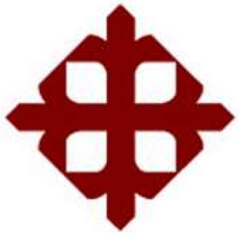


UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo.

AUTOR:
Ayapata Mendoza, Douglas Oswaldo

Trabajo de Titulación previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES

TUTOR:
M. Sc. Ruilova Aguirre, María Luzmila

Guayaquil, Ecuador

2 de marzo del 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Ayapata Mendoza, Douglas Oswaldo** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

_____

M. Sc. Ruilova Aguirre, María Luzmila

DIRECTOR DE CARRERA

_____

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, 2 de marzo del 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Ayapata Mendoza, Douglas Oswaldo**

DECLARÓ QUE:

El trabajo de titulación: **"Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo",** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

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

Guayaquil, 2 de marzo del 2020

EL AUTOR

_____

AYAPATA MENDOZA, DOUGLAS OSWALDO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Ayapata Mendoza, Douglas Oswaldo**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 2 de marzo del 2020

EL AUTOR

_____

AYAPATA MENDOZA, DOUGLAS OSWALDO

REPORTE DE URKUND

Reporte Urkund del trabajo de titulación en ingeniería Telecomunicaciones denominado: **Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo.** Del estudiante **Ayapata Mendoza, Douglas Oswaldo.** Se encuentra al 2% de coincidencias.

Atentamente.

Ing. Orlando Philco A. M.Sc.

Revisor

DEDICATORIA

El presente trabajo tesis lo dedico principalmente a Dios, por ser el guía para obtener uno de los anhelos más deseados de mi vida. A mis padres, por su amor, trabajo y sacrificio en todos estos años.

EL AUTOR

_____

AYAPATA MENDOZA, DOUGLAS OSWALDO

AGRADECIMIENTO

Quiero agradecer a Dios, por llevarme por el mejor camino, poniéndome en mi vida a un montón de personas que me han transmitido toda la sabiduría.
Agradezco el apoyo de mis padres, por darme todo lo necesité para estar aquí, por aconsejarme en todo momento que dudé y por ser la inspiración y pilar en mi vida.

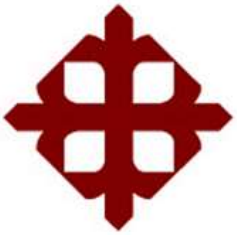
Agradezco a mi novia, por darme toda energía positiva y siempre inspirándome a para ser una mejor persona.

Agradecer especialmente a la Ing. Luzmila Ruilova, por ser una guía en toda mi etapa universitaria, llegándose a convertir en una amiga que siempre me aconsejo para ser un mejor profesional.

EL AUTOR

_____

AYAPATA MENDOZA, DOUGLAS OSWALDO



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA

f. _____

M. SC. VALLEJO SAMANIEGO, LUIS VICENTE

OPONENTE

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 2

Resumen

Software Defined Wide Area Network (SD-WAN), es conocido como la evolución de las redes de telecomunicaciones actuales. El uso de *Software Defined Network* (SDN) en las diferentes redes de comunicación, crearía un nuevo ecosistema de las redes. Este nuevo avance provocaría que la mayoría de redes y proveedores de servicios cambien su modelo de negocio de proveer servicios a proveer características, programación única y espacio en la nube para cada cliente corporativo. SD-WAN es una solución completa en caso de conectividad y seguridad ya que está bajo el cifrado de IPSec al momento de la creación de los túneles VPN, y la máxima flexibilidad de las redes, dando prioridad a la calidad según el servicio o los datos sin importar la gran demanda de usuarios a nivel masivo, pyme y corporativo. A nivel corporativo la solución SD-WAN representa un ahorro económico a nivel de hardware. En este trabajo se presentará como optimizar una WAN tradicional utilizando las redes definidas por *software* simulando caídas de la red en medio de una transmisión de información continua, donde podemos comprobar que una red WAN tradicional la comunicación se caería y existiría una gran pérdida de paquetes mientras que con la tecnología SD-WAN la perdida de paquetes seria mínima al punto de ser casi imperceptible.

Palabras claves: SD-WAN, VPN, WAN, SDN, PYME, IPSec.

CAPÍTULO 1

DESCRIPCIÓN GENERAL DEL TRABAJO DE TITULACIÓN

1.1. Introducción

Dado el abismal crecimiento del internet y la gran demanda de usuarios a nivel masivo, pyme y corporativo, esto impulsó a los diferentes sectores de trabajo a utilizar varios tipos de interconexión entre sí, llegando a utilizar múltiples tipos de conexiones para mejorar sus intercomunicaciones, para ofrecer al cliente una mejor experiencia y rápidas soluciones.

En la actualidad, la mayoría de los diferentes sectores productivos se ha decidido implementar el desarrollo de sistemas de comunicación entre sí, como medio inalámbrico tenemos a las redes de área amplia (WAN) y medios físicos como las redes de área local (LAN), ha abierto un sin número de posibilidades de redes de telecomunicaciones. A partir del nacimiento del TCP/IP se dio las primeras estructuras para una red de are amplia la cual provoco el nacimiento de las primeras redes inalámbricas, con el fin de entregar y redireccionar paquetes de datos. A finales del año ochenta el X.25 fue de poco en poco determinándose como un protocolo exclusivo para redes WAN y considerándose como la primera arquitectura base de las actuales redes de área amplias.

A finales de los años noventa, múltiples protocolos como el SDH, MPLS, ATM y Frame Relay se fueron anexando a la arquitectura de las redes WAN, junto a ello salió la necesidad de parte de los diferentes sectores de trabajo como proveer fiabilidad, rendimiento y seguridad a la información transmitidas en las redes WAN y LAN. Las VPN nacio como solución de económica a las necesidades para los diferentes clientes en solución de privacidad y exclusividad de conexión.

Tras la llegada del nuevo milenio, vino cargado con nuevos avances con ello el aumento de la demanda de clientes y la aparición de nuevos servicios con exigencias más rígidas, como una alta disponibilidad en la red con la premisa de reducir costos.

La llegada del SDN (Redes Definidas por Software) la cual llegó como una pieza fundamental para la evolución de las redes como actualmente las conocemos.

1.2. Antecedentes

En los años 60´ las redes de comunicación de daba solo en computadores aislados conectados entre sí solo por un cable, si existía un caso de un acceso remoto se debía realizar por las líneas telefónicas creando la base de las redes LAN, que en el 69 se dio la primera conexión LAN entre 3 diferentes universidades como prueba del funcionamiento del ARPANET como una de las primeras pruebas para una red de interconexión mundial conocida en la actualidad como Internet.

Robert Elliot Khan junto a Vinton Cerf, tras la necesidad de transmitir la información a todas partes del mundo, inventaron el protocolo TCP/IP aplicando en la primera prueba del Internet como actualmente lo conocemos, utilizando una conexión de múltiples ordenadores en la Conferencia internacional de comunicaciones Informáticas, siendo mostrado por primera vez este método de manera oficial, esto dio inicio el ambicioso proyecto estratégico de computación del gobierno de USA que estaba encargado del proyecto de comunicaciones por satélite.

En 1993, Lawrence Roberts y Thomas Merril, logran conectar 2 ordenadores por medio de una red telefónica de cobre de baja velocidad, con esto dio luz a la primera Red WAN (Wide Area Network), la creación de WAN se volvió necesaria para el avance de las redes de telecomunicaciones debido que la gran demanda de información de la parte corporativa y masiva no era suficiente para realizar el intercambio de datos de manera rápida y eficaz a grandes distancias.

El mundo de las redes empezó a desarrollarse de manera tenaz, la cual el tráfico de información cambió de solo enviar tráfico de datos y ahora a la actualidad el tráfico es de voz, datos, imágenes y video. También la inclusión de diversos protocolos FTP, UDP, TCP/IP, PPP etc, esto provoca un sin número de sistemas de conexiones (Unicast, Multicast, Broadcasting).

En la actualidad, el sector corporativo se beneficia de la proliferación de las redes, debido a que abarca una gran distribución geográfica dando nuevos puntos de accesos y servicios de telecomunicaciones. Sin embargo, aún existen directrices que se pueden solucionar.

1.3. Definición del problema

Debido al aumento del tráfico de datos, dado por el progreso digital que se encuentran el segmento corporativo, es necesario una solución para que se adapten al cambio de la conectividad y servicios de la nueva era. Uno de los grandes problemas de las redes WAN tradicionales es que se deben emplear equipos con una gran capacidad de memoria, este factor repercute directamente en la velocidad de acceso a la información. Todo esto se puede solucionar con las redes definidas por Software, dando control en la nube, dicho plano de control brinda una alta disponibilidad de las redes WAN existentes.

1.4. Justificación del problema

El aumento de redes y la necesidad de los clientes corporativos de expandirse y alta demanda de usuarios está dejando en evidencia las restricciones de las redes WAN actuales, con equipos físicos limitados con características no actualizables lo que provocaría una gran inversión en equipos físicos. Por estos motivos este trabajo se realizara en orden práctico debido que las redes definidas por software ayudaría a los clientes corporativos en la ampliación de características, reducción de espacios donde puedan administrar la información mucho más rápido, con un tiempo de respuesta progresiva.

1.5. Objetivos del problema de investigación

1.5.1. Objetivo general

- Realizar el modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo.

1.5.2. Objetivos específicos

- Identificar los fundamentos teóricos para reconocer la arquitectura, funcionamiento y beneficios del SD-WAN para crear un ambiente virtualizado de manera eficaz.
- Diseñar una WAN utilizando redes definidas por software de alta disponibilidad.
- Evaluar el rendimiento de una red SD-WAN a comparación de una red WAN.

1.5.3. Hipótesis

Utilizar las redes definidas por software en las redes WAN para el sector corporativo, aumentaría la disponibilidad y flexibilidad de la red, reduciendo la cantidad de equipos y saturación a nivel lógico de las redes. Un íntegro análisis de las redes definidas por software proveerá una alta disponibilidad en la red.

1.6. Metodología de investigación

En este trabajo de titulación se utilizará la metodología explorativa - experimental. Es explorativa por motivo que se estudiara sobre las redes definidas por software en base a los problemas existentes a nivel corporativo la cual exige de un amplio estudio de conceptos y realización de análisis explorativo; es experimental puesto que se utilizará una simulación y pruebas con equipos físicos para resolver el problema planteado.

CAPÍTULO 2

FUNDAMENTACIÓN TEÓRICA

2.1. Redes de Comunicación.

La red de comunicación son un grupo de periféricos de una red que se comunican entre si dando como resultado un sistema que te tiene como objetivo en difundir y compartir datos, información y recursos mediante el núcleo de una red.

Para lograr una comunicación o convergencia entre el conglomerado mundo de los dispositivos de red es necesario un protocolo red que permitan múltiples acuerdos y normas para llegar a realizar el intercambio de información, permitiendo una operabilidad en dispositivos de red sin importar la marca/modelo de un fabricante en especial. En la actualidad la evolución de las redes avanza a pasos agigantados de tal manera que la transmisión de información multimedia y datos se da en una red de comunicación creando una convergencia que brinda ventajas a nivel económico y de gestión de la red. Las redes de comunicación pueden llegar a clasificarse según su cobertura y alcance la cual tenemos redes PAN, redes LAN, redes MAN y redes WAN.

2.1.1 Red PAN

Red de Area Personal o según su significado en sus siglas en ingles Personal Area Network (PAN), es un tipo de red de comunicación entre múltiples dispositivos usadas de manera personal.

La red PAN es el claro concepto de una red centralizada hacia los usuarios finales dado por su alcance limitado, normalmente esta red tiene un alcance máximo de 10 metros.

2.1.2 Redes LAN

Red de área local o Local área network (LAN), es una red que puede interconectar de manera física múltiples periféricos de red dando como resultado

el intercambio de datos entre ellos. Esta red tiene una corta cobertura, pero es de mayor alcance que una Red PAN.

(Stallings, 2004) refiere que en la actualidad las redes LAN han evolucionado hasta transformarse en redes de alta velocidad que dependen del puerto (Fast ethernet, Gigabit Ethernet), el método de acceso, estándar y el canal físico (Fibra óptica, cable coaxial STP) para realizar las trasmisiones de alta velocidad. En la actualidad los puertos de alta velocidad se han expandido hasta tener velocidades de TenGigabit hasta FortyGigabit Ethernet estos puerto son usados para transmisión de información que requieran altos ancho de banda como ejemplo el *core network* del ISP.

Tabla 2.1: Características de redes LAN de alta velocidad.

	Fast Ethernet	**Gigabit Ethernet**	**Canal de Fibra**
Velocidad de datos	100 Mbps	1 Gbps, 10Gbps	100 Mbps - 3,2 Gbps
Medio de transmisión	UTP, STP, Fibra óptica	UTP, Cable apantallado, Fibra Óptica	Fibra óptica, cable coaxial, STP
Método de acceso	CSMA/CD	Conmutado	Conmutado
Estándar	IEEE 802.3	IEEE 802.3	Asociación del canal de fibra

Fuente: (Stallings, 2004)

Se puede observar en la tabla 2.1 las características físicas de las redes LAN, para altas velocidades según las interfaces físicas tanto en FastEthernet, GigabitEthernet o el canal de fibra.

2.1.3 Redes MAN

Red de Area Metropolitana (MAN) son redes que se ubican en múltiples edificios distribuidos en el medio urbano, regularmente una red MAN tiene como esquema base las redes LAN compartiendo una misma área geográfica. Este tipo de redes tiene como función conectar varios servicios para control urbano, tales como semaforización, seguridad a nivel metropolitano como lo muestra la figura 2.1.

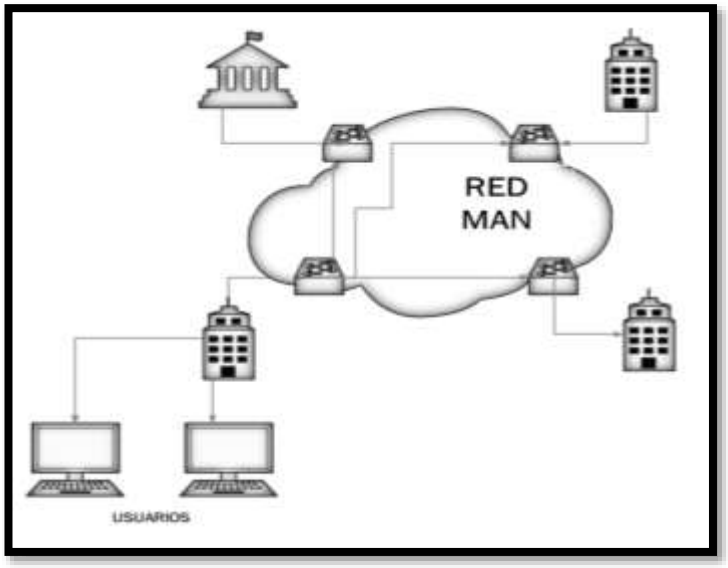


Figura 2. 1. Esquema básico de red MAN.
Elaborada por: Autor.

2.1.4 Redes WAN

Red de Area Amplia (WAN) son redes que se pueden distinguir a las anteriores habladas, debido a sus diferentes configuraciones y alcance de la red. Este tipo de redes involucra a las interconexiones entre equipos terminales u otras redes alejadas entre sí a nivel geográfico.

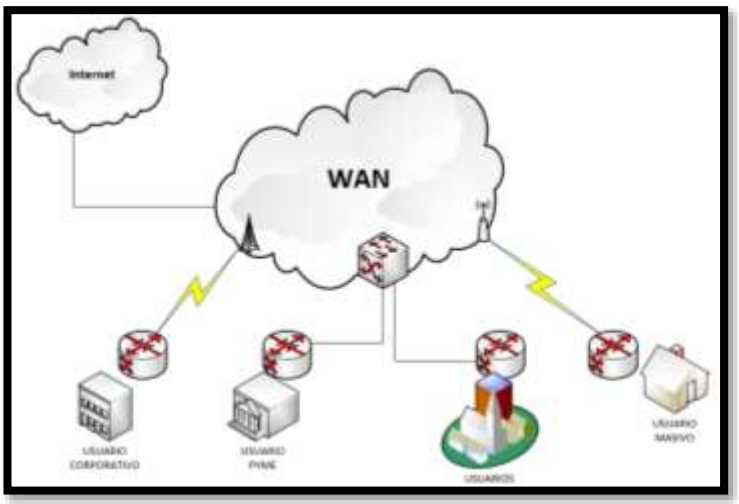


Figura 2. 2 Esquema de red WAN
Elaborada por: Autor.

En la figura 2.2 se puede observar un esquema de una red WAN básica donde se ve la necesidad de crear una infraestructura especial, debido a que

necesita nodos de conmutación y equipos físicos de gran capacidad para soportar el gran volumen del tráfico de datos. En gran mayoría este tipo de redes contiene cuantiosos medios de transmisión que se logran interconectar entre los enrutadores, si llega el caso que 2 o más enrutadores que no tienen relación con el medio o línea de transmisión, pero quieren conectarse, deberían hacerlo por otro tipo de transmisión, como enviando información a enrutadores intermedios creando así las subredes de almacenamiento y envió. Las redes de área amplia tienen como principio fundamental la conmutación de paquetes, este tipo de conmutación es método de agrupación de la información enviada por la red compuestas por un encabezado e información.

2.1.5 Redes Centralizadas

La distribución de las redes se puede dar en diferentes formas de agrupación y distribución de la información. La red centralizada es un tipo de distribución en un punto final, esta mantiene los datos en un solo ordenador/ubicación, para acceder a esta información se debe realizar en el computador centralizado (servidor).

Este tipo de distribución ya se ha implementado en las trasmisiones televisadas, debido que la información de emite de múltiples lados por diferentes medios pero se recibe en un punto como la televisión, este tipo de red como se muestra en la figura 2.3 donde se puede observar la emisión múltiple.

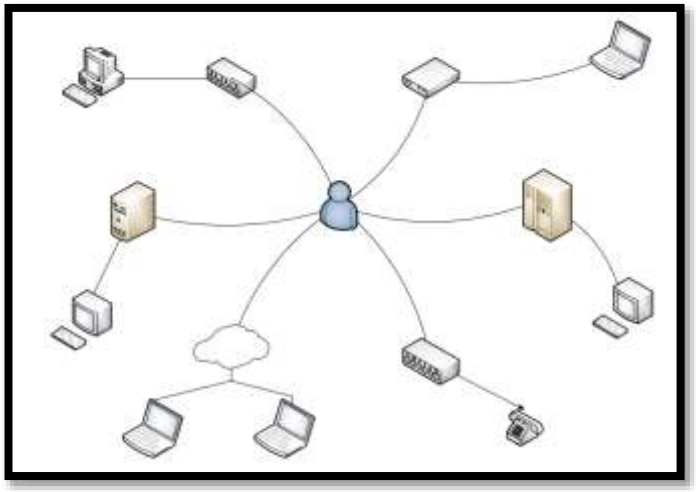


Figura 2. 3 Ejemplo de Red Centralizada
Elaborada por: Autor.

2.1.6 Redes descentralizadas

La red descentralizada es un tipo de distribución donde no existe un punto único, creando nodos colectivos, esta mantiene los datos en diferentes puntos, para acceder a esta información se debe realizar en cualquier nodo colectivo la cual el requerimiento de información pasara por un nodo central donde se distribuye a otros nodos. Este tipo de distribución ya se ha implementado en las páginas de información como Wikipedia, donde no es necesario tener un periférico único para poder agregar información y distribuirlas hacia los demás puntos.

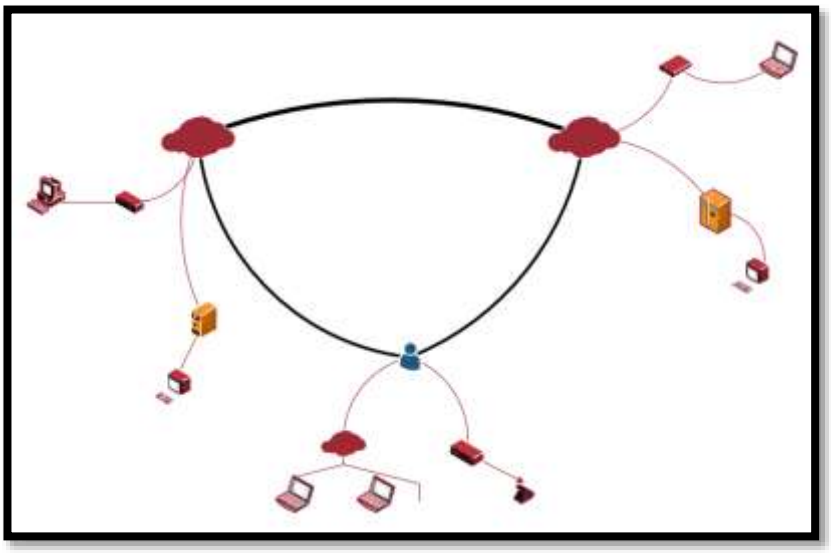


Figura 2. 4 Ejemplo de red descentralizada
Elaborada por: Autor.

2.1.7 Redes distribuidas

La red distribuida tiene como característica especial la ausencia de un nodo central o colectivo. Estos puntos se unen entre si dependiendo la dirección donde es emitida o enviada la información, acoplándose a la red para agilizar la transmisión.

Esta red transforma a los receptores finales en emisores y viceversa, como ejemplo el internet que es una gran fuente de emisión y recepción de información, la desconexión de un nodo nunca se aísla en caso desconexión.

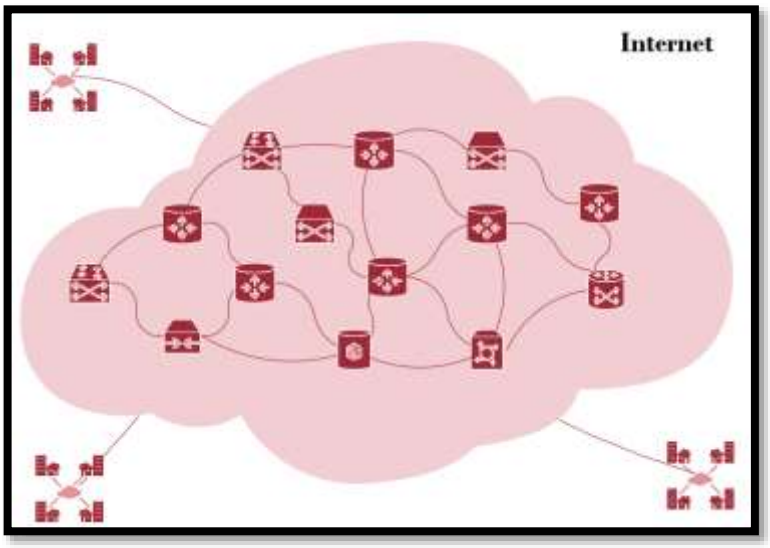


Figura 2. 5 Ejemplo de Red Distribuidas
Elaborada por: Autor.

2.1.8 Redes privadas VPN

Una VPN (*Virtual Private Network)* es una tecnología de seguridad que se aplica a las redes de comunicación que se utiliza para conectar de manera cifrada entre 1 o más dispositivos final a una red privada. Este es un recurso muy utilizado en el segmento corporativos.

Estas redes son muy utilizadas actualmente debido al avance de los modelos de negocios en sector corporativo, ya que hace posible la navegación en redes públicas evitando ataques de man in the middle.

Las VPN se conecta a un servidor donde crea una ruta segura y cifrada punto a punto que no puede ser violada ni si quiera por personas que tienen acceso al equipo.

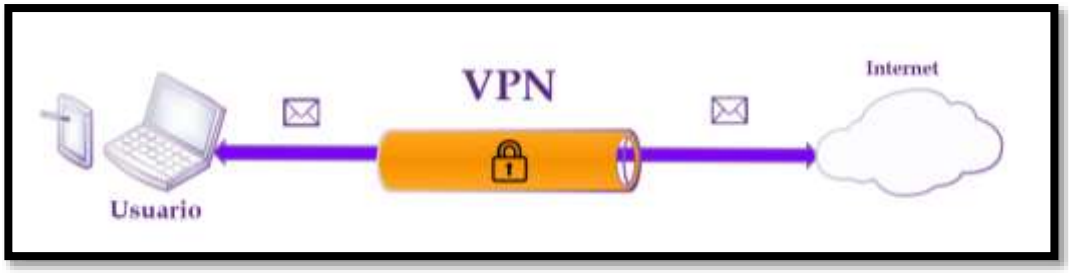


Figura 2. 6 Esquema de VPN
Elaborada por: Autor.

2.1.8.1 Tipos de VPN

Las VPN tienen varios tipos según su conexión y su arquitectura entre ellas tenemos.

2.1.8.1.1 VPN de acceso remoto

Este tipo de VPN es el modelo más usado ya que consiste en usuarios que se conectan hacia el destino desde cualquier punto remoto, usando como único vínculo el internet.

Este tipo de VPN puede igualar a la velocidad de una LAN, pero tiene como ventaja que es compatible a la mayoría de dispositivos y fácil de configurar. También tiene desventajas como seguridad comprometida o falla con el Firewall.

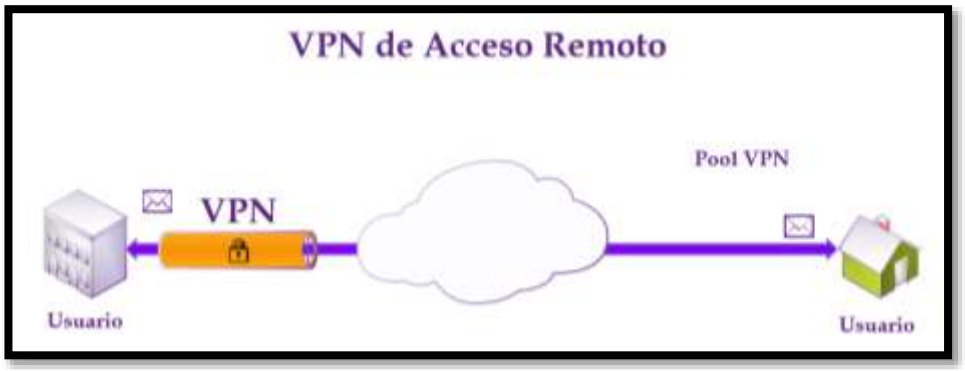


Figura 2. 7 Esquema de una VPN en acceso remoto
Elaborada por: Autor.

2.1.8.1.2 VPN punto a punto

Este tipo de VPN se lo considera solo para el uso de sector corporativo ya que utiliza para interconectar oficinas de manera remota entre cede principal y sucursales.

Esta establece por medio de un túnel VPN conectándose por medio de internet, esto permite conectarse por medio de un ISP, esto elimina las conexiones punto a punto tradicionales, dando una rápida conectividad muy parecida a una conexión punto a punto, este tipo de VPN suele ser la mas utilizadas en las empresas pero también suele ser usadas en el hogar.

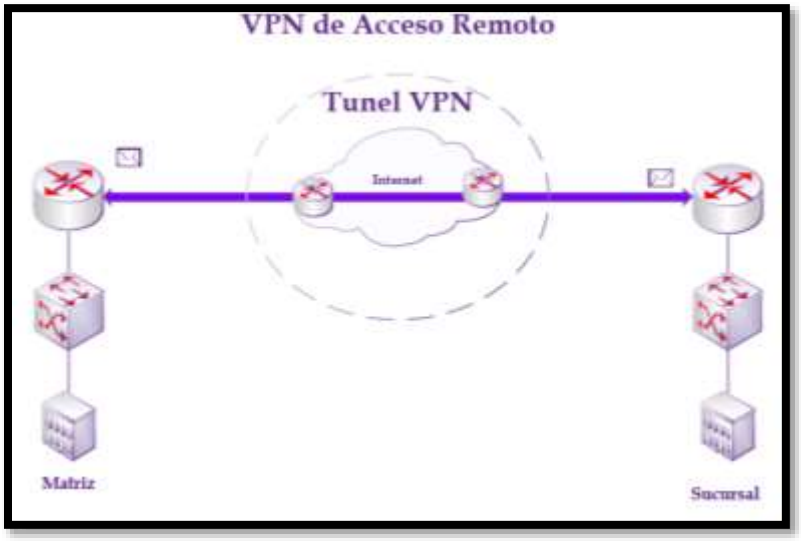


Figura 2. 8 Esquema de VPN punto a punto
Elaborada por: Autor.

2.1.8.1.3 VPN *over* LAN

Este tipo de VPN es el menos conocidos pero es uno de los más poderosos para utilizar en una empresa, este es una variante VPN de acceso remoto, pero este no usa el internet como interconexión, pero solo se emplea en una LAN de la empresa. Se las usa para dar seguridad en las redes inalámbricas.

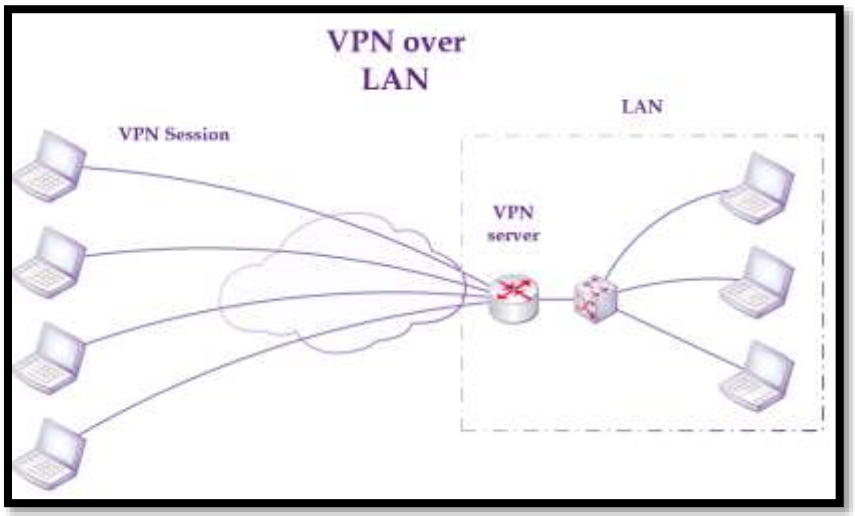


Figura 2. 9 Esquema de VPN over LAN
Elaborada por: Autor.

2.2. Arquitectura de protocolos.

La arquitectura de protocolo es el método de agrupación por capas o niveles para la organización de las redes. La cantidad de capas, su identificación y función difieren de cada arquitectura. Los niveles de cada arquitectura tienen como propósito principal ofrecer servicios hacia los niveles superiores.

Este método es importante para realizar el intercambio de información y datos entre terminales diferentes teniendo en cuenta unas tareas adicionales como la identificación y preparación del usuario destino al momento de recibir los datos, esta tarea adicional la realiza la capa N la cual tiene como objetivo mantener la comunicación con la otra capa N de la maquina destino.

La capa N es la que establece las reglas y protocolos utilizados para realizar la comunicación colectiva para la otra capa N, realizando un acuerdo entre las partes implicadas.

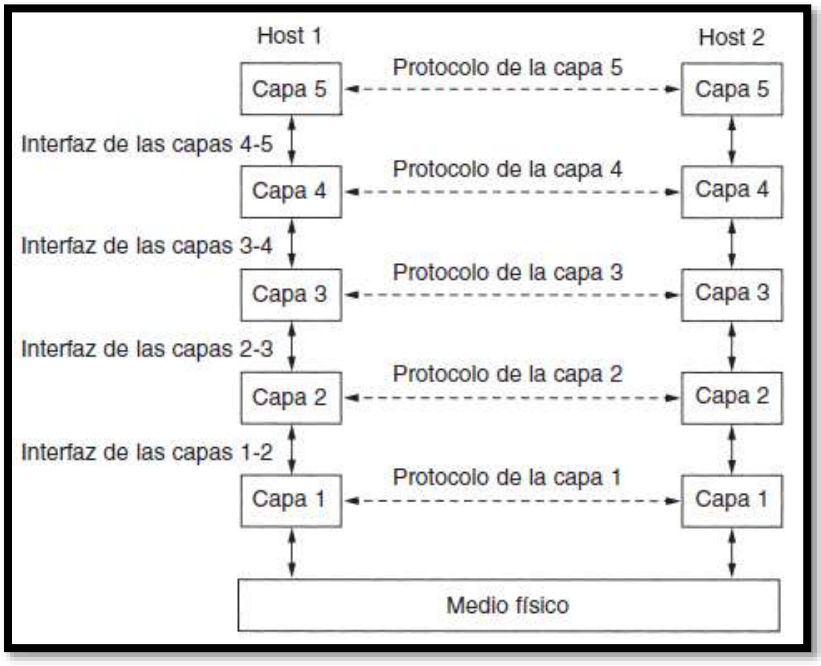


Figura 2. 10 Esquema de interface entre capas y protocolos.
Fuente: (Tananbaum, 2003)

Cabe recalcar que los datos no se comunican entre capa n de un dispositivo a otra capa n del dispositivo final, la forma de comunicación se da por medio de la capa inferior transmitida por el medio físico hacia el destino. Dependiendo del modelo de referencia dependerá la cantidad de capas.

2.2.1. Modelos de Referencias.

Los modelos de referencia son contemplaciones visuales que facilitan la comprensión de las múltiples arquitecturas de redes utilizados en la los sistemas de redes para la intercomunicación de dispositivos.

2.2.1.1. Modelos de Referencias OSI

Los modelos de referencia OSI, fue el modelo basado en una propuesta desarrollado por la Organización Internacional de Estándares, como uno de los principales pasos para realizar un esquema internacional para las arquitecturas de varios niveles. Este modelo se nombró como OSI (Interconexión de sistemas abiertos) de la ISO.

El modelo OSI es la referencia básica de las arquitecturas para las conexiones entre diferentes sistemas, esta normativa consta con 7 diferentes niveles por la cual debe pasar la información.

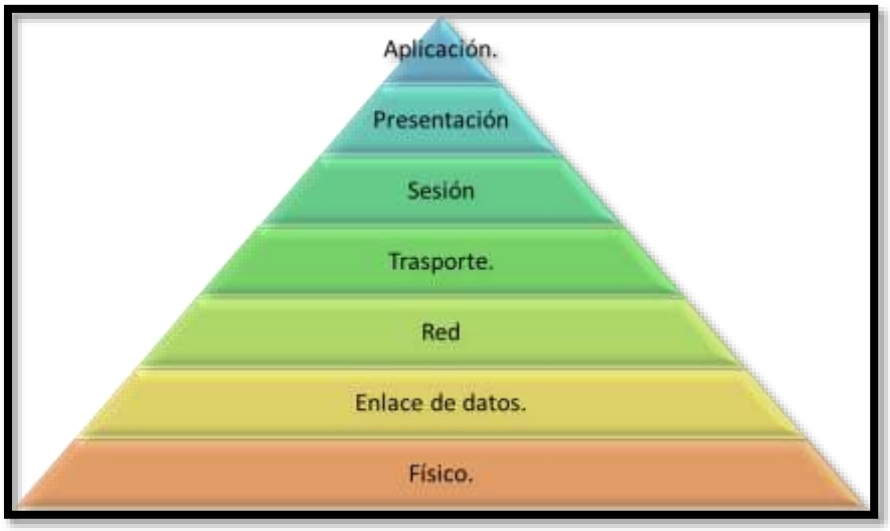


Figura 2. 11 Modelo OSI
Elaborada por: Autor.

- Capa Física: Es la que se encarga de la transmisión de información de manera binaria por medio de un canal de comunicación, la velocidad de transmisión depende de las interfaces mecánicas y los diferentes medios de físicos.

- Capa Enlace de Datos: Su función es transformar un medio en una línea de comunicación capaz de ser llevada a la capa superior. En esta capa los datos de entrada se agrupan formando tramas de datos que son enviadas secuencialmente donde cada terminal envía una trama de respuesta si la recepción fue exitosa.

- Capa de Red: Se ocupa del control de la subred. Realiza el encaminamiento de los paquetes del inicio hasta el final. En esta etapa se encuentra los dispositivos de encaminamiento como *routers* y *switches*.

- Capa de Transporte: Es la capa que provee un canal para enviar mensajes entre dos procesos que se comunican. Tiene control *end to end* (extremo a extremo), ósea esta capa es la que negocia con el destino la forma de comunicación y fragmentación de la información.

- Capa de sesión: Tiene como función organizar y sincronizar el intercambio de mensajes, controlar los procesos de comunicación.

- Capa de presentación: Esta capa corresponde a la estructura de la información proporcionando una sintaxis y la semántica de los datos.

- Capa de aplicación: Esta capa es la comunicación directa entre dispositivo y usuario proveyendo servicios y uso de aplicación como la extensión de HTTP al momento de entrar al internet.

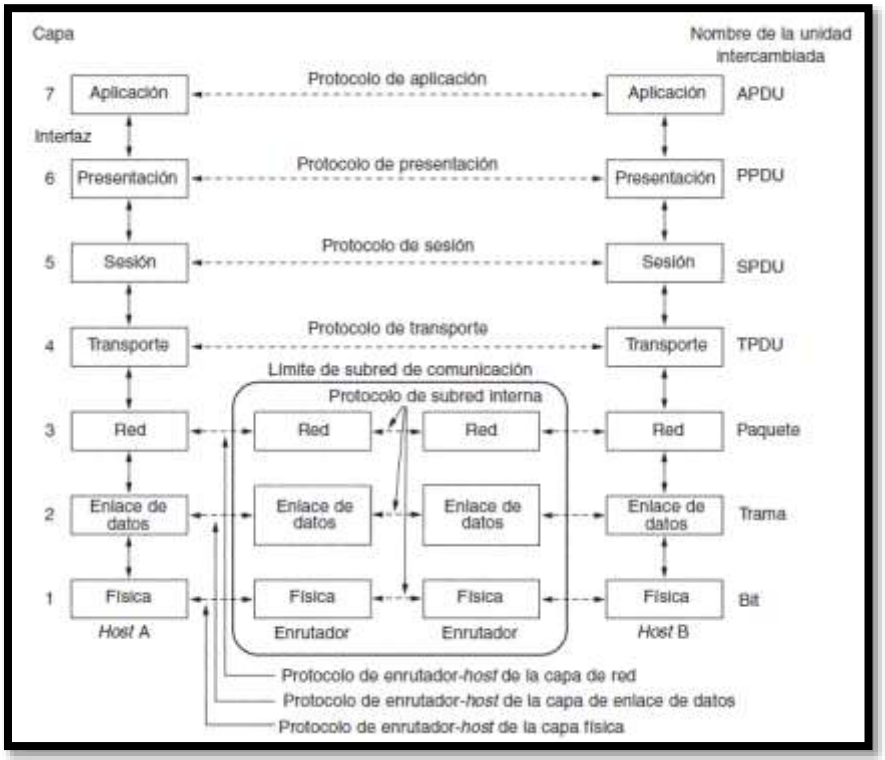


Figura 2. 12 Modelo de referencia OSI
Fuente: (Tananbaum, 2003)

2.2.1.2. Modelos de Referencias TCP/IP

Este Modelo vio la luz junto con el ARPANET de la mano de sus creadores (Cerf y Kahn) diseñado para respaldar a los equipos enrutadores y los Gateway entre las diferentes redes. Este modelo esta estructurado por 4 niveles en arquitectura, teniendo importación los protocolo que los niveles que los componen.

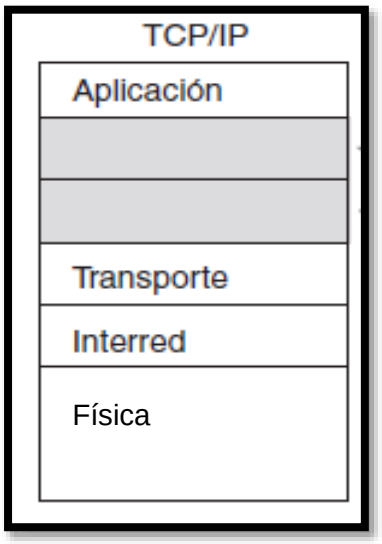


Figura 2.13 Modelo de referencia TCP/IP
Fuente: (Tananbaum, 2003)

- Capa física: esta capa es encargada de la interfaz del medio físico. Donde se describe las especificaciones de la transmisión de datos.

- Capa de Interred: En esta capa se encuentra todos los requerimientos de red para realizar el enrutamiento. Tananbaum, (2003) señalan que “el trabajo de esta capa es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente)” (p. 42).

- Capa de transporte: Esta diseñada para permitir que los hosts puedan comunicarse, de igual manera que el modelo OSI, esta se guía por la estructura Ethernet IEEE 802.2

- Capa de Aplicación: Esta capa tiene muchas similitudes con el modelo OSI, donde contiene los protocolos de nivel alto como él (TELNET) usada para terminales virtuales, (FTP) transferencia de archivos, (SMTP) correo electrónico.

2.2.1.2.1. Comparación entre modelos OSI y TCP/IP

Entre los modelos de referencias tienen muchas similitudes entre sí. Los dos toman como referencia la agrupación de protocolos independientes en formas de capas. La capa de transporte y aplicación tienen las mismas funciones.

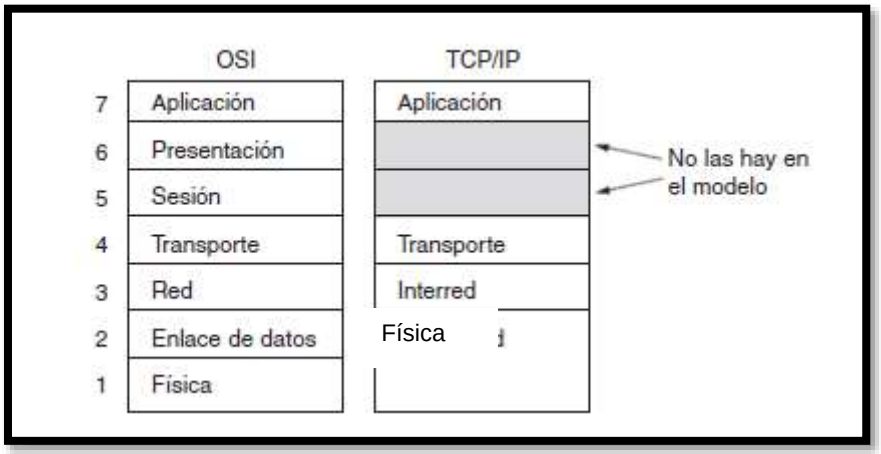


Figura 2.14 Comparación entre modelo OSI y TCP/IP
Fuente: (Tananbaum, 2003)

A pesar de sus similitudes, estos modelos tienen una diferencia en las capas inferiores. Como el TCP/IP combina algunas capas como enlace y física. La mayoría de las aplicaciones usadas en la actualidad usan el modelo de referencia de TCP/IP. La diferencia mas importante que el Modelo TCP/IP utiliza como protocolo para reducir la congestión el protocolo IPv4 y IPv6.

2.2.1.3. Protocolo IP SEC

El protocolo IPsec (*Internet Protocol security*) es el protocolo que tiene como función la seguridad de los datos en la comunicación usando el protocolo de internet (IP), la cual esta autentica y cifra cada paquete en un flujo de datos. IPsec también incluye protocolos de llaves tipo cifrados. Los protocolos de IPsec solo funcionen en el nivel 3 tomando como referencia el modelo OSI. Otros tipos de protocolos de seguridad operan de la capa de aplicación (capa 7 del modelo oSI). Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP.

2.3. Redes definidas por Software

Las rede definidas por software (SDN) es una opción diferente al momento de crear una red de telecomunicaciones la cual se desprende de una gran parte del control de un equipo físico y otorgándole la responsabilidad a un software o controlador virtual.

El termino de SDN (Software Defined Network o red Definida por software) se ha venido utilizando en los últimos años para dar entender que las arquitecturas se pueden desprenderse de plano de control y datos para crear redes más flexibles a nivel de programación y automatización realizando una virtualización de la red donde esta se independiza de la infraestructura existente.

SDN elimina la agudeza de las redes habituales que usan hardware capaces de tomar decisiones en un servidor. Esta tecnología separa las funciones de la capa de enlace de datos como el control de la información, automatizándola de manera que esta se vuelva independiente sin necesidad de un hardware o software especial que aumenten el costo de la red y reduciendo la dificultad al momento de gestionar la red.

Figuerola, (2013) señala que “En una red definida por software, un administrador de red puede darle forma al tráfico desde una consola de control centralizada sin tener que tocar conmutadores individuales” (p. 2). El administrador de la red puede cambiar las condiciones o reglas de los conmutadores cuando sea necesario creando un control y administración de manera detallada por paquetes.

Este tipo de administración de una red daría como resultado ventajoso una mayor flexibilidad, facilidad de gestión y rápida programación. Esta solución sería un anexo hacia el auge de los *Data Centers* y el *Cloud* ya que con la solución de SDN reduciría la cantidad de equipos físicos. En la actualidad los operadores de data center y empresas proveedoras de servicios de *cloud* están viendo como una nueva solución del SDN.

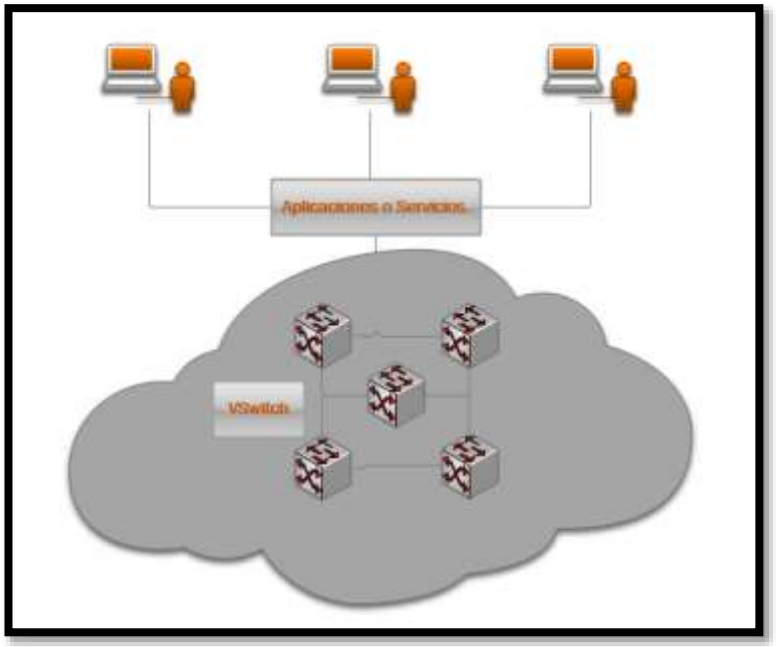


Figura 2. 15 Esquema Básico de SDN.
Elaborada por: Autor.

Los requerimientos básicos para la creación de una infraestructura SDN es que deben ser programables de manera sencilla entre otras importantes como:

- Automatización: se debe dar en nivel avanzado la cual debe reducir gastos operacionales y ayudar de manera inmediata al momento de diagnosticar problemas.

- Soporte: Control y manejo de servicios basados en la nube, dando control con respecto direcciones, topología, enrutamiento y seguridad.

- Flexibilidad: Manejo total de configuración de dispositivos a tiempo real.

- Virtualización de la red: Realizar una migración de las redes hacia las nubes con sus componentes como *Routers* a *Vrouters*.

2.3.1. Arquitectura de las redes definidas por software.

Las arquitecturas básicas de este tipo de redes son basadas en lo conceptos formales de la Ingeniería en Software. Este tipo de redes esta fraccionada en múltiples procesos como la configuración, exclusividad o priorización de los recursos de la red y el enrutamiento del camino según

elhardware, esta subdividida en 3 arquitecturas básicas: Aplicación, control y datos.

Esta arquitectura está definida por unas *APIs (*Aplicaciones de enlaces entre programas y aplicaciones). Los mecanismos principales de las infraestructuras son:

- Plano de Datos: Es la parte donde se encuentran componentes físicos y virtualizados de la red. Su propósito es crear el enrutamiento del trafico eliminando la inteligencia relativa de los equipos de encaminamiento tradicional.

- Plano de control: Es la parte encargada de las decisiones acerca del enrutamiento del tráfico. Este es la parte principal del SDN, verifica los requerimientos de la red para dar respuesta inmediata a las prioridades de ancho de banda y QoS (*Quality of Service)*.

- Plano de aplicación: Es la parte donde se encuentran todas las aplicaciones de red necesarias todas observadas por medio de las APIs.

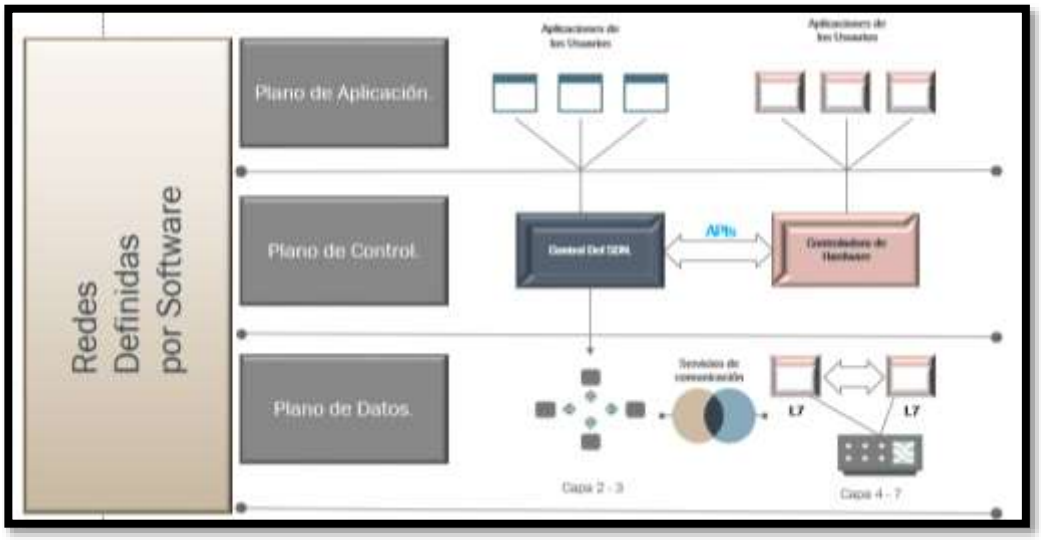


Figura 2. 16 Arquitectura de las SDN
Elaborada por: Autor.

2.3.2. Seguridad en las redes definidas por Software.

Las SDN están acaparando el mundo de las telecomunicaciones de una forma ágil la cual da inicio a un debate sobre la cantidad de retos con respecto a la seguridad de las SDN, tomando en cuenta que los diferentes planos estarán en una nube y su tecnología virtualizada. En la arquitectura de las SDN existe

varios tipos de seguridad, en el plano de control según su funcionamiento si detecta una falla o anomalía lo que hace la red enrutar hacia el controlador de las SDN la cual tendrá una visión general de los problemas dando una eficiencia en la seguridad, Con respecto a los otros planos existe el protocolo de *OpenFlow,* la cual crea reglas de encaminamiento para evitar elementos externos de la red.

Más allá de la arquitectura básica de SDN, el despliegue de una seguridad robusta es todavía un área que requiere gran estudio. Se cree que, además, sin un incremento significativo en cuanto a la seguridad en SDN se refiere, el paradigma solo conseguirá adaptarse en infraestructuras privadas y en despliegues autónomos de organizaciones. (Jimenez Moreno, 2018, p.26)

2.3.3. Protocolo *OpenFlow*

El *OpenFlow* es un protocolo de comunicación utilizado de manera exclusiva en las interfaces de las redes definidas por software entre crea una comunicación entre conmutadores de la red para dirigir los paquetes hacia un destino. Este protocolo usa reglas de encaminamiento que pueden ser agregadas o eliminadas según el servicio, así otorgando una flexibilidad a la red.

El OpenFlow fue creado en la fase de desarrollo del SDN con el fin de realizar el intercambio de información entre usuario final y la controladora del OpenFlow en su plano de control luego de eso la información regresa hacia la controladora de la SDN y hacia los elementos a el plano de datos.

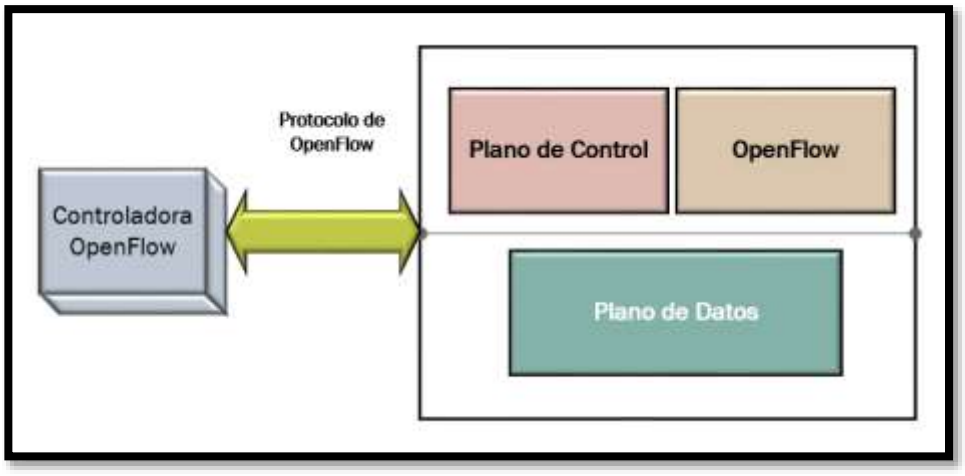


Figura 2.17 Esquema de intercambio de información en OpenFlow.
Elaborada por: Autor.

La controladora del *OpenFlow* se comunica con los conmutadores de los planos de control y datos por medio el protocolo de *OpenFlow,* esto permite usar la red de manera eficiente usando los recursos de una red tradicional. A nivel corporativo el uso de *OpenFlow* por medio de una Máquina Virtual ha crecido por la facilidad de movilidad y flexibilidad que puede otorgar el uso del SDN.

El objetivo fundamental de crear el *OpenFlow* es dar una ruta alternativa a los protocolos tradicionales, mediante modelos y esquemas basados en *software*. Este tipo de protocolos permite la convergencia de los recursos de la red con las redes existentes.

2.3.4. Funcionamiento del *OpenFlow*

Anteriormente se ha mencionado, OpenFlow ofrece múltiples ventajas que ayudan a la implementación y desarrollo de las redes, pero existe una interrogante que abunda el tema ¿cómo funciona? Por un lado, el plano de control funciona de manera independiente del switch, usando una controladora. Esta controladora se interconecta entre diferentes *Switches* lo que da como resultado una red más centralizada.

Esta controladora, puede configurarse acoplándose a un conjunto de reglas para cada switch, con el fin de controlar y darle flexibilidad al tráfico. Una vez establecida la conexión entre el *switch* y el controlador, se puede dar el intercambio de información entre ellos, crear condiciones de entrada en su tabla, gráficos estadísticos del tráfico o controlar sus características y parámetros, etc.

(Jiménez Moreno, 2018) afirma que “La parte fundamental del OpenFlow son las tablas de flujos. Debido que cada flujo está conformado por los diferentes campos de la cabecera, estos se emparejarán paquetes (match), contadores, que llevan los valores de los paquetes emparejados y acciones, que serán aquellas llevadas a cabo una vez se produzca el match.”(P.28)

OpenFlow tiene como beneficio principal que brinda una extensa cantidad campos a utilizar como: puertos de entrada, direcciones *Ethernet* , identidad o prioridad *VLAN,* direcciones origen y destino IPv4, prioridad IPv4, tipo de servicio *IPv4*, puertos de origen y destino *TCP o UDP*, tipo/código *ICMP*,...También se podrán utilizar las direcciones origen y destino Ipv6 en versiones de *OpenFlow* 1.2 o superiores.

Con respecto a contadores existen varios tipos: por tabla, por cola, por grupo, por flujo, por puerto, por conjunto de grupos,... Los más usados son los contadores por tabla, flujo y puerto. Con los contadores por tabla, se podrá llevar la cuenta de las entradas activas, las búsquedas llevadas a cabo en la tabla para cada paquete y el número de emparejamientos para cada paquete.

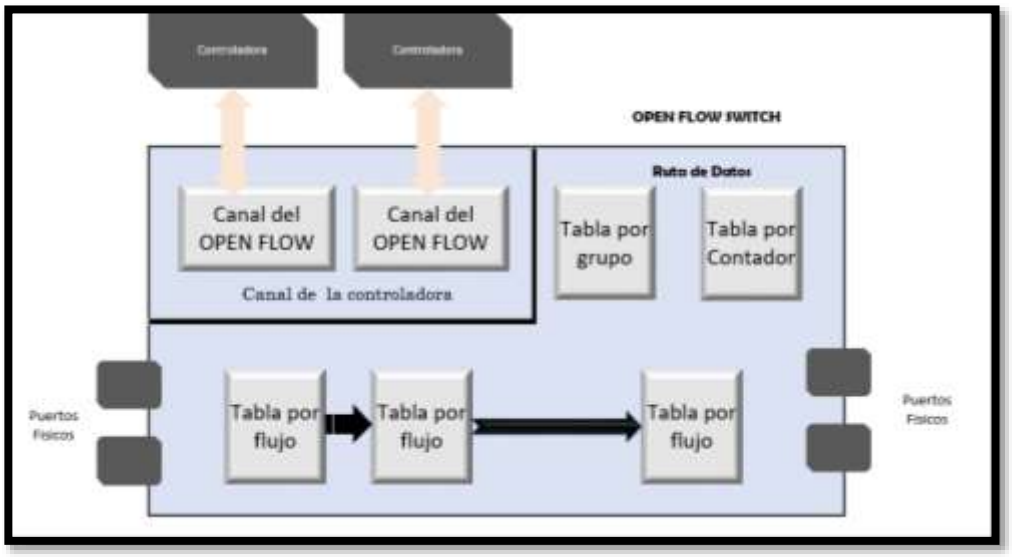


Figura 2. 18 Esquema Funcional del OpenFlow
Elaborada por: Autor

2.3.5. Estandarización de OpenFlow (ONF) .

El *OpenFlowSwitching Consortium* fue creado en 2008 con el objetivo de popularizar y acentuar en el mundo de las telecomunicaciones el protocolo OpenFlow. En marzo de 2011, múltiples empresas como *Deutsche Telecom, Facebook, Google, Microsoft, Verizon y Yahoo* se han aliado para crear la *Open Networking Foundation (ONF)* con el fin de dar a conocer las redes definidas por *software* (SDN). Cualquier actividad relacionada con el proceso de estandarización se lleva a cabo en la ONF con respecto al SDN.

La ONF ha creado grupos de trabajo que conducen la estandarización técnica de *SDN/OpenFlow*, manteniendo charlas técnicas, realizando estudios de compatibilidad, preparando borradores que, de ser aprobados, pasan a formar parte de la especificación estandarizada.

2.3.6. *OpenFlow* en la actualidad.

Grandes empresas a nivel mundial han incluido este tipo protocolo en sus redes tradicionales, empresas como IBM, Google y HP han anunciado al inicio del año 2018 que sus redes pueden soportar el protocolo *OpenFlow.* La unión de estos protocolos ha aumentado el uso de VM (*Virtual Machine*) y las redes en IP de nuevas generaciones. Esto hace posible el uso de las máquinas virtuales en todos los lugares para el centro de datos.

2.3.7. SD-WAN

La inducción del SDN en las diferentes redes de comunicación, también se puede aplicar en a las redes de comunicación WAN, esta unión se la define como SD-WAN, es un mercado que está en pleno auge en el mercado mundial.

Dadas las grandes proyecciones sobre el auge del SD-WAN, han surgido múltiples de soluciones tecnológicas y ISP (*Internet Service Provider*) de proveen este tipo de tecnologías/ servicios y propuestas de valor alrededor de esta nueva tecnología.

Por otro lado, hay un gran número de proveedores de servicios que no disponen una tecnología propia, pero ofrecen servicios intermediarios como el SD-WAN gestionados, por medio de los mismos fabricantes.

En caso que una corporación o empresa desea dar el paso adelante en la evolución de sus redes de comunicación actuales, hacia una solución basada en SD-WAN, se va a encontrar con un sin número de soluciones tecnológicas.

El auge del SD-WAN como se lo ha descrito anteriormente, ha llegado a formar parte de la nueva transformación digital del segmento corporativo, lo que ha provocado que se precipite la evolución en las redes corporativas. La tecnología de SD-WAN da otro tipo de visión de las redes tradicionales las misma que fueron diseñadas de manera centralizada con bajos niveles de latencia. En la actualidad la mayoría de las aplicaciones están migrando hacia la nube, lo que ha inducido a que el tráfico de datos se enrute por vías indirectas provocando un bajo rendimiento de la red.

SD-WAN suele estar conformada con un pequeño equipo físico virtualizado que ejecuta su propio software esto entraría como cambio a las tradicionales redes costosas con equipos específicos que realizan una sola función.

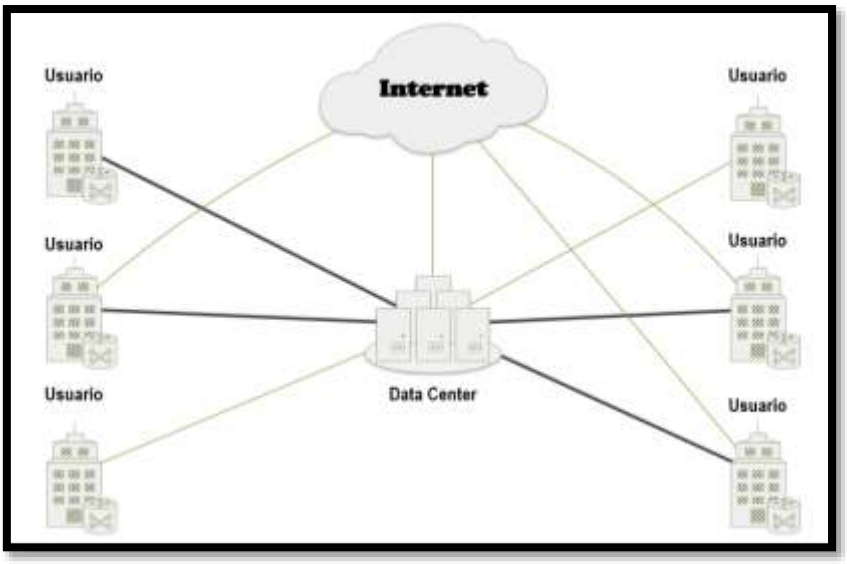


Figura 2. 19 Esquema básico de una red SD-WAN
Elaborada por: Autor

2.3.8. Soluciones SD-WAN

Las soluciones de esta tecnología teniendo en cuenta el origen del destino y de las aplicaciones, estas gestionan el tráfico de una forma diferente a los routers tradicionales, los cuales son completamente indiferentes al tipo de datos que transportan.

Pero el valor añadido que puede proporcionar a su negocio la implementación de soluciones SD-WAN va todavía más lejos. En concreto, una SD-WAN aporta:

- Un nuevo planteamiento para la conectividad de las sucursales que simplifica la infraestructura y supone un ahorro económico.
- Una manera de resolver los problemas de costo y rendimiento que plantean las conexiones con aplicaciones cloud públicas.
- La posibilidad de atender varios tipos de conexiones, desde redes VPN privadas a conexiones a internet locales.
- Mayor visibilidad y control.
- Posibilidad de asignación de rutas prioritarias a determinadas aplicaciones.
- Posibilidad de garantizar el rendimiento de las aplicaciones.

- Seguridad.
- Optimización de la WAN
- Posibilidad de elección de rutas más cortas o de mínimo costo.

2.4. Marco Regulador.

Tomando en cuenta de la inminente transición hacia las Redes definidas por Software, esto provocaría al sector corporativo unirse a esta transición junto a los ISP (*Internet Service Provider)*. El cambio de tecnologías de redes distribuidas a centralizadas la cual provocaría un cambio en los modelos de negocio basados en SDN. El proyecto de *OpenFlow* de aplicarlo como protocolo oficial para el uso del SDN.

2.4.1. Legislación y regulador

Como ente regulador principal se encuentra la IEEE *(Institute of Electrical and Electronics Engineers)*, siendo esta la mayor organización en la creación de estándares en el mundo relacionada con el desarrollo tecnológico, la misma que ha estado involucrado directamente en el desarrollo del SDN y aplicación en diferentes tecnologías tanto que puede estar en cualquiera de estos estándares.

Tabla 2. 2 Estándares regulatorios por parte de la IEEE

Estandar de la IEEE regulatorios	
IEEE P1903.1	*Standard for Content Delivery Protocols of Next Generation Service Overlay Network (NGSON).*
IEEE P1913.1	*Software-Defined Quantum Communication*
IEEE P1915.1	*Security for Virtualized Environments*
IEEE P1916.1	*Performance for Virtualized Environments*
IEEE P1917.1	*Reliability for Virtualized Environments*
IEEE P1921.1	*Software-Defined Networking Bootstrapping Procedures*
IEEE P1930.1	*SDN based Middleware for Control and Management of Networks*
IEEE P802.1CF	*Recommended Practice for Network Reference Model and Functional Description of IEEE 802 Access Network.*

Elaborada por: Autor

2.4.2. Estándar IEEE P1903.1

Este estándar de la Red de superposición de servicios de próxima generación (NGSON) describe un marco de los servicios basadas en el Protocolo de Internet (IP) y especifica el contexto (por ejemplo, el nivel de calidad de servicio que se requiere en un servicio (QoS), el tipo de servicio se da en tiempo real vs. datos, esto es dinámicamente adaptable (por ejemplo, usando información derivada localmente para descubrir, organizar y mantener el tráfico fluye en la red dentro de una red de área local) y capacidades de red autoorganizadas (por ejemplo, desarrollo de estructuras de red basadas en las necesidades de los clientes y las capacidades de las estructuras de red existentes), incluidos esquemas avanzados de enrutamiento y reenvío, y que son independientes de redes subyacentes.

2.4.2.1. Estándar IEEE P1913.1

Este estándar define el protocolo de comunicación cuántica definida por *software* (SDQC) que permite la configuración de puntos finales cuánticos en una red de comunicación para crear, modificar o eliminar dinámicamente protocolos o aplicaciones cuánticas.

Este protocolo reside en la capa de aplicación y se comunica a través del Protocolo de control de transmisión / Protocolo de Internet. El diseño del protocolo facilita la integración futura con las redes definidas por software y open Networking Foundation OpenFlow.

El estándar define un conjunto de comandos de configuración de dispositivos cuánticos que controlan la transmisión, recepción y operación de estados cuánticos. Estos comandos del dispositivo contienen parámetros que describen la preparación, medición y lectura del estado cuántico.

2.4.2.2. Estándar IEEE P1915.1

Este estándar define a la gran parte de las redes definidas por software (SDN) y la virtualización de funciones de red (NFV) aplicadas en las diferentes variedades de redes de comunicación, incluidas las redes móviles y de

computadoras. Este estándar define al SDN y NFV a nivel de hardware y software, la virtualización en todos los niveles de la red, la tenencia múltiple a través del control de recursos de múltiples usuarios la centralización del control y la capacidad de programación de cada tecnología .

Queda una pregunta clave: ¿cómo las redes virtualizadas y definidas por software proporcionan un cambio de paradigma en la forma en que las aplicaciones y los servicios están diseñados e interactúan con estas redes? Es necesario evaluar el impacto en los usuarios finales, la red y los proveedores de servicios. Existen varios aspectos técnicos que afectan varios elementos de la red relacionados con SDN y NFV. Se deben abordar varias áreas clave para la estandarización a fin de acelerar la adopción de redes que evolucionan con SDN y NFV.

2.4.2.3. Estándar IEEE P1916.1

Este estándar especifica el marco de rendimiento que incluye características, métricas, requisitos, modelos y casos de uso para redes definidas por software y virtualización de funciones de red (SDN / NFV).

2.4.2.4. Estándar IEEE P1917.1

Este estándar especifica el marco de confiabilidad, modelos, análisis y requisitos para Redes definidas por *software* y virtualización de funciones de red (SDN / NFV).

2.4.2.5. Actualidad de la regulación

Estas nuevas tecnologías aún no se han determinado en un estándar especifico de manera oficial , lo cual esto entra en un gran debate, este servicio aplica en el rango de SVA (Servicios de Valor Agregado). Debido a diferentes posturas, unas a favor que estén en el grupo de SVA, con argumentos de que este tipo de servicios son una innovación a toda a una red, tanto como para crear un nuevo sistema de redes; algo que a los fabricantes no defienden, mientras

que la postura contraria argumenta que la introducción del SDN en los diferentes tipos de redes de comunicación es el paso fundamental que necesita el hombre para avanzar tecnológicamente en el campo de las telecomunicaciones .

2.5. Packet Tracer

Es un programa de simulación de redes de telecomunicación de la empresa Cisco Systems, este simulador es usado para experimentar el comportamiento de la red. Este simulador es capaz de soportar protocolos de nivel de capa 7. Contiene los enrutamientos como RIP, OSPF y EIGRP pero este la capacidad de simular redes funcionales.

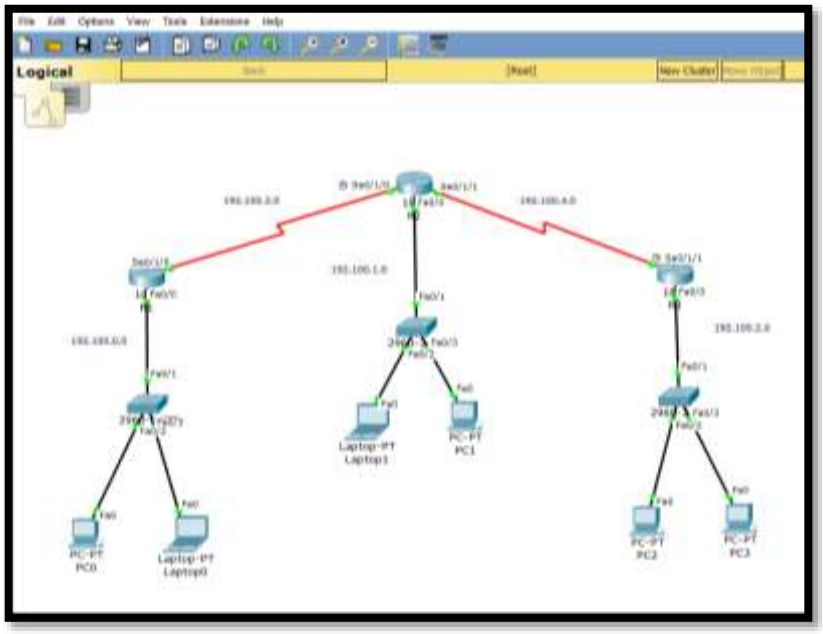


Figura 2.20 Pantalla principal de Cisco Packet Tracer
Elaborada por: Autor

Como se pude observar en la figura 2.20 programa goza con una facilidad al momento de crear una topología en modelo física de una forma simple, con solo arrastrando los dispositivos a la pantalla. Luego haciendo clic sobre ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IoS e incluso funciona la opción de completar con el tabulador un comando. Una vez completada la configuración física y lógica de la red, también se pueden hacer simulaciones de conectividad todo ello desde las mismas consolas incluidas.

CAPÍTULO 3:

DISEÑO, IMPLEMENTACIÓN Y RESULTADOS

3.1. Diseño de red WAN para el cliente

Para este diseño se creará una red WAN funcional para un cliente del segmento corporativo utilizando el simulador de redes *Packet Tracer*, creando una interconexión común en una empresa. Para efectos de prueba en este trabajo se usará el siguiente esquema de red.

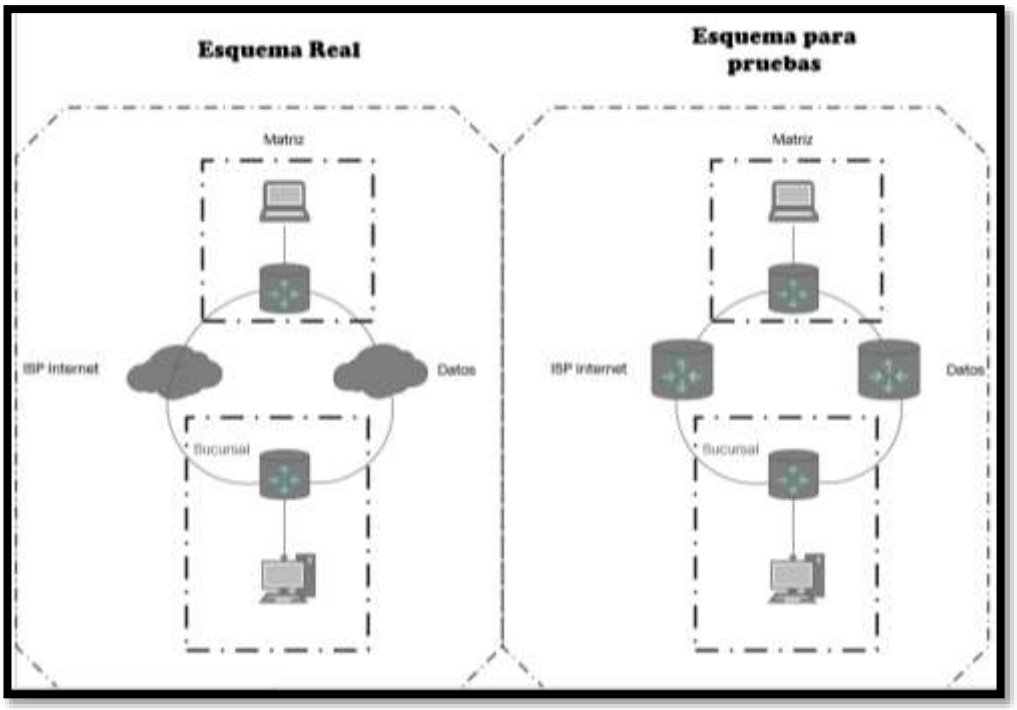


Figura 3.1 Esquema de Red WAN cliente
Elaborado por Autor.

En la figura 3.1 se encuentra el esquema inicial del cliente, pero para simular los ISP se coloca routers.

3.2. Diseño y pruebas de la red en Cisco Packet Tracer

Debemos elaborar la red WAN del cliente en el simulador de Cisco Packet Tracer.

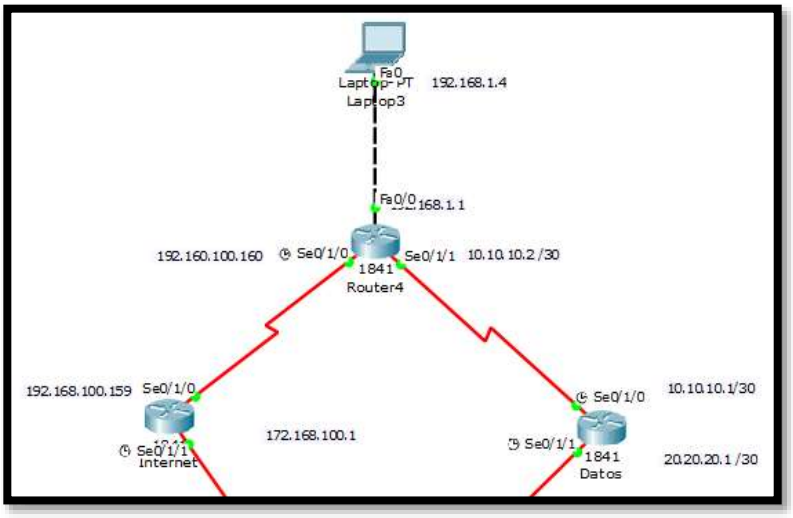


Figura 3. 2 Primera parte de la red WAN funcional del cliente
Elaborado por: Autor

En la figura 3.2 se observa las interfaces utilizadas como la Fa0/0 para laptop 3 con una ip de 192.168.1.4 y su gateway hacia el router 4 con la ip 192.168.1.1; el router 4 conectado hacia a los ISP, uno conectado por el puerto serial 0/1/0 con la ip 192.168.100.160 con el gateway del ISP “Internet” con una ip 192.168.100.159; otra interface del router 4 conectado hacia el ISP “Datos” por el puerto serial 0/1/1 con una ip 10.10.10.2 hacia su Gateway conectada en el puerto serial 0/1/0 con una Ip de 10.10.10.1

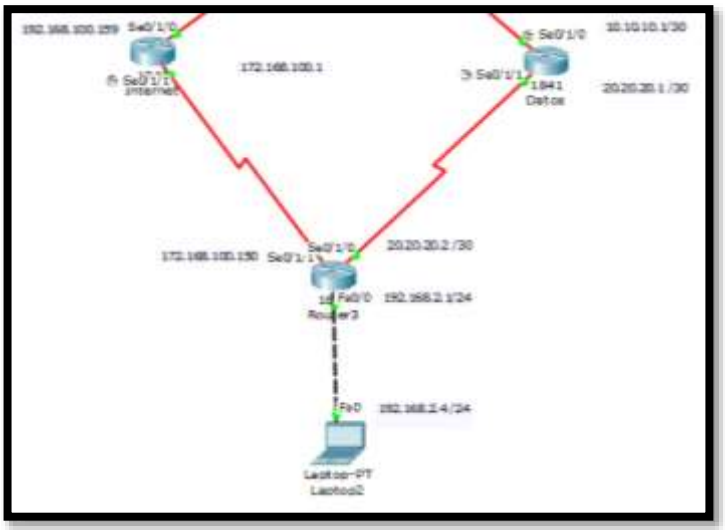


Figura 3.3 Primera parte de la red WAN funcional del cliente
Elaborado por: Autor

En la figura 3.3 se observa las interfaces utilizadas como la Fa0/0 para laptop 2 con una ip de 192.168.2.4 y su gateway hacia el Router 3 con la ip 192.168.2.1; el router 3 conectado hacia a los ISP, uno conectado por el puerto serial 0/1/1 con la ip 192.168.100.150 con el gateway del ISP “Internet” con una ip 172.168.100.1; otra interface del router 3 conectado hacia el ISP “Datos” por el puerto serial 0/1/0 con una ip 20.20.20.2 hacia su Gateway conectada en el puerto serial 0/1/1 con una Ip de 20.20.20.1. Realizamos las pruebas de conectividad entre cada punto.

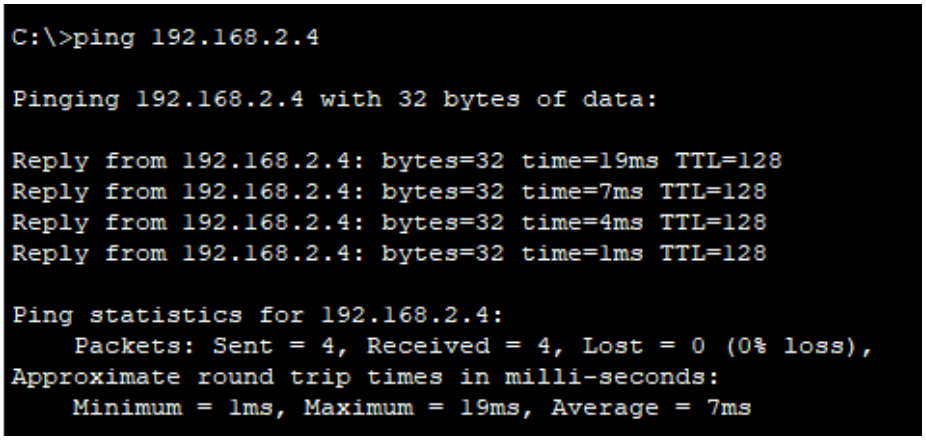


Figura 3. 4 Prueba de Ping a la Laptop 2.
Elaborado por: Autor

En la figura 3.4 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 192.168.2.4” para comprobar conectividad del equipo.

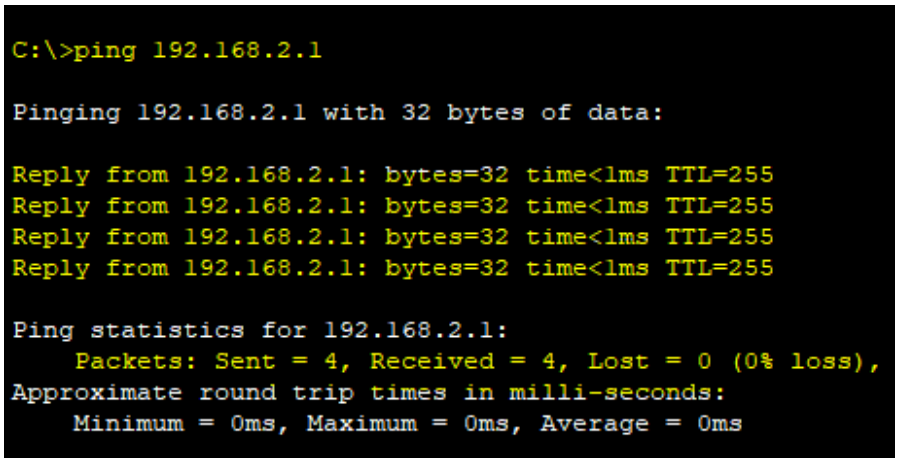


Figura 3. 5 Prueba de Ping al Gateway de Laptop 2
Elaborado por: Autor

En la figura 3.5 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 192.168.2.1” para comprobar conectividad del equipo y el ISP.

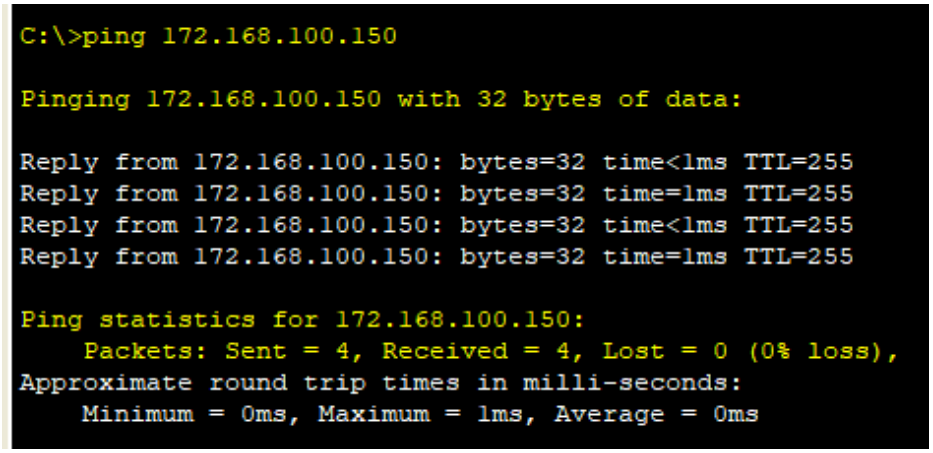


Figura 3.6 Prueba de Ping puerto Serial 0/1/1
Elaborado por: Autor

En la figura 3.6 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 172.168.100.150” para comprobar conectividad del equipo y con el gateway del ISP.

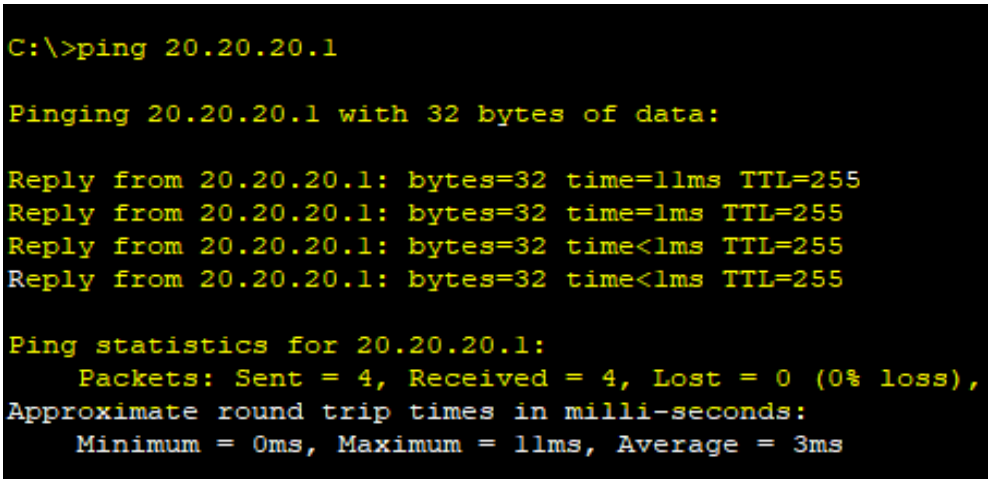


Figura 3.7 Prueba de Ping puerto Serial 0/1/0
Elaborado por: Autor

En la figura 3.7 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 20.20.20.1” para comprobar conectividad del equipo y con el gateway del ISP datos.

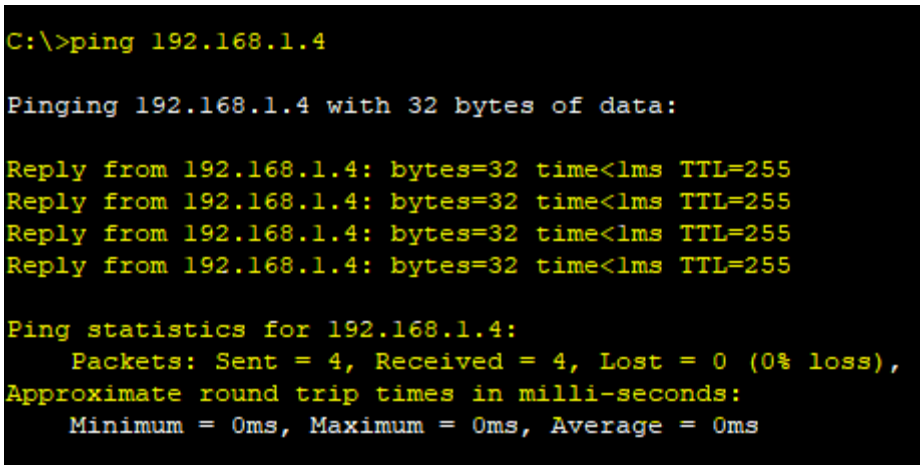


Figura 3. 8 Prueba de conectividad Laptop 3
Elaborado por: Autor

En la figura 3.8 en el CMD de la Laptop 3 del simulador, se ingresa el comando “Ping 192.168.1.4” para comprobar conectividad del equipo. Tras realizadas las pruebas de conectividad, se realizará pruebas en caso de caídas en cada caso. Se realiza una prueba conectividad antes de realizar una caída de un puerto.

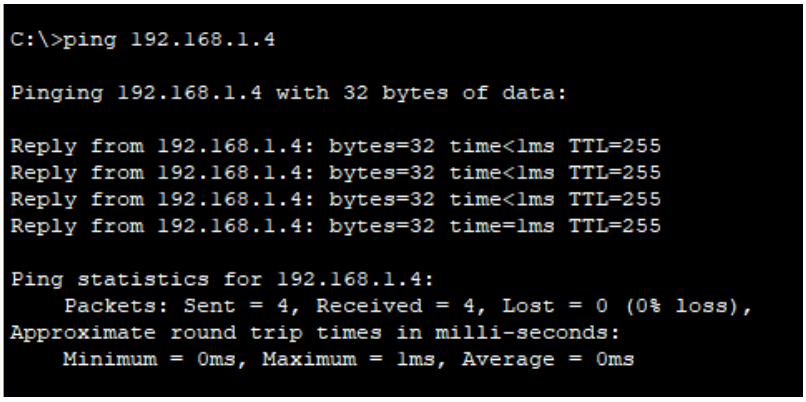


Figura 3. 9 Prueba de conectividad antes de desconectar
Elaborado por: Autor

En la figura 3.9 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 192.168.1.4” para comprobar conectividad a laptop 3. Tras eso se realiza la primera prueba de caída de red, se desconecta la red, en medio de la prueba de conectividad y se pierden paquetes, hasta que se reconecte.

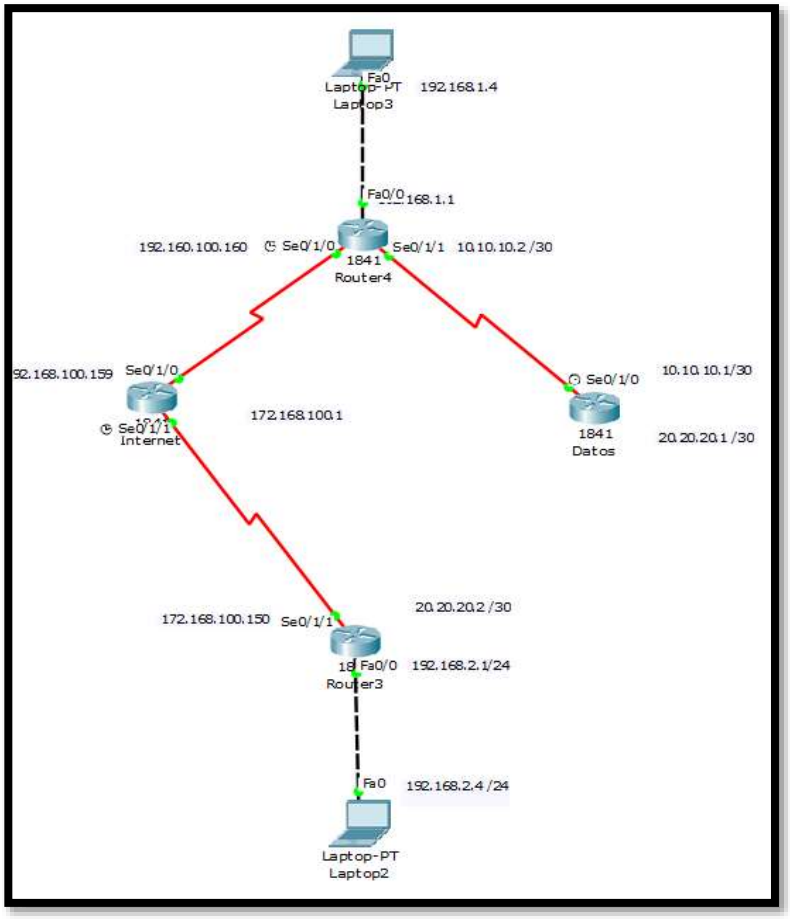


Figura 3. 10 Primera prueba de caída de red, diagrama de la red.
Elaborado por: Autor

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=255
Reply from 192.168.1.4: bytes=32 time<1ms TTL=255
Reply from 192.168.1.4: bytes=32 time<1ms TTL=255
Reply from 192.168.1.4: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 3. 11 Primera prueba de caída de red, configuración.
Elaborado por: Autor

En la figura 3.10 y figura 3.11 en el CMD de la Laptop 2 del simulador, se ingresa el comando “Ping 192.168.1.4” para comprobar conectividad a laptop 3, se observa una perdida de paquetes al momento de simular una caída en la interface Fa0/0.

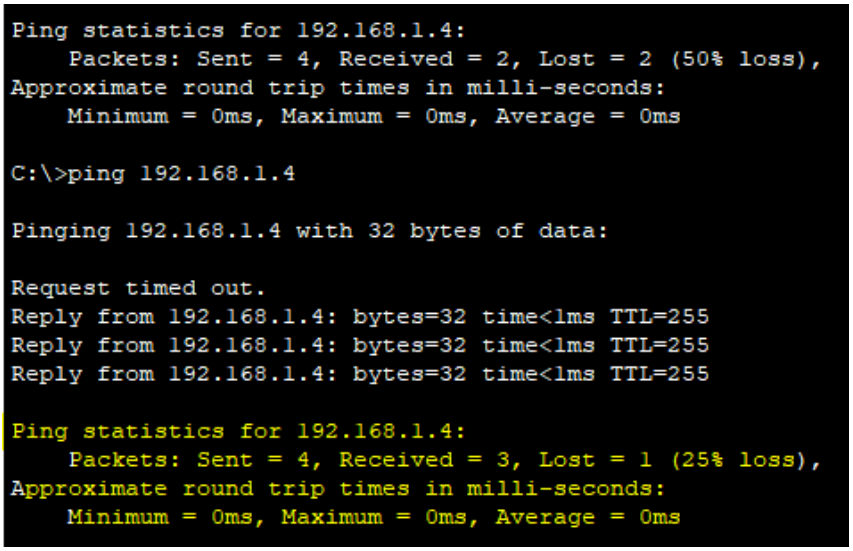


Figura 3. 12 Reconexión de la red.
Elaborado por: Autor

En la figura 3.12 se puede observar en el CMD, con otra prueba de conectividad, la red se vuelve a conectar pero existiendo perdidas de paquetes.

Este tipo de redes es común verlas en el segmento corporativo, pero en caso de una caída en las interfaces físicas, existe en una perdida significativa de paquetes y el tiempo de reconexión es pequeño, esto seria un gran problema en caso del uso de videoconferencias son paquetes que no se recuperan hace que la comunicación pierda calidad.

3.3. Implementación del SDN en la red WAN del cliente.

Para beneficio del trabajo, se utilizará equipos físicos para realizar pruebas que nos puede determinar tiempo real y el manejo de una Red SD-WAN desde su plataforma.

Para esta prueba se utilizará equipos de la empresa Fortinet (*Router Fortigate 80D* y *Router Fortigate* 60E) debido que estos equipos constan con una plataforma de creación de SD-WAN estable para todo tipo de casos.

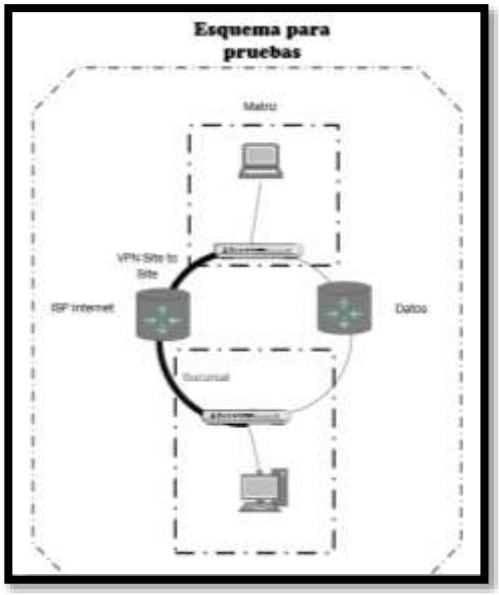


Figura 3. 13 Esquemas para red de implementación
Elaborado por: Autor.

En la figura 3.13 está el diseño de la red diagramado en Visio con los esquemas de los equipos Fortinet.

3.3.1. Configuración del equipo Fortigate 80D.

Se debe configurar primero el equipo Fortigate de la sucursal. El método de conexión es por medio cable consola, luego de eso se debe entrar en el modo de configuración. Luego programar los puertos con la IP designada, la descripción de cada puerto, los accesos de cada puerto y el rol de cada puerto.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.100.150 255.255.255.0
        set allowaccess ping https http fgfm capwap
        set type physical
        set alias "WAN"
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.10.100 255.255.255.0
        set allowaccess ping https http
        set type physical
        set alias "lan"
        set role lan
        set snmp-index 2
    next
```

Figura 3. 14 Configuración de los puertos en el router 80D
Elaborado por: Autor.

En la figura 3.14 se observa la configuración de los puertos 1 y 2 del FortiGate 80D. Ahora se debe configurar el puerto 3 de la misma manera que los anteriores.

```
FG080D3916003562 (port3) # show
config system interface
    edit "port3"
        set vdom "root"
        set ip 192.168.2.1 255.255.255.0
        set type physical
        set snmp-index 3
    next
FG080D3916003562 (port3) # set allowaccess ping https http
FG080D3916003562 (port3) # set mode static
```

Figura 3. 15 Configuración del puerto 3 en el router FortiGate 80D
Elaborado por: Autor.

En la figura 3.15 se observa la última parte de la configuración del puerto 3. Como siguiente paso se debe ingresar al gestor del equipo con la Ip configurada en el puerto 3 por medio de un navegador web colocando la siguiente dirección https://192.168.2.1.

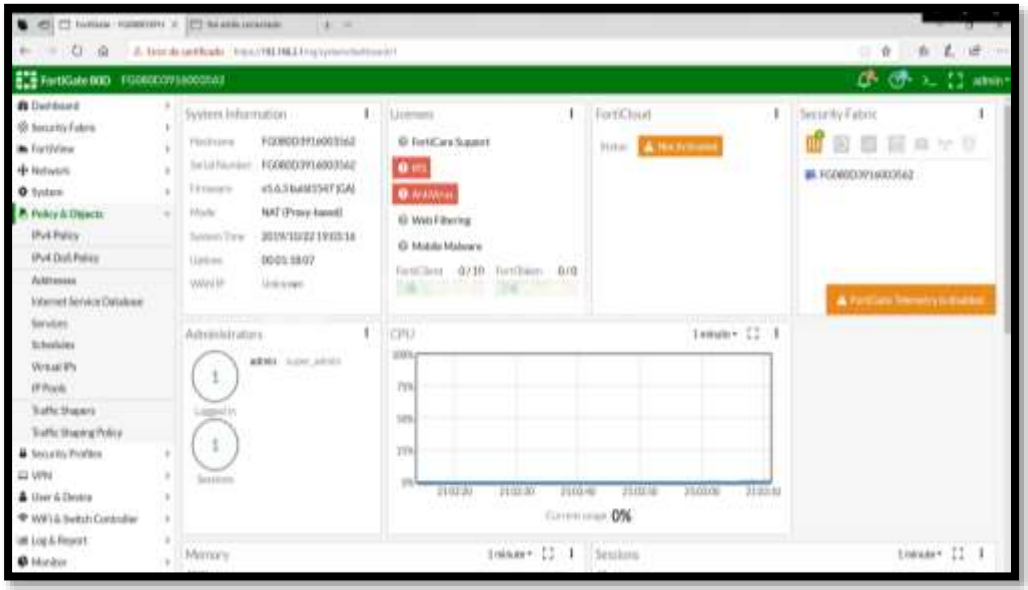


Figura 3. 16 Pantalla principal de un gestor
Elaborado por: Autor.

En la figura 3.16 se distingue en la pantalla principal, el análisis del equipo y la información del sistema. Ahora se debe configurar el puerto 3,

seleccionando la pestaña *Network*, luego a Interface y le asignamos el rol de LAN al puerto 3.

Figura 3. 17 Configuración del puerto 3
Elaborado por: Autor.

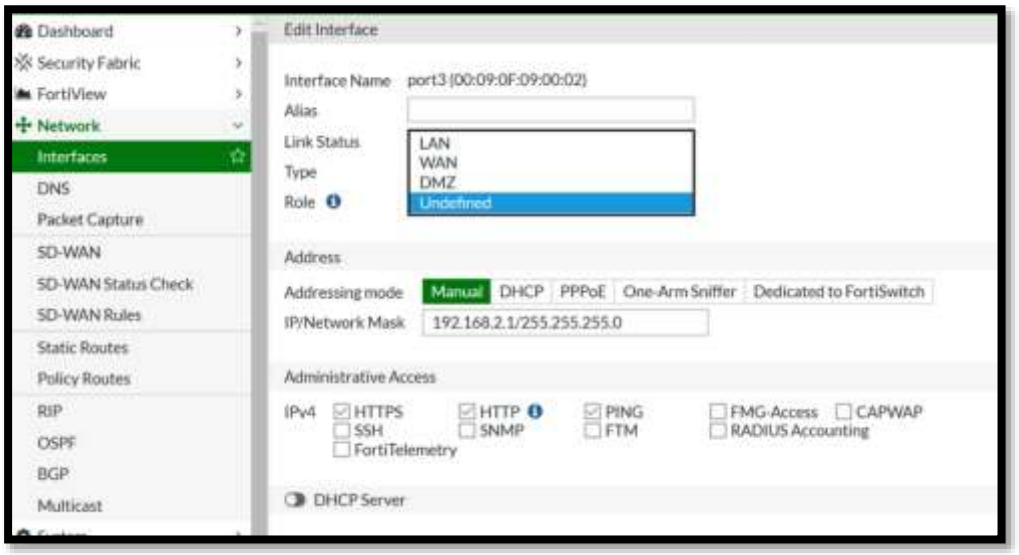


Figura 3. 18 Asignación de rol al puerto 3
Elaborado por: Autor.

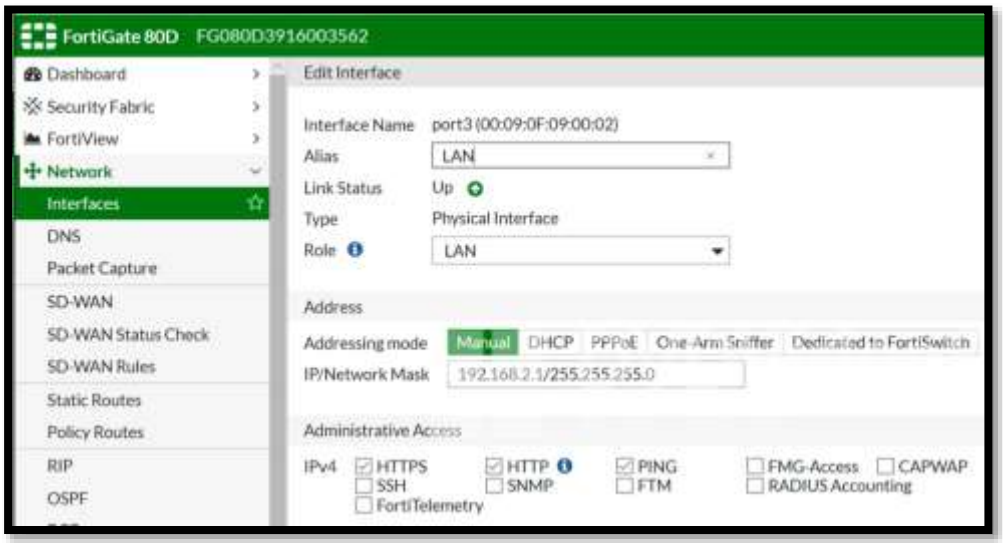


Figura 3. 19 Configuración final del puerto 3
Elaborado por: Autor.

En las figuras 3.17, 3.18 y 3.19 se define las configuraciones del tercer puerto . Después de eso se debe completar la configuración del puerto 1 y 2. Se debe seleccionar el aparatado de *Network*, luego a Interface y al fina se debe asignar el rol de WAN, el alias, el *addressing mode*, la IP con su máscara de red, los accesos permitidos.

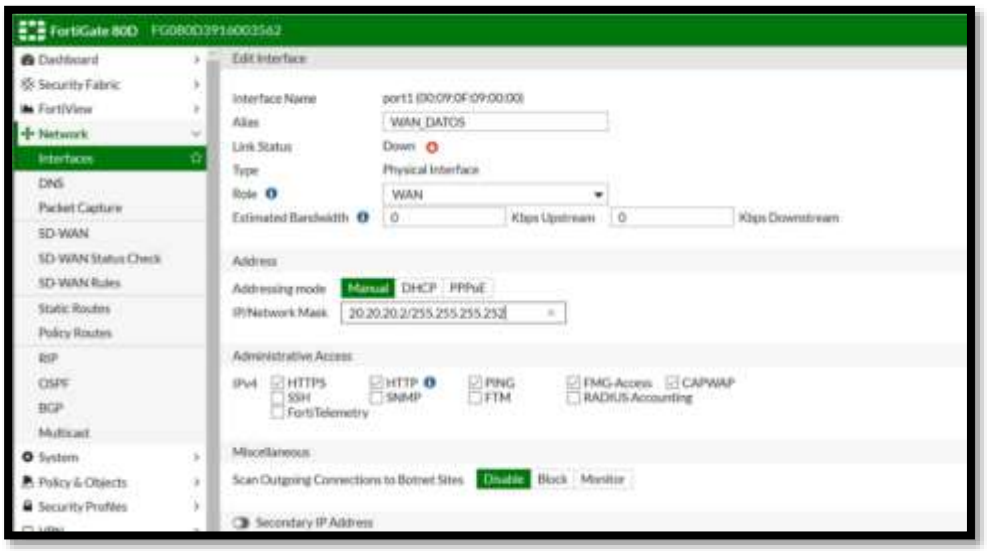


Figura 3. 20 Configuración del puerto 1
Elaborado por: Autor.

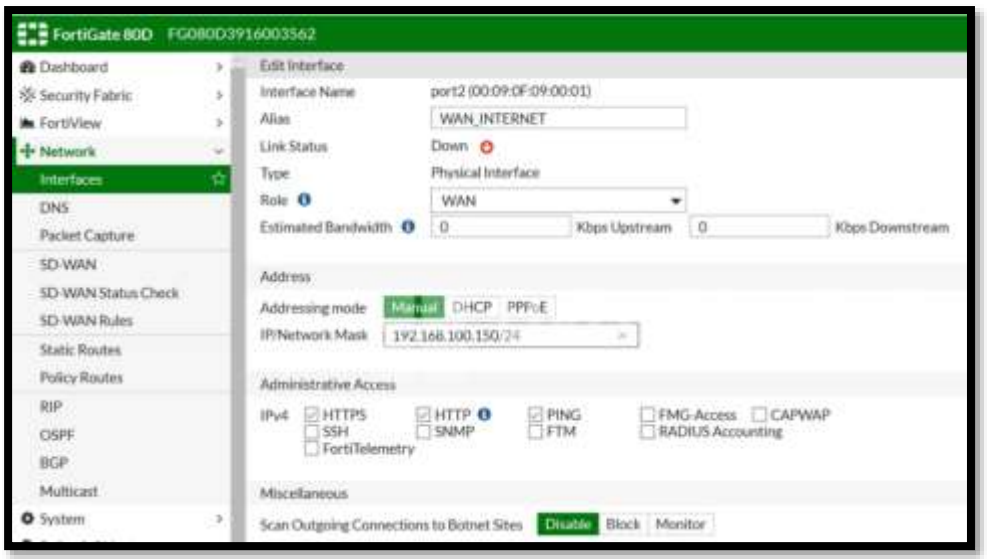


Figura 3. 21 Configuración del puerto 2
Elaborado por: Autor

.

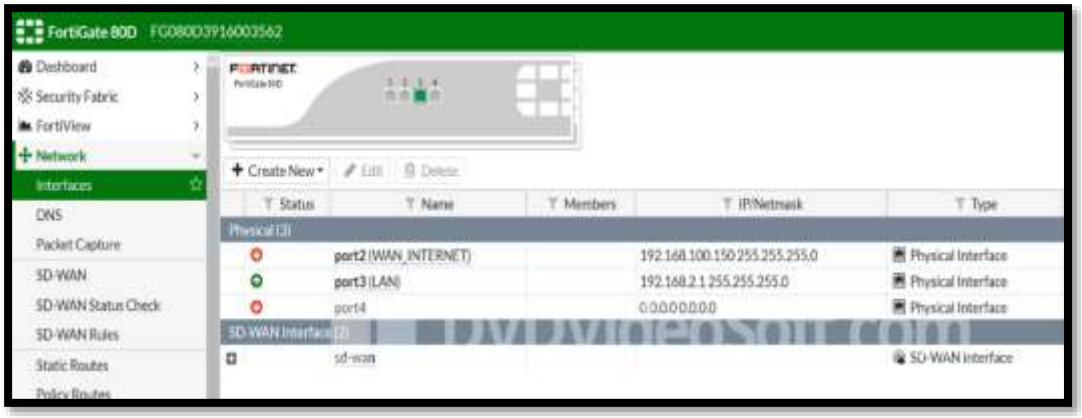


Figura 3. 22 Configuración final de todos los puertos.
Elaborado por: Autor.

En las figuras 3.20, 3.21, 3.22 se realiza la configuración de los puertos 1 y 2, tras realizar la configuración de los puertos se debe programar la *VPN Site o Site* o *VPN Ipsec*, seleccionando la pestaña de VPN luego la opción *Ipsec Wizzard*, configurando en la sección de *VPN Setup* el nombre de la VPN, el tipo y la configuración NAT como se puede observar en la figura 3.23.

Figura 3. 23 Pantalla de IPSec Wizzard sección VPN Setup
Elaborado por: Autor.

En la figura 3.23 se observa el menú principal del apartado de VPN Creation Wizard. Tras eso se debe configurar la sección de *Autentication* la *Ip Address*, la interfaz de salida, método de autenticación y la contraseña descrito en la figura 3.24 , luego en la pestaña de *Policy & Routing*, la interfaz local, la máscara de subred, las subredes remotas como se observa en la figura 3.25, al final se debe comprobar la información ingresada como se puede ver en la figura 3.26.

Figura 3. 24 Pantalla de IPSec Wizzard sección Autentication
Elaborado por: Autor.

Figura 3. 25 Pantalla de IPSec Wizzard sección Policy & Routing.
Elaborado por: Autor.

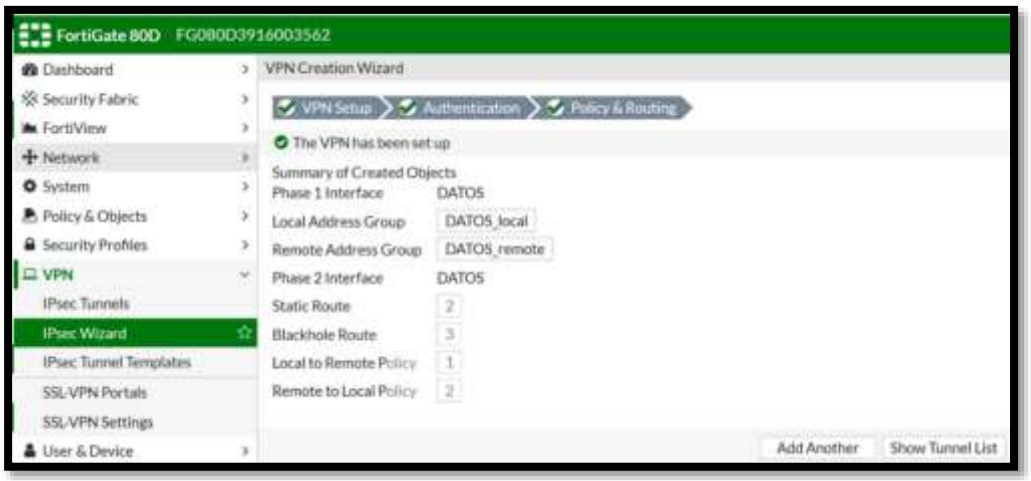


Figura 3. 26 Pantalla con la configuración final de IPSec Wizzard.
Elaborado por: Autor.

Como siguiente paso se debe revisar el estado de la *VPN site to site* seleccionando la opción de *Ipsec tunnels* como lo señala la figura 3.27.

Figura 3. 27 Pantalla con la configuración final de IPSec Tunnels
Elaborado por: Autor.

Ahora se debe configurar el apartado de SD-WAN del equipo. Se debe seleccionar la pestaña *network* luego la opción SD-WAN (en versiones anteriores el apartado de SD-WAN puede tener el nombre WAN Load Balance). Debe ser habilitada la interface en la parte de *Interface State,* luego se debe crear una nueva interface SD-WAN/ Wan LLB. Luego seleccionar la interface que va pasar por la SD-WAN, en este caso sería la interface de WAN_Datos luego se asigna el *gateway* correspondiente como indica la figura 3.28.

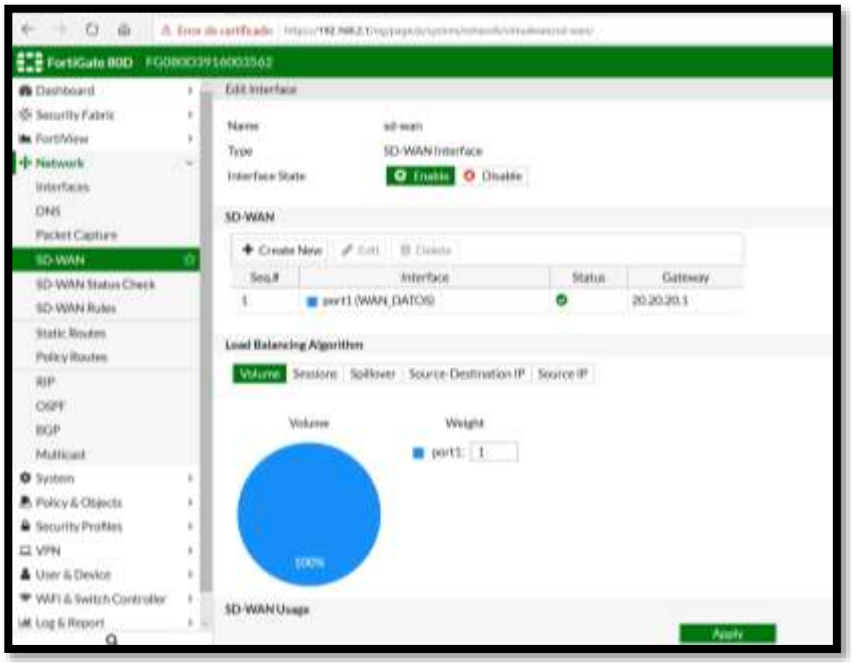


Figura 3. 28 Configuración de la opción SD-WAN.
Elaborado por: Autor.

Para dar la optimización de la red WAN del Cliente, se debe anexar a la SD-WAN la otra red conectada al equipo, en este caso sería la red de datos anteriormente creada como se observa en la figura 3.29.

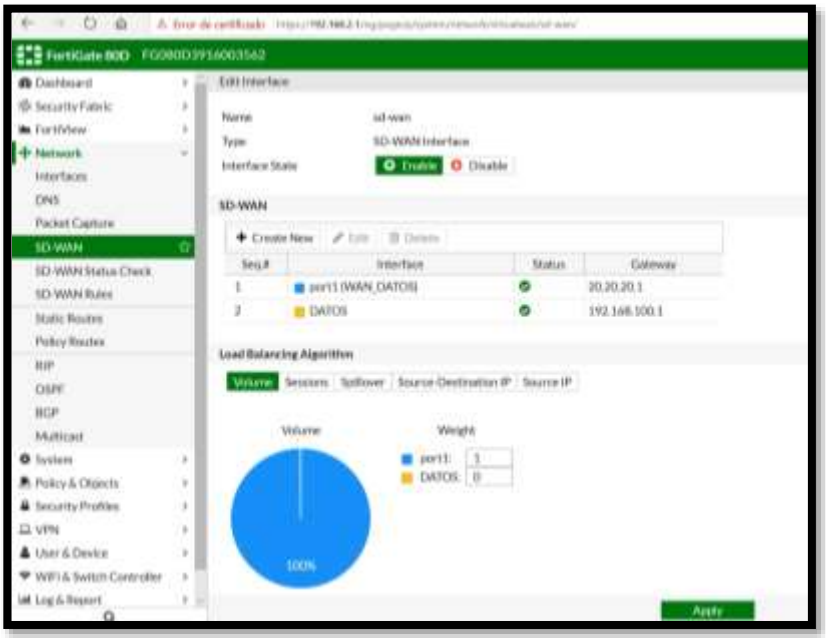


Figura 3. 29 Configuración de la SD-WAN y las interfaces.
Elaborado por: Autor.

Tras el paso anterior se debe establecer la ruta estática hacia el router que va simular la ISP esto se observa en la figura 3.30 en el apartado de *Static Routes*.

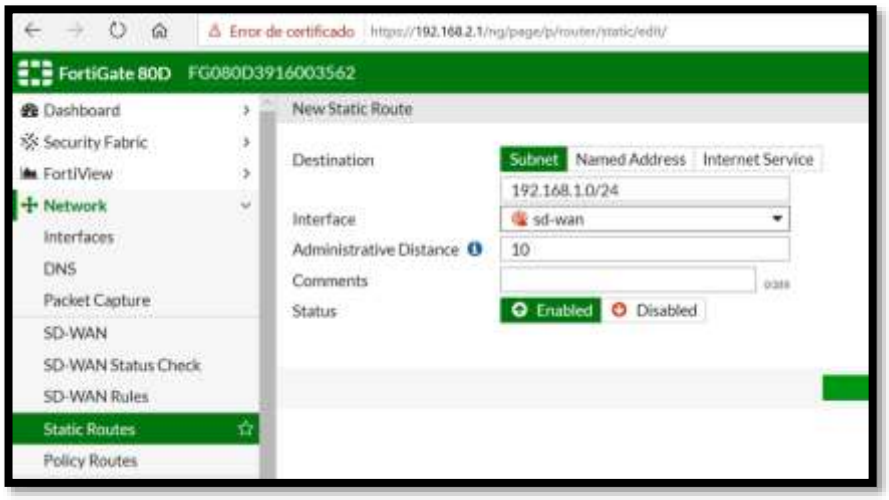


Figura 3. 30 Configuración de la ruta estática SD-WAN.
Elaborado por: Autor.

Como siguiente paso se configura las políticas de IPv4 para cada interface, este apartado se encuentra en la pestaña *Policy & Objets* como se puede observar en la figura 3.34 para definir las condiciones del tráfico, definir el tipo de datos transmitido, firewall, antivirus, las interfaces de entrada y salida. (Para este proyecto no se habilito el firewall y antivirus).

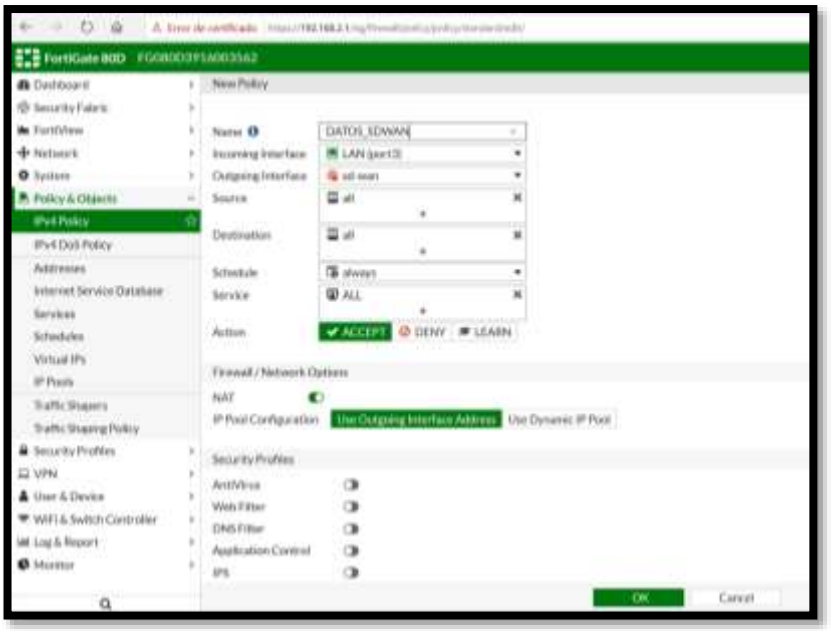


Figura 3. 31 Configuración de las políticas IPv4 del 80D
Elaborado por: Autor.

3.3.2. Configuración del equipo Fortigate 60E.

Como primer paso se configura el equipo Fortigate de la matriz. Usando el medio de cable consola se debe ingresar al equipo, luego de eso entramos al modo de configuración. Luego se programa los puertos con la IP designada, la descripción de cada puerto que vamos utilizar, colocando los accesos de cada puerto y el rol de cada puerto como se observa en la figura 3.32.

```
Config system interface
        edit "port3"
                set vdom "root"
                set ip 192.168.168.1.99 255.255.255.0
                set typr physical
                set snmp-index 3
```

Figura 3. 32 Configuración del equipo por modo consola del 60E
Elaborado por: Autor.

Ahora se debe ingresar al gestor del equipo con la Ip configurada en el puerto 3 por medio de un navegador web colocando la siguiente dirección https://192.168.1.99 como se grafica en la figura 3.33.

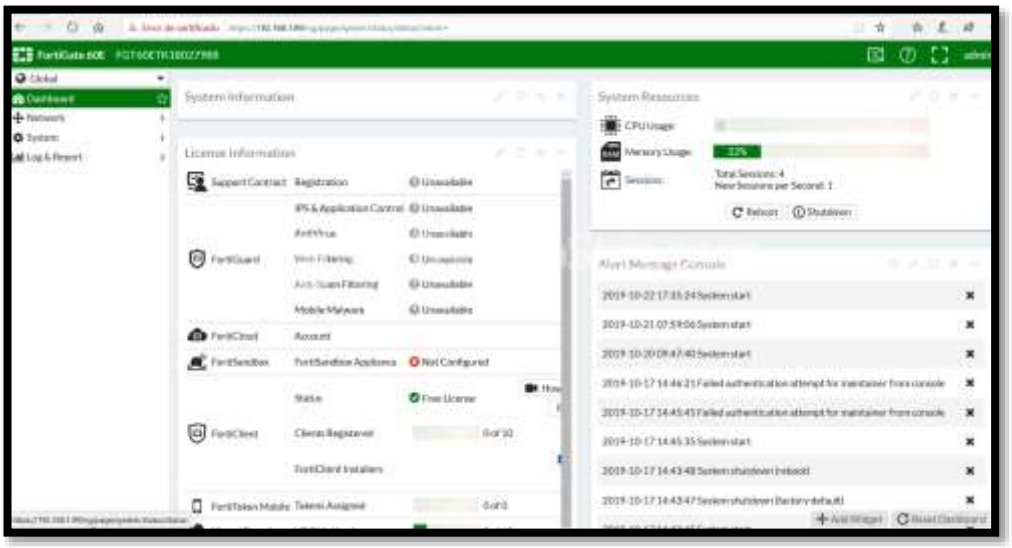


Figura 3. 33 Configuración del gestor del Fortigate 60E
Elaborado por: Autor.

Como siguiente paso se debe configurar el puerto 3, seleccionando la pestaña *Network*, luego a Interface y se asigna el rol de VLAN al puerto 3 como se observa en la figura 3.34.

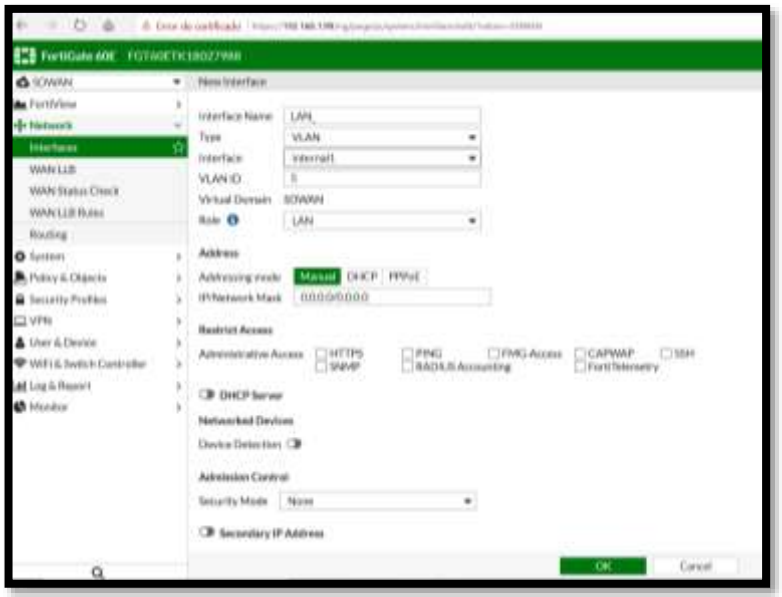


Figura 3. 34 Configuración de la interface LAN_
Elaborado por: Autor.

A continuación se debe seleccionar la pestaña *Network*, luego a Interface se le asigna el rol WAN, el alias de WAN_MPLS y WAN_INTERNET según el puerto como indica la figura 3.35 y figura3.36.

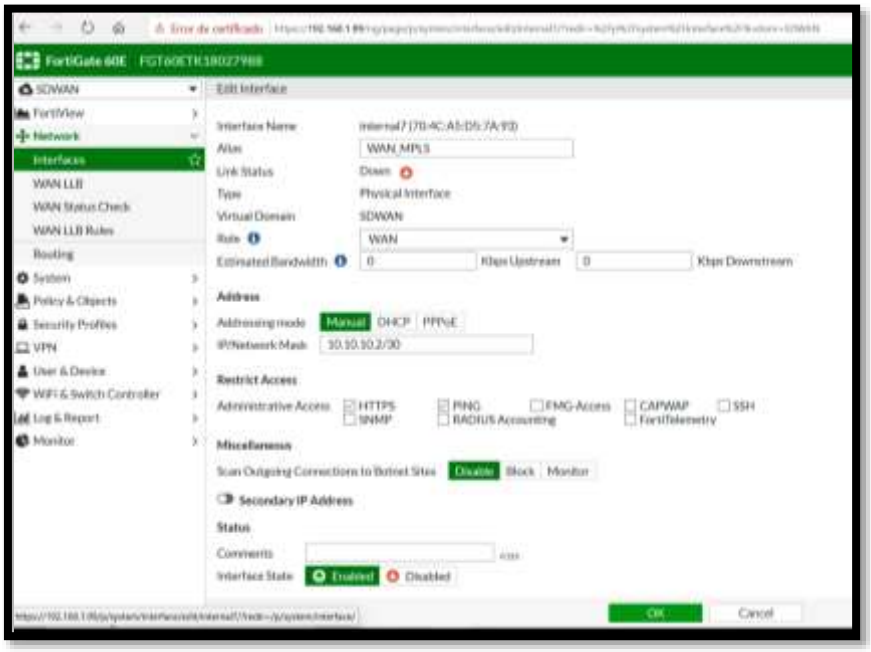


Figura 3. 35 Configuración de la interface WAN_MPLS
Elaborado por: Autor.

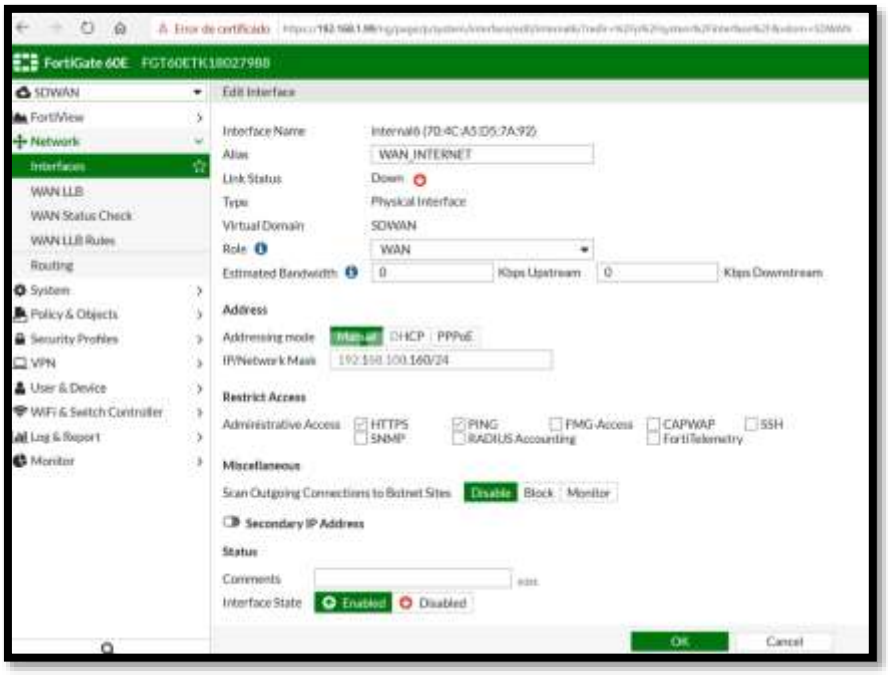


Figura 3. 36 Configuración de la interface WAN_INTERNET
Elaborado por: Autor.

Se debe de terminar la configuración de la *VPN Site o Site* o *VPN Ipsec*, seleccionando la pestaña de VPN luego la opción *Ipsec Wizzard*, se debe configurar en la sección de *VPN Setup* el nombre de la VPN, el tipo y la configuración NAT como se observa en la figura 3.37.

Figura 3. 37 Configuración de la VPN
Elaborado por: Autor.

Ahora se debe configurar la sección de *Authentication* con la las siguientes características como la dirección IP, la interface, método de autenticaciones y la contraseña, se puede observar este proceso en la figura 3.38.

Figura 3. 38 Configuración de la VPN sección Authentication.
Elaborado por: Autor.

En la figura 3.39 se deber configurar la sección de *Policy & Routing* con las siguientes características como la interfaz local, subredes locales, subredes remotas, al final se confirma toda la información como muestra la figura 3.40.

Figura 3. 39 Configuración de la VPN sección Policy & Routing.
Elaborado por: Autor.

Figura 3. 40 Confirmación que fue creada la VPN
Elaborado por: Autor.

Ahora se debe configurar la parte de SD-WAN del equipo. Seleccionamos la pestaña *network* luego la opción Sd-WAN (en versiones anteriores el apartado de SD-WAN puede tener el nombre WAN Load Balance). Se habilita la interface en la parte de *Interface State,* luego debemos crear una nueva interface SD-WAN/ Wan LLB como muestra la figura 3.41.

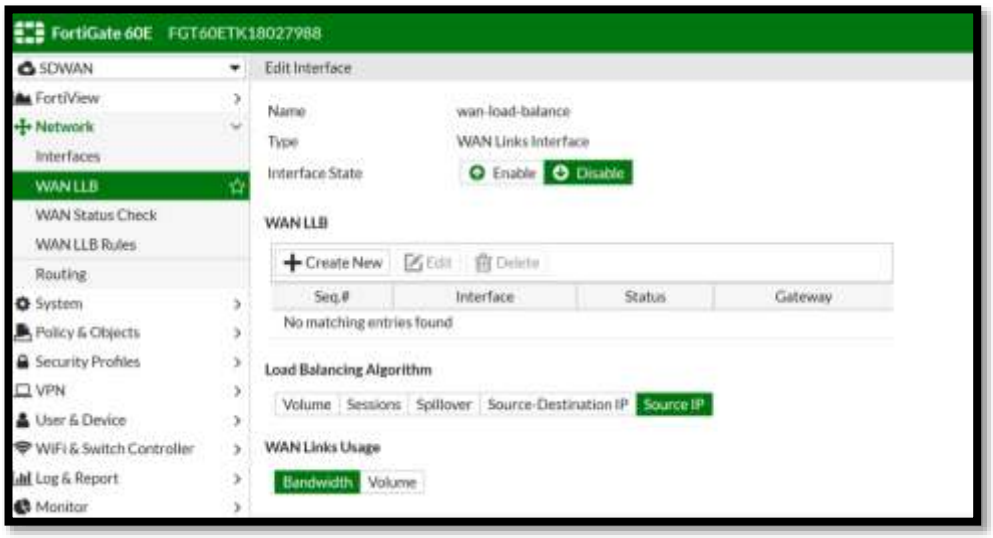


Figura 3. 41 Pantalla con la configuración del WAN LLB O SD-WAN
Elaborado por: Autor.

Se habilita la interface en la parte de *Interface State,* luego se debe crear una nueva interface SD-WAN/ Wan LLB mostrada en la figura 3.45.

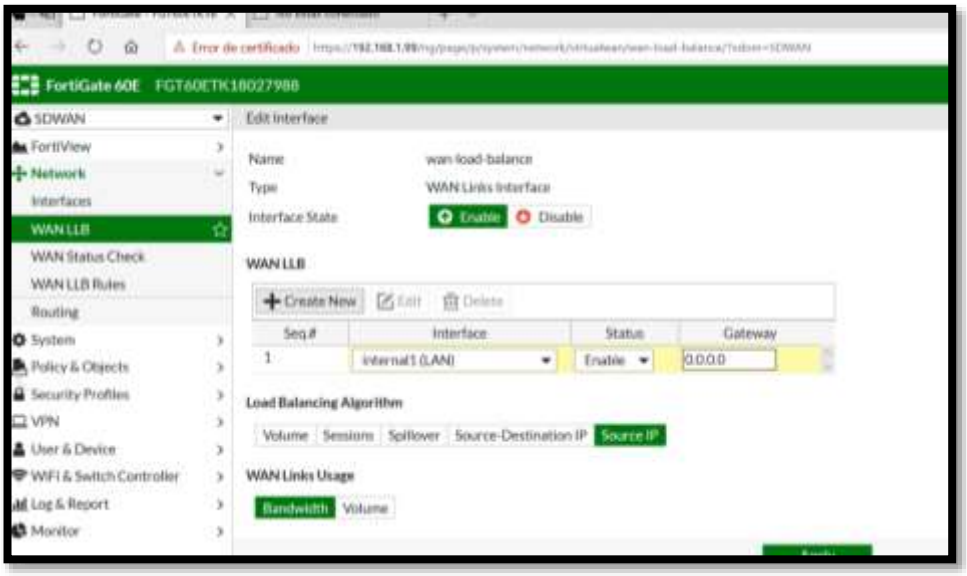


Figura 3. 42 Configuración de la Interface del SD-WAN.
Elaborado por: Autor.

Debe ser seleccionada la interface que va pasar por la SD-WAN, en este caso sería la interface de WAN_Internet luego se asigna el *gateway* correspondiente como lo muestra la figura 3.43.

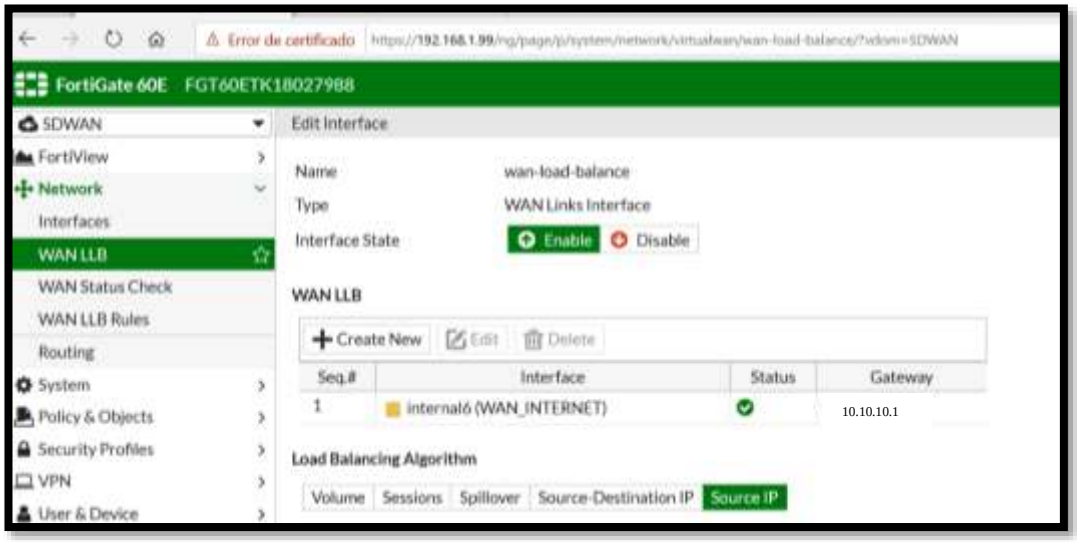


Figura 3. 43 Configuración del SD-WAN con su gateway.
Elaborado por: Autor.

Para dar la optimización de la red WAN del Cliente, se debe anexar a la SD-WAN la otra red conectada al equipo, en este caso sería la *VPN Site to Site* anteriormente creada mostrada en la figura 3.44.

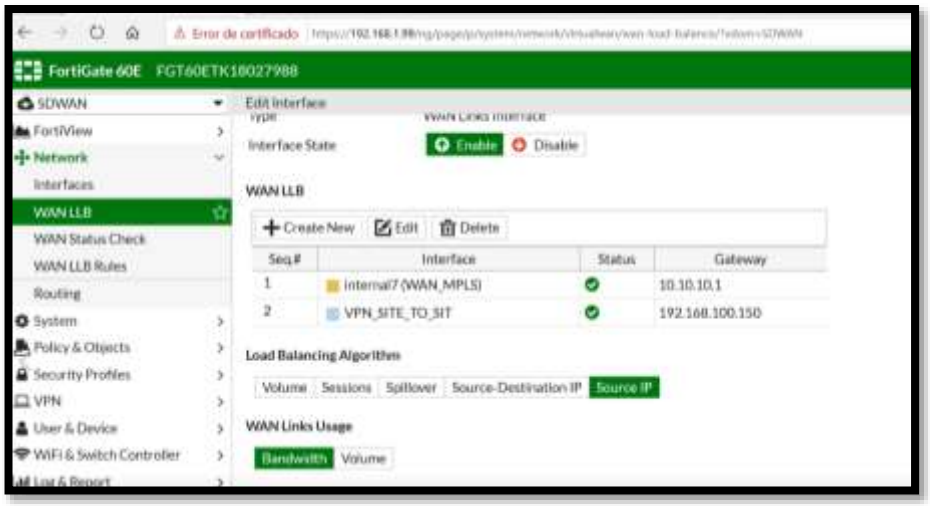


Figura 3. 44 Configuración de la 2da SD-WAN con su gateway.
Elaborado por: Autor.

Como siguiente paso se configura las políticas de IPv4 para cada interface, estas se encuentran en la pestaña *Policy & Objets* para definir las condiciones del tráfico, definir el tipo de datos transmitido, *firewall*, antivirus, las interfaces de entrada y salida demostradas en las figuras 3.45 y 3.46.

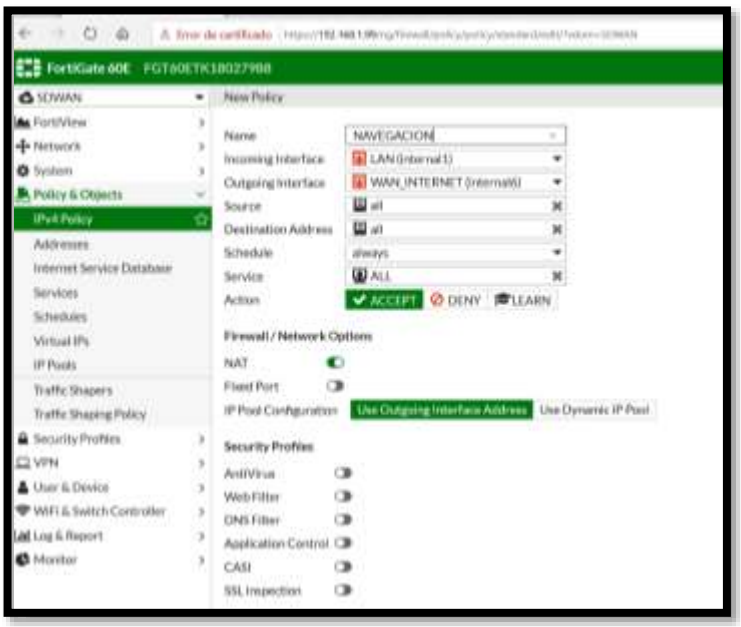


Figura 3. 45 Configuración de las políticas de IP en el LAN.
Elaborado por: Autor.

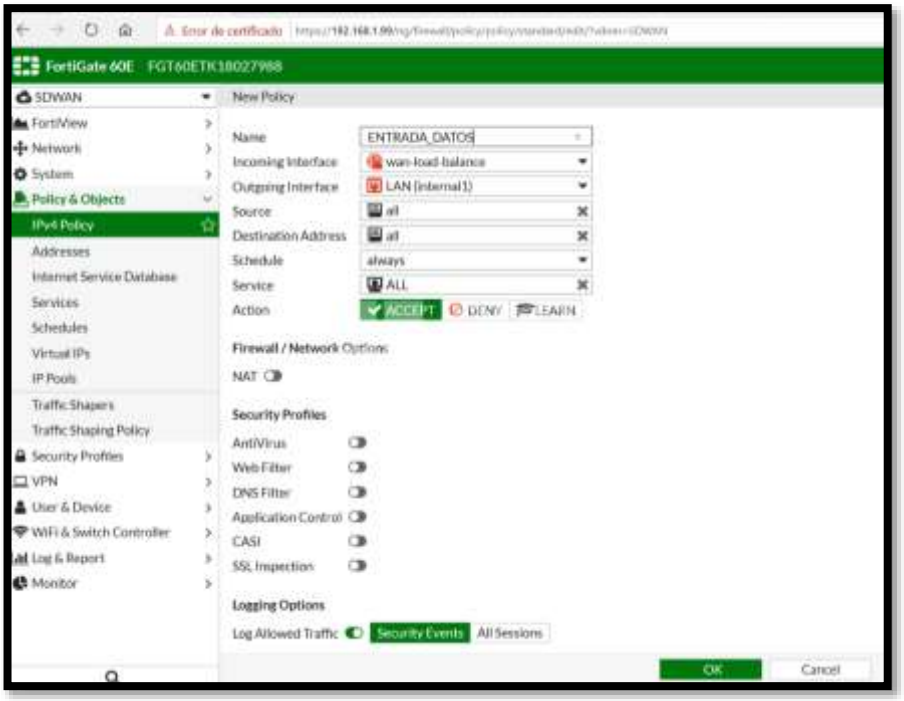


Figura 3. 46 Configuración de las políticas de IP del SD-WAN.
Elaborado por: Autor.

Se debe confirmar la ruta donde el Fortigate tendrá que hacer el encaminamiento de cada interface. Para realizar este proceso seleccionando las pestañas de *network* luego la opción *Routing.* Definimos el gateway y la IP como lo muestra las figuras 3.47 y 3.48

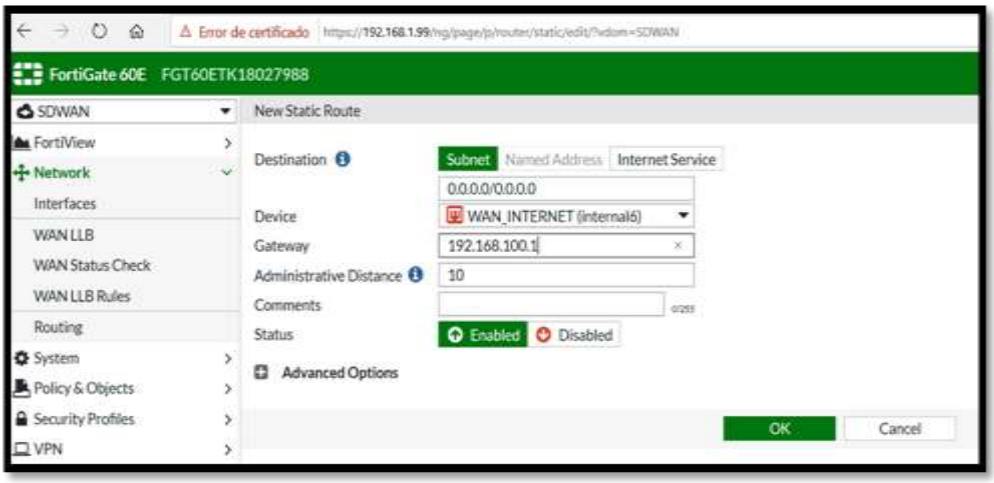


Figura 3. 47 Configuración del enrutamiento con el Internet.
Elaborado por: Autor.

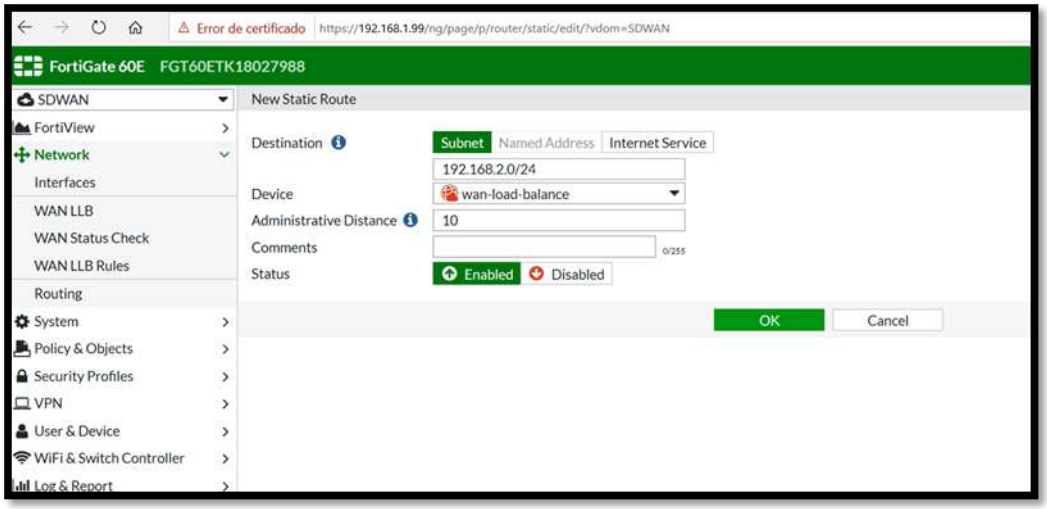


Figura 3. 48 Configuración del enrutamiento SD-WAN
Elaborado por: Autor.

3.4. Pruebas de conectividad en SD-WAN.

Paso 1. Para comprobar conectividad, por motivos de interfaces físicas y velocidad el balanceo automático se balanceo que la interfaz del puerto 1 (Internet) a 16% y la interfaz Datos 84% mostradas en la figura 3.49.

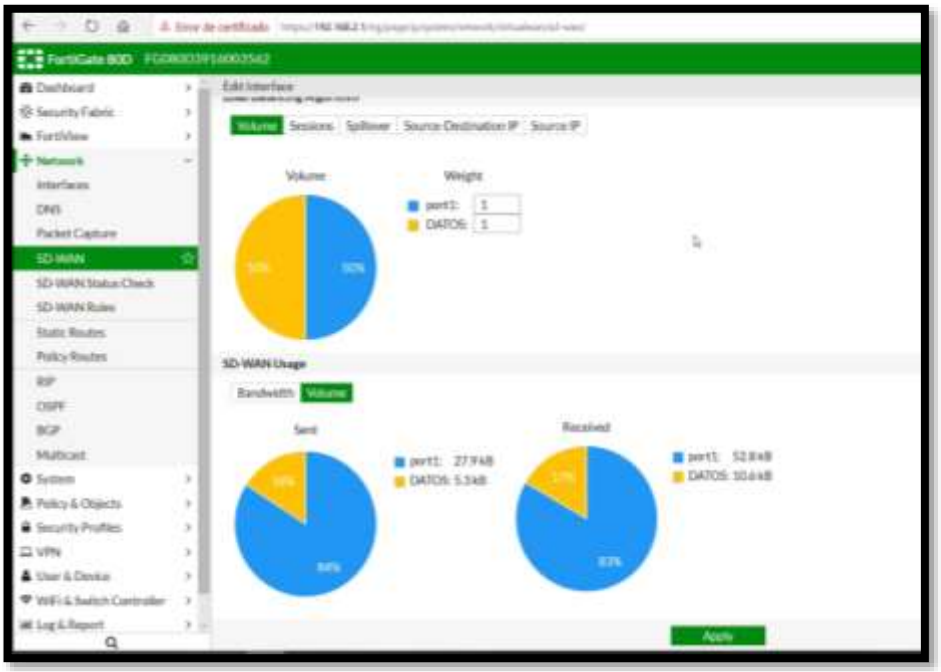


Figura 3. 49 Comprobación de conectividad de la interfaz SD-WAN.
Elaborado por: Autor.

Paso 2. Se desconecta la interfaz datos, y el Balanceo le da más prioridad a Puerto 1 (Internet) pero no pierde conectividad la interfaz Datos solo existe variaciones en balanceo del ancho de banda, mostrados en las figuras 3.50 hasta la figura 3.53 .

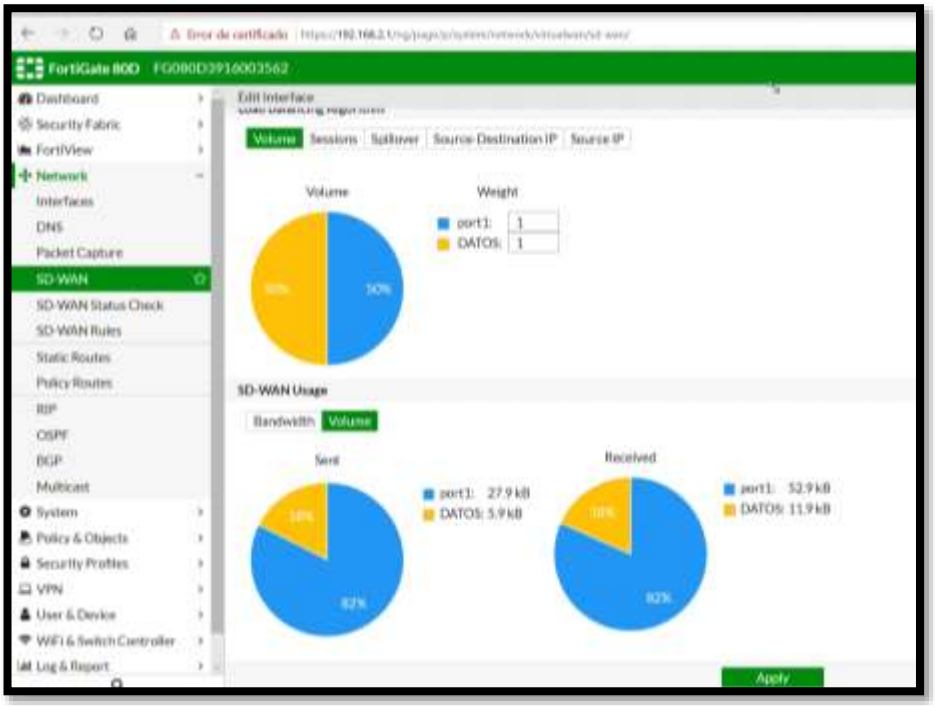


Figura 3. 50 Prueba 1 de Caída de interfaz Internet.
Elaborado por: Autor.

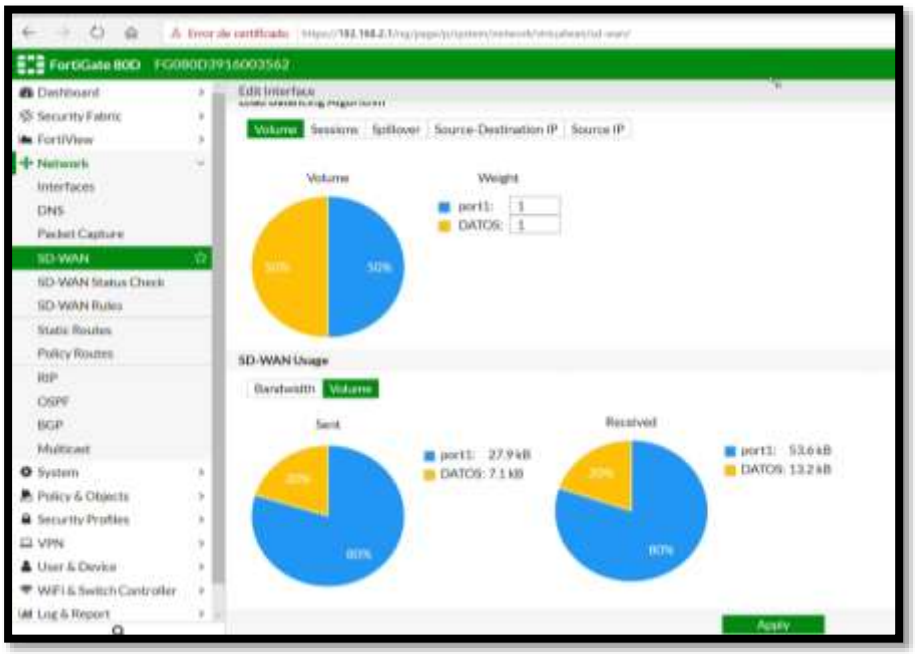


Figura 3. 51 Prueba 2 de Caída de interfaz Internet.
Elaborado por: Autor.

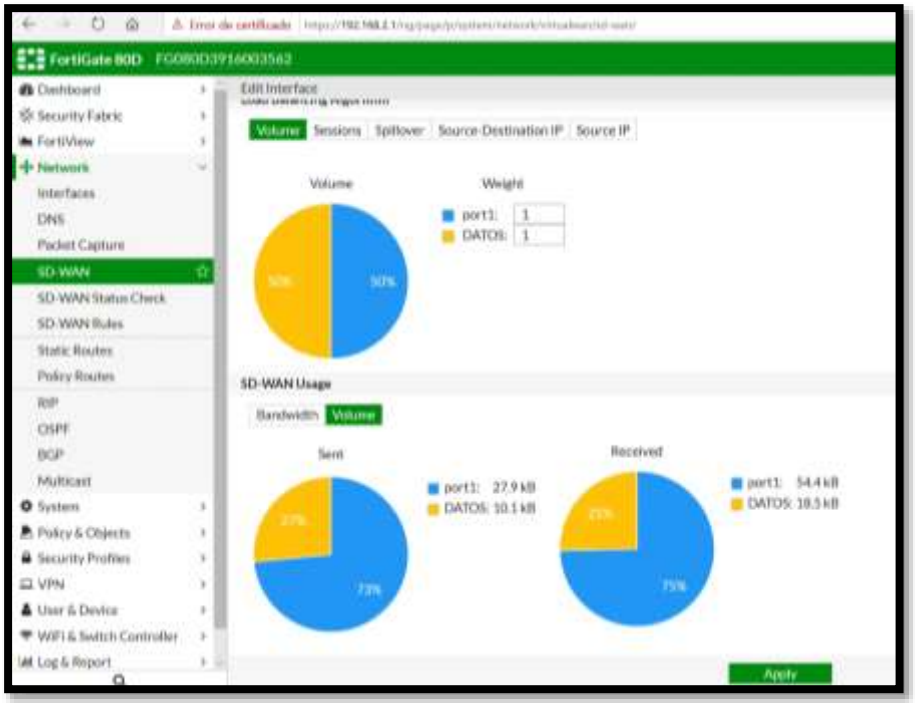


Figura 3. 52 Prueba 3 de Caída de interfaz Internet.
Elaborado por: Autor.

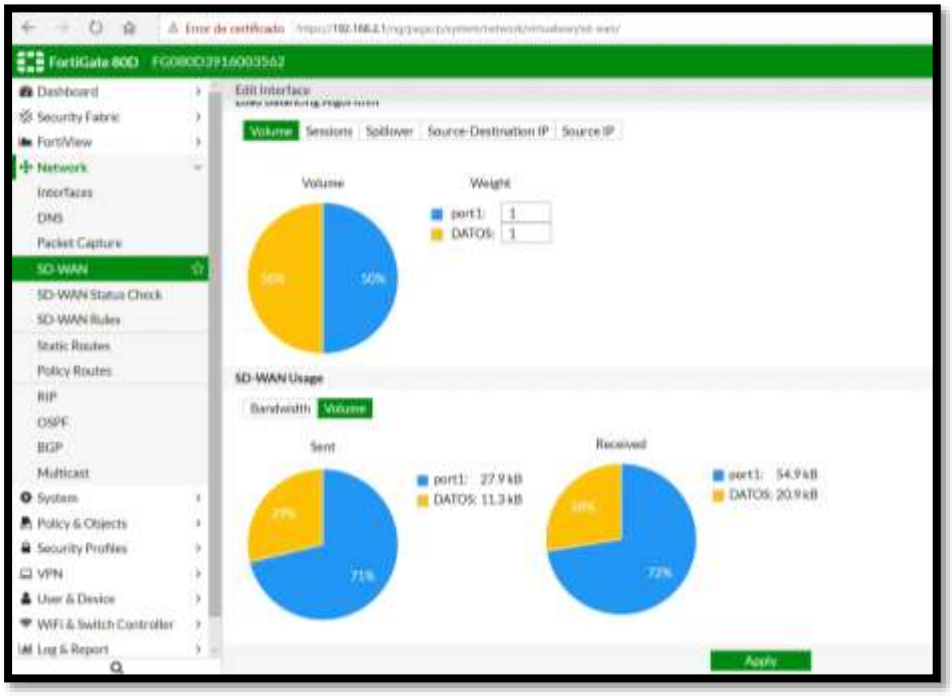


Figura 3. 53 Prueba 4 de Caída de interfaz internet.
Elaborado por: Autor.

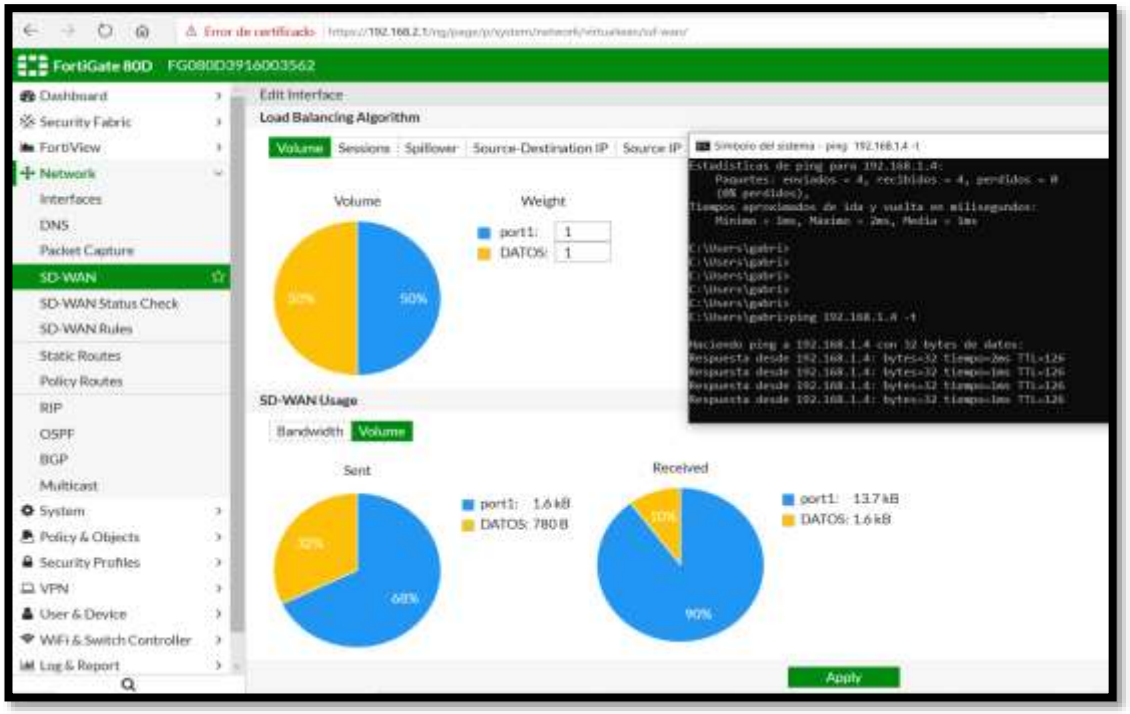


Figura 3. 54 Prueba 5 de Caída de interfaz internet.
Elaborado por: Autor.

Como se puede observar en la figura 3.54 que en la prueba aunque haya una caída de la interface, la conectividad se mantiene lo único que cambia es el balanceo de la red, lo cual se da por la creación del túnel *VPN Site to Site*, provocando que este factor. Para confirmar si se mantiene la conectividad se realiza un Ping a la otra maquina con el comando “Ping 192.168.1.4”

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones.

- En este documento, se realizó un estudio de la parte fundamental de las redes SD-WAN, definiendo varias temáticas o conceptos sobre el SDN, toda su metodología y procesos de funcionamiento de las redes definidas por software.

- En el diseño de la red del cliente usando tecnología SD-WAN, se puede comprobar que existe una alta disponibilidad de la red, aunque exista caídas en las interfaces, la tecnología SD-WAN balancea la carga de transmisión de información hacia otra interface asociada en su interfaz virtual por medio de la aplicación de gestión del equipo, así manteniendo la conectividad con la perdida mínima de paquetes.

- Finalmente tras realizar múltiples pruebas de conectividad y caídas de interfaces se puede comprobar el rendimiento superior de la red SD-WAN con respecto a disponibilidad y balanceo del ancho de banda a comparación de una WAN tradicional que se realiza un proceso de redundancia con pérdida de calidad y de información.

4.2 Recomendaciones.

- Para aumentar más la disponibilidad de la red, se recomienda crear túneles directamente a aplicaciones de capa 7, estableciendo prioridades por aplicaciones.

- Dependiendo la estandarización de la IEEE que se le otorgue a esta tecnología, se recomienda comenzar una migración de servicio y aplicaciones a la nube.

- Para otorgar mayor seguridad en la interfaz SD-WAN, se recomienda contratar una licencia para el Firewall de la red, en cada interfaz virtual.

- Para otorgar mas eficacia a una red es recomendable conectar múltiples túneles hacia las interfaces virtuales.

Bibliografía

Bautista, J. del O. (2019). *Presente y futuro de las redes WAN: SD-WAN y NFV* [Investigativa, Universidad Oberta de Catalunya]. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/87265/7/jdelolmobTFM0119memoria.pdf

Cisco Company. (s/f). *Software-Defined Networking (SDN) Definition—Cisco*. Recuperado el 3 de febrero de 2020, de https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

Dordoigne, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...)*. Ediciones ENI.

Figuerola, N. (2013). *SDN – Redes definidas por Software*. 4.

Freire García, J. (2019, junio 9). Redes SD-WAN, ¿qué son y para qué sirven? | Doctor Tecno | La Revista | El Universo. *El Universo*. https://www.eluniverso.com/larevista/2019/06/09/nota/7370043/redes-sd-wan-que-son-que-sirven

IEEE. (s/f-a). *IEEE P1915.1 Security in Virtualized Environments | P1915.1 SVE*. Recuperado el 2 de febrero de 2020, de https://site.ieee.org/p1915-1-sve/

IEEE. (s/f-b). *P1921.1—Standard for Software-Defined Networking (SDN) Bootstrapping Procedures*. Recuperado el 2 de febrero de 2020, de https://standards.ieee.org/project/1921_1.html

IEEE. (s/f-c). *Standards—IEEE Software Defined Networks*. Recuperado el 2 de febrero de 2020, de https://sdn.ieee.org/standardization

IEEE (Ed.). (2011). IEEE Draft Standard for a Next Generation Service Overlay Network. *IEEE P1903/D2, July 2011*, 1–148. https://doi.org/10.1109/IEEESTD.2011.5976962

Jimenez Moreno, A. (2018). *Desarrolo de solucion SD-WAN basada en SDN.* [Investigativa, Universidad Carlos III de Madrid]. https://e-archivo.uc3m.es/bitstream/handle/10016/29330/TFG_Alvaro_Jimenez_Moreno_2018.pdf?sequence=1&isAllowed=y

Martello Technologies. (s/f). *Finding the Right SD-WAN Solution | Game Changing SD-WAN*. Recuperado el 3 de febrero de 2020, de

https://martellotech.com/finding-the-right-sd-wan-solution/?utm_source=AdWords&utm_medium=cpc&utm_campaign=Finding%20the%20Right%20SD-WAN%20Solution&utm_term=SD-WAN&gclid=Cj0KCQiApt_xBRDxARIsAAMUMu-FZU6tABZxPNqUEi7sjpDAqAjXJGnAlN_Ii2NSWJ0g5iWZuZKhOdIaAoH5EALw_wcB

Riverbed Technology. (s/f). *What Is SD-WAN? | Riverbed's Guide to Software-Defined WAN*. Recuperado el 3 de febrero de 2020, de https://www.riverbed.com/faq/what-is-sd-wan.html

Santulli, J. (s/f). *P1913—Software-Defined Quantum Communication* [Investigativa]. P1913 - Software-Defined Quantum Communication. Recuperado el 1 de febrero de 2020, de https://standards.ieee.org/project/1913.html

Stallings, W. (2004). *Comunicaciones y Redes de Computadores* (7ma ed.). Pearson. https://www.academia.edu/5011511/Comunicaciones_y_Redes_de_Computadores_7ma_Edici%C3%B3n_-_William_Stallings

Tananbaum, A. (2003). *Redes de Computadoras* (CUARTA EDICIÓN, 2003). Pearson.

Glosario

ApIs: Interfaz de las Aplicaciones programables.
Arpanet: Advanced Research Projects Agency Network.
ATM: Asynchronous Transfer Mode.
Broadcasting: Amplia difusión.
Cable consola: Cable que se usa a menudo para conectar un terminal de computadora al puerto de la consola del enrutador.
Cisco IOS: Sistema operativo de equipos Cisco.
Cloud: Interfaz Virtual de almacenamiento o datos almacenados en internet.
CSMA/CD: Carrier Sense Multiple Access with Collision Detection.
Data Center: Centro de Datos.
Dashboard: Tablero de interfaz grafica con indicadores.
EIGRP: Enhanced Interior Gateway Routing Protocol.
End to end: Conexión de principio fin a fin.
Ethernet: Estándar de redes de área local.
FastEthernet: Ethernet de alta velocidad.
Firewall: Programa informático que controla el acceso de una computadora a la red.
Fortinet: Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad.
Fortigate 80D: Equipo End to End para enrutamiento físicos y virtuales de 4 puertos.
Fortigate 60E: Equipo End to End para enrutamiento físicos y virtuales de 8 puertos.
Frame Relay: Frame-mode Bearer Service.
FTP: File Transfer Protocol.
Gateway: Es la pueta de enlace definida por IP, donde se pueden conectar a un equipo.
GigabitEthernet: Ampliación del estándar Ethernet de alta velocidad.
ICMP: Internet Control Message Protocol.
IEEE: Institute of Electrical and Electronics Engineers.
IPSec: Protocolo de Seguridad de cifrado único.
IPv4: Protocolo de Internet versión 4.

IPv6: Protocolo de Internet versión 6.

ISO: Organización Internacional de Normalización.

ISP: Internet Service Provider.

LAN: Local Area Network.

Man in the Middle: Ataque de intermediario.

MAN: Red de área metropolitana.

MPLS: Multiprotocol Label Switching.

Multicast: Multiples destinos simultáneamente.

NAT: Traductor de direcciones de red.

NFV: Virtualización de las funciones de red.

NGSON: Next Generation of Service Overlay Networks.

ONF: Open Networking Foundation.

OpenFlow: Protocolo abierto de comunicaciones para servidor de software.

OSI: Open System Interconnection.

OSPF: Open Shortest Path First.

PAN: Personal Area Network.

PPP: Point-to-Point Protocol.

PYME: Pequeñas y Medianas empresas.

QoS: Quality of service.

RIP: Routing Information Protocol.

SDH: Synchronous Digital Hierarchy.

SDN: Software Defined Networking.

SDQC: Software Defined Quantic Comunication.

SD-WAN: Software Defined Wide Area Network.

SMTP: Simple Mail Transfer Protocol.

STP: Spanning Tree Protocol.

SVA: Servicios de Valor Agregado.

TCP/IP: Protocolo de control de transmisión/ IP.

Telnet: Telecommunication Network.

UDP: User Datagram Protocol.

Unicast: Difusión única.

Vlan: Red de área local virtual.

VM: Virtual Machine.

VPN over Lan: Virtual Private Network over Local Area Network, VPN aplicado a las LAN.

VPN Site to site: Tunel VPN creado por Fortigate.

VPN: Virtual Private Network.

VRouters: Router Virtual.

VSwitch: Switch Virtual.

WAN: Wide Area Network.

X.25: Estándar para redes de paquetes.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Ayapata Mendoza, Douglas Oswaldo** con C.C: # 093038878-0 autor del Trabajo de Titulación: **Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 2 de marzo del 2020

f. _____

Nombre: Ayapata Mendoza, Douglas Oswaldo

C.C: 093038878-0

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo.		
AUTOR(ES)	AYAPATA MENDOZA, DOUGLAS OSWALDO		
REVISOR(ES)/TUTOR(ES)	M. Sc. LUZMILA RUILOVA AGUIRRE		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	2 de marzo del 2020	**No. DE PÁGINAS:**	64
ÁREAS TEMÁTICAS:	Sistemas Telemáticos, Sistemas de Transmisión		
PALABRAS CLAVES/ KEYWORDS:	SDN, ONF, SDWAN, Controladora, Switch, Tunelización.		

RESUMEN/ABSTRACT:

Software Defined Wide Area Network (SD-WAN), es conocido como la evolución de las redes de telecomunicaciones actuales. El uso de Software Defined Network (SDN) en las diferentes redes de comunicación, crearía un nuevo ecosistema de las redes. Este nuevo avance provocaría que la mayoría de redes y proveedores de servicios cambien su modelo de negocio de proveer servicios a proveer características, programación única y espacio en la nube para cada cliente corporativo. SD-WAN es una solución completa en caso de conectividad y seguridad ya que está bajo el cifrado de IPSec al momento de la creación de los túneles VPN, y la máxima flexibilidad de las redes, dando prioridad a la calidad según el servicio o los datos sin importar la gran demanda de usuarios a nivel masivo, pyme y corporativo. A nivel corporativo la solución SD-WAN representa un ahorro económico a nivel de hardware. En este trabajo se presentará como optimizar una WAN tradicional utilizando las redes definidas por software simulando caídas de la red en medio de una transmisión de información continua, donde podemos comprobar que una red WAN tradicional la comunicación se caería y existiría una gran pérdida de paquetes mientras que con la tecnología SD-WAN la perdida de paquetes seria mínima al punto de ser casi imperceptible.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593968408198	E-mail: douglas.ayapata@gmail.com
CONTACTO CON LA INSTITUCIÓN:	**Nombre:** Palacios Meléndez, Edwin Fernando	
COORDINADOR DEL PROCESO DE UTE	**Teléfono:** +593-9-67608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	