PROPUESTA PARA EL USO DE SD-WAN EN LA RED CORPORATIVA EMTELCO CX & BPO SEDE BOGOTÁ

EDWARD STIVEN RUBIANO AGUILAR

MONOGRAFÍA DE PRÁCTICAS PARA OPTAR POR EL TITULO
DE INGENIERO DE TELECOMUNICACIONES

JOHN ALEXANDER CARDOZO RAMÍREZ
DIRECTOR

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2021

PROPUESTA PARA EL USO DE SD-WAN EN LA RED CORPORATIVA EMTELCO CX & BPO SEDE BOGOTÁ

EDWARD STIVEN RUBIANO AGUILAR

MONOGRAFÍA DE PRÁCTICAS PARA OPTAR POR EL TITULO
DE INGENIERO DE TELECOMUNICACIONES

JOHN ALEXANDER CARDOZO RAMÍREZ
DIRECTOR

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2021

Tabla de contenido

Tabla de Figuras

Introducción

Los servicios en la nube han ido ganando popularidad entre las compañías que hacen uso de centros de datos. Esto debido a que permiten mejoras dentro de la continuidad y calidad del servicio, y las ventajas que conlleva el uso de tecnologías de virtualización de procesos. Además, la seguridad en la red juega un papel fundamental dentro de estos servicios, al igual que la eficiencia energética de los equipos; por lo cual se hace necesario una herramienta que integre estas funcionalidades para ser gestionadas de una manera más práctica y segura (Sakir, Scott-Hayward, & Kaur, 2013).

Las redes definidas por software (SDN) surgieron como una tecnología eficiente, con la capacidad de dinamizar la red en cuanto a las diversas funcionalidades y aplicaciones que puede ofrecer, mientras reduce los costos operativos a través de la optimización de hardware y software. Por ello, se establece de qué manera las redes definidas por software pueden contribuir al éxito de la red objetivo, y qué características de rendimiento, escalabilidad y operatividad posibilitan el funcionamiento de una determinada solución.

Para mejorar la manera en que opera la red, más específicamente la red WAN de la empresa Emtelco, este documento busca mostrar una propuesta que beneficie el desempeño de la red a través de la demostración de una solución SD-WAN básica. A fin de facilitar la comprensión, inicialmente se presenta un marco teórico que puntualiza los conceptos de redes de área amplia definidas por software, su arquitectura y modelos. Posteriormente se hace una propuesta, teniendo en cuenta la infraestructura disponible y manteniendo los fabricantes que hacen parte de ella, más específicamente Fortinet, mediante su firewall FortiGate. Enseguida, para materializar la propuesta, se realiza una pequeña demostración de la solución a través de una simulación en GNS3 y se hacen las pruebas pertinentes para evidenciar la mejora en el rendimiento de la red, a través de una mayor efectividad de respuesta frente a caídas de la red y pérdida de paquetes. Finalmente, se sacan conclusiones y recomendaciones frente a la propuesta realizada.

Planteamiento Del Problema

Emtelco es una compañía que ofrece servicios de BPO[1] y Contact Center a clientes corporativos durante los últimos 18 años. Al integrar canales de comunicación y relacionamiento, entre los servicios que se ofrecen a usuarios finales se encuentran: Servicio al cliente, Venta, Cobranzas, Back Office y Mesa de Servicios; todos a través de canales virtuales, telefónicos y presenciales (Emtelco, 2021).

La conectividad mediante enlaces MPLS[2] ha sido la más usada durante los últimos 15 años en la empresa, mediante el despliegue de redes de Internet dedicado; sirviendo de proveedor para puntos remotos que requieren de grandes equipos, con alto tráfico de datos, y que permiten garantizar el flujo y seguridad en la red.

Con los servicios SD-WAN, se pretende que las nuevas implementaciones de la red se realicen bajo un menor costo y sentar un precedente para desplegar servicios mucho más robustos a futuro. Sin dejar de lado la optimización en el tráfico, estos servicios permiten definir acciones programadas para redireccionar el tráfico en caso de fallas o daños en la infraestructura, al igual que centralizar estadísticas de la red para facilitar su gestión remota.

Los servicios en la nube se han ido estableciendo en el mercado de soluciones empresariales, por lo cual lo ideal es aprovechar estas nuevas funcionalidades que se incorporan y, en lo posible, continuar usando la infraestructura actual de la red para aprovechar la vida útil de los equipos, evitando sobrecostos al sustituir todos los elementos de la red con nuevos dispositivos.

---

[1] **BPO**. *Business Process Outsourcing*. Tercerización de Procesos de Negocio.
[2] **MPLS**. *Multiprotocol Label Switching*. Conmutación de etiquetas multiprotocolo.

Objetivos

Objetivo General

Realizar una propuesta para el uso de tecnología SD-WAN para la empresa Emtelco CX & BPO, a fin de mejorar la conectividad y el comportamiento de la red frente a posibles fallas internas en la sede Bogotá.

Objetivos Específicos

- Explicar el concepto de red SD-WAN, junto con su arquitectura, topologías, funcionalidad y beneficios.

- Realizar una demostración en GNS3 de la solución SD-WAN planteada, mediante configuración del firewall Fortigate y demás elementos de red.

- Mostrar cómo se desempeña la red corporativa en el escenario actual, y en uno que implemente SD-WAN.

- Comprobar las funcionalidades de SD-WAN para optimizar el tráfico, mediante pruebas entre los enlaces de red que muestren pérdida de paquetes y caída de los enlaces.

Justificación

Muchas compañías mantienen tecnologías antiguas, generalmente MPLS, para conectar sus redes de área amplia (WAN). La arquitectura que se muestra en la figura, indica cómo fluye todo el tráfico entre el Data Center central y el tráfico de los ISP que conecta con Internet. El tráfico corporativo es transmitido a través de conexiones dedicadas, las cuales son los circuitos de conmutación de etiquetas multiprotocolo (MPLS).

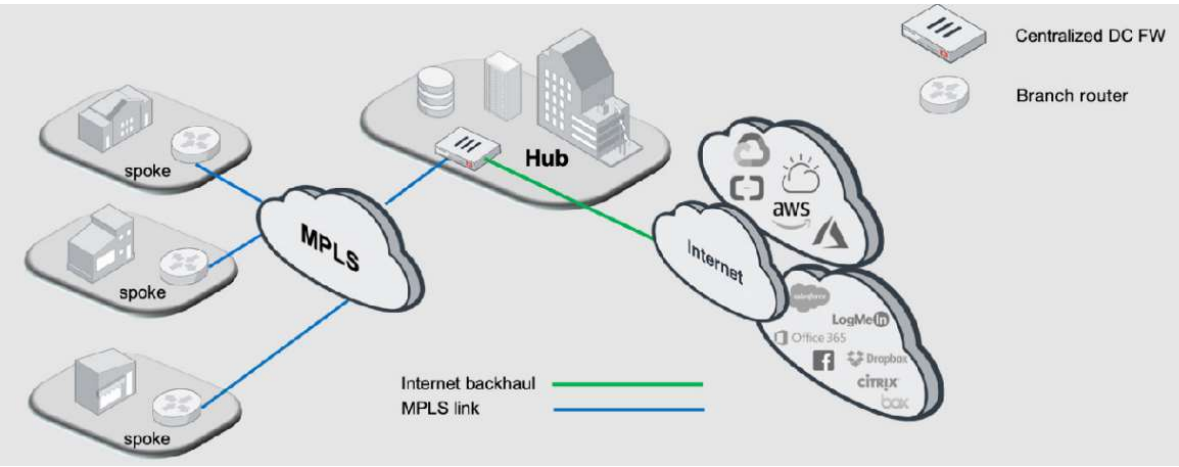


Figura 1. Arquitectura MPLS. Fuente: Fortinet.

La transformación digital es un movimiento que ha ido cambiando este modelo, a través de la digitalización en los negocios, la aparición de servicios basados en la nube (ej. SaaS[3]) y el consumo creciente de dispositivos que hacen uso de IoT (Internet de las cosas). Todos estos cambios requieren de nuevas formas de idealizar las redes.

Para que estas necesidades sean abordadas, algunas empresas han planteado el uso de soluciones de redes área amplia definidas por software (SD-WAN) junto con complementos de conectividad de bajo costo. Gracias a esta implementación, muchas compañías han logrado grandes procesos de transformación digital de su red WAN.

Los servicios de SD-WAN tienden a ser más contratados. Analistas de la firma Frost & Sullivan (MEF, 2020) estiman que para 2023, el mercado global de este servicio moverá cerca de $6400 millones de dólares, proyectando una tasa de crecimiento anual del 42% para el periodo 2018-2023.

A grandes rasgos, SD-WAN determina las rutas que cumplen mejor los requerimientos en rendimiento o en acuerdos de nivel de servicio (SLA) para cierta aplicación, asignando flujos de aplicaciones para la ruta WAN.

[3] **SaaS**. *Software as a Service*. Software como Servicio.

I. MARCO TEÓRICO

¿Qué es SDN?

Las redes definidas por software (SDN) hacen parte de un enfoque en la arquitectura de redes, en donde la red se controla de manera inteligente, a través de aplicaciones de software. Esto permite aumentar la velocidad y la flexibilidad de la red, separando los planos de control y reenvío, y facilita el diseño, desarrollo y administración de la red. De esta manera, el plano de control podrá ser programado, mientras la infraestructura subyacente (*underlay*) será utilizada para las aplicaciones y servicios de red.

Mediante controladores SDN programables y APIs (Interfaz de programación de aplicaciones), la red actúa de manera más lógica y centralizada, mejorando notablemente el rendimiento y permite vislumbrar el dominio de red de mejor manera.

Desde el punto de vista de las aplicaciones, las SDN actúan como un switch lógico. Para ello, las API descendentes se encargan de transmitir información a la infraestructura de red (*switches y routers)* y las API ascendentes son aquellas que se comunican directamente con los servicios y aplicaciones.

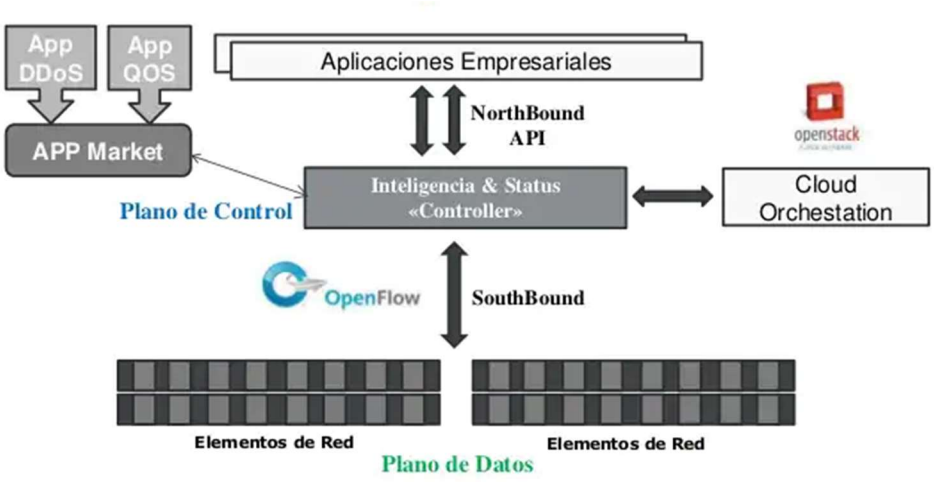


Figura 2. Planos funcionales de una red SDN. Fuente: Logicalis.

Entre los múltiples beneficios que estas redes otorgan, se destacan: mayor rapidez y automatización en la implementación de aplicaciones, mayor flexibilidad y uso de los recursos, y reducción de costos debido a la virtualización del Data Center.

Sin embargo, se debe tener en cuenta que existen ciertas limitaciones, en donde se incluyen cambios en el modelo de negocio, la necesidad de definir casos de uso y garantizar la funcionalidad constante.

SD/WAN

Los servicios SD-WAN (*Software Defined Networking Wide Area Network*) son el resultado de aplicar el concepto de SDN en redes WAN. Su principal objetivo es minimizar los costos que generan los servicios de conectividad, haciendo uso de infraestructura ya existente y algunos servicios en la nube que ofrecen soluciones empresariales más completas.

Según la definición del MEF[4], "un servicio SD-WAN proporciona una red de superposición virtual que permite la conectividad orquestada, controlada y orientada a aplicaciones entre interfaces de red de usuario SD-WAN, y proporciona la construcción lógica de una red enrutada privada virtual L3 para el suscriptor que transmite paquetes IP entre sitios".

Este servicio opera sobre una o más UCS[5]. Esto implica que puede ofrecer capacidades de prestación de servicios más diferenciadas, con respecto a los servicios basados en un único protocolo de transporte, al hacer uso de varias UCS diferentes.

Así mismo, SD-WAN reconoce y reenvía tráfico dependiendo de los requerimientos para el flujo en las aplicaciones. Esto implica especificar los flujos de aplicaciones y políticas que mejor se adaptan a las restricciones en el reenvío.

Beneficios

Las empresas cada vez más se están adaptando a la transformación digital dentro de su operación, a fin de mantenerse a la vanguardia en cuanto a tecnologías emergentes, los requerimientos de los clientes y el incremento de la competitividad. Las arquitecturas de red tradicionales no están hechas para soportar las cargas de trabajo y la complejidad que acarrean estas iniciativas de transformación. Aún más problemático, es que los servicios críticos suelen estar distribuidos a través de múltiples nubes, las cuales pueden comprometer el rendimiento de la red.

Dentro de los beneficios a nivel empresa más notorios, se encuentran la reducción de sobrecostos, mayor soporte de aplicaciones y el aumento del rendimiento de la red. Además, los costos de hardware se reducen, mientras se mantiene flexibilidad para acceder a múltiples servicios en la nube.

- Mejoras en el desempeño
  Como el tráfico de red varía en tamaño y contenido, SD-WAN es configurable para priorizar todo el tráfico relevante y los servicios en tiempo real que se tengan, como VoIP[6], para que le sea asignada la ruta más efectiva. Al aumentar el rendimiento y la seguridad en las conexiones, se reducen significativamente los problemas de latencia

[4] **MEF**. *Metro Ethernet Forum*. Foro Internacional de transformación digital en redes y tecnología.
[5] **UCS**. *Underlay Connectivity Service*. Servicio de conectividad subyacente.
[6] **VoIP**. *Voice over IP*. Voz sobre protocolo de internet.

y pérdida de paquetes; permitiendo mejoras en la productividad del personal y de la red en general.

- Aumenta la seguridad
  La transformación digital mejora muchos aspectos de cliente y de mercado, pero también va dejando vulnerabilidades y riesgos en seguridad de la información. Aunque SD-WAN ya ofrece un componente de seguridad integrado, se debe tener en cuenta que las funciones incluidas suelen ser muy básicas; lo cual implica desplegar funcionalidades más robustas para evitar la pérdida de datos, tiempos de inactividad, entre otros. Para ello, SD-WAN permite superponer seguridad externa a través de nuevas conexiones, dando mayor flexibilidad a la gestión de la red.

- Disminuye la complejidad
  Para evitar que el personal de TI de las compañías requiera desplazarse a sitio para gestionar la infraestructura de la red, SD-WAN simplifica la red WAN existente haciendo uso de banda ancha para aplicaciones corporativas, tareas de monitoreo y automatización, y para administrar el tráfico mediante controladora. También hay redes que permiten la administración dentro de la red local LAN.

- Uso de la nube
  SD-WAN permite el acceso directo a la nube desde remoto, enrutando todo el tráfico de la nube y la sede a través del centro de datos. Esto permite que el personal pueda acceder directamente a las aplicaciones de la nube sin importar su ubicación global, para evitar que la red central se sobrecargue de tráfico adicional para gestionar y proteger la red corporativa. Además, permite priorizar las aplicaciones clave para la compañía y habilitar conexiones para una comunicación directa con la red de Internet.

- Reduce costos
  Entre mayor uso de aplicaciones basadas en la nube sean desarrolladas, mayor será la cantidad de datos transmitidos a través de la red WAN, incrementando significativamente costos de operación. SD-WAN permite ahorrar dinero a través de accesos a Internet local de bajo costo, proporcionando acceso directo a la nube y disminuyendo la cantidad de tráfico de datos transmitida a través del *backbone* de la red.

La funcionalidad que brinda la red SD-WAN puede extenderse a distintas conexiones locales LAN para garantizar que la seguridad y la operación de la red están protegidas en todos los dispositivos y conexiones directas. La expansión de la red y los riesgos de seguridad se encuentran menos expuestos a fallas, y el aumento en el rendimiento es notable; por lo cual implementar una red WAN dentro de una organización se convierte en una herramienta muy útil para optimizar el desempeño de las operaciones corporativas.

Arquitectura SD-WAN

Según el estándar MEF 70, se tienen atributos de servicio para tres aspectos lógicos:

- Conexión virtual SD-WAN (SWVC)
- Conexión virtual End Point SD-WAN
- SD-WAN UNI (UNI)

Otros componentes a destacar son:

- Red del suscriptor
- Red del proveedor de servicio
- Servicio de Conectividad Subyacente (UCS)
- Túnel de Conexión Virtual (TVC)

Cuando se establecen los términos de contrato y el acuerdo de nivel de servicio entre el suscriptor y el proveedor, se debe tener un diagrama de bloques que muestre los componentes del servicio. Para ello, a partir del estándar (MEF, 2020), se tiene una descripción general a grandes rasgos de esos componentes, y la finalidad de uso para implementar el servicio SD-WAN.

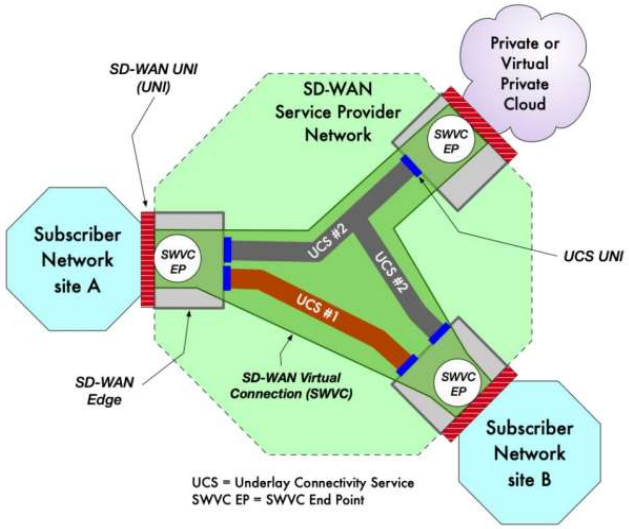


Figura 3. Componentes de un servicio SD-WAN. Fuente: MEF.

En la figura anterior, se muestra como los puntos de red del suscriptor se interconectan entre sí mediante UCS, y a través de los puntos de conexión virtual SD-WAN (SWVC EP), hacia la nube privada.

Tipos de Modelos de Despliegue SD-WAN

SD-WAN basada en Internet

Las redes SD-WAN basadas en Internet, hacen uso de equipos que se encuentran en las instalaciones de la empresa, añadiendo elementos como *routers* o reemplazándolos por dispositivos que optimizan la red WAN y firewalls. El tráfico de red continúa siendo enviado a través de los enlaces MPLS que han sido desplegados, dependiendo de las reglas definidas en la controladora. Además de complementar a estos enlaces MPLS, esta opción permite que su implementación sea económica, flexible y rápida, facilitando las conexiones hacia aplicaciones que se encuentran en la nube. Sin embargo, es una solución no tan recomendada para enlaces con distancias muy largas, ya que es inevitable que se presenten falencias como aumento de la latencia, *jitter* y pérdida de paquetes (Karkhanawala, 2021).

SD-WAN administrado por Telco o MSP SD-WAN

Con un servicio SD-WAN administrado por una compañía de telecomunicaciones, el cliente paga al proveedor de servicios para que instale y brinde conectividad, así como cualquier dispositivo que el servicio pueda requerir. La SD-WAN administrada es un servicio de valor agregado y puede venir con acuerdos de nivel de servicio (SLA), pero el servicio administrado usualmente se implementa utilizando parte del mismo hardware para admitir SD-WAN basadas en Internet. De igual manera, la velocidad en la conectividad va a depender del rendimiento de la aplicación y las distancias. Además, la empresa de telecomunicaciones o MSP[7] que ofrece el servicio, tendrá una alta dependencia del hardware y software de otros proveedores de redes y seguridad, por lo cual la experiencia con el soporte de los equipos va a ser más extensa, y tardará más tiempo en ejecutar soluciones a las incidencias presentadas (Karkhanawala, 2021).

SD-WAN as-a-Service (SD-WAN como Servicio)

Con SD-WAN as-a-Service, las empresas adquieren SD-WAN de la misma manera que se compran servicios en la nube, mediante un modelo de consumo. En lugar de construir su propia SD-WAN usando Internet, o hacer que un proveedor de servicios brinde la misma tecnología, las redes de próxima generación combinan características de una red privada con flexibilidad y costo por uso. Al habilitar esta conectividad, se permite un acceso remoto global, sin la necesidad de construir una infraestructura muy pesada o administrar otros tipos de hardware en el borde. Esta solución ha ido ganando acogida, sin embargo, no hay muchos proveedores que la ofrezcan y no se adecua para empresas con departamentos de TI que desean manejar su propia infraestructura o quieren usar dispositivos preexistentes,

Para sintetizar esta información, la siguiente tabla resume algunas ventajas y desventajas para el uso de cada modelo de despliegue SD-WAN:

[7] **MSP**. *Managed Service Provider*. Proveedor de servicios gestionados.

Tabla 1. Ventajas y desventajas por cada modelo de despliegue.
Fuente: Aryaka.

¿Qué Modelo de Despliegue SD-WAN es el más adecuado?		
	Ventajas	Desventajas
SD-WAN as-a-Service	• Conectividad de red privada • Rendimiento confiable y latencias consistentes • Conectividad directa IaaS / PaaS / SaaS • Funciona con todas las aplicaciones: locales, en la nube y SaaS • Optimización WAN incorporada • Monitoreo de redes y aplicaciones • Despliegue en horas o días, incluidos los servicios de última milla	• No es ideal para los departamentos de TI que desean construir su propia infraestructura de red. • Ofrecido por solo un puñado de proveedores
MSP SD-WAN	• Rendimiento confiable y latencias consistentes dentro de la región • Conectividad directa IaaS / PaaS / SaaS • Servicio totalmente gestionado con soporte	• Es posible que el proveedor deba asociarse con otros para la conectividad fuera de la región • Puede requerir que el cliente pague por funciones adicionales • Puede carecer de conectividad a algunos servicios en la nube / SaaS • Puede no incluir optimización WAN
Internet-based SD-WAN	• Implementación rápida y ahorro de costes si solo se utiliza Internet • Monitoreo de redes y aplicaciones • Excelente para implementaciones regionales • Se despliega en pocos días	• La empresa es responsable de todas las contrataciones de enlaces. • Cero CapEx (gastos en capital) • Falta de soporte para la optimización de la nube / SaaS

Casos de uso SD-WAN

Múltiples Servicios de Conectividad Subyacente (UCS)

Los servicios de SD-WAN logran minimizar el tiempo de inactividad que se produce en las aplicaciones al encontrar congestiones en la red. Sin involucrar bajas en el rendimiento o la compra de servicios dedicados adicionales, la clave radica en combinar dos o más Servicios de Conectividad Subyacente (UCS). Las combinaciones más comunes de dos servicios de conectividad son las siguientes:

- Red WAN de doble gestión (por ejemplo, VPN [8]de IP privada + VPN de IP privada)
- Red WAN híbrida (por ejemplo, VPN de IP privada + Acceso a Internet)
- Internet Dual (Acceso a Internet + Acceso a Internet)

1. Red WAN de Doble Gestión

Las empresas tienen el reto de ejecutar aplicaciones críticas sobre las UCS administradas por un sitio determinado, y deben incluir una UCS adicional para permitir redundancia, en caso de que el primer enlace falle. Sin embargo, esta UCS adicional permanece en estado inactivo hasta que alguna de las UCS activas falle y la UCS adicional se active de manera inmediata. Los servicios SD-WAN que ofrecen los proveedores, pueden hacer uso de estas UCS en modo activo-activo, mientras mantienen la misma resistencia ofrecida por la configuración activo-espera. La figura muestra un caso en el que la empresa tiene 2 servicios VPN de IP privada, en donde uno de estos se mantiene inactivo durante el 99% del tiempo. Con la implementación de SD-WAN, la capacidad de conexión corporativa se duplicó, reduciendo la redundancia sólo a la mitad (MEF, 2020).

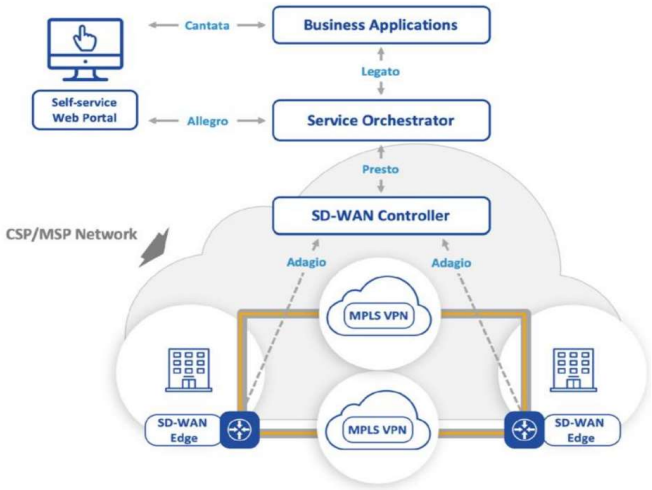


Figura 4. Caso de uso WAN de Doble Gestión. Fuente: MEF.

[8] VPN. *Virtual Private Network*. Red Privada Virtual.

2. Red WAN híbrida

En este caso, solo una de las UCS es administrada. El cliente había estado usando un servicio de VPN de IP Privada anteriormente, y necesitó expandir su disponibilidad de ancho de banda a un costo más eficiente. Este servicio puede ser usado para tráfico no crítico y durante altos periodos de uso. SD-WAN permite el uso simultáneo de varias UCS para diferentes necesidades corporativas. Cuando una conexión se cae, las aplicaciones más importantes pueden continuar ejecutándose dentro del servicio de conectividad que se encuentre activo (MEF, 2020).

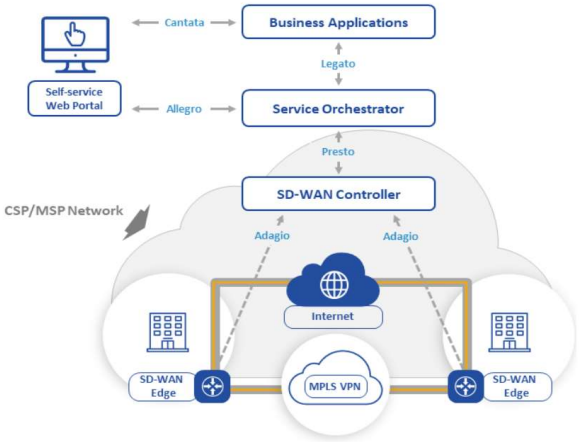


Figura 5. Caso de uso WAN híbrida. Fuente: MEF.

3. Internet Dual

En este último caso, el cliente SD-WAN no tiene gestión sobre la red WAN. Para maximizar la redundancia, el cliente usa el servicio de red dentro de una combinación de dos o más servicios de Internet desde diferentes proveedores con enrutamiento inteligente de los flujos de aplicaciones entre los servicios de Internet para maximizar el rendimiento (MEF, 2020).

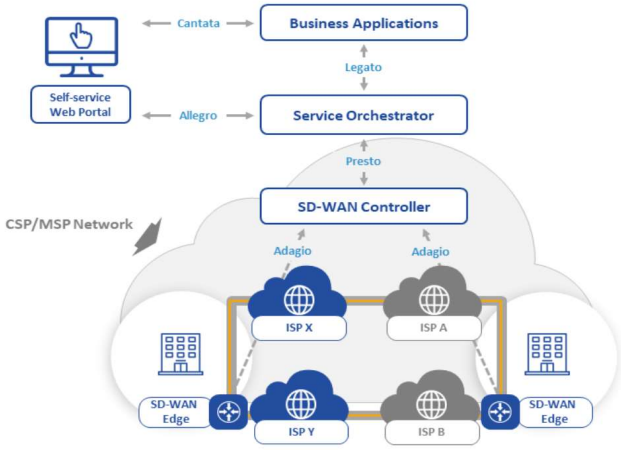


Figura 6. Caso de uso Internet Dual. Fuente: MEF.

FlexiWAN

FlexiWAN permite que las empresas y los proveedores de servicios adapten su solución SD-WAN sin verse limitados por el costo, bloqueos del fabricante y las capacidades de enrutamiento específicas que ofrecen los proveedores de SD-WAN. FlexiWAN ofrece una infraestructura SD-WAN de código abierto y de arquitectura abierta que incluye vRouter, administración, orquestación y automatización, así como las funcionalidades más básicas de SD-WAN (FlexiWAN, 2019).

Para implementar FlexiWAN, se requiere de 2 módulos principales, que se pueden descargar en su página oficial: flexiEdge, que requiere de un switch de borde que corra sin sistema operativo y una máquina virtual; y flexiManage, que hace una gestión centralizada como Saas o mediante el hosting del proveedor de servicios.

FortiGate NGFW

Los *Next-Generation Firewalls* (NGFW) FortiGate, son dispositivos que brindan un alto rendimiento, seguridad y visibilidad frente a ciberataques, mientras reducen la complejidad en la configuración de sus funcionalidades. Estos *firewalls* contienen procesadores de seguridad para garantizar mayor protección frente a amenazas y mejorar el rendimiento del tráfico a través de cifrado SSL (Fortinet, 2021).

Una de sus principales ventajas, es la posibilidad de incluir *appliances* (dispositivos complementarios) que identifican problemas de forma intuitiva y efectiva. Dentro de estos aplicativos, se encuentra una solución SD-WAN nativa, ofreciendo un control automático de las rutas en la WAN, mejorando el rendimiento del aplicativo de gestión de la red y facilitando su uso, al igual que reduce los gastos operativos de la WAN al detectar anomalías tempranas (Icorp, 2019).

Figura 7. FortiGate NGFW. Fuente: Fortinet

Esta funcionalidad está disponible en dispositivos NGFW que ejecuten el sistema FortiOS desde la versión 5.4 del año 2016. Sin embargo, para garantizar mayor seguridad en la red se recomienda hacer uso de la versión 6.0 en adelante. Esta versión incluye mayor visibilidad de las aplicaciones a través de una herramienta de monitoreo integrada y múltiples estrategias SLA (Fortinet, 2018).

Para efectos del diseño de la propuesta, se decide continuar usando el Fortigate 800C existente en la arquitectura de red corporativa, para que continúe gestionando la seguridad de la red y permita adicionar las funcionalidades que el complemento SD-WAN de Fortinet ofrece. Para ello, se va a requerir de la actualización del software del equipo, a una versión más reciente que soporte esta característica.

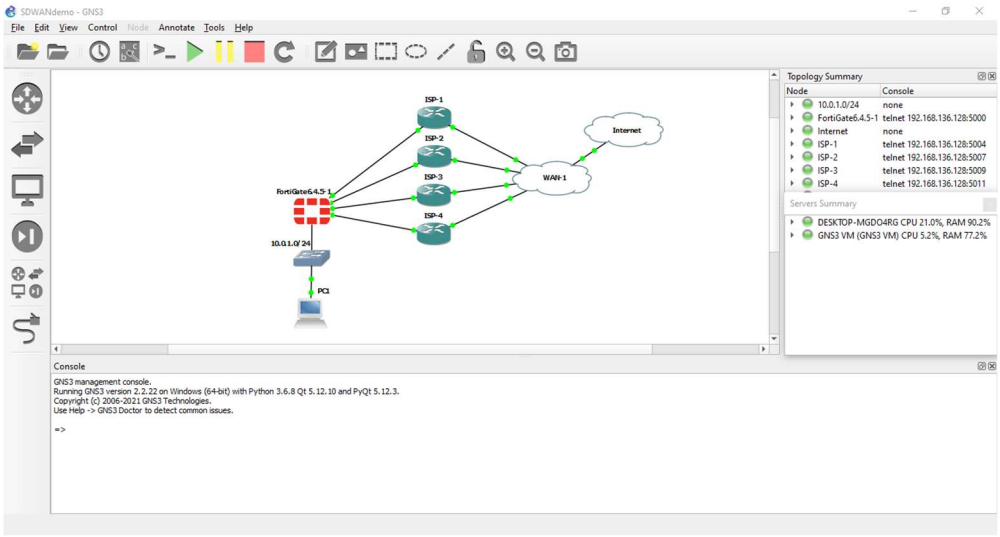
Figura 8. Fortigate 800C. Fuente: Fortinet.

Sin embargo, se deja planteada la posibilidad de usar una solución de código abierto como FlexiWAN en el futuro, para que las funcionalidades sean más variadas e innovadoras. Para efectos de una solución con corto alcance, pero también corto plazo, se opta por continuar con el Fortigate.

FUNDAMENTOS GNS3 (ENTORNO)

¿Qué es GNS3?

GNS3 es una herramienta utilizada para simular, configurar, probar y solucionar problemas de redes virtuales y reales. Es un software gratuito, de código abierto, creado originalmente por Jeremy Grossman como ayuda para estudiar para sus certificaciones de CCNP; por tanto, este software ha ayudado a personas a prepararse para exámenes de certificación, y también para probar y verificar implementaciones realistas. Originalmente solo emulaba dispositivos Cisco, a través de un software llamado Dynamips. Actualmente es compatible con muchos dispositivos de distintos proveedores, incluidos switches y routers virtuales Cisco, Fortinet, Cisco ASA, Brocade vRouters, Cumulus Linux, instancias Docker, HPE VSR, múltiples dispositivos Linux y muchos otros (GNS3, 2021).



Preparación del entorno

Para el uso del software GNS3, la computadora deberá tener instalada una herramienta de virtualización para ejecutar la máquina virtual GNS3 VM de manera paralela a la aplicación, debido a que la instalación local del programa en conjunto suele generar muchas fallas. GNS3 VM alojará la virtualización de los dispositivos utilizados durante la simulación, por lo cual se recomiendan los siguientes requerimientos mínimos de hardware: 16 GB de RAM, 35GB de espacio en el disco duro, procesador de 4 núcleos (GNS3, 2021)

Inicialmente, se carga la máquina virtual GNS3, que para este caso es alojada dentro de la herramienta VMware Workstation Pro, y muestra la siguiente pantalla al momento de ser iniciada:

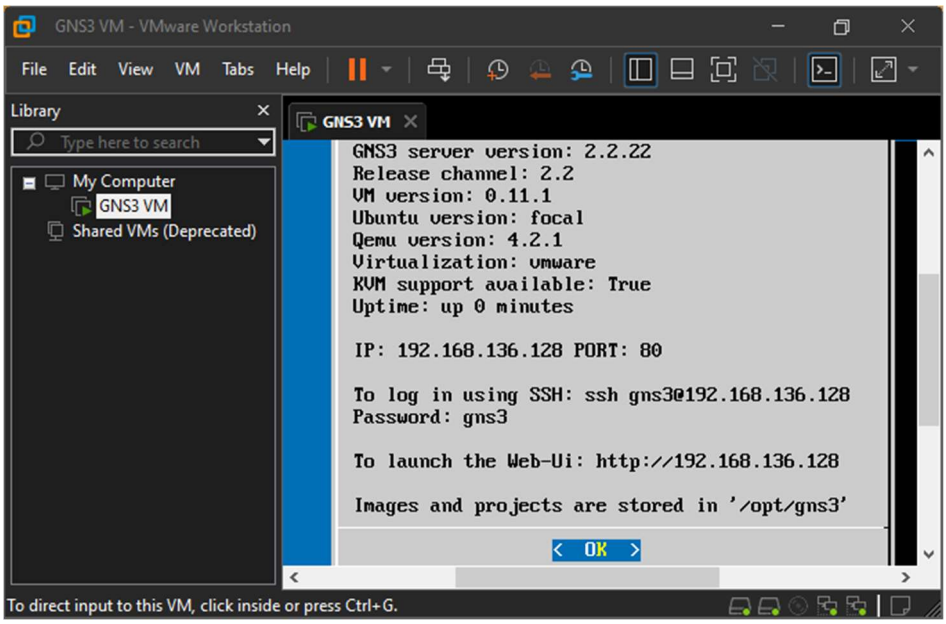


Figura 9. Máquina Virtual GNS3 iniciada

Posteriormente se ejecuta la herramienta GNS3, verificando si la máquina virtual se encuentra habilitada por la herramienta. Esto se hace en el panel de Servidores, ubicado en la parte lateral derecha, mediante el ícono indicador de GNS3 VM en color verde. Si no es habilitado, se deberá revisar la configuración del firewall del equipo que ejecuta el programa.

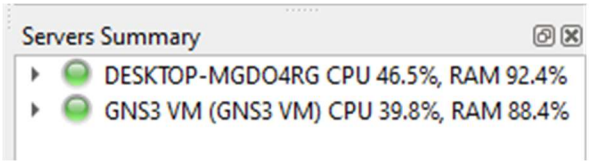
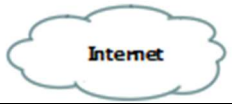


Figura 10. Servidores habilitados.

Teniendo la máquina virtual habilitada, se podrán comenzar las implementaciones. Por ello, se tienen en cuenta los siguientes elementos para elaborar la topología:

Tabla 2. Elementos a utilizar (GNS3, 2021)

Dispositivo	Nombre	Descripción
FortiGate6.4.5-1	FortiGate	Este aplicativo de Firewall virtualizado ofrece funciones avanzadas de prevención de amenazas para la implementación de dispositivos físicos en la nube.
webterm-1 PC1	Webterm (PC)	Se usará para representar los hosts (PC), con un menor consumo de recursos en la máquina virtual.

	Ethernet Switch	Este módulo básico de conmutación permite acceder a las funciones más comunes de un switch en capa física y algunas funcionalidades en capa de enlace.
	OpenWrt (WAN)	Es un router que representa la red WAN. Ethernet0 es el enlace LAN, mientras Eth1 es el enlace WAN.
	NAT (Internet)	Este nodo permite conectar la topología a Internet a través de NAT[9].
	NETem 0.4 (ISP)	Se usa para controlar la calidad en el tráfico, emulando un enlace de red WAN. Permite variar el límite de ancho de banda, retardo, fluctuación y pérdida de paquetes.

Instalación de appliances

Los *appliances* son todos aquellos dispositivos complemento que no se encuentran por defecto en GNS3. La principal ventaja que tienen estos elementos, radica en que tienen una preconfiguración que facilita la integración de dispositivos al proyecto. GNS3 tiene una amplia variedad de estos complementos, y facilita su instalación a través de la descarga directa desde el mismo software.

Para comprender como se realiza esta instalación, se ilustrará cómo instalar el *appliance* OpenWRT. Este último es necesario para la simulación a realizar, y más adelante se detallará su función.

Primeramente, se debe identificar la barra lateral izquierda, que permite agregar dispositivos y enlazarlos. Allí se seleccionará la herramienta *Browse All Devices*, y después la opción *New Template*, como se muestra en la siguiente figura:

[9] **NAT**. *Network Address Translation*. Protocolo de traducción de direcciones de red.

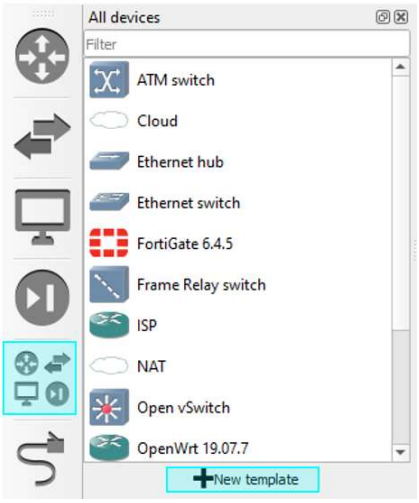


Figura 11. Agregar nuevos dispositivos.

Al presionar el botón *New template*, aparece la siguiente ventana:

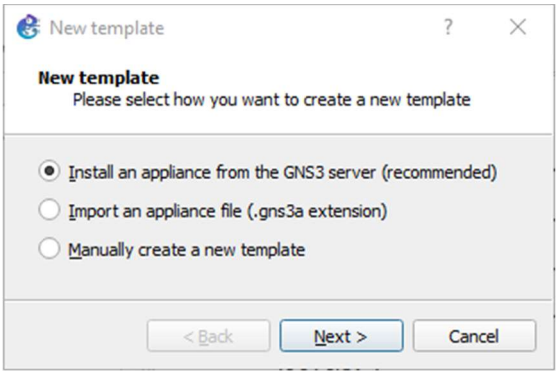


Figura 12. Opción New template

Se selecciona la opción seleccionada en la figura anterior, para instalar el appliance desde el servidor de GNS3, facilitando su instalación. Posteriormente, se buscará el nombre dentro de la barra de búsqueda, tal como se ilustra en la siguiente figura:

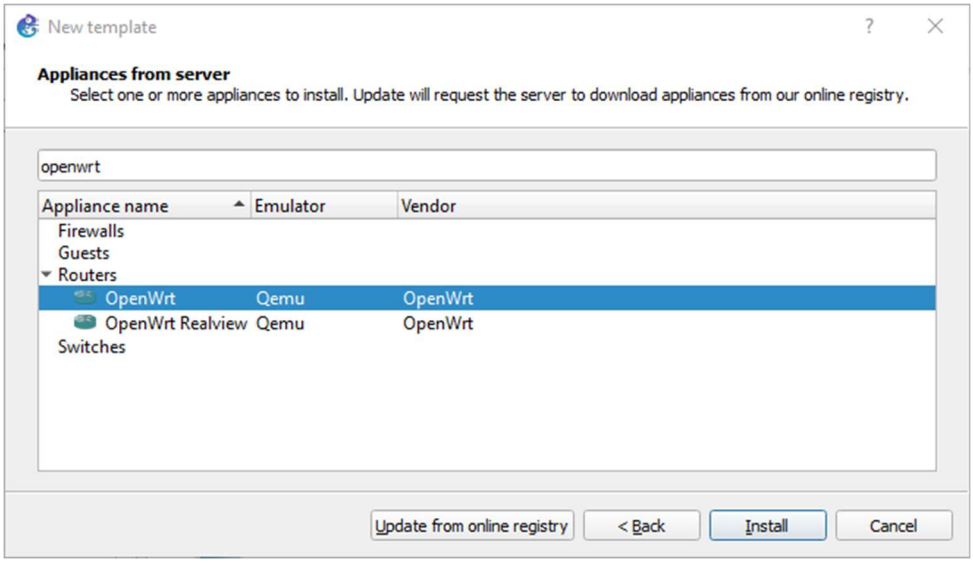


Figura 13. Búsqueda del appliance a instalar.

Luego de ser encontrado y seleccionado, se procede a la instalación. Para ello, GNS3 mostrará las versiones disponibles para el *appliance* seleccionado y mostrará que archivos se requieren para su instalación. Para este caso, el archivo fue encontrado en la máquina virtual, tal como se muestra en la siguiente figura:

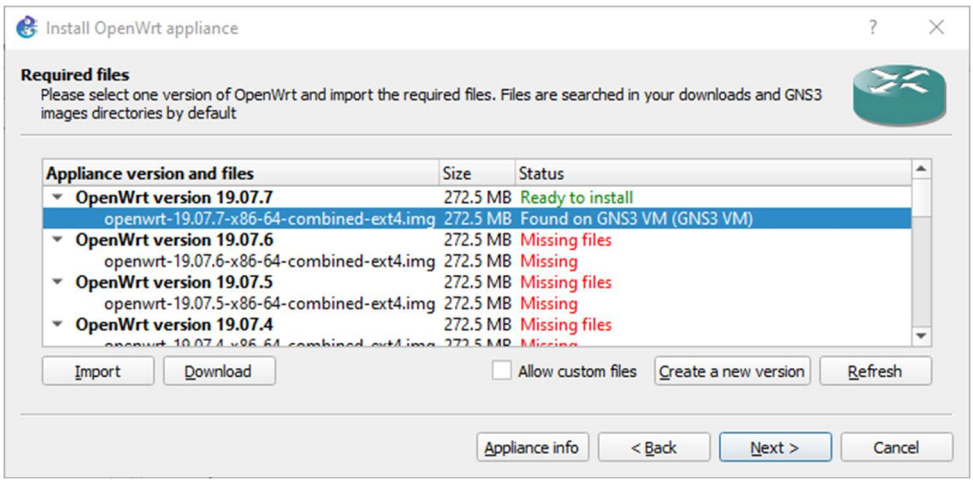


Figura 14. Archivos requeridos para la instalación.

Sin embargo, GNS3 permite la opción de importar el archivo necesario desde la máquina local, o descargarlo desde el servidor de GNS3. El botón *Download* redirige a la página de descargas de GNS3, facilitando la búsqueda de los archivos faltantes.

Finalmente, el asistente ejecutará el archivo de instalación y el *appliance* se podrá encontrar junto a los demás dispositivos.

Comandos para configurar Fortigate en CLI[10]

Para configuraciones en FortiGate (AprendeIT, 2018), se tienen en cuenta los siguientes comandos:

Tabla 3. Comandos para configurar en CLI FortiGate

Comando	Uso
CTRL+L	Borrar pantalla de ventana de comandos
TAB	Completa las palabras o predice el comando siguiente
config system interface edit port1 set ip 192.168.0.100 255.255.255.0 set allowaccess ping http (https telnet ssh) end	Configura interfaz de red
config router static edit 1 set device port1 set gateway end	Configura ruta
execute ping 8.8.8.8	Hace ping a la dirección indicada
get system performance status	Estado de la CPU y tiempo encendido
get system performance firewall statistics	Estadísticas de tráfico
show system interface	Muestra los cambios realizados en una interfaz
Ifconfig (interface config)	Muestra la configuración de todas las interfaces de red

Configuración WAN de bajos recursos

Para simular una red WAN con bajo consumo de recursos, se toma un *appliance* llamado *OpenWrt*. Este dispositivo es un router que simula una red de área amplia, permitiendo la

[10] **CLI**. *Command-Line Interface*. Interfaz de línea de comandos.

conexión entre el servicio de Internet (nodo NAT) y el nodo LAN. Para su configuración, se debe conectar primeramente a un *webterm* (PC), de la siguiente manera:

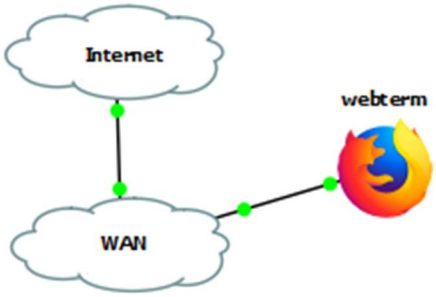


Figura 15. Topología para configurar red WAN

Para el router *OpenWrt*, el puerto *Eth0* es el enlace LAN, mientras *Eth1* es el enlace WAN que va hacia Internet. Inicialmente se configura el *webterm (PC)*, con la dirección IP 192.168.1.2 y puerta de enlace 192.168.1.1 usando el botón *Edit* de la etiqueta *Network configuration* y eliminando los comentarios (#), así:

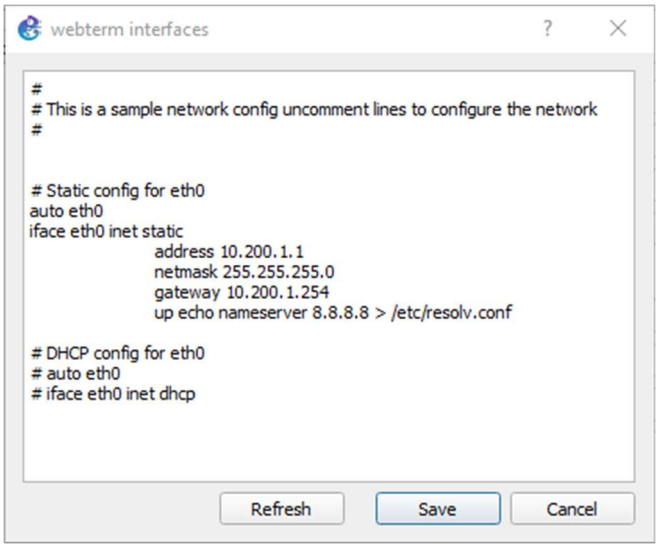


Figura 16. Configuración de red del webterm (PC)

Posteriormente, se ingresa al *webterm (PC)*, y se entra a la dirección 192.168.1.254 usando el explorador *Mozilla Firefox*. Por defecto, el usuario será root, y no tiene clave asignada, tal como se muestra en la figura:

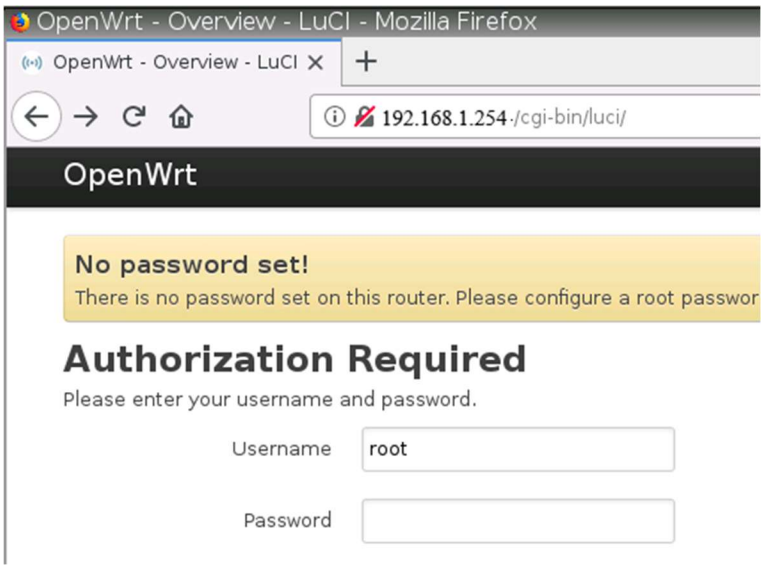


Figura 17. Inicio de sesión en OpenWRT.

Seguido a esto, en la pestaña Network>Interfaces. Allí se muestran todas las interfaces de red que han sido configuradas. En la parte inferior, se busca la acción *Add new interface*. Para evitar conflictos durante la configuración, la última a editar será la interfaz conectada al *webterm*, es decir, el puerto *Eth0*. Esto se debe a que, mediante esa dirección, se configuró el enlace para el ingreso al administrador del dispositivo.

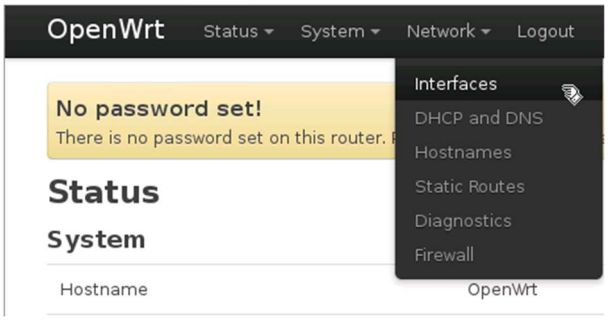


Figura 18. Selección de menú en OpenWrt.

Para agregar la nueva interfaz, se le asigna un nombre, se selecciona el protocolo para asignarle una dirección IP estática y luego el puerto a configurar, tal como se muestra en la figura, para el puerto *eth8*:

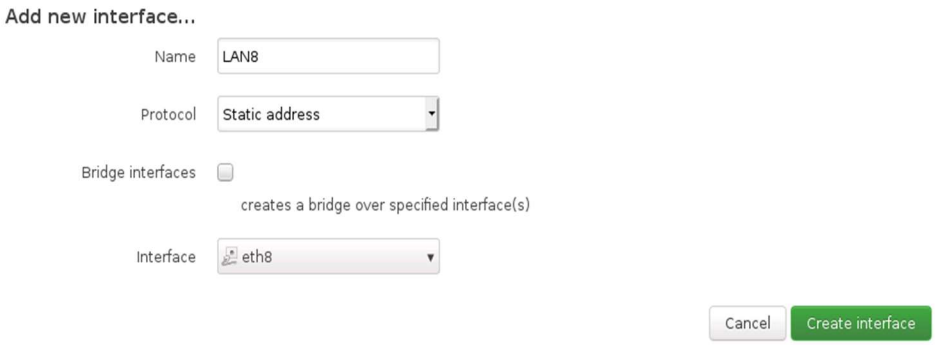


Figura 19. Creación de nueva interfaz de red.

Enseguida, se ingresa la dirección IP estática a asignar, y la máscara respectiva, como se muestra en la siguiente figura:

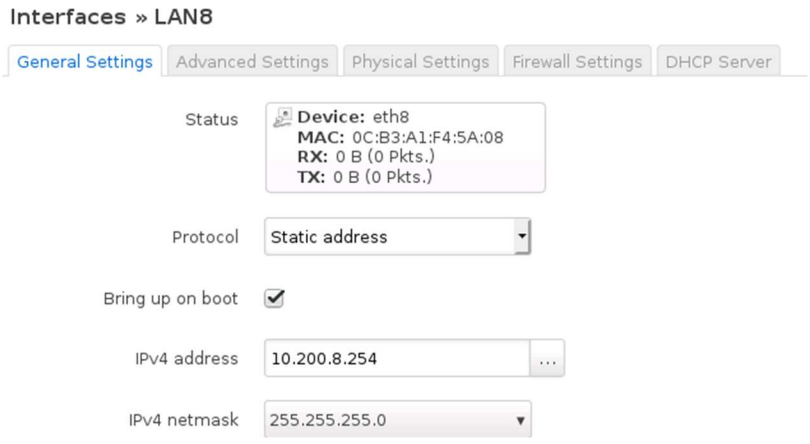


Figura 20. Asignación de dirección IP estática.

Además, se debe agregar a una zona de firewall, junto con las otras interfaces a ser configuradas, tal como se muestra en la figura:

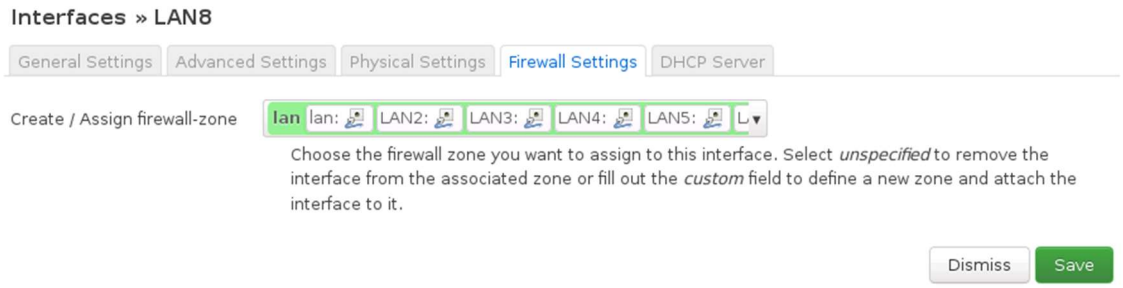


Figura 21. Asignación de zona de firewall.

Finalmente, se selecciona la opción de guardar y aplicar. Sin embargo, también se tienen las opciones de solamente guardar o resetear.

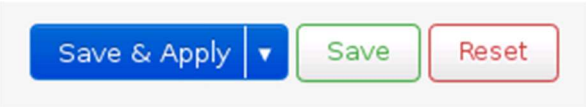


Figura 22. Opciones de guardado.

Para verificar que las interfaces estén correctamente configuradas, se ingresa al OpenWRT, y se ingresa el comando ifconfig, como se muestra en la siguiente figura:

```
root@OpenWrt:/# ifconfig
br-lan    Link encap:Ethernet  HWaddr 0C:B3:A1:F4:5A:00
          inet addr:10.200.1.254  Bcast:10.200.1.255  Mask:255.255.255.0
          inet6 addr: fe80::eb3:a1ff:fef4:5a00/64 Scope:Link
          inet6 addr: fd1a:eaf2:c52b::1/60 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7403 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:561331 (548.1 KiB)  TX bytes:10832928 (10.3 MiB)

eth0      Link encap:Ethernet  HWaddr 0C:B3:A1:F4:5A:00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7420 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9374 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:666263 (650.6 KiB)  TX bytes:10834463 (10.3 MiB)

eth1      Link encap:Ethernet  HWaddr 0C:B3:A1:F4:5A:01
          inet addr:192.168.110.130  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::eb3:a1ff:fef4:5a01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3861 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8289317 (7.9 MiB)  TX bytes:275771 (269.3 KiB)
```

Figura 23. Vista de la configuración de red.

Primera configuración en Fortigate 6.4.5

Aunque para la práctica se configurará mediante la GUI[11], para la primera configuración es indispensable hacer uso de la ventana de comandos (CLI). Para ello, se deberá realizar el proceso enunciado a continuación.

Para iniciar la configuración en la CLI (Interfaz de línea de comandos) de Fortigate, las credenciales de acceso son usuario: *admin* y la contraseña se deja vacía. Sin embargo, Fortigate va a requerir la creación de una nueva contraseña, tal como se muestra en la siguiente figura:

[11] **GUI**. *Graphical User Interface*. Interfaz gráfica de usuario.

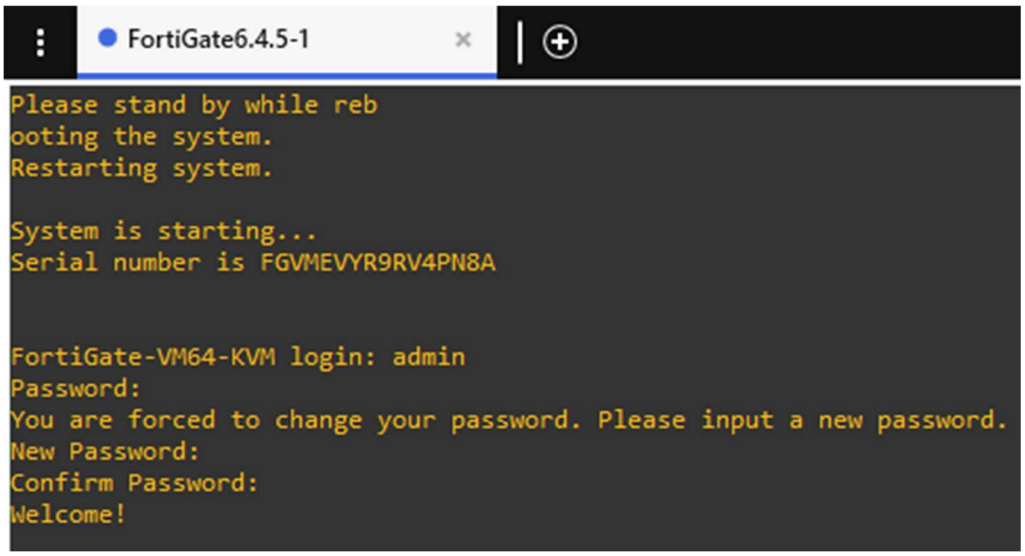


Figura 24. Inicialización de Fortigate 6.4.5

Posterior a ello, se deberán tener en cuenta los siguientes comandos para la asignación de dirección IP estática al puerto que va a permitir la conexión a la GUI de Fortinet. En este caso es el puerto 5, tal como se muestra en la figura:

```
FortiGate-VM64-KVM (interface) # edit port5

FortiGate-VM64-KVM (port5) # set ip 10.0.1.254/24

FortiGate-VM64-KVM (port5) # set allowaccess ping http https telnet ssh

FortiGate-VM64-KVM (port5) # end
```

Figura 25. Comandos para direccionar puertos.

Para corroborar el correcto funcionamiento de la conexión, se puede realizar un ping con el siguiente comando:

```
FortiGate-VM64-KVM # exe ping 10.0.1.10
PING 10.0.1.10 (10.0.1.10): 56 data bytes
64 bytes from 10.0.1.10: icmp_seq=0 ttl=64 time=1.6 ms
64 bytes from 10.0.1.10: icmp_seq=1 ttl=64 time=3.3 ms
64 bytes from 10.0.1.10: icmp_seq=2 ttl=64 time=2.7 ms
64 bytes from 10.0.1.10: icmp_seq=3 ttl=64 time=2.6 ms
^C
--- 10.0.1.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.6/2.5/3.3 ms
```

Figura 26. Comando para realizar ping.

Manejo de la GUI Fortinet

Para acceder a la GUI, se ingresa a la dirección IP definida para el puerto 5. En este caso, la URL es el Gateway 10.0.1.254 y se hace a través del PC (*webterm*) que fue conectado al dispositivo Fortinet:

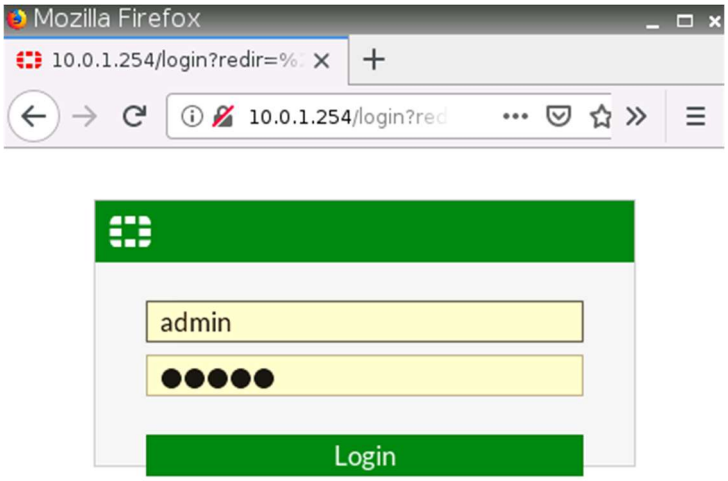


Figura 27. Acceso a la GUI.

Se recomienda cambiar el *Host Name* y el tiempo de inactividad (*idle timeout*) al máximo posible (480), debido a que el sistema puede ralentizarse a causa de los requerimientos de hardware. Esto se realiza en la pestaña *System* > *Settings*, como se muestra en la figura a continuación:

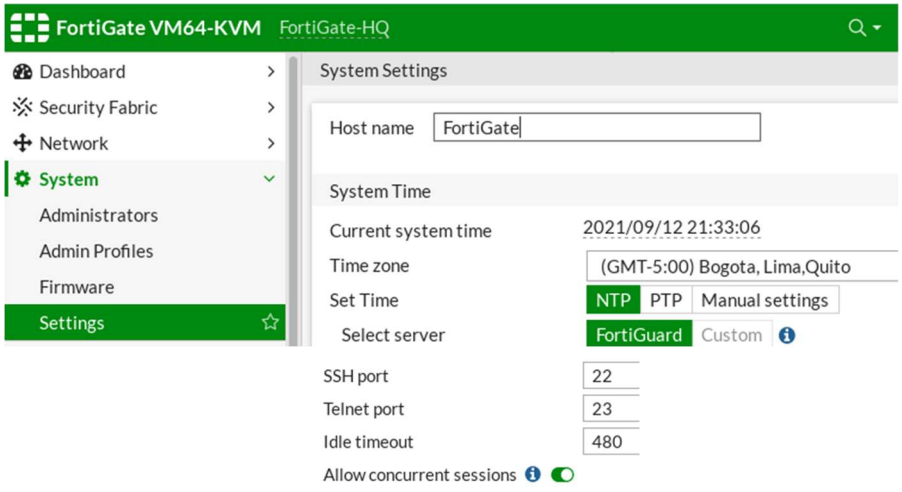


Figura 28. Configuraciones de sistema.

Para configurar las interfaces, se ingresa a través de la pestaña *Network* > *Interfaces*. Allí se pueden modificar protocolos, direcciones IP estáticas, tipos de acceso, entre otros. También permite verificar los puertos activos en el dispositivo.

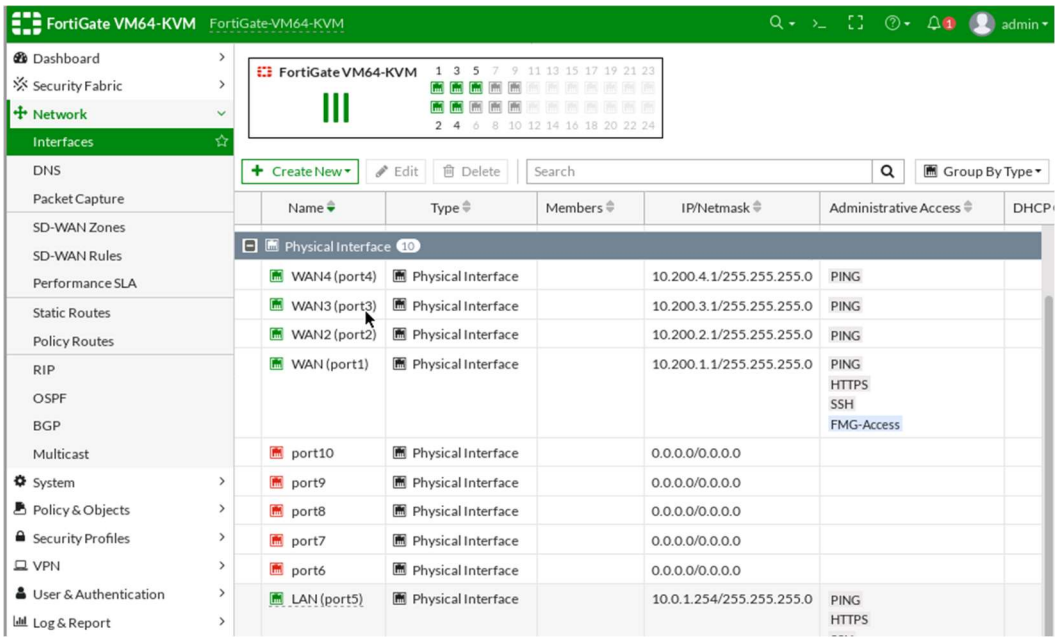


Figura 29. Administración de interfaces.

Para definir rutas estáticas, se ingresa a la pestaña *Network* > *Static Routes*. Allí se deberá definir el destino, el Gateway y la interfaz que tendrá la ruta.

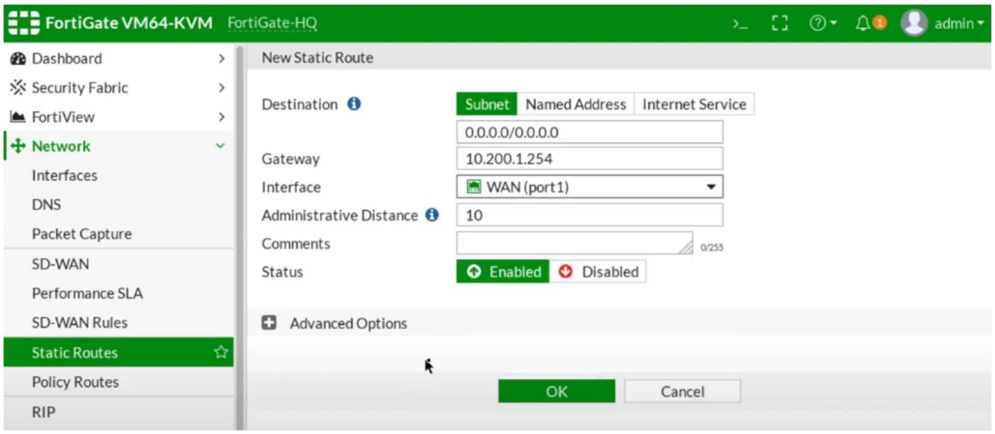


Figura 30. Rutas estáticas.

Para configurar el acceso a Internet, se deben revisar las políticas de Firewall, en la pestaña *Policy & Objects* > *Firewall Policy*. Allí se creará una nueva política que, para términos prácticos, aceptará todas las conexiones entrantes y salientes.

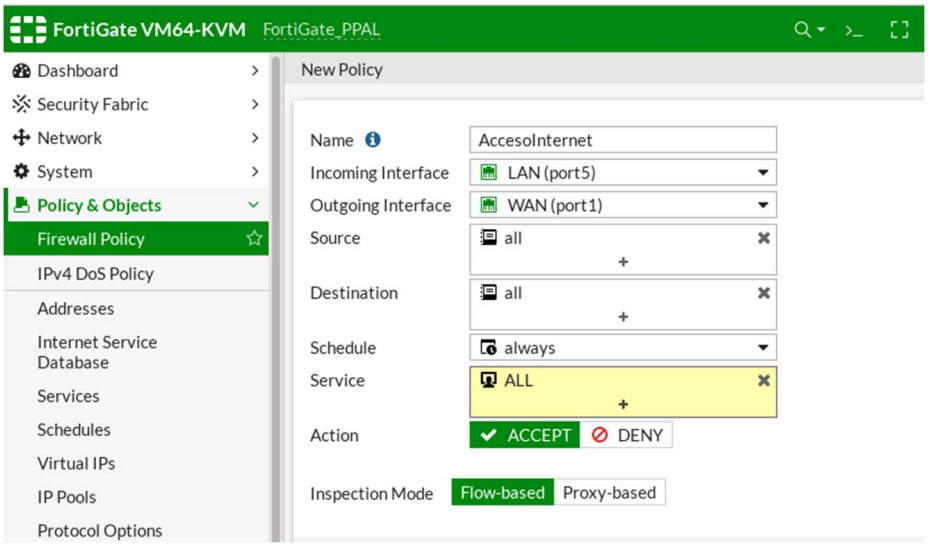


Figura 31. Políticas de Firewall.

Para mejorar el monitoreo, FortiView integra el historial de tráfico generado en la red, en tiempo real. Se accede a través de la pestaña *Dashboard* > *FortiView Sessions*. Esto permite registrar y monitorear amenazas a las redes, filtrar datos y realizar un seguimiento de las actividades corporativas (Fortinet, 2018).

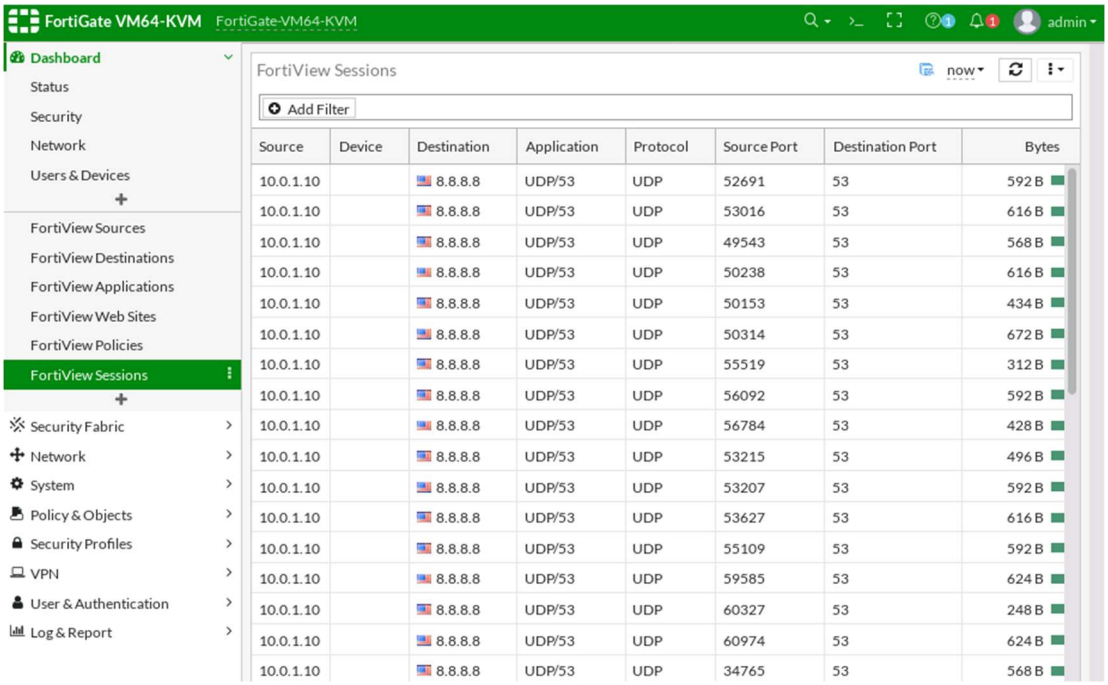


Figura 32. FortiView.

Adicionalmente, para el monitoreo SD-WAN, en la pestaña *Dashboard* > *SD-WAN Monitor*. Allí se podrá encontrar un tablero que muestra gráficas de aspectos como pérdida

de paquetes, latencia y jitter. Además, muestra la cantidad de sesiones de tráfico que cada interfaz ha tenido, y las velocidades de transferencia de subida y bajada que presentan.

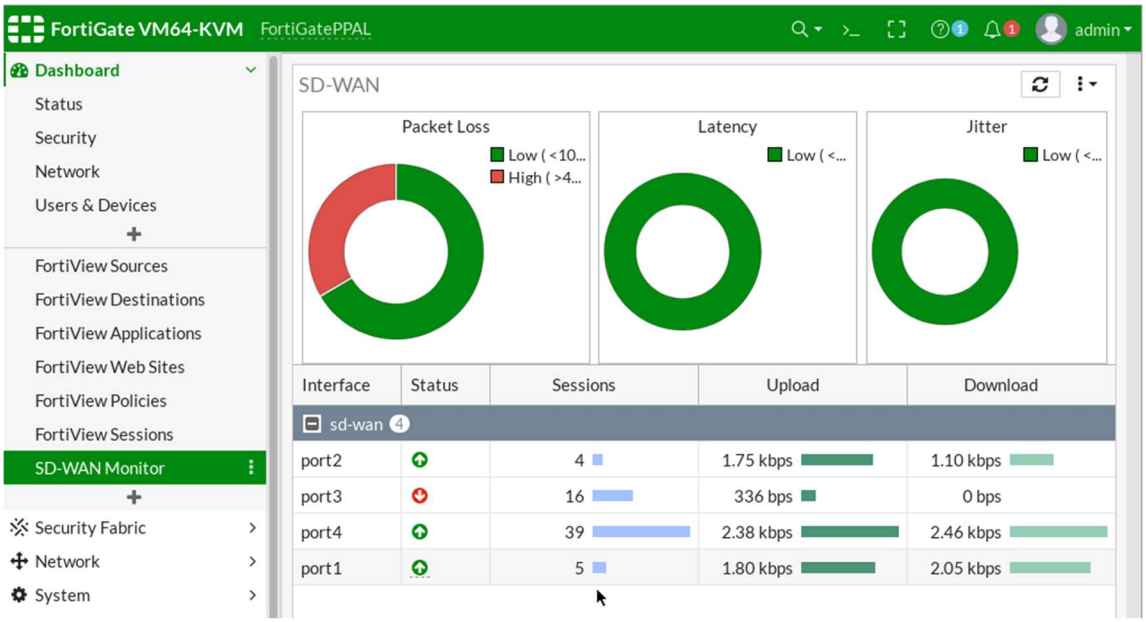


Figura 33. SD-WAN Monitor.

II. DESARROLLO

Topología

Para el desarrollo de la propuesta, se bosqueja la topología de red corporativa en la sede, para entender la distribución de las sedes y la manera en que funcionan los enlaces.

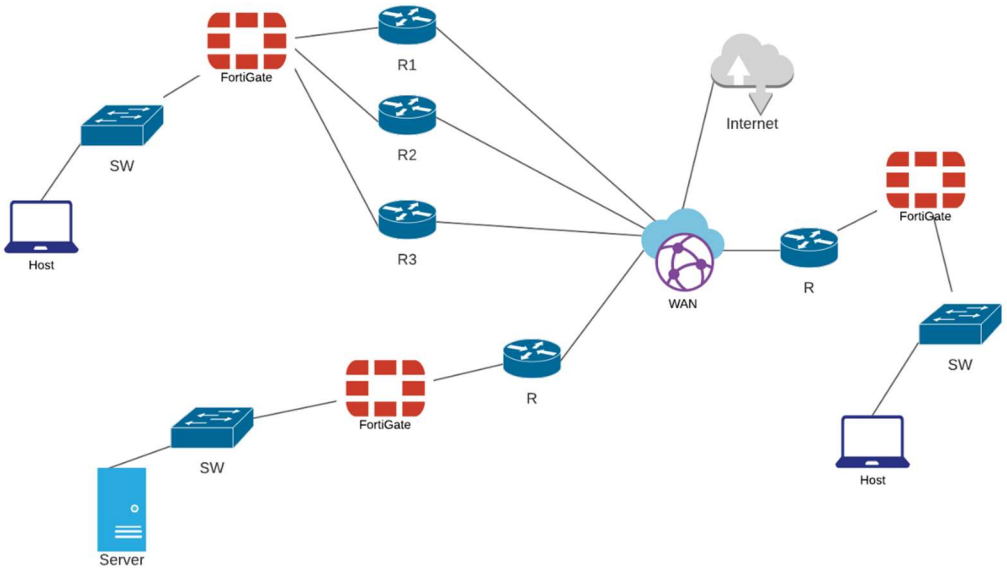


Figura 34. Topología de red corporativa.

Sin embargo, para acotar la situación y no sobrepasar la capacidad de memoria de la máquina con la que se realiza esta simulación, se realizó un diseño mucho menor que funciona como entorno de pruebas frente al concepto de SD-WAN en el segmento con más tráfico de la red corporativa.

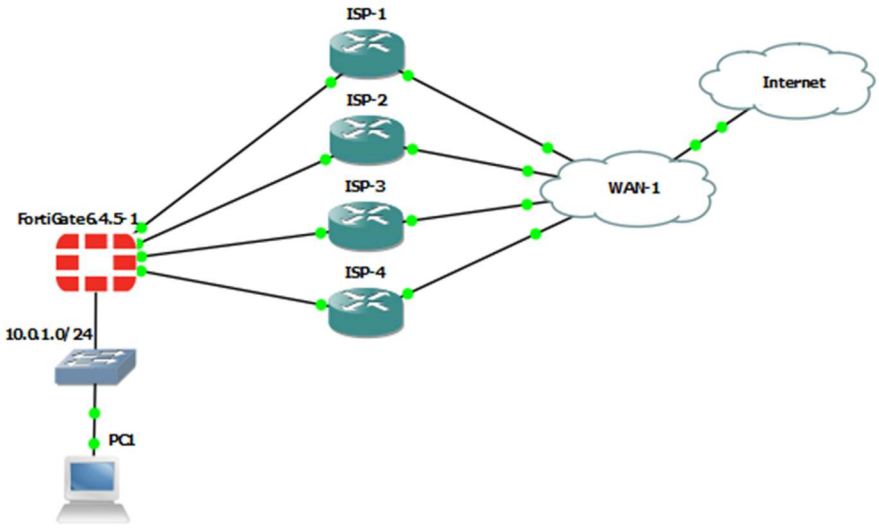


Figura 35. Topología a simular.

Cabe resaltar que la propuesta se realiza a través del modelo de despliegue SD-WAN basada en Internet, debido a que permite una implementación más rápida, con menores costos y ajustándose a los procesos que la empresa maneja.

Direccionamiento

Tal como se muestra en la figura de la topología, se han asignado las siguientes direcciones a cada una de las interfaces presentadas:

Tabla 4. Direccionamiento

Nombre	Interfaces	Dirección IP	Máscara	Gateway
FortiGate	Port 1	10.200.2.1/24	255.255.255.0	10.200.2.254
	Port 2	10.200.3.1/24	255.255.255.0	10.200.3.254
	Port 3	10.200.4.1/24	255.255.255.0	10.200.4.254
	Port 4	10.200.5.1/24	255.255.255.0	10.200.5.254
	Port 5	10.0.1.254/24	255.255.255.0	-
PC1	Eth0	10.0.1.10/24	255.255.255.0	10.0.1.254
OpenWRT (WAN)	Eth x	10.200.x.254/24	255.255.255.0	-
NAT	Nat0	192.168.1.1/24	255.255.255.0	-

Para configurar las interfaces en la GUI de FortiGate, se ingresa a través de la pestaña *Network > Interfaces*, seleccionando la interfaz a modificar y rellenando los campos que se muestran en la figura:

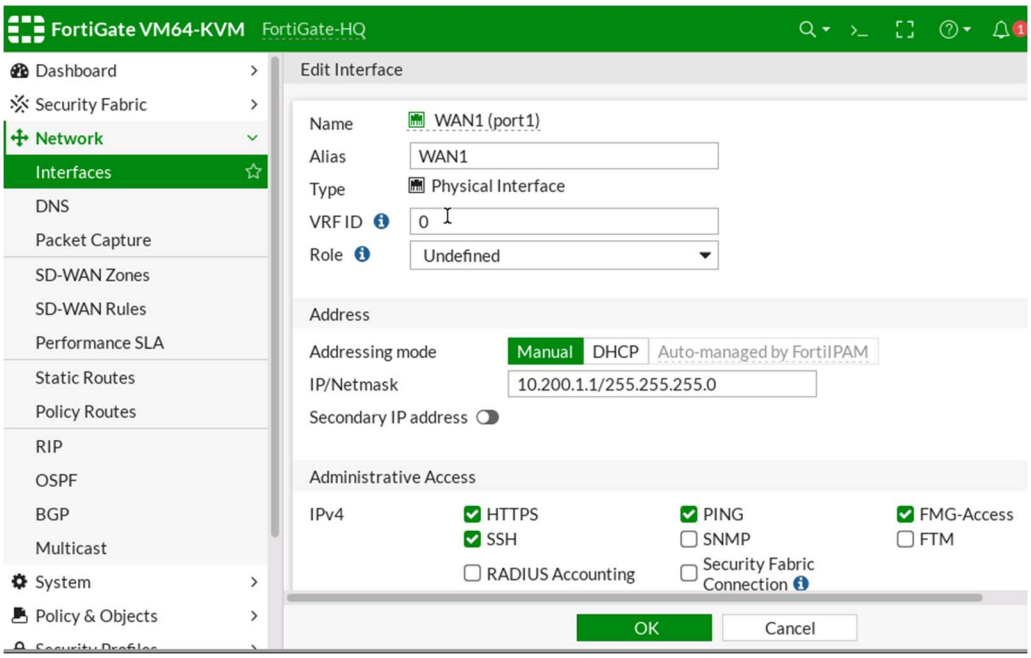


Figura 36.Modificación de parámetros de interfaz.

En el capítulo anterior, se detalla cómo asignar direcciones a los demás elementos de la topología a desarrollar. Para este caso se realizó un direccionamiento manual, a través de rutas estáticas para facilitar la identificación de los elementos. Sin embargo, es posible hacer uso del direccionamiento dinámico a través del protocolo DHCP.

Configuración SD-WAN

Luego de tener el entorno pre-configurado y el direccionamiento en las interfaces del dispositivo Fortigate, se procede a configurar la interfaz SD-WAN mediante zonas y reglas de Firewall. En la *pestaña Network > SD-WAN Zones* se agregan los Miembros de la nueva zona SD-WAN, tal como se muestra en la figura a continuación:

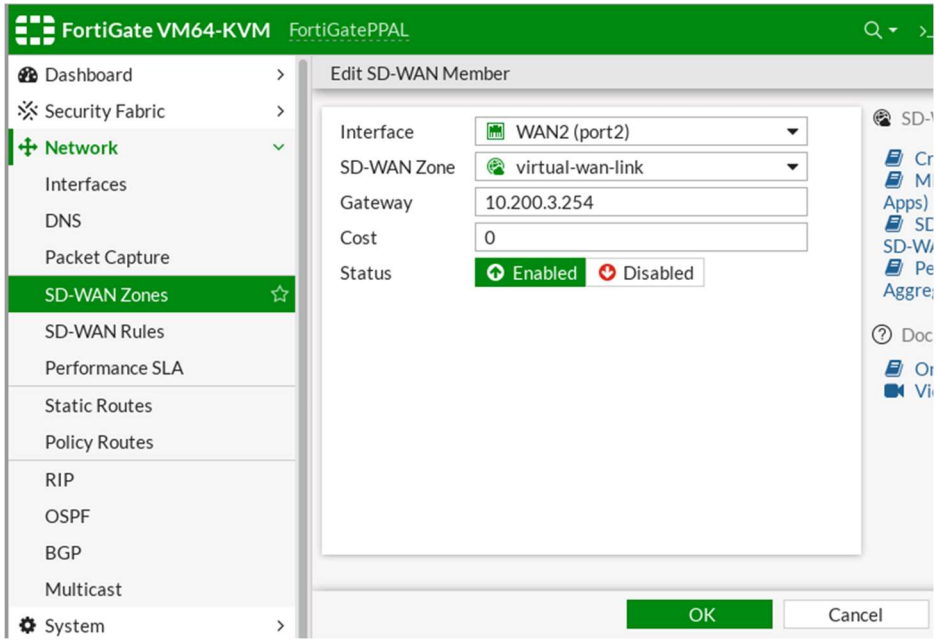


Figura 37. Agregar miembro a la zona SD-WAN.

Este proceso se puede realizar mientras la interfaz ya haya sido creada, y solo requiere definir la interfaz a utilizar, la zona SD-WAN de la que formará parte, la puerta de enlace que usará (en este caso a partir de una ruta estática) y el costo se deja en cero, teniendo en cuenta que el tráfico pasará a partir del enlace que tenga menor costo.

Posteriormente, en la pestaña *Policy & Objects > Firewall Policy,* se confirma que la zona SD-WAN se encuentre dentro de las reglas para el acceso a Internet. De no ser así, se crea una nueva, que garantice que la interfaz entrante (LAN port 5) y la interfaz saliente (zona SD-WAN) acepten todas las conexiones de origen y destino.

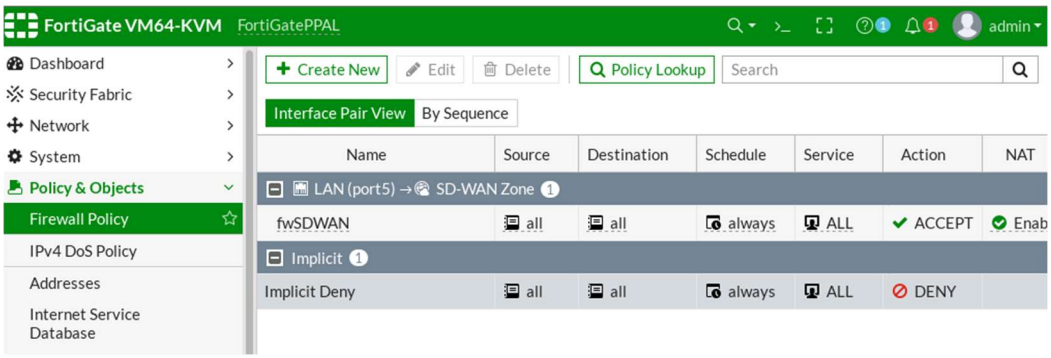


Figura 38. Política de Firewall SD-WAN

En un contexto más realista, el Firewall no debería aceptar todas las conexiones entrantes y salientes, por el contrario, debería contener las políticas de las páginas a las cuales se dará acceso, para garantizar la seguridad de la información.

Control del tráfico

Para permitir la correcta distribución del tráfico se hace uso de la herramienta de balanceador de carga que FortiGate ofrece. Allí se deberá verificar en la pestaña *Network* > *SD-WAN Rules*, que la regla implícita del algoritmo de balanceo de carga tenga habilitada la opción de IP de origen-destino, tal como se muestra en la siguiente figura:

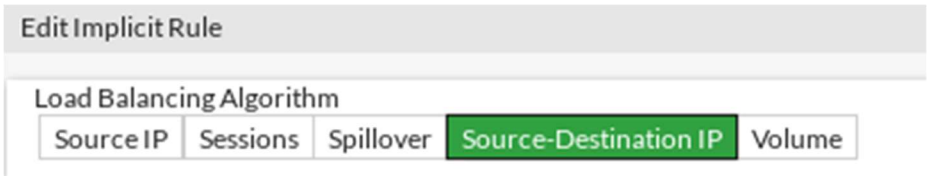


Figura 39. Algoritmo de balanceo de carga.

Esta última opción, permite que la carga de tráfico sea equilibrada por igual entre los miembros de la zona SD-WAN, a partir de un algoritmo *hash* que distribuye uniformemente la carga a partir de patrones de tráfico. Estos patrones cambian con el tiempo, por lo cual el sistema revisa periódicamente estos cambios para evitar congestiones en la red (Lee, 2014).

Con la herramienta *FortiView*, se procede a validar de qué manera se está distribuyendo el tráfico a través de los enlaces miembros de la zona SD-WAN, para corroborar que la regla anterior funciona de la mejor manera.

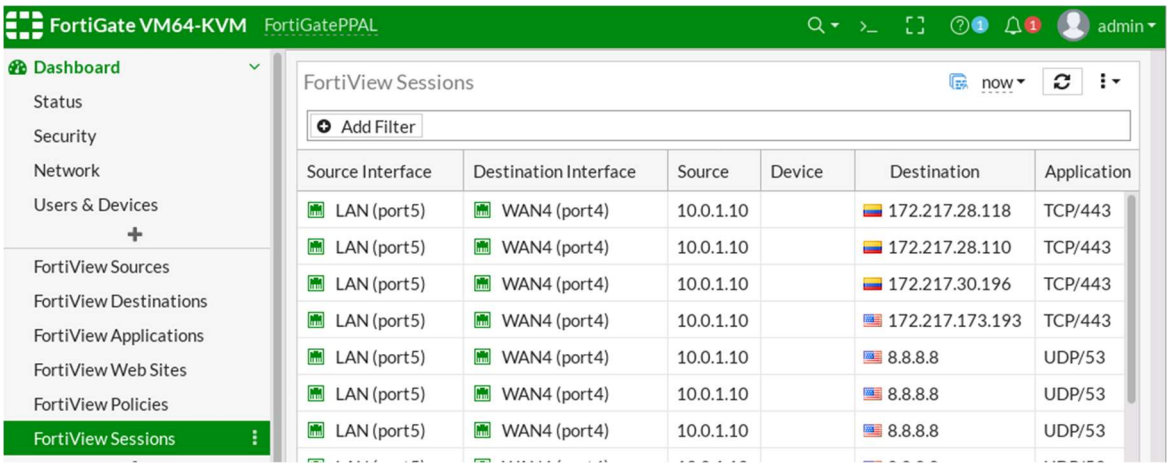


Figura 40. Sesiones de FortiView distribuidas con SD-WAN

Para realizar las pruebas, se han ubicado *appliances* NETem en medio de los enlaces que se encuentran entre el FortiGate y la red WAN. Estos dispositivos permiten insertar variables dentro del tráfico, tales como retardos, pérdidas y límites dentro del ancho de banda.

Monitoreo de enlaces con SLA de rendimiento

Este monitoreo permite la medición del estado de los enlaces que se encuentran conectados a las interfaces definidas como miembros SD-WAN. Para ello, este sistema envía señales a través de cada enlace para medir la calidad del enlace, proporcionando valores de latencia, retardos y pérdida de paquetes (Fortinet).

Con esta característica se permite inhabilitar aquellos enlaces que no se encuentran dentro del umbral esperado, permitiendo que el balanceador de carga actúe de una manera más óptima y enrute el tráfico hacia otros enlaces. Al no permitir el envío de tráfico por enlaces posiblemente rotos, se evita la pérdida de información.

Su configuración se realiza desde la pestaña *Network* > *Performance SLA*, seleccionando el protocolo a utilizar, los participantes o miembros involucrados, los tiempos para la revisión del enlace, y los límites de jitter, latencia y pérdida de paquetes.

Para este caso, se pondrá un umbral del 10% de pérdida de paquetes, por lo cual, el enlace solo funcionará si la medición arroja una pérdida menor o igual a ese 10% predefinido. De lo contrario, en enlace será inhabilitado automáticamente.

No se tuvieron en cuenta los demás umbrales SLA, debido a que GNS3 hace uso de varios hipervisores (Windows - GNS3 - KVM[12]) para la realización de esta práctica. Los hipervisores son los procesos que crean o ejecutan máquinas virtuales. Estos interfieren notablemente en el monitoreo, generando retardos considerables para el monitoreo de tráfico y por tanto no serán tenidos en cuenta para estas métricas (VMWare, 2021).

[12] **KVM**. *Kernel-based Virtual Machine*. Máquina virtual basada en el kernel.

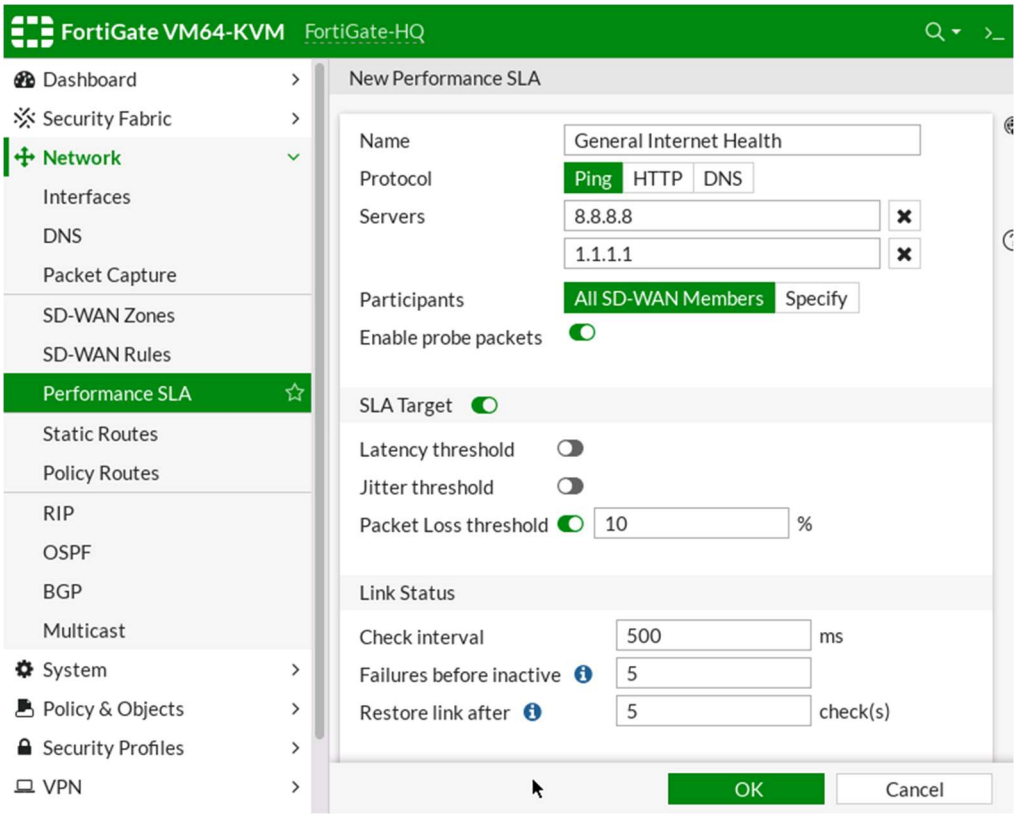


Figura 41. Creación de SLA de rendimiento.

Configuración de Reglas SD-WAN

Estas reglas se utilizan para controlar la distribución de las sesiones entre los miembros de SD-WAN. Las reglas se pueden configurar en modo Automático, Manual, Mejor Calidad, Menor Costo o Maximizar ancho de banda.

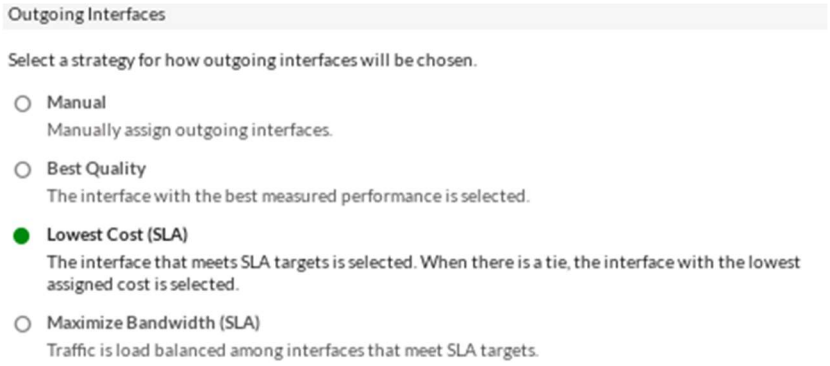


Figura 42. Modos de configuración de reglas SD-WAN.

Como se muestra en la figura anterior, el modo Automático asignará las interfaces a partir de una prioridad basada en su calidad, mientras el modo Manual, requerirá de la

asignación de prioridades a cada una de las interfaces. Por otro lado, el modo Mejor Calidad creará prioridades a partir del costo y rendimiento de enlace de la interfaz. El modo Menor Costo, creará prioridades a partir de la satisfacción de los indicadores SLA, evaluados en cada interfaz. El último modo, Maximizar ancho de banda, distribuye el tráfico entre las interfaces basado en el algoritmo de balanceo de cargas seleccionado.

Para realizar esta configuración, se accede a través de la pestaña Network > SD-WAN Rules, indicando el nombre de la regla, las direcciones de origen y destino, el modo de configuración de las interfaces y, por último, las interfaces involucradas.

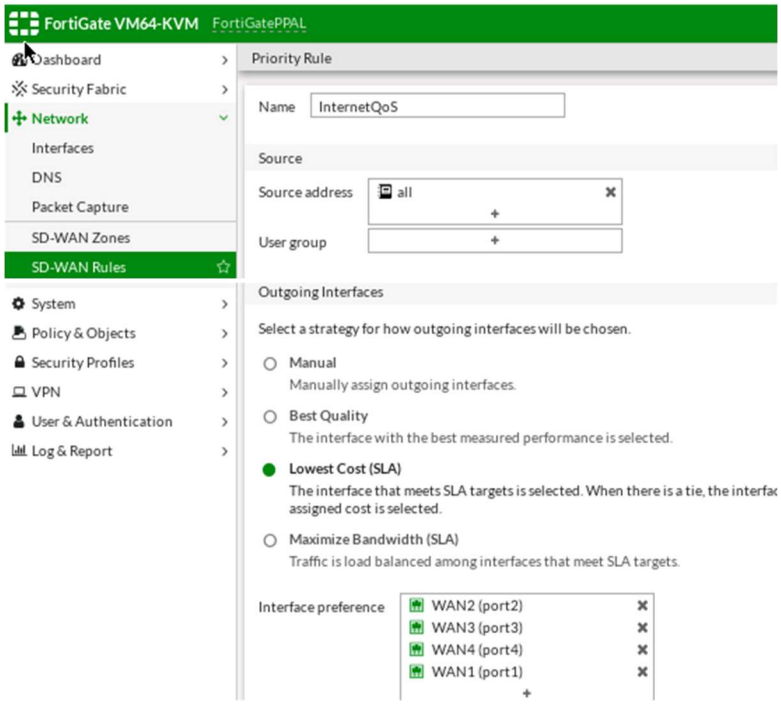


Figura 43. Configuración de reglas de prioridad SD-WAN.

En este caso, se tomó el modo Menor Costo (SLA), teniendo en cuenta que anteriormente se creó un indicador SLA que mide el estado general de las conexiones a Internet, y para finalizar la configuración, se seleccionaron las interfaces de preferencia y el indicador SLA requerido. La regla tomó el nombre de *Internet QoS* (Calidad del servicio de Internet).

Estas reglas usan un modelo top-down, permitiendo crear nuevas reglas para un tráfico más detallado. Las reglas más específicas se irán ubicando en la parte superior de la lista de reglas, mientras las reglas más generales van a permanecer en la parte de abajo de la lista.

III. RESULTADOS OBTENIDOS

Luego de haber configurado una regla para regular la calidad del servicio dentro de los enlaces SD-WAN, se procede a la realización de pruebas que determinarán si la regla se está desempeñando de la mejor manera. Al encontrar un problema en el enlace que se encuentra priorizado para llevar el tráfico, la herramienta deberá encontrar una ruta alterna para que la conexión se siga estableciendo, siguiendo los parámetros establecidos en la regla SD-WAN.

Para verificar qué enlace tiene menor costo, y por tanto suele llevar el tráfico, se abre la pestaña *Dashboard > FortiView Sessions* y se procede a generar tráfico en la red desde el PC1. Como se observa en la figura, el enlace por defecto es el WAN2.

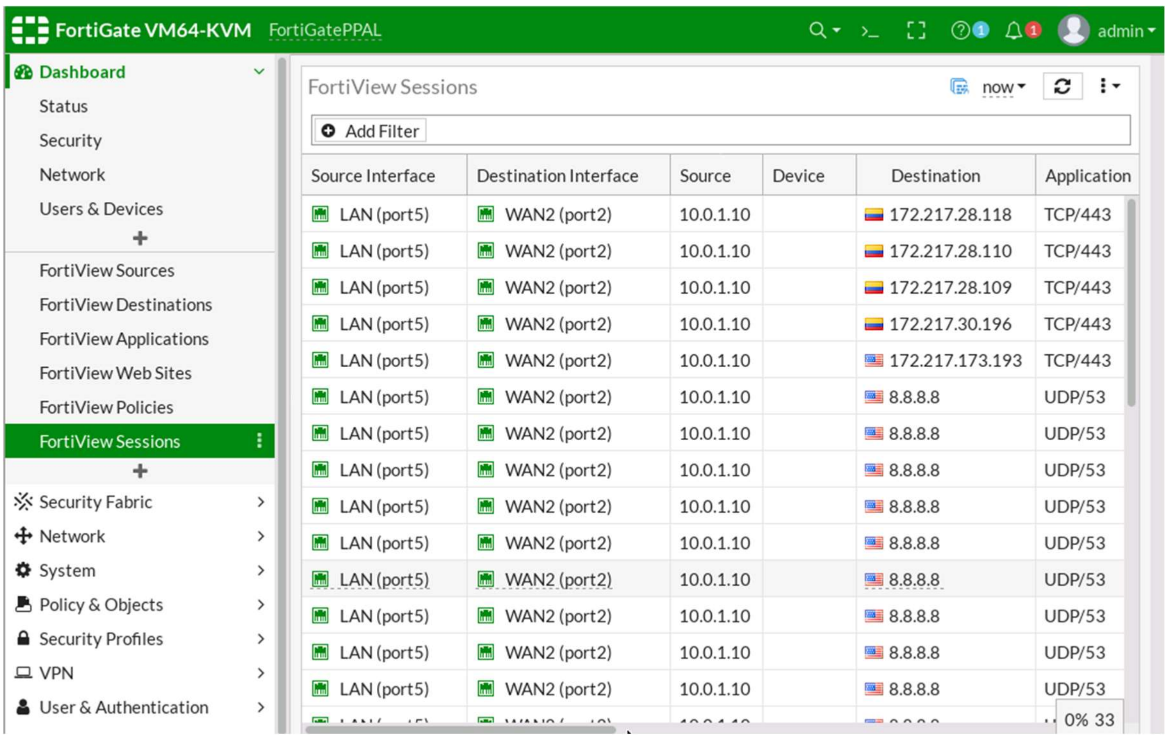


Figura 44. Vista de las sesiones inicial.

A pesar de que las cuatro interfaces tienen el mismo costo (0), la priorización asignada se dio en la configuración de la regla de prioridad, quedando de la siguiente manera:

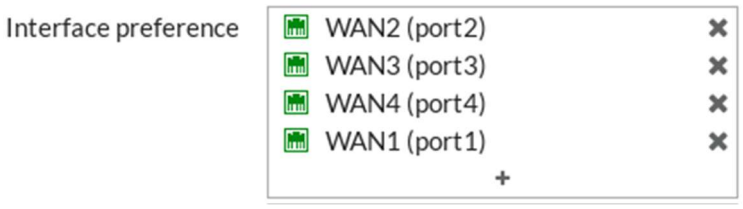


Figura 45. Preferencia de interfaces.

Prueba 1. Umbral de pérdida de paquetes alcanzado.

Para esta prueba, se hace uso del dispositivo NETem. Este permitirá manipular el tráfico, para que presente ciertos valores de retardo y pérdida de paquetes, al igual que cierto ancho de banda limitante. Teniendo en cuenta que la regla SD-WAN configurada solo admite un porcentaje máximo de 10% de pérdida de paquetes, se configura un 20%, tal como se muestra en la siguiente figura:

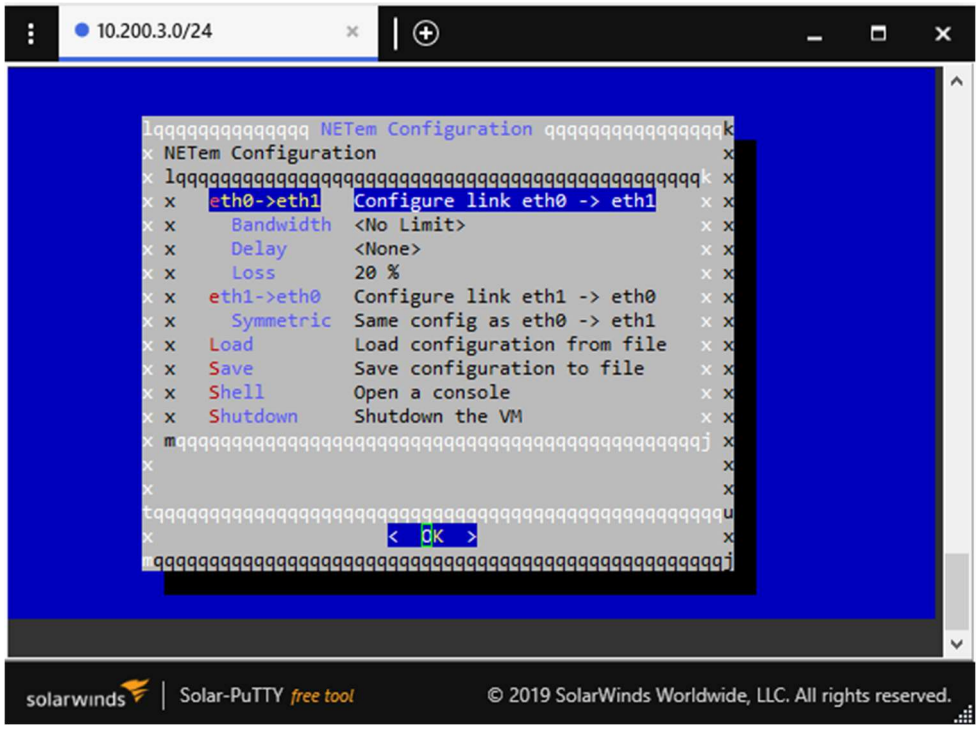


Figura 46. Variación de calidad de tráfico.

Posteriormente se genera tráfico en la red desde el PC1, para determinar por cuál de los enlaces está yendo el tráfico. En la pestaña *Dashboard* > *FortiView Sessions*, se logra evidenciar que el tráfico está siendo desviado a través del enlace WAN3, dado el aumento en la pérdida de paquetes en el enlace WAN2.

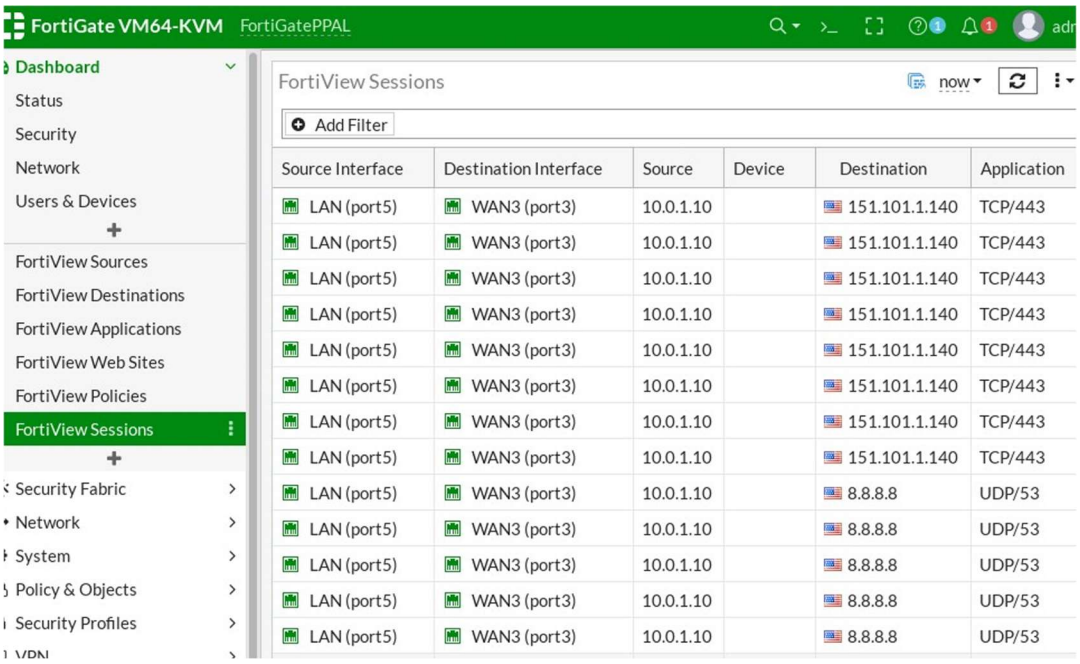


Figura 47. Vista de las sesiones luego de variar pérdida de paquetes.

En la pestaña *Network > Performance SLA,* se puede verificar el estado del enlace. Este debería evidenciar un aumento en el porcentaje de pérdida de paquetes, más no una caída del enlace.

Figura 48. Porcentaje de pérdida de paquetes en los puertos.

Como se muestra en la figura anterior, el enlace no presenta una caída debido a que sigue teniendo conectividad; solo que las pérdidas en el tráfico reducen notablemente los indicadores de calidad en el servicio, por lo cual se procede a migrar el tráfico a través de los enlaces restantes.

Prueba 2. Caída de enlace.

Al eliminar el enlace que se encuentra priorizado para distribuir el tráfico, la herramienta deberá encargarse de encontrar una ruta alterna para que la conexión se siga estableciendo. Para esta prueba, se apagará el enlace WAN3 para determinar si la redistribución se presenta.

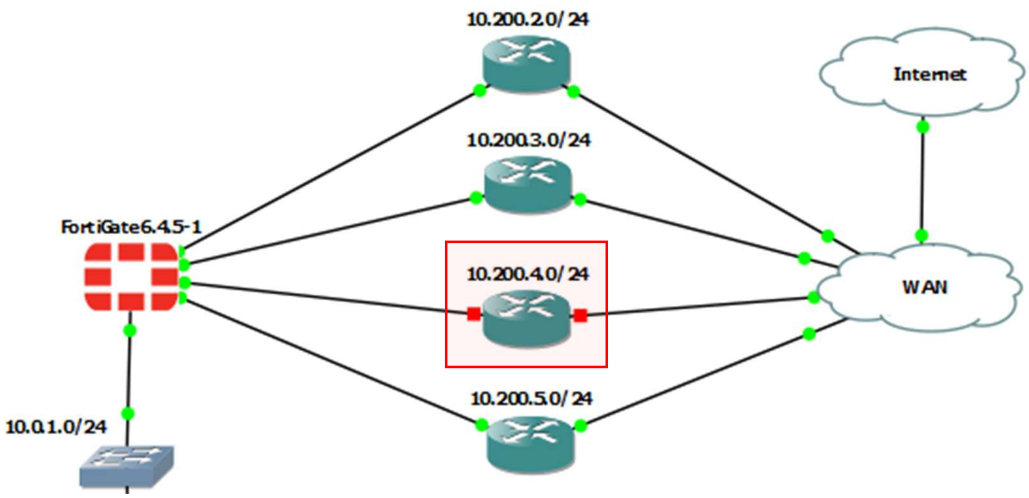


Figura 49. Apagado del enlace WAN3.

Ahora bien, tal como se realizó en la prueba anterior, se genera tráfico desde PC1 y se procede a verificar en la pestaña *Dashboard > FortiView Sessions*.

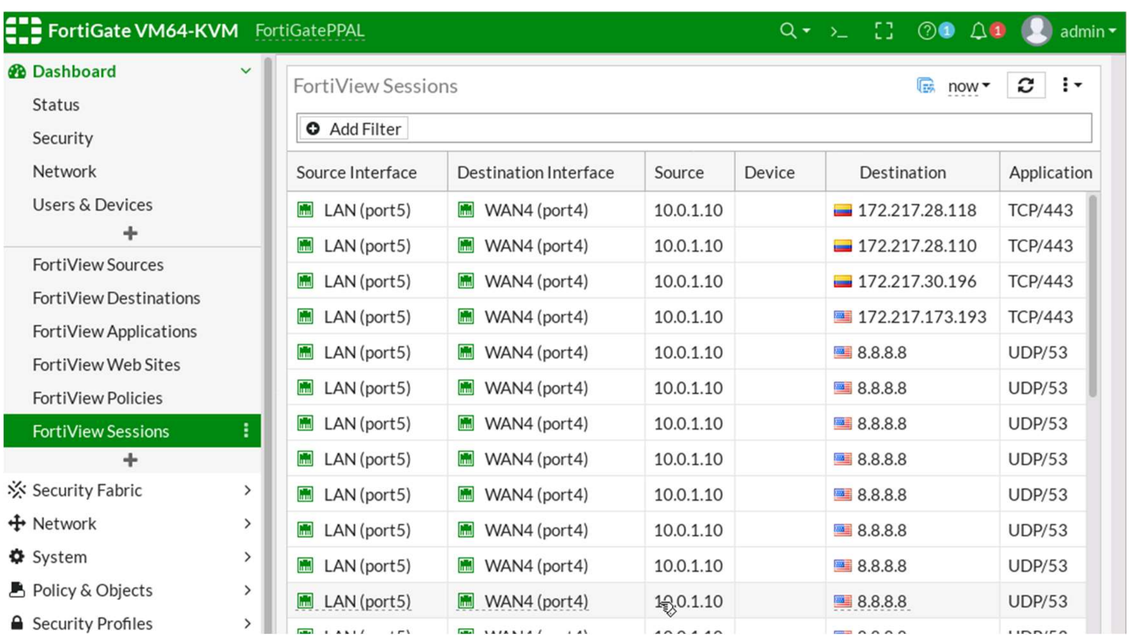


Figura 50. Vista de las sesiones luego de apagar el enlace WAN3.

En el caso de la figura anterior, es priorizado el enlace WAN4, debido a que el enlace WAN2 aún presenta pérdida de paquetes y el enlace WAN3 es el que se encuentra apagado. Nuevamente, en la pestaña *Network > Performance SLA,* se puede verificar el estado de los enlaces.

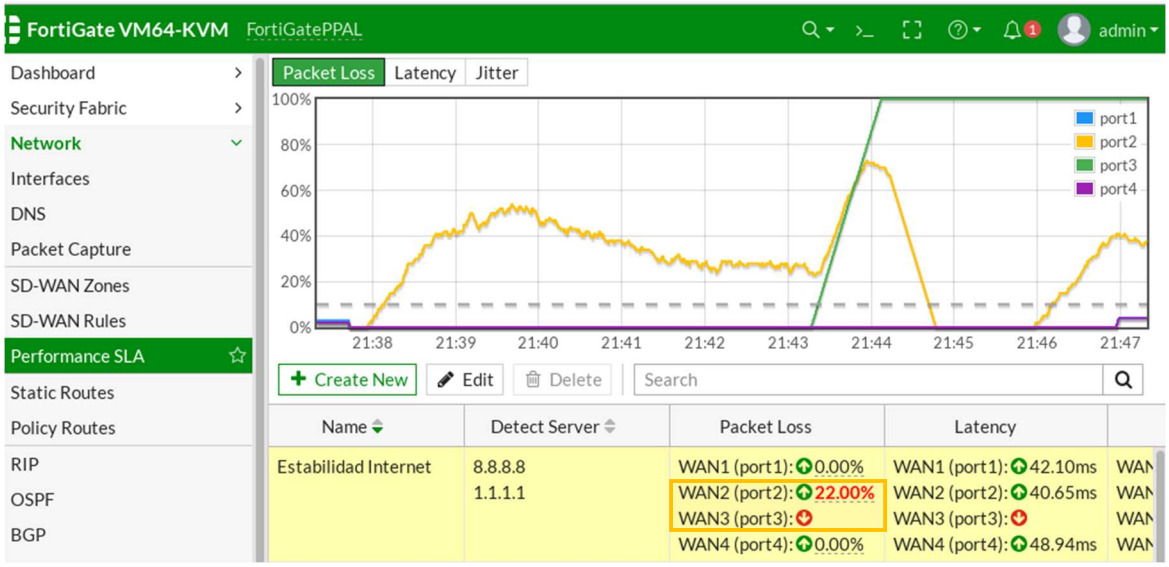


Figura 51. Monitoreo de rendimiento de SLA.

Conclusiones

- La tecnología SD-WAN permite gestionar la red de una manera más automatizada y centralizada, definiendo a través del software cada una de las limitantes y procesos que caracterizan a la red.

- La propuesta se hizo a través del modelo de despliegue SD-WAN basada en Internet, permitiendo una implementación más rápida, con menos requerimientos de hardware y ajustándose a la infraestructura y procesos que la empresa maneja.

- Con el uso de SD-WAN se agrupan funcionalidades que se desarrollaban con servicios adicionales. Por ejemplo, el uso de balanceadores de carga requería de un switch o servidor adicional. Para este caso, el software suple esas necesidades y permite que los servicios se concentren dentro de una sola plataforma de gestión.

- El controlador SD-WAN siempre encontrará rutas alternas para establecer conectividad, dependiendo de las reglas definidas y los enlaces que tenga disponibles.

- La importancia de esta solución, radica en que el usuario final no distingue entre el uso de un enlace u otro para asegurar su conectividad a la red.

Recomendaciones

- Para la instalación del GNS3, se debe ejecutar inicialmente el instalador de la máquina virtual que lo aloja, ejecutar la VM y posteriormente iniciar el software. Esto debido a que la instalación rápida que provee el software en su página web, aun presenta errores de estabilidad y de ficheros al momento de sincronizar la máquina virtual con el software.

- Los errores de sincronización de la aplicación y la VM son frecuentes, por lo cual muchas veces se debe proceder a reiniciar el computador donde se está ejecutando y verificar que el firewall no esté bloqueando el acceso a Internet de los elementos de GNS3 (principalmente el aplicativo Qemu).

- Dado que la licencia de prueba del FortiGate tiene una duración de 15 días, se recomienda usar el comando *exe factoryreset2* cada vez que esta licencia expire. Este comando permite realizar un reseteo de fábrica, sin perder la gestión remota del equipo. No obstante, todas las configuraciones referentes a Políticas de Firewall e interfaces manuales serán eliminadas.

- Para evitar inconvenientes con las configuraciones, se tiene como práctica el uso de *checkpoints* o punto de control. Esto se realiza en la pestaña del Usuario, ubicada en la parte superior derecha, y allí las opciones *Configuration* > *Revisions*. Así se puede ir creando un registro de los cambios realizados, con el objetivo de no afectar los servicios del Firewall y poder gestionar cambios o puntos de restauración con mayor eficacia.

- SD-WAN es una característica incluida en los FortiGate que operen bajo el sistema operativo FortiOS 5.4 o superior. Dado que ya se tienen estos dispositivos dentro de la topología de red de Emtelco, se recomienda actualizar el sistema operativo para implementar esta tecnología.

- A corto plazo, se recomienda cambiar estos Firewall por dispositivos más recientes y que soporten futuras actualizaciones del sistema operativo FortiOS. Esto se recomienda debido a que las actualizaciones incluyen mejoras en características de seguridad y funcionalidades adicionales para el monitoreo de la red.

- SD-WAN tiene una solución Open Source llamada FlexiWAN, por lo cual las características disponibles que varían entre los proveedores del servicio, pueden ser aplicadas a través de este código abierto.

Referencias

Aguilar, L. (Marzo de 2020). *Universidad Tecnológica del Perú.* Obtenido de Propuesta de Diseño de una Red Privada de Telecomunicaciones: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3495/Luis%20Aguilar_Tesis_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y

AprendeIT. (Julio de 2018). *Comandos de utilidad fortinet.* Obtenido de AprendeIT: https://aprendeit.com/top-comandos-de-utilidad-fortinet/

Carrasco, F. (2020). *UCSG.* Obtenido de Diseño y Simulación de una Red de Accesos en GNS3: http://201.159.223.180/bitstream/3317/15699/1/T-UCSG-POS-MTEL-179.pdf

Edge, P. (2019). *E-Prints USQ.* Obtenido de Security in the Software Defined Networking Infrastructure: https://eprints.usq.edu.au/36813/1/Peter_Edge_Thesis_MSCR_2019.pdf

Emtelco. (2021). *Acerca de Emtelco*. Obtenido de Emtelco CX & BPO: https://emtelco.com.co/acerca-de-emtelco/

FlexiWAN. (Agosto de 2019). *FlexiWAN SD-WAN Open Source.* Obtenido de FlexiWAN: https://flexiwan.com/wp-content/uploads/2019/08/flexiWAN-SD-WAN-Open-Source-Overview.pdf

Forninet. (2021). *Fortinet Secure SD-WAN.* Obtenido de Solution Overview and Architecture Guide: https://www.fortinet.com/content/dam/fortinet/assets/deployment-guides/dg-secure-sd-wan-architecture-guide.pdf

Fortinet. (Agosto de 2018). *FortiGate Secure SD-WAN Solution* . Obtenido de Magellan Netzwerke: https://www.magellan-net.de/files/magellan/content/Downloads/alte-website/Webinar_FortiGate_SecureSDWAN.pdf

Fortinet. (2018). *Fortiview.* Obtenido de Fortinet Help: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1900_FortiView/0000_FortiView.htm

Fortinet. (2021). *Next-Generation Firewall FortiGate de rango medio*. Obtenido de Fortinet: https://www.fortinet.com/lat/products/next-generation-firewall/mid-range

Fortinet. (s.f.). *Performance SLA - link monitoring.* Obtenido de Fortinet Document Library: https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/478384/performance-sla-link-monitoring

GNS3. (2021). *GNS3 Documentation.* Obtenido de Getting Started with GNS3: https://docs.gns3.com/docs/

GNS3. (2021). *GNS3 Marketplace*. Obtenido de GNS3: https://www.gns3.com/marketplace

GNS3. (2021). *GNS3 Windows Install.* Obtenido de GNS3 Documentation: https://docs.gns3.com/docs/getting-started/installation/windows

GNS3. (2021). *The NAT node.* Obtenido de GNS3 Docs: https://docs.gns3.com/docs/using-gns3/advanced/the-nat-node/

Icorp. (2019). *¿Qué es el SD-WAN del nuevo FortiGate?* Obtenido de Icorp: http://www.icorp.com.mx/blog/que-es-el-sd-wan-de-fortigate/

Karkhanawala, S. (5 de Agosto de 2021). *What is SDWAN and Which One is Right for Your Business?* Obtenido de Aryaka: https://www.aryaka.com/blog/what-is-sd-wan-which-one-right-for-your-business/

Lee, G. (2014). *Cloud Networking.* Elsevier Inc.

Lopez, J. (2020). *Biblioteca Digital EPN.* Obtenido de EMULACIÓN DE UNA RED SD-WAN UTILIZANDO TECNOLOGÍA FORTINET Y EL SOFTWARE GNS3: https://bibdigital.epn.edu.ec/bitstream/15000/21163/1/CD%2010688.pdf

MEF. (Noviembre de 2020). *MEF 3.0 SD-WAN & SASE FAQ.* Obtenido de MEF: https://www.mef.net/wp-content/uploads/2020/11/MEF-3-0-SD-WAN-and-SASE-FAQ-v10.pdf

Sakir, S., Scott-Hayward, S., & Kaur, C. P. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, 36-43.

Sambrano, J. (Diciembre de 2020). *Universidad de las Fuerzas Armadas.* Obtenido de Implementación de Redes SDN-WAN y evaluación de resultados sobre aplicaciones: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/23406/T-ESPE-044177.pdf?sequence=1&isAllowed=y

Suárez, D. (2020). *Universitat Oberta de Catalunya.* Obtenido de Redes WAN definidas por software: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/116386/8/astifrTFG0620memoria.pdf

VMWare. (2021). *Hipervisor*. Obtenido de VMWare Glosario: https://www.vmware.com/latam/topics/glossary/content/hypervisor.html