UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"DESARROLLO DE UN DISEÑO DE RED DE ÁREA EXTENSA BASADA EN UNA ARQUITECTURA DEFINIDA POR SOFTWARE SD-WAN ADAPTADA A UN MODELO MPLS E IMPLEMENTACIÓN DE POLÍTICAS DE CALIDAD DE SERVICIO QOS PARA EL ANÁLISIS DEL RENDIMIENTO DE UNA RED HÍBRIDA".

AUTOR: ISAURA MELANY JINGO CEVALLOS

DIRECTOR: MSC. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA- ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003841770		
APELLIDOS Y NOMBRES:	Jingo Cevallos Isaura Melany		
DIRECCIÓN:	Ibarra, Canoningo Flores y Armando Hidrovo		
EMAIL:	imjingoc@utn.edu.ec		
TELÉFONO FIJO:	062512064	**TELÉFONO MÓVIL:**	0987884963

DATOS DE LA OBRA	
TÍTULO:	"Desarrollo de un diseño de red de área extensa basada en una arquitectura definida por software SD-WAN adaptada a un modelo MPLS e implementación de políticas de calidad de servicio QoS para el análisis del rendimiento de una red híbrida".
AUTOR (ES):	Jingo Cevallos Isaura Melany
FECHA DE APROBACIÓN: DD/MM/AAAA	9 de febrero de 2023
PROGRAMA:	■ **PREGRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Fabiánn Geovanny Cuzme Rodríguez Ing. Carlos Alberto Vásquez

CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 15 días del mes de febrero de 2024

EL AUTOR:

.....

Isaura Melany Jingo Cevallos

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGÍSTER CARLOS VASQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que el presente trabajo de titulación: "DESARROLLO DE UN DISEÑO DE RED DE ÁREA EXTENSA BASADA EN UNA ARQUITECTURA DEFINIDA POR SOFTWARE SD-WAN ADAPTADA A UN MODELO MPLS E IMPLEMENTACIÓN DE POLÍTICAS DE CALIDAD DE SERVICIO QOS PARA EL ANÁLISIS DEL RENDIMIENTO DE UNA RED HÍBRIDA". Ha sido desarrollado por la señorita Jingo Cevallos Isaura Melany bajo mi supervisión. Es todo cuanto puedo certificar en honor a la verdad.

.....

MSc. Carlos Alberto Vásquez Ayala

DIRECTOR

DEDICATORIA

Este trabajo está dedicado a mi familia, que siempre están conmigo apoyándome incondicionalmente día a día brindándome su amor y comprensión.

A mi padre Marcelo que siempre ha sido mi ejemplo a seguir mi inspiración, a mi madre Marisol que realmente ha sido mi admiración de su forma de enfrentarse al mundo, a mi hermano menor Rodrigo que es mi motor a continuar el ha aprendido de mi y yo de el un hombre de voluntad, a Bryan mi pareja que se ha convertido en mi apoyo para culminar esta etapa importante.

AGRADECIMIENTO

Agradezco a Dios por permitirme ser fuerte a pesar de los tropiezos que tuve, a mi familia por apoyarme y comprenderme.

Agradezco mucho a mi pareja Bryan por la paciencia y el amor que me ha brindado a lo largo de esta etapa con sus consejos.

Agradezco el haber conocido personas que me caminaron conmigo esta etapa, con los que forje una gran amistad los cuales son excelentes personas y sé que también excelentes profesionales, a mis amigos y compañeros Karly, Blanquita, Ángel.

Agradezco de igual forma agradezco a la a la universidad por haberme abierto las puertas y formarme para la vida profesional y haberme permitido conocer personas que me ayudaron a conocer nuevos conocimientos y experiencias, a mis profesores de carrera cada uno me enseño algo importante y de manera especial a mi tutor el Msc Carlos Vásquez que supo guiarme ante este camino para culminar esta etapa siempre estaré agradecida con sus consejos.

ÍNDICE

CAPÍTULO I: ANTECEDENTES

1.1. Problema

Con el avance de la tecnología las redes de comunicación tradicionales van perdiendo territorio frente a nueva tecnología, mientras que en una red tradicional WAN se compone por routers los cuales son administrados localmente o de forma manual remota, también el alto costo y requerimiento del ancho de banda obliga a los encargados de la red a buscar soluciones alternativas para un mejor desempeño y ahorro de costos. Se tiene también la infraestructura más utilizada MPLS en donde garantiza el rendimiento de cierto tipo de tráfico en donde se asigna una determinada cantidad de ancho de banda dentro del circuito MPLS y no de todos los tipos de tráfico. El empezar la introducción de la tecnología SD-WAN permitirá simplificar la administración y operación de una WAN al separar dos planos el plano de control el plano de datos, también se da prioridad a aplicaciones específicas, pero estás van a tener el acceso a el ancho de banda completo.

Debido a la situación que atravesó el país debido al COVID-19 Se suspendieron las actividades presenciales de varias instituciones, trasladando así de manera abrupta el estudio y el trabajo a casa, lo que llevó a un incremento del tráfico de internet en los hogares el cual a mediados del año 2020 creció hasta un 63% de acuerdo con “El Universo” (El Universo, 2020). Ecuador experimenta un crecimiento en el acceso a internet y a redes sociales con 10.17 millones de usuarios de internet y 14 millones de perfiles en redes sociales, es decir, que el 57% de la población usa este servicio en relación con enero del 2020 hubo un crecimiento del 1.5%, lo que es igual a 147 mil nuevos usuarios y esto implica que se ha tenido mayores repercusiones, la población urbana es del 64,3% de 17.77 millones de habitantes y marca una diferencia

significativa respecto a otros países latinoamericanos y dice mucho acerca el acceso de la población a internet ya que del 35,7% de la población rural solo el 16% cuenta con acceso a internet de acuerdo con “Branch” (Alvino. C, 2021).

El aumento del tráfico de datos se ha visto reflejado en la alta demanda como lo son las clases virtuales y el teletrabajo por estos motivos la red se vuelve más pesada y requiere de más recursos lo que se refiere a una mejor calidad de servicio (QoS) para soportar el tráfico en mayor parte multimedia, en donde al poseer un modelo de red que no cubre totalmente las necesidades actuales, llega a provocar caídas abruptas de la red.

Para mejorar y disminuir la latencia se propone una metodología de red como SD-WAN para el diseño de una red que se combine al modelo actual y se enfoque en la gestión centralizada, el reenvío de datos a través de dispositivos conmutadores que soportan redes definidas por software para dirigir el tráfico de una manera inteligente y garantizar un QoS óptimo.

1.2. Objetivos

1.2.1. Objetivo General

Desarrollar un diseño de red de área extensa basada en una arquitectura definida por software SD-WAN adaptada a un modelo MPLS e implementación de políticas de la calidad de servicio QoS para analizar el rendimiento dentro de una red híbrida

1.2.2. Objetivos Específicas

- Definir los fundamentos teóricos necesarios acerca de la arquitectura, elementos y funcionamiento de una red extensa definida por software, así como también de la infraestructura MPLS enfocadas principalmente en la calidad de servicio (QoS).

- Determinar que dispositivo de red a utilizar con la tecnología Fortinet para una infraestructura de SD-WAN que tenga requisitos cambiantes para la conexión de usuarios finales con los servicios correspondientes para una red híbrida.
- Definir los diferentes mecanismos de calidad de servicio QoS para el establecimiento de las políticas adecuadas y mejora del rendimiento óptimo de una red combinada SD-WAN con MPLS.
- Elaborar un diseño de red híbrido con el objetivo de evidenciar las ventajas que ofrece aplicar políticas de QoS en la red.
- Realizar pruebas de rendimiento mediante una simulación en donde se analice diferentes escenarios en donde se destaque las ventajas del uso de políticas QoS.

1.3. Alcance

El presente proyecto tiene como objetivo la elaboración de un diseño de red extensa basada en una arquitectura definida por software SD-WAN en donde es necesario analizar el modelo MPLS para implementar las respectivas políticas de servicio QoS a través de simulaciones de alta disponibilidad para comprobar su funcionamiento, en donde se busca mejorar el rendimiento general de una red híbrida.

En primer lugar, se realizará la investigación acerca de los fundamentos teóricos necesarios acerca de la arquitectura y el funcionamiento de una red extensa definida por software, así como también el análisis de la infraestructura de MPLS junto con el respectivo equipamiento que deben ser tomados en cuenta para el control de tráfico de la red a través de la redirección inteligente sobre dos o más enlaces junto a la gestión basada en la nube. Además de analizar tanto los mecanismos como los modelos de QoS con lo cual se dará una solución que se adecuen al proyecto propuesto.

La implementación de una red hibrida SD-WAN y MPLS requerirá un análisis y comparación de las principales características de estos dos modelos de red a implementar, en donde se justificará la elección de este modelo en base a sus ventajas, además de su adaptabilidad con el modelo MPLS. Se permitirá establecer configuraciones WAN a lo largo de varias localidades y circuitos virtuales, así como también capturar datos sobre el rendimiento y errores de funcionamiento de la red. También el supervisar de forma dinámica el rendimiento de rutas y realizar el ajuste de flujos de tráfico los cuales existen entre los circuitos físicos disponibles para equilibrar la carga y reducir la congestión dando soporte mediante los canales vinculados y realizar reenvíos virtuales. Con las características mencionadas se analizará la arquitectura y se escogerá previamente los dispositivos SD-WAN de la tecnología Fortinet (FortiGate, FortiManager, FortiAnalizer)para los nodos correspondientes los cuales se realiza una simulación para comprobar el soporte del dispositivo mediante una simulación en el software GNS3 y posteriormente agregarlo a la topología correspondiente en donde se encargarán de implementar la función de plano de datos, administración y configuración de equipos de manera centralizada ya que el plano de control se encuentra separado del de datos en donde permitirá una red escalable de tal forma que se puede definir nuevas políticas de calidad de servicio y se podrá realizar de manera remota sin que el administrador de red tenga que desplazarse al sitio. Por esta razón se implementará LANs en cada sucursal y usarán conexiones de banda ancha para tráfico de internet que requiera menos latencia en donde se tendrá como controlador FortiManager y junto a FortiAnalyzer obtener acceso remoto para poder visualizar el estado. Para utilizar los equipos necesarios para la simulación se realizarán mediante la obtención de las ISO a través de la cuenta oficial de Fortinet. Dentro de los requisitos para la infraestructura de SD-WAN cabe resaltar los servicios y requerimientos a formar parte de la

conexión de los usuarios finales los cuales son los servicios de VoIp, Streamming, Hosting antes de implementar las políticas QoS los cuales serán claves dentro del comportamiento del proyecto planteado.

Dentro de la tercera parte se establecerán las políticas adecuadas para mejorar el rendimiento de la red y para eso se debe tomar en cuenta que la calidad de servicio QoS planea manejar los efectos de la congestión del tráfico utilizando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente capacidad. En este punto es necesario prestar atención especial al hecho de que la QoS no es aumentar ancho de banda sino distribuirlo de acuerdo con las necesidades que se requieran. Se denota el funcionamiento básico de los mecanismos de QoS en donde se definirá entre: control de admisión, abolición de congestión, administración de congestión, clasificación de tráfico, shaping y policing, señalización, mecanismos de eficiencia de enlace y administración, monitoreo y aprovisionamiento. Esto permitirá observar el funcionamiento de una red que actualmente se utiliza en la gran mayoría de empresas como lo es MPLS y conozcan los resultados al combinar con una red SD-WAN como afecta el QoS.

Se propone elaborar un diseño de red conformada con una MPLS y una SD-WAN en donde se emplearán diferentes servicios como VoIp, Streamming, Hosting. Cabe mencionar que para el uso del acceso remoto se utilizará SSL-VPN, mediante los equipos Fortinet se tendrá un manejo centralizado por lo que se puede agregar o remover cualquier política, regla o configurar la seguridad de forma óptima sin la necesidad de trasladarse al lugar.

Finalmente, mediante el uso de un modelo de red SD-WAN funcionando se realizará una verificación de su funcionamiento, para que posteriormente el diseño permita el mejor desempeño de la red mediante las políticas a implementar de QoS dentro del diseño a realizar,

haciendo uso de los servicios de VoIp, Streamming, Hosting, se realizarán pruebas en 2 escenarios principalmente el primero que será sin utilizar políticas de QoS y el segundo escenario utilizando las políticas QoS, en donde se demostrará el enrutamiento del tráfico optimizado debido a los parámetros que se verificarán como lo son la latencia, jitter, pérdida de paquetes.

1.4. Justificación

En la actualidad debido al incremento de intercambio de datos a través de la red, la demanda tanto de los usuarios para recibir un mejor servicio o de las empresas que necesitan cubrir tales necesidades como son mayor ancho de banda, la calidad de servicio QoS entre otros, a pesar de esto MPLS lleva en el mercado por mayor tiempo lo que ha generado confianza en su efectividad, pero se ha visto en auge la tecnología SD-WAN en el sector de telecomunicaciones.

La red SD-WAN ha surgido en los últimos años con el fin de simplificar la gestión y creación de conexiones de diferentes sitios como sucursales de una empresa o centros de datos entre sí y proporcionar la flexibilidad, control y monitoreo centralizado a un costo menor, en comparación a un red WAN convencional tiene dos principales aspectos mejores como lo es que proporciona un marco inherente para las aplicaciones de hosting ya que se desarrolla de forma centralizada en donde se toma en cuenta la calidad percibida por el usuario y segundo es que puede definir de forma centralizada las políticas de red y gestión del tráfico sin utilizar configuración manual. (Zhenjie, Yong, Baochun, Yadong, & Xu1, 2019)

La infraestructura MPLS ha servido y ha satisfecho las necesidades de la empresa durante alrededor de 20 años no hay que olvidar que pese a su confianza dada por el tiempo de uso tiende a llegar a un punto de inflexión por ejemplo es costoso ya que es complejo de desplegar e inflexible evitando el adaptarse a los requisitos de la nube los cuales sus aplicaciones han estado

en crecimiento. El virus COVID-19 fue un gran detonante para desencadenar varias transiciones como migrar a la nube y estudiar, trabajar desde casa o desde otro lugar (DIARIOTI, 2021). Es por eso que el surgimiento de SD-WAN ofrece soluciones alternativas ya que aun con el uso de MPLS en varios sectores una parte importante es tomar en cuenta que MPLS es un transporte de red, mientras que SD-WAN permite una solución en donde se utiliza MPLS y otros transportes para construir una red extensa con mejor rendimiento y mayores capacidades. (SDX Central, 2018)

Es así como, el presente proyecto propone el desarrollo de un diseño de red de área extensa basada en una arquitectura definida por software SD-WAN adaptada a un modelo MPLS e implementación de políticas de calidad de servicio QoS para el análisis del rendimiento de una conformada por estos dos modelos, en donde la verificación de su funcionamiento se lo hará con diferentes pruebas de rendimiento y distintos escenarios en un entorno de simulación.

2. CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

En este capítulo 2, la atención se centra en establecer una base teórica que sustente el contexto y los objetivos del proyecto. Este capítulo profundiza en los conceptos fundamentales necesarios para comprender el alcance del proyecto, incluidas las redes de área extensa definidas por software (SD-WAN), la conmutación multiprotocolo de etiquetas (MPLS), la calidad de servicio (QoS) y las tecnologías de red relacionadas. Al explorar estos fundamentos teóricos, este capítulo pretende proporcionar a los lectores una comprensión general del marco conceptual en el que se basara la implementación y análisis posteriores.

2.1. Conmutación de etiquetas multiprotocolo (MPLS)

El protocolo MPLS provee una conmutación de etiquetas para soportar el tráfico de diferentes envíos de paquetes y así poder diferenciarlos, generalmente se añaden las etiquetas de acuerdo con las direcciones de destino de la capa de red del modelo OSI. MPLS proporciona fiabilidad, rendimiento y prioridad a paquetes que lo requieran (Imagar,2021).

2.1.1. Arquitectura MPLS

La arquitectura MPLS es eficiente, ya que esta mejora el rendimiento mediante el incremento de velocidad de los datos a través de la red por lo que se basa en etiquetas y no en la cabecera IP. Entonces el enrutador utiliza información la cual se asigna a una corrección de errores hacia a delante, (FEC) entonces antes de la transferencia de paquetes se establecen rutas y la asignación de etiquetas para la distribución de estas y la creación de tablas los cuales no afecta a los demás enrutadores internos de la red correspondiente por lo que continúa con la recepción del paquete y la implantación de la etiqueta lo cual esto permite la conmutación de las etiquetas y la correspondiente transferencia del paquete en donde será extraído su etiqueta y finalmente entregar el paquete (Pérez, 2020).

2.1.2. Elementos de una red MPLS

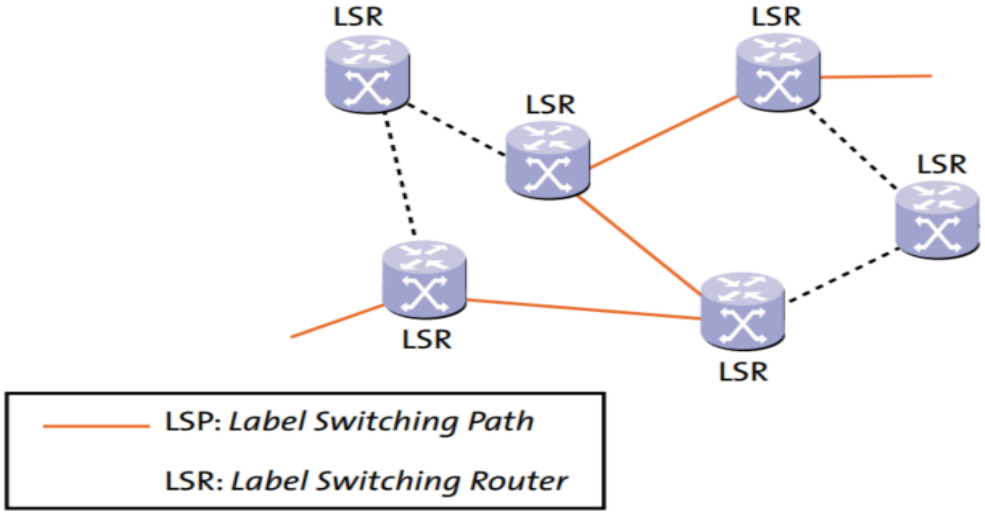
Se conforma principalmente de:

- **Label Switch Router (LSR):** Dispositivo de capa 3 que es parte del proveedor de servicios y realiza el proceso de distribución de etiquetas y transportación de paquetes.
- **Label**: La etiqueta tiene un tamaño de 20 bits la cual representa una FEC.
- **Label Switched Path** (**LSP):** Camino de un paquete a través de uno o más LSR.
- **Bindings**: Cuando la decisión de asignar una etiqueta a los paquetes depende del siguiente LSR.
- **Label Distribution Protocol (LDP)**: Aquellos procedimientos en donde un LSR comunica a otro los bindings realizados.
- **Label Edge Router (LER):** Dispositivos de capa 3 ubicados de conectar diferentes redes (ATM, Frame Relay,etc) e inserta y retira las etiquetas de acuerdo con la información de enrutamiento.
- **Forward Equivalence Class(FEC):** Conjunto de paquetes que tienen mismos requerimientos para ser transmitidos y transportados por un mismo camino.

Como se puede apreciar en la Figura 1 MPLS combina la gestión de tráfico capa 2 con la escalabilidad y flexibilidad del enrutamiento de capa 3, y permite que las redes de datagrama funciones como red de conmutación de circuito virtuales. Están compuestas por LSR y LER, los cuales realizan el encaminamiento de acuerdo con la etiqueta MPLS, y las tablas de conmutación que deben encontrarse en todos los nodos. El objetivo es realizar una adecuada gestión de recursos de la red de acuerdo con la reserva de capacidades de transmisión extremo a extremo.

Figura 1

Arquitectura básica de MPLS



Interfaz de entrada	Etiqueta de entrada	Interfaz de salida	Etiqueta de salida
13	17	5	7
4	7	12	11

Nota. La figura muestra los elementos de una red MPLS básica. Fuente: Telefónica I+D (2015).

2.1.3. Aplicaciones MPLS

MPLS es especialmente útil para la gestión y soporte de aplicaciones como:

- **Ingeniería de tráfico.** Esta busca optimizar el uso de los recursos físicos de la red para reducir el costo de operaciones y adaptar el flujo de tráfico, previniendo así posibles cuellos de botella, mientras otras son poco utilizadas y así determinar el camino disponible y más rápido.
- **Diferenciación de niveles de servicio mediante clases (CoS):** Se basa en modelos de la IETF para redes IP, estos modelos permiten priorizar diferentes aplicaciones que circulan en la red, tomando como parámetros el ancho de banda,

retardo, jitter y pérdida de datos, y clasificarlos en un tráfico reducido de clases de servicio.

- **Servicio de redes virtuales (VPN):** Ofrecen escalabilidad, fáciles de administrar y divide la red del proveedor en donde se constituye a base de conexiones realizadas sobre una infraestructura compartida con funciones de red parecidas a las de una red privada.

2.1.4. Ventajas y desventajas de MPLS

Ventajas

- Un paquete que se encuentre fuera de un dispositivo que no sea MPLS puede entrar si se encuentra el punto final conectado físicamente a la red
- Cuando se reenvía información mediante una búsqueda (lookup) en una tabla predeterminada en donde se enlaza los valores de las etiquetas con la dirección o direcciones del siguiente salto
- Cuando existe paquetes enviados desde puntos finales pueden tener diferentes FEC, por lo tanto, diferentes etiquetas y un PBH distinto tendrán en cada LSR y provoca flujos diferentes en la red.

Desventajas

- Tiene un costo alto en comparación al costo normal de conectividad de internet y más aún si se tiene más de un proveedor.
- Demora algún tiempo en el despliegue de una nueva sucursal, y muchas veces no es fácil llevar MPLS a ciertas zonas.
- Se requiere de una persona en cada sucursal de forma presencial para la configuración lo que implica un aumento de costos de operación.

2.2. Redes de área extendida (WAN)

Las redes de área extendida (WAN) se forma por numerosos nodos de conmutación que están interconectados y cubre largas distancias entre varias sucursales en donde se necesita atravesar rutas de acceso público (Tanenbaum et al., 2021).

2.2.1. Funcionamiento de WAN

Una WAN se forma de varios nodos de conmutación interconectados por lo que en una transmisión desde algún dispositivo es enrutado a través de estos dispositivos o nodos internos hasta el nodo destino especificado, a estos nodos no les concierne el contenido de los datos ya que su propósito es realizar la conmutación y que envié los datos de nodo en nodo hasta su destino. Se ha implementado principalmente dos tecnologías: conmutación de circuitos y conmutación de paquetes y en ocasiones se emplea la retransmisión de tramas (Stallings,2014).

- **Conmutación de circuitos:** Se necesita establecer un camino dedicado para interconectar estaciones a través de los dispositivos de red. Los datos que se generan en el nodo fuente se encaminan rápidamente por el camino dedicado. En cada dispositivo o nodo de entrada se dirige por el respectivo canal de salida sin demoras.
- **Conmutación de paquetes:** En esta situación no es necesario realizar asignación de capacidad de transmisión durante el camino ya que los datos son enviados en pequeñas secuencias llamados paquetes en donde cada paquete siguiendo la ruta entre estación origen y destino pasa por los nodos de la red en donde este recibe completamente y es almacenado por un lapso y posteriormente es transmitido al siguiente nodo y utilizan para comunicarse terminal-computador y computador-computador.

- **Retransmisión de tramas (frame relay):** Se añade información redundante a cada paquete para detectar errores

La subred de la WAN está compuesta de dos elementos como son: las líneas de transmisión y elementos de conmutación.

- **Líneas de transmisión:** Estas mueven los bits entre los dispositivos y pueden ser cobre, fibra óptica e incluso enlaces de radio usualmente alquilan las líneas de transmisión a empresas que disponen de este medio.
- **Elementos de conmutación:** Son dispositivos de conmutación los cuales conectas dos o más líneas de transmisión como lo son router

2.2.2. Tipos de WAN

El criterio para clasificarlos es el uso o no de circuitos dedicados en donde quiere decir si el medio de transmisión entre los nodos permanece abierto permanente o se debe conectar distintos canales físicos para establecer conexión en ese caso se habla de circuitos conmutados.

- **WAN dedicada:** Son conexiones permanentes entre las redes de área local o conocidas como enlaces punto a punto en donde brindan una ruta específica y se implementa un dispositivo de enrutamiento en cada red de área local.
- **WAN conmutada:** Conmutación de circuitos, se crea un circuito físico en donde se mantiene y finaliza con el mismo proporcionado por una compañía de telecomunicaciones en donde se mantiene un ancho de banda estable es similar a la tecnología utilizada en llamadas telefónicas

2.2.3. Ventajas y desventajas de WAN

Ventajas

- No tiene límite de espacio geográfico para establecer comunicación entre estaciones
- Tiene amplia escala de medios de transmisión
- Permite la expansión de sucursales ya que pueden expandir la red mediante el uso de puertas de enlaces, puentes y enrutadores.

Desventajas

- La configuración está distribuida en cada enrutador.
- La administración de nuevas políticas se debe realizar la manipulación por cada uno de los dispositivos.
- La arquitectura WAN es privada y estática, lo cual la vuelve un problema para migrar a la nube.
- Su ancho de banda es limitado debido al costo de los circuitos privados que se contratan lo que provoca en un bajo rendimiento de aplicaciones.
- Es dependiente de un centro de datos al no tener acceso a los recursos desde sucursales en el cual provoca un retardo y baja el rendimiento de la empresa.
- Infraestructura costosa y compleja.

2.3. Red definida por software (SDN)

El principal objetivo de las redes definidas por software (SDN) consiste en centralizar la inteligencia de la red separando el plano de control del plano de datos mediante la programación de aplicaciones que en este caso se denomina controladora SDN la cual mantiene una visión, gestión global y comunicación con los dispositivos de red a través de un protocolo. SDN delega las capacidades de la toma de decisiones en el servidor eliminando la inteligencia de redes tradicionales del hardware y se simplifica el diseño y control, en donde plano de datos y plano de

control cada uno está automatizado ya que se virtualizan las funciones de red en un solo hardware (NFV) (Ariganello, 2020).

2.3.1. Arquitectura SDN

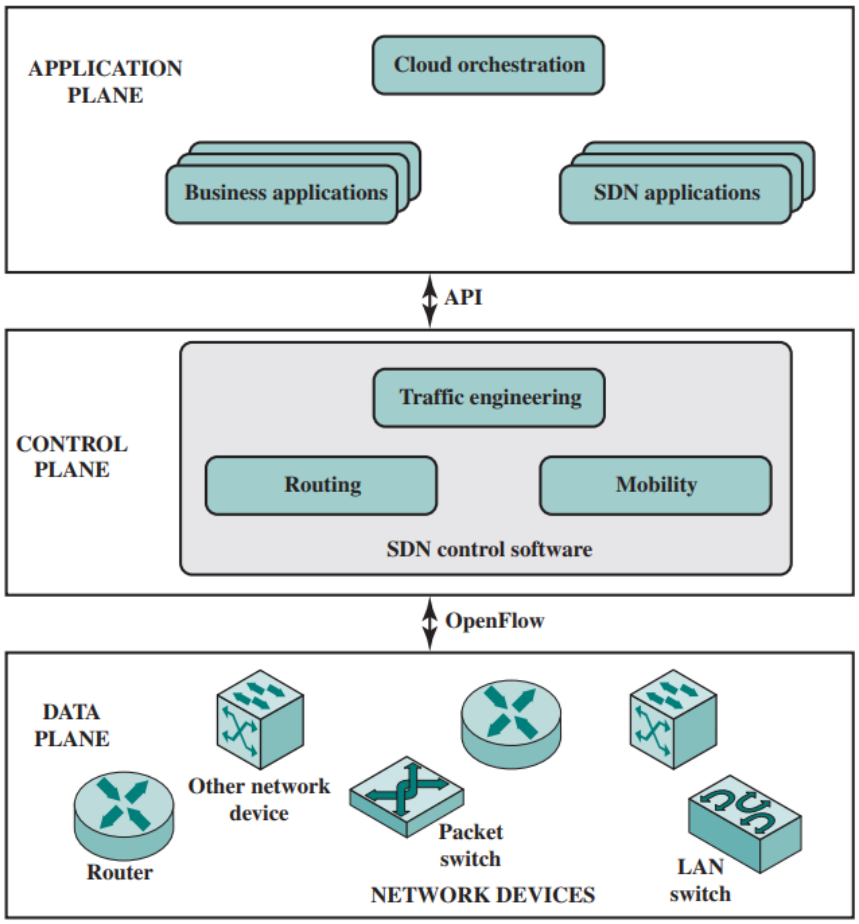
Según la Open Network Foundation (ONF) que es la organización que se encuentra más relacionada con SDN definen como una arquitectura que puede ser dinámica, gestionable, adaptable y rentable. Esta arquitectura al tener el plano de control y plano de datos separados permite que el control de la red pueda ser programado entonces se elimina la función de control en los dispositivos y se traspasa a la controladora (Open Networking Foundation, 2022).

La estructura de una SDN tal y como se observa en la Figura 2 muestra la relación de los dos planos y tres capas que son aplicación, control e infraestructura o de datos.

- **Capa Aplicación:** es responsable de comunicar las solicitudes de información o recursos acerca de la red.
- **Capa de control:** es responsable un grupo de datos local utilizado para crear entradas de la tabla de reenvío los cuales sirven para definir el funcionamiento y enrutamiento de la red y también la calidad de servicio (Qos). La comunicación entre la controladora y los conmutadores se la realiza mediante un protocolo y una interfaz de programación de aplicaciones (API).
- **Capa de datos o infraestructura**: es responsable del manejo de paquetes entrantes por medio de enlaces independientes de la interfaz física, mientras sucede el proceso de recolección, se realizan recopilación de estadísticas.

Figura 2

Arquitectura base de SDN.



Nota. La figura muestra las 3 capas que conforman una SDN. Fuente: Stallings (2014).

En una arquitectura SDN un switch se encarga de encapsular y reenviar el primer paquete a la controladora SDN, reenviar los paquetes el puerto correcto basado en la tabla de flujo dictada por la controladora, también puede dejar caer paquetes en un flujo específico de manera temporal o permanente según la controladora.

2.3.2. Protocolo OpenFlow

Es un protocolo utilizado en interfaces de SDN en donde establece la comunicación entre el plano de control y el plano de datos en cada dispositivo de red que lo permite para dirigir los

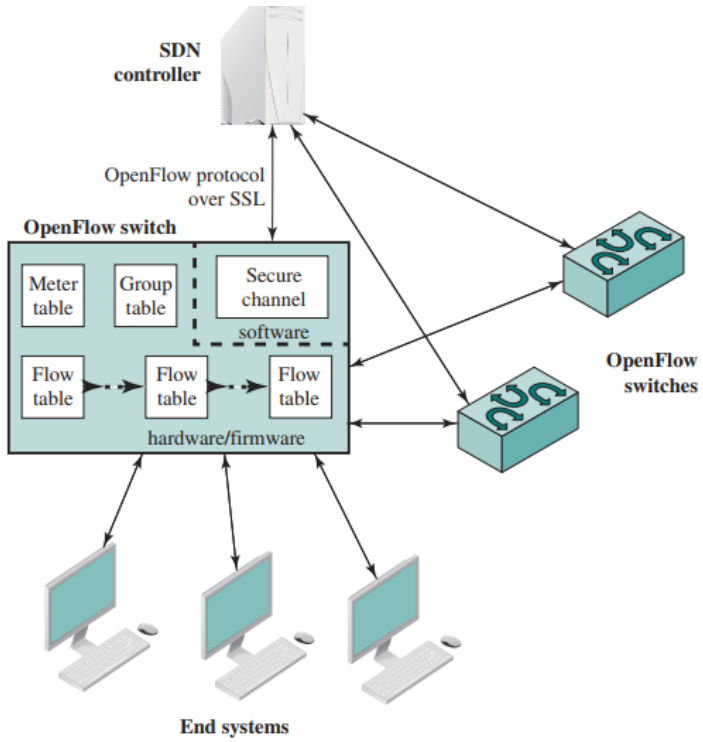
paquetes hacia el destino. Se ha formado para ofrecer una aplicación externa con acceso al plano de reenvío de un conmutador de red o enrutador el cual para el acceso al enrutador se pueda obtener mediante la red y permitir que el programa de control no deba tener necesariamente cerca al conmutador (Stallings, 2014).

Al centralizar el control de dispositivos, OpenFlow ayuda la administración de la red y la programación que SDN ofrece. Este protocolo utiliza el término de flujos para poder identificar el tráfico basado en reglas establecidas que son programadas de forma dinámica o estática en la controladora permitiendo a la red responder en tiempo real a nivel de sesión, usuario y aplicación. Entonces el uso de tablas de flujo sirve para identificar el tráfico de red y especifica que funciones deben realizarse en los paquetes, puede haber múltiples tablas de flujo las mismas dirigen un flujo a una tabla de grupo y desencadena acciones que afectan a uno o más flujos. Entonces OpenFlow permite la convergencia de recursos que posee la red con las demás redes existentes ya sea física o virtual, indica como fluir al tráfico basado en los requerimiento y parámetros de las aplicaciones además de establecer protocolos de red de manera centralizada.

OpenFlow utiliza una controladora como se observa en la Figura3 en donde el plano de control funciona independientemente del switch y esta se interconecta entre switches formando una red más centralizada. La controladora puede configurarse con el fin de controlar y dar flexibilidad al tráfico y una vez que se establece la comunicación entre switch y la controladora puede darse el intercambio de datos y crear reglas de entrada en su tabla, controlar características y parámetros.

Figura 3

Arquitectura OpenFlow switch.



Nota. En la figura se muestra como una controladora SDN se comunica con los conmutadores que son compatibles con OpenFlow. Fuente: Stallings (2014).

2.3.3. Controladoras SDN

Una controladora SDN es un elemento centralizado que ofrece gestión y control de una red definida por software. Los administradores de red pueden establecer políticas y reglas de enrutamiento mediante una interfaz de programación versátil y dinámica. Existen dos tipos de controladores: los de código libre y los de código licenciado. Por otro lado, es importante destacar que el software libre permite un ahorro económico, ofrece flexibilidad y facilita la gestión de la herramienta a lo largo del desarrollo de proyectos.

Las controladoras SDN de software libre son cada uno únicos para sus respectivos desarrolladores, que manejan cada uno una estructura operativa distinta. A continuación, se

ofrece una descripción completa de las estructuras que gestiona cada controlador que son controladores de software libre: ONOS, RYU, ODL, NOX/POX y Floodlight

2.3.3.1. ONOS (Open Network Operating System).

La controladora SDN de alto rendimiento, escalable y flexible conocido como ONOS (Open Network Operating System) ofrece una plataforma abierta para la administración y el control de redes, su principal objetivo es programar de forma centralizada los dispositivos de red y separar la capa de control. La arquitectura de ONOS se basa en un diseño modular basado en componentes, gracias a su arquitectura modular el sistema es más adaptable y extensible, además, ONOS está diseñado para ser extremadamente tolerante a fallos y distribuido, lo que garantiza su escalabilidad y resistencia en redes de gran tamaño (Berde et al., 2014).

En cuanto a la distribución, ONOS puede ejecutarse en varios nodos, lo que permite la distribución de la carga de trabajo y la capacidad de escalar horizontalmente de acuerdo con los requisitos de la red como se puede observar en la Figura 4 está formado por subsistemas y varios componentes que se encuentran agrupados por capas de diferentes funciones, se divide en Aplicaciones (Apps), Northbound (consumer) API, Core, Southbound (provider) API, Providers, Protocols y Network Elements (ONOS Project, 2016).

Las Aplicaciones a través de las interfaces AdminService y Service, acceden a la información recopilada por los gestores y la modifican. Cada programa tiene un ID especial (ApplicationId), que ONOS utiliza para gestionar el contexto con el que está vinculado. Las aplicaciones deben registrarse en el CoreService y proporcionar su nombre (por ejemplo, org.onoslab.onos.fwd) para recibir una identificación válida.

Northbound(**NB**) La interfaz que permite la comunicación entre el núcleo y la capa de aplicaciones o servicios es la Interfaz Northbound (NB). Es necesaria para la gestión de la red por aplicaciones externas, lo que significa que el controlador aplica políticas independientemente de su lógica subyacente tras recibir un anuncio de una aplicación de la capa superior.

El Core, por su parte, es el núcleo de la arquitectura y se encarga de controlar los nodos de la red, como conmutadores, enrutadores y puntos de acceso. Gestiona los puntos finales, incluidos los hosts que sirven de origen y destino de un tráfico determinado. El Core mantiene las conexiones entre nodos, dispositivos finales, reglas de tabla de flujo de equipos y ofrece una representación completa de la red. Existen servicios y subsistemas en el ONOS Core. Un servicio es una unidad funcionalmente distinta formada por numerosos componentes distintivos de la pila de software. Un subsistema es un grupo de partes que juntas proporcionan un servicio. En su núcleo, ONOS identifica los siguientes subsistemas clave:

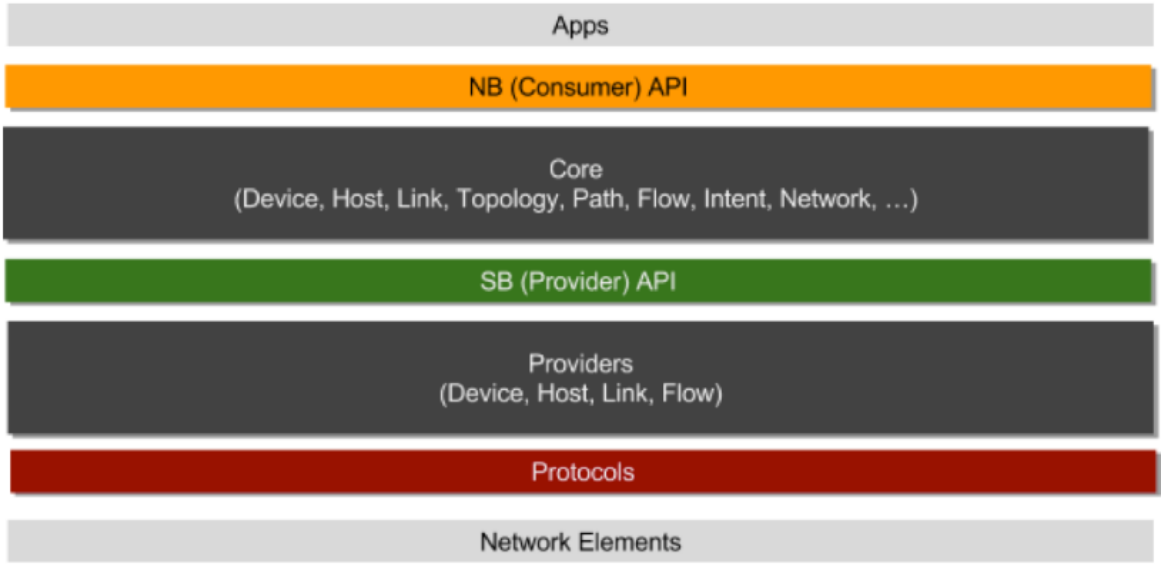
- Controla el inventario de dispositivos de red es el subsistema de dispositivos.
- Subsistema de enlaces: Controla el inventario de enlaces.
- Subsistema de hosts: Gestiona la lista de hosts finales y dónde están situados dentro de la red.
- Gestiona instantáneas ordenadas cronológicamente del gráfico de red.
- Utilizando la instantánea más reciente del grafo, el subsistema de rutas calcula y localiza rutas entre hosts o dispositivos de la red.
- Las reglas de match/action instaladas en los dispositivos de red son gestionadas por el subsistema de reglas de flujo, que también ofrece métricas de flujo.

- Subsistema de paquetes: Permite a las aplicaciones enviar y recibir paquetes de datos a través de uno o varios dispositivos y escuchar los paquetes procedentes de los dispositivos de red.
- **El Southbound (SB)** se encarga de facilitar la comunicación entre los componentes de red de capa inferior y la capa central. Utilizando una pila de protocolos de comunicación, como OpenFlow, NET-CONF y SNMP, entre otros, proporciona interoperabilidad, integración o eliminación de equipos mientras la red sigue operativa. Además, permite la integración de equipos virtuales para su estudio sin necesidad de equipos reales.

Providers se encuentran en la parte inferior. Los proveedores se comunican con el núcleo a través de la interfaz ProviderService y con la red a través de determinadas bibliotecas de protocolos. Los Proveedores que utilizan protocolos se encargan de comunicarse con el entorno de red a través de una serie de protocolos de control y configuración y de proporcionar al Núcleo determinados datos de servicio. Puede ser necesario que algunos Proveedores reciban peticiones del Core y las implementen en la red utilizando los protocolos adecuados. Cada Proveedor tiene una identificación única (ProviderId) que sirve como identidad externa. Esto permite que los dispositivos y otras entidades sigan vinculados a la identidad del Proveedor incluso después de que haya sido desinstalado o descargado.

Figura 4

Arquitectura ONOS



Nota. En la figura se muestra la arquitectura de la controladora ONOS que está diseñado con diferentes niveles de funciones. Fuente: ONOS Project (2016).

2.3.3.2. RYU

Es una controladora SDN la cual fue presentada por la empresa japonesa NTT y desarrollada por la misma. Ryu proporciona componentes de software con API bien definidas elcuál pone fácil para los desarrolladores crear una nueva administración y control de la red, también admite varios protocolos para administrar la red dispositivos, como OpenFlow, Netconf, OF-config, etc. Todo el código está disponible gratis bajo la licencia Apache 2.0, cabe resaltar que RYU está completamente escrito en Python.

La arquitectura de Ryu sigue un enfoque de controlador centralizado, lo que significa que el control y la gestión de la red se centralizan en un único punto, y facilita la administración, la configuración de la red. Al proporcionar una API sencilla y bien documentada permite la comunicación con switches OpenFlow. La arquitectura de Ryu también permite la

implementación de lógica de control personalizada mediante el uso de módulos Python para definir el comportamiento y la funcionalidad del controlador, lo que brinda una gran flexibilidad y capacidad de personalizar (Ryu NOS, 2014).

2.3.3.3. Floodlight

Esta controladora SDN de código abierto se basa en el protocolo OpenFlow. Su diseño se centra en ser modular, extensible y flexible, lo que permite el desarrollo de aplicaciones personalizadas y la gestión centralizada de la red. Está compuesto por diferentes módulos que se encargan de tareas específicas. También los desarrolladores tienen la capacidad de agregar nuevas funcionalidades y características al controlador mediante la implementación de módulos adicionales. Esta extensibilidad permite adaptar el controlador a escenarios de red más complejos y específicos.

En términos de arquitectura, Floodlight sigue un enfoque de controlador centralizado. Esto significa que todas las decisiones de control y gestión se toman en un solo punto central, lo que facilita la administración de la red. La lógica de control en Floodlight se implementa mediante el uso de módulos Java. Estos módulos Java son responsables de procesar los mensajes OpenFlow recibidos de los dispositivos de red y tomar decisiones sobre el comportamiento de la red (Project floodligth,(s.f)).

2.3.3.4. OpenDaylight (ODL)

Esta controladora SDN es un proyecto de código abierto que se destaca por ofrecer un servicio altamente modular y escalable, está diseñado para proporcionar un marco de trabajo flexible que permite la implementación de aplicaciones y servicios de red en entornos SDN. Una de las características importantes de OpenDaylight es su enfoque modular. Utiliza una arquitectura basada en plugins, lo que significa que se compone de diferentes módulos que

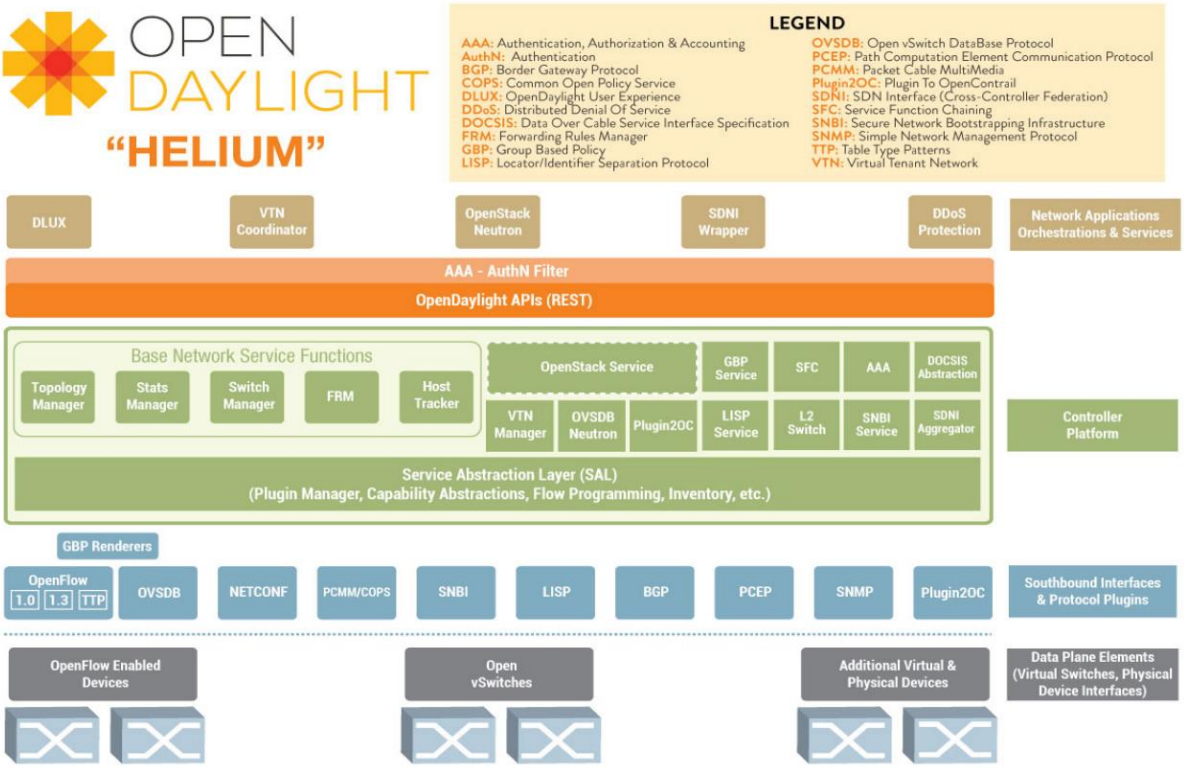
implementan funcionalidades específicas. Esto permite una mayor flexibilidad y extensibilidad, ya que los desarrolladores pueden seleccionar y combinar los módulos necesarios para adaptarse a los requisitos de su red. En cuanto a la arquitectura, OpenDaylight se basa en módulos que implementan diversas funcionalidades. Estos módulos pueden incluir el manejo del plano de control, el procesamiento de políticas, la gestión de topología de red, entre otros. La arquitectura de plugins permite la integración de diferentes componentes y tecnologías de red, lo que facilita la interoperabilidad y la adopción de estándares (Anderson et al., 2013).

La Figura 5 destaca una arquitectura de ODL la cual está representada por:

- The Southbound Interface and Protocols Plugins: OpenDaylight soporta una serie de protocolos SB a través de plugins, permitiendo la gestión, configuración y monitorización de componentes de red. Los plugins SB soportados incluyen OpenFlow, OVSDB, SNMP, BGP-LS/PCEP, y NETCONF, entre otros.
- The Controller Platform facilita la abstracción SDN. Ofrece API abiertas para que las aplicaciones de red puedan gestionar y controlar los componentes físicos y virtuales de la red. También consta de las Funciones de Servicio de Red Base (BNSFs), las Funciones de Servicio de Red de Plataforma y la Capa de Abstracción de Servicios (SAL).
- The Network Applications and Services: Las aplicaciones y servicios de red que controlan, administran y monitorizan toda la red se encuentran en la capa superior de OpenDaylight. La interfaz de usuario openDayLight User eXperience User Interface (DLUX), VTN Coordinator, DDoS Protection y SDNi Wrapper son algunos de estos programas.

Figura 5

Arquitectura de ODL



Nota. En la presente figura se observa la arquitectura completa de OpenDaylight lo que permite la integración de distintas tecnologías de red y componentes. Fuente: Hemid (2017).

2.3.4. Ventajas y desventajas de SDN

Ventajas

- La flexibilidad de la red
- Menos costo de operación
- Disminuye el trabajo de aprovisionamiento y administración de red
- Cumplimiento de la ingeniería de tráfico
- Se tiene una mejor visibilidad de la red debido a la separación de los planos de control y datos
- Ofrece mejor seguridad a la mayor visibilidad de la red.

Desventajas

- Escalabilidad ya que depende del controlador y de recursos de un conmutador, ya que si la controladora presenta problemas de rendimiento.
- Confiabilidad redundancias en la controladora central de la red.
- Amenazas de seguridad ya que cuando se desplegar la infraestructura nueva se elimina el uso de enrutadores.

2.4. Red de área extensa basada en una arquitectura definida por software (SD-WAN)

Las redes de área extensa basada en una arquitectura definida por software es un enfoque avanzado de red ya que crea redes híbridas para que sea integrado aspectos como el ancho de banda y otros servicios de red en la WAN empresarial, que sea capaz de mantener la seguridad y el rendimiento en tiempo real.

2.4.1. Introducción a SD-WAN

En la actualidad las telecomunicaciones se han expandido cada día más y más, dando lugar a la demanda de servicio y aplicaciones con diferentes requerimientos para las empresas y todos los usuarios en general trayendo dificultades y problemas para la administración de la red. Tiene similitud con las SDN, Mientras que este se encuentra enfocado a centros de datos internos de una sede, SD-WAN adquiere esos conceptos y desacopla del plano de control del plano de datos. Hay que ser conscientes que existe una gran parte de proveedores de servicio que no dispone una propia tecnología por eso se ofreces servicios intermediados con SD-WAN gestionados. SD-WAN ha llegado para formar parte de la transformación digital y da otro tipo de visión a las redes tradicionales que no eral centralizadas de manera óptima.

2.4.2. Definición de SD-WAN

SD-WAN lo que hace básicamente es combinar los servicios de transporte MPLS, TLE, o los de una red MPLS para posteriormente conectar de manera segura a los clientes con las aplicaciones evitando que el tráfico regrese a un hub. Este hace uso de una función de control centralizada para manejar el tráfico por medio de una red WAN siendo más segura ya que SD-WAN separa el plano de datos y el plano de control esto quiere decir que si la conexión llegara a perderse a su plataforma de control los servicios continúan funcionando sin problemas (IBM, 2022).

2.4.3. Arquitectura de SD-WAN

En SD-WAN se pretende simplificar las operaciones de red en las redes WAN, optimizar la gestión de red e introducir innovación y flexibilidad en comparación de esta arquitectura es por eso por lo que se tiene la arquitectura lógica y la arquitectura física.

2.4.3.1. Arquitectura lógica

Existen 3 capas principales como se muestra en la Figura 6 las cuales incluyen capa de datos, capa de control y capa de aplicación parecido a la arquitectura de las redes SDN.

- El reenvío de datos y la virtualización del ancho de banda son tareas de la capa de datos. Al combinar varios canales de red, la virtualización del ancho de banda crea una reserva de recursos que pueden utilizar todas las aplicaciones y servicios. Utilizando el ancho de banda puesto a disposición por la virtualización del ancho de banda, un grupo distribuido de componentes de red de reenvío principalmente conmutadores se encargarán del reenvío de datos. A través de protocolos de interfaz como OpenFlow, tanto la virtualización del ancho de banda como las

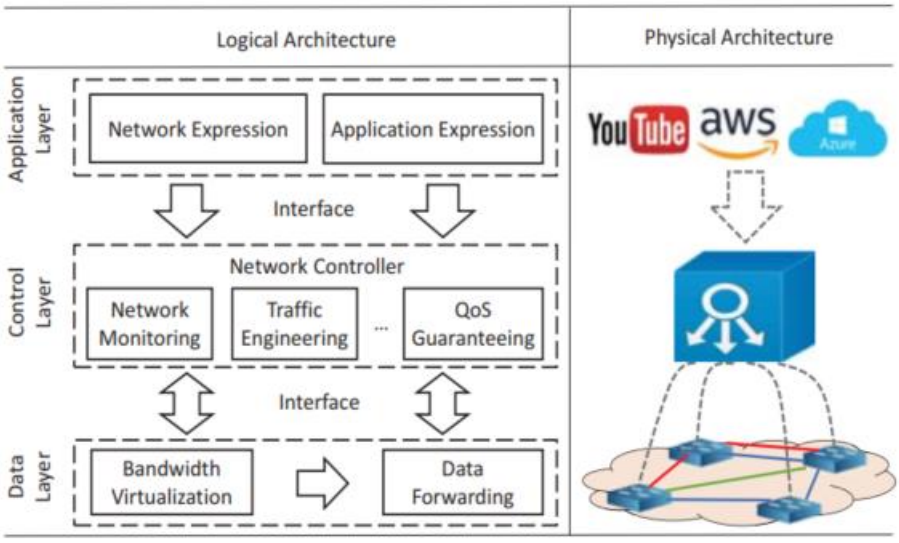
operaciones de reenvío de datos reciben instrucciones del controlador de red de capa superior.

- La capa de control consiste en una serie de funciones de red desarrolladas y que se gestionan de forma independiente. Los administradores de red pueden desarrollar, alterar, depurar y eliminar funciones concretas a un coste razonable sin afectar a otras gracias a la disociación de estas operaciones. La versatilidad de la SD-WAN aumenta gracias a la capacidad de unir o encadenar estas funciones de red para crear diversos servicios. Por ejemplo, la ingeniería de tráfico puede calcular las mejores opciones de programación utilizando la supervisión de red, que ofrece una visión global de la red. Durante la transmisión de datos, el aseguramiento de la calidad del servicio (QoS) garantiza que se satisfacen las necesidades de la aplicación.
- La capa de aplicación permite a los proveedores de red y desarrolladores de aplicaciones declarar sus requisitos de red específicos mediante expresiones de red y expresiones de aplicación. Las necesidades de alto nivel que casi se describen en lenguaje llano pueden convertirse en configuraciones de red conformes mediante estas expresiones. Las características de la aplicación deben tenerse en cuenta a la hora de adaptar la normativa de red, ya que los requisitos de las aplicaciones se complican y en ocasiones pueden entrar en conflicto entre estos requisitos, lo que exige personalizar las políticas de red teniendo en cuenta las características de la aplicación Por ejemplo, un servicio de streaming de vídeo en directo espera una alta tasa de bits y una baja latencia para satisfacer a los usuarios, pero estos objetivos entran en conflicto entre sí. Los desarrolladores

pueden declarar sus planteamientos para hacer frente a estos requisitos y ponerlos en práctica en la red de área extensa subyacente mediante la expresión de aplicaciones. Los requisitos de red similares, como la red multiobjetivo y la red rentable, se declaran mediante la expresión de red. Los proveedores de servicios de red y los desarrolladores de aplicaciones pueden tener más control sobre la red gracias a la capa de aplicación (Yang1 et al., 2019).

Figura 6

Arquitectura SD-WAN



Nota. En la figura se presenta un esquema de la arquitectura SD-WAN en donde muestra las 3 capas de las cuales está compuesta la arquitectura lógica. Fuente (Yang1 et al., 2019).

2.4.3.2. Arquitectura física

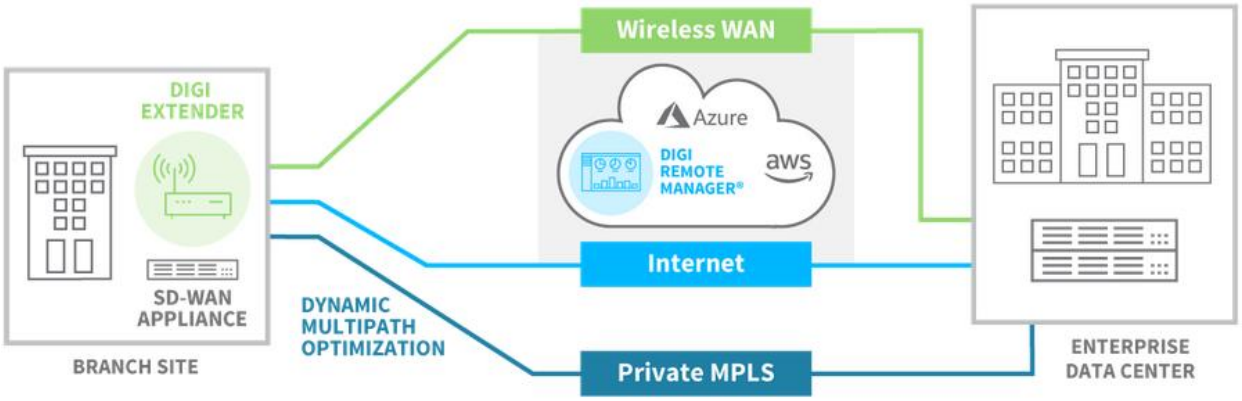
Como se mostró en la Figura 6 a la derecha de la arquitectura lógica, se muestra la arquitectura física de una red de área extensa definida por software. Varios conmutadores SDN están conectados entre sí a través de enlaces físicos en la capa de datos, estos dispositivos están controlados por un controlador de red. Dependiendo del tamaño y la complejidad de la red, el controlador de red suele ser un servidor o un clúster, se encarga de determinadas operaciones de

red. Las aplicaciones específicas se sitúan sobre el controlador de red este puede recibir requisitos de desarrolladores de aplicaciones y proveedores de servicios de red, y el controlador de red traducirá esos requisitos en políticas y configuraciones compatibles. (Yang1 et al., 2019).

2.4.4. Funcionamiento de SD-WAN

Como superposición a la red actual, SD-WAN prioriza una red sobre otra. Como se ve en la Figura 7, utiliza tunelización para distinguir entre la red física y la red lógica. Para administrar toda la red y establecer políticas, SD-WAN utiliza un controlador centralizado que sirve de panel único. Estas políticas permiten controlar el enrutamiento del tráfico, el SLA, la conmutación por error, la supervisión y otros factores. Zero Touch Provisioning (ZTP) es el proceso de configuración de cada nodo SD-WAN sin la intervención de un administrador de red una vez especificadas las políticas. A continuación, la red SD-WAN supervisa de forma inteligente el rendimiento de los enlaces en función de las políticas configuradas en cada nodo y comienza a enrutar el tráfico por la mejor ruta en función del Service Level Agreement (SLA) definido previamente. Al desviar el tráfico a un enlace de reserva o redundante en este momento, se elimina cualquier interrupción del circuito (Burwood Group, 2019).

Figura 7 Esquema de SD WAN



Nota. La figura muestra el funcionamiento de una red SD-WAN básico. Fuente: Digi International (2023).

Las aplicaciones suelen alojarse en un centro de datos en la sede corporativa cuando las grandes organizaciones geográficamente dispersas emplean redes de área extensa (WAN) tradicionales. Aunque la mayoría de los usuarios se encuentran en oficinas de campo y las propias aplicaciones están basadas en la nube y son accesibles a los usuarios a través de Internet, el tráfico de las aplicaciones se enruta hacia y desde el centro de datos a través de una conexión de línea alquilada. En este proceso hay mucho backhaul, lo que ralentiza el rendimiento de las aplicaciones y disminuye la productividad de los usuarios. Ni que decir tiene que el ancho de banda necesario para gestionar todo ese tráfico no es barato. Una estrategia más adaptable es la que ofrece SD-WAN, que permite a las empresas mantener sus propias redes de líneas alquiladas y complementarlas con la selección dinámica de rutas. Debido al uso casi universal de VPN basadas en IPsec en las SD-WAN, se pueden utilizar distintos mecanismos de transporte, incluida la banda ancha de consumo, sin sacrificar la seguridad (Digi International, 2023).

2.4.5. Ventajas y desventajas de SD-WAN

Ventajas

- Calidad de servicio (QoS) ya que administrando un canal añadido se toman decisiones que se acojan a las necesidades de la empresa.
- Tiene varios métodos para integrar VPN para así no afecte a la infraestructura actual y funcionar posteriormente de un firewall de nueva generación con enlaces de banda ancha.
- El establecimiento de conexiones redundantes para evitar cuello de botella en una sola ruta al limitar el ancho de banda.

- La seguridad al utilizar redes privadas que están basadas en Internet Protocol Security (IPSec) o Dynamic Multipoint VPN (DMVPN) lo que incrementa la seguridad para la protección de datos procesados en el Internet.
- No requiere de ingenieros de campo para su instalación ya que se puede hacer de manera remota o por medio de equipos ya configurados anteriormente lo que reduce gastos, la implementación es automática, la instalación es rápida y confiable.
- Gestión de tráfico desde cualquier sitio concluyente y puede realizarlo en la capa 7 del modelo OSI, esto permite que los administradores configuren sin bajarse a nivel IP.
- El rendimiento de las aplicaciones mejora, ya que las aplicaciones SD-WAN no tienen que enviarse a la oficina principal o central ya que pueden gestionarse directamente, su rendimiento mejorará, y permite aplicar funciones de calidad de servicio, priorizando las aplicaciones más cruciales para optimizar las aplicaciones con el fin de optimizar el tiempo de respuesta.
- Atender múltiples y diferentes tipos de conexiones, desde redes VPN.

Desventajas

- Es importante contar con el debido personal especializado TI para realizar la planificación, diseño y mantenimiento de esta solución.
- Existe la posibilidad de jitter y pérdida de paquetes al depender de la conexión de internet.

2.5. Calidad de servicio (QoS)

La calidad de servicio (QoS) es un conjunto de técnicas y normas del servicio los cuales nos permiten priorizar el tráfico, garantizar la calidad de la información y disponibilidad de ancho banda, las cuales determinan el grado de satisfacción del usuario. La QoS se ha convertido en un tema importante para los proveedores de servicios crecientes y buscan la forma de diferenciar los niveles de servicio proporcionados a clientes (Marqués, 2016).

2.5.1. Fundamentos de QoS

Actualmente existen diferentes tipos de aplicaciones que se encuentran en la red como envío de correo, VoIP, streamming, intercambio de archivos, hosting, entre otros, los cuales dependen en gran mayoría de la red y no todas son tan importantes en cada empresa varia por eso es fundamental conocer los aspectos importantes para determinar cómo priorizar las distintas aplicaciones entre los cuales tenemos: ancho de banda, latencia, jitter, pérdida de paquetes.

- Ancho de banda: no es más que la capacidad que un dispositivo tiene para transmitir y procesar información medidos en un determinado tiempo el cual se mide en bits por segundo (bps).
- Latencia o retardo: es el tiempo de retraso que sufren los paquetes desde su origen hasta el destinatario esta situación puede verse afectada por dispositivos intermediarios por los que atraviesan los datos, retraso en el proceso de encapsulación de la información que se dirige a un medio, demora de encolamiento, entre otros.
- Jitter (Delay Variation): prácticamente es aquella variación en el tiempo de llegada de los paquetes debido a congestión de la red de datos o por enviar paquetes por diferentes rutas.

- Perdida de paquetes (Loss): estas pérdidas de paquetes se pueden originar por hardware por si algún componente de red falla, también se puede dar por cuellos de botella en la red.

2.5.2. Herramientas y mecanismos de QoS

Tenemos varios mecanismos y herramientas para la Calidad de servicio:

- **Clasificación:** el tipo o grupo al que pertenece los paquetes va a depender del valor con el que fue marcado, Cada tipo tendrá un diferente procedimiento de acuerdo con las políticas establecida para cada clase.
- **Mercado:** para el marcado se necesita escribir un campo en el paquete con el fin de diferenciar un paquete de otro tipo. Se modifica DiffSer (DS) el cual ocupa sus seis primeros bits del Tipo de servicio IPv4 y Clase de tráfico en IPv6 los cuales se realiza en el router de borde.
- **Shaping:** se amortigua el tráfico a una predeterminada tasa de bits intentando no sobrepasar el límite establecido. Lo que implica la aparición de colas y el espacio suficiente de memoria para contener los paquetes pendientes.
- **Policing:** detecta el tráfico enorme, elimina los paquetes con el propósito de tener a los flujos de datos en los límites establecidos.
- **Congestion Avoidance:** es el esfuerzo realizado por los nodos de la red para evitar o prevenir sobrecargas de esta que conducen a la pérdida de paquetes. Los enrutadores contienen a los paquetes en colas hasta tener los recursos suficientes para reenviarlos por el puerto que corresponda.
- **Queuing:** esta técnica es una manera de manejar la congestión permite definir varias colas a la vez.

- **Auto QoS:** prioriza el tráfico sensible al retardo**,** prioriza el tráfico, preserva el ancho de banda demorando el reenvío de datos no críticos para el cliente, se puede modificar las políticas de QoS y volverlas a utilizar como si fuera un template, al mismo tiempo que se ahorra tiempo de configuración.
- **Call Admission control (CAC):** el control de admisión de llamadas es un sistema que se basa en parámetros de calidad de servicio para telefonía IP el cual utiliza SIP.

2.5.3. Modelos de calidad de servicio

Actualmente ha aumentado de manera rápida el número de usuarios de las redes de telecomunicación lo cual ha llevado a la división de los clientes ya que cada uno tiene necesidades diferentes buscando la utilidad necesaria a sus conexiones de red como lo es para trabajo, o entretenimiento y creyendo que el sobredimensionamiento de la red en lo que refiere a ancho de banda y prestación de equipos se piensa que evitará congestión en la red y retardos en las aplicaciones. Es por esto que se realizan esfuerzos considerables en que las nuevas arquitecturas tengan la capacidad de diferenciar flujos de tráfico con mecanismos de gestión de tráfico avanzados y así las redes de nueva generación soporten servicios en tiempo real (IBM, 2021).

La IETF ha propuesto algunas propuestas como best effort, servicios integrados (IntServ) y servicios diferenciados (DiffServ).

- **Best effort:** este modelo es el más simple ya que se envía información mediante una aplicación cuando lo desea en cualquier cantidad y sin permisos requeridos lo cual no tiene ninguna garantía de calidad de servicio (QoS).

- **IntServ:** este modelo permite reservar recursos de ancho de banda y el tamaño de cola, utiliza el protocolo RSVP para cierto tráfico, para cada flujo que nentra se definen los recursos de ancho de banda, retardo, jiter los cuales son necesarios la gran limitación de este modelo es almacenar una gran cantidad de datos en cada nodo provocando grande sumas de flujos entre los usuarios finales.
- **DiffServ:** este modelo se basa en que la información de QoS se escribe en los datagramas y no en los enrutadores. Nos va a remitir implementar una QoS escalable a todo tipo y cantidad de flujos.

2.5.4. Aplicación de QoS sobre MPLS y SD-WAN

MPLS

Las redes se construyeron inicialmente para transportar tanto tráfico de voz como de datos. Al no ser sensibles al retardo ni a la pérdida de paquetes, los datos no requieren muchas garantías. Por ejemplo, el tráfico HTTP (Hyper Text Transfer Protocol) y FTP (File Transfer Protocol) no requiere muchas garantías y puede enviarse utilizando modelos de red de mejor esfuerzo. En cambio, la voz requiere una red capaz de transmitir un nivel mínimo de calidad desde el remitente hasta el destino. Sólo se empleaban redes de tráfico en tiempo real para que el envío de voz fuera fiable.

Para dar cabida tanto al tráfico de datos como al de voz (y quizá al de vídeo), las empresas necesitaban desarrollar una infraestructura de red. Para lograrlo, los proveedores de servicios y los consumidores implantaron una red de conmutación de paquetes, que puede enviar tanto tráfico en tiempo real como datos.

Sin embargo, el tráfico en tiempo real se enfrenta a distintos problemas, como el retardo, la pérdida de paquetes y otros factores agravantes, cuando se transmite a través de una red de

conmutación de paquetes. Entonces, si queremos gestionar la voz en redes de conmutación de paquetes, es necesario un sistema de asignación de los recursos necesarios para el tráfico en tiempo real.

Para proporcionar a la voz una calidad de grano fino se utiliza una nueva tecnología llamada Calidad de Servicio con Conmutación Multiprotocolo de Etiquetas.

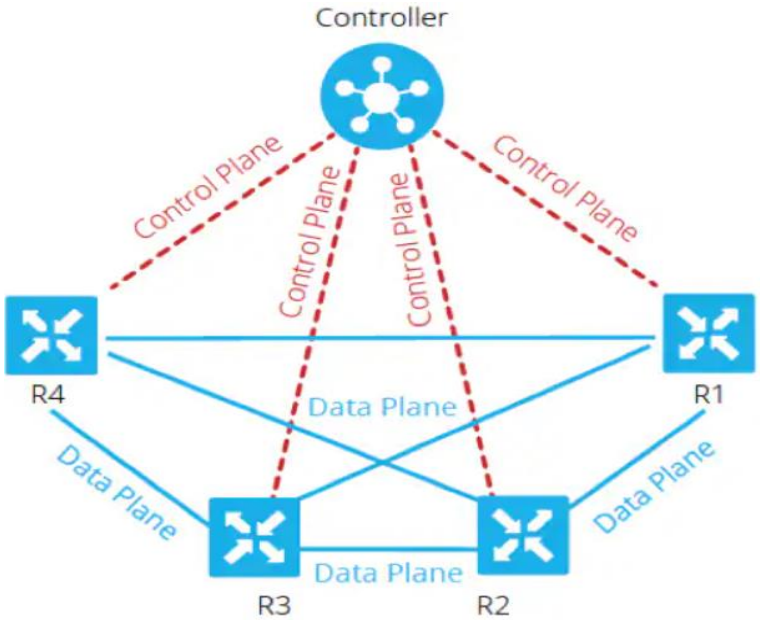
SD-WAN

Como se observa en la Figura 8 cada enrutador anuncia su información local al controlador. Aplicando políticas a cada enrutador local, el controlador central puede manipular fácilmente el flujo de datos.

Aunque un sistema SDN puede aumentar significativamente el ancho de banda a través de una SD-WAN, es necesario dar prioridad al tráfico de cada sistema. Deben ser capaces de dar forma al tráfico, identificarlo y clasificarlo. Además, debe ser capaz de equilibrar la carga en las distintas conexiones de comunicación y controlar las rutas. El rendimiento del tráfico no disminuirá gracias a la corrección de errores de reenvío, y los paquetes llegarán a sus destinos con precisión y a tiempo. Un sistema SD-WAN puede experimentar un tiempo de inactividad considerable si su enrutador de borde no puede ofrecer un grado suficientemente alto de QoS (Jimeno, 2020).

Figura 8

Ejemplo de una red SD-WAN



Nota. La figura muestra una topología en donde el controlador modifica y controla el flujo de tráfico de una forma fácil. Fuente: Cisco (2018).

2.6. Fortinet SD-WAN

Fortinet una de las primeras empresas en combinar muchas tareas en una sola plataforma para la gestión unificada de amenazas. Para proteger completamente sus contenidos, esta plataforma combina antivirus, control de aplicaciones, cortafuegos, VPN, prevención de intrusiones y filtrado web. Desde su creación, se ha hecho un nombre como el proveedor por excelencia de una solución vanguardista y eficaz para la protección de las redes empresariales. Opera con la idea de mantener seguras las redes corporativas de forma coherente, exhaustiva, integrada y automatizada (Lemus, 2020).

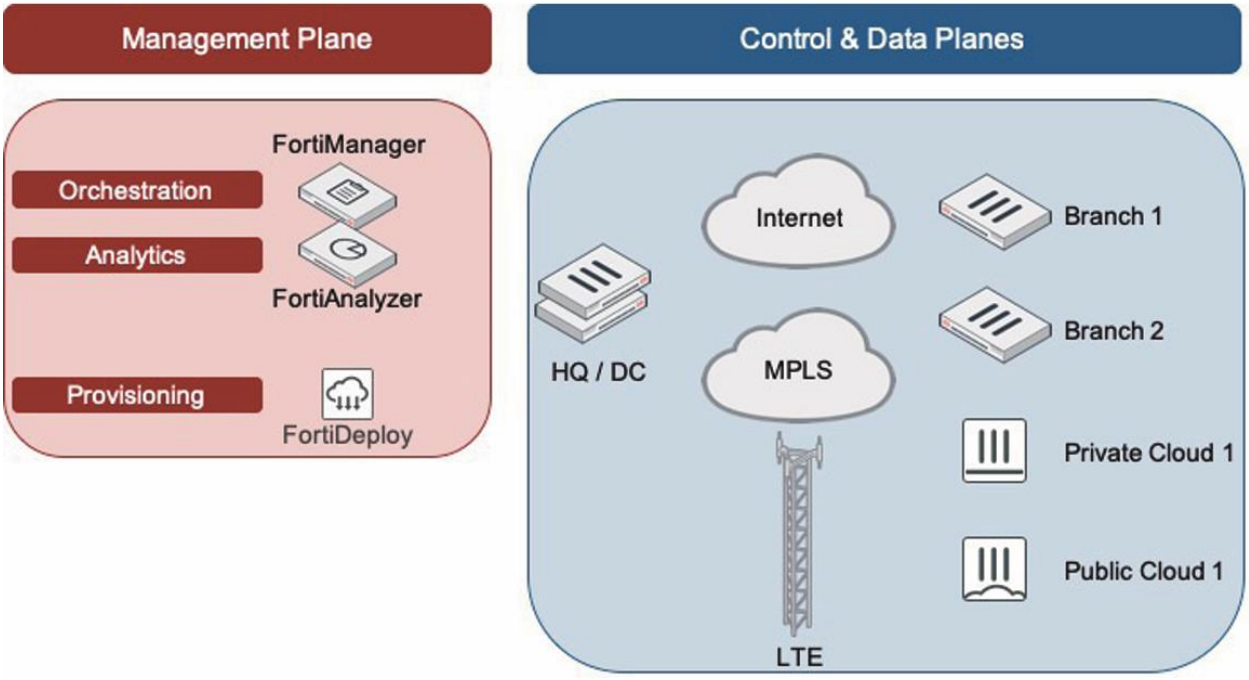
2.6.1. Arquitectura Fortinet SD-WAN

En organizaciones con despliegues pequeños de uno a tres sitios, cada FortiGate puede actuar como plano de gestión, control y datos. Más comúnmente, los despliegues distribuidos

utilizarán el espectro completo de componentes Secure SD-WAN. Tal despliegue dividirá los mismos roles, como se muestra en la Figura 9.

Figura 9

Arquitectura SD-WAN



Nota. La figura muestra los componentes de la arquitectura SD-WAN en donde muestra que es capaz de funcionar de forma autónoma y proporcionar funcionalidad completa. Fuente: Fortinet (2021).

2.6.2. Características FortiGate

La principal plataforma de cortafuegos empresarial de Fortinet se llama FortiGate, y es accesible para muchos tipos de empresas. Esta plataforma puede adaptarse a cualquier entorno empresarial sin sacrificar sus características de seguridad de vanguardia, proporciona una gestión unificada de amenazas con su hardware y software en una plataforma que combina dispositivos de seguridad físicos y virtuales. Estos dispositivos de seguridad llevan a cabo tareas de seguridad como filtrado web, detección de intrusiones, cortafuegos y protección contra spam y virus. La

instalación de FortiGate es una opción disponible para pequeñas, medianas y grandes empresas, así como para centros de datos y proveedores de servicios de Internet.

2.6.3. Características FortiManager

FortiManager ofrece configuración centralizada, directrices de aprovisionamiento, administración de actualizaciones y supervisión de extremo a extremo. Al clasificar los dispositivos y agentes en dominios de gestión geográficos o funcionales, le permite gestionar de forma segura y cómoda entornos enormes. El aprovisionamiento rápido, el seguimiento exhaustivo de parches y las amplias capacidades de auditoría contribuyen a reducir la carga de trabajo de gestión y los gastos operativos. La plataforma ofrece un editor visual centralizado con funciones de arrastrar y soltar que permite crear y modificar rápidamente objetos y políticas, ofrece gestión centralizada de actualizaciones de firmware y contenido de seguridad (Fortinet, 2022).

2.6.4. Características FortiAnalyzer

Para una supervisión eficaz de la red y la gestión de la seguridad, FortiAnalyzer ofrece una serie de herramientas y funcionalidades. Ofrece más de 550 informes en diferentes idiomas, así como gráficos programables, para realizar un seguimiento de los patrones de ataque, promulgar directrices de uso permitido y demostrar el cumplimiento de las políticas. Gracias a su arquitectura escalable, el dispositivo puede funcionar en modo recopilador o analizador, lo que optimiza el procesamiento de los registros. Ofrece servicios de integración web con aplicaciones de terceros a través de Web Services y puede instalarse en entornos virtuales. Para una gestión eficaz, se pueden configurar muchos usuarios de administración con varios perfiles basados en roles (Fortinet, 2022).

CAPÍTULO III: METODOLOGÍA, DISEÑO Y SIMULACIÓN DE RED SD-WAN

En este capítulo 3, la atención se centra en aspectos prácticos del proyecto, ya que se sumerge en la metodología, el diseño y simulación de la red hibrida. También se describe un enfoque sistemático para implementar una solución SD-WAN, incluye consideraciones de diseño, elecciones arquitectónicas y decisiones técnicas, que culminan con la creación de la red hibrida simulada con las herramientas adecuadas, Este capítulo profundiza el proceso de la simulación detallando la configuración de los componentes de red, establecimiento de conexiones seguras, ofreciendo así una visión de la aplicación de los conceptos teóricos tratados anteriormente.

3. Metodología

La metodología por utilizar para el desarrollo del presente proyecto de simulación es el método Top-down, con la finalidad de generar un diseño de red que se enfoque en entender las necesidades del usuario en donde se accede, cambian datos y procesos de una forma ordenada que permitirá analizar los requisitos necesarios, desarrollar, probar, optimizar tanto el diseño lógico como físico y monitorear el rendimiento de la red.

3.1. Descripción General del proyecto

El principal objetivo de la fase de investigación y análisis es adquirir un conocimiento exhaustivo de las tecnologías y mecanismos pertinentes para el proyecto, se examina el funcionamiento del modelo MPLS, así como los fundamentos teóricos de una red de área extensa definida por software (SD-WAN), además, se lleva a cabo un examen exhaustivo de la infraestructura y del hardware necesario para el control del tráfico de red, se examinan las técnicas y modelos de QoS para determinar cuál es el más adecuado para el proyecto, teniendo

en cuenta los servicios concretos que se utilizarán, como VoIP, streaming y hosting, así como el acceso remoto mediante SSL-VPN.

Para elegir el mejor modelo de red a utilizar, se realiza una comparación de los modelos de red SD-WAN y MPLS por esta razón dentro de este capítulo consistirá en 4 fases:

La primera fase consiste en el análisis de requisitos durante este proceso, se lleva a cabo un análisis exhaustivo para determinar los requisitos de hardware y software de la infraestructura de red. Esto incluye la evaluación de los nodos necesarios, sistemas operativos, controladores, componentes de almacenamiento como SSD, RAM, RAM virtual y CPU. Además, se tienen en cuenta los requisitos de virtualización, incluidas la compatibilidad y la escalabilidad.

Se emplea una metodología descendente para garantizar que el diseño de la red se ajusta a las necesidades del usuario, los requisitos de acceso a los datos y los flujos de procesos. Este enfoque permite analizar los requisitos necesarios y facilita el desarrollo, las pruebas y la optimización de los diseños de red lógicos y físicos. Se utilizan herramientas de supervisión del rendimiento como Wireshark, para evaluar métricas de rendimiento de red como ancho de banda, rendimiento, fluctuación, latencia y pérdida de paquetes.

La segunda fase selección de dispositivos implica analizar las opciones de arquitectura de red, como MPLS, SDN y WAN, teniendo en cuenta varios factores que incluyen la capacidad de la red para gestionar múltiples conexiones, monitorizar y optimizar el rendimiento, escalabilidad y flexibilidad, seguridad y facilidad de gestión. Los equipos de Fortinet se tienen en cuenta específicamente durante el proceso de selección de equipos, que abarca enrutadores, conmutadores, controladores y puertas de enlace, la capacidad de los enlaces de red y la gestión de la red son cruciales en una red híbrida MPLS con SD-WAN.

La fase tres consiste en el diseño de la topología de red abarca la arquitectura y el diseño de varios tipos de red, esto incluye la arquitectura y el diseño de la red MPLS, la arquitectura y el diseño de la red SDN, así como la arquitectura de red híbrida que integra capacidades SDN. La topología proporciona redundancia y alta disponibilidad para los nodos SD-WAN, garantizando la prestación continua de servicios incluso en caso de fallos de enlaces o dispositivos. Además, esta etapa implica el despliegue de nodos y servicios como servidores de alojamiento, streaming y VoIP.

La cuarta y última fase pruebas y desarrollo en donde consiste la realización de pruebas iniciales para evaluar la funcionalidad de la red MPLS y su integración con la red SDN para establecer la red híbrida. Se lleva a cabo una supervisión del rendimiento de la conectividad para garantizar conexiones de red fiables y eficientes. El tráfico de red se supervisa continuamente para identificar y solucionar cualquier problema de congestión o rendimiento. Además, se utilizan herramientas de supervisión de red para evaluar el rendimiento de la red en función de métricas predefinidas.

3.2. Etapa 1: Análisis de requerimientos

Mediante el análisis de los requerimientos que se implementarán en el proyecto, así como servicios y topología en donde se plantea un ambiente híbrido SD-WAN/MPLS que tendrá como fin realizar pruebas correspondientes a métricas de rendimiento de redes.

3.3. Análisis de Situación Actual

Antes de cambiar de un entorno MPLS estándar a una solución SD-WAN, hay que tener en cuenta una serie de aspectos. La conexión en la nube sin fallas y el rendimiento de aplicaciones de alta velocidad que ofrece SD-WAN son características de las que realmente carece MPLS, lo que convierte a SD-WAN en una alternativa deseable. Pero muchos

proveedores de SD-WAN siguen sin tener un componente de seguridad real, lo que deja a las empresas vulnerables a nuevas amenazas. En comparación con los proveedores que no incluyen seguridad en su solución SD-WAN, MPLS ofrece un mayor nivel de protección porque devuelve el tráfico al centro de datos.

MPLS es una tecnología bien establecida que proporciona un rendimiento fiable y constante. Sin embargo, es una tecnología cara, sobre todo para las conexiones con el extranjero. Una tecnología más reciente llamada SD-WAN proporciona más escalabilidad y flexibilidad a un precio reducido. Sin embargo, su rendimiento puede ser menos fiable que el de MPLS, es posible que desee utilizar MPLS para conectar a su red un servidor de alojamiento que es esencial para las operaciones de una empresa y se utiliza SD-WAN para servicios adicionales como VoIP o streaming. Para lo cual se realizó primero la prueba de rendimiento de dispositivos a utilizar para obtener los requerimientos en la plataforma de GNS3 en donde primeramente la página oficial de la herramienta nos muestra los requerimientos óptimos para utilizarla como son:

Tabla 1.

Requerimientos para usar la herramienta de simulación GNS3

Ítem	Requerimiento óptimo
Sistema Operativo	Windows 10, Ubuntu 22.04
Procesador	Core i7, i9 Intel CPU R7 o R9 AMD CPU 4 o más núcleos lógicos
Virtualización	Habilitar en Bios
Memoria	16GB a 32 GB de RAM
Espacio en disco	80GB

3.3.1. Requerimientos de sistema

Previo al análisis de la SD-WAN, en la Tabla 2 se describen los recursos que serán utilizados para la instalación del software y manejo óptimo de recursos son los siguientes:

Tabla 2

Requerimientos de sistema a utilizar para la simulación

Requerimiento	Descripción
Memoria RAM	24 GB
Disco Duro	450 GB
Procesador	Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
Servidores	Hosting, Streamming, VoIp, FTP.

Nota. En la tabla se muestra requisitos de hardware y software. Fuente: Elaboración propia

3.3.2. Requerimientos de funcionalidad de red

En esta parte se procede a la elección del controlador basado en las normas ISO/IEC/IEEE 29148:2018 y MEF 70. En la Tabla 3 se presentan los requerimientos funcionales que debe cumplir el controlador adecuado para el presente proyecto. Se valora con un puntaje de 1 a 3, en donde 3 es la más alta y 1 el más bajo para ser elegido. Cero hace referencia a que no cumple con la especificación de software (SRS) dentro de sus prestaciones. Aquel que posee un valor mayor dentro de la puntuación total es el más ideal para trabajar.

Tabla 3

Requerimientos de especificación de software de la controladora

		Prioridad			
Nro.	**Requerimiento**	ONOS	RYU	ODL	FLDL
SRS1	Gestión de topología de red	3	3	3	2
SRS2	Soporte de protocolos de enrutamiento	3	2	3	1
SRS3	Gestión de políticas de QoS	3	2	3	1
SRS4	Seguridad	3	2	3	1
SRS5	Escalabilidad	3	2	3	1
SRS6	Monitoreo y diagnóstico de red	2	2	2	1
SRS7	Alto rendimiento para investigación y desarrollo de pruebas	2	2	2	1
SRS8	Soporte del protocolo OpenFlow	3	3	3	3
	TOTAL	22	18	22	11

Nota. En la tabla se muestra requerimientos de la controladora los cuales serán los ideales para la red híbrida. Fuente: Elaboración propia

A continuación, en la Tabla 4 se presentan requerimiento que son necesarios para evaluar los controladores.

Tabla 4

Requerimientos para el desarrollo y levantamiento del controlador

		Prioridad			
Nro.	**Requerimiento**	ONOS	RYU	ODL	FLDL
SRS9	Lenguaje de programación	3	3	3	2
SRS10	Documentación disponible	3	3	3	3

SRS11	Facilidad de instalación	3	3	2	1
SRS12	Actualizaciones	3	3	3	3
SRS13	Simplicidad de uso	3	2	2	3
	TOTAL	15	14	13	12

Como se observa en las tablas de valoración gracias a su integración con MPLS, su sólida gestión de políticas y sus funciones de seguridad, ONOS es una gran opción para SD-WAN híbrida con MPLS. También ofrece una amplia funcionalidad, escalabilidad, alto rendimiento, soporte activo de la comunidad y una interfaz intuitiva. La flexibilidad, el énfasis en la comunidad y la facilidad de uso son otras posibles ventajas sobre ONOS.

3.3.3. Análisis de métricas de rendimiento de redes

El análisis de métricas de rendimiento de redes es un proceso fundamental para comprender el rendimiento actual de la red e identificar áreas de mejora. Las métricas de rendimiento se utilizan para medir el rendimiento de la red en términos de velocidad, latencia, pérdida de paquetes y otros factores.

El análisis de métricas de rendimiento puede ayudar a las organizaciones a:

- Identificar problemas de rendimiento
- Evaluar el impacto de los cambios en la red
- Planificar el crecimiento de la red

3.3.3.1. Métricas de rendimiento de redes

Una tecnología de red llamada MPLS permite ofrecer un servicio de red privada de alto rendimiento en varias zonas geográficas. Mientras que SD-WAN proporciona un enfoque flexible de la conectividad, MPLS hace hincapié en los servicios de red privada, y ambas

tecnologías se centran en maximizar la eficiencia de la red. Los indicadores de rendimiento de estas tecnologías incluyen variables como el rendimiento, la pérdida de paquetes y la latencia.

Tabla 5

Métricas MPLS

Indicador	Descripción
Ancho de banda	Factor esencial para el rendimiento óptimo de la red, los clientes pueden seleccionar diferentes opciones de ancho de banda según sus necesidades.
Latencia	Importante para aplicaciones en tiempo real como VoIP o videoconferencia. Una alta latencia puede afectar la calidad de estas aplicaciones.
Jitter	Crucial para aplicaciones de tiempo real, evita distorsiones en el sonido o la imagen. Se busca un jitter bajo para un rendimiento óptimo.
Pérdida de paquetes	Puede deberse a diversos factores y afectar negativamente el rendimiento de aplicaciones y la experiencia del usuario.
Disponibilidad	La capacidad de la red para estar en funcionamiento y proporcionar servicios de manera continua y confiable. Esencial en redes MPLS con SLA garantizado.

3.3.4. Análisis de herramientas de rendimiento de red

Selección del simulador de topología de red, para este proyecto de desarrollo de una red de área extensa basada en una arquitectura definida por software SD-WAN, adaptada a un modelo MPLS e implementando políticas de calidad de servicio (QoS) para el análisis del

rendimiento de una red híbrida, se ha seleccionado GNS3 como el simulador de red principal. La elección de GNS3 se fundamenta en varias razones clave que lo hacen idóneo para este propósito.

GNS3 se ha elegido el simulador de red para este proyecto debido a su flexibilidad, capacidad para representar dispositivos de red reales y la posibilidad de integrar múltiples tecnologías que nos permitirán diseñar, implementar y analizar una red híbrida SD-WAN y MPLS con políticas de QoS para garantizar un rendimiento óptimo y una experiencia satisfactoria para los usuarios.

Además de las métricas de rendimiento mencionadas anteriormente, hay varias herramientas de rendimiento de redes disponibles que pueden ayudar a medir el rendimiento de las redes y solucionar problemas de rendimiento. Algunas de estas herramientas incluyen:

Herramienta	**Descripción**
SNMP	Protocolo estándar para administrar y supervisar dispositivos de red. Permite recopilar datos de rendimiento como ancho de banda, latencia y utilización de CPU.
Ping	Herramienta para probar la conectividad y medir la latencia. Envía paquetes de datos a un destino y mide el tiempo de respuesta.
Traceroute	Utilidad para medir la ruta de los paquetes de datos a través de la red. Rastrea el camino que toman los paquetes hasta su destino.
IPERF	Herramienta para medir el ancho de banda y la tasa de transferencia de datos. Capaz de generar tráfico para realizar pruebas de rendimiento.

3.4. Etapa 2: Selección de dispositivos

La selección de equipos para una red híbrida MPLS con SD-WAN es un proceso importante para garantizar el éxito de una implementación de red eficiente y segura. Así que dentro de la etapa 2 se analiza la red híbrida a simular.

Por un lado, MPLS es una tecnología de red tradicionalmente utilizada para proporcionar conectividad confiable y segura en redes empresariales, mientras que SD-WAN (Software-Defined Wide Area Network) es una tecnología de red emergente que utiliza software y virtualización para mejorar el rendimiento y la agilidad de la red. La implementación de una red híbrida MPLS con SD-WAN puede combinar lo mejor de ambas tecnologías, proporcionando una conectividad de alta calidad para aplicaciones críticas de la empresa mientras se mejora la eficiencia y la flexibilidad de la red para aplicaciones en la nube y móviles.

Algunos de los factores clave que deben considerarse al seleccionar equipos para una red híbrida MPLS con SD-WAN incluyen la capacidad de gestionar múltiples conexiones de red, la capacidad de monitorear y optimizar el rendimiento de la red, la escalabilidad y flexibilidad de la red, la seguridad de la red y la facilidad de gestión.

Es importante trabajar con un proveedor de servicios de red de confianza y con experiencia para garantizar la selección de los equipos adecuados y una implementación eficaz de la red híbrida MPLS con SD-WAN.

3.4.1. Análisis de la arquitectura de red

La arquitectura de una red híbrida MPLS con SD-WAN combina dos tecnologías de red para proporcionar una conectividad confiable y segura para aplicaciones críticas de la empresa,

mientras se mejora la eficiencia y la flexibilidad de la red para aplicaciones en la nube y móviles. A continuación, se presenta un análisis de la arquitectura de la red híbrida:

Tabla 6

Arquitectura de red

Elemento	Descripción
Red MPLS	Proporciona conectividad segura y confiable para aplicaciones críticas. Utiliza etiquetas para enrutar el tráfico y mejorar el rendimiento y la seguridad.
Red SD-WAN	Red de área amplia virtualizada que optimiza el rendimiento utilizando múltiples conexiones de red, incluyendo banda ancha y 4G/LTE.
Dispositivos	Incluyen routers, switches, controladores y gateways para gestionar la conexión entre las redes MPLS y SD-WAN y optimizar el rendimiento y la seguridad.
Gestión de la red	Es crucial para garantizar una conectividad confiable y segura. Incluye monitorización, mantenimiento, implementación de políticas de seguridad y QoS.

La arquitectura de una red híbrida MPLS con SD-WAN combina la conectividad segura y confiable de la red MPLS con la eficiencia y la flexibilidad de la red SD-WAN para proporcionar una solución de red escalable, segura y de alto rendimiento. La implementación de una red híbrida MPLS con SD-WAN puede mejorar significativamente la eficiencia y la agilidad

de la red de una empresa al mismo tiempo que se proporciona una conectividad de alta calidad para aplicaciones críticas de la empresa.

3.4.2. Selección de equipos

Para el equipamiento hemos tenido en cuenta realizar el proyecto con dispositivos Fortinet por lo que hemos realizado un análisis previo de versiones y donde hemos tomado las siguientes:

FortiOS 7 es el sistema operativo utilizado dentro de la seguridad de los sistemas de red de Fortinet, como son los firewalls. Esta versión de FortiOS es específicamente adecuado para SD-WAN, que es proporcional a varias características importantes que son útiles para los siguientes tipos, incluyendo:

Soporte mejorado para conexiones WAN multiproveedor, que permite una mayor flexibilidad en la elección de proveedores de servicios y aumenta la redundancia de redundancia.

Capacidades mejoradas de calidad de servicio (QoS) y priorización del tráfico, que pueden ser útiles en redes SD-WAN para garantizar que las aplicaciones críticas tengan un rendimiento constante y predecible.

Capacidades avanzadas de enrutamiento que pueden ayudar a optimizar el tráfico de red y reducir la latencia.

Integración con otras herramientas de seguridad de Fortinet, lo que permite una fuerte protección contra las amenazas a la seguridad de la red.

Está diseñado para gestionar grandes volúmenes de tráfico de red, lo que lo hace adecuado para organizaciones de todos los tamaños.

Se integra con una amplia gama de productos de red y seguridad de terceros, lo que facilita su despliegue en las redes existentes.

3.5. Etapa 3: Diseño de topología de red

En la etapa 3 del proyecto, nos enfocaremos en el diseño de la topología de red para nuestra red híbrida basada en una arquitectura SD-WAN adaptada a un modelo MPLS, con la implementación de políticas de calidad de servicio (QoS). En esta fase, utilizaremos la plataforma GNS3 para simular y configurar los dispositivos de red necesarios, como routers y switches, para representar tanto la red SD-WAN como la red MPLS. La topología diseñada incluirá enlaces de conexión a través de Internet y la red MPLS, que simbolizarán las comunicaciones entre las diferentes sucursales de la empresa. Se establecerán los túneles IPSec y VPN para garantizar la confidencialidad y autenticidad de los datos transmitidos.

3.5.1. Diseño de la red híbrida

En primer lugar se realizó un bosquejo en un programa de diagrama como se representa en la Figura 10, por consiguiente a continuación se establecen los lineamientos de MPLS, políticas, reglas y otros aspectos relacionados con la funcionalidad de la red, con el objetivo de entender su funcionamiento antes de ser emulada. Luego, se procede a realizar la configuración de cada dispositivo, y se proporciona información detallada acerca de los recursos necesarios para instalar y utilizar el software GNS3 y su máquina virtual.

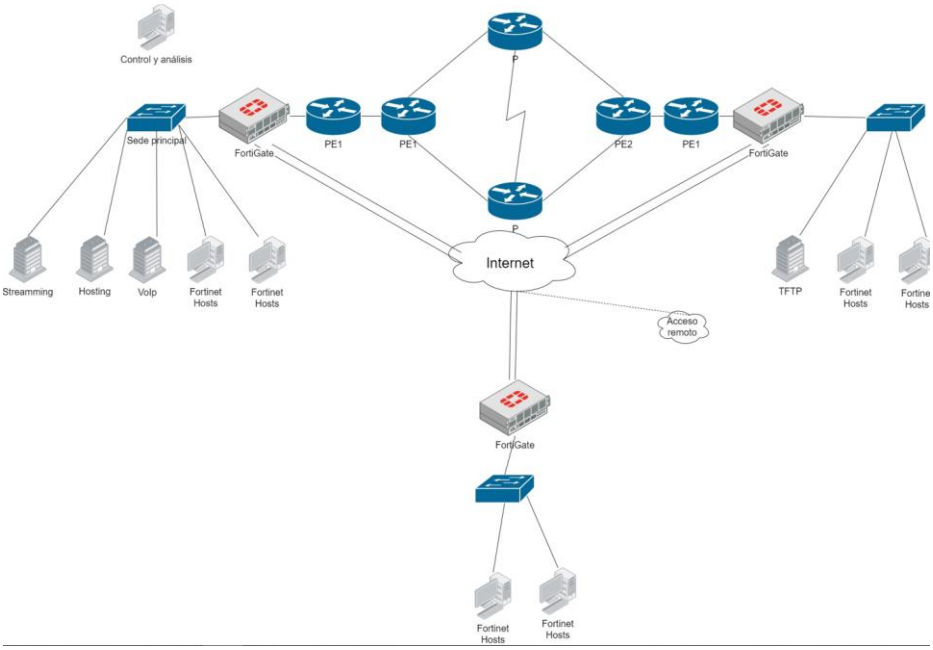
GNS3 es un emulador de redes que cuenta con múltiples funcionalidades y dispositivos virtuales de diferentes fabricantes, lo que permite a los profesionales en redes y telecomunicaciones prevenir errores y evitar la compra innecesaria de dispositivos en una implementación real. La elección de GNS3 se basó en tres factores principales: su naturaleza de código abierto, su capacidad para emular topologías complejas, y su disponibilidad tanto para Windows como para Linux.

La arquitectura de la red está compuesta por tres LAN (Redes de Área Local) ubicadas en diferentes locaciones, cada una con un papel específico. La LAN 1 actúa como sede principal y cuenta con 3 servidores, a los cuales necesitan acceder las otras dos LAN. La LAN 2 será utilizada como centro de datos y cuenta con 1 servidor, mientras que la LAN 3 es una sucursal que requiere acceso a los recursos y servidores de las otras dos LAN. Además, se implementa una red MPLS que representa la infraestructura de red tradicional de una empresa, para demostrar la viabilidad de utilizar la infraestructura MPLS junto con SD-WAN. Es importante mencionar que la LAN 3 no se conectará a la MPLS para comprobar el desempeño de la solución SD-WAN, lo que resultará en dos escenarios distintos durante la simulación.

Finalmente, se define el direccionamiento IP y se explica detalladamente el funcionamiento de cada una de las redes de área local y extendida, incluyendo información acerca de los dispositivos internos que las componen.

Figura 10

Diseño de red



Nota: La figura muestra una topología en se encuentra el diseño de red hibrida a utilizar. Fuente: Elaboración propia

3.5.2. Servidores para pruebas

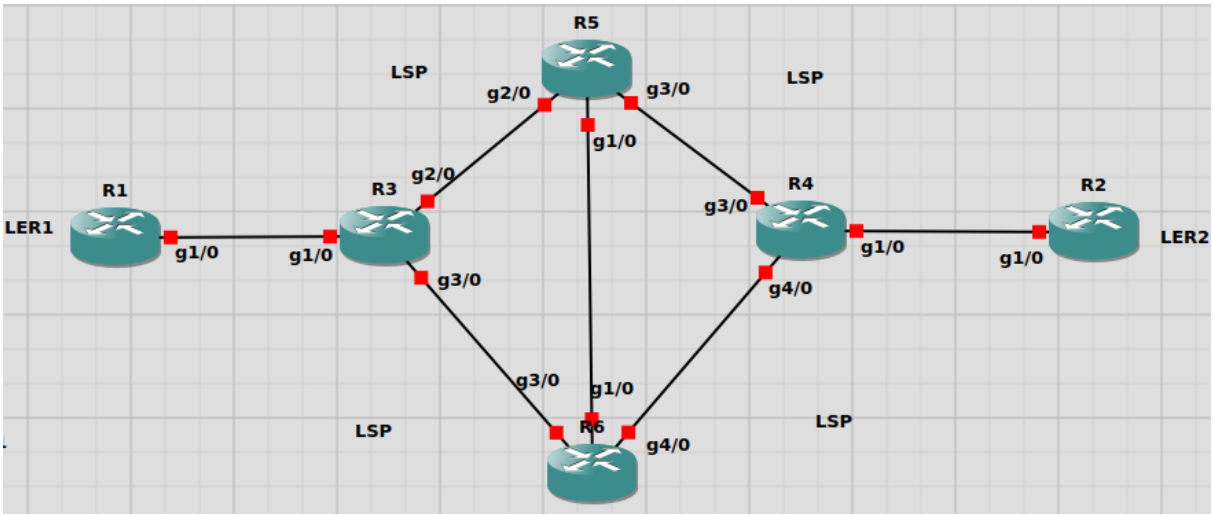
Para llevar a cabo las pruebas y evaluaciones en este punto del proyecto, requeriremos el uso de servidores especializados para simular diferentes escenarios y aplicaciones de nuestra red híbrida. Estos servidores desempeñarán un papel crucial para medir el rendimiento, la calidad de servicio y la eficacia de nuestra solución.

3.5.3. Implementación de MPLS

La infraestructura de red MPLS como se muestra en la figura 11 ha sido implementada con el objetivo de interconectar la sede principal LAN1 con el Centro de Datos LAN2. La red MPLS está compuesta por 6 routers, dos LER (Label Edge Routers), que actúan como los routers de borde de la red MPLS. El primer nodo SD-WAN está conectado al primer LER (LER1) y el segundo nodo SD-WAN está conectado al segundo LER (LER2). Entre LER1 y LER2, hay cuatro routers adicionales, dos de los cuales (LSR1 y LSR2) están directamente conectados a ambos LER y actúan como LSR (Label Switching Routers), mientras que el tercer router (LSR3) está conectado a LSR1 , LSR2 y LSR4 también actúa como un LSR, mientras que el cuarto router (LSR4) está conectado a LSR1 , LSR2 y LSR 3 también actúa como un LSR. Cada LSR tiene su propia LSP (Label Switched Path) configurado para enrutar los paquetes etiquetados a través de la red MPLS y garantizar la calidad de servicio (QoS) para aplicaciones críticas

Figura 11

Simulación de diseño de una red mpls



Nota: Se muestra en la figura el diseño de una red MPLS. Fuete: Elaboración propia

El protocolo de enrutamiento utilizado es Open Shortest Path First (OSPF), el cual es un protocolo de Estado de Enlace que proporciona a todos los equipos una visión completa de toda la red, realiza actualizaciones únicamente al detectar cambios en la red y emplea mejores métricas en comparación con los protocolos Vector-Distancia. OSPF no tiene limitación en cuenta de saltos y su base de datos se utiliza para construir un árbol con los enlaces de menor costo. En caso de existir más de una ruta con igual costo, la política es distribuir el tráfico de manera balanceada.

En la red MPLS, los dispositivos FortiGate actúan como Customer Edge Routers, de tal manera que la conmutación multiprotocolo de etiquetas está habilitada solamente en las interfaces direccionadas a los PE o P routers y no en las dirigidas a los equipos FortiGate.

La red MPLS debe funcionar en conjunto con la SD-WAN, de tal manera que, de acuerdo con los requerimientos o necesidades, la red automáticamente escogerá la mejor ruta para enviar el tráfico hacia las distintas oficinas remotas. Es importante mencionar que la configuración de cualquier parámetro o aspecto interno de la red MPLS se deberá realizar específicamente en cada

uno de los routers de la red, ya que es una infraestructura totalmente independiente a la SD-WAN.

Este conjunto de comandos configura el router R1_LER1 para que pueda enrutar tráfico en una red OSPF y BGP y configurar MPLS con RSVP y tráfico de ingeniería. También establece la autenticación de SSH, una contraseña de usuario y el banner de bienvenida.

Se configura la interfaz g1/0 con una dirección IP y se activa con "interface g1/0", "ip address 172.16.10.1 255.255.255.252" y "no shutdown". Luego se configura OSPF con el router-id 1.1.1.1, la red 172.16.10.0/30 y el área 0.

Después, se configura BGP con el AS 100, el vecino 172.16.10.6, la fuente de actualización Loopback0, el cliente del reflector de ruta y la red 10.0.0.0/24. Se activa el vecino con "neighbor 172.16.10.6 activate".

A continuación, se habilita RSVP con "ip rsvp bandwidth" y se configura una interfaz de loopback con la dirección IP 1.1.1.1/32.

Después, se configura MPLS con LDP, IP CEF y tráfico de ingeniería. Se habilita el tráfico de ingeniería.

3.5.4. Servidores para pruebas

Para llevar a cabo las pruebas y evaluaciones de nuestro proyecto, requeriremos el uso de servidores especializados para simular diferentes escenarios y aplicaciones de nuestra red híbrida. Estos servidores desempeñarán un papel crucial para medir el rendimiento, la calidad de servicio y la eficacia de nuestra solución.

3.5.5. Cálculo de ancho de banda de servicios

Para caracterizar una clase, se asigna ancho de banda, peso y máxima longitud de transmisión del paquete, el ancho de banda asignado a una clase es garantizado durante períodos de congestión. La suma de los anchos de banda no debe superar el 75% del disponible, dado que el restante se usa para información de control

Para la VoIP:

Utilizaremos la fórmula de cálculo del ancho de banda de VoIP de acuerdo con los RFC 3550 y 7711 con el códec G.711:

Ancho de banda = (Cantidad de llamadas simultáneas) x (Cantidad de paquetes por segundo por llamada) x (Tamaño del paquete) x (Overhead).

Para calcular el ancho de banda necesario para una llamada de VoIP que utiliza el códec G.711, se deben considerar varios factores:

- Tamaño del paquete: El tamaño típico de un paquete de voz utilizando el códec G.711 es de 160 bytes.
- Tasa de muestreo: El códec G.711 utiliza una tasa de muestreo de 8 kHz.
- Compresión: El códec G.711 no utiliza compresión.

Para una llamada de voz utilizando el codec G.711, se utiliza un canal, por lo que el número de canales es igual a 1. Por lo tanto, el ancho de banda necesario para una llamada de voz utilizando el codec G.711 como en la ecuación 1:

Ancho de banda = tamaño del paquete * tasa de muestreo * número de canales (1)

$$Ancho\ de\ banda = 160\ bytes * 8000 \frac{muestras}{s} * 1\ canal$$

$$Ancho\ de\ banda = 128kbps * llamadas\ simultaneas$$

$$Ancho\ de\ banda = 128kbps * 3$$

$$Ancho\ de\ banda = 0.384\ Mpbs$$

Para la Web:

Según un estudio de HTTP Archive, el tamaño promedio de una página web en 2021 es de alrededor de 2.23 MB por lo tanto mediante la ecuación 2 podremos observar el ancho de banda necesario:

$$Ancho\ de\ banda\ = \frac{Tamaño\ del\ archivo}{Tiempo\ de\ descarga} * Usuarios\ simultáneos \quad (2)$$

Utilizaremos el valor promedio de tamaño de página web, que investigamos anteriormente en la ecuación 3:

$$Ancho\ de\ banda\ = \frac{2.23Mb}{5\ s} * 5 \quad (3)$$

$$Ancho\ de\ banda\ = 17{,}48\ Mbps$$

Para el FTP/TFTP:

Para calcular el ancho de banda necesario para la transferencia de archivos a través de FTP, podemos utilizar la siguiente fórmula que se muestra en la ecuación 4:

$$Ancho\ de\ banda\ = \frac{Tamaño\ del\ archivo}{Tiempo\ de\ transferencia} * Usuarios\ simultáneos \quad (4)$$

Tamaño promedio de archivo transferido = 20 MB

Cantidad de usuarios simultáneos = 5

Tiempo de transferencia promedio = 100 segundos (valor estimado)

$$Ancho\ de\ banda\ = \frac{20Mb}{100s} * 5$$

$$Ancho\ de\ banda\ = 8\ Mbps$$

Para el streaming:

Tomando como referencia una resolución de video de 720p, una tasa de bits de 2 Mbps y con un número estimado de 5 espectadores simultáneos, se puede calcular el ancho de banda necesario de la siguiente manera como se muestra en la ecuación 5:

$$Ancho\ de\ banda\ = tasa\ de\ bits\ x\ número\ de\ espectadores \quad (5)$$

$$Ancho\ de\ banda = \ 2Mpbsx\ 5$$

$$Ancho\ de\ banda = 10Mbps$$

3.5.6. Implementación de SD-WAN

Cuando se combina con una red MPLS ya existente, SD-WAN se convierte en una herramienta extremadamente útil porque estas dos tecnologías funcionan en perfecta armonía. Gracias a esta interoperabilidad, las conexiones públicas a Internet pueden añadirse fácilmente a la infraestructura de red a un coste mucho menor que con MPLS, utilizando diferentes transportes IP como DSL, cable o fibra. El uso de estos enlaces públicos de Internet de bajo coste para priorizar sobre ellos el tráfico de menor prioridad permite a SD-WAN gestionar eficazmente los recursos de la red. En esencia, la WAN conectada a Internet se convierte en una extensión asequible con la ayuda de los dispositivos FortiGate colocados entre las LAN 1, 2 y 3. Para aplicaciones importantes en el emplazamiento principal LAN1, basta con una línea de banda ancha, lo que garantiza un tiempo de actividad suficiente. Por otro lado, el centro de datos LAN2 aprovecha sus múltiples conexiones de banda ancha, aunque depende de MPLS para la conectividad a Internet desde el sitio principal. Para reducir la latencia y garantizar una comunicación continua, LAN3 a nivel de sucursal utiliza enlaces de banda ancha redundantes, lo que subraya la solidez de SD-WAN a la hora de preservar la conectividad de la red. Al eliminar

el requisito de circuitos MPLS propietarios entre sucursales, el enfoque descentralizado de SD-WAN promueve un diseño de red seguro y conectado a través de Internet abierto. La capacidad de ver todas las conexiones a Internet en todas las ubicaciones pone de relieve la adaptabilidad de las implantaciones de SD-WAN, que pueden acomodar diferentes soluciones de transporte IP en función de las necesidades y preferencias de la empresa. Independientemente del medio de transporte seleccionado, esta flexibilidad garantiza una sólida conectividad de red, impulsando así la eficacia y fiabilidad de la arquitectura de red.

Configurar los dispositivos SD-WAN. Los dispositivos SD-WAN deben estar configurados con las siguientes configuraciones básicas:

Dirección IP y máscara de subred

Gateway predeterminado

Nombre de dominio

Configuración de seguridad (firewall, VPN, etc.)

Conectar los dispositivos SD-WAN a la red MPLS. Los dispositivos SD-WAN deben estar conectados a la red MPLS a través de interfaces físicas o virtuales.

Configurar la conectividad entre los dispositivos SD-WAN. Los dispositivos SD-WAN deben estar configurados para comunicarse entre sí. Esto se puede hacer utilizando un protocolo de enrutamiento, como OSPF o BGP.

Configurar la conectividad a Internet. Un dispositivo SD-WAN debe estar configurado para conectarse a Internet. Esto se puede hacer utilizando una conexión Ethernet, una conexión inalámbrica o una conexión de terceros.

En este caso, los dos nodos SD-WAN que se conectarán a la red MPLS son los siguientes:

- Nodo SD-WAN 1: Se conectará al LER1 a través de la interfaz física WAN1.
- Nodo SD-WAN 2: Se conectará al LER2 a través de la interfaz física WAN2.
- El tercer nodo SD-WAN se conectará a Internet a través de la interfaz física WAN3.

Con el fin de crear una infraestructura de red unificada entre los diferentes nodos de la organización, la arquitectura SD-WAN debe contar con líneas MPLS, enlaces de acceso a Internet y túneles o VPN. Curiosamente, cada uno de estos elementos -aparte de la red de acceso remoto gestionada por VPN- se integra fácilmente en la arquitectura SD-WAN. La complejidad y la interdependencia de estas redes dentro del sistema FortiGate en la sede central se capturan en la Figura 12. El objetivo principal es proporcionar una comunicación sin restricciones entre redes situadas en LAN separadas y proporcionar una gestión y un control centralizados a través de la plataforma FortiManager. Mediante la aplicación de reglas o políticas predeterminadas, esta orquestación crea un entorno de red automatizado, centralizado e inteligente que está preparado para mejorar el rendimiento de los enlaces. Estos principios cuidadosamente delineados a continuación controlan cómo se comporta la red, asegurando que los recursos se utilicen de la manera más eficiente posible y que pueda adaptarse a las cambiantes necesidades operativas. Curiosamente, las configuraciones de FortiGate en la sucursal y datos como se muestra en la Figura 13, 14 son idénticas a las de la sede central, con la excepción de que sus arquitecturas SD-WAN tienen enlaces conectados directamente. La escalabilidad y versatilidad de la solución SD-WAN destacan por su diseño y funcionamiento uniforme, que permite a las empresas ampliar sus capacidades de red a través de diversos sitios con facilidad y mantener paradigmas de gestión estándar.

Figura 12

SD-WAN LAN 1 Principal

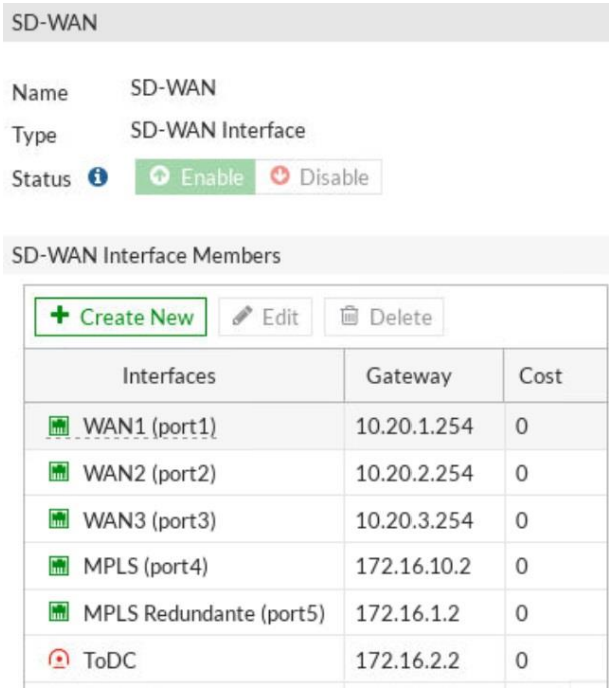


Figura 13

SD-WAN LAN 2 Datos

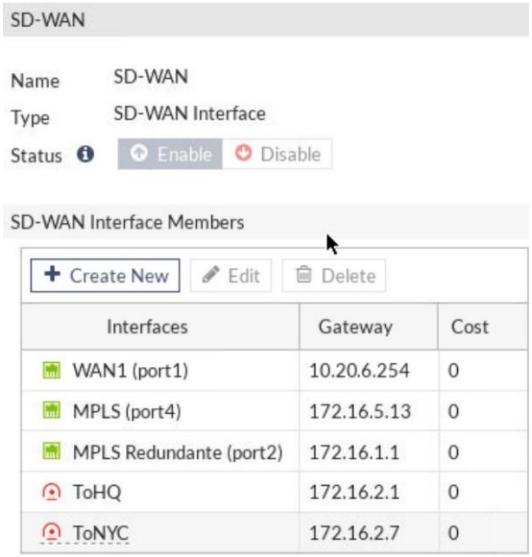
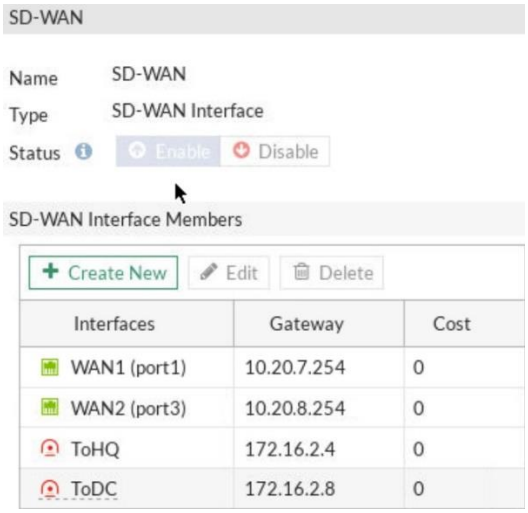


Figura 14

SD-WAN LAN 1 Sucursal



En lo que respecta a las VPN, Internet Protocol Security (IPSec) y Secure Sockets Layer (SSL) son los dos protocolos de tunelización más populares. La elección del protocolo detunelización depende de las especificaciones de seguridad y de los casos de uso particulares. En este caso, la empresa da prioridad a las medidas de seguridad sólidas y utiliza selectivamente túneles IPSec para las conexiones internas entre la oficina central, el centro de datos y la sucursal. Por otro lado, SSL-VPN, que es bien conocida por su facilidad de uso a través del navegador sin necesidad de descargar más software, se dirige específicamente al acceso remoto de los usuarios a través de Internet, proporcionando conectividad a las personas que trabajan fuera de las ubicaciones físicas de la empresa.

La arquitectura de red de la organización incluye túneles IPSec cuidadosamente diseñados para proporcionar una comunicación segura y fluida. En la sede central se crean dos VPN independientes: "ToDC", que es la VPN para el Centro de Datos, y "ToNYC", que es la VPN para la sucursal. De forma similar, se crean dos VPN dentro del centro de datos: "ToHQ" para la conectividad de la oficina central y "ToNYC" para la conectividad de la sucursal. Del mismo modo, la sucursal mantiene actualizadas dos VPN: "ToHQ" para la comunicación con la

sede central y "ToDC" para la conectividad con el centro de datos. La infraestructura VPN de la empresa es resistente y redundante gracias a su compleja topología de red, que garantiza una conectividad continua entre sus nodos organizativos dispersos.

A través de una cuidadosa planificación e implementación de los despliegues VPN, la organización protege su red de posibles brechas de seguridad y promueve una conexión sin fisuras entre sus distintas ubicaciones. Esta alineación estratégica de configuraciones de túneles y protocolos VPN pone de manifiesto la dedicación de la empresa a mantener una infraestructura de red sólida y resistente que pueda satisfacer sus necesidades operativas al tiempo que protege las transmisiones de datos confidenciales como se observa en la Figura 15.

Figura 15

IPSec-VPN de la red

Tunnel	Interface Binding	Status	Ref.
Custom 2 HQ			
ToDC	WAN1 (port1)	Inactive	2
ToNYC	WAN1 (port1)	Inactive	2
Custom 2 DC			
ToHQ	WAN1 (port1)	Inactive	2
ToNYC	WAN1 (port1)	Inactive	2
Custom 2 BO			
ToDC	WAN1 (port1)	Inactive	2
ToHQ	WAN1 (port1)	Inactive	2

Por el contrario, SSL-VPN se convierte en un canal crucial a través del cual los clientes pueden acceder a los servicios empresariales en línea, lo que supone una revolución en cuanto a facilidad de uso y accesibilidad. El uso deliberado de SSL-VPN se debe a su compatibilidad nativa con los navegadores web más utilizados, como Firefox y Google Chrome, lo que elimina la necesidad de laboriosas instalaciones de software y simplifica el acceso tanto para los clientes como para el personal. Pero esta facilidad de uso no está exenta de un coste; la simplicidad intrínseca de SSL-VPN la hace más vulnerable a los fallos de seguridad, una preocupación que debe equilibrarse cuidadosamente con el requisito de una accesibilidad sin problemas. Sin

embargo, la elección de adoptar SSL-VPN también se apoya en un análisis cuidadoso de los tipos de servicios a los que podrían acceder los clientes. En este caso, la mayoría de los usuarios de VPN

Dentro de la arquitectura SSL-VPN se distinguen dos despliegues distintos para atender las diferentes necesidades de acceso a servicios de los distintos nodos de la organización. En la sede central se instala una pasarela SSL-VPN que permite a los usuarios acceder a recursos vitales, como servidores DNS y TFTP. Al mismo tiempo, el centro de datos establece una arquitectura SSL-VPN paralela que permite el acceso al servidor de correo electrónico desde cualquier lugar. La dedicación de la empresa a promover la accesibilidad universal queda demostrada por este diseño SSL-VPN dividido, que también demuestra una sofisticada estrategia para coordinar las precauciones de seguridad con los requisitos de prestación de servicios. La infraestructura SSL-VPN aparece como un pilar en el esfuerzo de la organización por lograr el mejor equilibrio posible entre accesibilidad y seguridad, ya que trabaja a través de las complejidades del aprovisionamiento de acceso remoto, proporcionando el marco para una mayor eficiencia.

3.6. Etapa 4: Desarrollo de pruebas

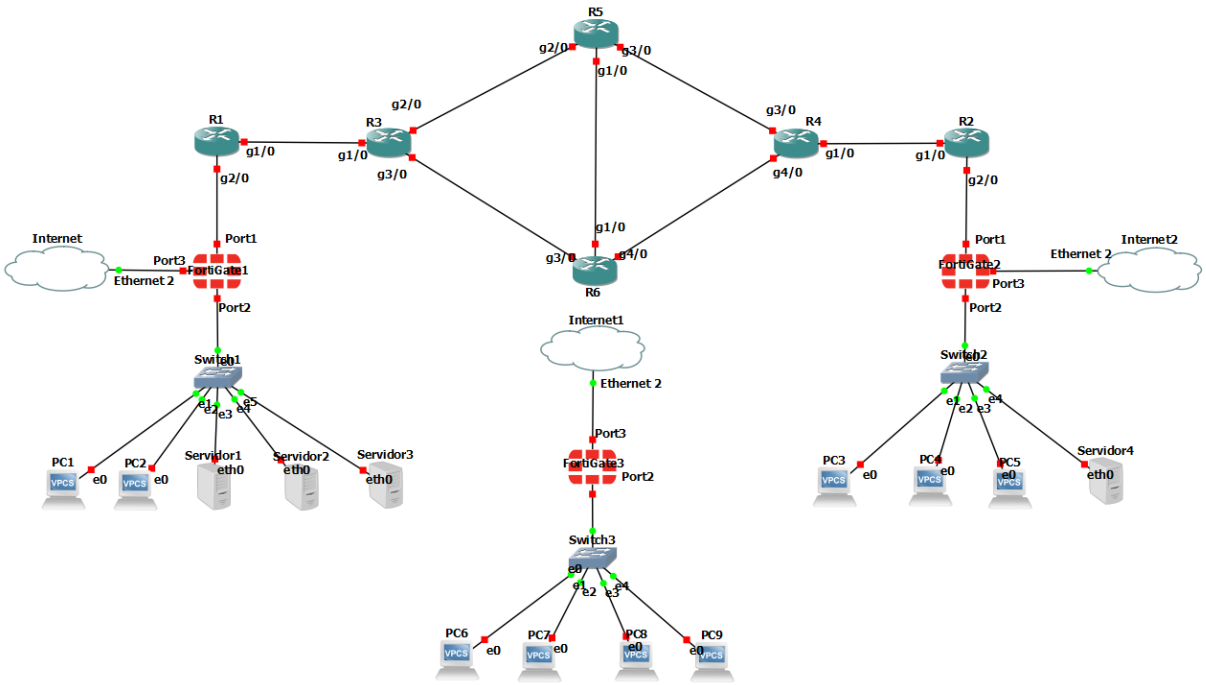
3.6.1. Simulación de la red híbrida

Para lograr el diseño y la implementación correctos, se utilizará el mismo programa de emulación (GNS3), que permite la instalación y configuración de equipos de red, incluidos enrutadores, conmutadores, PC y otros. Entre sus muchas funciones, este software puede conceder derechos y privilegios para la configuración de puertos y el acceso a Internet.

Cada sucursal de esta configuración tiene instalado un dispositivo SD-WAN, que la conecta a la red MPLS. Como se ve en la Figura 16, los dispositivos SD-WAN están conectados entre sí a través de la infraestructura MPLS actual.

Figura 16

Red hibrida realizada en GNS3



4. CAPÍTULO IV: IMPLEMENTACIÓN DE POLÍTICAS DE QOS

En este capítulo 4 se creará una representación realista de la red híbrida y sentar las bases para pruebas y análisis en etapas posteriores ya que permitirá evaluar el rendimiento y eficacia de las soluciones implementadas.

4.1. Definición de políticas de QoS

Se aplicará las políticas QoS para priorizar el tráfico de aplicaciones según su criticidad y demanda de ancho de banda. Antes de explorar los matices de las políticas de red, es esencial hacer hincapié en una fase crítica del procedimiento de configuración de SD-WAN. Después de que todos los enlaces necesarios se hayan incorporado sin problemas a la arquitectura SD-WAN que conecta la oficina central, el centro de datos y la sucursal, tiene lugar una configuración crucial: todos los dispositivos FortiGate crean una única ruta estática (0.0.0.0/0). Esta ruta estática actúa como puerta de enlace a Internet de la SD-WAN, que es un requisito esencial para activar la conectividad externa. Sin embargo, es importante recordar que la configuración de esta ruta por sí sola no proporciona acceso instantáneo a Internet. Aquí es donde entra en juego el establecimiento de los puertos de entrada y salida del tráfico y las subredes de origen y destino a la hora de aplicar las políticas. Estas normas desempeñan un papel crucial a la hora de permitir que la red.

4.2. Implementación de políticas QoS

4.2.1. Políticas de red principal

En el sitio principal se crean cuidadosamente seis políticas diferentes para controlar el tráfico de red. Una de las políticas, "Denegación implícita", es la política implícita o predeterminada que se aplica a todos los dispositivos FortiGate y tiene por objeto denegar explícitamente cualquier tráfico, entrante o saliente, a cualquier destino. Este principio rector

actúa como defensa contra el acceso no deseado a la red. El administrador de red ha creado cinco políticas adicionales además de la básica para abordar protocolos de seguridad y necesidades operativas particulares.

Entre estas políticas personalizadas destaca la política "InternetAccess", que define el puerto 6 como puerto de entrada (la LAN de Guayaquil) y los puertos SD-WAN como puertos de salida. Curiosamente, un aspecto especial de esta directriz es que SDWAN se designa como

Adicionalmente, la política "To_DC" realiza la gestión del flujo de tráfico unidireccional desde la oficina central hacia el Data Center y la sucursal. Especifica LAN como puerto de entrada y SD-WAN como puerto de salida, y las subredes de origen proceden de la "HQ_Subnet" y las subredes de destino incluyen la "DC_Subnet" y la "BO_Subnet". Esta política garantiza canales de comunicación eficientes al permitir la conectividad saliente desde la oficina central a la sucursal y al Centro de Datos.

De forma similar, la política "InterOfficeTraffic_BO_DC" hace hincapié en la conectividad entre oficinas al permitir el intercambio de tráfico a través de la sede central entre la sucursal y el centro de datos. Al utilizar SD-WAN como puertos de entrada y salida, esta política permite que el tráfico transite a través de enlaces de red MPLS y acceso a Internet en la sede central, promoviendo una comunicación fluida entre los distintos nodos de la organización.

Además, la política "SSL-VPN" define túneles SSL-VPN como puerto de entrada, lo que permite a los usuarios de todo el mundo acceder de forma segura y remota a los recursos de la sede. El puerto de salida dirige el tráfico a la subred "HQ_Subnet" a través de LAN. Esta estrategia mejora la movilidad y la colaboración de los trabajadores al permitir a los usuarios remotos acceder fácilmente a los recursos de la sede a través de Internet.

En conjunto, la compleja red de políticas que se muestra en la Figura 2.15 explica cómo se coordina cuidadosamente el tráfico de red en la sede central y capta un marco completo diseñado para maximizar la eficacia operativa y reforzar la seguridad de la red.

Figura 17

Políticas nodo principal LAN 1

D	Name	From	To	Source	Destination
2	To_DC	LAN (port6)	SD-WAN	HQ_Subnet	DC_Subnet BO_Subnet
3	From_DC	SD-WAN	LAN (port6)	DC_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	HQ_Subnet
1	InternetAccess	LAN (port6) SD-WAN	SD-WAN	HQ_Subnet DC_Subnet MPLS Network MPLS Redundancy	all
5	InterOfficeTraffic_BO_DC	SD-WAN	SD-WAN	BO_Subnet VPN DC_Subnet MPLS Redundancy MPLS Network	DC_Subnet BO_Subnet
6	SSL-VPN	SSL-VPN tunnel	LAN (port6)	SSLVPN_TUNNEL_ADDR1 PortalWeb_Users	HQ_Subnet
)	Implicit Deny	any	any	all	all

En el Nodo de Datos se han establecido seis reglas, exactamente igual que en la oficina principal. Hay una política de "Denegación implícita" y otras cinco políticas bien escritas que fueron creadas por el administrador de red. Aunque el funcionamiento general de estas políticas

sigue siendo el mismo que en la oficina principal, nos centramos en identificar las sutiles diferencias.

De forma similar a su homóloga para la oficina principal, la política "Acceso a Internet" identifica la SD-WAN como el puerto de salida específico del centro de datos y la LAN como el puerto de entrada. Pero ahora que la subred de origen coincide con "DC_Subnet", todos los usuarios del centro de datos pueden navegar por Internet sin interrupciones, ya que todos los destinos están abiertos al acceso sin restricciones.

Del mismo modo, la política "To_HQ_BO" conserva las mismas configuraciones de puertos salientes y entrantes, pero lo hace de acuerdo con la SD-WAN del Centro de Datos. las subredes de origen se limitan a "DC_Subnet", las subredes de destino incluyen "HQ_Subnet" y "BO_Subnet", y así se crea un enlace unidireccional desde el Centro de Datos a la oficina central y la sucursal.

Por otro lado, con "HQ_Subnet", "MPLS Network", "BO_Subnet" y "VPN" como subredes de origen y "DC_Subnet" como subred de destino, la política "From_HQ_BO" replica la configuración de puertos de la otra manera. Esta política dispone que las conexiones se realicen entre la oficina principal y la sucursal y el centro de datos a través de la red MPLS o VPN.

Al designar SD-WAN como puerto de entrada y salida, la política "InterOfficeTraffic_HQ_BO" facilita el intercambio de tráfico entre las sucursales y la oficina central, actuando el centro de datos como mediador. Las subredes de origen incluyen "BO_Subnet", "HQ_Subnet", "MPLS Network", "MPLS Redundancy" y "VPN", y las subredes de destino incluyen tanto "HQ_Subnet" como "BO_Subnet".

Por último, la política "SSL-VPN" mantiene un sistema comparable al de su homóloga de la oficina principal, pero con configuraciones de puertos exclusivas del Centro de Datos. Curiosamente, la subred de destino coincide ahora con "DC_Subnet", lo que permite a los usuarios de todo el mundo acceder en línea a los recursos del Centro de Datos. Esta política favorece la conectividad y la colaboración entre usuarios de distintas zonas geográficas al agilizar el acceso remoto de usuarios de todo el mundo.

Figura 18

Políticas nodo de datos LAN 2

ID	Name	From	To	Source	Destination
2	To_HQ_BO	LAN (port3)	SD-WAN	DC_Subnet	HQ_Subnet BO_Subnet
3	From_HQ	SD-WAN	LAN (port3)	HQ_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	DC_Subnet
1	InternetAccess	LAN (port3)	SD-WAN	DC_Subnet	all
4	InterOfficeTraffic_HQ_BO	SD-WAN	SD-WAN	BO_Subnet VPN HQ_Subnet MPLS Redundancy MPLS Network	HQ_Subnet BO_Subnet
5	SSL-VPN	SSL-VPN tunnel	LAN (port3)	SSLVPN_TUNNEL_ADDR1 DC_PortalWeb_Users	DC_Subnet
0	Implicit Deny	any	any	all	all

La sucursal se diferencia de la oficina principal y del centro de datos en que es una configuración a distancia más sencilla. Se distingue por la creación por parte del administrador de tres reglas además de la política estándar "Denegación implícita".

El puerto de entrada se designa como LAN y el de salida como SD-WAN específica de la sucursal mediante la política "InternetAccess"; la subred de origen se define como "BO_Subnet" y el destino se establece como "all". Para satisfacer las necesidades de conectividad de los usuarios de las sucursales, esta política les proporciona esencialmente acceso sin restricciones a Internet.

Al igual que la política anterior, la política "To_HQ_DC" mantiene la misma configuración de puertos y subred de origen; la única diferencia es que la subred de destino se cambia a "HQ_DC_Supernet". Esta política establece un enlace unidireccional entre la sede central y la sucursal, así como el Centro de Datos.

Por el contrario, la política "From_HQ" designa la SD-WAN como puerto de entrada y la LAN como puerto de salida, con subredes de origen que comprenden "HQ_DC_Supernet", "MPLS Network", "MPLS Redundancy" y "VPN", y la subred de destino establecida en "BO_Subnet". Esta política permite conexiones tanto desde la oficina central como desde el Centro de Datos a la sucursal, garantizando vías de comunicación sin fisuras.

Figura 19

Políticas nodo sucursal LAN 3

ID	Name	From	To	Source	Destination
3	To_HQ_DC	LAN (port2)	SD-WAN	BO_Subnet	HQ_DC_Supernet
1	InternetAccess	LAN (port2)	SD-WAN	BO_Subnet	all
2	From_HQ	SD-WAN	LAN (port2)	HQ_DC_Supernet VPN MPLS Redundancy MPLS Network	BO_Subnet
0	Implicit Deny	any	any	all	all

Las reglas que controlan el comportamiento de SD-WAN están cuidadosamente diseñadas para seguir las políticas de la red. Esto mejora la inteligencia de la red y hace posible

que las decisiones de enrutamiento del tráfico se tomen automáticamente en función de factores como el ancho de banda y la latencia. Aquí es donde se encuentra el mecanismo de reglas SD-WAN, cada una con objetivos específicos para la oficina central, el centro de datos y la sucursal.

La primera regla, llamada apropiadamente "To-DC", está diseñada para transportar tráfico al centro de datos desde la oficina principal o cualquier sucursal. La ruta ideal es elegida por SD-WAN de forma autónoma basándose en criterios de latencia, entre las posibles rutas están "MPLS" y "VPN ToDC". Cuando se producen picos de latencia imprevistos, SD-WAN se adapta dinámicamente para garantizar el mejor enrutamiento de tráfico posible.

A continuación, utilizando los mismos criterios de latencia para la toma de decisiones, se desarrolla la regla "To-BO" para encaminar el tráfico desde la sede central o el Centro de Datos a la sucursal utilizando la mejor vía disponible. En particular, los administradores o clientes pueden dar prioridad a cuestiones como el ancho de banda, la pérdida de paquetes o el cumplimiento de los SLA gracias a la flexibilidad de este parámetro para satisfacer requisitos únicos.

Además, el equilibrio del tráfico se gestiona mediante la regla "InternetAccess", que facilita al Centro de Datos y a la oficina central la navegación por Internet. Uno de los enlaces de la oficina central debe utilizarse como reserva en caso de que el enlace a Internet del Centro de Datos experimente problemas de conectividad. Utilizando técnicas de balanceo de carga para distribuir el tráfico uniformemente entre las conexiones en función de los parámetros del SLA, SD-WAN elige de forma inteligente la mejor conexión de banda ancha de las tres que están disponibles, garantizando un uso eficaz de los recursos y un acceso ininterrumpido a Internet.

Figura 20

Reglas nodo principal LAN 1

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	To-DC	HQ_Subnet BO_Subnet	DC_Subnet	Latency	MPLS Redundante (port5) ToDC MPLS (port7)
3	To-BO	HQ_Subnet DC_Subnet	BO_Subnet	Latency	ToNYC MPLS Redundante (port5) MPLS (port7)
1	InternetAccess	HQ_Subnet DC_Subnet	all	SLA	WAN1 (port1) WAN2 (port2) WAN3 (port3)
Implicit 1					
	sd-wan	all	all	Source IP	any

De forma similar, se establecen tres reglas SD-WAN independientes dentro del Centro de Datos para mejorar el rendimiento de la red y optimizar el enrutamiento del tráfico. La primera regla, "To-HQ", utiliza la latencia como criterio principal para la toma de decisiones y asume el deber crucial de averiguar la mejor ruta entre la oficina central y el centro de datos. Esto garantiza una conectividad eficaz y fiable entre los dos nodos clave de la infraestructura de red.

Posteriormente, la regla "To-BO" se encarga de determinar la mejor ruta para transferir el tráfico desde la oficina central o el centro de datos a la sucursal. Siguiendo las pautas anteriores, esta elección se basa en la latencia, permitiendo rutas de comunicación rápidas y sencillas entre los nodos centrales y los establecimientos periféricos.

Por último, la regla "InternetAccess" se encarga de proporcionar acceso a Internet a los clientes del Centro de Datos. Para encontrar la mejor ruta de acceso a Internet para los usuarios del Centro de Datos, esta regla utiliza un encaminamiento basado en la latencia. Curiosamente, los usuarios pueden elegir entre utilizar el dispositivo FortiGate de la sede central como puerta de enlace a Internet o utilizar su propia conexión de banda ancha dedicada. Para los clientes del Centro de Datos que acceden a servicios en línea, este enfoque de enrutamiento dinámico garantiza una conectividad fiable y un uso eficaz de los recursos disponibles.

Figura 21

Reglas nodo sucursal LAN 2

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	To-HQ	DC_Subnet	HQ_Subnet	Latency	MPLS Redundante (port2) ToHQ MPLS (port4)
3	To-BO	DC_Subnet HQ_Subnet	BO_Subnet	Latency	ToNYC MPLS Redundante (port2) MPLS (port4)
1	InternetAccess	DC_Subnet	all	Latency	WAN1 (port1) MPLS Redundante (port2) MPLS (port4)

Se han desarrollado tres reglas SD-WAN distintas para la sucursal. La primera, denominada "ToHQ", se encarga de determinar el método óptimo para llevar el tráfico de la sucursal a la oficina principal. Tiene en cuenta la latencia y selecciona entre las VPN "ToHQ" y "ToDC" como posibilidades de ruta.

Con un destino diferente, la regla "ToDC" funciona según el mismo principio y se encarga de transportar el tráfico desde la sucursal hasta el centro de datos.

Por último, los usuarios pueden utilizar la ruta óptima cuando navegan por Internet gracias a la regla "InternetAccess". Como se ve en la Figura, en este caso sólo hay dos enlaces de banda ancha. Como resultado, se puede utilizar el equilibrio de carga ya que hay un tráfico excesivo, como en la Figura 22.

Figura 22

REglas nodo sucursal LAN 3

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	ToHQ	BO_Subnet	HQ_Subnet	Latency	ToHQ ToDC
3	ToDC	BO_Subnet	DC_Subnet	Latency	ToHQ ToDC
1	Internet	BO_Subnet	all	SLA	WAN1 (port1) WAN2 (port3)

5. CAPÍTULO V: ANÁLISIS Y RESULTADOS

5.1. Monitoreo de la red SD-WAN

Esta parte facilita la supervisión de los enlaces miembros de la SD-WAN sondeando continuamente un servidor seleccionado en busca de señales. Con este método, es posible evaluar en profundidad las métricas de rendimiento de cada enlace. Estas métricas incluyen la pérdida de paquetes, la fluctuación de fase y la latencia, todas ellas cruciales para la supervisión de la calidad del servicio (QoS). La dirección IP del servidor de destino debe estar disponible para evaluar con precisión el rendimiento del enlace.

son los enlaces aprobados que vigilará la oficina principal. En primer lugar, las rutas a la sucursal se incluyen en la categoría "QoS", lo que permite evaluar en tiempo real las métricas de rendimiento para mantener los mejores canales de comunicación posibles entre la oficina principal y las sucursales periféricas. A continuación, para proporcionar un acceso ininterrumpido a los recursos y servicios en línea externos, la categoría "QoSInternet" se encarga de vigilar los enlaces que se conectan a Internet. Por último, los enlaces al Centro de Datos son supervisados por la categoría "QoS_DC", que facilita la evaluación continua de los indicadores de rendimiento para mantener una conectividad fiable y un intercambio de datos eficaz entre el depósito central de datos y la sede. Las organizaciones pueden proteger la eficiencia de la red y la experiencia del usuario identificando y abordando de forma proactiva los posibles cuellos de botella en el rendimiento mediante la supervisión sistemática de estos enlaces especificados.

Figura 23

Monitoreo de enlaces

Name	Detect Server	Packet Loss	Latency	Jitter
QoS	10.10.3.254	MPLS Redundante (port5): MPLS (port7): ToNYC:	MPLS Redundante (port5): MPLS (port7): ToNYC:	MPLS Redundante (port5): MPLS (port7): ToNYC:
QoSMPLS	10.10.2.100	MPLS Redundante (port5): MPLS (port7): ToDC:	MPLS Redundante (port5): MPLS (port7): ToDC:	MPLS Redundante (port5): MPLS (port7): ToDC:
Name	Detect Server	Packet Loss	Latency	Jitter
QoSMPLS	10.10.1.100	MPLS Redundante (port2): MPLS (port4): ToHQ:	MPLS Redundante (port2): MPLS (port4): ToHQ:	MPLS Redundante (port2): MPLS (port4): ToHQ:
QoS_To_BO	10.10.3.254	MPLS Redundante (port2): MPLS (port4): ToNYC:	MPLS Redundante (port2): MPLS (port4): ToNYC:	MPLS Redundante (port2): MPLS (port4): ToNYC:

En cuanto al Centro de Datos, sus tareas de supervisión incluyen el examen de las conexiones que apuntan a diversas ubicaciones. "QoS_Internet" es una categoría dedicada al seguimiento de los enlaces que conducen a Internet para garantizar una conectividad constante y el mejor rendimiento posible cuando se utilizan sitios web externos. De forma similar, la categoría "QoS_MPLS" se encarga de vigilar los enlaces que discurren a través de conexiones MPLS hacia la sede central, lo que resulta esencial para preservar unas líneas de comunicación sólidas entre el Centro de Datos y el núcleo administrativo central. Además, los enlaces con las sucursales se gestionan a través de la categoría "QoS_To_BO", lo que hace más eficaz el intercambio de datos y la comunicación entre el Centro de Datos y las sucursales periféricas. El Centro de Datos puede detectar y resolver proactivamente cualquier posible problema de rendimiento mediante la supervisión diligente de estos tipos de enlace asignados. De este modo se mantiene la fiabilidad de la red y se garantiza una comunicación fluida a través de los distintos tipos de enlaces.

Figura 24

Monitoreo de enlaces 2

Name	Detect Server	Packet Loss	Latency	Jitter
QoSDC	http://10.10.2.100/	ToDC: ToHQ:	ToDC: ToHQ:	ToDC: ToHQ:
QoSHQ	10.10.1.100	ToDC: ToHQ:	ToDC: ToHQ:	ToDC: ToHQ:

5.1.1. Análisis de ruta de datos

Utilizamos simuladores para realizar extensas pruebas con el fin de evaluar el flujo de datos dentro de nuestra configuración de red híbrida SD-WAN/MPLS. Gracias a estas simulaciones, pudimos ver y examinar el flujo de tráfico en varios segmentos de la red, como las conexiones MPLS y las superposiciones SD-WAN. Los resultados mostraron que el tráfico se enrutó dinámicamente según las políticas de calidad de servicio y las condiciones de la red, y que se crearon rutas de datos de forma eficaz. Conseguimos una formación y gestión de rutas de datos sin fisuras, garantizando un rendimiento óptimo en toda la red, mediante la integración de FortiGate para la gestión de SD-WAN y el controlador ONOS para el control centralizado de la red.

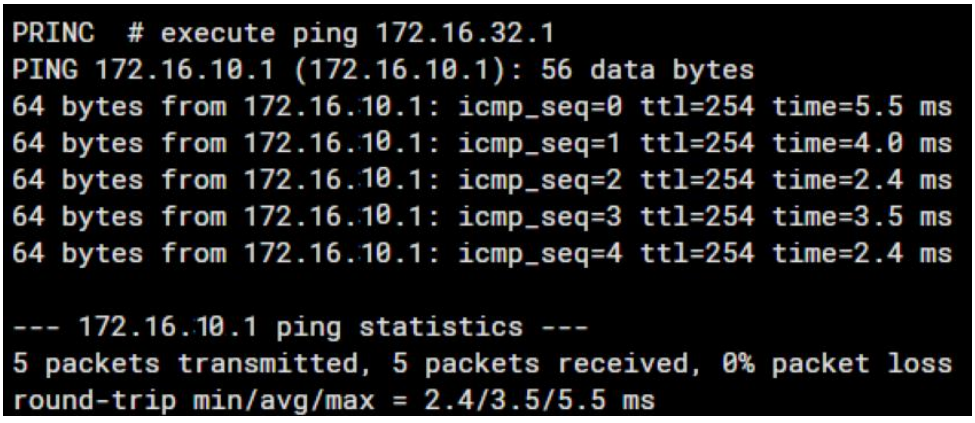
Siguiendo los procedimientos utilizados para la vigilancia de redes WAN, comenzamos nuestra evaluación con comprobaciones exhaustivas de conectividad habilitadas por el protocolo ICMP, también conocido como "ping". El objetivo de estas pruebas era verificar y evaluar la conectividad de la infraestructura de red entre uno o más hosts. Realizamos extensas pruebas de ping para evaluar el alcance y la capacidad de respuesta de los dispositivos de red en diferentes segmentos de red, haciendo uso de las características fiables de las herramientas de simulación.

La Figura 25 muestra una captura de pantalla de la prueba de conectividad entre el router marcado "DATOS" y el router de gestión "PRINCIPAL". Examinamos cuidadosamente la latencia, la pérdida de paquetes y la capacidad de respuesta general de la conexión utilizando una serie de pruebas de ping. Los resultados de estas pruebas proporcionan información importante sobre la estabilidad y el rendimiento de la red, permitiendo

Verificamos que los datos se transmitían a través de la red WAN con integridad y fiabilidad, probando la conectividad en los puntos de unión y los extremos importantes de la red. Adoptar una postura proactiva en lo que se refiere a la supervisión y solución de problemas de la red demuestra nuestra dedicación a preservar el máximo rendimiento de la red y a proporcionar experiencias de usuario excepcionales. Seguimos comprometidos con el mantenimiento de los más altos niveles de rendimiento y fiabilidad de la red en toda nuestra arquitectura híbrida SD-WAN/MPLS mediante esfuerzos continuos de supervisión y optimización.

Figura 25

Monitoreo de ruta conectividad



5.1.2. Análisis Ancho de banda

El análisis del ancho de banda se realizó en nuestro entorno de red simulado para evaluar la capacidad y el uso de los enlaces de red. Para evaluar la eficacia de la asignación y utilización

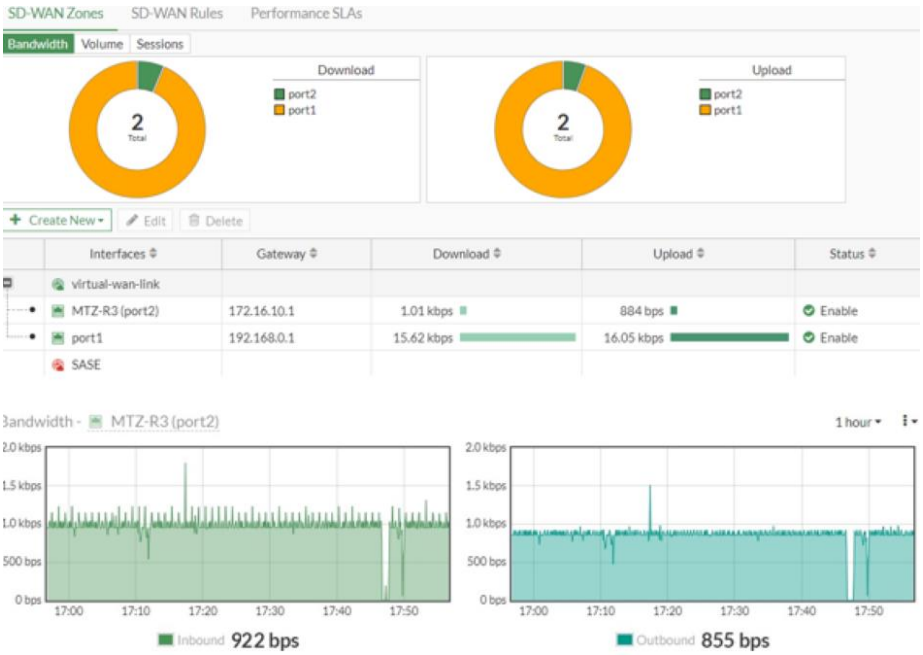
del ancho de banda, se realizaron mediciones de rendimiento en redes MPLS y conexiones SD-WAN. Los resultados demostraron lo bien que nuestra arquitectura de red utilizaba los recursos de ancho de banda a nuestra disposición, modificando dinámicamente los flujos de tráfico para maximizar la eficiencia y satisfacer los fluctuantes niveles de demanda. Pudimos dar prioridad al tráfico importante y garantizar una asignación de ancho de banda suficiente para las aplicaciones necesarias aplicando políticas de calidad de servicio y técnicas de modelado del tráfico, lo que mejoró la experiencia del usuario y la eficiencia general de la red.

Mediante herramientas de supervisión integradas en los dispositivos Fortigate, se midió el rendimiento de red de las interfaces que componen la SD-WAN. Estas tecnologías permitieron una evaluación completa de la escalabilidad de la red, la estabilidad y la capacidad de satisfacer las necesidades de un entorno empresarial dinámico, proporcionando información exhaustiva sobre diversos parámetros de rendimiento. Los resultados de la medición del ancho de banda confirman la resistencia de la infraestructura de red al demostrar su capacidad para gestionar eficazmente volúmenes de tráfico fluctuantes y ajustarse a las cambiantes demandas operativas.

La sección del estudio que sigue ofrece una comparación detallada de los resultados de la medición del ancho de banda, que demuestran el rendimiento de la red en varios escenarios de tráfico y a través de múltiples interfaces. La figura 26 del análisis muestra una representación gráfica de la mediión del ancho de banda realizada en los puertos.

Figura 26

Monitoreo de ancho de banda

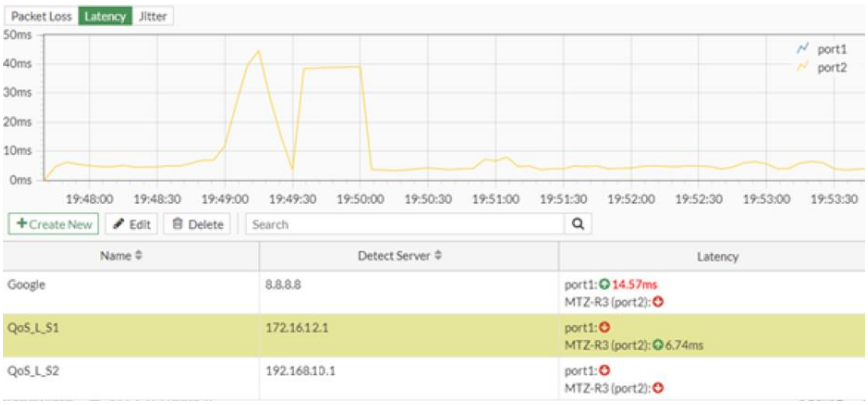


5.1.3. Análisis Latencia

Figura 27

Monitoreo de ancho de banda

Un componente clave de nuestra evaluación de la red fue el análisis de latencia, que cuantificó el tiempo que tardan los paquetes de datos en recorrer las rutas de la red. Simulamos flujos de tráfico en varios segmentos de la red y evaluamos las métricas de latencia en tiempo real con herramientas de GNS3 y Mininet. Los resultados mostraron retrasos mínimos y baja latencia en superposiciones SD-WAN y líneas MPLS, lo que demuestra la eficacia de la transferencia de datos.

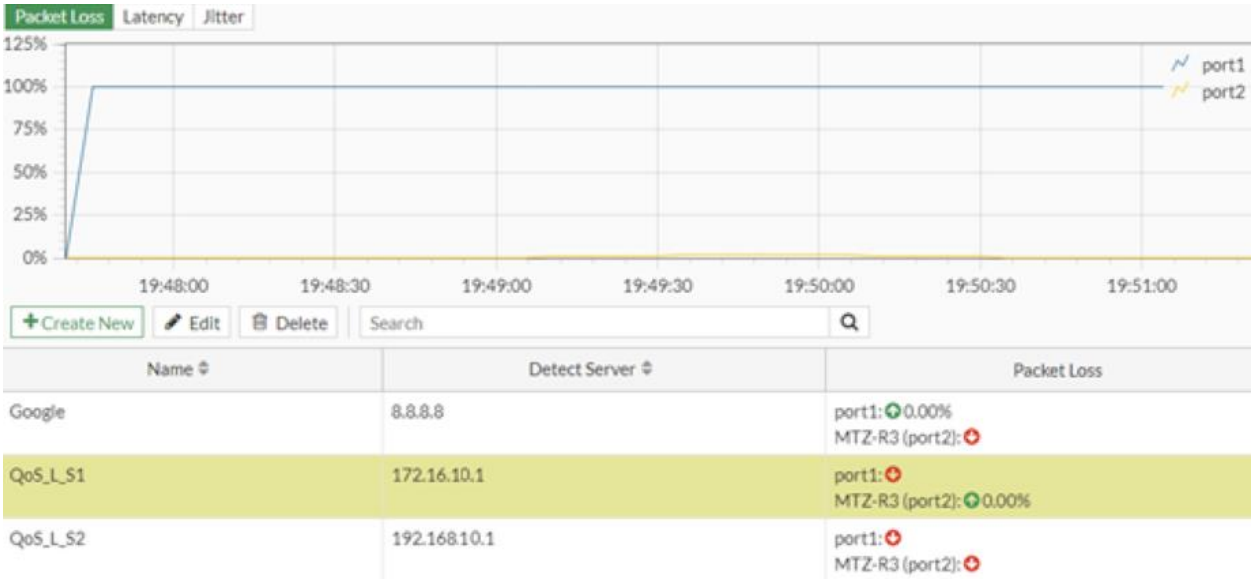


5.1.4. Análisis Pérdida de paquetes

Para evaluar la fiabilidad e integridad de la transmisión de datos en nuestro entorno de red, se realizó un análisis de pérdida de paquetes. Rastreamos las tasas de pérdida de paquetes a través de líneas MPLS y conexiones SD-WAN utilizando herramientas de captura de paquetes y utilidades de supervisión. Los resultados mostraron muy poca pérdida de paquetes, lo que pone de manifiesto la resistencia de nuestra arquitectura de red y la eficacia de las protecciones de calidad de servicio para reducir la pérdida de paquetes. Proporcionamos una alta fiabilidad e integridad de los datos en toda la red mediante mecanismos de corrección de errores y redundancia, lo que redujo el efecto de la pérdida de paquetes en el rendimiento general y la satisfacción del usuario, como se muestra en la Figura 28.

Figura 28

Monitoreo de pérdida de paquetes



Como resultado del plan de integración de la red MPLS tradicional a una infraestructura SD-WAN, el flujo de tráfico ha mejorado significativamente y la gestión de la red se ha vuelto más ágil y flexible. Estos resultados demuestran la transformación profundamente positiva que ha supuesto el plan de integración. Gracias a la utilización de múltiples conexiones y rutas más eficaces, la experiencia del usuario ha mejorado significativamente, garantizando un acceso más rápido y fiable. Además, la significativa disminución de la carga operativa relacionada con la administración de la red ha sido revolucionaria, como resultado de la abundancia de características y funcionalidades, entre las que destaca la incorporación sin problemas de sofisticados elementos de seguridad. Gracias a la gestión centralizada, esta integración ha agilizado la aplicación de políticas de seguridad, como cortafuegos, prevención de intrusiones y protección contra malware, eliminando la necesidad de instalar dispositivos adicionales y simplificando la gestión de la red. Componente clave de la administración de redes, la interfaz de gestión centralizada proporciona un único punto de vista desde el que se pueden establecer normas de tráfico, realizar un seguimiento del rendimiento de la red y llevar a cabo

actualizaciones con una rapidez inigualable, todo lo cual reduce la complejidad operativa. La eficiencia operativa se ha visto reforzada por la automatización y la orquestación, que han facilitado la implantación rápida y coherente de los cambios y la armonización de los servicios y las políticas en toda la infraestructura. Las técnicas de vanguardia para la supervisión y el análisis del tráfico han proporcionado una visibilidad total de las operaciones de la red, lo que ha permitido la detección temprana y la corrección de los problemas de rendimiento.

Además, se ha producido una notable mejora en la eficiencia de los recursos gracias a SD-WAN, que permite que el tráfico de red utilice numerosos enlaces y rutas de forma inteligente. Esta función reduce la latencia y aumenta la velocidad de las aplicaciones al permitir que el tráfico se enrute por las rutas más eficaces y disponibles. Esencialmente, el cambio a SD-WAN ha dado lugar a mejoras significativas en el rendimiento y la fiabilidad de la red, así como a una administración simplificada de la red al proporcionar una plataforma integral que combina seguridad, automatización, gestión centralizada y visibilidad mejorada. Al facilitar la gestión eficaz de la red y permitir respuestas rápidas a las cambiantes demandas de la red, este enfoque integrado posiciona a las empresas para el éxito a largo plazo en el siempre cambiante panorama digital.

Aparte de las ventajas mencionadas, la incorporación de mecanismos de calidad de servicio (QoS) en la infraestructura SD-WAN ha contribuido significativamente a mejorar el rendimiento de la red y la satisfacción de los usuarios. La QoS garantiza un rendimiento constante y fiable para funciones de misión crítica como audioconferencias y videoconferencias, herramientas de colaboración en tiempo real y aplicaciones corporativas, asegurándose de que las aplicaciones vitales tengan prioridad sobre el tráfico menos sensible al tiempo. Mediante el uso de criterios predeterminados como el ancho de banda, la latencia y la pérdida de paquetes,

los sistemas de QoS priorizan el tráfico para reducir la probabilidad de congestión de la red y garantizar que las aplicaciones críticas sigan funcionando sin interrupciones incluso en periodos de alta demanda.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La implementación con éxito de políticas de calidad de servicio (QoS) y la finalización del diseño de la red de área extensa basada en una arquitectura definida por software SD-WAN integrada con un modelo MPLS representan un hito importante en la optimización de redes y el análisis del rendimiento dentro de un entorno de red híbrido. La arquitectura de red se ha diseñado y puesto en marcha cuidadosamente para satisfacer las necesidades cambiantes y garantizar un control eficaz del tráfico y la prestación de servicios.

Para implantar y optimizar eficazmente la red híbrida es necesario disponer de un sólido marco teórico. Esto se ha logrado mediante un examen exhaustivo y la incorporación de fundamentos teóricos relativos a la arquitectura, los elementos y el funcionamiento de grandes redes definidas por software, así como una comprensión en profundidad de la infraestructura MPLS con un énfasis principal en la Calidad de Servicio (QoS).

Los conocimientos tecnológicos y la previsión estratégica demostrados en el uso de la tecnología Fortinet por parte de la infraestructura SD-WAN son evidentes en su capacidad para satisfacer las cambiantes necesidades de conectividad de los usuarios finales dentro de una red híbrida. El aprovechamiento de las capacidades de vanguardia de Fortinet garantiza la escalabilidad y la integración sin problemas, permitiendo respuestas rápidas a las cambiantes demandas de la red.

La optimización del rendimiento de la red se demuestra mediante la diferenciación y aplicación de diferentes algoritmos QoS en el entorno de red SD-WAN y MPLS. La red híbrida consigue una asignación de recursos y una capacidad de respuesta óptimas mediante la definición de políticas adecuadas, como la gestión del ancho de banda y la priorización del tráfico. Esto mejora la experiencia del usuario y la fiabilidad del servicio.

El desarrollo de una arquitectura de red híbrida completa demuestra las ventajas que conlleva el uso de ajustes de QoS para maximizar el rendimiento de la red. Con la ayuda de eficientes mecanismos de QoS y la estudiada combinación de tecnologías MPLS y SD-WAN, el diseño de la red exhibe durabilidad, escalabilidad y adaptabilidad para satisfacer una amplia gama de requisitos operativos.

Los resultados de las pruebas de rendimiento basadas en simulaciones demuestran las ventajas concretas del uso de normativas de QoS en el entorno de redes híbridas. La eficacia de los mecanismos de QoS para mejorar la eficiencia de la red, reducir la latencia y garantizar la calidad del servicio se comprueba empíricamente evaluando diferentes escenarios e indicadores de rendimiento, lo que confirma la practicidad y eficacia de la arquitectura de red.

6.2. Recomendaciones

Se aconseja seguir adelante con la implantación de la red de área extensa (WAN) prevista basada en la arquitectura definida por software SD-WAN modificada a un modelo MPLS a la luz de la finalización satisfactoria de las pruebas y análisis de rendimiento. Para garantizar el mejor rendimiento posible en la red híbrida, también debe darse la máxima prioridad a la aplicación de políticas de calidad de servicio (QoS).

Se aconseja seguir adelante con la selección de la tecnología Fortinet para la infraestructura SD-WAN a la luz de los resultados concluyentes de las pruebas. Su capacidad

para ajustarse a las necesidades cambiantes y enlazar eficazmente a los usuarios finales con los servicios relevantes dentro de la red híbrida, garantizando así una conectividad fluida y la optimización del rendimiento, respalda esta elección.

Se recomienda que, tras realizar pruebas y análisis exhaustivos, se documenten los fundamentos teóricos relativos a la estructura, los componentes y la funcionalidad de una red definida por software de gran tamaño, junto con un conocimiento de la infraestructura MPLS, con especial atención a la calidad del servicio (QoS). Este registro será una herramienta inestimable para la futura referencia y el intercambio de conocimientos de la organización.

Una vez validadas las pruebas de rendimiento, es aconsejable terminar de definir diferentes mecanismos de QoS para poder establecer reglas adecuadas en la red combinada MPLS y SD-WAN. Esto implica asignar el ancho de banda con sensatez, establecer prioridades para el tráfico importante y garantizar niveles de servicio constantes para una serie de aplicaciones y necesidades de los usuarios.

Entonces, para una integración sin problemas de MPLS y SD-WAN es necesaria una planificación, selección de la plataforma, una gestión eficaz del tráfico y una amplia formación del personal. Además, para garantizar un despliegue sin problemas y optimizar el rendimiento de la red, la implantación escalonada y la supervisión continua son buenas prácticas esenciales y se aconseja seguir adelante con el desarrollo de la arquitectura de red híbrida y poner de relieve sus ventajas.

7. BIBLIOGRAFÍA

Fortinet. (2021). Fortinet Secure SD-WAN Reference Architecture. Recuperado el 24 de mayo de 2023, de https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf

Cisco. (15 junio 2018). Implementación de QoS en Cisco SD-WAN. Recuperado el 24 de mayo de 2023, de https://www.cisco.com/c/es_mx/support/docs/routers/vedge-router/213408-implement-qos-in-cisco-sd-wan.html

Jimeno, R. (2020). No TitleSD-WAN Edge routers y su importancia en entornos. 23 Junio. https://www.teldat.com/es/blog/sd-wan-edge-router-qos-seguridad/

Teldat. (jun 23,2020). SD-WAN Edge routers y su importancia en entornos. Recuperado el 24 de mayo de 2023, de https://www.teldat.com/es/blog/sd-wan-edge-router-qos-seguridad/

IBM. (2021). Modelos QoS. https://www.ibm.com/docs/es/aix/7.2?topic=service-qos-models

Marqués, G. (2016). QoS en routers y switches Cisco. (n.p.): Lulu.com.

Digi International. (2023, May 18). SD-WAN: Software-Defined Wide Area Network. Retrieved May 18, 2023, from https://es.digi.com/solutions/by-technology/sd-wan-software-defined-wide-area-network

Burwood Group. (2023, May 18). Traditional WAN vs. SD-WAN: Here's What You Need to Know. Retrieved May 18, 2023, from https://www.burwood.com/blog-archive/traditional-wan-vs-sd-wan-heres-what-you-need-to-know

Yang1, Z., Cui1, Y., Li2, B., Liu, Y. and Xu1, Y. (2019). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. IEEE. https://ieeexplore.ieee.org/document/8847124

IBM. (2023, May 18). SD-WAN Services. Retrieved May 18, 2023, from https://www.ibm.com/es-es/services/network/sd-wan

ONOS Project. (2016). System Components. Retrieved May 18, 2023, from https://wiki.onosproject.org/display/ONOS/System+Components

Al-Shalash, A., & Al-Qahtani, A. (2021). Facilitation of The OpenDaylight Architecture. In 2021 16th International Conference on Information Technology (ICIT) (pp. 1-6). IEEE.

SDN and NFV Security: Security Analysis of Software-Defined Networking and Network Function Virtualization. (2018). Alemania: Springer International Publishing.

Stallings, W. (2014). Data and Computer Communications (PEARSON (ed.); 10ma ed.).

Berde, P., Gerola, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., Lantz, B., O'Connor, B., Radoslavov, P., Snow, W., & Parulkar, G. (2014). ONOS: Hacia un sistema operativo distribuido y abierto para SDN. En Actas del Tercer taller sobre temas candentes en redes definidas por software (páginas 1-6). Asociación de Maquinaria Informática. New York, NY, USA. doi: 10.1145/2620728.2620744.

Stallings, W. (2014). Data and Computer Communications (PEARSON (ed.); 10ma ed.). New Jerssey.

Tanenbaum, A. S. and Wetherall, D. J. (2012). Redes de Computadoras (PEARSON EDUCACIÓN (ed.); 5th ed.). https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Ariganello, E. (2020). Redes Cisco, Guía de estudio para la certificación CCNA 200-301. España: RA-MA S.A. Editorial y Publicaciones.

8. ANEXOS

Comprobación de dispositivos Fortigate

Figura 29

Colocar imagen iso en gns3 fortigate

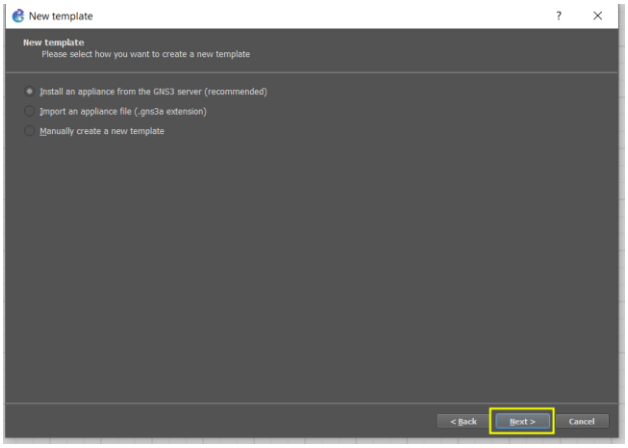


Figura 30

Colocar template en gns3 fortigate

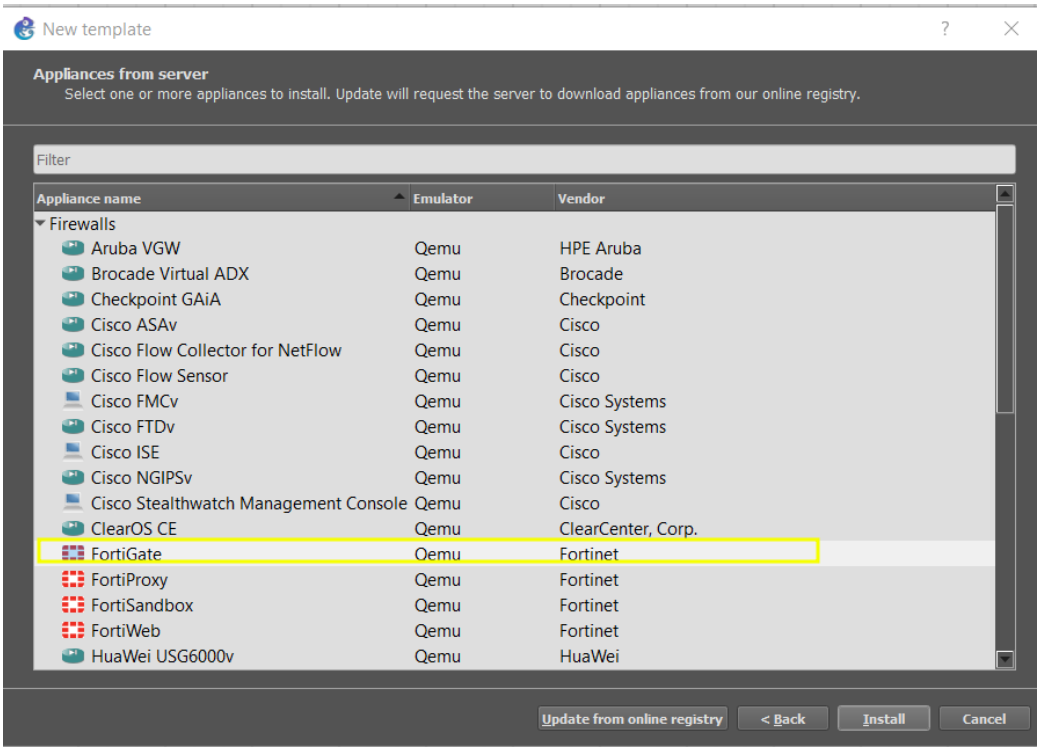


Figura 31

Colocar template en gns3 forti gate

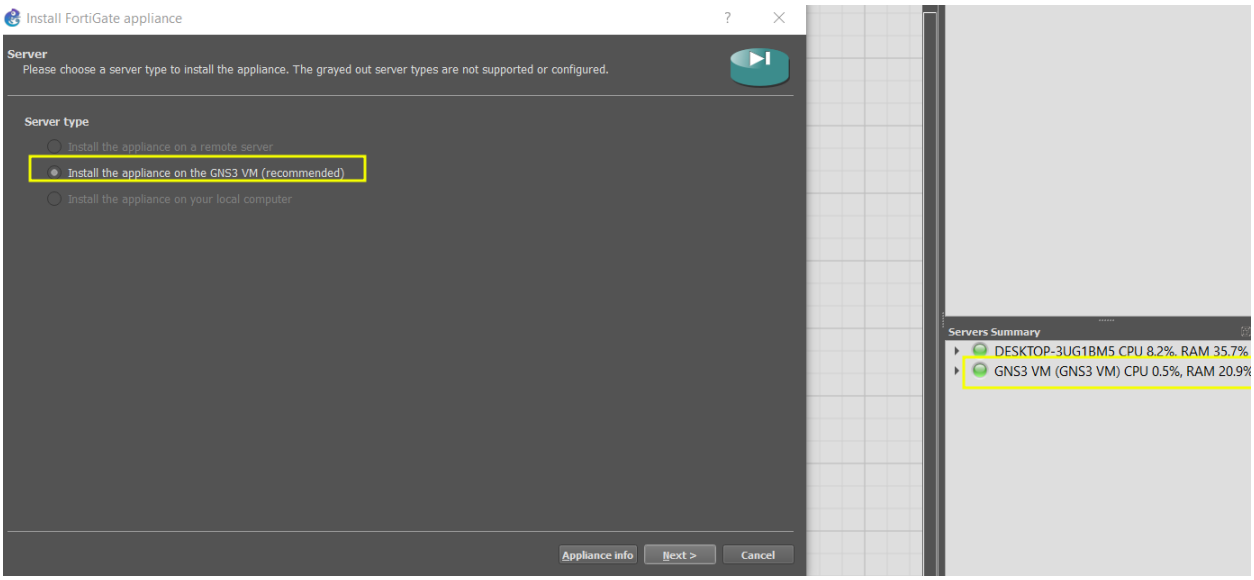


Figura 32

Colocar template en gns3 fortigate 7

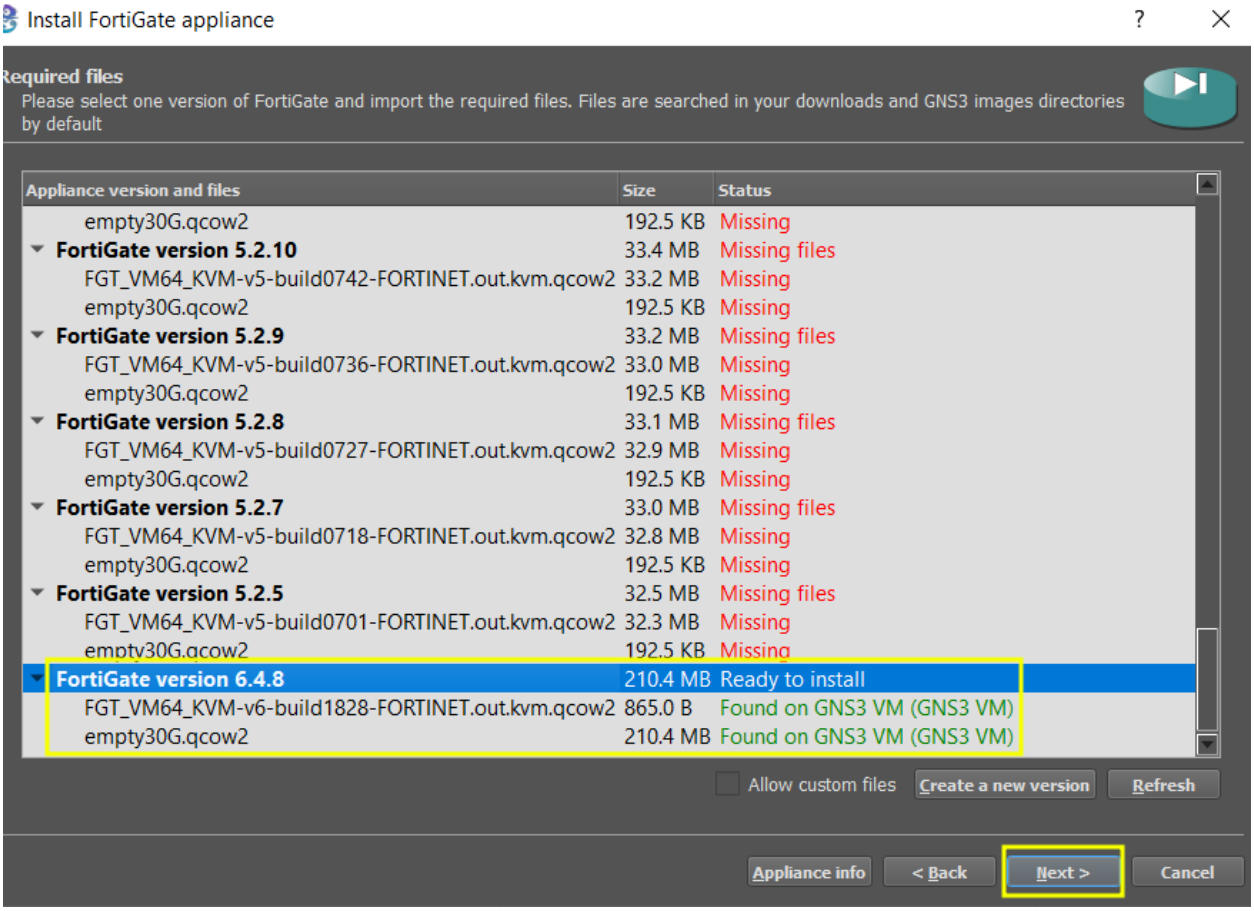


Figura 33

Colocar template en gns3 fortigate para pruebas

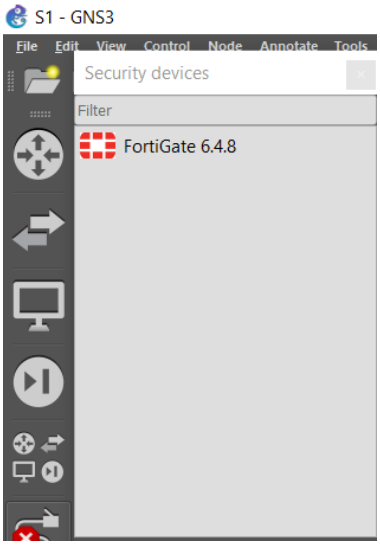


Figura 34

Colocar template en gns3 router

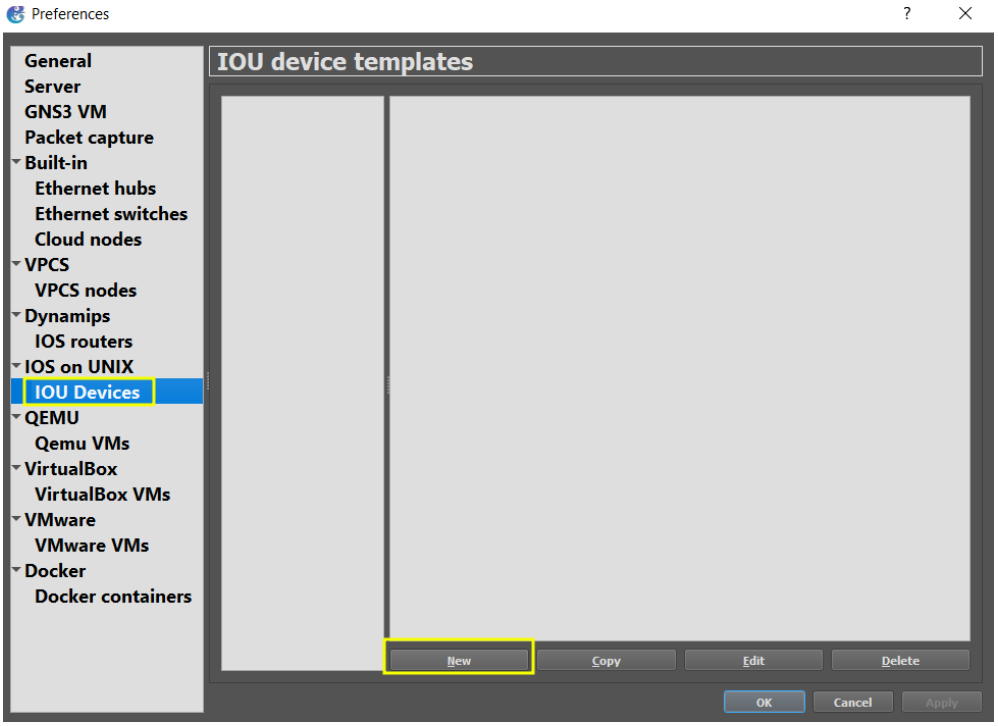


Figura 35

Colocar template en gns3 router

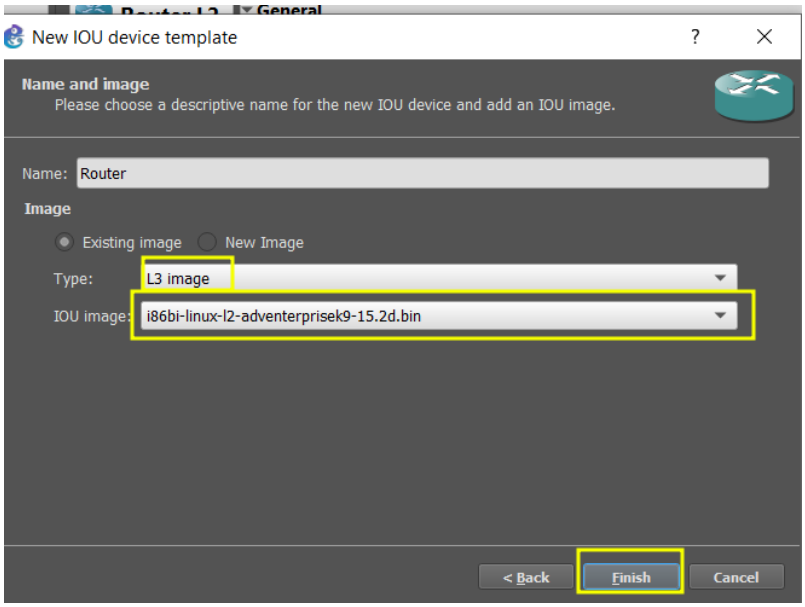


Figura 36

Prueba de red con equipo fortigate

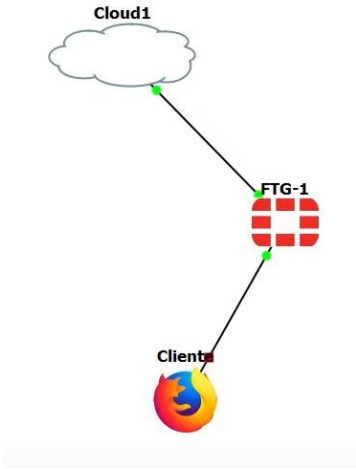


Figura 37

Prueba de funcionamiento equipo fortigate

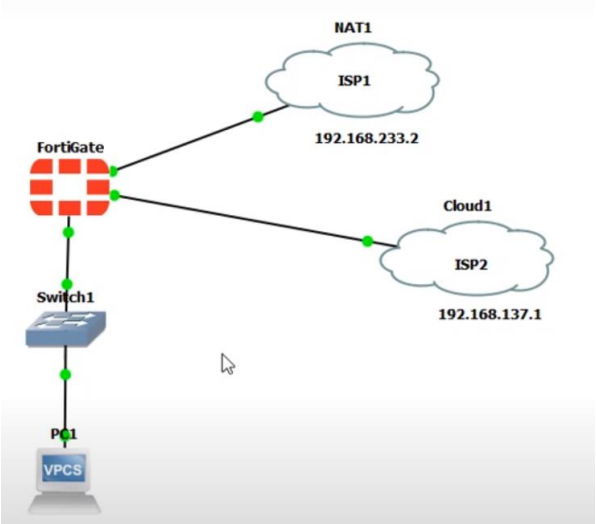


Figura 38

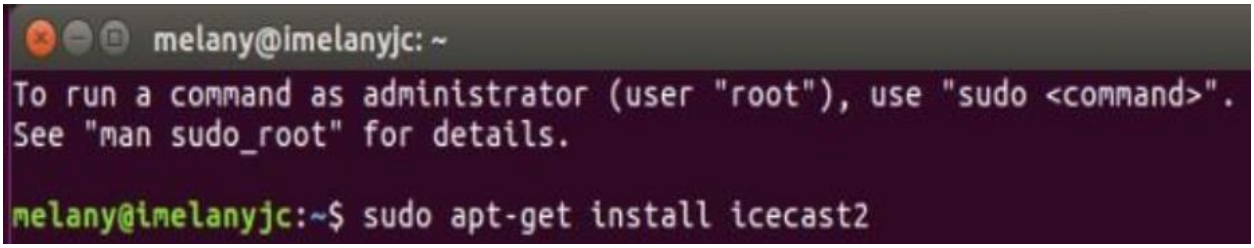
Prueba de fortigate

Instalación de Servidores

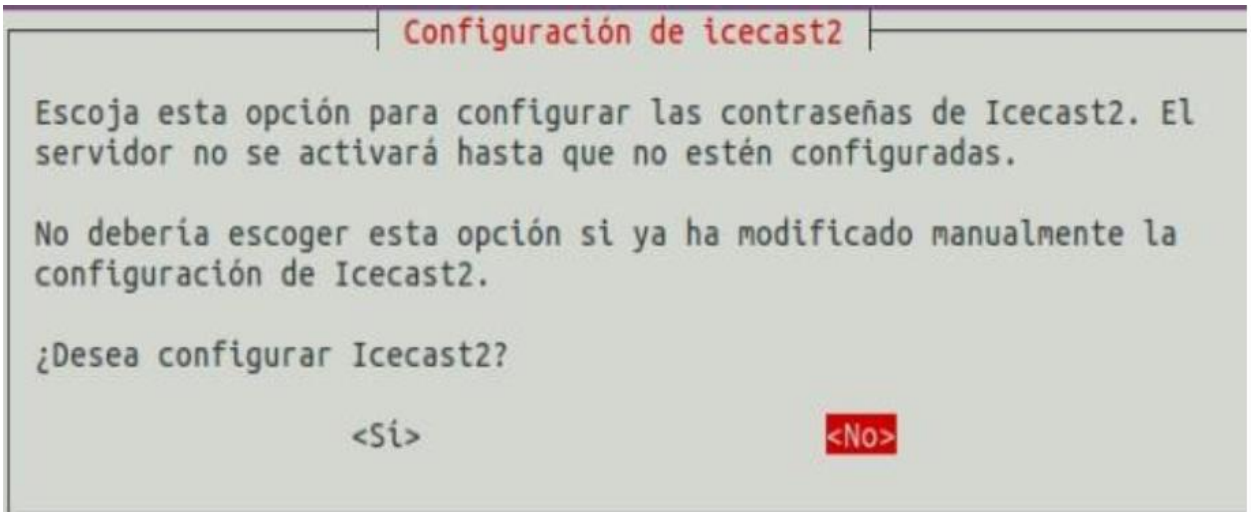
Servidor de streamming

Para configurar el servidor base de datos se lo hace en el sistema Operativo Ubuntu. Una vez instalado correctamente dentro de VirtualBox se hace lo siguiente, se instala la librería que

se va a usar para el servidor la cual es Icecast2 mediante el comando: sudo apt-get install icecast2



Seguidamente seleccionar la opción No ya que se va a realizar la configuración manualmente.



Editar el fichero de icecast

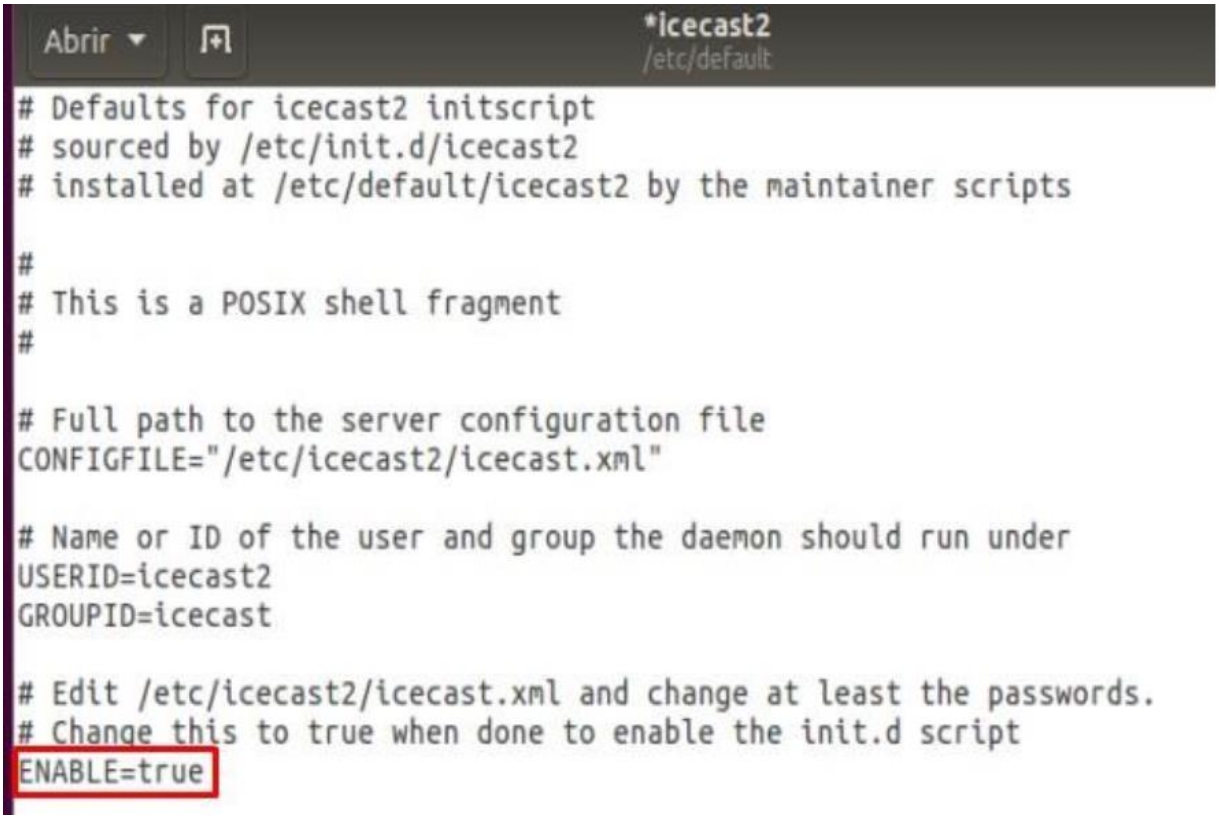
```
        It's also available here: http://icecast.org/docs/
    -->

    <limits>
        <clients>3</clients>
        <sources>2</sources>
        <queue-size>524288</queue-size>
        <client-timeout>30</client-timeout>
        <header-timeout>15</header-timeout>
        <source-timeout>10</source-timeout>
        <!-- If enabled, this will provide a burst of data when a client
             first connects, thereby significantly reducing the startup
             time for listeners that do substantial buffering. However,
             it also significantly increases latency between the source
             client and listening client.  For low-latency setups, you
             might want to disable this. -->
        <burst-on-connect>1</burst-on-connect>
        <!-- same as burst-on-connect, but this allows for being more
             specific on how much to burst. Most people won't need to
             change from the default 64k. Applies to all mountpoints  -->
        <burst-size>65535</burst-size>
```

```
<authentication>
    <!-- Sources log in with username 'source' -->
    <source-password>hackme</source-password>
    <!-- Relays log in with username 'relay' -->
    <relay-password>hackme</relay-password>

    <!-- Admin logs in with the username given below -->
    <admin-user>admin</admin-user>
    <admin-password>hackme</admin-password>
</authentication>
```

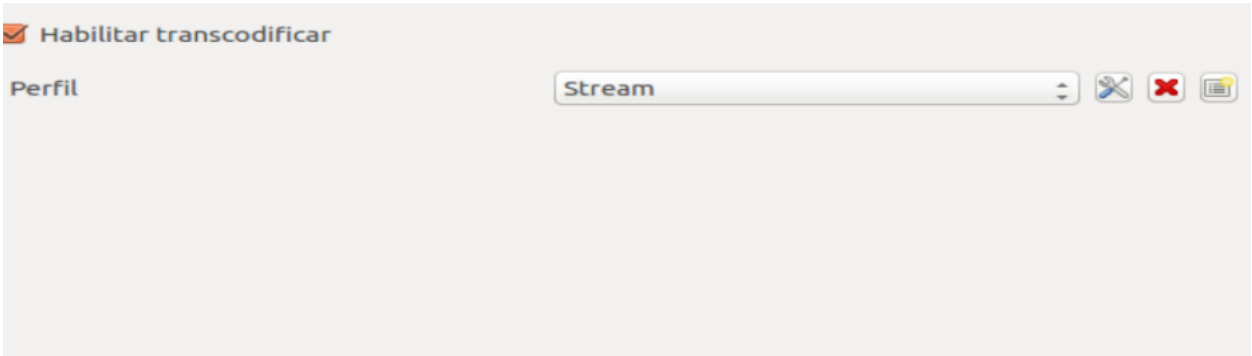
Configuramos la ip del servicio en la que va a trabajar “195.50.51.133” y el puerto que va a escuchar en este caso 8080 y 8000

```
<hostname>195.50.51.133</hostname>

<!-- You may have multiple <listener> elements -->
<listen-socket>
    <port>8000</port>
    <port>8080</port>
    <!-- <bind-address>127.0.0.1</bind-address> -->
    <!-- <shoutcast-mount>/stream</shoutcast-mount> -->
</listen-socket>
```

Fichero para activar el servicio : sudo gedit /etc/default/icecast2 cambiar a true



A continuación en el reproductor VLC se proceden con las configuraciones de video a emitir como son las características de audio, video, dirección de servidor.

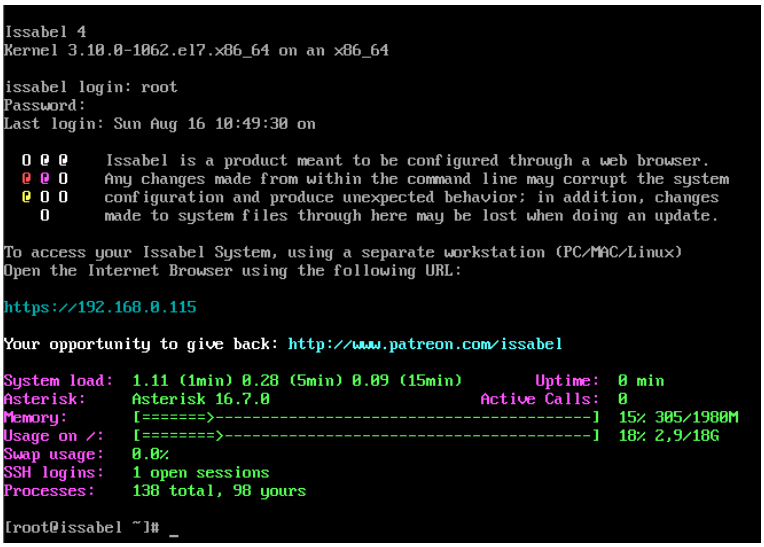


Servidor VoIP

Para la instalcion del servidor procedemos a descargar la imagen iso de la pagina web ***www.issabel.org***

Una ves descargado el el archivo procedemos a realizar la instalacion del servidor, esto se lo realiza en la una maquina virtual.

Una vez instalada nos aparecerá la siguiente pantalla con la dirección ip del servidor la cual usaremos un navegador para la creación de extensiones para poder realizar las llamadas entre clientes.

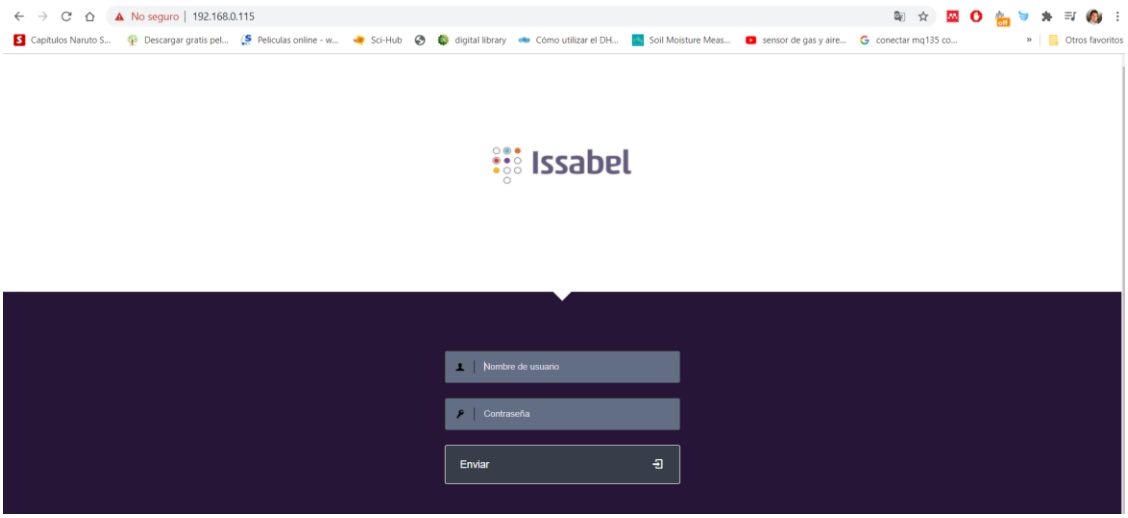


En un navegador se introduce la ip del servidor en este caso 192.168.0.115 De la misma forma podemos acceder al servidor con la ipv6.

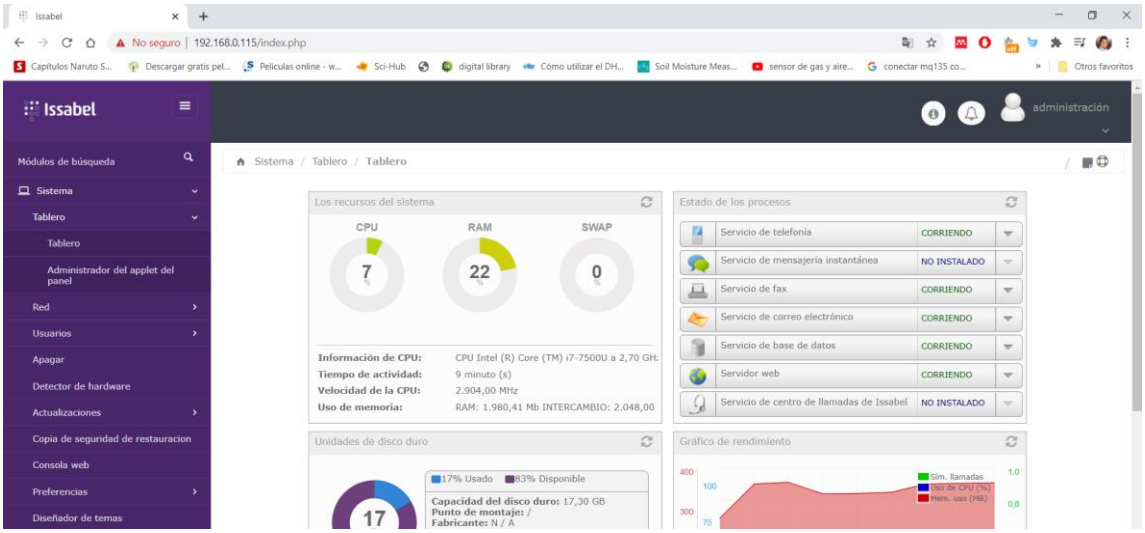
En la ventana que se muestra se debe introducir el nombre y usuario que se determinamos como administrador

Usuario: admin

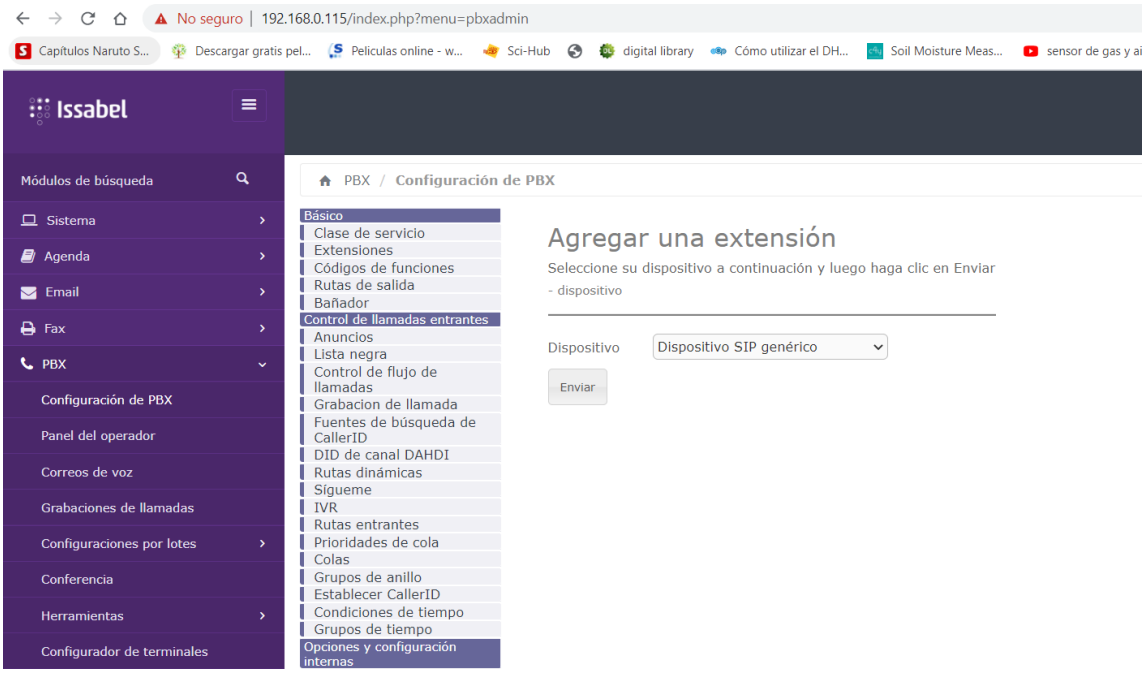
Contraseña: root



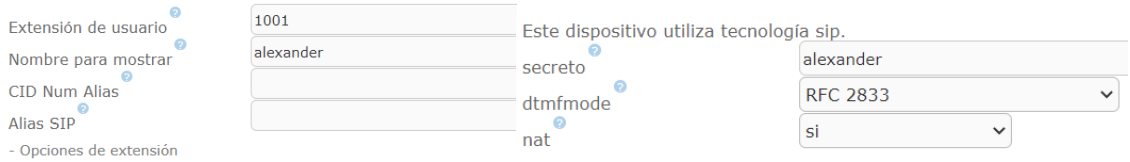
En la siguiente pantalla se observa la interfaz del servidor en la que se muestran las opciones que nos permite diferentes funciones



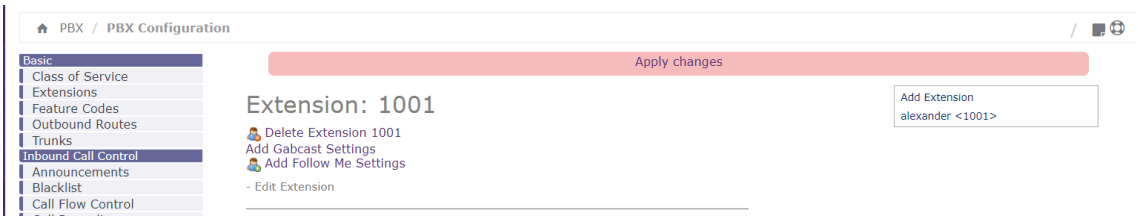
Para la creacion de extenciones nos dirigimos a la opcion PBX luego a configuracion de PBX y precionamos el boton enviar



Una vez que ingresemos los parámetros que se deben tomar en cuenta son los que los casilleros que llenamos como se muestra en las figuras.

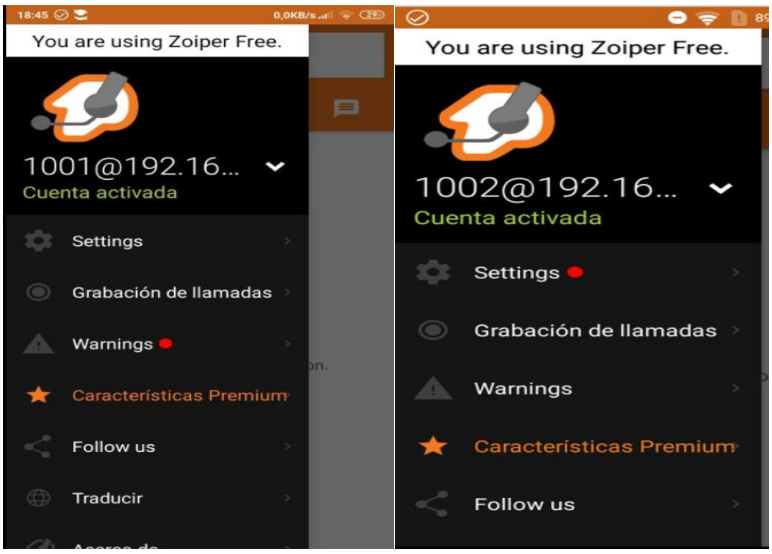


En la siguiente imagen se presenta la extensión ya creada lista para ser usada para la realización de las llamadas, para la realización de las pruebas se procedió a crear dos extensiones 1001 y la 1002

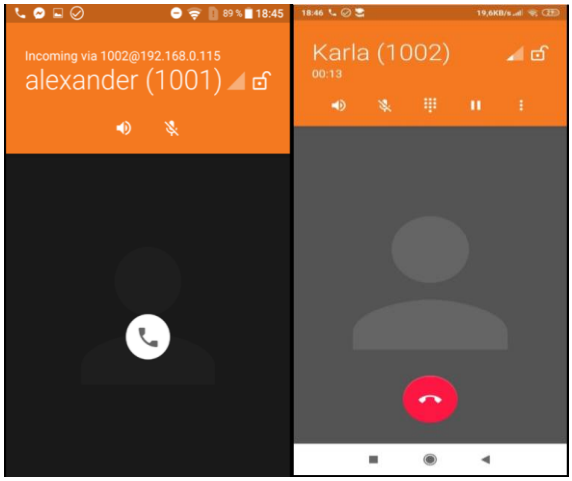


Resultados Servidor VoIP (IPv4)

Procedemos a realizar la configuración de zoiper que es una aplicación la cual nos permite realizar la prueba de funcionamiento del servidor.



Realizamos la llamada de un cliente a otro para la comprobación


Incoming via 1002@192.168.0.115
alexander (1001)
Karla (1002)
00:13