Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

DISEÑO DE UNA SD-WAN PARA COMUNICACIÓN DE ALTA REDUNDANCIA ENTRE ENLACES DE INTERNET

.

AUTOR:

ZABDIEL DAVID ESTUPIÑAN ESTÉVEZ

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE TECNOLOGÍA DE LA INFORMACIÓN

QUITO, DM, 2022

DEDICATORIA

Este trabajo de titulación se lo dedico a mi familia, los cuales siempre han estado en mis momentos buenos y malos mostrando su apoyo verdadero y siendo el pilar fundamental para seguir luchando día tras día por convertirme en un buen profesional y ser humano, a mis amigos de la carrera los cuales han hecho que esta etapa de mi vida fuera más fácil de manejar y más divertida de llevar. También dedico este trabajo a un gran amigo, Miguel Andrade que, desde el principio de la carrera, ha estado allí compartiendo buenos momentos de alegrías, preocupaciones y tristezas y que, por temas de salud, no pudo continuar con sus estudios ni graduarse junto con todos los que lo queremos.

AGRADECIMIENTO

Quiero agradecer a Dios por permitirme cumplir un sueño más en mi vida, el ser un profesional en un área que me apasiona (Tecnología de la Información).

A mis padres y hermana que, a pesar de todo, siempre estuvieron a mi lado en todo el proceso, alentándome y sosteniéndome cuando sentía que no podía más.

A mis amigos que, semestre tras semestre nos hemos ayudado mutuamente en el área del estudio aun sabiendo que al finalizar esta etapa seremos competencia en el mundo laboral.

A la Ingeniera Suyana Arcos que, con su sabiduría, inteligencia y experiencia ha sabido guiarme para culminar este trabajo con éxito y seguir mi camino para convertirme en un profesional.

Y finalmente, a Mary Ochoa, compañera de trabajo quien, a pesar de sus múltiples tareas y su poco tiempo disponible, estuvo allí ayudándome y alentándome para desarrollar y culminar con éxito este trabajo de titulación.

RESUMEN

Este proyecto surge de la necesidad de las empresas por la búsqueda de una mejor optimización de recursos tecnológicos, reducción de gastos y automatización de procesos que garantice una escalabilidad, flexibilidad y disponibilidad efectiva. Como respuesta a esta necesidad surge SD-WAN (Red de área amplia definida por software) que, con sus múltiples beneficios, brinda la posibilidad de hacer que una empresa u organización rompa el esquema tradicional y extienda su campo de visión a nuevas tecnologías. La red SD-WAN tiene un catálogo amplio de servicios y aplicaciones, por lo que, con ayuda de un emulador, se realizará la investigación que demostrará una alta redundancia o disponibilidad entre enlaces de internet adoptando la tecnología mencionada.

Abstract

This project arises from the need of companies in search of a better optimization of technological resources, cost reduction and process automation that guarantees scalability, flexibility and effective availability. In response to this need, SD-WAN (Software Defined Wide Area Network) arises, which, with its multiple benefits, offers the possibility of making a company or organization break the traditional scheme and extend its field of vision to new technologies. The SD-WAN network has a wide catalog of services and applications, so, with the help of an emulator, the investigation will be carried out that will demonstrate a high redundancy or availability between internet links adopting the mentioned technology.

ÍNDICE

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: MARCO DE REFERENCIA

1. Justificación

La tecnología va avanzando cada año de manera significativa, por lo que adoptar nuevas tendencias en las empresas es algo indispensable tanto para su crecimiento como para su competitividad.

Como menciona Castellano (2020) “La era digital está en la puerta de las nuevas generaciones, es nuestra permutación constante del conocimiento humano, conocido hoy día como la cuarta revolución o “INDUSTRIA 4.0””. (p.3)

Normalmente las grandes empresas cuentan con enlaces de internet que se usan para el tráfico de red en cuanto a conexiones a páginas externas de la organización, la mayoría de estas empresas configuran dichos enlaces de manera manual, lo que hace un trabajo pesado y tedioso para el personal de IT ya que tienen que analizar que aplicación irá porque enlace de internet muchas veces saturando la red e impidiendo el trabajo fluido de los colaboradores.

Este proyecto tiene como objetivo simular una Red (SD-WAN) entre centros de datos para enlaces de internet, con el fin de optimizar y balancear el tráfico de red. Esto permitirá una alta redundancia en cuanto a conectividad de enlaces eliminando la saturación o cuellos de botella que se puede presentar si estos se configuran manualmente, ya que SD-WAN determina qué enlace tiene mayor ancho de banda para pasar las aplicaciones con prioridad alta por ese canal.

2. Planteamiento del problema

Algunas empresas de tipo financiero o de servicios tienen enlaces de internet por los cuales se direccionan las diversas aplicaciones o servicios, si bien es conocido dichos enlaces tiene uno o varios proveedores que lo configuran, el direccionamiento de estos servicios está configurado de

manera manual, y estos dependen de un factor humano para levantarse o redireccionarse en caso de caídas o desconexiones.

Para solventar esta problemática, se plantea diseñar una red (SD-WAN) para enlaces de internet, ya que la mayoría de servicios o peticiones de los usuarios dentro de una organización realizan es a páginas externas. Dentro de esta tecnología se cuenta con un balanceo automático del tráfico de red, es decir que SD-WAN analiza el ancho de banda de los diferentes canales y direcciona los servicios dependiendo su prioridad e importancia, evitando la saturación de red y optimizando los recursos.

Este diseño se realizará mediante el simulador GNS3, debido a que es un software completo para el diseño y emulación de redes con versión gratuita y de prueba que permite crear Centros de Datos completos y emular diseños de redes mostrando el monitoreo en tiempo real del tráfico de datos.

3. Objetivo General

Diseñar una SD-WAN para comunicación de alta redundancia entre enlaces de internet

4. Objetivos Específicos

- Diseñar dos segmentos de proveedores de enlaces de internet de una institución financiera.
- Utilizar SD-WAN para conectar dos segmentos de enlaces de internet de una institución financiera.
- Analizar el monitoreo de red entre dos segmentos de enlaces de internet de la institución financiera para evidenciar alta redundancia.

5. Antecedentes

El presente trabajo acerca del diseño de una SD-WAN para comunicación de alta redundancia entre enlaces de internet, estará basado en revisiones de fuentes bibliográficas junto con otros trabajos y artículos de investigación relacionados con el área de redes WAN, SD-WAN, mejoras de tráfico de internet, etc.

Se define a una red WAN como una red de área local, la cual se basa en conectar varias redes LAN entre sí con el objetivo de tener conectados a los usuarios conjuntamente, en tiempo real y sin importar la distancia, teniendo una comunicación de voz, datos y video al instante. Un claro ejemplo de esto es el propio internet ya que este abarca una zona geográfica que se extiende desde ciudades hasta continentes, permitiendo conectar a personas de todo el mundo en segundos.

Actualmente, el crecimiento de datos en los bancos ha hecho que la infraestructura de redes presente quede corta para la gran cantidad de información que se transmite diariamente por los diferentes enlaces tanto de datos como de internet, por lo que optar por seguir usando o implementado una red tipo WAN no es una opción viable para el crecimiento y la escalabilidad de la empresa debido a que es necesario adoptar una tecnología que ofrezca mayor fluidez y seguridad para con los datos, y las redes WAN se limitan en muchas ocasiones a esta problemática.

Hoy en día una infraestructura que opte por WAN se encontrará con varias desventajas, una de las principales es la seguridad. Este tipo de redes no destaca por ofrecer una seguridad estable a sus usuarios. Otra desventaja que las empresas encuentran es el tema de costes, debido a que las WAN tienen un grado de complejidad alto, el implementarlas tiene un costo elevado dependiendo directamente de que tan grande sea la red por la cual optar.

Por estas razones surge la solución de diseñar una SD-WAN la cual permite una comunicación de alta redundancia más eficiente y con mayor seguridad.

Para este trabajo de se tomará como referencia y guía las siguientes investigaciones relacionadas con el tema principal:

Diseño de un banco de pruebas virtualizado usando la tecnología SD-WAN en dónde Vélez Álvaro y Vera (2021) encontraron una necesidad en su Universidad (Politécnica Salesiana) la cuál era que no contaban con un banco de pruebas virtualizado y se necesitaba ambiente en donde docentes y estudiantes puedan realizar pruebas, configurar diferentes dispositivos, verificar la confiabilidad de la red y así tengan un mejor aprendizaje. Lo interesante de este proyecto es que no se centran en usar una red típica como WAN, LAN, etc. Sin no que se implementa una tecnología nueva para muchas personas, pero muy potente. Por esta razón se escogió esta tesis como guía para el trabajo actual.

Diseño de una Red de Accesos utilizando tecnología SD-WAN para medianas empresas, en el cuál Cabrera (2020) considera que la tecnología vigente dentro de las medianas empresas no es suficiente para el crecimiento progresivo que las mismas tienen juntamente con la evolución de la tecnología, por lo que buscaron una solución o alternativa a esta problemática llegando así a diseñar e implementar SD-WAN, tecnología que garantiza una optimización de recursos, reducción de gastos y mayor versatilidad y crecimiento a la organización.

6. Alcance

Este trabajo tiene como alcance el diseño de una Red SD-WAN para comunicación de alta redundancia entre dos segmentos de proveedores de enlaces de internet de una institución financiera mediante el uso de herramientas de simulación como GNS3 la cual permite diseñar y monitorear tráfico de red en tiempo real. Este tema se llevará a cabo debido a que se identificó

que varias empresas tienen sus enlaces de internet configurados de manera manual lo cual hace que la conectividad de enlaces sea deficiente y que, al momento de existir caídas, los usuarios o funcionarios de la empresa tengan que esperar cierto tiempo para volver a tener conectividad causando molestias y pérdidas de productividad para la organización.

Como resultado de este trabajo se presentará el diseño completo que compete a la Red SD-WAN funcionando en conjunto con los dos segmentos del Centro de Datos al igual que un informe donde se evidencie el monitoreo de la red y se demuestre la alta redundancia y que, en efecto, implementar esta tecnología ayudará a las empresas a optimizar y balancear de manera automática el tráfico de red por los diferentes canales de enlaces con los que la organización cuente.

7. Metodología

Como metodología para este diseño, se establecieron las siguientes fases:

- Elaboración de plan de diseño: En esta fase se deberán establecer los puntos u objetivos principales, secundarios y terciarios. De igual manera se definirán los indicadores para determinar si el diseño creado es el adecuado a la solución de la problemática propuesta. Entre los indicadores se tiene:
    - Tiempo de respuesta
    - Costo de implementación
    - Escalabilidad
    - Seguridad
- Análisis de Red en sitio: Esta fase nos servirá para evaluar el estado de las redes ya existentes de manera general dentro de las diferentes organizaciones o empresas evaluando el tráfico de la red, fallas, puntos a mejorar, topología de red, etc.

- Nuevas exigencias: Plantearse preguntas tales como:
    - ¿Necesitan adoptar nuevas tecnologías las empresas necesariamente?
    - ¿Las empresas piensan expandirse más?
    - ¿La infraestructura actual amenora la producción de una organización?
- Viabilidad del diseño: Estudio del éxito o fracaso del diseño a simular. Dentro de este estudio se incluirá:
    - Viabilidad Técnica: Recursos tanto de Hardware como de Software que sean necesarios.
    - Viabilidad Funcional: Efecto que tendrá este diseño dentro de una organización.
- Configuración: Diseño de la Red propuesta en donde se evidenciará el monitoreo del tráfico de red.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. Marco Teórico

2.1. Redes de comunicación

Una definición técnica para “redes de comunicación” es que son un conjunto de equipos de comunicación con la capacidad de transmitir información a través de señales electromagnéticas entre diversos puntos ya sea analógica o digitalmente. Estas redes están fundamentadas en infraestructuras físicas (cableado) o inalámbricas.

Dentro de las grandes empresas, PYMES o micro emprendimientos, es necesario contar con una infraestructura de red estable, fluida y segura con la finalidad de que los datos que se manejan dentro de estas organizaciones puedan ser compartidos o transmitidos de manera protegida y que estos estén disponibles para todas las partes pertinentes.

Para lograr dicho cometido, las redes de comunicación cuentan con ciertas características que permiten que la transmisión de información sea efectiva. Entre las características se pueden apreciar:

- **Velocidad**

Se refiere a la rapidez o prontitud con la que se produce la transmisión de datos o información a través de la red. La velocidad normalmente se mide a través de un testeo en dónde se monitoreará la subida y descarga de la transmisión de datos, los cuales variaran dependiendo los estándares y protocolos que se utilicen para la configuración de los segmentos de redes. De igual manera este monitoreo dependerá del canal o medio por el que los datos son enviados (fibra óptica, inalámbrica, coaxial, etc.). Por ejemplo, entre una red cableada y una red inalámbrica, la red cableada, en la mayoría de casos, será más rápida

- **Seguridad**

Tanto las redes cableadas como las inalámbricas deben estar protegidas de manera robusta, ya que existen agentes externos que siempre querrán atacar y robar la información y datos con los que la empresa cuenta. Para esto la organización deberá contar con protocolos y estándares que aseguren la protección de datos. Entre los más conocidos se encontrarán:

- **TCP/IP:** Es un protocolo muy utilizado para la comunicación de equipos dentro de una red. TCP/IP está fundamentando en el modelo OSI. Debido a que es un modelo muy conocido, en toda organización es fundamental conocerlo, ya que facilita la configuración de redes básicas que trabajan con enlaces de internet. Tal y como lo menciona Estrada (2018), "El protocolo TCP/IP representa, entonces, las reglas que hacen posible la conexión de computadoras de marcas y tecnología diferentes."

  Dicho protocolo se divide en dos partes. TCP "Protocolo de Control de Transmisión", permite disponer de una conexión y mediante esta surge el intercambio de datos, generando así un medio seguro de datos. IP "Protocolo de Internet", se basa en un conjunto de normas o reglas que permiten el correcto enrutamiento y direccionamiento de paquetes, transportando los datos de una máquina a otra de la red.

- **POP:** Este protocolo, es más usado en lo referente a servicios de correo. Se encarga de fijar una conexión entre cliente – servidor de correo con el fin de una correcta gestión de envíos de paquetes o mensajes. Funciona tal que, el servidor de correo recibe el mensaje y, mediante el protocolo POP, este los envía al cliente de destino "agente que usa el correo". Se pueden enviar de dos maneras distintas. La primera es dejando una copia dentro del servidor de correo y la segunda, se moverá el correo

hacia el cliente directamente. Por ejemplo, para servicios de Gmail, Google (2020) nos menciona que, "El protocolo POP sirve para sincronizar el correo electrónico de Gmail con cualquier cliente de correo compatible, como Outlook, Thunderbird o Apple Mail."

- **SMTP:** Este protocolo va de la mano con TCP/IP y POP3, ya que sirve de igual manera cuando se tiene un servidor de correo y es usado cuando se realice una transferencia de información entre el cliente y el servidor de correo. Como lo menciona Sendinblue (2022), "Un servidor SMTP es simplemente el servidor que recibe, maneja, transfiere o almacena mensajes de acuerdo con las reglas de SMTP (el protocolo de comunicación)." Su punto fuerte es que funciona como protector, de manera que filtra todos los mensajes recibidos y enviados. De igual manera es capaz de limitar el número de correos que un agente puede enviar en un período de tiempo.
- **HTTPS:** Este protocolo es usado dentro de la World Wide Web en el cual, los datos de las páginas o aplicaciones web se transfieren alrededor de una red. Es una versión encriptada del protocolo HTTP, es decir más robusta y segura verificando así que el sitio web que se visite sea legítimo. Según Baldikov (2022), "Con el protocolo HTTPS se consigue que los datos de la web queden encriptados y que nadie pueda tener acceso a los mismos, aunque encontrase la manera de acceder."

- **Confiabilidad**

Según García (2014), "Es la probabilidad de que un componente o sistema pueda cumplir su función en las condiciones operativas especificadas durante un intervalo de tiempo dado."

La confiabilidad se encuentra basada en la probabilidad de hallar fallos o averías dentro de los nodos de la red. Es importante tenerlo en cuenta, ya que, depende de la topología de red que se esté usando y si un componente llegará a fallar, afectaría todo el funcionamiento de la red construyendo así un problema local. Para solventar esta problemática se buscó implementar un hardware redundante, para que así, en caso de algún fallo o avería, la tolerancia de errores sea baja y todos los sistemas puedan seguir trabajando con normalidad.

- **Escalabilidad**

Esta es una característica muy importante dentro de las empresas, ya que, para que la organización pueda ser más competitiva y crecer de una buena manera, es importante percibir la posibilidad de agregar o cambiar componentes tanto de hardware como de software para mejorar el rendimiento de la red. En otras palabras, es la capacidad que tiene una organización para la ampliación de sus sistemas informáticos con el fin de satisfacer las necesidades organizacionales. Así como lo menciona Arroyo (2016), "Los emprendimientos económicos y sociales persiguen diferentes fines, sin embargo, ambos requieren de la escalabilidad para crecer sin perder clientes, disminuir la calidad o cambiar la proposición de valor de la organización."

- **Disponibilidad**

La disponibilidad se refiere a la capacidad que una red tiene para estar apto y activo siempre y cuando se lo necesite. Como lo describe Grajales (2017), "En este mundo globalizado y altamente competitivo, el conocimiento técnico - científico es cada vez más necesario, siendo la confiabilidad, la disponibilidad y la mantenibilidad tres disciplinas que lo pueden propiciar." Este principio deberá asegurar la fiabilidad y acceso adecuado a los recursos por parte de los agentes interesados y/o autorizados.

2.2. ¿Qué es la segmentación de red?

La segmentación de la red es una técnica que consiste en dividir una red grande en varias subredes lo cual permite, a los equipos que se encuentran en red, compartimentar dichas subredes. Esto se realiza con el fin de otorgar permiso, controles, servicios únicos por cada subred. Tal y como lo menciona Fernández (2020), “Es un proceso que se encarga de dividir la red en pequeñas redes. Tiene el propósito de mejorar el rendimiento de la red, y, sobre todo, sus condiciones de seguridad.”

De igual manera se extrae una definición de parte de, VMware (2022), “El proceso de segmentación de red implica dividir una red física en diferentes subredes lógicas. Una vez la red se ha subdividido en unidades más pequeñas y manejables, se aplican controles a los segmentos individuales compartimentados.”

Una segmentación de red no es simplemente la división de la misma, esta deberá responder a ciertas preguntas que responden a la necesidad de la organización, estas son:

- **¿Dónde?:** Esta pregunta dará respuesta a la ubicación o establecimiento en los que se ubicaran los puntos de segmento de red y, de igual manera, la lógica que estos usan para aplicar la segmentación de los activos tecnológicos con los que la empresa cuente.
- **¿Cómo?:** Esta pregunta se refiere a la implementación de las metas de negocio vinculado con los controles de acceso refinados.
- **¿Qué?:** Será el encargado de reforzar los controles de acceso por medio de la aplicación de protocolos o medidas de seguridad.

2.3. Funcionamiento de la segmentación de red

2.3.1. Segmentación en base al perímetro

En este tipo de segmentación, se crean subredes internas y externas basados en el principio de la confianza, es decir, los elementos internos son considerados como fiables, mientras que los externos no.

Una de las herramientas más usadas o conocidas para este tipo de segmentación es el cortafuegos. Esta herramienta es utilizada para el control del tráfico “norte a sur” de la red, sin embargo, permitía la comunicación directa entre los elementos que se encontraban dentro del mismo segmento.

2.3.2. Virtualización de red

VMware (2020) nos dice que, “Hoy en día, muchas organizaciones mantienen una variedad de áreas de red con funciones específicas que requieren la segmentación en muchos puntos de la red.”

Debido a esta problemática, la segmentación en base al perímetro está quedando olvidada. Una causa de esta difusión es la aparición de la nube y el término (BYOD). Actualmente, para poder mejorar la administración, optimización, segura y rendimiento de la red, es necesario realizar una segmentación más profunda y aquí es donde entra la virtualización de red.

Dicha virtualización se entiende como el aprovisionamiento tanto de los servicios de red como de la seguridad de la IT. Al realizar una segmentación completa de la red y no solo del perímetro, la virtualización es primordial para que dicho segmento sea más eficiente.

2.4. Topología de Redes

Según la Real Academia Española (2021), "trata especialmente de la continuidad y de otros conceptos más generales originados de ella, como las propiedades de las figuras con independencia de su tamaño o forma," (p.1)

Para contar con una correcta manipulación de la información, una empresa u organización debe contar con redes de telecomunicación efectivas con el objetivo de proteger la información al momento de compartirlas con los agentes interesados o involucrados.

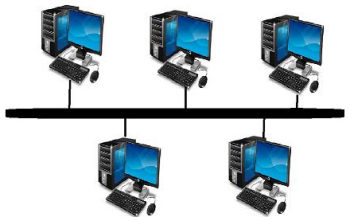
Dentro de las redes de comunicación existen varios tipos de estas las cuales serán escogidas dependiendo la necesidad que la empresa tenga en ese momento, por eso es importante conocer los tipos de redes más utilizadas dentro de las empresas.

2.4.1. En bus

Esta topología se basa en tener un único canal de comunicación (bus) mediante el cual se conectan los diversos dispositivos, por lo que todos los dispositivos conectados comparten el mismo canal. Una de las características principales de esta red, es que no necesita de muchos cables para la instalación y es relativamente fácil de implementar. Desde una vista técnica, como indica Julia (2018), "Habrá una serie de derivadores T, que son las ramas a las que se conectan los equipos informáticos." Una de sus mayores ventajas es el precio de su adquisición e implementación, ya que, a comparación de otras topologías, esta necesita una menor longitud de cableado.

Figura 1

Red en bus



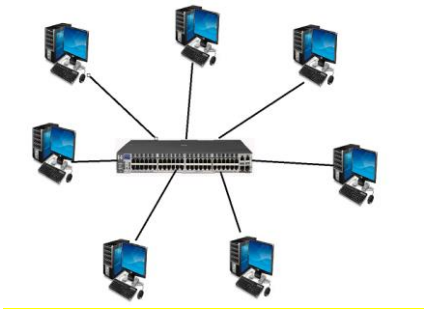
Nota. Dentro de la topología de red existe el tipo “bus” que se identifica como se muestra en la imagen.

2.4.2. En estrella

En esta topología, las estaciones de trabajo están conectadas a un sitio central. Este tipo de red es usado normalmente en empresas u organizaciones donde la comunicación es unidireccional, esto quiere decir que existe un agente central (usualmente el gerente) y los subordinados se encuentran alrededor de este. Una de ventajas es la facilidad que existe al momento de agregar nuevos equipos, ya que estos únicamente deberán conectarse al punto central y realizar la configuración respectiva. Según Álvarez (2015), “Suelen ser más estructuradas que en el caso del cableado en bus”. De igual manera este tipo de red es tolerante a fallos, es decir, que cuando una estación de trabajo deja de funcionar o tiene algún tipo de problemas, las demás estaciones o equipos no se verán afectados en lo absoluto.

Figura 2

Red en estrella



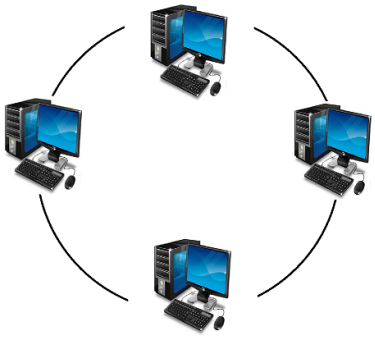
Nota. Dentro de la topología de red existe el tipo “estrella” que se identifica como se muestra en la imagen.

2.4.3. En anillo

Este tipo de red tiene la característica de que se conecta directamente con otros dos nodos o equipos. Esto permite el intercambio de información de una manera más ordenada haciendo que la transmisión sea de un nodo a otro hasta llegar al origen. Así como lo mencionan Casillas y Dominguez (2009), “Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.” Una de sus mayores desventajas es que cada nodo tiene contacto únicamente con los dos adyacentes. Sin embargo, esta red favorece al envío y recepción de los datos, resolviendo problemas de manera eficiente dejando a un lado los rangos o posiciones de cada nodo (usuario).

Figura 3

Red en anillo



Nota. Dentro de la topología de red existe el tipo “anillo” que se identifica como se muestra en la imagen.

2.4.4. En malla

Este tipo de red es lo contrario a la “Red en anillo” ya que cada nodo está conectado con el que quiera sin seguir un orden. Esto permite que todos los agentes de la organización puedan procesar la información con cualquier agente que se encuentre dentro de la empresa. De igual manera que en la anterior red, los rangos o jerarquías no intervienen.

Figura 4

Red en malla

Nota. Dentro de la topología de red existe el tipo “malla” que se identifica como se muestra en la imagen.

“Seleccionar el tipo de red comunicación más adecuado en una empresa no es fácil, por tal razón se recomienda acudir con un experto en el área que lleve a cabo el análisis, evaluación e implementación del mejor sistema.” (El Equipo de Marketing, 2016).

2.5. Tipos de Redes de Comunicación

2.5.1. Redes LAN

LAN “Red de Área Local, Local Area Network”, este tipo de red abarca espacios de cobertura muy pequeños, limitando a edificios, casas, por lo que se utiliza mucho dentro de escuelas, negocios, etc. Según Tanenbaum, (2012) “Las redes LAN las redes de área local, generalmente llamadas LAN (local área networks), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión.” Mediante esta red se podrá compartir recursos entre equipos, siempre y cuando se lo realice mediante cables Ethernet, es decir, los dispositivos relacionados estarán conectados mediante un router. Este tipo de red, permite al cliente una conexión a servidores internos, sitios web, etc.

2.5.2. Redes MAN

MAN “Red de Área Metropolitana, Metropolitan Area Network”, se podría definir a esta red como la hermana mayor de las redes LAN, ya que su extensión geográfica crece, expandiéndose a conexiones entre ciudades y regiones metropolitanas. Así como lo menciona Tanenbaum (2012) “Una red de área metropolitana o MAN (Metropolitan Área Network) es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar.” Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública. Este tipo de redes conectan varias LAN con ayuda de la fibra óptica.

2.5.3. Redes WAN

WAN “Red de Área amplia, Wide-Area Network”, es un tipo de red que conecta a las redes LAN, a comparación de la anterior, esta abarca espacios más grandes, una extensión de países y hasta continentes.

Como menciona Farrell (2018), “Las redes WAN son redes de área amplia (Wide Area Network). WAN es una red de ordenadores que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes.” Una red WAN muy conocida es el internet, ya que este te permite conectarte con usuarios de todas partes del mundo en tiempo real permitiendo una transaminación de datos o información inmediata.

De esta manera, se entiende que la red WAN no conecta varios ordenadores o equipos, si no que conecta varias redes LAN o MAN, estas están basadas en el modelo OSI, utilizando tres tipos de capas; capa física (Capa 1), capa de enlace (Capa 2), capa de red (Capa 3).

2.6. Protocolos de Redes de Comunicación

Se define como protocolo a un conjunto de reglas y estándares que están conformados por restricciones, formatos y procedimientos que establecen la comunicación de paquetes para así obtener una comunicación segura entre dos servidores o más dispositivos a través de la red.

Según lo menciona Herrero (2012), “El protocolo se ha convertido en una herramienta estratégica de comunicación de las empresas, tanto a nivel interno y corporativo como en su proyección externa.”

Estos están basados en el modelo OSI, ya que este proporciona una organización de los protocolos en cada capa del modelo. A continuación, se conocerán los protocolos más conocidos dependiendo la capa del modelo OSI.

Protocolos capa 1 (Capa Física)

- Ethernet: Ethernet physical layer (Capa Física de Ethernet).
- DSL: La transmisión de los datos se efectúa por medio de hilos telefónicos.
- Etherloop: Es una combinación entre Ethernet y DSL.
- Frame Relay.

- SONET: Red óptica sincronizada.

Protocolos capa 2 (Enlaces de datos)

- FDDI: Interfaz de distribución de datos en fibra.
- STP: Spanning Tree Protocol (protocolo del árbol esparcido).
- VTP VLAN: trunking virtual protocol para LAN virtual
- MPLS: Multiprotocol Label Switching (Conmutación multiprotocolo de la etiqueta)
- HDLC: High-Level Data Link Control (Control de enlace de datos de alto nivel)

Protocolos capa 3 (Red)

- ARP: Address Resolution Protocol (Protocolo de resolución de direcciones).
- IPv4: Internet Protocol version 4 (Protocolo de Internet versión 4).
- IPv6: Internet Protocol version 6 (Protocolo de Internet versión 6).
- ICMP: Internet Control Message Protocol (Protocolo de control de mensajes de Internet)
- OSPF: Open Shortest Path First (Abrir primero la ruta más corta)

Protocolos capa 4 (Transporte)

- TCP: Transmission Control Protocol (Protocolo de control de transmisión)
- UDP: User Datagram Protocol (Protocolo de datagramas de usuario)
- DCCP: Datagram Congestion Control Protocol (Protocolo de Control de Congestión de Datagramas).

Protocolos capa 5 (Sesión)

- SMB: Server Message Block (Bloque de mensajes del servidor)
- SMPP: Short message peer-to-peer (Mensaje corto punto a punto)
- NFS: Network File System (Sistema de archivos de red)

- SDP: Session Description Protocol (Protocolo de descripción de sesión).

Protocolos capa 6 (Presentación)

- TLS: Transport Layer Security (Seguridad de la capa de transporte)
- XDR: eXternal Data Representation (Representación de datos externos)
- SSL: Secure Sockets Layer (capa de sockets seguros)
- MIME: Multipurpose Internet Mail Extensions (extensiones multipropósito de correo de internet).

Protocolos capa 7 (Aplicación)

- Telnet: Protocolo de telecomunicaciones de red
- POP3: Post Office Protocol (Protocolo de oficina de correo)
- DNS: Domain Name System (Sistema de nombres de dominio)
- DHCP: Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host)

2.7. Red MPLS

Una red MPLS es una solución para los problemas de conexión fluida. Según RedHat (2022), "es una tecnología diseñada para mejorar la velocidad y la eficacia del reenvío de datos a través de las redes de gran tamaño o en las ubicaciones del extremo de la red."

Como lo menciona Cisco (2016), "MPLS es una tecnología de reenvío de paquetes que utiliza etiquetas para tomar decisiones de reenvío de datos. Con MPLS, el análisis del encabezado de la capa 3 se realiza solo una vez (cuando el paquete ingresa al dominio MPLS)."

Estas redes fueron diseñadas con el fin de unir tanto el servicio de envíos de datos para redes que son basadas en circuitos como para dichas redes que son basadas en paquetes o tramas.

2.7.1. Funcionamiento de la red MPLS

La manera en que las redes MPLS se interconectan es con la incorporación de un encabezado que contiene ciertas etiquetas agrupadas, en cada paquete de datos que se envía por medio de la red, estos pueden ser voz, imagen, video, texto. Esto se realiza con el fin de establecer circuitos vitales para poder alcanzar el destino. Es decir, este tipo de red es la encargada de implementar tanto enrutadores como etiquetas para así enviarlas por un camino de baja latencia, permitiendo una mejor velocidad al momento de transmitir datos como voz o imágenes. Otro funcionamiento de este tipo de redes según Tapasco (2018), "MPLS separa los dos componentes funcionales de control (enrutamiento - routing) y de envío (conmutación - forwarding)."

2.7.2. Elementos para una red MPLS

Para una correcta implementación, esta red deberá contar con los siguientes elementos:

- **Etiqueta**

Una etiqueta contendrá toda la información acerca de los enrutadores que MPLS utiliza, esto con el fin de determinar la trama o ruta que se deben reenviar los datos y así lograr una buena velocidad en su transmisión.

- **Bits Experimentales**

Estos serán usados para garantizar una mejora en la calidad de servicio. El uso de este elemento hará que ciertos paquetes puedan tener prioridad sobre otros dependiendo que tareas estén realizando los usuarios de red y así optimizando dicho proceso.

- **Parte inferior de la pila**

En este elemento se mostrará el mensaje que dará aviso a los enrutadores que ya no existen paquetes por compartir y los anteriores fueron enviados de manera correcta.

- **Tiempo de vida**

Finalmente, el tiempo de vida se refiere a las veces que el paquete podrá ser enviado sin ser descartado.

2.7.3. Ventajas de una red MPLS

El contar con una red MPLS dentro de las empresas tiene muchos beneficios, así como lo menciona García (2018), “Además, se garantiza la calidad del servicio (QoS) brindando 4 clases de servicio (CoS) que permiten la diferenciación y priorización del tráfico que se genere, para que las distintas aplicaciones (voz, datos y video) no se afecten entre sí.” Entre otras se cuenta con:

Optimización del presupuesto

Adquirir este tipo de tecnología reducirá de cierta manera los costes de infraestructura y mantenimiento. Existirá un menor coste de equipos, la seguridad en la red aumentará y la fluidez en la transmisión de datos mejorará considerablemente.

Adaptabilidad

Sin importar que tan grande o pequeña sea la empresa, MPLS pueden ser diseñadas y adaptadas según la necesidad del cliente.

Mejor rendimiento

Este tipo de redes, si bien es adaptable a cualquier empresa, es recomendable para aquellas que cuenten con más de una sede o sucursal, ya que, esta solución asegura una comunicación fluida y de latencia muy baja proporcionando una seguridad robusta a diferencia de redes tradicionales.

2.8. Red SD-WAN

A lo largo del tiempo, las redes de comunicación han ido evolucionando y expandiéndose de manera significativa, esto ha dado paso al crecimiento de las necesidades de servicios que las

empresas tienen, consiguiendo con esto que los administradores de la red tengan dificultades para gestionar y administrar las mismas de forma manual.

Con lo mencionado antes, se vuelve una necesidad cada vez más fuerte el buscar nuevas estrategias y nuevas tecnologías para garantizar tanto una fluidez de transmisión de datos como una seguridad en los mismos.

Los modelos tradicionales, hoy en día no cumplen con las expectativas presentadas por las empresas.

Como indica Aruba (2022), El modelo tradicional de dirigir el tráfico de retorno desde las sucursales al centro de datos para someterlo a una inspección de seguridad sólida ya no es la solución óptima, ya que se desperdicia ancho de banda y aumenta la latencia, lo que en última instancia perjudica el rendimiento de las aplicaciones.

De esta problemática surge SD-WAN, una red de área extendida por software es una nueva tecnología, capaz de simplificar el control, la gestión y administración de la infraestructura de IT (Infraestructura Tecnológica) garantizando un rendimiento y una adaptabilidad persistente de las aplicaciones.

SD-WAN, permite a los administradores de red usar el ancho de banda de una manera más efectiva, debido a que tiene la capacidad de reconocer que aplicaciones son nativas de internet y cuales no, por lo que, utiliza este conocimiento para direccionar el tráfico de la red, priorizando las aplicaciones con mayor rendimiento que se vayan por los enlaces propios de internet, mientras que las aplicaciones que no tienen mayor relevancia o mayor rendimiento pueden dirigirse por los enlaces tradicionales.

2.8.1. Funcionamiento

Debido al crecimiento y expansión de las empresas e instituciones, la información que transita por la red década tras década se hace más abundante, por lo que, si una empresa quiere ver crecimiento y desea ser competitiva en el mercado, es necesario que cuenten con una fluidez y seguridad de sus datos, lo que, en la actualidad, no pasa con las redes tradicionales WAN.

Actualmente, las redes WAN ofrecen servicios con un ancho de banda muy bajo, además tienen una alta latencia, lo que ocasiona que el usuario final, técnicos y personal en general de la empresa tenía una experiencia poco agradable. Esto hace que la empresa llegue a tener indisponibilidad de sus servicios primordiales, gracias a la lentitud de las comunicaciones, existan pérdida de datos y por ende una pérdida significativa de tiempo y dinero.

De esta problemática es que surge SD-WAN como una solución a los problemas mencionados, ya que, como menciona Aruba (2022), "SD-WAN garantiza un rendimiento y una resiliencia constantes de las aplicaciones, automatiza el direccionamiento del tráfico con un modelo basado en las aplicaciones en función de la intención comercial, mejora la seguridad de la red y simplifica la arquitectura WAN." Funciona tal que, SD-WAN crea una superposición con el fin de virtualizar las redes WAN y así simplificar y optimizar la administración e implementación de los servicios que las sucursales tienen.

El proceso de implementación de una red SD-WAN, se llevará a cabo tomando las siguientes consideraciones:

- **Conexión a la red:** Cuando un agente (usuario) conecta su equipo a la red empresarial, la señal que esta transmite es gestionada por un router que estará bajo una solución SD-WAN monitoreado vía software, lo cual permitirá el uso de cualquier aplicación en cualquier lugar, desde el centro de datos hacia la nube.

- **Establecer la ruta:** Esta solución es automatizada, por lo que, el software de gestión, es capaz de determinar la mejor manera o mejor ruta para otorgar servicios en base a las aplicaciones que se estén usando.
- **Enrutamiento:** Toda operación o proceso que se realice estarán monitoreadas o manejadas por un control de tráfico de datos dentro de la WAN virtualizada lo que asegurará seguridad, disponibilidad y continuidad. De manera que, si se necesita más ancho de banda para algún proceso u operación, se enruta automáticamente a través del dispositivo y, los demás tráficos que no son críticos, serán redireccionados a otro canal que cumpla con sus necesidades.

2.8.2. Ventajas de la red SD-WAN

Una arquitecta WAN tradicional únicamente puede enrutar las aplicaciones por medio de MPLS, mientras que SD-WAN está automatizado, permite seleccionar el camino más óptimo según los requerimientos de su funcionalidad. De igual manera, como lo menciona Pérez (2020), "Algunas de las ventajas de SD-WAN son la conmutación automática en caso de fallo, la redundancia, la administración simplificada y el ahorro de costes que reducen el costo de mantener la tecnología implementada en ubicaciones remota." A partir de esto, se mostrará algunas ventajas que posee SD-WAN,

Elevación de agilidad empresarial

- La conectividad entre las sucursales o sedes se incrementan de manera eficiente
- Integración de estaciones remotas que estén alineados bajo los mismos protocolos de seguridad gestionando y optimizando sus procesos
- Monitoreo de comunicaciones y flujo de información de manera más cercana presencial o remotamente.

- Implementación de políticas tipo SASE lo cual permitirá establecer perímetros seguros de la red.

Ahorro de Costes

- Una de sus funcionalidades es poder redirigir el ancho de banda dependiendo las necesidades lo que produce una optimización del ancho de banda haciendo que la empresa pueda sincerar en la contratación de servicios adicionales.
- Ofrece un control estricto en cuanto a navegación web restringiendo sitios sospechosos o actividades no permitidas de la organización, esto ayuda al consumo óptimo y eficiente de los recursos.

Seguridad Integral

- La solución SD-WAN, permite la adquisición de diversas arquitecturas de seguridad.
- Permite un elevado nivel de seguridad en cuanto a la red empresarial sin afectar la tasa de latencia.

2.9. Red MPLS vs Red SD-WAN

MPLS es la competencia directa con SD-WAN, esto se debe a que posee características de automatización del tráfico del ancho de banda de la red, muy similar a la red SD-WAN, sin embargo, los pros o ventajas que la red SD-WAN ofrece son mucho mayores a los de MPLS. A continuación, se detallarán algunos puntos para sustentar el comentario anterior.

- **Costo:** Una red SD-WAN es más económica adquirir que un MPLS, debido a que las redes MPLS trabajan con un servidor a través de un operador, en cambio SD-WAN se encarga de enviar el tráfico a través de internet.
- **Seguridad:** Aunque MPLS es considerada una red segura, esta no cuenta con un cifrado adecuado, por lo que la seguridad baja severamente. En cambio, SD-WAN, al estar situado

en internet, aumenta su seguridad de manera considerable al proporcionar de manera natural un tráfico de red encriptada.

- **Ancho de banda:** Mientras que la red MPLS está limitada a usar un ancho de banda que va desde los 40 Mbps hasta los 100 Mbps únicamente, SD-WAN no tiene limitantes, esta tecnología permite ampliar el ancho de banda según la necesidad del consumidor "empresa u organización", se realiza de manera que se agregar circuitos tipo WAN de cualquier proveedor y de cualquier tipo con el fin de minimizar o eliminar la congestión de la transmisión de datos.

CAPÍTULO III: DISEÑO DE RED SD-WAN

3. Diseño de la red SD-WAN con equipos Fortigate.

3.1. SD-WAN

En este capítulo se mostrará los requerimientos y pasos a seguir para una correcta simulación de una Red SD-WAN, se indicarán los recursos y configuraciones que permitirán el correcto análisis del monitoreo de la red. De igual manera se indicarán la red que la organización tiene inicialmente de Matriz del Banco, así como la propuesta dada con SD-WAN.

Para lograr un correcto diseño e implementación es necesario contar con un software especializado, el cual permita la implementación de equipos de red (Routers, Switches, computadoras, ect.) y la configuración de estos. Dicho software deberá ser capaz de proveer permisos, privilegios para acceso al internet, puertos, etc. Con estas consideraciones, se escogió el software GNS3 para realizar el proyecto mencionado.

3.2. GNS3

Hoy en día GNS3 es un software usado por ingenieros en redes para la simulación de diversos proyectos. Es una elección válida ya que permite diseñar topologías de redes con diversos dispositivos desde el computador o laptop.

Así como lo dice Telectrónika (2018), “GNS3 ha permitido a los ingenieros de red virtualizar dispositivos de hardware reales durante más de 10 años.”

Para la correcta instalación de este software es necesario un equipo con las siguientes características mínimas:

Tabla 1.

Características mínimas para instalación del emulador GNS3

Características Mínimas	
Sistema Operativo	Windows 7 (64 bits) en adelante, Linux (Cualquier variante), macOs.
Procesador	Mínimo 2 núcleos lógicos. Entre más núcleos se implementen mejor será la experiencia.
Memoria	4 GB (RAM).
Virtualización	Es compatible con: • Vmware. • VirtualBox. • Hyer-V (Windows).
Almacenamiento	Para la instalación 1GB de espacio disponible en disco (Instalación < 200MB).
Otros	Es necesario contar con más espacio libre en el disco para los diversos proyectos a crear.

Nota. Esta tabla muestra una descripción de las características mínimas que debe cumplir la PC o laptop que vaya a instalar GNS3 para su correcto funcionamiento.

Para la simulación de la propuesta que se planteará más adelante, es necesario contar con ciertos recursos recomendados para que el proyecto fluya de manera adecuada y su funcionamiento sea óptimo.

Tabla 2.

Características recomendadas para un correcto funcionamiento del GNS dentro de VMware.

Características Recomendadas	
Sistema Operativo	Windows 7 (64 bits) en adelante, Linux (Cualquier variante), macOs.
Procesador	• i5 – 9na Generación (Superior o equivalente) • 4 procesadores lógicos, entre más mejor.
Virtualización	VMware: • Activar dentro del VMware la opción (Virtualize Intel VT-x/EPT or AMD-V/RVI). "Virtualización por Hardware"
Memoria	8 GB (RAM).
Almacenamiento	Disco Sólido (SSD-M.2) con 50 GB o más de disco disponible.
Adaptador de Red	• Network Adapter (Red Bridged)

Nota. Esta tabla muestra las características que se recomienda tener en una PC o laptop para el levantamiento de GNS3 y el diseño de las redes dentro de VMware.

3.3. Red Actual

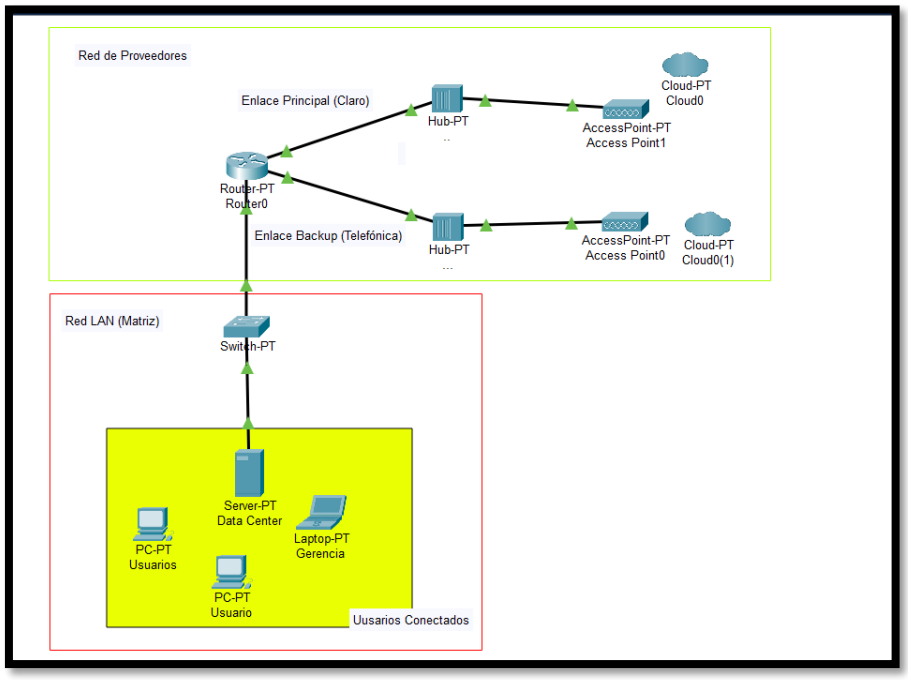
En este proyecto se quiere migrar la red actual que la empresa tiene a una red virtualizadas (SD-WAN). Actualmente la empresa es una organización financiera, en dónde se encuentran conectados los siguientes usuarios (Gerentes, Personal de TI, Administración, Mensajeros, Finanzas, ect.).

Existen varias sucursales a nivel nacional, sin embrago este trabajo se centrará en “Matriz” Quito debido a que en el edificio es dónde se encuentran los gerentes o altos mandos y demanda de una mejor calidad de conexión a la red.

A continuación, se observará un gráfico el cual muestra el estado de la red actual de la empresa.

Figura 5

Red actual banco Solidario



Nota. Esta figura muestra un segmento de la red actual del banco solidario y como se está trabajando tanto interna como externamente.

Como se puede apreciar, la red cuenta con dos enlaces, el principal y el de Backup, el enlace principal tiene el proveedor con la empresa “Claro”, mientras que el Backup es de telefónica y cuenta con un proveedor más reconocido en el mercado asociado a la empresa “Telconet”. No tienen un proveedor en la nube que gestione las conexiones a Internet como Azure o AWS, por

lo que, las subidas, caídas, intermitencias, tienen que ser monitoreadas a través de una pantalla en medio de la estación de trabajo.

En esta red, existe intermitencia redundante en el internet en Matriz – Quito interviniendo así, el trabajo diario de los usuarios internos. El problema con esto es que, no existe una alerta previa o un aviso cuando hay subidas del ancho de banda, es cierto que está el monitor para revisar la conectividad, sin embargo, existe poco personal en el área de IT (Infraestructura tecnológica), en el área de redes que no pueden estar atentos 24/7 a la pantalla para ver cuando se caen los enlaces. Por lo que, tienen que esperar a que varios usuarios tengan problemas de conectividad, estos usuarios generen un reclamo a su línea de supervisión directa y está última reporte al departamento para validar si es factible levantar de nuevo el enlace o pasarlo manualmente al de backup (Telefónica).

3.3.1. Desventajas de la red actual

- **Configuración Manual:** No existe una automatización en los enlaces de internet, por lo que, si un enlace falla, se cae o simplemente deja de funcionar, el equipo de IT tendrá que, manualmente levantar el enlace caído o pasar al de back up.
- **Robustez:** Debido a que los equipos están conectados a un único rack de servidores, si este se avería, todo el sistema quedaría obsoleto. Además, como se mencionó anteriormente, si existe un enlace central que falle, todo el sistema y la red de computadoras fallará.
- **Administración técnica:** Debido a que las configuraciones son manuales, el equipo de IT debe estar capacitado y actualizado al 100% en todo lo referente a redes de computadoras ya que son los encargados de administrar las conexiones y que estas funcionen de manera eficiente y óptima. Esto es una maña práctica, ya que, con los

equipos de la actualizada, el tema de administración y optimización puede ser gestionada por un proveedor de la nube. Estos servicios reducirán el tiempo que emplean los técnicos en monitorear, administrar y optimizar las redes de comunicación.

- **Costo elevado:** Para poder adquirir servidores, varios routers, switches, etc. se debe invertir una suma de dinero un poco elevada, la cual no garantice el 100% de eficiencia en el funcionamiento.

Teniendo en cuenta las problemáticas vista anteriormente, se propone una solución en la nube que garantice la alta redundancia y automatización de las redes de comunicación.

3.4. Propuesta Red SD-WAN

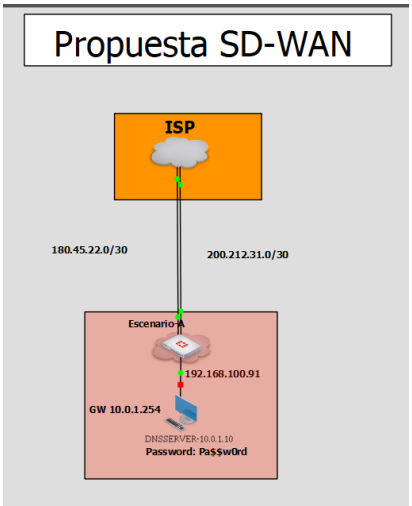
Como propuesta, se ha planteado una red en la cual se conecten equipos a internet mediante el firewall Fortinet, que conecte al Data Center y a las máquinas de los usuarios normales.

Se eligió Fortinet debido a que es un servicio que permite adoptar la tecnología SD-WAN de una manera sencilla y segura.

En el siguiente gráfico se verá la propuesta dada para SD-WAN la cual simplifica el hecho de estar gastando en equipos informáticos.

Figura 6

Propuesta de red SD-WAN para el banco solidario.



Nota. Esta figura muestra una red más sencilla que cuenta con secciones internas y externas únicamente con el uso del equipo Fortigate y los diferentes ISP que la empresa cuente.

Para este trabajo se debe en cuenta los equipos que se utilizarán para la simulación de conectividad. Estos son:

Tabla 3.

Equipos usados en GNS3

Equipo	Función
FORTIGATE	Firewall el cual nos permitirá configurar de manera sencilla y ágil SD-WAN
Switch	Switch LAN interno de la empresa
Servidor	Domain Server “Data Center”
PC´s	Diferentes equipos que los usuarios normales tienen.

WAN	"Internet" es la red de proveedores de servicio con la que se puede utilizar para conectar una sucursal a otra, etc.

Nota. Esta tabla muestra lo equipos se usaron para el diseño y configuración de la red SD-WAN con equipos Fortigate.

Para la asignación de IP en los equipos se usará la siguiente tabla:

Tabla 4.

Tabla de asignación de IP

Nombre	IP	Máscara	Gateway
ISP_1	200.212.31.0	255.255.255.252	200.212.31.2
ISP_2	180.45.22.0	255.255.255.252	180.45.22.2
SD-WAN (Fortigate)	192.168.100.91	223.255.255.255	192.168.100.0
DNS_Server	10.0.1.10	255.0.0.0	10.0.1.254

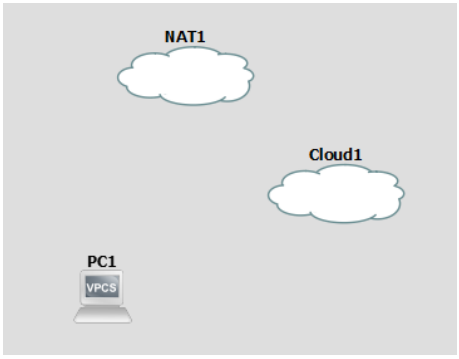
Nota. Esta tabla muestra las IP que se usarán en los diferentes equipos emulados en GNS3.

3.5. Levantar SD-WAN en FORTIGATE (GNS3)

En primer lugar, se coloca la red NAT y el Cloud para poder realizar la simulación de internet ya que es más sencillo si se usa una red NAT junto con una PC que servirá para el monitoreo de la red.

Figura 7

Ubicación de equipos

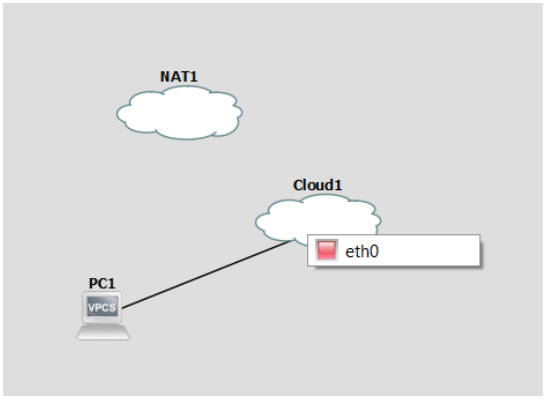


Nota. Esta imagen muestra la primera colocación de equipos para entender como conectar los diferentes encalces de internet.

Se realizá una conexión entre la PC1 y la nube simulando un enlace de internet.

Figura 8

Conexión PC a ISP

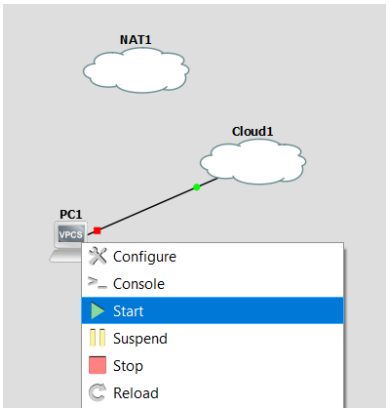


Nota. Esta imagen muestra cómo se conecta un equipo a un ISP por medio de ethernet.

Una vez conectada la PC se levanta el servicio y se abrió la consola para configurar este equipo.

Figura 9

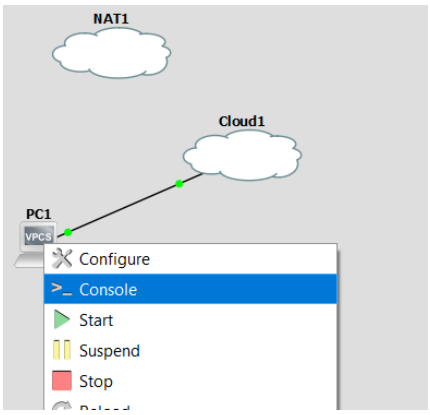
Iniciar el equipo requerido



Nota. En esta imagen se muestra la manera en que se debe iniciar un único equipo en el emulador GNS3.

Figura 10

Ingreso a CLI para configuración

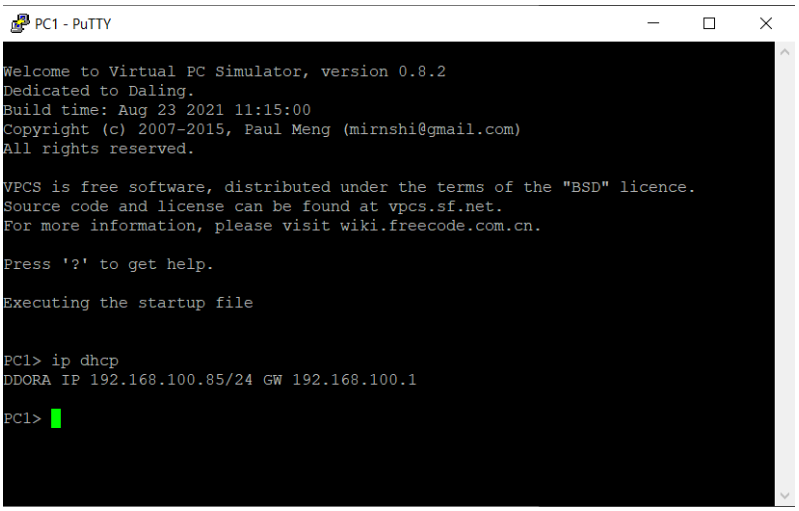


Nota. En esta imagen se muestra la manera más efectiva de ingresar a la consola para las diferentes configuraciones dentro del emulador GNS3.

Se coloca el comando IP DHCP para que entregue una IP dinámica: 192.168.100.85/24 – GW: 192.168.100.1

Figura 11

Obtener la IP del equipo conectado al ISP



Nota. Esta imagen nos muestra la manera de obtener la IP DHCP del equipo que se tenga conectado al ISP dentro de GNS3.

Se deberá realizar el mismo procedimiento para descubrir el Gateway y la IP de la red NAT.

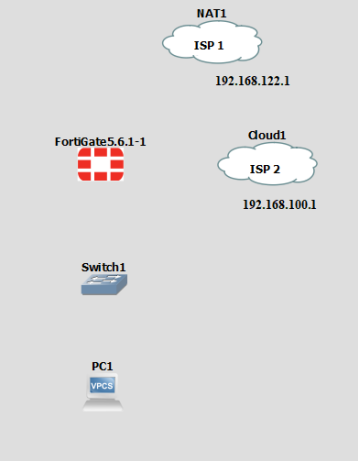
- Se conecta la PC a la red NAT
- Se enciende la consola en donde se colocará el comando IP DHCP para evidenciar la IP y el Gateway:

  IP 192.168.122.205/24 GW 192.168.122.1

Se añade el fortigate para poder configurar los ISP de manera correcta y un switch plano.

Figura 12

Colocación de equipos Switch y Foritgate

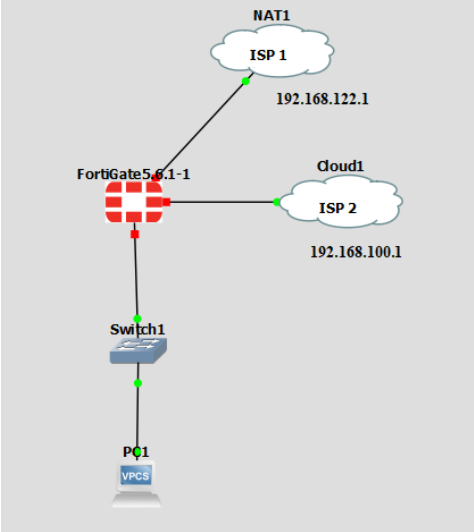


Nota. Esta imagen muestra los nuevos equipos que se conectaran en el emulador de GNS3.

Se conecta el equipo FORTIGATE a las dos redes, al switch y el switch a la PC. Quedará de la siguiente forma:

Figura 13

Conexión equipos



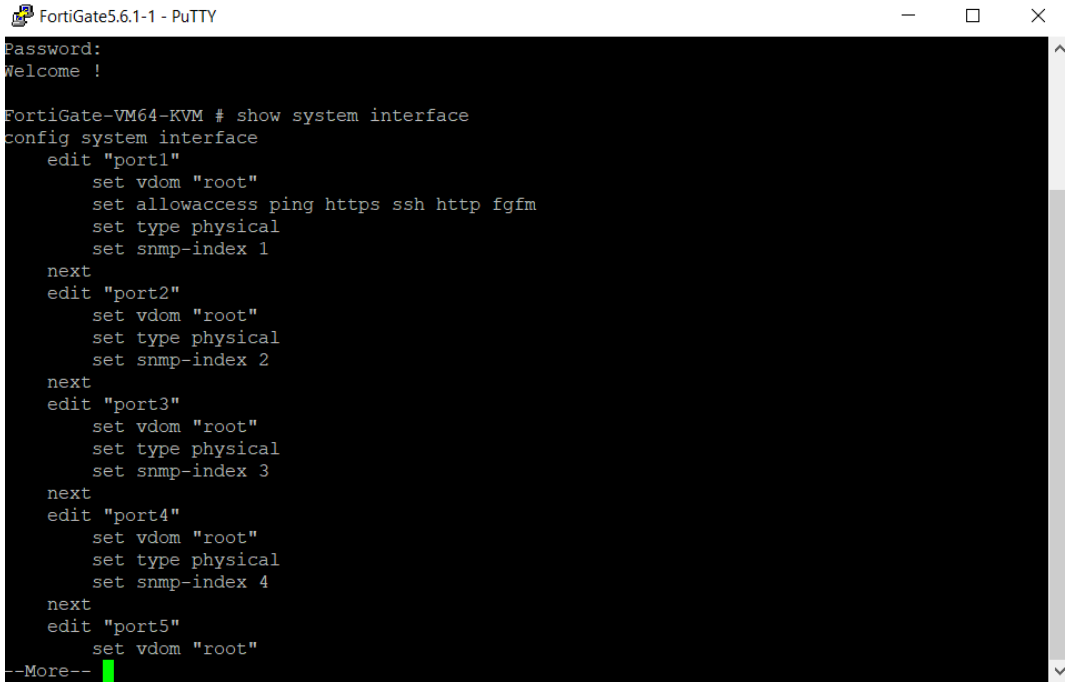
Nota. En esta imagen se muestra las nuevas conexiones realizadas con el equipo Fortigate.

Se deberá abrir el FORTIGATE y por siguiente la consola

Se coloca el comando show system interface para comprobar que no existan IP configuradas en los puertos recién conectados.

Figura 14

Verificación de configuración de puertos



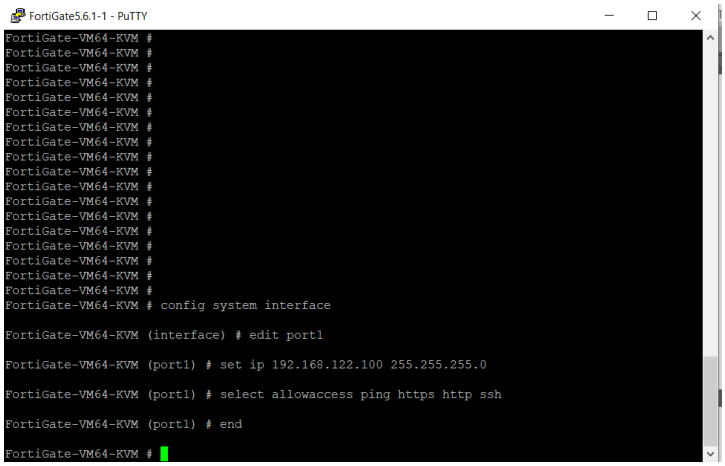
Nota. En esta figura, se muestra la configuración de todos los puertos con ayuda del comando "Show system interface".

Con los siguientes comandos se realizará lo siguiente:

- Colocar una IP al puerto 1
- Habilitar los puertos https, http y ssh

Figura 15

Configuración de IP y habilitación de puertos

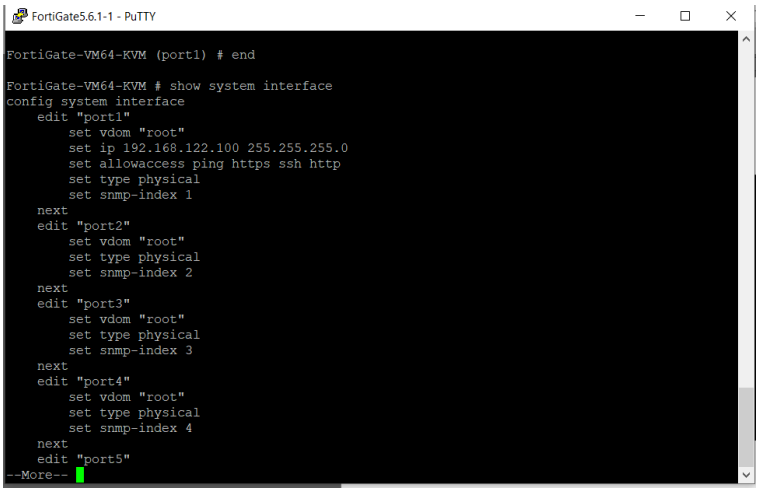


Nota. En esta figura, se muestra la manera de configurar una IP a un equipo Fortigate y a su vez la habilitación de diversos puertos.

Se verifica que se hayan efectuado los cambios

Figura 16

Verificación de cambios realizados.



Nota. En esta figura, se verificarán que los cambios se hayan realizado de manera correcta con ayuda del comando “Show system interface”.

Se realizan los mismos pasos para el puerto 2

- Se coloca una ip
- Se procede a habilitar los puertos https, http, ssh
- Se verifican los cambios

Una vez configuradas las IP y levantados los puertos se podrá ingresar a la interface del FORTIGATE para la administración y configuración de SD-WAN

CAPÍTULO IV: MONITOREO DE LA RED

En este capítulo, se evidenciará el balanceo de carga y la alta disponibilidad que tendrá el tráfico de internet al salir hacia los diferentes ISP.

4.1. Fortigate

Para realizar el cometido propuesto se hará uso del firewall mencionado en el anterior capítulo (FORTIGATE).

FORTIGATE es un firewall que se configura en dispositivos Fortinet los cuales ofrecen una creación de redes automatizadas, seguras y sofisticadas. Como lo menciona Fortinet (2022), "Las redes basadas en la seguridad de Fortinet abordan estos desafíos integrando estrechamente la infraestructura de red con la arquitectura de seguridad, es decir, su red permanecerá segura a medida que se amplíe y cambie."

Entre los beneficios que esta tecnología ofrece se tiene:

- Seguridad veloz, de extremo a extremo.
- Con ayuda de los servicios FortiGuard se ofrece una defensa consistente en tiempo real.
- Experiencia mejorada para el usuario con ayuda del procesamiento de seguridad.
- Automatización en los flujos de trabajo, así como una mayor eficiencia en la parte operativa.

4.2. Servicios Fortigate

4.2.1. Dashboard

En primer lugar, se tiene el Dashboard, este servicio muestra una vista general de los equipos que se tiene configurado dentro del Fortigate como:

- Status: Muestra el estado de los equipos conectados, la información de sistema, todo lo referente a la licencia del firewall, el rendimiento.
- Security: Muestra todo lo referente a seguridad del equipo Fortigate como vulnerabilidades detectadas, resumen de escaneo de hosts, etc.
- Network: Muestra una vista general de todos los equipos, configuraciones e IP que estén configurados dentro de la red y conectados al equipo Fortigate, un ejemplo de ellos es el “Routing” que muestra toda la configuración de los equipos que estén conectados al firewall.
- Users & Devices: Como el nombre lo menciona, muestra Widgets de los equipos onectados, usuarios creados de firewall, etc.

De igual manera, se cuenta con monitores, los cuales ayudarán a controlar el tráfico de red, destino, aplicaciones, es decir, cosas que el Fortigate etá procesando o procesó en el pasado. Entre ellos se tiene:

- FortiView Sources.
- FortiView Destinations.
- FortiView Aplications.
- FortiView Web Sites.
- FortiView Policies.
- FortiView Sessions.

4.2.2. Network

En segundo lugar, se tiene el servicio de Network, el cual mostrará todas las configuraciones de red que se hayan hecho en los equipos que estén conectados al firewall. Entre ellos se encuentran:

- Interfaces: Muestra una imagen global del Fortigate y las interfaces conectadas, es decir los puertos que se encuentran conectados y configurados o por configurar.
- DNS: Los equipos Fortigate cuentan con DNS que son protocolos de internet con la función de “resolución de nombres de dominio”. Hay la posibilidad de colocar DNS propias o dejar las que vienen por defecto (208.91.112.53, 208.91.112.52).
- Captura de paquetes: Se podrá hacer un escucha en algún puerto y luego volcar el resultado a algún analizador o verlo en pantalla.
- SD-WAN: Se podrá configurar redes tipo SD-WAN lo que servirá para probar la alta disponibilidad, seguridad, automatización, etc.
- Static Routes: Configuración manual de enrutamiento para los diferentes ISP.
- Policy Routes: Se podrá crear, en base a las rutas estáticas, criterios de navegación o envío de tráficos, por ejemplo, cierto tráfico que pase por una ruta y lo demás por otra creada.
- RIP: Protocolo de enrutamiento dinámico.
- OSPF: Protocolo de enrutamiento dinámico.
- BGP: Protocolo de enrutamiento dinámico.

4.2.3. Policy & Objects

En tercer lugar, se encuentran los servicios de políticas y objetos. Es uno de los menús o servicios más importantes, aquí en dónde se crearán todas las políticas y objetos dentro del firewall. Entre ellos se tiene:

- Firewall Policy: Se podrá crear todas las políticas de seguridad del firewall.

- IPv4 Dos Policy: Se usa para la creación de políticas para protección de ataques de denegación de servicios.
- Addresses: Se pude crear objetos de tipo adres donde se coloca un nombre y queda asociado una red o una dirección IP, un nombre de domino completo o crear un grupo que englobe a más de una dirección.
- Internet Service Database: Son los diferentes servicios de internet, Fortigate cuenta con 1.553 servicios predefinidos con la posibilidad de crear propios.
- Servicios: Configuración de los servicios creados.
- Schedules: Son ventanas de tiempo en el cual se puede especificar que una política esté activa o no dentro de un tiempo o fecha determinada.
- IP Pools: Sirve para la creación de pools de dirección IP en caso de tener algún "nateo" para salir a un servicio con tres o cuatro direcciones IP públicas, por ejemplo.
- Protocol Options: Nos servirá para asociar puertos a protocolos existentes.
- Traffic Shaping: Sirve para controlar el ancho de banda de los enlaces que se tenga.

4.2.4. Security Profiles

Como cuarto servicio se tienes los perfiles de seguridad. En esta sección se encontrará todos los perfiles de seguridad para brindar seguridad a los usuarios. Estos perfiles se usan en las políticas de firewalls dentro de la sección "políticas y objetos". Entre los perfiles de seguridad que se pueden crear se tiene:

- Perfiles de antivirus.
- Perfiles de filtrado web.
- Filtrado de video.

- Filtrado de DNS.
- Control de aplicación.
- Prevención de ataques del exterior o interior de la red.
- Filtrado a nivel de archivo.
- Inspección SSL/SSH.
- Firmas de aplicaciones.

4.2.5. VPN

Como quinto servicio, se encuentra el menú de VPN. Es la sección en dónde se configurará todo lo referente a "red privada virtual". Dentro de este servicio se encuentran:

- Controlador superpuesto VPN.
- Túneles IPSec.
- Asistentes de IPSec.
- Plantilla de túnel IPSec.
- Portales SSL-VPN.
- Configuración SSL-VPN.
- Clientes SSL-VPN.

4.2.6. User & Authentication

Como sexto servicio, se tiene los usuarios y autenticación. En esta sección se encontrará los apartados para configurar los usuarios, permisos de usuarios, autenticación de usuarios, entre otros. Entre los apartados se tienen:

- Definición de usuarios.
- Definición de grupos.
- Administración de huéspedes.

- Conectores contra servidores LDAP.
- Configuración de servidor de radio.
- Configuración de autenticación.

4.2.7. System

Como séptimo servicio, se cuenta con el apartado de sistema. En esta sección se podrá configurar todo lo referente a la interfaz del equipo Fortigate. La sección de sistema cuenta con los siguientes servicios:

- Configuración de la interfaz.
- Administración e informe del Firmware.
- Configuraciones de alta disponibilidad.
- Monitoreo por SNMP.
- Mensajes de reemplazo.
- FortiGuard: Servicios que tiene o no la licencia del equipo de Fortigate.
- Visibilidad de características.
- Certificados que cuenta el equipo Fortigate.

4.2.8. Security Fabric

Como octavo servicio, se tiene el "tejido de seguridad", en dónde se muestra la vista lógica y física del equipo Fortigate. En esta sección se muestra lo siguiente:

- Topología física.
- Topología lógica.
- Calificación de seguridad.
- Conectores de fábrica.
- Conectores externos.

- Centro de identidad de activos.

4.2.9. Log & Report

Finalmente, el último servicio con el que se cuenta son los logs y reportes, dónde se podrán encontrar todos los registros del equipo Fortigate. Entre los logs y reportes se tiene:

- Logs de tipo tráfico.
- Logs de tipo Sniffer.
- Eventos.
- Logs del Antivirus.
- Logs del filtrado de archivos.
- Logs del filtrado Web.
- Logs del control de aplicaciones.
- Configuración de retención o espacio del equipo Fortigate.

4.3.Configuración Seguridad

4.3.1. Gestión de administradores

Dentro de una empresa, existen varias áreas de trabajo (Departamento Técnico, Infraestructura Tecnológica, etc.), cada uno de ellos tiene su rol o función dentro de la organización. Unos se encargarán de configurar todo el tema de redes, firewall, VPN, mientras que otros se encargarán de crear políticas y reglas para las páginas web, usuarios, IP, etc. El problema es que no todos deben tener el mismo perfil o los mismos permisos de lectura y escritura.

Para esto, Fortigate nos permite crear usuarios y perfiles de administrador y otorgar permisos de solo lectura o completos.

Para poder crear un administrador con ciertos permisos se deberá seguir los siguientes pasos:

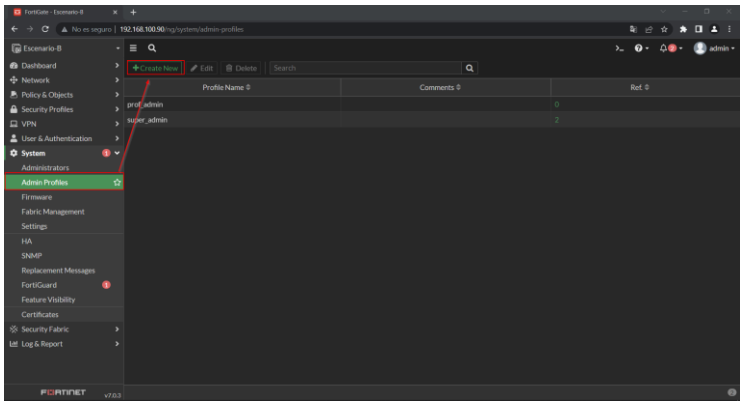
Suponiendo que se necesita crear un usuario de administrador para el área de Soporte de Usuario.

El primer paso será crear el perfil del usuario “Soporte”.

1. Dirigirse hacia el menú “System” Apartado “Admin Profiles” y “Create New”

Figura 17

Creación de perfil de administrador.

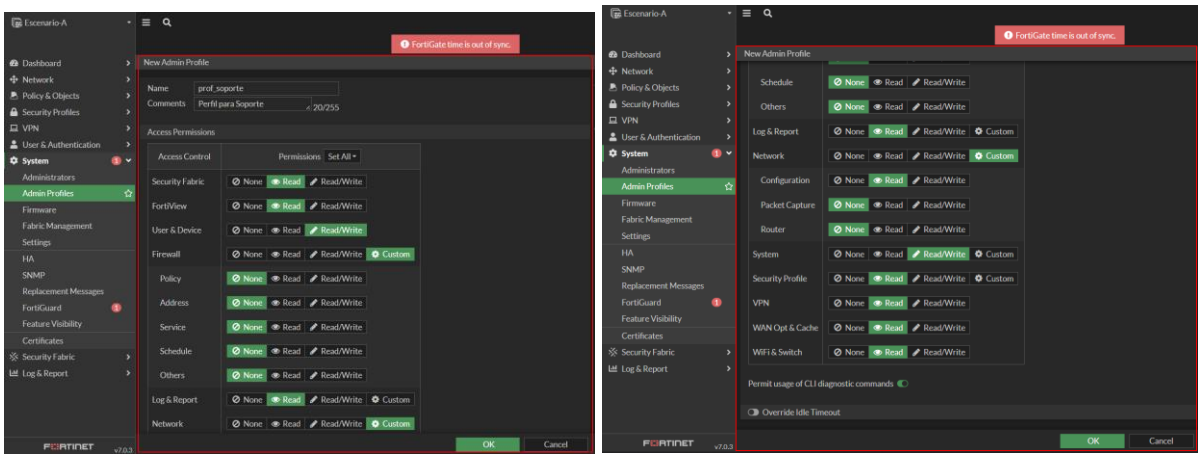


Nota. Esta figura muestra la manera en la que se debe crear un perfil de administrador

2. Dentro de la interfaz de nuevo perfil, se colocará un nombre y los privilegios que se requiera dar tal y como se muestra en la siguiente imagen.

Figura 18

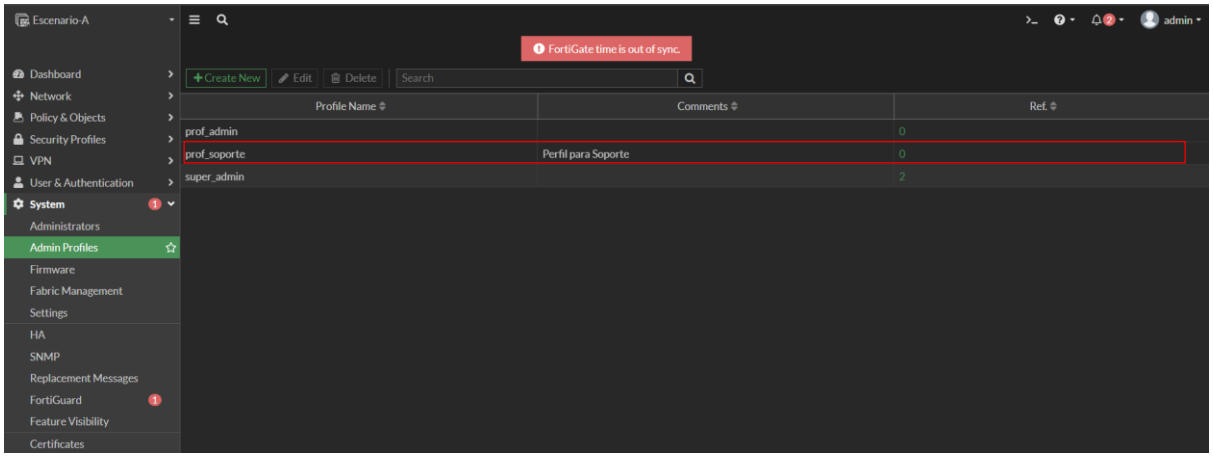
Privilegio del nuevo perfil de administrador.



Nota. Esta figura muestra los permisos de lectura y escritura que se otorgó al crear el nuevo perfil.

Figura 19

Visualización de cambios

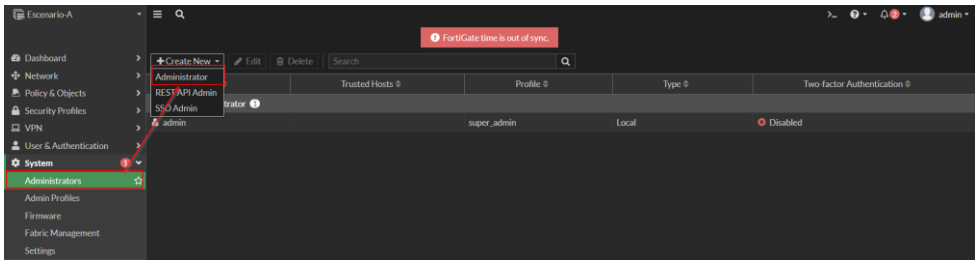


Nota. En esta imagen se muestra los cambios efectuados en la interfaz principal de “Admin Profiles”

3. En el apartado de “Administrators” se creará el usuario usando el perfil anteriormente creado.

Figura 20

Creación usuario Administrador

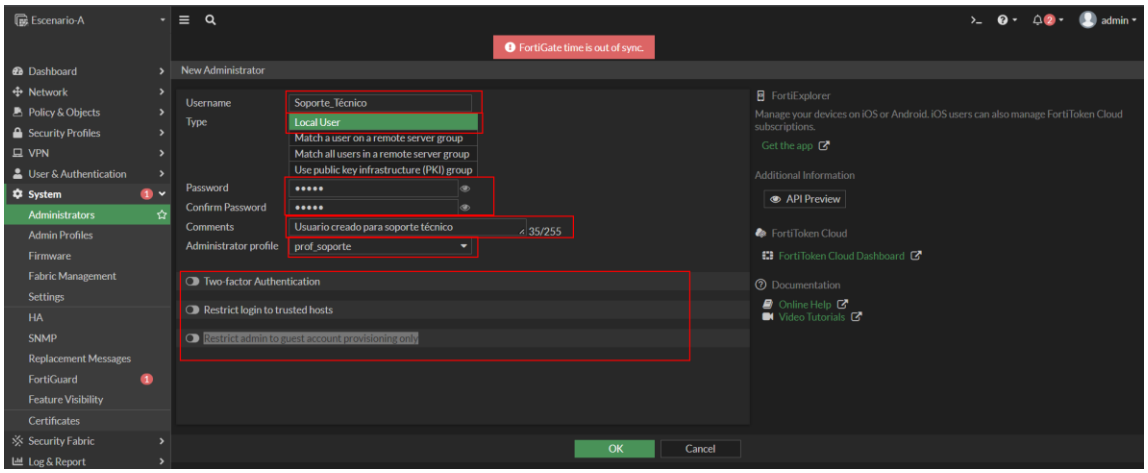


Nota. En esta imagen se está creando un usuario administrador en referencia al perfil creado anteriormente.

4. Se deberá colocar las siguientes características:
    a. Nombre del usuario.
    b. Dónde se creaará el usuario: En este caso, de manera local en el equipo Fortigate.
    c. Establecer una contraseña.
    d. Comentarios.
    e. Seleccionar el perfil de administración.
    f. Adicional se cuenta con parámetros de seguridad por si se desea implementar:
        i. Doble factor de autenticación.
        ii. Restricción del inicio de sesión a hosts de confianza.

Figura 21

Parámetros de administrador.

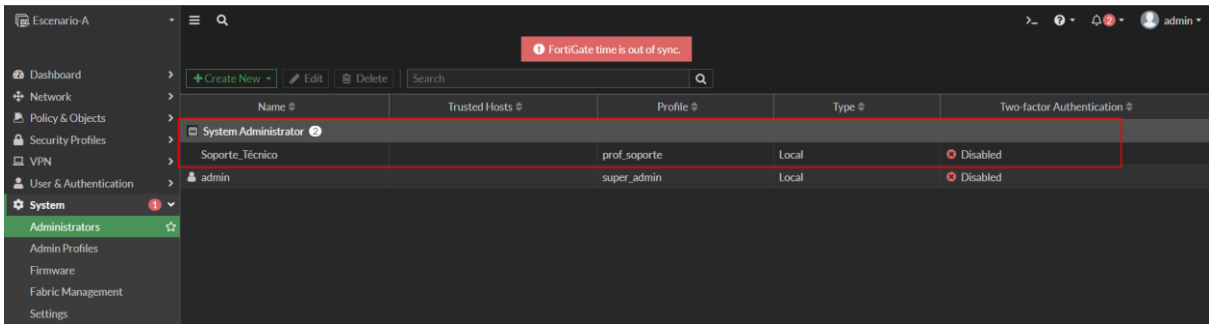


Nota. En esta imagen se muestran los parámetros que deberá tener el perfil de administrador que se creará.

Con estas configuraciones quedará creado el usuario “Soporte_Técnico” el cual se podrá evidenciar en la sección de administradores.

Figura 22

Verificación del usuario creado.



Nota. En esta figura se muestra el usuario ya creado con el nombre y el perfil que se le asignó.

4.4.Configuración red SD-WAN

Dentro de las empresas, existen enlaces de internet por los cuales sale el tráfico del mismo. En muchas ocasiones, el balanceo del tráfico es configurado manualmente, lo que hace que los técnicos tengan una carga de trabajo grande al tener que redireccionar los enlaces cuando estos dejan de funcionar. SD-WAN es una tecnología que permite automatizar y optimizar el tráfico de

la red, configurando de manera que, cierto ancho de banda vaya por un proveedor y el resto por otro proveedor distinto, siempre buscando el camino más óptimo y que, si alguno se llegará a caer, automáticamente se redireccione el tráfico hacia el enlace que se encuentra operativo y no de forma manual.

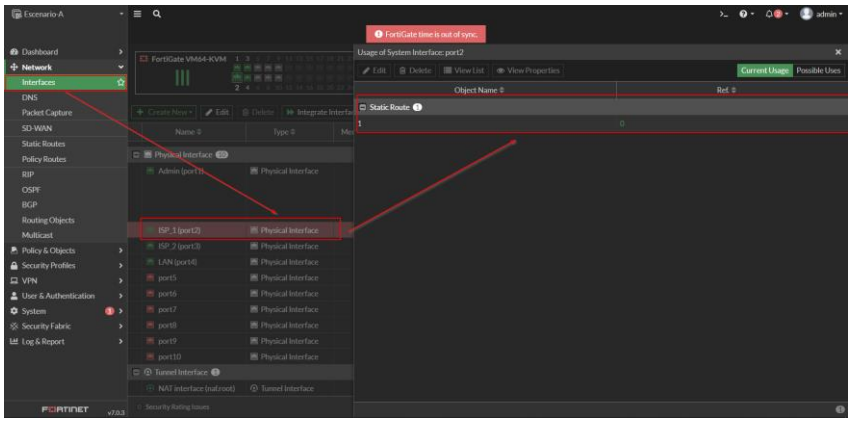
Para poder configurar la red SD-WAN se deberá realizar los siguientes acondicionamientos:

Para poder asociar los puertos o enlaces de internet a SD-WAN, estos no deben estar en uso, es decir no se debe tener ninguna referencia.

Como se puede apreciar en la siguiente figura, el IPS_1 tiene una referencia a “static Route”

Figura 23

Visualización de referencias.



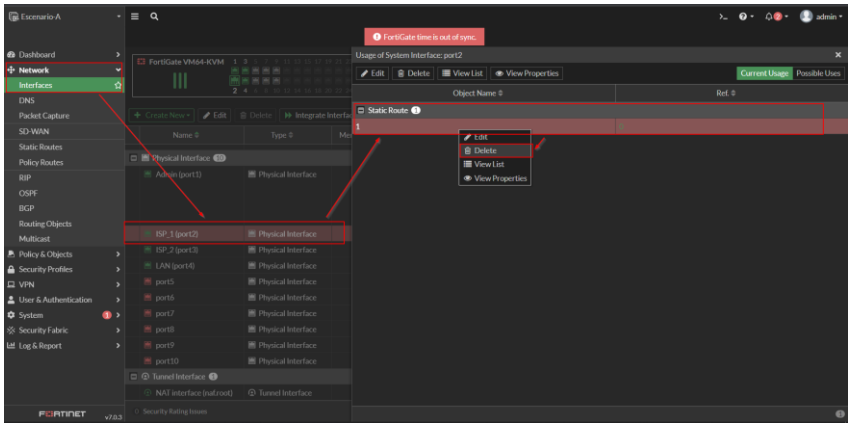
Nota. En esta figura se evidencia que un ISP está referenciado a alguna política o regla creada.

Para poder continuar con la configuración es necesario eliminar la referencia creada.

- Eliminar dicha referencia: Únicamente se presiona click derecho sobre la referencia creada y se procederá a aplastar “Delete”, esto hará que se elimine de manera permanente la referencia creada en el enlace de internet.

Figura 24

Eliminación de una referencia.

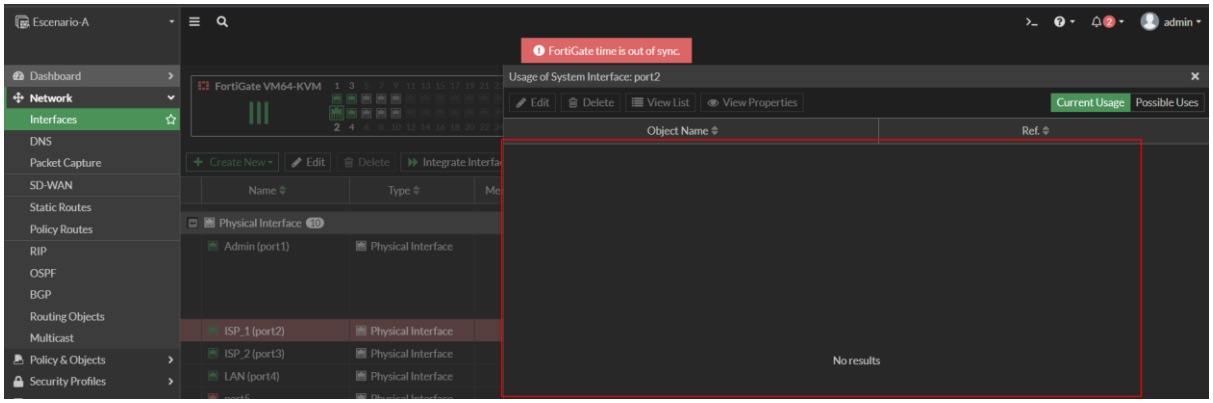


Nota. En esta figura se muestra la manera de eliminar de manera satisfactoria una referencia.

La referencia quedará borrada satisfactoriamente

Figura 25

Verificación de cambios.



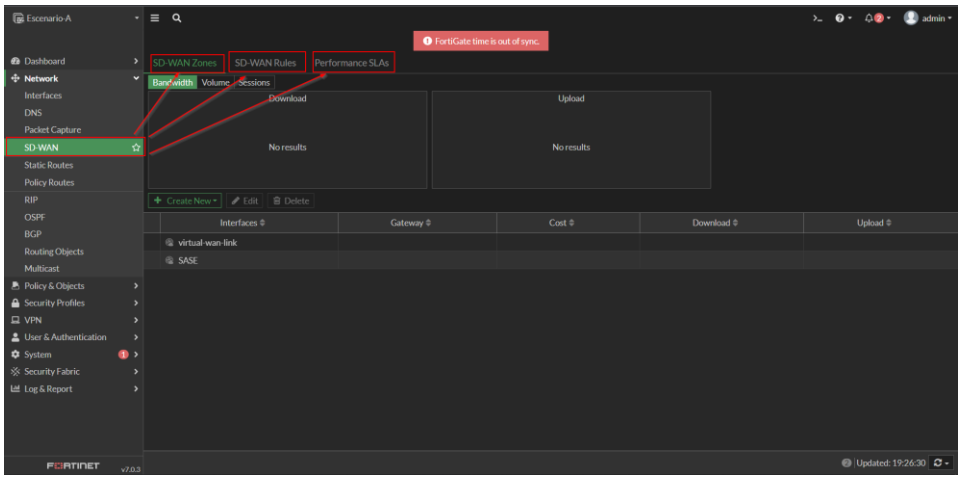
Nota. En esta figura, se muestra que en el ISP_1 no se encuentra ninguna referencia, es decir, que se eliminó satisfactoriamente.

El siguiente paso será dirigirse hacia “Network” → “SD-WAN”, allí se encontrarán tres opciones:

- SD-WAN Zones: Interfaces creadas de SD-WAN.
- SD-WAN Rules: Reglas y políticas para las redes SD-WAN.
- Performance SLA: Se podrá definir contra que servidores externos o internos se miden la salud de los enlaces.

Figura 26

Servicios SD-WAN



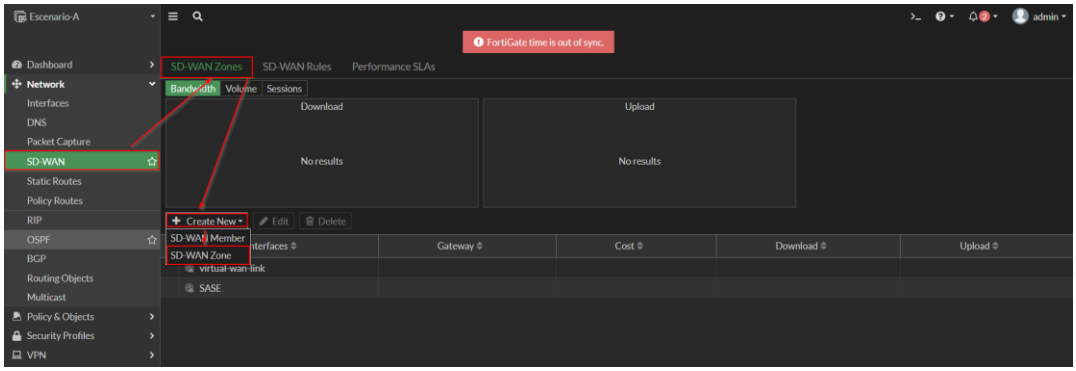
Nota. En esta figura se muestran los tres servicios esenciales de la red SD-WAN.

4.4.1. SD-WAN Zone

En primer lugar, se creará una “zona” o interfaz. Para esto se selecionará “Create Zone” → “SD-WAN Zone” dentro de la sección “Netwok” – “SD-WAN”

Figura 27

Creación de zonas para SD-WAN

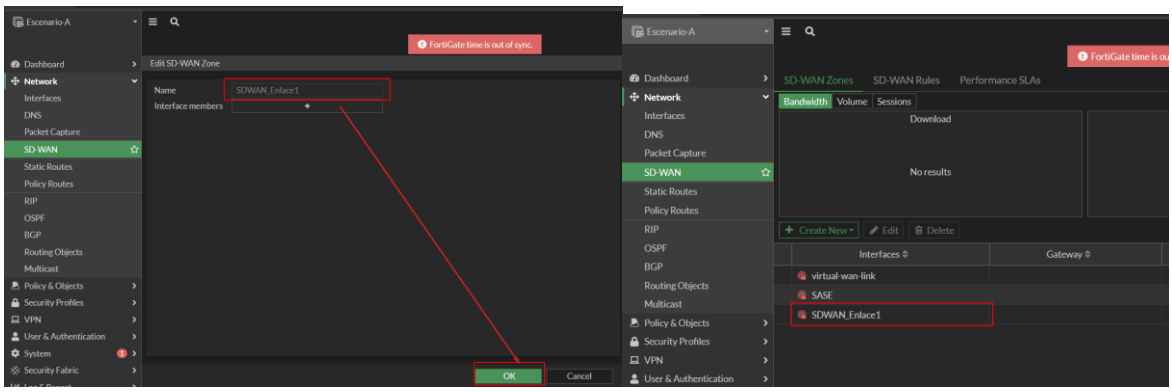


Nota. Esta figura muestra la manera en que se debe crear una zona o interfaz en SD-WAN.

Se deberá seleccionar un nombre para la nueva interfaz (SDWAN-Enlace1). Posterior a ello se colocará “OK” para que se guarden los resultados y poder crear una interfaz miembro más adelante.

Figura 28

Creación de la interface SDWAN-Enlace1



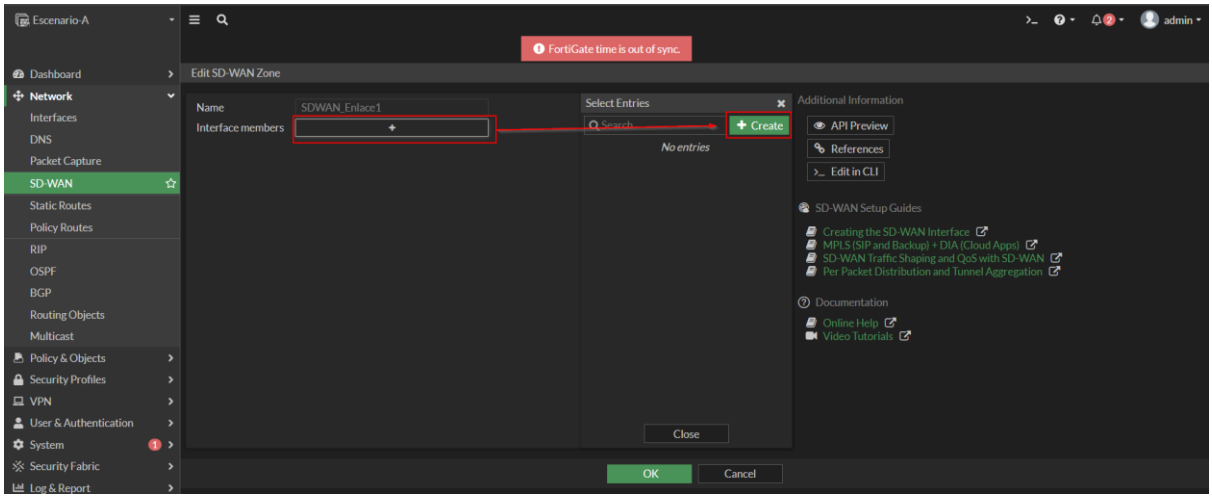
Nota. En esta imagen se muestra la manera que se visualiza la creación de la interfaz SD-WAN.

Se ingresa nuevamente a la interfaz creada, y se asociará un enlace o puerto de internet de la siguiente manera.

En primer lugar, se selecciona el “+” en Interface memebers y se procederá a crear una nueva “Create”.

Figura 29

Creación de miembros

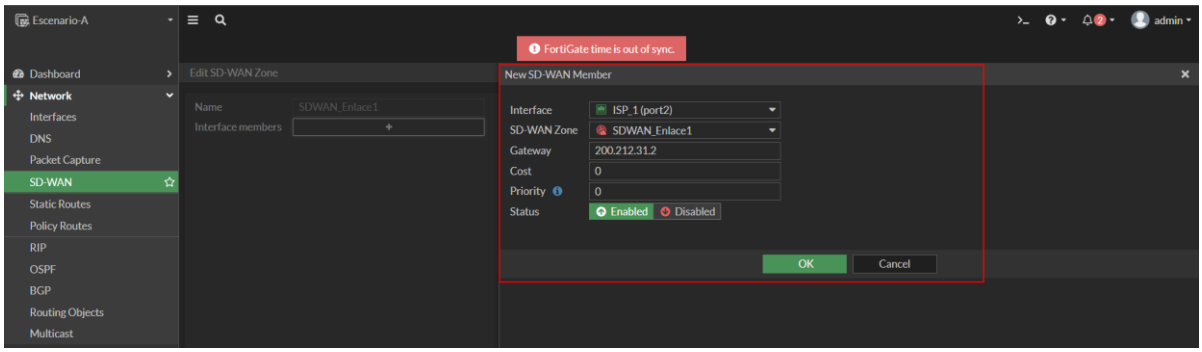


Nota. En esta figura se mostrará el miembro de la interfaz, es decir a que ISP estará asociada esta interfaz.

En segundo lugar, se selecciona el enlace que se vaya a asociar, la interfaz de SD-WAN creada y el Gateway del enlace mencionado.

Figura 30

Parámetros para el nuevo miembro de la interfaz SD-WAN.

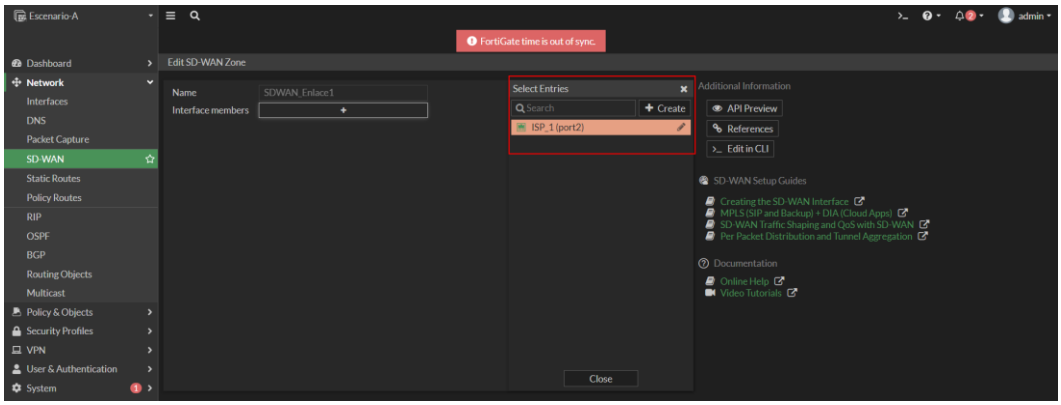


Nota. En esta figura se muestran los parámetros que se debe seguir para la creación de la interfaz miembro de SD-WAN.

El enlace se asoció de manera correcta

Figura 31

Verificación de creación de enlace.

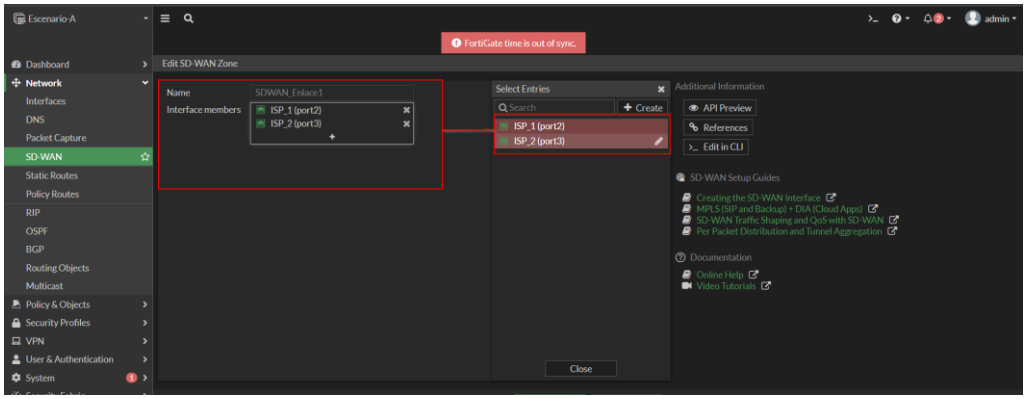


Nota. En esta figura se observa que se añadió de manera correcta el ISP creado

Se realizan los mismos pasos para el segundo enlace, por lo que debería quedar tal que así.

Figura 32

Visualización de configuración Interface members

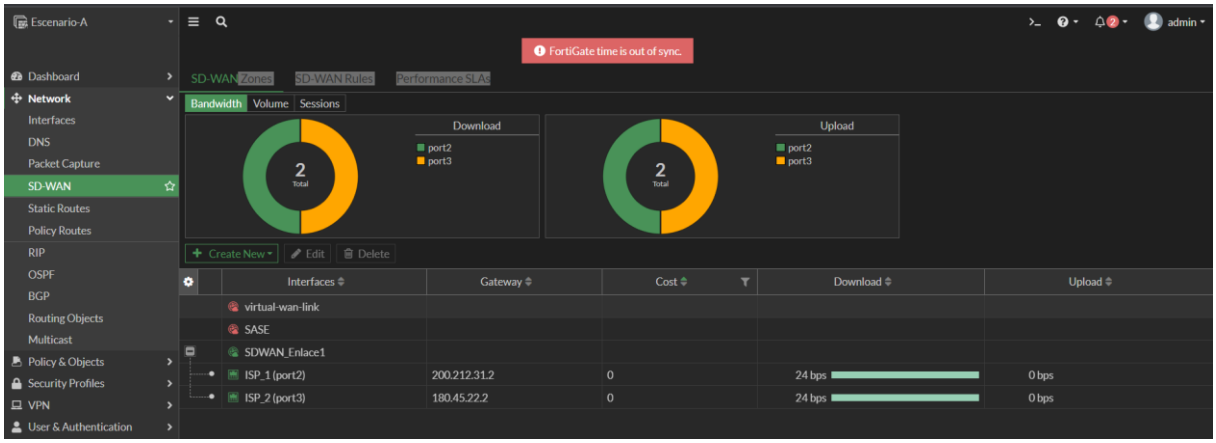


Nota. En esta figura se muestra como debe quedar la configuración de los enlaces en la interface SD-WAN.

Se puede apreciar que, una vez creada la asociación, en el apartado de interfaz, se muestra el ancho de banda usado por los dos enlaces de internet tanto de subida como de descarga.

Figura 33

Monitoreo del tráfico de internet.



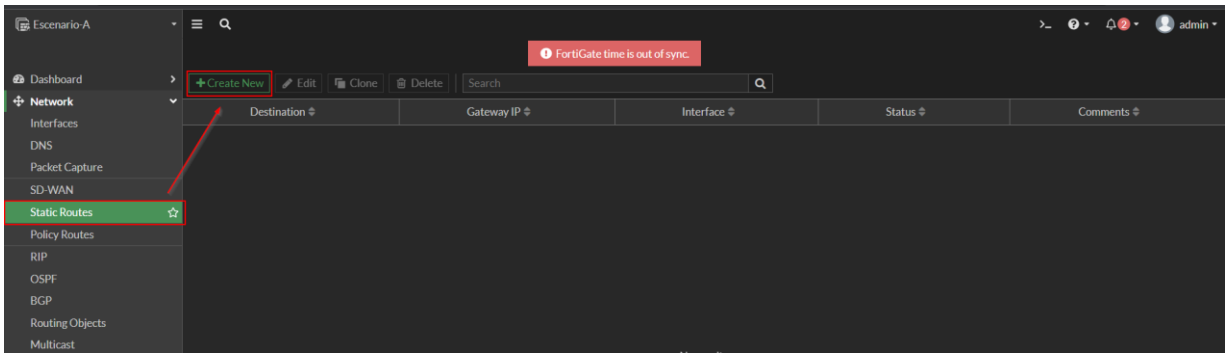
Nota. En esta figura, se puede apreciar el monitoreo de tráfico de red con los dos ISP creados.

Debido a que se eliminó las rutas estáticas para salida interenet y las políticas que permitía el acceso al mismo, se deberá volver a crear lo mencionado.

- **Creación de rutas estáticas**
  - Se selecciona el apartado “Static Routes” → “Create New”.

Figura 34

Creación de rutas estáticas

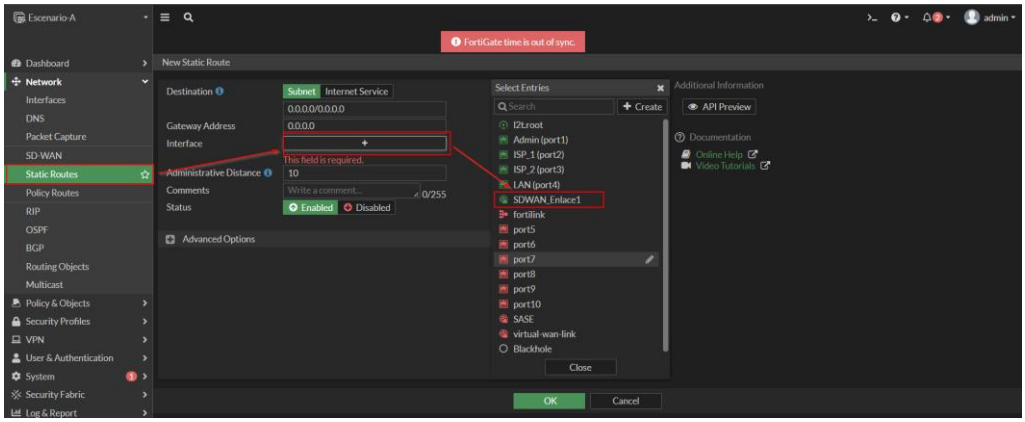


Nota. En esta figura se muestra la manera en la que se crea una ruta estática.

- En este caso, no se pondrá un Gateway debido a que ya se colocó al momento de configurar las interfaces miembros en SD-WAN, si no que se seleccionará la interface que se creó anteriormente “SDWAN-Enlace1”.

Figura 35

Creación de rutas estáticas.

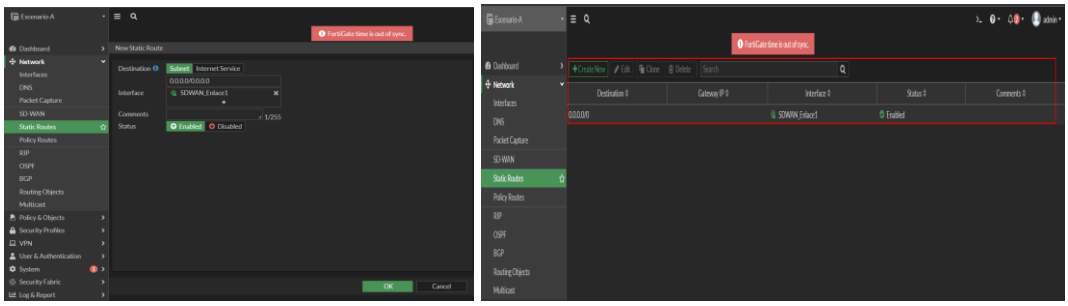


Nota. Esta figura muestra la manera en que se debe configurar de manera correcta la interfaz creada de SD-WAN

Quedando de la siguiente manera y permitiendo la salida a internet.

Figura 36

Visualización de cambios efectuados.



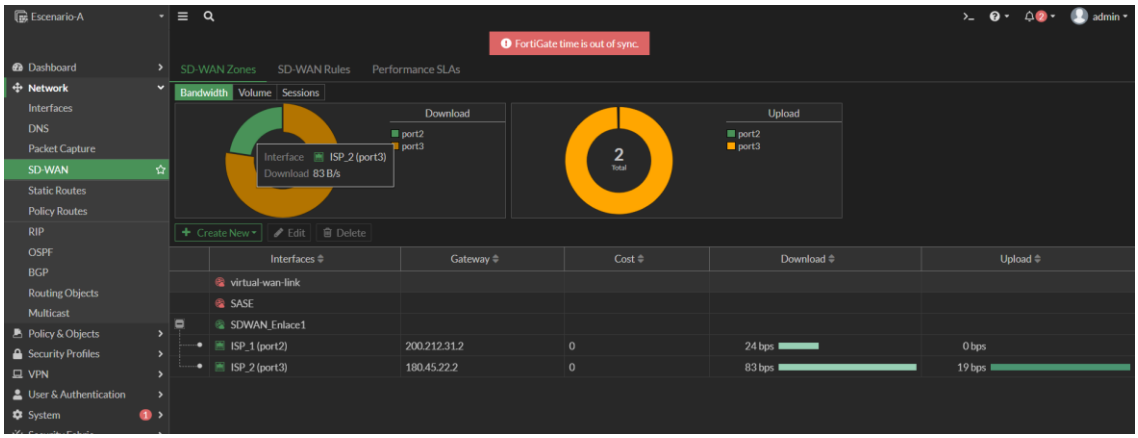
Nota. En esta figura se muestra la correcta configuración de las interfaces SD-WAN y su ruta estática.

Al momento de dirigirse hacia el monitor de SD-WAN se encontrarán 3 ventanas las cuales nos ayudarán a controlar el tráfico de internet.

La primera será “Bandwidth”, nos ayudará a monitorear cuanto ancho de banda se ha utilizado, y por lo que se puede evidenciar, de momento se está usando con mayor grado el segundo enlace.

Figura 37

Monitoreo del ancho de banda

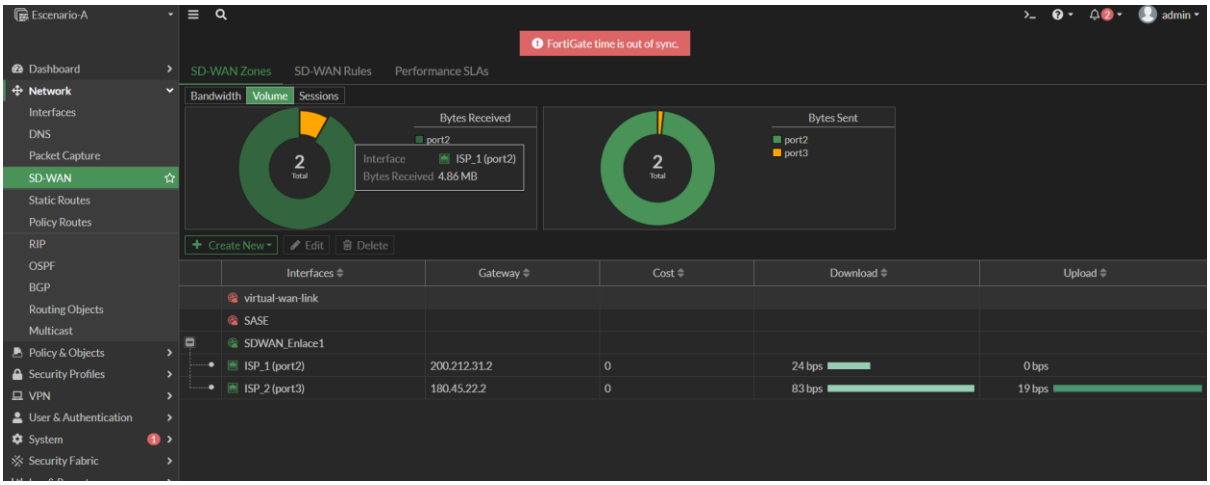


Nota. Esta imagen muestra la vista del monitoreo del ancho de banda de los ISP conectados y configurados en la red SD-WAN

El segundo será el “Volume”, es el monitoreo del volumen de datos enviados y recibidos. En este caso, se está utilizando de mayor grado el puerto dos igualmente.

Figura 38

Monitoreo del tráfico por Volumen

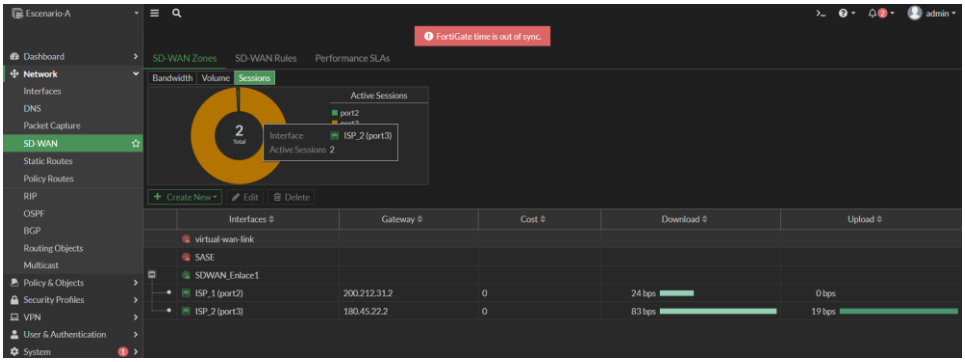


Nota. Esta figura muestra el monitoreo del tráfico de internet por medio del volumen.

Y, finalmente las sesiones usadas por cada enlace. De igual manera el segundo enlace está siendo usado a mayor gado.

Figura 39

Monitoreo del tráfico por sesiones.



Nota. Esta figura muestra el monitoreo del tráfico de internet por medio de las sesiones activas.

El criterio de selección se define en “SD-WAN Rules”, de momento se encuentra con una regla implícita que menciona lo siguiente:

- Nombre: SD-WAN.

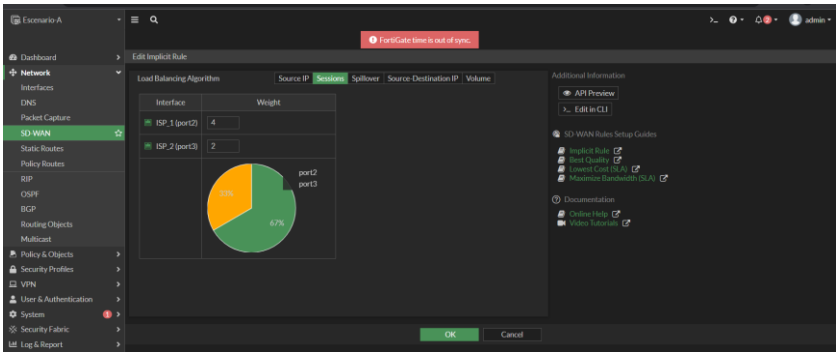
- Direccionado a todos los orígenes.
- Direccionado a todos los destinos.
- Criterio está basado en direcciones IP.
- Para todos los miembros.

Se puede cambiar el algoritmo de balanceo de carga. Para ello, se hará doble click en la regla implícita, se puede elegir el criterio dependiendo de la funcionalidad que se requiera.

- Basado en IP de origen.
- Basado en IP de origen y destino.
- Basado en el peso de las sesiones: Se podrá elegir que peso tendrá cada enlace.

Figura 40

Algoritmo basado en sesiones.

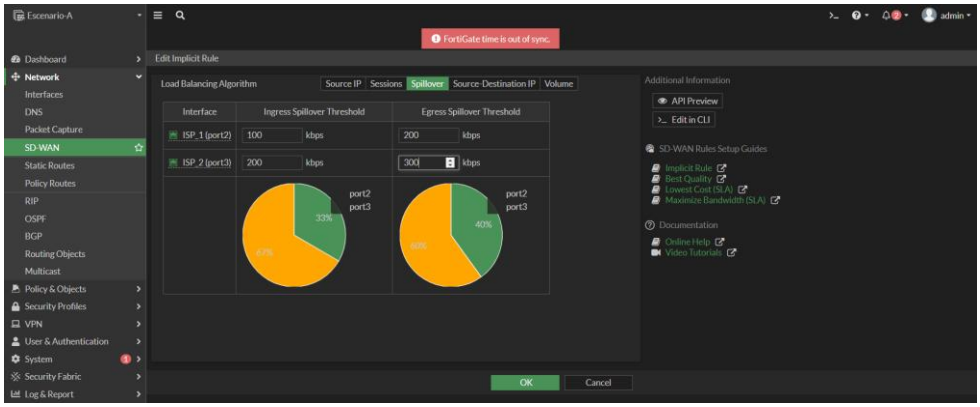


Nota. Esta imagen muestra el algoritmo de trafico de ancho de banda de modo “sesión”.

- Basado en el desbordamiento: Establece un umbral en Kbps el cual define que, si la cantidad de ancho de banda establecida en dicho umbral se excede, el ancho de banda excedió será enviado automáticamente a otra interfaz.

Figura 41

Algoritmo basado en desbordamiento.

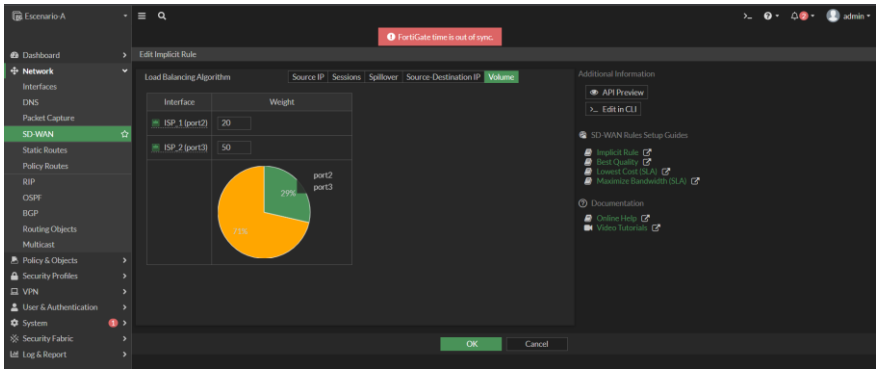


Nota. Esta imagen muestra el algoritmo de trafico de ancho de banda de modo "desbordamiento".

- Basado en volumen: En este criterio, se definirá cuanto ancho debanda en bits se necesita para cada enlace de internet.

Figura 42

Algoritmo basado en volumen.



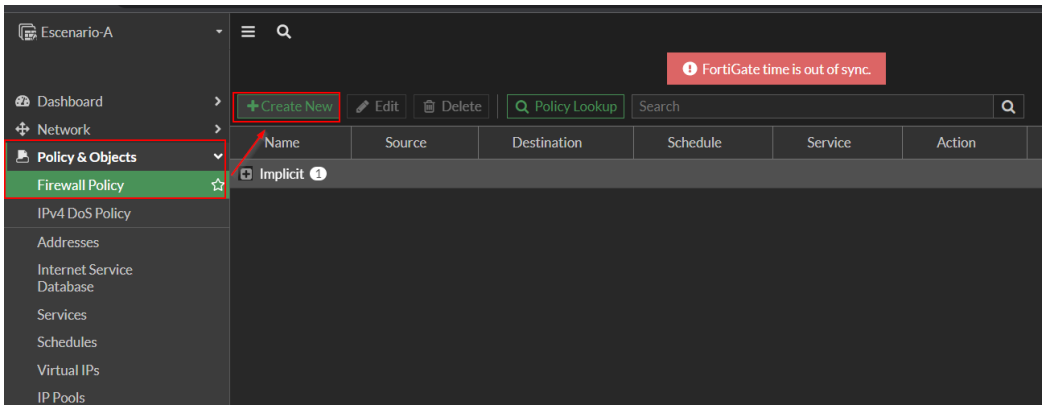
Nota. Nota. Esta imagen muestra el algoritmo de trafico de ancho de banda de modo "desbordamiento".

- Creación de política de firewall.

Para la creación de esta política y permitir que la red interna (LAN) de nuestros equipos tengan salida a internet, se deberá dirigir hacia "Firewall Policy" – "Create New"

Figura 43

Creación de políticas.



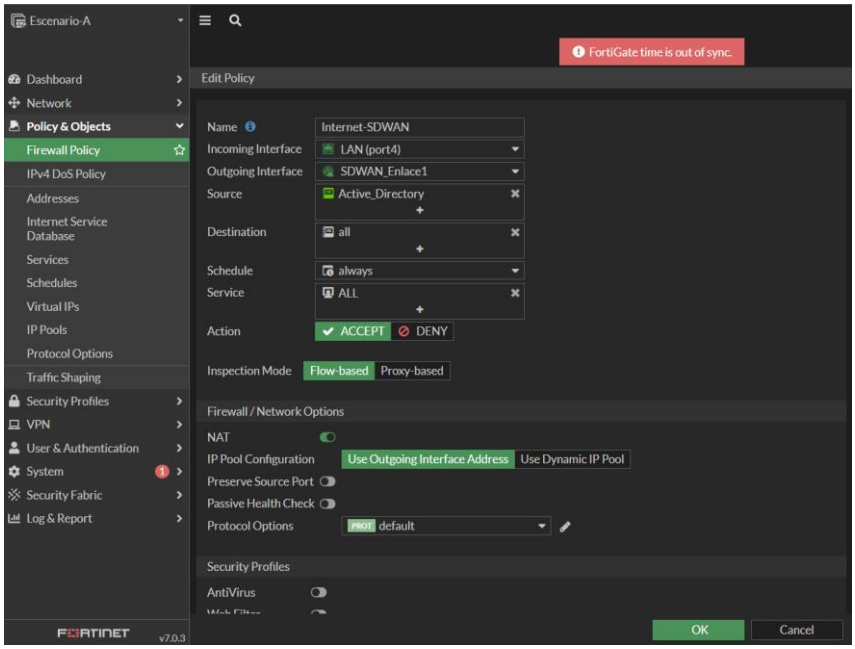
Nota. Esta imagen muestra como se crea una política de firewall desde lo más básico.

En donde se colocarán los siguientes parámetros:

- Nombre de la política.
- Puerto de entrada (Red LAN).
- Puerto de salida (Interfaz SDWAN-Enlace1)
- Como origen se selecciona el AD (Active Directory) que es el directorio activo dónde se encuentran los usuarios, equipos de la empresa.
- Destino “All” debido a es una póliza de internet.
- En todo momento.
- Para todos los servicios.

Figura 44

Parámetros de la política de firewall.

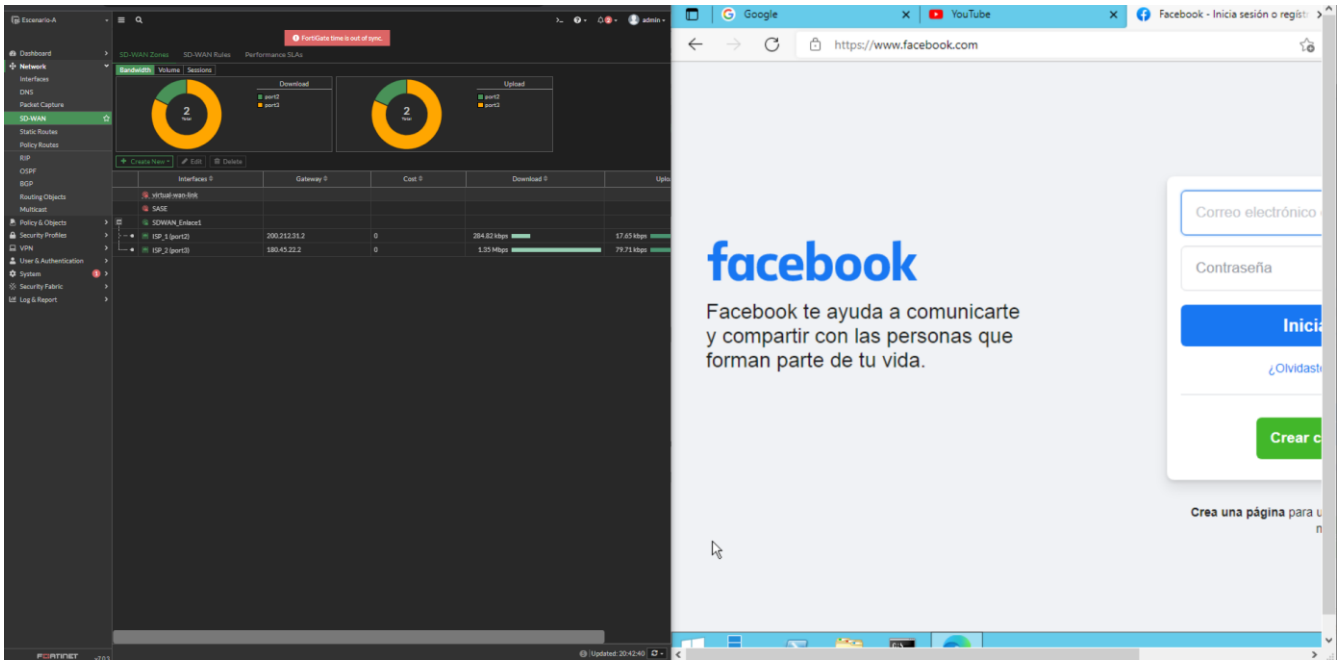


Nota. Esta imagen muestra los parámetros que se debe colocar para una correcta configuración de política de firewall.

Para comprobar las configuraciones, se abrirá el equipo conectado a este escenario y se abrirán varias páginas de internet para comprobar la salida al mismo y el monitoreo del ancho de banda de SD-WAN.

Figura 45

Comparación del monitoreo de ancho de banda



Nota. En esta imagen, se verifica que el monitoreo del tráfico de internet esté funcionando de manera normal.

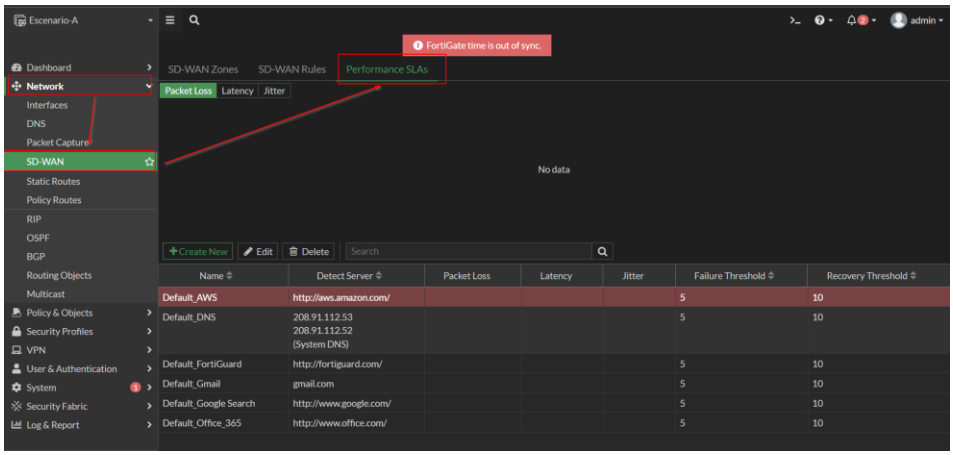
4.4.2. Performance SLA

Monitoreo de enlaces SLA es el encargado de medir el estado de los enlaces que se encuentren conectados a la interface de SD-WAN, se realizará mediante envío de señales medición por medio de cada enlace de internet con que se cuente. Una de las características esenciales de este servicio, es que, si un enlace se cae o se rompe todas las rutas asociadas a ese enlace se eliminan y el tráfico generado se enruta a través de otros enlaces asociados a SD-WAN, haciendo así, que nunca se pierda la conexión a los equipos, lo que permitirá una alta redundancia en los enlaces de la organización.

Este servicio se encuentra en la sección “Network” → “SD-WAN” → “Performance SLAs”

Figura 46

Visualización de interfaz Performance SLA.



Nota. Esta figura muestra la interfaz del servicio de Performance SLA.

Dentro de esta interfaz se encontrarán varios servicios pre cargados. Lo cual permitirá observar y verificar si responde o no el servicio. De igual manera sirve para determinar las pérdidas de paquetes, la latencia de los servicios. De esta manera, Fortinet podrá determinar si el enlace 1 (ISP_1) es más saludable que el enlace 2 (ISP_2) y redireccionar el tráfico hacia el más saludable.

En este caso, se usará un servicio ya pre definido (Default_AWS), dentro del mismo se encontrarán las siguientes definiciones o características:

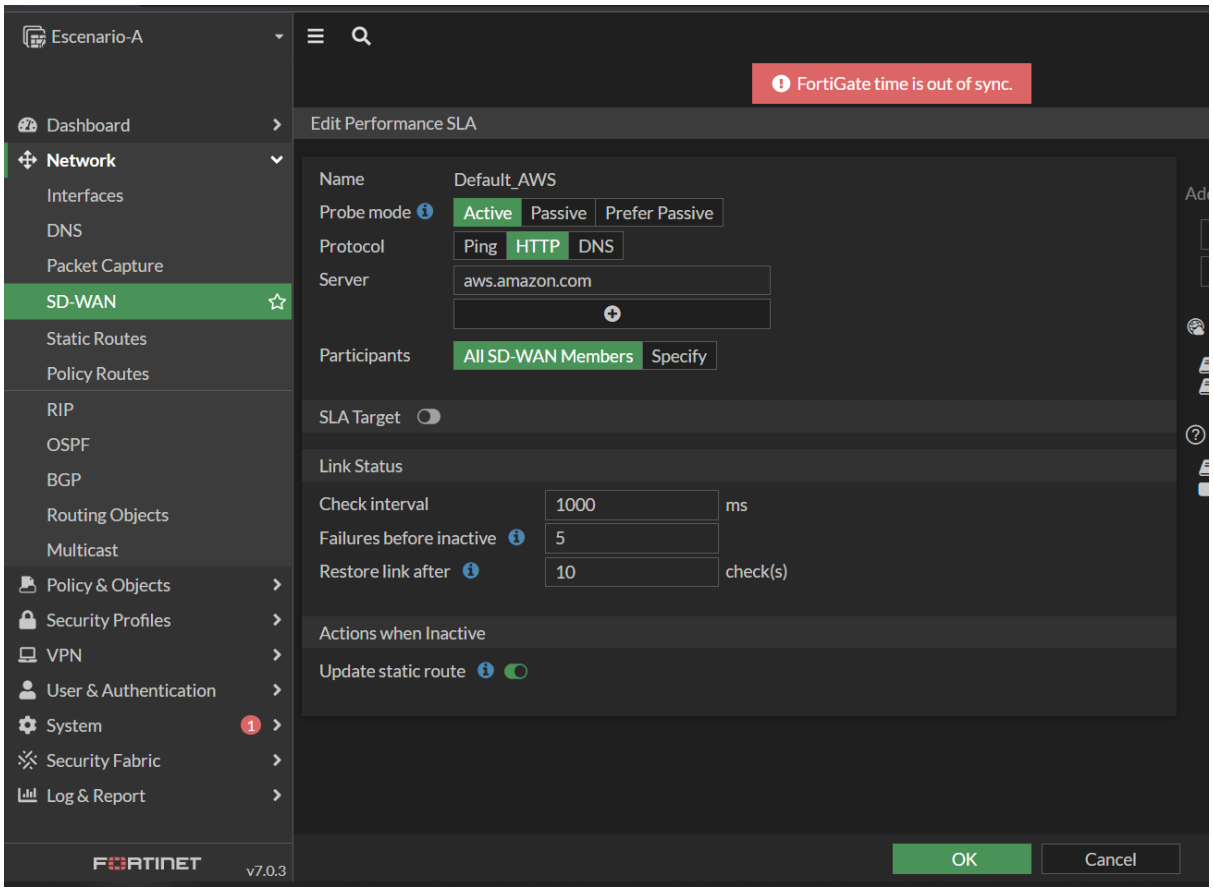
- Nombre: Default_AWS
- Probe mode: Define de qué forma Fortinet realizará las pruebas contra Amazon, se aprecian tres modos de prueba: Active – Passive – Prefer Passive.
    - Active: Fortinet envía paquetes contra el destino (aws.amazon.com)
    - Passive: Fortinet no envía paquetes de prueba, en cambio utiliza el tráfico generado para realizar la medición.
    - Prefer Passive: Es similar a “Active”, con la diferencia de que en el caso que no se genere tráfico contra Amazon, enviará recién los paquetes de prueba como si estuviera en Active.

- Protocolo: Ping – HTTP – DNS
- Server: Se elegirá el testigo, es decir a quien se enviará el paquete de prueba (aws.amazon.com).
- Participants: Se definirá que miembros de SD-WAN se utilizará para realizar la medición.
- Link status: Determinará si el vínvulo está activo o no:
    - Check Interval: Intervalo de tiempo (1 sg).
    - Failures before inactive: 5 paquetes
    - Restore link after: 10 check(s).

  Es decir, en intervalos de 1 segundo si 5 paquetes del protocolo fallan se de como caído el vínculo. Y, cuando el vínculo esté activo, deberán pasar 10 chequeas de manera satisfactorias para darlo como válido.
- Update static routes: Eliminará de las rutas estáticas el vínculo que haya fallado

Figura 47

Parámetros del servicio AWS.

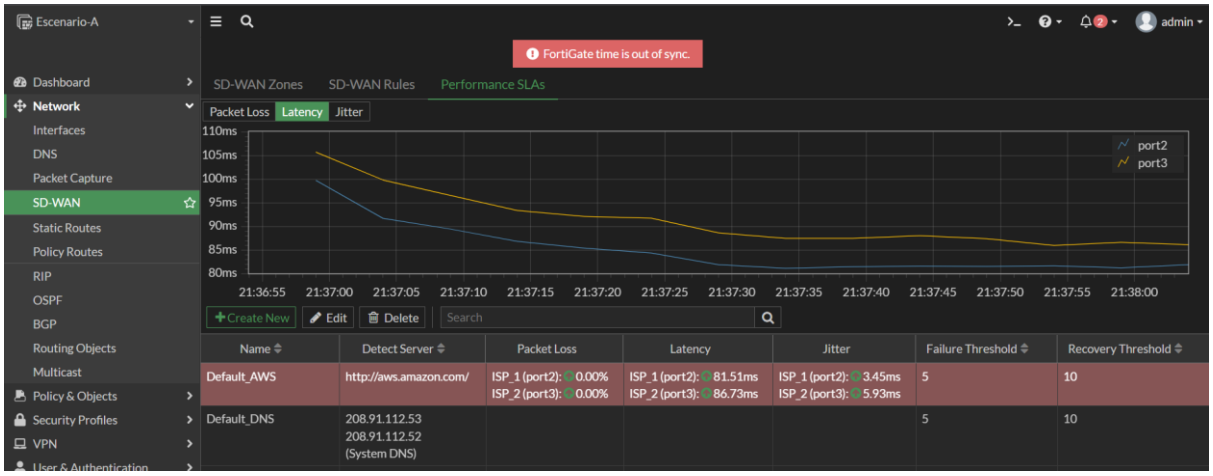


Nota. Esta figura muestra los parámetros que se deben considerar para un correcto monitoreo y gestión de servicios de Performance SLA.

La interfaz del Performance SLA, quedará de la siguiente manera, mostrando con las flechas verdes que el servicio se encuentra activo.

Figura 48

Monitoreo de la red con Performance SLA.



Nota. Esta figura muestra que los enlaces se encuentran trabajando de manera normal.

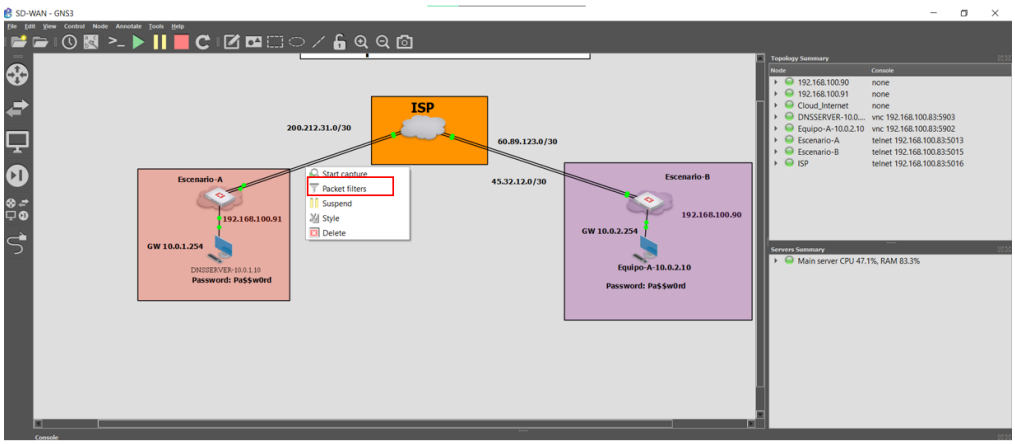
Se realizará una prueba en la que, el ISP_1 se sature de latencia lo que deberá causar que SD-WAN lo elimine de la tabla de enrutamiento para que no se pueda utilizar.

Con ayuda del GNS3, se procederá a ingresar ruido en el enlace ISP_1 para generar ciertas fallas y visualizar cómo funciona SD-WAN.

- Dentro de GNS3 se dará click derecho al enlace de internet ISP_1 y se colocará en la opción Packet filters

Figura 49

Ingreso al simulador para saturar la red.

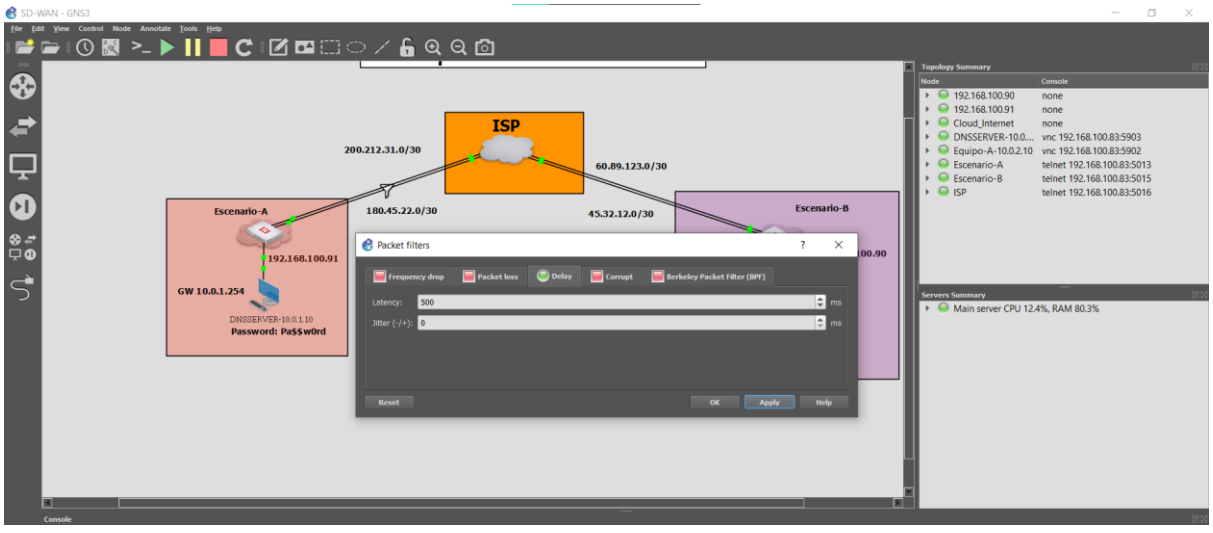


Nota. Esta figura muestra en dónde hay que entrar para saturar la red.

- En Delay, se aumentará la frecuencia a 500 ms

Figura 50

Saturación del enlace.

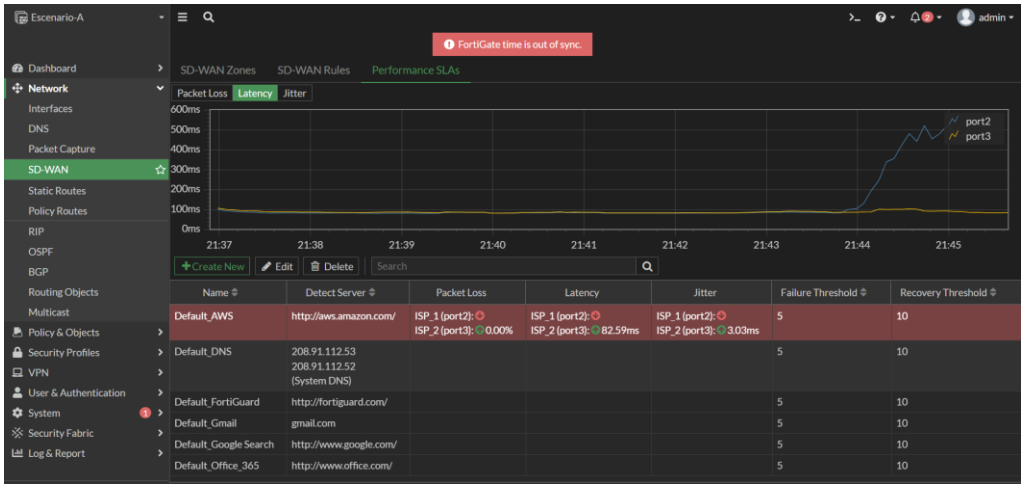


Nota. En esta figura se muestra la manera de saturar el ISP_1

- Como se puede apreciar, el ISP_1 se cayó, es decir no está saludable.

Figura 51

ISP_1 caído.

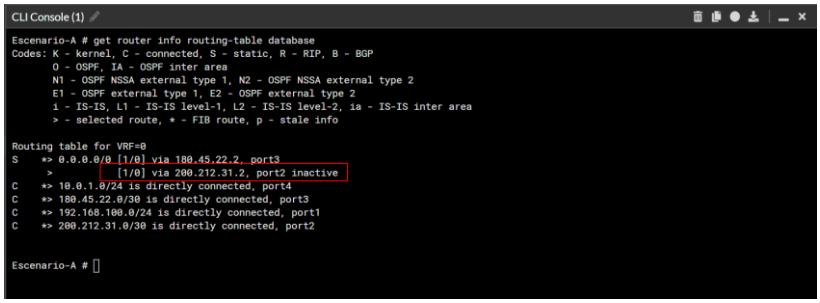


Nota. En esta figura se muestra el enlace caído por la anterior saturación.

- Si se comprueba la tabla de enrutamiento, se observa que el puerto 2 del ISP_1 está inactivo, esto es debido a que el Performance SLA lo eliminó de la tabla de enrutamiento.

Figura 52

Comprobación ISP caído



Nota. En esta figura se muestra como el ISP del puerto dos está caído por la saturación anterior.

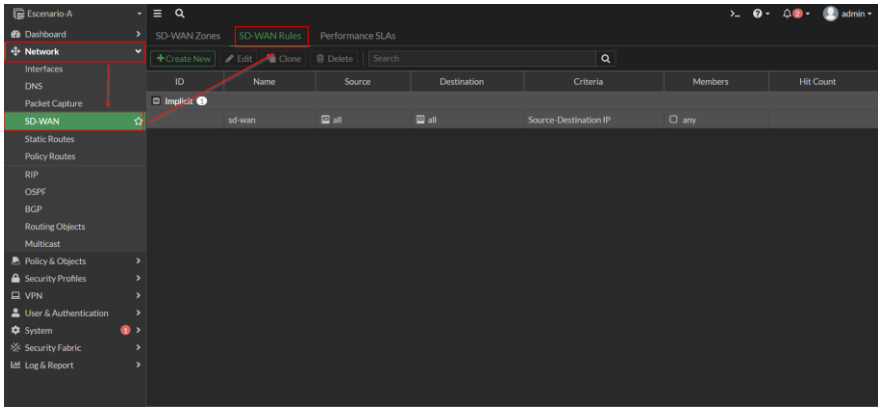
4.4.3. SD-WAN Rules

En este servicio se podrá definir que, para un cierto origen que necesite navegar a un cierto destino, se podrá definir que vaya por un enlace o por otro.

Dicho servicio se encuentra en el menú de “Network” a “SD-WAN” ♋ “SD-WAN Rules”.

Figura 53

Servicio SD-WAN Rules



Nota. Esta figura muestra la interfaz principal del servicio “SD-WAN Rules”

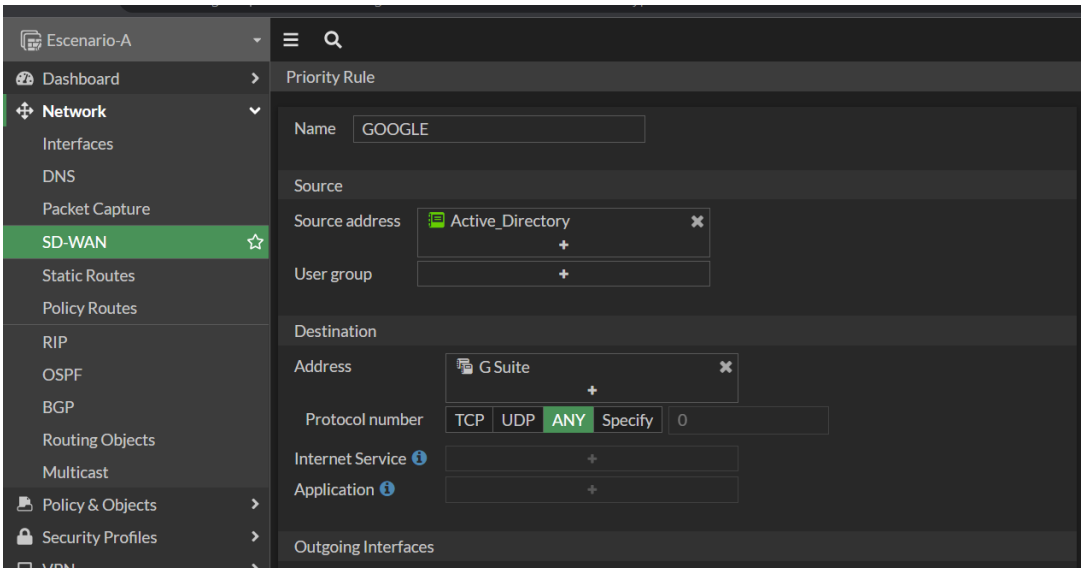
Para crear una nueva regla, se seleccionará “Create New”, en dónde se podrá configurar dependiendo el requerimiento de la regla. En este caso, se colocarán los siguientes parámetros.

- Name: Google.
- Source: Origen en dónde se definirá una dirección IP o un grupo de usuarios. En nuestro caso se usará el Active Directory.
- Destination: Se podrá elegir tres opciones:
  - Dirección de destino.
    - Si se trabaja con dirección de destino, se podrá especificar el protocolo (TCP – UDP – ANY - Specify)
  - Servicio de Internet.
  - Definir aplicación.

Esta primera parte se interpreta de la siguiente manera: “Cuándo nuestro Active Directory quiera navegar hacía Gmail.com”, hará mathc con la regla creada y realizará lo que el administrador configure.

Figura 54

Creación de regla SD-WAN

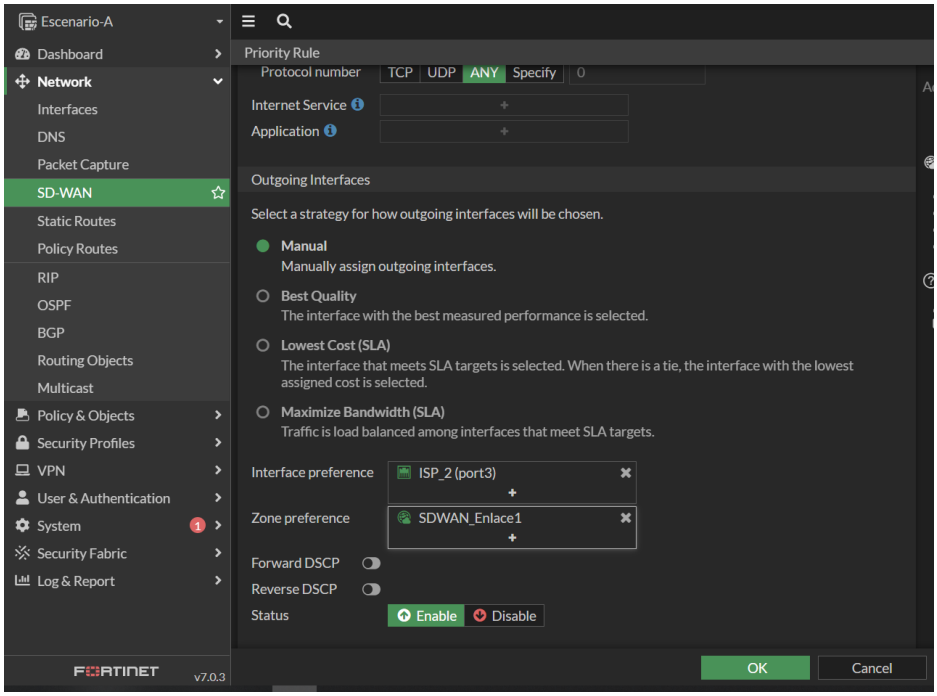


Nota. Esta figura muestra la primera parta para la creación de una Regla SD-WAN

- Se cuenta con cuatro estrategias para configurar:
    - Manual: Direcciona el tráfico que produce el AD al conectarse a servicios de Google hacía el ISP_2.

Figura 55

Estrategia Manual

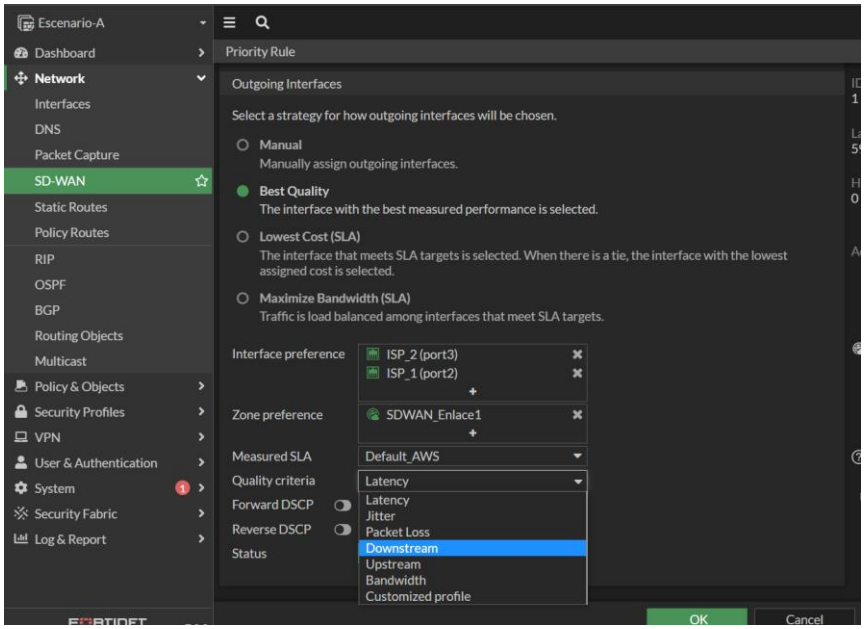


Nota. Esta imagen muestra la configuración de la estrategia manual en la creación de reglas SD-WAN.

- Mejor calidad: Se selecciona la interfaz con el mejor rendimiento medido, en dónde se elegirán más de un enlace de internet y el criterio de calidad. Es decir, el vínculo que tenga mejor latencia, será por el cual Fortinet envíe el tráfico al momento de que el AD se conecte a servicios de Google.

Figura 56

Estrategia Mejor Calidad

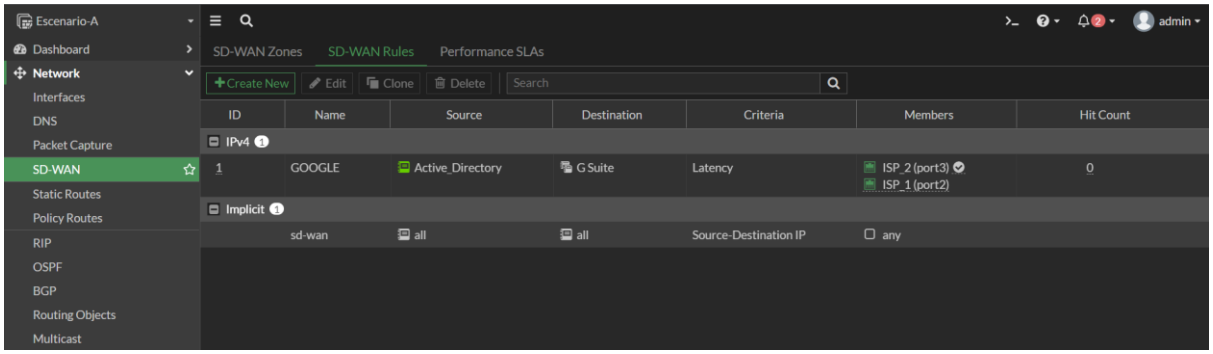


Nota. Esta figura muestra la configuración para una estrategia de mejor calidad.

Como se puede apreciar, el preferido es el ISP_2

Figura 57

ISP Preferido

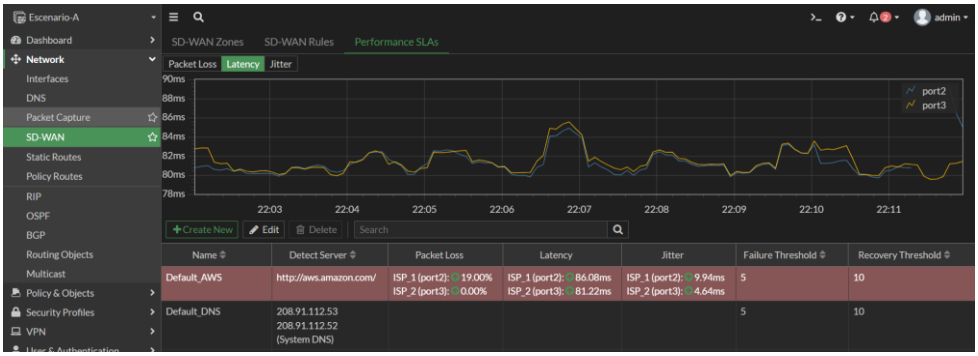


Nota. Esta figura muestra el ISP Preferido en la estrategia de mejor calidad

Esto sucede debido a que la latencia de dicho ISP es un poco menor a la otra.

Figura 58

Latencia ISP_1 & ISP_2



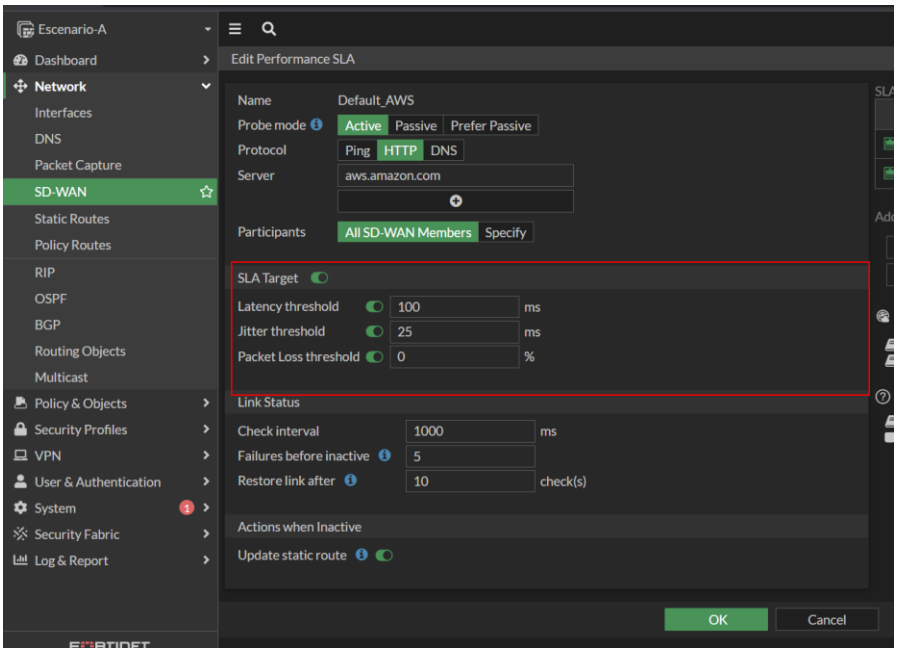
Nota. Esta imagen muestra la latencia que tienen los dos proveedores de internet.

- Costo más bajo (SLA): Se selecciona la interfaz que cumple con los objetivos de SLA. Cuando hay empate, se selecciona la interfaz con el costo asignado más bajo.

Este servicio trabaja en conjunto con “SLA Target” ubicado en el Performance SLA. En primer lugar, se deberá establecer los umbrales de latencia, jitter y paquetes perdidos.

Figura 59

Configuración SLA Target

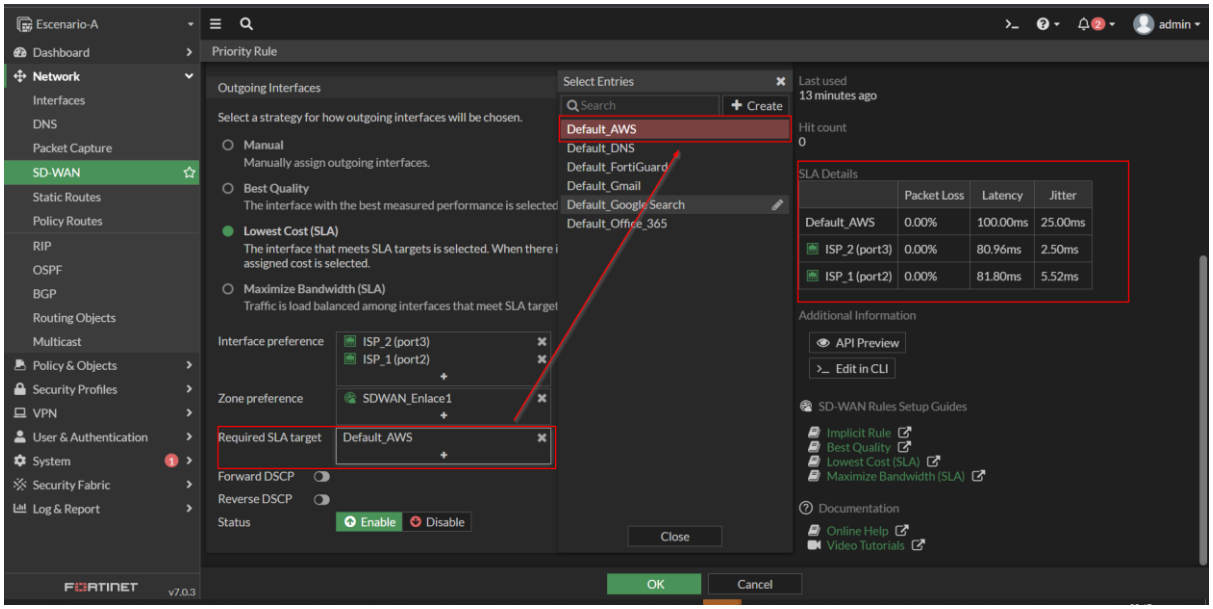


Nota. Esta figura muestra la configuración del SLA Target para configurar la estrategia de costo más bajo.

Una vez realizada dicha configuración, se deberá configurar la estrategia de “Lowest Cost (SLA)”.

Figura 60

Estrategia costo más bajo.

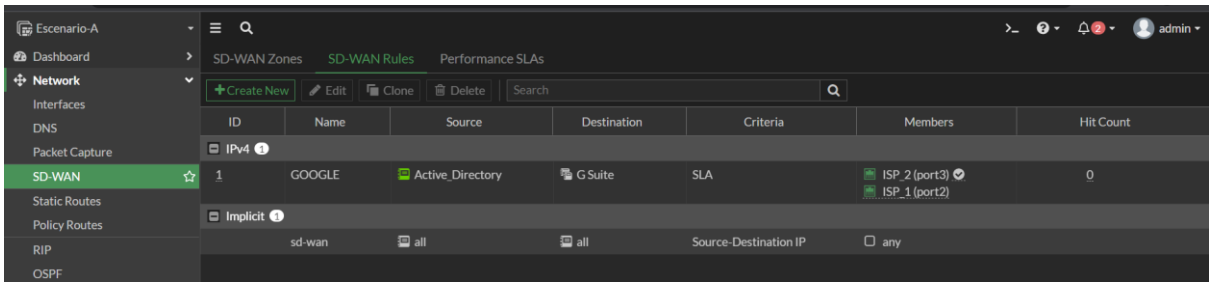


Nota. Esta figura muestra la configuración para la estrategia de costo más bajo.

Como se puede apreciar, el preferido para este caso será el ISP_2

Figura 61

ISP Preferido



Nota. Esta imagen muestra el ISP Preferido dependiendo de la latencia configura en el SLA Target.

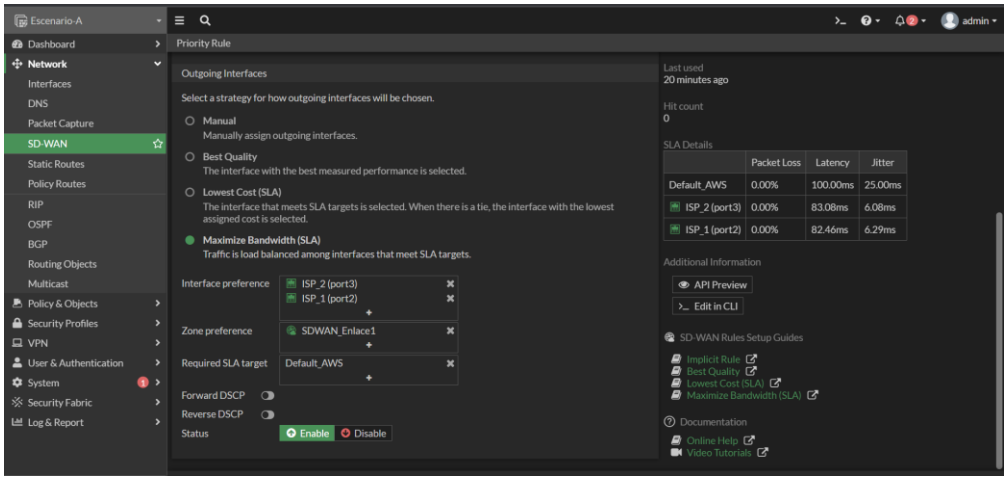
Esto se debe a que, el algoritmo decide que SLA está cumpliendo su cometido. Sin embrago, existe el caso de que los dos ISP cumplan el SLA establecido, en ese caso, el algoritmo enrutara el que tenga mejor respuesta de cumplimiento.

- Maximizar el ancho de banda (SLA): La carga del tráfico se equilibra entre las interfaces que cumplen los objetivos de SLA.

Este algoritmo balanceara el tráfico entre los dos ISP siempre y cuando ambas interfaces cumplan con el SLA establecido.

Figura 62

Configuración estrategia maximizar el ancho de banda.

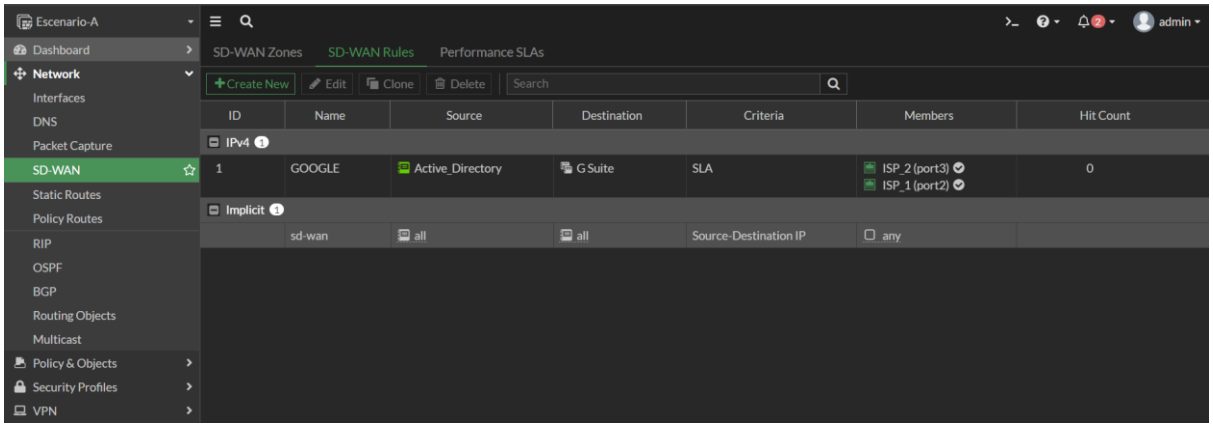


Nota. Esta figura muestra la configuración para la estrategia de maximizar el ancho de banda.

Como se puede apreciar preferirá los dos ISP debido a que estos cumplen con el SLA establecido.

Figura 63

IPS Preferido



Nota. Esta imagen muestra el ISP Preferido dependiendo de la latencia configura en el SLA Target.

Estos servicios, permitirán que el administrador pueda elegir cual es mejor para las necesidad o requerimientos que tenga la organización, así podrá alinearse a optar por una u otra opción o configuración.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se diseñó y configuró de manera exitosa una simulación que permitió evidenciar la alta redundancia y seguridad del tráfico de internet mediante la tecnología SD-WAN con ayuda de equipos Fortigate.
- Entre las principales ventajas de implementar SD-WAN en una organización, es la adaptabilidad a las necesidades de los administradores de infraestructura tecnológica, obteniendo la facilidad de modificación y actualización de políticas, rutas, y demás aplicaciones de red, siendo estas la base del funcionamiento de cualquier empresa.
- Dentro de los servicios que Fortinet ofrece, se cuenta con tres aspectos fundamentales para el cometido de este proyecto el cual era la alta redundancia, los cuales son: SD-WAN Zones (Creación de interfaces y monitoreo del tráfico de la red), SD-WAN Rules (Creación de reglas para los diversos servicios con diferentes estrategias para el balanceo del tráfico de internet) y Performance SLA (Se podrá definir contra que servidores externos o internos se miden la salud de los enlaces.).
- Con ayuda de la interfaz Fortigate, se evidenció el monitoreo del tráfico de red, realizando pruebas de funcionamiento en caso de que un enlace se caiga para que la comunicación no se pierda, sino que escale a otro enlace de manera automática. Mostrando que es posible la automatización de la infraestructura, lo que hasta el momento se ha venido realizando a través del personal técnico.

- La implementación de una red SD-WAN, ayudará a la empresa a tener un mejor control del tráfico de ancho de banda con ayuda de los servicios presentados y simulados en el presente proyecto del trabajo de titulación.

Recomendaciones

- Para realizar la simulación de enlaces de internet con equipos Fortigate para la creación de SD-WAN es necesario contar con un equipo con características, como: 8GB RAM, 256 Almacenamiento interno, Sistema Operativo Windows actualizado a la última versión, procesador i5 9th generación (igual o superior) con el fin de diseñar y configurar las diversas redes o equipos de manera satisfactoria.
- Es importante considerar la versión del firmware que se está utilizando en los equipos de Fortigate, a la fecha actual, se utilizó el firmare 7.0.3. Si se utilizan versiones anteriores, las configuraciones, servicios y aplicaciones SD-WAN no tendrán un comportamiento óptimo ni estarán disponibles todos los servicios.
- Para el diseño de una red SD-WAN se debe considerar el tamaño de la empresa y el giro del negocio de la misa, con este análisis se podrá obtener una mejor visión de que servicios o equipamiento SD-WAN se deberá adquirir para su configuración.

BIBLIOGRFÍA

- Roncancio Castellanos, J. A. La tecnología un avance social o una necesidad general.
- Rangan, R. K. (2020). Trends in SD-WAN and SDN. CSI Transactions on ICT, 8(1), 21-27.
- Pamplin, S. (2021). SD-WAN revolutionises IoT and edge security. Network Security, 2021(8), 14-15.
- Cusco-Pérez, W. X., Cabrera-Mejía, J. B., & Lugo-García, J. (2022). Análisis de las tecnologías SD-WAN usadas en Ecuador. Dominio de las Ciencias, 8(2), 870-886.
- Carrasco Cabrera, F. A. (2020). Diseño y simulación de una red de accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador.
- Ramos Fernández, J., & Fernández Navajas, J. (2019). Implementación y evaluación de un sistema SD-WAN para un entorno empresarial virtualizado.
- Marín Santamaría, L. A. (2021). Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos.
- Noboa, V. B. (2021, 24 abril). *Repositorio Institucional de la Universidad Politécnica Salesiana: Diseño e implementación de un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN) en el laboratorio de telecomunicaciones para la Universidad Politécnica Salesiana sede Guayaquil*. https://dspace.ups.edu.ec/handle/123456789/20114
- Fernández, L. (2020, 7 marzo). *Para qué sirve la segmentación de redes y por qué es recomendable implementarla*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/segmentacion-red-vlan-que-es/

GLOSARIO DE TÉRMINOS

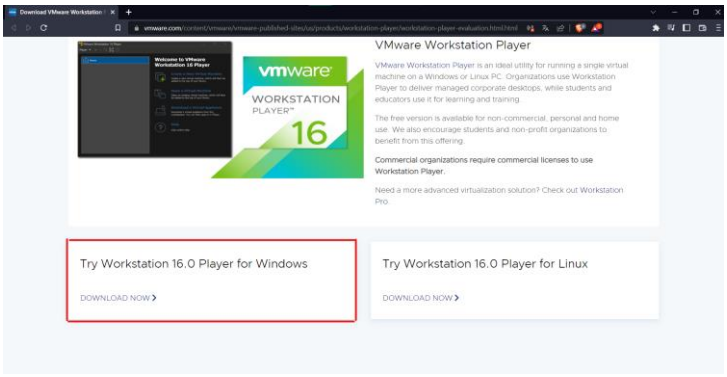
ANEXOS

Anexo A: Instalación VMware

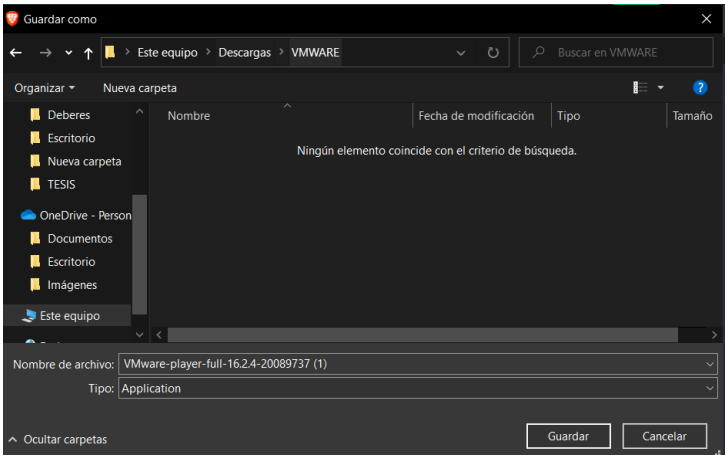
Paso 1

La siguiente página web contendrá el instalador de la máquina virtual VMware: https://www.vmware.com/content/vmware/vmware-published-sites/us/products/workstation-player/workstation-player-evaluation.html.html.

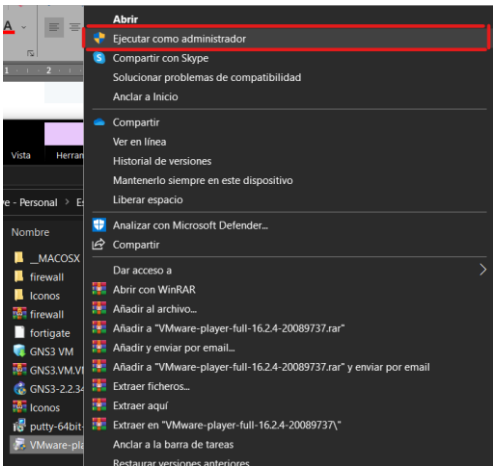
Al bajar, se encontrarán dos opciones, para Windows y para Linux, en nuestro caso se elige Windows.



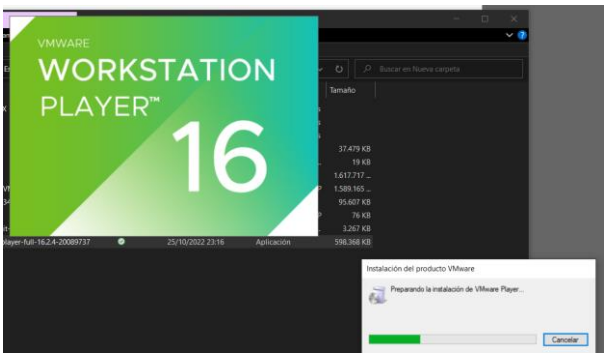
Se elige la ruta donde se requiere descargar el instalador.



Se ejecuta como administrador el instalador.

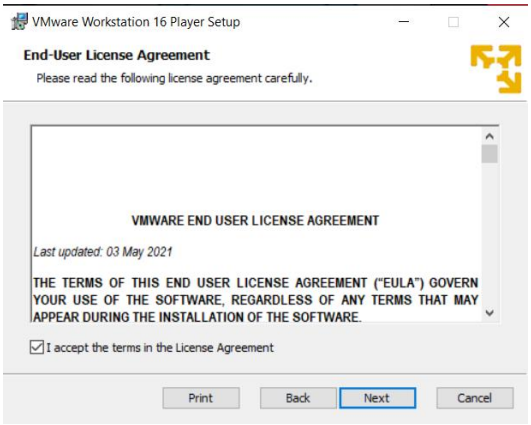


Se conceden los permisos necesarios de administrador y de inmediato procederá con la descarga.

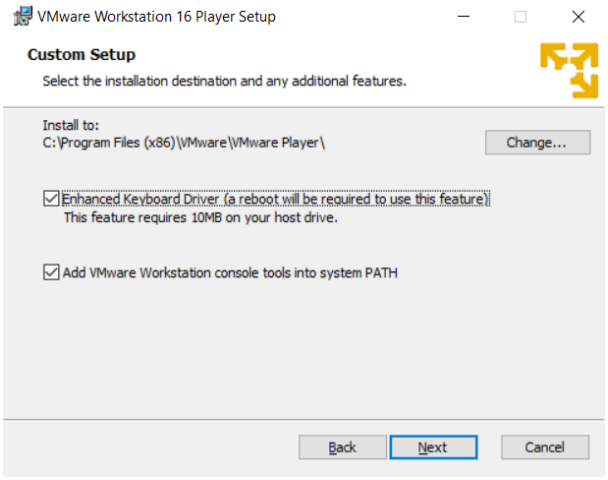


Se obtendrá una primera pantalla de bienvenida al VMware, click e “Next” o “Siguiente”.

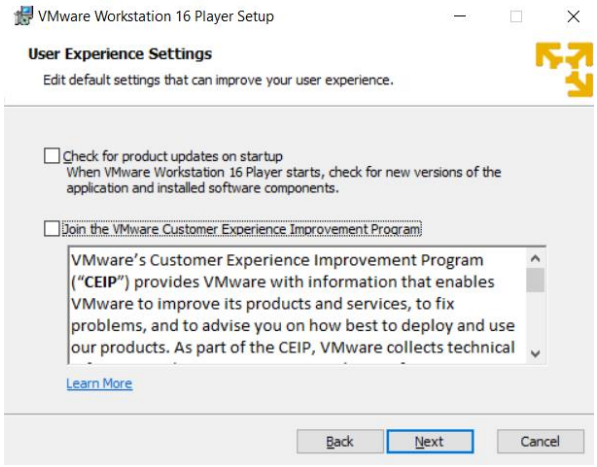
Se acepta la licencia y se continúa.



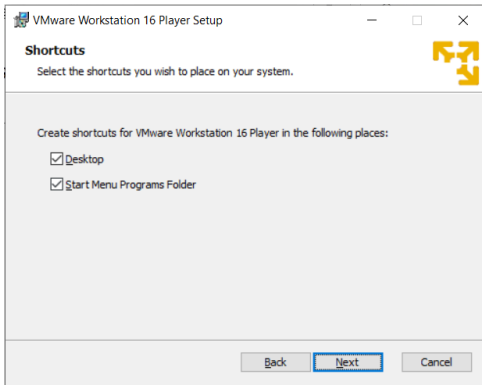
Se tendrán que marcar la opción para instalar el teclado mejorado.



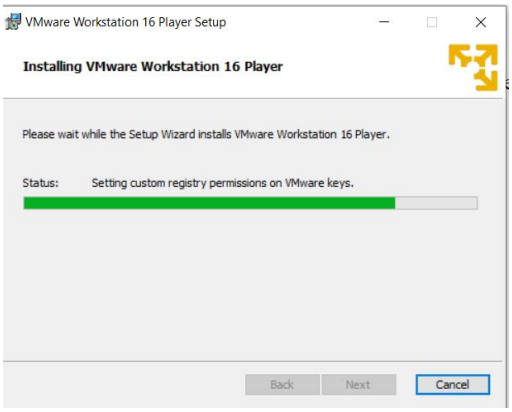
Se deberá desmarcar las opciones que harán que lleguen notificaciones de actualizaciones.



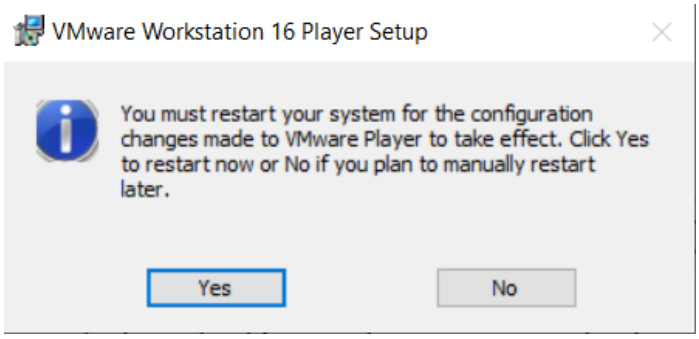
Se dejará marcado lo que viene predeterminando para que se cree un acceso directo en el escritorio.



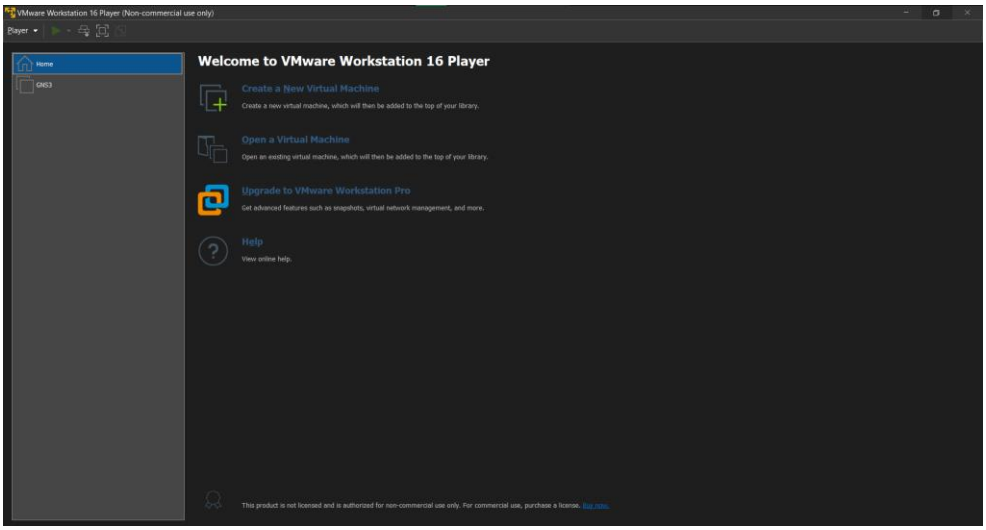
Al darle click en install, la instalación comenzará.



Y finalmente para acabar con la instalación se tendrá que reiniciar el equipo



La interfaz que se obtendrá es la siguiente



Con esta herramienta de virtualización se podrá montar el simulador GNS3 para proceder con el diseño y configuración de red SD-WAN para cumplir con el cometido del proyecto propuesto.

Anexo B: Instalación y configuración GNS3 en VMware

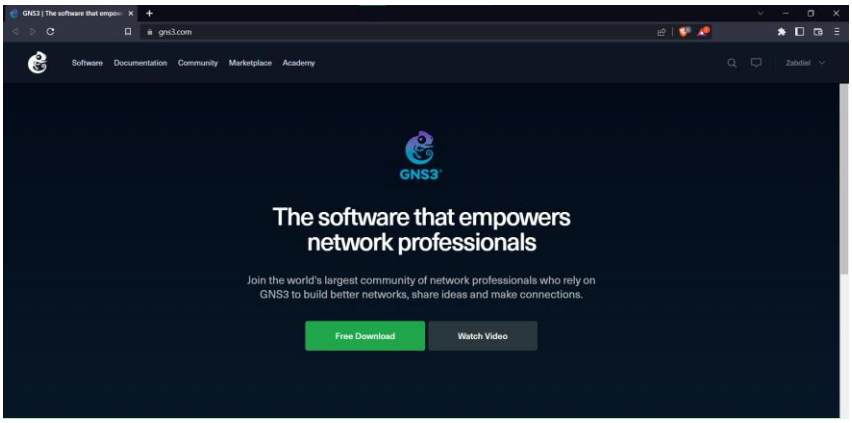
Para GNS3 se tendrá dos instaladores, cliente y el servidor.

El cliente se instala en la máquina normal donde se harán las pruebas, mientras que el servidor se montará en la VM antes instalada.

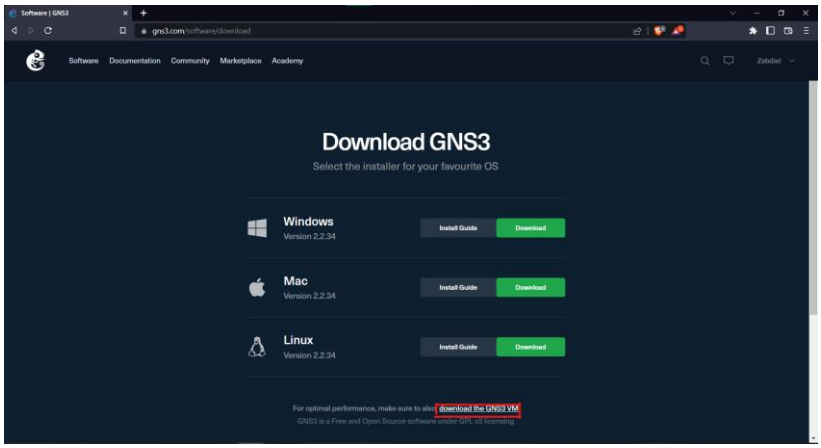
Instalación Servidor

Para la instalación del servidor de GNS3 se tendrá que dirigir hacia la página principal: https://gns3.com/.

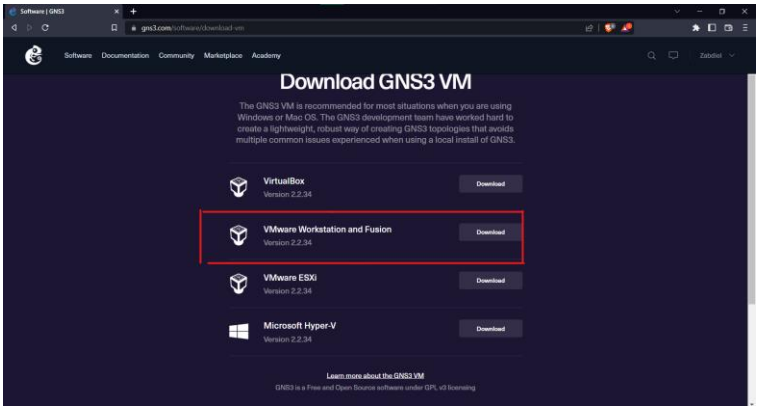
Se presiona en “Free Download”.



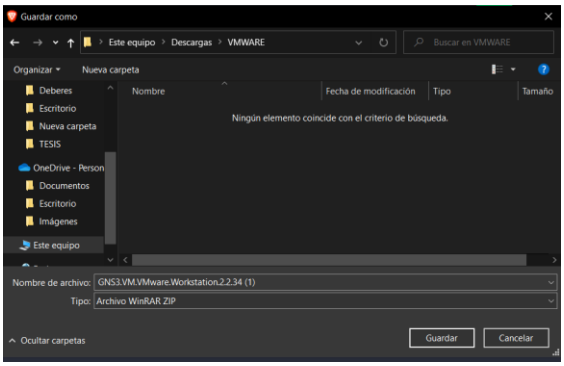
En la parte inferior se encuentra un apartado llamado “download the GNS3 VM”.



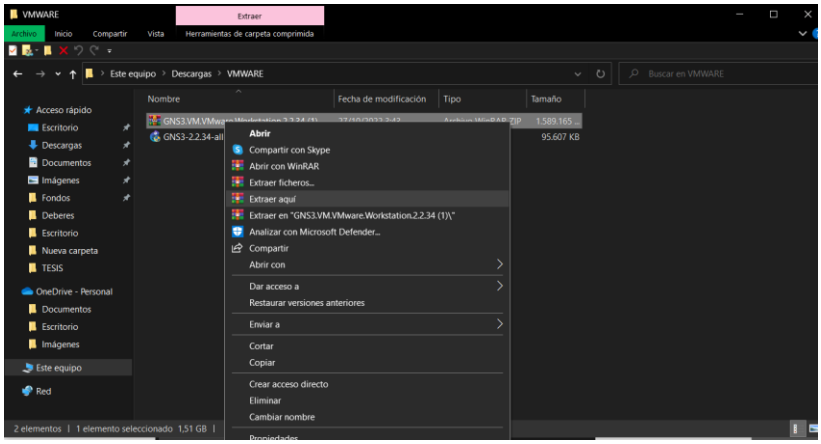
Al presiónalo aparecerán varias opciones para diversas VMs. En nuestro, caso se escoge el segundo para ejecutarlo en la VM instalada anteriormente.



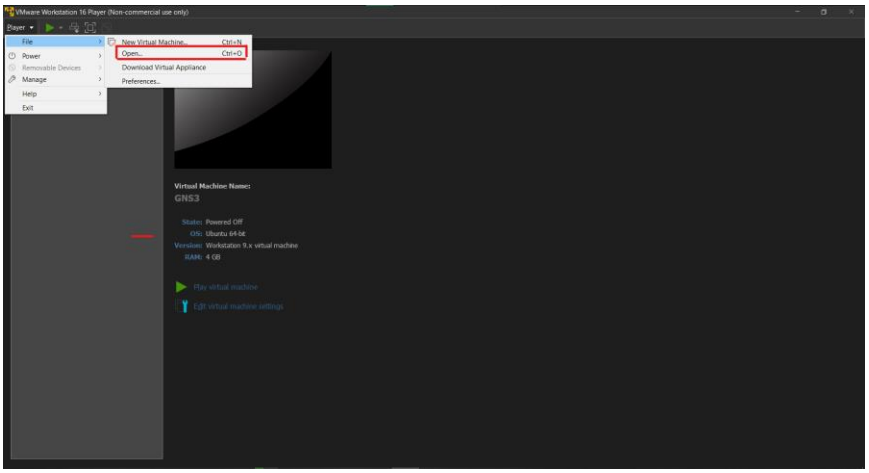
De igual manera se escoge la ruta donde se guardará el archivo.



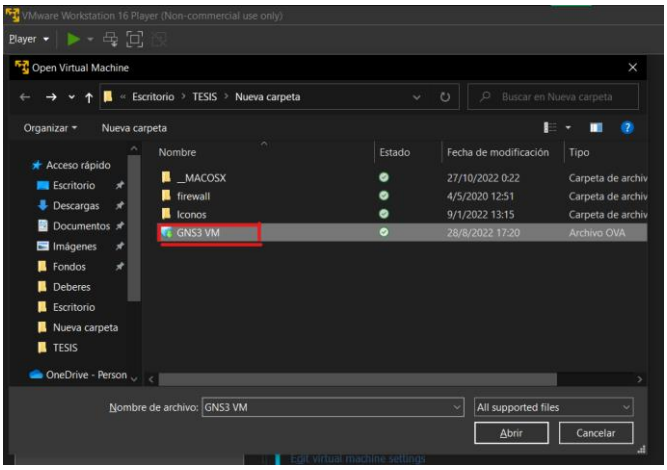
Este archivo viene en un .rar, se deberá descomprimir para que muestra la imagen necesaria.



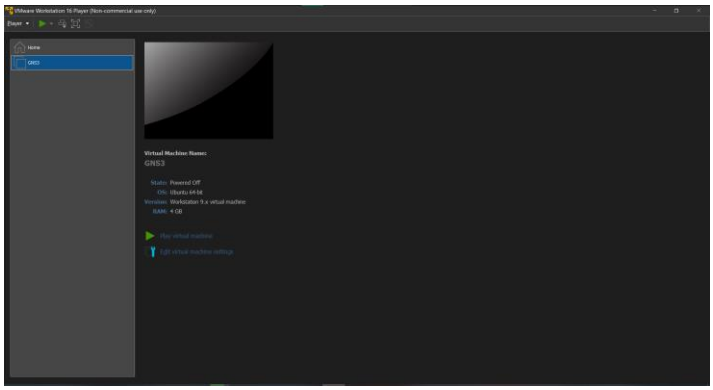
En VMware se deberá abrir la imagen descargada anteriormente.



Se buscará la ruta donde se había guardado la imagen, se elige dicha imagen y se abre.

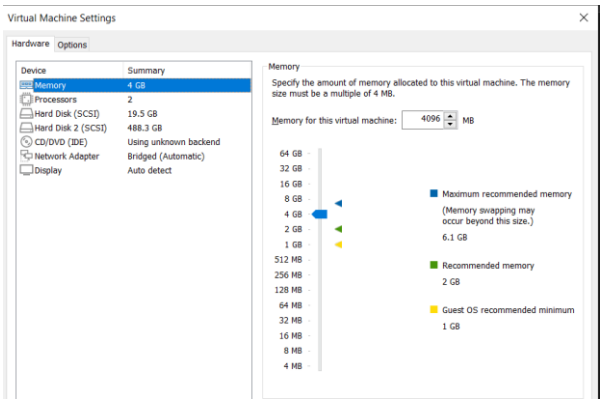


Quedará tal que así.

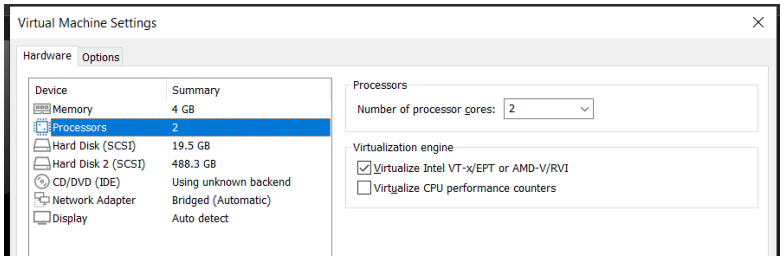


Un punto muy importante es que, antes de empezar, se debe configurar la máquina virtual de la siguiente manera:

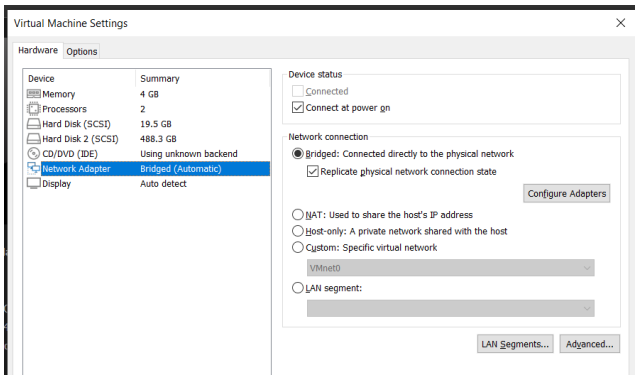
Memoria:



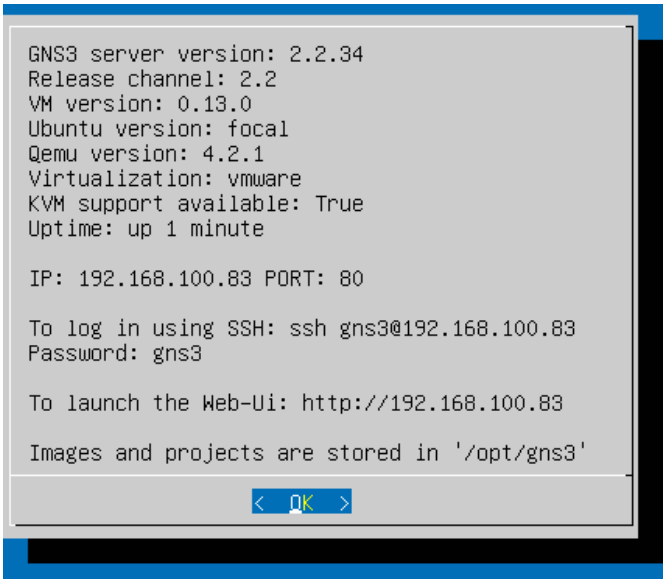
Procesadores



Adaptador de Red



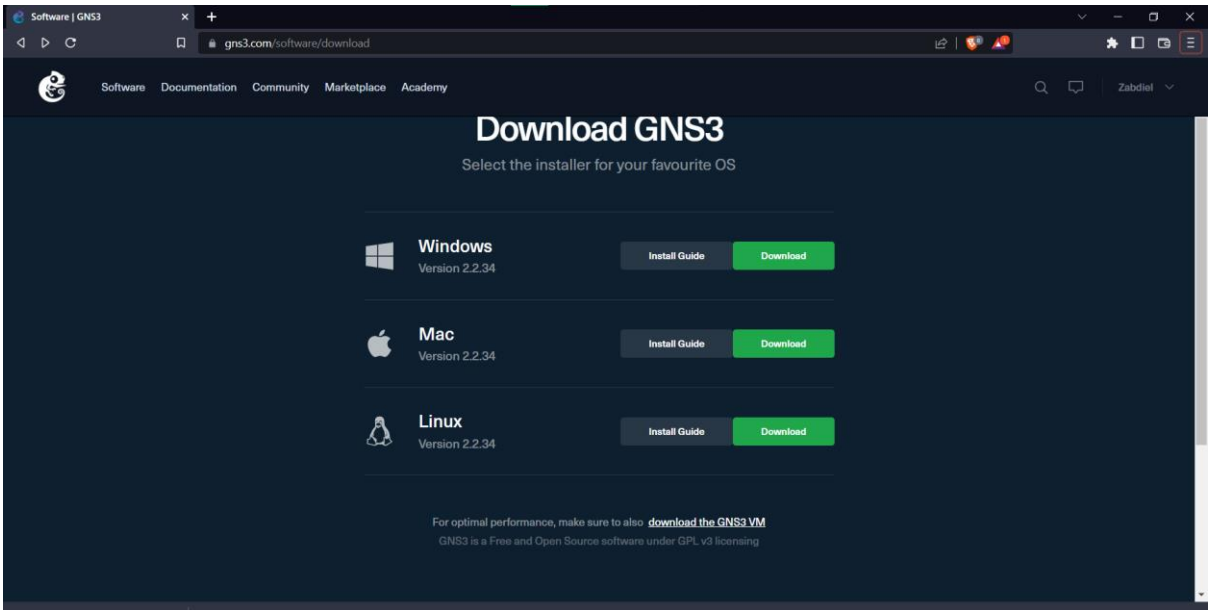
Al iniciar la máquina virtual saltará la siguiente pantalla:



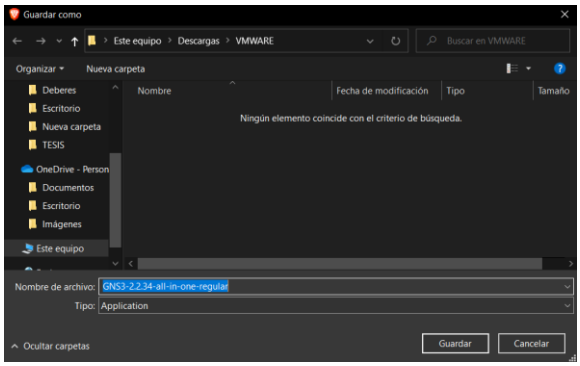
La información que muestra es muy relevante para GNS3 Cliente ya que muestra la IP, el puerto, usuario y contraseña.

Instalación Cliente

Para instalar el cliente, de igual manera se buscará la página: https://gns3.com/software/download y se selecciona el SO que se esté manejando



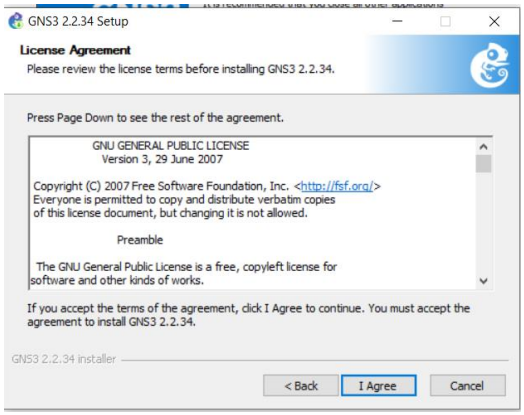
De igual manera se selecciona la ruta donde se guardará el instalador



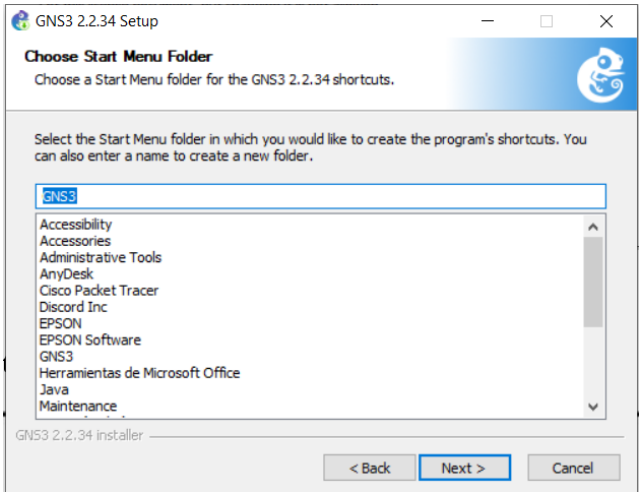
Se ejecuta la aplicación

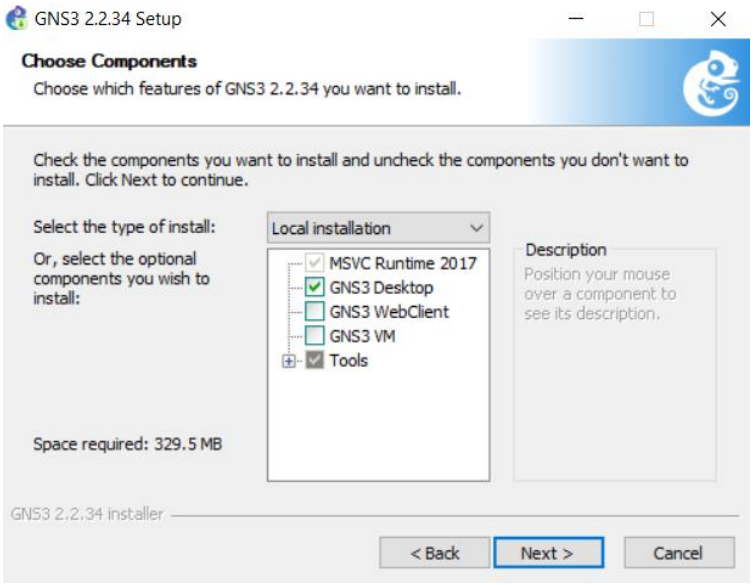
Así como VMware, GNS3 nos da la bienvenida a lo que se debe presionar en siguiente:

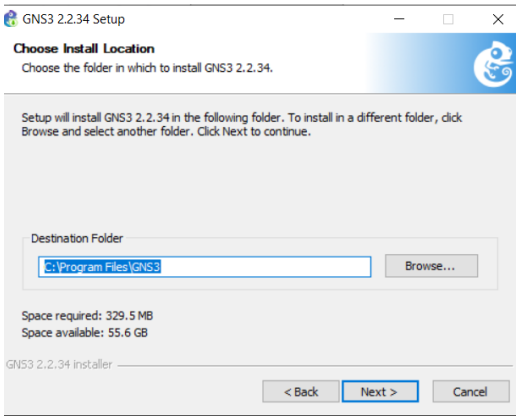
Se acepta la licencia



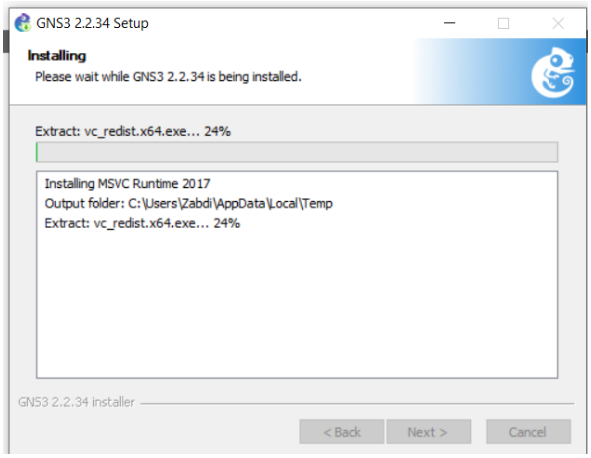
Se deja predeterminado todo lo siguiente.



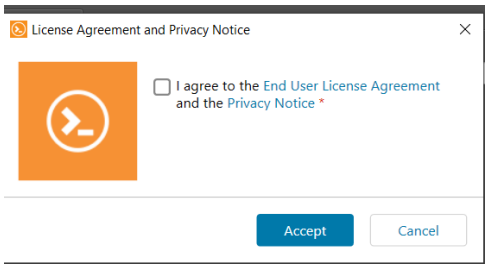




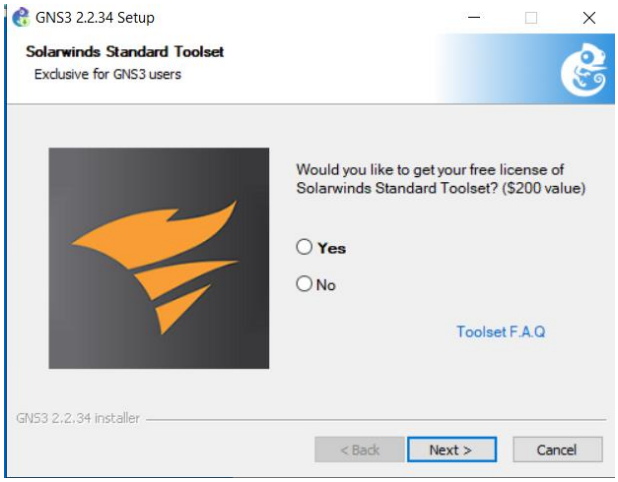
Empezará con la instalación.



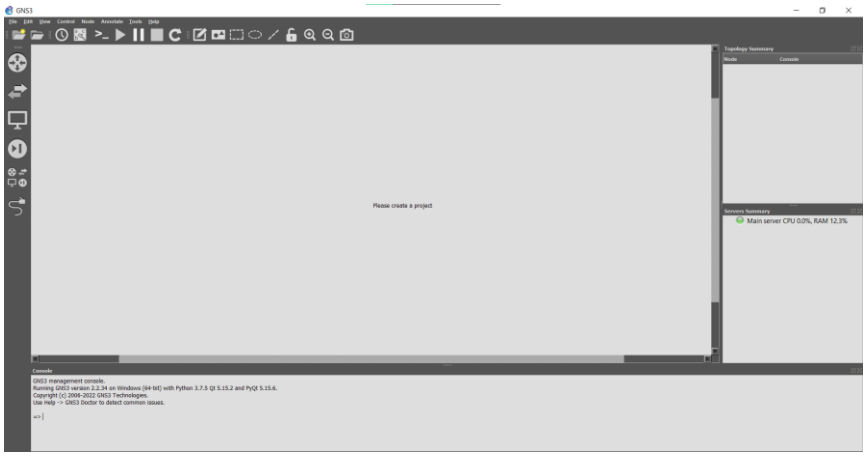
´Se cancela la siguiente pestaña.



Y se coloca “NO” en la última fase de la instalación.

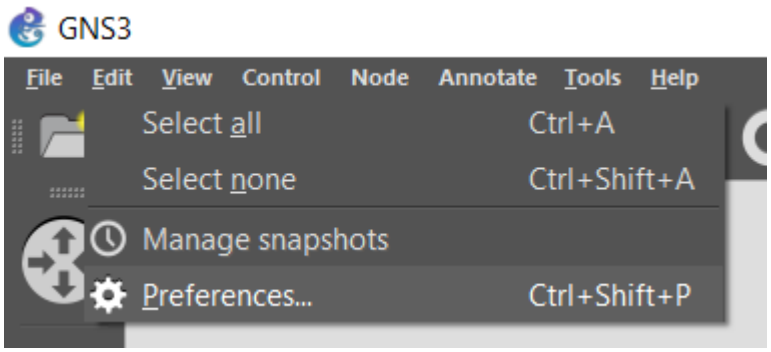


La interfaz que se obtiene es la siguiente.

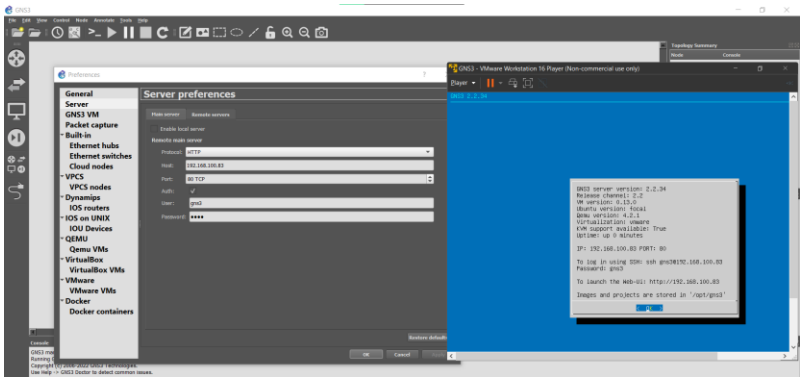


Finalmente se procede con la configuración en base al GNS3 servidor.

Se debe buscar “preferencias”, ubicada en la pestaña “edit”



En server, se colocan los datos del servidor, tal como en la siguiente imagen



Y el emulador GNS3 estaría correctamente instalado.

El fin de dicha instalación es, usar el emulador instalado para el diseño y configuración de la red SD-WAN con equipos Fortigate, en dónde se colocará los dispositivos y enlaces

necesarios para demostrar que usando una red SD-WAN existe una alta disponibilidad o redundancia entre enlaces de internet.