UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos.

AUTOR:

Luis Andrés Marín Santamaría, Ing.

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

Ilen Rivero Pouymiro, MSc.

Guayaquil, a los 13 días del mes agosto del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Luis Andrés Marín Santamaría como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

MSc. Ilen Rivero Pouymiro

DIRECTOR DEL PROGRAMA

MSc. Manuel Romero Paz

Guayaquil, a los 13 días del mes agosto del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, Luis Andrés Marín Santamaría.

DECLARO QUE:

El trabajo de Titulación Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos previa 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, a los 13 días del mes agosto del año 2021

EL AUTOR

Luis Andrés Marín Santamaría, Ing.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

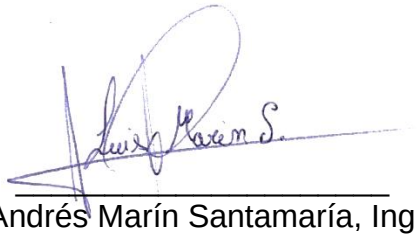
AUTORIZACIÓN

Yo, Luis Andrés Marín Santamaría.

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 WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 13 días del mes agosto del año 2021

EL AUTOR

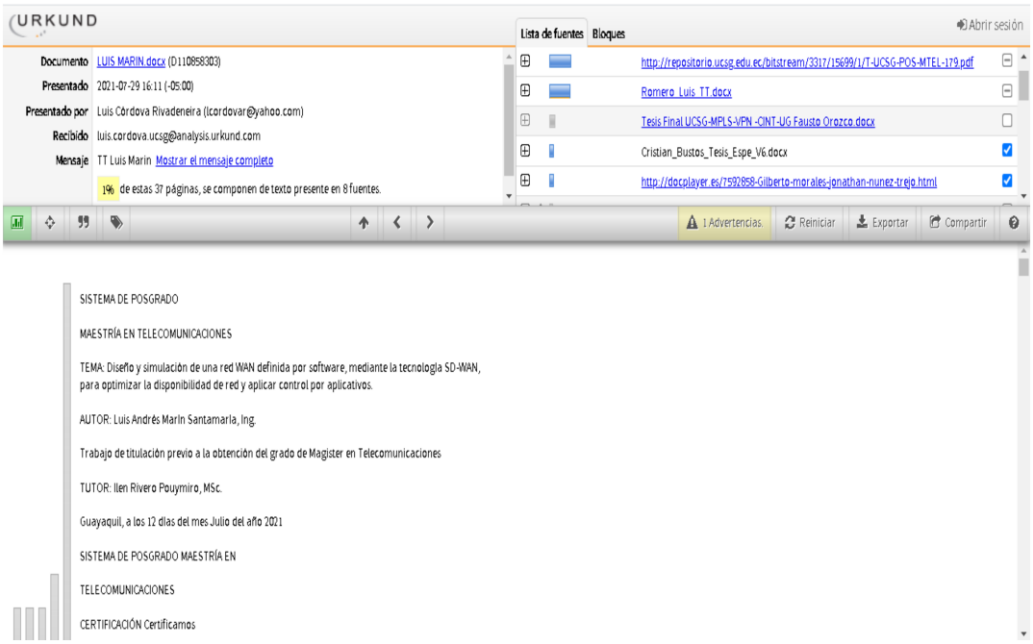


Luis Andrés Marín Santamaría, Ing.

REPORTE URKUND

Informe del URKUND correspondiente al Trabajo de Titulación del Ing. Luis Andrés Marín Santamaría,

El presente trabajo de Titulación contiene 1% de similitud con otros trabajos similares.



Dedicatoria

Dedico con todo mi amor este esfuerzo a mis ángeles que partieron en un año atípico. A papá Luis que me enseñó a ser fuerte, pero con humildad, ver oportunidades donde todos ven oscuridad y que rendirme nunca es la opción. A mi abuelo Freddy que me brindó todo su amor y enseñanza. A mi pequeño primogénito que no creció, pero me brindó la fuerza para continuar.

Agradecimientos

Agradezco a Dios la oportunidad de estar con vida y poder culminar una meta que me propuse.

Agradezco a mi madre que me dio siempre su apoyo incondicional y jamás permitió que me rindiera y junto a mi padre me formaron en valores. Siempre lucharon para que no me falte nada y tenga la mejor educación.

Agradezco a mis hermanas Malena y Sheyla que han sido pilar importante en mi vida. Mi hermana mayor mi inspiración a siempre superar, y mi hermana menor que yo sea su inspiración de superación.

Agradezco de manera especial a mi esposa Valeria que es mi apoyo y quien me dio el impulso a tomar la maestría cursada. Permaneció conmigo día y noche no dejándome decaer, siempre estando dispuesta a ayudarme sin importar cuantas veces preguntaba lo mismo y con mucho amor explicando.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Ilen Rivero Pouymiro
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

_____

MSc. Edgar Quezada Calle
REVISOR

RESUMEN

Debido a la emergencia sanitaria que el país se encuentra atravesando la compañía Construl S.A. se ha visto en la necesidad de optimizar el uso de sus recursos tecnológicos debido a la implementación del teletrabajo y nuevos requerimientos de servicios, sin encarecer sus costos y manteniendo la calidad de los recursos que se utilizan en el desarrollo de sus labores. Por tal motivo, se da paso al estudio de disponibilidad y factibilidad de implementación de nuevas tecnologías que permitan mantener un equilibrio económico a la empresa Construl S.A. Este estudio propone la implementación de la tecnología SD-WAN (*Wide Area Network*) que permite a los usuarios realizar trabajos constantes, sin perder la comunicación en ningún momento, al activar enlaces de respaldo o backups, cuando el enlace de conexión principal falle. La tecnología SD-WAN no requiere del uso de un número alto de megabytes de ancho de banda o recursos de red. Para el desarrollo y demostración de las ventajas y mejoras que esta tecnología trae a las empresas se usa un simulador que facilita la demostración. Finalmente se determina que la implementación de esta tecnología cumple con lo requerimientos tecnológicos de la compañía Construl S.A.

Palabras clave: SD-WAN, Tecnologías, WAN, Fortigate, SLA, seguridad, túneles.

ABSTRACT

Due to the health emergency that the country is going through, the company Construl SA has seen the need to optimize the use of its technological resources due to the implementation of teleworking and new service requirements, without increasing its costs and maintaining the quality of the resources used in the development of their work. For this reason, the study of availability and feasibility of implementation of new technologies is carried out that allows the company Construl SA to maintain an economic balance. This study proposes the implementation of SD-WAN (Wide Area Network) technology that allows Users carry out constant work, without losing communication at any time, when activating backup links or backups, when the main connection link fails. SD-WAN technology does not require the use of a high number of megabytes of bandwidth or network resources. For the development and demonstration of the improvements and improvements that this technology brings to companies, a simulator is used to facilitate the demonstration. Finally, it is determined that the implementation of this technology meets the technological requirements of the company Construl S.A.

Keywords: SD-WAN, Tecnologías, WAN, Fortigate, SLA, seguridad, Tuneles.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 . Capítulo 1 Introducción

Las redes WAN (*Wide Area Network*) definidas por software dan inicio a una evolución en las redes de comunicación (Shaw, 2018). Este avance se da por las necesidades presentadas en las empresas o entidades, para mejorar la distribución, administración de las redes y reducción de costos. Con el presente proyecto se busca diseñar y simular una red eficaz para cubrir la demanda actual de una compañía, tener los recursos y la infraestructura lista para expandirse.

SD-WAN(*Software Defined WAN*) está ayudando a actualizar los equipos periféricos del cliente en sitios remotos, integrando servicios que ayudan en carga compartida a través de múltiples enlaces ascendentes de cualquier tipo. También proporciona una interfaz simplificada para la gestión de políticas para rendimiento de la aplicación en tiempo real (Iddalagi, 2020).

De acuerdo a estudios de mercado de Acumen Research and Consulting, estiman una tasa de crecimiento anual del 47% para las redes definidas por software, esto está pronosticado para el periodo del 2016-2022 (Larosa, 2018).

En el 2017, la IDC (*International Data Corporation*) estimó que los ingresos por servicios e infraestructura SD-WAN estarían alcanzando una tasa compuesta anual del 69.6%, logrando llegar a los 8 mil millones de dólares en el 2021 (Larosa, 2018).

El desarrollo de las redes definidas por software tiene un enfoque arquitectónico, son el resultado del estudio y aplicación de la virtualización de las redes. Buscan separar la parte lógica de la parte física para que los procesos y utilización de las redes sean más dinámicos y enfocados a reducir el uso de recursos de red (Larosa, 2018).

Teniendo en cuenta que las redes definidas por software son virtualizaciones y se manejan en el ámbito lógico de las redes, en la actualidad las empresas presentan un estancamiento de crecimiento. Esto se debe a que los ISP (*Internet Service Provider)* siguen ofreciendo redes con infraestructuras orientadas a la parte física y esto genera un mayor

costo de operaciones, menor seguridad para la empresas y estancamiento en el desarrollo. La pandemia ocasionada por la Covid-19, a nivel mundial originó que muchas empresas opten por emplear la modalidad de trabajo no presencial, saturando sus redes, ya que la infraestructura que poseen, no se adecúa a las nuevas necesidades.

Normalmente las empresas utilizan para la comunicación de datos la red MPLS. Lo que no siempre implica la contratación del servicio de datos e internet en conjunto, ni tampoco implica que estos paquetes de servicios sean proporcionados con sus correspondientes respaldos. Situaciones que originan que se tenga que contratar varios servicios, en diferentes proveedores encareciendo los costos para tener una mejor contingencia. Con la tecnología SD-WAN se puede utilizar solo la red de Internet para comunicarse también a nivel de datos. La tecnología SD-WAN, además configura enlaces de contingencias lo que genera el aprovechamiento total de los recursos.

En el tiempo actual, la Tecnología SD-WAN se encuentra en desarrollo por su gran utilidad, su rápida conmutación y redundancia entre sus redes y aplicativos, esto es gracias a equipos que complementan sus características como son los Fortigate, los cuales brindan todos los beneficios para trabajos desde casa, campus, subir la información a la nube y seguridad en su gestión (DatacenterDynamics, 2020).

Normalmente las empresas que requieren tener comunicación constante y no presentar problemas si un enlace falla, para evitar el estancamiento de sus operaciones contratan dos enlaces, uno principal y otro de reserva (backup), manteniendo el segundo sin uso hasta que el principal no se encuentre operativo. Con esta nueva tecnología y de la mano con los equipos Fortigate se busca tener alta disponibilidad en la red, y el uso equitativo de los dos enlaces. Permitiendo que los enlaces de datos o internet funcionen permanentemente y el tráfico de datos o internet sea balanceado, y con esto aprovechar al máximo los recursos contratados, generando confianza al usuario y que los negocios puedan extenderse.

1.1 Antecedentes.

Se define una red, como una colección de nodos (*hosts*), capaces de comunicarse entre sí, a veces confiando en los servicios de un número determinado de máquinas que se encargan de transmitir datos entre quienes lo demanden. Los nodos son casi siempre computadoras, pero no necesariamente; se puede pensar, sin equivocación, en terminales X o impresoras inteligentes como nodos. Por otro lado, a las pequeñas aglomeraciones de estos, se las denomina sitios. La comunicación, sería imposible sin algún tipo de lenguaje o código. Estos lenguajes se denominan conjuntamente como protocolos. Así, los protocolos usados en las redes de computadoras no son más que reglas muy estrictas de intercambio de mensajes entre dos o más servidores (Kirch & Dawson, 2002).

La administración de redes de área amplia está sujeta a la realización de trabajos a través de recursos disminuidos que implica el uso de más usuarios y aplicativos a un menor costo, utilizando equipos de menor dimensión sin la intención de alterar la confiabilidad y seguridad de estas redes (Bustos, 2019). Los trabajos que se realizan en la administración de redes es manejar los recursos de red de la empresa y distribuirlos de una manera equitativa a cada usuario de la red, los usuarios serán los encargados de usar los recursos y aplicativos de la red los cuales ocuparán un ancho de banda determinado, se busca que los equipos usados para la administración de la red sean de un menor tamaño y así disminuir el uso de infraestructura física, esto sin perder la confiabilidad y seguridad. El alto costo de las redes WAN tradicionales y el alto requerimiento de ancho de banda de los aplicativos, están obligando a los encargados de la red a buscar soluciones alternativas para un mejor desempeño y ahorro de los costos de producción (Bustos, 2019).

Las aplicaciones emergentes y los escenarios operativos plantean requisitos estrictos para la transmisión de datos a larga distancia, lo que impulsa a los operadores de red a diseñar redes de área amplia desde una nueva perspectiva. La red de área amplia definida por software, es decir,

SD-WAN, se ha considerado como la arquitectura prometedora de la red de área amplia de próxima generación (Yang, Cui, Li, Liu, & Xu, 2019)

Las empresas y entidades financieras, las cuales no pueden perder la comunicación en ningún momento, buscan siempre una mejora en su rendimiento operacional y de intercomunicación con sus extremos. En años anteriores a la aparición de estas tecnologías, las empresas tenían contratados dos enlaces. Uno de los enlaces se manejaba como principal y el otro lo tenían en estado no activo (standby) como respaldo; el cual no era utilizado a menos que el principal falle o presente algún tipo de problema. Esto provoca que las empresas empleen un costo mayor, en la contratación de los servicios al querer tener una disponibilidad adecuada, y también genera un alto costo en contratación de recursos externos para mantener las redes activas.

Con el diseño propuesto se podrá demostrar que al tener dos enlaces se aprovecha el cien por ciento de la red ya que, al virtualizar la IP WAN. Además, se requiere menor ancho de banda contratado en cada enlace. Para virtualizar las IP WAN se utiliza un equipo Fortigate que soporte los requerimientos que la empresa solicita, se evite saturación y se proteja de ataques externos en la red.

La introducción de la tecnología SD-WAN podría ser determinante para la adaptación de las pequeñas y medianas empresas a estos rápidos y complejos desarrollos (Guerrero, 2018). La tecnología SD-WAN empieza a desarrollarse aproximadamente hace 10 años con su primer modelo en la tecnología SDN (del inglés *software defined networks*), desde sus inicios la intención de SDN y SD-WAN fue realizar una automatización de la red, encapsular y virtualizar los enlaces, y al aplicar SD-WAN en los servicios internos del cliente se tendrá control en la red y se optimizará los recursos.

1.2 Planteamiento del problema

Las redes de comunicación se han visto afectadas por la alta demanda de tráfico en la red que genera los aplicativos, expansión de red y nuevos requerimientos de los usuarios. Por tal motivo el tráfico de la red se vuelve más pesado y requiere más recursos, requiriendo mayor inversión en la

contratación de nuevos servicios. Las empresas requieren mayor rapidez y utilización de recursos sin generar costos más altos que perjudiquen en el desarrollo y expansión de la compañía.

Si bien se conoce que la expansión y rápido crecimiento de muchas empresas requieren mayor capacidad y disponibilidad en la red, con la aparición de la pandemia se observó la necesidad técnica de tener alta disponibilidad y control sobre la red tanto en ambiente laboral como en el hogar. La pandemia de COVID 19 que golpeó al mundo en el 2020 hasta la actualidad hizo que las empresas, y usuarios en los hogares se replanteen la forma que se lleva a cabo los trabajos y se aplican los recursos necesarios para realizarlo.

1.3 Definición del problema

La empresa Construl S.A. presenta problemas debido la latencia que se genera por la sumatoria de retardos dentro de la red, en la seguridad para no permitir filtraciones de información y controlar el acceso a páginas no permitidas por la empresa Construl S.A., en la saturación por consumo excesivo de ancho de banda de algún usuario en especial. Situaciones que se traducen en una gestión ineficiente del servicio de Internet, con algoritmos de enrutamiento inadecuados, retardo en la comunicación, generando pérdidas económicas a la empresa.

1.4 Justificación del problema

En la actualidad con la pandemia que vive el Ecuador los trabajos están más orientados a realizarse por medio de teletrabajo, lo cual las empresas se han visto obligadas a utilizar redes SD-WAN para cumplir las nuevas exigencias que el entorno lo requiere. Es importante tomar en cuenta que los usuarios de las empresas y hogares requieren un servicio sólido sin la necesidad de contratar nuevos planes y elevar sus costos mensuales.

1.5 OBJETIVOS

Objetivo General

Diseñar y simular una red de Internet y datos utilizando tecnología SD-WAN, y administrar la red para tener alta disponibilidad.

1.5.1 Objetivos Específicos

- Plantear diseño adecuado para la utilización de un enlace con alta disponibilidad.
- Analizar el mejor algoritmo de carga para evitar saturación en la red obteniendo alta disponibilidad de los recursos.
- Establecer una red segura y controlando la navegación de acuerdo a las actividades de cada área.
- Determinar las correctas configuraciones de la red SD-WAN a través de los FortiGate.

1.5.2 Hipótesis

Con la utilización de la tecnología SD-WAN, misma genera una concentración de datos para una posterior distribución, a través de la aplicación de algoritmos de enrutamientos modernos que permiten la distribución de la carga de estos datos, se mejora su transporte y se disminuye el tiempo de respuesta de todos los requerimientos que realicen las diferentes sucursales establecidas de Construl S.A. Lo que mejora la utilización del servicio de Internet y de datos, aprovechando en su totalidad los recursos contratados. De esta manera se garantiza una mejor interacción y experiencia de los usuarios al utilizar la red empresarial de Construl S.A.

1.5.3 Metodología de investigación

Las metodologías a utilizar para este documento son la descriptiva, deductiva y la experimental, se usará la metodología descriptiva para explicar fundamentos ya establecidos y delimitar el problema, observar y registrar los datos con los cuales se pueda buscar la solución al problema. En el método deductivo se utiliza la deducción lógica para determinar conclusiones a partir de principios, leyes y hechos realizados. El método experimental se usará con la manipulación de las variantes, observando y analizando la conducta que tomará en cada cambio con el cual se puede determinar un mejor diseño que permita cumplir con todos los requerimientos de red.

2 . Capítulo 2 Marco Teórico

Este capítulo expone y plantea los documentos teóricos que sustenten y detallen los componentes a usar para desarrollar la simulación de la tecnología SD-WAN en los cuales se podrá observar cuales son los beneficios de la tecnología y los alcances que se puede llegar a tener para mejorar así la utilización de los recursos de la red en la empresa Construl S.A.

2.1 Redes definidas por software

Son arquitecturas de redes diseñadas para ser administradas a nivel lógico con una destreza dinámica que ayude a la ampliación, utilización de nuevos aplicativos y futuras restructuraciones en la red. Las redes definidas por software logran una rápida restructuración debido a la separación de la red física de la virtual creada para la administración y control de la red WAN de una manera eficiente donde se controle la propia red de manera centralizada.

Pese a todas las modificaciones que se han realizado durante los últimos años, la arquitectura de Internet actualmente no satisface las demandas de nuevas aplicaciones y sistemas. Las redes informáticas se volvieron comerciales y los equipos de red son solo “Cajas negras”, es decir, implementaciones integradas basadas en software y hardware propietarios. Frente a esta realidad, los investigadores de la red y la comunidad científica desarrollaron nuevas propuestas para la creación de las redes informáticas del futuro, es decir, nuevas arquitecturas de implementación del núcleo de la red. Una de las principales propuestas para esta nueva arquitectura de redes se basa en redes capaces de ser programadas bajo demanda, es decir, redes que son programables o redes que son flexibles para manejar los requisitos y problemas actuales. Una de las formas de brindar programabilidad a las redes es a través de la implementación de Redes Definidas por Software (Rodrigues, 2013).

Una de las cualidades que llama la atención de la tecnología SD-WAN es la facilidad de administrar una red de forma remota, permitir o denegar

tráfico aplicando seguridad en la red. Esto se puede realizar aprovechando en su totalidad el ancho de banda asignado sin necesidad de contratar uno de mayor capacidad.

Esta situación permite que los usuarios obtengan un alto ahorro en su inversión de recursos a un mediado plazo. En esta instancia no es necesario adquirir mayores recursos en la red para satisfacer las necesidades de los nuevos aplicativos. Con una correcta administración de las redes definidas por software SD-WAN se puede obtener el mayor provecho de los recursos. La arquitectura de rede SD-WAN son muy usadas en clientes corporativos los cuales cuentan con matriz y sucursales. Uno de los objetivos de las redes definidas por software con SD-WAN es dinamizar, flexibilizar el uso de los recursos y poder tener una red centralizada, pero con seguridad tanto a nivel de ataques como evitando pérdidas de comunicación.

2.2 Internet y las TIC

Las Tecnologías de la Información y Comunicación o TIC, se conforman por la unión de diferentes redes de comunicación interconectadas, las cuales usan el protocolo TCP/IP para establecer la comunicación de los servicios entre los diferentes nodos de cada proveedor. Estas redes están conformadas desde grandes sistemas informáticos, hasta por terminales móviles y elementos domésticos, como conexiones de luz de un hogar. Las TIC son empleadas en la administración y distribución de varios tipos de información. (Romero, y otros, 2018).

La figura 2.1 representa las redes interconectadas en una misma red, cada una pertenece a un nodo, proveedor o servidores diferentes y la unión de ellas hace el internet.

Figura 2.1: Esquema de cómo se conforma el Internet.
Fuente: (Yañez, 2020)

2.3 Tipos de redes.

2.3.1 Redes LAN.

Las redes LAN (*Local Area Network*) son redes controladas desarrolladas para transmitir datos y comunicar dentro de un mismo espacio de trabajo. Con las redes LAN se puede compartir no solo datos, sino recursos entre equipos dentro de un espacio delimitado. Una red LAN es de broadcast, en la cual se emite un mensaje de una computadora y llega a los diferentes computadores que pertenecen a la red, pero solo es legible para el equipo con dirección destino (Artunduaga & Morales, 2018).

Las redes LAN suelen emplear tecnología de difusión mediante un cable sencillo, al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps. Tienen bajo retardo y experimentan pocos errores (Reina & Ruiz, 2016).

En la figura 2.2 se muestra una red LAN local tradicional compuesta con equipos comunes para el desarrollo de actividades como son router, PC (*Personal Computer*), impresora y escáner, los cuales están conectados entre sí por medio del equipo router interno del cliente final.

Figura 2.2: Esquema de una red LAN (Cliente final)
Fuente: (SS00, 2020)

2.3.2 Redes WAN.

Las redes WAN son redes de gran tamaño, la cuales logran abarcar países o continentes, se forman de la unión de varias redes locales. Como se puede evidenciar en la figura 2.3 donde hay varias redes LAN de diferentes empresas o instituciones y en la unión de dichas redes forma la red WAN, esto permite al usuario estar conectado con más personas o transmitir datos de la misma empresa a otros puntos que geográficamente no se encuentren cerca o conectados directamente. Cada red se identifica por una IP la cual facilita la localización de un usuario dentro de la red WAN.

En la mayoría de las redes WAN, la subred cuenta con dos componentes distintos: líneas de transmisión y elementos de conmutación. Las líneas de transmisión mueven bits entre máquinas. Se pueden fabricar a partir de alambre de cobre, fibra óptica o incluso enlaces de radio.

La mayoría de las empresas no poseen líneas de transmisión y tienen que rentarlas a una compañía de telecomunicaciones. Los elementos de conmutación o switches son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea entrante, el elemento de conmutación debe elegir una línea saliente hacia la cual reenviarlos. En el pasado, estas computadoras de conmutación han

recibido varios nombres; ahora se conocen como enrutador (Tanenbaum, 2013)

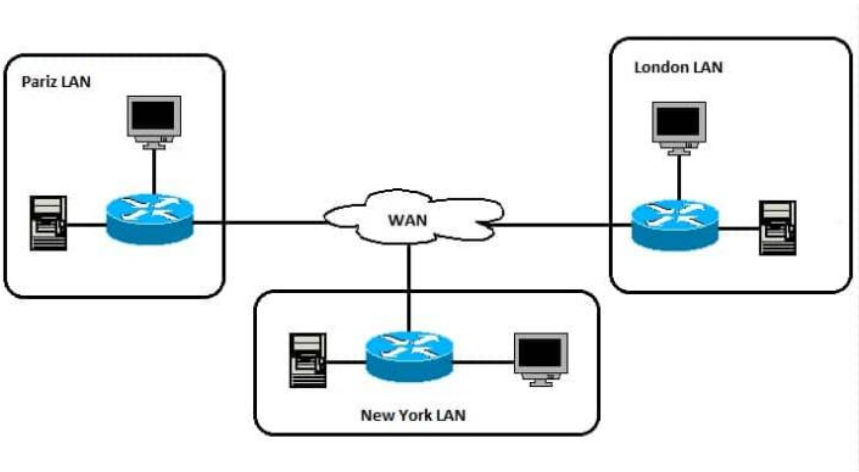


Figura 2.3: Esquema de una red WAN (Unión de 1 o varias LAN)
Fuente: (SS00, 2020)

2.4 Red MPLS

La red MPLS (*Multi Protocol Label Switching*) realiza conmutación de datos por etiquetas. Fue diseñada para soportar el tráfico de diferentes tipos de conexiones como son los datos, el internet, y la telefonía. La red MPLS agrupa diferentes tipos de datos que se transmiten mediante una misma red a las cuales se le agrega etiquetas (Castro, 2015).

Una propiedad fundamental de una red MPLS es que se puede utilizar para tunelizar múltiples tipos de tráfico, a través del núcleo de la red. La construcción de túneles es una herramienta poderosa porque solo los enrutadores en la entrada y salida del túnel necesitan comprender el contexto del tráfico subyacente transportado por el túnel. Como consecuencia, los dispositivos centrales solo necesitan tener un estado suficiente para permitirles conmutar paquetes encapsulados en MPLS sin tener en cuenta su contenido subyacente. Esta red MPLS consta de dispositivos de borde conocidos como enrutadores de borde de etiqueta (LER) o enrutadores de borde de proveedor (PE) y enrutadores de núcleo conocidos como enrutadores de conmutación de etiquetas (LSR) o enrutadores de proveedor (P) (Minei & Lucek, 2011).

A continuación, se hablará sobre la red MPLS donde se conocerá sus funciones, como está estructurada, sus características, sus ventajas y desventajas y como es implementada en los servicios de red.

2.4.1 Conceptos de la red MPLS.

La red MPLS desde su aparición en la década de los 90 ya como estándar fue acogida en el mercado y su crecimiento fue rotundo, las redes MPLS reemplazó a Frame Relay y ATM ya que puede llevar datos de alta velocidad y voz en una sola conexión. Esta red permite mejorar el flujo de trabajo, incrementando la capacidad de transmisión en los enlaces mediante una mejor eficiencia de la red (Hosting, 2017).

MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete IP para identificar un FEC (*Forward Equivalence Class*) o Clase de Equivalencia de Reenvío, término empleado para describir un conjunto de paquetes con características similares o idénticas que pueden reenviarse de la misma manera, es decir, pueden ser enlazado a la misma etiqueta y reenviarse sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes (infotecs, 2020).

MPLS se encuentra en una capa intermedia del modelo OSI (*Open Interconection System*), trabaja con características de la capa 2 y 3, al entrar el paquete a la red se le otorga una etiqueta de reenvío específico FEC , esto quiere decir que cada enrutador tiene una tabla para poder enviar de manera más rápida y precisa los paquetes FEC.

Las redes MPLS se caracterizan por presentar una mejora en su rendimiento y optimización de recursos. Este diseño puede ser desarrollado en diferentes protocolos como el protocolo Unicast, Multicast y Broadcasting. Adicionalmente, las MPLS se pueden agregar a la red de calidad de servicio Qos.

Como ventajas de las redes MPLS se reconoce que estas permiten la creación de rutas específicas con etiquetas para la transmisión de

paquetes. Generan seguridad en la red y menor tiempo de comunicación al reducir saltos entre puntos. El MTU (*Maximun Transmission Unit*) que utilizan es mayor a 1500. Así también trabaja en capa 2 y 3 del modelo OSI el cual implica una normativa conformada por siete capas con diferentes etapas por las que atraviesan los datos en el viaje de un dispositivo a otro sobre una red de comunicaciones.

Sin embargo, así como las MPLS presentan ventajas presentan desventajas, entre las cuales se contemplan una mayor complejidad en la instalación de nuevas sucursales, y en consecuencia un alto costo de implementación. Las redes MPLS no son flexibles para la adecuación a nuevas tecnologías como por ejemplo aplicativos de una nube. Requiere constante mantenimiento y administración de la red, generando a su vez un alto costo para tener contingencia del enlace.

2.4.2 Estructura de la etiqueta MPLS

La estructura MPLS conocida como Shim Header que se encuentra entre la capa 2 y 3 del modelo OSI con un tamaño de 4 bytes (32 bits), es una estructura sencilla la cual es agregada al paquete IP para su envío a través de la red como se muestra la estructura en la figura 2.4 en la cual se detalla la distribución de la etiqueta donde en total tiene 32 bits.

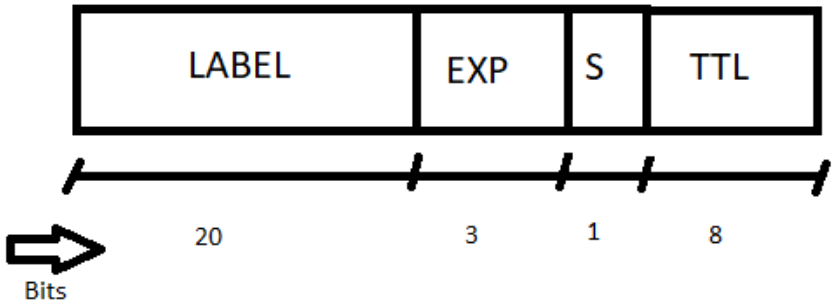


Figura 2.4: Estructura de la etiqueta MPLS

Fuente: Autor

- **Label:** la etiqueta contiene la información central de la cabecera MPLS, razón por la cual constituye, con 20 bits, la parte más larga de la cabecera (IONOS, 2017).
- **EXP:** con ayuda de este campo la cabecera informa sobre servicios diferenciados (DiffServ) y se puede utilizar para clasificar paquetes IP en función de su importancia con el objetivo de garantizar la calidad del servicio: estos 3 bits podrían servir para priorizar a un paquete de datos sobre el resto o para clasificarlo como secundario (IONOS, 2017).
- **Bottom of Stack (S):** este único bit define si la ruta de transmisión más profunda es una ruta simple o está compuesta por varias LSP intercaladas entre sí porque, si este fuera el caso, el paquete estaría marcado por varias etiquetas agrupadas en una pila (Label stack). Este campo informa al router, en definitiva, de si aún siguen más etiquetas (S=0) o si, por el contrario, la entrada contiene la última etiqueta MPLS de la pila (S=1) (IONOS, 2017).
- **TTL (del inglés Time to live:** es el tiempo de vida de un paquete de información que se va disminuyendo desde los 255 paquetes hasta llegar a cero, lo que equivale a la perdida de esta información.

2.5 Reenvío de enrutamiento virtual

Las VRF (*Virtual Routing Forwarding*) son etapas del enrutamiento y envío de paquetes que se desarrollan dentro de un PE (*Perimetral Equipment*), en el PE se pueden conectar varias VPNs (*Virtual Private Network*), este tipo de conexión integra dentro de una misma red, varios clientes con una identificación única, que es la VRF.

Esto se lo logra implementando túneles VPNs que son fundamentales en MPLS. Cada VRF es asociado a un enlace PE-CE. Cuando los enlaces reciben paquetes IP, buscan el destino donde debe ir de acuerdo a la VRF de los enlaces. Si el paquete no está asociado a una VRF, el destino se determinará de acuerdo a la tabla de direccionamiento por defecto (Ruiz, 2019).

2.6 Red privada virtual

VPNs son redes que se extienden sobre un área geográfica extensa, dichas redes cuentan con diferentes máquinas para la ejecución de los requerimientos del usuario. Con las redes VPN se reduce tiempo y dinero a las empresas que cuentan con sucursales en diferentes puntos geográficos (Ñacato, 2007). En el sentido más simple, una VPN conecta dos puntos finales a través de una red pública para formar una conexión lógica.

Las conexiones lógicas se pueden realizar en la capa 2 o en la capa 3 del modelo OSI, y las tecnologías VPN se pueden clasificar ampliamente en estos modelos de conexión lógica como VPN de capa 2 o VPN de capa 3 (Bollapragada, Khalid, & Wainner, 2005). Para entender que significa VPNs es necesario saber cómo funciona, y está conformado con PE, CE (Carrier Ethernet) los cuales se detallan a continuación:

- PE: Los routers finales que sirven de fronteras para un proveedor de servicios.
- CE: Los routers que se comunican directamente con el cliente que solicita el servicio.

En la figura 2.5 se muestra el diseño de una VPN en la cual se comunican entre CE y PE por medio de túneles.

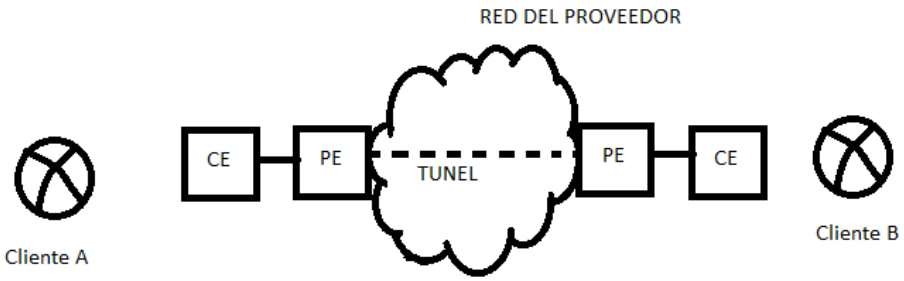


Figura 2.5: Diseño de comunicación de una VPN

Fuente: Autor

Para cada VPN debe estar asociada una o varias VRF específicas, con las que determina el camino a seguir una comunicación de un punto a otro.

Esto facilita el trabajo de comunicar clientes que tengas varias sucursales en diferentes partes geográficas. Con la VPN asignada y una VRF cada cliente puede manejar sus rangos de IP sin afectar a las redes de otros clientes.

2.7 Conceptos de las redes SD-WAN.

SD-WAN es un enfoque de red avanzado que crea redes híbridas para integrar banda ancha y otros servicios de red en la WAN corporativa, no solo manejando cargas de trabajo y tráfico comerciales generales, sino que también es capaz de mantener el rendimiento y la seguridad en tiempo real. La SD-WAN también crea una nueva plataforma digital para alojar y habilitar aplicaciones empresariales más innovadoras, no es de extrañar que la SD-WAN esté captando rápidamente la atención de la industria y los mercados se estén realizando implementaciones masivas tanto de empresas como de proveedores de servicios (Wang, 2019) .

SD-WAN permite gestionar y controlar de forma centralizada todos los componentes de hardware a través de software, y todo ello de una manera realmente sencilla. Una de las claves de SD-WAN es poder permitir a las empresas construir su WAN a medida, pagando por lo que necesitan realmente (Espinosa, 2019).

En la actualidad las telecomunicaciones han registrado un cambio en su funcionamiento ya que no solo las empresas grandes requieren rapidez y un óptimo desarrollo sino todos los usuarios en general. Con la aparición del virus Covid-19 la humanidad se ha visto vulnerada y obligada a adoptar otras formas de trabajo y comunicación las cuales exigen una mejor calidad de servicio. Lo que requiere una red centralizada para el manejo interno del usuario final y también en la administración de la red en las empresas que requieren que sus trabajadores laboren desde casa teniendo acceso a los recursos de red como si se esté en la oficina.

La tecnología SD-WAN guarda parentesco con las redes definidas por software. Están relacionados, ambos están definidos por software, pero mientras que SDN está destinado a centros de datos internos en una sede, SD-WAN toma esos conceptos definidos por software similares y el

desacoplamiento del plano de control del plano de datos a la WAN (Butler, 2017).

2.7.1 SD-WAN y sus características.

Las características de SD-WAN permiten trabajar con diferentes tipos de servicios por tal motivo proporciona funciones diferentes, las cuales se detallarán a continuación:

- Permite conexiones de datos, Internet, telefonía y MPLS.
- Posee flexibilidad para tomar diferentes rutas y no cargar una wan.
- Cuenta con VPN que permite la conexión a diferentes puntos.
- Tiene estándares de seguridad que permiten la tranquilidad a los usuarios que lo utilizan.
- La interfaz que manejan son amigables con el usuario.
- Menor costos en las conexiones y más velocidad.
- Realiza un análisis completo del tráfico que ingresa para asi administrar de mejor manera los datos.
- SD-WAN maneja diferentes rutas las cuales permiten conexiones rápidas y aprovechan el total de ancho de banda.
- Permite un monitoreo constante del tráfico en tiempo real, lo cual ayuda a mantener una calidad de servicio alta.
- La implementación de SD-WAN es más rápida y con menor complicaciones.

2.7.2 Funcionamiento de SD-WAN

Las herramientas que gestiona SD-WAN podrán proporcionar un servicio a menor precio para cada usuario (Nolle, 2021).Con la llegada de la tecnología SD-WAN la forma de administrar y monitorear los elementos de red cambian pues todo el manejo pasa a ser más centralizado. Con el uso de la tecnología SD-WAN se tiene la facilidad de poder tener agrupadas todo tipo de conexiones, tanto las seguras, como las públicas logrando así una mejor gestión de estas redes (Zuluaga, 2020).

El funcionamiento de la tecnología SD-WAN se basa en crear una red virtual para en ella administrar todas las redes que pertenecen a una empresa o sector. Como se muestra en la figura 2.6 donde se administra de forma general la red, y con esto se logra centralizar los servicios. Las redes virtuales para diferenciarse de las redes físicas se crean túneles como se muestra en la figura con los puntos remotos.

Los datos que ingresan a la red virtual se analizan y dependiendo de su requerimiento, el algoritmo de SD-WAN distribuye de una manera rápida y balanceada por medio de su mejor enlace. Esto abre las puertas a que las empresas busquen esta nueva tecnología debido a que las redes tradicionales limitan su ancho de banda. Con la finalidad de salvaguardar la integridad y continuidad del trabajo las empresas contratan dos enlaces el cual, solo uno se encuentra en funcionamiento y el otro entra en funcionamiento cuando este falle.

Con SD-WAN se solventa la problemática de tener contratado otro enlace y no tenerlo en funcionamiento, debido a que pueden trabajar las 2 WAN al mismo tiempo y aprovechar el ancho de banda de cada enlace para así sumarlo y tener un mejor acceso.

La figura 2.6 muestra diagrama de funcionamiento de la red SD-WAN en la cual se observa dos puntos remotos interconectados y realizando peticiones al internet y datos. Se centra la comunicación en uno de los puntos y de ahí realice las decisiones para la solicitud al internet o datos de una empresa.

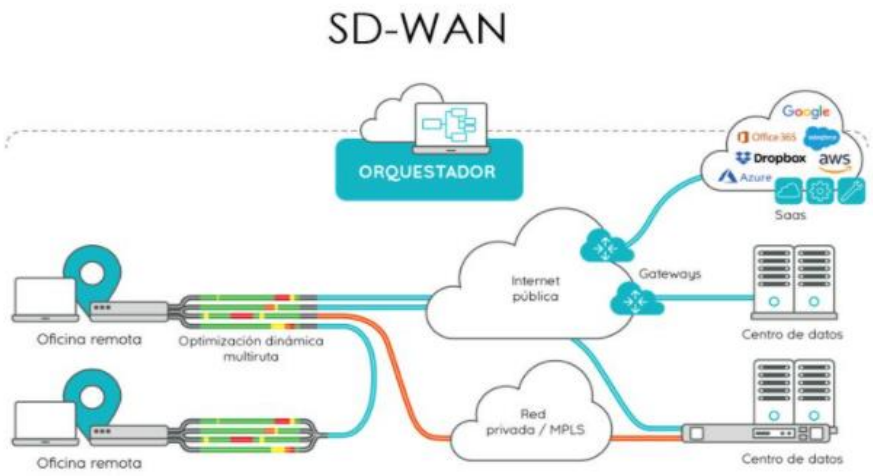


Figura 2.6: Diagrama de funcionamiento de una red aplicada SD-WAN

Fuente: (ICA, 2020)

2.7.3 Ventajas de SD-WAN.

Las principales ventajas de usar SD-WAN, aparte de mejorar el rendimiento de las aplicaciones, es que permite administrar de mejor manera el ancho de banda, adaptándolo a las necesidades y prioridades de las empresas de forma totalmente personalizada. Todo este control y gestión se realiza desde una única plataforma centralizada (Espinosa, 2019).

A continuación, se detalla las ventajas de SD-WAN:

- Fácil instalación: Se puede realizar configuraciones centralizadas y realizar cambios remotos.
- Seguridad: Garantiza una comunicación segura de extremo a extremo usando cifrado IPsec o SSL, las configuraciones son gestionadas por las mismas empresas y no dependen de agentes terceros.
- Uso de menor ancho de banda: al utilizar los enlaces principal y backup, al mismo tiempo que permite tener un mejor aprovechamiento del ancho de banda disponible.
- Calidad de servicio (Qos) : Se garantiza la optimización de la mejor WAN disponible para la comunicación.

2.7.4 Arquitecturas de SD-WAN

La SD-WAN presenta 3 tipos de arquitecturas definidas para uso local, MPLS e Internet. Las soluciones SD-WAN basadas en locales incluyen un dispositivo que se coloca en el sitio para lograr la funcionalidad SD-WAN. Las SD-WAN basadas en locales pueden ser soluciones rentables para empresas más pequeñas y localizadas. Las soluciones SD-WAN basadas en MPLS involucran múltiples dispositivos ubicados en los puntos finales de la red. Estas soluciones crean una red IP virtual entre los dispositivos propietarios del proveedor, dándoles el control de los paquetes de red de extremo a extremo. Las soluciones SD-WAN basadas en Internet también utilizan múltiples dispositivos en cada ubicación del cliente, utilizando conexiones públicas a Internet de proveedores elegidos por el cliente. El cliente paga por una parte de sus conexiones a Internet para que sea SD-WAN (Uribe, 2021).

2.7.5 Calidad de servicio en SD-WAN

En la SD-WAN se usan diferentes parámetros para calcular la calidad de servicio y la mejor ruta para transmitir la información. Para el diseño actual se han tomado parámetros de calidad como son:

- Latencia: Es la verificación del tiempo de respuesta de un enlace hasta llegar al otro punto (retardos). El camino que tenga mayor tiempo ese indicará mayor latencia es decir tiene retardo en la recepción del mensaje.
- Jitter: Es la cantidad de retardos que hay entre 2 puntos, al tener mayor tiempo de Jitter se puede decir que un enlace se encuentra intermitente.

2.8 Seguridad de SD-WAN

La tensión en la conectividad a la WAN puede aumentar la vulnerabilidad de las organizaciones a un ciberataque . La SD-WAN es una tecnología que permite a las organizaciones centralizar el control o dirigir de manera inteligente su tráfico WAN.

Una solución de seguridad que se vincule con SD-WAN significa que las organizaciones pueden proteger sus datos y garantizar que un nuevo enfoque de la red no signifique un mayor riesgo (Sollars, 2018). SD-WAN es una oportunidad para proveer autenticación y políticas de cifrado, independientemente del mecanismo de transporte o proveedor de servicios subyacente (informaticahabana, 2020). Esta tecnología aparte de realizar un adecuado manejo de aplicaciones, mejora el rendimiento de software y servicios. Sin embargo, uno de los principales problemas es la seguridad de las SD-WAN por motivo que se transmite directamente por Internet (López, 2020).

Teniendo en consideración este defecto, *Secure* SD-WAN de FORTINET cuenta con una de las funciones de seguridad como NGFW (Next-Generation Firewall) y otras como SD-WAN, Secure SD-WAN tiene como fin reducir costos, simplificar las operaciones, mejorar el rendimiento, habilitar una postura de alta seguridad y proporcionar un mecanismo de control centralizado que pueda determinar y enrutar la trayectoria ideal para el tráfico (López, 2020).

2.9 Seguridad del protocolo de Internet

IPSEC (*Internet Protocol Security*) es la recopilación de protocolos que están dedicados a garantizar la seguridad en la capa de red, esto se logra por medio de la implementación de encriptación y autenticación de los paquetes que entren a la red. Ipsec está diseñado para cumplir la misión que todos los paquetes enviados en la red sean invisibles e inaccesibles para terceros.

Este protocolo forma un conjunto de mecanismos que intervienen en la seguridad de la comunicación de los protocolos de Internet. Para un mejor control de la seguridad Ipsec usa criptografía y la autenticación a nivel de

red de pares, integridad de datos, origen de datos, confidencialidad (Rico & Lobo, 2012).

2.9.1 Funcionamiento de Ipsec.

IPSEC es un estándar de con mucha eficacia el cual brinda servicios de seguridad en redes IP de cualquier topología. El mismo se conforma por un conjunto de estándares del IETF (*Internet Engineering Task Force*) que suministran servicios de seguridad en la capa IP de la comunicación entre sistemas electrónicos. Se añade a todos los protocolos de niveles superiores que están basados en IPS como TCP (*Transmision Control Protocol*), UDP (*User Datagram Protocol*), ICMP (Internet *Control Message Protocol*), y otros (Olguín, y otros, 2005).

El IPSEC es usado en las conexiones VPN junto a los protocolos L2TP e IKEv2 con ellos se garantiza un servicio rápido y seguro (DeLuz, 2021). Utiliza un método para protegerse de los ataques de denegación de servicio usando ventanas deslizantes, a las cuales se le asigna un número a cada paquete y es aceptada en la recepción del paquete, si se encuentra dentro de la misma ventana o posterior a ella. Luego de esto si se vuelve a recibir un paquete que ya ingresó se descarta inmediatamente, con esto se evita el ataque por reenvío de paquetes.

El L2TP: Es un protocolo de encriptación que en conjunto con Ipsec ofrece altos estándares de seguridad y rapidez en la información. L2TP usa códigos de encriptación AES (Advanced Encryption Standard). El protocolo L2TP canaliza el tráfico PPP (Point-to-Point Protocol) por medio de redes públicas IP, incluyendo distinto tipo de contenido como de voz. Por lo tanto, el manejo de los paquetes de datos del protocolo L2TP son Vulnerables al ataque (Patel, Aboba, Dixon, Zorn, & Booth, 2001). El IKEv2: Es un protocolo flexible utilizado para tunelización, al unirse con Ipsec se logra flexibilidad en la red y permite cambios en ella, al tener pérdida de comunicación permite reconectarse automáticamente.

Figura 2.7: Características del protocolo IPSec.
Fuente: (DeLuz, Sergio, 2021)

En la figura 2.7 se puede observar de una manera más explícita el funcionamiento del túnel IPSec en el cual está formado por el canal lógico. La información viaja de un extremo al otro completamente segura ya que los atacantes al tratar de ingresar se toparán con la protección externa del túnel que son protocolos que no permiten intrusos.

2.9.2 Fases de comunicación Ipsec.

ISAKMP (*Internet Security Association and Key Management Protocol*) el cual es un protocolo criptográfico que permite que en la primera fase se establezca una conexión estable y segura la cual toma el nombre de conexión de control. La misma es usada para pactar los parámetros requeridos para enlazar la segunda fase de la conexión. La comunicación Ipsec está formada por ISAKMP fase 1 y fase 2. En la primera fase se usa protocolo UDP. En la fase 2 tomando la ya existente conexión de control los dispositivos pactan y establecen dos conexiones más, las cuales serán detalladas como una entrante y otra saliente. Estas conexiones van a trasladar el tráfico de información protegido (Marqués, 2016).

2.9.3 Características de Ipsec.

En la figura 2.8 se muestran las características que forman parte de IPSec, y son las siguiente: confidencialidad, integridad, autenticidad, anti-repetición. Ipsec se caracteriza por:

- Confidencialidad: ofrece la seguridad que los datos no sean vistos mientras se transmite.
- Integridad: Válida que al llegar los paquetes estén completos y no hayan pérdidas en la comunicación.
- Autenticidad: Se encarga de verificar la autenticidad del remitente y asegurarse que los datos sean confiables.
- Anti-repetición: Se descarta todos los datos que ya hayan sido recibidos y se genere un reenvío de los mismos.

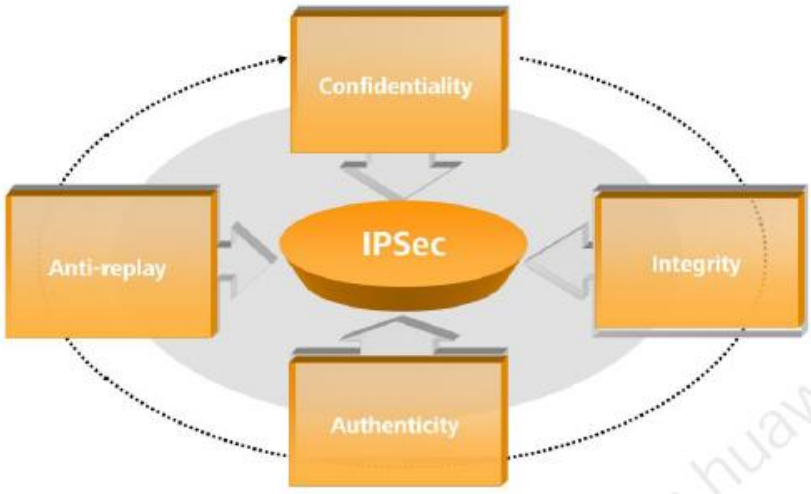


Figura 2.8: Características del protocolo IPSec.
Fuente: (Jimenez, 2020)

2.10 Diferencia entre SD-WAN y WAN tradicional

La tecnología SD-WAN ofrece un menor uso de ancho de banda frente a lo requerido en la WAN tradicional. También SD-WAN permite tener un rendimiento óptimo y controlado de los aplicativos y los costos en la infraestructura son mucho menores frente a la WAN tradicional que exige muchos recursos y un equipamiento complejo. Con SD-WAN se tiene seguridad garantizada en la transmisión de datos. Usando SD-WAN la administración de la red se vuelve más sencilla y ofrece un mejor control sobre toda la WAN por medio de una interfaz gráfica (López, 2020).

2.11 Utilitario utilizado para el diseño y simulación

Para la realización del diseño y simulación de la red planteada se utiliza Gns3 y como elementos internos para interpretar la red MPLS (Pfsense) y para la SD-WAN (Fortigate).

2.11.1 GNS3

Software utilizado para emular, configurar, probar y solucionar problemas de redes virtuales y reales. Le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube (Telectronika, 2018).

2.11.2 Arquitectura de GNS3

Se puede ejecutar la arquitectura de GNS3 de 2 formas:

1. Software GNS3: Se instala todo el programa en la máquina y se toma los recursos de ella.
2. Máquina virtual: Al utilizar Máquina virtual en GNS3 se está utilizando la interfaz gráfica, pero todos los elementos creados y

configurados se guardarán en la máquina virtual instalada o en el servidor GNS3.

2.11.3 Requerimientos técnicos de GNS3

Para la utilización del programa GNS3 en las computadoras o portátiles se debe tener las siguientes consideraciones de acuerdo a lo requerido para cada proyecto.

Tabla 2.1 : Requerimientos para el uso de GNS3

ITEM	Req. Mínimo	Req. Medio	Req. máximo
Sistema Operativo	Windows 7(64 bit) o superior	Windows 7(64 bit) o superior	Windows 7(64 bit) o superior
Procesador	2 o más núcleos lógicos	4 o más núcleos lógicos- AMD-V/RV1 Series o Intel VT-X/EPT	Core i7 o i9 intel CPU R7 o R9 AMD CPU 8 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización	Se requieren extensiones de virtualización.	Se requieren extensiones de virtualización.
Memoria	4 GB RAM	16 GB RAM	32 GB RAM
Espacio en disco	1GB de espacio disponible	Disco de estado sólido (SDD)35 GB de espacio disponible	Disco de estado sólido (SDD)
Notas adicionales	Es posible que necesite almacenamiento adicional para su sistema operativo e imágenes de los equipos.	La virtualización de dispositivos consume mucho procesador y memoria, tener en cuenta si el dispositivo configurado correctamente	La virtualización de dispositivos consume mucho procesador y memoria, tener en cuenta si el dispositivo configurado correctamente

		supera la RAM y la potencia del procesador.	supera la RAM y la potencia del procesador.

Fuente: (Telectronika, 2018)

Para este diseño se cuenta con el equipo que cumple con los requerimientos medio para instalar y ejecutar con normalidad las configuraciones necesarias para realizar la simulación de una red SD-WAN.

2.11.4 Ventajas y desventajas de GNS3

El uso de GNS3 tiene grandes ventajas en el desarrollo del proyecto de la presente tesis, implementando mejores opciones con respecto a Cisco Packet Tracer. A continuación, se detallan las ventajas y desventajas del uso del software GNS3.

Como ventajas de usar GNS3 el programa es compatible con diferentes Sistemas operativos. Además, que no se paga por su uso al ser Open Source. El GUI (*graphical user interface*) es amigable y fácil de usar para las personas que recientemente operen con el programa. El programa trabaja con ISO de dispositivos reales, esto quiere decir que da un ambiente de trabajo real. El análisis y topología de la red se emula en tiempo y ambiente real, usando Wiresshark para la captura de paquetes, generado una amplia documentación en la red para consulta de soportes requeridos.

Entre las desventajas de usar GNS3, se encuentra el requerimiento de instalación de una máquina virtual, dado que la instalación se vuelve un poco compleja, pues se somete a varias actualizaciones que varían los trabajos y configuraciones que se realizan. Entre otra desventaja se tiene el alto consumo de recursos físicos de la RAM. Finalmente, como desventaja también se verifica que los archivos ISO no vienen incluidos en el software.

2.12 Fortigate

El sistema FortiGate nació siguiendo una filosofía simple que implementa las soluciones de seguridad de red más importantes en un solo dispositivo con el mayor rendimiento posible y la interfaz gráfica más sencilla (Fabbri & Volpe, 2013).

FortiGate es una empresa de aplicativos y hardware de seguridad con sede en Sunnyvale, California, Fortinet reporta que tiene más de 21,000 clientes de SD-WAN. Su principal producto es FortiGate Secure SD-WAN, que se basa en capas de seguridad. Actualmente, tiene capacidad de ser virtualizado, implementado como un dispositivo o en una solución Cloud. Se administra mediante una aplicación Cloud o en premisas llamada Forti Manager y permite tener una única ventana de administración de las aplicaciones de SD-WAN, LAN y dispositivos de seguridad (Cordero, 2020).

Características de los equipos Fortigate.

- FortiASIC.
- Antispam.
- VPN IPsec / SSL VPN
- Anti-Virus / Antispyware.
- Control de aplicaciones.
- Web Filtering.
- Reportes Flexibles.
- Optimización WAN.
- IPS.
- DLP.
- Traffic Shaping.

2.12.1 FortiASIC

Los FortiASIC son procesadores creados por Fortinet para el correcto funcionamiento de los equipos Fortigate en los cuales se ejecutan configuraciones como SD-WAN.

El procesador de red FortiASISC está diseñado para acelerar la operación de los servicios de red. Su uso acelera el funcionamiento del cortafuegos, los procedimientos de cifrado, las búsquedas de firmas y las tecnologías

heurísticas. Como resultado de la transferencia, las funciones de procesamiento y análisis de tráfico a nivel de hardware, la detección y eliminación de amenazas se pueden realizar en tiempo real y sin pérdida de ancho de banda de la red, y los procesadores de red se descargan para otras tareas (Petrenko, 2018).

2.12.2 Antispam

Forti Antispam proporciona un enfoque completo y de múltiples capas para detectar y filtrar el spam procesado por las organizaciones. La tecnología de detección de doble paso puede reducir drásticamente el volumen de spam en el perímetro, brindándole un control inigualable de los ataques e infecciones por correo electrónico (Fortinet, 2021).

2.12.3 Tipos de inspección SSL

Las inspecciones SSL se pueden realizar de 2 maneras en Fortigate las cuales se detallan a continuación. La primera manera es *Certificate Inspection*, en la cual la inspección de certificados permite a los FortiGate inspeccionar los encabezados hasta llegar a la capa SSL / TLS. La segunda la *Deep Inspection* la cual se utiliza inspección profunda permite desencriptar el contenido y Fortigate se hace pasar por el destinatario para poder analizar los datos desencriptados y descartar virus en la información, luego de ser analizados los encripta nuevamente y es enviado al destinatario correcto (Fortinet, 2020).

2.12.4 Antivirus

La opción antivirus de Fortigate es usada o activada en cada política que se establece en el equipo. Esta seguridad extra ayuda a prevenir ataques o ingreso de archivos maliciosos que perjudiquen a la red. El antivirus de Fortigate no reemplaza a los antivirus instalados es un complemento para evitar ataques (López, 2020).

2.12.5 Control de aplicaciones

El control por aplicativos ofrece un control granular el cual puede reconocer el tráfico de red generado por diferentes aplicaciones los cuales especifican que acción tomar con el tráfico producido por los aplicativos. El control de aplicaciones descodifica el tráfico por medio de protocolos IPS que analizan el tráfico de aplicaciones. Incluso se utiliza puertos o protocolos sin estándares. Esto ayuda a permitir o bloquear el tráfico de diferentes aplicativos y así mantener un control en la red y administrar de mejor manera el ancho de banda contratado (Fortinet, 2020).

2.12.6 Web filter

El filtrado por web es aplicado en las políticas creadas el cual restringe o controla el acceso web a los usuarios, dentro de los filtros en FortiOS, hay tres componentes principales del filtrado web: (Fortinet, 2020).

- Filtro de contenido web: Realiza bloqueos directos a las páginas web, con patrones o palabras específicas.
- Filtro de URL: Permite el bloqueo de sitios web por patrones o URL específicas.
- Servicio de filtrado web FortiGuard: Bloquea de acuerdo a diferentes categorías que maneja Fortigate y permite controlar la navegación que tendrá el usuario.

2.12.7 Reportes Flexibles.

Los reportes flexibles de Fortigate permiten realizar auditorías en las cuales se pueden descubrir las aplicaciones que se encuentren utilizando los recursos de la red. Con los reportes realizados se puede verificar los usuarios que con mayor frecuencia usan la red y aplicaciones específicas.

2.12.8 Optimización WAN Fortigate.

Para la optimización WAN se reemplazó los enrutadores, SD-WAN otorga asignaciones de rutas dinámicas basadas en políticas de control (Sambrano, 2020).

2.12.9 IPS Fortigate

IPS es un sistema de prevención de intrusos, el cual ayuda a las organizaciones a identificar intrusos, tráfico malicioso y bloqueo de aplicativos que perjudiquen a la red. La tecnología IPS se puede implementar para monitorear el tráfico entrante e inspeccionar ese tráfico en busca de vulnerabilidades y, si se detectan, tomar las medidas adecuadas según lo definido en la política de seguridad como: bloquear el acceso, poner en cuarentena hosts o bloquear el acceso a sitios web externos que podría resultar en una posible infracción (Fortinet, 2020).

2.12.10 DLP Fortigate

DLP es una solución de ciberseguridad que censa, detecta y previene intromisiones de datos. Cumple con bloquear la extracción de datos confidenciales. Las compañías lo utilizan para la seguridad interna y el cumplimiento normativo. Permite a las empresas identificar la pérdida de datos, así como prevenir la salida de datos fuera de la organización y la destrucción no deseada de datos confidenciales o de identificación personal (PII) (Fortinet, 2021).

2.12.11 Traffic Shaping Fortigate

Traffic shaping de Fortigate garantiza que el tráfico que ingresa a la red no consuma más del ancho de banda configurado para la red. El tráfico que sobrepasa la tasa de transferencia máxima está sujeto a vigilancia del tráfico. También se usa para limitar el ancho de banda de una IP en particular.

3 . Capítulo 3 Presentación de la propuesta de red SD-WAN

El diseño de este trabajo fue realizado para una empresa del área de ventas de equipos de construcción. La empresa Construl S.A. se encarga de importar, vender, tener stock en bodega y dar mantenimiento a los equipos vendidos. Para el diseño primero se crean segmentos de redes los cuales puedan ser utilizados por cada área y manejar un control en la red. Se limita el acceso al Internet a las diferentes áreas permitidas. Para navegar en Internet se realiza un control por aplicativos de navegación, esto permite controlar la navegación y asegurar que el uso de los elementos de la empresa sea netamente para trabajo y no exista distracción en el desarrollo de las actividades.

La empresa Construl S.A al ser importadora de maquinaria pesada de construcción requiere tener alta disponibilidad en la red y continua comunicación para realizar los debidos contactos con las aduanas y los países de importación. Para mantener la comunicación activa se contratan 2 enlaces de Internet por diferentes proveedores. Esto asegura que si una infraestructura de 1 proveedor falla o presenta intermitencias pueda pasar el tráfico por el otro proveedor inmediatamente sin que la empresa sienta afectación o pérdida del servicio. También para una mejor distribución de la red, se generan reglas para que determinados dispositivos utilicen una salida específica y de caerse esa salida conmuten inmediatamente por el otro proveedor.

3.1 Justificación de las configuraciones utilizadas en el diseño de la red SD-WAN.

En el desarrollo de la red SD-WAN se suscitan varios eventos. Para mejorar el rendimiento y control en la red se delimitan los permisos para cada segmento que serán incluidos en los equipos Fortigate a nivel de IP LAN. Se debe configurar en el Fortigate las interfaces WAN (proporcionadas por el proveedor) y LAN (asignadas por el administrador de red).

Una vez realizadas las configuraciones de la WAN en el Fortigate se debe realizar el encapsulamiento virtual de la WAN y con esto se obtiene el SD-WAN. Luego de configurar la SD-WAN se debe realizar una política en la cual indique la ruta desde que puerto va a ser generado el tráfico. Para este diseño se toma como origen el puerto 4 (LAN) y como puerto destino el puerto WAN virtual (SD-WAN). Para completar la configuración hacia el Internet se debe crear una ruta estática donde se indique que cualquier tráfico no especificado vaya hacia la SD-WAN.

Luego de tener ya configurada la salida al Internet por la SD-WAN se debe realizar la configuración del SLA para determinar la mejor ruta que la SDWAN deba elegir. Posteriormente se realiza el monitoreo SLA, con la información que arroja se configura las reglas SD-WAN que determinará la mejor ruta que tendrá la información para llegar a su destino.

Para establecer la comunicación de la matriz con los diferentes extremos se crea en el Fortigate túneles Ipsec asignando IP's identificativa para cada túnel. Luego de crear túneles hay que agregar los túneles a las configuraciones SD-WAN en el Fortigate. Se crea una loopback para más adelante utilizarlo para realizar monitoreo SLA del sistema y se configura el BGP en el Fortigate para propagar las rutas de forma dinámica a través de lso túneles, creando el monitoreo SLA. Se utiliza l IP loopback de los puntos donde se quiere llegar como ejemplo. En el punto matriz se debe configurar las ip loopback de las sucursales y datacenter ya que son los puntos que se mantendrá la comunicación.

Para que el tráfico sea direccionado por los túneles se realizan las políticas de seguridad tanto para la comunicación entre matriz, sucursal y otra política para el tráfico entre sucursales. Luego de configurar el monitoreo SLA de los túneles con la información que arroja se configura la regla SD-WAN para determinar la mejor ruta de comunicación. Par culminar la configuración del Fortigate de la red de Construl S.A. se configura dentro de la política de Internet controles de aplicativos y navegación para restringir la salida.

3.2 Diseño de red propuesto desarrollado en GNS3

A continuación, en la Figura 3.1 se muestra el diseño planteado el cual cuenta con 2 sucursales, una ubicada en la ciudad Guayaquil y otra ubicada en la ciudad Quito. El punto matriz de datos e internet se comunica con todos los extremos. La parte operativa de Construl S.A. se comunica con Datacenter donde se encuentran instalados los servidores.

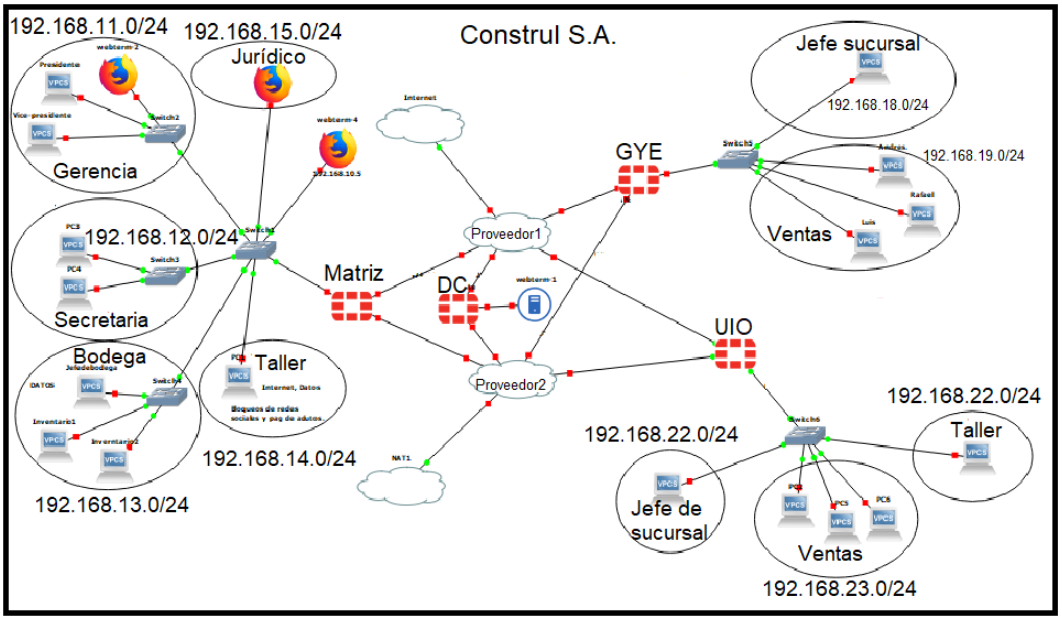


Figura 3.1: Diseño de comunicación de la red SD-WAN Construl S.A.

Fuente: Autor

Dado el diseño propuesto se tienen los siguientes sujetos de la red, los cuales se detallan en la Tabla 3.1, con los que se logra la comunicación entre matriz, los puntos extremos y Datacenter. Para la comunicación entre las sucursales y Datacenter se usa los túneles que tiene levantado matriz con cada extremo y por medio de una política creada en el Fortigate en matriz se genera la comunicación entre toda la red.

Tabla 3.1: Sujetos que intervienen en la RED.

Sujetos que intervienen en la RED	Cantidad.	Características.
Proveedor 1 (Telconet)	1	WAN
Proveedor 2 (CNT)	1	WAN
Sucursales	2	GYE,UIO salida por los 2 proveedores
Datacenter	1	Salida por los 2 proveedores
Matriz	1	Maneja centralizado de la red planteada.

Fuente: Autor.

La red de la empresa Construl S.A también cuenta con elementos que conjuntamente con los sujetos de la red hacen que la red SD-WAN funcione correctamente, se tenga alta disponibilidad en la red y se pueda controlar la navegación por aplicativos o preferencia dependiendo del administrador de la red. En la Tabla 3.2 se detallan los elementos que se utilizarán para la elaboración del proyecto.

Tabla 3.2: Elementos de la RED

Elementos de la RED	Cantidad	Característica
Fortigate	4	Elementos en el cual se configuran las políticas y controles.
Switch no administrable	6	Usado para la distribución interna de los puntos.
Central telefónica	1	Elemento usado para la telefonía de la empresa.
Computadoras	20	Equipos usados en la empresa

Fuente: Autor.

3.3 Análisis del ancho de banda requerido.

De acuerdo con la tabla 3.3 de valores de ancho de banda de la empresa AT&T y los parámetros del Codec G.711 se procede a calcular lo requerido de ancho de banda de acuerdo a los requerimientos de cada punto.

Tabla 3.3 Cálculo de consumo de ancho de banda Matriz

Actividad	Tamaño de datos
1 correo electrónico (sin archivos adjuntos)	20 kbps
1 correo electrónico (con archivos adjuntos estándar)	300 kbps
1 teléfono Codec G.711	64 kbps
1 usuario	512 kbps

Fuente: (AT&T, 2021)

Matriz

Para los correos se tiene estimado recibir un máximo de 500 correos diarios, de los cuales 100 no tendrán archivos adjuntos y 400 si tendrán archivos adjuntos de cotizaciones y otros archivos. Se plantea ecuación para obtener los anchos de banda necesarios.

$$Ancho\ de\ Banda = Capacidad \cdot Cantidad\ total \quad (4.1)$$

Se sustituyen los valores en la ecuación 1 tomando como referencia 100 correos diarios sin adjuntos. Utilizando los valores correspondientes da un resultado de 2000 kbps el ancho de banda.

$$Ancho\ de\ banda = 20\ kbps \cdot 100 = 2000 kbps \quad (4.2)$$

Sustituyendo en la ecuación 4.1 las estimaciones realizadas el ancho de banda para correos con adjunto con un promedio de 400 correos sería:

$$Ancho\ de\ banda = 300\ kbps \cdot 400 = 120\ 000\ kbps\ .\ (4.3)$$

Realizando la sustitución de valores de los correos con adjunto se alcanza un resultado de 120 000 kbps.

Para obtener el ancho de banda total se suma los resultados de correos con adjuntos y correos sin adjuntos como se muestra a continuación:

$$\sum 2\ 000\ kbps + 120\ 000\ kbps = \mathbf{122\ 000\ kbps}\ \ (4.4)$$

Sustituyendo en la ecuación 1 los valores de diez teléfonos con codec de sesenta kbps:

$$Ancho\ de\ banda\ Telefonía = 64\ kbps \cdot 10 = \ \mathbf{640\ kbps}\ \ (4.5)$$

Para estimar el ancho de banda necesario en la navegación, se considera que los usuarios (gerencia, jurídico y taller) no tendrán visualización de redes sociales ni videos, 512 kbps para navegación en páginas que no requieran mayor consumo. Sustituyendo en la ecuación 1 se obtiene los siguientes resultados:

$$Ancho\ de\ banda\ Navegación = 512\ kbps \cdot 5\ usuarios = \mathbf{2560\ kbps}\ (4.6)$$

Tabla 3.4 Cálculo de consumo de ancho de banda Matriz

Aplicación	Ancho de banda requerido	Detalles
Correos	122000 kbps	Considerando un promedio de 500 correos.
Impresoras	5 kbps	Host
Telefonía	640 kbps	10 teléfonos
Navegación	2560 kbps	Navegación sin redes sociales.

Fuente: Autor.

Para obtener el ancho de banda total que se usará en matriz se realiza la suma de las estimaciones realizadas de los anchos de banda usados en cada aplicativo. El equivalente a 125,21 Mbps corresponde al ancho de banda requerido por correos, impresoras, telefonía y navegación.

$$\sum TOTAL = 122\,000 + 5 + 640 + 2560 = \ 125205\ kbps = \mathbf{125,21\ Mbps}$$

El ancho de banda requerido para la Matriz es de 125,21 Megas, con este valor calculado se puede saber cuánto se debe contratar en cada proveedor de servicio y tener una mejor visión de cómo funcionará las configuraciones de SD-WAN. Usualmente se contrata la misma cantidad de megas tanto para enlace principal como backup.

Sucursales GYE

De la misma manera que se realiza el análisis en matriz se usa la misma metodología para realizar los cálculos en sucursal GYE. Se reemplaza los valores en la ecuación 1 para obtener los anchos de banda.
Se llegan a los resultados siguientes con la información detallada para este punto extremo GYE.

Tabla 3.5 Cálculo de consumo de ancho de banda sucursal GYE

Aplicación	Ancho de banda requerido	Detalles
Correos	46000 kbps	Considerando un promedio de 200 correo diarios de los cuales 50 serán sin adjuntos
Impresoras	5 kbps	Host
Telefonía	256 kbps	4 Teléfonos
Navegación	512 kbps	Navegación sin redes sociales.

Fuente: Autor.

Para obtener el ancho de banda total que se usará en sucursal GYE se realiza la suma en kbps de los anchos de banda usados en cada aplicativo. El equivalente a 46,77 Mbps corresponde al ancho de banda requerido por correos, impresoras, telefonía y navegación.

$$\sum TOTAL = 46000 + 5 + 256 + 512 = \ 46773\ kbps = \mathbf{46,77\ Mbps}$$

El ancho de banda requerido para Sucursal GYE es de 46,77 Megas, este valor va en relación a la cantidad de personal que cuenta es menor y con relación a Matriz y sucursal UIO.

Sucursal UIO

De igual manera para el punto de sucursal UIO se usa el análisis de matriz y se usa la misma metodología para realizar los cálculos. Utilizando la ecuación 1 para determinar los anchos de banda.

Tabla 3.6 Cálculo de consumo de ancho de banda sucursal UIO

Aplicación	Ancho de banda requerido	Detalles
Correos	46000 kbps	Considerando un promedio de 200 correo diarios de los cuales 50 serán sin adjuntos.
Impresoras	5 kbps	Host
Telefonía	320 kbps	5 teléfonos
Navegación	1024 kbps	Navegación sin redes sociales.

Fuente: Autor.

Para obtener el ancho de banda total que se usará en sucursal UIO se realiza la suma en kbps de los anchos de banda usados en cada aplicativo.

El equivalente a 47,35 Mbps corresponde al ancho de banda requerido por correos, impresoras, telefonía y navegación.

$$\sum TOTAL = 46000 + 5 + 320 + 1024 = 47349\ kbps = \mathbf{47,35\ Mbps}$$

El ancho de banda requerido para Sucursal UIO es de 47,35 Megas. El valor de ancho de banda va en relación al personal y áreas que cuenta sucursal.

Datacenter.

Correos: se tiene estimado recibir un máximo de 900 correos diarios en toda su red, de los cuales 300 no tendrán archivos adjuntos y 600 si tendrán archivos adjuntos de cotizaciones y otros archivos.
Sustituyendo en la ecuación 1 las estimaciones realizadas el ancho de banda sería:

$$Ancho\ de\ banda\ \text{sin}\ adjuntos = 20\ kbps \cdot 300 = 6000\ kbps.$$

Sustituyendo en la ecuación 4.1 los valores para determinar el ancho de banda de correos con adjunto se obtienen:

$$Ancho\ de\ banda\ \text{con}\ adjuntos = 300\ kbps \cdot 600 = 180\ 000\ kbps$$

El total de ancho de banda considerando las estimaciones realizadas en cuanto a la mensajería es de:

$$\sum 6\ 000\ kbps + 180\ 000\ kbps = \mathbf{186\ 000\ kbps}$$

En el análisis de la telefonía se considera que, Construl S.A tendrá configurado el servidor en datacenter. Se sustituyen los valores en la ecuación 1 y con19 teléfonos y un consumo de 64 kbps se obtiene que:

$$Ancho\ de\ banda\ Telefonía = 64\ kbps * 19 == \mathbf{1216\ kbps}$$

Tabla 3.7 Cálculo de consumo de ancho de banda sucursal UIO

Aplicación	Ancho de banda requerido	Detalles
Servidor de correos y navegación para actualizar equipos.	186000 kbps	Considerando 900 correos que pasen por el servidor.
Telefonía	1216 kbps	Central interna.

Fuente: Autor.

Para obtener el ancho de banda total que se usará en Datacenter se realiza la suma en kbps de los anchos de banda usados en cada aplicativo. El equivalente a 182,22 Mbps corresponde al ancho de banda requerido por servidor de correos y navegación para actualización de equipos, y telefonía.

$$\sum TOTAL = 187216\ kbps = \mathbf{187,22\ Mbps}$$

El ancho de banda requerido para Sucursal UIO es de 187,22 Megas usados de acuerdo con los recursos que solicita la empresa Construl S.A.

3.4 Distribución de la red Construl S.A

En el apartado 3.4 se describe la distribución que la empresa Construl S.A. tendrá a nivel de cada área y también la distribución que cada punto tiene a nivel WAN (Ips brindadas por los proveedores) y LAN (Configuración de la red interna para cada área).

3.4.1 Distribución de permisos de Internet y datos.

Para la distribución de la red se estudia las necesidades requeridas en cada área, también se realizan bloqueos para que no se pueda ingresar a las redes sociales y páginas de videos. Los bloqueos se realizan por el alto

grado de distracción que generan en los trabajadores y la baja de productividad que esto genera (eltelegrafo, 2021). Otro de los motivos de mantener los bloqueos es la seguridad en la red y evitar así la saturación, a continuación, en la Tabla 3.8 se puede observar la distribución que se realiza de acuerdo a la actividad de cada área.

Tabla 3.8 Distribución y permisos de la red.

Accesos permitidos		
Elementos	Distribucion	Detalle
Matriz	Gerencia	Comunicación de Internet y datos.
	Secretaria	Comunicación de datos.
	Bodega	Comunicación de datos.
	Taller	Comunicación de Internet y datos.
	Jurídico	comunicación de Internet.
Sucursal norte GYE	Jefatura sucursal	Comunicación de Internet y datos.
	Ventas	Comunicación de datos.
Sucursal centro UIO	Jefatura sucursal	Comunicación de Internet y datos.
	Ventas	Comunicación de datos.
	Taller	Comunicación de Internet y datos.
Datacenter	Servidores	Comunicación de Internet y datos.

Fuente: Autor.

3.4.2 Distribución de las redes WAN.

La distribución de la red WAN depende de las IPs asignadas por cada proveedor, pero para el diseño y simulación de la red SD-WAN se han tomado las siguientes WAN detallada en la Tabla 3.9, se detallará las IPs que pertenecen a cada proveedor.

Tabla 3.9 Distribución de las redes WAN

Identificación de los elementos	Proveedor	IP	MÁSCARA	Gateway
Matriz	Proveedor1	172.16.100.1	255.255.255.0	172.16.100.4
	Proveedor2	172.16.90.1	255.255.255.0	172.16.90.4
Sucursal norte GYE	Proveedor1	172.16.150.1	255.255.255.0	172.16.150.2
	Proveedor2	172.16.70.1	255.255.255.0	172.16.70.2
Sucursal centro UIO	Proveedor1	172.16.200.1	255.255.255.0	172.16.200.2
	Proveedor2	172.16.80.1	255.255.255.0	172.16.80.2
Datacenter	Proveedor1	172.16.110.1	255.255.255.0	172.16.110.2
	Proveedor2	172.16.60.1	255.255.255.0	172.16.60.2

Fuente: Autor

3.4.3 Distribución de las redes LAN.

Para la distribución LAN se divide de acuerdo a las necesidades de cada área y posibles expansiones de equipos terminales. De acuerdo con la distribución presentada en la tabla 3.10 se observan los recursos necesarios para la comunicación de la empresa Construl S.A. hacia los extremos y viceversa.

Tabla 3.10 Distribución de las redes WAN

Identificación	Detalle	IP	Gateway
Matriz	Administrativa	192.168.10.0/24	192.168.10.1
	Gerencia	192.168.11.0/24	192.168.11.1
	Secretaria	192.168.12.0/24	192.168.12.1
	Bodega	192.168.13.0/24	192.168.13.1
	Taller	192.168.14.0/24	192.168.14.1
	Jurídico	192.168.15.0/24	192.168.15.1
Sucursal norte GYE	Jefatura sucursal	192.168.18.0/24	192.168.18.1
	Ventas	192.168.19.0/24	192.168.19.1
Sucursal centro UIO	Jefatura sucursal	192.168.22.0/24	192.168.22.1
	Ventas	192.168.23.0/24	192.168.23.1
	Taller	192.168.22.0/24	192.168.22.1
Datacenter	Servidores	192.168.30.0/24	192.168.30.1

Fuente: Autor

3.5 Configuración de las interfaces WAN y LAN en equipo Fortigate.

Las configuraciones de la WAN y la LAN se las realiza en el Fortigate para poder verificar aspectos básicos y poder ingresar en modo gráfico, también es necesario configurar la WAN para luego poder realizarla la SD-WAN, a continuación, se mostrará cómo se realiza la configuración de la WAN y la LAN por medio de comandos y como se refleja en modo gráfico.

Estas primeras configuraciones darán paso a realizar las interfaces lógicas para luego poder continuar con el SD-WAN. Las IP WAN son dadas por cada proveedor dependiendo su pool de IP, las IP LAN son elegidas y

asignadas por el administrador de la red de acuerdo a los requerimientos necesarios de la empresa Construl S.A.

3.5.1 Configuración de la WAN.

Cada proveedor va a proporcionar una IP WAN y se procede a configurar de acuerdo a cada punto asignado como se muestra a continuación en el extracto del código de configuración de la WAN del proveedor 1. Esta misma codificación se debe replicar para las WAN de acuerdo a las IP's indicadas por los proveedores. En la Figura 1 del anexo 1 se muestra un consolidado de todos los puntos con los que los equipos Fortigate se van a comunicar con la red del proveedor 1 y 2. Para configurar las IPs brindadas hay 2 formas: código (CLI) y por modo gráfico.

```
Matriz # config system interface
        edit "port1"
        set vdom "root"
        set ip 172.16.100.4 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type physical
        set alias "WAN1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
next
```

Figura 3.2: Configuración del puerto WAN en el Fortigate.

Fuente: Autor

En la primera línea del código de la figura 3.2 se registra el comando para ingresar a la configuración de las interfaces. Luego en la segunda línea se edita el puerto donde se va a conectar el cable proveniente del proveedor. Después la tercera línea administra la configuración global de FortiGate. A continuación, se agrega la IP brindada por el proveedor. De forma continua en la quinta línea se agrega los permisos que se van a tener en el puerto. Además, en la sexta línea se especifica que el tipo de conexión que será física y en la séptima se detalla el nombre que va a llevar la interfaz. En la octava línea se declara la recepción de mensajes LLDP y en la novena se

detalla el rol que va a tomar en la interfaz. A su vez en la décima línea se define el número de interfaz que pertenece.

3.5.2 Configuración de la LAN.

Para la administración interna de Construl S.A. se requiere configurar segmentos los cuales serán usados por los usuarios de la empresa. Se configura también las subredes dentro del mismo puerto las cuales van a ser usadas para las diferentes áreas de la empresa. Para realizar las configuraciones de las redes LAN existen 2 formas de hacerlo tanto por CLI o modo gráfico como se muestra a continuación en el extracto de código para configurar las redes LAN. En las Figura 2 del anexo 1 se muestra un consolidado de la configuración LAN de todos los puntos.

```
edit "port4"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set stpforward enable
        set type physical
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
        set snmp-index 4
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip 192.168.11.1 255.255.255.0
                set allowaccess ping fgfm fabric
            next
            edit 2
                set ip 192.168.12.1 255.255.255.0
                set allowaccess ping fgfm fabric
            next
            edit 3
                set ip 192.168.13.1 255.255.255.0
                set allowaccess ping fgfm fabric
            next
            edit 4
                set ip 192.168.14.1 255.255.255.0
                set allowaccess ping fgfm fabric
            next
        end
    next
```

Figura 3.3: Configuración del puerto LAN en el Fortigate.

Fuente: Autor

En la figura 3.3 se detalla la configuración del puerto LAN en la cual se realiza una configuración igual a la del puerto WAN. Se toman en consideración la declaración de las IP'S internas y agregando las IP's secundarias.

3.6 Configuración de SD-WAN en equipo Fortigate

Una vez realizada la configuración de la WAN y LAN dentro de los Fortigate se procede a la configuración del SD-WAN en los equipos de matriz, sucursales y datacenter de Construl S.A. Este encapsulamiento virtual de las WAN se lo puede realizar por modo comando (CLI) o en modo gráfico, dependiendo de la destreza de la persona que realiza las configuraciones. Luego de cargar las 2 WAN en la Interfaz virtual SD-WAN se debe configurar la política para que todo el tráfico llegue al mundo por la Interfaz lógica creada. Para completar el enrutamiento para la navegación se debe configurar una ruta por defecto hacia la interfaz lógica creada, a continuación, en las imágenes se va a detallar como realizarlo por CLI o modo gráfico.

Para la configuración de la SD-WAN se usa la interfaz física WAN configurada y para el Gateway se usan los parámetros indicados por el proveedor como se observa en el extracto de código de la configuración de la SD-WAN. En las figuras 3 del anexo 1 se muestra un consolidado de la configuración SD-WAN de todos los puntos.

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.100.1
        next
        edit 2
            set interface "port2"
            set gateway 172.16.90.1
        next
```

Figura 3.4: Virtualización de las WAN de los proveedores para formar el SD-WAN.

Fuente: Autor

En la figura 3.4 La primera línea del código sirve para ingresar a las configuraciones y virtualizar la WAN, a continuación, la segunda línea activa la virtualización, luego en la tercera línea se ingresa el parámetro para configurar los miembros de la SD-WAN, después se edita los puertos y se agrega la IP Gateway que el proveedor indica.

3.6.1 Configuración de la política de salida al mundo por medio de la interfaz virtual.

Para tener navegación a través de la SD-WAN, se declara que todo el tráfico que viene de la LAN sea direccionado a la interfaz lógica creada (SD-WAN), también se activa el perfil NAT para que el tráfico pueda salir por la WAN de los proveedores. En esta política se puede realizar también la asignación de las LAN que pueden navegar y generar control a nivel de navegación, en la Figura 3.5 y 3.6 se indican las configuraciones realizadas de acuerdo a los requerimientos establecidos por la empresa Construl S.A. en matriz, datacenter y sucursales.

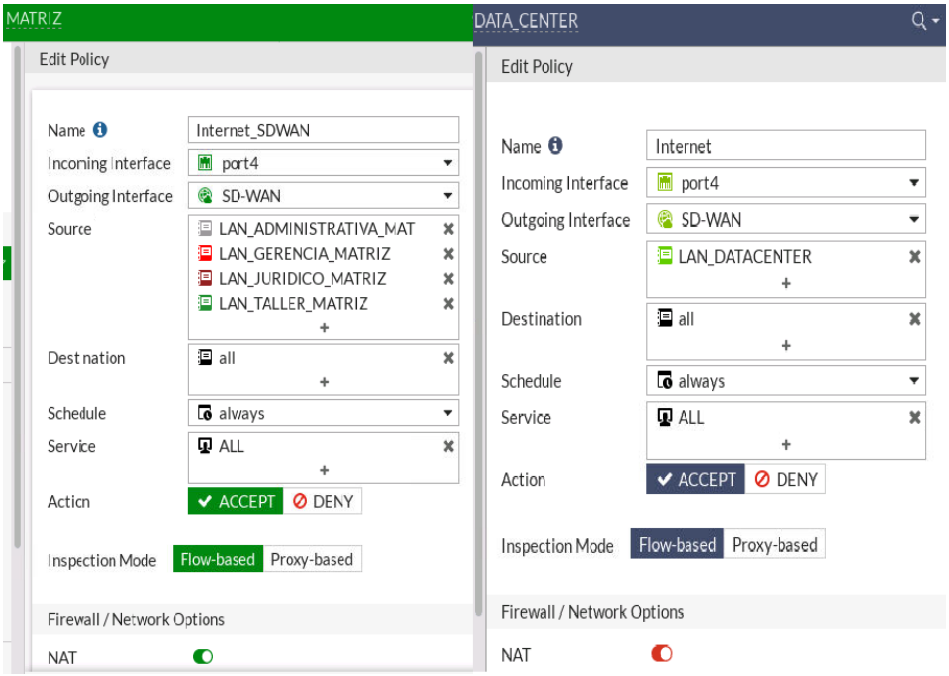


Figura 3.5: Configuración de la política para salida al Internet por la SD-WAN (Matriz, datacenter)

Fuente: Autor

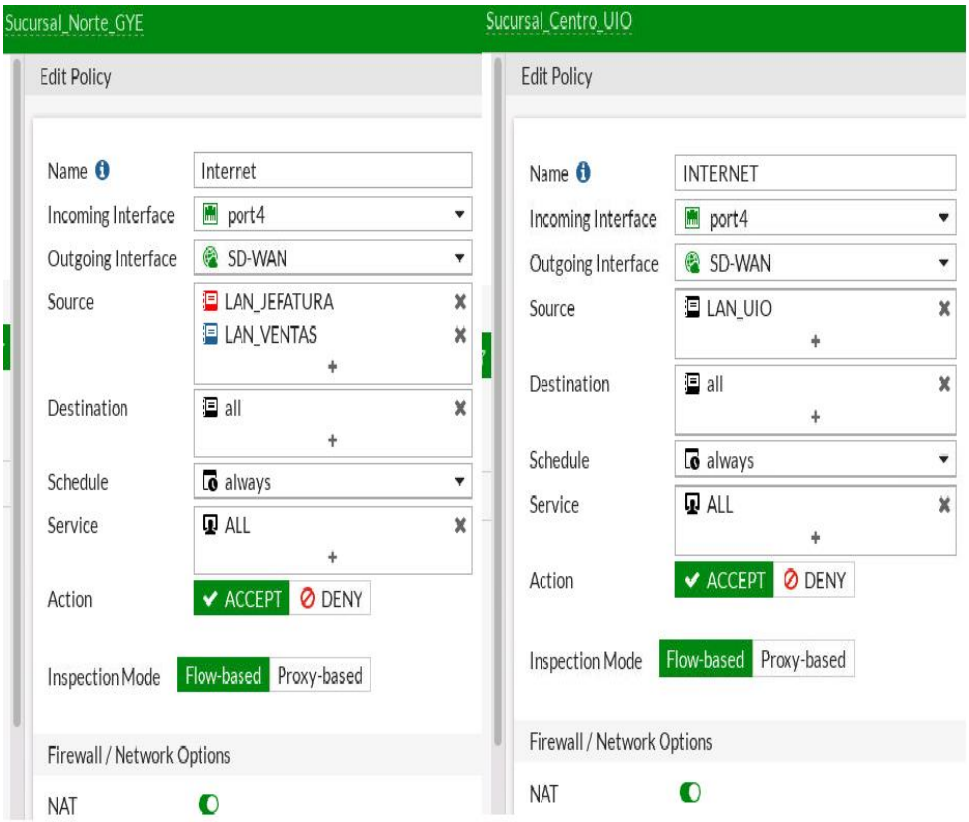


Figura 3.6: Configuración de la política para salida al Internet por la SD-WAN (sucursal GYE, sucursal UIO.)

Fuente: Autor

Como se observa en las Figuras 3.5 y 3.6 en las cuales se detalla como primer punto el nombre que tendrá la política. A continuación, se declara el puerto de donde proviene el tráfico y también en la siguiente línea se indica la interfaz por donde saldrá al mundo en este caso la interfaz lógica SD-WAN. Luego se declara IP's o segmento de IP que permitirá la salida del tráfico y como destino a todos lados, también se permite todo el tráfico en servicios sin restricciones d puertos y por último se activa el NAT para que tenga salida por el Internet.

3.6.2 Configuración de ruta estática.

Para completar las configuraciones de salida al mundo por medio de la interfaz lógica se debe crear ruta por defecto 0.0.0.0 hacia la interfaz del SD-WAN como se muestra en la figura 3.7. Esta configuración va a ayudar a enrutar el tráfico que no tenga ruta específica en las redes de datos, toda información desconocida será enviada por la ruta por defecto.

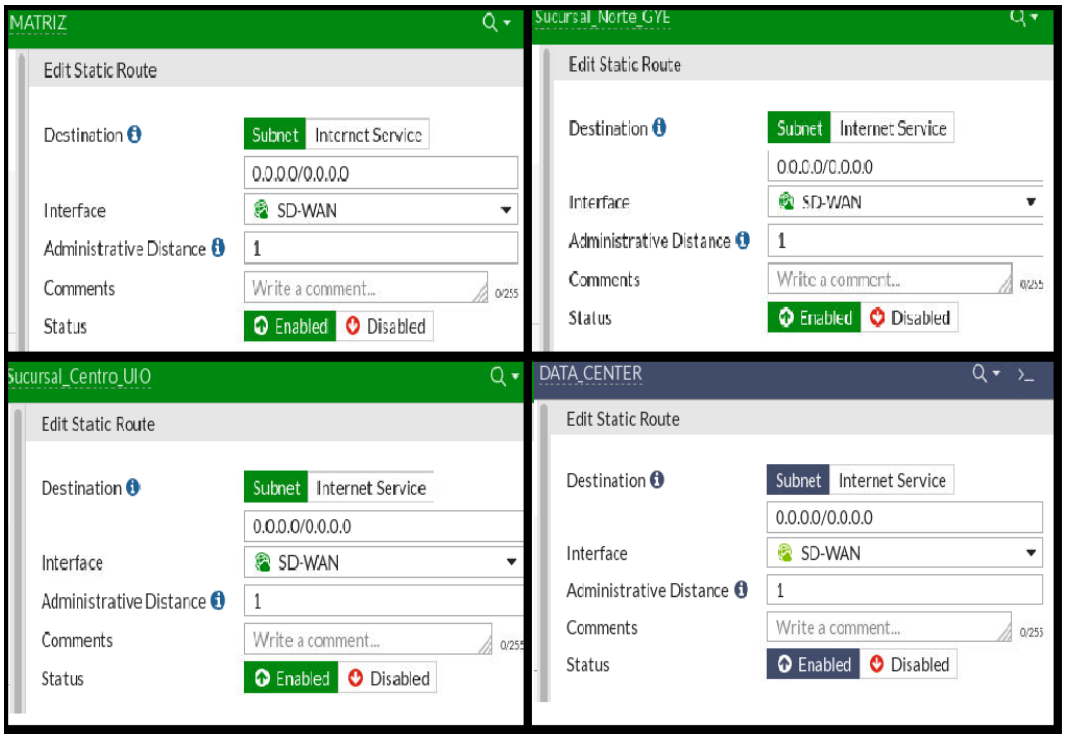


Figura 3.7: Configuración de rutas para salida al Internet por la SD-WAN

Fuente: Autor

3.7 Configuración del SLA para determinar mejor ruta entre proveedor 1 y proveedor 2.

Para el desarrollo y optimización de los recursos de red de la empresa Construl S.A. se realiza la configuración de Preformance SLA y SD-WAN rule. Una vez realizada la configuración se obtendrá mejor disponibilidad y no se genera saturación o retardo en la red. Se realiza la configuración para que la comunicación se ejerza de acuerdo al proveedor con menor tiempo de respuesta, se obtiene un beneficio al realizar de esta manera la configuración, ya que si un proveedor se encuentra intermitente la información se verificará en alto tiempo de respuesta (latencia) y tomará la ruta por el proveedor 2 o viceversa. En la figura 3.8 se muestra el monitoreo y tiempo de respuesta de las WAN de ambos proveedores en matriz con la cual se podrá elegir el mejor camino por medio de la SD-WAN rule.

3.7.1 Cumplimiento SLA

Para verificar el desempeño SLA se realiza un monitoreo constante hacia los servidores 8.8.8.8 y 4.2.2.2. Como se observa en la Figura 3.8 los cuales miden el tiempo de latencia y permiten validar la respuesta al mundo de cada proveedor.

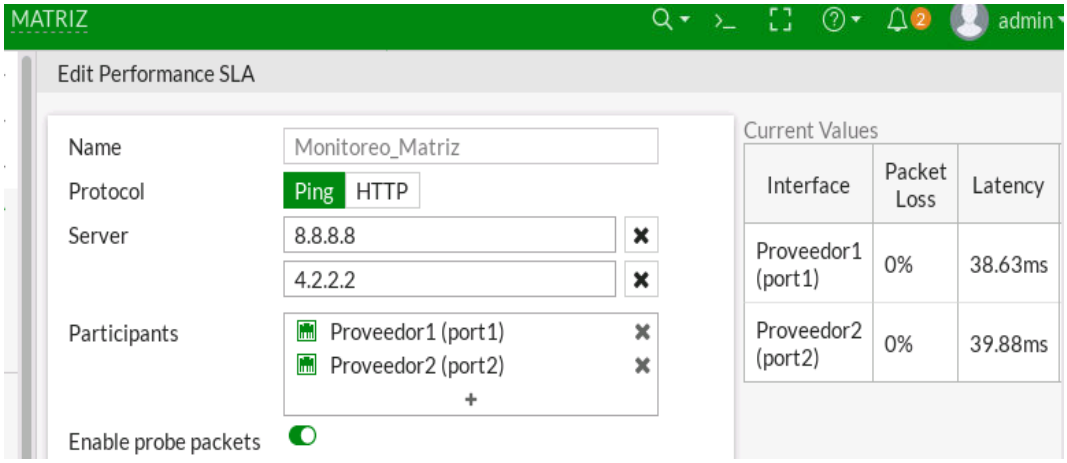


Figura 3.8: Configuración de performance SLA del SD-WAN

Fuente: Autor

En la Figura 3.9 muestra de manera gráfica el monitoreo de las WAN que se encuentran configuradas en el FortiGate. En la cual se observa cuando una de ellas se encuentre fallando o intermitente. Esto permite elegir la ruta que los datos tomarán para mantener la comunicación. Las líneas presentadas en azul y amarillo representan cada una a un proveedor de datos o Internet y con esto se valida la operatividad de cada uno.

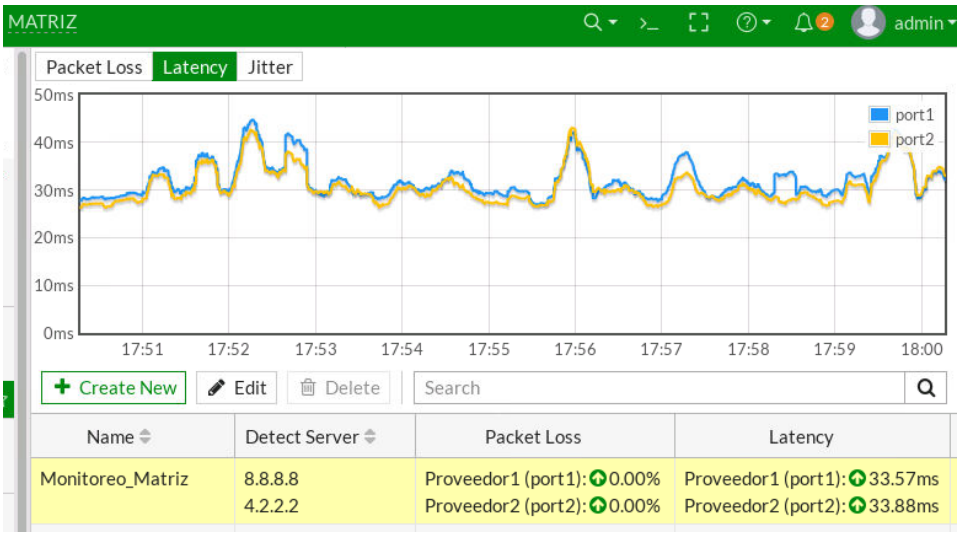


Figura 3.9: Visualización del monitoreo performance SLA

Fuente: Autor

3.7.2 SD-WAN rule

Una vez realizada el preformance SLA se configuran las reglas para que tome el camino con menor latencia como se muestra en la Figura 3.10. La mejor ruta va a ser tomada de acuerdo con el monitoreo que realiza constantemente hacia el Internet.

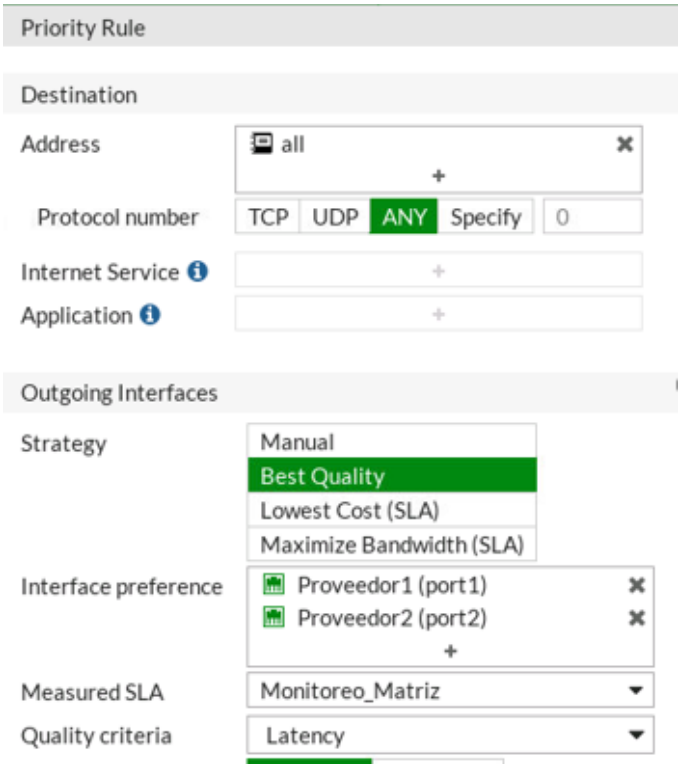


Figura 3.10: Configuración de la regla SD-WAN

Fuente: Autor

3.8 Comunicación entre las diferentes sucursales a través de túneles IPSec.

Para realizar la comunicación entre matriz y las sucursales de la empresa Construl S.A. se levantan túneles IPSec. Estos túneles tienen la particularidad de ser confiables, siempre estar activos y disponibles para establecer la comunicación de información netamente de datos. Los túneles que se crean se encapsularan en la SD-WAN para entrar a ser parte de la red con alta disponibilidad.

Al desarrollar los túneles se tomará como referencia la matriz en la cual luego realizará la creación de políticas, monitoreo y reglas de SD-WAN para

poder lograr túneles dinámicos entre las sucursales y datacenter. Así se logra que todos los puntos se comuniquen entre sí, sin tener que levantar túneles entre ellos como se muestra en la Figura 3.11 en la cual todas las sucursales se conectan por medio de túneles hacia matriz pasando por la nube de Internet y es en la matriz donde se produce la comunicación hacia los diferentes extremos.

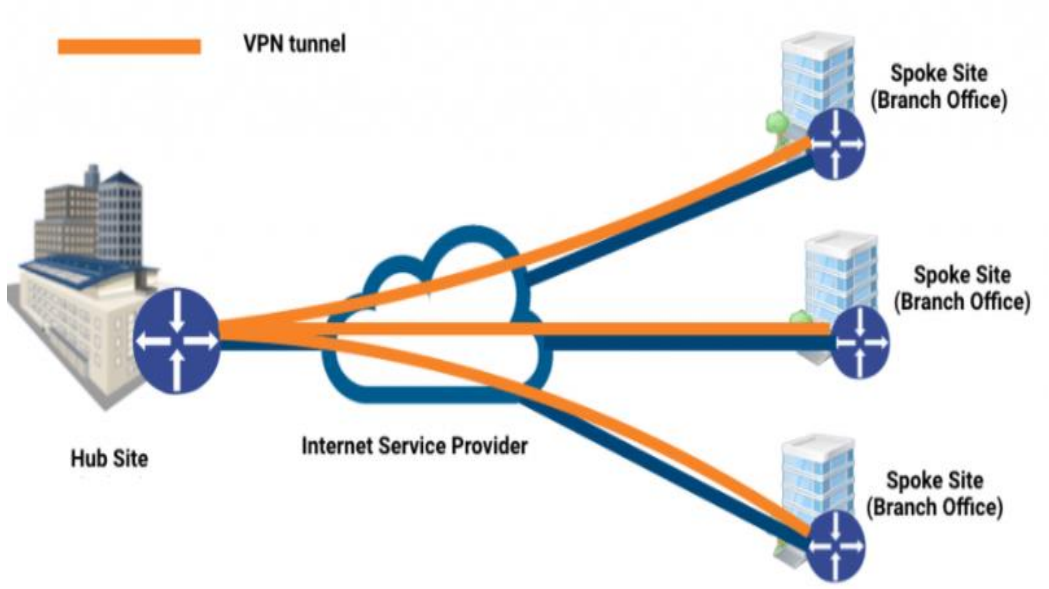


Figura 3.11: Configuración de túnel con SD-WAN.
Fuente: (Gridelli, 2020)

3.8.1 Asignación de Ip para los túneles IPSec.

Para la comunicación la matriz, sucursales y datacenter se asignan IPs para configurar en los túneles. Los cuales deben registrar la IP de origen del túnel y la IP de extremo del túnel para saber llegar al otro punto. Del punto extremo se guarda la configuración, tomando en cuenta que la IP de este punto extremo se convertirá en la IP de origen, y la IP de origen se convertirá en la IP del extremo. A continuación, se presenta las IPs configuradas para cada punto teniendo en cuenta las consideraciones antes indicadas.

Tabla 3.11 Distribución de las IP para las VPN IPSec.

VPN-IPSec	Interfaces	IP ORIGEN	IP EXTREMO
Matriz-DC	wan 1	10.10.10.1	10.10.10.2
	wan 2	10.10.10.3	10.10.10.4
DC-Matriz	wan 1	10.10.10.2	10.10.10.1
	wan 2	10.10.10.4	10.10.10.3
Matriz-Suc GYE	wan 1	10.10.20.1	10.10.20.2
	wan 2	10.10.20.3	10.10.20.4
Suc GYE-Matriz	wan 1	10.10.20.2	10.10.20.1
	wan 2	10.10.20.4	10.10.20.3
Matriz-Suc UIO	wan 1	10.10.30.1	10.10.30.2
	wan 2	10.10.30.3	10.10.30.4
Suc UIO-Matriz	wan 1	10.10.30.2	10.10.30.1
	wan 2	10.10.30.4	10.10.30.3

Fuente: Autor

3.8.2 Levantar túneles IPSec

Para establecer la comunicación entre los diferentes puntos se establece cifrados de seguridad y rutas directas tomando como Gateway remoto el punto donde se va a establecer la comunicación como se subraya en las figuras siguientes.

3.8.3 Configuración de los túneles IPSec en la SD-WAN.

Luego de realizar la configuración de los túneles, para que la comunicación entre los extremos, matriz y viceversa se de, deben incluirse en la interfaz lógica SD-WAN. De acuerdo con las reglas configuradas para el SD-WAN, es necesario que se identifiquen con las IP antes descritas en la tabla 3.11.

En la figura 3.12 se detalla la configuración por CLI, también se observa la visualización en modo gráfico de los túneles incluidos en la interfaz lógica, los cuales permitirán la comunicación entre la sucursal hacia los diferentes extremos ya declarados en la SD-WAN. En cada extremo se debe realizar la misma configuración presentada en la figura 3.12 pero con respecto a los túneles hacia matriz. Para completar la configuración de los túneles y tener comunicación se deben agregar 2 políticas (una saliente de

la LAN y una entrante a la LAN), y para pruebas se deben agregar rutas estáticas ya que para el diseño de la empresa Construl S.A. se usará propagación de las redes por medio de BGP.

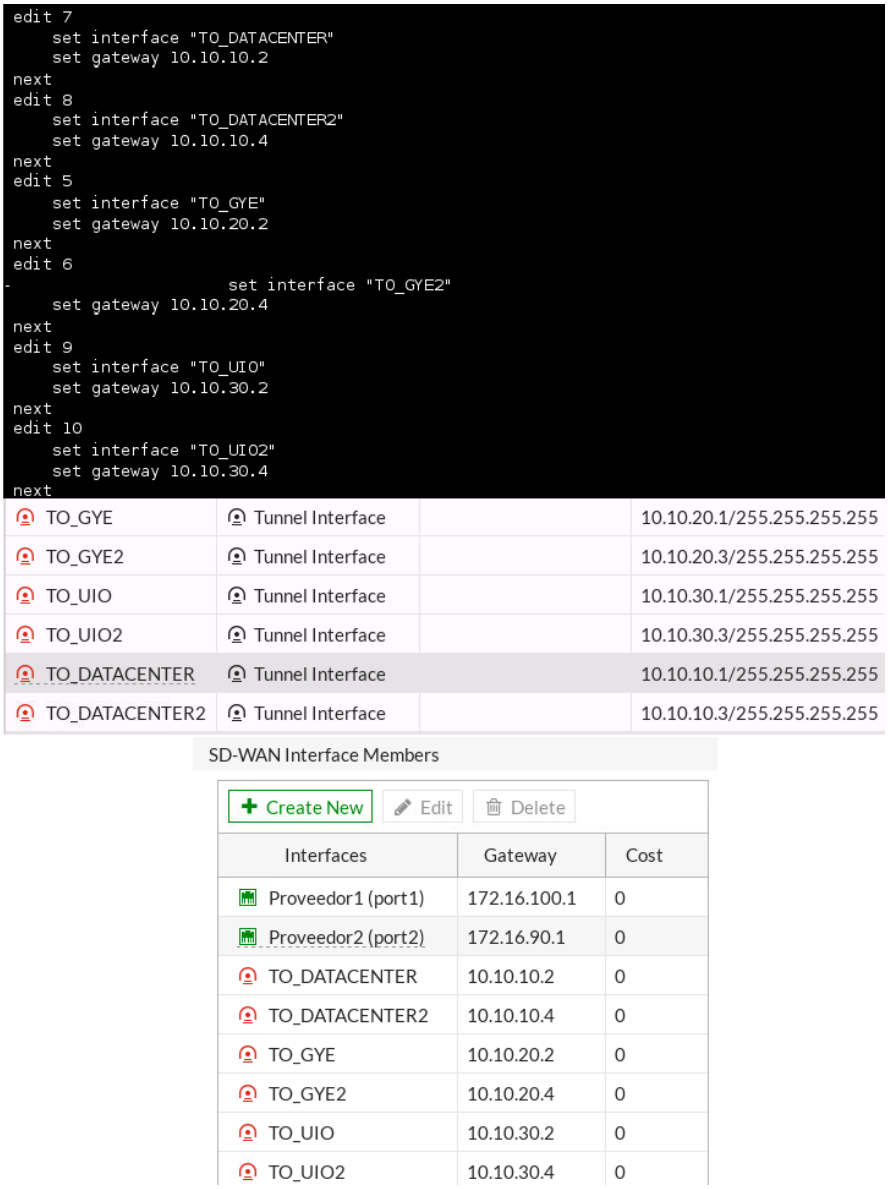


Figura 3.12: Configuración de túneles IPSec en la interfaz SD-WAN.

Fuente: Autor

3.9 Configuración de loopback

En la Figura 3.13 se muestran las loopback creadas para la empresa Construl S.A. Las mismas serán utilizadas para sondear las interfaces que pertenecen al SD-WAN en los otros Fortigate. Las loopback cumplen con

la función de enviar pequeños paquetes a las interfaces pertenecientes al SD-WAN para determinar que se encuentren activas y también verificar el tiempo de respuesta o pérdidas de cada túnel. Esta verificación ayuda a elegir la mejor ruta en conjunto con las reglas que se crearán en el SD-WAN.

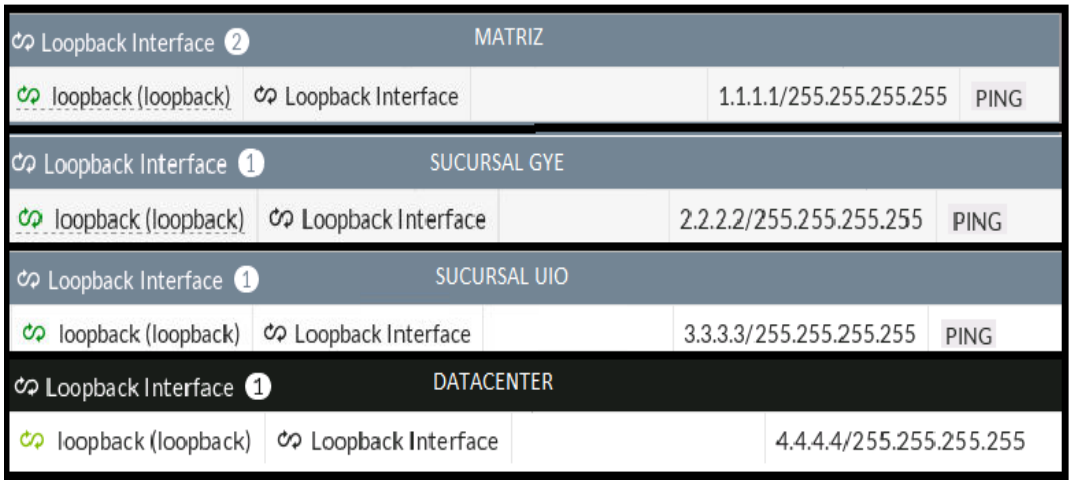


Figura 3.13: Configuración de loopback en los diferentes equipos Fortigate.

Fuente: Autor

3.10 Enrutamiento por BGP

El protocolo BGP se configura para poder propagar los datos de forma dinámica, a través de los túneles creados entre matriz y los diferentes puntos que tiene Construl S.A. Para la configuración del BGP interno se usa la identificación AS 61000. Hay que tener en cuenta que se debe declarar en matriz todo el segmento de IPs usadas para levantar los túneles en el SD-WAN. Se debe declarar todos los segmentos de redes usados a nivel LAN para que así puedan ser propagados y vistos desde los puntos extremos. El enrutamiento por BGP facilita que se haga la comunicación entre las sucursales.

Al conocer las redes dinámicamente se pueden crear los túneles dinámicos y establecer la comunicación. A continuación, se analiza un extracto del código utilizado para configurar el BGP en Matriz, se detallan todas las configuraciones BGP realizadas en los diferentes extremos en la figura 4, y 5 las cuales se encuentran en el anexo 1.

```
Matriz (bgp) # sh
config router bgp
    set as 61000
    set router-id 1.1.1.1
    config neighbor-group
        edit "remote-peers"
            set next-hop-self enable
            set remote-as 61000
            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 192.168.10.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.11.0 255.255.255.0
        next
        edit 3
            set prefix 192.168.12.0 255.255.255.0
        next
        edit 4
            set prefix 192.168.13.0 255.255.255.0
        next
        edit 5
            set prefix 192.168.14.0 255.255.255.0
        next
        edit 6
            set prefix 192.168.15.0 255.255.255.0
        next
        edit 7
            set prefix 1.1.1.1 255.255.255.255
        next
```

Figura 3.14: Configuración del BGP en el Fortigate.

Fuente: Autor

La figura 3.14 explica la configuración del BGP primero hay que ingresar al modo configuración de BGP luego hay que asignar un AS el cual servirá para ver a los elementos de sucursal que se encuentran dentro del mismo AS. En el caso de matriz se configura como router reflejo para manejar la red de una mejor manera, luego se declara todos los segmentos de redes que pertenecen al BGP en este caso del diseño se configura la Ip de red y las subredes.

Redes aprendidas dinámicamente por BGP.

Al configurar el protocolo BGP se aprenderá las redes dinámicamente de los extremos como se observa a continuación en la figura 3.15 en la cual antes de cada ip aparece la letra B que representa o indica que fue enrutada por medio del protocolo BGP.

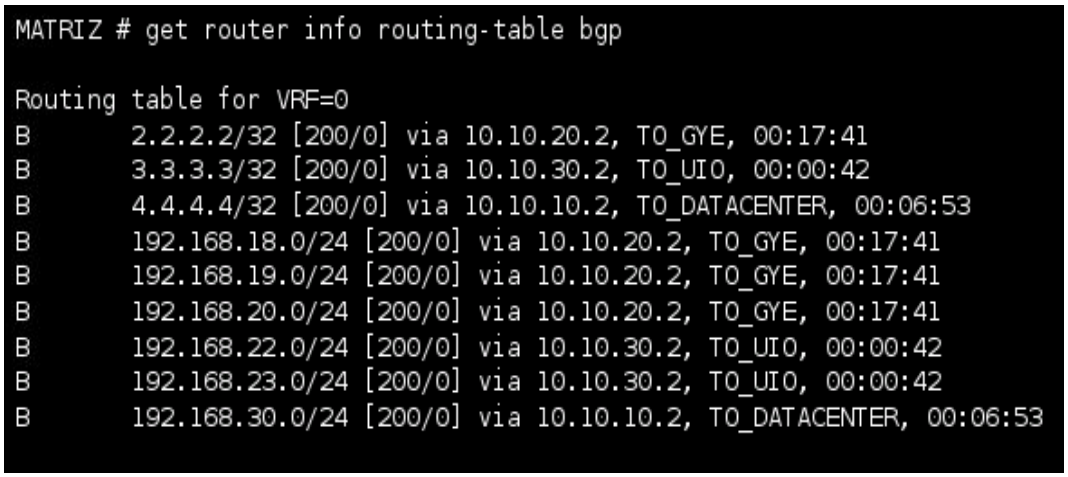


Figura 3.15: Redes aprendidas dinámicamente por BGP.

Fuente: Autor

3.11 Parámetros para la medición de la calidad del enlace.

Para la medición de calidad y disponibilidad del servicio se configura también en el SLA del SD-WAN el monitoreo de las ip loopback referenciando el punto donde se requiere la comunicación. En matriz se debe configurar la ip loopback de las sucursales haciendo referencia a los 2 túneles creados de contingencia para posibles fallos, y en las sucursales se monitorea la ip loopback de matriz también tomando como referencia los 2 túneles creados. En la Figura 3.16 se podrá observar de manera gráfica el monitoreo creado para las loopback tanto en matriz, sucursales y datacenter. Se destaca en el monitoreo el análisis de la pérdida de paquetes, latencia y jitter.

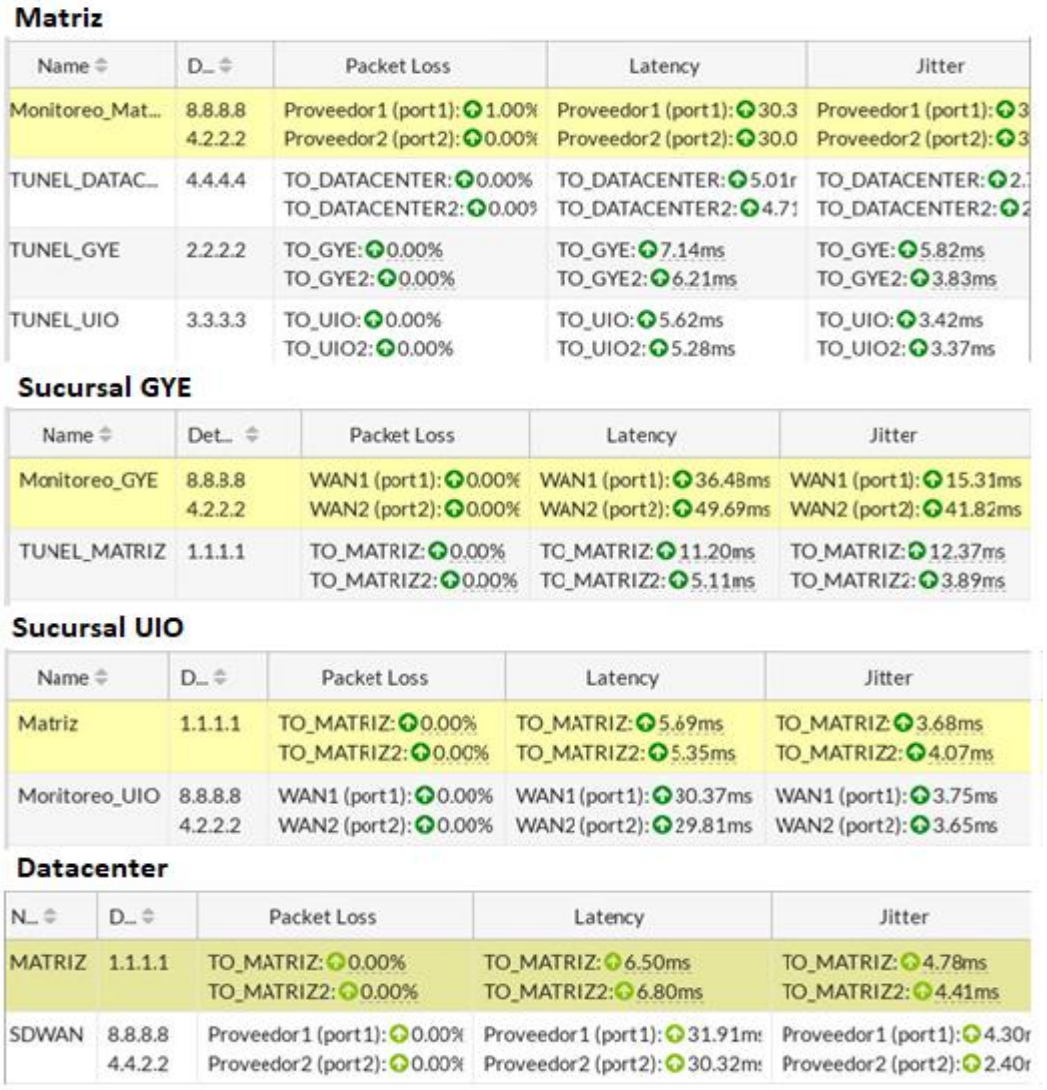


Figura 3.16: Monitoreo sucursal GYE de enlaces y túneles donde se mide la latencia y el Jitter.
Fuente: Autor

3.12 Configuración de políticas para la comunicación SD-WAN y asignación de etiquetas para los segmentos de red.

Como parte final de las configuraciones, para lograr la comunicación por SD-WAN se establecen las políticas en las cuales se pueden detallar los segmentos de red que van a poder comunicarse por datos o Internet. Para un mejor manejo de las redes a incluir en las políticas, se les asigna una etiqueta a cada segmento de red como se muestra a continuación. La figura

3.17 detalla los nombres que va a tener cada segmento de red que intervienen en la configuración del diseño.

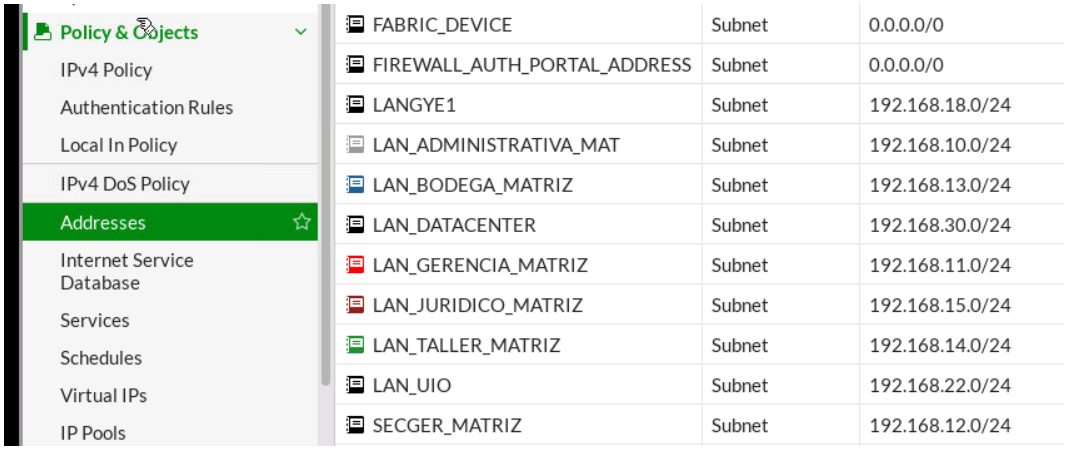


Figura 3.17: Asignación de nombres a los segmentos de IP utilizados en la comunicación LAN.

Fuente: Autor

Las políticas que se indican a continuación, se observan los segmentos que fueron detallados en la tabla 3.7 con las restricciones para cada área de la empresa Construl S.A. Los elementos que pertenecen a los túneles se encuentran desactivados. Solo la política que permite la salida al Internet está activada para que el tráfico que disminuya en la misma pueda tener comunicación al mundo. Estas configuraciones se deben realizar en cada sucursal y Datacenter de acuerdo a las restricciones de cada área.

En la figura 3.18 se puede observar que la política tiene que ser configurada en 2 sentidos refiriéndose al origen de los datos y el destino, primero se configura la política de origen de datos desde el puerto 4 hacia SD-WAN y luego se configura otra política donde cuente el origen de los datos que ingresan desde la SD-WAN hacia la red interna que es el puerto 4 del Fortigate.

Matriz

ID	Name	Source	Destination	Service	NAT
port4 → sd-wan 2					
2	Tuneles	LAN_ADMINISTRATIVA_MAT LAN_BODEGA_MATRIZ LAN_GERENCIA_MATRIZ LAN_TALLER_MATRIZ SECGER_MATRIZ	LAN_DATACENTER LAN_UIO LANGYE1 VENTAS_GYE VENTAS_UIO	ALL	Disable
1	Internet_SDWAN	LAN_GERENCIA_MATRIZ LAN_ADMINISTRATIVA_MAT LAN_JURIDICO_MATRIZ LAN_TALLER_MATRIZ	all	ALL	Enablec
sd-wan → loopback (loopback) 1					
4	LOOPBACK	all	all	ALL	Disable
sd-wan → port4 1					
3	Tunel	LAN_UIO LANGYE1 VENTAS_GYE VENTAS_UIO	LAN_BODEGA_MATF SECGER_MATRIZ LAN_TALLER_MATRI LAN_GERENCIA_MA LAN_ADMINISTRATI	ALL	Disable

Figura 3.18: Asignación de nombres a los segmentos de IP utilizados en la comunicación LAN.

Fuente: Autor

3.13 Configuración de política para la comunicación entre sucursales.

Para lograr la comunicación dinámica entre sucursales se configura una política en matriz que permita aprovechar los túneles creados y tener comunicación con los extremos. A continuación, se observa en la figura 3.19 la política que permite la interacción entre las sucursales sin levantar túneles entre ellas. Al ser la comunicación entre extremos un tráfico que no entra al Fortigate de matriz a realizar consultas en la red interna se configura una política en la cual el origen y destino sea la interfaz virtual SD-WAN esto permitirá comunicar las sucursales. En el origen y destino de las redes LAN de las sucursales, se agregan todas las solicitudes que se requieran tengan comunicación y esto permite la interacción con todos los extremos ahorrando recursos.

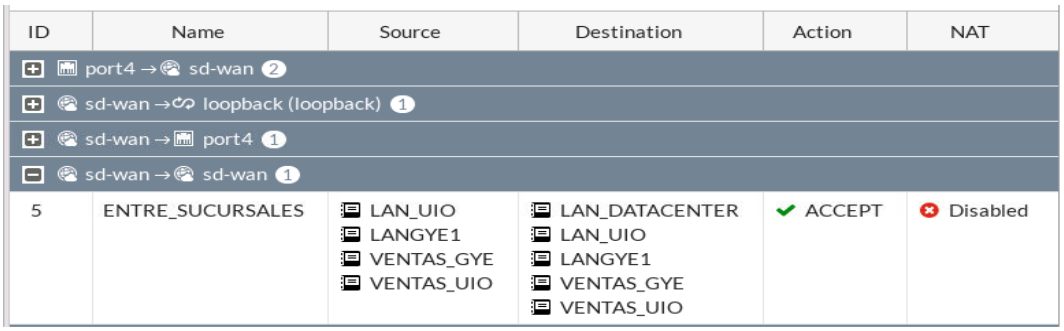


Figura 3.19: Políticas de comunicación entre sucursales

Fuente: Autor

3.14 Configuración de reglas para tomar mejor ruta de acuerdo al SLA establecido.

Para la elección de la mejor ruta de comunicación se declaran reglas tomando en cuenta el monitoreo SLA. Esto permite al SD-WAN ser óptimo por el motivo que la elección se realiza por medio del monitoreo SLA el cual indica la latencia y el Jitter de cada enlace, se elige el mejor camino al enlace con menor latencia y el Jitter que se encuentre al momento de la comunicación de un paquete determinado.

En la figura 3.20 se indica la configuración de las reglas en cada extremo de la red de Construl S.A. Se tiene en cuenta para las políticas de SLA que el tráfico origen es la LAN configurada en cada Fortigate y el tráfico destino es a las otras redes LAN que intervienen en la comunicación de los enlaces.

En las configuraciones se observa que el enlace tomará el camino que tenga menor latencia, esto ayuda a que, si un proveedor está presentando problemas, a nivel de UM en las oficinas no sientan esas intermitencias y a nivel lógico se haga la evaluación de la mejor ruta y sea elegida para la comunicación.

Matriz

ID	Name	Source	Destination	Criteria	Members
IPv4 4					
4	VPN_UIO	LAN_ADMINISTRATIVA_MAT LAN_BODEGA_MATRIZ LAN_DATACENTER LAN_GERENCIA_MATRIZ +6	LAN_UIO VENTAS_UIO	Latency	TO_UIO TO_UIO2
3	VPN_GYE	LAN_ADMINISTRATIVA_MAT LAN_BODEGA_MATRIZ LAN_DATACENTER LAN_GERENCIA_MATRIZ +6	LANGYE1 VENTAS_GYE	Latency	TO_GYE TO_GYE2
2	VPN_DATACE...	LAN_ADMINISTRATIVA_MAT LAN_BODEGA_MATRIZ LAN_DATACENTER LAN_GERENCIA_MATRIZ +6	LAN_DATACEN1	Latency	TO_DATACE TO_DATACE
1	Salida_Internet.	all	all	Latency	Proveedor1 Proveedor2

Sucursal GYE

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
2	VPN_MATRIZ	LAN_JEFATURA LAN_VENTAS	BODEGA_MATRIZ GERENTE_MATRIZ LAN_MATRIZ SECGEIREN_MATRIZ +4	Latency	TO_MATRIZ TO_MATRIZ2
1	Salida_Internet	all	all	Latency	WAN1 (port1) WAN2 (port2)

Sucursal UIO

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
2	VPN_MATRIZ	LAN_JEFESUCURSAL LAN_VENTA	BODEGA_MATRIZ LAN_MATRIZ SECGER_MATRIZ TALLER_MATRIZ +5	Latency	TO_MATRIZ TO_MATRIZ2
1	Salida_Internet	all	all	Latency	WAN1 (port1) WAN2 (port2)

Datacenter

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
1	TO_MATRIZ	LAN_DATACENTER	LAN_MATRIZ ABOGADO_MATRIZ BODEGA_MATRIZ GERENCIA_MATRIZ +6	Latency	TO_MATRIZ TO_MATRIZ2
2	Salida_Internet	all	all	Latency	Proveedor1 (port1) Proveedor2 (port2)

Figura 3.20: Regla de SD-WAN establecida para tomar mejor ruta.

Fuente: Autor

3.15 Control por aplicativos.

Para la red de la Construl S.A. se estableció el bloqueo para los aplicativos de las redes sociales y videos de Internet como se muestra en la figura 3.21; que, en la aplicación de filtros se bloquea todo acceso a las páginas antes nombradas. Estas configuraciones se realizan para tener un control más exacto en la red y no genere saturación con actividades que no pertenecen al desarrollo diario, también de esta manera se genera una red más segura evitando intromisión vía redes sociales. El bloqueo que se realiza es para todos los segmentos de red que tienen permitido la navegación. Hay varias formas que se puede denegar el tráfico hacia aplicativos o páginas específicas. Para la empresa Construl S.A. se eligió control por aplicaciones que cuenta con mayor eficacia y no permite el ingreso o violar la seguridad de los bloqueos establecidos.

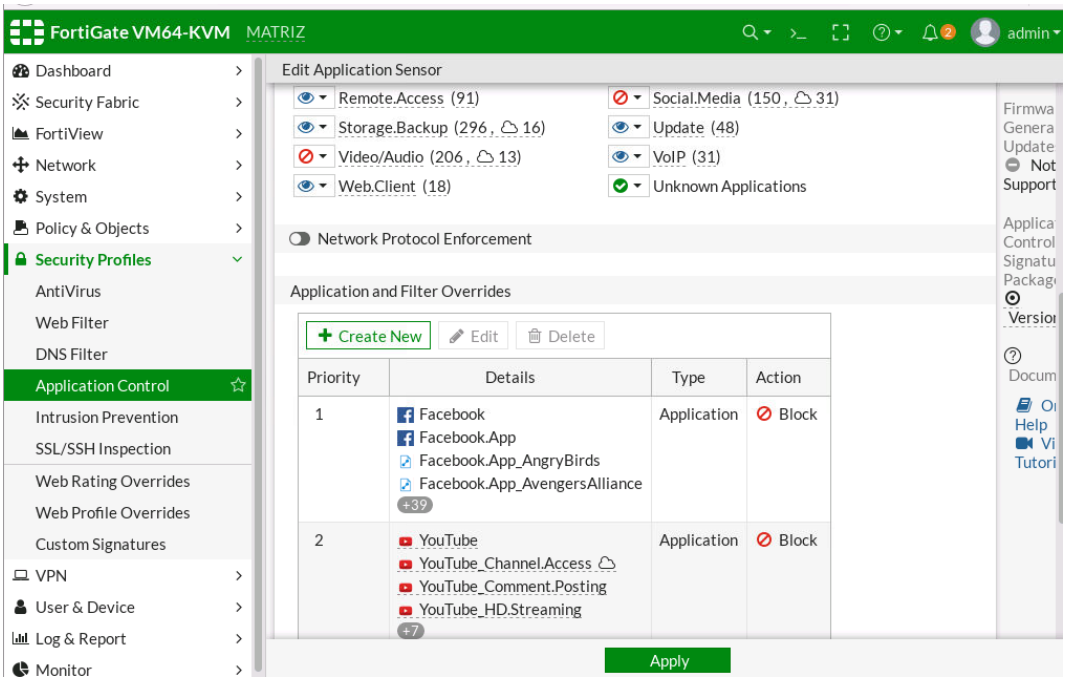


Figura 3.21: Bloqueo de redes sociales y Videos.

Fuente: Autor

CAPÍTULO 4. Evaluación de la red SD-WAN y resultados obtenidos

En el actual capítulo se detallará los resultados evaluados en la simulación y diseño que cuenta este proyecto. En el análisis de los resultados se realiza por medio del método de experimentación en la cual se va a observar los resultados de las configuraciones antes realizadas. Como primeras pruebas se verificará la salida al Internet por medio de las interfaces lógicas creadas SD-WAN, una vez validado la respuesta al mundo se procede con las pruebas de comunicación hacia los diferentes extremos validando que los túneles se encuentren operativos y correctamente configurados al tener respuesta de LAN a LAN de acuerdo a las políticas de acceso de cada segmento.

Se realiza la comprobación de comunicación de datos de acuerdo a los permisos detallados en la tabla 3.7. Para validar la correcta configuración de la política en matriz que permite la comunicación entre sucursales se realiza prueba de comunicación desde los diferentes extremos. En este punto se validará uno de los temas medulares del proyecto planteado que es el bloqueo por aplicativos para los diferentes segmentos de red que cuenta la empresa Construl S.A. Finalmente se pone a prueba las características de SD-WAN que es el motivo de los nuevos estudios y planteamientos de mejoras para tener una red dinámica y de alta disponibilidad.

4.1 Prueba de Salida al Internet por las interfaces SD-WAN.

En la figura 4.1 se realiza prueba del PING desde el equipo Fortigate hacia el Internet. Luego de configurar la interfaz lógica SD-WAN, se observa un correcto funcionamiento de los 2 proveedores. Esta prueba se realiza para validar que la interfaz lógica SD-WAN esté correctamente configurada y se encuentre realizando los saltos correctos para que transmita información por las diferentes WAN de los proveedores como se muestra en los cuadros marcados donde el primer salto es la LAN del Fortigate y el segundo salto son los Gateway de los proveedores. La ruta al Internet va a ser de acuerdo

a la medición de latencia en el momento de la prueba, cuya latencia esta monitorizada de manera continua.

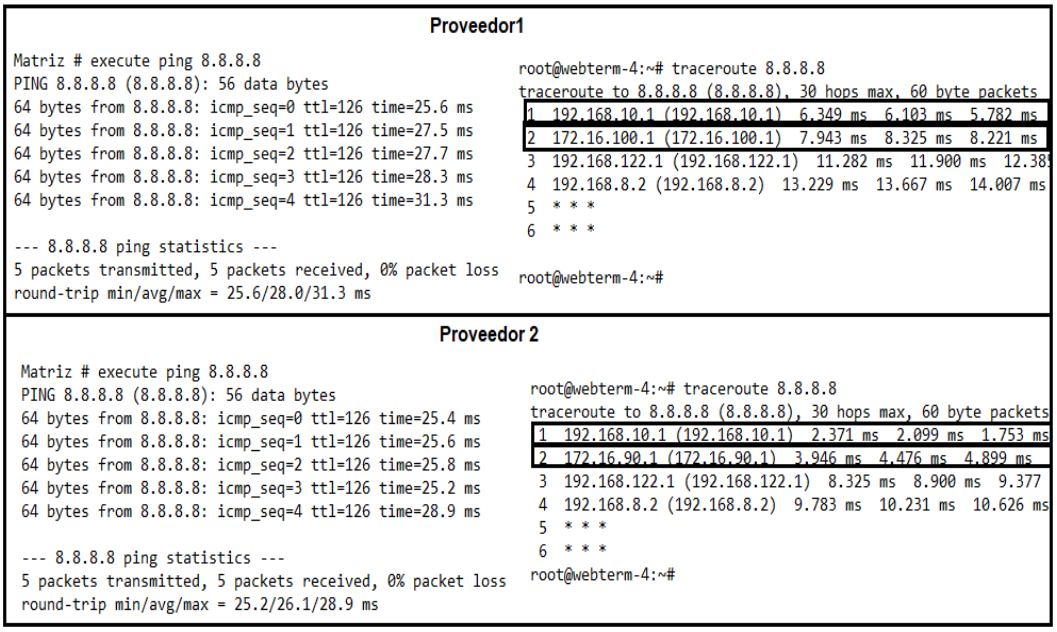
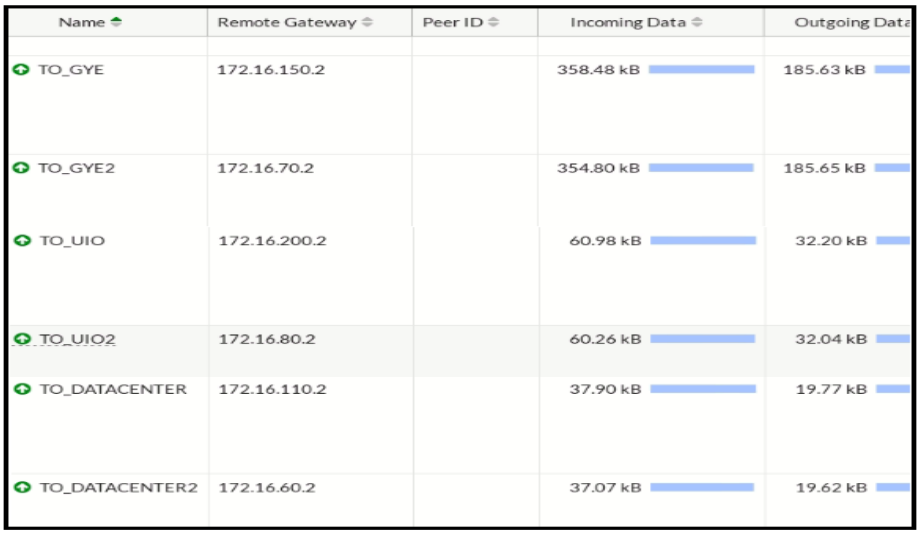


Figura 4.1: Respuesta al Internet por la WAN1 (SD-WAN), WAN2 (SD-WAN)

Fuente: Autor

4.2 Verificación de túneles operativos.

A continuación, en la figura 4.2 se podrá observar los túneles levantados en matriz para la comunicación hacia los diferentes extremos. Estos túneles facilitan la comunicación y permite que los enlaces se conecten de una forma segura entre los diferentes puntos. En el anexo 2 se adjunta las figuras 1, 2 y 3 donde se evidencia los túneles levantados para establecer la comunicación entre los diferentes puntos de la empresa Construl S.A. teniendo en cuenta que en los puntos extremos y datacenter solo se tiene túneles hacia matriz. En matriz levanta túneles dinámicos para establecer comunicación entre los extremos.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
TO_GYE	172.16.150.2		358.48 kB	185.63 kB
TO_GYE2	172.16.70.2		354.80 kB	185.65 kB
TO_UIO	172.16.200.2		60.98 kB	32.20 kB
TO_UIO2	172.16.80.2		60.26 kB	32.04 kB
TO_DATACENTER	172.16.110.2		37.90 kB	19.77 kB
TO_DATACENTER2	172.16.60.2		37.07 kB	19.62 kB

Figura 4.2: Túneles levantados visto desde Fortigate Matriz

Fuente: Autor

4.3 Prueba de comunicación de datos a través de los túneles.

Haciendo referencia a la tabla 3.7 se realiza las pruebas de comunicación entre los diferentes puntos que componen la red de la empresa Construl S.A. En la figura 4.3 se valida la comunicación de datos LAN a LAN entre matriz y sucursal GYE tomando este ejemplo como referencia para las demás pruebas de comunicación las cuales se adjuntan en el anexo 2 figuras 4 y 5. Para las pruebas de comunicación se toma como referencia las IPs de matriz que permiten la comunicación de datos y como destino las IPs de la sucursal y datacenter que permite establecer la comunicación de datos internos de la empresa Construl S.A.

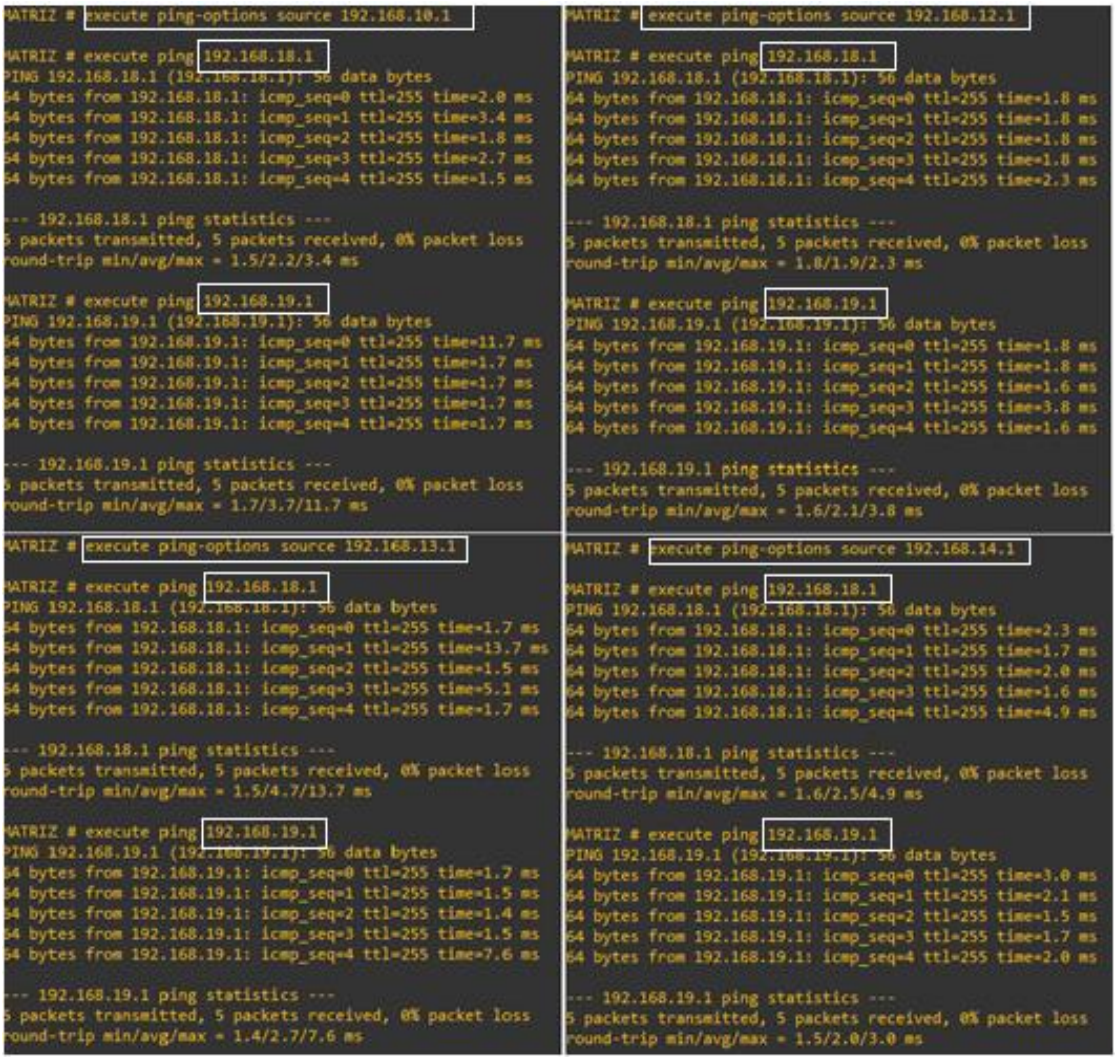


Figura 4.3: Comunicación entre Matriz-Sucursal GYE

Fuente: Autor

4.4 Prueba de comunicación entre sucursales a través de túnel dinámico.

A continuación, en la figura 4.4 se visualiza la comunicación entre el extremo sucursal GYE y sucursal UIO de la empresa Construl S.A. el cual se toma como ejemplo de las pruebas que se realizan y se adjuntan en el anexo 2 figura 6. Previamente se configuró en matriz la política de seguridad para que haya comunicación entre las sucursales y así intercambiar información entre ellas. Se podrá administrar las redes desde la matriz.

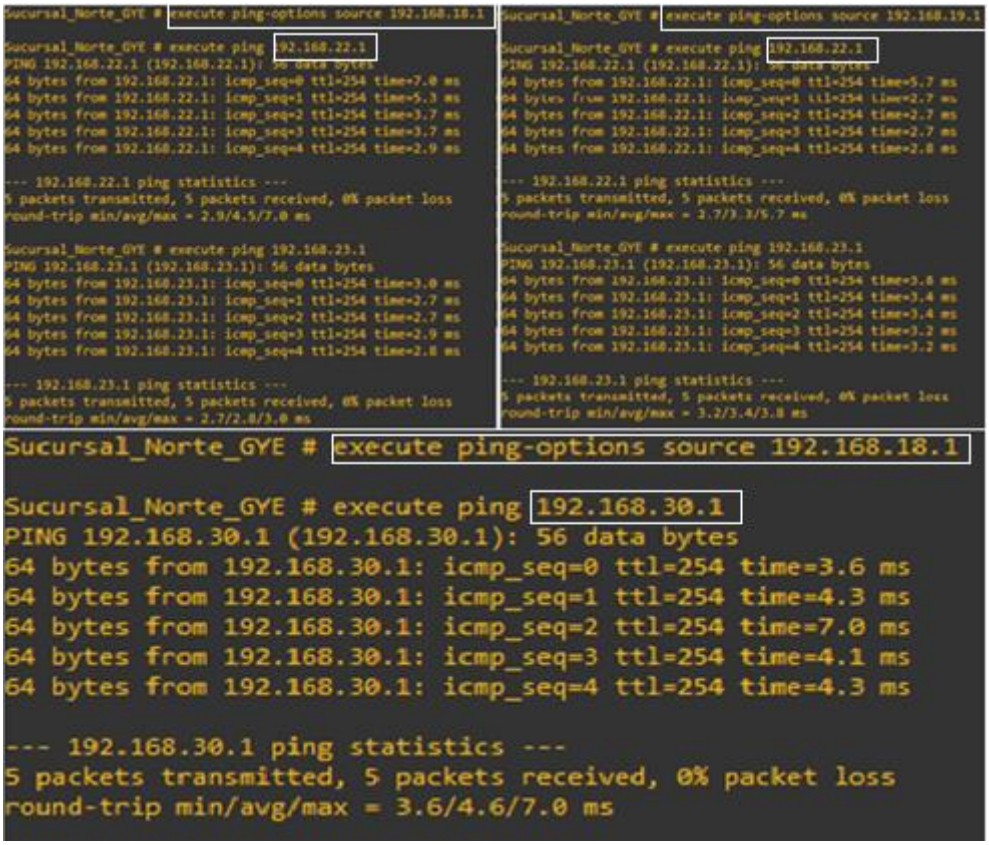


Figura 4.4: Comunicación entre Sucursal GYE-Sucursal UIO, Sucursal GYE-Datacenter.
Fuente: Autor

4.5 Prueba de comunicación hacia Internet desde las redes permitidas.

La prueba de comunicación hacia Internet consiste en validar que los segmentos de red que se configuran para tener salida al Internet puedan navegar sin problemas. De esta manera se establece un control en la red y se asegura que los recursos serán utilizados en obligaciones laborales. Se toma como referencia matriz para realizar las pruebas. El área de Gerencia, Talleres y jurídico tienen acceso a Internet con restricción a nivel de aplicativos de redes sociales y videos en Internet.

4.5.1 Gerencia.

En la figura 4.8 se realiza pruebas de salida al Internet por el segmento de red LAN asignado para el área de gerencia, se valida con el *traceroute* que

al momento se encuentra saliendo por el proveedor 1 el cual presenta menor tiempo de respuesta hacia el internet. De esta manera se activa la regla de SD-WAN que censa el canal que presente menor latencia para la comunicación. En la figura 4.8 también se detalla la configuración del equipo terminal (PC del cliente) el cual presenta registrada una ip dentro del rango de gerencia. Por medio del *traceroute* se confirma que el momento que se toma la captura el enlace con menor latencia es del proveedor 1.

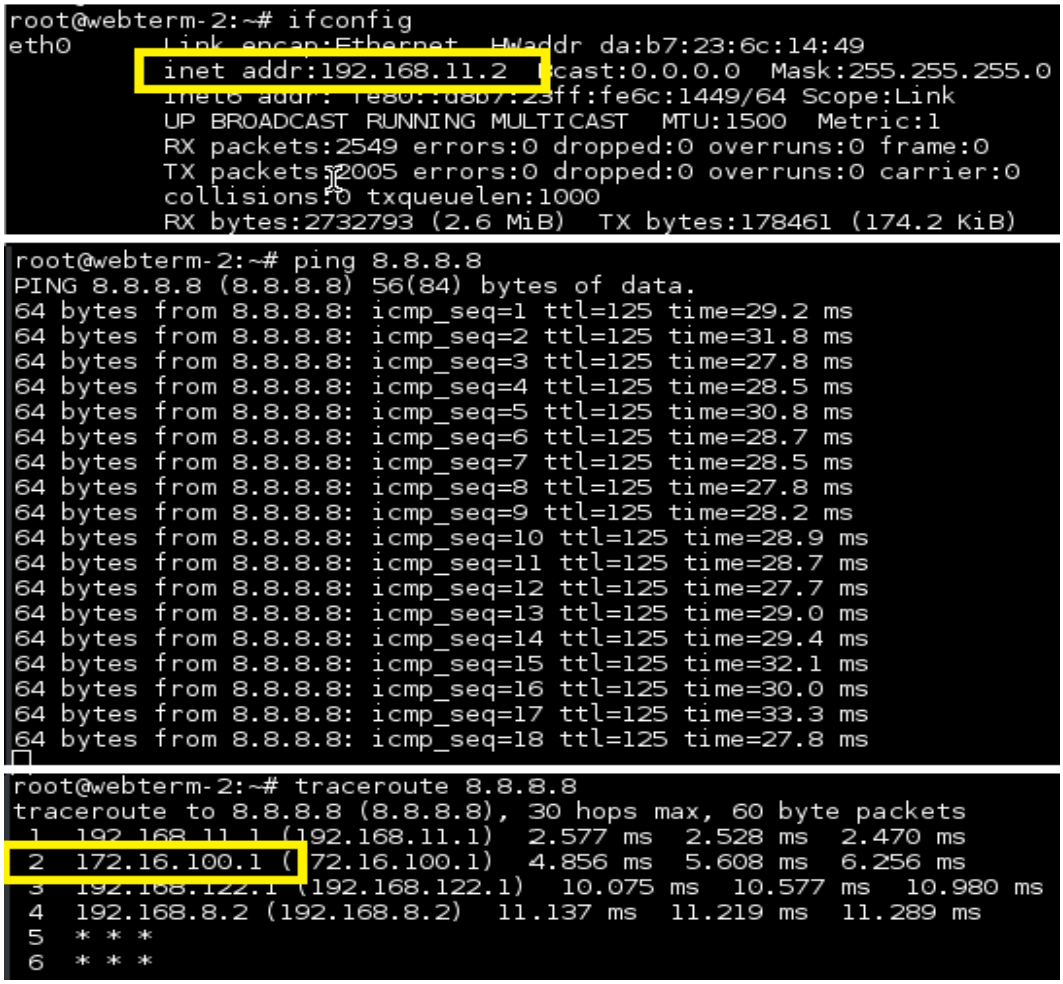


Figura 4.5: Respuesta al Internet desde la red de Gerencia.

Fuente: Autor

4.5.2 Talleres

A continuación, en la figura 4.10 se valida la respuesta al mundo del área de talleres. Las configuraciones de la red talleres se basa en la misma que la red de Gerencia, al tener esta particularidad se utiliza la misma política

que se usa para la red de gerencia y se llama a la red talleres para que también intervenga en la política. El permiso para navegar a internet o datos va a depender del administrador de red dependiendo del requerimiento de Construl S.A. La ruta que va a elegir para la comunicación al internet depende de las configuraciones SD-WAN. Para esta área los paquetes toman la ruta por el primer proveedor.

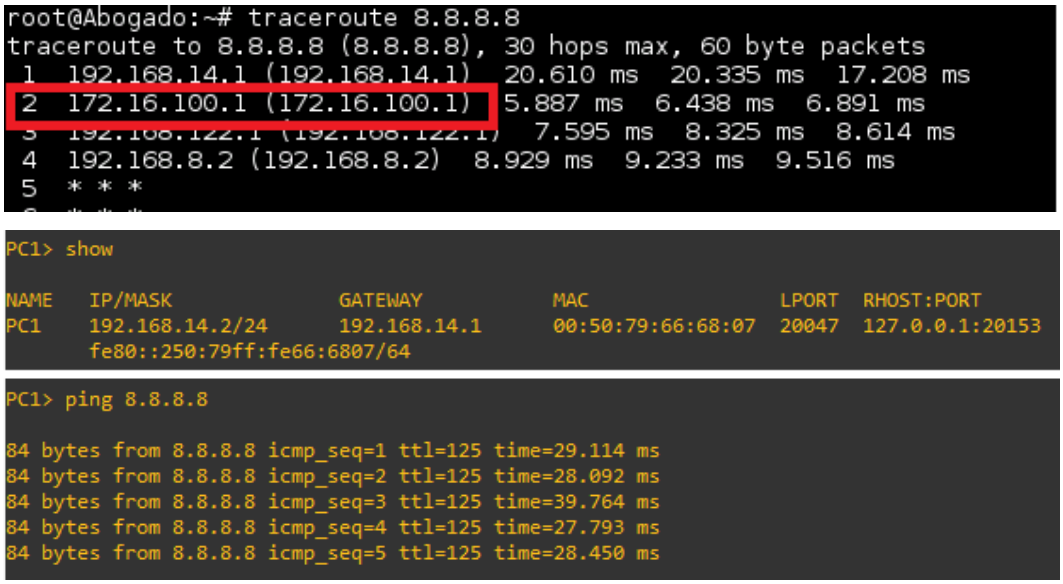


Figura 4.6: Salida al mundo por la red LAN de Talleres

Fuente: Autor

4.5.3 Jurídico

En la figura 4.7 se valida la respuesta al mundo desde la red de Jurídico. Se destaca también que este segmento de red solo puede salir al Internet por tal motivo solo es llamada esa red en la política de seguridad de Internet. La red de jurídico también cuenta con las mismas restricciones brindada para las demás áreas que tienen navegación. En esta prueba los paquetes toman la ruta del proveedor 2 por presentar menor latencia y esto se da por las configuraciones establecidas de la SD-WAN.

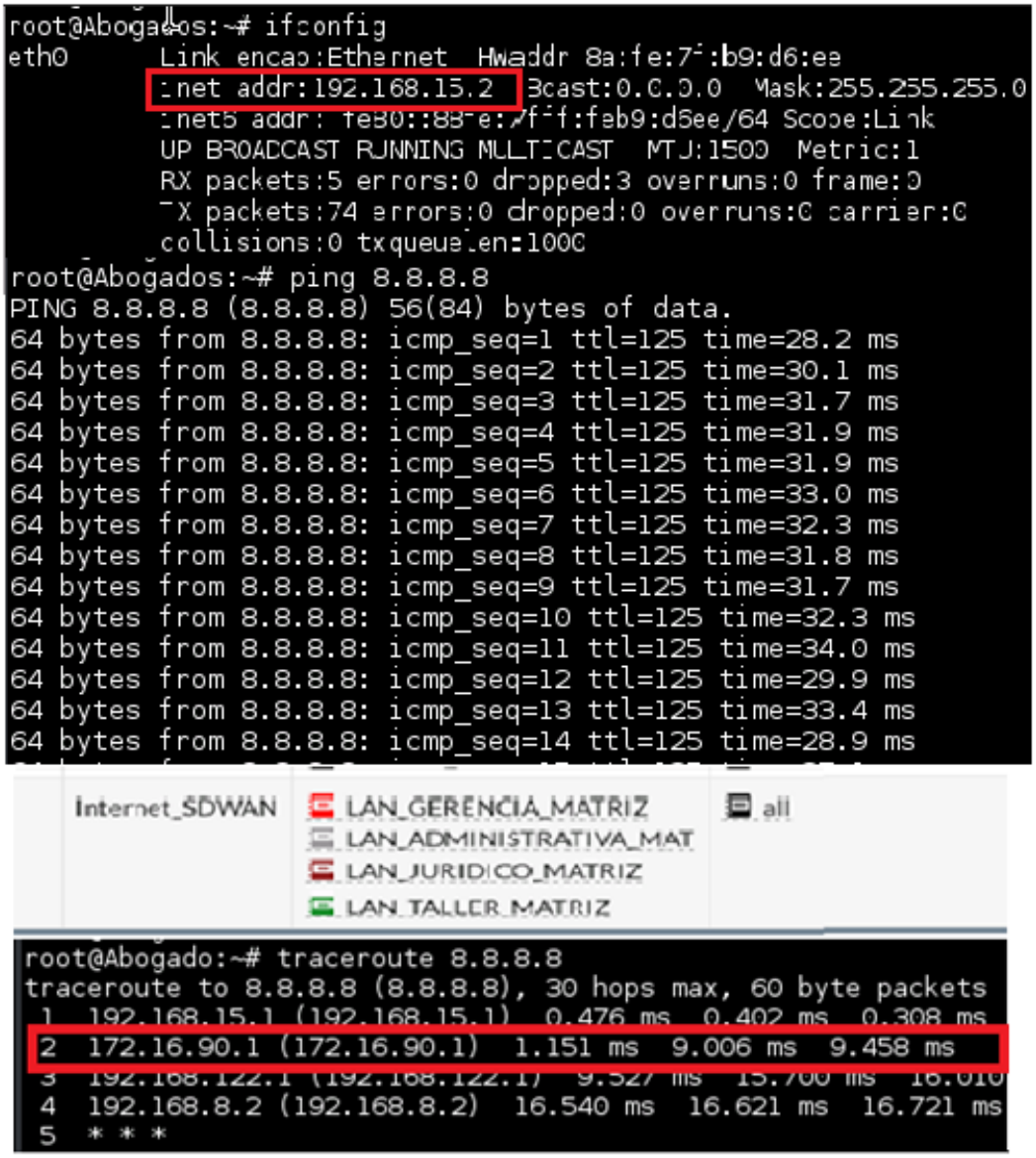


Figura 4.7: Respuesta al Internet desde la red de Jurídico

Fuente: Autor

4.6 Bloqueo de aplicativos de acuerdo a los controles establecidos.

Dentro de las políticas del Fortigate de navegación hacia el Internet se llama a los controles de acceso y servicio web para que funcionen en los bloqueos requeridos para la red de Construl S.A. Estas configuraciones se replican en las sucursales y datacenter para mantener una red segura y en la cual se use para fines laborales y no haya distracción.

En la Figura 4.8 se muestra en modo grafico como es el bloqueo hacia los aplicativos que se requiera, en este caso se utiliza para pruebas a Facebook por parte de los aplicativos de redes sociales y a YouTube en videos.

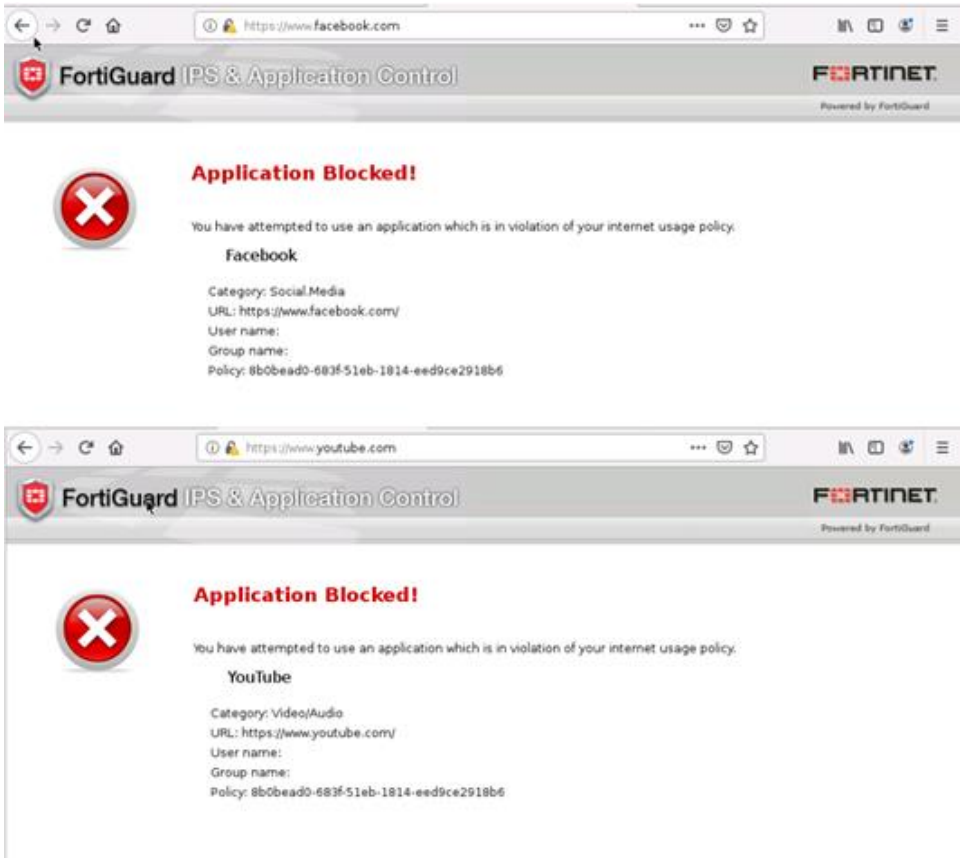


Figura 4.8: Bloqueo de aplicativos (Redes sociales y videos).

Fuente: Autor

En la figura 4.9 se evidencia los perfiles de seguridad que se activan para que la funcione las restricciones solicitadas por Construl S.A. Cada perfil antes de ser activado se configura con las páginas o aplicativos que se quiere limitar la navegación. Se puede configurar de diferente forma los perfiles de seguridad esto va a depender del administrador de red.

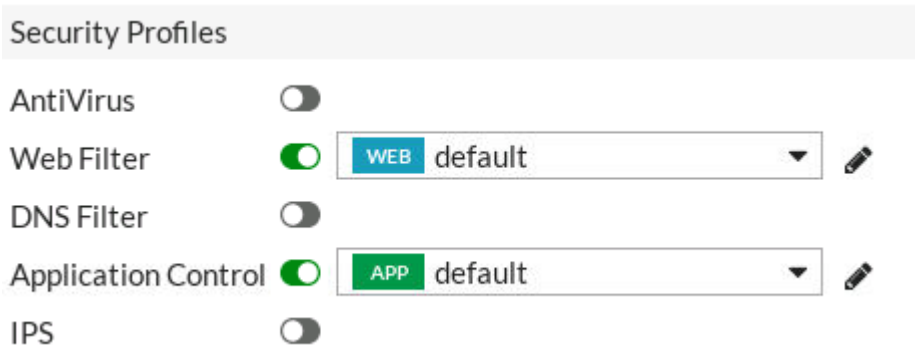


Figura 4.9: Perfiles de seguridad necesarios para limitar la navegación.

Fuente: Autor

4.7 Prueba de conmutación SD-WAN

Una de las características más importantes en SD-WAN es su rápida conmutación para que el trabajo diario de Construl S.A. no se vea afectado. Para el diseño planteado en la figura 4.10 se realizan las pruebas de conmutación. Primero se observan las 2 WAN operativas y funcionando correctamente. Luego se procede a dar de baja a la WAN del primer proveedor y se valida la conmutación. Se activa el funcionamiento de la WAN del segundo proveedor inmediatamente.

Este panorama también se presenta cuando un proveedor de servicios presenta tiempos altos, tomando la ruta con menor latencia. Luego de validar su funcionamiento se subirá la WAN del primer proveedor y dar de baja la WAN del segundo proveedor y analizar que el comportamiento sea de acuerdo a lo configurado tanto para datos como para Internet.

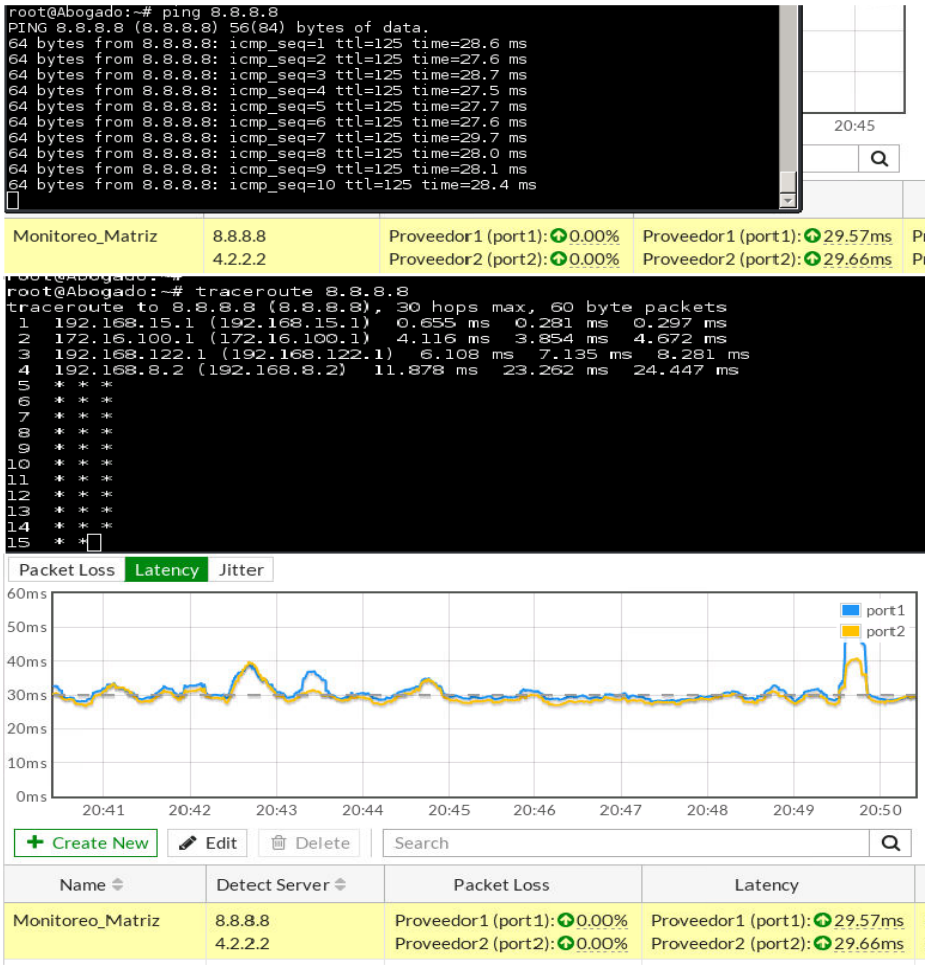


Figura 4.10: Red SD-WAN operativa tomando la ruta con menor latencia.

Fuente: Autor

En la figura 4.11 se observa las pruebas de conmutación luego de la desconexión del enlace del proveedor 2 que usualmente era considerado como enlace de respaldo. Para esta prueba se dio de baja el enlace del proveedor 2 físicamente en el GNS3 pero también es válida la prueba teniendo en consideración si el enlace de respaldo presenta tiempos altos se evidenciará en el monitoreo SLA y por medio de las reglas establecidas para SD-WAN tomará la mejor ruta en este caso haciendo referencia al proveedor 1.

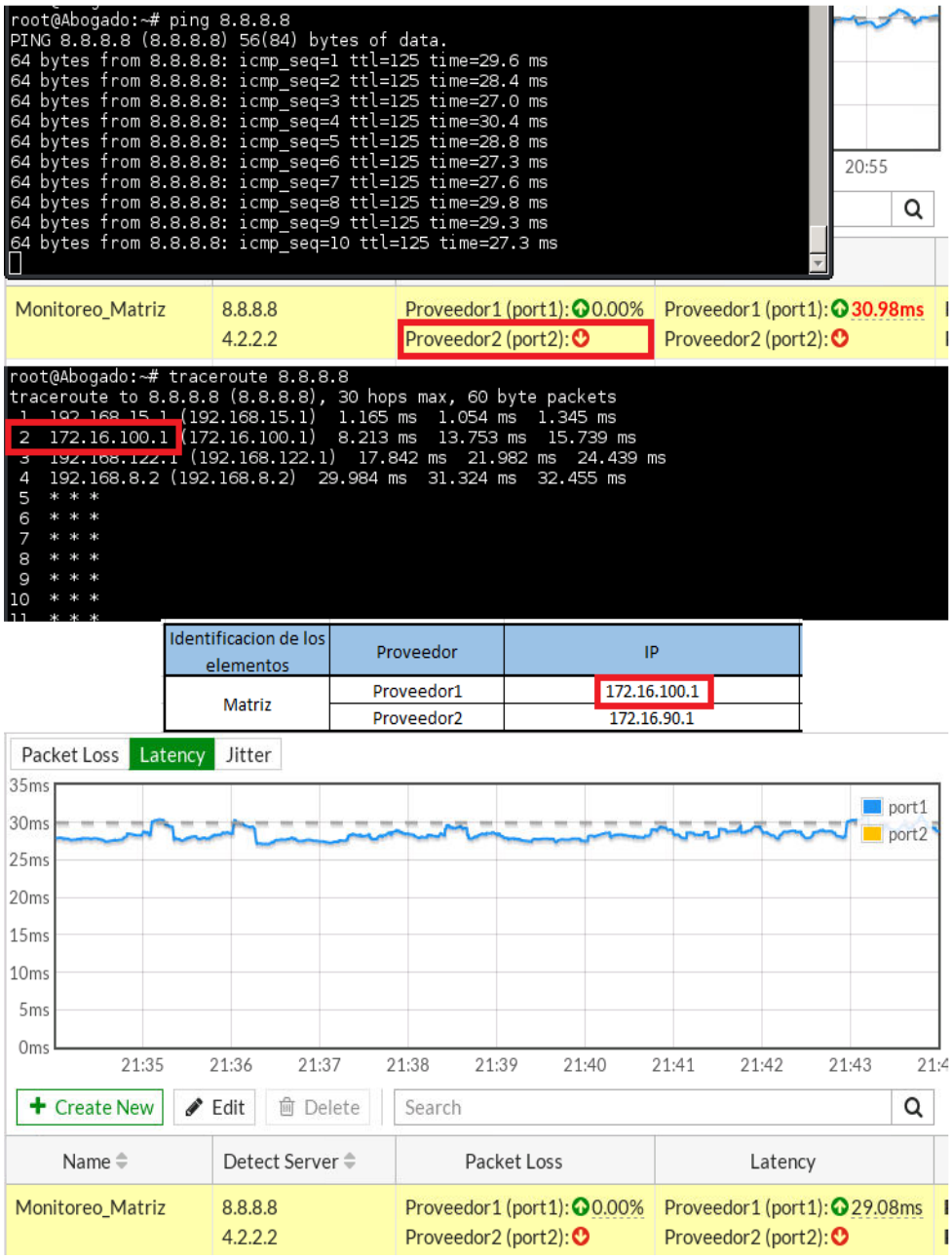


Figura 4.11: Red SD-WAN para Internet operativa por la WAN de proveedor 1.

Fuente: Autor

En la figura 4.12 se observa las pruebas de conmutación luego de la desconexión del enlace del proveedor 1 que usualmente es considerado enlace principal. Para esta prueba de igual forma que la anterior se da de baja físicamente el proveedor 1 y todo el tráfico saldrá por la WAN secundaria. De igual manera si el proveedor 1 tiene intermitencias o tiempos elevados la configuración hecha en las reglas de SD-WAN envía el tráfico por el proveedor 2.

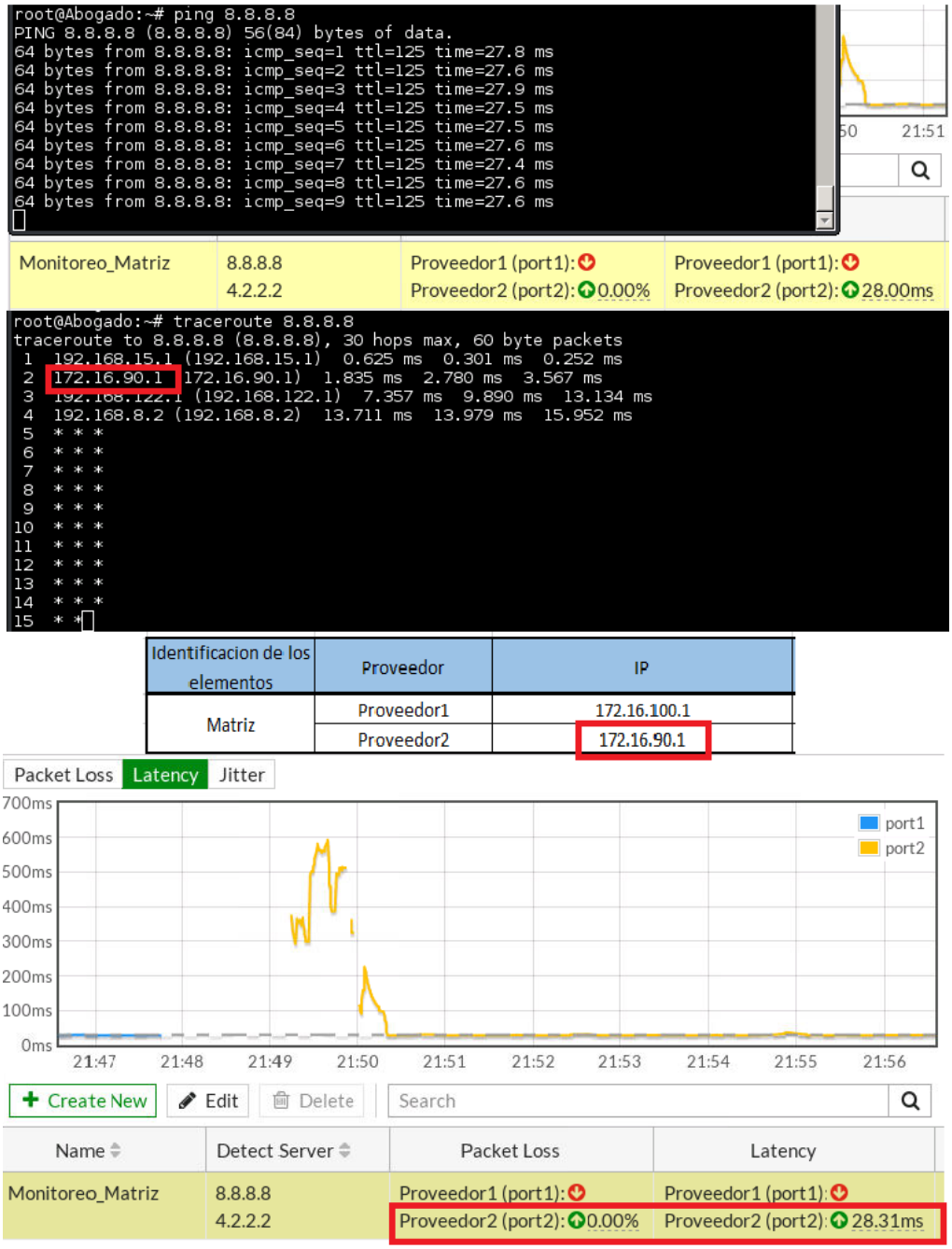


Figura 4.12: Red SD-WAN para Internet operativa por la WAN de proveedor 2.

Fuente: Autor

En la figura 4.13 se observa las pruebas de conmutación y funcionamiento al caer el proveedor dos de la comunicación del enlace de datos. Estas pruebas se realizan desde el Fortigate de matriz para los canales de datos los cuales no presentan una afectación al momento de cambiar de ruta. Se toma como referencia la respuesta de comunicación de matriz hacia sucursal UIO.

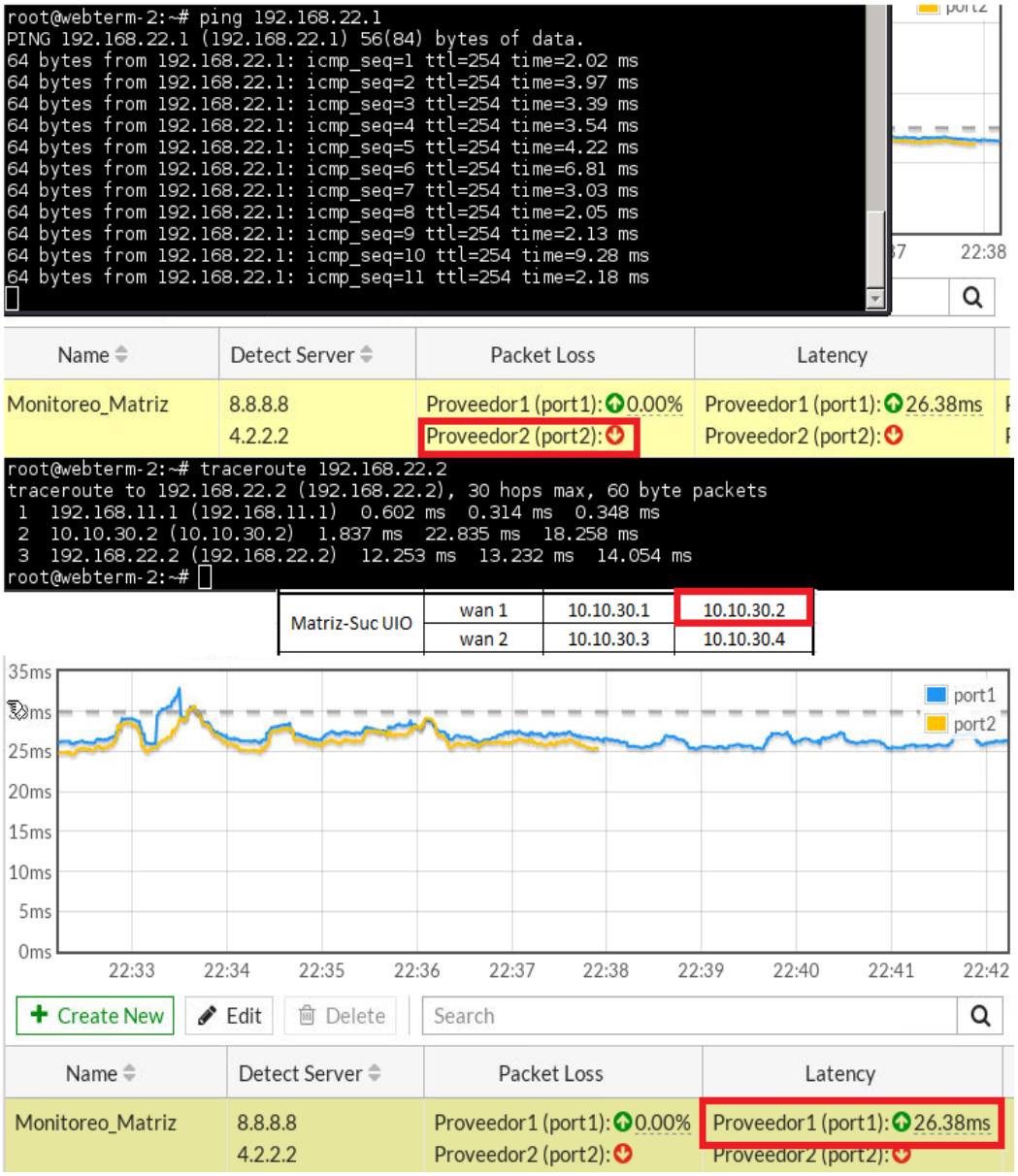


Figura 4.13: Red SD-WAN para datos operativa por la WAN de proveedor 1

Fuente: Autor

En la figura 4.14 se observan las pruebas de conmutación y funcionamiento al caer el proveedor1 de la comunicación del enlace de datos. Al dar de baja el proveedor 1 no se observa interrupción en la comunicación de datos pero se valida por medio de la traza que el tráfico se está comunicando por medio del proveedor 2.

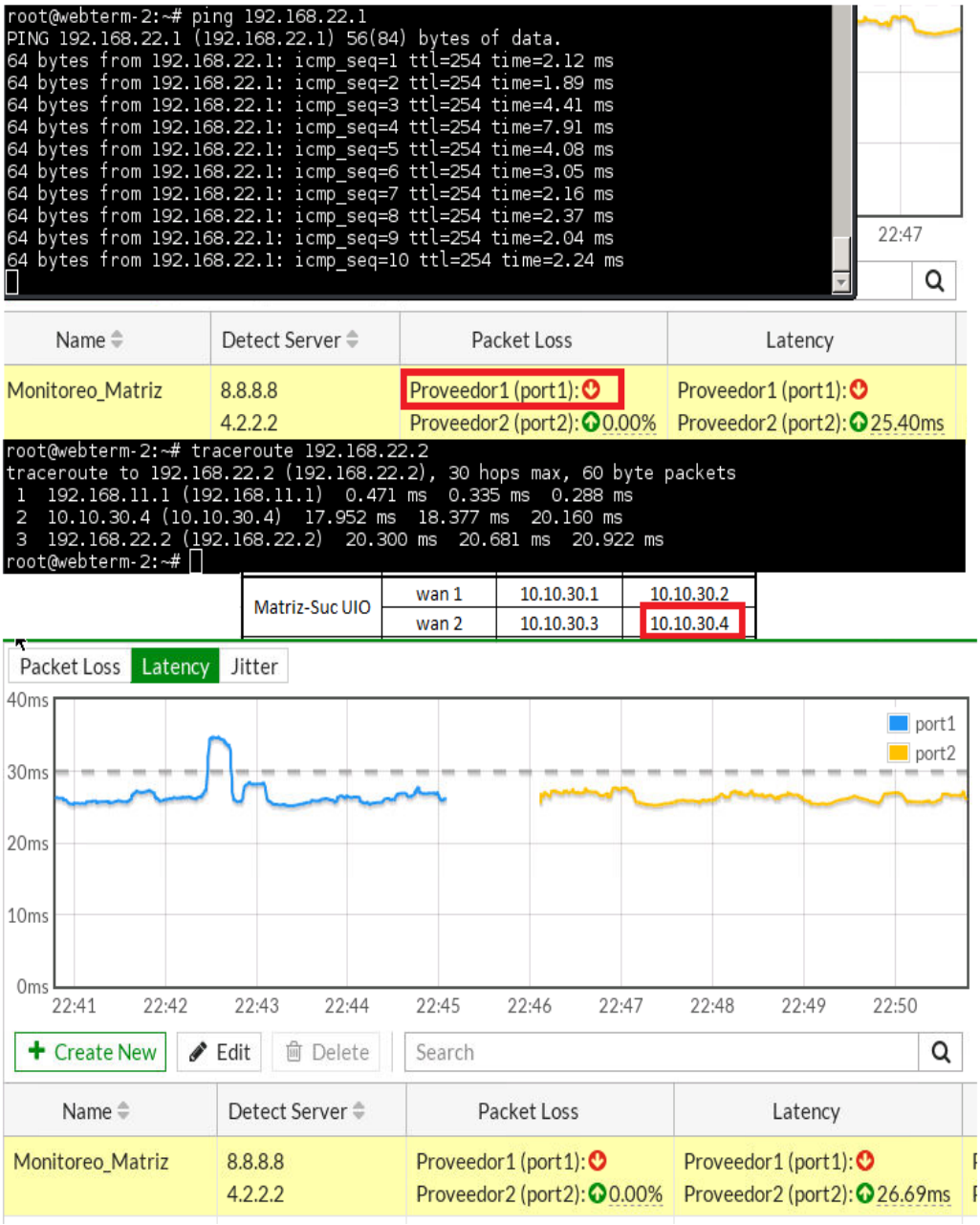


Figura 4.14: Red SD-WAN para datos operativa por la WAN de proveedor 2

Fuente: Autor

CONCLUSIONES

Como conclusión se comprobó que el diseño planteado para la empresa Construl S.A. cumple con los requerimientos para el desarrollo de la tecnología SD-WAN con equipos Fortigate. Los mismos facilitan los trabajos y control de la red a los encargados y obtienen alta disponibilidad en la red. Para observar el comportamiento del diseño de red la simulación se realiza mediante GNS3.

Así también, luego de analizar los requerimientos de la Construl S.A., se utilizó algoritmo de menor latencia, para tomar la mejor ruta, de acuerdo al análisis del SLA. Esto crea la ventaja de tener dos enlaces activos y poder elegir el camino a tomar para tener una mejor y más eficiente comunicación, brindada por la tecnología SD-WAN a través del Fortigate, generando mejores ingresos por tema de alta disponibilidad.

Además, se concluye que con el diseño de red realizado para el uso de SD-WAN con equipos Fortigate se tiene una administración completa de los enlaces y de cada usuario para así determinar que equipos o grupo de equipos pueden navegar en las diferentes páginas web. Con esto se garantiza a la empresa Construl S.A. que los recursos de red serán utilizados para actividades laborales de acuerdo a cada área de la empresa y garantizar la seguridad ante ataques que se realizan en aplicativos bloqueados. Finalmente, se determinó que con la simulación de la red de servicios de Internet y datos por medio de la tecnología SD-WAN de la empresa Construl S.A. se observa alta disponibilidad y administración de toda la red en todos sus segmentos.

RECOMENDACIONES

Como recomendación se plantea, que es necesario socializar la tecnología SD-WAN, para dar a conocer a las empresas los beneficios que otorga y que les permiten obtener un mejor servicio de comunicaciones, sin necesidad de realizar una mayor inversión de dinero. Deberia indicarse que para implementar esta red debe determinarse con anterioridad el tipo de diseño y alcance que tendá.Debido a que en el software gratuito, ofrecido por FortiGate no se tiene acceso a todas la funciones activas del programa; por lo que, en la socialización que se realice debería permitirse que el software de prueba permita la práctica de todas las funciones de la tecnología.

En base a la investigación recolectada se recomienda que toda empresa que requiera la implementación de este tipo de proyectos capacite al personal correspondiente en la administración de esta tecnología para un mejor desempeño de la red, y de esta forma conseguir que el servicio que se contrata sea eficaz y eficiente. Finalmente se recomienda que para los equipos de Fortigate que se usan en la implementación del SD-WAN, se instalen firmwares mayores a la actualización 6.0.0, ya que versiones anteriores a estas no pueden ser aplicadas en la tecnología SD-WAN.

Se recomienda que todas las conexiones de la red interna de la empresa Construl S.A. sean instaladas a través de un medio físico como un cable UTP. El no uso de equipos inalámbricos permitirá a la compañía garantizar el correcto funcionamiento de la red interna, para que los usuarios no se conecten desde sus dispositivos móviles, los cuales generarían mayor tráfico ocasionando saturación en la red no correspondientes a actividades laborales. Así también, se recomienda el uso de equipos switch de alto rendimiento para evitar pérdidas en la conexión a los diferentes departamentos de la empresa que dependen de la conexión por switch.

Bibliografía

Artunduaga, A., & Morales, L. (2018). *Diseño de la red LAN de la empresa ALTADIS FARMACEUTICA en la ciudad de Bogotá.* Obtenido de Repositorio UCC: https://repository.ucc.edu.co/bitstream/20.500.12494/6476/2/2018_diseno_red_lan.pdf

AT&T. (2021). *Internet Data Calculator*. Obtenido de https://www.att.com/es-us/support/data-calculator/

Bollapragada, V., Khalid, M., & Wainner, S. (2005). *IPSec VPN Design.* Indianapolis: Cisco Press.

Bustos, C. (2019). *Análisis de Factibilidad Técnico y Económico entre una red MPLS Traffic Engineering (TE) con Ipsec y una red Sd-Wan moderna.* Obtenido de Repositorio ESPE: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/15877/T-ESPE-038530.pdf?sequence=1&isAllowed=y

Butler, B. (2017). *SD-WAN: qué es y por qué lo va a usar*. Obtenido de Network World: https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar

Castro, E. (2015). *Diseño y simulación de una red MPLS para interconectar estaciones remotas utilizando el emulador GNS3.* Obtenido de Repositorio UPS: http://dspace.ups.edu.ec/handle/123456789/10297

Cordero, M. (2020). *Diseño y elaboración de plan para migración de redes WAN a SD-WAN.* Obtenido de Repositorio Universidad Latina de Costa Rica: https://repositorio.ulatina.ac.cr/bitstream/20.500.12411/280/1/TFG_Ulatina_Mario_Cordero_Hernandez.pdf

DatacenterDynamics. (2020). *La innovadora solución Secure SD-WAN de Fortinet facilita el teletrabajo desde una red doméstica a la nube distribuida*. Obtenido de https://www.datacenterdynamics.com/es/noticias/la-innovadora-

soluci%C3%B3n-secure-sd-wan-de-fortinet-facilita-el-teletrabajo-desde-una-red-dom%C3%A9stica-a-la-nube-distribuida/

DeLuz, S. (2021). *Cuál es el protocolo VPN más seguro: Conoce todos los que existen*. Obtenido de Redes Zone: https://www.redeszone.net/tutoriales/vpn/protocolo-vpn-mas-seguro/

DeLuz, Sergio. (2021). *Mejora la seguridad de tu VPN con el protocolo IPsec*. Obtenido de https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

eltelegrafo. (2021). págs. https://www.eltelegrafo.com.ec/noticias/septimo/1/es-improductivo-el-tiempo-invertido-en-redes-sociales.

Espinosa, O. (2019). *Qué es el servicio SD-WAN en las operadoras*. Obtenido de Redes Zone: https://www.redeszone.net/tutoriales/redes-cable/que-es-sd-wan/

Fabbri, R., & Volpe, F. (2013). *Getting Started with FortiGate.* Birmingham: Packt.

Fortinet. (2020). *Certificate inspection.* Obtenido de Fortinet Document Library: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/505842/certificate-inspection

Fortinet. (2021). *FortiGuard Antispam Service*. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/anti-spam

Gridelli, S. (2020). *Top 3 Challenges for SD-WAN Performance*. Obtenido de netbeez: https://netbeez.net/blog/top-3-challenges-for-sd-wan-performance/

Guerrero, F. (2018). *Tecnología SD-WAN en las pymes; ¿se puede aplicar?* Obtenido de Teldat: https://www.teldat.com/blog/es/tecnologia-sd-wan-para-pymes-plataforma-wan-lan-wi-fi-transformacion-digital/

Hosting. (2017). *La Tecnología MPLS al servicio de las redes privadas*. Obtenido de Revista Cloud: https://revistacloud.com/tecnologia-mpls-servicio-redes-privadas/

ICA. (2020). *Redes SD-WAN. ¿Cómo es que aún no las tienes?* Obtenido de I.C.A. Informática y Comunicaciones Avanzadas, S.L.: https://www.grupoica.com/blog/-/blogs/redes-sd-wan-como-es-que-aun-no-las-tienes-

Iddalagi, P. (2020). *SDWAN – Its Impact and The Need of Time.* Obtenido de Journal of Ubiquitous Computing and Communication Technologies (UCCT) Vol.02/ No.04: https://irojournals.com/jucct/V2/I4/02.pdf

informaticahabana. (2020). Obtenido de http://www.informaticahabana.cu/sites/default/files/ponencia-2020/TEL23.pdf

infotecs. (2020). *MPLS: Conmutación de Etiqueta Multiprotocolo*. Obtenido de https://infotecs.mx/blog/mpls.html

IONOS. (2017). *MPLS: estándar de transporte de datos en redes*. Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/mpls-que-es-el-multiprotocol-label-switching/

Jimenez, L. (2020). *Que es y caracteristicas de una IPSec VPN*. Obtenido de Comunidad Huawei: https://forum.huawei.com/enterprise/es/que-es-y-caracteristicas-de-una-ipsec-vpn/thread/537837-100233

Kirch, O., & Dawson, T. (2002). *Guía de Administración de Redes con Linux*. Obtenido de Guía Linux: http://ganimides.ucm.cl/haraya/doc/GuiaLinux.pdf

Larosa, A. (2018). *¿Cómo las redes definidas por Software cambian nuestra visión sobre las redes? pandorafms*. Obtenido de pandorafms: https://pandorafms.com/blog/es/redes-definidas-por-software/

Library, F. D. (2020). Obtenido de https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/505842/certificate-inspection

López, J. (2020). *Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el software GNS3.* Obtenido de Repositorio EPN: http://bibdigital.epn.edu.ec/handle/15000/21163

Marqués, G. (2016). *IPsec y redes privadas virtuales.* lulu.

Minei, I., & Lucek, J. (2011). *MPLS Enabled-Applications: Emerging Developments and New Technologies.* New York: Wiley.

Nolle, T. (2021). *La SD-WAN puede ser la clave de los servicios de red inteligentes*. Obtenido de Network World: https://www.networkworld.es/networking/la-sdwan-puede-ser-la-clave-de-los-servicios-de-red-inteligentes

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

Olguín, M., Rivera, I., Martínez, A., Barrón, E., Rivera, L., & Padilla, F. (2005). *Introducción a la Seguridad con IP Seguro en Internet (IPSec).* Obtenido de https://polibits.cidetec.ipn.mx: https://polibits.cidetec.ipn.mx/ojs/index.php/polibits/article/viewFile/3597/2915

Patel, B., Aboba, B., Dixon, W., Zorn, G., & Booth, S. (2001). *Securing L2TP using IPsec*. Obtenido de www.hjp.at: https://www.hjp.at/doc/rfc/rfc3193.html

Petrenko, S. (2018). *Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation (River Publishers Series in Security and Digital Forensics) .* River Publishers.

Reina, F., & Ruiz, J. (2016). *Redes de área local*. Obtenido de ing.unne.edu.ar: http://ing.unne.edu.ar/pub/local.pdf

Rico, D., & Lobo, J. (2012). *Implementación de la seguridad del protocolo de internet versión 6.* Obtenido de Dialnet: file:///C:/Users/User/Downloads/Dialnet-ImplementacionDeLaSeguridadDelProtocoloDeInternetV-4183248.pdf

Rodrigues, L. (2013). *OpenFlow e o Paradigma de Redes Definidas por.* Obtenido de Universidade de Brasília: https://bdm.unb.br/bitstream/10483/5674/1/2013_LucasRodriguesCosta.pdf

Romero, V., Romero, R., Toala, M., Parrales, G., Delgado, H., Castillo, M., & Choez, M. (2018). *Metodologia y tecnología de la informacion en la educación.* Portoviejo: Área de innovación y desarollo, S.L.

Ruiz, A. (2019). *Diseño de una práctica para la enseñanza de redes privadas virtuales de capa 3 (L3VPN) con MPLS.* Obtenido de Repositorio Universidad Carlos II de Madrid: https://e-archivo.uc3m.es/bitstream/handle/10016/29783/TFG_Andrea_Ruiz_Pedraza_2019.pdf?sequence=1&isAllowed=y

Sambrano, J. (2020). *Implementación de redes SDN-WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP's)*. Obtenido de Repositorio ESPE: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/23406/T-ESPE-044177.pdf?sequence=1&isAllowed=y

Shaw, K. (2018). *Entornos SD-WAN: Su evolución*. Obtenido de computerworld: https://www.computerworld.es/tecnologia/entornos-sdwan-su-evolucion

Sollars, M. (2018). *Love and marriage: why security and SD-WAN need to go together*. Obtenido de Network Security. Volume 2018, Issue 10, October 2018, Pages 10-12: https://www.sciencedirect.com/science/article/abs/pii/S1353485818301004

SS00. (2020). *¿Qué son las redes LAN? Principales características*. Obtenido de https://www.todosobretusistemaoperativo.com/que-son-las-redes-lan/

Tanenbaum, A. (2013). *Redes de computadoras.* Pearson.

Telectronika. (2018). *GNS3 Guía Introductoria: Características y Requerimientos Mínimos*. Obtenido de https://www.telectronika.com/articulos/ti/que-es-gns3/

Uribe, J. (2021). *Tipos de arquitectura SD-WAN*. Obtenido de Taiga-Consulting: https://www.taiga-consulting.com/blog/tecnologia-de-la-informacion-1/tipos-de-arquitectura-sd-wan-1

Wang, D. (2019). *Software Defined-WAN for the Digital Age.* New York: CRC.

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). *Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities*. Obtenido de 28th International Conference on Computer Communication and Networks (ICCCN): https://ieeexplore.ieee.org/abstract/document/8847124

Yañez, M. (2020). *Internet y las TIC: un mundo interconectado*. Obtenido de Biocuriosidades: https://www.biocuriosidades.com/internet-y-las-tic-mundo-interconectado/

Zuluaga, H. (2020). *Seguridad en el cifrado de las redes sd-wan mediante la utilización de aplicaciones en la nube.* Obtenido de Repositorio UNAD: https://repository.unad.edu.co/handle/10596/38710

GLOSARIO DE TÉRMINOS

TIC: Las tecnologías de la información y la comunicación.

BGP: Protocolo de Puerta de Enlace de Borde.

CE*:* Router anterior al cliente final.

FEC: Etiqueta de reenvió especifico.

IDC: Corporación internacional de datos.

Ipsec: Seguridad del protocolo de Internet.

LAN: Redes de área local.

MPLS: Cambio de etiquetas multiprotocolo.

MTU: Unidad máxima de transferencia.

OSI: Modelo de interconexión de sistemas abiertos.

PE: Router frontera de un proveedor de servicio de red.

Qos: calidad de servicio.

SDN: Redes definidas por software.

SD-WAN: Redes WAN definida por software.

SLA: Acuerdo de Nivel de Servicio.

SSL: capa de conexión segura.

TTL: Tiempo de vida de un paquete.

VPN: red privada virtual.

VPN: R*edes privada virtual.*

VRF: Reenvío de enrutamiento virtual.

WAN: Red de Área Amplia.

IETF: Grupo de Trabajo de Ingeniería de Internet.

GUI: Interfaz gráfica de usuario.

ISO: Organización Internacional de Normalización.

AES: Estándar de cifrado avanzado.

PPP: Protocolo punto a punto.

Anexo 1

```
Matriz (interface) # sh
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.100.4 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "WAN1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 172.16.90.4 255.255.255.0
        set allowaccess ping https ssh snmp
        set type physical
        set alias "WAN2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
```

```
Sucursal_Norte_GYE (interface) # sh
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.150.2 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "WAN1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 172.16.70.2 255.255.255.0
        set allowaccess ping https ssh snmp
        set type physical
        set alias "WAN2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
```

```
Sucursal_Centro_UIO (interface) # sh
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.200.2 255.255.255.0
        set allowaccess ping https ssh htt
        set type physical
        set alias "WAN1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 172.16.80.2 255.255.255.0
        set allowaccess ping https ssh snm
        set type physical
        set alias "WAN2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
```

```
DATA_CENTER (interface) # sh
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.110.2 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "Proveedor1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 172.16.60.2 255.255.255.0
        set allowaccess ping https ssh snmp
        set type physical
        set alias "Proveedor2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
```

Figura 1 Anexo1: Configuración de la WAN Matriz, sucursales y data center por CLI

Fuente: Autor

MATRIZ

```
edit "port4"
    set vdom "root"
    set ip 192.168.10.1 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set type physical
    set device-identification enable
    set lldp-reception disable
    set role lan
    set snmp-index 4
    set secondary-IP enable
    config secondaryip
        edit 1
            set ip 192.168.11.1 255.255.255.0
            set allowaccess ping fabric
        next
        edit 2
            set ip 192.168.12.1 255.255.255.0
            set allowaccess ping fabric
        next
        edit 3
            set ip 192.168.13.1 255.255.255.0
            set allowaccess ping fabric
        next
        edit 4
            set ip 192.168.14.1 255.255.255.0
            set allowaccess ping fabric
        next
        edit 5
            set ip 192.168.15.1 255.255.255.0
            set allowaccess ping fabric
        next
```

SUCURSAL GYE

```
edit "port4"
    set vdom "root"
    set ip 192.168.18.1 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set stpforward enable
    set type physical
    set device-identification enable
    set lldp-reception enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
    set secondary-IP enable
    config secondaryip
        edit 1
            set ip 192.168.19.1 255.255.255.0
            set allowaccess ping fgfm fabric ftm
        next
        edit 2
            set ip 192.168.20.1 255.255.255.0
            set allowaccess ping fabric
        next
        edit 3
            set ip 192.168.21.1 255.255.255.0
            set allowaccess ping fabric
        next
```

SUCURSAL UIO

```
edit "port4"
    set vdom "root"
    set ip 192.168.22.1 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set stpforward enable
    set type physical
    set device-identification enable
    set lldp-reception enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
    set secondary-IP enable
    config secondaryip
        edit 1
            set ip 192.168.23.1 255.255.255.0
            set allowaccess ping fgfm fabric
```

DATACENTER

```
edit "port4"
    set vdom "root"
    set ip 192.168.30.1 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set stpforward enable
    set type physical
    set device-identification enable
    set lldp-reception enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
next
```

Figura 2 Anexo1: Configuración de la LAN Matriz, sucursales y data center por CLI

Fuente: Autor

```
MATRIZ (virtual-wan-link) # sh
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.100.1
        next
        edit 2
            set interface "port2"
            set gateway 172.16.90.1
        next
```

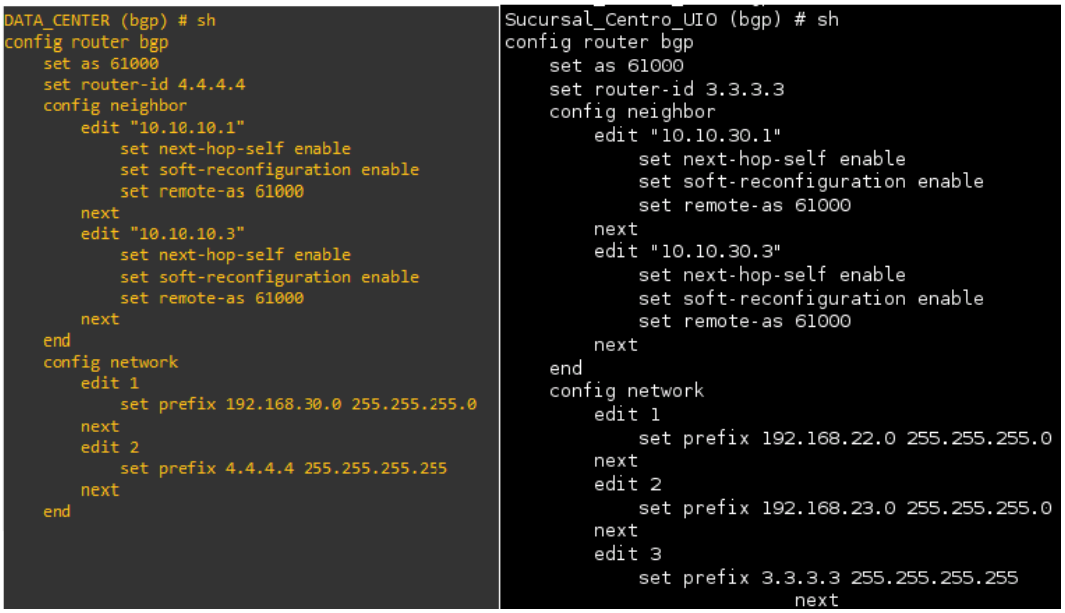
```
Sucursal_Norte_GYE (virtual-wan-link) # sh
config system virtual-wan-link
    set status enable
    set load-balance-mode measured-volume-based
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.150.1
        next
        edit 2
            set interface "port2"
            set gateway 172.16.70.1
        next
```

```
Sucursal_Centro_UIO (virtual-wan-link) # sh
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.200.1
        next
        edit 2
            set interface "port2"
            set gateway 172.16.80.1
        next
```

```
DATA_CENTER (virtual-wan-link) # sh
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.110.1
        next
        edit 2
            set interface "port2"
            set gateway 172.16.60.1
        next
```

Figura 3 Anexo1: Configuración SD-WAN por CLI de matriz, sucursales y datacenter

Fuente: Autor

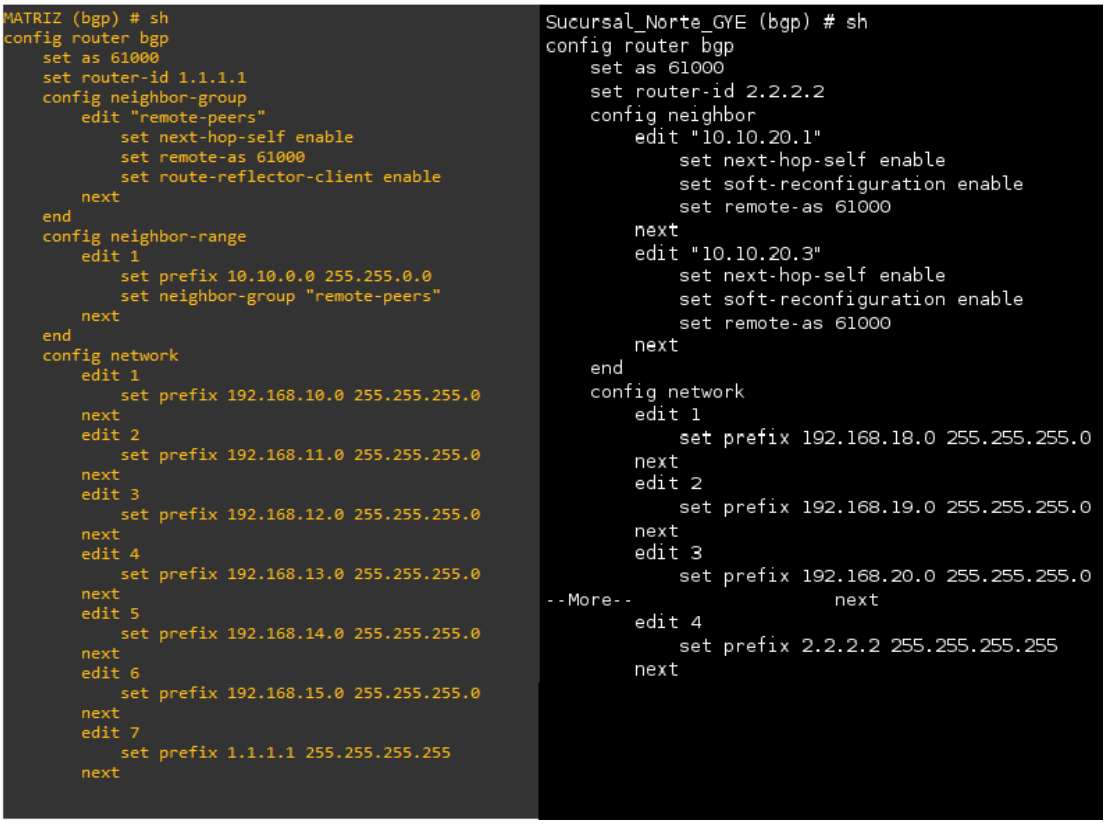


```
DATA_CENTER (bgp) # sh
config router bgp
    set as 61000
    set router-id 4.4.4.4
    config neighbor
        edit "10.10.10.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
        edit "10.10.10.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
    end
    config network
        edit 1
            set prefix 192.168.30.0 255.255.255.0
        next
        edit 2
            set prefix 4.4.4.4 255.255.255.255
        next
    end
```

```
Sucursal_Centro_UIO (bgp) # sh
config router bgp
    set as 61000
    set router-id 3.3.3.3
    config neighbor
        edit "10.10.30.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
        edit "10.10.30.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
    end
    config network
        edit 1
            set prefix 192.168.22.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.23.0 255.255.255.0
        next
        edit 3
            set prefix 3.3.3.3 255.255.255.255
                        next
```

Figura 4 Anexo1: Configuración de BGP en Matriz y sucursal GYE.

Fuente: Autor



```
MATRIZ (bgp) # sh
config router bgp
    set as 61000
    set router-id 1.1.1.1
    config neighbor-group
        edit "remote-peers"
            set next-hop-self enable
            set remote-as 61000
            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 192.168.10.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.11.0 255.255.255.0
        next
        edit 3
            set prefix 192.168.12.0 255.255.255.0
        next
        edit 4
            set prefix 192.168.13.0 255.255.255.0
        next
        edit 5
            set prefix 192.168.14.0 255.255.255.0
        next
        edit 6
            set prefix 192.168.15.0 255.255.255.0
        next
        edit 7
            set prefix 1.1.1.1 255.255.255.255
        next
```

```
Sucursal_Norte_GYE (bgp) # sh
config router bgp
    set as 61000
    set router-id 2.2.2.2
    config neighbor
        edit "10.10.20.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
        edit "10.10.20.3"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 61000
        next
    end
    config network
        edit 1
            set prefix 192.168.18.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.19.0 255.255.255.0
        next
        edit 3
            set prefix 192.168.20.0 255.255.255.0
--More--                    next
        edit 4
            set prefix 2.2.2.2 255.255.255.255
        next
```

Figura 5 Anexo1: Configuración de BGP en Matriz y sucursal UIO.

Fuente: Autor

Anexo 2

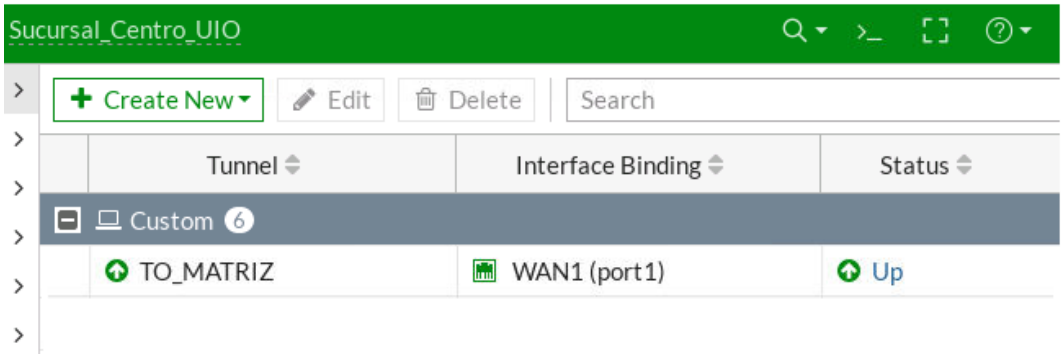


Figura 1 Anexo2: Túneles levantados visto desde Fortigate Sucursal UIO

Fuente: Autor

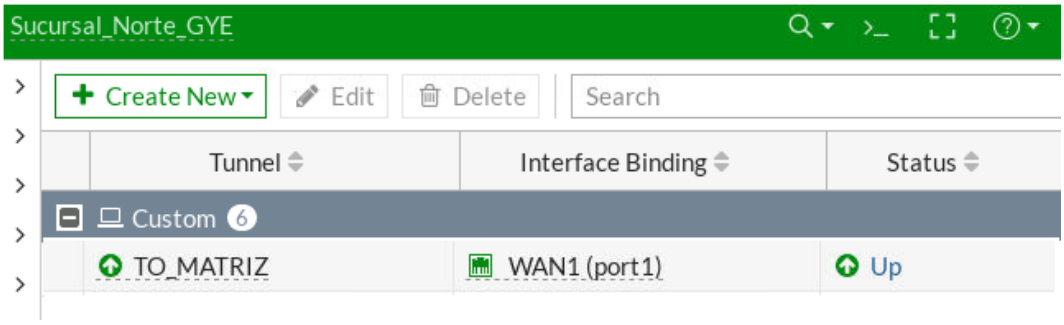


Figura 2 Anexo2: Túneles levantados visto desde Fortigate Sucursal GYE

Fuente: Autor

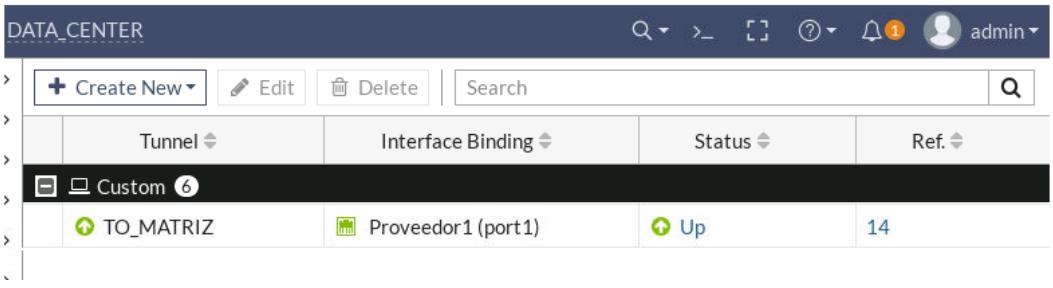


Figura 3 Anexo2: Túneles levantados visto desde Fortigate Sucursal GYE

Fuente: Autor

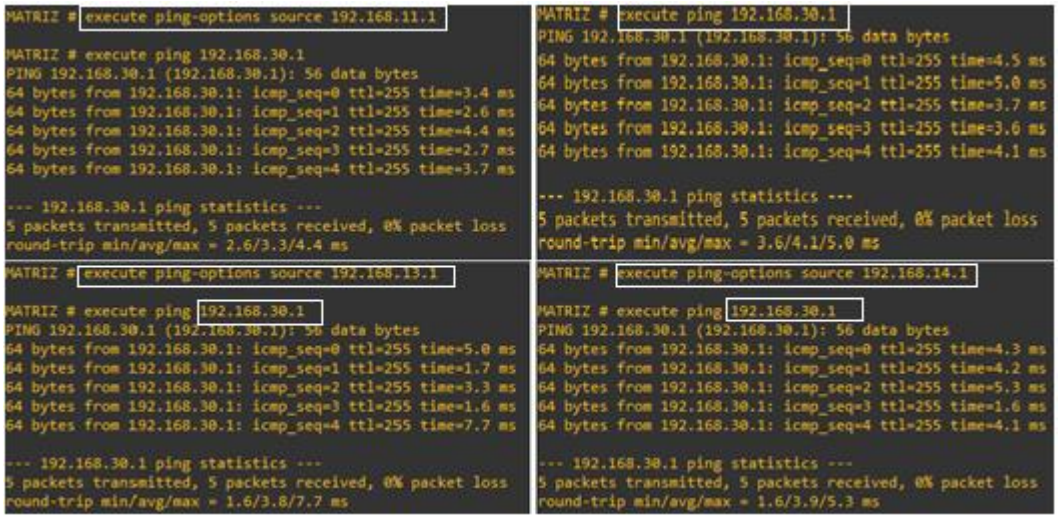


Figura 4 Anexo2: Comunicación entre Matriz-Sucursal UIO

Fuente: Autor

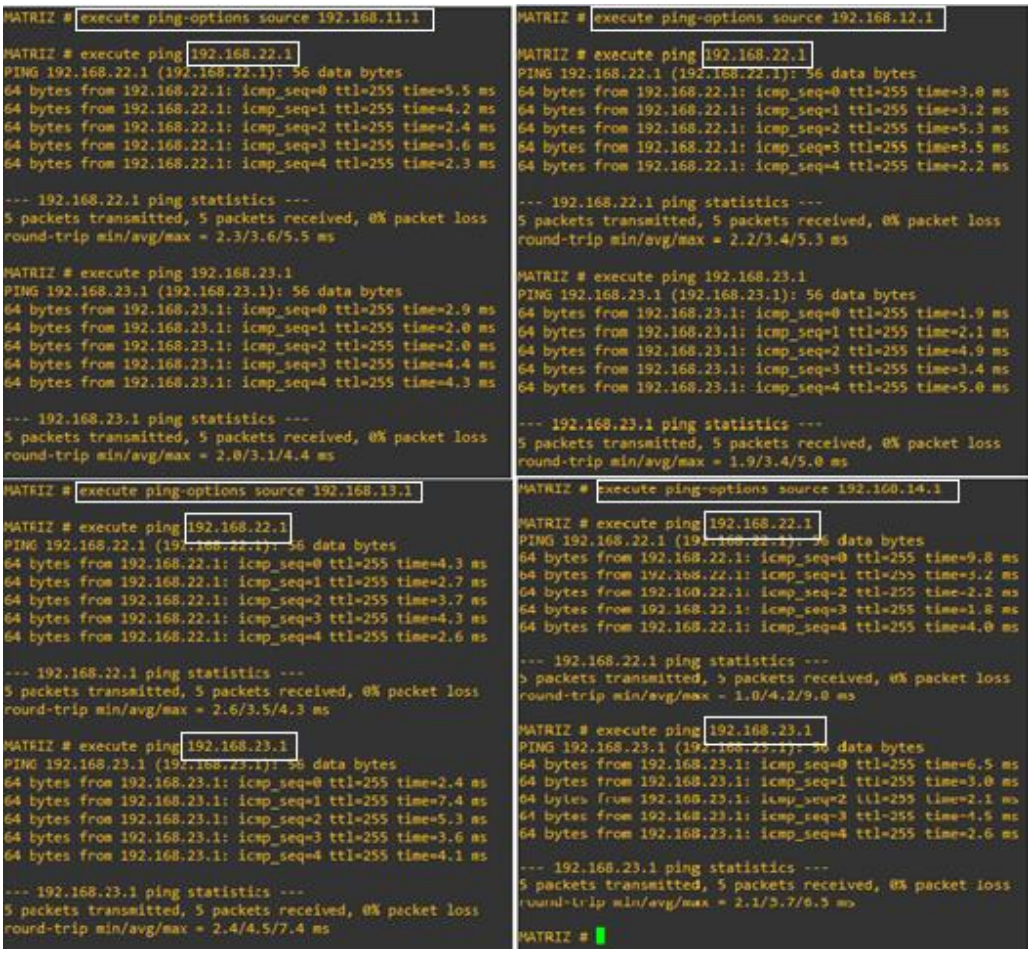


Figura 5 Anexo2: Comunicación entre Matriz-Datacenter

Fuente: Autor

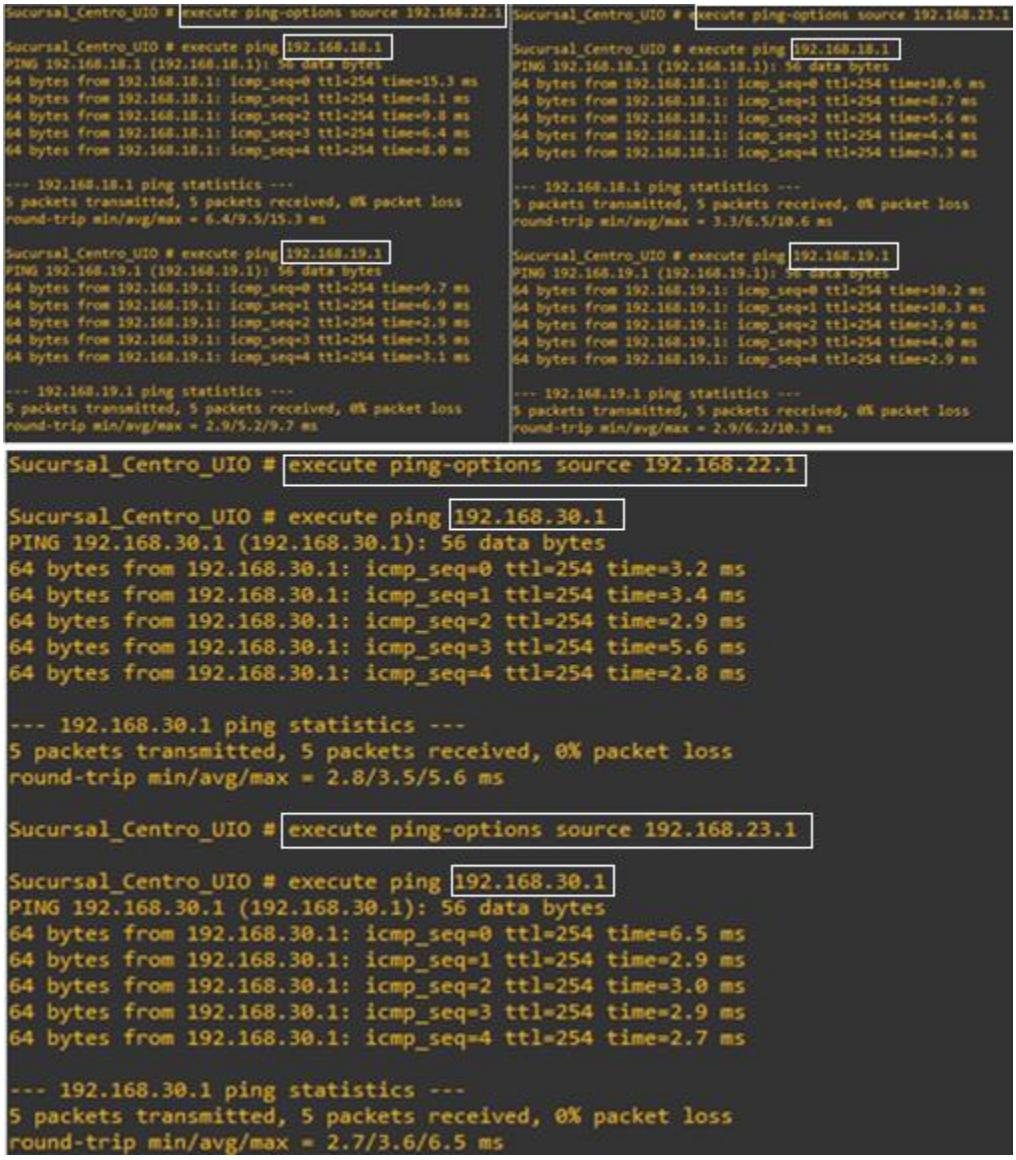


Figura 6 Anexo2: Comunicación entre Sucursal UIO- Sucursal GYE, UIO- Datacenter

Fuente: Autor

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Luis Andres Marin Santamaria**, con C.C: # **0927689919** autor del trabajo de titulación: **Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos,** 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, a los 13 días del mes agosto del año 2021

f. _____

Nombre: Luis Andres Marin Santamaria, Ing.

C.C: 0927689919

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

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

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos	
AUTOR(ES)	Luis Andres Marin Santamaria	
REVISOR(ES)/TUTOR	MSc. Luis Córdova Rivadeneira; MSc. Edgar Quezada Calle/ MSc. Ilen Rivero Pouymiro	
INSTITUCIÓN:	Universidad Católica Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	Guayaquil, 13 de agosto de 2021	No. DE PÁGINAS: 113
ÁREAS TEMÁTICAS:	Redes, MPLS, enrutamiento virtual, SD-WAN, Seguridad, GNS3	
PALABRAS CLAVES/ KEYWORDS:	SD-WAN, Tecnologías, WAN, Fortigate, SLA, seguridad, túneles	

RESUMEN/ABSTRACT: Debido a la emergencia sanitaria que el país se encuentra atravesando la compañía Construl S.A. se ha visto en la necesidad de optimizar el uso de sus recursos tecnológicos debido a la implementación del teletrabajo y nuevos requerimientos de servicios, sin encarecer sus costos y manteniendo la calidad de los recursos que se utilizan en el desarrollo de sus labores. Por tal motivo, se da paso al estudio de disponibilidad y factibilidad de implementación de nuevas tecnologías que permitan mantener un equilibrio económico a la empresa Construl S.A. Este estudio propone la implementación de la tecnología SD-WAN (del inglés wide area network) que permite a los usuarios realizar trabajos constantes, sin perder la comunicación en ningún momento, al activar enlaces de respaldo o backups, cuando el enlace de conexión principal falle. La tecnología SD-WAN no requiere del uso de un número alto de megabytes de ancho de banda o recursos de red. Para el desarrollo y demostración de las ventajas y mejoras que esta tecnología trae a las empresas se usa un simulador que facilita la demostración. Finalmente se determina que la implementación de esta tecnología cumple con lo requerimientos tecnológicos de la compañía Construl S.A.

ADJUNTO PDF:	■ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-984180134	**E-mail:** dmarinsantamaria@gmail.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):	