0/17 y fueron configuradas las siguientes VLANs en el Switch L3: Docentes y Administrativos (VLAN 10), Alumnos (VLAN 20), Visitantes (VLAN 30) y Gestión (VLAN 40).

Dentro de la mejora del rendimiento y seguridad de la red interna del centro se han configurado VLANs en el Switch de Core para los grupos: Docentes y Administrativos, Alumnos de los programas TESPA/UESPA, Visitantes y Gestión; de esta manera se garantiza que los datos que transmite cada dependencia sean independientes entre sí. Así también, se elaboraron listas de acceso (ACLs) como parte de las políticas de seguridad, las cuales permiten el tráfico de los protocolos: HTTP, HTTPS, DHCP, DNS.

A continuación, en la Tabla 2.2, se muestra el estimado de puntos de acceso y datos descritos en el diseño inicial con el fin de realizar un análisis que sea coherente a las necesidades del centro.

Tabla 2.2 Puntos de red para el CFCSB

Área de Trabajo	Puntos de Red	Puntos de Acceso
Planta Baja	126	8
Planta Alta	20	6
TESPA	75	8
Auditorio-Cafetería	8	5
Total	229	27

Puntos de red estimados en las diferentes áreas del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

2.3 Problemas Detectados

Los problemas que fueron detectados en el análisis de la situación inicial fueron:

- El diseño de red campus no contempla un sistema de seguridad en la frontera.
- Se requiere aplicar criterios de calidad de servicio para la priorización del tráfico entrante y saliente de la red.
- No se ha dimensionado un conjunto de bloques para los equipos de la red de frontera.
- Se debe implementar políticas de seguridad preventivas como: bloqueo en tráfico InterVLAN, bloqueo de puertos, filtrado de contenido, protección contra virus y spam.
- No se ha dimensionado un enlace WAN para la conexión con el campus sur de la Universidad Politécnica Salesiana.
- Se debe distribuir el ancho de banda provisto por el Proveedor de Servicios de Internet (ISP) para brindar a los usuarios una conexión estable.
- No se cuenta con un sistema de alimentación ininterrumpida para la protección de los equipos instalados en el rack de piso.

2.4 Análisis de Requerimientos

Se analizaron los resultados obtenidos con las simulaciones realizadas en OPNET Molder del desempeño de la red y Packet Tracer para la distribución y configuración de dispositivos en la topología, el número aproximado de estudiantes, docentes, personal administrativo de la red de campus para el CFCSB.

Se debe considerar el Ancho de Banda mínimo requerido por el centro para la contratación de un ISP y así cumplir con las exigencias básicas de conexión y la cobertura necesaria para brindar conectividad entre la red del centro y el campus sur de la Universidad Politécnica Salesiana, conexiones remotas para colaboradores por medio de Redes Privadas Virtuales (VPN) basadas en OpenVPN y una Troncal de Red Telefónica Conmutada Pública (PSTN) para las transferencias de llamadas en tiempo real entre los teléfonos móviles y fijos de la red interna hacia su matriz el campus sur.

El valor agregado del proyecto es la utilización de aplicativos de software libre que simplifiquen la configuración, el uso de equipos, administración y que a la vez unifiquen los servicios de conectividad y seguridad.

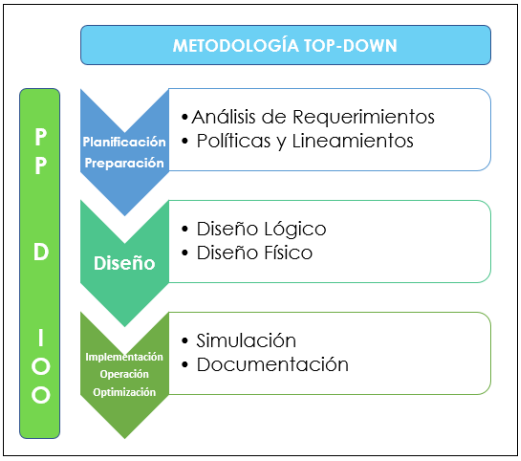
CAPÍTULO 3
PROPUESTA DE DISEÑO DE LA RED DE BORDE

3.1 Metodología

El desarrollo metodológico del diseño de la red de frontera para el CFCSB sigue lineamientos de PPDIOO como bases para el diseño de la red y se añade un enfoque Top-Down con el cual se reconocen las necesidades y cómo cubrirlas siguiendo un proceso sistemático que resulte en una infraestructura que aporte una conexión confiable, segura y tolerante a fallos para el crecimiento profesional de sus estudiantes y el desempeño laboral de los docentes y personal administrativos.

En la siguiente figura se muestra la correlación entre PPDIOO y Top-Down.

Figura 3.1 Metodologías



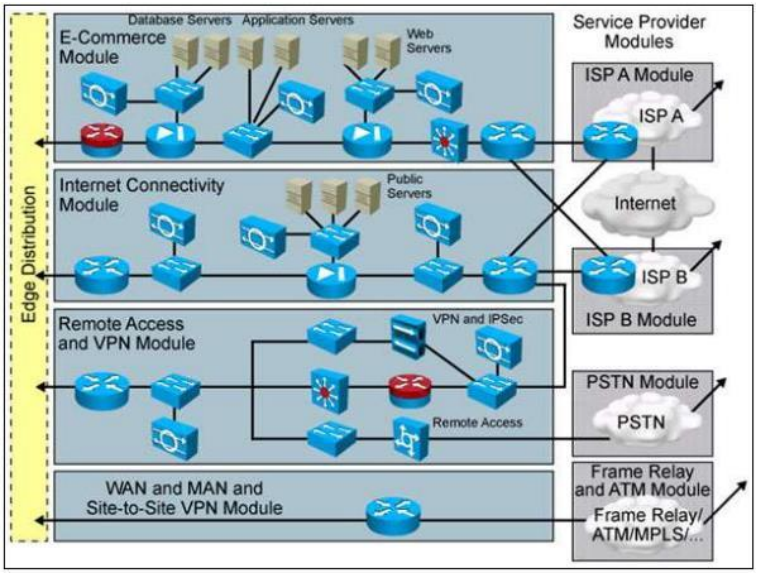
Correlación entre las PPDIOO y Top-Down. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan

3.2 Diseño de la Solución

A continuación, se describirá gráficamente la distribución de los equipos que conformarán la red de frontera de la institución, los módulos funcionales y una descripción de lo que se desea alcanzar con la propuesta.

En la Figura 3.2 se describen de una manera detallada todos los equipos que conforman una red de frontera en el ámbito empresarial, cabe recalcar que algunos de los equipos presentes en determinadas áreas del Diseño Empresarial de Borde de Internet de Cisco no están dedicados únicamente para cada área; además, que muchos otros se usan para garantizar las seguridades y la disponibilidad del servicio de todo un módulo.

Figura 3.2 Módulos de la Red de Frontera

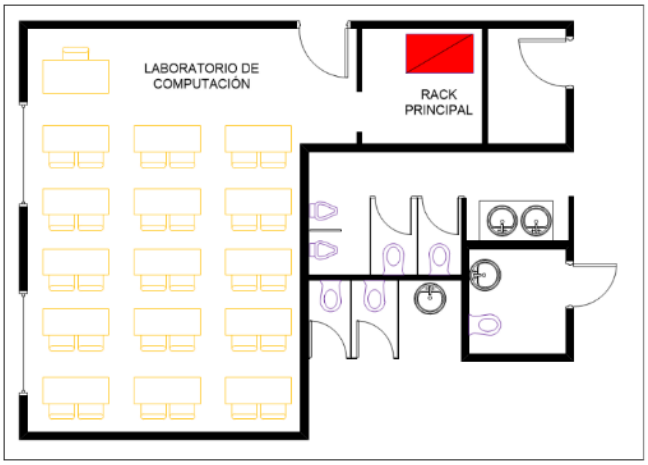


Módulos de la Red de frontera de Cisco con los equipos que la conforman. Fuente: (Cisco Networking Academy, 2014)

Hoy en día, es posible alcanzar los mismos resultados con el uso de aplicativos basados en software libre que realicen funciones similares o mejoradas y levantarlas en un solo equipo sin repercutir en el desempeño de la red.

En el diseño de red de campus se ha ubicado un rack de piso en el centro de datos que se encuentra en la planta baja del edificio principal junto al laboratorio de computación; como se muestra en la Figura 3.3.

Figura 3.3 Ubicación del Cuarto de Telecomunicaciones



Planta Baja del edificio principal del centro de formación donde se ubica el rack central. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Se propone que los equipos de la red perimetral sean ubicados en mencionada infraestructura desde la cual se conectará la red proveedor de servicios de internet,

PSTN y WAN de datos.

3.2.1 Diseño del Módulo de Conectividad a Internet

En la presente propuesta el módulo de conectividad a Internet para la red de frontera del CFCSB constituye un servidor, donde se instale una distribución de software libre que contenga herramientas y utilidades para sustituir el uso de dispositivos, con la finalidad de reducir costos y maximizar el espacio.

3.2.2 Selección del Servidor

La selección del equipo en donde se alojará el software de virtualización que gestione la seguridad, comunicación, monitoreo y autenticación de la red del centro de formación se lo realiza en base a la competitividad y tendencia en el mercado de determinadas marcas. A partir de lo mencionado anteriormente, los proveedores con mayor puntuación son las empresas HPE, Cisco y Dell. (Anexo 1)

Para la elección final se otorgará un puntaje impar, siendo 1: Malo y 5: Bueno a cada una de las opciones, al final se sumarán los resultados con el objetivo de seleccionar la opción de mayor puntaje. Este procedimiento se mantendrá para la selección de los demás dispositivos que conformarán la red de frontera del CFCSB.

Tabla 3.1 Selección del Servidor

Marca / Parámetros	HPE ProLiant DL160 Gen10	CISCO UCS C220 M4	DELL EMC PowerEdge R740
Precio	5	1	3
Factor de Forma	5	5	5
Conexiones de red	5	1	5
Procesador	5	3	5
Memoria RAM	5	5	5
Ranuras de Memoria	5	1	5
Ranuras de expansión	3	3	5
Unidades de Disco Duro	5	3	3
Opciones de Alimentación	5	3	3
Total	43	25	39

Tabla de evaluación para la selección del Servidor (Parámetros detallados, ver Anexo 2). Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.2.3 Selección de Software NGFW

Para la selección del Contrafuegos de Siguiente Generación, se presenta a continuación una tabla con cuatro distintas distribuciones, de las que se han seleccionado las funcionalidades que se alinean con los requerimientos de la institución.

Tabla 3.2 Selección de NGFW

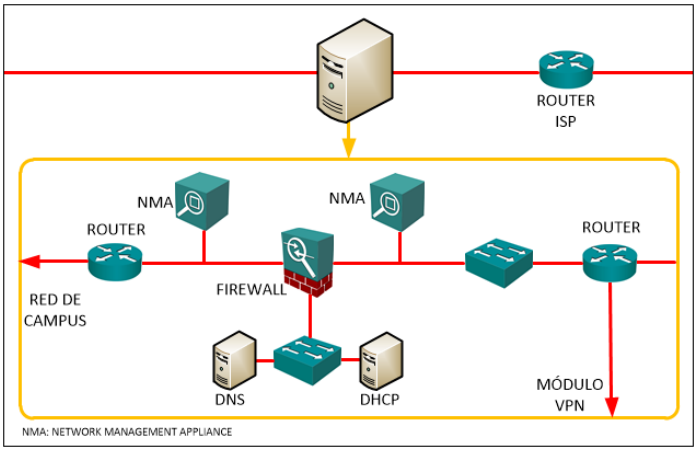
	ClearOS	Untangle	ZeroShell	pfSense
Costo	1	1	5	5
Alta Disponibilidad	5	5	5	1
Balance de WAN y Failover	5	5	5	5
Firewall	5	5	5	5
Routing	5	5	5	5
AP inalámbrico	1	1	1	5
Filtrado Web	5	1	5	5
Antivirus	5	1	5	5
Antispam	5	1	5	1
Portal Cautivo	1	5	5	5
Servidor DHCP	5	5	5	5
Servidor DNS	5	5	5	5
Servidor Open VPN	5	5	5	5
Cliente Open VPN	5	5	5	5
IPsec VPN	5	5	5	5
Servidor PPTP	5	5	1	5
Servidor RADIUS	5	5	1	5
Servidor SSH	5	5	5	5
Servidor File	5	1	1	5
Servidor Web	5	1	1	5
Servidor SMTP	5	1	5	1
Servidor VoIP	1	1	1	5
Total	94	75	86	98

Tabla comparativa para la selección del Contrafuegos de Siguiente Generación (NGFW) (Configuraciones, ver Anexo 3). Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Como se muestra en la Tabla 3.2 se elegirá pfSense ya que cuenta con la capacidad de proporcionar los servicios que requiere la red del centro además de haber obtenido un puntaje de 98/110.

En la Figura 3.4 se muestra la propuesta de diseño del Módulo de conectividad a Internet. En el Sistema Operativo del NGFW se configurarán sus utilidades para proveer de conectividad a Internet además de la seguridad y los servicios que garanticen un desempeño óptimo de la red de campus para el uso de los estudiantes, docentes, personal administrativo y visitantes; además se observa que todos los equipos que usualmente son implementados en una red empresarial como: Firewalls, Servidores, Switchs y Routers pueden ser reemplazados por una appliance que puede igualar o mejorar el rendimiento de la red reduciendo gastos y espacio en el rack principal del CFCSB, además se añade la funcionalidad de administración que es de gran utilidad para el monitoreo constante de esta.

Figura 3.4 Módulo de Conectividad a Internet



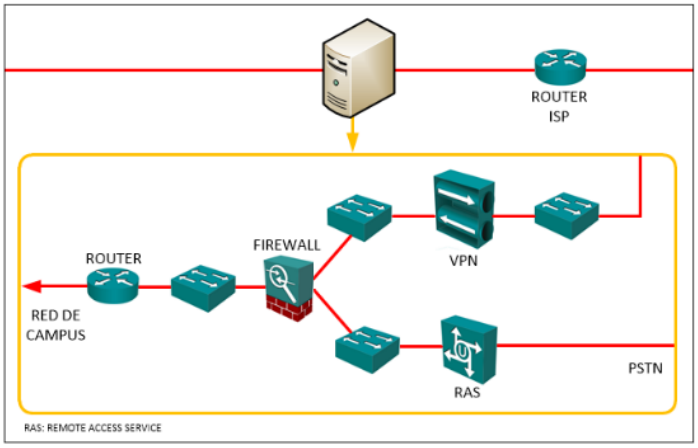
Representación de los equipos físicos de una red tradiciones, embebidos en el software NGFW. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.2.4 Diseño del Módulo de Acceso Remoto y VPN

Entre sus funcionalidades, el sistema Operativo pfSense cuenta con un servidor y un cliente OpenVPN, que utiliza certificados para que los usuarios que traten de acceder por este medio al servidor sean identificados y seguidamente autorizar o no la conexión.

En la Figura 3.5 se muestran los equipos activos que intervendrían en este módulo.

Figura 3.5 Módulo de Acceso Remoto y VPN



Representación de los equipos físicos de una red tradiciones, embebidos en el software NGFW. (Configuraciones, ver Anexo 4). Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Como se muestra en la figura anterior, la funcionalidad de los equipos es reducida solamente al trabajo realizado por el software pfSense; ya que las peticiones de conexión que ingresan por el módulo de conectividad a Internet deben ser validadas por el Firewall que concede el acceso después de autenticar al usuario o usuarios

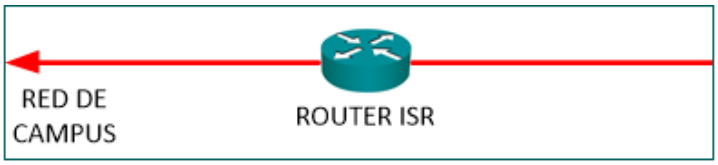
remotos.

Aquellos servicios que facilitan el acceso VPN son: Telefonía IP, Acceso a Internet y Conexión por medio de RAS (Servicio de Acceso Remoto).

3.2.5 Diseño del Módulo WAN

El módulo WAN estará conformado por un equipo que se encargue de enrutar todo el tráfico que provenga desde el campus Sur de la Universidad Politécnica Salesiana y viceversa.

Figura 3.6 Módulo WAN



Descripción del equipo para la conexión WAN. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Los equipos que logran proporcionar una conectividad confiable y segura son los ISR (Routers de Servicios Integrados), que han sido diseñados para organizaciones que cuentan con oficinas remotas y/o sucursales que requieren de un uso exigente de la red.

3.2.6 Selección del Router de Servicios Integrados (ISR)

En el caso del CFCSB se requiere que exista una interconexión entre la Sede de la Universidad Politécnica Salesiana Campus Sur y administradores remotos por medio de WAN, PSTN y VPN a través de Internet; por otra parte, la selección de este equipo será favorable para la futura implementación del servicio de VoIP para la institución.

En la Tabla 3.3 indica la selección del dispositivo ISR, el equipo ISR que cumple con las necesidades requeridas para la red del centro es de la marca Cisco, con un puntaje de 40/50. (Parámetros detallados, ver Anexo 5)

3.3 Dimensionamiento del Tráfico

Dimensionar el tráfico generado en la red de campus por parte de los estudiantes, visitantes, personal administrativo y docentes; ayudará a obtener el valor mínimo de la capacidad del canal que requiere el CFCSB para la conexión a Internet y que debe de ser provista por el ISP.

Tabla 3.3 Selección del Router de Servicios Integrados

Marca / Parámetros	Huawei 2200 Enterprise Router	Juniper Networks J4350	Cisco 4221 ISR
Precio	3	1	5
Procesador	5	3	3
Capacidad de Reenvío	3	5	3
Número de puertos	3	5	5
Módulos E1/T1	5	5	5
Puertos WAN	3	3	5
Seguridad	5	5	3
Fuente Redundante	1	3	1
Consumo de potencia	1	3	5
Factor de forma	3	5	5
Total	32	38	40

Tabla de evaluación para la selección del Router de Servicios Integrados. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Para el análisis de tráfico de red se han tomado los datos de la Tabla 1.6 del Capítulo 1 y se considera el número de usuarios basándose en la Tabla 2.2 de la sección anterior. El tráfico que circulará a través de la red de borde se ha dividido por aplicaciones, acceso al Internet y correo electrónico, video y voz.

Para cada caso se incluye un factor de crecimiento del 5% anual a 5 años del uso de la red y de los usuarios de la red.

3.3.1 Tráfico de Aplicaciones

Ya que la institución brindará cursos de formación técnica y tecnológica a los estudiantes se prevé que la red será utilizada 12 horas diariamente. Por otra parte, de los 256 puntos de red se proyecta que sean utilizados un total de 118 host y se asume que a los puntos de acceso se conecten un total 50 usuarios para el uso de aplicaciones web dando un total de 168 usuarios conectados, de acuerdo con la tabla 3.1 se procede a realizar los cálculos.

$$T_A = [(usuarios * \ Navegación\ (Mb)] * horas \qquad Ec.(3.1)$$

$$T_A = (168\ usuarios * \ 1\ Mb) * \ 12\ horas = 2016\ Mb$$

$$AB = \frac{T_A}{12\ horas} * \frac{8\ bites}{1\ byte} * \frac{1\ hora}{3600\ segundos} \qquad Ec.(3.2)$$

$$AB = \frac{2016\ Mb}{12\ horas} * \frac{8\ bites}{1\ byte} * \frac{1\ hora}{3600\ segundos} = 373{,}3\ Kbps$$

Tráfico de aplicaciones previsto en 5 años con 5% de crecimiento anual.

$$T_p = AB + (AB * 5\ años * 5\%) \qquad Ec.(3.3)$$

$$T_{Ap} = 373{,}3\ Kbps + (373{,}3\ Kbps * 5 * 0{,}05) = 466{,}63\ Kbps$$

Tráfico de Acceso a Internet y Correo Electrónico

Para el respectivo cálculo del tráfico para el acceso a Internet y correo electrónico se parte del tamaño promedio de una página web 3378 Kb; mencionado en el Capítulo 1, y se estima que cada usuario tenga acceso a 20 sitios por hora.

$$T_I = número\ de\ sitios *\ tamaño\ de\ página\ (Kb) \qquad Ec.(3.4)$$

$$T_I = 20\ sitios *\ 3378\ Kb =\ 67560 \frac{Kbytes}{hora}\ por\ cada\ usuario$$

$$AB = \frac{67560\ Kbytes}{1\ hora} * \frac{8\ bites}{1\ byte} * \frac{1\ hora}{3600\ segundos} * \frac{1000}{1\ KB}$$

$$AB =\ 150{,}13\ kbps\ por\ cada\ usuario$$

$$Tt_I = Número\ de\ usuarios * AB \qquad Ec.(3.5)$$

$$Tt_I = 168 * 150{,}13\ kbps = 25{,}22\ Mbps$$

Tráfico de acceso a Internet en 5 años con un crecimiento del 5% anual.

$$T_{Ip} = 25{,}22\ Mbps + (25{,}22\ Mbps * 5 * 0{,}05) = 31{,}53\ Mbps$$

Para el uso de correo electrónico por parte del personal Docente y Administrativo se proyecta el envío de 30 correos y cada usuario genere un flujo de 0,1 Mbps.

$$T_C = número\ de\ correos * flujo\ estimado \qquad Ec.(3.6)$$

$$T_C = 30 * 0{,}1\ Mbps = 3\ Mbps$$

Tráfico de correo electrónico en 5 años con un crecimiento del 5% anual.

$$T_{Cp} = 3\ Mbps + (3\ Kbps * 5 * 0{,}05) = 3{,}75\ Mbps$$

3.3.2 Tráfico de Video Conferencia

Para el análisis del tráfico de Video Conferencia se estima que diariamente se realicen 20 llamadas por parte del personal del centro.

$$T_{VC} = número\ de\ llamadas * tamaño\ (Mbps) \qquad Ec.(3.7)$$

$$20\ llamdas * 1{,}5\ Mbps = 30\ Mbps$$

Tráfico de video conferencia en 5 años con un crecimiento del 5% anual.

$$T_{VCp} = 30\ Mbps + (30\ Mbps * 5 * 0{,}05) = 37{,}5\ Mbps$$

A este valor se le añade el 25% de sobrecarga.

$$T_{VCt} = 37{,}5\ Mbps + (37{,}5\ Mbps * 0{,}25) = 46{,}88\ Mbps \qquad Ec.\ (3.8)$$

3.3.3 Ingeniería de Tráfico para Servicios de Telefonía IP

Para realizar la ingeniería de tráfico de telefonía IP del centro se deben calcular los parámetros de la Intensidad de Tráfico Instantánea con a siguiente relación:

$$A = \frac{V}{T} \qquad Ec.\ (3.9)$$

Donde:

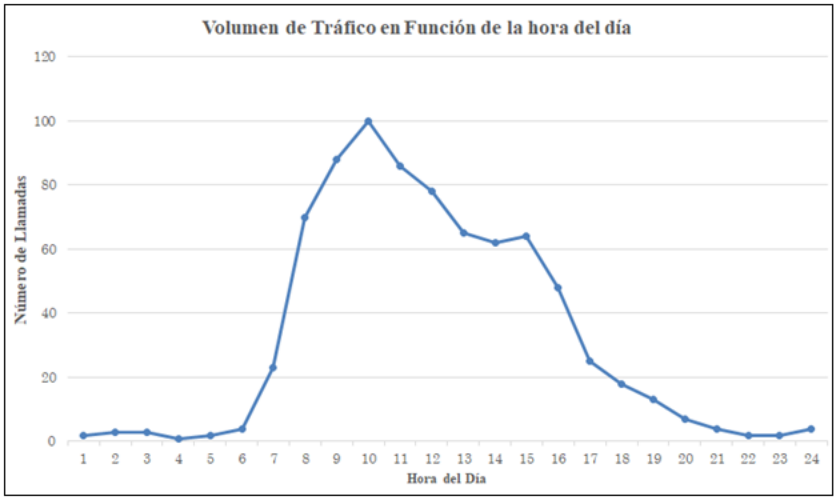
A: Intensidad de Tráfico en Erlangs

V: Volumen de Tráfico

T: Periodo de Observación

En la Figura 3.7 se muestra la estimación de volumen diario de tráfico en una entidad educativa con la que se realizarán las estimaciones para los cálculos y así dimensionar la red telefónica de la institución.

Figura 3.7 Volumen de Tráfico en Función a la hora del día



Tasa de llamadas referencial para la Medición de Recursos de telefonía. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Como se puede apreciar, existe un mayor volumen de tráfico de 9H00 a 10H00; estimando que se realizan 100 llamadas en un tiempo de 15614 segundos, se tiene:

- Una llamada tiene un promedio:

$$t^{'} = \frac{tiempo * número\ de\ llamadas}{número\ total\ de\ llamadas} \qquad Ec.(3.10)$$

$$t' = \frac{15614\ seg * 1\ llamada}{100\ llamadas} = 156{,}14\ seg$$

$$t^{'} = \frac{156{,}14\ seg}{3600\ seg} * 1\ hora$$

$$t^{'} = 0{,}043\ horas$$

- Calculando el Volumen de Tráfico

$$V = n * t \qquad Ec.(3.11)$$

$$V = 100 * 0{,}043\ horas = 4{,}3\ Erlangs$$

- Calculando la Intensidad de Tráfico

$$A = \frac{V}{1\ hora} \qquad Ec.(3.12)$$

$$A = \frac{4{,}3\ Erlangs}{1\ hora} = 4{,}3\ Erlangs$$

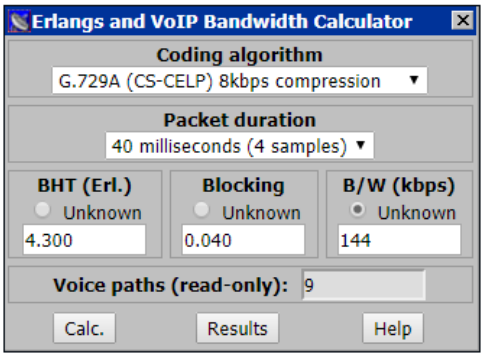
El número de líneas se lo ha realizado por medio de la Tabla de Erlang B y se ha considerado un 4% de probabilidad de bloqueo p durante el mayor tiempo de actividad en el sistema telefónico del centro.

$$N = 9\ troncales$$

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. Como se puede apreciar en la Figura 3.8 el resultado es:

$$AB_V = 144\ Kbps$$

Figura 3.8 Ancho de Banda Estimado



Ancho de Banda necesario para las llamadas de voz del centro. Fuente: (Westway Engineers, 2017)

Para el cálculo del Ancho de Banda mínimo que requiere el CFCSB se procede a realizar la sumatoria de los resultados obtenidos anteriormente.

$$AB = T_{Ap} + T_{Ip} + T_{Cp} + T_{VCt} + AB_V \qquad Ec.(3.13)$$

$$AB = 466{,}63\ Kbps + 31{,}53\ Mbps + 3{,}75\ Mbps + 46{,}88\ Mbps + 144\ Kbps$$

$$AB = 82{,}77\ Mbps$$

3.3.4 Distribución de Ancho de Banda de Internet

De acuerdo con el escenario de prueba definido para el análisis, se recomienda que para el centro se contrate un plan de al menos 100 Mbps de ancho de banda que permitirá una adecuada velocidad de navegación.

Cabe mencionar que la tasa de distribución de ancho de banda se lo llevará a cabo en base criterios propios apegados a las necesidades de cada área de la institución.

En la siguiente tabla se muestra la propuesta de distribución de ancho de banda para el CFCSB.

Tabla 3.4 Distribución de Ancho de Banda de Internet

Área	Porcentaje de Ancho de Banda
Red de Docentes & Administravivos	39%
Red de Estudiantes	48%
Red de Gestión	10%
Red de Telefonía	3%
TOTAL	100%

Distribución porcentual del Ancho de Banda de Internet para el centro. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.4 Redundancia

Para aportar esta capacidad a la red de frontera del CFCSB; con el fin de mantener las actividades educativas y de conexión de manera ininterrumpida, se debe incorporar enlaces suplementarios que permitan que los datos tomen un camino alterno al momento de producirse un fallo, para ello se han previsto dos escenarios.

El primero es en caso de producirse un error en la conexión por parte del ISP, para ello pfSense cuenta con la funcionalidad Failover (conmutación por error) que redireccionará toda la información generada desde la red de campus y la enviará a través del ISR hacia el enlace WAN hasta el campus Sur de la Universidad Politécnica Salesiana.

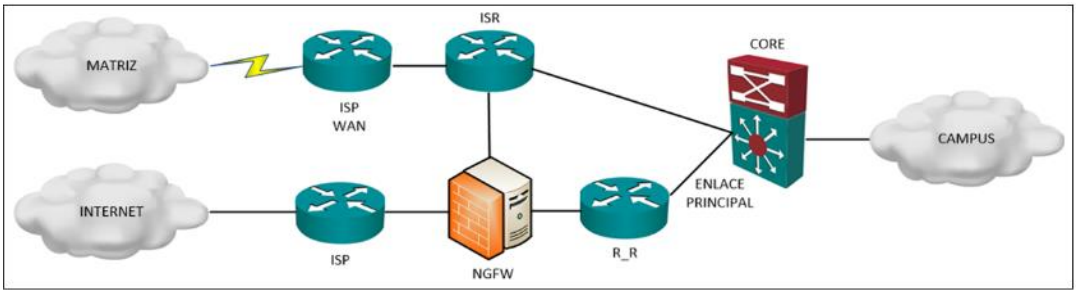
El segundo escenario sería en caso de caída del servidor o del enlace que conecta este con el Switch de Core de la red de campus del CFCSB, para esto se plantea conectar los dos equipos a través de un Router en el que se configuren protocolos de alta disponibilidad, en este caso se realizará VRRP (Virtual Router Redundancy Protocol).

3.4.1 Selección del Router de Redundancia

Para la selección del equipo de redundancia se consideran equipos de enrutamiento SOHO (Small Office Home Office), debido a que el dispositivo solo se activará cuando ocurra el segundo escenario descrito anteriormente. (Parámetros detallados, ver Anexo 6)

En la Figura 3.9 se presenta la conexión del equipo de Backup para la red del centro.

Figura 3.9 Backup de la red de frontera



Enlaces de redundancia en la red del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la tabla a continuación, el enrutador Cisco 921-4P es el que satisface los requerimientos para el diseño de un enlace redundante entre el servidor y el Switch L3 de la red de campus.

Tabla 3.5 Selección del Router de Alta Disponibilidad

Marca / Parámetros	Huawei AR 201	Juniper SRX 320	Cisco 921-4P
Precio	5	3	1
Número de Puertos	5	5	5
Protocolos de Alta Disponibilidad	3	3	5
Seguridad	5	5	5
Velocidad Upload/Download	3	3	5
Protocolos de Enrutamiento	3	5	5
Calidad de Servicio	3	5	5
Administración	1	3	5
Consumo de potencia	3	5	5
IPv4/IPv6	5	5	5
Total	36	42	46

Tabla de evaluación para la selección del Router de Alta Disponibilidad. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.5 Diseño de Topología Lógica y Física de la Red de Frontera

3.5.1 Direccionamiento IPv4

Considerado que el direccionamiento de la red de frontera es una ampliación de las direcciones aplicadas en el diseño de la red interna del centro, que se diseñó a partir de la dirección 172.16.0.0/17, se configuraron cuatro VLANs en el Switch L3 para los grupos: Docentes y Administrativos (VLAN 10), Estudiantes (VLAN 20), Visitantes (VALAN 30) y Gestión (VLAN 40).

Se llevará a cabo la asignación de direcciones para los equipos que formarán parte de la red perimetral, se conservará la VLAN de Gestión y se añadirá la LAN virtual Telefonía (VLAN 50) para la futura implementación de este servicio en el CFCSB partiendo de la dirección 172.16.80.0/20, con el propósito de proveer de direcciones a los enlaces y dispositivos que serán configurados asegurando escalabilidad de la infraestructura.

Tabla 3.6 Segmentación IPv4

DISPOSITIVO	Subred	DIRECCIÓN	MÁSCARA	PRIMERA DIRECCIÓN	BROADCAST
Gestión	4	172.16.64.0	255.255.240.0	172.16.64.1	172.16.79.255
Telefonía	5	172.16.80.0	255.255.240.0	172.16.80.1	172.16.80.255
WAN	6	172.16.96.0	255.255.240.0	172.16.96.1	172.16.111.255
VPN	7	172.16.112.0	255.255.240.0	172.16.112.1	172.16.127.255
Internet	8	172.16.128.0	255.255.255.0	172.16.128.1	172.16.128.255
Backup	9	172.16.129.0	255.255.255.0	172.16.129.1	172.16.129.255
L-Campus	10	172.16.130.0	255.255.255.0	172.16.130.1	172.16.130.255
Granja de servidores	11	172.16.131.0	255.255.255.0	172.16.131.1	172.16.131.255

Asignación de bloques de direcciones IPv4. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la Tabla 3.7 se presenta el direccionamiento para los dispositivos que conforman la red de frontera.

Tabla 3.7 Direccionamiento IPv4

Dispositivo	VLAN	Interfaz	Dirección	Máscara de subred	Gateway
Switch L3	40	VLAN40	172.16.64.1	255.255.240.0	-
	50	VLAN50	172.16.80.1	255.255.240.0	-
Gestión	40	F0/15 SW L3	172.16.64.10	255.255.255.0	172.16.64.1
ISP	-	G0/0	ISP	ISP	ISP
		G0/1	172.16.128.2	-	
		SIP	SIP	SIP	-
Router Backup	-	G0/0	172.16.130.2	-	-
		G0/1	TRUNK	TRUNK	-
NGFW	-	ETH0	172.16.128.1	-	-
		ETH1	172.16.130.1	-	-
		ETH2	172.16.129.1	-	-
ISR	-	G0/0	TRUNK	TRUNK	-
		G0/1	172.16.129.2	-	-
		G0/2	172.16.96.2	-	-
		SIP	SIP	SIP	-

Propuesta de direccionamiento IPv4 para los equipos de la red. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.5.2 Direccionamiento IPv6

De la misma manera que se llevó a cabo en el diseño IPv4, se mantendrá las configuraciones para IPv6 con el prefijo global 2000:16:62 y dejando 64 bits para la asignación en los dispositivos de la institución como se indica en la tabla a continuación.

Tabla 3.8 Direccionamiento IPv6

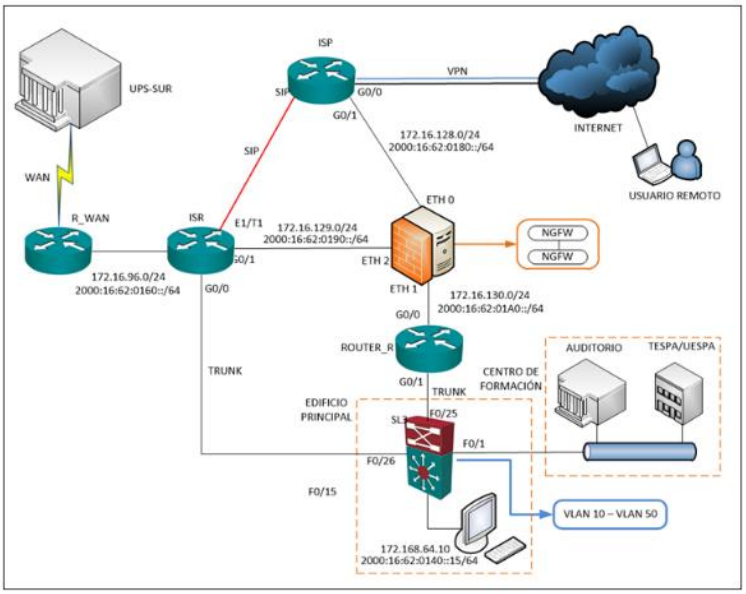
Dispositivo	VLAN	Interfaz	Dirección	Gateway
Switch L3	40	VLAN40	2000:16:62:0140::1/64	-
	50	VLAN50	2000:16:62:0150::1/64	-
Gestión	40	F0/15 SW L3	2000:16:62:0140::15/64	2000:16:62:0140::1/64
ISP	-	G0/0	ISP	ISP
		G0/1	2000:16:62:0180::2/64	-
		SIP	SIP	-
Router Backup	-	G0/0	2000:16:62:1A0::2/64	-
		G0/1	TRUNK	-
NGFW	-	ETH0	2000:16:62:0180::1/64	-
		ETH1	2000:16:62:1A0::1/64	-
		ETH2	2000:16:62:0190::1/64	-
ISR	-	G0/0	TRUNK	-
		G0/1	2000:16:62:0190::2/64	-
		G0/2	2000:16:62:0160::2/64	-
		SIP	SIP	-

Propuesta de direccionamiento IPv6 para los equipos de la red. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.5.3 Diseño de Topología Lógica de la Red de Frontera

Una vez diseñados lo módulos basados en el Diseño Empresarial de Borde de Internet de Cisco, así como la selección de equipos y los esquemas de direccionamiento IPv4 e IPv6, en la Figura 3.10 se propone la siguiente topología lógica para el CFCSB con la cual se procura optimizar el rendimiento, disponibilidad y capacidades de la red hacia las redes exteriores.

Figura 3.10 Topología Lógica IPv4/IPv6 de la Red de Frontera

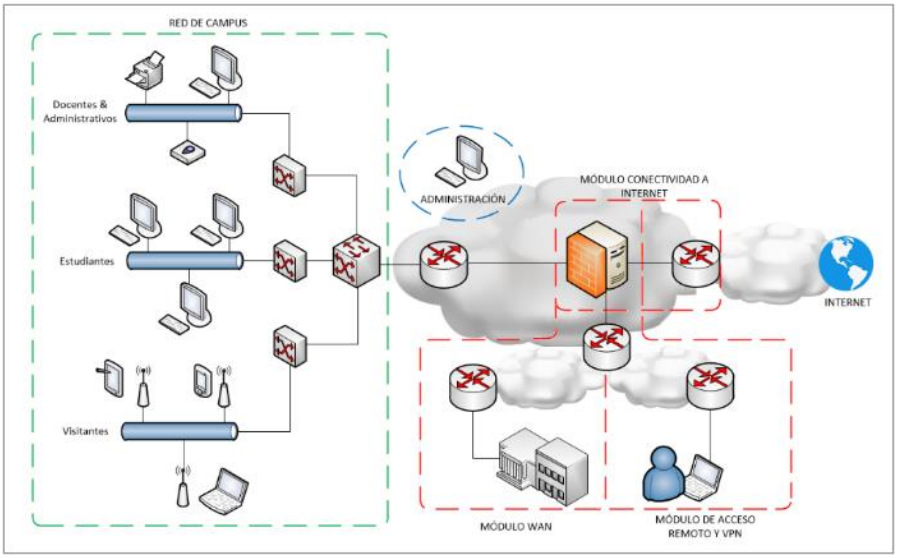


Diseño de la Topología Lógica de la Red de Frontera para el centro. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.5.4 Diseño de Topología Física de la Red de Frontera

A continuación, se presenta la topología física de la red borde para el centro, la cual está basada en Internet Edge Designe de Cisco, en esta se describen los módulos que la conforman incluyendo la red de campus.

Figura 3.11 Topología Física de la Red de Frontera



Diseño de la Topología Física de la Red de Frontera para el CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.5.5 Seguridad de la Red de Frontera

Con la aplicación de políticas de seguridad se busca salvaguardar los recursos informáticos del centro, evitar ataques externos e internos y garantizar la disponibilidad de la red; para lo cual se utilizará Next Generation Firewall como primera línea defensiva, listas de control de acceso, Filtrado URL y autenticación de los usuarios remotos.

En las Tablas 3.9, 3.10 y 3.11, se muestran las propuestas para: Las listas de control de acceso (ACLs) de filtrado por puertos y configuradas en el NGFW, el filtrado de puertos para las VLANs Docentes & Administrativos, Estudiantes, Visitantes, Gestión y Telefonía y filtrado InterVLAN aplicado en los equipos de enrutamiento ISR y Router de Redundancia.

Tabla 3.9 Listas de Control de Acceso en NGFW

Interfaz	Origen	Destino	Puertos	Estado	Descripción
Interfaz Internet	172.16.128.0/24 2000:16:62:180::/64	any	80, 443, 53, 123, 1194, 1812-1813, 444, 5004, 33434-33598	Permitir	Recursos necesarios estimados
	any		any	Bloqueo	Bloqueo de recurso innecesarios
Interfaz WAN	172.16.129.0/24 2000:16:62:190::/64	any	80, 443, 20-21, 22, 69, 23, 123, 1194, 1812-1813, 5060-5061-4569, 444, 5004, 3343-33598	Permitir	Recursos necesarios estimados
	any		any	Bloqueo	Bloqueo de recurso innecesarios
Interfaz CAMPUS	any	172.16.130.0/24 2000:16:62:1A0::/64	80, 443, 22, 25-26, 53, 23, 123, 631, 1194, 1812-1813, 5060-5061-4569, 444, 5004, 33434-33598	Permitir	Recursos necesarios estimados
	any	any	any	Bloqueo	Bloqueo de recurso innecesarios

Propuesta de listas de Control de Acceso de filtrado por puertos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Tabla 3.10 Filtrado de puertos para las VLANs

Interfaz	Origen	Destino	Puertos	Estado	Descripción
VLAN 10	any	172.16.16.0/20 2000:16:62:110::/64	80, 443, 20-21, 53, 69, 123, 631, 67-68, 546-547, 546-547, 1194, 1812-1813, 5060-5061-4569, 444, 5004, 33434-33598	Permitir	Recursos necesarios estimados
VLAN 20	any	172.16.32.0/20 2000:16:62:120::/64	80, 443, 20-21, 53, 69, 123, 67-68, 546-547, 1812-1813, 444, 5004, 33434-33598	Permitir	Recursos necesarios estimados
VLAN 30	any	172.16.48.0/20 2000:16:130::/64	80, 443, 53, 67-68, 546-547, 1812-1813, 444	Permitir	Recursos necesarios estimados
VLAN 40	any	172.16.64.0/20 2000:16:62:140::/64	any	Permitir	Recursos necesarios estimados

Filtrado de puertos para las VLANs. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Tabla 3.11 Filtrado InterVLAN

	Interfaz	Origen	Destino	Puertos	Estado	Descripción
Docentes & Administrativos	VLAN 10	172.16.16.0/20 2000:16:62:110::/64	172.16.16.1 2000:16:62:110::1	20-21, 53, 67-68, 546-547, 1812-1813	Permitir	Recurso de Gateway
			172.16.32.0/20 2000:16:62:120::/64	20-21, 69		Compartir archivos
			172.16.48.0/20 2000:16:130::/64	any	Bloqueo	Acceso no permitido
			172.16.64.0/20 2000:16:62:140::/64			
			172.16.80.0/20 2000:16:62:150::/	5004, 5060-5061-4569	Permitir	Recursos de Telefonía
Estudiantes	VLAN 20	172.16.32.0/20 2000:16:62:120::/64	172.16.16.0/20 2000:16:62:110::/64	any	Bloqueo	Acceso no permitido
			172.16.32.1 2000:16:62:120::1	20-21, 53, 67-68, 546-547, 1812-1813	Permitir	Recurso de Gateway
			172.16.48.0/20 2000:16:130::/64	any	Bloqueo	Acceso no permitido
			172.16.64.0/20 2000:16:62:140::/64			
			172.16.80.0/20 2000:16:62:150::/			
Visitantes	VLAN 30	172.16.48.0/20 2000:16:130::/64	172.16.16.0/20 2000:16:62:110::/64	any	Bloqueo	Acceso no permitido
			172.16.32.0/20 2000:16:62:120::/64			
			172.16.48.1 2000:16:62:130::1	20-21, 53, 67-68, 546-547, 1812-1813	Permitir	Recurso de Gateway
			172.16.64.0/20 2000:16:62:140::/64	any	Bloqueo	Acceso no permitido
			172.16.80.0/20 2000:16:62:150::/			
Gestión	VLAN 40	172.16.64.0/20 2000:16:62:140::/64	172.16.16.0/20 2000:16:62:110::/64	any	Permitir	Control
			172.16.32.0/20 2000:16:62:120::/64			
			172.16.48.0/20 2000:16:130::/64			
			172.16.64.1 2000:16:62:140::1			
			172.16.80.0/20 2000:16:62:150::/			
Telefonía	VLAN 50	172.16.80.0/20 2000:16:62:150::/	172.16.80.1 2000:16:62:150::1/	5004, 5060-5061-4569	Permitir	Recurso de Gateway
			172.16.16.0/20 2000:16:62:110::/64	any		Recursos de Telefonía
			172.16.32.0/20 2000:16:62:120::/64		Bloqueo	Acceso no permitido
			172.16.48.1 2000:16:62:130::1			
			172.16.64.0/20 2000:16:62:140::/64			

Filtrado InterVLAN por puerto. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

3.6 Equipo de Alimentación Ininterrumpida (SAI)

El Sistema de Alimentación Ininterrumpida es un factor importante que considerar, debido a que garantiza una alimentación continua para los equipos que se encuentren en el rack principal del centro evitando que sean afectados por problemas eléctricos o cortes imprevistos.

Para el dimensionamiento del SAI adecuado se debe recurrir a las especificaciones técnicas de los equipos para realizar los cálculos y precisar la potencia aparente (VA) necesaria con la siguiente relación:

$$1VA = 1W/cos\varphi \qquad Ec.(3.14)$$

Donde $cos\varphi$ es el factor de potencia, que en cargas típicas de sistemas informáticos se encuentra entre 0,65 y 0,8.

En la Tabla 3.12 se muestran los datos de placa de los equipos que se ubicarán en el rack principal y x| respectivo dimensionamiento para el SAI tomando un factor de potencia promedio de 0,725 y un 25% de factor de crecimiento.

Tabla 3.12 Dimensionamiento de Sistema de Alimentación Ininterrumpida

Equipos Protegidos	Cantidad	Potencia (W)	Potencia Aparente (VA)
Equipo ISP	1	30	41.38
Servidor	1	500	689.7
Router Servicios Integrados	1	150	206.89
Router de Alta Disponibilidad	1	30	41.38
Switch Capa 3	1	435	600
Switch Capa 2	4	100	137.9
Subtotal	9	1545	2130.95
Factor de Crecimiento de 25%		1931.25	2663.8
VA Requeridos		3476.25 (3.47 KW)	4794.75 (4.79 KVA)

Tabla de evaluación de potencia aparente de SAI a partir de los datos de placa de los equipos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Se recomienda la instalación de un equipo de capacidad superior a 4.79 KVA para asegurar la protección de los elementos activos del centro.

3.7 Propuesta de Calidad de Servicio QoS

3.7.1 Definición de Políticas y Clases de Calidad de Servicio

Para definir políticas de calidad de servicio se debe clasificar y evaluar el tráfico sensible a retardos para luego proceder a priorizar los servicios que proporciona la red de acuerdo al ancho de banda disponible.

3.7.2 Clasificación de Tráfico

Se propone un flujo estándar de paquetes entrantes y salientes desde la red lo que permite generar clases de tráfico, a los mismos que se les puede brindar un trato diferenciado introduciendo una base para la gestión de QoS.

En la Tabla 3.13 se muestran las seis clases que forman parte de las políticas de Calidad de Servicio de la red de borde de la institución con niveles de prioridad que van desde 0 (Bajo) hasta 5 (Baja) para cada una de las aplicaciones que son utilizados en una red.

Tabla 3.13 Definición de Clases para las Políticas de Calidad de Servicio

NIVEL	DESCRIPCIÓN	PRIORIDAD	DSCP	Probabilidad de Pérdida	APLICACIONES
5	REENVÍO EXPRESS	CRÍTICO	EF	N/A	VoIP
4	CLASE 4	ALTO	AF41	BAJO	Video Conferencia
			AF42	MEDIO	N/A
			AF43	ALTO	N/A
3	CLASE 3		AF31	BAJO	Datos de Misión Crítica
			AF32	MEDIO	N/A
			AF33	ALTO	N/A
2	CLASE 2	MEDIO	AF21	BAJO	WEB HTTP, Datos, Transaccionales, Base de Datos
			AF22	MEDIO	N/A
			AF23	ALTO	N/A
1	CLASE 1	BAJO	AF11	BAJO	BULK DATA
			AF12	MEDIO	N/A
			AF13	ALTO	N/A
0	BEST EFFORT		-	N/A	FTP DEFAULT

Definición de Clases con su respectiva prioridad y los principales puertos usado por cada aplicación. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

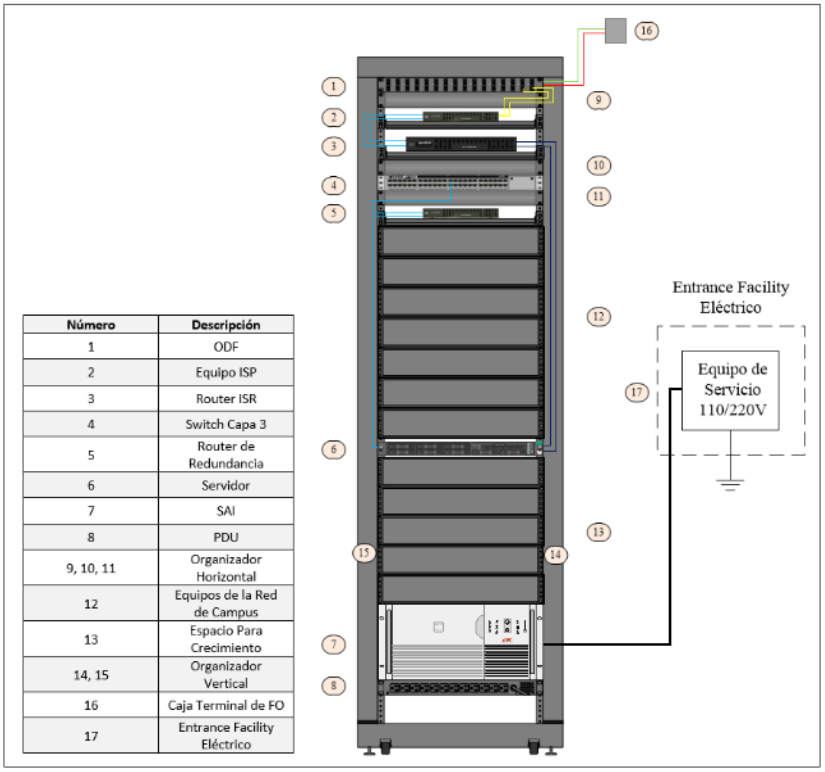
3.7.3 Filtrado de Contenido

En base a los requerimientos de la institución se debe bloquear el acceso hacia determinados sitios de Internet, ya que su contenido no es relevante en la formación de los estudiantes ni son herramientas de apoyo para los docentes y personal administrativo. Basándose en la orientación de carácter educativo del centro de formación, se llevará a cabo el filtrado de contenido con la utilidad de pfSense pfBlockerNG que descarga listas con la categoría de distintos sitios en el Internet y crea reglas de Firewall para proteger a los usuarios. (Configuraciones, ver Anexo 7)

3.8 Distribución del Equipo Activo

La ubicación de los equipos activos de la red de frontera será llevada a cabo en el espacio para ampliación en el rack principal localizado en la planta baja del edificio principal del centro. Se ha seleccionado un gabinete de 45UR con un ancho estándar de 24 pulgadas, profundidad de 42 pulgadas, puerta de vidrio templado, paneles laterales y ventilación para la protección de los equipos a ser ubicados. En la Figura 3.11 se observa la distribución recomendada para los elementos pasivos y equipos activos.

Figura 3.12 Distribución de equipos



Número	Descripción
1	ODF
2	Equipo ISP
3	Router ISR
4	Switch Capa 3
5	Router de Redundancia
6	Servidor
7	SAI
8	PDU
9, 10, 11	Organizador Horizontal
12	Equipos de la Red de Campus
13	Espacio Para Crecimiento
14, 15	Organizador Vertical
16	Caja Terminal de FO
17	Entrance Facility Eléctrico

Propuesta para la distribución de equipos en el rack de piso. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

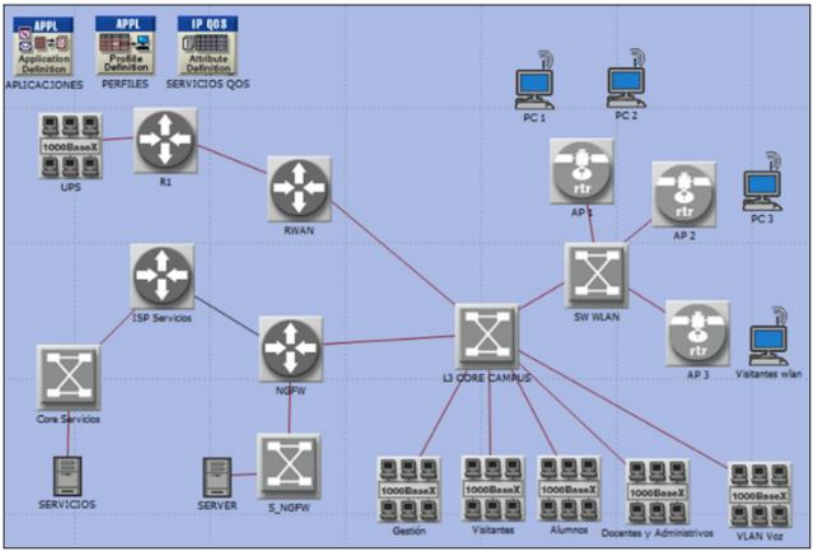
CAPÍTULO 4
ANÁLISIS DE TRÁFICO DE LA RED Y ANÁLISIS DE COSTOS

4.1 Simulación de la Red de Borde

4.1.1 Desempeño de la Red de Borde con el Software OPNET Modeler

Con el propósito de conocer el comportamiento y desempeño del diseño de toda la red del centro, se ha implementado la topología en el software OPNET Modeler, aplicando políticas de calidad de servicio descritas en la Tabla 3.13 del capítulo anterior, se evaluarán que los parámetros estén dentro de los márgenes óptimos de funcionamiento. En la Figura 4.1 se muestra el escenario implementado en el software de simulación. (Configuración, ver a partir del Anexo 8).

Figura 4.1 Simulación de la Topología de Red de Borde del Centro



Simulación de las redes de frontera y campus del centro en el software de simulación OPNET Modeler, Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la figura anterior se ha modelado la topología de las redes de borde y de campus para la simulación en el software OPNET Modeler, el cual presenta gráficamente el desempeño de toda la red.

En las Figuras 4.2, y 4.3 se presentan los resultados de Delay, Traffic Dropped, Jitter y Throughput; respectivamente, obtenidas aplicando el Encolamiento FIFO entre en el enlace de los dispositivos con las etiquetas NGFW y L3 CORE CAMPUS, el cual es un mecanismo simple de QoS llevado a cabo en un tiempo de observación de 72 horas.

Figura 4.2 Mediciones Globales de Delay y Traffic Dropped

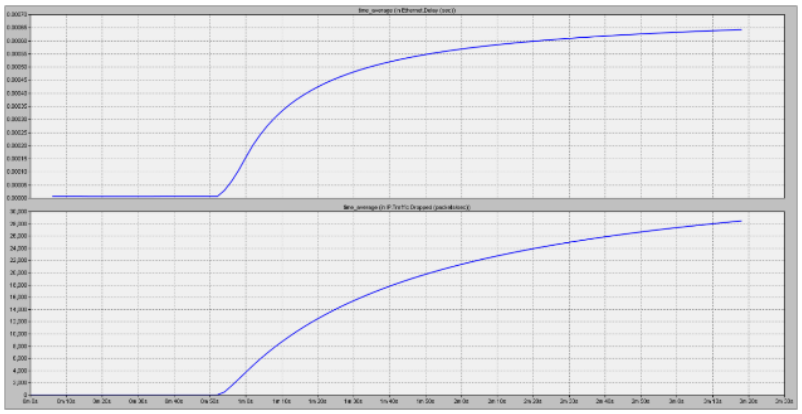


Gráfico de resultados de Delay y Traffic Dropped de la Red de Frontera del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

La ilustración superior de la Figura 4.2 muestra el retardo global de la red, el cual se incrementa hasta llegar a un máximo de 0,65 ms después de 3 minutos y 20 segundos del tiempo total de observación. La ITU-T G.114 recomienda que el valor de retardo no sobrepase los 400 ms al momento de planificar una red. En la ilustración inferior se observa que el número de datagramas o paquetes IP perdidos con encolamiento FIFO llegan sobrepasan los 28.000 paquetes/segundo.

Figura 4.3 Estadística Global del Jitter y Throughput

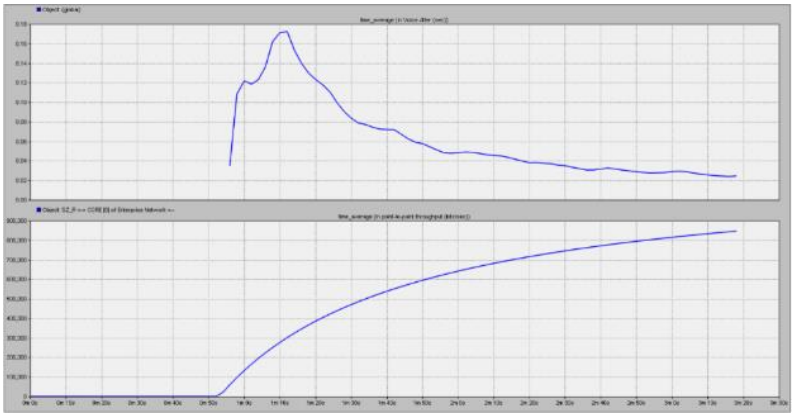


Gráfico de resultados del Traffic Dropped y Jitter de la Red de Frontera del CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la ilustración superior de la Figura 4.3, se muestra el Jitter en la red de voz utilizando el códec G.729A, el cual presenta una traza discontinua y con un valor máximo cercano a los de 0,18 segundos durante el tiempo de simulación. Seguidamente, en la ilustración inferior el desempeño de la red se incrementa gradualmente hasta sobrepasar los 0,8Mbps.

4.1.2 Implementación de Servicios Diferenciados (DiffServ)

Con la implementación del mecanismo de Servicios Diferenciados (DiffServ) en el software OPNET Modeler se busca agrupar los flujos de datos en clases según su comportamiento con el fin de garantizar calidad de servicio para la red. (Configuración, ver Anexo 9)

Se han llevado a cabo las configuraciones de Servicios Diferenciados basados en los encolamientos Priority Queueing (PQ) y Weighted Fair Queuing (WFQ) con el objetivo de comparar sus resultados y determinar el mecanismo óptimo de calidad de servicio, los resultados obtenidos se muestran de la Figura 4.4 a la Figura 4.7 a continuación.

Figura 4.4 Comparación del Delay

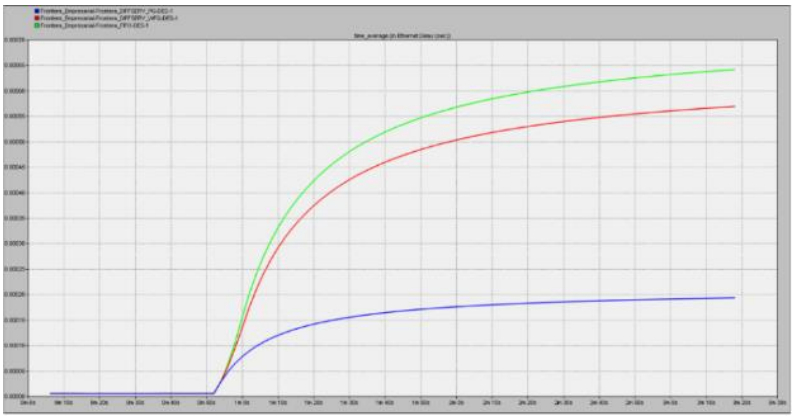


Gráfico comparativo del retardo global de la red aplicando Servicios Diferenciados basados en PQ, WFQ y encolamiento FIFO. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la figura anterior se puede apreciar las trazas obtenidas del retardo global de la red de borde aplicando encolamiento FIFO (verde), DiffServ basados en WFQ (rojo) y DiffServ basados en PQ (azul), reduciendo considerablemente su valor con este último hasta un valor inferior a los 0,2 ms.

En la siguiente figura se puede apreciar la notable reducción en la pérdida de paquetes con el método DiffServ basado en encolamiento PQ, reduciendo su valor a 19.000 paquetes/segundo después de 3 minutos y 10 segundos del tiempo total de observación.

Figura 4.5 Comparación del Traffic Dropped

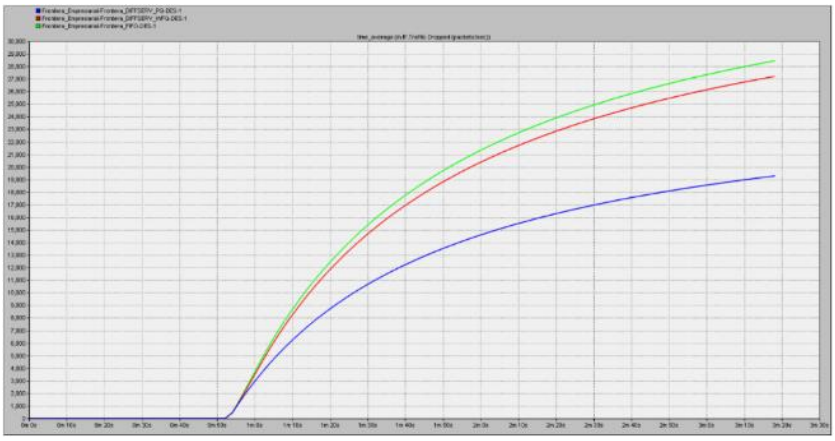


Gráfico comparativo del Traffic Dropped global de la red aplicando Servicios Diferenciados basados en PQ, WFQ y encolamiento FIFO. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Figura 4.6 Comparación del Throughput

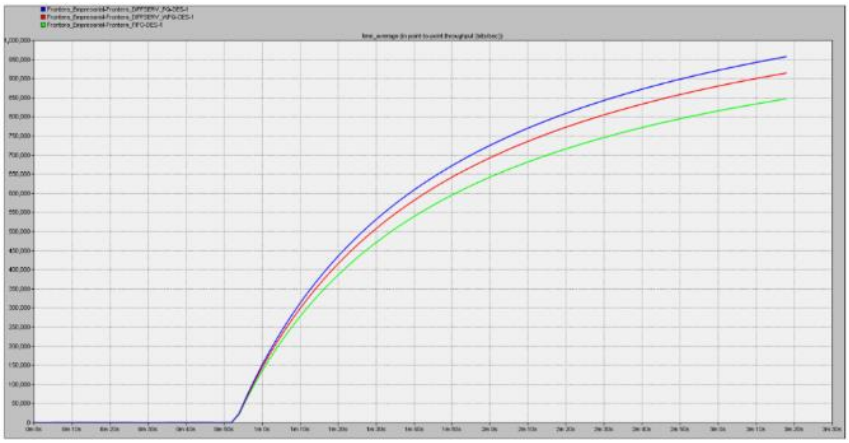
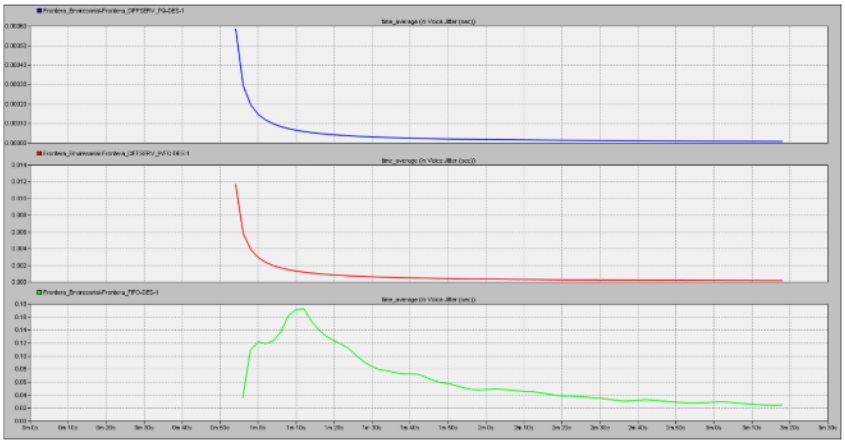


Gráfico comparativo del Throughput. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Al igual que en los dos casos anteriores, en la Figura 4.6 se puede observar que con el método DiffServ basado en PQ en el enlace Core - NGFW, el desempeño de la red se incrementó 150.000 bits/segundos transcurridos 3 minutos y 10 segundos del tiempo total de observación.

En las ilustraciones de la Figura 4.7 puede observarse que aplicando DiffServ basado en PQ y WFQ se obtienen trazas continuas a diferencia del encolamiento FIFO, siendo más evidente la reducción del Jitter en la ilustración superior donde la fluctuación máxima alcanza un valor aproximado a los 0.6 ms.

Figura 4.7 Comparación del Jitter

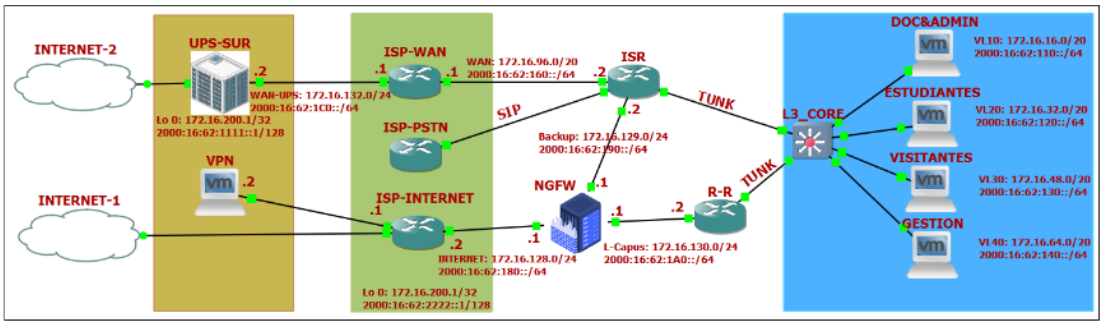


Ilustraciones comparativas del Jitter de voz de la red aplicando Servicios Diferenciados basados en PQ, WFQ y encolamiento FIFO. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

4.1.3 Simulación de la Red de Borde en GNS3

Se ha llevado a cabo la simulación de la red de frontera en el software GNS3, con la finalidad de comprobar la conectividad y proponer un diseño apegado a la realidad por las facilidades y flexibilidades del programa. Además, han sido levantadas máquinas virtuales en el software VMware que representan a los puntos finales conectados a las VLANs: Docentes & Administrativos, Estudiantes, Visitantes y Gestión.

Figura 4.8 Simulación en el Software GNS3

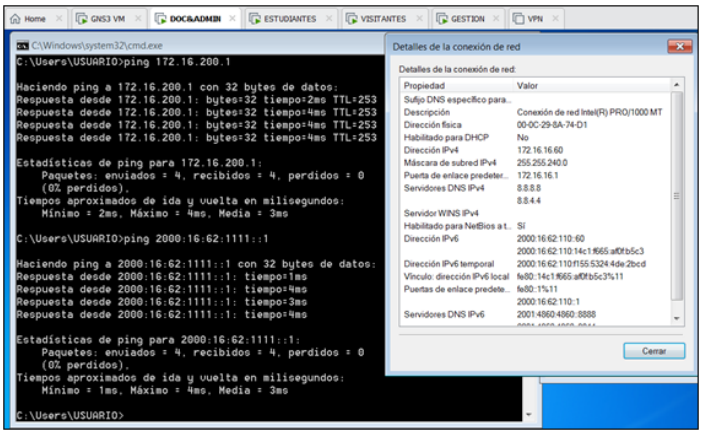


Distribución de los equipos de la Red de Borde en el Software GNS3. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

4.2 Comprobación de Conectividad

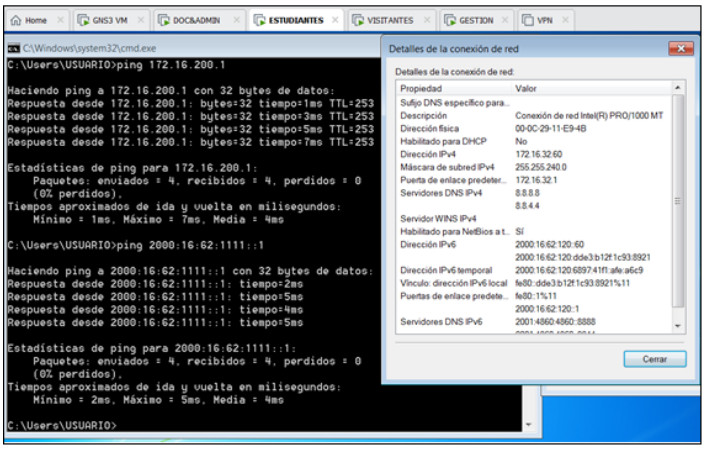
A partir de la Figura 4.9 hasta la Figura 4.12, se muestra la comprobación de la conectividad WAN de las redes Docentes & Administrativos, Alumnos, Visitantes y Gestión.

Figura 4.9 Comprobación de Conectividad WAN



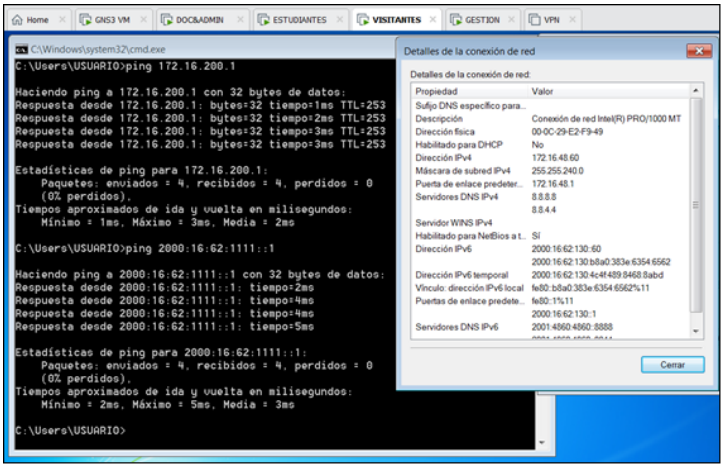
Comprobación de Conectividad WAN desde un host virtual en la VLAN Docentes & Administrativos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Figura 4.10 Comprobación de Conectividad Internet



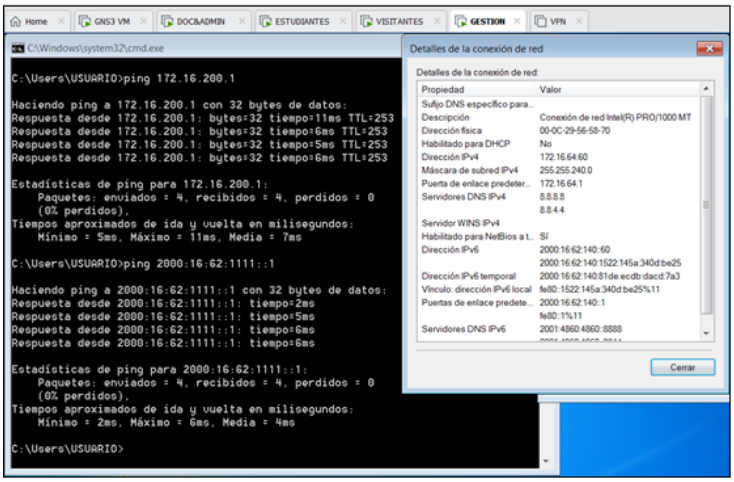
Comprobación de Conectividad WAN desde un host virtual en la VLAN Alumnos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Figura 4.11 Comprobación de Conectividad WAN



Comprobación de Conectividad WAN desde un host virtual en la VLAN Visitantes. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

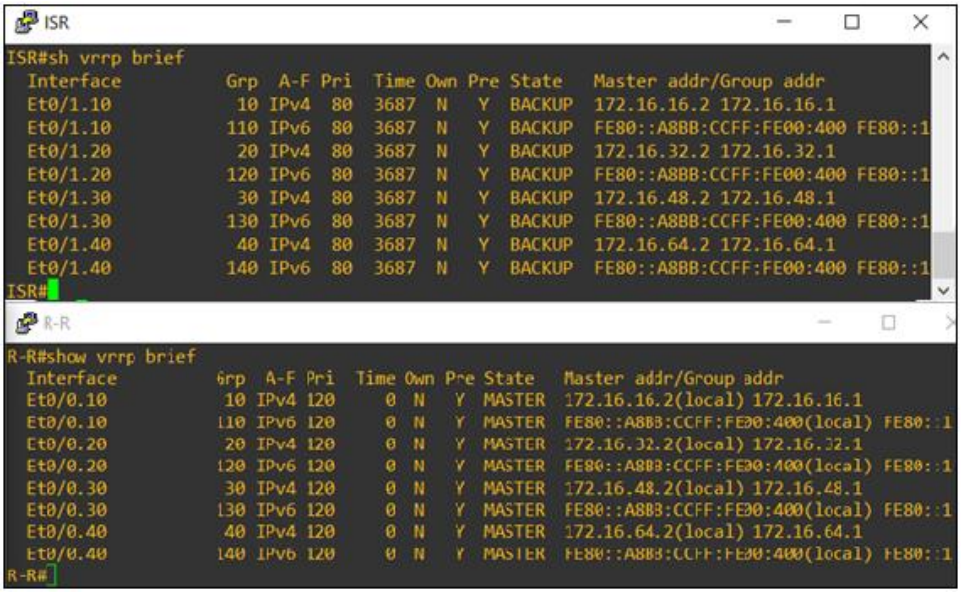
Figura 4.12 Comprobación de Conectividad WAN



Comprobación de Conectividad WAN desde un host virtual en la VLAN Gestión. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la Figura 3.13 se indica el estado de los enlaces MAESTRO y BACKUP para asegurar alta disponibilidad entre los equipos de la red de frontera.

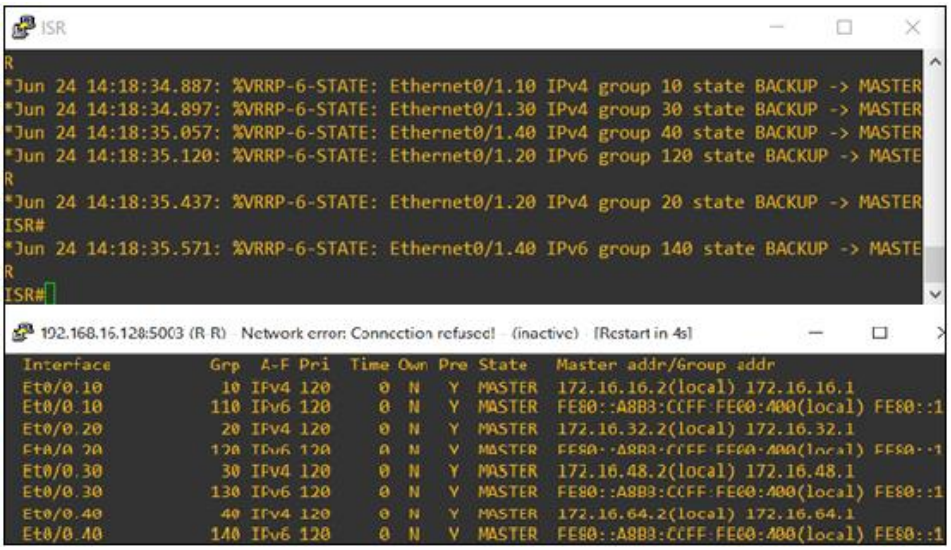
Figura 4.13 Estado de los enlaces de Alta Disponibilidad



Estado de los enlaces entre equipos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

En la Figura 3.14 se indica el cambio entre los enlaces MAESTRO y BACKUP cuando haya ocurrido una falla física entre los equipos L3_CORE entre R_R a L3_CORE entre ISR.

Figura 4.14 Cambio entre enlaces de Alta Disponibilidad



Cambio del enlace MAESTRO al enlace BACKUP. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

4.3 Análisis del Costo de Implementación

A continuación, se presenta el análisis CAPEX (Costos de Capital) y OPEX (Costos de Operación) para determinar la viabilidad del proyecto.

4.3.1 CAPEX

En la tabla a continuación se muestran una lista de los equipos y respectivos costos que intervienen en el diseño de la red de frontera para el CFCSB en base a cotizaciones realizadas por parte de distribuidores. (Anexo 10)

Tabla 4.1 Listado y descripción de equipos

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR				11/06/2019
Proyecto de Diseño de la Red de Frontera para el Centro de Formación Continua San Bartolo				
ÍTEM	**DESCRIPCIÓN**	**CANTIDAD**	**P. UNITARIO**	**TOTAL**
1	HPE ProLiant DL160 Gen10	1	5843,47	5843,47
2	CISCO 4421 ISR	1	1571,43	1571,43
3	UPS CDP on-line 6KVA 5400 W bifásico bypass 220/110V	1	2400	2400
4	CISCO 921-4P	1	845	845
5	Distribuidor de fibra óptica modelo: DFOP 1	1	90	90
6	Patch cord 3 pies (certificado)	7	11,25	78,75
7	Patch cord 7 pies (certificado)	3	14,25	42,75
	Precio Sin IVA			10871,4
	IVA 12%			1304,57
	Precio TOTAL			12175,97

Listado de equipos y costos. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

4.3.2 OPEX

Los costos de operación que conllevan el correcto funcionamiento y operación de la red de frontera del centro son aquellos para la administración, operación y mantenimiento de los equipos y del sistema de alimentación ininterrumpida (SAI), como también la contratación de un proveedor de servicios de que preste su infraestructura de fibra óptica o de cobre para el enlace WAN como también que de acceso al Internet.

En la Tabla 4.2 se muestra el costo de mano de obra mensual requerido para el diseño técnico de la red de frontera.

Tabla 4.2 Costo mensual del trabajo técnico

Trabajador	Días/Mes	Horas diarias	Costo Hora	TOTAL
Cahueñas Juan	6	4	$12	$ 288
Lizarzaburu Jonathan	6	4	$12	$ 288
VALOR MENSUAL TOTAL				$ 576

Detalle del costo mensual del trabajo técnico de la red de frontera. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Se prevé que las labores se lleven a cabo en un transcurso de cuatro meses, por lo que el valor total de mano de obra es de $2304, el cual se añade al costo total mostrado en la Tabla 4.1, ascendiendo a un valor total de inversión de $14479,97.

En la siguiente tabla se presentan los costos operativos mensuales previstos de la red de frontera ya en operaciones.

Tabla 4.3 Costos operativos mensuales

Egresos	Valor mensual (USD)
Plan de Internet de 100 Mbps	149,59
Costo de enlace WAN	45
Gastos de Operación	161,62
VALOR TOTAL DE EGRESOS	356,21

Costos operativos mensuales de la red de frontera en operaciones. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

A continuación, se muestran la tabla con los valores que el CFCSB ahorrará con la implementación de la red de frontera.

Tabla 4.4 Valor de ahorro para el centro

Detalle	Cantidad	Costo (USD)			Costo Mensual (USD)
Llamadas hacia la matriz	500	Pensión Mensual (USD)	Costo Minuto (USD)	Duración (min)	78,44
		13,44	0,026	5	
NGFW dedicado	1	108 (Anual)			9
Planes celulares	110	11,50			1265
VALOR TOTAL DE AHORRO					1352,44

Costo total de ahorro para el CFCSB. Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

4.3.3 Recuperación de la Inversión

Ya que se han definido los egresos y el ahorro que el proyecto llegaría a generar, es posible determinar el flujo efectivo.

En la Tabla 4.4 se indica el flujo neto efectivo trimestral, con una depreciación anual del 10% del costo total del proyecto. (Derecho Ecuador, 2019)

Tabla 4.5 Flujo Neto de Efectivo

Periodo	0	1er Trimestre	2do Trimestre	3er Trimestre	4to Trimestre	5to Trimestre	6to Trimestre
Ahorro	-	4057,32	4057,32	4057,32	4057,32	4057,32	4057,32
Gastos Operativos	-	1068,63	1068,63	1068,63	1068,63	1068,63	1068,63
Depreciación	-	361,98	361,98	361,98	361,98	361,98	361,98
Utilidad	-	2626,71	2626,71	2626,71	2626,71	2626,71	2626,71
Inversión	-14479,97						
Flujo Efectivo Neto	-14479,97	-11853,26	-9226,55	-6599,64	-3973,12	-1346.42	1280,29

Recuperación de la inversión (Detalle, ver Anexo 11). Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

El análisis realizado en la tabla anterior muestra que la inversión retornará en un periodo de seis trimestres; es decir, en un año y seis meses.

CONCLUSIONES

En base al Diseño Empresarial de Borde de Internet de Cisco y el uso de herramientas de software libre, se ha presentado una propuesta para la red de frontera para el Centro de Formación Continua San Bartolo brindando a estudiantes, docentes y personal administrativo de los recursos de red para acceder al Internet enriqueciendo el proceso de enseñanza-aprendizaje dentro de sus aulas y laboratorios.

La configuración de los módulos: Conexión a Internet, Acceso Remoto y VPN; y los mecanismos de seguridad: Firewall, ACLs, Filtrado de Contenido y Autenticación de usuarios remotos en S.O. open source, disminuyen el número de dispositivos activos necesarios y se añaden funcionalidades de administración para la red en conjunto, reduciendo los costos de la implementación del proyecto.

Por medio del modelamiento de las redes de campus y frontera en el software OPNET Modeler se determinó que el mecanismo de calidad de servicio óptimo es el de Servicios Diferenciados (DiffServ) basados en PQ con el que se ha conseguido reducir el Delay de 6 ms a 2 ms, Jitter a valores menores a 1 ms y Throughput de 0,8 Mbps a 0,95 Mbps del diseño preliminar de la red del centro.

El análisis del costo de implementación del proyecto determinó que es viable económicamente, ya que ahorrará a la institución aproximadamente 16229 USD anuales, valor con el cual la inversión retornará en un período de un año y seis meses.

RECOMENDACIONES

Para implementar un bloqueo avanzado de amenazas se recomienda la instalación de equipos Cisco Firepower o Cisco Meraki MX a la red de borde, ya que estos dispositivos de alto rendimiento brindan funciones dedicadas de Firewall y brindan mecanismos de seguridad avanzados que aseguran la continuidad del funcionamiento de la red.

Se recomienda la contratación de un proveedor de servicios de Internet que provea al centro un ancho de banda mínimo de 100 Mbps para asegurar una comunicación y conexión a Internet estable por parte de quienes se conecten a la red.

Se recomienda la instalación de un sistema de alimentación ininterrumpida tipo torre y un tablero de bypass, para que de esta manera los procesos de mantenimiento sean desarrollados con seguridad, en un menor tiempo y con mayor comodidad.

De acuerdo al número y tipo de equipos instalados en el rack principal, se recomienda establecer una fuente de alimentación de 220 VAC para suministrar la tensión indicada por el fabricante del equipo.

BIBLIOGRAFÍA

Al-shawi, M. (2016). CCDE Study Guide. Indianápolis: Pearson Education, Inc.

Álvarez L., Suárez K. (septiembre de 2018). Diseño De La Red De Campus Para El Centro De Formación Continua San Bartolo De La Universidad Politécnica Salesiana. Quito.

Bustamante, R. (25 de Marzo de 2017). Parámetros de Calidad de Servicio (QoS). Perú: Universidad Nacional Mayor de San Marcos. Obtenido de https://www.academia.edu/10963565/PARAMETROS_DE_CALIDAD_DE_SERVICIO_CALIDAD_DE_SERVICIO_QoS

Camarena, A. (20 de noviembre de 2017). ¿Cual debería de ser el tamaño de una página web? Obtenido de https://www.espai.es/blog/2017/11/cual-deberia-ser-el-tamano-de-una-pagina-web/

Chung, J., Pueblas, M., Nadimi, A., Hamilton, D., & Farrington, S. (2016). Cisco SAFE Reference Guide. Estados Unidos: Cisco Systems, Inc.

CISCO. (Octubre de 2015). Cisco Validated Design, Internet Edge Design Summary. Obtenido de https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/Internet_Edge_Design_Oct2015.pdf

Cisco Networking Academy. (9 de mayo de 2014). Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Obtenido de http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=6

Derecho Ecuador. (2019). DEPRECIACIONES DE ACTIVOS FIJOS. Obtenido de https://www.derechoecuador.com/depreciaciones-de-activos-fijos

Federal Communications Commission. (6 de Febrero de 2018). Guía de Velocidades de Banda Ancha. Obtenido de https://www.fcc.gov/consumers/guides/guia-de-velocidades-de-banda-ancha

González, M. (2016). Tecnologías de Virtualización. España: CreateSpace Independent Pub.

Google Maps. (23 de febrero de 2019). Obtenido de https://www.google.com/maps/place/Joaquin+Gutierrez+%26+Teodoro+Gomez+de+La+Torre,+Quito+170148/@-0.2622576,-78.5259067,3a,75y,110.4h,100.55t/data=!3m9!1e1!3m7!1sc8IDOgeUAhbvpv8k0i32YQ!2e0!7i13312!8i6656!9m2!1b1!2i26!4m5!3m4!1s0x91d598f9628

c7c81:0x339924e

INEC. (2017). Encuesta Tecnológica. Quito.

ISO. (2019). Sistemas de Gestión de Riesgos y Seguridad. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Juca, P. (2016). Estudio de la implementación de Calidad de Servicio (QoS) para el mejoramiento de la red de datos que optimice el acceso a los servicios en la Planta de Producción de la Compañía Yanbal Ecuador S.A. Quito.

Khosrow-Pour, M. (2018). Optimizing Contemporary Application and Processes in Open Source Software. Estados Unidos: IGI Global.

Menéndez, S. (2016). UF1880 - Gestión de redes telemáticas. España: Editorial Elearning S.L.

Oppenheimer, P. (s.f). Top-Down Network Design. Indianapolis: Cisco Systems, Inc.

Oracle. (Julio de 2014). Planificación de la Política de Calidad de Servicio. Obtenido de https://docs.oracle.com/cd/E56339_01/html/E53875/ipqos-config-planning-7.html#scrolltoc

Pope, S. (5 de Junio de 2018). Your Security 'Game Plan': Is it Reactive or Proactive? Obtenido de https://blogs.cisco.com/security/its-time-to-turn-your-access-control-perimeter-into-a-threat-control-perimeter

Salazar, E. (2015). Tráfico en Redes de Voz. Pereira.

Salazar, G. (30 de Septiembre de 2016). Fundamentos de QoS - Calidad de Servicio en Capa 2 y Capa 3. Quito. Obtenido de https://community.cisco.com/t5/blogs-routing-y-switching/fundamentos-de-qos-calidad-de-servicio-en-capa-2-y-capa-3/ba-p/3103715

Singh, H. (2017). Implementing Cisco Networking Solutions. Birmingham: Packt Publishing.

Team Nuggets. (11 de Enero de 2016). Top-Down vs. Bottom-Up Network Design. Obtenido de https://www.cbtnuggets.com/blog/2016/01/top-down-vs-bottom-up-network-design/

Westway Engineers. (16 de Junio de 2017). Erlangs and VoIP Bandwidth Calculator. Obtenido de https://www.erlang.com/calculator/eipb/

Xyfon Solutions. (24 de Octubre de 2013). How Virtualization Works. Obtenido de https://xyfon.com/how-virtualization-works/

Zientara, D. (2018). Mastering pfSense (Segunda Edición ed.). Birmingham, Reino Unido: Packt Publishing Ltd.

ANEXOS

Anexo 1. Cuadrante de Gartner para la selección del servidor

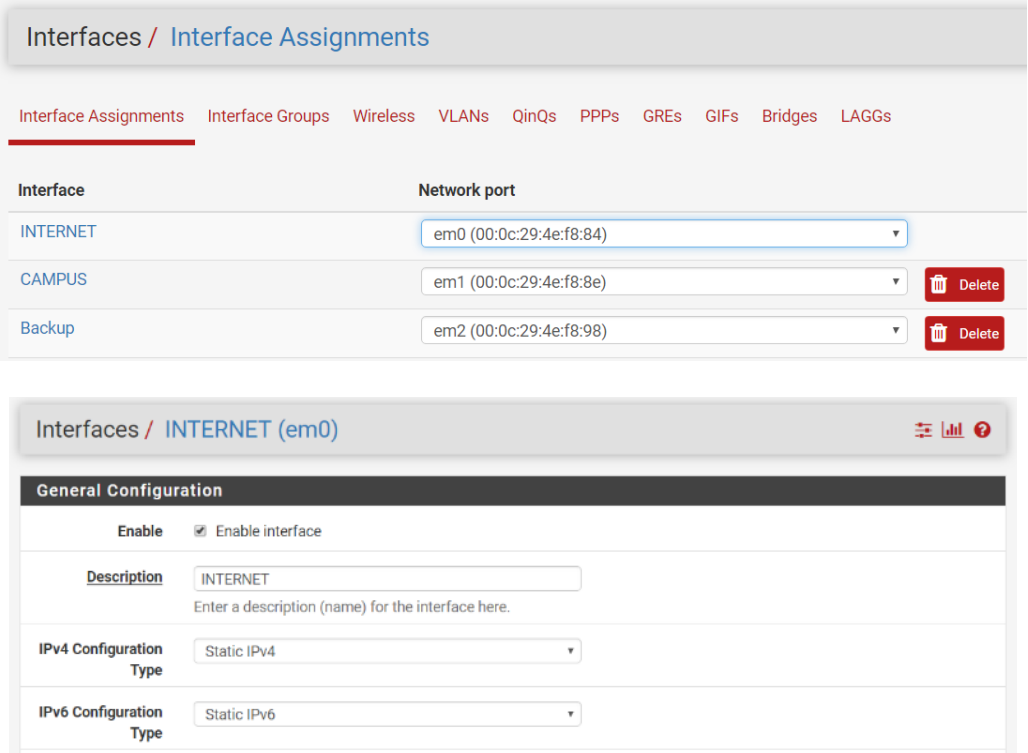
Fuente: (Houston, 2016)

Anexo 2. Características para la selección de Servidor

Marca / Parámetros	HPE ProLiant DL160 Gen10		CISCO UCS C220 M4		DELL EMC PowerEdge R740	
	Disco Duro 120GB/16 GB RDIMM	Disco Duro 120GB/32 GB RDIMM	Disco Duro 1TB/16 GB RDIMM	Disco Duro 5TB/32 GB RDIMM	Disco Duro 1.6TB/16 GB RDIMM	Disco Duro 1.6TB/32 GB RDIMM
Precio	$ 5.843,47	$ 6.177,48	$ 6.878.40	$ 8.122.30	$ 5.537,15	$ 5.790,63
Procesador	Intel Xeon Silver 4110	Intel Xeon Silver 4110	Intel Xeon E5-2600 v3	Intel Xeon E5-2600 v3	Intel Xeon de 2da Generación	Intel Xeon de 2da Generación
Capacidad Máxima de Memoria	RDIMM 256 GB	RDIMM 256 GB	Cisco 64G SAS Modular RAID	Cisco 64G SAS Modular RAID	3 TG DIMM DDR4	3 TG DIMM DDR4
RAID Software	HPE Smart Array S100i SR Gen10 SW RAID	HPE Smart Array S100i SR Gen10 SW RAID	Cisco 12G SAS Modular RAID	Cisco 12G SAS Modular RAID	PERC H330, H730p, H740p, RAID de software (SWRAID) S140	PERC H330, H730p, H740p, RAID de software (SWRAID) S140
Almacenamiento interno máximo	9.6 TB	9.6 TB	64 GB (x2)	64 GB (x2)	240 GB	240 Gb
Fuente de Poder	HPE 500W Flex Slot	HPE 500W Flex Slot	770 W (CA) 0 1050 W (CC)	770 W (CA) 0 1050 W (CC)	Titanium de 750 W, Platinum de 495 W, 750 W, 1100 W, 1600 W y 2000 W	Titanium de 750 W, Platinum de 495 W, 750 W, 1100 W, 1600 W y 2000 W
Fuente de Poder Redundante	Si	Si	Si	Si	Si	Si
Interfaces	Video, Puertos de red, HPE iLO Remote Management Network Port, Front iLO Service Port, Micro SD Slot, USB 3.0	Video, Puertos de red, HPE iLO Remote Management Network Port, Front iLO Service Port, Micro SD Slot, USB 3.0	2 puertos i350, GBeth, PXE boot, DB15 VGA connector, RJ45 serial port, USB 3.0 (x2), KVM, VIC, CNA, HBA.	2 puertos i350, GBeth, PXE boot, DB15 VGA connector, RJ45 serial port, USB 3.0 (x2), KVM, VIC, CNA, HBA.	4 x 1 GE o 2 x 10 GE + 2 x 1 GE o 4 x 10 GE o 2 x 25 GE, Video, 2 x USB 2.0, USB 3.0 disponible, IDRAC dedicada, Tarjeta de video VGA	4 x 1 GE o 2 x 10 GE + 2 x 1 GE o 4 x 10 GE o 2 x 25 GE, Video, 2 x USB 2.0, USB 3.0 disponible, IDRAC dedicada, Tarjeta de video VGA
Sistemas Operativos	Windows Server (2016/2019), VMware (U1/U2/U3), Red Hat Enterprise Linux, SUSE Linux Enterprise Server	Windows Server (2016/2019), VMware (U1/U2/U3), Red Hat Enterprise Linux, SUSE Linux Enterprise Server	Windows 8 posterior, Windows Server 2012 o posterior, Linux RHEL (6.5/6.6/6.7/7.0/7.2/ SLES) VMware	Windows 8 posterior, Windows Server 2012 o posterior, 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, VMware ESXi	Canonical, Ubuntu LTS Citrix XenServer Microsoft Windows Server con Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi
Gráficos	Modos de Video de 32 bpp 16MB de Memori de Video	Modos de Video de 32 bpp 16MB de Memoria de Video	Matrox G200e video/controlador gráfico	Matrox G200e video/controlador gráfico	Matrox G200eW3 16MB de Memoria de Video	Matrox G200eW3 16MB de Memoria de Video
Chasis	4 LFF 8 SFF	4 LFF 8 SFF	M4 LFF M4 SFF	M4 LFF M4 SFF	SFF	SFF
Ventiladores	3 Estándar	3 Estándar	6	6	6	6
Factor de Forma	1U Rack	1U Rack	1U Rack	1U Rack	2U Rack	2U Rack
Garantía	3 en partes 3 de funcionamiento, 3 años de asistencia en el sitio con respuesta al siguiente día hábil	3 en partes 3 de funcionamiento, 3 años de asistencia en el sitio con respuesta al siguiente día hábil	3 años en partes, 90 días en software con respuesta al siguiente día hábil	3 años en partes, 90 días en software con respuesta al siguiente día hábil	No especificada	No especificada
Slots	3 Slots PCIe 3.0	3 Slots PCIe 3.0	2 Slots PCIe Riser	2 Slots PCIe Riser	8 Gen3	8 Gen3
Batería Reemplazable	Si	Si	Si	Si	Si	Si

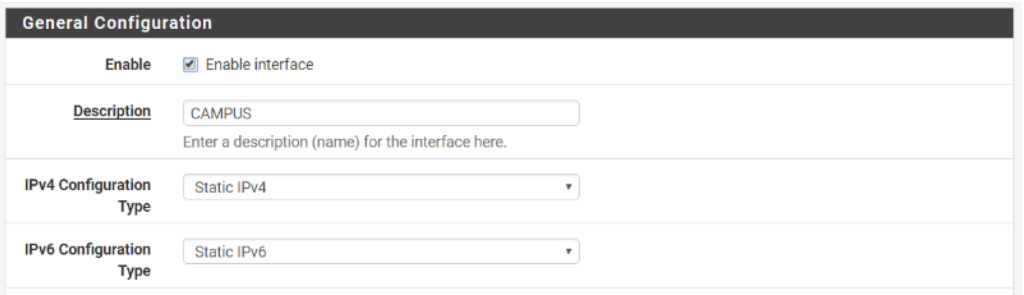
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Anexo 3. Configuración del Firewall de Siguiente Generación

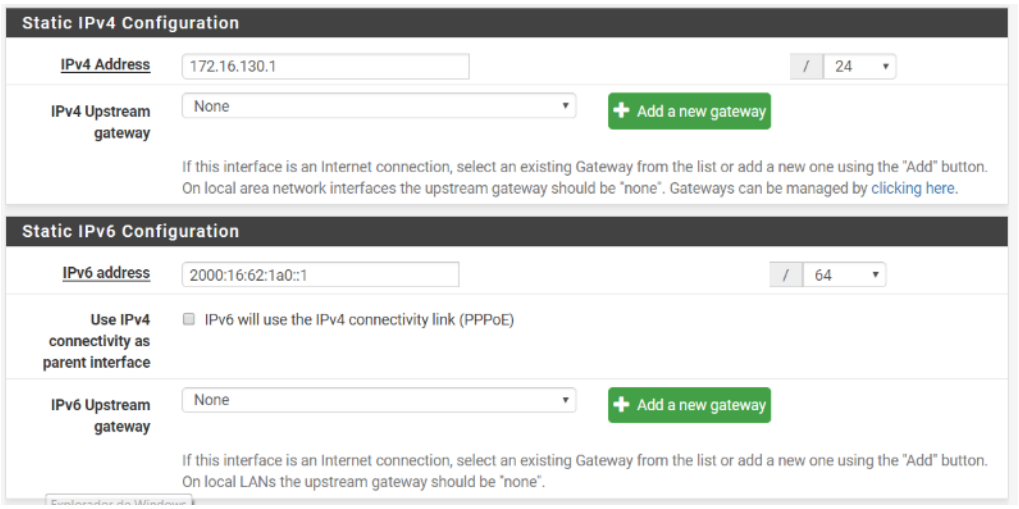


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

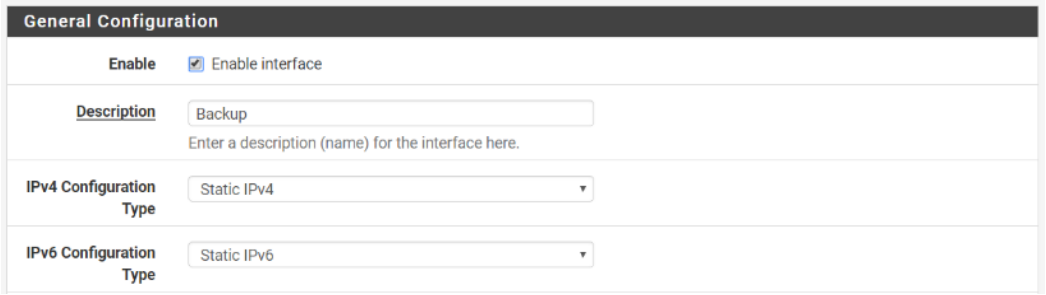
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

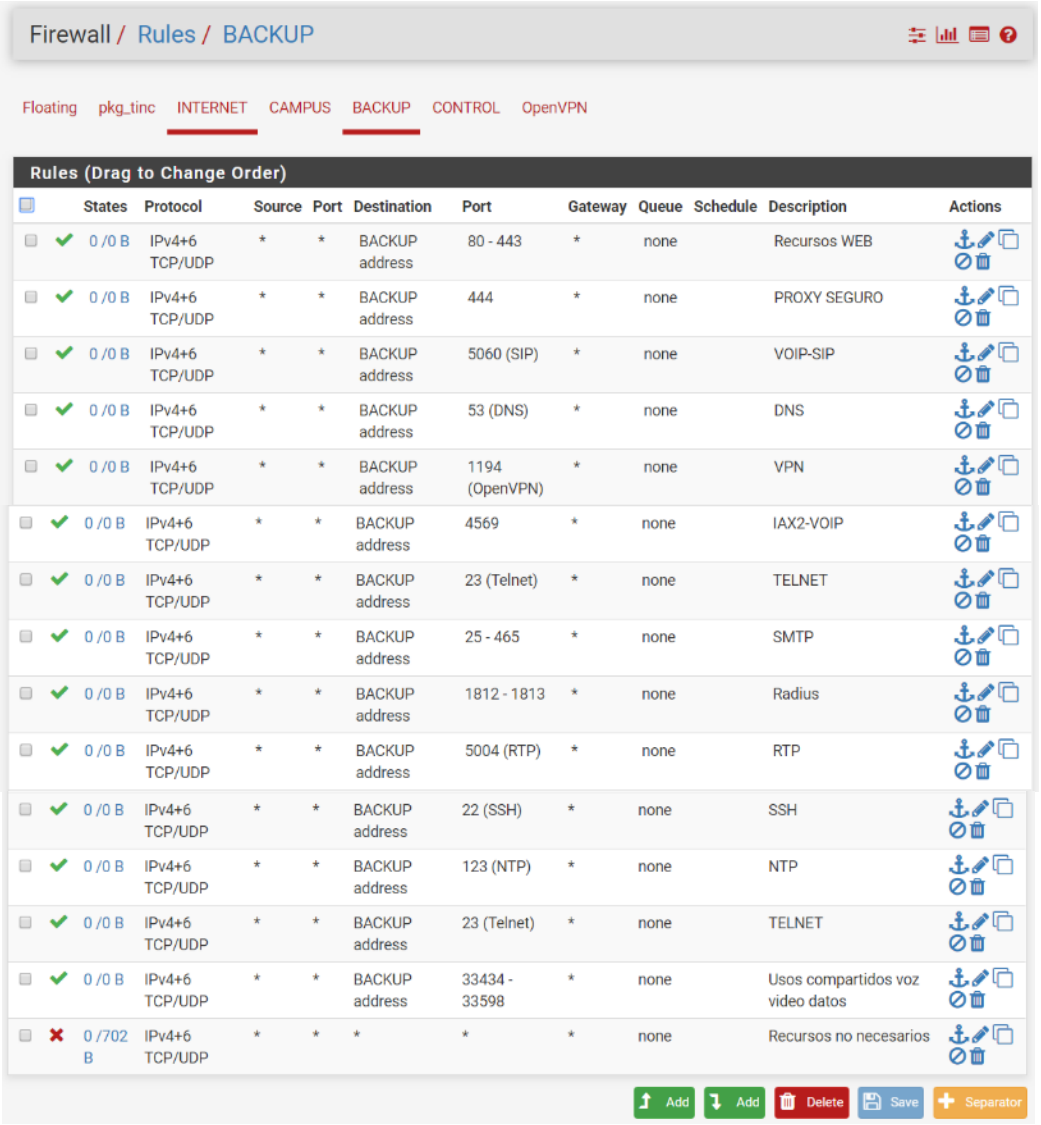


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

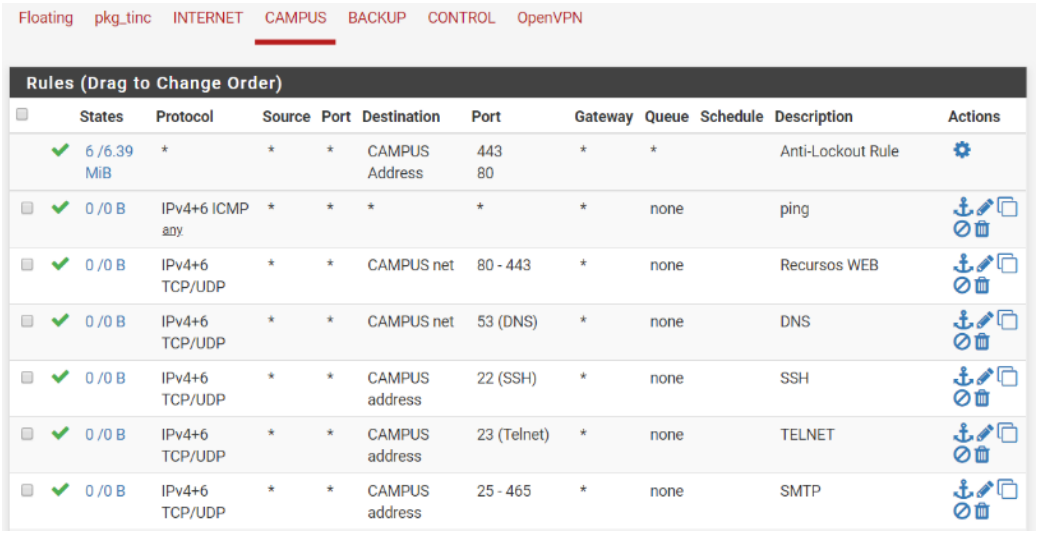


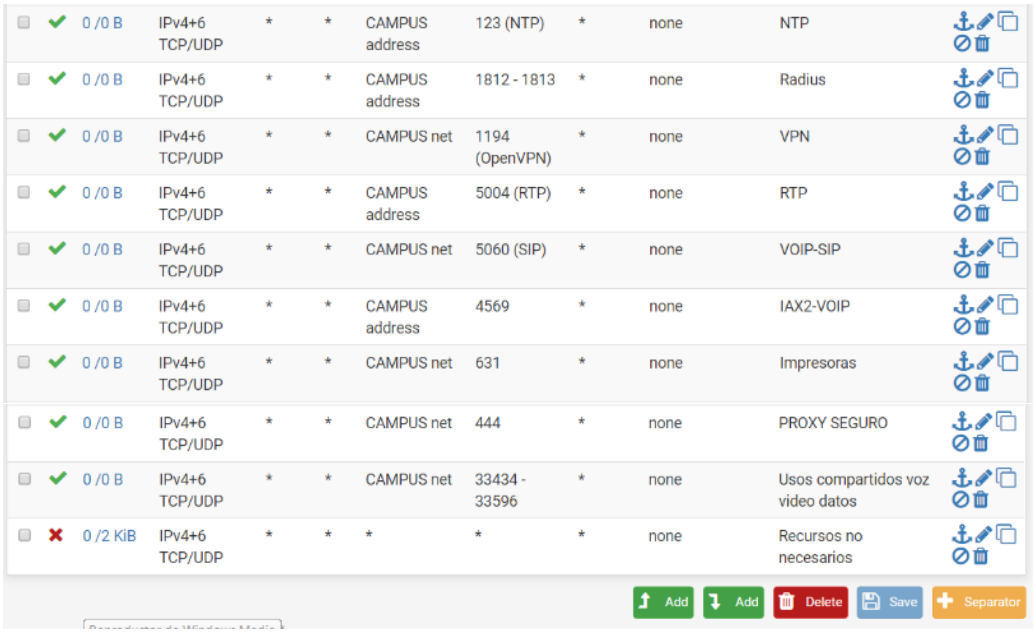
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

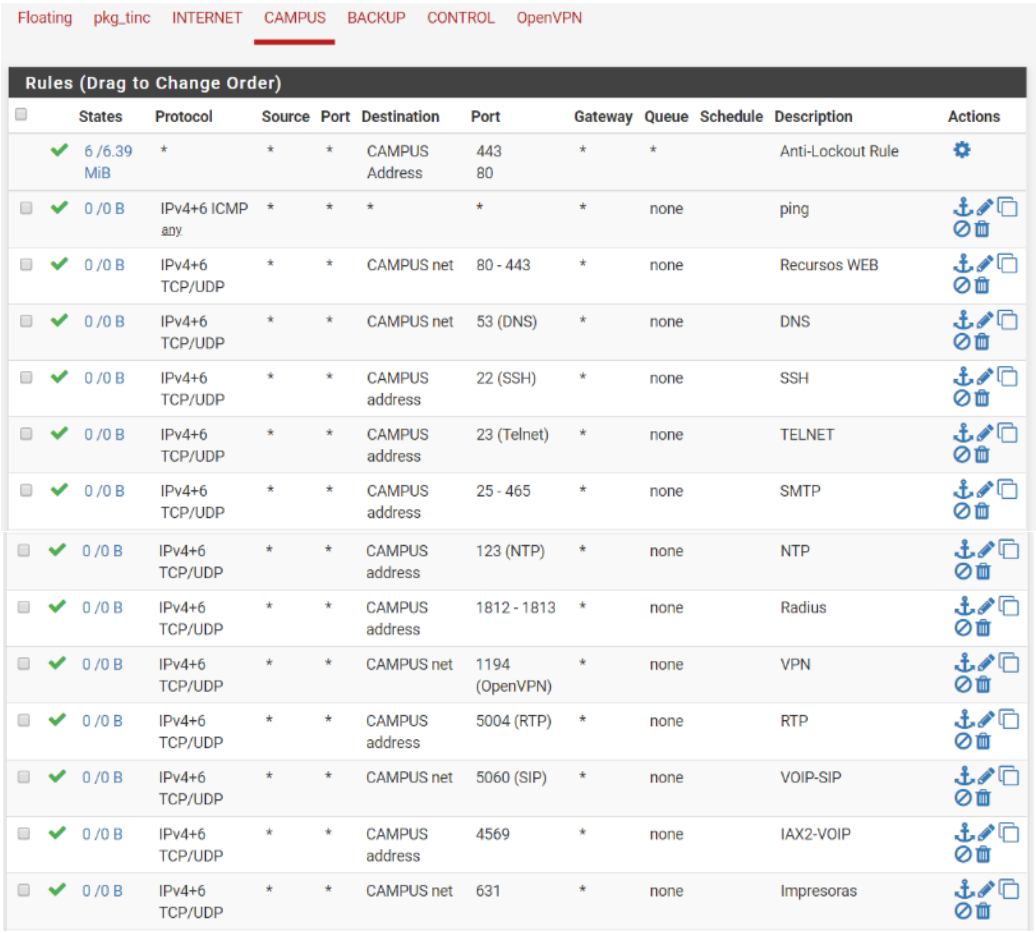




✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	123 (NTP)	*	none	NTP
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	1812 - 1813	*	none	Radius
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	1194 (OpenVPN)	*	none	VPN
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	5004 (RTP)	*	none	RTP
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	5060 (SIP)	*	none	VOIP-SIP
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	4569	*	none	IAX2-VOIP
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	631	*	none	Impresoras
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	444	*	none	PROXY SEGURO
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	33434 - 33596	*	none	Usos compartidos voz video datos
✗	0 /2 KiB	IPv4+6 TCP/UDP	*	*	*	*	*	none	Recursos no necesarios

Add Add Delete Save Separator

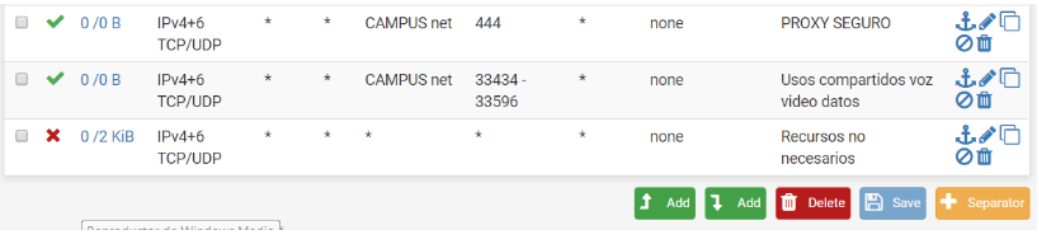
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Floating pkg_tinc INTERNET CAMPUS BACKUP CONTROL OpenVPN

Rules (Drag to Change Order)

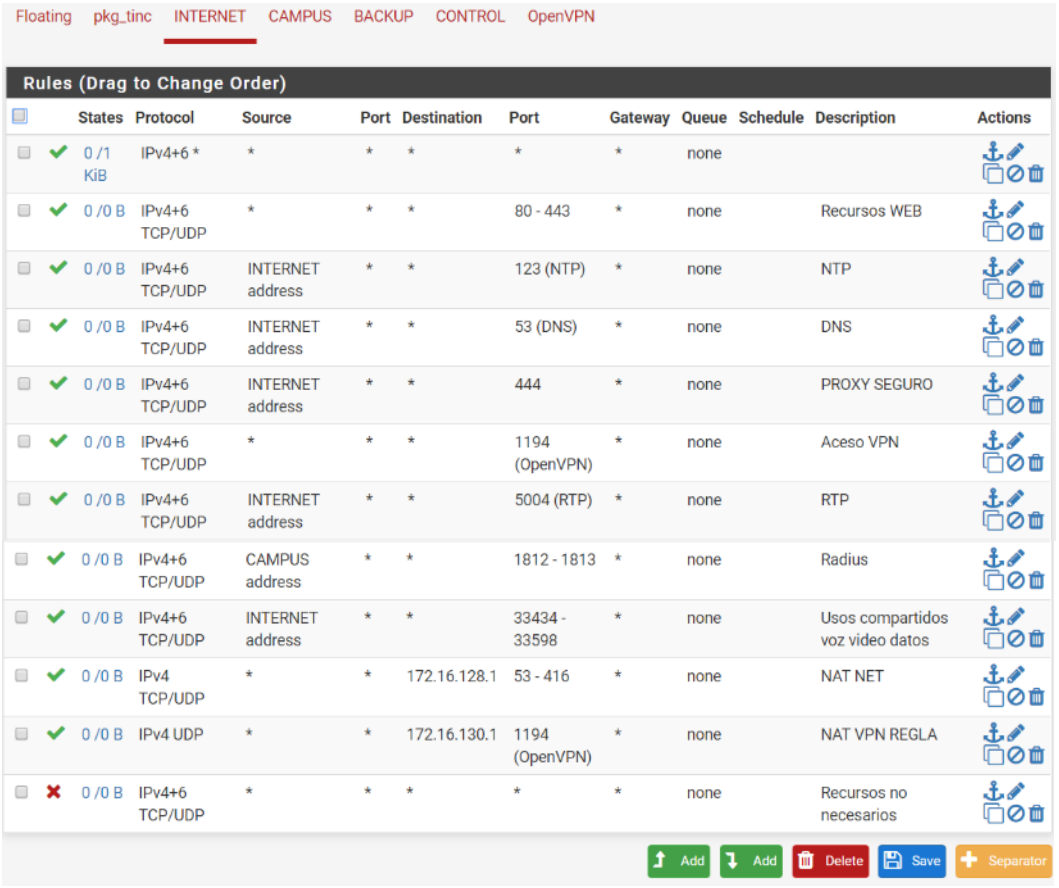
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	6 /6.39 MiB	*	*	*	CAMPUS Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	0 /0 B	IPv4+6 ICMP any	*	*	*	*	*	none		ping	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	80 - 443	*	none		Recursos WEB	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	53 (DNS)	*	none		DNS	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	22 (SSH)	*	none		SSH	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	23 (Telnet)	*	none		TELNET	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	25 - 465	*	none		SMTP	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	123 (NTP)	*	none		NTP	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	1812 - 1813	*	none		Radius	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	1194 (OpenVPN)	*	none		VPN	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	5004 (RTP)	*	none		RTP	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	5060 (SIP)	*	none		VOIP-SIP	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS address	4569	*	none		IAX2-VOIP	
✓	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	631	*	none		Impresoras	



	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	444	*	none	PROXY SEGURO	
	0 /0 B	IPv4+6 TCP/UDP	*	*	CAMPUS net	33434 - 33596	*	none	Usos compartidos voz video datos	
	0 /2 KiB	IPv4+6 TCP/UDP	*	*	*	*	*	none	Recursos no necesarios	

Add Add Delete Save Separator

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



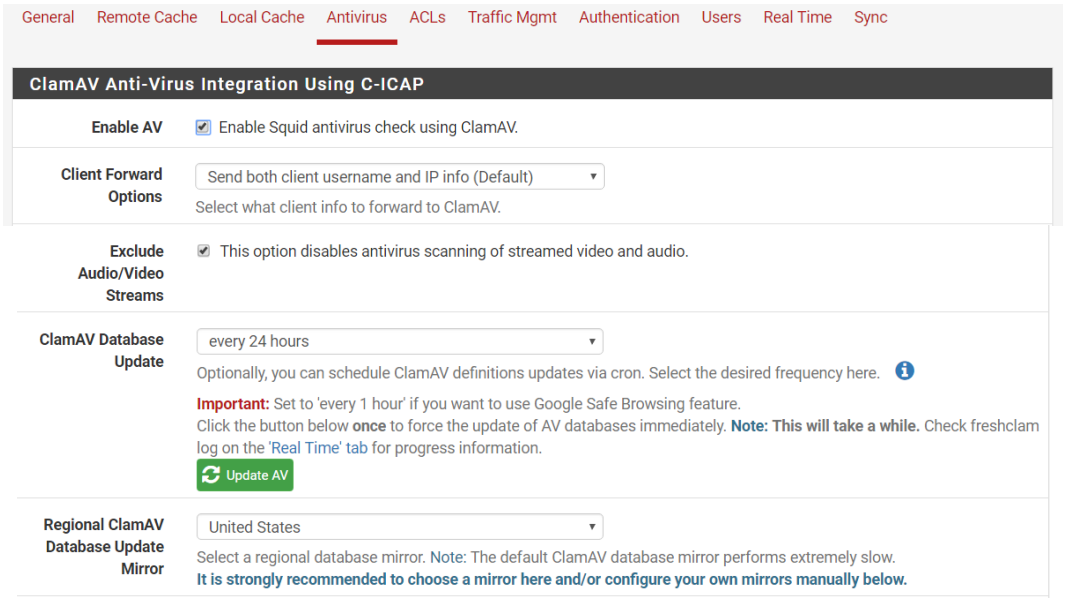
Floating pkg_tinc INTERNET CAMPUS BACKUP CONTROL OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /1 KiB	IPv4+6 *	*	*	*	*	*	none			
	0 /0 B	IPv4+6 TCP/UDP	*	*	*	80 - 443	*	none		Recursos WEB	
	0 /0 B	IPv4+6 TCP/UDP	INTERNET address	*	*	123 (NTP)	*	none		NTP	
	0 /0 B	IPv4+6 TCP/UDP	INTERNET address	*	*	53 (DNS)	*	none		DNS	
	0 /0 B	IPv4+6 TCP/UDP	INTERNET address	*	*	444	*	none		PROXY SEGURO	
	0 /0 B	IPv4+6 TCP/UDP	*	*	*	1194 (OpenVPN)	*	none		Aceso VPN	
	0 /0 B	IPv4+6 TCP/UDP	INTERNET address	*	*	5004 (RTP)	*	none		RTP	
	0 /0 B	IPv4+6 TCP/UDP	CAMPUS address	*	*	1812 - 1813	*	none		Radius	
	0 /0 B	IPv4+6 TCP/UDP	INTERNET address	*	*	33434 - 33598	*	none		Usos compartidos voz video datos	
	0 /0 B	IPv4 TCP/UDP	*	*	172.16.128.1	53 - 416	*	none		NAT NET	
	0 /0 B	IPv4 UDP	*	*	172.16.130.1	1194 (OpenVPN)	*	none		NAT VPN REGLA	
	0 /0 B	IPv4+6 TCP/UDP	*	*	*	*	*	none		Recursos no necesarios	

Add Add Delete Save Separator

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

ClamAV Anti-Virus Integration Using C-ICAP

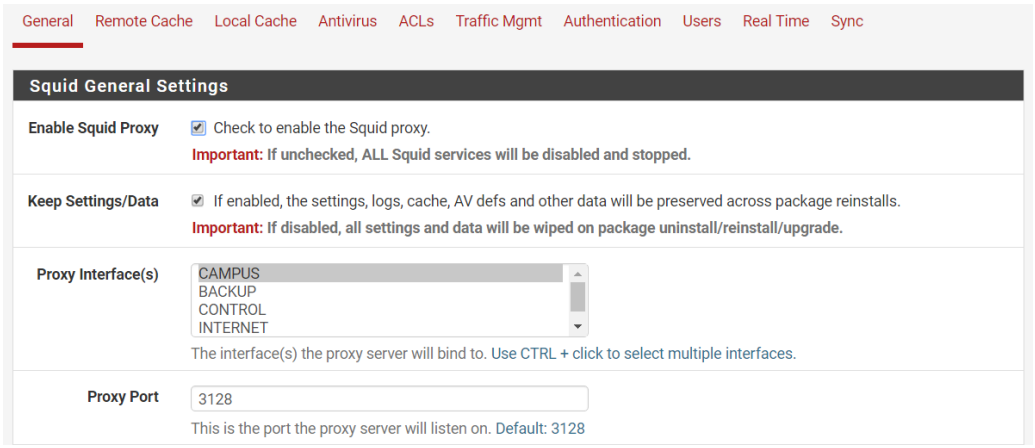
Enable AV — Enable Squid antivirus check using ClamAV.

Client Forward Options — Send both client username and IP info (Default)
Select what client info to forward to ClamAV.

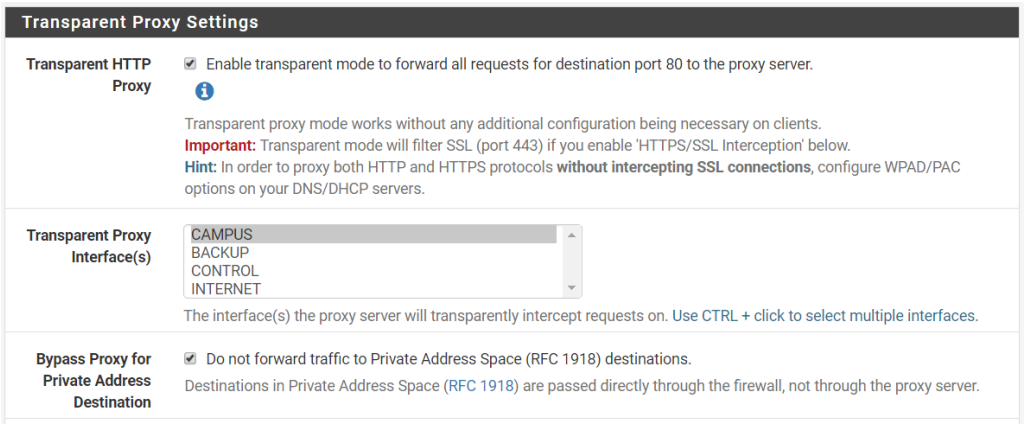
Exclude Audio/Video Streams — This option disables antivirus scanning of streamed video and audio.

ClamAV Database Update — every 24 hours
Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here.
Important: Set to 'every 1 hour' if you want to use Google Safe Browsing feature.
Click the button below **once** to force the update of AV databases immediately. **Note: This will take a while.** Check freshclam log on the 'Real Time' tab for progress information.
Update AV

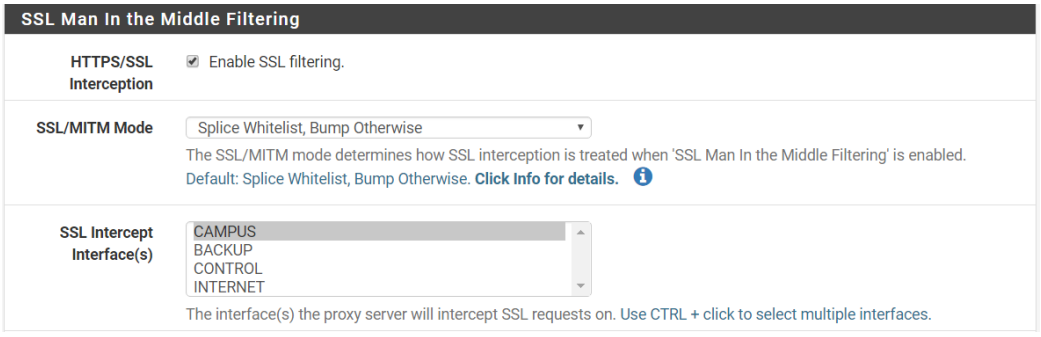
Regional ClamAV Database Update Mirror — United States
Select a regional database mirror. Note: The default ClamAV database mirror performs extremely slow.
It is strongly recommended to choose a mirror here and/or configure your own mirrors manually below.



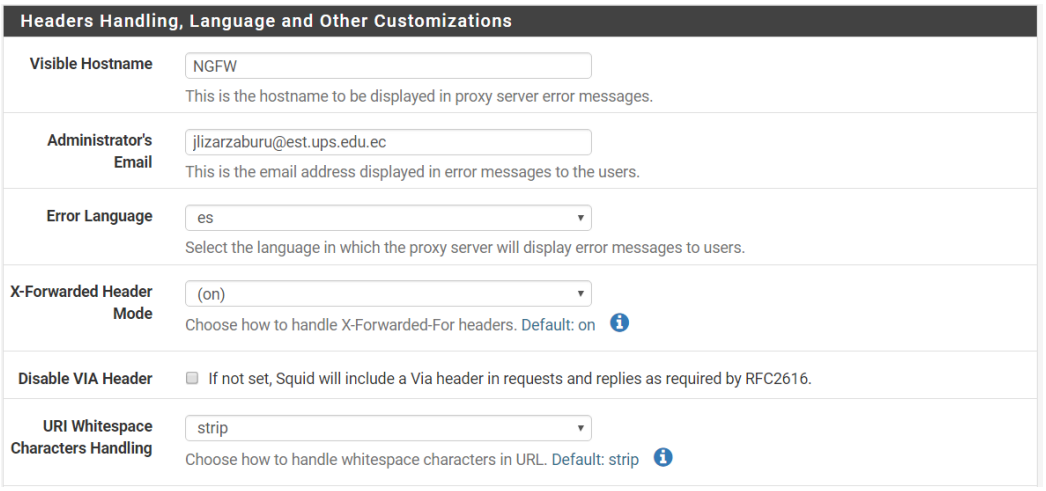
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

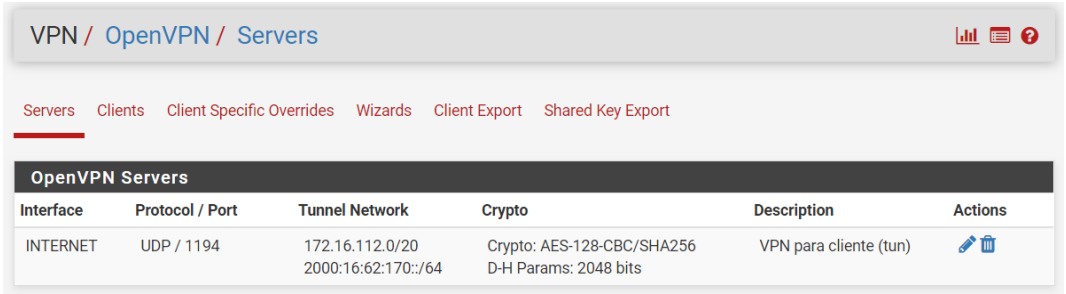


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

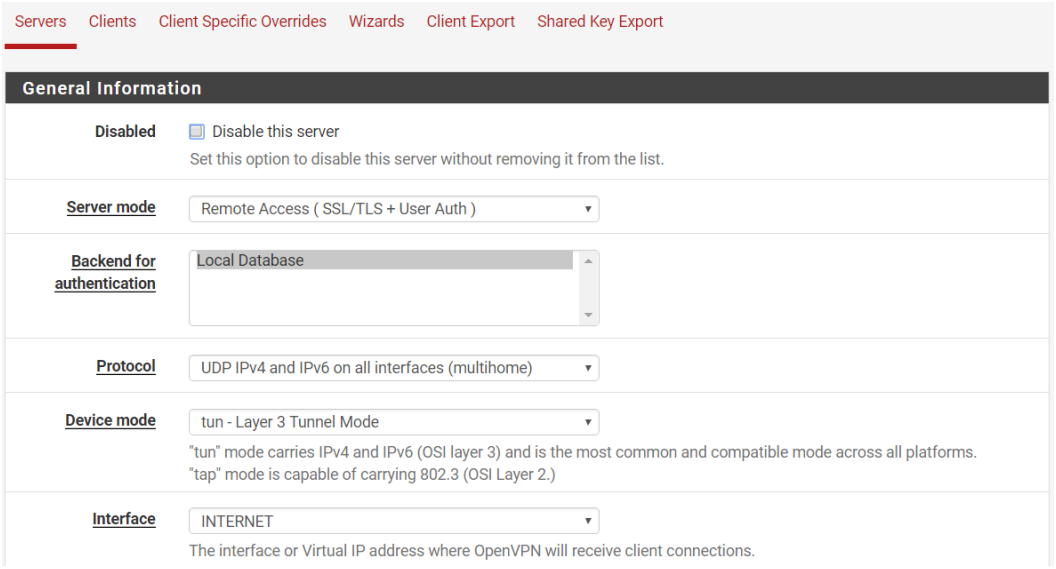


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

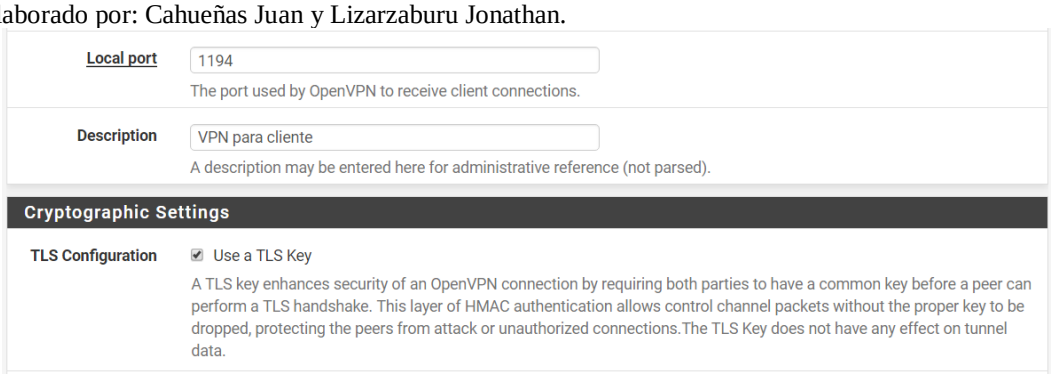
Anexo 4. Configuración de Usuarios VPN

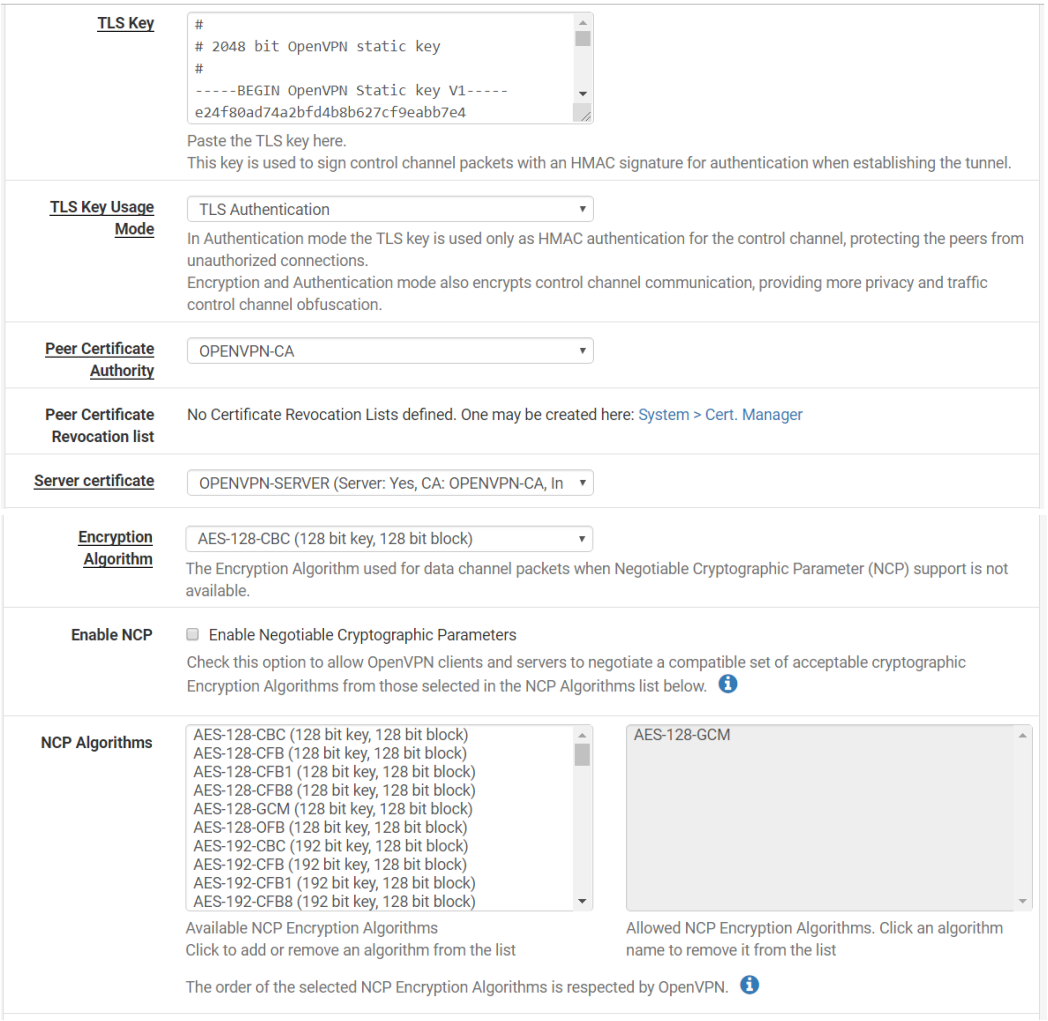


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

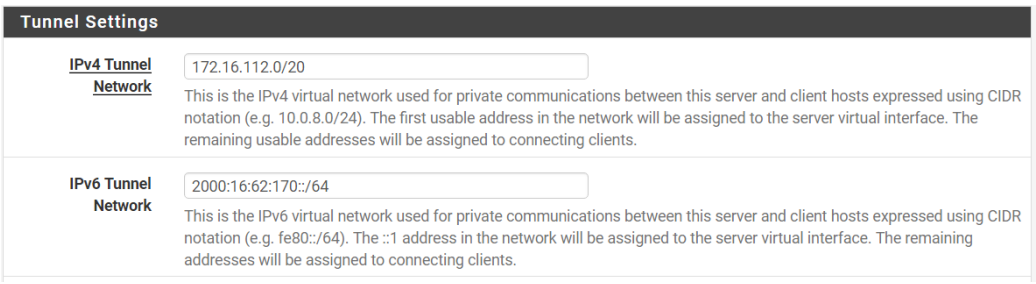


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

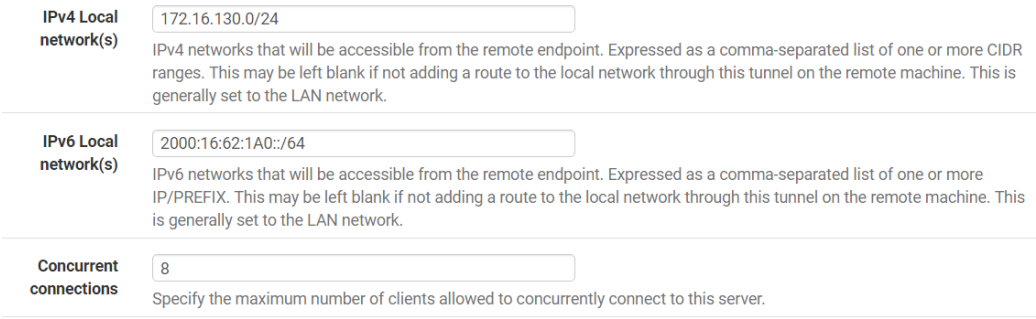


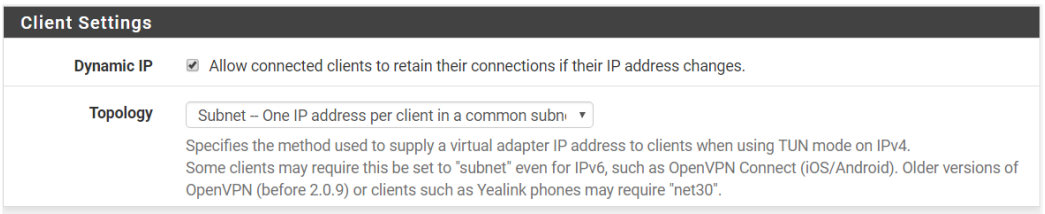


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

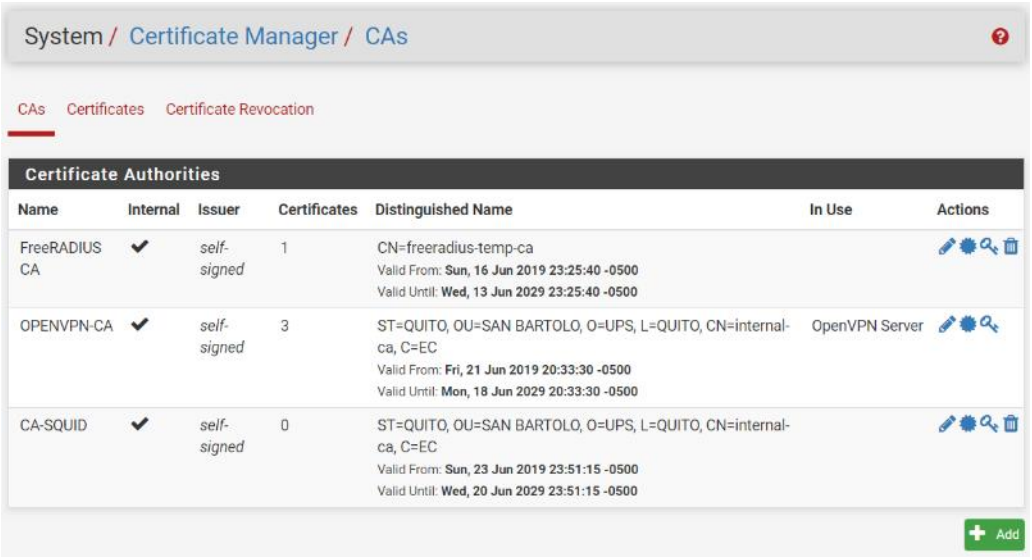


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

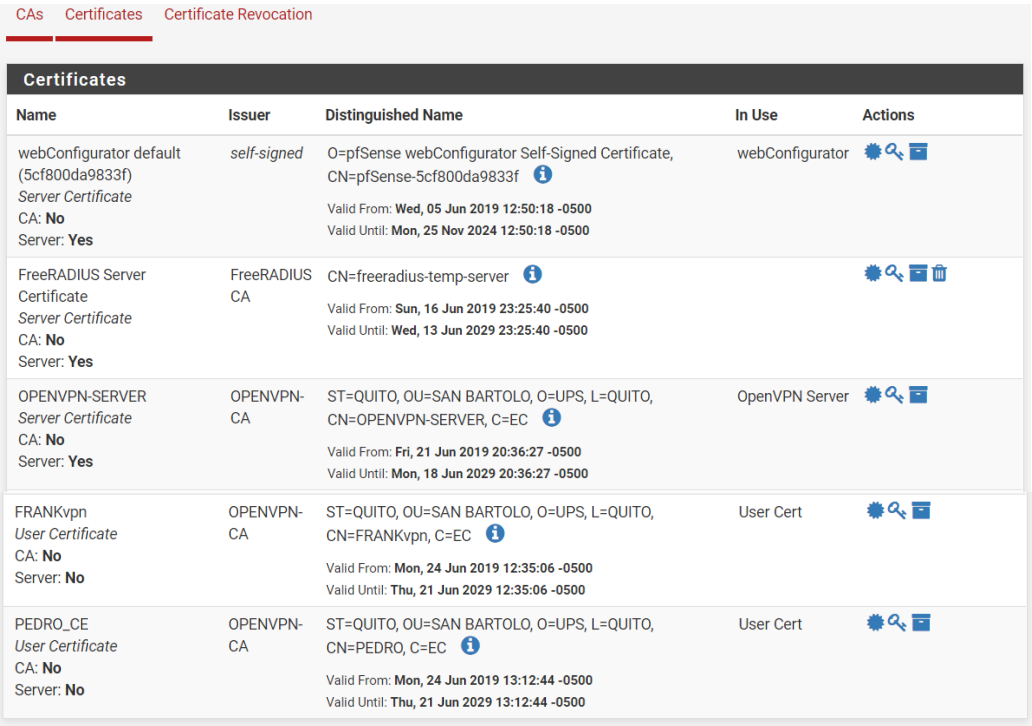




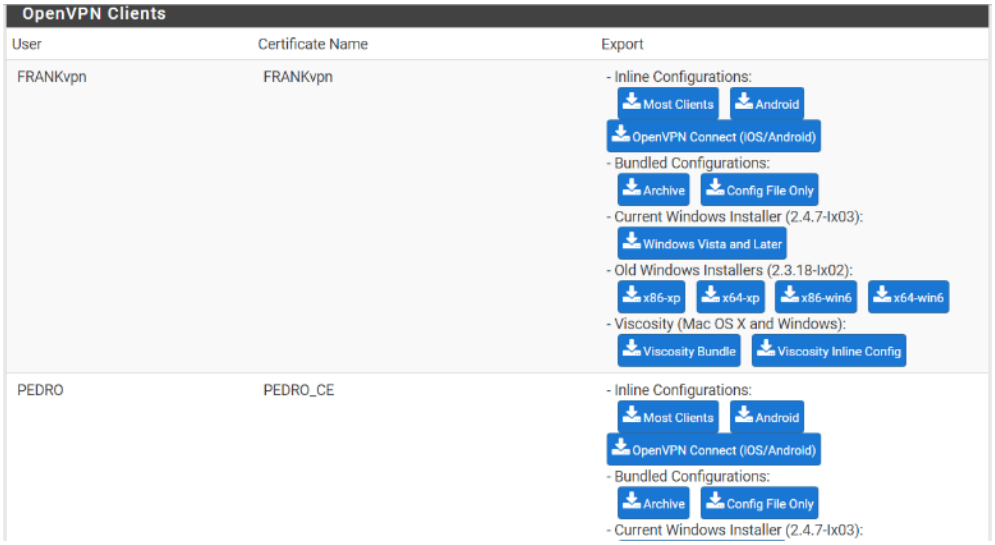
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



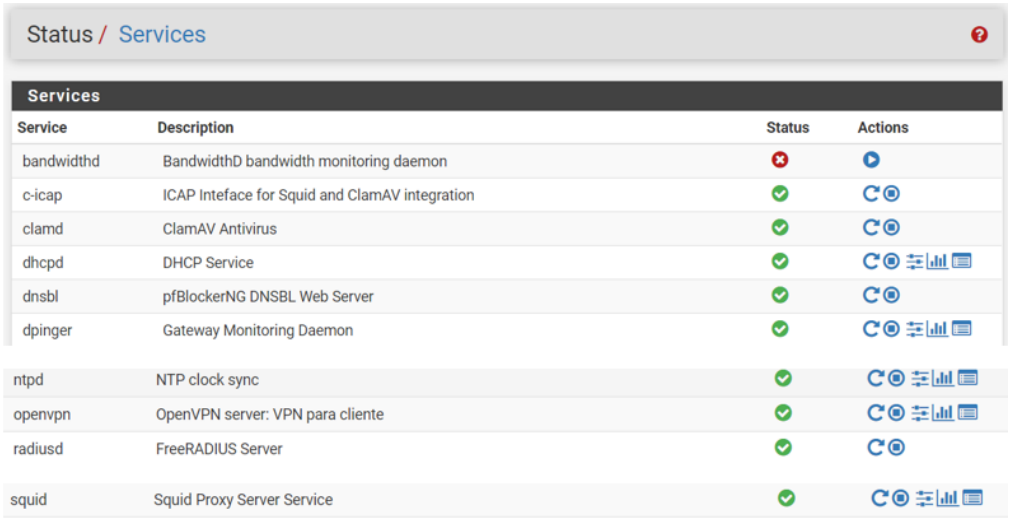
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Anexo 5. Características para la selección del Router de Servicios Integrados (ISR)

Marca / Parámetros	Cisco 4000 Series ISR		Juniper Network		Huawei Serie 2200	
	CISCO 4221	Cisco 4321	Juniper J4350	Juniper J6350	Huawei AR2220E	Huawei AR2240
Precio	$1571.43	$2242.00	$1134.00	$1326.00	$1339.00	$1570.00
Puertos	4 x 10/100/1000 para WAN o LAN	6 x 10/100/1000 para WAN o LAN	4 x 10/100/1000 Ethernet, Soporta E1/T1, Serial, ISDN BRI, ADSL, SHDSL, DS3, E3, 4 x GE LAN.	4 x 10/100/1000 Ethernet, Soporta E1/T1, Serial, ISDN BRI, ADSL, SHDSL, DS3, E3, 4 x GE LAN.	3 x Gigabit Ethernet (1 x Combo)	SRU40: 3 x GE (2 x Combo) SRU80: 3 x GE (2 x Combo) SRU100E: 4 x GE Combo+ 2 x GE SFP SRU200: 4 x GE Combo+ 2 x 10GE SFP+
Protocolos de Enrutamiento	RIP v1/v2, EIGRP, OSPF, BGP, PBR, PfR. PIM-SM, mroute (static route), and MLD. EIGRP, RIP, OSPFv3, IS-IS, BGP, PBR	RIP v1/v2, EIGRP, OSPF, BGP, PBR, PfR. PIM-SM, mroute (static route), and MLD. EIGRP, RIP, OSPFv3, IS-IS, BGP, PBR	OSPF, BGP, RIPv2, Static routes, IS-IS Multicast, MPLS, IPv6 MLD, DHCP	OSPF, BGP, RIPv2, Static routes, IS-IS Multicast, MPLS, IPv6 MLD, DHCP	Routing policy, static route, RIP, OSPF, IS-IS, BGP, IPv6 unicast routing Routing policy, static route, RIPng, OSPFv3, IS-ISv6, BGP4+	Routing policy, static route, RIP, OSPF, IS-IS, BGP, IPv6 unicast routing Routing policy, static route, RIPng, OSPFv3, IS-ISv6, BGP4+
Factor Forma	1 U de Rack	1 U Rack	2 U de Rack	2 U Rack	1 U Rack	2 U Rack
Encapsulación	GRE, Ethernet, 802.1q VLAN, PPP, Multilink Point-to-Point MLPPP, Frame Relay, MLFR, HDLC, Serial, EIA-530, PPPoE	GRE, Ethernet, 802.1q VLAN, PPP, Multilink Point-to-Point MLPPP, Frame Relay, MLFR, HDLC, Serial, EIA-530, PPPoE	Ethernet, PPP (Synch), Frame Relay, HDLC, Serial, 802.1q support, MLPPP, MLFR, PPPoE, DLSw	Ethernet, PPP (Synch), Frame Relay, HDLC, Serial, 802.1q support, MLPPP, MLFR, PPPoE, DLSw	GRE, Ethernet, 802.1q VLAN, PPP, Multilink Point-to-Point MLPPP, Frame Relay, MLFR, HDLC, Serial, EIA-530, PPPoE	GRE, Ethernet, 802.1q VLAN, PPP, Multilink Point-to-Point MLPPP, Frame Relay, MLFR, HDLC, Serial, EIA-530, PPPoE
Rendimiento	35 Mbps	50 Mbps	1 Gbps	2 Gbps+	1.2 Gbps	5.5 Gbps
Memora Flash	8 GB	4 GB/8 GB	256 MB	256 MB	512 MB / 4 GB	2 GB / 4 GB
Consumo de energía	150 Watts	330 Watts	143 Watts	166 Watts	150 Watts	350 Watts
Seguridad	FlexVPN, Easy VPN remote server, Enhanced Easy VPN, VPN (DMVPN), VPN (GET VPN), V3PN, MPLS VPN	FlexVPN, Easy VPN remote server, Enhanced Easy VPN, VPN (DMVPN), VPN (GET VPN), V3PN, MPLS VPN	IPSec, AES, DES, 3DES, HMAC-MD5, SHA-1, Prevenir ataques de repetición, filtros de firewall de estado	IPSec, AES, DES, 3DES, HMAC-MD5, SHA-1, Prevenir ataques de repetición, filtros de firewall de estado	ACL, Firewall, AAA, RADIUS, HWTACACS, ARP, ICMP, URPF, CPCAR, Black List	ACL, Firewall, AAA, RADIUS, HWTACACS, ARP, ICMP, URPF, CPCAR, Black List
Fuente Redundante	No	No	No	Si	Si	Si

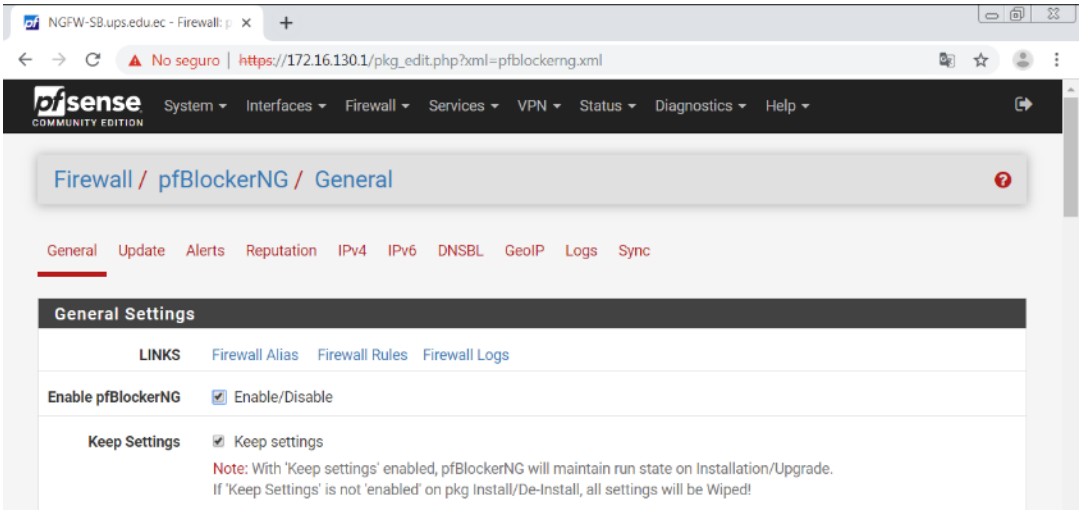
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Anexo 6. Características para la selección del Router de Alta Disponibilidad

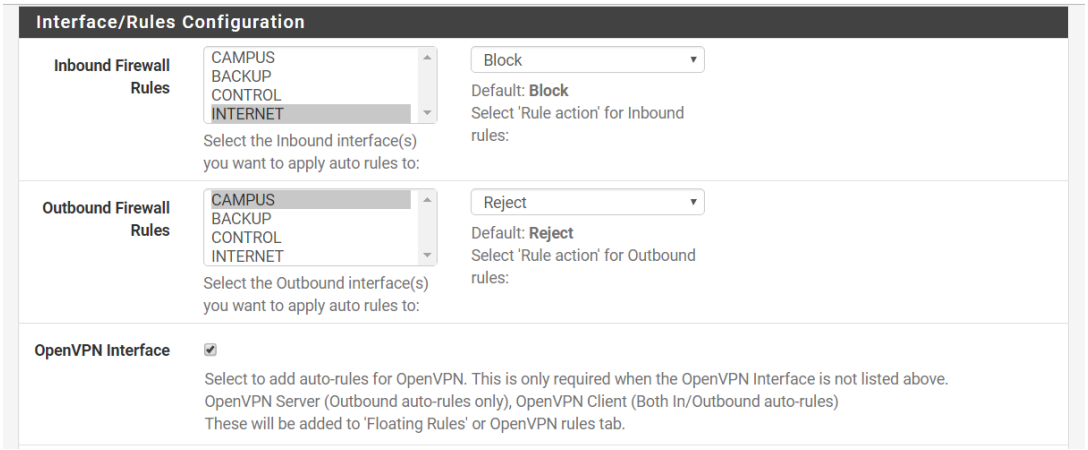
Marca / Precio	**Cisco 921-4P**	**Juniper SRX-320**	**Huawei AR 201**
Precio	$845.00	$1095.00	$520.00
Puertos	2 x GE WAN 4 x GE LAN	8 x 1 GE	8 x FE LAN 1 x FE WAN
Protocolos de Enrutamiento	RIPv1/v2, GRE, MGRE, CEF, Standard 802.1d, L2TP/v3, NAT, DHCP, OSPF, BGP, PfR, EIGRP, VRF, NHRP, BFD, WCCP	Static routes, RIP v1/v2, OSPF/OSPFv3, BGP, IS-IS, Multicast, Virtual Routes,	Routing policy, static route, RIP, BGP RIPng, BGP4+
Factor Forma	Desktop	Desktop	Desktop
Encapsulación	802.1P, 802.1Q, 802.3, VLAN management, MSTP, MAC address management.	VLAN, PPP, HDLC, MLPPP, MLFR, PPPoE	802.1P, 802.1Q, 802.3, VLAN management, MAC address management, MSTP
Rendimiento	150 Mbps	200 Mbps	450 Kpps
Memora Flash	2 GB	8 Gb	512 Mb
Consumo de energía	30 Watts	27 Watts	36 Watts
Seguridad	SSL, DES, 3DES, AES 128, PKI, IPSec, VRF-aware firewall, SIP, DMVPN,	Application visibility and control, Application-based firewall, Application QoS, Application-based, advanced policy-based routing	GRE VPN IPSEC VPN DSVPN L2TP VPN
QoS	LLQ, WFQ, CBWFQ, CBTS, CBTP, PRB, MIB, CoS DSCP, HQoS, cRTP, LFI, CBWRED, NBAR	DSCP, EXP, DLCI, WRED, Guaranteed and maximum bandwidth, Ingress traffic policing, Virtual channels, Hierarchical shaping and policing	DiffServ mode, CAR, traffic shaping, congestion avoidance, SP/WRR/SP+WRR; PQ/CBWFQ, MQC, Hierarchical QoS, SAC

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

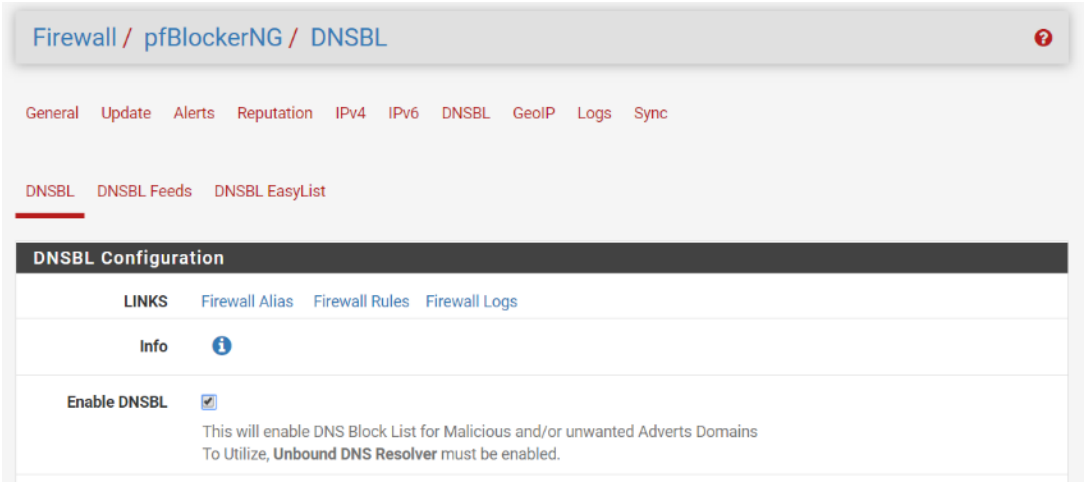
Anexo 7. Configuración de pfBlockerNG



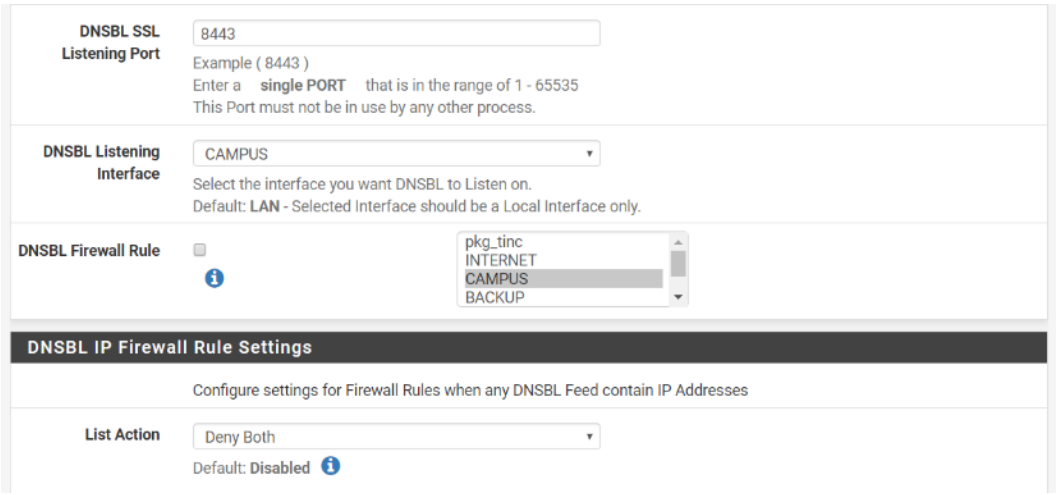
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



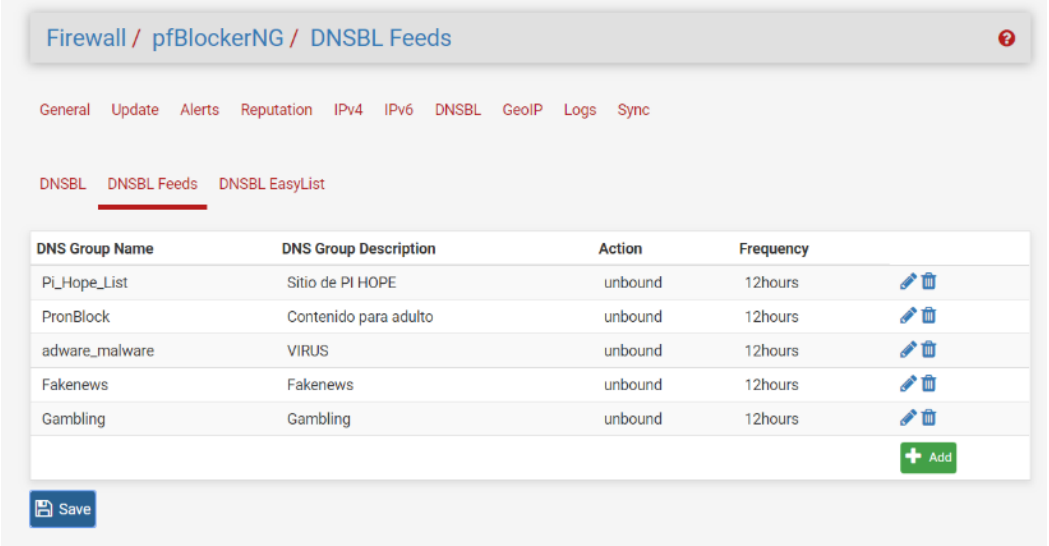
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



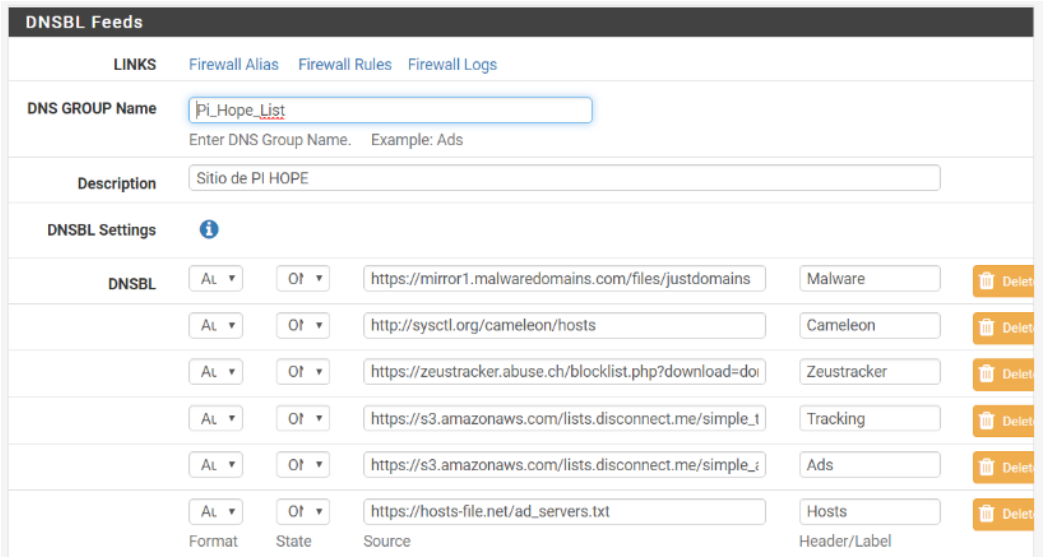
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



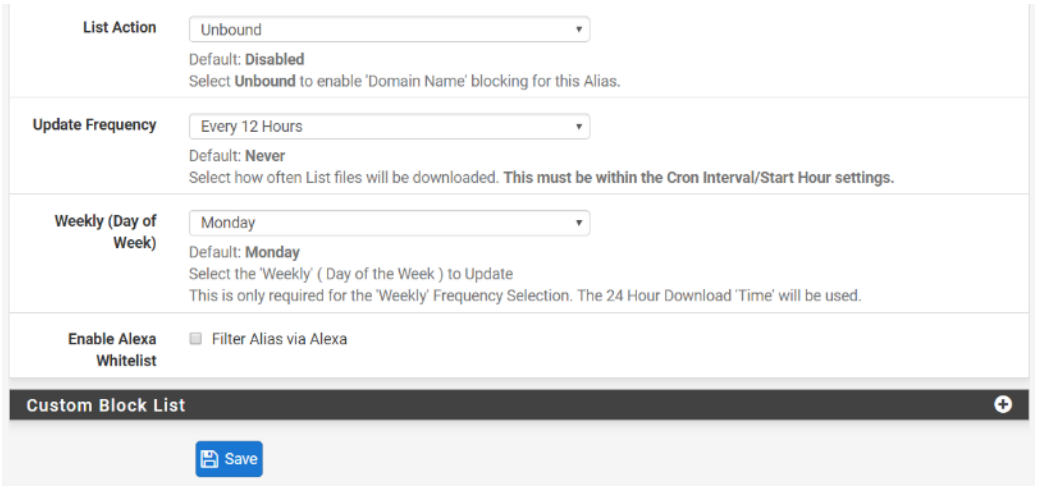
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



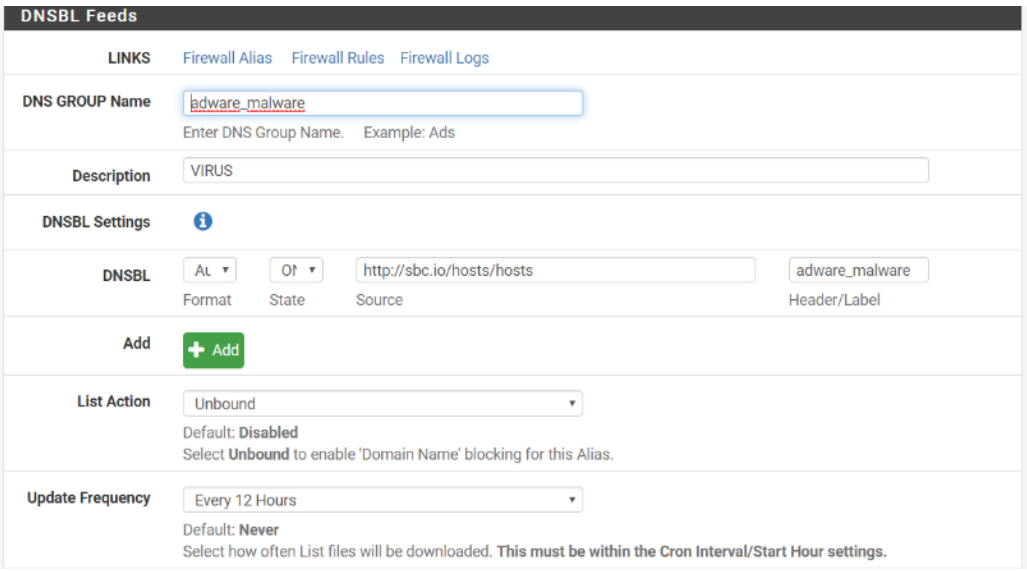
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

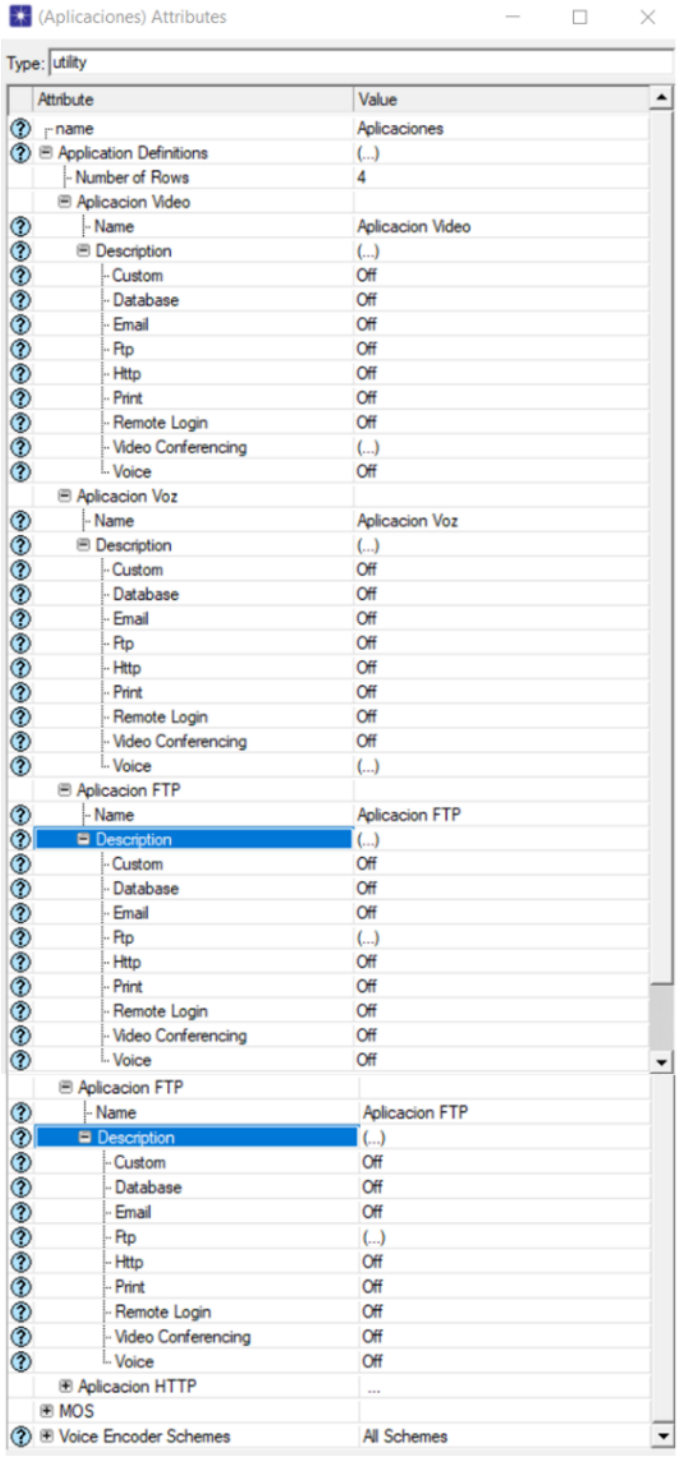


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

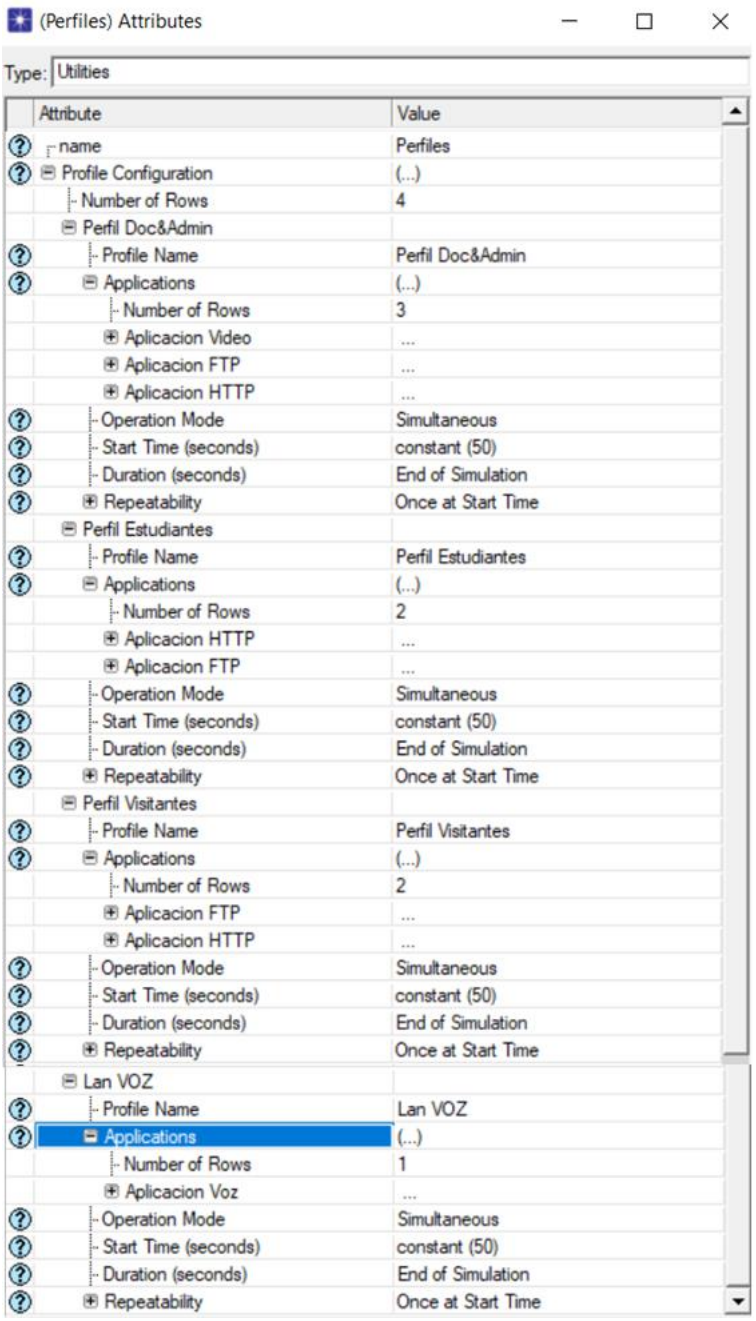


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

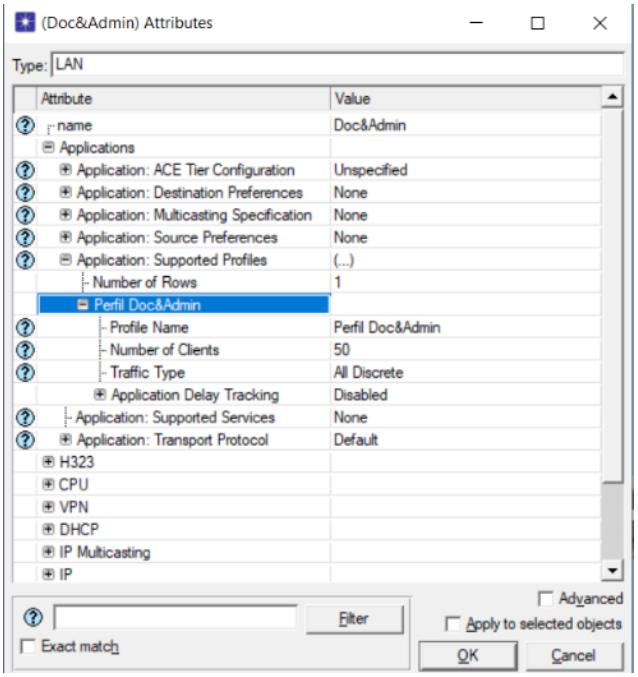
Anexo 8. Configuración de Aplicaciones en OPNET Modeler



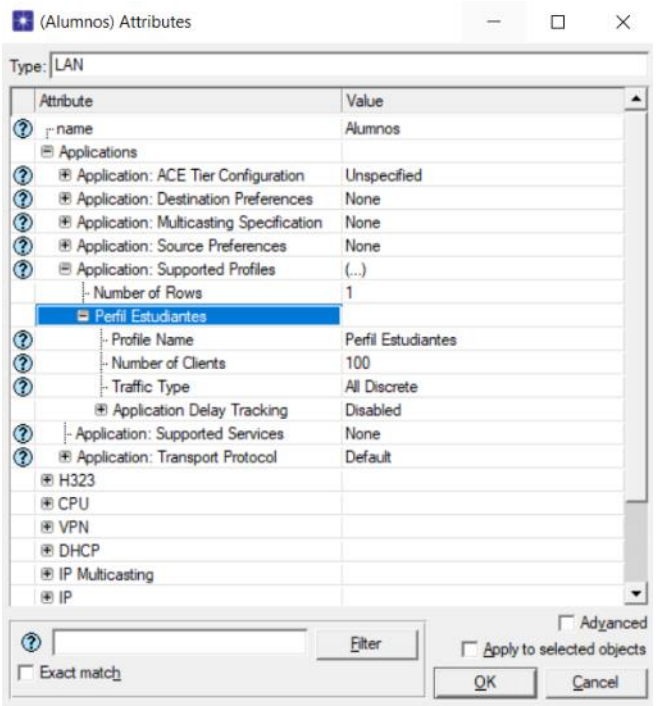
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



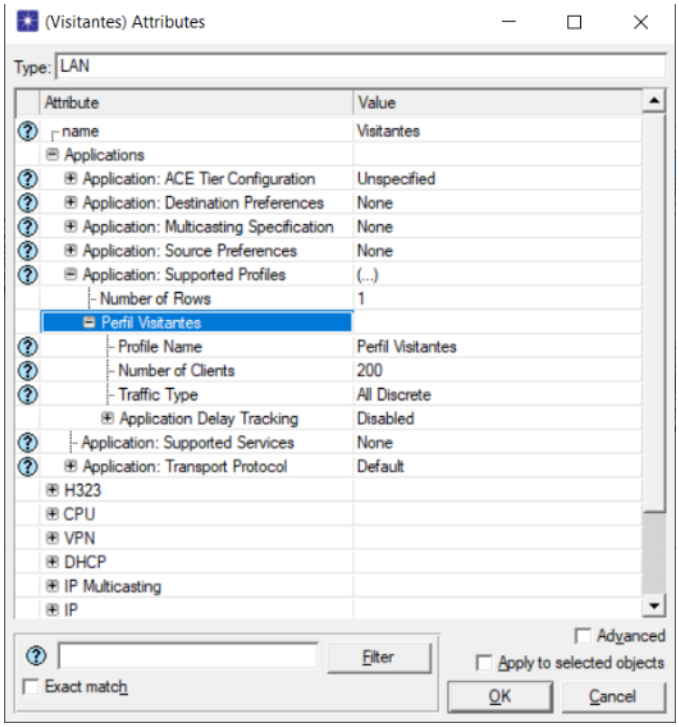
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



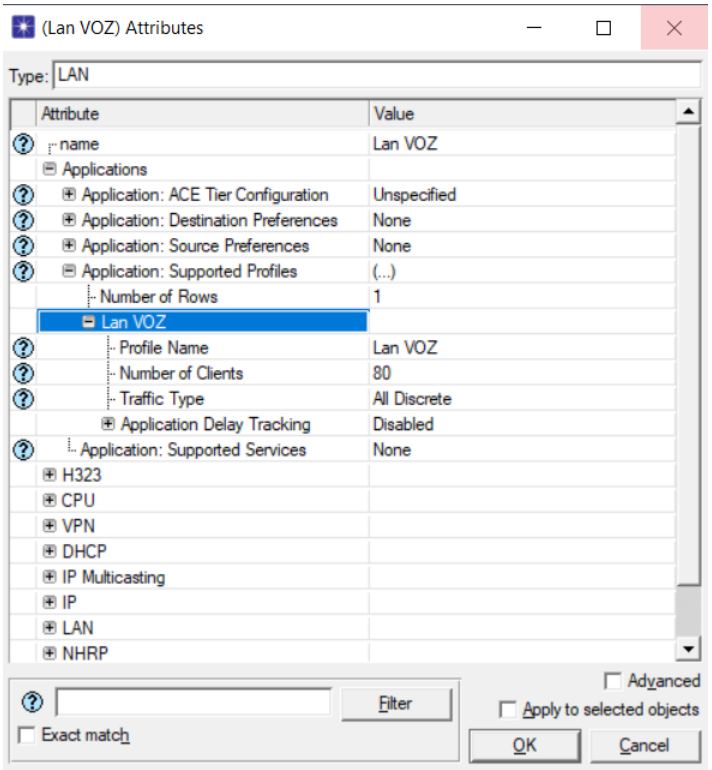
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



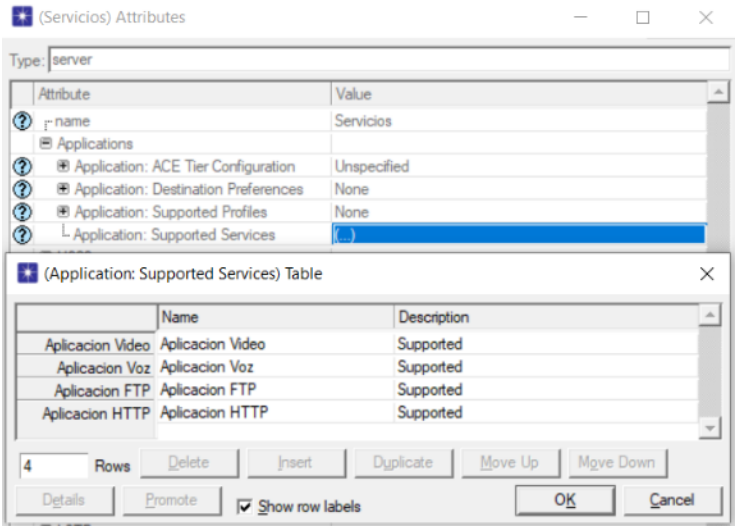
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



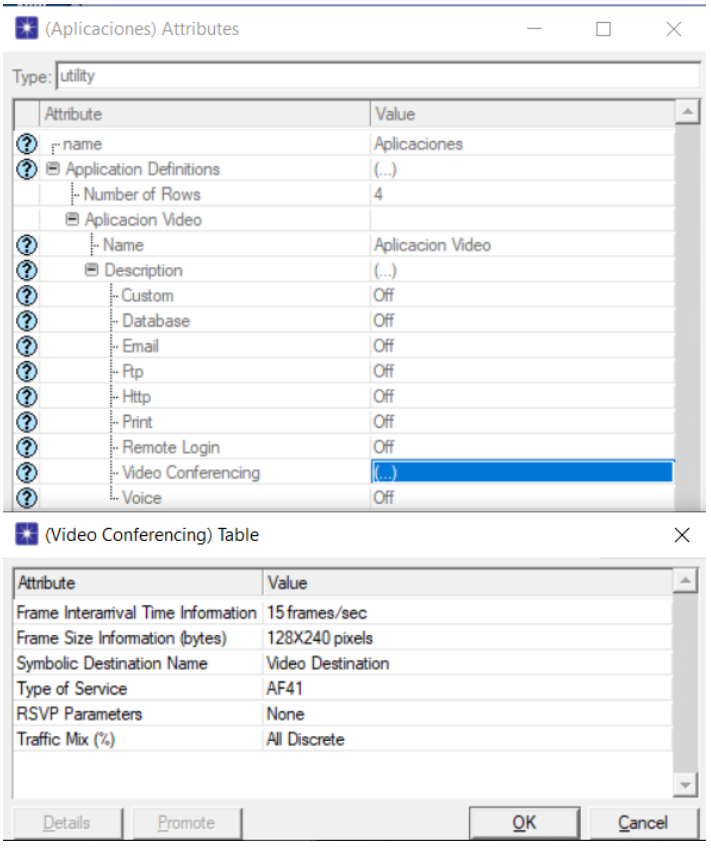
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



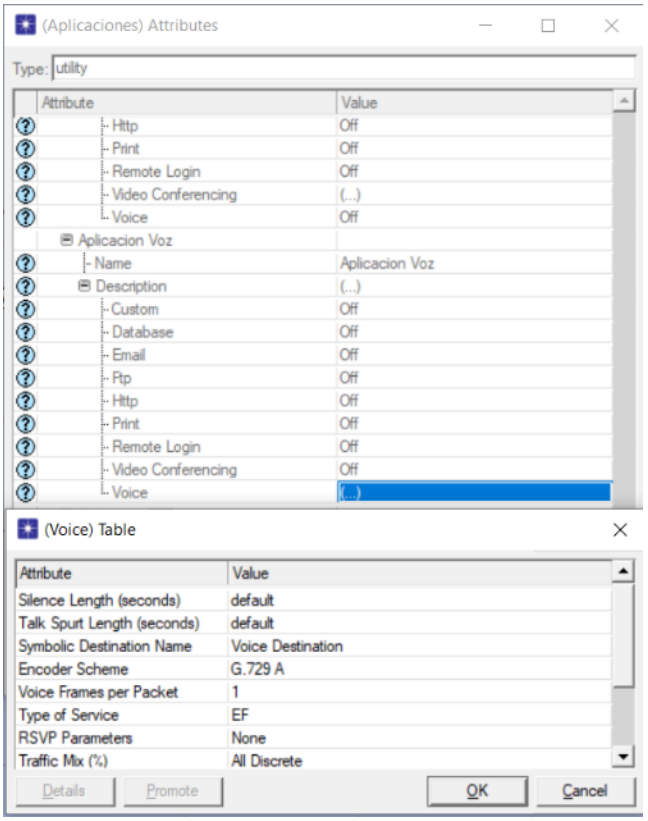
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



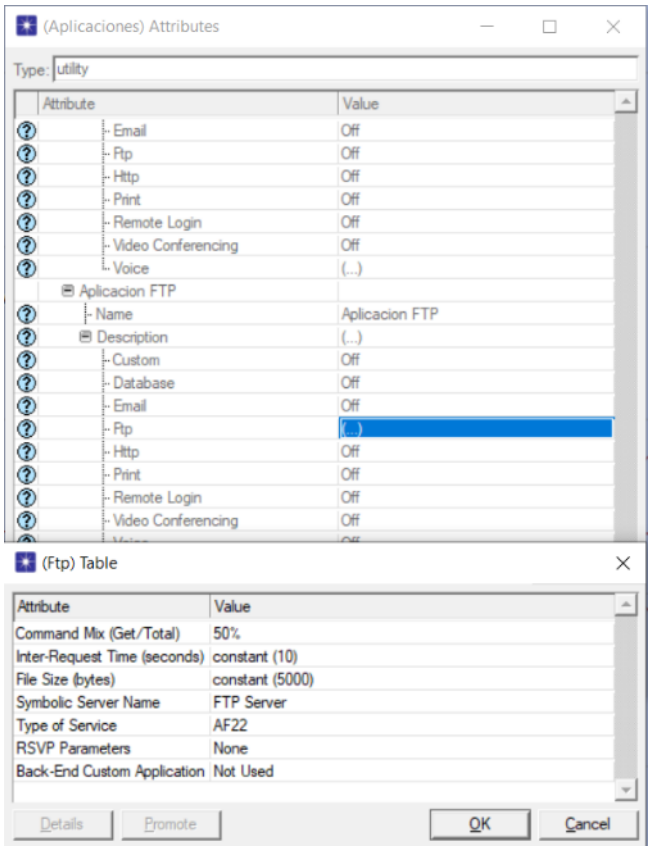
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.



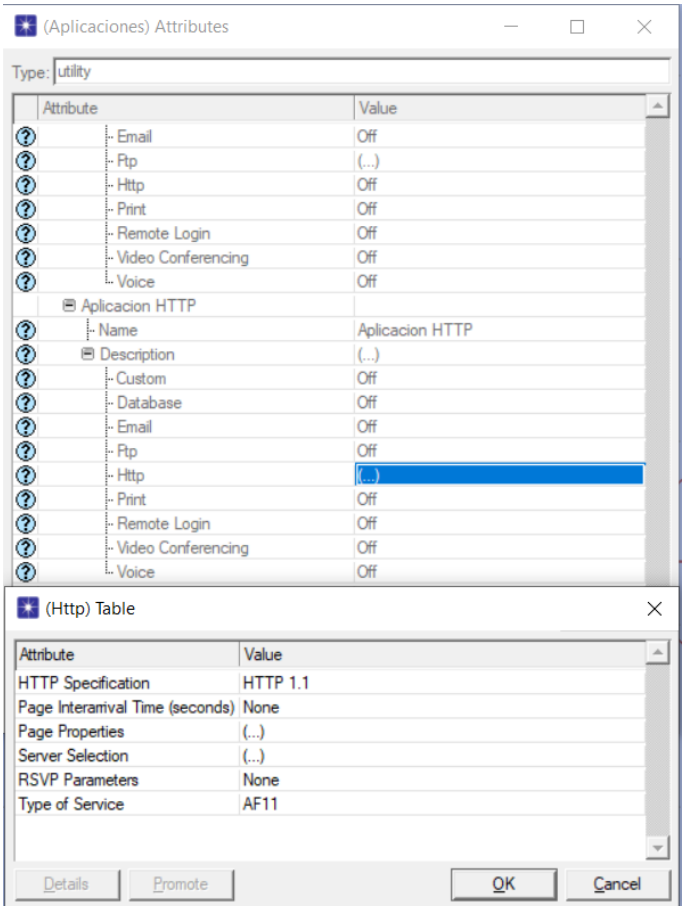
Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

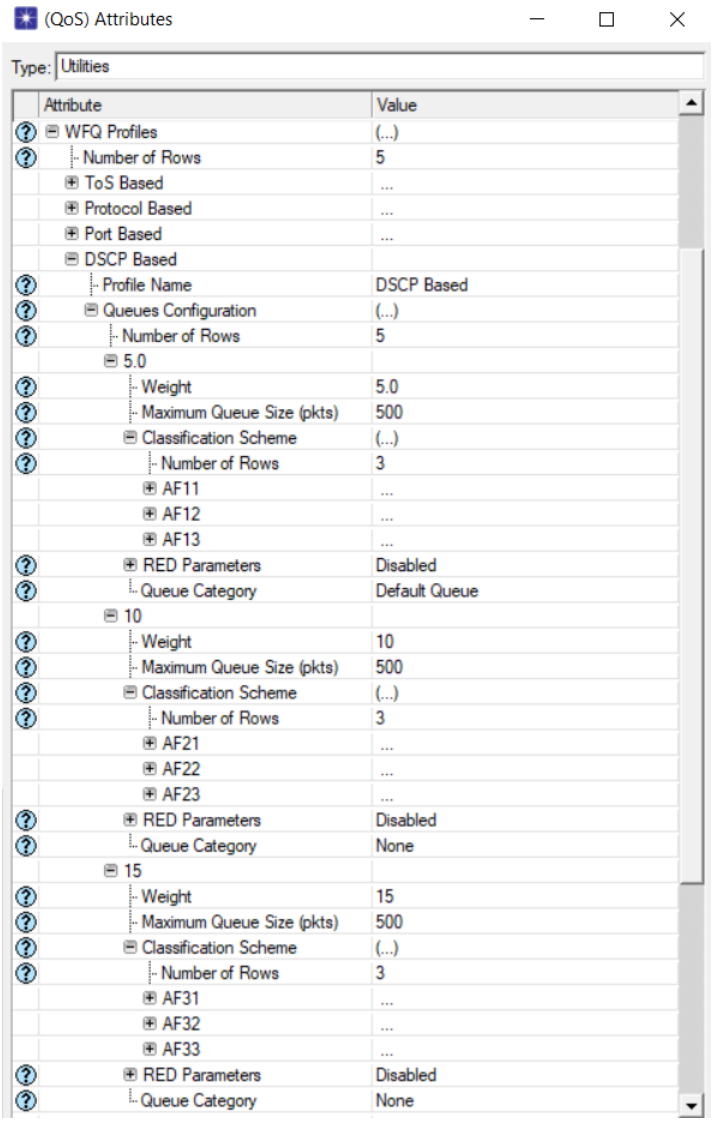


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

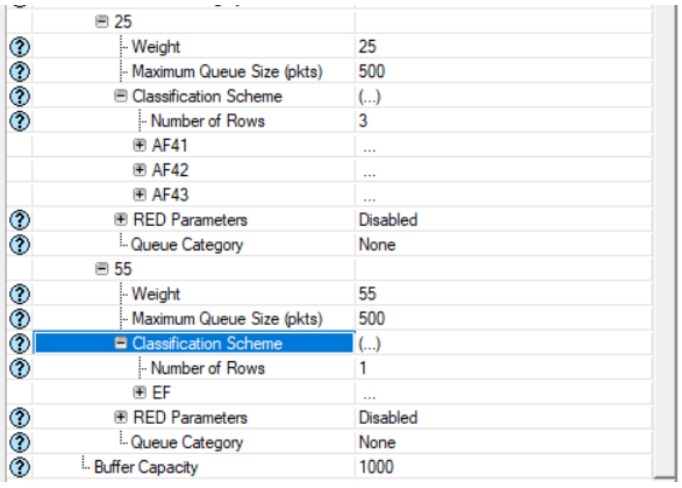


Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Anexo 9. Configuración de Calidad de Servicio en OPNET Modeler



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan



Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan

Anexo 10. Cotización de equipos para la red de frontera y tabla de costos totales

DEPARTAMENTO DE SEGURIDAD

INTCOMEX DEL ECUADOR

INTCOMEX ECUADOR

INTCOMEX del Ecuador S.A.

Yánez Pinzón 295 y la Niña
Quito, EC14
TEL: +593 3973000

COTIZACION
INTCOT- 9014
Fecha: 12/06/2019
Vencimiento: 27/06/2019

EMPRESA: FERNANDO CAHUEÑAS — EMAIL:

Cliente: 10000001, FENANDO CAHUEÑAS , N/A
Dirección: UPS, QUITO
Operador: JR
Solución:

Vendedor: JR
Término: Cont.Efectivo
Localidad: QUITO
Transportista: LOCAL

CANTIDAD	PRODUCTO	CODIGO	DESCRIPCION	COSTO	TOTAL
1	CISCO UCS C220 M5	CISCO UCS C220 M5	CISCO UCS C220 M5	$ 6,141.43	$ 6,141.43
1	CISCO 4221 ISR	CISCO 4221 ISR	CISCO 4221 ISR	$ 1,571.43	$ 1,571.43

Memo:
Emitir pago a Nombre de FIDEICOMISO FLUJOS INTCOMEX, Transferencias a cuenta corriente de BANCO DE PICHINCHA # 2100055794. Precios, Términos y Condiciones están sujetos a cambios sin previo aviso. http://store.intcomex.com/es-XEC/HOME

Condiciones:

SUBTOTAL	$ 7,712.86
IVA (12%)	$ 925.54
TOTAL	$ 8,638.40

Pagina: 1 de 1

xecrnico

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

ALTALA®
THE NETWORK COMPANY

Quito, martes, 11 de junio de 2019

ALTALA S.A.

Shyris N39-281 y Gaspar de Villarrorel Centro Comercial La Galería Of. 28

Cliente: UNIVERSIDAD POLITECNICA SALESIANA
Dirección:
Teléfono:
Contacto:

Cotización Número: 2335

Forma de Pago:
Aceptamos Todas las Tarjetas de Crédito
Todos Nuestros Productos Cuentan con 1 año de Garantía contra defectos de fábrica

Cod.	Unidades	Artículo	Precio Unitario	Precio Total
	1	Router ISR Huawei AR2220E	1400,55	1400,55
	7	Patch cord 3 ft Certificado	12,25	86,75
	3	Patch cord 7 ft Certificado	14,25	42,75
	1	Forsa UPS 6KVA	3.199,33	3.199,33
	1	CDP UPS 6KVA	2,400	2,400

Base IVA:	% IVA	IVA:	Total:	5.299,59
4731,78	12	567,81		

Ing. Andrés Amores
Bissines Development
Telf: (02)2 442082 Ext. 1014
Cel: 0983871019
Email: telecom4@altala.net

*precios y stock pueden variar sin previo aviso

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

07/06/2019
19:26

Kamay Solutions S.A

PROFORMA NUMERO 2019-0402-1615

Anteponiendo nuestro más cordial saludo a continuación nos es grato cotizar a usted (s), el servicio de creación de CRM desde cero (0).

Cliente:	Universidad Politécnica Salesiana
Tiempo de Entrega:	1 semana
Forma de Pago:	60 % antes de la entrega y 40% al finalizar

SE ADJUNTARÁ LA DESCRIPCION CORTA DEL LA PROFORMA DE LOS PRODUCTOS O SERVICIOS A COMERCIALIZAR.

CANTIDAD	DESCRIPCCIÓN	VALOR UNIT	VALOR TOTAL
1	HPE ProLiant DL360 Gen10 Performance - Servidor - se puede montar en bastidor	4.415,94 USD	4.415,94 USD
1	HPE Midline - Disco duro – 60 GB	180,84 USD	180,84 USD
1	HPE SmartMemory - DDR4 - 16 GB	577,60 USD	577,60 USD
1	HPE Midline - Disco duro – 120 GB	246,33 USD	246,33 USD
1	HPE SmartMemory - DDR4 - 32 GB	853,34 USD	853,34 USD
1	CISCO C921-4P	845,00 USD	845,00 USD
1	Router ISR Huawei AR2220E	1445,00 USD	1445,00 USD
7	Patch cord 3 ft	11,25 USD	78,75 USD
3	Patch cord 7 ft	18,66 USD	55,98 USD
1	UPS CDP on-line 6kva 5400 kw bifásico bypass 220/110V	2.899,99 USD	2.899,99 USD
		SUB TOTAL	8.368,78 USD
		IVA 12%	1.043,86 USD
		TOTAL	9.742,03 USD

ATENTAMENTE

Damián Hurtado
GERENTE
Kamay Solutions S. A

José Joaquin del Olmedo N2-52 y Simón Bolivar, Conocoto
info@kamaysolutions.com.ec
www.kamaysolutions.com.ec
02 - 207 3824

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.

Anexo 11. Período de recuperación de la Inversión

Egresos	Valor Mensual (USD)	Valor Trimestral (USD)
Ahorro	1352,44	4057,32
Gastos de Operación	356,21	1068,63
Depreciación	120,66	361,98

Elaborado por: Cahueñas Juan y Lizarzaburu Jonathan.