UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Diseño y Simulación de una Red de Accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador

AUTOR:

Ing. Fulvio Andrés Carrasco Cabrera

Trabajo de Titulación previo a la obtención del grado de

Magister en Telecomunicaciones

TUTOR:

Ing. Manuel de Jesús Romero Paz, MSc.

Guayaquil, 6 de noviembre de 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Fulvio Andrés Carrasco Cabrera**, como requerimiento para la obtención del Título de **Magíster en Telecomunicaciones**.

TUTOR

f. _____

Romero Paz, Manuel, MSc.

DIRECTOR DEL PROGRAMA

f. _____

Romero Paz Manuel, MSc.

Guayaquil, 6 de noviembre de 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Fulvio Andrés Carrasco Cabrera**

DECLARO QUE:

El Trabajo de Titulación, **Diseño y Simulación de una Red de Accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador** previo a la obtención del Título de **Magíster 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, 6 de noviembre de 2020

EL AUTOR

f. _____

Fulvio Andrés Carrasco Cabrera

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Fulvio Andrés Carrasco Cabrera**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación **Diseño y Simulación de una Red de Accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

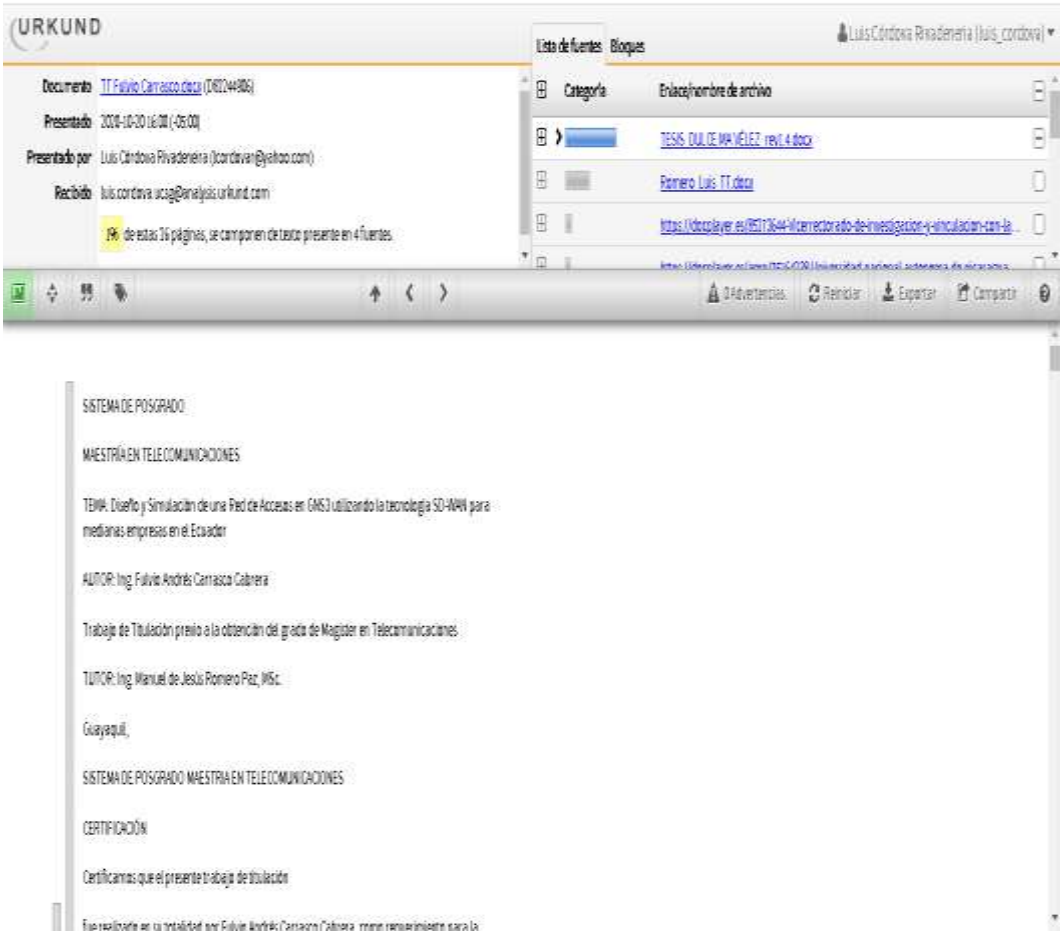
Guayaquil, 6 de noviembre de 2020

EL AUTOR:

f. _____

Fulvio Andrés Carrasco Cabrera

REPORTE DE URKUND



DEDICATORIA

Este proyecto de titulación está dedicado a Dios, que me ha dado la sabiduría, la perseverancia y la inteligencia para seguir creciendo en mi formación profesional, de igual manera a mis padres Fulvio y Narcisa que con su esfuerzo, dedicación y mucho amor han sido en todo momento mi inspiración y mi gran fortaleza. A mis hermanos Luis y Roberto que en todo momento estuvieron conmigo, alentándome para lograr esta meta.

Fulvio Andres Carrasco Cabrera

AGRADECIMIENTOS

Mi agradecimiento a Dios por darme la oportunidad de cumplir una nueva meta en mi formación profesional.

A mis padres Fulvio Carrasco y Narcisa Cabrera, quienes siempre han sido mi ejemplo y ese pilar fundamental para poder cumplir con mis logros.

A mis hermanos Luis y Roberto por el apoyo incondicional para cumplir con este reto.

Al Ing. Manuel Romero quien, con sus conocimientos, experiencia, y motivación ha logrado que pueda terminar con éxito este trabajo de titulación.

Fulvio Andres Carrasco Cabrera

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. 

MSc. Manuel Romero Paz

TUTOR

f. 

MSc. Edgar Quezada Calle

REVISOR

f. 

MSc. Luis Córdova Rivadeneira

REVISOR

f. 

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En atención a la necesidad que tienen muchas empresas en el Ecuador en optimizar recursos, reducir gastos y tener procesos que permitan garantizar calidad, que pueda crecer, flexible y versátil, surge SD-Wan (Red de Área Amplia Definida por Software), que brinda muchas ventajas ante las tecnologías actuales. Este trabajo de titulación se realizará mediante el método deductivo, lo que permitirá caracterizar y aprender las aplicaciones de esta tecnología para poder realizar el diseño y simulación para empresas medianas en el Ecuador. La tecnología SD-Wan hoy en día tiene un amplio campo de aplicaciones, debido a que se requiere de pocos recursos para su configuración e implementación, por lo que, por medio de un programa brindado por un simulador lo cual se realizará en esta investigación, demostrando la flexibilidad, versatilidad y escalabilidad de esta tecnología.

Palabras clave: SD-Wan, MPLS, PBR, IP-Sec, BGP, GNS3.

ABSTRACT

In response to the need that many companies in Ecuador have to optimize resources, reduce expenses and have processes that allow guaranteeing quality, which can grow, flexible and versatile, SD-Wan (Wide Area Network Defined by Software) arises, which provides many advantages over current technologies. This degree work will be carried out through the deductive method, which will allow characterizing and learning the applications of this technology in order to carry out the design and simulation for medium-sized companies in Ecuador. SD-Wan technology today has a wide field of applications, due to the fact that few resources are required for its configuration and implementation, therefore, through a program provided by a simulator which will be carried out in this research, demonstrating the flexibility, versatility and scalability of this technology.

Keywords: SD-Wan, MPLS, PBR, IP-Sec, BGP, GNS3.

Capítulo 1: Descripción del proyecto de intervención.

Con el reto de abarcar con todas las expectativas en la comunicación de datos e internet de las medianas y grandes empresas, es necesario implementar una nueva tecnología de telecomunicaciones llamada SD-WAN (Software Defined - Wide Area Network) la misma que se basa en un ruteo más inteligente que los convencionales, capaz de enrutar el tráfico convencional de una manera más ágil y segura, obteniendo así, el control total del ancho de banda de los enlaces y optimizar de mejor manera los recursos de la red.

1.1 Introducción.

Debido a la alta demanda de conectividad y transmisión de datos en el mundo de redes de telecomunicaciones digitales, se ha desarrollado la tecnología SD-WAN, la misma que al ser implementada en una empresa u organización corporativa, permitirá a través de la gestión de un software, tener el control de múltiples conexiones y el manejo de un gran volumen de información que hoy en día circula por las redes a nivel mundial.

Actualmente optimizar una red es posible, gracias a esta nueva tecnología SD-WAN, la cual permite enrutar el tráfico convencional de una manera ágil y segura, y converger con tecnologías ya definidas y comercializadas desde hace muchos años en materia de conectividad como MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) y sus protocolos, e incluso tecnología móvil como 3G y LTE (Long Term Evolution) o 4G sobre Internet, dejando atrás los canales privados de datos, los cuales utilizan las grandes o medianas empresas a nivel mundial.

Si ya se tiene una opción en el mercado para que las redes WAN, con un enfoque empresarial cuenten con seguridades de información y a la vez sean flexibles administrativamente, es muy beneficioso para una empresa migrar a SD-WAN y dejar a un lado las conexiones a través de MPLS, que como es de conocimiento general son muy costosas, y de esta manera se mejorará el rendimiento y consumo del ancho de banda contratado, así por ejemplo, ya no se requerirá en sitio de

instalaciones complejas y configuraciones de equipos de una nueva sucursal (routers y más conexiones).

En el presente trabajo de investigación, se desarrolla el estudio y simulación de la implementación de esta red con los beneficios que puede conceder esta tecnología, que a base de una infraestructura totalmente digital que cumple con parámetros importantes como son productividad, eficiencia y reducción de costos, puede solucionar y optimizar muchos recursos cumpliendo con las garantías de calidad de servicios QoS (Quality of Service).

1.2 Antecedentes.

La WAN es una red de larga distancia con gran extensión geográfica. Un buen ejemplo de representación de la WAN es la propia Internet, por abarcar una zona geográfica global, interconectando ciudades, países y continentes.

Con tanta información circulando en las redes, tendrán éxito las empresas que saben cómo usarlo todo a su favor. Y para ello, es necesario que estos datos puedan seguir con más fluidez y seguridad, algo que no sucede en forma efectiva con las infraestructuras de WAN que se tiene hoy en día.

Actualmente la mayoría de las infraestructuras de WAN tienen un bajo ancho de banda y una alta latencia, debido al tráfico de backhauling y la falta de visibilidad de las aplicaciones, resultando a menudo en una pésima experiencia para el usuario. En este sentido, las empresas que tienen su núcleo empresarial basadas en servicios y procesos realizados a través de Internet pueden sufrir con los reflejos de comunicaciones lentas, indisponibilidad de sistemas esenciales, pérdida de datos, además de diversos otros problemas que generan pérdida de tiempo y dinero.

Así surge como una alternativa para solucionar estos problemas el SD-WAN, que permite una comunicación más eficiente y segura.

1.3 Planteamiento del Problema.

En la actualidad las empresas necesitan incrementar recursos en sus sistemas de comunicación ya sea de datos o internet, lo cual genera diversas acciones a tomar (Vélez, 2018).

El incremento de nuevos recursos para los enlaces de redes WAN generan diferentes tipos de tráfico en su red, pudiendo llegar a que esto sature o se presente alguna falla en la red, provocando la degradación, latencia o pérdida del enlace, en algún escenario de comunicación puede conllevar a que estos equipos no sepan cómo redireccionar y optimizar el tráfico de los enlaces de manera dinámica buscando otros caminos.

Por estas razones o motivos, la función del operador de la red se vuelve más complicada en manejar y proteger una red que cumpla los requerimientos y necesidades de una empresa, debido a que actualmente las entidades requieren cumplimientos en sus acuerdos de disponibilidad de sus redes o SLA (Service Level Agreements) (Vélez, 2018).

1.4 Definición del Problema.

La necesidad de contar con el diseño y simulación de una red de accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador.

1.5 Justificación del Problema.

Con la simulación de una red de accesos utilizando la tecnología SD-WAN mediante el Software GNS3 (Graphic Network Simulation), se podrá conocer las ventajas y beneficios que brinda esta tecnología, ya que se estudiará y se analizará esta nueva arquitectura en la red y a su vez logrará optimizar y simplificar los recursos, haciendo las redes más seguras y dinámicas (Vélez, 2018).

La implementación de la tecnología SD-WAN tiene una amplia utilidad, pero en este proyecto se lo enfocará en los beneficios y soluciones que se tendrá al migrar esta tecnología de las redes tradicionales de comunicación (Vélez, 2018).

1.6 Objetivos

A continuación, se detallan los objetivos planteados para la investigación.

1.6.1 Objetivo General:

Diseñar y simular una red de accesos utilizando la tecnología SD-WAN mediante el Software GNS3 al fin de cumplir con las necesidades y requerimientos de las medianas empresas en el Ecuador

1.6.2 Objetivos específicos:

- ✓ Describir y comparar los recursos de implementación y configuración de los componentes que se requieren en tecnología SD-WAN respecto a las tecnologías tradicionales.

- ✓ Describir los beneficios y servicios que brinda una red de accesos utilizando la tecnología SD-WAN para las medianas empresas.

- ✓ Analizar mediante el gestor de simulación GNS3 la operación que brinda la tecnología SD-WAN.

1.7 Hipótesis

Las exigencias e insuficiencias de las empresas en ésta época impulsan el desarrollo de una red de accesos utilizando la tecnología SD-WAN brindará optimización de recursos, redes más seguras, mejor rendimiento en el ancho de banda, optimización del rendimiento de las aplicaciones lo cual es útil para para el cliente, diferenciando el tráfico y exponiendo prelaciones en sus servicios.

1.8 Metodología de investigación

El estudio empieza con una investigación exploratoria de las redes de acceso de comunicación tradicional en las medianas empresas en el Ecuador y pretende explorar los beneficios que brindará a los clientes haciendo sus redes más seguras.

Para el desarrollo de este proyecto se aplica el método científico utilizando la investigación descriptiva y exploratoria, con la finalidad de describir las características de la tecnología SD-WAN que permitirá tener en cuenta aspectos de relevancia al momento de desarrollar el diseño de una Red de Accesos utilizando dicha tecnología.

Asimismo, es del tipo experimental y analítico ya que requiere ejecutar mediante la simulación, un análisis de los beneficios que brindará a las empresas dicha tecnología

Capítulo 2: Fundamentación Teórica

En este capítulo se explicará la fundamentación teórica del funcionamiento y componentes que integran la tecnología SD-WAN, como también los grandes beneficios que se obtendrán respecto a las redes de comunicaciones tradicionales.
Antes de realizar la explicación de la tecnología SD-WAN, a continuación, se hará un breve repaso de las redes más tradicionales por su forma y por su cobertura en el mundo de las telecomunicaciones.

2.1 Tipos de Redes de comunicaciones empresariales

Para poder tener un adecuado manejo de la información de una empresa es necesario contar con redes de comunicaciones adecuadas y efectivas a fin de poder compartir y proteger dicha información y de manera primordial que la misma esté disponible para todos los miembros involucrados.

En el mundo de las telecomunicaciones existen diferentes tipos de redes de comunicación que se adaptan de forma efectiva, práctica y segura a las necesidades de las diferentes empresas.

La clasificación más común son las redes centralizadas y descentralizadas. En las centralizadas la comunicación gira en torno a una única persona que es la encargada de dirigir todo el proceso y funciona como eje principal para los otros miembros de la empresa. En la descentralizada la comunicación interactúa constantemente entre los miembros de la empresa sin que haya un líder o miembro destacado en la cadena.

También existen otras maneras de clasificación, entre las más comunes y utilizadas en las organizaciones son las siguientes:

- ✓ **Red en cadena**. La utilizan empresas que necesitan procesar la información respetando la estructura organizacional de ésta, de manera que el intercambio de información que se dé entre los usuarios que se encuentran más próximos, por ejemplo, de un técnico de campo a su supervisor y viceversa.

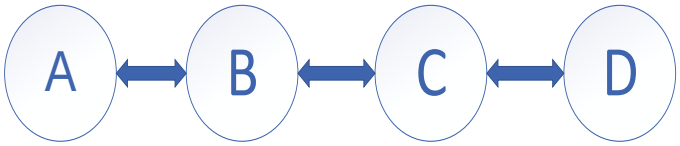


Figura 2.1: Red en Cadena
Fuente: Autor

- ✓ **Red en estrella**. Son utilizadas por empresas con estructuras tradicionales con comunicación unidireccional en donde un usuario ocupa la posición central, (jefe, gerente), mientras que los otros subordinados de la empresa están a su alrededor.

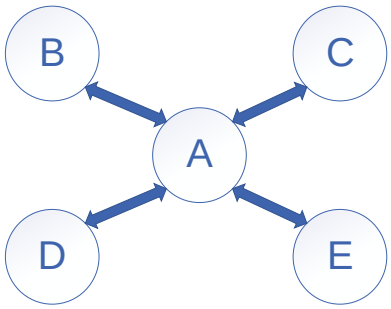


Figura 2.2: Red Estrella
Fuente: Autor

- ✓ **Red en círculo**. Permite intercambiar información de un usuario a otro hasta llegar de nuevo al usuario de origen. Su inconveniente más frecuente es que cada usuario de la red tiene contacto directo únicamente con otros dos usuarios. Sin embargo, este tipo de red facilita notablemente la trasmisión y recepción de la información, lo cual permite resolver problemas complejos de manera eficiente sin importar el rango o jerarquía de cada usuario.

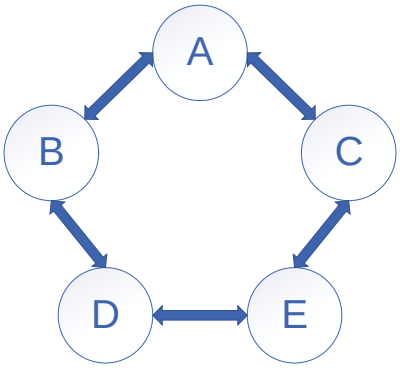


Figura 2.3: Red en Circulo
Fuente: Autor

- ✓ **Red en "Y".** Es muy semejante a la red en cadena, diferenciándose de que uno de los usuarios de los niveles jerárquicos, ya sea un jefe o un supervisor, a fin de que se pueda mejorar el proceso de información, es decir cuando dos usuarios de bajo nivel jerárquico informan a su supervisor individualmente una incidencia laboral, a fin de que éste a su vez presente el informe o haga conocer de esta incidencia al siguiente usuario en el rango jerárquico ascendente.

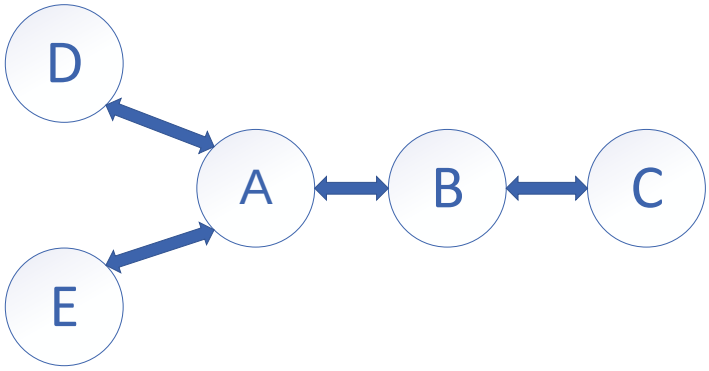


Figura 2.4: Red en Y
Fuente: Autor

- ✓ **Red en Multiconexión**. En este caso todos los usuarios de una empresa tienen la posibilidad de procesar información con cualquier otro usuario de la misma compañía, sin tener limitantes según la jerarquía organizacional de la empresa.

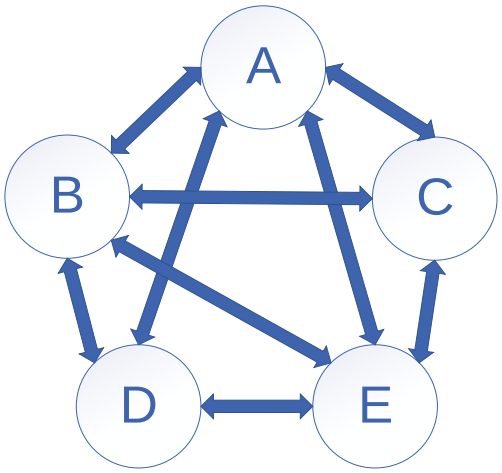


Figura 2.5: Red en Multiconexión
Fuente: Autor

Seleccionar el tipo de red comunicación más adecuado en una empresa no es fácil, por tal razón se recomienda acudir con un experto en el área que lleve a cabo el análisis, evaluación e implementación del mejor sistema a fin de poder compartir e intercambiar información y así mejorar el rendimiento de la organización (El Equipo de Marketing, 2016)

2.2 Red LAN

LAN (Local Area Network, Red de área local), es una red que une los terminales finales (computadoras de escritorio, laptops, impresoras, etc.) en un espacio relativamente pequeño y predeterminado (sala de rack, oficinas, etc.).

Las redes LAN se pueden conectar entre ellas a través de fibra óptica, líneas de cobre y sistemas de microondas. Las oficinas de trabajo con sus terminales finales se encuentran conectados en una red LAN, lo que permite que los usuarios a través de sus terminales finales procesen información y compartan el acceso a los archivos.

2.3 Red WAN

WAN (Wide-Area Network, Red de Área Amplia), es un sistema de conexión de redes LAN, es una red de larga distancia que abarca una gran extensión geográfica que une varias redes, aunque no se encuentren en el mismo sitio.

Comúnmente las redes WAN son utilizadas para comunicar redes LAN y la mayoría de las veces son implementadas por los proveedores de servicios de telecomunicaciones y éstos proporcionarán conexiones LAN a la empresa. En el mundo de las telecomunicaciones el internet es un claro ejemplo de una red WAN, ya que abarca una zona geográfica global, interconectando ciudades, países y continentes (GPC, 2019)

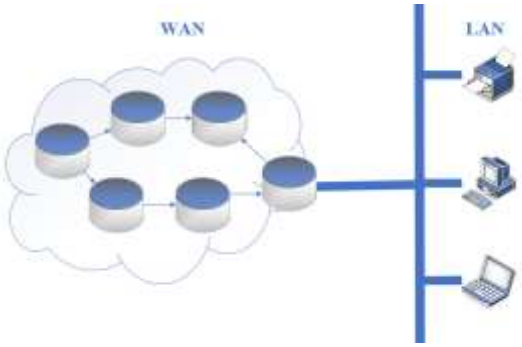


Figura 2.6: Red de Comunicación
Fuente: Autor

2.3.1 Red MPLS

Las redes MPLS fueron concebidas para equiparar el servicio de datos para las redes comunicación implementadas en base a circuitos y en base a paquetes de información**.** Esta red se basa principalmente en la conmutación de etiquetas, de tal manera que se pueda transmitir voz, datos y vídeos en redes VPN/MPLS.

2.3.2 Funcionamiento

Las etiquetas en las que se basa una red MPLS, son insertadas en una capa intermedia del modelo OSI (Open Systems Interconnection), es decir entre los encabezados de la capa de red (capa 2) y la de enlace (capa 3). En otras palabras, lo que MPLS hace es identificar la dirección IP (Internet Protocol) destino, para luego asignarle una etiqueta en el primer router de la red, luego cada equipo dentro de ella se limita a conmutar las etiquetas hacia el último router, logrando independizar la dirección IP y en este último equipo se vuelve a conocer la IP destino. Esta es la manera en la que MPLS se independiza de las tablas de enrutamiento que manejan los routers en una red (Vélez, 2018).

2.3.3 Componentes

Una red MPLS está constituida por dos tipos de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers), Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS, siendo su administrador el que configura su uso. Los nodos MPLS y los routers IP normales, intercambian información sobre la topología de la red mediante los

protocolos de enrutamiento, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de enrutamiento, basándose en la alcanzabilidad a las redes IP destinatarias (Quintana & Tabares, 2011).

- ✓ **LSR** (Label Switching Router): enrutador de alta velocidad dedicado al envío de paquetes etiquetados por MPLS (Quintana & Tabares, 2011).
- ✓ **Etiqueta**: es un identificador corto (de longitud fija) y con significado local, empleado para identificar un FEC (Forwarding Equivalence Class). Un paquete puede tener una o más etiquetas apiladas según la jerarquía.
- ✓ **FEC**: Agrupación de paquetes que comparten las mismas características como dirección destino, VPN, etc. Además, es un término muy usado en MPLS para describir un grupo de paquetes semejantes que pueden reenviase de la misma forma, todos los paquetes que forman parte de la agrupación siguen una misma ruta o LSP (Label Switched Path).
- ✓ **LSP**: Se describe como una ruta con uno o varios LSRs determinados por los niveles de jerárquicos que debe seguir un paquete de datos en un FEC determinado. Esta ruta puede configurase mediante protocolos de enrutamiento o manualmente (Hesselbach & Altés, 2015).

2.3.4 Protocolos

Un protocolo de red es una serie de acuerdos que actúan en la capa de red del modelo OSI que tiene la particularidad de realizar el intercambio de datos, regulando de esa manera las condiciones para el direccionamiento, transporte, enrutamiento y el control de errores.

Es decir, para que dos elementos finales de red puedan intercambiar información entre ellos, deberán configurarse con protocolos de enrutamiento similares, de tal manera que tengan las mismas condiciones para la transmisión:

2.3.4.1 Clasificación de los protocolos de red

Existe diferentes aspectos técnicos al interconectar dos elementos finales (Computadoras) una red local que conectar un computador a Internet, es decir a un conjunto muy amplio de computadoras con las que intercambian información. De la misma manera, los niveles jerárquicos de los usuarios tienen muchas consideraciones en la comunicación, lo que da lugar a que se utilicen diferentes protocolos de red para cada una de las formas de intercambio de datos, tomando en cuenta las necesidades particulares entre sí, como:

- **Número de participantes en la comunicación**:

  Unicast: Si los datos que se transmiten solo tienen un destinatario.

  Multicast: si el intercambio se produce entre dos o más destinatarios.

  Broadcasting: si el envío de paquetes de datos implica a todos los usuarios de la red.

- **Modo de transmisión de los datos**:

  Símplex: Solo admite la comunicación en una sola dirección, en la cual un terminal funciona solamente como trasmisor y el otro como receptor.

  Half Dúplex: Permite el intercambio de información de forma no simultanea entre dos terminales es decir pueden intercambian sus funciones de trasmisor y receptor y viceversa.

  Full Dúplex: Permite el intercambio de información de datos en ambas direcciones de manera simultánea.

- **Jerarquía de los participantes**:

  Comunicación asimétrica: Es cuando varios clientes pueden iniciar la conexión con un único servidor, el cual procesa los requerimientos.

  Comunicación simétrica: Es cuando los terminales tienen las mismas condiciones y permisos para proporcionar servicios y requerimientos.

- **Sincronización de la comunicación**: la transmisión de datos también se puede diferenciar en función de si se sincronizan los datos transmitidos y recibidos entre un emisor y un receptor.

- **Tipo de conexión**:

  Los protocolos de red orientados a la conexión requieren enlaces seguros entre emisor y receptor durante el intercambio de información y su principal

función es que en todo momento los paquetes lleguen a su destino final en un orden preestablecido de tal manera que, en caso de no entrega de datos, estos se reenvíen nuevamente.

Los protocolos de red que no están orientados a la conexión, envían sus paquetes al destinatario con menos información adicional, provocando que la información no pueda llegar secuencialmente al destinatario y además en caso de no entrega de datos estos no se vuelven a reenviar

2.3.4.2 Cantidad de protocolos existentes en una red

Existen más de 500 protocolos entre los que también se incluye el más importante y popular protocolo de red IP, que constituye el fundamento de Internet.

La principal función de IP es transportar los paquetes de información de un transmisor a un receptor a través de múltiples caminos o redes. Con este objetivo, este protocolo señala las directrices de direccionamiento y de enrutamiento, que deberán seguir los paquetes de información o datos

2.3.4.3 Estructura del protocolo MPLS:

A continuación, se detalla la estructura del protocolo MPLS

- **Multiprotocol .-** Se refiere a los protocolos de Capa 2 o 3 (Vélez, 2018).
- **Label Switching.-** Orientación de paquetes basada en etiquetas (Vélez, 2018)

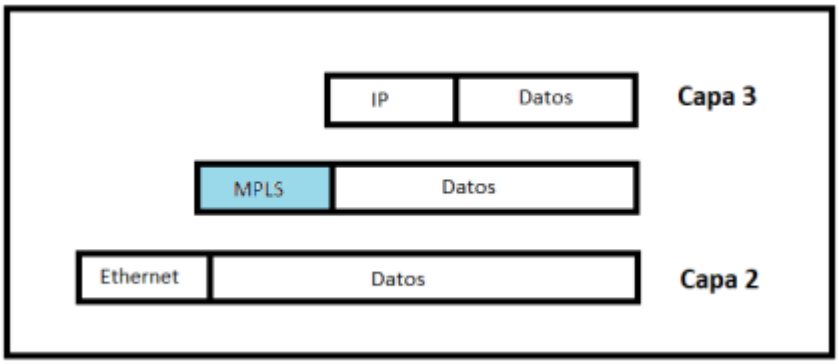


Figura 2.7: Estructura de Protocolo MPLS
Fuente: (Vélez, 2018)

2.4 SD-WAN

En el transcurso del tiempo las redes de telecomunicaciones se han ido expandiendo cada día más y más, dando lugar al crecimiento de la demanda de aplicaciones y servicios para los diferentes tipos de requerimientos y soporte de las empresas, trayendo consigo a los operadores de red dificultades y problemas para gestionar y administrar la red.

Con el antecedente antes indicado, se vuelve imperativo que nuevas tecnologías sean utilizadas para garantizar que la información que se transmita fluya con plena seguridad, de manera particular en las redes corporativas.

La SD-WAN es una nueva manera de conectividad de las redes de datos, que esta siendo utilizada en el mundo de las telecomunicaciones, la cual permite a los administradores tener una mayor flexibilidad de la red y un manejo eficiente del ancho de banda. Reduciendo significativamente los gastos operativos y el tiempo utilizado a la administración del ancho de banda, es decir simplifica la gestión de una red WAN (Ostec, 2018).

Esta tecnología permite a los administradores u operadores de red, usar el ancho de banda de manera más eficiente y efectiva, garantizando a las empresas el mayor nivel de rendimiento para aplicaciones particulares sin tener que perder seguridad o privacidad de la información y a su vez ayuda a evitar interrupciones de tráfico altamente sensible como VoIP (Voice Over Internet Protocol). Además, permite que la red se ajuste dinámicamente a las condiciones cambiantes o redundancias de una WAN sin necesidad de la intervención manual de un operador (CISCO, 2018).

Resumiendo, SD-WAN no tiene límites geográficos para su aplicación, pudiendo registrar mejoras en cuanto a la visibilidad, escalabilidad, rendimiento y funcionamiento de su red.

2.5 Funcionamiento de la Tecnología SD-WAN

La información que circula por las redes es cada día más y más abundante, por tal razón, las empresas que tendrán éxito son las que podrán explotar y usar toda esa información a su favor. Para ello, es necesario que estos datos puedan transitar y llegar a su destino con más fluidez y seguridad, algo que no sucede hoy en día con las redes WAN.

Hoy en día la mayoría de las redes WAN tienen un bajo ancho de banda, alta latencia debido al tráfico de backhauling y falta de visibilidad de las aplicaciones, provocando en el usuario una experiencia poco agradable. En otras palabras, las empresas que se fundamentan en servicios y procesos realizados a través de Internet pueden sufrir indisponibilidad de sus sistemas de control y operaciones esenciales, debido a las comunicaciones lentas, pérdida de datos, además de acarrear otros diversos problemas que generan pérdida de tiempo y dinero.

Es así como emerge SD-WAN como una nueva solución para los problemas antes indicados, la misma que permite una transmisión de datos más eficiente y económica. Gestionar una WAN siempre ha sido muy costoso y no permite fácilmente realizar cambios en la operación de una red empresarial, actualmente SD-WAN permite simplificar la gestión con aplicaciones en dispositivos de red programables, que facilitan a los técnicos de redes realizar remotamente las configuraciones necesarias para su operación y a su vez el sistema realiza de manera automática la elección del mejor camino o enrutamiento, disminuyendo de esta manera los gastos operativos, favoreciendo el rendimiento de la red empresarial, calidad de servicio y aseguramiento de datos en los enlaces de Internet.

Lo que hace que SD-Wan sea tan capaz y eficiente es exactamente su software inteligente, que permite que el tráfico LAN se enrute automáticamente por el camino más óptimo de la WAN, el mismo que utilizará métricas de calidad de los enlaces, como el tiempo de respuesta para la elección del mejor camino, evitando que el enrutamiento se base sólo en el protocolo dinámico, con esto se garantizara la calidad del servicio y la seguridad de la información que fluye por el Internet (Ostec, 2018).

2.6 SD-WAN y su uso como red WAN híbrida e inteligente

Las empresas que todavía utilizan la WAN convencional y tienen la demanda de una gran cantidad de tráfico de datos, pueden verse obligadas a adquirir más de un enlace de comunicación para evitar cuellos de botella, producto del abundante uso de información y también aplicar medidas de contingencia, en caso de que el enlace principal sufra alguna caída.

SD-WAN se utiliza para crear o simular redes WAN híbridas e inteligentes que puede incluir una VPN IP para empresas, servicios de banda ancha e inalámbricos. SD-WAN monitorea los enlaces disponibles y conoce las exigencias de cada aplicación, puede entonces elegir el mejor camino para enviar el tráfico de determinada aplicación en ese momento.

Con la incorporación de SD-WAN es factible usar enlaces de comunicación redundantes, administrados automáticamente por la aplicación, es decir, la posibilidad de caídas y fallas en la comunicación es casi nula. Si se está realizando una video llamada, y por ejemplo uno de los enlaces se queda sin conexión, el software automáticamente cambia al servicio más adecuado, como un circuito inalámbrico 4G, sin que esta llamada tenga interferencias. De esta forma el usuario obtiene un balanceo automático de la carga de trabajo, generando mayor desempeño y menor costo de enrutamiento.

Las funcionalidades de la SD-WAN están dando como resultado:

- ✓ reducción de costos,
- ✓ más eficiencia y productividad.

SD-WAN, a más de facilitar y automatizar la administración de la red, brinda a los clientes la oportunidad de tomar medidas para el futuro, soportando mayor tráfico de datos, más seguridad y colaborando para el desarrollo de toda la red y los nuevos avances tecnológicos.

2.7 Definición de PBR (Policy Based Routing)

Las grandes empresas requieren que sus redes IP, tengan facilidades para implementar enrutamientos en función de sus requerimientos y necesidades, que no están contempladas dentro de los aspectos técnicos de encaminamiento para transmitir datos.

Los operadores de la red pueden crear políticas que determinen selectivamente que cierta parte del tráfico deba ser enviado por unas rutas específicas y que otro parte del tráfico sea enviado por otras trayectorias o utilicen caminos diferentes.

El PBR permite etiquetar los paquetes y así distinguir los distintos tipos de tráfico, lo que facilitará la gestión del transporte de la información (Generar confianza, 2018).

2.7.1 Enrutamiento basado en políticas (PBR)

El funcionamiento normal de un router es que cuando recibe un paquete de información debe reenviarlo en función de la dirección IP de destino, a fin de poder comparar ésta con su tabla de enrutamiento.

El PBR o el enrutamiento selectivo está basado en función de las directrices y políticas prestablecidas por la empresa o por el gerente de esta.

2.7.2 Beneficios de implementar PBR

Entre los beneficios más importantes de implementar PBR se destacan:

- Selección de proveedor de internet que utiliza PBR para enrutamiento de tráfico.
- Calidad de Servicio (QoS).
- Balanceo de carga en función de las características del tráfico.

PBR permite al administrador de la red seleccionar el tráfico, haciendo uso de listas de acceso con la finalidad de fijar los valores IP precedentes, esto conlleva a etiquetar los paquetes de información en función de una clasificación establecida.

La clasificación de tráfico permite al administrador determinar diversos tipos de tráfico con permisibilidad de servicios en el entorno de la red e implementar calidad del servicio en el CORE utilizando técnicas de encolado.

2.7.3 Aplicaciones de PBR

Esta técnica permite a los routers dejar pasar a los paquetes por unos filtros llamados mapas de ruta, los cuales son reenviados al siguiente router.

2.8 Mapas de ruta

Las listas de acceso de una entrada son declaradas en un mapa de ruta, el cual contiene los siguientes elementos:

- Sentencias de comprobación definidas para determinados paquetes según la política de condición dada por el administrador.
- Sentencias de acción que se cumplen luego de la de comprobación donde el paquete de información será enrutado a su destino.

Todas las sentencias de comprobación y acción definidas en un mapa de rutas se deben cumplir, primero de comprobación para que posteriormente se apliquen las de acción en el paquete de información (Cisco, 2008).

2.8.1 Selección dinámica de ruta

SD-WAN mejora la calidad del servicio al permitir que el tráfico sea redirigido hacia otras trayectorias o rutas de respaldo operadas con tecnologías WAN.
El mejoramiento de asignación de rutas y uso de ancho de banda se implementan en la ficha Supervisión para mostrar los flujos de tráfico. Por ejemplo, cuando una ruta virtual está sirviendo a una conexión de red y si ésta se vuelve inactiva, se elige una nueva mejor trayectoria y la inicial se convierte en la última mejor ruta. Este

escenario se implementa cuando la demanda de ancho de banda es menor y cuando solo se elige un enlace.

Cuando es necesario implementar más enlaces para cursar tráfico con diferentes demandas de ancho de banda, se debe seleccionar más de una ruta virtual que pueda ser utilizada para proteger a una conexión de red, es ahí cuando SD-WAN analiza entre sus rutas disponibles, primero la mejor ruta en ese momento, luego a la siguiente y así sucesivamente.

Normalmente según la tasa de tráfico entrante que hace uso exigente de ancho de banda, se necesitarán una o más rutas para procesar y proteger el envío y recepción de información.

Para determinar cómo se realiza la asignación de rutas, se ve a continuación los siguientes escenarios:

- **Transmisión equilibrada de carga**

Se cumple cuando todas las rutas están operativas, permitiendo de esa manera seleccionar la mejor, teniendo como premisa que la demanda de ancho de banda de ese camino es suficiente para ser atendida por una ruta.

- **Transmisión duplicada**

La duplicación de transmisión de paquetes asegura que se tomen primero dos rutas para procesar paquetes de la misma conexión, a fin de garantizar una entrega confiable duplicando los paquetes en dos trayectorias independientes. Cuando se aplica el concepto de asignación de rutas, se toman en cuenta dos de la tabla de flujo, siempre y cuando exista la disponibilidad para procesar flujos duplicados.

- **Transmisión de ruta persistente**

La transmisión de ruta persistente consiste en retener paquetes de un flujo de información que está en función de la impedancia de la latencia de ruta (Purdy, 2016).

2.9 Beneficios de SD-WAN

Actualmente las empresas y organizaciones requieren que sus redes tengan los siguientes aspectos:

- Más económicas
- Flexibles, adaptables a sus necesidades.

Con el análisis de estos requerimientos se puede ahondar en los beneficios de SD-WAN:

a. Es bastante económica: Las redes SD-WAN son considerablemente más económicas que las redes privadas MPLS.

b. Son seguras: SD-WAN se fundamenta en el uso de Internet, utilizando redes privadas basadas en IPSec (Internet Protocol security) o DMVPN (Dynamic Multipoint VPN), incrementando de esta manera el nivel de seguridad para proteger los datos procesados en Internet.

c. Optimización del ancho de banda: SD-WAN administra sin ningún inconveniente el uso del ancho de banda. Lo cual implica que las empresas pueden agregar más enlaces a su red, sin que sea necesario realizar cambios en la infraestructura de ésta.

d. Son flexibles en el diseño del "underlay": es flexible para configurar la red underlay (García, 2018). Es decir:

- Se puede usar el ancho de banda más apropiado tomando en cuenta la ubicación del lugar de trabajo.
- Es posible asignar distintos tipos de enlaces a tráficos diferentes en función de los requerimientos de seguridad que necesita la empresa.
- En caso de pérdida de uno de sus enlaces, el sistema quedará garantizado por el respaldo underlay.

Esta flexibilidad permite entre otros aspectos facilitar y cubrir la alta demanda, operar los sistemas de gestión, programar los mantenimientos, gestionar los sistemas de seguridad, etc.

e. Son de fácil instalación: No requiere los servicios de ingenieros de campo. La configuración de equipos de oficina en redes SD-WAN puede hacerse remotamente o a través de equipos configurados con anterioridad. Este sistema elimina las

instalaciones tradicionales ya que a través de comandos es posible activar los módulos mediante la red LAN, proporcionando las siguientes ventajas (García, 2018)**:**

- La reducción de gastos, los dispositivos pueden cambiarse de ubicación sin utilizar técnicos (García, 2018).
- La implementación es automática, por lo cual disminuye la probabilidad de error y la intervención de técnicos en sitio (García, 2018).
- Las instalaciones son más rápidas y confiables**.**

f. Es Simplificada y fácil la configuración de la red: SD-WAN permite modificar, actualizar y agregar más aplicaciones en la red. Es decir, que puede gestionarse fácilmente y de manera centralizada en su totalidad.

g. Pueden gestionar las aplicaciones: Una de las ventajas de SD-WAN consiste en gestionar el tráfico desde un sitio determinado y pueden participar en la capa 7 del modelo OSI (aplicaciones), lo cual permite a los administradores configurar o gestionar la red sin necesidad de bajarse a nivel IP. Actualmente las aplicaciones son la base de muchas empresas, las cuales se almacenan en la nube pública.

h. Optimiza el rendimiento de las aplicaciones: las aplicaciones SD-WAN no requieren enviarse a su matriz u oficina central. Es decir, se puede administrar directamente las aplicaciones, lo cual implica un incremento en su rendimiento y a su vez permite usar funciones de calidad de servicio, priorizando las aplicaciones más importantes con el fin de optimizar el tiempo de respuesta (García, 2018).

2.10 Visibilidad y gestión centralizada.

Para determinar la mejor ruta en función del estado de cada enlace, SD-WAN usa diversos algoritmos en función del mejor camino y otros parámetros como pérdida o saturación de enlace, intermitencias y calidad de servicio.

Es necesario tener visibilidad de todo el enlace (desde el origen al final) para la entrega de aplicaciones y datos con el fin de poder localizar, analizar y corregir con exactitud las incidencias de interrupciones (Kesavan, 2016).

2.11 Calidad de servicio garantizada

SD-WAN proporciona un alto nivel de calidad de servicio y flexibilidad a un costo mucho menor que una solución WAN estática. Actualmente los nuevos servicios y aplicaciones se están expandiendo con mayor volumen y rapidez, lo que conlleva a que la garantía de servicio sea cada vez más exigente. Es por ello que calidad del servicio SD-WAN está garantizada a través de redes híbridas y varios proveedores.

El servicio de datos normalmente abarca múltiples proveedores, anchos de banda, elementos físicos y virtuales, niveles de rendimiento, clases de servicio, fiabilidad de la red, interrupciones y fallas relacionadas con fenómenos atmosféricos e incluso eventos multitudinarios que afectan el tráfico de datos que fluyen por la red.

Los operadores de red deben ser capaces de visualizar, monitorizar y gestionar el servicio completo, de extremo a extremo, a fin de asegurar la calidad del servicio de datos y analizar en profundidad porque un servicio falla. El aseguramiento de servicios unificados permite a los proveedores de servicio ver cómo y dónde radican los problemas que afectan la experiencia del cliente y no sólo determinar qué dispositivo, fabricado por un proveedor en particular, está teniendo problemas en un sector particular de la red.

Por ejemplo, si hay mucha intermitencia en un enlace de fibra óptica. Los administradores de la SD-WAN pueden ver sin ningún problema, qué enlace de ésta se encuentra con dificultades y a su vez que clientes se encuentra afectados, a fin de redirigir el tráfico por otras rutas que los usuarios reporten convenientes con su servicio (Purdy, 2016).

2.12 Segmentación de redes.

En las redes SD-WAN, cada cliente tiene diversas necesidades, por ello el tráfico debe gestionarse de forma individual, teniendo como prioridad la no afectación de los otros enlaces que la conforman.

Al segmentar la red se producen unidades aisladas, similares a una privada en cada fracción, entonces lo que ocurre en una parte no perturba a las otras. Permitiendo de esta manera bloquear de forma contralada un posible ataque o virus que afecte a la red (Esnoz, 2019).

Figura 2.8: Segmentación de la Red SDWAN
Fuente: (Purdy, 2016)

2.13 Ventajas de SD-WAN vs MPLS

Ambas tecnologías tienen un papel que jugar en las redes WAN modernas. SD-WAN es la aplicación de conceptos de redes SDN a la WAN. Esto significa la implementación de dispositivos que soportan SD-WAN, que se configura bajo parámetros y políticas de una estructura organizacional de una empresa para enviar tráfico por la mejor ruta.

SD-WAN puede enrutar diferentes tipos de tráficos, como MPLS y otros, debido a que puede superponer el transporte de forma independiente. La principal ventaja de SD-WAN es que un administrador del tráfico WAN, puede aplicar sin dificultad las disposiciones y políticas de la empresa a todos los dispositivos WAN.

A diferencia de la tecnología SD-WAN, para realizar un cambio en la red MPLS, las rutas deberán estar aprovisionadas con todo lo necesario para su correcto funcionamiento.

Cuando una red MPLS es implementada, garantiza un rendimiento óptimo para el transporte del tráfico en tiempo real. Mientras que SD-WAN enruta el tráfico por la ruta óptima, con la particularidad de que, al llegar la información a internet, éste puede presentar dificultades que no dependerán del proveedor del servicio (Weinberg & Till, 2018).

2.14 Diferencias entre SD-WAN y MPLS

Una de las principales diferencias es que el costo del ancho de banda de las redes MPLS e alto, ya que consiste en adquirir un servicio a través de un operador, mientras que redes como SD-WAN son más económicas ya que envían tráfico a través de Internet.

MPLS suele considerarse segura, pero al no proporcionar cifrado se vuelve insegura. En cambio, SD-WAN, al estar alojada en Internet, aumenta considerablemente su seguridad.

La capacidad del ancho de banda de MPLS actualmente se ve congestionada ya que los usuarios tienen necesidades de información de contenido multimedia. Esto no sucede con SD-WAN debido a que posee una capacidad de ancho de banda bastante considerable y óptima (Lucas, 2020).

Capítulo 3: Diseño y Simulación de una red de accesos utilizando la tecnología SD-WAN

En el capítulo 3 se muestra todos los requerimientos y pasos a seguir para la implementación de la simulación de una Red de Accesos utilizando la tecnología SD-WAN, y se indicará los recursos necesarios que permitan realizar un correcto análisis e implementación de esta tecnología.

Para lograr simular el diseño de una Red de accesos utilizando la tecnología de SD-WAN, se requiere usar un software que permita implementar y configurar equipos con rutas principales y de respaldo, así como la configuración de permisos y privilegios de accesos a internet u otros terminales, por este motivo para el desarrollo de este trabajo de investigación se utilizará el simulador GNS3.

3.1 GNS3

GNS3 es un software que permite simular, diseñar y construir topologías o escenarios de red en un ambiente controlado previo a una implementación, lo que permitirá realizar configuraciones a la red sin poner en peligro a la que se encuentre en operación. Este software, al ser una herramienta de simulación avanzada, permite la simulación de una red de accesos utilizando tecnología SD-WAN.

Figura 3.1: GNS3
Fuente: (GNS3, 2017)

Para la instalación del software GNS3 en una computadora se debe considerar los aspectos que muestra la tabla 3.1.

Tabla 3.1: Requerimientos Mínimos GNS3

equerimientos Mínimos	
Sistema Operativo	Windows 7 (64 bit) o posterior, Mavericks (10.9) o posterior, Cualquier distribución de Linux - Debian/Ubuntu son soportadas
Procesador	2 o más núcleos lógicos - AMD-V / RVI Series o Intel VT-X / EPT - con extensiones de virtualización habilitadas en la BIOS.
Memoria	4 GB RAM
Almacenamiento	1 GB available space (Windows Installation is < 200MB
Notas Adicionales	Se requiere almacenamiento adicional para las imágenes de los equipos.

Fuente: (GNS3, 2017)

Los recursos de simulación están en función de la topología de red a implementar, en este trabajo de simulación se recomiendan los requerimientos de la tabla 3.2 para su correcto funcionamiento.

Tabla 3.2: Requerimientos Mínimos para el funcionamiento del proyecto en GNS3

Requerimientos Recomendados	
Sistema Operativo	Windows 7 (64 bit) o posterior, Mavericks (10.9) o posterior, Cualquier distribución de Linux - Debian/Ubuntu son soportadas
Procesador	4 o más núcleos lógicos - AMD-V / RVI Series o Intel VT-X / EPT - con extensiones de virtualización habilitadas en la BIOS.
Memoria	16 GB RAM
Almacenamiento	SSD - 50 GB de espacio disponible
Notas Adicionales	RAM hasta 32 GB y procesador i7 o equivalente para uso óptimo.

Fuente: Autor

3.2 Diseño y Simulación de una Red de Accesos

En este trabajo de investigación se propone a la empresa de telecomunicaciones CONSTELEC la simulación de la migración de la red de accesos actual a una con tecnología SD-WAN. Esta empresa se encarga del diseño, instalación y soporte de redes de Fibra Óptica. Actualmente todas sus oficinas de administración, bodegas y operaciones se encuentran centralizadas en la ciudad de Guayaquil y próximamente se tiene previsto la apertura de las sucursales en Quito, Cuenca y Machala para lo cual se requerirá la contratación de los servicios de telecomunicaciones en todas las ciudades.

CONSTELEC por ser una empresa que brinda soporte técnico 24/7, tiene implementado en su red un enlace de internet fijo de respaldo que en muchas ocasiones les ha presentado intermitencias, latencias y falta total del servicio, consecuentemente se han quedado sin comunicación y sin el servicio de soporte técnico para el cual fueron contratados, por tal motivo el requerimiento principal a considerarse en las nuevas sucursales es tener enlaces redundantes y administrables que garanticen una comunicación continua.

En atención a dichos requerimientos del cliente, la solución más óptima, segura y menos costosa es que todos sus servicios migren a una red de accesos con tecnología SD-WAN. Para el diseño de la cual es necesario que el proveedor de servicios esté dotado de equipos que soporten esta tecnología, por tal motivo en este proyecto se utilizará equipos Fortigate de la marca Fortinet tanto en la matriz como en las sucursales.

En la tabla 3.3 se indican los equipos a ser utilizados en la simulación del proyecto y la función que cumplen cada uno de ellos en la Red de Accesos.

Tabla 3.3: Equipos utilizados en GNS3

EQUIPO	HOSTNAME	FUNCIONALIDAD
FORTIGATE	CONSTELEC MATRIZ	Equipo para configurar la tecnología SD-WAN
SWITCH LAN	LAN	Switch interno de la empresa
Servidor	DMZ	Equipos que maneja su base de datos de datos (DATACENTER)
PCs	192.168.X.X	Hosts de la empresa
WAN	WAN-INTERNET	RED del proveedor de servicios

Fuente: Autor

3.3 Topología de la RED

- ✓ **Red actual CONSTELEC**

En el siguiente grafico se muestra el diagrama actual de la red de accesos de CONSTELEC (Figura 3.2).

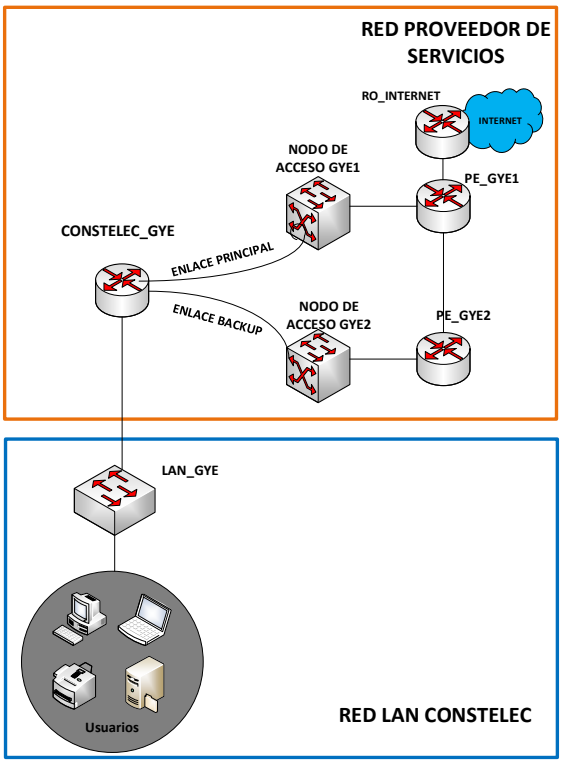


Figura 3.2: Red Actual CONSTELEC
Fuente: autor

- ✓ **Red Propuesta de CONSTELEC**

En base a su crecimiento y necesidades la empresa CONSTELEC requiere que su red cumpla con los siguientes requerimientos:

GERENCIA:

- Acceso a la base de datos (DATACENTER)
- Acceso a comunicarse con el exterior de su red sin restricciones a través del Internet.
- Acceso a comunicación con las sucursales de Quito, Cuenca y Machala

ADMINISTRACION:

- Acceso a la base de datos (DATACENTER), pero no con gerencia técnica, Bodegas y las sucursales Quito, Cuenca y Machala
- Acceso a comunicarse con el exterior de su red sin restricciones a través de internet

BODEGA:

- Acceso a la base de datos y las sucursales Quito, Cuenca y Machala

- Acceso a comunicarse con el exterior de su red sin restricciones a través de internet

GERENCIA TECNICA:

- Acceso a la base de datos y las sucursales Quito, Cuenca y Machala
- Acceso a comunicarse con el exterior de su red sin restricciones a través del internet

SUCURSALES DE QUITO, MACHALA Y CUENCA

- Acceso a la base de datos y comunicación con las Gerencia técnica y Bodegas
- Acceso a comunicarse con el exterior de su red sin restricciones a través del internet

DATACENTER

- Servidor de datos

✓ **Diagrama de bloques de la configuración de la Red CONSTELEC a Implementarse**

A continuación, se muestra en bloques la configuración de la red a implementarse (Figura 3.3).

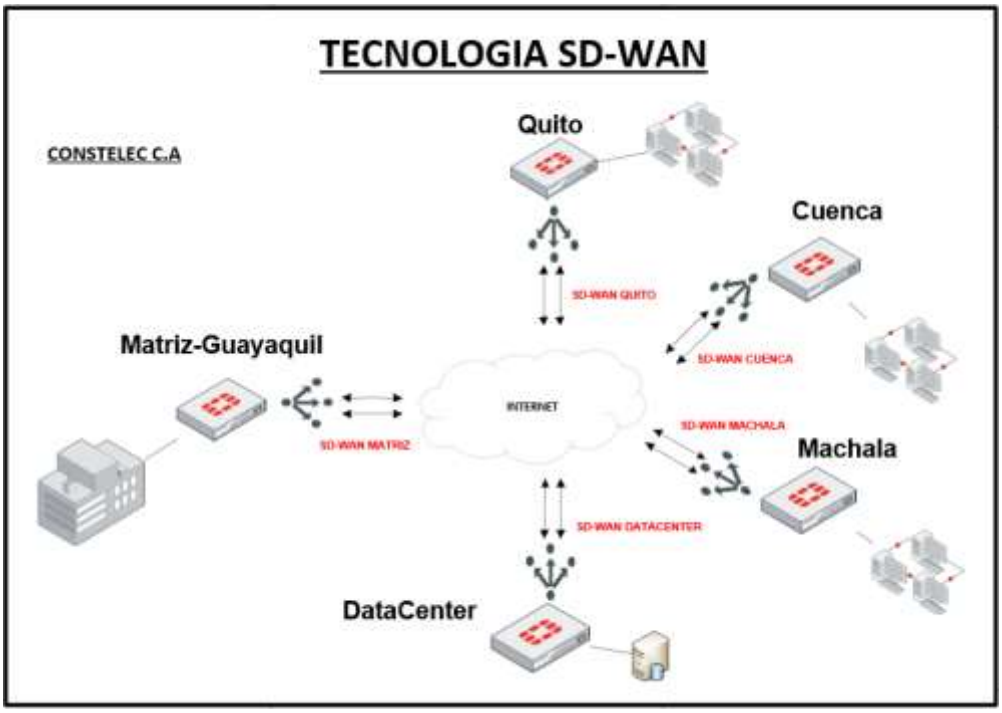


Figura 3.3: Red propuesta SD-WAN CONSTELEC
Fuente: autor

Como en cualquier red se empieza con la configuración de la red CONSTELEC, asignando las direcciones IP a las interfaces físicas WAN. En la tabla 3.4 se muestra el direccionamiento IP de las interfaces físicas WAN.

Tabla 3.4: Tabla de direccionamiento IP WAN

NOMBRE	WAN	IP	MASCARA	GATEWAY
SD-WAN MATRIZ	WAN-GYE1	10.100.1.1	255.255.255.0	10.100.1.254
	WAN-GYE2	10.100.2.1	255.255.255.0	10.100.2.254
SD-WAN QUITO	WAN-UIO1	10.100.3.1	255.255.255.0	10.100.3.254
	WAN-UIO2	10.100.4.1	255.255.255.0	10.100.4.254
SD-WAN CUENCA	WAN-CUE1	10.100.5.1	255.255.255.0	10.100.5.254
	WAN-CUE2	10.100.6.1	255.255.255.0	10.100.6.254
SD-WAN MACHALA	WAN-MCH1	10.100.7.1	255.255.255.0	10.100.7.254
	WAN-MCH2	10.100.8.1	255.255.255.0	10.100.8.254
SD-WAN DATACENTER	WAN-DC1	10.100.100.1	255.255.255.0	10.100.100.254
	WAN-DC2	10.100.200.1	255.255.255.0	10.100.200.254

Fuente: autor

Siguiendo con la configuración y en atención a los requerimientos del cliente, se presenta a continuación en forma gráfica (figura 3.4) las redes LAN a implementarse en la Matriz Guayaquil y en las Sucursales de Quito, Cuenca, Machala y DataCenter.

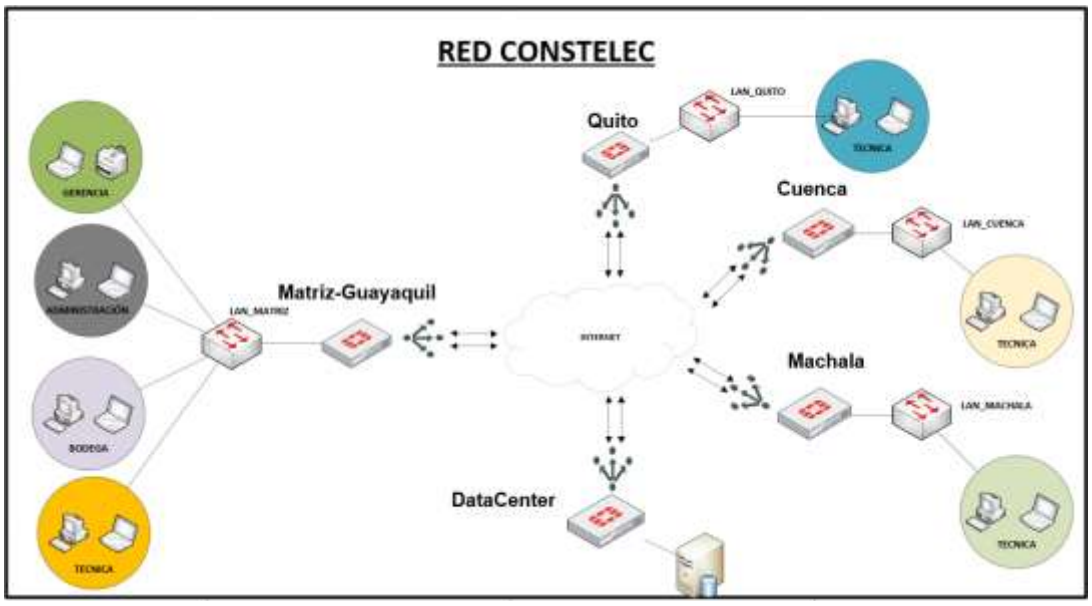


Figura 3.4: Red SD-WAN CONSTELEC
Fuente: autor

En la tabla 3.5 se muestran las direcciones IP de las Redes LAN de la Matriz y sucursales y Data center de la empresa CONSTELEC.

Tabla 3.5 Tabla de direccionamiento IP LAN

NOMBRE	LAN	RED	HOST	GATEWAY
MATRIZ-GUAYAQUIL	LAN_GERENCIA	192.168.1.0/24	192.168.1.1	192.168.1.254
			192.168.1.2	
	LAN_ADMINISTRACION	192.168.2.0/24	192.168.2.1	192.168.2.254
			192.168.2.2	
	LAN_BODEGA	192.168.3.0/24	192.168.3.1	192.168.3.254
			192.168.3.2	
	LAN_TECNICA	192.168.4.0/24	192.168.4.1	192.168.4.254
			192.168.4.2	
QUITO	LAN_QUITO	192.168.10.0/24	192.168.10.1	192.168.10.254
			192.168.10.2	
CUENCA	LAN_CUENCA	192.168.20.0/24	192.168.20.1	192.168.20.254
			192.168.20.2	
MACHALA	LAN_MACHALA	192.168.30.0/24	192.168.30.1	192.168.30.254
			192.168.30.2	
DATACENTER	SERVIDOR	50.50.50.0/24	50.50.50.50	50.50.50.254

Fuente: autor

En la figura 3.5 se presenta el diseño del proyecto en el simulador GNS3.

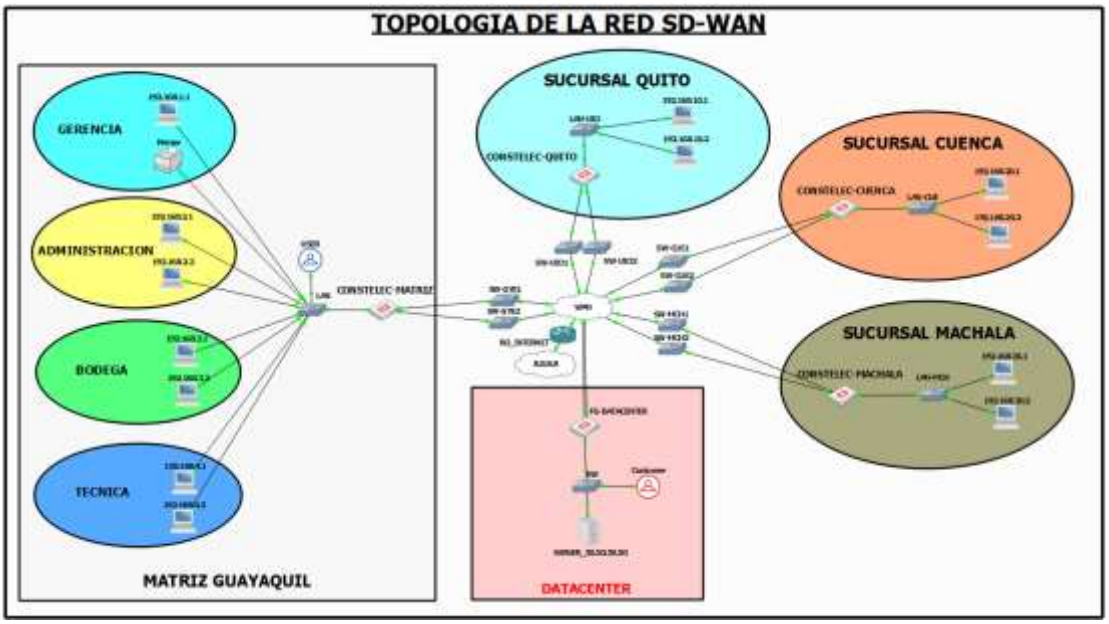


Figura 3.5: Red SD-WAN CONSTELEC en GNS3
Fuente: autor

3.4 Configuración SD-WAN

Como se indicó en el capítulo anterior las configuraciones SD-WAN se realizan solamente en el equipo Fortigate, las cuales podrán realzarse de manera gráfica o CLI.

Para continuar con la configuración de la tecnología SD-WAN se debe tener previamente establecidos y asignados los puertos de las interfaces WAN y LAN de CONSTELEC Matriz en el Fortigate como se indica en la figura 3.6.

```
CONSTELEC-MATRIZ # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.100.1.1 255.255.255.0
        set allowaccess ping https ssh http fgfm fabric
        set type physical
        set alias "WAN1"
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 10.100.2.1 255.255.255.0
        set allowaccess ping fabric
        set type physical
        set alias "WAN2"
        set role wan
        set snmp-index 2
```

```
edit "port5"
    set vdom "root"
    set ip 192.168.1.254 255.255.255.0
    set allowaccess ping https ssh http telnet fgfm fabric
    set type physical
    set alias "LAN_MATRIZ"
    set role lan
    set snmp-index 5
    set secondary-IP enable
    config secondaryip
        edit 1
            set ip 192.168.2.254 255.255.255.0
            set allowaccess ping fabric
        next
        edit 2
            set ip 192.168.3.254 255.255.255.0
            set allowaccess ping fabric
        next
        edit 3
            set ip 192.168.4.254 255.255.255.0
            set allowaccess ping fabric
```

Figura 3.6: Configuración Wan y Lan CONSTELEC Matriz
Fuente: autor

En la figura 3.7 se puede observar y comprobar la configuración y habilitación de la interfaz lógica SD-WAN MATRIZ, agrupando las interfaces físicas WAN1 y WAN2.

```
CONSTELEC-MATRIZ # show system virtual-wan-link
config system virtual-wan-link
    set status enable
    set load-balance-mode source-dest-ip-based
    config members
        edit 1
            set interface "port1"
            set gateway 10.100.1.254
        next
        edit 2
            set interface "port2"
            set gateway 10.100.2.254
```

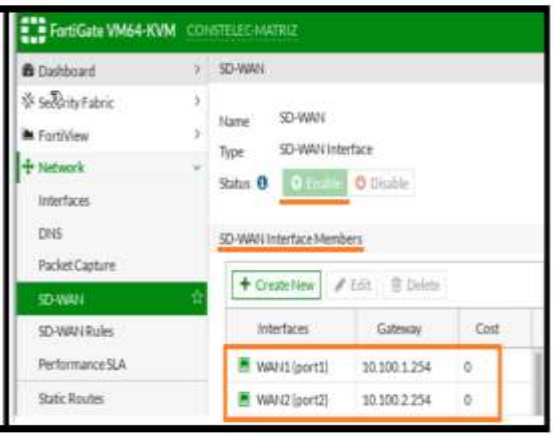


Figura 3.7: Configuración SD-WAN MATRIZ
Fuente: autor

Para que el tráfico proveniente de la red LAN de CONSTELEC-Matriz tenga salida a Internet, se deberá cumplir con los permisos y facilidades de enrutamiento que permite el Fortigate en base a políticas previamente establecidas por el usuario, las mismas que deberán ser dirigidas a la interfaz lógica SD-WAN CONSTELEC-Matriz, especificando las redes de origen y destino, en este caso el destino será all ya que es a Internet y el cual deberá estar el NAT habilitado para enmascarar las direcciones IP privadas en una dirección pública como se muestra en la figura 3.8.

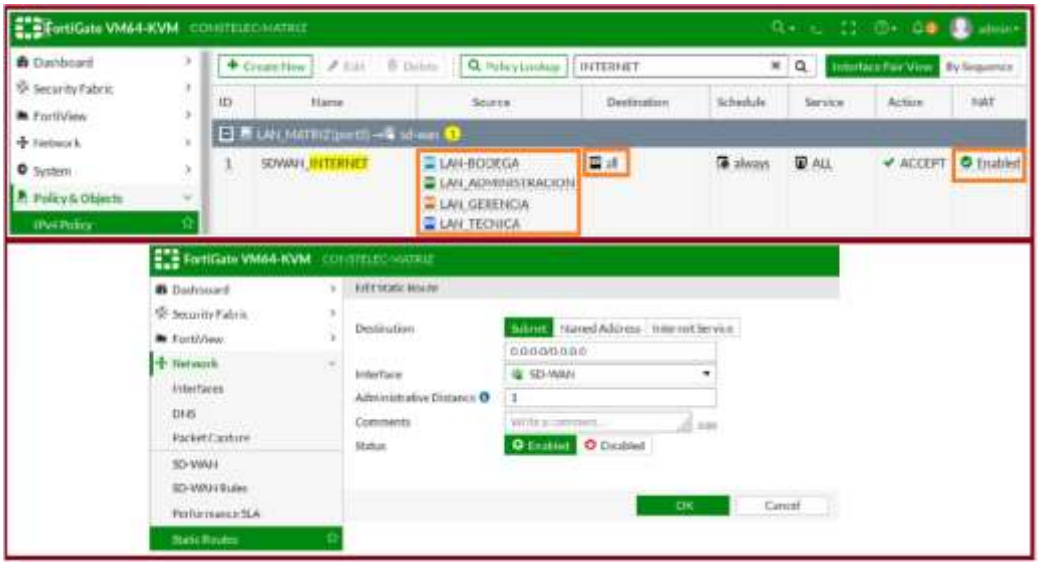


Figura 3.8: Políticas y enrutamiento de LAN_MATRIZ hacia SDWAN MATRIZ
Fuente: autor

A fin de mejorar el rendimiento del SD-WAN CONSTELEC-Matriz en función de la elección de la mejor ruta, se configurarán a continuación diversos parámetros basados en SLA, los cuales se muestran en la figura 3.9 hacia el servidor de Google, indicando el tiempo maximo de latencia para que dentro de ese rango funcionen de manera estable las interfaces de SD-WAN.

Luego de realizada la configuración se puede validar que en condiciones óptimas y sin afectaciones en el medio de transmisión, se obtendrán resultados de tiempos de latencia óptimos a internet entre 60ms a 120ms como se muestra en la figura 3.10.

- ✓ Latencia WAN1 (port1) 95.05ms
- ✓ Latencia WAN2 (port2) 105.19ms

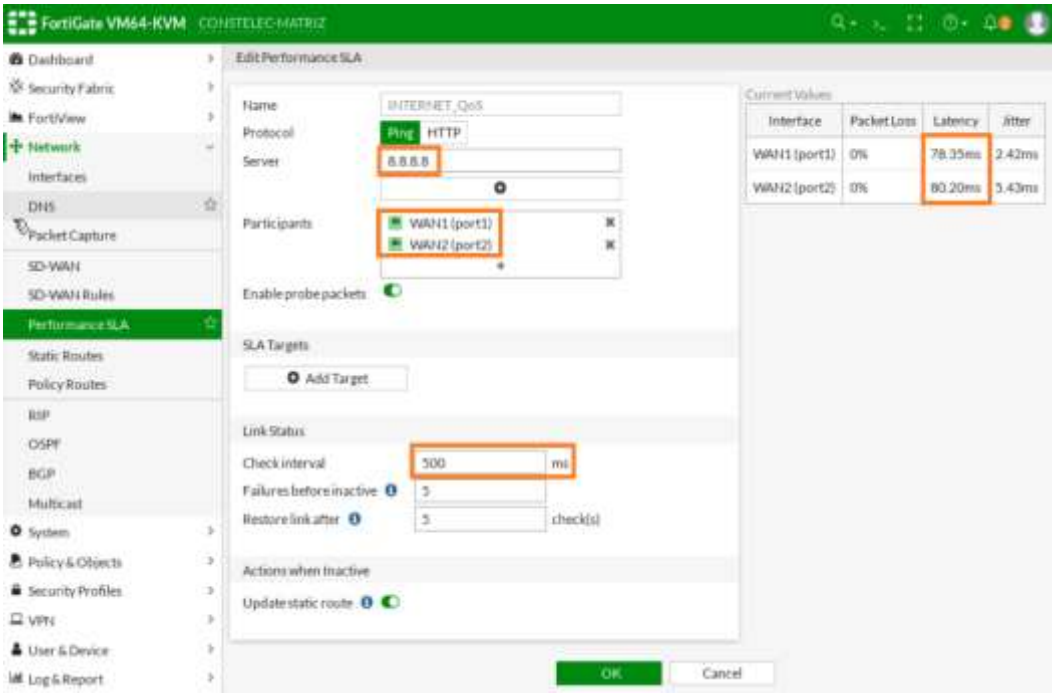


Figura 3.9: Parámetros de configuración del SLA de Internet en CONSTELEC Matriz
Fuente: autor

Figura 3.10: Performance SLA hacia Internet
Fuente: autor

En la figura 3.11 se muestra la configuración de la regla SD-WAN basada en el SLA configurado anteriormente, para que en el caso de que existiese afectación en el medio de transmisión, esta configuración permitirá elegir la mejor ruta a nivel WAN y de esta manera se logrará evitar el corte de tráfico.

Para verificar que el SD-WAN se encuentra cumpliendo con su función en forma óptima, se procede a revisar la tabla de enrutamiento, la misma que debera indicar que se están generando 2 rutas por defecto hacia los Gateway de los equipos de

borde del proveedor de servicios, y en la interfaz SD-WAN se deberá observar de manera gráfica el consumo de datos entrantes y salientes que están pasando por las interfaces fisicas involucradas (Figura 3.12).

Figura 3.11: Regla SD-WAN hacia Internet basado en SLA
Fuente: autor

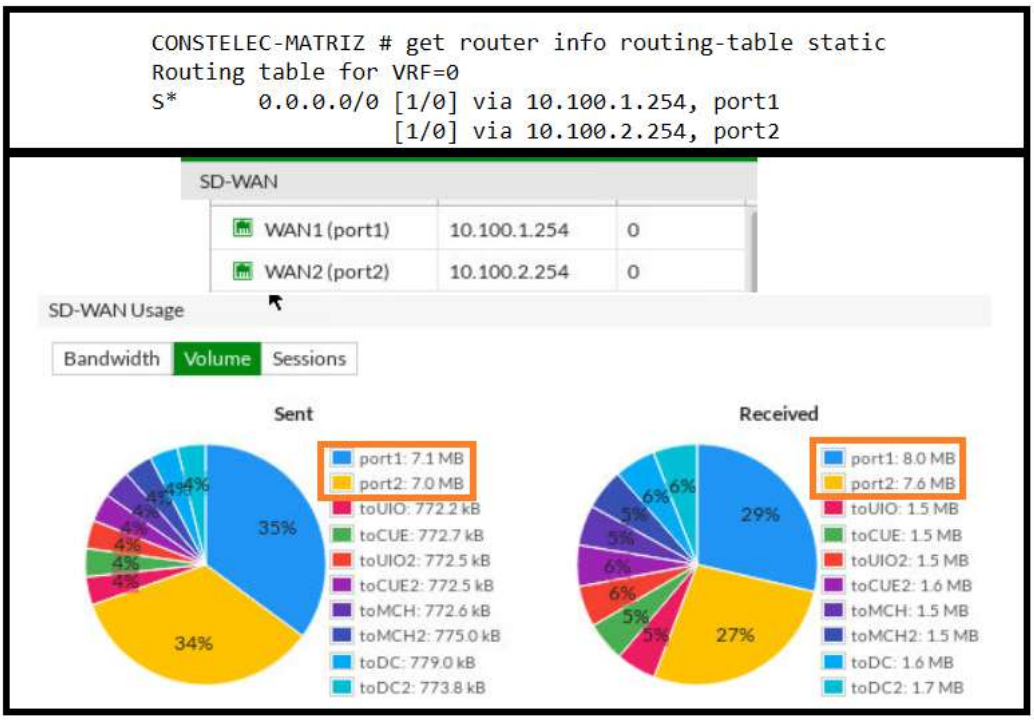


Figura 3.12: Consumo entrante y saliente de la Interfaz SD-WAN-MATRIZ
Fuente: autor

Las configuraciones de las sucursales de CONSTELEC en Quito, Cuenca y Machala se efectuarán de igual manera que la configuración realizada en el SD-WAN CONSTELEC-Matriz, teniendo en cuenta las propias redes WAN y LAN de cada una de las sucursales, cuyas rutas fueron propagadas hacia los equipos de Borde del proveedor de servicios, validando una vez más el funcionamiento del SD-WAN (Figura3.13).

```
CONSTELEC-QUITO # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.3.254, port1
                  [1/0] via 10.100.4.254, port2
```

```
CONSTELEC-MACHALA # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.7.254, port1
                  [1/0] via 10.100.8.254, port2
```

```
CONSTELEC-CUENCA # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.5.254, port1
                  [1/0] via 10.100.6.254, port2
```

```
DATACENTER # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.100.254, port1
                  [1/0] via 10.100.200.254, port2
```

Figura 3.13: Enrutamiento hacia el SD-WAN Sucursales
Fuente: autor

3.5 Comunicación entre redes de CONSTELEC a través de Internet

Debido a la necesidad que tiene la empresa de tener comunicaciones seguras y libres de ataques externos desde y hacia todas las sucursales. Se ha realizado la creación de túneles IPSEC a través de Internet, los cuales tienen una particularidad hoy en día de ser muy seguros y confiables, ya que los paquetes enviados o recibidos se transmiten protegidos o encriptados.

Para la creación de los Túneles IPSEC se toma como punto de referencia CONSTELEC-Matriz, quien será el origen de todos los túneles estáticos establecidos con las sucursales, para lograr esta configuración se crearán 2 túneles estáticos por cada sucursal, debido a que las mismas disponen de 2 enlaces de última milla.

Estos túneles IPSEC creados entre la matriz y sucursales serán encapsulados en la interfaz lógica SD-WAN de cada uno de los equipos Fortigate de CONSTELEC. Dicha topología se denomina HUB AND SPOKE con SD-WAN como se muestra en la figura 3.14, donde CONSTELEC matriz se encargará de receptar, direccionar y enrutar todos los paquetes enviados y recibidos de las sucursales.

Para lograr una comunicación entre sucursales se configurarán políticas, requerimientos, SLA y reglas en el SD-WAN de CONSTELEC matriz dando lugar a la formación automática de túneles dinámicos.

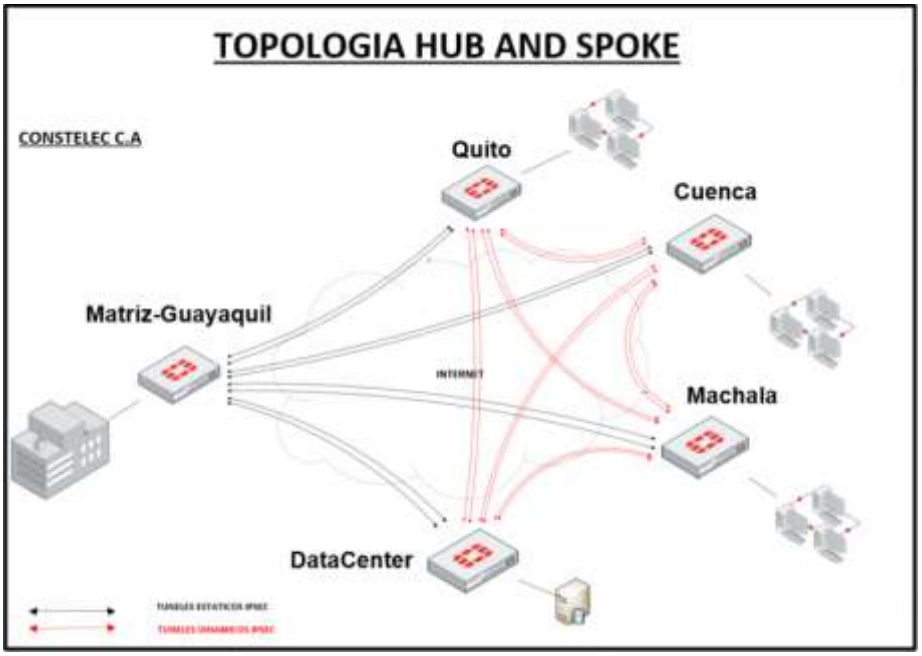


Figura 3.14: Topología HUB and SPOKE con SDWAN para la empresa CONSTELEC
Fuente: autor

✓ Configuración de Túneles IPSec

Para la configuración de los túneles IPSEC estáticos entre las interfaces Wan de CONSTELEC-Matriz. Sucursales y Data Center, se establecerá caminos directos entre ellas, con un nivel cifrado de seguridad en cada uno de los túneles como las que se indican en las figuras 3-15, 3-16, 3-17 y 3-18.

VPN IPSEC_MATRIZ				VPN IPSEC_QUITO			
NOMBRE	INTERFAZ	IP	IP REMOTA	NOMBRE	INTERFAZ	IP	IP REMOTA
MATRIZ-to-UIO	WAN 1	10.10.20.1	10.10.20.2	UIO-to-MATRIZ	WAN 1	10.10.20.2	10.10.20.1
MATRIZ-to-UIO	WAN 2	10.10.20.3	10.10.20.4	UIO2-to-MATRIZ	WAN 2	10.10.20.4	10.10.20.3

```
CONSTELEC-MATRIZ # config vpn ipsec phase1-interface
CONSTELEC-MATRIZ (phase1-interface) # sh
config vpn ipsec phase1-interface
    edit "touIO"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: touIO"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.3.1
        set psksecret ENC
+eAoc6htQD6lqYUbu231VGR7d3e9nFVJ
+iVYVDr9Ilks54JGzEfSgbepqTjns7SPJgWhpaePTeKwqT2VldT1
hmBUDE1rmSbZgW9VP3bz/2dLE3b6pBbopuF7/6m4eg13XDeHoxi6
42M7SZPjACdHwbOPO6MjgzHNfN9anV2xxwdN4l
+h7K/WWNLxsBwaerB4B4C6vg==
    next
    edit "touIO2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: touIO2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.4.1
        set psksecret ENC
tojilFyOPfTmDmmMJZiZWQEVF6B8PHTJBXbYQFMyJXovvrxXtt4P
B8MgNj3mWRDj6B+v5zR2YTEttRZH8h5
+keVUiLupgM5flTwfynEgfBd8I4vAGetXnqNKyUmOohgwyO8Q9TZ
bwWgIlVzwragKh6dpzbMWU7bCK0LG5+R0mLZ/P5lxUJYEwRnNmO
gtJBuQyoLtg==
```

```
CONSTELEC-QUITO # config vpn ipsec phase1-interface
CONSTELEC-QUITO (phase1-interface) # show
config vpn ipsec phase1-interface
    edit "toMATRIZ"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.1.1
        set psksecret ENC 5uQGf
+ATU4DkZBF7tS8YB/cyGsYqi3DkhLtCWPmiulU/JQ7yaLZuJH8W
y2VvUGXe6fMSgTEUVfkDCpaqHCM5C7E9DXIbPJDmst7Qg)
+WL48d8auFWBXucixo2V/LZ3zEhXLQ///WxL46d9JmIYHDeI72v
xSXdZ1fopOxEJevQThWCl/0sDuqrCUpdFF8JffXk38EE/w==
    next
    edit "toMATRIZ2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.2.1
        set psksecret ENC
3jXIogPKG6mxgRCWcPuKFXBqO1s3EK
+20fp1tomsF31wWMgE5HM4RU3rFlvADjkor9QZhgI6Zvj72e/0
XZQB1R0v8adVrJcoAQg2bfPfiMO2Z38vNog
+iwxXQIef7rMYnP6h3FFmqWQK0RmCwchFFxP0qjcXMJuwgfB
+N/H2RXfIKt7oGbPu2E4cA1p3sd8dnxkZw==
```

Figura 3.15: Túneles IPSec CONSTELEC MATRIZ-CONSTELEC QUITO
Fuente: autor

VPN IPSEC_MATRIZ				VPN IPSEC_CUENCA			
NOMBRE	INTERFAZ	IP	IP REMOTA	NOMBRE	INTERFAZ	IP	IP REMOTA
MATRIZ-to-CUE	WAN 1	10.10.30.1	10.10.30.2	CUE-to-MATRIZ	WAN 1	10.10.30.2	10.10.30.1
MATRIZ-to-CUE2	WAN 2	10.10.30.3	10.10.30.4	CUE2-to-MATRIZ	WAN 2	10.10.30.4	10.10.30.3

```
CONSTELEC-MATRIZ # config vpn ipsec phase1-interface
CONSTELEC-MATRIZ (phase1-interface) # sh
config vpn ipsec phase1-interface
    edit "toCUE"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toCUE"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.5.1
        set psksecret ENC
T2KRzxJTW7qlDLqPkFsPQmqcl9gfzpj3dClyC6qUT/mmqUnYOA6k
JwVNE5MIr+KCV1yoq2bshOhbZomKjYObmvUwPpdTDLcTU
+dx8GTG93WR462kXuTx8vU12QaHfk1mSqOrVFYBBObqwtG4a65U/
H7w1mB5A+MOdwRaUoUxF4A0uWWbI0T6FEojfHtfhaznFTv2Q==
    next
    edit "toCUE2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toCUE2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.6.1
        set psksecret ENC
dXh4jm8PyY2RP1mcXyQ8YW7QH0FfawHny
+chfvhuGjnBNj1rIrezkaNhrQeEUnMtra7iO4uFyasiAsqtMZPjh
aFWrnQJJZrCphR0k9ylxZay8VKQ1Nbv88b67EwhwKEPmYFfuIiIQ
ixLufjnLv5aptpGC1K4H7hPndd1eWVzFrMRuJTf8ZK/5jmcLti5K
SJ8TWgL7g==
gtJBuQyoLtg==
```

```
CONSTELEC-CUENCA # config vpn ipsec phase1-interface
CONSTELEC-CUENCA (phase1-interface) # show
config vpn ipsec phase1-interface
    edit "ToMatriz"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: ToMatriz"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.1.1
        set psksecret ENC gCrSEk9J3y
iUQ8d6Bt1SfCqEETYGJq280EQ1Aikpnww6/c99VY6ITi4tdji
+nWFHt0Bity4tNUlPmp+7bhza//+wf4eTBbxxJy
+ZRCeXapuT92LpifQVvr44Cx2kd5Cyp1kC
+miE1VknDpRjS9wTnYYwGac1UwCYtap64Pe3nHm3cjjqjHgwg0yJ
oe1DhAD2dKrrGg==
    next
    edit "toMatriz2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMatriz2 "
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.2.1
        set psksecret ENC
vY6iJsDtyCfW8Gk4yjTrK12qWZI36RC
+8S35ztGSh8k91G3Mhi0T
+JKR8NzNwFg5rHhtYSNloLMzwuMUpNVyxwMYT5KfFva7xwUKEY4t
TSVO8NhuktTIDoKMHH96PY62xdaiiE2NOg74z1xCmQ
+Qnnfj9nFUxPnpllZ2JdCM28H8o8v2/s5OpzFm8QJBu4uRZl5tQQ
==
```

Figura 3.16: Túneles IPSec CONSTELEC Matriz-CONSTELEC Cuenca
Fuente: autor

VPN IPSEC_MATRIZ				VPN IPSEC_MACHALA			
NOMBRE	INTERFAZ	IP	IP REMOTA	NOMBRE	INTERFAZ	IP	IP REMOTA
MATRIZ-to-MCH	WAN 1	10.10.40.1	10.10.40.2	MCH-to-MATRIZ	WAN 1	10.10.40.2	10.10.40.1
MATRIZ-to-MCH2	WAN 2	10.10.40.3	10.10.40.4	MCH2-to-MATRIZ	WAN 2	10.10.40.4	10.10.40.3

```
CONSTELEC-MATRIZ # config vpn ipsec phase1-interface
CONSTELEC-MATRIZ (phase1-interface) # sh
config vpn ipsec phase1-interface
    edit "toMCH"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMCH"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.7.1
        set psksecret ENC XUwkQ6v/PaxVpWFaOaiLb
+PhBXfNxGhdng0s9T7EtiQ9I0MxZC0kW
+ep/q8inMmpC50IHlEOPFUJH8ceVVeDs03UHjE+z
+BR9u3Lnll/RHP67gieaG9P9+LyOnS3kRh/pSuLj9KY8R7MFQffo
U/
+tBdFQfc/TsQEGtNJmbw3J6brAPuiSbcEVFo3e5IaODiImQJfBw=
=
    next
    edit "toMCH2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMCH2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.8.1
        set psksecret ENC di8EDjyMzVdrCI7W
+qfamV4JJMZre5Evwnzwjcv8YamxIhDNkHVpsqV1z7Ej1RsejF74
bbwOL1SyqKnQ0j56DYahFvoNVaASWsCNAQtBJg6LCmljc9r0HIgj
9UUlaHtlkVBnbLD9BvEW3G9rR63eUNqUb/bWmaDCUOGPiU9jUZZZ
hkZ+2r9GhcMr0hXEp5QeTjNZg==
```

```
CONSTELEC-MACHALA # config vpn ipsec phase1-interface
CONSTELEC-MACHALA (phase1-interface) # show
config vpn ipsec phase1-interface
    edit "toMATRIZ"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ (Created by VPN
wizard for SD-WAN)"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.1.1
        set psksecret ENC
YoryMkd1AyeDWxhFWFEi/jWARrzIY5tho75A0ZXSIZmcDywcGOxHD
yZRuIAdspmAYKfUn/uxcNlcmEa45MfH58Hu13u2u1V2hVPtMudW3h
YBLzO8Vdz
+l4sXa58q1SkH81+xAQfiyLiRxOMS9t1VDVi3YlriN5zx2D0BLEX6
U0u78wfmbRv/qrjdemRX9L0W1lJDgQ==
    next
    edit "toMATRIZ2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ2 (Created by VPN
wizard for SD-WAN)"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.2.1
        set psksecret ENC VHfUsw1iuv
+0JFx/9PUyegEZwcJkwpMiRqCfk8yuIBYm3PtGdVzcjPSU/2QR
+vswhOYj4ovmoGQdLzSKDqnVcTaNgS27aZxBDDmQwMQckW7wO2M9q
HOTyEUsyovnVdZHB24zksaHargjbuLDC9KwlCxo9BHdWCRpjnT7ju
3YqL9tbqk5vNYGh/Fxf5e5hll3A8cUyw==
```

Figura 3.17: Túneles IPSec CONSTELEC Matriz-CONSTELEC Machala
Fuente: autor

VPN IPSEC_MATRIZ				VPN IPSEC_DC			
NOMBRE	INTERFAZ	IP	IP REMOTA	NOMBRE	INTERFAZ	IP	IP REMOTA
MATRIZ-TO-DC	WAN 1	10.10.100.1	10.10.100.2	DC-TO-MATRIZ	WAN 1	10.10.100.2	10.10.100.1
MATRIZ-TO-DC2	WAN 2	10.10.100.3	10.10.100.4	DC2-TO-MATRIZ	WAN 2	10.10.100.4	10.10.100.3

```
CONSTELEC-MATRIZ # config vpn ipsec phase1-interface
CONSTELEC-MATRIZ (phase1-interface) # sh
config vpn ipsec phase1-interface
    edit "toDC"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toDC"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.100.1
        set psksecret ENC
zufAql0O6uMEDDJMT3+Io5pb8YgLlaYlPdU9GDauRKU
+77DpyvueOiLvIfiztB4UIKVCTY8SDb6Mf2HE9rJITF9fa1k/rxx
2YnndpnmyYbq30ZHvsXuf3TPFTemG2HiRRy5FgK9CNYMlpTmYFoJ
5Cvy0U0wVSEbKlXsipeGH9ULYHKTpRfdIOCXPanRASrHGQJ
+N4Q==
    next
    edit "toDC2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toDC2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.200.1
        set psksecret ENC
8+taZNt0GfwqyesHhyBVDyb2Y7GyXYubllhT/VXKYksN/aQyG
+FRatHy6g1fekxp/WC892PuGNBfgOO7h10b4SyAzxB1nzQgrEg0l
i2EW2cAmP3F4bCXfln6z5EmIc/1u9nbj/WXwffaqrs0rPNSuqhsn
OdFqTTRyAmxU/IRiZEGDa3c7dTddGq4PKuMLuw/EA3SdA==
```

```
DATACENTER # config vpn ipsec phase1-interface
DATACENTER (phase1-interface) # show
config vpn ipsec phase1-interface
    edit "toMATRIZ"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.1.1
        set psksecret ENC
LgQEcBZFMqZAQ1jFrJuLVY8jLmipP
+Z3Eelx1cpPM2C4b1iA/96bRMJDVhpKPWyj3v+Oz
+et3jE4HNonJuaCvy9QMM5ZP5Y0C8z0wHMBNU/BoBEORubFoDKHV
Qq/HJWbQLYyi0ozmUpcVPHjA2CI7d8AbMODcx1IDL0Bqf95XjdfA
NQO9p0lmT2wno22tmHBVVBpNQ==
    next
    edit "toMATRIZ2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN: toMATRIZ2"
        set wizard-type simplified-static-fortigate
        set remote-gw 10.100.2.1
        set psksecret ENC
Ut/ztZXIkL9wZPSu93HpFf9n1flfdbeASirwmQL
+7tgIGCoqOGhVwgGgo5FSKMiLstRoRahYI7OVMjfsR00rPXy0nJF
N3Y8EIBqn2a5bdIqRn7DAJmZMphFBem8TYLVNfR34PzQpkCCXbCo
Csy1vwAYykwtsPRWr1cE1xWMaTalFQWdq8FfhZ2qSBUJxX3tnP2Q
Ltw==
```

Figura 3.18: Túneles IPSec CONSTELEC Matriz-Datacenter
Fuente: autor

Después de establecer todos los túneles IPSec en la red de CONSTELEC, estos serán configurados en las interfaces SD-WAN correspondiente de cada Fortigate, con el fin de generar comunicación con las sucursales a través SD-WAN como se muestra en la figura 3.19.

```
CONSTELEC-MATRIZ # conf system virtual-wan-link
        edit 3
            set interface "toUIO"
            set gateway 10.10.20.2
        next
        edit 4
            set interface "toCUE"
            set gateway 10.10.30.2
        next
        edit 5
            set interface "toUIO2"
            set gateway 10.10.20.4
        next
        edit 6
            set interface "toCUE2"
            set gateway 10.10.30.4
        next
        edit 7
            set interface "toMCH"
            set gateway 10.10.40.2
        next
        edit 8
            set interface "toMCH2"
            set gateway 10.10.40.4
        next
        edit 9
            set interface "toDC"
            set gateway 10.10.100.2
        next
        edit 10
            set interface "toDC2"
            set gateway 10.10.100.4
```

```
CONSTELEC-QUITO # config system virtual-wan-link
        edit 3
            set interface "toMATRIZ"
            set gateway 10.10.20.1
        next
        edit 4
            set interface "toMATRIZ2"
            set gateway 10.10.20.3
```

```
CONSTELEC-CUENCA #config system virtual-wan-link
        edit 3
            set interface "ToMatriz"
            set gateway 10.10.30.1
        next
        edit 4
            set interface "toMatriz2"
            set gateway 10.10.30.3
```

```
CONSTELEC-MACHALA #config system virtual-wan-link
        edit 3
            set interface "toMATRIZ"
            set gateway 10.10.40.1
        next
        edit 4
            set interface "toMATRIZ2"
            set gateway 10.10.40.3
```

```
DATACENTER #config system virtual-wan-link
        edit 3
            set interface "toMATRIZ"
            set gateway 10.10.100.1
        next
        edit 4
            set interface "toMATRIZ2"
            set gateway 10.10.100.3
```

Figura 3.19: Configuración de los Túneles IPSEC CONSTELEC a las interfaces SD-WAN
Fuente: autor

3.6 Configuración de Loopbacks

La creación de Loopbacks en todos los equipos Fortigate de CONSTELEC (Figura 3.20) es fundamental, ya que a través de estos se podrá monitorear y supervisar la operatividad de los túneles IPSec tales como los tiempos de latencia, paquetes perdidos y jitter en tiempo real.

```
CONSTELEC-MATRIZ # sh system interface loopback
config system interface
    edit "loopback"
        set vdom "root"
        set ip 10.127.0.1 255.255.255.255
        set allowaccess ping
        set type loopback
        set alias "loopback"
        set role lan
        set snmp-index 12
```

```
CONSTELEC-MACHALA # sh system interface loopback
config system interface
    edit "loopback"
        set vdom "root"
        set ip 10.127.0.4 255.255.255.255
        set allowaccess ping
        set type loopback
        set alias "loopback"
        set role lan
        set snmp-index 12
```

```
CONSTELEC-QUITO # sh system interface loopback
config system interface
    edit "loopback"
        set vdom "root"
        set ip 10.127.0.2 255.255.255.255
        set allowaccess ping
        set type loopback
        set alias "loopback"
        set role lan
        set snmp-index 12
```

```
DATACENTER # sh system interface loopback
config system interface
    edit "loopback"
        set vdom "root"
        set ip 10.127.0.254 255.255.255.255
        set allowaccess ping
        set type loopback
        set alias "loopback"
        set role lan
        set snmp-index 12
```

```
CONSTELEC-CUENCA # sh system interface loopback
config system interface
    edit "loopback"
        set vdom "root"
        set ip 10.127.0.3 255.255.255.255
        set allowaccess ping
        set type loopback
        set alias "loopback"
        set role lan
        set snmp-index 12
```

Figura 3.20: Configuración de Loopbacks en los equipos Fortigate de CONSTELEC Y Datacenter
Fuente: autor

3.7 Configuración de SLA y Reglas en el SD-WAN para túneles IPSec

La configuración de SLA en los Tuneles IPSec estaticos de CONSTELEC matriz a sucursales y Datacenter, servirá para eligir automaticamente la mejor ruta de comunicación entre sus redes en base a lo antes indicado, como son los tiempos de latencia, paquetes perdidos y jitter en los túneles, para ilustrar de mejor manera esta configuracion de tuneles de Constelec Matriz a Sucursales y Datacenter. Ver figura 3.21

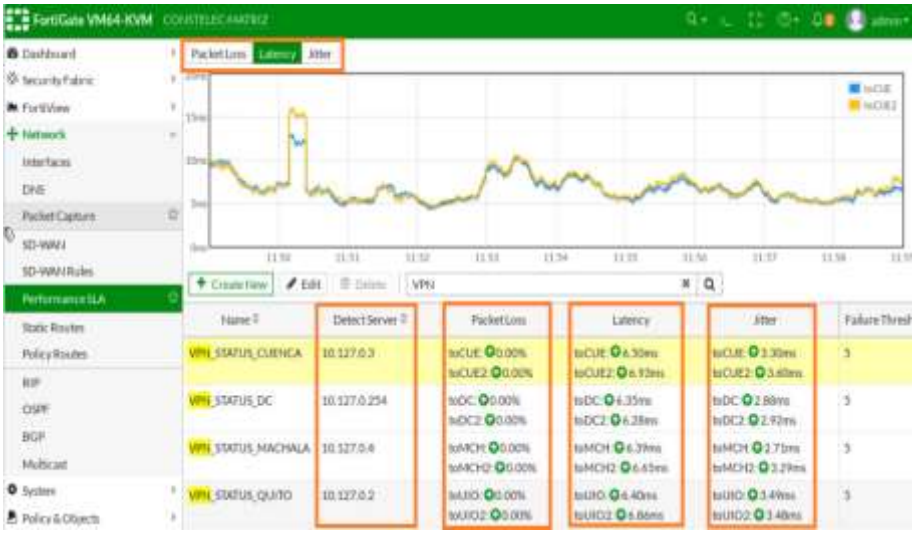


Figura 3.21: Performance SLA entre los Túneles IPSec Matriz a Sucursales
Fuente: autor

Para la configuración de las reglas SD-WAN referente a los tuneles IPSEC se definirán varios aspectos como son las redes de origen, destino y SLA, a fin de elegir la mejor ruta disponible. Cabe recalcar que las reglas creadas (recuadro naranja) para los tuneles IPSec, deberán estar por encima de la regla de Internet, ya que el Fortigate al momento de elegir dará prioridad a la primera regla de la cola de reglas creadas, de tal manera, que en caso de no caer en la regla correcta esta continuará con la siguiente y asi sucesivamente hasta encontrar la regla correspondiente. Por ejemplo, si la red de LAN_BODEGA requiere comunicase con la red SERVIDORES_DC, el Fortigate comenzará a leer desde la primera regla Quito_VPN_QoS, en caso de no ser la regla correcta este irá descartando una por una hasta llegar a la regla correcta, que en este caso será la regla DC_VPN_QoS donde se encuentra la red origen y destino.

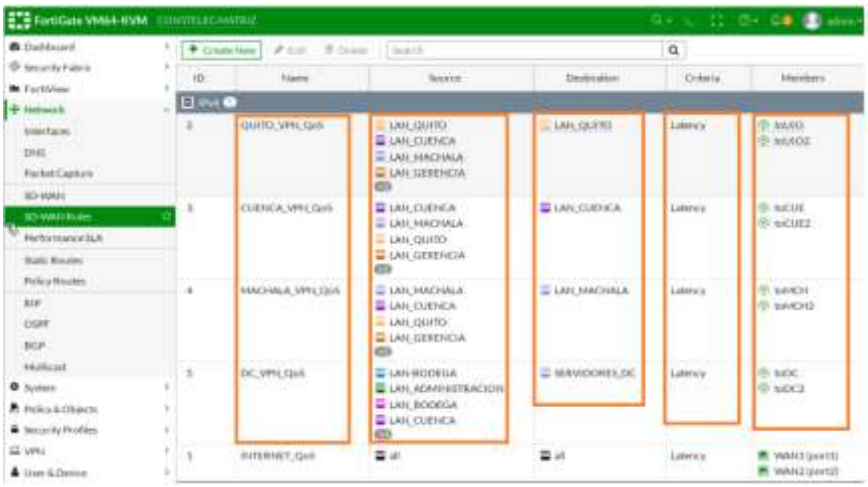


Figura 3.22: Reglas SD-WAN para túneles IPSec de CONSTELEC MATRIZ hacia las Sucursales basado en SLA
Fuente: autor

De igual manera como se realizó la configiración de los SLA y reglas en el SD-WAN para los tuneles IPSec estaticos en CONSTELEC-Matriz, estas serán replicadas en las sucursales y Datacenter .

A continuación se observa en las figuras 3.23, 3.24, 3.25 y 3.26 las configuraciones de SLA y reglas creadas en los Fortigate de las sucursales y Datacenter hacia CONSTELEC-matriz

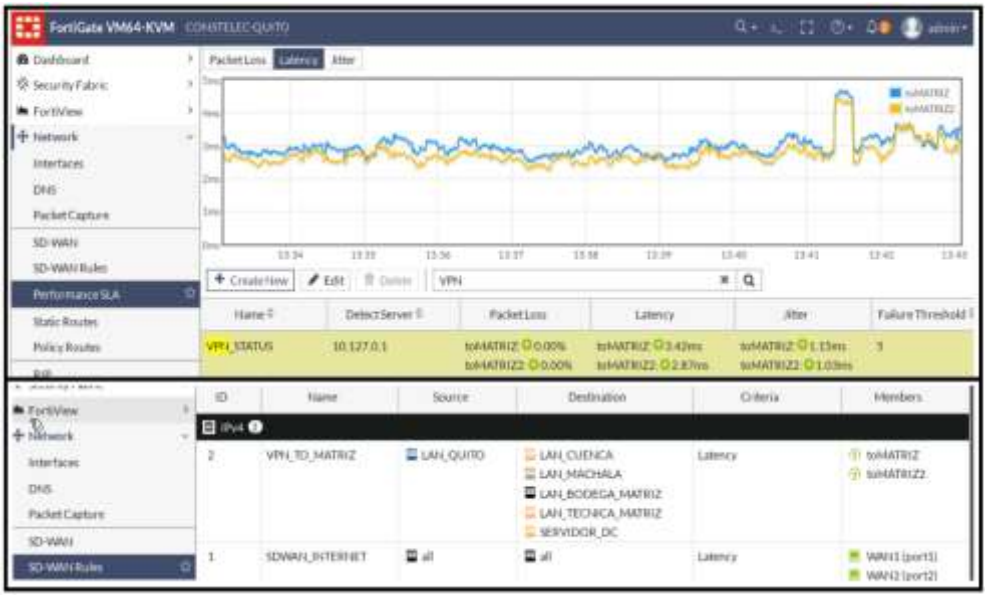


Figura 3.23: SLA y reglas entre los Túneles CONSTELEC Quito hacia Matriz
Fuente: autor

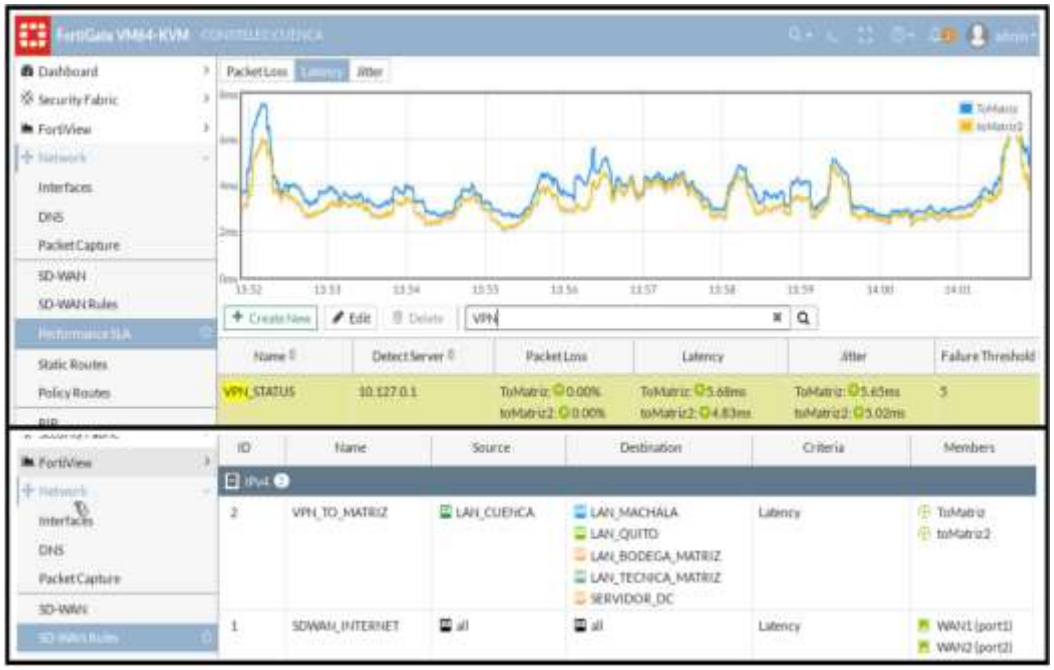


Figura 3.24: SLA y reglas entre los Túneles CONSTELEC Cuenca hacia Matriz
Fuente: autor

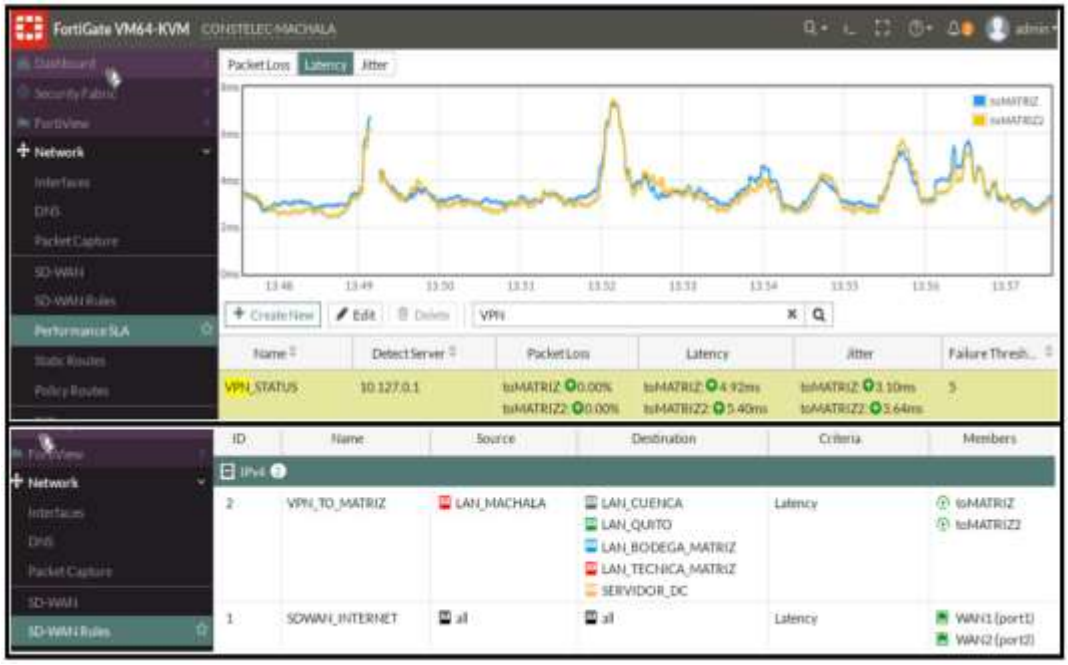


Figura 3.25: SLA y reglas entre los Túneles CONSTELEC Machala hacia Matriz
Fuente: autor

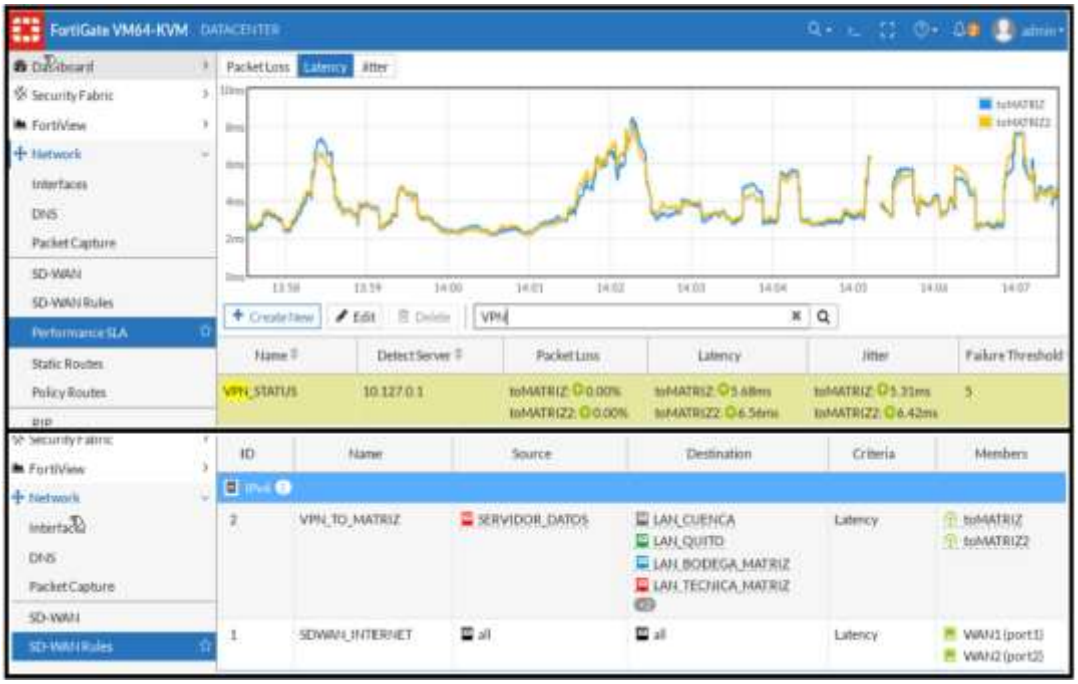


Figura 3.26: SLA y reglas entre los Túneles Datacenter hacia Matriz
Fuente: autor

3.8 Configuración BGP

A fin de propagar las redes LAN de CONSTELEC por el protocolo dinámico BGP a través de los túneles IPSec declarados, se establecerán sesiones BGP en los Fortigate de las Sucursales con el de matriz, el cual aprenderá dinámicamente todos los neighbors publicados en las sucursales. A continuación, se indican las

configuraciones BGP realizadas en los Fortigate de Matriz, Sucursales y Datacenter. ver figuras 3.27 y 3.28.

```
CONSTELEC-MATRIZ # config router bgp
CONSTELEC-MATRIZ (bgp) # show
config router bgp
    set as 65000
    set router-id 10.127.0.1
    config neighbor-group
        edit "remote-peers"
            set next-hop-self enable
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.0.0 255.255.0.0
            set neighbor-group "remote-peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.2.0 255.255.255.0
        next
        edit 3
            set prefix 192.168.3.0 255.255.255.0
        next
        edit 4
            set prefix 192.168.4.0 255.255.255.0
        next
        edit 6
            set prefix 10.127.0.1 255.255.255.255
```

Figura 3.27: Configuración BGP CONSTELEC MATRIZ
Fuente: autor

```
CONSTELEC-QUITO # config router bgp
CONSTELEC-QUITO (bgp) # sh
config router bgp
    set as 65000
    set router-id 10.127.0.2
    config neighbor
        edit "10.10.20.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "10.10.20.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.10.0 255.255.255.0
        next
        edit 2
            set prefix 10.127.0.2 255.255.255.255
```

```
CONSTELEC-CUENCA # config router bgp
CONSTELEC-CUENCA (bgp) # show
config router bgp
    set as 65000
    set router-id 10.127.0.3
    config neighbor
        edit "10.10.30.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "10.10.30.3"
            set next-hop-self enable
            set soft-reconfiguration enable

            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.20.0 255.255.255.0
        next
        edit 2
            set prefix 10.127.0.3 255.255.255.255
```

```
CONSTELEC-MACHALA # config router bgp
CONSTELEC-MACHALA (bgp) # show
config router bgp
    set as 65000
    set router-id 10.127.0.4
    config neighbor
        edit "10.10.40.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "10.10.40.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.30.0 255.255.255.0
        next
        edit 2
            set prefix 10.127.0.4 255.255.255.255
```

```
DATACENTER # config router bgp
DATACENTER (bgp) # show
config router bgp
    set as 65000
    set router-id 10.127.0.254
    config neighbor
        edit "10.10.100.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "10.10.100.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 50.50.50.0 255.255.255.0
        next
        edit 2
            set prefix 10.127.0.254 255.255.255.255
```

Figura 3.28: Configuración BGP Sucursales y Datacenter
Fuente: autor

- ✓ **Verificación de las sesiones BGP**

Luego de la configuración BGP realizada en los Fortigate de CONSTELEC se verificará en la matriz el estado de todos los neighbors, los cuales deberán encontrarse en estado UP como se indica a continuación.

```
CONSTELEC-MATRIZ # get router info bgp summary
BGP router identifier 10.127.0.1, local AS number 65000
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 34 seconds

Neighbor     V      AS    MsgRcvd   MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.10.20.2   4     65000      3         5         3      0    0    00:00:14        2
10.10.20.4   4     65000      3         4         2      0    0    00:00:15        2
10.10.30.2   4     65000      3         7         4      0    0    00:00:13        2
10.10.30.4   4     65000      3         5         3      0    0    00:00:14        2
10.10.40.2   4     65000      3         7         4      0    0    00:00:13        2
10.10.40.4   4     65000      3         5         3      0    0    00:00:14        2
10.10.100.2  4     65000      3         4         2      0    0    00:00:15        2
10.10.100.4  4     65000      3         3         1      0    0    00:00:16        2

Total, number of neighbors 8
```

- ✓ **Verificación de las rutas aprendidas por BGP**

A continuación, se puede observar todas las redes aprendidas por BGP en CONSTELEC-Matriz, las mismas que fueron publicadas desde las Sucursales y Datacenter (Redes Lan, Loopbacks, Servidor-DC).

```
CONSTELEC-MATRIZ # get router info routing-table bgp
Routing table for VRF=0
B       10.127.0.2/32 [200/0] via 10.10.20.2, toUIO, 03:19:10
B       10.127.0.3/32 [200/0] via 10.10.30.2, toCUE, 03:00:39
B       10.127.0.4/32 [200/0] via 10.10.40.2, toMCH, 03:19:09
B       10.127.0.254/32 [200/0] via 10.10.100.2, toDC, 03:19:11
B       50.50.50.0/24 [200/0] via 10.10.100.2, toDC, 03:19:11
B       192.168.10.0/24 [200/0] via 10.10.20.2, toUIO, 03:19:10
B       192.168.20.0/24 [200/0] via 10.10.30.2, toCUE, 03:00:39
B       192.168.30.0/24 [200/0] via 10.10.40.2, toMCH, 03:19:09
```

3.9 Configuración de Políticas en el Fortigate

Para permitir el paso del tráfico de las redes LAN y que estas puedan comunicarse entre sí, ya sea LAN-matriz a LAN-sucursales o LAN-sucursal a LAN-sucursal, se

configuró políticas en el Fortigate especificando todas las redes LAN de CONSTELEC.

A continuación, se detallan las políticas creadas en cada Fortigate.

- ✓ **CONSTELEC Matriz**

En la figura 3.29 se puede observar las políticas creadas para los túneles IPSec, especificando las redes de origen y destino, no será necesario tener habilitado el NAT ya que estas no tendrán permiso de navegación a través de Internet.

- La política VPN_SUCURSALES permite que todas las redes LAN de matriz tengan conexión hacia las redes LAN de las sucursales.
- La política VPN_TO_MATRIZ permite a todas las redes LAN de las sucursales tener conexión hacia la LAN de matriz.
- La política SUCURSALES_TO_SUCURSALES se encargará de crear los túneles IPSec dinámicos entre las sucursales y puedan tener conexión a través de matriz. Dicha política solo deberá ser creada en matriz.

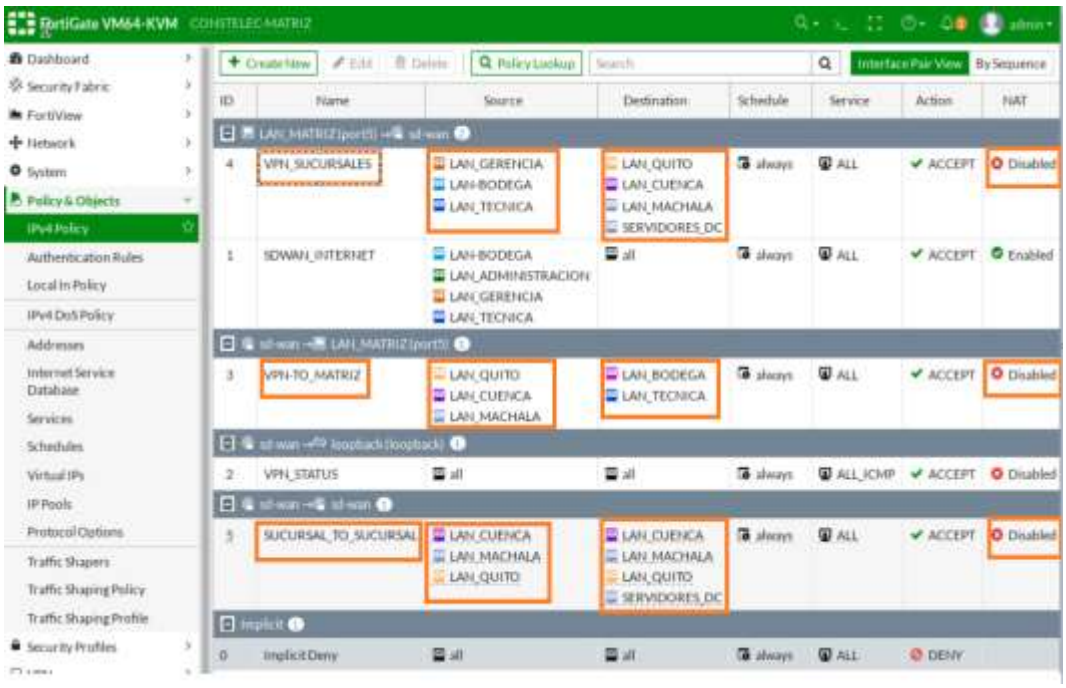


Figura 3.29: Políticas para el tráfico entrante y saliente de los túneles IPSEC Matriz
Fuente: autor

En las figuras 3.30, 3.31, 3.32 y 3.33 se pueden observar las políticas creadas para los túneles de CONSTELEC sucursales y Datacenter.

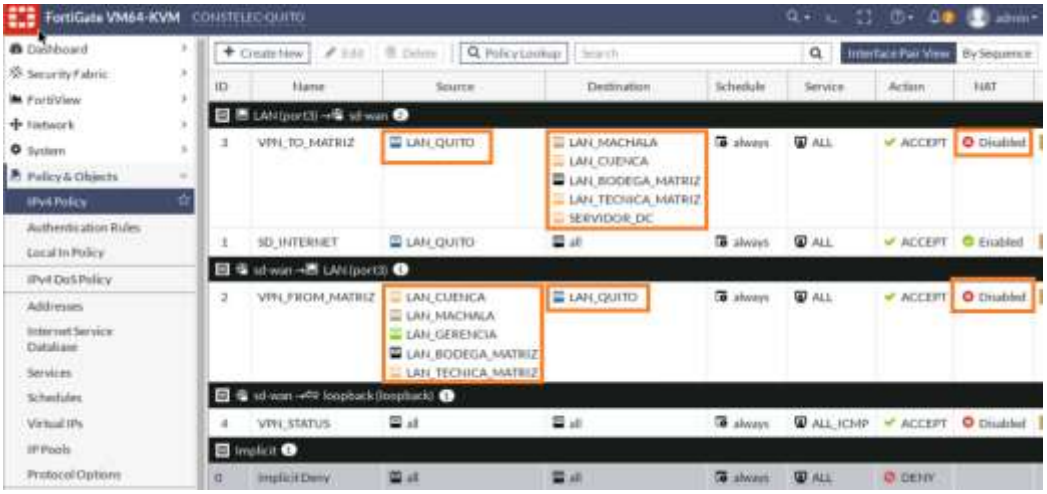


Figura 3.30: Políticas para el tráfico entrante y saliente de los túneles IPSec QUITO
Fuente: autor

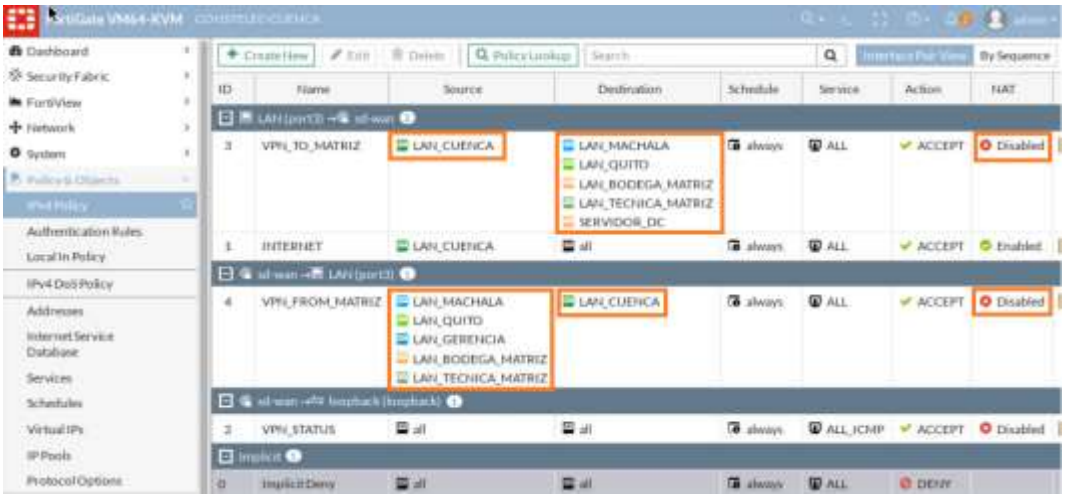


Figura 3.31: Políticas para el tráfico entrante y saliente de los túneles IPSec Cuenca
Fuente: autor

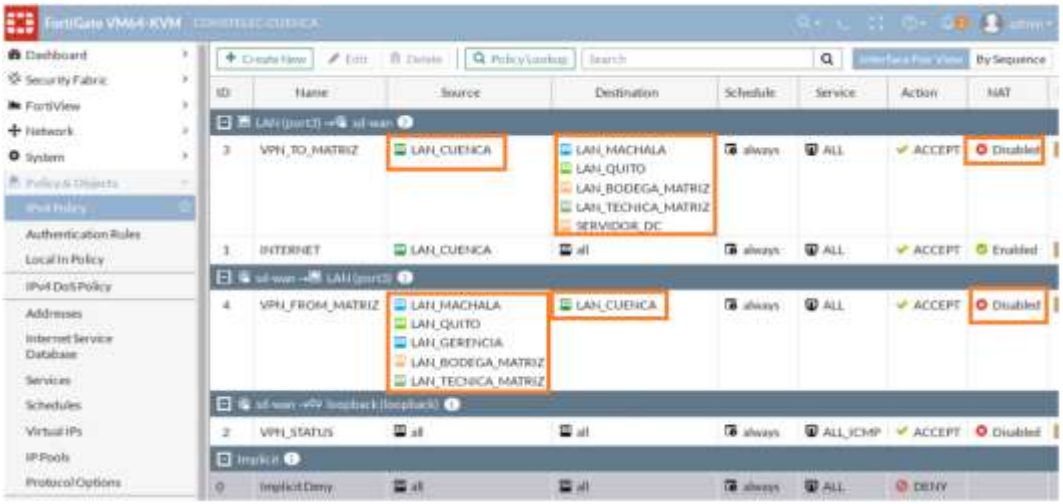


Figura 3.32: Políticas para el tráfico entrante y saliente de los túneles IPSec Machala
Fuente: autor

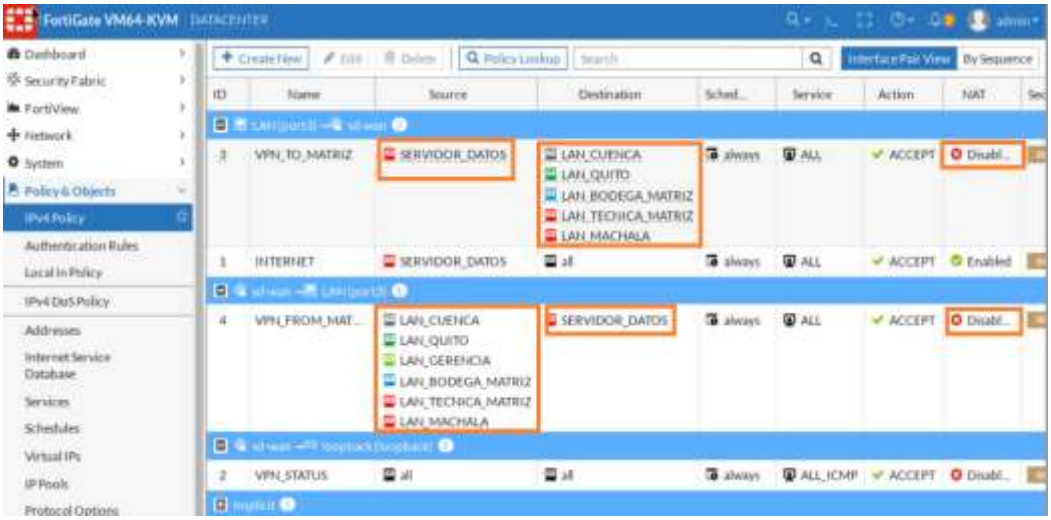


Figura 3.33: Políticas para el tráfico entrante y saliente de los túneles IPSec Datacenter
Fuente: autor

3.10 Conectividad a Internet desde los Hosts

Para realizar estas pruebas se verifican que todos los hosts de los segmentos de la red Lan CONSTELEC tengan conectividad a Internet como se muestra en las figuras 3.34 y 3.35. Con ello se validarán que las reglas y políticas especificadas en las figuras 3.8 y 3.11 han sido aplicadas correctamente para el SD-WAN.

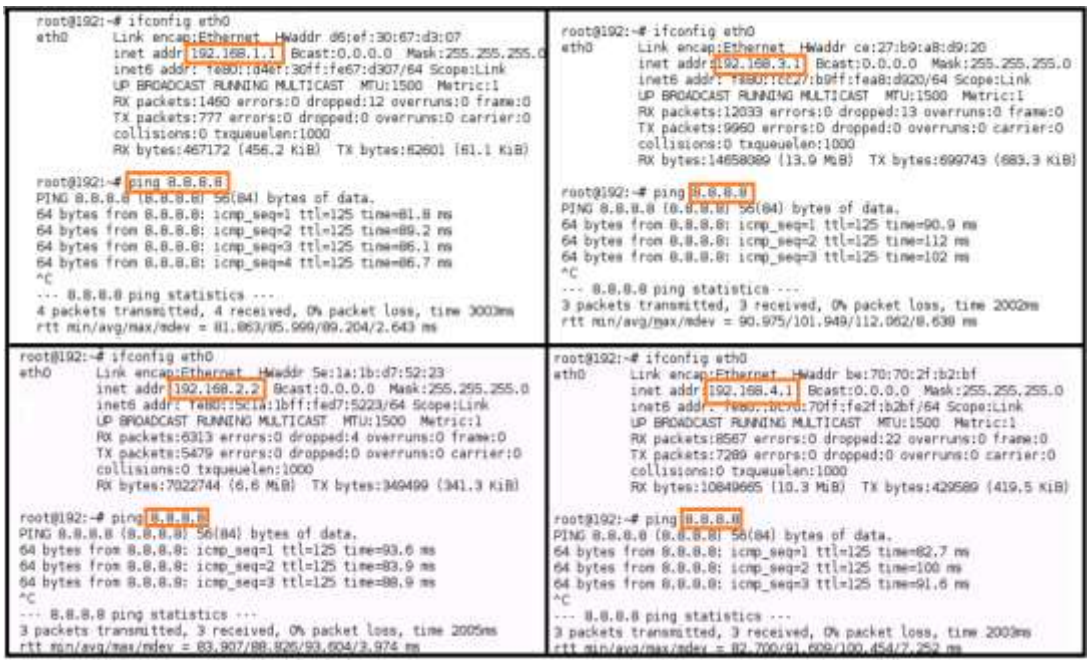


Figura 3.34: Conectividad a Internet desde la red Lan Matriz
Fuente: autor

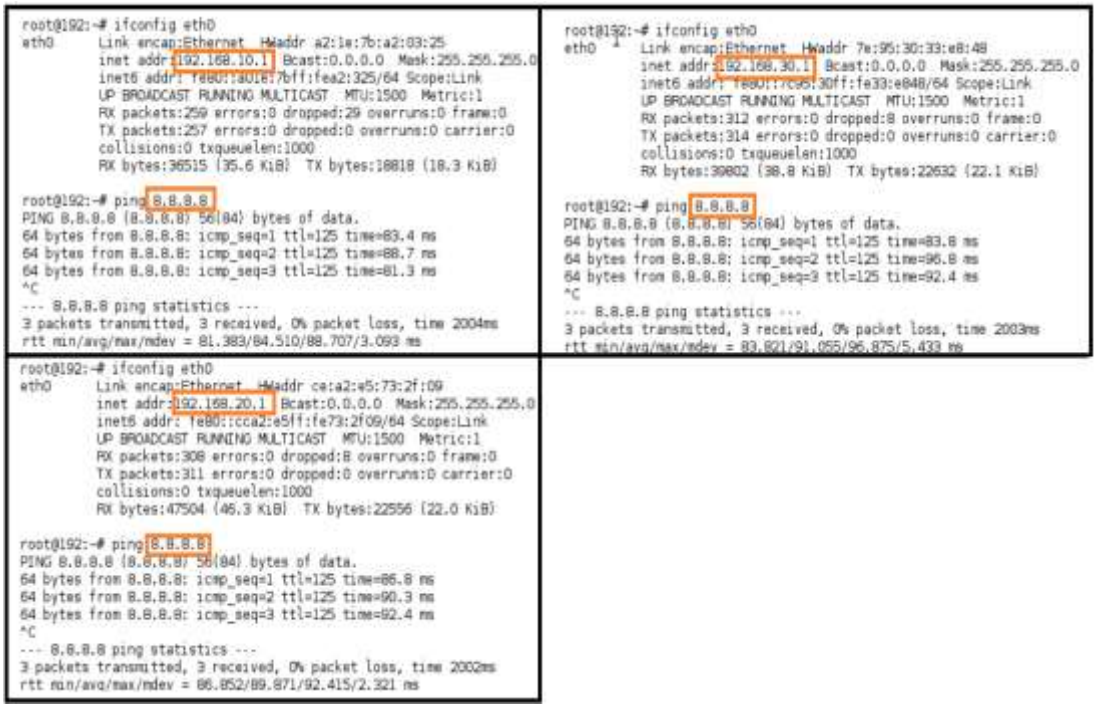


Figura 3.35: Conectividad a Internet desde la red Lan Sucursales
Fuente: autor

3.11 Pruebas de Conectividad por los Túneles IPSEC

A fin de comprobar los requerimientos y permisos de comunicaciones entre las redes LAN de CONSTELEC se procederá a realizar pruebas de Lan a Lan como las que se muestran en las figuras 3.36, 3.37, 3.38, 3.39, 3.40, 3.41 y 3.42.

- ✓ **Lan Gerencia**

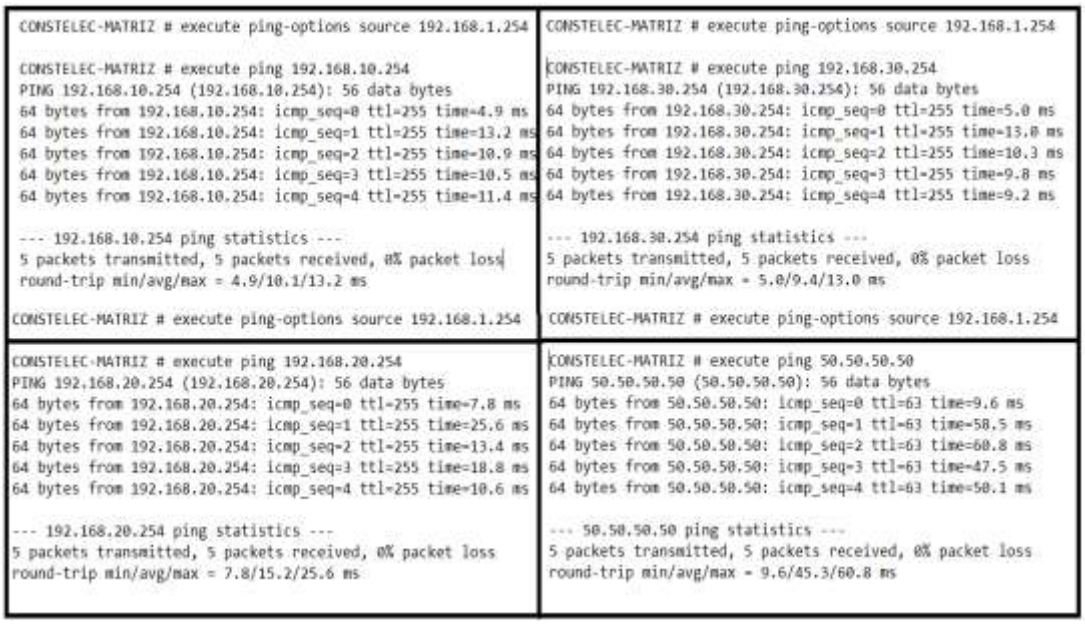


Figura 3.36: Conectividad a puntos remotos desde la red Lan Gerencia
Fuente: autor

✓ Lan Administración

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.2.254

CONSTELEC-MATRIZ # execute ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254): 56 data bytes

--- 192.168.10.254 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.2.254

CONSTELEC-MATRIZ # execute ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254): 56 data bytes

--- 192.168.20.254 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.2.254

CONSTELEC-MATRIZ # execute ping 192.168.30.254
PING 192.168.30.254 (192.168.30.254): 56 data bytes

--- 192.168.30.254 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.2.254

CONSTELEC-MATRIZ # execute ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: icmp_seq=0 ttl=63 time=17.4 ms
64 bytes from 50.50.50.50: icmp_seq=1 ttl=63 time=25.1 ms
64 bytes from 50.50.50.50: icmp_seq=2 ttl=63 time=34.4 ms
64 bytes from 50.50.50.50: icmp_seq=3 ttl=63 time=111.8 ms
64 bytes from 50.50.50.50: icmp_seq=4 ttl=63 time=13.9 ms

--- 50.50.50.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 13.9/40.5/111.8 ms
```

Figura 3.37: Conectividad a puntos remotos desde la red Lan Administración
Fuente: autor

✓ Lan Bodega

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.1.254

CONSTELEC-MATRIZ # execute ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254): 56 data bytes
64 bytes from 192.168.10.254: icmp_seq=0 ttl=255 time=10.3 ms
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=25.9 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=34.3 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=24.5 ms
64 bytes from 192.168.10.254: icmp_seq=4 ttl=255 time=33.4 ms

--- 192.168.10.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.3/25.6/34.3 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.1.254

CONSTELEC-MATRIZ # execute ping 192.168.30.254
PING 192.168.30.254 (192.168.30.254): 56 data bytes
64 bytes from 192.168.30.254: icmp_seq=0 ttl=255 time=8.3 ms
64 bytes from 192.168.30.254: icmp_seq=1 ttl=255 time=32.2 ms
64 bytes from 192.168.30.254: icmp_seq=2 ttl=255 time=58.1 ms
64 bytes from 192.168.30.254: icmp_seq=3 ttl=255 time=29.3 ms
64 bytes from 192.168.30.254: icmp_seq=4 ttl=255 time=13.8 ms

--- 192.168.30.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 8.3/28.3/58.1 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.3.254

CONSTELEC-MATRIZ # execute ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254): 56 data bytes
64 bytes from 192.168.20.254: icmp_seq=0 ttl=255 time=13.8 ms
64 bytes from 192.168.20.254: icmp_seq=1 ttl=255 time=48.8 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=255 time=21.5 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=255 time=64.7 ms
64 bytes from 192.168.20.254: icmp_seq=4 ttl=255 time=15.3 ms

--- 192.168.20.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 13.8/32.8/64.7 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.3.254

CONSTELEC-MATRIZ # execute ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: icmp_seq=0 ttl=63 time=13.9 ms
64 bytes from 50.50.50.50: icmp_seq=1 ttl=63 time=32.3 ms
64 bytes from 50.50.50.50: icmp_seq=2 ttl=63 time=62.9 ms
64 bytes from 50.50.50.50: icmp_seq=3 ttl=63 time=17.8 ms
64 bytes from 50.50.50.50: icmp_seq=4 ttl=63 time=26.4 ms

--- 50.50.50.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 13.9/30.6/62.9 ms
```

Figura 3.38: Conectividad a puntos remotos desde la red Lan Bodega
Fuente: autor

✓ Lan Técnica

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.4.254

CONSTELEC-MATRIZ # execute ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254): 56 data bytes
64 bytes from 192.168.10.254: icmp_seq=0 ttl=255 time=4.7 ms
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=41.1 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=65.8 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=47.4 ms
64 bytes from 192.168.10.254: icmp_seq=4 ttl=255 time=36.4 ms

--- 192.168.10.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.7/35.0/47.4 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.4.254

CONSTELEC-MATRIZ # execute ping 192.168.30.254
PING 192.168.30.254 (192.168.30.254): 56 data bytes
64 bytes from 192.168.30.254: icmp_seq=0 ttl=255 time=12.5 ms
64 bytes from 192.168.30.254: icmp_seq=1 ttl=255 time=6.7 ms
64 bytes from 192.168.30.254: icmp_seq=2 ttl=255 time=28.8 ms
64 bytes from 192.168.30.254: icmp_seq=3 ttl=255 time=7.0 ms
64 bytes from 192.168.30.254: icmp_seq=4 ttl=255 time=25.2 ms

--- 192.168.30.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 6.7/15.2/25.2 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.4.254

CONSTELEC-MATRIZ # execute ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254): 56 data bytes
64 bytes from 192.168.20.254: icmp_seq=0 ttl=255 time=23.5 ms
64 bytes from 192.168.20.254: icmp_seq=1 ttl=255 time=12.5 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=255 time=62.7 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=255 time=64.3 ms
64 bytes from 192.168.20.254: icmp_seq=4 ttl=255 time=17.3 ms

--- 192.168.20.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 12.5/40.0/64.3 ms
```

```
CONSTELEC-MATRIZ # execute ping-options source 192.168.4.254

CONSTELEC-MATRIZ # execute ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: icmp_seq=0 ttl=63 time=11.8 ms
64 bytes from 50.50.50.50: icmp_seq=1 ttl=63 time=18.2 ms
64 bytes from 50.50.50.50: icmp_seq=2 ttl=63 time=18.2 ms
64 bytes from 50.50.50.50: icmp_seq=3 ttl=63 time=16.9 ms
64 bytes from 50.50.50.50: icmp_seq=4 ttl=63 time=17.0 ms

--- 50.50.50.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 11.8/16.8/18.2 ms
```

Figura 3.39: Conectividad a puntos remotos desde la red Lan Técnica
Fuente: autor

✓ Lan Quito

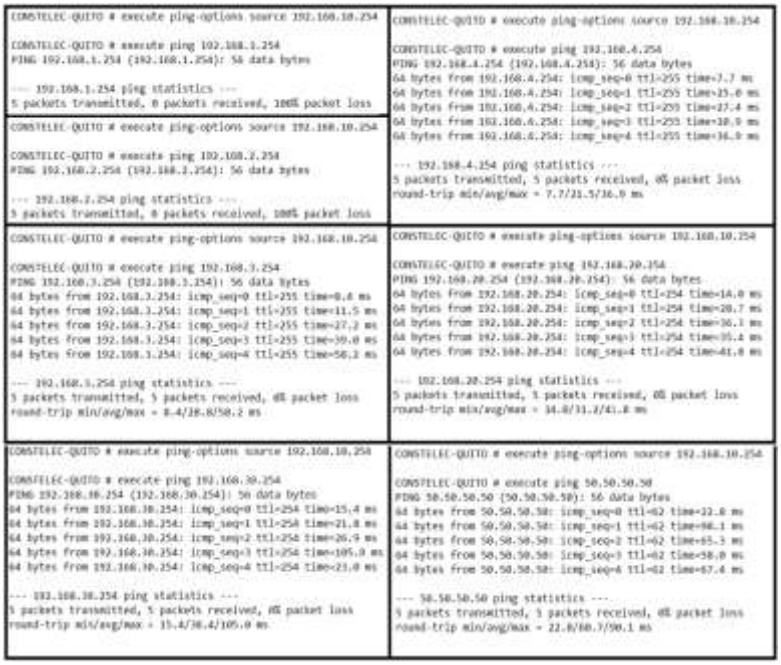


Figura 3.40: Conectividad a puntos remotos desde la red Lan Quito
Fuente: autor

✓ Lan Cuenca

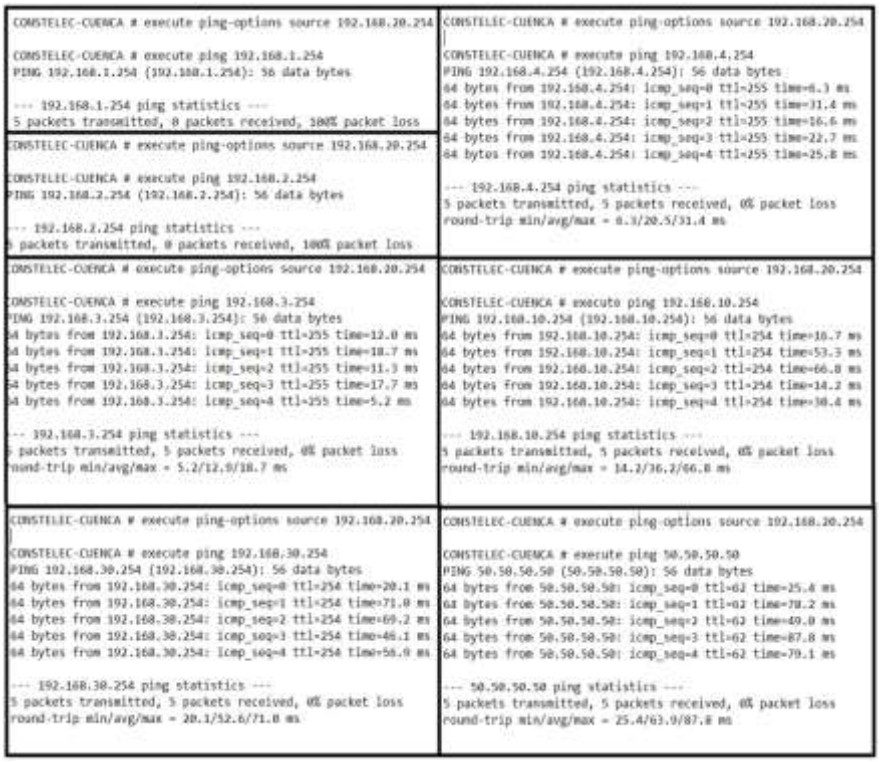


Figura 3.41: Conectividad a puntos remotos desde la red Lan Cuenca
Fuente: autor

- ✓ **Lan Machala**

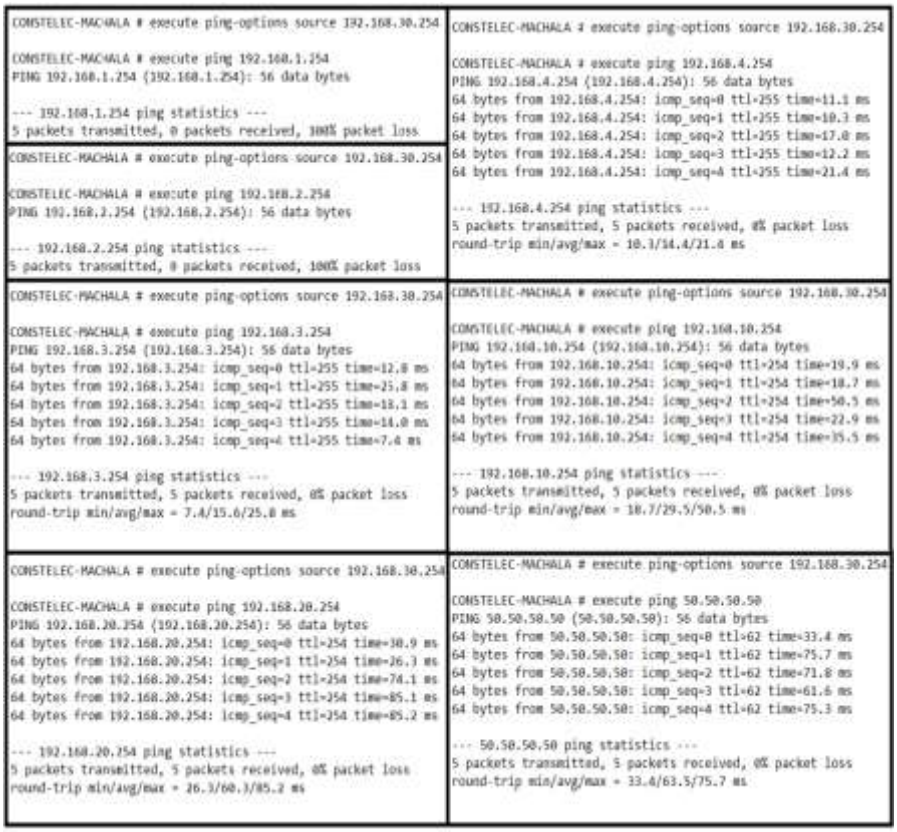


Figura 3.42: Conectividad a puntos remotos desde la red Lan Machala
Fuente: autor

3.12 Pruebas en el SD-WAN

En esta parte del trabajo de investigación se realizarán pruebas para verificar el correcto funcionamiento del SD-WAN a través de la simulación en GNS3, las mismas que permitirán validar las ventajas de la tecnología SD-WAN ante las redes tradicionales.

- ✓ **Flexibilidad y Administración total de la red**

Como prueba de la flexibilidad y administración total de la red SD-WAN se configurará como ejemplo, que el tráfico a Internet de la red LAN-Gerencia 192.168.1.X/24 vaya por la WAN2 10.100.2.254, mientras que el tráfico de la red Lan-Administración 192.168.2.X/24 vaya por la WAN1 10.100.1.254. Estas reglas deberán tener prioridad antes que la de Internet en general como se muestra en la figura3.43.

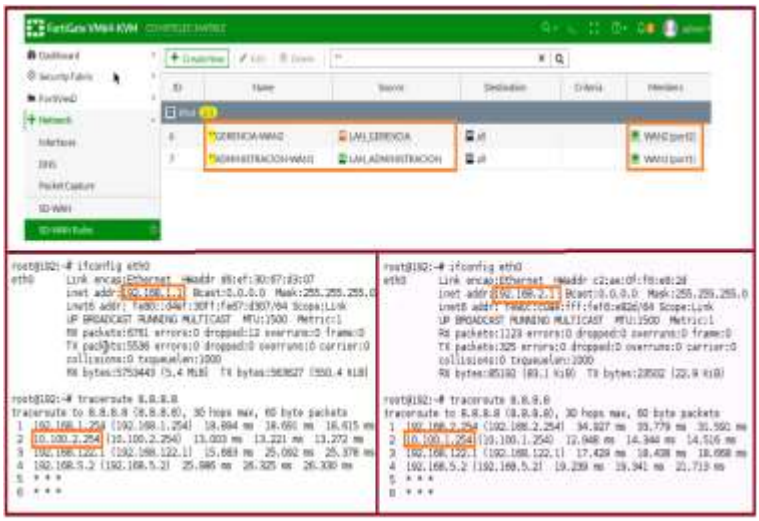


Figura 3.43: Flexibilidad y Administracion y administración de la red
Fuente: autor

- ✓ **Red de alta de disponibilidad**

Continuando con el ejemplo anterior, se simulará ahora la caída de la Interfaz WAN2, en la cual se encontraba la LAN-Gerencia navegando en Internet, y se evidenciará que la conectividad a Internet no va a caer, ya que conmutará todo el tráfico por la interfaz de la WAN1, esto se debe a que la regla **GERENCIA-WAN2 dejará de funcionar y pasará la funcionar la regla INTERNET_QoS. Ver figura 3.44.

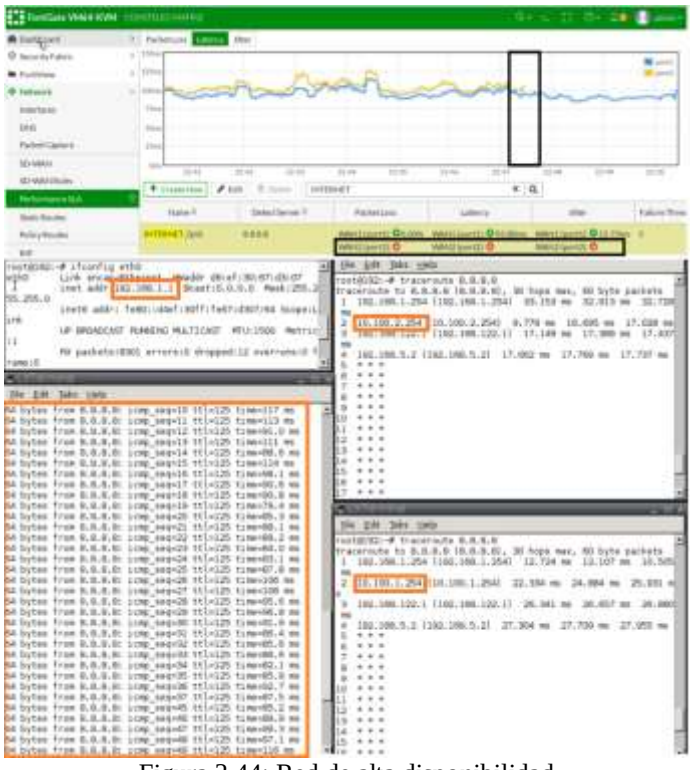


Figura 3.44: Red de alta disponibilidad
Fuente: autor

- ✓ **Seguridad en la Red**

La comunicación de datos entre sucursales a través de Internet será muy segura ya que solamente serán a través de los túneles IPSec, con el fin de salvaguardar la información trasmitida. En la figura 3.45 se realizó una traza desde un host de la LAN de CONSTELEC-Quito 192.168.10.1 hacia un host de la LAN de Constelec-Machala 192.168.30.1 y se verifica que su conectividad será a través de los túneles IPSEC.

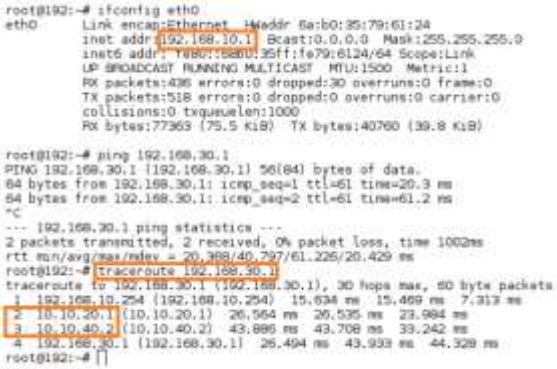


Figura 3.45: Seguridad de la Red
Fuente: autor

De igual manera se realizará una simulación de la caída del túnel IPsec de la WAN1 en Machala y se validará la rápida conmutación hacia el otro túnel disponible. Ver figura 3.46

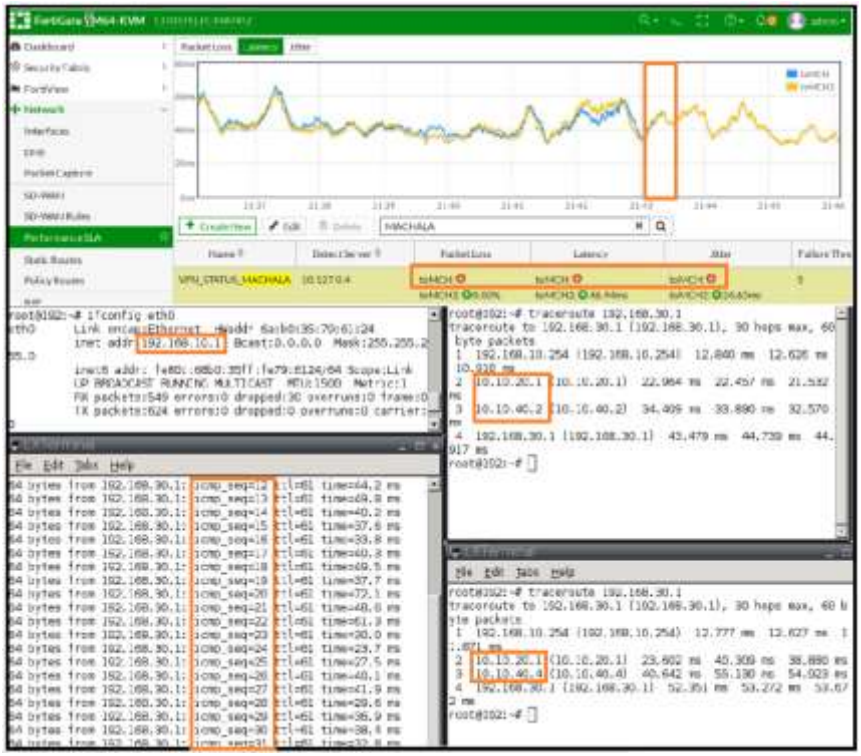


Figura 3.46: Alta disponibilidad en los Túneles IPSec
Fuente: autor

Conclusiones

- ✓ Se diseñó y configuró mediante el Software GNS3 una red de accesos para medianas empresas en el Ecuador como CONSTELEC, utilizando la tecnología SD-WAN con equipos Fortigate, a fin de cumplir con sus requerimientos, necesidades y alternativas de servicio que requieren los administradores de la red.

- ✓ Se describió las ventajas que brinda la tecnología SD-WAN sobre las redes tradicionales, que hacen que estas redes sean más flexibles, adaptables, seguras y económicas a las necesidades de las medianas empresas en el Ecuador.

- ✓ Entre los principales beneficios que se brinda a una red de accesos utilizando la tecnología SD-WAN es su flexibilidad y adaptabilidad a los requerimientos de los administradores de la misma, permitiendo fácilmente modificar, actualizar y agregar más aplicaciones en la red, ya que están son la base de muchas empresas.

- ✓ Se logro simular e implementar el diseño de la red para este proyecto de investigación a través del simulador GNS3 aplicando la tecnología SD-WAN, el mismo que permite configurar de forma manual o gráfica los enrutamientos, gestión de equipos, tiempos de latencia, conmutación rápida, etc., y observar gráficamente mediante curvas el rendimiento del comportamiento parcial o total de la red.

Recomendaciones

- ✓ Para diseñar una red de acceso de una mediana empresa utilizando la tecnología SD-WAN, se tendrá que considerar el tipo de equipamiento a configurar ya que estos deberán cumplir con las características que soporte dicha tecnología.

- ✓ Para la implementación de un proyecto de simulación en GNS3 se debe considerar la capacidad de la RAM (24 G) de la computadora en la que se realizará este trabajo, de tal manera que el programa pueda ejecutarse.

- ✓ Se debe considerar el tipo de firmware que se utiliza en los Fortigate, en este proyecto se trabajó con la versión 6.2.3 ya que con versiones anteriores de la 6.0.0 puede que la SD-WAN no tenga un comportamiento óptimo.

Bibliografía

Cisco. (2008). *Mapas de rutas para la configuración de la redistribución del protocolo de enrutamiento IP*. Obtenido de https://www.cisco.com/c/es_mx: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/49111-route-map-bestp.html

CISCO. (2018). *¿Qué es SD-WAN?* Obtenido de Cisco. SD-WAN Solution: https://www.cisco.com/c/es_co/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html

El Equipo de Marketing. (2016). *antenna comunicaciones.* Obtenido de Tipos de redes de comunicación empresariales: https://www.antennacomunicaciones.com/tipos-redes-comunicacion-empresariales/

Esnoz, I. (2019). *Mayor seguridad con la segmentación de las redes SD-WAN.* Obtenido de Teldat: https://www.teldat.com/blog/es/sd-wan-segmentacion-en-redes-seguridad/

García, J. (2018). *Beneficios de SD-WAN para empresas y organizaciones.* Obtenido de Teldad: https://www.teldat.com/blog/es/beneficios-sd-wan-red-economica-flexibilidad-ancho-de-banda-seguridad-gestion-de-aplicaciones/

Generar confianza. (2018). *Seguridad de enrutamiento para legisladores*. Obtenido de Internet Society: https://www.internetsociety.org/es/resources/doc/2018/seguridad-de-enrutamiento-para-legisladores/

GPC. (2019). *Redes Informáticas LAN, MAN y WAN: ¿Cuál es la diferencia entre ellas?* Obtenido de gpcinc.mx: https://gpcinc.mx/blog/redes-lan-man-wan/

Hesselbach, X., & Altés, J. (2015). *MPLS Multi Protocol Label*. Obtenido de Redes de conmutacion orientadas a la conexion: https://redesconmutacion.weebly.com/componentes.html

Kesavan, A. (2016). *Recomendaciones para crear una SD-WAN*. Obtenido de Network world: https://www.networkworld.es/networking/recomendaciones-para-crear-una-sdwan

Lucas, E. (2020). *SD-WAN vs MPLS, ¿Qué tecnología elegir?* Obtenido de Taiga Consulting: https://www.taiga-consulting.com/blog/sdwan-vs-mpls

Ostec. (2018). *SD-WAN, principales conceptos y modelo de funcionamiento*. Obtenido de Ostec seguridad digital de resultados: https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento

Purdy, C. (2016). *Aprovechando al máximo la emergente tecnología SD-WAN*. Obtenido de DiarioTi.com: https://diarioti.com/aprovechando-al-maximo-la-emergente-tecnologia-sd-wan/101408

Quintana, S., & Tabares, M. (2011). *Multiprotocol Label Switching (MPLS): usos, aplicaciones y áreas promisorias de la tecnología.* Obtenido de Universidad Tecnológica de Bolívar: https://biblioteca.utb.edu.co/notas/tesis/0062650.pdf

Vélez, D. (2018). *Repositorio Universidad Catolica de Santiago de Guayaquil*. Obtenido de Diseño y simulacion en GNS3 de una red multiservicios MPLS para medianas empresas en el Ecuador: http://repositorio.ucsg.edu.ec/bitstream/3317/11887/1/T-UCSG-POS-MTEL-115.pdf

Weinberg, N., & Till, J. (2018). *Cómo funciona MPLS* . Obtenido de Network world: https://www.networkworld.es/telecomunicaciones/como-funciona-mpls

Glosario de Términos

BGP (Border Gateway Protocol, Protocolo de Puerta de Enlace de Borde)

DMVPN (Dynamic Multipoint Virtual Private Network, Red privada virtual multipunto dinámica)

FEC (Forwarding Equivalence Class, Clase de equivalencia de reenvío)

GNS3 (Graphic Network Simulation,Simulador Gráfico de Redes)

IP (Internet Protocol,Protocolo de Internet)

IPSec (Internet Protocol security, Seguridad del Protocolo de Internet)

LAN (Local Area Network, Red de área local)

LER (Label Edge Routers, Enrutador frontera de etiquetado)

LSP (Label Switched Path,Camino de Conmutación de Etiquetas)

LSR (Label Switching Routers, Enrutador de conmutación de etiquetas)

LTE (Long Term Evolution, Evolución a largo plazo)

MPLS (Multiprotocol Label Switching, Conmutación de Etiquetas Multi-Protocolo)

OSI (Open Systems Interconnection,Sistema Abierto de Interconexión)

OSPF (Open Shortest Path First, Primer Camino Más Corto)

PBR (Policy Based Routing, Enrutamiento basado en políticas)

QoS (Quality of Service, Calidad de Servicio)

RIP (Routing Information Protocol, Protocolo de información de enrutamiento)

SDN (Software defined networking, Redes definidas por software)

SD-WAN (Software Defined-Wide Area Network, Red de Área Amplia Definida por Software)

SLA (Service Level Agreements,Acuerdo de Nivel de Servicio)

VoIP (Voice Over Internet Protocol, Voz sobre Protocolo de Internet)

VPN (Virtual Private Network, Red Privada Virtual)

WAN (Wide-Area Network, Red de Área Amplia)

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Fulvio Andrés Carrasco Cabrera**, con C.C: # **0923939797** autor/a del trabajo de titulación: **Diseño y Simulación de una Red de Accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador,** previo a la obtención del título de **Magíster 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, 6 de noviembre del 2020

Fulvio Andrés Carrasco Cabrera

C.C: 0923939797

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	Diseño y Simulación de una Red de Accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador	
AUTOR(ES)	Fulvio Andrés Carrasco Cabrera	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz	
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	**Guayaquil, 6 de noviembre del 2020**	**No. DE PÁGINAS: 75**
ÁREAS TEMÁTICAS:	Redes de comunicaciones empresariales, Protocolos de red, Tecnología SD-WAN, Definición de PBR, Mapas de ruta, Red de Accesos	
PALABRAS CLAVES/ KEYWORDS:	SD-Wan, MPLS, PBR, IP-Sec, BGP, GNS3	
RESUMEN/ABSTRACT: En atención a la necesidad que tienen muchas empresas en el Ecuador en optimizar recursos, reducir gastos y tener procesos que permitan garantizar calidad, que pueda crecer, flexible y versátil, surge SD-Wan (Red de Área Amplia Definida por Software), que brinda muchas ventajas ante las tecnologías actuales. Este trabajo de titulación se realizará mediante el método deductivo, lo que permitirá caracterizar y aprender las aplicaciones de esta tecnología para poder realizar el diseño y simulación para empresas medianas en el Ecuador. La tecnología SD-Wan hoy en día tiene un amplio campo de aplicaciones, debido a que se requiere de pocos recursos para su configuración e implementación, por lo que, por medio de un programa brindado por un simulador lo cual se realizará en esta investigación, demostrando la flexibilidad, versatilidad y escalabilidad de esta tecnología.		
ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO AUTOR/ES:	**Teléfono:** +593-996541555	**E-mail:** fulvio_barce93@hotmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@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):		