UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

DISEÑO DE IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD GESTIONADA CON SD-WAN PARA UNA RED MPLS QUE PROVEE SERVICIOS DE INTERNET Y DATOS PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA

AUTOR:

MARÍA FERNANDA RODRÍGUEZ LIMONES

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

TUTOR:

MSC. MANUEL ROMERO PAZ

Guayaquil, a los 10 días del mes noviembre 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 María Fernanda Rodríguez Limones como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

MSC. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

MSc. Manuel Romero Paz

Guayaquil, a los 10 días del mes noviembre del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, María Fernanda Rodríguez Limones

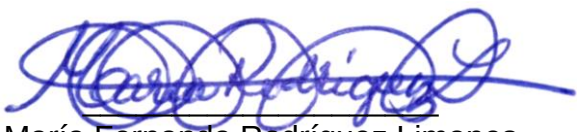
DECLARO QUE:

El trabajo de Titulación **"**Diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana**"** 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 10 días del mes noviembre del año 2021

EL AUTOR



María Fernanda Rodríguez Limones

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, María Fernanda Rodríguez Limones

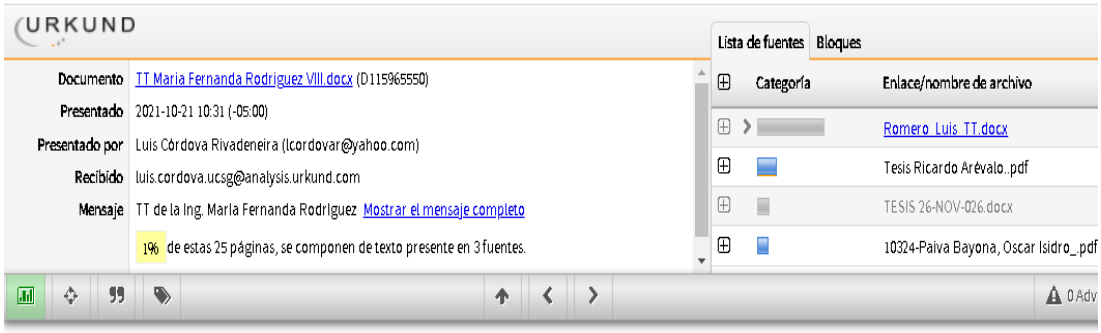
Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación, **"**Diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana**"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 10 días del mes noviembre del año 2021

EL AUTOR

María Fernanda Rodríguez Limones

REPORTE URKUND



SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA: DISEÑO DE IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD GESTIONADA CON SD-WAN PARA UNA RED MPLS QUE PROVEE SERVICIOS DE INTERNET Y DATOS PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA

AUTOR: MARÍA FERNANDA RODRÍGUEZ LIMONES

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

TUTOR: MSC. MANUEL ROMERO PAZ

Guayaquil, a los 25 días del mes junio del año 2020

SISTEMA DE POSGRADO MAESTRÍA EN

TELECOMUNICACIONES

Dedicatoria

Dedico este trabajo con todo amor a Dios, ya que sin él no hubiera sido posible lograr esta meta, ni compartir tanta alegría con mi familia.

A mis padres por darme siempre su apoyo incondicional y depositar su entera confianza en cada paso que doy, demostrando cada uno de los valores que me fueron inculcados.

Agradecimientos

Agradezco a Dios por permitirme llegar hasta este momento tan anhelado, por guiarme siempre por el camino indicado, sin desviarme de la meta.

A mi padre, Arcelino Rodríguez, por su amor y por ser un apoyo incondicional y un ejemplo a seguir, enseñándome que se puede salir adelante a pesar de cualquier situación.

A Sonia Limones, por ser una excelente madre, dándome siempre su cariño y los mejores consejos, por enseñarme a no rendirme sin importar lo complicado que sean los obstáculos.

Un agradecimiento total a todos los docentes de la Maestría de Telecomunicaciones y a todos mis compañeros, con quienes compartimos momentos amenos y sembramos una gran amistad.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Manuel Romero Paz
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

_____

MSc. Edgar Quezada Calle
REVISOR

RESUMEN:

El presente trabajo describe el diseño de un esquema SD-WAN utilizando Firewalls marca Fortigate para la Universidad Politécnica Salesiana, con el fin de poder balancear la carga de tráfico a través de dos proveedores de servicios de internet y datos, siendo estos Telconet y Cedia. El balanceo de carga podrá permitir a los equipos Fortigate elegir la mejor ruta, es decir, el camino que cumpla con los parámetros necesarios de calidad de servicio para poder enviar datos hacia las distintas sedes, evitando de esta manera que se produzcan saturaciones o tiempos elevados de respuestas. El diseño utilizará ambos proveedores en modo activo – activo, dicho de otra manera, cada proveedor enviará constantemente datos establecidos mediante reglas, que a su vez también servirán como contingencia en caso de que exista algún inconveniente lógico o físico con uno de los proveedores antes mencionados, ofreciendo de esta manera un servicio confiable por los perfiles de seguridad, y operatividad constante al usuario final.

Palabras clave: SD-WAN, balanceo, ruta, contingencia, seguridad, tiempo de respuesta, calidad de servicio, operatividad.

ABSTRACT

This paper describes the design of an SD-WAN scheme using Fortigate brand Firewalls for the Universidad Politécnica Salesiana, in order to be able to balance the traffic load through two internet and data service providers, these being Telconet and Cedia. Load balancing may allow Fortigate teams to choose the best route, that is, the path that meets the necessary quality of service parameters to be able to send data to the different locations, thus avoiding saturations or high times. of responses. The design will use both providers in active-active mode, in other words, each provider will constantly send data established by rules, which in turn will also serve as a contingency in case there is a logical or physical problem with one of the aforementioned providers, thus offering a reliable service due to the security profiles and constant operability to the end user.

Keywords: SD-WAN, balance, route, contingency, response time, security, quality of service, operability

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

ÍNDICE DE TABLAS

Capítulo 1: Diseño metodológico

Durante este capítulo se desarrollará una breve introducción y se explicarán los motivos por los cuáles nace la urgencia del tema de investigación, detallando el problema que se tiene actualmente en la Universidad Politécnica Salesiana y los objetivos que se plantearon para poder cumplir con la meta y obtener los resultados esperados.

1.1 Introducción

El presente proyecto trata sobre el diseño de implementación de un sistema de seguridad gestionada con SD-WAN (Software-Defined Wide Area Network) para una red MPLS (Multiprotocol Label Switching) que provee servicios de internet y datos para la Universidad Politécnica Salesiana, además de equipos Fortigate.

Se encuentra enfocado en convertirse en una solución para una Institución Educativa que actualmente tiene problemas de saturación en los enlaces de datos e internet debido a la cantidad de usuarios que utilizan sus aplicaciones y plataformas.

El objetivo principal de la aplicación es enrutar automáticamente el tráfico al siguiente mejor enlace disponible en caso de una interrupción del enlace principal, ofreciendo una experiencia de usuario mejorada.

En el capítulo 1 se detallan los hechos preliminares como, antecedentes, problemática, técnicas, metodología, así como el impacto del proyecto recibido por los usuarios.

En el capítulo 2 se explican los conceptos generales, descripción y características de los elementos que conforman el SD-WAN y sus políticas.

Durante el capítulo 3 y 4 se elabora el análisis y diseño del proyecto, se explican paso a paso las configuraciones realizadas, conclusiones y recomendaciones.

1.2 Antecedentes

Dado los grandes avances en comunicaciones y conectividad corporativa en las redes privadas, las MPLS proporcionan seguridad a la hora de poder comunicar las distintas sedes de una empresa de una forma fiable y segura.

En todas las empresas surge la necesidad de que los tiempos de respuesta, al momento de realizar alguna petición sea la más rápida y ágil, sin perder conexión, más aun refiriéndose a una Institución Educativa, por este motivo se desea desarrollar el diseño de un Sistema de Seguridad Gestionada con SD-WAN para una red MPLS, con esto se descongestionará los sistemas de enrutamiento que soportaban una enorme carga, en lugar de dejar que sean las estaciones intermedias las que determinen la mejor ruta del paquete de datos.

Dado que las empresas acceden directamente a internet, es fundamental implementar estrategias de seguridad de última generación junto con la habilitación de una red WAN (Wide Area Network) de múltiples rutas para mejorar el rendimiento de las aplicaciones.

La SD-WAN de Fortigate reemplaza los enrutadores de la WAN y los dispositivos de seguridad y optimización por separado con una única solución que reconoce las aplicaciones.

Con el diseño que propone este tema de tesis se desea obtener la satisfacción de los usuarios tanto a nivel administrativo como estudiantil.

1.3 Definición del problema

Dado el notorio aumento de estudiantes en la Universidad Politécnica Salesiana, se ha tenido la necesidad de construir nuevas instalaciones en diferentes sectores, lo cual provoca el incremento del consumo en los servicios de datos, internet y telefonía, dando como resultado saturación en los enlaces, además de tiempos elevados en procesos administrativos internos y atención a trámites estudiantiles.

En el presente proyecto se diseñará la implementación de un sistema de seguridad gestionada con SD-WAN, para determinar la manera más eficaz de enrutar el tráfico a puntos remotos, en este caso a las demás sedes de la Universidad, a partir del siguiente problema de investigación:

La necesidad de contar con un diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana a causa del incremento de estudiantes.

1.4 Objetivos

Los objetivos planteados para este trabajo son los siguientes:

1.4.1 Objetivo general

Diseñar la implementación de un sistema de seguridad gestionada con SDWAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana.

1.4.2 Objetivos específicos

- Contrastar las diferencias entre las redes MPLS tradicionales y las que utilizan optimización SD-WAN.

- Examinar el comportamiento de las soluciones SD-WAN, con los diferentes algoritmos de balanceo de carga.

- Identificar las necesidades y requerimientos de la Universidad Politécnica Salesiana, a nivel de redes y enrutamiento.

- Diseñar la infraestructura lógica optimizando el uso del ancho de banda, maximizando la funcionalidad de la tecnología SD-WAN.

- Evaluar el desempeño de la red durante la transmisión de datos entre redes locales, remotas e Internet.

1.5 Justificación

Puesto que SD-WAN usa todos los servicios WAN disponibles de manera más eficaz y económica, proporciona a los usuarios de toda la Universidad la oportunidad de optimizar los procesos empresariales e innovar. También hace que la gestión de WAN sea más rentable.

Este proyecto tiene como finalidad ofrecer a la Universidad Politécnica Salesiana un sistema que conmuta por defecto rápida y automáticamente al mejor vínculo disponible. Esta transición no afecta a los usuarios, que continúan teniendo un rendimiento eficiente de la aplicación. Una vez que se estabiliza el vínculo principal, Fortigate vuelve a conmutar por error automáticamente al vínculo principal.

1.6 Hipótesis

Mediante el diseño de un sistema de seguridad gestionada con redes definidas por software SDWAN, la Universidad Politécnica Salesiana sede Guayaquil podrá incrementar servicios aparte de datos e internet. La saturación en los enlaces disminuirá notablemente mediante las SDWAN, el acceso a trámites administrativos será mucho más ágil y el uso de las plataformas de la Universidad serán seguras y con tiempos de respuesta

inmediata. Tendrá una herramienta en la que podrá monitorear el uso de distintas aplicaciones, y el consumo en los enlaces contratados con su proveedor.

1.7 Metodología

A continuación, se detalla la metodología de investigación a aplicarse en este trabajo:

1.7.1 Métodos

Para el desarrollo de esta investigación se han utilizado dos métodos:

Método explicativo

Se empleó el método explicativo al analizar el comportamiento de las soluciones SD-WAN, con los diferentes algoritmos de balanceo de carga. El objetivo de este modelo es observar las secuencias de causa-efecto del diseño de un sistema de seguridad gestionada con SD-WAN.

Método deductivo

Después de haber efectuado un estudio previo tanto en conceptos como en análisis de tráfico que abarcan las telecomunicaciones, se realiza el diseño de un sistema de seguridad gestionada con SD-WAN para una red MPLS.

Capítulo 2: Red MPLS

MPLS es un estándar que surgió para conciliar distintas soluciones de conmutación multinivel. Es posible considerar MPLS como un avance en las tecnologías de enrutamiento y reenvío en las redes IP (Internet Protocol), lo que implica una evolución en la manera de construir y gestionar estas redes.

2.1 Características MPLS

MPLS se encuentra situado entre las capas de enlace de datos y de red del modelo OSI (Open Systems Interconnection), se podría considerar que es un protocolo de la unión entre la capa de enlace y la de red. MPLS emplea IP como direccionamiento de nivel 3. Hace uso de los protocolos de routing IP heredados, por medio de los cuales, MPLS dispone de un conocimiento preciso del estado de la red, incluyendo la Ingeniería de tráfico, plano de control MPLS. Será necesario añadir extensiones TE (Trafic Extension):

- Se habilitan mecanismos de señalización, su empleo siempre precederá al establecimiento de una comunicación extremo-extremo. LDP (Label Distribution Protocol) y RSVP (Resource Reservation Protocol) son los protocolos de señalización elegidos, los cuales soportarán reserva de recursos para satisfacer TE.

- Cada conexión transita por un trayecto virtual extremo a extremo. El cual es pactado y establecido según el estado de la red y las necesidades de la conexión.

- El proceso de Forward no actúa sobre el contenido de nivel 3 de cada paquete. Se añade una etiqueta a cada paquete, en función de ésta se realiza el Forward. La interpretación y sustitución de cada etiqueta se circunscribe a un ámbito local, es decir, en cada conmutador MPLS.

- MPLS añade a IP un nivel orientado a la conexión.

- IP dispondrá de señalización TE orientada a tráfico (RSVP-TE) o clase de servicio (CR-LDP – Constraint Route - Label Distribution Protocol) en MPLS se acelera y simplifica el proceso de Forward.

- El proceso de Forward se abstrae de los niveles superiores, permitiendo desarrollar MPLS en los actuales conmutadores ATM (Asyncronous Transfer Mode), Frame Relay, Ethernet y por supuesto routers/switches IP.

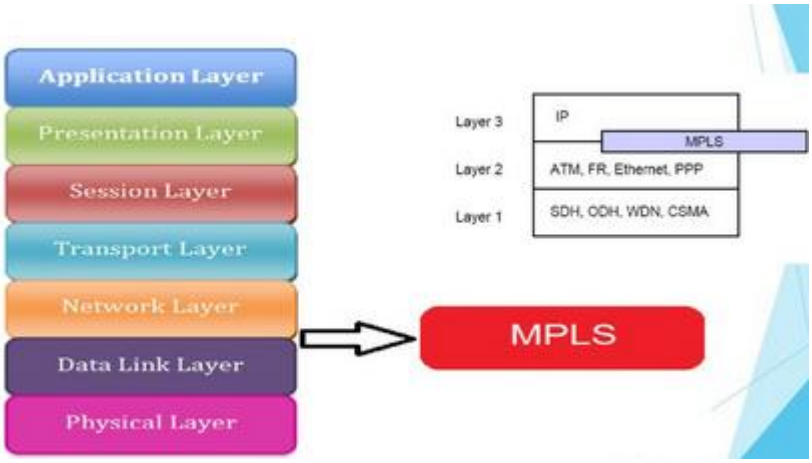


Figura 2. 1 Modelo OSI
Fuente: (Aguilar, 2020)

2.1.1 Arquitectura de MPLS

Una red MPLS se compone de 3 tipos de enrutadores LSR (Label Switching Router), figura 2.2:

- **Ingress LSR:** Es un LSR de borde por donde ingresan los paquetes sin etiquetar.
- **LSR intermedio:** son enrutadores que se encuentran en el medio de la red y reenvían los paquetes etiquetados.

- **Egress LSR:** Es el LSR de salida, se encarga de retirar todas las etiquetas antes de entregar el paquete a su destino.

2.1.2 Beneficios de usar MPLS

MPLS es una tecnología ampliamente utilizada por la gran mayoría de empresas a nivel mundial, principalmente por proveedores de servicios de Internet y grandes operadoras de Telecomunicaciones.

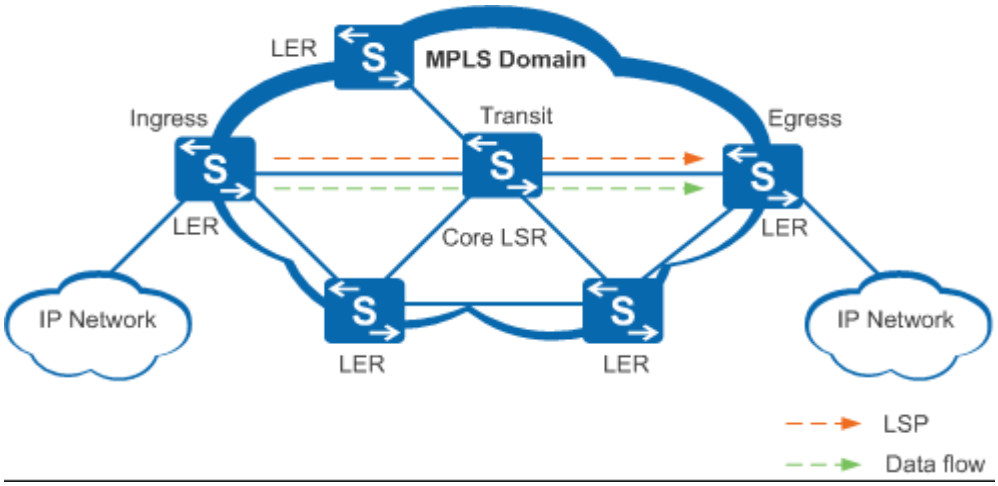


Figura 2. 2 Arquitectura MPLS
Fuente: (Hernandez, 2019)

Esto es debido a que proporciona un gran número de ventajas en cuanto a la operación y la eficiencia del transporte de servicios de voz, datos y video en entornos de gran complejidad y donde es importante maximizar la experiencia de usuario.

Entre sus principales beneficios se encuentran:

- Reduce considerablemente la latencia al tomar decisiones de conmutación basadas en etiquetas.

- Incrementa el rendimiento de la red.
- Posee mecanismos de MPLS QoS (Quality of Service) que permiten diferenciar servicios y priorizar el tráfico por su importancia o naturaleza.

- Es de fácil implementación y despliegue.

- Incluye métodos de Ingeniería de Tráfico para optimizar el ancho de banda y reducir la congestión.

- Proporciona la capacidad de administrar alto volumen de tráfico en redes de gran tamaño, sin reducir la eficiencia (Telecapp, 2021).

El principal objetivo de MPLS, es estandarizar una tecnología base que integre el intercambio de etiquetas durante el reenvío de paquetes con el sistema de enrutamiento actual de redes.

Esta tecnología mejora la relación precio/desempeño del enrutamiento que se realiza en la capa de red, la cual mejora la escalabilidad de la misma capa y provee una gran flexibilidad en la entrega de servicios de enrutamiento.

Es una herramienta efectiva para ser aplicada en grandes Backbones, dado que:

- Permite obtener estadísticas de uso LSP (Label Switched Path), que se pueden utilizar en la planificación de la red y como herramienta de análisis de cuellos de botella y carga en los enlaces, lo cual es de gran utilidad para planes de expansión futura.

- MPLS permite hacer Encaminamiento Restringido CBR (Constraint Based Routing) de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales como, por ejemplo: Garantías explícitas de retardo, Ancho de banda, Perdida de paquetes, etc.

2.1.3 Soporte a las clases de servicio (CoS, Class of Service)

Normalmente las redes IP solo ofrecían una clase de servicio Best Effort (mejor esfuerzo), pero actualmente se desea emplear todo tipo de tráfico como lo es voz, datos y video, por lo que MPLS es la solución a todos estos inconvenientes, ya que con el Modelo DiffServ (Servicios Diferenciados) se puede clasificar el tráfico con distintas prioridades en base a las necesidades del usuario (Tapasco, 2008).

2.1.4 Reenvío de paquetes MPLS

Los paquetes MPLS entran en la red a través de un LSR de entrada (Ingress LSR) y salen de ella a través de uno de salida (Egress LSR). La vía que toma un paquete de un lado a otro se denomina LSP, ésta ruta es construida a partir de la información que se toma de una FEC. Un LSP trabaja en un esquema orientado a conexión, es decir que la ruta tiene que ser formada antes de que cualquier flujo de tráfico empiece a circular por éste.

Cuando un paquete atraviesa la red MPLS, cada LSR cambia la etiqueta entrante por una nueva saliente, tal como el mecanismo usado por ATM donde los VPI/VCI (Virtual Path Identifier / Virtual Channel Identifier) son cambiados por un par diferente cuando salen del Switch ATM, este proceso continúa hasta que el último LSR ha sido alcanzado.

2.1.5 Elementos necesarios de una red MPLS

A continuación, se detallan los elementos necesarios en una red MPLS:
La etiqueta: Posee toda la información de los enrutadores MPLS para determinar el camino por dónde se debe reenviar los datos para lograr una buena velocidad de transmisión.

Experimental: Se usan bits experimentales para mejorar la calidad de servicio, debido a estos bits se le puede dar prioridad a paquetes de

información sobre otros, esto dependiendo de las actividades que realicen los usuarios de la red.

Parte inferior de la pila: Es aquel mensaje que indica a los enrutadores que no existen más paquetes que compartir y que los paquetes anteriores fueron enviados de manera exitosa.

Tiempo de vida: Es el número de veces que un paquete puede ser enviado antes de ser descartado.
Con todos estos elementos antes mencionados, se puede transmitir información en dos puntos de dos ubicaciones separadas por grandes distancias geográficas como sería una oficina en Latinoamérica y una central en Canadá, puede conectarse y visualizar información a través del protocolo IP gracias a la red MPLS (Figura 2.3).

2.2 SD-WAN

Las soluciones de red SD-WAN transforman las capacidades de una organización al aprovechar la red corporativa WAN, así como la conectividad de múltiples nubes para poder brindar un rendimiento de aplicaciones de alta velocidad en el borde de dicha red de las sucursales. Uno de los principales beneficios de la SD-WAN es que proporciona una selección de ruta dinámica entre las opciones de conectividad, MPLS, 4G/5G o banda ancha, lo que garantiza que las organizaciones puedan acceder rápida y fácilmente a las aplicaciones de nube críticas para el negocio.

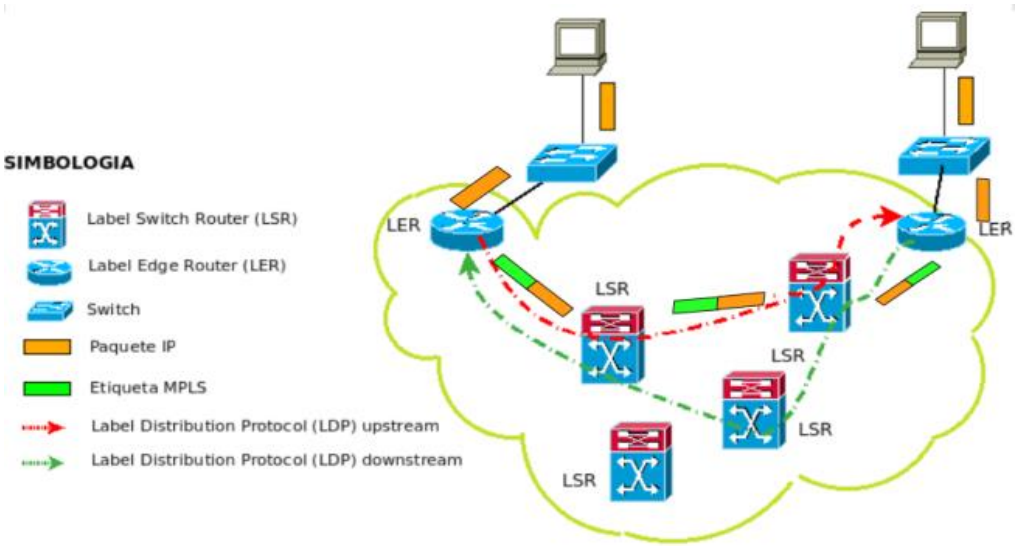


Figura 2.3 Elementos de una red MPLS
Fuente: (edualejo77, 2011)

Las soluciones SD-WAN son cada vez más populares a medida que las organizaciones solicitan conectividad rápida, escalable y flexible entre diferentes entornos de red y buscan reducir el costo total de propiedad general al mismo tiempo que preservan la experiencia del usuario (Fortinet, 2021).

2.2.1 Historia y evolución de SD-WAN

La tecnología SD-WAN moderna evolucionó a partir de soluciones de red anteriores, como líneas arrendadas punto a punto (PPP, Point-to-Point Protocol), frame relay y MPLS. PPP era el modo original para conectar múltiples redes de área local (LAN, Local Área Network) antes de que frame relay eliminara la necesidad de comprar y administrar enlaces de conexión individuales entre varias ubicaciones corporativas.

En la década de 2000, MPLS se hizo popular y pronto superó en popularidad al frame relay debido a la forma en que se aprovecha la tecnología basada en el IP para llevar funciones previamente separadas como redes de voz, video y datos a la misma red. En la actualidad, MPLS es la tecnología más común en uso para las WAN corporativas por la latencia reducida y los beneficios de QoS que proporciona.

En la década de 2010, específicamente en 2013, nació SD-WAN y a medida que más técnicos la examinaron por sus beneficios, se dieron cuenta de muchas de las mismas ventajas que SD-WAN tiene sobre MPLS, similar a cómo MPLS traía más ventajas que frame relay. Como una explicación simple, SD-WAN ofrece QoS a nivel de MPLS a la vez que es significativamente menos costoso y mucho más fácil de escalar.

SD-WAN puede manejar gran variedad de conexiones y mover dinámicamente el tráfico sobre el mejor transporte disponible y proporcionar tanto redundancia como mucha más capacidad utilizando enlaces de menor costo. Las soluciones SD-WAN son significativamente más baratas que MPLS en general cuando también se consideran el tiempo de instalación y el tiempo de entrega del servicio.

2.2.2 Cómo funciona la SD-WAN

SD-WAN conecta a los usuarios a cualquier aplicación donde sea que se encuentre desde el centro de datos a la nube. Determina de forma inteligente qué ruta satisface mejor los requerimientos de rendimiento ideales para una aplicación específica.

Luego encamina el tráfico a la ruta ideal de la WAN, mientras que las arquitecturas tradicionales solo tienen la capacidad de enrutar todas las aplicaciones a través de MPLS.

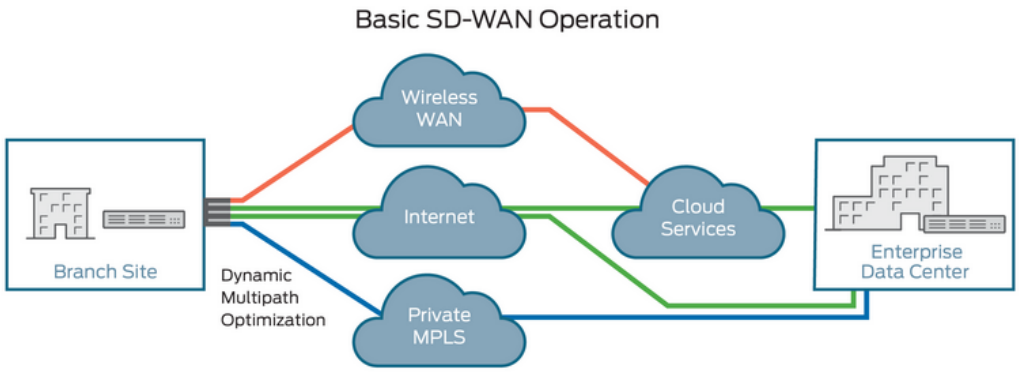


Figura 2. 4 Operación básica de SD-WAN
Fuente: (Sánchez, 2020)

2.2.3 Conocimiento de la aplicación

Con las soluciones WAN tradicionales, las organizaciones presentan una calidad de experiencia menos que ideal y les resulta difícil ofrecer un ancho de banda de alto rendimiento para aplicaciones críticas. Debido a que las arquitecturas WAN heredadas dependen del enrutamiento de paquetes, carecen de una visibilidad detallada de la aplicación.

Sin embargo, las soluciones SD-WAN identifican de manera inteligente las aplicaciones desde el primer paquete de tráfico de datos. Los equipos de red obtienen la visibilidad que necesitan sobre qué aplicaciones se utilizan más ampliamente en toda la organización, lo que les ayuda a aplicar políticas y tomar decisiones más inteligentes y mejor informadas (Fortinet, 2021).

2.2.4 Selección de ruta dinámica

SD-WAN permiten seleccionar una ruta dinámica para que fluya el tráfico. La solución SD-WAN puede identificar de manera inteligente las aplicaciones y determinar la mejor ruta que debe tomar para optimizar la funcionalidad. Las capacidades de recuperación automática enrutan automáticamente el tráfico al siguiente mejor enlace disponible en caso de una interrupción del enlace principal.

Esta capacidad automatizada no solamente puede reducir la complejidad dentro de la red, sino que además ofrece una experiencia de usuario mejorada y por lo tanto mejora el rendimiento de las aplicaciones.

2.2.5 Implementación sin intervención

SD-WAN ofrece control y separación del plano de datos para garantizar una administración y orquestación centralizadas. SD-WAN permite implementaciones más rápidas con capacidades de aprovisionamiento sin intervención mientras escala.

2.2.6 Orquestación centralizada

El orquestador para Secure SD-WAN de Fortinet permite a las empresas simplificar la implementación centralizada y establecer la automatización para ahorrar tiempo y responder más rápido a las demandas del negocio.

La administración centralizada puede proporcionar un flujo de trabajo intuitivo para que las políticas diseñen estrategias para la distribución de aplicaciones y otro tráfico a través y entre las sucursales.

Con la visualización automatizada de superposición de VPN (Virtual Private Network), la conectividad en malla a través de los hubs y las sucursales, especialmente en implementaciones SD-WAN más grandes, se administra fácilmente con una sobrecarga mínima.

Los análisis mejorados para la disponibilidad de enlaces WAN, los SLA (Service Level Agreement) de rendimiento, el tráfico de aplicaciones en tiempo de ejecución y las estadísticas históricas permiten al equipo de infraestructura solucionar problemas y resolver rápidamente los problemas de red (FORTINET, 2021).

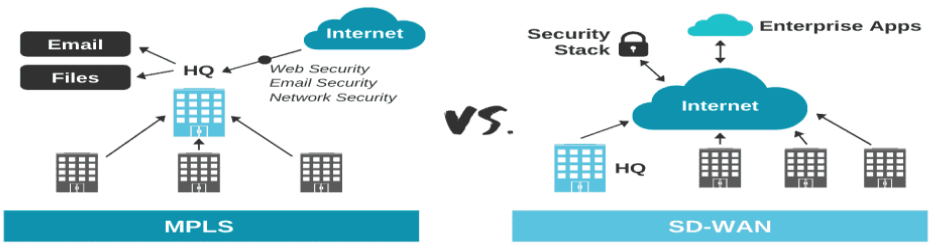


Figura 2. 5 Comparación entre red MPLS y SD-WAN
Fuente: (Parra, 2020)

2.2.7 Ventajas y desventajas

Conforme a estudios de la firma de investigación IDC (International Data Corporation), el mercado de SD-WAN continuará creciendo a una tasa superior al 30% durante los próximos años, aproximándose a los USD5.3 mil millones para el año 2023.

Muchas empresas están optando por soluciones SD-WAN para obtener una serie de beneficios, incluidos los siguientes:

Experiencia del usuario mejorada: La tecnología subyacente en SD-WAN permite que los sitios remotos se conecten más fácilmente a las redes, con menor latencia, mejor rendimiento y con una conectividad más segura.

CTP más bajo: MPLS y otras tecnologías de conectividad no solo están desactualizadas, también son más caras cuando se tiene en consideración el costo total de propiedad (CTP). SD-WAN reduce significativamente los costos de ancho de banda y, cuando puede ofrecer beneficios como el aprovisionamiento sin intervención, automatiza mejor los procesos y reduce la cantidad de equipos y administración manual necesarios para el éxito.

Simplicidad: SD-WAN utiliza la automatización y otros beneficios para hacer que la conectividad sea un proceso más simple en entornos mixtos, incluidos locales, híbridos y en la nube.

Preparación para múltiples nubes: Una nube múltiple no es lo mismo que una híbrida, en la que se integran nubes públicas y privadas para optimizar el rendimiento, la seguridad y la flexibilidad. Múltiples nubes simplemente significan que las organizaciones tienen la flexibilidad de seleccionar el mejor proveedor de nube para cada una de sus diversas necesidades de infraestructura y aplicaciones.

Mejor seguridad en general: Una solución SD-WAN debe tener seguridad integrada; de lo contrario, es solo una opción más de conectividad que desafortunadamente se convierte en un vector de ataque. Cuando se implementa de forma correcta, Secure SD-WAN mejora la seguridad de la empresa en general (FORTINET, 2021).

2.2.8 Principales capacidades de la solución SD-WAN

SD-WAN es la clave para que los equipos de TI empresariales solucionen los problemas del mundo real. La mayoría de las soluciones SD-WAN han tomado un enfoque centrado en el software, al ejecutarse en una localización centralizada con un CPE (Customer Premises Equipment) al borde del límite, o en un uCPE (universal CPE) en la localidad del cliente. Las soluciones SD-WAN normalmente incluyen las siguientes capacidades principales:

Gestión central y controles basados en la nube: Las soluciones de SD-WAN brindan una vista única que permite que los equipos de TI establezcan configuraciones de WAN a lo largo de varias localidades y circuitos virtuales.

Cifrado completo: La mayoría de las soluciones SD-WAN brindan seguridad a través de túneles IPSec (o de otro tipo de túneles cifrados) que protegen automáticamente las WAN virtuales privadas que cruzan redes públicas y compartidas.

Soporte a multiruta y multienlace con selección dinámica de rutas: La capacidad de vincular varios circuitos físicos en un único canal lógico para incrementar la capacidad y la confiabilidad es una de las principales funciones de SD-WAN. También debe de supervisar dinámicamente el rendimiento de las rutas y ajustar los flujos de tráfico que existen entre los circuitos físicos disponibles para equilibrar la carga y reducir la congestión y el exceso de suscripciones.

Condicionamiento de rutas y optimización de la WAN: Entre las capacidades están la compresión y la deduplicación de datos, la configuración del tráfico para controlar la contención y la latencia, el cacheo por el lado del cliente y la optimización de protocolos TCP (Transmission Control Protocol).

Servicios de seguridad de firewalls: La mayoría de las plataformas de SD-WAN proporcionan algún nivel de capacidades de firewall y de seguridad, que van desde el simple bloqueo basado en puertos TCP/UDP (User Datagram Protocol) a la detección y prevención de malware sofisticado.

Priorización de tráfico para calidad de servicio, con corrección de reenvío de errores: La categorización de las aplicaciones con gestión de tráfico para proporcionar garantías de ancho de banda para diferentes clases de servicio puede mejorar el rendimiento de latencia y pérdida en determinadas aplicaciones.

Controles basados en políticas y encadenamientos de servicios: Las plataformas SD-WAN normalmente proporcionan un redireccionamiento inteligente basado en políticas de tráfico y la capacidad de introducir dinámicamente el flujo de servicios de redes virtuales (VNF, Virtualized Network Function) como firewalls, filtros de contenido, proxies y otras funciones de la red, sin interrumpir a la red subyacente.

Derivación local para los servicios en la nube: Muchas soluciones SD-WAN permiten la inspección local y la creación de rutas de tráfico destinados a servicios de nubes confiables, como SalesForce, lo cual acaba con la necesidad de transmitir todo el tráfico a una ubicación centralizada para inspeccionarlo (SDxCentral LLC, 2018).

2.2.9 Capacidades avanzadas de ancho de banda SD-WAN

SD-WAN permite la creación de una red flexible, resistente y segura que puede brindar los servicios completos y la interconectividad a la SD-Branch remota que requieren las empresas digitales de hoy. Ahora es el segmento de tecnología de redes de más rápido crecimiento.

Según IDC, la optimización del ancho de banda WAN y la seguridad constante de las aplicaciones son las dos principales motivaciones para las implementaciones de SD-WAN.

SD-WAN no solo debe proporcionar conectividad WAN de bajo costo, sino que también debe garantizar que el rendimiento de las aplicaciones de comunicaciones unificadas críticas para el negocio se mantenga alto, sin comprometer la seguridad efectiva.

La corrección de la ruta WAN utiliza la corrección de errores de reenvío para superar las condiciones adversas de la WAN, como enlaces deficientes o ruidosos. Esto mejora la confiabilidad de los datos y brinda una mejor experiencia de usuario para aplicaciones como servicios de voz y video (SDxCentral LLC, 2018).

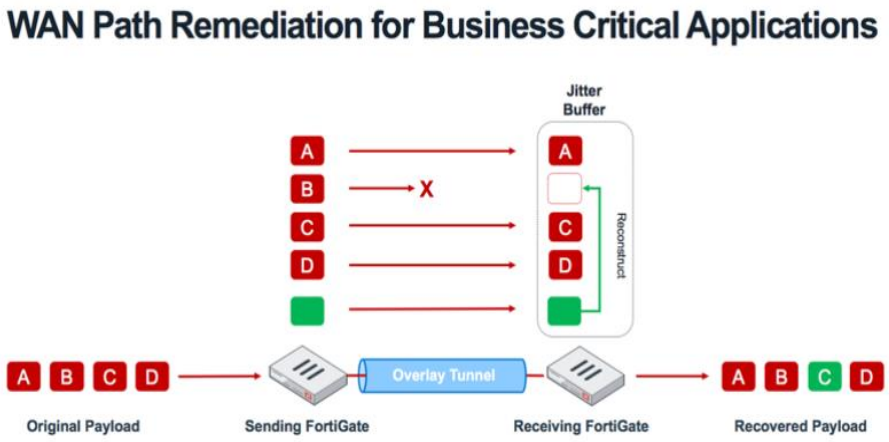


Figura 2. 6 Remediación de la ruta WAN
Fuente: (Shah, 2019)

2.2.10 Agregación SD-WAN

La agregación de WAN de ancho de banda de túnel utiliza el equilibrio de carga por paquete para maximizar la utilización del ancho de banda y garantizar que las aplicaciones de conversación tengan el rendimiento que necesitan, sin comprometer el ancho de banda de otras aplicaciones.

Para proporcionar una mejor visión de la gestión del ancho de banda, Fortinet Secure SD-WAN también puede detectar y reportar el ancho de banda WAN bajo demanda (Shah, 2019).

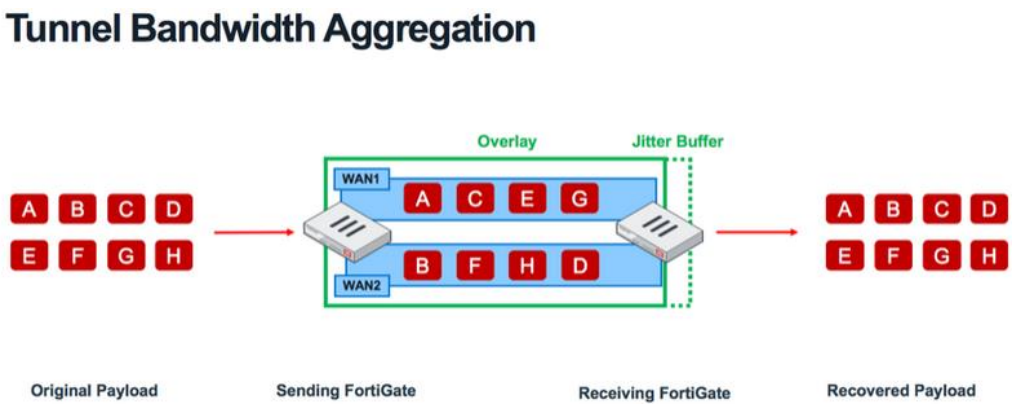


Figura 2. 7 Agregación de ancho de banda de un túnel
Fuente: (Shah, 2019)

La dirección de aplicaciones a través de una red VPN superpuesta acelerada proporciona la mejor calidad de experiencia en una WAN de bajo costo a través de una precisión de reconocimiento de aplicaciones mejorada combinada con una inspección SSL (Secure Sockets Layer) profunda y el menor impacto en el rendimiento.

2.2.11 Solución SD-WAN completa y de alto rendimiento

SD-WAN acelera el reconocimiento de aplicaciones y extiende la conectividad y funcionalidad de seguridad y el rendimiento desde la conexión SD-WAN a la WAN de la sucursal, optimizando la experiencia de SD-Branch.

Las organizaciones de hoy en día están cambiando cada vez más de MPLS a SD-WAN. Si bien muchas soluciones SD-WAN brindan

conectividad básica, luchan por brindar la gama completa de velocidad, interconectividad, flexibilidad y seguridad que realmente requieren las sucursales de hoy (Fortinet, 2021).

2.2.12 SD-WAN administrada

Los proveedores de SD-WAN administrados agregan valor a través de la experiencia que las empresas luchan por retener internamente, a través de la inversión continua en las últimas tecnologías SD-WAN para el beneficio de sus clientes y a través del conocimiento detallado de cómo las soluciones SD-WAN se integran con otros proveedores. particularmente proveedores de infraestructura en la nube (Figura 2.8).

2.2.13 SD-WAN contra internet público

El Internet de banda ancha disponible públicamente, en referencia a los servicios de Internet de alta velocidad que son más rápidos que la de alta velocidad tradicional, es ubicua y económica.

La Internet de banda ancha tampoco suele ser segura y los datos pueden verse comprometidos si los usuarios, especialmente los remotos, acceden a las redes utilizando una conexión no segura. La SD-WAN hace que la experiencia general sea sin problemas, más ágil y segura (si la seguridad está integrada correctamente). Figura 2.8.

2.2.14 Convierta la seguridad de SD-WAN en una prioridad

Una solución Secure SD-WAN está diseñada explícitamente para interoperar como una oferta única, idealmente con cada elemento que se ejecuta en el mismo sistema operativo y administrado mediante una interfaz de panel único.

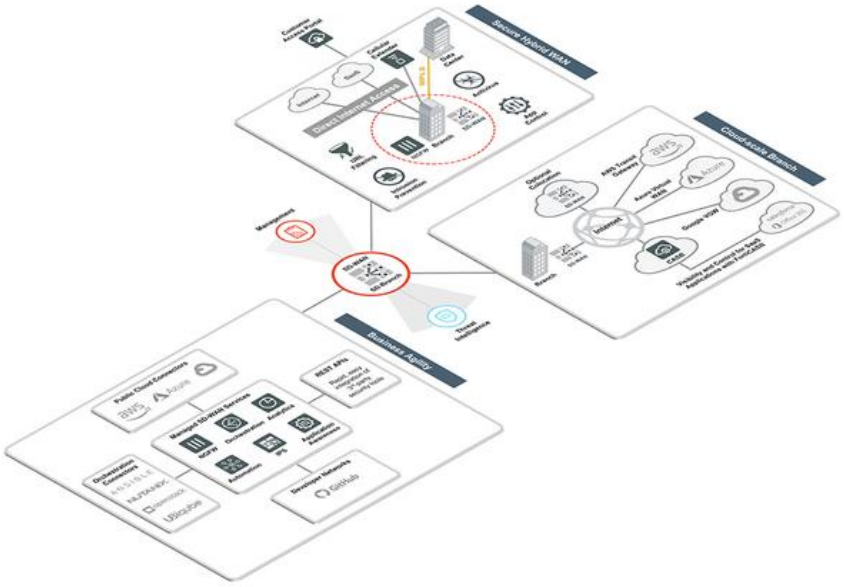


Figura 2. 8 Esquema de SD-WAN administrada
Fuente: (Fortinet, 2021)

Debido a la naturaleza dinámica y la alta escalabilidad de la SD-WAN, la seguridad de superposición no solo es muy costosa de implementar y mantener, sino que a menudo termina con demoras al reaccionar a los cambios de conectividad, lo que deja las conexiones críticas y los datos vulnerables. Un sistema integrado asegura que la conectividad SD-WAN, las funciones de administración del tráfico y la seguridad avanzada funcionen como una única solución holística (Fortinet, 2021).

2.2.15 Entender las razones empresariales para adoptar SD-WAN

Aunque se ha discutido mucho acerca de los principales impulsores empresariales para utilizar SD-WAN, la encuesta arroja más luz sobre los promotores más convincentes.

La encuesta muestra que los principales impulsores para la implementación de SD-WAN son la reducción de costos, la gestión y la necesidad de agilidad de red. Sin embargo, el argumento de las empresas que no han implementado SD-WAN es la agilidad de la red dentro de su entorno. Aquellas que ya han implementado SD-WAN consideran que los costos y la mejora en la gestión y automatización de la red son los impulsores principales.

Se cree que esta diferencia en las opiniones refleja el hecho de que los usuarios pioneros están por delante de sus colegas en la adopción de la automatización, y que es probable que utilicen esta como una justificación para implementar SD-WAN con el objetivo de mejorar los ahorros operativos y de capital.

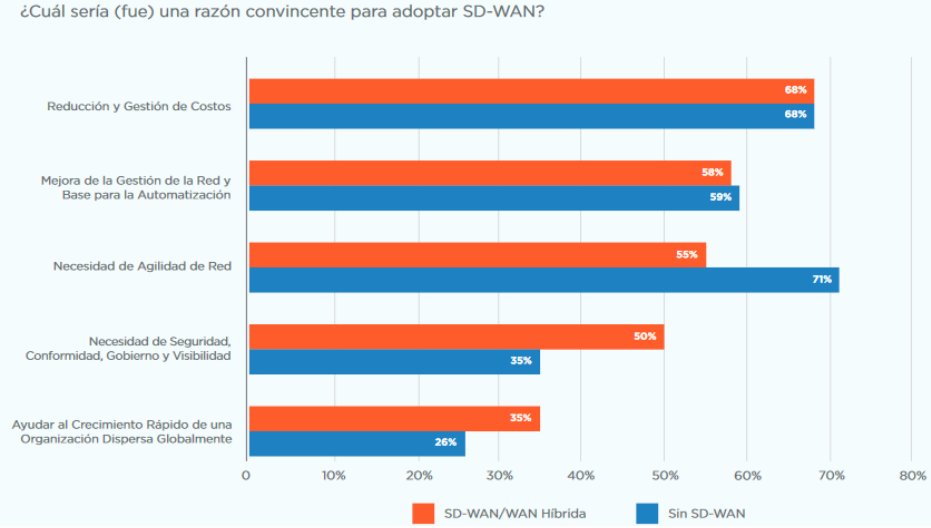


Figura 2. 9 Porcentajes de empresas por adopción SD-WAN
Fuente: (SDxCentral LLC, 2018)

2.2.16 Desafíos de la transición a una SD-WAN

Para aquellos que todavía no han implementado una solución SD-WAN, seleccionar un proveedor o asociado para la transformación de la red (incluida la SD-WAN) se considera particularmente desafiante. De hecho, la selección del proveedor se ve como un desafío importante incluso para aquellas empresas que ya han comenzado su camino hacia SD-WAN.

Al final del día, los beneficios de implementar SD-WAN superan los desafíos. Entre ellos están el soporte multicloud, mejor seguridad y visibilidad. Lo que es bastante notable es la similitud en las clasificaciones entre las empresas que la han implementado y frente a aquellas que todavía la tienen que implementar (SDxCentral LLC, 2018).

2.3 Seguridad gestionada

La Seguridad Gestionada incluye soluciones de gestión de seguridad inteligentes, automatizadas y personalizadas acorde a las necesidades de la empresa.

La supervisión y administración de la seguridad de la empresa es una tarea cada vez más compleja:

- Por un lado, las amenazas cibernéticas son cada vez más sofisticadas. Existe una gran cantidad de amenazas latentes capaces de mutar rápidamente.

- El perímetro tradicional de seguridad corporativo ha desaparecido y los posibles puntos de entrada se han multiplicado.

- No olvidar tampoco la necesidad de cumplir con múltiples regulaciones, la salvaguarda de la marca y la reputación. Se debe proteger la ventaja competitiva y garantizar la satisfacción del cliente. También buscar eficiencias mediante la automatización para conseguir la reducción de costos.

Los servicios de seguridad gestionados agrupan servicios habituales en este campo (antivirus, firewalls, detección de intrusos, actualizaciones, auditoria de seguridad, filtrado de contenidos, etcétera), pero adoptando un nuevo enfoque de las necesidades de seguridad de la empresa (LIDER IT, 2020).

2.3.1 ¿Qué proveen los MSSP?

Los MSSP ofrecen un amplio abanico de medidas de protección, comenzando desde lo más básico como podría ser un antivirus, hasta lo complejo siendo este el caso del SOC (Security Operations Center) (ODS, 2020).

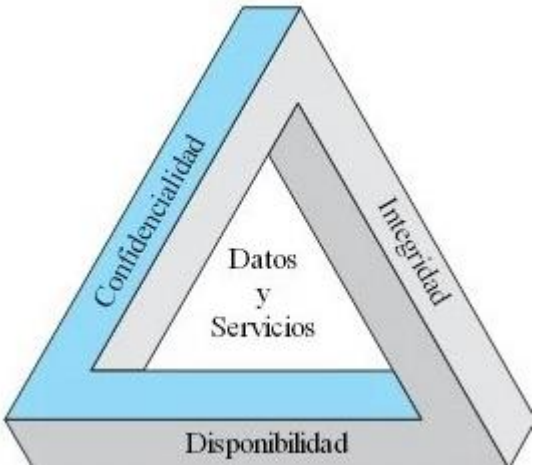


Figura 2. 10 Principios de la Seguridad gestionada
Fuente: (Zuñiga, 2019)

Los MSSP pueden incluir la implantación, configuración y administración de los siguientes activos tecnológicos (Figura 2.11):

- Antivirus
- Anti-spam
- VPN
- Firewall
- Sistemas de prevención de intrusos (IPS, Intrusion Prevention System)
- Inteligencia de amenazas
- Gestión de accesos
- Prevención de pérdida de la información

2.3.2 Redes y seguridad perimetral

Un porcentaje muy importante de los servicios de seguridad gestionada se centran en la administración de los dispositivos de seguridad de red, fundamentalmente firewalls e IDS/IPS. Sin embargo, es fundamental para el ISP que su personal se encuentre capacitado y cuente con la experiencia necesaria para asumir completamente el mantenimiento y control de estos equipos.

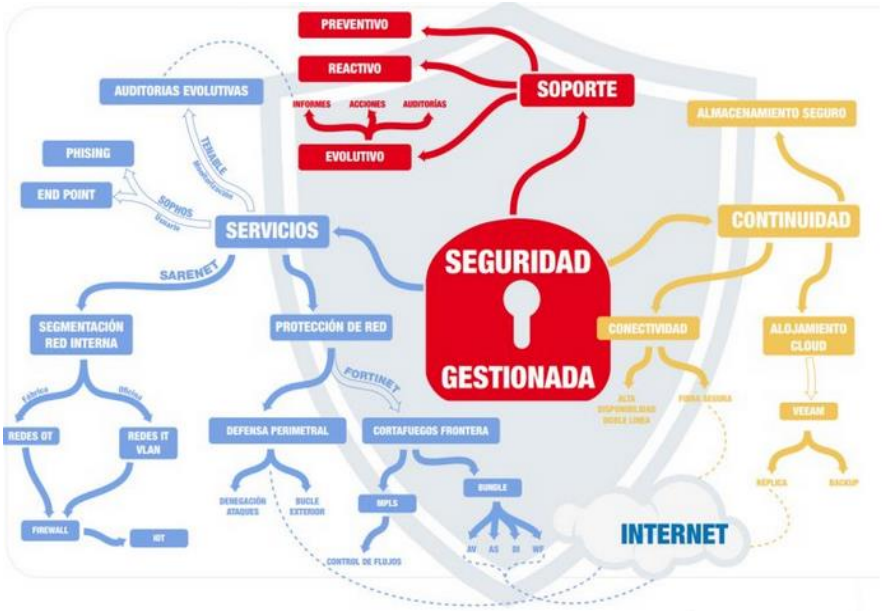


Figura 2. 11 Funciones que provee un MSSP
Fuente: (Sarenet, 2019)

2.3.3 Infraestructuras y seguridad física

Existe una especie de abismo entre el mundo de la seguridad física y de los sistemas de información. No tiene sentido hablar de seguridad de sistemas si no está garantizada la física y el suministro de servicios básicos.

La gestión externalizada de la seguridad física es una práctica habitual, aunque se haga de forma aislada con respecto a la gestión de la seguridad de sistemas. Igualmente, la gestión de las infraestructuras de suministro eléctrico, climatización, detección y extinción de incendios, etc. suele externalizarse.

2.4 Next-generation firewall

Los Next-Generation Firewall (NGFW) filtran el tráfico de red para proteger a una organización de amenazas internas y externas. Además de mantener las características de los firewalls como el filtrado de paquetes, la compatibilidad con IPsec y VPN SSL, la supervisión de red y

las funciones de mapeo de IP, los NGFW poseen capacidades de inspección de contenido más profundas.

Estas capacidades ofrecen la habilidad de poder identificar ataques, malware y otras amenazas, y permiten a los NGFW bloquear estas amenazas.

También ofrecen a las empresas inspección de SSL, Application Control, prevención de intrusiones y visibilidad avanzada a través de toda la superficie de ataque.

Los NGFW no solo bloquean el malware, también incluyen rutas para futuras actualizaciones que les proporcionan flexibilidad para evolucionar con el panorama de amenazas y mantener la red segura a medida que surgen nuevas amenazas. Es decir, los Firewalls son un componente vital para implementar la seguridad de red (RebootSystems, 2021).

2.4.1 Next-generation firewall de Fortigate

Los NGFW de FortiGate son firewalls de red que funcionan con unidades de procesamiento de seguridad (SPU, Security Processing Units) especialmente diseñadas, incluido el último NP7 (Network Processor 7). Estos habilitan las redes basadas en seguridad y son firewall de red ideales para centros de datos híbridos y de hiperescala.

Como parte integral del Fortinet Security Fabric, los NGFW de FortiGate se pueden comunicar en la cartera de seguridad integral de Fortinet, así como con soluciones de seguridad de terceros en un entorno de múltiples proveedores (Figura 2.12).

2.4.2 Casos de uso de NGFW de Fortigate

Los NGFW de FortiGate ayudan a las organizaciones a alcanzar la transformación digital al proteger cualquier borde y aplicación a cualquier

escala al mejorar la eficiencia operativa, automatizar los flujos de trabajo y ofrecer una postura de seguridad sólida con la mejor protección contra amenazas. Los NGFW de FortiGate ofrecen la clasificación informática de seguridad más alta de la industria y proveen los siguientes beneficios:

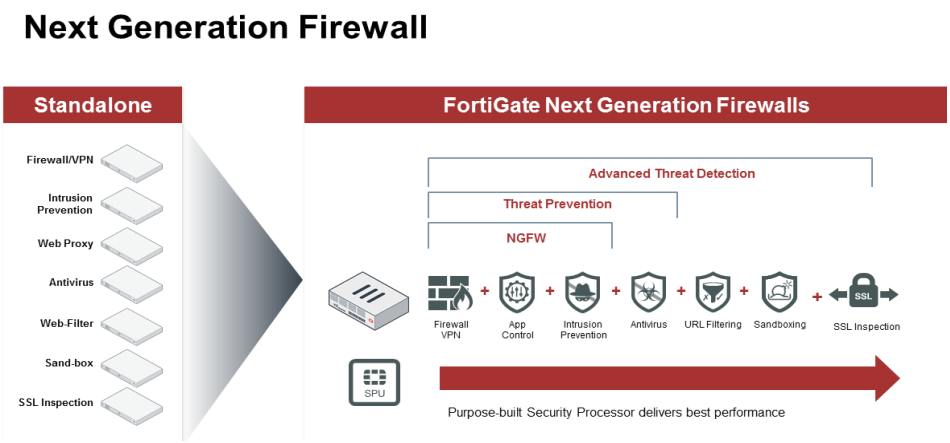


Figura 2. 12 Principales características de Fortigate Next Generation Firewalls
Fuente: (Adaptix, 2017)

Gestión de riesgos de seguridad externos

Los NGFW de FortiGate ofrecen redes basadas en la seguridad para alcanzar la visibilidad completa de las aplicaciones, amenazas y redes, lo que protege cualquier borde con la mejor seguridad validada por la industria para mantener las operaciones en ejecución y lograr la continuidad del negocio.

Ofrecer seguridad a hiperescala

Los firewalls tradicionales colapsan cuando manejan la gran afluencia de tráfico de usuarios requerida a velocidades de hiperescala. Como resultado, la experiencia del usuario resulta afectada. Renunciar a la seguridad abre las puertas a los atacantes para interrumpir sus servicios. Los NGFW de Fortinet ofrecen una seguridad única e incomparable para garantizar que los sitios web de su empresa sigan siendo accesibles, receptivos y brinden una experiencia del usuario óptima.

Gestión de vulnerabilidades

La mayoría de malware se propaga utilizando vulnerabilidades conocidas y es una causa principal de ataques. Los NGFW de FortiGate ofrecen IPS consolidado sin degradar el rendimiento para proveer parcheo virtual y prevenir contra ataques conocidos.

2.4.3 Servicios de seguridad Fortiguard para Fortigate: next-generation firewalls

El NGFW de FortiGate recibe actualizaciones continuas de inteligencia frente a amenazas de los servicios de seguridad de FortiGuard Labs. La prevención de intrusiones, antimalware, sandbox en la nube, Application Control y Web Filtering protegen a las empresas de ataques avanzados conocidos y desconocidos (FORTINET, 2021).

2.4.4 Fortimanager Cloud

Simplifica la administración y el aprovisionamiento sin intervención, con un amplio conjunto de herramientas para administrar de manera centralizada cualquier número de dispositivos desde una única consola con controles de acceso basados en funciones, administración de configuración central, administración de cambios y cumplimiento de las mejores prácticas.

2.4.5 FortiAnalyzer Cloud

FortiAnalyzer Cloud permite a los clientes identificar anomalías operativas en tiempo real en su red.

2.4.6 Servicio de clasificación de seguridad

El Security Fabric se basa fundamentalmente en las mejores prácticas de seguridad y al ejecutar estas revisiones de auditoría, los equipos de

seguridad podrán identificar las vulnerabilidades críticas y las deficiencias en su configuración de Security Fabric e implementar recomendaciones de mejores prácticas.

2.4.7 Application control

Con el Application Control de FortiGuard puede crear rápidamente políticas para permitir o restringir el acceso a aplicaciones o a categorías enteras de aplicaciones.

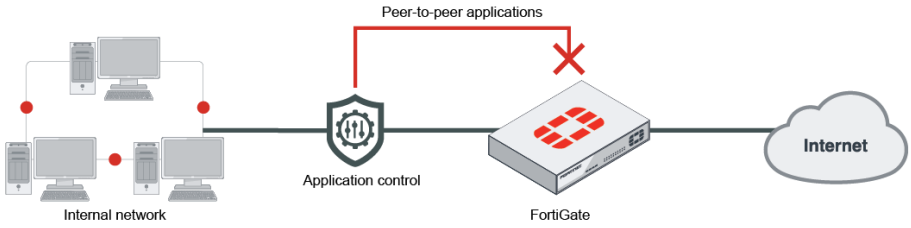


Figura 2. 13 Esquema de control de aplicación
Fuente: *(FortinetDocumentLibrary, 2021)*

2.4.8 Web filtering

Protege su organización al bloquear el acceso a sitios web maliciosos, pirateados o inapropiados.

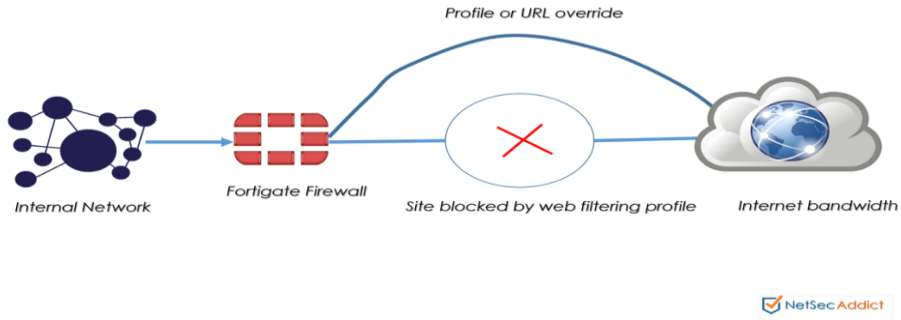


Figura 2. 14 Esquema de un filtro web
Fuente: *(Javiya, 2018)*

2.4.9 Antivirus

FortiGuard Antivirus protege contra los más recientes virus, spyware y otras amenazas a nivel de contenido. Utiliza los motores de detección avanzada, líderes en la industria para evitar que las amenazas nuevas y

en evolución obtengan una posición establecida dentro de su red y accedan a contenido valioso (Fortinet, 2021).

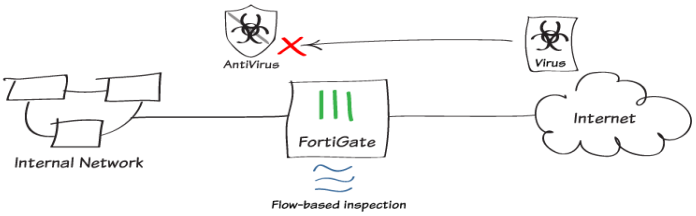


Figura 2. 15 Esquema de operación de antivirus
Fuente: *(Fortinet Document Library, 2021)*

2.4.10 Prevención de intrusiones

FortiGuard IPS protege contra las últimas intrusiones de red al detectar y bloquear las amenazas antes de que lleguen a los dispositivos de red.

CAPÍTULO 3: Diseño y Análisis de la propuesta

La gran mayoría de empresas e industrias tienen sus redes diseñadas en MPLS, y en estos últimos años, no hay duda de los grandes avances que han sucedido en las telecomunicaciones, por lo tanto, las empresas también deben ir renovando y creciendo en cuanto a diseños lógicos acorde a sus necesidades.

Los cambios o modificaciones en MPLS no son inmediatos ni fáciles de implementar en tiempo, forma y costo. Es por ello que se ha notado un aumento de empresas que están optando por el sistema de seguridad gestionada SD-WAN, esto debido a un alto grado de independencia y control, se obtiene un mejor nivel de respuesta a cambios y solicitudes, aparte que se puede priorizar el tipo de tráfico de conexión que se envía.

En este capítulo se tratará el diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana, en el cual se detallará los equipos y configuraciones necesarias para la presente propuesta.

3.1 Escenario actual de la Universidad

Actualmente la Universidad tiene diseñada su red MPLS en malla para ambos servicios, datos e internet con un solo proveedor.

Los ruteadores en cada uno de los puntos poseen un número significativo de rutas estáticas para poder alcanzar otros segmentos de redes. Se tiene un número considerable de conexiones físicas, lo cual genera que la administración de la infraestructura de red sea más complicada.

Ejecutar modificaciones o cambios inmediatamente no es conveniente con el diseño actual, dado que se requiere de un tiempo considerable, sin dejar a un lado los costos que estos podrían implicar.

3.2 Diagrama lógico actual

A continuación, se detalla el esquema lógico de conexión entre los campus de la Universidad, relacionado a nivel de direccionamiento WAN.

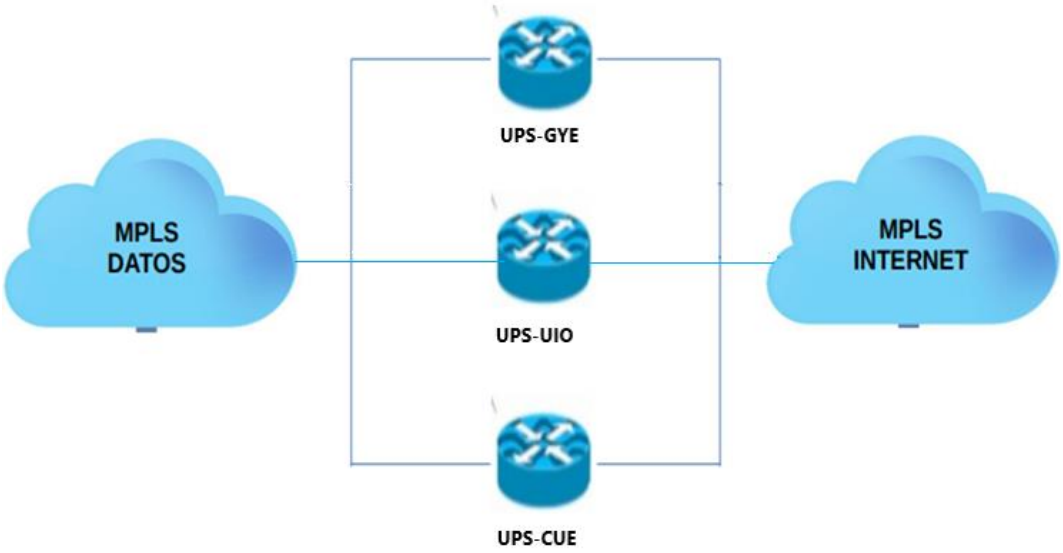


Figura 3. 1 Diagrama lógico actual entre sedes
Fuente: Autora

3.3 Esquema lógico básico de los campus

A continuación, se detalla el esquema lógico de conexión en cada sede de la Universidad Politécnica Salesiana, incluido el nodo de backbone.

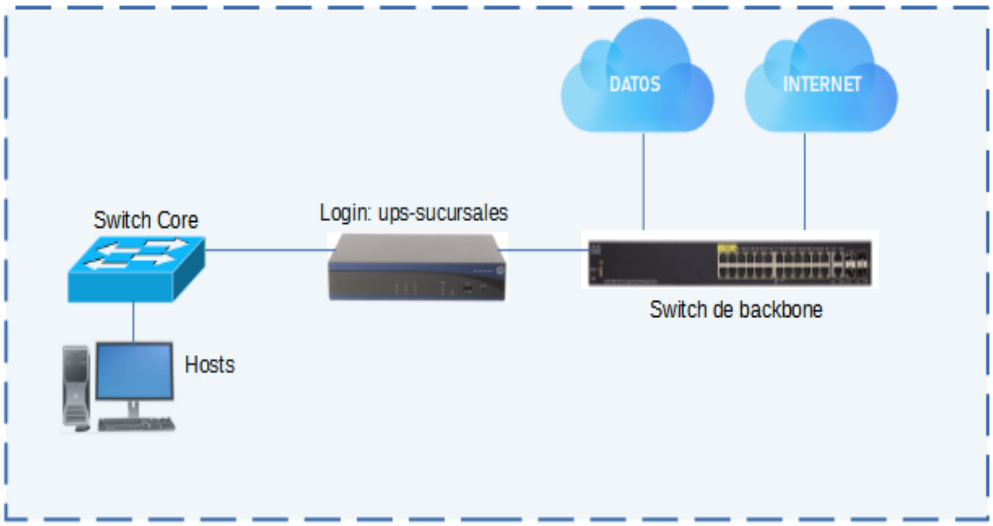


Figura 3. 2 2 Diagrama lógico general de las sucursales
Fuente: Autora

3.4 Direccionamiento de redes de cada sucursal

Tabla 3.1 Redes actuales

UBICACIÓN	NOMBRE	RED	GATEWAY
SEDE CUENCA	Red Administrativa	192.168.31.0/24	192.168.31.1
	Red Servidores 1	192.168.10.0/24	192.168.10.1
	Red Servidores 2	192.168.2.0/24	192.168.2.1
	Red Operaciones	192.168.28.0/24	192.168.28.1
	Red Camaras	10.10.15.0/24	10.10.15.1
	Red Telefonos IP	10.10.20.0/24	10.10.20.1
	Red WiFi	192.168.42.0/24	192.168.42.1
	Administracion de Equipos	172.16.0.0/24	172.16.0.1
	Red Enlaces	10.10.10.0/26	10.10.10.1
SEDE GUAYAQUIL	Red Administrativa	192.168.7.0/24	192.168.7.1
	Red Servidores	192.168.0.0/24	192.168.0.1
	Red Servidores	192.168.4.0/24	192.168.4.1
	Red Camaras	10.30.12.0/26	10.30.12.1
	Red WiFi	172.16.20.0/24	172.16.20.1
	Red Telefonos IP	10.10.30.0/24	10.10.30.1
	Administracion de Equipos	172.16.1.0/24	172.16.1.1
	Red Enlaces	10.10.12.0/26	10.10.12.1
SEDE QUITO	Red Administrativa	192.168.169.0/24	192.168.169.1
	Red TMK	192.168.40.0/24	192.168.40.1
	Red Telefonos IP	192.169.20.0/25	192.169.20.1
	Administracion de Equipos	192.68.170.0/23	192.168.170.1
	Red Enlaces	10.10.11.0/26	10.10.11.1
	Red Servidores	192.169.21.0/24	192.168.21.1
	Red Wifi	172.16.100.0/24	172.16.100.1

Fuente: Autora

3.5 Requisitos para la propuesta del diseño

Para el diseño del presente trabajo se requiere de las siguientes herramientas:

A nivel WAN

- Puertos de backbone en Giga
- Fortigate 80E para Matriz
- Fortigate 50E para sedes Gye y UIO
- CPE o Router Cisco 1111 - 8P

A nivel LAN

- Switch de Core Cisco
- PCs

Para este escenario se tomarán 2 proveedores de servicios de datos e internet: Cedia – Telconet.

3.6 Topología de Diseño para propuesta de implementación de SD-WAN

A continuación, se detallará el diagrama de conexiones para cada una de las sucursales, incluyendo equipos de ambos proveedores.

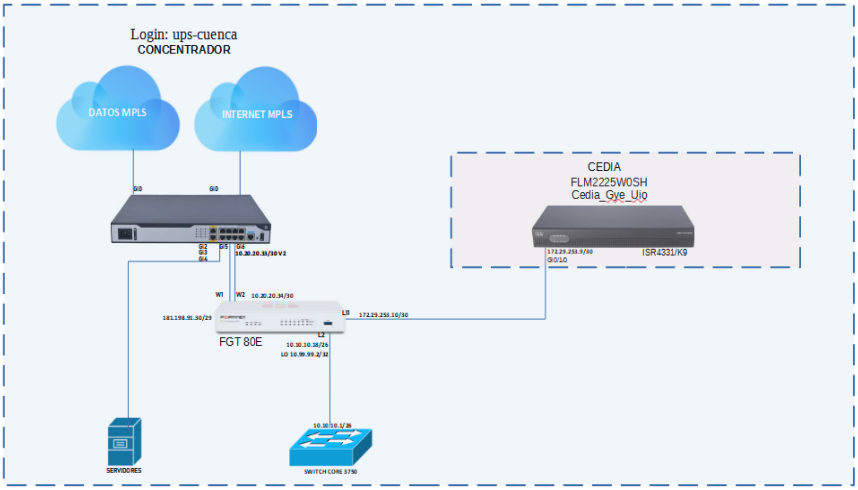


Figura 3. 3 Diagrama de conexiones Sede Cuenca
Fuente: Autora

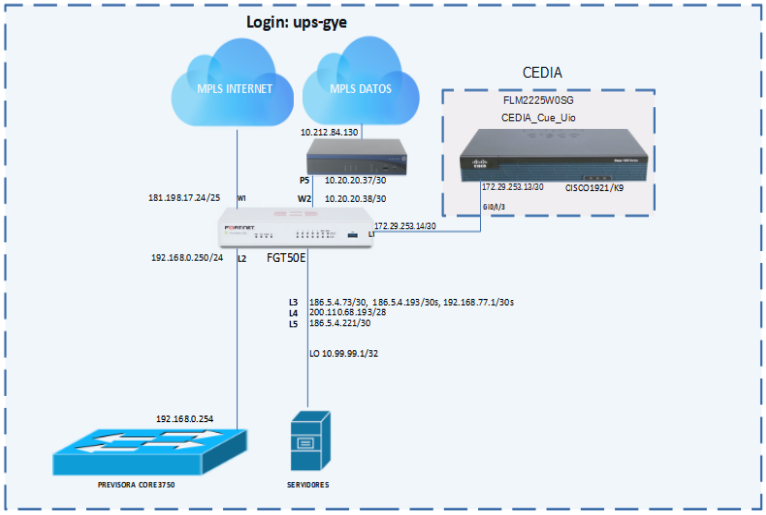


Figura 3. 4 Diagrama de conexiones Sede Guayaquil
Fuente: Autora

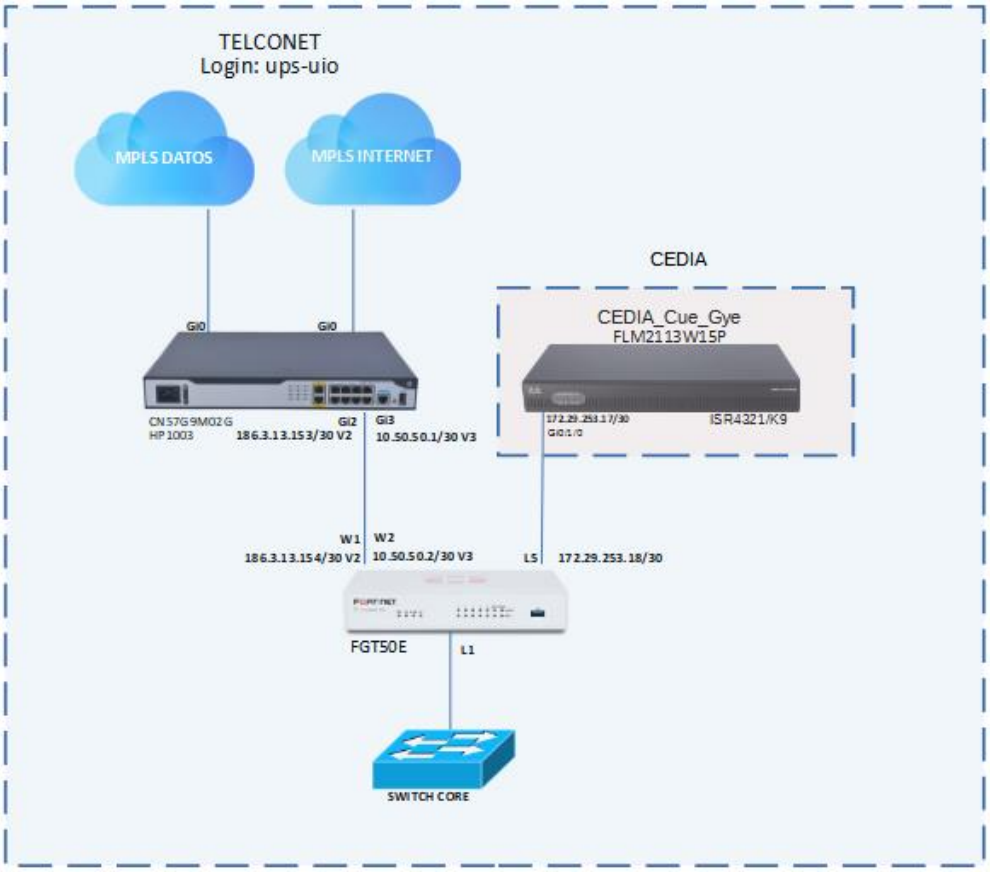


Figura 3. 5 Diagrama de conexiones Sede Quito
Fuente: Autora

3.7 Descripción del diseño de implementación

En las gráficas anteriores se muestra el diseño de implementación SD-WAN de aplicaciones y tráfico, empleando la marca Fortinet. También se puede observar que para la presente propuesta se tendrán dos proveedores: Cedia y Telconet.

Con el proveedor Telconet se tendrá conectividad mediante túneles punto a punto entre todos los puntos, y con el proveedor Cedia se realizará a través de un puerto del Firewall conectado directamente al router Cedia de cada punto.

Para la sede de Cuenca de acuerdo con sus necesidades se utilizará un equipo Fortigate 80E y para las sedes de Quito y Guayaquil se empleará el modelo Fortigate 50E.

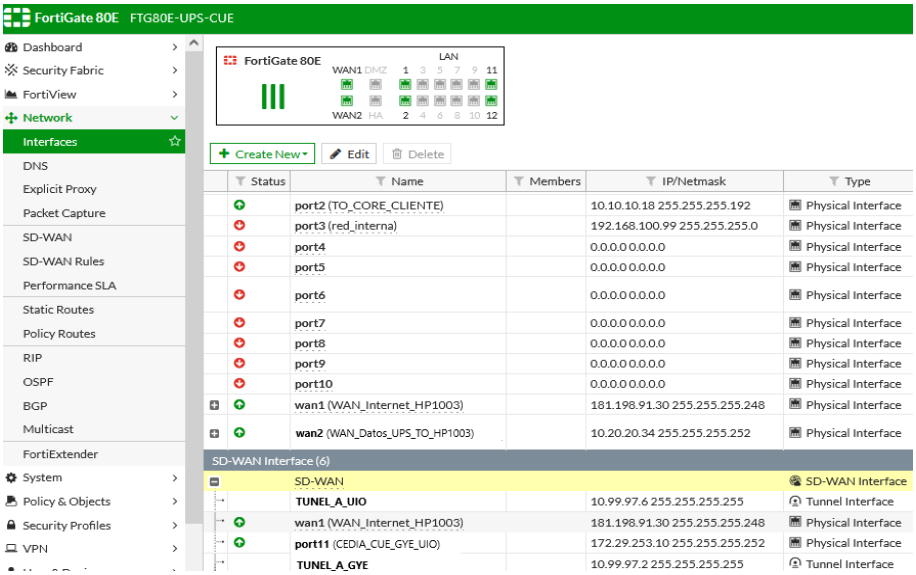


Figura 3. 6 Interfaz gráfica de equipo Fortigate 80E en Sede Cuenca
Fuente: Autora

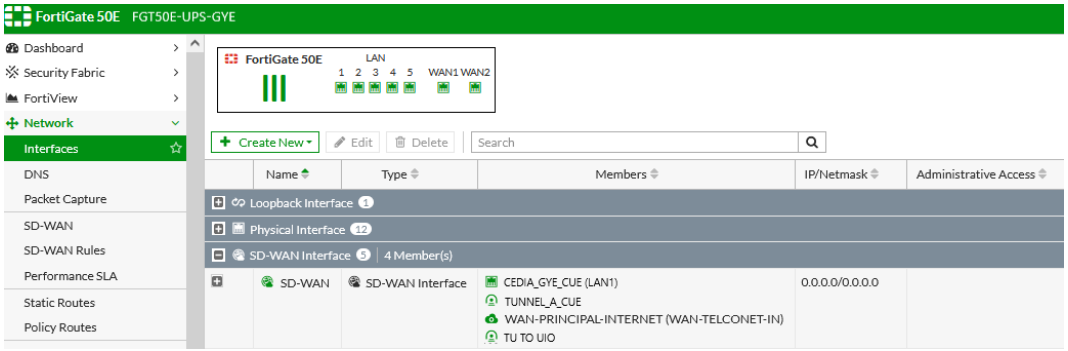


Figura 3. 7 7 Interfaz gráfica de equipo Fortigate 50E en Sede Guayaquil
Fuente: Autora

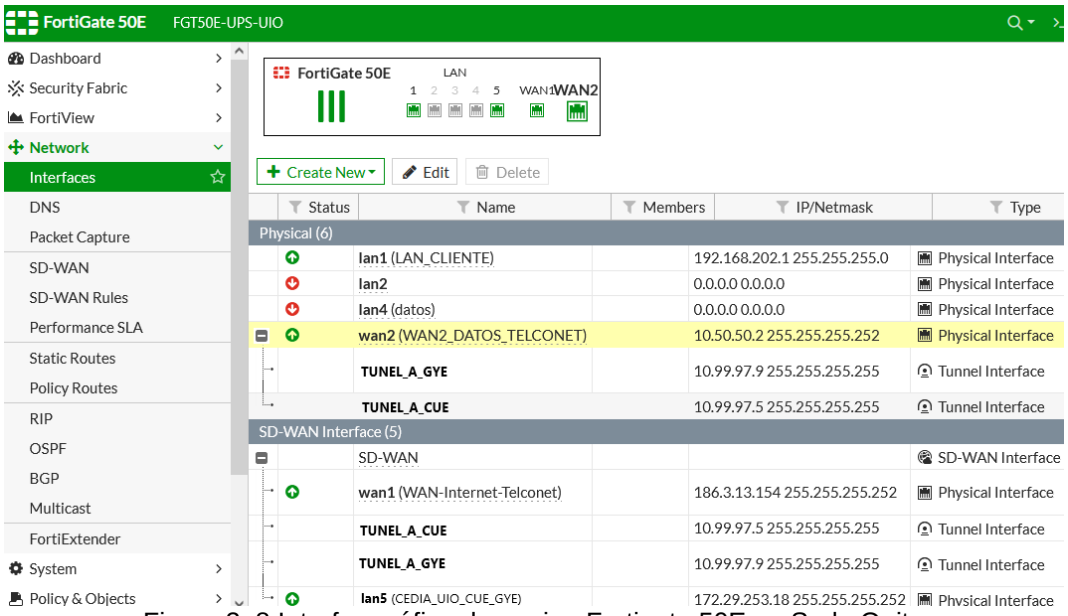
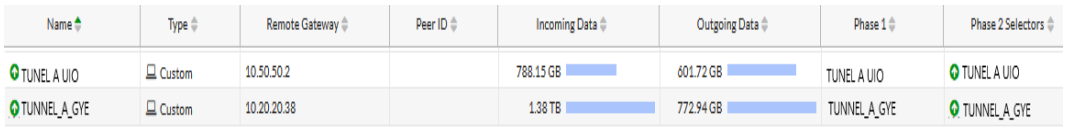


Figura 3. 8 Interfaz gráfica de equipo Fortigate 50E en Sede Quito
Fuente: Autora

3.7.1 Establecimiento de Túneles punto a punto

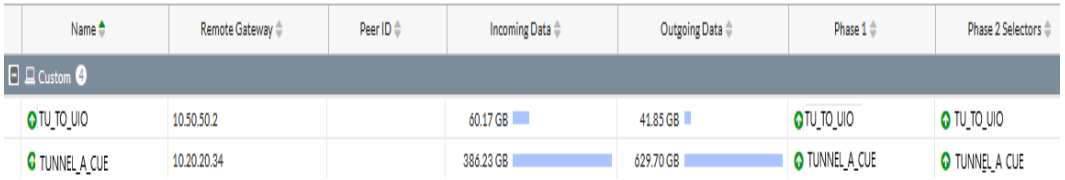
Tal como se indicó en el apartado anterior, para la propuesta, en los equipos Fortigate se crearán túneles punto a punto entre las sedes para un proveedor, en este caso Telconet; para el segundo proveedor se tiene asignado un puerto en el cual se levantan las comunicaciones entre todos los puntos.

Este tipo de arquitectura no solamente permite interconectar diferentes sedes, sino también acceder a todos sus recursos. Cabe mencionar que esta configuración es uno de los primeros pasos para el presente diseño, dado que luego de levantar las sesiones se deben añadir los segmentos de red que se desean alcanzar por medio del túnel y crear sus correspondientes políticas para establecer la comunicación y poder asignar los perfiles de seguridad de acuerdo a las necesidades de las sedes.



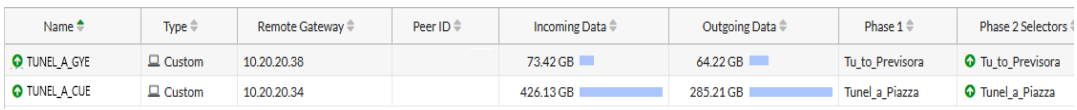
Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
TUNEL A UIO	Custom	10.50.50.2		788.15 GB	601.72 GB	TUNEL A UIO	TUNEL A UIO
TUNNEL_A_GYE	Custom	10.20.20.38		1.38 TB	772.94 GB	TUNNEL_A_GYE	TUNNEL_A_GYE

Figura 3. 9 Visualización de estado de los túneles en sede Cuenca
Fuente: Autora



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 4						
TU_TO_UIO	10.50.50.2		60.17 GB	41.85 GB	TU_TO_UIO	TU_TO_UIO
TUNNEL_A_CUE	10.20.20.34		386.23 GB	629.70 GB	TUNNEL_A_CUE	TUNNEL_A_CUE

Figura 3. 10 Visualización de estado de los túneles en sede Guayaquil
Fuente: Autora



Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
TUNEL_A_GYE	Custom	10.20.20.38		73.42 GB	64.22 GB	Tu_to_Previsora	Tu_to_Previsora
TUNEL_A_CUE	Custom	10.20.20.34		426.13 GB	285.21 GB	Tunel_a_Piazza	Tunel_a_Piazza

Figura 3. 11 Visualización de estado de los túneles en sede Quito
Fuente: Autora

Se toma como método de autenticación Pre-shared Key que es una clave secreta compartida con anterioridad entre los extremos, proporcionando

un canal seguro. En las 3 localidades se tiene equipos Fortigate, lo cual facilita la configuración de los túneles sitio a sitio.

3.7.2 Miembros SD-WAN

Para establecer las reglas de balanceo, primero se deben ingresar las interfaces involucradas como miembros del SD-WAN, estableciendo sus puertas de enlace y el costo de las mismas.

Estas interfaces deben ser configuradas previamente y no deben estar referenciadas en ninguna política, hasta que sean parte del SD-WAN. En el punto matriz se tiene como miembros el Túnel hacia Guayaquil y Quito, también la interfaz por la cual se tiene conectividad a los equipos del segundo proveedor y la interfaz de conectividad hacia internet, tal como se muestra a continuación.

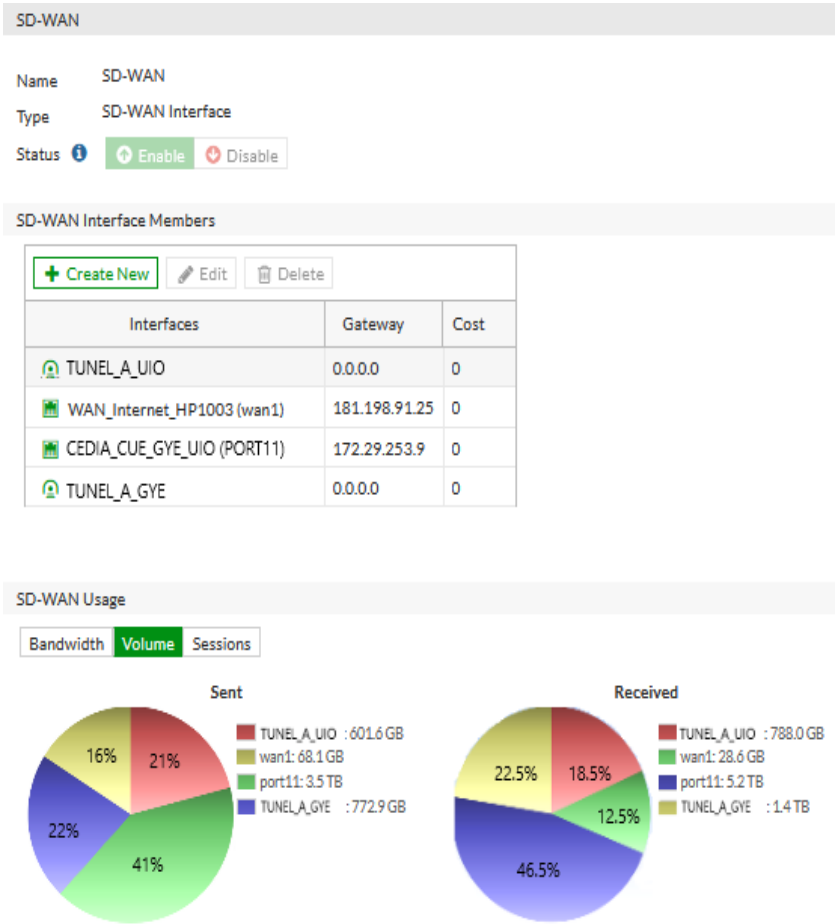


Figura 3. 12 Miembros SD-WAN en sede Cuenca
Fuente: Autora

En el punto de Guayaquil la interfaz SD-WAN la integra los túneles hacia Cuenca y Quito, además del puerto dedicado para la conexión hacia el segundo proveedor Cedia y la interfaz de conectividad hacia internet.

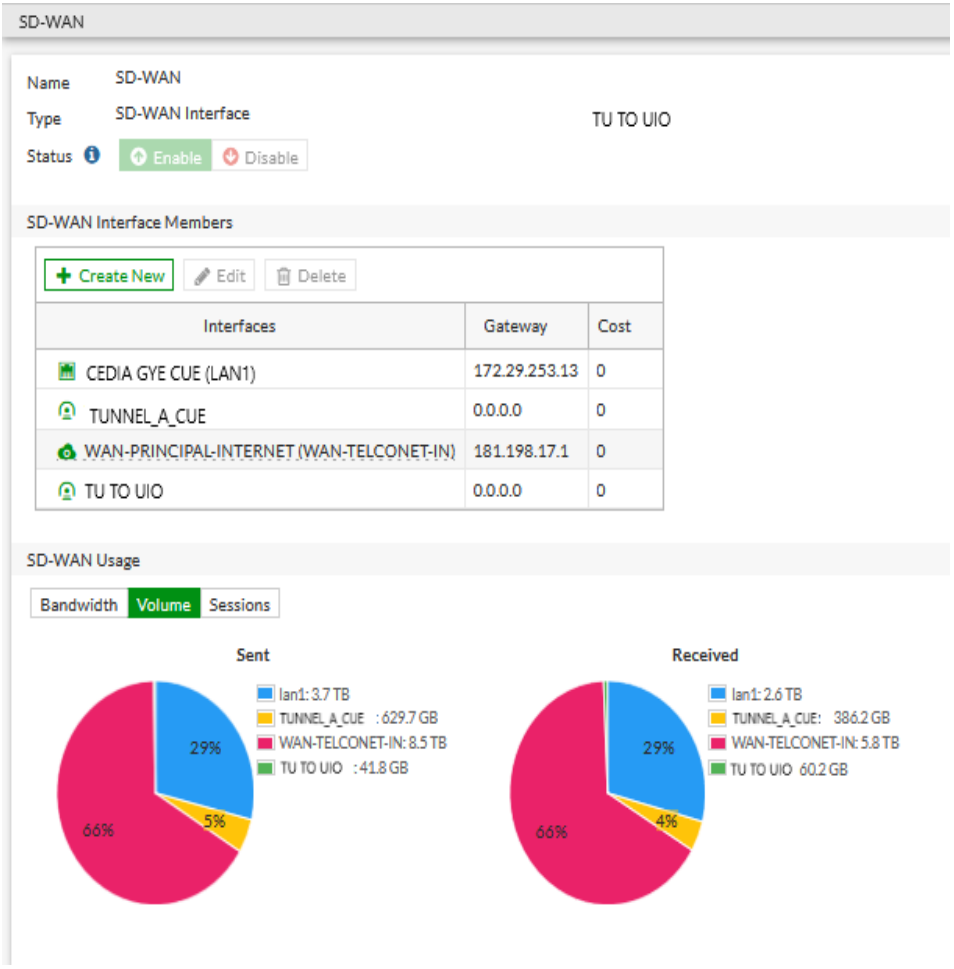


Figura 3. 13 Miembros SD-WAN en sede Guayaquil
Fuente: Autora

En el punto de Quito se configura como miembros SD-WAN los túneles que permiten la conexión hacia las demás sedes, la interfaz por la cual se tiene conectividad a los equipos del segundo proveedor y la interfaz de conectividad hacia internet (Figura 3.14).

Luego de ingresar los miembros al SD-WAN, se configura la ruta por defecto en todos los puntos, tal como se puede apreciar en la figura 3.15, para que la programación defina las salidas de acuerdo con el algoritmo que se integró.

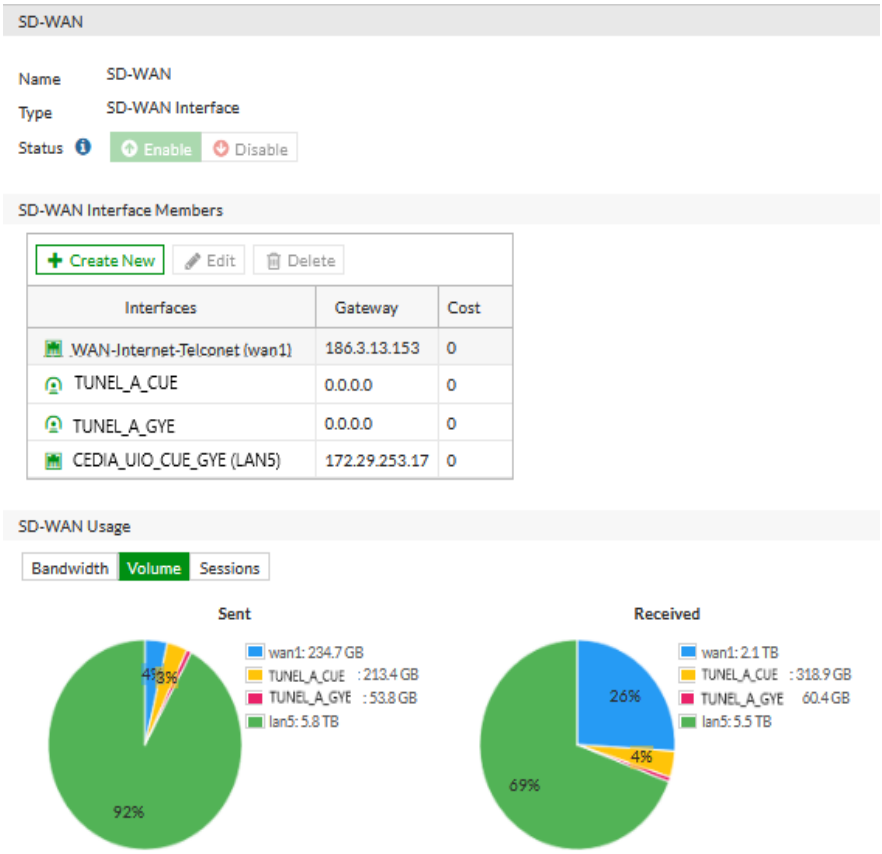


Figura 3. 14 Miembros SD-WAN en sede Quito
Fuente: Autora

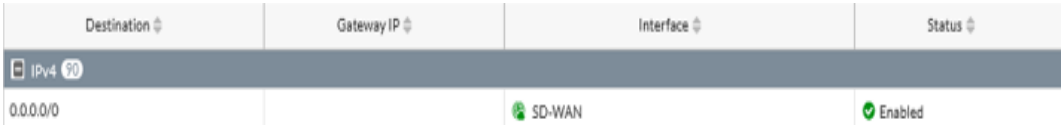


Figura 3. 15 Ruta default SD-WAN
Fuente: Autora

3.8 Disponibilidad de proveedores

Para la disponibilidad de los proveedores se puede medir por tres métodos: pérdida de paquetes, latencia y jitter. Para el presente trabajo se ha optado por la opción de latencia.

Dentro de los parámetros que se debe definir se tiene lo siguiente:

En primer lugar, se elige protocolo a Ping, y al pertenecer a una opción de chequeo de enlace hacia internet, el ping debe ser dirigido hacia la dirección IP 8.8.8.8, correspondiente a los DNS de Google. En el campo

de participante se selecciona la interfaz WAN1. Dentro de los campos a elegir en el objetivo del SLA se encuentran los siguientes:

Umbral de latencia: 10ms
Umbral de fluctuación: 5ms
Umbral de pérdida de paquetes: 15%

En caso de que los campos antes mencionados llegaran a exceder los valores predeterminados, daría como resultado la pérdida en la conexión hacia internet.

A continuación, se presentan capturas del performance SLA (Service Level Agreement) para conectividad a Internet en cada una de las sucursales.

Figura 3. 16 Health-Check hacia internet en sede Cuenca
Fuente: Autora

Para la sede de Guayaquil, se repite la misma configuración para el Health-check hacia internet.

Figura 3. 17 Health-Check hacia internet en sede Guayaquil
Fuente: Autora

Para la detección hacia las demás sedes, se asigna la IP de cada servidor que se desea alcanzar y la interfaz del servicio, en este caso los túneles previamente configurados.

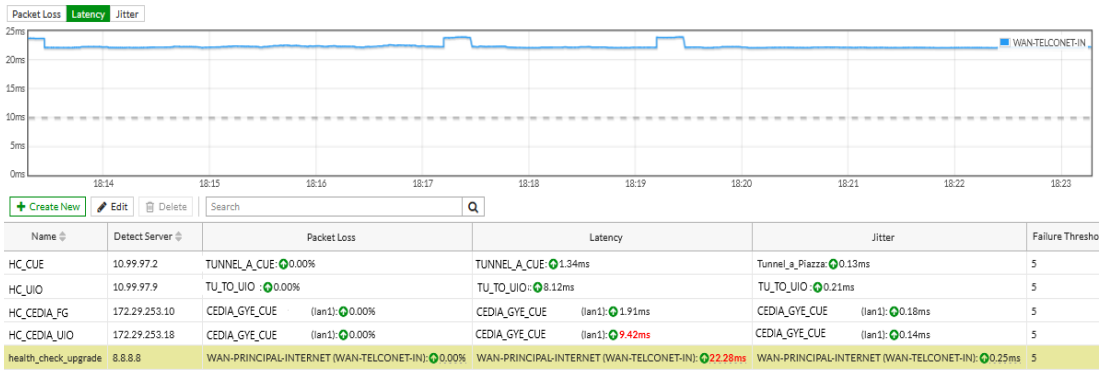


Figura 3. 18 Listado de Health-Check en sede Guayaquil
Fuente: Autora

El Health-Check hacia internet en la sede de Quito tiene como servidor la dirección IP 8.8.8.8, y como participante la interfaz WAN1.

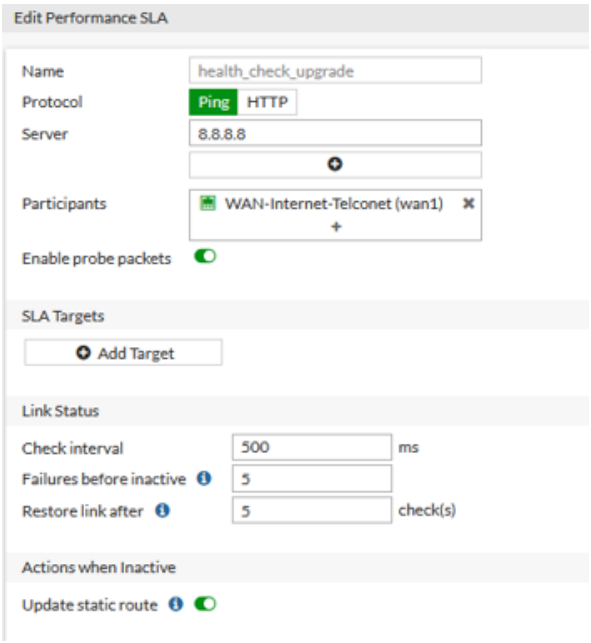


Figura 3. 19 Health-Check hacia internet en sede Quito
Fuente: Autora

En los SLA hacia las demás sedes, se asigna la IP de cada servidor que se desea detectar y la interfaz del servicio por la cual se alcanzará este enlace.

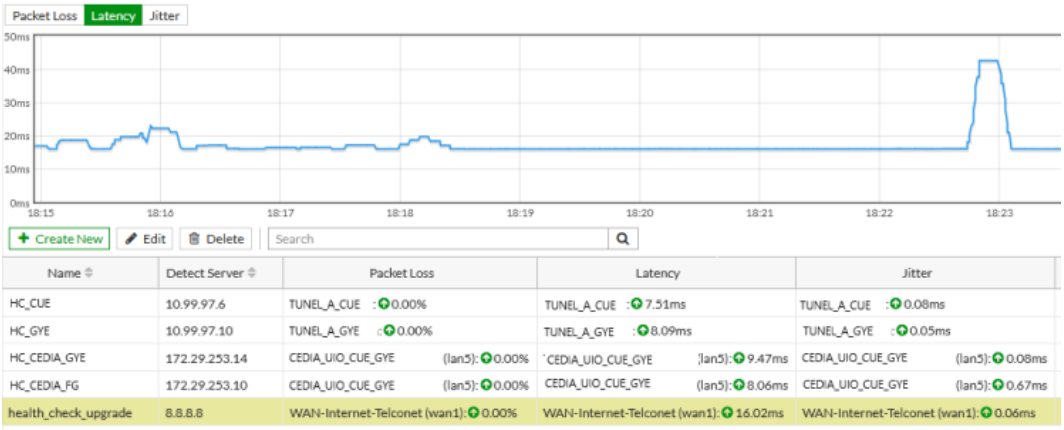


Figura 3. 20 Listado de Health-Check en sede Quito
Fuente: Autora

3.8.1 Reglas SD-WAN

Las reglas SD-WAN establecen el comportamiento para la selección del mejor canal. Para la creación de las reglas SD-WAN, se tiene en consideración las necesidades de la empresa como tal, es decir, como destino se puede ingresar segmentos de red o aplicaciones que son de

mayor uso; para el criterio se puede elegir varias opciones, en este caso se tiene SLA y latencia.

Como se puede apreciar en la figura 3.21, se tiene como fuente un “todo”, es decir, que desde cualquier segmento de red se puede enviar datos, siempre que los destinos sean los segmentos que se encuentran dentro del grupo de redes elegidas en el campo de destino; para criterios SLA se selecciona los Health-Check configurados previamente, y como preferencia de interfaces se eligen aquellas físicas y lógicas que permiten la conexión hacia ambos proveedores.

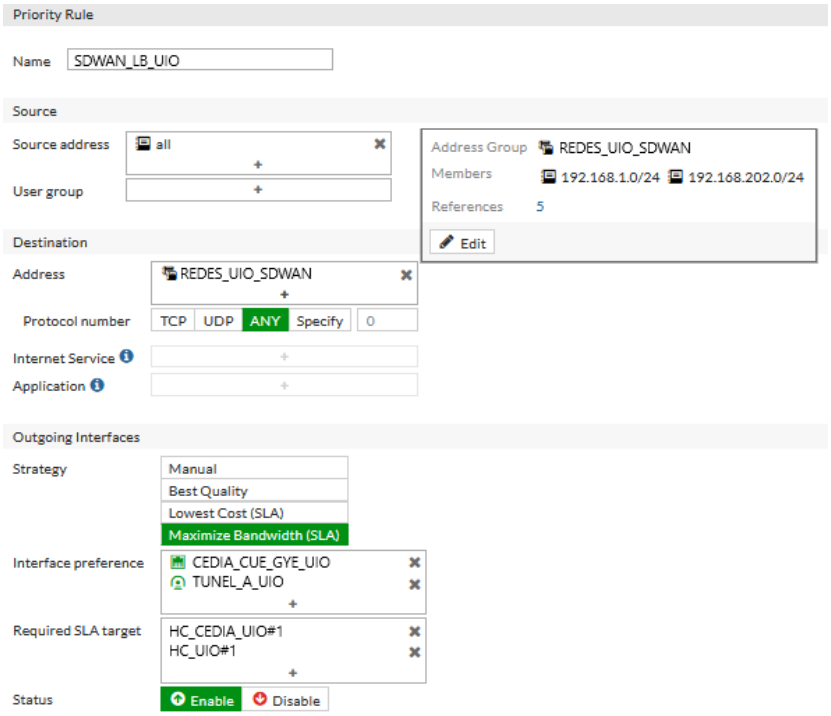
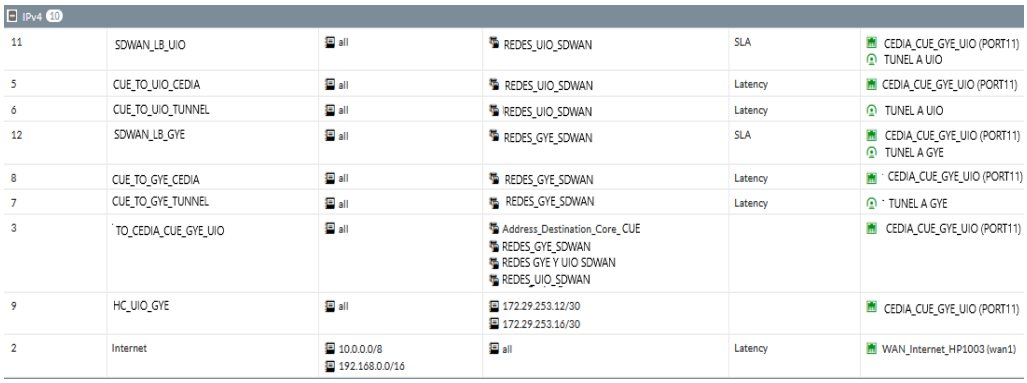


Figura 3. 21 Regla SD-WAN de tráfico desde Cuenca hacia Quito
Fuente: Autora

Entre las reglas SD-WAN se tiene como destino las redes hacia Quito, Guayaquil, equipo Core de la red interna de Cuenca, dos segmentos de redes con máscara 30, cada regla tiene su propia interfaz de salida, sea ésta por los túneles a las demás localidades o por el segundo proveedor Cedia.

Los únicos segmentos de red que pueden tener navegación en este punto son 10.0.0.0/8 y 192.168.0.0/16, se utilizaron máscaras grandes para que puedan abarcar más segmentos en caso de aumentar subredes en el punto; en destino se tiene un “todo” para que puedan conectarse a cualquier lugar.

La interfaz de salida WAN1, perteneciente al proveedor Telconet, será la única interfaz utilizada para el servicio de internet.



IPv4 10

11	SDWAN_LB_UIO	all	REDES_UIO_SDWAN	SLA	CEDIA_CUE_GYE_UIO (PORT11) TUNEL A UIO
5	CUE_TO_UIO_CEDIA	all	REDES_UIO_SDWAN	Latency	CEDIA_CUE_GYE_UIO (PORT11)
6	CUE_TO_UIO_TUNNEL	all	REDES_UIO_SDWAN	Latency	TUNEL A UIO
12	SDWAN_LB_GYE	all	REDES_GYE_SDWAN	SLA	CEDIA_CUE_GYE_UIO (PORT11) TUNEL A GYE
8	CUE_TO_GYE_CEDIA	all	REDES_GYE_SDWAN	Latency	CEDIA_CUE_GYE_UIO (PORT11)
7	CUE_TO_GYE_TUNNEL	all	REDES_GYE_SDWAN	Latency	TUNEL A GYE
3	TO_CEDIA_CUE_GYE_UIO	all	Address_Destination_Core_CUE REDES_GYE_SDWAN REDES GYE Y UIO SDWAN REDES_UIO_SDWAN		CEDIA_CUE_GYE_UIO (PORT11)
9	HC_UIO_GYE	all	172.29.253.12/30 172.29.253.16/30		CEDIA_CUE_GYE_UIO (PORT11)
2	Internet	10.0.0.0/8 192.168.0.0/16	all	Latency	WAN_Internet_HP1003 (wan1)

Figura 3. 22 Listado de Reglas SD-WAN para el tráfico desde Cuenca hacia otras sedes
Fuente: Autora

Para la sede de Quito se detalla una de las reglas SD-WAN, la cual corresponde al envío del tráfico desde Quito hacia Cuenca. Como fuente se configura “todo”, es decir que desde cualquier IP se puede generar el tráfico.

En el campo de destino se agrega el grupo de redes llamado REDES_CUENCA_SDWAN, este grupo contiene las redes que se desean alcanzar mediante el SD-WAN en el punto matriz.

Dentro de los parámetros de la interfaz de salida se tiene como estrategia SLA, la de maximizar el ancho de banda (SLA) equilibra el tráfico entre las interfaces de miembros de SD-WAN que cumplen los objetivos del SLA, según el método de equilibrio de carga que se configuró (Figuras 3.23 y 3.24).

Para el punto de Guayaquil se tienen 11 reglas, entre ellas se encuentra la regla para establecer la conexión al Fortianalyzer, el cual permitirá un monitoreo para el tráfico de datos, en este caso la interfaz de salida será la del proveedor Telconet.

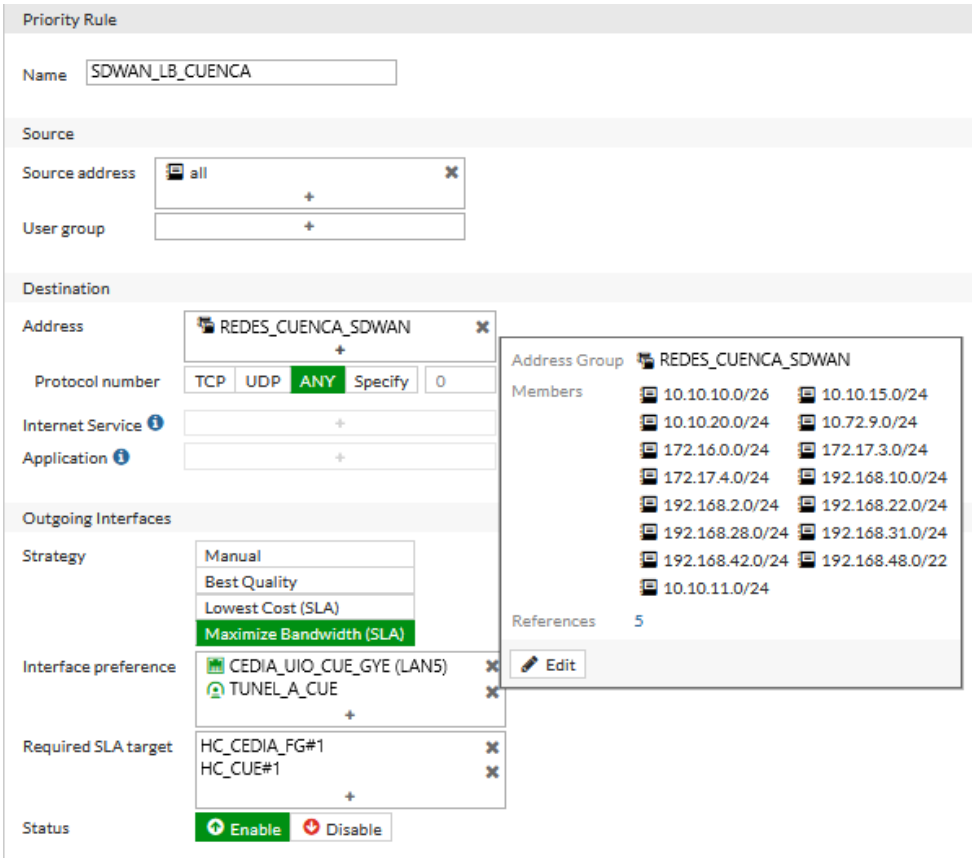
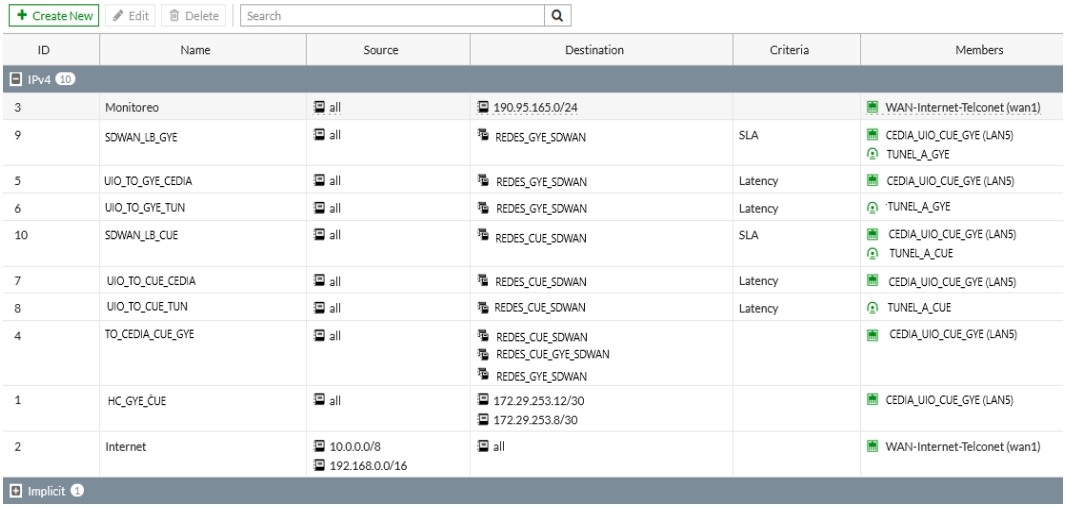


Figura 3. 23 Regla SD-WAN de tráfico desde Quito hacia Cuenca
Fuente: Autora



ID	Name	Source	Destination	Criteria	Members
IPv4 10					
3	Monitoreo	all	190.95.165.0/24		WAN-Internet-Telconet (wan1)
9	SDWAN_LB_GYE	all	REDES_GYE_SDWAN	SLA	CEDIA_UIO_CUE_GYE (LAN5) TUNEL_A_GYE
5	UIO_TO_GYE_CEDIA	all	REDES_GYE_SDWAN	Latency	CEDIA_UIO_CUE_GYE (LAN5)
6	UIO_TO_GYE_TUN	all	REDES_GYE_SDWAN	Latency	TUNEL_A_GYE
10	SDWAN_LB_CUE	all	REDES_CUE_SDWAN	SLA	CEDIA_UIO_CUE_GYE (LAN5) TUNEL_A_CUE
7	UIO_TO_CUE_CEDIA	all	REDES_CUE_SDWAN	Latency	CEDIA_UIO_CUE_GYE (LAN5)
8	UIO_TO_CUE_TUN	all	REDES_CUE_SDWAN	Latency	TUNEL_A_CUE
4	TO_CEDIA_CUE_GYE	all	REDES_CUE_SDWAN REDES_CUE_GYE_SDWAN REDES_GYE_SDWAN		CEDIA_UIO_CUE_GYE (LAN5)
1	HC_GYE_CUE	all	172.29.253.12/30 172.29.253.8/30		CEDIA_UIO_CUE_GYE (LAN5)
2	Internet	10.0.0.0/8 192.168.0.0/16	all		WAN-Internet-Telconet (wan1)
Implicit 1					

Figura 3. 24 Listado de Reglas SD-WAN para el tráfico desde Quito hacia otras sedes
Fuente: Autora

ID	Name	Source	Destination	Criteria	Members
IPv4 11					
11	Fortiguard	all	Fortinet-FortiGuard Fortinet-DNS Fortinet-FortiCloud Fortinet-FortiMail.Cloud +12	SLA	WAN-PRINCIPAL-INTERNET (WAN-TELC... CEDIA_GYE_CUE (LAN1)
12	FAZ	181.198.17.24/32	FAZ		WAN-PRINCIPAL-INTERNET (WAN-TELC...
9	SDWAN_LB_UIO	all	REDES_UIO_SDWAN	SLA	CEDIA_GYE_CUE (LAN1) TU_TO_UIO
5	GYE_TO_UIO_CEDIA	all	REDES_UIO_SDWAN	Latency	CEDIA_GYE_CUE (LAN1)
6	GYE_TO_UIO_TUNEL	all	REDES_UIO_SDWAN	Latency	TU_TO_UIO
10	SDWAN_LB_CUE	all	Address_Destination_Core_GYE REDES CUE SDWAN	SLA	CEDIA_GYE_CUE (LAN1) TUNNEL A CUE
3	GYE_TO_CUE_CEDIA	all	REDES CUE SDWAN Address_Destination_Core_GYE	Latency	CEDIA_GYE_CUE (LAN1)
4	GYE_TO_CUE_TUNEL	all	REDES CUE SDWAN Address_Destination_Core_GYE	Latency	TUNNEL A CUE
1	TO_CEDIA_GYE_CUE	all	Address_Destination_Core_GYE REDES CUE SDWAN REDES_UIO_SDWAN REDES_UIO_Y_CUE_SDWAN		CEDIA_GYE_CUE (LAN1)
8	HC_UIO_CUE	all	172.29.253.16/30 172.29.253.8/30		CEDIA_GYE_CUE (LAN1)
7	Internet	all	all		WAN-PRINCIPAL-INTERNET (WAN-TELC...
Implicit 1					

Figura 3. 25 Listado de Reglas SD-WAN para el tráfico desde Guayaquil hacia otras sedes
Fuente: Autora

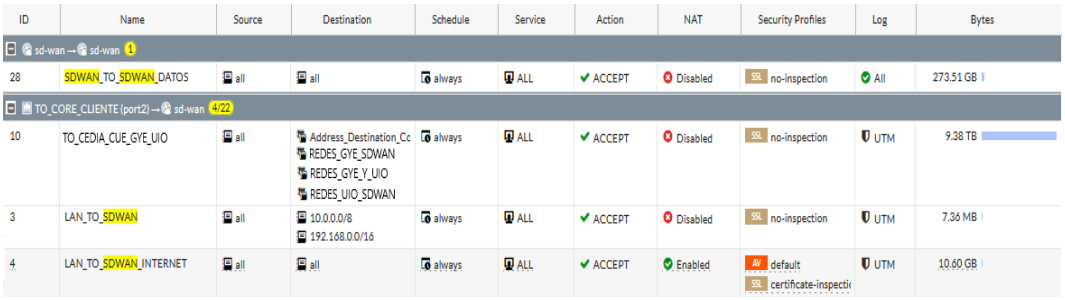
En cada regla, para un segmento de red en específico como destino, se utiliza de interfaz a uno de los proveedores de servicio. Es muy importante mencionar que el orden de las reglas SD-WAN define la prioridad del tráfico. En caso de que ninguna de las interfaces cumpla con los criterios del SLA, FortiGate equilibra el tráfico entre todas las interfaces.

Cabe mencionar que la regla en común que tienen todos los puntos es aquella implícita para balancear el tráfico, esta regla es por defecto fuente-destino cualquier IP.

3.8.2 Políticas de Firewall

En los firewalls Fortigate se debe habilitar permisos de direccionamiento de tráfico, tanto en entrada como salida. En la figura que se tiene de las políticas se muestra el consumo de ancho de banda acumulado. Para el equipo Fortigate instalado en el punto de Cuenca se configuraron políticas de SD-WAN a SD-WAN y desde el Core hacia SD-WAN.

Una de las diferencias radica en que la política de navegación hacia internet (ID 4) tiene habilitado el NAT (Network Address Translation).

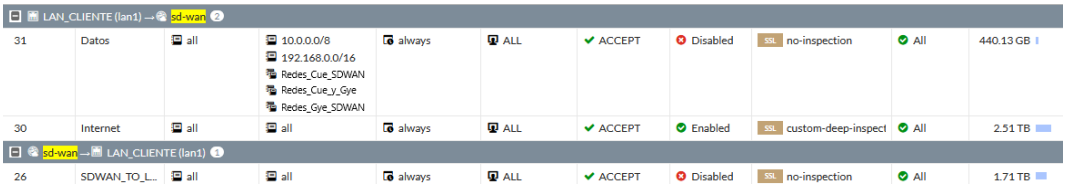


ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
sd-wan → sd-wan 1										
28	SDWAN_TO_SDWAN_DATOS	all	all	always	ALL	ACCEPT	Disabled	no-inspection	All	273.51 GB
TO_CORE_CLIENTE (port2) → sd-wan 4/22										
10	TO_CEDIA_CUE_GYE_UIO	all	Address_Destination_Cc REDES_GYE_SDWAN REDES_GYE_Y_UIO REDES_UIO_SDWAN	always	ALL	ACCEPT	Disabled	no-inspection	UTM	9.38 TB
3	LAN_TO_SDWAN	all	10.0.0.0/8 192.168.0.0/16	always	ALL	ACCEPT	Disabled	no-inspection	UTM	7.36 MB
4	LAN_TO_SDWAN_INTERNET	all	all	always	ALL	ACCEPT	Enabled	default certificate-inspecti	UTM	10.60 GB

Figura 3. 26 Políticas de tráfico desde Cuenca hacia SD-WAN
Fuente: Autora

Para el equipo Fortigate instalado en el punto de Guayaquil se tienen políticas de LAN públicas a SD-WAN, corresponde a la navegación hacia internet desde el segmento público, por tal motivo no sale enmascarado.

Las políticas que tienen el flujo del Core Cliente a SD-WAN, corresponde a la navegación hacia internet desde el segmento privado, se habilitó el enmascaramiento de IP, se aplicaron niveles de perfiles de seguridad dependiendo de los permisos que se desean habilitar a los grupos de usuarios.

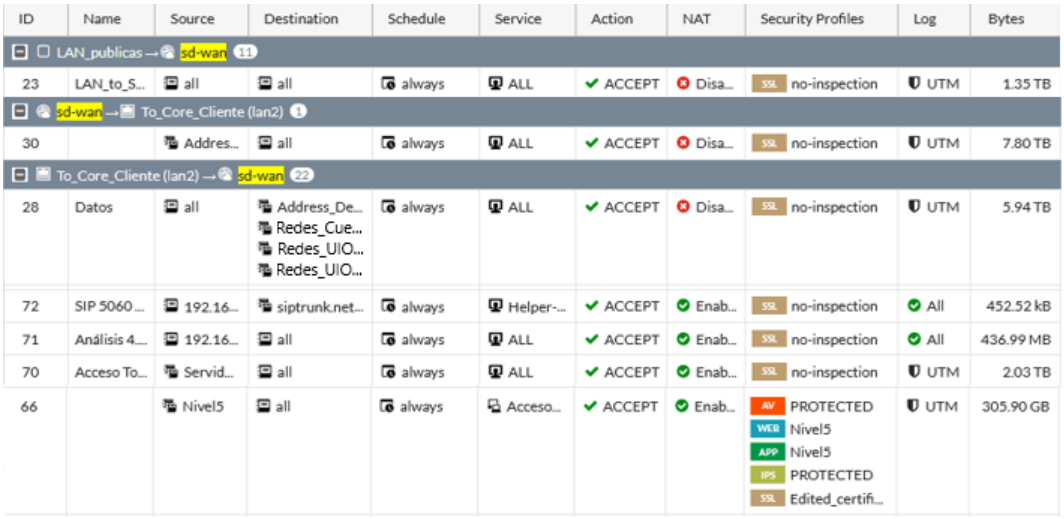


LAN_CLIENTE (lan1) → sd-wan 2										
31	Datos	all	10.0.0.0/8 192.168.0.0/16 Redes_Cue_SDWAN Redes_Cue_y_Gye Redes_Gye_SDWAN	always	ALL	ACCEPT	Disabled	no-inspection	All	440.13 GB
30	Internet	all	all	always	ALL	ACCEPT	Enabled	custom-deep-inspect	All	2.51 TB
sd-wan → LAN_CLIENTE (lan1) 1										
26	SDWAN_TO_L...	all	all	always	ALL	ACCEPT	Disabled	no-inspection	All	1.71 TB

Figura 3. 27 Políticas de tráfico desde Guayaquil hacia SD-WAN
Fuente: Autora

En el punto de Quito se tienen políticas de LAN a SD-WAN, correspondientes a la navegación hacia internet desde el segmento privado, por tal motivo sale enmascarado. La política con ID 31 corresponde al flujo de LAN a SD-WAN para el servicio de datos, es decir el envío de paquetes desde Quito hacia los demás puntos.

Las políticas que tienen el flujo del Core Cliente a SD-WAN, corresponde a la navegación hacia internet desde el segmento privado, por lo tanto se habilita el enmascaramiento de IP.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
LAN_publicas → sd-wan 11										
23	LAN_to_S...	all	all	always	ALL	ACCEPT	Disa...	no-inspection	UTM	1.35 TB
sd-wan → To_Core_Cliente (lan2) 1										
30		Addres...	all	always	ALL	ACCEPT	Disa...	no-inspection	UTM	7.80 TB
To_Core_Cliente (lan2) → sd-wan 22										
28	Datos	all	Address_De... Redes_Cue... Redes_UIO... Redes_UIO...	always	ALL	ACCEPT	Disa...	no-inspection	UTM	5.94 TB
72	SIP 5060 ...	192.16...	siptrunk.net...	always	Helper-...	ACCEPT	Enab...	no-inspection	All	452.52 kB
71	Análisis 4...	192.16...	all	always	ALL	ACCEPT	Enab...	no-inspection	All	436.99 MB
70	Acceso To...	Servid...	all	always	ALL	ACCEPT	Enab...	no-inspection	UTM	2.03 TB
66		Nivel5	all	always	Acceso...	ACCEPT	Enab...	AV PROTECTED WEB Nivel5 APP Nivel5 IPS PROTECTED SSL Edited_certifi...	UTM	305.90 GB

Figura 3. 28 Políticas de tráfico desde Quito hacia SD-WAN
Fuente: Autora

3.9 Resultados de SLA en hora pico de trabajo

Para el SLA de rendimiento se mide el estado de los enlaces o interfaces que son miembros del SD-WAN, esto lo realiza mediante el envío de señales de sondeo por cada uno de los enlaces a un servidor y midiendo la calidad del enlace.

En caso de detectar que uno de los enlaces no supera todas las comprobaciones del estado, las rutas de ese enlace se eliminan del grupo de equilibrio de carga del enlace SD-WAN y el tráfico se enruta a través de otros enlaces. Cuando el enlace vuelve a operar, se restablecen las rutas. De esta manera se evita que el tráfico se envíe a un enlace roto y se pierdan los datos.

Para el escenario del punto de Cuenca se muestra la representación de los parámetros de rendimiento medidos en milisegundos por un lapso de

10 minutos, para ambos proveedores, sea por túneles o interfaces físicas en el horario de las 09h00 am.

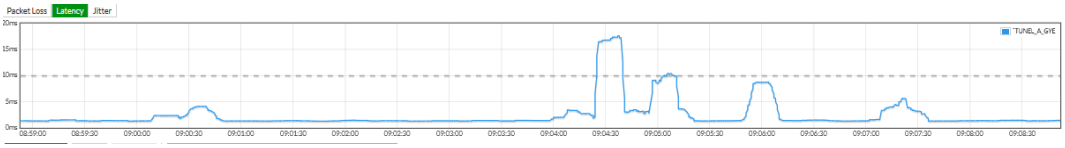


Figura 3. 29 Monitoreo de Health-check desde Cuenca hacia Guayaquil
Fuente: Autora

El servidor por detectar en el HC hacia Guayaquil tiene la IP 10.99.97.1. En la figura 3.29, se observa que en un determinado tiempo se superaron los 10ms del umbral de latencia, durante estos segundos la conexión hacia Guayaquil se realiza mediante el proveedor Cedia, una vez que la latencia se ha regularizado, se regresa a enviar el tráfico por el proveedor Telconet.

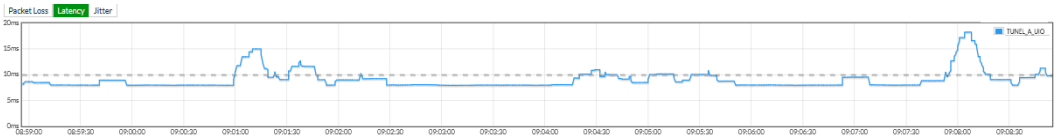


Figura 3. 30 Monitoreo de Health-check desde Cuenca hacia Quito
Fuente: Autora

Para el HC de Cedia se observa un constante valor de latencia, el cual permite que el envío de tráfico se realice mediante este proveedor.

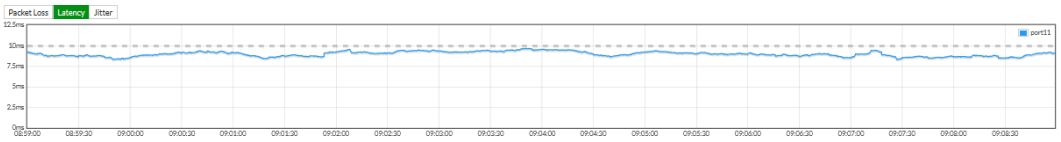


Figura 3. 31 Monitoreo de Health-check para Cedia en Cuenca
Fuente: Autora

Para el equipo Fortigate instalado en el punto de Guayaquil, se muestra la representación de los parámetros de rendimiento medidos en milisegundos por un lapso de 10 minutos, para ambos proveedores, sea por túneles o interfaces físicas. Horario 09h00.

El servidor por detectar en el HC hacia Cuenca tiene la IP 10.99.97.2. En la figura 3.32, se observa que se mantiene un umbral de latencia menor a

los 25ms, lo cual indica que el tráfico determinado es enviado durante este lapso a través del proveedor Telconet mediante el Túnel a Cuenca.

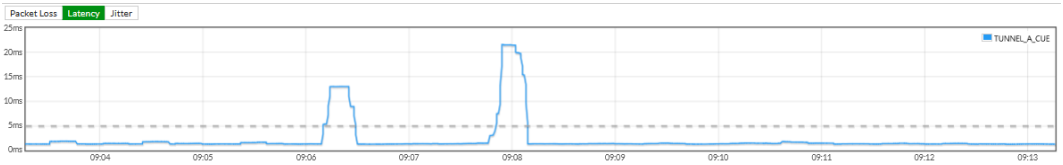


Figura 3. 32 Monitoreo de Health-check desde Guayaquil hacia Cuenca
Fuente: Autora

El servidor por detectar en el HC hacia Quito tiene la IP 10.99.97.9. En la figura 3.33, se observa que en un determinado tiempo se superaron los 10ms del umbral de latencia, durante estos segundos la conexión hacia Guayaquil se realiza mediante el proveedor Cedia, una vez que la latencia se ha regularizado, se regresa a enviar el tráfico por el proveedor Telconet.

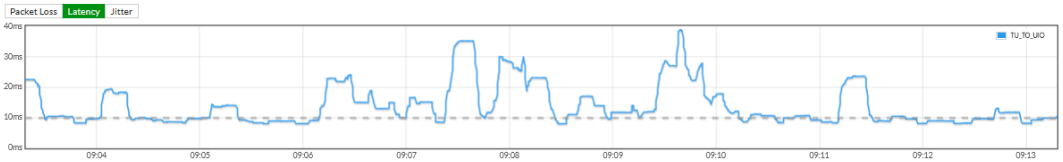


Figura 3. 33 Monitoreo de Health-check desde Guayaquil hacia Quito
Fuente: Autora

Para el HC de Cedia se observa un constante valor de latencia, el cual permite que el envío de tráfico se realice mediante este proveedor.

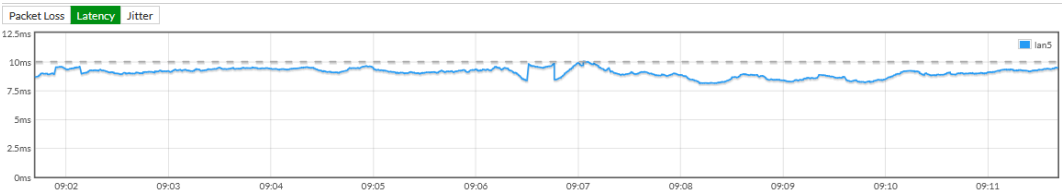


Figura 3. 34 Monitoreo de Health-check para Cedia en Guayaquil
Fuente: Autora

Para el equipo Fortigate instalado en el punto de Quito, se muestra la representación de los parámetros de rendimiento medidos en milisegundos por un lapso de 10 minutos, para ambos proveedores, sea por túneles o interfaces físicas. Horario 09h00.

El servidor a detectar en el HC hacia Cuenca tiene la IP 10.99.97.6. En la figura 3.35, se observa que se mantiene un umbral de latencia mayor a los 10ms, durante estos segundos la conexión hacia Cuenca se realiza mediante el proveedor Cedia pese a no tener pérdidas de paquetes, una vez que la latencia se ha regularizado, se regresa a enviar el tráfico por el proveedor Telconet.

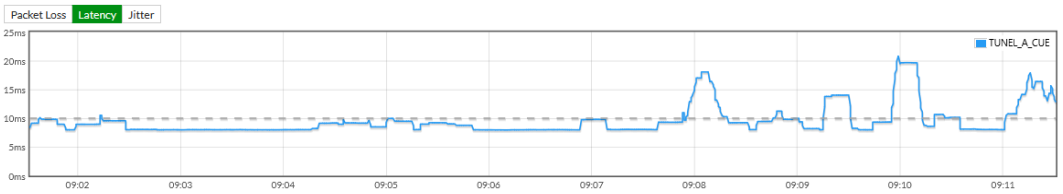


Figura 3. 35 Monitoreo de Health-check desde Quito hacia Cuenca
Fuente: Autora

El mismo escenario se presenta para el HC hacia Guayaquil, el cual tiene como servidor a detectar la IP 10.99.97.10.

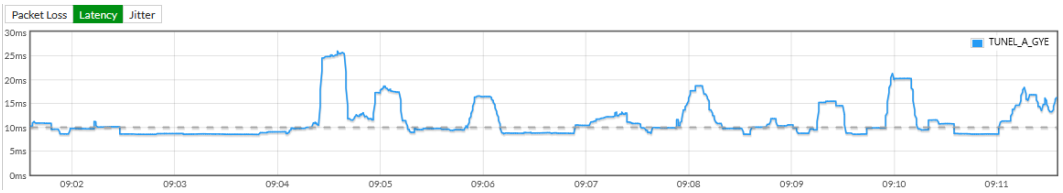


Figura 3. 36 Monitoreo de Health-check desde Quito hacia Guayaquil
Fuente: Autora

Para el HC de cedia se observa un constante valor de latencia, el cual permite que el envío de tráfico se realice mediante este proveedor.

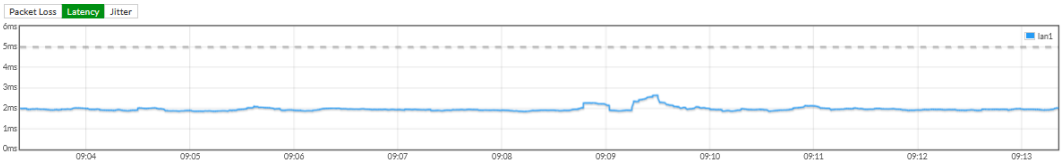


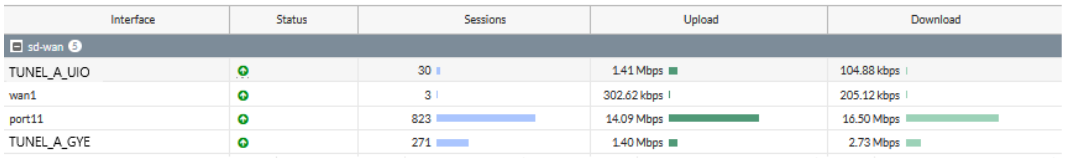
Figura 3. 37 Monitoreo de Health-check para Cedia en Quito
Fuente: Autora

3.10 Monitoreo de SD-WAN

Para verificar el consumo de ancho de banda en cada miembro del SD-WAN, se realizan los siguientes pasos:

- Monitor
- SD-WAN

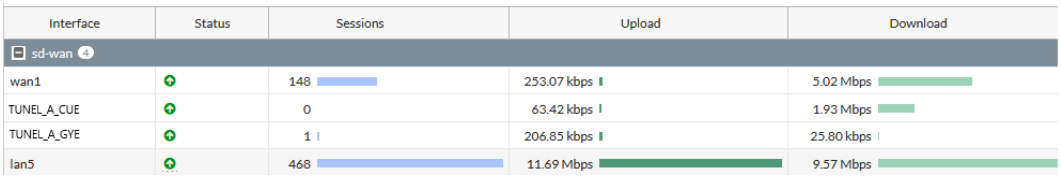
Como se aprecia en la figura 3.38, las interfaces pertenecientes al punto de Cuenca presentan datos de consumo tanto en carga como para descarga. Al momento de la captura se obtiene como resultado que la interfaz que consume mayores recursos es el puerto11 (Cedia_Cue_Gye_Uio) es decir el enlace que se tiene con el segundo proveedor, el cual presenta 823 sesiones; seguido por el túnel a Guayaquil, el cual tiene 271 sesiones, este es levantado por el proveedor Telconet.



Interface	Status	Sessions	Upload	Download
sd-wan 5				
TUNEL_A_UIO		30	1.41 Mbps	104.88 kbps
wan1		3	302.62 kbps	205.12 kbps
port11		823	14.09 Mbps	16.50 Mbps
TUNEL_A_GYE		271	1.40 Mbps	2.73 Mbps

Figura 3. 38 Monitoreo de SD-WAN en sede Cuenca
Fuente: Autora

Para el punto de Quito se obtuvo como resultado que el miembro SD-WAN con mayor número de sesiones es el puerto lan5, el cual corresponde al enlace con Cedia, teniendo en carga 11.69Mbps y en descarga 9.57Mbps. La interfaz de menor consumo es el túnel a Cuenca, el cual tiene 63.42Kbps de carga y 1.93Mbps de descarga, este enlace pertenece al proveedor Telconet.



Interface	Status	Sessions	Upload	Download
sd-wan 4				
wan1		148	253.07 kbps	5.02 Mbps
TUNEL_A_CUE		0	63.42 kbps	1.93 Mbps
TUNEL_A_GYE		1	206.85 kbps	25.80 kbps
lan5		468	11.69 Mbps	9.57 Mbps

Figura 3. 39 Monitoreo de SD-WAN en sede Quito
Fuente: Autora

Para el punto de Guayaquil se obtuvo como resultado que el miembro SD-WAN con mayor número de sesiones es el WAN1, el cual corresponde al servicio de internet, teniendo en carga 6.59Mbps y en descarga 5.82Mbps.

La interfaz de menor consumo es el túnel a Quito, el cual tiene 550.20Kbps de carga y 730.51Kbps de descarga, ambos enlaces pertenecen al proveedor Telconet.

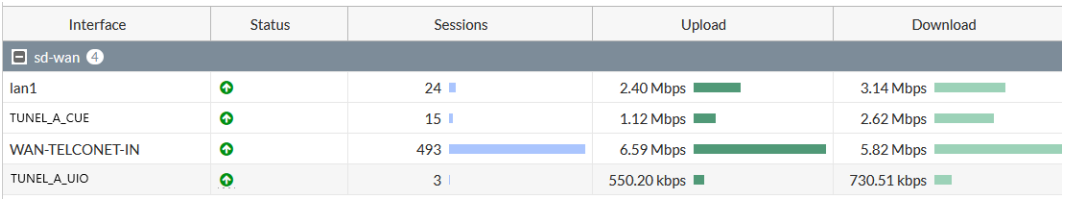


Figura 3. 40 Monitoreo de SD-WAN en sede Guayaquil
Fuente: Autora

Es importante mencionar que los valores presentados fueron medidos en tiempo real, es decir, los valores de carga y descarga muestran el consumo realizado en ese momento, no son valores acumulados.

Conclusiones

En cuanto a lo abordado con anterioridad para el diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la universidad Politécnica Salesiana, se constató que este diseño permite tener el control total de comunicaciones entre redes, pudiendo realizar cualquier tipo de cambios en todo momento, sabiendo que las modificaciones se realizan en tiempo real en todas las sedes.

Para poder definir este diseño se analizó el modo de comunicación entre redes, por tal motivo se levantaron túneles punto a punto en cada una de las sedes de la Universidad, esto debido a que es confiable para tráfico sensible a retrasos, además que el túnel encriptado permite que los datos se transmitan de manera segura, evitando así que se presenten intersecciones maliciosas.

De acuerdo a los resultados presentados durante las horas de mayor consumo, se evidenció que las reglas SD-WAN se establecieron de manera correcta, permitiendo que la transmisión de datos se realice por el segundo proveedor, dado que con el primer proveedor no se cumplían los valores establecidos en las restricciones del SLA, y una vez estabilizados los valores, el tráfico comenzó a circular por el primer proveedor, siendo esto imperceptible para los usuarios finales.

En base a lo anteriormente expuesto se concluye que la tecnología SD-WAN es la mejor herramienta para poder establecer un balanceo de carga, es decir, poder utilizar múltiples proveedores de modo activo-activo, administrando de mejor manera el ancho de banda, adaptándolo a las prioridades y necesidades de la Universidad de forma totalmente personalizada.

Recomendaciones

Llevar un control periódico de mediciones o evaluación del comportamiento de las reglas SD-WAN, sobre todo para poder tener conocimiento del mayor tráfico enviado por cada proveedor.

Revisar en el portal de Fortinet la versión del Firmware recomendada para implementar SD-WAN, debido que en cada actualización se corrigen errores en el sistema.

Mantener actualizados en conocimientos sobre SD-WAN al personal de TI mediante capacitaciones constantes.

Aprovechar las funcionalidades que los equipos Fortigate poseen, e implementar perfiles de seguridad mediante la activación de la licencia.

Bibliografía

Adaptix. (2017). *Redefiniendo los Firewalls de Nueva Generación.* Obtenido de https://www.adaptixnetworks.com/firewalls-nueva-generacion/

Aguilar, I. (2020). *Fibertel Perú MPLS.* Obtenido de https://slideplayer.es/slide/17987155/

edualejo77. (2011). *VPN's y MPLS cuál es su relación???* Obtenido de https://edualejo77.wordpress.com/2011/08/16/vpns-y-mpls-cual-es-su-relacion/

Fortinet. (2021). *Managed SD-WAN for Service Providers.* Obtenido de https://www.fortinet.com/solutions/service-provider/managed-secure-sd-wan-service-with-fortinet

FORTINET. (2021). *Next-Generation Firewall (NGFW).* Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall

Fortinet. (2021). *Servicios del paquete 360 Protection.* Obtenido de https://www.fortinet.com/lat/products/360-protection-bundle/services

Hernandez, G. (2019). *Conociendo la arquitectura básica de una red MPLS.* Obtenido de Huawei: https://forum.huawei.com/enterprise/es/conociendo-la-arquitectura-b%C3%A1sica-de-una-red-mpls/thread/582304-100237

LIDER IT. (2020). *¿Qué es la seguridad gestionada?* Obtenido de https://www.liderit.es/ventajas-seguridad-gestionada/

ODS. (2020). *Servicios de seguridad gestionados – MSSP.* Obtenido de https://opendatasecurity.io/servicios-de-seguridad-gestionados-mssp/

Parra, D. (2020). *SD-WAN vs MPLS: ¿Qué es lo mejor?* Obtenido de https://www.bits.com.mx/sd-wan-vs-mpls-que-es-lo-mejor/

RebootSystems. (2021). *Next-Generation Firewall (NGFW).* Obtenido de http://rebootsystems.mx:8069/blog/nuestro-blog-1/next-generation-firewall-ngfw-2

Sánchez, D. (2020). *¿Qué es SD-WAN? Explicación sencilla ¿Para qué sirve?* Obtenido de https://info.ita.tech/blog/que-es-sd-wan

Sarenet. (2019). *Seguridad gestionada: protección desde el perímetro hasta el end-point.* Obtenido de https://blog.sarenet.es/ciberseguridad-seguridad-gestionada/

SDxCentral LLC. (2018). *Implementación de SD-WAN en el Mundo Real.* Obtenido de https://www.ibm.com/downloads/cas/3AW5O9OR

Shah, N. (2019). *Using SD-WAN Aggregation to Meet Bandwidth Needs.* Obtenido de https://www.fortinet.com/blog/business-and-technology/fortinets-advanced-sdwan-capabilities-help-achieve-max-performance

Tapasco, M. (2008). *MPLS, el presente de las redes IP.* Obtenido de https://core.ac.uk/download/pdf/71395663.pdf

Telecapp. (2021). *¿Qué es MPLS y cómo funciona?* Obtenido de https://telecapp.com/introduccion-redes-mpls

Zuñiga, M. (2019). *Integridad, Disponibilidad y Privacidad.* Obtenido de https://ticbachillermzf.home.blog/2019/01/08/integridad-disponibilidad-y-privacidad/

Glosario de términos

ATM: Modo de transferencia asíncrona

CBR: Codificación de tasa de bits constante

CPE: Equipo Local del Cliente

CR-LDP: Protocolo de Distribución de Etiquetas con Encaminamiento Basado en Restricciones

DIFFSERV: Servicios Diferenciados

FEC: Corrección de errores hacia adelante

IDS: Sistema de detección de intrusiones

IP: Protocolo de internet

IPSEC: Seguridad del protocolo de Internet. es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando cada paquete IP en un flujo de datos.

LAN: Área de red local

LDP: Protocolo para distribuir etiquetas en aplicaciones sin ingeniería de tráfico

LSR: Es un encaminador de alta velocidad dentro de una red MPLS que participa en el establecimiento de los LSP

MPLS: Multiprotocol Label Switching

MSSP: Proveedores de servicios de seguridad administrados

NGFW: Cortafuegos de próxima generación. Filtran el tráfico de red para proteger a una organización de amenazas internas y externas

NP7: Procesador de red 7

OSI: Modelo de interconexión de sistemas abiertos

PPP: Protocolo punto a punto

RSVP: Protocolo de reserva de recursos

SD-WAN: Software-Defined Wide Area Network

SLA: Acuerdo de Nivel de servicio. Es un contrato que describe el nivel de servicio que un cliente espera de su proveedor

SPU: Servicio Postal Universal

SSL: Capa de Puertos Seguros

TE: Ingeniería de tráfico

TLS: Capa de transporte seguro

UCPE: Es una plataforma para uso general que integra computación, almacenamiento y redes en un servidor genérico

VCI: Identificador de Canal Virtual

VNF: Funciones de red virtualizadas

VPI: Identificador de Ruta Virtual

VRF: Enrutamiento y reenvío virtual es una tecnología que permite que un enrutador ejecute más de una tabla de enrutamiento simultáneamente.

WAN: Red de área extensa

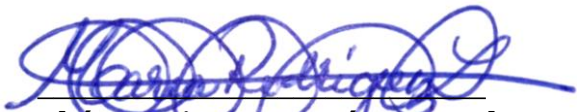
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Rodríguez Limones María Fernanda**, con C.C: # **0927104463** autor/a del trabajo de titulación: **Diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana,** 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 10 días del mes de noviembre del 2021



Rodríguez Limones María Fernanda
C.C: 0927104463

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	Diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la Universidad Politécnica Salesiana	
AUTOR(ES)	Rodríguez Limones Maria Fernanda	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz	
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	**Guayaquil, a los 10 días del mes de noviembre del 2021**	**No. DE PÁGINAS: 76**
ÁREAS TEMÁTICAS:	Red MPLS, SD-WAN, ruta dinámica, Orquestación centralizada, Redes y seguridad perimetral, Next-generation firewall, Fortigate	
PALABRAS CLAVES/ KEYWORDS:	SD-WAN, balanceo, ruta, contingencia, seguridad, tiempo de respuesta, calidad de servicio, operatividad	
RESUMEN/ABSTRACT: El presente trabajo describe el diseño de un esquema SD-WAN utilizando Firewalls marca Fortigate para la Universidad Politécnica Salesiana, con el fin de poder balancear la carga de tráfico a través de dos proveedores de servicios de internet y datos, siendo estos Telconet y Cedia. El balanceo de carga podrá permitir a los equipos Fortigate elegir la mejor ruta, es decir, el camino que cumpla con los parámetros necesarios de calidad de servicio para poder enviar datos hacia las distintas sedes, evitando de esta manera que se produzcan saturaciones o tiempos elevados de respuestas. El diseño utilizará ambos proveedores en modo activo – activo, dicho de otra manera, cada proveedor enviará constantemente datos establecidos mediante reglas, que a su vez también servirán como contingencia en caso de que exista algún inconveniente lógico o físico con uno de los proveedores antes mencionados, ofreciendo de esta manera un servicio confiable por los perfiles de seguridad, y operatividad constante al usuario final.		
ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO AUTOR/ES:	**Teléfono:** +593-959149526	**E-mail:** mafer_rodriguez@outlook.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):		