ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"DISEÑO DE UNA RED SD-WAN SEGURA BASADA EN LA APLICACIÓN DE CÓDIGO ABIERTO ZEROTIER"

Trabajo de Titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR:

LUIS ROMARIO GARCÍA SANTANA

Riobamba – Ecuador

2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"DISEÑO DE UNA RED SD-WAN SEGURA BASADA EN LAS APLICACIÓN DE CÓDIGO ABIERTO ZEROTIER"

Trabajo de Titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: LUIS ROMARIO GARCÍA SANTANA

DIRECTOR: ING. ALBERTO LEOPOLDO ARELLANO AUCANCELA MSc.

Riobamba – Ecuador

2022

Yo, **Luis Romario García Santana**, declaro que el presente trabajo de titulación es de mi autoría y que los resultados de este son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 13 de abril de 2022

Luis Romario García Santana

080297107-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y TELECOMUNICACIONES

El Tribunal del Trabajo de Titulación certifica que: El Trabajo de Titulación; Tipo: Proyecto de Investigación, **"DISEÑO DE UNA RED SD-WAN SEGURA BASADA EN LA APLICACIÓN DE CÓDIGO ABIERTO ZEROTIER"**, realizado por el señor **LUIS ROMARIO GARCÍA SANTANA**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Lourdes Del Carmen Zuñiga Lema **PRESIDENTE DEL TRIBUNAL**		2022-04-13
Ing. Alberto Leopoldo Arellano Aucancela MSc. **DIRECTOR DE TRABAJO DE TITULACIÓN**		2022-04-13
Ing. Hugo Oswaldo Moreno Avilés PhD. **MIEMBRO DEL TRIBUNAL**		2022-04-13

DEDICATORIA

Mi principal agradecimiento a Dios, ser divino quien me ha guiado y me ha dado la fortaleza para seguir adelante. A mi familia por siempre darme ánimos cuando decaída y nunca me abandonaron a mis profesores, colegas, participantes de la investigación y a todos mis ingenieros que me guiaron y me dieron todo el apoyo para realizar esta investigación, también agradezco a la universidad por las oportunidades que me ha brindado.

Romario

AGRADECIMIENTO

Lleno de regocijo, de amor y esperanza, dedicó este proyecto, a cada uno de mis seres queridos, quienes han sido mis pilares para seguir adelante. Es para mí una gran satisfacción poder dedicarles a ellos, que con mucho esfuerzo, esmero y trabajo me lo he ganado.

Romario

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

AC:	Corriente Alterna
BW:	Ancho de banda
CC:	Corriente Continua
EMI:	Interferencia electromagnética
FM:	Frecuencia modulada
IEEE:	Instituto de Ingenieros Eléctricos y Electrónicos
IDC:	International Data Corporation
IP:	Protocolo de internet
ISM:	Industrial, científico y médico
LAN:	Red de Área Local
MHz:	Megahercio
SD-WAN:	Red de Área Amplia Definida por Software
TIC:	Tecnologías de la información y la comunicación
VPN:	Red Virtual Privada
WAN:	Red de Área Amplia
Wi-Fi:	Fidelidad inalámbrica

RESUMEN

El objetivo de este proyecto de investigación fue diseñar una red SD-WAN segura basada en la aplicación de código abierto ZeroTier, para lo cual se estudió las ventajas que tiene la utilización de esta tecnología, además del aporte a la infraestructura de la red, permitiendo conocer el funcionamiento, arquitectura y comportamiento de esta. La estructura y funcionamiento de la red SD-WAN se llevó a cabo mediante la investigación y conceptualización de los componentes. Se especificó las aplicaciones de código abierto existentes que intervienen en el diseño, tomando en cuenta que permitan la utilización de diferentes topologías de red para conectar dos sitios remotamente. Se implemento un prototipo simulado bajo la aplicación ZeroTier, usando dos proveedores de servicios en una red Ip/mpls como caminos de conexión hacia el internet. Se verifico el correcto funcionamiento de las principales características presentes en el ambiente simulado creando un servidor Web que utiliza el protocolo HTTP a través del servidor Apache enrutando las redes locales de los sitios A y B a través del túnel de ZeroTier, donde se realizó un conjunto de cincuenta pruebas de petición de descargas entre cliente – servidor y caídas de enlace. Se describió los beneficios de la red diseñada en base a un análisis estadístico que determinó que los datos llevan una distribución normal y un valor representativo de la media de cada tecnología. Se concluye que las ventajas de usar ZeroTier son notables indudablemente ya que tiene la capacidad de adaptarse a cualquier entorno de red, trabaja de manera segura, reduce precios en costos, debido a que es un *software* de código abierto y se puede acoplar a las demandas que se necesitan. Se recomienda dar seguimiento a los resultados obtenidos en el presente estudio, debido a que estos son empíricos, ya que se aplicaron en simulaciones.

Palabras clave: <RED SD-WAN>, <APLICACIÓN>, <PROTOTIPO SIMULADO>, <CÓDIGO ABIERTO>, <TOPOLOGÍA DE RED>, <CONEXIÓN REMOTA>, <PROTOCOLO>.

SUMMARY

The objective of this research project was to design a secure SD-WAN network based on the ZeroTier open source application, for which the advantages of using this technology were studied, in addition to the contribution to the network infrastructure, allowing know the operation, architecture and behavior of this. The structure and operation of the SD-WAN network was carried out through the investigation and conceptualization of the components. The existing open source applications that are involved in the design were specified, taking into account that they allow the use of different network topologies to connect two sites remotely. A simulated prototype was implemented under the ZeroTier application, using two service providers in an Ip/mpls network as connection paths to the internet. The correct operation of the main features present in the simulated environment was verified by creating a Web server that uses the HTTP protocol through the Apache server, routing the local networks of sites A and B through the ZeroTier tunnel, where a set of of fifty download request tests between client – server and link failures. The benefits of the designed network were described based on a statistical analysis that determined that the data has a normal distribution and a representative value of the mean of each technology. It is concluded that the advantages of using ZeroTier are undoubtedly notable since it has the ability to adapt to any network environment, works safely, reduces cost prices, because it is open source software and it can be coupled to the demands that are needed. It is recommended to follow up on the results obtained in this study, because they are empirical, since they were applied in simulations.

Keywords: <SD-WAN NETWORK>, <OPEN SOURCE APPLICATION>, < SIMULATED PROTOTYPE>, <NETWORK TOPOLOGY>, <REMOTE CONNECTION>.

MsC. Wilson G. Rojas
0602361842

INTRODUCCIÓN

En el Ecuador, las pequeñas y medianas empresas (PYMES), son un bloque de la cultura empresarial, que engloba micro, pequeñas y medianas empresas, las cuales en conglomerado representan el 99,5% del total de empresas legalmente constituidas en la Superintendencia de Compañías, estas empresas se caracterizan por los limites en cuanto al recurso económico y por el hecho de que estas se van adaptando conforme se experimentan cambios en el mercado, lo cual, en el peor de los casos, desembocan en el cierre de las mismas.

En cuanto, a sus redes digitales, estas emplean las redes WAN, las cuales están adaptadas más bien para satisfacer las necesidades de conectividad de los hogares, donde el tráfico de usuarios es limitado, además de que, para dar acceso a sus sucursales u oficinas en lugares remotos, las PYMES deben invertir en dispositivos (*hardware*), específicos los cuales muchas veces cuentan con altos valores debido a que son importados.

Teniendo en cuenta que en la actualidad han ganado espacio los dispositivos conectados a la nube, que demandan de mejores rendimientos de red, en aspectos tales como la movilidad y redes sociales son empleadas por las empresas, no solo para impulsar su competitividad, sino para ofrecer una mejor experiencia dentro de sus entornos digitales. Con base en lo antes mencionado, se establece que el objetivo general del presente estudio es “Diseñar una red SD-WAN segura basada en la aplicación de código abierto ZeroTier”. Con lo cual se espera obtener mejores rendimientos de manera que las PYMES se decidan por aplicar esta tecnología en sus redes.

Es preciso mencionar que esta tecnología permitirá que las empresas brinden garantías de conexión estable a sus usuarios, sin contar, la seguridad de su información y una reducción en la volatilidad de los datos, mientras que para sí mismas, se tiene una reducción de costos en casi la mitad, debido a que experimentarán una merma en los costos de las redes, ya que no deberán comprar *hardware* para poder enrolar las sucursales, porque en este caso ZeroTier, se encarga de virtualizar la red enlazándola de manera directa a la nube.

Este estudio contará con tres capítulos los cuales serán descritos a continuación:

El primer capítulo corresponde al marco teórico de la investigación donde se determinarán conceptualizaciones sobre los componentes y las diferentes aplicaciones que intervienen dentro de la arquitectura SD – WAN que se pretende diseñar en el presente estudio.

En el segundo capítulo, se determinarán aspectos tales los métodos empleados para el desarrollo de una red SD- WAN, para lo cual, se establecieron fases, que parten de los requerimientos de *Hardware* y *Software*, para posteriormente realizar la configuración y puesta en marcha de la red.

En el tercer capítulo, se realizó un análisis del comportamiento de la red SD – WAN, para lo cual se toman en consideración aspectos tales como administrar la red mediante ZeroTier, balance – xor, alta disponibilidad en la red denominada Failover, Adicionalmente se realizará una comparación entre OPENVPN y ZeroTier, para conocer cuál de las dos tecnologías ofrece un tiempo rendimiento en cuanto a la disponibilidad de la red.

ANTECEDENTES

Las empresas están adoptando tecnologías digitales (como la nube, la movilidad, Big Data y redes sociales) para aumentar su ventaja competitiva al cambiar fundamentalmente la forma en que hacen negocios. Esta transformación digital de sus procesos, productos y estrategias de salida al mercado debe ir de la mano de una evolución de la red de área extensa (WAN). La conectividad de red sustenta todos los aspectos de esta transformación, que al mismo tiempo impulsa los requisitos de red a nuevas alturas. Las arquitecturas de red híbrida, la conectividad en la nube y la virtualización de red se han convertido en elementos clave para ofrecer la flexibilidad, la capacidad de administración, la escalabilidad y la rentabilidad que las empresas demandarán de su WAN (CASTELLOTE, 2018).

International Data Corporation (IDC) ha publicado dos nuevos informes de investigación sobre el mercado de infraestructura de red de área amplia definida por *software* (SD-WAN) de rápido crecimiento. Este importante segmento del mercado de redes empresariales crecerá a una tasa de crecimiento anual compuesta (CAGR) del 30,8% de 2018 a 2023 para alcanzar los $ 5,250 millones, según el pronóstico de infraestructura SD-WAN de IDC. El informe de cuotas de mercado de IDC incluye los ingresos de 2017 y 2018 por proveedor para la infraestructura SDWAN (IDC, 2019).

Según un informe publicado recientemente por Dell'Oro Group, la fuente confiable de información de mercado sobre las industrias de telecomunicaciones, redes y centros de datos de TI, el mercado mundial de SD-WAN creció un 64 % y superó el nivel de mil millones de dólares durante todo el año. 2019. El informe inaugural de participación de mercado de SD-WAN de Dell'Oro Group muestra que los cinco proveedores líderes, Cisco, Silver Peak, Versa, VMWare y Fortinet, tuvieron una participación de ingresos combinada de casi el 60% en 2019 (POSTSUS, 2021) .

La tecnología SD-WAN en estos últimos años ha ido creciendo debido al aumento de aplicaciones que se encuentran en la nube, y la demanda de equipos para la sostenibilidad de estas, existen varios proyectos realizados utilizando esta arquitectura. Se han realizado varios estudios en los cuales tenemos:

AN EFFICIENT MPLS-BASED SOURCE ROUTING SCHEME IN SOFTWARE-DEFINED WIDE AREA NETWORKS (SD-WAN).

Este documento trata sobre el concepto de enrutamiento de origen utilizando etiquetas MPLS. Garantizando flexibilidad y es adecuado para su aplicación tanto en SD-LAN como en SD-WAN al admitir varios conmutadores de n puertos ($n \geq 4$). Utilizando un algoritmo de agrupación en clústeres MaxHop, la red se divide en varias secciones (ALI, y otros, 2017).

SD-WAN: AN OPEN-SOURCE IMPLEMENTATION FOR ENTERPRISE NETWORKING SERVICES.

Este documento propone una implementación temprana de SD-WAN basada en componentes de código abierto, como OpenDaylight como SDN_controller, OpenvSwitch (OvS) y un conjunto de servicios para monitoreo de red y selección de ruta basada en políticas (TROIA, 2020).

IMPLEMENTATION OF A SD-WAN FOR THE INTERCONNECTION OF TWO SOFTWARE DEFINED DATA CENTERS

Este proyecto se basa en una implementación de una red de área amplia definida por *software* (SD-WAN) para conectar dos centros de datos definidos por *software*, lo que garantiza una calidad de servicio (QoS) predefinida y priorización de tráfico. Se realizan varias simulaciones en escenarios regidos por servicios VoIP y se miden el ancho de banda, el retardo, la fluctuación y la carga de la CPU (MORA, 2019).

FORMULACIÓN DEL PROBLEMA

¿Es posible diseñar y simular una red SD-WAN empleando la aplicación de código abierto ZeroTier?

SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cuáles son los principales componentes de la arquitectura de una red SD-WAN?
- ¿Cuáles son las aplicaciones de código abierto que permiten implementar redes SDWAN? ¿Qué ventajas tiene el uso de aplicaciones de Código abierto en la implementación de redes SD-WAN?

- ¿Qué parámetros deben ser monitoreados dentro de una infraestructura SD-WAN, para verificar su rendimiento?

JUSTIFICACIÓN TEÓRICA

Las empresas han estado utilizando redes WAN durante décadas, principalmente para conectar sus oficinas o sucursales remotas con sus oficinas centrales mediante el arrendamiento de capacidades de redes seguras de operadores de telecomunicaciones y la ejecución de redes privadas sobre ellos. Los protocolos WAN subyacentes han evolucionado a lo largo de los años y el actual es Multiprotocol Label Switching (MPLS) (BLOOMBERG, 2017).

La forma de trabajar en las organizaciones ha ido sufriendo cambios notables en estos últimos años. Así, hasta hace poco resultaba factible para una empresa trabajar mediante conexiones de red estáticas con sus sucursales, sin embargo, hoy en día con la llegada de distintos servicios y aplicaciones en la nube, les surge la necesidad de expandirse geográficamente para mantenerse competitivas en un mercado cada vez global (VARGAS BRAVO, 2020).

Esta mayor distribución geográfica de las instituciones les obliga a disponer de una infraestructura de red dinámica, flexible y reducida en cuantos a costes. Las organizaciones necesitan resolver algunos problemas que las conexiones de red tradicionales MPLS como son (VARGAS BRAVO, 2020):

- Incremento de costes ante la necesidad de un mayor ancho de banda, una gran complejidad y un mayor tiempo en el despliegue e implementación de nuevas sucursales, la falta de automatización de los equipos.
- Al utilizar Redes WAN tradicionales por medio del protocolo de transporte MPLS ya no es sostenible para las empresas debido a la creciente demanda de tráfico de la red, esto es un problema presente en las redes WAN ya que existen muchas aplicaciones empresariales que se trasladan hacia un centro de datos virtuales basados en la nube y requieren una mayor capacidad de recursos, incluyendo los servicios SaaS.
- Al implementar las redes con infraestructura SD WAN se trata de resolver problemas debido a que comprende un diseño de red escalable y flexible con la capacidad de que el usuario pueda acceder a cualquier aplicación para las empresas desde cualquier lugar de la red , a su vez ayuda aumentar el ancho de banda para las mismas, brindando seguridad de información, una reducción significativa de costos, y la manera de controlar las redes de forma automática para el control del tráfico, por lo tanto, las instituciones deben adaptarse y evolucionar para el nuevo entorno computacional como lo es el uso de la arquitectura SD-WAN.

El presente trabajo de investigación detalla un profundo análisis de la red SD-WAN utilizando la herramienta de código abierto ZeroTier, realizando la simulación en entornos virtuales.

JUSTIFICACIÓN APLICATIVA

Para este apartado se hizo uso de la arquitectura de la red SD-WAN, mismo que se puede visualizar en la figura 1-0.

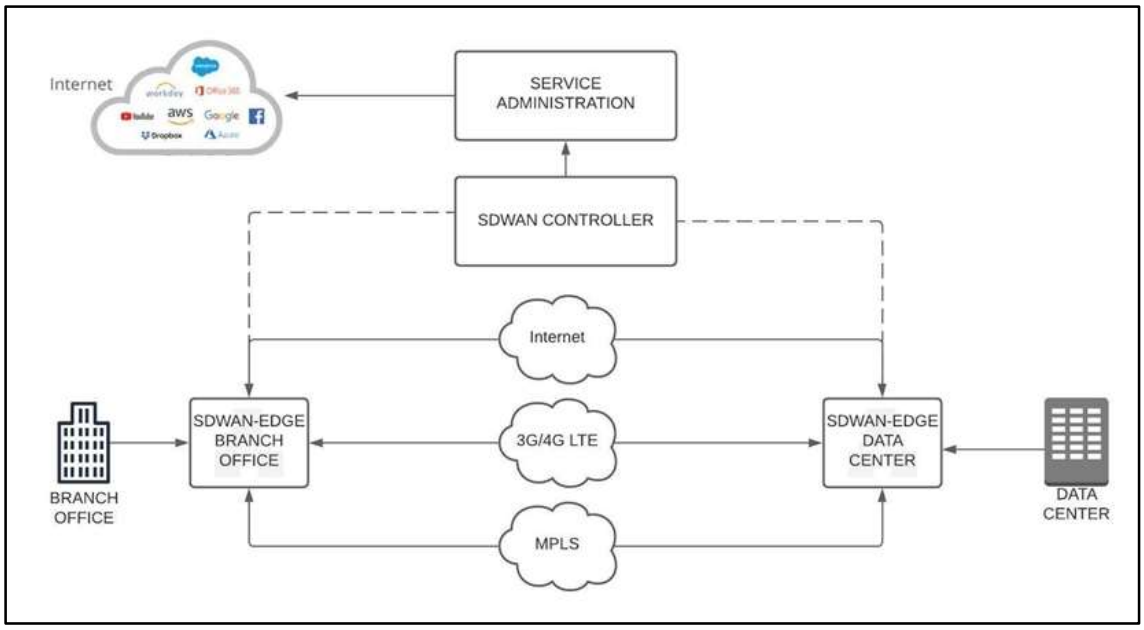


Figura 1-0: Arquitectura de red SD-WAN

Realizado por: García, Luis, 2022.

En la actualidad las empresas apuntan a avances tecnológicos con nuevas exigencias, aplicaciones y servicios que requieren un despliegue automatizado e individual de recursos en la red. Para solventar los problemas de las redes WAN tradicionales como son los de costos de anchos de banda, disponibilidad de las aplicaciones basadas en la nube para los diversos servicios de las empresas, complejidad y falta de automatización de los equipos. Se propone una red SD-WAN que va a constar de una infraestructura explicada en tres partes.

Dentro del plano de datos se encuentran los bordes de SD-WAN que permite crear y terminar túneles seguros a través de distintos tipos de redes subyacentes como son: Internet, redes 3G/4G LTE y centrales MPLS. SD-WAN Controller permite administrar los dispositivos físicos o virtuales para todos los bordes SD-WAN y Gateway asociadas al controlador, permite identificar el estado operativo de los túneles y determina métricas de rendimiento de QoS. El servicio administrativo proporciona el control, uso, análisis, seguridad y política de servicio de la red.

Este diseño de Red SD-WAN tiene como funcionalidad solventar problemas existentes en las Redes WAN tradicionales dar disponibilidad en el caso si un enlace esta experimentado una pérdida de paquete, el controlador SD-WAN utiliza técnicas con el fin de determinar que medio es el adecuado para poder asegurarse de que la aplicación al que está intentando acceder un usuario funcione correctamente y tengan una mejor experiencia de interactividad. A través de la aplicación de código libre ZeroTier la red podrá combinar las capacidades de VPN y SD-WAN para las conexiones entre sitios remoto, para poder simplificar la administración de esta.

OBJETIVOS

OBJETIVO GENERAL

Diseñar una red SD-WAN segura basada en la aplicación de código abierto ZeroTier.

OBJETIVOS ESPECÍFICOS

- Analizar la estructura y funcionamiento de la red SD-WAN.
- Especificar las aplicaciones SD-WAN de código abierto existentes.
- Implementar un prototipo simulado de red SD-WAN bajo la aplicación de código abierto ZeroTier.
- Verificar el correcto funcionamiento de las principales características SD-WAN en el ambiente simulado.
- Describir las ventajas de usar una red SD-WAN diseñada con la aplicación de código Abierto ZeroTier.

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

En este capítulo se presenta los principales temas que constituyen al tema del proyecto de investigación.

1.1 Redes definidas por *software* (SDN)

Son una alternativa para la creación de redes de telecomunicación, la cual se caracteriza por el desprendimiento en gran medida el control de un equipo físico, otorgando toda la responsabilidad a un controlador virtual o *software.*

El termino SDN se ha vuelto muy relevante en los últimos años porque ofrece la posibilidad de separar el plano de control y el plano de datos para la creación de redes más flexibles a nivel de programación y automatización, logrando una virtualización de la red para que se independice de la infraestructura existente.

Las SDN elimina la necesidad de las redes convencionales que basan en *hardware* que toman decisiones en un servidor. Esta tecnología divide las funciones de la capa de enlace de datos, para automatizarla con la finalidad que se vuelva autónoma. Esto implica que no necesitaría un *hardware* o *software* especial, contribuyendo a la reducción de costos y simplicidad de gestión de red.

En una red definida por *software* el administrador tiene la capacidad de asignar tráfico desde consola sin la necesidad de prestar atención en los conmutadores individuales. El administrador tiene la apertura para cambiar las reglas de los conmutadores en el momento que sea necesario, lo que posibilita la administración y control de paquetes de forma detallada.

La administración que ofrecen las SDN proporciona atributos importantes como una mayor flexibilidad, programación rápida y gestión fácil. Esta solución es un gran aporte a los Data Centers y el Cloud, puesto que con el uso de las SDN se reduciría la cantidad de equipos físicos. En la actualidad las empresas que ofrecen servicios iCloud y data centers observan a las SDN como una solución bastante útil. Un ejemplo de red definida por *software* se muestra en la figura 1-1.

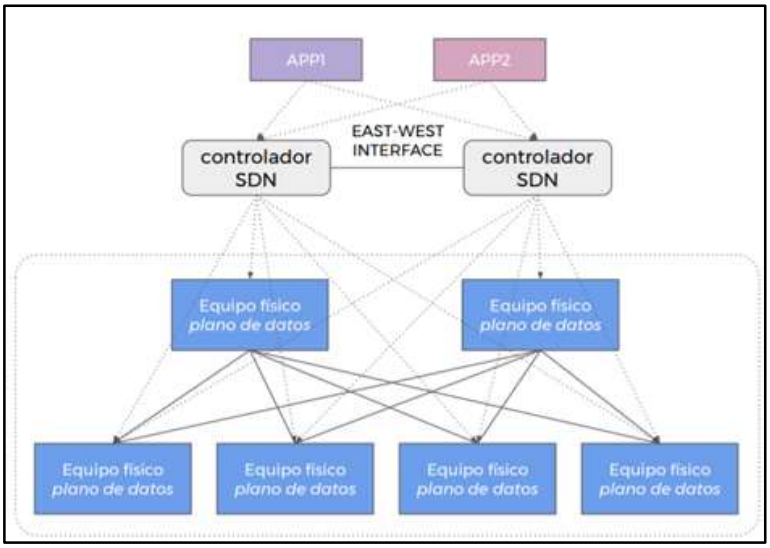


Figura 1-1: Red definida por BCX(RDS)

Fuente: (LAVADO, y otros, 2017)

Existen atributos básicos para la creación de una infraestructura SDN:

- **Automatización:** es necesario un nivel avanzado de automatización con el fin de minimizar gastos operacionales y contribuir a la detección de problemas.
- **Soporte:** es necesario el manejo y control de servicios en la nube, brindando control de direcciones, topología, seguridad y enrutamiento.
- **Flexibilidad:** control total de parametrización de dispositivos a tiempo real.
- **Virtualización de la red:** debe existir la posibilidad de realizar una migración de las redes hacia la nube con todos sus componentes como los Vrouters y Routers.

1.2 Red de área amplia definida por *software* (SD-WAN)

Es importante comprender el concepto de redes definidas por *software* SDN, debido a que representa una arquitectura de utilidad para el control de redes de forma inteligente, con la ayuda de aplicaciones de *software.* Esto contribuye a que la gestión de la red sea integral y constante, independientemente del medio de acceso que posea cada punto remoto.

La solución SD-WAN está orientada al uso eficiente y controlado de las conexiones WAN, a diferencia de las SDN que se emplean sobre centros de datos internos de una organización. SD-WAN usa los conceptos de las SDN y el desacoplamiento de datos en el plano de control, puesto que consideran toda la infraestructura compleja que poseen las empresas en cada sitio remoto. Los equipamientos comunes son routers, controladores de rutas WAN, optimizadores WAN, firewalls, entre otros componentes.

Uno de los principales objetivos de las redes SD-WAN es proporcionar servicios de conectividad a bajo coste. Esto es posible en gran medida al rápido crecimiento que ha tenido el internet en los últimos años y al bajo costo de los servicios en la nube que oferta el mercado.

Las soluciones MPLS han tenido una presencia importante en el ámbito empresarial, porque ofertan redes privadas dedicadas para la interconexión de puntos remotos con un nodo central de forma segura. El inconveniente de este tipo de solución es que se necesita de concentradores muy robustos para que soporten todo el tráfico que se genere en los puntos de la red, lo que implica un alto costo y tiempos de implementación considerables.

Existen muchos servicios basados en la nube que usan las empresas de forma cotidiana, lo que ha producido que el tráfico de datos vaya en aumento. Un tráfico de datos mayor implica un problema razonable para los enlaces MPLS de las empresas, lo que representa una necesidad de equipos más robustos acompañados de un número mayor de filtros y reglas que permitan un control sobre el tráfico de la red.

Las redes SD-WAN ofrecen una solución alternativa que se integra a los costosos enlaces MPLS, además se adaptan al gran volumen de datos que representan los servicios en la nube. Este tipo de redes implican un ahorro sustancial de costos, dado que emplean los canales de banda ancha tradicional.

1.2.1 Ventajas de SD-WAN

Entre ellas están (VARGAS BRAVO, 2020):

- **Mejora del rendimiento:** En SD-WAN es posible realizar configuraciones para priorizar el tráfico critico o importante y los servicios en tiempo real como el protocolo de voz sobre internet (VoIP), para redirigirlo de forma rápida sobre la ruta más eficiente. La atención de las aplicaciones críticas a través de conexiones confiables de alto rendimiento contribuye a la reducción de problemas como la perdida de paquetes y latencia, lo que mejora la productividad.

- **Aumento de seguridad:** Las redes SD-WAN ofrecen seguridad integrada como NGFW, IPS y capacidades de espacio aislado que contribuyen a prevenir la perdida de datos, el tiempo de inactividad y las infracciones regulatorias. Sin embargo, es indispensable seleccionar de forma adecuada la solución SD-WAN, porque no todas las aplicaciones ofrecen la misma protección de seguridad.

- **Disminución de complejidad:** La SD-WAN puede aliviar la carga de datos a la vez que simplifica la infraestructura WAN. Utiliza banda ancha para descargar aplicaciones

comerciales no críticas, automatiza las tareas de monitoreo y administra el tráfico por medio de un controlador centralizado con diseño de interfaz muy sencilla.

- **Habilita el uso de la nube:** Las redes SD-WAN permiten el acceso directo a la nube en las sucursales remotas, eliminando el tráfico de Backhauling (enrutamiento de todo el tráfico de la nube y de las sucursales a través del centro de datos). Esto significa que los trabajadores pueden acceder directamente a las aplicaciones en la nube sin importar su ubicación y sin sobrecargar la red principal con tráfico adicional. Además, mejora el rendimiento de las aplicaciones basadas en la nube, debido que prioriza las aplicaciones críticas para la organización y permite que las sucursales se comuniquen directamente a internet.

- **Reduce costos:** A medida que las organizaciones adoptan una mayor cantidad de aplicaciones basadas en la nube, los datos que se transmiten a través de la WAN aumentan exponencialmente, lo que aumenta los costos operativos. SD-WAN es capaz de reducir los costos porque aprovecha el acceso a internet local, reduciendo una cantidad de tráfico considerable de la red WAN central de la organización.

1.2.2 Arquitectura SD-WAN

SD-WAN se divide en cuatro planos que se presentan en la figura 2-2, y se describen a continuación:

- Plano de orquestación.
- Plano de gestión.
- Plano de control.
- Plano de datos.

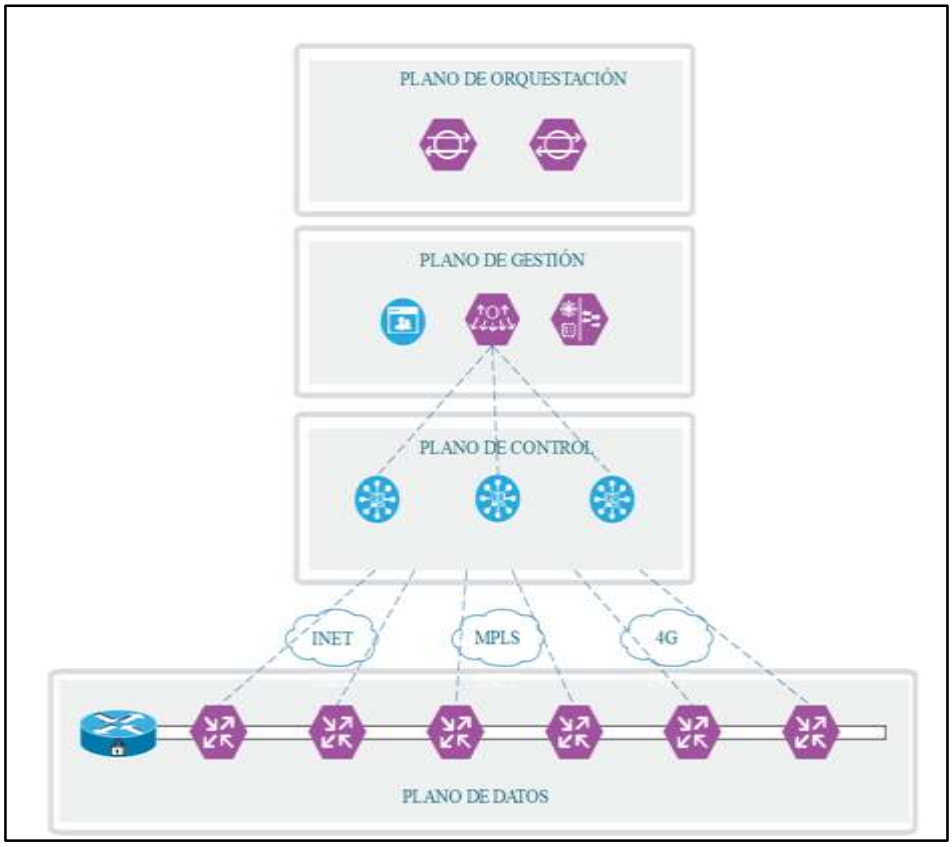


Figura 2-1: Arquitectura SD-WAN

Realizado por: García, Luis, 2022.

1.2.2.1 Plano de orquestación

Se trata de un componente basado en *software* que se encarga de la autentificación inicial de los dispositivos del plano de datos y coordina la conectividad entre el plano de control y el plano de gestión. Además, es prescindible para la comunicación de dispositivos que se encuentra en la NAT y se lo debe fijar con una IP pública.

1.2.2.2 Plano de gestión

Se encarga de administrar la red de forma centralizada, además ofrece una interfaz GUI para configurar, monitorear y mantener los enlaces de la red.

1.2.2.3 Plano de control

Se encarga del control centralizado de la red en base a un *software.* Además, establece conexiones seguras a cada plano de datos y proporciona rutas e información referente a las políticas aplicando el Protocolo de administración de superposición (OMP), mismo que actúa como reflector de ruta. También se encarga de garantizar la conexión segura entre los diversos planos de datos por medio de claves criptográficas.

1.2.2.4 Plano de datos

Constan de dispositivos de *hardware* y *software* que se pueden localizar de forma física o en la nube. Estos se encargan de proporcionar conectividad segura del plano de datos entre los diferentes sitios. Además, se encargan del cifrado, la seguridad, la calidad del servicio (QoS) y los protocolos de enrutamiento como OSPF, BGP, entre otros.

1.2.3 Topología lógica SD-WAN

Consisten en enrutamientos de anuncios para mantener el flujo de datos en toda la red por medio de una segmentación de capa 3 (VRF). Emplea conectividad punto a punto para establecer y mantener conexiones por cada par de protocolos. Además, se establece la encriptación y autentificación juntamente con Políticas de enrutamiento y tráfico de datos (GOOLEY, 2020).

La red de transporte es la encargada de conducir paquetes de un equipo de red a otro, por lo que es necesario conocer la ruta que debe seguir para llegar a los distintos routers. La segmentación de la red de transporte y la red de servicios permite al administrador de red controlar la comunicación entre routers indistintamente de la comunicación entre hosts.

Los routers de borde de la red consideran dos partes para el enrutamiento: el primero se refiere a la red de transporte, mientras que el segundo se refiere al servicio de la red. Para que una conexión se llevó a cabo es necesario que todos los routers de la red aprendan todos los prefijos necesarios. Por lo general el aprendizaje de prefijos se lleva a cabo utilizando IGP /BGP de malla compuesta o a su vez se habilita el enrutamiento en el túnel superpuesto. Por ejemplo, IGP o BGP sobre MPLS o GRE. Existe varias técnicas que permiten eliminar los problemas asociados con la topología full-mesh debido a sus adyacencias de enrutamiento, un ejemplo de ello es el uso de un reflector de ruta para BGP (MONTES, y otros, 2019).

SD-WAN describe un modelo reflector de ruta descentralizado para lograr un enrutamiento inteligente. Por lo que todos los prefijos aprendidos por los routers desde la parte de servicio se notifican en un controlador centralizado para posteriormente reflejarse en otros routers por medio del plano de control de red. Los controladores no realizan el manejo de tráfico de datos, únicamente son involucrados en el proceso de comunicación del plano de control. En la figura 3-2 se presenta el transporte y el enrutamiento.

SD-WAN posibilita la identificación de enlaces desde la parte de transporte de la red y cifra automáticamente el tráfico entre sitios. Las claves de cifrado se comparten mediante una sesión segura del controlador centralizado. Las sesiones seguras se configuran usando RSA e infraestructura de certificados (DSL/TLS tunnel) de forma automática.

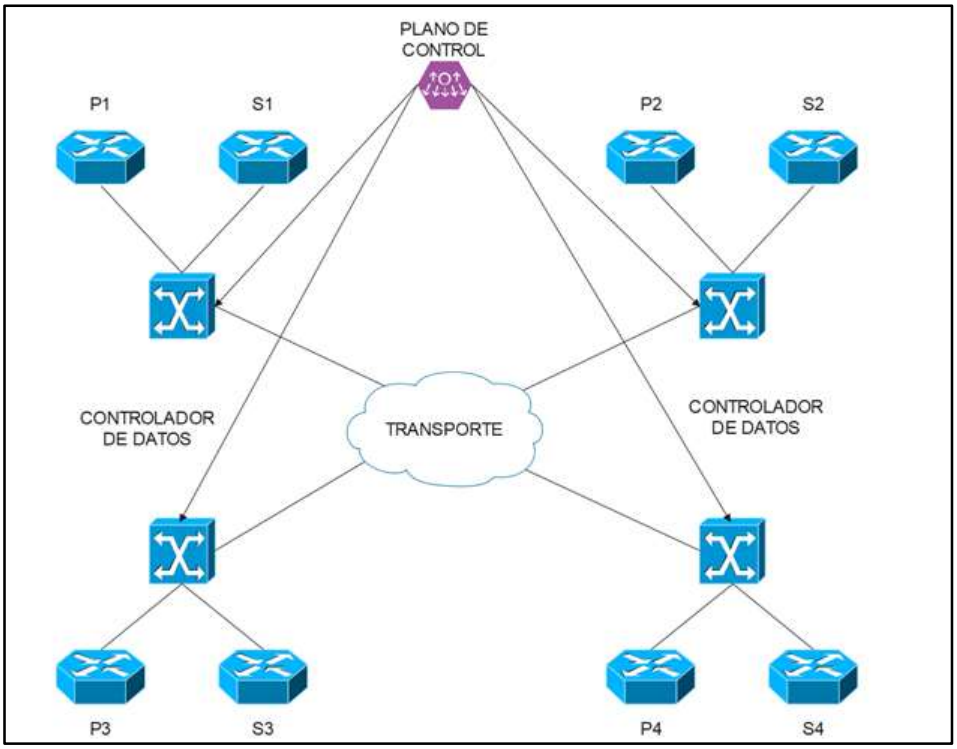


Figura 3-1: Transporte y enrutamiento

Realizado por: García, Luis, 2022.

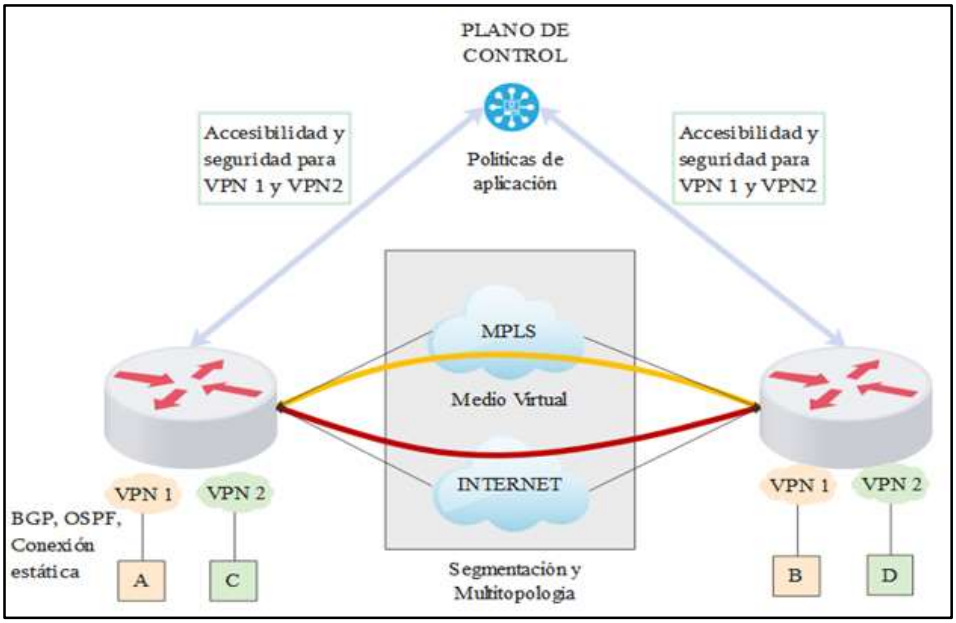


Figura 4-1: Tipos de enlaces

Realizado por: García, Luis, 2022.

La centralización de conectividad permite la administración eficiente de los prefijos de comunicación dentro de la misma VPN, lo que posibilita la asignación de enlaces para llevar a cabo la comunicación y la implementación de políticas de calidad QoS. Todo el procedimiento se enfoca a la mejora de transporte de datos y como consecuencia mejora en la percepción de las aplicaciones del usuario.

Una de las grandes facultades de SD-WAN es que simplifica y centraliza la administración del sistema mediante el Sistema de administración de red (NMS). Este ofrece una interfaz gráfica amigable con el usuario, que permite monitorear, configurar y mantener los enlaces de todos los dispositivos de la red. Por ejemplo, desde el panel de control se puede facilitar el aprovisionamiento de un servicio, es decir que se puede enviar dicho servicio a todos los servidores específicos de la empresa y elementos comunes a la red de una forma muy fácil.

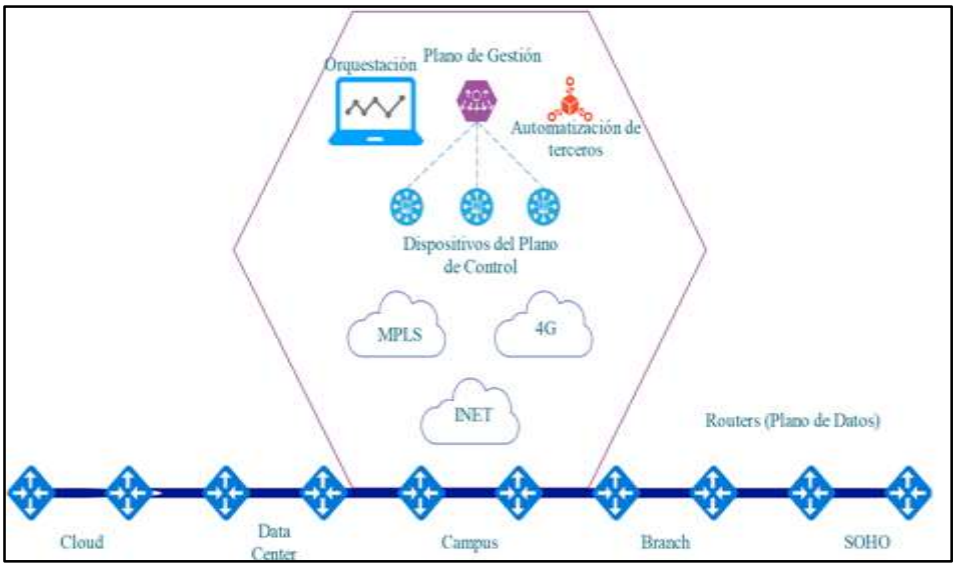


Figura 5-1: Plano de gestión

Realizado por: García, Luis, 2022.

1.2.4 Virtualización de red

La función de superposición de red en SD – WAN, posibilita el tráfico originado a partir de las aplicaciones, sea transportado de manera autónoma sea a través de la capa física o mediante transporte subyacente, lo que permite brindar una superposición autónoma del transporte. Un conjunto de enlaces, lo cuales pueden ser propiedad de varios proveedores, conforma lo que se denomina como WAN virtual, es esto lo que posibilita que las redes SD – WAN, provean de una amplia disponibilidad e incluso de un mejor rendimiento para el caso de aplicaciones. Estas redes además son capaces de incrementar el nivel de uso de los recursos, pero a su vez realizan un proceso de implicación de red, lo que conlleva a que los operadores, tengan facilidades para incorporar nuevos enlaces y aplicación, gracias a la inexistencia de un vínculo estático entre elementos tales como la aplicación en cuestión y el enlace que se usará, a esto se le llama principio de abstracción.

1.2.5 Superposición

Se debe tener en cuenta que la superposición que brinda SD-WAN, se caracteriza por el alto nivel de seguridad y su independencia de transportes subyacentes, esto debido a que los dispositivos

que se desea vincular deben pasar por un proceso de autenticación previo a dicha superposición, en este caso las posibles combinaciones entre los circuitos y los diferentes proveedores, dan paso a una transmisión que estará cifrada de extremo a extremo, lo que le confiere seguridad. En lo que respecta al plano de control, el hecho de estar separado hace posible que tanto la configuración como la gestión de contraseñas se realicen de manera automática en las diferentes sucursales de una empresa. Se debe tomar en consideración que los diseñadores de redes, son capaces de implementar procesos de segmentación, a manera de superposición, sin embargo, esta tendrá la característica ser independiente y a la vez guardará coherencia con respecto a la diversidad de componentes subyacentes (WILEY, 2018).

1.3 Soluciones SD-WAN existentes en el mercado

A continuación, se procede a realizar una revisión de las soluciones de código propietarios de tipo privada, más importantes a nivel mundial.

1.3.1 Soluciones de código propietario (privadas)

A continuación, se procede a realizar una revisión de las soluciones de código propietarios de tipo privada, más importantes a nivel mundial.

1.3.1.1 Fortinet

Esta empresa tiene una gran envergadura, puesto que, posee filiales a nivel mundial, sin embargo, la sede se encuentra en Estados Unidos, su actividad económica, consiste en el desarrollo de *software* y su posterior comercialización, donde además también incluye en su oferta dispositivos y ciertos servicios ciberseguridad, como es el caso de firewall, antivirus o sistemas de detección de intruso. La empresa lleva en funciones poco más de 20 años, siendo referente de desarrollo e innovación en materia de ciberseguridad y su aplicación en redes, constituyendo la mejor alternativa para brindar solución a problemas de seguridad a redes implementadas y patentadas pertenecientes a diferentes industrias (MADDISON, 2020).

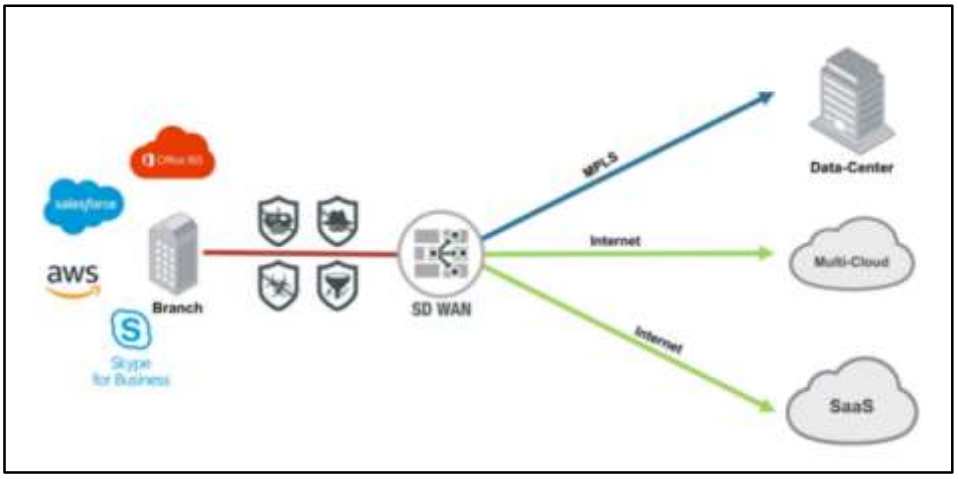


Figura 6-1: Fortinet

Realizado por: García, Luis, 2022.

- **Security Fabric:** Es el lugar en el cual se encuentran alojados los tejidos de seguridad, los cuales, brindan la oportunidad a las empresas para que estas consigan resultados en cuanto a innovación, sin compromiso alguno, esto gracias a que, a la oferta de una plataforma de ciberseguridad, que trae como beneficios, expandir la visibilidad, una integración exitosa y una interrelación operativa entre elementos tales como seguridad, monitoreo y automatización (MADDISON, 2020).

Según cifras de DCI, la empresa desarrolladora de *software* Fortinet, su oferta de soluciones de ciberseguridad ofertadas, cuenta con el mayor número de implementaciones en el año 2021, haciéndose con una participación de por lo menos un tercio de los envíos realizados por todos los cortafuegos.

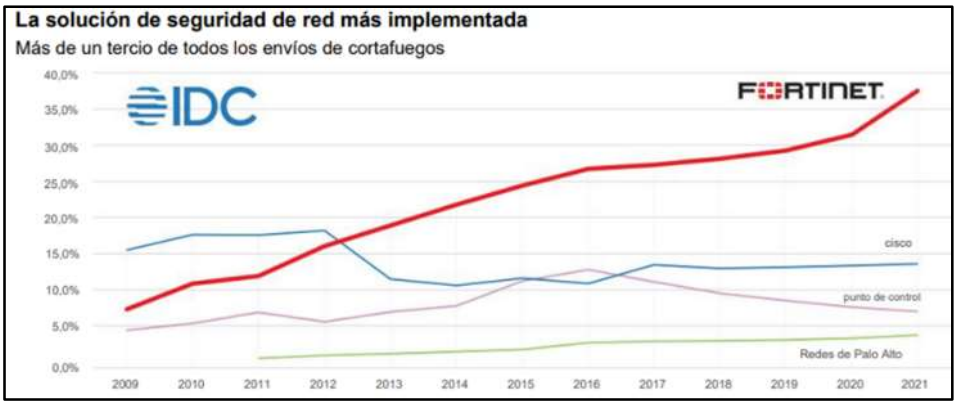


Figura 7-1: Fortinet, primer lugar en soluciones de ciberseguridad

Fuente: (FORTINET, 2022)

La oferta de Fortinet, también incluye dispositivos y *software*, orientados a la prestación de servicios como son el diseño de redes SD – WAN y VoIP, asi como también para la autenticación de dispositivos o aplicaciones. Entre los dispositivos más destacado se pueden identificar

Fortigate, FortiManager y FortiAnalizer, a continuaciones se realizará una revisión de las características esenciales de cada uno de estos:

- **Fortigate:** Provee de una seguridad integral, la cual, incluye funciones con alto nivel de eficacia, en términos de seguridad para las comunicaciones, entre las cuales se enlistan firewall, VPN (IPSEC y SSL), antimalware Anti-Botnet, Anti-DOS, Sistemas de detección/prevención de intrusos, filtrado Web, entre otros, lo nnovedoso de esta es que las funciones antes mencionadas, se integran con algunas añadidas como son Traffic Shaping, balanceo de carga, aceleración y WAN, soporte VoIP, enrutamientos RIP, OSPF y BGP, etc (FORTINET, 2020b).

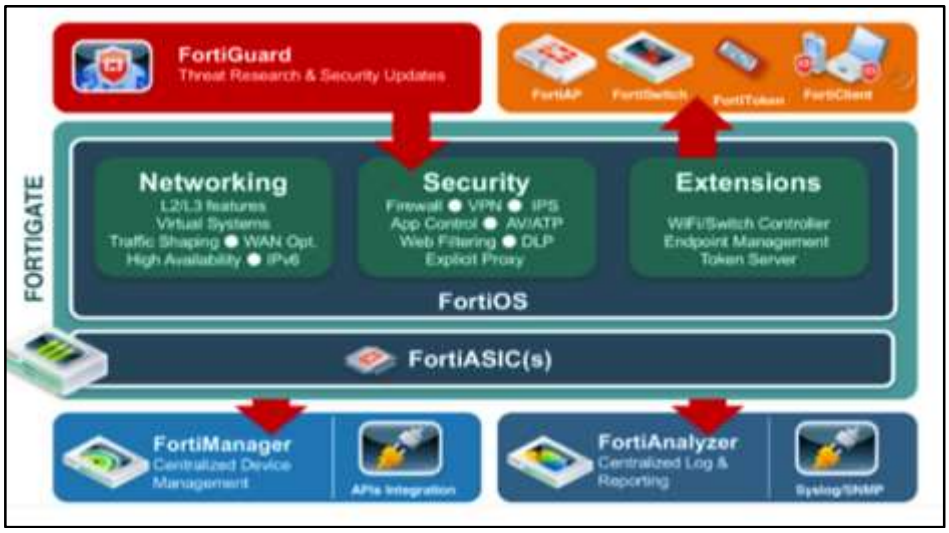


Figura 8-1: Estructura de Fortigate

Fuente: (FORTINET, 2020b)

- **FortiManager:** Su oferta comprende una capacidad recia para la gestión de redes SD – WAN, esto haciendo uso de trabajos automáticos y una simplificación en la gestión de aprovisionamiento, para lo cual, se vale de las políticas comerciales de SD – WAN, las cuales se enfocan en aplicaciones con la finalidad de realizar un ajuste en el direccionamiento del tráfico, mismo que se realiza dependiendo de las metas del Service Level Agreement (SLA), con respecto a rendimiento de cada proveedor dentro de las redes WAN. En este caso el panel de control de las redes SD – WAN, permite que los administradores, tengan control sobre el rendimiento de las aplicaciones, además de poder emplear el ancho de banda por enlace WAN (FORTINET, 2020c).

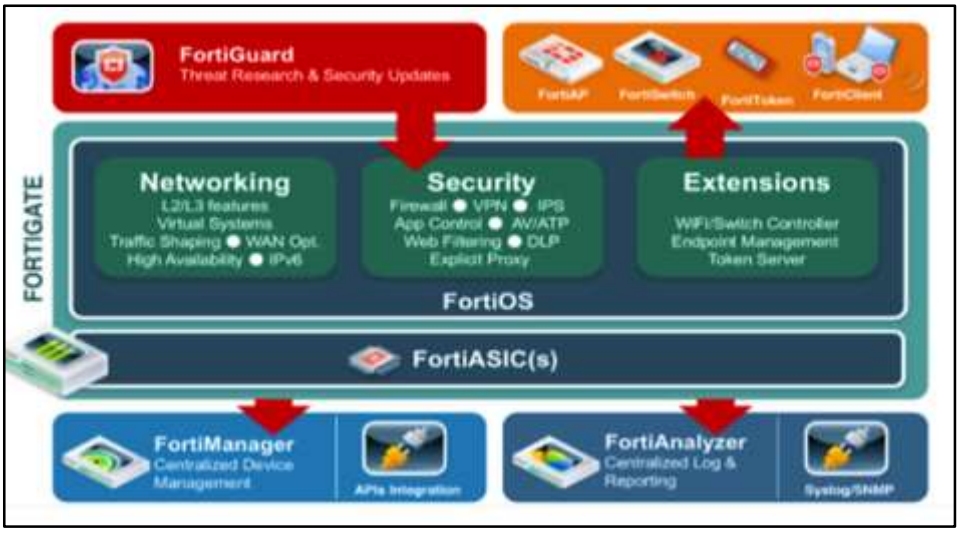


Figura 9-1: Tablero de FortiManager

Fuente: (FORTINET, 2020c)

- **FortiAnalyzer:** Esta puede ser integrada a FortiManager, con la finalidad de poder conseguir una visión analítica perfeccionada, así como también generar informas sobre el rendimiento de las redes SD – WAN. Es considera a nivel mundial como la plataforma más importante dentro de lo que compete a la gestión de registros, diagnósticos y generación de informes, esto gracias a que permite que las empresas organicen, automaticen y formulen respuestas desde un panel para brindar una simplificación de seguridades, además de una identificación automática y la ejecución de medidas correctivas que reducen el riesgo, esto hace que sea posible contar con la visibilidad necesaria para apreciar los estragos ocasionados en la superficie que esta siendo atacada. La integración con Security Fabri, cualidades tales como el detector de amenazas, el diagnóstico de seguridad, la conciencia y control de la postura de seguridad de extremo a extremo, coadyuban a los equipos para que estos puedan realizar la identificación y eliminación de cualquier amenaza de manera oportuna, evitando que estas ocasionen algún daño (FORTINET, 2020d).

Figura 10-1: Tablero de control de FortiAnalyzer

Fuente: (FORTINET, 2020d)

1.3.1.2 VMware

Esta solución ayuda a que los sitios puedan realizar de manera rápida la implementación de accesos dentro del nivel empresarial para aplicaciones heredadas y aplicaciones en la nube, haciendo uso de redes privadas o la banda ancha de internet. La WAN que es definida por *Software* misma que es proporcionada mediante la nube, permite dar garantías a las organizaciones sobre el rendimiento de las aplicaciones conectadas de manera directa con la red, esto a partir de internet y las redes WAN hibridas, sin contar una implementación simplificada y la reducción de costos (VMWARE, 2021a).

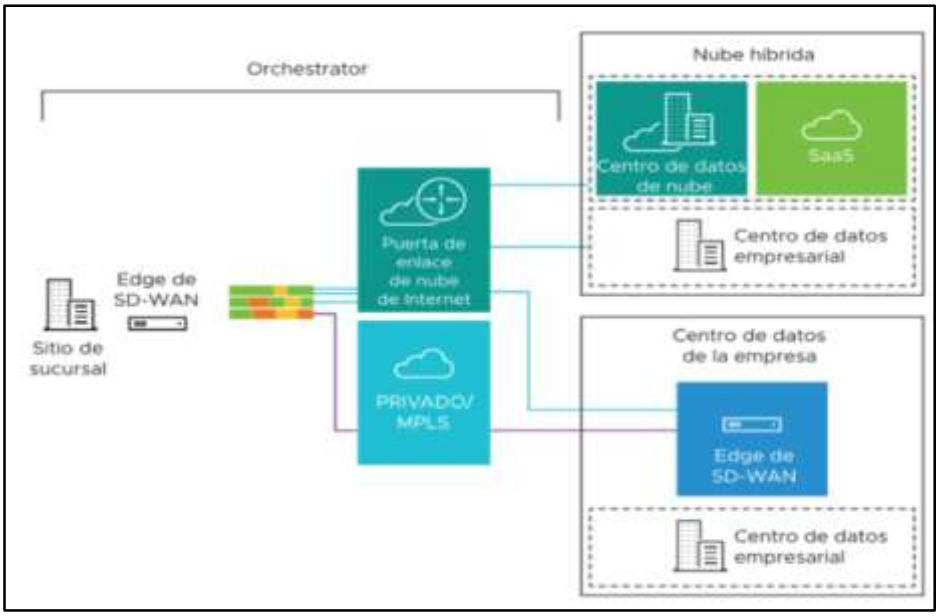


Figura 11-1: VMware SD-WAN componentes

Fuente: (VMWARE, 2021b)

Entre los componentes de la solución están:

- **VMware SD-WAN Edge:** La instancia Edge limitada, libre de intervenciones de TI, es suministrada desde la nube con la intención de brindar seguridad en las conexiones y una optimización tanto para las aplicaciones como para los servicios que experimentaron procesos de virtualización. Las SD-WAN Edge, son dispositivo que no se experimentan intervención de tipo empresarial o alguno *software* virtual, lo que permite garantizar una conexión segura para aplicaciones indiferentemente de su naturaleza, sea esta privada, pública o incluso hibrida, este beneficio se extiende a recursos informáticos y servicios que pasaron por una virtualización. Otros beneficios propios de esta instancia son una profundidad considerable en cuanto al reconocimiento de aplicaciones, controles tanto por paquetes como por aplicaciones, indicadores de rendimiento QoS de extremo a extremo, los servicios VNF. La instalación de instancias Edge, supone una alta disponibilidad de HA. Es preciso mencionar

que el campo de aplicación incluye derivaciones, grandes sitios y centros de datos, el resto de infraestructuras de red son brindadas a petición en la nube (VMWARE, 2021b).

- **VMware SD-WAN Gateways:** Esta radica en las puertas de enlaces cuya implementación se realiza en centros de datos en la nube y puntos de presencia de nivel superior a nivel mundial, lo que posibilita la prestación de servicios SD – WAN en los umbrales SaaS y IaaS, además de aquellos servicios conectados en la nube y accesibilidad a redes privadas. La implementación de puertas de enlace virtual y de diversos tenantes, se da por parte de socios del proveedor de servicios en la nube y de tránsito de VMware SD-WAN. Estas puertas ofertan redes a petición, las cuales tienen la característica de ser escalable y redundante cuando se trata de rutas de acceso con cierto nivel de optimización con destino a la nube y de igual manera para aplicaciones sin instalación (VMWARE, 2021b).

1.3.1.3 Versa Networks

Esta es considerada como líder dentro de la industria SD – WAN, cuenta con una amplia cartera de servicios, dentro de los cuales se enlistan la dirección de paquetes con velocidades inferiores a un segundo los cuales son transportados mediante múltiples redes WAN, una reducida perdida de paquetes, replicación de paquetes, además de que evita enlaces de bajo rendimiento. Adicionalmente se tiene que estas ofrecen superposiciones con y sin cifrado mediante MPLS, GRE o VXLAN, controladores de SD-WAN, soporte para los circuitos WAN, topología de malla completa y de radio concentrador, Superposicines IPSec dinámicas acceso directo a Internet y un matrimonio perfecto de proxy HTTP/S.Versa posee una diferenciación con respecto a otras tecnologías SD – WAN, la cual radica en la implementación de capacidades alcanzar la perfección en arquitecturas SASE, lo cual, permite mayor visibilidad del tráfico de red entre usuarios, aplicaciones y dispositivos, sin importar su ubicación (SPRINT NETWORKS, 2022).

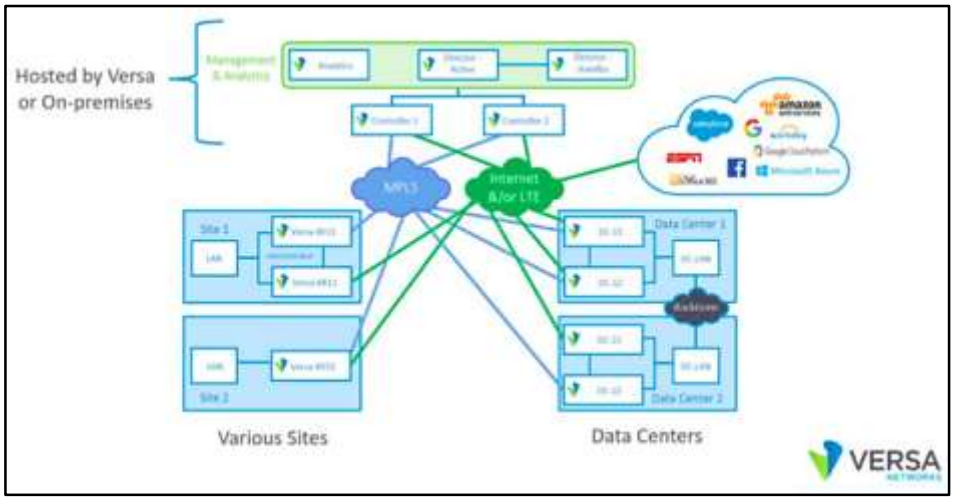


Figura 12-1: Red SD-WAN segura con Versa Networks

Fuente: (SPRINT NETWORKS, 2022)

Entre sus componentes tenemos:

- **Versa Director:** Es la versión virtualizada de Versa Network, esta plataforma digital permite la creación de servicios, donde se consigue la simplificación en el diseño, automatización y la prestación de servicios mediante Versa WAN con instancia Edge y FlexVNF. En lo que compete a Versa Director, se tiene que este es un proveedor de capacidades básicas para la gestión, supervisión y orquestación requeridas para ofertar servicios de seguridad y arquitecturas Secure Cloud IP. Esta plataforma brinda la posibilidad de administrar a través de un panel único para conectividad y servicios, este se tiene la capacidad de adaptarse a miles de clientes finales o empresas, mediante la jerarquización administrativa de funciones y la capacidad de albergar múltiples inquilinos (VERSA NETWORKS, 2022a).

Figura 13-1: Monitoreo del tablero de Versa Director

Fuente: (VERSA NETWORKS, 2022a)

- **Versa Analytics:** Este componente fue creado como elemento para Versa Cloud IP Plataform, cuya función es los análisis centrados en usos que cubren SD-Routing, SD-WAN, SD-Security y SD Branch. Esta es una solución de big data en tiempo casi real, la cual, permite la visibilidad y control línea de base, correlación, predicción y bucle de retroalimentación en las soluciones de *software* Versa. Esta cuenta con una empresa cuya integración habilita a un solo cluster como proveedor de servicios que atenderá a centenares de clientes, lo que brinda una implementación con alto nivel de flexibilidad e incluso la posibilidad de obtener economías a escala. La integración con Versa Director es estrecha y posibilita el desarrollo de controles de acceso basados en roles. Cabe mencionar que es complemente operativo y permite la admisión de protocolos y formatos de registros como es el caso de Syslog e IPFIX, lo que desemboca en una compatibilidad con sistemas SIEM, de monitoreos e informes, mediante el uso de API Rest, se consigue que Versa Analytics, adquiera las características de extensible y flexible (VERSA NETWORKS, 2022b).

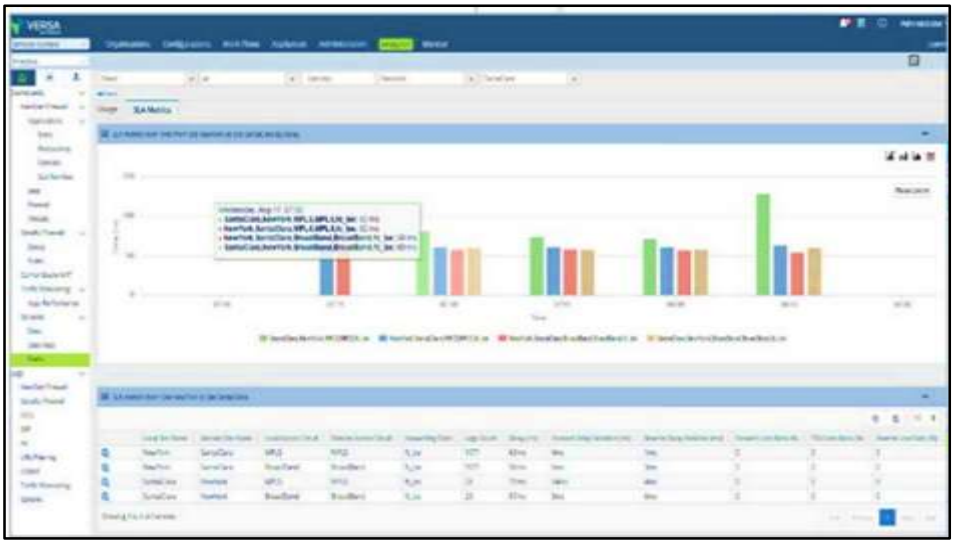


Figura 14-1: Panel de métricas de Versa Analytics SLA

Fuente: (VERSA NETWORKS, 2022b)

- **Versa Operating System (VOS):** Posee una alta flexibilidad que permite a empresas y proveedores realizar la implementación de soluciones definidas a traves de *software*, dentro de las cuales se incluyen Secure SDWAN y Secure Access Service Edge (SASE), para su uso en sucursales, nube o central de datos, es preciso mencionar esto es independientemente del espacio en el cual sea aplicado VOS, mismo que es funciona de manera simultánea Versa Director, para proveyendo visibilidad, línea de base, correlación y análisis predictivo para eventos de red, uso de aplicaciones y seguridad. Con Versa Analytics, toda la seguridad de la red, el uso de aplicaciones, los informes de exportación y los registros se analizan, filtran y se pueden buscar eventos fácilmente para obtener información procesable (VERSA NETWORKS, 2022c).

Figura 15-1: Panel de métricas de Versa Vos

Fuente: (VERSA NETWORKS, 2022c)

1.3.1.4 Cisco

Esta es una solución WAN, que se caracteriza por proveer a sus usuarios que en este caso son empresas de una conexión seguras a sus aplicaciones. Al igual que las antes mencionados, también permiten la superposición, la cual es ejecutada a partir del transporte de red estándar, dentro de los cuales se incluyen MPLS, el ancho de banda e internet, en la oferta tanto de aplicaciones como de servicios. La superposición de las redes hace que las redes de las empresas se extiendan a entorno de infraestructuras como IaaS y los multinubes, que otorgan mayor rapidez en el cambio de la nube (GRUPO SIRT, 2019).

Cisco Viptela, el control de la red es desempeñado por VSmart, mismo que está ubicado en la nube, donde vEdges son CPE y deben contar con conexión de vBonf y vSmart, para poder contar con una máxima operatividad, se debe tener cuenta que el vEdge, es muy común en las instalaciones de los clientes, donde se lo puede encontrar de manera física o virtual, no obstante, también pueden ser instalados en nubes, sean estas públicas o privadas

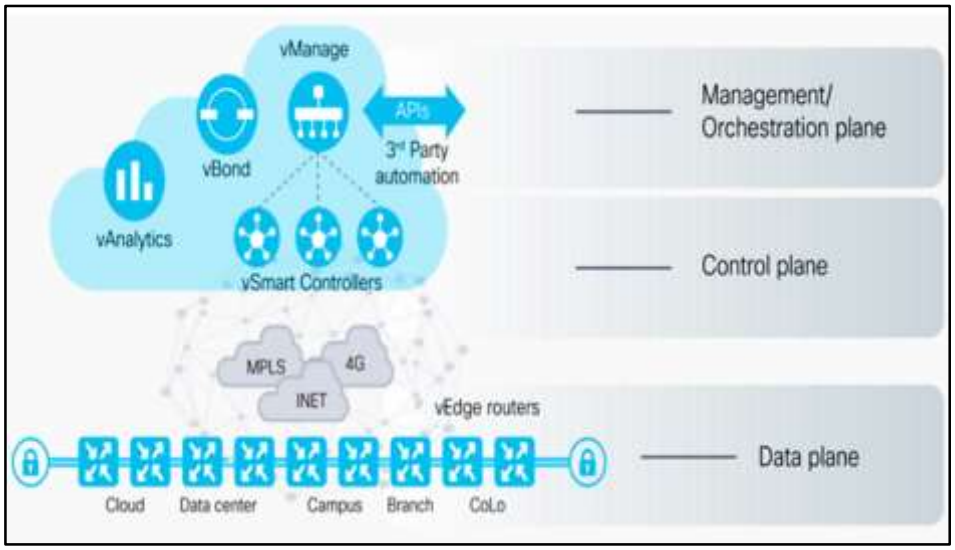


Figura 16-1: Arquitectura de red SD-WAN Cisco

Fuente: (OZGA, 2018)

La vManage, es una herramienta empleada por administradores de redes para brindar claridad a las reglas dentro de lo que compete a las comunicaciones WAN, además de que desde interfaces graficas podrán realizar la administración de políticas. Los beneficios que trae vManage para los administradores, incluyen las facilidades para diseñar topologías a partir de las necesidades, como pueden ser sucursales en las cuales se apliquen líneas MPLS/internet sean estas simples o dobles, topologías de concentrador y radio o conectividad de radio a radio (OZGA, 2018).

A continuación, se presentan los cuatro elementos que conforman CISCO:

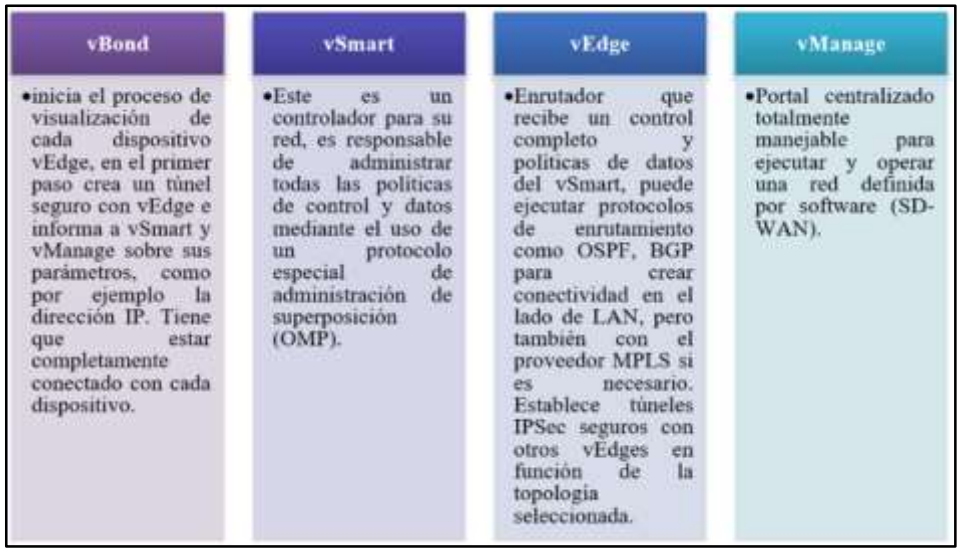


Figura 17-1: Elementos de Cisco

Fuente: (OZGA, 2018)

Es preciso mencionar la oferta de Cisco, incluye una extensa cantidad de plataformas e incluso de dispositivos compatibles con las redes SD – WAN indiferentemente de lugar donde se aplique, lo que, la convierten en la plataforma con mayor nivel de innovación en lo que respecta a redes con conexión en la nube que cuenta con soporte multicapa, cuyo cifrado se ve acelerado por *hardware* y una robustecida flexibilidad puertos con la cual brindan conexión en la nube. La creación de redes SD – WAN a través de Cisco, suelen ser más completas y permiten escalar todo el negocio hacia entornos digitales híbridos (SCC, 2022).

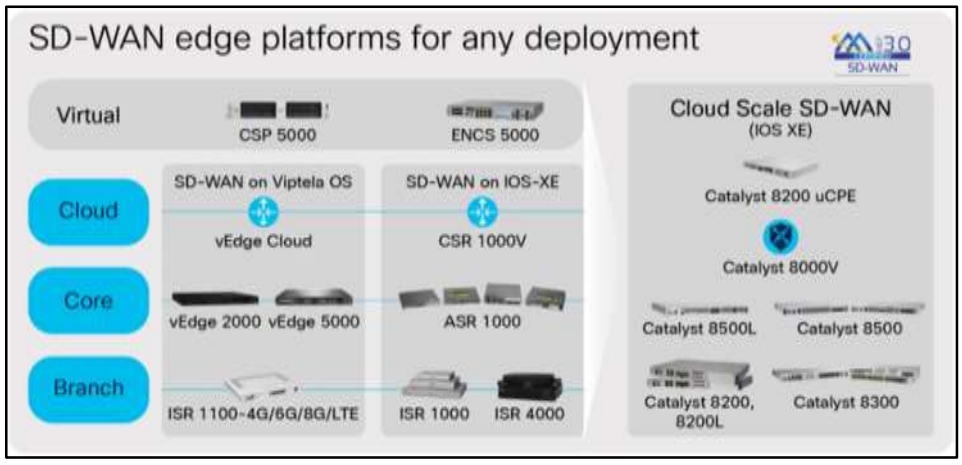


Figura 18-1: Capacidades de la plataforma Cisco SD-WAN

Fuente: (SCC, 2022)

1.3.2 Soluciones de código abierto Open Source

El impacto de los códigos abiertos en los sistemas operativos fue considerable, lo que hizo que durante los últimos años las TI, experimentarán una transformación radical con lo cual empezaron a admitir redes, partiendo del hecho de que las redes se transformen en todo *software*, es lógico

que sean incorporadas a la comunidad de código abierto. En la actualidad las empresas incurren en gastos de al menos $ 4 millones USD, por concepto de *software* y los implementos necesarios para el enrutamiento. En este sentido el *hardware* de propietarios es reemplazado por el *hardware* de uso general, a través del cual se realiza la ejecución del *software* de enrutamiento virtualizado, que constituyen el punto de partida para bloqueo de proveedor y brindar una escala horizontal rentable. El segundo paso es descomponer el *software* mediante la integración de tecnología de terceros en el núcleo del sistema, no está demás mencionar que estas tecnologías son consideradas como la segunda ola de lo que se conoce SD- WAN (CISION, 2019).

Las soluciones de código abierto u Open Source se comprenden como un modelo de desarrollo de *software* de manera descentralizada que promueve la contribución altruista. El objetivo principal de este tipo de contribución es ofrecer el acceso libre al código fuente, planos y documentación relevante al *software.*

1.3.3 SD-WAN código abierto

En su mayoría las empresas proveedoras de servicios de SD – WAN emplean elementos de código abierto aplicados a sus productos, que generalmente, traen intrínsecos codigos propietarios, los cuales fueron desarrollados en colaboración con bloques de construcción de terceros sublicenciados, para asi dar origen a los productos SD – WAN con código cerrado. Existen proveedores de SD – WAN, los cuales con la finalidad de efectuar funciones específicas ofrecen API, con la finalidad de proveer y configurar dispositivos de borde.

La SD – WAN de código abierto, ofrece el código con la finalidad de estar disponible dentro de repositorios públicos como GitHub o GitLab, mientras que, por otro lado, se tiene la licencia para usar el código, lo más común es que las empresas ofertantes de productos con código abierto, cobren por tales servicios complementarios.

1.3.3.1 Productos SD-WAN abiertos

Consisten en la agrupación de tecnologías y características dentro de un conglomerado de *software*, estas arquitecturas inhiben la flexibilidad para la incorporación de tecnologías de otros proveedores, haciendo necesario incorporar tecnología de un solo proveedor (FLEXIWAN, 2020).

Figura 19-1: Principales proyectos abiertos en telecomunicaciones

Fuente: (FLEXIWAN, 2020)

1.3.4 Open Daylight (ODL)

Es una plataforma modular abierta que sirve para automatizar la gestión de redes de cualquier magnitud. El proyecto Open Daylinght surge como iniciativa del movimiento SDN que se enfoca a la programación de redes. Además, es parte del proyecto Linux Fundation Networking, que posee un enfoque global, de carácter colaborativo y abierto hacia organizaciones. En la actualidad se integra con más de 35 soluciones para diversos servicios.

1.3.4.1 Arquitectura de ODL

La plataforma consta de un core denominado MD-SAL (Model Driven Service Abstraction Layer). En ODL todos las aplicaciones y dispositivos se representan como modelos, sobre los cuales las interacciones son procesadas por la capa de abstracción SAL.

La capa SAL es el eje central de la arquitectura puesto que permite la abstracción absoluta del comportamiento de los equipos de red y de los diversos servicios de la plataforma, cuando se accede mediante aplicaciones. Además, se trata de un mecanismo que sirve para el intercambio de datos, así como para la adaptación de modelos YANG que describen los dispositivos de red y aplicaciones. Los modelos poseen descripciones de los dispositivos y de las aplicaciones lo cual permite que exista una comunicación entre ellos sin necesidad de conocer detalles sobre el resto de los dispositivos.

La capa central SAL posee diferentes roles:

- Implementación de API y provisión de datos.
- Consumidor de API y consumo de datos.

En la capa SAL se ubica la interfaz northbound, misma que sirve para que las aplicaciones se conecten a ella. También se encuentra la interfaz southbound que permite la comunicación de los dispositivos de red.

En conclusión, la capa central SAL empareja a consumidores y productores de los almacenes de datos para hacer posible el intercambio de información.

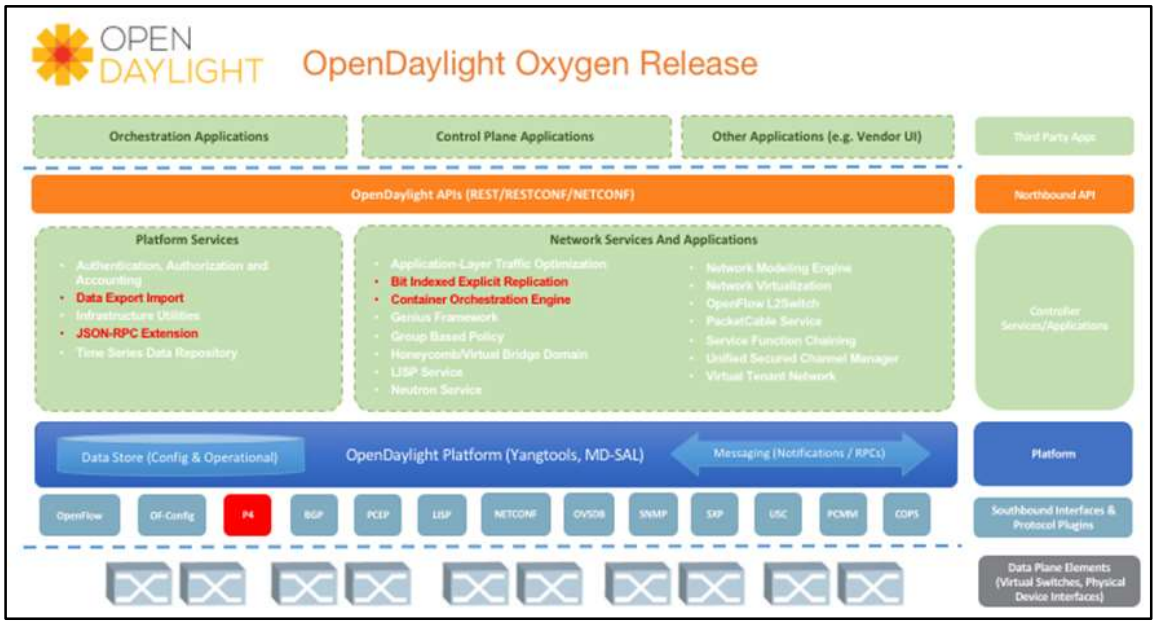


Figura 20-1: Arquitectura Open Daylight

Fuente: (PROGRAMADOR CLIC, 2020)

1.3.4.2 Multiprotocolo

El diseño de la plataforma ODL es modular, lo que permite a los usuarios crear un controlador SDN que se ajuste perfectamente a sus necesidades. Además, permite hacer uso de servicios creados por terceros y si es necesario modificarlos en función de las necesidades de la organización. Una de las grandes ventajas es que soporta una gran cantidad de protocolos Southbonud como OpenFlow, BGP, NETCONF, OVSDN, entre otros.

ODL al ser de código abierto necesita un sistema que aislé cada característica para trabajarlas por separado, de esta forma se evita una interferencia entre funcionalidades. La separación de características es posible con el uso de OSGi y Maven pues permite construir características Karaf y sus respectivas interacciones.

1.3.4.3 P3P

La comunidad creadora de ODL se esfuerza mucho para mejorar todas las áreas de seguridad, rendimiento, estabilidad y escalabilidad. Cuando surge alguna vulnerabilidad o error en la plataforma de ODL la comunidad tras ella esta alerta para corregirla lo más pronto posible, convirtiéndose en un punto a favor de la solución de código abierto.

1.3.5 ONF CORD

Se trata de un proyecto de Open Networking Fundation que integra varias soluciones. La propuesta de este proyecto es virtualizar toda la infraestructura de la red que se despliega en áreas locales haciendo uso de equipos de propósito general, a los que le denomina POD.

CORD describe las siguientes características:

- Creación de redes virtuales bajo demanda Zero touch.
- QoS para el tráfico empresarial y SLAS robustos.
- Emplea una pila de *software* que permite la innovación de servicios.
- Simplicidad en los equipos de clientes y mantenimiento sencillo

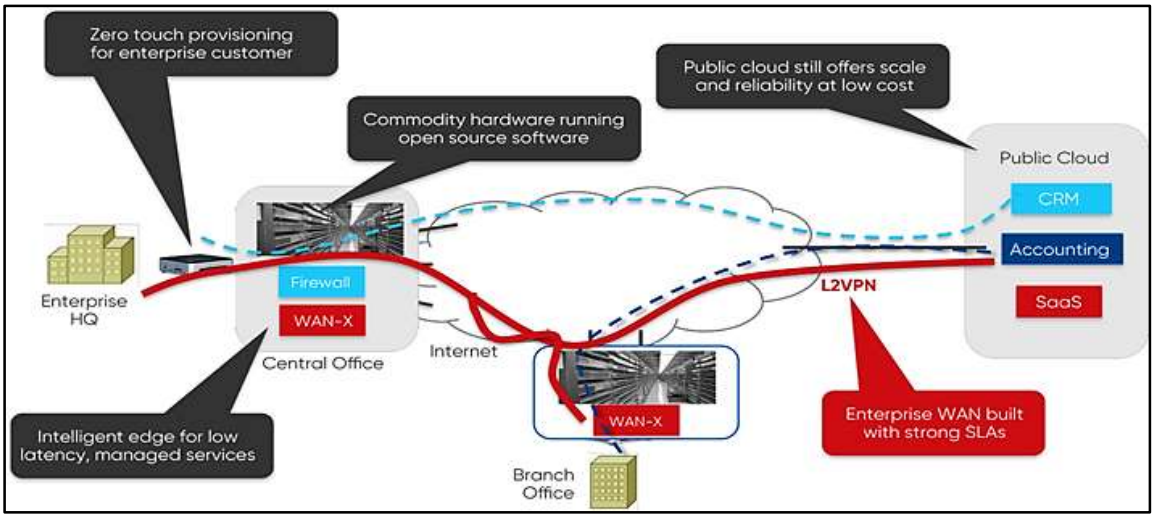


Figura 21-1: Red de datos CORD

Fuente: (SPADARO, 2012)

1.3.5.1 Arquitectura CORD

La plataforma CORD consta de tres elementos principales:

- XOS
- ONOS
- OpenStacks

En donde los dos últimos se instalan en POD.

- **XOS:** se describe como un entorno que admite la composición de servicios relacionados con las funciones de red y aplicaciones que se extienden sobre ONOS y OpenStacks. La función de XOS es actuar como orquestador NFV, de tal forma que gestiona el ciclo de vida de los servicios, aplicaciones y funciones de red.
- **ONOS:** se trata de un controlador SDN que administra los conmutadores POD con el fin de crear redes virtuales. Sobre ONOS se virtualizan las funciones de red como el NAT, el routing, entre otras.
- **OpenStacks:** es un sistema operativo cloud diseñado para controlar grandes centros de datos en base al modelo de Infraestructura como servicio (IaaS). Se encarga de proporcionar las redes y máquinas virtuales para implementar los servicios que proporciona CORD, como las VNF.

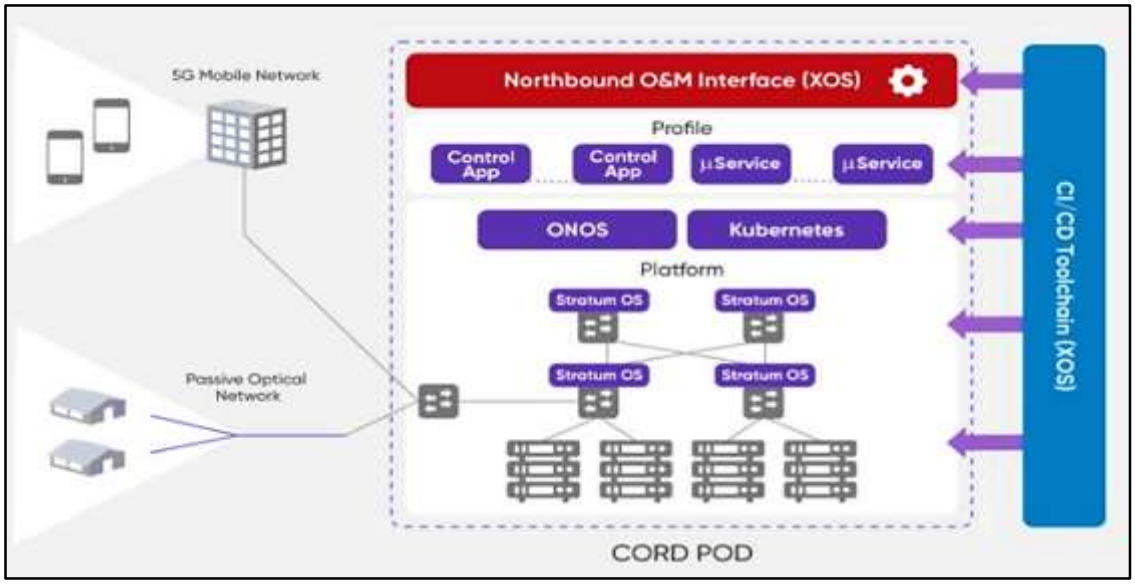


Figura 22-1: Arquitectura CORD

Fuente: (ONF CORD, 2020)

1.3.6 FlexiWAN

Se desarrollo con la idea de proporcionar una solución Open Source de SD-WAN 2.0, con una arquitectura de código abierto. FlexiWAN adopta dentro de su arquitectura diferentes soluciones de código abierto, entre ellas se incluyen Vrouters, orquestación, automatización y administración con el fin de lograr una funcionalidad SD-WAN.

El principal objetivo de la solución FlexiWan es democratizar el mercado SD-WAN, para reducir de forma sustancial las barreras de entrada para que las empresas ofrezcan sus servicios.

1.3.6.1 Arquitectura FlexiWAN

Consta de dos dispositivos:

- **FlexiEdge:** es el nodo SD-WAN que se despliega en diferentes ubicaciones.
- **FlexiManage:** es el sistema central de administración, en donde se conecta mediante una API a FlexiEdge para realizar tareas de administración y orquestación.

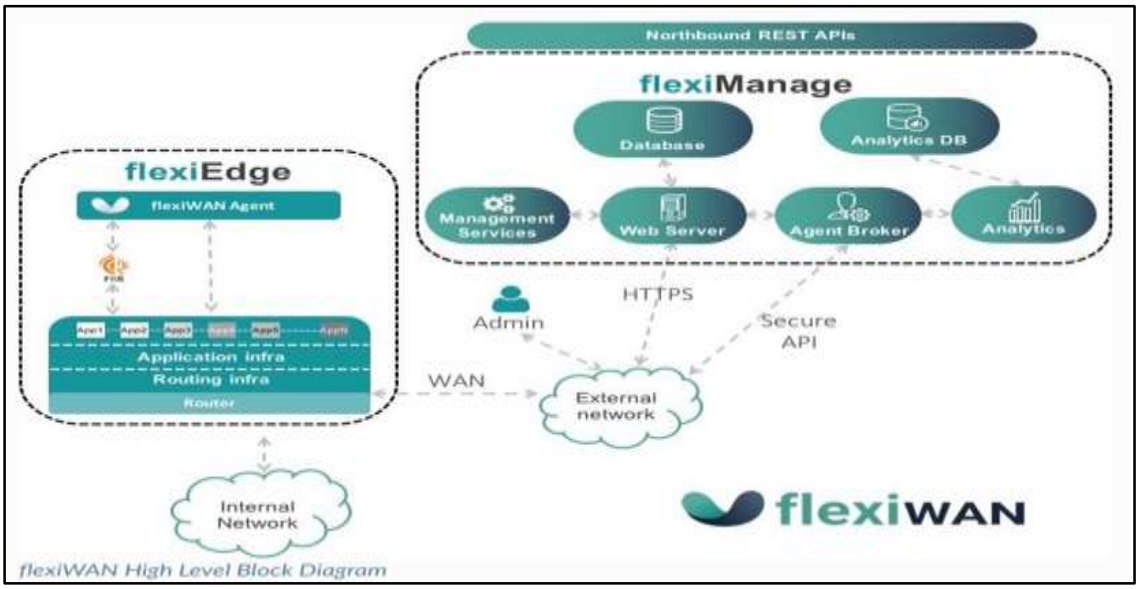


Figura 23-1: Arquitectura FlexiWAN

Fuente: (FLEXIWAN, 2020)

FlexiEdge consta de tres componentes clave:

- Infraestructura de router: posee una versión modificada de FD io Vector Packet Processor (VRRP).
- Plano de control de routing: Free Range Routing (FRR).
- FlexiWan Agent: es el componente de *software* que se encarga de la comunicación a través de API segura de FlexiManage y FlexiEdge.

FlexiAgent se conecta con FlexiManage por medio de un web socket bidireccional para la configuración y estadísticas. A continuación, se presentan las características de FlexiAgent:

- Comandos GET JSON simplificados.
- Orquesta la secuencia de ejecución entre varios elementos.
- Mantiene el orden de configuración.
- Proporciona comandos de consola para la solución de problemas.
- Procesamiento de transaccione y posibilidad de restablecimiento en caso de falla.
- Monitorización de los componentes posibilidad de restablecimiento en caso de fallos.

- Ofrece una estructura JSON para la configuración.
- APIs individuales ofrecidas por Linux.
- Posibilidad de configurar el almacenamiento del tipo clave-valor.

FlexiManage ejecuta un servidor de red para la administración de esta. Por medio de su portal un administrador puede gestionar todos los dispositivos que componen la red. FlexiManage es el encargado de la comunicación de todos los dispositivos flexiEdge que componen la red. También se encarga de recopilar datos estadísticos de los dispositivos flexiEdge, para posteriormente procesarlos y entregar un informe al administrador.

FlexiWan es un *software* que está en desarrollo a comparación de lo que se pretende presentar como producto final, sin embargo, las versiones actuales disponen de las características funcionales suficientes para su despliegue. La solución ofrece multi-Wan y multi-Lan, pero a futuro pretende ofrecer funciones de routing basado en políticas y otras funcionalidades.

1.3.7 ZeroTier

Es un programa de administración de red distribuida construido sobre una red global peer-to-peer cifrada y segura. Proporciona las mismas funciones de virtualización y administración de red avanzadas que los conmutadores SDN empresariales, pero abarca redes de área local y amplia. Además, puede conectarse a casi cualquier tipo de aplicación o dispositivo.

1.3.7.1 Hipervisor de red

El programa de administración de red ZeroTier es un motor de virtualización de red independiente que implementa una capa de virtualización Ethernet similar a VXLAN sobre una red global peer-to-peer encriptada.

El protocolo ZeroTier es un protocolo original, aunque sus aspectos son similares a VXLAN e IPSec. En lo que respecta a OSI, tiene dos capas conceptualmente separadas, pero estrechamente acopladas: VL1 y VL2. VL1 es la capa básica de transmisión punto a punto, o "cable virtual", mientras que VL2 es la capa de Ethernet simulada que proporciona un medio de comunicación familiar para sistemas operativos y aplicaciones.

1.3.7.2 ZeroTier Peer to Peer

Los centros de datos globales necesitan de grandes cantidades de cables a nivel global. En la red convencional L1 (capa 1 de modelo OSI), se refiere al cable CAT5 / CAT6 real o al canal inalámbrico en el que se transmiten los datos y al chip transceptor físico para la modulación y demodulación. VL1 es una red peer-to-peer que utiliza cifrado, autenticación y una gran cantidad

de habilidades de red para crear de forma dinámica enlaces virtuales según sea necesario para lograr el mismo propósito (ZEROTIER, 2020).

1.4 Topología de red

VL1 está diseñado para ser configurada desde cero. Los usuarios pueden iniciar un nuevo nodo ZeroTier sin escribir archivos de configuración ni proporcionar las direcciones IP de otros nodos, también está diseñado para ser rápida. Por ejemplo, dos dispositivos ubicados en áreas geográficas distantes en el mundo deben poder ubicarse y comunicarse casi de inmediato.

VL1 se organiza como DNS, en la base de la red existe una colección de servidores raíz permanentes, que son similares a los servidores raíz DNS. La raíz ejecuta el mismo *software* que un punto final normal, pero la raíz está ubicada en una ubicación rápida y estable en la red que posee una definición mundial. La definición del mundo tiene dos formas: planetas y uno o más satélites. El protocolo incluye un mecanismo de seguridad, si la dirección IP o la dirección ZeroTier del servidor raíz cambia, el mecanismo puede actualizar la definición del mundo en banda.

Los servidores a nivel mundial son operados por ZeroTier, Inc. como un servicio gratuito. Actualmente, hay doce servidores raíz organizados en dos grupos de seis miembros, que se distribuyen en los principales continentes y varios proveedores de red. La latencia de red es menos de 100 milisegundos en casi todo el mundo.

Un nodo se puede encontrar circundante a cualquier nodo central. Los usuarios pueden crear ventanas para reducir la dependencia de la infraestructura de ZeroTier, Inc. o juntar servidores raíz para mejorar el rendimiento. Para SDN locales, el clúster de servidores raíz puede estar ubicado en un edificio o centro de datos, de modo que, si se desconecta la conexión a Internet, ZeroTier puede continuar funcionando normalmente.

Los nodos comienzan sin un vínculo directo entre sí, solo aguas arriba de la raíz. Cada par en VL1 tiene una dirección ZeroTier de 40 dígitos única a nivel mundial (10 dígitos hexadecimales), pero a diferencia de las direcciones IP son identificadores de contraseña opacos y no codifican ninguna información de enrutamiento. Para comunicarse con los pares, los paquetes de datos se envían primero por la red, a medida que estos paquetes de datos atraviesan la red, desencadenan la creación oportunista de enlaces directos en el camino (ZEROTIER, 2020).

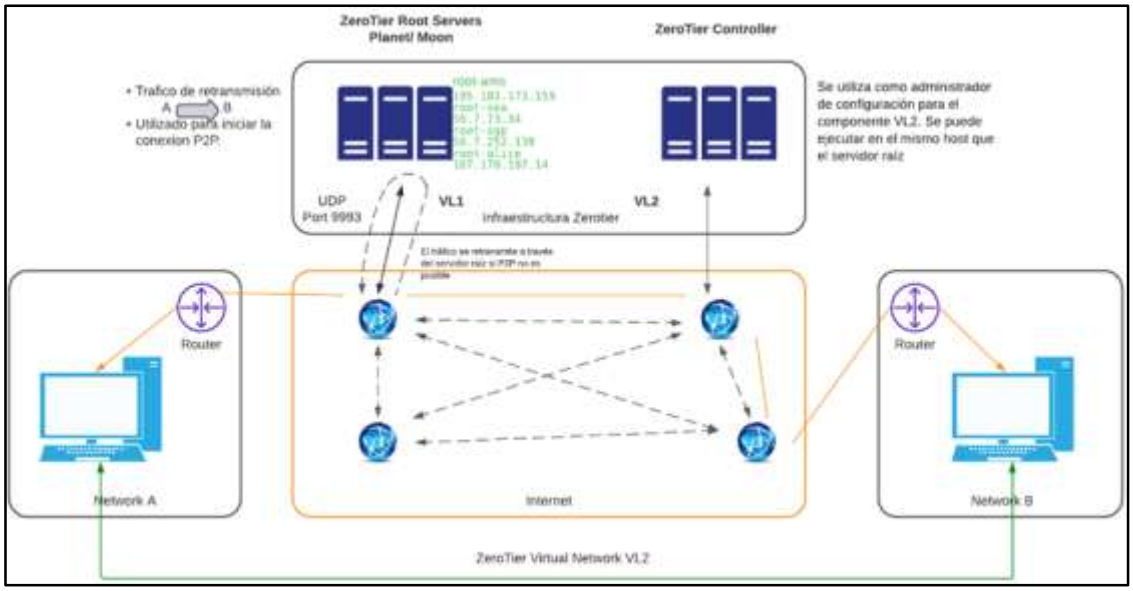


Figura 24-1: Infraestructura ZeroTier

Fuente: (ZEROTIER, 2020)

1.4.1 Funcionamiento ZeroTier

En este aspecto ZeroTier, establece comunicación con dos tipos de servidores, por un lado, están los planetarios, mismos que se encargan de asignar una ID, mientras que por el otro están los lunares, responsables del enrutamiento del tráfico, de manera que un cliente pueda visualizar donde se encuentra otro cliente dentro del internet. Adicionalmente esta la capacitad de establecer controles de acceso. Esta interacción puede ser visualizada a continuación en la figura 25-1.

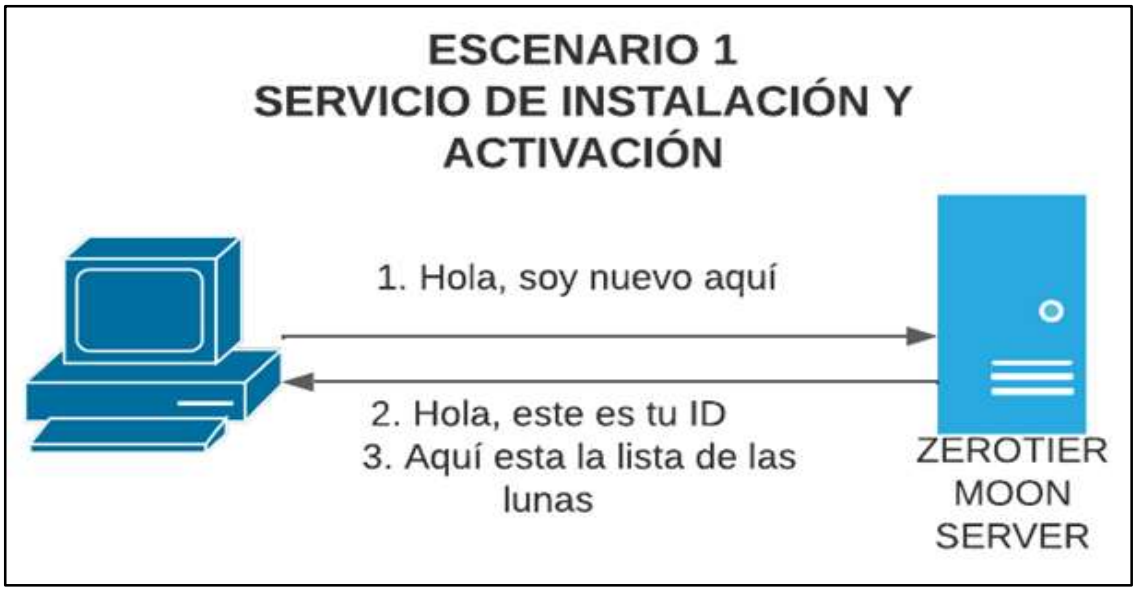


Figura 25-1: Escenario 1, Servicio de instalación y activación

Fuente: (ZEROTIER, 2020)

El nodo, se encargará de comunicar al servidor luna que intenta unirse a la red, la cual identificaremos como XXXXYYYY, posteriormente el servidor procede con la verificación de la

red, donde se determina si esta es pública o privada, con lo cual, surge una condicionante, cuando la red es pública, el nodo realiza una vinculación automática, caso contrario, cuando la red es privada, la autorización para que el dispositivo acceda a la red, llegará proveniente del administrador de la misma.

Tras la aprobación del dispositivo, el servidor luna emite una respuesta, dirigida al nodo, a través de la cual se autoriza su entrada y automáticamente asignará una dirección IP. A continuación, se puede visualizar la interacción antes mencionada:

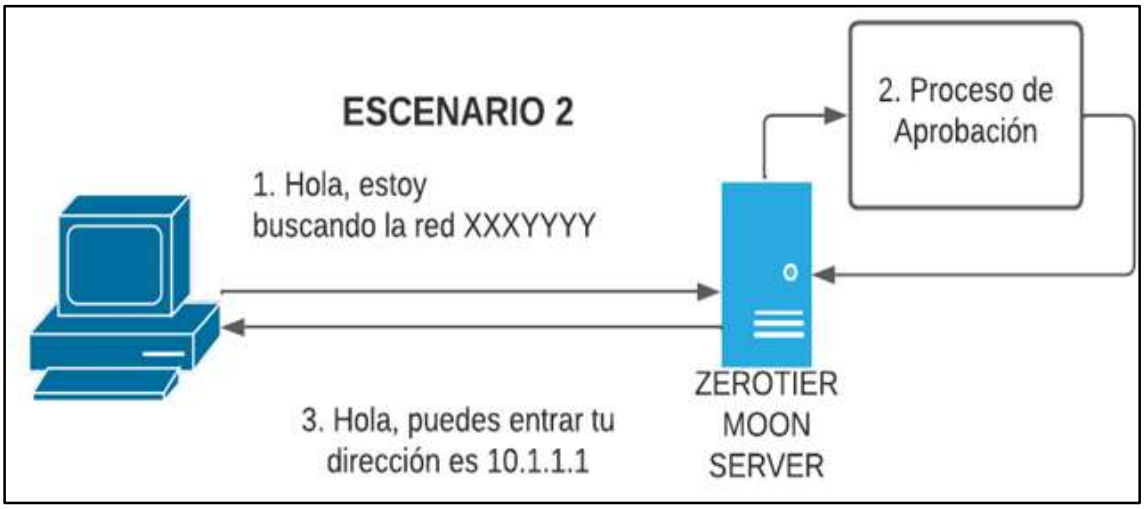


Figura 26-1: Escenario 2, Acceso a la red

Fuente: (ZEROTIER, 2020)

El nodo ejecuta la remisión de mensajes a Keep Alive, con una periodicidad de cada dos minutos, estos cuentan con una codificación rígida, mientras que en cuanto al servidor luna, este realizará la remisión de información concerniente a nuevos dispositivos que accedieron a la red. A continuación, se puede visualizar la interacción antes mencionada.

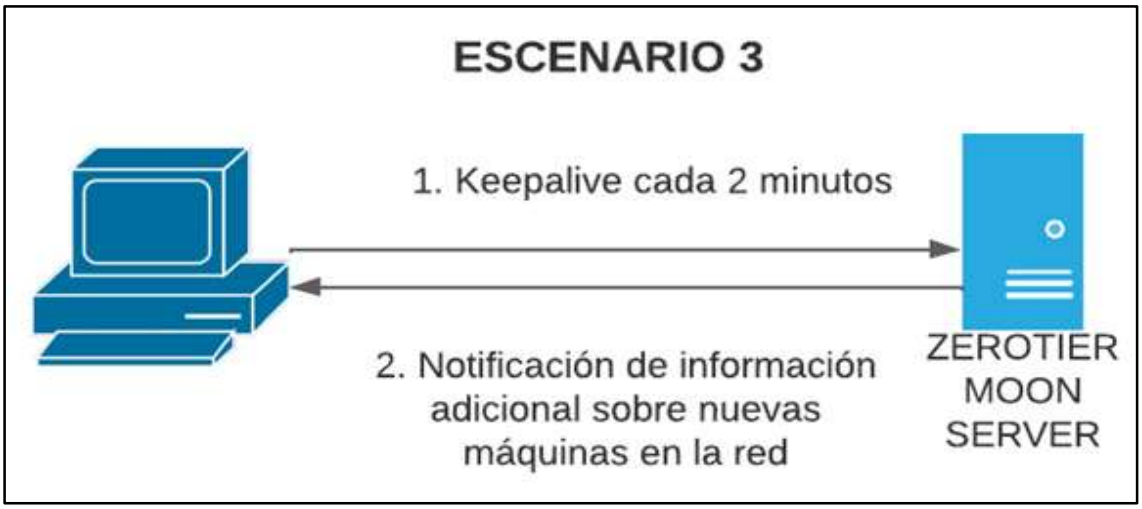


Figura 27-1: Escenario 3, Conectividad

Fuente: (ZEROTIER, 2020)

1.4.2 Criptografía

Hace referencia al encriptamiento de los paquetes por ambos extremos, estos códigos no pueden ser leídos absolutamente por nadie, la criptografía más moderna es la de 256 bits, mismas que cuenta con el respaldo de los criptógrafos que dieron origen a esta ciencia. En ZeroTier, los cifrados de clave para redes públicas, normalmente es asimétrica y puede ser Curve25519/Ed25519, que no es otra cosa que una variación de la curva elíptica de 256 bits.

Para el cifrado de los paquetes VL1, se emplea la versión actualizada de Salsa20 de 256 bits, mientras que para la autenticación se recurre a algoritmos de mensajes (MAC), como es poly 1305, este es calculado posterior al cifrado, donde su composición es igual a la que se emplea para implementar referencia de NACl.

En la actualidad no se realizan implementaciones de secreto hacia adelante y mucho menos características relacionadas con criptografía en VL1, esto debido a que ZeroTier, busca simplificar procesos, brindarle mayor confiabilidad a su gestión y dejar una huella de código, además de que realizar este tipo de instalaciones complica la tarea de agrupar clústeres o la de conmutar por error.

Para profesionales que prefieren emplear secreto hacia adelante, se recomienda emplear protocolos de criptografía como son SSL o SSh sobre ZeroTier, lo que permite contar con una defensa a profundidad. La criptografía puede verse afectada por fallas en la implementación más que por errores en la codificación, sin embargo, la probabilidad de incurrir en estos errores se reduce al emplear dos transportes con alto nivel de seguridad, finalmente es importante tener en claro que la sobrecarga que pudiera experimentar un CPU, producto del doble cifrado, es poco significativa en la mayoría de las cargas.

1.4.3 Identificadores y controladores de red

Las redes VL2 (VLAN), pueden ser identificadas a través de un código de 64 – bits ZeroTier ID de red, donde se encuentra contenida la dirección ZeroTier de 40 bits para el caso de los controladores, mientras que para la identificación de red se emplea 24 bits. A continuación, se presentan la ID y la direcciones.

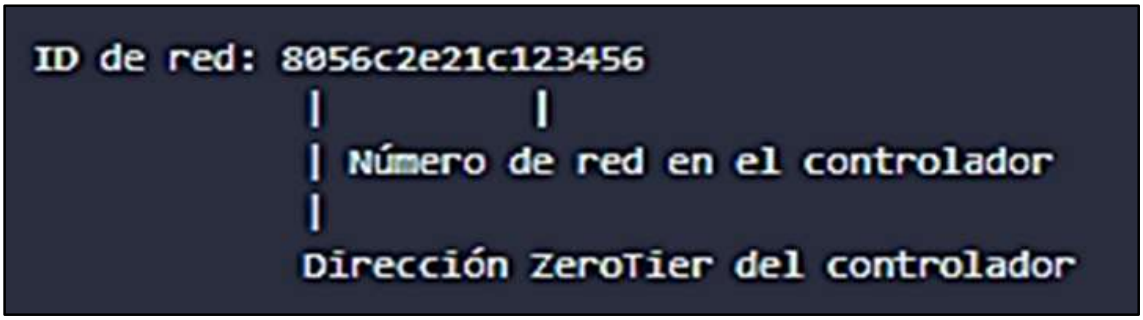


Figura 28-1: Identificadores y controladores de red

Fuente: (ZEROTIER, 2020)

Cuando un nodo se une o gestiona una actualización a la red, realiza la remisión de un mensaje a través del cual se hace efectiva una consulta sobre la configuración de la red en cuestión, esto mediante VL1, en este caso el controlador tiene la opción de emplear la dirección VL1 de dicho nodo, para realizar la determinación de su ubicación en la red y remitir los certificados, credenciales e información concerniente a la configuración que se está realizando.

Desde el punto de vista de las redes virtuales VL2, las direcciones VL1, adquieren la consideración de número de puertos dentro de un conmutador a gran escala. Es común que los controladores de red sean confundidos con servidores raíz, teniendo así que la diferencia radica en que los, servidores raíz, tienen como función facilitar la conexión y su campo de acción es el nivel VL1, mientras que los controladores, tienen como función administrar configuraciones y autorizar certificaciones dentro del nivel VL2, en este caso se deja por sentado cuáles son sus funciones, sin embargo, existen nodos que pueden realizar ambas tareas a la vez.

Dentro de las redes de ZeroTier, los controladores tienen la tarea de autorizar certificaciones, lo cual, supone que su identity secret, deba ser resguardada, en caso de que esta clave, sea manipulada por un atacante, le brindaría la libertad de poder generar configuraciones fraudulentas e incluso realizar la admisión de miembros sin autorización alguna. Para el caso de pérdida de dicha clave, se tiene que los profesionales en el área ya no tendrán control sobre la red, sobre todo para actualizar su configuración, dejándola inutilizada.

A manera de precaución, es recomendable mantener los relojes de los controladores a precisión, resguardándolos de cualquier tipo de manipulación remota, en este aspecto existen proveedores de fuentes de tiempo, con alto margen de seguridad, estos servicios pueden ser directos o también prestarse a través de hipervisor o NTP dentro de la misma red.

1.4.4 Certificados y otras credenciales

Las credenciales generadas por los controladores de la red a los diferentes nodos que la componen cuentan con un rubrica que no es otra cosa que la clave secreta, esto permite que cada uno de los

miembros puedan ser verificados, estas credenciales cuentan con un campo de tiempo, mismo que es completado por el controlador, permitiendo realizar comparaciones y evitar dar mayor confianza al reloj del nodo.

Cabe mencionar que las credenciales solo son generadas para los propietarios, sin embargo, estas pueden ser remitidas por parte de los nodos que buscan interactuar con otros nodos dentro de la misma red, esto propicia el crecimiento del tamaño de las redes, sin necesidad de que las credenciales en caché sean almacenadas dentro de los nodos. A continuación, se presentan los tipos de credenciales.

Figura 29-1: Tipos de certificaciones

Fuente: (ZEROTIER, 2020)

Los certificados de pertenencia son aquellos empleados para adquirir un derecho de comunicación dentro de una determinada red. En cuanto a los certificados de membresía, se tiene que estos son aceptados solo en caso de estar de acuerdo, de manera que existe coincidencia entre la marca de tiempo del certificado del miembro y la del destinatario.

Las revocaciones, son instantáneas y crean un límite de marca de tiempo, antes del cual no serán receptadas, su propagación es vertiginosa, en este caso se da libertad a los controladores para que estos puedan realizar la revocación de cualquier miembro, aun cuando la conexión con estos carece de confiabilidad.

Las capacidades son un conglomerado de reglas de red, mismas que cuenta con la rúbrica del controlador y pueden ser visualizadas por los miembros de la red, con la finalidad de que estos accedan a privilegios en lo que concierne reglas base.

Las etiquetas, son identificadas como claves o valores firmados por el controlador, los cuales son presentados de manera automática por los miembros, estos pueden combinarse con reglas de red o capacidad, además se las emplea como medio de categorización de miembros, puesto que, se los puede clasear por criterios tales como función, departamentos, etc.

Finalmente están los certificados de propiedad, los cuales permiten acreditar la posesión de algún elemento a un miembro en específico, como ejemplo de esto se tiene las direcciones IP. En la actualidad son empleadas como una forma de evitar la falsificación de ID, sin embargo, cuentan con el potencial para certificar propiedades de otros elementos a nivel de red, a los cuales se puede realizar el emparejamiento de filtros.

1.4.5 Modos de direccionamiento especial ARP, NDP y multidifusión

Dentro de las redes ZeroTier, es posible admitir multidifusiones, esto mediante un sistema de publicaciones/suscripción. Para casos donde un nodo, está interesado en receptar multidifusiones para un determinado grupo de multidifusión, debe realizar el anuncio de pertenencia a dicho grupo, a los demás miembros de la red y al controlador, si el caso es que el nodo desea realizar el envío de una multidifusión, debe en primer lugar consultar su caché de anuncios y con cierta periodicidad realizar la solicitud de anuncios adicionales.

La difusión es un grupo en el cual estarán suscritos todos los miembros, esta puede ser desactivada dentro de la red, para evitar una saturación del tráfico interno. IPc4 ARP, será manipulado de manera espacial y se mantendrá activo, cuando la transmisión esta deshabilitada. La propagación de las multidifusiones se da a través de la replicación por los remitentes.

Para llevar a cabo estas acciones se debe colocar la carga completa del ancho de banda de salida para la multidifusión en el remitente y minimizar la latencia de la multidifusión. Es preciso mencionar que las redes, cuentan con un límite máximo de multidifusiones, en casos donde el número de destinatarios excede los limites preestablecidos, le remitente deberá elegir un subconjunto de destinatarios aleatoriamente.

1.4.6 Motor de reglas

Aspectos tales como el tráfico dentro de las redes ZeroTier, puede ser monitoreado y regulado mediante un conjunto de reglas aplicables a nivel global, las cuales aplican tanto para remitentes como para destinatarios de los paquetes. El motor de regla solo puede ser burlado por parte de un atacante, si este compromete en su totalidad los dos extremos de una conversación.

Para el motor de reglas de ZeroTier en el nivel VL2, existe una diferencia con respecto a demás firewalls y otros motores de reglas SDN, entre estas la más relevante es que el motor de reglas ZeroTier no cuenta con estados, lo que permite entrever las falencias con respecto al seguimiento de la conexión. Esto supone que no se puede conseguir una lista blanca bidireccional, solo por contar con la lista de blanca de paquetes de respuesta a las conexiones establecidas, no obstante, se debe gestionar la manera de brindar a ambos extremos el flujo deseado (ZEROTIER, 2020).

La conversión del motor de reglas a una apátrida, es una manera de compensar varias preocupaciones, entre las cuales están el mantenimiento de la complejidad, la huella de código y una reducción en el uso de memoria que permitiera la admisión de pequeños dispositivos y la segunda preocupación es la sincronización de los estados, lo que generaría normalmente un gran volumen de tráfico adicional, además de la aparición de inestabilidades y vulneraciones de la seguridad.

A pesar de las falencias en cuanto al seguimiento de estado, ZeroTier presenta una cualidad inigualable que es la seguridad basada en capacidades, así como también las etiquetas de dispositivos, lo que permiten estructurar sistemas de reglas micro segmentadas con alto nivel de complejidad, las cuales son fácil de entender para los profesionales y con alto nivel de eficiencia en el manejo por parte de máquinas.

1.4.7 Etiquetas

En las redes de ZeroTier, existe una segunda alternativa para regular la complejidad de las reglas, que son las etiquetas, las cuales actúan como credenciales compuestas por una relación clave – valor numérico de 32 bits, los cuales son emitidos para los miembros de una red y reciben la firma por parte del controlador, para posteriormente distribuirse en igualdad de condiciones tomando como base las necesidades de conocerlos.

Las etiquetas representan una alternativa para suprimir o permitir el tráfico, de manera condicional entre los miembros por clasificación, así como también permite la microsegmentación de redes bajo el criterio de roles, permiso y función, sin necesidad de una explosión combinatoria en el tamaño de la tabla de reglas (ZEROTIER, 2020).

1.4.8 Multitrayecto

En ZeroTier, existe la posibilidad de que los pares puedan establecer comunicación a través de variadas rutas físicas, que de manera simultánea y equilibrada de forma automática con la fuerza de la ruta. En casos donde un par que admite múltiples rutas, adoptará un comportamiento de no múltiples rutas en casos donde otros pares no las admite, esto gracias a la implementación de técnicas de medición pasivas y activas, en cuanto al tráfico adicional, este se detendrá en el momento en que cese el tráfico de usuarios, ya que no hay tráfico ambiental cuanto este se encuentra inactivo.

- **Modos:** En la actualidad existen dos alternativas o modos, el aleatorio o proporcionalmente equilibrado. En lo que respecta al modo aleatorio, este se encarga de enviar tráfico a través de las rutas que logre detectar, a pesar de que este no presenta equilibrio alguno, es capaz de

detener el envío de tráfico, en caso de expirar. En lo concerniente al modo proporcionalmente equilibrado, se tiene que realizará mediciones continuas sobre la calidad de las diferentes rutas y realiza la asignación de tráfico tomando en consideración estabilidad y rendimiento de las mismas.

- **Noción de calidad del enlace:** En este caso la calidad a la que se hace referencia es con respecto a otras rutas, donde se toma como referencia, los valores para proceder con la determinación de la frecuencia de distribución del tráfico entre rutas. Este se compone de dos categorías, que son stability y performance. Es preciso mencionar que estas cantidades son cruciales para futuros proyectos sobre la calidad de los servicios (QOS).

En este sentido, en caso de desear una asignación de cierto tipo de tráfico a rutas con alto nivel de estabilidad, cuando no sea necesario contar con altos rendimientos, las cantidades serán definidas bajo los siguientes criterios.

Figura 30-1: Nociones de la calidad de enlace

Fuente: (ZEROTIER, 2020)

1.4.9 Agregación de enlaces

Esta opción permite emplear de manera simultánea o condicional, múltiples enlaces físicos para permitir increased, total throughput, load balancing, redundancy y fault tolerance. Dentro de esta opción existen políticas estándar de uso inmediato, que no requieren de complejas configuraciones, las cuales se inspiran en las políticas ofertadas por Kernel de Linux, sin embargo, en tiempos actuales, se pueden encontrar en plataformas que guardan compatibilidad con ZeroTier (ZEROTIER, 2020).

1.4.10 Políticas estándar

Dentro de las políticas estándar se pueden identificar la tolerancia al fallo, es decir, cuan susceptibles son a interrupción por falla en la conexión, la conmutación por error, que se refiere al tiempo de reacción para cambiar de red, en caso de que la primera experimente una caída y la

eficiencia de agregación que se refiere la facilidad para agregar paquetes. A continuación, se presentan las políticas estándar de ZeroTier.

Tabla 1-1: Políticas estándar ZeroTier

Nombre	Tolerancia a fallos	Conmutación por error mínimo	Conmutación por error predeterminada	Equilibrio	Eficiencia de agregación	Redundancia
Active-Backup	Breve interrupción	0,25 Seg	10 Seg	N/A	Baja	1
Balance-Xor	Autocuración	0,25 Seg	10 Seg	Basado en flujo	Muy Alta	1

Fuente: (ZEROTIER, 2020)

Realizado por: García, Luis, 2022.

1.4.11 Copia de seguridad activa (Active - Backup)

En este caso, el envío se realiza únicamente en la ruta1, en un momento determinado, en caso de que se experimente un fallo en la ruta activa, se activará una ruta diferente, lo que permite brindar una tolerancia al fallo, además de una conmutación por error, de manera inmediata, es preciso mencionar que estas acciones no suponen un aumento de los niveles de rendimiento. A continuación, se presenta la Active – Backup.

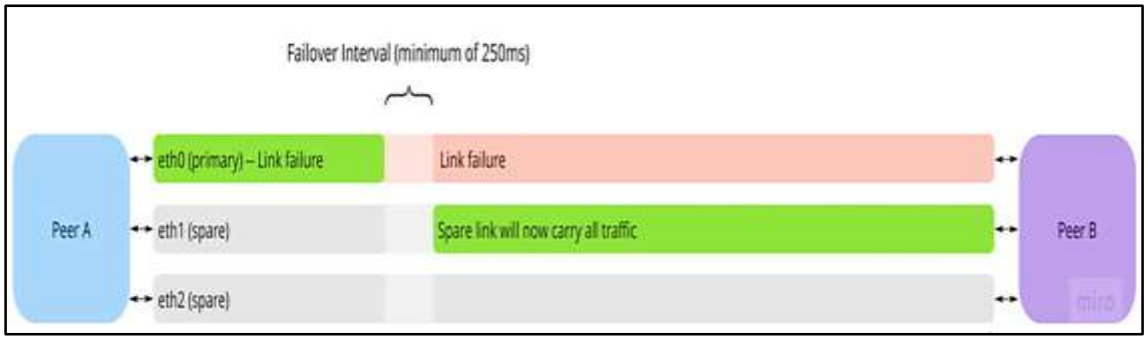


Figura 31-1: Active - Backup

Fuente: (ZEROTIER, 2020)

1.4.12 Equilibrio XOR (Balance - XOR)

En esta política el tráfico es clasificado en función al puerto de origen, el de destino e incluso por el tipo de protocolo, los flujos en cuestión son agrupados en los enlaces disponible, cada uno de estos persistirá en su respectiva interfaz de enlace. En cuanto al tráfico, este no cuenta con un puerto asignado y serán distribuidos de manera aleatoria entre los diferentes enlaces. La sintaxis de la función hash, es la siguiente src_port^ dst_port^proto. A continuación, se presenta el balance – xor.

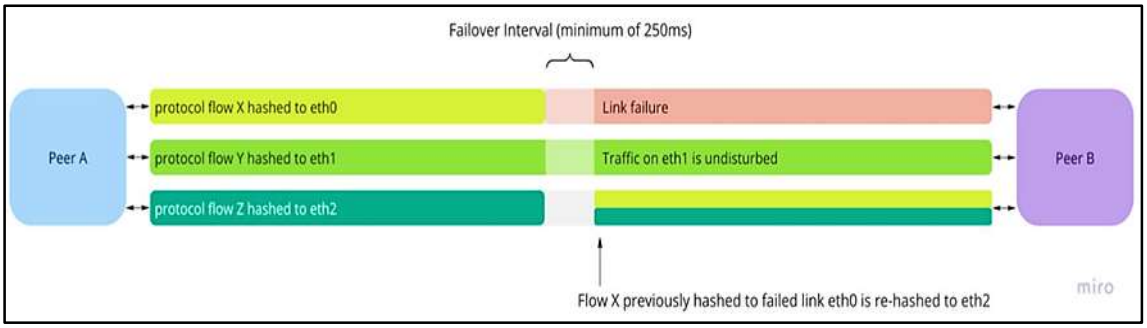


Figura 32-1: Balance – XOR

Fuente: (ZEROTIER, 2020)

1.4.13 Calidad del enlace

ZeroTier, realiza diferentes mediciones sobre las propiedades de los enlaces, entre las cuales se enlistan, la latencia, rendimiento, fluctuaciones o el índice de perdida de paquetes, con base a estos indicadores, realiza la estimación de la calidad. En cuanto a las políticas de vinculación, estas toman la estimación emitida para decidir una asignación o conmutación por error (ZEROTIER, 2020). A continuación, se presentan los parámetros en cuestión.

Tabla 2-1: Calidad del enlace

Nombre de directiva	Como se utilizan las medidas
Active – backup	Determina el orden de la cola de conmutación por error. Y si activeReselect=optimize se selecciona un nuevo enlace activo
Broadcast	No utiliza medidas de calidad
Balance – rr	Puede desencadenar la eliminación del enlace del enlace
Balance – xor	Puede desencadenar la eliminación del enlace del enlace
Balance - aware	Informa las asignaciones de flujo y (reasignaciones). Puede desencadenar la eliminación del enlace del enlace.

Fuente: (ZEROTIER, 2020)

Realizado por: García, Luis, 2022.

La elección de un enlace dependerá de la calidad percibida del mismo, en caso de que la ruta detecte un elevado índice de pérdida de paquetes, corrupción o tenga incapacidad para procesar el tráfico, procederá con la eliminación de dicho enlace, en cuanto al tráfico, este será reasignado y será objeto de castigo, mismo que desaparecerá gradualmente y podrá realizarse la admisión de un vínculo con tiempo. Los castigos pueden aumentar su magnitud, si se registran más de una vez dentro de un mismo periodo.

CAPÍTULO II

2. MARCO METODOLÓGICO

En este capítulo se procede con el desarrollo del marco metodológico, para lo cual, se procederá a realizar una descripción ordenada y detallada de las fases de desarrollo del prototipo de red SD – WAN, donde el punto de partida es cumplir con los requerimientos de red, para posteriormente comenzar con la ejecución y los respectivos controles.

2.1 Fases del proyecto

Para poder entender de mejor manera el prototipo, es necesario presentar un esquema de las fases involucradas para el desarrollo de este proyecto.

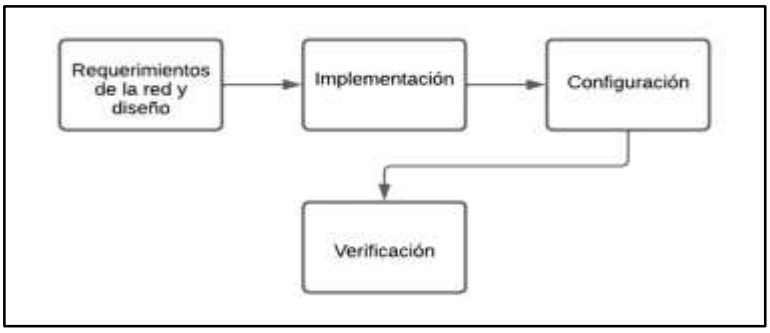


Figura 1-2: Fases del proyecto

Fuente: García, Luis, 2022.

A continuación, se procede a describir el contenido de cada una de las etapas antes mencionadas:

- **Requerimientos de la red y diseño:** En esta fase se entregará un detalle de los componentes a nivel de *hardware* y *software*. Se plantera una topología de red que se acople al diseño SDWAN.
- **Implementación:** Se implementa el modelo propuesto en el diseño mediante en el *software* de emulación GNS3 utilizando los equipos, componentes y conexiones necesarias.
- **Configuración:** En esta fase se ejecutarán las configuraciones de red, tales como: direccionamiento IP, Protocolos y plugins necesarios para la red SDWAN.
- **Verificación:** En esta fase se revisa se revisa las funcionalidades de la red SDWAN.

2.2 Requerimientos y diseño

Esto se indica en el siguiente apartado.

2.2.1 Requerimientos de hardware y software

Teniendo en consideración el diseño de la red SD-WAN, se analizan los requerimientos necesarios, donde el sistema se compondrá de *software* y *hardware* con la finalidad de poder tener un correcto funcionamiento y rendimiento de la red.

2.2.1.1 Gns3

Los siguientes son los requerimientos mínimos para un entorno Windows en GNS3.

Tabla 1-2: Requerimientos para configurar GNS3

Ítem	Requerimientos mínimos
Sistema operativo	Windows 7 (64) o superior
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización
Memoria	4GB RAM
Espacio en disco	1GB de espacio disponible
Notas adicionales	Es posible que necesite almacenamiento adicional

Fuente: (REJÓN, 2019)

Realizado por: Patachi B., Ramos C., 2022.

2.2.1.2 OPNSENSE

Para la aplicación del firewall OPNSENSE, existen determinados requerimientos de *hardware*, mismos que se presentan a continuación.

Figura 2-2: Requerimientos de *hardware* OPNSENSE

Fuente: García, Luis, 2022.

2.2.1.3 PFSENSE

Se basa en FreeBSD, su lista de compatibilidad de *hardware* es la misma que la de FreeBSD. A continuación, se describe los requerimientos mínimos de *hardware* del *software* Pfsense.

Tabla 2-2: Requerimientos de *hardware* para configuración PFSense

Requerimientos mínimos
64-bit amd64 (x86-64) compatible CPU
CPU: 500Mhz
RAM: 512 MB
Unidad de disco de 8 GB o más grande (SSD, HDD, etc.)
2 interfaces de red mínimo

Fuente: (PFSENSE, 2022)

Realizado por: García, Luis, 2022.

2.2.1.4 Ubuntu LINUX

En la actualidad las distribuciones de Linux están migrando a arquitecturas de 64 bits, lo que supone que conforme se lanzan nuevos sistemas, los requerimientos experimentan variaciones (IBARRA, 2020). Para la instalación de Ubuntu – Linux se requieren los siguientes requisitos.

Figura 3-2: Requerimientos Ubuntu Linux

Fuente: (IBARRA, 2020)

2.2.1.5 Diseño de la red

"Para el desarrollo de la red, se empleará el Software GNS3, mismo que entre sus bondades esta la posibilidad de realizar planificación de actividades, simular y gestionar soluciones para problemas que pudieran presentarse en la red que se está diseñando" (JIMÉNEZ, 2020).

Con la intención de poder realizar simulaciones de los modelos antes mencionados, surge la necesidad de diseñar la red Ip/Mpls, con lo cual, se crearán dos redes WAN totalmente funcionales, donde se emplean en un simulador de redes GNS3. Esta arquitectura estará compuesta por dos proveedores de internet, proveedor 1 y proveedor 2, esto con la finalidad de que el circuito en cuestión tenga salida a internet.

La red del proveedor 1 se compone de varios routers en topología Mesh, para ello se usarán los routers Mikrotik (Chr 6.39), como una mejor opción para la rápida configuración de salida hacia

internet. Para el transporte de los paquetes de una manera segura se utilizará Mpls. En lo que respecta a la configuración, los routers intermedios contarán tanto con la funcionalidad de P (Backbone/core), como la de conmutación de etiquetas, mientras que por otro lado, los routers externos tienen la funcionalidad de PE (Border del proveedor), que además de conmutación por etiqueta, también tienen el enrutamiento de paquetes, hacia servicios que cuenta con mínimo una interfaz y se encuentra conectada a los equipos de los clientes (CEs). Como enrutamiento dinámico se empleará OSPF de tal manera que permita tener una mejor conectividad entre los routers y lograr estabilidad en la red (JIMÉNEZ, 2020).

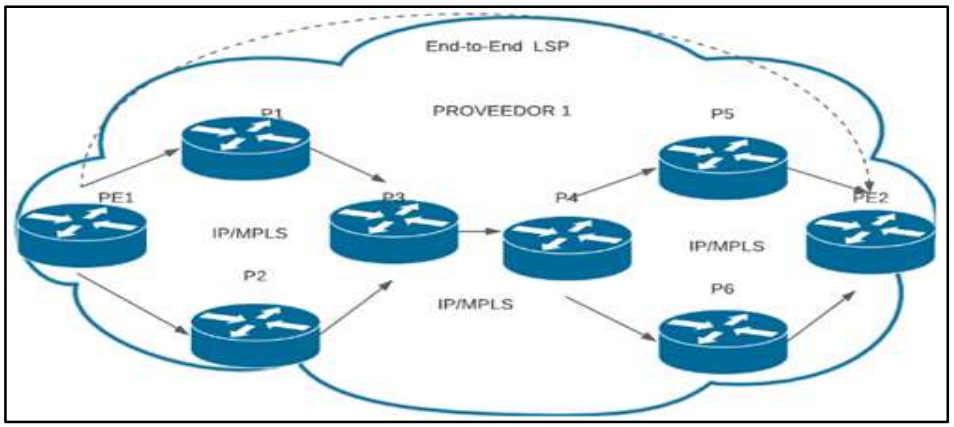


Figura 4-2: Topología de red Mpls para el proveedor 1

Fuente: (LUCID, 2021)

Para los equipos CEs se emplearan los Firewall OPNSENSE, estos son basados en un entorno FREE BSD, estos equipos tienen como funcionalidad proporcionar la interconexión de los sitios de manera remota, cabe mencionar que estos firewalls fueron instalados en el entorno de virtualización denominado Virtual Box.

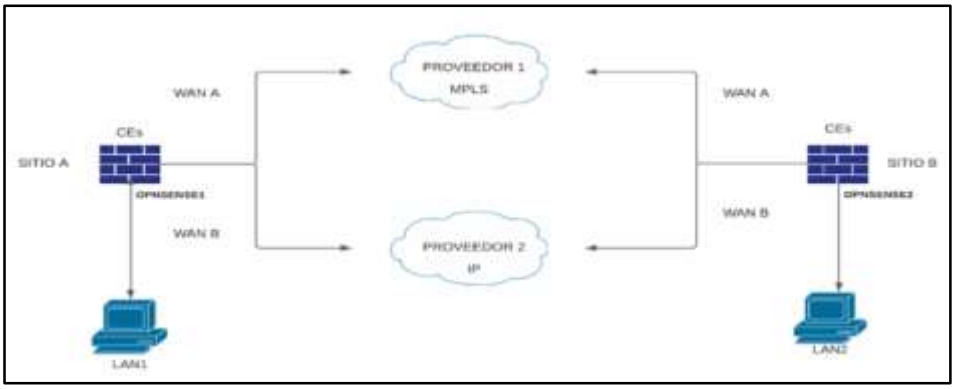


Figura 5-2: Virtual box

Fuente: (LUCID, 2021)

Cada sitio a través de su router de borde para tener una seguridad básica y evitar que existan ataques, se dividirá en 3 zonas perimetrales como son la red Wan, Dmz, Lan. La red Wan permite tener salida hacia internet, la DMZ se configurará como un mecanismo de seguridad con el fin de

tener la red protegida, y por último la red Lan donde se encontrarán los usuarios finales, donde se encontrará instalado Ubuntu 20.0.01 LTS.

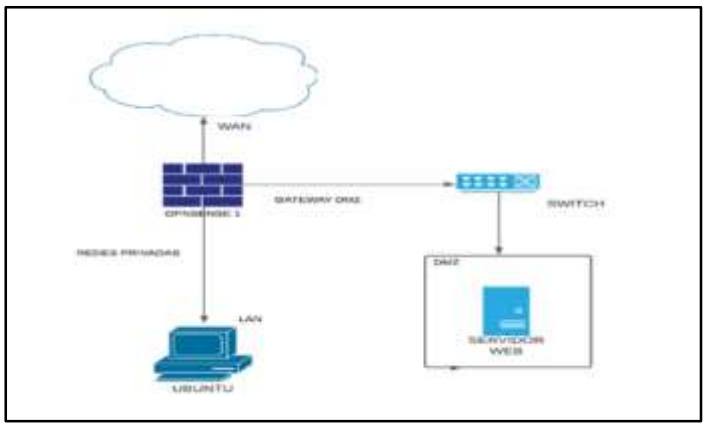


Figura 6-2: Incorporación de Ubuntu 20.0.1 LTS

Fuente: (LUCID, 2021)

2.2.2 Implementación

2.2.2.1 Implementación de la red SDWAN

A continuación, se muestra la topología desplegada mostrando los elementos de la arquitectura SDWAN en el entorno virtualizado GNS3, donde podrá apreciarse la conexión entre los sites A y B, con el proveedor 1 y la red IP/MPLS (KLUSAITE, 2022).

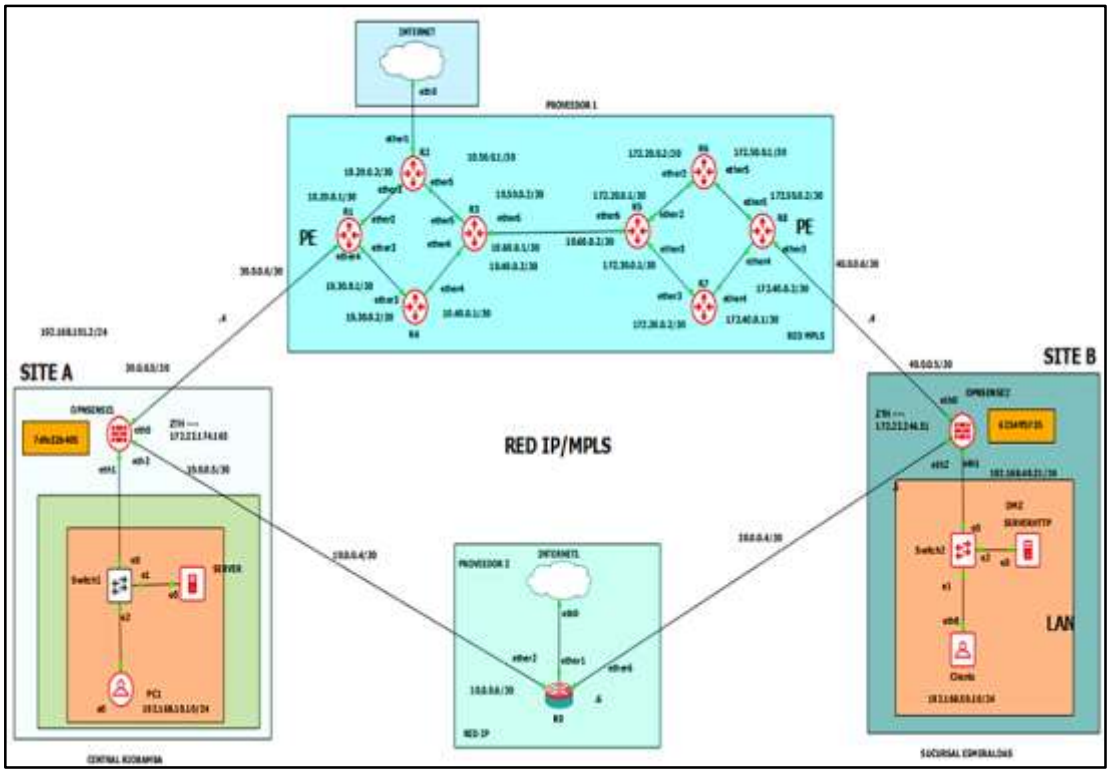


Figura 7-2: Red SDWAN simulada en GNS3

Realizado por: García, Luis, 2022.

2.2.3 Configuración

2.2.3.1 Direccionamiento lógico IPV4

Funciona como un identificador de tipo numérico, el cual se compone de cuatro grupos de número que van desde 0 a 255, cada grupo estará separado por un punto. Para el diseño del Proveedor 1 y Proveedor 2 se presenta la siguiente información de direcciones las cuales pertenecen a la Clase A y B.

Tabla 3-2: Direccionamiento IPV4

	Equipo	*Interfaz*	*Dirección IP*	*Mascara de Red*	*Gateway*	*Router ID*
Proveedor 1	R1	Eth2	10.20.0.1/30	255.255.255.252	10.20.0.2	1.1.1.1.
		Eth3	10.30.0.1/30	255.255.255.252	10.30.0.2	
		Eth4	30.0.0.6/30	255.255.255.252	30.0.0.5	
		Lo0	1.1.1.1/32	255.255.255.255		
	R2	Eth2	10.20.0.2/30	255.255.255.252	10.20.0.1	2.2.2.2
		Eth5	10.50.0.1/30	255.255.255.252	10.20.0.2	
		Lo0	2.2.2.2/30	255.255.255.255		
	R3	Eth4	10.40.0.2/30	255.255.255.252	10.40.0.1/30	3.3.3.3
		Eth5	10.50.0.2/30	255.255.255.252	10.50.0.1/30	
		Eth6	10.60.0.1/30	255.255.255.252	10.60.0.2/30	
		Lo0	3.3.3.3/32	255.255.255.255		
	R4	Eth3	10.30.0.2	255.255.255.252	10.30.0.1/30	4.4.4.4
		Eth4	10.40.0.1/30	255.255.255.252	10.40.0.2/30	
		Lo0	4.4.4.4/32	255.255.255.255		
	R5	Eth2	172.20.0.1/30	255.255.255.252	172.20.0.2/30	5.5.5.5
		Eth3	172.30.0.1/30	255.255.255.252	172.30.0.2/30	
		Eth6	10.60.0.2/30	255.255.255.252	10.60.0.1/30	
		Lo0	5.5.5.5/32	255.255.255.255		
	R6	Eth2	172.20.0.2/30	255.255.255.252	172.20.0.1/30	6.6.6.6
		Eth5	172.50.0.1/30	255.255.255.252	172.50.0.2/30	
		Lo0	6.6.6.6/32	255.255.255.255		
	R7	Eth3	172.30.0.2/30	255.255.255.252	172.30.0.1/30	7.7.7.7
		Eth4	172.40.0.1/30	255.255.255.252	172.40.0.2/30	
		Lo0	7.7.7.7/30	255.255.255.255		
	R8	Eth3	40.0.0.6/30	255.255.255.252	40.0.0.5/30	8.8.8.8
		Eth4	172.40.0.2/30	255.255.255.252	172.40.0.1/30	
		Eth5	172.50.0.2/30	255.255.255.252	172.50.0.1/30	
		Lo0	8.8.8.8/32	255.255.255.255		
Proveedor 2	R9	Eth1	20.0.0.6/30	255.255.255.252	20.0.0.5/30	9.9.9.9
		Eth2	10.0.0.6/30	255.255.255.252	10.0.0.5/30	
		Lo0	9.9.9.9/32	255.255.255.255		

Realizado por: García, Luis, 2022.

Se debe tener en cuenta que en la red SD-WAN, no es estrictamente necesario contar con protocolos de direccionamiento entre PE y Ces, basta con realizar una configuración Gateway para cada interfaz del CE, de manera que, por defecto, se añade la ruta a cada enlace (JIMÉNEZ, 2020).

Dentro de cada OPNSENSE se usan dos direcciones IP correspondientes a la red WANA y WANB y una interfaz LAN como se muestra a continuación.

Tabla 4-2: Direccionamiento sitia A - sitio B

	Equipo	*Interfaz*	*Dirección IP*	*Máscara*
SITIO A	CE1 OPNSENSE1	Em0	30.0.0.5/30	255.255.255.252
		Em3	10.0.0.5/30	255.255.255.252
		Em1	192.168.10.1/24	255.255.255.0
	CLIENTE 1	Eth0	192.168.10.10/24	255.255.255.0
SITIO B	CE2 OPNSENSE2	Em0	40.0.0.5/30	255.255.255.252
		Em3	20.0.0.5/30	255.255.255.252
		Em1	192.168.50.1/24	255.255.255.0
	CLIENTE 2	Eth0	192.168.10.10/24	255.255.255.0

Realizado por: García, Luis, 2022.

2.2.3.2 ZeroTier plugin

Tras haberse realizado el diseño de la arquitectura SD-WAN, en primer lugar, se debe obtener una cuenta en Zerotier.com, esto con la finalidad de contar con una identificación en la red. La red en cuestión por defecto será privada, visible únicamente para los nodos.

Figura 8-2: ZeroTier central

Realizado por: García, Luis, 2022.

Para casos como estos donde se requiere de la instalación de ZeroTier – one, el firewall OPNSENSE, brindará los plugins necesarios para efectuar una correcta implementación de una arquitectura SD-WAN. Para el presente estudio se realizó la instalación de ZeroTier -one en su versión 1.6.5 y en simultaneo un conjunto de complementos que permitirán controlar y monitorear la red.

Luego de haberse realizado la suscripción en ZeroTier central, se debe buscar la aplicación ZeroTier la cual se la encuentra en la ventana Firmware → Plugins, cabe mencionar que antes de realizar dicha acción se debe actualizar los repositorios de OPNSENSE.

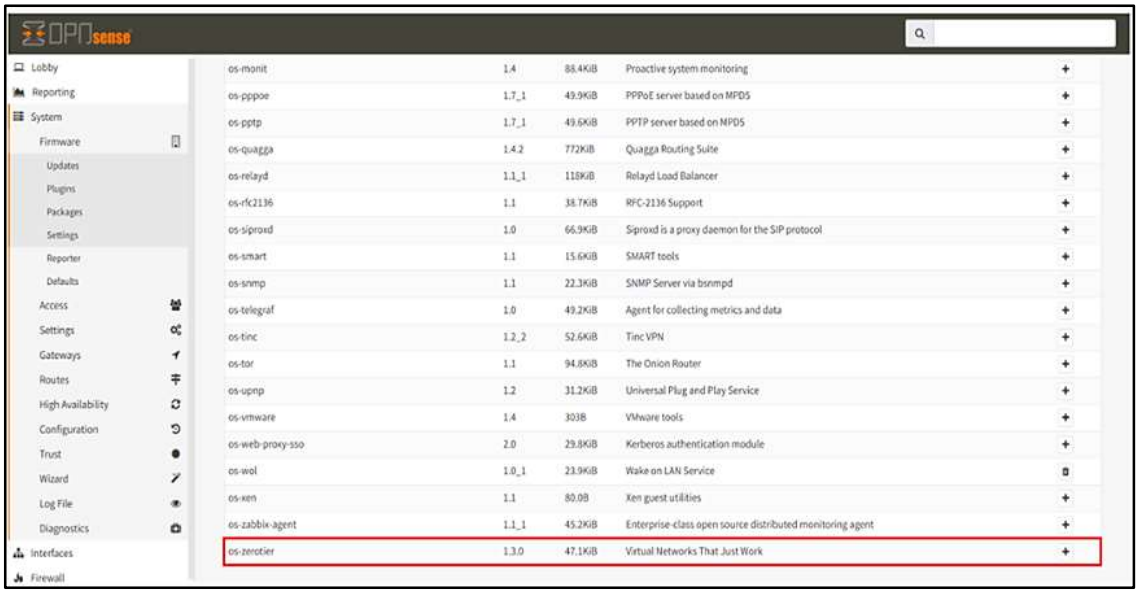


Figura 9-2: Plugins OPNSENSE

Realizado por: García, Luis, 2022.

Tras la instalación del paquete de ZeroTier, se visualizará los elementos del submenú, que en este caso son la configuración y descripción general, posteriormente se debe empezar la habilitación del servicio ZeroTier.

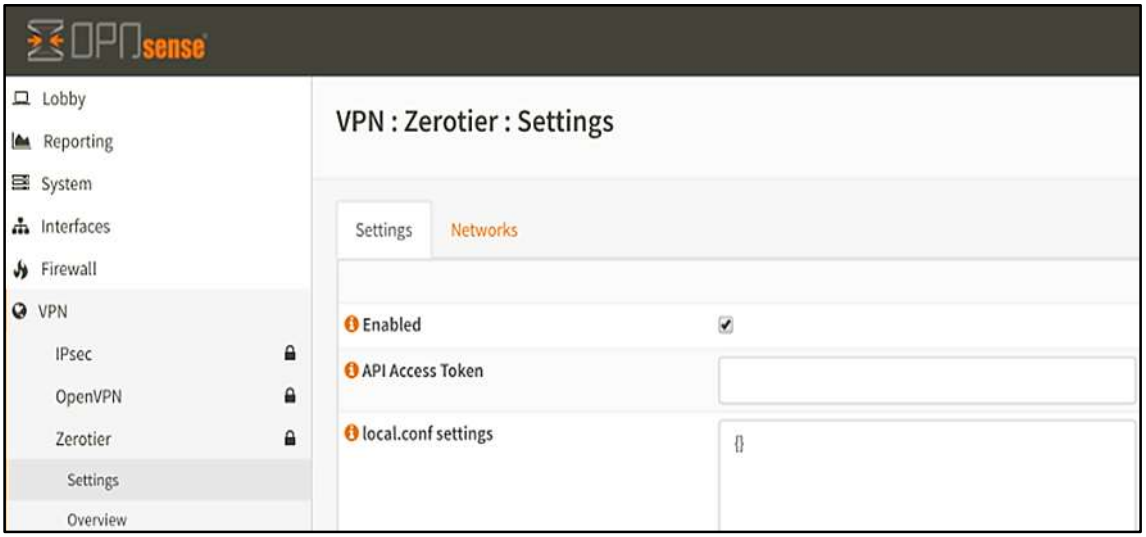


Figura 10-2: Submenú ZeroTier

Realizado por: García, Luis, 2022.

Se debe unir a la red establecida en ZeroTier central, para lo cual en la parte izquierda del menú desplegable vamos a **ZeroTier → settings → Networks**. Se procede a añadir la red creada ingresado el ID generado en ZeroTier Central.

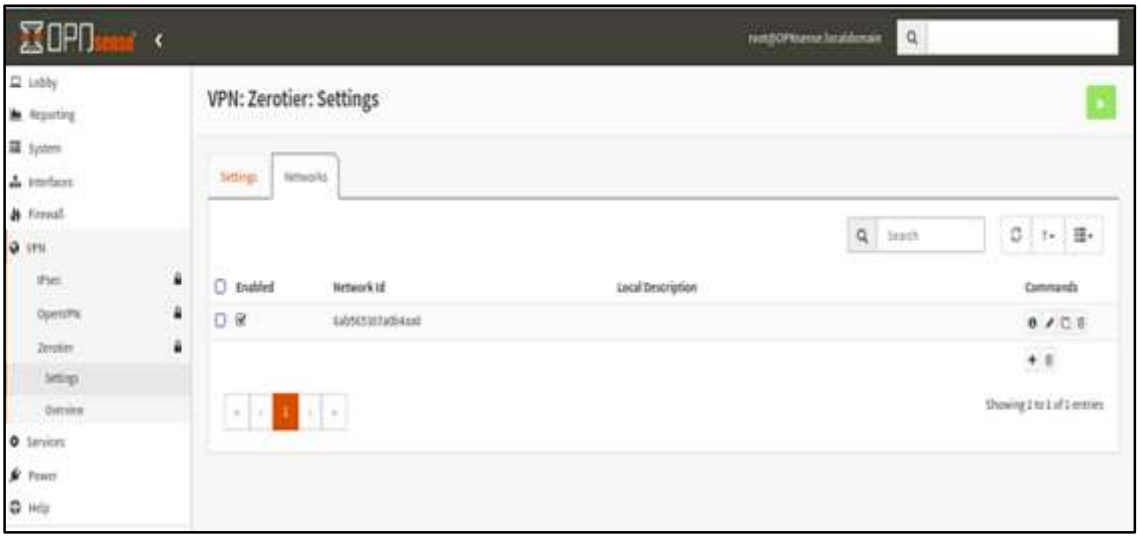


Figura 11-2: Configuración ZeroTier

Realizado por: García, Luis, 2022.

Una vez que se ha agregado y habilitado la red, en el portal, el nodo debe estar autorizado para unirse a la red, se debe habilitar en ZeroTier central dando la autorización, con la finalidad de que se pueda comunicar con los otros nodos de la red creada.

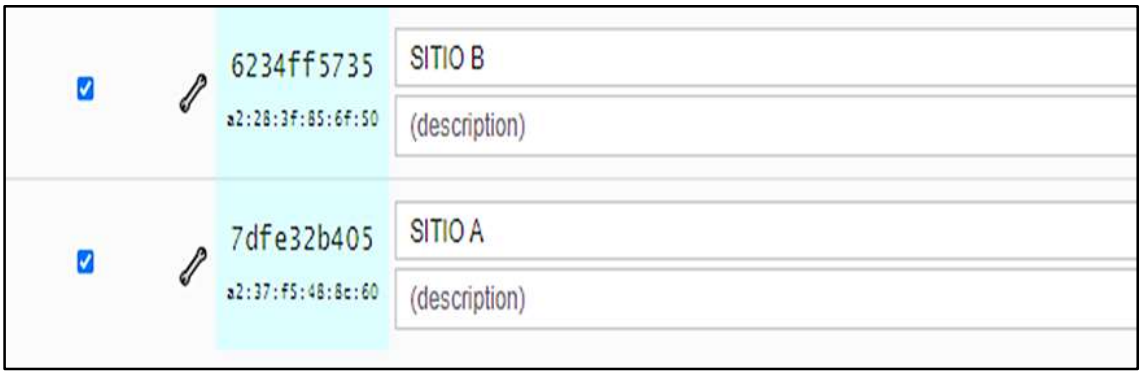


Figura 12-2: Nodos ZeroTier

Realizado por: García, Luis, 2022.

Luego de unirse a la red ZeroTier, se debe aplicar la conexión de ambos nodos, en este caso, dentro de cada firewall, se crea una interfaz Virtual de ZeroTier asignándole un rango de direcciones, las mismas que pertenecen a las direcciones de redes privadas clase A, B, C. Para el escenario se escogió las direcciones de clase B en el rango 172.22.0.0/16. Una vez creada la conexión se crea un túnel entre el SITIO A y el SITIO B. Véase Anexo A.

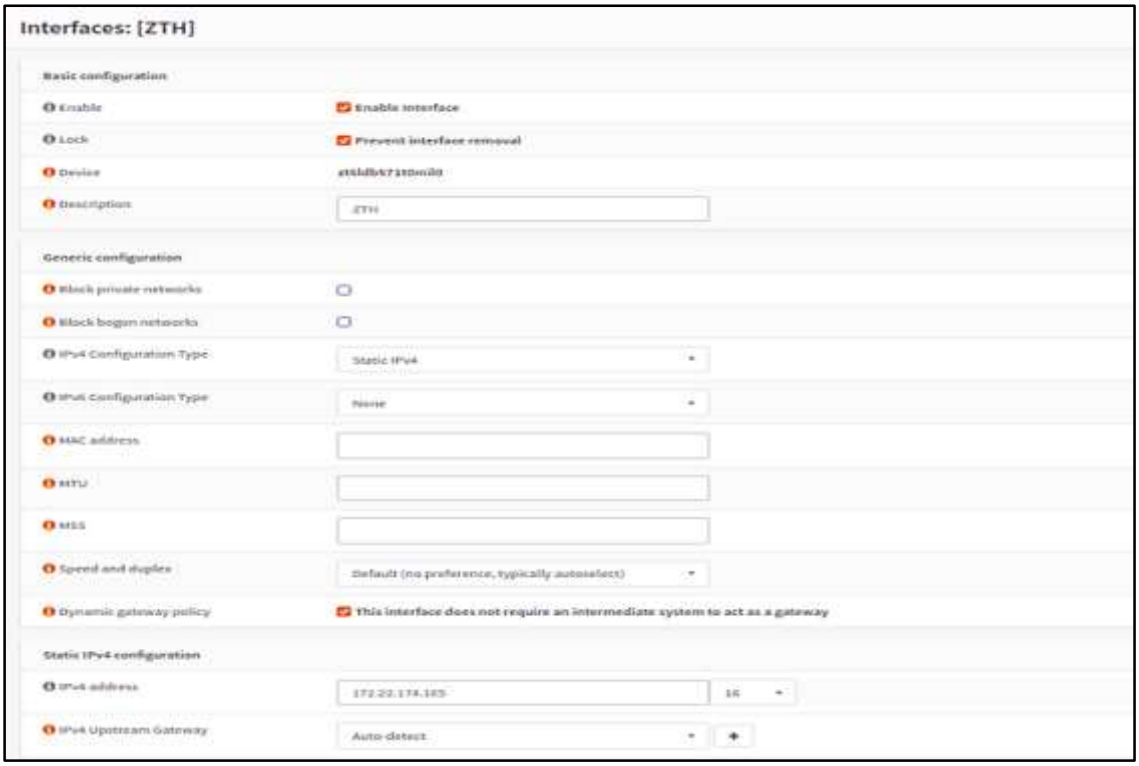


Figura 13-2: Creación de interfaz virtual

Realizado por: García, Luis, 2022.

```
Mar 17 18:10:28 OPNsense opnsense[75546]: /usr/local/etc/rc.newwanip: IPv4 renewal is starting
on 'zt6ldb571t0mil0'
Mar 17 18:10:28 OPNsense opnsense[75546]: /usr/local/etc/rc.newwanip: On (IP address: 172.22.17
4.165) (interface: ZTH[opt3]) (real interface: zt6ldb571t0mil0).
```

Figura 14-2: Interfaz vista desde el OPNSENSE

Realizado por: García, Luis, 2022.

2.2.3.3 Configuración de políticas

Dentro de la opción de ZeroTier se encuentra un apartado denominado ***local.conf settings***, En el cual se configuran las políticas de enrutamiento, básicamente consiste en un archivo denominado ***local.conf*** donde contiene opciones de configuración que se aplica al nodo local (ZEROTIER, 2020).

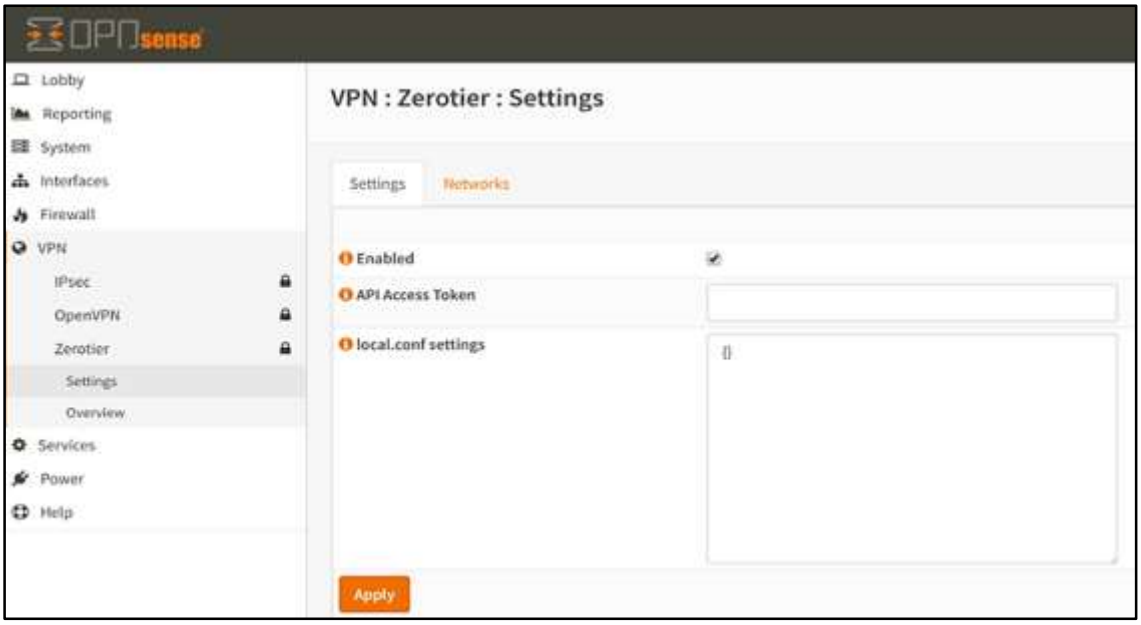


Figura 15-2: Pantalla de configuración de políticas de enrutamiento

Realizado por: García, Luis, 2022.

El siguiente paso es la configuración de las políticas de enrutamiento, que son una de las características esenciales de las arquitecturas SD-WAN, motivo por el cual, fue necesario proceder con la elección de ruta dinámica entre las opciones de conectividad Mpls, o IP, donde, ZeroTier, pone a disposición un conjunto de políticas estándar, las cuales son revisadas y visualizadas en la tabla 2-1.

```
{
  "settings": {
    "defaultBondingPolicy": "myPolicy",
    "policies": {
      "myPolicy": {
       "basePolicy": "active-backup",
                              "links": {
                                        "em0": {
                                                  "ipvPref": 4,
                                                  "failoverTo": "em3",
                                                  "mode": "primary",
                                                  "enabled": true
                                        },
                                        "em3": {
                                                  "ipvPref": 4,
                                                  "mode": "spare",
                                                  "enabled": true
                                        }
                              }
                    }
          },
          "peerSpecificBonds": {"6234ff5735":"myPolicy"}
    }
}
```

Figura 16-2: Política estándar active-backup

Realizado por: García, Luis, 2022.

Dentro de la política estándar active-backup se detallan los enlaces Em0 y Em3 correspondientes a la interfaz WANA y WANB respectivamente. Em0 como una ruta principal y Em3 como en

modo espera o escucha, en el caso, en que la interfaz principal falle o emita pérdidas de paquetes, Em3 entra en funcionamiento como un enlace de respaldo. Se debe especificar en el apartado de ¨peerSpecificBonds¨ el nodo en el cual se va a entablar la política, en donde se indica el código identificador que otorga ZeroTier central al nodo. En la Tabla 2-1 se muestra que existe una conmutación por error cuando en el enlace existan retardos de aproximadamente 250ms.

Una vez configurada las políticas en el nodo OPNSENSE, se visualizará el bonding Policy = 1, mismo que concierne a activebackup, acto seguido se escoge una ruta dinámica de preferencia correspondiente a la interfaz Em0, con una dirección IP equivalente a 40.0.0.5/30.

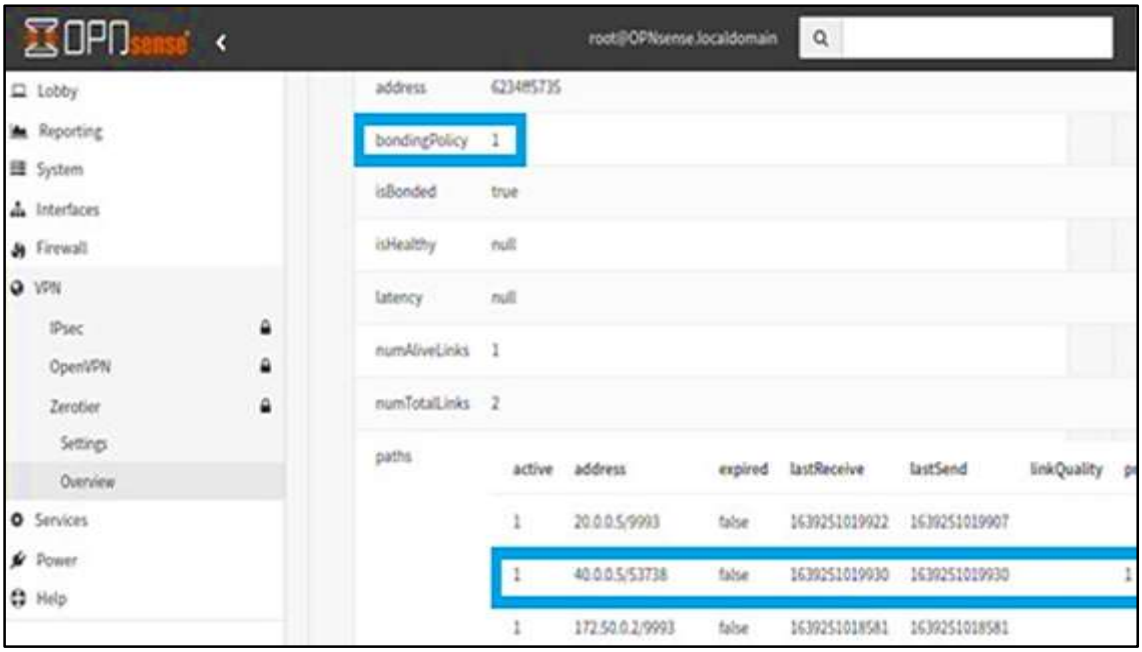


Figura 17-2: Información general de las conexiones ZeroTier

Realizado por: García, Luis, 2022.

Para realizar la configuración de Balance-XOR, los pasos a seguir son similares con respecto a la política estándar, misma que se detalla a continuación.

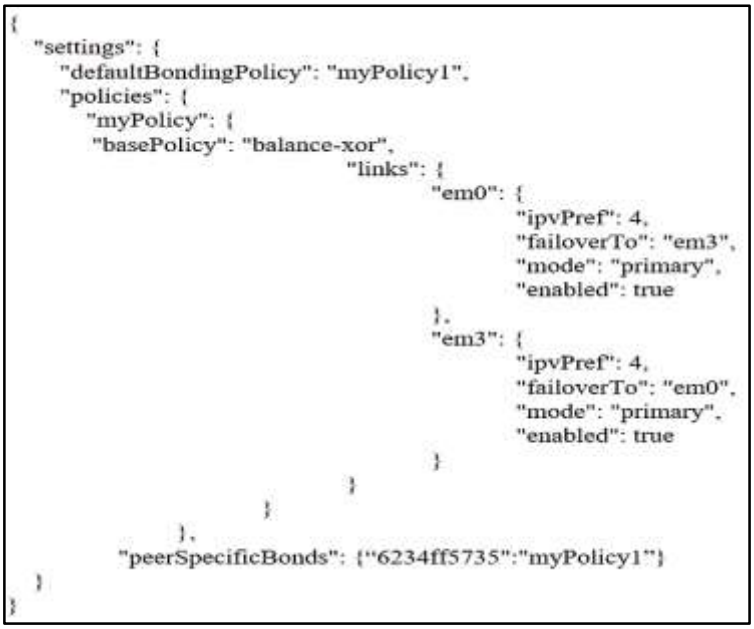


Figura 18-2: Política estándar balance-xor

Realizado por: García, Luis, 2022.

Dentro de la política estándar Balance-xor se detallan los enlaces Em0 y Em3 correspondientes a la interfaz WANA y WANB respectivamente. Estos enlaces se encuentran en modo primario, es decir, que se encuentran activos al mismo tiempo, razón por la cual los paquetes transitados por estos enlaces lo van a hacer de una manera equilibrada.

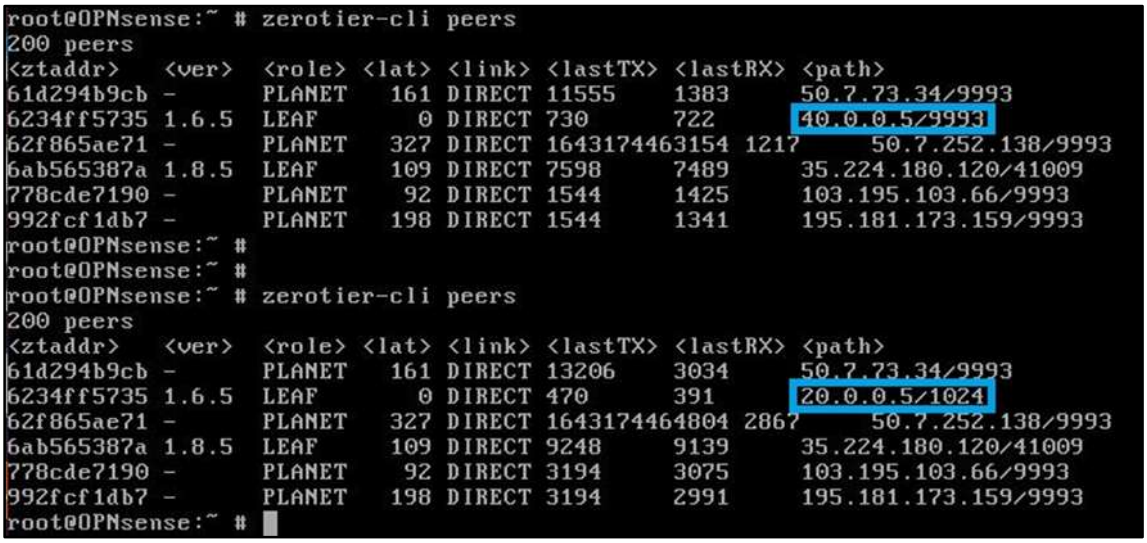


Figura 19-2: Balanceo Xor

Realizado por: García, Luis, 2022.

Como se muestra en la figura 18-2, en los equipos OPNSENSE por medio del Shell se realiza una consulta ¨***ZeroTier-cli peers***¨ y se puede observar que para conectarse a el nodo con un **ID: 6234ff5735.** Se tiene dos caminos tanto la ***40.0.0.5*** y la ***20.0.0.5*** y se comprueba que el envío y recepción de paquetes se realiza secuencialmente por cada interfaz activa.

Finalmente se procede a detallar las reglas de ZeroTier, donde se tiene que el motor de reglas de dicha aplicación asemeja un firewall, mismo que puede ser configurado en la interfaz de ZeroTier Central que se encuentra alojada en la nube, lo que brinda al administrador de red múltiples funciones, entre las cuales se enlista, la posibilidad de realizar el cambio de conexión entre los nodos y permitir el acceso a la red. En este paso, fue necesario realizar varias pruebas, para poder llevar a cabo, el etiquetado entre departamentos de cada sitio es preciso mencionar que, para esto, se tomó como base la siguiente configuración.

```
# Drop all Ethernet frame types that are not IPv4 or IPv
drop
        not ethertype ipv4
        and not ethertype arp
        and not ethertype ipv6
;
```

Figura 20-2: Etiquetado entre departamentos

Realizado por: García, Luis, 2022.

El comando #declaracion de etiquetas, permite asignar tanto un nombre como una ID aleatoria a la clase y cada etiqueta. A continuación, se presenta la sintaxis en cuestión.

```
tag departament
  id 2
  enum 100 VentasSR
  enum 200 VentasSE
  enum 300 FinanzasSR
  enum 400 FinanzasSE
  default NO; #No utilizar valores por defectos
```

Figura 21-2: Declaración de etiquetas

Realizado por: García, Luis, 2022.

Por último, se tiene el comando #regla de control de acceso a puertos, cuya sintaxis es la siguientes.

```
drop not ipprotocol tcp; # Denegar el servicio de todos los paquetes TCP.
accept dport 80 and tseq departament 300;
accept dport 22 and tseq departament 400; #Aceptar puertos TCP para el envio de paquetes.
accept dport 21 and tseq departament 400; #tseq permite que los equipos con la etiqueta del departamento 400 envien paquetes
#accept dport 22 and tseq departament 300;
#accept dport 22 and tseq departament 200;
drop chr tcp_syn and not chr tcp_ack; # Deniega los paquetes TCP. Elimina los paquetes no explicados en la lista blanca.
                                      # tcp_syn los paquetes nunca coincidiran con paquetes que no sean TCP.
                                      # tcp_ack Acuse de recibo del paquete.
```

Figura 22-2: Comando para acceso a puertos

Realizado por: García, Luis, 2022.

La configuración descrita permite entrever, la capacidad que tiene ZeroTier para el etiquetado por departamentos, en ZeroTier Central se despliega una casilla, a través de la cual se da la verificación que tanto el Nodo A y el Nodo B, se encuentran en el mismo departamento por lo tanto la conexión se dará satisfactoriamente, cuando existe un cambio entre los departamentos la conexión se anula automáticamente. Véase Anexo B

2.2.3.4 Red comparativa

La red que se describe a continuación servirá como comparativa con respecto a la red propuesta de ZeroTier. Misma que estará compuesta por dos equipos PFSENSE, que actuará como routers de borde, para enrutamiento dinámico se utiliza OSPF, la configuración y direccionamiento de cada uno de los routers de los proveedores de internet es la misma que se presentó en la tabla 7-2, para llevar a cabo la conexión entre los sitios, se realizará mediante el protocolo OPENVPN.

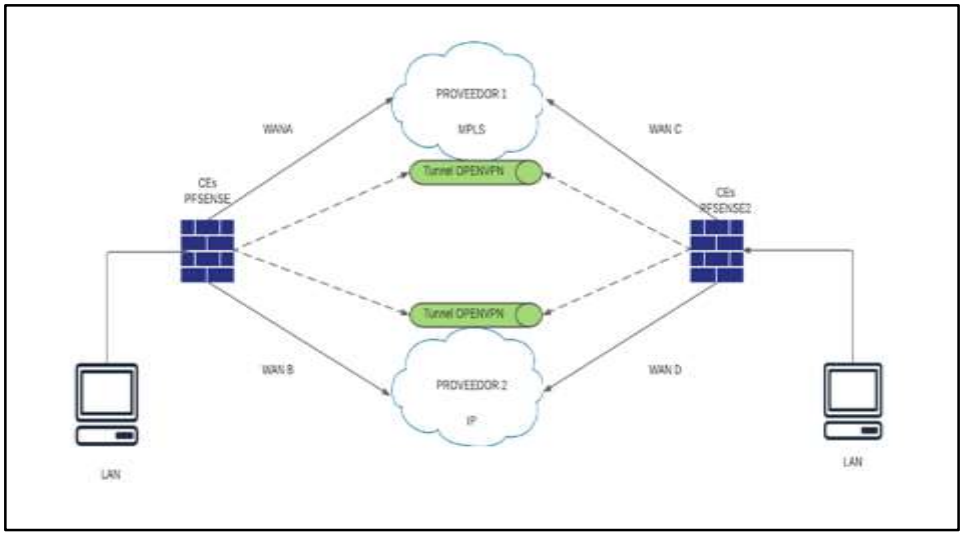


Figura 23-2: Red comparativa

Realizado por: García, Luis, 2022.

Los PFSENSE permiten brindar seguridad a entornos sean estos domésticos o empresariales, cumplen la función de un firewall, no obstante, también pueden ser empleados como equipos Ces,

lo que permite entrever una de sus características principales es la disponibilidad de diversas configuraciones avanzadas (DE LUZ, 2021). Para efecto de este estudio, los PFSENSE, contienen el siguiente direccionamiento.

Tabla 5-2: Direccionamiento de los equipos CEs

Sitio	*Equipo*	*Interfaz*	*Dirección IP*	*Máscara*
SITIO A	CE1 PFSENSE1	Em0	30.0.0.5/30	255.255.255.252
		Em3	10.0.0.5/30	255.255.255.252
		Em1	192.168.10.1/24	255.255.255.0
	CLIENTE 1	Eth0	192.168.10.10/24	255.255.255.0
SITIO B	CE2 PFSENSE2	Em0	40.0.0.5/30	255.255.255.252
		Em3	20.0.0.5/30	255.255.255.252
		Em1	192.168.50.1/24	255.255.255.0
	CLIENTE 2	Eth0	192.168.10.10/24	255.255.255.0

Realizado por: García, Luis, 2022.

OPENVPN, es una herramienta empleada para el diseño de redes virtuales privadas, este cuenta con un canal de control, que facilita la gestión de levantamiento de túnel, adicionalmente, las negociaciones de protocolos cifrados. Finalmente se puede identificar un canal de datos, para proceder con la verificación del tráfico del túnel, mismo que estará cifrado punto por punto (JIMÉNEZ, 2020).

Para configurar el túnel OPENVPN entre el Sitio A y el Sitio B, se deben asignar los siguientes parámetros de negociación.

Tabla 6-2: Parámetros de negociación del túnel OPNVPN en PFSENSE1

Propiedades del Túnel	**PFSENSE1**	
	Server 1	**Server 2**
Modo de Servidor	Peer to peer clave compartida	Peer to peer clave compartida
Modo del dispositivo	Tun-Capa 3	Tun-Capa 3
Interfaz	WAN A	WAN B
Puerto	1194	1195
Algoritmo de Cifrado	AES-256-GCM AES 128-GCM	AES-256-GCM AES 128-GCM
Algoritmo Hashing	SHA256(256bit)	SHA256(256bit)
Red de túnel Ipv4	50.0.0.8/30	60.0.0.8/30

Realizado por: García, Luis, 2022.

Tabla 7-2: Parámetros de negociación del túnel OPNVPN en PFSENSE2

Propiedades del Túnel	PFSENSE2	
	Cliente 1	Cliente 2
Modo de Servidor	Peer to peer clave compartida	Peer to peer clave compartida
Modo del dispositivo	Tun-Capa 3	Tun-Capa 3
Interfaz	WAN C	WAN D
Puerto	1194	1195
Host del Servidor	192.168.10.10	192.168.10.10
Algoritmo de Cifrado	AES-256-GCM AES 128-GCM	AES-256-GCM AES 128-GCM
Algoritmo Hashing	SHA256(256bit)	SHA256(256bit)
Red de túnel Ipv4	50.0.0.8/30	60.0.0.8/30

Realizado por: García, Luis, 2022.

Se procede con la configuración de las reglas de Firewall dentro de los dos equipos PFSENSE, con la finalidad de realizar el levantamiento del tunel OpenVpn, para lo cual, se utiliza el puerto por defecto 1194, la conexión se debe ajustar mediante el protocolo UDP.

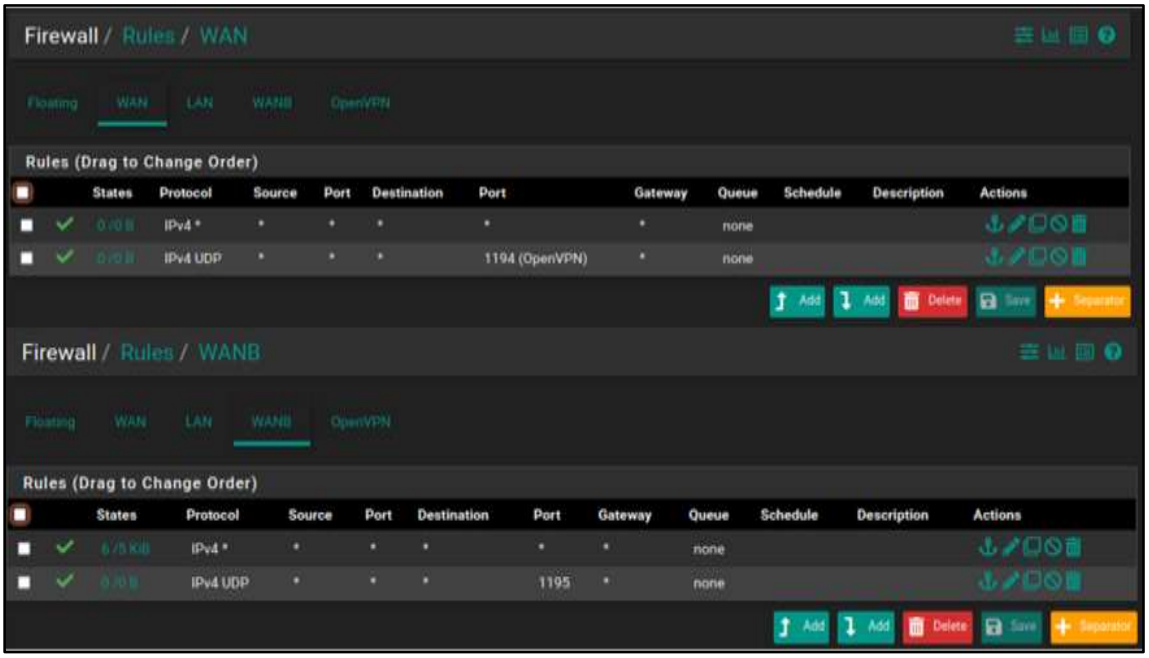


Figura 24-2: Configuración de Firewall interfaz WAN A-WAN B

Realizado por: García, Luis, 2022.

Dentro de la interfaz LAN se realiza la siguiente configuración, eligiendo como gateway a, FO_BOSS, que consiste en un grupo de gateways, en donde agrupa la WANA y la WANB con el fin de tener alta disponibilidad. A continuación, se presenta la Configuración del Firewall Interfaz LAN.

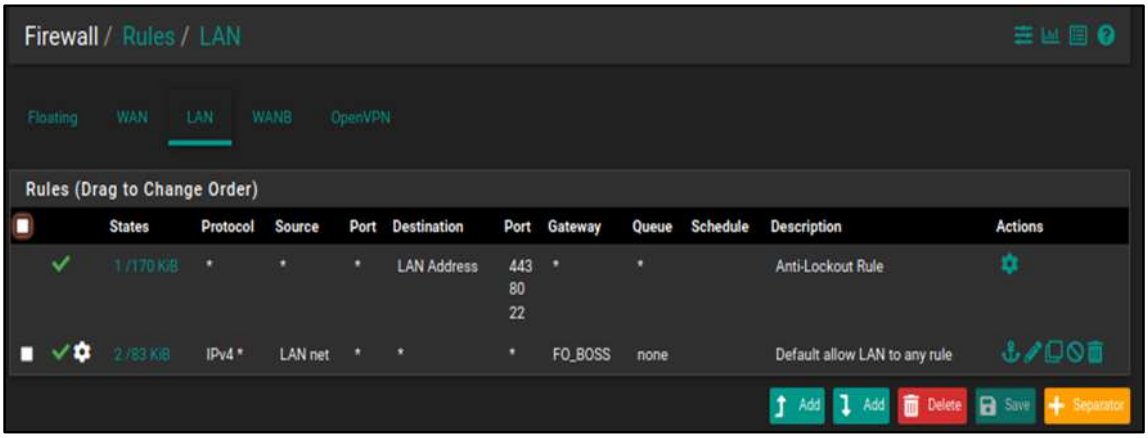


Figura 25-2: Configuración de Firewall interfaz LAN

Realizado por: García, Luis, 2022.

Las reglas de OpenVpn se debe autorizar por medio del protocolo TCP, la conectividad desde la red del tunel ipv4.

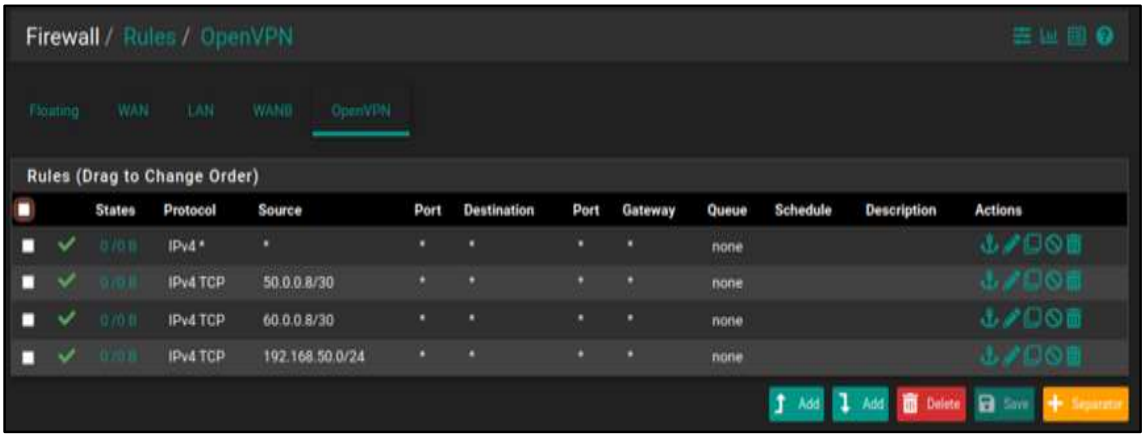


Figura 26-2: Configuración de Firewall interfaz OpenVpn

Realizado por: García, Luis, 2022.

2.2.4 Verificación

2.2.4.1 Comunicación entre los nodos

Con la finalidad de poder verificar la conexión del túnel entre los equipos del sitio A y B, se ejecuta una experimentación, la cual consiste en poner a prueba de ping, lo que permitirá constatar la conectividad entre dichos sitios.

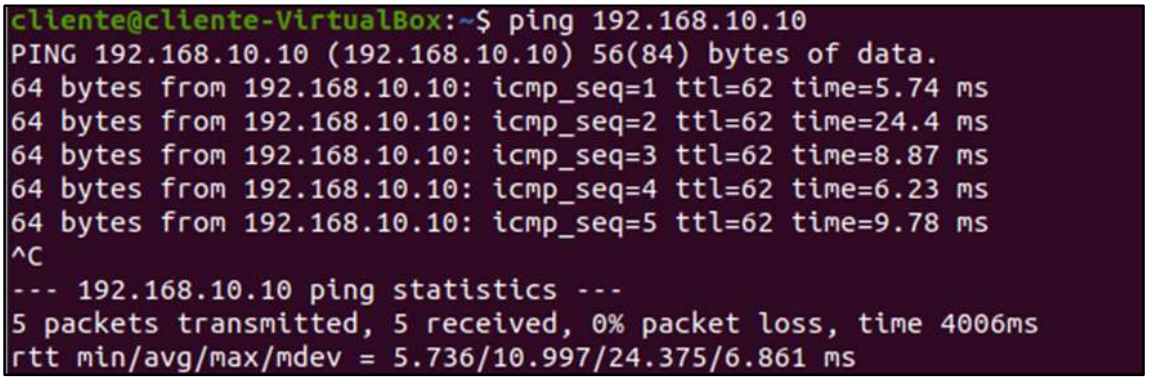


Figura 27-2: Comunicación cliente-servidor

Realizado por: García, Luis, 2022.

Tomando en consideración que ZeroTier crea redes virtuales con el fin de poder enrutar el tráfico a una dirección IP creada por el mismo, para efectos del presente estudio, se decide trabajar con la dirección 172.22.246.51/16 para el sitio A, mientras que, para el sitio B 172.22.174.165/16. A continuación se muestra la ruta trazada utilizando el comando ***Traceroute.***

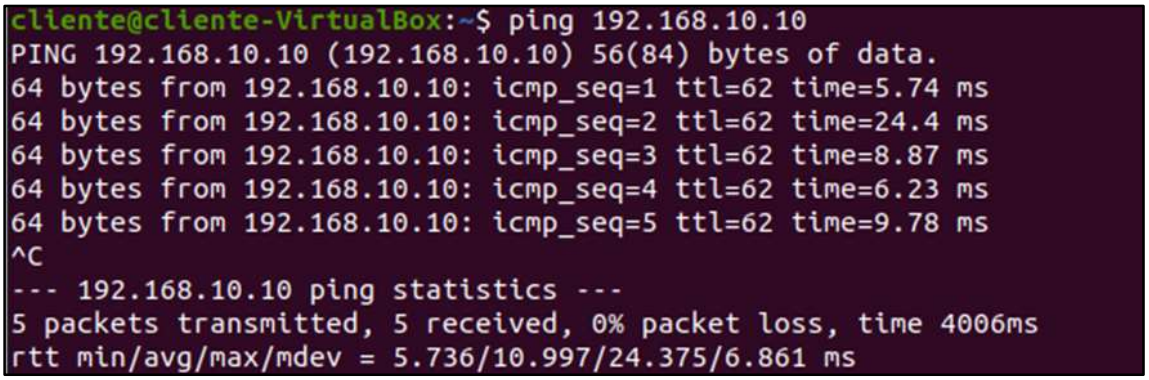


Figura 28-2: Saltos desde el sitio A al sitio B mediante ZeroTier

Realizado por: García, Luis, 2022.

En la figura 28-2, es posible apreciar que los paquetes, son enviados desde equipo cliente, los cuales circularan por la puerta de enlace con la dirección 192.168.10.1. para posteriormente recalar en los servidores de ZeroTier, mediante túnel con una dirección de 172.22.246.51, con lo cual, el paquete llegue al destino y alcanza el host remoto.

El tablero de control del OPNSENSE ofrece varias opciones para realizar el monitoreo de la red, como son paquetes en bytes, tanto recibidos como enviados, el tiempo en RTT (Tiempo trascurrido desde el envío de paquetes desde el origen hacia el destino, también se le denomina latencia) de los enlaces WAN, y las gráficas del tráfico de la red.

Figura 29-2: Tablero de control de OPNSENSE

Realizado por: García, Luis, 2022.

Con la información concerniente al RTT y RTTsd, los equipos CEs OPNSENSE proceden con la verificación del estado de los enlaces, con lo cual, se puede tener un control sobre la calidad de los enlaces, lo que consiste en poder determinar que enlace se encuentra saludable. Según OPNSENSE, se considera un enlace es defectuoso cuando las pérdidas de paquetes corresponden al 20%. y un RTT de más de 500ms.

Los aspectos antes mencionados sobre integridad del enlace se corroboran a través de las reglas establecidas para la evaluación de la carga de enlaces, donde se deja por sentado que en umbrales con índice de pérdidas de 20%, estos adquieren la consideración de inactivo y de igual manera para aquellos que presentan una latencia de 500 ms (TECH EXPERT, 2022).

Antes de comenzar a hacer las pruebas de comunicación, conviene revisar si los dos equipos CEs, tanto como el OPNSENSE1 y el OPNSENSE2 están encapsulando correctamente el tráfico. ZeroTier utiliza tres puertos UDP que permiten estar en modo escucha.

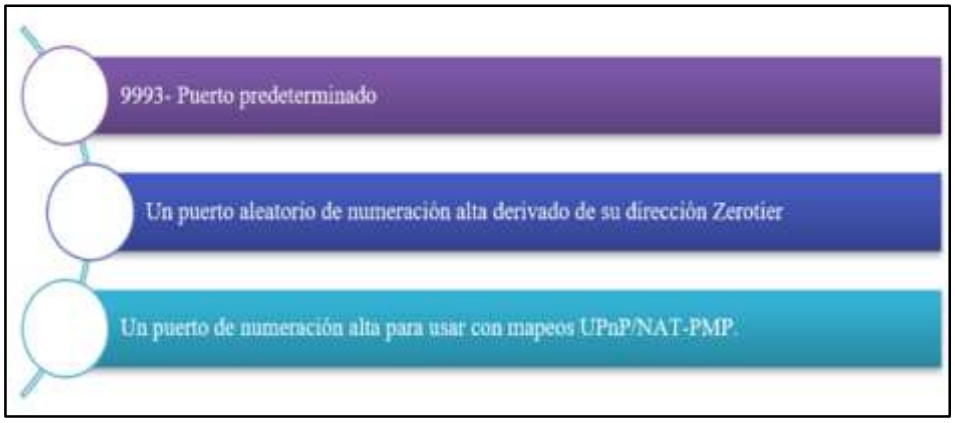


Figura 30-2: Puertos UDP - ZeroTier

Realizado por: García, Luis, 2022.

Mediante la Herramienta analizador de protocolos Wireshark (véase Anexo C), se comprueba haciendo una captura de tráfico y se obtiene lo siguiente.

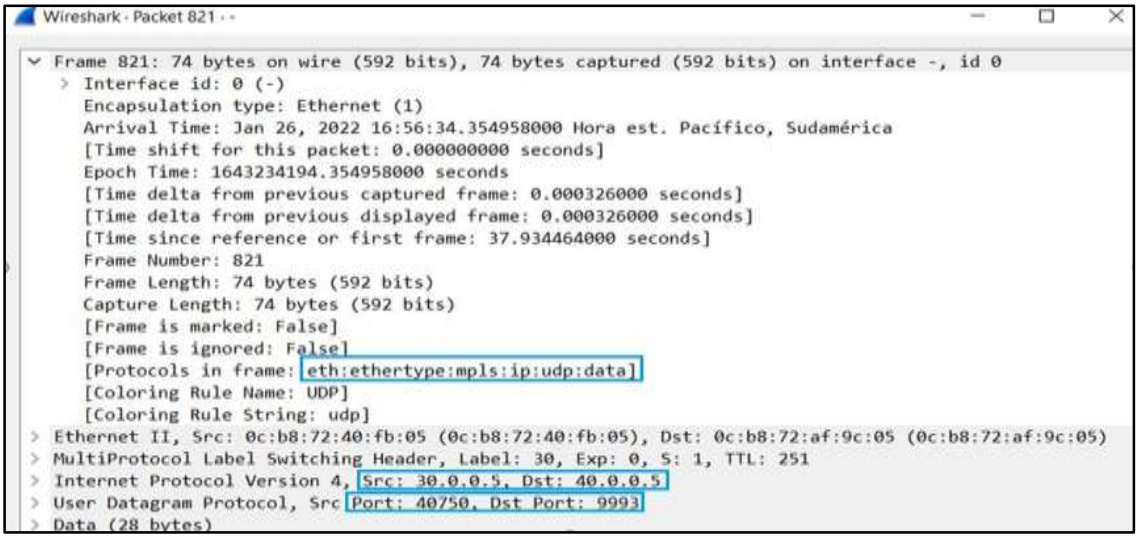


Figura 31-2: Analizador de protocolos Wireshark – Proveedor 1

Realizado por: García, Luis, 2022.

En la figura 31-2, se puede apreciar la captura de los paquetes mediante la herramienta Wireshark, esta captura se realizó en el interior de la red Mpls, correspondiente al proveedor1. los protocolos existentes en la trama como lo es el etiquetado Mpls, el medio de transporte del paquete que se realiza mediante UDP. Dentro del protocolo Ipv4 se muestra la dirección de origen es 30.0.0.5, que es la dirección del OPNSENSE del sitio A, mientras que la dirección de destino es 40.0.0.5 que corresponde al OPNSENSE del sitio B. El protocolo donde se transporta ZeroTier es mediante UDP, el puerto de origen es un puerto UDP 40750, hacia un puerto de destino 9993 que utiliza ZeroTier para la comunicación.

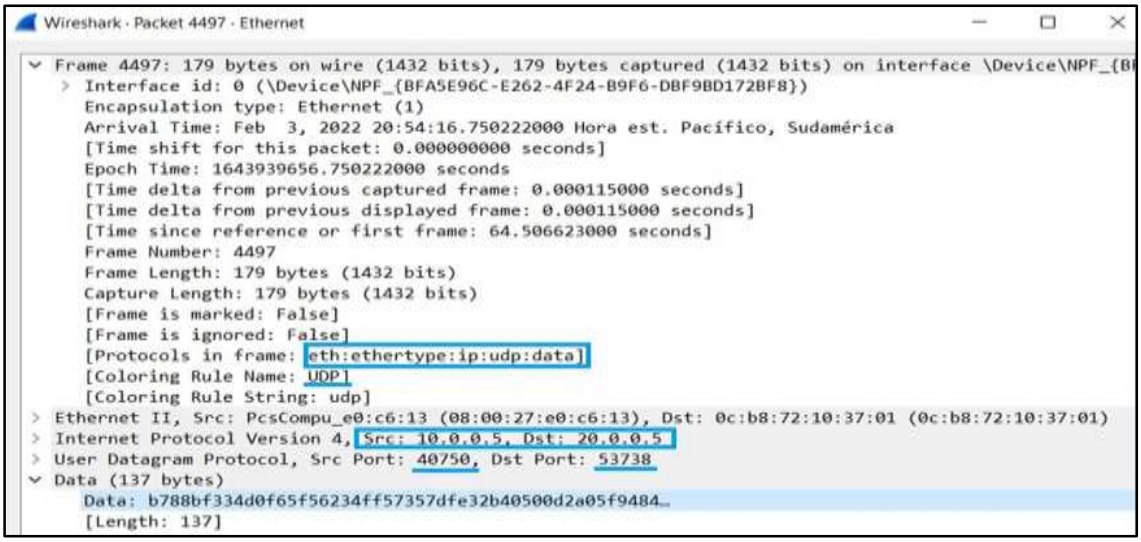


Figura 32-2: Analizador de protocolos Wireshark – Proveedor 2

Realizado por: García, Luis, 2022.

En la figura 28-2, se visualiza la captura de los paquetes mediante la herramienta Wireshark, mismas que hace referencia al proveedor2. los protocolos existentes en la trama son Ethernet, el protocolo Ipv4, y el medio de transporte del paquete UDP. Se puede apreciar que la dirección de origen 10.0.0.5 corresponde a la interfaz Wan del sitio A, debido a que mediante esa interfaz realiza el enrutamiento a través de ZeroTier para llegar al destino que es la dirección 20.0.0.5 correspondiente al OPNSENSE del Sitio B.

Dentro de la interfaz de OPNSENSE, se encuentra una herramienta que permite capturar del tráfico, lo que coadyuba con en la tarea de determinar que protocolos se encuentran dentro de sus enlaces. Para ello se utilizó la herramienta Packet Capture, con el fin de capturar el tráfico del túnel ZeroTier que se genera de sitio a sitio, como se muestra a continuación.

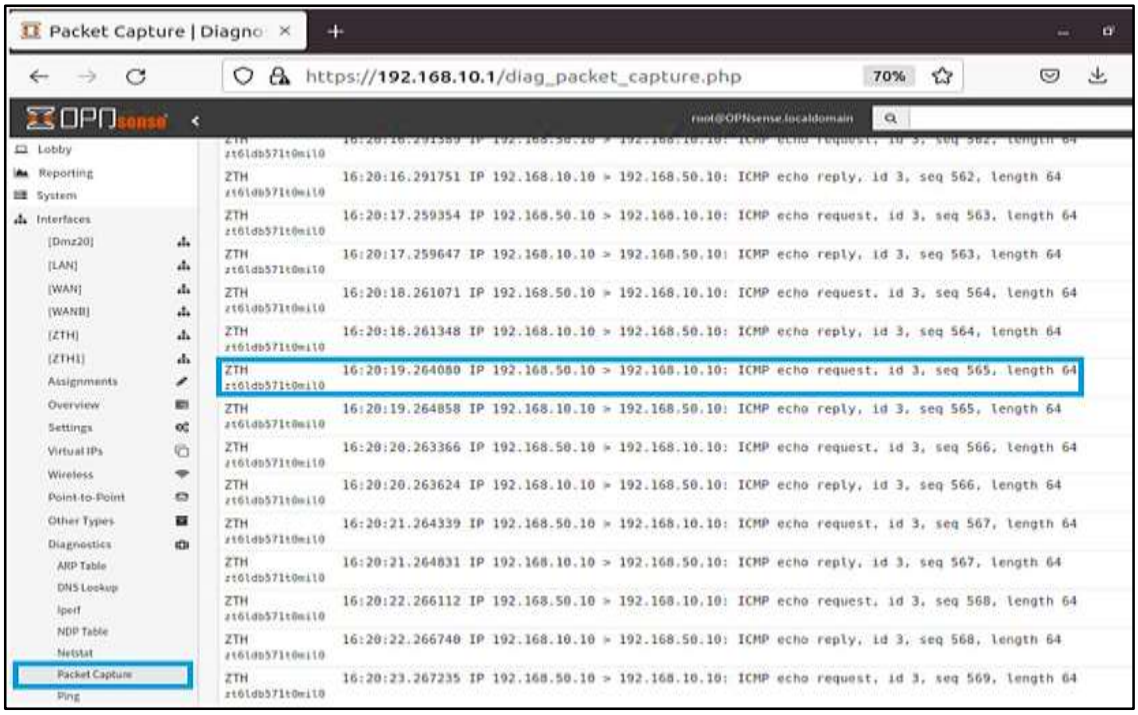


Figura 33-2: Captura realizada desde el OPNSENSE del sitio 1

Realizado por: García, Luis, 2022.

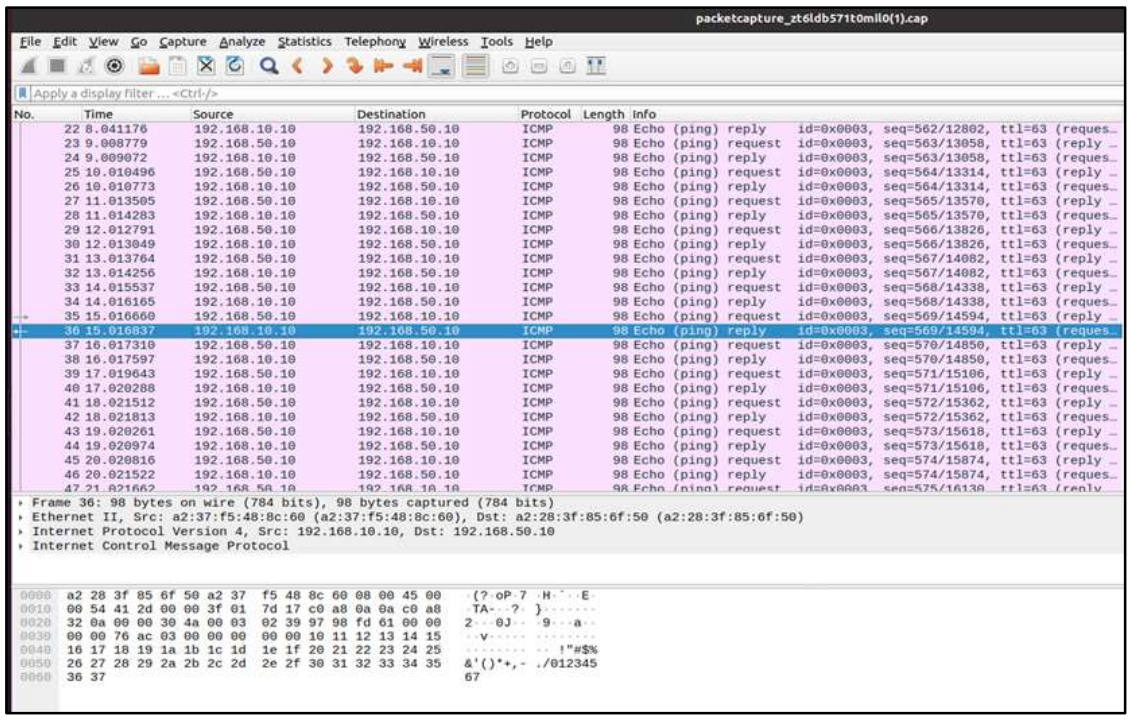


Figura 34-2: Tráfico capturado desde Wireshark Linux

Realizado por: García, Luis, 2022.

A continuación, en la figura 35-2, se observa la Trama del túnel, donde indica la dirección Mac de origen del Cliente con dirección a la Mac de destino del servidor, a su vez se detalla el protocolo que se está usando como es el ICMP.

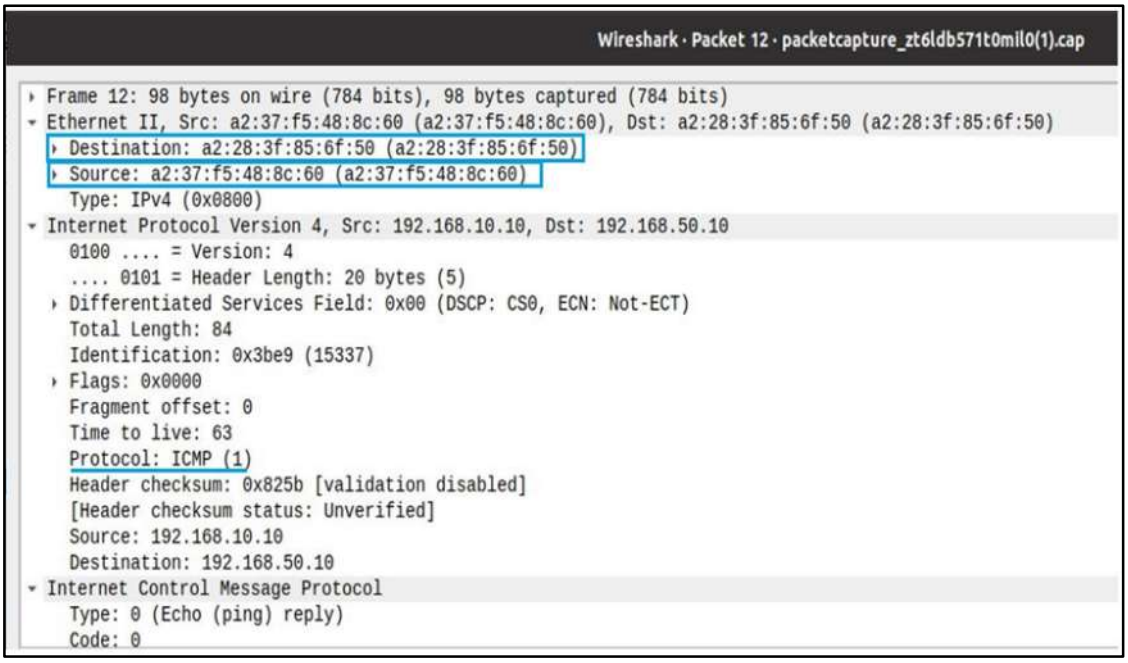


Figura 35-2: Protocolos que intervienen en la trama

Realizado por: García, Luis, 2022.

A continuación, en la figura 36-2, se muestra la interfaz 10.0.0.5, la cual corresponde al OPNSENSE del sitio A, se realiza la conexión mediante el protocolo UDP con los servidores lunares de ZeroTier alojados en la nube, dicho servidor se identifica con la dirección 195.181.173.159.

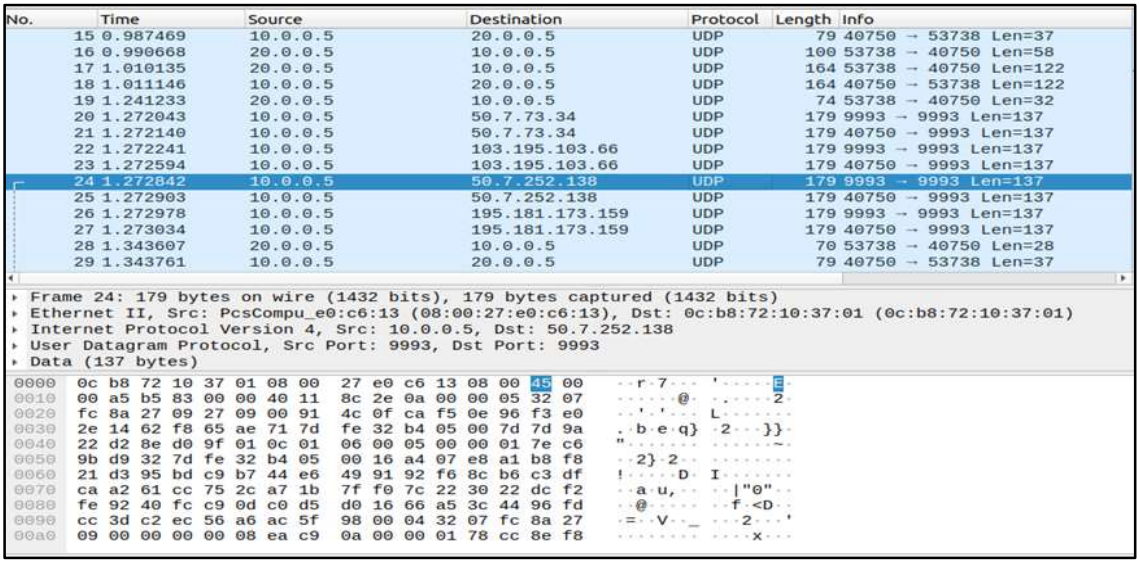
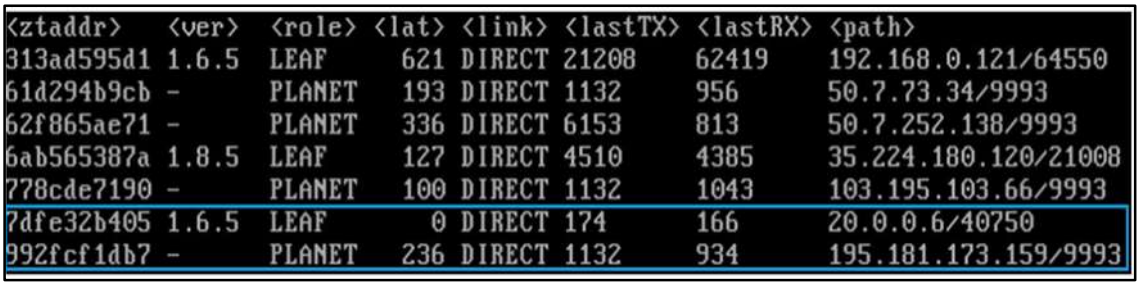


Figura 36-2: Conexión entre los nodos y los servidores planetarios

Realizado por: García, Luis, 2022.

Una vez que se conectan a los servidores planetarios, se negocia esa conexión para poder realizar la perforación UDP, la conexión con estos servidores tiene la finalidad de poder tener redundancia. A continuación, se presentan la conexión de los nodos con los servidores planetarios.



<ztaddr>	<ver>	<role>	<lat>	<link>	<lastTX>	<lastRX>	<path>
313ad595d1	1.6.5	LEAF	621	DIRECT	21208	62419	192.168.0.121/64550
61d294b9cb	-	PLANET	193	DIRECT	1132	956	50.7.73.34/9993
62f865ae71	-	PLANET	336	DIRECT	6153	813	50.7.252.138/9993
6ab565387a	1.8.5	LEAF	127	DIRECT	4510	4385	35.224.180.120/21008
778cde7190	-	PLANET	100	DIRECT	1132	1043	103.195.103.66/9993
7dfe32b405	1.6.5	LEAF	0	DIRECT	174	166	20.0.0.6/40750
992fcf1db7	-	PLANET	236	DIRECT	1132	934	195.181.173.159/9993

Figura 37-2: Conexión de los nodos con los servidores planetarios

Realizado por: García, Luis, 2022.

2.3 Método de generación de tráfico

La manera en la que se va a generar el tráfico es mediante un servidor web dentro de una máquina virtual con el sistema operativo Ubuntu 20.0.4 LTS, utilizando la herramienta Apache 2. El protocolo a utilizar es Http, debido a que la gran parte de las empresas utilizan la web como medio de comunicación y gestión de recursos (MARÍN, 2015).

La figura 38-2, muestra el archivo de configuración del servidor apache se encuentra alojado dentro del directorio /var/www/html.

Figura 38-2: Configuración del servidor web

Realizado por: García, Luis, 2022.

En el servidor web se aloja un archivo de 20 MB la cual nos permitirá hacer la descarga cliente-servidor y poder simular el tráfico de extremo a extremo

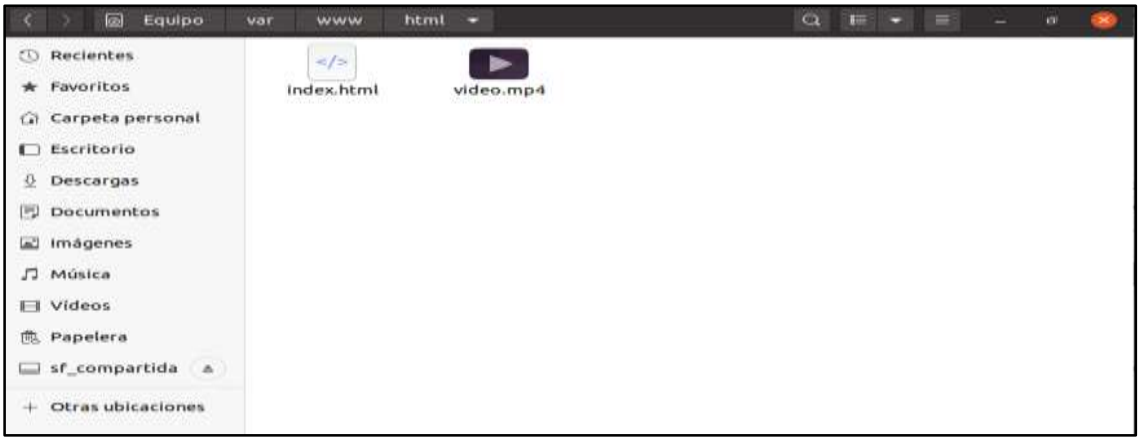


Figura 39-2: Archivos dentro del directorio html para la descarga por servidor web

Realizado por: García, Luis, 2022.

Figura 40-2: Vista del servidor web utilizando el navegador Firefox

Realizado por: García, Luis, 2022.

CAPÍTULO III

3. MARCO DE RSULTADOS Y DISCUSIÓN DE LOS RESULTADOS

En esta parte del trabajo de investigación se realizarán pruebas para verificar el correcto funcionamiento de la red SD-WAN, las mismas que permitirán validar las ventajas de la tecnología SD-WAN utilizando el *software* ZeroTier.

Tras desarrollarse la arquitectura de red SD – WAN, en esta sección se procede a demostrar el comportamiento de la red, con indicadores tales como Administración de la red, Conexión de túneles dinámicamente, Balanceo de carga y la disponibilidad de la red, de igual manera en los resultados se hace referencia a la medición del parámetro de alta disponibilidad utilizando el método del Failover, estos parámetros son obtenidos en la red SD – WAN (ZeroTier), mismos que serán comparados con el comportamiento de una red WAN utilizando como mecanismo de conexión (OpenVPN).

3.1 Administración de la red

Para poder verificar la administración de la red SD-WAN, ZeroTier se contará con un control de reglas de flujo en el controlador de red, y a su vez una microsegmentación de esta. Para ello se tiene como ejemplo lo siguiente, permitir el tráfico entre los dispositivos que pertenecen a la red Finanzas.

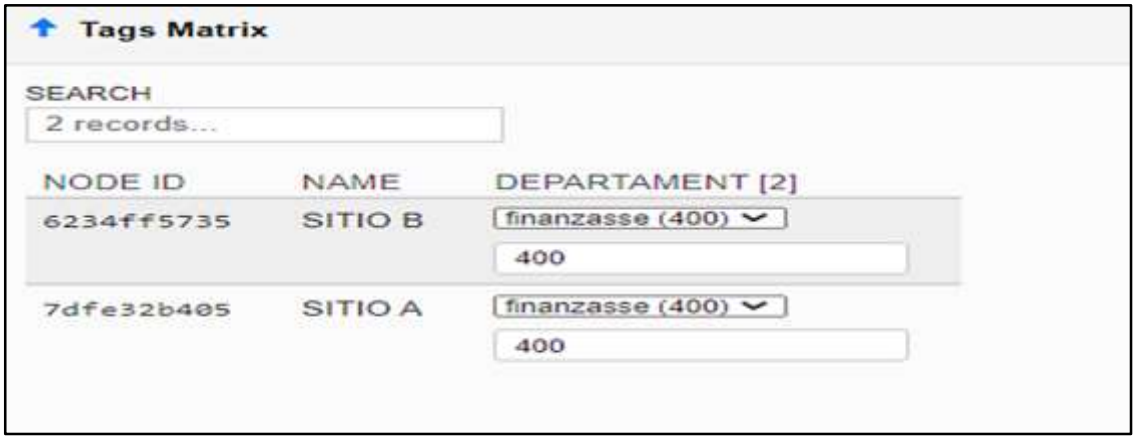


Figura 1-3: Etiquetado en el control de reglas de flujo ZeroTier

Realizado por: García, Luis, 2022.

Cada Dispositivo consta con un ID de nodo único a nivel de ZeroTier, el mismo que sirve para poder administrar la red, como se aprecia en la figura 1-3, se esta permitiendo el acceso entre los nodos que pertenecen a la etiqueta finanzas con ID igual a 400. Esta configuración se encuentra

en el apartado (Configuración). La conexión se la verificó mediante el protocolo SSH, como se muestra en la figura 2-3:

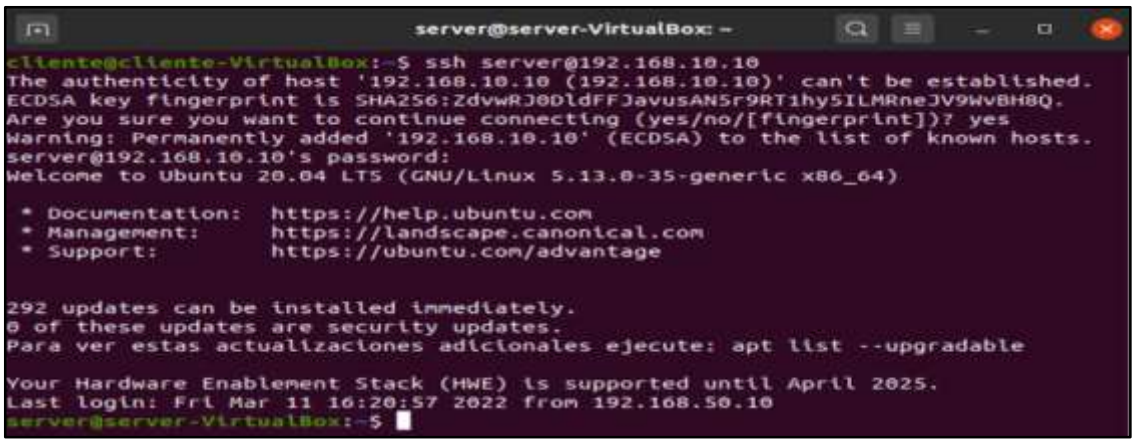


Figura 2-3: Conexión de los sitios mediante SSH utilizando etiquetas

Realizado por: García, Luis, 2022.

3.2 Conexión de túneles

ZeroTier crea una superposición virtual de túneles dinámicamente utilizando una dirección privada virtual, dentro del análisis de la red, se tiene que ZeroTier encapsula el tráfico de la red Lan por medio de la dirección virtual creada en ZeroTier central, con la finalidad de mantener los enlaces WAN existentes y permitir una gestión ágil del tráfico a través de estos enlaces.

Para analizar el control de la ruta de ZeroTier se acude a los OPNSENSE, se verifica a través de dos métodos, el primero realizando una consulta por medio del Shell con la siguiente instrucción: Zerotier-Cli peers, con esto se comprueba que ruta está actuando como principal.

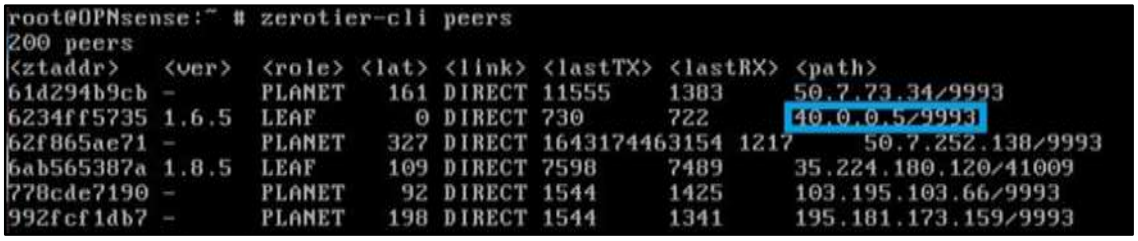


Figura 3-3: Lista de Peers ZeroTier

Realizado por: García, Luis, 2022.

Como segundo método se utiliza la herramienta TCPDUMP, la misma que sirve para capturar tráfico en tiempo real, para poder verificar que enlace WAN es el que se encuentra activo el túnel de ZeroTier.

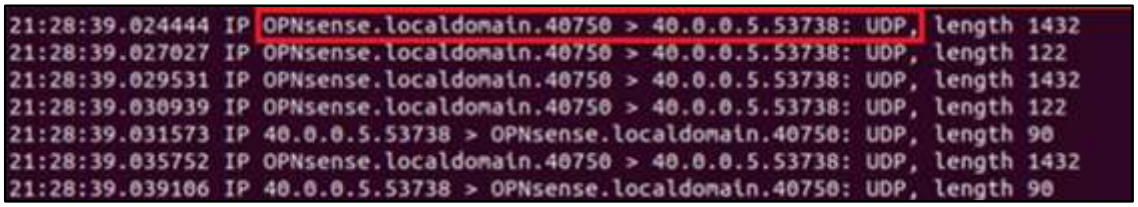


Figura 4-3: Conexión peer to Peer

Realizado por: García, Luis, 2022.

En la figura 3-3, se muestra la conexión Peer to peer mediante ZeroTier, la cual refleja que OPNSENSE.Local.domain.40750 pertenece al OPNSENSE del Sitio A mientas que la dirección 40.0.0.5 pertenece la WAN A del OPNSENSE correspondiente al sitio B, esta conexión se la realiza mediante el puerto UDP 40750.

Figura 5-3: Prueba de ping y acceso al servicio en el servidor web

Realizado por: García, Luis, 2022.

3.3 Balanceo de carga

Para poder evidenciar el comportamiento del balanceo de carga en la red SD-WAN, se dispone de dos enlaces Wan con salida a internet conectados a los equipos de borde OPNSENSE. ZeroTier brinda políticas de enrutamiento, una de ellas es el balanceo-Xor, dicho comportamiento se muestra en la figura 6-3, realizando una consulta por medio del Shell del equipo se tiene.

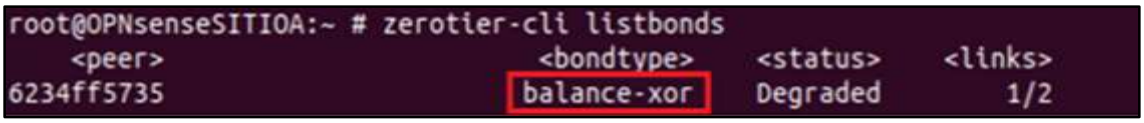


Figura 6-3: Lista de bonding ZeroTier

Realizado por: García, Luis, 2022.

Dentro del tablero de monitoreo del ZeroTier, se puede verificar el bonding Policy = 4, mismo que concierne al Balanceo-xor.

Figura 7-3: ZeroTier Overview

Realizado por: García, Luis, 2022.

Se realizan envíos de peticiones simultaneas, dicho comportamiento queda registrado en los Logs de los equipos OPNSENSE, donde se verifica que las conexiones se realizan aleatoriamente desde el sitio B con la dirección 40.0.0.5 para la WAN A y la dirección 20.0.0.5 correspondiente a la WAN B.

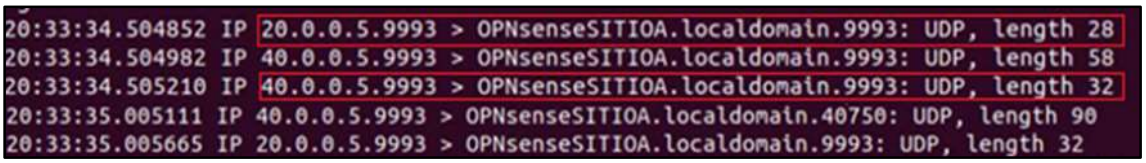


Figura 8-3: Balanceo Xor registrado en OPNSENSE

Realizado por: García, Luis, 2022.

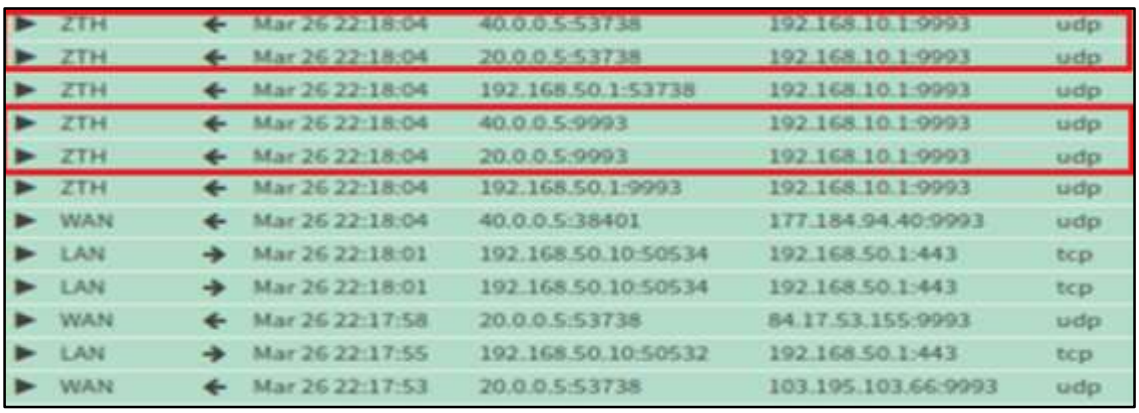


Figura 9-3: Captación de Logs en OPNSENSE

Realizado por: García, Luis, 2022.

3.4 Alta disponibilidad (Failover)

Para poder medir el Failover en la red se debe analizar el tráfico dentro de los equipos de borde como son los OPNSENSE, por medio de la herramienta TCPDUMP, se realizará el monitoreo a

través de la interfaz del túnel ZeroTier, para ello se escribe la siguiente instrucción: TCPDUMP -I zt6ldb571t0mil0, se verifica realizando descargas desde el cliente hacia el servidor web, mismo que se encuentra alojado un video de 20MB, con el propósito de poder medir el tiempo de disponibilidad en la red.

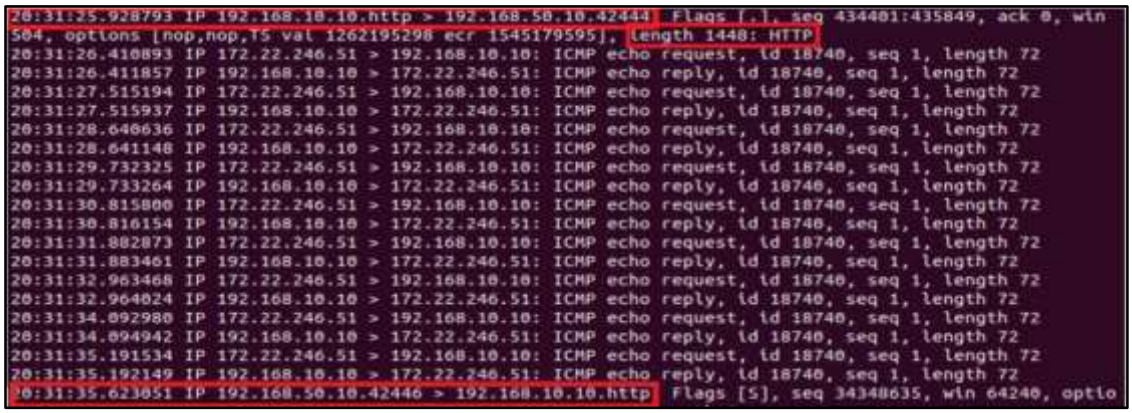


Figura 10-3: Conmutación del túnel dinámico ZeroTier

Realizado por: García, Luis, 2022.

SD-WAN aprovecha los múltiples enlaces existentes de proveedores de internet con el fin de escalar la capacidad y reducir costos que se presentan con los enlaces de datos, en la figura 11-3 se puede evidenciar que se logra la conmutación por error hasta 10 seg.

Si ZeroTier detecta que el enlace principal en OPNSENSE se encuentra nuevamente disponible, se vuelve a crear el túnel dinámicamente como se muestra a continuación.

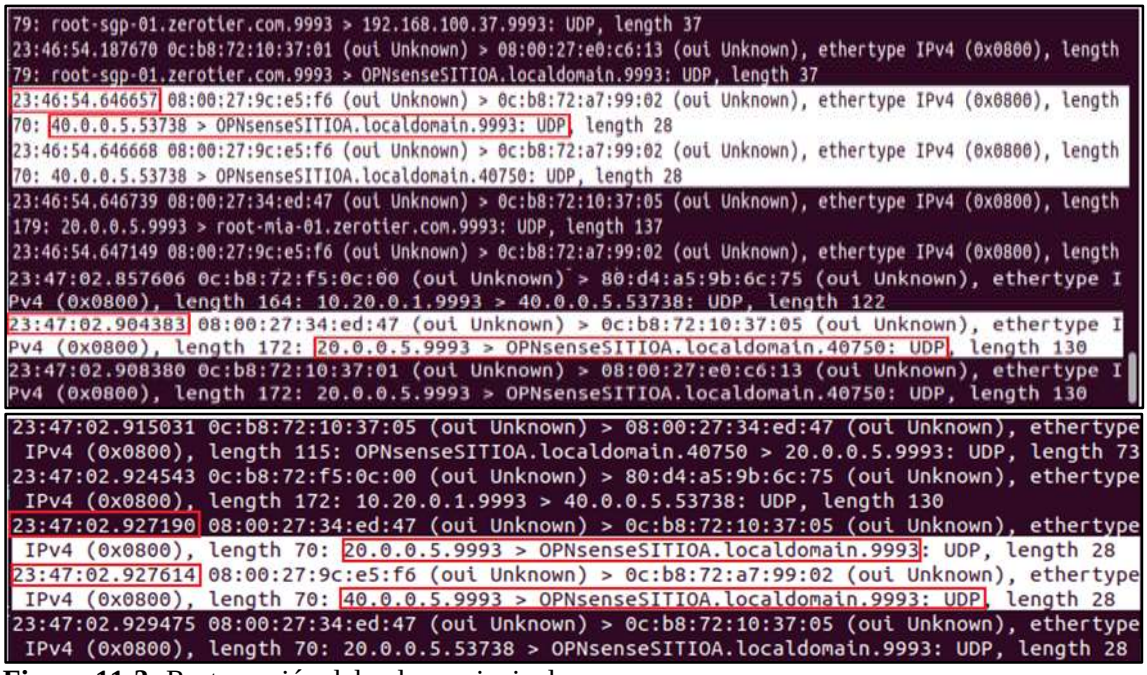


Figura 11-3: Restauración del enlace principal

Realizado por: García, Luis, 2022.

A continuación, se procede con el desarrollo de las pruebas de Failover, realizando 50 pruebas para poder determinar el comportamiento de la red SD-WAN, a su vez, comparar el tiempo de respuesta ante situaciones como altas latencias o el enlace se encuentre caído en su totalidad.

Tabla 1-3: Resultados de la prueba de disponibilidad

Tiempo Failover										
# Pruebas	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5	Prueba 6	Prueba 7	Prueba 8	Prueba 9	Prueba 10
Zerotier (seg)	6	11	12	7	11	10	11	9	8	9
OpenVpn (Seg)	20	24	22	22	21	34	28	25	27	27
Tiempo Failover										
# Pruebas	Prueba 11	Prueba 12	Prueba 13	Prueba 14	Prueba 15	Prueba 16	Prueba 17	Prueba 18	Prueba 19	Prueba 20
Zerotier (seg)	9	7	11	7	8	7	11	9	5	11
OpenVpn (Seg)	28	26	24	22	21	29	32	33	34	25
Tiempo Failover										
# Pruebas	Prueba 21	Prueba 22	Prueba 23	Prueba 24	Prueba 25	Prueba 26	Prueba 27	Prueba 28	Prueba 29	Prueba 30
Zerotier (seg)	13	10	10	8	11	7	8	6	9	10
OpenVpn (Seg)	26	20	28	24	21	23	28	25	26	25
Tiempo Failover										
# Pruebas	Prueba 31	Prueba 32	Prueba 33	Prueba 34	Prueba 35	Prueba 36	Prueba 37	Prueba 38	Prueba 39	Prueba 40
Zerotier (seg)	10	9	8	6	8	11	8	12	9	8
OpenVpn (Seg)	27	29	31	30	31	32	28	26	28	28
Tiempo Failover										
# Pruebas	Prueba 41	Prueba42	Prueba 43	Prueba 44	Prueba 45	Prueba 46	Prueba 47	Prueba 48	Prueba 49	Prueba 50
Zerotier (seg)	10	11	9	16	9	6	14	8	10	11
OpenVpn (Seg)	24	30	31	30	29	24	25	26	26	27

Realizado por: García, Luis, 2022.

Como se muestra en la tabla 1- 3, los tiempos obtenidos en ZeroTier Oscilan entre 5seg y 16sg, este último se detecta como tiempo más alto registrado, mientras que OpenVPN muestra entre 20seg y 34 seg, se demuestra que notoriamente OpenVpn supera en tiempos de respuesta, cuyos resultados son más altos con respecto a ZeroTier.

Gráfico 1-3: Tiempos de Failover ZeroTier

Realizado por: García, Luis, 2022.

Gráfico 2-3: Tiempos de Failover OpenVpn

Realizado por: García, Luis, 2022.

El uso de la navegación web corresponde a una prioridad media, ya que, al ser una aplicación disponible para los usuarios, pueden trabajar sin problema a pesar de los retardos que pueda presentar en la red.

Para poder realizar una muestra del tráfico utilizado, se recurre al protocolo http, lo cual, se explica, por el hecho que este es empleado a nivel mundial dentro del sector corporativo, mismo que establece un cuadro comparativo, mediante el cual, es posible identificar, las necesidades del tráfico IP.

APLICACIÓN	ANCHO DE BANDA	RETARDO	FLUCTUACIÓN DE RETARDO	ERRORES O PÉRDIDAS
Correo electrónico	*Baja*	*Baja*	*Baja*	*Alta*
Transferencia de archivo	*Alta*	*Baja*	*Baja*	*Alta*
Navegación Web	*Mediana*	*Mediana*	*Mediana*	*Alta*
Datos interactivos	*Baja*	*Baja*	*Baja*	*Alta*
Difusión de audio	*Mediana*	*Baja*	*Alta*	*Mediana*
Voz	*Mediana*	*Mediana*	*Alta*	*Baja*
Difusión de video	*Alta*	*Baja*	*Alta*	*Mediana*
Video y audio interactivo	*Alta*	*Mediana*	*Alta*	*Mediana*

Figura 12-3: Necesidades de los distintos tipos de tráfico para redes Ip

Realizado por: García, Luis, 2022.

Se realiza la prueba de normalidad denominada Shapiro-Wilk utilizando la herramienta excel, con la finalidad de poder constatar que los datos obtenidos registrados de la prueba de alta disponibilidad se distribuyen normalmente.

La prueba de Shapiro-Wilk plantea la hipótesis nula que las muestras provienen de una distribución normal, eligiendo un nivel de significancia de 0,05. Dando como hipótesis alternativa que sostiene que la distribución no es normal, con ello se tiene:

$$H_0: La\ distribución\ es\ normal$$

$$H_1: La\ distribución\ no\ es\ normal$$

Tabla 2-3: Resultados de la prueba de normalidad

Shapiro-Wilk Test		
	Zerotier	OpenVpn
	6	*20*
W-stat	0,95987782	0,978751395
p-value	0,093644692	0,514089912
alpha	0,05	0,05
normal	yes	yes

Realizado por: García, Luis, 2022

En los resultados en la Tabla 2-3, utilizando Zerotier y OpenVpn se muestra que el p-valor es mayor a 0,05, entonces se acepta la hipótesis nula (H_0), por lo que se afirma que los datos obtenidos se distribuyen siguiendo una normal. Se concluye que la media es una medida representativa en los datos obtenidos.

Para poder determinar el grado de significatividad estadística de las diferencias entre las medias de los datos obtenidos de la prueba de alta disponibilidad, se realiza la prueba Z.

Se plantea una hipótesis nula dando como indicador que los valores promedios son significativamente iguales, y una hipótesis alternativa la cual indica que los valores promedios son diferentes.

$$H_0 = u_1 - u_2 \geq 0$$
$$H_1 = u_1 - u_2 \ < 0$$

Tabla 3-3: Resultados de la prueba Z

Prueba z para medias de dos muestras		
	Zerotier	*OpenVpn*
Media	9,28	26,64
Varianza (conocida)	4,73632653	13,0514286
Observaciones	50	50
Diferencia hipotética de las medias	0	
z	-29,10543885	
P(Z<=z) una cola	0	
Valor crítico de z (una cola)	1,644853627	
Valor crítico de z (dos colas)	0	
Valor crítico de z (dos colas)	1,959963985	

Realizado por: García, Luis, 2022

En la tabla 3-3 se muestra que el valor de $Z_p = -29{,}105$ lo que significa que es mucho menor que el valor crítico correspondiente a $Z_c = -1{,}64485$, por lo tanto, se rechaza la hipótesis nula, con ello se puede afirmar que la media de los valores de los tiempos de la tecnología ZeroTier es menor que la media de los tiempos de OpenVpn con un nivel de confianza del 95%.

3.5 Comparaciones

3.5.1 Alta disponibilidad de ZeroTier con respecto a otras tecnologías (OpenVPN)

Con la intención de demostrar el parámetro disponibilidad de la red, se decide realizar un análisis comparativo, con otra tecnología. Es preciso mencionar que las redes WAN, no son suficientes para que puedan brindarle un servicio de calidad a sus usuarios, es entonces que se plantea comparar los resultados de las SD – WAN, a partir del indicador Failover.

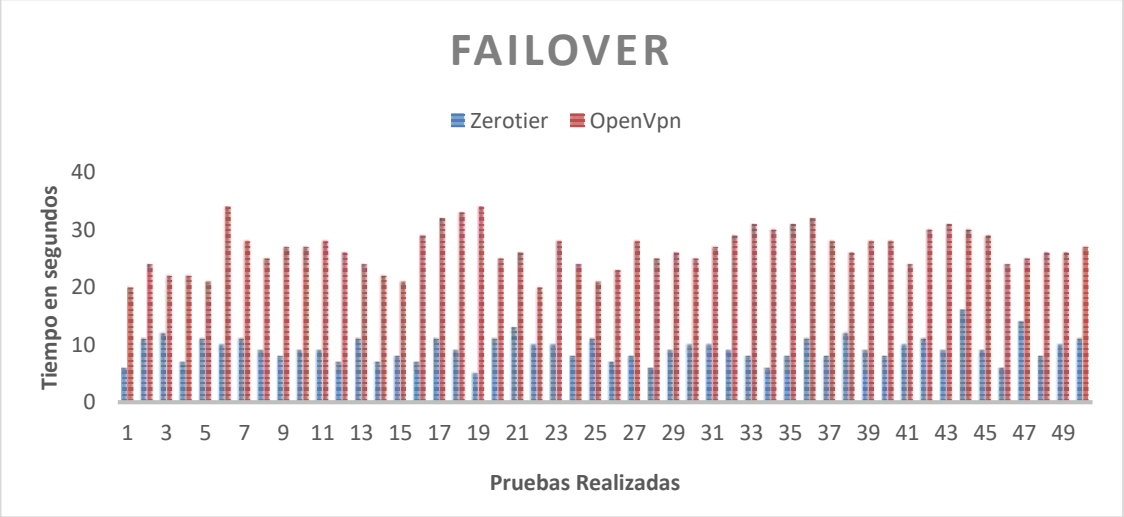


Gráfico 3-3: Comparación de tiempos Failover

Realizado por: García, Luis, 2022.

Como se demuestra en el gráfico 3-3. La comparación entre las dos tecnologías, tomando en consideración el indicador de alta disponibilidad en la red, en las 50 pruebas realizadas se tiene como resultado que en ZeroTier el valor de tiempo promedio es 9,28 seg y en OpenVPN de 26,64 seg. Demostrándonos así que la diferencia del valor promedio del tiempo de respuesta de Failover en ZeroTier es del 65,16% menor que OpenVPN.

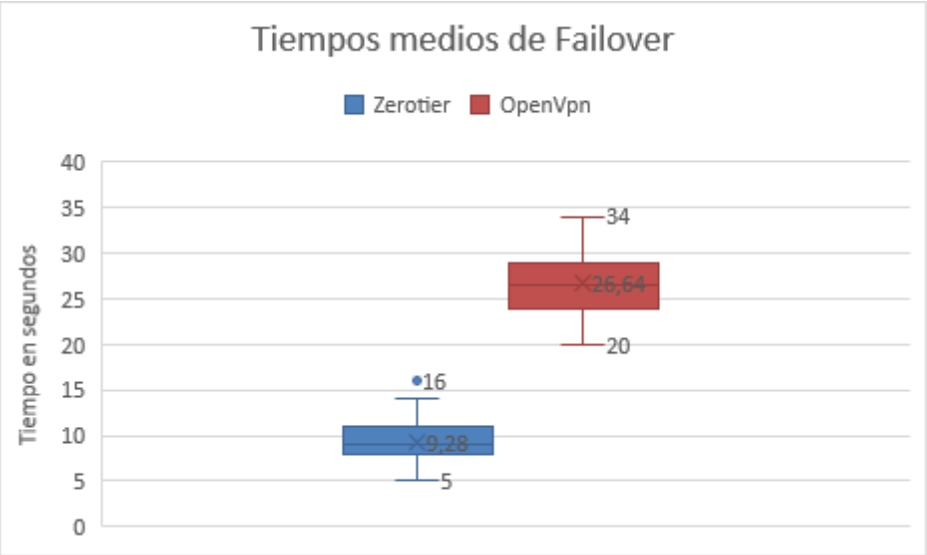


Gráfico 4-3: Valores medios entre Zerotier y OpenVpn

Realizado por: García, Luis, 2022.

Al configurar la política de active-backup en ZeroTier, se tiene una conmutación por error mínima al detectar que los enlaces presentan retardos iguales o mayores a 250ms, este valor se lo puede visualizar en el tablero de control de OPNSENSE. Mientras que en el proceso de OpenVPN, los tiempos que oscilan son mayores, y es debido a que se enruta mediante Ospf, la conmutación por error se la realiza dinámicamente, cuando el enlace detecta valores de latencias iguales o mayores a 500ms y pérdidas por encima del 20%, una vez que el firewall detecte algún comportamiento de los antes mencionados, Ospf acuta realizando una actualización de las tablas de ruta, luego que ocurra este suceso se procede a la activación del túnel por la ruta de backup.

3.5.2 Comparación con Firewall comerciales

Sophos es un firewall de siguiente generación, utilizado para realizar arquitecturas SD-WAN, según Quezada (2021) en esta tecnología comercial dentro de la configuración de puerta de enlace, se pueden configurar tiempos de conmutación por error entre 1-10seg. En base al estudio realizado, ZeroTier obtuvo tiempos entre 5 – 16seg. Esto quiere decir que con tiempos mínimos de ZeroTier se encuentra en el rango de una solución comercial.

CONCLUSIONES

- La red SD-WAN, permite mejorar el rendimiento de la red mediante el uso de redes superpuestas obteniendo alta disponibilidad en sus servicios, proporcionando escalabilidad y conectividad a través de un área centralizada mediante la nube y una administración automatizada con el fin de controlar el tráfico de la red.

- Se consigue especificar que la aplicación SD – WAN de código abierto, fueron pensadas para apoyar el cambio tecnológico a nivel mundial, donde todo se conecta a la nube, además de que este permite mayor fiabilidad en aspecto tales como videoconferencia, transferencia de datos e incluso para garantizar la conectividad y seguridad de datos a los usuarios.

- Se diseñó una red sd-wan basada en la aplicación de código abierto ZeroTier para interconectar dos sitios remotos, la misma que permite dar una administración especializada a los equipos que conforman la red, además que abarca tanto redes locales como amplias y puede conectarse a cualquier dispositivo. Se puede realizar la virtualización de las redes, las cuales terminan siendo encriptadas de extremo a extremo.

- Se pudo verificar el óptimo funcionamiento en el ambiente simulado de la red SD-WAN a través de ZeroTier, donde se conectaron dos sitios de manera remota, enrutando las redes locales de los sitios A y B a través del túnel de ZeroTier para la comunicación de las mismas. ZeroTier nos permitió trabajar de manera segura facilitando al administrador de red mediante la capa de control centralizada denominada ¨ZeroTier Central¨, controlar acceso a los servicios que se utilizan en la red usando reglas de flujo hacia los nodos.

- Se garantizó la redundancia y alta disponibilidad en la red utilizando políticas estándar como lo son active backup y balance-xor. Se pudo verificar que el rango de tiempo de conmutación entre el enlace principal y de respaldo en ZeroTier oscila los 10 seg, brindando el rango en el que se puede predefinir en una solución comercial. Con lo cual se demuestra de manera empírica que ZeroTier obtiene tiempos mínimos de conmutación por error.

- En los resultados obtenidos dentro del parámetro de alta disponibilidad utilizando Zerotier se logra un tiempo entre 5 a 16seg con un promedio de 9,28 seg y una distribución estadística normal de los datos, mientras que en el escenario con OpenVpn se obtiene entre 20 a 34 seg con un promedio de 26,54 seg, por lo que se concluye que el uso de la tecnología Zerotier brinda un mejor tiempo promedio de respuesta en las redes SD-WAN.

- Las ventajas de usar ZeroTier son notables indudablemente ya que tiene la capacidad de adaptarse a cualquier entorno de red, utiliza conexión peer to peer es decir que trabaja de manera ¨segura¨. Reduce precios en costos, debido a que es un *software* de código abierto y se puede acoplar a las demandas de la red que se necesitan, así como también permite trabajar como VPN hacia sus redes locales debido a que maneja en la capa de control ubicada en ZeroTier central, una tabla de enrutamiento y asignación de Ip. Mediante la conexión Plug and Play ZeroTier otorga un ID a sus nodos, mismo que se puede utilizar en el cuadro de flujo de reglas para etiquetar y controlar las acciones que este puede hacer dentro de la red.

RECOMENDACIONES

- Se recomienda Comprobar dentro de los Equipos OPNSENSE verificar que los enlaces WAN estén activos con salida a internet, para así ZeroTier pueda realizar las peticiones al ZeroTier central y exista la conexión P2P entre los nodos.

- Al configurar ZeroTier, se debe realizar como una interfaz adicional en el nodo, en la cual se recomienda que la dirección Ip de ZeroTier sea de manera estática para identificación rápida de los nodos existentes. A su vez a nivel de seguridad a través del Firewall, se recomienda habilitar los puertos UDP 9993 para permitir la conexión.

- Al establecer los parámetros de bonding Policy dentro del apartado Local.conf, se recomienda que la codificación de la política se encuentre con los espacios correctos, y llevar consigo una buena estructura, con la finalidad de poder crearla de manera inmediata y así evitar errores en la aplicación.

- Una vez que los equipos están enlazados y autentificados. En la tabla de rutas de ZeroTier. Se recomienda bloquear la red física de la LAN para que no exista error al momento de la conmutación por error, debido a que ZeroTier escoge como una ruta a estas interfaces, con ello evite mostrarse como una ruta saliente. Introduciendo el siguiente comando dentro de la opción local.conf:

```
{
   " Physical ”: {
            " direccion_del_host ”: {“ blacklist ”: true}
  }
}
```

- Para el entorno Simulado Gns3 se recomienda considerar las limitaciones del ancho de banda, debido a las licencias de los equipos de prueba, en este escenario se utilizó los routers Mikrotik, y consta con un alcance máximo de ancho de banda de 1Mbps aprox, por ende, los resultados y el rendimiento en cuanto al ancho de banda afecta notablemente.

- Se recomienda a las instituciones de educación superior, incluir en sus mallas curriculares, contenido referente al diseño e implementación de las redes SD -WAN, con la finalidad de que cuando esta tendencia este plenamente posicionada, los profesionales estén plenamente

capacitados no solo para crear estas infraestructuras, sino también para prestar servicios adyacentes a las necesidades emergentes de los usuarios.

BIBLIOGRAFÍA

ALI, El Kamel; & MANEL, Majdoub. An efficient MPLS-based source routing scheme in software-defined wide area networks (SD-WAN). *IEEE.* [En línea] 2017. [Citado el: 03 de Agosto de 2021.] https://ieeexplore.ieee.org/document/8308427. 21615330.

BLOOMBERG, Jason. SD-WAN: Entry Point For Software-Defined Everything. *Forbes.* [En línea] 2017. [Citado el: 06 de Agosto de 2021.] https://www.forbes.com/sites/jasonbloomberg/2017/03/20/sd-wan-entry-point-for-software-defined-everything/?sh=69fc7b546ee4..

CASTELLOTE, Emilio. El mercado SD-WAN y su potencial en EMEA. *Idcspain.* [En línea] 2018. [Citado el: 01 de Agosto de 2021.] https://www.idcspain.com/COMMONS/ATTACHMENTS/El-mercado-SDWAN-potencialidad-EMEA.PDF.

CISION. The first SD-WAN Open Source drivig the second wave of SD-WAN by flexiWAN. *Prnewswire.* [En línea] 2019. [Citado el: 24 de Agosto de 2021.] https://www.prnewswire.com/il/news-releases/the-first-sd-wan-open-source-driving-the-second-wave-of-sd-wan-by-flexiwan-300827827.html..

DE LUZ, Sergio. Configura pfSense para proteger tu hogar o empresa con este firewall. *Reonedes Z.* [En línea] 2021. [Citado el: 20 de Febrero de 2022.] https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/.

FLEXIWAN. High Level Architecture Diagram. *FlexiWAN.* [En línea] 2020. [Citado el: 27 de Agosto de 2021.] https://docs.flexiwan.com/overview/architecture.html.

FLEXIWAN. The wold first SD-WAN Open source . *Flexiwan.* [En línea] 2020. [Citado el: 22 de Agosto de 2021.] https://flexiwan.com/..

FORTINET. FortiGate. *Fortinet.* [En línea] 2020b. [Citado el: 14 de Agosto de 2021.] https://www.fortinet.com/lat/products/next-generation-firewall.

FORTINET. Fortinet, primer lugar en soluciones de ciberseguridad. *Fortinet.* [En línea] 2022. [Citado el: 01 de Febrero de 2022.] https://www.fortinet.com/lat.

FORTINET. Modelos y especificaciones de análisis y administración FortiAnalyzer. *Fortinet.* [En línea] 2020d. [Citado el: 15 de Agosto de 2021.] https://www.fortinet.com/lat/products/management/fortianalyzer/models-specs.

FORTINET. Modelos y especificaciones de la administración de FortiManager. *Fortinet.* [En línea] 2020c. [Citado el: 14 de Agosto de 2021.] https://www.fortinet.com/lat/products/management/fortimanager/models-specs.

GOOLEY, Jason; et al. *Cisco Software-Defined Access.* Hoboken : Pearson, 2020. 9780136448389.

GRUPO SIRT. Cisco SD-WAN ¿Qué es y por qué es importante? *Grupo Sirt.* [En línea] 2019. [Citado el: 20 de Agosto de 2021.] https://www.sirt.com/2019/03/cisco-sd-wan-que-es-y-por-que-es-importante/..

IBARRA, David. Requerimientos del sistema Ubuntu Linux 20.04 LTS. *Cunoticias.* [En línea] 2020. [Citado el: 10 de Febrero de 2022.] https://www.cunoticias.com/linux/requisitos-del-sistema-ubuntu-linux-20-04-lts.php..

IDC. SD-WAN Infrastructure Market Poised to Reach $5.25 Billion in 2023, According to New IDC Forecast. *Idc.* [En línea] 2019. [Citado el: 02 de Agosto de 2021.] https://www.idc.com/getdoc.jsp?containerId=prUS45380319.

JIMÉNEZ, Nora. Implementación de un prototipo de una red SDWAN (Software - Defined Wide Area Network) utilizando tecnología de Juniper Networks. *Escuela Politécnica Nacional.* [En línea] 2020. [Citado el: 04 de Septiembre de 2021.] http://bibdigital.epn.edu.ec/handle/15000/21292.

KLUSAITE, Laura. ¿Qué es MPLS? Diferencia entre MPLS y VPN. *Nordvpn.* [En línea] 2022. [Citado el: 18 de Febrero de 2022.] https://nordvpn.com/es/blog/que-es-mpls/..

LAVADO, Gianpietro; & GUZMÁN, José. Aplicando SDN, NFV, DevOps y Cloud en LATAM. *Lacnic.* [En línea] 2017. [Citado el: 06 de Agosto de 2021.] http://slides.lacnic.net/wp-content/uploads/2017/09/tutorial-aplicando-sdn-sdn-devops-y-cloud-en-latinoame%C3%8C%C2%81rica.pdf.

LUCID. Donde los equipos se reúnen para ver y construir el futuro. *Lucid.* [En línea] 2021. [Citado el: 07 de Febrero de 2022.] https://lucid.co/es..

MADDISON, John. The Challenge of Converging Security and Networking. *Fortinet.* [En línea] 2020. [Citado el: 13 de Agosto de 2021.] https://www.fortinet.com/blog/industry-trends/the-challenge-of-converging-security-and-networking.

MONTES, Bryan; & SOLANO, José. Estudio para la implementación de un sistema de redes definida por software (SDN) para una red de área amplia (WAN). *Universidad Distrital Francisco José Caldas.* [En línea] 2019. [Citado el: 07 de Agosto de 2021.] https://repository.udistrital.edu.co/bitstream/handle/11349/16248/MontesCasta%F1edaBryan2019.pdf;jsessionid=F96D1725946AF6655651D1AB853D4FD8?sequence=1.

MORA, Rubén; et al. Implementation of a SD-WAN for the interconnection of two software defined data centers. *IEEE.* [En línea] 2019. [Citado el: 05 de Agosto de 2021.] https://ieeexplore.ieee.org/document/8809153.

ONF CORD. Ransforming access and edge networks by collaboratively building next generation mobile and broadband infrastructures. *Opennetworking.* [En línea] 2020. [Citado el: 27 de Agosto de 2021.] https://opennetworking.org/..

OZGA, Jacek. Cisco Viptela SD-WAN components and connectivity. *Grandmetric.* [En línea] 2018. [Citado el: 22 de Agosto de 2021.] https://www.grandmetric.com/2018/02/19/cisco-viptela-sd-wan-components-connectivity-viptela-part-1/..

PFSENSE. Dispositivos de puerta de enlace de seguridad Netgate PFsense. *Pfsense.* [En línea] 2022. [Citado el: 02 de Septiembre de 2021.] https://www.pfsense.org/products/.

POSTSUS. El informe del grupo Dell'Oro muestra que Versa Networks es el líder de participación de mercado de SASE unificado para 2021 con una participación de mercado del 84 por ciento. *Postsus.* [En línea] 2021. [Citado el: 03 de Agosto de 2021.] https://es.postsus.com/negocio/75487.html.

PROGRAMADOR CLIC. Arquitectura Open Daylight. *Programador Clic.* [En línea] 2020. [Citado el: 25 de Agosto de 2021.] https://programmerclick.com/article/30441695746/.

REJÓN, Javier. Simulador de red GNS3. *Mundo telematico.* [En línea] 2019. [Citado el: 01 de Septiembre de 2021.] https://www.mundotelematico.com/simulador-de-red-gns3/..

SCC. SD-WAN: Todo lo que debes saber según Cisco. *Sccenlared.* [En línea] 2022. [Citado el: 17 de Febrero de 2022.] https://www.sccenlared.es/sd-wan-segun-cisco/#:~:text=Administraci%C3%B3n%20simplificada,campus%20o%20en%20el%20cloud...

SPADARO, Gustavo. Diseño de red WAN. *Openaccess.* [En línea] 2012. [Citado el: 26 de Agosto de 2021.] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/21801/1/Memoria_Gustavo_Spadaro.pdf.

SPRINT NETWORKS. ¿Porque Versa SD-WAN? *Sprint Networks.* [En línea] 2022. [Citado el: 04 de Febrero de 2022.] https://www.sprintnetworks.com.au/learn-about-sd-wan/..

TECH EXPERT. Failover o comunicación por error. *Tech Expert.* [En línea] 2022. [Citado el: 14 de Febrero de 2022.] https://techexpert.tips/es/pfsense-es/pfsense-equilibrio-de-carga-de-enlace-wan-multiple/.

TROIA, Sebastian; et al. SD-WAN: An Open-Source Implementation for Enterprise Networking Services. *IEEE.* [En línea] 2020. [Citado el: 04 de Agosto de 2021.] https://ieeexplore.ieee.org/document/9203058.

VARGAS BRAVO, José Luis. Evolución de una red en suscursales a SD-WAN - UOC. *Openaccess.* [En línea] 2020. [Citado el: 06 de Agosto de 2021.] http://openaccess.uoc.edu /webapps/o2/bitstream/10609/116646/6/jvargasbTFG0620memoria.pdf.

VERSA NETWORKS. Versa Analytics. *Versa Networks.* [En línea] 2022b. [Citado el: 17 de Febrero de 2022.] https://versa-networks.com/products/analytics.php.

VERSA NETWORKS. Versa Director. *Versa Networks.* [En línea] 2022a. [Citado el: 18 de Febrero de 2022.] https://versa-networks.com/documents/datasheets/versa-director.pdf.

VERSA NETWORKS. Versa Operating System (VOS). *Versa Networks.* [En línea] 2022c. [Citado el: 19 de Febrero de 2022.] https://versa-networks.com/documents/datasheets/versa-vos.pdf.

VMWARE. Componentes de la solución. *Vmware.* [En línea] 2021b. [Citado el: 17 de Agosto de 2021.] https://docs.vmware.com/es/VMware-SD-WAN/4.0/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-16C592CA-8F02-4CEF-B8FB-769A0CDA0231.html..

VMWARE. VMWARE: Información general. *Vmware.* [En línea] 2021a. [Citado el: 16 de Agosto de 2021.] https://docs.vmware.com/es/VMware-SD-WAN/4.0/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-EE8C35B8-FA4E-4C59-9AC2-4FD14509F60C.html..

WILEY, John. Software-Defined WAN. *Velocloud.* [En línea] Wmware, 2018. [Citado el: 12 de Agosto de 2021.] http://wan.velocloud.com/rs/098-RBR-178/images/SD_WAN_For_Dummies_VMware_2nd_SpecialEdition.pdf. 978-1-119-53558-4.

ZEROTIER. Arquitectura ZeroTier. *Zerotier.* [En línea] 2020. [Citado el: 30 de Agosto de 2021.] https://www.zerotier.com/manual/.

ANEXOS

ANEXO A: INSTALACIÓN DE ZEROTIER – ONE

ANEXO B: ANALIZADOR DE PROTOCOLOS WIRESHARK