UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica de la UCSG.

AUTOR:

Romero Naula, Luis Fernando

Trabajo de Titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

M. Sc. Bastidas Cabrera, Tomas Gaspar

Guayaquil, Ecuador

15 de septiembre 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. **Romero Naula, Luis Fernando** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

M. Sc. Bastidas Cabrera, Tomas Gaspar

DIRECTOR DE CARRERA

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los de 15 días del mes de septiembre del año 2020

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Romero Naula, Luis Fernando**

DECLARÓ QUE:

El trabajo de titulación: **"Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica de la UCSG",** 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, a los 15 días del mes de septiembre del año 2020

EL AUTOR

ROMERO NAULA, LUIS FERNANDO

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Romero Naula, Luis Fernando**

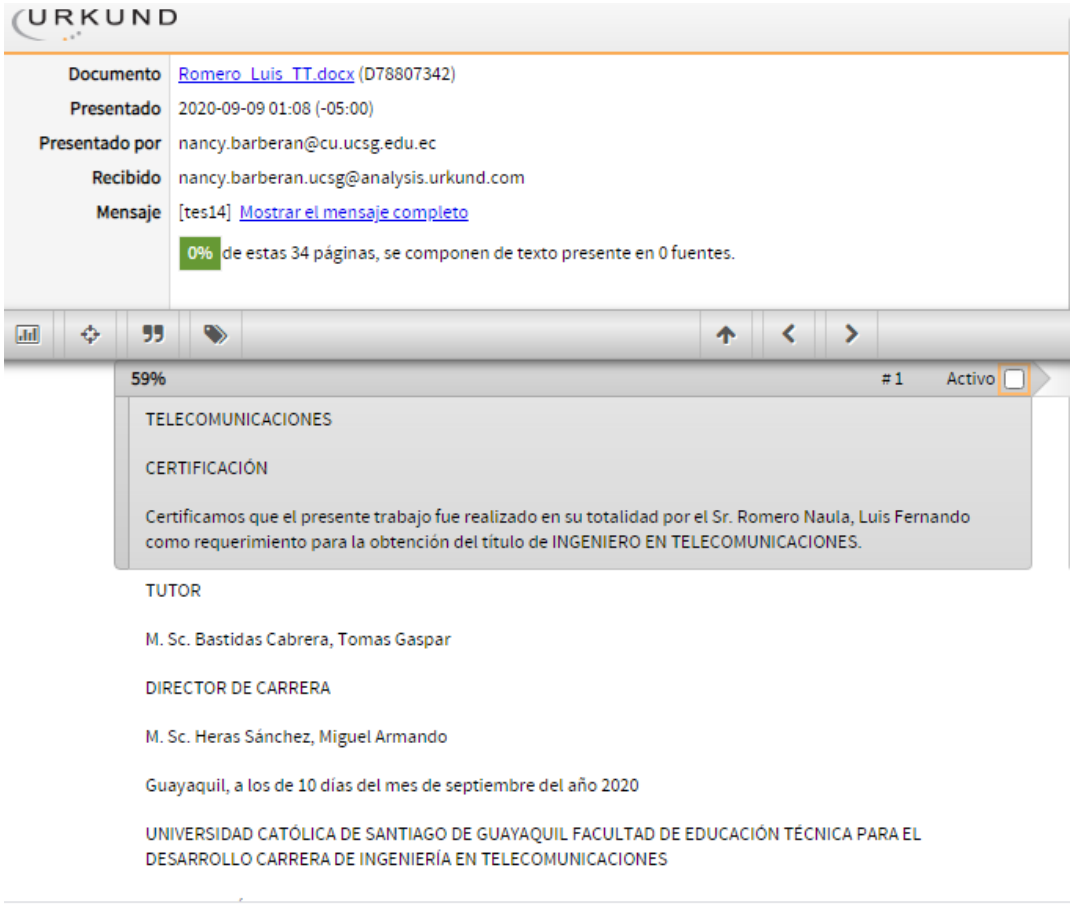
Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica de la UCSG"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 15 días de septiembre del 2020

EL AUTOR

ROMERO NAULA, LUIS FERNANDO

REPORTE DE URKUND


URKUND

Documento Romero_Luis_TT.docx (D78807342)

Presentado 2020-09-09 01:08 (-05:00)

Presentado por nancy.barberan@cu.ucsg.edu.ec

Recibido nancy.barberan.ucsg@analysis.urkund.com

Mensaje [tes14] Mostrar el mensaje completo

0% de estas 34 páginas, se componen de texto presente en 0 fuentes.

59% #1 Activo

TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. Romero Naula, Luis Fernando como requerimiento para la obtención del título de INGENIERO EN TELECOMUNICACIONES.

TUTOR

M. Sc. Bastidas Cabrera, Tomas Gaspar

DIRECTOR DE CARRERA

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los de 10 días del mes de septiembre del año 2020

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Reporte Urkund del trabajo de titulación de ingeniería en Telecomunicaciones; denominado **Diseño de una solución SD-WAN (Software-Defined Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica.** Del estudiante **Romero Naula, Luis Fernando** se encuentra al 0% de coincidencias.

Atentamente.

Ing. Tomás Bastidas Cabrera

Revisor

DEDICATORIA

Este trabajo de titulación se la dedico de manera muy especial a mis padres, Modesto Romero y Rosa Naula, quienes han sido los pilares en mi vida, con todo su amor, esfuerzo, confianza, dedicación y apoyo incondicional las cuales me han permitido obtener mi carrera universitaria y ser una mejor persona.

A mis hermanos por estar siempre presentes, durante todo este proceso acompañándome, motivándome y brindándome todo su apoyo.

EL AUTOR

ROMERO NAULA, LUIS FERNANDO

AGRADECIMIENTO

A mis padres Modesto Romero y Rosa Naula, por estar siempre pendientes de mí en todo momento, por dedicar tiempo y esfuerzo para ser un hombre de bien, y sobre todo por darme valiosos consejos los cuales he puesto en práctica y me han servido en mi formación como profesional.

A mis hermanos, quienes me brindan su apoyo, deseándome lo mejor de los éxitos en mi vida.

.

EL AUTOR

ROMERO NAULA, LUIS FERNANDO

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. ZAMORA CEDEÑO, NESTOR ZAMORA

OPONENTE

Índice General

CAPÍTULO 1 2

DESCRIPCIÓN GENERAL DEL TRABAJO DE TITULACIÓN 2

1.1. Introducción 2

1.2. Antecedentes 2

1.3. Definición del problema 3

1.4. Justificación del problema 3

1.5. Objetivos del problema de investigación 4

1.5.1. Objetivo general 4

1.5.2. Objetivos específicos 4

1.5.3. Hipótesis 4

1.6. Metodología de investigación 4

CAPÍTULO 2 FUNDAMENTACIÓN TEÓRICA 6

2.1. Antecedentes de las redes WAN 6

2.1.1. Redes WAN tradicionales 6

2.1.2. Red WAN 9

2.1.3. Clasificación de líneas de conmutación 10

2.1.3.1. Líneas Conmutadas 10

2.1.3.2. Líneas Dedicadas 10

2.1.3.3. Líneas Punto a Punto 11

2.1.3.4. Líneas Digitales 11

2.1.4. Limitaciones de la WAN 11

2.2. Redes Privadas Virtuales (VPN) 12

2.2.1. Funcionalidades de la VPN 12

2.2.2. Topologías VPN 13

2.2.3. Elementos de una VPN 15

2.2.4. Tipos de VPN 16

2.2.4.1. Sistemas basados en Software 16

2.2.4.2. Sistemas basados en Hardware 16

2.2.5. Arquitectura VPN 16

2.2.5.1. VPN de Acceso Remoto 16

2.2.5.2. VPN sitio a sitio 17

2.3. Protocolos de Tunneling 18

2.3.1. Protocolo PPTP 19

2.3.2. Protocolo L2TP 20

2.3.3. Protocolo IPsec 21

2.3.4. Modos de IPsec 23

2.4. Virtualización de Red (NV) 25

2.4.1. Virtualización de funciones de red (NFV) 26

2.4.2. Arquitectura NFV 28

2.4.2.1. VNF Virtual Networks Funtions 28

2.4.2.2. NFVI Infraestructura de virtualización de funciones de red 29

2.4.2.3. NFV–MANO (Orquestación y gestión) 29

2.4.3. Redes definidas por Software (SDN) 30

2.4.4. Arquitectura SDN 31

2.4.4.1. Capa de Aplicación 32

2.4.4.2. Capa de Control 32

2.4.4.3. Capa de Infraestructura 32

2.4.5. Interfaces SDN 33

2.4.6. Beneficios de SDN 33

2.4.7. Controlador SDN 34

2.5. SD-WAN (Software Defined Wide Area Network) 35

2.5.1. Características de una red SD-WAN 36

2.5.2. Arquitectura de la red SD-WAN 36

2.5.3. Ventajas de una solución SD-WAN 39

2.5.4. SD-WAN vs Redes Tradicionales 40

2.5.1. Marco Regulador 41

2.5.2. Legislación y regulación 41

CAPÍTULO 3: 43

DISEÑO, IMPLEMENTACIÓN Y RESULTADOS 43

3.1. Diseño de la red SD-WAN aplicada al laboratorio de la facultad técnica de la UCSG 43

3.2. Diseño y pruebas de la red en un simulador virtual 44

3.3. Pruebas de conectividad aplicando una solucón SD-WAN. 77

CAPÍTULO 4 81

CONCLUSIONES Y RECOMENDACIONES 81

4.1 Conclusiones. 81

4.2 Recomendaciones. 82

Bibliografía 83

Glosario 87

Índice de Figuras

Capítulo 2

Figura 2. 1 Arquitectura de red tradicional……..……7
Figura 2. 2 Escenario típico de la WAN……7
Figura 2. 3 Red de área amplia (WAN)……...9
Figura 2. 4 Esquema de una VPN……..12
Figura 2. 5 Topología cliente servidor……13
Figura 2. 6 Topología cliente a red interna.……14
Figura 2. 7 Topología red interna a red interna……14
Figura 2. 8 Elementos de una VPN……...15
Figura 2. 9 VPN de Acceso Remoto……..17
Figura 2. 10 VPN sitio a sitio……..17
Figura 2. 11 Protocolo PPTP……..19
Figura 2. 12 Protocolo L2TP……..20
Figura 2. 13 Diseño de túneles L2TP……21
Figura 2. 14 Arquitectura IPsec……22
Figura 2. 15 Diferentes modos de IPsec……23
Figura 2. 16 Modos de empaquetamiento……..24
Figura 2. 17 Forma de trabajo de IPsec……...24
Figura 2. 18 Componentes de la NV……25
Figura 2. 19 Visión de la NFV ……27
Figura 2. 20 Arquitectura NFV……30
Figura 2. 9 VPN de Acceso Remoto……..……17
Figura 2. 10 VPN sitio a sitio……..17
Figura 2. 11 Protocolo PPTP……..19
Figura 2. 12 Protocolo L2TP……...20
Figura 2. 13 Diseño de túneles L2TP……21
Figura 2. 14 Arquitectura IPsec……22
Figura 2. 15 Diferentes modos de IPsec ……...23
Figura 2. 16 Modos de empaquetamiento……..24

Figura 2. 17 Forma de trabajo de IPsec ……..24
Figura 2. 18 Componentes de la NV…….25
Figura 2. 19 Evolución del modelo de red ……..26
Figura 2. 20 Visión de la NFV…….27
Figura 2. 21 Arquitectura NFV……....28
Figura 2. 22 Ejemplo del uso de una SDN……..31
Figura 2. 23 Arquitectura SDN……...31
Figura 2. 24 SD-WAN: arquitectura lógica y física……...37
Figura 2. 25 Comparativa de la redes tradicionales y SD-WAN……40

Capítulo 3

Figura 3. 1 Diseño de red aplicando una solución SD-WA ……...…43
Figura 3. 2 Diseño de la red WAN empleada para pruebas……44
Figura 3. 3 Interfaces de los puertos del equipo del laboratorio……45
Figura 3. 4 IP asignada en el puerto 3 del laboratorio……45
Figura 3. 5 Protocolos habilitados del puerto 3……46
Figura 3. 6 Prueba de conectividad del equipo……46
Figura 3. 7 IP asignada en el puerto 1 del laboratorio……47
Figura 3. 8 Protocolos habilitados del puerto 1……47
Figura 3. 9 IP asignada en el puerto 2 del laboratorio……48
Figura 3. 10 Protocolos habilitados del puerto 2. 48
Figura 3. 11 IP asignadas del equipo del laboratorio. 49
Figura 3. 12 IP asignada en el puerto 2 del centro de cómputo.....49
Figura 3. 13 IP asignada en el puerto 1 del centro de cómputo.....50
Figura 3. 14 IP asignada en el puerto 3 del centro de cómputo.....50
Figura 3. 15 Prueba de conectividad de las IP asignadas.....51
Figura 3. 16 Prueba de conectividad de las IP asignadas.....51
Figura 3. 17 IP asignadas del equipo del centro de cómputo 52
Figura 3. 18 IP asignadas del equipo del rectorado.....52
Figura 3. 19 Prueba de conectividad de las IP asignadas.....53

Figura 3. 20 Creación de la ruta estática del rectorado.....54
Figura 3. 21 Creación de la ruta estática del laboratorio. 54
Figura 3. 22 Creación de la ruta estática del centro de cómputo 55
Figura 3. 23 Creación del túnel del equipo ubicado en el laboratorio 56
Figura 3. 24 Paso 1 para crear un túnel IPsec hacia el rectorado …,.…56
Figura 3. 25 Paso 2 para crear un túnel IPsec……...57
Figura 3. 26 Paso 2 para crear un túnel IPsec.....57
Figura 3. 27 Confirmación que el túnel ha sido creado y activado 58
Figura 3. 28 Paso 1 para crear un túnel IPsec hacia el laboratorio 58
Figura 3. 29 Paso 2 para crear un túnel IPsec.....59
Figura 3. 30 Paso 3 para crear un túnel IPsec. 59
Figura 3. 31 Confirmación que el túnel ha sido creado y activado 60
Figura 3. 32 Paso 1 para crear un túnel IPsec hacia el (CC).....60
Figura 3. 33 Paso 2 para crear un túnel IPsec.....61
Figura 3. 34 Paso 3 para crear un túnel IPsec.....61
Figura 3. 35 Confirmación que el túnel ha sido creado y activado 62
Figura 3. 36 Paso 1 para crear un túnel IPsec hacia el laboratorio 62
Figura 3. 37 Paso 2 para crear un túnel IPsec.....63
Figura 3. 38 Paso 3 para crear un túnel IPsec. 63
Figura 3. 39 Confirmación que el túnel ha sido creado y activado 64
Figura 3. 40 Como crear una interfaz SD-WAN. 64
Figura 3. 41 La interface TUNEL_RECT como enlace SD-WAN 65
Figura 3. 42 La interface WAN_FO_RECT como enlace SD-WAN. 65
Figura 3. 43 La interface TUNEL_CC como enlace SD-WAN 65
Figura 3. 44 La interface WAN_FO_CCOMP como enlace SD-WAN.....66
Figura 3. 45 Interfaces creadas como miembro del enlace SD-WAN.....66
Figura 3. 46 Porcentajes de los puertos creados del enlace SD-WAN. ..67
Figura 3. 47 Gráfica del volumen SD-WAN dividido en los 4 puertos.....67
Figura 3. 48 Interfaces creadas como miembro del enlace SD-WAN.....68
Figura 3. 49 Porcentajes de los puertos creados del enlace SD-WAN. ..68
Figura 3. 50 Gráfica del volumen dividido en los 2 enlaces SD-WAN….69
Figura 3. 51 Interfaces creadas como enlace SD-WAN del (CC).....69
Figura 3. 52 Porcentajes de los puertos creados del enlace SD-WAN ...70
Figura 3. 53 Gráfica del volumen dividido en los 2 enlaces SD-WAN.....70

Figura 3. 54 Creación de la ruta estática del laboratorio 71
Figura 3. 55 Creación de la ruta estática del rectorado.....71
Figura 3. 56 Creación de la ruta estática del centro de cómputo. 72
Figura 3. 57 Prueba de conectividad de las IP asignadas 72
Figura 3. 58 Prueba de conectividad de las IP asignadas. 73
Figura 3. 59 Creación de política de salida del laboratorio 73
Figura 3. 60 Creación de política de entrada del laboratorio.....74
Figura 3. 61 Políticas creadas de entrada y salida.....74
Figura 3. 62 Creación de política de salida del rectorado.....75
Figura 3. 63 Creación de política de entrada del rectorado. 75
Figura 3. 64 Políticas creadas de entrada y salida.....76
Figura 3. 65 Interfaz WAN_FO_TECNICA.....76
Figura 3. 66 Interfaz WAN_FO_RECT 77
Figura 3. 67 Comprobación de conectividad de la interfaz SD-WAN.....77
Figura 3. 68 Prueba 1 PING extendido al centro de cómputo. 78
Figura 3. 69 Prueba 2 Tráfico fluye solo por la interfaz del (CC).....78
Figura 3. 70 Prueba 3 Tráfico que fluye por el enlace de internet.....79
Figura 3. 71 PING a la IP 172.16.38.2 prueba de conectividad 3 79
Figura 3. 72 Prueba 4 volumen asignado a cada puerto 80
Figura 3. 73 PING a la IP 172.16.30.2. 80

Índice de Tablas

Capítulo 2

Tabla 2. 1: Problemas de MPLS e internet en la WAN…...……..……8

Tabla 2. 2 Diferencia entre las redes tradicionales y SD-WAN ……41

Resumen

El presente trabajo tiene como objetivo principal la implementación de una solución de área amplia definida por software (SD-WAN) aplicada al laboratorio de la facultad técnica de la UCSG. Se definieron conceptos básicos como: arquitectura SD-WAN, tecnologías de tunneling, redes virtualizadas. Mediante una máquina virtual se realizó la simulación de una red de área amplia definida por software de la cual se crearon enlaces que conectan con el rectorado, con el centro de cómputo y con salida a internet. En las pruebas que se realizaron en la implementación de la solución SD-WAN fueron por los métodos de balanceo de cargas, pruebas de conectividad y simulaciones de caída de interfaces en la red la cual establece una completa conectividad de la WAN entre sus sucursales, por medio de un mecanismo de control centralizado, abordando la creciente lactancia y el costo con el uso de enlaces de ancho de banda más económicos. En conclusión, al emplear nuevas tecnologías de red es posible implementar soluciones de alta capacidad, eficientes para el rendimiento de la red por medio del balanceo de carga y priorización de tráfico basadas en políticas SD-WAN.

Palabras claves: SD-WAN, SDN, TUNNELING, WAN, POLÏTICAS,

CAPÍTULO 1

DESCRIPCIÓN GENERAL DEL TRABAJO DE TITULACIÓN

1.1. Introducción

Las redes actuales se encuentran limitadas debido al crecimiento del internet y la gran demanda de aplicaciones requeridas por usuarios a nivel masivo, provocando que las organizaciones y empresas requieran utilizar múltiples conexiones en sus redes de datos mejorando las intercomunicaciones con el objetivo principal de ofrecer excelente servicio, una mejor experiencia para los usuarios y solventes soluciones. Las redes de área amplia definidas por software (SD-WAN), es una nueva tecnología enfocada a la conectividad de redes WAN haciendo posible optimizar los costos operativos y mejora el desempeño de los recursos para las implementaren en diversas sucursales. SD-WAN surge básicamente debido que el 50% del tráfico de datos de las empresas es de manera externo, es decir viene de internet, haciendo vulnerable la red de amenazas cibernéticas (Meneses, 2019).

Por lo tanto, la SD-WAN permite el enrutamiento del tráfico de manera dinámica brindando la función de elegir el camino más adecuado a través de la WAN, con protección contra amenazas ya que cuenta con un sistema de seguridad integrada implementación sin intervención brindando control y separación del plano de datos garantizando una orquestación y administración centralizada.

1.2. Antecedentes

Desde el nacimiento de la red WAN la mayor parte de estas redes son establecidas por los proveedores de internet (ISP), para brindar servicios a sus clientes, otras son construidas por empresas u organizaciones para uso privado. Tradicionalmente las arquitecturas consistían en un diseño de WAN basada en enlaces de una conectividad MPLS lenta y costosa que aparte ofrece una experiencia de usuario inferior con respecto a sus necesidades, especialmente para aplicaciones que están basadas en la nube

A medida que aumenta la demanda del uso de aplicaciones, herramientas basadas en la nube y más aún que los servicios se están digitalizando ponen en estado crítico a la red empresarial, la gran mayoría de organizaciones que están distribuidas en múltiples oficinas remotas emigran a las redes definidas por software (SD-WAN). Esto se debe a las nuevas características presentes en la tecnología SD-WAN han permitido reducir considerablemente la administración por medio de la aplicación de dispositivos de red programables integrados en su arquitectura, permitiendo realizar ajustes de forma remota. La SD-WAN surgió como una alternativa que permite la fácil innovación de protocolos y permitir un control sencillo al programar y configurar las rutas de los datos en la red (Farhady et al., 2015).

SD-WAN es catalogado como un servicio tan eficiente gracias a su capa de software que garantiza, alta disponibilidad, flexibilidad, la calidad de servicio y sobre todo la seguridad de datos de los enlaces de internet de extremo a extremo.

1.3. Definición del problema

Debido a que el uso de aplicaciones, herramientas basadas en la nube, dispositivos conectados al internet, demanda masiva de información, alta disponibilidad y ancho de banda ha aumentado de manera exponencial, por lo tanto, están llevando al colapso de las redes tradicionales por tal motivo es necesario una solución que mejore la conectividad, el ancho de banda y el tráfico de la red. Estos problemas se pueden solucionar reemplazando las redes de área extensa (WAN) con rendimiento limitado por las arquitecturas de redes WAN definidas por software (SD-WAN), separando el plano de control del plano de datos, dando control a la nube brindando alta disponibilidad, mejor conectividad de red, manejo de aplicaciones comerciales y reduciendo los costos operativos de las redes existentes.

1.4. Justificación del problema

Las redes de datos han aumentado considerablemente en muchos aspectos tanto en tamaño como en complejidad, dejando en evidencia la capacidad limitada de las redes tradicionales para cubrir dichas necesidades.

Por estos motivos este trabajo mostrará los beneficios de utilizar las redes definidas por software (SD-WAN), proporcionando un mecanismo de control centralizado, eligiendo el mejor camino para desplegar el tráfico de datos entre todos sus enlaces garantizando acceso fácil y rápido a las aplicaciones críticas en la nube.

1.5. Objetivos del problema de investigación

1.5.1. Objetivo general

Diseñar e implementar una solución de alta capacidad y disponibilidad utilizando redes definidas por software aplicada al laboratorio de la facultad técnica.

1.5.2. Objetivos específicos

- Identificar los fundamentos teóricos necesarios para crear canales SD-WAN de alta capacidad.
- Diseñar un esquema SD-WAN de alta capacidad y disponibilidad a través de un emulador de enrutamiento basado en aplicaciones y salud de la red.
- Evaluar rendimiento de la red por medio del balanceo de carga y priorización de tráfico basadas en reglas SD-WAN,

1.6. Hipótesis

Diseñar un esquema de red utilizando SD-WAN para proporcionar calidad de servicio, alta disponibilidad y flexibilidad de la red aplicada al laboratorio de la facultad técnica, proveyendo de forma inteligente la mejor ruta de tráfico manteniendo el rendimiento de la red en condiciones favorables.

1.7. Metodología de investigación

En este trabajo de titulación se utilizará la metodología explorativa - experimental. Es explorativa ya que se estudiará acerca de las redes definidas por software y las soluciones que ofrecen, ya que aportan una nueva forma de gestión y securización de la WAN aplicada al laboratorio de la facultad

técnica es experimental dado que se utilizará un simulador de red virtual y se realizará pruebas con equipos físicos para aplicar dichas soluciones SD-WAN.

CAPÍTULO 2 FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de las redes WAN

Desde la década de 1980, y probablemente hasta el día de hoy las redes de área amplia (WAN), eran redes basadas en TDM (Time Division Multiplexing), para servicios de voz y datos. A principios de los años 90, las empresas empezaron a desplegar redes basadas en paquetes para las redes WAN, predominando la tecnología Frame Relay. En esta misma década surgió la tecnología ATM (Asynchronous Transfer Mode), empleadas por muchas organizaciones de telecomunicaciones. Finalmente, en el año 2000 empieza el auge de MPLS (Multi Protocol Label Switching), siendo como la nueva tecnología dominante para la WAN (Heredia, 2019).

La evolución de la WAN tiene como aspecto fundamental la necesidad de mejorar el desempeño de las aplicaciones, incremento de la disponibilidad, reducir costes de equipos y la seguridad. Las organizaciones atienden estos aspectos de muchas formas de todo esto surge el concepto de Optimización de WAN, que tiene como objetivo mejorar el crecimiento de los enlaces existentes (MPLS), por ejemplo, reduciendo el ancho banda contratado para las aplicaciones instaladas o incluso enlaces de internet, utilizando la optimización permitiendo equipar las prestaciones de los enlaces costosos para la WAN (Heredia, 2019).

2.1.1. Redes WAN tradicionales

Una red WAN tradicional es básicamente un conjunto de medios de transmisión como la fibra óptica, par de cobre, más los elementos de conmutación tales como routers, switches, entre otros.

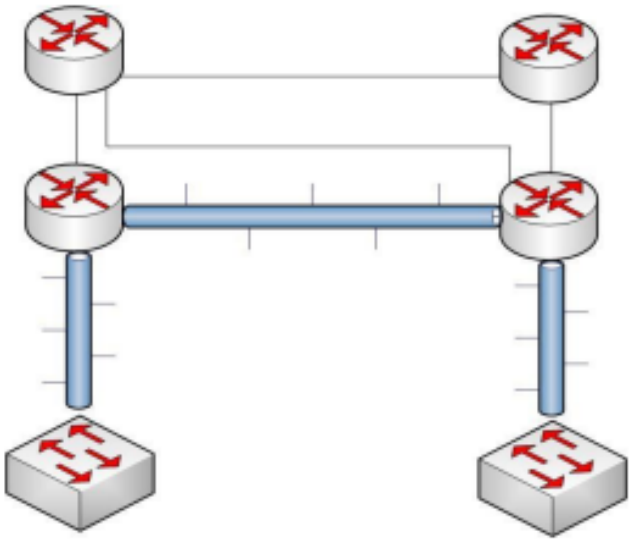


Figura 2. 1 Arquitectura de red tradicional
Fuente: (Roncero, 2014)

Tradicionalmente, las redes WAN manejan un entorno de red en 2 partes:

- La primera parte de la red conecta las sucursales de la empresa con la sede principal, de manera centralizada utilizando la topología tipo estrella.
- La segunda parte de la red interconecta el centro de datos de la sede principal con otro centro de datos secundario.

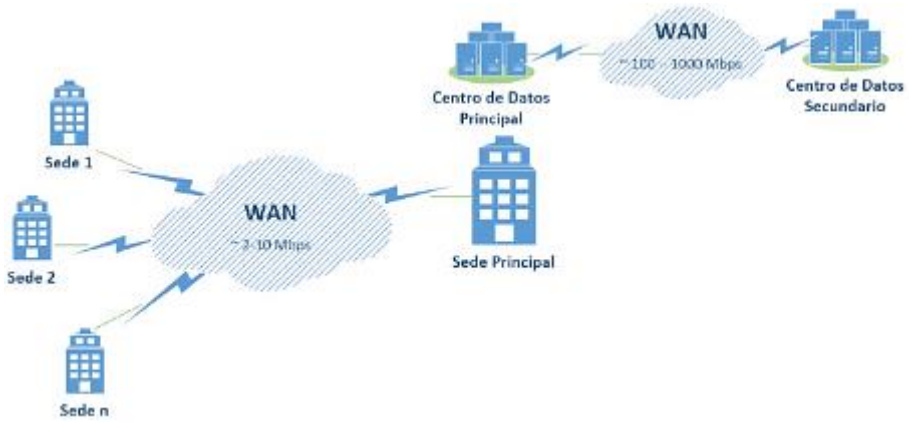


Figura 2. 2 Escenario típico de la WAN
Fuente: (Webmaster, 2019)

Desde hace 20 años se vienen haciendo las redes empresariales de la misma manera, donde las aplicaciones que utilizan los usuarios se ubicaban en las oficinas centrales o en los data centers. Cuando las empresas crecen y se expanden debían garantizar que las sucursales se conecten de forma correcta para ellos empleaban distintas tecnologías como en este caso:

- MPLS
- Líneas privadas
- Frame relay
- Dial-up

.

Estás tecnologías que utiliza la WAN tradicional, tienen en común que no fueron diseñadas para la explosión de internet y la nube. Por otro lado, existen problemas con MPLS e internet que se presentan en la siguiente tabla.

MPLS	Internet
Costo de equipamiento	Capacidad para aumentar los circuitos
Lactancia	Tasa de pérdida de paquetes
Tiempo operativo	Flexibilidad
Seguridad y vulnerabilidad	Disponibilidad
Complejidad de la red	Lactancia
Adopción de nuevas tecnologías	Tiempo operativo
Retraso en el despliegue de nuevos servicios	Seguridad y vulnerabilidad

Tabla 2. 1 Problemas de MPLS e Internet en la WAN
Fuente: (Autor)

2.1.2. Red WAN

La red de área amplia es un conjunto de redes LAN y MAN interconectadas entre sí cubren un área geográfica muy extensa como ciudades, estados, países y continentes. La WAN utiliza conexiones conmutadas o dedicadas para conectar redes LAN que estén ubicadas en sitios geográficamente remotos. Para tener una buena conexión es necesario hacerlo a través de una red pública o una red privada. Las redes WAN están diseñadas para cumplir con las siguientes funciones:

- Capacidad de realizar comunicaciones en tiempo real entre usuarios.
- Incorporan nuevos servicios como voz, datos, direccionamiento IP.
- Reduce costos de servicios
- Ofrece diversos medios de transmisión como por ejemplo los enlaces satelitales.

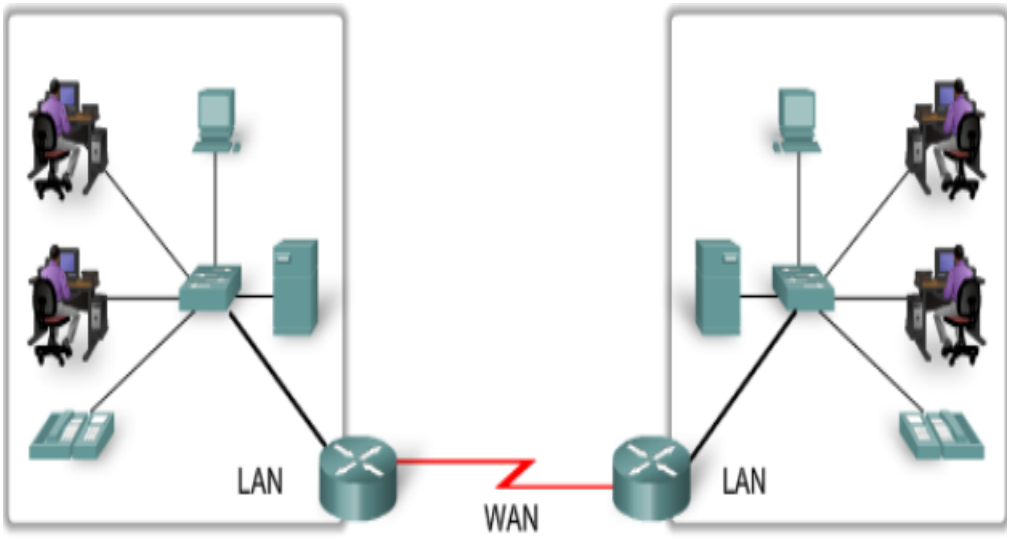


Figura 2. 3 Red de área amplia (WAN)
Fuente: (W. Herrera, 2015)

Estas redes utilizan dispositivos de red especialmente diseñados para las interconexiones entre las LAN permitiendo diversas formas de comunicación como pueden ser el intercambio de información interna (ventas, contabilidad, marketing, investigación y desarrollo) y el acceso a recursos para operar.

La WAN, cuenta con distintas tecnologías empleadas para el ámbito empresarial, cada uno de ellas cuenta con sus diferentes características, fortalezas y debilidades. Los servicios WAN más solicitados son: ATM (Modo de Transferencia Asíncrono – Asynchronous Transfer Mode), Retrasmisión de Tramas (Frame Relay), WAE (Ethernet de Área Amplia – Wide Area Ethernet) y MPLS (Conmutación de Etiquetas Multiprotocolo – Multiprotocol Label Switching) (Pérez, 2017).

2.1.3. Clasificación de líneas de conmutación

2.1.3.1. Líneas Conmutadas

Las líneas conmutadas, son típicamente líneas de telefonía convencional que requieren de marcar un código específico para poder establecer la comunicación con el otro extremo de la conexión.

2.1.3.2. Líneas Dedicadas

Las líneas dedicadas o también llamadas línea privada, es una solución fiable y segura que mantiene una permanente conexión entre 2 o más puntos, estás líneas suelen ser de 2 o 4 hilos. Se puede definir como un contrato de servicios a largo plazo entre cliente y proveedor a cambio de un pago mensual (Navas, 2006)

2.1.3.3. Líneas Punto a Punto

Las líneas punto a punto son las encargadas de enlazar dos DTE (Equipo Terminal de Datos) líneas multipunto, utilizados por dispositivos que visualizan, generan o almacenan la información para el usuario.

2.1.3.4. Líneas Digitales

En las líneas digitales, los bits son transmitidos en forma de señales digitales, por el cual cada bit se representa por una variación de voltaje empleando la codificación digital. Estas líneas están diseñadas para el transporte de tráfico de datos a velocidades de hasta 45 Mbps (Navas, 2006).

2.1.4. Limitaciones de la WAN

Con tanta información siendo creada de manera muy rápida y desplazada por la red implica que las empresas evolucionen a redes centralizadas adoptando tendencias como la nube, IoT, nuevas tecnologías y soluciones garantizando la trasmisión de datos de manera segura, aumentando la importancia de la red corporativa (Rodríguez, 2019).

En los últimos años, las redes actuales de los operadores de red han crecido en gran volumen con múltiples variedades de dispositivos de hardware propietarios como consecuencia se producen limitaciones al poner en marcha un nuevo servicio de red, como son:

- Disponer de operadores de red con habilidades para diseñar, integrar y operar equipos basados en hardware más complejos.
- El periodo de vida útil de los equipos hardware son cada vez más cortos debido al aumento de servicios y consumo de ancho de banda.
- Alto consumo de energía en el uso de múltiples equipos propietarios.

2.2. Redes Privadas Virtuales (VPN)

Una red privada virtual es un sistema o implementación que habilita una comunicación segura a través de un medio inseguro, sin causar ningún problema para el usuario u aplicación que realiza y recibe la comunicación (Fernández, 2006).

En la VPN se combinan dos conceptos fundamentales: redes privadas y redes virtuales. Los enlaces de las redes virtuales son lógicos y no físicos. La topología de la red virtual es independiente de la topología de la red física, por lo tanto un usuario de red virtual no podrá detectar la red física, el solo será capaz de ver la red virtual (Atencio, 2017).

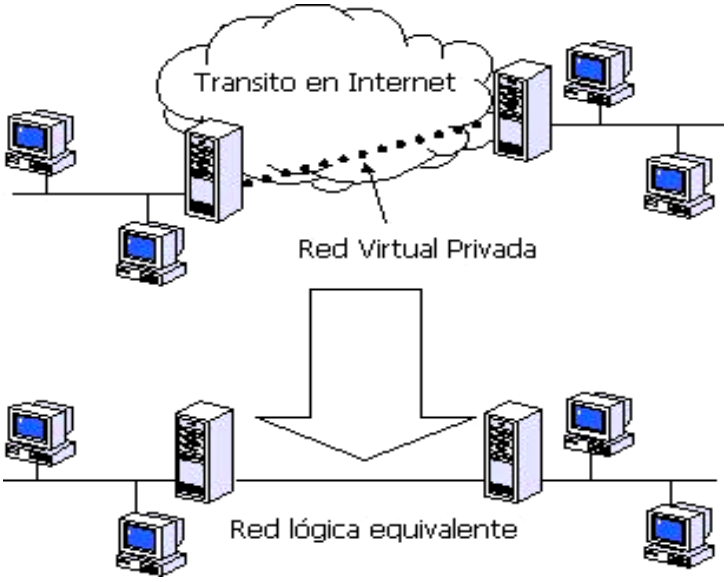


Figura 2. 4 Esquema de una VPN
Fuente: (Rugerio, 2013)

2.2.1. Funcionalidades de la VPN

- **Confiabilidad o integridad:** Es decir, los datos que se transfieren entre remitente y receptor no se deben de cambiar.

- **Disponibilidad:** Deben de estar disponibles los datos transferidos en cualquier momento que se los necesite.
- **Confidencialidad o privacidad:** Los datos que son transferidos, únicamente estarán disponibles solo para usuarios autorizados.
- **No repudio:** Es un respaldo que caso que se impida que un documento firmado se trataste o niegue de haberlo redactado.

2.2.2. Topologías VPN

En las redes privadas virtuales, existen tres tipos de topologías las cuales son: cliente a servidor, cliente a red interna y red interna a red interna.

a) **Cliente a servidor:** EL usuario remoto puede ejecutar aplicaciones desde el servidor, para ello necesita tener ciertos privilegios para entrar al servidor VPN.

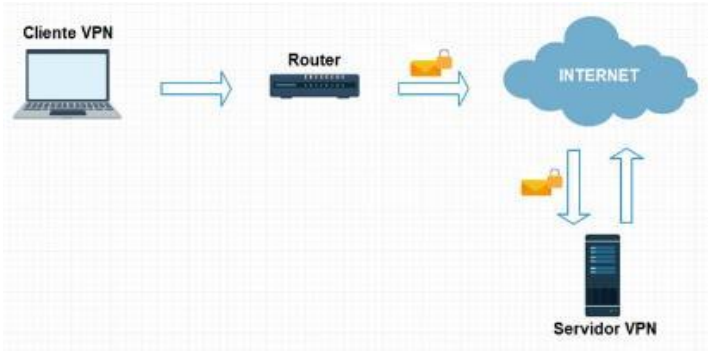


Figura 2. 5 Topología cliente servidor
Fuente: (Romero, 2019)

b) **Cliente a Red Interna:** Existen varios equipos de cómputo dentro de esta misma red que permiten al usuario remoto ejecutar aplicaciones o utilizar múltiples servicios. Es utilizada por entidades bancarias por su gran número de solicitudes diarias por cada servicio.

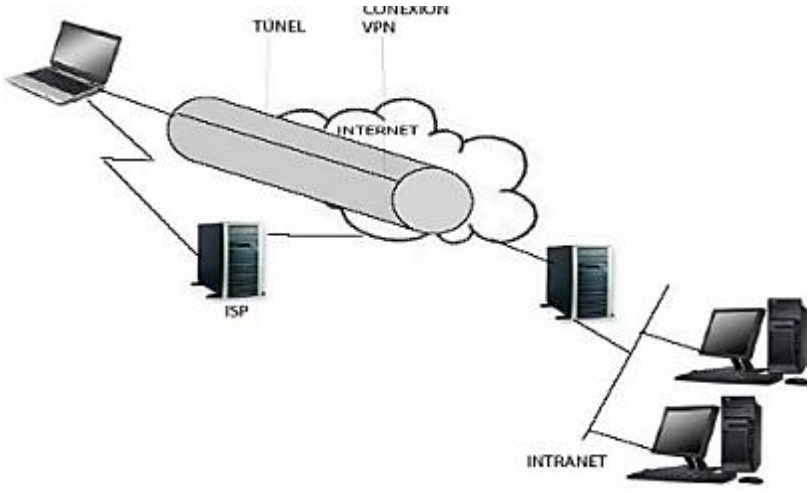


Figura 2. 6 Topología cliente a red interna
Fuente: (Mejía, 2012)

c) **Red interna a Red Interna:** Es la que conecta dos redes internas, mediante dispositivos como routers, switches, haciendo posible intercambiar datos entre sucursales, sin importar las aplicaciones o servicios que utilicen ambas redes.

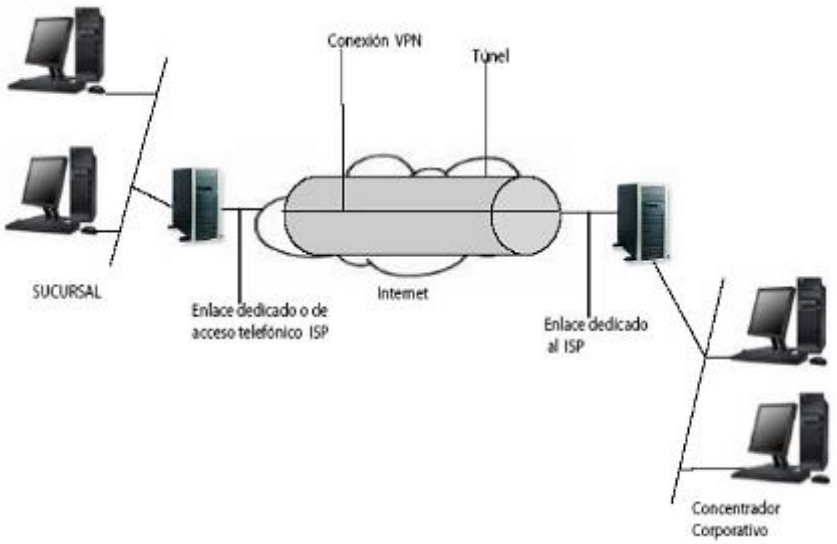


Figura 2. 7 Topología red interna a red interna
Fuente: (Mejía, 2012)

2.2.3. Elementos de una VPN

Los elementos que integran una VPN son:

- **Servicio VPN:** Es un computador físico o virtual que habilita la conectividad entre redes, permitiendo configurar y administrar conexiones que incluyen seguridad, permisos de usuarios, parámetros de autenticación de los puertos de enrutamiento.
- **Túnel:** Es una parte de la conexión en la que los datos están encapsulados y se transfieren de extremo a extremo.
- **Conexión VPN:** Son parte del enlace en donde los datos son encriptados para más seguridad a lo largo de toda la conexión VPN.
- **Red Pública:** Es la red en la que se transfieren los datos de un lugar a otro, de forma insegura. LA red pública utiliza VPN para agregar seguridad a los datos que viajan encapsulados.
- **Cliente VPN:** Es un computador que realiza conexiones desde un enrutador o servidor individual.

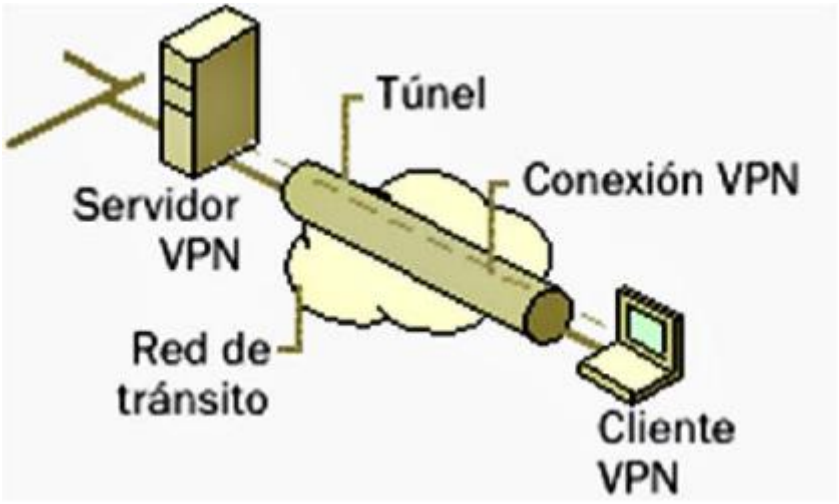


Figura 2. 8 Elementos de una VPN
Fuente: (Atencio, 2017)

2.2.4. Tipos de VPN

2.2.4.1. Sistemas basados en Software

Las redes privadas virtuales basadas en software son programas que establecen conexión de host a host, caracterizado por su flexibilidad del tráfico, fácil configuración y adaptación a varias plataformas. Estos sistemas son precisos en conexiones entre VPN que no está controladas por la misma organización, se utiliza el modelo cliente servidor. En esta clase de arquitectura es indispensable contar con una buena administración de claves y llaves públicas (Pacheco, 2015).

2.2.4.2. Sistemas basados en Hardware

Por otro lado, la red privada virtual basada en hardware, está conformada por dispositivos con VPN incorporada como, por ejemplo: los routers, firewalls, switches, son fáciles de usar brindan un mejor rendimiento y seguridad. Estos dispositivos tienen integrado un procesador, algoritmos de encriptación y desencriptación. El sistema es independiente de las maquinas conectadas a la red, hasta un solo elemento logra habilitar varias VPNs ubicadas en diferentes sitios (Pacheco, 2015).

2.2.5. Arquitectura VPN

2.2.5.1. VPN de Acceso Remoto

Este tipo de VPN es el más usado por las empresas, consiste en usuarios remotos que se conectan desde cualquier parte del mundo hacia la empresa, utiliza como medio de comunicación internet de banda ancha. Para lograr la conexión de la VPN de acceso remoto con la empresa, es necesario que el usuario remoto utilice dispositivos con funciones de enrutamiento o un firewall para un túnel virtual que conduce hacia la organización, validando la identidad del usuario que acceda a la red (Martel, 2019)

Figura 2. 9 VPN de Acceso Remoto
Fuente: (Martel, 2019)

2.2.5.2. VPN sitio a sitio

Este tipo de VPN se utiliza para conectar sucursales remotas con la sede de la organización. En este caso el servidor VPN ubicado en la sede principal aprueba las conexiones vía internet estableciendo un túnel virtual. La conexión a internet permite eliminar costos de enlaces punto a punto especialmente en conexiones distantes. (Martel, 2019)

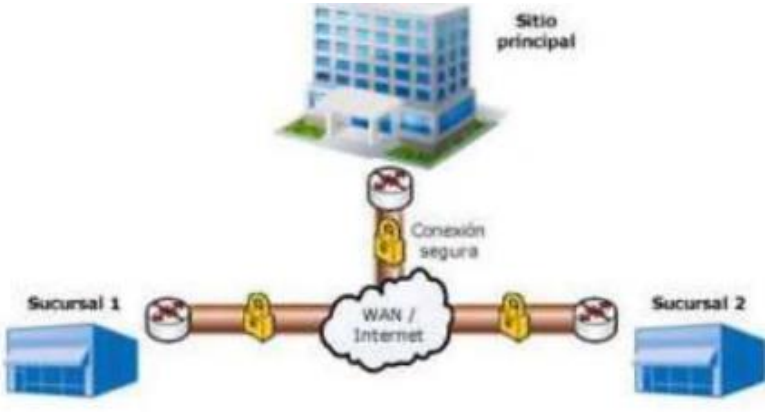


Figura 2. 10 VPN sitio a sitio
Fuente: (Martel, 2019)

2.3. Protocolos de Tunneling

Basándose en el modelo OSI, las VPN pueden crear un túnel de extremo a extremo utilizando tecnologías de tunneling, tomando en cuenta que ambos puntos deben de estar sincronizadas de igual manera como son los parámetros de comprensión, encriptación, configuraciones y asignación de direcciones. La tecnología de tunneling utiliza protocolos basado en datagramas para transferir los datos (Ramos, 2016).

Es el proceso que realiza una infraestructura entre redes para la transmisión de datos exclusivamente privados. El protocolo de tunelización hace uso de una red intermedia por la cual las tramas transferidos son encriptados y encapsulados de extremo a extremo. Cuando una trama pasa por el camino lógico se desencapsula y se envía a su destino final dentro de la red (Ñacato, 2007).

Las tecnologías de tunneling son:

- IPX for Novell Netware over IP
- DLSW – Data Link Switching (SNA over IP)
- GRE – Generic Routing Encapsulation (rfc 1701/2)
- Mobile IP – For mobile users
- PPTP – Point to Point Tunneling Protocol
- ATMP – Ascend Tunnel Management Protocol
- IPSec – Internet Protocol Security Tunnel Mode
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

Entre estas tecnologías se destacan 3 protocolos que son:

- IPSec – Internet Protocol Security Tunnel Mode
- L2TP – Layer 2 Tunneling Protocol
- PPTP – Point to Point Tunneling Protocol

2.3.1. Protocolo PPTP

El protocolo PPTP o por sus siglas en inglés, Point to Point Tunneling Protocol que significa Protocolo Tunelizado Punto a Punto, es utilizado comúnmente para conexiones dial-up, empleando líneas telefónicas como internet desplazados en redes privadas permiten la transferencia desde clientes remotos a servidores de manera segura (Atencio, 2017).

PPTP es una extensión del acceso remoto del protocolo PPP (Point to Point Protocol), encapsula tramas PPP en datagramas IP para la transmisión empleando redes basadas en TCP/IP tal como el internet. El protocolo PPTP utiliza el puerto 1723 para el envió de tramas PPP encapsuladas y poder realizar el mantenimiento del túnel (Ramos, 2016).

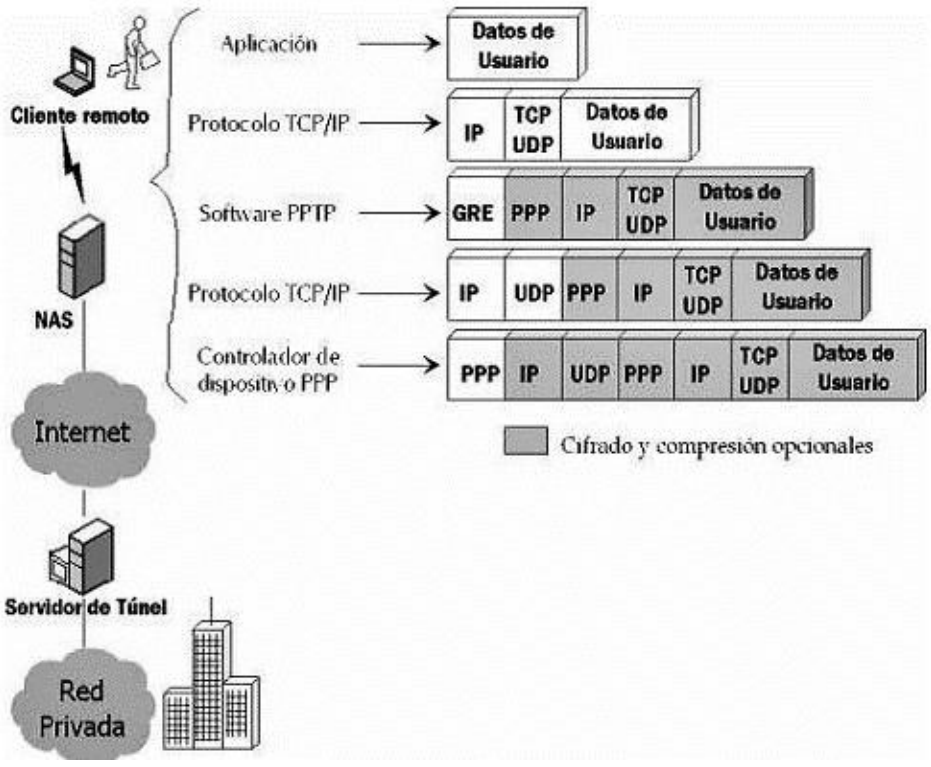


Figura 2. 11 Protocolo PPTP
Fuente: (Ramos, 2016)

2.3.2. Protocolo L2TP

El protocolo L2TP o por sus siglas en inglés, Layer Tunneling Protocol que significa Protocolo de Túnel de Capa 2, es una tecnología de túnel multiprotocolo, basado en el protocolo PPTP creado para conectar redes a través de internet y transmitir datos de forma segura. Proporciona un método de encapsulamiento que permite crear un túnel dentro de una red IP para el transporte de tramas PPP sobre redes IP, Frame Relay, o ATM (Ramos, 2016).

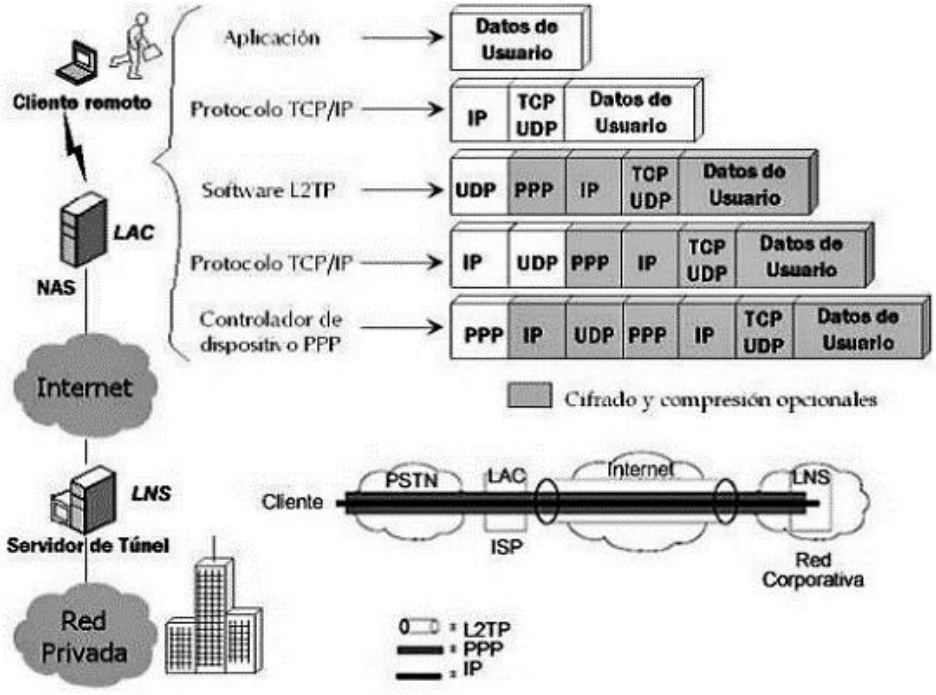


Figura 2. 12 Protocolo L2TP
Fuente: (Ramos, 2016)

Un túnel L2TP es similar a una sesión, diseñado principalmente para conexiones de acceso remoto, conexiones sitio a sitio. El protocolo L2TP requiere de certificados digitales y negociar variables de configuración:

- Parámetros de comprensión
- Cifrado
- Asignación de direcciones

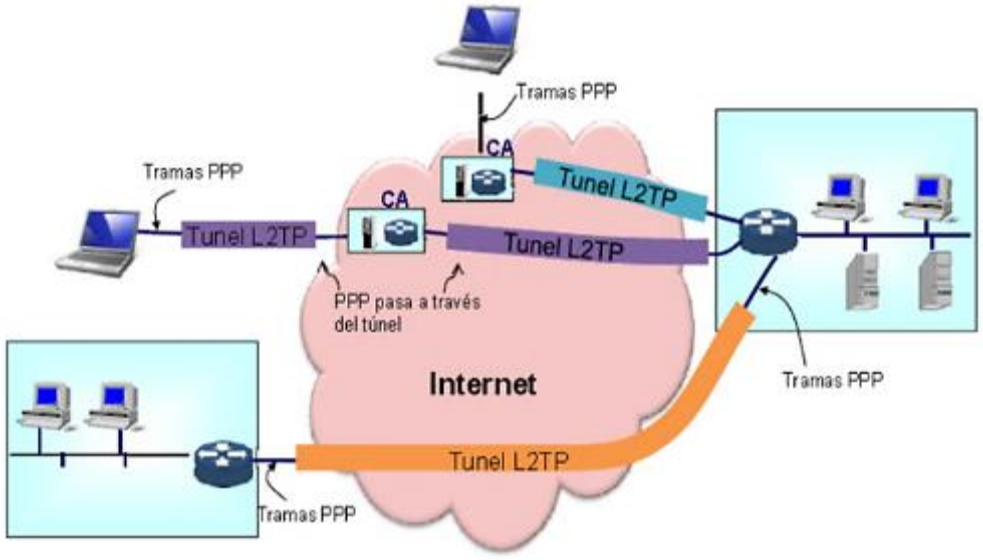


Figura 2. 13 Diseño de túneles L2TP
Fuente: (Autor)

El protocolo L2TP, trabaja sobre UDP en el puerto 1701. No es un protocolo de VPN debido a la falta de seguridad, sin embargo, se puede combinar con el protocolo IPsec para crear un entorno seguro.

2.3.3. Protocolo IPsec

El protocolo de seguridad de internet (IPsec, Internet Protocol Security), es una de las tecnologías de seguridad más importante y ampliamente utilizado en redes privada virtuales (VPN). Trabaja a nivel de capa 3 diseñado para proporcionar seguridad end to end de la capa de red implementada en los clientes, servidores o routers.

IPsec es un conjunto de protocolos IP, basados en algoritmos que proveen servicios de seguridad en las redes ofreciendo:

- Confidencialidad
- Autenticación
- Integridad
- Intercambio de claves

Diseñado para brindar optima seguridad las organizaciones o empresas a través de los routers y cortafuegos. El protocolo IPsec tiene como ventaja fundamental especificar el tráfico a proteger, que mecanismo utiliza para proteger el tráfico y elegir a quien se envía el tráfico. Los componentes del protocolo IPsec son.

- Protocolos de autenticación, cifrado y comprensión:
  - AH (Authentication Header) o Cabecera de Autenticación. - Proporciona autenticación de origen de los paquetes IP, integridad en la conexión y protección contra ataques de mensajes de repetición.
  - ESP (Encapsulating Security Payload) o Carga de seguridad de encapsulación. – Provee servicios en conjunto de chequeo de integridad, confidencialidad en sus enlaces limitados de flujo de tráfico, autenticación de origen y protección contra paquetes de repetición.
- Protocolos relacionados con la gestión de claves:
  - IKE (Internet Key Exchange Protocol) o. Protocolo de intercambio de claves de internet. – Maneja el intercambio de las negociaciones de seguridad y distribución de llaves de autenticación. Para levantar una VPN IPsec se utiliza el protocolo IKE

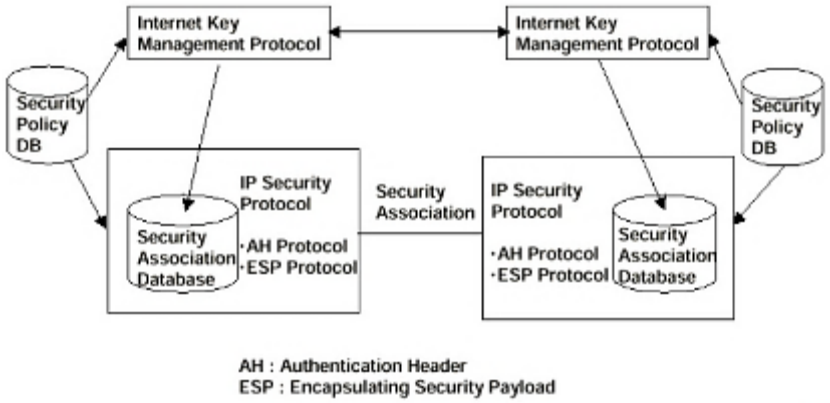


Figura 2. 14 Arquitectura IPsec
Fuente: (Autor)

2.3.4. Modos de IPsec

El protocolo de seguridad de internet (IPsec), soporta dos modos de uso:

- Modo transporte:
  - Comunicación segura, autenticación extrema a extremo
  - Seguridad en la carga útil del paquete (payload)
  - Los protocolos AH y ESP ofrecen protección a los protocolos de capas superiores
  - El enrutamiento permanece intacto por lo que la cabecera IP no se modifica

- Modo túnel:
  - Se utiliza este modo solo para la comunicación segura entre routers o gateways
  - Se encripta el datagrama IP protegiendo los paquetes en la capa de red
  - Este modo se integra de manera cómoda. en las VPNs
  - Solo funciona para los datagramas IP en IP

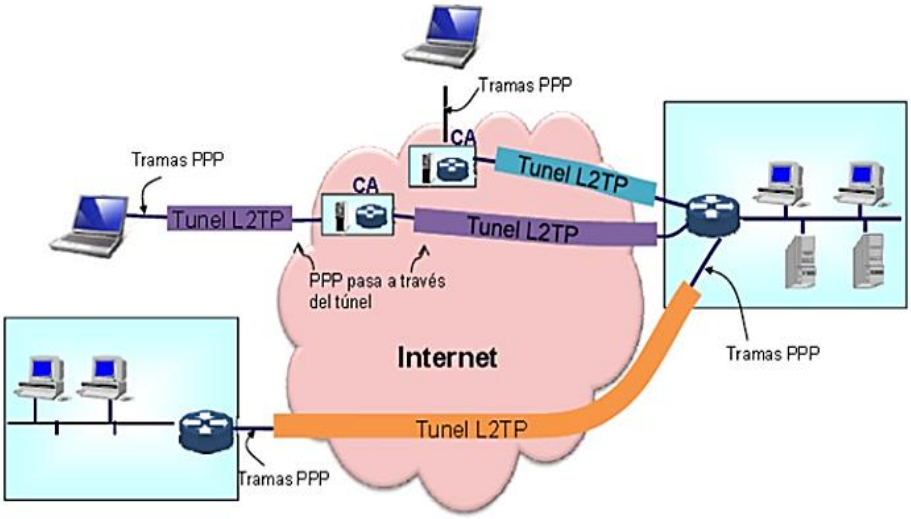


Figura 2. 15 Arquitectura IPsec
Fuente: (Quijano, 2014)

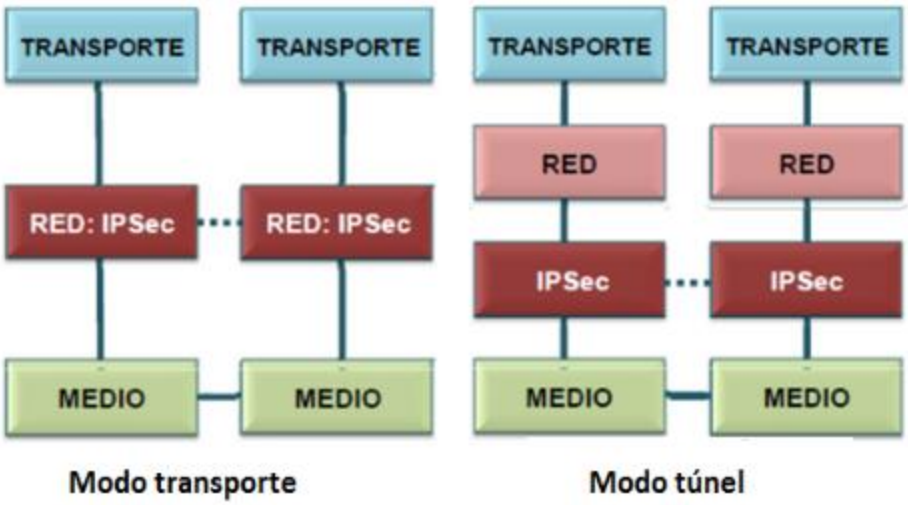


Figura 2. 16 Modos de empaquetamiento
Fuente: (Autor)

La tecnología IPsec fue desarrollado para IPv6 con implementaciones de IPv4, permite asegurar protocolos de la capa de transporte (TCP/UDP) y operar sobre la capa de red. Una VPN IPsec puede implementar un túnel entre dos puntos extremos considerándose segura y protegida (Ramos, 2016).

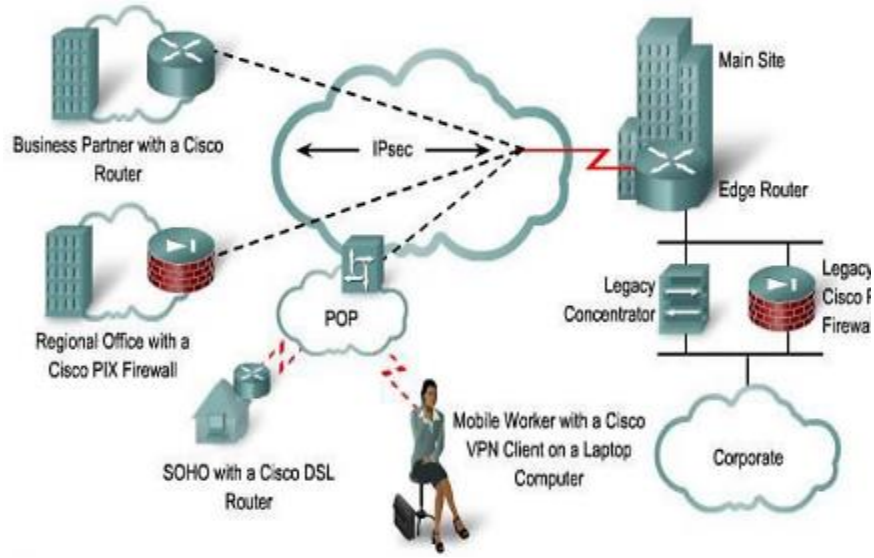


Figura 2. 17 Forma de trabajo de IPsec
Fuente: (Atencio, 2017)

2.4. Virtualización de Red (NV)

Es la combinación de los recursos de red del software con los recursos de red del hardware por medio de una sola unidad administrativa. Permite facilitar el uso compartido de recursos de redes de manera controlada, segura para los usuarios, programar, diseñar, y gestionar los servicios de red bajo demanda sin necesidad de contar con un acceso físico como conmutadores y enrutadores a la infraestructura de la red (Telefónica, 2016)

La virtualización de red utiliza dos tecnologías NFV (Virtualización de Funciones de Red) y SDN (Redes Definidas por Software), simula en software una plataforma de hardware, proporcionando redes de extremo a extremo que se dividen de la red física subyacente. El software computacional o virtual reside en un servidor en otro lugar de la red mientras que le hardware físico no cambia (Ríos, 2016)

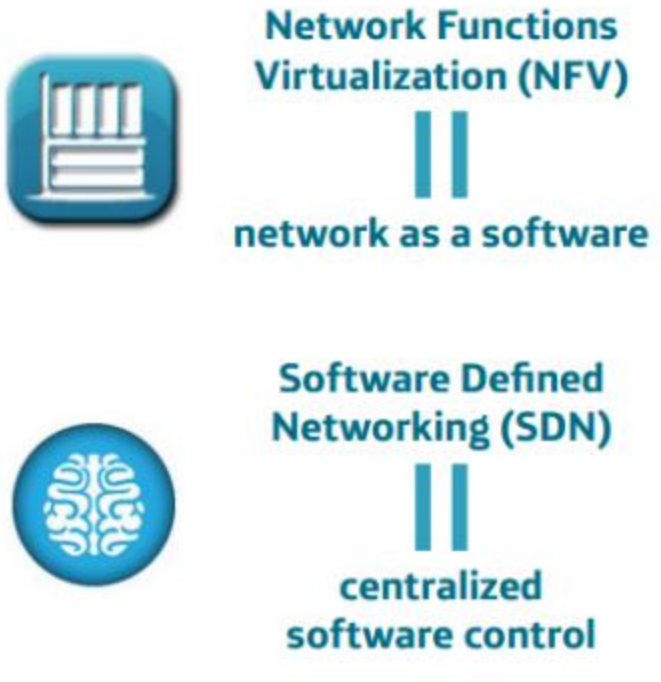


Figura 2. 18 Componentes de la NV
Fuente: (Telefónica, 2016)

2.4.1. Virtualización de funciones de red (NFV)

La virtualización de funciones de red, permite convertir cada nodo de red en un microcentro de datos en la que se pueden alojar varias aplicaciones, es decir puede convertir un nodo local en el operador de los servicios que distribuye a sus clientes. (López, 2019)

Es una tecnología que desvincula las funciones de red de dispositivos de hardware, ubicándolos en servidores virtuales permitiendo múltiples funciones en un único servidor físico. De esta manera reduce los costos en los equipos más cercanos al cliente, ahorro de instalación, mantenimiento y servicio técnico. NFV está regulada por la ETSI (Instituto de Normas Europeas), especifica que la virtualización de funciones de red, se basa en 3 criterios clave (Carbonel, 2018).

- Desacoplo del software y hardware
- Despliegue flexible de funciones de red
- Gestión dinámica

La premisa básica de la NFV es la migración de las funciones de hardware dedicado hacia dispositivos genéricos como por ejemplo los servidores x86.

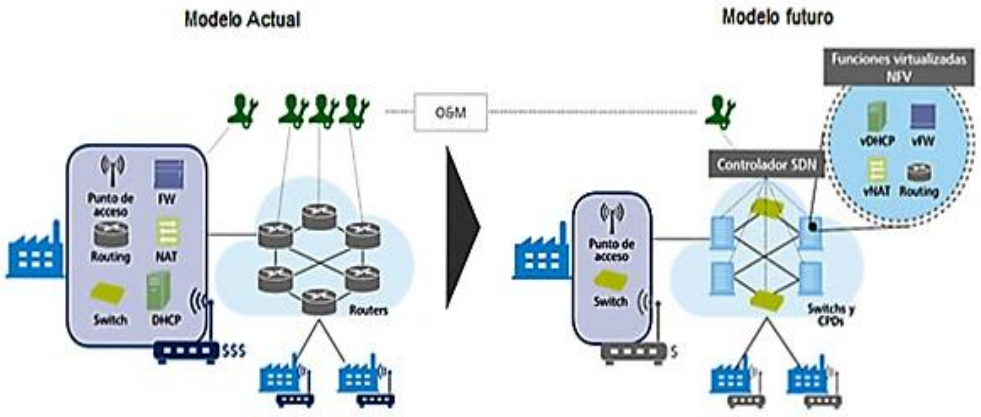


Figura 2. 19 Evolución del modelo de red.
Fuente: (Ríos, 2016)

El enfoque de esta tecnología tiene como principal ventaja la flexibilidad que ofrece a los operadores de red para la gestión de servicios ofrecidos, mediante NFV los controladores de red pueden orquestar funciones de red de forma dinámica sin necesidad de modificar el equipo físico de las instalaciones del cliente, adaptándose a las necesidades de la red (Carbonel, 2018).

En general, la virtualización se enfoca en los siguientes elementos:

- Dispositivos de IT: firewalls, sistemas de gestión de dispositivos de red, sistemas de detección de intrusos (IDS).
- Dispositivos de función de red: routers, switches, puntos de acceso a red.
- Almacenamiento vinculado a red: servidores de archivos o bases de datos conectados a red.

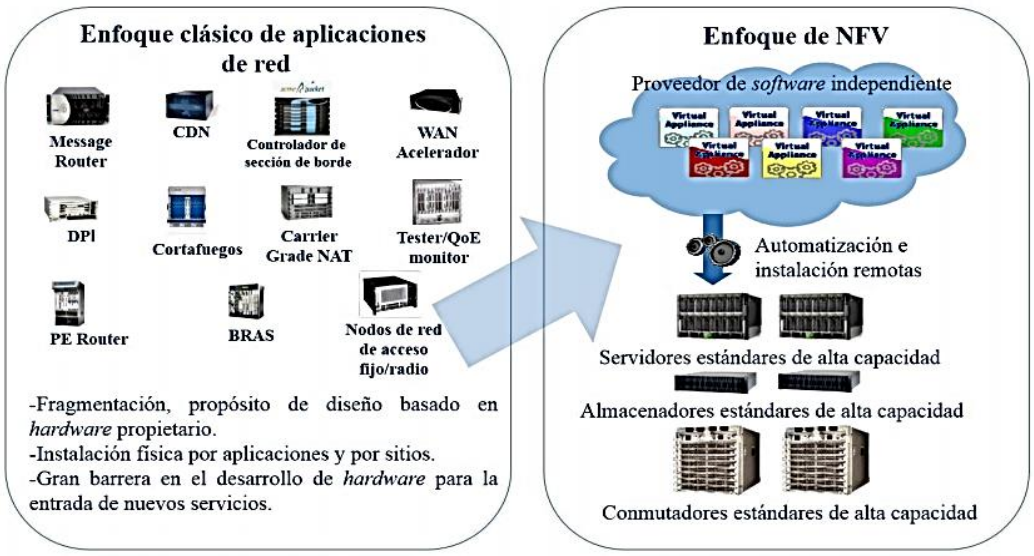


Figura 2. 20 Visión de la NFV
Fuente: (J. Herrera, 2019)

Con este método se logra sustituir elementos especializados y complejos que se ejecutan sobre un hardware genérico empleando soluciones basadas en plataformas compartidas que brindan flexibilidad a la red e independencia de los fabricantes (J. Herrera, 2019)

2.4.2. Arquitectura NFV

Las funciones de red virtuales (NFV), consta de 3 elementos claves: las funciones de red virtuales VNF, infraestructura de la NFV o NFVI y una capa paralela de orquestación y gestión MANO.

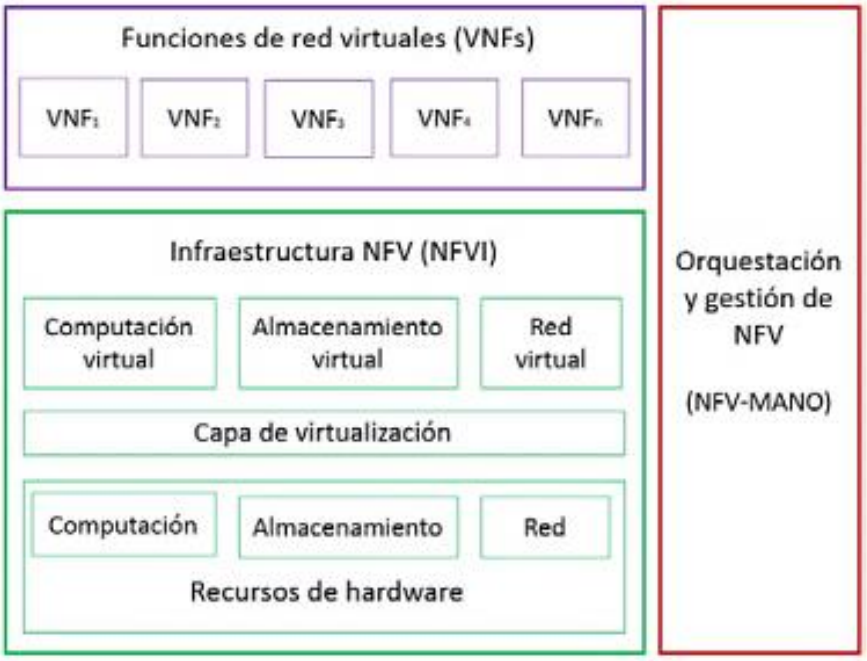


Figura 2. 21 Arquitectura NFV
Fuente: (Dorantes, 2017)

2.4.2.1. VNF Virtual Networks Funtions

Es una implementación de una función de red virtualizada más conocida como servicio de red (firewall, routers, balanceadores de cargas), se pueden instalar en una o múltiples máquinas virtuales. Estas funciones son gestionadas por controladores (VNF manager) para comunicarse con los elementos de la red por medio de interfaces abiertas, o haciendo uso de los sistemas de gestión de elementos (EMS), se conecta con los sistemas de gestión de la red y con las VNF para proporcionar información requerida por los sistemas de soporte de operaciones (Dorantes, 2017)

2.4.2.2. NFVI Infraestructura de virtualización de funciones de red

La infraestructura NFVI, es la que integra todos los componentes de infraestructura tales como:

- Computadoras
- Redes
- Almacenamiento
- Red definida por software
- Servicio de Red

Todos estos componentes se ubican en una plataforma para soportar software como pueden ser un hipervisor o una plataforma de administración las cuales son necesarias para la ejecución de las aplicaciones de red. Se puede decir que la NFVI es el entorno por el cual las funciones de red virtuales son desplegadas ya que esta infraestructura NFVI combina los recursos de hardware y software (J. Herrera, 2019)

2.4.2.3. NFV–MANO (Orquestación y gestión)

La capa de MANO se encarga de la orquestación y gestión de los recursos tanto del hardware como del software las cuales soporta la infraestructura virtualizada (NFVI) y las funciones de redes virtuales (VNF).

LA orquestación tiene como función dirigir, gestionar y automatizar las operaciones de red principalmente a los servicios de red de extremo a extremo que son utilizados para el intercambio de información entre los componentes para garantizar el correcto funcionamiento en la red. Los gestores de NFV, son responsables de la administración de la virtualización incluyendo actualizaciones, escalamiento consultas y terminación (J. Herrera, 2019)

2.4.3. Redes definidas por Software (SDN)

Las Redes Definidas por Software (Software Define Network), es una reciente tecnología diseñada para hacer más versatil y flexible la red empresarial. En las redes actuales muchas de las veces estás son estáticas, lentas para cambiar, y dedicadas a servicios individuales. Con las redes definidas por software se pueden crear una red que administre muchos servicios distintos de manera dinámica permitiendo consolidar múltiples servicios en una infraestructura común para proveedores y operadoras. Por ejemplo, un proveedor de servicios (ISP), desea asignar el mayor ancho de banda de su red metro a servicios empresariales durante el día, a servicios de internet durante la noche, movimientos de máquinas virtuales y soluciones de backup durante la noche, esto permite al proveedor de servicios consolidar tres redes diferentes en una red poderosa que puede asignarse bajo demanda.

La SDN es un nuevo modelo de gestión de networking que pretende estandarizar y automatizar la administración de las redes, ideal para un gran ancho de banda y facilitando la escalabilidad de la red. Por lo tanto, se puede decir que las redes definidas por software, es una manera de virtualizar redes con el objetivo de facilitar la configuración y el mantenimiento de la misma forma que los servidores.

La red definida por software es una arquitectura que separa el plano de control de los enrutadores subyacentes y plano de datos de conmutadores que reenvían el tráfico. Esta separación de planos permite que los conmutadores de red se transformen en simples dispositivos de reenvió implementando la lógica de control por medio de un controlador lógico centralizado, reduciendo la configuración de red y las aplicaciones de políticas (Ahmed et al., 2018)

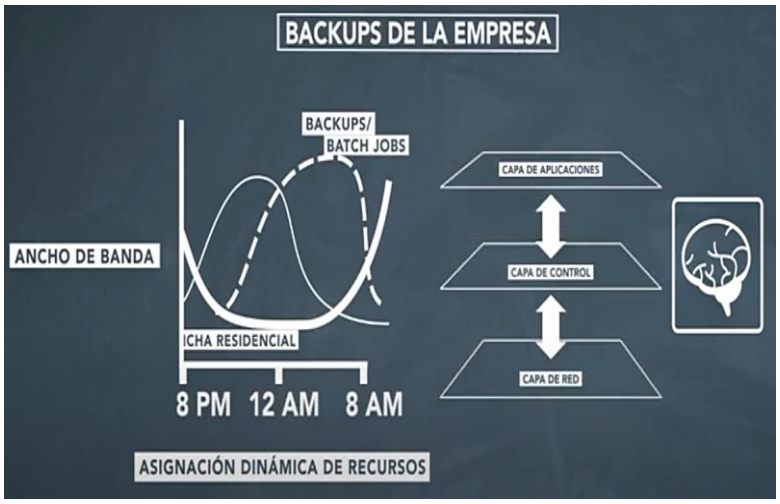


Figura 2. 22 Ejemplo del uso de una SDN
Fuente: (Autor)

2.4.4. Arquitectura SDN

Las redes definidas por software se caracterizan por el desacoplo entre el plano de control y el plano de datos de esta separación la arquitectura SDN se compone de tres capas: Capa de Aplicación, Capa de Control y Capa de Infraestructura.

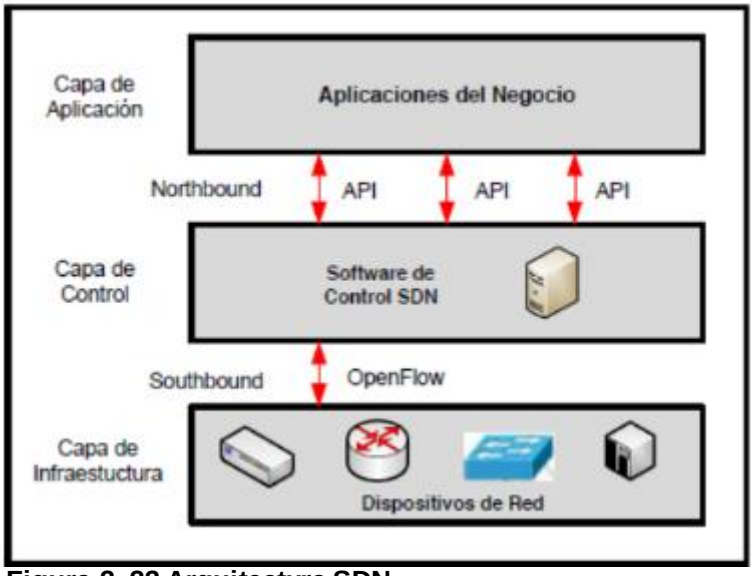


Figura 2. 23 Arquitectura SDN
Fuente: (Bonilla, 2016)

2.4.4.1. Capa de Aplicación

Es donde las aplicaciones empresariales, de nube, de administración colocan sus demandas de red sobre la capa de control. Esta capa contiene aplicaciones de red que incorporan nuevas funciones de red tales como capacidad de administración, reenvió a la capa de control y seguridad. Posee una vista global de toda la red. Cabe mencionar que la interfaz entre la capa de aplicación y la capa de red se la denomina Interfaz hacia el Norte (Northbound Interface), esta interfaz proporciona su propia API a las aplicaciones de red (Manzano, 2020).

2.4.4.2. Capa de Control

Es la capa intermedia o capa de control es la encargada de configurar la capa de infraestructura lo hace recibiendo solicitudes de servicios desde la tercera capa. La capa de control especifica las solicitudes de servicios sobre la capa de infraestructura de la manera más óptima posible configurando dinámicamente la capa de infraestructura

2.4.4.3. Capa de Infraestructura

También llamada capa de plano de datos, es la capa inferior formada por conmutadores y enrutadores físicos o virtuales (routers, switches, firewalls), los cuales están conectados por una interfaz abierta permitiendo el reenvió de datos, el monitoreo de la información local y la administración de las tablas de flujo por medio de un controlador empeñado en agregar o cambiar dispositivos. Estas conexiones se realizan a través de diferentes medios de transmisión como el cobre, fibra óptica incluyendo las redes inalámbricas (Lobo, 2016)

2.4.5. Interfaces SDN

En las interfaces abiertas que posee la capa de control, la primera interfaz interactúa con la capa de datos llamada Interfaz hacia el Sur (Southbound), mientras que la otra interactúa con la capa de gestión llamada Interfaz hacia el Norte (Northbound). Por otra parte, existen interfaces que permiten la comunicación con los demás controladores denomidanas Interfaces hacia el Este (Eastbound) e Interfaces hacia el Oeste (Westbound).

- **Interfaz Southbound:** Permiten que los sistemas de administración de red puedan conectarse directamente sin problema a los elementos de la red y que a su vez los administren.
- **Interfaz Northbound:** Permite la comunicación entre aplicaciones y controladores, realizando configuraciones de red con las peticiones de cada aplicación.
- **Interfaces Eastbound y Westbound:** Permiten enlazar e interconectar las redes convencionales con las redes definidas por software. A demás consigue una visión global influyendo en las decisiones de enrutamiento de cada controlador.

2.4.6. Beneficios de SDN

- Basada en estándares abiertos, permite que los operadores o administradores de red manipulen e implementen mejoras de forma independiente.
- Gestión centralizada, por medio de un controlador SDN empleando múltiples configuraciones para el tráfico que fluye por la red.
- Administrar dinámicamente los recursos de ancho de banda dependiendo a las necesidades de cada usuario.

- Reduce la complejidad a través de la automatización, haciendo posible el desarrollo de herramientas para simplificar la administración de red.
- Incrementa la seguridad y fiabilidad de la red, mediante el uso de políticas y reglas específicas garantizan mayor disponibilidad, confiabilidad y sobre todo seguridad reduciendo el riesgo de fallas.
- Bajo costo de inversión y operación, siendo una infraestructura mucho más simple, reduce los gastos en mano de obra especializada y costos de interfaces de ancho de banda.
- Agilidad en crecimiento y desarrollo de aplicaciones, gracias a estos recursos los administradores de red pueden adecuar la infraestructura en base a las necesidades del usuario final.
- Mejor experiencia por parte del usuario, se adapta mejor a las necesidades del usuario de manera dinámica.

2.4.7. Controlador SDN

Las redes definidas por software poseen integrado un controlador que es la parte central de toda la arquitectura SDN. Dentro del controlador los administradores son responsables de definir reglas para gestionar el flujo de datos en la red, permitiendo una rápida configuración a diferencias de las redes tradicionales. Se puede decir que el controlador SDN es el cerebro de la arquitectura de las redes definidas por software ya que maneja toda la inteligencia de la red (Albán, 2015).

2.5. SD-WAN (Software Defined Wide Area Network)

La red de área amplia definida por software es considerada como la tecnología de arquitectura más prometedora de la red de área amplia de próxima generación, ya que simplifican drásticamente los procesos de administración permitiendo su innovación y evolución. Separa el plano de control del plano de datos simplificando la construcción de conexiones y la gestión entre diferentes sitios como centros de datos en redes de centros de datos y sucursales en redes empresariales, proporcionando alta disponibilidad, flexibilidad, control centralizado, garantizando fácil y rápido acceso a las aplicaciones críticas en la nube reduciendo costos de enlaces WAN privados para la empresa (Yang et al., 2019).

SD-WAN puede definirse como el hermano menor de las redes definidas por software (SDN), ya que ambos están definidos por software, pero la diferencia es que SDN es una arquitectura dirigida a los centros de datos internos en una sede, mientras SD-WAN es una tecnología que utiliza estos conceptos definidos por software para la distribución de tráfico de la red a través de una WAN y mejora el desempeño de los recursos para las implementaciones en distintas sucursales (Lerner, 2017). Es una tecnología que nos permite de manera lógica unificar diversos tipos de enlaces en un solo camino y enviar tráfico con alta disponibilidad para los servicios y clientes (Gartner, 2019).

Las redes de área amplia definidas por software (SD-WAN), tienen como principal objetivo proporcionar control centralizado en puntos de acceso (AP), como por ejemplos equipos que se encuentran alojados en parques o negocios mejorando la administración, la flexibilidad facilitando el uso de entornos de redes inalámbricas (Sánchez, s. f.)

2.5.1. Características de una red SD-WAN

- **Elección y control optimizado:** Proporciona control centralizado para la configuración, administración y orquestación de la red WAN, con la aplicación de dispositivos de red programables.
- **Seguridad integrada:** Mediante la aplicación de políticas contextuales brinda protección contra amenazas a los usuarios, dispositivos y aplicaciones. Enrutamiento del tráfico de forma segura a través de enlaces de internet de banda ancha de bajo costos.
- **Escalamiento y optimización para la nube:** Conecta su red WAN a múltiples nubes públicas, ofreciendo rendimiento optimizado para aplicaciones críticas y plataformas de la nube como Azure, Aws, Orange cloud, Microsoft teams.
- **Experiencia de aplicación:** Mejora la productividad de los usuarios mediante análisis, visibilidad y control de la red en tiempo real. Mediante la optimización brinda un óptimo rendimiento de las aplicaciones en la nube, desde diferentes nubes hasta los usuarios en cualquier lugar.

2.5.2. Arquitectura de la red SD-WAN

La arquitectura tradicional de la red de área amplia ya no es la adecuada para el aumento de tendencias de redes, usos de aplicaciones y cumplir con los requisitos de calidad de servicios para los usuarios. La redes de área amplia definida por software tienen como visión simplificar la creación de redes , reducir operaciones, optimizar e introducir innovación y flexibilidad en comparación de las redes de área amplia tradicionales (Yang et al., 2019).

A continuación, damos visión del plano lógico y físico de las arquitecturas de red de área amplia definida por software (SD-WAN)

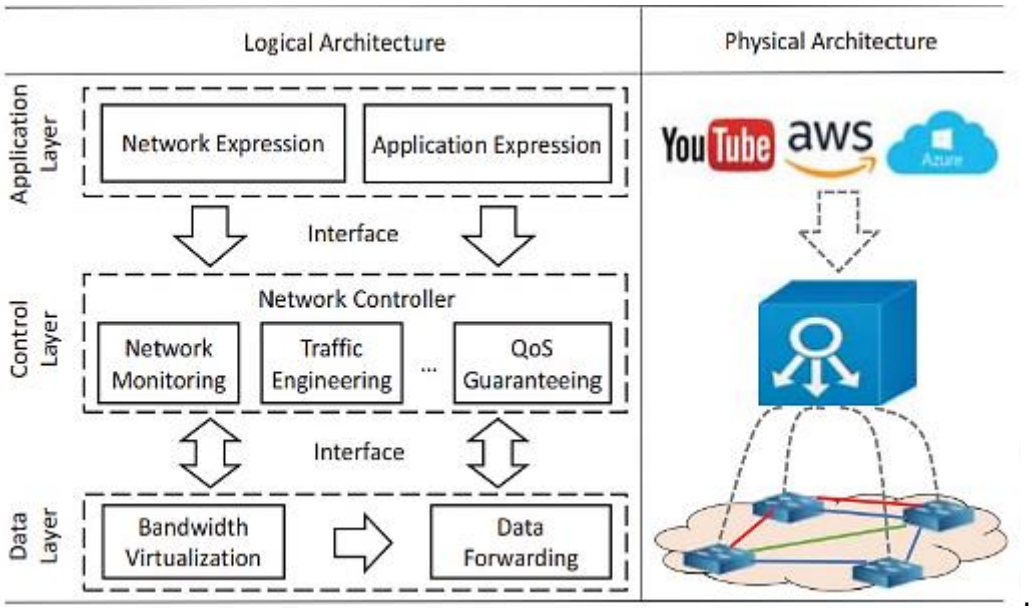


Figura 2. 24 SD-WAN: arquitectura lógica y física
Fuente: (Yang et al., 2019)

Arquitectura lógica:

Existen 3 capas de abajo hacia arriba en la red de área amplia definida por software, las cuales incluyen la capa de software, capa de control y capa de aplicación como se muestra en la figura 2.1

- **Capa de datos:** Se clasifica en virtualización de ancho de banda y reenvío de datos. Para utilizar completamente los recursos de ancho de banda, la virtualización combina múltiples enlaces de red brindando una ubicación de recursos disponibles para todos los servicios y aplicaciones (Yang et al., 2019)

  El reenvío de datos es un conjunto de elementos de red de reenvió distribuido para reenviar paquetes utilizando el ancho de banda proporcionado por la virtualización (Bannour et al., 2018)

- **Capa de control:** Es la capa más importante dentro de la arquitectura SD-WAN, ya que se encarga de centralizar las aplicaciones, visualizar la estructura de red y configurar cada nodo de red colocado en distintas rutas para el envío y recepción de trafico seleccionando el mejor camino y tomando las decisiones de enrutamiento de tráfico para la red (Guanoluisa, 2019).

- **Capa de aplicación:** Es la capa de más alto nivel, encargada de establecer aplicaciones de manera centralizada ejecutando las configuraciones, abastecimiento y extendiendo nuevos servicios en la red. La comunicación entre la capa de aplicación y la capa de control se la realiza mediante una API, la cual permite conocer el estado general de la red ayudando a mejorar la transmisión de datos para aplicaciones específicas (Brito, 2018)

  La API de red muestra la topología completa y la conectividad de la red. Las aplicaciones definen el comportamiento de la red, pueden consultar información de las propiedades como las cargas de tráfico (Cosío, 2017)

Arquitectura física:

En la capa de datos existen un conjunto de controladores SDN interconectados entre sí por medio de enlaces físicos. Cada controlador de red está encargado de estos dispositivos.

Comúnmente el controlador de red es un servidor o un clúster, esto dependerá de la complejidad y tamaño de la red. Los proveedores y desarrolladores de aplicaciones pueden expresar sus requisitos al controlador de red y a su vez los transformará en políticas y configuraciones compatibles. En general existen más de un controlador de red distribuido por diferentes sitios, seleccionando un controlador como el principal y los demás como respaldo, es decir cuando se genera una falla en el controlador principal los controladores de respaldo de manera automática se harán cargo de su función (Yang et al., 2019).

2.5.3. Ventajas de una solución SD-WAN

Las redes de área amplia definidas por software, ofrecen múltiples beneficios para las empresas u organizaciones que buscan nuevas alternativas para aplicarlas en la administración de la red, entre ellas tenemos:

- **Reducción de costos con independencia de transporte:** Por un lado, el costo de una solución SD-WAN en promedio es de 2 veces menor que una arquitectura tradicional, por otro lado, se ahorra en soporte, mantenimiento y personal necesario encargado de la infraestructura.
- **Simplificación y automatización de las operaciones basadas en la nube:** SD-WAN es una tecnología que nos permite simplificar la administración de red por medio de la aplicación de dispositivos de red programables, este sistema puede realizar ajustes de manera remota.
- **Seguridad integrada:** Provee de protección contra amenazas y flujo de tráfico a través de internet mediante políticas de reconocimiento de aplicaciones en tiempo real
- **Aumento de agilidad y mejora del rendimiento de las aplicaciones:** Garantiza un fácil y rápido acceso desde cualquier punto hacia otro.
- **Optimización de la experiencia de usuario:** Debido a su capa de software SD-WAN, garantiza a los usuarios mejor calidad de servicio y seguridad da datos en los enlaces de internet.
- **Nuevo enfoque para la conectividad de red:** Los administradores de red aprovechan el ancho de banda de forma mucho más eficiente asegurando el mayor nivel de rendimiento de las principales aplicaciones de manera segura. Una solución SD-WAN, muy aparte que automatiza y facilita la gestión de la red, permite a las empresas prepararse para abordar la transformación digital (Gartner, 2019).

2.5.4. SD-WAN vs Redes Tradicionales

Las redes tradicionales hoy en día, tienen un bajo ancho de banda, falta de visibilidad de las aplicaciones, alta lactancia imposibilitando aplicar calidad de servicio, políticas de seguridad, siendo muy baja la satisfacción del usuario, conduciendo a las empresas a emigrar a nuevas arquitecturas de manera inmediata. En la figura 2.2 se presenta las arquitecturas, tanto de la red tradicional como las redes SD-WAN (Cevallos, 2018).

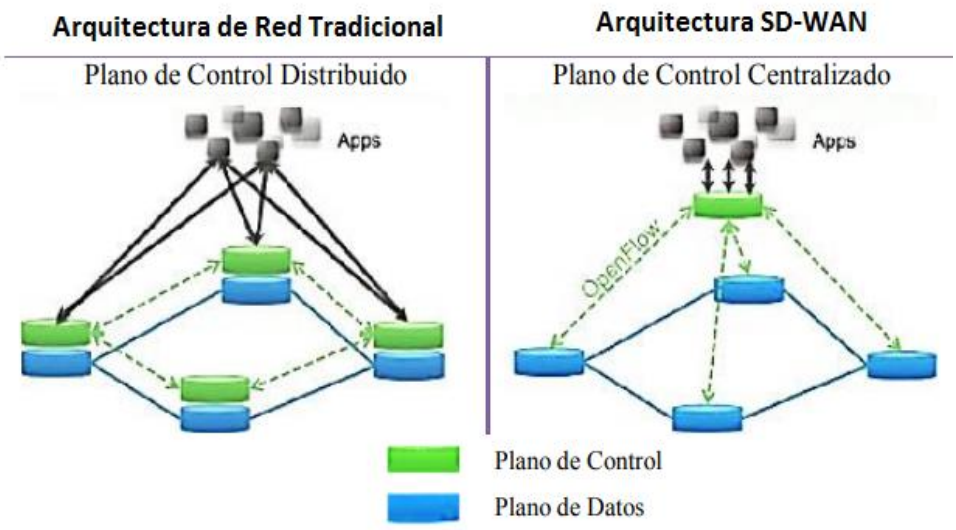


Figura 2. 25 Comparativa de la redes tradicionales y SD-WAN
Fuente: (Cevallos, 2018)

De esta manera, las redes de área amplia definidas por software, se presentan como una solución inteligente estandarizada con el objetivo de cumplir las necesidades de las empresas y usuarios facilitando la gestión de la red, dando paso a la transformación digital. La siguiente tabla 2.1 identifica las diferencias entre la red tradicionales y la SD-WAN (Cevallos, 2018)

Red Tradicional	SD-WAN
- Configuración manual - Alto costo en equipos y sistemas operativos - Incapaz de ser escalable - Infraestructura estática - Nuevas aplicaciones en mayor tiempo - Difícil de aplicar políticas - Menor seguridad - Baja experiencia de usuario - Lenta - Poco rendimiento	- Configuración centralizada - Reducción de costos operativos y financieros - Escalabilidad - Infraestructura Dinámica - Nuevas aplicaciones en menos tiempo - Añade seguridad a la red - Mejora la experiencia del usuario - Más ágil - Mayor rendimiento

Tabla 2. 2 Diferencia de la redes tradicionales y SD-WAN
Fuente: (Guanoluisa, 2019)

2.5.1. Marco Regulador

Elegir emigrar hacia las redes definidas por software resulta un gran esfuerzo por parte de los proveedores de servicio ya que el cambio de las redes distribuidas a redes centralizadas tiene como objetivo trasladar el control por hardware a un nodo centralizado de control por software.

2.5.2. Legislación y regulación

La IEEE (Institute of Electrical and Electronics Engineers), es la organización líder en el desarrollo de sistemas de estandarización relacionada directamente con la evolución de la SDN y en la aplicación de múltiples tecnologías que la asocian.

Existen proyectos en la IEEE que están directamente vinculados con las redes definidas por software, los cuales son:

- IEEE P1903.1 – Standard for Content Delivery Protocols of Next Generation Service Overlay Network (NGSON).
- IEEE P1913.1 – Software-Defined Quantum Communication.
- 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.

Un aspecto que hay que considerar sobre las redes de área amplia definidas por software es el cumplimiento de la regulación y legislación por partes de las compañías, que a su vez no sufren tanto al momento de cumplir con la regulación ya que suelen tomar caminos distintos con diferentes políticas que deben de ser aplicadas.

CAPÍTULO 3:

DISEÑO, IMPLEMENTACIÓN Y RESULTADOS

3.1. Diseño de la red SD-WAN aplicada al laboratorio de la facultad técnica de la UCSG

Para realizar el diseño de red, se procederá a crear una red WAN aplicando una solución SD-WAN entre el laboratorio de la facultad técnica de la UCSG, la red del Rectorado y la red de Computo empleando un simulador de red virtual. Para realizar las respectivas de prueba se utilizar el siguiente esquema de red.

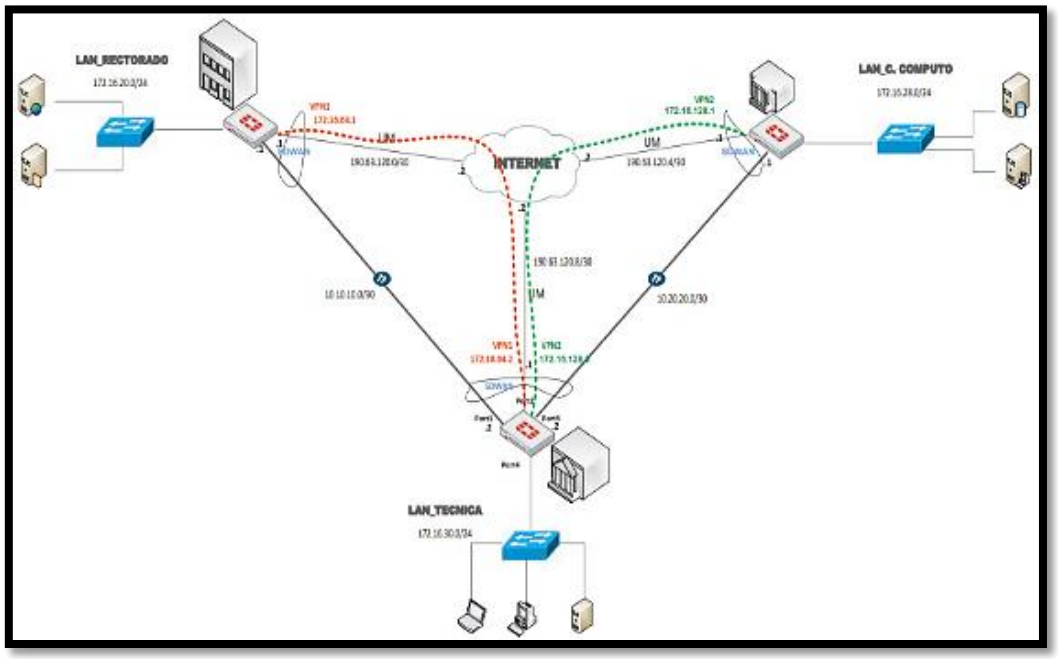


Figura 3. 1 Diseño de red aplicando una solución SD-WAN en el laboratorio de la facultad técnica de la UCSG. Elaborado por: Autor

.

En la figura 3.1 se muestra el esquema de la red que se utilizará para simular una solución SD-WAN entre las respectivas áreas que se aprecian en la figura para ellos se utilizaran, 3 switch y 3 equipos fortinet

3.2. Diseño y pruebas de la red en un simulador virtual

Se procede a elaborar el diseño de la red WAN que conforma las áreas en las que se va a simular un enlace SD-WAN de alta disponibilidad, capacidad y flexibilidad.

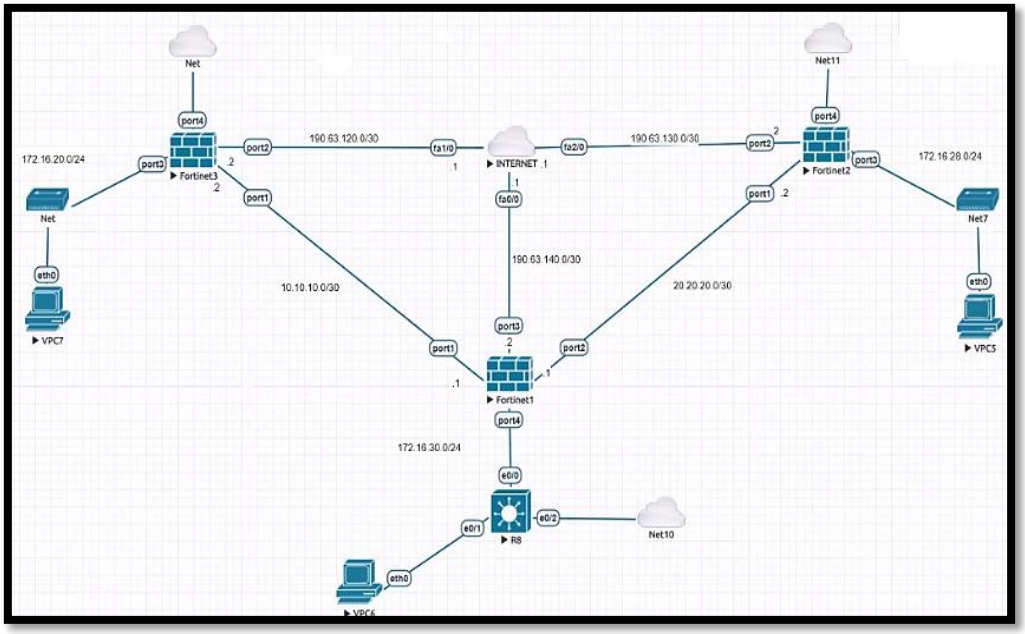


Figura 3. 2 Diseño de la red WAN en la que se realizarán las respectivas pruebas. Elaborado por: Autor

En la figura 3.1 se muestra como la red LAN del laboratorio de la facultad técnica está conectado mediante enlace físico a la LAN del rectorado con un IP de 10.10.10.0/30 en el puerto 1 y la LAN de Cómputo con una IP de 20.20.20.0/30. En la cual se observa que la PC de la facultad técnica utiliza una IP de 172.16.30.0 en el puerto 4 de su respectivo equipo, para salida a internet utiliza la IP 190.63.140.0/30 en el puerto 2 mientras que la PC del rectorado utiliza una IP de 172.16.20.0 en el puerto 4 de su respectivo equipo, para salida a internet utiliza la IP 190.63.120.0/30 en el puerto 2 y la PC de computo con una IP de 172.16.25.0 en el puerto 4 de su respectivo equipo, para salida a internet utiliza la IP 190.63.130.0/30 en el puerto 2.

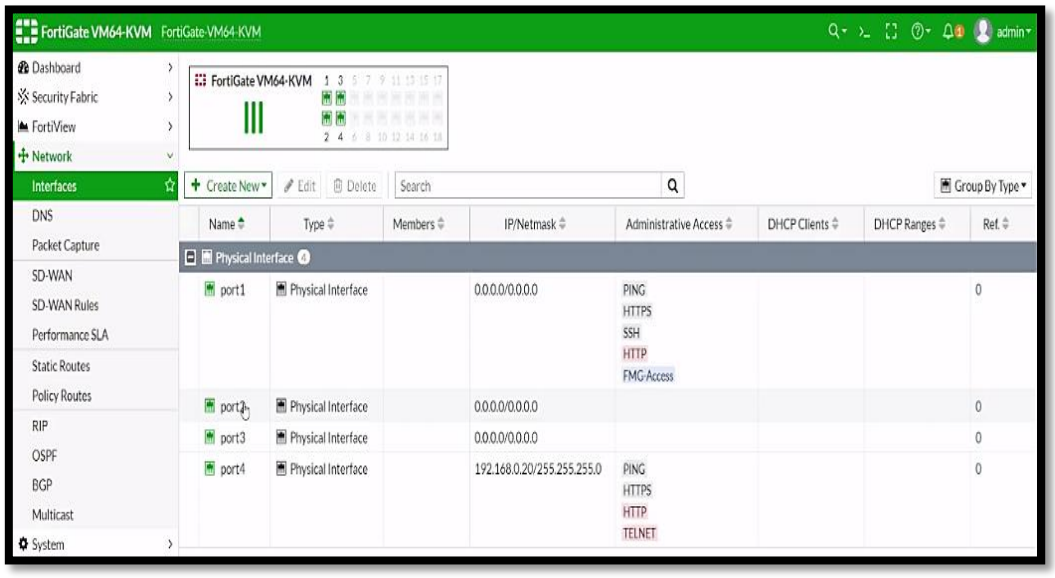


Figura 3.3 Interfaces de los puertos del equipo del laboratorio.
Elaborado por: Autor

En la figura 3.3 se observa los puertos de cada interfaz que posee el equipo Fortigate ubicado en el laboratorio de la facultad técnica de la UCSG, se procede asignar la dirección IP 192.168.0.20 y con la máscara de subred 255.255.255.0 al puerto 4.

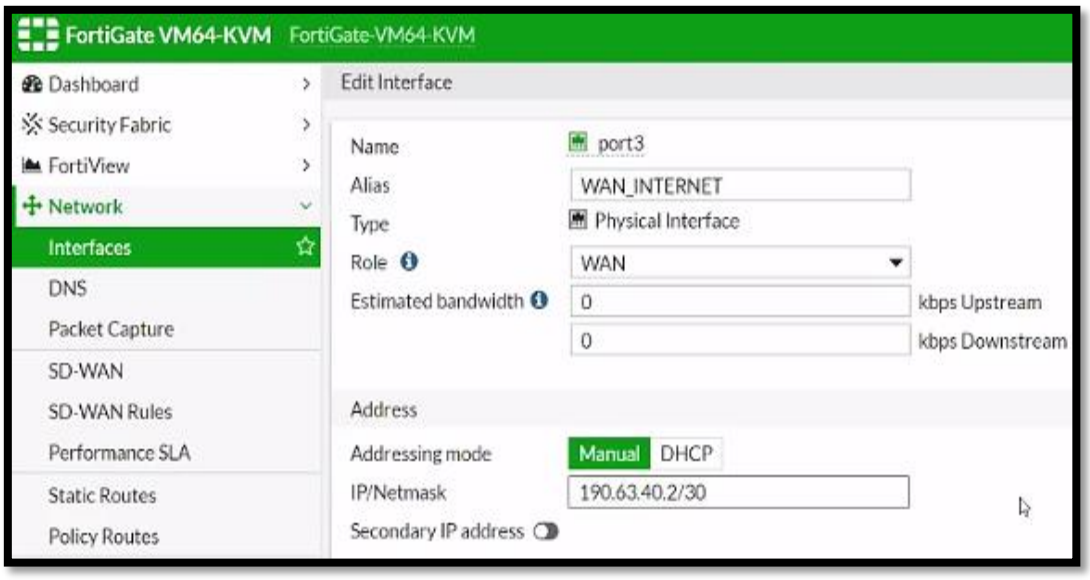


Figura 3.4 IP asignada en el puerto 3 del laboratorio.
Elaborado por: Autor

En la figura 3.4 se observa la ip 190.63.40.2 asignada en el puerto 3 que da salida a internet en el área del laboratorio.

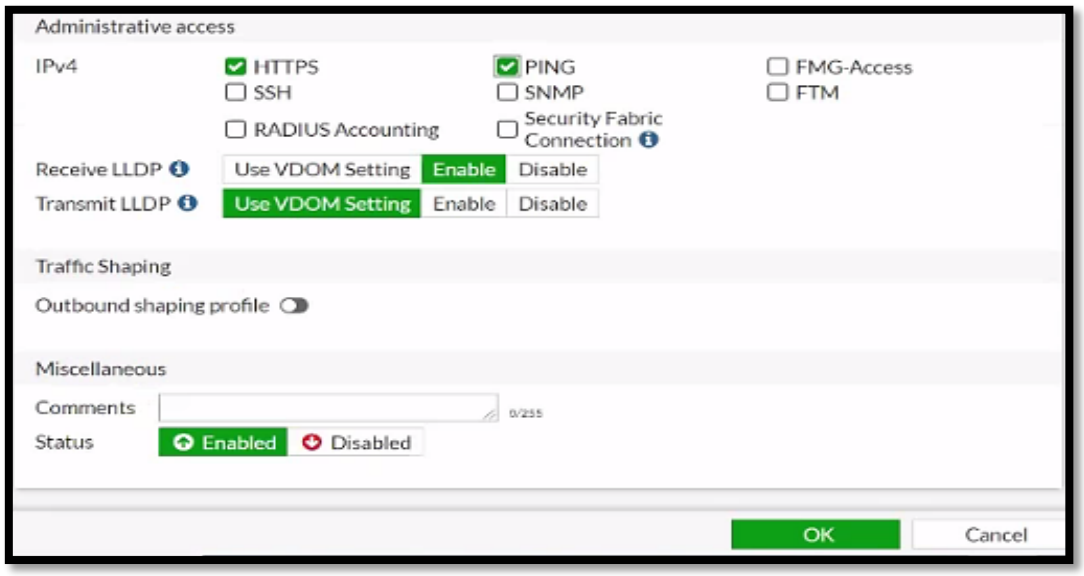


Figura 3.5 Protocolos habilitados del puerto 3
Elaborado por: Autor

En la figura 3.5 muestra los protocolos que se habilitan en el puerto 3, en este caso el https, el ping y el LLDP que se lo utiliza para la transmisión y retransmisión de paquetes.

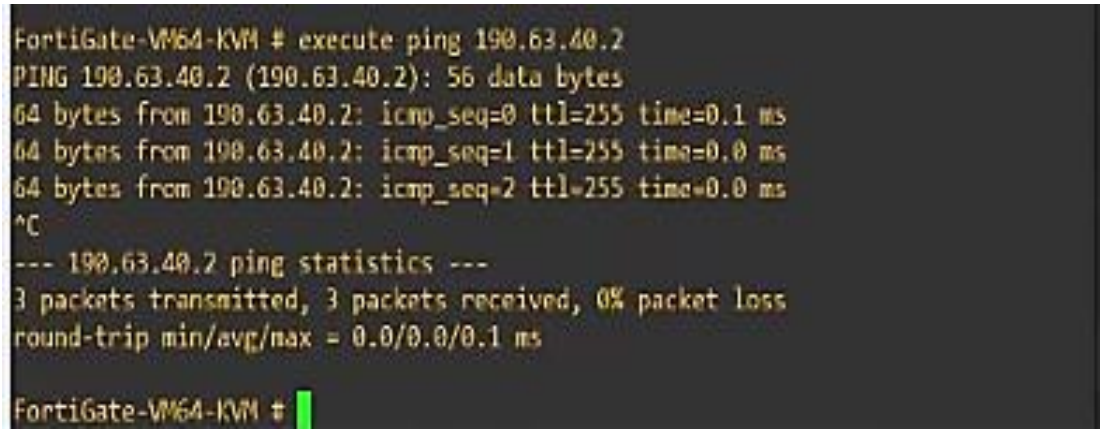


Figura 3.6 Prueba de conectividad del equipo
Elaborado por: Autor

En la figura 3.6 se realiza una prueba de conectividad ejecutando el comando PING a la IP 190.63.40.2 en el equipo del laboratorio.

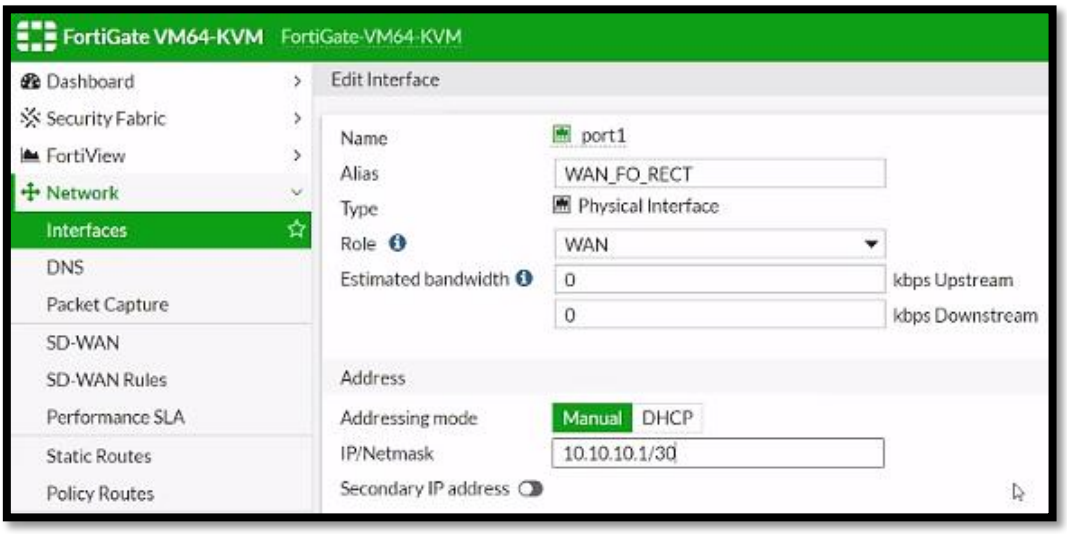


Figura 3.7 IP asignada en el puerto 1 del laboratorio.
Elaborado por: Autor

En la figura 3.7 se observa la IP 10.10.10.1 asignada en el puerto 1 que es la del enlace con el área del Rectorado.

Figura 3.8 Protocolos habilitados del puerto 1.
Elaborado por: Autor

En la figura 3.8 muestra los protocolos que se habilitan en el puerto 1, en este caso el https, http, FMS-Access, ping, ssh y el LLDP que se lo utiliza para la transmisión y retransmisión de paquetes

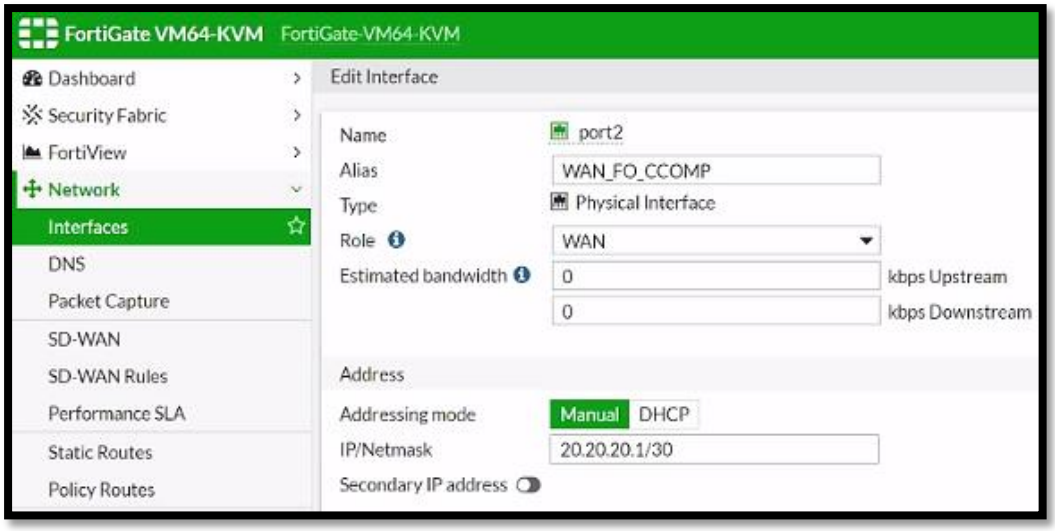


Figura 3.9 IP asignada en el puerto 2 del laboratorio.
Elaborado por: Autor

En la figura 3.9 se observa la IP 20.20.20.1 asignada en el puerto 2 que es la del enlace con el centro de cómputo.

Figura 3.10 Protocolos habilitados del puerto 2.
Elaborado por: Autor

En la figura 3.10 muestra los protocolos que se habilitan en el puerto 2, en este caso el https, http, FMS-Access, ping, ssh y el LLDP que se lo utiliza para la transmisión y retransmisión de paquetes

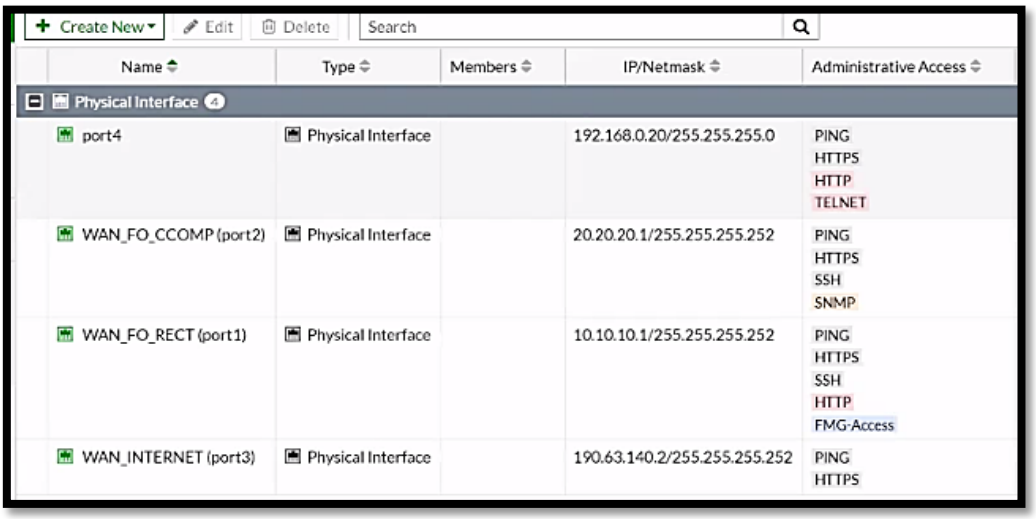


Figura 3.11 IP asignadas del equipo del laboratorio.
Elaborado por: Autor

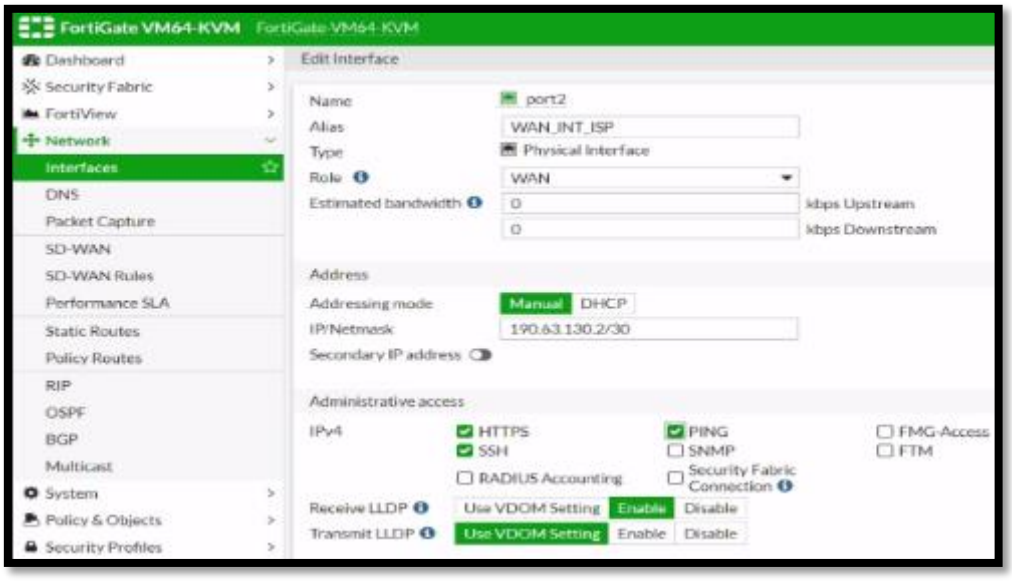


Figura 3.12 IP asignada en el puerto 2 del centro de cómputo.
Elaborado por: Autor

En la figura 3.11 se observa la IP 190.63.130.2 asignada en el puerto 3 que da salida a internet en el centro de cómputo, además se procede habilitar los protocolos https, ssh, ping, LLDP de trasmisión y retrasmisión.

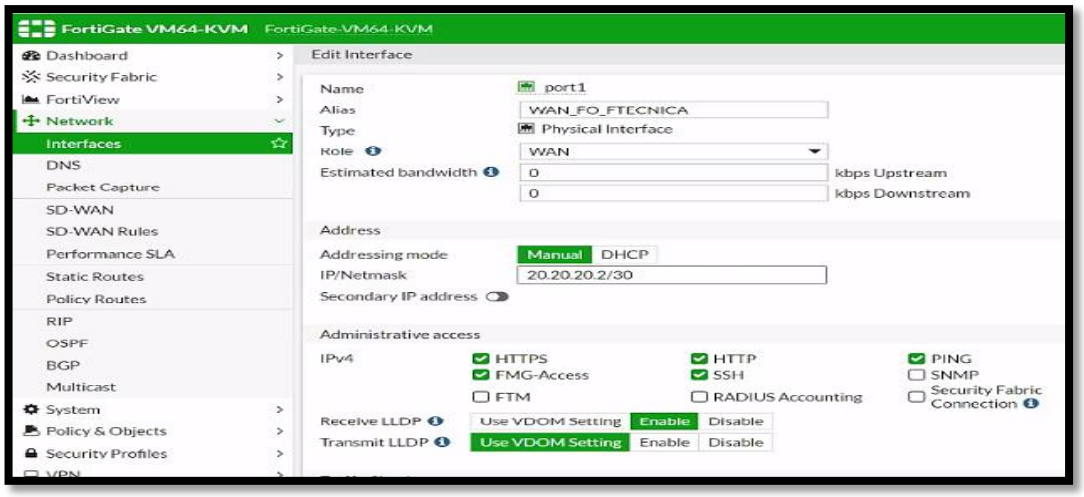


Figura 3.13 IP asignada en el puerto 1 del centro de cómputo.
Elaborado por: Auto

En la figura 3.12 se observa la IP 20.20.20.2 asignada en el puerto 1 que enlaza con el laboratorio de la facultad técnica, además se procede habilitar los protocolos https, ssh, ping, LLDP de trasmisión y retrasmisión.

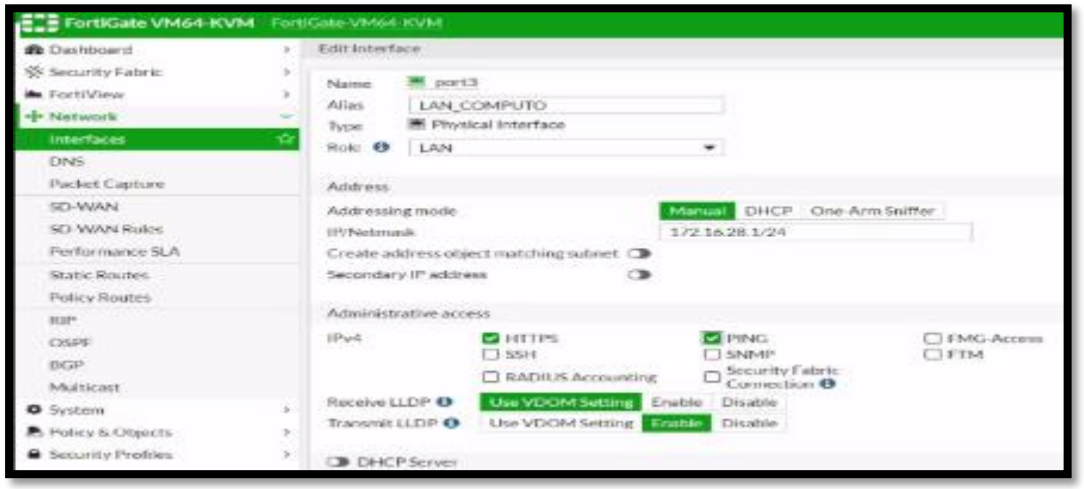


Figura 3.14 IP asignada en el puerto 1 del centro de cómputo.
Elaborado por: Autor

En la figura 3.13 se observa la IP 190.63.130.2 asignada en el puerto 3 que es la del enlace con el centro de cómputo, además se procede habilitar los protocolos https, ssh, ping, LLDP de trasmisión y retrasmisión.

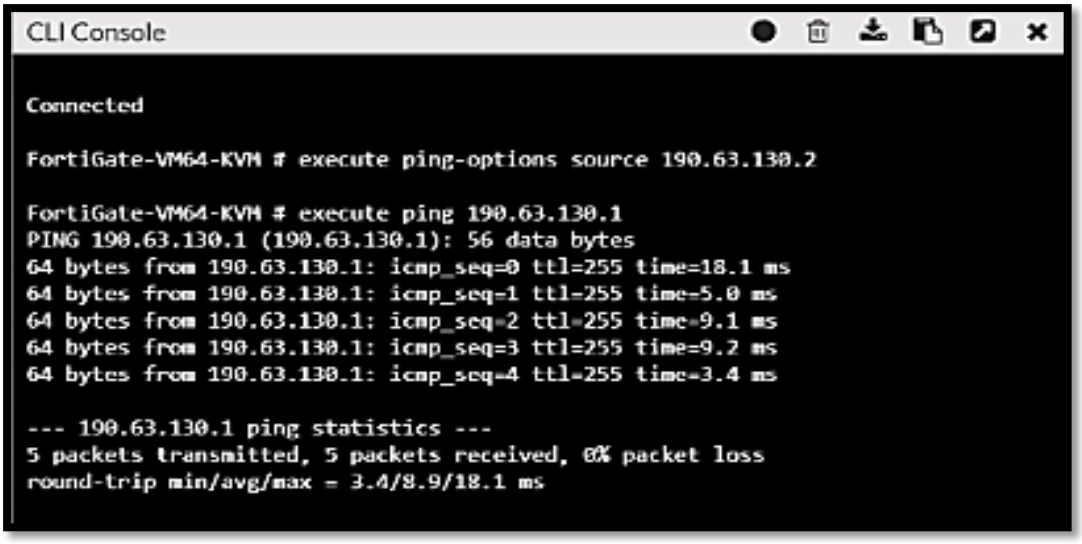


Figura 3.15 Prueba de conectividad de las IP asignadas.
Elaborado por: Autor

En la figura 3.14 se realiza una prueba de conectividad ejecutando el comando PING a la IP 190.63.130.1 en el equipo. Se comprueba que existe conexión con el enlace de internet.

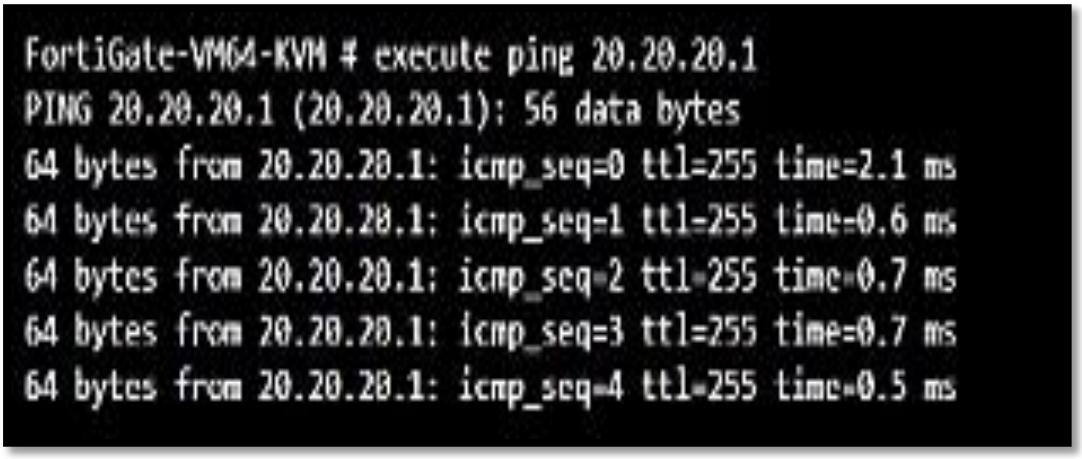


Figura 3.16 Prueba de conectividad de las IP asignadas.
Elaborado por: Autor

En la figura 3.15 se realiza una prueba de conectividad ejecutando el comando PING a la IP 190.63.130.1 en el equipo. Se comprueba que existe conexión con el enlace de internet

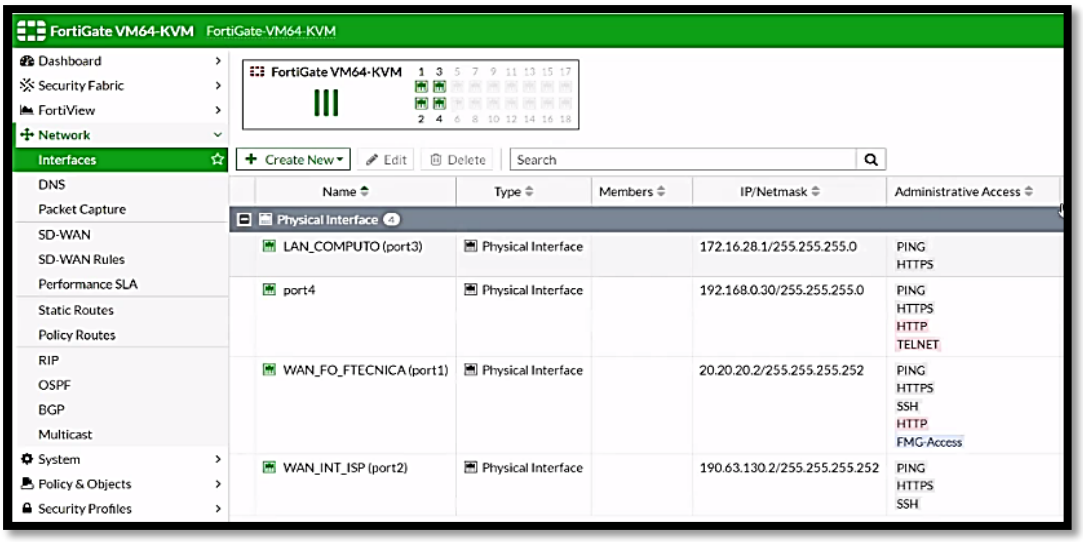


Figura 3.17 IP asignadas del equipo del centro de cómputo.
Elaborado por: Autor

En la figura 3.16 se observa las IP asignadas a cada uno de los puertos del equipo ubicado en el centro de cómputo, entre ellas tenemos la IP 172.16.28.1 que corresponde al puerto 3 de la LAN del centro de cómputo con los protocolos habilitados https y ping. La IP 192.168.0.30 que corresponde al puerto 4 con los protocolos habilitados https, http, ping, telnet. La IP 20.20.20.2 que corresponde al puerto 1 del enlace de la red WAN del laboratorio con los protocolos habilitados https, http, ping, shh y FMG Access. Por último, la IP 190.63.130.2 que corresponde al puerto 2 del enlace a internet con los protocolos habilitados ping, https y ssh.

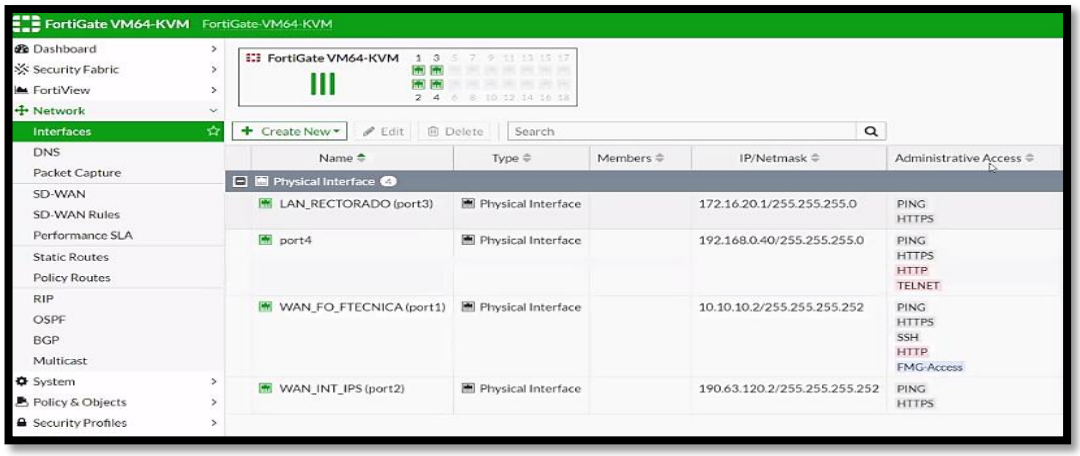


Figura 3.18 IP asignadas del equipo del rectorado.
Elaborado por: Autor

En la figura 3.17 se observa las IP asignadas a cada uno de los puertos del equipo ubicado en el área del rectorado, entre ellas tenemos la IP 172.16.20.1 que corresponde al puerto 3 de la LAN del rectorado con los protocolos habilitados https y ping. La IP 192.168.0.40 que corresponde al puerto 4 con los protocolos habilitados https, http, ping, telnet. La IP 10.10.10.2 que corresponde al puerto 1 del enlace de la red WAN del laboratorio con los protocolos habilitados https, http, ping, shh y FMG Access. Por último, la IP 190.63.120.2 que corresponde al puerto 2 del enlace a internet con los protocolos habilitados ping, https.

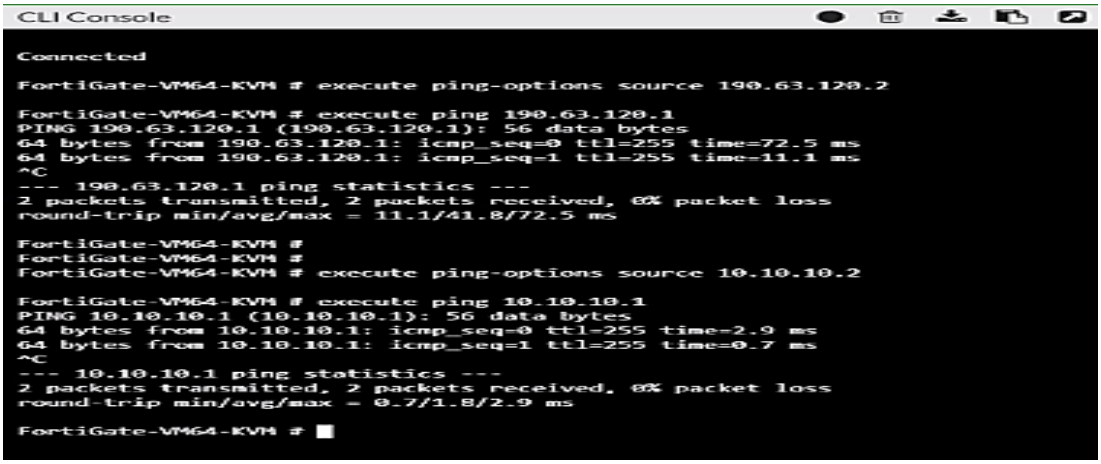


Figura 3.19 Prueba de conectividad de las IP asignadas.
Elaborado por: Autor

En la figura 3.18 se realiza una prueba de conectividad ejecutando el comando PING a la IP 190.63.120.1, PING a la IP 10.10.10.1 en el equipo. Se comprueba que existe conexión con el enlace de internet y con el enlace de la red del laboratorio de la facultad técnica.

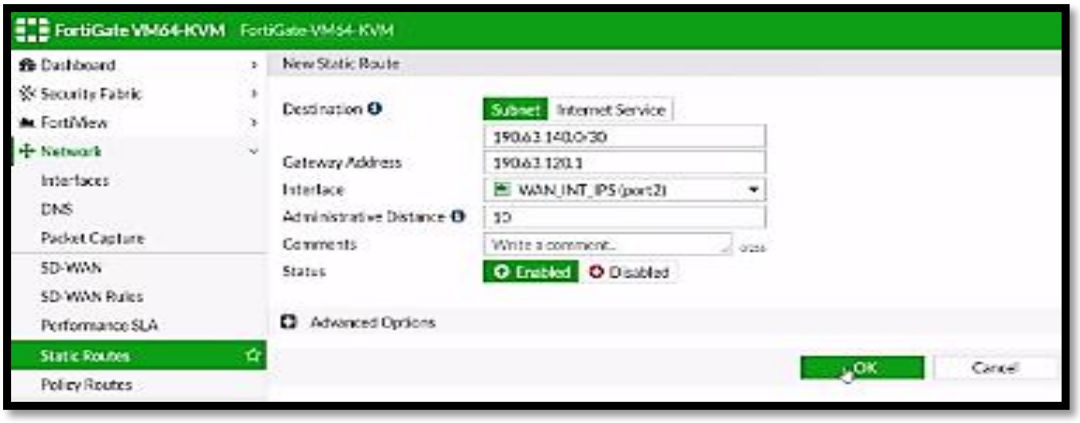


Figura 3.20 Creación de la ruta estática del equipo ubicado en el rectorado.
Elaborado por: Autor

En la figura 3.19 se procede a crear una ruta estática, vamos a la opción de network elegimos la opción static routes y creamos la nueva ruta en este caso con la IP 192.162.140.0 y su Gateway 190.63.120.1 de la interfaz WAN de internet perteneciente al puerto 2 del equipo ubicado en el rectorado. Se asigna al rango 10 en la distancia administrativa y habilitamos el estatus de la ruta.

Figura 3.21 Creación de la ruta estática del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.20 se procede a crear una ruta estática, vamos a la opción de network elegimos la opción static routes y creamos la nueva ruta en este caso con la IP 192.162.120.0 y su Gateway 190.63.140.1 de la interfaz WAN de internet perteneciente al puerto 3 del equipo ubicado en el laboratorio de la facultad técnica. Se asigna al rango 10 en la distancia administrativa y habilitamos el estatus de la ruta.

Figura 3.22 Creación de la ruta estática del equipo ubicado en el centro de cómputo.
Elaborado por: Autor

En la figura 3.21 se procede a crear una ruta estática, vamos a la opción de network elegimos la opción static routes y creamos la nueva ruta en este caso con la IP 192.162.130.0 y su Gateway 190.63.140.1 de la interfaz WAN de internet perteneciente al puerto 3 del equipo ubicado en el laboratorio de la facultad técnica. Se asigna al rango 10 en la distancia administrativa y habilitamos el estatus de la ruta.

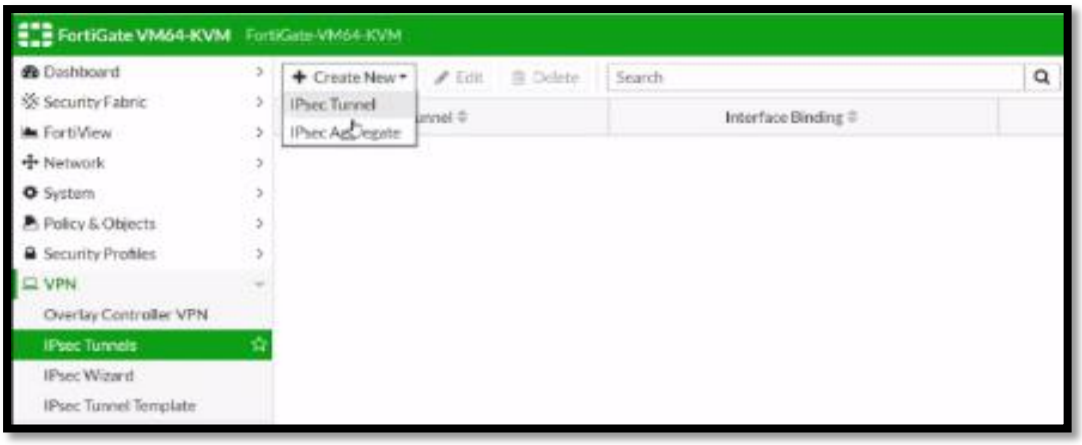


Figura 3.23 Creación del túnel IPsec del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.22 se observa el procedimiento para crear un túnel IPsec, primero nos dirigimos a la opción de VPN y elegimos la opción IPsec Tunnels, seleccionamos en créate news posteriormente IPsec tunnel.

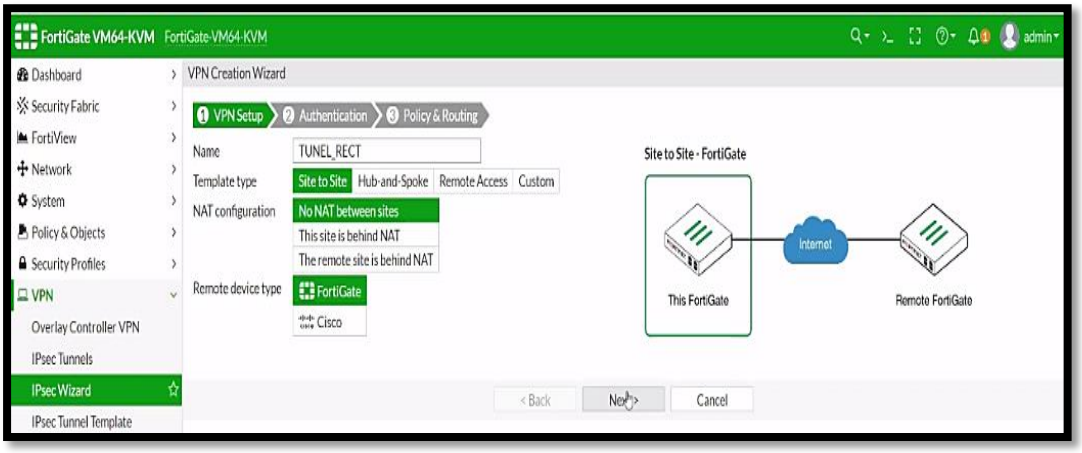


Figura 3.24 Paso 1 para crear un túnel IPsec hacia el rectorado del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.23 se observa cómo crear un túnel IPsec hacia el rectorado, seleccionando la opción Site to Site, luego la opción No Nat between sites, elegimos el tipo de dispositivo remoto en este caso el Fortigate procedemos a elegir Next.

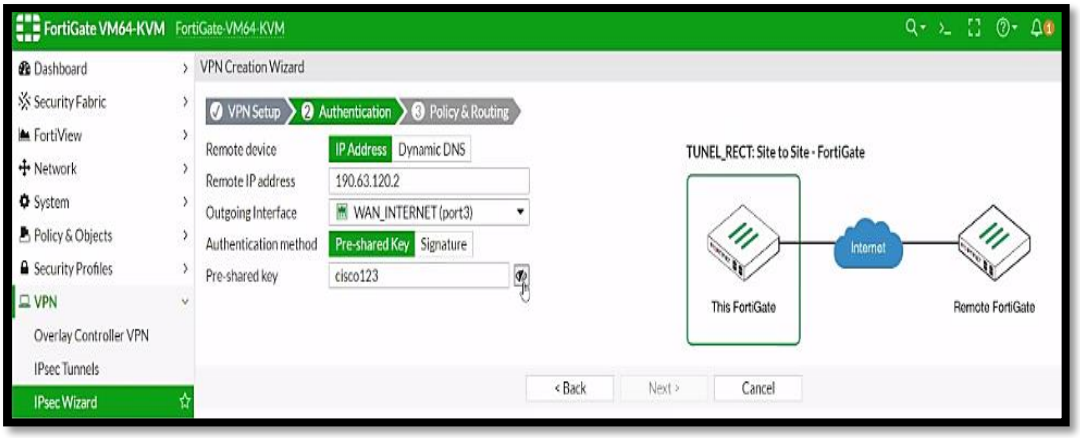


Figura 3.25 Paso 2 para crear un túnel IPsec hacia el rectorado del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.24 en Authentication se asigna la remote IP address, en este caso la 190.63.120.2, en outgoin interface se escoge la WAN_INTERNET correspondiente al puerto 3. Se asigna una contraseña en este casi cisco123 y seleccionamos next.

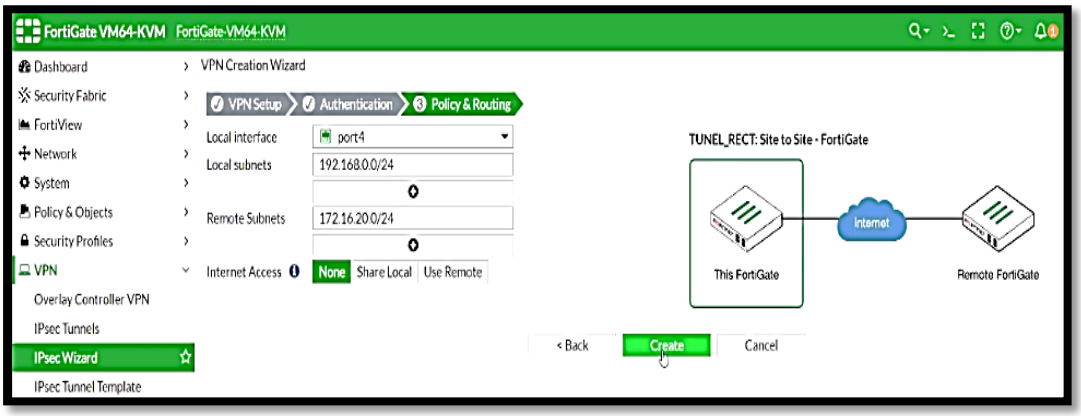


Figura 3.26 Paso 3 para crear túnel IPsec hacia el rectorado del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.25 se observa el último paso para crear un túnel IPsec en Policy Routing seleccionamos el puerto 4 en la sección de local interface, se asigna la ip 192.168.0.0 en local subnets y la IP 172.16.20.0 en remote subnets y se procede a seleccionar la opción create.

Figura 3.27 Confirmación que el túnel ha sido creado y activado.
Elaborado por: Autor

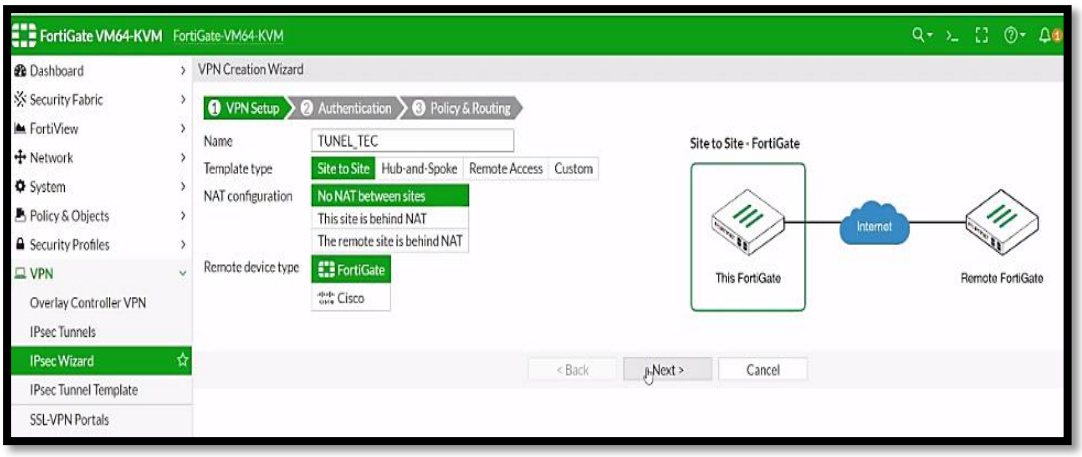


Figura 3.28 Paso 1 para crear un túnel IPsec hacia el laboratorio del equipo ubicado en el rectorado.
Elaborado por: Autor

En la figura 3.27 se observa cómo crear un túnel IPsec hacia el laboratorio de la facultad técnica, seleccionando la opción Site to Site, luego la opción No Nat between sites, elegimos el tipo de dispositivo remoto en este caso el Fortigate procedemos a elegir Next.

En la figura 3.28 en Authentication se asigna la remote IP address, en este caso la 190.63.140.2, en outgoin interface se escoge la WAN_INTERNET correspondiente al puerto 2. Se asigna una contraseña en este casi cisco123 y seleccionamos next.

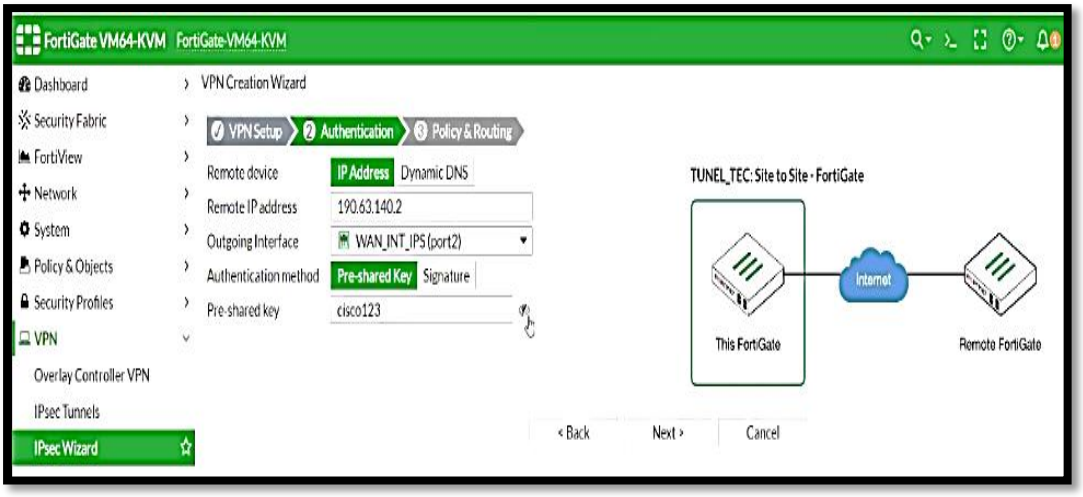


Figura 3.29 Paso 2 para crear un túnel IPsec hacia el laboratorio del equipo ubicado en el rectorado.
Elaborado por: Autor

En la figura 3.29 en Authentication se asigna la remote IP address, en este caso la 190.63.140.2, en outgoin interface se escoge la WAN_INTERNET correspondiente al puerto 2. Se asigna una contraseña en este casi cisco123 y seleccionamos next.

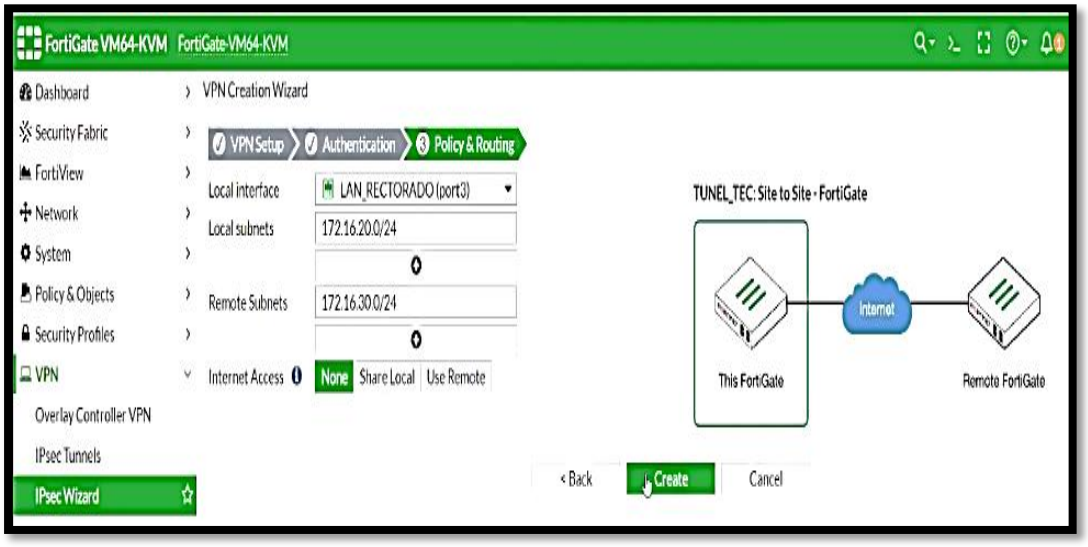


Figura 3.30 Paso 3 para crear túnel IPsec hacia el laboratorio del equipo ubicado en el rectorado.
Elaborado por: Autor

En la figura 3.30 se observa el último paso para crear un túnel IPsec en Policy Routing seleccionamos local interface escogemos LAN_RECTORADO correspondiente al puerto 3 en la sección de local interface, se asigna la ip 172.16.20.0 en local subnets y la IP 172.16.30.0 en remote subnets y se procede a seleccionar la opción create.

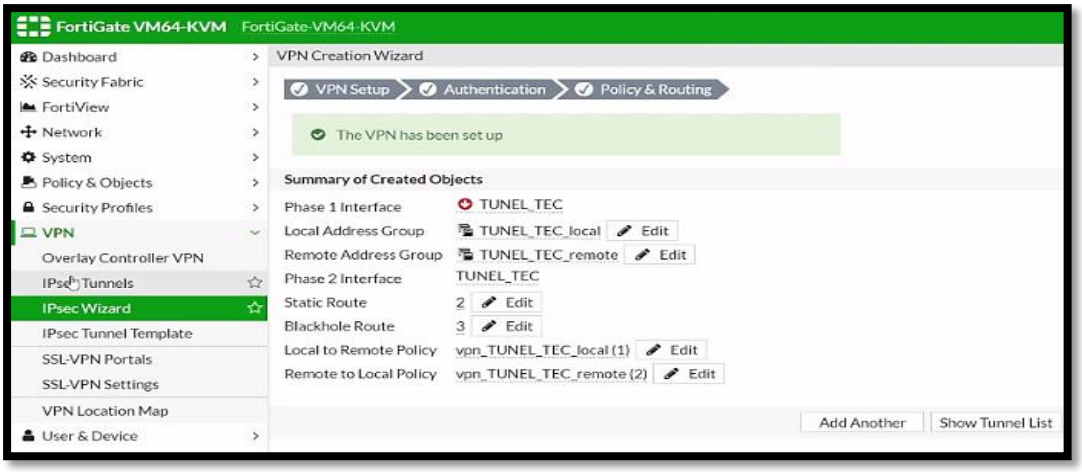


Figura 3.31 Confirmación que el túnel ha sido creado y activado.
Elaborado por: Autor

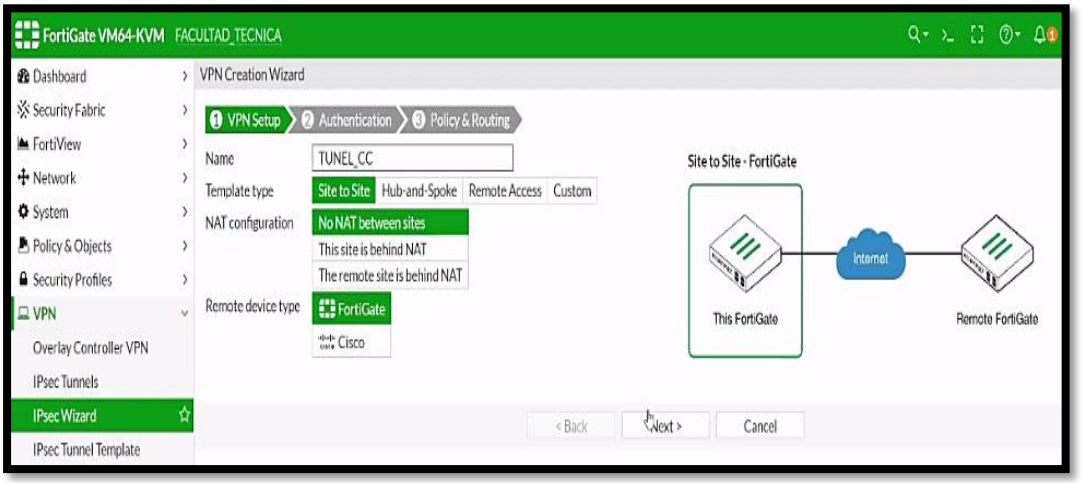


Figura 3.32 Paso 1 para crear un túnel IPsec hacia el centro de cómputo del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.32 se observa cómo crear un túnel IPsec hacia el centro de cómputo, seleccionando la opción Site to Site, luego la opción No Nat between sites, elegimos el tipo de dispositivo remoto en este caso el Fortigate procedemos a elegir Next

Figura 3.33 Paso 2 para crear un túnel IPsec hacia el centro de cómputo del equipo ubicado en el laboratorio.
Elaborado por: Autor

En la figura 3.33 en Authentication se asigna la remote IP address, en este caso la 190.63.130.2, en outgoin interface se escoge la WAN_INTERNET correspondiente al puerto 3. Se asigna una contraseña en este casi cisco123 y seleccionamos next.

Figura 3.34 Paso 3 para crear túnel IPsec hacia el centro de cómputo del equipo ubicado en el laboratorio.
Elaborado por: Autor

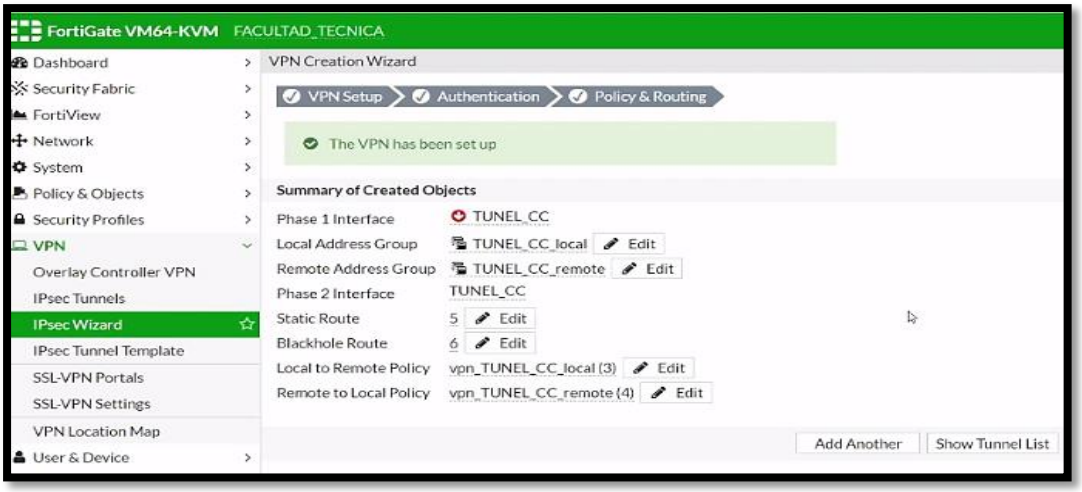


Figura 3.35 Confirmación que el túnel ha sido creado y activado.
Elaborado por: Autor

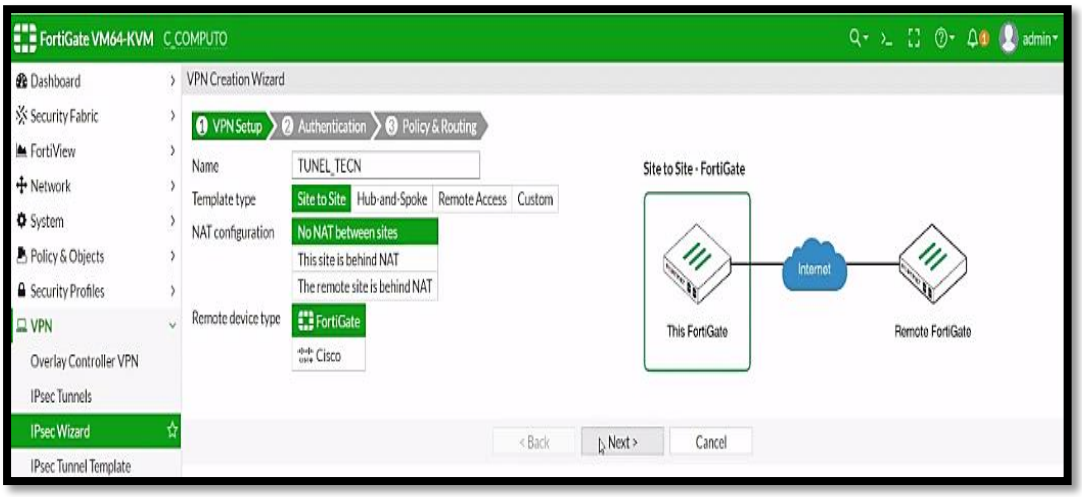


Figura 3.36 Paso 1 para crear un túnel IPsec hacia el laboratorio del equipo ubicado en el centro de cómputo.
Elaborado por: Autor

En la figura 3.36 se observa cómo crear un túnel IPsec hacia el laboratorio de la facultad técnica, seleccionando la opción Site to Site, luego la opción No Nat between sites, elegimos el tipo de dispositivo remoto en este caso el Fortigate procedemos a elegir Next

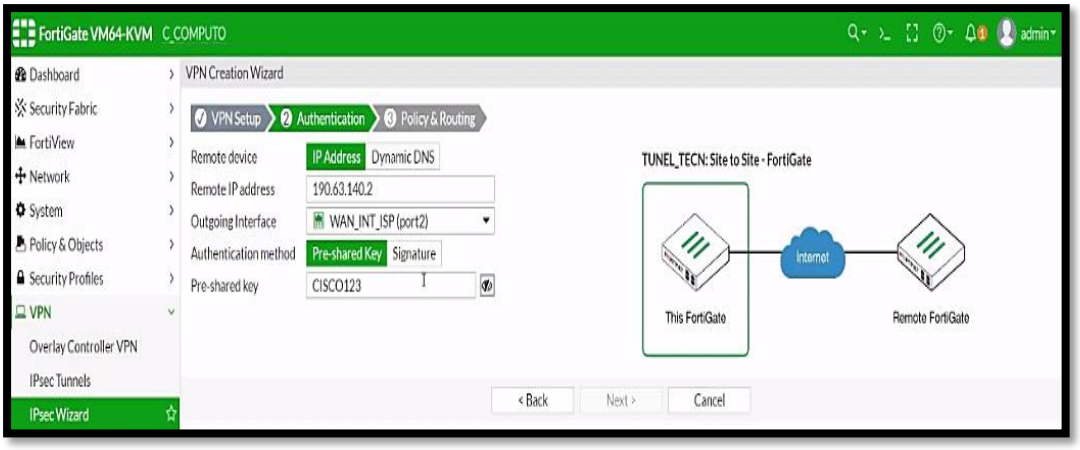


Figura 3.37 Paso 2 para crear un túnel IPsec hacia el laboratorio del equipo ubicado en el centro de cómputo.
Elaborado por: Autor

En la figura 3.37 en Authentication se asigna la remote IP address, en este caso la 190.63.140.2, en outgoin interface se escoge la WAN_INTERNET correspondiente al puerto 3. Se asigna una contraseña en este casi cisco123 y seleccionamos next

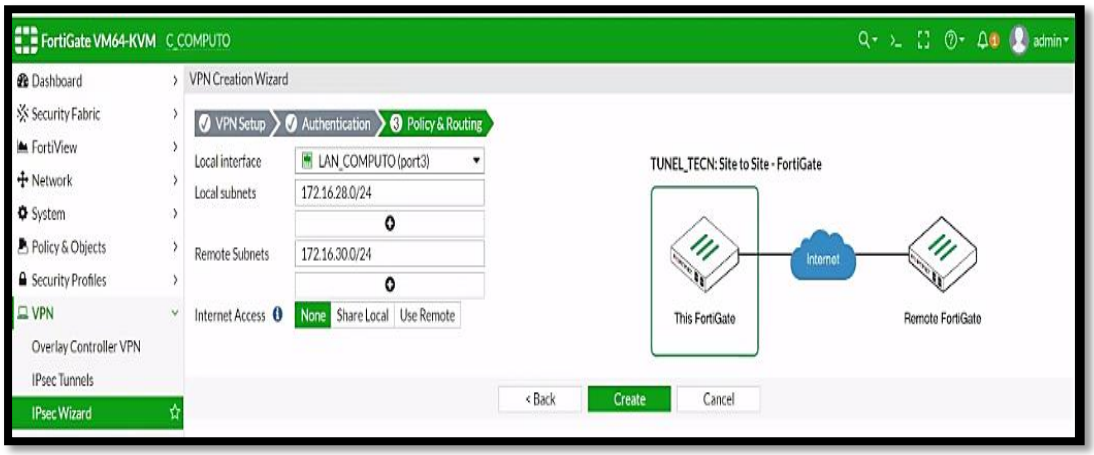


Figura 3.38 Paso 3 para crear túnel IPsec hacia el laboratorio del equipo ubicado en el centro de cómputo.
Elaborado por: Autor

En la figura 3.38 se observa el último paso para crear un túnel IPsec en Policy Routing seleccionamos local interface escogemos LAN_COMPUTO correspondiente al puerto 3 en la sección de local interface.

Se asigna la ip 172.16.28.0 en local subnets y la IP 172.16.30.0 en remote subnets y se procede a seleccionar la opción create.

Figura 3.39 Confirmación que el túnel ha sido creado y activado.
Elaborado por: Autor

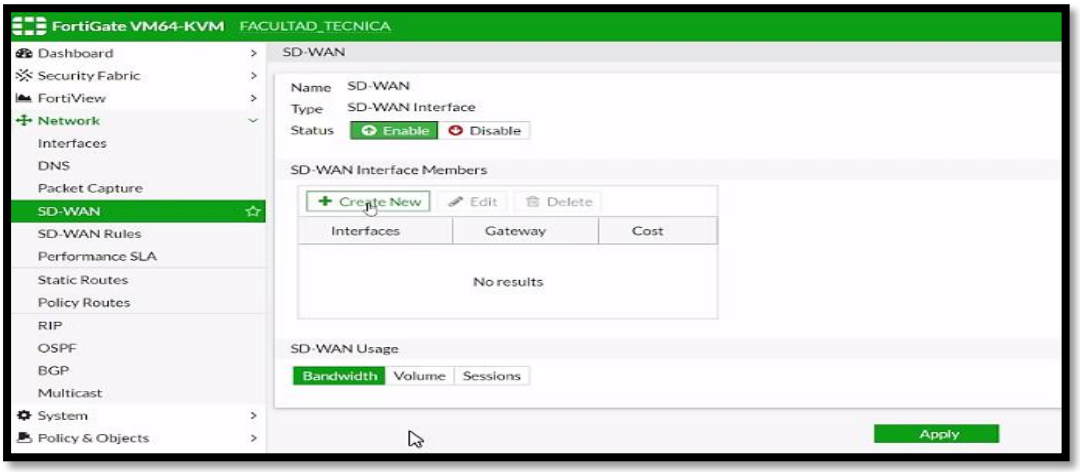


Figura 3.40 Como crear una interfaz SD-WAN.
Elaborado por: Autor

En la figura 3.40 se procede a crear una interfaz SD-WAN en el equipo ubicado en el laboratorio de la facultad técnica, seleccionamos Network, elegimos la opción SD-WAN habilitamos el status o estado, luego seleccionamos Create New.

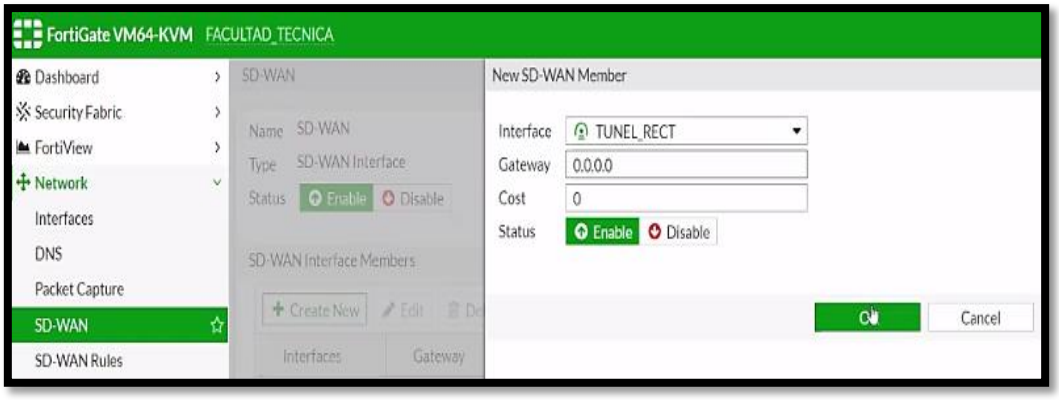


Figura 3.41 La interface TUNEL_RECT como miembro del enlace SD-WAN.
Elaborado por: Autor

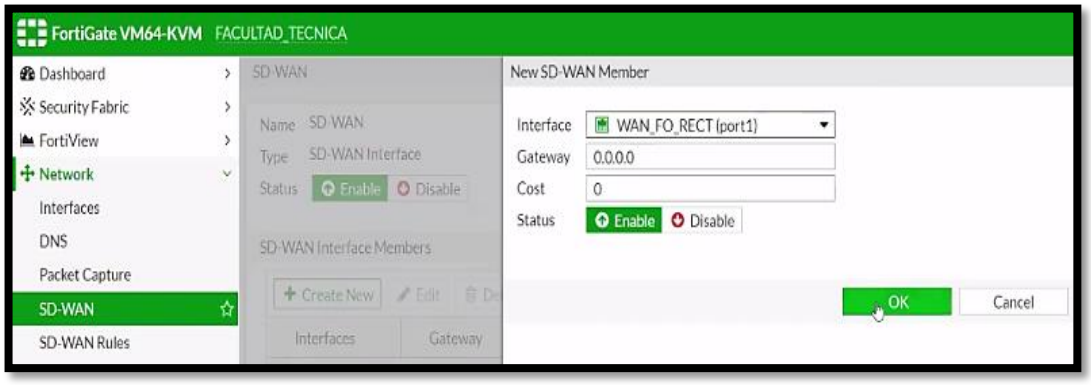


Figura 3.42 La interface WAN_FO_RECT como miembro del enlace SD-WAN.
Elaborado por: Autor

Figura 3.43 La interface TUNEL_CC como miembro del enlace SD-WAN.
Elaborado por: Autor

Figura 3.44 La interface WAN_FO_CCOMP como miembro del enlace SD-WAN.
Elaborado por: Autor

Figura 3.45 Interfaces creadas como miembro del enlace SD-WAN del equipo del laboratorio.
Elaborado por: Autor

En la figura 3.45 se observa todas las interfaces creadas en el equipo ubicado en el laboratorio de la facultad técnica y configuradas como miembros de un enlace SD-WAN, como son el puerto TUNEL_RECT correspondiente al puerto 3, el TUNEL_CC correspondiente al puerto 4, la WAN FO_REC, WAN_FO_CCOMP correspondiente al puerto 2. Todos tienen asignados como Gateway la dirección 0.0.0.0 que representa salida al mundo por cualquier dirección IP.

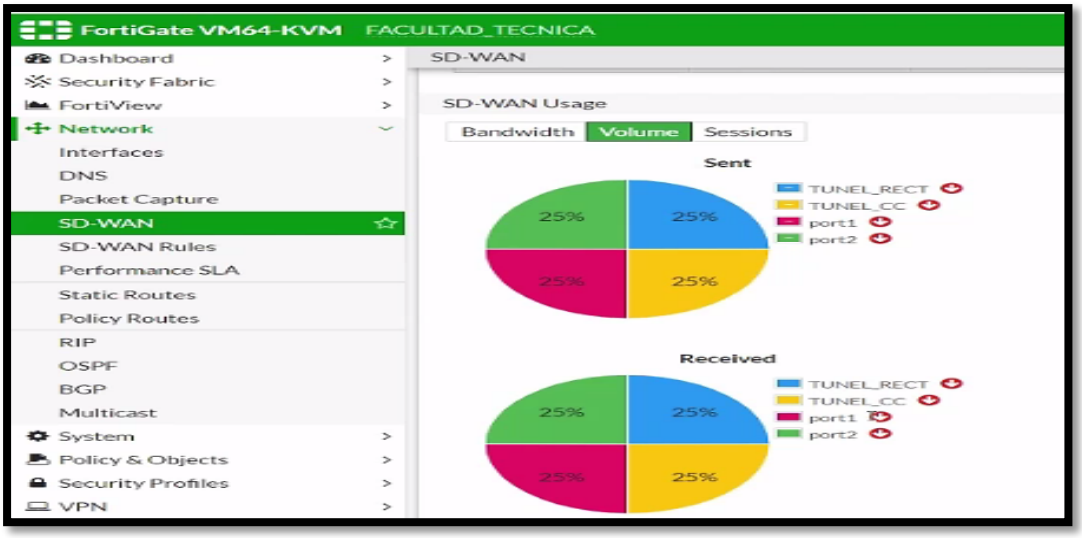


Figura 3.46 Porcentajes de los puertos creados como miembro del enlace SD-WAN del equipo del laboratorio.
Elaborado por: Autor

En la figura 3.46 se observa las gráficas de cada uno de los 4 puertos configurado como miembro de una interfaz SD-WAN, en este caso nos vamos a enfocar en los porcentajes de volumen de los paquetes de información que son enviados y recibidos en cada puerto configurado.

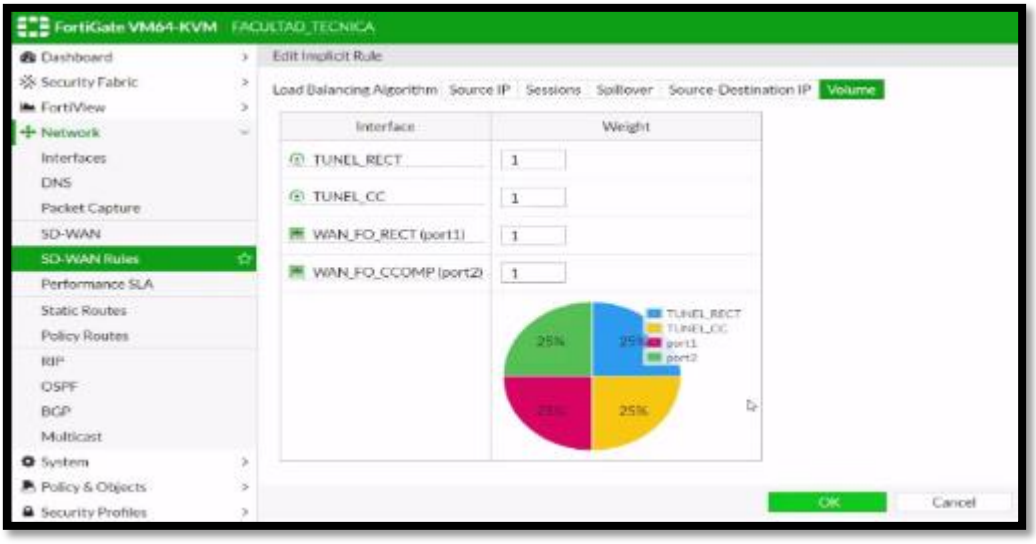


Figura 3.47 Gráfica del volumen SD-WAN dividido en los 4 puertos creados como miembro del enlace SD-WAN del equipo del laboratorio.
Elaborado por: Autor

En la figura 3.47 se procede a crear una regla de SD-WAN, seleccionando Network, luego SD-WAN Rules, asignamos el porcentaje de por cada puerto en este caso 1 lo que significa que cada puerto recibirá y enviará información de manera equivalente, brindando alta disponibilidad a la red.

Figura 3.48 Interfaces creadas como miembro del enlace SD-WAN del equipo del laboratorio.
Elaborado por: Autor

En la figura 3.48 se observa todas las interfaces creadas en el equipo ubicado en el rectorado y configuradas como miembros de un enlace SD-WAN, como son el puerto TUNEL_TEC correspondiente al puerto 2, la WAN FO_FTECNICA correspondiente al puerto 1. Ambos tienen asignados como Gateway la dirección 0.0.0.0 que representa salida al mundo por cualquier dirección IP.

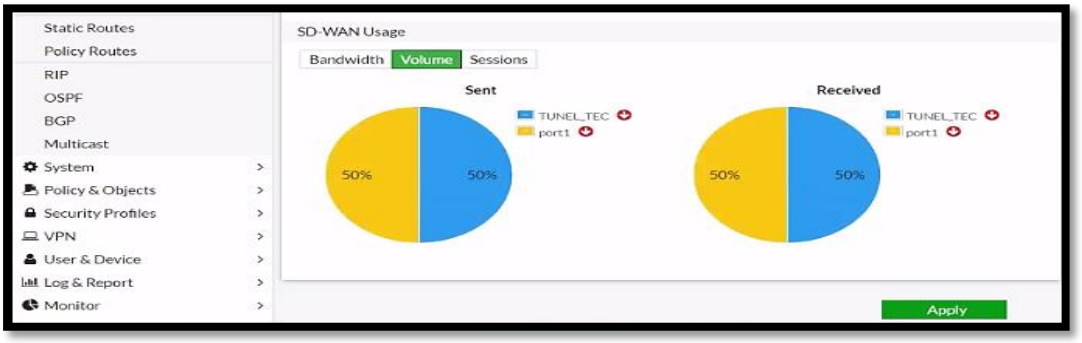


Figura 3.49 Porcentajes de los puertos creados como miembro del enlace SD-WAN del equipo del rectorado.
Elaborado por: Autor

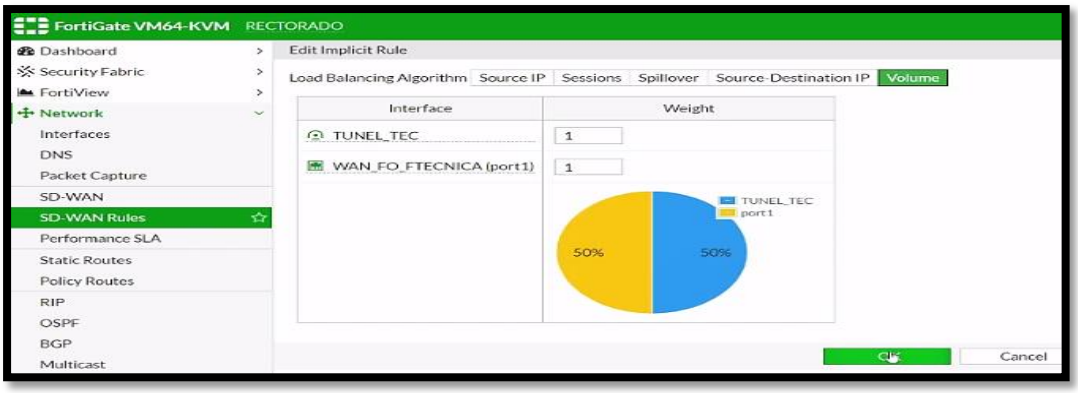


Figura 3.50 Gráfica del volumen SD-WAN dividido en los 2 puertos creados como miembro del enlace SD-WAN del equipo del rectorado.
Elaborado por: Autor

En la figura 3.50 se procede a crear una regla de SD-WAN, seleccionando Network, luego SD-WAN Rules, asignamos el porcentaje del puerto del TUNEL_TEC y del puerto WAN_FO_FTECNICA en este con un volumen del 1% lo que significa que cada puerto recibirá y enviará información de manera equivalente, brindando alta disponibilidad a la red.

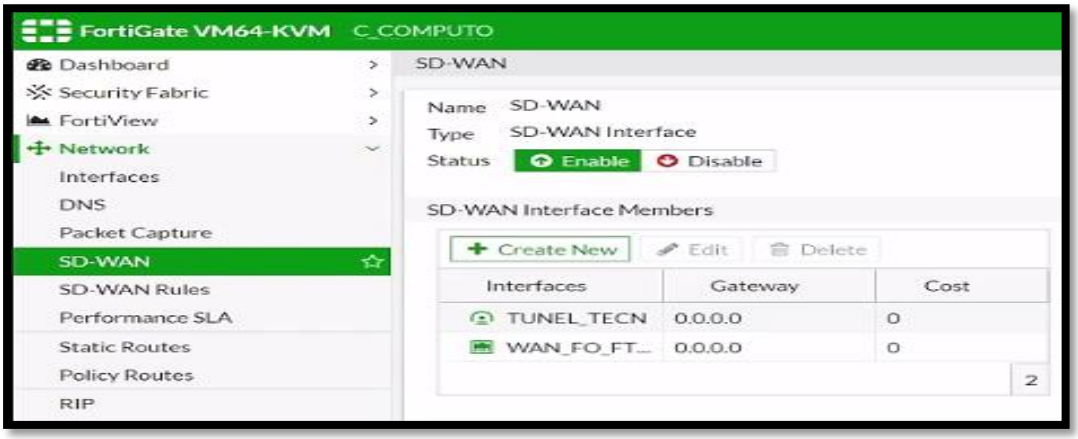


Figura 3.51 Interfaces creadas como miembro del enlace SD-WAN del equipo del centro de cómputo.
Elaborado por: Autor

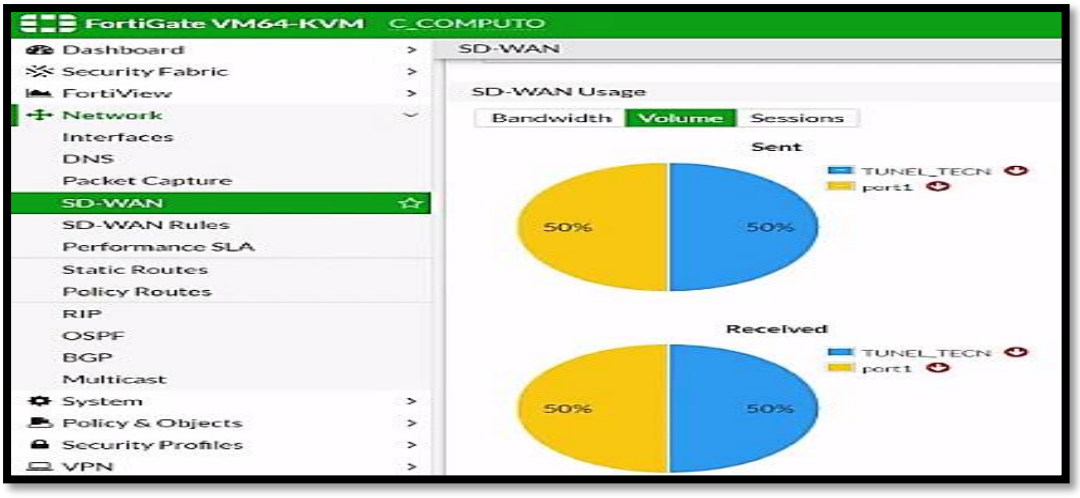


Figura 3.52 Porcentajes de los puertos creados como miembro del enlace SD-WAN del equipo del centro de cómputo.
Elaborado por: Autor

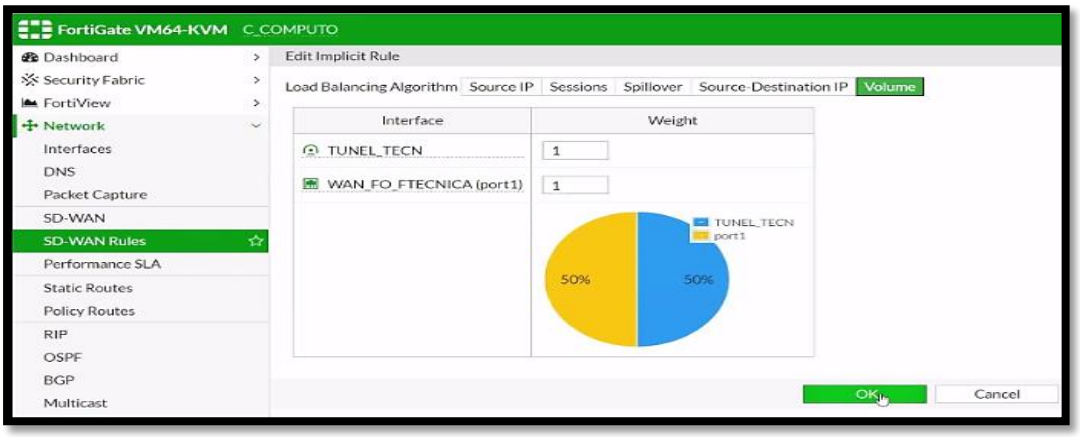


Figura 3.53 Gráfica del volumen SD-WAN dividido en los 2 de los puertos creados como miembro del enlace SD-WAN del centro de cómputo.
Elaborado por: Autor

En la figura 3.53 se procede a crear una regla de SD-WAN, seleccionando Network, luego SD-WAN Rules, asignamos el porcentaje del puerto del TUNEL_TECN y del puerto WAN_FO_FTECNICA en este con un volumen del 1% lo que significa que cada puerto recibirá y enviará información de manera equivalente, brindando alta disponibilidad a la red.

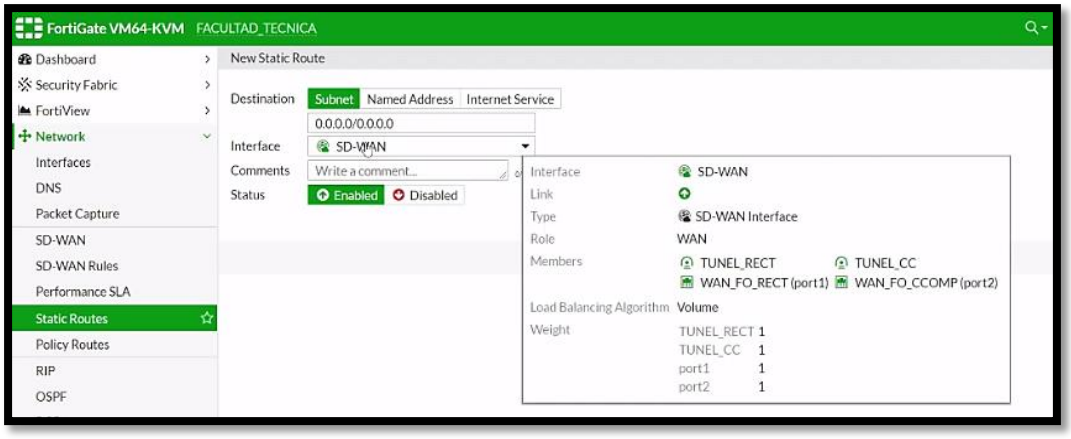


Figura 3.54 Creación de una ruta estática con SD-WAN en el equipo del laboratorio.
Elaborado por: Autor

En la figura 3.54 se procede a crear una ruta estática, asignamos la IP 0.0.0.0 en la sección de destination para poder tener salida al mundo desde cualquier IP, luego seleccionamos SD-WAN en la sección de interface ya que esta misma alberga a los puertos configurados del equipo del laboratorio de la facultad técnica.

Figura 3.55 Creación de una ruta estática con SD-WAN en el equipo del rectorado.
Elaborado por: Autor

En la figura 3.55 se procede a crear una ruta estática en el equipo ubicado en el rectorado, asignamos la IP 0.0.0.0 en la sección de destination para poder tener salida al mundo desde cualquier IP, luego seleccionamos SD-WAN en la sección de interface ya que esta misma alberga a los puertos configurados del equipo.

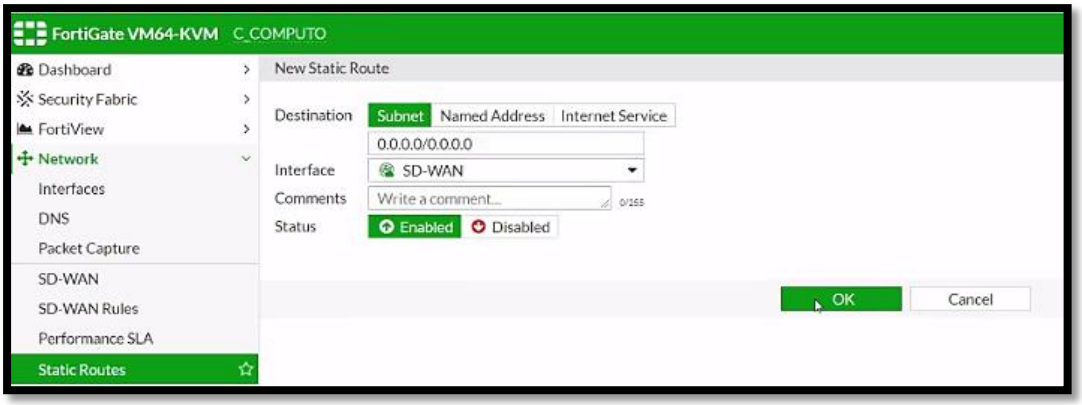


Figura 3.56 Creación de una ruta estática con SD-WAN en el equipo del centro de cómputo.
Elaborado por: Autor

En la figura 3.56 se procede a crear una ruta estática en el equipo ubicado en el centro de cómputo, asignamos la IP 0.0.0.0 en la sección de destination para poder tener salida al mundo desde cualquier IP, luego seleccionamos SD-WAN en la sección de interface ya que esta misma alberga a los 2 puertos configurados del equipo.

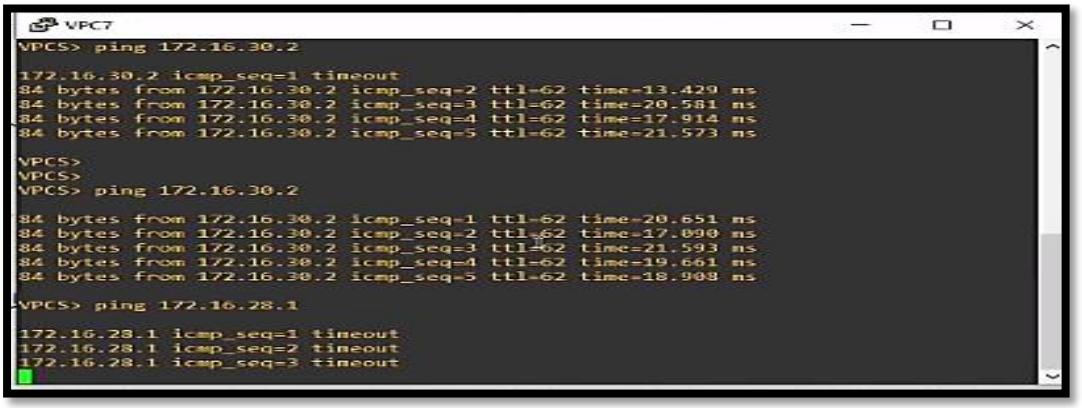


Figura 3.57 Prueba de conectividad de las interfaces SD-WAN con las IP asignadas.
Elaborado por: Autor

En la figura 3.57 se realiza una prueba de conectividad ejecutando el comando PING a la IP 172.16.20.2, PING a la IP 172.16.28.2 en el equipo. Se comprueba que existe conexión con la red ubicada en el rectorado mediante la interfaz SD-WAN así mismo con el enlace de la red del laboratorio de la facultad técnica.

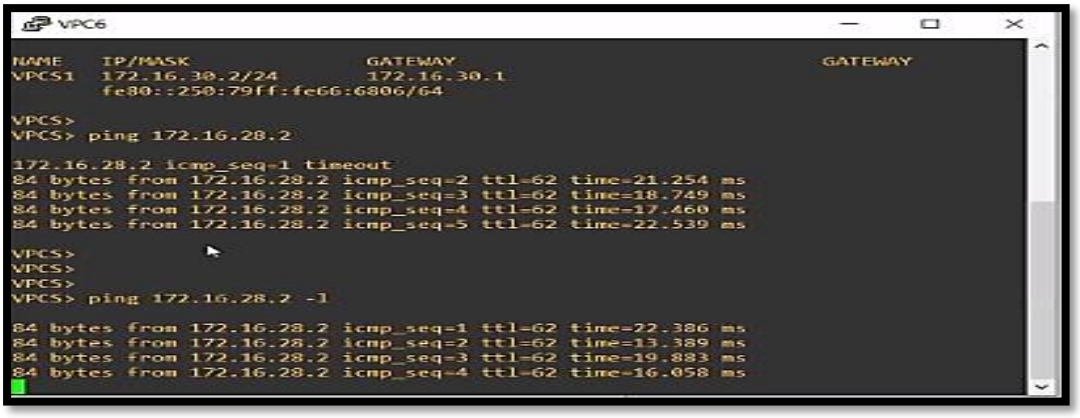


Figura 3.58 Prueba de conectividad de las IP asignadas. Elaborado por: Autor

En la figura 3.58 se realiza una prueba de conectividad ejecutando el comando PING a la IP 172.16.20.2 comprobando que existe conexión con la red del rectorado mediante la interfaz SD-WAN. PING a la IP 172.16.28.2 comprobando que existe conexión con el centro de cómputo mediante la interfaz SD-WAN.

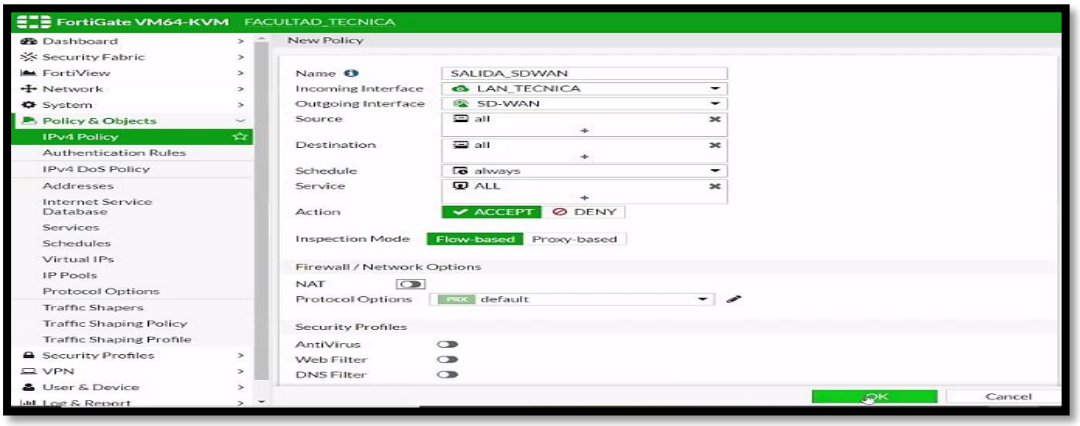


Figura 3.59 Creación de política de salida del laboratorio.
Elaborado por: Autor

En la figura 3.59 se procede a crear una política de direccionamiento para ello nos ubicamos en Policy and Objects, seleccionamos IPv4 Policy nombramos a la política como Salida, asignamos SD-WAN en la interfaz entrante asignamos a la LAN_TECNICA y en la interfaz de salida a la SD-WAN con cualquier IP de origen y destino

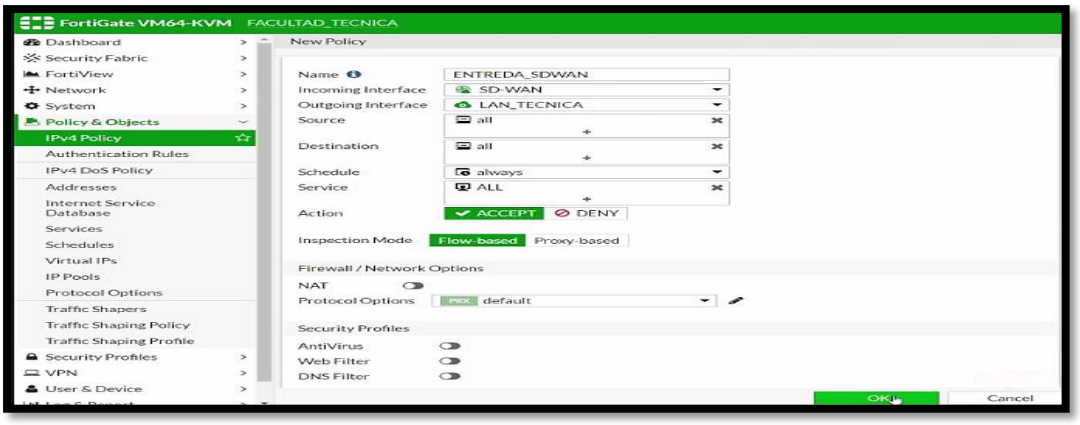


Figura 3.60 Creación de política de entrada del laboratorio.
Elaborado por: Autor

En la figura 3.60 se procede a crear una política de direccionamiento para ello nos ubicamos en Policy and Objects, seleccionamos IPv4 Policy nombramos a la política como Entrada. Asignamos SD-WAN en la interfaz entrante, asignamos a la LAN_TECNICA y en la interfaz de salida a la SD-WAN con cualquier IP de origen y destino.

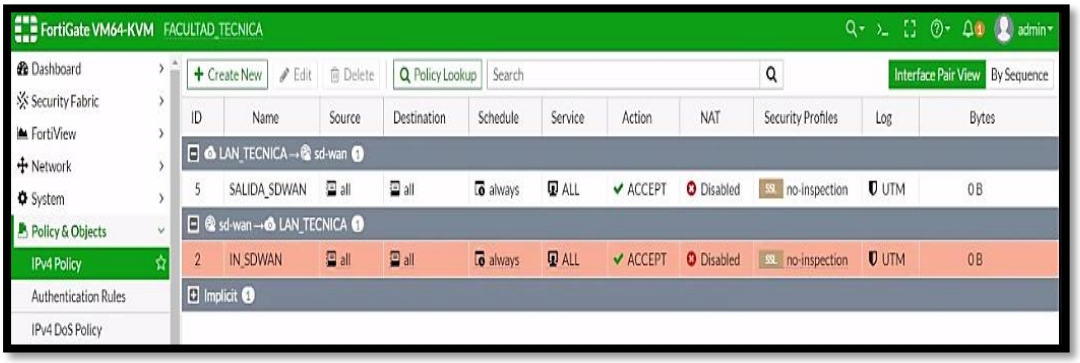


Figura 3.61 Políticas creadas de entrada y salida.
Elaborado por: Autor

Figura 3.62 Creación de política de salida del rectorado.
Elaborado por: Autor

En la figura 3.62 se procede a crear una política de direccionamiento para ello nos ubicamos en Policy and Objects, seleccionamos IPv4 Policy nombramos a la política como Salida, asignamos la LAN_RECTORADO en la interfaz entrante en la interfaz de salida asignamos a la SD-WAN con cualquier IP de origen y destino.

Figura 3.63 Creación de política de entrada del rectorado.
Elaborado por: Autor

En la figura 3.62 se procede a crear una política de direccionamiento para ello nos ubicamos en Policy and Objects, seleccionamos IPv4 Policy nombramos a la política como IN_SD-WAN.

Asignamos SD-WAN en la interfaz entrante, asignamos a la LAN_RECTORADO como la interfaz de salida con cualquier IP de origen y destino.

Figura 3.64 Políticas creadas de entrada y salida.
Elaborado por: Autor

Figura 3.65 Interfaz WAN_FO_TECNICA.
Elaborado por: Autor

En la figura 3.65 se procede asignar a la interfaz de la WAN_FO_FTECNICA correspondiente al puerto 1 un Gateway 10.10.10.1 del equipo ubicado en el rectorado.

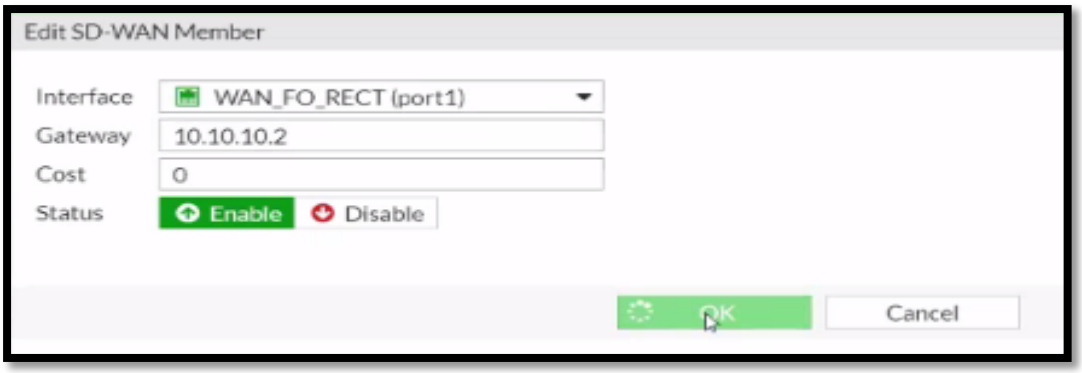


Figura 3.66 Interfaz WAN_FO_RECT.
Elaborado por: Autor

En la figura 3.65 se procede asignar a la interfaz de la WAN_FO_RECT correspondiente al puerto 1 un Gateway 10.10.10.1 del equipo ubicado en el laboratorio de la facultad técnica.

3.3. Pruebas de conectividad aplicando una solucón SD-WAN.

Paso 1. Para realizar de manera correcta las pruebas de conectividad se emplean métodos como balanceo de cargas en este caso se comprobará las conexiones del equipo ubicado en el laboratorio de la facultad técnica al que se le asignó a cada interfaz un porcentaje del 25% como muestra la figura 3.66.

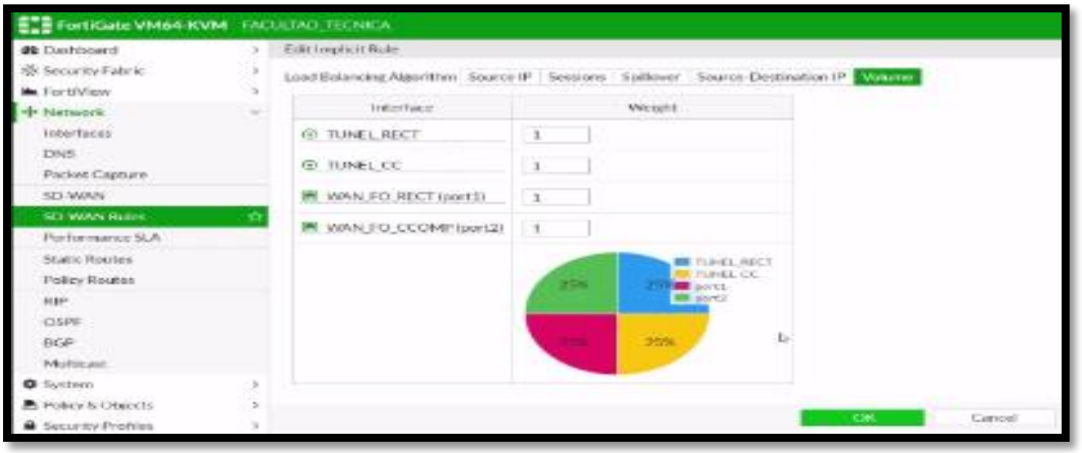


Figura 3. 67 Comprobación de conectividad de la interfaz SD-WAN.
Elaborado por: Autor.

Paso 2. Se procede a ejecutar un PING extendido sobre el centro de cómputo demostrando que el puerto que corresponde a esta interfaz tiene más prioridad al realizar el balanceo y que de ninguna manera se pierde conectividad. Lo único que varía son las gráficas de volumen por donde circula los datos como muestra la figura 3.67.

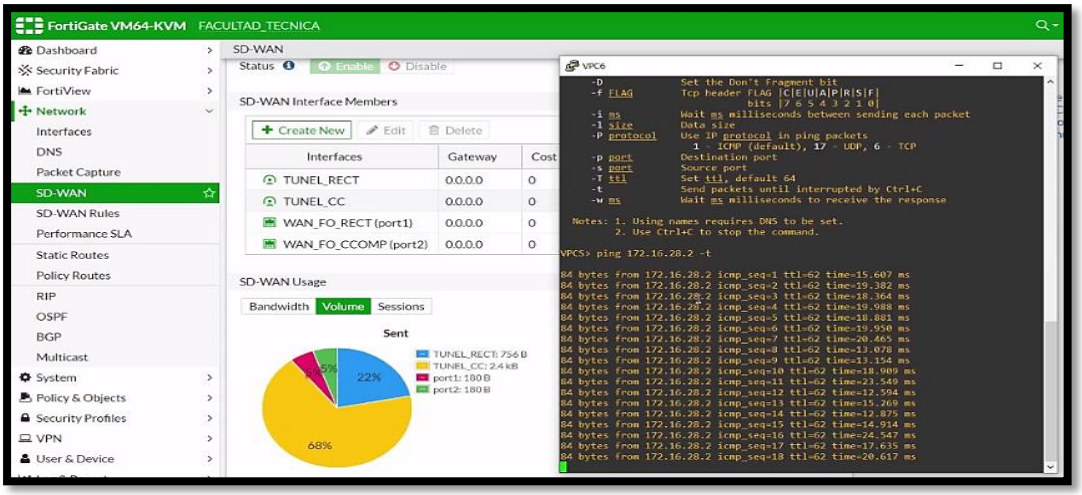


Figura 3.68 Prueba 1 PING extendido al centro de cómputo.
Elaborado por: Autor.

Figura 3.69 Prueba 2 Tráfico fluye solo por la interfaz del centro de cómputo.
Elaborado por: Autor.

Como se puede observar en la figura 3.69. Se realiza la desconexión de la interfaz de datos demostrando que el balanceo de cargas tiene como prioridad al puerto que pertenece a internet. Ejecutamos un PING a la IP 172.16.38.2 para verificar que la conexión no se haya caído lo cual muestra resultados positivos.

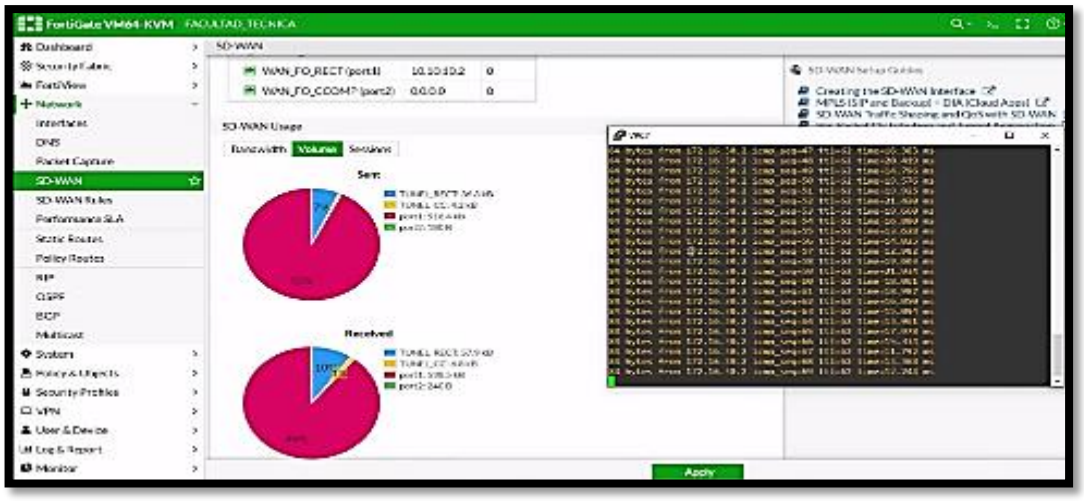


Figura 3.70 Prueba 3. Tráfico que fluye por el enlace de internet.
Elaborado por: Autor.

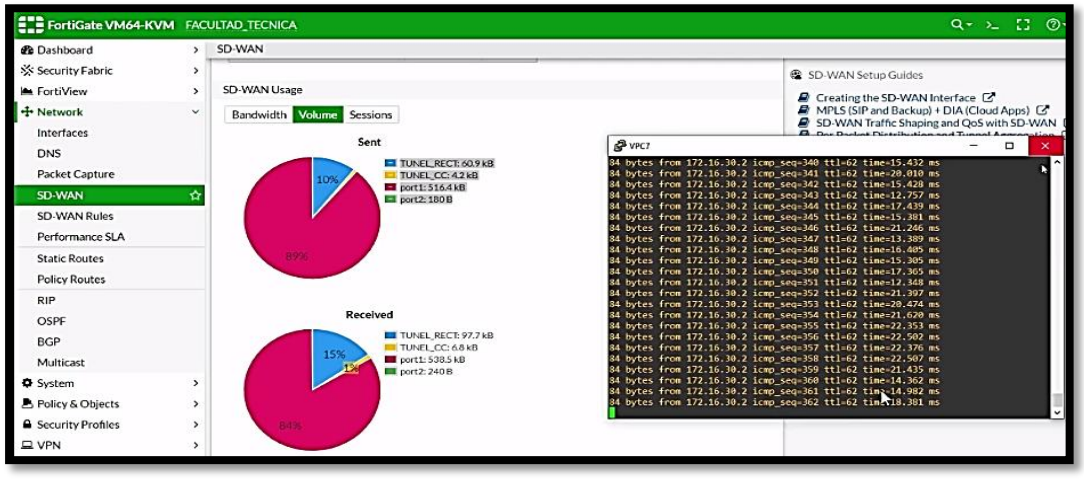


Figura 3.71 PING a la IP 172.16.38.2 prueba de conectividad 3.
Elaborado por: Autor

Como se puede observar en la figura 3.71 las pruebas realizadas de conectividad demuestran la alta capacidad que poseen la tecnología SD-WAN brindando alta disponibilidad de conexiones de red. Aunque exista una caída en la interfaz la conectividad se mantiene ya que el trafico fluye por el enlace SD-WAN que tiene asignado túneles que conectan al rectorado y al centro de cómputo.

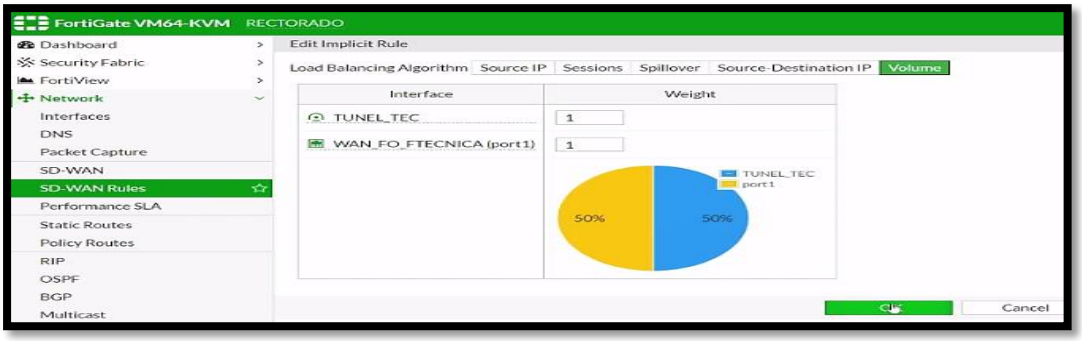


Figura 3.72 Prueba 4 volumen asignado a cada puerto para prueba de balanceo de cargas.
Elaborado por: Autor.

Como se puede observar en la figura 3.72 se asigna el volumen a cada puerto en los enlaces del equipo ubicado del rectorado hacia el laboratorio de la facultad técnica. Se procede a realizar las pruebas de conectividad ejecutando un PING a la IP 172.16.30.2 con la finalidad de realizar el balanceo, se muestra en la gráfica que el mayor tráfico de datos fluye por el enlace del rectorado manteniendo la conectividad en todo momento como muestra la figura 3.72.

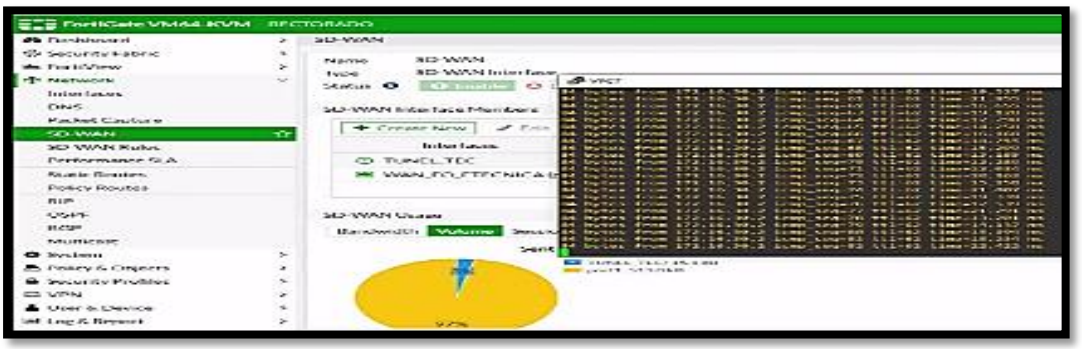


Figura 3.73 PING a la IP 172.16.30.2.
Elaborado por: Autor.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones.

- En el presente documento, se procedió a realizar un estudio acerca de la parte fundamental de las redes de área amplia definida por software (SD-WAN), enfocándose varios conceptos sobre la red definida por software (SDN), como es su arquitectura, y sobre todo los procesos de funcionamiento.

- En el diseño de la red SD-WAN aplicada al laboratorio de la facultad técnica de la UCSG, se puede comprobar la alta capacidad que posee la red al momento de realizar balanceo de carga proporcionando una alta disponibilidad a la red, y si se presentan problemas como la caída en una interfaz, la tecnología SD-WAN procede a enviar el tráfico de información hacia otra interface vinculada a través de su interfaz virtual, manteniendo la conectividad, se tiene una mayor efectividad en la administración, ampliación de la red

- Finalmente, luego de proceder a realizar las respectivas pruebas de conectividad y caídas de interfaces de la red SD-WAN queda demostrado la alta capacidad que posee está tecnología además de tener una mayor efectividad en la administración, ampliación de la red y un control centralizado de toda la red.

4.2 Recomendaciones.

- Para incorporar alta disponibilidad en la red, se recomienda implementar túneles virtuales IPsec estableciendo prioridades por cada enlace de la red.

- Para mejorar el rendimiento de las apps críticas y controlar su funcionamiento se recomienda implementar enlaces SD-WAN para poder ver la actividad en tiempo real y aplicar cambios de manera sencilla.

- Para establecer conexiones de manera segura a través de enlaces internet, se recomienda establecer VPN site to site sin necesidad de tener un enlace de internet contratado.

- Para emigrar de una red tradicional a una red con tecnología SD-WAN, el porcentaje de ahorro en promedio es de un 50% en gastos de equipos y mano de obra con respecto a las demás.

Bibliografía

Ahmed, K., Blech, J., Gregory, M., & Schmidt, H. (2018). Software Defined Networks in Industrial Automation. *Journal of Sensor and Actuator Networks*, *7*(3), 33. Obtenido de: https://doi.org/10.3390/jsan7030033

Albán, P. (2015). *Diseño e implementación del prototipo de una red definida por software (SDN) en la Universidad de las Fuerzas Armadas ESPE*. Obtenido de: http://repositorio.espe.edu.ec/jspui/handle/21000/9848

Atencio, A. (2017). Diseño e implementación de un prototipo de red privada virtual en capa 3 utilizando Cisco IOS para la Universidad Nacional del Altiplano. *Universidad Nacional del Altiplano*. Obtenido de: http://repositorio.unap.edu.pe/handle/UNAP/5789

Bannour, F., Souihi, S., & Mellouk, A. (2018). Distributed SDN Control: Survey, Taxonomy, and Challenges. *IEEE Communications Surveys Tutorials*, *20*(1), 333-354. Obtenido de: https://doi.org/10.1109/COMST.2017.2782482

Bonilla, J. (2016). *"Diseño e implementación de un firewall l2 utilizando redes definidas por software (SDN)"*. Obtenido de: http://repositorio.puce.edu.ec:80/xmlui/handle/22000/13153

Brito, M. (2018). *Características de las redes definidas por software(SDN) para su Implementación en el Ecuador. Obtenido de:* http://repositorio.ucsg.edu.ec/handle/3317/9748

Carbonel, A. (2018). *Estudio de la virtualización de funciones de red (NFV) y aplicación del encadenado de funciones (SFC) para un diseño flexible de red*. Universidad de Zaragoza.

Cevallos, L. (2018). *Implementación de redes definidas por software (SDN) sobre redes IEEE 802.11 mediante MININET Wi-Fi.*

Cosío, E. (2017). *Item 1007/898 | Repositorio CICESE*. Obtenido de: http://cicese.repositorioinstitucional.mx/jspui/handle/1007/898

Dorantes, G. (2017). *Caracterización de las redes NFV*. Obtenido de: http://dspace.uclv.edu.cu:8089/xmlui/handle/123456789/10917

Farhady, H., Lee, H., & Nakao, A. (2015). Software-Defined Networking: A survey. *Computer Networks*, *81*, 79-95. Obtenido de: https://doi.org/10.1016/j.comnet.2015.02.014

Fernández, J. (2006). *Redes Privadas Virtuales*. Obtenido de: http://eprints.rclis.org/13992/

Gartner, G. (2019). SD-WAN, calidad y versatilidad para las comunicaciones remotas | IT Whitepapers. *IT User*. Obtenido de: https://www.ituser.es/it-whitepapers/2019/06/sdwan-calidad-y-versatilidad-para-las-comunicaciones-remotas

Guanoluisa, E. (2019). *Diseño de la arquitectura de una red SDN mediante el protocolo Openflow con simulación en el software mininet para la infraestructura de una PYMES*. Obtenido de: http://dspace.udla.edu.ec/handle/33000/10884

Heredia, (2019). Introducción a las Tecnologías de Optimización de WAN. *Netquarks Technologies*. Obtenido de: https://netquarks.org/2019/05/28/introduccion-a-las-tecnologias-de-optimizacion-de-wan/

Herrera, J. (2019). *Uso de la tecnología de virtualización de funciones de red (nfv) en el laboratorio de redes de la universidad técnica de Cotopaxi. Obtenido de:* http://repositorio.utc.edu.ec/handle/27000/5319

Herrera, W. (2015). *Diseño, configuración y prueba de conectividad de una topología de red para área local y extensa*. Obtenido de: http://repositorio.utmachala.edu.ec/handle/48000/5123

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

Lerner, A. (2017). SD-WAN: Qué es y por qué lo va a usar. *NetworkWorld*. Obtenido de: https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar

Lobo, O. (2016). *Diseño de una arquitectura basada en tecnología "SDN" (REDES DEFINIDAS POR SOFTWARE) para el laboratorio de redes y telecomunicaciones de la UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA*.

López, (2019). ¿Qué es la virtualización de red y por qué se habla de ello? *El blog de Orange*. Obtenido de; http://blog.orange.es/red/la-virtualizacion-red-se-habla-ello/

Manzano, V. (2020). *Internet de las cosas basado en redes definidas por software*. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30708

Martel, V. (2019). Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764. *Universidad Peruana de Ciencias Aplicadas (UPC)*. Obtenido de: https://doi.org/10.19083/tesis/625693

Mejía, J. (2012). *Mecanismos de seguridad para un servidor VPN en LINUX en el laboratorio de redes y seguridad*. Obtenido de: http://132.248.52.100:8080/xmlui/handle/132.248.52.100/250

Meneses, J. (2019). *Revista Gerencia—SD-WAN: La transformación de las redes*. Obtenido de: http://www.emb.cl/gerencia/articulo.mvc?xid=4768&ni=sd-wan-la-transformacion-de-las-redes

Navas, M. (2006). *Estudio y diseño de la red wan para el centro de capacitación informática CECAI*. Obtenido de: http://repositorio.espe.edu.ec/jspui/handle/21000/126

Ñacato, M. (2007). *Diseño e implementación de una red privada virtual (VPN) para la empresa Hato telecomunicaciones*. Obtenido de: http://bibdigital.epn.edu.ec/handle/15000/1309

Pacheco, E. (2015). *Red privada virtual (VPN) para un sistema de telemedicina entre el Hospital Provincial General Docente Ambato y sus Centros de Salud*. Obtenido de: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/8597

Pérez, S. (2017). *Dispositivos y Protocolos en Redes LAN Y WAN*.

Quijano, J. (2014). *Acl seguridad-ip* [Tecnología]. Obtenido de: https://es.slideshare.net/jcquijano/acl-seguridadip

Ramos, L. (2016). *Diseño de una red VPN para la integración de los servicios de VOIP y video vigilancia para los infocentros comunitarios. Obtenido de:* http://repositorio.puce.edu.ec:80/xmlui/handle/22000/12606

Ríos, R. (2016). Conceptualización de SDN y NFV. *Maskay*, *6*(1), 29-34

Rodríguez, J. (2019). *SD-WAN, la respuesta a las necesidades de la red empresarial*. Obtenido de: https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/sd-wan-the-answer-to-networking-demands-es.pdf

Romero, H. (2019). VPN de tipo SSTP con autenticación RADIUS. *TechClub Tajamar*. Obtenido de: https://techclub.tajamar.es/vpn-de-tipo-sstp-con-autenticacion-radius/

Roncero, Ó. (2014). *Software Defined Networking*. Obtenido de: https://upcommons.upc.edu/handle/2099.1/21633/

Rugerio, A. (2013). *Seguridad en redes virtuales privadas (VPNs)*. Obtenido de: https://repository.uaeh.edu.mx/bitstream/handle/123456789/10536

Sánchez, L. P. C. (s. f.). *INGENIERA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES*. 85.

Telefónica, A. (2016). *La-virtualización-de-red-el-futuro-de-la-red-para-la-empresa-digital.pdf*. 8

Webmaster, (2019). Introducción a las Tecnologías de Optimización de WAN. *Netquarks Technologies*.

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*.

Glosario

API: Interfaz de Programación de Aplicaciones.

ATM: Modo de Transferencia Asíncrona.

Backup: Proceso de copia de seguridad.

Cloud: Interfaz Virtual de almacenamiento.

Data Center: Centro de Datos.

Dial-up: Conexión por línea conmutada.

DTE: Equipo Terminal de Datos.

EMS: Sistema de gestión de elementos.

ETSI: Instituto de Normas Europeas.

Frame Relay: Retransmisión de tramas.

Híbridas: Redes que agregan múltiples tecnologías de acceso.

Hipervisor: Software que crea y ejecuta máquinas virtuales.

IEEE: Instituto de ingeniería Eléctrica y Electrónica.

IPsec: Protocolo de Seguridad de Internet.

ISP: Proveedor de Servicios de Internet.

L2TP: Protocolo de Tunelización de Capa 2.

MPLS: MultiProtocol Label Switching.

NFV: Virtualización de las funciones de red.

NFVI: Infraestructura de Virtualización de Funciones de Red.

Políticas: Bloquea o permite determinados tipos de tráfico de red.

PPP: Protocolo Punto Punto.

PPTP: Protocolo de Tunelización de Punto a Punto.

SDN: Redes definidas por software.

SD-WAN: Redes de Área Amplia Definida por Software.

TCP/IP: Protocolo de Control de Transmisión IP.

TDM: Multiplexación por división de tiempo.

Tunneling: Técnica que encapsula un protocolo de red sobre otro.

VNF: Funcione de Red Virtualizada.

VPN: Red Privada Virtual.

WAE: Ethernet de Área Amplia.

WAN: Red de Área Amplia.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Romero Naula, Luis Fernando** con C.C: # 070509950-5 autor del Trabajo de Titulación: **Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica de la UCSG** 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, 15 de septiembre del 2020

f._____

Nombre: Romero Naula, Luis Fernando

C.C: 070509950-5

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la facultad técnica de la UCSG		
AUTOR(ES)	Romero Naula, Luis Fernando		
REVISOR(ES)/TUTOR(ES)	M. Sc. Bastidas Cabrera Tomas Gaspar		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	15 de septiembre del 2020	**No. DE PÁGINAS:**	88
ÁREAS TEMÁTICAS:	Sistemas Telemáticos, Sistemas de Transmisión		
PALABRAS CLAVES/ KEYWORDS:	SD-WAN, MPLS, WAN, Políticas, Híbridas.		

RESUMEN/ABSTRACT:

El presente trabajo como objetivo principal la implementación de una solución de área amplia definida por software (SD-WAN), aplicada al laboratorio de la facultad técnica de la UCSG. Se definieron conceptos básicos como: arquitectura SD-WAN, tecnologías de tunneling, redes virtualizadas. Mediante una máquina virtual se realizó la simulación de una red de área amplia definida por software de la cual se crearon enlaces que conectan con el rectorado, con el centro de cómputo y con salida a internet. En las pruebas que se realizaron en la implementación de la solución SD-WAN fueron por los métodos de balanceo de cargas, pruebas de conectividad y simulaciones de caída de interfaces en la red la cual establece una completa conectividad de la WAN entre sus sucursales, por medio de un mecanismo de control centralizado, abordando la creciente lactancia y el costo con el uso de enlaces de ancho de banda más económicos. En conclusión, al emplear nuevas tecnologías de red es posible implementar soluciones de alta capacidad, eficientes para el rendimiento de la red por medio del balanceo de cargas y priorización de tráfico basadas en políticas SD-WAN

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593986707875	E-mail: fernandoromeronaula@gmaill.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez, Edwin Fernando	
	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):	