NOMBRE DEL TRABAJO
T088A_70030277_T.pdf

AUTOR
mamani

RECUENTO DE PALABRAS
10353 Words

RECUENTO DE CARACTERES
60770 Characters

RECUENTO DE PÁGINAS
76 Pages

TAMAÑO DEL ARCHIVO
4.8MB

FECHA DE ENTREGA
Aug 29, 2023 3:12 PM GMT-5

FECHA DEL INFORME
Aug 29, 2023 3:12 PM GMT-5

14% de similitud general

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

- 14% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Base de datos de trabajos entregados
- Material bibliográfico
- Material citado
- Material citado

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: MAMANI DIAZ CANDY MARIELA
D.N.I.: 70030277
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 954386249
e-mail: CMMAMANID@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: "IMPLEMENTACIÓN DE SD-WAN Y TÚNEL VPN IPSEC PARA REDUNDACIA DE COMUNICACIONES HACIA SERVICIOS INTERNOS Y EXTERNOS EN AGENCIA ACCHA DE UNA ENTIDAD FINANCIERA"
Fecha de Sustentación: 15/12/2021
Calificación: APROBADO CON DISTINCIÓN
Año de Publicación: 2023

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 N° 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:

MAMANI DIAZ CANDY MARIELA

APELLIDOS Y NOMBRES

70030277

DNI

Firma y huella:

Lima, 20 de julio del 2023

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“IMPLEMENTACIÓN DE SD-WAN Y TÚNEL VPN IPSEC PARA REDUNDANCIA DE COMUNICACIONES HACIA SERVICIOS INTERNOS Y EXTERNOS EN AGENCIA ACCHA DE UNA ENTIDAD FINANCIERA”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

MAMANI DIAZ, CANDY MARIELA

ORCID: 0009-0001-1277-6012

ASESOR

CRUZ YUPANQUI, GLADYS MARCIONILA

ORCID: 0000-0002-2810-1968

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 **11:00 horas** del día miércoles **15 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/ada-ippr-euj), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. RUBIÑOS JIMENEZ, Santiago Linder	CIP N° **112655**
Secretario	: MSc. CUZCANO RIVAS, Abilio Bernardino	CIP N° **129009**
Vocal	: MG. GRADOS ESPINOZA, Herbert Junior	CIP N° **190674**

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: **MAMANI DIAZ, CANDY MARIELA**

Sustentó su Trabajo de Suficiencia Profesional: **"IMPLEMENTACIÓN DE SD-WAN Y TÚNEL VPN IPSEC PARA REDUNDANCIA DE COMUNICACIONES HACIA SERVICIOS INTERNOS Y EXTERNOS EN AGENCIA ACCHA DE UNA ENTIDAD FINANCIERA"**

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

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

Siendo las **11:45 horas** del día miércoles 15 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. Santiago Linder Rubiños Jiménez
CIP N°112655
PRESIDENTE

MSc. Abilio B. Cuzcano Rivas
CIP N°129009
SECRETARIO

Mg. Herbert J. Grados Espinoza
CIP N°190674
VOCAL

PARTICIPANTE
Bachiller: CANDY MARIELA MAMANI DIAZ

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 **11:00 horas** del día miércoles **15 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/ada-ippr-euj), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. RUBIÑOS JIMENEZ, Santiago Linder	CIP N° **112655**
Secretario	: MSc. CUZCANO RIVAS, Abilio Bernardino	CIP N° **129009**
Vocal	: MG. GRADOS ESPINOZA, Herbert Junior	CIP N° **190674**

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): **MAMANI DIAZ, CANDY MARIELA**

Nota de sustentación del Trabajo de Suficiencia Profesional	Condición	Equivalente
18	APROBADO CON DISTINCIÓN	MUY BUENO

Dr. Santiago Linder Rubiños Jiménez
CIP N°112655
PRESIDENTE

MSc. Abilio B. Cuzcano Rivas
CIP N°129009
SECRETARIO

Mg. Herbert J. Grados Espinoza
CIP N°190674
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

Dedico este trabajo a mi madre Bonifacia Diaz, por siempre confiar en mí y seguir apoyándome para crecer profesionalmente, a mis hermanos Deyvis, Rafael y Lily, por siempre enseñarme y ser un modelo para mí, a mis tíos Marcial, Lucio, Marcelina, Faustina, Demetrio, Rolando e Isabel, por brindarme el calor paterno que no tuve.

AGRADECIMIENTO

Agradecimiento a toda la plana docente de la UNTELS, por los conocimientos brindados a lo largo de mi formación, caben destacar al M.Sc. Campos Aguado, M.Sc. Machuca Mines, Ing. Mendoza Panduro y Mg. Oporto Díaz, los cuales me brindaron sólidos conocimientos para poder seguir desarrollándome en el área de telecomunicaciones, así como también ser un modelo de referencia a seguir, debido a las actitudes profesional mostradas durante la impartición de sus clases.

Agradecimiento especial a mi asesora Mg. Cruz Yupanqui, por el apoyo para desarrollar el presente trabajo, así como por brindarme las pautas necesarias y motivarme a seguir adelante.

Agradecimiento a John Marín un experto en seguridad perimetral por sus enseñanzas y el apoyo brindado a mi persona, en mis inicios en el área de seguridad de redes.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El presente proyecto consistió en implementar una solución para poder agregar redundancia de comunicación, hacia servicios internos y externos desde la Agencia Accha, hacia los Site principal y secundario, con una propuesta aplicando SD-WAN para conseguir automatización basada en criterios de calidad de enlaces y de esta forma poder utilizar un internet convencional para la conectividad entre sede, debido a que, en zonas rurales, es menos costoso adquirir un servicio de internet de un ISP local que un servicio de VPN mediante la red MPLS de un proveedor.

Otra problemática que también se abordó, es la necesidad de poder utilizar algún mecanismo para la encriptación de los datos, que son transportados entre sucursales de una empresa. Los túneles VPN IPsec, permiten utilizar mecanismo de encriptación, con la finalidad de mitigar el impacto en caso alguien quiera interceptar la comunicación.

Se empleo como base las funcionalidades del equipamiento Fortigate de Fortinet, tomando en cuenta la compatibilidad con otras marcas dentro de la infraestructura del Cliente. NG-FW Fortigate permite poder utilizar las características de SD-WAN, VPN IPsec, filtrado de contenido mediante UTM y IPS.

INTRODUCCIÓN

En la actualidad las empresas del sector financiero son con frecuencia objetivos de diversos ataques cibernéticos, debido a que realizan el tratamiento de datos sensibles en sus operaciones, estos son principalmente datos de carácter identificativo, datos de carácter personal, datos de carácter económico, datos de carácter social; lo que conlleva a que la empresa encargada del procesamiento de esta información deba implementar diferentes capas de seguridad dentro de su infraestructura de red.

Otro factor importante para considerar dentro del rubro del sector financiero, son los tiempos de disponibilidad de los servicios, debido a que los datos que se manejan deben ser procesados en tiempo real, por lo que es importante utilizar diferentes mecanismos que brinden redundancia en sus enlaces WAN, para de esta forma mitigar la indisponibilidad de alguna incidencia en la red de sus proveedores ISP.

La solución SD-WAN de fortinet busca suplir tanto la necesidad de gestionar los enlaces WAN independientemente de los proveedores ISP, dando un mayor control a la empresa y proporcionando alta disponibilidad; adicionalmente a esto busca dotar la infraestructura de red de todas las características de seguridad que sus soluciones presentan.

El presente proyecto tuvo como principal objetivo implementar la solución SD-WAN en la Agencia Accha, para tener alta disponibilidad, es decir redundancia en la comunicación de servicios internos y externos de la empresa Financiera Credinka, basándose en la automatización de la elección de los enlaces según el performance, además para mejorar la transferencia de datos de forma segura hacia la sede central, se utilizaron túneles IPsec dial-up para poder cifrar la comunicación desde la agencia Accha hasta la sede central, los cuales se levantaron sobre los enlaces MPLS de los proveedores ISP y sobre el enlace de internet propio de la agencia, del mismo modo se configuraron perfiles UTM para navegación segura según los perfiles asignados a cada empleado, tomando en cuenta las actividades que realizan.

Para implementar la solución se desarrolló una prueba de concepto utilizando el software GNS3, para validar el correcto funcionamiento y reducir el tiempo de inactividad del servicio. Se realizó además el análisis de las especificaciones del equipamiento tanto a nivel de hardware y software, para validar que pueda soportar las características de la solución planteada, empleando la documentación de la librería de FORTINET.

Se detalla el desarrollo de los capítulos:

- En el primer capítulo se realizó una breve descripción del contexto de la empresa, se definió la delimitación del proyecto y se formularon los objetivos del presente trabajo.

- En el segundo capítulo se describió las investigaciones nacionales e internacionales empleadas como bases para el presente trabajo, también se desarrolló las bases teóricas de la investigación en la cual se definieron los conceptos necesarios para entender el funcionamiento del SD-WAN, así como también el empleo del cifrado de la comunicación mediante túneles IPSec.

- En el tercer capítulo se describe el análisis del problema, el modelo de solución propuesto, la documentación empleada para la implementación del proyecto y finalmente se muestran los resultados obtenidos.

CAPÍTULO I: ASPECTOS GENERALES

1.1 Contexto

La implementación se realizó para la empresa Financiera Credinka S.A. la cual es una entidad financiera, que tiene como visión ser una de las principales instituciones financieras líder en microfinanzas en el Perú, basándose en tres pilares fundamentales, la confianza, innovación y el trabajo en equipo.

Credinka inició sus actividades el 12 de febrero de 1994, buscando suplir la necesidad de brindar productos y servicios financieros, accesibles y confiables, centrándose en el mercado del sector rural, con la finalidad de contribuir con el desarrollo de la economía regional y nacional. Credinka tuvo una expansión en agosto del 2015, iniciando las operaciones formalmente como Financiera Credinka y siendo reconocida a nivel nacional como una de las financieras más importantes del sistema peruano.

En la actualidad la empresa Financiera Credinka posee una infraestructura de red que utiliza servicios tanto internos para comunicaciones entre los propios servidores de la empresa, recursos compartidos, así como comunicación con servicios externos alojados en la nube.

El rubro de la empresa es del sector bancario, por los que los tiempos de inactividad del servicio tienen un gran impacto en las operaciones que se realizan en el manejo de los datos en tiempo real, lo que también puede conllevar en un bajo nivel de satisfacción por parte de los clientes de la empresa Financiera Credinka.

Los servicios brindados por las empresas del sector financiero están dentro de las actividades esenciales de cada país, por lo que necesitan mantener sus infraestructuras de red con alta disponibilidad y seguridad, para poder efectuar todas sus operaciones internas y externas.

1.2 Delimitación del proyecto

1.2.1 Temporal

El proyecto tuvo una duración de 6 meses, iniciando en febrero de 2021 hasta agosto de 2021.

1.2.2 Espacial

La implementación del proyecto se realizó de forma remota en la Agencia Accha, ubicada en Barrio Urinsaya Calle Garcilazo S/N, distrito de Accha, provincia de Paruro, departamento de Cusco.

1.3 Objetivos

1.3.1 Objetivo General

Implementar la solución SD-WAN y túneles IPsec utilizando equipos fortigate para redundancia basada en criterios de calidad de los enlaces y cifrado de las comunicaciones de la Agencia Accha.

1.3.2 Objetivo Específico

- Implementar la solución SD-WAN en la Agencia Accha para automatizar la elección de enlaces por criterios de calidad y balanceo de carga.
- Implementar túneles IPsec dial-up para cifrar los datos transportados hacia la sede principal y alterna desde la Agencia Accha.
- Implementar políticas de navegación utilizando perfiles UTM para acceso seguro hacia los servicios internos y externos según los perfiles de cada usuario de la Agencia Accha.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes Internacionales

- En el INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Mora Huiracocha Rubén, Gallegos Segovia Pablo, Vintimilla Tapia Paúl, Bravo Torres Jack, Cedillo Elias Julieta y Larios Rosillo Victor, en su artículo de investigación titulado IMPLEMENTATION OF A SD-WAN FOR THE INTERCONNECTION OF TWO SOFTWARE DEFINED DATA CENTERS, realizaron un despliegue experimental basado en living lab para analizar la interconexión entre dos centros de datos utilizando SD-WAN. Este trabajo se basó en los siguientes puntos críticos a tomar en cuenta para el despliegue, el tamaño de la red, la característica de los equipos, aplicaciones y servicios prestados por diferentes fabricantes, vendedores y proveedores; y el tiempo de inactividad en los elementos de la red como resultado de interrupciones causadas por factores humanos. Los autores configuraron la solución SD-WAN empleando Mininet y el controlador FloodLight, dentro de un servidor con sistema operativo Ubuntu 12.04 en VMware. El objetivo principal de este trabajo fue verificar que se puede garantizar un nivel adecuado de QoS y dar prioridad al tráfico en una red SD-WAN, los resultados obtenidos luego de la simulación demostraron que SD-WAN es una solución válida para resolver las dificultades relacionadas con las limitaciones de las redes actuales, debido que se pudo asegurar un nivel adecuado de calidad de servicio del ancho de banda, aplicando políticas para la priorización del tráfico. En los escenarios implementados, el controlador puede administrar de manera eficiente 300 llamadas VoIP, usando un máximo de carga de CPU del 16%. Esto refleja una gestión eficiente de los recursos en la red. (Mora, et al, 2019)

- En la UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL (Ecuador), Douglas Oswaldo Ayapata Mendoza, en su trabajo titulado MODELADO DE UNA WAN UTILIZANDO REDES DEFINIDAS POR SOFTWARE DE ALTA DISPONIBILIDAD EN EL SEGMENTO CORPORATIVO, realizó el modelado de una WAN utilizando redes definidas por software para evaluar el rendimiento de una red SD-WAN a comparación de una red WAN tradicional, se detallan los problemas presentados: (a) Necesidad de una solución que sea flexible frente a cambios de conectividad y servicios según las demandas actuales. (b) Costo de una infraestructura de red WAN convencional elevado. El autor simulo la infraestructura de red utilizando el software Packet tracer, implementando la solución SD-WAN sobre equipos Fortigate 80D y Fortigate 60E y configuró túneles IPsec site-to-site para la comunicación entre sedes. El autor finalmente pudo concluir que existe alta disponibilidad después de implementar la solución, así como también el balanceo de carga por parte de la solución SD-WAN. (Ayapata, 2020)

- En la ESCUELA POLITÉCNICA NACIONAL (Ecuador), López Arévalo Jonathan Javier, en su trabajo titulado EMULACIÓN DE UNA RED SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA FORTINET Y EL SOFTWARE GNS3, desarrolló un análisis de las Redes de Área Extendida Definidas por Software (SD-WAN), utilizando el programa GNS3 y empleando los dispositivos de la tecnología FORTINET. Se detallan los objetivos desarrollados: (a) Analizar las características y funcionalidades de la red MPLS y SD-WAN. (b) Analizar la arquitectura de red a emular, incluyendo tecnología MPLS, basado en SD-WAN. (c) Implementar el prototipo mediante tecnología FORTINET y el software GNS3. El autor pudo determinar que la solución SD-WAN de FORTINET representa un ahorro de costos en tres aspectos principales. En primer lugar, en cuanto a costos de operación (OPEX) a través de las funcionalidades ZTP y control centralizado; en segundo lugar, en los

gastos de capital (CAPEX), al integrar las funcionalidades de SD-WAN, optimización WAN, Firewall, entre otras, en un único dispositivo (FortiGate); y, en tercer lugar, respecto al ancho de banda gracias a los enlaces directos a Internet, pues resulta más conveniente actualizar solamente la suscripción con el ISP. (López, 2020)

- En la UNIVERSIDAD CATÓLICA DE CUENCA (Ecuador), Romero Valdivieso Ernesto Remigio y Cuenca Tapia Juan Pablo, en su artículo de investigación titulado, IMPLEMENTACIÓN DE SD-WAN CORPORATIVO PARA EL USO EFICIENTE DE LAS TELECOMUNICACIONES PARA EL HOLDING QUITO MOTORS, buscaron determinar la forma correcta de asignación de ancho de banda de forma automatizada para conseguir eficiencia en la red y poder garantizar altos niveles de rendimiento, para aplicaciones críticas sin sacrificar la seguridad o privacidad de la data, se detallan los principales objetivos desarrollados: (a) Disponer de una administración centralizada y segmentar la red a nivel nacional. (b) Disponer de control perimetral por cada agencia y control del contenido del tráfico. (c) Disponer del monitoreo de los servicios a nivel de red y reducir los costos. Los autores emplearon equipamiento Fortigate en la sede principal y SD-WAN Cisco Meraki en las agencias, tomando en cuenta la compatibilidad entre los equipos empleados en la infraestructura de red de holding Quito Motors. Finalmente, los autores pudieron determinar que se mejoró notablemente el rendimiento, la administración, gestión, la seguridad y la disponibilidad de la red y a su vez maximizar los beneficios minimizando costes. (Romero & Cuenca, 2020)

2.1.2 Antecedentes Nacionales

- En la UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS (Perú), Orosco Pahuara Bequer Brayan, en su trabajo titulado IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE

LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL, buscó evaluar y determinar las causas de la baja calidad en la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas, se detallan los principales objetivos desarrollados: a) Identificar la situación actual a nivel de red y comunicaciones de la Universidad. b) Realizar pruebas de comunicación de voz, video y datos entre los locales de la Universidad. c) Determinar la causa de la baja calidad en la comunicación de voz, video y datos en la Universidad. El autor utilizo la herramienta CACTI para monitorear el rendimiento de la red antes y después de implementar la solución propuesta, realizó las pruebas con una central de telefonía Yeastar y Firewalls FortiGate-VM para determinar la elección del enlace óptimo utilizando los features link-monitor y wan-load-balance. El autor pudo concluir que la baja calidad en la comunicación de voz es a causa a un deficiente servicio de Internet contratado, y los equipos de redes instalados en cada local. (Orosco, 2018)

- En la UNIVERSIDAD TECNOLÓGICA DEL PERU (Perú), Aguilar Ruiz Luis Enrique, 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, realizó una propuesta de diseño para conectar sucursales de forma segura utilizando internet doméstico mediante tecnología SD-WAN, se detallan los problemas presentados: (a) El BW del servicio de interconexión por MPLS de los ISP es demasiado costoso. (b) Riesgo de indisponibilidad del servicio por no contar con alta disponibilidad. (c) Es posible determinar la cantidad de BW correcto para que una oficina pueda trabajar de manera rápida y sin latencia. Se implementó una solución SD-WAN sobre equipos Fortigate 50E y Fortigate 400E, sobre tuneles IPsec. Se validó que se pudo determinar la cantidad de BW requerido por cada oficina en la propuesta de diseño, se validó que los costos al

utilizar una solución SD-WAN sobre internet para conexión fue menor que al utilizar un enlace MPLS de un ISP, se validó que los datos para la comunicación entre sucursales estaban cifrados y se validó que con las redes SD-WAN se obtuvo una mayor disponibilidad en la comunicación de sucursales. (Aguilar, 2020)

- En la UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS (Perú), Rodríguez Guerrero Ernesto, en su trabajo titulado DISEÑO Y SIMULACIÓN DE UNA RED DEFINIDA POR SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO AVANZADO DE DATOS PARA LA EP DE TELECOMUNICACIONES DE LA FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA DE LA UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS, realizó una propuesta de Red Definida por Software-SDN para la implementación de un laboratorio avanzado de datos en la UNMSM, se detallan los principales objetivos desarrollados: (a) Diseñar la topología de laboratorio SDN para la FIEE-UNMSM, incluyendo la descripción de los equipos que debe tener. (b) Simular el funcionamiento del controlador open-source elegido para la red de laboratorio SDN. El autor utilizó Mininet y Wireshark para el análisis y simulación del escenario propuesto, así como equipamiento Fortigate 100E para el filtrado de contenido mediante UTM y para las conexiones VPN SSL. Finalmente, el autor determinó que las simulaciones de la red SDN propuesta fueron realizadas usando la herramienta Mininet tanto para escenarios en IPv4 como IPv6: observándose que IPv6 es un 76.216 % superior en throughput y que el controlador open-source SDN OpenDayLight es el más recomendado debido a que ofrece más flexibilidad y posee mayor documentación. (Rodríguez, 2020)

- En la UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS (Perú), Munayco Coronado Roberto Willy, en su trabajo titulado DISEÑO DE REDES LAN BASADA EN SOFTWARE PARA UN PROVEEDOR DE DATACENTER LIDER EN PERU, determinó los mecanismos para tener en cuenta al transformar una red LAN tradicional, siguiendo las

demandas que se requieren actualmente al usar aplicativos en la nube, basándose en el cuadrante de Gartner. Se detallan los principales objetivos desarrollados: (a) Mantener las características de la red tradicional en nuestro diseño de la red basada en software defined network (SDN). (b) Reducir a horas el tiempo de implementación de una red LAN, para un nuevo cliente. (c) Evaluar que el equipamiento a elegir cumpla con los requerimientos técnicos que solicita la organización según el cuadrante de gartner y flexibilidad en crecimiento hacia nubes públicas. (d) Evaluación económica para implementar una nueva red tradicional contra una red basada en software que muestra los beneficios de reducción de costos. Para el desarrollo del presente trabajo se utilizó equipamiento de Cisco N9K-C9364C y N9K-C93180YC-EX para la implementación del SDN. El autor determinó que la infraestructura propuesta ofrece un alto grado de estabilidad para poder soportar el crecimiento exponencial de los servicios, así mismo se determinó que al implementar una red SDN los costos son menores que al implementar una red tradicional, debido a que posee una gestión centralizada. (Munayco, 2020)

2.2 Bases teóricas

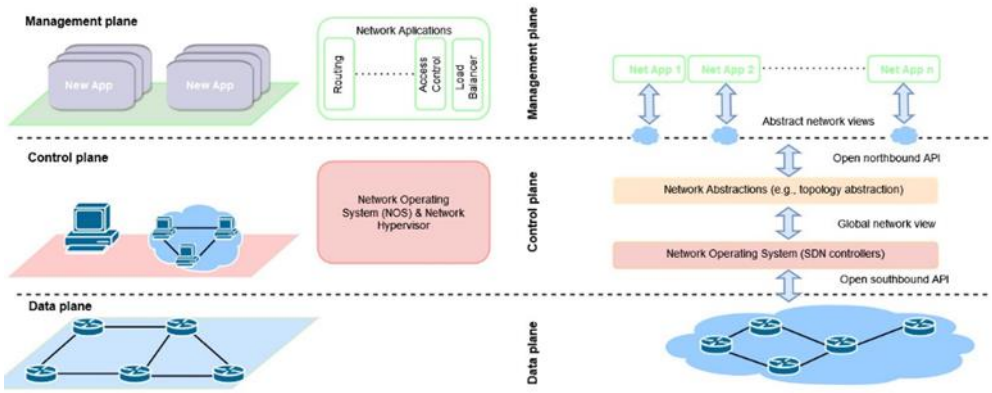
2.2.1 SD-WAN

SD-WAN permite una gestión centralizada de redes WAN, que va de la mano con la computación en la nube y la seguridad, lo que significa ser capaz de instalar servicios de comunicación con soporte de virtualización y aplicación de políticas de seguridad. La tecnología SD-WAN utiliza algunos enfoques de Redes definidas por software (SDN) que se aplican a las redes WAN, la segunda tecnología clave que es importante conocer para comprender el concepto SD-WAN es la virtualización de funciones de red (NFV). (Kreutz, et al, 2015)

2.2.2 Redes Definidas por Software (SDN)

Las redes definidas por software, nació como un nuevo enfoque para el diseño y operación de la infraestructura de red, donde el plano de control de red se encarga de la lógica de control, el cual está separado del plano de datos que se encarga de las funciones de reenvío de datos de los dispositivos. Las funciones de control en SDN se extraen de dispositivos individuales y se integran en un nodo de control centralizado, llamado lógica inteligente de SDN o Sistema Operativo de Red (NOS). Los dispositivos de red física están en las redes SDN y se utilizan solo para sus funciones relacionadas con el reenvío de datos o conmutación. Este enfoque permite la abstracción del control de la infraestructura de red física, a menudo representada como un conmutador virtual, y permite la programación central y automatizada del comportamiento de la red, políticas o servicios en un solo lugar, las cuales emplean interfaces y herramientas de programación). (Segeč, et al, 2020)

Figura 1: *Distribución de planos, según la Arquitectura SDN.*



Nota: *El gráfico muestra que los planos separados se interconectan mediante la utilización de API del tipo Southbound y Northbound. Adaptado de Software-Defined Networking: A Comprehensive Survey (p.24), de Kreutz, et al, 2015, IEEE, 103.*

La Northbound API se utiliza para conectar, mediante programación, el controlador al plano de la aplicación, donde se encuentran todas las aplicaciones de red SDN. Este tipo de interfaz permite a los administradores aprovechar la capacidad de programación y la automatización de red de alto nivel. De igual forma la Southbound API se encuentra entre el nivel de infraestructura de red y el controlador. A través de esta API, el controlador controla las funciones de reenvío de los elementos de la infraestructura de red. (Segeč, et al, 2020)

2.2.3 Virtualización de Funciones de Red (NFV)

La virtualización de funciones de red permite reemplazar dispositivos de red físicos por dispositivos o funciones de red de software denominados, función de red virtual, el propósito de este es ahorrar recursos mediante el uso de hardware genérico y, por lo tanto, rentable para la aplicación de funcionalidades de red. La transición a instancias de software de funciones de red también ofrece la

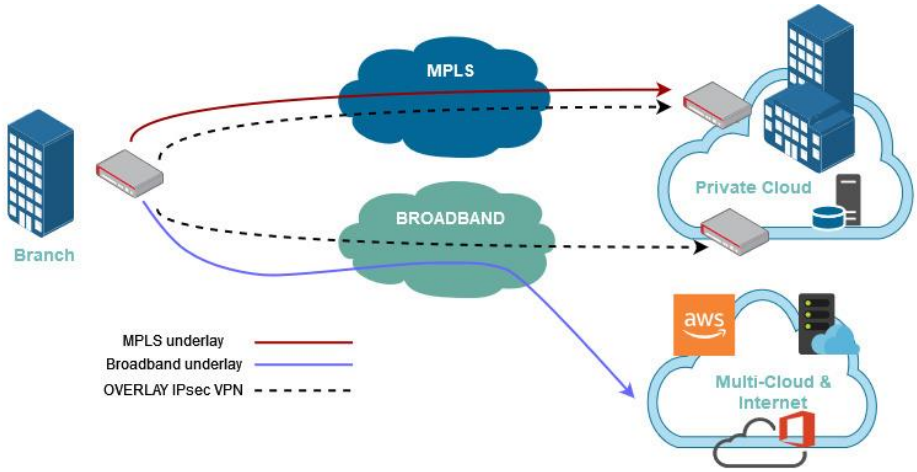
posibilidad de flexibilidad a través de la gestión de recursos dinámicos programables a través de SDN. Sin embargo, SDN no es una parte obligatoria de VNF, es una tecnología complementaria adecuada a VNF. (Segeč, et al, 2020)

2.2.4 SD-WAN sobre FortiOS

FortiOS, es el componente básico de la solución Secure SD-WAN, debido a su capacidad autónoma de proporcionar una funcionalidad completa que incluye NGFW, funciones de seguridad avanzadas y capacidades SD-WAN. FortiOS también ofrece compatibilidad entre diversos protocolos de enrutamiento y emparejamiento de VPN como radio o hub, permite la optimización WAN mediante la optimización del protocolo, el almacenamiento en caché de bytes y objetos, e incluso actúa como un controlador de capa de acceso. Además, FortiGate admite la prioridad de paquetes para garantizar que las aplicaciones críticas para el negocio tengan prioridad en tiempos de congestión. (Fortinet, Fortinet Secure SD-WAN Reference Architecture, 2019)

La funcionalidad de Secure SD-WAN permite agrupar interfaces miembros, las cuales pueden ser físicas o virtuales. En las versiones anteriores al FortiOS 6.4 solo se permitía crear un SD-WAN sobre un dominio virtual como tal, sin embargo, Fortinet lanzo la mejora para poder establecer varios grupos SD-WAN y no tener la limitante de adquirir un equipo adicional o adicionar dominios virtuales.

Figura 2: *Interfaces WAN miembros de SD-WAN*



Nota: *Existen dos interfaces físicas WAN1 y WAN2, sobre diferentes tecnologías, las cuales pueden ser miembros del SD-WAN al igual que las interfaces virtuales de los túneles IPsec.* Adaptado de *Fortinet Secure SD-WAN Reference Architecture (p.9)* de*, Fortinet, 2019.*

2.2.5 IPsec VPN

IPSec es un protocolo de capa 3 de acceso remoto, intranet y extranet. Una red privada virtual (VPN) permite a los usuarios remotos conectarse a redes informáticas privadas para obtener acceso a sus recursos de forma segura. El uso de una VPN garantiza que las partes no autorizadas no puedan acceder a la red de la oficina y no puedan interceptar la información que se intercambia entre el empleado y la oficina, debido a que utiliza un mecanismo de autenticación y encriptación. La ruta de datos entre la computadora de un usuario y una red privada a través de una VPN se conoce como túnel, debido a que su funcionamiento es como la de un túnel físico, la ruta de datos es accesible solo en ambos extremos. En el escenario del teletrabajo, el túnel se ejecuta entre la aplicación FortiClient en la PC del usuario, o una unidad FortiGate u otro dispositivo de red y la unidad FortiGate en la red privada de la oficina. (Fortinet, FortiOS 6.0 Handbook, 2020)

2.2.6 Mecanismo de encriptación en VPN Ipsec

El cifrado se utiliza para poder convertir datos a un código secreto, para que luego pueda ser transportado de forma segura. Existen dos mecanismos de encriptación, simétrico y asimétrico. (Xtream Team México, 2007)

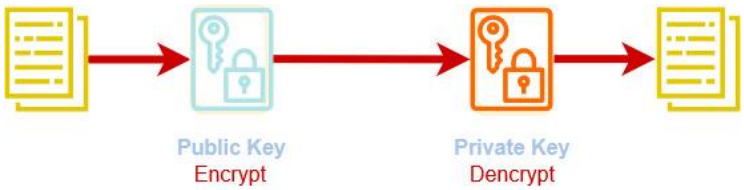
Encriptación simétrica, utiliza la misma llave para cifrar y decifrar la información.

Figura 3: *proceso de encriptación simétrica*

Nota: *Los mecanismos de encriptación simétrica más comunes utilizados son DES, 3DES, RC5, Rijndael.* Adaptado de *Concepts, Interoperability and Diagnose of VPN (p.16),* de *Xtream Team México, 2007.*

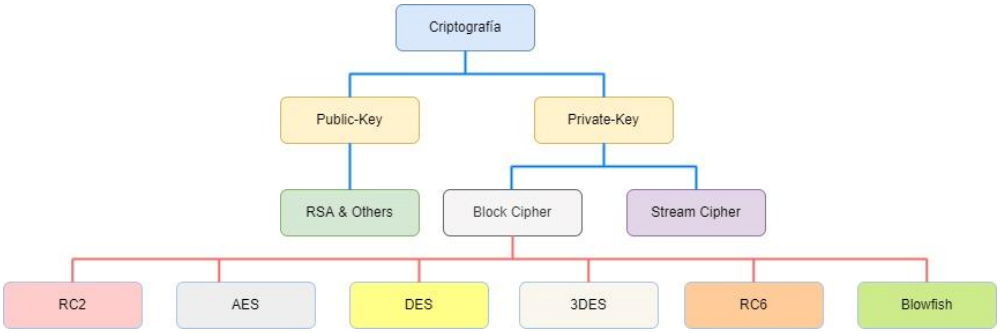
Encriptación asimétrica, utiliza diferentes tipos de llaves para cifrar y descifrar la información.

Figura 4: *Encriptación asimétrica*



Nota: *Se emplean dos llaves, una llave denominada pública y la otra privada.* Adaptado de *Concepts, Interoperability and Diagnose of VPN (p.17),* de *Xtream Team México, 2007.*

Figura 5: *Mecanismos de cifrado según la llave*

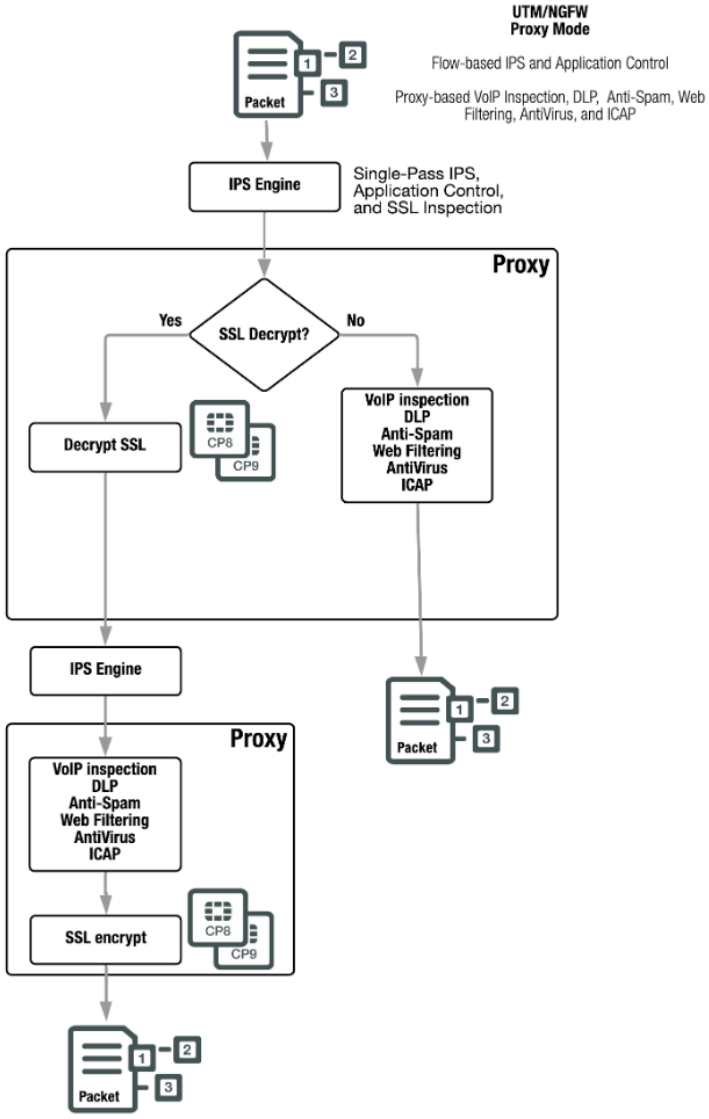


Nota: *Como se muestra en el gráfico, los mecanismos de cifrado AES, 3DES y DES se clasifican como simétricos, debido a que solo emplean la llave privada tanto para cifrar como descifrar la información.* Adaptado de *Performance Evaluation of Cryptographic Algorithms: DES and AES* (p.1)*,* port *Mandal, et al, 2012, IEEE.*

2.2.7 Gestión Unificada de Amenazas (UTM)

La gestión unificada de amenazas está configurada para realizar la inspección en dos modos, proxy o flow-based. La inspección UTM basada en proxy, puede aplicar tanto la inspección flow-based como la basada en proxy. Los paquetes encuentran inicialmente el motor IPS, que puede aplicar IPS y Control de aplicaciones basados en flujo de una sola pasada. Luego, los paquetes se envían al proxy para una inspección basada en el proxy. La inspección basada en proxy puede aplicar inspección VoIP, DLP, AntiSpam, Filtrado web, Antivirus e ICAP. (Fortinet, FortiOS- ParallelPath Processing, 2019)

Figura 6: *Flujo de paquetes en UTM modo proxy*



Nota: *La desencriptación y encriptación de los paquetes, al realizar el análisis de inspección profunda, está condicionado según las categorías configuradas en el SSL/Inspection a ser baipaseadas.* Adaptado de *FortiOS- ParallelPath Processing* (p.22) de*, Fortinet, 2019.*

2.2.8 GNS3

GNS3 permite crear escenarios para emular redes actuales, además que actualmente GNS3 tiene incluida en sus librerías equipamiento virtualizado de diferentes fabricantes, lo que lo hace óptimo para recrear un entorno casi real. GNS3 consta de dos componentes de software, el software GNS3-todo-en-uno (GUI) y la máquina virtual GNS3 (VM). GNS3 todo en uno: esta es la parte del cliente de GNS3 y es la interfaz gráfica de usuario (GUI). Instala el software todo en uno en su PC local y crea sus topologías utilizando este software. Si decide utilizar la máquina virtual GNS3, puede ejecutar la máquina virtual GNS3 localmente en su PC utilizando software de virtualización como VMware Workstation, Virtualbox o Hyper-V; o puede ejecutar la máquina virtual GNS3 de forma remota en un servidor utilizando VMware ESXi o incluso en la nube. (GNS3, GNS3 Documentation, 2021)

2.3 Definición de términos básicos

- **SD-WAN:** Solución de red de área ancha definida por software (SD-WAN), permite transformar las capacidades de una organización al aprovechar los WAN, así como la conectividad de múltiples nubes para brindar un rendimiento de aplicaciones de alta velocidad en el borde de la red. (Fortinet, Fortinet Products, 2020)

- **Dial-up**: Tipo de VPN que permite a los usuarios conectarse a Internet mediante una conexión de acceso telefónico a través de líneas telefónicas tradicionales POTS o ISDN, se utilizan protocolos de red privada virtual para proteger estas conexiones privadas. (Fortinet, Docs Fortinet Cookbook, 2020)

- **Latency:** Tiempo total de ida y vuelta para el envío de un paquete de datos, se mide en milisegundos como parámetro de configuración dentro de las reglas sd-wan. (Fortinet, Fortinet Resources Cyberglossary, 2021)

- **Jitter:** El valor absoluto de la diferencia entre el retraso de reenvío de dos paquetes recibidos consecutivos que pertenecen al mismo flujo, se mide en milisegundos como parámetro de configuración dentro de las reglas sd-wan. (IETF, 2016)

- **Packet Loss:** Paquetes de datos que no se completan o transmiten correctamente, se mide en (%) como parámetro de configuración de reglas sd-wan. (Fortinet, Fortinet Resources Cyberglossary, 2020)

- **UTM (Unified Threat Manager):** múltiples funciones o servicios de seguridad que incluye antivirus, filtrado de contenido, filtrado de correo electrónico y web, antispam, etc. (Fortinet, Fortinet Resources Cyberglossary, 2020)

- **GNS3:** software de códgio abierto utilizado para emular, configurar, probar y solucionar entornos de redes virtuales y reales. (GNS3, 2021)

- **Fortigate:** Equipamiento Next-Generation Firewall propietario de Fortinet, además de mantener las características de un firewall, como el filtrado de paquetes, la compatibilidad con IPsec y VPN SSL, la supervisión de la red y las funciones de mapeo de IP, los NGFW poseen capacidades de inspección de contenido más profundas. Estas capacidades ofrecen la habilidad de identificar ataques, malware y otras amenazas. (Fortinet, Fortinet Products, 2020)

- **IPsec:** La tecnología de red privada virtual (VPN) permite a los usuarios remotos conectarse a redes informáticas privadas para obtener acceso a sus recursos de forma segura. (Fortinet, Fortinet Products, 2020)

- **Forwarding Device (FD):** Dispositivos de reenvío basados en hardware o software del plano de datos, que tienen conjuntos de instrucciones bien definidos para realizar una acción sobre los paquetes entrantes, como

reenvío por puertos específicos, reescribir algún encabezado, descartar o reenviar paquetes al controlador. (Segeč, et al, 2020)

- **Data Plane (DP):** Dispositivos de reenvío interconectados inalámbrica o alámbricamente. (Segeč, et al, 2020)

- **Southbound Interface (SI):** Define los protocolos de comunicación entre los dispositivos de reenvío y los elementos del plano de control. El conjunto de instrucciones de los dispositivos de reenvío está definido por el southbound API. (Segeč, et al, 2020)

- **Control Plane (CP):** La lógica de control descansa en las aplicaciones y controladores que forman parte del plano de control. (Segeč, et al, 2020)

- **Northbound Interface (NI):** Una interfaz northbound abstrae los conjuntos de instrucciones de bajo nivel utilizados por las southbound interface para programar los dispositivos de reenvío. (Segeč, et al, 2020)

- **Management Plane (MP):** Conjunto de aplicaciones que aprovechan las funciones que ofrece la NI para implementar el control de la red y la lógica de operación. (Segeč, et al, 2020)

CAPÍTULO III: DESARROLLO DEL TRABAJO PROFESIONAL

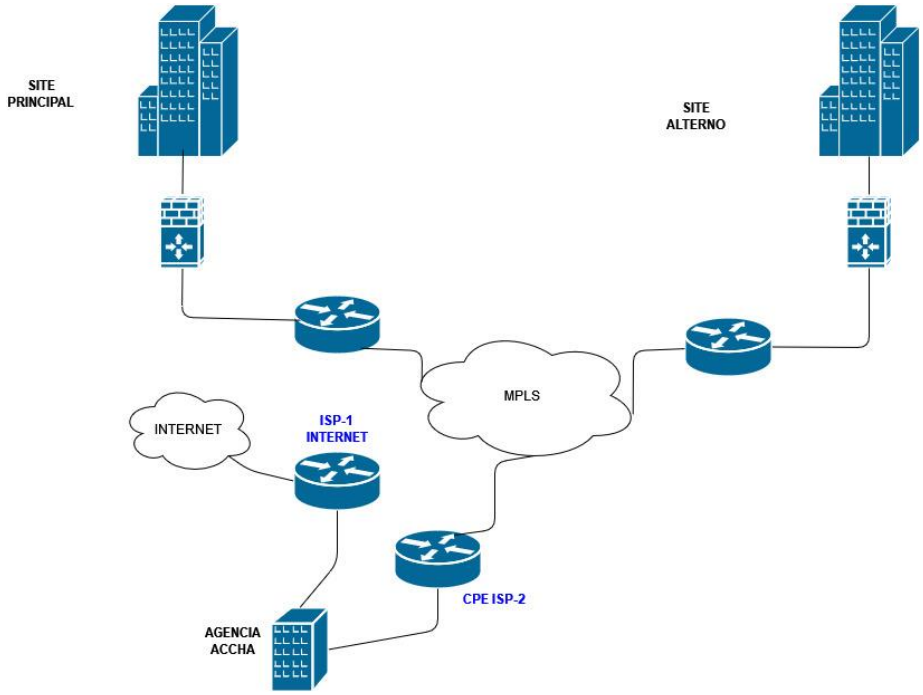
3.1 Determinación y análisis del problema

3.1.1 Descripción de la realidad problemática

Según la topología de la infraestructura de red, de la agencia Accha, mostrada en la **Figura 7**, se observó que cuenta con dos equipos de red CPE, uno provisto por el ISP-1 para salida a internet y el segundo por el ISP-2 que brinda el servicio de RPV para la conexión entre sus sedes principales.

Se visualiza que el enlace del ISP-2 solo le permite salida a internet, no se tiene un equipo configurado para brindar automatización basándose en criterios de calidad de los enlaces tales como latency, jitter y packet loss, así como tampoco poder utilizar el enlace del ISP-2 para comunicaciones con los servidores del Site Principal y el Site alterno y de esta forma brindar redundancia en sus comunicaciones.

Figura 7: *Topología Agencia ACCHA*



Nota: *El gráfico muestra que la agencia Accha no posee dos proveedores ISP con el servicio de VPN. El proveedor ISP-1 brinda servicio de salida a internet con un BW de 1Mbps y el proveedor ISP-2 brinda el servicio de RPV que le permite realizar comunicación desde la agencia hacia el Site Principal y el Site Alterno mediante su red MPLS con un BW de 2Mbps.*

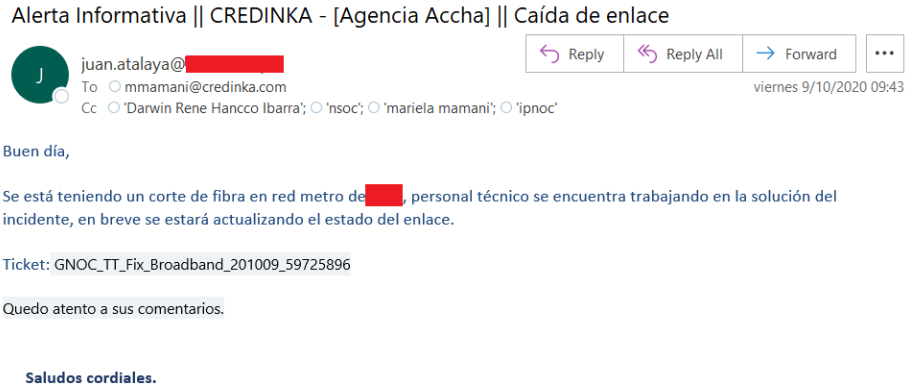
De la **Figura 7,** se visualiza que en el caso de que la red del proveedor ISP-2 tenga una incidencia en su infraestructura, la agencia solo tendría salida a internet por el proveedor ISP-1, lo que ocasiona que los servicios de la Agencia Accha no puedan comunicarse con los servidores del Site principal y el Site alterno.

Figura 8: *Reporte de incidencia con ISP-2.*

Nota: *Según el correo de la incidencia, se reportó la caída del enlace del ISP-2 a las 08:16hrs del 9 de octubre del 2020.*

Generalmente las incidencias se deben a problemas de corte de fibra o caída de energía en el nodo, debido a que Accha es una agencia ubicada en una zona rural, el SLA ante una incidencia es de 12 horas.

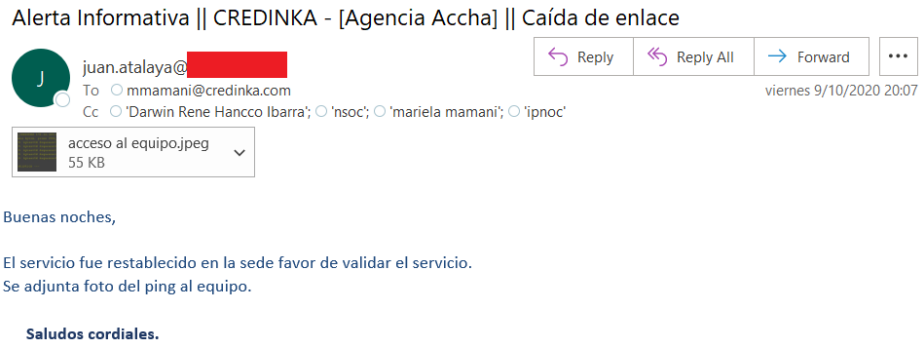
Figura 9: *Ticket de incidencia brindado por parte del ISP-2*



Nota: *Se tiene respuesta del ISP-2 a las 09:43 hrs con el número de ticket asociado al incidente, según se detalla en el correo, se debe a un corte de fibra.*

El cliente solo puede pedir una penalización ante una incidencia cuando se pase el SLA, sin embargo 12 horas es un tiempo elevado para que la agencia pueda seguir con sus operaciones.

Figura 10: *Reporte de solución de la incidencia por parte del ISP-2*



Nota: *Se visualiza que la finalización de la incidencia fue a las 20:07hrs del 9 de octubre del 2020. El tiempo de duración aproximado es de 12hrs por lo que se encuentra dentro del SLA al ser una agencia catalogada como rural.*

Los datos del análisis de incidencias muestran la problemática que surge cuando no se cuenta con el ISP-2, debido a que la agencia

Accha solo cuenta con salida a internet, mientras se restablezca el enlace por parte del proveedor ISP-2.

De igual forma, los datos que se transmiten para realizar la comunicación entre recursos internos o externos, mediante la red MPLS del ISP-2, no deben viajar en texto plano por la red del proveedor, debido a que genera una brecha de seguridad en el tratamiento de los datos sensibles que se manejan.

La infraestructura de red de esta agencia no tenía implementado un dispositivo de seguridad, como se aprecia en la **Figura 8**. Para poder restringir el acceso hacia internet por parte de los usuarios, lo que puede ocasionar que accedan a páginas que contengan contenido malicioso, que representa una brecha de seguridad.

El rubro de la empresa es del sector bancario, por lo que los tiempos de inactividad, así como también la falta de seguridad en el transporte de los datos hacia la sede central del servicio tienen un gran impacto en las operaciones que se realizan, lo que también puede conllevar en un bajo nivel de satisfacción por parte de los clientes de la empresa, así como también que pueda ser utilizada alguna brecha de seguridad por un actor malicioso.

La implementación del Fortigate 60E busca mitigar estas brechas de seguridad presentes en la infraestructura de red, así como también poder utilizar las diferentes funcionalidades para poder gestionar de una forma eficiente el BW de la Agencia Accha.

3.1.2 Formulación del problema

- **Problema general**

¿Cómo mejorar la redundancia para la comunicación de la agencia Accha, considerando los criterios de calidad de los enlaces y seguridad de los datos transportados?

- **Problemas específicos**

¿Qué solución brinda redundancia basada en criterios de calidad de los enlaces WAN?

¿Qué mecanismo se debe utilizar para la protección de los datos sensibles transportados por la red MPLS del proveedor ISP?

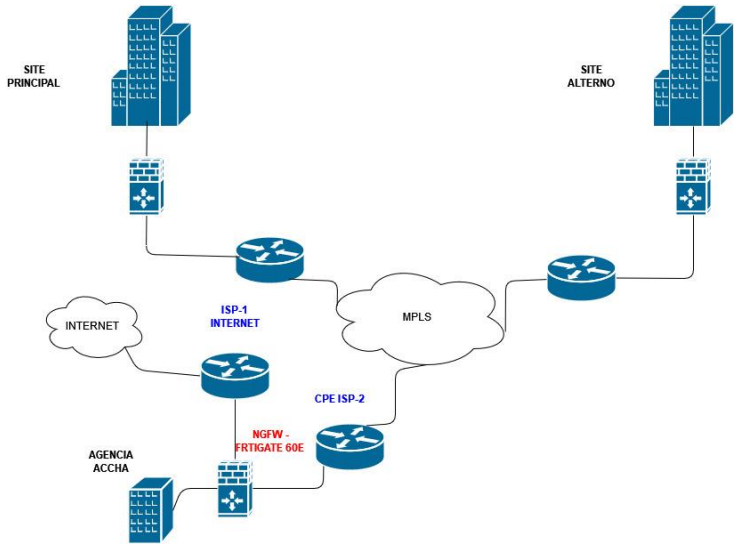
¿Cómo mejorar acceso seguro hacia comunicaciones internas y externas desde la agencia Accha?

3.2 Modelo de solución propuesto

3.2.1 Análisis de la topología

La topología mostrada en la **Figura 7**, no presenta un dispositivo de seguridad perimetral desde la agencia Accha, del mismo modo se visualiza que tiene salida a internet directa sin ninguna restricción por el ISP-1 para la navegación por parte de los usuarios.

***Figura 11**: Topología Accha utilizando un Fortigate perimetral en agencia.*



***Nota:** Fortigate 60E conectado directamente con el router CPE del ISP-1 de salida a internet directa y el CPE del ISP-2 que brinda el servicio de RPV para la interconexión entre sedes.*

La topología de la **Figura 11**, muestra un firewall NGFW Fortigate 60E incorporado dentro de la infraestructura de red de la Agencia Accha, lo que propuso poder definir políticas de seguridad para acceso hacia internet por parte de los usuarios. Con la incorporación de un firewall también se propuso poder levantar túneles IPsec dial-up hacia la sede principal y alterna desde los proveedores ISP-1 y ISP-2, para cifrar los datos que se transfieren por la red MPLS del proveedor e internet. Del mismo modo se buscó aprovechar la característica de SD-WAN habilitada dentro del equipo Fortigate, para redundancia de acceso a servicios internos mediante la elección del enlace que presente el mejor performance y además tener la capacidad de gestionar el tráfico hacia los enlaces WAN independientemente de los proveedores contratados.

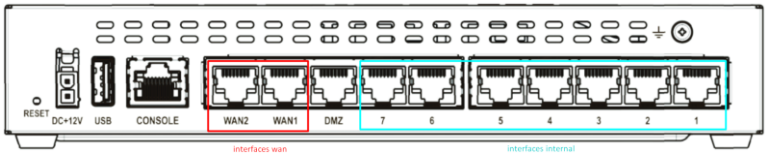
3.2.2 Análisis del equipamiento Fortigate

Especificaciones del Hardware

Para implementar las soluciones planteadas se utilizó un equipo fortigate 60E, se detallan a continuación las especificaciones del hardware, así como también los features compatibles con la solución planteada.

Fortigate 60E cuenta con 2 interfaces por defecto del tipo WAN (WAN1 y WAN2), las cuales tienen una velocidad de transferencia de 1 Gigabyte mediante un conector Ethernet del tipo RJ45. Este equipo también cuenta con 7 interfaces por defecto del tipo internal, las cuales tienen una velocidad de transferencia de 1 Gigabyte mediante un conector Ethernet del tipo RJ45. La velocidad de transferencia contratada en la Agencia Accha no supera los 10Mbps, por lo que cumple con lo requerido.

Figura 12: *Fortigate 60E parte posterior. (Fortinet, 2021)*



Nota: *Se muestran las interfaces del Fortigate 60E, existen dos interfaces del tipo WAN y una del tipo DMZ, y siete del tipo LAN por defecto.* Adaptado de *FortiOS- ParallelPath Processing* (p.22) de, *Fortinet, 2019.*

Fortigate 60E soporta 1.3 Millones de sesiones en simultaneo, soporta hasta 5000 políticas de seguridad, 200 túneles VPN IPsec, con una latencia por Firewall de 3µs y tiene un throughput de 4.5 Mpps.

Tabla 1: *System performance Fortigate 60E. (Fortinet, 2021)*

System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	3 / 3 / 3 Gbps
Firewall Latency (64 byte UDP packets)	3 µs
Firewall Throughput (Packets Per Second)	4.5 Mpps
Concurrent Sessions (TCP)	1.3 Million
New Sessions/Second (TCP)	30,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) [1]	2 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
SSL-VPN Throughput	150 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	135 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	135
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	75,000
Application Control Throughput (HTTP 64K) [2]	650 Mbps
CAPWAP Throughput (HTTP 64K)	890 Mbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	16
Maximum Number of FortiAPs (Total / Tunnel Mode)	30 / 10
Maximum Number of FortiTokens	500
High Availability Configurations	Active / Active, Active / Passive, Clustering

Nota: *En la hoja de especificaciones del equipo Fortigate 60E, se validó que soporta los features de un NGFW, para poder implementar filtrado de contenido, protección mediante IPs y Antivirus. (describir las funcionalidades para justificar la valdiación.)*

Figura 13: *Features soportados por Fortigate 60E. (Fortinet, 2021)*

DEPLOYMENT

Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN Orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real- time threat protection

Nota: *También se visualizó que es compatible para habilitar SD-WAN para la conmutación de enlaces de forma automática en tiempo real basado en el tráfico, de la misma forma se indica la compatibilidad con la encriptación de los túneles IPsec.*

Tabla 2: *Rangos ambientales de operación Fortigate 60E. (Fortinet, 2021)*

	FORTIGATE 60E	FORTIGATE 60E-POE
Operating Environment and Certifications		
Input Rating	12Vdc, 3A	12Vdc, 7A
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz	
Maximum Current	115V AC / 0.7 A, 230V AC / 0.48 A	0.8A
Total Available PoE Power Budget*	–	75 W
Power Consumption (Average / Maximum)	11.5 / 14 W	20 / 95 W
Heat Dissipation	48 BTU/h	324 BTU/h
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
Dimensions		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38 × 216 × 160	
Weight	1.9 lbs (0.9 kg)	2.2 lbs (1.0 kg)
Form Factor	Desktop	

Especificaciones del Software

La versión de FortiOs empleada, fue la 6.0.4, debido a la compatibilidad para sincronización con otros equipos internos de la infraestructura del cliente, tales como FortiManager y FortiAnalyzer.

Se validó que la versión FortiOS 6.0.4 es soportada desde la versión 6.0.6 del FortiManager, de acuerdo a la Figura 12.

Figura 14: *Matiz de compatibilidad FortiOS & Fortimanager. (Fortinet, 2021)*

FORTINET

FortiManager Support for FortiOS

Compatibility Chart

The following table lists the FortiManager support for FortiOS. For detailed information on limitations, refer to the FortiManager Release Notes available at the Fortinet Document Library.

FortiOS	FortiManager																														
	5.6.0	5.6.1	5.6.2	5.6.3	5.6.4	5.6.5	5.6.6	5.6.7	5.6.8	5.6.9	5.6.10	5.6.11	6.0.0	6.0.1	6.0.2	6.0.3	6.0.4	6.0.5	6.0.6	6.0.7	6.0.8	6.0.9	6.0.10	6.0.11	6.2.0	6.2.1	6.2.2	6.2.3	6.2.5	6.2.6	6.2.7	6.2.8
5.6.0	◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.1	◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.2		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.3		◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.4				◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.5				✓	◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.6						◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.7								✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.8									✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.9									✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
5.6.10										✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.11											✓	✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.12											✓	✓						✓	✓	◆	✓	✓	✓	✓	✓	◆	◆	✓	✓	✓	✓	✓
5.6.13											✓	✓						✓	✓	◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.14											✓	✓						✓	✓	◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.0													✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.1														✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.2															✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.3																◆	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.4																	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.5																		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
6.0.6																			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Nota: *Se validó que la versión FortiOS 6.0.4 es soportada desde la versión 6.0.6 del FortiAnalyzer.*

Figura 15: *Matriz de compatibilidad FortiOS & FAZ. (Fortinet, 2021)*

FORTINET

FortiAnalyzer Support for FortiOS

Compatibility Chart

The following table lists the FortiAnalyzer support for FortiOS. For detailed information on limitations, refer to the FortiAnalyzer Release Notes available at the Fortinet Document Library.

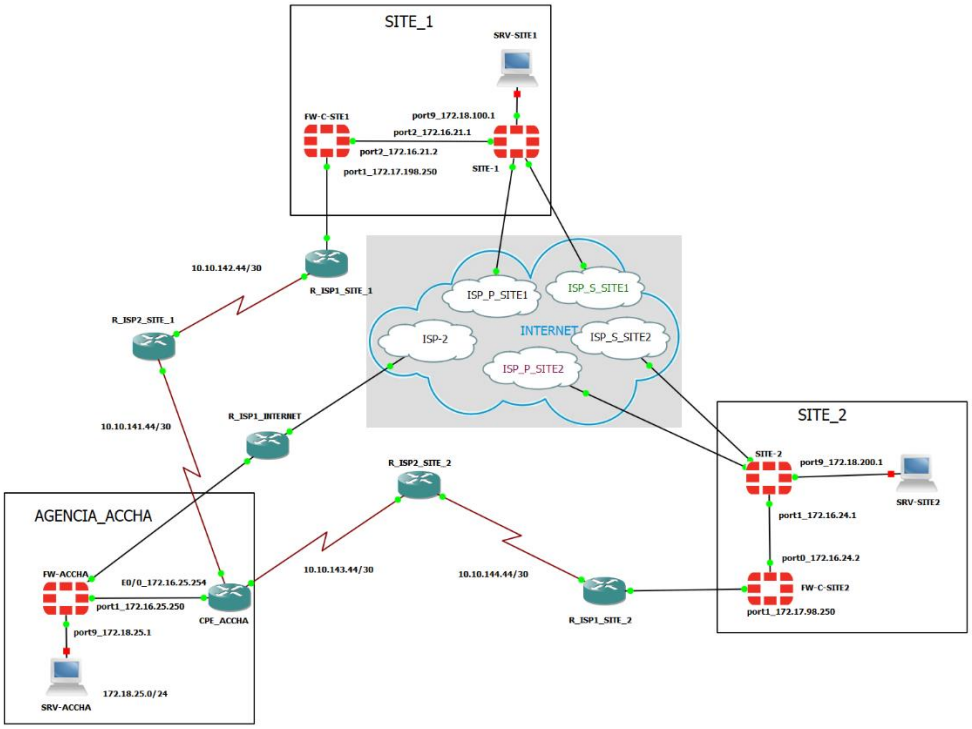
FortiOS	FortiAnalyzer																															
	5.6.0	5.6.1	5.6.2	5.6.3	5.6.4	5.6.5	5.6.6	5.6.7	5.6.8	5.6.9	5.6.10	5.6.11	6.0.0	6.0.1	6.0.2	6.0.3	6.0.4	6.0.5	6.0.6	6.0.7	6.0.8	6.0.9	6.0.10	6.0.11	6.2.0	6.2.1	6.2.2	6.2.3	6.2.5	6.2.6	6.2.7	6.2.8
5.6.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.4				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.5				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.6							✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.7								✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.8									✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.9									✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.10										✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.11											✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.12											✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.13											✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.6.14											✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.0													✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.1														✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.2														✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.3																✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.4																	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.5																		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.6																			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Nota: *Se validó que la versión FortiOS 6.0.4 es soportada por el modelo Fortigate 60E.*

3.2.3 Prueba de concepto

Se desarrolló la simulación utilizando GNS3, para poder validar el correcto funcionamiento de la solución planteada en un entorno controlado y de esta forma reducir los tiempos de inactividad del servicio.

Figura 16: *Simulación red Accha.*



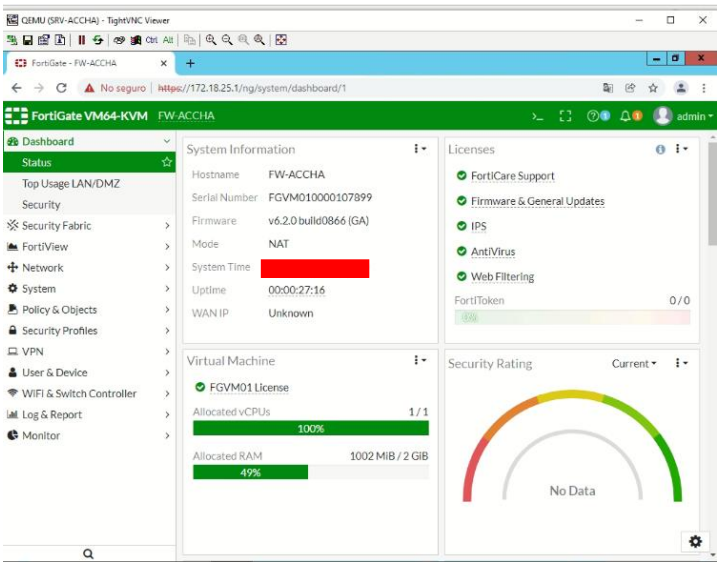
Nota: *Se simuló la infraestructura de conectividad de la Agencia Accha, hacia el Site 1 y Site 2. Se visualiza que la agencia Accha tiene servicio de MPLS por el proveedor ISP-2 y salida a internet directa mediante el proveedor ISP-1.*

Para recrear la infraestructura de comunicación entre la Agencia Accha y el Site-1 y Site-2, se configuraron cinco equipos fortigate KVM, de los cuales se licenciaron tres equipos: SITE-1-P, SITE-2 y FW-ACCHA.

La necesidad de contar con una licencia en los equipos es debido a que Fortinet te restringe a solo crear cinco políticas de seguridad por equipos, al igual que tampoco se puede emplear los perfiles UTM.

Se cargo una licencia al equipo virtualizado FW-ACCHA, debido a que se necesita crear más de cinco políticas, tanto para salida a internet como también para la comunicación hacia el Site principal y el Site secundario.

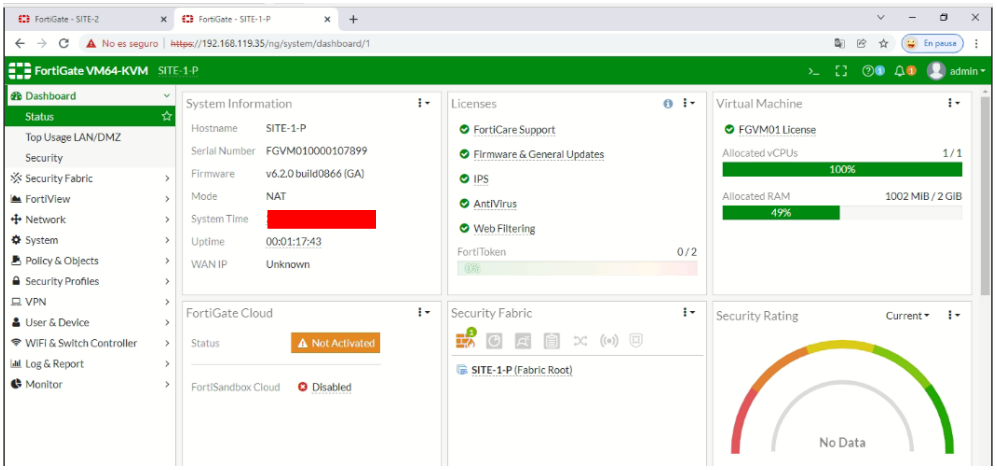
Figura 17: *Fortigate VM64-KVM FW-ACCHA*



Nota: *El FW-ACCHA se encuentra licenciado para poder utilizar, FortiCare Support, Firmware &General Updates, IPS, Antivirus y Web Filtering.*

Además de la limitante de la cantidad de políticas, también se debe utilizar licenciamiento para poder utilizar el filtrado de navegación mediante las categorías de Web Filtering.

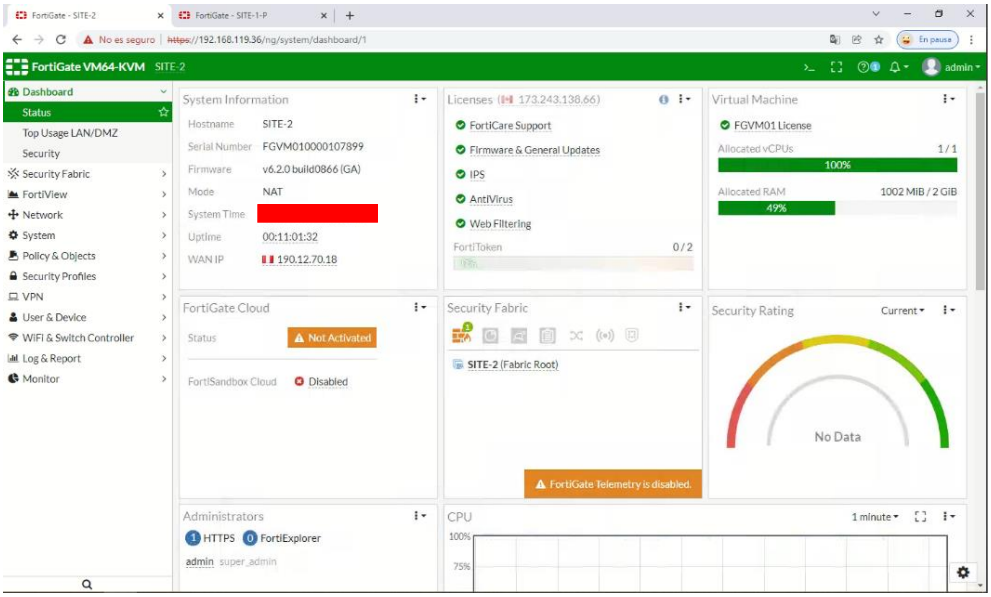
Figura 18: *Fortigate VM64-KVM SITE-1-P*



Nota: *Fortigate SITE-P KVM se encuentra licenciado para poder utilizar Forticare support, Firmware & General Updates, IPS, Antitvirus y Web Filtering.*

El Site-2, posee una configuración que debe estar homologada a la configuración del Site-1, debido a ello también debe contar con un licenciamiento.

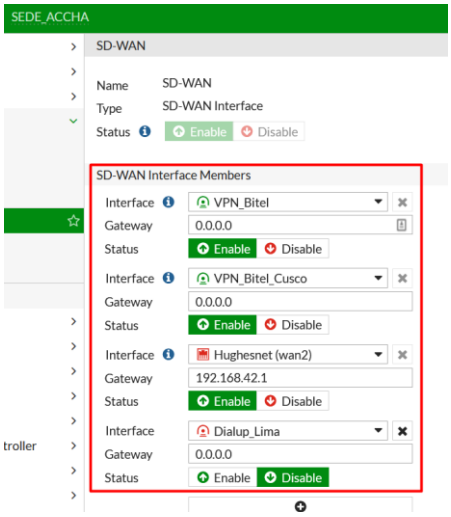
Figura 19:*Fortigate VM64-KVM SITE-2*



Nota: *Fortigate SITE-2 KVM, se encuentra licenciado para poder utilizar Forticare support, Firmware & General Updates, IPS, Antitvirus y Web Filtering.*

Se configuraron como miembros del SD-WAN los puertos port1, VPN_ISP_P y VPN_ISP_S, en la simulación, mientras que en el equipo real se configuraron las interfaces VPN_Bitel, VPN_Bitel_Cusco, Hughesnet y Dialup_Lima, se debe tener en cuenta que para configurar una interface como miembro del sd-wan, no deben existir políticas de seguridad configuradas que hagan referencia a la interface como tal, de lo contrario deberá eliminarse todas políticas donde sea referenciada, esto se debe a que cuando se agrega a la interface al sd-wan, se transforma en una interface virtual donde es referenciada de forma global, esta interface se conoce como virtual-wan-link.

Figura 20: *Miembros de SD-WAN SEDE-ACCHA*

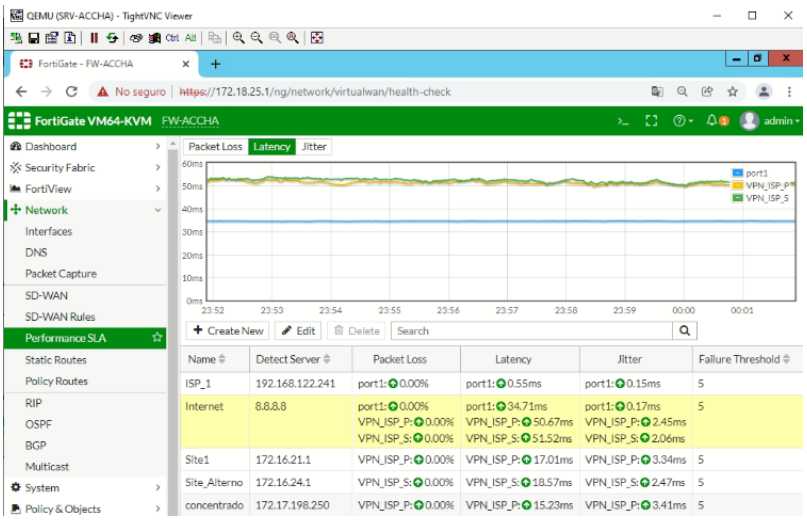


Nota: *Las interfaces miembros del SD-WAN, pueden ser tanto física como en el caso de Hughesnet o virtuales, como en el caso de VPN_Bitel.*

Para configurar el Performance SLA, se debe tener en cuenta el Detect server, ya que los sondeos del performance son medidos según este, generalmente para una configuración a internet, se recomienda realizar el sondeo hacia el dns de Google (8.8.8.8), siendo el valor de latencia de 20ms el óptimo, desde el Firewall KVM FW-ACCHA, se visualiza que la latencia para salida a internet directa por la interface por1, tiene un valor de 34.71ms, mientras que la salida

a internet por el Site principal (VPN_ISP_P) tiene un valor de 50.67ms y la salida por el Site secundario (VPN_ISP_S) tiene un valor de 51.52ms.

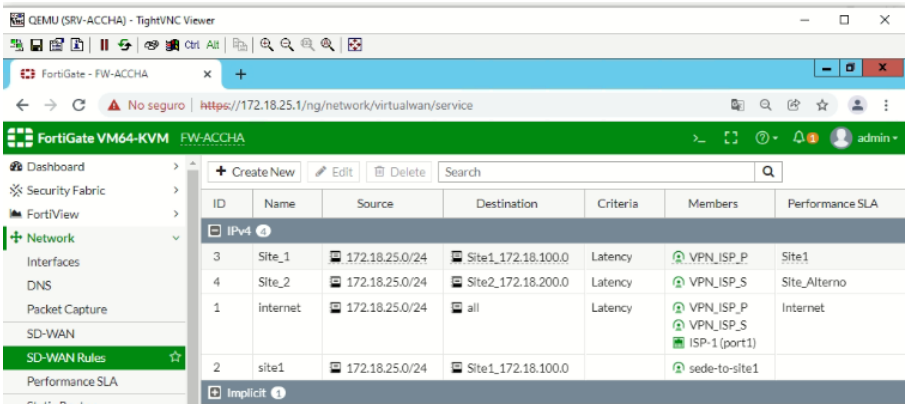
Figura 21: *Performace SLA desde FW-ACCHA*



Nota: *Los valores simulados son parecidos a los valores reales, siendo el valor de salida a internet mediante el port1, el óptimo.*

Las SD-WAN rules, se configurar a manera de condicionales tomando en cuenta el valor del sondeo de los detect server, siendo estos los valores de Packet Loss, Jitter y Latency. También debe tomarse en cuenta las interfaces con las que se quiere evaluar esta medición.

Figura 22: *SD-WAN rules*

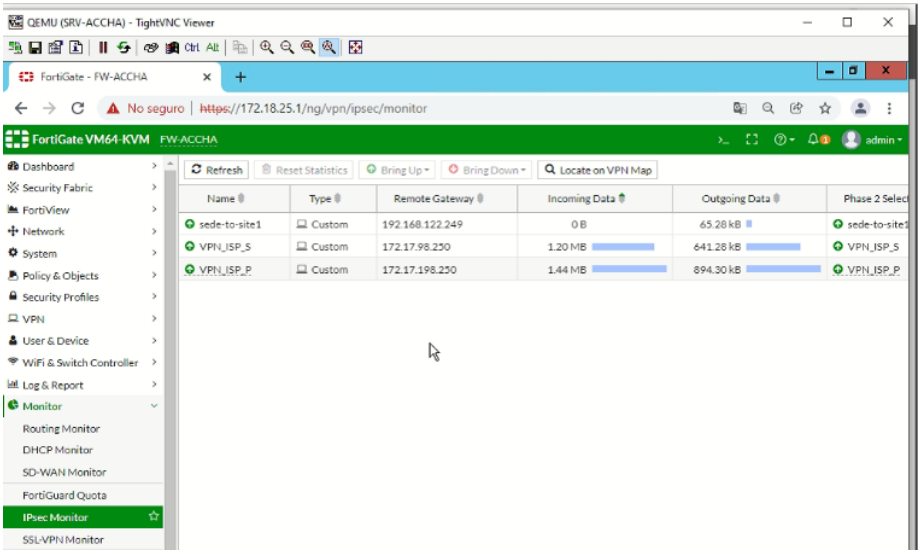


Nota: *Para salida internet, se tiene configurada la sd-wan rule 1, donde el perfomarnce SLA referenciado es el Internet, el cual realiza*

el sondeo hacia el dns de Google, además los miembros a tomar en cuenta en esta política son VPN_ISP_P, VPN_ISP_S y ISP-1.

Los túneles configurados desde el FW-ACCHA, son hacia el Site Principal mediante el túnel sede-to-site1, el cual se levanta sobre el enlace de internet y el túnel VPN_ISP_1, el cual se levanta sobre la red MPLS del proveedor ISP-2.

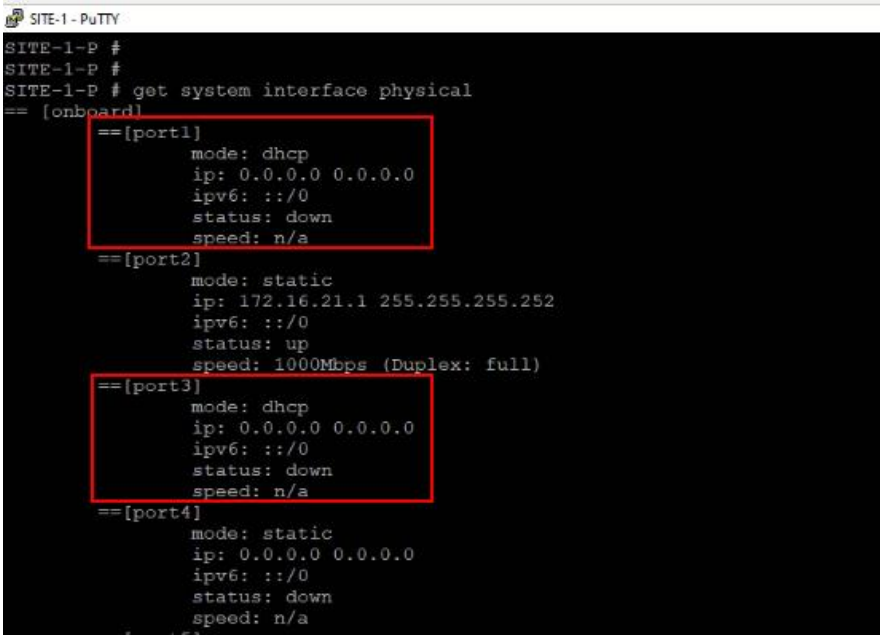
Figura 23:*IPsec monitor*



Nota: *El tráfico hacia los recursos de lima se realizan mediante el túnel VPN_ISP_P principalmente, siendo el túnel sede-to-site1 el enlace de contingencia, por ello solo se muestra tráfico bidireccional en VPN_ISP_P.*

Se realizó la prueba de simulación de caída de internet, para validar que los enlaces de contingencia funcionen correctamente.

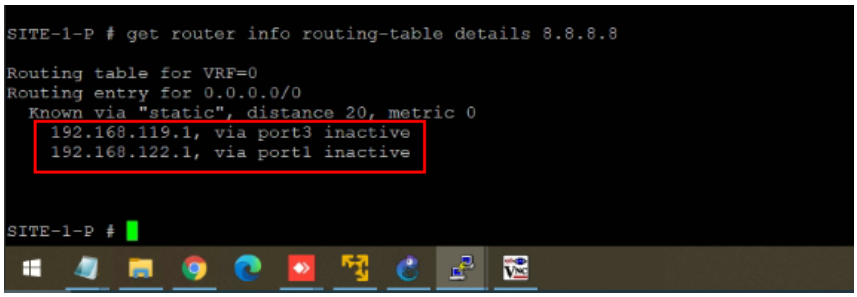
***Figura 24**:Caída de internet por SITE-1*



***Nota:** Las interfaces port1 y port3 de salida a internet directa desde el FW SITE-1-P, se encuentra en down.*

Debido a que actualmente los enlaces de salida a internet del Site principal se encuentra en down, las mediciones del performance SLA desde la agencia FW-ACCHA, deben seleccionar como enlaces para salida a internet, los enlaces de salida a internet directa y el enlace de salida a internet mediante el Site secundario

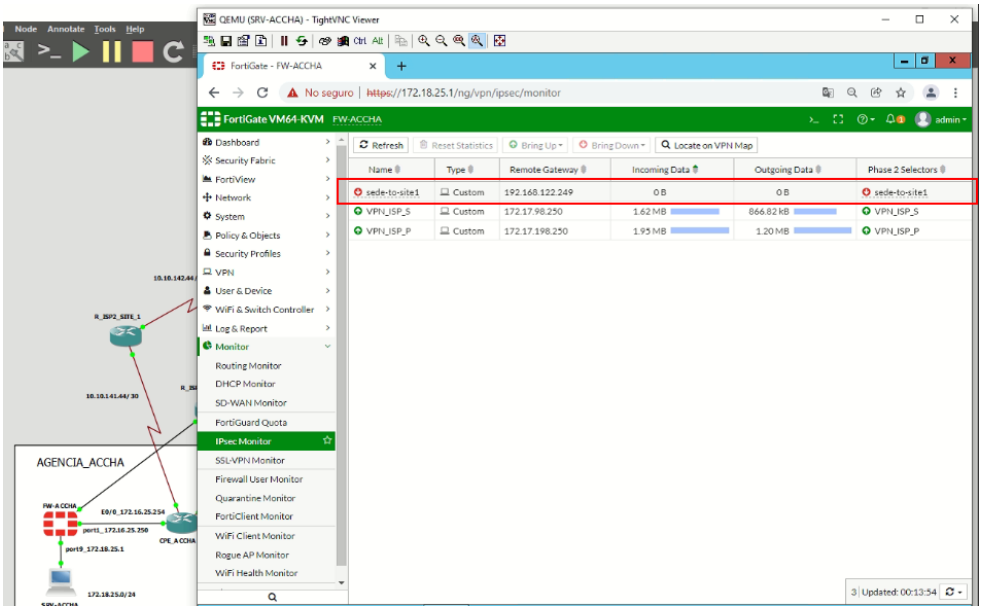
***Figura 25**: Interfaces de salida a internet ISP-1*



***Nota:** La ruta por defecto desde el FW SITE-1-P se encuentra inactiva, debido a que ambas interfaces de salida a internet se encuentran en down.*

El túnel VPN que se levanta por en enlace de internet desde el FW-ACCHA se debería encontrar en down, debido a que el Remote Gateway 192.168.122.249, el cual es la ip de la interface port1 del FW SITE-1-P se encuentra en down.

Figura 26: *VPN atravez la interface port3 de SITE-1*



Nota: *Los túneles que siguen activos luego de la caída a internet del Site principal, son el VPN_ISP_S y el VPN_ISP_P, debido a que ambos Remote Gateway se encuentran dentro de la red MPLS del proveedor ISP-2 de cara al FW-ACCHA.*

Figura 27: *Performance SLA por ISP-P*

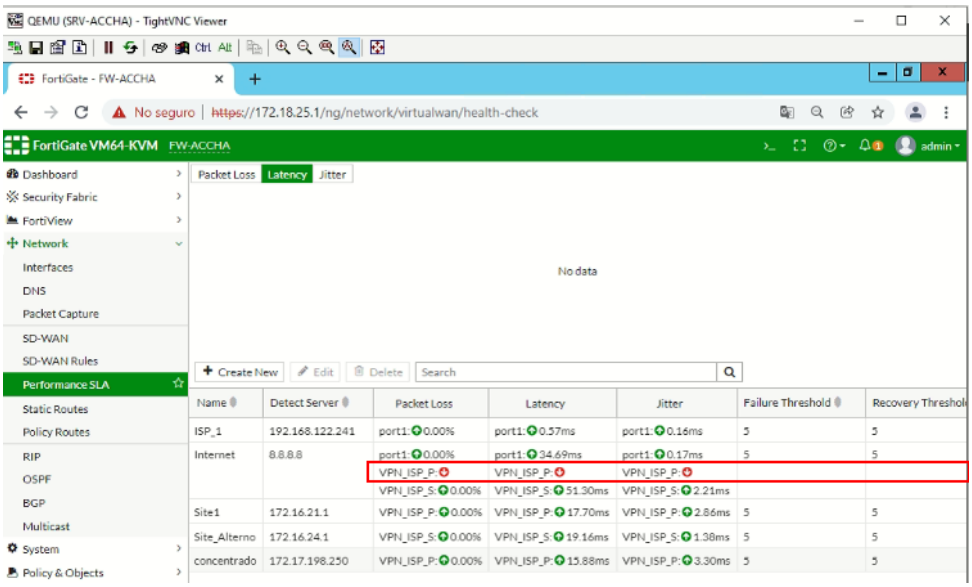


Figura 28: *Salida a internet ISP-1*

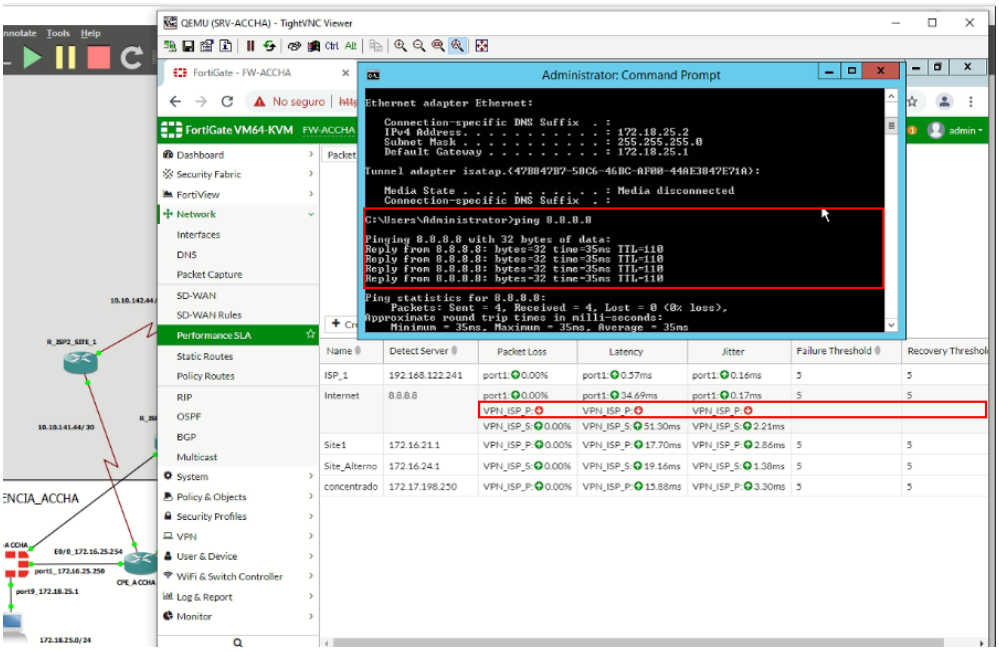


Figura 29: *Salida a internet desde site-1 mediante el port3*

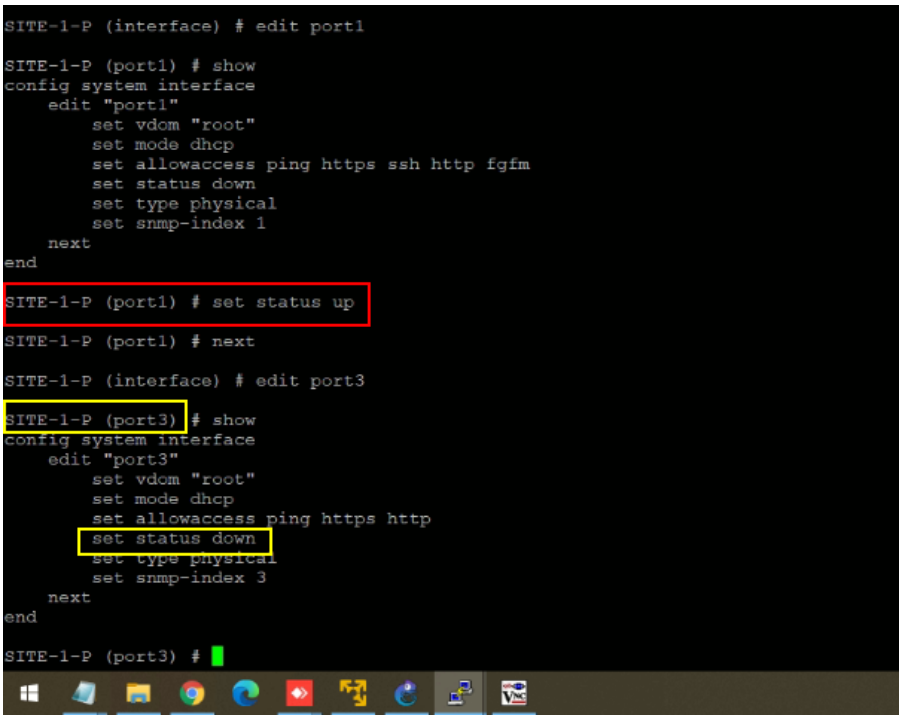
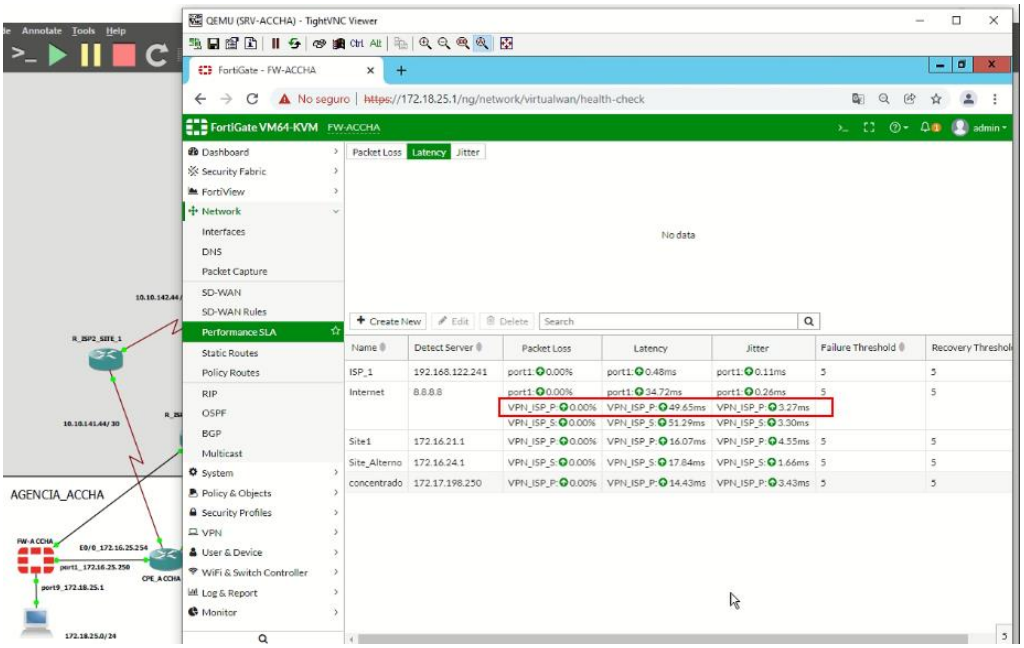


Figura 30: *Salida internet por Site-1*



caída red mpls proveedor ISP_2 solo internet ISP_1

Figura 31: *Caída de ISP-2 de Accha*

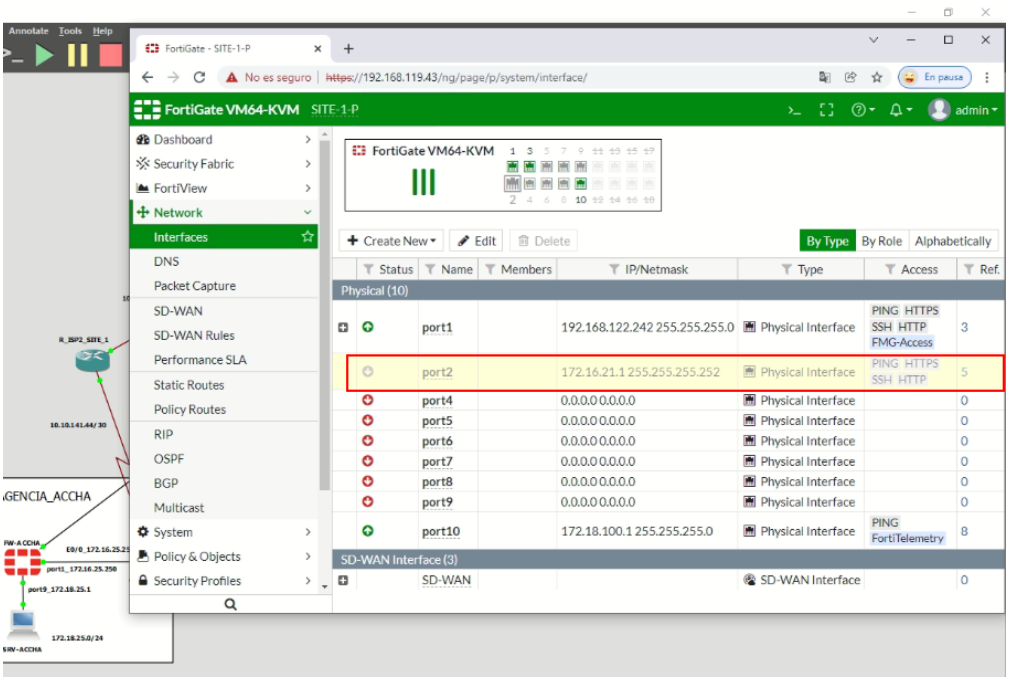


Figura 32: *Salida a internet mediante ISP-1*

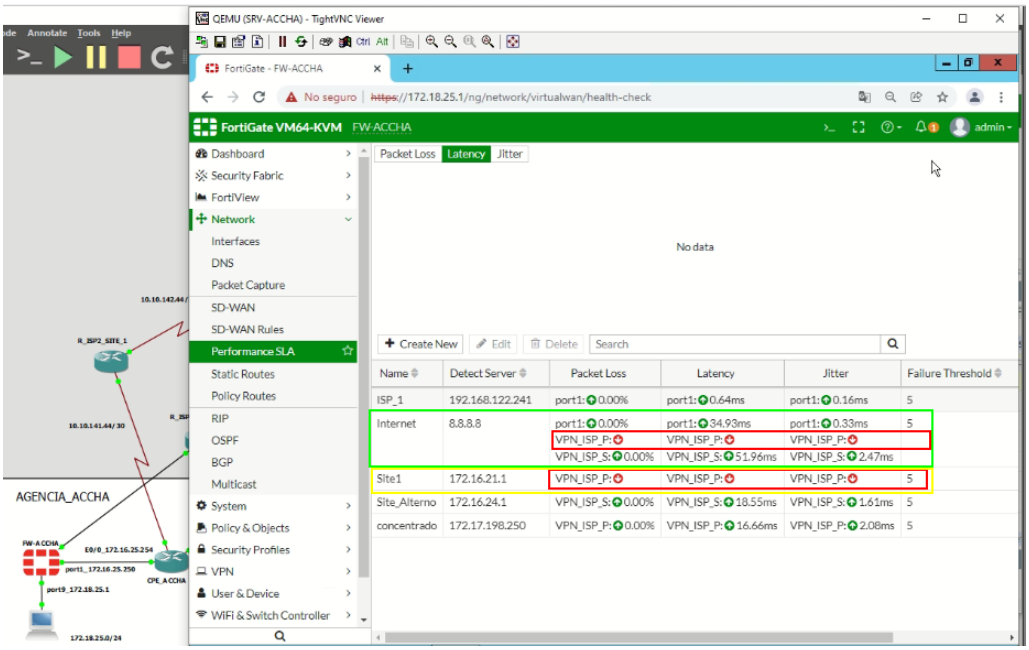


Figura 33: *Comunicación con servicios internet mediante VPN IPsec Dial-UP*

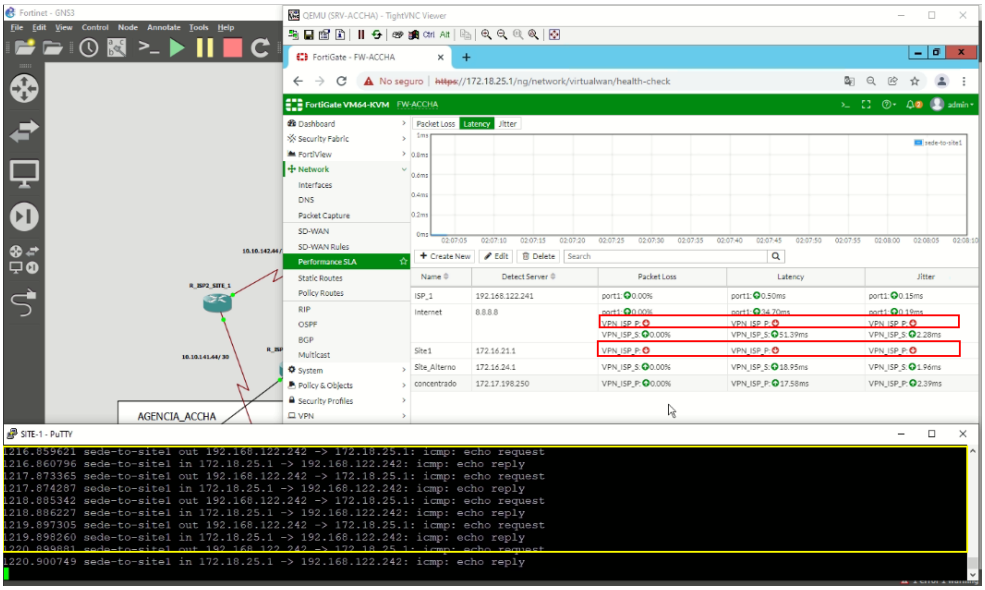


Figura 34: *Tráfico hacia el Site-1 desde Accha*

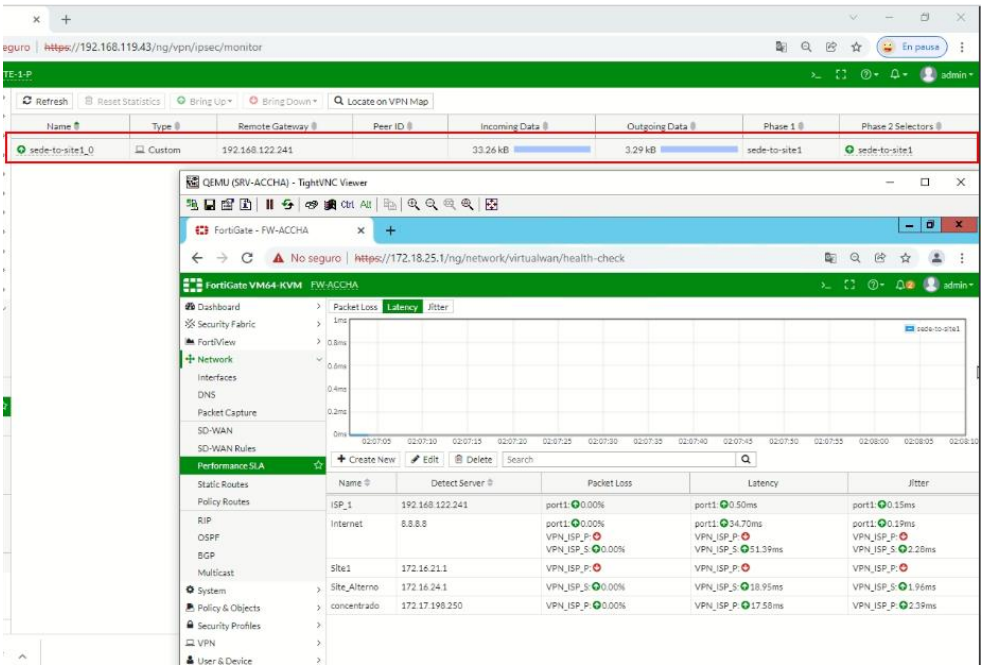


Figura 35: *Salida a internet desde sede Accha por ISP-1*

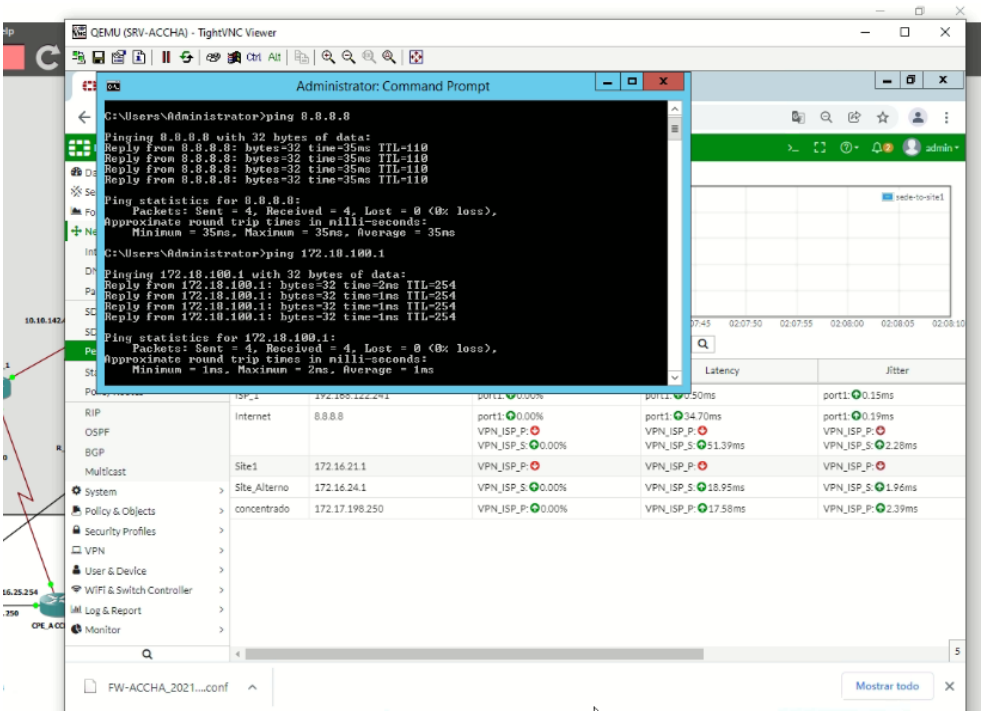


Figura 36: *Salida a internet desde Accha*

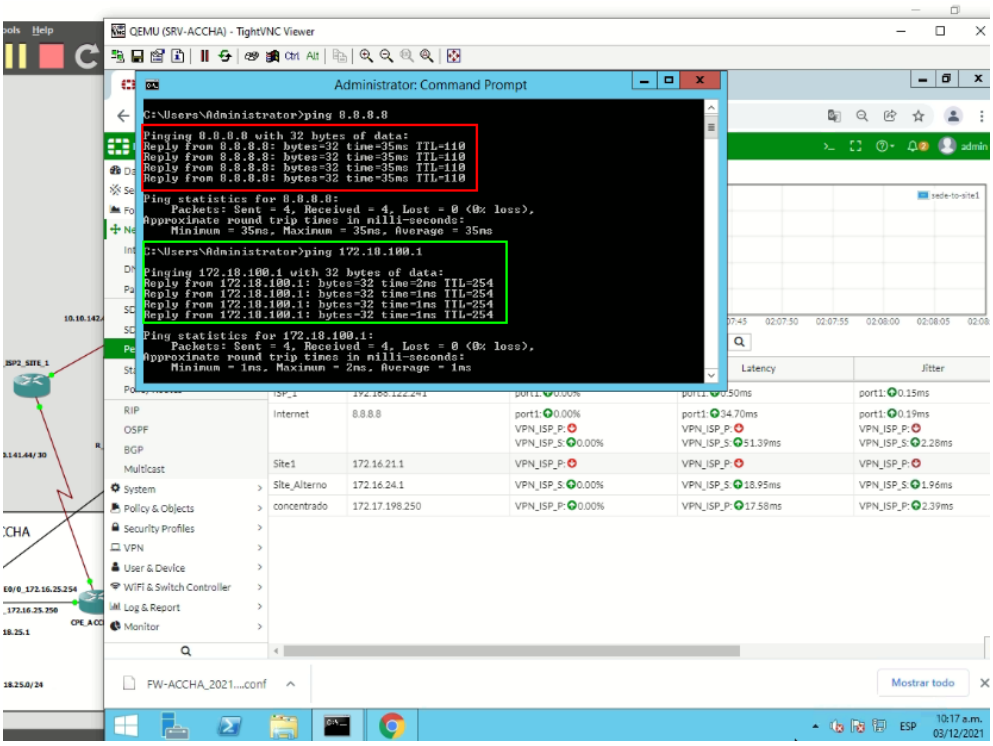
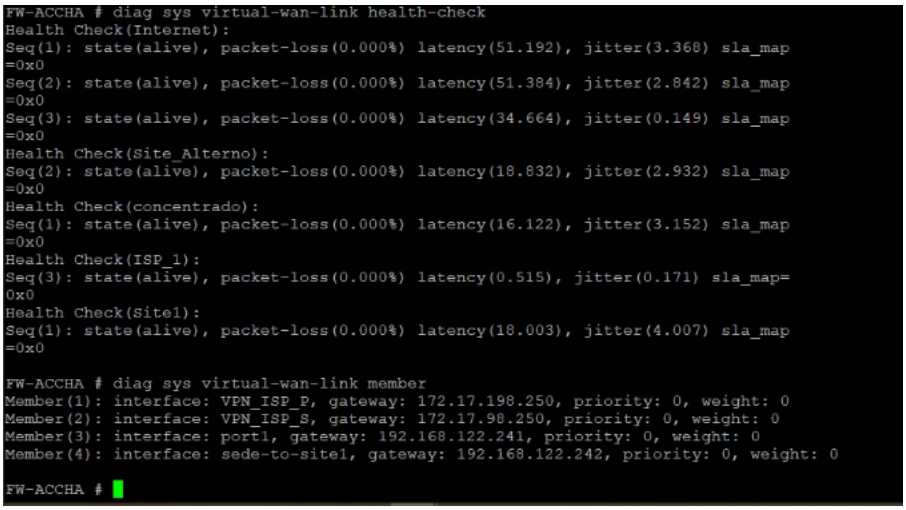
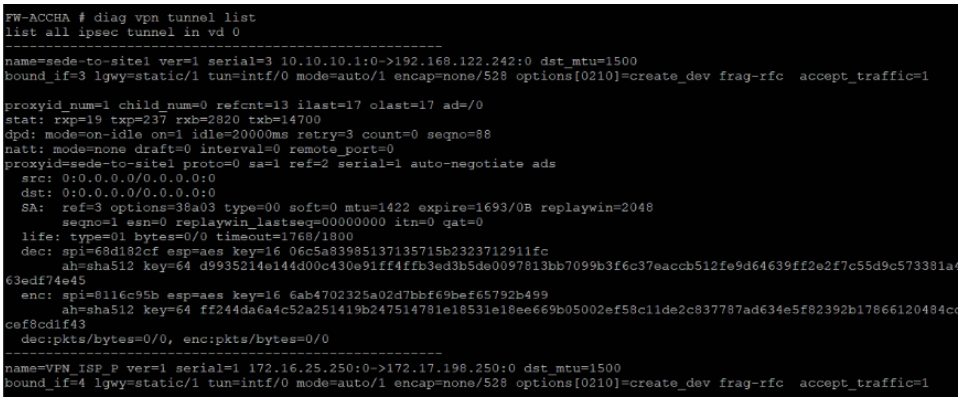


Figura 37: *Integrantes del SD-WAN*

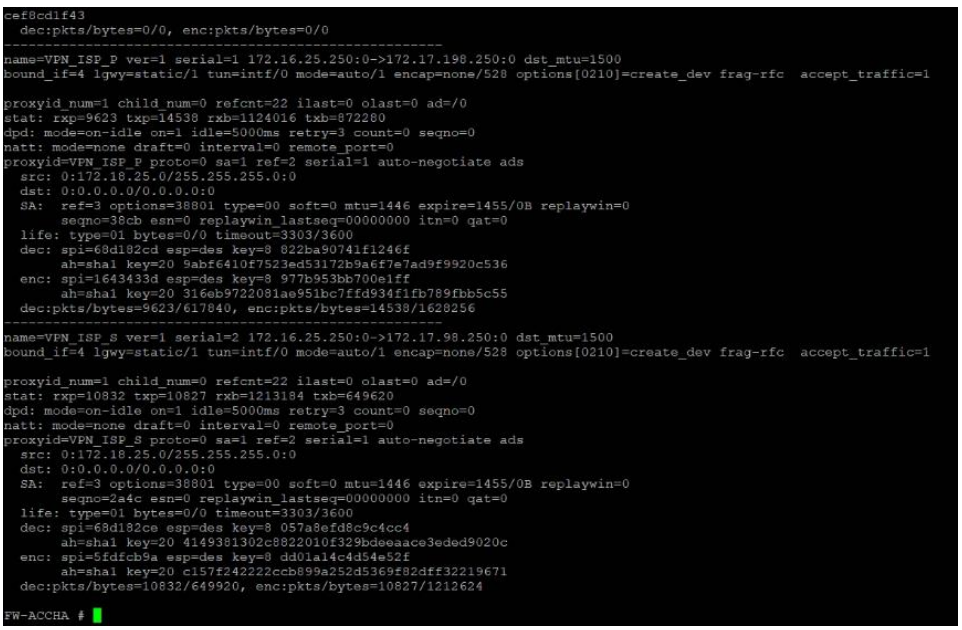


```
FW-ACCHA # diag sys virtual-wan-link health-check
Health Check(Internet):
Seq(1): state(alive), packet-loss(0.000%) latency(51.192), jitter(3.368) sla_map
=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(51.384), jitter(2.842) sla_map
=0x0
Seq(3): state(alive), packet-loss(0.000%) latency(34.664), jitter(0.149) sla_map
=0x0
Health Check(Site_Alterno):
Seq(2): state(alive), packet-loss(0.000%) latency(18.832), jitter(2.932) sla_map
=0x0
Health Check(concentrado):
Seq(1): state(alive), packet-loss(0.000%) latency(16.122), jitter(3.152) sla_map
=0x0
Health Check(ISP_1):
Seq(3): state(alive), packet-loss(0.000%) latency(0.515), jitter(0.171) sla_map=
0x0
Health Check(Site1):
Seq(1): state(alive), packet-loss(0.000%) latency(18.003), jitter(4.007) sla_map
=0x0

FW-ACCHA # diag sys virtual-wan-link member
Member(1): interface: VPN_ISP_P, gateway: 172.17.198.250, priority: 0, weight: 0
Member(2): interface: VPN_ISP_S, gateway: 172.17.98.250, priority: 0, weight: 0
Member(3): interface: port1, gateway: 192.168.122.241, priority: 0, weight: 0
Member(4): interface: sede-to-site1, gateway: 192.168.122.242, priority: 0, weight: 0

FW-ACCHA #
```

Figura 38: *VPN IPsec desde Accha*



```
FW-ACCHA # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=sede-to-site1 ver=1 serial=3 10.10.10.1:0->192.168.122.242:0 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-rfc  accept_traffic=1

proxyid_num=1 child_num=0 refcnt=13 ilast=17 olast=17 ad=/0
stat: rxp=19 txp=237 rxb=2820 txb=14700
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=88
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=sede-to-site1 proto=0 sa=1 ref=2 serial=1 auto-negotiate ads
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=38a03 type=00 soft=0 mtu=1422 expire=1693/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=1768/1800
  dec: spi=68d182cf esp=aes key=16 06c5a83985137135715b2323712911fc
       ah=sha512 key=64 d9935214e144d00c430e91ff4ffb3ed3b5de0097813bb7099b3f6c37eaccb512fe9d64639ff2e2f7c55d9c573381a6
63edf74e45
  enc: spi=8116c95b esp=aes key=16 6ab4702325a02d7bbf69bef65792b499
       ah=sha512 key=64 ff244da6a4c52a251419b247514781e18531e18ee669b05002ef58c11de2c837787ad634e5f82392b17866120484cc
cef8cd1f43
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
------------------------------------------------------
name=VPN_ISP_P ver=1 serial=1 172.16.25.250:0->172.17.198.250:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-rfc  accept_traffic=1
```



```
cef8cd1f43
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
------------------------------------------------------
name=VPN_ISP_P ver=1 serial=1 172.16.25.250:0->172.17.198.250:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-rfc  accept_traffic=1

proxyid_num=1 child_num=0 refcnt=22 ilast=0 olast=0 ad=/0
stat: rxp=9623 txp=14538 rxb=1124016 txb=872280
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN_ISP_P proto=0 sa=1 ref=2 serial=1 auto-negotiate ads
  src: 0:172.18.25.0/255.255.255.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=38801 type=00 soft=0 mtu=1446 expire=1455/0B replaywin=0
       seqno=38cb esn=0 replaywin_lastseq=00000000 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=3303/3600
  dec: spi=68d182cd esp=des key=8 822ba90741f1246f
       ah=sha1 key=20 9abf6410f7523ed53172b9a6f7e7ad9f9920c536
  enc: spi=1643433d esp=des key=8 977b953bb700e1ff
       ah=sha1 key=20 316eb9722081ae951bc7ffd934f1fb789fbb5c55
  dec:pkts/bytes=9623/617840, enc:pkts/bytes=14538/1628256
------------------------------------------------------
name=VPN_ISP_S ver=1 serial=2 172.16.25.250:0->172.17.98.250:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-rfc  accept_traffic=1

proxyid_num=1 child_num=0 refcnt=22 ilast=0 olast=0 ad=/0
stat: rxp=10832 txp=10827 rxb=1213184 txb=649620
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN_ISP_S proto=0 sa=1 ref=2 serial=1 auto-negotiate ads
  src: 0:172.18.25.0/255.255.255.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=38801 type=00 soft=0 mtu=1446 expire=1455/0B replaywin=0
       seqno=2a4c esn=0 replaywin_lastseq=00000000 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=3303/3600
  dec: spi=68d182ce esp=des key=8 057a8efd8c9c4cc4
       ah=sha1 key=20 4149381302c8822010f329bdeeaace3eded9020c
  enc: spi=5fdfcb9a esp=des key=8 dd01a14c4d54e52f
       ah=sha1 key=20 c157f242222ccb899a252d5369f82dff32219671
  dec:pkts/bytes=10832/649920, enc:pkts/bytes=10827/1212624

FW-ACCHA #
```

3.2.4 Desarrollo de la configuración

VPN IPsec

Se debe tomar en cuenta el mecanismo de cifrado empleado en el equipo hacia el cual se va a levantar el tunnel, debido a que se debe tener compatibilidad, ya sea por las especificaciones técnicas o por la antigüedad del equipo del otro site, por defecto en la versión 6.0.4, fortinet nos permite utilizar los mecanismos de cifrado para encriptación DES-3DES-AES128-AES192-AES256 y para autenticación MD5-SHA1-SHA256-SHA384-SHA512.

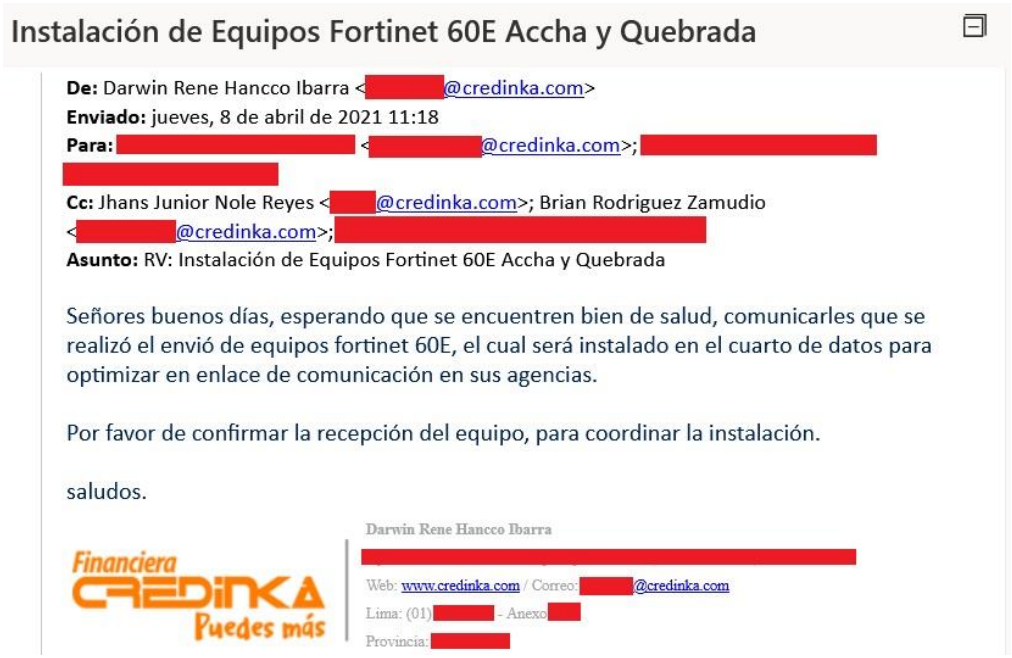
SD-WAN

Se debe definir los detect server en los performace SLA para poder mediar el rendimiento de los parámetros de packet loss, latency y Jitter, para la elección del mejor enlace al utilizar el sd-wan.

3.2.5 Implementación del equipamiento fortigate

Para la implementación de equipo fortigate en sede, previamente se realizó la configuración y posteriormente el envío a la agencia para realizar el conexionado del equipo con ayuda del personal de Credinka.

Figura 39: *Instalación Fortigate 60E Accha y Quebrada*



Instalación de Equipos Fortinet 60E Accha y Quebrada

De: Darwin Rene Hancco Ibarra <[redacted]@credinka.com>
Enviado: jueves, 8 de abril de 2021 11:18
Para: [redacted] <[redacted]@credinka.com>; [redacted]
Cc: Jhans Junior Nole Reyes <[redacted]@credinka.com>; Brian Rodriguez Zamudio <[redacted]@credinka.com>; [redacted]
Asunto: RV: Instalación de Equipos Fortinet 60E Accha y Quebrada

Señores buenos días, esperando que se encuentren bien de salud, comunicarles que se realizó el envió de equipos fortinet 60E, el cual será instalado en el cuarto de datos para optimizar en enlace de comunicación en sus agencias.

Por favor de confirmar la recepción del equipo, para coordinar la instalación.

saludos.

Financiera CREDINKA Puedes más

Darwin Rene Hancco Ibarra
[redacted]
Web: www.credinka.com / Correo: [redacted]@credinka.com
Lima: (01) [redacted] - Anexo [redacted]
Provincia: [redacted]

Nota: *La instalación del FW Fortigate 60E se realizó con apoyo de personal de Credinka.*

Figura 40: *Configuración básica empleada*

CREDINKA || CHECKLIST DE ATENCIONES

M mariela.mamani@smartglobal.pe
To 'nsoc'
Cc 'Jeanpierre Soto'; 'mariela.mamani@smartglobal.pe'

Reply | Reply All | Forward | ...
viernes 16/04/2021 18:55

SEDE_ACCHA_20210416_1830.conf
162 KB

Se envía el checklist de los requerimientos del cliente Credinka del 16/04/2021.

REQUERIMIENTO 1: Implementación FW sede Accha
Se adjunta el archivo de configuración.
Equipo configurado: FW SEDE_ACCHA

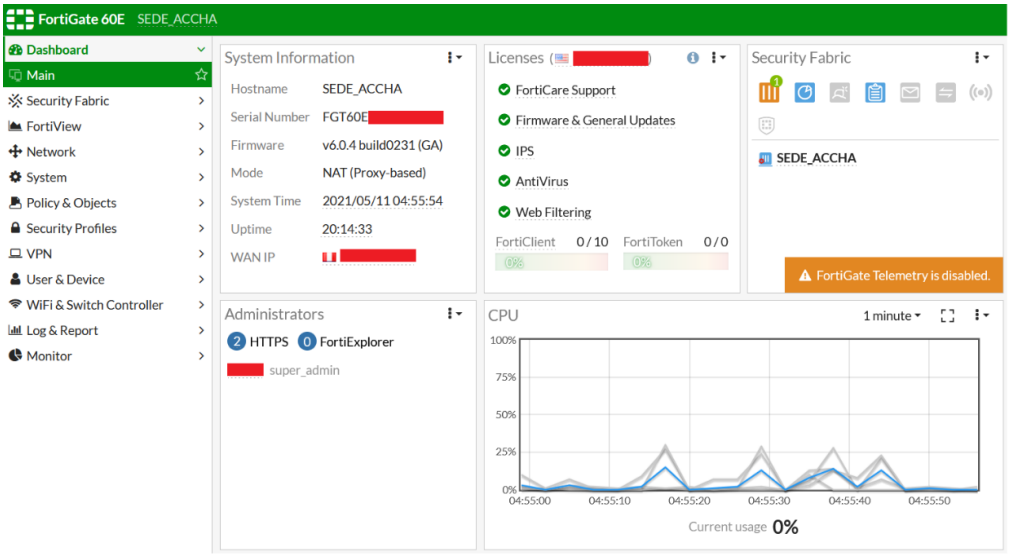
Saludos cordiales

Mariela Mamani
Ingeniero Onsite Credinka
Cel: +51 954386249
Correo: mariela.mamani@smartglobal.pe

Nota: *Envío del archivo de configuración del FW Fortigate 60E luego de la implementación.*

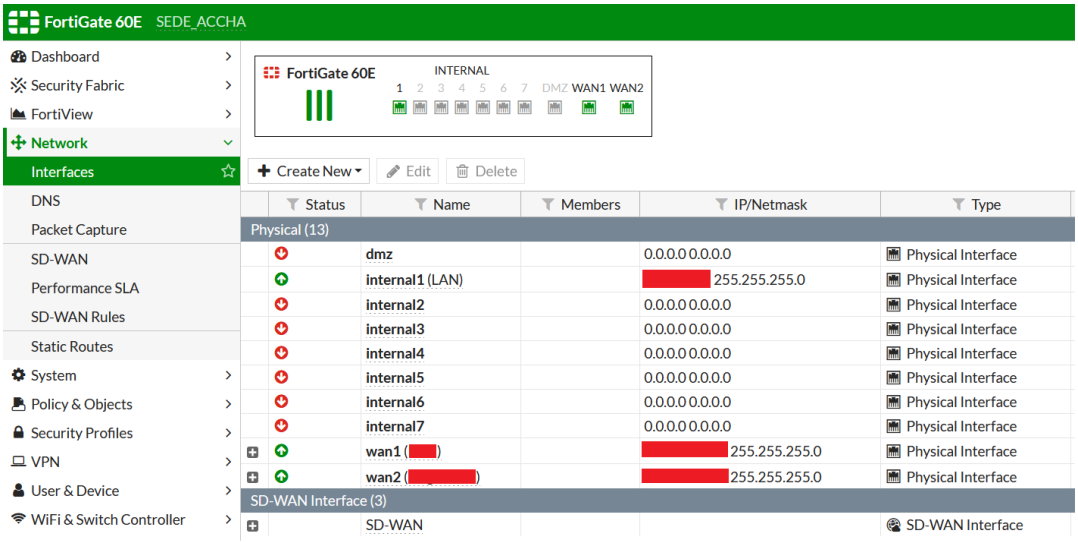
Se visualiza que el equipo se instaló correctamente en la agencia, se valida el tiempo de operatividad.

Figura 41: *Forigate 60E Agencia Accha*



Nota: *Se visualiza que el tiempo de operatividad es de 20:14:33 hrs, además se visualiza que el equipo cuenta con las licencias FortiCare support, Firmware & Generate Updates, IPS, Antivirus y Web Filtering.*

Figura 42: *Operatividad de puertos Fortigate 60E*



Nota: *Se visualiza que los puertos en que están activos tanto lógica como físicamente, son los Internal1, el cual está conectado directamente al Switch de acceso de Agencia, wan1 que es conectado al router del ISP-1 y wan2 que va conectador al router del ISP-2.*

3.3 Resultados

3.3.1 Integración del equipamiento

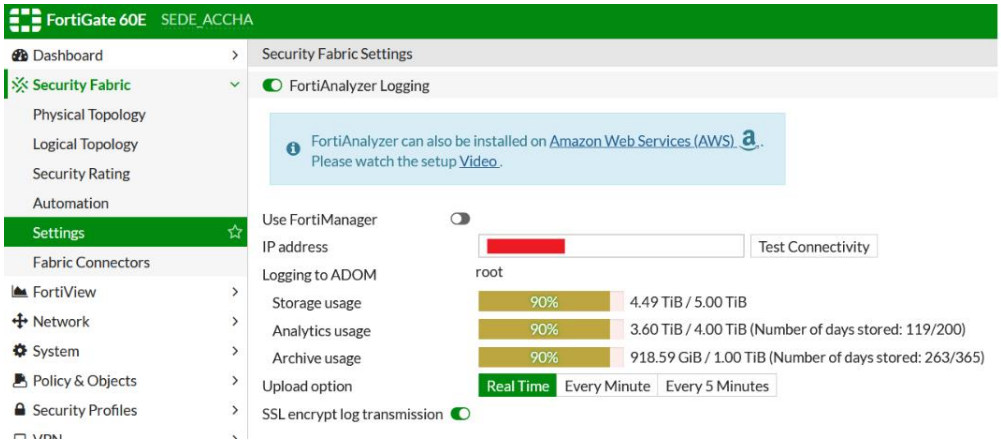
Luego de la implementación del equipo Fortigate 60E, se muestra en el dashboard del Fortianalyzer la sincronización hacia el Fortigate SEDE_ACCHA, para la recolección de logs del equipo.

Figura 43: *Gestión de equipos de FortiAnalyzer*

Nota: *El Fortigate 60E instalado en la agencia, con el hostname SEDE_ACCHA se encuentra sincronizado, para utilizar las herramientas de monitoreo y la generación de reportes.*

Desde el Fortigate SEDE_ACCHA se debe tener en cuenta el tiempo de sincronización de logs hacia el fortianalyzer, en este caso se configuro en tiempo real, para realizar un troubleshooting y obtener más información del tráfico a través del firewall.

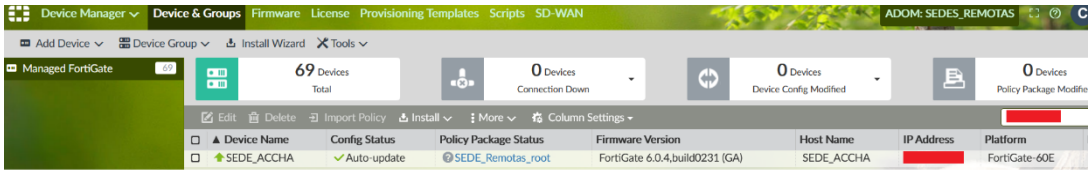
Figura 44: Sincronización Forigate 60E con FAZ



Nota: *Se visualiza la sincronización desde el Fortigate hacia el Fortianalyzer.*

La integración desde el FortiManager, se emplea para la gestión centralizada de todas las soluciones de Fortinet, en este caso se asocia el firewall Fortigate 60E de la agencia Accha.

Figura 45: *Gestión de equipos de FortiManager*



Nota: *El Fortigate 60E instalado en la agencia, con el hostname SEDE_ACCHA se encuentra sincronizado, para poder utilizar las herramientas de configuración desde el FortiManager.*

3.3.2 Encriptación de los datos

El tipo de encriptación de los datos que van desde la interfaz virtual VPN_Bitel es des-sha1, tanto para encriptar como desencriptar la información.

Figura 46: *Detalle de tunel Ipsec VPN_Bitel*

```
name=VPN_Bitel ver=1 serial=1 10.12.25.250:0->10.10.198.250:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=34 ilast=0 olast=0 ad=/0
stat: rxp=4790273 txp=6566606 rxb=1714933710 txb=1427928235
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=23
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN_Bitel proto=0 sa=1 ref=43 serial=1 auto-negotiate ads
  src: 0:10.10.25.0/255.255.255.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=6 options=18825 type=00 soft=0 mtu=1446 expire=683/0B replaywin=0
       seqno=649d esn=0 replaywin_lastseq=00000000 itn=0
  life: type=01 bytes=0/0 timeout=3298/3600
  dec: spi=2d5a2a32 esp=des key=8 a522ba92c71534d2
       ah=sha1 key=20 438fc215bd25d030b1233c938048f4865f47c235
  enc: spi=1d651a71 esp=des key=8 5650164d36ca991b
       ah=sha1 key=20 a894ad5f318e6f8f7cfb77c3e8e5f0ef6f54a827
  dec:pkts/bytes=26624/3686378, enc:pkts/bytes=44323/6120763
  npu_flag=03 npu_rgwy=10.10.198.250 npu_lgwy=10.12.25.250 npu_selid=1 dec_npuid=1 enc_npuid=1
```

Se visualiza que los tuneles VPN_Bitel y VPN_Bitel_Cusco, se encuentran establecidos, con mecanismo empleado para el cifrado de datos de DES y para la autenticación entre los túneles hacia el Site-1 de sha1.

Figura 47: *Estado de VPN_Bitel*

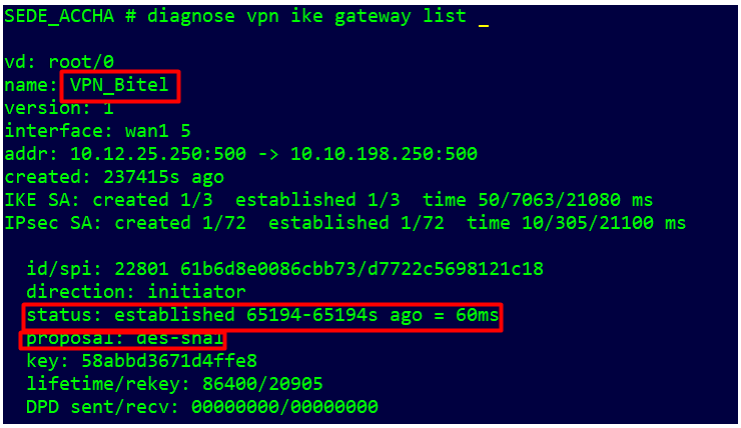
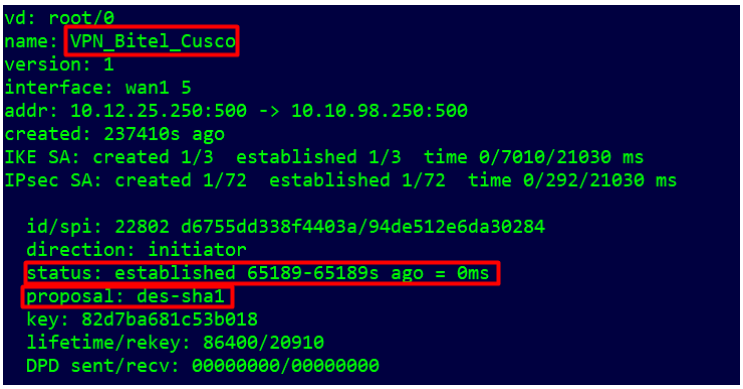


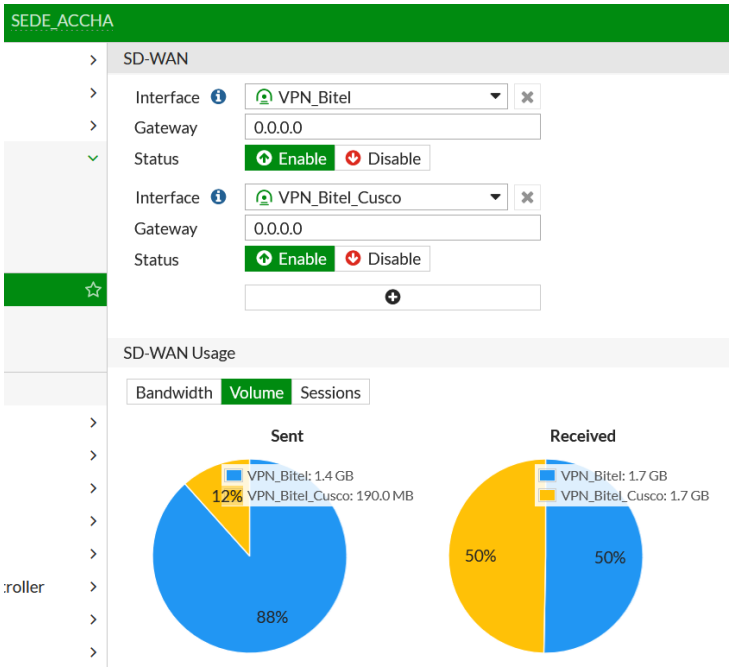
Figura 48: *Estado de VPN_Bitel_Cusco*



3.3.3 Balanceo del tráfico SD-WAN

Las interfaces miembros del SD-WAN, son las interfaces virtuales VPN_Bitel, la cual es el túnel ipsec desde el FW-ACCHA hacia el Site-1 y VPN_Bitel_Cusco, que es el túnel desde FW-ACCHA hacia el Site-2.

Figura 49: *Estado de SD-WAN Accha*



Nota: El porcentaje de tráfico de salida tiene un porcentaje del 12% por el enlace VPN_Bitel_Cusco y un porcentaje de uso de 88% por el enlace VPN_Bitel; en el caso de tráfico entrante, se tiene una proporción de 50% tanto por VPN_Bitel y VPN_Bitel_Cusco.

La detección para la elección del enlace prioritario está basada en la detección del performance hacia el dns de Google 8.8.8.8.

Figura 50: *Performace SLA hacia DNS-google*

Detect Server	Packet Loss	Latency	Jitter
8.8.8.8	VPN_Bitel: 0.00 % VPN_Bitel_Cusco: 0.00 %	VPN_Bitel: 81.92 ms VPN_Bitel_Cusco: 51.80 ms	VPN_Bitel: 0.10 ms VPN_Bitel_Cusco: 1.97 ms

Nota: Se visualiza que las interfaces miembros del SD-WAN son VPN_Bitel con id 2 y VPN_Bitel_Cusco con id 5:

Figura 51: *Estado de Miembros SD-WAN Accha*

```
SEDE ACCHA # diag sys virtual-wan-link member
Member(2): interface: VPN_Bitel, gateway: 10.10.198.250, priority: 0, weight: 50
  Config volume ratio: 50, last reading: 3150000000B, volume room 50MB
Member(5): interface: VPN_Bitel_Cusco, gateway: 10.10.98.250, priority: 0, weight: 0
  Config volume ratio: 0, last reading: 1878000000B, overload volume 1878MB
```

Nota: Se muestra que las mediciones del performance del SD-WAN no difieren en un valor de 10, para la elección de ruta por packet-loss o jitter.

Figura 52: *Performance de enlace SD-WAN Accha*

```
SEDE ACCHA # diagnose sys virtual-wan-link health-check
Health Check(Claro_Internet):
Seq(2): state(alive), packet-loss(0.000%) latency(81.906), jitter(0.091) sla_map=0x0
Seq(5): state(alive), packet-loss(0.000%) latency(50.409), jitter(0.311) sla_map=0x0
Health Check(FGT_1500_BITEL):
Seq(2): state(alive), packet-loss(0.000%) latency(19.386), jitter(0.066) sla_map=0x0
Health Check(VPN_CUSCO):
Seq(5): state(alive), packet-loss(0.000%) latency(2.400), jitter(0.061) sla_map=0x0
Health Check(VPN_LIMA):
Seq(2): state(alive), packet-loss(0.000%) latency(19.328), jitter(0.059) sla_map=0x0
```

Nota: Se visualiza que la salida a internet se encuentra en el Service (6), siendo la salida para la ruta por defecto (0.0.0.0 255.255.255.255), con el criterio de elección de jitter, con una diferencia de este parámetro de 10 para la elección de uno prioritario.

Figura 53: *Parámetros de SLA Internet desde Accha*

```
Service(3): Address Mode(IPV4) flags=0x0
  TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(jitter),
  link-cost-threshold(10), health-check(Claro_Internet)
  Members:
    1: Seq_num(2), alive, jitter: 0.141, selected
  Src address: 0.0.0.0-255.255.255.255
  Dst address: 0.0.0.0-255.255.255.255
```

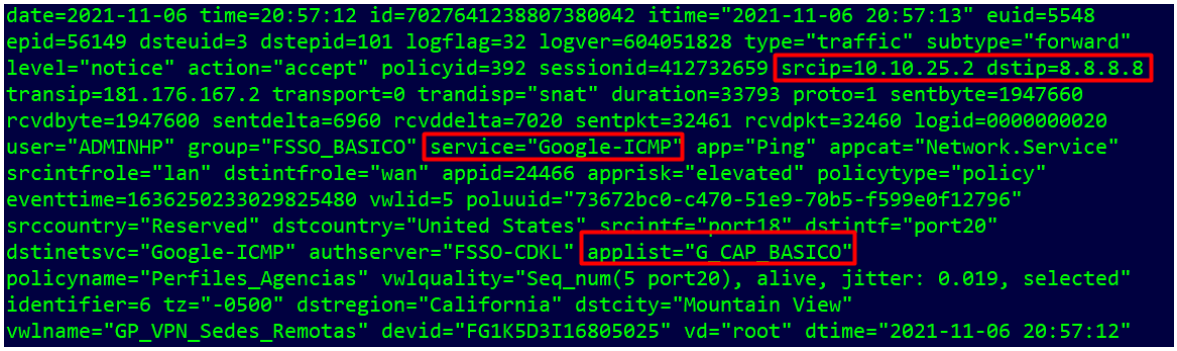
Como los valores de jitter son de 0.091 y 0.311, la diferencia no es igual a 10, según lo definido en el parámetro link-cost-threshold(10), por lo que se realizara el balanceo de tráfico entre ambas interfaces para

salida a internet, la definición de la elección de los enlaces se realiza sondeando el servidor de Google 8.8.8.8 en tiempo real.

3.3.4 Control UTM

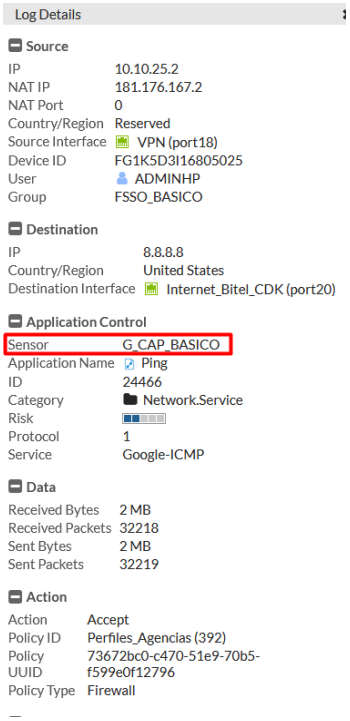
Se realizó la captura del tráfico generado por el equipo 10.10.25.2, se visualiza que el tráfico realiza el filtrado de cometido utilizado el perfil de App Control G_CAP_BASICO

Figura 54: *Debug de salida a internet desde Site-1*



En este caso la IP 10.10.25.2 está realizando una consulta hacia el dns de Google 8.8.8.8, donde recae en la política Perfiles_Agencias (392), al realizar el análisis del tráfico por el Application control, que es parte del filtrado UTM, se visualiza que la consulta recae en la categoría Network.Service la cual está permitida, por lo que se deja pasar el tráfico y se observa que se tiene una recepción de 2MB y envío de 2MB.

Figura 55: *Detalle de perfíl UTM para salida a internet por SITE-1*



Nota: La política configurada para navegación es la 392, de salida a internet por el Site-1. Se muestra tráfico bidireccional hacia el dns de google, siendo la acción permit, debido a que esta permitida la categoria Network Service, dentro del perfil G_CAP_BASICO.

CONCLUSIONES

- Se logro implementar el sd-wan para la agencia SEDE_ACCHA, utilizando el criterio de jitter para el balanceo de carga automático, con un valor de diferencia entre los miembros del sd-wan de 10, para la elección del enlace prioritario.

- Los túneles VPN_Bitel y VPN_Bitel_Cusco, fueron implementados y se observa que los datos transportados utilizan el mecanismo des-sha1 para encriptar y desencriptar la información, los túneles son del tipo dial-up, lo que permite que se puedan conectar diversas agencias hacia el Site principal y secundario.

- El control de tráfico mediante filtrado UTM, se realiza con una política para salida a internet directa desde la agencia y además también se tiene implementadas políticas para salida a internet desde los equipos de seguridad principales FW SITE-1 y FW SITE-2.

RECOMENDACIONES

- Se debe tener en cuenta el mecanismo de cifrado empleado, debido a que la compatibilidad con el equipo hacia el cual se va a levantar el tunnel IPsec, en este caso se definió des-sha1, sin embargo, se solicita emplear un cifrado más robusto.

- La versión empleada es la FortiOs 6.0.4, debido a la compatibilidad con los demás equipos como Fortimanager y FortiAnalyzer, sin embargo, se solicita poder realizar la actualización hacia una versión posterior a la 6.4, con la finalidad de poder utilizar más características del sd-wan y no tener la limitante de solo configurar uno por equipo.

- Se recomienda utilizar equipos Fortigate KVM con licencia sobre GNS3, para poder realizar una simulación más real de la infraestructura de red.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, L. E. (2020). *Propuesta de Diseño de una Red Privada de Telecomunicaciones para Accesos a Aplicaciones de una Entidad Bancaria a través de Internet.* Lima: UNIVERSIDAD TECNOLÓGICA DEL PERÚ.

Ayapata, D. O. (2020). *Modelado de una WAN utilizando redes definidas por software de alta disponibilidad en el segmento corporativo.* Guayaquil: UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL.

Fortinet. (3 de April de 2019). *Fortinet Secure SD-WAN Reference Architecture.* Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf?utm_source=social&utm_medium=twitter-org&utm_campaign=sprinklr

Fortinet. (20 de July de 2019). *FortiOS- ParallelPath Processing.* Obtenido de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee15d53-a99c-11e9-81a4-00505692583a/FortiOS-6.0-Parallel_Path_Processing_%28Life_of_a_Packet%29.pdf

Fortinet. (2020). *Docs Fortinet Cookbook.* Obtenido de https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/184590/dialup-vpn

Fortinet. (2020). *Fortinet Products*. Obtenido de https://www.fortinet.com/lat/products/sd-wan

Fortinet. (2020). *Fortinet Products*. Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall

Fortinet. (2020). *Fortinet Resources Cyberglossary.* Obtenido de https://www.fortinet.com/resources/cyberglossary/what-is-packet-loss

Fortinet. (2020). *Fortinet Resources Cyberglossary.* Obtenido de https://www.fortinet.com/resources/cyberglossary/unified-threat-management

Fortinet. (17 de June de 2020). *FortiOS 6.0 Handbook.* Obtenido de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf

Fortinet. (2021). *Fortinet Resources Cyberglossary*. Obtenido de https://www.fortinet.com/resources/cyberglossary/latency

GNS3. (2021). *GN3 Documentation.* Obtenido de https://docs.gns3.com/docs/

IETF. (octubre de 2016). *Terminology for Benchmarking Network-layer Traffic Control Mechanisms*. Obtenido de https://datatracker.ietf.org/doc/html/rfc4689#section-3.2.5

Kreutz, D., Ramos, F., Veríssimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *IEEE*, 14-76.

López Arévalo, J. J. (2020). *EMULACIÓN DE UNA RED SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA FORTINET Y EL SOFTWARE GNS3.* Quito. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/21163/1/CD%2010688.pdf

Mora Huiracocha, R., Gallegos Segovia, P., Vintimilla Tapia, P., Bravo Torres, J., Cedillo Elias, J., & Larios Rosillo, V. (2019). *Implementation of a SD-WAN for the interconnection of two software defined data centers.* Barranquilla: IEEE.

Munayco Coronado, R. W. (2020). *Diseño de redes LAN basada en software para un proveedor de Datacenter líder en Perú.* Lima: Universidad Peruana de Ciencias Aplicadas (UPC).

Orosco Pahuara, B. B. (2018). *IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS*

ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL. Andhuaylas: UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS.

Rodríguez Guerrero, E. (2020). *Diseño y simulación de una red definida por software para la implementación de un laboratorio avanzado de datos para la EP de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos.* Lima: Universidad Nacional Mayor de San Marcos.

Romero Valdivieso, E. R., & Cuenca Tapia, J. P. (2020). Implementación de SD-WAN Corporativo para el uso eficiente de las telecomunicaciones para el Holding Quito Motors. *Pol. Con. (Edición núm.51) Vol. 5, Especial No 1*, 163-179.

Segeč, P., Moravčík, M., Uramová, J., Papán, J., & Yeremenko, O. (2020). SD-WAN – architecture, functions and benefits. *18th International Conference on Emerging eLearning Technologies and Applications (ICETA).* London: IEEE.

R. E. Mora-Huiracocha, P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, E. J. Cedillo-Elias and V. M. Larios-Rosillo, "Implementation of a SD-WAN for the interconnection of two software defined data centers," *2019 IEEE Colombian Conference on Communications and Computing (COLCOM)*, 2019, pp. 1-6, doi: 10.1109/ColComCon.2019.8809153.

ANEXOS

ANEXO 1. CONFIGURACIÓN TÚNEL VPN AGENCIA FW-ACCHA PHASE-1

```
config vpn ipsec phase1-interface
    edit "VPN_ISP_P"
        set interface "port2"
        set keylife 1800
        set peertype any
        set net-device enable
        set proposal des-sha1
        set localid "sucursal"
        set dpd on-idle
        set dhgrp 2
        set auto-discovery-sender enable
        set nattraversal disable
        set remote-gw 172.17.198.250
        set psksecret ENC
        eYT3ipSMCvozvozhay2VUYAyRPh7Rrh58XYU/PkzovCM3V1Mgfh0mkt01bn0M82
        TSjjyHxQBWgNnygwkUf7PPwESzyZRIC3kNYnYtqAx0l/QQziBduJePijXN+a+HF
        J84xmwiDkmsXEQvkia7yr7EcZVLf343r8scrZpm8H5/g4E6Q8XY6hgeon0sEGfe
        +L6L237gw==
        set dpd-retryinterval 5
    next
    edit "VPN_ISP_S"
        set interface "port2"
        set keylife 1800
        set peertype any
        set net-device enable
        set proposal des-sha1
        set localid "sucursal"
        set dpd on-idle
        set dhgrp 2
        set auto-discovery-sender enable
        set nattraversal disable
        set remote-gw 172.17.98.250
        set psksecret ENC
        KsmYLMN2yCSUBTnJP6Py6aZMvP1cwKHDO3N5FFHPQdgF1PCzaD4wcYKF5K+cahW
        NiKQkDpw1+0bdY5Ye9bhiyvi4MMS79he0D4Y2lWzEZezREZlNQuBWuQh9DMQ89G
        bKaffDmVZ+vRtRm+eLU11GQdmmls9I5F/N/j5/HERgy3ABOPgqn2kHGrPnEoYFr
        b8IcsUYSg==
        set dpd-retryinterval 5
    next
    edit "sede-to-site1"
        set interface "port1"
        set keylife 1800
        set peertype any
        set net-device enable
        set proposal aes128-sha512
        set localid "agencia"
        set dpd on-idle
        set dhgrp 2
        set auto-discovery-sender enable
        set nattraversal disable
        set remote-gw 192.168.122.242
        set psksecret ENC
        FXxP5oBmZk4lFUusdwGbtUDHJghpmaCBCXMNSXmaDc5W5fkVU8ROMfKdx1CsjmE
        vs8xXMQse2ARoN7HHRjJzXmaR6DPedxLH5WkLW/HpebGh3pMYJwVvbF6f8G9yF2
        DkRpyQBMxZTr/9bHEmBhnBm/+DrOKztCpZvF9CeDv+5YOMNileoZ1D/eQc1gdpQ
        N7CoT+YJQ==
    next
end
```

ANEXO 2. CONFIGURACIÓN TÚNEL VPN AGENCIA FW-ACCHA PHASE-2

```
config vpn ipsec phase2-interface
    edit "VPN_ISP_P"
        set phase1name "VPN_ISP_P"
        set proposal des-sha1
        set pfs disable
        set replay disable
        set auto-negotiate enable
        set keylifeseconds 3600
        set src-subnet 172.18.25.0 255.255.255.0
    next
    edit "VPN_ISP_S"
        set phase1name "VPN_ISP_S"
        set proposal des-sha1
        set pfs disable
        set replay disable
        set auto-negotiate enable
        set keylifeseconds 3600
        set src-subnet 172.18.25.0 255.255.255.0
    next
    edit "sede-to-site1"
        set phase1name "sede-to-site1"
        set proposal aes128-sha512
        set dhgrp 2
        set auto-negotiate enable
        set keylifeseconds 1800
    next
end
```

ANEXO 3. CONFIGURACIÓN DE MIEMBROS SD-WAN FW-ACCHA

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "VPN_ISP_P"
            set source 172.18.25.1
        next
        edit 2
            set interface "VPN_ISP_S"
            set source 172.18.25.1
        next
        edit 3
            set interface "port1"
            set gateway 192.168.122.241
        next
        edit 4
            set interface "sede-to-site1"
        next
    end
```

ANEXO 4. CONFIGURACIÓN PERFORMANCE SLA POR SONDEO DE SERVER FW-ACCHA

```
config system virtual-wan-link
    config health-check
        edit "Internet"
            set server "8.8.8.8"
            set members 1 2 3
        next
        edit "Site_Alterno"
            set server "172.16.24.1"
            set members 2
        next
        edit "concentrado"
            set server "172.17.198.250"
            set members 1
        next
        edit "ISP_1"
            set server "192.168.122.241"
            set members 3
        next
        edit "Site1"
            set server "172.16.21.1"
            set members 1
        next
    end
```

ANEXO 5. CONFIGURACIÓN DE REGLAS SD-WAN FW-ACCHA

```
config system virtual-wan-link
    config service
        edit 2
            set name "site1"
            set member 4
            set dst "Site1_172.18.100.0"
            set src "172.18.25.0/24"
        next
        edit 3
            set name "Site_1"
            set mode priority
            set dst "Site1_172.18.100.0"
            set src "172.18.25.0/24"
            set health-check "Site1"
            set priority-members 1
        next
        edit 4
            set name "Site_2"
            set mode priority
            set dst "Site2_172.18.200.0"
            set src "172.18.25.0/24"
            set health-check "Site_Alterno"
            set priority-members 2
        next
        edit 1
            set name "internet"
            set mode priority
            set dst "all"
            set src "172.18.25.0/24"
            set health-check "Internet"
            set priority-members 1 2 3
        next
    end
```