NOMBRE DEL TRABAJO

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED PARA CLIENTES EMPRESARIALES DE UN ISP EN EL SOFTWARE EVE-NGU

AUTOR

CARLOS JULIAN REA ZAPATA

RECUENTO DE PALABRAS

13015 Words

RECUENTO DE CARACTERES

74322 Characters

RECUENTO DE PÁGINAS

87 Pages

TAMAÑO DEL ARCHIVO

2.2MB

FECHA DE ENTREGA

May 30, 2024 8:39 AM GMT-5

FECHA DEL INFORME

May 30, 2024 8:41 AM GMT-5

13% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 13% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45° de la ley N° 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (X)

DATOS PERSONALES

Apellidos y Nombres:	REA ZAPATA CARLOS JULIAN
D.N.I.:	77564840
Otro Documento:	
Nacionalidad:	PERUANA
Teléfono:	949309487
e-mail:	carlosrea46@gmail.com

DATOS ACADÉMICOS

Pregrado

Facultad:	FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico:	TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado:	INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:	
País:	
Grado Académico otorgado:	

Datos de trabajo de investigación

Título:	PROPUESTA DE IMPLEMENTACIÓN DE UNA RED PARA CLIENTES EMPRESARIALES DE UN ISP EN EL SOFTWARE EVE-NG UTILIZANDO LA TECNOLOGÍA SD-WAN
Fecha de Sustentación:	16 DE DICIEMBRE DE 2021
Calificación:	APROBADO POR UNANIMIDAD
Año de Publicación:	2024

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo X No autorizo _____

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	(X)

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva Nº 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	( )
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

_____

_____

Motivos de la elección del acceso restringido:

_____

_____

_____

_____

_____

REA ZAPATA CARLOS JULIAN

APELLIDOS Y NOMBRES

77564840

DNI

Firma y huella:

Lima, 30 de ABRIL del 2024

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“PROPUESTA DE IMPLEMENTACIÓN DE UNA RED PARA CLIENTES EMPRESARIALES DE UN ISP EN EL SOFTWARE EVE-NG UTILIZANDO LA TECNOLOGÍA SD-WAN”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

REA ZAPATA, CARLOS JULIAN
ORCID: 0000-0001-9632-7419

ASESOR

CASTRO PULCHA, BERNARDO ELIAS
ORCID: 0000-0001-8578-5940

Villa El Salvador
2021

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional
Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Siendo las **15:30 horas** del día jueves **16 de diciembre del 2021**, y debido a la emergencia sanitaria y aislamiento social por el COVID-19, se reunieron vía google meet (https://meet.google.com/cye-qitg-knd), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. LA ROSA LONGOBARDI, Carlos Jacinto	CIP N° **055254**
Secretario	: MG. CAMPOS AGUADO, Fredy	CIP N° **173769**
Vocal	: MG. LOPEZ CORDOVA, Jorge Luis	CIP N° **183016**

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN Nº 432-2021-UNTELS-CO-V.ACAD-FIG, de fecha 09 de Diciembre del 2021.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional. (Resolución de Comisión Organizadora Nº 126-2021-UNTELS de fecha 06 de agosto del 2021, en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur", siendo que el Art. 4º del precitado Reglamento establece que: **"**La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo de Suficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar 02 años de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019-SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)…", en el cual;

El Bachiller: **REA ZAPATA, CARLOS JULIAN**

Sustentó su Trabajo de Suficiencia Profesional: **"PROPUESTA DE IMPLEMENTACIÓN DE UNA RED PARA CLIENTES EMPRESARIALES DE UN ISP EN EL SOFTWARE EVE-NG UTILIZANDO LA TECNOLOGÍA SD-WAN"**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición **Aprobado por Unanimidad**, Equivalencia **Bueno**, de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS, vigente.

Siendo las **16:15 horas** del día jueves 16 de diciembre del 2021, se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado Evaluador.

Dr. Carlos Jacinto La Rosa Longobardi
CIP N°055254
PRESIDENTE

Mg. Fredy Campos Aguado
CIP N°173769
SECRETARIO

Mg. Jorge Luis López Córdova
CIP N°183016
VOCAL

PARTICIPANTE
Bachiller: CARLOS JULIAN REA ZAPATA

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público y conservando las medidas de distanciamiento social y de emergencia sanitaria. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del Jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del Jurado, la sustentación será reprogramada durante los cinco (05) días siguientes.

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional
Facultad de Ingeniería y Gestión

ACTA FINAL DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Siendo las **15:30 horas** del día jueves **16 de diciembre del 2021**, y debido a la emergencia sanitaria y aislamiento social por el COVID-19, se reunieron vía google meet (https://meet.google.com/cye-qitg-knd), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. LA ROSA LONGOBARDI, Carlos Jacinto	CIP N° **055254**
Secretario	: MG. CAMPOS AGUADO, Fredy	CIP N° **173769**
Vocal	: MG. LOPEZ CORDOVA, Jorge Luis	CIP N° **183016**

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN Nº 432-2021-UNTELS-CO-V.ACAD-FIG, de fecha 09 de Diciembre del 2021.

Concluida la Sustentación del Trabajo de Actualidad, se procede a registrar la nota obtenida en la Sustentación del Trabajo de Suficiencia Profesional.

BACHILLER EVALUADO (A): **REA ZAPATA, CARLOS JULIAN**

Nota de sustentación del Trabajo de Suficiencia Profesional	Condición	Equivalente
14	Aprobado por Unanimidad	Bueno

Dr. Carlos Jacinto La Rosa Longobardi
CIP N°055254
PRESIDENTE

Mg. Fredy Campos Aguado
CIP N°173769
SECRETARIO

Mg. Jorge Luis López Córdova
CIP N°183016
VOCAL

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público y conservando las medidas de distanciamiento social y de emergencia sanitaria. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del Jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del Jurado, la sustentación será reprogramada durante los cinco (05) días siguientes.

DEDICATORIA

A Dios y la Virgen.

Por ser siempre guía en mi camino y dar fortaleza a mi familia. Por darme la voluntad de seguir adelante y permitirme estar con familia, cuidándola y protegiéndola.

A mis padres y hermanos.

Por siempre estar ahí, apoyándome en mis estudios y trabajo. Darle gracias, por sus buenos consejos y la enseñanza que cada día me brindan para seguir por el buen camino. Gracias también, por ser ejemplo de dedicación y trabajo.

AGRADECIMIENTO

Al terminar de redactar el presente trabajo de suficiencia profesional me gustaría expresar mi profundo agradecimiento en primer lugar a mi familia por su apoyo incondicional, y seguidamente a mi alma máter UNTELS por ser la casa de estudios con la cual me formé como profesional.

Asimismo, quiero extender este agradecimiento a mis distinguidos profesores que me inculcaron sus enseñanzas, y en especial al Mg. Bernardo Elias Castro Pulcha que, en su función, ha tenido a bien asesorarme en el desarrollo del trabajo.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El presente trabajo abarca la necesidad, que actualmente buscan muchas empresas, para obtener una mejora en la transmisión de sus datos de internet y de procesos en la nube que garanticen escalabilidad, flexibilidad y seguridad en sus comunicaciones. Ante esto, surge la tecnología SD-WAN (Software Defined WAN), la cual tiene como características principales la optimización de recursos, la reducción de costos en la implementación y la seguridad en las conexiones de sus redes siendo estas de primera necesidad en el mercado de las redes de telecomunicaciones, las cuales buscan reemplazar las limitaciones actuales que tiene una tecnología tradicional como es MPLS (Multiprotocol Label Switching) a nivel de impacto en los servicios del cliente los cuales son, el costo elevado en la implementación y la dificultad para comunicar servicios en la nube. Este trabajo de investigación precisa desarrollar las bondades y aplicaciones que ofrece esta tecnología, y con esto poder realizar la propuesta de la implementación y simulación mediante el software de EVE-NG (Emulated Virtual Enviroment – Next Generation). Como parte del área de Red de clientes y centro de atención técnica del ISP (Internet Service Provider) Entel, el cual se encarga de atender solicitudes, configuración, monitoreo, soporte y averías de clientes. Por consiguiente, se tiene la solicitud de migración hacia la tecnología SD-WAN de un cliente empresarial, el cual requiere lo siguiente; dos enlaces de internet: principal y contingencia cada uno con una tecnología de transmisión distinta (Fibra óptica y Radio microondas), alta disponibilidad en sus enlaces mencionados y seguridad perimetral de sus redes. Ante esto, se le brinda como solución una red de cliente empresarial basada en la tecnología SD-WAN. Esta solución validará una mejora en los problemas de comunicación en sus conexiones que percibe el cliente empresarial en su operación y producción diaria. La metodología usada para la solución es la denominada en cascada, la cual se detallará más adelante. Una vez definida, se llevará a cabo la migración hacia la tecnología SD-WAN con la implementación de la red de cliente empresarial, el cual implica configuración, simulación y validación de la solución propuesta.

INTRODUCCIÓN

El presente trabajo titulado “Propuesta de implementación de una red para clientes empresariales de un ISP en el software EVE-NG utilizando la tecnología SD-WAN”. Se desarrolla con el objetivo de determinar una propuesta de implementación de una red de un cliente empresarial y simular su funcionamiento utilizando la tecnología SD-WAN, previa a su constitución final. Para esto se tiene una propuesta de implementación el cual comprende: dos enlaces de internet (principal y contingencia) las cuales serán brindadas por dos tecnologías de transmisión distintas.

Vivimos en tiempos en donde las empresas están evolucionando y volviéndose más digitales, por lo que las empresas necesitan evolucionar su infraestructura para hacer frente a nuevas tecnologías. Una de estas, es la conectividad de redes de internet las cuales se encuentran en constante transformación debido al alto flujo de tráfico y procesos robustos en la nube.

SD-WAN simplifica la construcción de conexiones y gestión entre diferentes sitios, por ejemplo, entre centros de datos y sucursales en redes empresariales, y proporciona la flexibilidad necesaria, control centralizado y monitoreo con menores costos.

Ante lo mencionado, se desarrollará un estudio preliminar de una red de un cliente empresarial y se simulará en el software EVE-NG con equipos o marcas de equipos que soportan la tecnología SD-WAN.

Como parte del área red de clientes y centro de atención técnica, se propone disponer de dos enlaces principal (fibra óptica) y contingencia (radio Enlace) conectadas a un mismo ISP, y con esto se podrá exponer los resultados esperados por el cliente. Así mismo, con estos resultados, se validará el rendimiento de la red y las pruebas necesarias para la entrega del servicio.

El informe consta de los siguientes capítulos:

CAPÍTULO I: Aspectos generales, que aborda entre otras el contexto de la empresa, delimitación del proyecto y los objetivos de la investigación.

CAPÍTULO II: Marco teórico, que aborda el estudio de antecedentes, bases teóricas y definición de términos básicos.

CAPÍTULO III: Desarrollo del trabajo de suficiencia profesional, en el cual se ha realizado la propuesta de implementación de una red de cliente empresarial de un ISP y con base a ello se simulará en el Software EVE-NG para validar los resultados que el cliente espera, como son la alta disponibilidad de los enlaces, conectividad hacia internet y la seguridad perimetral en sus comunicaciones. Finaliza la investigación con las conclusiones, recomendaciones y referencias bibliográficas que se estilan para este nivel de investigación.

CAPÍTULO I: ASPECTOS GENERALES

1.1 Contexto

ALL TELECOM EIRL es una empresa con más de 7 años de experiencia brindando servicios y suministros en tecnologías de la información y telecomunicaciones. Como también, presta servicios de soporte tercerizado en diferentes áreas del proveedor de servicios Entel Perú.

Entel Perú es una empresa del grupo Entel Chile que inició operaciones en nuestro país en 2014, ofreciendo diversos servicios de telecomunicaciones. Siendo reconocidos como líderes en telecomunicaciones en Latinoamérica, con más de 50 años de experiencia. En Chile brindan servicios integrados de telecomunicaciones y servicios de Tecnologías de la Información dirigidos a los mercados de personas, empresas y corporaciones. Esta operación cuenta con una posición líder en la industria y participa en el Perú a través de sus filiales Entel Perú, Americatel Perú y Servicios de Call Center del Perú. Asimismo, ofrece servicios de arriendo de redes a mayoristas, centro de atención telefónica, contacto remoto y mesas técnicas de ayuda en ambos países.

Para el presente trabajo, se tiene una solicitud de migración hacia la tecnología SD-WAN para un cliente empresarial del ISP, en la cual requieren dos enlaces de internet, uno principal y el otro de contingencia utilizando la tecnología SD-WAN como solución para la alta disponibilidad de sus enlaces.

Como parte del área red de clientes y centro de atención técnica del ISP, realizamos las funciones de configuración, monitoreo, soporte, atención de solicitudes de nuevos servicios y averías de los clientes empresariales. Así mismo como parte del equipo llevamos a cabo la migración a la tecnología SD-WAN con la implementación de esta solución a los clientes empresariales del ISP como, por ejemplo: Kaeser Compresores del Perú S.R.L., The Fox Impul S S.A.C., entre otros.

1.2 Delimitación del proyecto

1.2.1 Temporal

El tiempo requerido para realizar la implementación completa, va a depender de los requerimientos de los clientes empresariales. Como, por ejemplo, para el cliente empresarial Compresores del Perú se tuvo un tiempo estimado de 30 – 35 días, comprendidos entre los meses de agosto y setiembre del año 2020, esto incluye el análisis de la factibilidad, asignación de los recursos de provisión, implementación de las tecnologías de transmisión y pruebas finales con el ingeniero en campo y el cliente.

1.2.2 Espacial

Para nuestro ejemplo especifico, el cliente empresarial está ubicado en la zona sur de Lima. En las coordenadas: -12.2636690, -76.8960950 (Ref. Almacenes BSF).

1.3 Objetivos

1.3.1 Objetivo general

Determinar una propuesta de implementación de una red para clientes empresariales de un ISP en el Software EVE-NG utilizando la tecnología SD-WAN a fin de cumplir los requerimientos solicitados por el cliente.

1.3.2 Objetivos específicos

- Analizar la tecnología SD-WAN en el lado cliente como solución para los clientes empresariales ante las tecnologías tradicionales de comunicación, como lo es la MPLS.
- Garantizar la seguridad perimetral del cliente con la realización del cambio de enrutador.
- Ejecutar las pruebas de conectividad a internet y de alta disponibilidad de los enlaces y monitorear el tráfico cursado en su red en tiempo real.
- Validar a través de la simulación, como funciona y opera la tecnología SD-WAN, previo a su configuración en línea.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

En la actualidad, las redes empresariales han ido evolucionando su infraestructura tecnológica, haciendo que estas migren y obtengan mejoras en sus conexiones a internet.

Luis Antonio Delgado Avendaño de la Universidad Autónoma de México - UNAM (2019) en su trabajo titulado *"Implementación de una solución de alta disponibilidad SD-WAN para la construcción de redes híbridas y sustitución de la tecnología MPLS"* propuso la migración de servicios de dos empresas importantes en México a la tecnología SD-WAN, ya que estas presentaban caídas constantes del servicio de internet a través de la conexión MPLS y esto generaba pérdidas en la producción diaria de estas. Tras la implementación, concluyó que existe una mejora en la experiencia del usuario final al reducir las caídas de operación y así mismo se preservaron las funcionalidades del servicio, disminuyendo los costos de la solución. Este trabajo guarda relación con la problemática que presentan los clientes empresariales en mi trabajo de suficiencia profesional.

Douglas Oswaldo Ayapata Mendoza de la Universidad Católica de Santiago de Guayaquil (2020) en su trabajo titulado *"Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo"* realizó el estudio y diseño de una red de un cliente corporativo para empresas del Ecuador basado en la tecnología SD-WAN, debido a los problemas que atraviesan los clientes corporativos en la transmisión de información en sus redes y las necesidades que estos buscan al expandir su infraestructura tecnológica. Tras el modelado de la red corporativa, concluyó que, con la comprobación de alta disponibilidad del enlace, aunque exista caídas en las interfaces, la tecnología SD-WAN balancea la carga de transmisión de información hacia otra interfaz asociada en su interfaz virtual por medio de la aplicación de gestión del equipo, así manteniendo la conectividad con la perdida mínima de paquetes. Este trabajo nos una

idea de cómo se dio el enfoque de SD-WAN para nuestro presente trabajo.

Luis Andrés Marín Santamaría de la Universidad Católica de Santiago de Guayaquil (2021) en su trabajo titulado *"Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos"* planteó el diseño de red para la empresa Construl S.A. en Ecuador utilizando la tecnología SD-WAN con la necesidad de optimizar los recursos tecnológicos de la empresa, sin aumentar los costos y manteniendo la calidad del servicio. Dentro de la solución brindada se dispone de las pruebas de alta disponibilidad. Tras el diseño y simulación, concluyó que, la solución planteada para la empresa Construl S.A. cumple con los requerimientos para el desarrollo de la tecnología SD-WAN con equipos Fortigate (Equipo de seguridad). Los mismos facilitan los trabajos y control de la red a los encargados y obtienen alta disponibilidad en la red. Para observar el comportamiento del diseño de red la simulación se realiza mediante GNS3 (Graphical Network Simulator). Este trabajo nos da el aporte que el uso de un emulador para realizar las pruebas de conectividad y alta disponibilidad son necesarias para demostrar la validez del funcionamiento de la red de un cliente empresarial, previa a su implementación final.

Luis Enrique Aguilar Ruiz de la Universidad Tecnológica del Perú - UTP (2020) en su trabajo titulado *"Propuesta de Diseño de una Red Privada de Telecomunicaciones para Accesos a Aplicaciones de una Entidad Bancaria a través de Internet"* propuso en brindar una solución a los problemas que perciben las oficinas de una Entidad Bancaria en el Perú como son ancho banda, sin alta disponibilidad de sus enlaces, entre otros. Esto conllevó a brindar una solución basada en la tecnología SD-WAN. Tras la propuesta de la red privada, concluyó que, el costo de un enlace de internet más los equipos SD-WAN para una implementación en una Entidad Bancaria es menor a los enlaces de MPLS que utilizan actualmente las empresas para lograr la conectividad. Así mismo los equipos SD-WAN, usados en la red privada de la entidad bancaria, son seguros debido a los protocolos de encriptación y autenticación que utilizan. Esta solución basada en SD-WAN nos da una idea como debe ser brindada la solución a los clientes empresariales en nuestro trabajo, ya que existe una similitud en la problemática de los clientes y muestra

los beneficios que ofrece esta tecnología.

Gustavo Adolfo Velasquez Ruiz de la Universidad Tecnológica de Lima Sur - UNTELS (2017) en su trabajo titulado *"Diseño e Implementación de un servicio de seguridad administrada e interconexión de datos utilizando tecnología MPLS para el Instituto Del Mar Del Peru"* realizó un diseño e implementación de una red basada en la tecnología MPLS, reemplazando la anterior tecnología de comunicación que tenía IMARPE, el cual era de protocolo PPP (punto a punto). Esta le provocaba, según lo comentado por el autor, congestión en su red al intentar la comunicación en simultáneo de todas de sus sedes. Así mismo no contaba con un monitoreo de los enlaces, lo cual dificultaba la administración correcta de la red de IMARPE. Tras la implementación del servicio, concluyó que, con la implementación de la tecnología MPLS le ayudara a la comunicación entre sedes, la especialización de la tecnología y la comunicación fluida de estos. Destaco la importancia del trabajo de suficiencia profesional UNTELS por la metodología utilizada para la implementación de la tecnología MPLS brindada para mejorar las conexiones de la red de IMARPE. En nuestro caso la mejora se realizará en una migración de la conexión MPLS a SD-WAN, motivo de mi trabajo.

Estos son los trabajos que dieron una mayor influencia en el desarrollo de mi trabajo propuesto, teniendo en cuenta los temas a tratar como, por ejemplo, la migración de una tecnología anterior a una más reciente, implementación de una red SD-WAN a nivel empresarial y las pruebas y/o validaciones del servicio una vez implementado. Así también cabe mencionar que la problemática presentada en cada una de ellas tiene una similitud con mi trabajo de suficiencia profesional.

2.2. Bases teóricas

En este apartado, se detalla los sustentos teóricos del presente trabajo de suficiencia profesional, donde se irá desarrollando desde el nivel más general a un nivel especifico, los cuales se relacionarán directamente con el tema propuesto.

2.2.1. Redes empresariales en las telecomunicaciones

Las redes corporativas o empresariales a menudo se enfocan en estándares de redes LAN (Local Area Network), que generalmente usan conmutadores de hardware, dispositivos de enrutamiento, conexión ethernet, conexiones inalámbricas y sistemas de cortafuegos integrados para crear una red local. (VMware, s.f.)

Los avances de hoy en las redes corporativas están impulsados por nuevos estándares de redes SDN (Software Defined) como SDWAN y LAN virtual expandible (VXLAN). (VMware, s.f.)

2.2.1.1. Ventajas de las redes empresariales.

Hoy en día, las redes empresariales son la columna vertebral de todos los departamentos de TI (Technology Information) comerciales y, tradicionalmente, han allanado el camino para que millones de personas sigan carreras en esta industria. Cada empresa necesita crear una solución única para su red corporativa de acuerdo con sus necesidades de flujo de trabajo, producción, demanda del consumidor, logística, etc. (VMware, s.f.)

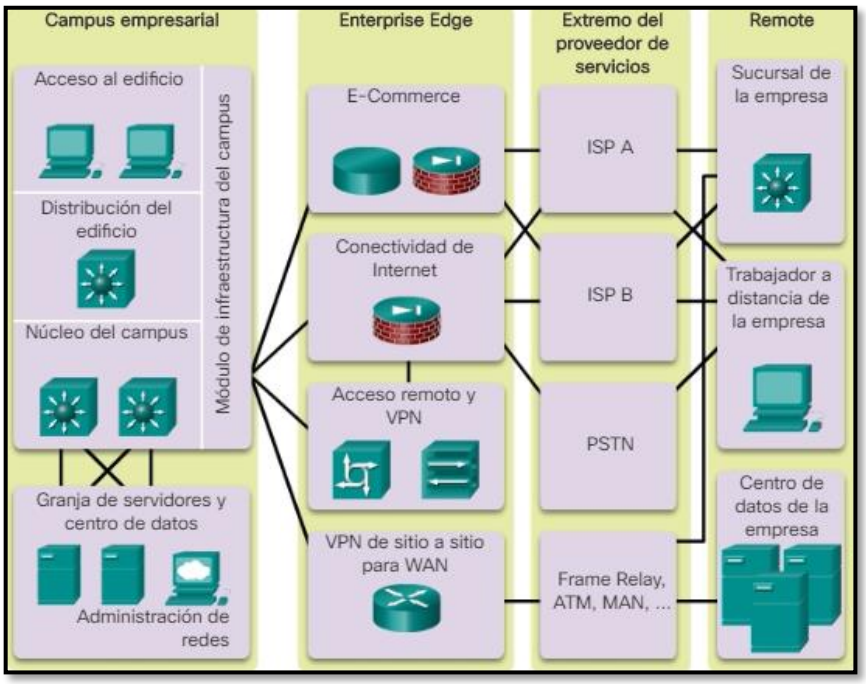
Entre las principales ventajas, se puede mencionar lo siguiente:

- Eficiencia mediante la colaboración
- Acceso controlado a los recursos de la empresa
- Acceso compartido a software propietario
- Mayor productividad de los trabajadores
- Costos reducidos

2.2.1.2. Arquitectura de las redes empresariales.

La arquitectura de una red corporativa o empresarial se basa en la combinación de enrutadores y conmutadores que permiten a los administradores de red crear una red de área local. En la siguiente figura 1, se muestra una arquitectura típica de una red empresarial. (VMware, s.f.)

Figura 1. Modelo de una red empresarial



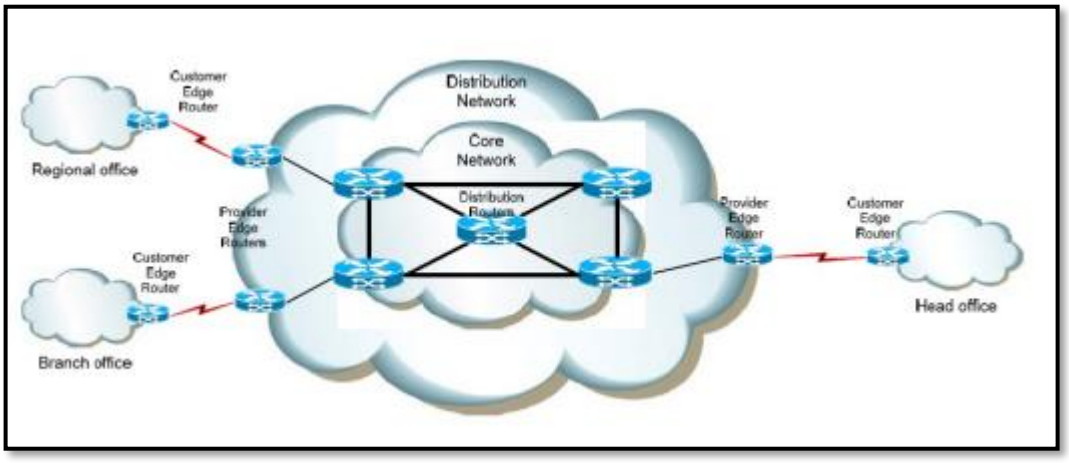
Fuente: https://ccnadesdecero.es/arquitectura-red-empresarial-cisco/

2.2.2. Conmutación de etiquetas multiprotocolo (MPLS)

La tecnología MPLS (Multiprotocol Label Switching) se ha utilizado con mayor auge desde mediados de la década de 2000, y ha ido mejorado la velocidad de datos de la red y el rendimiento de la red para las redes corporativas. Un enrutador analiza el encabezado IP (Internet Protocol) y decide dónde reenviar el paquete. Con MPLS, la

decisión de enrutamiento se toma en función de la asignación de etiquetas en lugar del encabezado IP. Una etiqueta es un identificador corto de cuatro octetos de longitud fija de importancia local que se utiliza para identificar una clase de equivalencia de transferencia (FEC). (Rajendran A., 2016). La figura 2, muestra una topología típica basada en MPLS.

Figura 2. Red de la tecnología MPLS



Fuente: http://www.nastechgroup.com/our-services/mpls-data-network-setup/

2.2.2.1. Desventajas en la tecnología MPLS.

Las soluciones basadas en MPLS son ampliamente aceptadas por la mayoría de las empresas por su rendimiento, pero existen algunas desventajas que crean la necesidad de nuevas tecnologías. Las principales desventajas de MPLS son los costos y la adaptación a nuevas tecnologías como la nube. El costo de la WAN (Wide Area Network) privada basada en MPLS es más alto que el costo normal de conectividad a Internet. Además, MPLS es una tecnología antigua, que se desarrolló en el año 2000 y aún sigue siendo utilizado por más de 20 años. (Andy Gottlieb, 2012).

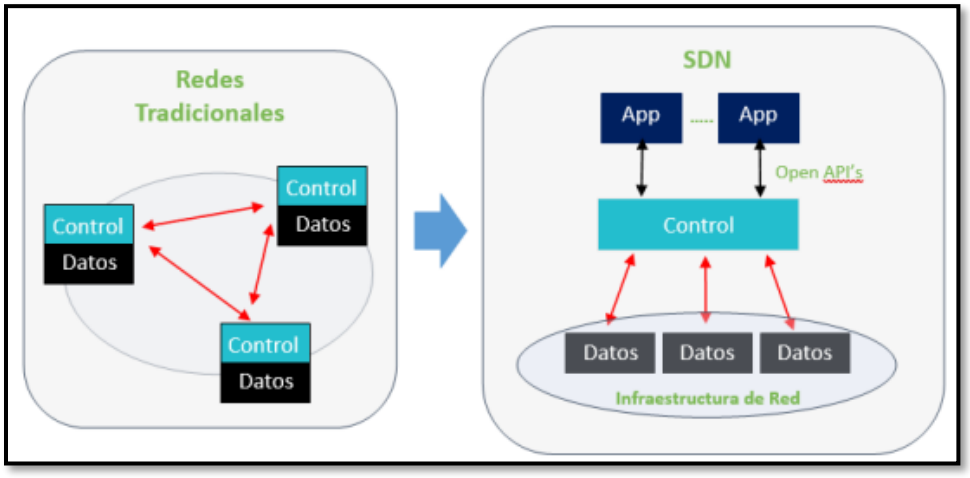
Durante este tiempo, nuevas tecnologías han ido desarrollándose como por ejemplo la virtualización de las redes (NFV) y las redes definidas por software (SDN). Por tanto, no es de extrañar que se hayan desarrollado nuevas alternativas para reemplazar la tecnología MPLS.

2.2.3. Redes definidas por software (SDN)

Las redes definidas por software (SDN) son un nuevo enfoque para diseñar, construir y administrar redes, este enfoque se basa en la separación entre el plano de control y los datos plano para optimizar mejor cada parte. SDN centraliza el control de la red implementándola como software en una entidad separada llamada controlador. (Kreutz et al., 2015).

Este controlador es responsable de insertar reglas en enrutadores y conmutadores en el plano de datos en función de las decisiones tomadas por el plano de control para simplificar la entrega de datos en la capa de infraestructura. Este método ayuda a realizar cambios a nivel mundial y a mejorar la eficiencia de la red y a simplificar su gestión. (Nunes et al., 2014). La figura 3 muestra la evolución de la red tradicional, en la cual podemos observar como una red tradicional maneja sus reglas en el hardware en conjunto, mientras que la red SDN realiza la separación de estas reglas y los implementa en módulos de software para un mejor manejo.

Figura 3. Evolución de las Redes Tradicionales

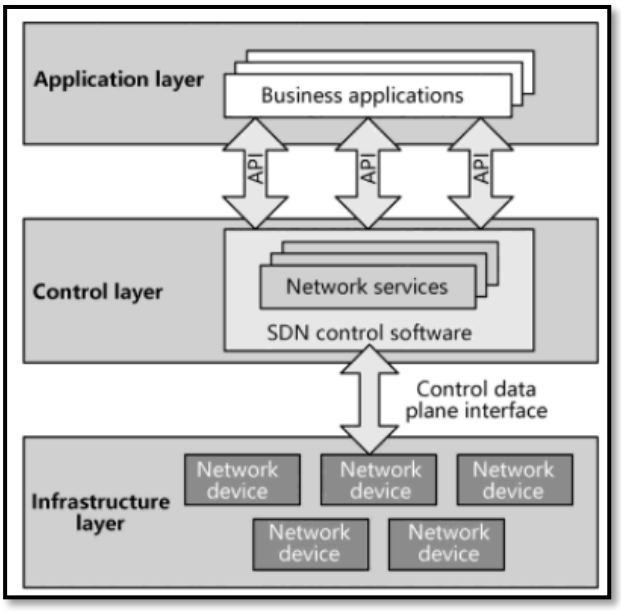


Fuente: http://openaccess.uoc.edu/webapps/

2.2.4. Capas de la arquitectura SDN

La arquitectura SDN consiste en tres capas: aplicación, control e infraestructura. La figura 4 muestra de forma detallada como está conformada esta arquitectura SDN.

Figura 4. Arquitectura de la SDN



Fuente: Tomado del Libro: Cheng Sheng, Jie Bai, Qi Sun, Software-Defined Wide Area Network Architectures and Technologies 2021

2.2.4.1. Capa de aplicación.

La capa de aplicación es la interfaz de interacción más alta de la arquitectura SDN y es responsable de la comunicación con los sistemas externos. Esta capa consta de varias aplicaciones comerciales y es responsable de interpretar los requisitos de los servicios de los usuarios y de definir y orquestar los servicios de red en función de los requisitos del usuario. (Cheng Sheng, Jie Bai, Qi Sun, 2021)

2.2.4.2. Capa de control.

La capa de control es el cerebro de la arquitectura SDN. Une la capa de aplicación y la capa de infraestructura. Para elaborar, proporciona funciones y servicios de red abiertos y abstractos para la capa de aplicación a través de interfaces de programación de aplicaciones (API), y controla los comportamientos de reenvío de datos de los dispositivos de red en la capa de infraestructura a través de interfaces. (Cheng Sheng, Jie Bai, Qi Sun, 2021)

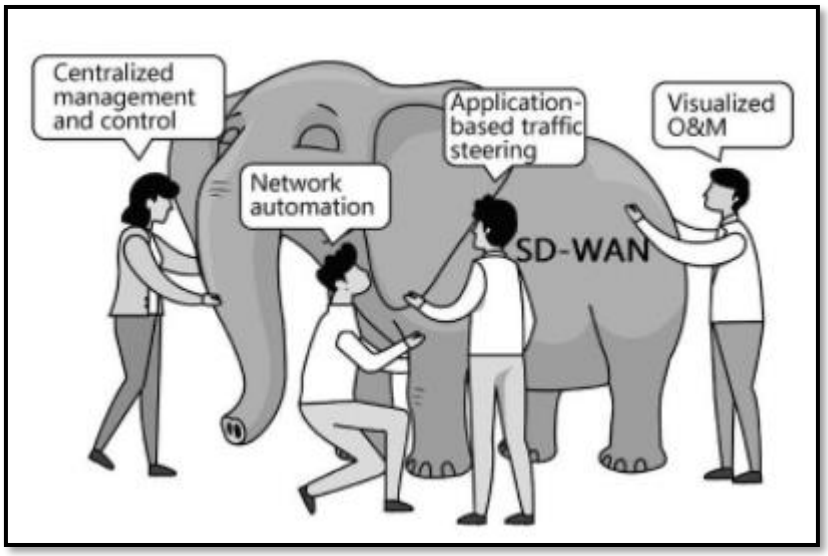
2.2.4.3. Capa de infraestructura.

La capa de infraestructura es el cuerpo de la arquitectura SDN. Contiene una amplia gama de dispositivos de red comunes que reenvían el tráfico de acuerdo con las políticas entregadas por la capa de control. En resumen, SDN no es un concepto complejo que solo tiene sentido a un nivel teórico o simplemente un truco y un enfoque de diseño de red inviable, sino que es un enfoque robusto y alcanzable para el diseño de redes, que marcó una diferencia significativa, redefiniendo de forma innovadora el marco de DCN para satisfacer mejor los requisitos de servicio en evolución (Cheng Sheng, Jie Bai, Qi Sun, 2021).

2.2.5. Red de área amplia definida por software (SD-WAN)

SD-WAN es un tipo de servicio de red que aplica la tecnología SDN a la interconexión WAN en las empresas. SD-WAN integra profundamente las tecnologías WAN empresariales convencionales, como enrutamiento, QoS (Quality of Services), seguridad y aceleración de la WAN, así como tecnologías completamente nuevas y preparadas para el futuro, incluidas SDN, NFV y unificación de servicios. Como tal, al usar el controlador SDN, SD-WAN logra la unificación, el control y la administración centralizados de las interconexiones WAN. Como se muestra en la Figura 5, la industria tiene diferentes opiniones sobre lo que es SD-WAN y aún no ha llegado a un consenso sobre una definición unificada.

Figura 5. Opiniones de la SD-WAN en el entorno empresarial



Fuente: Tomado del Libro: Cheng Sheng, Jie Bai, Qi Sun, Software-Defined Wide Area Network Architectures and Technologies 2021

2.2.5.1. Beneficios de la tecnología SD-WAN.

Al considerar adquirir la tecnología SD-WAN, las organizaciones o empresas deben evaluar los beneficios de SD-WAN. A medida que los expertos en redes se dan cuenta de los suficientes beneficios que ofrece SD-WAN, la decisión de adoptar la tecnología se vuelve más clara. Por ejemplo, si una organización ha aceptado el alto costo de MPLS para satisfacer las necesidades de tráfico críticas del negocio, la arquitectura SD-WAN permitirá el uso de enlaces de bajo costo, como circuitos de Internet.

SD-WAN ofrece redundancia entre las conexiones WAN, conmutando automáticamente a una segunda ruta si la principal falla o no está disponible. SD-WAN también puede utilizar el balanceo de carga en varias conexiones para mejorar el rendimiento de la red y las aplicaciones. (Sandra Gittlen, 2021)

2.2.5.2. SD-WAN vs WAN tradicional.

Las WAN tradicionales también tienen muchas funciones integradas en SD-WAN, como el equilibrio de carga y la conmutación por error. Sin embargo, en las WAN tradicionales, agregar estas capacidades puede resultar complejo y requerir mucho tiempo. Las SD-WAN le permiten estandarizar, automatizar y, en tiempo real, reducir el riesgo de error humano que a menudo ocurre durante la configuración manual requerida por las WAN tradicionales. (Sandra Gittlen, 2021)

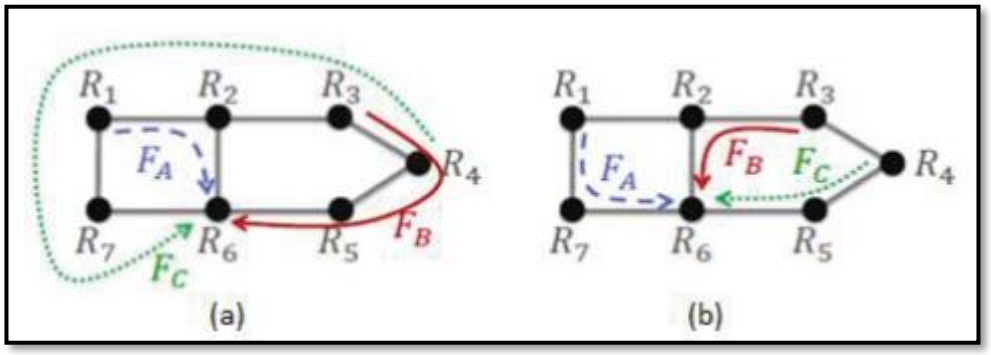
Lo más importante es que SD-WAN detecta automáticamente las condiciones de la red y proporciona visibilidad en la red, creando el nivel óptimo de rendimiento en el lado del cliente. Razón por la cual es motivo de mi trabajo, ya que se le ofrece al cliente empresarial una solución que facilite la labor del operador de red y también reduzca el impacto de falla en el lado cliente.

2.2.5.3. SD-WAN vs MPLS.

MPLS ha sido una opción de conectividad confiable para las organizaciones durante décadas, pero también es costosa y algo rígida. La arquitectura SD-WAN permite que las organizaciones o empresas continúen utilizando circuitos MPLS, mientras logran una mayor eficiencia y ahorros de costos con la adición de enlaces alternativos más baratos, como banda ancha o inalámbricos. (Sandra Gittlen, 2021)

SD-WAN proporciona una descripción general centralizada del estado actual de la red de clientes corporativos, que se utilizará para una toma de decisiones óptima al asignar recursos. En la siguiente figura 6, visualizamos como la tecnología tradicional toma decisiones no óptimas para asignar o dirigir los recursos, mientras que SD-WAN se basa en tomar óptimas decisiones.

Figura 6. (a) Toma de decisiones usando tecnología tradicional. (b) Toma de decisiones usando SD-WAN



Fuente: Tomado de Hong et al. (2013)

En resumen, “SD-WAN necesita detectar la aplicación y la calidad del enlace en tiempo real y ejecutar dinámicamente las políticas de dirección del tráfico cuando no se cumplen las aplicaciones o la calidad del enlace.”. (Pág. 6-13. Cheng Sheng, Jie Bai, Qi Sun-, 2021).

Así mismo las funcionalidades y características por cada tecnología difieren muchísimo. En la siguiente figura 7, se muestra un cuadro comparativo que muestra las principales aplicaciones de cada tecnología.

Figura 7. Cuadro comparativo: SD-WAN vs MPLS

Features	SD-WAN	MPLS Dedicated	MPLS Hybrid
Attractive Pricing	✓		✓
Full Mesh VPN	✓	✓	
Rapidly Add New Applications	✓		
Application Performance Monitoring	✓		
Optimize Support of Cloud Applications	✓		
Load Balancing included as Standard	✓		
3G/4G Failover	✓	✓	✓
Dynamic Path Selection	✓		
Voice / Real-time Application Failover	✓		
Bi-directional priority routing at all locations	✓	✓	
Advanced Firewall & UTM	✓	✓	✓
Access Redundancy Included as Standard	✓		✓

Fuente: https://www.fusionconnect.com/blog/blog-archive/sd-wan-vs-mpls/

En este sentido, teniendo en cuenta la comparación entre estas dos tecnologías de comunicación, es que el trabajo de suficiencia profesional se basa en la migración de un servicio de internet utilizando la tecnología SD-WAN como solución, la cual le brindará mayor eficiencia en sus enlaces y tendrá un considerable ahorro de costos en su implementación.

2.2.6. Cortafuegos (FIREWALL)

Un firewall es una solución de seguridad de red que protege su red del tráfico no deseado. Los cortafuegos bloquean el programa maligno entrante según un conjunto de reglas preprogramadas. Estas reglas también pueden evitar que los usuarios dentro de la red accedan a ciertos sitios y programas.

Los cortafuegos se basan en la simple idea de que el tráfico de red de entornos menos seguros debe autenticarse e inspeccionarse antes de pasar a un entorno más seguro, evitando que usuarios, dispositivos y aplicaciones no autorizados entren en un segmento, red o entorno protegido. En su red son susceptibles a los piratas informáticos y lo convierten en un blanco fácil de ataques. (Fortinet, s.f.)

2.2.6.1. Importancia de los cortafuegos.

Los firewalls de red son componentes fundamentales de la infraestructura de seguridad de una organización. Su trabajo principal es monitorear el tráfico entrante y saliente y permitirlo o bloquearlo. Ayudan a proteger la red de amenazas como:

- Software malicioso
- Exploits
- Páginas web maliciosas

Algunas de las consecuencias inmediatas de una violación del firewall son la interrupción en toda la empresa, lo que resulta en una pérdida de productividad. Los problemas a largo plazo incluyen violaciones de datos y daños a la reputación. (Fortinet, s.f.)

2.2.6.2. Tipos de cortafuegos.

Los principales de tipos de firewall o cortafuegos son los siguientes:

- Cortafuegos de aplicaciones web (WAF)
- Cortafuegos de gestión unificada de amenazas (UTMF)
- Cortafuegos de traducción de direcciones de red
- Cortafuegos de segmentación interna (ISFW)
- Cortafuegos de próxima generación (NGFW)

2.2.7. Software emulador de redes

El software de emulación de red facilita que los estudiantes (por ejemplo, las personas que se preparan para los exámenes de Cisco) aprendan los conceptos básicos de las redes informáticas y TCP / IP en general. Incluso los profesionales podrían beneficiarse de estas herramientas al estudiarlas y hacerse una idea de cómo funciona y funcionará una red antes de la implementación real.

Además, los administradores de sistemas o red podrían utilizarlos como campos de prueba para nuevas topologías de red y pruebas de sistemas. El entorno de simulación permite a los especialistas probar ideas sin dañar las redes existentes.

Entre los principales emuladores de red tenemos los siguientes: GNS3, EVE-NG, Cisco VIRL entre otros.

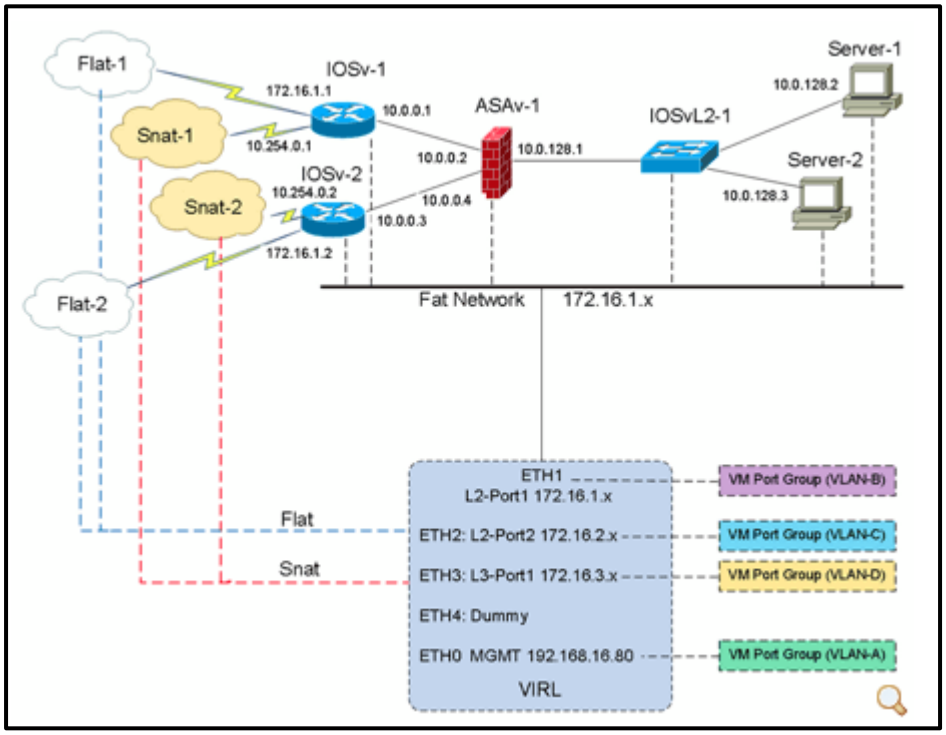
2.2.8. Principales emuladores de red

2.2.8.1. Cisco VIRL.

Cisco Virtual Internet Routing Lab (VIRL) es una herramienta de software que Cisco desarrolló para crear y ejecutar simulaciones de red sin necesidad de hardware físico.

VIRL es una plataforma basada en OpenStack que ejecuta imágenes de software IOSv, IOSvL2, IOS XRv, NX-OSv, CSR1000v y ASAv en el hipervisor integrado. VIRL proporciona un entorno de simulación y diseño de red amplia y escalable utilizando la interfaz VM Maestro. VIRL también tiene una amplia capacidad para integrarse con máquinas virtuales de terceros como Juniper, Palo Alto Networks, Fortinet, F5 BigIP, Extreme Networks, Arista, Alcatel, Citrix y más. (Jack Wang, s.f.). En la siguiente figura 8 observamos una topología de red en CISCO VIRL.

Figura 8. Topología de red en Cisco VIRL



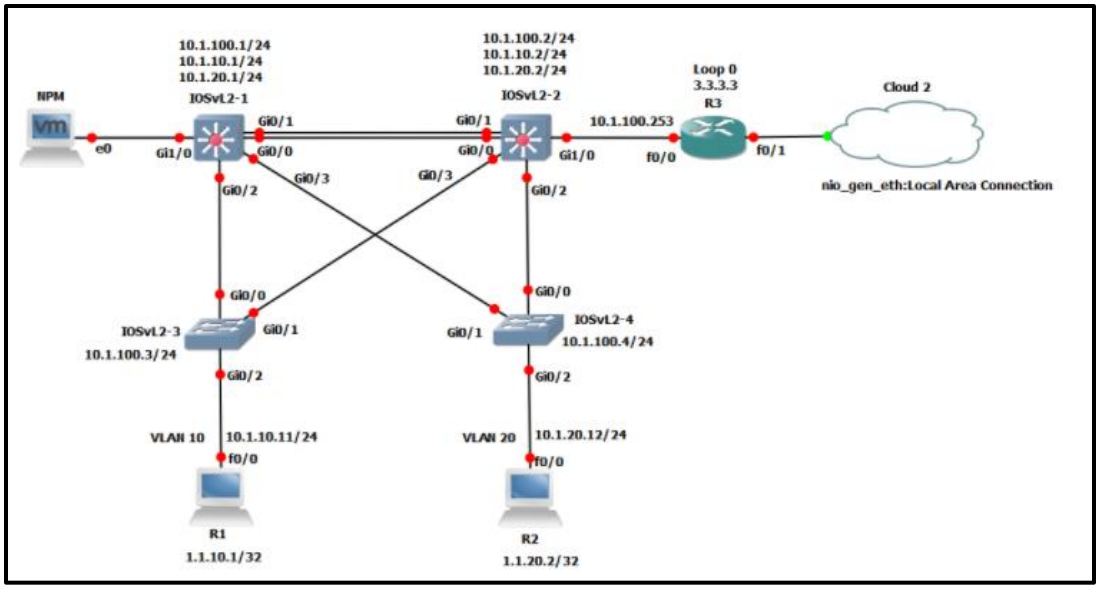
Fuente: https://www.firewall.cx/cisco-technical-knowledgebase/cisco-services-tech/1172-cisco-virl-virtual-internet-routing-lab-introduction.html

2.2.8.2. Graphical Network Simulator (GNS3).

GNS3 es utilizado por cientos de miles de ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, hasta aquellos que tienen muchos dispositivos alojados en varios servidores o incluso alojados en la nube. (GNS3, s.f.).

En la siguiente figura 9, visualizamos una topología de red en el GNS3.

Figura 9. Topología de red en GNS3



Fuente: https://docs.gns3.com/docs/

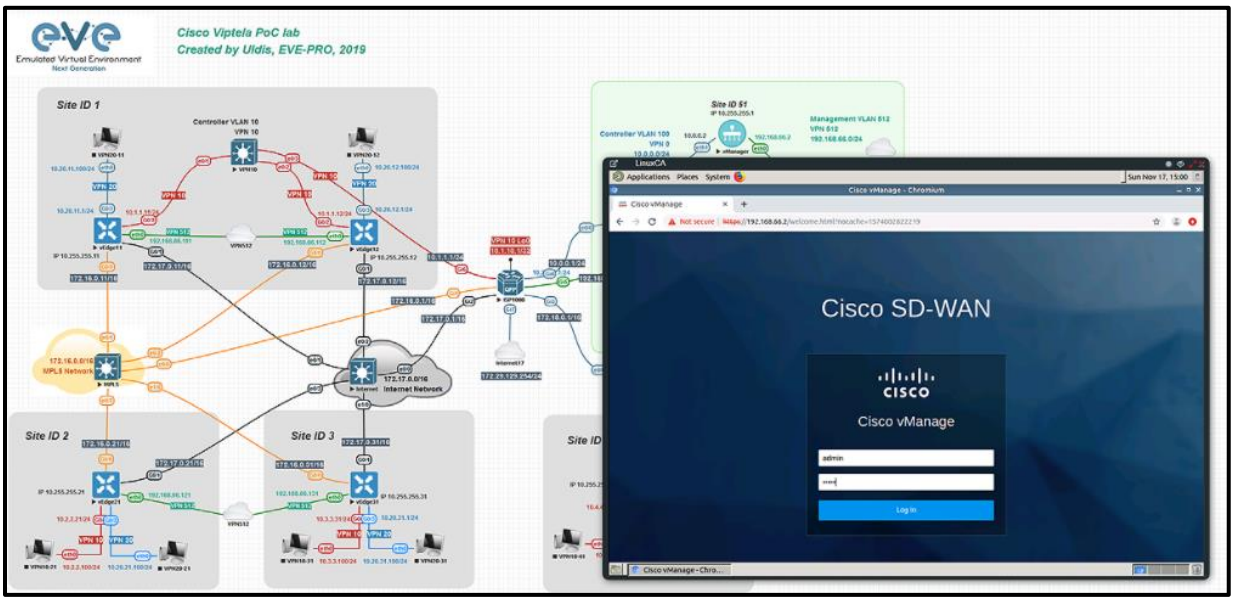
2.2.8.3. Emulated Virtual Enviroment – Next Generation (EVE-NG).

EVE-NG es una herramienta similar a GNS3 que proporciona a los administradores de red formas de simular enrutadores, conmutadores, cortafuegos y muchos otros dispositivos virtuales. Puede crear un laboratorio de red con dispositivos de Cisco, Juniper, Citrix, Arista, A10, Alcatel, Checkpoint, F5, Palo Alto, PFSense, SonicWALL, Trend Micro TippingPoint vTPS y mucho más

EVE-NG le brinda herramientas para usar en dispositivos virtuales e interconectarlos con otros dispositivos virtuales o físicos. Muchas de sus funciones simplifican enormemente la usabilidad, reutilización, manejabilidad, interconectividad, distribución y por lo tanto la capacidad de comprender y compartir topologías, trabajos, ideas, conceptos o simplemente “laboratorios”. Esto puede simplemente significar reducirá el costo y el tiempo para configurar lo que necesita o podría permitirle realizar las tareas que necesita. (EVE-NG, CookBook, s.f.).

En la siguiente figura 10, visualizamos una topología de red en el EVE-NG.

Figura 10. Topología de red en EVE-NG



Fuente: https://www.eve-ng.net/index.php/screenshots/

En la siguiente tabla 1 observamos una comparación básica entre los principales emuladores de red.

Tabla 1. Cuadro comparativo entre los principales emuladores de red

	GNS3	CISCO VIRL	EVE-NG
SOFTWARE	Es un software Open Source y es de libre uso para cualquier usuario.	Es un software de paga anual.	Es un software de libre uso y también cuenta con una versión de paga.
INTERFAZ	Requiere la instalación local del software (GUI) y además requiere un virtualizador (VmWare, Esxi, VirtualBox).	Requiere software de virtualización (VMware Workstation Player / Pro, Fusion o ESXi).	Requiere tan solo el virtualizador para poder ejecutar el EVE-NG, ya que utiliza una interfaz HTML5 (Cliente WEB), sin software GUI adicional.
IMÁGENES SOPORTADAS	Admite todas las imágenes VIRL (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASAv) y también soporta multiples proveedores.	Sin soporte de múltiples proveedores: solo es compatible con dispositivos de red de Cisco (IOSv, IOSvL2, ASAv).	Admite todas las imágenes VIRL, y soporta multiples proveedores (Fortigate, Juniper, Cisco, Windows, Linux, Firepower, etc)
RECURSOS	La utlización de los recursos de la PC/Server se ve aminorada por las limitaciones en la caracteristicas del equipo local.	Intensivo en recursos (requiere grandes cantidades de RAM y CPU)	Los cantidad de recursos a utilizar pueden ser modificados durante la instalación y adecuarlo a las caracteristicas de tu equipo.

Fuente: Elaboración propia.

EVE-NG tiene más ventajas en modo interactivo, que es completamente diferente de GNS3. GNS3 se parece más a un software utilizado por los usuarios, y solo se puede utilizar el sistema operativo compatible con GNS3; mientras que EVE-NG se parece más a un modelo CS, EVE-NG es el servidor y el usuario puede ser cualquier sistema operativo que admita http / https. EVE-NG nos ofrece trabajar en un entorno virtual con las imágenes propias de cada equipamiento (CISCO, Fortinet, Juniper, etc). Así mismo brinda un entorno amigable, ya que utiliza una interfaz HTML5 lo cual facilita la labor de operador de red al momento de diseñar. Es por ello por lo que para este trabajo de suficiencia profesional se utiliza el software EVE-NG para poder realizar la simulación y comprobar la operatividad de la red. Así mismo los recursos utilizados por la PC/Laptop/Server pueden adecuarse con respecto a las características o limitaciones de cada equipo. Como sustento de su uso del EVE-NG es que ya estaba adquirido por la empresa y por el análisis comparativo anterior consideramos su utilidad en nuestro trabajo de suficiencia profesional.

2.3. Definición de términos básicos

SD-WAN: Una red de área amplia definida por software es un servicio virtualizado que conecta y extiende redes corporativas a grandes distancias geográficas. SD-WAN monitorea el rendimiento de las conexiones WAN y administra el tráfico para mantener altas velocidades y optimizar la conectividad.

ISP: El término proveedor de servicios de Internet (ISP) se refiere a una empresa que proporciona acceso a Internet tanto a clientes personales como comerciales.

MPLS: Multiprotocol Label Switching o MPLS, por su traducción: conmutación de etiquetas multiprotocolo, es un estándar para transmitir datos bajo diferentes etiquetas, creado por la Internet Engineering Task Force, una organización dedicada a mejorar el flujo de trabajo de Internet.

SDN: La red definida por software (SDN) es un enfoque de la red que utiliza controladores basados en software o interfaces de programación de aplicaciones (API) para comunicarse con la infraestructura de hardware subyacente y el tráfico directo en una red.

NFV: La virtualización de funciones de red (NFV) es una forma de virtualizar servicios de red, como enrutadores, firewalls y equilibradores de carga, que tradicionalmente se han ejecutado en hardware propietario.

WAN: Una red de área amplia (Wide Area Network, o WAN) es una red privada de telecomunicaciones geográficamente distribuida que interconecta múltiples redes de área local (LAN).

LAN: Una red de área local (LAN) consta de una serie de computadoras conectadas entre sí para formar una red en una ubicación circunscrita. Las computadoras en una LAN se conectan entre sí a través de TCP / IP ethernet o Wi-Fi.

INTERNET: Internet es una red de área amplia global que conecta sistemas informáticos en todo el mundo. Incluye varias líneas de datos de gran ancho de banda que componen la "columna vertebral" de Internet.

TCP/IP: Es un protocolo de enlace de datos que se utiliza en Internet para permitir que las computadoras y otros dispositivos envíen y reciban datos. TCP / IP significa Protocolo de control de transmisión / Protocolo de Internet y hace posible que los dispositivos conectados a Internet se comuniquen entre sí a través de redes. (Cloudfare, s.f.)

TI: La tecnología de la información (TI) es el uso de cualquier computadora, almacenamiento, redes y otros dispositivos físicos, infraestructura y procesos para crear, procesar, almacenar, proteger e intercambiar todas las formas de datos

electrónicos. (Rich Castagna, s.f.)

QoS: La calidad de servicio (QoS) es un conjunto de tecnologías que funcionan en una red para garantizar su capacidad para ejecutar de manera confiable aplicaciones y tráfico de alta prioridad con una capacidad de red limitada. Las medidas que preocupan a la QoS son el ancho de banda (rendimiento), la latencia (retraso), la fluctuación (variación en la latencia) y la tasa de error. (Palo Alto Networks, s.f.)

TAC: El TAC significa centro de asistencia técnica. Proporciona servicios completos de hardware, software, planificación y resolución de problemas a los clientes de una empresa de redes y telecomunicaciones.

Enrutadores: Un enrutador es un dispositivo que conecta dos o más redes o subredes de conmutación de paquetes. Existen varios tipos de enrutadores, pero la mayoría de los enrutadores pasan datos entre LAN y WAN. (Cloudfare, s.f.)

Conmutadores: Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red.

Ancho de Banda: El ancho de banda se refiere a la cantidad de datos que se pueden transmitir en un período de tiempo fijo. (Intel, s.f.)

Alta disponibilidad: Un protocolo de alta disponibilidad, conocido por sus siglas en ingles HA (High Availability) se aplica cuando queremos tener un plan de contingencia sobre cualquier componente que tenga alguna situación anómala para poder seguir dando el servicio. (IMF -Formación, s.f.)

Seguridad Perimetral: La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de

intrusos en instalaciones especialmente sensibles.

Latencia: La latencia es el tiempo que tarda en transmitirse un paquete de datos dentro de la red. Es decir, es el tiempo exacto que pasa desde que tu dispositivo hizo una solicitud al servidor y el tiempo que tardas en recibir una respuesta desde el servidor. (Movistar CL, s.f.)

Redes Empresariales: Las redes empresariales se suelen centrar en los estándares LAN, que normalmente utilizan conmutadores de hardware, dispositivos de enrutamiento, cableado de Ethernet, conexiones wifi y software de cortafuegos integrado para crear una red de área local. (VMware, s.f.)

Firewall: Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad. (Cisco, s.f.)

SAF: Solicitud de Análisis de Factibilidad.

OIT: Orden Interna de Trabajo.

NAT: NAT significa traducción de direcciones de red. Es una forma de asignar varias direcciones privadas locales a una pública antes de transferir la información. (Comptia, s.f.)

SLA: El significado del acrónimo SLA es" Service Level Agreement", en español (Acuerdo de nivel de servicio o Garantía de nivel de servicio).

CAPÍTULO III: DESARROLLO DEL TRABAJO DE SUFICIENCIA PROFESIONAL

3.1. Determinación y análisis del problema

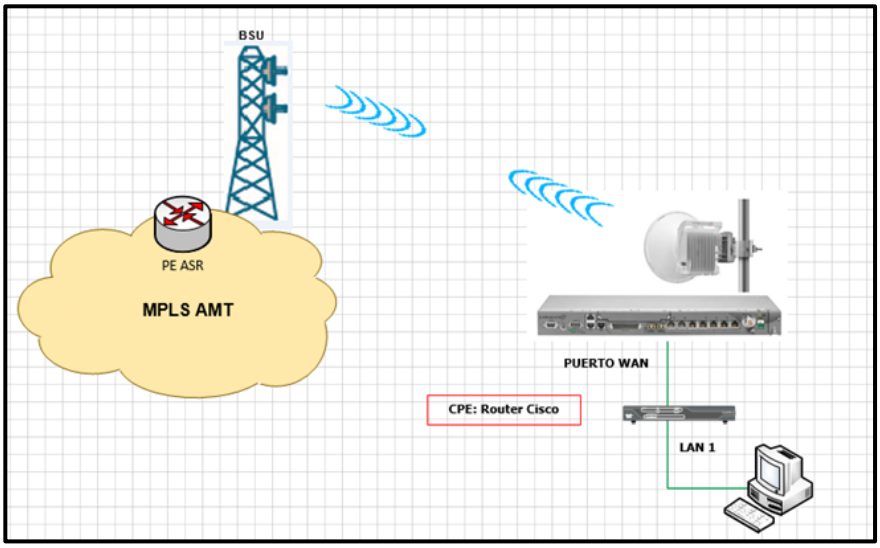
En la actualidad las empresas tienden a expandir y/o mejorar su infraestructura tecnológica, lo que les conlleva a obtener mejoras en sus servicios dedicados de internet. La robustez de los procesos en internet requiere soluciones que faciliten la manejabilidad, escalabilidad y seguridad de sus servicios.

Para nuestro caso, la empresa Compresores del Perú solicitó se realice una mejora en la conectividad hacia internet para poder satisfacer sus necesidades en la nueva sede en donde establecerá su centro de operaciones. Es por ello por lo que para obtener esta mejora nos generamos la interrogante siguiente: ¿Es posible determinar una propuesta de implementación sobre una red de cliente empresarial en el software EVE-NG utilizando la tecnología SD-WAN? Ante esta premisa, el objetivo principal es determinar esta propuesta de red y para esto se tuvo que analizar la situación actual de la red del cliente, el cual se detalla más adelante. Una vez analizada la situación actual de la red se podrá contar con el diseño de red, la cual se simulará en el software EVE-NG para poder cumplir los objetivos propuestos y el requerimiento actual del cliente.

Así mismo lo que se busca con la simulación a través del software EVE-NG es demostrar la validez de la red a implementar en el cliente. Con esta simulación se pudo obtener los resultados de conectividad hacia internet, alta disponibilidad y conectividad entre los usuarios internos de su red.

Anteriormente el cliente contaba con un solo enlace de internet (radio enlace) y un ancho de banda de 25 Mbps con un CIR 1:1. En la siguiente figura 11 se muestra la topología para este cliente.

Figura 11. Topología del Radio Enlace



Fuente: Elaboración propia

Este enlace fue brindado con la capacidad Radio enlace mediante equipamientos CERAGON y como enrutador final CISCO, el cual no le brindaba seguridad gestionada a su red local, por la antigüedad de la versión del equipo.

Durante el período de 2019 al 2020 las caídas que experimentaba el cliente con respecto a su servicio de internet afectaban su operación. En la siguiente tabla 2 se muestra el consolidado de tiques de avería presentados entre los años 2019 y 2020 principalmente por fallas en el radio enlace o enrutador.

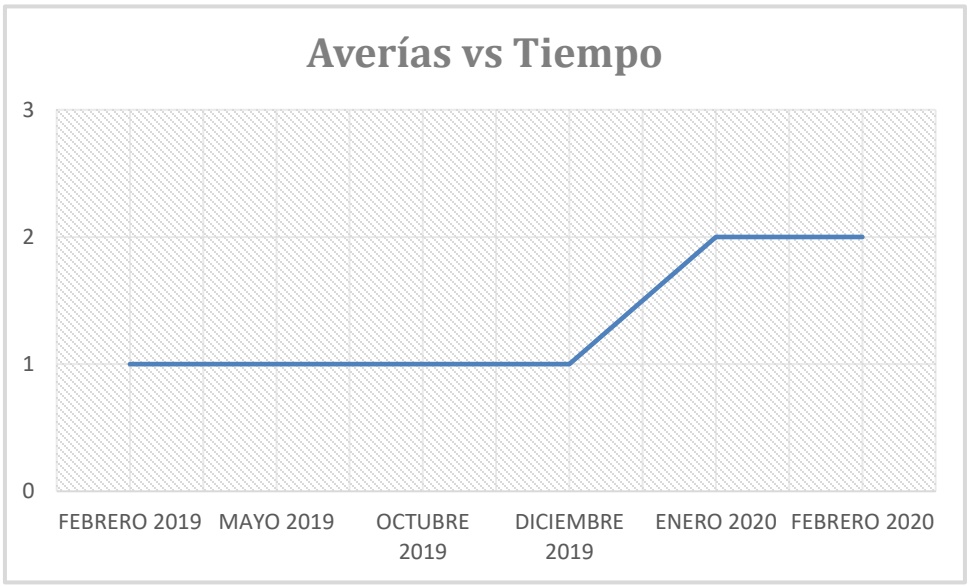
Tabla 2. Averías presentadas en el lapso 2019 - 2020

N° Remedy	N° Regulado	MES	AÑO	TIPO de TICKET
INC000000188499	A15071457	FEBRERO	2019	RECLAMO DE AVERÍA
INC000000233933	A14057281	MAYO	2019	RECLAMO DE AVERÍA
INC000000299246	A13055753	OCTUBRE	2019	RECLAMO DE AVERÍA
INC000000324211	A13057783	DICIEMBRE	2019	RECLAMO DE AVERÍA
INC000000331675	A13058618	ENERO	2020	RECLAMO DE AVERÍA
INC000000344126	A13059586	ENERO	2020	RECLAMO DE AVERÍA
INC000000349088	A13059945	FEBRERO	2020	RECLAMO DE AVERÍA
INC000000349596	A13059975	FEBRERO	2020	RECLAMO DE AVERÍA

Fuente: Elaboración propia

En la siguiente figura 12 podemos observar que existe una tendencia de incremento de averías presentadas comprendidas entre el mes de diciembre 2019 hacia el mes de febrero del 2020 y por lo tanto su criticidad.

Figura 12. Gráfica de averías vs Tiempo

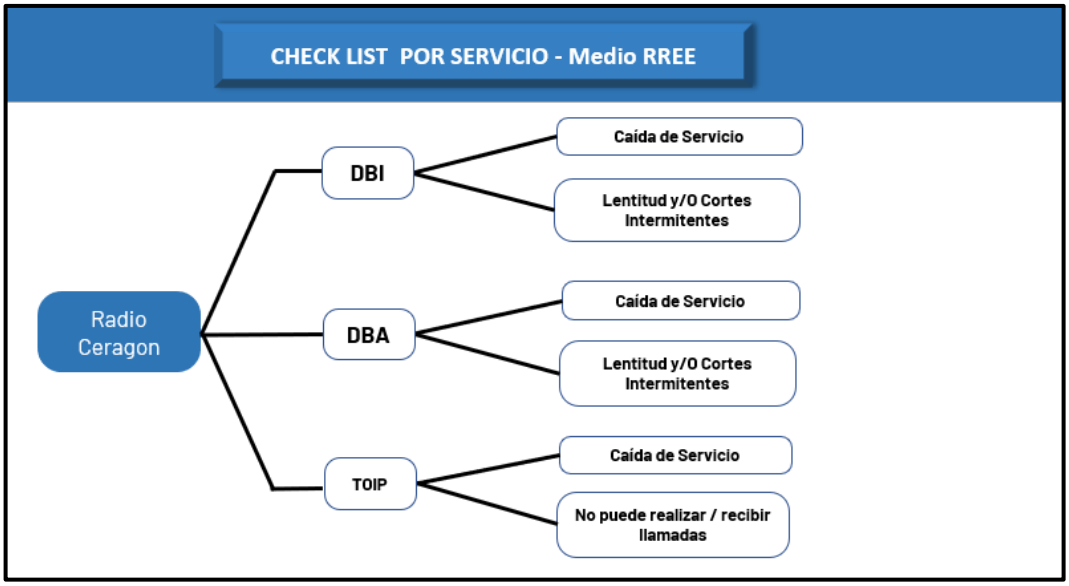


Fuente: Elaboración propia

Así mismo al tener solo un enlace de internet, no cuenta con un enlace de contingencia que solvente las caídas de su enlace y que permita la continuidad de su servicio.

Además, cuando sufría una caída de su enlace, el tiempo que tomaba en resolverse dependía de la falla que presentaba, y seguía un procedimiento de revisión por parte del operador y/o soporte. En la siguiente figura 13 se muestra el procedimiento de verificación para cada tipo de servicio.

Figura 13. Checklist por servicio



Fuente: Elaboración propia

De acuerdo con lo anterior, la problemática se desarrolló ante la necesidad de los clientes empresariales para obtener una mejora en sus servicios dedicados de internet, es por ello se determinó una propuesta de implementación de una red de cliente empresarial basada en la tecnología SD-WAN, la cual se validó a través de la simulación en el software EVE-NG obteniendo los resultados de alta disponibilidad, conectividad hacia a internet y validación del tráfico de internet.

Una vez se obtuvo los resultados de la simulación, se realizó un comparativo con los resultados reales de la red del lado cliente.

3.2. Modelo de solución propuesto

En atención a la problemática expuesta nuestra participación en la solución como parte del área de redes cliente y TAC (Technical Assistance Center) de la

empresa Entel fue desarrollar la propuesta de implementación de una red para clientes empresariales de un ISP en el software EVE-NG utilizando la tecnología SD-WAN y garantizar la seguridad perimetral del cliente con nuevo equipo Firewall Fortigate.

Nuestro trabajo se desarrolla mediante una metodología denominada en cascada, el cual se divide en 4 partes las cuales son: análisis de factibilidad, asignación de los recursos de provisión, implementación de las tecnologías de transmisión y validación de la operatividad del enlace.

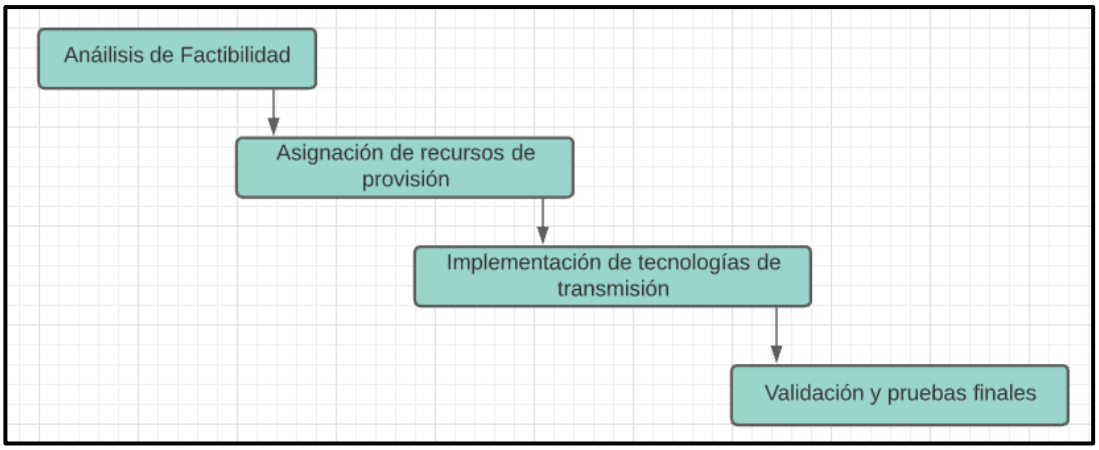
En la primera parte, se evaluó la factibilidad de la solicitud del cliente mediante una SAF (Solicitud de Análisis de Factibilidad), para determinar el equipo a utilizar y los costos de los trabajos que involucran las implementaciones de las tecnologías de transmisión.

En la segunda parte, se procedió con la asignación de recursos provisión mediante una OIT (Orden Interna de Trabajo), el cual implica la asignación de los segmentos IPs y la configuración a nivel Core y equipamiento del cliente.

En la tercera parte el área encargada de la implementación de las tecnologías de transmisión realizó los tendidos de fibra (Planta Externa) y alineamiento de los enlaces microondas (Radio Enlace) desde los nodos hasta el sitio donde está ubicado el cliente.

Por último, se realizó las pruebas de validación de la operatividad del enlace, así como también se realizó la simulación de la caída de un enlace para validar la alta disponibilidad. En conclusión, se validó los resultados de las pruebas de validación del enlace las cuales son: alta disponibilidad, conectividad hacia internet y seguridad gestionada mediante el FW Fortigate. En la siguiente figura 14 se detalla el diagrama de flujo de la metodología a seguir

Figura 14. Metodología del trabajo



Fuente: Elaboración propia

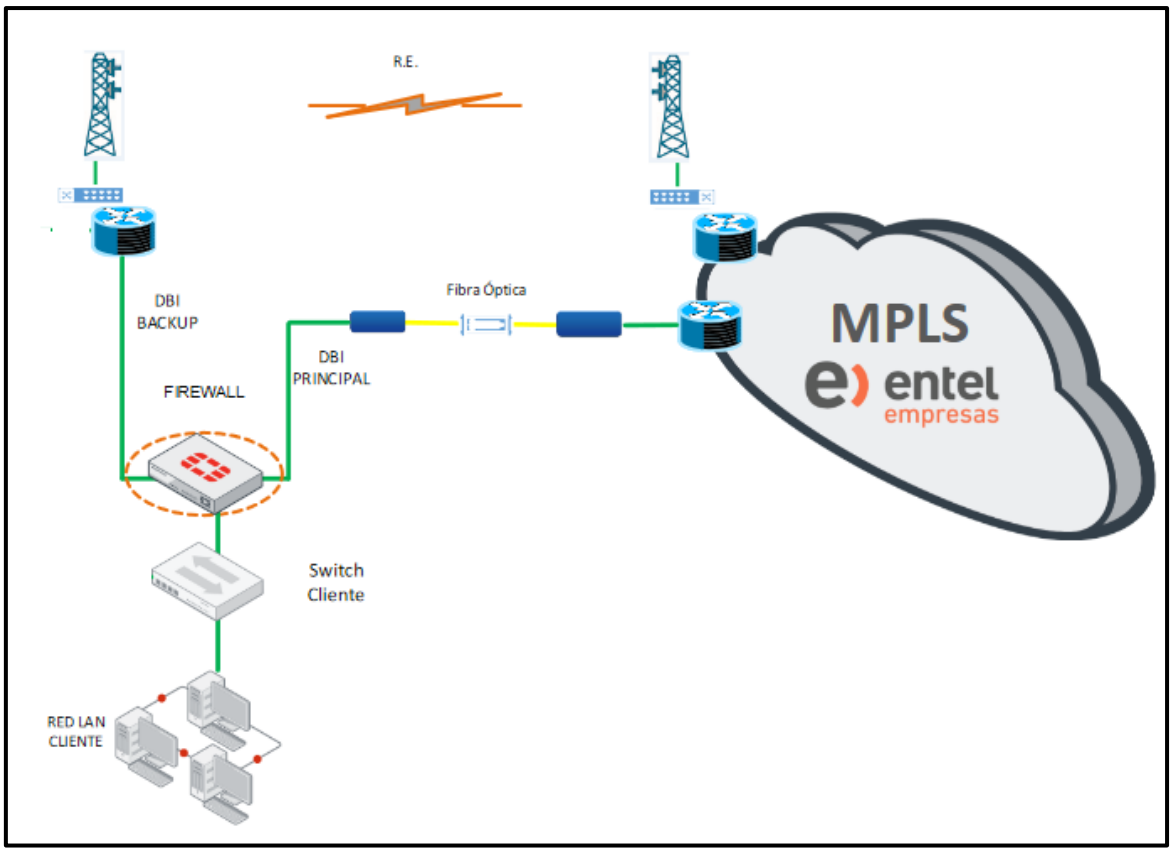
En la figura 15, se muestra el diagrama de Gantt de las actividades realizadas para la implementación de los enlaces.

Figura 15. Diagrama de Gantt de las actividades

Fuente: Elaboración propia

En la siguiente figura 16, se muestra la topología de red propuesta para la solución, sobre la cual se implementó nuestra propuesta para la red del cliente empresarial Compresores del Perú.

Figura 16. Topología de red propuesta



Fuente: Elaboración propia

Donde observamos los dos enlaces de internet conectados al equipo Firewall para la alta disponibilidad usando SD-WAN como solución. Con esto se obtuvo la mejora que solicita el cliente.

3.2.1. Análisis de factibilidad

La solicitud del cliente fue recibida a través de un gestor interno denominado SAF, en el cual se detalló el requerimiento del cliente. Para nuestro caso particular, el cliente Compresores del Perú solicitó lo siguiente:

- Mudanza de su servicio activo de internet del distrito de Chorrillos a Punta Hermosa.
- Un enlace adicional, con el cual tendrá alta disponibilidad para su redundancia.
- Seguridad gestionada.
- Ancho de Banda de 30 Mbps CIR 1:1

En el siguiente paso se definió los costos de los nuevos enlaces tanto para el de radio enlace y fibra. Así como también los equipamientos a utilizados en la sede del cliente.

En la siguiente tabla 3 se presentan los costos por cada enlace y tiempo que promedio para la implementación de las tecnologías de transmisión.

Tabla 3. Costos de la implementación de los enlaces

MEDIO	COSTO	TIEMPO	N° SAF
FO CAPEX	$840.00	33 días hábiles	236136
RE CAPEX	$4,644.20	21 días hábiles	236134

Fuente: Elaboración propia

Así mismo se estableció los equipamientos a utilizar para brindar esta solución SD-WAN, los cuales son los siguientes:

- 1 Firewall Fortigate 100E
- 1 Cisco C1111-8PLTELA

En la tabla 4 se detalla el costo del equipamiento a utilizar.

Tabla 4. Costos de los equipos de accesos

EQUIPO	COSTO	UNIDAD
Firewall Fortigate	$2,200.00	1
Cisco C1111-8PLTELA	$960.00	1

Fuente: Elaboración propia

En la tabla 5 se muestra la renta mensual por la contratación de servicios, en el cual se detalla la renta por cada enlace.

Tabla 5. Renta Mensual por contratación de servicios

ARRENDAMIENTO DE CIRCUITOS FISCOS Y/O VIRTUALES PARA ACCESO DEDICADO A INTERNET		
1	Dirección a conectar	CARRETERA PANAMERICANA SUR KM. 38 - PUNTA HERMOSA - LIMA

Valorización						
N°	Velocidad (Mbps)	Medio	Servicio	Renta Mensual Equipo Seguridad	Renta Mensual del Servicio	Plazo de Contrato (Meses)
1	30 (1:1)	Radio Enlace	Traslado	S/ 400	S/ 600	36
1	30 (1:1)	Fibra optica	Nuevo Servicio		S/ 800	36

Fuente: Elaboración propia

3.2.2. Asignación de recursos de provisión

Previamente se detalla las características de los equipos de acceso brindados para esta solución y también las características de los equipos Core.

3.2.2.1. Equipo Core.

A nivel Core, se utilizan equipamiento de la marca Huawei, los cuales están diseñados para soportar configuraciones tanto en capa 2 y capa 3. Estos se conectan directamente a los equipos de borde para brindar la salida a internet.

Para nuestro caso, de acuerdo con la topología y ubicación del cliente final. Se tiene los equipos Core denominados QUIPA y LURIN.

En la siguiente figura 17 se muestra el equipamiento Core utilizado actualmente en la red del proveedor de servicios de internet que es un enrutador Huawei de la serie NE40E-X8.

Figura 17. Equipo Core Huawei NE40E-X8

Fuente: https://www.ycict.net/es/products/huawei-ne40e-x8-router/

En la siguiente tabla 6 se muestra las características técnicas del equipamiento Core:

Tabla 6. Características técnicas equipo Core Huawei NE40E-X8

ESPECIFICACIONES TÉCNICAS	
Marca	HUAWEI
Serie	NE40E-X8
Capacidad	7.08 Tbps
Nro de SLOTS	11
Protocolos de enrutamiento	Admite el protocolo de enrutamiento estático y los protocolos de enrutamiento dinámico IPv4 como RIP, OSPF, IS-IS y BGP-4.
Estandares	IEEE802.1q, IEEE802.1p, IEEE 802.3ad, and IEEE 802.1ab.
Gestión de usuario	PAP, CHAP, MSCHAP, RADIUS, HWTACACS
Seguridad	SSH, SSH v2
Tipo de Interfaz	100 GE, 40 GE , GE, FE, CE1, CT1

Fuente: Elaboración propia

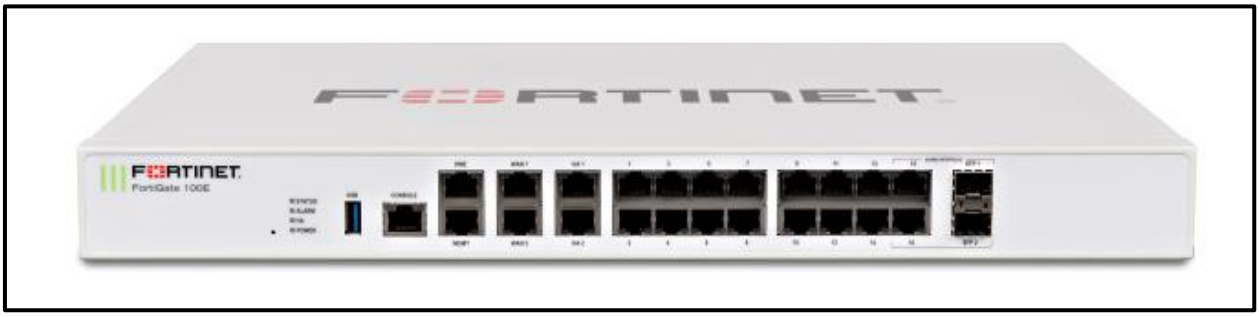
3.2.2.2. Equipos de Acceso.

Los equipos de accesos, la cuales ya fueron definidos en el apartado del análisis de factibilidad, son los enrutadores Firewall Fortigate 100E y Cisco C1111.

Los dos equipos para nuestro caso actúan en Capa 3 y tienen las funcionalidades para soportar las configuraciones necesarias para la implementación de este servicio.

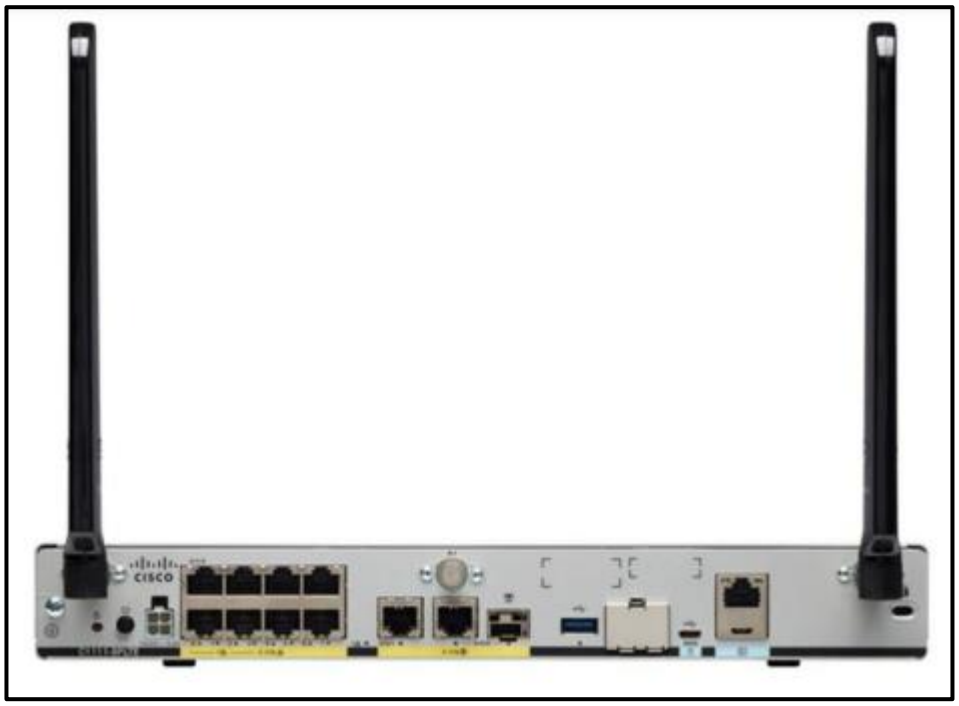
Estos dos equipos están ubicados en la sede del cliente. En las siguientes figuras 18 y 19 se observan los enrutadores de acceso a utilizar.

Figura 18. Equipo de acceso Fortigate 100E



Fuente: https://www.fortinet.com/content/dam/fortinet

Figura 19. Equipo de acceso Cisco C1111



Fuente: https://datacenter360.net/download/

Se especifica las características más relevantes de cada equipo de acceso en las tablas 7 y 8.

Tabla 7. Características técnicas equipo Fortigate 100E

ESPECIFICACIONES TÉCNICAS	
Marca	FORTINET
Serie	Fortigate 100E
Puertos	2x WAN, 14x LAN, 1x DMZ
Capacidad	7.4 Gbps
Protocolos de enrutamiento	Admite el protocolo de enrutamiento estático y los protocolos de enrutamiento dinámico IPv4 como RIP, OSPF y BGP-4.
Certificaciones	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6
Despliegue	NGFW, SD-WAN,SGW
Seguridad	SSH, Telnet, HTTPS, HTTP
Tipo de Interfaz	GE

Fuente: Elaboración propia

Tabla 8. Características técnicas equipo Cisco C1111

ESPECIFICACIONES TÉCNICAS	
Marca	CISCO
Serie	C1111-8P
Puertos	2 WAN , 8 LAN
Memoria Flash	4GB
Protocolos de enrutamiento	Admite el protocolo de enrutamiento estático y los protocolos de enrutamiento dinámico IPv4 como RIP, OSPF, IS-IS y BGP-4, entre otros.
Encapsulación	GRE, Ethernet, 802.1q VLAN, entre otros.
Gestión de usuario	WPA2,802.1x, RADIUS AAA, 802.11r
Seguridad	SSH, SSH v2 , Telnet, HTTP
Tipo de Interfaz	10,100, 1000 Ethernet

Fuente: Elaboración propia

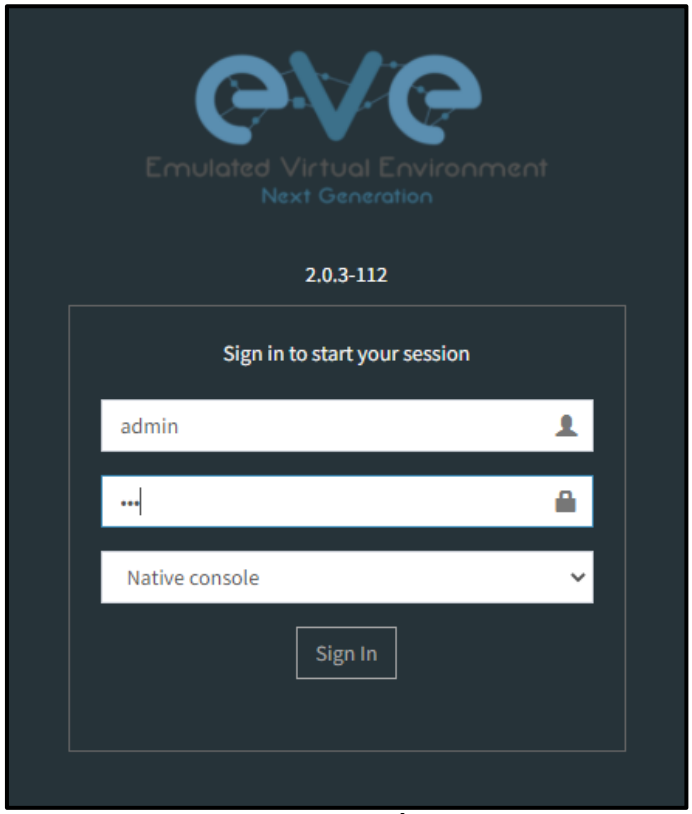
3.2.2.3. Dimensionamiento de red.

Para el dimensionamiento de red, tuvimos en cuenta la orden de trabajo interno (OIT) donde se especifica el nodo de donde se atenderá, como también los segmentos IP a asignar.

Una vez definidos los segmentos IP de prueba se procedió a diagramar el diseño propuesto en el software EVE-NG teniendo en cuenta los equipamientos a utilizar ya previamente definidos.

Para acceder a EVE-NG se debe tener una máquina virtual, en el cual se instalará el disco (.ISO) del EVE-NG una vez instalado bajo el sistema operativo LINUX, se procederá a ingresar mediante la web. En la siguiente figura 20 se muestra el perfil de ingreso al software.

Figura 20. Interfaz de acceso al EVE-NG

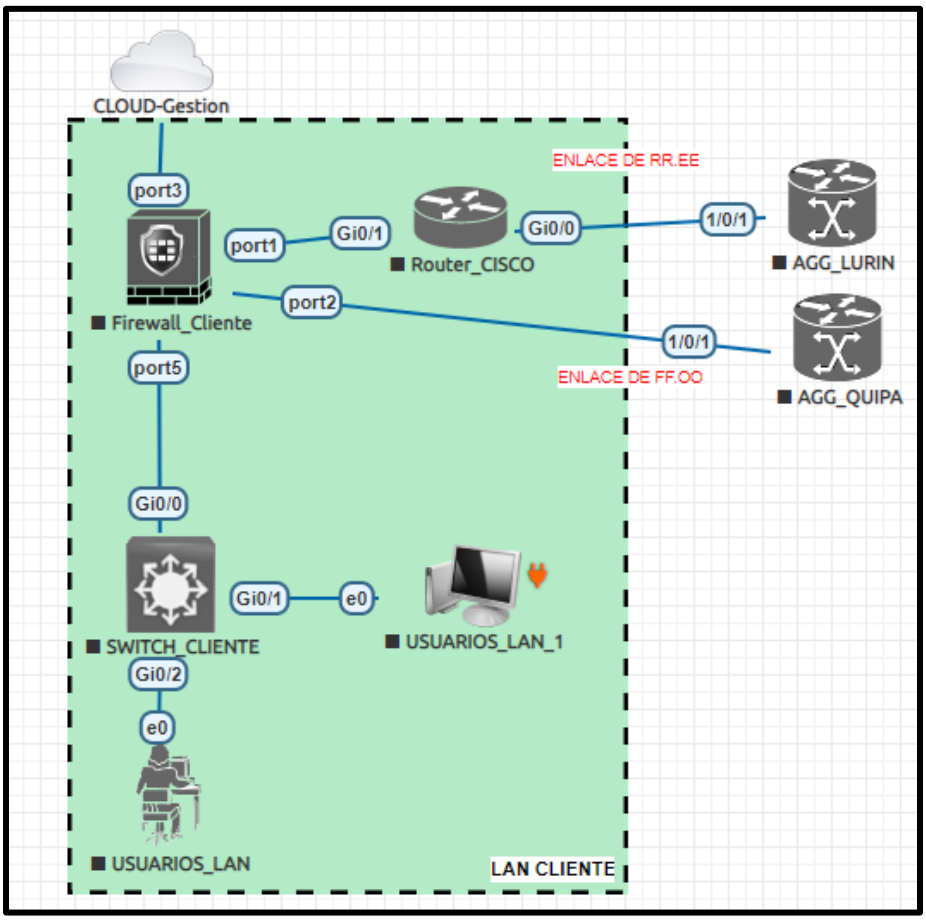


Fuente: Elaboración propia

Ya dentro de la interfaz del EVE-NG podemos utilizar las imágenes de los equipos que previamente hemos cargado con el fin de poder realizar la diagramación de estos.

En la siguiente figura 21 se tiene la vista de la red topológica del servicio en el software EVE-NG, con los equipos de Core y de acceso y la red LAN del cliente.

Figura 21. Diagrama general de la red propuesta en el software EVE-NG



Fuente: Elaboración propia

En base a ello procedimos a brindar los recursos de provisión para cada equipo Core y también para los equipos de acceso. En la siguiente tabla 9 se detalla la segmentación IP.

Tabla 9. Asignación IP para cada interfaz

EQUIPO	RED	RANGO IP	INTERFACE
AGG_QUIPA	10.10.10.0/29	10.10.10.1 - 10.10.10.6	GigabitEthernet0/0/1.906
AGG_LURIN	10.10.20.0/29	10.10.20.1 - 10.10.20.6	GigabitEthernet0/0/1.900
S383281 - FW	192.168.20.0/29	192.168.20.1 - 192.168.20.6	VLAN906
S383279 - CISCO	192.168.15.0/29	192.168.15.1 - 192.168.15.6	GigabitEthernet0/1
S383281 - FW	192.168.0.0/24	192.168.0.1 - 192.168.0.254	Port5

Fuente: Elaboración propia

Una vez definidos los segmentos de red, así como también los nodos en donde se atenderán los dos enlaces. Se procederá con la configuración.

3.2.2.4. Configuración en los equipos Core.

En los equipos Core empezamos creando las subinterfaces con las Vlans asignadas para cada enlace, así como también se tiene la interfaz física que para este caso es la interfaz Gigabit Ethernet 0/0/1.

En el agregador Nodo de Lurín asignamos la vlan 900 con la IP 10.10.20.1 máscara /29 y esta se interconecta con el equipo en el equipo Cisco C1111. En la figura 22 se muestra la configuración de la interfaz que se conecta al equipo Cisco.

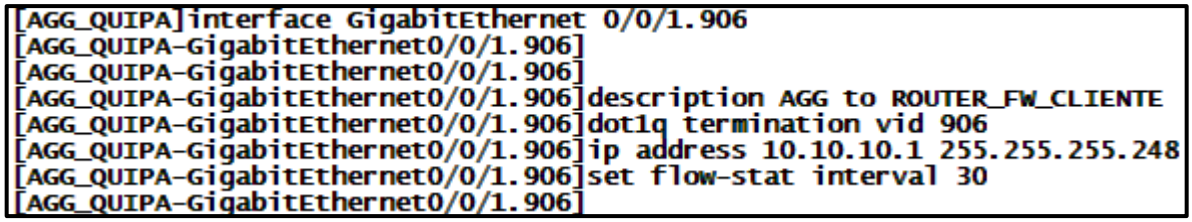
Figura 22. Creación de la subinterfaz en el nodo Lurín

```
[AGG_LURIN]interface GigabitEthernet0/0/1.900
[AGG_LURIN-GigabitEthernet0/0/1.900]
[AGG_LURIN-GigabitEthernet0/0/1.900]description AGG to ROUTER_WAN_CISCO
[AGG_LURIN-GigabitEthernet0/0/1.900]dot1q termination vid 900
[AGG_LURIN-GigabitEthernet0/0/1.900]ip address 10.10.20.1 255.255.255.248
[AGG_LURIN-GigabitEthernet0/0/1.900]set flow-stat interval 30
[AGG_LURIN-GigabitEthernet0/0/1.900]
```

Fuente: Elaboración propia

Seguidamente en el agregador Nodo de Quipa asignamos la vlan 906 con la IP 10.10.10.1 máscara /29 y esta se interconecta con el equipo firewall Fortigate 100E. En la figura 23 se muestra la configuración de la interfaz que se conectará al equipo Fortigate 100E.

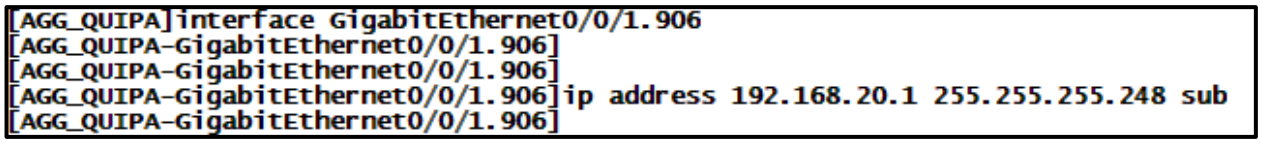
Figura 23. Creación de la subinterfaz en el nodo Quipa



Fuente: Elaboración propia

Como parte de una configuración adicional sobre esta subinterfaz configuramos una IP adicional que actúa como IP secundaria. En la figura 24 se muestra la IP 192.168.20.1 máscara /29 como secundaria.

Figura 24. Adición de IP secundaria sobre la vlan 906



Fuente: Elaboración propia

De esta manera se termina la configuración en los equipos Core. Para la salida a internet, estos equipos ya están conectados a los equipos de Borde del proveedor de servicios de internet (ISP).

3.2.2.5. Configuración en los equipos de acceso.

En los equipos de acceso iniciamos creando las subinterfaces WAN para cada equipo que sirve también como subinterfaces de gestión remota del equipo, estas vienen de la interconexión de los puertos físicos brindados en los nodos. Y después se procedió con las demás configuraciones tanto para el Cisco C1111 y el equipo Fortigate 100E.

- **Configuración de la subinterfaz WAN del enrutador CISCO**

Procedimos creando la subinterfaz Gigabit Ethernet 0/0 con la vlan 900 en el enrutador Cisco y se configura la IP 10.10.20.2 máscara /29. En la siguiente figura 25 se muestra la configuración de la subinterfaz WAN del enrutador Cisco.

Figura 25. Creación de la subinterfaz WAN en el enrutador Cisco

```
S383279_CISCO(config)#interface gigabitEthernet 0/0.900
S383279_CISCO(config-subif)#
S383279_CISCO(config-subif)#description WAN_CISCO
S383279_CISCO(config-subif)#encapsulation dot1Q 900
S383279_CISCO(config-subif)#ip address 10.10.20.2 255.255.255.248
```

Fuente: Elaboración propia

- **Configuración de la ruta por defecto en el enrutador CISCO**

Configuramos la ruta por defecto apuntando hacia la puerta de enlace, es decir la IP configurada en la subinterfaz del nodo Lurín IP 10.10.20.1, en la figura 26 se muestra la configuración de la ruta por defecto.

Figura 26. Creación de la ruta por defecto en el enrutador Cisco

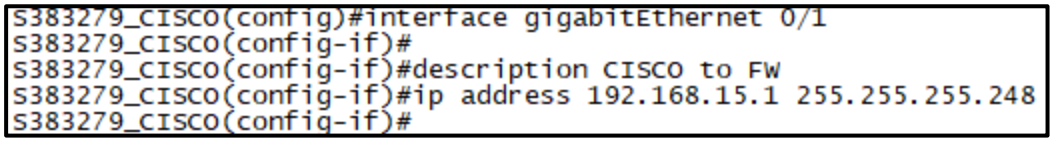
```
S383279_CISCO(config)#
S383279_CISCO(config)#ip route 0.0.0.0 0.0.0.0 10.10.20.1
S383279_CISCO(config)#
```

Fuente: Elaboración propia

- **Configuración de la interfaz de conexión hacia el FW**

Seguidamente, configuramos la IP asignada para la interconexión del Cisco hacia la WAN de Firewall. En la siguiente figura 27 se muestra la configuración de la interfaz Gigabit Ethernet 0/1 del enrutador Cisco.

Figura 27. Creación de la interfaz Gigabit Ethernet 0/1 en el enrutador

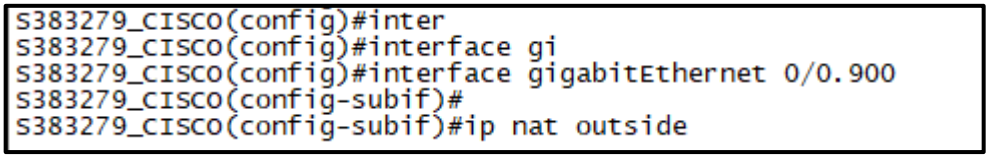


Fuente: Elaboración propia

- **Configuración del NAT y ACL en el enrutador CISCO**

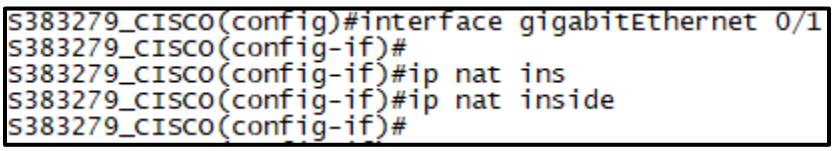
Para poder brindar la salida a internet a la interfaz Gigabit Ethernet 0/1 se necesita crear un NAT (Network Address Translation) que realizará las traducciones del segmento de red 192.168.15.0/29 hacia la interfaz WAN del enrutador cisco. Ante esto, definimos las interfaces que actúan como inside (Gigabit Ethernet 0/0) y outside (Gigabit Ethernet 0/1). En las siguientes figuras 28 y 29 se muestran la ejecución de los comandos.

Figura 28. Asignación de la interfaz outside



Fuente: Elaboración propia

Figura 29. Asignación de la interfaz inside



Fuente: Elaboración propia

Paso seguido, procedimos a crear la lista de acceso (ACL) sobre la red 192.168.15.0/29 y con esto se culmina la configuración de NAT. En la figura 30 se muestra la ejecución de los comandos del ACL y NAT.

Figura 30. Configuración de ACL y NAT

```
S383279_CISCO(config)#access-list 10 permit 192.168.15.0 0.0.0.7
S383279_CISCO(config)#ip nat inside source list 10 interface gigabitEthernet0/$
S383279_CISCO(config)#
```

Fuente: Elaboración propia

Con esto podemos demostrar que las traducciones se realicen de manera correcta y se verifica que la interfaz que contiene el segmento 192.168.15.0/29 tenga conectividad hacia internet. En la figura 31 se muestra los resultados de la configuración del NAT.

Figura 31. NAT del segmento red 192.168.15.0

```
S383279_CISCO#ping 8.8.8.8 source GigabitEthernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.15.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 61/76/95 ms
S383279_CISCO#
S383279_CISCO#sh ip nat
S383279_CISCO#sh ip nat tran
S383279_CISCO#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.10.20.2:6      192.168.15.1:6     8.8.8.8:6          8.8.8.8:6
udp 10.10.20.2:1263    192.168.15.2:1263  173.243.138.221:53 173.243.138.221:53
udp 10.10.20.2:1452    192.168.15.2:1452  194.69.172.53:53   194.69.172.53:53
udp 10.10.20.2:1604    192.168.15.2:1604  208.184.237.71:53  208.184.237.71:53
udp 10.10.20.2:1632    192.168.15.2:1632  8.8.8.8:53         8.8.8.8:53
udp 10.10.20.2:1632    192.168.15.2:1632  208.91.112.52:53   208.91.112.52:53
udp 10.10.20.2:2493    192.168.15.2:2493  149.5.232.53:53    149.5.232.53:53
udp 10.10.20.2:2500    192.168.15.2:2500  8.8.8.8:53         8.8.8.8:53
udp 10.10.20.2:2559    192.168.15.2:2559  208.91.112.220:53  208.91.112.220:53
udp 10.10.20.2:3261    192.168.15.2:3261  83.231.212.53:53   83.231.212.53:53
udp 10.10.20.2:3314    192.168.15.2:3314  140.174.22.53:53   140.174.22.53:53
udp 10.10.20.2:3776    192.168.15.2:3776  210.7.96.53:53     210.7.96.53:53
tcp 10.10.20.2:14307   192.168.15.2:14307 206.47.184.1:443   206.47.184.1:443
tcp 10.10.20.2:18742   192.168.15.2:18742 206.47.184.6:443   206.47.184.6:443
S383279_CISCO#
```

Fuente: Elaboración propia

- **Configuración de los puertos WAN del enrutador Firewall Fortigate**

El siguiente paso es configurar el Firewall, el cual tiene la configuración de SD-WAN para balancear las cargas de los dos enlaces de internet. Se definen los puertos 1 y 2 como las interfaces WAN y el puerto 5 que conecta directamente al switch del cliente.

Para el puerto 1 se le denomina WAN RADIO y tiene la configuración como se muestra en la figura 32.

Figura 32. Configuración del puerto 1 del FW

```
S383281_FW # conf system interface
S383281_FW (interface) # edit port1
S383281_FW (port1) # set mode static
S383281_FW (port1) # set ip 192.168.15.2 255.255.255.248
S383281_FW (port1) # set allowaccess ping https ssh snmp fgfm ftm telnet
S383281_FW (port1) # set alias "WAN RADIO"
S383281_FW (port1) # set snmp-index 1
S383281_FW (port1) # end
```

Fuente: Elaboración propia

Para el puerto 2 se le denomina WAN FIBRA y tiene la configuración como se muestra en la figura 33.

Figura 33. Configuración del puerto 2 del FW

```
S383281_FW # config sys interface
S383281_FW (interface) # edit VLAN906
S383281_FW (VLAN906) # set ip 192.168.20.2 255.255.255.248
S383281_FW (VLAN906) # set allowaccess ping https ssh snmp fgfm ftm
S383281_FW (VLAN906) # set alias "VLAN906"
S383281_FW (VLAN906) # set role wan
S383281_FW (VLAN906) # set snmp-index 10
S383281_FW (VLAN906) # set interface "port2"
S383281_FW (VLAN906) # set vlanid 906
S383281_FW (VLAN906) # end
```

Fuente: Elaboración propia

- **Configuración de la interfaz SD-WAN en el enrutador Firewall Fortigate**

Una vez configurada las interfaces WAN en el enrutador FW procedimos con la ejecución de los comandos para crear la interfaz SD-WAN, el cual tiene como miembros a los puertos 1 y 2 de este equipo. En la figura 34 se muestra la configuración SD-WAN en el Firewall.

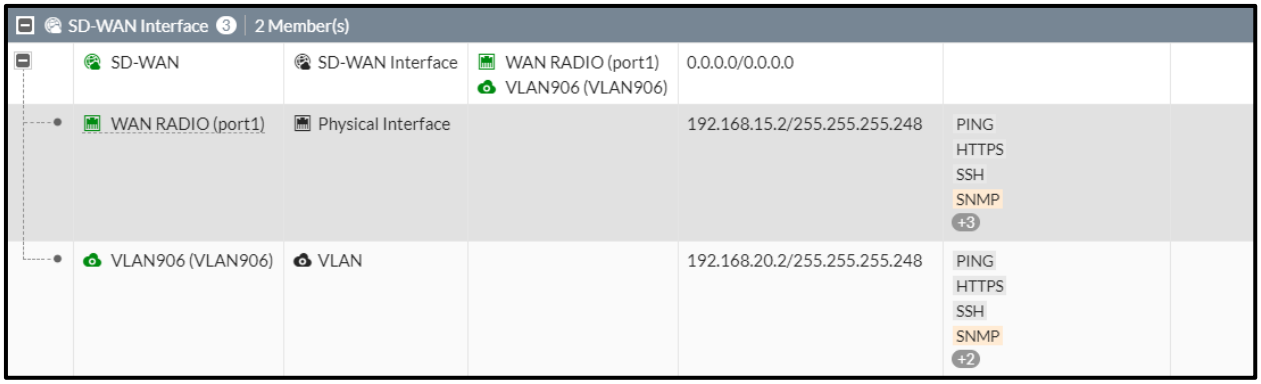
Figura 34. Configuración de la interfaz SD-WAN en el Firewall

```
S383281_FW # config system virtual-wan-link
 <Enter>

S383281_FW # config system virtual-wan-link

S383281_FW (virtual-wan-link) # set status enable

S383281_FW (virtual-wan-link) # config members

S383281_FW (members) # edit 1

S383281_FW (1) # set interface "port1"

S383281_FW (1) # set gateway 192.168.15.1

S383281_FW (1) # next

S383281_FW (members) # edit 2

S383281_FW (2) # set interface "VLAN906"

S383281_FW (2) # set gateway 192.168.20.1

S383281_FW (2) # end

S383281_FW (virtual-wan-link) # end

S383281_FW #
```

Fuente: Elaboración propia

En la siguiente figura 35 se muestra la interfaz SD-WAN creada en el Firewall.

Figura 35. Interfaz SD-WAN en el Firewall



Fuente: Elaboración propia

- **Configuración de la ruta por defecto en el enrutador Firewall Fortigate**

Al igual que en el enrutador Cisco, en el Firewall se configura la ruta por defecto hacia la interfaz SD-WAN. En la figura 36 se muestra la ejecución de comandos para habilitar la ruta estática.

Figura 36. Configuración de la ruta por defecto sobre la interfaz SD-WAN

```
S383281_FW # config router static

S383281_FW (static) # edit 1

S383281_FW (1) # set distance 1

S383281_FW (1) # set virtual-wan-link enable
 <Enter>

S383281_FW (1) # set virtual-wan-link enable

S383281_FW (1) # end

S383281_FW #
```

Fuente: Elaboración propia

- **Configuración del puerto LAN del enrutador Firewall Fortigate**

En el Firewall configuramos en el puerto 5 la red LAN del cliente. En la figura 37 se muestra la ejecución de comandos para la configuración de la red LAN.

Figura 37. Configuración del puerto 5 del FW

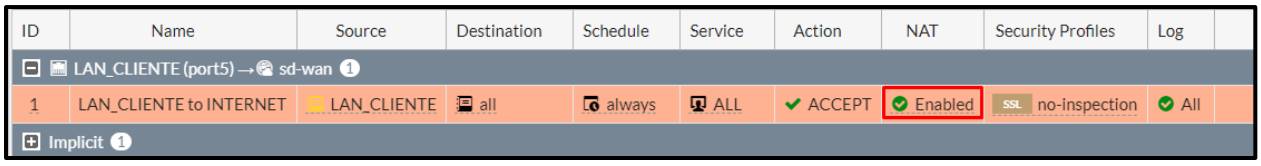
```
S383281_FW (interface) #
S383281_FW (interface) # edit port5

S383281_FW (port5) # set mode static

S383281_FW (port5) # set ip 192.168.0.1 255.255.255.0

S383281_FW (port5) # set allowaccess ping http https ssh telnet snmp

S383281_FW (port5) # set alias "LAN_CLIENTE"
```

Fuente: Elaboración propia

- **Creación de la política de enrutamiento para el acceso a internet de la red LAN**

Para que el tráfico que proviene de la LAN_CLIENTE pueda tener acceso a internet, se creó políticas de enrutamiento para brindar los permisos necesarios a la red del cliente, así como también se tuvo en cuenta el origen y destino para esta política de enrutamiento. En esta política debe estar habilitado el NAT para el enmascaramiento de las direcciones privadas hacia la dirección que actuará como pública. En la figura 38 se muestra la política de enrutamiento para la salida a internet de la LAN_CLIENTE.

Figura 38. Política de enrutamiento para el acceso a internet de la LAN

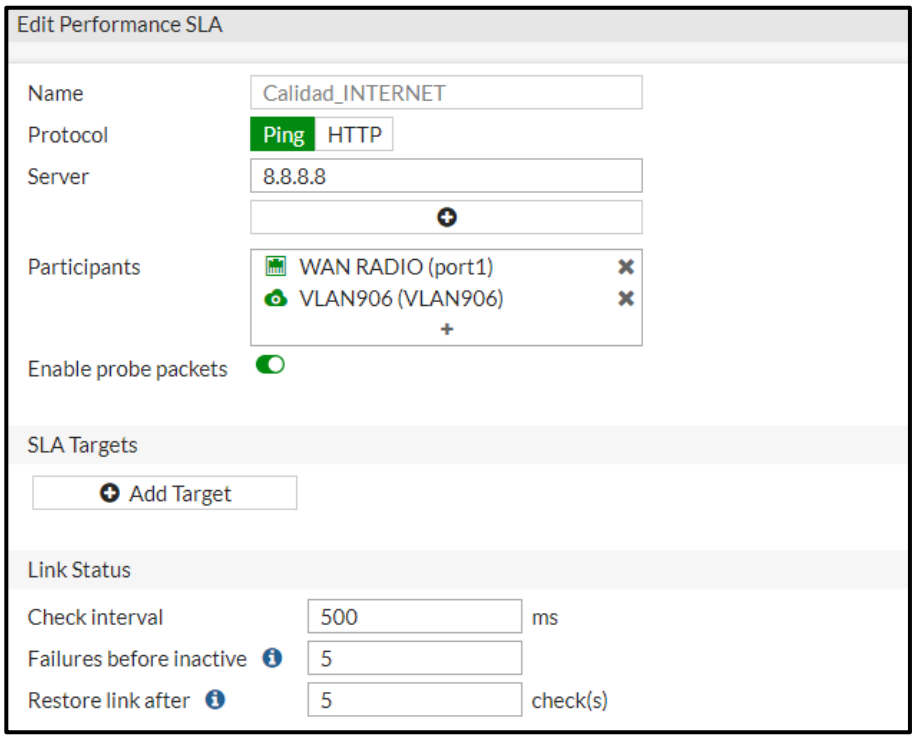


Fuente: Elaboración propia

- **Creación del parámetro de SLA en el enrutador Firewall Fortigate**

Para mejorar el rendimiento de la interfaz SD-WAN, el Firewall nos permite configurar parámetros basados en SLA (Service Level Agreement), con esto podemos optimizar el tráfico de internet hacia las interfaces WAN. En la figura 39 se define la configuración del parámetro basado en SLA hacia internet (8.8.8.8).

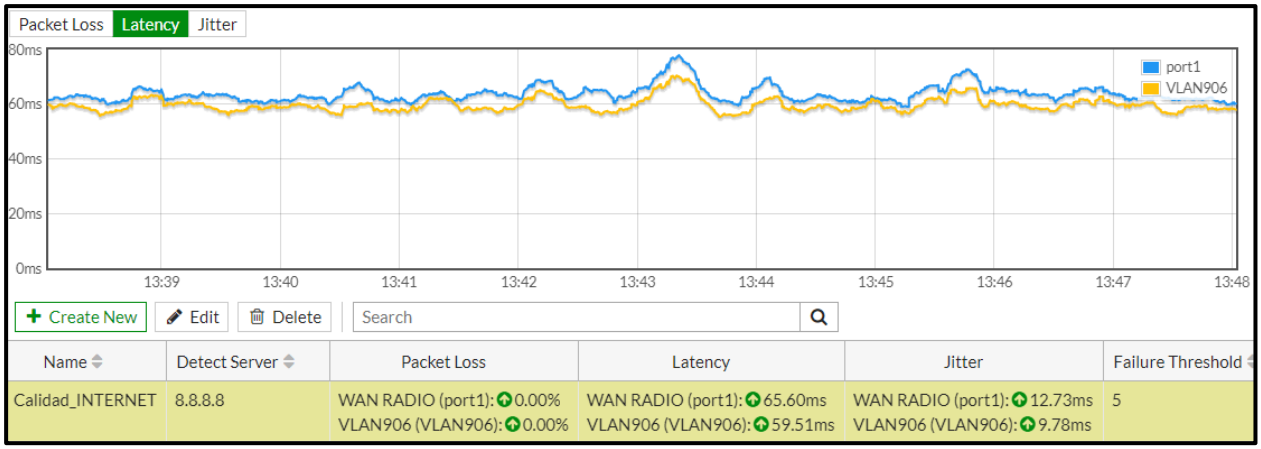
Figura 39. Configuración del parámetro del SLA



Fuente: Elaboración propia

Como visualizamos los dos enlaces tienen un comportamiento estable. En la figura 40 se observa el comportamiento de la performance del SLA en base a la conectividad hacia el servidor de Google

Figura 40. Performance del SLA

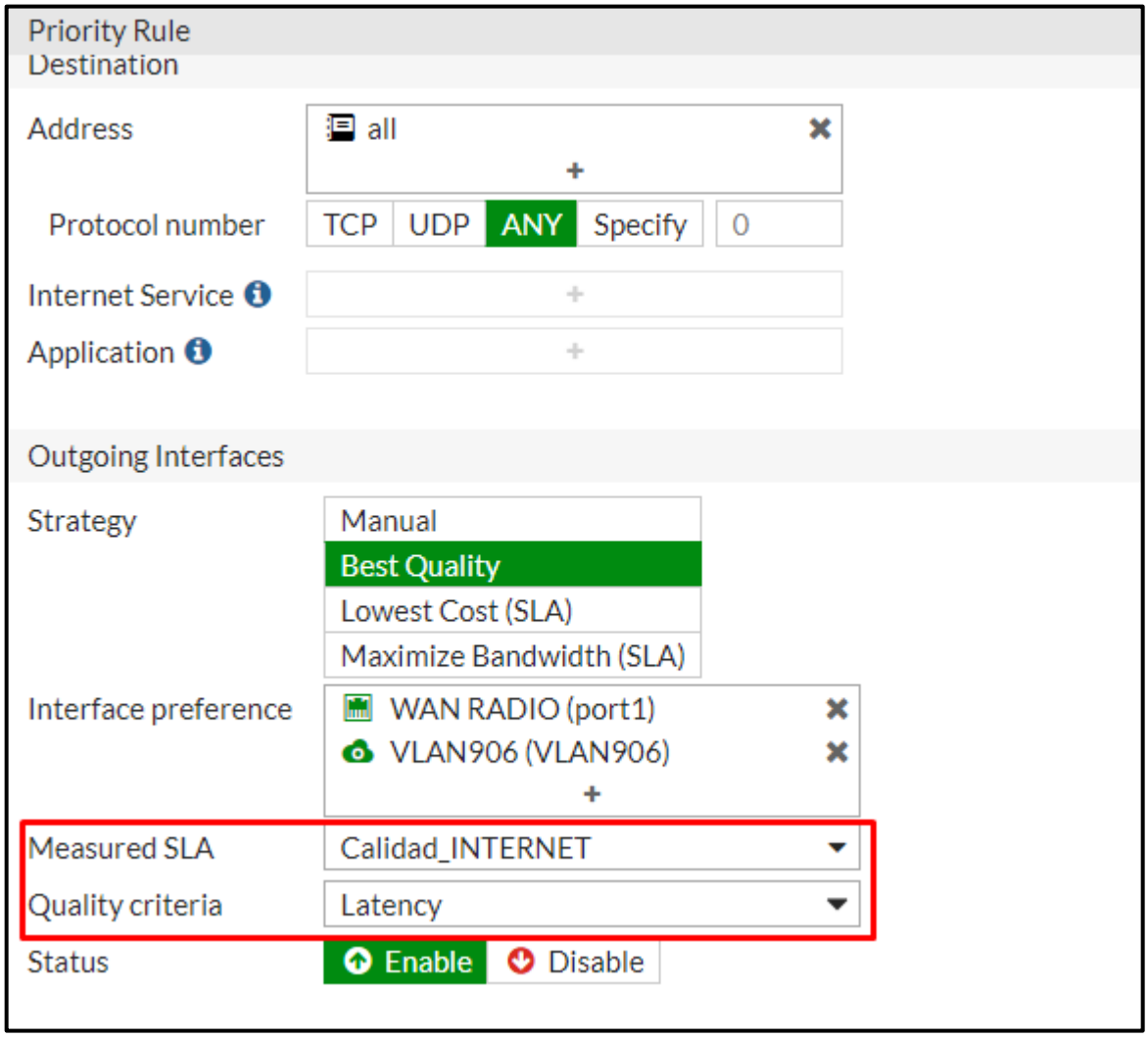


Fuente: Elaboración propia

- **Configuración de la regla SD-WAN en el enrutador Firewall Fortigate**

Añadimos la regla SD-WAN, la cual está basada en el parámetro SLA anteriormente definido y que tiene como criterio de calidad la latencia. En la figura 41 se observa la configuración de la regla SD-WAN.

Figura 41. Configuración de la regla SD-WAN en el FW



Fuente: Elaboración propia

Esta regla tiene la función de elegir el mejor enlace de internet de acuerdo con el parámetro de latencia definido en el SLA. En la figura 42 podemos observar la regla SD-WAN creada.

Figura 42. Regla SD-WAN

ID	Name	Source	Destination	Criteria	Members	Performance SLA	Status
IPv4 1							
1	Calidad_INTERNET	all	all	Latency	WAN RADIO (port1) VLAN906 (VLAN906)	Calidad_INTERNET	Enabled

Fuente: Elaboración propia

Con estas configuraciones se asegura el correcto funcionamiento del Firewall, así mismo se verifica que los usuarios de la red local del cliente cuentan con salida a internet. En la figura 43 se muestra la IP LAN asignada al usuario y en la figura 44 se observa la conectividad a internet.

Figura 43. IP asignada por DHCP al usuario

```
Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6852:3dd7:c89b:37af%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{B38C53AB-C3A4-4F97-9082-8B3DA3AB95D9}:
```

Fuente: Elaboración propia

Figura 44. Conectividad a internet

```
C:\Users\Administrator>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=96ms TTL=125
Reply from 8.8.8.8: bytes=32 time=60ms TTL=125
Reply from 8.8.8.8: bytes=32 time=81ms TTL=125
Reply from 8.8.8.8: bytes=32 time=99ms TTL=125
Reply from 8.8.8.8: bytes=32 time=59ms TTL=125
Reply from 8.8.8.8: bytes=32 time=60ms TTL=125
Reply from 8.8.8.8: bytes=32 time=62ms TTL=125
```

Fuente: Elaboración propia

3.2.3. Implementación de las tecnologías de transmisión

La implementación de las tecnologías de transmisión fue llevada a cabo por el área correspondiente. En la siguiente figura 45 y 46 se muestra los nodos correspondientes para cada enlace tanto de fibra como radio microondas.

Figura 45. Línea de vista para enlace microondas

Fuente: Elaboración propia

Figura 46. Recorrido de la fibra desde el punto del cliente

Fuente: Elaboración propia

3.3. Resultados

Después de realizada la configuración en los equipos que denominamos accesos y Core en el software EVE-NG. Con este emulador, se buscó realizar validaciones preliminares que permitan obtener resultados previos a la implementación real de la red. Ya que, al ser una red emulada en un entorno virtual, este nos permite realizar y/o analizar los resultados como son las pruebas de conectividad a internet, alta disponibilidad de los enlaces y comunicación entre usuarios internos dentro su red LAN. En conclusión, se cumplió con los objetivos propuestos y como evidencia de ello presentamos las acciones respectivas.

Para obtener los resultados preliminares se definió dos usuarios con IPs de su segmento de red LAN. En la tabla 10 se muestra la asignación de las IPs para las pruebas.

Tabla 10. Asignación de IPs para los usuarios LAN

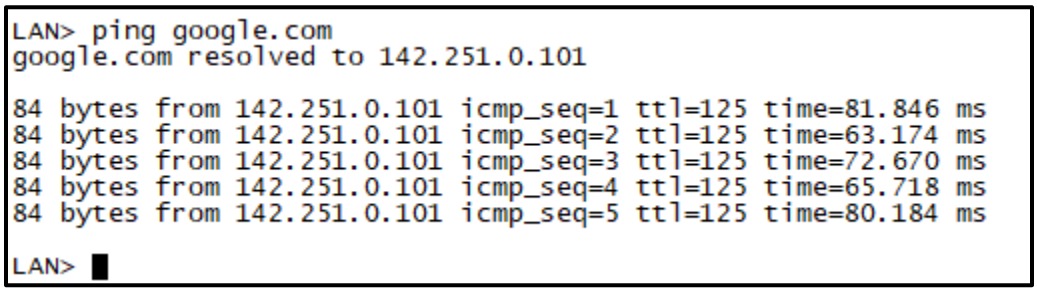
EQUIPO	IP ASIGNADA
LAN	192.168.0.3/24
LAN1	192.168.0.4/24

Fuente: Elaboración propia

3.3.1. Conectividad a internet

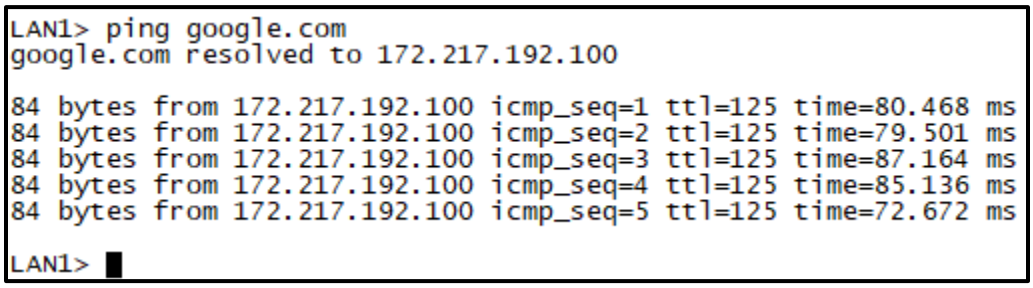
Se dio verificación de salida a internet de los dos usuarios LAN definidos en la tabla anterior. En la figura 47 y 48 se valida la salida a internet de los dos usuarios.

Figura 47. Conectividad a internet del usuario LAN



Fuente: Elaboración propia

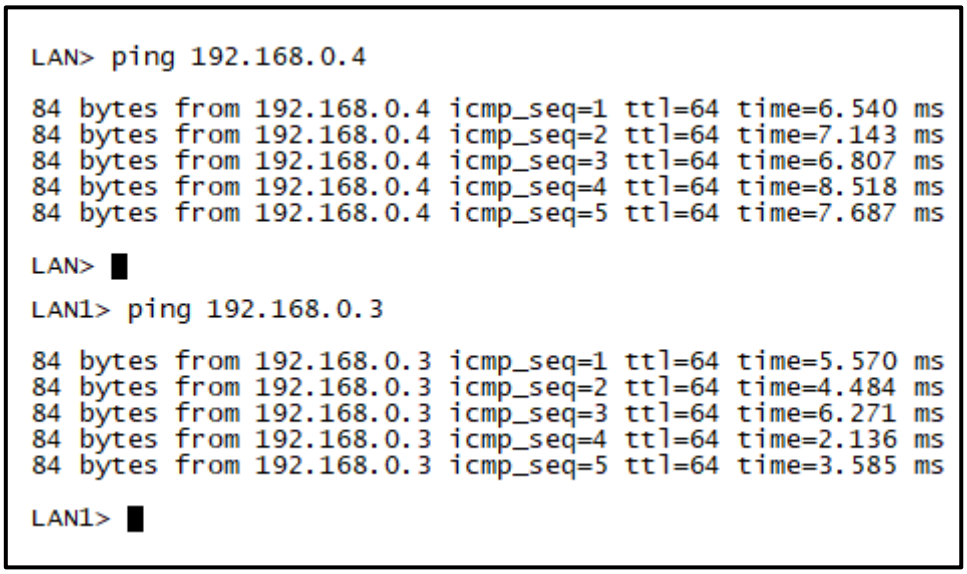
Figura 48. Conectividad a internet del usuario LAN1



Fuente: Elaboración propia

Podemos verificar también que existe comunicación entre sus usuarios, en la siguiente figura 49 se observa la comunicación entre los dos equipos.

Figura 49. Comunicación entre los dos usuarios LAN y LAN1



Fuente: Elaboración propia

Actualmente todo el tráfico de internet de los dos usuarios está siendo dirigido hacia la interfaz de fibra como se puede observar en la figura 50.

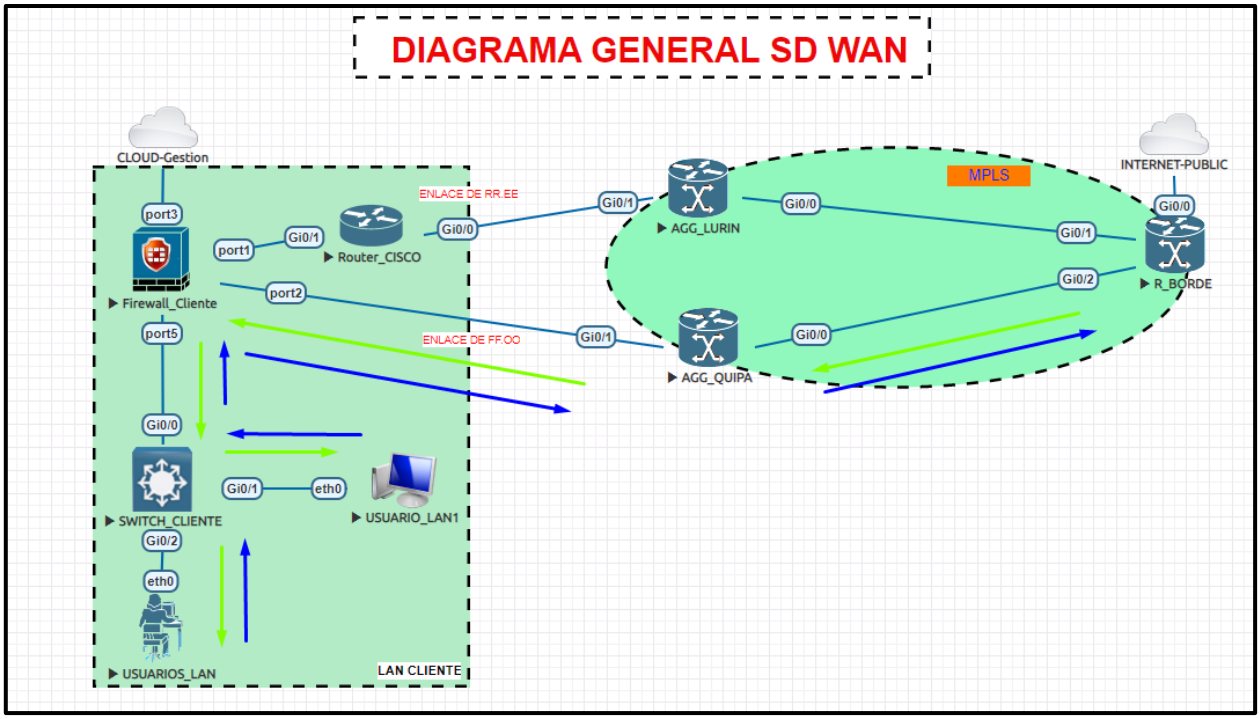
Figura 50. Dirección actual del tráfico de los usuarios

192.168.0.4	VPCS1	8.8.8.8	ICMP/8	168 B	2	VLAN906 (VLAN906)	192.168.20.2
192.168.0.3	VPCS1	8.8.8.8	ICMP/8	168 B	2	VLAN906 (VLAN906)	192.168.20.2

Fuente: Elaboración propia

Esto lo podemos interpretar en la figura 51 siguiente, los paquetes de internet son enviados del usuario LAN hasta el Firewall y estos lo reenvían hasta el equipo Core QUIPA quien a su vez conecta al enrutador BORDE que brinda el acceso a internet.

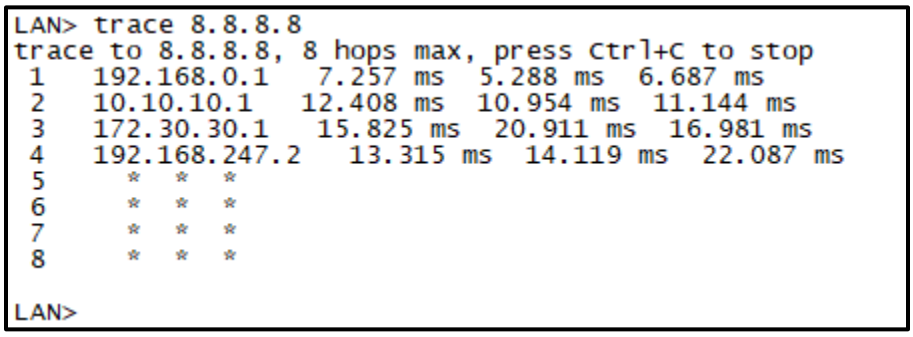
Figura 51. Dirección del tráfico de internet actual



Fuente: Elaboración propia

El tráfico de internet es enviado hacia el Firewall y este elige la mejor ruta para reenviar los paquetes. En la figura 52 se muestra la traza hacia el servidor Google, donde podemos observar que lo envía hacia la puerta de enlace del puerto LAN (192.168.0.1) del Firewall y después en reenviarlo hacia el equipo Core QUIPA (10.10.10.1) para finalmente llegar al equipo de BORDE (192.168.247.2).

Figura 52. Traza hacia a internet del usuario LAN

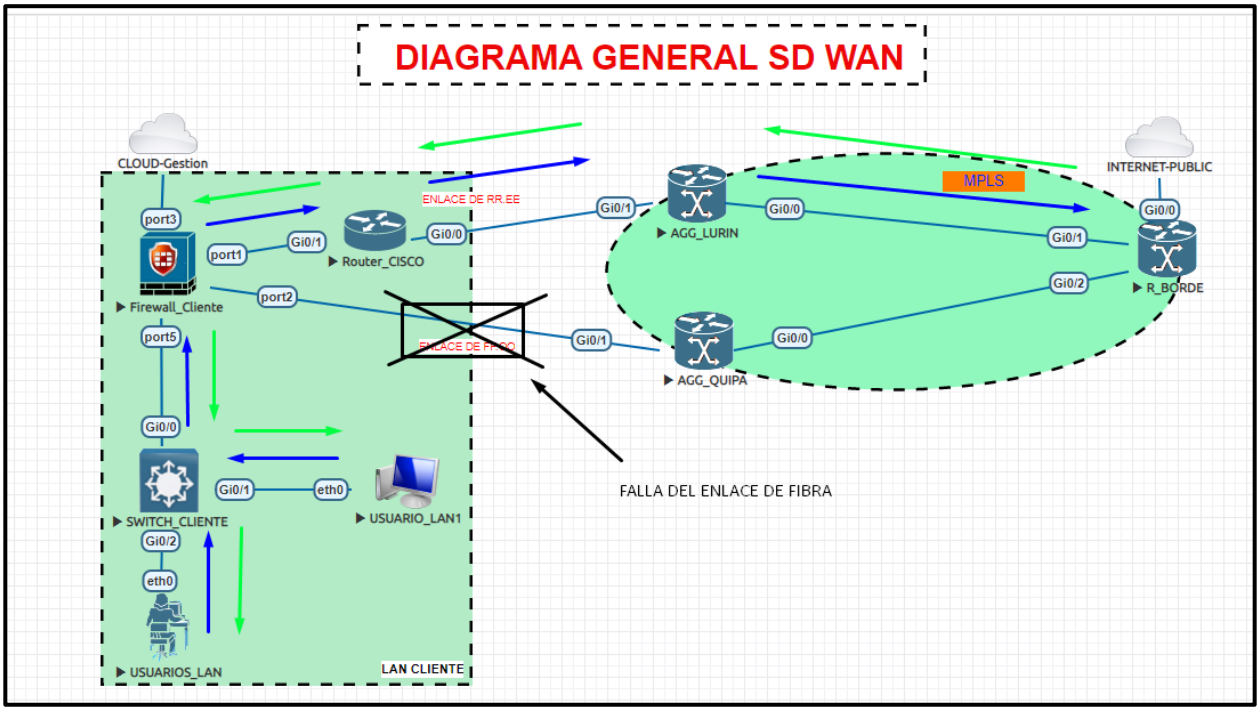


Fuente: Elaboración propia

3.3.2. Alta Disponibilidad de los enlaces

Para las validaciones de alta disponibilidad de los enlaces, tenemos el siguiente escenario donde simularemos en el EVE-NG la caída del enlace fibra y enlace de radio tomará el papel de brindar el acceso a internet a los usuarios. En la siguiente figura 53 se muestra como tomará la ruta los paquetes de internet ante la falla.

Figura 53. Falla del enlace de fibra



Fuente: Elaboración propia

Ante la caída del enlace fibra se validó que el enlace de radio toma el tráfico de internet de todos los usuarios de la red LAN. Y esto lo podremos validar en la traza, donde observamos que el camino para llegar al enrutador de BORDE cambia. En la figura 54 se muestra la traza ante la caída del enlace de fibra.

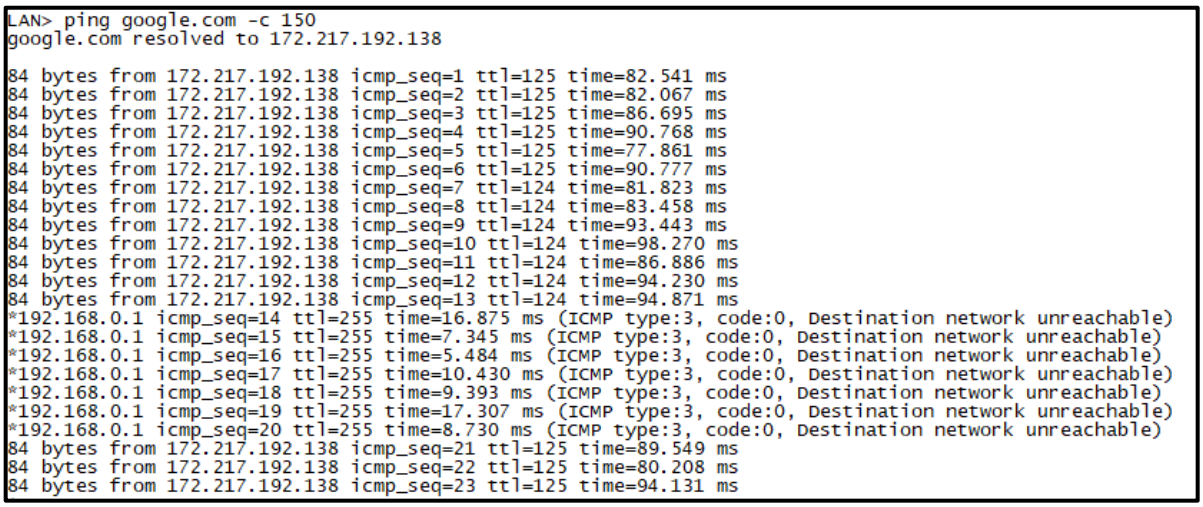
Figura 54. Traza hacia internet ante caída del enlace de fibra

```
LAN> trace google.com
google.com resolved to 172.217.192.101
trace to google.com, 8 hops max, press Ctrl+C to stop
 1   192.168.0.1    7.256 ms   13.933 ms   9.517 ms
 2   192.168.15.1    14.573 ms   12.034 ms   16.406 ms
 3   10.10.20.1    19.951 ms   46.642 ms   15.749 ms
 4   172.30.20.1    24.043 ms   21.718 ms   17.210 ms
 5   192.168.247.2    25.581 ms   25.420 ms   16.140 ms
 6      *   *   *
 7      *   *   *
 8      *   *   *

LAN>
```

Fuente: Elaboración propia

En la figura 55 se muestra la recuperación de acceso a internet ante la conmutación del enlace, se observa una cantidad mínima de paquetes perdidos, es equivalente a unos segundos de indisponibilidad.

Figura 55. Recuperación del servicio de internet en los usuarios de red



Fuente: Elaboración propia

Una vez se repare la falla sobre el enlace de fibra el enlace retorna hacia su tráfico principal, y la recuperación del servicio no afecta la operatividad del servicio. En la figura 56 siguiente observamos las peticiones hacia internet del usuario LAN1.

Figura 56. Peticiones hacia internet del usuario LAN1

Source	Device	Destination	Application	Bytes	Packets	Destination Interface	Source NAT Address
192.168.0.4	VPCS1	8.8.8.8	UDP/29794	8.70 kB	96	VLAN906 (VLAN906)	192.168.20.2
192.168.0.4	VPCS1	8.8.8.8	UDP/4994	3.44 kB	40	WAN RADIO (port1)	192.168.15.2

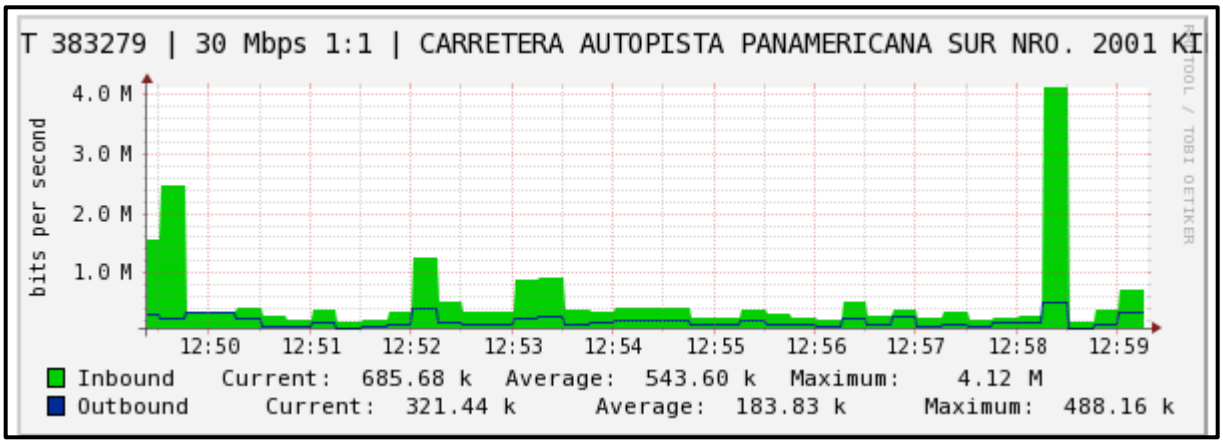
Fuente: Elaboración propia

Después de realizar estas pruebas, tenemos los resultados preliminares obtenidos mediante la simulación de la red propuesta en el software EVE-NG. Con respecto a la validación del tráfico o ancho de banda, el área cuenta con un gestor que contiene las gráficas de consumo de los clientes. En el siguiente apartado se mostró la validez del consumo del ancho de banda real del cliente, así como los resultados reales al implementar la red propuesta.

3.3.3. Validación del ancho de banda

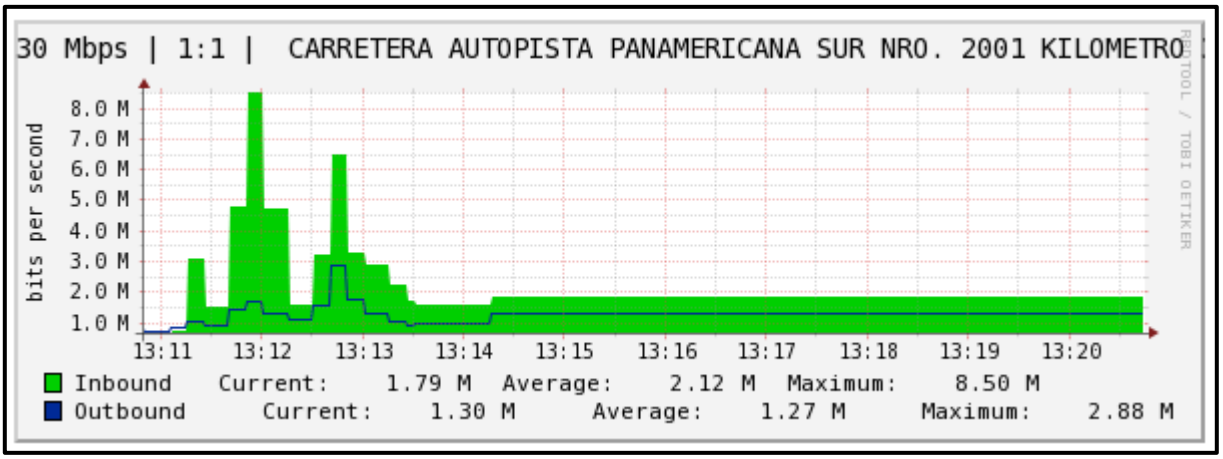
Para la validación del tráfico en tiempo real, se utiliza el NETMONITOR (CACTI) para el monitoreo. En las siguientes figuras 57 y 58 se muestra el tráfico real de internet de los enlaces.

Figura 57. Tráfico en tiempo real del enlace de Radio



Fuente: Elaboración propia

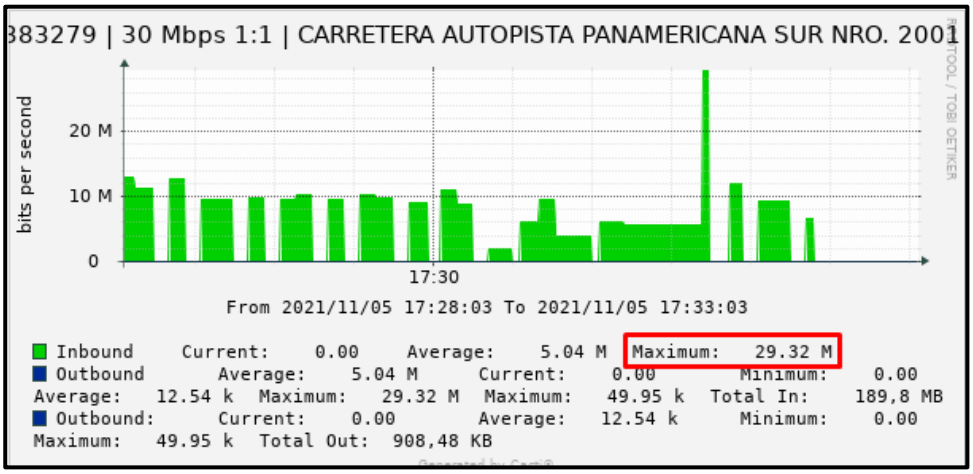
Figura 58. Tráfico en tiempo real del enlace de Fibra



Fuente: Elaboración propia

Se puede verificar que, realizando la saturación del enlace, el ancho de banda contratado por el cliente cumple con los 30 Mbps 1:1. En la figura 59 se muestra un pico de velocidad de 30 Mbps en el NETMONITOR.

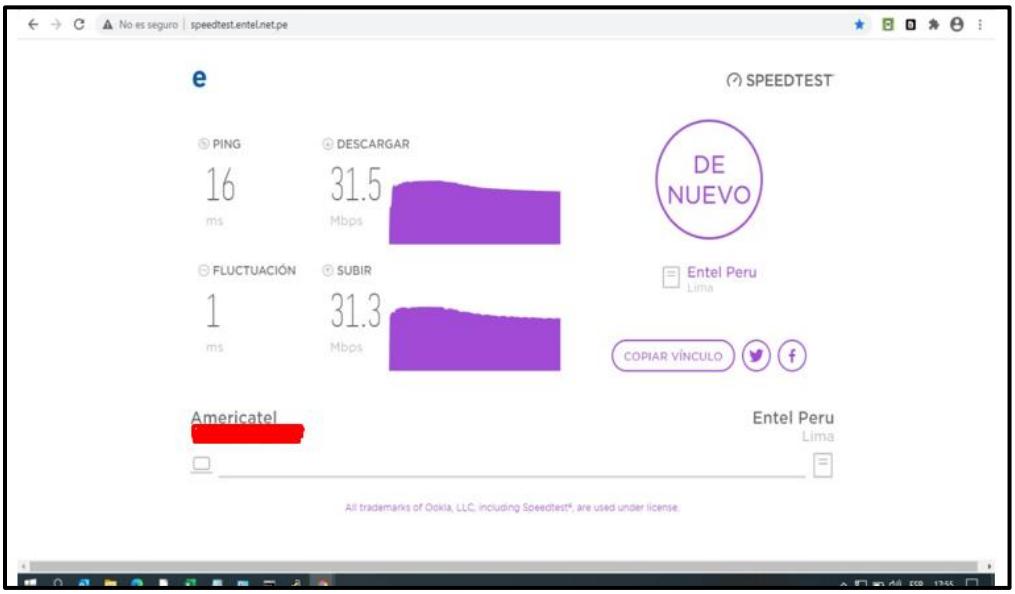
Figura 59. Pico de velocidad en el NETMONITOR



Fuente: Elaboración propia

Como verificación final, se realiza la de medición de velocidad mediante el aplicativo Web “Speedtest” para corroborar que se cumple el ancho de banda contratado. En le figura 60 se muestra los resultados de esta medición.

Figura 60. Medición del Ancho de Banda mediante el SPEEDTEST

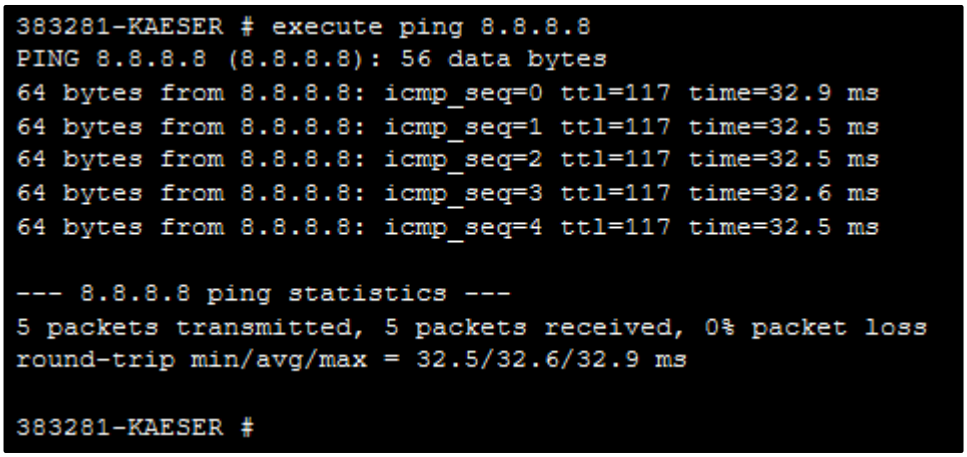


Fuente: Elaboración propia

Así mismo se muestran los resultados de las pruebas realizadas con el servicio una vez ya implementado y en funcionamiento.

En la siguiente figura 61 se observa la conectividad hacia a internet desde el FW, donde podemos validar tiempos de respuesta normales para el enlace.

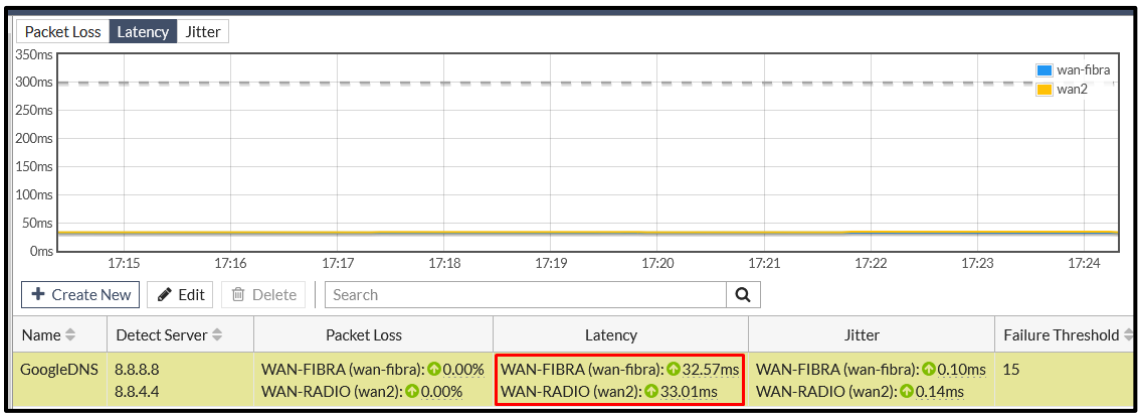
Figura 61. Conectividad hacia a internet desde el FW



Fuente: Elaboración propia

En la siguiente figura 62 se muestra el performance real del SLA de los dos enlaces en funcionamiento.

Figura 62. Performance real del SLA de los dos enlaces



Fuente: Elaboración propia

De cual concluimos que la red propuesta para el cliente empresarial cumple con los objetivos de mantener dos enlaces activos con el fin de cumplir los requerimientos del cliente.

Así mismo la simulación en el software EVE-NG cumple con lo propuesto, ya que teniendo en cuenta las configuraciones aplicadas en el entorno virtual de prueba, esto pudo replicarse en la configuración de los equipos en el cliente.

Además, para la solución del cliente se brindó un equipo de seguridad denominado Firewall Fortigate 100E para garantizar seguridad a su red interna.

Los resultados que se obtuvieron al implementar esta propuesta de red para el cliente fueron analizados mediante una comparación entre las averías ocurridas antes y después de la solución brindada. En la siguiente tabla 11 se muestra que las averías o fallas que presentó en el transcurso desde que se implementó hasta hoy en día.

Tabla 11. Averías presentadas después de la implementación.

N° Remedy	N° Regulado	MES	AÑO	TIPO de TICKET
INC000000465214	A15087800	NOVIEMBRE	2020	Reclamo de Avería
INC000000496709	A15088628	ENERO	2021	Reclamo de Avería
INC000000467411	A15087866	MARZO	2021	Reclamo de Avería

Fuente: Elaboración propia

Como podemos observar existe una clara disminución en las averías presentadas, teniendo en cuenta que anteriormente en el periodo entre las fechas de febrero de 2019 y febrero del 2020 fueron un total 8. En la siguiente tabla 12 se muestra la comparativa del total de averías entre los dos periodos.

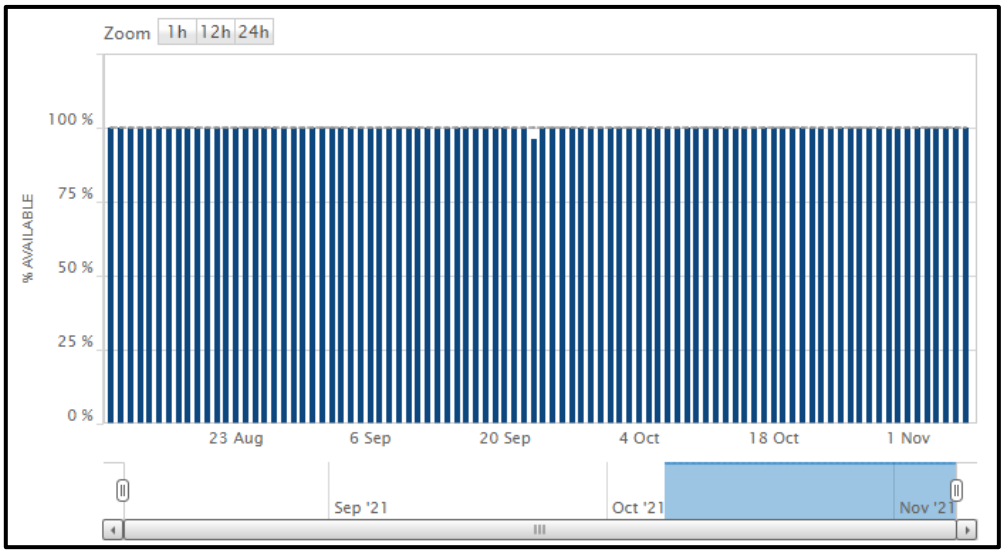
Tabla 12. Comparativo entre el total de averías.

Período	N° Total de Averías
Febrero 2019 - Febrero 2020	8
Octubre 2020 - Octubre 2021	3

Fuente: Elaboración propia

Así mismo podemos validar que el porcentaje de disponibilidad de los enlaces en los últimos 7 meses ha estado siempre en el orden mayor a 99%. En la siguiente figura 63 se muestra el porcentaje de disponibilidad de los enlaces en los últimos 4 meses.

Figura 63. Porcentaje de disponibilidad de los enlaces.



Fuente: Elaboración propia

CONCLUSIONES

- Se logró determinar la propuesta de implementación de una red para el cliente empresarial en el software EVE-NG utilizando la tecnología SD-WAN como solución con el fin de cumplir los requerimientos actuales del cliente y obtener la mejora solicitada, esto quiere decir que la conectividad hacia a internet será más fluida.

- Se verificó que las tecnologías de comunicación tradicionales, como lo es la MPLS a nivel de usuario cliente, presenta desventajas que hacen que la tecnología SD-WAN sea ofrecida como solución para las medianas y grandes empresas, esto es por el coste reducido en la implementación y por la flexibilidad de cómo opera SD-WAN.

- Se brindó un equipo de acceso para garantizar la seguridad perimetral de la red del cliente mediante un equipo Firewall Fortigate, como parte de la solución brindada al cliente.

- Se validó la conectividad hacia a internet desde la red LAN cliente, así como también las pruebas de comunicación entre los usuarios LAN, siendo estas exitosas y validando que la política de enrutamiento configurada en el Firewall funciona correctamente.

- Se validó mediante la simulación en el EVE-NG que las pruebas de alta disponibilidad resultaron favorables, esto quiere decir que cuando el enlace de fibra óptica quede inoperativo, el enlace de radio microondas actuará como respaldo y asumirá todo el tráfico de salida a internet de los usuarios, el tiempo de recuperación de servicio ante la caída tiene como promedio de 10 segundos.

- Se validó mediante la herramienta de monitoreo que el servicio de internet cumple con el ancho de banda contratado por el cliente.

RECOMENDACIONES

- Se recomienda distribuir de manera equitativa las cargas de tráfico de su navegación a internet a través de sus dos enlaces, esto con el fin de aprovechar de una manera mejor sus dos enlaces de internet.

- Se recomienda establecer políticas de enrutamiento y aplicar filtros de navegación en la configuración de su Firewall para evitar que los usuarios accedan a páginas maliciosas.

- Se recomienda que, para los aplicativos de mayor uso por parte de los usuarios, se aplique la configuración de Traffic Shaper en el Firewall, esto quiere decir que los aplicativos que consumen un mayor ancho de banda sean limitados con cierta cantidad de ancho de banda.

- Para evitar las fallas (bugs) de software propias del Firewall, se recomienda tener actualizado el firmware del Firewall a la versión más reciente.

- Para que los equipos de acceso no sufran daños por cortes de luz inesperados, se recomienda utilizar un UPS como respaldo de energía y protección de los equipos.

- Se recomienda solicitar un mantenimiento periódico de sus equipamientos y conexiones como medida preventiva.

BIBLIOGRAFÍA

Luis A. Delgado A. (2019). *Implementación de una solución de alta disponibilidad SD-WAN para la construcción de redes híbridas y sustitución de la tecnología MPLS*. [Trabajo de postgrado, Universidad Nacional Autónoma de México]. México. http://132.248.52.100:8080/xmlui/bitstream/handle/132.248.52.100/17016/Informe.pdf.pdf?sequence=1&isAllowed=y

Luis E. Aguilar R. (2020). *Propuesta de Diseño de una Red Privada de Telecomunicaciones para Accesos a Aplicaciones de una Entidad Bancaria a través de Internet*. [Tesis, Universidad Tecnológica del Perú]. Perú. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3495/Luis%20Aguilar_Tesis_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y

Gustavo A. Velasquez R. (2017). *Diseño e Implementación de un servicio de seguridad administrada e interconexión de datos utilizando tecnología MPLS para el Instituto del Mar del Peru*. [Trabajo de postgrado, Universidad Nacional Tecnológica de Lima Sur]. Perú. http://repositorio.untels.edu.pe/jspui/bitstream/123456789/589/1/T088A_43009408_T.pdf

Luis A. Marin S. (2021). *Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos*. [Trabajo de postgrado, Universidad Católica de Santiago de Guayaquil]. Ecuador. http://201.159.223.180/bitstream/3317/16888/1/T-UCSG-POS-MTEL-200.pdf

Douglas O. Ayapata M. (2020). *Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo*. [Trabajo de postgrado, Universidad Católica de Santiago de Guayaquil]. Ecuador. http://repositorio.ucsg.edu.ec/bitstream/3317/14271/1/T-UCSG-PRE-TEC-ITEL-362.pdf

WMware (s.f.). *¿Qué son las redes empresariales?* Obtenido de https://www.vmware.com/es/topics/glossary/content/enterprise-networking.html

Bob Vachon and Rick Graziani (2008). *Accessing the WAN. Cisco Press.* Obtenido de https://ptgmedia.pearsoncmg.com/images/9781587132056/samplepages/1587132052.pdf

Jim Metzler, Ashton Metzler, and Associates (2015). *Guide to WAN Architecture Design.* Obtenido de http://www.webtorials.com/main/resource/papers/webtorials/2015-Guide-Wan-Architecture/2015_Guide_to_WAN_Architecture_and_Design.pdf

Andy Gottlieb (2012). *¿Why does MPLS cost so much more than Internet connectivity?* Obtenido de https://www.networkworld.com/article/2222196/why-does-mpls-cost-so-much-more-than-internet-connectivity.html

Kreutz, D., F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky et S. Uhlig (2015). *Software-Defined Networking: A Comprehensive Survey.* Proceedings of the IEEE, vol. 103, no 1, p. 14-76.

Cheng Sheng, Jie Bai, Qi Sun (2021). *Software-Defined Wide Area Network Architectures and Technologies.*

Sandra Gittlen (2021). *SD-WAN explained: Ultimate guide to SD-WAN architecture.* Obtenido de https://www.techtarget.com/searchnetworking/SD-WAN-explained-The-ultimate-guide-to-SD-WAN-architecture

Nunes, B. A. A., M. Mendonca, X. N. Nguyen, K. Obraczka et T. Turletti (2014). *A Survey of Software-Defined Networking: Past, Present, and Future of Programmable*

Networks.
IEEE Communications Surveys & Tutorials, vol. 16, no 3, p. 1617-1634.

Fortinet (s.f.). *What Is a Network Firewall?* Obtenido de https://www.fortinet.com/resources/cyberglossary/firewall

Palo Alto Networks (s.f.). *What is Quality of Service?* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos

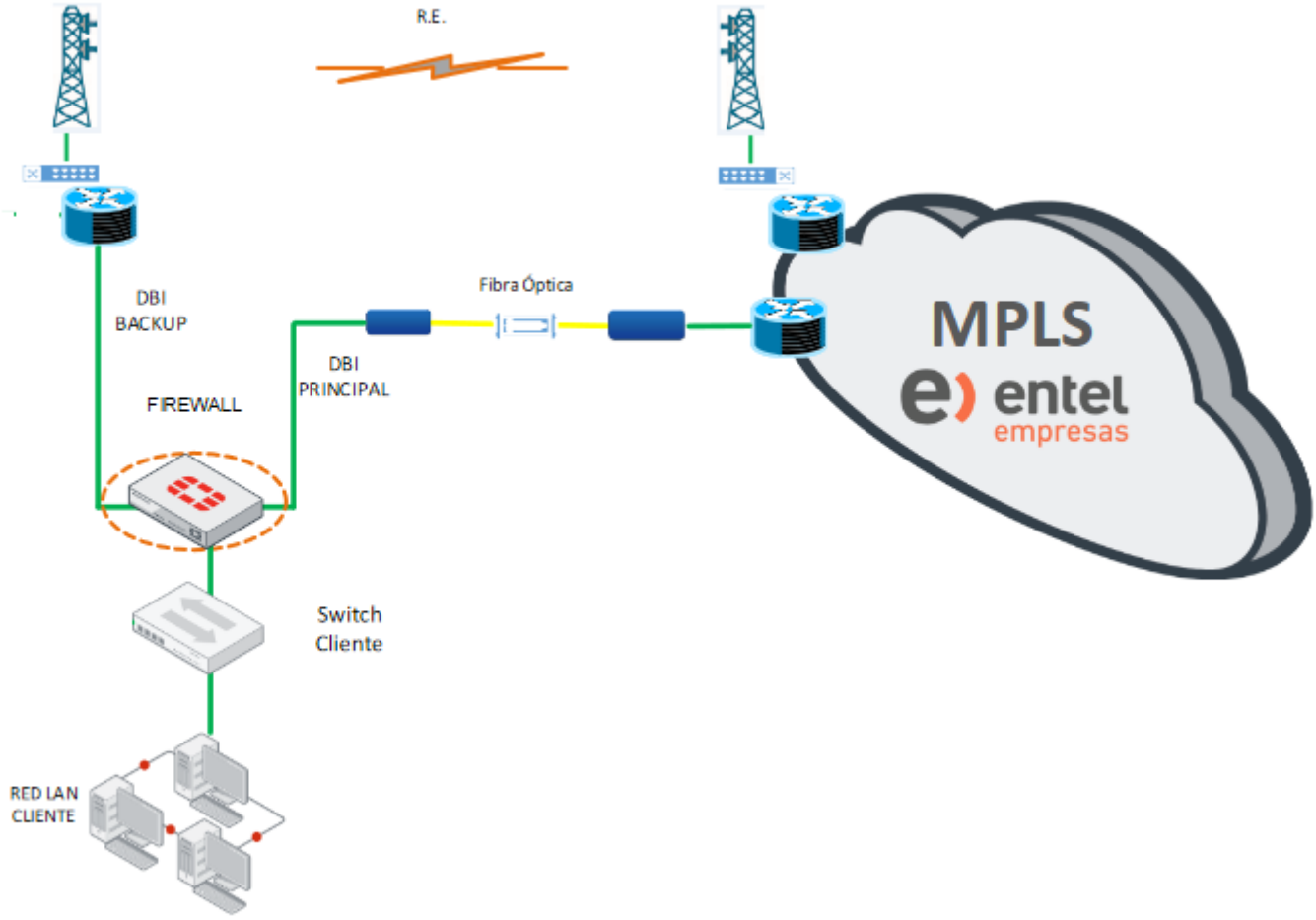
GNS3 (s.f.). *Getting Started with GNS3* Obtenido de https://docs.gns3.com/docs/

EVE-NG (s.f.). *EVE-NG Professional Cookbook* Obtenido de https://www.eve-ng.net/images/EVE-COOK-BOOK-1.0.pdf

Rajendran, A. (2016). *Security Analysis of a Software Defined Wide Area Network Solution.* [Tesis, Aalto University]

ANEXOS

Diagrama general de la solución de una red de cliente empresarial basada en SD-WAN.



Solicitud de análisis de factibilidad (SAF) para la migración hacía la tecnología SD-WAN.

Enlace Principal:

SOLICITUD DE ANALISIS DE FACTIBILIDAD (SAF 236136) GRANDES Privado Vel. Simétrica Americatel

Detalles

Servicio	Medio Provisional	Tecn. de Tx	Red	Fecha Apertura	Fecha Activación	Fecha Actualización	Fecha Cierre	Consideraciones
Internet dedicado	**Planta Externa**	**FO PP**	Entel Perú	2020-08-15 15:48:02	2020-08-15 15:48:12	2020-08-18 08:37:24	2020-08-17 18:18:48	**PSI-1980 Cliente mudará sus servicios activos por RE de DBI y SipTrunk (Upgrade de 25 a 30Mb del DBI //mantener las mismas configuraciones actuales del servicio y la misma numeracion) Asi mismo; instalará un servicio DBI nuevo por FO con FW E100 en SD WAN**

Datos del Cliente

Segmento	Razón Social	RUC	Tipo Cliente	Contacto	Teléfono	Sucursal	Centro Poblado
GRANDES Privado	KAESER COMPRESORES DE PERU S.R.L.	20538349730	Americatel	BENAVIDES TORRES, EDUARDO ARMANDO	3727700	CARRETERA AUTOPISTA PANAMERICANA SUR NRO. 2001 KILOMETRO 38 (PUNTA HERMOSA - LIMA - LIMA) (REF: ALMACENES BSF) **CARRETERA** AUTOPISTA PANAMERICANA SUR **NRO.** 2001 **KILOMETRO** 38	PUNTA HERMOSA

Detalle del Producto Solicitado Internet Dedicado

Velocidad de Bajada: 30 Mbps **Velocidad Simétrica**	**CIR de Bajada:** 1:1
Velocidad de Subida: 30 Mbps	**CIR de Subida:** 1:1
Número de IPs Solicitadas: 8	**Requiere VPN?:** NO
Requiere Firewall?: Si	**Tipo Firewall:** Físico
	Se debe adjuntar formato de configuración para ISP.
Tipo de Instalación: Nuevo Servicio	
OIT de Instalación: No especifica	
Solicitud de Visita Obligatoria: NO	**Alquiler de Equipo de Conectividad:** No

Enlace Contingencia:

SOLICITUD DE ANALISIS DE FACTIBILIDAD (SAF 236134) GRANDES Privado Vel. Simétrica Americatel

Detalles

Servicio	Medio Provisional	Red	Fecha Apertura	Fecha Activación	Fecha Actualización	Fecha Cierre	Consideraciones
Internet dedicado	**Radio Enlace**	Entel Perú	2020-08-15 15:44:26	2020-08-15 15:48:12	2020-08-18 08:37:23	2020-08-17 18:18:37	**PSI-1980 Cliente mudará sus servicios activos por RE de DBI y SipTrunk (Upgrade de 25 a 30Mb del DBI //mantener las mismas configuraciones actuales del servicio y la misma numeracion) Asi mismo; instalará un servicio DBI nuevo por FO,**

Datos del Cliente

Segmento	Razón Social	RUC	Tipo Cliente	Contacto	Teléfono	Sucursal	Centro Poblado
GRANDES Privado	KAESER COMPRESORES DE PERU S.R.L.	20538349730	Americatel			CARRETERA AUTOPISTA PANAMERICANA SUR NRO. 2001 KILOMETRO 38 (PUNTA HERMOSA - LIMA - LIMA) (REF: ALMACENES BSF) **CARRETERA** AUTOPISTA PANAMERICANA SUR **NRO.** 2001 **KILOMETRO** 38	PUNTA HERMOSA

Detalle del Producto Solicitado Internet Dedicado

Velocidad de Bajada: 30 Mbps **Velocidad Simétrica**	**CIR de Bajada:** 1:1
Velocidad de Subida: 30 Mbps	**CIR de Subida:** 1:1
Número de IPs Solicitadas: 8	**Requiere VPN?:** NO
Requiere Firewall?: No especifica	
Tipo de Instalación: Mudanza Local	
OIT de Instalación: 330119	
Solicitud de Visita Obligatoria: NO	**Alquiler de Equipo de Conectividad:** No

Acta de entrega de servicio y conformidad del cliente.

GERENCIA DE OPERACIONES DIGITALES
JEFATURA DE ATENCION TECNICA EN TERRENO
AREA DE INSTALACIONES

ACTA DE CONFORMIDAD DE SERVICIO — 119 Nº 0000001

CLIENTE:	KAESER COMPRESORES DE PERU SRL	Nº OIT / SE: S383280	
DIRECCION:	PANAMERICANA SUR N°2001 KM38 – PUNTA HERMOSA	Nº CID:	
Contacto:	JHONATAN ORTIZ	Teléfono Fijo / Celular: 943944048	

1. Conformidad por: INSTALACIÓN [ ] ENTREGA DE SERVICIO [X] OTRO [ ]

MEDIO: PLANTA EXTERNA [ ] RADIOENLACE: [X] WIMAX [ ]

2. Equipos y accesorios instalados — GUIA REMISION Nº

Equipo	Marca	Código Americatel	Ubicación

3. Servicio de Líneas NGN

4. Configuración IP LAN

5. Servicio se entrega funcionando correctamente: SI, servicio funciona correctamente

6. Observaciones y/o recomendaciones:

Se configuró el servicios y se realizaron las pruebas de telefonía satisfactorias.

7. Condiciones del local del cliente

8. Recomendaciones al cliente

POR AMERICATEL PERU		POR CLIENTE	
Nombre: HALLIER MOZOMBITE		Nombre:	Michel Montes Rivera
DNI: 36211909		DNI:	43134422
Fecha y Hora (entrega de servicio): 30/ 09 /2020 - 12:12		Cargo:	T.S.
Firma:		Firma:	

Americatel Perú - Centro de Atención al Cliente Telf. 0800-77-500

Acta de instalación de los equipos y validación del servicio.

INFORMACIÓN GENERAL INSTALACIONES PLANTA EXTERNA

N° OIT / SE	$383281	Fecha Trabajo	17/09/2020	Supervisor Americatel	
EMPRESA CONTRATISTA	SERTELEC	Instalador	Richard Gómez	Supervisor Contratista	NATHALY CRISTOBAL

Empresa (Razon Social):	KAESER COMPRESORES DE PERU S.R.L.			
Dirección:	Carretera Autopista Panamericana Sur Nro. 2001	INFORMACION GEOGRAFICA / ALTURA		
Contacto:	Michel Mantor	Coord Geo WGS84 / UTM	LATITUD	LONGITUD
Teléfono / email			-12.2636690	-76.8960950
Servicio contratado	INTERNET DEDICADO	MODO		

DURACION DE INSTALACION	FECHA	HORA
INICIO	17/09/2020	9:30 AM
FIN	17/09/2020	5:20 PM

OBSERVACIONES Y DETALLES DE LA INSTALACION:

SE REALIZA INSTALACION Y CONFIGURACION DE EQUIPO FORTIGATE 100E, SE VALIDA CON EL NOC CARLOS REA LA CONFIGURACIÓN Y SE REALIZA A LAS PRUEBAS DE NAVEGACION Y SATURACION LLEGANDO A LA VELOCIDAD CONTRATADA(UL=30,DL=30).

	N° de Guia Remision	012 - 0029559			
EQUIPOS INSTALADOS LADO CLIENTE					
Equipo	Marca				
Conversor: 1G SFP RF45 MC		Serie :		Codigo :	
Router		Serie :		Codigo :	
SPF	HUAWEI	Serie :	MA1922043#2149	Codigo :	
FUENTE 12v		Serie :		Codigo :	
Switch Cisco		Serie :		Codigo :	
Fortinet 100E		Serie :	FG100ETK1#030093	Codigo :	340205
Modulo 100fx		Serie :		Codigo :	
Telefono Itelecon		Serie :		Codigo :	
router gaoke 2 puertos		Serie :		Codigo :	
Telefono Itelecon		Serie :		Codigo :	
Telefono Itelecon		Serie :		Codigo :	
Fuente 12v		Serie :		Codigo :	
Router ISR 4331		Serie :		Codigo :	
Modulo		Serie :		Codigo :	
Router:		Serie :		Codigo :	

Equipos de acceso instalados en la sede del cliente.