PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de
Magíster en Tecnologías de Información mención Gestión y Administración de TI

ESTUDIO DE COMPARACIÓN DE TECNOLOGÍAS SD-WAN COMO ALTERNATIVA PARA ENLACES MPLS DEDICADOS

Autor: Mishell Stefany Viteri Barrera
Director: Santiago Silva Proaño

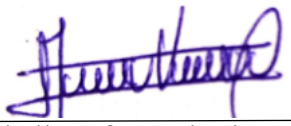
Quito, 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, MISHELL STEFANY VITERI BARRERA, declaro y autorizo revisar y evaluar mi trabajo de titulación denominado " ESTUDIO DE COMPARACIÓN DE TECNOLOGÍAS SD-WAN COMO ALTERNATIVA PARA ENLACES MPLS DEDICADOS".

Además, autorizo mis derechos de propiedad intelectual a la Pontificia Universidad Católica del Ecuador a conservar una copia de la tesis en su biblioteca digital, con el propósito de compartir el conocimiento generado con otros estudiantes, profesores y personas interesadas.



Mishell Stefany Viteri Barrera

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: "**ESTUDIO DE COMPARACIÓN DE TECNOLOGÍAS SD-WAN COMO ALTERNATIVA PARA ENLACES MPLS DEDICADOS**", presentado por el maestrante MISHELL STEFANY VITERI BARRERA titular de la Cédula de Identidad Nº 1600712770 para optar al Grado de Magíster en Tecnologías de Información mención Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los 31 días de mayo de 2023



Santiago David Silva Proaño C.I. 171481593-1

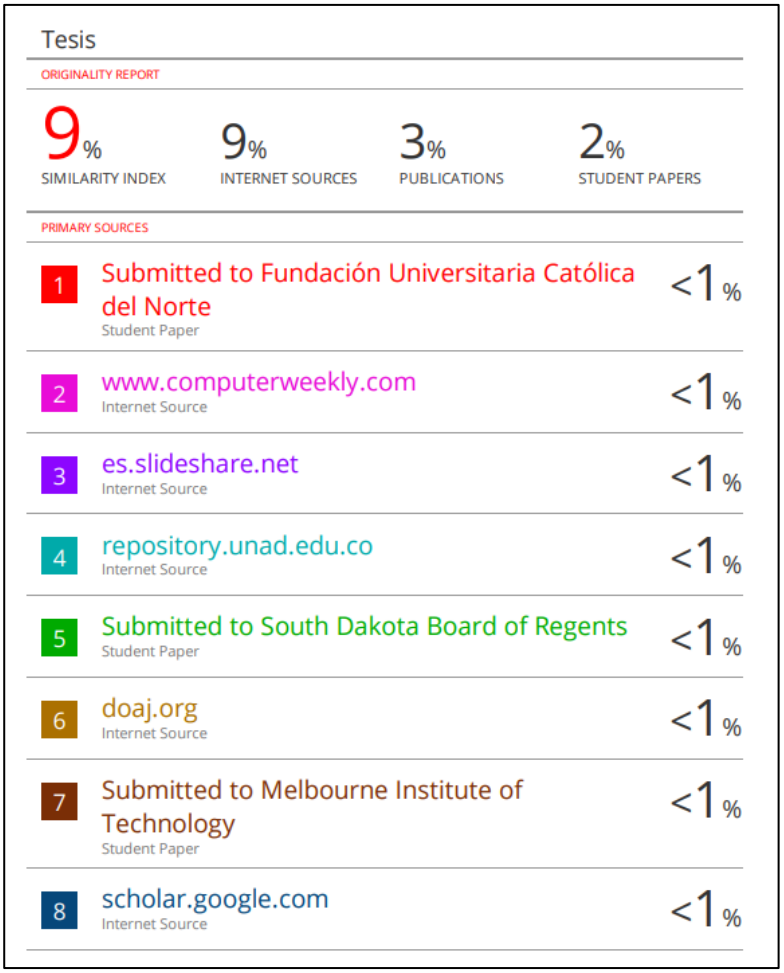
ssilva068@puce.edu.ec

NRO TELEFONO: 0992388692

NOTA: 30/30

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 9% índice de similitud con otras fuentes.

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE



Tesis

ORIGINALITY REPORT

9%	9%	3%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

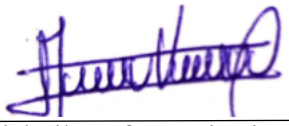
PRIMARY SOURCES

1	Submitted to Fundación Universitaria Católica del Norte Student Paper	<1%
2	www.computerweekly.com Internet Source	<1%
3	es.slideshare.net Internet Source	<1%
4	repository.unad.edu.co Internet Source	<1%
5	Submitted to South Dakota Board of Regents Student Paper	<1%
6	doaj.org Internet Source	<1%
7	Submitted to Melbourne Institute of Technology Student Paper	<1%
8	scholar.google.com Internet Source	<1%

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Mishell Stefany Viteri Barrera, en calidad de autor de la tesis titulada " ESTUDIO DE COMPARACIÓN DE TECNOLOGÍAS SD-WAN COMO ALTERNATIVA PARA ENLACES MPLS DEDICADOS", presentada para optar por el grado de Magister en Tecnologías de Información mención Gestión y Administración de TI, hago la siguiente declaración de autenticidad y responsabilidad:

1. Declaro que el presente trabajo de tesis es el resultado de mi propia investigación y esfuerzo. Todas las ideas, conceptos, teorías, resultados y conclusiones presentados en este documento son de mi autoría, excepto cuando se indique lo contrario con una adecuada referencia y cita a las fuentes correspondientes.
2. Asimismo, declaro que este trabajo es original y ha sido desarrollado de manera ética, respetando los principios de integridad académica. Cualquier referencia, cita o material utilizado de otras fuentes ha sido debidamente reconocido y citado según las normas establecidas por la institución.
3. También, he seguido los principios de integridad académica y ética en la realización de esta tesis, manteniendo la honestidad intelectual y la rigurosidad científica en todo el proceso de investigación.



Mishell Stefany Viteri Barrera

DEDICATORIA

Dedico este trabajo de investigación a aquellas personas que han sido fundamentales en mi camino académico y personal, brindándome su apoyo, aliento y amor incondicional.

A mi madrecita Mirian, por brindarme el soporte emocional y económico necesario para lograr mis metas. Su constante sacrificio y dedicación son una inspiración para mí.

A mi hijo Emilio, por ser luz en mi vida, mi mayor inspiración y motivo de orgullo. Su presencia en mi vida ha sido un impulso constante para superar desafíos y alcanzar metas.

A mi esposo Oscar, por su paciencia, comprensión y apoyo durante todo este proceso, las palabras de aliento y amor incondicional han sido mi motor para seguir adelante.

Mishell Stefany Viteri Barrera

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN 14

Antecedentes de la Investigación 14

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 16

1.1 Formulación del problema 16

1.2 Objetivos de la Investigación 16

1.2.1 Objetivo General 16

1.2.2 Objetivos Específicos 16

1.3 Justificación de la Investigación 17

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA 18

2.1 CONMUTACIÓN DE ETIQUETAS MULTIPROCOLO (MPLS) 18

2.1.1 Arquitectura MPLS 18

2.1.2 Componentes MPLS 19

2.1.3 Aplicaciones de MPLS 20

2.2 SDN 24

2.2.1 Arquitectura SDN 24

2.3 SD-WAN 25

2.3.1 Arquitectura SD-WAN 26

2.3.1.1 Tipos de arquitectura 26

2.3.2 Funcionamiento 26

2.3.3 Beneficios de SD-WAN 27

2.3.4 Soluciones SD-WAN 27

CAPÍTULO III: METODOLOGÍA 31

3.1 Tipo de Investigación 31

3.2 Diseño de Investigación 31

3.3 Unidades de Estudio 31

3.4 Técnicas e instrumentos de recolección de datos 31

3.5 Técnica de Análisis de Datos 31

CAPÍTULO IV: ANÁLISIS Y DISUSION DE RESULTADOS 32

4.1 Análisis General de la situación de las tecnologías MPLS y SD-WAN 32

4.2 SD-WAN vs MPLS 33

4.3 Fabricantes de SD-WAN y sus soluciones 35

4.3.1 Enfoque 36

4.3.2 Gestión centralizada 36

4.3.3 Características de seguridad 36

4.3.4 Plataforma unificada de seguridad 36
4.3.5 Integración de servicios en la nube 36
4.3.6 Técnicas avanzadas de optimización de tráfico 36
4.3.7 Escalabilidad 37
4.3.8 Interfaz de usuario 37
4.3.9 Compatibilidad con infraestructuras MPLS existentes 37
4.3.10 Compatibilidad con túneles Ipsec 37
4.3.11 Enlaces SD-WAN 37
CAPITULO V: PRESENTACION DE LA PROPUESTA 39
5.1 SD-WAN como alternativa de solución 39
CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES 41
6.1 CONCLUSIONES 41
6.2 RECOMENDACIONES 42

ÍNDICE DE GRÁFICOS

Figura 1: Arquitectura MPLS 18
Figura 2: Plano de datos y control en un router MPLS. 19
Figura 3: Flujo de trabajo de un sistema MPLS. 20
Figura 4: Encabezado SHIM en MPLS 21
Figura 5: Funcionamiento MPLS 22
Figura 6: Arquitectura SDN. 25
Figura 7: Cuadrante mágico de Gartner 2022. 27
Figura 8: Arquitectura Cisco Viptela SD-WAN 28
Figura 9: Arquitectura de Fortinet SD-WAN. 29
Figura 10: Caso de éxito: SD-WAN Viptela en Banco Pichincha. 37
Figura 11: Caso de éxito: SD-WAN Fortinet UNIANDES 38
Figura 12: Aspectos SD-WAN 39
Figura 13: Recomendaciones para la implementación SD-WAN 40

ÍNDICE DE TABLAS

Tabla 1: Ventajas y desventajas SD-WAN y MPLS..... 32
Tabla 2: Comparativa SD-WAN vs MPLS..... 34
Tabla 3: Comparativa Cisco vs Fortinet 35

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN
Y ADMINISTRACIÓN DE TI

ESTUDIO DE COMPARACIÓN DE TECNOLOGÍAS SD-WAN COMO ALTERNATIVA PARA ENLACES MPLS DEDICADOS

Autor: Mishell Stefany Viteri

Director -Tutor: Santiago Silva

Fecha:31 de mayo de 2023

RESUMEN

A medida que las empresas crecen, necesitan construir una infraestructura de red que conecte sucursales en diferentes regiones geográficas. Ante esta necesidad los equipos de redes de TI deben equilibrar las necesidades de simplicidad, rendimiento, confiabilidad y seguridad de la organización, al tiempo que consideran los costos y el cumplimiento.
La tecnología de conmutación de etiquetas multiprotocolo (MPLS) surgió como una tecnología de red pionera en la que muchos proveedores de servicios de Internet han realizado grandes inversiones.

Las MPLS son redes basadas en paquetes que ofrecen ventajas considerables, que incluyen una mejor utilización de la red, una latencia de red reducida y la capacidad de cumplir con la calidad de servicio y los estrictos requisitos de acuerdo de nivel de cualquier tráfico entrante.
Por otra parte, SD-WAN es una tecnología que ha recibido mucha atención en los últimos años y tiene el potencial de satisfacer las crecientes demandas de redes de área extendida (WAN por sus siglas en inglés Wide Area Network) por ser confiables y eficientes entre las empresas de hoy.

Este trabajo de investigación pretende comparar los beneficios, ventajas y desventajas de MPLS y SD-WAN con el objetivo de brindar al lector conceptos básicos e indispensables de un conocimiento integral sobre las tecnologías. Además, en el estudio, se hace un breve análisis de las soluciones de SD-WAN existentes en el mercado ecuatoriano que son Cisco y Fortinet, fabricantes que lideran el cuadrante mágico de Gartner con el fin de proporcionar una base de conocimientos sobre la tecnología a futuros investigadores de la academia estudiantil y a futuros clientes que busquen incorporar esta tecnología en sus empresas.

Palabras clave: SD-WAN, MPLS, Red de área amplia (WAN), Conectividad.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

COMPARATIVE STUDY OF SD-WAN TECHNOLOGIES AS AN ALTERNATIVE OF MPLS DEDICATED LINKS

Author: Mishell Stefany Viteri Barrera

Director -Tutor: Santiago Silva

Date:31 de Mayo de2023

ABSTRACT

Companies must build a network infrastructure connecting branches in different geographic regions as they continue growing. With this need, IT network teams must balance the organization's needs for simplicity, performance, reliability, and security while considering costs and compliance.
Multiprotocol Label Switching (MPLS) technology emerged as a pioneering network technology in which many Internet service providers have invested heavily.

MPLS are packet-based networks that offer considerable benefits, including better network utilization, reduced network latency, and the ability to meet strict QoS and level agreement requirements for any incoming traffic.
On the other hand, SD-WAN is a technology that has received much attention in recent years and has the potential to meet the increasing demands of Wide Area Networks (WANs) for being reliable and efficient between companies today.

This research compares the benefits, advantages, and disadvantages of MPLS and SD-WAN to provide the reader with basic and essential concepts of comprehensive knowledge about the technologies. In addition, in the study, a brief analysis is made of the existing SD-WAN solutions in the Ecuadorian market are Cisco and Fortinet, manufacturers that lead the Gartner magic quadrant in order to provide a knowledge base on the technology to future researchers from the student academy and future clients seeking to incorporate this technology into their companies.

Keywords: SD-WAN, MPLS, Wide Area Network (WAN), Connectivity.

INTRODUCCIÓN

Teniendo en cuenta el gran avance de la comunicación y la colaboración empresarial sobre redes privadas, MPLS brinda seguridad a la hora de poder comunicarse de manera confiable y segura con distintas empresas.

MPLS es conocido en el campo tecnológico como el protocolo de comunicación más popular, destinado a conectar varios tipos de datos enviados a través de la misma red para que los paquetes de información no generen retrasos durante la transmisión de la información (Stepanova & Nouma, 2022).

Sin embargo, las redes empresariales que tienen arquitecturas tradicionales luchan por mantenerse al día con el aumento de las modernas aplicaciones nativas de la nube y las tecnologías avanzadas. Las arquitecturas tradicionales se centran en el hardware y son incompatibles con los requisitos de red de la nueva era, dando lugar a la red de área amplia definida por software (SD-WAN) que utiliza los conceptos de redes definidas por software (SDN) para distribuir el tráfico de red a través de una red de área amplia (WAN).

En este contexto, las SD-WAN son una solución innovadora para satisfacer las necesidades de redes en la era de la nube. Al aplicar la virtualización sobre conexiones WAN para conectar redes empresariales, sucursales y centros de datos, las SD-WAN mejoran la calidad del servicio, la latencia y los problemas de carga que desafían a las arquitecturas WAN tradicionales.

Este trabajo de investigación tiene como fin la comparación entre MPLS y SD-WAN, la cual proporciona al lector la posibilidad de diferenciar cada una de ellas, teniendo como antecedente el funcionamiento, arquitectura y componentes esenciales que caracterizan a las tecnologías mencionadas. Sin embargo, mediante esta comparativa se espera considerar a SD-WAN como alternativa para enlaces MPLS, el cual permitirá tener una mejor visión y selección de la tecnología aplicable a un proyecto de telecomunicaciones.

Antecedentes de la Investigación

Las primeras WAN públicas se implementaron a principios de la década de 1980 y experimentaron un desarrollo continuo. Inicialmente, las conexiones de área amplia se diseñaron para conectar dos sitios remotos mediante el uso de líneas arrendadas que tenían altos costos y velocidades limitadas.
Como resultado, se propusieron muchas tecnologías diferentes para mejorar las WAN en términos de costo y calidad, como el modo de transferencia asíncrono (ATM), Frame Relay (FR) y la conmutación de etiquetas multiprotocolo (MPLS). De estas tecnologías, MPLS es la que garantiza mayor calidad de eficiencia y calidad de servicio, pero a cambio de un alto costo (W.Cusco, J.Lugo, & J.Cabrera, 2022).

Asimismo, se debe considerar que no solo influye los costos, sino también el tiempo que lleva implementar estas tecnologías tradicionales, la complejidad en la gestión de las redes y el tiempo de transición/actualización.

SD-WAN cambia el paradigma de un sistema de enrutamiento de red basado en paquetes a un sistema de enrutamiento basado en aplicaciones. Esto permite a las organizaciones utilizar internet de banda ancha para consumirlo con calidad, rendimiento mejorado y a

un costo por megabyte más bajo que su predecesor MPLS.

La administración de una red WAN ha sido uno de los factores más costosos en una empresa, pero con el avance tecnológico dan lugar a las SD-WAN, diseñadas para satisfacer las necesidades comerciales, cuya solución ofrece ventajas sobre MPLS, ya que el tráfico actual que consiste en aplicaciones web avanzadas y flujos de trabajo complejos requiere opciones de conectividad más flexibles y dinámicas que las redes MPLS tradicionales no pueden proporcionar.

Según (IDC, 2019), la firma de inteligencia de mercado señala que SD-WAN "…ofrece un valor atractivo por su capacidad para sufragar los costos de MPLS, simplificar y automatizar las operaciones de WAN, mejorar la gestión del tráfico de aplicaciones y entregar dinámicamente los beneficios de costo y eficiencia asociados con la tecnología inteligente.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Formulación del problema

La emergencia sanitaria covid-19 generó una necesidad comercial de automatizar procesos y priorizar iniciativas de transformación digital, lo que implica el aumento constante en la demanda de conectividad WAN de mayor capacidad y calidad. En lugar de crear, actualizar y mantener sistemas y aplicaciones basados en inversiones mediante gastos de capital (CAPEX) en centros de datos locales, las organizaciones emplean cada vez más modelos de entrega en la nube, como infraestructura como servicio (IaaS) y software como servicio (SaaS) para crear nuevas oportunidades y pasar a un modelo de gasto por servicio o subscripciones (OPEX).

Para la conectividad WAN tradicional, la conmutación de etiquetas multiprotocolo (MPLS) ha sido un componente clave, que ofrece ancho de banda garantizado, privacidad y latencia predecible, sin embargo, es costoso y no es accesible geográficamente, dando lugar a las redes de área amplia definidas por software (SD-WAN) que cubren estas necesidades.

SD-WAN por su parte, es una implementación de red de nueva generación que forma parte del enfoque de redes definidas por software (SDN) donde la red es controlada por software y tiene como objetivo mejorar la seguridad y proporcionar un entorno de red más ágil y eficiente.

Este trabajo de investigación nace de la necesidad de estar a la vanguardia de aquellas tecnologías que se consolidan actualmente en el mercado global de las redes y telecomunicaciones, como es el caso de MPLS y SD-WAN.
Considerando que MPLS es una tecnología que data de varios años atrás, se propone la comparativa de estas dos tecnologías con la finalidad de determinar en qué aspectos una es superior que la otro.

1.2 Objetivos de la Investigación

1.2.1 Objetivo General

Realizar un estudio de comparación de tecnologías SD-WAN como alternativa para enlaces MPLS dedicados.

1.2.2 Objetivos Específicos

- Identificar los fundamentos teóricos necesarios para comparar tecnologías SD-WAN con la tecnología de enlaces MPLS dedicados.
- Analizar las soluciones de SDWAN existentes en el mercado ecuatoriano.
- Realizar un estudio comparativo de los beneficios, ventajas y desventajas que solucionan las SD-WAN.

1.3 Justificación de la Investigación

Con la evolución en las comunicaciones y conectividad corporativa en las redes privadas, las MPLS brindan seguridad de manera fiable y segura al momento de comunicarse con varias sedes corporativas, a pesar de ello, varias empresas pretenden adoptar nuevas soluciones tecnológicas en función a las necesidades actuales (mayor ancho de banda, calidad de servicio, agilidad, entre otros). En efecto surgen las SD-WAN con un enfoque moderno para gestionar la conectividad WAN, con mayor adopción de la nube que impulsa la transformación digital en las empresas para facilitar el acceso a aplicaciones en la nube de una manera segura y rentable.

El presente proyecto de investigación está basado en una investigación documental, la cual pretende demostrar la comparación de tecnologías MPLS y SD-WAN. En primer lugar, se definen conceptos relevantes, seguidamente se analizan las soluciones SD-WAN existentes en el Ecuador para finalmente realizar un estudio comparativo y analizar los parámetros como: funcionalidad, rendimiento, fiabilidad, seguridad, entre otros.

La comparación de las tecnologías es indispensable debido a que en la actualidad las empresas buscan gestionar una red WAN más inteligente y centralizada, cuyo aporte será de interés para profesionales y empleados que estén considerando implementar estas tecnologías.

El presente trabajo de investigación se ha dividido en varias secciones, en el capítulo I, se especificarán los hechos preliminares como: el planteamiento del problema, seguido de los objetivos general y específicos, y la justificación de la investigación, el cual definen las razones por lo que se desarrolla la comparación de tecnologías SD-WAN y MPLS.

En el capítulo II de fundamentación teórica, se examinará toda la materia teórica que abarca el proyecto de investigación como: conceptos generales, estructura, características que conforman cada tecnología MPLS y SD-WAN, toda esta información ayuda a comprender de mejor manera la fundamentación del proyecto.

En el capítulo III, se elaborará la metodología utilizada para el desarrollo del proyecto.
En el capítulo IV, presentación y análisis de datos, se presentarán los resultados finales obtenidos de la comparación de las dos tecnologías.
En el capítulo V, presentación de la propuesta, finalmente se determina un análisis de los resultados investigados. De la misma manera se realizarán conclusiones y recomendaciones importantes de las tecnologías analizadas.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1 CONMUTACIÓN DE ETIQUETAS MULTIPROCOLO (MPLS)

MPLS es una técnica de enrutamiento diseñada para transportar y enrutar el tráfico a través de redes corporativas y de proveedores de servicios de Internet (ISP). MPLS se desarrolló a fines de la década de 1990 como una alternativa eficaz a la conmutación IP y multicapa en el modo de transferencia asíncrono (ATM) (Y.Vanaubel, 2018). Una de sus principales ventajas es que puede aumentar la tasa de flujo del tráfico de la red, ya que los enrutadores pueden reenviar los paquetes recibidos mirando tablas de etiquetas que suelen ser significativamente más pequeñas que las tablas de enrutamiento tradicionales. En particular, un enrutador puede identificar la ruta completa que el paquete tendrá que recorrer y, por lo tanto, los siguientes saltos solo necesitan reenviar los paquetes recibidos al puerto correcto. MPLS, por lo tanto, reenvía paquetes en el nivel 2 de la pila ISO-OSI y, por esta razón, informalmente se indica que opera en el nivel intermedio o 2.5 de la pila ISO-OSI (S.Yadav, 2021).

2.1.1 Arquitectura MPLS

La red MPLS es una red conmutada que consta de múltiples enrutadores de conmutación de etiquetas (LSR), donde la ruta está predeterminada en función del origen y el destino. Estas rutas se denominan rutas conmutadas por etiquetas. Un enrutador de conmutación de etiquetas (LSR) es un componente fundamental de una red MPLS (S.Yadav, 2021).

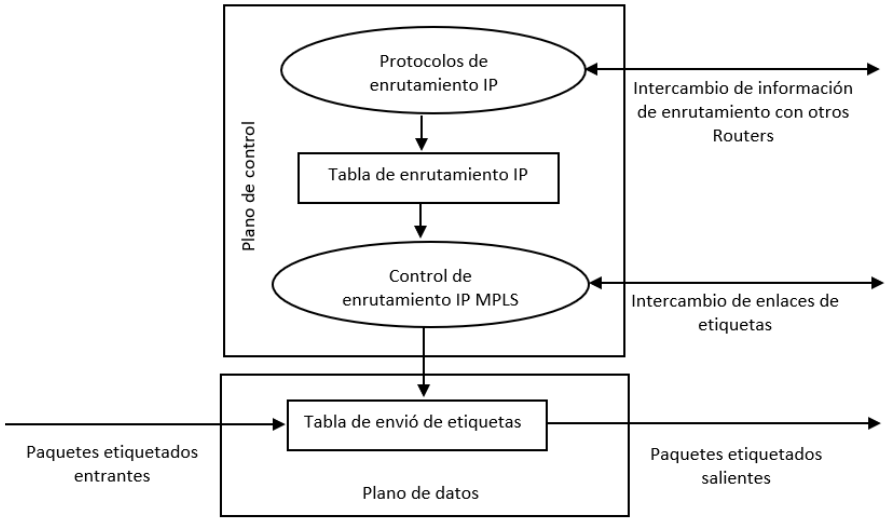


Figura 1: Arquitectura MPLS
Fuente: El autor

La arquitectura MPLS es la combinación de conmutación de Capa 2 y Capa 3 de las redes IP convencionales. Los pasos necesarios para que un paquete de datos viaje a través del dominio MPLS según lo indicado en la figura 1 son:

- Creación y distribución de etiquetas: la etiqueta debe crearse en función de la clase de equivalencia de reenvío (FEC) y debe distribuirse entre los enrutadores utilizando protocolos como LDP.

- Creación de tablas en cada enrutador: la base de información de reenvío de etiquetas (LFIB)debe completarse por completo en cada enrutador.
- Creación de ruta de conmutación de etiquetas (LSP): la ruta de conmutación de etiquetas debe establecerse antes de reenviar los paquetes.
- Inserción de etiquetas/búsqueda en tablas: cuando un paquete de datos llega al enrutador de entrada, según el FEC, se inserta una etiqueta y se indexa en el LFIB para su próximo salto.
- Reenvío de paquetes: el paquete se reenvía en cada enrutador intercambiando la etiqueta (Y.Vanaubel, 2018).

2.1.2 Componentes MPLS

En la figura 2 se puede visualizar los componentes característicos de MPLS: plano de control y de reenvío.

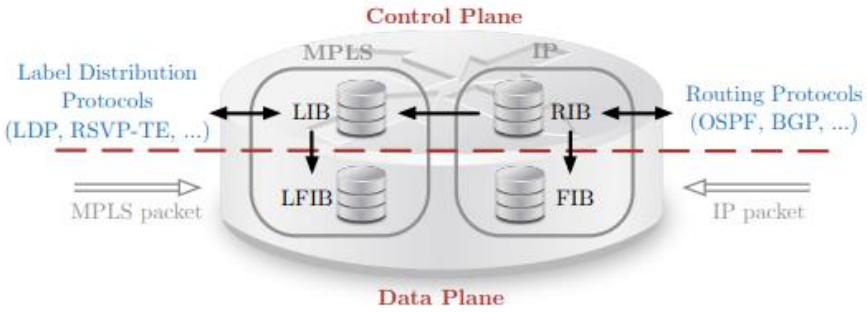


Figura 2: Plano de datos y control en un router MPLS.
Fuente: (Y.Vanaubel, 2018)

El plano de control es responsable de crear y mantener la información de enrutamiento y etiquetas (M.Karakus & A.Durresi, 2019).

El plano de datos o plano de reenvío está orientado a la conexión, lo que significa que sus conexiones pueden realizarse a través de una red de capa 2, como redes ATM y Ethernet. Este plano agrega o elimina etiquetas de paquetes IP y reenvía los paquetes recibidos basados en el LFIB (M.Karakus & A.Durresi, 2019).

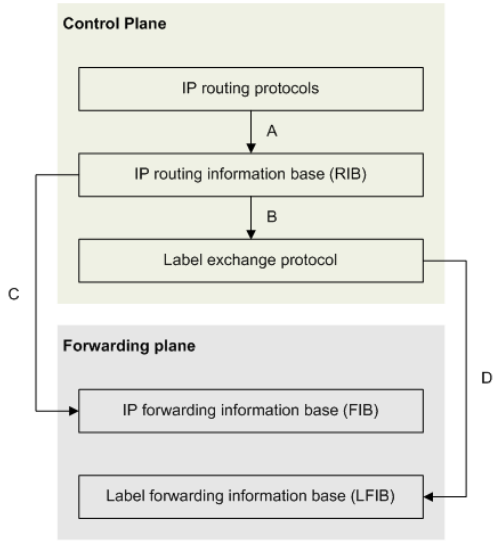


Figura 3: Flujo de trabajo de un sistema MPLS.
Fuente: (Huawei, 2022).

Según lo indicado en la figura 3, describe el flujo de trabajo de un sistema MPLS de la siguiente manera:

- A: Un protocolo de enrutamiento IP establece una relación de vecino, intercambia información de enrutamiento y genera la base de información de enrutamiento IP (RIB).
- B: Un protocolo de conmutación de etiquetas obtiene información de enrutamiento IP RIB. Un prefijo de ruta en la IP RIB se asigna a una clase de equivalencia de reenvío (FEC) y todos los paquetes transmitidos por la misma ruta pertenecen a una FEC.
- C: La ruta óptima activa en la IP RIB se utiliza para generar una entrada de reenvío en una base de información de reenvío IP (FIB).
- D: Un protocolo de conmutación de etiquetas establece una relación vecina, asigna una etiqueta a cada FEC y anuncia una etiqueta a un nodo ascendente. Además, obtiene una etiqueta de un nodo descendente y utiliza la información de la etiqueta para generar un LFIB (M.Karakus & A.Durresi, 2019).

2.1.3 Aplicaciones de MPLS

MPLS permite aplicaciones flexibles y escalables como son:

2.1.3.1 Ingeniería de tráfico (MPLS TE)

Se ocupa del rendimiento de una red para respaldar a los clientes de la red y sus necesidades de QoS (D.Țurcanu, 2020).
MPLS es estratégicamente importante para la ingeniería de tráfico porque tiene el potencial para proporcionar la mayor parte de la funcionalidad disponible de los modelos superpuestos como IP sobre ATM o IP sobre Frame Relay de manera integrada y también a un costo menor que las alternativas actuales de la competencia (M.Gales & V.Croitoru, 2020).

2.1.3.2 Calidad del Servicio (QoS)

MPLS se menciona con frecuencia entre las principales tecnologías de calidad de servicio (QoS) para redes de paquetes. MPLS no define una nueva arquitectura QoS, la mayor parte del trabajo en MPLS se centra en soportar las arquitecturas IP QoS (M.Gales & V.Croitoru, 2020).

Existen dos formas de llevar a cabo la QoS en una red IP como son:

Servicios integrados (Intserv), utiliza el protocolo de reserva de recursos (RSVP) para requerir recursos en toda la red y mantener un estado de reenvío para cada flujo de datos, lo que dificulta la extensibilidad. Por tanto, IntServ no prevalece en las redes, sin embargo, las normas pertinentes amplían RSVP al permitir que los mensajes RSVP PATH lleven solicitudes de etiquetas y RSVP mensajes RESV para admitir la asignación de etiquetas.
El RSVP extendido se conoce como protocolo de reserva de recursos ingeniería de tráfico (RSVP-TE) que permite que MPLS controle la ruta del tráfico y reserve recursos al configurar LSP para que el tráfico pueda pasar por alto los nodos (D.Țurcanu, 2020).

Servicios diferenciados (DiffServ), define una arquitectura QoS basada en agregados de flujo que requiere que el tráfico se acondicione y marque en los bordes de la red y nodos internos para dar un tratamiento diferente de QoS a los paquetes en función de sus marcas. Los paquetes MPLS deben llevar la marca del paquete en sus encabezados porque los LSR no examinan el encabezado IP durante el reenvío, para este propósito se utiliza un campo experimental de 3 bits en el encabezado shim de MPLS (Alemayehu, 2019).

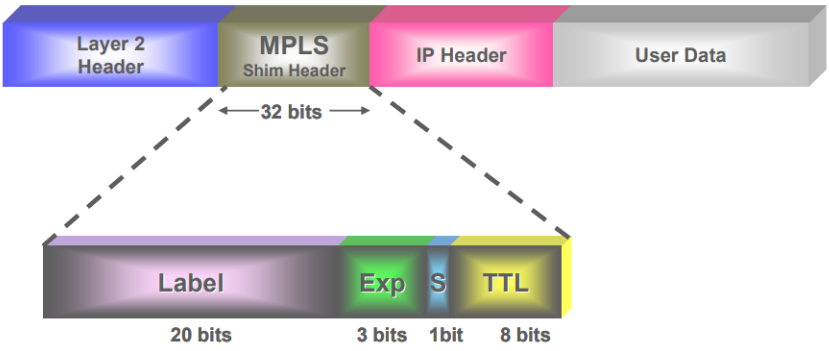


Figura 4: Encabezado SHIM en MPLS
Fuente: (Z.Hussain, P.Shah, & S.Abid, 2021).

El encabezado Shim según lo indicado en la Figura 4, reside entre la capa 2 y los encabezados de la capa IP. El encabezado de corrección de compatibilidad (etiqueta MPLS) es un valor de 32 bits que incluye una etiqueta utilizada para tomar decisiones de reenvío. El campo Exp tiene 3 bits reservados y se utiliza para identificar la clase de servicio. Si se establece en 1, el campo S indica que la etiqueta es la parte inferior de la pila de etiquetas y el campo TTL de 8 bits indica el tiempo de vida, es decir, el número de nodos por los que pasa el paquete de datos para llegar a su destino (Z.Hussain, P.Shah, & S.Abid, 2021).

2.1.3.3 Redes Privadas Virtuales (VPN)

Significa una red privada de múltiples sitios creada mediante el uso de recursos compartidos dentro de una red pública. Las VPN convencionales se basan en crear y mantener una malla completa de túneles o circuitos virtuales permanentes entre todos los sitios que pertenecen a una VPN en particular, utilizando IPSec, L2TP, L2F, GRE, Frame Relay o ATM (Zhipeng, y otros, 2018).
Las VPN basadas en MPLS, que se crean en la Capa 3, no tienen conexión y, por lo tanto, son sustancialmente más escalables, fáciles de construir y administrar que las VPN convencionales.
Los componentes de VPN son enrutadores de borde del cliente (CE) y de cliente (C), que se colocan en el extremo del cliente y enrutadores de borde del proveedor (PE) y del proveedor (P), que se colocan en el extremo del proveedor de servicios (A.Pica, G.Predusca, N.Angelescu, D.Circiumarescu, & D.Puchianu, 2022).

2.1.4 Protocolos

Se divide en dos categorías: protocolos de enrutamiento y protocolos de señalización.

Los protocolos de enrutamiento son responsables de la distribución de la información de enrutamiento entre los LSR. Los protocolos de enrutamiento son: OSPF, IS-IS, BGP.

Los protocolos de señalización son los encargados de la distribución de etiquetas entre los LSR, la información de vinculación de etiquetas se distribuye mediante los protocolos LDP o RSVP. Cabe decir que los protocolos OSPF, IS-IS, BGP también se pueden usar para distribuir la información de las etiquetas y ampliarlas (A.Pica, G.Predusca, N.Angelescu, D.Circiumarescu, & D.Puchianu, 2022).
Los protocolos de señalización son: LDP, RSVP, CR-LDP y RSVP-TE.

2.1.5 Funcionamiento

Se basa en seguir un paquete a través de una red de proveedor de servicios habilitada para MPLS.

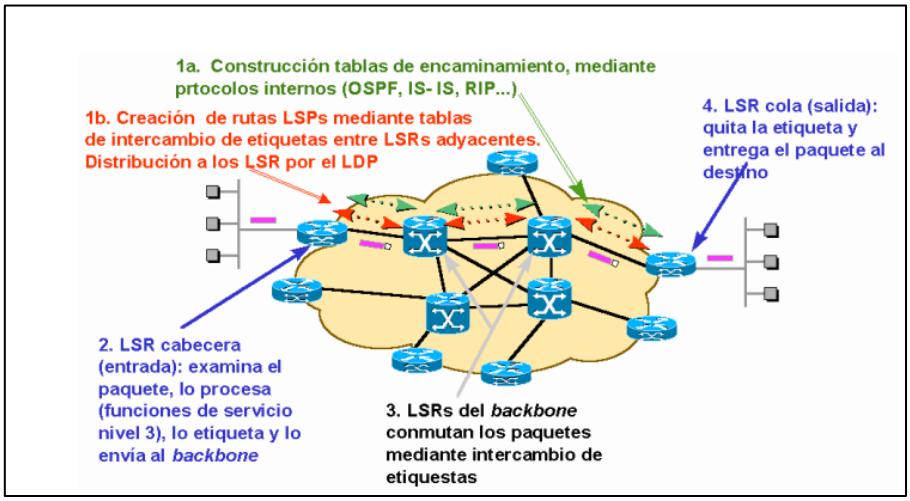


Figura 5: Funcionamiento MPLS
Fuente: (Stepanova & Nouma, 2022).

El funcionamiento de MPLS según lo indicado en la figura 5 es el siguiente:

- Paso 1: La red crea automáticamente tablas de enrutamiento a medida que los routers con capacidad MPLS participan en protocolos de pasarela interna (OSPF, IS-IS) en toda la red. El protocolo de distribución de etiquetas (LDP) crea asignaciones de etiquetas para las redes de destino y utiliza la topología de enrutamiento de las tablas para establecer valores de etiquetas entre los dispositivos adyacentes. Esta operación crea mapas preconfigurados de rutas de conmutación de etiquetas (LSP) entre los puntos finales de destino.
- Paso 2: Un paquete entra en el router de conmutación de etiquetas (LSR) del borde de entrada, donde se procesa para determinar qué servicio de capa 3 requiere, como, por ejemplo, calidad de servicio (QoS) y gestión del ancho de banda. El LSR de borde selecciona y aplica una etiqueta al encabezado del paquete y lo reenvía.
- Paso 3: El LSR lee la etiqueta de cada paquete, la reemplaza por la nueva que aparece en la tabla y reenvía el paquete.
- Paso 4: El router de borde de salida elimina la etiqueta, lee el encabezado del paquete y lo reenvía a su destino final (Aurel, Gabriel, Denisa, Nicoleta, & P.Constantin, 2022).

2.1.6 Beneficios

MPLS tuvo su origen en los años 90 gracias a las empresas Ipsilon y Toshiba, consideradas pioneras en este campo. Ipsilon lanzó al mercado el producto IP Switching, mientras que Toshiba presentó Cell Switch Route. Ambos enfoques eran similares, con la ventaja adicional de que IP Switching permitía que un conmutador ATM desempeñara la función de un enrutador (Aijaz & Idrees, 2020).

En respuesta a las oportunidades surgidas a partir de 1996, Cascade Communications, Cisco Systems e IBM presentaron sus propios productos, como IP Navigator, Tag Switching y Aggregate Route-Based IP Switching, respectivamente (Aijaz & Idrees, 2020). Estas compañías se propusieron abordar los desafíos existentes asociados a las redes IP convencionales y ofrecer soluciones innovadoras tales como:

- El enrutamiento IP presentaba dificultades tanto en las implementaciones de hardware como de software debido a las restricciones de velocidad de reenvío de paquetes en los routers IP.
- La congestión de la red se debía a que el proceso de enrutamiento IP estaba estrechamente ligado al reenvío de paquetes en los routers, lo que resultaba en una utilización desigual de las líneas principales, con algunas sobrecargadas y otras subutilizadas.
- Además, las redes IP se superponían a las redes ATM, lo cual implicaba costos significativos. Sin embargo, esta superposición tenía una ventaja importante: los paquetes IP podían ser direccionados a circuitos ATM específicos, evitando así el enrutamiento convencional. Esto permitía reducir la congestión mencionada anteriormente, en un proceso conocido como ingeniería de tráfico (Stanescu, y otros, 2022).

De la misma manera, el Grupo de Trabajo de Ingeniería de Internet (IETF) creó el Grupo de Trabajo MPLS a principios de 1997 para abordar inicialmente el desarrollo de MPLS

a profundidad y desarrollar un estándar común, mismo que fue publicado la norma inicial en 2001 (Stanescu, y otros, 2022).

MPLS permite a empresas y proveedores de servicios beneficios como son:

- Redes multiservicio, ayuda a las redes a transportar todo tipo de tráfico, por ejemplo, tráfico IP, voz sobre IP, tráfico de capa 2, etc. MPLS integra diferentes tecnologías tales como VPN de Capa 2, VPN de Capa 3, Ingeniería de Tráfico, QoS, GMPLS e IPv6, que permiten desarrollar redes escalables y seguras que garantizan los Acuerdos de Nivel de Servicio (SLA) (Ridwan & Zakaria, 2020).

- Red Privada Virtual MPLS (MPLS VPN), proporciona redes privadas y seguras sobre la misma topología de red a muchos clientes. También proporciona capacidad para dividir la red en redes más pequeñas y es escalable.

- Escalabilidad

- Ingeniería de tráfico, ayuda a utilizar la infraestructura de red de forma óptima, al distribuir el tráfico de manera más uniforme en todos los enlaces disponibles coste (Ridwan, y otros, 2020).

2.2 SDN

Uno de los enfoques revolucionarios del último período en el campo de las redes es el surgimiento considerado de las llamadas Redes Definidas por Software (Software Defined Network por sus siglas en inglés). SDN como concepto se enfoca a la solución de uno de los problemas de las redes actuales, este problema es de complejidad creciente en muchos aspectos (P.Segec, M.Moravcik, J.Uratmová, J.Papán, & O.Yeremenko, 2020).
La complejidad de las redes IP resulta de sus principios de diseño, construcción y administración como sistema distribuido de forma nativa (diversos dispositivos de integración, protocolos, políticas de administración, etc.), que se integra verticalmente en forma de plano de datos y control común e interconectado implementado en un sistema operativo (SO) específico del dispositivo de red, por ejemplo, Cisco IOS, Juniper JunOS, etc. (P.Segec, M.Moravcik, J.Uratmová, J.Papán, & O.Yeremenko, 2020).
SDN crea así un nuevo enfoque para el diseño y operación de infraestructura de red, donde el plano de control de red (lógica de control) está separado del nivel de datos (funciones de reenvío de dispositivos).
Las funciones de control en SDN se extraen de dispositivos individuales y se integran en un nodo de control centralizado, llamado controlador (lógica inteligente de SDN), o también Sistema Operativo de Red (NOS), este enfoque permite la abstracción del control de la infraestructura de la red física, a menudo representada como un conmutador virtual, y permite la programación central (automatización) del comportamiento de la red, políticas o servicios en un solo lugar (J.Correa, J.Cuatindioy, & J.Botero, 2020).

2.2.1 Arquitectura SDN

En la figura 6, se puede visualizar la arquitectura SDN dividido en tres capas: aplicación, control e infraestructura. A continuación, se detalla cada una de ellas.

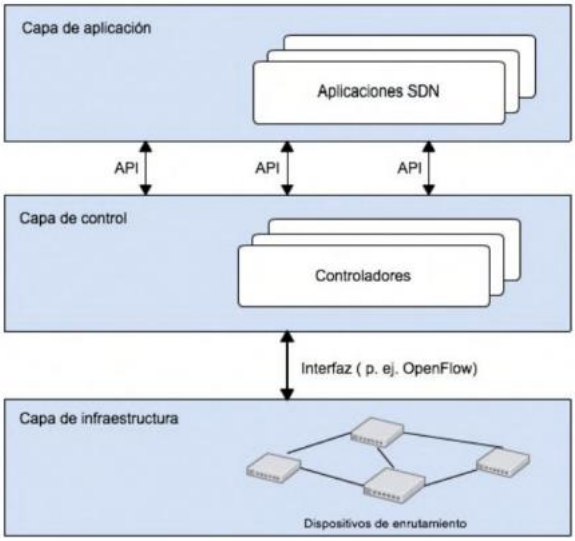


Figura 6: Arquitectura SDN.
Fuente: (D.Rodríguez, C.Talay, & C.González, 2020).

- Capa de aplicación, utiliza funciones y servicios brindados por el plano de control para crear la lógica de las aplicaciones de red SDN, que se traduce por el controlador en una configuración específica del dispositivo de red e instalado en el dispositivo de red.

- Capa de control / plano del controlador SDN, componente indispensable utilizado como entidad de software denominado controlador o (NOS), que combina el control y la gestión de funciones de red. NOS a través de API (interfaz de programación de aplicaciones) proporciona una abstracción de funciones de red y servicios de plano de datos, por ejemplo: red estado, información topológica, configuración y reconfiguración de dispositivos, gestión, etc.).

- Capa de infraestructura / plano de datos, consiste en dispositivos de red de hardware o software (elementos de reenvío de datos, como enrutadores, conmutadores, firewalls, etc.) similar a las redes IP (Protocolo de Internet) tradicionales, pero con funciones de control excluidas (P.Segec, M.Moravcik, J.Uratmová, J.Papán, & O.Yeremenko, 2020).

2.3 SD-WAN

Las técnicas antiguas para WAN sufrían múltiples limitaciones, ya que tienen una conexión limitada entre empresas, sucursales y centros de datos. Hoy en día, como TI, la industria está adoptando varios servicios de aplicaciones basados en la nube que utilizan modelos de servicio como SaaS (Software como servicio) e IaaS (Infraestructura como servicio).
La mayoría de estas empresas utilizan la arquitectura WAN, que es muy compleja, ya que utilizan hardware propio que es específico del proveedor, inflexible y muy costoso de comprar y, por lo tanto, la arquitectura WAN de estas tecnologías es muy compleja.
SD-WAN se basa en el principio básico de SDN, diseñado para administrar la WAN. SD-WAN brinda a los profesionales de TI la capacidad de enrutar, proteger contra amenazas y simplificar la gestión de redes WAN (E.Ali, M.Manel, & Y.Habib, 2017).

2.3.1 Arquitectura SD-WAN

Según (P.Segec, M.Moravcik, J.Uratmová, J.Papán, & O.Yeremenko, 2020), la arquitectura SD-WAN es similar a la arquitectura SDN, consta de tres planos arquitectónicos tales como: plano de datos, plano de control y plano de orquestación.

- Plano de datos, capaz de establecer conexiones a través de infraestructuras IP/WAN tanto privadas como públicas. Está diseñado para simplificar la comunicación entre sitios separados geográficamente, así como con aplicaciones y servicios en la nube.

- Plano de control, es responsable de optimizar el flujo de comunicación enviado a través del túnel VPN a cada uno de los diferentes tipos de servicios, como servicios de sucursales, servicios de centros de datos y servicios en la nube. La entidad principal es el controlador, que puede estar ubicado en una sucursal, sede, centro de datos o en la nube.

- Plano de orquestación, es el autenticador principal para todos los componentes SD-WAN, facilita el descubrimiento de los nuevos elementos en la red y notifica a los bordes de su IP pública en caso de que se utilice la traducción de direcciones de red (NAT), además proporciona un marco de política empresarial y aborda las políticas de seguridad del servicio y estrategias de gobierno corporativo (Gianlorenzo, 2021).

2.3.1.1 Tipos de arquitectura

La solución SD-WAN ha segmentado distintos tipos de arquitectura: local, nube y hibrida.
En primer lugar, SD-WAN local es el tipo más básico porque incluye solo conectividad de red completa entre todos los sectores comerciales, no necesita conexión de puerta de enlace en la nube, por lo que es apropiado para las empresas que alojan las aplicaciones internamente.
En segundo lugar, SD-WAN habilitada para nube es ideal para las empresas que desean optimizar el rendimiento e integración de las aplicaciones, debido a que están conectadas a un Gateway virtual.
Por último, SD-WAN hibrida permite una mayor flexibilidad, pero se vuelve más complejo en términos de configuración y seguridad que la solución anterior.

2.3.2 Funcionamiento

SD-WAN ofrece la capacidad de utilizar software para gestionar la conectividad, administración y servicios entre el centro de datos y las sucursales remotas o las instancias en la nube.
Por lo general, los flujos de datos entre dos sitios generalmente se enrutan a través del enlace que se considera más adecuado según las políticas aplicadas a ese flujo.
Todos los flujos a través de enlaces WAN normalmente atraviesan redes públicas sin precauciones especiales, se ingresan en un túnel VPN construido ad hoc entre la fuente y el destino, de esta forma, garantiza la confidencialidad y seguridad de los datos transmitidos (Gianlorenzo, 2021).

2.3.3 Beneficios de SD-WAN

- SDWAN utiliza tres planos: el plano de datos, que facilita la comunicación entre sitios, porque crea una infraestructura lógica que funciona sobre una infraestructura física y permite transferir datos de origen a destino de manera fluida; el plano de control que lleva a cabo el control de las configuraciones de los dispositivos conectados a la red, tales como políticas, información de enrutamiento, accesos (S.Badotra & S, 2020) y el plano de orquestación, que proporciona una política comercial y un marco de seguridad.
- Permite una configuración y gestión de conexiones entre sucursales de una empresa de manera simple, flexible, fácil de controlar y supervisar, lo que se traduce en menores costos operativos a mediano y largo plazo (C.Mena; L.Andrade; J.Utrilla; M.Cano, 2022).
- Permite administrar, controlar y configurar una red corporativa desde una plataforma web centralizada (C.Mena; L.Andrade; J.Utrilla; M.Cano, 2022).
- Gracias al aprovisionamiento sin contacto (ZTP)permite la reducción de tiempos de implementación.
- Es multi-transporte, permite distintas conexiones para el envío de datos.
- Proporciona interoperabilidad, lo que significa que puede funcionar y coexistir con la infraestructura de red existente.

2.3.4 Soluciones SD-WAN

Tomando en consideración el cuadrante mágico de Gartner que se encuentra en la figura 7, se analizarán las soluciones de dos proveedores que se han convertido en líderes y tienen un buen desempeño en el mercado ecuatoriano.



Figura 7: Cuadrante mágico de Gartner 2022.
Fuente: (Gartner, 2022).

2.3.4.1 Cisco Viptela SD-WAN

Esta solución de Cisco está destinada a grandes organizaciones con sedes en varios países, la solución separa los planos de orquestación, administración, control y datos en componentes discretos y unifica su funcionalidad bajo una sola estructura.
Cisco Viptela SD-WAN puede usar cualquier medio de transporte y transferir distintos tipos de servicio a través de tres áreas específicas que son, simplicidad, seguridad sobre multicapas y el método de optimización para la entrega de servicios.

La Figura 8, que muestra la arquitectura de una topología de Cisco Viptela SD-WAN, tiene como objetivo definir todos sus componentes, entre los que se encuentran Cisco vManage, Cisco vBond, Cisco vSmart y Cisco vEdge. Cada uno de ellos se describe a continuación.

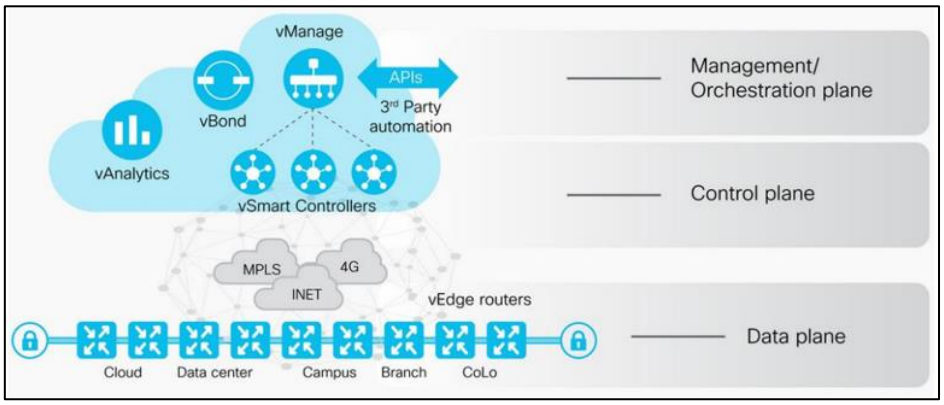


Figura 8: Arquitectura Cisco Viptela SD-WAN
Fuente: *(Cisco, 2023)*

- **Cisco vManage**

Corresponde al plano de administración/gestión, representa la interfaz API REST responsable de brindar una mejor visibilidad de sus operaciones, control sobre el mantenimiento e información sobre su estado.

- **Cisco vBond**

Corresponde al plano de orquestación y se encarga del proceso inicial de seguridad y Zero Touch. También es responsable de conectar los vEdge a la SD-WAN para intercambiar información y mantener la conexión.

- **Cisco vSmart**

Corresponde al plano de control y es responsable de centralizar la implementación de políticas, cuyas políticas se crean en vManage. Funciona con el protocolo OMP para la red overlay SD-WAN, por lo que la información de vManage se puede compartir con vEdge.

- **Cisco vEdge**

Corresponde al plano de datos y básicamente es el dispositivo que se coloca en el

centro de datos para efectuar la interconexión con el ISP y la red.

2.3.4.2 Fortinet SD-WAN

Este fabricante se enfoca en desarrollar y comercializar software, dispositivos y servicios de ciberseguridad, su solución SD-WAN se centra en entornos de red donde la seguridad es un componente principal, debido a que las conexiones se implementan como funciones integradas en el dispositivo NGFW, cada enlace se configura automáticamente con una VPN de red dinámica para proteger los datos que se transfieren.

La Figura 9, muestra la arquitectura de Fortinet SD-WAN, en donde no requiere una red MPLS para funcionar, pero usa para equilibrar el tráfico y enviar los paquetes más sensibles a la latencia a través del canal más apropiado.

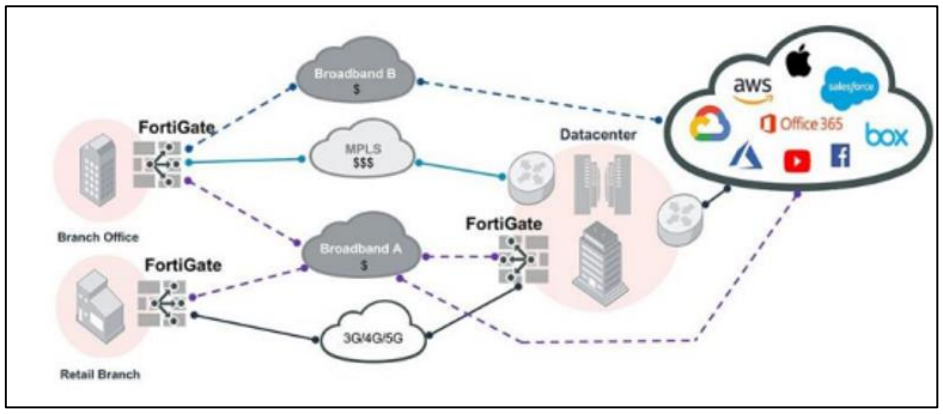


Figura 9: Arquitectura de Fortinet SD-WAN.
Fuente: (DatAustral, 2021).

Los componentes que caracterizan esta solución son: FortiManager, FortiAnalyzer y FortiGate.

- **FortiManager**

Se responsabiliza de la gestión y ajuste de diversos dispositivos de Fortinet, como FortiGate, FortiAnalyzer y FortiSwitch. Este dispositivo lleva a cabo la función de aprovisionamiento de configuración cero (ZTP). Asimismo, proporcionan herramientas mejoradas para la instalación y automatización, lo que posibilita una administración y supervisión efectiva de los dispositivos de red.

- **FortiAnalyzer**

Responsable del análisis y monitoreo de registros, así como la generación automatizada de reportes de eventos de seguridad, tráfico de red, contenido web, etc. Esta totalmente sincronizado con FortiManager, es decir, la funcionalidad de ambas se administra desde un solo dispositivo, disponible a través de hardware o modo virtual.

- **FortiGate**

Considerado como un sistema completo debido a que combina redes de seguridad que incluyen funciones como filtrado web, IPS, inspección SSL y SD-WAN, entre otras. Puede ser implementado tanto como hardware local o administrado, virtualizado o como

un servicio en la nube (SaaS).

CAPÍTULO III: METODOLOGÍA

3.1 Tipo de Investigación

El tipo de investigación se enmarca en un modelo tipo cualitativa, pues se justifica la comparación de dos tecnologías MPLS y SD-WAN de forma clara y concisa, lo cual exige un amplio estudio de conceptos que caracterizan a cada tecnología. De esta manera se logra tener una visión panorámica del tema de investigación.

3.2 Diseño de Investigación

Es de tipo descriptivo porque a través del estudio que este conlleva de manera teórica se analizan cada una de las tecnologías y se detalla las ventajas y desventajas que cada tecnología ofrece para así establecer una comparativa entre ellos.

3.3 Unidades de Estudio

En la investigación no se dispone de Unidades de Estudio (población y muestra) porque es un estudio comparativo, las cuales implican el análisis y la síntesis de similitudes, diferencias y patrones de dos o más casos que comparten un enfoque común, al analizar las tecnologías MPLS y SD-WAN.

3.4 Técnicas e instrumentos de recolección de datos

Al ser una investigación documental, se recopila datos teóricos que sustentan conceptualmente toda la información relacionada con la tecnología MPLS y SD-WAN. Así mismo se realiza una revisión de la literatura basada en las soluciones de SD-WAN existentes en el mercado ecuatoriano, para ello se toma en cuenta a dos fabricantes a estudiar Cisco y Fortinet.
Es importante mencionar las principales fuentes que se toma como sustento bibliográfico:

- Documentos oficiales de fabricantes tales como: Cisco, Fortinet, IBM.
- Prensa digital (artículos, conferencias, patentes) publicados en: IEEE, Scopus.com, Bibliotecas Ecuador (COBUEC), Scielo Ecuador, entre otros.
- Tesis magistrales y doctorales.

3.5 Técnica de Análisis de Datos

Se utiliza la técnica documental porque detalla información mediante el análisis y revisión de información científica de revistas, conferencias, tesis entre otros, relacionados con cada una de las tecnologías a estudiar.

CAPÍTULO IV: ANÁLISIS Y DISUSION DE RESULTADOS

4.1 Análisis General de la situación de las tecnologías MPLS y SD-WAN

Luego del realizar un análisis de los conceptos fundamentales entre las dos tecnologías MPLS y SD-WAN, se procede a plasmar las ventajas y desventajas de cada una de ellas, tal como se visualiza en la Tabla 1.

Tabla 1: Ventajas y desventajas SD-WAN y MPLS

	Ventajas	Desventajas
MPLS	-Confiabilidad/fiabilidad -Alto nivel de QoS -Garantiza la privacidad de datos	-Costo -Accesibilidad -Manejo complejo -Desafíos en la nube
SD-WAN	-Ahorro en costos -Rendimiento -Administración sencilla	-Errores -Disminuye la confiabilidad en la entrega de paquetes.

Fuente: El autor

En primera instancia se analizan las ventajas y desventajas de MPLS. Como ventaja principal es la entrega de paquetes de manera confiable con una alta QoS. Con MPLS el tráfico de mayor prioridad tiene la menor pérdida de paquetes y mantiene el flujo de tráfico más importante de una organización, necesario para mantener la calidad de los protocolos en tiempo real como VoIP.

Otro atributo valioso de MPLS, es que garantiza la privacidad de datos, debido a que está dedicado a una organización y está virtualmente aislado, por lo que proporciona un alto nivel de privacidad y una base de seguridad de hardware.

En cambio, una de las principales desventajas de MPLS, es el alto costo de implementación y mantenimiento, porque requieren de circuitos dedicados y líneas alquiladas.

De igual forma, es que son redes complejas de administrar, dado que requieren habilidades y experiencia para configurarlas y mantenerlas. Finalmente, MPLS fue diseñado exclusivamente para la conectividad punto a punto, por lo que no permite el acceso directo a aplicaciones en la nube y SaaS.

A continuación, se analizan las ventajas y desventajas de SD-WAN. Una de las principales ventajas incluye su capacidad para reducir el costo WAN, al ofrecer acceso directo a la nube y utilizar conexiones de menor precio como banda ancha y LTE.

Asimismo, SD-WAN permite aprovechar todas las conexiones de red disponibles a su máxima capacidad, lo que ayuda a evitar los costos asociados con la pérdida de productividad, al tiempo que facilita el mejor rendimiento de las aplicaciones críticas.

SD-WAN es más fácil de administrar, porque permite el control total de la WAN a través de una GUI simple, el cual proporciona una visión más holística de la red, incluida las estadísticas de red.

Finalmente es importante mencionar las desventajas de SD-WAN, uno de ellos son los errores, porque pueden experimentar fluctuaciones y pérdida de paquetes. Así mismo, se disminuye el nivel de confiabilidad en la entrega de paquetes con relación a MPLS, porque usa la internet pública como red de transporte.

4.2 SD-WAN vs MPLS

A continuación, se procede con un debate comparativo en base a parámetros importantes que caracterizan a cada tecnología.

- **Rendimiento y Priorización de aplicaciones**

MPLS ofrece un alto rendimiento y una calidad de servicio garantizada, porque utiliza una red privada dedicada y una configuración de enrutamiento manual. Sin embargo, la configuración manual es compleja y requiere una gestión de red dedicada.
SD-WAN por su parte, detecta y reconstruye paquetes perdidos en tránsito para garantizar que se mantenga o mejore el rendimiento. También permite una mejor configuración de protocolos para paquetes, lo que evita atascos de tráfico y otorga alta disponibilidad. Además, puede ofrecer un rendimiento superior en términos de costo, porque las conexiones de Internet públicas suelen ser menos costosas que las redes privadas dedicadas de MPLS.

- **Banda ancha**

MPLS provee un ancho de banda garantizado y estable, ideal para aplicaciones críticas que requieren de un alto nivel de disponibilidad y rendimiento. Sin embargo, tienen limitaciones relacionadas con la capacidad que se puede aprovisionar a través de la conexión de una sola vez.
SD-WAN no tiene problema de limitación de ancho de banda, porque usa una combinación de múltiples conexiones a Internet, mismo que se puede seguir agregando la capacidad según lo requieran varias conexiones, por tanto, proporciona equilibrio de carga granular entre ellas, e incluso conmutar por error a una nueva conexión si decrece el ancho de banda disponible.

- **Fiabilidad**

MPLS usa un enfoque orientado a la conexión que proporciona un canal virtual privado para cada VPN del cliente, lo cual suele garantizar una alta disponibilidad y una baja latencia. Estas redes privadas ofrecen una garantía de calidad de servicio (QoS) y una disponibilidad de red más confiables en comparación con SD-WAN basada Internet.
Aunque SD-WAN no puede ofrecer una garantía de calidad de servicio (QoS), tiene la capacidad de permitir la selección de rutas de forma dinámica. Esto implica que el

controlador de SD-WAN puede elegir la ruta más apropiada para el tráfico de aplicaciones específicas, mejorando el equilibrio de carga y asegurando que los paquetes de datos eviten la congestión.

- **Seguridad**

MPLS proporciona un alto nivel de seguridad debido a su arquitectura centralizada, es decir, los paquetes enviados a través de una conexión MPLS son privados y solo la conexión MPLS destinada puede verlo, esto significa que solo se permite la comunicación de sitio a sitio, lo que lo hace ideal para organizaciones que manejan información confidencial.
SD-WAN, por otro lado, mantiene su tráfico seguro mediante el cifrado de extremo a extremo a través de una VPN (una red privada virtual). El beneficio de usar esta tecnología es que puede integrar e implementar fácilmente capas de seguridad adicionales, como firewalls, para una administración unificada de amenazas.
En la siguiente tabla se hace un resumen comparativo de los parámetros más relevantes de las tecnologías SD-WAN y MPLS.

Tabla 2: Comparativa SD-WAN vs MPLS

Parámetros	SD-WAN	MPLS
Tecnología	Definida por software	Conmutación de etiquetas
Banda Ancha	El ancho de banda MPLS depende de la configuración. Limita la capacidad que se puede aprovisionar a través de cualquier enlace MPLS en cualquier momento.	Flexible en términos de ancho de banda al combinar múltiples conexiones y usar software para identificar y utilizar la conectividad más rápida.
Rendimiento	Cuenta con herramientas de seguimiento y control. Permite supervisar el estado del enlace y redirigir el tráfico directamente desde la plataforma.	Mayor garantía de rendimiento.
Fiabilidad	Maneja con múltiples enlaces. Usa enrutamiento de aplicaciones de forma prioritaria sobre la mejor conexión. Aplicaciones basadas en sesiones ininterrumpidas.	Garantiza la entrega confiable de paquetes. Usa la conmutación de error basado en BGP. VPN para conectarse a MPLS
Seguridad	Túnel seguro basado en	Direccionamiento privado de

	VPN (IPsec) y varias rutas activas múltiples aumentan la seguridad. Admite capas de seguridad adicionales. La mayoría del software SD-WAN incluye un firewall de estado incorporado.	paquetes. Un único proveedor de servicios.

Fuente: El autor

Es importante tener en cuenta que elegir entre SD-WAN y MPLS dependerá de las necesidades particulares de las organizaciones y de los servicios prestados por los proveedores.

4.3 Fabricantes de SD-WAN y sus soluciones

En este inciso, se establece una comparación de cada una de las características comunes entre los fabricantes estudiados anteriormente. El objetivo de este apartado es dar a conocer las principales soluciones tecnológicas que existen actualmente en el mercado.
Cisco SD-WAN es una solución que permite a las organizaciones simplificar la administración y la configuración de sus redes WAN. Ofrece una plataforma de administración centralizada que permite a los administradores de red gestionar fácilmente los enlaces WAN y los dispositivos de borde, y también proporciona una gestión de políticas granular y automatizada. Además, la solución de Cisco utiliza técnicas avanzadas de optimización de tráfico para mejorar la eficiencia y el rendimiento de la red.

Fortinet SD-WAN, por su parte, es una solución que adopta la seguridad y la conectividad en una sola plataforma. Ofrece una plataforma unificada de seguridad de borde que integra funciones de firewall, VPN, seguridad de aplicaciones y WAN. Fortinet SD-WAN también utiliza técnicas avanzadas de optimización de tráfico para mejorar el rendimiento de la red, y proporciona una plataforma de administración centralizada para una gestión fácil y eficiente de la red.

En la tabla 3, se establece una comparación de parámetros importantes entre los fabricantes mencionados.

Tabla 3: Comparativa Cisco vs Fortinet

Características	Cisco Viptela SD-WAN	Fortinet SD-WAN
Enfoque	Conectividad y administración de red	Seguridad y conectividad de red
Gestión Centralizada	Si	Si
Características de Seguridad	Básica	Avanzada
Plataforma unificada de seguridad	No	Si
Integración de servicios en la nube	Si	Si
Técnicas avanzadas de	Si	Si

optimización de trafico		
Escalabilidad	Escalable	Escalable
Interfaz de usuario	Fácil de usar, personalizable	Fácil de usar, personalizable
Compatibilidad con infraestructuras MPLS existentes	Si	Si
Compatibilidad con túneles Ipsec	Si	Si
Enlaces SD-WAN	Si	Si

Fuente: El autor

4.3.1 Enfoque

Cisco SD-WAN se centra en la conectividad y la administración de la red, mientras que Fortinet SD-WAN se centra en la seguridad y la conectividad de la red. Esto significa que, si la organización prioriza la seguridad, Fortinet puede ser una mejor opción. Por otro lado, si la organización prioriza la conectividad y la facilidad de gestión de la red, Cisco puede ser más adecuado.

4.3.2 Gestión centralizada

Ambas soluciones tienen una plataforma de administración centralizada, lo que facilita la gestión y el control de la red desde una única interfaz. Esto reduce el tiempo y el esfuerzo necesarios para configurar, monitorizar y mantener la red.

4.3.3 Características de seguridad

Cisco SD-WAN ofrece características de seguridad básicas, mientras que Fortinet SD-WAN ofrece características de seguridad avanzadas. Fortinet se destaca por su plataforma unificada de seguridad de borde, que integra funciones de firewall, VPN, seguridad de aplicaciones y WAN, el cual facilita una mayor protección contra las amenazas.

4.3.4 Plataforma unificada de seguridad

Fortinet SD-WAN ofrece una plataforma unificada de seguridad de borde que integra funciones de firewall, VPN, seguridad de aplicaciones y WAN en una sola plataforma. Esto simplifica la gestión de la seguridad de la red y proporciona una mayor protección contra las amenazas.

4.3.5 Integración de servicios en la nube

Ambas soluciones admiten la integración de servicios en la nube, lo que significa que las organizaciones pueden aprovechar las aplicaciones y los servicios basados en la nube de manera más eficiente.

4.3.6 Técnicas avanzadas de optimización de tráfico

Tanto Cisco como Fortinet SD-WAN utilizan técnicas avanzadas de optimización de

tráfico para mejorar el rendimiento de la red, lo que garantiza un mejor ancho de banda y una mayor velocidad en la transferencia de datos.

4.3.7 Escalabilidad

Ambas soluciones son escalables y pueden adaptarse a las necesidades cambiantes de la organización a medida que la red crece y evoluciona.

4.3.8 Interfaz de usuario

Tanto Cisco como Fortinet SD-WAN tienen una interfaz de usuario fácil de usar y personalizable que permite a los usuarios adaptar la plataforma a sus necesidades específicas.

4.3.9 Compatibilidad con infraestructuras MPLS existentes

Ambas soluciones son compatibles con infraestructuras MPLS existentes, lo que permite a las organizaciones aprovechar sus inversiones existentes en infraestructuras WAN.

4.3.10 Compatibilidad con túneles Ipsec

Tanto Cisco como Fortinet SD-WAN son compatibles con túneles IPsec, lo que significa que las organizaciones pueden utilizar cualquier enlace WAN, incluyendo conexiones a Internet, para crear una red privada segura.

4.3.11 Enlaces SD-WAN

Tanto Cisco como Fortinet SD-WAN permiten el uso de enlaces SD-WAN, lo que permite a las organizaciones utilizar múltiples proveedores de servicios WAN para lograr una mayor flexibilidad y redundancia en la red.

Ambas soluciones ofrecen características únicas que pueden ser beneficiosas para diferentes organizaciones. Por esta razón, se menciona dos casos exitosos de empresas ecuatorianas que adoptaron soluciones SD-WAN: Banco Pichincha y Uniandes.

Caso de éxito: SD-WAN Viptela en Banco Pichincha



Figura 10: Caso de éxito: SD-WAN Viptela en Banco Pichincha
Fuente: *(Cisco, 2022)*.

El Banco Pichincha implementó la solución de red definida por software (SD-WAN) de Cisco Viptela para mejorar la conectividad de sus sucursales, reducir los costos de su red y simplificar su gestión. La solución permitió al banco tener una red más segura, confiable y escalable, lo que mejoró la experiencia del cliente y la eficiencia operativa.

Antes de la implementación de SD-WAN, el Banco Pichincha experimentaba problemas de conectividad, lentitud y caídas en su red de sucursales, lo que afectaba negativamente a la experiencia del cliente. Además, la gestión de la red era costosa y compleja.

La solución de Cisco incluye características de seguridad integradas, como firewall y cifrado de datos, que ayudaron a proteger la red del banco contra amenazas cibernéticas. En resumen, la implementación de SD-WAN de Cisco permitió al Banco reducir los costos de infraestructura de red, mejorar la gestión y seguridad de la red y proporcionar una mejor experiencia de conectividad para sus empleados y clientes.

Caso de éxito: SD-WAN Fortinet UNIANDES



Figura 11: Caso de éxito: SD-WAN Fortinet UNIANDES
Fuente: *(Fortinet, 2022)*.

La Universidad de los Andes (Uniandes) implementó una solución SD-WAN de Fortinet para mejorar la conectividad entre sus campus y proporcionar una mejor experiencia de usuario para sus estudiantes, profesores y personal administrativo.

Antes de la implementación de SD-WAN, la universidad presentaba varios incidentes de seguridad que afectaban su operación y ponían en riesgo los datos de la institución, además no ofrecía el rendimiento que necesitaba para respaldar sus aplicaciones críticas, como los servicios de pagos en línea, así como también del portal institucional y la intranet.

Como resultado de la implementación de la solución SD-WAN de Fortinet, la Uniandes pudo mejorar el rendimiento, la capacidad de la red y proporcionar una mejor experiencia de conectividad para sus estudiantes, profesores y personal administrativo. Además de mejorar la seguridad de la red de la universidad al proporcionar una visibilidad y control más granular sobre el tráfico de red.

CAPITULO V: PRESENTACION DE LA PROPUESTA

5.1 SD-WAN como alternativa de solución

La investigación ha permitido determinar que SD-WAN puede resultar una alternativa de solución a MPLS, debido a los siguientes aspectos:

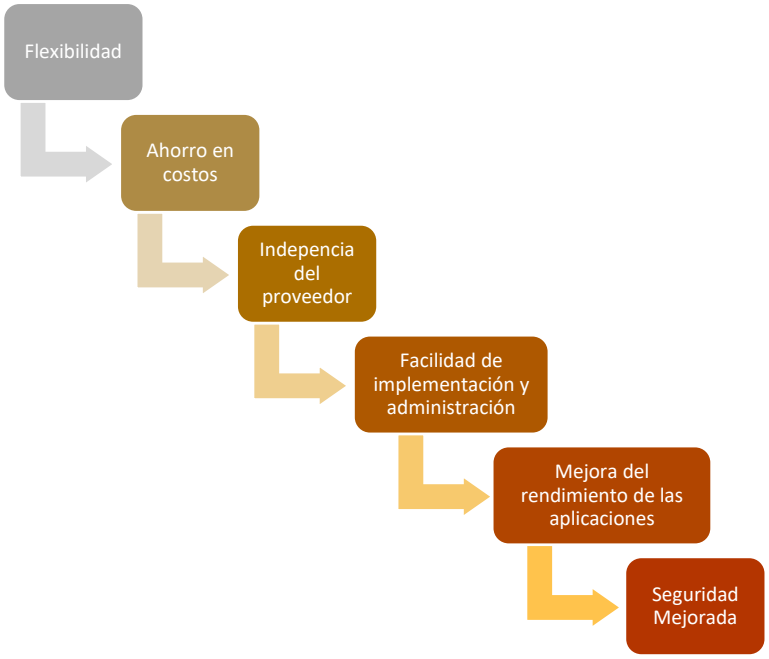


Figura 12: Aspectos SD-WAN
Fuente: El autor

Otros aspectos adicionales son:

- SD-WAN es una red de área amplia con una superposición virtualizada, que abstrae el software del hardware.
- Sus características clave incluyen abstracción de red, virtualización WAN, administración centralizada basada en políticas y administración de tráfico elástico.
- Su arquitectura puede estar basada en la nube, basada en la nube con una red troncal o solo en las instalaciones.
- Sus beneficios incluyen una administración simplificada, una mejor visibilidad de la red, un costo reducido y menos dependencia de proveedores.

En consecuencia, se puede decir que, la adopción de esta tecnología es particularmente atractiva en un contexto donde las organizaciones buscan reducir costos y adoptar nuevas aplicaciones y servicios para apoyar el trabajo remoto.

Por esto es necesario tener en cuenta las siguientes recomendaciones para la implementación de SD-WAN en organizaciones que utilizan enlaces MPLS dedicados, tal como se visualiza en la figura 13.

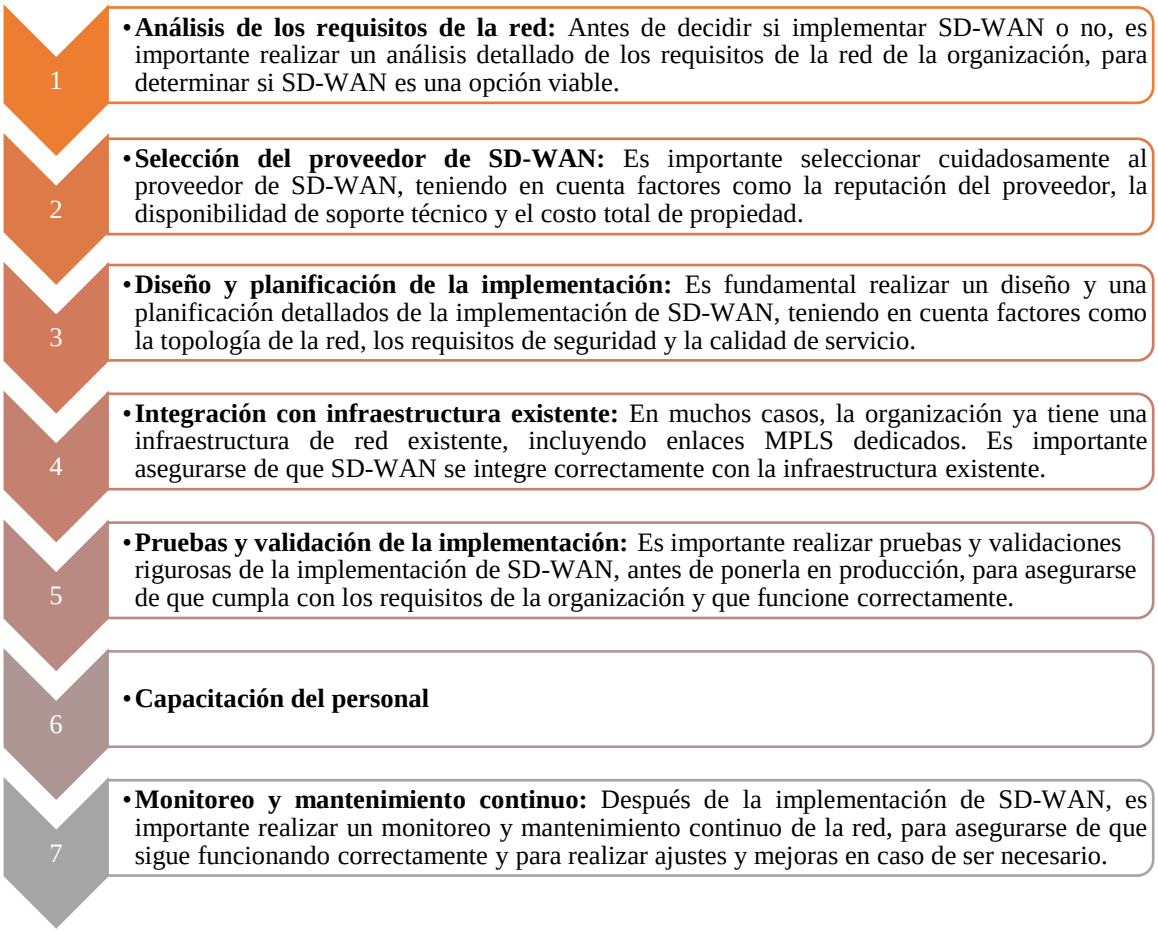


Figura 13: Recomendaciones para la implementación SD-WAN
Fuente: El autor

En definitiva, SD-WAN está cambiando fundamentalmente el panorama de la red, permitiendo que las organizaciones adopten modelos comerciales digitales y administren los crecientes volúmenes de datos y la cantidad cada vez mayor de dispositivos de usuario y la IoT que son fundamentales para sus estrategias comerciales.

No obstante, la elección de la tecnología dependerá de las necesidades específicas de la organización y sus aplicaciones empresariales.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Se concluye que MPLS es un circuito dedicado, mientras que SD-WAN se basa en una superposición de enlaces físicos aislados y virtualizados, lo que favorece en un principio a MPLS, debido a que ofrece una mayor protección contra la pérdida de paquetes. Sin embargo, las empresas tienen que asumir más costes por cada megabit transmitidos, no obstante, la naturaleza del overlay virtualizado que propone SD-WAN trae consigo mejor conectividad como MPLS, 4G LTE o Internet, lo que hace que la red sea más flexible.

- La comparación realizada entre ambas tecnologías permite diferenciar cada uno de los temas relevantes teniendo como antecedente el funcionamiento, arquitectura y componentes esenciales que caracterizan a las tecnologías mencionadas en el capítulo II referente al marco teórico, permitiendo tener una visión global sobre su importancia y beneficios que brindan. Así también en el capítulo IV se plasman aspectos importantes a comparar entre los cuales se pueden mencionar: rendimiento, seguridad, escalabilidad, fiabilidad, costo, etc., de tal manera que este conocimiento previo contribuye en gran medida a que la academia conozca exactamente cada uno de ellos y lo importante que es este tema en la actualidad.

- El estudio llevado a cabo en esta investigación ha permitido concluir que SD-WAN proporciona una excelente oportunidad para que las empresas optimicen costos (tanto de operación como de capital), al mismo tiempo que obtienen un mayor control y experiencia mejorada para los usuarios y las aplicaciones. Esto se debe a la flexibilidad inherente de SD-WAN, su facilidad de implementación y administración, así como a su capacidad para mejorar el rendimiento de las aplicaciones a través de técnicas como el enrutamiento inteligente y la optimización del tráfico, de tal manera que SD-WAN se posiciona como una solución tecnológica beneficiosa para las organizaciones, porque brinda ventajas económicas y un mayor nivel de control y rendimiento en la gestión de redes.

- Tras analizar algunos parámetros entre las tecnologías MPLS y SD-WAN, se concluye que las conexiones MPLS ofrece un alto nivel de seguridad debido a la transferencia y administración de datos por un solo operador. Sin embargo, esta ventaja de seguridad se acompaña de algunas limitaciones. Los costos de implementación y mantenimiento de una red MPLS suelen ser altos, lo que puede ser prohibitivo para algunas organizaciones, especialmente aquellas con presupuestos limitados. Por otro lado, SD-WAN ofrece la posibilidad de implementar capas adicionales de seguridad, como firewalls, en diferentes puntos de la red. Esto permite una gestión unificada de amenazas y una mayor protección contra ataques y brechas de seguridad. Al mismo tiempo, la implementación de estas capas adicionales de seguridad puede ser más rápida y sencilla en comparación con MPLS.

- Durante el análisis del funcionamiento de SD-WAN de Cisco y Fortinet, se identificaron y confirmaron las ventajas que fomentan la adopción de SD-WAN. Algunos de estos aspectos son: control centralizado, escalabilidad, integración de

servicios en la nube, seguridad, entre otros, mismas que fueron validadas en las soluciones de ambos fabricantes, lo que lleva a la conclusión de que ambas opciones son adecuadas para su implementación según las necesidades de cada organización destacados en esta área, tal como se visualiza en el presente trabajo de investigación.

- Al comparar a los fabricantes Cisco y Fortinet, no se observan diferencias significativas, de hecho, ambas opciones son adecuadas. Sin embargo, este estudio destaca que Fortinet ofrece ventajas en términos de seguridad al proporcionar una plataforma unificada de seguridad de borde (firewall, VPN, seguridad de aplicaciones y WAN en una sola plataforma), esta integración de funciones simplifica la gestión de la seguridad de la red y brinda una mayor protección contra amenazas.

- Como resultado de este trabajo de investigación, se concluye que la tecnología SD-WAN ha demostrado numerosos beneficios en Ecuador, lo que ha llevado a proveedores como Cisco y Fortinet a ofrecer soluciones tecnológicas. Los casos de éxito del Banco Pichincha y Uniandes respaldan la efectividad de SD-WAN en mejorar la organización, cuya adopción representa una valiosa oportunidad para que las empresas ecuatorianas puedan optimizar sus operaciones y mantenerse a la vanguardia tecnológica.

- Finalmente, este trabajo de investigación concluye que SD-WAN ofrece una alternativa viable a MPLS en términos de soluciones de red. SD-WAN proporciona una mayor flexibilidad y escalabilidad, lo que permite a las organizaciones adaptarse rápidamente a las demandas cambiantes de la red. Además, SD-WAN ofrece beneficios significativos, como una administración simplificada y una mejor visibilidad de la red, opción atractiva para las organizaciones que buscan mejorar su infraestructura de red y optimizar sus recursos.

6.2 RECOMENDACIONES

- Se recomienda examinar los desafíos y las mejores prácticas para conectar redes SD-WAN a proveedores de servicios en la nube como AWS, Azure o Google Cloud, considerando aspectos como la conectividad directa, la optimización del tráfico hacia la nube, la gestión de políticas de seguridad y la visibilidad del rendimiento de las aplicaciones en la nube.

- Con la creciente adopción de tecnologías emergentes como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el edge computing, se espera que SD-WAN desempeñe un papel importante en la gestión y optimización de las redes distribuidas. Se recomienda explorar cómo SD-WAN puede integrarse con estas tecnologías para mejorar la eficiencia, seguridad y rendimiento de las redes empresariales del futuro. Esta investigación resultará beneficiosa tanto para los estudiantes como para aquellos que se están formando profesionalmente en el campo de las redes, ya que les permitirá estar preparados para los desafíos y oportunidades que presentan estas tecnologías emergentes.

- Se recomienda ampliar el estudio a fabricantes adicionales como VMware o Palo Alto Networks, para obtener una visión más completa del campo de SD-WAN. Analizar el funcionamiento de sus soluciones y compararlas con los fabricantes mencionados en este proyecto de investigación permitirá obtener una comprensión actualizada de las diferentes opciones de SD-WAN disponibles en el mercado. Esta ampliación del estudio brindará una perspectiva enriquecedora sobre las soluciones de SD-WAN, lo que la convierte en un campo de estudio esencial para los futuros ingenieros dedicados al área de redes e infraestructura.

REFERENCIAS

A.Pica, G.Predusca, N.Angelescu, D.Circiumarescu, D., & D.Puchianu. (2022). Analysis of MPLS Technology in the Case of Virtual Networks. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1-6. doi: 10.1109/ECAI54874.2022.9847502

Aijaz, I., & Idrees, S. (2020). Performance Evaluation of Multi-protocol Label Switching-Traffic EngineeringSchemes. *EAI Endorsed Transactions on Mobile Communications and Applications, 6*(19), 1-12. doi:10.4108/eai.8-10-2020.166550

Alemayehu, A. (2019). Analyzing Impact of Segment Routing MPLS on QoS. *Masters of Science in Telecommunication Engineering.* Addis Ababa University.

Aurel, P., Gabriel, P., Denisa, C., Nicoleta, A., & P.Constantin. (2022). Analysis of file transfer traffic using MPLS technology. *2022 26th International Conference on System Theory, Control and Computing (ICSTCC)*, (págs. 52-57). Sinaia, Romania. doi:10.1109/ICSTCC55426.2022.9931894

Bannour, F., Souihi, S., & A.Mellouk. (2018). Distributed SDN Control: Survey, Taxonomy, and Challenges. *IEEE Communications Surveys & Tutorials, 2*(1), 333-354. doi:10.1109/COMST.2017.2782482

C.Mena; L.Andrade; J.Utrilla; M.Cano. (2022). Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity. *(IJACSA) International Journal of Advanced Computer Science and Applications, 13*(1), 757-767.

Cisco. (2022). *Cisco.com.* Obtenido de https://www.cisco.com/c/es_mx/about/case-studies-customer-success-stories/pichincha.html

Cisco. (2022). *www.cisco.com.* Obtenido de https://www.cisco.com/c/es_mx/about/case-studies-customer-success-stories/pichincha.html

Cisco. (2023). *cisco.com*. Obtenido de https://www.cisco.com/c/en_uk/solutions/enterprise-networks/sd-wan/index.html?dtid=pseggl000183&oid=0&ccid=cc001404#~architecture

D.Rodríguez, C.Talay, & C.González. (2020). Explorando las redes definidas por software (SDN). *XXII Workshop de Investigadores en Ciencias de la Computación*, (págs. 100-104).

D.Țurcanu. (2020). Quality of services in MPLS networks. *Journal of Engineering Sciences, 27*(3), 102-110. doi:https://doi.org/10.5281/zenodo.3949674

DatAustral. (11 de Junio de 2021). Obtenido de https://dataustral.com/2021/06/11/sd-wan-de-fortinet/

E.Ali, M.Manel, & Y.Habib. (2017). An Efficient MPLS-Based Source Routing Scheme in Software-Defined Wide Area Networks (SD-WAN). *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, (págs. 1205-1211). doi:10.1109/AICCSA.2017.165

Fortinet. (29 de Abril de 2021). *www.fortinet.com.* Obtenido de : https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-uniandes.pdf

Fortinet. (2022). *Fortinet.com.* Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-uniandes.pdf

Gartner. (12 de Septiembre de 2022). Obtenido de https://www.gartner.com/en/documents/4018621

Gianlorenzo, M. (2021). Performance Analysis of an SD-WAN Infrastructure Implemented Using Cisco System Technologies. *(Tesis de Master).* KTH, School of Electrical Engineering and Computer Science (EECS).

Huawei. (2022). *Huawei*. Obtenido de https://support.huawei.com/enterprise/es/doc/EDOC1100118961

IDC. (Noviembre de 2019). *www.idclatin.com.* (S. &. Enrique Phun, Ed.) Obtenido de https://www.idclatin.com/imp/AssetsExamplesIMP/ExecutiveBrief.pdf

J.Correa, J.Cuatindioy, & J.Botero. (2020). Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications, 159*(1).

doi:https://doi.org/10.1016/j.jnca.2020.102595
M.Gales, & V.Croitoru. (2020). Traffic Engineering and QoS in a Proposed MPLS-VPN., (págs. 1-4). doi:10.1109/ISETC50328.2020.9301135.
M.Karakus, & A.Durresi. (2019). An economic framework for analysis of network architectures: SDN and MPLS cases. *Journal of Network and Computer Application, 136*, 132-146. doi:10.1016/j.jnca.2019.02.032
P.Segec, M.Moravcik, J.Uratmová, J.Papán, & O.Yeremenko. (2020). SD-WAN - architecture, functions and benefits. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, (págs. 593-599). doi:10.1109/ICETA51985.2020.9379257.
R.Alaoui, S.Traore, T.Camara, I.Zahraoui, & A.Bahnasse. (2020). Toward a new SDN based approach for smart management and routing of VPN-MPLS networks. *Solid State Technology, 63*, 1593-1601.
Rajagopalan, S. (2021). A Study on MPLS Vs SD-WAN. En S. Rajagopalan, *Lecture Notes on Data Engineering and Communications Technologies* (págs. 297-299). Springer, Singapur. doi:https://doi.org/10.1007/978-981-16-0965-7_25
Ridwan, M. R., & Zakaria, M. (Junio de 2020). Recent trends in MPLS networks: technologies, applications and challenges. *IET Communications, 14*(2), 177-185. doi:https://doi.org/10.1049/iet-com.2018.6129
Ridwan, M., Radzi, N., Ahmad, W. S., Abdullah, F., Jamaludin, M., & Zakaria, M. (2020). Recent trends in MPLS networks: technologies, applications and challenges. *IET Communications, 14*(2), 177-185. Obtenido de https://doi.org/10.1049/iet-com.2018.6129
S.Badotra, & S, P. (2020). A Survey on Software Defined Wide Area Network. *International Journal of Applied Science and Engineering, 17*(1), 59-73. Obtenido de https://gigvvy.com/journals/ijase/articles/ijase-202003-17-1-059.pdf
S.Troia, L.Moreira, A.Maralit, & G.Maier. (2020). SD-WAN: An Open-Source Implementation for Enterprise Networking Services. *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, (págs. 1-4). doi:10.1109/ICTON51198.2020.9203058.
S.Yadav. (2021). SD-WAN Service Analysis, Solution, and its Applications. *(Master of Science in Internetworking)* . University of Alberta.
Stanescu, C., Predusca, G., Circiumarescu, D., Angelescu, N., Puchianu, D., & Dumitrache, C. (2022). Analysis of web traffic using MPLS technology. *2022 International Symposium on Electronics and Telecommunications (ISETC)* (págs. 1-4). Timisoara, Romania: IEEE. doi:10.1109/ISETC56213.2022.10009987
Stepanova, I., & Nouma, K. (2022). Analysis of the capabilities of MPLS technology for managing traffic in communication networks. *Communications, 16*(5), 63-68. doi:10.36724/2072-8735-2022-16-5-63-68
W.Cusco, J.Lugo, & J.Cabrera. (2022). Análisis de las tecnologías SD-WAN usadas en Ecuador. *Dominio de las Ciencias, 8*(2), 870-886.
Y.Vanaubel. (2018). Revealing and Characterizing MPLS. *Doctor in applied Sciencie.* University of Liege-Belguim. Obtenido de https://orbi.uliege.be/handle/2268/228532
Z.Hussain, P.Shah, & S.Abid. (2021). A Seamless Handoff Scheme for Mobility Management in MPLS based Wireless Network. *2021 International Conference on Innovative Computing (ICIC)*, (págs. 1-8). doi: 10.1109/ICIC53490.2021.9693015.
Z.Yang, Y.Cui, B.Li, Y.Liu, & Y.Xu. (2019). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, (págs. 1-9). doi:doi: 10.1109 / ICCCN.2019.8847124
Zhipeng, Z., Chandel, S., Jingyao, S., Shilin, Y., Yunnan, Y., & Jingji, Z. (2018). VPN: a Boon or Trap? : A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks. *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, (págs. 510-515). doi:10.1109/ICCMC.2018.8487653

ANEXOS


Case study
Cisco public
cisco
The bridge to possible
Banco Pichincha:
La Confianza de una Red SD-WAN
Resumen del cliente
Nombre del cliente
Banco Pichincha
Industria
Finanzas
Ubicación
Ecuador

Banco Pichincha es el grupo financiero más importante del Ecuador. Desde su fundación en el año 1906, sus valores de progreso e innovación lo han posicionado como líder en el país, permitiéndoles expandir sus operaciones internacionalmente. Con presencia en Perú, Colombia, Panamá y España, Banco Pichincha se ha convertido en sinónimo de solidez y confianza financiera para todos los ecuatorianos.

Hoy, su operación se mantiene a la vanguardia ofreciendo soluciones innovadoras para sus clientes, trabajando por el desarrollo de la economía nacional. Su excelente gestión ha sido merecedora de reconocimientos internacionales, posicionándose entre los 25 mejores bancos de América Latina en 2011 y reconocido como 'Empresa Ejemplar' por el Centro Mexicano para la Filantropía y Forum Empresa en 2013.

Cisco SD-WAN, el inicio de la transformación

Con el objetivo de ofrecer mejores servicios a sus clientes, el equipo de TI Banco Pichincha inició un proceso de transformación digital, dando el primer paso hacia una infraestructura SD-WAN. Para esto, trabajó junto al partner local TEUNO y el equipo de Cisco Ecuador, diseñando un modelo de red moderno, que pueda reemplazar la infraestructura tradicional de red WAN con la que operaba el banco. En 2019, a través de un Enterprise Agreement, Banco Pichincha comenzó el proceso de implementación, convirtiéndose en un early adopter de este tipo de tecnología en el país.

Desafíos de la implementación

- Actualizar una infraestructura de red WAN migrando todos los servicios hacia la tecnología SD-WAN.
- Integrar la solución con plataformas externas, críticas para la operación del banco.
- Capacitar al equipo de TI del banco frente a esta nueva tecnología.

"Uno de los principales retos de esta implementación, ha sido la rápida adopción respecto a la curva de aprendizaje necesaria que el equipo de trabajo requería. Y cambiar una mentalidad de gestión de red tradicional, interiorizar esta nueva tecnología y aprovecharla al máximo"

Paul Torres
Arquitecto de TI
Banco Pichincha

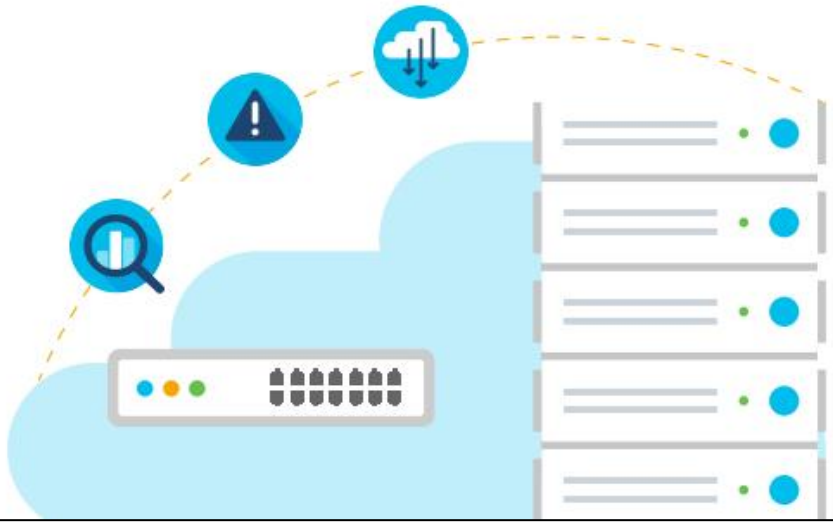
Beneficios obtenidos

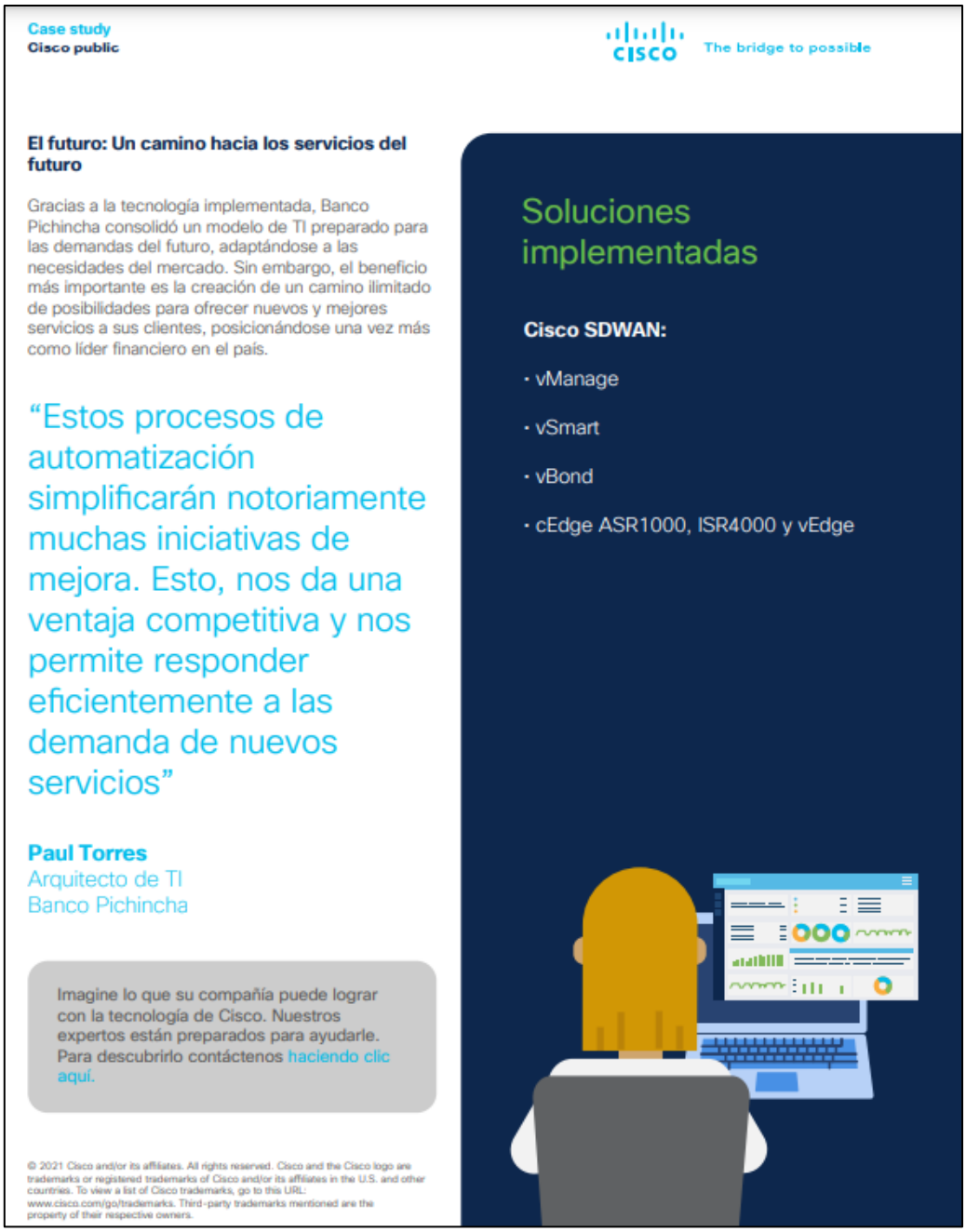
- El despliegue de esta nueva infraestructura de red mejoró positivamente la operación del banco, pero, sobre todo, abrió la puerta a un sin número de posibilidades para el futuro. Entre los beneficios más destacados se encuentran:
- Reducción de costos en un 35%, al reemplazar uno de sus enlaces MPLS por internet.
- Facilidad de gestión, con un dashboard inteligente que simplifica el trabajo del equipo de TI, tanto para tareas de soporte como en para nuevas implementaciones.
- Las características de Cisco Viptela, les permiten obtener una segmentación de red inteligente, priorizando el tráfico según las necesidades de cada aplicación o servicio del banco.

- Escalabilidad y facilidad de expansión, minimizando el costo de despliegue en nuevas sedes, gracias a la tecnología tipo "Plug & Play" de la solución.
- Facilidad de integración con aplicaciones como Salesforce, críticas para la operación diaria del banco.
- Las propiedades de seguridad de Cisco SD-WAN brindan capacidades de: Firewall, IPS, Filtrado URL, protección de malware, segmentación y seguridad de firmware.
- Mejor velocidad de conexión en más de 260 sedes.
- Facilidad de integración con plataformas de nube, tanto locales como internacionales.

"Gracias a la tecnología de SD-WAN, pasamos de tener una topología complicada que requería muchos conocimientos de red, a manejar una interfaz sencilla, automática y gráfica; simplificando notoriamente el trabajo de nuestro equipo"

Paul Torres
Arquitecto de TI
Banco Pichincha





Fuente: (Cisco, 2022).

FORTINET

CASO DE ESTUDIO

Universidad ecuatoriana conecta de forma segura sus sedes y optimiza su red con Fortinet Secure SD-WAN



La Universidad Regional Autónoma de los Andes (UNIANDES) es una institución de educación superior líder en Ecuador que cuenta con 7 sedes distribuidas en todo el país. La entidad nació en 1997 en la céntrica ciudad de Ambato y ha crecido de forma positiva durante este tiempo para llegar a contar hoy con cerca de 12.000 estudiantes de pregrado y posgrado, así como unos 1.200 empleados entre docentes y personal administrativo.

En una reciente evaluación, UNIANDES se ubicó entre las 10 mejores universidades del país. Como parte de su plan de expansión, la entidad está próxima a recibir la aprobación de las autoridades educativas para poder abrir operación en las ciudades de Quito, Guayaquil y Cuenca, unas de las principales de Ecuador.

Este crecimiento acelerado ha puesto de manifiesto la necesidad de implementar tecnologías que permitan asegurar la información que circula en las redes de la universidad. UNIANDES, hasta hace 5 años, tenía una protección en seguridad informática casi nula, por lo que se presentaban varios incidentes de seguridad que afectaban su operación y ponían en riesgo los datos. Los primeros pasos llevaron a la institución a equipar su sede principal con un firewall. Sin embargo, vio pronto la necesidad de ampliar esta protección para cuidar las transacciones realizadas con entidades bancarias, así como para brindar un servicio seguro de conectividad para toda la comunidad universitaria.

Comunicación segura para múltiples sedes

Un reto esencial de UNIANDES fue darles seguridad a sus 7 sedes remotas, pues no tenían protección y se exponía a un ataque en la sede principal a través de ellas. De hecho, en varias de ellas experimentaban ataques, al igual que afectaciones por virus y malware. Además, la universidad tenía la necesidad de asegurar su red de comunicaciones para proteger el sistema de pagos en línea.

La institución analizó varias soluciones del mercado y escogió a Fortinet por la funcionalidad de sus productos, el costo y su visión holística de la seguridad. "Fortinet nos ofrecía tres veces mejores prestaciones que las demás marcas del mercado. Además, con el mismo presupuesto pudimos instalar equipos más avanzados y que ofrecen una arquitectura completa de seguridad para la universidad", comenta Víctor Manuel Proaño, Administrador de Red de UNIANDES.

UNIANDES tenía un data center en su sede principal de Ambato. Desde allí se conectaba con las demás sedes a través de un enlace de datos dedicado y de una red privada virtual (VPN, por sus siglas en inglés) contratada con otro

UNIVERSIDAD UNIANDES

"Fortinet nos ofrecía tres veces mejores prestaciones que las demás marcas del mercado. Además, con el mismo presupuesto pudimos instalar equipos más avanzados y que nos ofrecen una arquitectura completa de seguridad".

– Victor Manuel Proaño, Administrator de Red, UNIANDES

Detalles

Cliente: Universidad Regional Autónoma de los Andes (UNIANDES)

Industria: Educación

Ubicación: Ecuador

Business impact

- Gestión y analítica centralizada de red
- Optimización de recurso humano y tiempo para la gestión de seguridad
- Mayor aprovechamiento de las capacidades de red al priorizar el uso de recursos

proveedor. Esta infraestructura de red necesitaba mejoras, pues el proveedor del enlace dedicado bajó su nivel de servicio en los años recientes y eso afectaba la conectividad de la institución.

A través de la solución Fortinet Secure Software-Defined Wide-Area Networking (SD-WAN) soportada en cada sede con un firewall FortiGate de próxima generación (NGFW, por su sigla en inglés), la entidad solucionó el inconveniente. De manera automática, el sistema escoge el enlace que funciona y garantiza la conectividad permanente de la red. Además, el tráfico a la red de la entidad ingresa únicamente por la oficina principal ubicada en Ambato; luego, de manera transparente y segura para los usuarios, se distribuye a las demás locaciones.

Por los buenos resultados y gracias a la confianza en Fortinet, la Universidad está evaluando la posibilidad de prescindir del canal dedicado de datos y así obtener un ahorro en costos al integrar una solución segura de SD-Branch con FortiSwitch.

Gestión optimizada y rápida de la red

El manejo centralizado de la red de UNIANDES es uno de los beneficios más importantes logrados con la solución Fortinet, resalta Proaño. En la actualidad, la gestión de seguridad la realiza desde un solo punto por medio de la herramienta FortiManager. Desde allí se generan políticas de seguridad, se implementan nuevas funcionalidades y se definen acciones para cada sede. "Con la solución anterior, implementar una política de seguridad podía tardar hasta 5 minutos. Las soluciones de Fortinet permiten un manejo optimizado para que al hacer ajustes desde la sede principal se repliquen los cambios en las demás locaciones de forma inmediata", dice Proaño.

Esta ventaja ha facilitado el trabajo del equipo de TI, pues apenas dos personas son las encargadas de administrar la red de comunicaciones de la matriz y las 7 sedes que tiene UNIANDES. "Ahorro mucho tiempo en la gestión. Cuando sucede algo recibo reportes y ya puedo tomar una decisión para solucionar un error o un ataque específico", explica Proaño. Además, FortiAnalyzer ayuda a llevar un registro detallado de cada acción para encontrar fallos rápidamente y a partir de allí determinar posibles soluciones. "Siempre existen ataques. Lo importante es tener la confianza de que la solución sí está funcionando. Con Fortinet tenemos más tranquilidad y sabemos que todas las sedes y la matriz están protegidas por una solución integrada", agrega Proaño.

Tecnología preparada para los desafíos

Hace dos años, por los resultados positivos obtenidos con las herramientas Fortinet, UNIANDES sumó la solución FortiMail a su infraestructura de seguridad. La universidad estaba recibiendo múltiples ataques a través de correo electrónico, por lo que necesitaba controlar estos incidentes y optimizar la experiencia de los usuarios con el servicio. Esta implementación, sumada a una red segura con soluciones Fortinet, le permitió a la institución estar preparada para atender la dinámica de trabajo remoto obligada por la pandemia.

La entidad no tuvo que hacer inversiones adicionales. El equipo de TI configuró los equipos de los usuarios para que pudieran comunicarse de manera segura a través de la VPN protegida. Igualmente, el correo electrónico contaba ya con su solución propia de seguridad, teniendo en cuenta que es el medio de comunicación más utilizado. La institución segmentó y priorizó el tráfico de navegación, optimizando las capacidades de uso y consumo de los recursos de Internet durante esta época. "Comprobamos que Fortinet es una solución muy robusta y que ofrece gran flexibilidad. Así, pudimos configurar de manera inmediata la red para habilitar capacidades de teletrabajo y re-enrutar las redes y ambientes de seguridad para todos los usuarios", expresa Proaño.

Business impact(Cont)

- Alta disponibilidad de los servicios mediante una gestión optimizada de los proveedores de red
- Habilitación de capacidades de teletrabajo en tiempo récord

Soluciones

- FortiGate
- Fortinet Secure SD-WAN
- Fortinet Secure SD-Branch
- FortiSwitch
- FortiManager
- FortiAnalyzer
- FortiMail
- FortiWeb

"Comprobamos que Fortinet es una solución muy robusta y que ofrece gran flexibilidad. Así, pudimos configurar de manera inmediata la red para habilitar capacidades de teletrabajo y re-enrutar las redes y ambientes de seguridad para todos los usuarios".

– Victor Manuel Proaño, Administrator de Red, UNIANDES



CASO DE ESTUDIO | Universidad ecuatoriana conecta de forma segura sus sedes y optimiza su red con Fortinet Secure SD-WAN

En los próximos meses, con las proyecciones de crecimiento a nuevas ciudades de Ecuador, el objetivo es que cada una de ellas inicie su operación con productos Fortinet. Así, pueden funcionar de manera segura e integradas al instante a la red existente. A su vez, la universidad inició recientemente la implementación de la solución FortiWeb (WAF) para la protección de la interconexión con los bancos, los servicios de pagos en línea, así como también del portal institucional y la intranet. La entidad maneja en promedio unas 1.000 conexiones concurrentes en su sitio web, pues allí están concentrados casi todos los servicios como pagos en línea, visualización de facturas, o aplicación a programas académicos y becas. "Tenemos la protección del FortiGate, pero queríamos implementar una solución especializada para este propósito. FortiWeb ha sido una muy buena adquisición adicional en beneficio de toda la colectividad estudiantil ", concluye Proaño.

FORTINET

www.fortinet.com

Fuente (Fortinet, 2021).