Implementación de Redes SDN-WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP's)

Sambrano Velasco, Johanna Olivia

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previos a la obtención del título de Ingeniera en Electrónica y Telecomunicaciones

Msc. Aguilar Salazar, Darwin Leonidas

14 de diciembre 2020

URKUND

Document Information

Analyzed document	TRABAJO DE TITULACIÓN-JS-APA2020_FINAL.pdf (D89481045)
Submitted	12/15/2020 2:24:00 PM
Submitted by	
Submitter email	dlaguilar@espe.edu.ec
Similarity	5%
Analysis address	dlaguilar.espe@analysis.urkund.com

Sources included in the report

SA	**Universidad de las Fuerzas Armadas ESPE / TESIS-V0.6.docx** Document TESIS-V0.6.docx (D34378411) Submitted by: jepazmino@espe.edu.ec Receiver: evcarrera.espe@analysis.urkund.com	1
W	URL: https://repositorio.espe.edu.ec/bitstream/21000/13847/1/T-ESPE-057535.pdf Fetched: 6/14/2020 9:37:08 PM	1
SA	**1599884198_537__2020_MET_Cisneros_Estefania.pdf** Document 1599884198_537__2020_MET_Cisneros_Estefania.pdf (D80631133)	1
SA	**TT Fulvio Carrasco.docx** Document TT Fulvio Carrasco.docx (D81959056)	1
W	URL: https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar Fetched: 12/15/2020 2:33:00 PM	2
SA	**TT Fulvio Carrasco.docx** Document TT Fulvio Carrasco.docx (D82244906)	1
W	URL: https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-global- ... Fetched: 12/15/2020 2:33:00 PM	3
W	URL: https://openzen.wordpress.com/2015/02/12/historia-del-sdn/ Fetched: 12/15/2020 2:33:00 PM	1
W	URL: http://www.revistatonoetecsa.cu/articulo/desarrollo-de-aplicaciones-sdn Fetched: 12/15/2020 2:33:00 PM	1
W	URL: https://jci.uniautonoma.edu.co/2018/2018-7.pdf Fetched: 12/15/2020 2:33:00 PM	5
SA	**Universidad de las Fuerzas Armadas ESPE / Cristian_Bustos_Tesis_Espe_V6.docx** Document Cristian_Bustos_Tesis_Espe_V6.docx (D45646918) Submitted by: dmmarcillo@espe.edu.ec Receiver: dmmarcillo.espe@analysis.urkund.com	2
	URL : https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-senati.pdf	

URKUND

W	Fetched: 12/15/2020 2:33:00 PM	1
W	URL: https://repositorio.ucp.edu.co/bitstream/10785/3674/1/CDMIST127.pdf Fetched: 12/9/2020 7:22:56 PM	1
W	URL: http://www.firewall.cx/general-topics-reviews/sd-wan/1210-sd-wan-networks-benefits ... Fetched: 12/15/2020 2:33:00 PM	1
W	URL: https://revistas.utp.ac.pa/index.php/memoutp/article/view/1842 Fetched: 12/15/2020 2:33:00 PM	1
W	URL: https://ieeexplore.ieee.org/document/7502469/authors#authors Fetched: 12/15/2020 2:33:00 PM	1
W	URL: http://laccei.org/LACCEI2019-MontegoBay/full_papers/FP478.pdf Fetched: 12/15/2020 2:33:00 PM	1

Sangolquí, 15 de diciembre 2020

ING. DARWIN AGUILAR SALAZAR
DOCENTE DEEL
TUTOR TRABAJO TITULACIÓN

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Implementación de Redes SDN – WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP´S)**" fue realizado por la señorita **Sambrano Velasco, Johanna Olivia** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 14 de diciembre del 2020

Firma:

.....

Aguilar Salazar, Darwin Leonidas

C. C 110303682-6

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

RESPONSABILIDAD DE AUTORÍA

Yo, **Sambrano Velasco, Johanna Olivia**, con cédula de ciudadanía n° **1713677100**, declaro que el contenido, ideas y criterios del trabajo de titulación**: Implementación de Redes SDN – WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP´S)** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 14 de diciembre del 2020

Firma

.....

Sambrano Velasco, Johanna Olivia

C.C.: 171367710-0

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

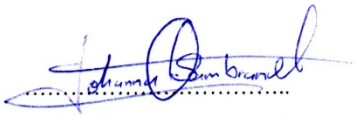
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Sambrano Velasco, Johanna Olivia,** con cédula de ciudadanía n° **1713677100**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Implementación de Redes SDN – WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP´S)** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 14 de diciembre del 2020

Firma



Sambrano Velasco, Johanna Olivia

C.C.: 171367710-0

DEDICATORIA

El apoyo incondicional y el tiempo brindado son las acciones que fueron participes en la realización y culminación de este proyecto, es por eso por lo que lo dedico de todo corazón a todas las personas que me brindaron un consejo, una guía, un soporte, una mano. No hay valor o cantidad que pueda representar la gran alegría que siento al haber tenido a mi lado tantas personas empezando por mi familia, siempre al tanto de lo que necesitara, mis amigos y compañeros de trabajo que supieron ser oportunos y mis guías para realizar el mejor trabajo posible, mis mentores en la universidad, que sin ellos no estuviera donde estoy y sobre todo Dios con las bendiciones me otorgó, para estar aquí en este momento.

¡Con toda la alegría que quiere transmitirles, esto es por y para ustedes!

AGRADECIMIENTO

Quisiera empezar agradeciendo a Dios, no hay mayor fuerza y bendiciones que las que te otorga el Señor. Agradezco a mi familia, primero a mis padres Olivia y Julio que gracias a su esfuerzo pude tener educación, nunca me abandonan y estuvieron y están siempre en mi corazón, son las personas por las que ahora lucho yo y no hay palabras que pueda describir todo lo grandioso que significan para mí. Mis hermanos Rory y Yeslie, que siempre estuvieron ahí para cualquier cosita que pude necesitar aparte del apoyo de hermanos y cariño que nos tenemos. A mis compañeros de trabajo les puedo decir que mi agradecimiento infinito, no lo hubiera logrado sin su apoyo más que compañeros de trabajo son mis amigos y hemos podido disfrutar de alegrías y momentos duros durante esta etapa, les agradezco por el tiempo que me brindaron porque dar un minuto de vida no se lo da a cualquiera y eso marcó mi vida. A los profesores de mi carrera universitaria, fueron los impulsores de mi carrera y aprecio todo los que nos dedicaron para poder enseñarnos, a mi director del proyecto Darwin Aguilar por toda la ayuda, paciencia, tiempo, consejos y aportes, le doy mi agradecimiento de todo corazón ya que el tiempo es invaluable y el otorgármelo en sus momentos es un bien infinito; al ingeniero Carlos Romero por su apoyo. Quisiera por último agradecer a mis amigos que preguntaban por la culminación de este trabajo y estuvieron en el seguimiento, a mi novio que durante todo este tiempo estuvo a mi lado, siempre creyendo en mí y aunque ha pasado mucho tiempo, no hay mejor apoyo y cariño que el incondicional.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente en el Ecuador se evidencia que existe una tendencia de crecimiento exponencial en lo que respecta al uso de Internet en redes Fijas y Móviles, lo que a su vez ha llevado a los usuarios finales o abonados a demandar altos Anchos de Banda para su consumo. Es por ello que se han venido desarrollando medios de transmisión para conseguir el acceso de mayores velocidades, como el caso de la implementación del cable submarino, el cual se terminó de construir en mayo del 2017; esto nos ha permitido obtener mayores anchos de banda, pero reflejados en altos costos. Por lo que además de contar con medios de transmisión, se debe contar con tecnologías que optimicen la utilización del ancho de banda que se contrate, buscando obtener el mayor provecho para que las aplicaciones que cursen sobre el canal, tengan el menor impacto a nivel de indisponibilidad considerando que se disponga de varios proveedores. En este trabajo se expone a la tecnología SD-WAN implementa en hardware, de forma que las prestaciones y algoritmos utilizados, permitan a lo largo del desarrollo del estudio y realizar la evaluación de uno o más proveedores (ISP), considerando aplicaciones de mayor prioridad para el cliente tomando como ejemplo videoconferencias, transmisión de datos, o aplicaciones que cursen a través de internet, la referencia, el análisis que se debe aplicar y la toma de decisiones para una correcta configuración por ende óptima experiencia.

PALABRAS CLAVES:

- **ANCHOS DE BANDA**
- **ISP**
- **SD-WAN**
- **WAN**

ABSTRACT

Currently in Ecuador there is evidence of an exponential growth trend in the use of Internet in fixed and mobile networks, which in turn has led to end users or subscribers to demand high bandwidth for their consumption. That is why we have been developing transmission means to achieve higher speed access, as in the case of the implementation of the submarine cable, which was completed in May 2017; this has allowed us to obtain higher bandwidths, but reflected in high costs. Therefore, in addition to having transmission means, we must have technologies that optimize the use of the contracted bandwidth, seeking to obtain the greatest benefit so that the applications on the channel have the least impact at the level of unavailability, considering that there are several suppliers. In this work is exposed to the technology SD-WAN implemented in hardware, so that the benefits and algorithms used, allow throughout the development of the study and make the evaluation of one or more providers (ISP), considering applications of higher priority for the client taking as an example videoconferencing, data transmission, or applications running over the Internet, the reference, the analysis to be applied and decision making for a correct configuration therefore optimal experience.

KEYWORDS:

- **BANDWITH**
- **ISP**
- **SD-WAN**
- **WAN**

CAPÍTULO I

GENERALIDADES

Introducción

Las redes definidas por software (SDN), como se conoce, es un desarrollo que apareció hace 20 años como una necesidad de gestionar y controlar de manera centralizada e inteligente los elementos que se dispongan en una arquitectura de red (hardware) con ayuda de software.

El crecimiento del internet en el transcurso del tiempo y los dispositivos que se han desarrollado para el uso del mismo como smartphones, Smart TV, tecnología IoT en general, han reflejado el aumento de consumo, e incremento de anchos de banda. Por lo que esto generó la necesidad en las diferentes empresas proveedoras de Internet, el direccionar esfuerzos y colocar en el mercado un producto que otorgue las mejores prestaciones para de esta manera cumplir con el cometido de optimizar el consumo del ancho de banda, no sólo a nivel de protocolos que en un inicio lo desarrolló OpenFlow, sino que se haga un mayor enfoque a la capa de aplicación que es lo que más representa a nivel de consumo. Adicional a lo mencionado se consideró que en países en desarrollo como el Ecuador las infraestructuras de los proveedores locales (ISP) presentan aun bajos anchos de banda, alta latencia por la interconexión hacia las redes internacionales que no poseen gestión; lo cual repercute en la calidad de servicio que reciben los usuarios que comprenden pequeñas y grandes empresas como: pérdida de datos, comunicaciones lentas, indisponibilidad de sistemas y por ende pérdida de tiempo y dinero.

Para no incrementar la contratación de mayor ancho de banda y poder trabajar en forma adecuada con las múltiples aplicaciones y servicios que a través del internet se dispone en el mercado

surge la tecnología SD-WAN, la cual puede considerarse como la SDN (Software Define Network) de la WAN.

Se entiende a SD-WAN como una red de área amplia definida por software y se la considera como una aplicación de redes definidas por software (SDN). Los principales objetivos de SD-WAN son simplificar, controlar y automatizar la implementación y administración de la red. Tiene la capacidad de disminuir costos y permite un incrementó en la agilidad de red con diversos enlaces WAN.

Las soluciones SD-WAN son el reemplazo de los enrutadores WAN tradicionales y están relacionadas a las tecnologías de transporte WAN. SD-WAN proporciona una selección de ruta de aplicación dinámica, basada en políticas, a través de múltiples conexiones WAN y soporta el encadenamiento de servicios para servicios adicionales como la optimización de la WAN y firewall. La inteligencia se abstrae en una superposición virtual, lo que permite una agrupación segura de conexiones tanto privadas, como públicas y permite la automatización, el control centralizado de la red y la gestión del tráfico ágil.

Esta tecnología permite garantizar la calidad del servicio y la protección de datos de los enlaces de Internet, independientemente de su tipo, permitiendo que el tráfico se direccione automáticamente a través del camino más adecuado de la WAN, tomando en cuenta las condiciones de seguridad, el costo de los enlaces y las exigencias que presenten las aplicaciones del usuario el momento en que las utilice.

En el país al año anterior se ha conocido la incursión a esta tecnología, mediante comunicados de diarios nacionales como en El Universo, Notiempresariales, Metroecuador entre otros, luego la oferta del

producto en cada proveedor el cual han adoptado el desarrollo para la implementación en clientes que lo necesiten, difundiendo las ventajas del mismo.

Siendo así que se puede decir que la tecnología SD WAN se encuentra aún en un campo desconocido. Se ha validado que la implementación del mismo se ha logrado en entidades bancarias, pero debemos preguntarnos si es en el sector bancario donde se debe concentrar esta tecnología, pues la respuesta es fácil y es no; cada usuario, empresa y persona que esté interesado en optimizar sus recursos podrá ejecutar el desarrollo de la tecnología SD WAN dentro de su ámbito, cualquiera que este sea.

Es por ello que con el presente trabajo se pretende implementar un escenario con equipos que permitan configurar y posteriormente evaluar tecnología SD-WAN. En este escenario, se van a conectar las 2 últimas millas de proveedores diferentes, para de esta manera y, mediante la realización de pruebas y evaluaciones de estas, exponer el muestreo del rendimiento y funcionamiento de las aplicaciones más concurrentes que los usuarios pueden generar hacia el internet, haciendo a su vez un análisis comparativo para validar prioridades y establecer perfiles de configuración en el equipo. Estas pruebas y resultados permitirán optimizar los canales de internet mitigando los problemas de pérdidas de información, retardo, fallas en la configuración de QoS entre otros.

Justificación e Importancia

El avance de la tecnología y el hecho de que hoy en día el uso de la Internet es algo prácticamente imprescindible, ha hecho que el volumen de información con el que se trabaja en la actualidad sea algo surrealista ya que se estima que en el 2020 cada usuario en el mundo generará 1.7 Megabytes de datos por segundo (GRUPO.BIT, 2020), lo que genera que nuevas soluciones tecnológicas sean puestas en

práctica para garantizar que todos estos datos puedan transmitirse sin ningún tipo de problema, haciendo énfasis principalmente en redes empresariales.

Actualmente la mayor parte de infraestructuras WAN no aseguran que los datos que circulan por la red cuenten con valores próximos al 100% de seguridad y fluidez, ya que tienen: alta latencia generada por el tráfico de backhauling, bajo ancho de banda y una total falta de visibilidad de las aplicaciones, lo que ocasiona que usuarios o empresas que tengan procesos o servicios que se realicen a través de la Internet sufran una mala experiencia con comunicaciones lentas o la pérdida de datos lo que repercute en la pérdida de tiempo de conexión.

En el ámbito empresarial, el hecho de seguir manteniendo una infraestructura de tipo WAN (routers, optimizadores, controladores de rutas, firewalls, entre otros), además de los problemas antes mencionados; implica un alto costo en cuanto a la adquisición, mantenimiento y administración de equipos por lo que la implementación de la tecnología SD-WAN es una opción atractiva por la reducción de costos, para argumentar esto podríamos tomar como referencia a la empresa y de investigación de las tecnologías de la información “Gartner”, quienes estiman que la tecnología SD-WAN puede ser hasta 2 veces y medio menos costosa que una arquitectura WAN tradicional (Butler, 2017).

Pese a que la tecnología SD-WAN lleva algún tiempo ya en el mercado, en el Ecuador la introducción de esta, es un tema aún escaso por explotar y que sólo se la ha implementado en empresas de alta rentabilidad y con altos estándares de seguridad como lo son las instituciones bancarias. Esto no descarta que el resto de empresas locales no lo puedan usar, el objetivo es dar a conocer cual exequible es la tecnología y cómo podemos adaptarlas a las diferentes líneas de negocio, presentar la importancia

que puede representar en la optimización de los enlaces y cómo podríamos maximizar nuestros recursos sin gastos adicionales.

Es importante considerar que parte del estudio también radica realizar un análisis de los distribuidores del hardware de redes en el país, a fin de determinar cuáles serían los equipos ideales para implementar SD-WAN. Se deberá establecer comparativas de las distintas marcas en el mercado y seleccionar el que se adapte a las necesidades esenciales de las líneas de negocio, ejecutando una sola inversión alcanzando altos niveles de calidad, como también validando herramientas adicionales que incluya el producto.

Al disponer de SD-WAN es esencial obtener enlaces redundantes en donde el manejo será administrado por el software, el resultado será la eliminación de caídas o intermitencias en la comunicación, de cierta manera la eliminación de los tiempos de conmutación. Se podrá aprovechar la experiencia SD-WAN en video llamadas, pasa de data, en definitiva, cualquier tipo de información que se considere muy sensible que esté cursando por el canal.

El resultado de la puesta en producción significa mucho más que facilitar y automatizar la gestión de la red, permite a las empresas prepararse para la transformación digital, soportando mayor tráfico de datos, más seguridad y colaborando para el desarrollo de toda la red.

Alcance del Proyecto

Para poder desarrollar el proyecto se iniciará con la investigación de las marcas de mayor distribución en el país siendo: Cisco, Fortinet, Citrix, aunque el proceso de investigación podría incluirse

marcas adicionales también. Como parte de la investigación se deberá analizar las características, rendimiento, prestaciones y valores para establecer cual se seleccionará acorde a los requerimientos SD-WAN

Tomando como referencia el hardware que se seleccione se acondicionará un ambiente de implementación que consiste en:

1. Disponer de un enlace de Internet con el proveedor A.
2. Disponer de un enlace de Internet con el proveedor B.
3. Se escogerá a conveniencia las aplicaciones que se requiera priorizar
4. Las dos últimas millas o enlaces de proveedores se conectarán al equipo.

Se deberá ejecutar un protocolo de pruebas para el análisis y evaluación de resultados:

a) Antes de la aplicación SD-WAN
b) Luego de la aplicación SD-WAN
c) Repetir con diferentes aplicaciones
d) Definir umbrales para los diferentes servicios.

Una vez establecidos los parámetros se aplicará la configuración en el software y se recolectará la información de presentación de resultados del software.

A partir de esto se podrá desarrollar recomendaciones sobre las diferentes aplicaciones y configuraciones que sean requeridas y establecer una técnica procedimental para futuros trabajos.

Objetivos

General

Realizar el diseño, implementación la evaluación de SDN integrado a la tecnología SD-WAN a fin de analizar la mejora en el rendimiento en aplicaciones prioritarias para los usuarios de Internet.

Específicos

- Investigar y evaluar el hardware adecuado para la implementación SD-WAN.
- Efectuar un análisis de las latencias que presente los proveedores de servicios hacia una aplicación común.
- Llevar a cabo la instalación, configuración y evaluación de las herramientas considerando la optimización, mediante la transmisión de aplicaciones como video.
- Realizar un análisis comparativo de la eficiencia de SD-WAN de optimización (software).
- Presentar resultados según el escaneo que realiza SD-WAN sobre el hardware seleccionado.
- Generar políticas para la configuración de escenarios SD-WAN de forma que se garantice mejorar los niveles de calidad que se ofertan por parte de los proveedores a los usuarios de Internet.

Trabajos Relacionados

Teniendo en cuenta que esta tecnología ya lleva algunos años en el mercado, podremos partir de trabajos ejecutados en empresas como National Instruments dedicada a la manufactura tecnológica; menciona que SD-WAN permitió a NI transportar grandes cantidades de red de tráfico a través de conexiones de Internet de bajo costo en lugar de enlaces caros de MPLS.

Se evidenció una diferencia en la reducción de costos/inversión en ancho de banda MPLS que se cuantifica en un promedio de 64% por sucursal. Personal de TI de la empresa menciona que en una oficina con alrededor de 80 personas haciendo todo tipo de trabajo en lo que respecta soluciones de TI ya no se encuentran compitiendo en un enlace de 10 Mbps. Pudo catalogar el tráfico en su red por tipo y función, adicional logró enviar el tráfico restante sobre la Internet bajo un parámetro de nivel de servicio (SLA). Con esto logró eliminar un cuello de botella que se le presentaba en los recursos de su ancho de banda de su circuito MPLS. National Instruments se encuentra aún en proceso de su migración a SD-WAN, dispone de un 36% de la tecnología puesto en marcha de su infraestructura total, aun así, se ha reflejado en el ahorro del 25% neto que equivale más o menos a 450.000 dólares sólo en el 2018.

También indica que ha aumentado el promedio de ancho de banda en un 3075%, haciendo una referencia se supone el caso de un peaje en el cual pasan 50 vehículos por minuto en un día, la optimización equivaldría al mismo peaje con una capacidad de gestión de 1500 vehículos por minuto. (CISCO, 2018).

Se encuentra presente también la empresa de Burger King Brasil, que administra y maneja las franquicias de las cadenas Burger King y Popeyes Louisiana Kitchen, sumando a esto que supervisa todos los restaurantes BURGER KING® y POPEYES® en Brasil, para la selección de una mejor solución se basaron

en el ideal de aumentar la seguridad de la información, ampliar y automatizar el control de los procesos de su red. Con la implementación de SD-WAN redujo costos de conectividad a Internet que en consecuencia permitió el uso de conexiones más baratas, más específicas y seguras. Ellos visualizaron el cambio en el siguiente comportamiento sólo en llamada sobre internet existían ocasiones que consumían la totalidad del ancho de banda y de forma insegura abierta a cualquier ataque, la implementación de esta tecnología redujo en un 26% a incidentes relacionados con conectividad. En la empresa se han centrado e identificado cuatro pilares una mayor seguridad informática, mejor visibilidad, control y procesos de trabajo que se puedan automatizar. (FORTINET, 2019)

En el sector académico se tiene el caso de la Universidad SENATI en la ciudad de Lima, Perú. Presentan un aforo estudiantil de alrededor de 90 mil alumnos e incluyendo al personal docente y administrativo que conforman 5 mil personas, las carreras que manejan en la universidad son de índole operativas, tecnológicas y también incluye ese personal administrativo distribuido a nivel nacional. Todos sus puntos se interconectan con el área administrativa a consecuencia generó el reto de que la conexión a esta sea segura y que las operaciones administrativas funcionen sin inconvenientes. Al trabajar con SD-WAN consideraron la función de un sistema embebido en el hardware aportando a no incluir algún software adicional. Esta solución se pudo aplicar para el control de la entrada y salida de alumnos, una comunicación constante entre las administraciones provinciales y su sede matriz como también se pudo perpetuar seguridad en los puntos de acceso Wi-Fi con un óptimo ancho de banda. Se ha logrado identificar que esta optimización en cuestión ancho de bando se lo logró con SD-WAN en un 60%, se pudo orientar el ancho de banda hacia sitios que los alumnos necesitaban para evitar congestión. De que se visualiza también tiene presente un constante monitoreo de comportamiento de tráfico el cual la herramienta muestrea los datos recolectado y con ello la toma de mejores decisiones. (FORTINET)

La Danish AgriFish Agency, se encarga de la supervisión de las industrias danesas de agricultura y pesca, su función es la de promocionar el crecimiento y la gestión de los recursos naturales de Dinamarca. Su forma de trabajo es inspeccionar desde una flota de barcos las actividades que se recepten en aguas territoriales danesas, siendo así el personal de mencionada agencia trabajan sobre mar, como ya es conocido la cobertura móvil es extremadamente limitada y como parte de su trabajo se requiere comunicación con el personal en tierra. Para poder establecer comunicación se busca navegar cerca de la costa lo que implica apartarse de donde se encuentran ejecutando su trabajo, lo hacen con comunicaciones vía satélite lo cual son muy costosas.

Zentura que es socio de Citrix, ejecutó una propuesta a NetScaler SD-WAN de automatizar la selección de enlaces móviles o vía satélite basándose en función de las condiciones, con lo que el tráfico fluiría mejor sin intervención manual. Utilizando como adicional Citrix XenDesktop y XenApp, que se puede decir que garantiza un acceso remoto a las aplicaciones sin problemas de rendimiento dio como resultado la fiabilidad de conexión en el mar su cobertura móvil se ha incrementado significativamente reflejado en distancia antes mantenían conectividad a 5/8 millas náuticas de la costa y ahora lo realizan a 23 millas de Skagen, se comenta que es un alivio centrarse en las inspecciones o trabajar a realizar que estar buscando un lugar conveniente donde establecer conexión a tierra. Lo que se resumen que la solución SD-WAN en este ámbito es un esfuerzo donde se conectan a través de la red móvil y satelital usando la mejor en la ubicación o situación del personal, es un cambio automático entre los dos medios de transmisión lo que elimina el trabajo de cambio manual, también es evidente la mejor de velocidad de conexión ya que analiza las latencias de cada enlace. (CITRIX)

Organización del Trabajo

Primer Capítulo

Este capítulo presenta lo más relevante de la tecnología que se identifica en la introducción, nos muestra trabajos en su proceso de implementación con resultados parciales representativos tanto a nivel de infraestructura como a nivel económico y lo que se puede lograr con el desarrollo del mismo en nuestro ámbito local. Se detalla también los propósitos que es parte de un proceso al cual requerimos cumplir, especificados como objetivos.

Segundo Capítulo

Se presenta la información más relevante sobre la tecnología SD-WAN en su proceso de desarrollo y llegada al país, las tecnologías que hoy por hoy se maneja en el Ecuador en los diferentes ISP, como también el establecimiento y las condiciones para poder incursionar en SD-WAN. Se habla de la importancia de las aplicaciones que cursan sobre nuestro canal, el aspecto de condiciones de funcionamiento y como difieren sus parámetros a nivel de protocolos. Se muestra dos marcas representativas en el país para la implementación SD-WAN.

Tercer Capítulo

Muestra la descripción sobre el desarrollo del proyecto, tenemos como primer paso la presentación de las marcas seleccionadas que implica detallar las diferencias a nivel de su programación, una vez establecidos nuestras conexiones, se puntualizará los proveedores que intervendrán en estas conexiones, se continua con el establecimiento de políticas aplicables a cada hardware y la ejecución de pruebas sobre los canales.

Cuarto Capítulo

Contiene la información resultante de las pruebas realizadas con sus respectivas variaciones y el análisis del comportamiento deseado a las aplicaciones de mayor demanda. Se presenta una comparativa y evaluación de la tecnología aplicada a los diferentes ISP y marcas que intervengan.

Quinto Capítulo

Se establece un análisis de comportamiento de las aplicaciones y cómo podemos integrarlos en nuestros negocios, vida diaria, etc., dando a conocer de manera básica criterio de configuración. Se muestra el cumplimiento de nuestros objetivos transparentados en las conclusiones. Adicional se proponen trabajos que se logren desplegar a diferentes líneas del mercado en el país y conferir continuidad del trabajo presentado.

CAPÍTULO II

FUNDAMENTO TEÓRICO

Redes Definidas por Software (SDN)

Antecedentes

Para que surja las redes SDN, existieron algunas contribuciones, se puede citar una de ellas a principios de los años 80, que fue SOFTNET, una red multisalto que tienen cierta similitud a las redes WSN (Wireless Sensor Networks) que se utilizan en la actualidad. Esta programación permitió en cada paquete transmitido, incluía ya ciertas sentencias en donde los diferentes puntos de red cuando los recibía los iba procesando, lo cual permitió que en cualquier momento se modifique la red según instrucciones de manera dinámica. Este proyecto se la puede considerar como uno que trató establecer una red de autogestión, que impulsaba a crear nuevos protocolos, no se registró un seguimiento a este tipo de proyectos, pero la idea se la considera como la raíz de lo que luego se definió como Redes Activas (Roncero Hervás, 2014).

A partir de este trabajo a principios de los años 90 y tomando como principio las Redes Activas se podrá identificar 3 etapas:

- Las redes activas (1995-2000 aprox.)

El lanzamiento del internet desembocó a que los desarrolladores apresuraran la creación de nuevos protocolos ya que las redes tradicionales de ese entonces no eran programables, se utiliza entonces las Redes Activas, que, transportaban paquetes embebidos en cortos programas que se

ejecutaban en los dispositivos de red por los que pasaba, los enrutadores y conmutadores participaban de este proceso. De lo que se percataron fue de la complejidad que se manejaba, por lo que los desarrolladores se dedicaron a investigar posibilidades a los servicios que se brindaban por internet mediante IP o ATM.

- La separación del plano de control del plano de datos (2001-2007 aprox.)

Desde los inicios de internet que fue a partir de los 90 durante los 10 años consiguientes existió un aumento de tráfico de manera exponencial, con este desborde nace una nueva necesidad, seguridad sobre las redes.

En el siglo XXI los esfuerzos empiezan a enfocarse a redes más seguras, resultado de esto programadores buscaron mejores maneras de gestionar la red, se hablaba de ingeniería de tráfico, pero los protocolos convencionales de enrutamiento todavía eran muy precarios.

Otro esfuerzo que surgió fue la implementación del reenvío de paquetes por el plano de datos separada del plano de control.

- La aparición de la interfaz de programación de aplicaciones de Openflow (2007-2010 aprox.)

En los años siguientes proponen investigaciones sobre el desarrollo de manejo de las redes a escala con lo que la Universidad de Standford y un grupo de investigadores crean el Clean Slate Program

presentando una interfaz abierta, muestran diferentes maneras de separar el plano de datos del de control y a su a vez escalable, todo esto a través de la creación del protocolo Openflow y cabe recalcar que se la pudo lograr gracias también a la vinculación de la virtualización, consecuentemente las diferentes empresas apertura sus APIs para el estudio conjunto de su programación y los comportamientos de reenvío, en un lanzamiento del protocolo a nivel general se la pudo ejecutar en los conmutadores sin ningún cambio de hardware sino con actualizaciones de firmware. Esto se consolidó en un gran logro que instauró un modelo en la evolución de SDN (Garden, 2015).

Generalidades

Viendo en retrospectiva del uso más común que se le daba al internet hace algún tiempo, podremos recordar que, a parte de la navegación común, se enviaba correo, búsqueda de información, descargas archivos, programas, música, etc.

Se evidencia que en menos de una década se ha dado un gran salto en el avance de desarrollo de software mediante aplicaciones que podemos obtenerlas a través de internet, como por ejemplo las redes sociales, aplicaciones de transmisión de video y voz, aplicaciones que son cargadas en la nube, entre otros. Si bien el mundo del internet se ha desarrollado de esta manera podemos darnos cuenta en primera instancia que la velocidad en nuestra conexión de enlace, cada vez nos queda más corta, puesto que estos avances ocupan mucha más programación, elementos y recursos.

La unión de estas circunstancias, junto a otros términos de igual influencia como Cloud Computing y Big Data, requiere un constante estudio, avance y desarrollo en el mundo de las telecomunicaciones,

para que los diferentes ISP faciliten una alta calidad de conexión, tolerante a cambios y sobre todo con menos trabajo manual por parte del hombre, que es susceptible a fallos.

Los diferentes medios de transmisión que se disponen en el mercado son tecnologías que se ha venido usando desde siempre y con menos creciente en innovación. También se ha realizado el intento de cubrir estas necesidades de mejora mediante protocolos, su punto en contra es que requieren mucho tiempo para ser estandarizados; son parches de soluciones que no han llegado a la raíz del problema, es decir, la existencia de un proceso de comunicación más eficiente.

Se propone una solución en el cual parte de sus requerimientos es que, no exista demasiada interacción con el hombre, otorgue inteligencia sobre redes y un hardware especializado en procesar todo lo antes mencionado.

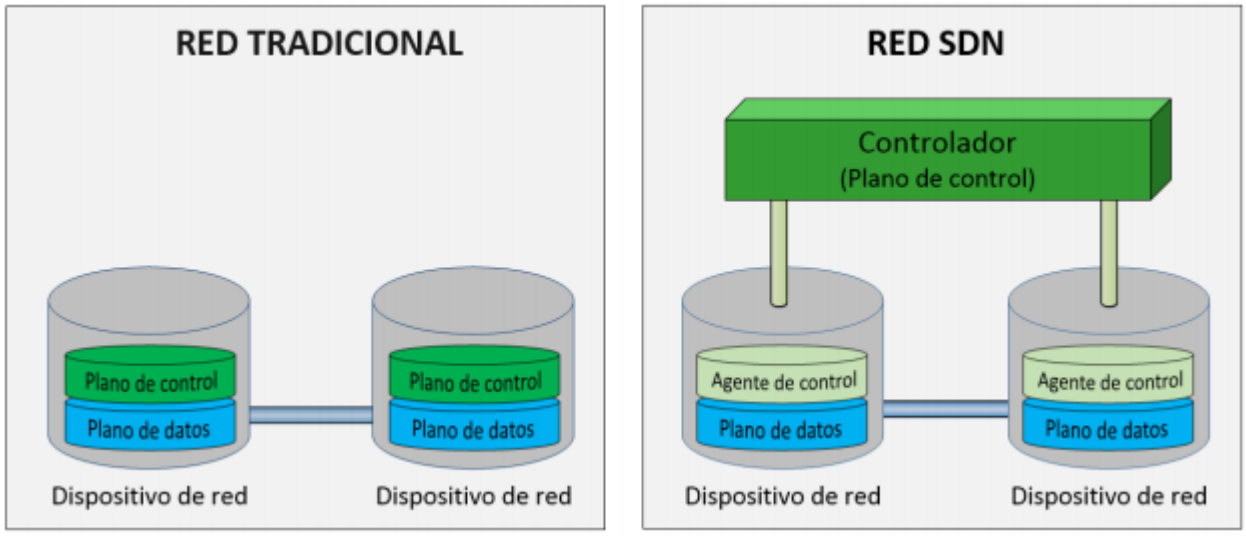
Es donde se considera el concepto de Redes Definidas por Software (SDN) el cual hace referencia a una arquitectura que establece dividir el plano de control del plano de datos, donde dispone de un controlador lógicamente centralizado el cual posee una vista de red global y que a su vez es el encargado de la toma de decisiones de control estableciendo vías de comunicación para reenvíos en la red ejecutándolo mediante la parte física que son las interfaces designadas, de esta manera se considera que SDN virtualiza la red colocando muy a parte el tema físico.

Si bien es cierto que SDN ha existido desde los inicios de Internet, en los últimos años es donde ha tomado mayor impulso para su focalización y desarrollo, para un mejor entendimiento de lo mencionado se compara con las redes tradicionales actuales. Las redes actuales ejecutan el procesamiento de paquetes

el cual dependen netamente de la programación, a diferencia de SDN ésta ya incluye la programación precargada en software que administra su comportamiento. Actualmente los nodos dependen de la definición de su programador para el procesamiento de paquetes, la manera en cómo lo maneja, es el software quien envía las indicaciones de procesamientos de dichos paquetes a la red con la inteligencia de ejecutarlo de una manera dinámica.

Figura 1

Redes Tradicionales vs Redes SDN.



Nota. Fuente: (Álvarez Pinilla, 2015)

Como se logra visualizar en la Figura 1 en las redes tradicionales cada dispositivo de red tiene un control independiente de los otros, las funciones que ejecute y la aplicación de programación sólo intervendrá el dispositivo como único. De lo que se logra observar en redes SDN existe un agente controlador relegando a los dispositivos de red ejecutar un plano de control, y este controlador a su vez será el encargado de anunciar a los dispositivos de red los requisitos que se requiera para dicha red, los

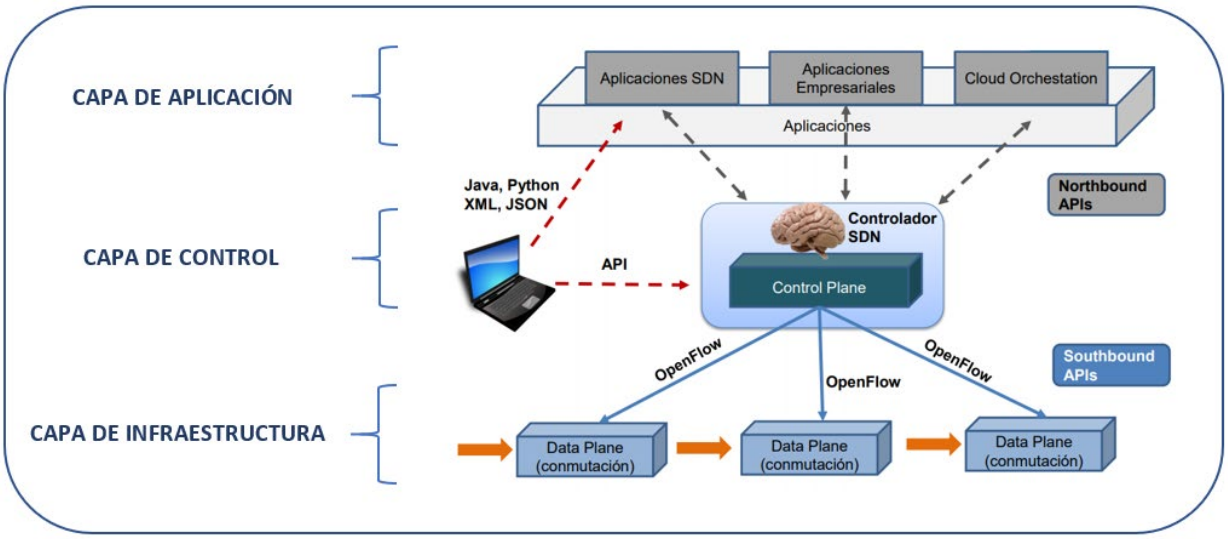
dispositivos red dispondrán de un agente que recepta la información anunciada por el controlador y sólo las ejecutará.

Arquitectura SDN

La arquitectura que comprende SDN es definida en 3 capas como se muestra en la Figura 2:

Figura 2

Arquitectura SDN.



Nota. Adaptado de Arquitectura SDN, Fuente: (Ccoyllo Sulca, 2018)

Capa de Aplicación. – En esta capa se ubican las aplicaciones de los usuarios que se encuentran conectadas hacia la capa de control utilizando servicios de comunicación de SDN que son las denominadas APIs, hacia arriba (Northbound), tales como: Java, XML, JSON, Phyton, REST, etc. (Millán Tejedor, 2014)

Las APIs Northbound ya vienen programadas con la toma de muestras de uso en la red de cada aplicación, y su objetivo es dar a conocer estas muestras a la capa de control para que se procese y ejecute las normas correctas con respecto a toma de decisiones, cabe mencionar que, para finalizar el procesamiento de la data, el controlador SDN proyecta las decisiones procesadas y las comunica a la capa inferior que es la de infraestructura mediante SouthBound APIs. (Roncero Hervás, 2014)

Capa de Control. – La capa de control como su nombre lo indica es el ente controlador entre la interacción de la capa de infraestructura y la capa de aplicaciones utilizando interfaces: Northbound y Southbound, y protocolos. Esta capa puede poseer un controlador o un grupo de dos o más controladores SDN dispuestos para la administración de políticas. (Gonzalez, 2018)

El controlador SDN es el cerebro de operación de la red que controla los recursos para luego ser designados, encargándose de la comunicación entre las aplicaciones y dispositivos. Recepta los requisitos de la capa de Aplicación y los traduce hacia los elementos de red por medio de protocolos en este caso por medio de Openflow; en viceversa proporciona data de importancia a las aplicaciones SDN. (Garcia Centeno, Rodríguez Vergel, Anías Calderón, & Casmartiño Bondarenko, 2014).

En esta capa se controla y configura los dispositivos que intervienen en la red de manera que el flujo de tráfico sea correctamente direccionado. En el caso de las redes tradicionales los puntos de red ejecutan el trabajo de conmutaciones y dirigían el tráfico según sus políticas internas, en el plano de control de SDN estas actividades son relegadas al controlador y considerando que los dispositivos de red sólo procesarán órdenes dadas por el controlador, se podría decir que no aplica la selección de protocolos

específicos dependiendo de cuáles manejen las interfaces, el controlador tiene a disposición vastos recursos del plano de datos para poder unificar y facilitar su configuración. (Millán Tejedor, 2014)

Capa de Infraestructura. – Se establece que la capa de infraestructura es muy similar a la red tradicional, ya que se compone de los equipos físicos que será los medios de transmisión los switches, routers, hosts y demás elementos, estos deberán disponer como característica incluyente que soporten el protocolo Openflow. Este protocolo distribuye el reenvío de paquetes mediante la red llevando consigo la información de recolección de las capas superiores. (Salinas Santiago, Sánchez Venegas, Herrera Velásquez, & Santiago C, 2019)

Se cita que SDN se debe diferenciar bien los elementos de la arquitectura de los componentes.

Componentes. Los componentes son la manera en cómo están conformados dichos elementos y bajo qué características, en general mostrado en la Figura 3.

Aplicaciones SDN. – Comprende todas las aplicaciones que se destinan para los usuarios, de estas se puede detallar lo que respecta ingeniería de tráfico, calidad de servicio, también existen las aplicaciones empresariales, un manejador en la nube y muchas otras. Las aplicaciones SDN son programas que comunican sus requerimientos de red y el comportamiento requerido al controlador SDN a través de las interfaces de frontera norte (NBI – Northbound Interfaces). Asimismo, están conformadas por un método de aplicación y uno o más NBI, lo cual logra ampliar y reemplazar los mecanismos de operación que se efectúan en los dispositivos de hardware de una red tradicional (Open Networking Foundation, 2013).

Estas aplicaciones SDN tienen la posibilidad de cambiar su proceder de la red en tiempo real, de esta manera se adaptan a los diferentes cambios requeridos que pueda existir en una organización o empresa como, por ejemplo, una adaptación dinámica por parámetros aceptable del ancho de banda a nivel de los servicios que se necesite acceder, la selección de la ruta más óptima para envío de información, descartar intrusiones que pueda existir a la red interna, entre otras (Frómeta Fonseca, Anías Calderón, Ballester Macías, & León González, 2016).

Controlador SDN. – Como su nombre lo indica es un controlado, que trabaja de manera centralizada y lógicamente se recepta la información de la capa de aplicación, lo traduce y realiza la deliberación hacia la capa de infraestructura mediante las interfaces de frontera sur (SBI – Southbound Interfaces), para las aplicaciones SDN provee visibilidad abstracta de la red que incluye eventos y estadísticas. El controlador SDN está compuesto por uno o más agentes NBI, el controlador lógico, que corresponde al sistema operativo de la red que opera todas las comunicaciones ente dispositivos y aplicativos, y por último el controlador lo denominado la interfaz entre el control y el plano de datos (CDPI) (Open Networking Foundation, 2013).

Ruta de datos SDN (SDN Datapath). – Corresponde a un dispositivo lógico de la red que nos muestra y controla su capacidad de reenvío y procesamiento de los datos, se puede decir que incorpora a un todo o subconjunto de recursos físicos.

Un Datapath SDN se encuentra conformado por un agente CDPI, mecanismos de reenvío de tráfico y funciones de procesamiento de tráfico. Se puede decir que es la mezcla física constituida de varios

recursos de comunicaciones, gestionados como una unidad, o también a través de varios dispositivos físicos en la red.

Control SDN a la Interfaz del Plano de Datos (CDPI). - Es la interfaz que delimita entre un Controlador SDN y un Datapath SDN, su función es la de controlar de manera ordenada todos los reenvíos operacionales, notificación de capacidades, reportes estadísticos y notificación de eventos

El valor agregado de SDN incide en la probabilidad de que CDPI pueda ser puesta en producción en un sistema abierto, neutral para el vendedor y de forma inter operativa.

Interfaces de frontera norte (Northbound Interfaces - NBI). – Son interfaces que se ubican entre la capa de aplicación o aplicaciones y el Controlador SDN, básicamente proveen la visibilidad de la red de manera abstracta y permiten el intercambio de información del comportamientos y requisitos de la red.

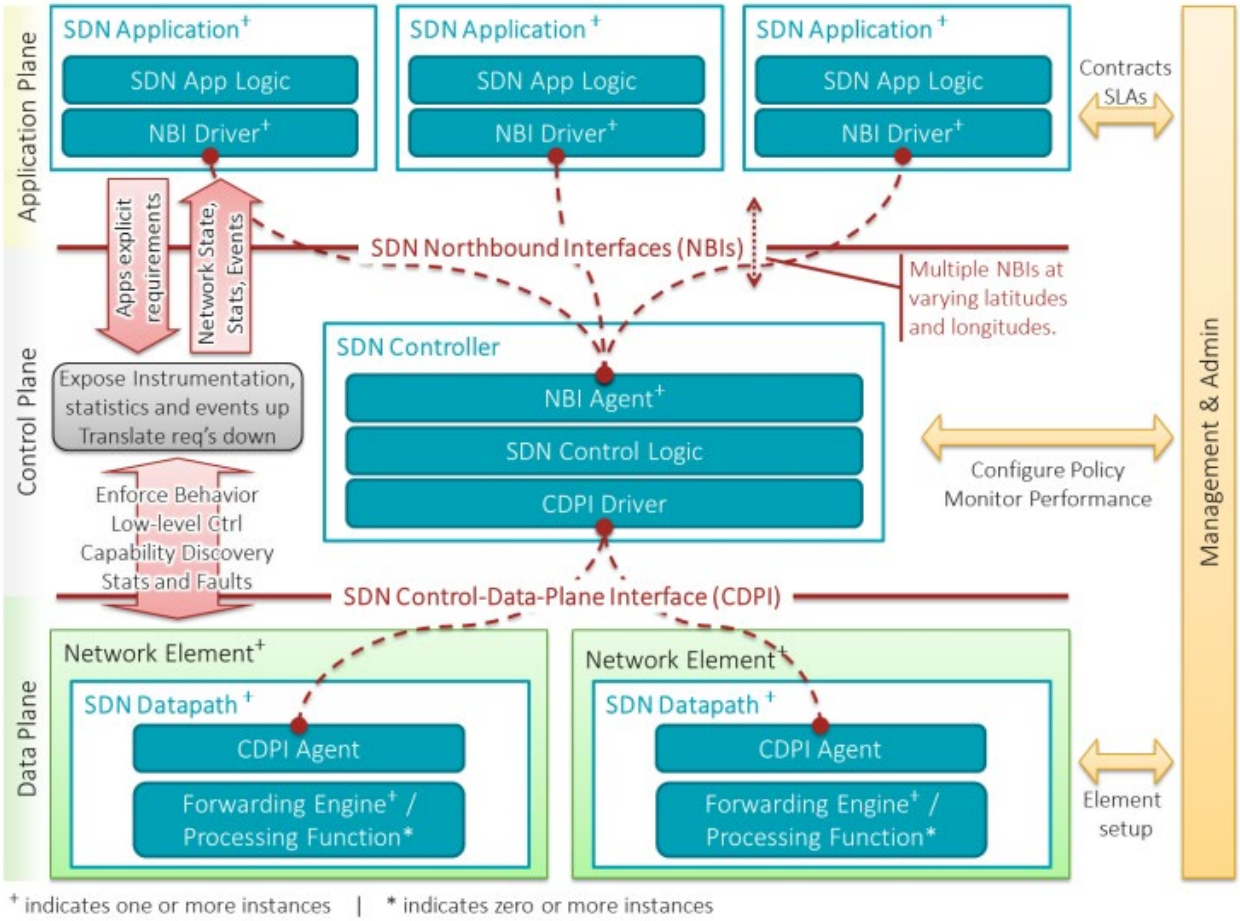
Las NBI desempeñan un rol importante que lo que respecta SDN ya que faculta a los programadores la libertad de desarrollar sus aplicaciones de manera general y no se limitan por complejidades de las redes subyacentes. Cada programador ejecutaría su aplicación con el lenguaje de programación de su elección, únicamente el Controlador SDN deberá realizar la traducción con el lenguaje que maneje y aprovisionar recursos y servicios de red satisfagan las condiciones de la aplicación (Pham & B. Hoang, 2016).

Controladores y agentes de la interfaz. - Cada interfaz en esta arquitectura es implementada por un par: conductor-agente, el conductor está relacionado con el que da la vía a la capa superior que es la de aplicación y el agente está relacionado con el que da la vía hacia la capa de infraestructura.

Gestión y Administración. – El plano de Gestión comprende las tareas estáticas que se usan por fuera del plano de aplicación, control y datos, se puede citar las configuraciones de los equipos físicos, credenciales de acceso, asignación de recursos lógicos para el cliente.

Figura 3

Vista general Arquitectura SDN - Componentes.



Nota. Fuente (Open Networking Foundation, 2013)

Elementos. Los elementos son los que intervienen en la arquitectura.

Protocolo (Software). – El primer protocolo que se creó para desarrollo de redes SDN fue OpenFlow, un trabajo que fue guía la ONF (Open Networking Foundation). Existen otros protocolos que los desarrolladores conjuntamente con las marcas han ido creando adaptándose a sus necesidades como lo son:

- NETCONF/YANG
- ForCES
- LISP
- PCEP
- OpFlex

Equipo de cómputo controlador (hardware y software) SO. – Puede ser según amerite o sea de selección de la marca:

- GNU/Linux
- Mac
- Windows

Sistema Operativo de Red (Software del controlador). –

- ONOS, OpenDaylight y Beacon – Tres controladores basados en Java, modulares y multiplataforma.

- NOX – Plataforma OpenSource escrita en C++ o Python
- Trema – Full-Stack Framework de OpenFlow para lenguajes Ruby y ANSI C
- Maestro – Escrito en JAVA con soporte para Switches OpenFlow
- MUL – Escrito en lenguaje C con una arquitectura centralizada.

Lenguaje de programación de alto nivel para el establecimiento las de políticas de comunicación:

- Frenetic – Escrito en Python posee dos módulos, uno para monitoreo de los recursos de la red y otro para el establecimiento de las políticas.
- Procera – Políticas de flujo y enrutamiento basadas en hora del día, cantidad de datos transmitidos, privilegios o grupos de usuarios y tipo de tráfico transmitido. Se puede usar FRP (Funtional Reactive Programming) y Haskell.
- Directamente a través de lenguajes de programación como C, C++, Java, Python, o de especificación directa de flujos como JSON y XML.

Equipos convencionales switching y routing con soporte para el protocolo SDN. – Aquí citaremos las empresas que en el transcurso y crecimiento de las redes SDN han ido lanzando sus versiones en hardware y software para implementaciones:

- NEC
- HP Networking
- Cisco Systems
- Alcatel-Lucent

- Huawei
- Spirent
- ICIA
- DCN
- xNet
- Greenet
- ZTE
- Pica8
- H3C
- EstiNet

(Ramírez Giraldo & López Echeverry, 2018)

Objetivos SDN

La principal idea que se requiere de las redes SDN es la de dotar a los administradores de las suficientes herramientas que sean manejadas de manera centralizada, para programar, virtualizar y monitorear su infraestructura en tiempo real, adaptándose de manera eficiente e instantánea a los cambios que se puedan aplicar según requerimientos que vayan surgiendo, consecuentemente acelerará el proceso de renovación de los Datacenter hacia una nueva concepción más escalable que logre también: automatizar recursos, facilitar las diferentes tareas y marcar un precedente en el antes y después en del mundo de las redes y comunicaciones. Con SDN el análisis de paquetes ya no se origina de una serie de archivos de configuración en cada nodo que exista, sino lo ejecuta de manera dinámica través de una cada de software que virtualiza la red y la separa de la infraestructura física subyacente.

Se puede ver el grado de importancia a medida que las redes digitales crecen y son más complejas, también lo hace la virtualización y la necesidad de que sean tolerantes y escalables al máximo.

Se resume en la mejora de capacidad frente a las redes tradicionales con las siguientes características:

- No existe la necesidad de configurar cada equipo o sistema operativo de manera aislada una de la otra.
- El mantenimiento de la red y su gestión se reduce de manera significativa.
- El costo que involucra el hardware y su funcionamiento disminuyen.
- Dispone de la facultad de proveer y registrar recursos en tiempo real en un procedimiento dinámico.
- Existe una desvinculación de relación limitada con los fabricantes de software, no es necesario sólo poseer un proveedor por disponer de software propietario. El disponer de un protocolo abierto como lo es OpenFlow transforma a SDN en una selección extraordinaria si se gestiona dispositivos de diferentes fabricantes en la red.

SD-WAN

SD-WAN (Software-Defined Wide Area Network) o Redes de Área Amplia Definidas por Software, es el nuevo enfoque que se ha tomado para la construcción de redes WAN, en donde tanto la configuración de la red como las aplicaciones se encuentran aisladas de los servicios de red los cuales pueden ser: tipos de acceso al internet, servicios de datos (privados), entre otros. Como resultado de la aplicación de esta nueva tecnología, se pueden configurar, añadir o eliminar los servicios de una red sin afectar la misma.

Las soluciones que ofrece esta tecnología responden a preocupaciones generadas en las redes WAN tradicionales como los altos costos que al momento tiene la contratación de paquetes de ancho de banda, los tiempos de despliegue, las recurrentes reconfiguraciones que se deben estar haciendo, entre otros aspectos.

Estos procesos deben funcionar todo el tiempo, ya que de ellos depende la capacidad de informar instantáneamente la inminencia de un peligro, y deben estar siempre en proceso de mejora continua.

El Problema con las Redes WAN Tradicionales

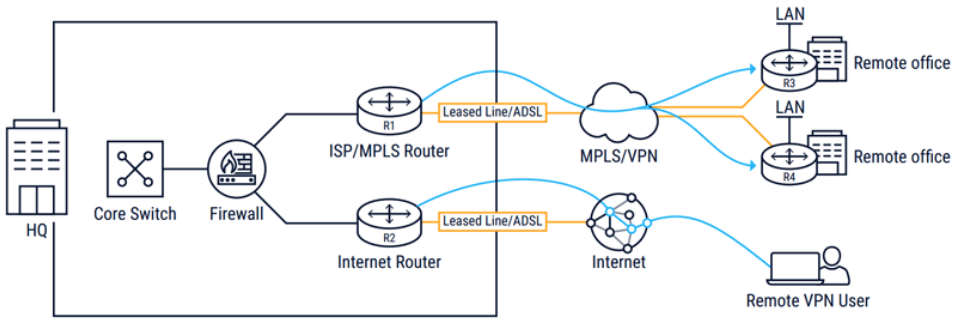
Durante muchos años, las organizaciones han conectado sus puntos con servicios de datos privados mediante el protocolo MPLS (MultiProtocol Label Switching). Donde las empresas contratan con un Proveedor de Internet, un servicio, el cual por defecto trae consigo un enrutador MPLS. Estos enrutadores tienen una interconexión entre varios puntos a través de los servicios que ofrecen las Redes MPLS y pueden ser considerados como servicios:

- Privados: El tráfico del cliente está separado del resto.
- Predecibles: Toda red MPLS tiene un diseño en el cual existe una pérdida de paquetes muy baja.
- Confiables: Los proveedores respaldan las redes MPLS con servicio y soporte, lo que ofrece garantías de tiempo de actividad o funcionabilidad y confiabilidad.

En la Figura 4 se dispone del detalle de las líneas de comunicación que se levantan en una red tradicional MPLS para los diferentes servicios ya sea internet y datos y engloba las consideraciones antes mencionados.

Figura 4

Redes VPN MPLS tradicionales de alto costo.



Nota. Fuente *(FIREWALL.CX, 2020)*

Por lo que los servicios MPLS tienen altos costos en relación con la conectividad a Internet, tomando en cuenta que existen casos que estos servicios pueden llegar a costar un 90% más que el ancho de banda de Internet. Es por esto que las organizaciones deben siempre tener mesura en cuanto al uso de ancho de banda.

A menudo los puntos de una organización están conectados por una sola línea MPLS, lo que genera una potencial falla en ese punto, ya que estas líneas muchas veces carecen de capacidad necesaria para acomodar cambios de tráfico o nuevas actualizaciones.

Por último, los nuevos despliegues dentro de una Red MPLS toman mucho más tiempo que las líneas de Internet, pueden ser semanas o en casos extremos meses, mientras que el acceso al Internet se lo puedo desplegar en minutos o máximo en unos cuantos días.

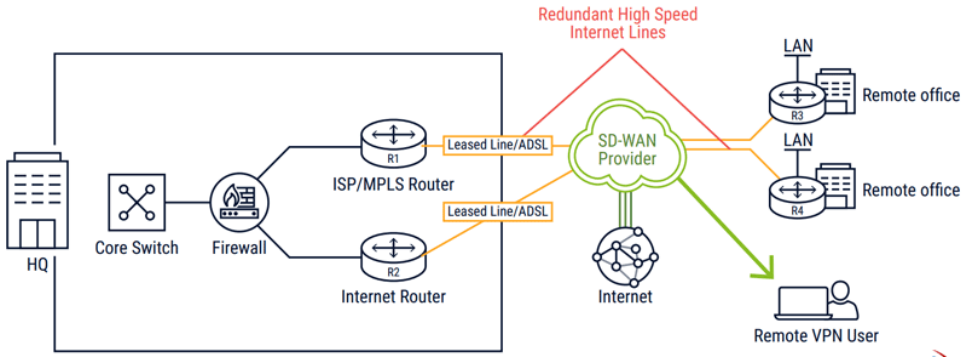
Por todo lo mencionado anteriormente, en la actualidad, muchas organizaciones desean que el tráfico de Internet y de la nube sea una norma y no una excepción, ya que de esta manera se puede llegar a constituir la mitad del tráfico de la red MPLS, obteniendo como resultado la disminución de los costos de transmisión de datos.

Funcionamiento SD-WAN

La tecnología SD-WAN aprovecha en su totalidad las conexiones de Internet ubicuas para reemplazar las redes MPLS. Hablando de un alto nivel, SD-WAN asila las aplicaciones de los servicios de red subyacente. Los algoritmos de enrutamiento inteligente, las políticas, y otras características que trae consigo SD-WAN hacen posible que la red se adapte a la aplicación.

Figura 5

Esquema de funcionamiento SD-WAN.



Nota. Fuente: (FIREWALL.CX, 2020)

Videoconferencia

A medida que la tecnología se desarrolla de manera exponencial como herramienta para diferentes ámbitos y debido a los cambios que en la actualidad afrontamos, los cuales han causado un gran impacto en el uso de los mismos; uno de los métodos de comunicación tecnológica que ha tenido mucha relevancia es lo que llamamos la videoconferencia.

La videoconferencia es un sistema o servicio de comunicación que nos permite interactuar en tiempo real de manera visual, auditiva y verbal entre individuos ubicados en distintas áreas geográficas, así como también el intercambio interactivo de información.

Componentes básicos de Videoconferencia

Red de comunicación. La red de comunicación es el elemento fundamental y necesario, el cual permitirá la transmisión multimedia entre usuarios. Se requiere disponer de una red adecuada para poder tener flujos de datos estables, ya que las condiciones de red se van a encontrar en constante cambio en cada uno de los usuarios. Actualmente existe variedad en cuanto a redes de comunicación, por lo que dependerá de las necesidades y requerimientos del usuario para poder obtener un sistema de videoconferencia confiable y de calidad.

Terminales de videoconferencia. Los terminales son los equipos de control de audio y video, lo cuales puedes ser personales, de sala o para propósitos específicos.

- Los terminales personales son dirigidos para un único usuario o grupos pequeños ya que son equipos funcionales y de uso diario, tales como ordenadores de escritorio (monitor, cámara web, micrófono y altavoces), laptops, teléfonos inteligentes.

- Los terminales de sala son dirigidos para grupos grandes, los cuales son ubicados en salas de conferencia. Son de coste más elevado, ya que requieren una red de comunicación de calidad con un mayor ancho de banda y usan equipos más robustos como pantallas grandes, proyectores, más de un ordenador, etc.

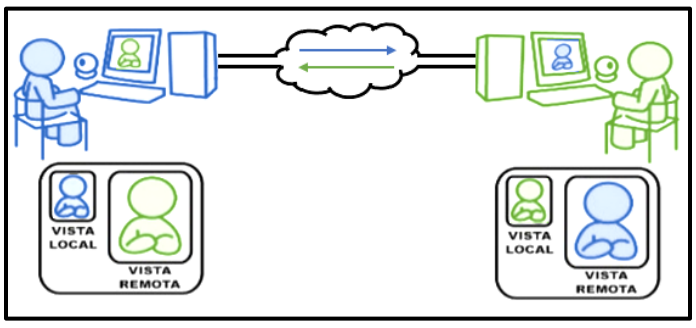
- Los terminales de propósito específico cumplen una función concreta para el cual ha sido diseñado, tales como terminales para aplicaciones médicas y telemedicina, terminales de uso público, terminales educativas y de formación a distancia, etc.

Tipos de Videoconferencia

Punto a punto. Es una conexión directa bidireccional entre dos usuarios, mostrada en la Figura 6.

Figura 6

Conexión bidireccional punto a punto.

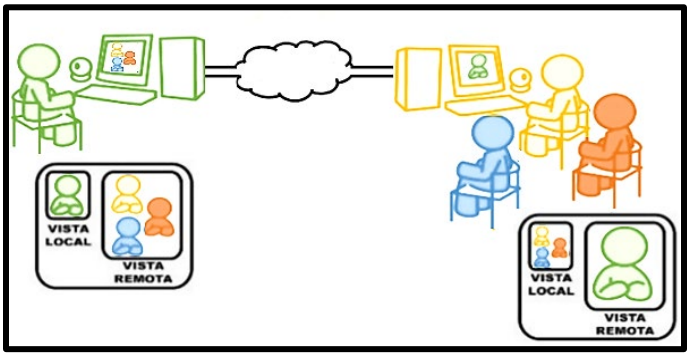


Nota. Fuente (Lajara, Martí, & Villagarcía, 2016)

Multipunto. Permite enlazar una conexión con más de tres usuarios en una misma videoconferencia, las cuales pueden ser interactivas o por difusión; es decir, los usuarios intercambian información entre si simultáneamente o la señal (Figura 7) de un solo usuario se transmite hacia los demás sin interacción de los demás usuarios durante la sesión de videoconferencia. Este tipo de videoconferencia hace referencia de manera gráfica según la Figura 8.

Figura 7

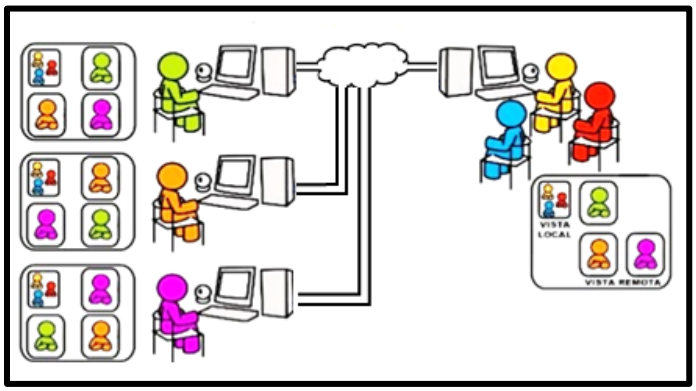
Configuraciones de la señal de finalización.



Nota. (Lajara, Martí, & Villagarcía, 2016)

Figura 8

Conexión bidireccional multipunto.



Nota. Fuente (Romo & Zatarin, 2008)

Aplicaciones y beneficios de la videoconferencia.

- Aplicaciones:

  - Educación y formación a distancia
  - Reuniones empresariales
  - Soporte a clientes de manera remota
  - Comunicación entre usuarios físicamente distantes
  - Capacitaciones / Seminarios
  - Telemedicina / Teletrabajo

- Beneficios

- Fácil de usar: Su interfaz es muy sencilla de utilizar.

- Comunicación: Facilita la comunicación entre personas de distintas áreas geográficas; a diferencia de una llamada telefónica, se tiene contacto visual y esto permite que la interacción sea más real.

- Reduce tiempo y costos: No es necesario trasladarse a otra área geográfica para comunicarte con otras personas, por lo que se reducen los costos y el tiempo invertido de desplazamiento.

- Aumento de productividad: El tiempo ahorrado en el desplazamiento puede ser invertido en otras actividades o tareas.

- Herramienta de colaboración: Permite que los usuarios trabajen en conjunto compartiendo información, contenido de pantalla, diapositivas, etc.; facilitando la formación académicamente a distancia y las reuniones de tipo empresariales.

Estándares ITU de videoconferencia

Se detalla los estándares definidos según la ITU (Unión Internacional de Telecomunicaciones) para los protocolos de videoconferencia:

- H.320

Es un conjunto de recomendaciones dictadas por la ITU para la trasmisión multimedia de audio, video y datos a través de la red digital de servicios integrados (ISDN) en banda estrecha, especificando los requerimientos técnicos que deben tener los sistemas de videoconferencia; tales como: métodos de comunicación, tipos de terminales, disposiciones de control de llamadas, aspectos relacionados con el terminal y requisitos de funcionamiento.

- H.321

Se describe los requerimientos técnicos de los sistemas de videoconferencia a través de ISDN de banda ancha haciendo uso de tecnologías de redes ATM. Este estándar se originó para poder adaptar los terminales de banda estrecha del estándar H.320 a entornos de banda ancha y puedan ser compatible entre sí.

- H.322

Se originó como una versión mejorada del estándar H.320, por lo que abarca con los requerimientos técnicos del mismo para transmisiones en ISDN de banda estrecha y en una o más redes de área local (LAN), estando configuradas y gestionadas para ofrecer calidad de servicio (QoS). Este fue el primer estándar utilizado por la IEEE en su norma 802.9 para redes LAN Ethernet.

- H.323

Se describe los requerimientos técnicos de los sistemas de videoconferencia basada en transmisión de paquetes (PBN), proporcionando capacidad de comunicación punto a punto, multipunto o de difusión. Este estándar no garantiza calidad de servicio (QoS), por lo que se encuentran fallas en la transmisión de datos, siendo más evidentes en la transmisión de voz y video.

Este estándar cuenta con varias características que permiten tener un rendimiento óptimo, tales como:

- Interoperabilidad
- Robustez
- Flexibilidad
- Independiente a la naturaleza de la red.
- Independiente en cuanto a plataformas y aplicaciones.
- Rapidez en establecimiento de llamadas.
- Permite gestionar el ancho de banda, limitando el número de conexiones que pueda soportar.

- H.324

Se describen los requerimientos técnicos para terminales con comunicación multimedia de baja velocidad binaria que operan a través de la red telefónica general conmutada (GSTN), proporcionando un buen rendimiento y una funcionalidad más consistente en cuanto a audio, video, datos en tiempo real o la combinación de estos.

Protocolos para transmisión de videoconferencia

Cada uno de los estándares dichos anteriormente requieren la utilización de protocolos de audio, video y datos que permitirán establecer la sesión de videoconferencia.

Protocolos de Audios

- G.711: conocido como modulación por impulsos codificados (MIC); representa señales de audio en frecuencias vocales a partir de una tasa de 8000 muestras por segundo, obteniendo un flujo de datos de 64 Kbits/s.

- G.722: este sistema permite la codificación de audio de 7 KHz dentro de 64Kbit/s, proporcionando una buena calidad de voz. Se basa en la modulación por impulsos codificados diferencial adaptada en sub-banda (MICDA-SB), por lo que se tienen tres modos de operación básica: 48Kbit/s, 56 Kbit/s y 64 Kbit/s.

- G.728: codifica señales de voz a 16Kbit/s utilizando métodos de predicción lineal de bajo retardo (LD-CELP). Su retraso es de solo 0,625 ms.

- G.729: utilizado mayormente para aplicaciones de VoIP por su bajo uso en ancho de banda. Codifica señales de voz a 8Kbit/s utilizando métodos de predicción algebraico de estructura conjugada (CS-ACELP).

Se muestra en la Tabla 1 la comparativa de los diferentes protocolos de audio explicados.

Tabla 1

*Tabla comparativa protocolos de audio ITU***.**

Protocolo	*Codificación*	*Tasa binaria (Kbit/s)*	*Retardo (ms)*	*Calidad General (MOS)*
G.711	PCM	64	0.125	4.1
G.722	MICDA-SB	48, 56 o 64	0.125/1.5	4.3
G.728	LD-CELP	16	0.625	3.61
G.729	CS-ACELP	8	15	3.92

Protocolos de Video

- H.261: protocolo de compresión de video diseñado para la transmisión de señales a través de ISDN, utilizando métodos de codificación y decodificación vídeo con velocidades de px64Kbit/s, siendo p un número entero en el rango de 1 a 30.

- H.263: diseñado para la transmisión de señales de video a bajas velocidades binarias. Tiene similitudes con el H.261 en cuanto a la estructura de codificación y decodificación, con la diferencia que se implementaron mejoras en aspectos de calidad de imagen y corrección de errores.

- H.264: conocido como codificador de video avanzado (AVC) o MPEG-4, fue desarrollado en conjunto por la ITU y la ISO como una evolución optimizada sus antecesores para poder suministrar imágenes de mayor calidad sin consumir demasiado ancho de banda, una mayor eficiencia de codificación y robustez ante una amplia variedad de entornos de red.

Este estándar cubre una diversa gama de aplicaciones, tales como:

- CATV: TV por cable.
- DBS: Transmisión directa vía satétile.
- DSL: Línea de abonado digital.
- DTTB: Televisión digital terrestre.
- ISM: Medios de almacenamiento interactivo
- MMM: Envio multimedia (Multimedia mailing).
- MSPN: Servicios multimedia sobre redes de paquetes.
- RTP: Servicios de comunicación en tiempo real.
- RVS: Sistemas de video vigilancia remota.
- SSM: Medios de almacenamiento seriales.

Tabla 2

Tabla Comparativa Protocolos de Video ITU

Protocolo	*Ancho de banda típico (Kbit/s)*	*Eficiencia*	*Retardo*	*Aplicación*
H.261	64 - 2000	Media	Pequeño	Video conferencia, telefonía
H.263	28.8 – 768	Alta	Medio	Video conferencia con baja tasa de bits.
H.264	28.8 - 500	Alta	Grande	Video conferencia, telefonía, video interactivo, televisión digital, video streaming.

Protocolos de Datos

- T.120: diseñado para la transmisión de datos en entornos de conferencias multimedia; se compone de una familia de normas de la serie T que forman parte de su arquitectura y funcionamiento. Proporciona y garantiza la comunicación en tiempo real entre dos o más usuarios independientemente del tipo de red en la que transmiten y asegurando la integridad de los datos.

Fortinet SD WAN

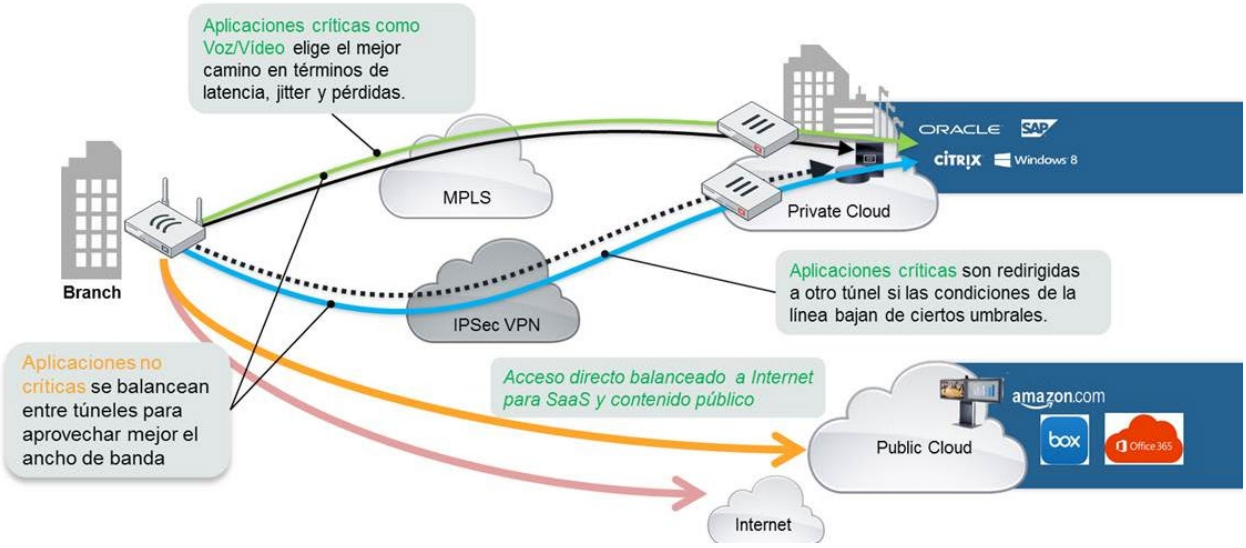
Para Fortinet, SD WAN es una funcionalidad integrada en su sistema operativo que permite a los firewalls Fortigate simplificar la operación y seleccionar los mejores caminos para enviar el tráfico de paquetes hacia un destino. Ofrecen a sus clientes tener múltiples conexiones y seleccionar automáticamente la mejor alternativa para conectarlos del punto A al punto B, considerando las aplicaciones, dándoles prioridad y diferenciación; todo esto aplicando QoS, redes sobrepuestas (VPNs) y seguridad NGFW (Next Generation Firewall).

Arquitectura Fortinet SD-WAN

La solución SD-WAN de Fortinet ofrece una arquitectura de red escalable y rentable que aprovecha todas las capacidades esenciales de SD-WAN entre nubes y permite a los usuarios crear una infraestructura de red de nube a nube segura sin interrupciones y de alta velocidad.

Figura 9

Arquitectura Fortinet SD WAN.



Nota. Fuente: (FortiXpert, 2017)

Características Fortigate SD-WAN

- Reconocimiento de Aplicaciones

Integra una base de datos para identificar más de 3000 aplicaciones, incluso a partir del momento en que se transfiere el primer paquete; lo que permite a sus clientes tener visibilidad completa de las aplicaciones utilizadas en toda su empresa y así estos puedan supervisar y tomar decisiones fundamentales al crear políticas de SD-WAN en función de la criticidad de las aplicaciones.

- Inteligencia de Rutas Múltiples

La inteligencia de reconocimiento de rutas tiene la capacidad de brindar información de rutas WAN, tales como: inestabilidad, latencia y pérdida de paquetes, y en función de este la tecnología de

múltiples caminos decide y selecciona dinámicamente cual es el mejor enlace para enviar el tráfico de cada una de las aplicaciones sin afectar a los usuarios.

- Ancho de Banda Múltiple

Independiente del transporte, por lo que lo hace compatible a una amplia gama de conexiones de ancho de banda como Internet, MPLS, 3G/4G, VPN, etc. Ofreciendo así un impulso agregado a la resiliencia y rentabilidad, evitando interrupciones y la degradación del rendimiento.

- Monitoreo Simplificado

Ofrece monitoreo muy sencillo a través de su producto FortiManager, ya sea de manera local o en la nube, permite ver, gestionar, administrar, configurar y actualizar sus dispositivos Fortigate habilitados con SD-WAN de manera centralizada implementados en cualquier ubicación. Contiene visualizaciones bastante intuitivas, facilitando la supervisión de las topologías de red físicas y lógicas.

- Seguridad NGFW Confiable

La siguiente generación de Firewalls (NGFW) de Fortigate ofrece de las más sólidas protecciones frente a amenazas, siendo el único proveedor de SD-WAN con una recomendación de NSS Labs NGFW. Su arquitectura optimizada provee un profundo análisis de seguridad y capacidades de inspección, algunas de sus características claves son:

  - Protección completa frente a amenazas ocultas en el tráfico web cifrado, antivirus, firewall, IPS y control de aplicaciones.

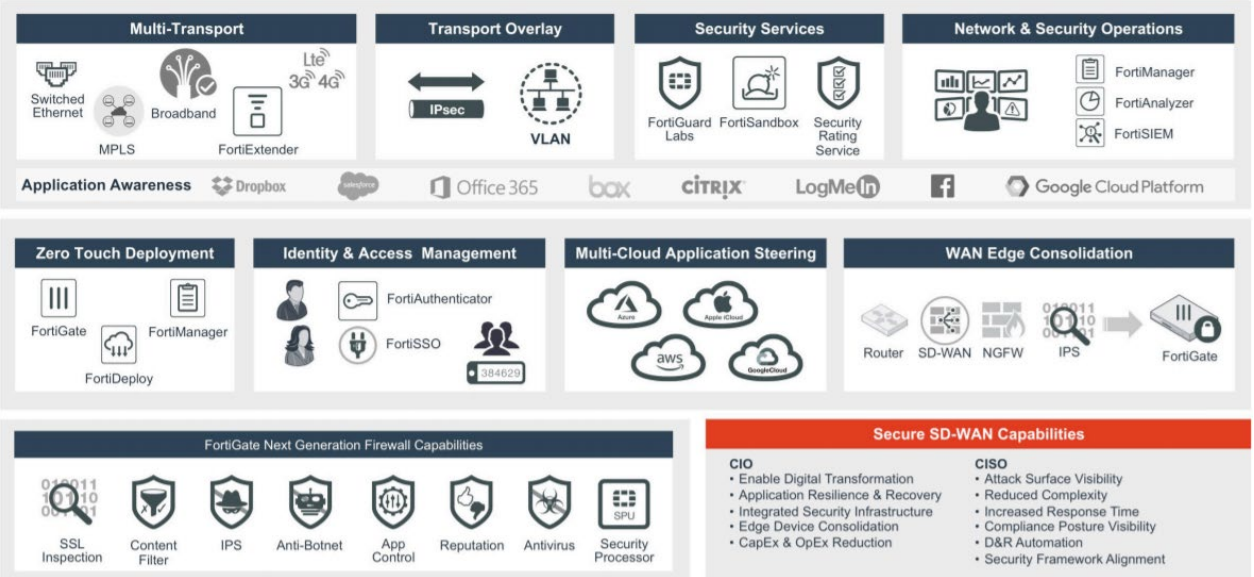
- Servicio de Filtrado Web como primera línea de defensa contra ataques en la web al bloquear el acceso a sitios web maliciosos, y elimina la necesidad de requerir un SWG (Secure Web Gateway) independiente.

- Inspección SSL (Secure Sockets Layer), el cual puede desbloquear sesiones, encontrar amenazas en paquetes cifrados y bloquearlas.

- Establece VPNs IPsec que garantizan el cifrado y autenticación de cada paquete IP para comunicaciones confiables y seguras.

- Informes y seguimiento en tiempo real de la actividad de amenazas, lo que permite facilitar la evaluación de riesgos, localizar y mitigar problemas potenciales. También supervisa políticas y reglas de firewall para automatizar auditorías de cumplimiento.

Figura 10



Componentes de la arquitectura segura SD-WAN de Fortinet.

Nota. Fuente: (Hwang, 2019)

Especificaciones generales Fortigate SD WAN

Fortinet cuenta con una amplia gama de modelos Fortigate que proporcionan una solución SD-WAN escalable, rápida y segura. En la siguiente Tabla 3, se mostrará una comparación general de tres modelos de Fortigate basados en el rendimiento del sistema.

Tabla 3

Especificaciones Generales Modelos FortiGate.

	FortiGate 30E	**FortiGate 60F**	**FortiGate 100F**
			

NGFW Throughput	200 Mbps	1 Gbps	1.6 Gbps
GW to GW IP Sec VPN Tunnels	200	200	2500
VPN Performance	75 Mbps	6.5 Gbps	11.5 Gbps
1 GbE Interface	4	10	26
10 GbE Interface	0	0	2
Threat Protection throughput	150 Mbps	700 Mbps	1 Gbps
SSL Inspection throughput	125 Mbps	630 Mbps	1 Gbps
High availabity configurations	Active/Active, Active/Passive, Clustering	Active/Active, Active/Passive, Clustering	Active/Active, Active/Passive, Clustering
Virtual Domains	5/5	10/10	10/10

Nota. Fuente (FORTINET, 2020), (FORTINET, 2020), (FORTINET, 2020)

Meraki SD WAN

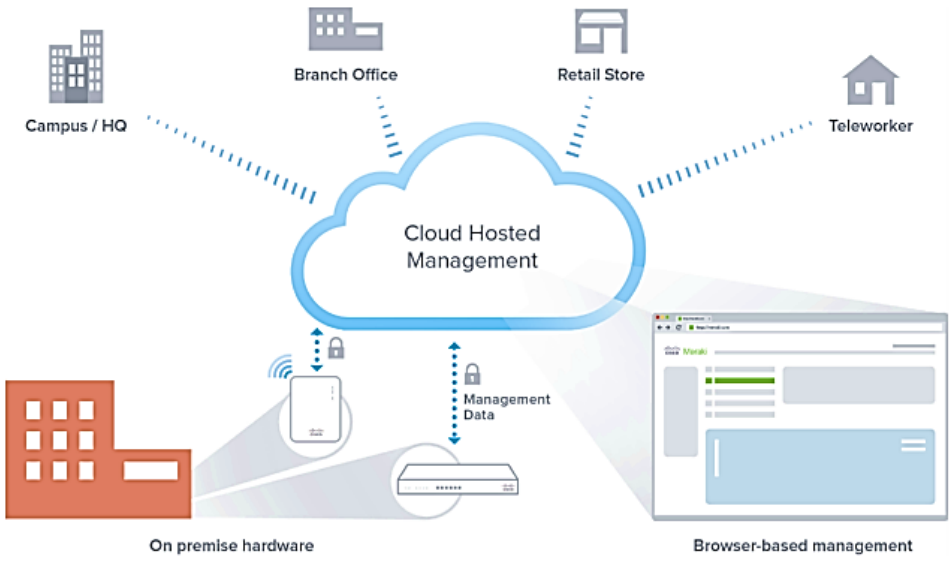
Meraki SD-WAN de Cisco ofrece una serie de funciones basándose en su portfolio de soluciones de seguridad Meraki MX, utilizando una combinación de estas tecnologías para crear esta solución que permite reducir costos operativos, optimizar el uso de recursos para implementación y ancho de banda sin comprometer el rendimiento y la privacidad de los datos; siendo una solución fácil de configurar, implementar y administrar.

Arquitectura Meraki SD WAN

Meraki SD-WAN proporciona una arquitectura fluida 100% centralizada desde la nube (Figura 11) para la administración unificada de amenazas (UTM) y SD-WAN en un solo dispositivo mediante la consola de Cisco. Las potentes herramientas de administración remota brindan visibilidad y control en toda la red.

Figura 11

Arquitectura Cisco Meraki administrada en la nube.



Nota. Fuente: (Cisco)

La arquitectura SD-WAN recomendada para la mayoría de las implementaciones es la siguiente, el cual no excluye el uso de topologías alternativas:

- MX en el centro de datos, desplegado como un concentrador de un solo brazo.
- Warm spare y alta disponibilidad en el datacenter.

- Notificación de ruta OSPF para una conectividad ascendente escalable a subredes VPN conectadas.
- Redundancia del datacenter.
- Túnel VPN dividido de las sucursales y oficinas remotas.
- Dual WAN uplinks en todas las sucursales y oficinas remotas.

Características Meraki SD WAN

- Independencia del transporte.
- Aplica políticas de ancho de banda, enrutamiento y seguridad a través de un cualquier tipo de conexión (MPLS, Internet, 3G/4G LTE) con un único flujo de trabajo consistente e intuitivo.
- Optimización de Aplicaciones
- La priorización de las aplicaciones optimiza el tráfico para aplicaciones críticas y la experiencia del usuario.
- Gestión Centralizada
- Ofrece visibilidad y control centralizados de la red, así como gestión de ancho de banda y calidad de servicio (QoS) con el control de tráfico Meraki.
- Control de ruta inteligente
- La selección de ruta dinámica permite a un administrador de red configurar políticas y criterios de rendimiento para diferentes tipos de tráfico. Las decisiones de ruta se toman por flujo en función de cuál de los túneles IPsec VPN disponibles cumple con estos criterios, determinados mediante el uso de métricas de pérdida de paquetes, latencia y fluctuación que recopila automáticamente el MX.
- Alta disponibilidad y conmutación por error

- Proporciona integridad del dispositivo y la conexión a través de múltiples enlaces directamente conectados, funcionalidad de protocolo dinámico a nivel LAN como mecanismo de conmutación por error y VPN con recuperación automática.
- Conectividad Segura
- Ofrece una variedad de tecnologías integradas altamente efectivas de defensa contra amenazas de seguridad para acceso directo a Internet combinadas con IPsec VPN para garantizar una comunicación segura con aplicaciones en la nube, oficinas remotas o centros de datos. Las funciones se seguridad integradas son:

  - Firewall de próxima generación basado en identidad, el cual asigna automáticamente reglas de firewall, tags de VLANs y limitación de ancho de banda para hacer cumplir las políticas adecuadas para cada tipo de usuarios.

  - Prevención de intrusos, protegiendo los recursos de la red ante amenazas de seguridad más recientes realizando un barrido para comprobar si se ha presentado algún tipo de incidencia, el cual será avisado al administrador del sitio.

  - Protección avanzada contra malware, en la cual la red se defiende utilizando detección inteligente de amenazas más recientes e identificando archivos maliciosos previamente desconocidos.

  - Filtrado de contenido, el cual bloquea contenido web indeseable a través de más de 70 categorías y aprovecha la búsqueda en la nube para filtrar miles de millones de URLs.

- Auto VPN, es una tecnología automatizada simple que permite construir rápida y fácilmente túneles VPN entre dispositivos en sus sucursales de red separadas, brindando resiliencia, seguridad y optimización de las aplicaciones. Tiene generación automática de rutas VPN usando túneles tipo IKE / IPSec y todo esto se hace en la nube Meraki.

Especificaciones generales Meraki SD WAN

Meraki ofrece una variedad de modelos multifuncionales de seguridad y equipados con capacidades SD-WAN tanto para organizaciones de pequeña escala hasta organizaciones de gran escala. En la siguiente Tabla 4 se muestra una comparación general entre modelos Meraki.

Tabla 4

Especificaciones Generales Modelos Meraki.

	Z3	**MX68**	**MX84**
			
Recommended Use Cases	Teleworker with VoIP or PoE, IoT, and M2M	Small Branch	Medium Branch
Recommended max clients	Up to 5	50	200
Interfaces	5 × GbE PoE: 1 × 802.3af PoE enabled port USB 3G/4G	12 × GbE (2 PoE+) USB 3G/4G	10 × GbE 2 × SFP USB 3G/4G
Stateful firewall throughput	100 Mbps	450 Mbps	500 Mbps

Maximum VPN throughput	50 Mbps	200 Mbps	250 Mbps
VPN tunnels	-	50	100
Web caching	-	-	Si
Redundant power	-	-	-

Nota. (Meraki), (Cisco Meraki)

CAPÍTULO III

METODOLOGÍA

Materiales

Para la ejecución del presente trabajo se menciona las herramientas que se utilizarán:

- Equipos que incluya la programación de la tecnología SD-WAN. Para este propósito se ha seleccionado dos marcas:
  - Fortinet: Fortigate 30E
  - Cisco: Meraki MX68 - SPOKE
  - Cisco: Meraki Z3 - HUB
- Software de Videoconferencia: WEBEX, ZOOM, SKYPE, GOOGLE MET, etc
- 2 videoconferencias Cisco.
- PC´s.
- 2 enlaces proveedores diferentes: Telefónica, Telconet.

Topología de prueba - Diagrama de implementación

Para un mejor entendimiento de funcionamiento de las pruebas realizadas y su estructura se muestra el escenario físico de implementación del desarrollo del proyecto.

Diagrama de implementación Fortigate

En la Figura 12, se muestra la ingeniería de implementación ejecutada para la marca Fortinet y cómo éste a su vez dispone de una línea de comunicación hacia el internet mediante los dos proveedores.

En un inicio disponemos del usuario de prueba conectado al equipo Fortigate 30E, este a su vez se ha conectado en dos interfaces físicas, los dos proveedores de internet que disponemos.

Los dos proveedores por disponer de infraestructuras diferentes tendrán una salida hacia el internet con su proveedor internacional respectivamente.

La comunicación final será a la aplicación de videoconferencia, como se visualiza a WEBEX.

Figura 12

Diagrama de implementación SD WAN - Fortigate.

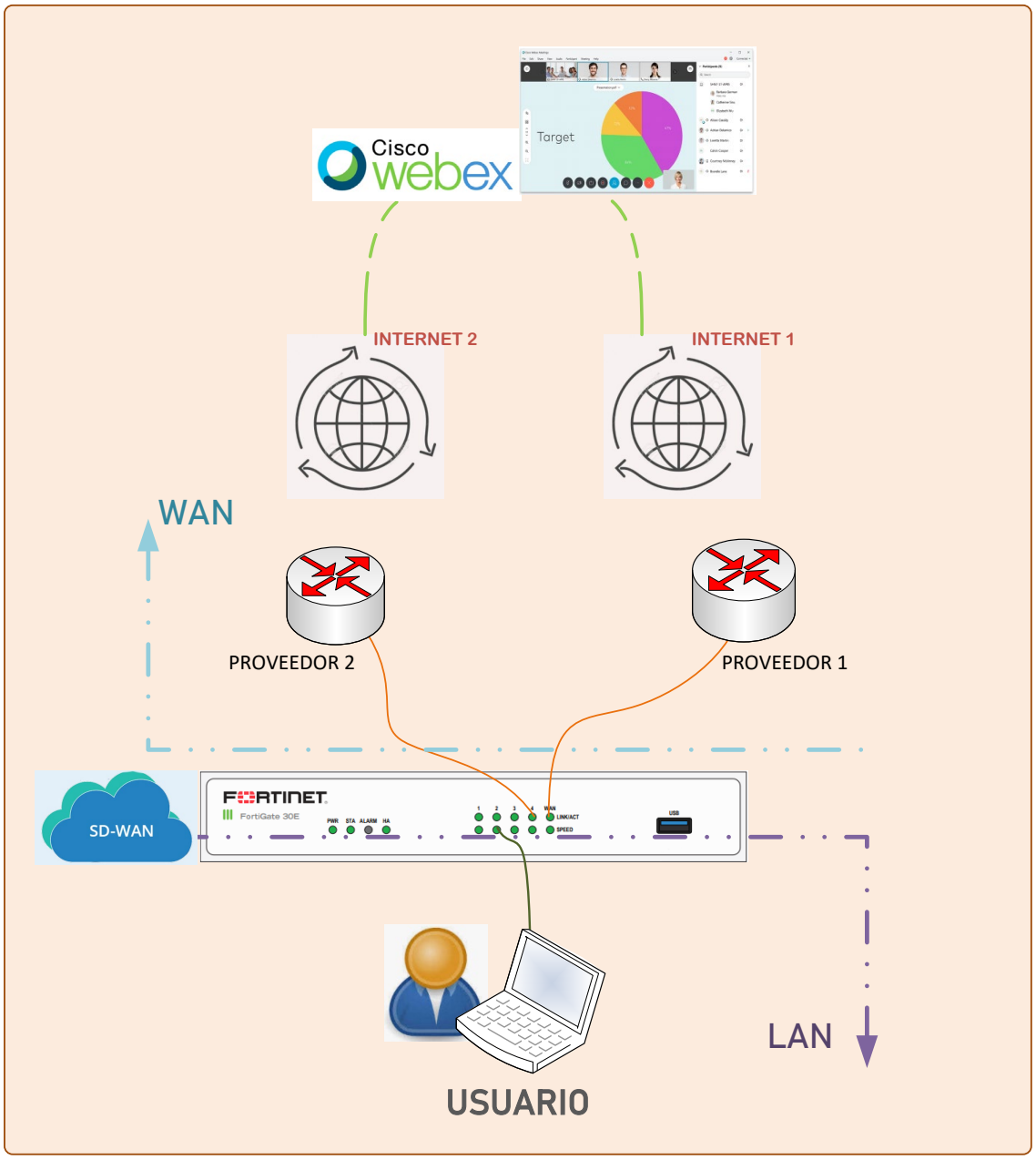
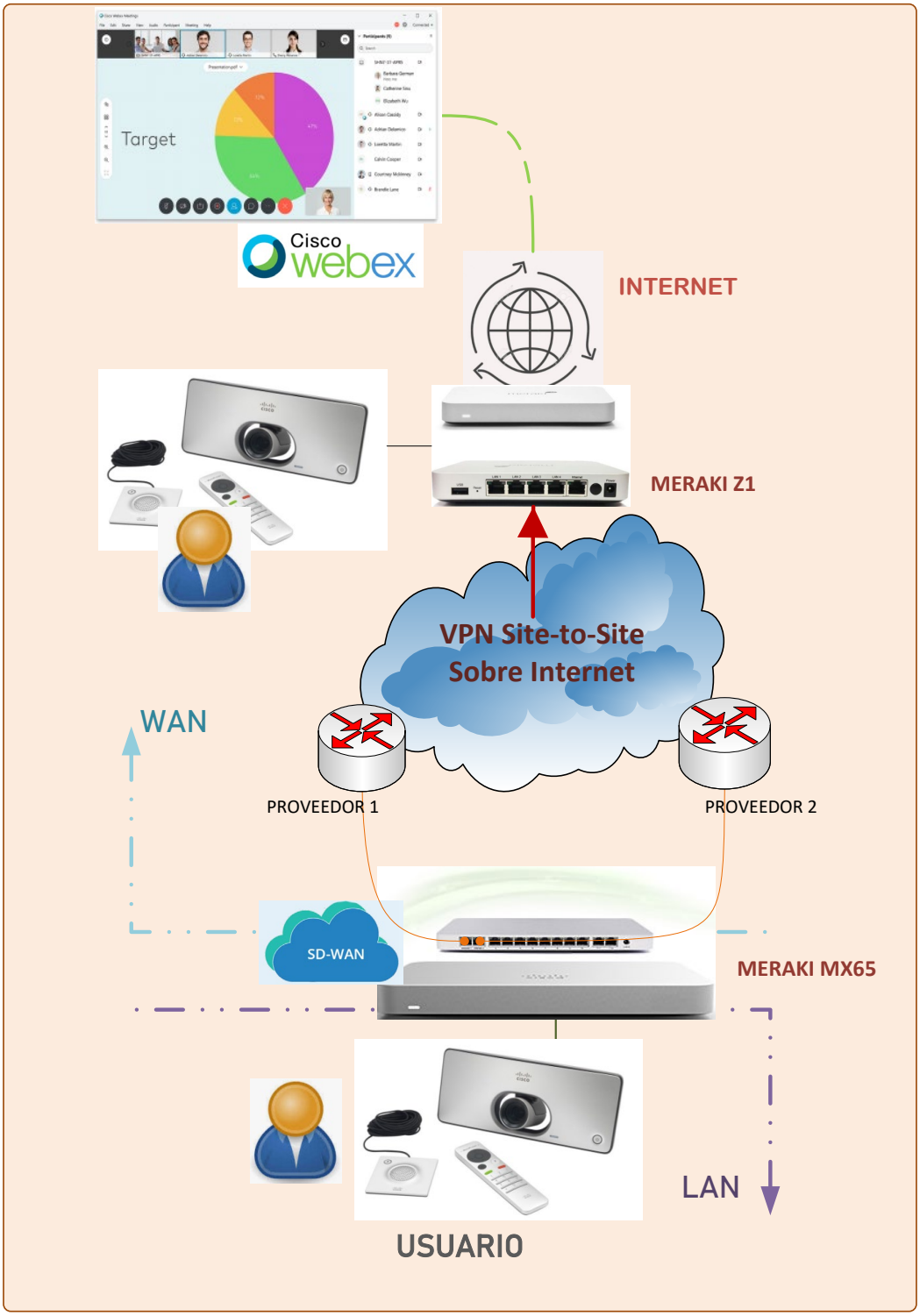


Diagrama de implementación Meraki

En la Figura 13, se muestra la ingeniería de implementación ejecutada para la marca Meraki. En Meraki según las especificaciones de funcionamiento para llevar a cabo la evaluación SD-WAN de aplicaciones y tráfico, este lo realiza mediante VPN Site-to-Site, por lo tanto, se dispone del usuario conectado directamente al Meraki MX68, en este equipo se encuentra conectado los dos proveedores. El Meraki MX68 levanta una conexión VPN Site-to-Site sobre internet hacia su sede principal Meraki Z3 y este equipo por último será el responsable de alcanzar internet.

Figura 13

Diagrama de implementación SD WAN – Meraki.



Análisis de la disponibilidad de los proveedores

Para el análisis de disponibilidad de los proveedores se muestra la información presentada en tres características de rendimiento, siendo: jitter, latencia y pérdida de paquetes.

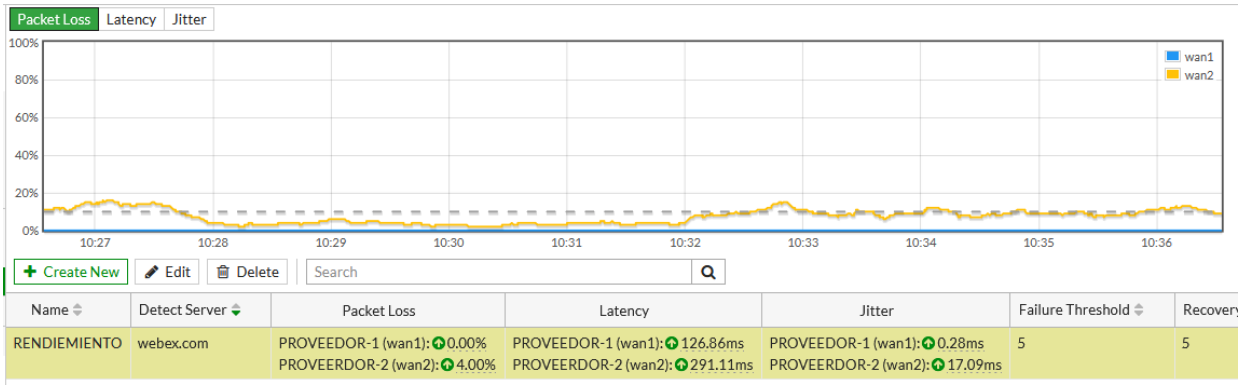
En cada hardware en su consola o GUI (siglas en inglés: Graphical User Interface) se obtiene la medición de las características mencionadas, y es por eso que se presentará los valores obtenidos y en donde hemos considerado capturar de forma más clara como pueden variar respecto a diferentes horas en las cuales consideramos horas de mayor uso común definidas como horas pico, alrededor de las 10am y las 8pm, u horas de menor consumo que será medio día, esto se lo muestra en las figuras siguientes.

CAPTURA 1:

En la captura 1 tomada de la Figura 14, corresponde a la recolección de información del porcentaje que presenta los parámetros de rendimiento, en un lapso de 10 minutos en el equipo Fortigate que detecta de los dos proveedores Telconet (WAN1) - Telefónica (WAN2) en el horario alrededor de las 10am.

Figura 14

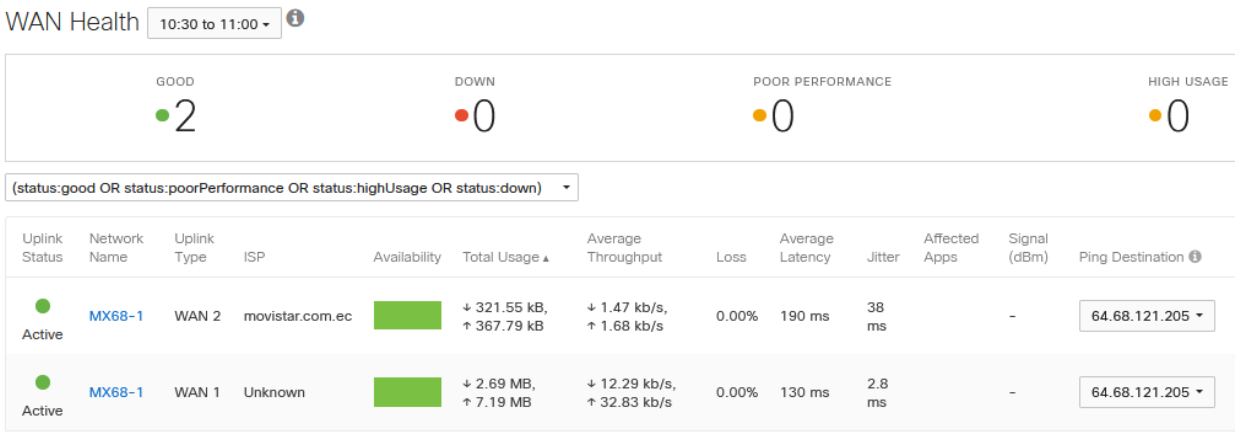
Muestra SLA – Alrededor 10am - Fortigate.



En la Figura 15 representa la captura 1 de información tomada alrededor de las 10m, la diferencia que es un monitoreo de los proveedores Telconet (WAN1) – Telefónica (WAN2). Se menciona que el lapso de recolección de información es de 30 minutos en el equipo Meraki.

Figura 15

Muestra SLA – Alrededor 10am - Meraki.

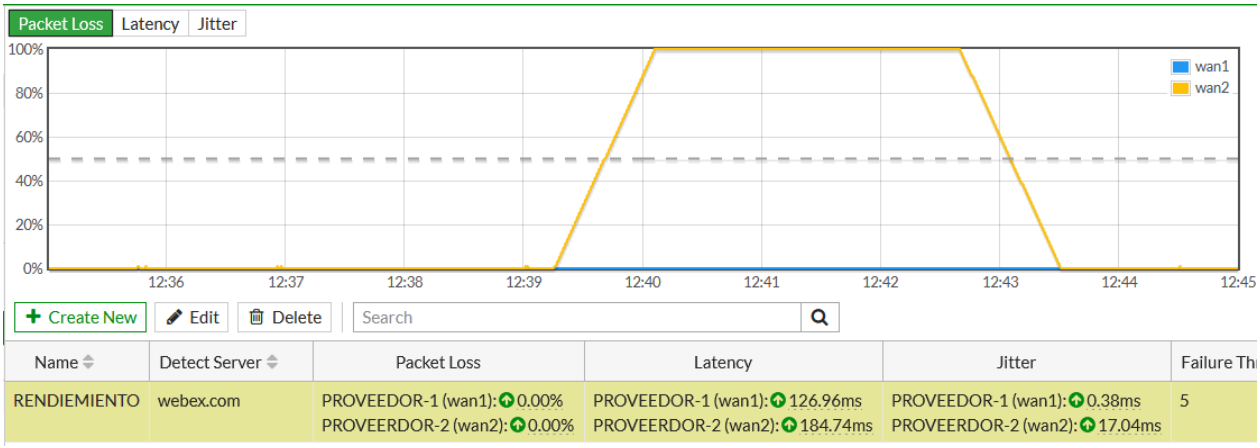


CAPTURA 2:

En la captura 2 tomada de la Figura 16, corresponde a la recolección de información del porcentaje que presenta los parámetros de rendimiento, en un lapso de 10 minutos en el equipo Fortigate que detecta de los dos proveedores Telconet (WAN1) - Telefónica (WAN2) en el horario del medio día.

Figura 16

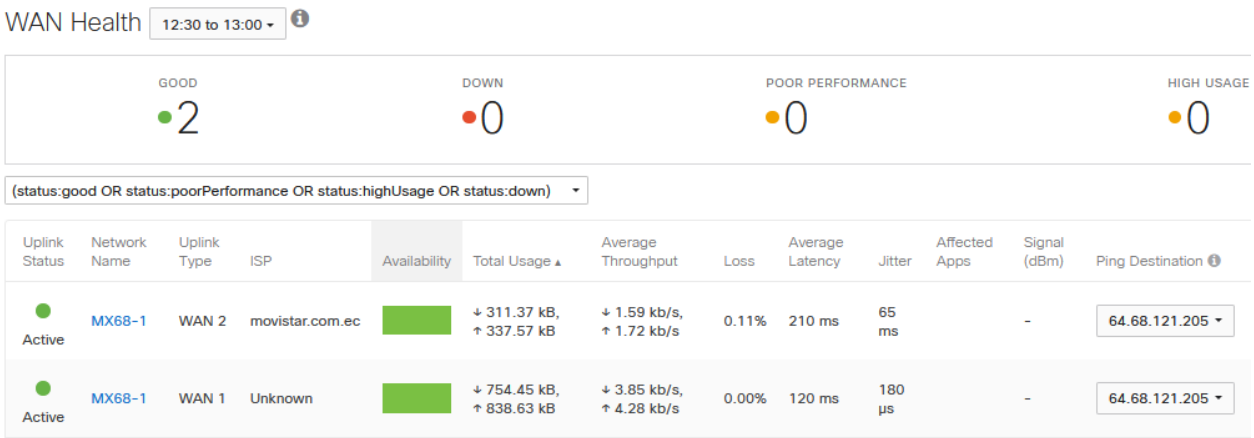
Muestra SLA – Medio día - Fortigate.



En la Figura 17 representa la captura 2 de información tomada alrededor de las 10m, la diferencia que es un monitoreo de los proveedores Telconet (WAN1) – Telefónica (WAN2). Se menciona que el lapso de recolección de información es de 30 minutos en el equipo Meraki.

Figura 17

Muestra SLA – Medio día - Meraki.

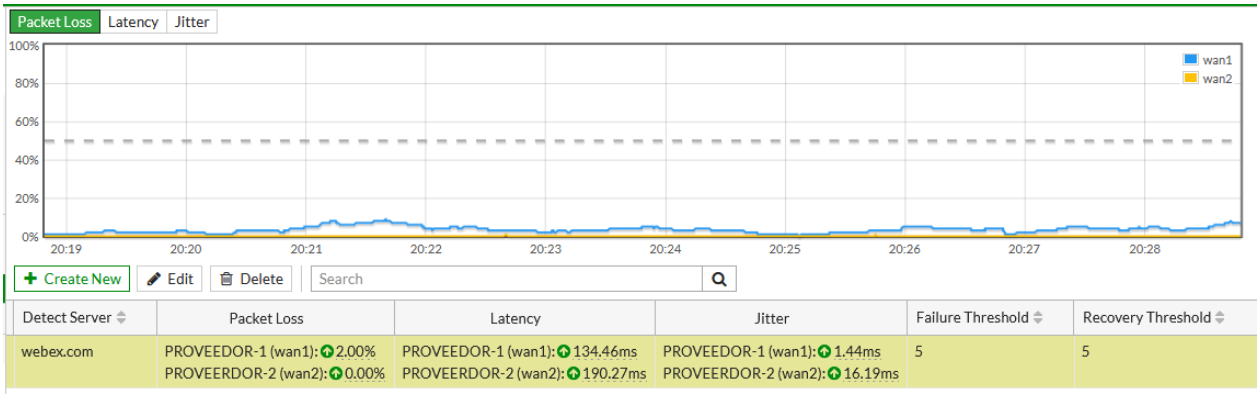


CAPTURA 3:

En la captura 3 tomada de la Figura 18, corresponde a la recolección de información del porcentaje que presenta los parámetros de rendimiento, en un lapso de 10 minutos en el equipo Fortigate que detecta de los dos proveedores Telconet (WAN1) - Telefónica (WAN2) en el horario de alrededor de las 8pm.

Figura 18

Muestra SLA – Alrededor de las 8pm - Fortigate.



En la Figura 19 representa la captura 3 de información tomada alrededor de las 10m, la diferencia que es un monitoreo de los proveedores Telconet (WAN1) – Telefónica (WAN2). Se menciona que el lapso de recolección de información es de 30 minutos en el equipo Meraki.

Figura 19

Muestra SLA – Alrededor de las 8pm - Meraki.

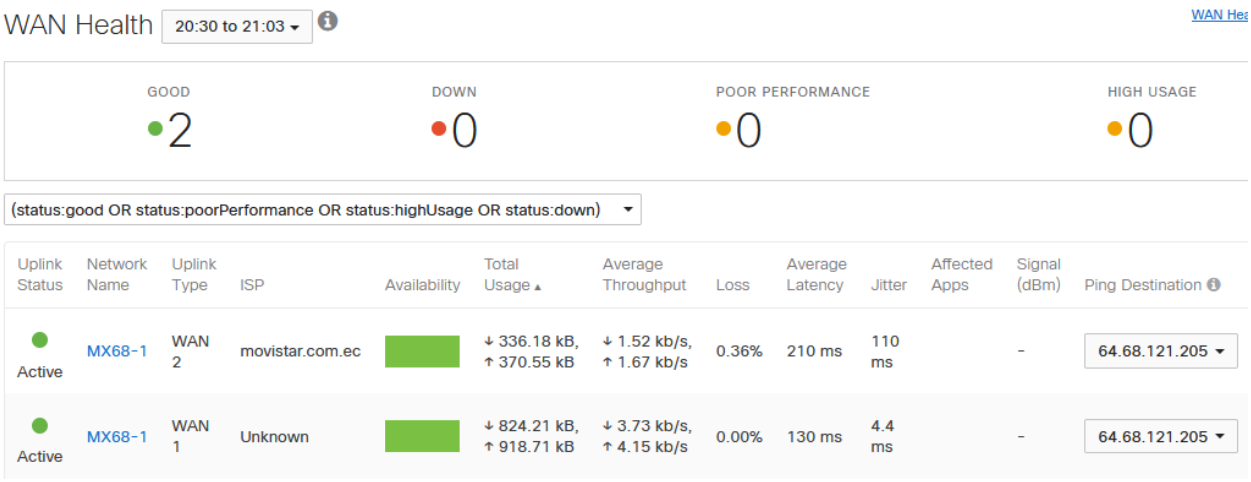


Tabla 5

Capturas de parámetros de rendimiento Fortigate.

FORTIGATE 30E	**Jitter**		**Paquetes Perdidos**		**Latencia**	
Proveedor 1= Telconet **Proveedor 2= Telefónica**	Proveedor 1	Proveedor 2	Proveedor 1	Proveedor 2	Proveedor 1	Proveedor 2
CAPTURA 1	0.28 ms	17.09 ms	0.00 %	4.00 %	126.86 ms	291.11 ms
CAPTURA 2	0.38 ms	17.04 ms	0.00 %	0.00 %	126.96 ms	184.74 ms
CAPTURA 3	1.44 ms	16.19 ms	2.00 %	0.00 %	134.46 ms	190.27 ms

Tabla 6

Capturas de parámetros de rendimiento Meraki.

MERAKI MX68	**Jitter**		**Paquetes Perdidos**		**Latencia**	
Proveedor 1= Telconet **Proveedor 2= Telefónica**	Proveedor 1	Proveedor 2	Proveedor 1	Proveedor 2	Proveedor 1	Proveedor 2
CAPTURA 1	2.8 ms	38 ms	0.00 %	0.00 %	130 ms	190 ms
CAPTURA 2	180 µs	65 ms	0.00 %	0.11 %	120 ms	210 ms
CAPTURA 3	4.4 ms	110 ms	0.00 %	0.36 %	130 ms	210 ms

En las Tablas 5 y 6 se recopila la información mostradas en las figuras anteriores para establecer y conocer los tiempos que cada proveedor dispone hacia la herramienta de evaluación que es Webex, estos datos se las obtuvo de manera simultánea en los diferentes horarios establecidos para la captura. Todos los valores son el promedio establecido de 10 minutos para Fortigate y de 30 minutos para Meraki, lo que se puede comprobar es que cada equipo presenta resultados y no similares del otro, adicional a esto lo que si se evidencia para el proveedor 2 siendo una conexión a través de la RED 4G es que las mediciones de los diferentes parámetros son mayores al ser un tipo de conexión inalámbrica.

Configuración y escenarios de implementación SD-WAN

Se detalla las configuraciones aplicadas a los equipos con tecnología SD-WAN, ya que cada uno maneja lógicas diferentes de programación. Esta programación a su vez se realizó para dos estados:

Estado inicial. – Que representa el estado antes de la aplicación de reglas de priorización de tráfico a aplicativos de videoconferencia.

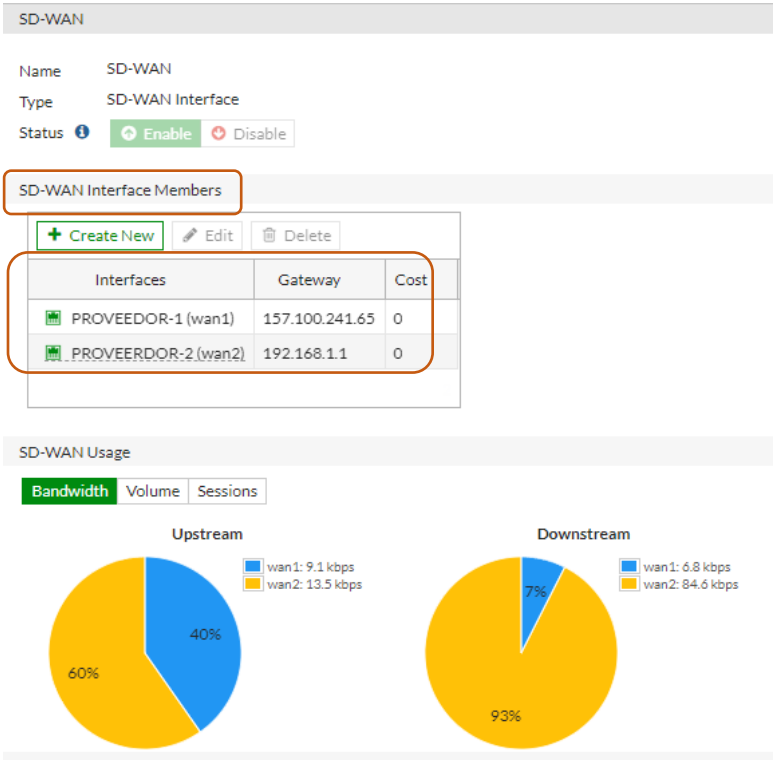
Estado de selección del mejor canal. – Que nos muestra los resultados del después de la aplicación de la regla de priorización y también para evaluación del funcionamiento de la tecnología SD-WAN.

Fortigate – Configuraciones SD-WAN.

Configuración General. Para empezar, en el equipo Fortigate se procedió a configurar 2 interfaces que pertenezcan a la zona global SD-WAN, como se muestra en la Figura 20:

Figura 20

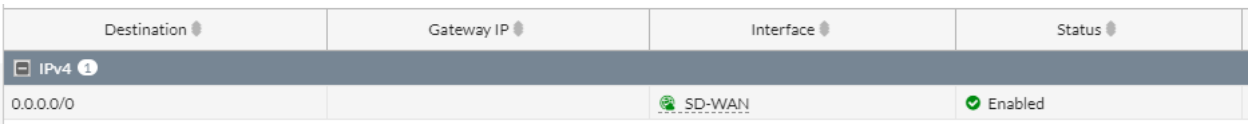
Integración interfaces SD WAN Fortigate.



Una vez con la zona creada, se configura en el equipo la ruta de último recurso tal como se representa en la Figura 21, para que la programación defina las salidas según el algoritmo integrado:

Figura 21

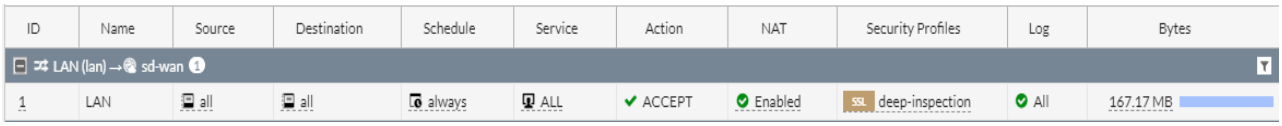
Ruta último recurso Fortigate.



En la marca Fortigate es necesario habilitar permisos de direccionamiento de tráfico, entrante o saliente, por lo tanto, se instaura la política que se visualiza en la Figura 22 desde nuestra RED LAN hacia la WAN, que a su vez está representada o incluida en la zona SD-WAN.

Figura 22

Política LAN – SD WAN, Fortigate.



Configuración y Estado Inicial – Fortigate. En el equipo Fortigate por defecto viene preconfigurada una regla SD-WAN llamada: Implícita, en esta regla se puede definir diferentes maneras de balanceo de carga, la seleccionada para nuestro escenario es:

- Source IP (basado en IP de la fuente): SD-WAN equilibrará el tráfico por igual entre sus miembros de acuerdo con un algoritmo hash basado en las direcciones IP de origen. Lo representado en la Figura 23.

Figura 23

Regla implícita SD WAN – Fortigate con criterio IP fuente.

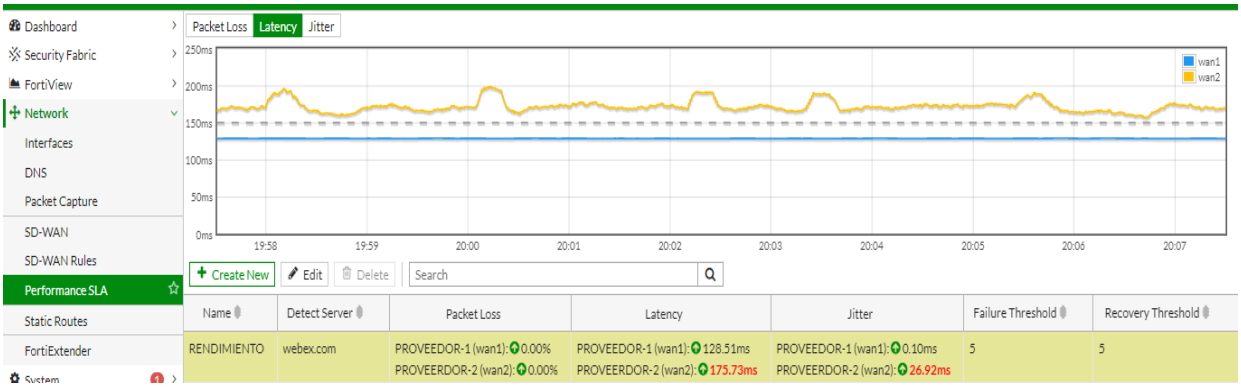
Name	Source	Destination	Criteria	Members
sd-wan	All	All	source-ip-based	All

Con esta selección tomará el tráfico por defecto que ingrese al equipo Fortigate y su salida al internet, lo enviará por cualquiera de los dos canales según la definición del algoritmo.

Configuración y Estado de selección del mejor enlace – Fortigate. Se estableció la configuración del SLA (Service Level Agreement), que será el encargado de seleccionar el canal requerido según las siguientes características y el cual se obtuvo de manera gráfica tal como se muestra en la Figura 24:

Figura 24

Rendimiento SLA Fortigate.



Link Health Monitor: Para el propósito del SLA, el objetivo seleccionado para monitoreo es el dominio de la aplicación RTP, por la razón de que la aplicación puede disponer de una o más IPs en rangos diferentes. A su vez se incluye las interfaces participantes correspondientes a los enlaces de los proveedores que ejecutaran el monitoreo.

SLA Target: El siguiente paso es la selección de nuestro criterio de monitoreo, ingresando valores umbrales de: Latency, Jitter, Packet Loss, para establecer estos parámetros se toma como referencia las recomendaciones de la aplicación, Webex (propietario Cisco), Figura 25.

Figura 25

Parámetros de funcionamiento Webex (Cisco).

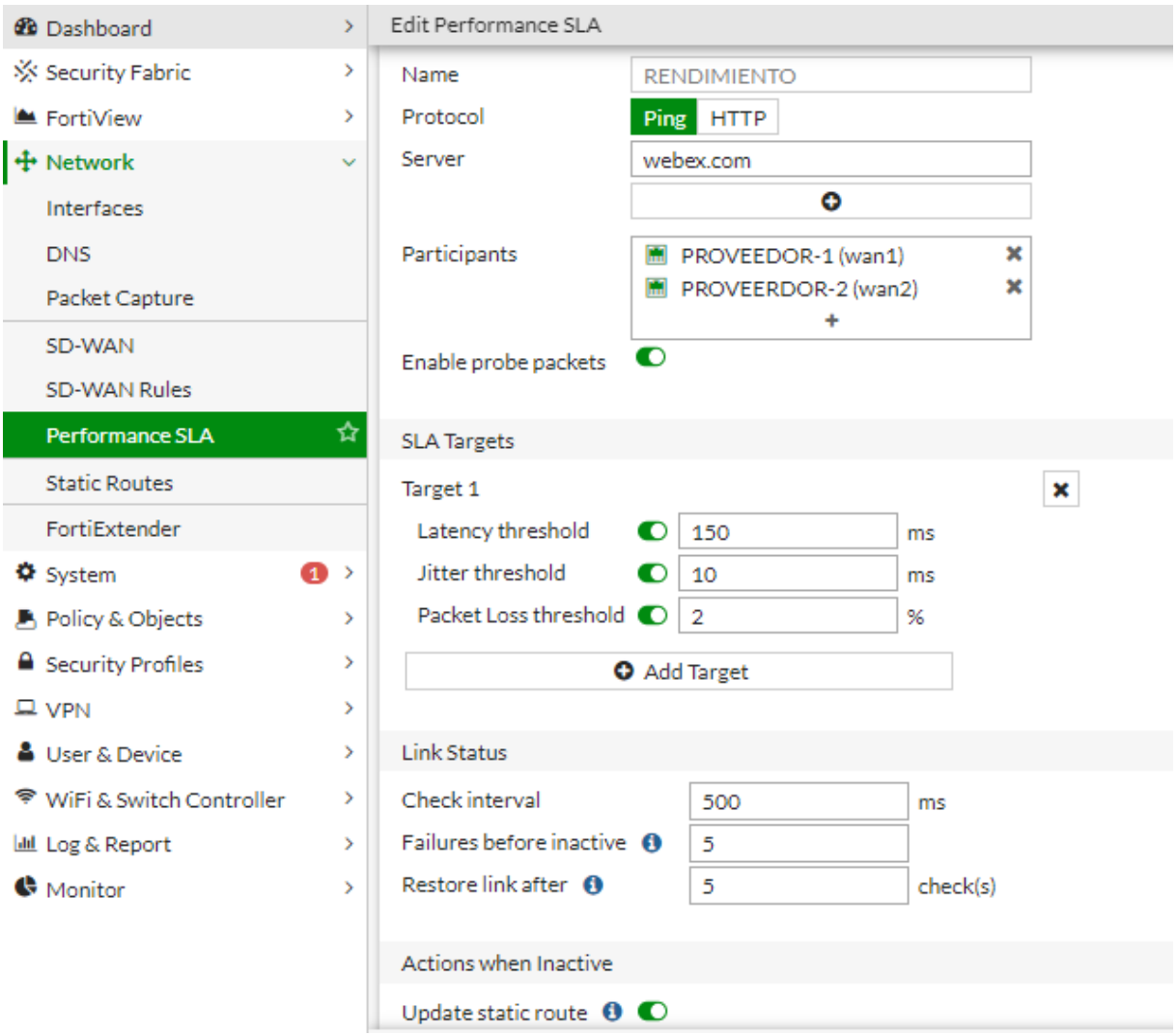
Webex Participant	Packet Loss	Latency [RTT/ms]	Jitter [cumulative]
SIP/H323 Devices into Webex Meetings	Good = <0.05% OK = <1%	Good =<150ms OK = <250ms	Cumulative end-end jitter must be less than ~40-50ms
Webex Meetings Clients [UDP]	Good =<2% OK =<6-8%	Good =<300ms OK =<400ms	“”
Webex Meetings Clients [TCP]	Good = <1% OK =<1-2%	Good =<200ms OK =<300ms	“”
Webex Teams Clients [UDP]	Good =<2% OK =<6-10%	Good =<300ms OK =<400ms	“”

Nota. Fuente: (Tansey, 2010)

Link Status: En este campo se recomienda mantener los valores ya mostrados en la configuración. Lo que significa, intervalos de revisión, fallas y límites de restauración, que son usados para prevenir flapeos. Es decir, según la Figura 26 una prueba es enviada cada 500 milisegundos, el estado del SLA para un miembro de la SD-WAN cambia después de 5 respuestas consecutivas fallidas detectadas hacia el servidor de prueba y el estado se restaura después de 5 respuestas consecutivas exitosas desde el monitoreo que se realiza al servidor de prueba. Es un tipo de monitoreo de fallas físicas de las interfaces de los equipos.

Figura 26

Configuración Rendimiento SLA - Fortigate.

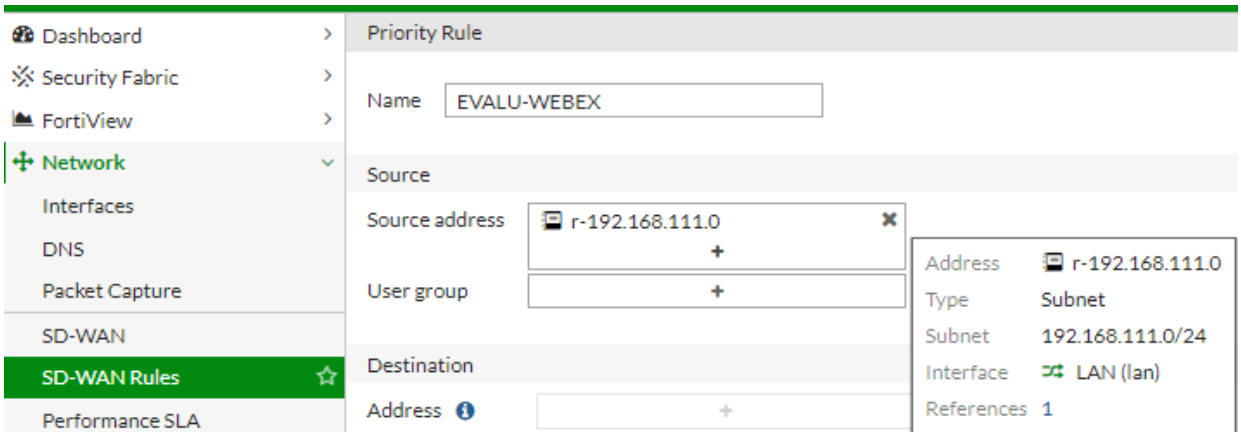


Se configura la regla SD-WAN que establecerá el comportamiento de selección del mejor canal para nuestra aplicación RTP, en este caso Webex, cumpliendo con la siguiente estrategia:

- Source Address: Se define nuestra RED LAN que es la 192.168.111.0/24, Figura 27.

Figura 27

Definición red fuente.



- Destination: En este apartado escogimos los servicios de internet y aplicaciones que involucra WEBEX, Figura 28.

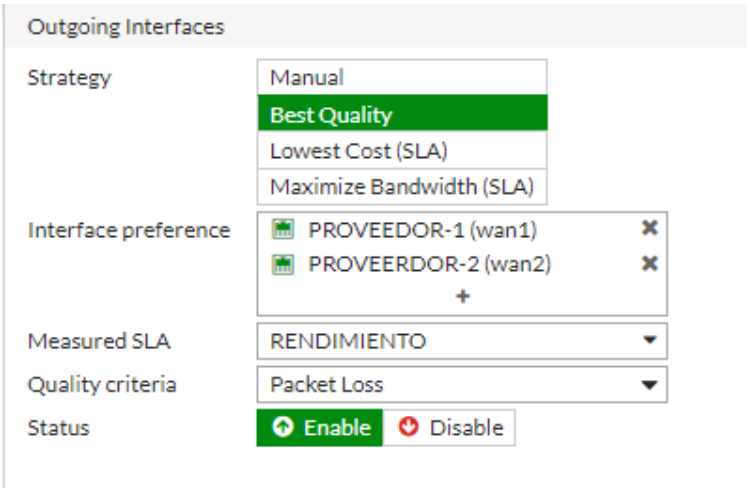
Figura 28

Definición aplicación/servicio destino.

- Interfaces de Salida: La estrategia seleccionada es la de “mejor calidad”, las interfaces participantes que se podrá enviar el tráfico son la que disponemos de nuestros dos diferentes proveedores. Para la selección de direccionamiento de tráfico es necesario involucrar nuestra definición de monitoreo SLA, y por último el criterio de calidad “Packet Loss”, que tomará en cuenta al momento de escoger cierto canal del proveedor ya que los tiempos varían y evalúa el servicio prestado por el proveedor. La Figura 29 indica lo escogido para la configuración.

Figura 29

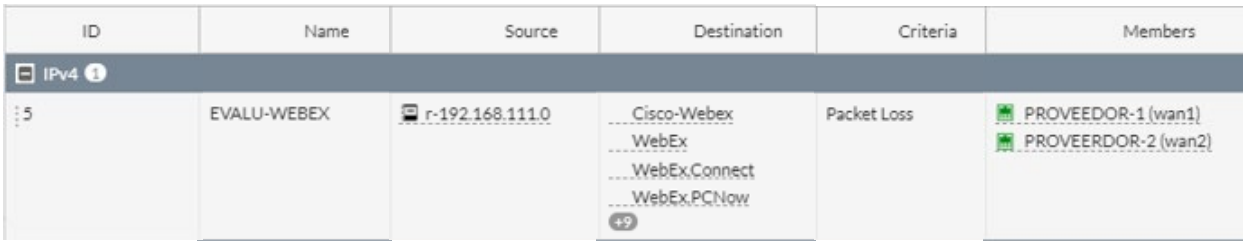
Parámetros interfaz de salida.



En la interfaz gráfica para el usuario del equipo nos mostrará la siguiente pantalla una vez definida nuestra regla SD-WAN, como la mostrada en la Figura 30:

Figura 30

GUI Regla SD WAN para evaluar Webex.



Meraki – Configuraciones SD-WAN.

Configuración General. La solución que nos ofrece el fabricante para la implementación SD-WAN y su funcionamiento no es directamente por las conexiones de los proveedores hacia internet, como en el caso de la marca Fortinet, sino más bien esta tecnología la tiene desarrollada en la funcionalidad de VPN Site-to-Site. En nuestro escenario se utilizó un esquema HUB-SPOKE, es decir, el HUB es el sitio central de VPNs y dispone de un acceso directo a internet, el SPOKE se considera una sede remota que accederá al internet a través de la VPN que se configuró hacia el HUB.

También se incluyó dos equipos de video conferencia en cada punto: HUB y SPOKE.

Meraki solamente considera para balanceo de carga SD-WAN la capacidad de sus enlaces: WAN1, WAN2.

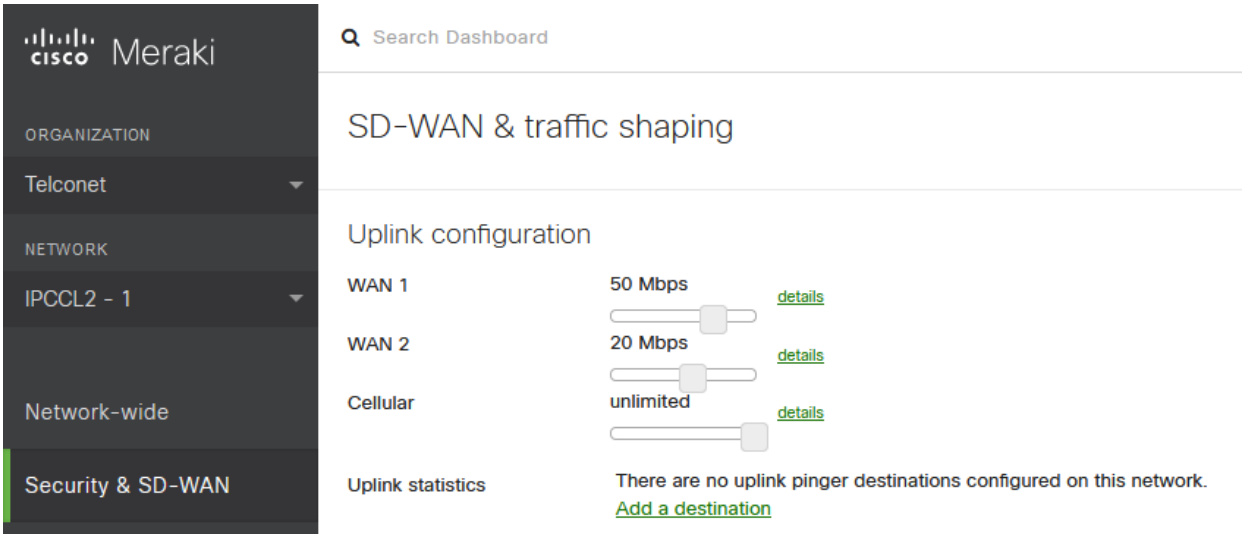
Se hace una connotación para el ingreso de los valores en las interfaces WAN1 y WAN2, en lo que respecta Meraki la asignación de los valores se lo debe realizar referenciado en ciertas consideraciones como:

- SLA ofrecido por el proveedor.
- Tipo de medio de transmisión.
- por último, ancho de banda contratado.

Es decir que la definición de los valores en las interfaces recae directamente en el administrador. Para el proyecto que se desarrolló se ingresaron los siguientes valores que se visualizan en la Figura 31.

Figura 31

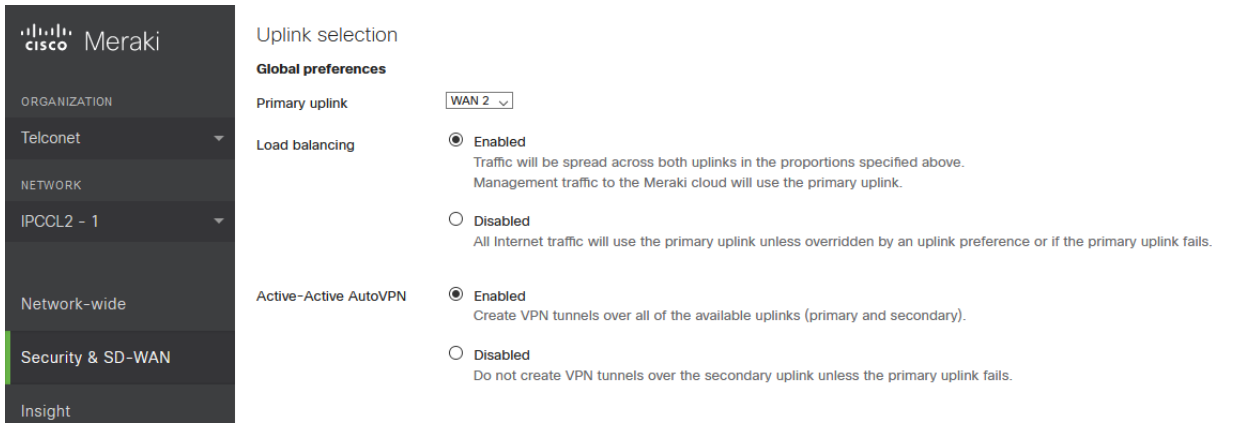
Definición de ancho de banda para cada enlace del proveedor.



Adicional la habilitación SD-WAN en el equipo se relaciona directamente con la habilitación de: balanceo de carga y AutoVPN, como se muestra en la Figura 32.

Figura 32

Preferencias Globales.

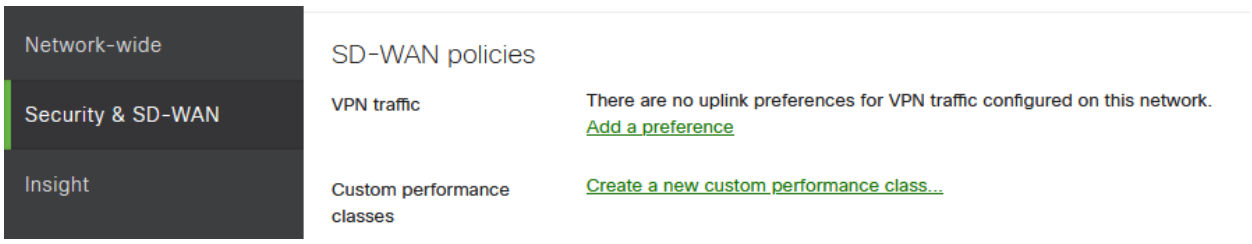


Configuración y Estado inicial – Meraki. En el equipo Meraki el balanceo de carga está regido exclusivamente por los valores que se establecieron en las interfaces, que es el ancho banda, como se estableció en la Figura 31.

Este balanceo prevalecerá siempre y cuando no exista políticas SD-WAN (VPN Traffic) como se muestra en la Figura 33, siendo esta una regla implícita en la toma de decisión de balanceo de tráfico.

Figura 33

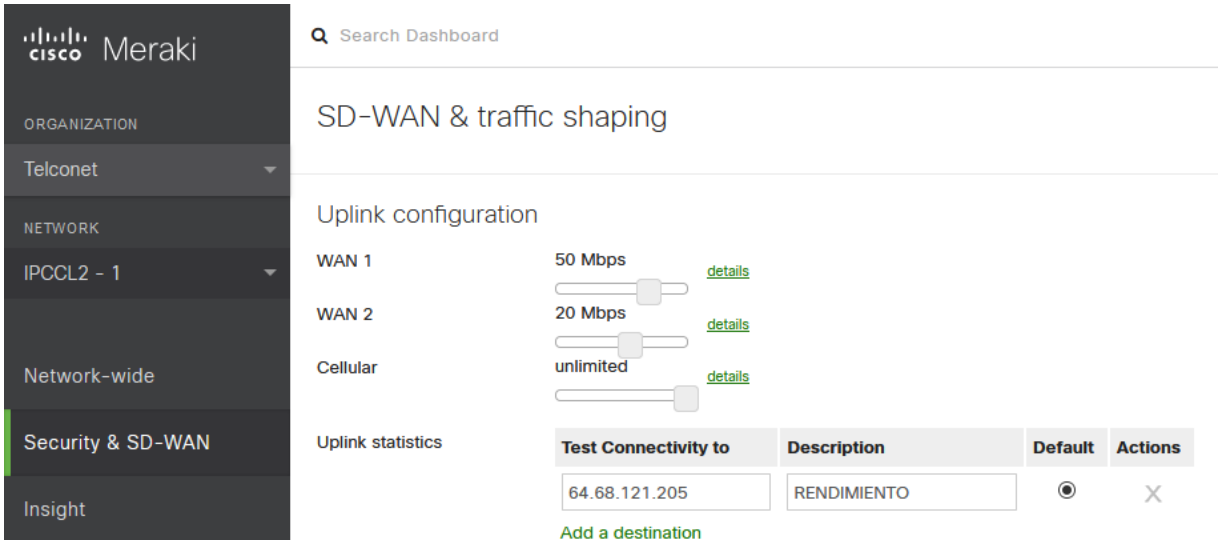
Sección definición políticas SD WAN.



Configuración y Estado de selección del mejor enlace - Meraki. El ingreso del valor para la prueba de conectividad en Meraki se basa en monitorear la respuesta ICMP a la IP relacionada al servicio RTP que se utilizó para la prueba de SD-WAN, en la figura F se indica la IP a monitorear que es la 64.68.121.205 (Figura 34) que pertenece al rango asignado para el dominio webex.com

Figura 34

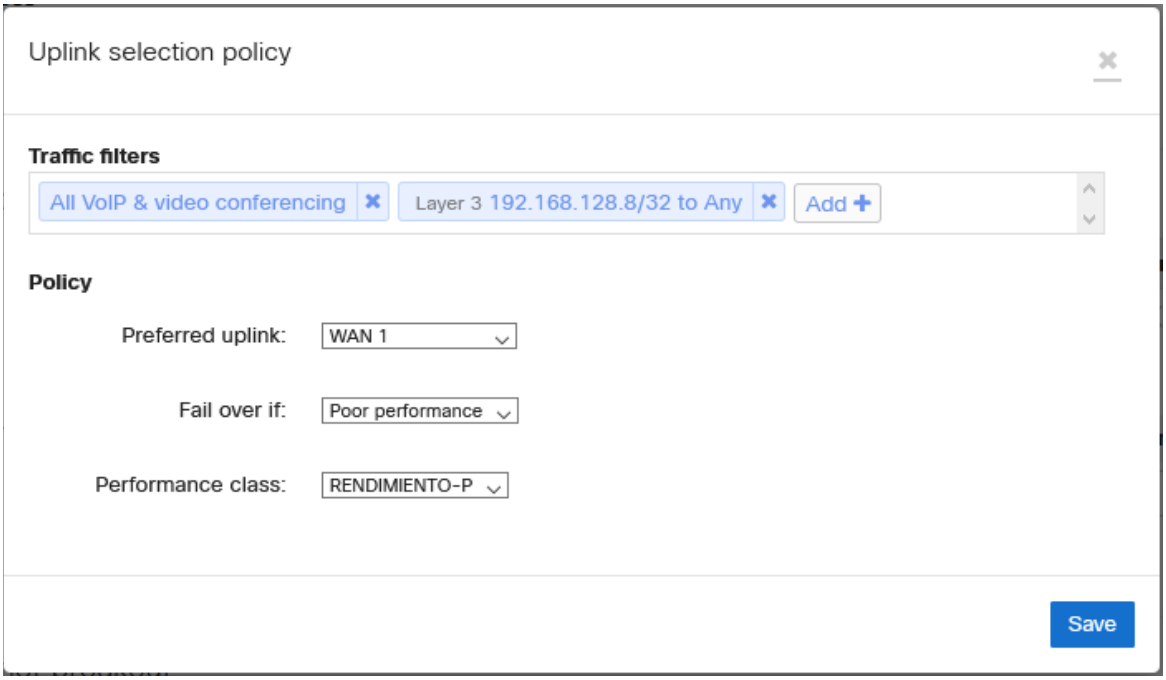
Ingreso prueba de conectividad IP.



En la Figura 35 se visualiza la definición de la regla SD-WAN creada para la selección del mejor enlace, siendo:

Figura 35

Política SD WAN selección mejor enlace.



Traffic filters. – La opción general (Todo VozIp & Video Conferencia) la cual incluye todos los servicios y aplicaciones de video conferencia y voz sobre IP.

Se incluye la IP de videoconferencia del punto SPOKE siendo la: 192.168.128.8/32, de tal manera que realice una conjugación con la categoría de aplicación de Todo VozIp & Video Conferencia.

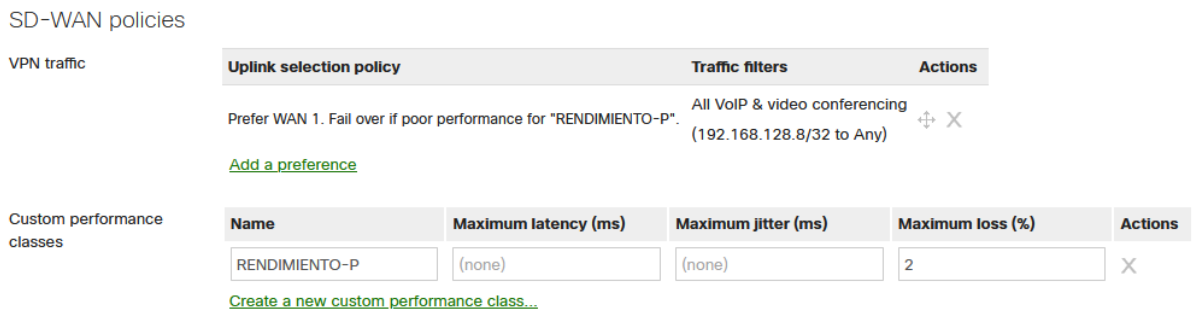
Preferred uplink. – Se prioriza el tráfico de video conferencia y voz para que su preferencia sea por la interfaz WAN1.

Fail over if. – Para la conmutación de tráfico hacia el enlace de mejores prestaciones según el monitoreo del rendimiento, la característica seleccionada es la de: bajo rendimiento. Si el enlace que se dispone por la WAN1 presenta bajo rendimiento conmuta el tráfico a WAN2.

Performance class. – La prioridad de traficó se la realizó según la clase de rendimiento definido que se muestra en la Figura 36 y nombrada “RENDIMIENTO-P”, es decir cuando el enlace de preferencia (WAN1) tenga mayor porcentaje de pérdidas superiores al 2 % conmutará inmediatamente al otro enlace disponible WAN2.

Figura 36

Clase de rendimiento definido.



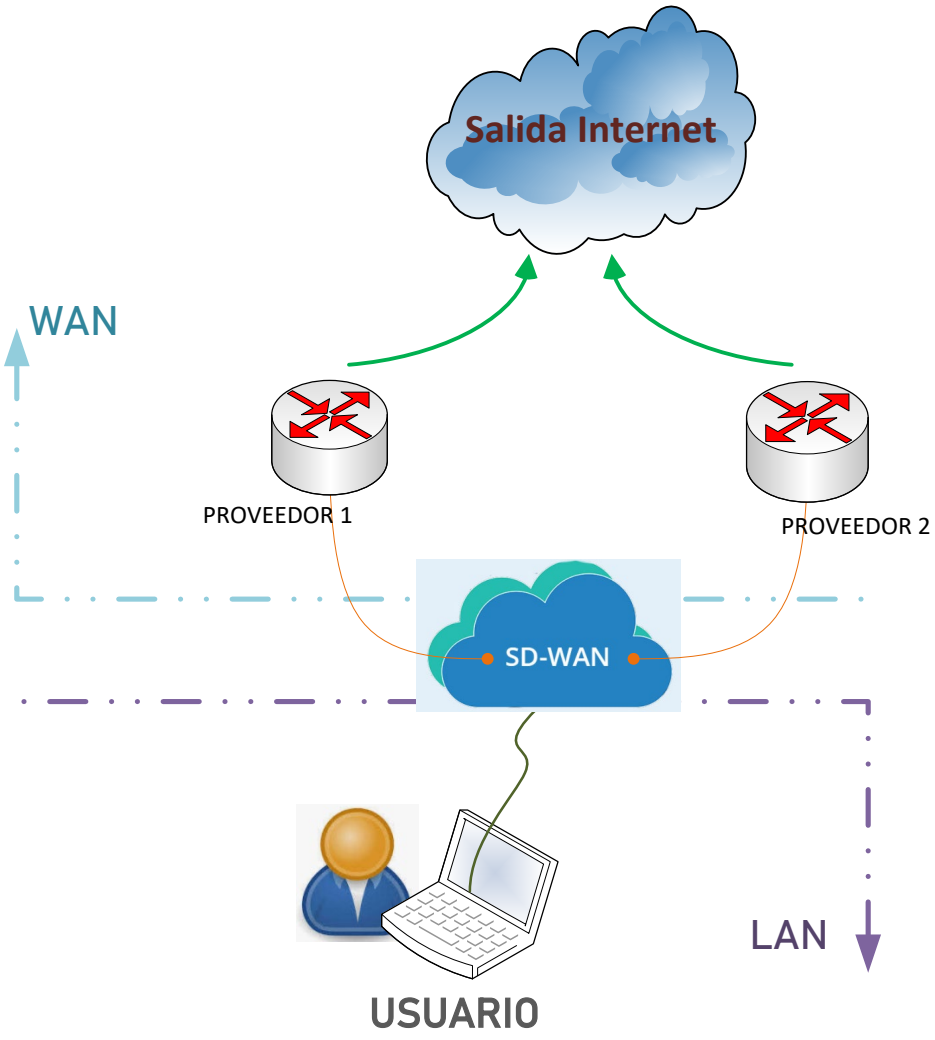
Funcionamiento del Escenario Implementado

La salida al internet en un inicio en donde el usuario haga las peticiones a varias aplicaciones o navegación web, esta será basada según la programación o algoritmo que maneje la marca ya sea de Fortigate o Meraki.

Se visualizará en la Figura 37, su salida por las interfaces participantes en la tecnología SD-WAN ejecutando un proceso de por sí de balanceo de carga.

Figura 37

Balanceo de carga que aplica SD WAN.



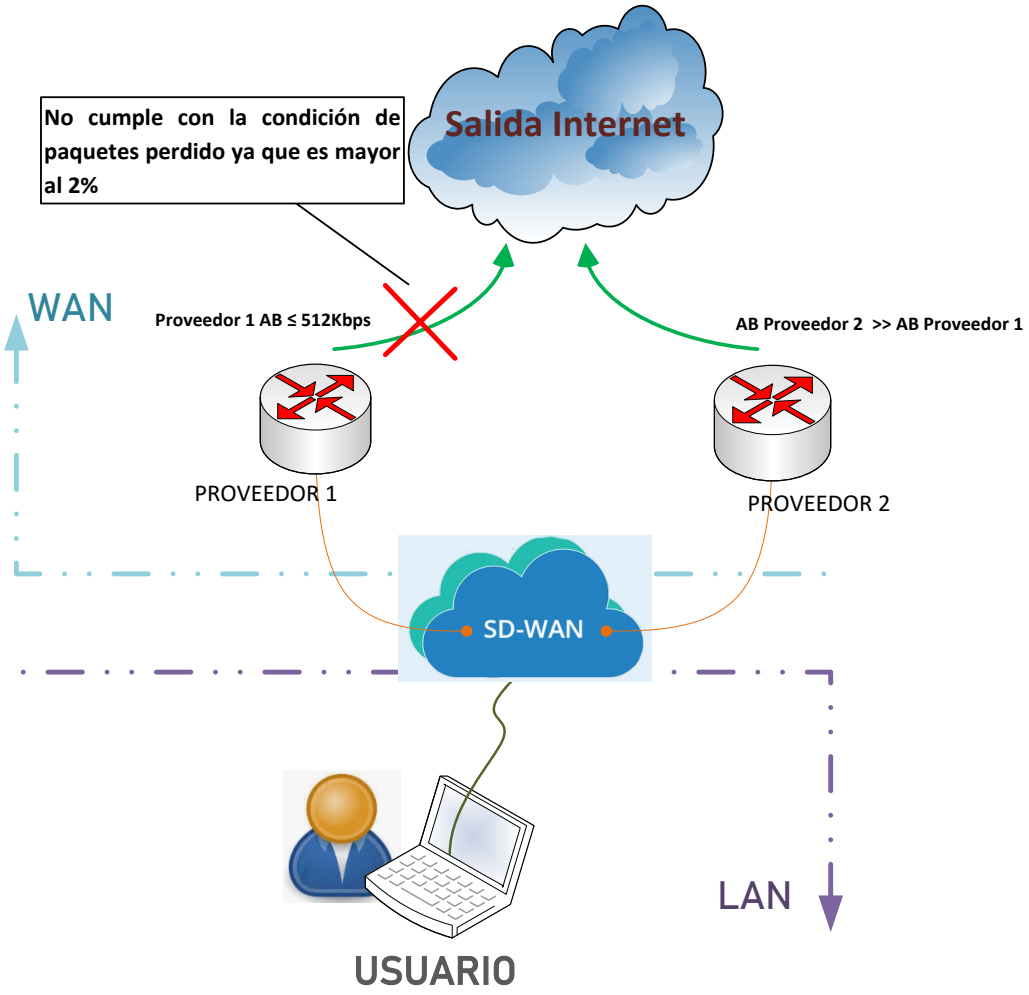
Una vez definidos los parámetros de cumplimiento de SLA, para demostrar el comportamiento de conmutación de enlace o selección del mejor enlace, debemos emular la degradación de uno de ellos para que no cumpla con los parámetros de eficiencia. Una opción que se tuvo en cuenta es la de disminuir el ancho de banda en el proveedor 1 de tal manera que se produzca pérdidas de paquetes o a su vez saturar el enlace.

Al decrementar la capacidad de AB del proveedor 1 o saturarlo, se empieza a visualizar en el rendimiento de enlace, como estos valores van cambiado y consecuentemente se incrementan los paquetes perdidos, dichos parámetros se muestran en cada consola de gestión de los equipos Fortigate y Meraki.

Cuando alcanza y sobrepasa el umbral del parámetro de paquetes perdidos el algoritmo de los equipos lo detecta y en su toma de decisión redirige el tráfico hacia el canal que lo cumpla. Como se simula en el diagrama que se presenta en la Figura 38.

Figura 38

Balanceo por canal que cumpla el rendimiento definido.



CAPÍTULO IV

ANÁLISIS DE RESULTADOS

Para el análisis de resultados se procedió a realizar 4 escenarios de prueba.

Escenario Nº 1 – Estado inicial Fortigate

Este escenario fue necesario mostrarlo para evidenciar el comportamiento de balanceo de carga que ejecuta el equipo. Se dispone de los dos enlaces de internet funcionando y conectados a nuestro equipo Fortigate. En el equipo no está más que la regla implícita SD-WAN (Rule ID = 0), desde la LAN se generan peticiones hacia el internet usando varias aplicaciones o sitios en las cuales tomará como salida aleatoriamente los enlaces disponibles de los dos proveedores. Estas son pruebas de laboratorio para indicar el comportamiento. Como se puede ver en la Figura 39 se ejecutan varias peticiones hacia el internet.

Figura 39

Captación LOGs – Escenario 1, tomado desde Fortigate.

Date/Time	Source	Destination	Application Name	Policy	SD-WAN Rule ID	Destination Interface
2020/11/07 22:33:49	192.168.111.170	151.101.1.195 (td2-desktop-api.timedoctor.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:33:39	192.168.111.170	64.68.101.79 (mta2mcs143.webex.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:39	192.168.111.170	172.24.27.13	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:36	192.168.111.170	64.68.101.79 (mta2mcs143.webex.com)	udp/9000	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:24	192.168.111.170	172.24.27.13	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:24	192.168.111.170	8.8.8.8 (dns.google)	DNS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:22	192.168.111.170	31.13.67.16 (star.c10r.facebook.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:33:18	192.168.111.170	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:33:14	192.168.111.170	209.197.3.15 (stackpath.bootstrapcdn.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:33:12	192.168.111.170	8.8.8.8 (dns.google)	DNS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:32:56	192.168.111.170	172.24.27.13	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:32:56	192.168.111.170	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:32:54	192.168.111.170	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)

Date/Time	Source	Destination	Application Name	Policy	SD-WAN Rule ID	Destination Interface
2020/11/07 22:40:43	192.168.111.150	40.114.54.223 (otf.msn.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:39	192.168.111.150	23.92.189.244 (api.cxense.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:31	192.168.111.150	35.211.114.141 (us-east-sync.bidswitch.net)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:31	192.168.111.150	185.201.11.215 (laprensa.ec)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:30	192.168.111.150	54.239.17.112 (s.amazon-adsystem.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:29	192.168.111.150	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:27	192.168.111.150	23.5.227.90 (a23-5-227-90.deploy.static.akamaitechnologies.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:27	192.168.111.150	99.192.248.119 (www.gecpublicidad.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:25	192.168.111.150	104.244.42.67 (s.twitter.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:23	192.168.111.150	190.95.221.137 (iess.gob.ec)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:21	192.168.111.150	23.92.189.245 (id.cxense.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:19	192.168.111.150	104.244.42.67 (s.twitter.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:32	192.168.111.150	68.67.179.154 (secure.adnxs.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:31	192.168.111.150	52.69.214.112	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:30	192.168.111.150	54.158.170.153 (pm.w55c.net)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:30	192.168.111.150	209.197.3.24 (cds.s5x3j6q5.hwcdn.net)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:40:22	192.168.111.150	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:40:17	192.168.111.150	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)

Date/Time	Source	Destination	Application Name	Policy	SD-WAN Rule ID	Destination Interface
2020/11/07 22:46:07	192.168.111.160	104.208.156.39 (trouter-eus2-a.trouter.skype.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:46:02	192.168.111.160	142.250.64.226 (googleads.g.doubleclick.net)	udp/443	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:46:02	192.168.111.160	142.250.64.226 (googleads.g.doubleclick.net)	udp/443	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:46:01	192.168.111.160	13.107.42.23 (b.config.skype.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:46:01	192.168.111.160	74.125.21.113 (yv-in-f113.1e100.net)	udp/443	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:46:01	192.168.111.160	92.223.66.71 (relay-f4a12b99.net.anydesk.com)	HTTP	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:46:01	192.168.111.160	74.125.21.113 (yv-in-f113.1e100.net)	udp/443	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:46:01	192.168.111.160	74.125.21.113 (yv-in-f113.1e100.net)	udp/443	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:45:59	192.168.111.160	172.217.2.195 (ssl.gstatic.com)	udp/443	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:45:59	192.168.111.160	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:45:59	192.168.111.160	172.217.2.195 (ssl.gstatic.com)	udp/443	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 22:45:55	192.168.111.160	142.250.64.225	udp/443	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 22:45:52	192.168.111.160	172.217.3.138 (imasdk.googleapis.com)	udp/443	LAN (1)	0	PROVEERDOR-2 (wan2)

En la Tabla 7 se ha tomado muestras de los diferentes usuarios de la red interna hacia un destino en común, como la página web del Comercio, y otros sitios que cada usuario accede independientemente, evidenciando que se produce la salida distribuida de tráfico según el algoritmo de balanceo.

Tabla 7

Toma de captura de LOGs Fortigate – varios destinos.

Fecha-Tiempo	IP Fuente	IP Destino/Aplicación	Interfaz Destino	Regla ID
2020/11/07 22:33:18	192.168.111.170	El Comercio	Wan1	0
2020/11/07 22:33:36	192.168.111.170	Webex	Wan1	0
2020/11/07 22:40:23	192.168.111.150	IESS	Wan2	0
2020/11/07 22:40:29	192.168.111.150	El Comercio	Wan1	0
2020/11/07 22:45:59	192.168.111.160	El Comercio	Wan2	0
2020/11/07 22:46:01	192.168.111.160	Skype	Wan1	0

De igual manera podemos visualizar el comportamiento de consumo que se presenta en cada enlace en las Figuras 40 y 41.

Figura 40

Tráfico captado de la interfaz del proveedor 1 – Fortigate.

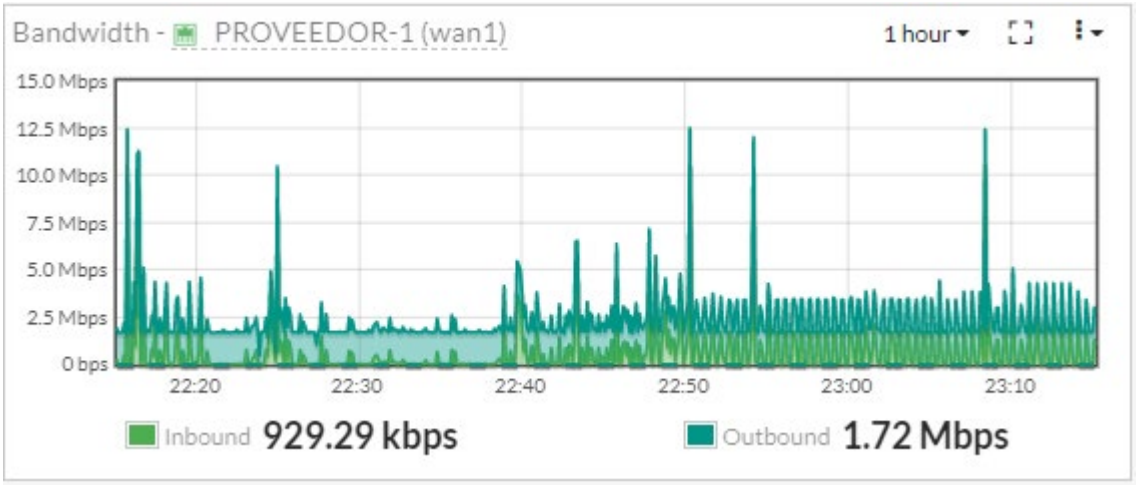
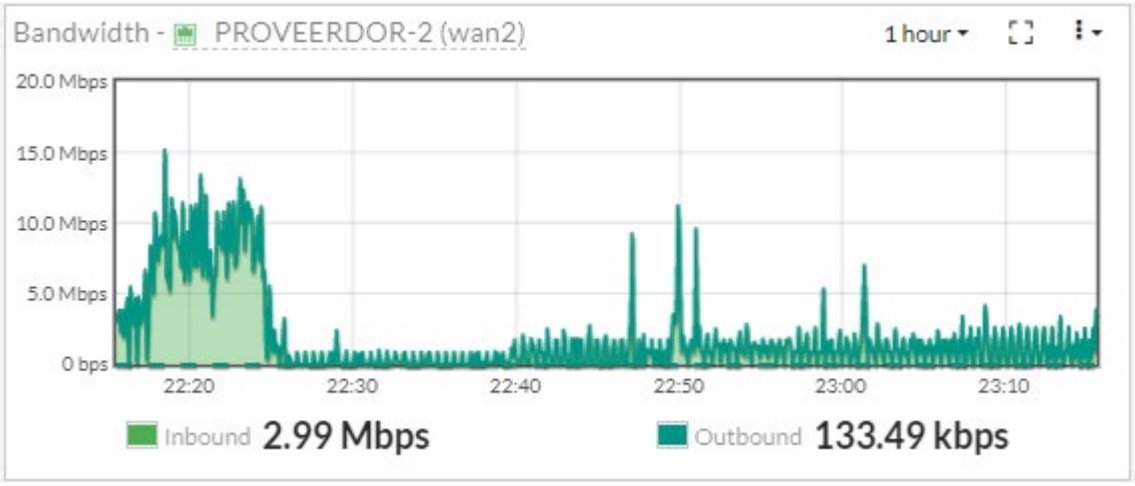


Figura 41

Tráfico captado de la interfaz del proveedor 2 – Fortigate.



Se observa tráfico tanto entrante como saliente en cada una de las interfaces que conectan a sus respectivos proveedores. Ya que se aplica balanceo de carga en SD-WAN los consumos son aleatorios.

Escenario Nº 2 – Estado inicial Meraki

Este escenario de igual manera que en el escenario 1, se analizó y se obtuvo la información mostrada por el equipo Meraki con sus respectivas características, encontrando algunas diferencias en cuanto a visualización de información. Se obtiene el balanceo de carga ejecutado por el equipo, pero a diferencia de Fortigate este lo hace específicamente bajo el análisis de ancho de banda que dispone los dos canales, aunque no descarta balancear por el enlace con menor ancho de banda.

Figura 42

Tráfico generado por equipo de videoconferencia.

Uplink decisions

192.168.128.8

Peer	Protocol	Source	Destination	Uplink decision	Reason	Policy	Last seen
IPCCL2 - 2	TCP	192.168.128.8:11001	192.168.30.7:5555	WAN 1	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	UDP	192.168.128.8:2431	192.168.30.7:2431	WAN 1	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	UDP	192.168.128.8:2337	192.168.30.7:2331	WAN 2	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	UDP	192.168.128.8:2373	192.168.30.7:2377	WAN 1	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	UDP	192.168.128.8:2336	192.168.30.7:2330	WAN 1	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	UDP	192.168.128.8:2372	192.168.30.7:2376	WAN 2	Load balanced	Fail over if uplink is down	21:10
IPCCL2 - 2	TCP	192.168.128.8:11000	192.168.30.7:1720	WAN 2	Load balanced	Fail over if uplink is down	21:09
IPCCL2 - 2	UDP	192.168.128.8:56207	200.93.192.169:123	WAN 2	Load balanced	Fail over if uplink is down	21:09

En la Figura 42, se obtuvo los registros de tráfico generado por el equipo de videoconferencia en el SPOKE (IP: 192.168.128.8) hacia su contraparte en el HUB (IP: 192.168.30.7), evidenciando en este escenario ya que no dispone de reglas SD-WAN el balanceo lo realiza con su accionar por defecto del hardware, que corresponde al balanceo basado en el ancho de banda de cada enlace.

En la Tabla 8, se recolecta y muestra en una tabla el balanceo que realiza el equipo Meraki.

Tabla 8

LOG´s de balanceo por las dos interfaces WAN.

Hora	IP FUENTE	IP DESTINO/APLICACIÓN	INTERFAZ DESTINO	RAZÓN
21:10	192.168.128.8:2372	192.168.30.7:2376	WAN2	Balanceo de Carga/por Defecto
21:10	192.168.128.8:11001	192.168.30.7:5555	WAN1	Balanceo de Carga/por Defecto

Se confirmó el funcionamiento SD-WAN con una prueba adicional de conectar dos usuarios aparte de la videoconferencia cuyos registros se muestran en las Figuras 43, 44 y 45.

Figura 43

LOG usuarios varios hacia página web IESS.

Uplink decisions

190.95.221.137

Peer	Protocol	Source	Destination	Uplink decision	Reason	Policy	Last seen
IPCCL2 - 2	TCP	192.168.128.4:57555	190.95.221.137:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57563	190.95.221.137:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.5:54800	190.95.221.137:443	WAN 1	Load balanced	Fail over if uplink is down	21:02
IPCCL2 - 2	TCP	192.168.128.5:54798	190.95.221.137:443	WAN 1	Load balanced	Fail over if uplink is down	21:02
IPCCL2 - 2	TCP	192.168.128.5:54802	190.95.221.137:443	WAN 1	Load balanced	Fail over if uplink is down	21:02
IPCCL2 - 2	TCP	192.168.128.4:57554	190.95.221.137:443	WAN 1	Load balanced	Fail over if uplink is down	21:02
IPCCL2 - 2	TCP	192.168.128.4:57536	190.95.221.137:443	WAN 1	Load balanced	Fail over if uplink is down	21:01
IPCCL2 - 2	ICMP	192.168.128.4:1	190.95.221.137:0	WAN 1	Load balanced	Fail over if uplink is down	21:01
IPCCL2 - 2	TCP	192.168.128.4:57535	190.95.221.137:443	WAN 2	Load balanced	Fail over if uplink is down	21:01

Figura 44

LOG usuarios varios hacia página web ESPE.

Uplink decisions

192.188.58.167

Peer	Protocol	Source	Destination	Uplink decision	Reason	Policy	Last seen ▾
IPCCL2 - 2	TCP	192.168.128.4:57589	192.188.58.167:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57599	192.188.58.167:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57587	192.188.58.167:443	WAN 1	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57612	192.188.58.167:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57616	192.188.58.167:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57613	192.188.58.167:443	WAN 1	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.5:54767	192.188.58.167:443	WAN 1	Load balanced	Fail over if uplink is down	20:58
IPCCL2 - 2	TCP	192.168.128.5:54769	192.188.58.167:443	WAN 2	Load balanced	Fail over if uplink is down	20:58
IPCCL2 - 2	TCP	192.168.128.5:54765	192.188.58.167:443	WAN 1	Load balanced	Fail over if uplink is down	20:58

Figura 45

LOG usuarios varios hacia página web Banco Pichincha.

Uplink decisions

200.0.63.48

Peer	Protocol	Source	Destination	Uplink decision	Reason	Policy	Last seen ▾
IPCCL2 - 2	TCP	192.168.128.4:57571	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:04
IPCCL2 - 2	TCP	192.168.128.4:57558	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57565	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57567	200.0.63.48:443	WAN 1	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57559	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57569	200.0.63.48:443	WAN 1	Load balanced	Fail over if uplink is down	21:03
IPCCL2 - 2	TCP	192.168.128.4:57478	200.0.63.48:443	WAN 1	Load balanced	Fail over if uplink is down	21:01
IPCCL2 - 2	TCP	192.168.128.4:57476	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:01
IPCCL2 - 2	TCP	192.168.128.5:54777	200.0.63.48:443	WAN 2	Load balanced	Fail over if uplink is down	21:00

En la Tabla 9 se obtuvo los registros de los usuarios ejecutando peticiones hacia el internet.

En este escenario específicamente se realizó una consulta previa para conocer las IPs corresponden a las páginas:

Tabla 9

IP sitios destino.

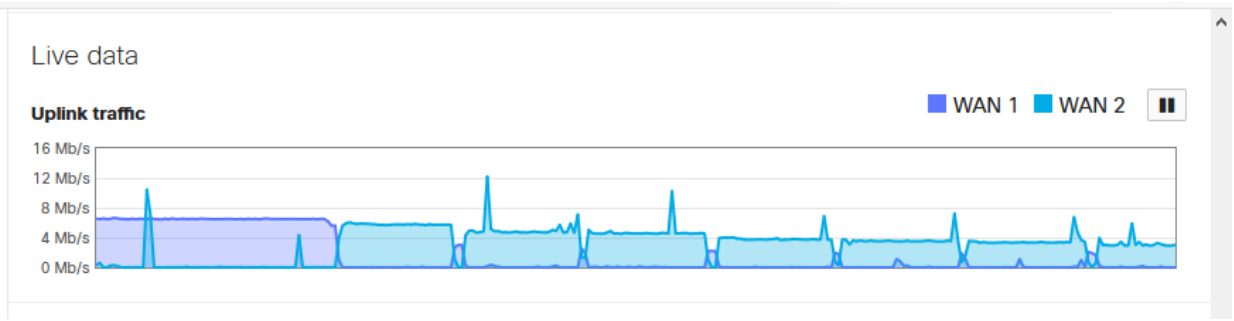
SITIO DESTINO PRUEBA	IP
VIDEO CONFERENCIA HUB	192.168.30.7
www.iess.gob.ec	190.95.221.137
www.espe.edu.ec	192.188.58.167
www.pichincha.com	200.0.63.48

Se realizó este proceso ya que en los registros de Meraki sólo presenta a nivel IP el destino, mas no resuelve el reverso, es decir la correspondencia de su sitio web con la IP Pública.

De igual manera se puede captar el tráfico en la Figura 46 que cursa en el balanceo de carga que realiza el equipo, ya que selecciona el mejor canal con mejor ancho de banda según su herramienta de análisis de rendimiento.

Figura 46

Tráfico captado por las interfaces de los 2 proveedores – Meraki.



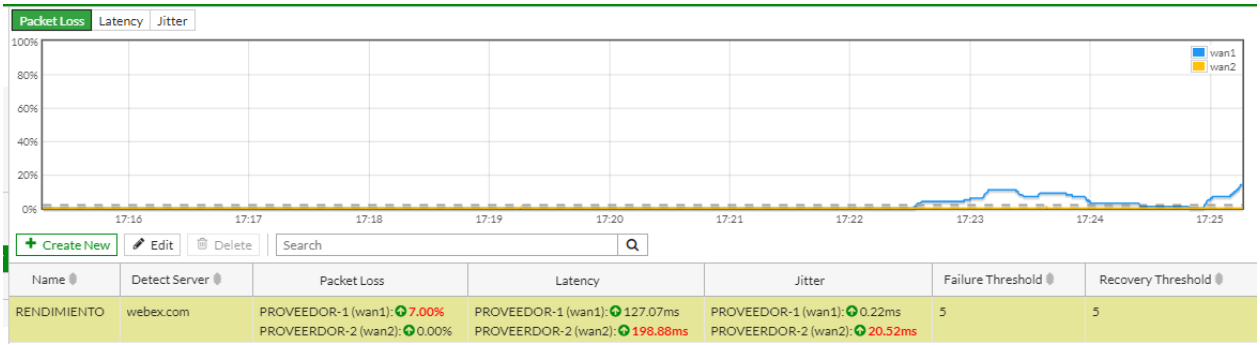
Escenario Nº 3 - Estado de selección del mejor enlace Fortigate

Para el estado de selección del mejor enlace lo que realiza el equipo es la revisión de las reglas definidas, esta las hace en un orden específico es decir las lee en el orden de la secuencia o posición definida siendo la ubicada en la parte superior la de mayor prioridad o en la que empieza la lectura de las reglas para su cumplimiento.

Se indica el estado del SLA predefinido en la Figura 47 con parámetros marcados en color rojo, el cual significa que está sobrepasando el umbral colocado.

Figura 47

Estado SLA - Fortigate.



Al declarar una sola regla SD-WAN, esta será la prioritaria, la cual corresponde a la de análisis de la aplicación Webex, el resto de tráfico que no coincida la orden a seguir será la de la regla implícita.

Como se puede visualizar en la Figura 48 se valida que al cursar tráfico no especificado en la regla “EVALU-WEBEX” esta cae en la implícita y consecuentemente al activarse la regla SD-WAN se obtiene los siguientes registros.

Regla ID 5 = Priorización Aplicación Webex

Regla ID 0 = Regla implícita

Figura 48

LOG selección mejor enlace aplicada regla SD WAN.

Date/Time	Source	Destination	Application Name	Policy	SD-WAN Rule ID	Destination Interface
2020/11/07 17:27:49	192.168.111.160	190.95.221.137 (www.iess.gob.ec)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:49	192.168.111.150	68.67.160.134 (ib.adnxs.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:48	192.168.111.150	3.22.156.195 (mcs-cloudstation-us-east-2.prod.hydra.sophos.com)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:47	192.168.111.111	99.192.248.32 (especiales.elcomercio.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:47	192.168.111.111	173.243.1.71 (mta2mcs218.webex.com)	udp/9000	LAN (1)	5	PROVEERDOR-2 (wan2)
2020/11/07 17:27:45	192.168.111.111	8.8.8.8 (dns.google)	DNS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:43	192.168.111.111	23.92.189.247 (scomcluster.cxense.com)	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:11	192.168.111.150	3.225.217.224 (http.00.s.sophosxl.net)	HTTP	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:11	192.168.111.111	8.8.8.8 (dns.google)	DNS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:11	192.168.111.111	8.8.8.8 (dns.google)	DNS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:49	192.168.111.160	190.95.221.137 (www.iess.gob.ec)	HTTPS	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:47	192.168.111.150	172.24.5.132	tcp/13000	LAN (1)	0	PROVEEDOR-1 (wan1)
2020/11/07 17:27:47	192.168.111.111	13.227.205.153	HTTPS	LAN (1)	0	PROVEERDOR-2 (wan2)
2020/11/07 17:27:47	192.168.111.111	173.243.1.71 (mta2mcs218.webex.com)	udp/9000	LAN (1)	5	PROVEERDOR-2 (wan2)

Adicional se podrá evidenciar en cómo el tráfico aumenta por la selección de mejor enlace, esto se lo demuestra en la Figura 49 que dispone de una caída mientras existe tráfico de videoconferencia, este tráfico desciende alrededor de las 17:20.

Figura 49

Tráfico que cursa por proveedor 1 antes de coincidencia regla SD WAN.

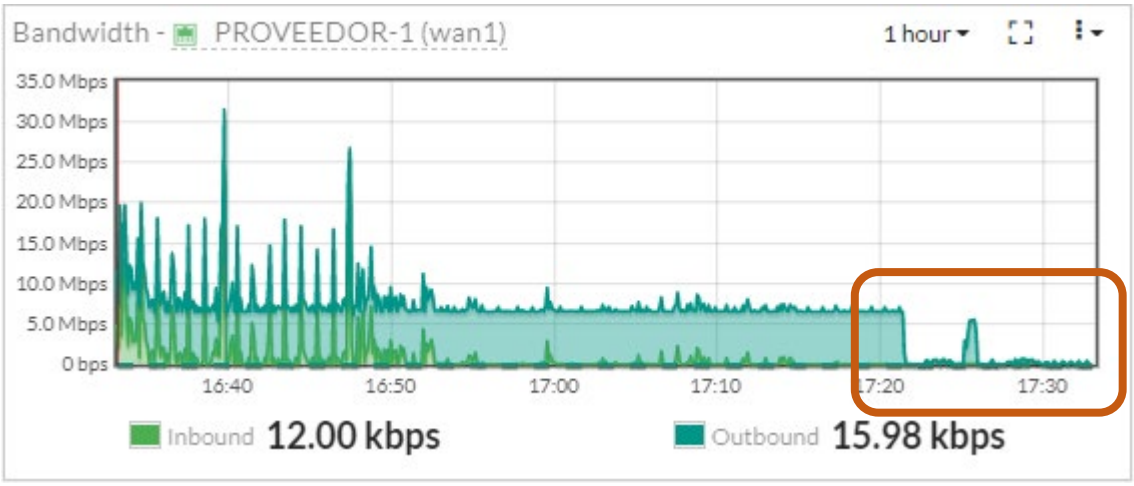
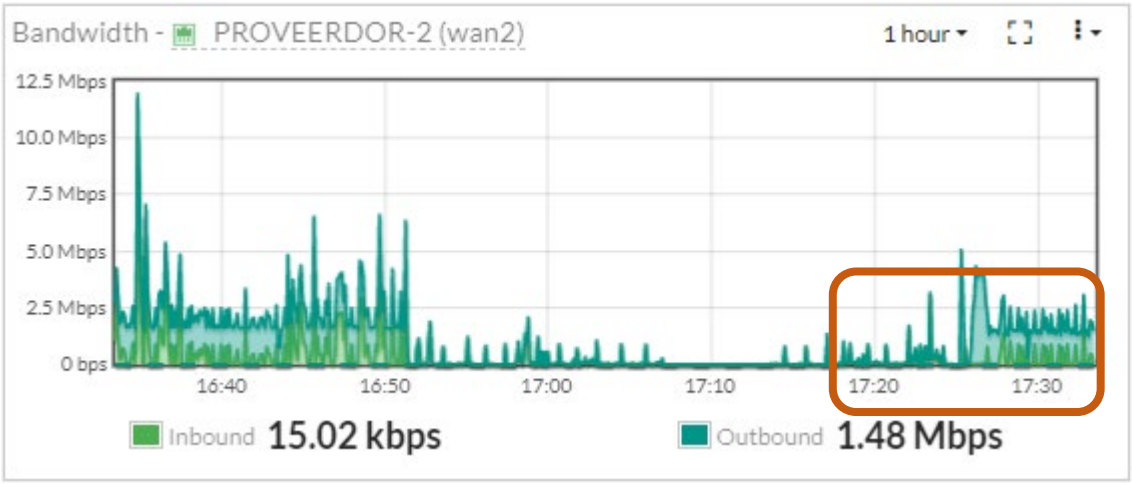


Figura 50

Tráfico que cursa por proveedor 2 después de coincidencia regla SD WAN.



En la Figura 50 se demuestra que al realizar la coincidencia de la regla SD WAN y validando que no cumple con el rendimiento pre definido este tipo de tráfico conmuta al enlace del proveedor 2.

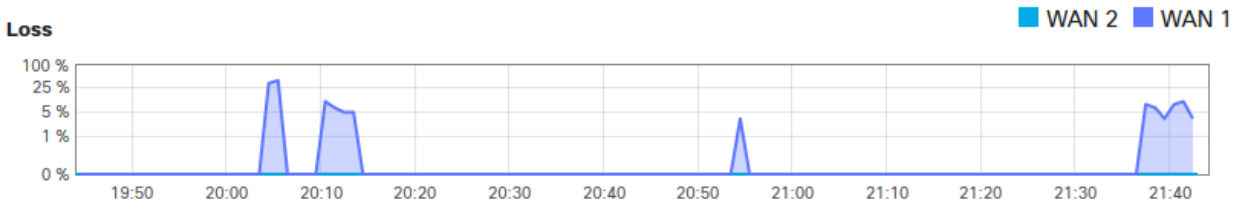
Escenario Nº4 - Estado de selección del mejor enlace Meraki

En este escenario para el estado de selección del mejor enlace se redujo el ancha de banda del enlace y se lo saturó en el proveedor 1.

En consecuencia, se evidencia un incremento de paquetes perdidos de alrededor del 5% como se indica en la Figura 51.

Figura 51

Paquetes perdidos WAN1.



Al haber configurado nuestra política SD-WAN, seleccionando la interfaz WAN2 cuando se degrade el enlace correspondiente a la WAN 1, el equipo Meraki da como resultado los siguientes registros mostrados en las Figuras 52, 53.

Figura 52

Balanceo proveedor 2 según política establecida.

Peer	Protocol	Source	Destination	Uplink decision	Reason	Policy	Last seen ▾
IPCCL2 - 2	TCP	192.168.128.8:11000	192.168.30.7:1720	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:02
IPCCL2 - 2	TCP	192.168.128.4:58207	52.54.16.202:443	WAN 2	Load balanced	Fail over if uplink is down	22:02
IPCCL2 - 2	TCP	192.168.128.5:55080	151.101.65.195:443	WAN 1	Load balanced	Fail over if uplink is down	22:02
IPCCL2 - 2	TCP	192.168.128.5:55081	13.68.20.25:443	WAN 2	Performance-based	Fail over if uplink is down	22:02
IPCCL2 - 2	TCP	192.168.128.5:53932	20.185.212.106:443	WAN 2	Performance-based	Fail over if uplink is down	22:02
IPCCL2 - 2	TCP	192.168.128.5:55082	192.16.48.200:443	WAN 2	Load balanced	Fail over if uplink is down	22:02
IPCCL2 - 2	TCP	192.168.128.5:55083	192.16.48.200:443	WAN 1	Load balanced	Fail over if uplink is down	22:02

Figura 53

Preferencia de salida de interfaz según política establecida.

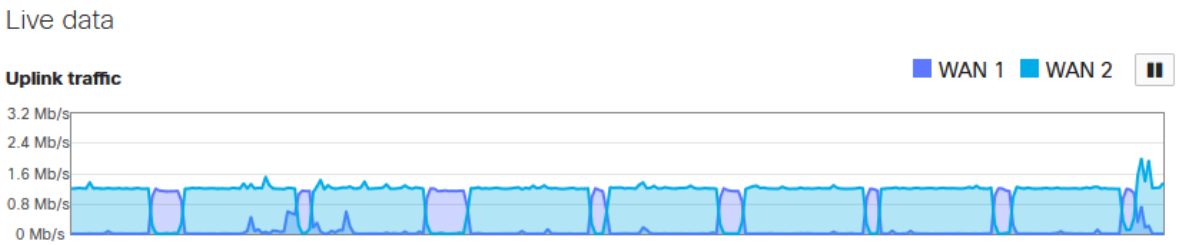
IPCCL2 - 2	TCP	192.168.128.8:11000	192.168.30.7:1720	WAN 1	Preferred uplink	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	UDP	192.168.128.8:2337	192.168.30.7:2331	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	UDP	192.168.128.8:2431	192.168.30.7:2431	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	UDP	192.168.128.8:2373	192.168.30.7:2377	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	UDP	192.168.128.8:2336	192.168.30.7:2330	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	UDP	192.168.128.8:2372	192.168.30.7:2376	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:07
IPCCL2 - 2	TCP	192.168.128.8:11001	192.168.30.7:5555	WAN 1	Preferred uplink	Prefer WAN 1. Fail over if poor performance for "RENDIMIENTO-P"	22:06

La utilización de tráfico que produce la videoconferencia, se confirma en el balanceo de carga realizado por Meraki, en la Figura 54 se denota la utilización del enlace WAN2 que es el enlace por donde la videoconferencia ejecuta la conmutación ya que WAN1 no cumple con los requerimientos de

funcionamiento definidos, en ciertos momentos se evidencia estabilidad por la WAN1 por ende vuelve a su estado original o de preferencia.

Figura 54

Tráfico que cursa por los dos proveedores después de la aplicación de la regla SD WAN.



CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Dentro del análisis expuesto en la implementación y funcionamiento de la tecnología SD-WAN de cada marca, se evidenció que para el esquema de acceso a las aplicaciones de videoconferencia por internet fue necesario utilizar un mayor número de equipos en Meraki e inclusive adquirir licenciamiento caso contrario que en Fortinet, es decir con Fortinet fue necesario un solo equipo conectado los dos enlaces y con Meraki fue necesario implementar un modelo HUB-SPOKE para que el acceso a internet pueda ser mediante el HUB, puesto que se comprueba que existe limitaciones de desarrollo en el software; consecuentemente los costos en la implementación en la marca Meraki son mayores en referencia a adquisición y mantenimiento, siendo esto una consideración importante en la toma de decisión del usuario en que equipos adquirir.

Se verificó en base a los resultados de obtención de registros indicados en las Figuras 39 y 42, que el software de la tecnología SD-WAN, se establece simultáneamente una sesión origen-destino, por cada enlace que se disponga, teniendo la ventaja de balancear tráfico de capa 3 hasta capa 7 según modelo OSI versus redes tradicionales MPLS que soporta hasta capa 3 debido que se apoya en protocolos de enrutamiento en el plano de datos.

En base a lo analizado se puede crear o generar una o varias políticas de rendimiento ya mostradas en el capítulo 4 y sus diferentes escenarios, que se dispone en cada marca de equipo con la tecnología SD-

WAN, en donde se puede realizar la selección del enlace de acuerdo a un rendimiento SLA conformado por: pérdida de paquetes, latencia y jitter utilizando uno de ellos o la combinación de todos al mismo tiempo, al contrario que en las redes tradicionales MPLS la conmutación de los enlaces se produce mediante las capacidades de los protocolos de enrutamiento que al final son limitadas por los cambios en la tabla de enrutamiento.

Al momento de la implementación de las políticas SD-WAN se pudo evidenciar que las programaciones aunque apliquen SD-WAN de manera exitosa, en Fortinet (Fortigate) puede ser mucho más específico pudiendo seleccionar características de cada aplicación, en el caso de Webex características como chat, compartición de pantalla, control remoto, entre otras, de la misma manera maneja una base de datos de servicios de internet que engloba todo el conjunto de IP's públicas asociadas al dominio de la aplicación y Cisco (Meraki) sólo maneja categorías generalizadas.

Al utilizar diferentes proveedores y analizando su rendimiento en cada intervalo de tiempo como se lo mostró en la Tabla 5 de rendimiento de los tres proveedores, se hace necesario el uso de la tecnología SD-WAN, por ejemplo, en aplicaciones críticas o como de videoconferencia en nuestro caso de estudio, al momento que se presente una incidencia de pérdida total del enlace o degradación del mismo, el usuario no percibió una indisponibilidad en el proceso de conmutación del enlace.

Frente a la evidencia de la implementación de esquema SD-WAN, desarrollada en el presente estudio se concluye que esta tecnología es completamente aplicable para todo tipo de negocios que requieran acceso a internet y uso de diferentes aplicaciones, puesto que la tendencia es que los servicios ya sean de correo, bases de datos, videoconferencia se alojen en la nube, debido que todo este tipo de

aplicaciones son muy críticas se requiere que la inteligencia que maneja el software SD-WAN permita alta disponibilidad y un uso eficiente del ancho de banda contratado por el usuario, contrarrestando en evitar pérdidas de información teniendo impacto en el tema económico.

Recomendaciones

En la implementación del proyecto se recomienda validar las licencias activas para los dispositivos Meraki, al no disponer de una licencia activa no permite la configuración de las características que son necesarias del equipo, la administración de los dispositivos Meraki son en la nube y no se los puede configurar de manera local.

Se recomienda crear una interfaz lógica VPN Site-to-Site en los dispositivos Meraki usando el protocolo IPsec para establecer las funcionalidades SD-WAN sobre este, en el presente trabajo se lo detalla en la Configuración General de Meraki.

Se requiere IP's fijas públicas que sean provistas por el proveedor para la asignación en cada una de las interfaces WAN del Meraki MX en vista de que, sin ellas, no permitirá la conexión VPN Site-to-Site hacia el HUB, y como resultado la conmutación de canal no sucederá.

Se recomienda revisar la versión de firmware en Fortigate ya que a partir de la versión 5.0.X se tiene habilitado la funcionalidad SD-WAN mientras que en Meraki, sólo lo permite por hardware que corresponden a la serie MX-Router con doble interfaz WAN.

Se sugiere configurar los parámetros críticos, según la definición de la aplicación o priorización de tráfico que se vaya a realizar ya que en la latencia se puede presentar falsos positivos o una eventualidad fortuita del enlace por un pico de saturación. Lo que respecta al jitter y la latencia, dependen e influye la conexión hacia donde la estemos levantando, el evaluar los paquetes perdidos en los enlaces permite mayor efectividad en la conmutación o selección del mejor enlace.

Trabajos Futuros

Con la llegada del 5G se propone establecer la tecnología SD-WAN para lugares remotos ya que la red móvil es una de las mejores opciones para poder conectar estos sitios, esto incluye también sitios de difícil acceso al exterior. Ya de por sí existen equipos que ya integran la capacidad de la inserción de un chip e impulsaría a disponer mayor conectividad en lugares que no existe cobertura y también considerando las altas capacidades que manejan.

Ya que SD-WAN ofrece también seguridad y cifrado punto a punto y que las aplicaciones que se utilizan como herramientas de trabajo se encuentran más en la nube como: Office 365, AWS, Azure, se podrían establecer conexiones VPN a estos sitios y evaluar el rendimiento de conexión hacia los servicios que nos ofrecen, aún más también se considera y se encuentra en desarrollo vCPE (Un equipo virtual de las instalaciones del cliente), que aun más permite la reducción de costos en las implementaciones de oficinas y equipamiento en sitio, se obtendría: seguridad, alta disponibilidad, proyección para aumento de recursos y sin incurrir en gastos adicionales.

REFERENCIAS

Álvarez Pinilla, R. (2015). *Open Access These and Dissertations.* Retrieved from http://oa.upm.es/42968/1/TFM_RAUL_ALVAREZ_PINILLA.pdf

Butler, B. B. (2017, 06 20). *NETWORK WORLD.* Retrieved from SD-WAN: qué es y por qué lo va a usar: https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar

Ccoyllo Sulca, I. (2018). *TECSUP.* Retrieved from Redes definidas por Software (SDN): https://informatica.ucm.es/data/cont/media/www/pag-103596/transparencias/redes-por-software-SDN.pdf

CISCO. (2018). *National Instruments ramps up network.* Retrieved from https://www.cisco.com/c/dam/en_us/services/it-case-studies/ni-case-study.pdf

Cisco. (n.d.). *MX Cloud Managed Security Appliance Series.* Retrieved from Meraki: https://meraki.cisco.com/wp-content/uploads/2020/05/meraki_datasheet_mx60_family.pdf

CITRIX. (n.d.). *SD-WAN, la respuesta a la necesidades de la red empresarial.* Retrieved from https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/sd-wan-the-answer-to-networking-demands-es.pdf

FIREWALL.CX. (2020, Agosto 31). *COMPLETE GUIDE TO SD-WAN. TECHNOLOGY BENEFITS, SD-WAN SECURITY, MANAGEMENT, MOBILITY, VPNS, ARCHITECTURE & COMPARISON WITH TRADITIONAL WANS. SD-WAN PROVIDERS FEATURE CHECKLIST.* Retrieved from FIREWALL.CX: http://www.firewall.cx/general-topics-reviews/sd-wan/1210-sd-wan-networks-benefits-management-security-architecture.html

FORTINET. (2019). *Cadena global de restaurantes.* Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-global-restaurant-chain-adopts-secure-sd-wan-to-improve-connectivity-and-security-in-brazil.pdf

FORTINET. (n.d.). *SENATI: Desplegando una red segura para conectar a todo el Perú.* Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/case-studies/es_la/cs-senati.pdf

FortiXpert. (2017, Marzo 30). *SD-WAN y Fortinet: El paso natural.* Retrieved from https://fortixpert.blogspot.com/2017/03/sd-wan-y-fortinet-el-paso-natural.html

Frómeta Fonseca, D., Anías Calderón, C., Ballester Macías, S., & León González, S. (2016). *Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A.* Retrieved from Desarrollo de aplicaciones SDN: http://www.revistatonoetecsa.cu/articulo/desarrollo-de-aplicaciones-sdn

Garcia Centeno, A., Rodríguez Vergel, C., Anías Calderón, C., & Casmartiño Bondarenko, C. (2014, Septiembre-Diciembre). *Controladores SDN, elementos para su selección y evaluación.* Retrieved from TELEMÁTICA MAGAZINE: http://revistatelematica.cujae.edu.cu/index.php/tele/article/view/164

Garden, Z. (2015, Febrero 23). *Open Zen.* Retrieved from PROVEYENDO HERRAMIENTAS PARA LA ADMINISTRACIÓN DE WLANS A TRAVÉS DE SDN: https://openzen.wordpress.com/2015/02/12/historia-del-sdn/

Gonzalez, C. F. (2018, Agosto 22). *Portal de Revistas UTP, Memorias de Congresos.* Retrieved from https://revistas.utp.ac.pa/index.php/memoutp/article/view/1842

GRUPO.BIT. (2020). *GTUPO-BIT Business Analytics.* Retrieved from ANALISIS DE DATOS - ¿Cuantos Datos se produce en un minuto?: https://business-intelligence.grupobit.net/blog/cuantos-datos-se-producen-en-un-minuto

Hwang, S. (2019, Abril 3). *Fortinet Secure SD-WAN Reference Arquitecture.* Retrieved from FORTINET: https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf?utm_source=social&utm_medium=twitter-org&utm_campaign=sprinklr

Lajara, C., Martí, M., & Villagarcía, L. (2016, Enero 4). *Videoconferencia Educativas.* Retrieved from Slideshare: https://www.slideshare.net/mariamartinsanchez18/videoconferencias-educativas-presentacin

Millán Tejedor, R. (2014). *CONSULTORÍA ESTRATÉGICA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.* Retrieved from https://www.ramonmillan.com/tutoriales/sdnredesinteligentes.php

Open Networking Foundation. (2013, Diciembre 12). *SDN Architecture Overview.* Retrieved from https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf

Pham, M., & B. Hoang, D. (2016, Junio 6-10). *IEEE Xplore.* Retrieved from SDN applications - The intent-based Northbound Interface realisation for extended applications: https://ieeexplore.ieee.org/document/7502469/authors#authors

Ramírez Giraldo, M., & López Echeverry, A. M. (2018, Enero 09). *Redes de datos definidas por software - SDN, arquitectura, componentes y funcionamiento.* Retrieved from Journal de Ciencia e Ingeniería: https://jci.uniautonoma.edu.co/2018/2018-7.pdf

Romo, M. E., & Zatarin, N. (2008). *La Videoconferencia.* Retrieved from Universidad Autónoma de Guadalajara: https://slideplayer.es/slide/1048936/

Roncero Hervás, Ó. (2014, Mayo 20). *UPCommons. Portal de acceso abierto al conocimiento de la UPC.* Retrieved from UPCommons: https://upcommons.upc.edu/bitstream/handle/2099.1/21633/Memoria.pdf

Salinas Santiago, J., Sánchez Venegas, C., Herrera Velásquez, J., & Santiago C, C. (2019, Julio 24-26). *SDN Implementation of virtual computing.* Retrieved from 17th LACCEI International Multi-Conference for Engineering, Education, and Technology: http://laccei.org/LACCEI2019-MontegoBay/full_papers/FP478.pdf

Tansey, J. (2010). *Deploying Webex in Enterprise Networks.* Retrieved from Cisco Live: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKCOL-2010.pdf