ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

IMPLEMENTACIÓN DE UNA SOLUCIÓN SD-WAN PARA EL USO EFICIENTE DE LOS RECURSOS DE RED EN SU APLICACIÓN EN LA EMPRESA ASERTIA EN EL AÑO 2021

JULIO OSWALDO HEREDIA ARIAS

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN INTERCONECTIVIDAD DE REDES

Riobamba - Ecuador

Agosto 2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado: IMPLEMENTACIÓN DE UNA SOLUCIÓN SD-WAN PARA EL USO EFICIENTE DE LOS RECURSOS DE RED EN SU APLICACIÓN EN LA EMPRESA ASERTIA EN EL AÑO 2021, de responsabilidad del señor Julio Oswaldo Heredia Arias ha sido prolijamente revisado y se autoriza su presentación.

Ing. Ruth Genoveva Barba Vera; Mag.
PRESIDENTE

Firma

Ing. Diego Fernando Ávila Pesantez; Ph. D.
DIRECTOR

Firmado electrónicamente por:
DIEGO FERNANDO AVILA PESANTEZ

Firma

Ing. Alberto Leopoldo Arellano Aucancela; Mag.
MIEMBRO

Firmado electrónicamente por:
ALBERTO LEOPOLDO ARELLANO AUCANCELA

Firma

Ing. Oswaldo Geovanny Martínez Guashima; Mag.
MIEMBRO

OSWALDO GEOVANNY MARTINEZ GUASHIMA

Firmado digitalmente por OSWALDO GEOVANNY MARTINEZ GUASHIMA

Firma

Riobamba, agosto de 2022

DERECHOS INTELECTUALES

Yo, **JULIO OSWALDO HEREDIA ARIAS**, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

JULIO OSWALDO HEREDIA ARIAS

Firmado digitalmente por JULIO OSWALDO HEREDIA ARIAS
Fecha: 2022.10.04 14:51:39 -05'00'

Ing. Julio Oswaldo Heredia Arias

C.I. 0603183526

DEDICATORIA

Dedico este trabajo primeramente a Dios, por ser nuestro creador y ayudarme a cumplir esta meta. Además, Dedico este trabajo con gran amor a toda mi familia por el apoyo incondicional, por siempre impulsarme a ser mejor y lograr con éxito un paso más en mi vida laboral, al alcanzar el título de Máster, en especial a mi esposa Verito mis hijos Danna Julié y Julio Ignacio, ustedes fueron mi mayor inspiración los amo profundamente.

Julio

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

El objetivo de esta investigación fue implementar una solución SD-WAN para el uso eficiente de recursos de red y control de accesos hacia aplicaciones corporativas e internet, inicialmente, se realizó un análisis de la red MPLS y sus riesgos informáticos, se evidenció que el acceso hacia los servicios corporativos que tiene Asertia de forma local en su oficina Matriz y en la nube a través de internet son afectados por la falta de control, esto conlleva a tener latencia con tiempos muy altos y gran cantidad de perdida de paquetes en la comunicación desde las sucursales a la Matriz e Internet que afecta económicamente a la empresa. Una vez ejecutada la implementación de SD-WAN, se aplicó pruebas para obtener la latencia y cantidad de paquetes perdidos y se analizó la información utilizando la prueba de U de Mann-Whitney para comprobar estadísticamente que existe una diferencia significativa en los escenarios de MPLS y SD-WAN. Los resultados obtenidos demuestran que la solución SD-WAN presenta mejoras considerables en valores de latencia y cantidad de paquetes perdidos y los riesgos informáticos se mitigaron a través del control de accesos hacia los servicios locales y en nube aplicando una conexión cifrada a través de VPN IPSec y aplicando los perfiles de seguridad perimetral como IPS, Antivirus, Sandboxing, Web Filtering y Application Control.

Palabras clave: <RED DE ÁREA EXTENSA DEFINIDA POR EL SOFTWARE (SD-WAN)>, <CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO (MPLS)>, < SEGURIDAD DEL PROTOCOLO DE INTERNET (IP-SEC)>, <SEGURIDAD>, <LATENCIA>.

ABSTRACT

The aim of this research was to implement an SD-WAN solution for the efficient use of network resources and access control to corporate applications and the Internet. Initially, an analysis of the MPLS network and its computer risks was carried out to demonstrate that the access towards the corporate services that Asertia has locally in its head office and in the cloud through the internet are affected by the lack of control. It leads to latency with very high times and a large amount of packet loss in the communication from the branches to the headquarters and the Internet that economically affects the company. Once the SD-WAN implementation was executed, tests were applied to obtain the latency and number of lost packets and this information was analyzed using the Mann-Whitney U test to statistically verify that there is a significant difference in the MPLS and MPLS scenarios and SD-WAN. The results obtained shown that the SD-WAN solution presents considerable improvements in latency values and the number of lost packets and computer risks were mitigated through access control to local and cloud services by applying an encrypted connection through IPSec VPN and applying perimeter security profiles such as IPS, Antivirus, Sandboxing, Web Filtering and Application Control.

Keywords: <SOFTWARE DEFINED WIDE AREA NETWORK (SD-WAN)>, <MULTI-PROTOCOL LABEL SWITCHING (MPLS)>, < INTERNET PROTOCOL SECURITY (IP-SEC)>, <SECURITY>, <LATENCY>.

CAPITULO I

1. INTRODUCCIÓN

Las redes de área amplia definidas por software (SD-WAN, por sus siglas en inglés) inician un avance en las redes de comunicación, por la demanda alta en la transmisión de datos y buscar de mejor manera la conectividad de las redes de telecomunicaciones digitales en el mundo. SD-WAN ayuda a actualizar los equipos periféricos del cliente en sitios remotos, integrando servicios que ayudan en carga compartida, a través de múltiples enlaces ascendentes de cualquier tipo. Además. proporciona una interfaz simplificada para la gestión de políticas para rendimiento de la aplicación en tiempo real (Ayapata Mendoza, 2020).

En Ecuador, más empresas están integrando redes administradas por software en sus organizaciones, eliminando claramente tecnologías utilizadas en el pasado (como ATM, Frame Relay, o MPLS). Las tendencias actuales muestran claramente que el objetivo empresarial es aprovechar al máximo la red y los nuevos servicios tales como: imagen, video, audio, voz, entre otros, cuyo tráfico es enviado por una ruta de menor latencia. La contratación de los enlaces de datos e internet es de forma independiente, y tener múltiples contratos de servicio con diferentes proveedores aumenta el costo de administración y servicios de contingencia. Gracias a la tecnología SD-WAN, es posible utilizar Internet para la comunicación a nivel de datos y aprovechar al máximo los recursos disponibles en la infraestructura del proveedor.

Las empresas están indagando la transformación digital. En este sentido, Asertia S.A. y su crecimiento tecnológico está planificando un servicio de redes WAN que tenga un enfoque de seguridad de la información y de fácil administración. Por esta razón, Asertia S.A. ha decidido migrar a la tecnología SD-WAN y eliminar las conexiones a través de MPLS (por sus costos), que le permitirá manejar de forma eficiente los recursos de red.

Esta investigación desarrolla una propuesta de implementación de una red SD-WAN en la empresa Asertia S.A, que tendrá una infraestructura completamente digital, para cumplir con parámetros críticos como la productividad, la eficiencia y la reducción de costos, al tiempo que aprovecha los beneficios que la tecnología puede brindar.

1.1. Planteamiento del problema

La transformación digital que al momento está sucediendo en el segmento corporativo aumenta el tráfico de datos y recursos que provocan que los enlaces de redes WAN actuales tengan saturación, degradación, latencia y pérdida del enlace. Con el incremento de aplicativos, requerimientos de usuarios, servicios de nueva generación las redes WAN tradicionales implementadas en las empresas requieren mayor inversión para satisfacer estas necesidades, por lo que es necesario una solución que brinde una mejor utilización de recursos, acceso seguro a la información, mayor rapidez y disponibilidad en la red sin generar costos muy altos que perjudiquen en el crecimiento de la empresa.

La empresa Asertia S.A. tiene problemas en el acceso a sus aplicaciones corporativas por saturación y degradación de los enlaces de datos, el acceso a internet de los usuarios no cuenta con ningún control de seguridad y ancho de banda, esto genera ineficiencias en la gestión de los servicios de Internet, retrasos en las comunicaciones y pérdidas económicas para la empresa por servicios no disponibles.

1.2. Formulación del problema

¿Con la implementación de una solución SD-WAN se utilizará de manera eficiente los recursos de red en la empresa Asertia?

1.3. Sistematización del problema

- ¿Qué problemas y riesgos tiene la empresa Asertia con la red de accesos actual?
- ¿Cómo ayudaría la implementación de una solución SD-WAN en la empresa Asertia?
- ¿Cuáles son los resultados obtenidos después de implementar una solución SD-WAN en la red de Asertia?

1.4. Justificación de la Investigación

El incremento de las necesidades corporativas pone en evidencia las restricciones de las redes WAN que tiene la empresa al momento de acceder a sus servicios corporativos. Asertia está buscando constantemente mejorar su infraestructura tecnológica y el servicio que brinda al cliente. Por estos motivos, la implementación de redes SD-WAN permitirá

lograr el uso eficiente de los recursos de red y se enfocará en los beneficios de optimización, seguridad, disponibilidad, administración y control de los accesos a las aplicaciones teniendo redes más seguras y dinámicas.

1.5. Objetivos

1.5.1. General

Implementar una solución SD-WAN para el uso eficiente de los recursos de red en su aplicación en la empresa Asertia en el año 2021.

1.5.2. Específicos

- Diagnosticar el estado actual de la red WAN de Asertia y sus riesgos informáticos.
- Configurar una red de accesos WAN basado en tecnología SD-WAN para Asertia.
- Verificar el uso eficiente de los recursos de red y la seguridad en el acceso a aplicaciones corporativas de Asertia.

1.6. Hipótesis

¿La implementación de una solución SD-WAN en la empresa Asertia optimizará el uso eficiente de los recursos de red en el acceso hacia las aplicaciones corporativas e internet?

CAPITULO II

2. MARCO REFERENCIAL

2.1. Antecedentes del problema

La WAN es una red de larga distancia con gran extensión geográfica. Un buen ejemplo de representación de la WAN es la propia Internet, por comprender una zona geográfica global, interconectando ciudades, países y continentes. Con tanta información circulando en las redes, tendrán éxito las empresas o instituciones que saben cómo usarlo adecuadamente todo a su favor. Y para ello, es importante que estos datos consigan seguir con más fluidez y seguridad, algo que no sucede en forma efectiva con las infraestructuras de WAN disponibles (OSTEC, 2018).

Actualmente, la mayoría de las infraestructuras de WAN tienen un bajo ancho de banda y una alta latencia, debido al tráfico de backhauling y la falta de visibilidad de las aplicaciones, resultando a menudo en una pésima experiencia para el usuario. En este sentido, las empresas que tienen su núcleo empresarial basadas en servicios y procesos elaborados a través de Internet pueden tolerar con los reflejos de comunicaciones lentas, indisponibilidad de sistemas esenciales, pérdida de datos, además de varios otros problemas que generan pérdida de tiempo y dinero. Así surge como una alternativa para corregir estos problemas, la tecnología SD-WAN, que permite una comunicación más eficiente y segura (OSTEC, 2018).

2.2. Bases Teóricas

2.2.1. Redes LAN

Las redes LAN son consideradas eficientes recursos tecnológicos que permiten el intercambio de información entre equipos de cómputo interconectados entre sí: son un conjunto de dispositivos interconectados que ocupa un lugar físico, como una oficina de una empresa o una habitación en el hogar; estas pueden ser grandes o pequeñas, y puede ir desde la conexión de un usuario a la red doméstica hasta miles que estén conectados a la red de una empresa, institución, organismo o corporación. (Ley Leyva, 2021)

Las LAN están divididas en cinco áreas principales de aplicación; informática distribuida, sistemas de oficina, redes de terminales, sistemas de fábrica y micro redes; son redes

privadas de acceso múltiple y alta velocidad, que transfieren millones de bits/s mucho mejor que los sistemas ordinarios de comunicación, lo que las transforma en un poderoso herramienta de trabajo en el ámbito empresarial; pero al estar conectadas a la Internet existe el potencial peligro de sufrir ataques cibernéticos por parte de delincuentes con diferentes propósitos: tener acceso a información, robar datos, introducir diferentes tipos de malware a los equipos, dañar los sistemas, interrumpir u obstaculizar el funcionamiento de la red, etc. (Ley Leyva, 2021)

Así mismo, se precisa definir los beneficios de la Red LAN, dentro de los cuales se muestra los siguientes:

- Recursos compartidos: su finalidad es optimizar los recursos de la entidad, obteniendo la mayor productividad de estos y garantizando el servicio a los ordenadores que se encuentran comunicados de forma cableada o inalámbrica.
- Ficheros y datos compartidos: materializa el trabajo en grupo ya que los usuarios consiguen acceder y trabajar sobre el mismo fichero, disponer de información inmediata y facilitar los procesos dentro de la entidad.
- Administración centralizada: si bien la Red Punto a Punto o P2P diseño el software que permite al ordenador ser servidos o cliente, esto no imposibilita que se otorguen permisos de administrador a un servidor, para que se garantice un nivel de seguridad y los permisos pertinentes a los ordenadores vinculados en la Red LAN (López Jaimes, Mojica Marín, & Rodríguez González, 2021).

En lo que respecta a las características, encontramos que accede la elección de un sistema cableado o inalámbrico; la velocidad de transmisión de datos oscila entre 1 Mbps y 1 Gbps; al tratarse de un sistema cableado, la longitud máxima de este será de 100 Mt, sin embargo, esta medida puede elevar al utilizar repetidores. (López Jaimes, Mojica Marín, & Rodríguez González, 2021)

2.2.2. Redes WAN

WAN (Wide-Area Network, Red de Área Amplia), es un sistema de conexión de redes LAN, es una red de larga distancia que abarca una gran extensión geográfica que une varias redes, aunque no se encuentren en el mismo sitio (Soluciones de GPC Inc , 2021).

Comúnmente las redes WAN son utilizadas para comunicar redes LAN y la mayoría de las veces son implementadas por los proveedores de servicios de telecomunicaciones y éstos proporcionarán conexiones LAN a la empresa. En el mundo de las telecomunicaciones el internet es un claro ejemplo de una red WAN, ya que abarca una zona geográfica global, interconectando ciudades, países y continentes (Soluciones de GPC Inc , 2021)

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

La mayoría de las empresas no tienen líneas de transmisión y tienen que rentarlas a una compañía de telecomunicaciones. Los elementos de conmutación o switches son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea entrante, el elemento de conmutación debe preferir una línea saliente hacia la cual reenviarlos. En el pasado, estas computadoras de conmutación han recibido varios nombres; ahora se conocen como enrutador (Tanenbaum & Wetherall , 2012).

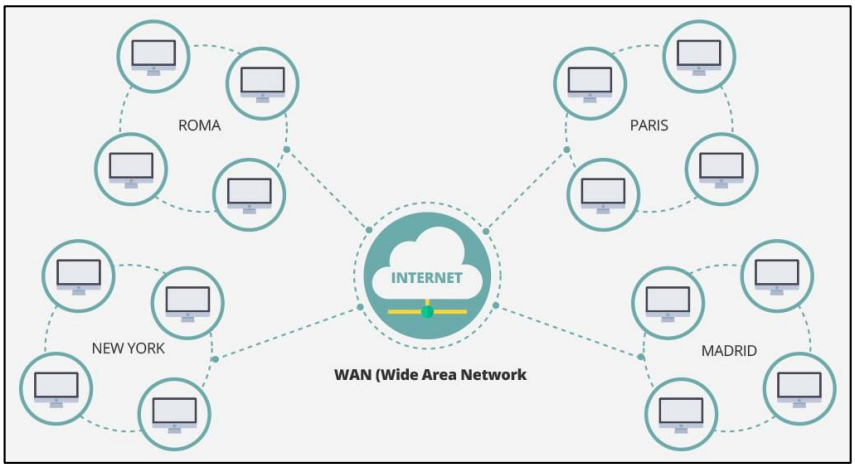


Figura 1-2: Red WAN
Fuente: GPC Inc, 2021

2.2.3. Redes WAN MPLS

MPLS es un protocolo que permite el acceso a redes inteligentes sobre una misma infraestructura ofreciendo servicios IP de extremo a extremo, se caracteriza por aprobar la unión de los bordes MPLS a cualquier tipo de tecnología de acceso ya existente como Ethernet, IP, ATM y Frame Relay, ya que esta es totalmente independiente de los tipos de enlace de acceso (Moreno Alayón, 2021).

El estándar MPLS es apto para cualquier protocolo de capa de red y evita principalmente el retardo ocasionado en los enrutadores de una red convencional al hacer un reenvío de capa de red. Es decir, en la red convencional es usual que cada uno de los enrutadores que recibe un paquete, deba hacer un análisis de su encabezado de la capa de red, asignarlo a una Forward error correction (FEC) y definir el siguiente salto, finalmente, en cada salto el enrutador debe volver a hacer ese reproceso. Según la RFC 3031 (2001), MPLS no asigna una nueva FEC en cada salto, sino que lo asigna una única vez, al identificar el ingreso del paquete a la red. La FEC se codifica en un código corto denominado "Etiqueta", que permitirá identificar el paquete a lo largo de la red (Moreno Alayón, 2021).

La etiqueta especifica el siguiente salto y una nueva etiqueta, con el fin de sustituir la antigua etiqueta por la nueva en cada salto hasta alcanzar su destino. Lo anterior, ofrece algunas ventajas frente al enrutamiento IP convencional, ya que en una red convencional internet no acepta aplicaciones para video conferencia, apps en tiempo real y otros, ahora con MPLS se alcanza integrar los niveles de enlace de datos (capa 2) con la rápida conmutación y el nivel de red (capa 3) con el control de enrutamiento. MPLS usa el Label Distribution Protocol (LDP) para brindar a la red los medios para enviar y proporcionar acceso a la información de enlace de etiquetas entre los enrutadores LSR, los enrutadores instituyen las secciones LDP con su par potencial y finalmente, definen una ruta de conmutacion LSP logrando el intercambio de conmutacion de etiquetas y enviando el paquete a su destino. (Moreno Alayón, 2021)

Básicamente una red MPLS segura y funcional, requiere de:

1. Interconectar los enrutadores por medio de cables o Wireless (capa 2)
2. Un protocolo de enrutamiento junto con el protocolo LDP para sincronizar los enrutadores con capa 2 y capa 3.
3. Un túnel VPLS.
4. La unión lógica de la interfaz física con el túnel VPLS y lo que se reconoce como un puente "BRIDGE". (Moreno Alayón, 2021)

2.2.2.1. Arquitectura MPLS

MPLS (Multi Protocol Label Switching) Conmutación múltiple protocolo mediante etiquetas, una etiqueta MPLS tiene el siguiente formato de 4Bytes:

Tabla 1-2: Formato de Etiqueta de MPLS

Bits→	20	3	1	8
	Etiqueta	**Exp**	**S**	**TTL**

Realizado por: Heredia, J. 2022

20 bits se utilizan para la etiqueta (valor numérico desde 0 hasta 1048572.

3 bits corresponden a los bits experimentales relacionados con la calidad de servicio (QoS).

1 Bit corresponde (0 para todas las etiquetas y 1 solo cuando se trata de una etiqueta final.

8 bits corresponden al tiempo de vida del paquete (TTL). (Spadaro, 2012)

2.2.2.2. Elementos de MPLS

Una red MPLS está concertada por dos tipos principales de nodos, los Routers de Etiquetado de Frontera (LER: Label Edge Routers), y los Routers de Conmutación de Etiquetas (LSR: Label Switching Routers). (Spadaro, 2012)

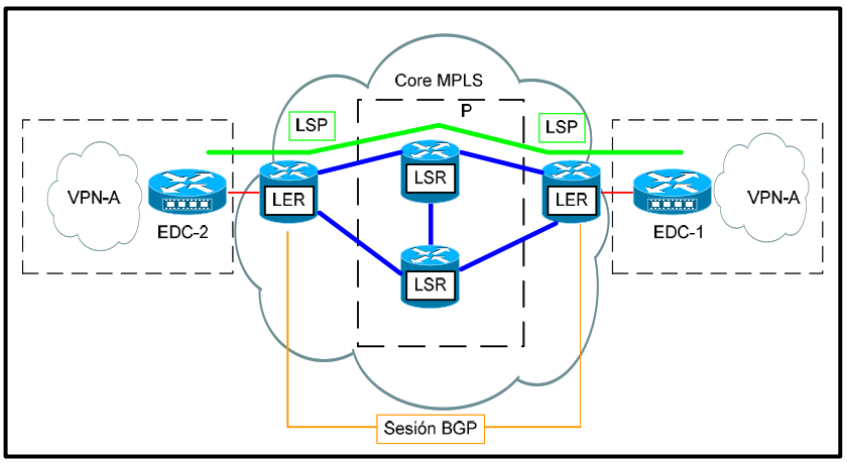


Figura 2-2: Elementos de MLPS
Fuente: Heredia, J. 2022

- LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router.

- LSR (Label Switching Router): elemento que conmuta etiquetas.
- LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.
- LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador (Spadaro, 2012).

2.2.3. Redes Definidas por Software SDN

Las redes definidas por software (SDN, por sus siglas en inglés) son usadas para la creación de redes que serán administradas y serán gestionadas mediante un controlador, de una manera ágil y efectiva. Este nuevo paradigma de redes ayuda a un desarrollo acelerado de los centros de datos, al no tener que conseguir más equipamiento reduciendo costos operativos a las empresas y optimando la administración a traves de una gestión concentrada (Valarezo Constante, 2020).

Así mismo, se puede definir como una arquitectura de red dinámica, manejable, adaptable, de costo eficiente. Lo cual, la hace ideal para las altas demandas de ancho de banda y la naturaleza dinámica de las aplicaciones actuales. Esta arquitectura desacopla el control de la red y la funcionalidad de reenvío de información aprobando el control de la red alcance ser completamente programable, adquiriendo una infraestructura de red subyacente sea abstraída por las aplicaciones y servicios de red (Valarezo Constante, 2020).

Las redes actuales se encuentran limitadas a medida que crece la demanda de aplicaciones para los diferentes tipos de requerimientos de los usuarios finales, quienes no se sienten a gusto atados a un escritorio. Al aplicar SDN se les conseguir manifestar la opción de la libertad de movilidad y la facilidad de acceso a la información en cualquier lugar y hora que esta sea requerida. Las SDN se encuentran en pleno crecimiento, a nivel mundial, por las bondades de sus características en programación que ofrecen una mayor garantía en lo referente a seguridad (Valarezo Constante, 2020).

La arquitectura de las SDN consta de tres partes:

- **Capa de aplicación,** comunican las solicitudes de recursos o información sobre la red en su conjunto.
- **Capa de control**, que manejan la información de las aplicaciones para resolver las enrutar como un paquete de datos.
- **Capa de infraestructura,** que recogen información del controlador sobre dónde mover los datos.

Estos tres elementos pueden encontrarse en diferentes ubicaciones físicas.Los dispositivos de redes virtuales o físicas son los que realmente trasladan los datos a través de la red. Los conmutadores virtuales, que pueden estar integrados en el software o en el hardware, en algunos casos asumen las responsabilidades de los conmutadores físicos y consolidan sus funciones en un único conmutador inteligente. El conmutador comprueba la integridad tanto de los paquetes de datos como de los destinos de las máquinas virtuales y traslada los paquetes. (vmware, 2022)

2.2.3.1 Ventajas de las Redes Definidas por Software

En respuesta a las prohibiciones que tienen las infraestructuras tradicionales las empresas prefieren por este tipo de redes, algunas de sus ventajas son las siguientes:

Escalabilidad y flexibilidad: La virtualización de la infraestructura de red le admite desarrollar y contraer los recursos de red según sea necesario, sin necesidad de hardware propietario adicional. Los administradores de red también tienen más flexibilidad para optar el hardware de la red, ya que logran preferir protocolos de código abierto para comunicarse con cualquier cantidad de dispositivos de hardware a través de un controlador central.

Seguridad: Las redes definidas por software incrementan la visibilidad en toda la red al proveer una visibilidad completa de las amenazas de seguridad. Con el predominio de los dispositivos inteligentes conectados a Internet, SDN ofrece una clara ventaja sobre las redes tradicionales. Los desarrolladores consiguen crear zonas separadas para dispositivos que requieren diferentes niveles de seguridad o aislar instantáneamente un dispositivo vulnerable para que no infecte el resto de la red.

Administración simplificada: Las redes definidas por software proporcionan la gestión y el mantenimiento de la infraestructura general, ya que no requieren profesionales altamente especializados para administrarla.

Menor costo: Las infraestructuras de red definidas por software generalmente cuestan menos que sus contrapartes de hardware porque se elaboran en servidores o en infraestructura preexistente. También ocupan menos espacio. Esto se debe a que aprueban establecer múltiples funciones en un solo servidor. Al reducir la necesidad de equipos físicos, se alcanza la consolidación de recursos, lo que resulta en menos espacio, energía y costos generales.

2.2.3.2 Diferencias entre SDN y redes tradicionales

La diferencia clave entre las SDN y las redes tradicionales es la infraestructura: las SDN están basadas en software, mientras que las redes tradicionales están basadas en hardware. Ya que el plano de control está basado en software, las SDN son mucho más flexibles que las redes tradicionales. Permiten que los administradores controlen la red, cambien los ajustes de configuración, provean recursos y eleven la capacidad de la red, todo ello desde una interfaz de usuario centralizada y sin necesidad de añadir más hardware.

Asimismo hay diferencias relativas a la seguridad entre las SDN y las redes tradicionales. Gracias a una mayor visibilidad y a la capacidad de definir rutas seguras, las SDN ofrecen una seguridad mejor en muchos aspectos. Sin embargo, puesto que las redes definidas por software hacen uso de un controlador centralizado, protegerlo es crucial para proteger una red segura, puesto que este punto único de fallo simboliza una posible vulnerabilidad de las SDN. (Ayapata Mendoza, 2020).

2.2.3.3 Modelos de Redes Definidas por Software

Existen diferentes modelos de SDN:

- **SDN abierta:** los administradores de red manejan un protocolo como OpenFlow para vigilar el comportamiento de los conmutadores virtuales y físicos en el plano de datos.

- **SDN por API:** en lugar de manejar un protocolo abierto, las interfaces de programación de aplicaciones controlan cómo se desplazan los datos a través de la red en cada dispositivo.
- **Modelo de superposición de SDN:** otro tipo de red definida por software confecciona una red virtual sobre una infraestructura de hardware existente, lo que crea túneles dinámicos hasta diferentes centros de datos locales y remotos. La red virtual asigna el ancho de banda en diversos canales y asigna dispositivos a cada canal, de forma que la red física queda intacta.
- **SDN híbrida:** este modelo ajusta la red definida por software con los protocolos de red tradicionales en un solo entorno a fin de respaldar las diferentes funciones de una red. Los protocolos de red estándar siguen dirigiendo parte del tráfico, mientras que la SDN asume la responsabilidad de otra parte, lo que consiente a los administradores de red introducir la SDN por etapas en un entorno heredado. (Ayapata Mendoza, 2020)

2.2.4. SD-WAN

Los servicios SD-WAN (Software Defined Networking Wide Area Network) son el resultado de aplicar el concepto de SDN en redes WAN. Su objetivo principal es minimizar los costos que generan los servicios de conectividad, usando una infraestructura ya existente y algunos servicios en la nube que ofrecen soluciones empresariales más completas. SD-WAN se define como un servicio SD-WAN proporciona una red de superposición virtual que permite la conectividad orquestada, controlada y orientada a aplicaciones entre interfaces de red de usuario SD-WAN, y proporciona la construcción lógica de una red enrutada privada virtual L3 para el suscriptor que transmite paquetes IP entre sitios. (Rubiano Aguilar, 2021)

2.2.5. Componentes

Cada uno de los componentes de la arquitectura de SD-WAN se describen con su propia infraestructura, dependiendo el fabricante que ofrece la solución, utilizando software libre o software propietario. Entre los componentes principales de la ejecución se cuenta con los siguientes:

- Virtualización
- Servicios de red: procesamiento de paquetes, proxy, enrutamiento, plano de datos.

- Administración de servicios: base de datos, intercambio de mensajes, servidores web, servidores de aplicación web, monitoreo de recursos.
- Servicios de seguridad: cifrado, firewall, WAF, IDS, IPS, filtrado y clasificación, antivirus, seguridad DNS
- Software de sistema: sistema operativo.

2.2.6. Arquitectura de SD-WAN.

La tecnología SD-WAN busca facilitar las operaciones en redes WAN, optimizando la gestión e incluyendo flexibilidad. Se estudia la arquitectura desde los puntos de vista lógico y físico, describiendo los componentes y capas. SD-WAN separa en plano de control y plano de datos el tráfico que maneja para conseguir centralizar la gestión de los dispositivos.

2.2.6.1. Arquitectura lógica

Se consideran tres capas en SD-WAN definidas como capa de datos, capa de control y capa de aplicación, como se muestra en la Figura 3-2.

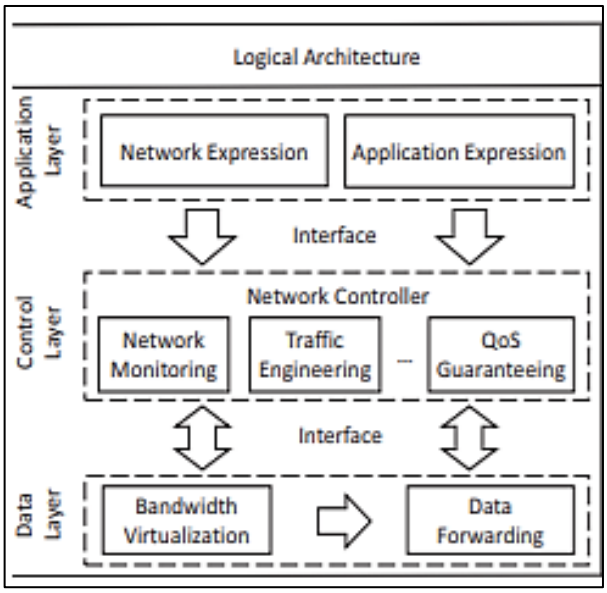


Figura 3-2: Arquitectura lógica de SD-WAN
Fuente: Sergey, 2018.

En la capa de datos, se ejecutan funciones como reenvío de datos y virtualización del ancho de banda. La virtualización del ancho de banda combina diferentes enlaces para un lugar, colocando de una reserva de ancho de banda a ser distribuido entre las aplicaciones. El reenvío de datos consiste en la repartición de datos a través de dispositivos de red,

usando el ancho de banda proporcionado. El plano de datos funciona solo según las instrucciones de la capa superior de control.

En la capa de control, se muestran las funciones implementadas y administradas independientemente, para que los operadores de red puedan modificar, desarrollar y revisar cada una de ellas. Las funciones pueden ser conectadas para trabajar juntas e elevar la flexibilidad de la red WAN, de esta forma se garantiza la calidad de servicio (QoS, quality of service) para aplicaciones que así lo requieren.

En capa de aplicación, se da la posibilidad de definir los requerimientos específicos para la red y aplicaciones. Es posible declarar estos requerimientos en alto nivel, de forma que la solución realice la traducción de estos requerimientos a configuraciones de red. La capa de aplicación permite que los administradores de red y desarrolladores de aplicaciones puedan estar implicados en el control del funcionamiento de la red.

2.2.6.2. Arquitectura física

Como se observa en la Figura 4-2, el plano de datos de SD-WAN consiste en los dispositivos que realizan la entrega de datos a los destinos conectados por routers y enlaces físicos.

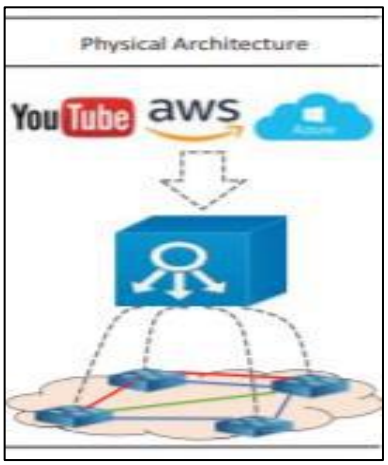


Figura 4-2: Arquitectura física de SD-WAN
Fuente: Sergey, 2018.

Un controlador de red está a cargo de estos dispositivos, el cual es un servidor y un cluster, dependiendo de la necesidad de procesamiento y del tamaño de la red. Por último, la capa de aplicación está expresada por los servicios finales que maneja el negocio y sus usuarios, mediante políticas para que un controlador de red distribuya los recursos

disponibles entre los sitios según la necesidad. De forma que se tenga disponibilidad de información, debe considerarse controladores de respaldo de forma que asuman las tareas de control cuando los controladores principales presenten algún fallo.

2.2.6.3. Arquitectura SD-WAN

En este caso particular, detalla tres capas esenciales: datos, control, gestión y orquestación, Figura 5-2.

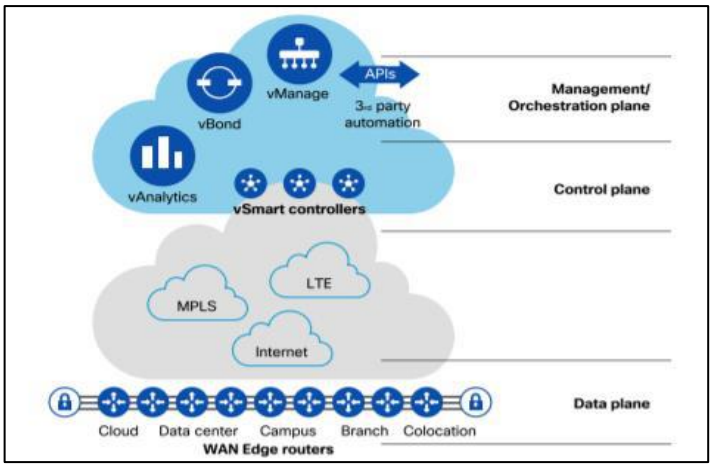


Figura 5-2: Arquitectura SD-WAN
Fuente: SD-WAN Cloudscale architecture.

Incluye distintos servidores para lo mencionado: gestión de los administradores de red y despliegue de configuración, resolución de problemas y monitoreo. La gestión y la asignación de recursos zero-touch después de realizar autenticación. Plano de control y servidor para la ejecución de las políticas creadas, enrutamiento. Por último, los routers Edge, son responsables del flujo del tráfico. Estos componentes y su interconectividad se representan en la Figura 6-2. Los controladores son máquinas virtuales con sistema operativo Linux.

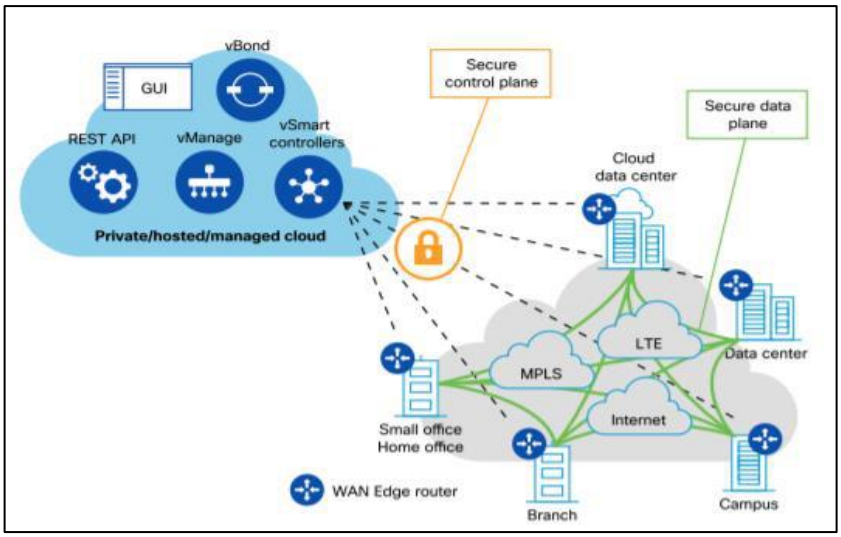


Figura 6-2: Interacción componentes Cisco SD-WAN Cisco
Fuente: Cisco (2019). Cisco SD-WAN Cloudscale architecture.

De esta forma, el objetivo de la presente investigación es efectuar el análisis de caso para una implementación segura para la tecnología emergente SD-WAN, la misma que aún no ha sido adaptada en su totalidad en el medio local. Al contar con varios componentes, se debe cumplir el análisis para cada uno de ellos de forma que se proteja integralmente la solución. (Velasquez Blacutt, 2020).

2.2.7. Como funciona SD-WAN

SD-WAN conecta a los usuarios a cualquier aplicación donde sea que se encuentre desde el centro de datos a la nube. Determina de forma inteligente qué ruta satisface mejor los requerimientos de rendimiento ideales para una aplicación específica. Luego encamina el tráfico a la ruta ideal de la WAN, mientras que las arquitecturas tradicionales solo tienen la capacidad de enrutar todas las aplicaciones a través de MPLS (AXESS, 2019).

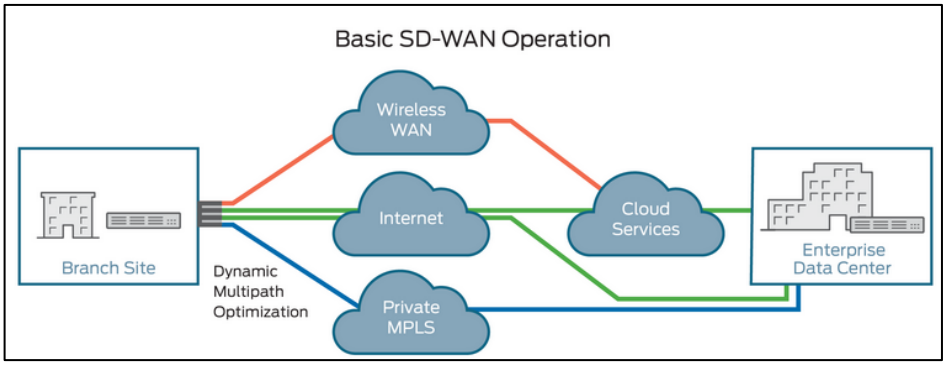


Figura 7-2: Operación básica de SD-WAN
Fuente: Sánchez, 2020.

2.2.8 Conocimiento de la aplicación

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

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

2.2.9 Selección de ruta dinámica

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

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

2.2.10 Implementación sin intervención

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

2.2.11 Orquestación centralizada

El gestor de SD-WAN a los administradores de red de las empresas acceder a una interface para simplificar, implemetar y automatizar de forma simple y ahorrar tiempo y responder más rápido a las demandas del negocio.

La administración centralizada puede proporcionar un flujo de trabajo intuitivo para que las políticas diseñen estrategias para la distribución de aplicaciones y otro tráfico a través y entre las sucursales. Con la visualización automatizada de superposición de VPN (Virtual Private Network), la conectividad en malla a través de los hubs y las sucursales, especialmente en implementaciones SD-WAN más grandes, se administra fácilmente con una sobrecarga mínima (FORTINET, 2021).

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

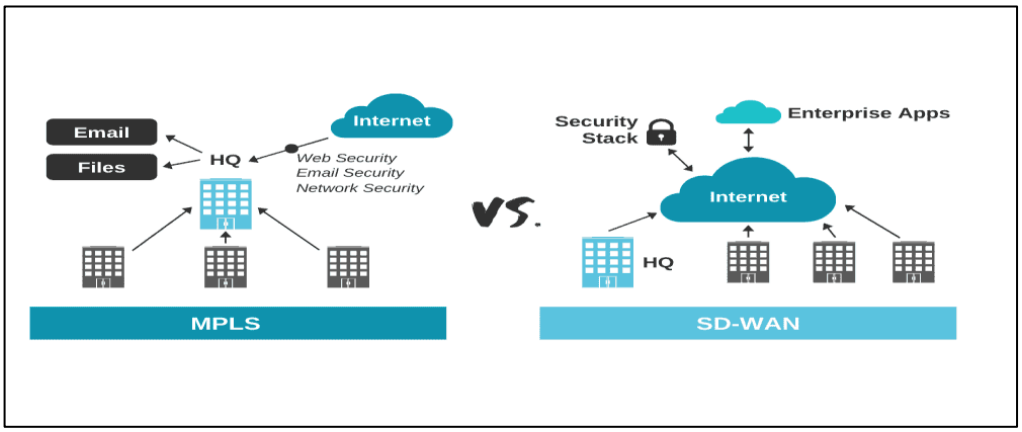


Figura 8-2: Comparación entre red MPLS y SD-WAN
Fuente: (Parra, 2020)

2.2.12 Ventajas y desventajas

Conforme a estudios de la firma de investigación IDC (International Data Corporation), el mercado de SD-WAN continuará creciendo a una tasa superior al 30% durante los próximos años, aproximándose a los USD5.3 mil millones para el año 2023. (FORTINET, 2021). Muchas empresas están optando por soluciones SD-WAN para alcanzar una serie de beneficios, incluidos los siguientes:

Experiencia del usuario mejorada: SD-WAN permite que los sitios remotos se conecten de forma más fácil a las redes, con menor latencia, mejor rendimiento y con una conectividad más segura.

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

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

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

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

2.2.13 Principales capacidades de la solución SD-WAN

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

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

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

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

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

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

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

Controles basados en políticas y encadenamientos de servicios: Las plataformas SD-WAN normalmente proporcionan un redireccionamiento inteligente basado en políticas de tráfico y la capacidad de encajar dinámicamente el flujo de servicios de redes virtuales

(VNF, Virtualized Network Function) como firewalls, filtros de contenido, proxies y otras funciones de la red, sin interrumpir a la red subyacente.

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

2.2.14 Capacidades avanzadas de ancho de banda SD-WAN

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

Según IDC, la optimización del ancho de banda WAN y la seguridad constante de las aplicaciones son las dos principales motivaciones para las implementaciones de SD-WAN.
SD-WAN no solo debe suministrar conectividad WAN de bajo costo, sino que también debe garantizar que el rendimiento de las aplicaciones de comunicaciones unificadas críticas para el negocio se mantenga alto, sin comprometer la seguridad efectiva.

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

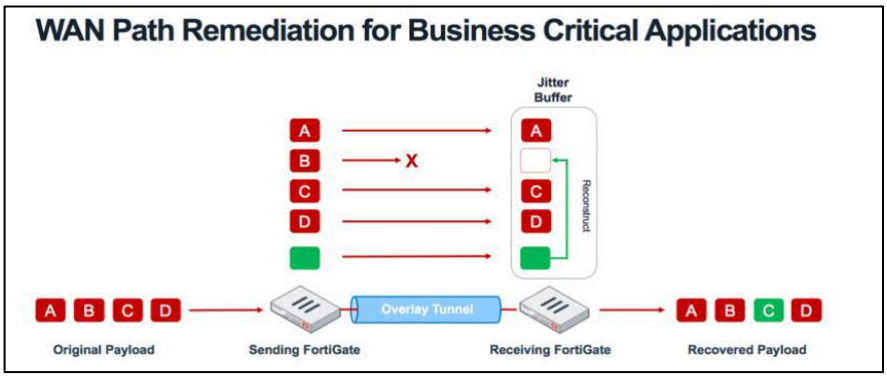


Figura 9-2: Remediación de la ruta WAN
Fuente: (Shah, 2019)

2.2.15 Agregación SD-WAN

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

Para proporcionar una mejor visión de la gestión del ancho de banda, Fortinet Secure SD-WAN también puede detectar y reportar el ancho de banda WAN bajo demanda (FORTINET, 2021).

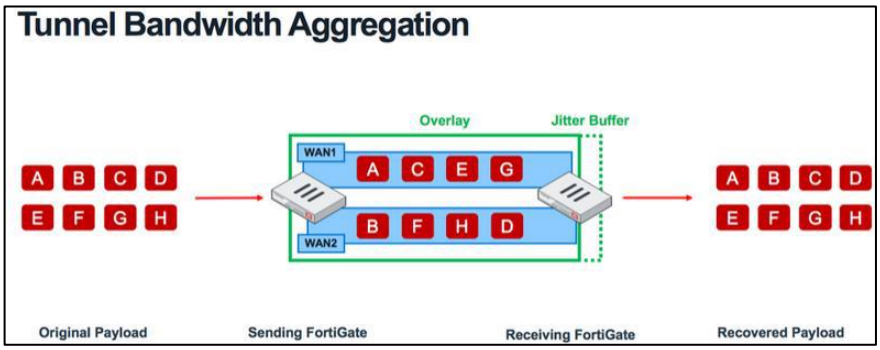


Figura 10-2: Agregación de ancho de banda de un túnel
Fuente: (Shah, 2019)

La dirección de aplicaciones a través de una red VPN superpuesta acelerada proporciona la mejor calidad de experiencia en una WAN de bajo costo a través de una exactitud de reconocimiento de aplicaciones mejorada combinada con una inspección SSL (Secure Sockets Layer) profunda y el menor impacto en el rendimiento (FORTINET, 2021).

2.2.16 Solución SD-WAN completa y de alto rendimiento

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

Las organizaciones de hoy en día están cambiando cada vez más de MPLS a SD-WAN. Si bien muchas soluciones SD-WAN brindan conectividad básica, luchan por brindar la gama completa de velocidad, interconectividad, flexibilidad y seguridad que realmente requieren las sucursales de hoy (FORTINET, 2021).

2.2.17 SD-WAN administrada

Los proveedores de SD-WAN administrados agregan valor a través de la experiencia que las empresas luchan por retener internamente, a través de la inversión continua en las últimas tecnologías SD-WAN para el beneficio de sus clientes y a través del conocimiento detallado de cómo las soluciones SD-WAN se integran con otros proveedores, particularmente proveedores de infraestructura en la nube (Figura 2.11).

2.2.18 SD-WAN contra internet público

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

La Internet de banda ancha tampoco suele ser segura y los datos pueden verse comprometidos si los usuarios, especialmente los remotos, acceden a las redes utilizando una conexión no segura. La SD-WAN hace que la experiencia general sea sin problemas, más ágil y segura (si la seguridad está integrada correctamente). Figura 2.11.

2.2.19 Convierta la seguridad de SD-WAN en una prioridad

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

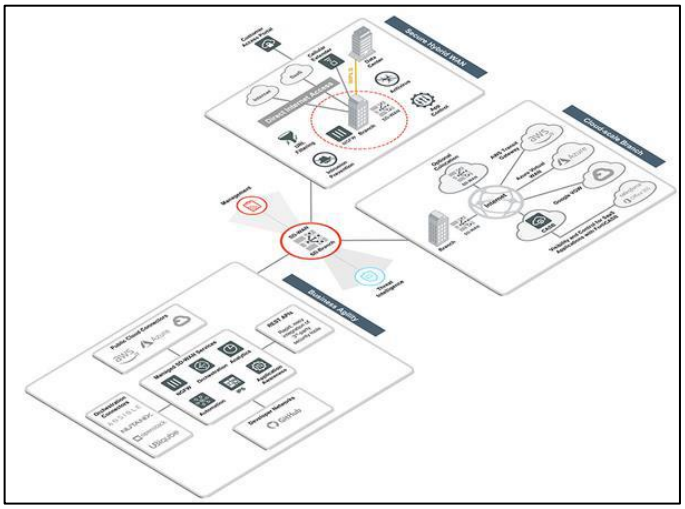


Figura 11-2: Esquema de SD-WAN administrada
Fuente: (Fortinet, 2021)

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

2.2.20 Entender las razones empresariales para adoptar SD-WAN

Aunque se ha discutido mucho acerca de los principales impulsores empresariales para utilizar SD-WAN, mediante una encuesta se puede mostrar que los principales impulsores para la implementación de SD-WAN son la reducción de costos, la gestión y la necesidad de agilidad de red. Sin embargo, el incremento de las empresas que no han efectuado SD-WAN es la agilidad de la red dentro de su entorno. Aquellas que ya han implementado SD-WAN consideran que los costos y la mejora en la gestión y automatización de la red son los aspectos principales (SDxCentral LLC, 2018).

Se cree que esta diferencia en las opiniones refleja el hecho de que los usuarios pioneros están por delante de sus colegas en la adopción de la automatización, y que es probable que utilicen esta como una justificación para realizar SD-WAN con el objetivo de optimizar los ahorros operativos y de capital (SDxCentral LLC, 2018).

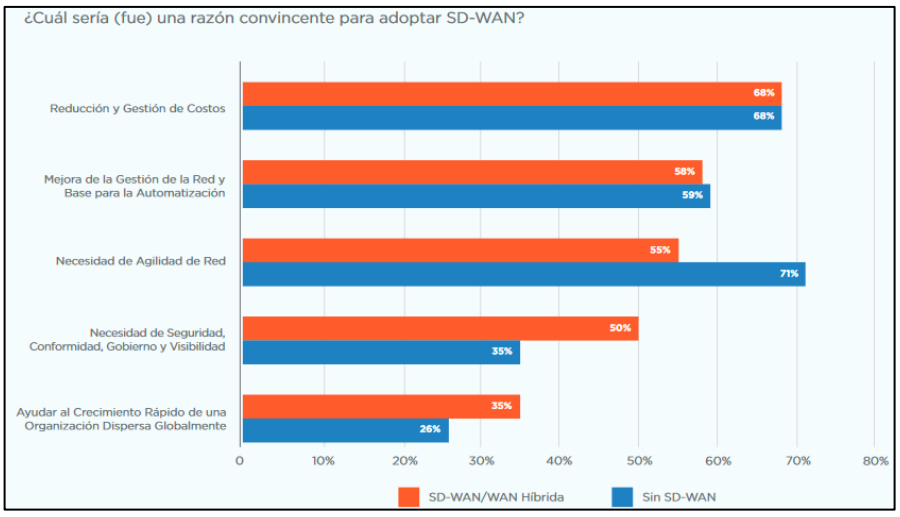


Figura 12-2: Porcentajes de empresas por adopción SD-WAN
Fuente: (SDxCentral LLC, 2018)

2.2.21 Desafíos de la transición a una SD-WAN

Para aquellos que todavía no han efectuado una solución SD-WAN, escoger un proveedor o asociado para la transformación de la red (incluida la SD-WAN) se considera particularmente desafiante. De hecho, la selección del proveedor se ve como un desafío importante incluso para aquellas empresas que ya han comenzado su camino hacia SD-WAN (SDxCentral LLC, 2018).

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

2.2.21.1 Seguridad gestionada

La seguridad gestionada o MSSP (Managed Security Service Provider) destaca por ser un servicio con profesionales altamente cualificados y con experiencia que velarán de forma proactiva por la seguridad de su organización. Este servicio se ha convertido en una de las figuras clave más demandadas por las organizaciones por su capacidad de brindar una visión integral y multidisciplinar de la seguridad corporativa en todas y cada una de sus las áreas de una organización; desde la infraestructura tecnológicas, hasta la concienciación del personal (AUDITECH, 2021).

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

2.2.22. Comparación entre SD-WAN y MPLS

En el siguiente cuadro se hace un resumen comparativo de las ventajas y desventajas más relevante de las tecnologías SD-WAN vs MPLS.

Tabla 2-2: Comparación entre SD-WAN y MPLS

	SD-WAN	MPLS
Costo	Consolidación de servicios, su administración es centralizada basada en políticas.	El mantenimiento es costoso, un técnico especializado debe ir al lugar.
Escalabilidad	Permite aumentar fácilmente la capacidad según sea necesario.	Se requiere de un análisis para aumentar la capacidad lo que lleva más tiempo.
Rendimiento	Permite monitorear el estado del enlace y redirigir el tráfico según sea necesario directamente desde la plataforma.	MPLS presenta latencia dependiendo del número de saltos que requiera y para el monitoreo se requiere de otras aplicaciones.
Agilidad	Respuesta rápida a las solicitudes de nuevos servicios WAN.	La respuesta requiere tiempo para ofrecer un producto acorde a lo solicitado.

Realizado por: Heredia, J. 2022

CAPITULO III

3. DISEÑO DE LA INVESTIGACIÓN

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

La presente investigación puede clasificarse de dos tipos: Aplicativa y Cuasiexperimental.

- **Aplicativa:**

Con la información y conocimientos existentes, producto de investigaciones previas, así como del estudio y la investigación científica se pretende solucionar problemas cotidianos de una forma práctica desarrollando una implementación de una solución SD-WAN en la red de Asertia, con lo que fue factible establecer y documentar los beneficios que brinda esta tecnología a la empresa.

- **Experimental:**

Dado que es una investigación objetiva, sistemática y controlada, basada en los principios encontrados en el método científico, en la experimenta el escenario de una solución SD-WAN para evaluar y examinar el desempeño de la misma.

3.2. Métodos de Investigación

3.2.1. Método experimental y de observación

En la presente investigación se utilizaron los siguientes métodos:

- **Método científico:** Mediante un proceso sistemático y ordenado se establecerá qué relación existe entre la arquitectura actual y propuesta, evaluando el comportamiento de las mismas, consta de las siguientes etapas:
  - Planteamiento del problema
  - Levantamiento de la información necesaria
  - Análisis e interpretación de Resultados
  - Proceso de la comprobación de la Hipótesis y difusión de resultados
- **Método comparativo:** Una vez realizado el estudio general se deberá comparar cada una de las arquitecturas, con el objetivo de establecer sus similitudes y diferencias y de ello sacar conclusiones.

- **Método Analítico Sistemático:** Se realizará un estudio individual analizando el rendimiento de cada una de las arquitecturas actual y propuesta, posteriormente se ejecutará un análisis integro para comparar las arquitecturas y determinar si existe un mejor nivel de seguridad y control de accesos a los servicios corporativos de la red.

3.3. Enfoque de la investigación

El enfoque de la investigación es cualitativo - cuantitativo, mediante los resultados que se obtendrá de la comparación de las arquitecturas de red, se busca medir, Latencia, y la cantidad de pérdida de paquetes, además interpretar los resultados, que permitan determinar que con la arquitectura propuesta logrará un mejor rendimiento en la red.

3.4. Alcance investigativo

El propósito de la investigación es evaluar el nuevo diseño de red con la arquitectura SD-WAN, lo que accederá el uso eficiente de los recursos de red en Asertia. También se realizará un análisis como alcance explicativo de los resultados.

3.5. Población de estudio

Para la presente investigación la población de estudio está conformado por:

- Los equipos servidores de la agencia Matriz (12)
- 14 equipos de cada sucursal

3.6. Unidad de análisis

La unidad de análisis de la investigación son las arquitecturas de la red (tradicional y propuesta) con el propósito de evaluar la latencia de la red y la pérdida de en los dos escenarios.

3.7. Selección de la muestra

En la presente investigación se analizará mediante la siguiente muestra:

1 equipo de cada sucursal y 2 servidores (1 local y 1 en nube)

8 test de conectividad a cada servidor por cada sucursal ejecutadas en cada escenario

48 pruebas para el escenario MPLS

48 pruebas para el escenario SD-WAN

3.8. Recolección de datos primarios y secundarios.

Para la realización de la presente investigación se utilizaron las siguientes técnicas:

- ***Búsqueda de información:*** permite conseguir la información necesaria sobre la red de SD-WAN, utilizando las fuentes secundarias disponibles.
- ***Pruebas:*** permite realizar comparaciones para considerar el rendimiento de las 2 arquitecturas de red (MPLS y SD-WAN).
- ***Observación****:* permite cualificar y cuantificar los resultados de las pruebas realizadas en las 2 arquitecturas de red (MPLS y SD-WAN).
- ***Análisis:*** permite determinar los resultados de la investigación.

Las fuentes que se tomarán como base para esta investigación serán:

- **Primarias**

Papers y revistas científicas.

Investigaciones e implementaciones realizadas y libros

- **Secundarias**

Observaciones y Textos

3.9. Variables e indicadores

De acuerdo con la hipótesis planteada, se determina las siguientes variables:

Variable independiente: Solución SD-WAN.

Variable dependiente: Uso eficiente de recursos de red

3.10. Operacionalización conceptual de variables

Teniendo la variable dependiente e independiente se realizó la siguiente generalización de conceptos.

Tabla 1-3: Operacionalización conceptual de variables

Variable	Tipo	Concepto
Solución SD-WAN	Variable Independiente	Esta arquitectura es el nuevo enfoque para la conectividad de redes.
Uso eficiente de recursos de red	Variable Dependiente	Eficacia en el manejo de tráfico sobre múltiples conexiones disponibles.

Realizado por: Heredia, J. 2022

Tabla 2-3: Operacionalización metodológica de variables

Variable	Indicador	Técnica	Instrumento/Fuente
Solución SD-WAN	Ingeniería de tráfico Seguridad	• Observación • Pruebas • Análisis	Diagramas de red, topología física y lógica. Equipos físicos Fortigate
Uso eficiente de recursos de red	Latencia Perdidas de paquetes	• Observación • Pruebas • Análisis	Diagramas de red, topología física y lógica. Equipos físicos Fortigate Arquitectura SD-WAN

Realizado por: Heredia, J. 2022

3.10.1. Matriz de consistencia

Al realizar la matriz de consistencia se estarán estableciendo los indicadores e índices que nos permitirán evaluar la variable tanto independiente y dependiente y obtener resultados a partir de las mediciones, este proceso se realiza mediante descripciones de tablas en donde se ingresa el objetivo general, la hipótesis, la variable y su tipo, los indicadores, técnicas e instrumentos de medición de la siguiente manera:

Tabla 3-3: Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	¿Con la implementación de una solución SD-WAN se utilizará de manera eficiente los recursos de red en la empresa Asertia?
OBJETIVO GENERAL	Implementar una solución SD-WAN para el uso eficiente de los recursos de red en su aplicación en la empresa Asertia en el año 2021.
HIPÓTESIS GENERAL	¿La implementación de una solución SD-WAN en la empresa Asertia optimizará el uso eficiente de los recursos de red en el acceso hacia las aplicaciones corporativas e internet?
VARIABLES	• Solución SD-WAN • Uso eficiente de recursos de red
INDICADORES	• Arquitecturas • Número de equipos y enlaces. • Latencia. • Cantidad de pérdida de paquetes.
TÉCNICAS	Observaciones
INSTRUMENTOS	Diagramas de red, topología física y lógica, cálculos de latencia, cálculo cantidad de pérdida de paquetes.

3.11. Diseño de la investigación

El presente estudio de investigación es de tipo cuasiexperimental, puesto que se comparará el rendimiento una red MPLS tradicional con el de una red SD-WAN. Con el objeto de establecer latencia y pérdida de paquetes. Para este propósito se evaluarán 2 escenarios los mismos que por medio de un test de conectividad serán monitoreados.

Cada uno de los escenarios de pruebas, fue construido con el mismo número de equipos y topología física. En los dos escenarios se utilizó MPLS (Multiprotocol Label Switching) y SD-WAN (Software-Defined approach to managing the WAN).

Tabla 4-3: Equipos utilizados en la investigación

Nombre	Sucursal	Direccionamiento
SRV-FACT-ASERTIA	Matriz-Asertia	192.168.1.100
SRV-NUBE-ORACLE	Oracle-Asertia	
CAJ-STD-AV-QUITO	Santo Domingo – Sucursal	192.168.10.50
CAJ-ESM	Esmeraldas	192.168.20.50
CAJ-QDO	Quevedo	192.168.30.50
CAJ-PDR	Pedernales	192.168.40.50
CAJ-UIO	Quito	192.168.50.50
CAJ-BHY	Babahoyo	192.168.60.50

Realizado por: Heredia, J. 2022

Tabla 5-3: Hardware Fortigate

Modelo	Características	Sucursal
Fortigate 100E	Firewall/IPS/NGFW/Threat Protection	Matriz
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Bodega-2
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Bodega-2
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Sucursal-1
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Quevedo
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Esmeraldas
Fortigate 60F	Firewall/IPS/NGFW/Threat Protection	Pedernales

Realizado por: Heredia, J. 2022

3.12. Herramientas

Las herramientas que se utilizaron para analizar y examinar las arquitecturas de red MPLS y SD-WAN, así como para comprobar la hipótesis planteada son:

3.12.1 Para la implementación:

- Arquitectura de red MPLS actual
- Arquitectura de red SD-WAN con equipos Fortigate

3.12.2 Para el análisis estadístico:

- Paquete estadístico SPSS
- Microsoft Excel 2019

3.13. Diagnóstico de arquitectura de red de accesos MPLS de Asertia.

Asertia S.A es una empresa líder en el mercado de consumo masivo que se encarga de la distribución y venta de productos de consumo masivo que vende sus productos a distintos clientes como autoservicios, mayoristas, minimarkets, tiendas de barrio, etc. Las redes de acceso WAN de Asertia y una gran cantidad de empresas tienen redes de acceso basadas en MPLS, que buscan su transformación digital con nuevas tecnologías y servicios y con una red WAN tradicional no se puede alcanzar este objetivo, por ende, Asertia buscar renovar su infraestructura tecnología e implementar una red de accesos WAN que maneje eficientemente los recursos de red. Realizar una solución SD-WAN en las empresas genera un alto grado de independencia y control, se obtiene un mejor nivel de seguridad en los distintos accesos corporativos, aparte que se puede priorizar el tipo de tráfico de conexión que se envía.

Para la recolección de información se utilizó la observación y el análisis de la red MPLS y SD-WAN con la finalidad de verificar si la solución SD-WAN optimizó el uso eficiente de los recursos de red en la empresa Asertia S. A.

3.13.1. Red WAN MPLS de Asertia.

La empresa tenía una red WAN basada en MPLS, para datos e internet con un solo proveedor. La interconexión entre las agencias y sucursal Matriz se realizaba a través de la red de datos de Alfanet que contaba con un router de borde en cada agencia que permitía conexión a la red MPLS del proveedor. En cada agencia había una topología de red jerárquica, que consta de un switch de core/acceso donde se conectaban los usuarios de dichas sucursales, no existía segmentación de red con VLANs. El acceso a internet desde las agencias se realizaba a través de la oficina matriz.

Matriz contaba con equipos de interconexión (switches) de core y acceso, esta red se encontraba segmentada con vlans para las distintas redes como red de servidores, telefonía, usuarios, adicional cuenta con un firewall pfSense (Sistema Operativo orientado a firewall) que se utiliza para el control de accesos de los usuarios corporativos a internet. Sus servicios de facturación (actualmente en nube) ERP y SAP se están planificando migrar a la nube. El principal problema que tenía Asertia era la falta de control y visibilidad de la utilización de los recursos de red, es decir en horas de mayor

afluencia el acceso a los servicios corporativos (sistemas de facturación local y en nube) estaban afectados, esto generaba retrasos y molestias en los clientes y usuarios corporativos. El acceso desde las sucursales hacia los servidores en matriz y en nube producía muchas perdidas de paquetes y latencia, el ingreso al aplicativo de facturación generaba errores y su tiempo de acceso era muy alto, debido a que la navegación a internet de los usuarios no contaba con ningún control de accesos hacia URL de gran consumo de ancho de banda esto generaba problemas que afectan al negocio de la empresa Asertia.

En la presente investigación se analizó el acceso a los servidores corporativos y en nube en base a la implementación de una solución SD-WAN y se verificará el uso eficiente de los recursos de red.

3.13.2. Diagrama de red WAN con MPLS Matriz y Sucursales de Asertia.

Se detalla el esquema lógico de la conexión WAN entre Matriz y sucursales de Asertia S. A.

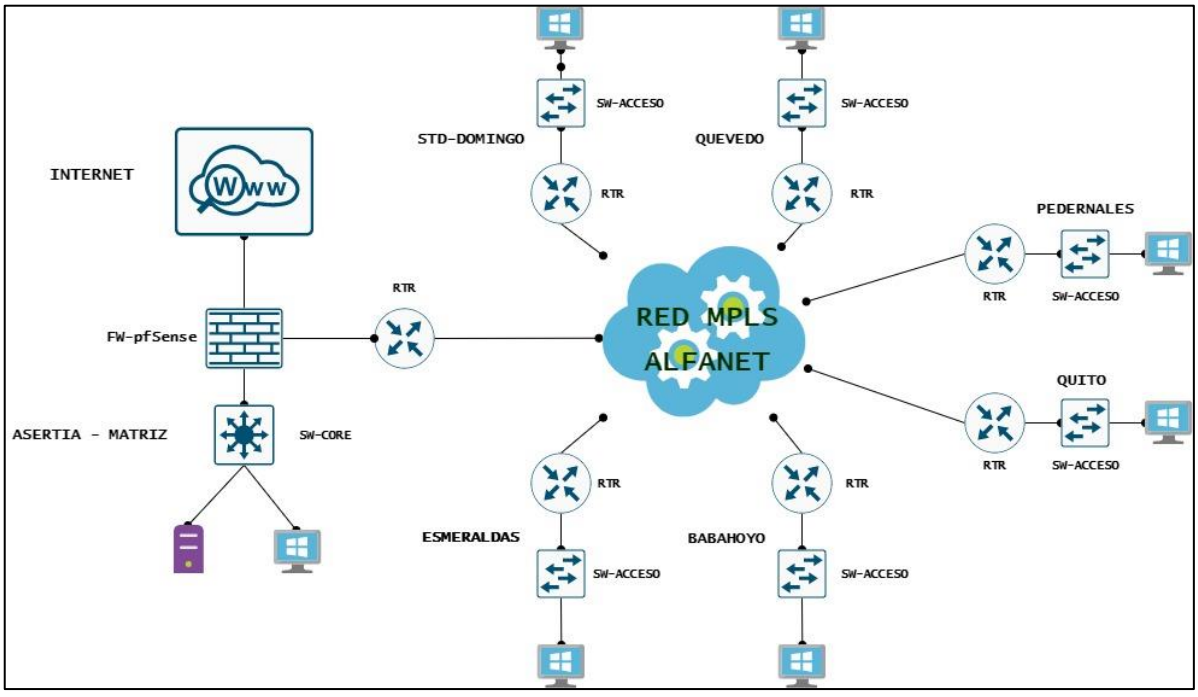


Figura 1-3: Diagrama lógico red WAN con MPLS
Realizado por: Heredia, J. 2022

3.13.3. Esquema lógico de matriz y sucursales en el escenario MPLS

Se detalla el esquema lógico de conexión en cada sucursal y Matriz.

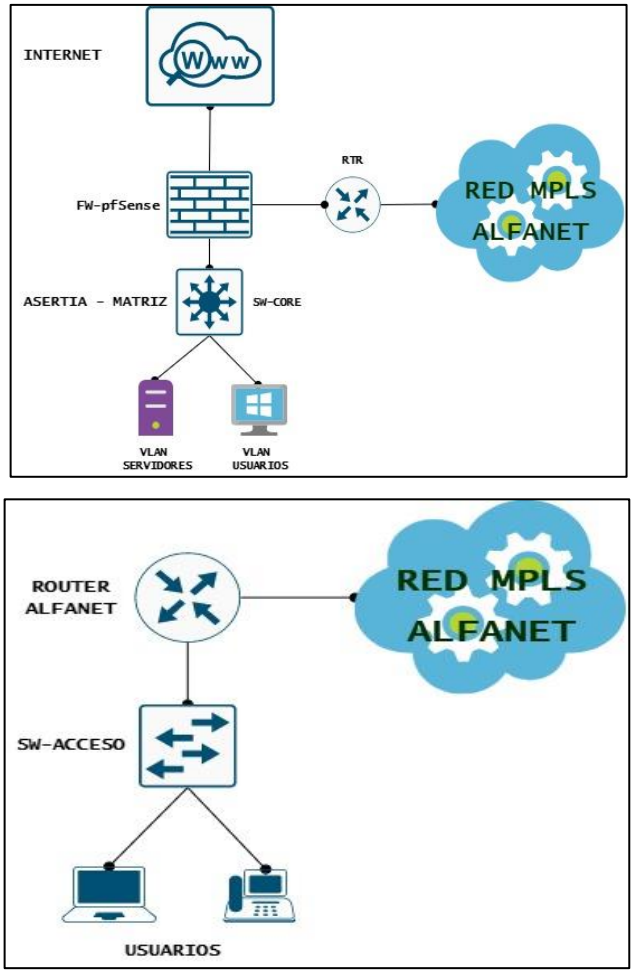


Figura 2-3: Esquema lógico matriz y sucursales
Realizado por: Heredia, J. 2022

3.14 Arquitectura de red de accesos SD-WAN de Asertia.

La solución SD-WAN permite a las empresas mejorar los servicios con orientación empresarial, la administración de red se simplifica y automatiza eliminando la complejidad y extensión de los dispositivos en sucursales, brinda acceso seguro a aplicaciones en la nube y SaaS y se obtiene mayor capacidad de ancho de banda y disponibilidad para aplicaciones, como IoT, VoIP, SaaS y servicios de seguridad perimetral.

3.14.1. Escenario red de accesos SD-WAN de Asertia.

Asertia Matriz y sucursales en la ejecución de la solución SD-WAN manejan equipos Fortigate y accesos de internet independientes en cada sucursal que reemplazan a los enlaces MPLS del proveedor. Matriz tiene dos enlaces hacia Internet que se manipulan para la interconexión con las sucursales y configuración de SD-WAN como se muestra en la figura 3-3.

Las sucursales tienen un servicio de internet independiente con su proveedor Alfanet, de la misma forma se utiliza equipos Fortigate, la interconexión con matriz está basada en SD-WAN con túneles VPN IPSec. Se aplica controles de seguridad de accesos hacia distintos aplicativos de internet, se prioriza el tráfico hacia el servidor de facturación local y en nube. Se puntualiza el esquema lógico de conexión entre Matriz y sucursales de Asertia S. A.

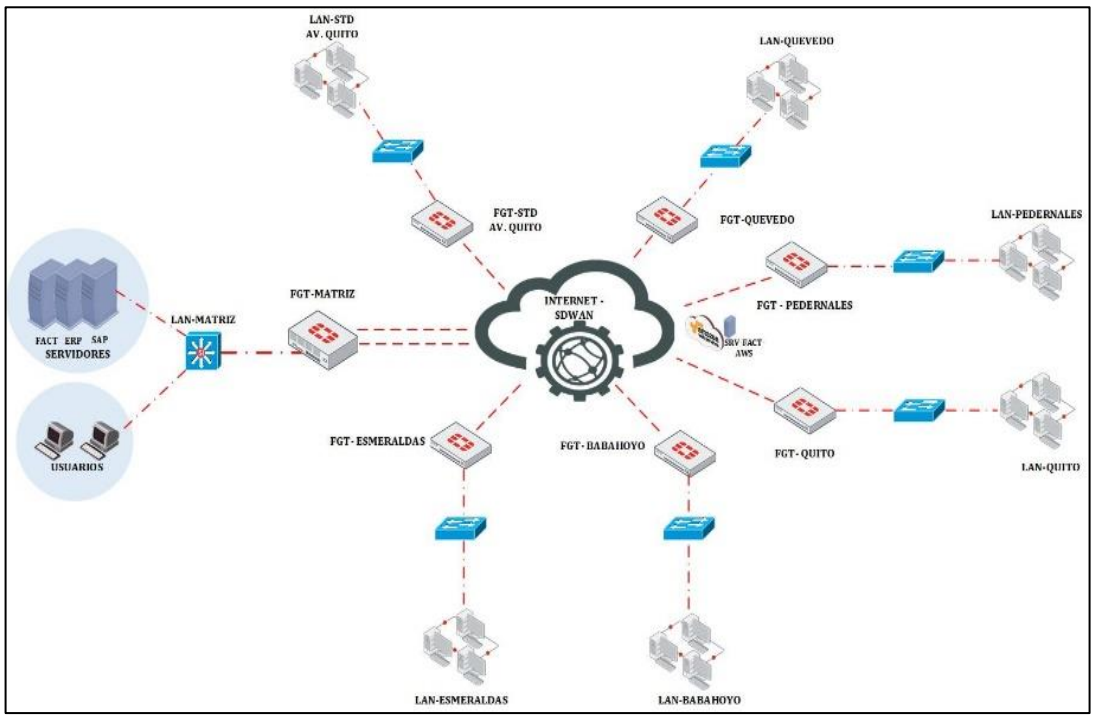


Figura 3-3: Diagrama lógico de red SD-WAN
Realizado por: Heredia, J. 2022

3.14.2 Direccionamiento de red SD-WAN Asertia

A continuación, se detalla el direccionamiento público y privado de Matriz y Sucursales en la implementación de SD-WAN.

Tabla 6-3: Direccionamiento de red SD-WAN

AGENCIA	DIRECCIONAMIENTO LAN	GATEWAY	DIRECCIONAMIENTO PUBLICO
MATRIZ	192.168.1.0/24	192.168.1.254	45.230.240.54
			181.39.76.82
STD-AV. QUITO	192.168.10.0/24	192.168.10.254	45.230.240.38
ESMERALDAS	192.168.20.0/24	192.168.20.254	45.224.153.130
QUEVEDO	192.168.30.0/24	192.168.30.254	45.169.144.70
PEDERNALES	192.168.40.0/24	192.168.40.254	45.169.144.206
QUITO	192.168.50.0/24	192.168.50.254	45.230.240.34
BABAHOYO	192.168.60.0/24	192.168.60.254	45.230.240.58

Realizado por: Heredia, J. 2022

3.15 Análisis de escenarios MPLS y SD-WAN para el uso eficiente de recursos de red.

3.15.1 Recopilación de Datos

El presente trabajo de investigación se verificará el uso eficiente de los recursos de red, con la ejecución de la solución SD-WAN en comparación con la red MPLS tradicional que tenía la empresa. Se recopiló los datos de latencia de red y pérdida de paquetes en el acceso al servidor de facturación local y en nube durante las horas pico de trabajo.

Los datos fueron recolectados en horarios de 09h00 – 10h00 y 16h30 – 17h30 en distintos días de trabajo. A la red WAN MPLS se le denominó Escenario 1 y a la red SD-WAN se denominó Escenario 2. Los equipos involucrados en este proceso son los siguientes:

Tabla 7-3: Equipos involucrados en la investigación

AGENCIA	HOST-AGENCIA	SERVIDOR LOCAL	SERVIDOR FACTURACIÓN NUBE
STD-SUCURSAL	192.168.10.50	192.168.110.100	40.117.188.104
ESMERALDAS	192.168.20.50	192.168.110.100	40.117.188.104
QUEVEDO	192.168.30.50	192.168.110.100	40.117.188.104
PEDERNALES	192.168.40.50	192.168.110.100	40.117.188.104
QUITO	192.168.50.50	192.168.110.100	40.117.188.104
BABAHOYO	192.168.60.50	192.168.110.100	40.117.188.104

Realizado por: Heredia, J. 2022

3.15.1.1 Latencia en la red

El análisis de la latencia se basó en el uso del comando ping desde el equipo de cada agencia hacia el servidor local SRV-FAC-MTR y al servidor en nube SRV-FAC-CITRIX. En los horarios de 9h00 – 10h00 y 16h30 – 17h30 se ejecutaron pruebas de ping en un tiempo de 40 minutos, se enviaron aproximadamente 2200 paquetes de 1400 bytes en el acceso hacia los dos servidores. Se efectuaron 8 pruebas en distintos días del mes por cada sucursal.

Tabla 8-3: Pruebas latencia hacia SRV-FACT-MTR

	Escenario 1 MPLS			**Escenario 2 SD-WAN**		
AGENCIA	**Min**	**Avg**	**Max**	**Min**	**Avg**	**Max**
Quito	45	63	81	31	36	54
	53	65	77	26	35	46
	57	66	80	33	37	44
	49	63	86	24	34	41
	53	63	74	29	38	53
	57	67	91	23	36	47
	61	69	94	31	37	50
	57	65	87	34	39	48
Esmeraldas	39	63	82	20	34	43
	49	65	91	26	41	51
	45	63	76	33	44	55
	50	67	89	29	36	47
	49	65	84	22	26	39
	52	70	98	32	38	45
	41	64	76	27	34	42
	51	65	74	18	27	37
Quevedo	45	64	74	26	34	47
	49	63	81	21	31	44
	44	65	95	24	33	58
	51	62	72	29	37	49
	46	59	69	36	42	65
	57	74	99	20	32	44
	52	59	67	27	39	43
	51	64	89	40	51	74
Pedernales	39	61	76	27	32	44
	41	57	77	18	32	53
	40	58	86	22	35	61

	55	67	96	32	39	47
	51	62	74	21	28	36
	43	53	62	19	28	41
	55	68	89	32	44	59
	38	51	62	23	29	41
Babahoyo	33	49	61	25	29	42
	37	51	76	19	28	39
	34	50	69	26	35	56
	41	54	84	22	30	43
	46	54	78	18	28	41
	39	48	63	19	29	51
	36	47	60	31	36	56
	44	52	60	19	29	40
SDT-SUCURSAL	44	55	87	27	35	53
	35	53	75	16	36	54
	35	50	67	23	33	43
	32	52	74	19	28	39
	49	62	91	23	29	41
	39	50	72	15	26	37
	36	44	59	26	35	59
	44	56	69	23	30	38

Realizado por: Heredia, J. 2022

Tabla 9-3: Pruebas latencia hacia SRV-FACT-CITRIX

	Escenario 1 MPLS			**Escenario 2 SD-WAN**		
AGENCIA	**Min**	**Avg**	**Max**	**Min**	**Avg**	**Max**
Quito	114	158	246	83	86	175
	96	151	234	68	71	190
	100	162	274	60	85	210
	99	164	286	67	101	187
	77	160	267	68	71	172
	92	155	233	60	64	192
	96	165	241	59	85	175
	104	162	236	68	71	129
Esmeraldas	116	164	238	54	87	167
	88	164	265	62	96	104
	156	167	219	68	87	124
	156	174	192	59	91	116
	120	160	207	63	92	140
	140	178	216	68	98	160

	168	190	212	62	80	121
	136	170	233	54	77	128
Quevedo	110	170	235	71	86	112
	102	165	224	70	89	144
	156	178	200	92	112	132
	98	159	219	69	88	136
	100	163	247	72	101	180
	95	156	210	84	126	168
	96	154	198	88	116	144
	100	160	218	68	87	116
Pedernales	84	109	156	60	61	82
	76	98	120	56	76	99
	100	106	112	54	69	90
	80	90	100	72	78	101
	76	80	84	57	70	87
	76	94	112	64	76	102
	80	82	84	80	100	120
	76	90	104	84	94	104
Babahoyo	96	108	155	62	74	102
	82	102	124	59	75	91
	116	130	144	59	69	86
	108	128	148	67	78	91
	104	118	132	58	66	79
	100	114	128	57	68	78
	96	98	100	63	70	91
	112	112	112	65	74	104
STD. SUCURSAL	104	124	144	61	71	99
	82	97	148	59	66	78
	79	95	134	60	67	87
	104	112	120	67	70	84
	100	110	120	54	65	79
	84	98	150	71	77	97
	72	89	133	56	76	96
	76	100	124	62	71	77

Realizado por: Heredia, J. 2022

3.15.1.2 Perdida de paquetes

Con el análisis de latencia se logró la cantidad de paquetes perdidos durante las horas pico de trabajo en las mismas condiciones de análisis anterior.

Tabla 10-3: Perdidas de paquetes hacia SRV-FACT-MTR

	Escenario 1 MPLS		Escenario 2 SD-WAN	
AGENCIA	**Cantidad**	**%**	**Cantidad**	**%**
Quito	528	24	2	0,09
	704	32	5	0,23
	308	14	1	0,05
	374	17	9	0,41
	770	35	9	0,41
	1232	56	4	0,18
	462	21	17	0,77
	264	12	9	0,41
Esmeraldas	594	27	0	0,00
	792	36	4	0,18
	1584	72	10	0,45
	682	31	24	1,09
	330	15	10	0,45
	748	34	16	0,73
	990	45	19	0,86
	418	19	0	0,00
Quevedo	484	22	16	0,73
	594	27	11	0,50
	1210	55	1	0,05
	836	38	7	0,32
	506	23	14	0,64
	462	21	9	0,41
	1540	70	2	0,09
	748	34	8	0,36
Pedernales	220	10	0	0,00
	330	15	2	0,09
	154	7	6	0,27
	198	9	0	0,00
	506	23	2	0,09
	528	24	9	0,41
	286	13	2	0,09
	220	10	1	0,05
Babahoyo	242	11	4	0,18
	110	5	1	0,05
	264	12	0	0,00
	462	21	8	0,36
	308	14	2	0,09
	66	3	8	0,36
	176	8	10	0,45

	550	25	15	0,68
STD. SUCURSAL	462	21	8	0,36
	352	16	36	1,64
	198	9	29	1,32
	308	14	43	1,95
	638	29	12	0,55
	44	2	2	0,09
	396	18	1	0,05
	286	13	6	0,27

Realizado por: Heredia, J. 2022

Tabla 11-3: Perdidas de paquetes hacia SRV-FACT-CITRIX

	Escenario 1 MPLS		**Escenario 2 SD-WAN**	
AGENCIA	**Cantidad**	**%**	**Cantidad**	**%**
Quito	1034	47	6	0,27
	704	32	12	0,55
	638	29	8	0,36
	946	43	22	1,00
	550	25	4	0,18
	726	33	11	0,50
	396	18	30	1,36
	770	35	16	0,73
Esmeraldas	352	16	4	0,18
	946	43	9	0,41
	594	27	12	0,55
	264	12	35	1,59
	880	40	11	0,50
	638	29	23	1,05
	1364	62	24	1,09
	374	17	0	0,00
Quevedo	704	32	27	1,23
	528	24	19	0,86
	1012	46	5	0,23
	462	21	10	0,45
	396	18	17	0,77
	286	13	12	0,55
	682	31	6	0,27
	638	29	9	0,41
Pedernales	616	28	1	0,05
	418	19	4	0,18
	242	11	8	0,36
	154	7	1	0,05

	374	17	3	0,14
	748	34	12	0,55
	308	14	8	0,36
	550	25	2	0,09
Babahoyo	374	17	14	0,64
	198	9	3	0,14
	264	12	1	0,05
	528	24	17	0,77
	374	17	6	0,27
	176	8	9	0,41
	242	11	12	0,55
	726	33	24	1,09
STD. SUCURSAL	924	42	14	0,64
	594	27	98	4,45
	396	18	46	2,09
	594	27	54	2,45
	748	34	21	0,95
	198	9	8	0,36
	550	25	2	0,09
	396	18	7	0,32

Realizado por: Heredia, J. 2022

CAPÍTULO IV

4. PRESENTACIÓN DE RESULTADOS

En el presente capítulo se muestran los resultados obtenidos del análisis y procesamiento de los datos en base a las mediciones realizadas para los indicadores: latencia y perdida de paquetes.

Con la finalidad de generar el diagnóstico de los escenarios MPLS y SD-WAN se utilizó un análisis exploratorio de datos de acuerdo con la latencia y la pérdida de paquetes de información durante las pruebas de conectividad elaboradas entre las sucursales y el servidor de facturación local y en nube.

4.1. Análisis de riesgos informáticos en la red MPLS

Con base a la información recopilada de la red MPLS se evidencian varios riesgos a nivel de seguridad porque la navegación a internet de los usuarios corporativos no tiene ningún control de accesos, es decir tiene libre acceso ej.: Proxys, P2P, Youtube, Spotify, Facebook, descargas, Netflix, etc., esto genera un consumo elevado de ancho de banda y por ende problemas en el ingreso al aplicativo de facturación tanto local como en la nube (CITRIX).

4.1.1. Consumo de Ancho de banda

En las Figuras 1-4, 2-4, 3-4 muestran el consumo de ancho de banda y saturación del enlace MPLS de las sucursales.

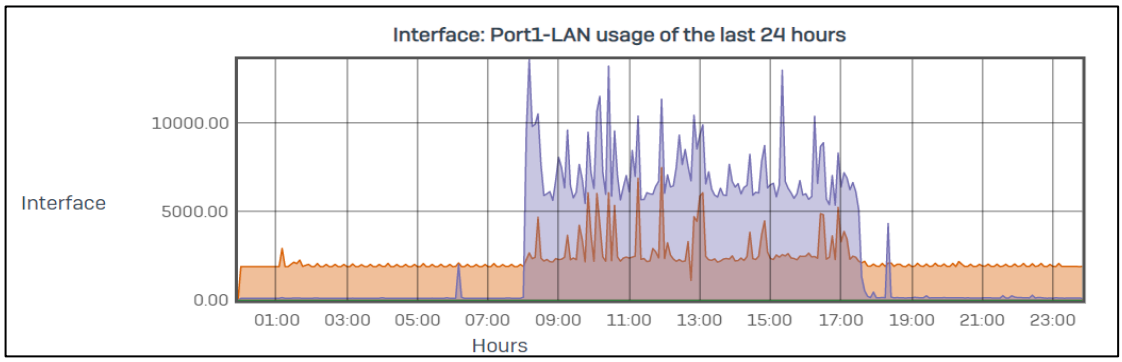


Figura 1-4: Consumo ancho de banda de sucursal Quito
Realizado por: Heredia, J. 2022

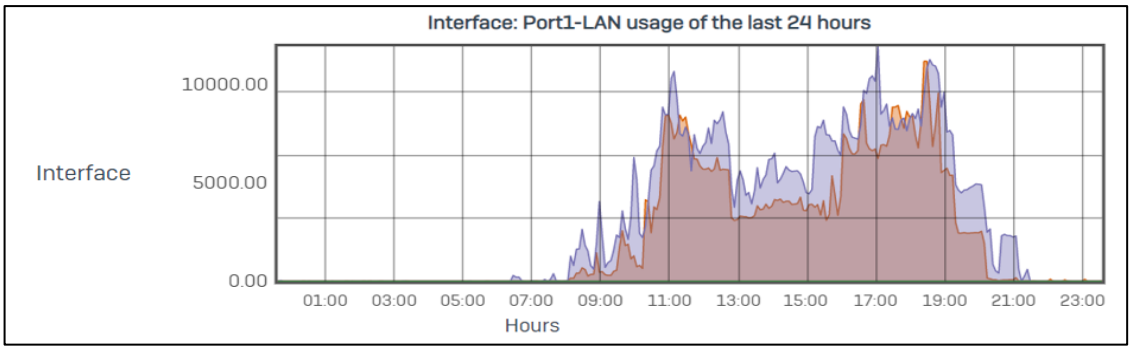


Figura 2-4: Consumo ancho de banda de sucursal Quevedo
Realizado por: Heredia, J. 2022

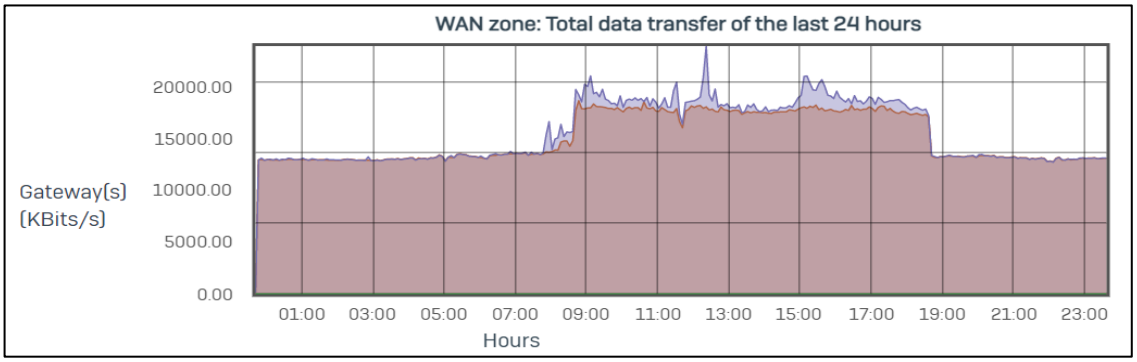


Figura 3-4: Consumo ancho de banda de INTERNET
Realizado por: Heredia, J. 2022

4.1.2. Ingreso a distintas URLs

Los usuarios corporativos tienen navegación a internet sin restricciones, en las Figuras 4-4, 5-4, 6-4, descubren el acceso a distintas páginas de música, videos, descargas, proxys, etc.

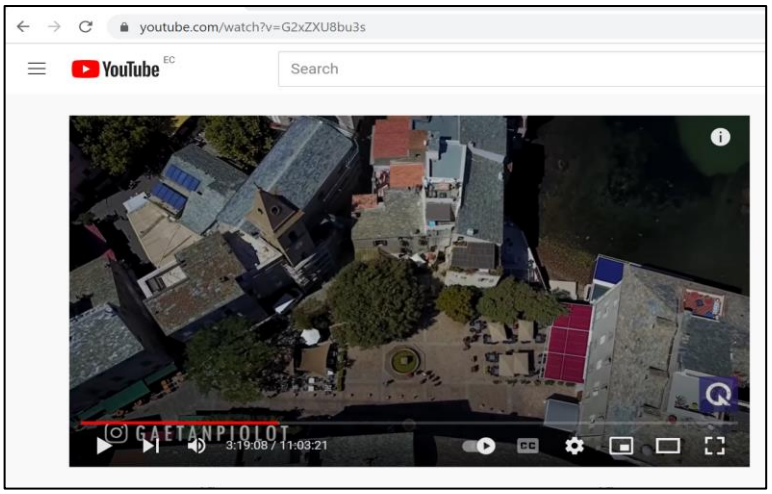


Figura 4-4: Ingreso páginas de videos
Realizado por: Heredia, J. 2022

Figura 5-4: Ingreso páginas de películas
Realizado por: Heredia, J. 2022

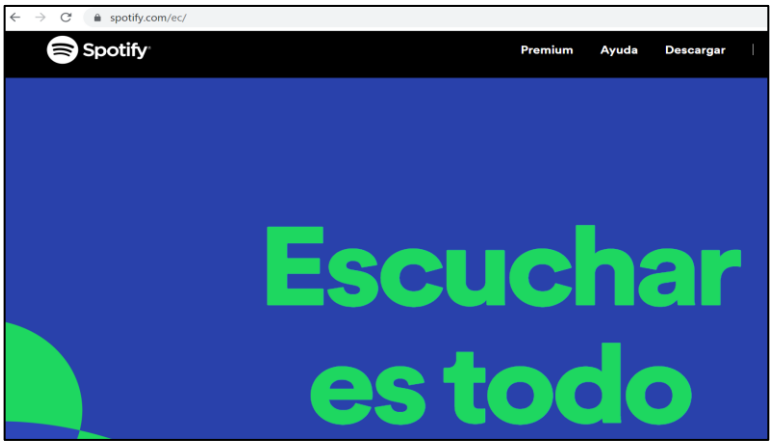


Figura 6-4: Ingreso páginas de música
Realizado por: Heredia, J. 2022

4.1.3. Problemas en el acceso al aplicativos de facturación

El acceso sin restricciones que tienen las sucursales a internet genera problemas de un alto consumo de ancho de banda que afecta el ingreso al aplicativo de facturación como nos muestra la Figura 7-4.

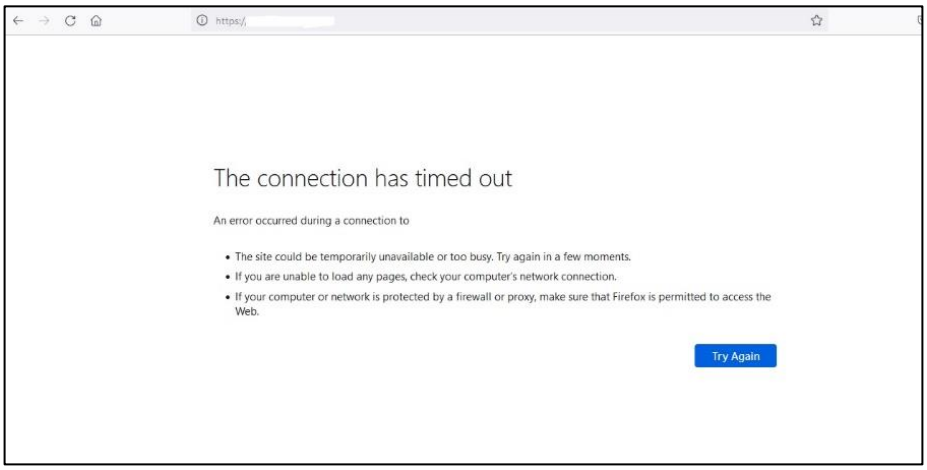


Figura 7-4: Problemas en el acceso al aplicativos de facturación
Realizado por: Heredia, J. 2022.

4.2. Indicadores

En la presente investigación se han estimado cada uno de los indicadores y en esta sección se muestran los resultados obtenidos.

4.2.1 Latencia

Elaborado el procesamiento de datos de las pruebas realizadas para los escenarios 1 MPLS y 2 SD-WAN, la Tabla 1-4 nos muestra los resultados obtenidos del indicador y nos indica que arquitectura WAN presenta mejores valores de latencia.

Tabla 1-4: Resultados Indicador: Latencia

Latencia	Estadísticos		Escenario MPLS	Escenario SD-WAN
Local	Media		59,93 ms	33,98 ms
	IC para la media al 95%	LI	57,90 ms	32,51 ms
		LS	61,97 ms	35,45 ms
Nube	Media		128,11 ms	81,94 ms
	IC para la media al 95%	LI	126,11 ms	77,85 ms
		LS	145,37 ms	86,03 ms

Realizado por: Heredia, J. 2022

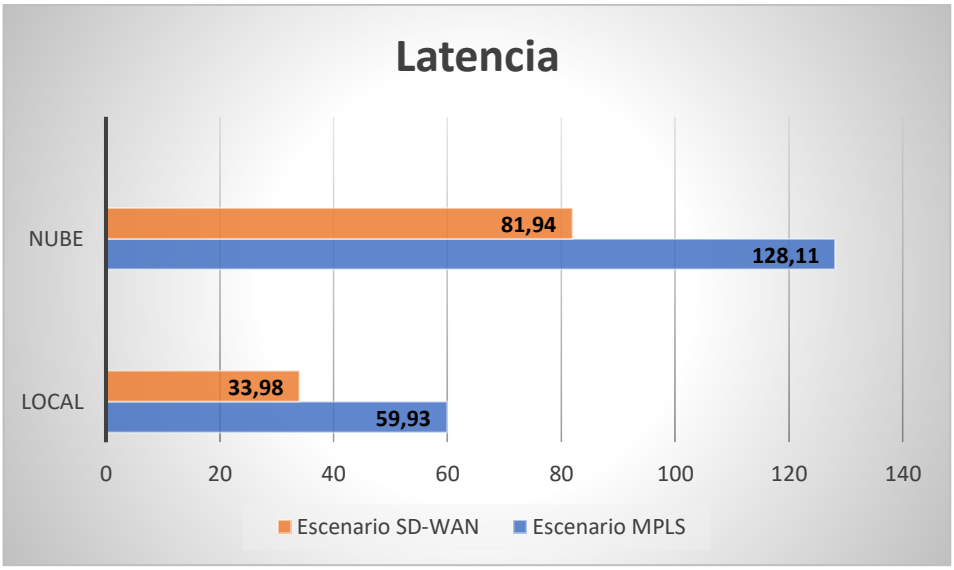


Gráfico 1-4: Promedio de Latencia
Realizado por: Heredia, J. 2022

La latencia local evidenció que, el escenario MPLS utilizó un tiempo promedio de 59,93ms, de acuerdo con el intervalo de confianza pudo variar entre 57,90 y 61,97ms; con el escenario SD-WAN, en cambio se evidenció un decremento significativo, su

latencia promedio fue de 33,98 ms, de acuerdo con el intervalo de confianza pudo variar entre 32,51 y 35,45ms. En cuanto a la latencia en la nube se mantuvo el patrón local, el escenario MPLS utilizó un tiempo de 128,11ms con un rango de variación entre 126,11 y 145,37ms, mientras que, el escenario SD-WAN el tiempo fue de 81,94ms con un rango de variación entre 77,85 y 86,03ms.

4.2.2 Pérdidas de paquetes

Después del análisis realizado se determinó que las pérdidas de paquetes en cada una de las pruebas tienen una diferencia estadísticamente significativa para los escenarios 1 MPLS y 2 SD-WAN, en la Tabla 4-2 se detalla los resultados obtenidos.

Tabla 2-4: Resultados Indicador: Cantidad de Pérdida de Paquetes

Pérdidas de paquetes	Estadísticos		Escenario MPLS	Escenario SD-WAN
Locales	Media		517	22
	IC para la media al 95%	LI	412	3
		LS	622	41
Nube	Media		557	33
	IC para la media al 95%	LI	477	6
		LS	637	60

Realizado por: Heredia, J. 2022

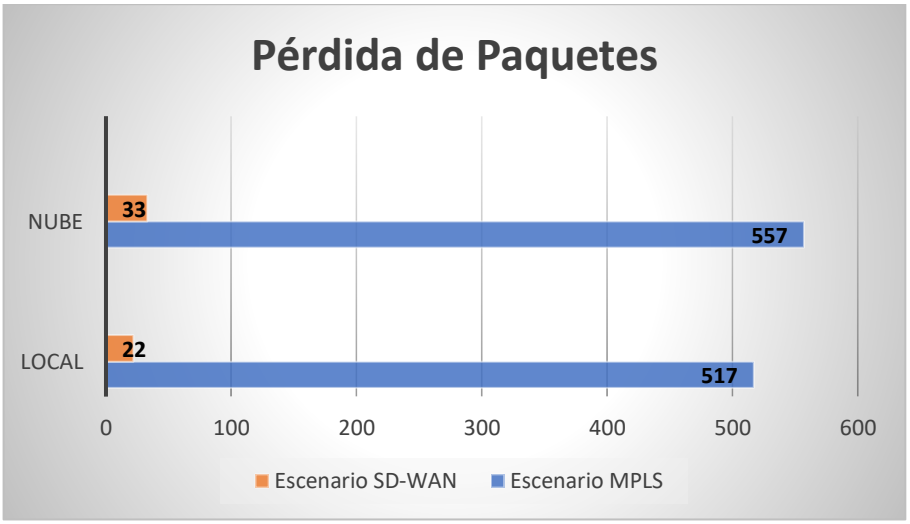


Gráfico 2-4: Promedio de Pérdida de Paquetes
Realizado por: Heredia, J. 2022

Con respecto a la cantidad de pérdida de paquetes locales se observó que, el escenario MPLS en promedio perdió 517 paquetes, de acuerdo con el intervalo de confianza pudo variar entre 412 y 622 paquetes; con el escenario SD-WAN en cambio se evidenció un

decremento significativo, su promedio de pérdida fue de 22 paquetes, de acuerdo con el intervalo de confianza pudo variar entre 3 y 41 paquetes. En cuanto a la pérdida de paquetes en la nube se mantuvo el patrón local, el escenario MPLS perdió 557 paquetes con un rango de variación entre 477 y 637 paquetes, mientras que, el escenario SD-WAN perdió 33 paquetes con un rango de variación entre 6 y 60 paquetes.

Seguido se ejecutaron pruebas de normalidad para elegir técnicas paramétricas o no paramétricas inferenciales que permitieron comprobar las diferencias significativas entre los escenarios MPLS y SD-WAN, para el análisis se utilizó el contraste de Shapiro Wilk por su potencia para estudio de muestras inferiores a 50 datos.

4.2.3 Pruebas de Normalidad

El estudio de normalidad trabajó con una significancia del 5%.

Tabla 3-4: Pruebas de Normalidad-Latencia

Latencia	Escenario	Shapiro-Wilk		
		Estadístico	gl	p-value
Locales	Escenario MPLS	0,93	46	0,01
	Escenario SD-WAN	0,95	50	0,02
Nube	Escenario MPLS	0,89	46	0,01
	Escenario SD-WAN	0,92	50	0,01

Realizado por: Heredia, J. 2022

Las variables de latencia local y en la nube en los escenarios MPLS y SD-WAN no se ajustaron a una distribución normal, los valores de probabilidad (0,01; 0,02; 0,01; 0,01) fueron inferiores al 5% de significancia.

Tabla 4-4: Pruebas de Normalidad-Pérdidas de Paquetes

Pérdidas de paquetes	Escenario	Shapiro-Wilk		
		Estadístico	gl	p-value
Locales	Escenario MPLS	0,88	46	0,02
	Escenario SD-WAN	0,30	50	0,01
Nube	Escenario MPLS	0,95	46	0,07
	Escenario SD-WAN	0,32	50	0,01

Realizado por: Heredia, J. 2022

Las variables de pérdidas de paquetes locales y en la nube en los escenarios MPLS y SD-WAN no se ajustaron a una distribución normal, los valores de probabilidad (0,02; 0,01; 0,07; 0,01) fueron inferiores al 5% de significancia.

4.2.4 Comprobación de hipótesis

Los resultados anteriores derivaron a la selección de una prueba no paramétrica denominada U de Mann Whitney para analizar las diferencias significativas entre los escenarios de estudio; el contraste trabajó con un nivel de significancia del 5% bajo las siguientes hipótesis:

Ho: *La implementación de una solución SD-WAN en la empresa Asertia no optimizará el uso eficiente de los recursos de red en el acceso hacia las aplicaciones corporativas*

H_1: *La implementación de una solución SD-WAN en la empresa Asertia optimizará el uso eficiente de los recursos de red en el acceso hacia las aplicaciones corporativas*

Para la comprobación de la hipótesis se utilizó el promedio de latencia local y en la nube, así como también el promedio de pérdidas de paquetes tanto locales como en la nube. La elección de la hipótesis depende del valor de probabilidad, si es menor que el nivel de significancia se rechaza la hipótesis nula (H_0) caso contrario no se rechaza.

Tabla 5-4: Comprobación de la Hipótesis

Estadísticos de contraste[a]				
	Latencia local	Latencia nube	Pérdidas de paquetes locales	Pérdidas de paquetes en la nube
U de Mann-Whitney	7,000	141,500	32,500	39,500
W de Wilcoxon	1282,000	1416,500	1307,500	1314,500
Z	-8,389	-7,398	-8,200	-8,147
Sig. asintót. unilateral	,000	,000	,000	,000

Realizado por: Heredia, J. 2022

Como todos los valores de probabilidad fueron inferiores al 5% de significancia se rechaza la H_O.

Lo que evidenció que el tiempo de latencia local y en la nube de escenario MPLS es superior al tiempo del escenario SD-WAN, así también sucedió con las pérdidas de paquetes tanto para el servidor local como el servidor en la nube se generó mayor perdida en escenario MPLS; por tanto, la implementación de una solución SD-WAN en la empresa Asertia optimizó el uso eficiente de los recursos de red en el acceso hacia las aplicaciones corporativas y en el uso de internet.

CAPITULO V

5. PROPUESTA

La empresa Asertia está conformada por su oficina Matriz y sucursales en Esmeraldas, Quevedo, Babahoyo, Pedernales, Santo Domingo Av. Quito, Quito, por lo que este capítulo detalla los requerimientos y pasos a seguir en la implementación de la solución SD-WAN.

5.1 Topología de red para la implementación de la solución SD-WAN

En base al crecimiento y necesidades de la empresa se detalla el diagrama de red utilizado para la implementación de la solución SD-WAN en Asertia.

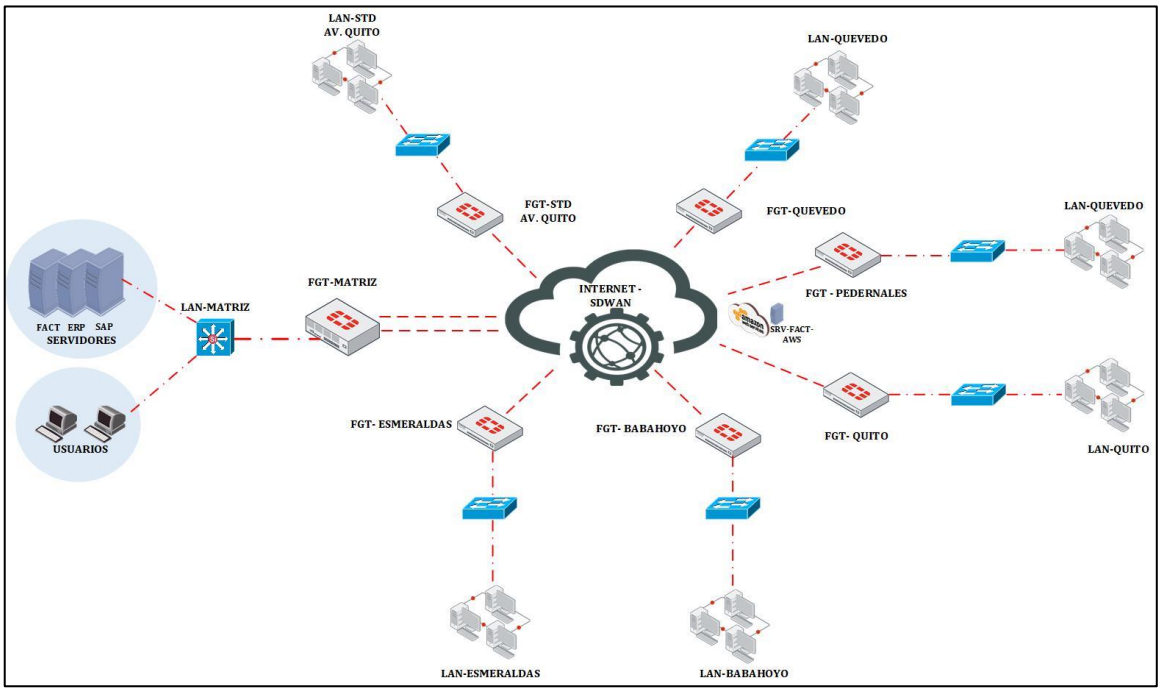


Figura 1-5: Diagrama de red para implementación de solución SD-WAN en Asertia
Realizado por: Heredia, J. 2022

5.2 Descripción de la implementación de la solución SD-WAN

En la ejecución de la solución SD-WAN en Asertia fueron utilizados equipos Fortigate, en matriz se manejó dos proveedores de internet Alfanet y Telconet, mientras que en cada sucursal se interconectaron utilizando Alfanet. Desde la oficina Matriz se tiene conectividad hacia las sucursales mediante túneles VPN IPSEC de forma redundante.

A continuación, se detalla los equipos utilizados para la implementación:

Tabla 1-5: Equipos Fortigate con serie.

SUCURSAL	MODELO	SERIE
MATRIZ	Fortigate 100E	FG100ETK18031194
		FG100ETK19031597
SANTO DOMINGO	Fortigate 60F	FGT60FTK19013876
ESMERALDAS	Fortigate 60F	FGT60FTK19013268
QUEVEDO	Fortigate 60F	FGT60FTK19013501
PEDERNALES	Fortigate 60F	FGT60FTK20076260
QUITO	Fortigate 60F	FGT60FTK19015164
BABAHOYO	Fortigate 60F	FGT60FTK19014985

Realizado por: Heredia, J. 2022

5.3 Direccionamiento y Nomenclatura

En la Tabla 2-5, se detalla las redes de Matriz y sucursales, la asignación de direccionamiento IP Publico para cada sucursal y la IP asignada al firewall Fortigate. Los equipos que forman parte de una red deben mantener una nomenclatura que identifique el rol o función que desempeña en la red y su ubicación geográfica, por lo cual para una mejor administración se estableció la siguiente nomenclatura para los firewalls Fortigate.

Tabla 2-5: Direccionamiento.

SUCURSAL	NOMENCLATURA	DIRECCIONAMIENTO PUBLICO	DIRECCIONAMIENTO PRIVADO
MATRIZ	FGT-MTR-ASERTIA	45.230.240.54	192.168.1.254
		181.39.76.82	
SANTO DOMINGO	FGT-STD-ASERTIA	45.230.240.38	192.168.10.254
ESMERALDAS	FGT-ESM-ASERTIA	45.224.153.130	192.168.20.254
QUEVEDO	FGT-QVO-ASERTIA	45.169.144.70	192.168.30.254
PEDERNALES	FGT-PDN-ASERTIA	45.169.144.206	192.168.40.254
QUITO	FGT-STD-ASERTIA	45.230.240.58	192.168.50.254
BABAHOYO	FGT-UIO-ASERTIA	45.230.240.34	192.168.60.254

Realizado por: Heredia, J. 2022

5.4 Configuración de las interfaces WAN y LAN en equipo Fortigate

En la configuración WAN y LAN se asigna el direccionamiento establecido en la Figura 2-5, está configuración es necesaria para luego poder realizar la SD-WAN, a continuación, se mostrará un ejemplo de cómo se realiza la configuración de la WAN y la LAN vía WebGUI y por medio de comandos en la matriz y sucursales.

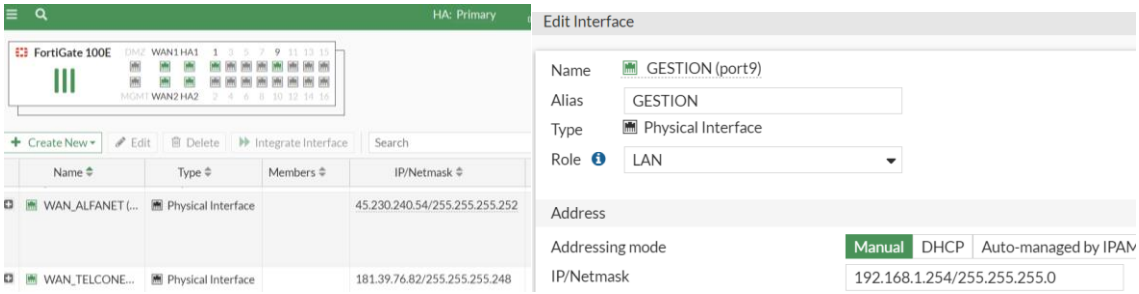


Figura 2-5: Asignación IP WAN y LAN -Matriz
Fuente: Heredia, J. 2022

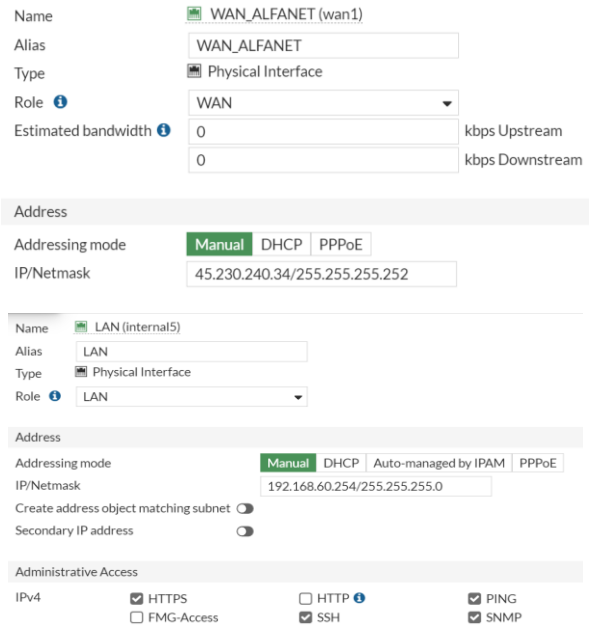


Figura 3-5: Asignación IP WAN y LAN – Babahoyo
Fuente: Heredia, J. 2022

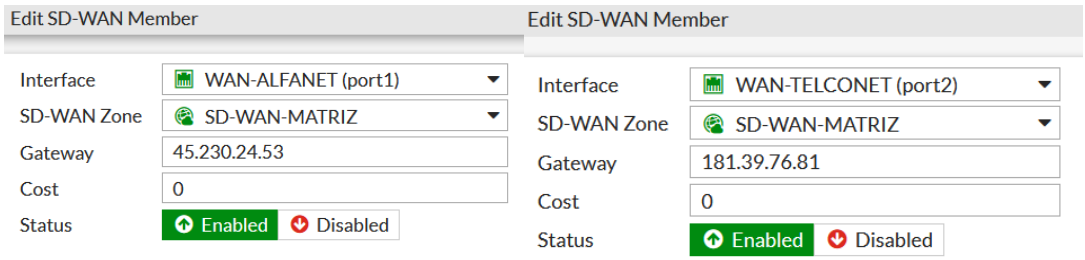
```
FGT-ESM-ASERTIA (interface) # show
config system interface
    edit "port1"
        set vdom "root"
        set ip 45.224.153.130 255.255.255.252
        set allowaccess ping https ssh http
        set type physical
        set alias "WAN-ALFANET"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 192.168.20.254 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "LAN-ESMERALDAS"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 3
    next
```

Figura 4-5: Asignación IP WAN y LAN – Esmeraldas vía CLI
Realizado por: Heredia, J. 2022

5.5 Configuración SD-WAN

SD-WAN debe estar habilitado y las interfaces miembros deben ser seleccionadas y añadidas a una zona. Las interfaces FortiGate seleccionadas consiguen ser de cualquier tipo (físicas, agregadas, VLAN, IPsec y otras), pero deben eliminarse de cualquier otra configuración en el FortiGate.

En este paso, se configuran dos interfaces (WAN Alfanet e WAN Telconet) y se añaden a la zona SD-WAN llamada SD-WAN-INTERNET como interfaces miembros de SD-WAN. Se puede utilizar mezcla de direcciones IP estáticas y dinámicas; para la implementación solamente se utilizó direccionamiento estático asignado por los proveedores. Una vez creados los miembros de la SD-WAN y añadidos a una zona, ésta puede utilizarse en distintas configuraciones como políticas, enrutamiento, etc.



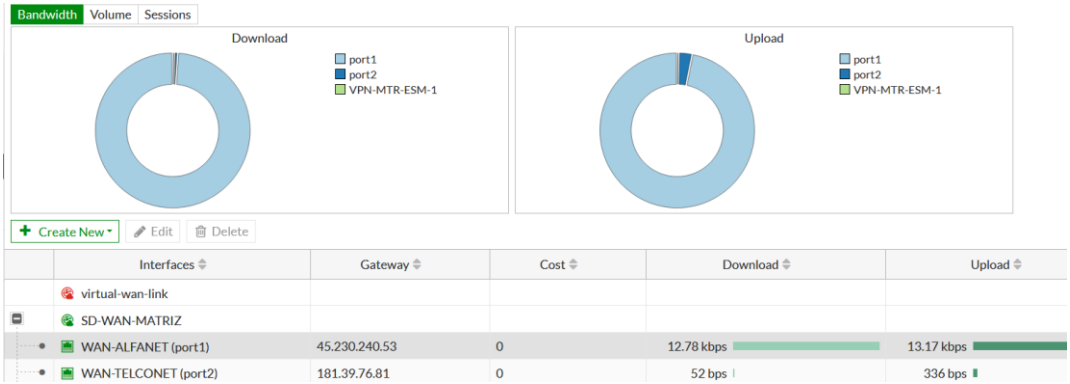


Figura 5-5: SD-WAN Interfaces
Realizado por: Heredia, J. 2022

5.5 Configuración enrutamiento estático

Debe configurar una ruta por defecto para la SD-WAN, esta configuración sirve para enrutar el tráfico hacia internet, no es necesario definir las puertas de enlace por defecto para cada interfaz miembro de la SD-WAN en la tabla de rutas estáticas. FortiGate decidirá qué ruta o rutas se prefieren utilizando Equal Cost Multi-Path (ECMP) en función de la distancia y la prioridad.

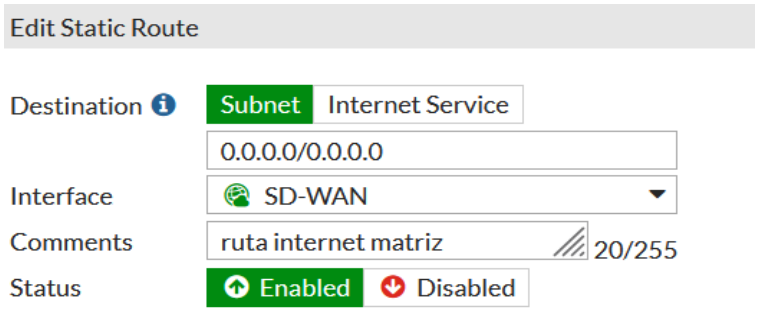


Figura 6-5: Configuración de rutas hacia Internet por SD-WAN
Realizado por: Heredia, J. 2022

5.6 Configuración del SLA en Asertia Matriz y Sucursales.

El monitoreo de enlaces se realiza mediante un SLA de rendimiento (Performance SLA), que comprueba el estado de los enlaces que pertenecen a la zona SD-WAN enviando señales de sondeo a un servidor para el caso de Internet (8.8.8.8) y para la conexión Matriz-Sucursales se creó interfaces loopback esto sirve para medir la calidad del enlace basado en **latencia**, **perdida de paquetes** y jitter. Si un enlace falla, la ruta de ese enlace se eliminará y el tráfico se redirigirá hacia los otros enlaces. El enrutamiento se volverá a habilitar cuando se restablezca el enlace. Esto evita que el tráfico se envíe por un enlace

que presente deterioro o falla en su rendimiento, estas configuraciones utilizan para optimizar los recursos de red de Asertia S. A.

Al crear un SLA de rendimiento se maneja el protocolo ping, si el ping falla según las métricas definidas, las rutas de la interfaz con problemas se eliminan y el tráfico se enruta hacia la otra interfaz disponible. Se maneja el protocolo ping, pero también podrían utilizarse otros protocolos como DNS, HTTP.

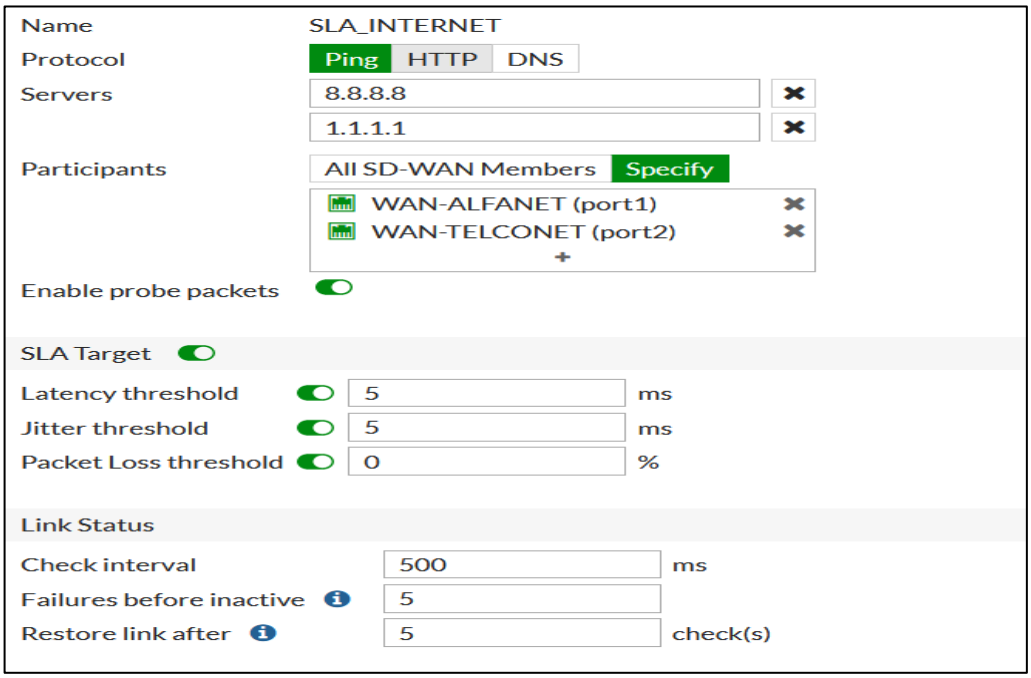


Figura 7-5: Configuración de performance SLA del SD-WAN Matriz y Sucursales
Realizado por: Heredia, J. 2022

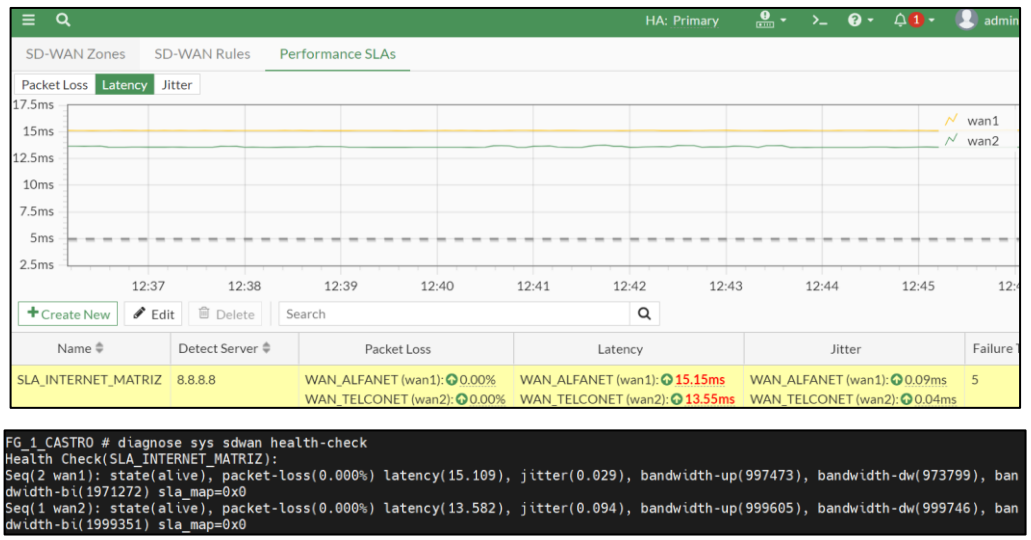


Figura 8-5: Visualización del monitoreo performance SLA
Realizado por: Heredia, J. 2022

5.7 SD-WAN rule

Las reglas SD-WAN establecen el comportamiento para la selección del mejor enlace. Una vez realizado el SLA de rendimiento se configuran las reglas para que el tráfico tome el enlace con menor latencia como se muestra en la Figura 8-5, estas reglas están basadas en las necesidades empresariales, es decir, como destino se puede ingresar segmentos de red o aplicaciones que son de mayor uso. La mejor ruta va a ser tomada de acuerdo con el monitoreo que realiza constantemente hacia el Internet.

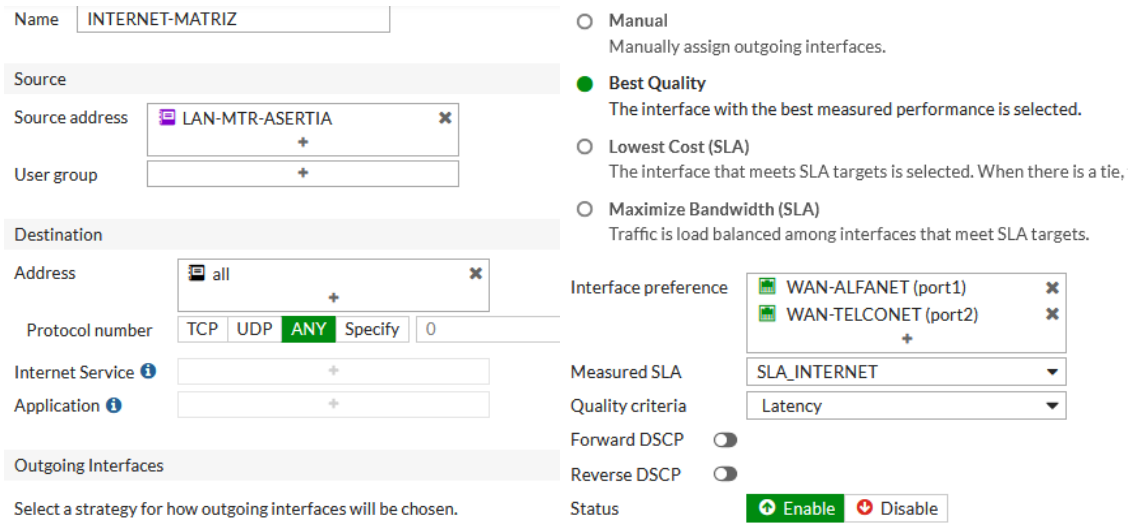


Figura 9-5: Configuración de la regla SD-WAN
Realizado por: Heredia, J. 2022

5.8 SEGURIDAD DE ACCESOS A LOS APLICATIVOS

5.8.1 Configuración de túneles IPSec para la comunicación entre Matriz y Sucursales.

En la comunicación entre matriz y las sucursales de la empresa Asertia S.A. se utilizan túneles IPSec. Estos túneles proporcionan seguridad, confiabilidad y disponibilidad para formar la comunicación de datos entre las oficinas de la empresa. Los túneles que se crean se encapsularan en la SD-WAN para entrar a ser parte de la red con alta disponibilidad.

La oficina matriz dispone de dos enlaces de Internet (Alfanet(1)y Telconet(2)), las sucursales por el momento disponen de un solo proveedor de Internet (Alfanet) por lo tanto se configuraron dos túneles IPSec por cada oficina. Como referencia se tiene la siguiente nomenclatura: VPN-MTR-SUC-1 y VPN-MTR-SUC-2 para matriz y para las agencias VPN-SUC-MTR-1 y VPN-SUC-MTR-2, donde los números identifican los

proveedores de internet. Para las VPNs IPSec se estableció utilizar el siguiente direccionamiento para los túneles punto a punto

Tabla 3-5: Direccionamiento túneles IPSec

NOMENCLATURA	DIRECCIONAMIENTO MATRIZ	DIRECCIONAMIENTO SUCURSAL	SUCURSAL
VPN-MTR-STD-1	10.10.10.1/25	10.10.10.126/25	SANTO DOMINGO
VPN-MTR-STD-2	10.10.10.129/25	10.10.10.254/25	
VPN-MTR-ESM-1	10.10.20.1/25	10.10.20.2/25	ESMERALDAS
VPN-MTR-ESM-2	10.10.20.129/25	10.10.20.130/25	
VPN-MTR-QDO-1	10.10.30.1/25	10.10.30.2/25	QUEVEDO
VPN-MTR-QDO-2	10.10.30.129/25	10.10.30.130/25	
VPN-MTR-PDN-1	10.10.40.1/25	10.10.40.2/25	PEDERNALES
VPN-MTR-PDN-2	10.10.40.129/25	10.10.40.130/25	
VPN-MTR-UIO-1	10.10.50.1/25	10.10.50.2/25	QUITO
VPN-MTR-UIO-2	10.10.50.129/25	10.10.50.130/25	
VPN-MTR-BHO-1	10.10.60.1/25	10.10.60.2/25	BABAHOYO
VPN-MTR-BHO-2	10.10.60.129/25	10.10.60.130/25	

Realizado por: Heredia, J. 2022

La configuración de las VPNs IPSec garantiza un acceso seguro a los recursos locales, se maneja una clave compartida (Preshared-key) y los algoritmos utilizados en la creación de las VPNs se basan en las mejores prácticas que nos indica Fortinet.

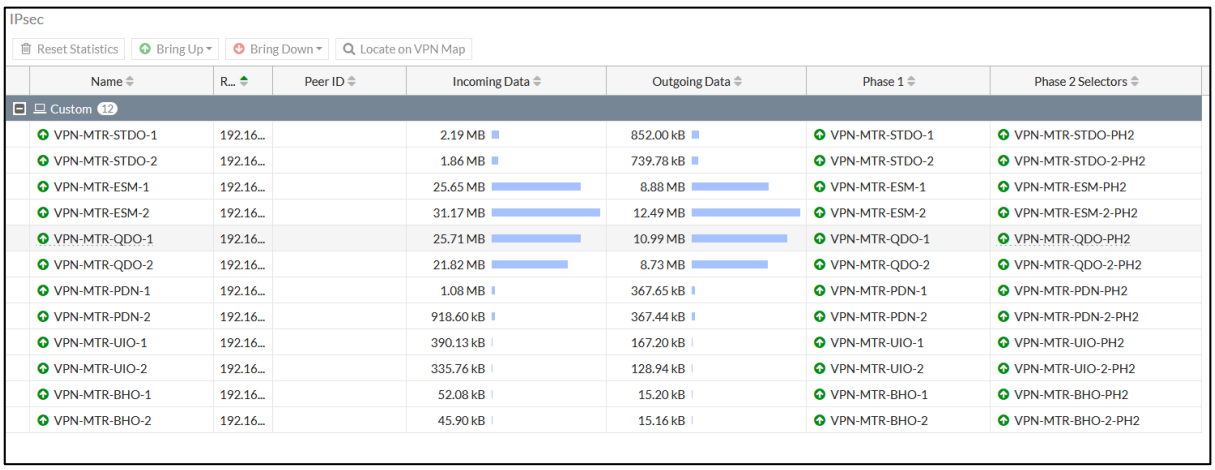


Figura 10-5: Visualización de estado de los túneles en Matriz
Fuente: Heredia, J. 2022

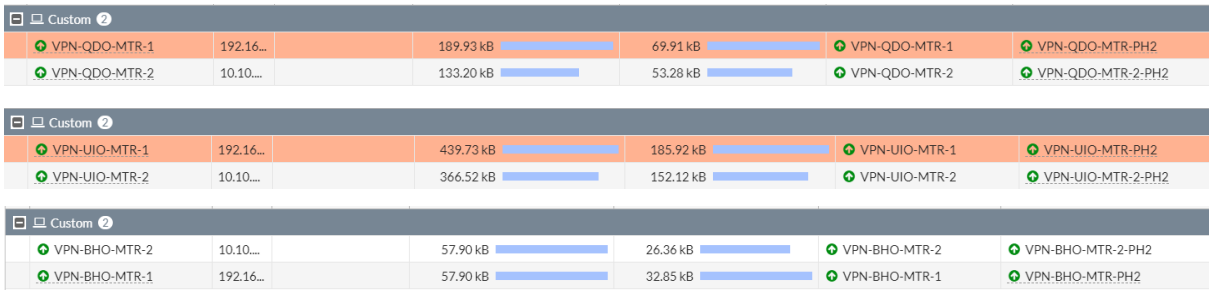


Figura 11-5: Visualización de estado de los túneles en Sucursales
Fuente: Heredia, J. 2022

Los túneles IPSec con agregados en la SD-WAN para garantizar la disponibilidad de los servicios y comunicación de las sucursales con la oficina matriz.

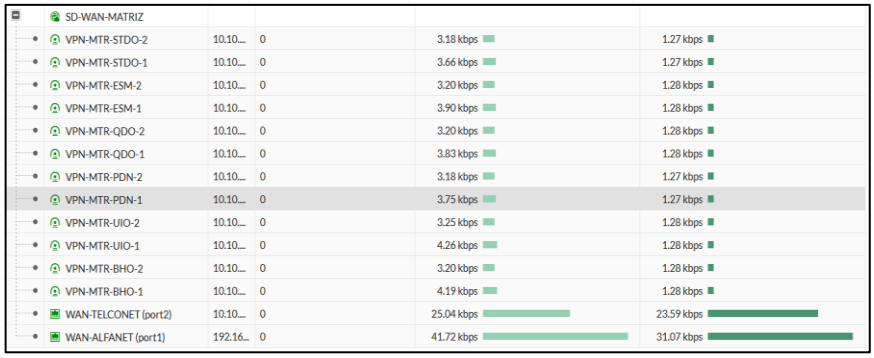


Figura 12-5: Configuración de túneles IPSec en la interfaz SD-WAN.
Fuente: Heredia, J. 2022

5.8.2 Configuración de loopback

Las interfaces de loopback sirven para supervisar que los túneles IPSec estén operativos, el monitoreo está basado en parámetros de latencia, perdida de paquetes y jitter. Las loopback tienen como función enviar paquetes pequeños a las interfaces que pertenecen a la SD-WAN para establecer que estén activas y validar las perdidas o tiempos de respuesta de cada túnel, esta verificación permite elegir la mejor ruta en conjunto con las reglas creadas en el SD-WAN.

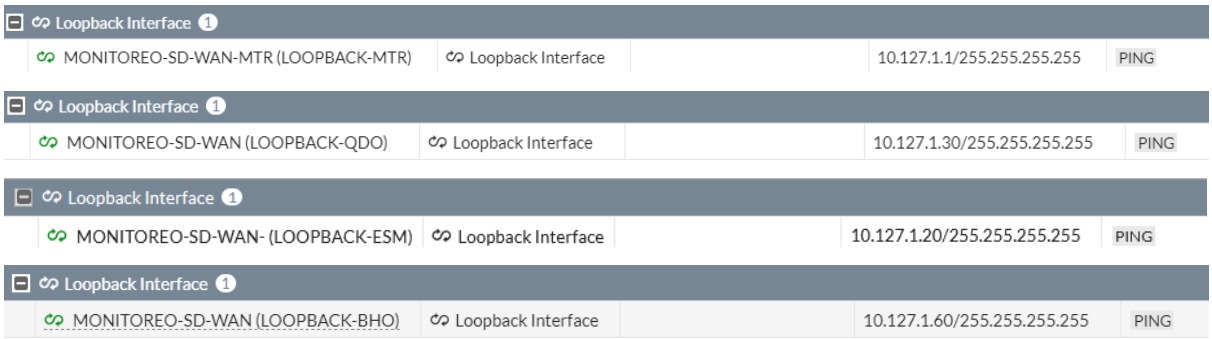


Figura 13-5: Configuración de loopback en los diferentes equipos Fortigate.
Fuente: Heredia, J. 2022

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

Los SLA y reglas de SD-WAN permiten tener una optimización de recursos de red, la configuración permite elegir automáticamente la mejor ruta hacia matriz y sucursales, para la elección se ejecuta mediante el monitoreo SLA el cual nos indica la latencia y perdidas de paquetes de cada enlace, se elige la ruta con menor tiempo en latencia y menor cantidad de paquetes perdidos como nos indica la Figura 14-5.

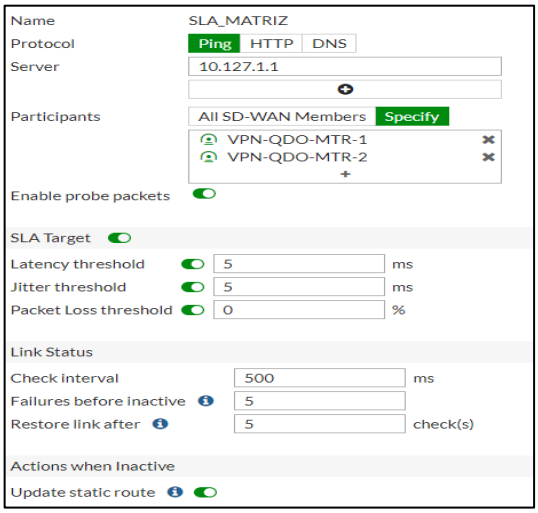


Figura 14-5: Performance SLA
Fuente: Heredia, J. 2022

En la Figura 15-5 se indica la configuración de las reglas SD-WAN en cada extremo de la red de Asertia S.A. Las políticas para las Sucursales tienen como origen la red LAN de cada Fortigate y destino las redes de matriz, en caso de Matriz se configuró políticas de forma inversa. En las configuraciones se observa que el enlace tomará el camino que tenga menor latencia, esto ayuda a que, si un proveedor está presentando problemas, esto permite que la comunicación entre matriz y sucursales no sientan esas intermitencias y a nivel lógico se haga la evaluación de la mejor ruta y sea elegida para la comunicación.

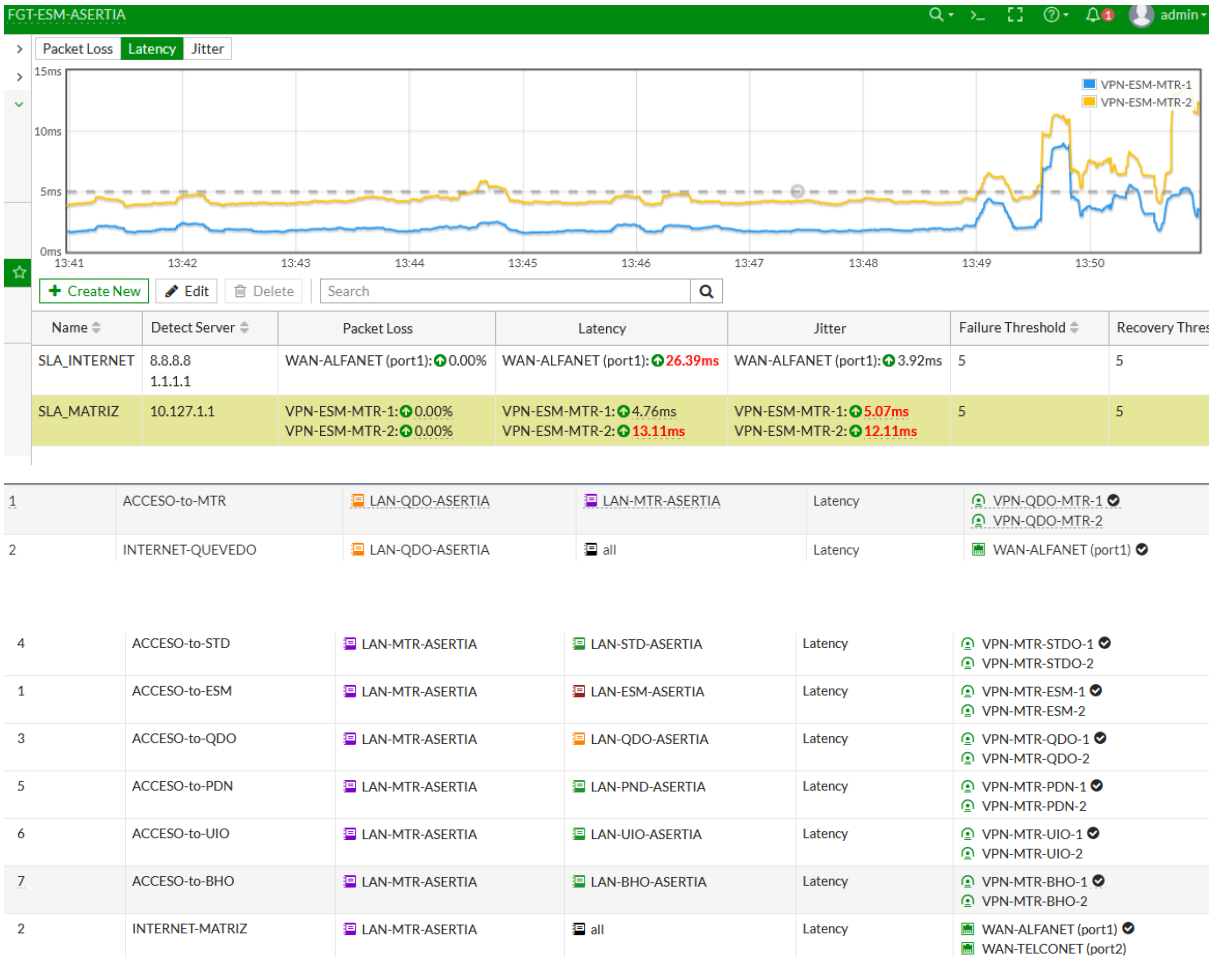


Figura 15-5: Monitoreo y Políticas SD-WAN
Fuente: Heredia, J. 2022

5.8.4 Configuración de Políticas en el Fortigate

Para mantener un acceso seguro desde matriz y sucursales hacia Internet, se configuraron políticas de acceso en las mismas que se habilitaron distintos perfiles de seguridad (WebFiltering, Application Control, IPS y Antivirus). Las restricciones creadas están basadas en las restricciones de cada área.

A continuación, se detallan las políticas creadas en cada Fortigate. En la Figura 16-5 se puede observar las políticas creadas para los túneles IPSec, en donde se especificó las redes de origen y destino, en este tipo de políticas no es necesario tener habilitado el NAT ya que estas no tendrán permiso de navegación a través de Internet.

Se configura una política en la cual el origen LAN y destino sea la interfaz virtual SD-WAN esto permitirá comunicar las sucursales.

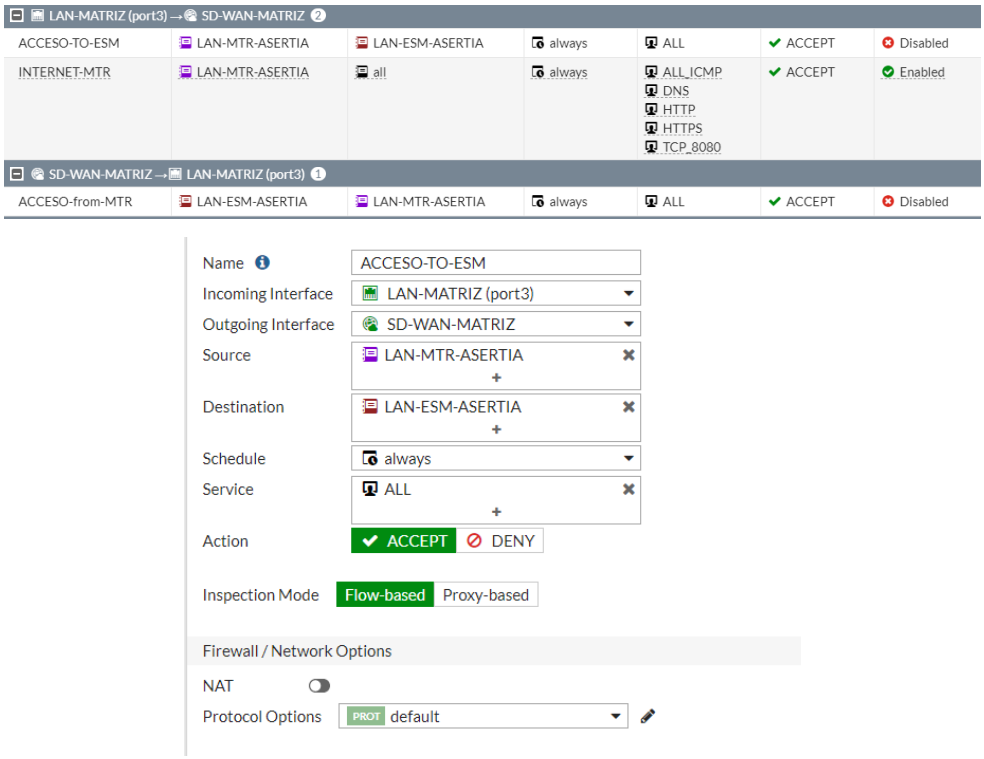


Figura 16-5: Políticas de Acceso Sucursales
Fuente: Heredia, J. 2022

En la Figura 17-5 se puede observar las políticas creadas para el acceso a Internet en Matriz y sucursales, en estas políticas necesitan tener habilitado el NAT y restricción de puertos, al momento se configuró acceso para los puertos http, https, dns, ping, puerto 8080.

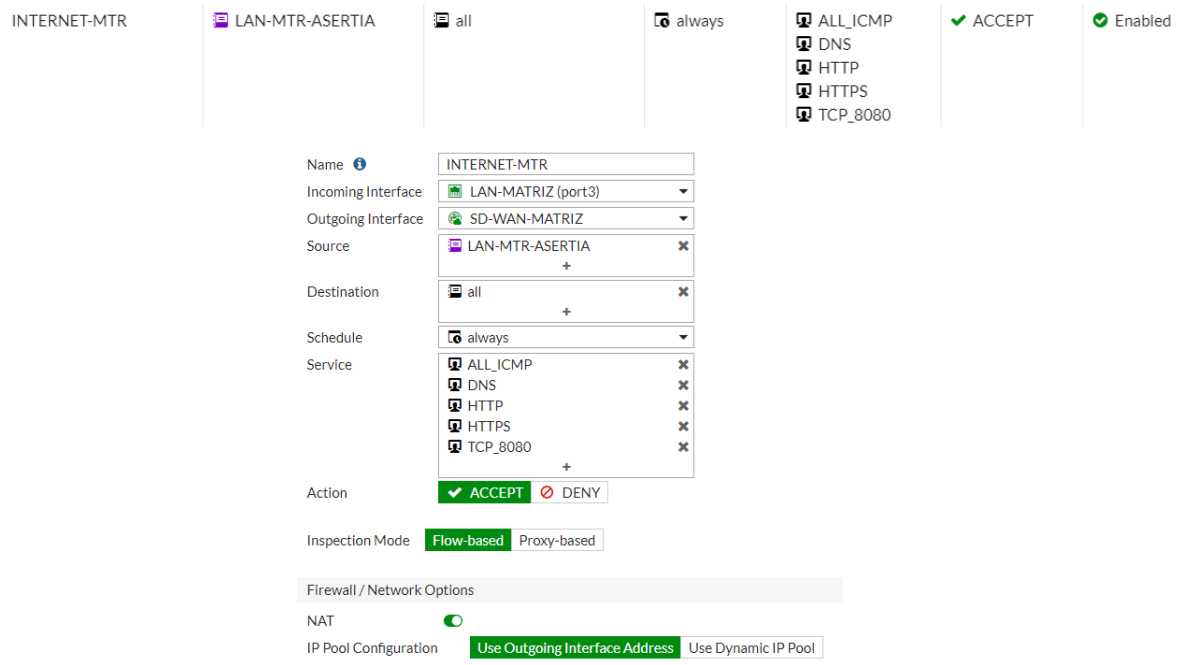


Figura 17-5: Políticas de Acceso Internet
Fuente: Heredia, J. 2022

5.8.5 Control por aplicativos y Web Filtering.

Para la red de la Asertia S.A. se instituyó el bloqueo para los aplicativos de las redes Proxys, Apuestas, Contenido adulto y video hosting, como se muestra en la Figura 18-5; que, en la aplicación de filtros se bloquea todo acceso a las páginas antes nombradas. Estos perfiles están diseñados para controlar y no saturar la red con actividades que no forman parte del desarrollo diario, también para crear una red más segura.

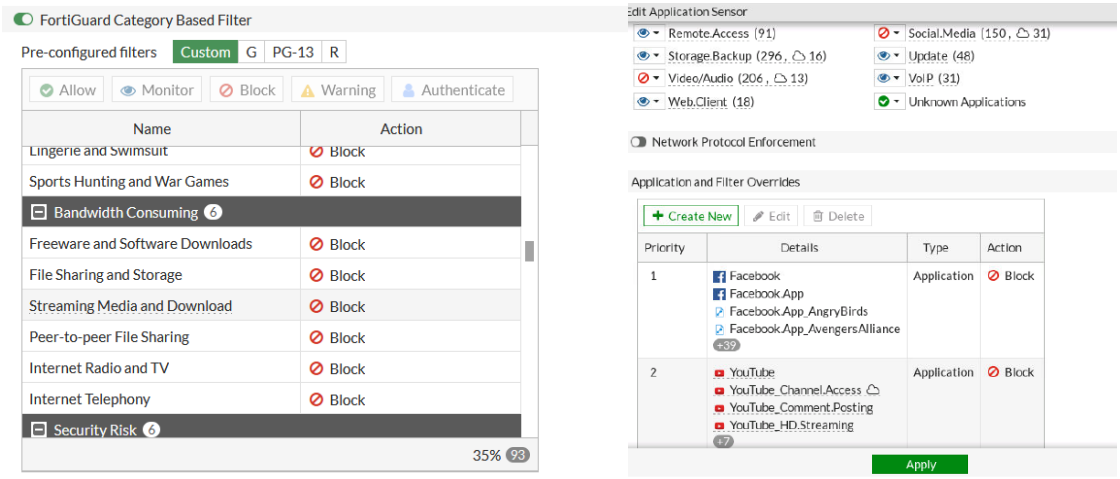


Figura 18-5: Políticas de Web Filtering y Application Control
Fuente: Heredia, J. 2022

5.9 PRUEBAS DE ACCESO Y OPTIMIZACIÓN DE RECURSOS.

5.9.1 Pruebas de acceso al servidor local

Mediante los controles de seguridad aplicados en las reglas de SD-WAN se tiene acceso sin interrupciones a los aplicativos tanto de forma local como en nube.

El acceso al servidor local no presenta perdidas de paquetes y su latencia promedio es 15ms, por lo que el proceso de facturación se realiza sin ningún retraso como se producía anteriormente, en las Figuras 19-5 y 20-5 se detalla que el acceso al servidor local.

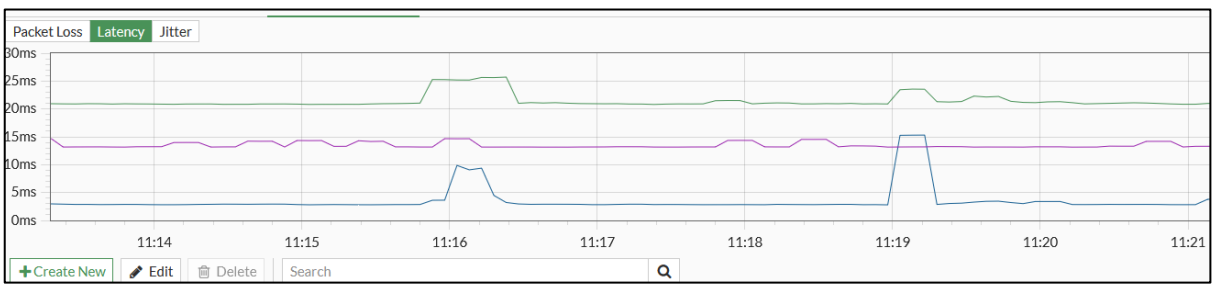


Figura 19-5: Latencia
Fuente: Heredia, J. 2022

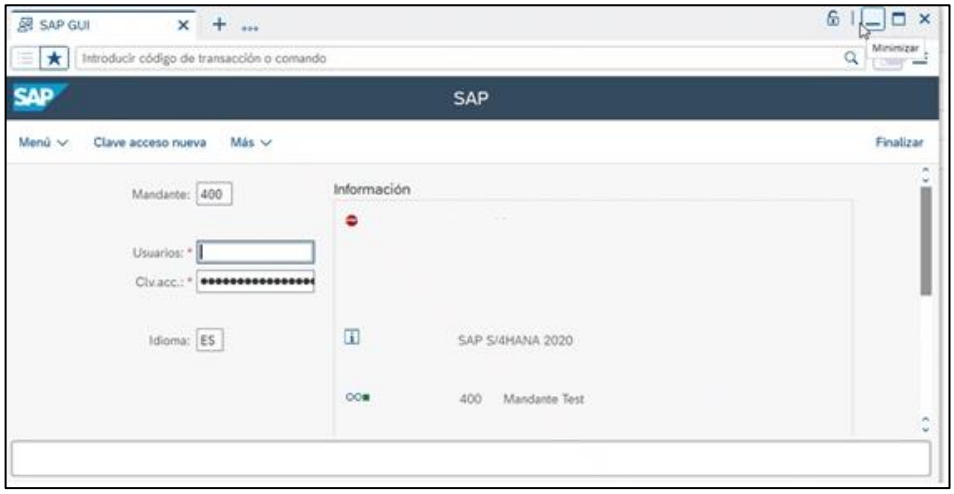


Figura 20-5: Sistema de facturación local
Fuente: Heredia, J. 2022

5.9.2 Pruebas de acceso al servidor en nube CMC.

En las Figuras 21-5 y 22-5, se detalla el acceso a la nube de Citrix y posterior el ingreso al servidor CMC que se encuentra en la nube se ejecuta a través de Internet, con los perfiles de seguridad y políticas de SD-WAN que tienen la oficina matriz y sucursales permitieron un acceso rápido hacia los aplicativos, esto ayuda a que las tareas diarias que realiza el personal de Asertia no se vean afectadas por problemas acceso hacia los aplicativos en nube.

Figura 21-5: Acceso nube Citrix
Fuente: Heredia, J. 2022

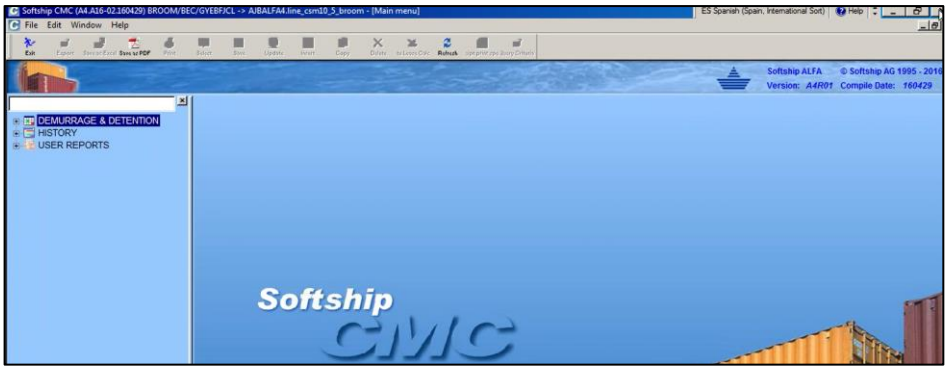


Figura 22-5: Acceso servidor CMC
Fuente: Heredia, J. 2022

5.9.3 Bloqueo de aplicativos de acuerdo con los perfiles de seguridad

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

En la Figura 23-5 se muestra en modo grafico como es el bloqueo hacia los aplicativos que se solicite, en este caso se utiliza para pruebas a Facebook por parte de los aplicativos de redes sociales y a YouTube en videos.

Figura 23-5: Bloqueo de aplicativos (Redes sociales y videos).
Realizado por: Heredia, J. 2022

CONCLUSIONES

- En el análisis realizado a la red WAN de Asertia, en horas de mayor uso de los enlaces el ingreso a las aplicaciones corporativas no estaba disponible causando retrasos en facturación y atención a clientes, la empresa no contaba con ningún equipo de seguridad perimetral que aplique controles a los accesos de los empleados lo que provocaba saturación de ancho de banda por el uso indebido de internet aumentando la propagación de ransonware, phishing, y otros riesgos informáticos a lo que estaba expuesta la empresa Asertia.

- Con la implementación de la solución SD-WAN en Asertia se optimizó el uso de los recursos de red permitiendo que la conexión sea segura, confiable y tenga alta disponibilidad por las VPNs IPSec creadas en cada sucursal que permiten el acceso a aplicaciones corporativas, se configuró perfiles de seguridad perimetral para el control de la navegación a internet en base a la necesidades y prioridades de forma totalmente personalizada minimizando los riesgos informáticos que tenía la empresa anteriormente.

- En los resultados de accesos a los aplicativos del servidor local y en la nube durante las horas pico, se evidenció que no presentaron ninguna perdida de conexión y el tráfico permaneció estable esto nos indica que las reglas SD-WAN aplicadas se configuraron de manera correcta, permitiendo disponibilidad en los servicios corporativos de Asertia, que los recursos de red sean utilizados para actividades laborales en base a los requerimientos de cada área y garantizar la seguridad perimetral mediante los perfiles de IPS, Antivirus, DoS, WebFiltering y Application Control.

RECOMENDACIONES

- Tener estadísticas del comportamiento de las reglas SD-WAN y SLA de forma periódica para tener mejor visibilidad, rendimiento, escalabilidad y control de los accesos hacia los aplicativos empresariales.

- En las sucursales se recomienda tener otro proveedor de internet para alcanzar la alta disponibilidad de accesos y poder aplicar enrutamiento dinámico BGP para aprovechar al máximo las capacidades de la solución SD-WAN.

- Aplicar todas las funcionalidades que los equipos Fortigate poseen, en base a las revisiones y estadísticas recolectadas por parte del administrador se recomienda aplicar distintos controles de QoS para aplicaciones corporativas.

BIBLIOGRAFÍA

Arévalo García, R. X. (10 de Diciembre de 2020). Análisis de factibilidad técnica y económica para la implementación de SD-WAN considerando su eficiencia operacional frente al servicio de MPLS en la Puntonet .

AUDITECH. (2021). Obtenido de https://auditech.es/seguridad-gestionada/

AXESS. (2019). AXESS Networks. Obtenido de https://axessnet.com/sd-wan-para-que-sirve-y-cuales-son-sus-ventajas-frente-a-la-wan-tradicional/

Ayapata Mendoza, D. O. (2 de Marzo de 2020). Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo. Guayaquil, Guayas, Ecuador.

FORTINET. (2021). Obtenido de https://www.fortinet.com/lat/products/sd-wan

Hernández Sampieri, R. (2014). *Metodología de la Investigación.* Mc Graw Hill.

Ley Leyva, N. V. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. *Sociedad & Tecnología*, 18.

LIDER IT. (11 de Junio de 2020). *LIDER IT Consulting*. Obtenido de https://www.liderit.es/ventajas-seguridad-gestionada/

López Jaimes, A. P., Mojica Marín, D. A., & Rodríguez González, B. C. (25 de Enero de 2021). Diseño de ua Red de Área Local Genérica para las empresas dedicadas añl Diseño de Software, ubicadas en la localidad de Teusaquillo en Bogotá. Bogotá, Colombia.

Moreno Alayón, S. M. (2021). Comparación de aspectos operativos y económicos entre SD-WAN y MPLS para establecer la mejor opción de una empresa corporativa a nivel nacional e internacional. Bogotá.

OSTEC. (18 de Julio de 2018). *Seguridad Digital de Resultados*. Obtenido de https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento/

Rodriguez Limones, M. F. (10 de Noviembre de 2021). DISEÑO DE IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD GESTIONADA CON SD-WAN PARA UNA RED MPLS QUE PROVEEE SERVICIOS DE INTERNET Y DATOS PARA LA UNIVERSIDAD POLITECNICA SALESIANA. Guayaquil, Guayas, Ecuador.

Rubiano Aguilar, E. S. (2021). PROPUEST ARA EL USO DE SD-WAN EN LA RED CORPORATIVA EMTELCO CX&BPO SEDE BOGOTÁ. Bogotá.

SDxCentral LLC. (2018). Obtenido de https://www.ibm.com/downloads/cas/3AW5O9OR

Selltiz, C. (1980). *Métodos de investigación en las relaciones sociales.* Madrid: Rialp.

Silva, J. (2021). Tecnología de red definida por software para el aprendizaje en grupos de investigación y educación. *Innova Educación*, 12.

Soluciones de GPC Inc . (2021). Obtenido de https://gpcinc.mx/blog/redes-lan-man-wan

Spadaro, G. F. (2012). Diseño de red WAN.

Tanenbaum, A. S., & Wetherall , D. J. (2012). *Redes de Computadoras.* Mexico: PEARSON EDUCACIÓN.

Valarezo Constante, J. R. (2020). DESARROLLO DE UN PROTOTIPO DE RED DE AREA AMPLIA BASADO EN UNA ARQUITECTURA DEFINIDA POR SOFTWARE EN UNA INSTITUCION FINANCIERA. Guayaquil, Guayas, Ecuador.

Velasquez Blacutt, M. N. (2020). Ciberseguridad en la implementación de SD-WAN. *PGI. Investigación, Ciencia y Tecnología en Informática*, 1-2.

vmware. (12 de 02 de 2022). *vmware.com.* Obtenido de https://www.vmware.com/es/topics/glossary/content/software-defined-networking.html