ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

SIMULACIÓN DE UNA RED SD-WAN MEDIANTE EQUIPOS DE NETWORKING EN GNS3

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

Félix Adrian Pérez Chávez
felix.perez@epn.edu.ec

Jefferson Francisco Gualoto Ramírez
jefferson.gualoto@epn.edu.ec

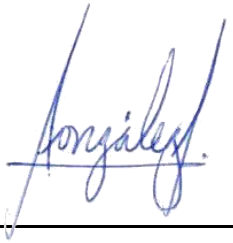
DIRECTOR: ING. Fernando Vinicio Becerra Camacho
fernando.becerrac@epn.edu.ec

CODIRECTOR: ING. Fabio Matías González González
fabio.gonzalez@epn.edu.ec

Quito, Enero 2022

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por los señores Félix Adrian Pérez Chávez y Jefferson Francisco Gualoto Ramírez como requerimiento parcial a la obtención del título de TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES, bajo mi/nuestra supervisión:



Fernando Vinicio Becerra Camacho

DIRECTOR DEL PROYECTO

ING. Fabio Matías González González

CODIRECTOR DEL PROYECTO

DECLARACIÓN

Nosotros Félix Adrián Pérez Chávez con CI: 1722169099 y Jefferson Francisco Gualoto Ramírez con CI: 1723408207 declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

Sin prejuicio de los derechos reconocidos en el primer párrafo del artículo 144 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación – COESC-, somos titulares de la obra en mención y otorgamos una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la Escuela Politécnica Nacional.

Entrego/Entregamos toda la información técnica pertinente, en caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa nacional vigente.

Félix Adrian Pérez Chávez

Jefferson Francisco Gualoto Ramírez

DEDICATORIA

El presente proyecto de investigación lo dedico principalmente a Dios por haberme inspirado y por brindarme la fuerza necesaria para culminar todo el proceso en mi preparación académica.

A mis padres, ya que con su amor, esfuerzo, paciencia y sacrificio a lo largo de los años me han permitido llegar a este momento que tanto han esperado y a través de su orientación y consejo convertirme en un gran profesional y buena persona reflejo de todas sus enseñanzas, ha sido para mí un orgullo y un privilegio ser su hijo, son los mejores padres que un hijo podría desear.

A mis abuelos Julio y Dolores y tíos Franklin, William, Silvani, Gilian y Leidy quienes me brindaron su cariño y apoyo en las más difíciles situaciones y que gracias a sus consejos y oraciones hicieron posible que llegue hasta este punto importante en mi vida.

A mis primos Elian, Sebastián, Elizabeth y Madelein quienes estuvieron ahí para ayudarme en largas jornadas de estudio y gracias a eso me permitieron aumentar mis conocimientos y convertirme así en un buen profesional capaz de hacer frente a las adversidades.

A mi tío Eduardo quien durante sus últimos años de vida me lleno de tantos consejos y me dio las fuerzas necesarias para jamás darme por vencido, siempre lo llevare presente en mi mente y en mi corazón y sé que en cada paso que estará apoyándome incondicionalmente como solía hacerlo.

A mi tía Elena quien a través de su forma increíble de ser me dio la mano cada vez que lo necesite y que por medio de sus enseñanzas he logrado alcanzar cada uno de los objetivos que me he propuesto.

Finalmente, quiero dedicar esta tesis a todos mis amigos y amigas quienes me acompañaron hombro a hombro durante todo este proceso, por extenderme su mano en los momentos difíciles y por la comprensión, paciencia que me brindaron siempre los llevo en mi corazón.

Adrián Pérez

AGRADECIMIENTO

Agradezco a Dios por bendecirme la vida, por brindar la fortaleza, apoyo y salud necesarios para poder culminar mis estudios en tan prestigiosa universidad.

Agradezco a mis padres Nancy Chávez y Félix Pérez quienes, a través de su amor, consejos, paciencia me han inculcados los valores y principios para volverme no solo un buen profesional si no también un gran hombre, por haberse sacrificado tanto tiempo por mí por haberme brindado el apoyo desde el inicio de mis estudios hasta este momento y por creer en mí y haberme brindado la posibilidad de alcanzar mis sueños.

A toda mi familia quienes me acompañaron desde el principio brindándome su apoyo y me han sabido dar consejos los mismos que me han sido útiles para alcanzar todas mis metas.

A los docentes que conformaron toda mi carrera universitaria ya que gracias a sus enseñanzas y sus consejos sabios he podido crecer tanto profesionalmente como personalmente y siempre los llevaré conmigo en mi transitar profesional. Gracias por su paciencia por compartir sus conocimientos de manera invaluable y por toda la dedicación, perseverancia y tolerancia durante estos años.

A mis amigos y compañeros en toda esta travesía, no puedo dejar de recordar las innumerables ocasiones en que nos juntábamos a estudiar y las largas horas de trabajo que han permitido culminar nuestra carrera, a ustedes Jefferson, César, Israel, Jessenia y Katherine por brindarme su apoyo y compartir conmigo su conocimiento, experiencias y por todas las anécdotas que viví junto a ustedes. Gracias por siempre estar allí.

Finalmente, agradezco a mi tutor y jefe Fernando Becerra por haberme brindado sus consejos, así como haberme guiado en el desarrollo de este trabajo de titulación, gracias por creer en mí y por su confianza desde el inicio de mi formación profesional dentro de la Escuela Politécnica Nacional.

Adrián Pérez

DEDICATORIA

Este proyecto de titulación va dedicado a aquellas personas que nuca se han rendido conmigo, mis padres. A mi madre, Gloria Ramírez, que con su amor y paciencia a sabido guiarme y con sus sabias palabras y correcciones me ha educado de la mejor manera. A mi padre, Pedro Gualoto, que con su ejemplo a sabido inculcarme el amor en lo que hago y que con su compromiso y entrega en el trabajo me ha enseñado a nunca darse por vencido. A mi familia que siempre ha estado conmigo, apoyándome, corrigiéndome y acompañándome en aquellos días de estudio y noches sin dormir. A mis sobrinos Esteban Gualoto, Romina López, Dannae Diaz y Viviana Quilumba que han sido una fuente de amor y alegría para mí, y para que sepan que con perseverancia se puede llegar a cumplir los objetivos propuestos y aprendan a disfrutar de cada ocasión que se tiene. Y a mi abuelita María Andrea Álvaro que me ha llenado de amor y que con sus historias a llenado mi vida de felicidad, dándome ganas de superarme día a día.

A todas las personas que confiaron en mí, que conocí durante el trayecto de la carrera y en especial a Dios por darme las fuerzas y la sabiduría para seguir adelante.

Jefferson Gualoto

AGRADECIMIENTO

Al culminar mis estudios, quiero agradecer en a mis licenciados por la dedicación y la entrega a la hora de enseñar, a mis compañeros que han hecho de este proceso algo más llevadero y que han sabido presionarme y sacar lo mejor de mí, a la Escuela Politécnica Nacional por la oportunidad de poder estudiar esta bella carrera.

Agradezco a mis padres que siempre han creído en mí y me apoyan en todos mis planes, dejándome el compromiso de ser una mejor persona. Agradezco a mi hermana, Karla Gualoto, por ser mi confidente y mi soporte, ya vez lo logre, y a su familia que se ha robado mi corazón. Agradezco a mi hermano, Mauricio Gualoto, por sus charlas y alentarme a ser mejor y a su familia por el cariño que me tienen. A mi hermana Ruth Gualoto que siempre ha estado dándome su apoyo y ha sabido soportar mis malos días. A la familia de Viviana Quilumba por apreciarme y acompañarme durante esta etapa. Mi más grande agradecimiento a mi abuelita por estar siempre conmigo, por preocuparse por mí, y por qué siempre ha sabido darme su bendición. A mi gran familia que me tiene aprecio. Y a mis sobrinos que son mi motor y mi alegría.

Un agradecimiento a todos los ingenieros que me supieron ayudar, apoyar y orientar, con las dudas que surgieron al momento de realizar este proyecto de titulación, además lograron proveerme de los recursos necesarios para el mismo. Al ing. Fernando Becerra tutor de este proyecto de grado, por proponer retos en la carrera, con los cuales pudimos adquirir nuevos conocimientos.

A Dios por la vida y la salud, a mis amigos por su amistad y a todos lo que confiaron en mí.

Jefferson Gualoto

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación SIMULACIÓN DE UNA RED SD-WAN MEDIANTE EQUIPOS DE NETWORKING EN GNS3 busca comprender la red Software-Defined Wide Area Network (SD-WAN) que se ha empezado a utilizar en el área de las comunicaciones. SD-WAN se utiliza para disminuir los tiempos de transmisión y el costo de redes dedicadas. Estos tipos de redes han comenzado con su despliegue a nivel global. Por ello es indispensable conocer de qué trata, sus elementos y su configuración.

En la sección uno se realizó una breve investigación sobre el funcionamiento de las redes SDWAN, así como los desafíos que implican las mismas a las tecnologías de la información.

En la sección dos se analizó la metodología usada para este proyecto la cual es la metodología cuantitativa la misma que estará basada en la observación del funcionamiento de la red.

En sección tres se han implementado cuatro redes SD-WAN utilizando diferentes proveedores de equipos. Por un lado, se tiene una red SD-WAN Cisco-Viptela de Cisco que cuenta con 4 equipos: vManage, vBond, vSmart y vEdge de la versión 19.2.4. Por otro lado, se tiene tres redes SD-WAN con equipos Fortinet donde utilizaremos equipos FortiGate de la versión 5.6.

En la sección cuatro se definen conclusiones y recomendaciones en base a los resultados obtenidos de las pruebas de funcionamiento y de las investigaciones realizadas previamente.

En la sección cinco se detallarán todas las fuentes que sirvieron de apoyo para las investigaciones de este proyecto.

PALABRAS CLAVE: *vMmanage, vBond, vEdge, vSmart, SDWAN, Fortigate*

ABSTRACT

The present degree project SIMULATION OF AN SD-WAN NETWORK THROUGH GNS3 NETWORKING EQUIPMENT seeks to understand the Software-Defined Wide Area Network (SD-WAN) that has begun to be used in the communications area. SD-WAN is used to decrease transmission times and the cost of dedicated networks. These types of networks have begun to be deployed globally. Therefore, it is essential to know what it is about, its elements and its configuration.

In section one, a brief investigation was carried out on the operation of SDWAN networks, as well as the challenges that they imply for information technologies.

In section two, the methodology used for this project was analyzed, which is the same quantitative methodology that will be based on observing the operation of the network.

In section three four SD-WAN networks have been implemented using different equipment vendors. On the one hand, there is a Cisco Cisco-Viptela SD-WAN network that has 4 computers: vManage, vBond, vSmart and vEdge from version 19.2.4. On the other hand, there are three SD-WAN networks with Fortinet equipment where we will use FortiGate equipment of version 5.6.

In section four conclusions and recommendations are defined based on the results obtained from the performance tests and the investigations previously carried out.

In section five all the sources that supported the research of this project will be detailed.

KEYWORDS: *vMmanage, vBond, vEdge, vSmart, SDWAN, Fortigate*

1 INTRODUCCIÓN

Con el avance de las tecnologías de redes, la información y los servicios que están disponibles actualmente en las múltiples nubes, la experiencia para los usuarios se vuelve un verdadero desafío para los departamentos de *networking*. El principal problema es que las redes actuales basadas en WAN no están listas para un inminente aumento en el tráfico de los datos que manejan las distintas nubes.

La red SD-WAN brinda una experiencia distinta al cliente debido a que la forma de conexión con los servicios ya no se dará de forma alámbrica, esta nueva experiencia la hace mediante virtualización y conexión directamente con la nube brindando una mayor seguridad debido a la utilización de túneles creados desde el proveedor de servicios hasta el *gateway* del cliente [1].

Este aumento de tráfico se traduce en una mayor complejidad en la gestión de la información, así como aumentos de latencia y una mayor dificultad en el momento del monitoreo de la red para la gestión de los datos que están viajando. SD-WAN aborda los desafíos que están pasando los departamentos de redes mejorando la conectividad y reduciendo de manera significativa los costos operativos para gestión y monitoreo de la red. Esto se traduce en usar el ancho de banda disponible de forma eficiente y garantizar la disponibilidad para los usuarios sin sacrificar la privacidad de los datos, mitigando así todo tipo de vulnerabilidades que se puedan presentar dentro de una red [2].

1.1 Objetivo general

Simular una red SD-WAN mediante equipos de networking en GNS3.

1.2 Objetivos específicos

- Investigar sobre la tecnología SD-WAN.
- Configurar el equipo de simulación para que soporte SD-WAN.
- Configurar una red en base a SD-WAN.
- Realizar pruebas sobre la red virtualizada SD-WAN en GNS3.

1.3 Fundamentos

Toda esta sección se encuentra detallada en la sección 3.1.

2 METODOLOGÍA

2.1 Descripción de la metodología usada

La metodología que se va a implementó en el presente proyecto de titulación se basa en 2 tipos de metodologías de investigación. La metodología cuantitativa la misma que se utilizó en la observación del comportamiento de la red SD-WAN con el uso de los equipos proporcionados por Cisco-Viptela como lo son *vEdge, vSmart, vManage* y paralelamente recolectando datos de forma estadística. Datos que fueron proporcionados por el vManage y el equipo central Fortigate en tiempo real junto con el monitoreo de la red a tiempo real para analizarlos posteriormente.

Una segunda metodología usada es la exploratoria la cual se utilizó para hacer un estudio del problema para poder de ese modo comprenderlo de mejor manera y poder de este modo encontrar soluciones que permitan optimizar y mejorar el rendimiento de la red SD-WAN. Para poder reconocer los diferentes problemas que se pueden encontrar se hizo uso del protocolo OSPF y del establecimiento de las políticas necesarias en los distintos niveles que se requieran para que con ayuda de vManage.

De este modo tener un mejor panorama del comportamiento de las redes de área extendida y como SD-WAN mejoraría las mismas por medio de la aplicación de una topología adecuada para que de ese modo exista una alta disponibilidad y eficiencia logrando así mejorar la experiencia del usuario y reduciendo latencias en la transmisión de datos.

3 RESULTADOS Y DISCUSIÓN

Las redes definidas por *software* abren posibilidades para la administración de las redes dentro de una organización reduciendo costes y optimizando el tiempo que le toma al administrador monitorear la red y tomar decisiones en tiempo real. Para la simulación de los equipos se deben considerar algunos de los requisitos mínimos que se especificarán dentro de esta sección, así como los pasos necesarios para poder realizar una simulación de una red SD-WAN mediante equipos de *networking.*

Para llevar un control de cómo se están estableciendo las topologías se han elaborado tablas en las cuales se detalla el direccionamiento de los equipos, así como los *gateways* que permitirán la salida hacia distintas redes o hacia internet.

3.1 Investigar sobre la tecnología SD-WAN.

SD-WAN o también conocidas como redes definidas por *software* fueron diseñadas para simplificar las diferentes redes en las sucursales y adicionalmente para optimizar el rendimiento de las aplicaciones existentes dentro de la Internet y las redes WAN comunes. Estas redes se manejan por *software* lo que comúnmente se conoce como redes SDN, esto quiere decir que los servicios que se ofertan por *software* no están directamente vinculados al *hardware* de los equipos prestadores de dichos servicios [3].

Por otro lado, la conmutación de etiquetas multiprotocolo es un estándar que está orientado a unir los diferentes tipos de datos que se transmiten a través de la misma red con el fin de que los paquetes de información no generen latencias en la velocidad de transmisión. Debe quedar claro que *Multiprotocol Label Switching* (MPLS) no es un servicio como tal sino es una técnica para la transmisión de información, sin embargo, no es una técnica muy usada dentro de los *Internet Service Provider* (ISP) puesto que posee costos elevados [4].

Las diferentes ventajas que presentan las redes SD-WAN son variadas, entre las más relevantes se tiene que se reducen significativamente los costos de transferencia de información con MPLS para las tecnologías 4G y 5G, así como en diferentes tipos de conexión. Adicionalmente esta tecnología mejora el rendimiento de las redes gracias a su manejo eficaz en el transporte de la información aumentando de este modo la agilidad con la que viaja la información, adicionalmente optimiza la experiencia del usuario para los distintos *softwares* que ofrecen servicios en la nube pública simplificando de este modo las operaciones que se llevan a cabo en la misma [5].

La arquitectura con la que cuentan las redes WAN hoy en día es direccionada solamente a empresas, sucursales y los centros de datos. Cuando una empresa usa las aplicaciones que están disponibles en la nube como *Software As A Service* (SAAS) las redes WAN sufren un excedente de tráfico lo que causa severos problemas en el rendimiento de las redes causando que existan elevados costos de mantenimiento ya que se necesitan canales dedicados y de respaldo. Uno de los principales inconvenientes es poder conectar múltiples usuarios a varios tipos de dispositivos que se encuentran en diferentes entornos de la nube [6].

SD-WAN entre sus servicios ofrece enrutamiento entre los equipos, protección de cualquier tipo de amenazas, descargas mucho más eficientes de los canales dedicados y una administración mucho más eficiente de la red WAN. Causando una alta disponibilidad para todas las aplicaciones empresariales, adicionalmente se dispone de tráfico enrutado dinámicamente esto es posible por el enrutamiento basado en aplicaciones. OpEX o también conocido como gasto operacional, que remplaza a todos los servicios de conmutación que se prestaban anteriormente con MPLS además de una banda ancha mucho más económica y flexible esto incluye a conexiones mediante VPN seguras. Por otra parte, se brinda mucha más seguridad cifrando la información de extremo a extremo con control de acceso en tiempo real para el usuario, adicionalmente se dispone de la posibilidad de distribuir la seguridad a las sucursales de la organización por medio de *Next Generation FireWalls* (NGFW), *Next Generation AntiVirus* (NGAV) y seguridad por medio de DNS [7].

Una de las principales características que poseen las redes SD-WAN es llevar los servicios de las redes WAN a varias nubes públicas, así como una gestión mucho más simplificada contando con un panel de administración único que opera de manera centralizada. Con el añadido de poder contar con informes periódicos detallados sobre el rendimiento de las aplicaciones y la red WAN, así como llevar un control sobre el ancho de banda que se está utilizando [7].

SD-WAN surgió como una evolución o respuesta a la tecnología MPLS, si se observa de manera más objetiva puede parecer que SD-WAN realiza las mismas acciones que MPLS. Sin embargo, se aplica a escenarios más amplios brindando conectividad de forma segura y privada que se envía de forma independiente y además es compatible con la nube, por otra parte, MPLS se maneja con respaldos independientes y SD-WAN unifica la red troncal que maneja WAN [7].

Una de las tecnologías utilizadas para la creación de redes SD-WAN es conocida como Cisco-Viptela, la cual maneja como base independizarse completamente del medio físico de forma automática y de manera segura obteniendo de este modo una visibilidad en tiempo real de todos los cambios que van ocurriendo dentro de la red. Esto con el fin de optimizar las decisiones que afecten en este entorno de forma mucho más rápida y eficaz, es decir, si se tiene una organización que maneja la tecnología de acceso MPLS y posee adicionalmente otro acceso a Internet, Cisco-Viptela automáticamente encaminará todo el tráfico de la red a un acceso o al otro en función de las latencias que se presenten en ese momento. De este modo Cisco-Viptela es capaz de brindar una arquitectura WAN desde un servicio en la nube, esto reduce de forma muy significativa todos los costes y tiempos al momento de desplegar la red proporcionando adicionalmente una arquitectura de seguridad mucho más robusta [8].

Cisco-Viptela cuenta con cuatro componentes cada uno de ellos está orientado a cuatro campos diferentes. *vEdge* que está orientado al plano de datos es en esencia el router que se encuentra en las oficinas, es decir, posee la capacidad de conectarse de forma segura con el resto de componentes de la red y una de sus funciones principales es establecer sesiones IPSec con el resto de *vEdge* en la red WAN. De este modo dar como resultado topologías completamente malladas, parcialmente malladas, punto a punto y *hub&spoke*, esta última topología es usada para una VPN de datos mientras que una topología completamente mallada es usada comúnmente para una VPN de voz. Esto hace posible tener una segmentación segura de todo el tráfico en una misma infraestructura física [8].

vSmart por otra parte, establece todas las conexiones *Secure Sockets Layer* (SSL), las cuales cifran el tráfico que circula entre un navegador web con un sitio web o simplemente entre dos servidores protegiendo la conexión, con el resto de componentes dentro de la red SD-WAN de Cisco-Viptela usando el protocolo *Overlay Management Protocol* (OMP). El cual va a determinar todas las políticas relacionadas con el encaminamiento de la información, así como de la seguridad y control de todos los accesos que se encuentren definidos de forma centralizada. Para poder comprender mejor como funciona este dispositivo se puede decir que es el equivalente a un *route reflector* de *Border Gateway Protocol* (BGP) haciendo posible que exista más de un dispositivo *vSmart* dentro de la red de la organización [8].

Un *route reflector* es un equipo que está configurado para enviar actualizaciones a sus vecinos a través del mismo sistema autónomo, es decir modifica la regla de horizonte dividido que se encuentra actualmente en BGP. Sin embargo, este equipo necesita un

emparejamiento completo con los clientes que maneje, aunque entre vecinos no es necesario, esto con el fin de formar un *cluster* [8].

El protocolo OMP es quien establece y mantiene el plano de control en una red SD-WAN proporcionando servicios como la conectividad entre toda la red, distribución de rutas de enrutamiento a nivel de servicio, así como la distribución de los diferentes parámetros de seguridad. Adicionalmente el control y distribución de las políticas de enrutamiento, es decir controla el flujo de tráfico entre los dispositivos *vSmart y vEdge*, algunas de las características principales que posee este protocolo son las siguientes [8]:

- Está basado en el protocolo *Transmission Control Protocol* (TCP).
- Funciona para mallas completas.
- Realiza la segmentación de *Virtual Private Network* (VPN).
- Brinda accesibilidad, seguridad.
- Proporciona rutas de servicio.
- Establece políticas de ruta de datos en toda la red.

vManage funciona por medio de un tablero centralizado el cual permite una correcta configuración, gestión y monitoreo de toda la red SD-WAN creada por medio de Cisco-Viptela. Esto quiere decir que permitirá monitorear toda la red en tiempo real y tomar las decisiones más acertadas posibles con respecto al encaminamiento y para que el transporte de información cambie de un medio a otro. Cabe resaltar que este dispositivo es el más importante dentro de la red sin embargo depende de los demás dispositivos para mostrar toda la información posible, es decir va a depender de los equipos *vEdge* para poder mostrar los resultados a nivel de aplicación [9].

vBond es un dispositivo encargado de realizar el despliegue inicial de la red realizando las acciones de autenticación y autorización de todos los elementos dentro de la red. Esto es de vital importancia puesto que proporciona la información sobre el cómo cada uno de los componentes deben conectarse entre sí [9].

El funcionamiento de Cisco-Viptela usa como base la formación de VPN junto con *Internet Protocol Security* (IPSec) entre los diferentes equipos *vEdge* en la red para el monitoreo del tráfico de la información y de igual manera poder establecer túneles por medio de *vSmart* para gestionar todo el tráfico que se encuentre en el plano de control. Conjunto con *vManage* se crearán las políticas para el comportamiento de los equipos dentro de la red y a su vez el equipo que implementará las políticas sobre *vEdge* será *vSmart* haciendo uso del protocolo OMP.

En la Figura 3.1 se explica cómo es el establecimiento de las rutas de servicio, así como la comunicación entre los dispositivos *vSmart* y *vEdge*. Una vez establecido el emparejamiento, se proceden a aplicar las diferentes políticas de enrutamiento de la información, políticas que son administradas por medio del dispositivo *vManage* [9].

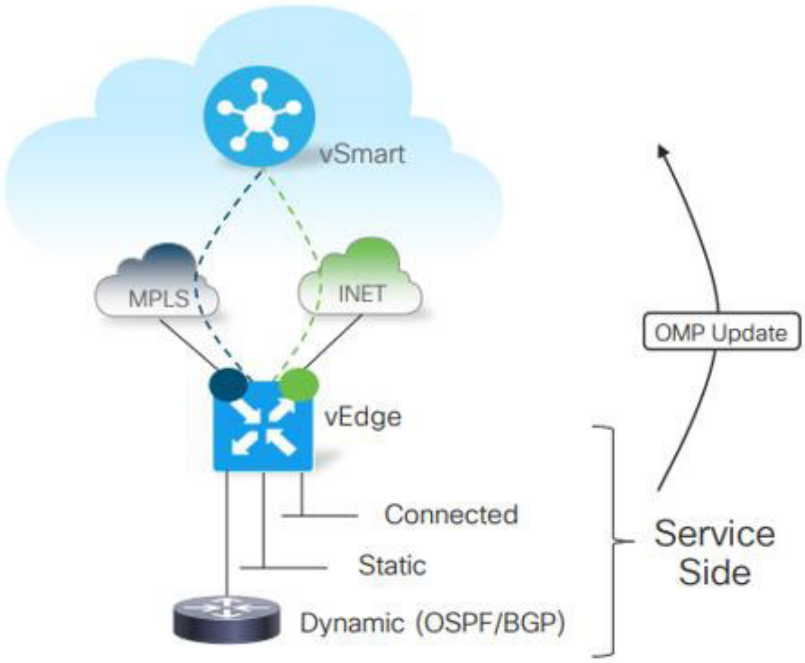


Figura 3.1 Rutas de servicio protocolo OMP *[10]*.

Estas políticas están compuestas por 3 bloques importantes donde el primero de ellos es la elaboración de listas para seleccionar el tráfico sobre el cual se aplicarán las políticas. El segundo bloque hace referencia a la acción que se tomará sobre dicho tráfico seleccionado y finalmente, mediante directivas se establecen los diferentes sitios sobre los cuales se deben aplicar las políticas [10].

Actualmente existen dos tipos de políticas principales, las centralizadas, las cuales funcionan en base a la independización del medio físico es decir afecta a varios de los sitios sino a todos los sitios de la empresa. Por otra parte, las localizadas las cuales afectan únicamente a un solo sitio de la organización. Estas últimas políticas son ejecutadas por el *vEdge* que se encuentra en el sitio de donde se quiere implementar la política [10].

En cuanto las políticas centralizadas existen actualmente 3 tipos:

- Las políticas de control, las cuales se van a ejecutar en el *vSmart* definen el encaminamiento de toda la red o bien de un número específico de sitios [10].

- Las políticas de datos las cuales van a ser configuradas desde el *vManage* y se transmiten por medio de los dispositivos *vEdge* y *vSmart* [10].
- Las políticas de enrutamiento consistente de la aplicación se manejan junto a los acuerdos de nivel de servicio o SLA. Los cuales proporcionan las características de rendimiento base de todos los servicios es decir características como latencias, pérdidas de paquetes y fluctuaciones del servicio, estas políticas serán aplicadas en los dispositivos *vEdge* [10].

Adicionalmente Cisco-Viptela proporciona múltiples ventajas para las redes SD-WAN algunas de ellas son:

- Independizarse completamente de la capa de transporte, es decir con Cisco-Viptela es posible trabajar sobre diferentes medios físicos lo que significa un aumento en la disponibilidad [10].
- Disponer de seguridad en las comunicaciones [10].
- Posibilidad de segmentación para construir diferentes topologías [10].
- Gestión centralizada, esta es sin duda la mayor ventaja que ofrece Cisco-Viptela sobre una red SD-WAN ya que permite el monitoreo constante de toda la red lo que se traduce en un gran ahorro en tiempo y costes en comparación con las redes MPLS [10].

Entre los diferentes niveles de *software* que se dispone para las redes SD-WAN se tienen 3 niveles. El primero conocido como *Cisco DNA Essentials* provee de una administración, así como enrutamiento hasta 50 dispositivos en la red, optimizando de este modo la conectividad en la nube. El segundo nivel conocido como *Cisco DNA Advantage* provee de segmentación ilimitada para las redes, así como análisis en tiempo real. Finalmente, el tercer nivel conocido como *Cisco DNA Premier* permite una funcionalidad segura en la nube a nivel empresarial, esto quiere decir que provee una puerta de enlace segura para la internet [11].

Los precios con los que se manejan las redes SD-WAN establecidas por Cisco se encuentran especificadas en la Tabla 3.1.

Tabla 3.1 Listado De Precios Red SD-WAN *[12]*.

PRODUCTO	DESCRIPCIÓN	PRECIO
NED-CISCO-VIPTELA-VMNG-P	NSO NED Cisco-Viptela vManage: 1 Active Prod Net Srv Perpetual	$40,000.00
NED-CISCO-VMGE-PS	NSO NED Cisco Cisco-Viptela vManage:1 Active Prod Netw Svr-PS	$24,156.00
NED-CISCO-VMGE-SIA	NSO NED Cisco Cisco-Viptela vManage:1 Active Prod Netw Svr -SIA	$24,156.00
NED-CISCO-VMGE-P	NSO NED Cisco Cisco-Viptela vManage:1 Active Prod Netw Svr-Perp	$40,000.00

Fortinet es una empresa estadounidense que se encarga de crear equipos para la seguridad de las redes. Fortinet gestiona las amenazas de la red por medio de *firewalls*, VPN, filtrado web, detección de intrusos, entre otras funciones para asegurar las redes. Dado su enfoque en seguridad y costo es utilizado en todo tipo de empresas [13].

FortiGate es un equipo de la marca Fortinet con funcionalidades hacia la seguridad de las redes. Estos equipos se consideran como equipos todo en uno ya que es adaptable a sus entornos, y tienen grandes capacidades y rendimientos. Estos equipos pueden ser físicos, así como virtuales y se pueden utilizar en diferentes plataformas virtuales. Gracias a su sistema de Circuitos Integrados de Aplicación Específica (ASIC) permite realizar los análisis de seguridad sin afectar los procesos de comunicaciones. Se maneja por un sistema operativo propio de Fortinet llamado FortiOS, que utiliza un *kernel* dedicado para trabajar en tiempo real y procesamiento de paquetes, permitiendo utilizar un mismo sistema operativo en todos sus equipos [14].

Dado que la empresa Fortinet tiene su enfoque en seguridad en esta versión se implementaron funciones de seguridad como la de *Security Fabric Audit,* para el análisis de vulnerabilidades, entre otras. Lo que respecta a red se implementó mejoras para el enrutamiento, nateo, conmutación, WI-FI WAN, y la más llamativa SD-WAN permitiendo poder tener la tecnología SD-WAN dentro de los dispositivos FortiGate. Con ello Fortinet logra tener administración simple y centralizar la red [15].

Dentro de la solución de *Huawei* encontramos 3 elementos principales:

iMaster NCE-WAN: este equipo se encarga del monitoreo, control, funciones y administración de la red. A este equipo le llegaran todas las solicitudes y este equipo se encargará de procesarlas. Sus funciones son *plug-and-play* por lo cual basta con conectarlo para que funcione además de que puede funcionar para múltiples redes [16].

RR: Es un equipo que se encarga del control del *Client's Local Team* (CPE). Este equipo se encarga de la distribución de las rutas a los CPE, además realiza los túneles entre los CPE [16].

CPE: es el equipo de borde, se utilizan los equipos *NetEngine AR* que es un modelo de equipo de la marca *Huawei*, dichos equipos son de siguiente generación [16].

Esta solución crea una interconexión entre las diferentes redes que se tienen creadas y la nube, para ello se realizan túneles. Existen 3 tipos de escenarios para la utilización de la red SD-WAN. El primer escenario es el sitio a sitio, el segundo sitio a internet y el tercero sitio a sitio heredado [16].

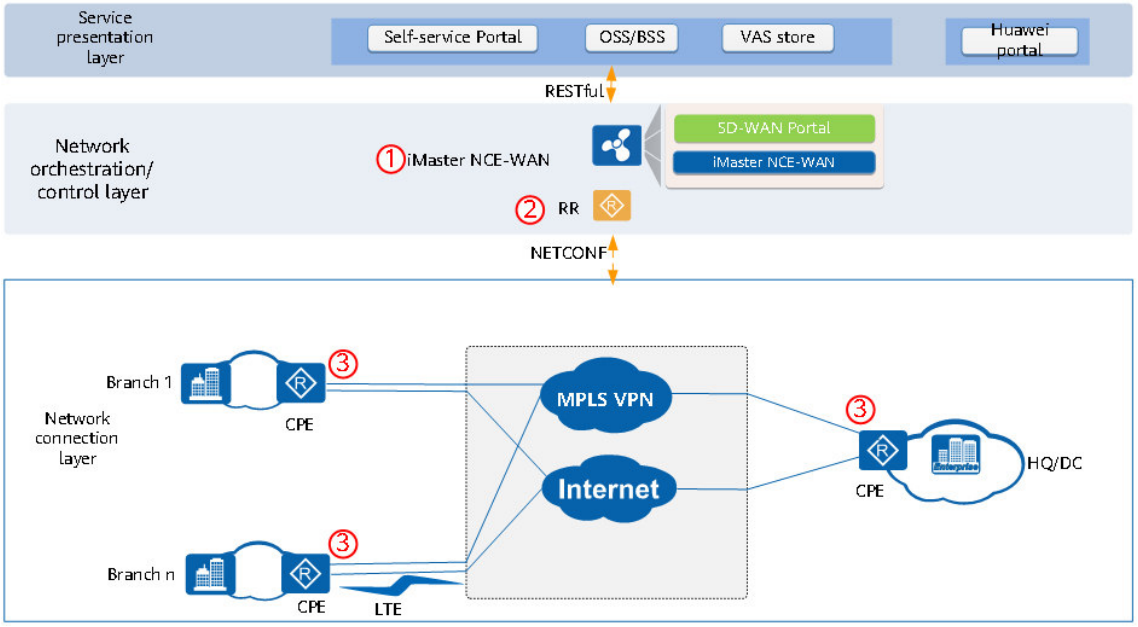


Figura 3.2 Solución SD-WAN Huawei *[16].*

Juniper tiene una solución SD-WAN *Session Smart,* esta solución es centralizada y busca mejorar los errores heredados de las primeras SD-WAN, se basa en la nube al igual que las otras redes SD-WAN en la cual el fin es conectar a los usuarios con los servicios, pero además se preocupa de mejorar. Utiliza *Artificial Intelligence* (IA) para dar servicios de QoS además de elegir la ruta adecuada entre *Multiprotocol Label Switching* (MPLS), 4G e Internet y proporciona balanceo de carga [17].

Lo más llamativo de la solución de Juniper es su arquitectura sin túneles que es remplazada con *Secure Vector Routing* (SVR) que reduce la carga en un 30% en comparación con el protocolo Ipsec [17].

Los *Smart Service Router* (SSR) son colocados como equipos de borde proporcionando conocer el estado de la red, los datos que proporciona el SSR son evaluados por Marvis, un asistente para la Wan que utiliza IA, que identifica los problemas y proporciona un resumen de los fallos y permite corregirlos [17].

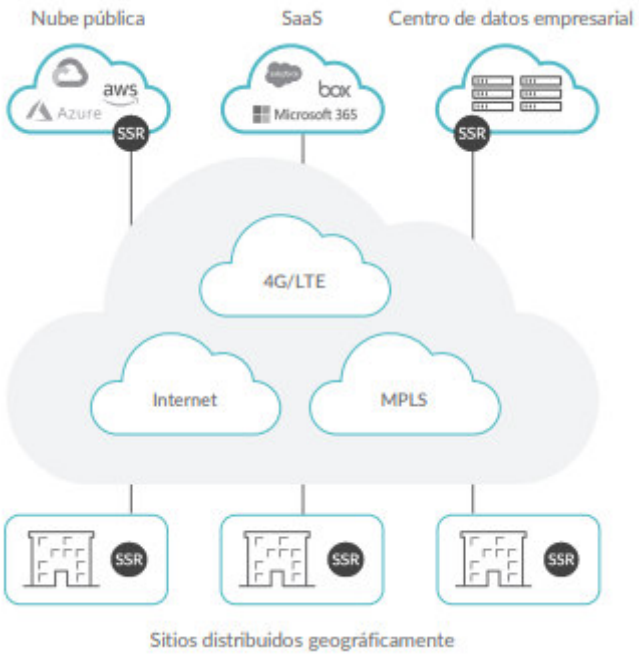


Figura 3.3 Solución SD-WAN Juniper *[17]*.

3.2 Configuración del equipo de simulación para que soporte SD-WAN

Para poder realizar una correcta simulación de una red SD-WAN usando equipos propietarios de Cisco como lo es Cisco-Viptela se deben contar con algunos de los requisitos mínimos dentro del equipo en el cual se va a realizar la simulación. Algunos de estos requisitos son:

- Contar con procesador Intel Core i7 o superior, puede contar con un procesador Ryzen 5 1600 o superior.
- Memoria RAM de al menos 120 (Gb) para una ejecución fluida de los equipos de Cisco-Viptela. Sin embargo, para que los equipos simplemente se ejecuten con cierta latencia (mayor a 20 (min) en vManage) es necesario solamente 64 (Gb).

- Almacenamiento interno debe ser de disco de estado sólido de al menos 2 (Tb) de capacidad, para que la ejecución sea fluida en los equipos se recomienda que sea mayor a 4 (Tb) de capacidad.
- El equipo debe contar con la virtualización asistida por *hardware* activa, así como los servicios de virtualización Hyper-V de Windows desactivados. Si la ejecución se realiza en un sistema operativo propietario de Linux la virtualización puede ser activada desde el BIOS del ordenador.

Para la realización de la simulación se contó con un servidor perteneciente a la Escuela Politécnica Nacional el cual cuenta con un CPU con una capacidad de procesamiento equivalente a 52.8 (GHz) y posee una memoria RAM de 127.91 (Gb), así como un almacenamiento interno de disco de estado sólido disponible de 923.5 (Gb). Este servidor tiene una interfaz gráfica proporcionada por *VMware* denominada ESXI y la versión de este sistema que se está utilizando es la 6.0 la cual permite usar a las máquinas virtuales que se creen hasta 2 CPUs virtualizados. Estas especificaciones se pueden observar en la Figura 3.4.

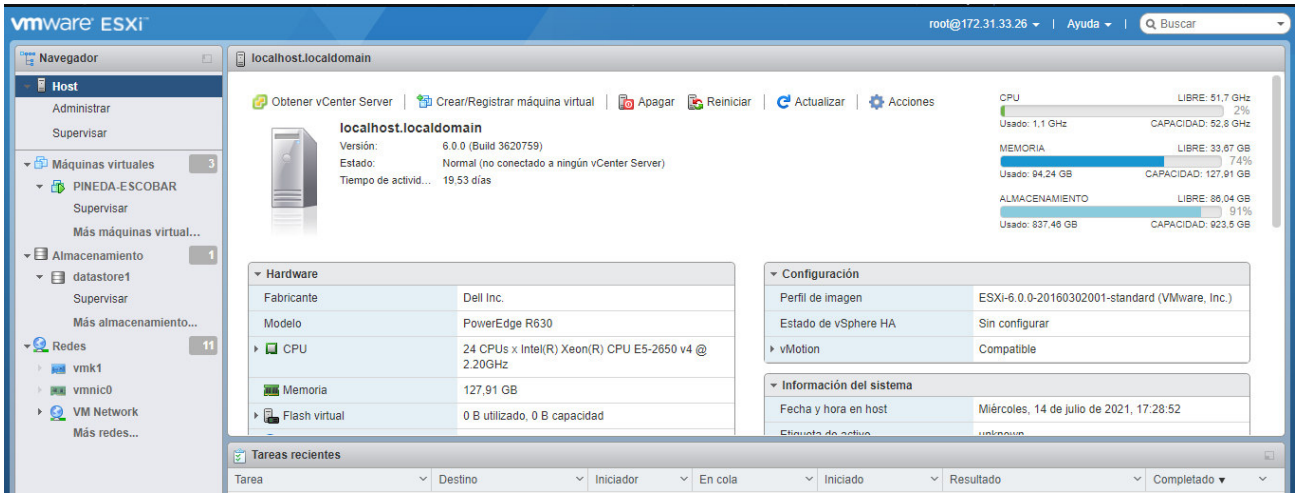


Figura 3.4 Especificaciones técnicas del servidor

Dentro de este servidor se creó una máquina virtual con el fin de instalar el sistema operativo Windows 10 dentro del cual se ejecutaría la simulación de la red SD-WAN. Para ello las características con las que contó esta máquina virtual fueron las siguientes:

- 8 CPUs virtualizados, sin embargo, el sistema ESXI 6.0 solo permite el uso de un máximo de 2 CPUs virtualizados.
- Una memoria RAM de 68.36 (Gb) para una ejecución óptima de los equipos de Cisco-Viptela.
- Dos discos de almacenamiento interno con 220 y 250 (Gb) respectivamente.

- Una red virtual conectada a la red física dentro de la Escuela Politécnica Nacional.
- Una tarjeta de video de 4 (Mb).

Estas características dentro del servidor se pueden apreciar en la Figura 3.5.

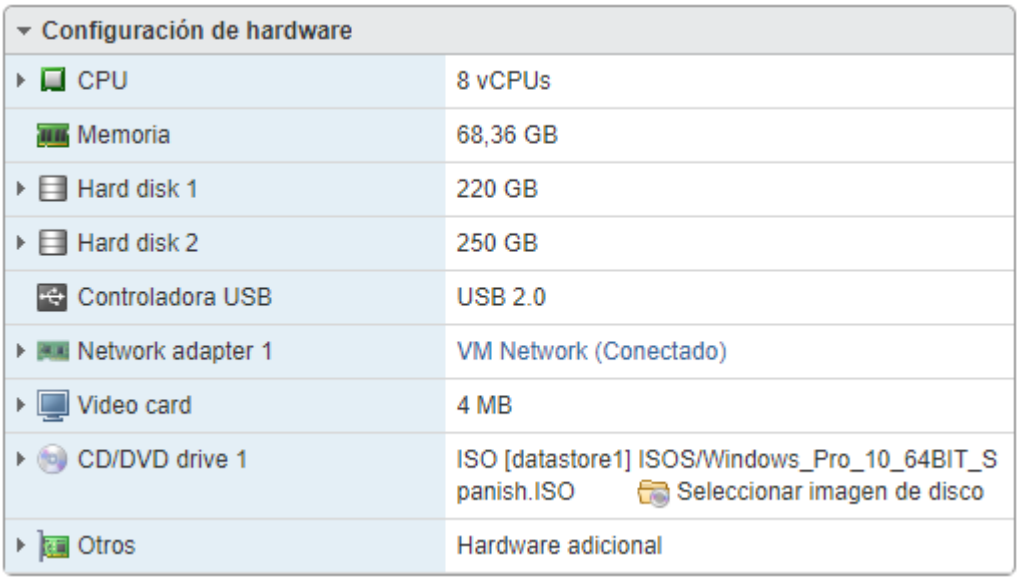


Figura 3.5 Especificaciones técnicas de la máquina virtual

Una vez creada la máquina virtual se procede a la instalación del sistema operativo Windows 10 Pro, por medio de una ISO presente ya en el servidor y configurando a la máquina virtual para que lea el disco desde el arranque instalando así el sistema operativo. Como se observa a continuación en la Figura 3.6.

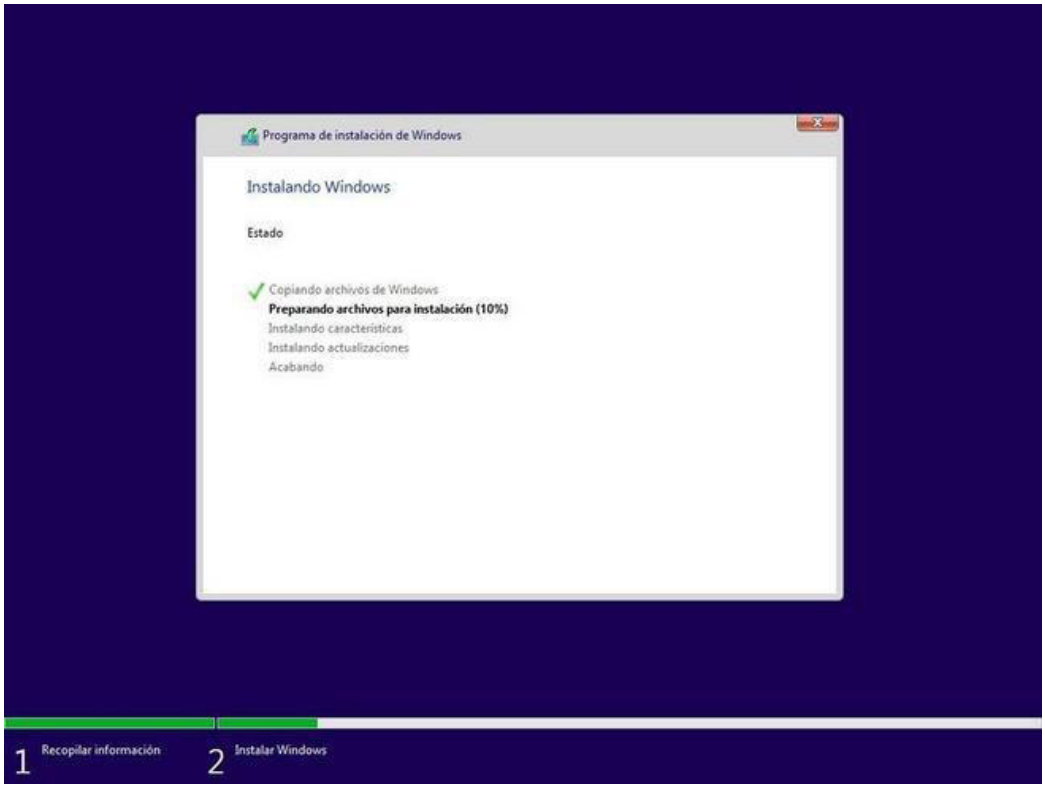


Figura 3.6 Instalación de Windows 10 Pro en máquina Virtual

Una vez finalizada la instalación de la máquina virtual se procede a darle una conexión a Internet a dicha máquina. Para lograrlo se debe conocer que la dirección IP del *gateway* a la cual está conectado el servidor es la 172.31.33.28 por lo que para colocarle una nueva dirección estática al equipo se debe acceder al centro de recursos compartidos y acceder a la configuración de la red para cambiar el parámetro protocolo de Internet IPv4. Como se muestra en la Figura 3.7 a continuación.

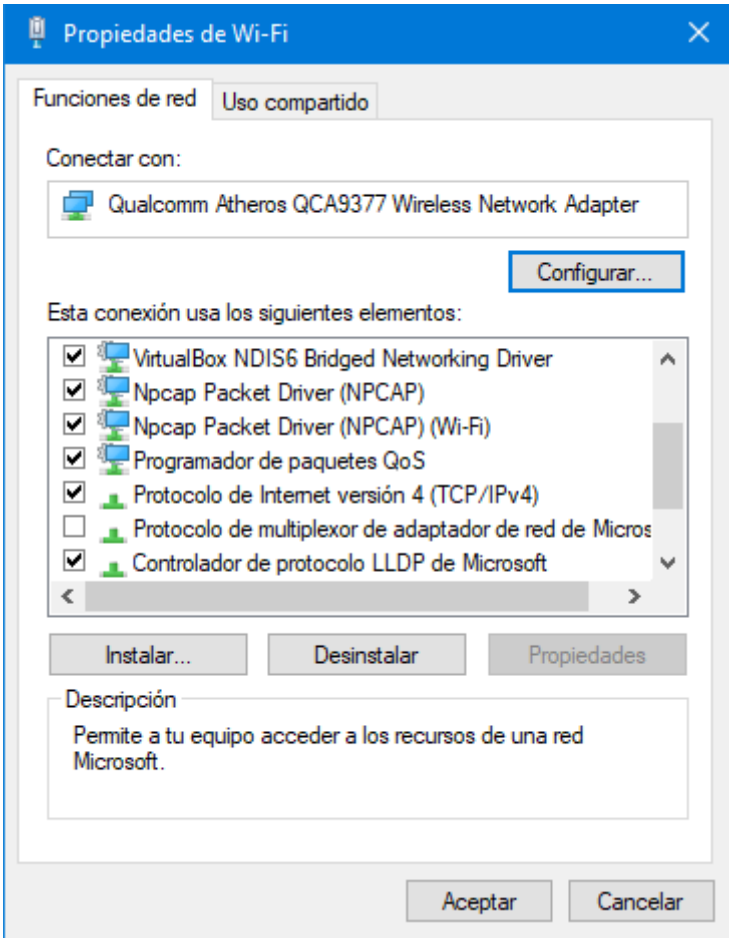


Figura 3.7 Propiedades de Red

Dentro de esta opción se seleccionan la opción estática donde se cambian los siguientes parámetros:

- Dirección IP: 172.31.33.34
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada: 172.31.33.1
- Servidor DNS preferido: 8.8.8.8
- Servidor DNS alternativo: 172.31.4.2

Una vez realizados esos cambios se verifica que exista conexión a Internet realizando un PING hacia la página de *Google* como se muestra en la Figura 3.8 a continuación.

Figura 3.8 Comprobación de conexión a Internet

Una vez establecida la conexión a internet se procedió a descargar los diferentes programas que se utilizarán en la simulación de una red SD-WAN. Algunos de estos programas son los siguientes:

- *Any Desk* programa que funciona como control remoto de la PC.
- GNS3 programa que funciona para la simulación de redes complejas.
- *VMware* programa que funciona para realizar máquinas virtuales. Así como para ejecutar servidores con las imágenes de los equipos de Cisco-Viptela.
- *Camtasia Studio 8* programa que permite grabar todos los avances del proyecto.
- *UltraISO Premium* programa que permite compactar un archivo ZIP en una imagen ISO.
- *WireShark* programa que permite realizar un testeo adecuado de la red para poder lograr conectividad con los diferentes equipos de la topología.

Con la descarga de GNS3 se procede a instalarlo con las configuraciones especiales para que las imágenes de los equipos las ejecute desde un servidor externo que estará en VMware y no desde la propia máquina. Esto se realiza con el fin de optimizar tanto la memoria RAM como el almacenamiento en disco para el uso de equipos robustos dentro de la red, esta selección se puede apreciar en la Figura 3.9 a continuación.

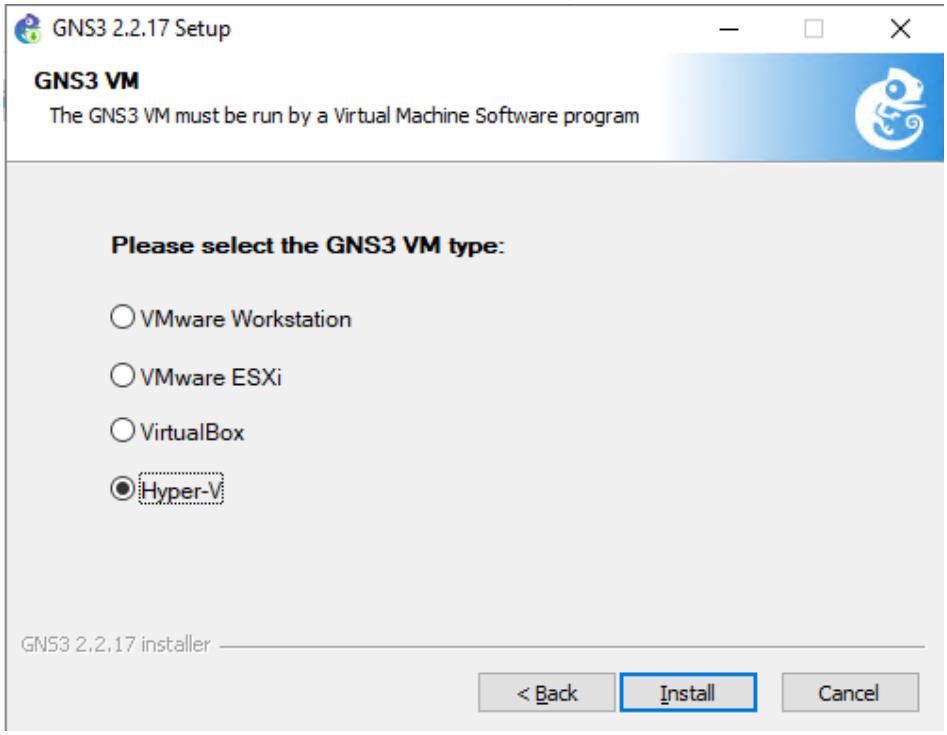


Figura 3.9 Instalación de GNS3

Una vez instalado el GNS3 con la posibilidad que ejecute las imágenes desde un servidor externo se procede a instalar VMware y posteriormente se procede a activarlo con la clave de activación proporcionada por la empresa misma. Una vez que se ha activado el producto se tiene acceso a todas las herramientas disponibles en *VMware* como se aprecia en la Figura 3.10 a continuación.

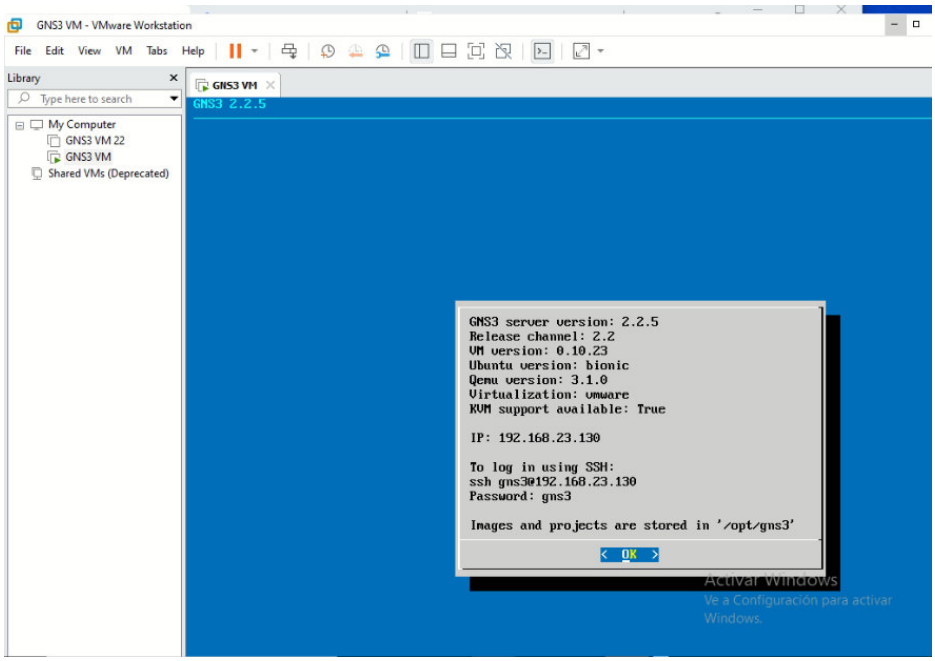


Figura 3.10 VMware activado

Una vez instalado y activado *VMware*, se debe descargar la máquina virtual de GNS3 ésta a su vez actuará como un servidor desde el cual se ejecutarán todas las imágenes necesarias para formar una red SD-WAN. Esta máquina virtual se la conoce como “ova” y se encuentra disponible para descargar desde la propia página de GNS3, la máquina virtual debe almacenarse en el disco que posea mayor cantidad de almacenamiento disponible esto con el fin de evitar latencias en la ejecución de los equipos. Como se muestra en la Figura 3.11 a continuación.

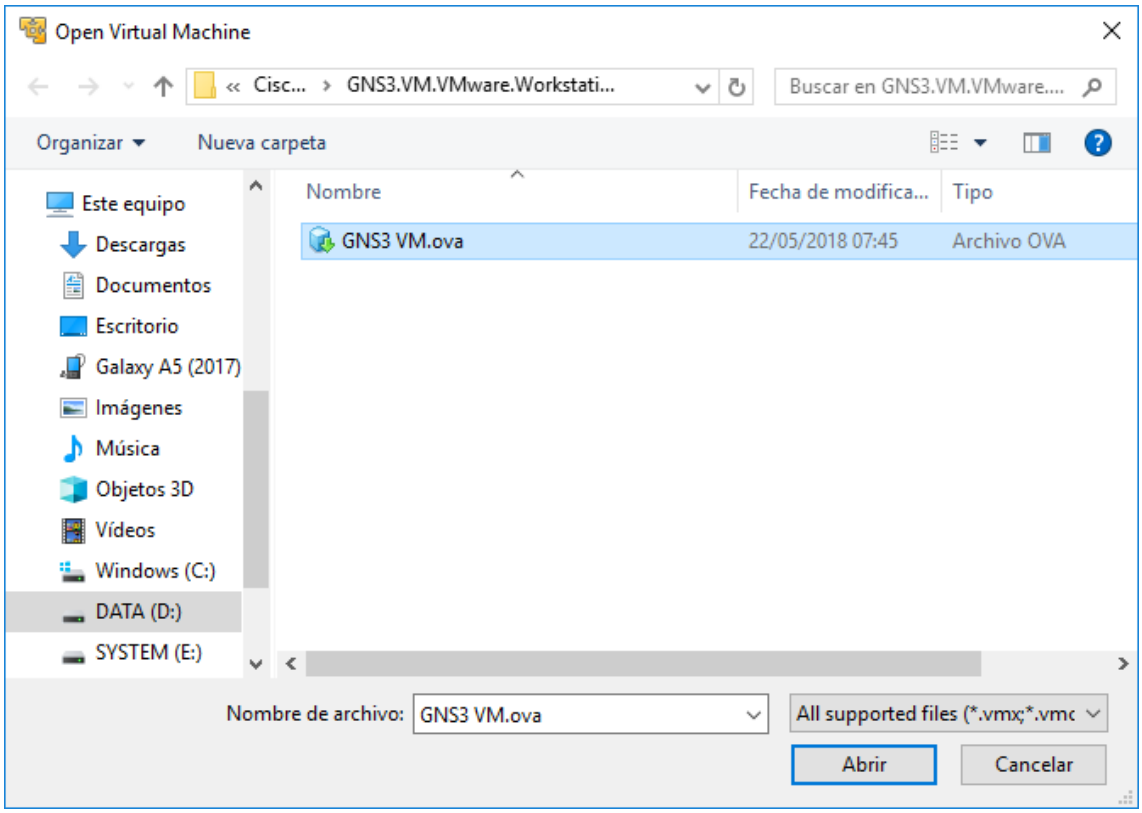


Figura 3.11 Descarga de “ova” de GNS3

Una vez instalada la máquina virtual “ova” se procede a ejecutarla desde el GNS3 para que de este modo las imágenes de los equipos que se monten para la simulación se ejecuten de forma adecuada. En la Figura 3.12 se puede observar que tanto el GNS3 y la máquina virtual están operacionales.

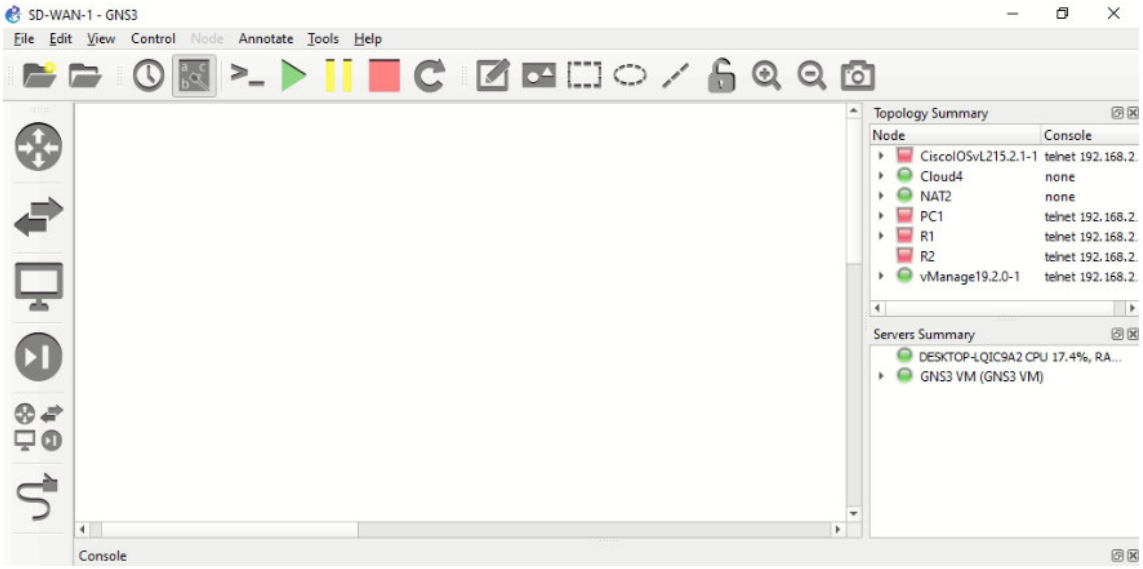


Figura 3.12 GNS3 y su máquina virtual en operación

Una de las configuraciones adicionales que se tiene en cuenta para el presente proyecto es la utilización de *software* de simulación eve-ng. El mismo que permitirá realizar la implementación de una red SDWAN mediante equipos Cisco. Para poder correr este programa se requiere de hacer uso de los servicios proporcionados por la plataforma *Google Cloud.*

En la Figura 3.13 se puede observar cómo una vez creada la cuenta en la plataforma se tiene el sistema listo para poder crear cualquier proyecto que se desee dentro de un proyecto se procederá a instalar un sistema operativo dentro del cual se ejecutará el *software* de simulación requerido.

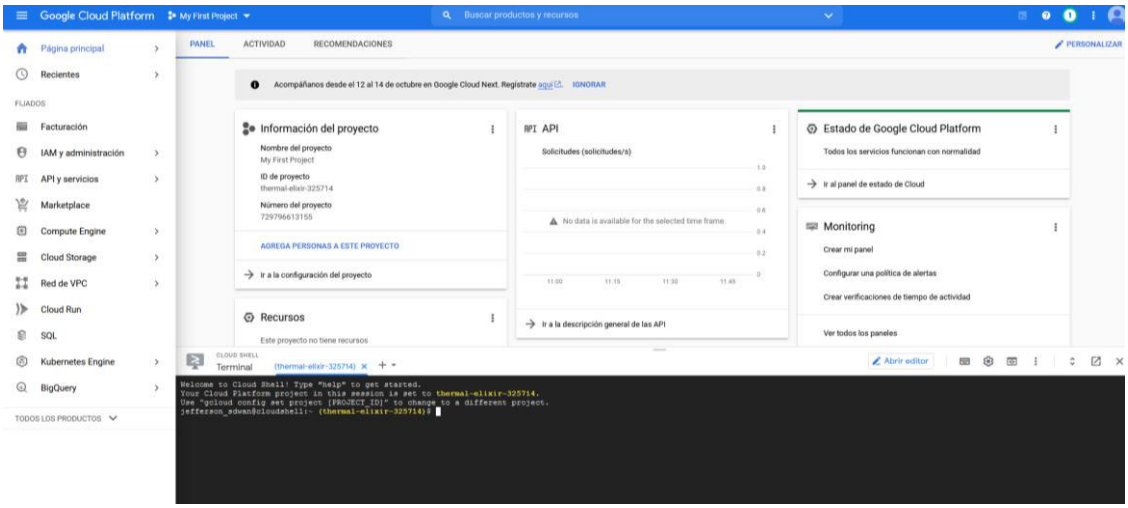


Figura 3.13 Inicio de plataforma *Google Cloud*

Para la creación de un nuevo proyecto se debe ingresar al apartado de “selección de proyecto > proyecto nuevo” como se muestra en la Figura 3.14.

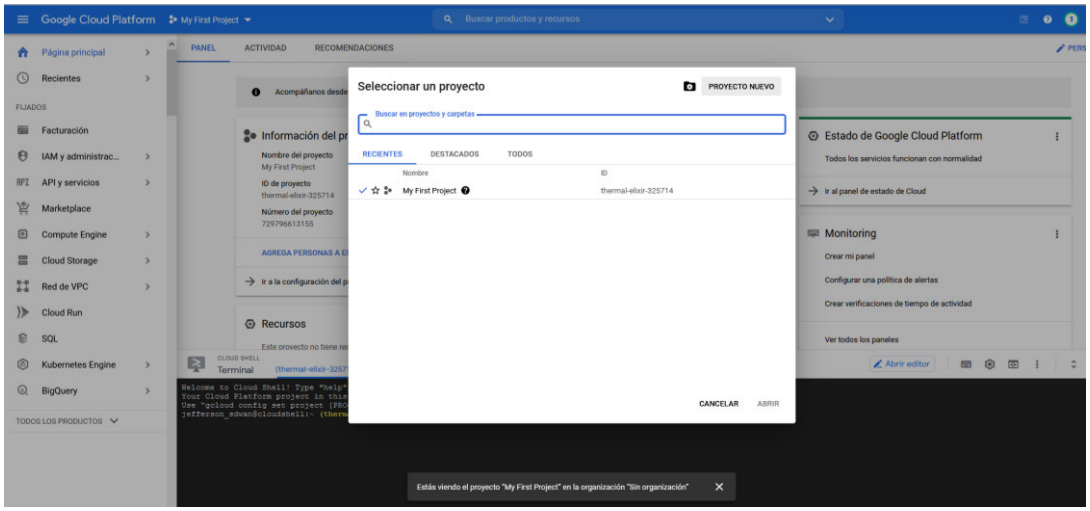


Figura 3.14 Creación de proyecto en *Google Cloud*

Una vez iniciado un nuevo proyecto se procede a asignarle el nombre de “*Eve-ng Cloud*” al mismo. Es importante que si se desea realizar simplemente una simulación a tipo de práctica el apartado de organización no sea alterado, caso contrario se puede enlazar el proyecto creado a una empresa en particular. Este procedimiento se observa en la Figura 3.15.

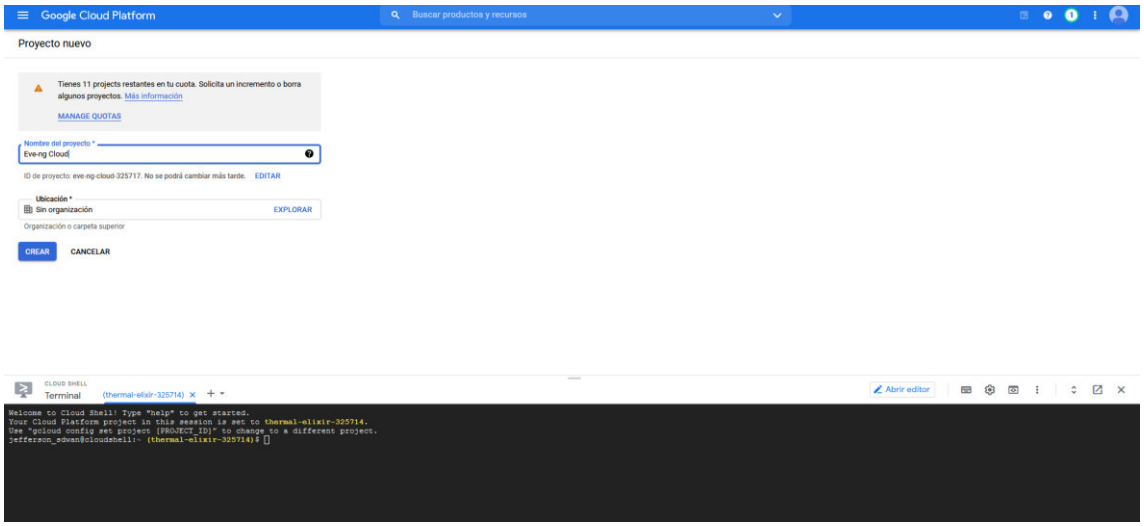


Figura 3.15 Asignación de nombre de proyecto

A continuación, se procede a descargar la versión de Ubuntu dentro de la cual se va a ejecutar el *software eve-ng*. Esta descarga se realiza mediante la terminal de comandos utilizada en la plataforma de *Google Cloud* y el comando para realizar esta acción es el siguiente:

gcloud compute images create nested-ubuntu-xenial –source-image-family=Ubuntu-1604-lts—source-image-project=Ubuntu-os-cloud-licenses=https://compute.googleapis.com/compute/v1/projects/vm-options/global/licenses/enable-vmx

Este comando descargará la versión de Ubuntu 16.04 así como las licencias de activación del mismo a través de la página de las aplicaciones de *Google* como se aprecia en la Figura 3.16.

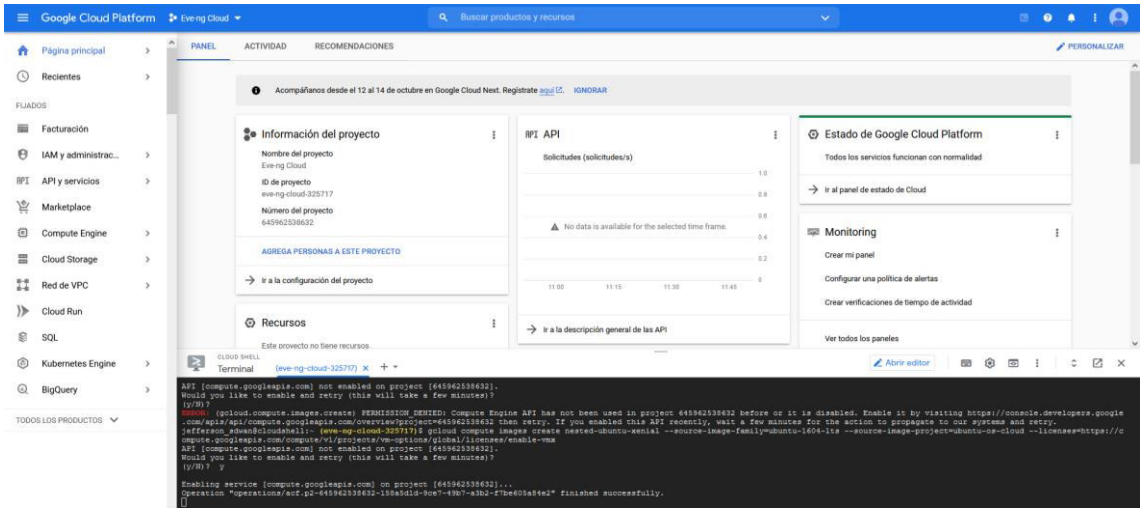


Figura 3.16 Instalación del sistema operativo Ubuntu 16.04

Con la instalación de este sistema finalizada se procede a configurar las instancias para la máquina virtual de Ubuntu. Estas instancias estarán basadas en los requerimientos del administrador, así como los requerimientos establecidos por eve-ng para funcionar, como se observa en la Figura 3.17.

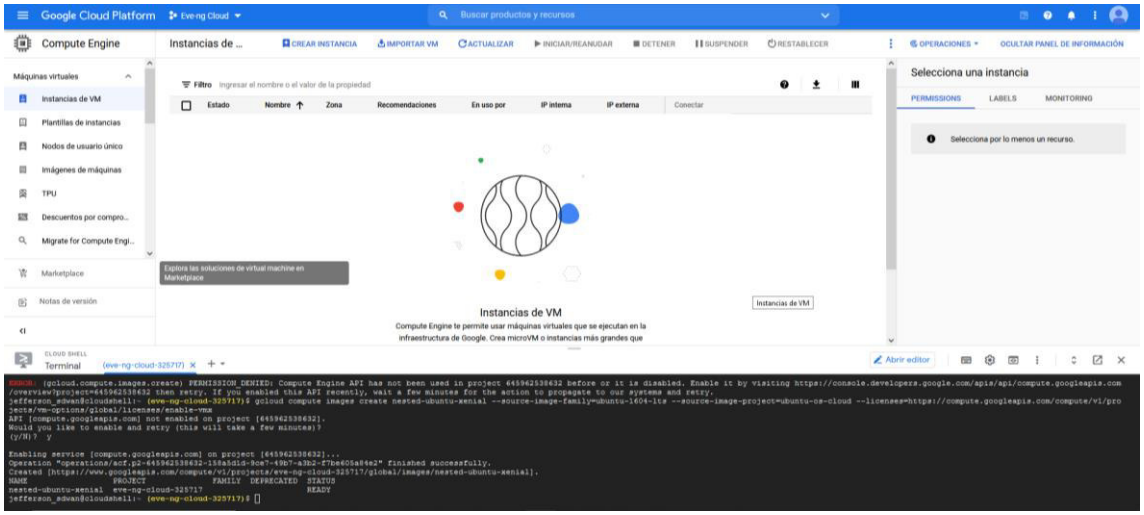


Figura 3.17 Configuración de instancias

El siguiente paso consiste en seleccionar la imagen correspondiente al sistema operativo que la máquina virtual leerá al momento del arranque. Para ello se accede al apartado “Disco de arranque > imágenes personalizadas”, donde la imagen que se debe seleccionar es la denominada *nested-ubuntu-xenial*, la cual corresponde al sistema operativo activado como se aprecia en la Figura 3.18.

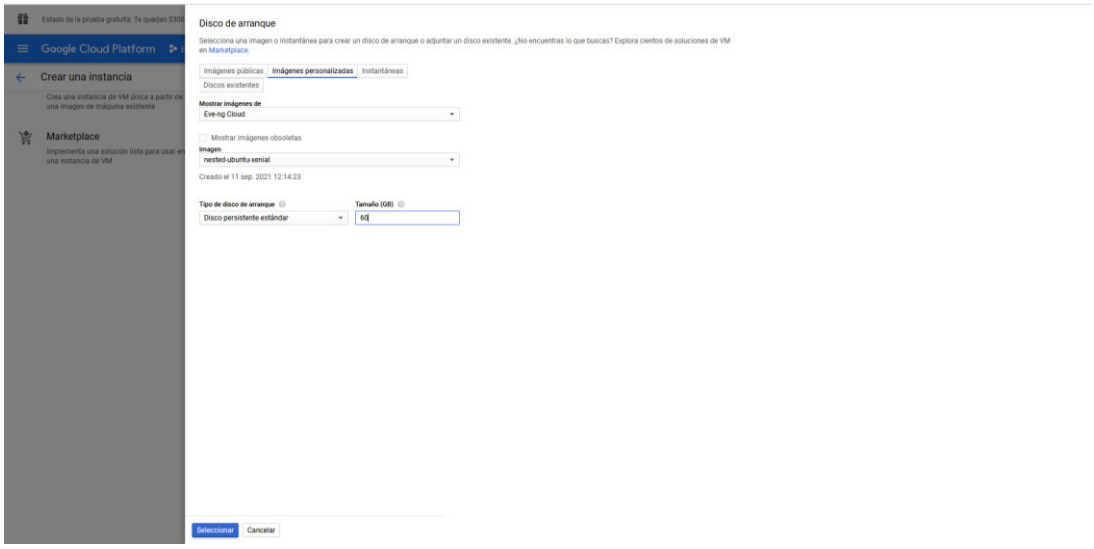


Figura 3.18 Selección de imagen de sistema operativo

A continuación, se procede a la configuración de los parámetros con los que contará la máquina virtual. Para este caso se configura un sistema que cuente con 16 procesadores virtuales, esta cantidad es la ideal para soportar la simulación de los equipos pertenecientes a Cisco. Adicionalmente se asigna un valor de 60 (Gb) de memoria, así como la configuración de los permisos de acceso que para este apartado se asignarán como predeterminados y se habilitará el tráfico procedente tanto de *Hypertext Transfer Protocol* (HTTP) como de *Hypertext Transfer Protocol* Secure (HTTPS). Es decir, se habilita la recepción de tráfico de los puertos 80 y 443 como se muestra en la Figura 3.19 y Figura 3.20.

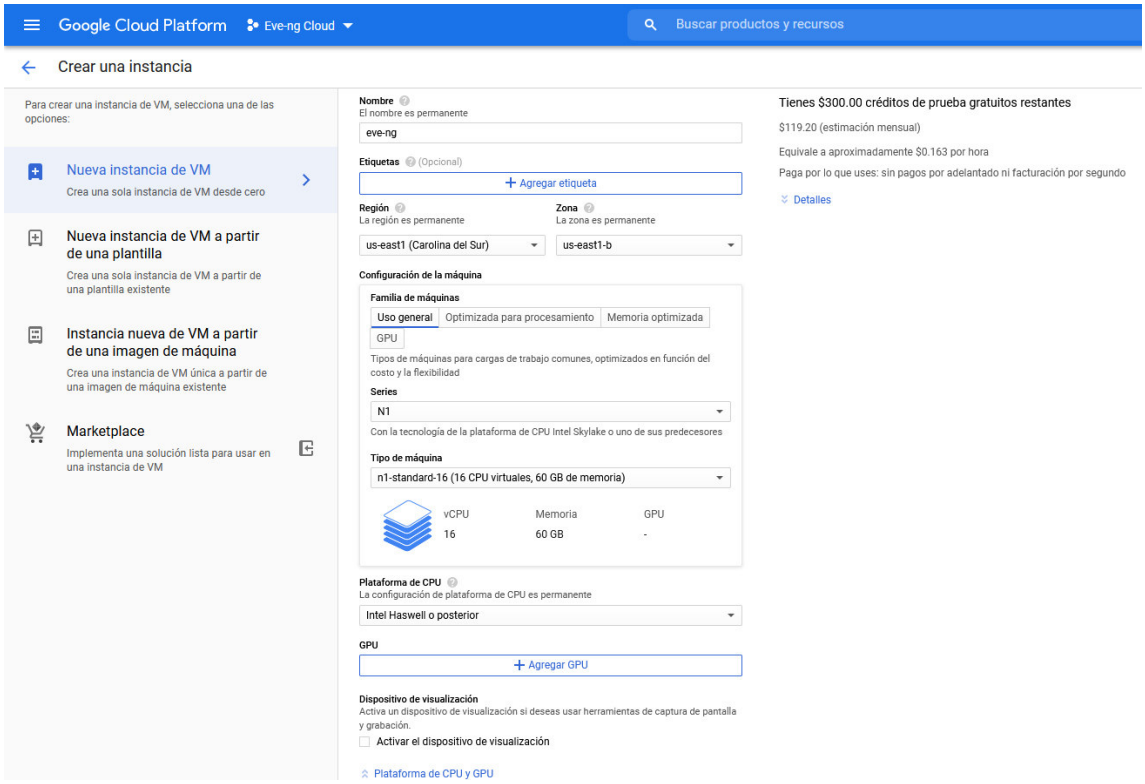


Figura 3.19 Parámetros de instalación máquina virtual

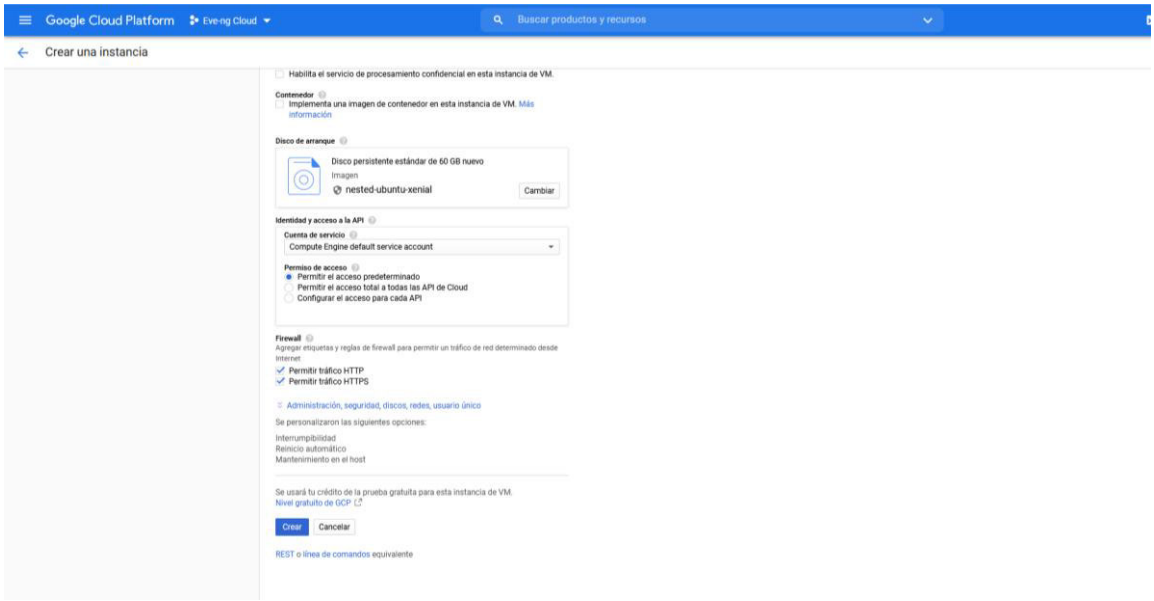


Figura 3.20 Asignación de permisos máquina virtual

A continuación, se verifica que la máquina virtual fue correctamente instalada para ello se deben comprobar que posea tanto una dirección IP interna como una dirección IP externa y que el estado actual de la máquina se encuentre disponible como se muestra en la Figura 3.21.

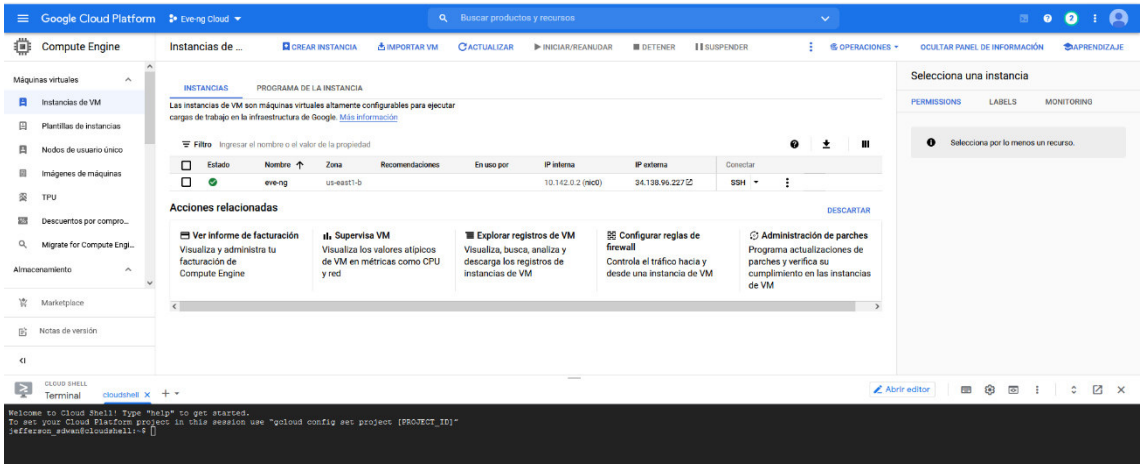


Figura 3.21 Máquina virtual disponible

El siguiente paso es realizar la instalación del *software* de simulación eve-ng, esto se realiza por medio de la terminal de ssh aplicando los siguientes comandos:

- sudo -i
- wget -O - https://www.eve-ng.net/repo/install-eve.sh | bash -i
- apt update
- apt upgrade
- apt install eve-ng-dockers
- reboot

Con el comando wget se obtienen los recursos necesarios para la instalación del *software* eve-ng desde la página oficial de este *software*. Posteriormente se procede a actualizar los archivos en el sistema y a cargar estas actualizaciones, luego se procede con la instalación de los diferentes paquetes que requiere eve-ng para operar correctamente. Finalmente para cargar todos los cambios realizados se reinicia el sistema como se observa en la Figura 3.22.

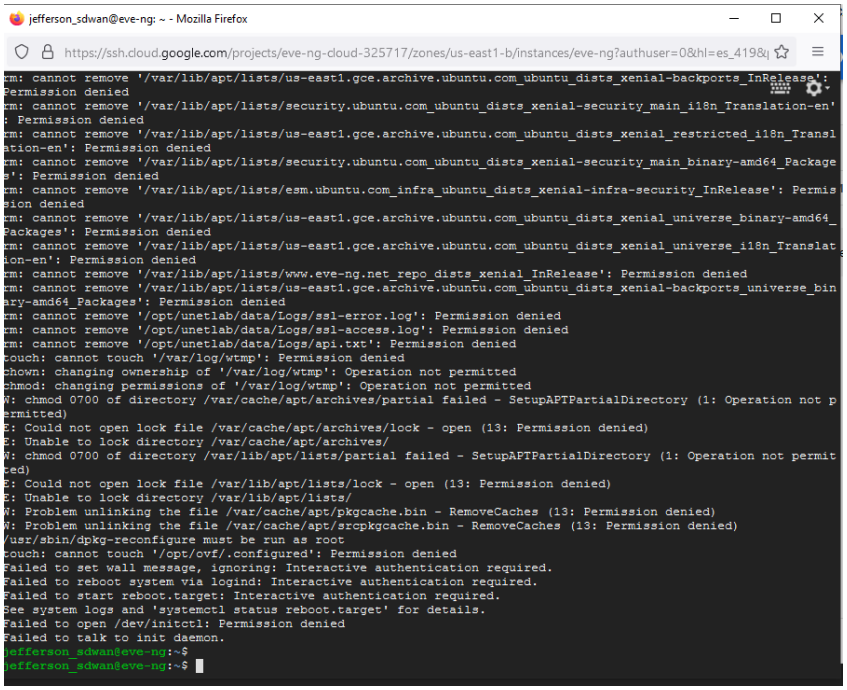


Figura 3.22 Instalación de Eve-ng

De este modo concluye la instalación del *software* eve-ng.

3.3 Configuración de redes SDWAN Cisco-Fortinet

Configuración de red SDWAN mediante equipos Cisco

Con el *software* eve-ng correctamente instalado se procede a ingresar a este emulador haciendo uso de las credenciales por defecto del sistema las mismas que tienen como usuario “admin” y como contraseña “eve” como se aprecia en la Figura 3.23.

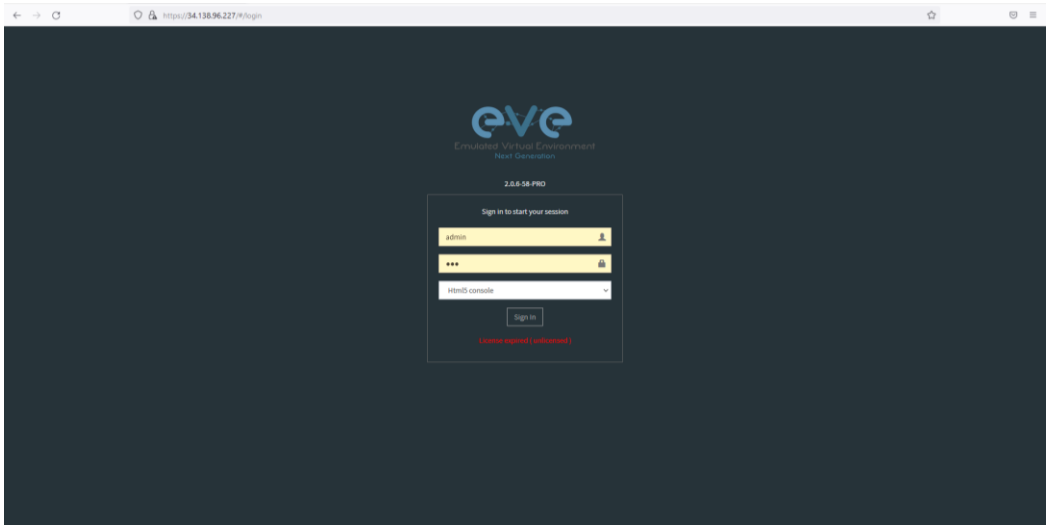


Figura 3.23 Credenciales de ingreso al emulador eve-ng

El siguiente paso a configurar es la creación de un nuevo laboratorio el cual tendrá por nombre SD-WAN. Esta acción se realiza ingresando al apartado "*New > Add new lab*", como se muestra en la Figura 3.24.

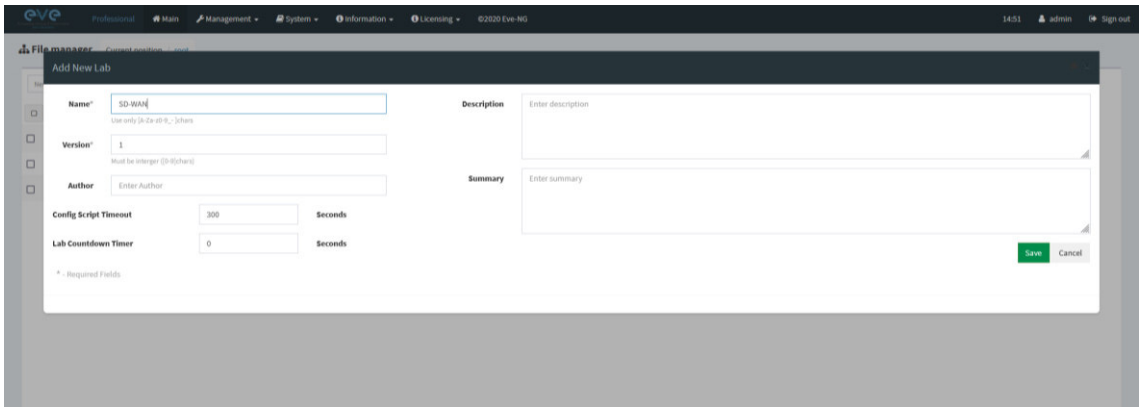


Figura 3.24 Creación de laboratorio SD-WAN

Una vez creado el laboratorio se procede a la descarga de los equipos correspondientes a la serie Cisco-Viptela pertenecientes a Cisco. Los mismos que se pueden adquirir dentro del repositorio virtual de Cisco directamente de la página de *IT Training* como se muestra en la Figura 3.25.

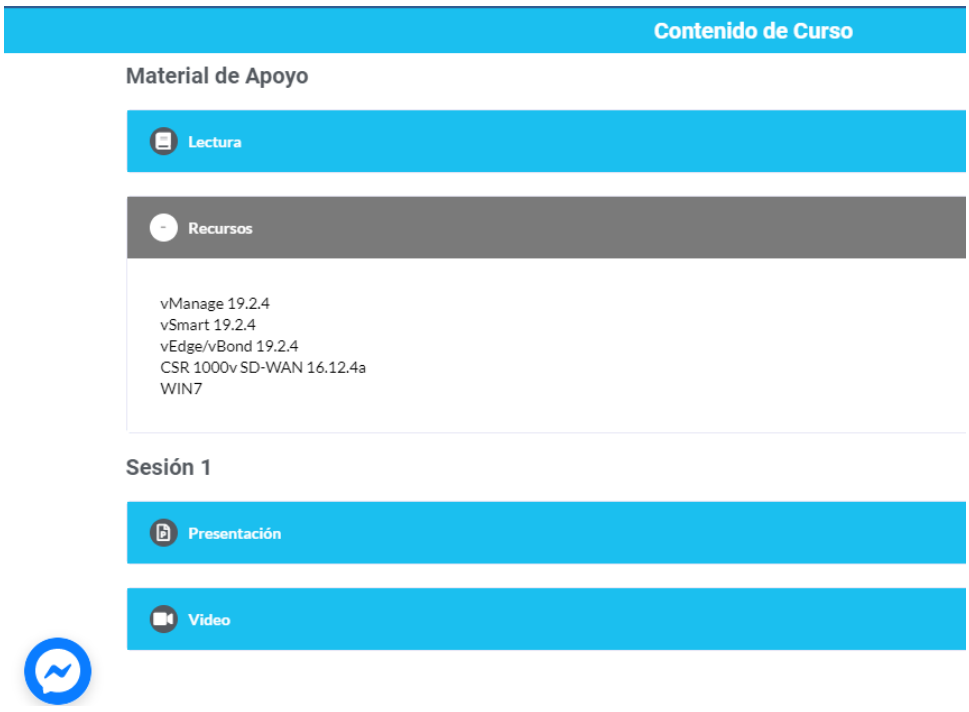


Figura 3.25 Equipos Cisco Cisco-Viptela en repositorio

A continuación, se procede a cargar los equipos dentro del emulador eve-ng para ello se requiere de un programa denominado WinSCP el cual haciendo uso del protocolo

Secure File Transfer Protocol (SFTP) hacia el puerto 22 permite la conexión directa hacia una dirección IP especificada, la cual para este caso corresponde a "34.138.96.227". Adicionalmente para poder entablar una comunicación se requiere ingresar con las credenciales previamente establecidas como usuario "*root*" y contraseña "tesis" como se muestra en la Figura 3.26.

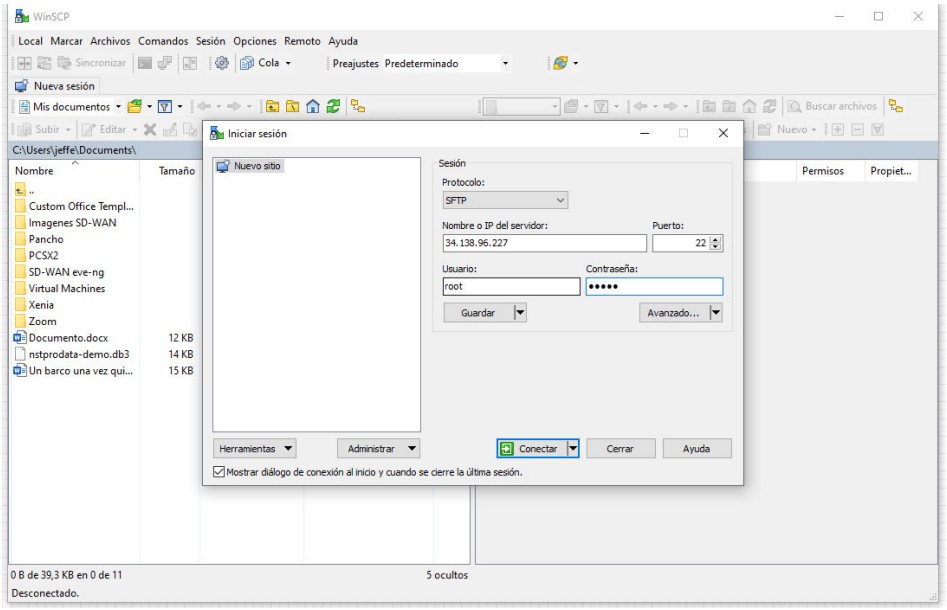


Figura 3.26 Sesión por medio de WinSCP

A continuación, se procede a ingresar al directorio "/opt/unetlab/addons/quemu/" dentro del cual se procederán a crear los directorios respectivos para cada equipo. Como se muestran en la Figura 3.27 y la Figura 3.28 respectivamente

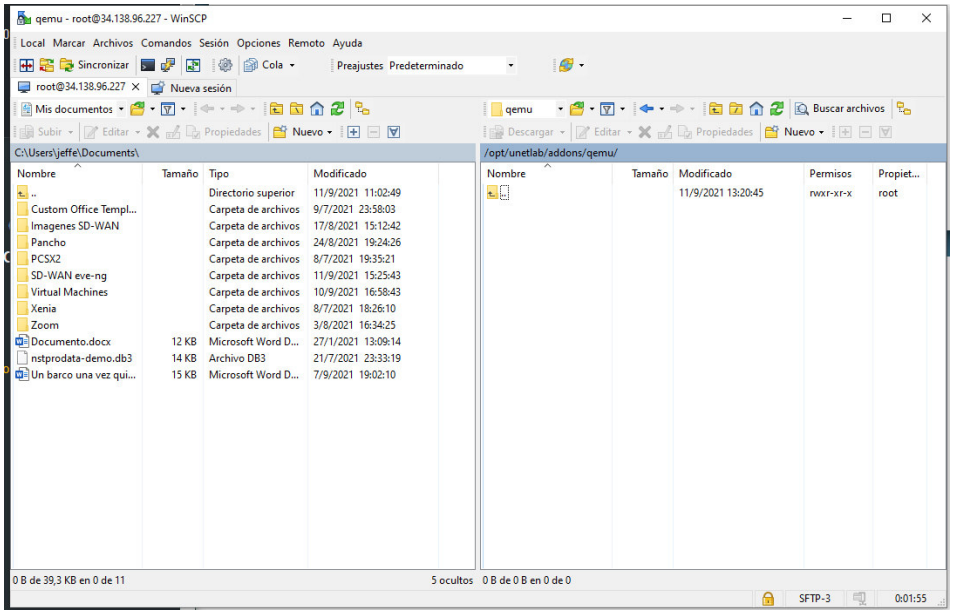


Figura 3.27 Directorio para subir imágenes

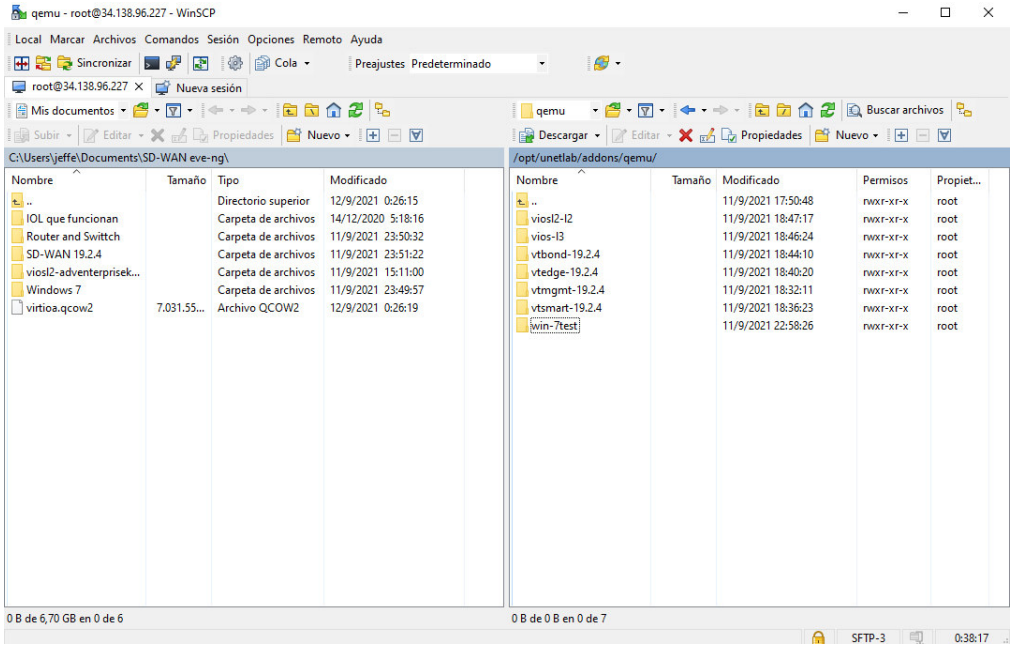


Figura 3.28 Directorios de imágenes

A continuación, se procede a ubicar el directorio dentro del cual se tienen descargadas las imágenes en la máquina local y una vez localizadas se procede a ubicar el directorio para la imagen qcow correspondiente y se procede a arrastrar los archivos y cargarlos manualmente como se aprecia en la Figura 3.29. Posteriormente el nombre de este archivo debe ser renombrado para hacerlo compatible con el sistema el nombre que debe llevar es “virtioa.qcow”, este procedimiento se replica para todos los componentes de la red, como se muestra en la Figura 3.30.

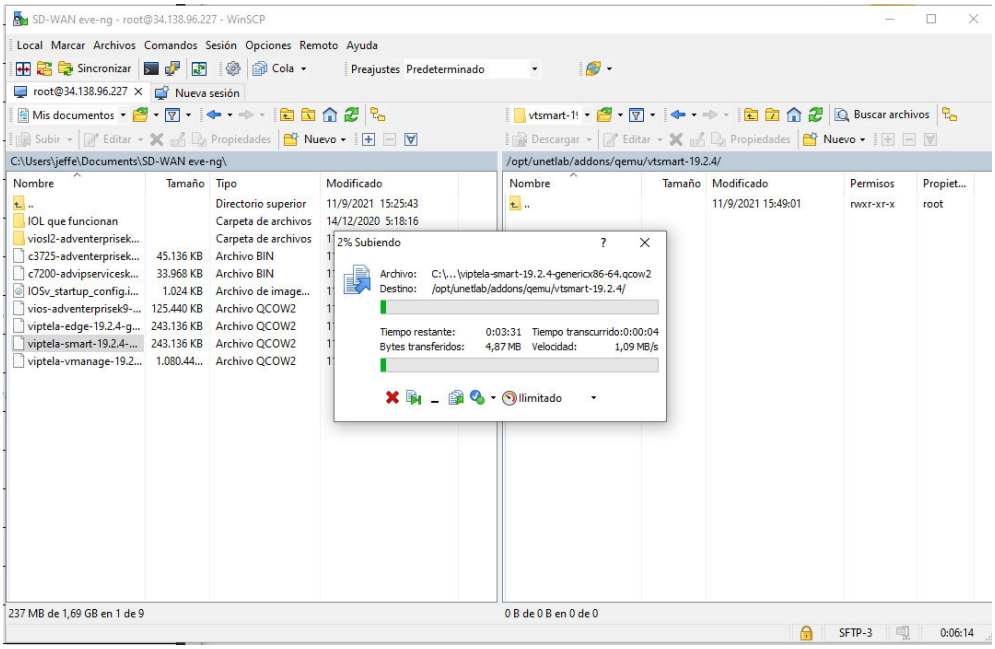


Figura 3.29 Cargar de archivos hacia emulador

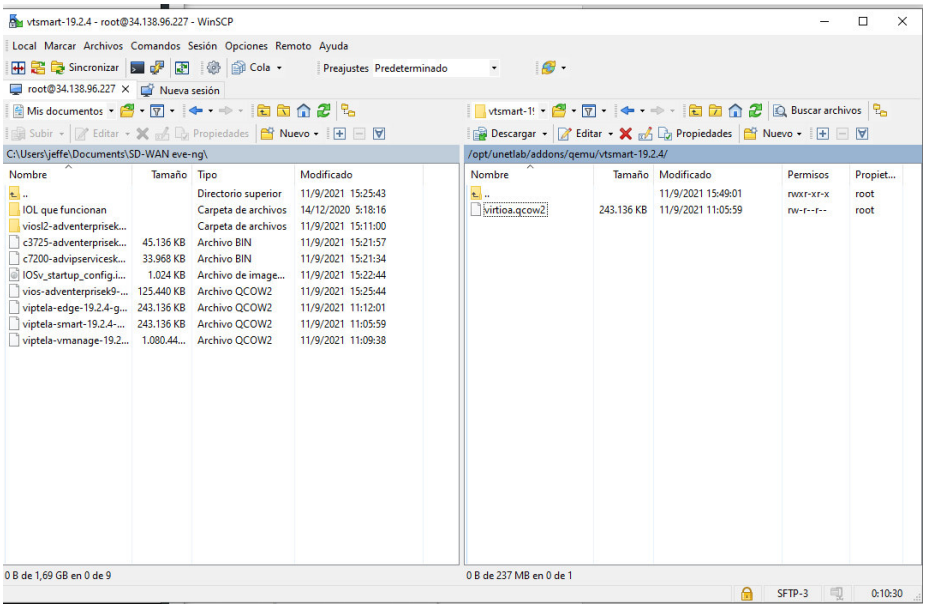


Figura 3.30 Asignación de nombres a imágenes ISO

Para el caso del dispositivo *vManage* se requiere crear un disco virtual adicional dentro del cual se almacenará toda la información correspondiente a las configuraciones de los diferentes dispositivos que conforman la red SD-WAN. El comando utilizado se detalla continuación:

- qemu-img create -f qcow2 virtiob.qcow2 100G

Este comando permite la creación de un disco de 100 (Gb) virtuales y se lo debe ejecutar dentro del sistema ssh como se muestra en la Figura 3.31.

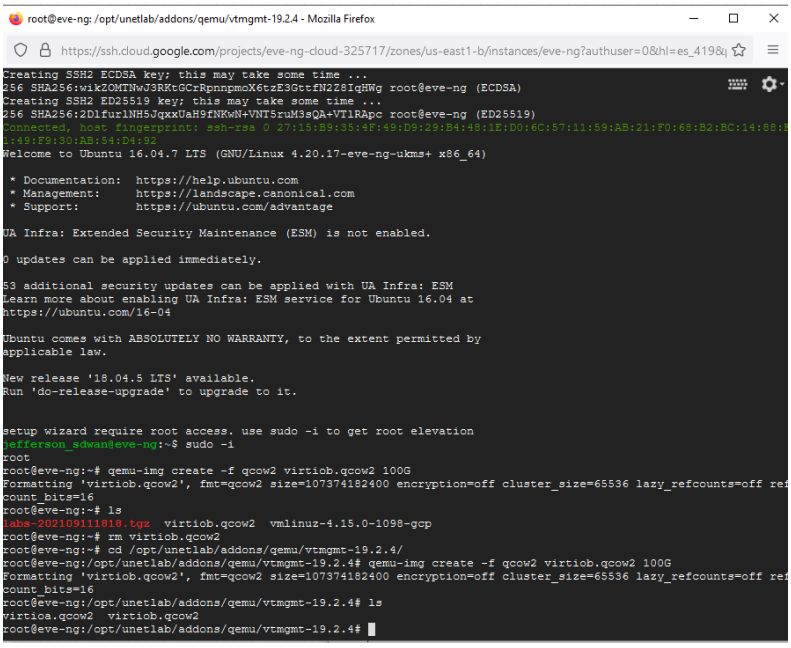


Figura 3.31 Creación de disco virtual para *vManage*

Finalmente, se procede a añadir cada uno de los nodos mediante la especificación del equipo a desplegar en el sistema. Adicionalmente cabe recalcar que las versiones que se utilizan para este proyecto son las versiones 19.2.4, adicionalmente se especifica la versión de archivo qcow y también de ser necesario se le puede dar una configuración inicial al arrancar el equipo. Esto se realiza para todos los equipos que conforman la red como se muestra en la Figura 3.32, la Figura 3.33, y la Figura 3.34 respectivamente

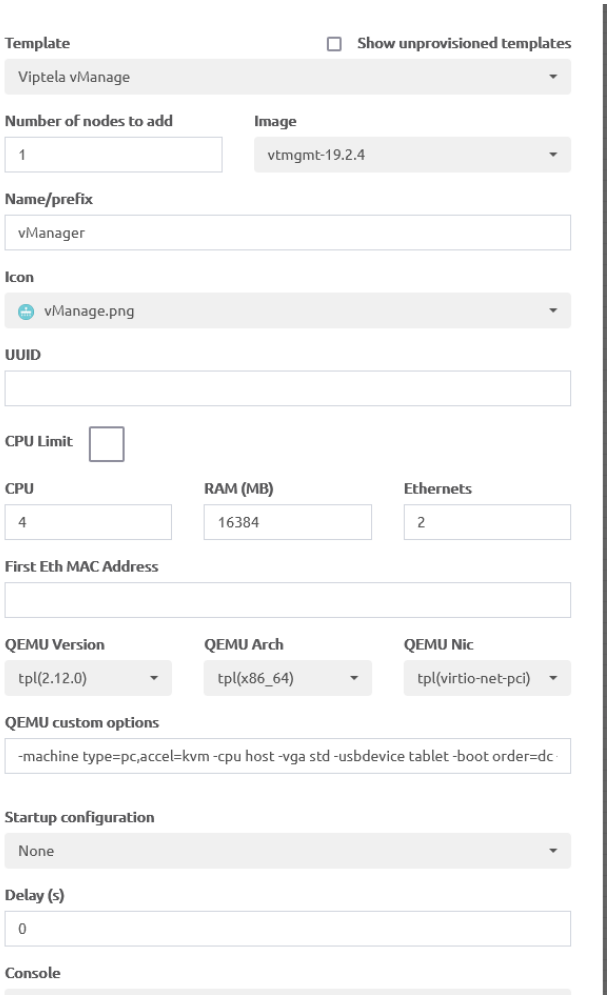


Figura 3.32 Despliegue de *vManage*

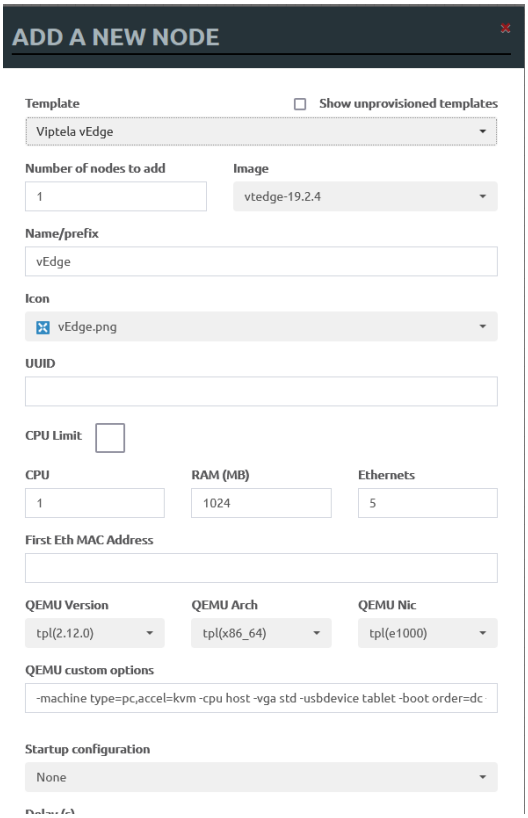


Figura 3.33 Despliegue de *vEdge*

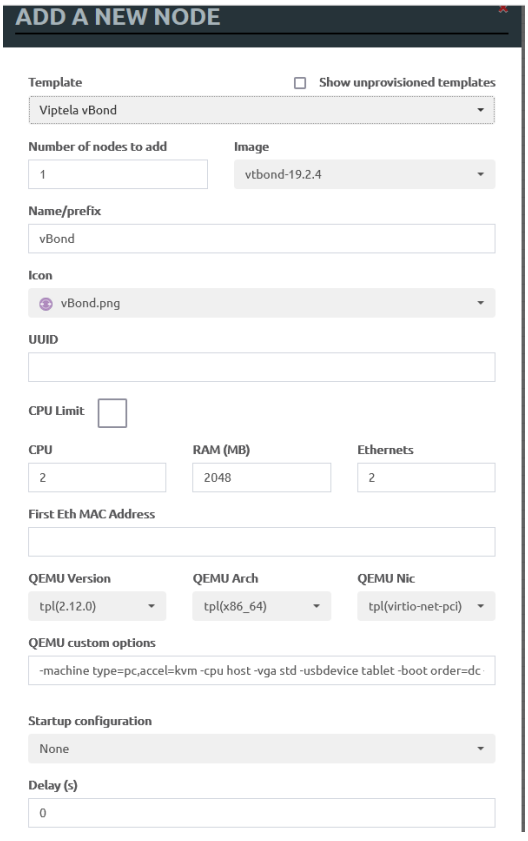


Figura 3.34 Despliegue de *vBond*

Posteriormente, se procede a realizar la configuración del equipo vManage. El primer paso a configurar en este equipo es seleccionar el disco donde se va a almacenar toda la información procedente de este router, para este caso y debido a que se desea que esta información se guarde en el disco principal se selecciona la primera opción y se confirma esta selección presionando la tecla “y” cuando el sistema lo requiere. Una vez completada esta tarea se puede acceder a la interfaz de comandos de vManage como se observa en la Figura 3.35.

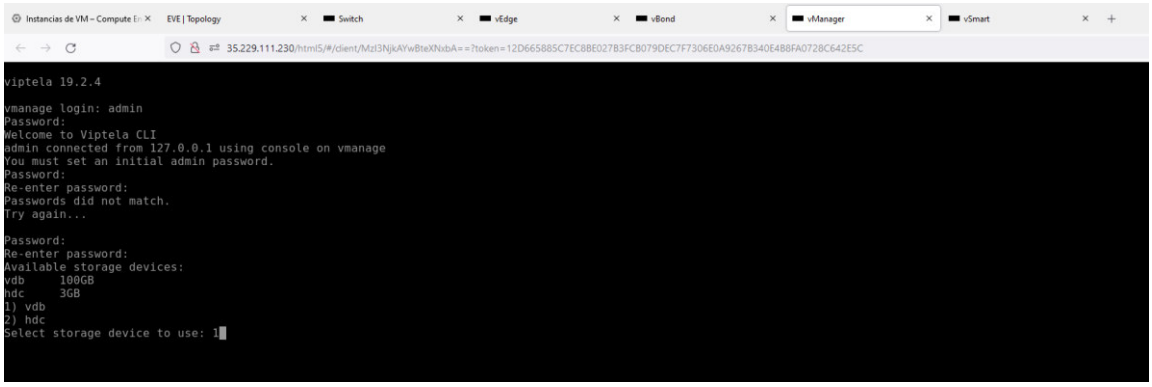


Figura 3.35 Interfaz de comandos *vManage*

Una vez dentro del router *vManage* se procede a realizar la configuración del mismo por medio de los siguientes comandos:

- config
- system
- system-ip 50.3.0.2
- site-id 503
- organization-name “sd-wan-lab”
- vbond 200.1.1.1
- host-name *vManage*

El comando “config” permite el ingreso a las configuraciones del router *vManage* y por medio del uso del comando “*system”* se pueden establecer los parámetros para este sistema en específico. La dirección IP del sistema es una dirección única que se le asigna a cada router para que pueda ser identificado dentro de un área en específico, esa dirección pertenece a una red IPv4 y puede ser establecida haciendo uso del comando “*system-ip* 50.3.0.2”. Posteriormente se procede a configurar el número de área correspondiente en este router el cual será de 503 esto se realiza mediante el comando “*site-id*”. También se define la dirección IP del equipo *vBond* la cual tendrá

como valor 200.1.1.1/24 para ser identificado dentro de la red, finalmente para concluir con las configuraciones dentro del sistema se define el nombre del equipo con el comando "*host-name*" el cual será *vManage.*

A continuación, también se configuran las conexiones VPN dentro del equipo, para poder realizar este procedimiento se utilizaron los siguientes comandos:

- Vpn 0
- ip route 0.0.0.0/0 200.1.1.5
- Interface eth0
- Ip add 200.1.1.2/24
- No shut

Lo que primero debe realizarse es definir la VPN que se desea configurar para el caso de este equipo la VPN es la 0. Posteriormente se procede a ingresar a la interfaz a la cual se encuentra conectado el router para poder configurar una VPN, la dirección que se va a utilizar durante esta comunicación es la 20.1.1.2/24 la cual permitirá la comunicación hacia el exterior. Finalmente haciendo uso del comando "*no shutdown*" se procede a levantar la interfaz, este procedimiento se puede analizar en la Figura 3.36.

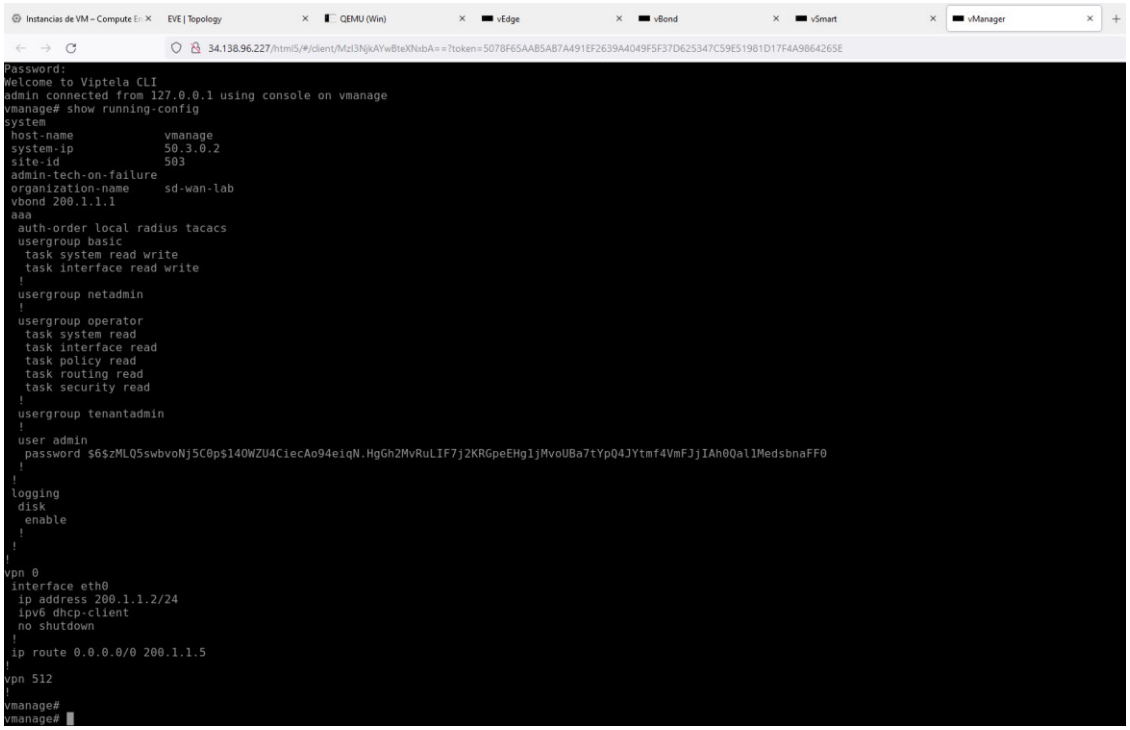


Figura 3.36 Configuración inicial vManage

Con las primeras configuraciones realizadas en el equipo *vManage* se procede a realizar las configuraciones dentro del equipo vSmart. Los comandos que se usarán para el establecimiento de los diferentes parámetros son los siguientes:

- Config
- System
- Host-name vsmart
- System-ip 50.3.0.3
- Site-id 503
- Organization-name “sd-wan-lab”
- Vbond 200.1.1.1

Dentro de este equipo vSmart se procede a configurar una dirección fija para ser identificable dentro del área de trabajo y adicionalmente se procede a colocar el número del área que al igual que en el equipo pasado es de 503 esto gracias al comando “*site-id*”. Adicionalmente también se establece el nombre de la organización que para este proyecto fue definido como SD-WAN y la dirección del equipo complemento vBond la cual es la 200.1.1.1.

Este equipo también requiere una conexión de tipo VPN para lo cual se utilizarán los siguientes comandos en su configuración:

- VPN 0
- ip route 0.0.0.0/0 200.1.1.5
- Interface th0
- Ip add 200.1.1.3/24
- No shut
- Commit and-quit

Al igual que en vManage se configura la VPN 0 para que pueda salir a la red por medio del uso de la dirección IP establecida 200.1.1.3. Esto permitirá al equipo ser reconocido en la red, finalmente toda la configuración es guardada en el router haciendo uso del comando “*commit and-quit*” como se aprecia en la Figura 3.37.

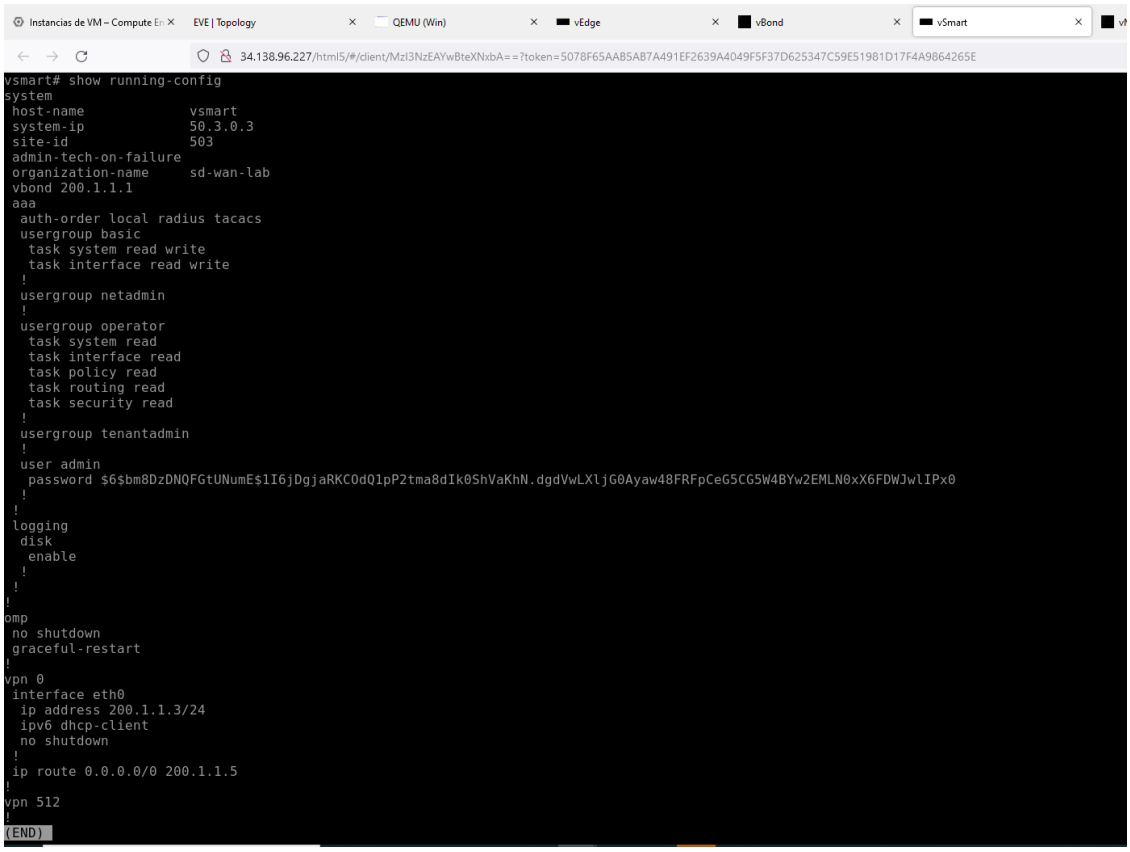


Figura 3.37 Configuración inicial vSmart

Con la configuración básica establecida en los dos equipos principales como lo son vManage y vSmart y con la configuración de la nube realizada para poder mantener una conexión con el equipo físico se debe acceder a la interfaz gráfica del router vManage. Para poder realizar las configuraciones de los certificados en los diferentes equipos, se debe acceder a la interfaz gráfica para lo cual se procede a abrir el navegador de preferencia *Google Chrome* y se escribe como URL el siguiente parámetro https://200.1.1.2 dirección que corresponde al equipo *vManage.* Una vez que la página cargue se obtiene el resultado que se observa en la Figura 3.38 a continuación.

Figura 3.38 Ingreso a interfaz gráfica vManage

Las credenciales de acceso a esta interfaz son las mismas que por defecto vienen establecidas en los equipos Cisco-Viptela y tanto para el usuario como para la contraseña será "*admin"*. Al ingresar a esta interfaz gráfica se tienen diferentes parámetros los cuales mostrarán al administrador el estado actual de la red SD-WAN. En la parte superior se tiene la cantidad de equipos que se dispone es decir cuántos equipos *vEdge*, *vSmart*, *vBond* y *vManage* está manejando la red. También se cuenta con la cantidad de reinicios que ha presentado el sistema y la cantidad de advertencias o emergencias que se presentaron en la red, algunas de las aplicaciones de la interfaz gráfica se detallan a continuación:

- *Control Status.* – permite conocer el estado actual de la red si se encuentra totalmente activa, parcialmente activa o caída.
- *WAN Edge Inventory.* – muestra la cantidad de equipos vEdge que posee la red, así como cuántos de estos equipos están autorizados, cuántos están desplegados y cuántos están pausados.
- *Top Applications*. – muestra la cantidad de aplicaciones que se están ejecutando, así como las más relevantes dentro de la organización.
- *Site Health*. – dentro de este apartado se puede conocer cuántos sitios WAN dentro de la red SD-WAN se están llevando a cabo correctamente, es decir cuántas de estas redes tienen conectividad total, parcial o sin conectividad.
- *Wan Edge Health.* – este apartado muestra en qué estado se encuentran los equipos vEdge dentro de la infraestructura. Es decir, cuántos de los equipos están

en estado normal, cuantos tienen alguna advertencia y cuántos de ellos presentan error

- *Trasport Interface Distribution*. – aquí se muestran las velocidades en las cuales la información pasa a través de la red SD-WAN teniendo valores menores a 10 (Mbps) hasta mayores a 500 (Mbps).
- *Transport Health.* – este apartado muestra la situación en el transporte de los datos, si alguna ruta se cayó o si algún dato se ve alterado de alguna manera en el trayecto.
- *Application-Aware Routing.* – aquí se muestra el estado de las conexiones VPN que se configuraron en los equipos, así como el tiempo de latencia de cada uno.

Todos y cada uno de estos parámetros es fundamental para determinar el estado de la red SD-WAN por lo que el administrador deberá mantenerse atento a cualquier advertencia que pueda presentarse a futuro. La interfaz gráfica se puede observar en la Figura 3.39 a continuación.

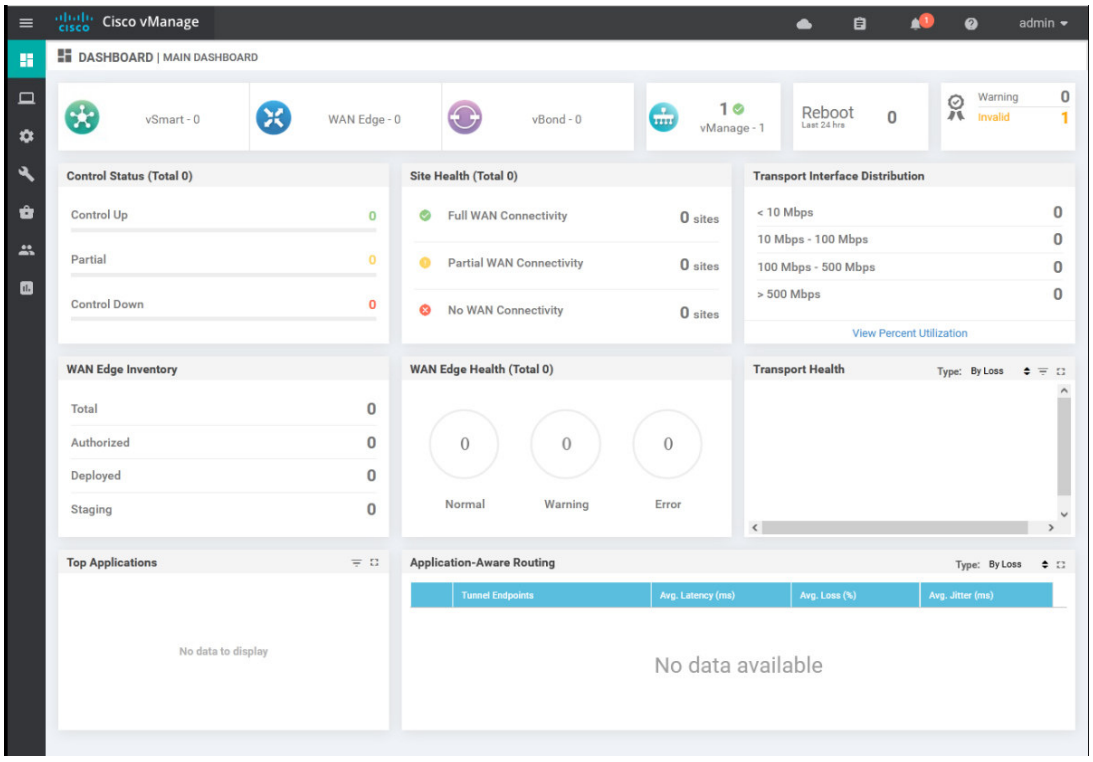


Figura 3.39 Opciones en interfaz gráfica vManage

Una vez que se ha verificado la conectividad hacia la interfaz gráfica del equipo vManage se procede a ingresar a la terminal del equipo vSmart para comprobar la conectividad del mismo. Para llevar esto a cabo se realiza un ping hacia la dirección establecida del equipo es decir la 200.1.1.2 como se muestra en la Figura 3.40.

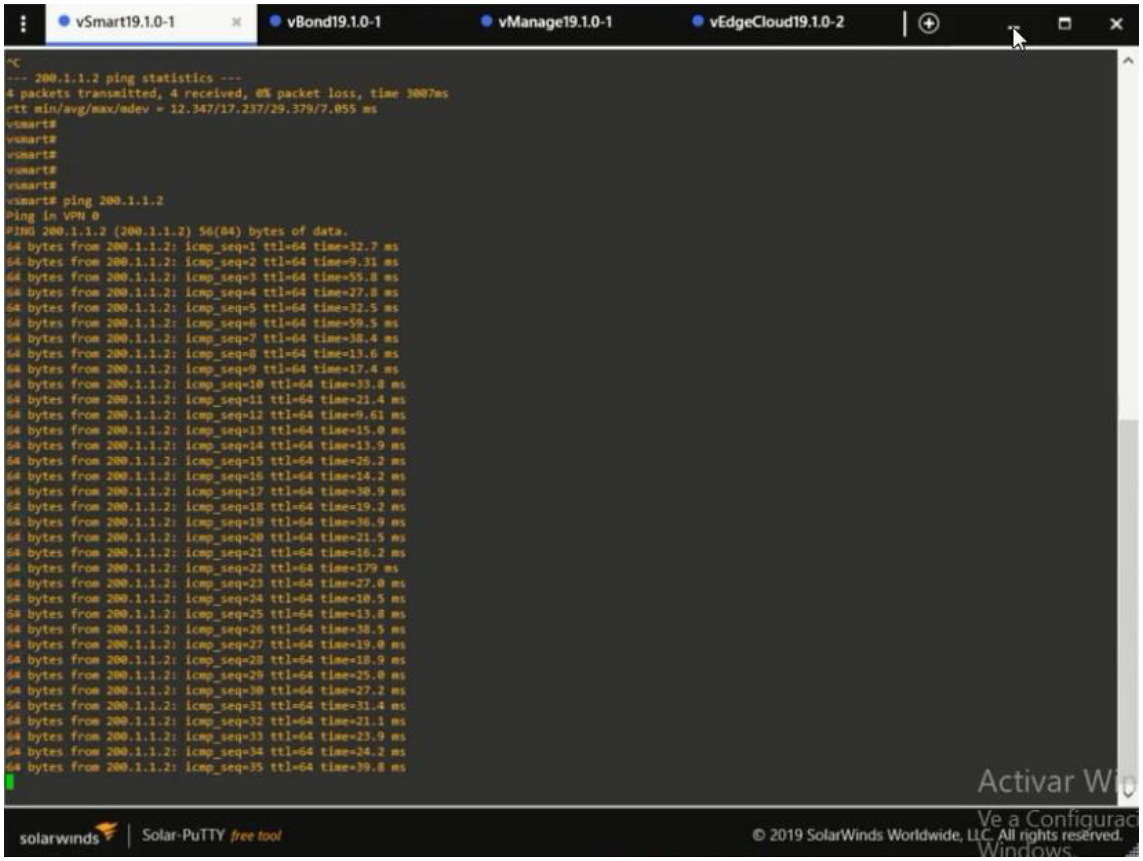


Figura 3.40 Verificación de conexión mediante mensajes ICMP vSmart

Con los equipos *vEdge* y *vManage* configurados se procede a configurar algunos de los parámetros importantes dentro de la interfaz gráfica. Para esto se accede al apartado de administración y se configura el nombre de la organización que como ya se había configurado previamente en los equipos será “SD-WAN” una vez hecho este cambio se procede a guardar los cambios como se aprecia en la Figura 3.41.

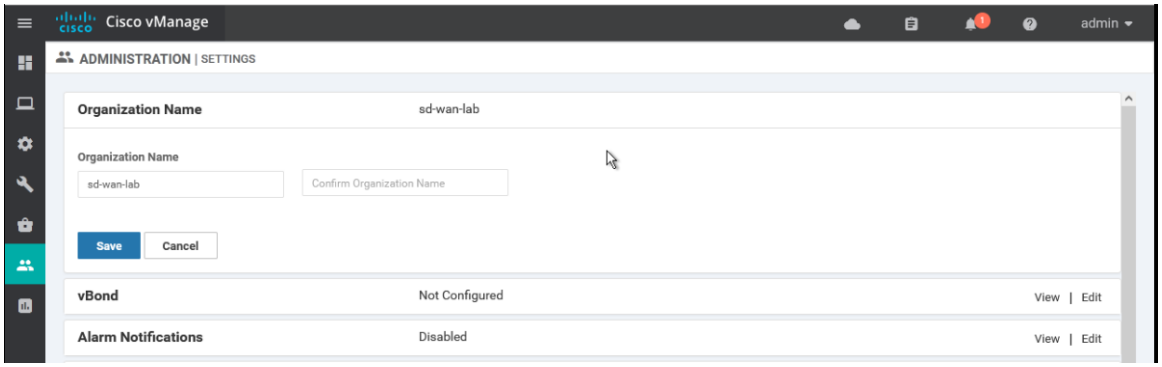


Figura 3.41 Establecimiento de nombre de organización

El siguiente parámetro a configurar es la dirección del equipo vBond la cual será 200.1.1.1. Esta dirección ya se la había configurado previamente dentro del equipo vManage y vSmart, esta configuración se aprecia en la Figura 3.42.

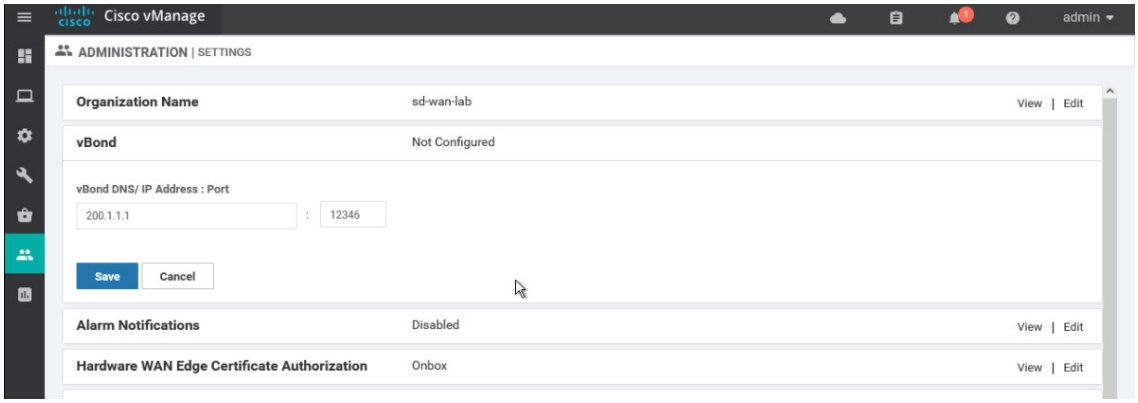


Figura 3.42 Establecimiento de dirección IP de equipo vBond

Con estos parámetros configurados se ingresa al vManage para poder configurar los diferentes certificados en este caso se comenzará configurando el certificado raíz el cual es un certificado que utiliza una clave pública para autentificar al usuario root. Este certificado será emitido por la autoridad de certificación (CA) hacia el usuario raíz para poder ingresar a solicitar estos certificados se debe acceder a la interfaz de línea de comandos dentro del router para esto se usa el comando "vshell". Una vez dentro se utilizará el comando "openssl genrsa –out ROOTCA.key 2048", el objetivo principal de este comando es generar una clave RSA para el usuario raíz con una longitud de 2048 bits esta clave será de tipo privado y proporcionará el certificado para poder ser ingresado en la interfaz gráfica. Adicionalmente para poder validar esta clave con los nuevos nodos a crearse y establecer a su vez un tiempo de validez de este certificado. Para comprobar que esta clave fue generada de manera exitosa se utiliza el comando "ls" para desplegar todos los archivos contenidos en ese directorio, estos archivos deberán ser:

- ROOTCA.key
- ROOTCA.pem
- Archive_id_rsa.pub

Una vez que se ha comprobado que estos archivos existen y se crearon de manera exitosa por medio del uso del comando "cat" se despliega el certificado guardado en ROOTCA.pem para posteriormente copiarlo a la interfaz gráfica de vManage. El certificado se puede observar en la Figura 3.43.

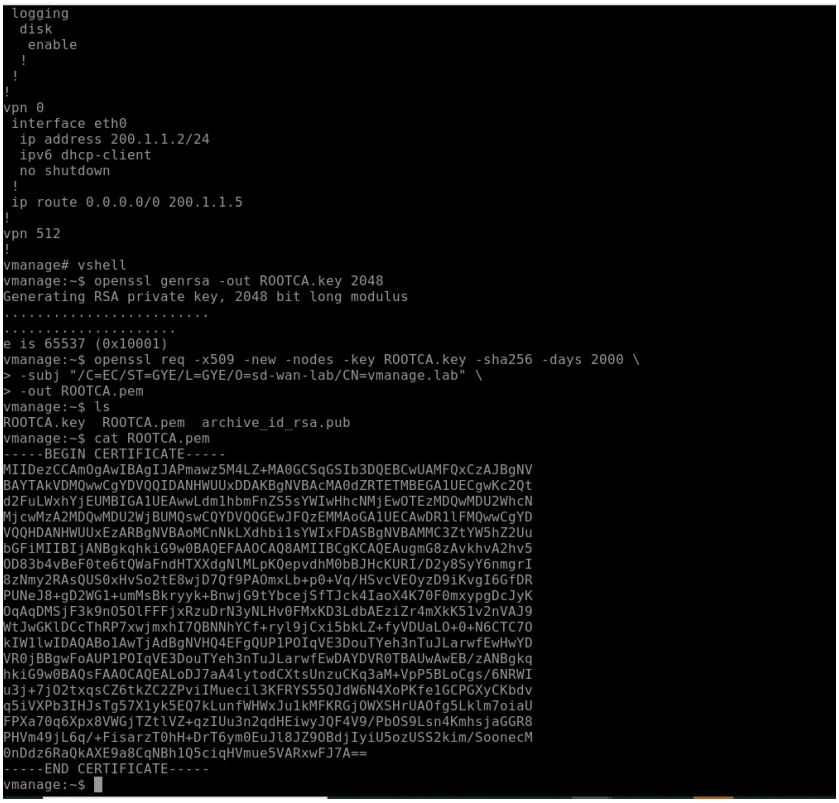


Figura 3.43 Generación de certificado raíz vManage

Con las claves ROOTCA generada se procede a ir a la interfaz gráfica de vManage donde en el apartado de administración se debe acceder a la opción de autorización de certificados de control. Aquí se pueden seleccionar diferentes tipos de certificados ya sean firmados por Cisco, Symantec, manual, o empresarial; para el caso de este proyecto se usará la opción de "*Enterprise Root Certificate"*. En el apartado de certificado se pega todo el certificado generado en ROOTCA.pem como se aprecia en la Figura 3.44.

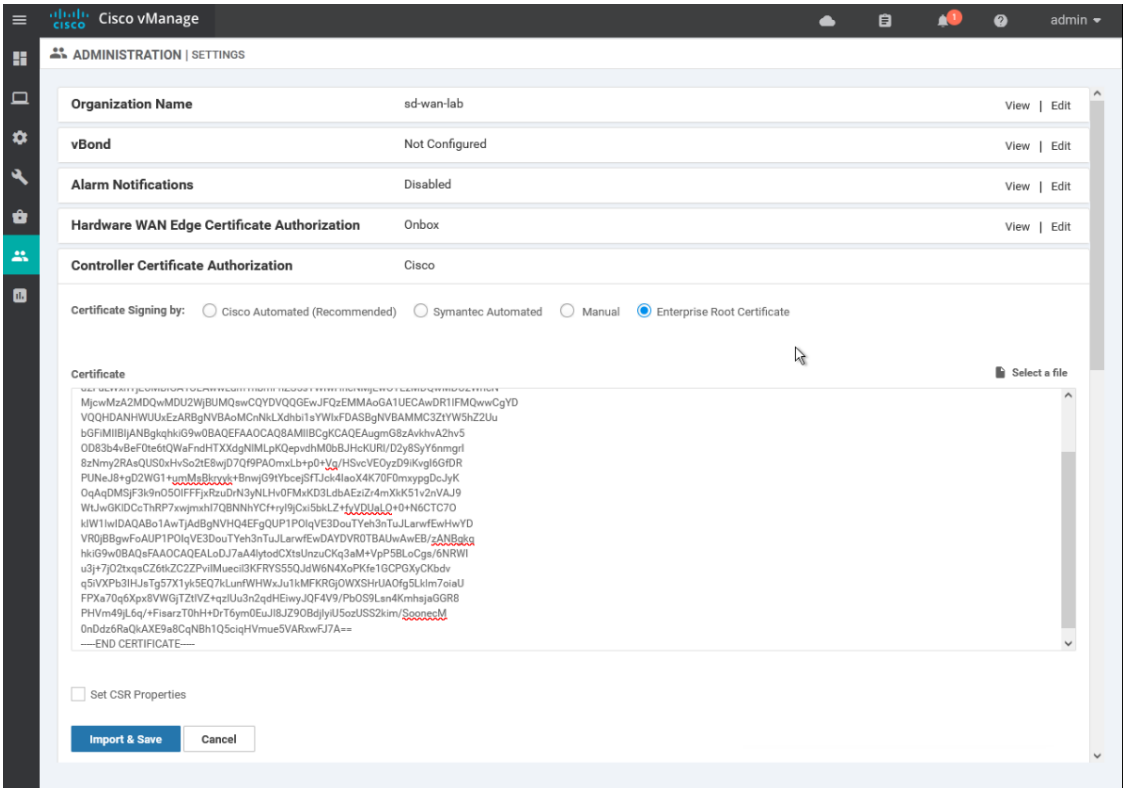


Figura 3.44 Ingreso de certificado en interfaz gráfica

Con el certificado raíz configurado, se accede en la interfaz gráfica al apartado de configuraciones. Aquí se encuentran dos opciones importantes las cuales son *WAN Edge List y Controllers*. Dentro de la primera opción se encuentran todos los equipos vEdge configurados y certificados y dentro de la segunda opción se encuentran todos los equipos vManage, vSmart y vBond que estén configurados y listos para certificar. El proceso de certificación se realizará primero en el vManage como se aprecia en la Figura 3.45.

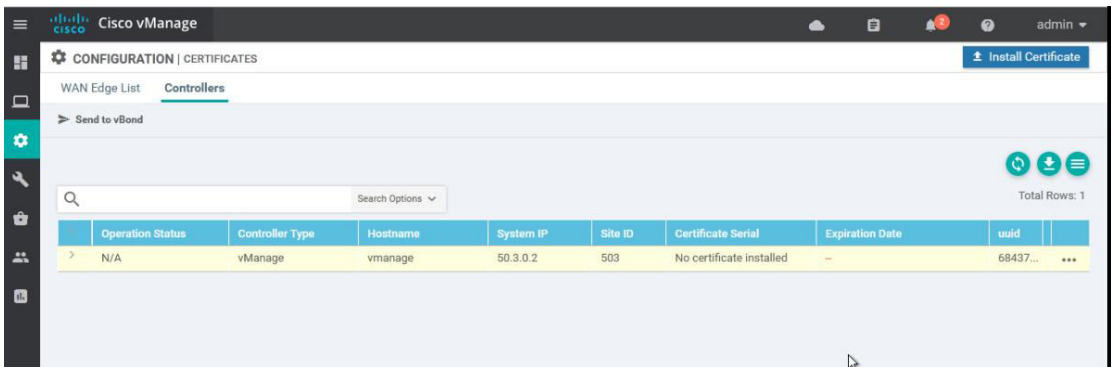


Figura 3.45 Equipo vManage listo para certificar

Para comenzar con la certificación de este equipo se debe generar una clave csr para esto en la misma interfaz gráfica se accede a más opciones del dispositivo vManage y se utiliza la opción "*generate CSR*" como se aprecia en la Figura 3.46.

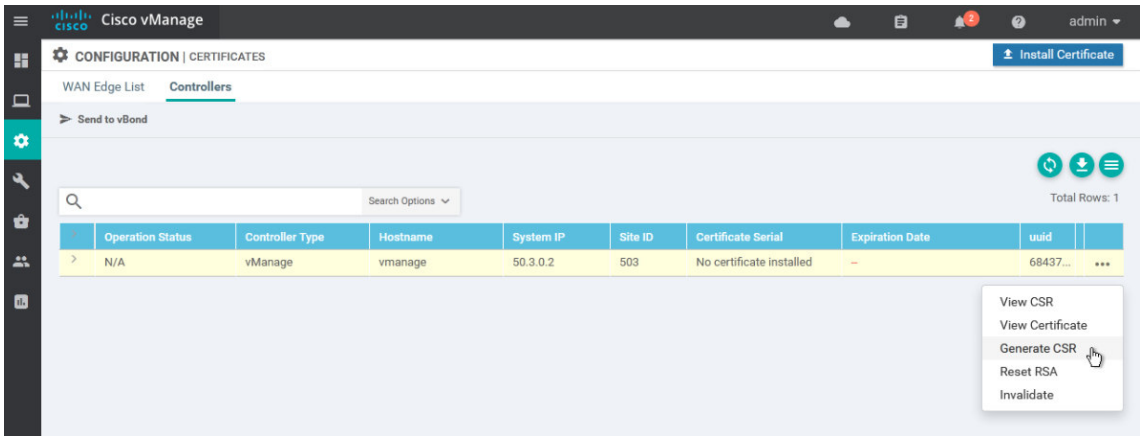


Figura 3.46 Generación de CSR vManage

La clave CSR ayudará a que se ejecute de manera correcta un certificado de tipo SSL motivo por el cual esta clave la cual es de tipo público deberá ser copiada al equipo vManage. La clave para este equipo se muestra en la Figura 3.47.

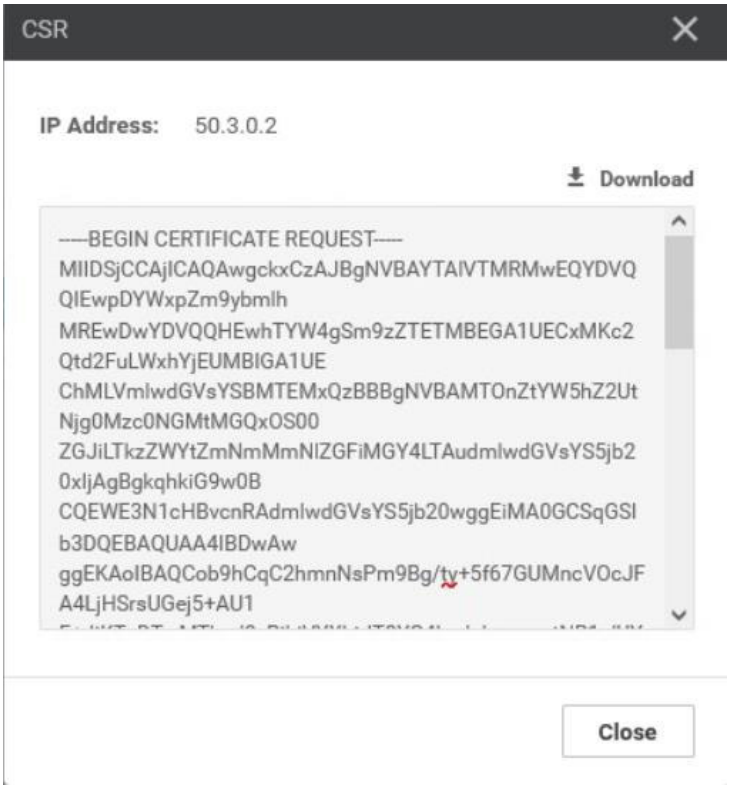


Figura 3.47 Certificado CRS vManage

Con la clave CRS lista se accede a la terminal de comandos dentro del equipo *vManage,* y por medio del uso del comando “vim vManage_csr”, se accede al editor de texto dentro del cual se colocará la clave CSR, previamente copiada desde la interfaz gráfica e ingreso a este archivo. Así como la colocación de la clave se observan en la Figura 3.48 y la Figura 3.49 respectivamente.

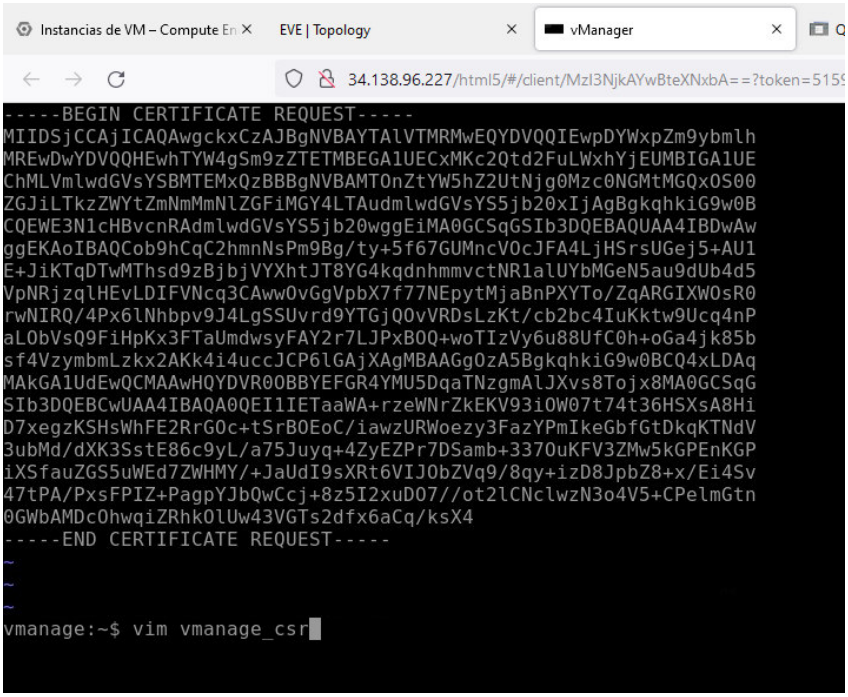


Figura 3.48 Procedimiento para el ingreso de CRS en vManage

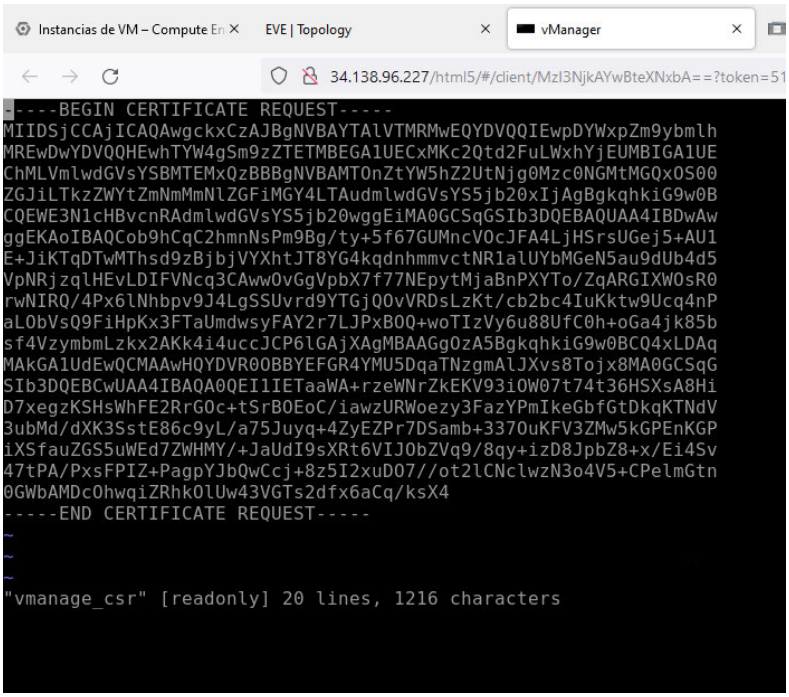


Figura 3.49 Ingreso de CRS en vManage

A continuación, se procede a verificar que estos archivos se crearon de manera exitosa dentro del directorio raíz por medio del comando “ls”. Se debe verificar los siguientes archivos:

- ROOTCA.key
- ROOTCA.pem
- Archive_id_rsa.pub
- Vmanage_csr

Una vez verificados los archivos se procede a que el usuario root acceda a esta clave privada esto se realiza haciendo uso del comando “openssl x500 –req –in vmanage_csr \”, esto se puede apreciar en la Figura 3.50.

```
vmanage:~$
vmanage:~$ ls
ROOTCA.key  ROOTCA.pem  archive_id_rsa.pub  vmanage_csr
vmanage:~$ openssl x509 -req -in vmanage_csr \
> -CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \
> -out vmanage.crt -days 2000 -sha256
Signature ok
subject=/C=US/ST=California/L=San Jose/OU=sd-wan-lab/O=Viptela LLC/CN=vmanage-6843744c-0d19-4d
bb-93ef-fcf2cedab0f8-0.viptela.com/emailAddress=support@viptela.com
Getting CA Private Key
vmanage:~$
```

Figura 3.50 Acceso de root a clave privada

A continuación, se procede a verificar los archivos dentro del directorio raíz para constatar que efectivamente fueron creadas las claves y que las mismas se encuentren disponibles para el administrador. Los archivos que deben existir son los siguientes, como se aprecia en la Figura 3.51.

- ROOTCA.key
- ROOTCA.pem
- Archive_id_rsa.pub
- Vmanage_csr
- Vmanage.crt

```
vmanage:~$ ls
ROOTCA.key  ROOTCA.srl          vmanage.crt
ROOTCA.pem  archive_id_rsa.pub  vmanage_csr
vmanage:~$
```

Figura 3.51 Comprobación crt y csr de archivos en vManage

El siguiente paso a realizar es acceder a la última clave de validación por medio del uso del comando “cat vmanage.crt” para desplegar la clave generada y posteriormente esta

clave instalarla en los certificados de la interfaz gráfica, la clave se puede observar en la Figura 3.52 a continuación

Figura 3.52 Clave generada para vManage

Con la clave lista se debe ingresar a la interfaz gráfica. En el apartado de “aplicaciones > certificados” se debe seleccionar el equipo en el que se esté trabajando en este caso el equipo es vManage y acto seguido se debe seleccionar la opción de instalar certificado y colocar ahí la clave previamente generada como se muestra en la Figura 3.53.

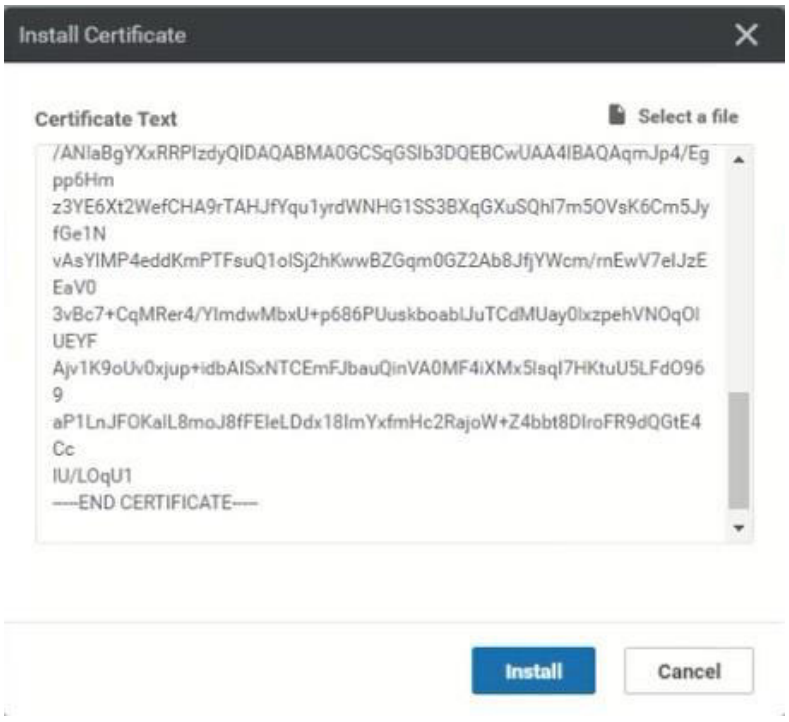


Figura 3.53 Instalación de certificado vManage

Una vez realizada esta acción se debe esperar un corto periodo de tiempo para poder verificar que en efecto el certificado fue instalado correctamente y el equipo se encuentra operacional y listo para ser usado, esto se aprecia en la Figura 3.54.

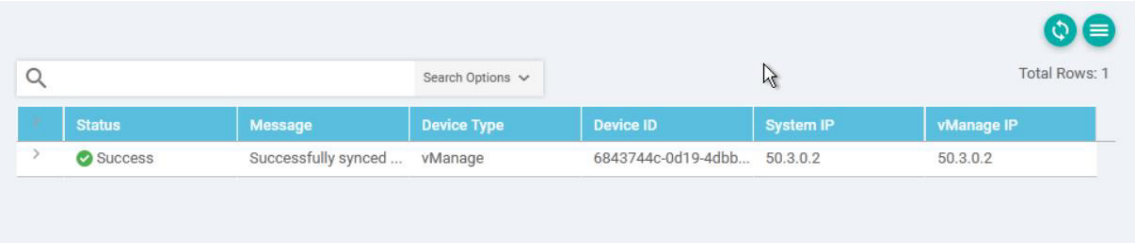


Figura 3.54 Instalación correcta de certificado vManage

A continuación, se procede a ingresar el equipo vSmart, para ello se debe agregar este dispositivo dentro de la interfaz gráfica. En el apartado de "configuración > dispositivos" se debe seleccionar la opción añadir controlador y seleccionar el equipo que se desea integrar. Para completar esta tarea el sistema solicitará el ingreso de la dirección IP previamente configurada que para el dispositivo vSmart es la 200.1.1.3/24 y las contraseñas de este equipo que serán las contraseñas por defecto es decir tanto usuario como contraseña será "*admin*". Con esto ya se puede añadir el dispositivo para poder generar las claves respectivas, esta adición se observa en la Figura 3.55.

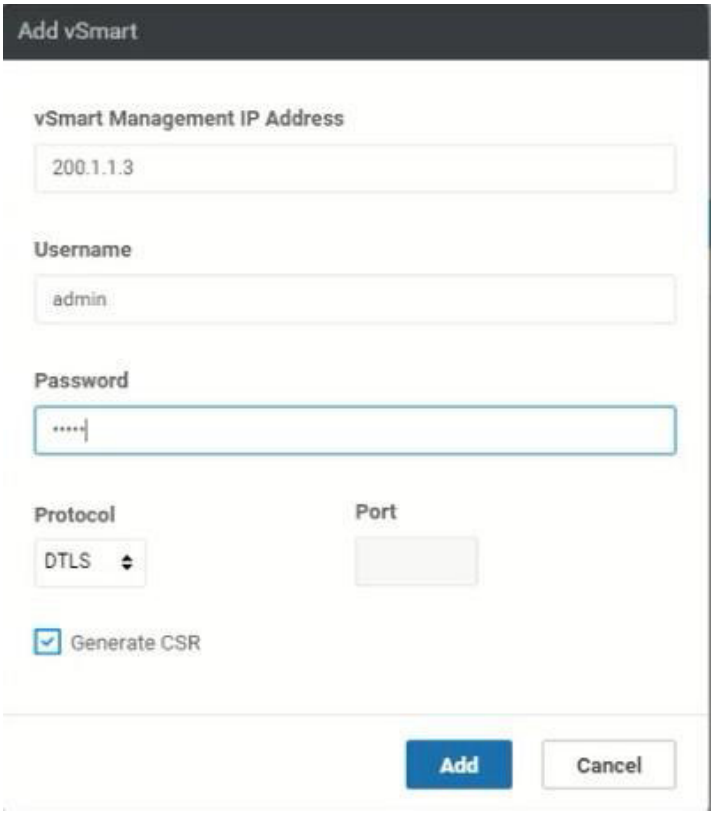


Figura 3.55 Ingreso de dispositivo vSmart en interfaz gráfica

Para poder añadir el equipo vBond en la interfaz gráfica se deben desactivar todas las comunicaciones tipo VPN esto con el fin de poder generar las claves sin que las mismas interfieran con la encriptación que se lleva a cabo dentro de estos túneles. Al finalizar con las certificaciones se deben levantar todas las comunicaciones VPN para mantener un canal seguro de comunicación, para poder realizar esta acción se deben utilizar los siguientes comandos:

- Config
- VPN0
- Interface ge0/0
- No tunnel-interface
- Commit and-quit

El procedimiento se sigue ingresando primero a las configuraciones del router para posteriormente ingresar a la conexión VPN0 por defecto y accediendo a la interfaz que establece la comunicación de ese router con el resto de la red. Posteriormente bajar todas las conexiones de tipo túnel y de ese modo poder realizar las certificaciones respectivas como se muestra en la Figura 3.56.

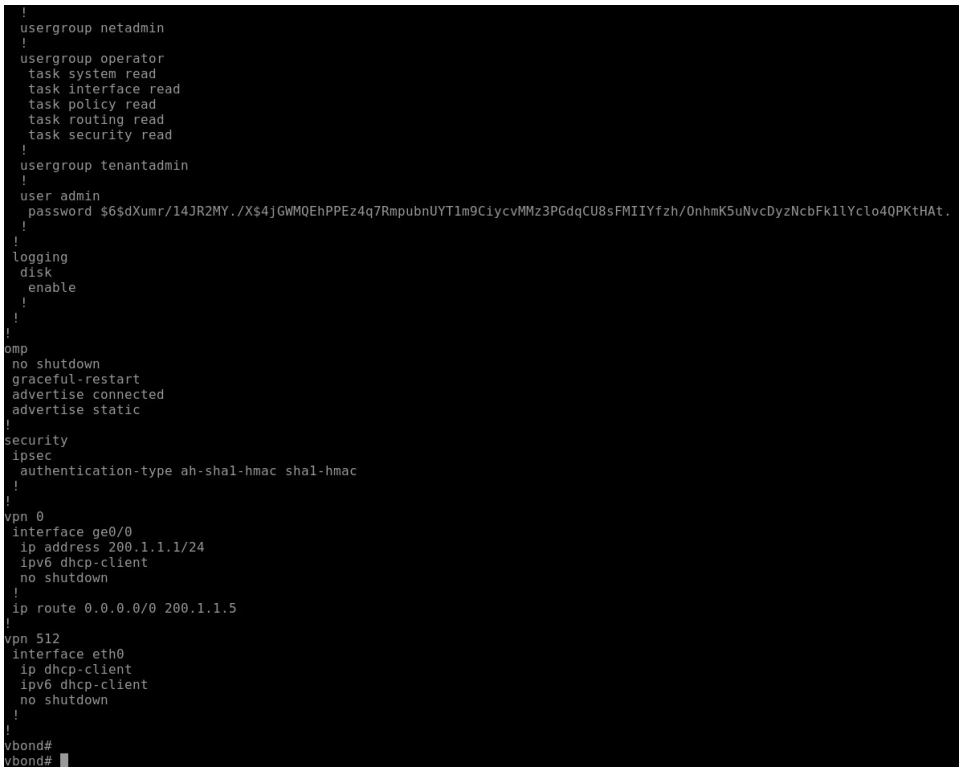


Figura 3.56 Desactivación de túneles VPN

Con las comunicaciones de tipo VPN desactivadas se procede a confirmar que dentro de la interfaz gráfica conste el equipo vSmart al cual se desea realizar los certificados esto se muestra en la Figura 3.57.

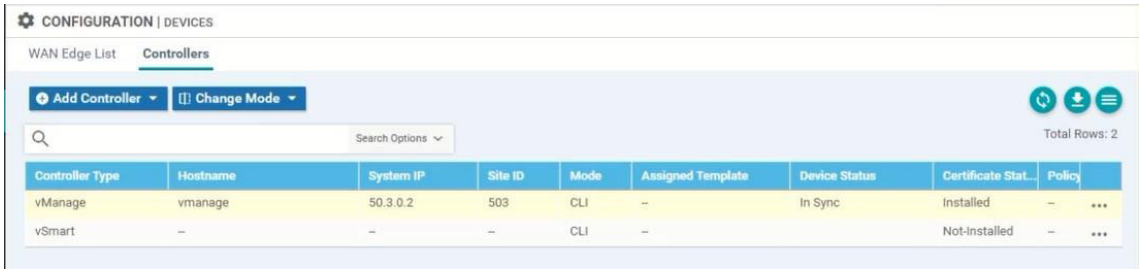


Figura 3.57 Listado de equipos disponibles en interfaz gráfica

Para poder realizar estos certificados de manera continua se añade también el equipo vBond de la misma manera que se añadió el equipo vSmart. Es decir, en el apartado de añadir controlador se selecciona el equipo vBond y se coloca los parámetros solicitados por el sistema, la dirección IP de este equipo es la 200.1.1.1. De igual manera que los demás equipos el usuario y contraseña serán “admin” como se muestra en la Figura 3.58.

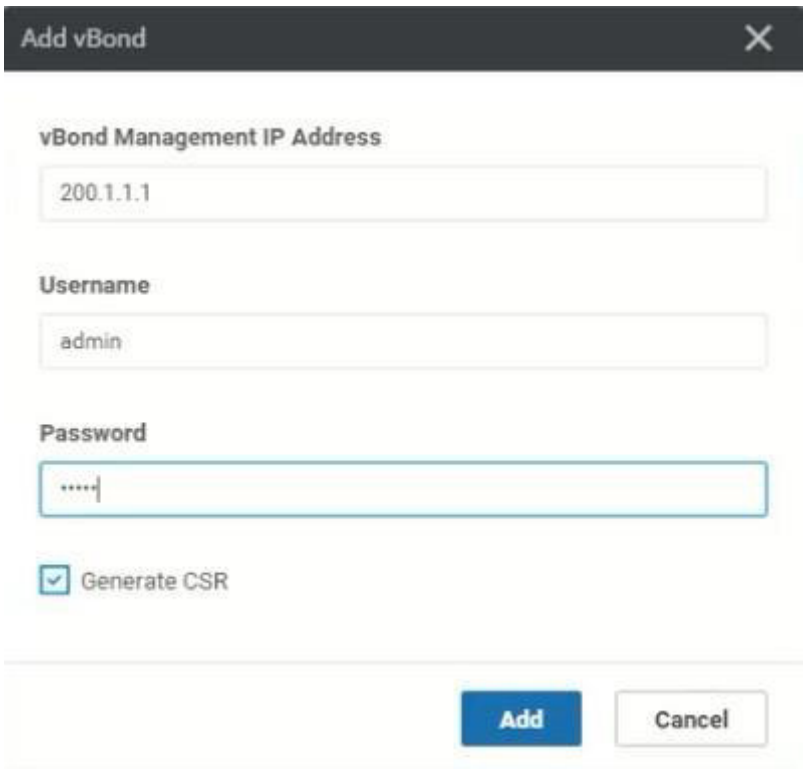


Figura 3.58 Ingreso de dispositivo vBond en vManage

Con todos los campos llenos y al añadir el equipo, se procede a confirmar que conste dentro de la interfaz gráfica en el apartado de dispositivos como se muestra en la Figura 3.59.

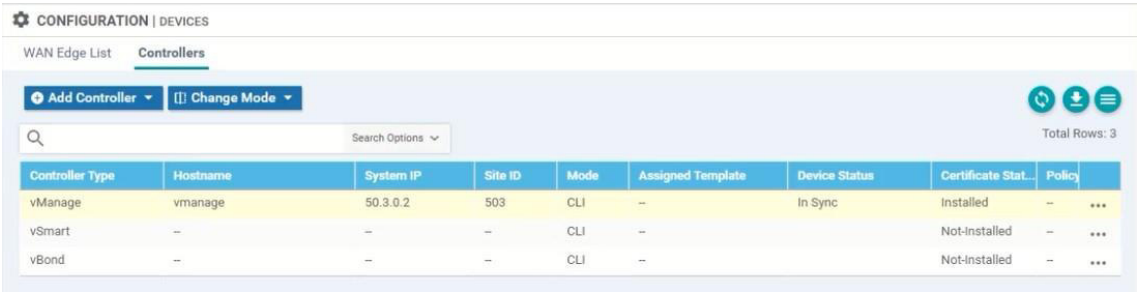


Figura 3.59 Listado de equipo vBond disponible en interfaz gráfica

Una vez que se han confirmado que todos los equipos están siendo reconocidos por la interfaz gráfica de vManage se accede al apartado de “configuración > certificados” y dentro de los mismos se despliegan los equipos. Así como el certificado de vManage previamente realizado como se muestra en la Figura 3.60.

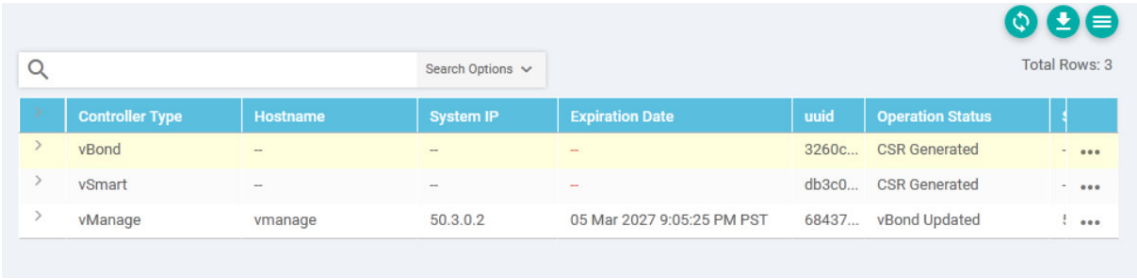


Figura 3.60 Listado de equipos listos a certificar

El primer dispositivo a certificar será vBond y de igual manera que vManage se procede a como primer paso generar la clave CSR en las opciones del equipo vBond como se aprecia en la Figura 3.61.

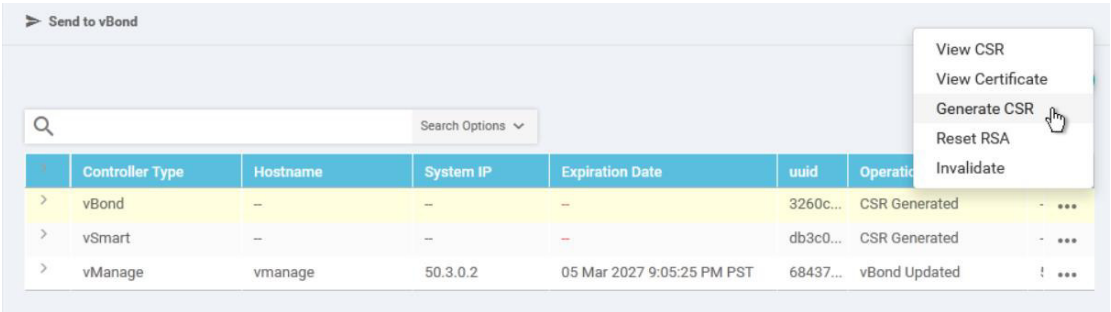


Figura 3.61 Generación de clave CSR de vBond

A continuación, se desplegará la clave CSR correspondiente al equipo vBond esta clave deberá ser copiada dentro del equipo vManage para poder de este modo posteriormente generar el archivo “vbond.crt” y poder instalar con dicha clave el certificado en el equipo. La clave CSR se muestra a continuación en la Figura 3.62.

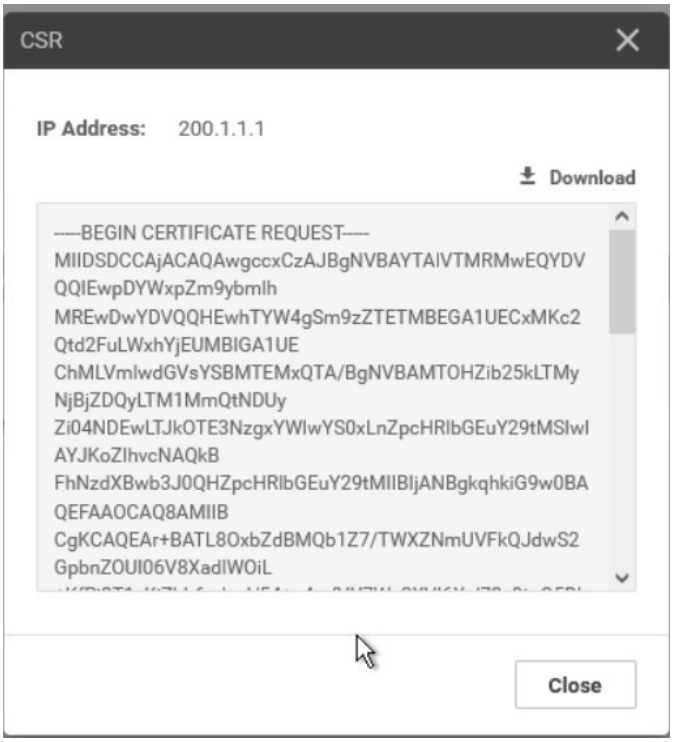


Figura 3.62 Clave CSR vBond

Con la clave CSR lista se accede al dispositivo vManage dentro del cual por medio del uso del comando “vim vbon_csr” se accede a un archivo dentro del cual se coloca la clave CSR. Como se aprecia en la Figura 3.63 y Figura 3.64.

Figura 3.63 Proceso para ingreso de certificado CSR vBond en equipo vManage

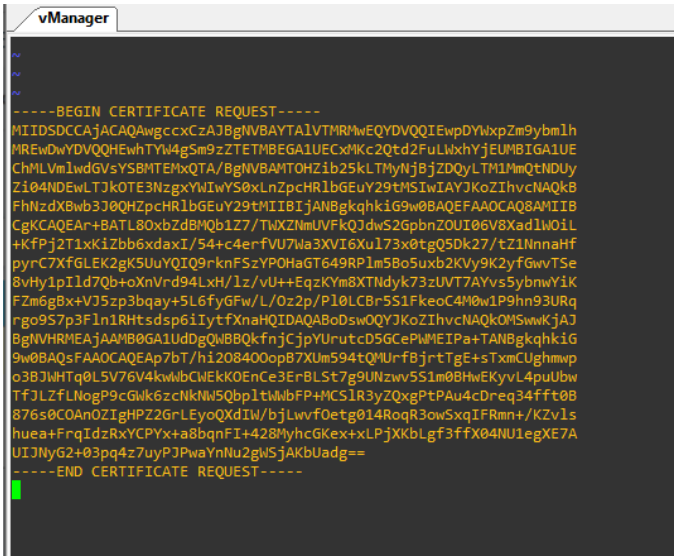


Figura 3.64 Ingreso de certificado CSR vBond en equipo vManage

Para que el usuario root pueda validar estas claves privadas con su propia clave almacenada en ROOTCA se hace uso del comando “openssl x509 –req –in vbond_csr”. De este modo cuando el usuario raíz valide la clave se generará un nuevo archivo llamado vbond.crt dentro del cual se encuentra la clave que será usada posteriormente en la certificación. Para confirmar que esta clave fue generada se utiliza el comando “ls”, los archivos dentro del directorio se aprecian en la Figura 3.65 y son los siguientes:

- ROOTCA.key
- ROOTCA.pem
- Archive_id_rsa.pub
- Vmanage_csr
- Vmanage.crt
- Vbond.crt
- Vbond_csr

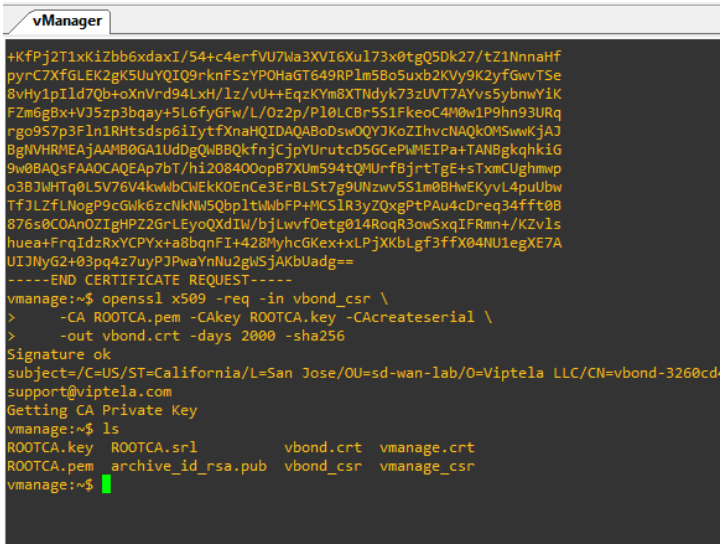


Figura 3.65 Verificación de archivos csr y crt de vBond en vManage

Una vez verificado que el archivo “vbond.crt” se creó de manera exitosa se procede a abrirlo mediante el comando “cat vim vbond.crt”. Posteriormente esta clave se copia hacia la instalación del certificado en la interfaz gráfica de vManage, esta clave se aprecia en la Figura 3.66.

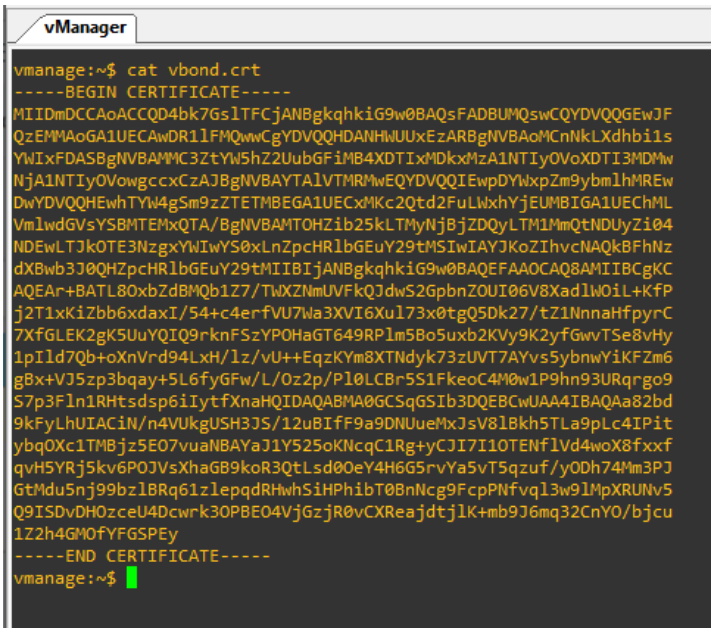


Figura 3.66 Despliegue de certificado para vBond

Dentro de la interfaz gráfica de vManage y en apartado de certificados se procede a seleccionar el equipo vBond e instalar el certificado como se lo realizó en el equipo vManage este procedimiento se muestra en la Figura 3.67.

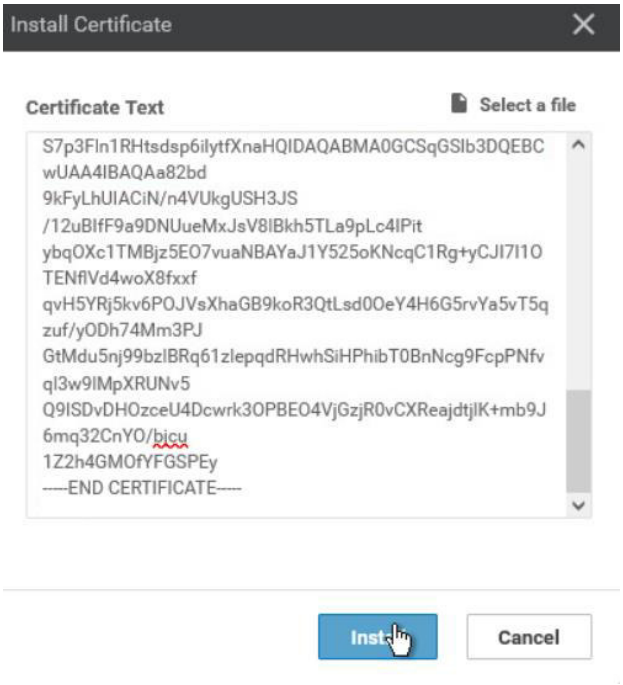


Figura 3.67 Instalación de certificado vBond

Después de esperar un corto periodo de tiempo se puede observar que el certificado fue instalado con éxito dentro de la interfaz gráfica de vManage como se muestra en la Figura 3.68.

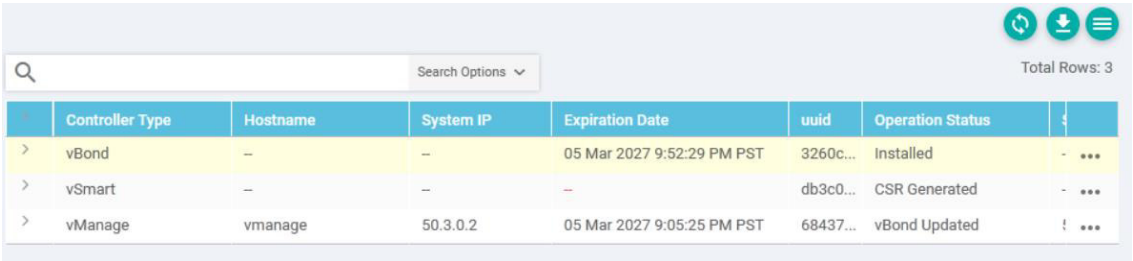


Figura 3.68 Verificación de instalación de certificado vBond

Del mismo modo para instalar el certificado del equipo vSmart se procede a realizar el mismo procedimiento, como primer paso se genera la clave CSR la misma que será copiada al equipo vManage como se muestra en la Figura 3.69.

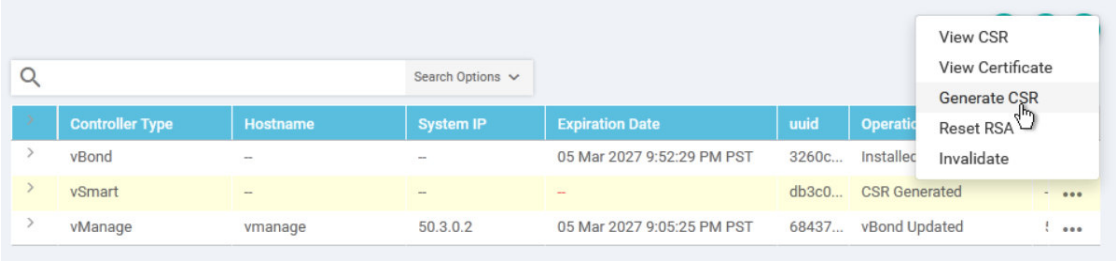


Figura 3.69 Generación de certificado CSR vSmart

Una vez se obtenga el certificado se debe confirmar que la dirección IP coincida con la del equipo vSmart dirección que fue confirmada previamente dentro de vManage esta dirección es la 200.1.1.3/24 y la clave CSR se observa en la Figura 3.70.

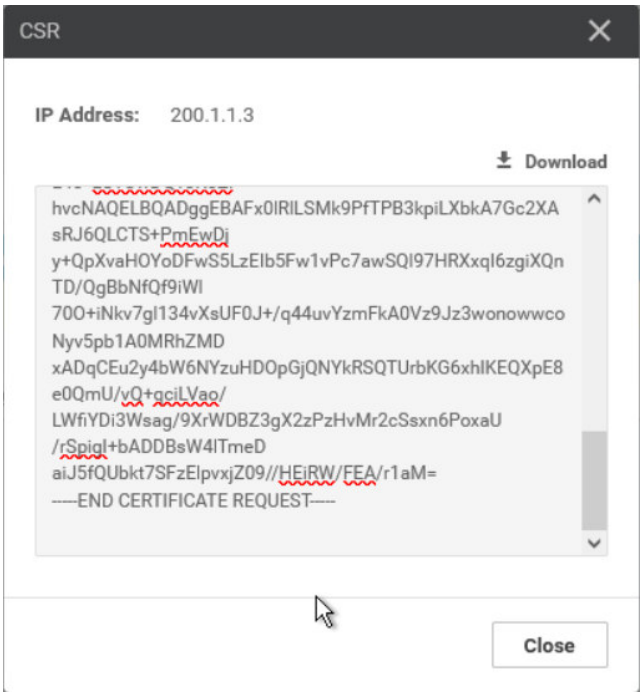


Figura 3.70 Certificado CSR vSmart

A continuación, se procede a abrir el archivo donde se copia esta clave CSR dentro del equipo vManage esto por medio del uso del comando “vim vsmart_csr” como se aprecia en la Figura 3.71.

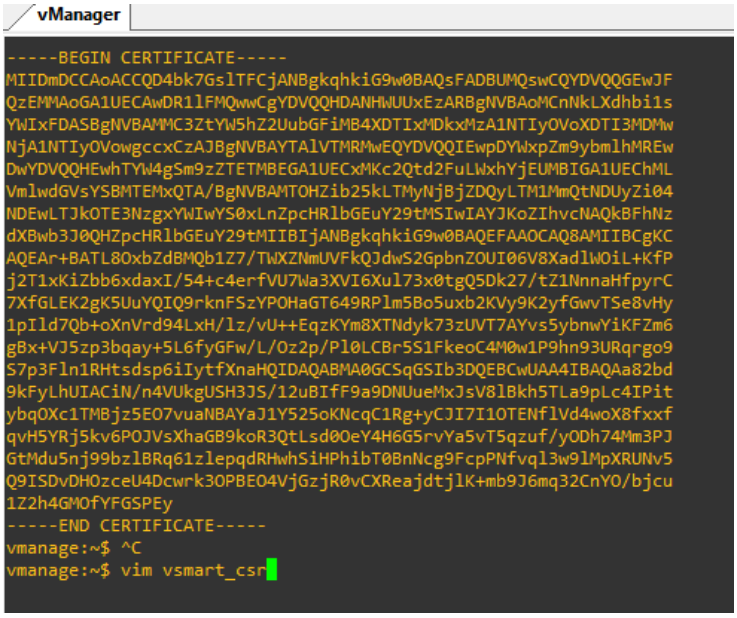


Figura 3.71 Procedimiento para ingreso de certificado vSmart en vManage

Dentro de este archivo se coloca la clave CSR la misma que será validada posteriormente con la clave en ROOTCA dentro del usuario raíz. El archivo con la clave se observa en la Figura 3.72.

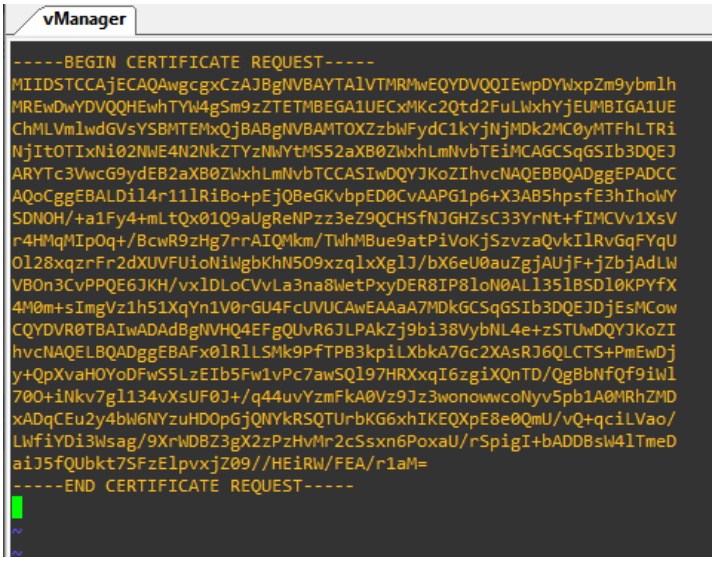


Figura 3.72 Ingreso de certificado vSmart en vManage

Del mismo modo que en los anteriores equipos esta clave también debe ser validada por el usuario raíz; para poder realizar esta acción se utiliza el comando “openssl x509 –req –in vsmart_csr”. Si la validación se realiza de manera exitosa se crea un archivo llamado vsmar.crt el cual será el que contenga el certificado que deberá ser copiado a la interfaz gráfica de vManage. Para verificar que este archivo se creó de manera correcta se usa el comando “ls” que se aprecia en la Figura 3.73 y los archivos que contiene son los siguientes:

- ROOTCA.key
- ROOTCA.pem
- Archive_id_rsa.pub
- Vmanage_csr
- Vmanage.crt
- Vbond.crt
- Vbond_csr
- Vsmart.crt
- Vsmart_csr

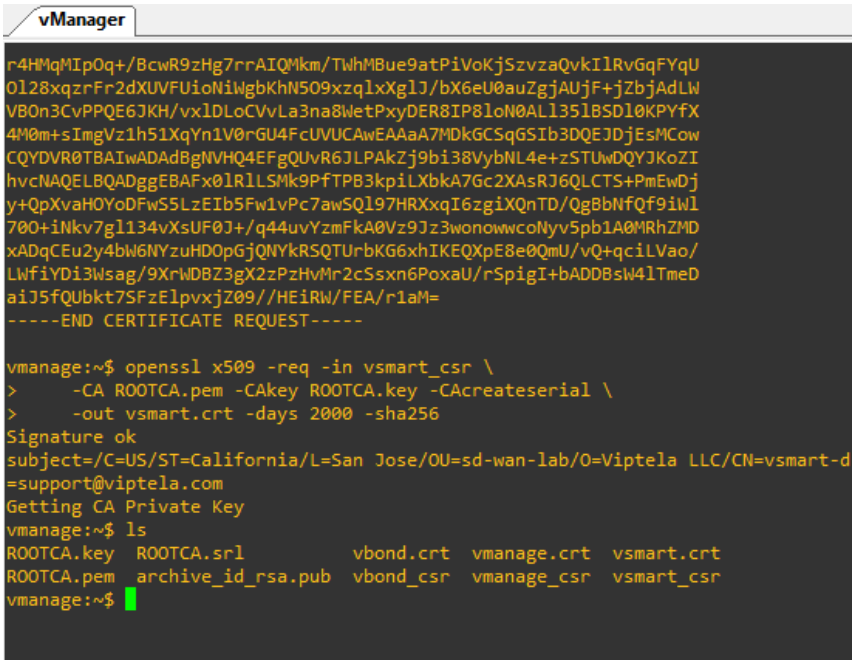


Figura 3.73 Verificación de archivos csr y crt de vSmart en vManage

Si el archivo vsmart.crt se creó correctamente se procede a verificar su contenido para copiarlo a la interfaz gráfica de vManage y de este modo poder obtener el certificado, el contenido de este archivo se observa a continuación en la Figura 3.74.

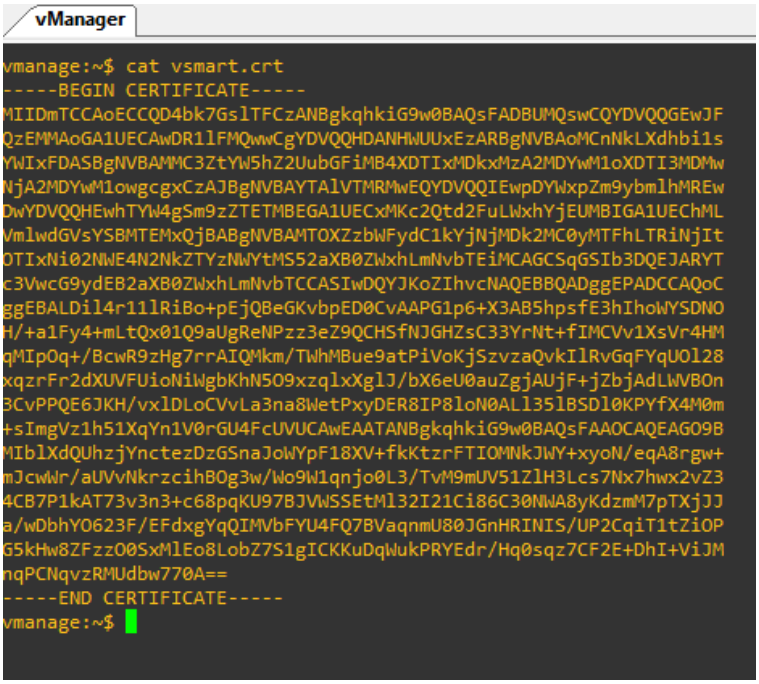


Figura 3.74 Generación de certificado para vSmart

El siguiente paso consiste en la interfaz gráfica de *vManage*, en el apartado de certificados se selecciona el equipo *vSmart* e instala el certificado haciendo uso de la clave copiada previamente como se muestra en la Figura 3.75.

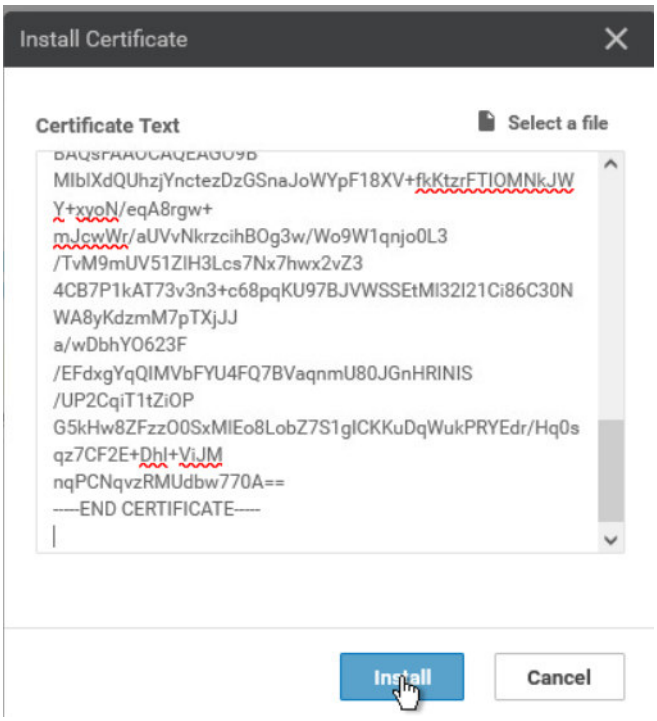


Figura 3.75 Ingreso de certificado vSmart

Después de esperar un corto periodo de tiempo en el apartado de "configuración > dispositivos" se verifica que los 3 equipos cuenten con los certificados instalados como se muestra en la Figura 3.76.

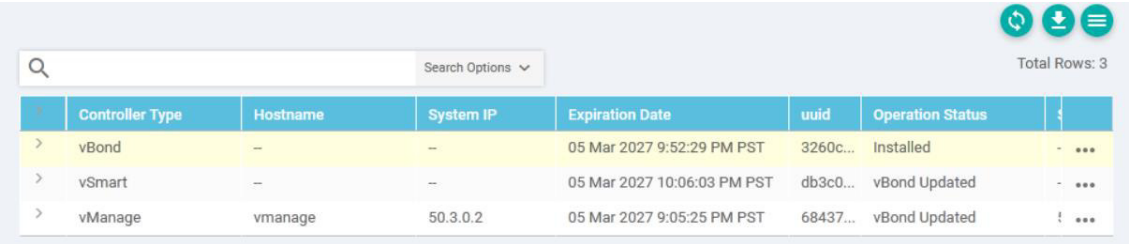


Figura 3.76 Comprobación de instalación de certificado vSmart

Como se explicó previamente la comunicación por VPN debe ser restablecida para tener conexiones seguras con el resto de la red por lo que dentro del equipo central vManage se procede a levantar esta comunicación haciendo uso de los siguientes comandos:

- Config
- VPN0

- Interface eth0
- Tunnel-interface
- Commit and-quit

Esta acción se lleva a cabo en los equipos vSmart, vEdge, vBond y al restablecer esta comunicación todos los routers podrán tener conexiones seguras entre sí. Como se muestra en las Figura 3.77, Figura 3.78, Figura 3.79 respectivamente

Figura 3.77 Restablecimiento de comunicación mediante túneles VPN parte 1

Figura 3.78 Restablecimiento de comunicación mediante túneles VPN parte 2

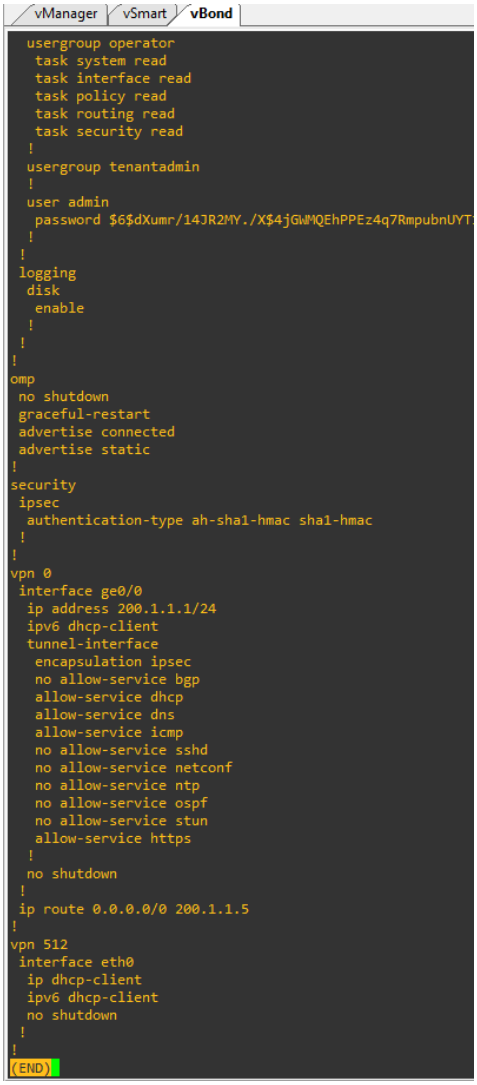


Figura 3.79 Restablecimiento de comunicación mediante túneles VPN parte 3

Para verificar que todo se encuentra operando de manera correcta se revisan los certificados dentro de la interfaz gráfica del equipo central vManage como se muestra en la Figura 3.80.

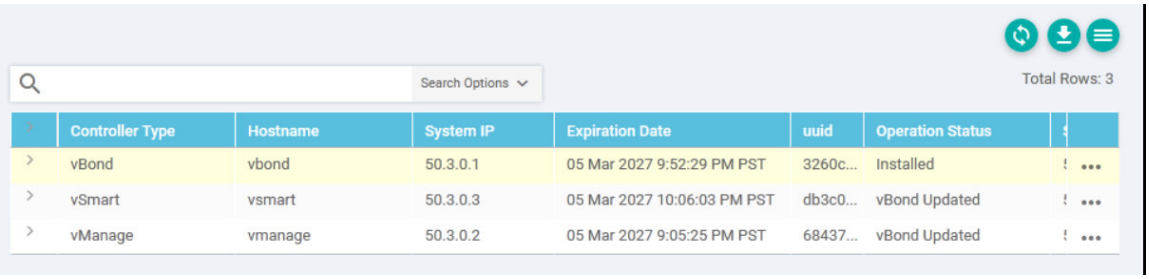


Figura 3.80 Equipos certificados dentro de la interfaz gráfica

Con los certificados de los equipos vManage, vBond y vSmart correctamente instalados se procede a configurar el equipo vEdge para poder certificarlo. La configuración de este equipo se la realiza con los siguientes comandos:

- Config
- System
- Host-name vEdge-1
- System-ip 50.3.0.4
- Site-id 503
- Admin-tech-on-failure
- Organization-name “sd-wan-lab”
- Vbond 200.1.1.1

El primer paso es ingresar a las configuraciones del Sistema dentro del equipo para posteriormente nombrarlo haciendo uso del comando “*host-name*”. Acto seguido se procede a asignarle una dirección para que pueda ser reconocido dentro del área de trabajo la dirección de operación del equipo es la 50.3.0.4 y se asignará el número de área correspondiente de trabajo que para este caso será de 503. El comando “*admin-tech-on-failure*” sirve para crear un archivo dentro del cual se guardará toda la configuración realizada en el equipo, así como el estado de las conexiones esto con el fin de que al presentarse un error o falla en la red el administrador puede ingresar a este archivo para revisar el estado del equipo y la red. Adicionalmente se denomina a la organización que pertenece que para este proyecto será de “SD-WAN” para finalmente colocar la dirección de vBond para obtener conexión entre la red.

Adicionalmente se debe configurar las conexiones mediante VPN para tener comunicación segura dentro de la red; los comandos necesarios para realizar esta acción son:

- VPN0
- ip route 0.0.0.0/0 200.1.1.5
- Interface ge0/0
- Ip add 200.1.1.4/24
- No shutdown

El primer paso para configurar la VPN es entrar a la interfaz por medio de la cual el equipo está conectado a toda la red. Dentro de la misma se configura la dirección IP correspondiente al equipo en este caso la dirección es 200.1.1.4/24 y una vez hecho

esto se procede a guardar los cambios realizados con el comando “commit and-quit” como se aprecia en la Figura 3.81.

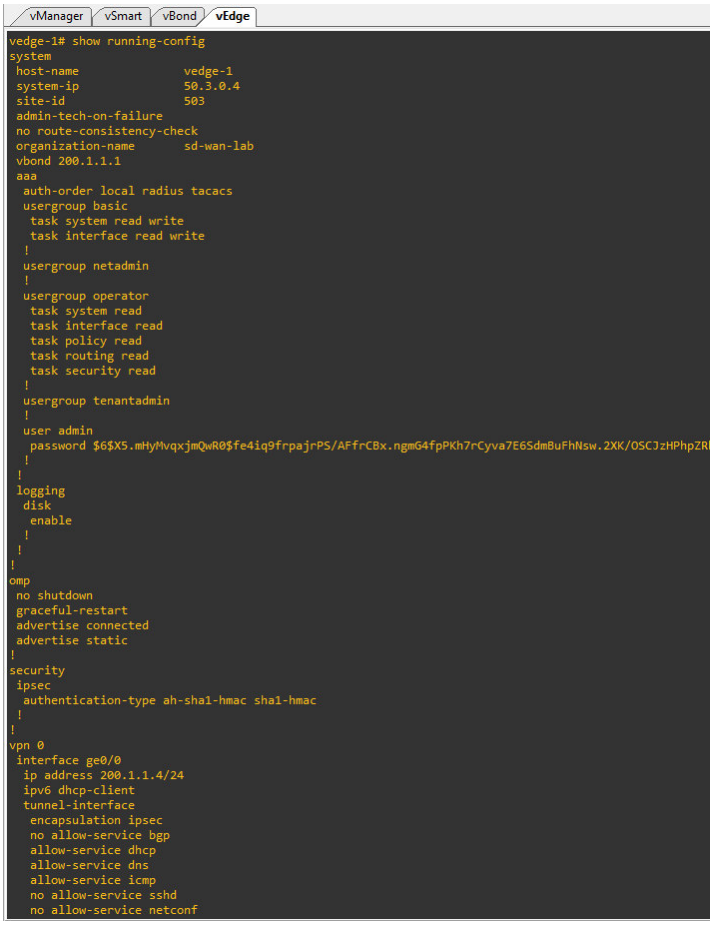


Figura 3.81 Configuración inicial equipo vEdge

Para realizar la certificación a este dispositivo es necesario acceder a la interfaz de comandos del router por medio del comando “vshell” y abrir la clave de usuario raíz que se encuentra almacenada en el archivo ROOTCA.pem. Posteriormente se copia esta clave hacia el mismo archivo para de este modo actualizarlo, la clave se muestra en la Figura 3.82.

Figura 3.82 Certificado root para vEdge

A continuación, se procede a ingresar a este archivo para poder actualizar la clave generada haciendo uso del comando “vi ROOTCA.pem” como se muestra en la Figura 3.83.

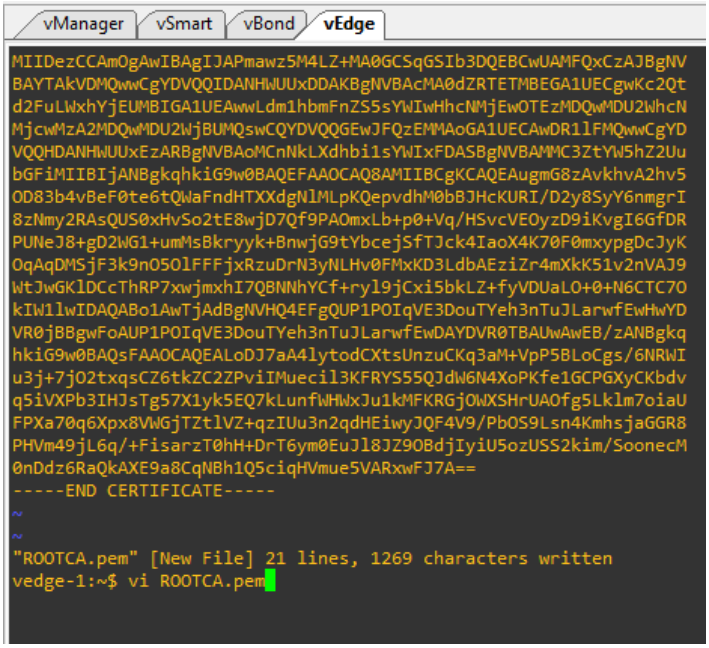


Figura 3.83 Ingreso al archivo de clave root

Dentro de este archivo se copia nuevamente el certificado generado para de este modo poder iniciarlo posteriormente, este certificado se muestra en la Figura 3.84.

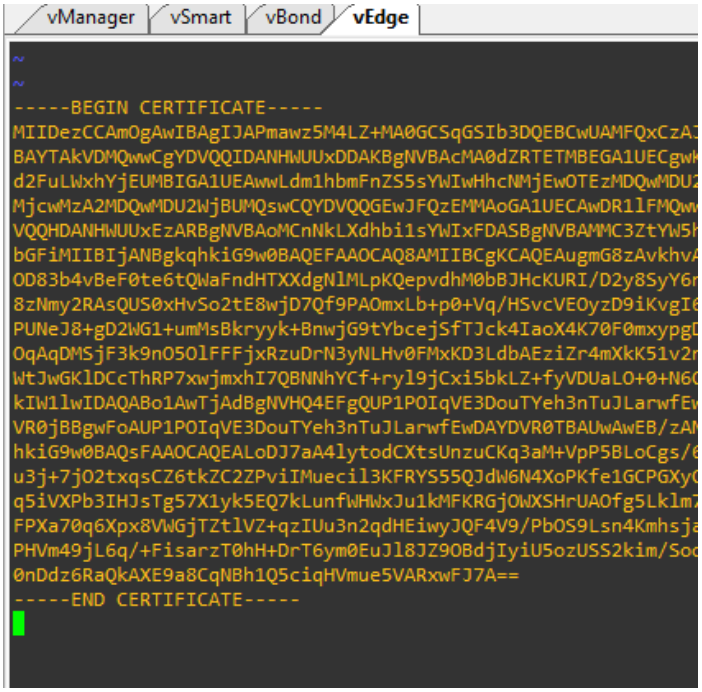


Figura 3.84 certificado de root para vEdge

Para verificar que todo se realizó correctamente se despliega nuevamente la clave haciendo uso del comando “cat” como se observa en la Figura 3.85 a continuación.

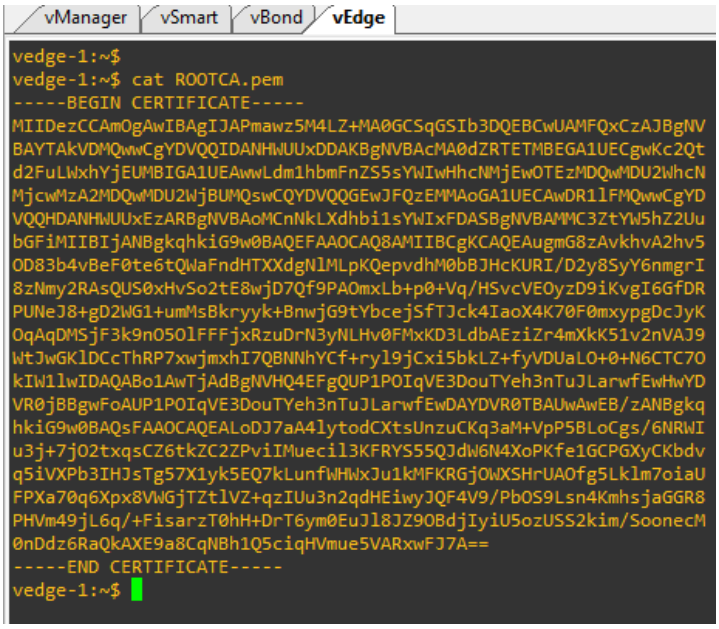


Figura 3.85 Despliegue del certificado root para vEdge

Finalmente, se procede a instalar el certificado dentro de vEdge haciendo uso del comando “request root-cert-chain install /home/admin/ROOTCA.pem”. Este comando buscará en el usuario admin el certificado previamente añadido y lo instalará en el

equipo dando como resultado que vEdge cuente con la certificación para el correcto funcionamiento, esta instalación se aprecia en la Figura 3.86.

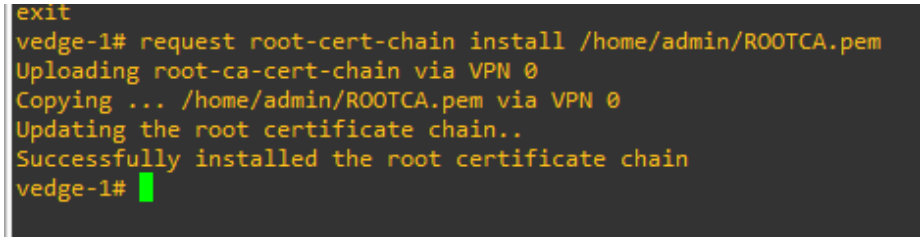


Figura 3.86 Verificación de instalación de certificado vEdge

Posteriormente, previo a generar el número serial correspondiente al equipo vEdge se procede a cargar el archivo de Cisco-Viptela con todos los equipos vEdge disponibles. Este archivo se puede conseguir solamente si se tiene una licencia educativa por parte de Cisco o si se ha adquirido el producto por completo. Para añadir esta lista se debe acceder al apartado de "*devices* > *upload wan edge list*" y se selecciona el archivo correspondiente como se muestra en la Figura 3.87.

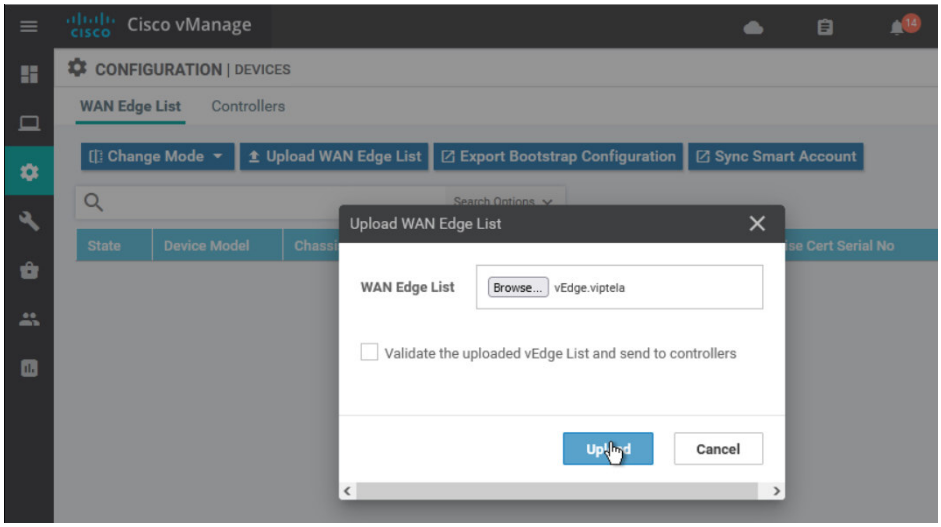


Figura 3.87 Ingreso de equipos vEdge

Una vez cargados los archivos de listado se procede a seleccionar uno de los equipos vEdge Cloud los cuales poseen un número de serie, así como se muestra en la Figura 3.88.

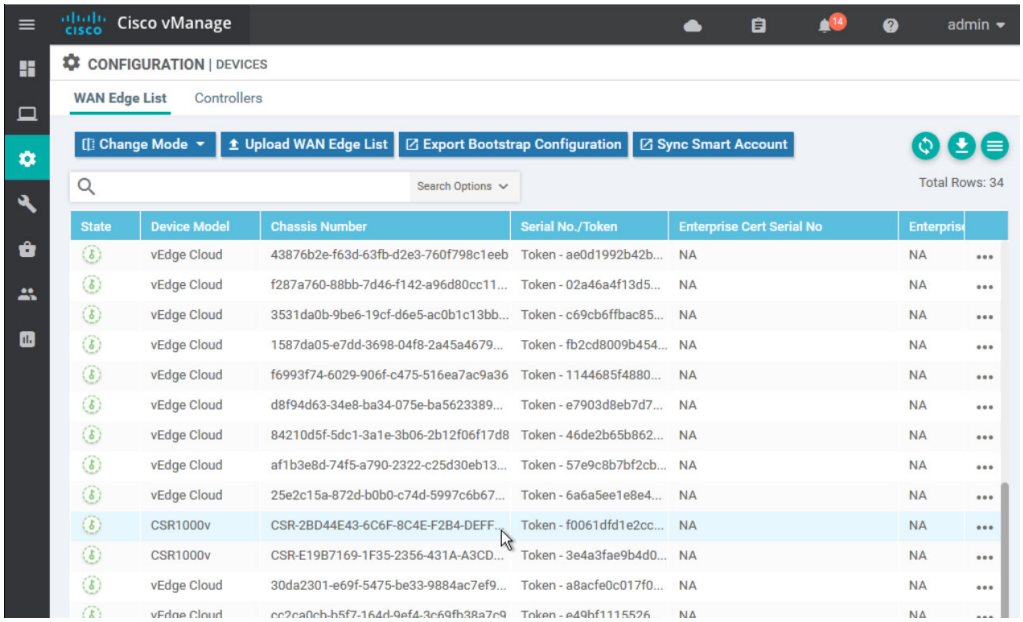


Figura 3.88 Listado de equipos vEdge Cloud

El siguiente paso es configurar que tipo de arranque tendrá este nodo, para este caso se utiliza la configuración de arranque a través de la nube o "*Cloud-Init*" como se muestra en la Figura 3.89.

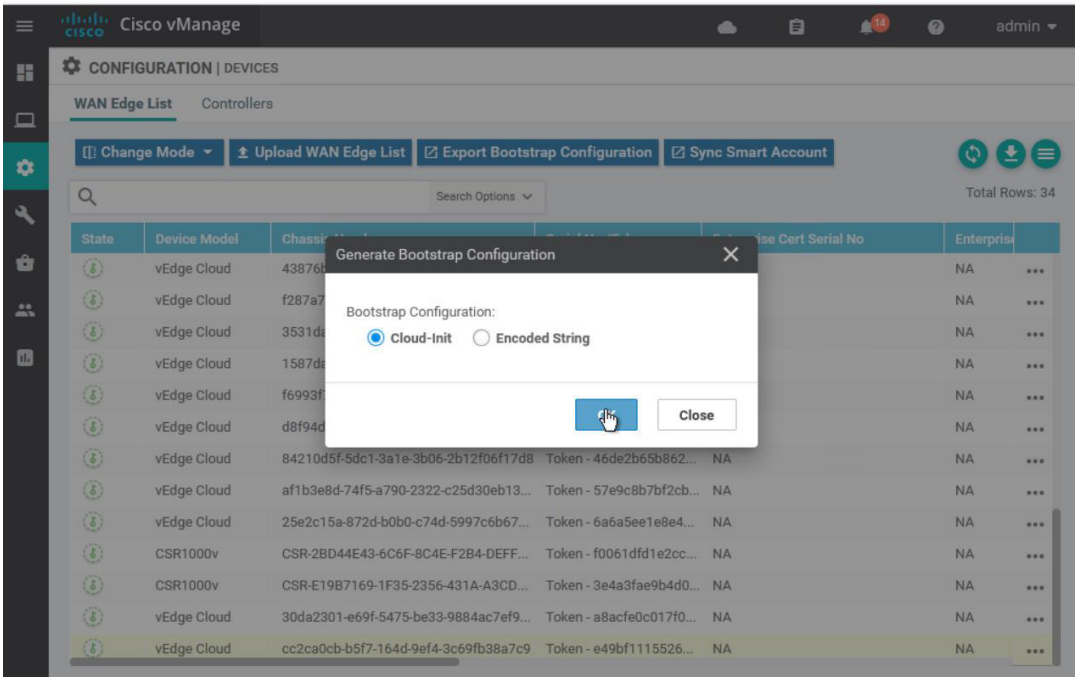


Figura 3.89 Configuración de arranque vEdge Cloud

Una vez que se acepte esta configuración se despliegan los valores tanto del código serial correspondiente al equipo como el número de identificación correspondiente al

mismo. Valores que se especifican en los apartados “uuid y otp” como se aprecia en la Figura 3.90.

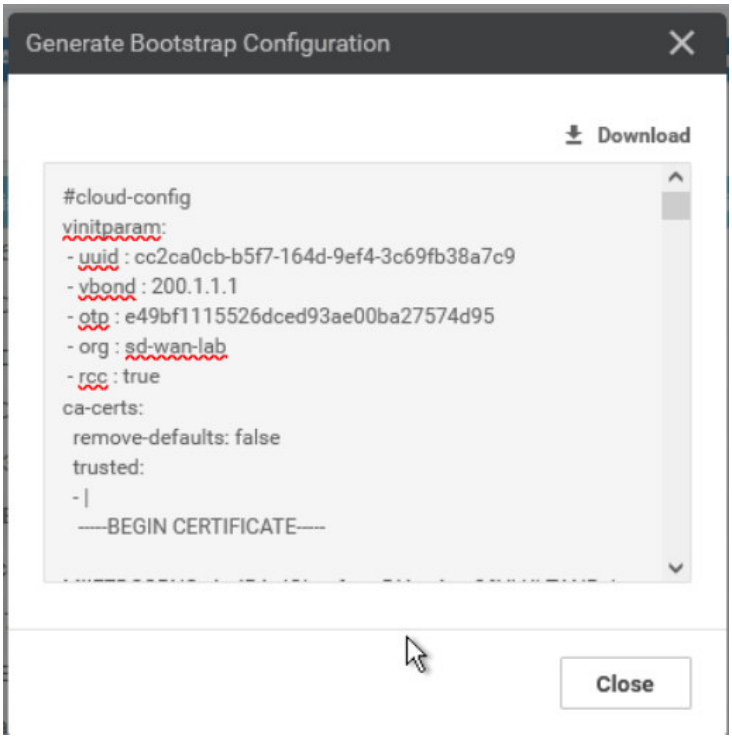


Figura 3.90 Código serial de vEdge cloud

Acto seguido se procede a ingresar esta codificación manualmente al equipo vEdge por medio del ingreso del siguiente comando como se muestra en la Figura 3.91.

- Request vEdge-cloud activate chassis-number “código serial” token “numeración de equipo”

```
!
vedge-1# request vedge-cloud activate chassis-number cc2ca0cb-b5f7-164d-9ef4-3c69fb38a7c9 token e49bf1115526dced93ae00ba27574d95
vedge-1#
```

Figura 3.91 Comando de activación vEdge

El procedimiento previamente mencionado se realiza para ambos equipos vEdge, a continuación, en la Figura 3.92 se muestra la configuración del segundo equipo vEdge que será enlazado en la red.

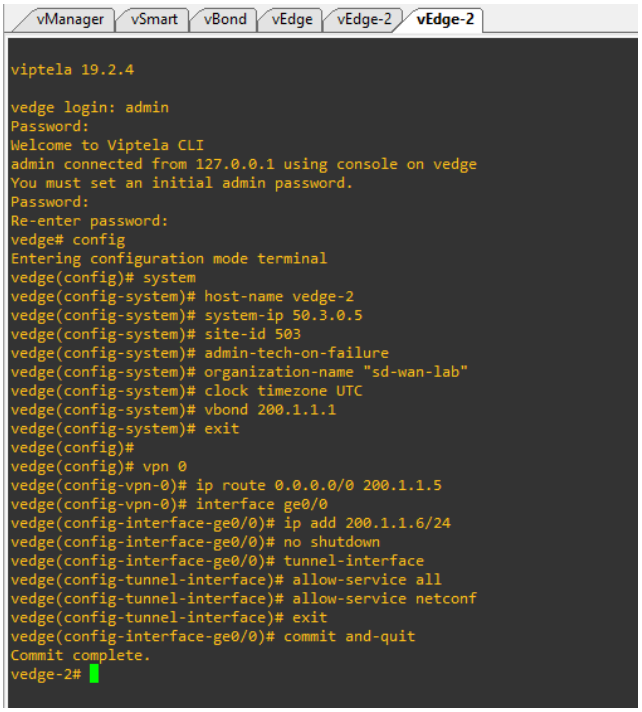


Figura 3.92 Configuración vEdge-2

Una vez activados ambos equipos vEdge se procede a la verificación de que todos los equipos se encuentren activos y con su respectivo número de serie como se muestra en la Figura 3.93.

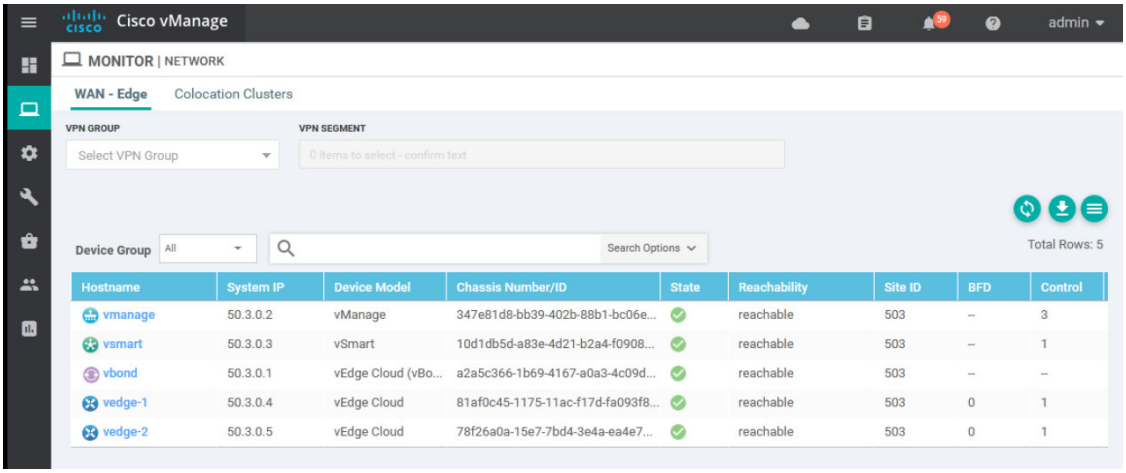


Figura 3.93 Estado de equipos SD-WAN

Adicionalmente, en la interfaz gráfica de vManage se comprueba que se encuentren enlazados todos los elementos de la red SDWAN como se aprecia en la Figura 3.94.

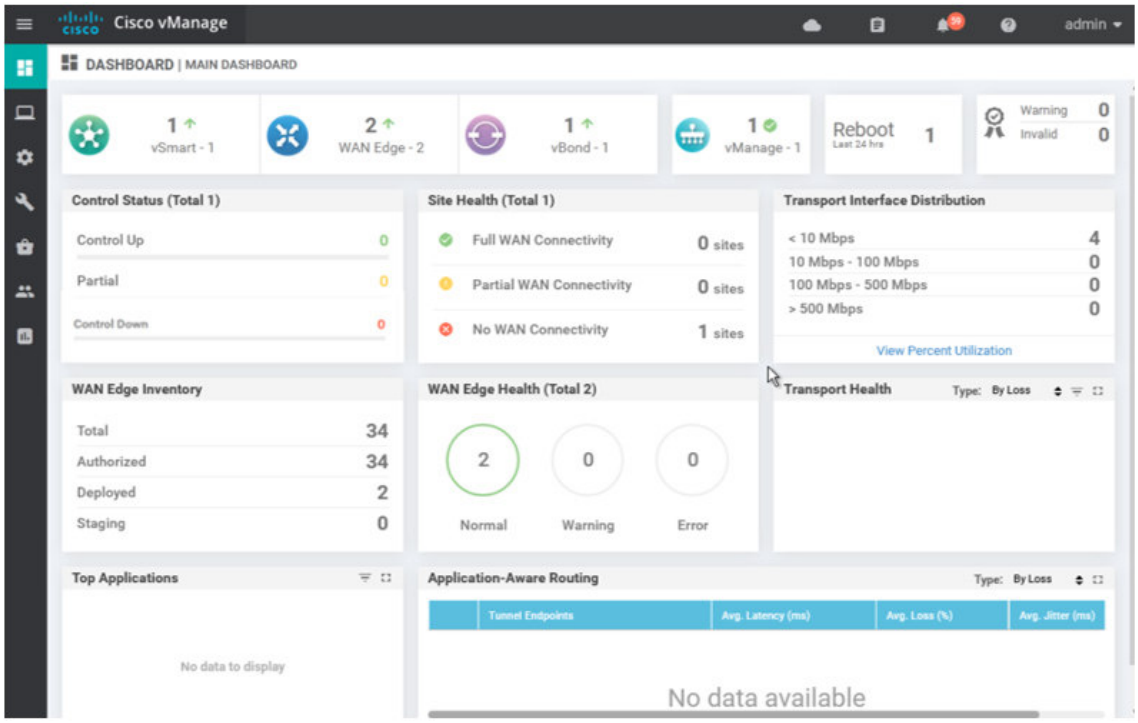


Figura 3.94 Dispositivos en Interfaz Gráfica

Finalmente, con los certificados instalados ya se pueden utilizar los equipos normalmente por lo que como resultado se tiene la topología presentada en la Figura 3.95 en donde se detallan todos los equipos. Así como la información más relevante sobre los mismos

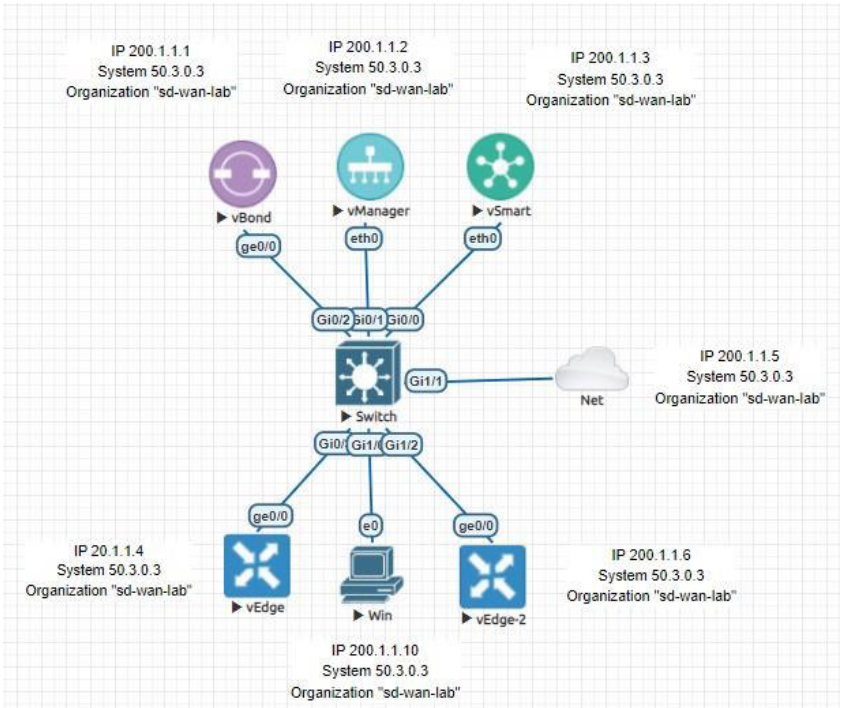


Figura 3.95 Topología SDWAN-CISCO

Configuración de red SDWAN mediante equipos Fortinet

Red SDWAN-OSPF

Para la configuración de una red que opere con comunicación por medio de SD-WAN en sus enlaces seriales se requerirán los siguientes dispositivos:

- 4 equipos FortiGate 5.6.1
- 7 equipos *switch* propietarios de Cisco
- 6 computadores *Virtual PCs* (VPCS)
- 1 nube de conexión hacia internet

El primer paso para la configuración de esta red es poder conocer el *Gateway* que se está utilizando en los equipos para poder realizar una salida a internet exitosamente. El procedimiento a realizarse consiste en conectar un equipo VPCS a la red *Network Address Translation* (NAT) dentro del simulador GNS3 y por medio del comando "ip dhcp" saber en qué red se está manejando el equipo real, de este modo todos los *gateways* que salgan desde los equipos FortiGate hacia internet deberán encontrarse en la red de NAT. Este procedimiento se muestra en la Figura 3.96 y Figura 3.97 respectivamente.

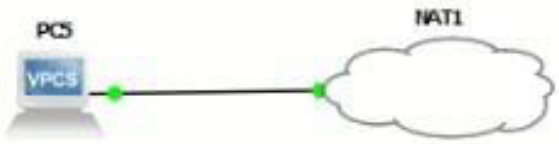


Figura 3.96 Conexión a NAT para verificación

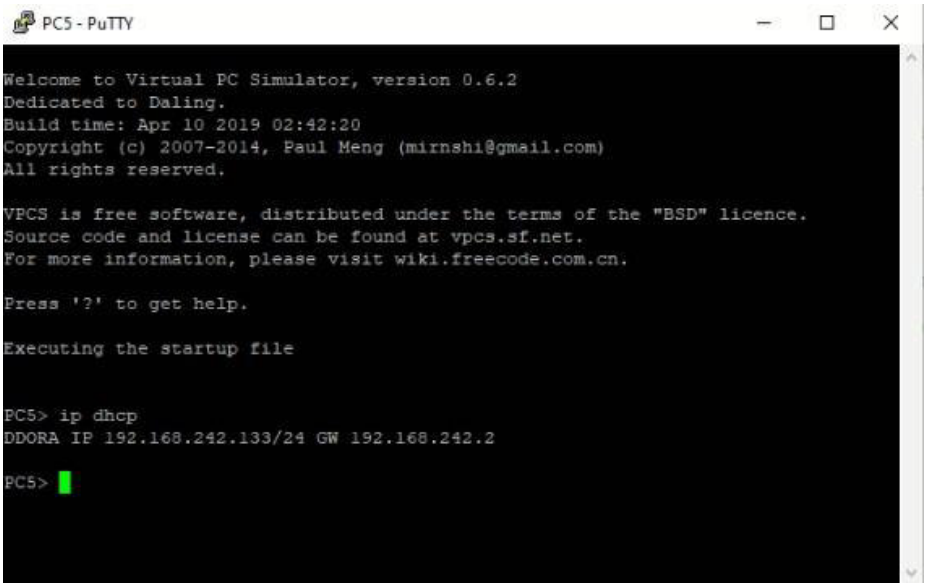


Figura 3.97 Verificación de la red conectada a Internet

Esta red adicionalmente funcionará con un enrutamiento dinámico por medio del protocolo OSPF. Esto permitirá las conexiones que se realicen en todos los dispositivos de la red, a continuación, en la Tabla 3.2 Direccionamiento Red SDWAN-OSPF se puede observar el listado de direcciones que se utilizaron para el establecimiento de esta red.

Tabla 3.2 Direccionamiento Red SDWAN-OSPF

TIPO	DIRECCIÓN
SERIAL 1	10.1.1.1/30
SERIAL 2	10.1.1.2/30
SERIAL 3	20.1.1.1/30
SERIAL 4	20.1.1.2/30
SERIAL 5	30.1.1.1/30
SERIAL 6	30.1.1.2/30
SERIAL 7	40.1.1.1/30
SERIAL 8	40.1.1.2/30
RED 1	10.10.10.0/24
RED 2	20.20.20.0/24
RED 3	30.30.30.0/24
RED 4	40.40.40.0/24
GATEWAY INTERNET RED 1	192.168.242.10/24
GATEWAY INTERNET RED 2	192.168.242.20/24
GATEWAY INTERNET RED 3	192.168.242.30/24
GATEWAY INTERNET RED 4	192.168.242.40/24

Una vez establecidas las direcciones que tendrán cada uno de los enlaces se procede a la implementación de la red. En la Figura 3.98 se muestran tanto los dispositivos utilizados, así como los enlaces y números de puerto a los cuales se encuentran conectados los equipos, esto es de vital importancia conocer para la posterior configuración en los equipos FortiGate.

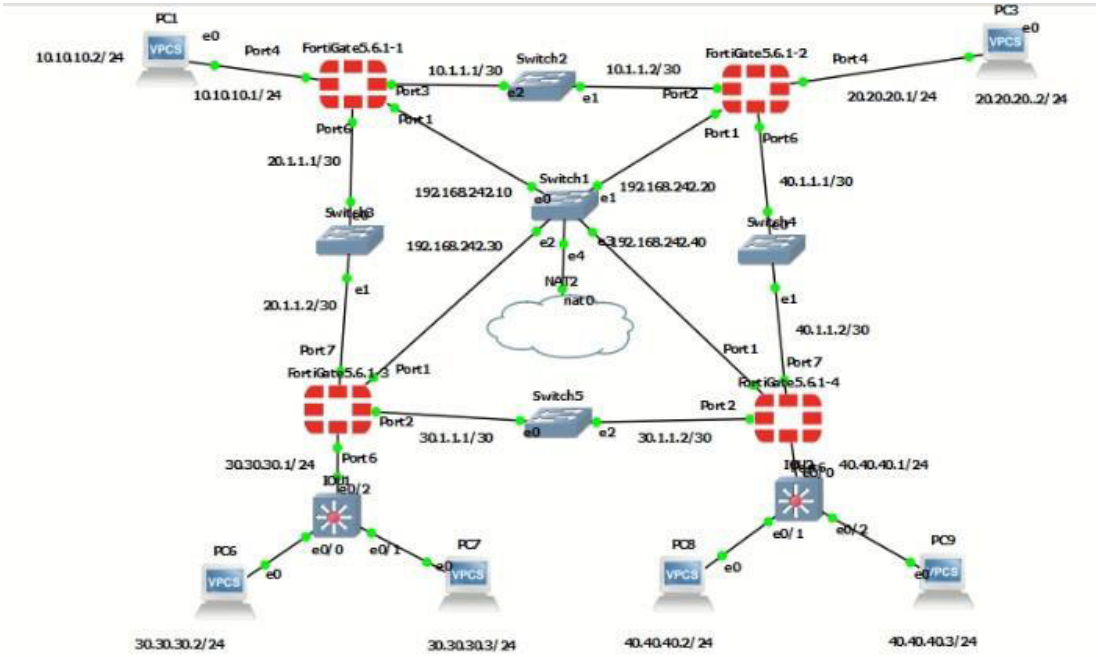


Figura 3.98 Topología Red SDWAN-OSPF

Para la configuración de cada uno de los equipos FortiGate se debe acceder a la consola de los mismos y se procede a la asignación del *Gateway* de internet respectivo a cada equipo esto se realiza por medio de la implementación de los siguientes comandos:

- config system interface
- edit port1
- set ip 192.168.242.10/24
- set allowaccess http ping
- end
- show system interface

El primer comando mencionado permitirá el acceso hacia la configuración del equipo. Posteriormente se procede a indicar en que puerto es el deseado a configurar en este caso debe ser el puerto que va conectado a la red NAT, a continuación, se procede a indicar la dirección del *Gateway* de internet y adicionalmente se indica el acceso que debe receptar ese puerto en cuestión. Estos parámetros se pueden cambiar en la interfaz gráfica del equipo, pero se debe configurar como parámetro inicial conexiones por http y ping es decir permitir conexiones del puerto 80 así como el envío y recepción de paquetes *Internet Control Message Protocol* (ICMP). Finalmente se muestra la configuración de ese puerto para de este modo comprobar que todo funciona

correctamente, esta configuración se muestra en la Figura 3.99 presentada a continuación.

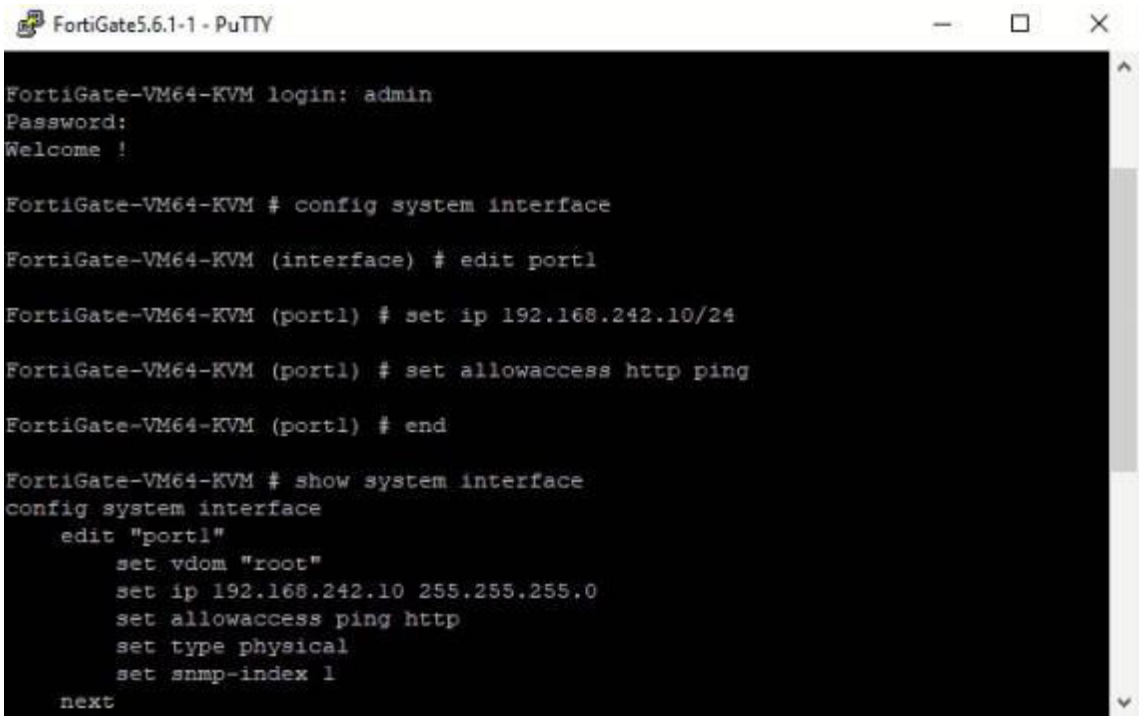


Figura 3.99 Configuración de equipo Fortigate RED 1

Esta configuración se procede a realizar en cada uno de los equipos FortiGate de cada una de las redes. Esta configuración se muestra en la Figura 3.100, la Figura 3.101 y la Figura 3.102 respectivamente.

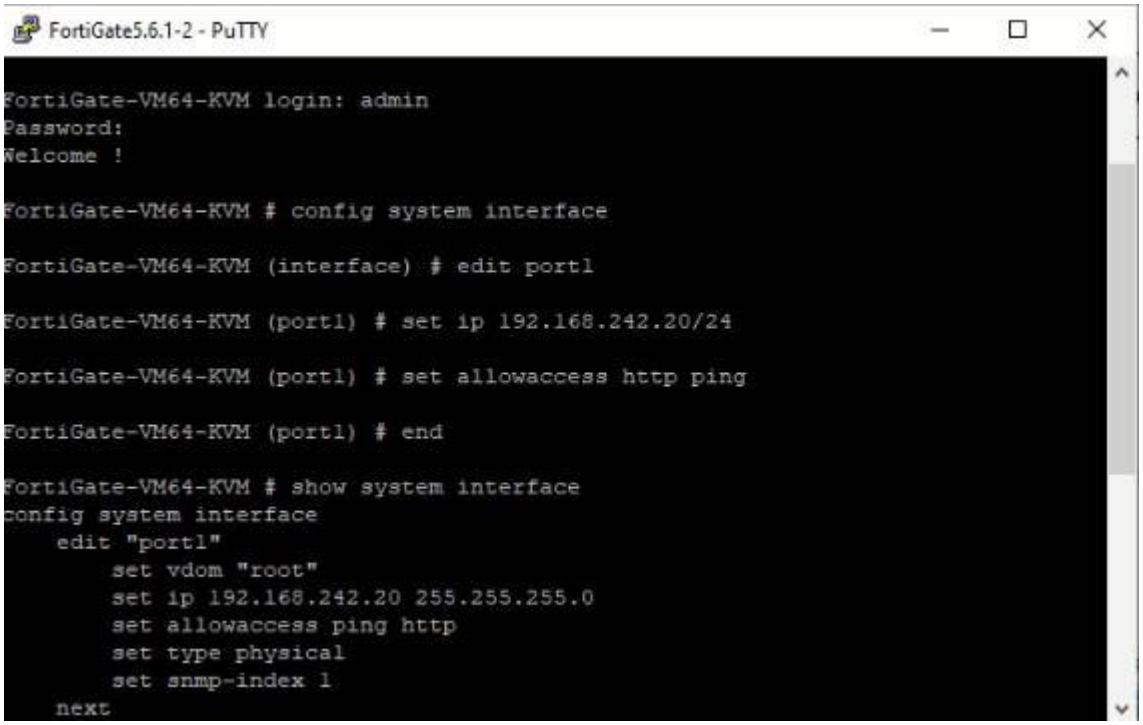


Figura 3.100 Configuración de equipo Fortigate RED 2

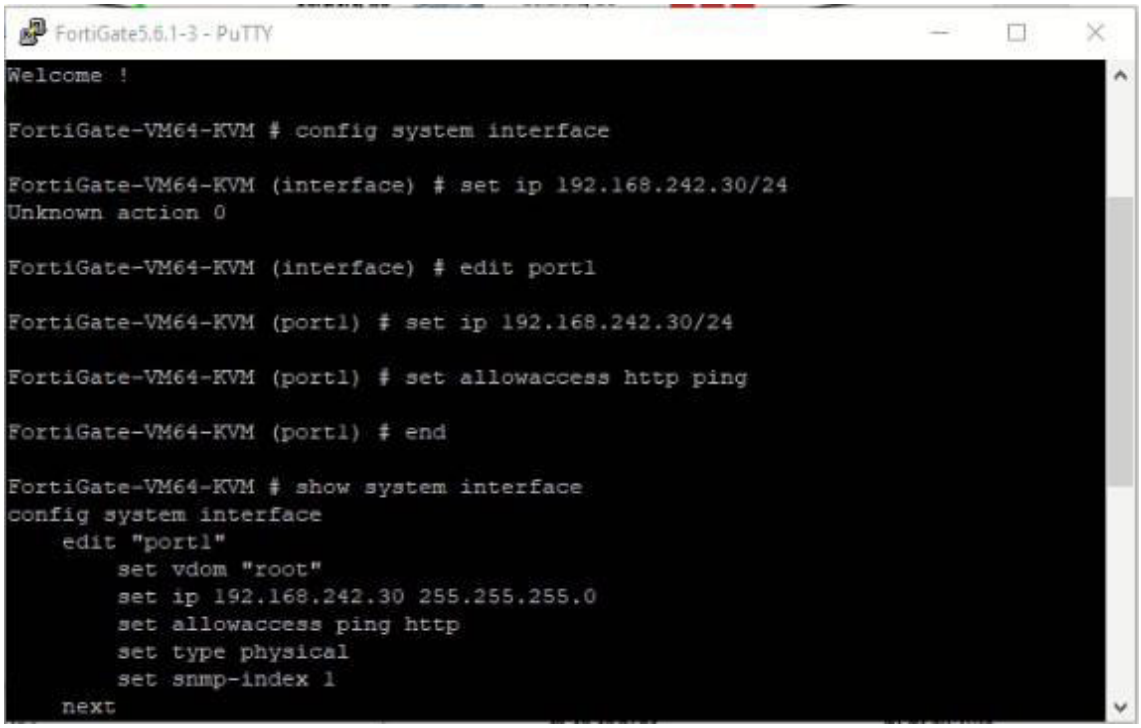


Figura 3.101 Configuración de equipo Fortigate RED 3

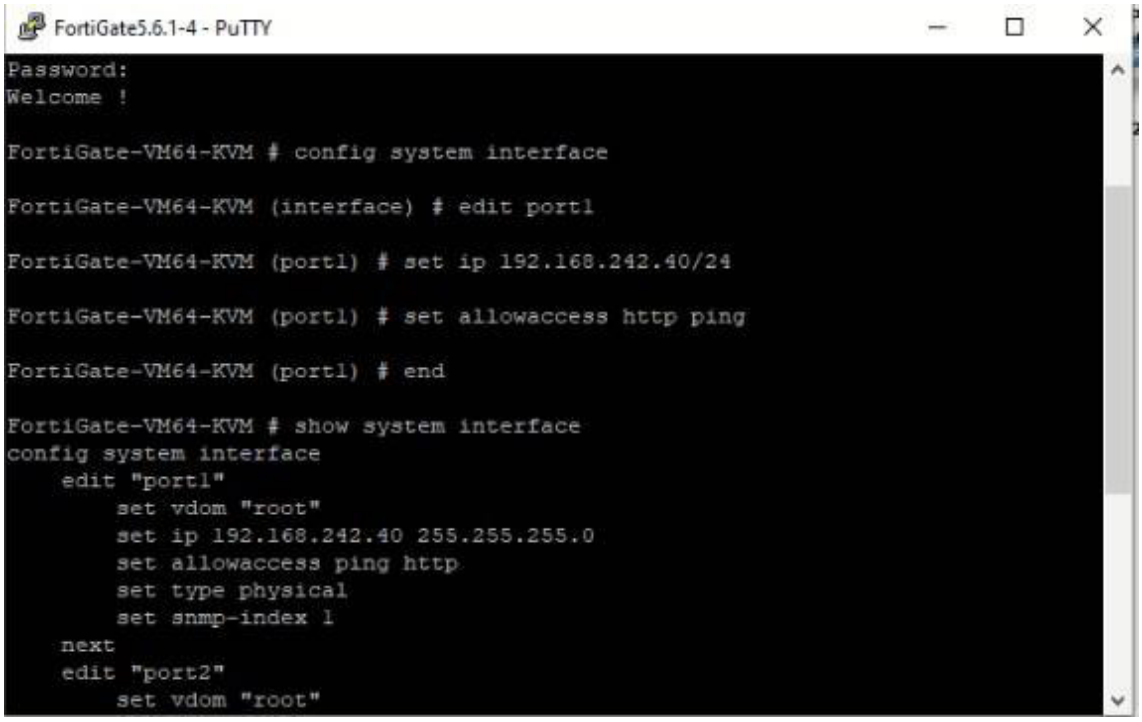


Figura 3.102 Configuración de equipo Fortigate RED 4

El siguiente aspecto a configurar son las VPCS de cada red con su respectivo *Gateway.* Para llevar a cabo esta acción se procede a asignar una dirección IP a cada uno de los equipos VPCS en las diferentes redes como se muestra en la Tabla 3.3 Direccionamiento RED SDWAN-VLAN-OSPF a continuación.

Tabla 3.3 Direcciones y *Gateways* VPCS SDWAN-OSPF

VPCS	DIRECCIÓN	GATEWAY
PC1	10.10.10.2/24	10.10.10.1
PC3	20.20.20.2/24	20.20.20.1
PC6	30.30.30.2/24	30.30.30.1
PC7	30.30.30.3/24	30.30.30.1
PC8	40.40.40.2/24	40.40.40.1
PC9	40.40.40.3/24	40.40.40.1

El comando para la asignación de estas direcciones es el siguiente “ip [dirección IP]/[máscara] [*Gateway*]”, como se muestra en la Figura 3.103 a continuación.

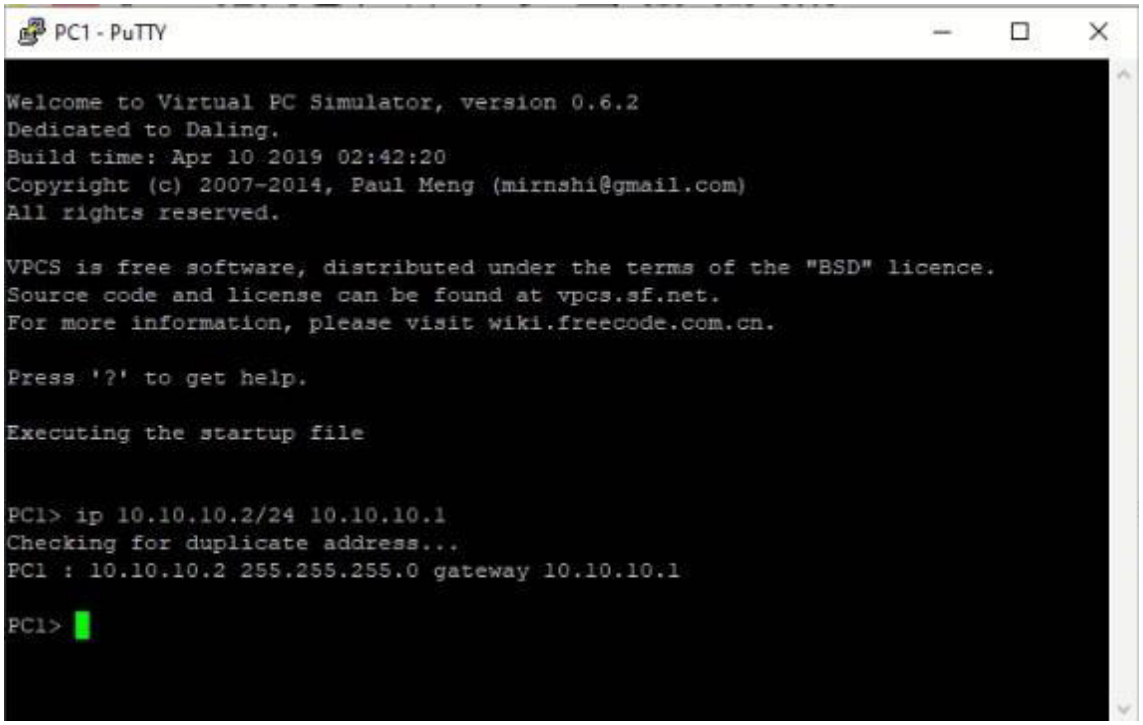


Figura 3.103 Establecimiento de IP en VPCS RED 1

Una vez realizadas las primeras configuraciones se procede a ingresar a la interfaz gráfica de cada uno de los equipos FortiGate de cada red.

Configuración Red 1

En esta parte se realizará la configuración del primer equipo FortiGate perteneciente a la red 1. Para acceder a la interfaz gráfica del mismo se debe escribir en el buscador de preferencia la dirección previamente configurada para este equipo la cual es 192.168.242.10. Una vez que se acceda al equipo solicitará un usuario y una clave de ingreso, tanto el usuario como la clave serán los configurados por defecto, es decir "admin" para cada uno de los equipos FortiGate. El primer paso a realizar consiste en editar las interfaces, la primera interfaz es la conectada directamente a la red internet, dentro de la misma se deben configurar los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.10/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING

El parámetro alias define el nombre que se le va a asignar a esta interfaz, como esta es la que va conectada a internet se le asigna el nombre de WAN. El parámetro role define qué papel jugará esta interfaz dentro de la red en este caso del mismo modo será el papel de un enlace WAN. Adicionalmente se debe establecer o verificar que tanto la dirección como la máscara sea la adecuada, finalmente el parámetro de acceso administrativo determinará el tipo de paquetes que podrán viajar por medio de este enlace, esta configuración se puede observar en la Figura 3.104.

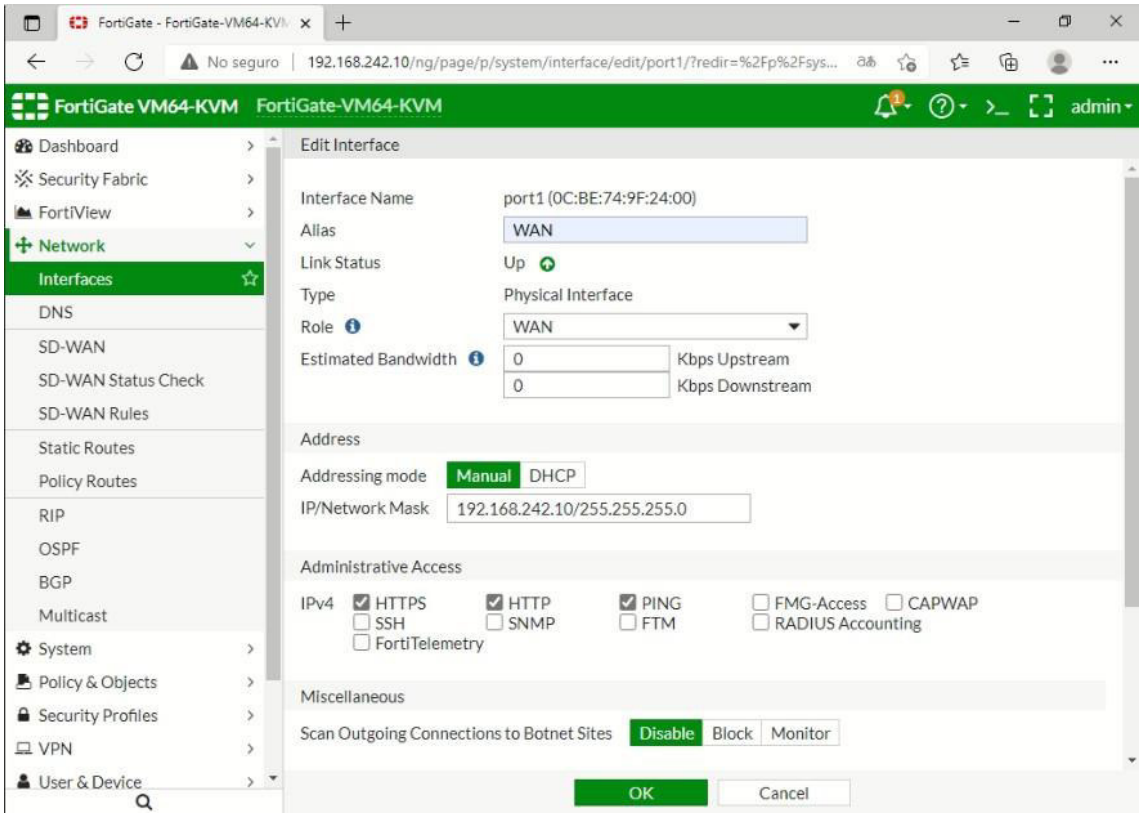


Figura 3.104 Configuración de interfaz WAN RED 1

Del mismo modo que en la anterior interfaz se proceden a editar cada una de las interfaces conectadas al equipo, en este caso el nombre de la interfaz corresponderá a un enlace ISP-1 ya que será el primer enlace serial entre equipos a configurar. Los parámetros a cambiar son los siguientes, mismos que se aprecian en la Figura 3.105. Este procedimiento se aplica para ambas conexiones IPS seriales.

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 10.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH
- Alias: ISP-2
- Role: WAN
- IP/Network Mask: 20.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH

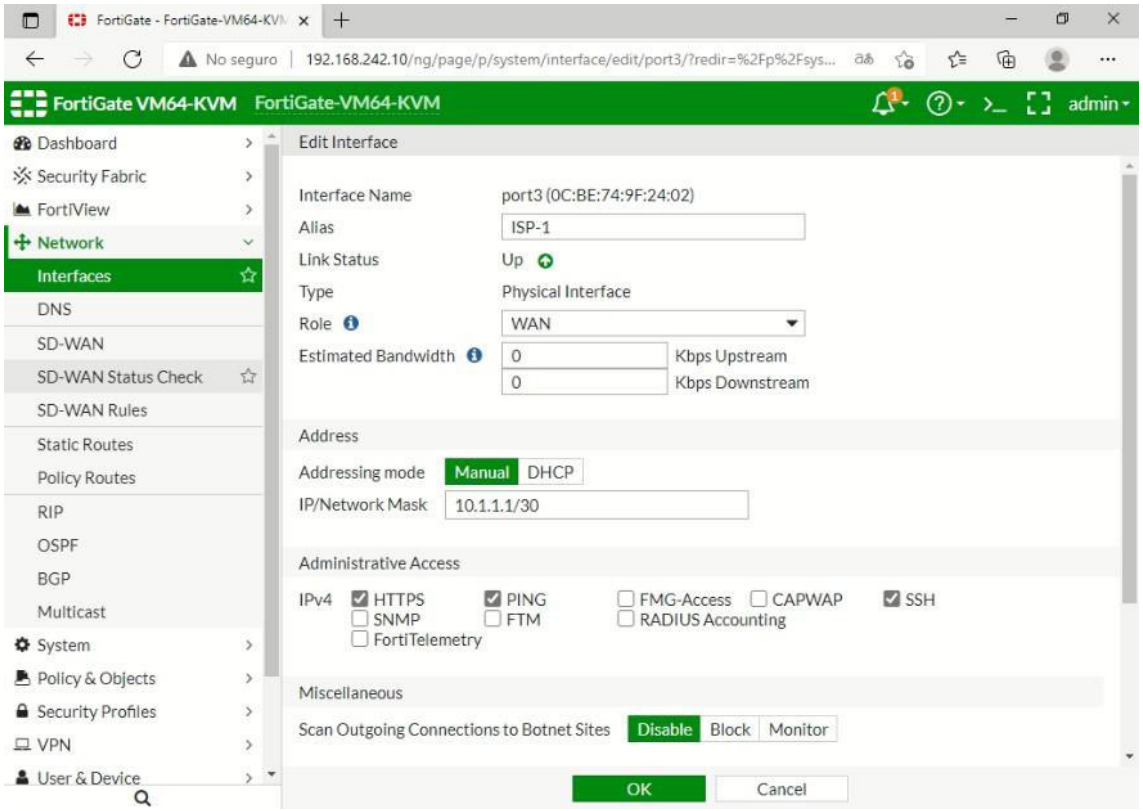


Figura 3.105 Configuración de interfaz ISP RED 1

Siguiendo el procedimiento anterior se procede a configurar la interfaz LAN para esta red. El cambio en esta configuración es en el rol que jugará esta interfaz ya que debe ser establecida como una LAN. Los parámetros utilizados se detallan a continuación mismos que pueden ser observados en la Figura 3.106.

- Alias: LAN
- Role: LAN
- IP/Network Mask: 10.10.10.1/24
- Administrative Access: HTTPS, HTTP, PING,SSH

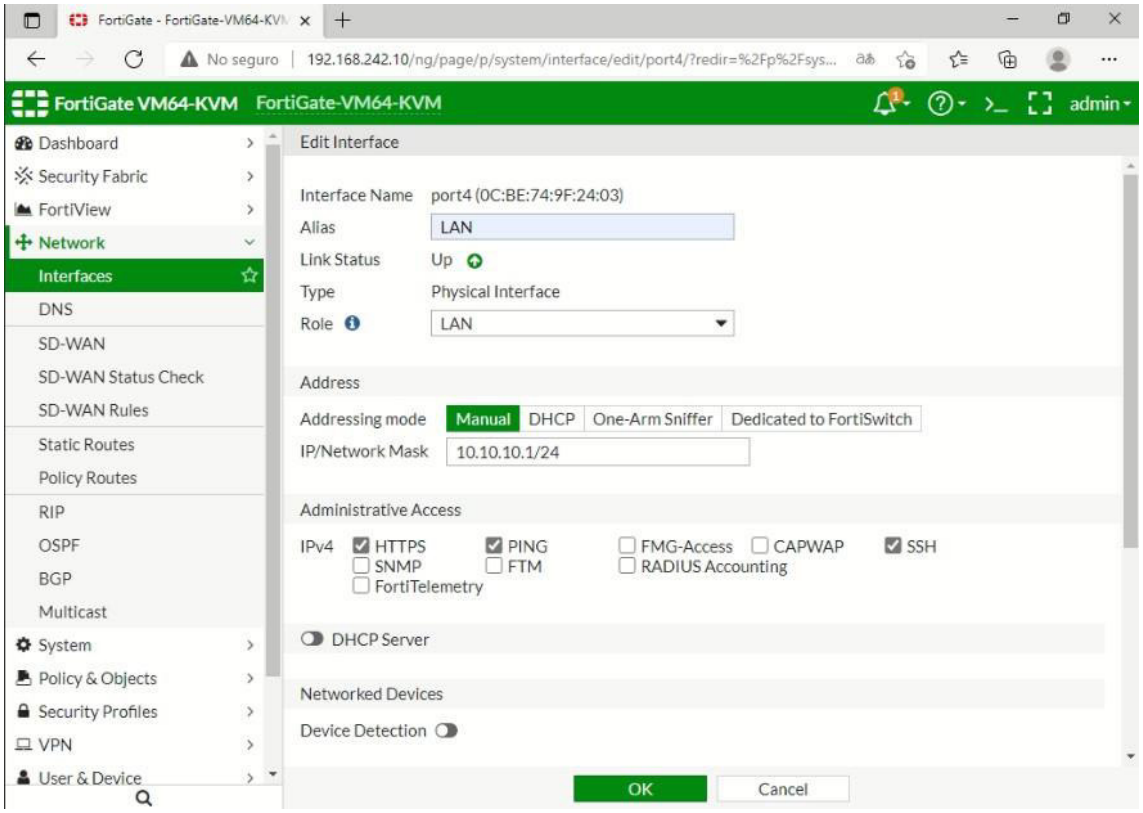


Figura 3.106 Configuración de interfaz LAN RED 1

Adicionalmente a las interfaces previamente definidas se debe crear una nueva interfaz virtual de tipo *loopback* la misma que ayudará al host de la red para redirigir el tráfico hacia ellos mismos con el fin de acceder directamente a los servicios que se ejecuten en los propios dispositivos. Para crear esta interfaz se debe seleccionar la opción de crear nueva interfaz dentro del apartado "*network > interfaces*", una vez dentro se configuran los siguientes parámetros como se muestra en la Figura 3.107.

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 1.1.1.1/32
- Administrative Access: HTTPS, PING, SSH

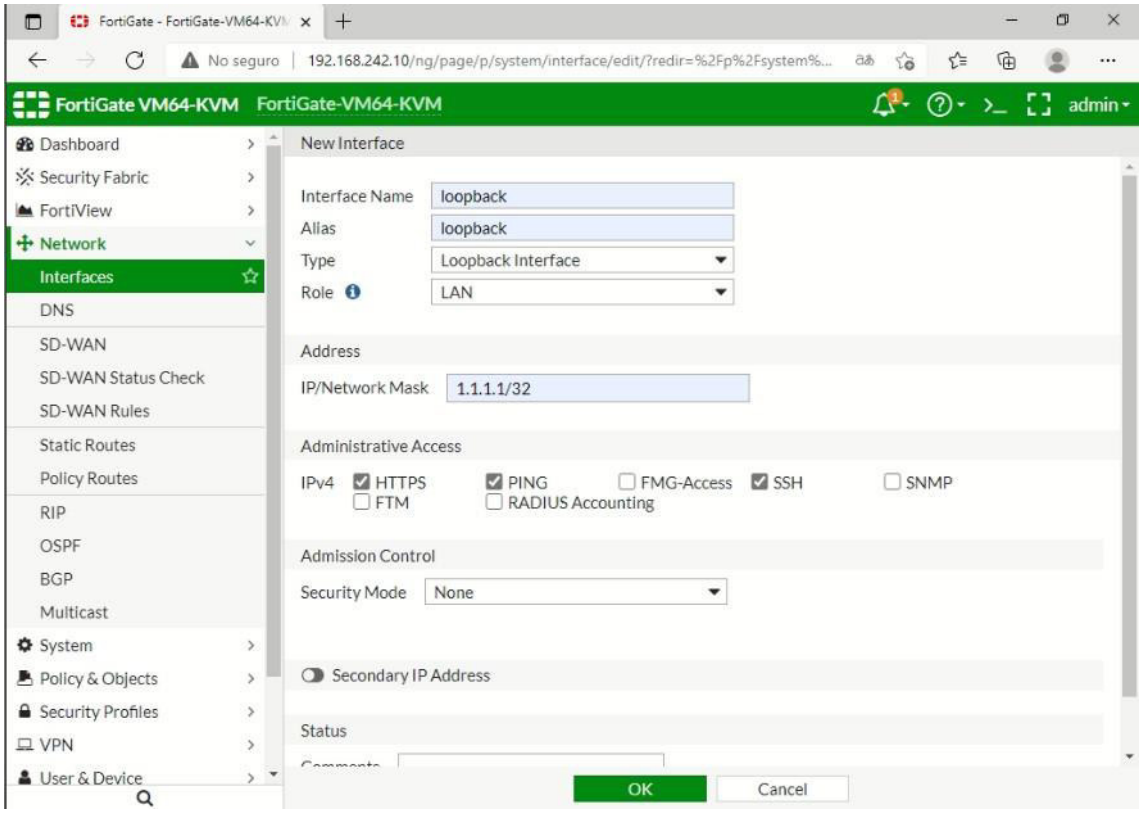


Figura 3.107 Configuración de interfaz loopback

Para comprobar que las interfaces fueron configuradas correctamente se debe revisar las direcciones. Así como los accesos que están destinados a cada uno de los puertos como se muestra en la Figura 3.108.

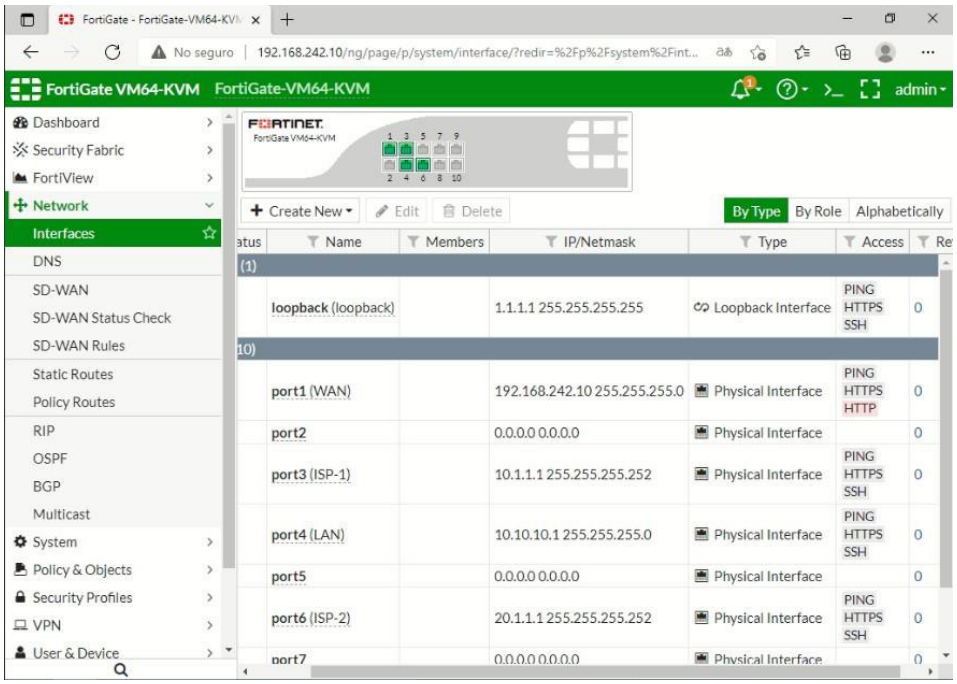


Figura 3.108 Interfaces en Fortigate RED 1

Con las interfaces configuradas se procede a acceder al apartado "*Network > SDWAN*" dentro del cual se configurarán los enlaces a los cuales se les será asignada una conexión SDWAN. En el caso de esta primera red se usan los dos enlaces seriales denominados como ISP-1 e ISP-2 respectivamente y se asigna su *Gateway* respectivo para finalizar con la configuración como se muestra en la Figura 3.109.

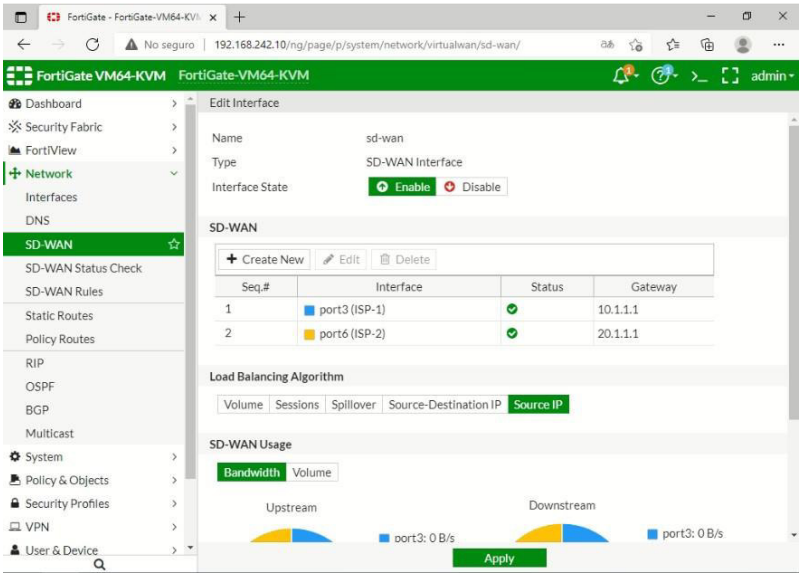


Figura 3.109 Configuración de SDWAN RED 1

Una vez definidas las interfaces por las cuales circulará el tráfico de SDWAN se deben establecer normas o leyes las cuales permitirán posteriormente verificar el estado de las conexiones de las mismas. Para configurar esta ley se debe acceder a "*Network > SD-WAN Status Check*" y se deben configurar los siguientes parámetros:

- Name: Ley-1
- Server: 10.1.1.1
- Timeout: 10 (s)

En el apartado de server se configura el *Gateway* por medio del cual viaja el tráfico de SDWAN y el tiempo de salida de cada paquete para que se registre en el monitoreo en este caso se establece de 10 segundos, pero este valor puede variar. Esta configuración se muestra en la Figura 3.110 a continuación.

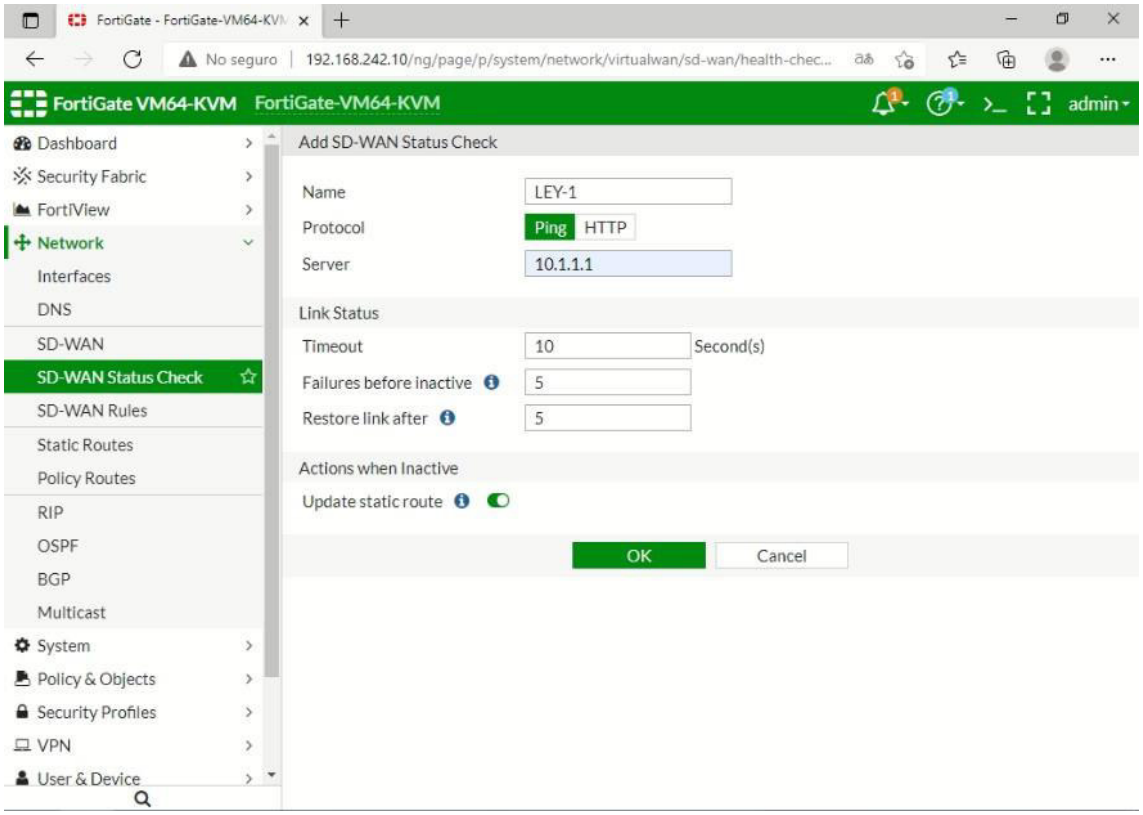


Figura 3.110 Configuración de SD-WAN Status Check RED 1

Adicionalmente se procede a configurar las reglas respectivas para el correcto funcionamiento de SDWAN, los parámetros que se deben configurar son los siguientes:

- Name: LEY_1
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 10.1.1.1 & Gateway 20.1.1.1
- Status Check: LEY1

En el parámetro de Fuente se debe asignar a todas las fuentes disponibles. De este modo todo el tráfico proveniente de la red LAN podrá salir por estas interfaces sin ningún problema y de la misma manera la dirección de destino debe ser hacia todas las direcciones para tener una comunicación total en la red. También se procede a asignar los *gateways* de las interfaces ISP y finalmente se selecciona la ley previamente configurada para que el monitoreo pueda realizarse, esta configuración se aprecia en la Figura 3.111.

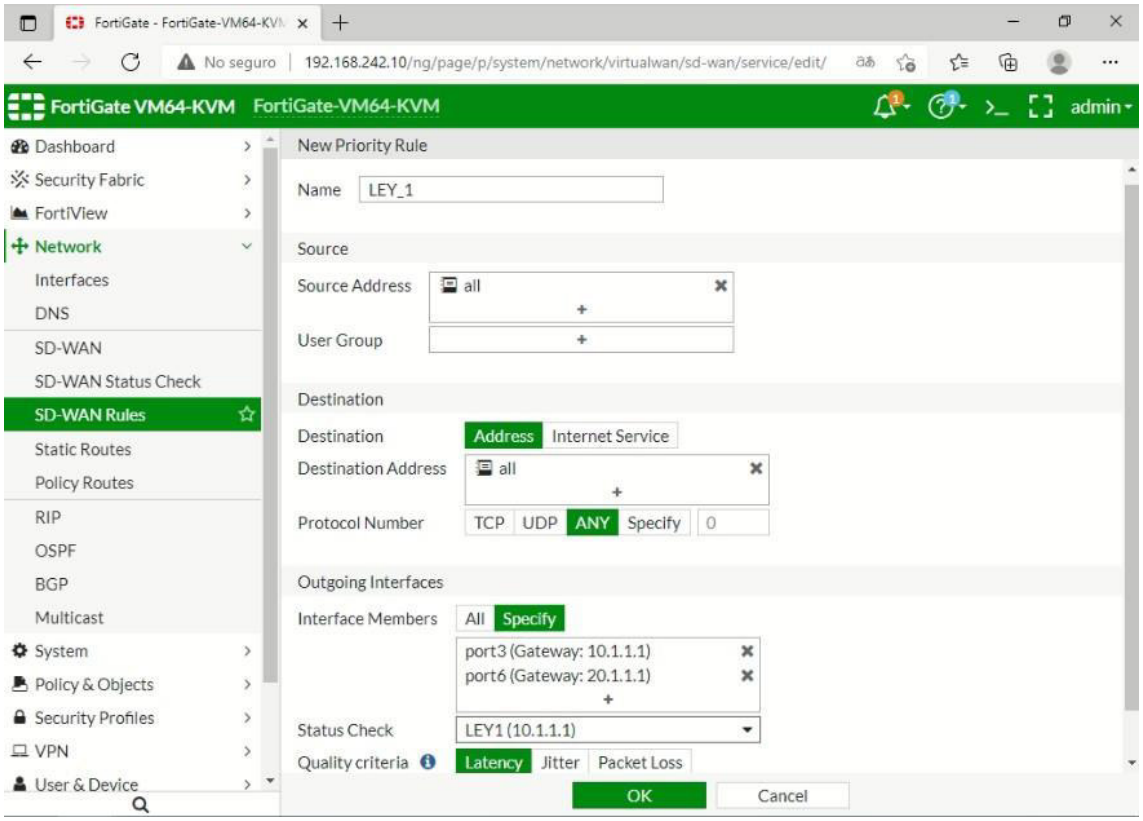


Figura 3.111 Configuración de reglas SDWAN RED 1

Para lograr que la red LAN tenga salida a internet se debe configurar una ruta por defecto con salida hacia el *Gateway* predefinido por la NAT previamente revisada. Para realizar esta configuración se accede a "*Network > Static Routes*" y dentro de la misma se configuran los siguientes parámetros:

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

Como se puede apreciar el destino es una ruta por defecto de modo que toda conexión desconocida por la red LAN viajará por esta dirección hacia la Internet. El dispositivo es la interfaz WAN previamente configurada para la salida a internet y el *Gateway* es el definido por la NAT, esta configuración se muestra en la Figura 3.112. A continuación.

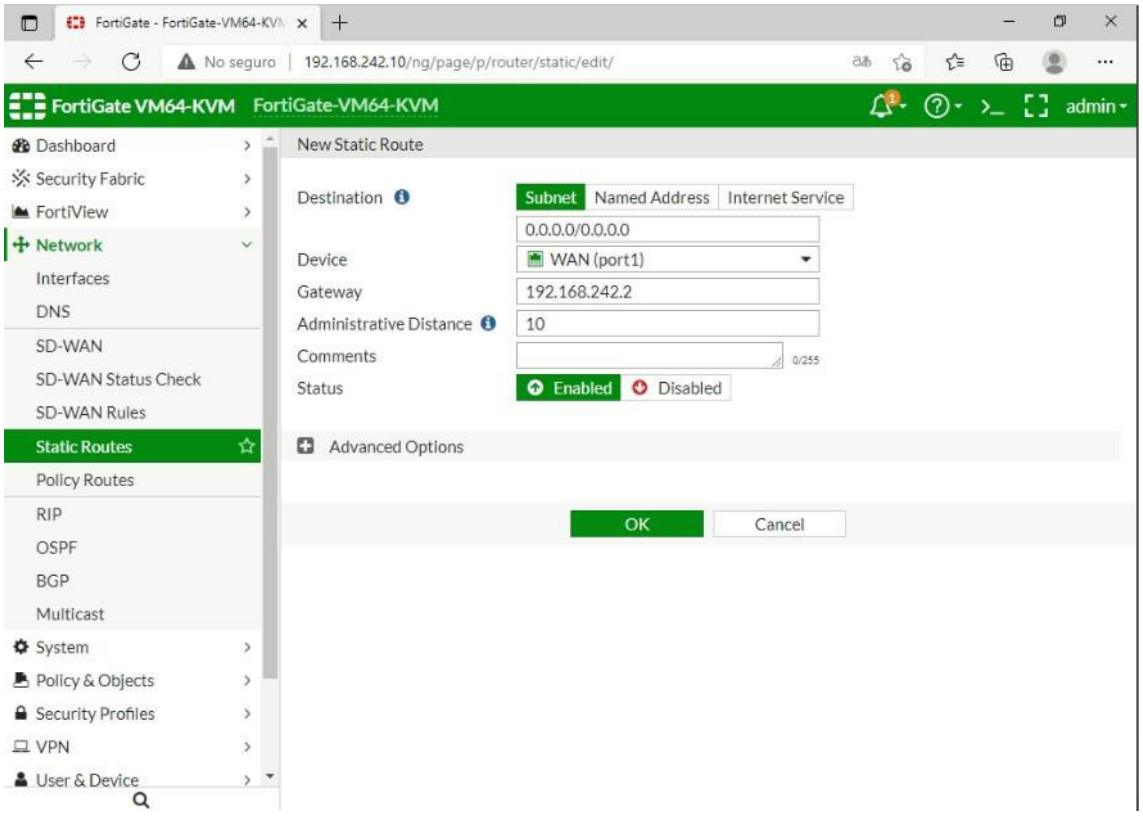


Figura 3.112 Configuración de una ruta por defecto

Para que todos los cambios que se han realizado hasta el momento puedan operar de forma correcta se deben establecer políticas las cuales permitirán el tráfico dentro de la red. Previo a definir estas políticas se configura la dirección de la red LAN para que esté disponible dentro de las configuraciones del equipo; para llevar esto a cabo se accede a "*Policy & Objects > Addresses*" y dentro de este apartado se crea una nueva dirección modificando los siguientes parámetros:

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 10.10.10.0/24
- Interface: LAN

Es importante que en el parámetro de interface se coloque el puerto por medio del cual está viajando la red LAN ya que de lo contrario las configuraciones de las políticas no se pueden llevar a cabo. Estas configuraciones se observan en la Figura 3.113.

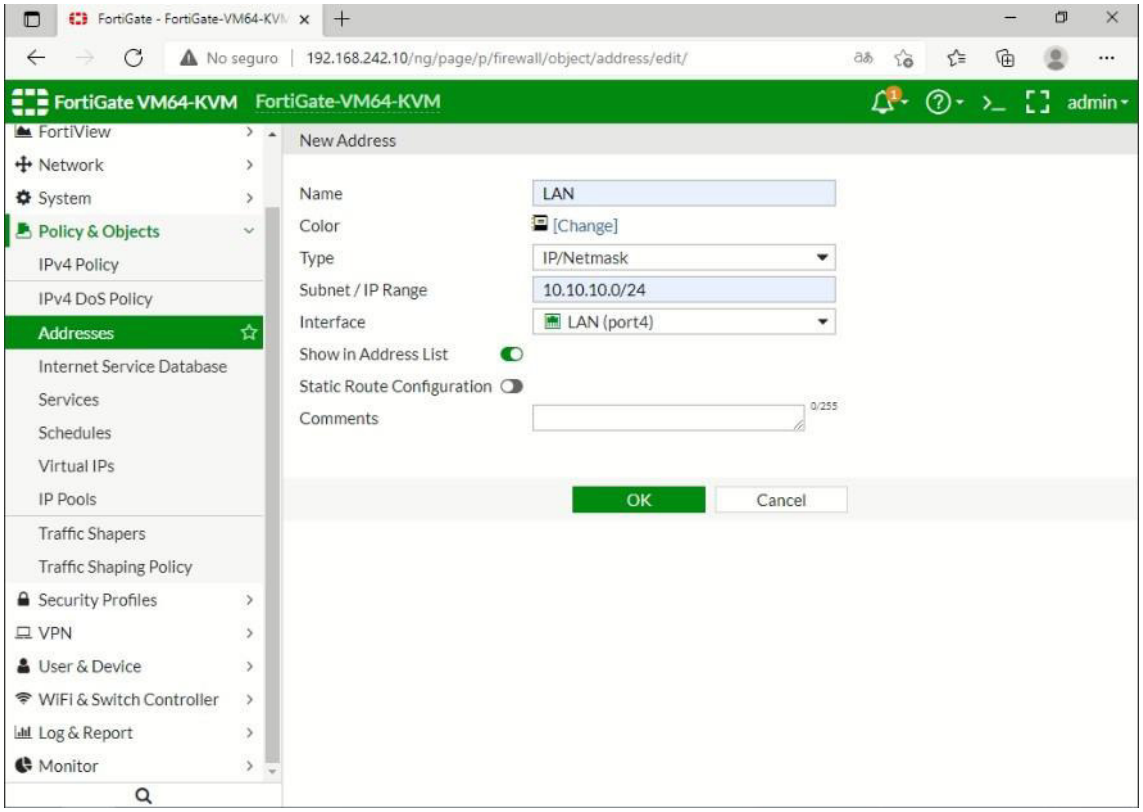


Figura 3.113 Configuración de dirección para políticas RED 1

Un aspecto importante a tener en cuenta es que por ser equipos con licencias de prueba de parte de FortiGate se tiene un máximo de 6 políticas para definir ya que por defecto el equipo niega todas las comunicaciones entrantes o salientes. Para poder obtener una correcta comunicación se proceden a configurar 4 políticas. La primera de ellas es la política para tener acceso a internet para ello se debe configurar los siguientes parámetros:

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

En los parámetros tanto de interfaz de entrada como la interfaz de salida se debe definir desde donde viene el tráfico y hacia dónde va dirigido; del mismo modo se define la fuente y los destinatarios que en este caso serán todo tipo de redes ya que es una salida a internet. Adicionalmente se configuran todo tipo de servicios como se muestra en la Figura 3.114.

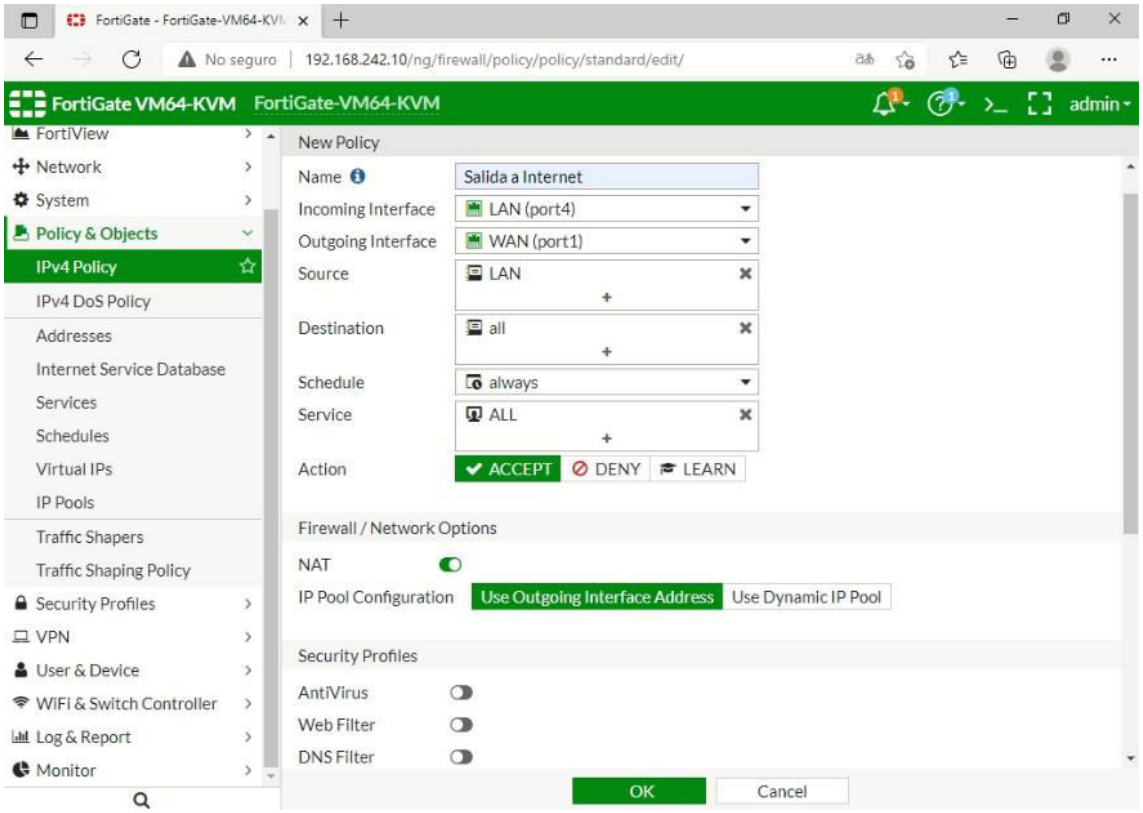


Figura 3.114 Política de salida a internet RED 1

La siguiente política a determinar es para lograr conectividad dentro de la red. Por eso la interfaz por la que debe pasar el tráfico primero para salir hacia la red es por la interfaz de *loopback*. La interfaz hacia dónde va dirigido todo el tráfico es la interfaz de SD-WAN es decir los dos enlaces seriales y el tráfico que se debe permitir es de todo tipo. Los parámetros que se deben configurar son los siguientes, mismos que se observan en la Figura 3.115.

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

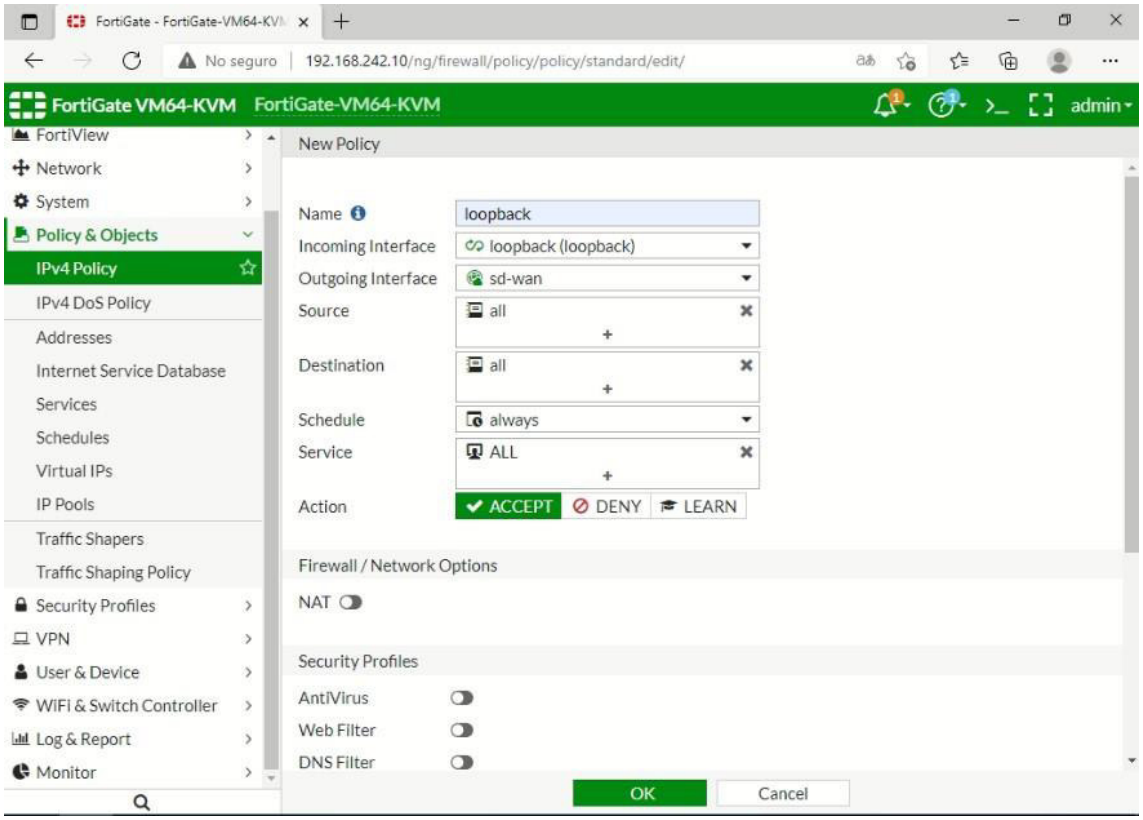


Figura 3.115 Configuración de política de loopback RED 1

La tercera regla es para definir que todo el tráfico de la red LAN salga al resto de la red por medio de las interfaces seriales SD-WAN. Los parámetros que se deben configurar son los siguientes:

- Name: LAN
- Incoming Interface: LAN
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Adicionalmente, se deben permitir todos los servicios esto con el fin de que todas las comunicaciones se puedan llevar a cabo correctamente. Como se muestra en la Figura 3.116.

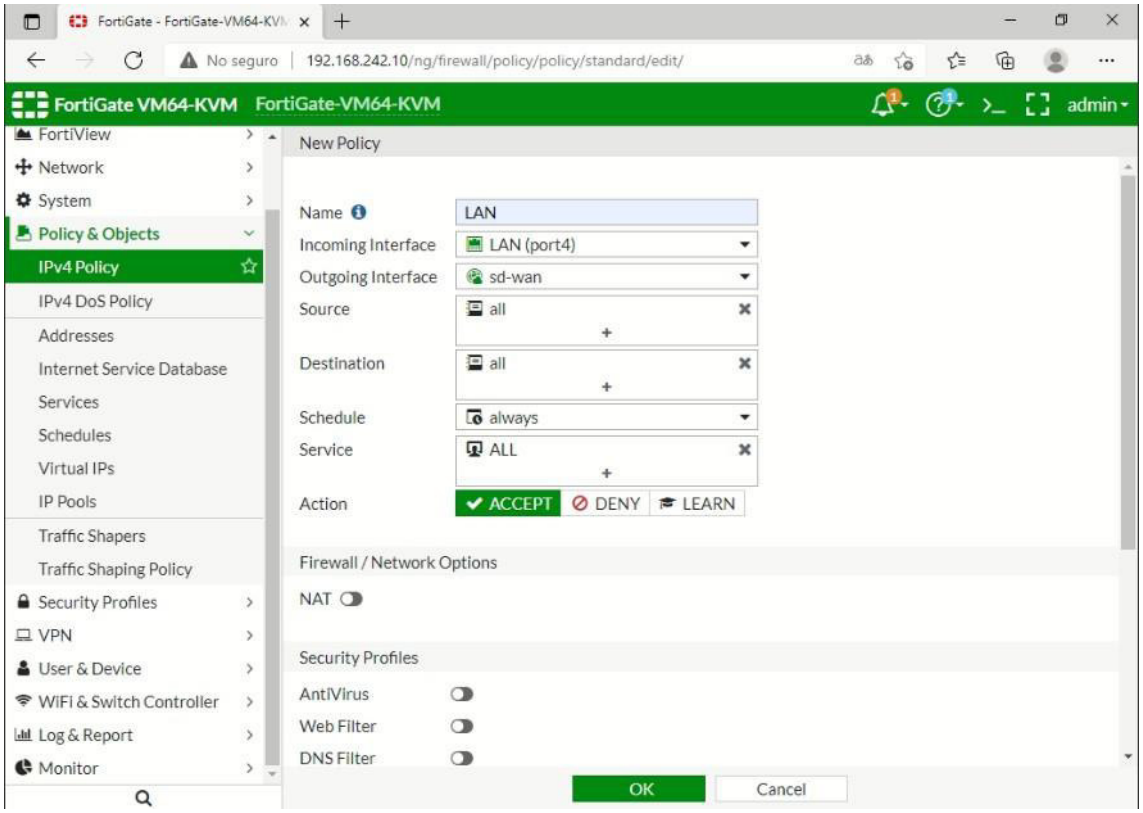


Figura 3.116 Configuración de política de la red LAN RED 1

Finalmente, la última política consiste en permitir el tráfico de regreso desde los enlaces de SD-WAN hacia la red LAN habilitando adicionalmente todos los servicios para que ninguna comunicación se vea comprometida en un futuro. Los parámetros a configurar son los siguientes, los mismos que se pueden apreciar en la Figura 3.117.

- Name: LAN_1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

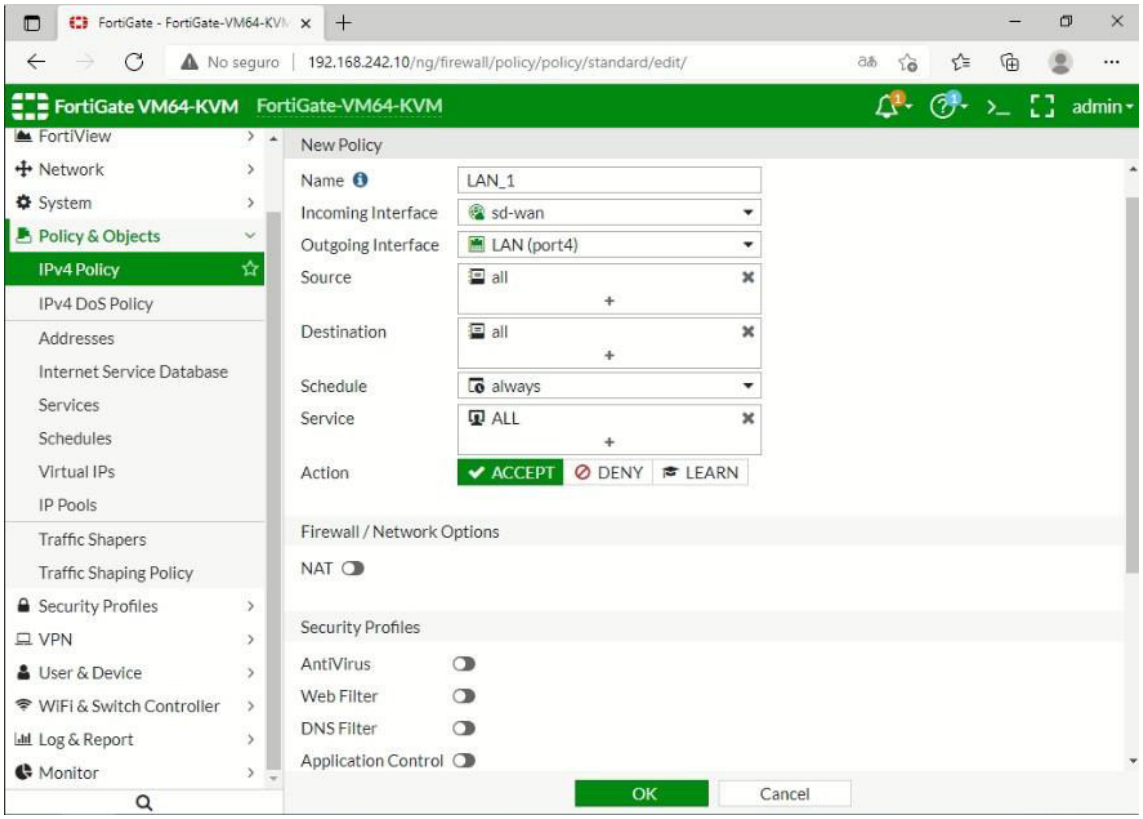


Figura 3.117 Configuración de política de retorno LAN RED 1

Para comprobar que todas las políticas se escribieron correctamente, se las revisa en el apartado de "*Policy & Objects > IPv4 Policy*". Para comprobar que todas están operativas la acción esperada es *ACCEPT* en todas las políticas escritas previamente como se aprecia en la Figura 3.118.

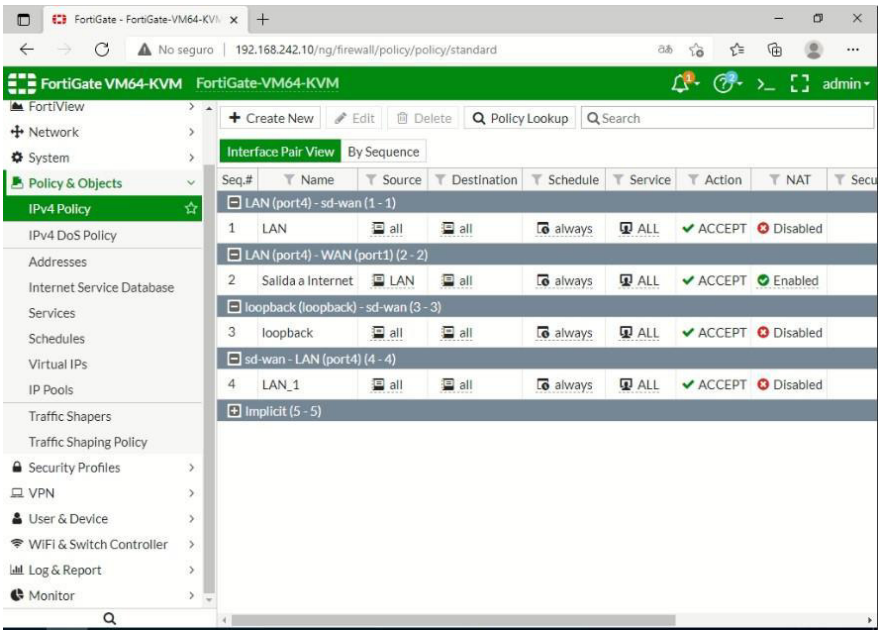


Figura 3.118 Políticas para acceso en la RED 1

Una vez definidas las políticas, se procede a configurar el protocolo de enrutamiento dinámico definido para esta ocasión el cual es el protocolo OSPF. Para poder configurar este protocolo es obligatorio asignar una identificación al *router* de lo contrario no se podrán establecer las redes ni el área de trabajo respectiva. La identificación de *router* que funcionará para este equipo en específico es 1.1.1.1. El primer parámetro a configurar es el establecimiento de un área la cual será el área por defecto es decir la 0.0.0.0 y dentro de esta área operarán todas las interfaces definidas. El paso que se debe ejecutar a continuación es definir porque interfaces va a circular todo el tráfico. En este caso en particular las interfaces SD-WAN serán las encargadas de hacer distribuir el tráfico, finalmente se deben hacer conocer todas las interfaces que se encuentran conectadas a este equipo las cuales se detallan a continuación:

- 1.1.1.1/255.255.255.255
- 10.1.1.0/255.255.255.252
- 20.1.1.0/255.255.255.252
- 10.10.10.0/255.255.255.0

Una vez configuradas las interfaces, se aplican todos los cambios como se muestra en la Figura 3.119 a continuación.

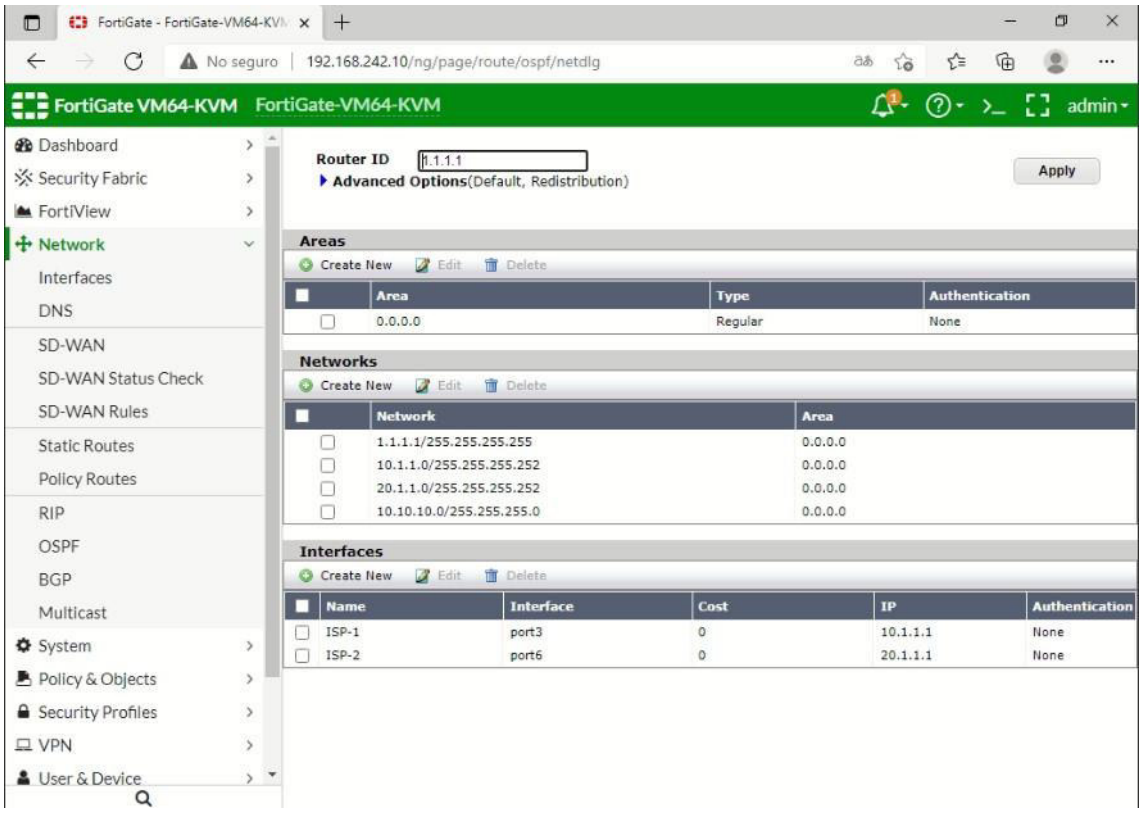


Figura 3.119 Configuración de protocolo OSPF RED 1

Con este paso concluye la configuración de la primera red y se procede a para comprobar que todas las interfaces. Así como los permisos y servicios que se tienen asignados, se encuentran correctamente configurados. Se procede a comprobar en "*Network > Interfaces*" como se muestra en las Figura 3.120 y Figura 3.121.

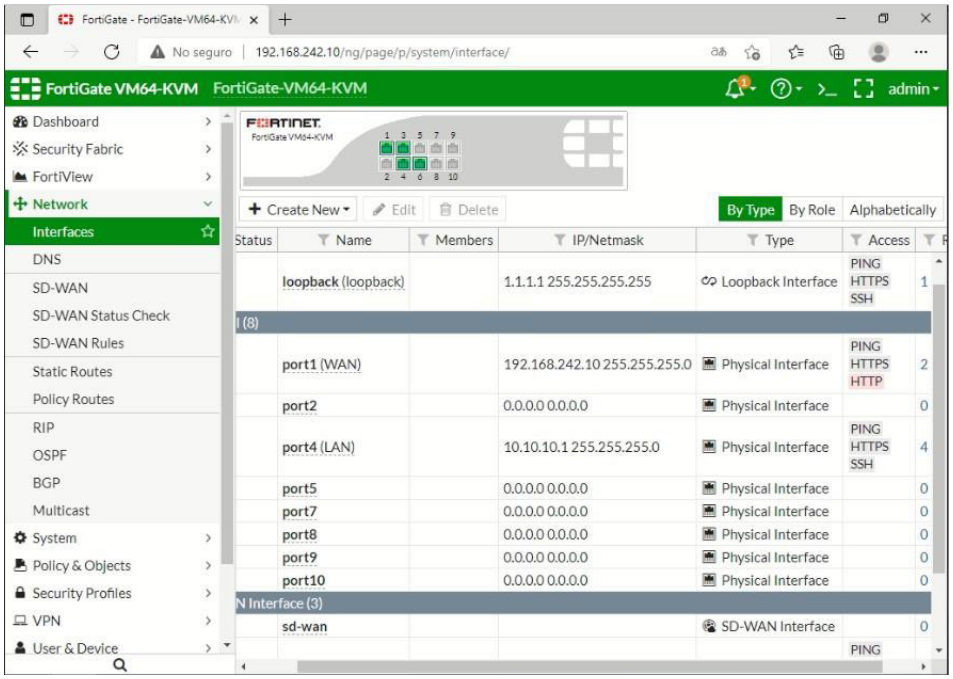


Figura 3.120 Interfaces en RED 1

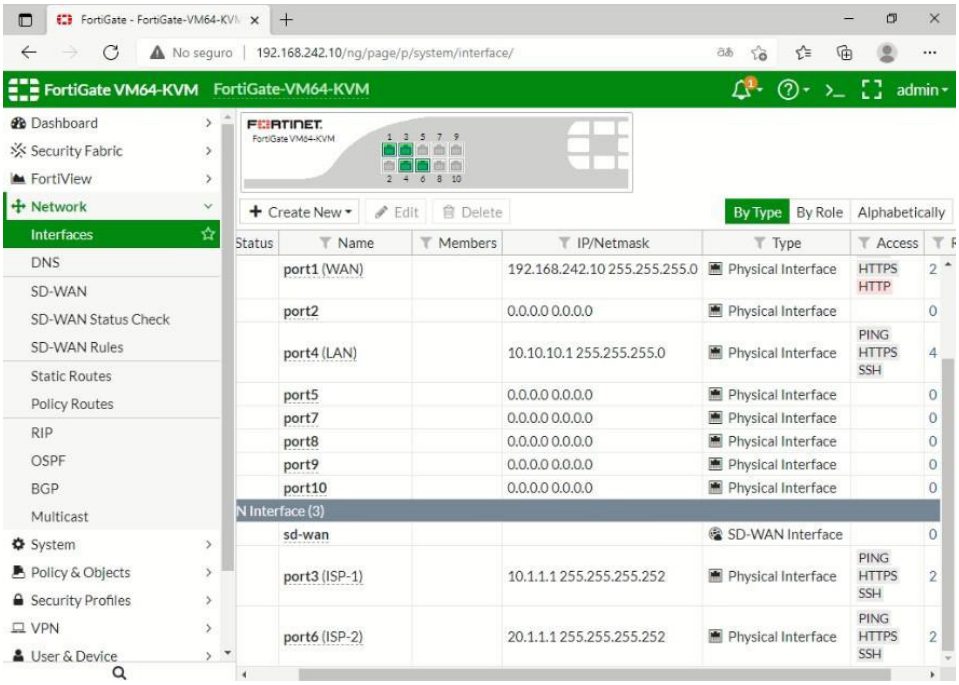


Figura 3.121 Interfaces SDWAN en RED 1

Configuración Red 2

Para la configuración del segundo equipo FortiGate perteneciente a la segunda red, se debe acceder a la interfaz gráfica del mismo; es decir se debe colocar en el buscador la dirección 192.168.242.20 y colocar tanto el usuario y contraseña por defecto. Los pasos a realizar en esta configuración son los mismos que en la primera red, el primer paso es asignar un nuevo nombre a la interfaz que sale a internet por medio de la configuración de los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.20/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING

De igual manera se procede a configurar los dos enlaces seriales con sus respectivos nombres ISP para que puedan ser reconocidos dentro de la red. Esto se logra configurando los siguientes parámetros:

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 10.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING, SSH
- Alias: ISP-2
- Role: WAN
- IP/Network Mask: 40.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Conforme al procedimiento presentado previamente, se procede a configurar la red LAN de esa red por medio de la implementación de los siguientes parámetros:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 20.20.20.1/24
- Administrative Access: HTTPS, HTTP, PING,SSH

Adicionalmente se debe configurar una interfaz *loopback* para que sea reconocida dentro de la red, esto también facilitará la comunicación por el protocolo OSFP además de redirigir todo el tráfico hacia los *hosts* disponibles en esa red. Esto por medio de la implementación de los siguientes parámetros:

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 1.1.1.2/32
- Administrative Access: HTTPS, PING, SSH

Para comprobar que todas las interfaces fueron configuradas correctamente se accede al apartado de interfaces dentro del equipo FortiGate. Como se muestra en la Figura 3.122.

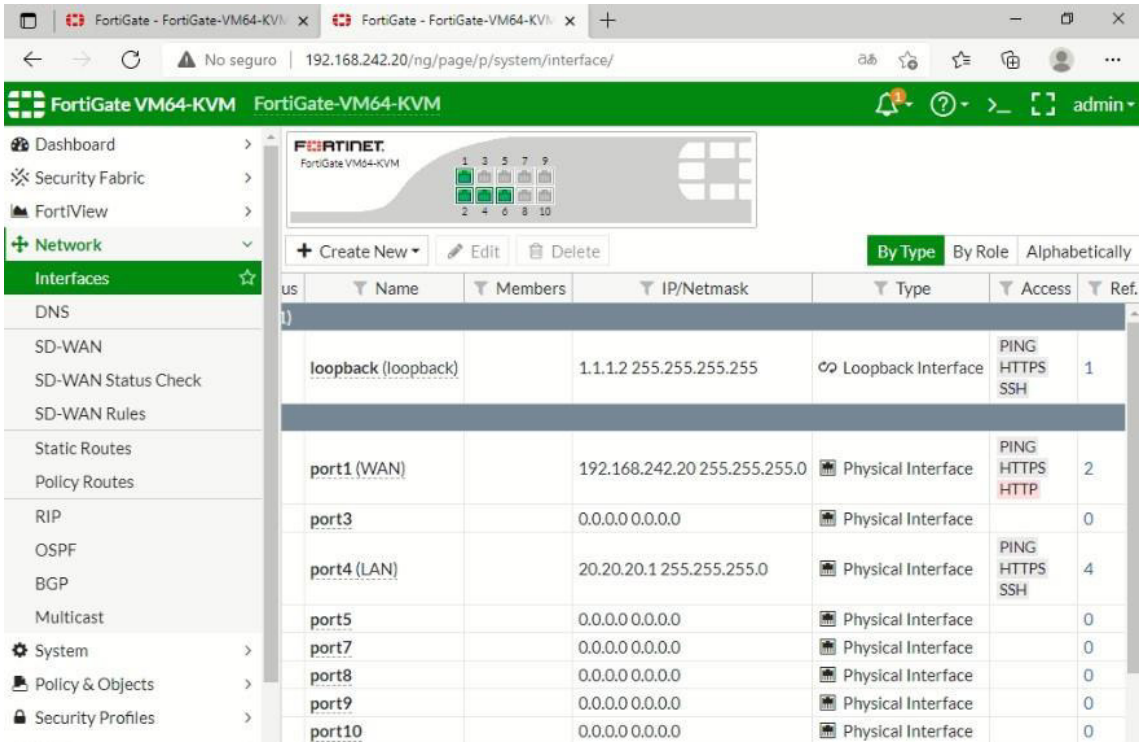


Figura 3.122 Interfaces Configuradas RED 2

De igual manera que en la primera red se debe configurar el apartado de SDWAN para ello se debe asignar el *Gateway* de cada uno de los enlaces seriales ISP por los cuales circulará todo el tráfico perteneciente a dicha red como se muestra en la Figura 3.123.

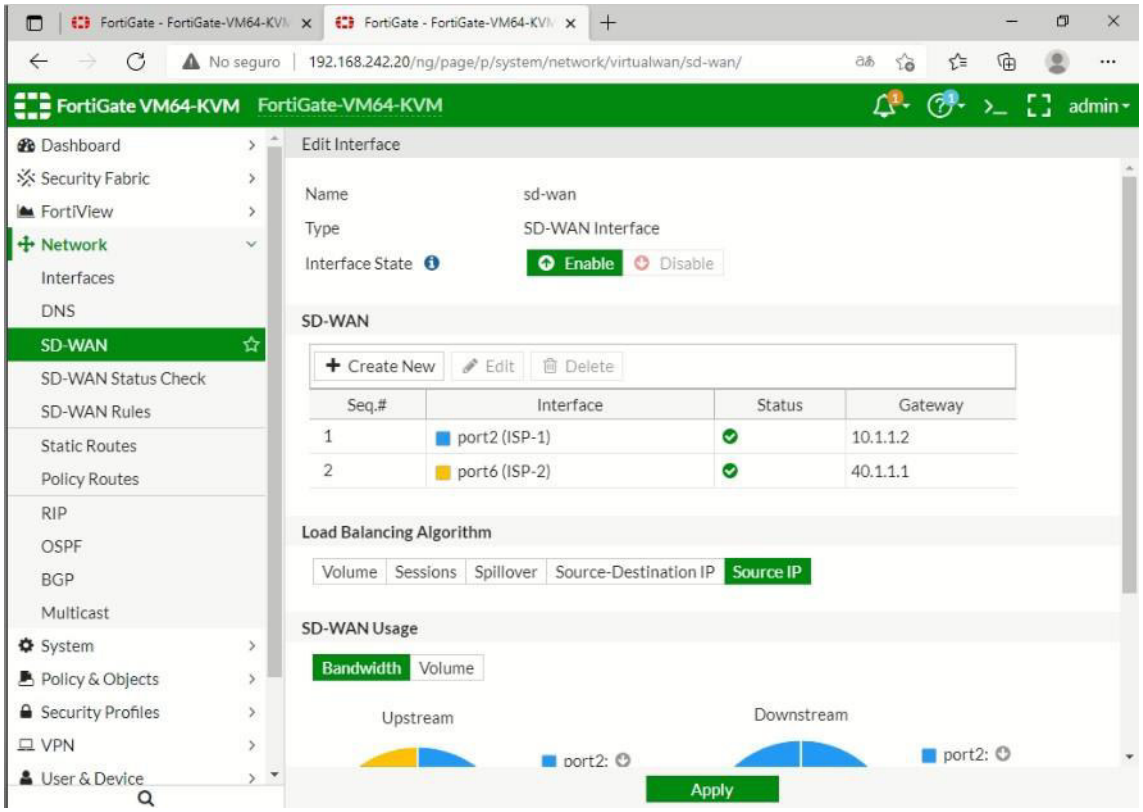


Figura 3.123 Configuración de SDWAN RED 2

El siguiente paso a configurar es el apartado de definir una ley para poder realizar el monitoreo correctamente de los enlaces SD-WAN para poder realizarlo se sigue los siguientes parámetros:

- Name: LEY2
- Server: 10.1.1.2
- Timeout: 10 (s)

Es importante notar que las leyes definidas no pueden ser nombradas del mismo modo en todos los equipos FortiGate de la red puesto que generaría un conflicto en las reglas causando así un colapso del tráfico y que la red se caiga.

A continuación, se procede a configurar las reglas de SD-WAN para esta red y se siguen los siguientes parámetros, mismos que se pueden observar en la Figura 3.124.

- Name: ley_2
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 10.1.1.2 & Gateway 40.1.1.1
- Status Check: LEY2

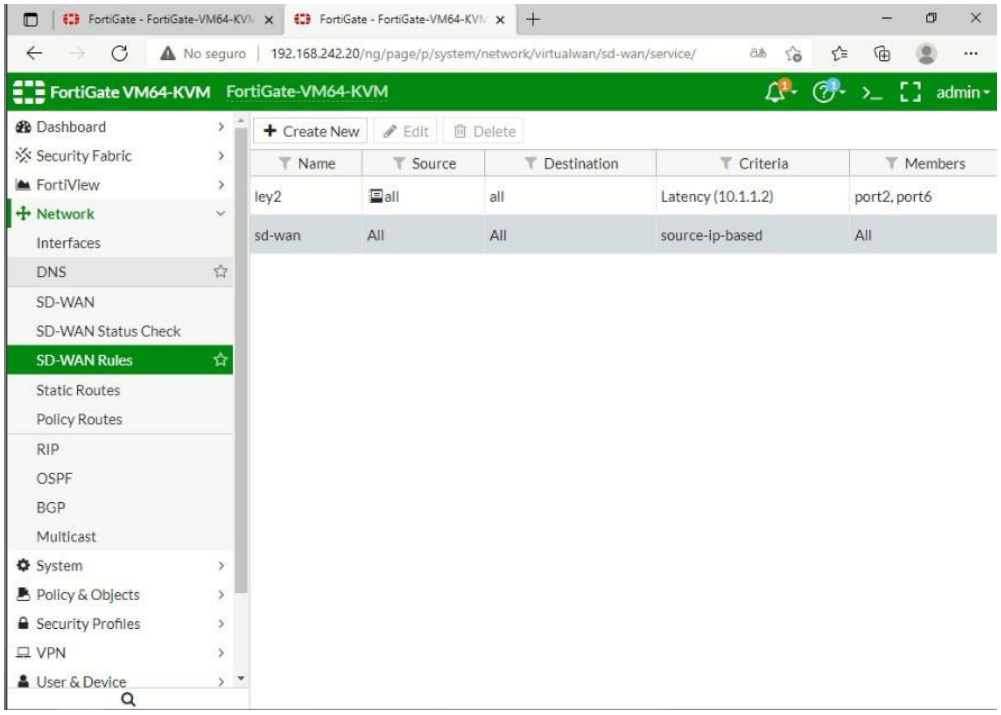


Figura 3.124 Configuración de reglas SDWAN RED 2

Al igual que en la primera red se debe configurar una ruta estática por *default* mediante la aplicación de los siguientes parámetros. Mismos que se aprecian en la Figura 3.125.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

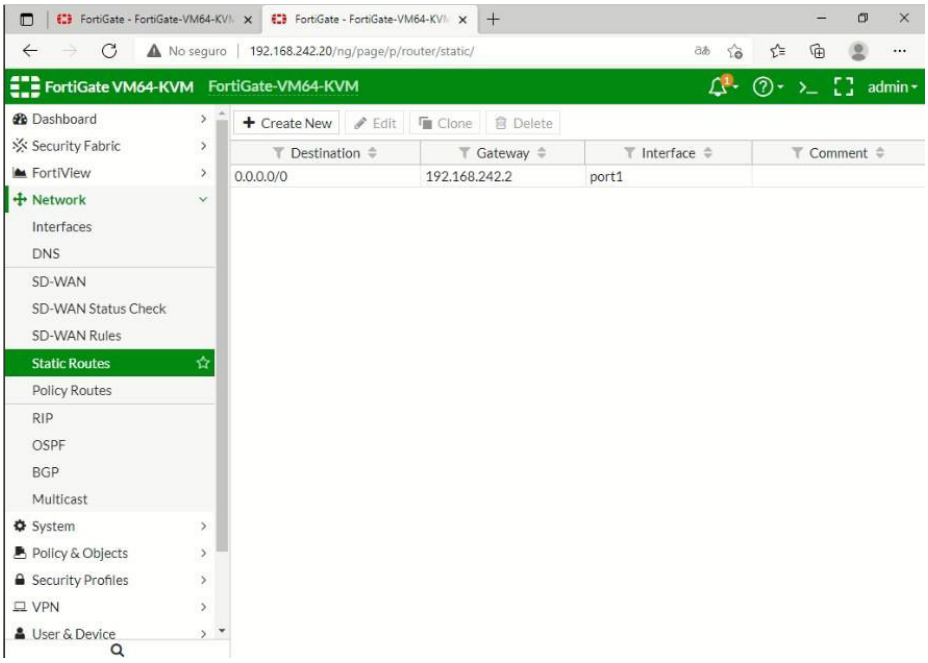


Figura 3.125 Configuración de una ruta por defecto RED2

Para poder tener un buen funcionamiento en cuanto a las reglas y aplicación de las mismas se debe implementar una dirección modificando los siguientes parámetros:

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 20.20.20.0/24
- Interface: LAN

La configuración de esta dirección establecida se puede observar en la Figura 3.126 a continuación.

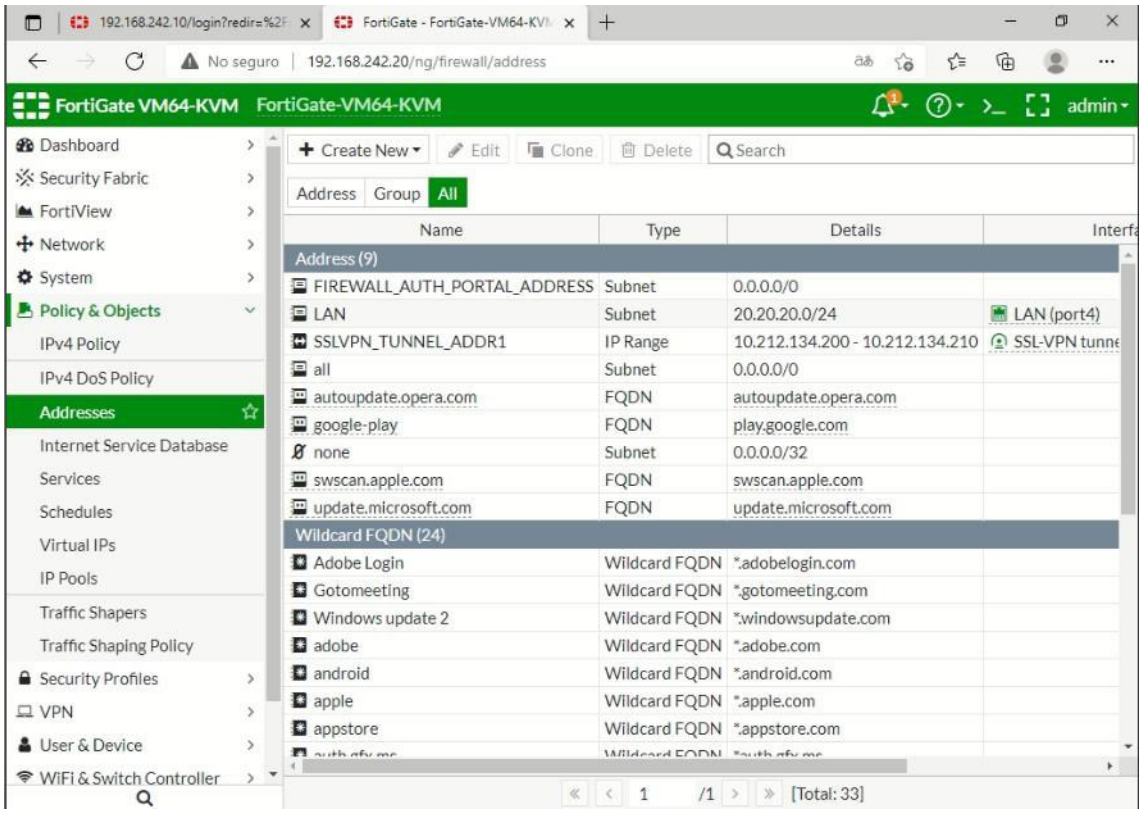


Figura 3.126 Configuración de dirección para políticas RED 2

De igual manera se proceden a implementar las diferentes políticas las cuales permitirán la circulación del tráfico en la red y hacia Internet. La primera política a configurar es la salida a Internet y para ello se modifican los siguientes parámetros:

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL

- Service: ALL

Con esta ley todos los equipos dispondrán de una conexión segura a Internet. La segunda política a establecerse es la salida de la interfaz loopback por las interfaces seriales SDWAN. Para poder realizarlo se modifican los siguientes parámetros:

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Como ya se realizó previamente se deben configurar dos políticas adicionales una tanto para tener acceso desde la red LAN hacia las interfaces SD-WAN y otra política para tener acceso desde la red SDWAN hacia la red LAN respectivamente. Estas dos políticas se detallan a continuación:

Política 1

- Name: LAN
- Incoming Interface: LAN
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política 2

- Name: LAN_1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

Para verificar el correcto funcionamiento de estas políticas se procede a notar que todas las acciones sean aceptadas como se muestra en la Figura 3.127.

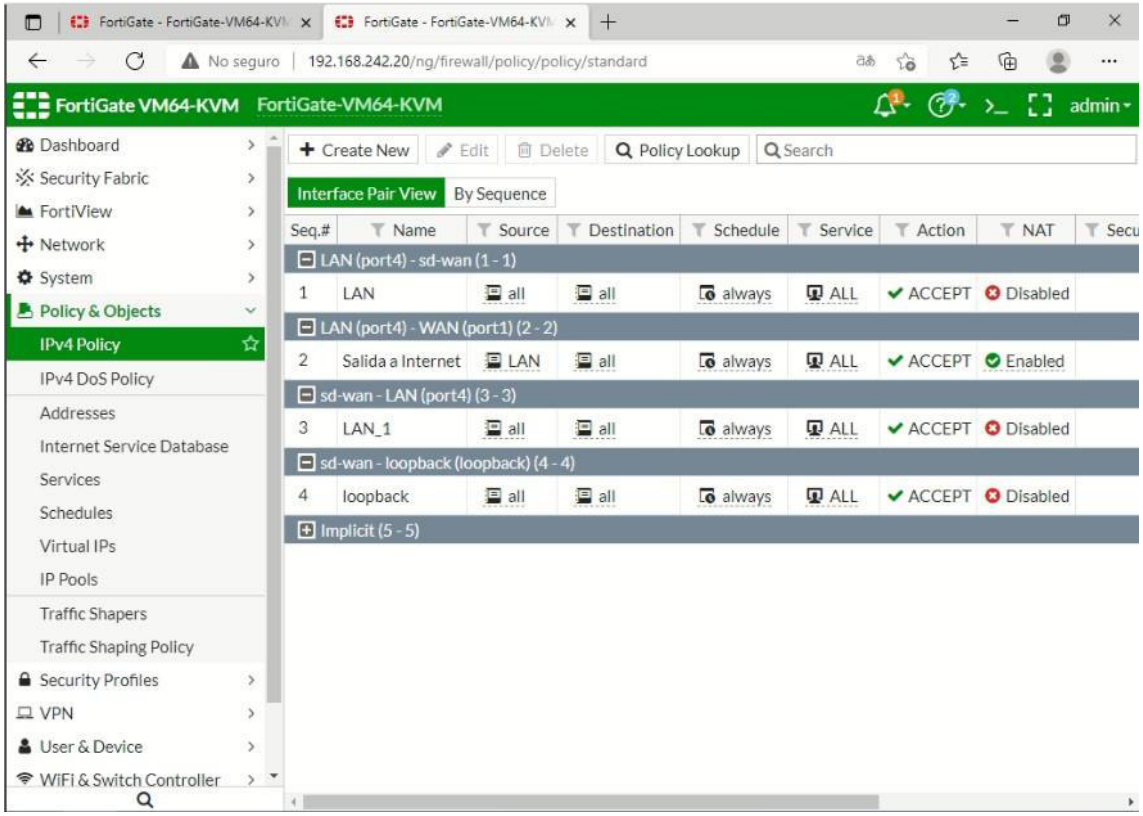


Figura 3.127 Políticas para acceso en la RED 2

Con las políticas activas se procede a configurar el protocolo de enrutamiento dinámico OPSF para hacerlo se debe asignar una ID de *router* que para este caso será de 1.1.1.2. El área con la que se va a trabajar es la misma área por defecto es decir la 0.0.0.0. Las interfaces por las cuales el protocolo debe operar son las interfaces SD-WAN pertenecientes a los enlaces ISP y las redes directamente conectadas en este equipo son las siguientes:

- 1.1.1.2/255.255.255.255
- 10.1.1.0/255.255.255.252
- 40.1.1.0/255.255.255.252
- 20.20.20.0/255.255.255.0

La configuración de este protocolo se puede observar en la Figura 3.128 a continuación.

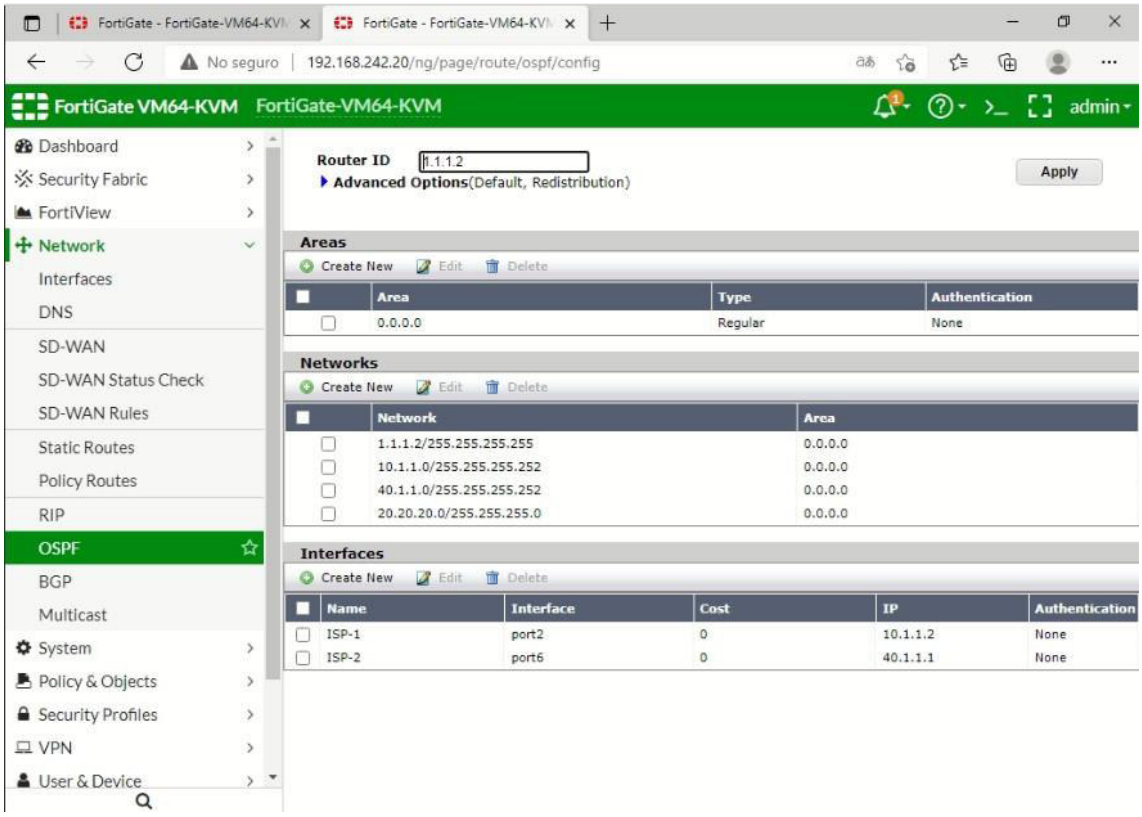


Figura 3.128 Configuración de protocolo OSPF RED 2

Finalmente se comprueban que todos los cambios fueron aplicados correctamente como se aprecia en la Figura 3.129 y la Figura 3.130.

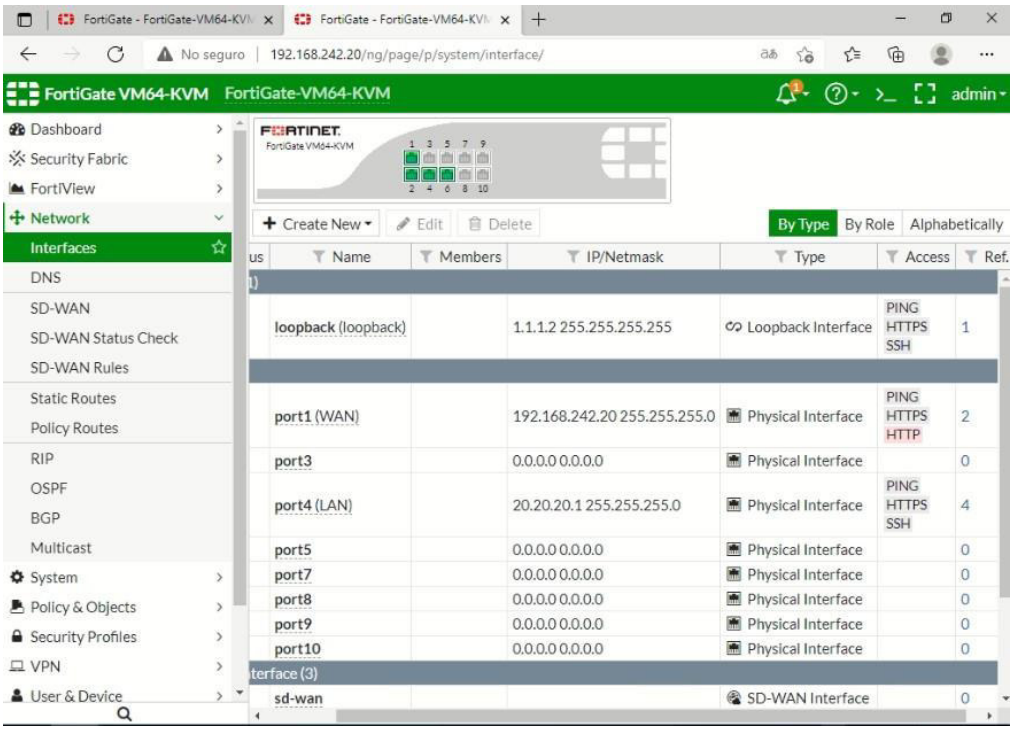


Figura 3.129 Interfaces en RED 2

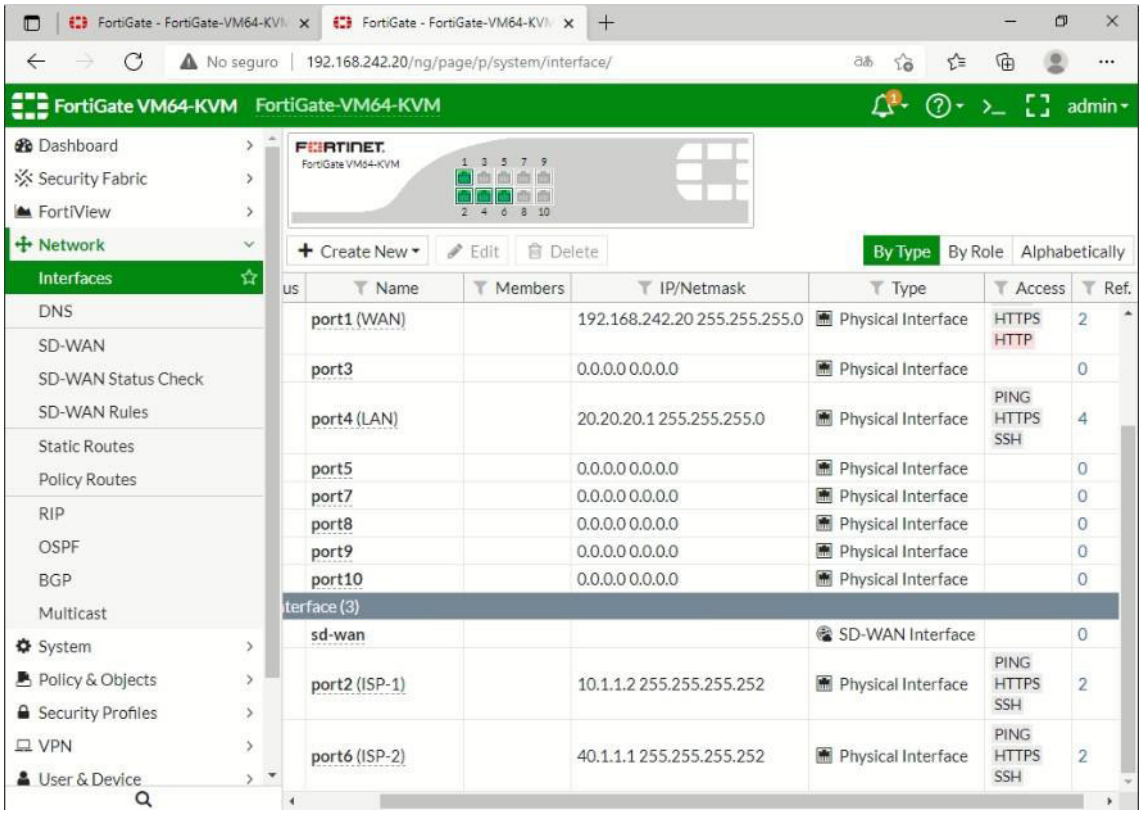


Figura 3.130 Interfaces SDWAN en RED 2

Configuración Red 3

Como ya se ha realizado en las dos redes previas para la configuración de esta red se debe acceder a la interfaz gráfica del dispositivo. Para hacerlo se debe digitar en el buscador de preferencia la dirección 192.168.242.30 y acceder con las credenciales por defecto del sistema. Una vez dentro del sistema se configurarán las diferentes interfaces, acorde a lo que se ha tratado en casos anteriores. La primera interfaz es la de salida a internet y consta de los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.30/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING

Las siguientes interfaces a configurar son las interfaces seriales del dispositivo. Las cuales recibirán el nombre de ISP mediante la aplicación de los siguientes parámetros:

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 30.1.1.1/30

- Administrative Access: HTTPS, HTTP, PING, SSH
- Alias: ISP-2
- Role: WAN
- IP/Network Mask: 20.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Una vez finalizada la configuración de estas interfaces se procede a configurar la interfaz para la red LAN mediante la aplicación de los siguientes parámetros:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 30.30.30.1/24
- Administrative Access: HTTPS, HTTP, PING,SSH

Finalmente, la interfaz que se debe configurar y que ayudará a la comunicación del dispositivo en la red es la interfaz de *loopback* y para lograrlo se aplican los siguientes parámetros:

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 2.2.2.1/32
- Administrative Access: HTTPS, PING, SSH

Todas estas configuraciones se pueden observar en la Figura 3.131 a continuación.

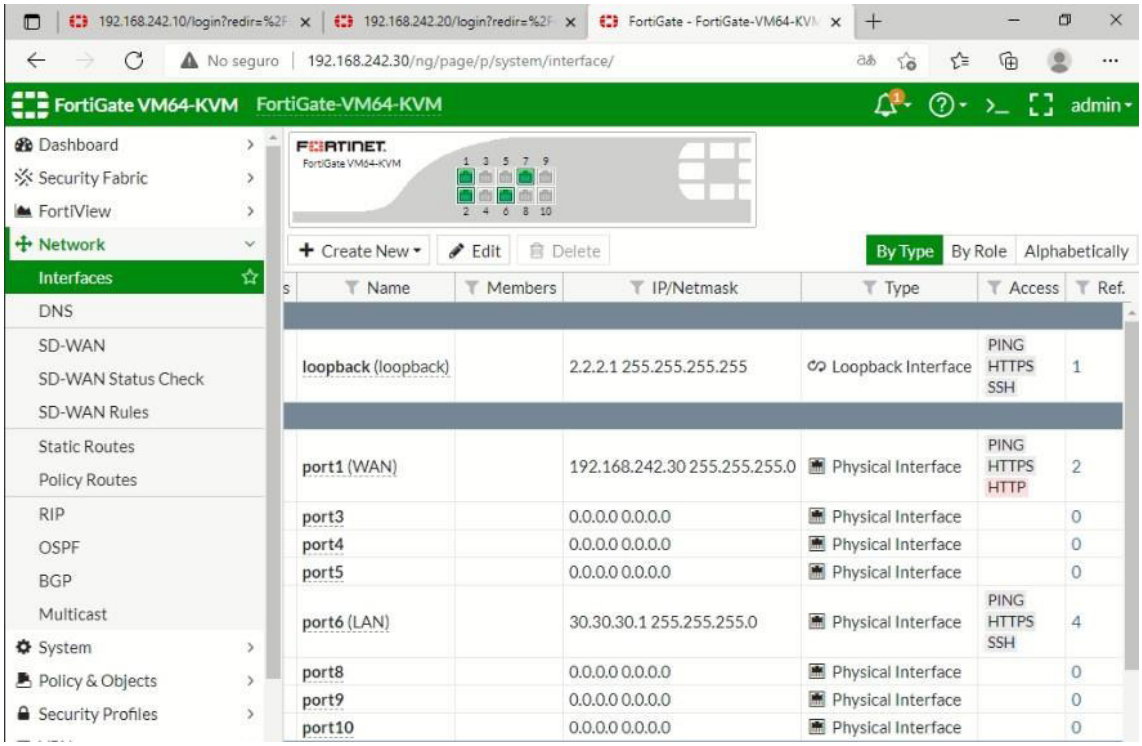


Figura 3.131 Interfaces en Fortigate RED 3

El siguiente paso a configurar es la asignación de las interfaces con sus respectivos *gateways* para las conexiones mediante SDWAN. En el caso de esta red se asignan los dos *gateways* de los dos enlaces ISP como se muestra en la Figura 3.132.

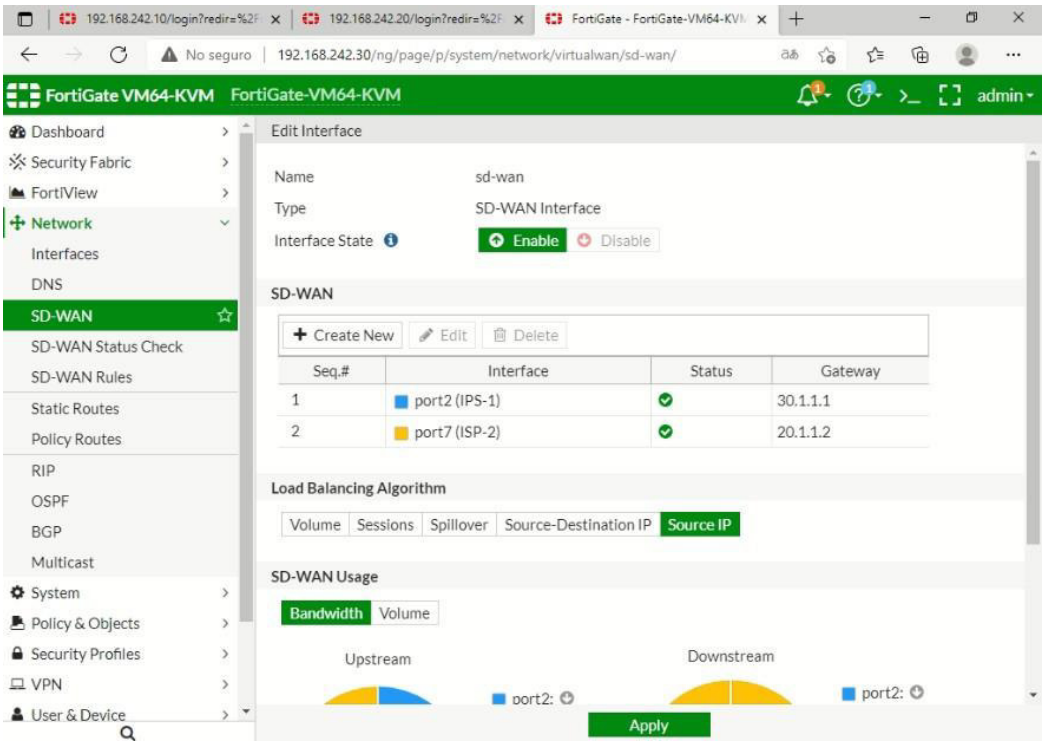


Figura 3.132 Configuración de SDWAN RED 3

Con las interfaces SDWAN definidas se proceden a establecer las diferentes reglas que manejarán estas interfaces esto mediante la aplicación de los siguientes parámetros:

- Name: LEY3
- Server: 20.1.1.2
- Timeout: 10 seconds

Una vez establecida esta ley se procede a enlazar la nueva regla a esta ley creada para ambos *gateways* por los cuales está operando la transmisión de datos por SDWAN. El procedimiento para lograrlo es el siguiente, así como se aprecia en la Figura 3.133.

- Name: ley3
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 30.1.1.1 & Gateway 20.1.1.2
- Status Check: LEY3

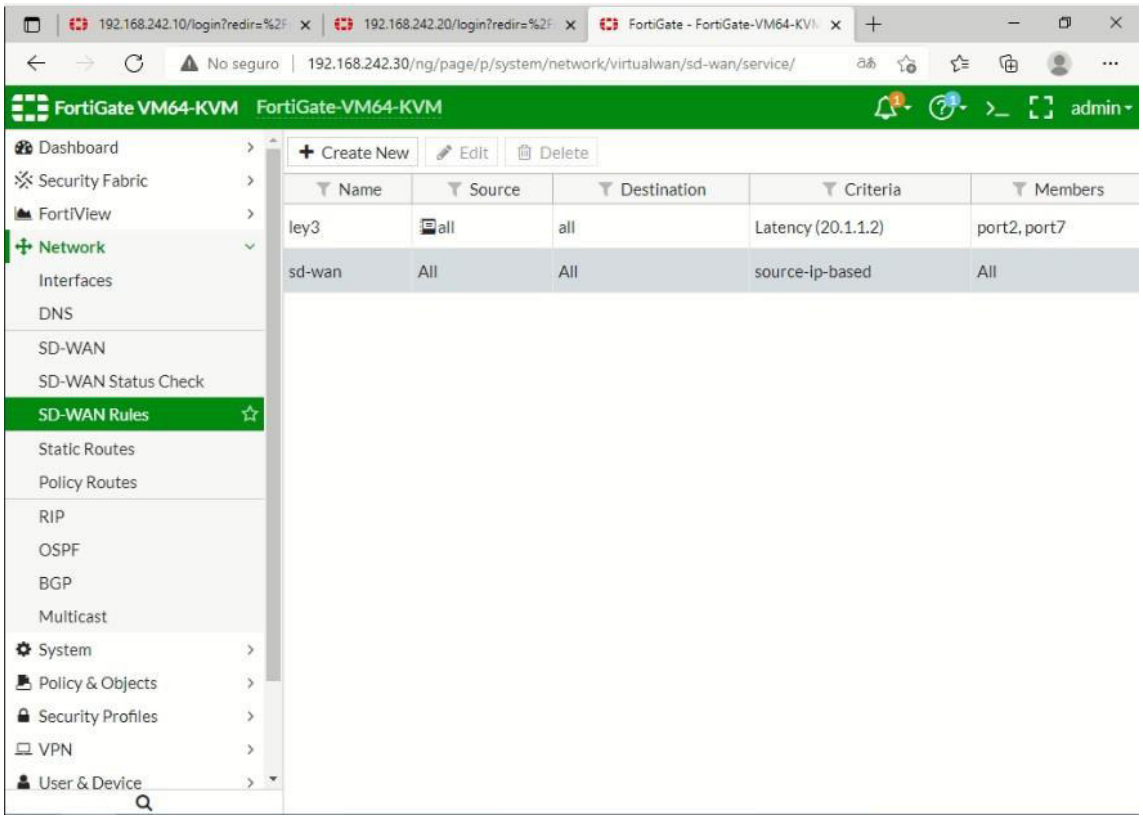


Figura 3.133 Configuración de reglas SDWAN RED 3

Una vez definidas las interfaces seriales se procede a configurar una ruta por defecto para poder salir a la Internet. Esta ruta por defecto tendrá un *Gateway* predefinido por

el sistema y para configurar esta ruta se modifican estos parámetros como se observa en la Figura 3.134.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

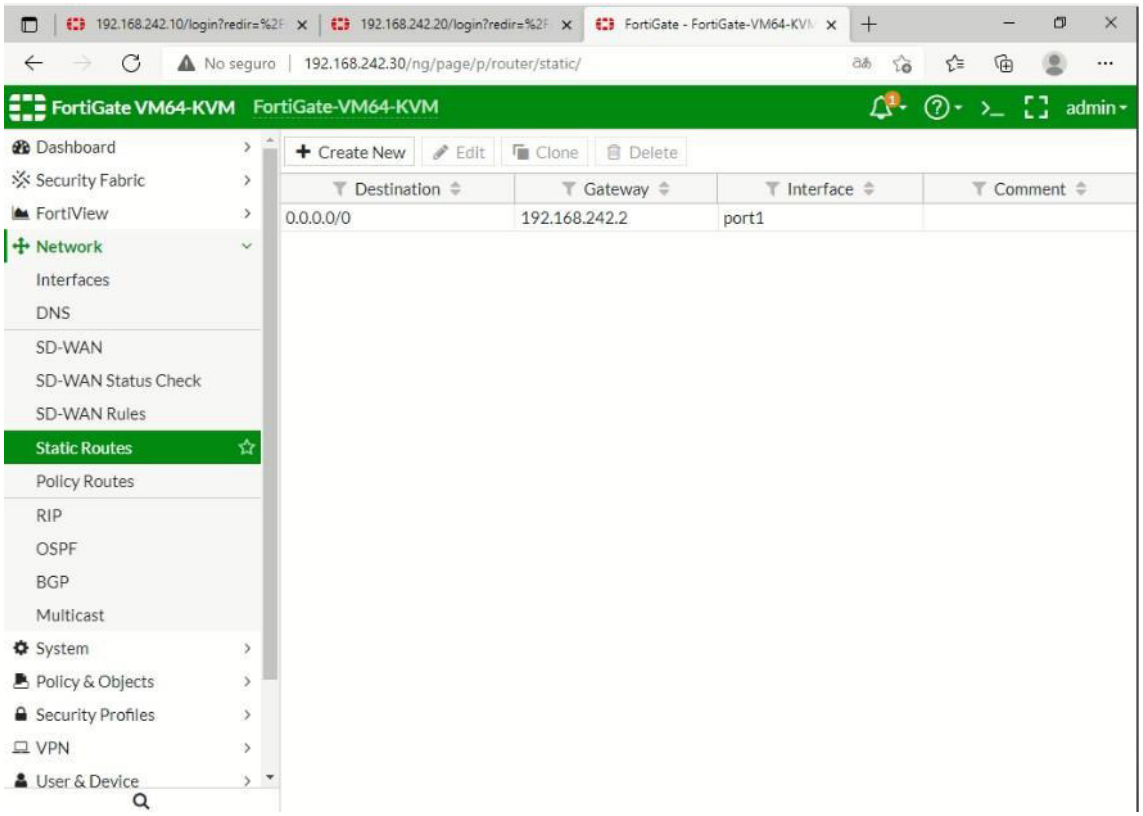


Figura 3.134 Configuración de una ruta por defecto RED 3

Una vez configurada esta ruta por defecto se procede a agregar la red LAN a los archivos de direcciones del equipo esto con el fin que en las próximas configuraciones esta red se encuentre siempre disponible. Esto se logra modificando los siguientes parámetros como se muestra en la Figura 3.135.

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 30.30.30.0/24
- Interface: LAN

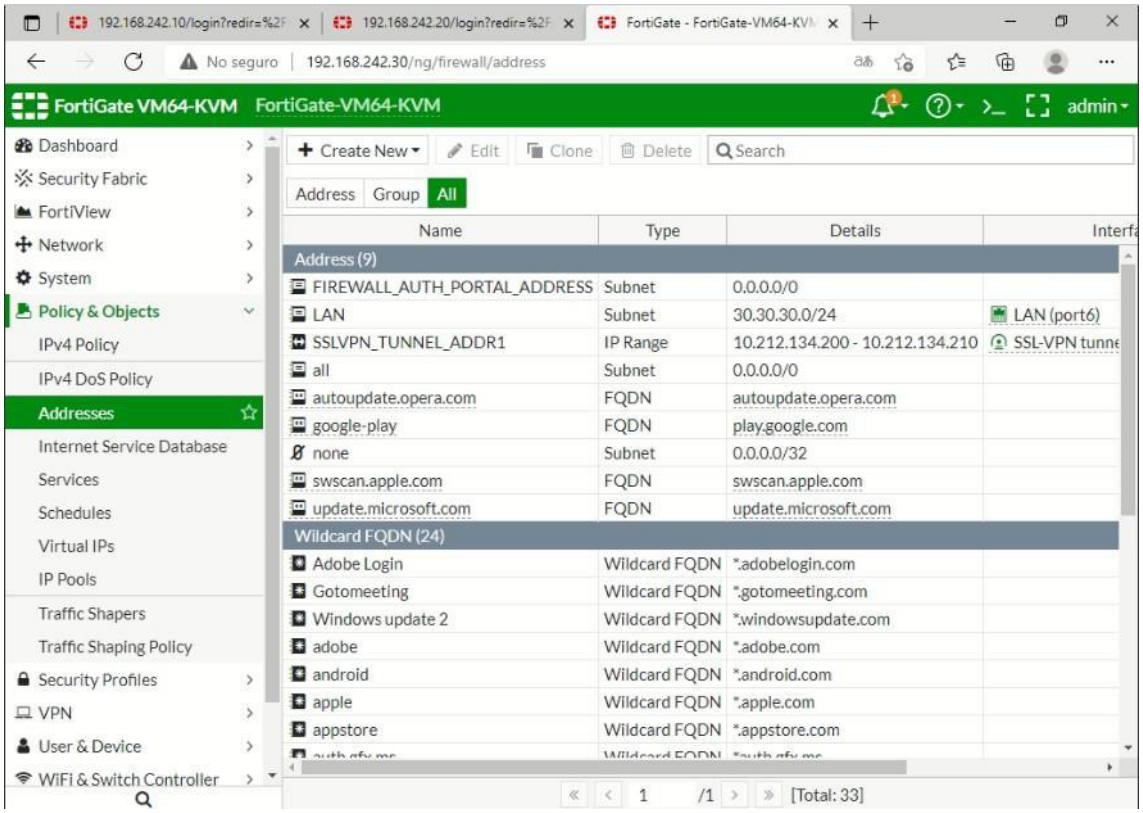


Figura 3.135 Configuración de dirección para políticas RED 3

Con todo lo anterior configurado correctamente se proceden a configurar las diferentes políticas para permitir las conexiones entrantes y salientes del equipo. La primera política que se configura es para conceder el acceso a internet a los *hosts* de la red y se lo realiza modificando los siguientes parámetros:

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

La siguiente política a configurar es la que permite que la conexión *loopback* tenga comunicación por los canales de ISP. Es decir, por medio de SDWAN y para lograrlo se modificaron los siguientes parámetros:

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan

- Source: ALL
- Destination: ALL
- Service: ALL

La tercera y la cuarta política a configurar es aquella que permite el tráfico desde la red LAN hacia SD-WAN y viceversa esto con el fin de que ningún tipo de paquete se vea perdido o comprometido de ninguna manera. Esto se realiza mediante la aplicación de los siguientes parámetros:

Política 1

- Name: LAN
- Incoming Interface: LAN
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política 2

- Name: LAN_1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

Finalmente, para conocer que todas las reglas fueron configuradas correctamente se debe acceder al apartado de IPV4 *Policy* y verificar que todas las acciones sean aceptadas como se muestra en la Figura 3.136 a continuación.

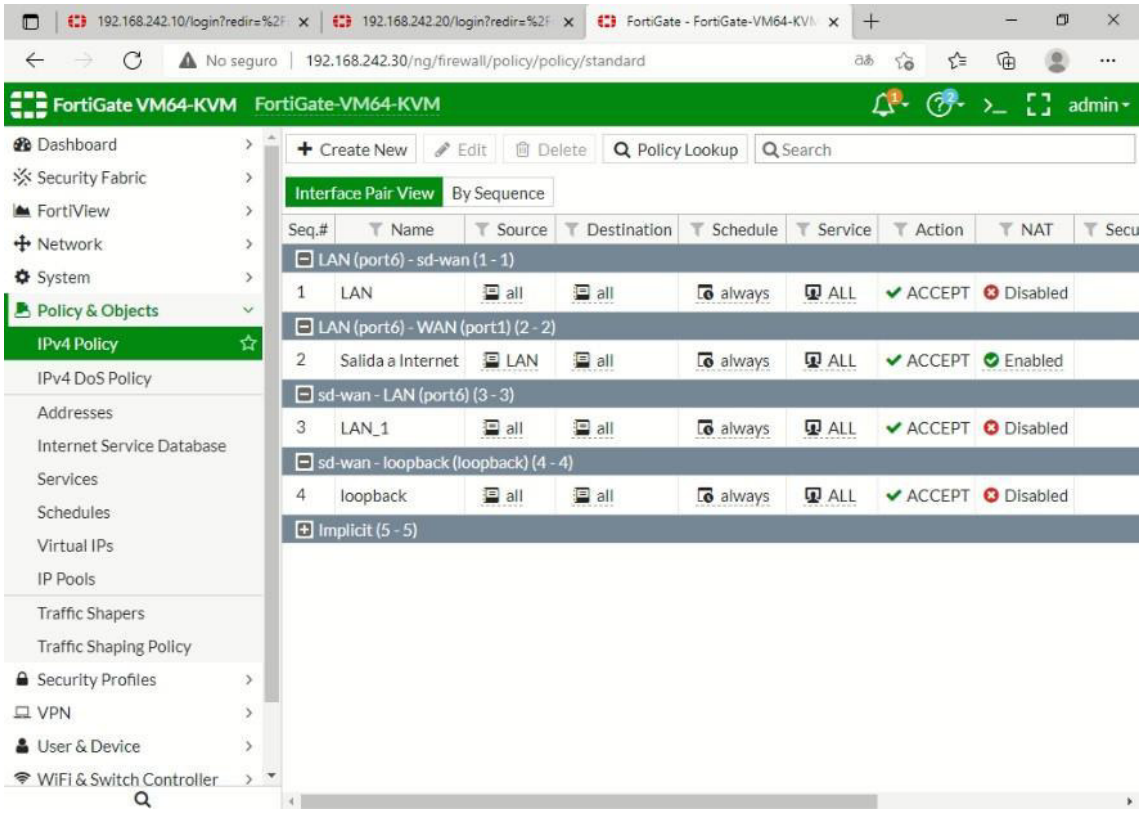


Figura 3.136 Políticas para acceso en la RED 3

Con las políticas de acceso a la red definidas se procede a configurar el protocolo de enrutamiento dinámico OSPF en esta red. Siguiendo con los lineamientos de las redes previas se establece un *router* ID que para este caso será de 2.2.2.1 y de igual manera se establecen las interfaces por las cuales viajarán los paquetes que vendrían a ser las interfaces definidas por SD-WAN ISP. Finalmente las redes que se deben hacer conocer son las siguientes mismas que se pueden apreciar en la Figura 3.137.

- 2.2.2.1/255.255.255.255
- 20.1.1.0/255.255.255.252
- 30.1.1.0/255.255.255.252
- 30.30.30.0/255.255.255.0

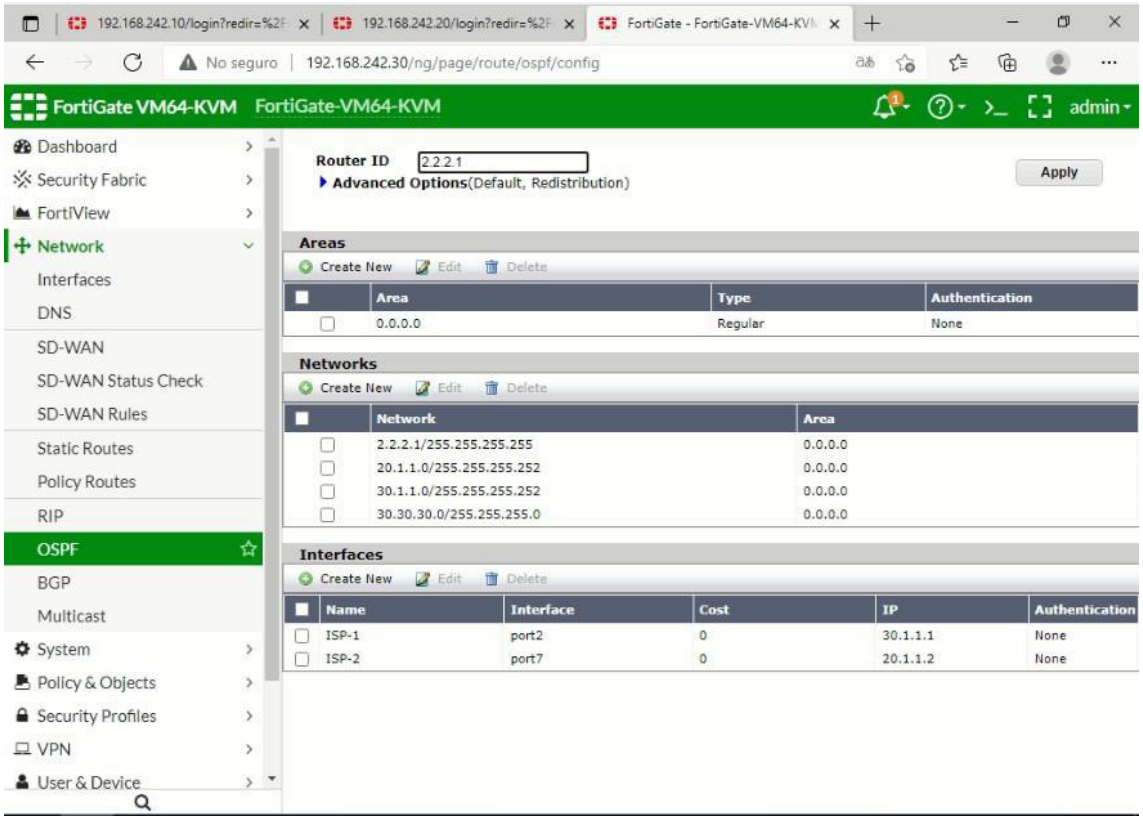


Figura 3.137 Configuración de protocolo OSPF RED 3

Con todos los cambios realizados se procede a verificar los resultados de las interfaces. Estos cambios, así como los servicios disponibles para cada una de las interfaces se pueden verificar en la Figura 3.138 y la Figura 3.139 a continuación.

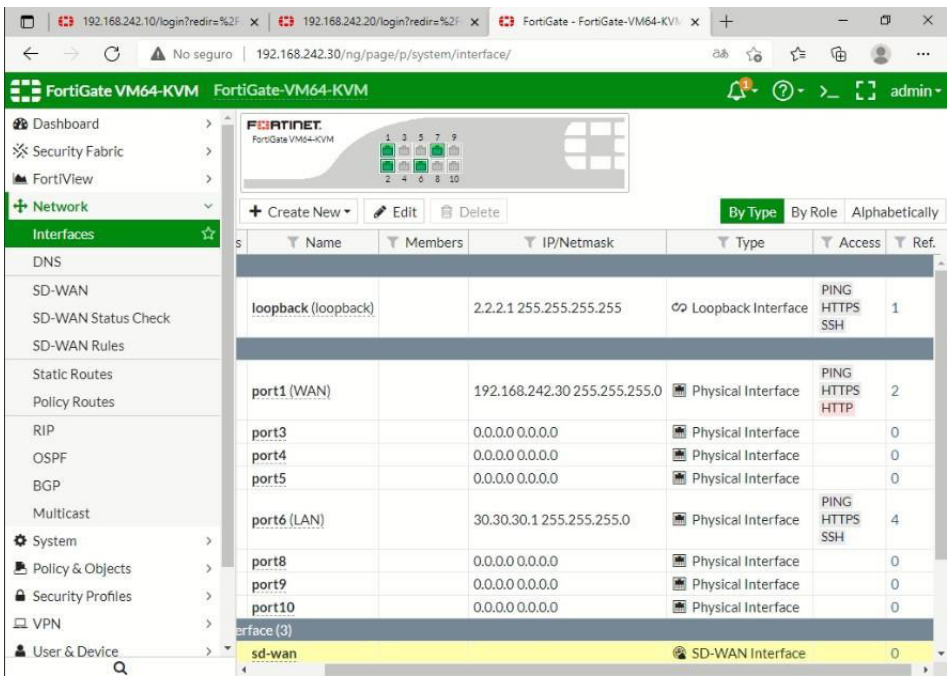


Figura 3.138 Interfaces en RED 3

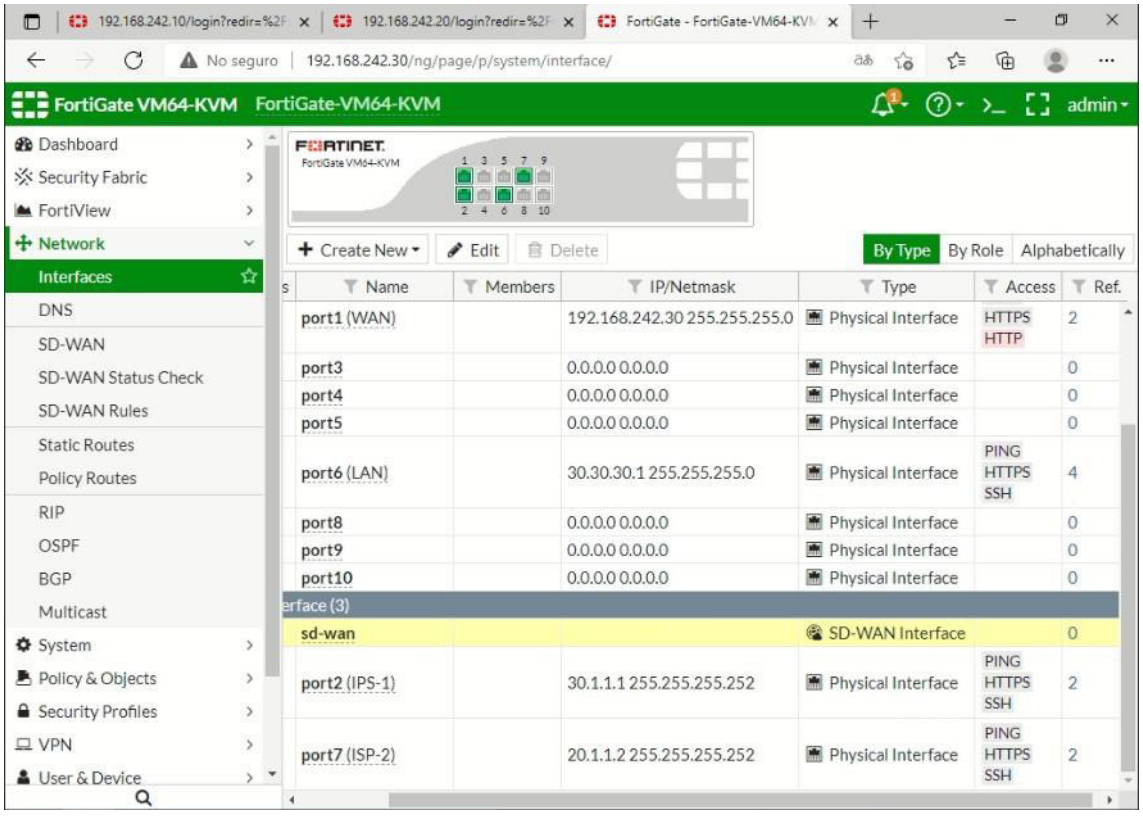


Figura 3.139 Interfaces SDWAN en RED 3

Configuración Red 4

Finalmente se configurará la cuarta red perteneciente a esta topología para ello y al igual que en casos anteriores se debe acceder a la interfaz gráfica del equipo FortiGate que para este caso será la dirección IP 192.168.242.40 y se accede de igual forma con las credenciales previamente mencionadas. Posteriormente se procede a configurar todas las interfaces conectadas al equipo, la primera interfaz a configurar es la conectada directamente a internet para lo cual se modifican los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.40/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING

Una vez configurada esta interfaz se procede a realizar la configuración de los enlaces seriales denominados IPS a los cuales posteriormente se les asignará una definición SDWAN para ello se modifican los siguientes parámetros:

- Alias: ISP-1
- Role: WAN

- IP/Network Mask: 30.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING,SSH
- Alias: ISP-2
- Role: WAN
- IP/Network Mask: 40.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Acto seguido se procede a configurar la red LAN para el equipo, esta configuración se realiza modificando los siguientes parámetros:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 40.40.40.1/24
- Administrative Access: HTTPS, HTTP, PING,SSH

El último paso para concluir con las configuraciones de las interfaces es definir una dirección de *loopback* para que pueda ser el equipo reconocido en la red y el tráfico de los paquetes se lleve a cabo satisfactoriamente. Esto se realiza modificando los siguientes parámetros:

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 2.2.2.2/32
- Administrative Access: HTTPS, PING, SSH

Estas configuraciones se pueden revisar en la Figura 3.140 a continuación:

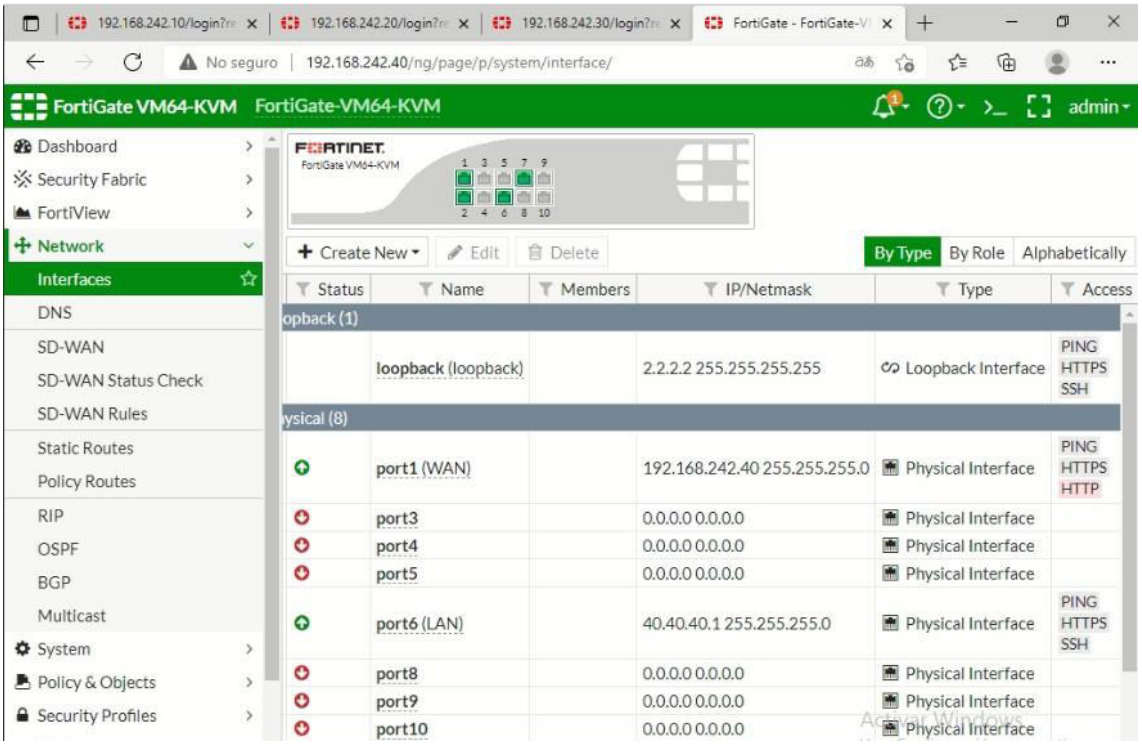


Figura 3.140 Interfaces en Fortigate RED 4

El siguiente paso a realizar es asignar las direcciones de los ISP a las interfaces de SDWAN. Para que de este modo se optimice todo el envío de paquetes este procedimiento se lleva mediante la asignación de los distintos *gateways* como se muestra en la Figura 3.141.

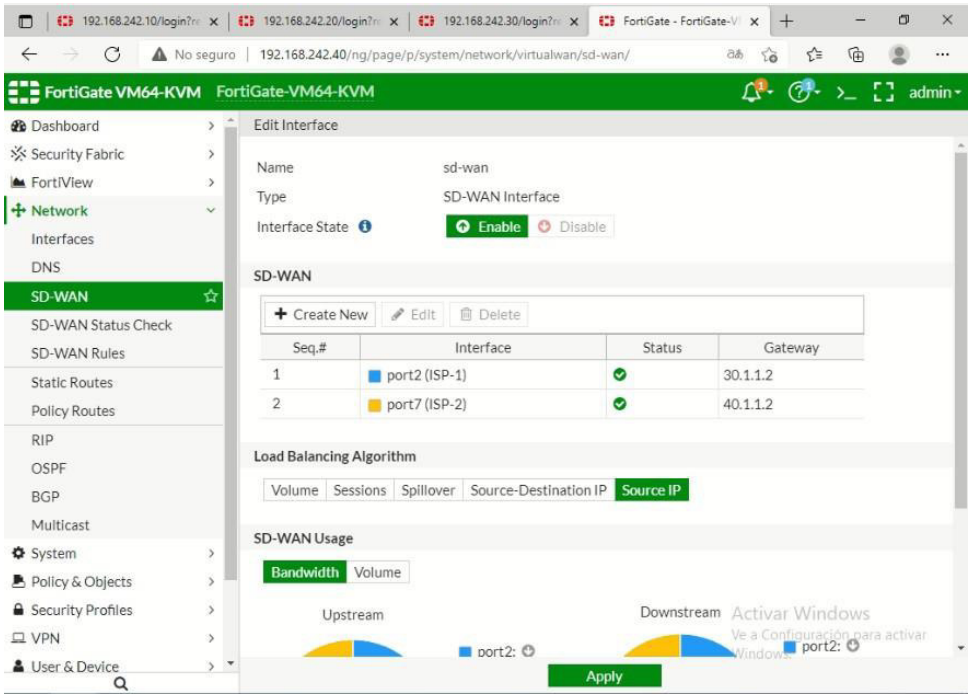


Figura 3.141 Configuración de SDWAN RED 4

Como se observó en casos previos se procede a configurar la ley definida para estas interfaces SDWAN esta acción se realiza mediante la aplicación de los siguientes parámetros:

- Name: LEY4
- Server: 30.1.1.2
- Timeout: 10 seconds

Una vez establecida esta ley se procede a configurar la regla respectiva para este caso mediante la aplicación de los siguientes parámetros. Mismos que se pueden observar en la Figura 3.142.

- Name: ley4
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 30.1.1.2 & Gateway 40.1.1.2
- Status Check: LEY4

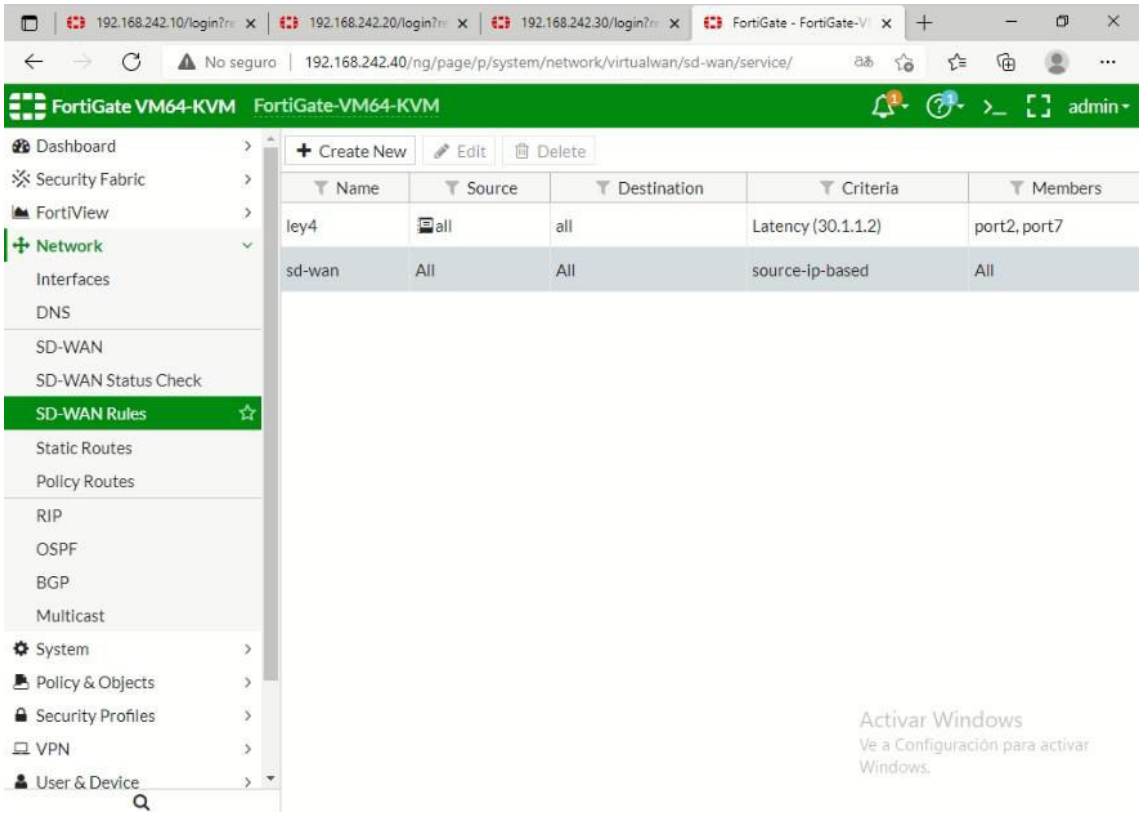


Figura 3.142 Configuración de reglas SDWAN RED 4

El siguiente paso a configurar es la aplicación de una ruta por defecto para poder salir a Internet. Los parámetros a seguir son los siguientes, como se observa en la Figura 3.143.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

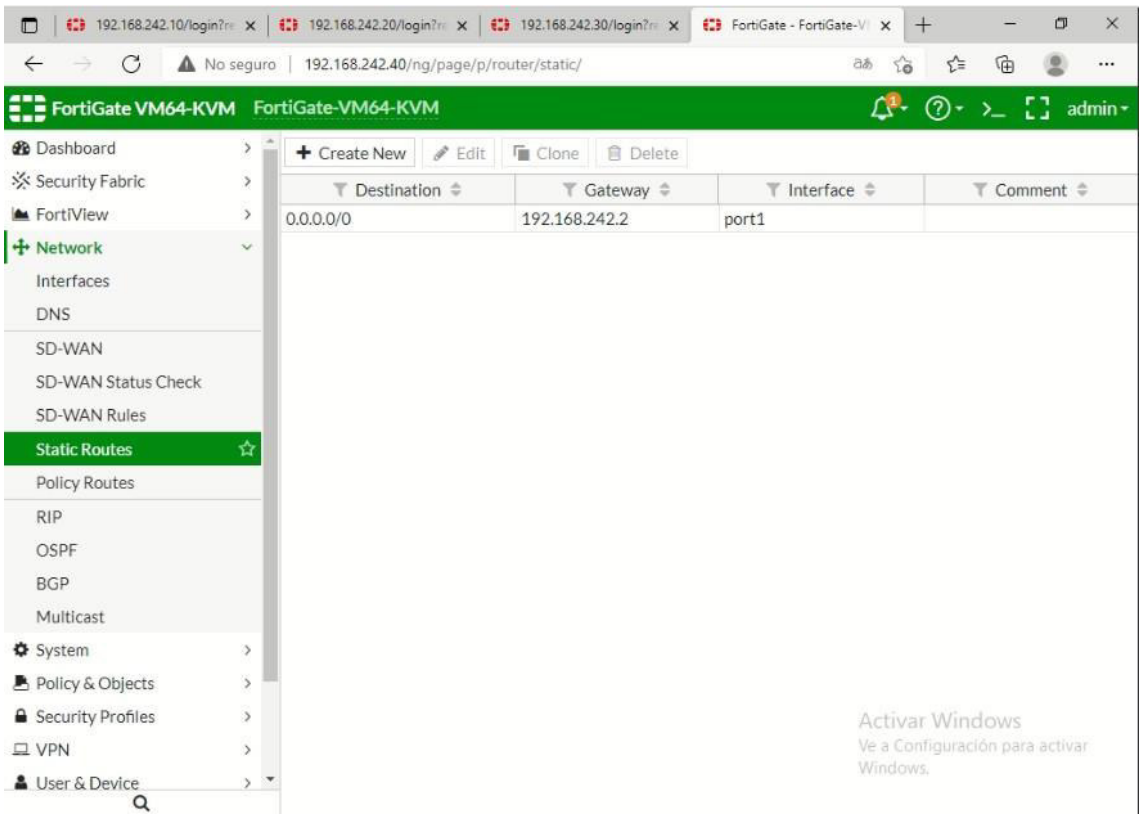


Figura 3.143 Configuración de una ruta por defecto RED 4

Al igual que en casos previos se procede a establecer una dirección LAN dentro de las configuraciones del equipo FortiGate para poder acceder a esta dirección en cualquier momento. Para lograrlo se modifican los siguientes parámetros mismos que se aprecian en la Figura 3.144.

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 40.40.40.0/24
- Interface: LAN

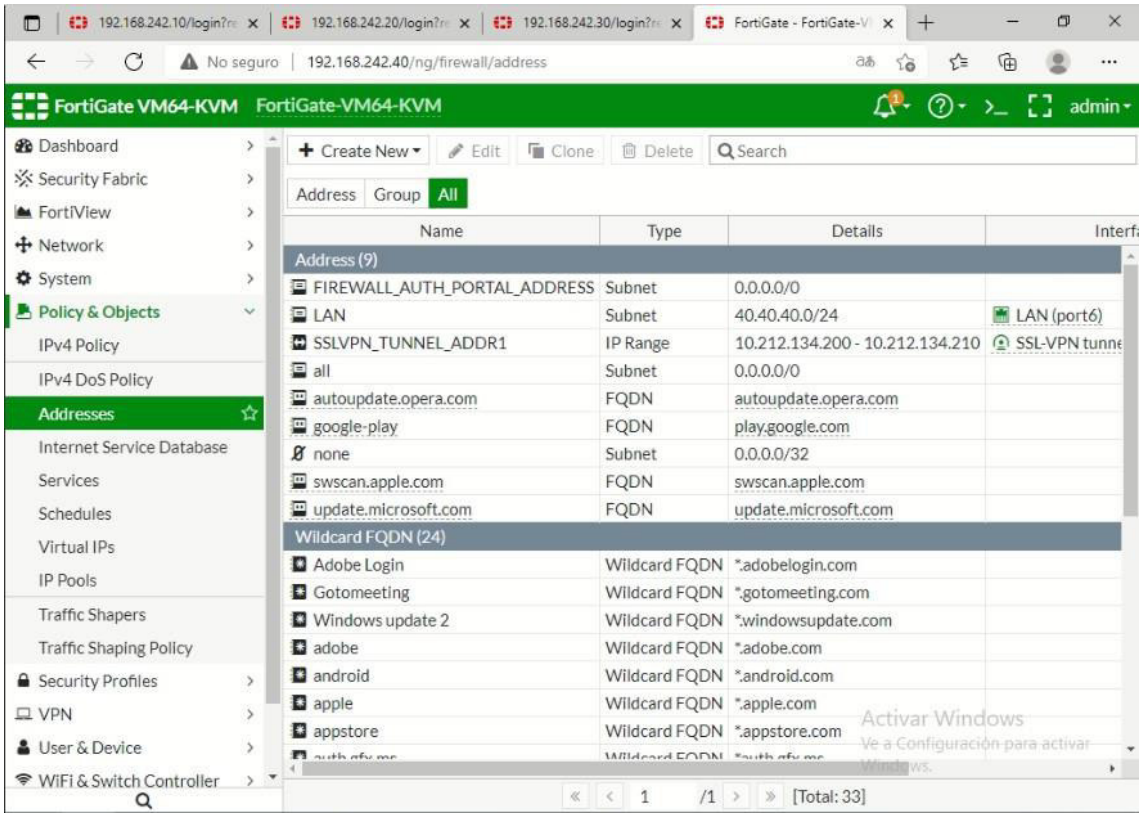


Figura 3.144 Configuración de dirección para políticas RED 4

El siguiente paso es realizar las configuraciones respectivas con respecto a las políticas del equipo las cuales siguen el mismo procedimiento previamente mencionado que se muestra a continuación:

Política de salida a internet

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

Política de salida a red por interfaz loopback

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL

- Service: ALL

Política de salida a red por interfaz LAN

- Name: LAN
- Incoming Interface: LAN
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política de retorno a la red por interfaz SDWAN

- Name: LAN_1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

Del mismo modo que en casos anteriores se procede a la comprobación de las políticas verificando que todas tengan la acción de aceptar el tráfico en la red como se muestra en la Figura 3.145.

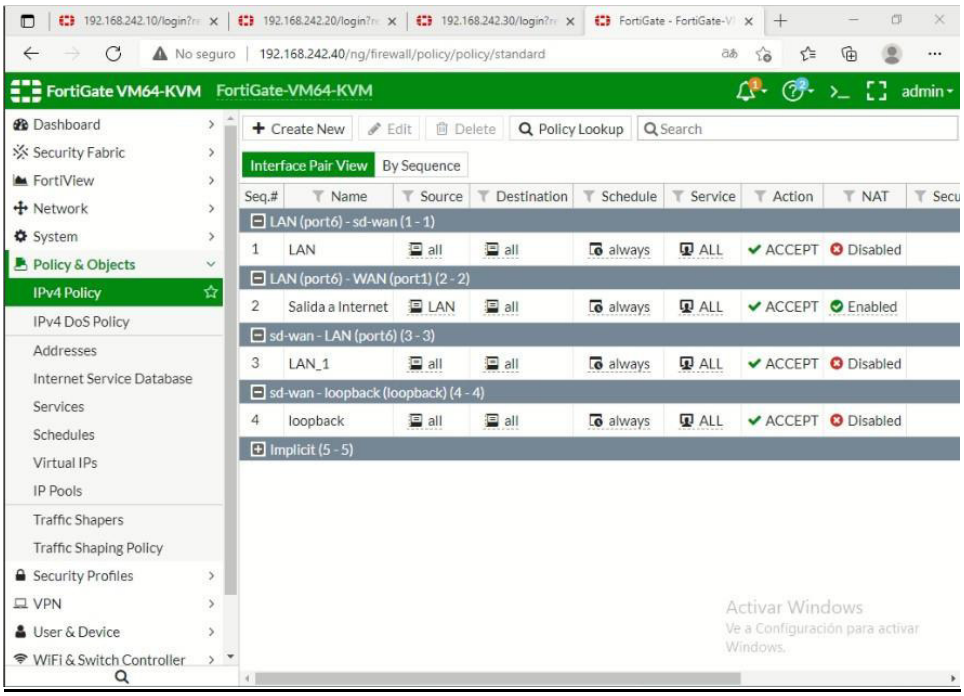


Figura 3.145 Políticas para acceso en la RED 4

Finalmente, se configura el protocolo de enrutamiento dinámico OSPF el cual se ha venido utilizando en toda la red, para ello la identificación de router será de 2.2.2.2 y las interfaces por las cuales circulará el tráfico se definen como las interfaces SDWAN. Las redes que debe conocer el protocolo para llevar a toda la red son las siguientes las cuales se observan en la Figura 3.146.

- 2.2.2.2/255.255.255.255
- 30.1.1.0/255.255.255.252
- 40.1.1.0/255.255.255.252
- 40.40.40.0/255.255.255.0

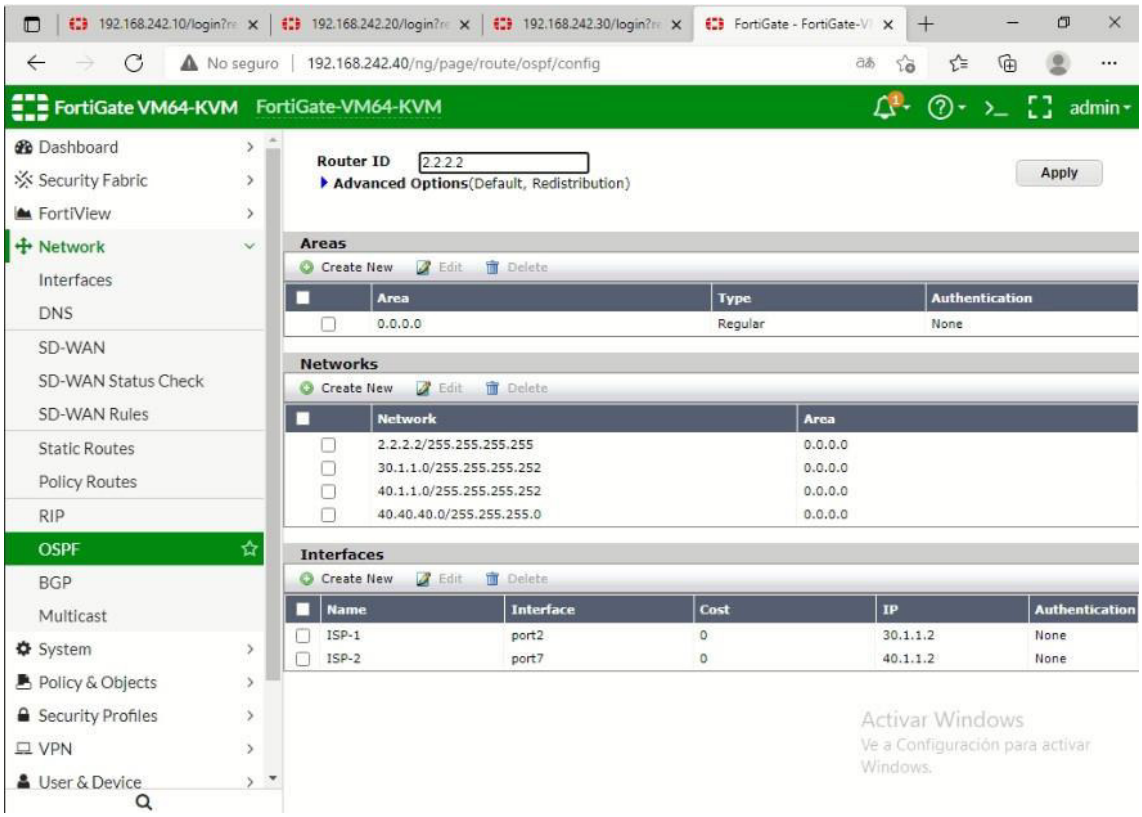


Figura 3.146 Configuración de protocolo OSPF RED 4

Para terminar con la configuración de esta red se procede a realizar una revisión final de las interfaces para corroborar que tanto las direcciones como los servicios se encuentran configurados correctamente como se muestra en la Figura 3.147 y la Figura 3.148 respectivamente.

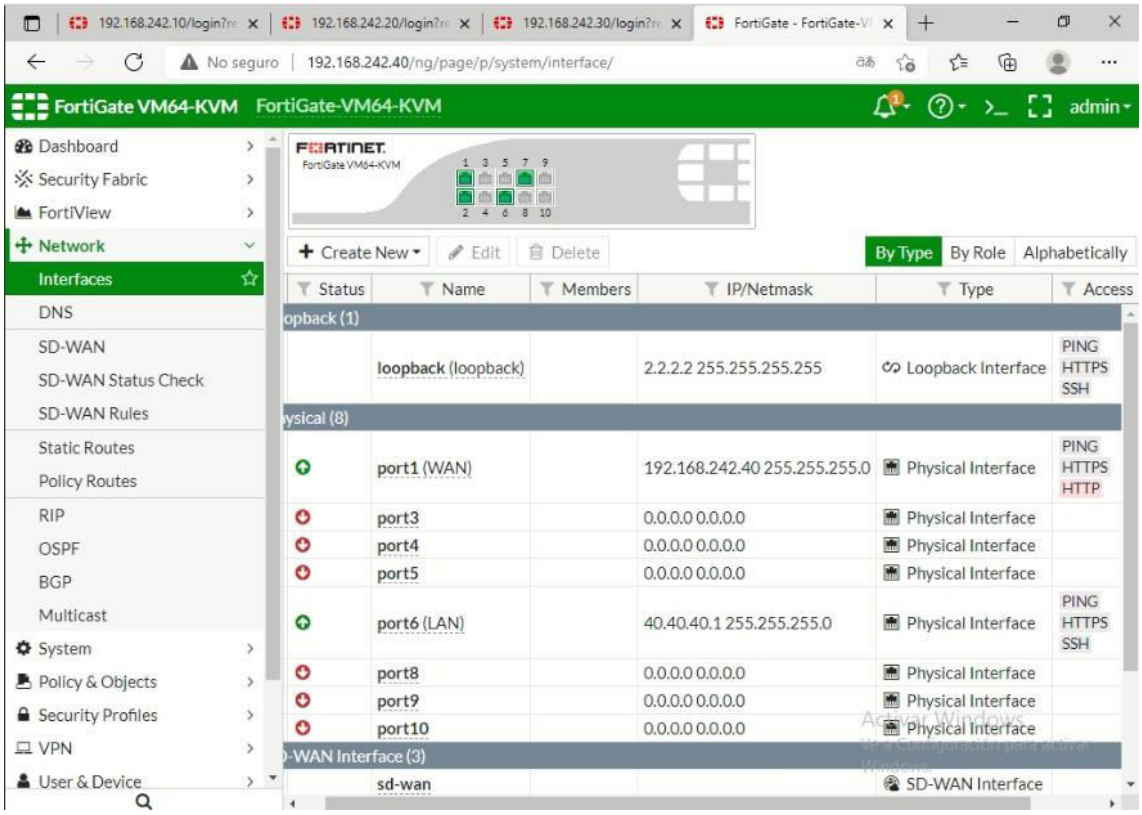


Figura 3.147 Interfaces en RED 4

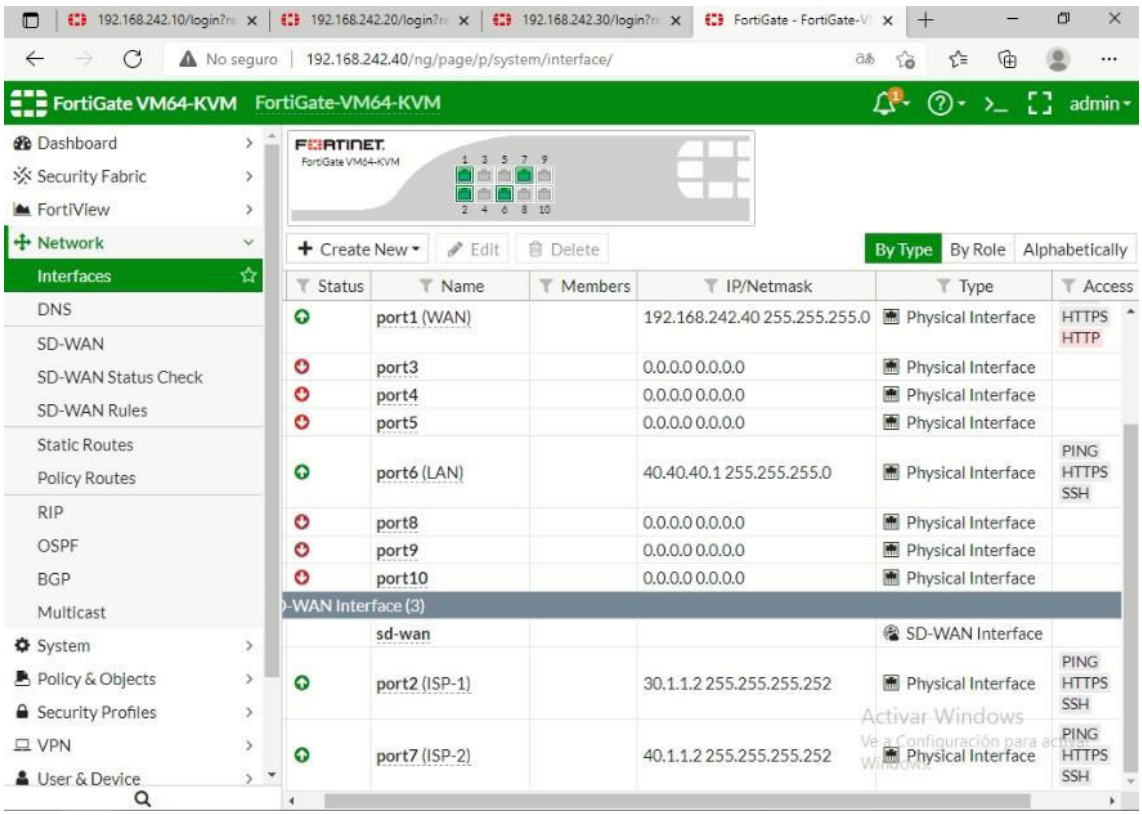


Figura 3.148 Interfaces SDWAN en RED 4

Red SDWAN-VLAN-OSPF

Para la configuración de esta red la cual dispondrá de comunicación entre dispositivos por medio del protocolo OSPF y VLANS además de contar con enlaces SDWAN en sus interfaces seriales se requerirán de los siguientes dispositivos:

- 2 equipos FortiGate 5.6.1
- 4 equipos *switch* propietarios de Cisco
- 6 computadores VPCS
- 1 nube de conexión hacia internet

Como previamente en la red anterior ya se pudo conocer el *Gateway* por defecto de la red NAT este proceso no es necesario volverlo a llevar a cabo en esta red ya que el *Gateway* por defecto pertenece a la red 192.168.242.x se puede configurar los equipos FortiGate dentro de ese rango de red. Para esta red se utilizaron las direcciones mencionadas en la Tabla 3.3 Direccionamiento RED SDWAN-VLAN-OSPF a continuación:

Tabla 3.3 Direccionamiento RED SDWAN-VLAN-OSPF

TIPO	DIRECCIÓN
SERIAL 1	10.1.1.1/30
SERIAL 2	10.1.1.2/30
RED 1	192.168.10.0/24
RED 2	192.168.20.0/24
RED 3	192.168.30.0/24
RED 4	192.168.40.0/24
RED 5	192.168.50.0/24
RED 6	192.168.60.0/24
GATEWAY INTERNET RED 1	192.168.242.60/24
GATEWAY INTERNET RED 2	192.168.242.50/24

Con las direcciones que se van a utilizar establecidas se procede a armar la topología la misma que se puede apreciar en la Figura 3.149.

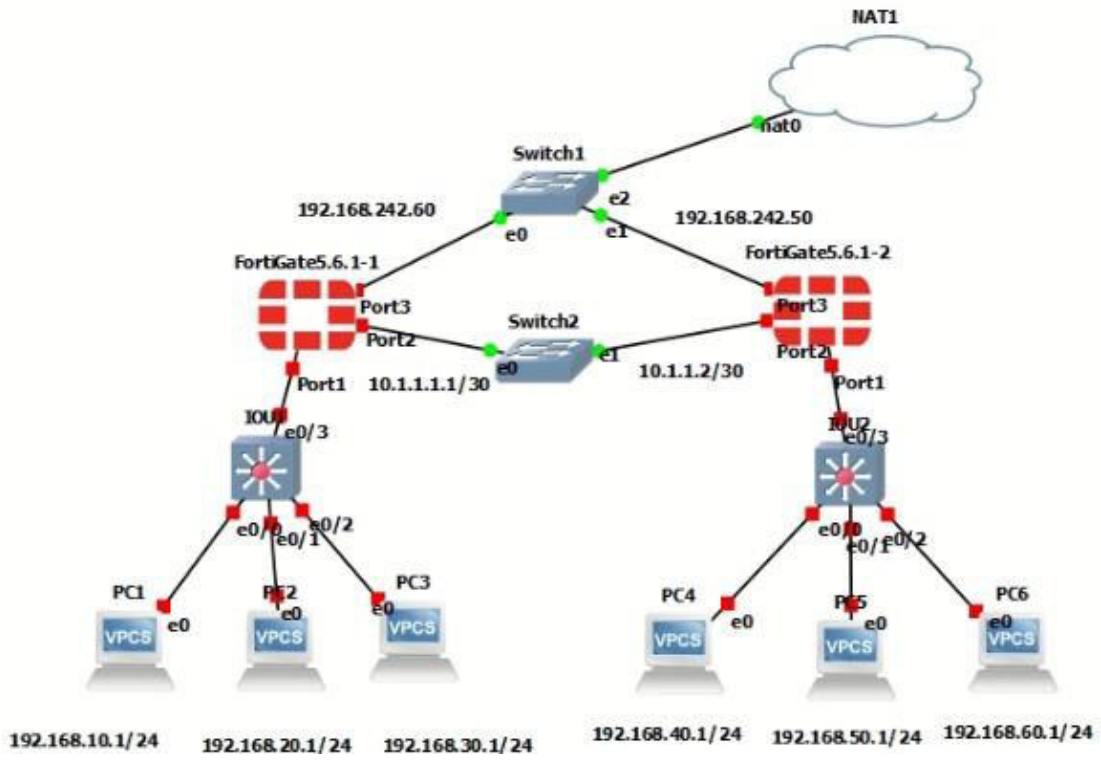


Figura 3.149 Topología Red SDWAN-VLAN-OSPF

Para la configuración de los equipos FortiGate es necesario acceder a la interfaz gráfica, por lo que estos equipos necesitan de una dirección IP que este dentro del rango del *Gateway* de salida a Internet. Para la configuración del primer equipo se implementan los siguientes comandos:

- config system interface
- edit port3
- set ip 192.168.242.60/24
- set allowaccess http ping
- end
- show system interface

Este procedimiento se realiza tanto para el primer equipo FortiGate como para el segundo ingresando los comandos respectivos que se muestran a continuación:

- config system interface
- edit port3
- set ip 192.168.242.50/24
- set allowaccess http ping
- end

- show system interface

Las configuraciones de estos dos equipos se pueden observar en la Figura 3.150 y la Figura 3.151 respectivamente presentadas a continuación:

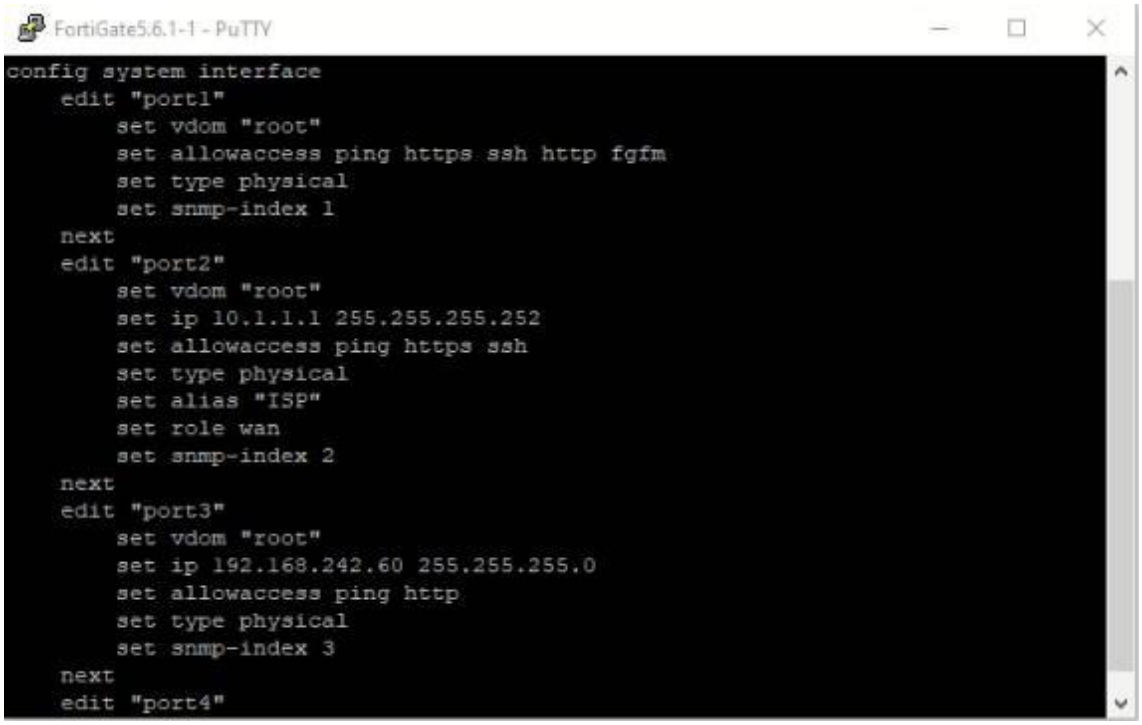


Figura 3.150 Configuración de equipo RED 1

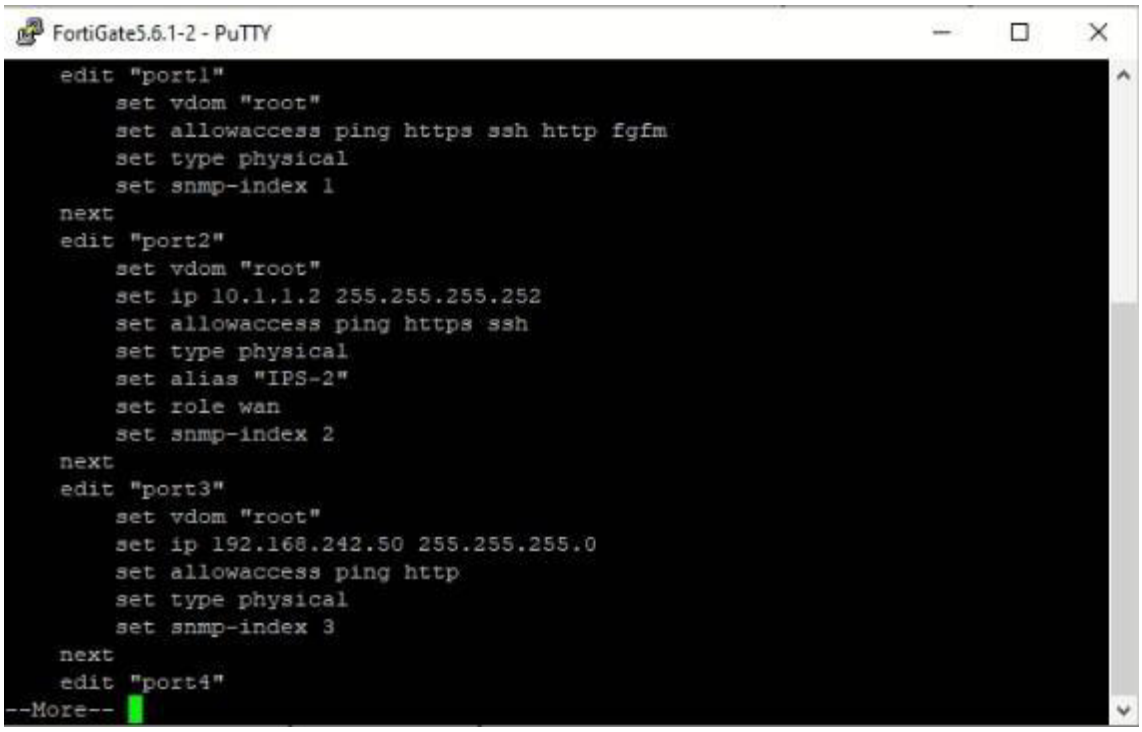


Figura 3.151 Configuración de equipo RED 2

Una vez configuradas las direcciones de los equipos FortiGate se procede a configurar las direcciones como los *gateways* de las distintas VPCS acorde a lo presentado en la Tabla 3.4.

Tabla 3.4 Direcciones y Gateways VPCS SDWAN-VLAN-OSPF

VPCS	DIRECCIÓN	GATEWAY
PC1	192.168.10.2/24	192.168.10.1/24
PC2	192.168.20.2/24	192.168.20.1/24
PC3	192.168.30.2/24	192.168.30.1/24
PC4	192.168.40.2/24	192.168.40.1/24
PC5	192.168.50.2/24	192.168.50.1/24
PC6	192.168.60.2/24	192.168.60.1/24

Configuración Red 1

Para la configuración de esta red el primer paso al igual que en casos anteriores es acceder a la interfaz gráfica de la red para ello en el buscador de preferencia se escribe la dirección del equipo es decir 192.168.242.60 y se accede con las credenciales previamente mencionadas. La primera configuración que se debe realizar es acceder al puerto al cual están conectadas todas las redes de esta parte de la topología y crear nuevas interfaces de tipo vlan, una para cada red LAN como se muestra en la Figura 3.152.

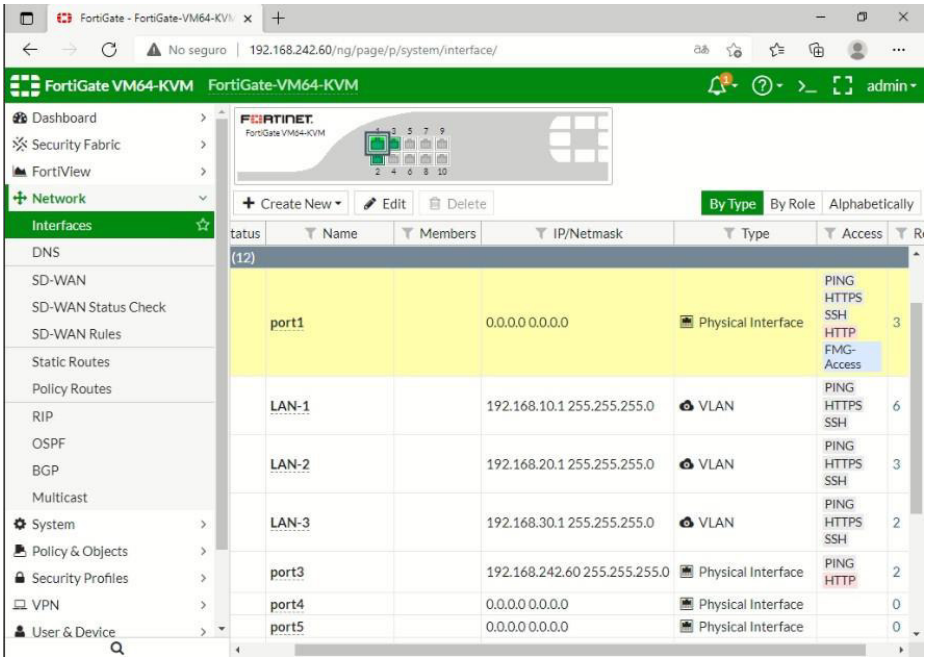


Figura 3.152 Configuración de interfaces VLAN

El siguiente paso a realizar es la configuración del enlace serial el mismo que será denominado ISP y para su configuración se modifican los siguientes parámetros:

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 10.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Adicionalmente, esta red requiere de una interfaz de tipo *loopback* ya que a través de la misma se podrá realizar el enrutamiento dinámico por medio de OSPF correctamente. Para la correcta implementación de esta interfaz se modifican los siguientes parámetros:

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 1.1.1.1/32
- Administrative Access: HTTPS, PING, SSH

La configuración de estas interfaces se muestra en la Figura 3.153.

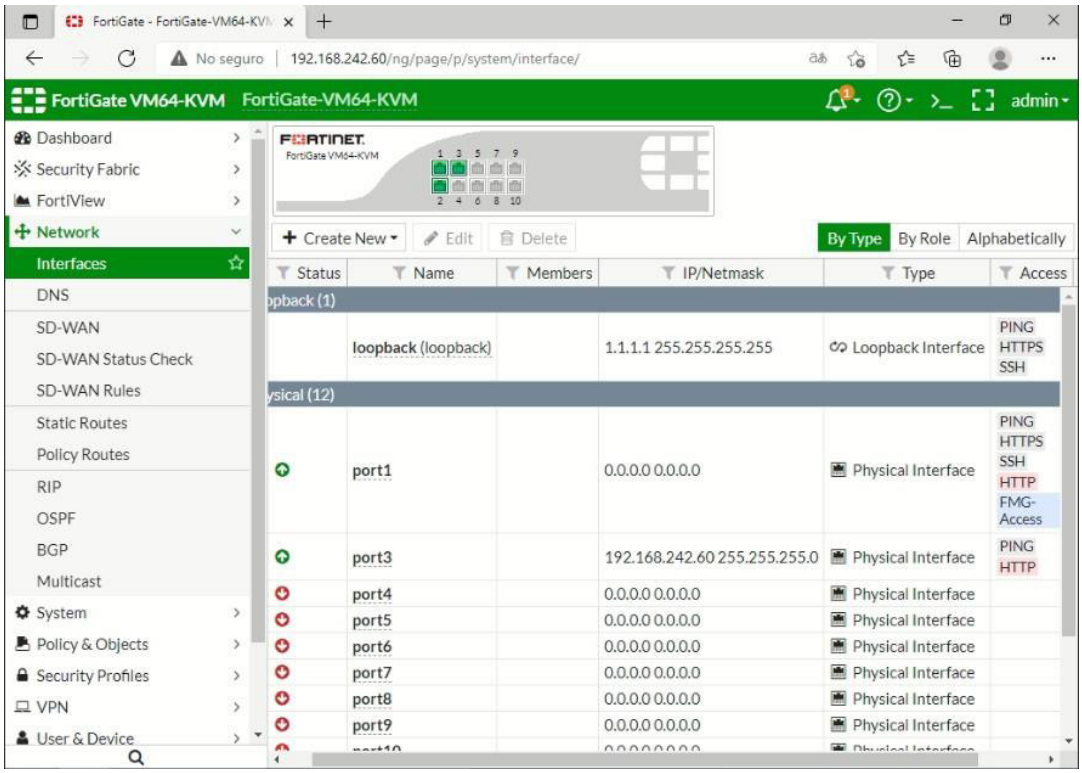


Figura 3.153 Configuración de interfaces en la red 1

Una vez establecidas todas las interfaces se procede a la correspondiente asignación del *Gateway* del enlace serial para definir este enlace como SDWAN. Para realizarlo se dirige hacia "*Network > SD-WAN*" y se coloca el *Gateway* del enlace ISP como se muestra en la Figura 3.154.

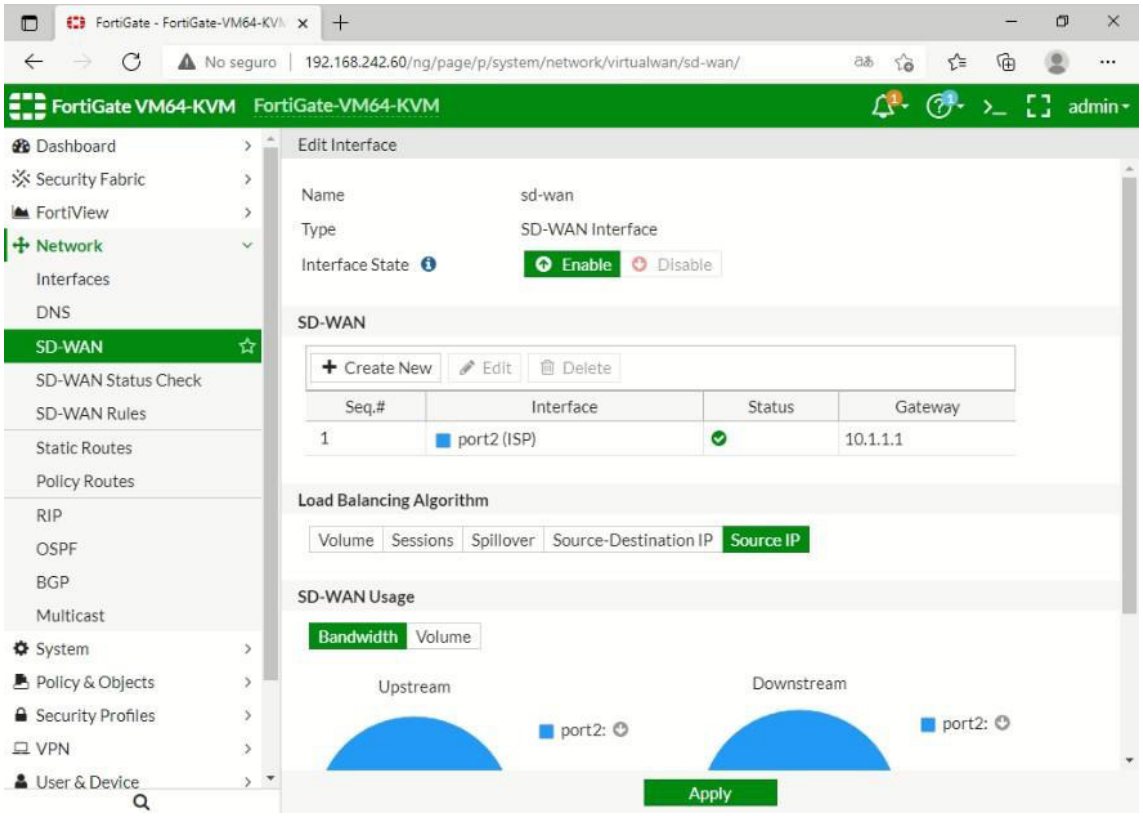


Figura 3.154 Configuración de enlace SDWAN en la red 1

Una vez establecida la interfaz respectiva para SDWAN se accede al apartado de *"SD-WAN Status Check*" para implementar la ley respectiva como ya se lo explicó previamente. Los parámetros a cambiar en esta parte son los siguientes:

- Name: VOICE
- Server: 10.1.1.1
- Timeout: 10 seconds

Una vez configurada la ley se procede a implementar la regla que ayudará a mantener un control, sobre todo el tráfico que proviene de las interfaces VLAN hacia la red 2. Para configurar correctamente se modifican los siguientes parámetros los cuales se observan en la Figura 3.155.

- Name: voice
- Source Address: All

- Destination Address: All
- Interface Members: Gateway 1.1.1.1
- Status Check: VOICE

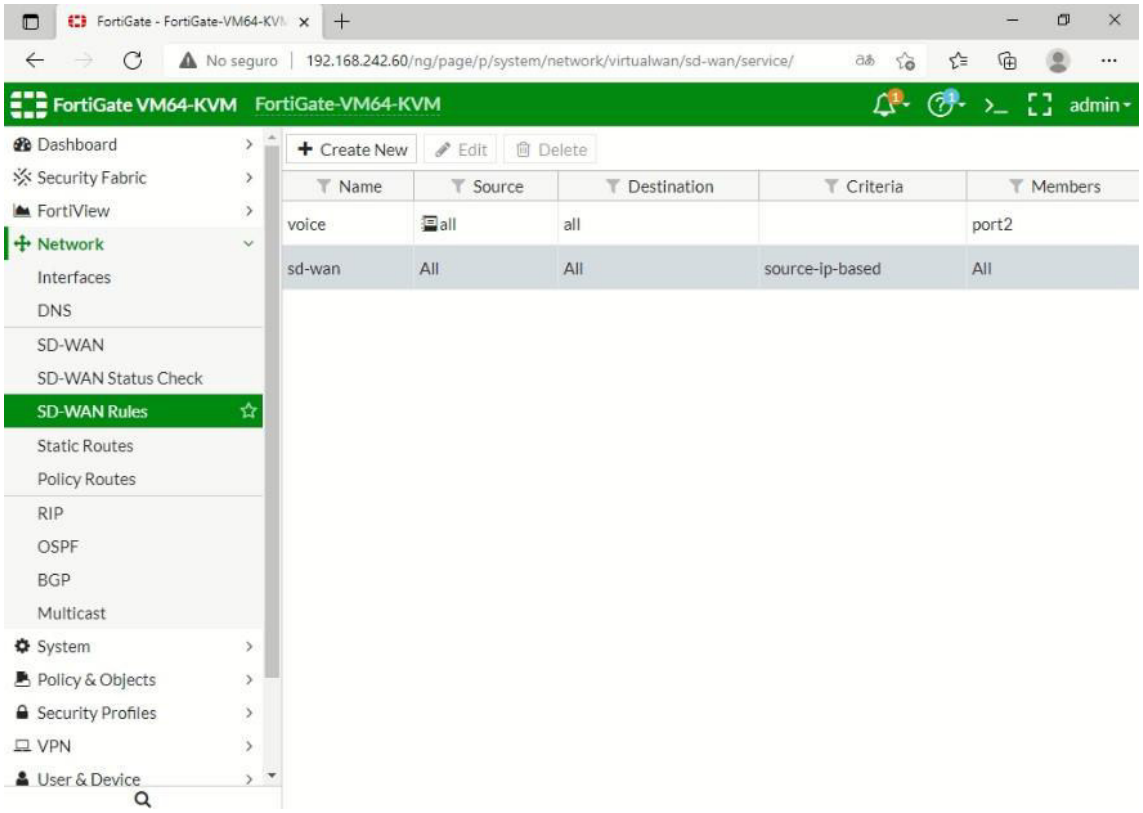


Figura 3.155 Configuración de reglas SDWAN en la red 1

Adicionalmente para lograr una comunicación con internet se procede a establecer una ruta por defecto haciendo uso del *Gateway* predefinido de la red y accediendo al apartado "*Network* > *Static Routes".* Se procede a modificar los siguientes parámetros los mismos que se encuentran especificados en la Figura 3.156.

- Destination: 0.0.0.0/0.0.0.0
- Device: Port3
- Gateway: 192.168.242.2

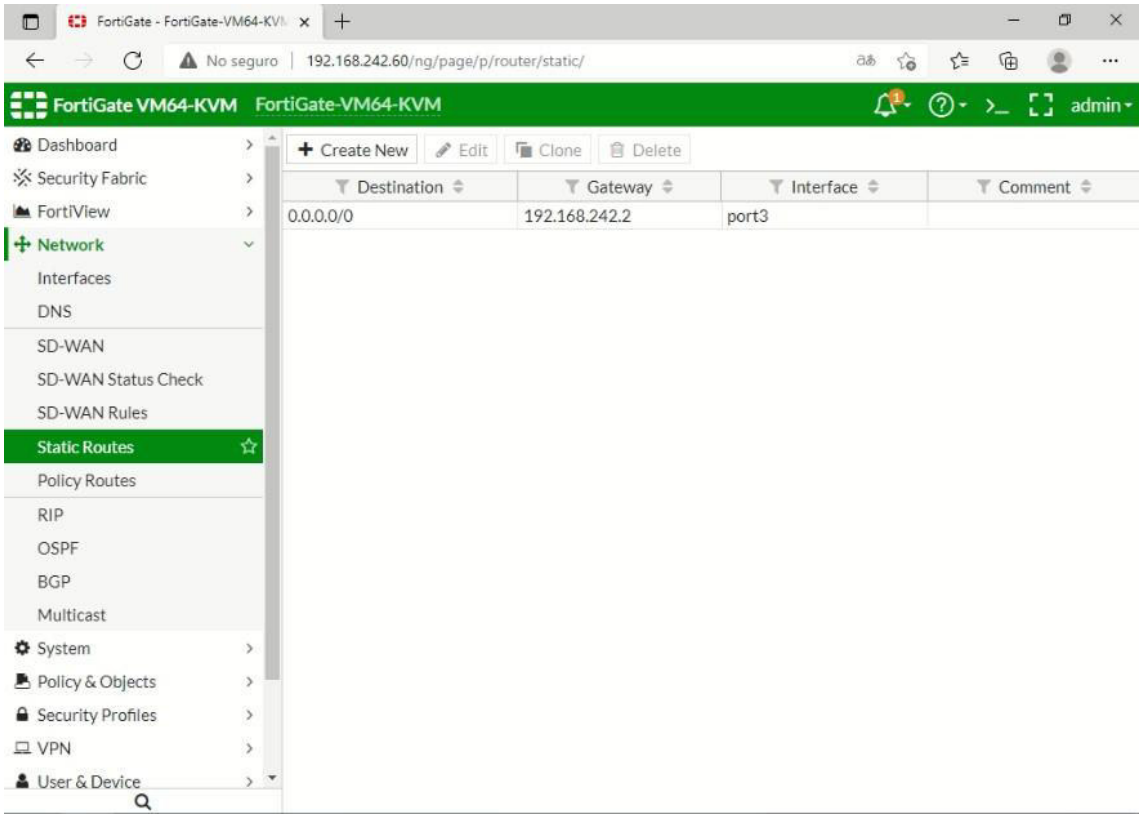


Figura 3.156 Configuración de una ruta por defecto en la red 1

Para poder configurar las políticas de conexión, previamente se debe añadir las direcciones IP de las interfaces VLAN dentro del equipo, esto con el fin de tener estas direcciones disponibles en cualquier momento. Para realizar esta acción se accede al apartado *"Policy & Objects > Addresses"* y se modifican los siguientes parámetros los mismos que se aprecian en la Figura 3.157.

VLAN 1

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.10.0/24
- Interface: LAN

VLAN 2

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.20.0/24
- Interface: LAN

VLAN 3

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.30.0/24
- Interface: LAN

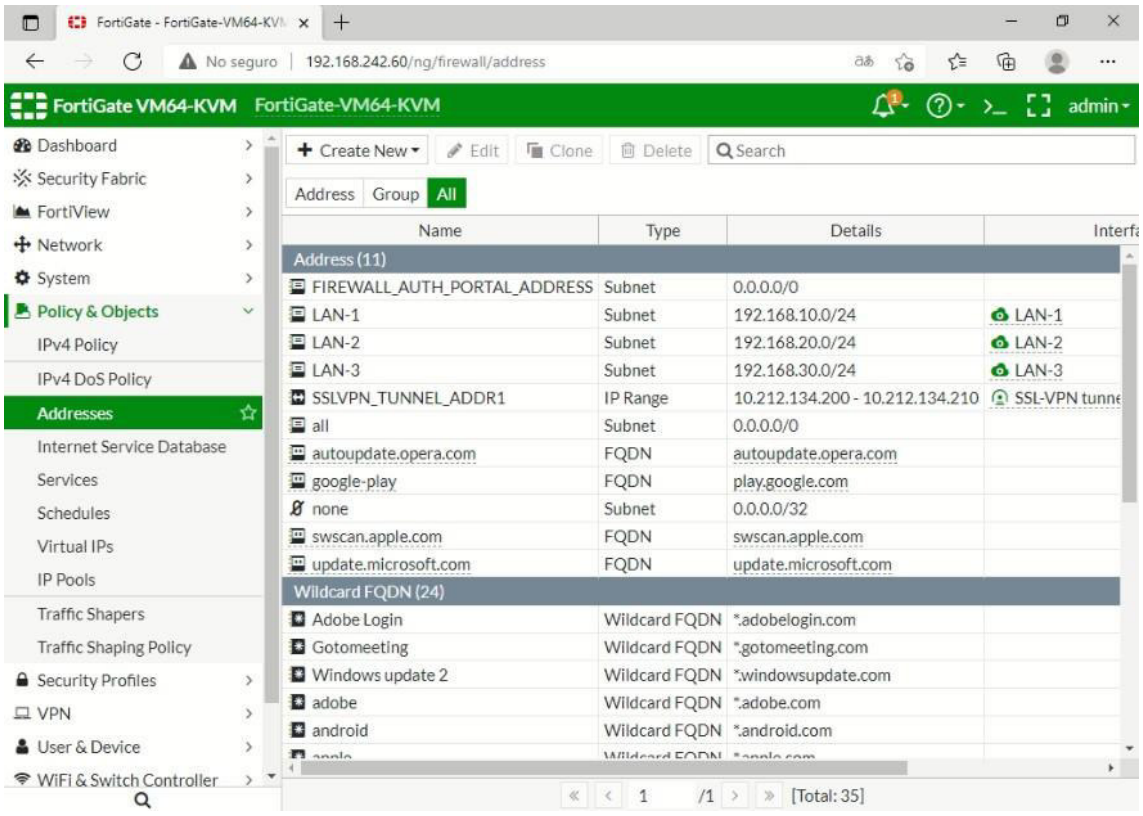


Figura 3.157 Configuración de dirección para políticas en la primera red

Una vez establecidas las direcciones, se procede a la configuración de las políticas respectivas tanto para la conexión de las interfaces a internet como para la comunicación entre vlans de la primera red. La primera política a implementar es la conexión hacia internet para lo cual se siguen estos parámetros:

- Name: WAN
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

A continuación, se muestran las políticas para el enrutamiento estándar que se ha venido realizando durante este proyecto. Estas políticas no cambian ya que son las políticas necesarias para la comunicación por protocolo OSPF.

Política de salida a red por interfaz loopback

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política de salida a red por interfaz LAN

- Name: LAN
- Incoming Interface: LAN-1
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política de retorno a la red por interfaz SDWAN

- Name: LAN.1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

Finalmente, una de las políticas importantes en este apartado es la política para el establecimiento de una comunicación entre vlans de la misma red; para lograrlo se modifican los siguientes parámetros:

- Name: LAN TO LAN 1&2
- Incoming Interface: LAN 1
- Outgoing Interface: LAN 2
- Source: ALL
- Destination: ALL

- Service: ALL

Para comprobar que todas las políticas se ejecutaron correctamente se procede a verificar en el apartado de "*Policy & Objects"* como se muestra en la Figura 3.158.

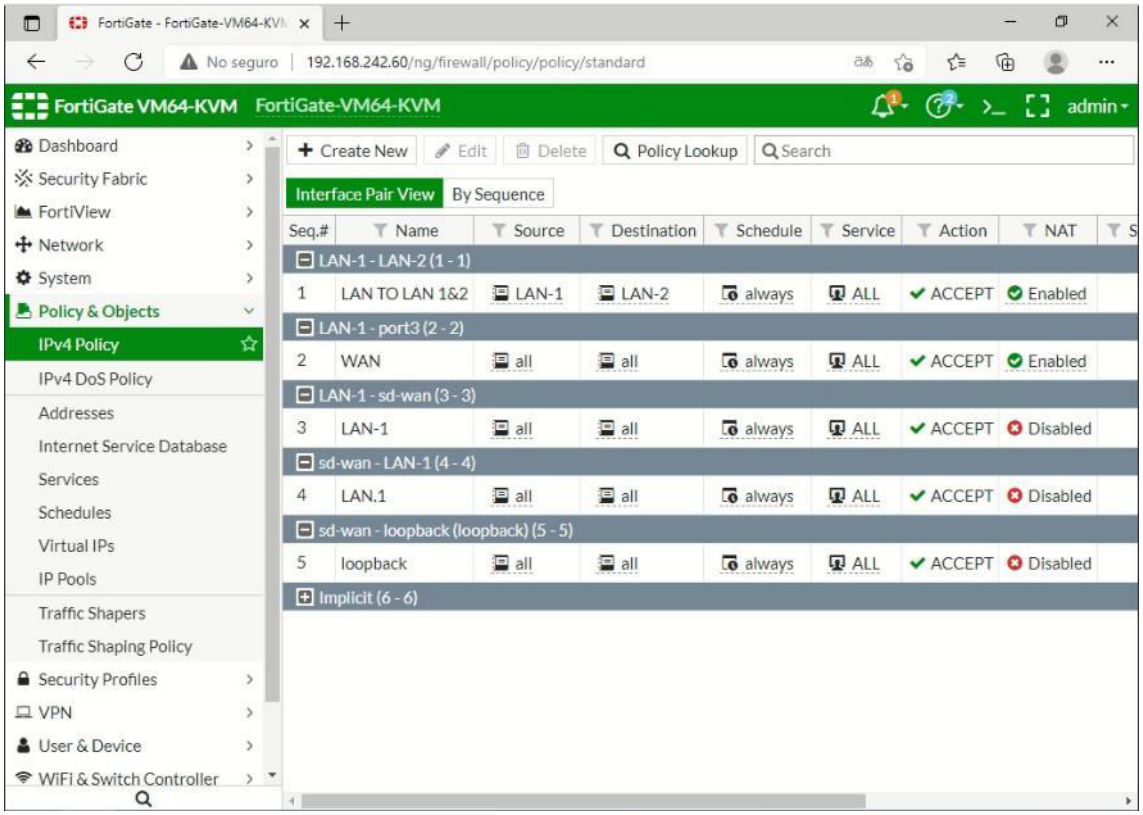


Figura 3.158 Políticas para acceso en la red 1

El último paso a configurar dentro de esta red es el establecimiento del protocolo de enrutamiento dinámico OSPF; para ello se define la interfaz por medio de la cual viajará todo el tráfico hacia la red. Esta interfaz es la configurada para SDWAN, posteriormente se configuran todas las redes que debe conocer el equipo FortiGate para poder hacer el envío de tráfico hacia la red, dichas redes se detallan a continuación:

- 1.1.1.1/255.255.255.255
- 10.1.1.0/255.255.255.252
- 192.168.10.0/255.255.255.0
- 192.168.20.0/255.255.255.0
- 192.168.30.0/255.255.255.0

Adicionalmente cabe recalcar que el área por defecto para la configuración de OSPF que se utiliza es la 0.0.0.0 y la identificación de *router* es 1.1.1.1 como se muestra en la Figura 3.159.

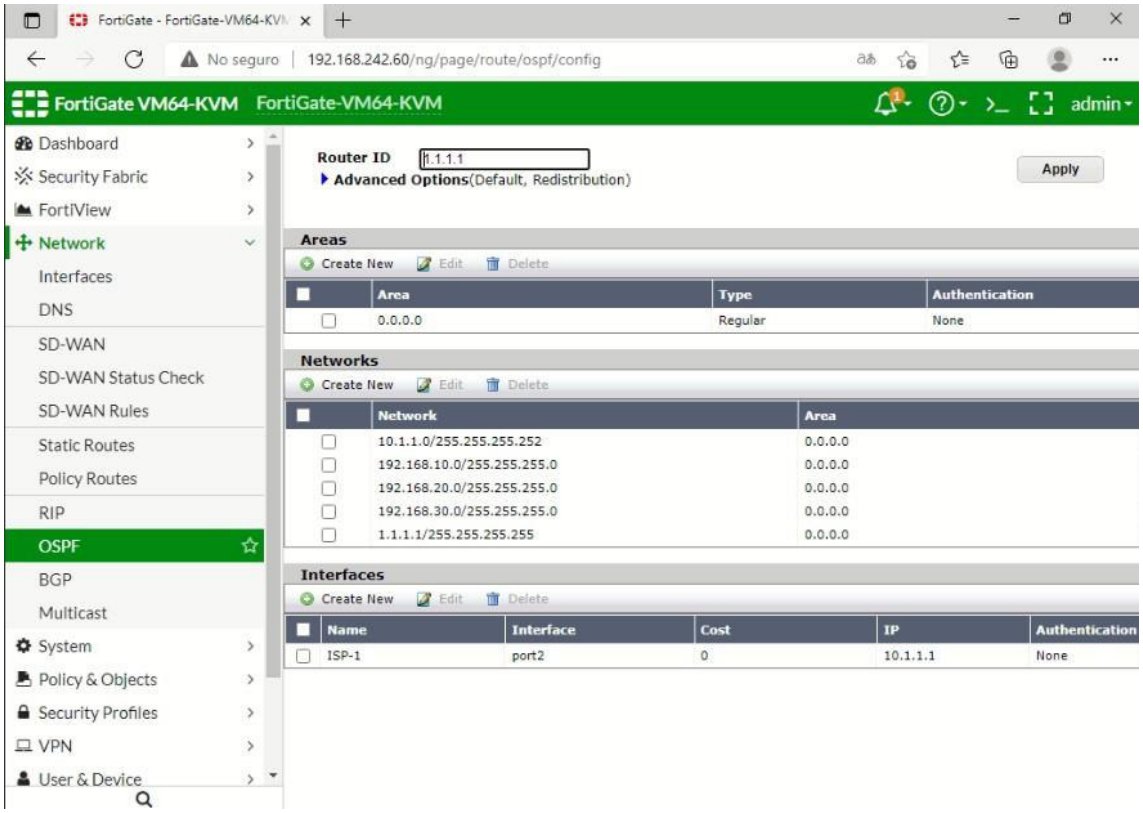


Figura 3.159 Configuración de protocolo OSPF en la red 1

Una vez finalizada la configuración de las interfaces dentro de este equipo FortiGate se procede a la verificación de las mismas en "*Network > Interfaces",* como se muestra en la Figura 3.160 y en la Figura 3.161 respectivamente.

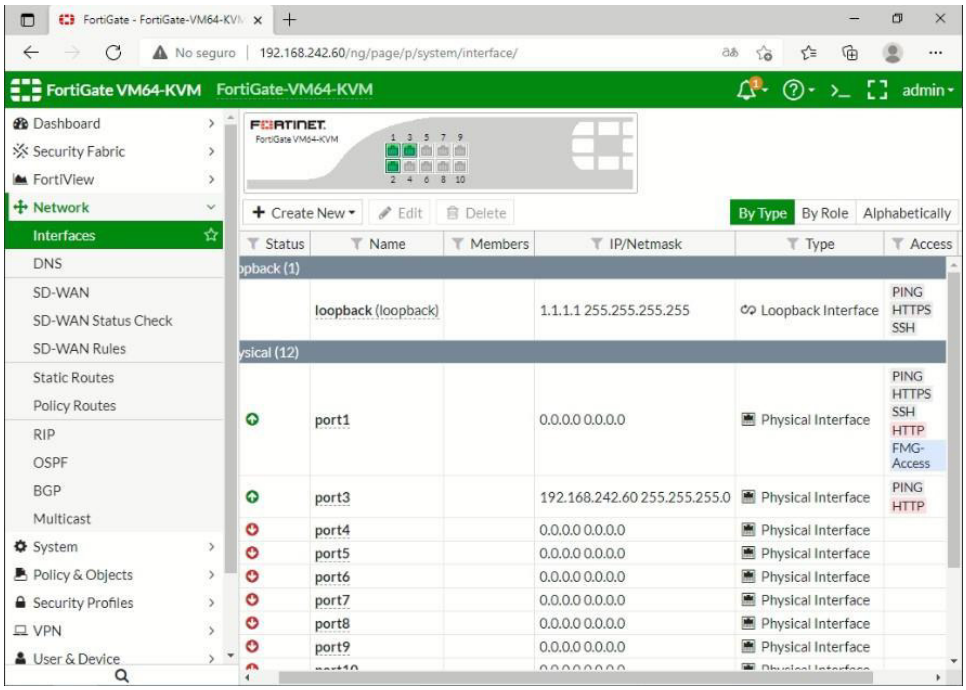


Figura 3.160 Interfaces en la red 1

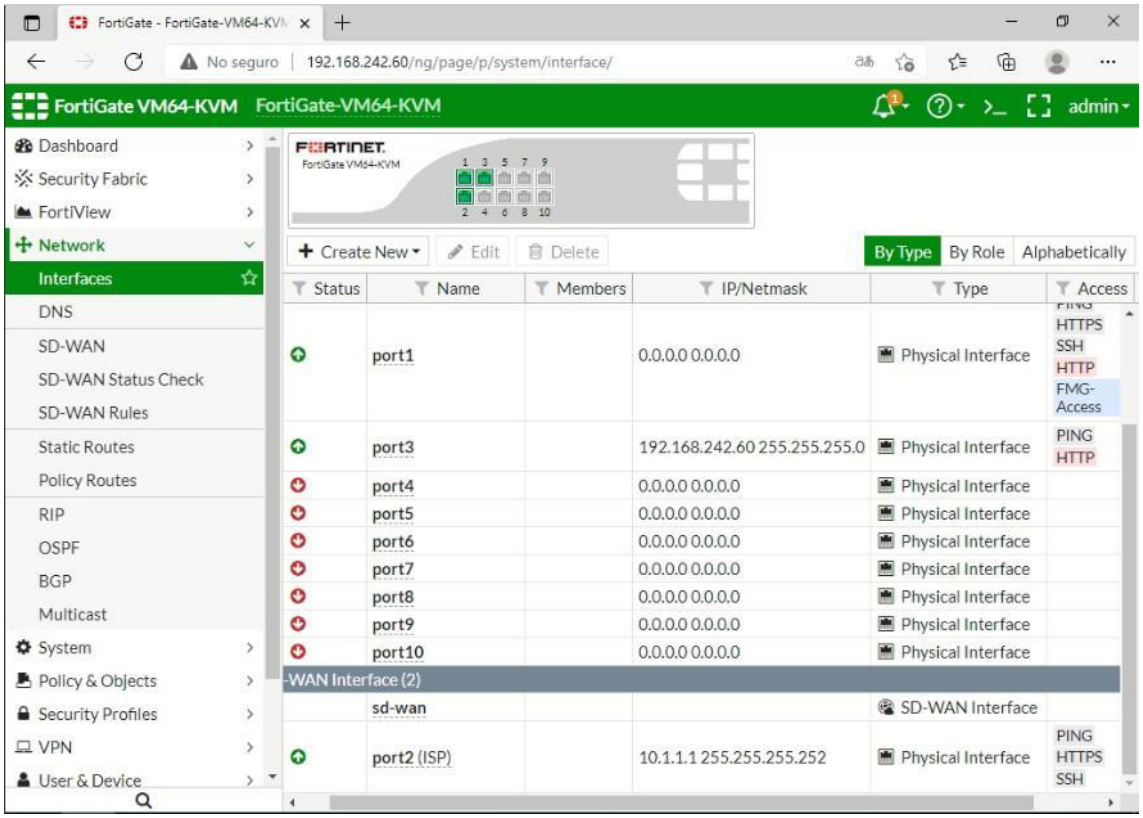


Figura 3.161 Interfaces SDWAN en la red 1

Para continuar con la configuración de esta red se procede a realizar la configuración en los equipos de capa 2 de cada lado de la topología para ello se debe acceder a la configuración del sistema mediante el comando "*configure terminal".* Los primeros parámetros a configurar son la asignación de los nombres de usuario para cada vlan previamente creada esto por medio de la aplicación de los siguientes comandos:

- Vlan 2
- Name user 1
- Vlan 3
- Name user 2
- Vlan 4
- Name user 3

Posteriormente se configuran los accesos a cada vlan accediendo a cada una de las interfaces de tipo *Ethernet* dentro del *switch*. El primer parámetro a configurar es un enlace de tipo troncal con el fin de que toda comunicación que se lleve a cabo viaje por este enlace al exterior u otra red; esto por medio de la aplicación del siguiente comando:

- Interface Ethernet 0/3
- Swtichport trunk encapsulation dot1q
- Switchport mode trunk

Una vez configurado el enlace de tipo troncal, se procede a dar los accesos a cada vlan según su interfaz ethernet correspondiente como se muestra en los siguientes comandos:

- Interface Ethernet 0/0
- Switchport mode access
- Switchport access vlan 2
- Interface Ethernet 0/1
- Switchport mode access
- Switchport access vlan 3
- Interface Ethernet 0/2
- Switchport mode access
- Switchport access vlan 4

Finalmente, para comprobar que todo se realizó correctamente se procede a ejecutar el comando "*show vlan brief*" como se muestra en la Figura 3.162.

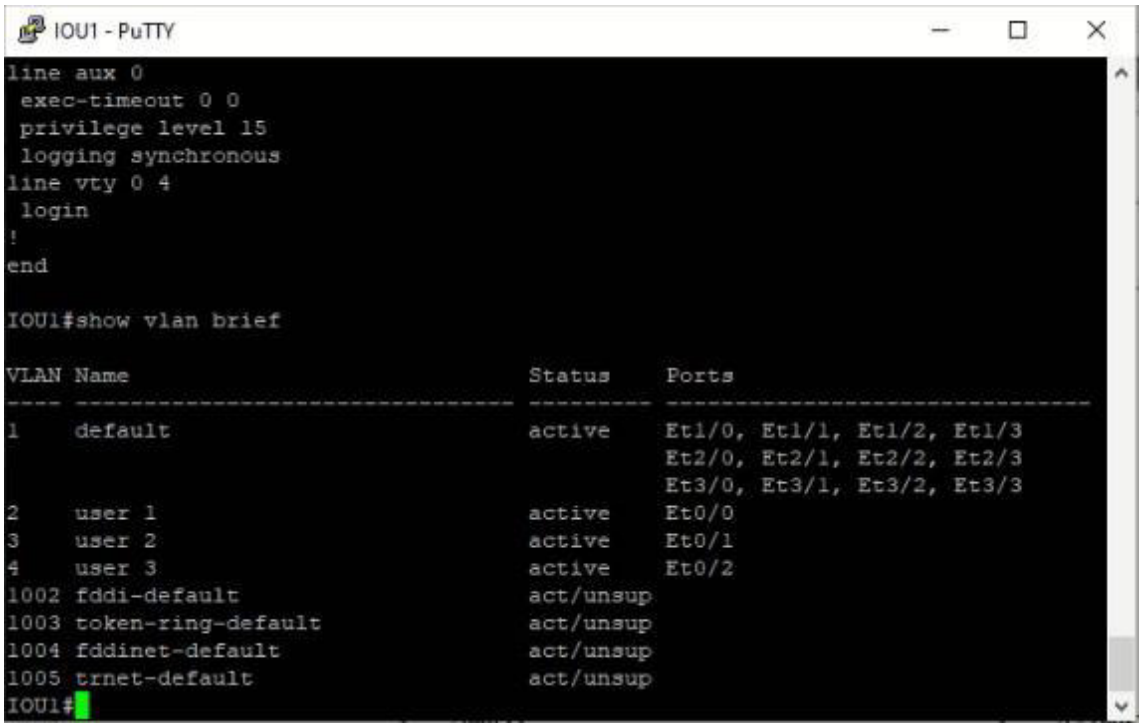


Figura 3.162 Comprobación de Vlans en switch de la red 1

Configuración Red 2

Para la configuración de esta parte de la red se debe acceder a la interfaz gráfica del equipo FortiGate colocando la dirección 192.168.242.50 y al igual que en el caso anterior acceder con las credenciales respectivas y se debe repetir el mismo procedimiento previamente mencionado. La primera parte a configurar es asignar las vlans en el puerto que se encuentra conectada la red LAN como se muestra en la Figura 3.163.

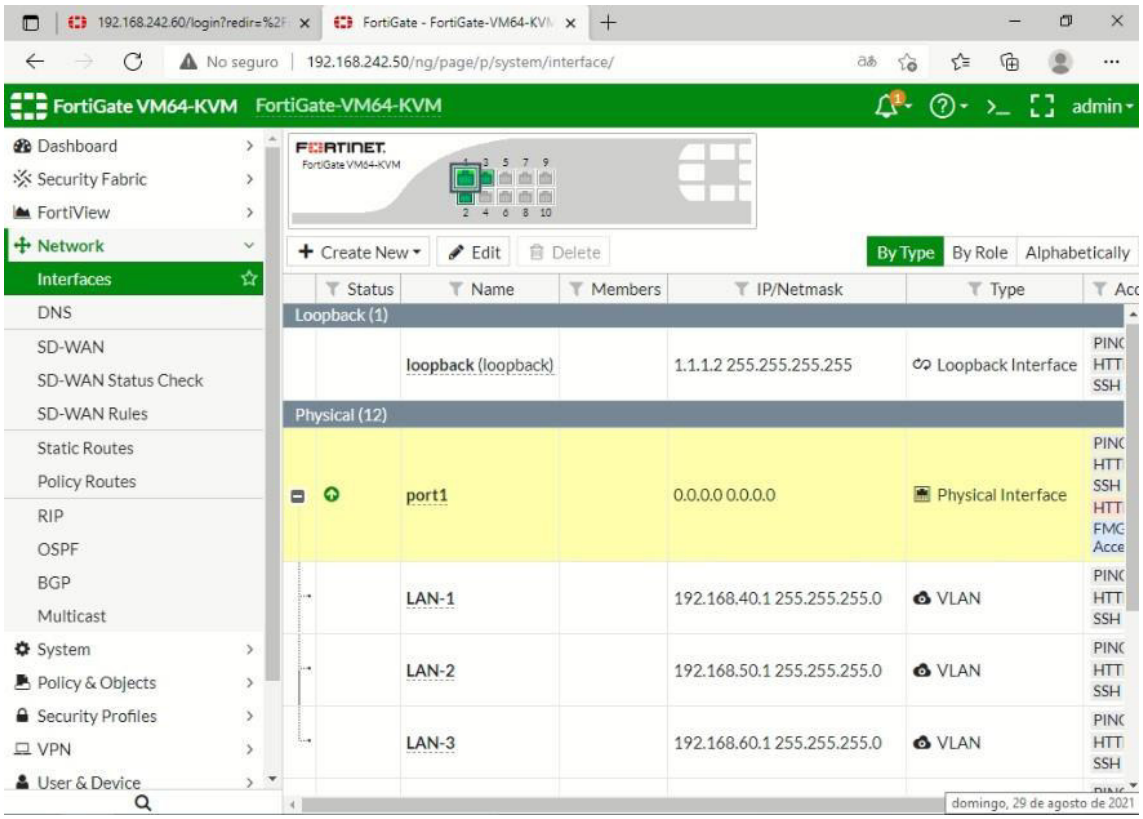


Figura 3.163 Configuración de interfaces VLAN en la red 2

El siguiente paso a realizar es configurar el enlace serial denominado ISP para lo cual se deben establecer los siguientes parámetros:

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 10.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING,SSH

De la misma manera que en el caso anterior se debe configurar una interfaz de tipo *loopback* con el fin de facilitar el enrutamiento dinámico por OSPF por lo que se deben modificar los siguientes parámetros:

- Interface Name: loopback
- Alias: loopback
- Type: Loopback Interface
- Role: LAN
- IP/Network Mask: 1.1.1.2/32
- Administrative Access: HTTPS, PING, SSH

Con las interfaces definidas se procede a configurar el *Gateway* que será asignado para funcionar mediante conexiones SDWAN este procedimiento se realiza mediante el acceso al apartado de "*Network > SD-WAN"* como se muestra en la Figura 3.164.

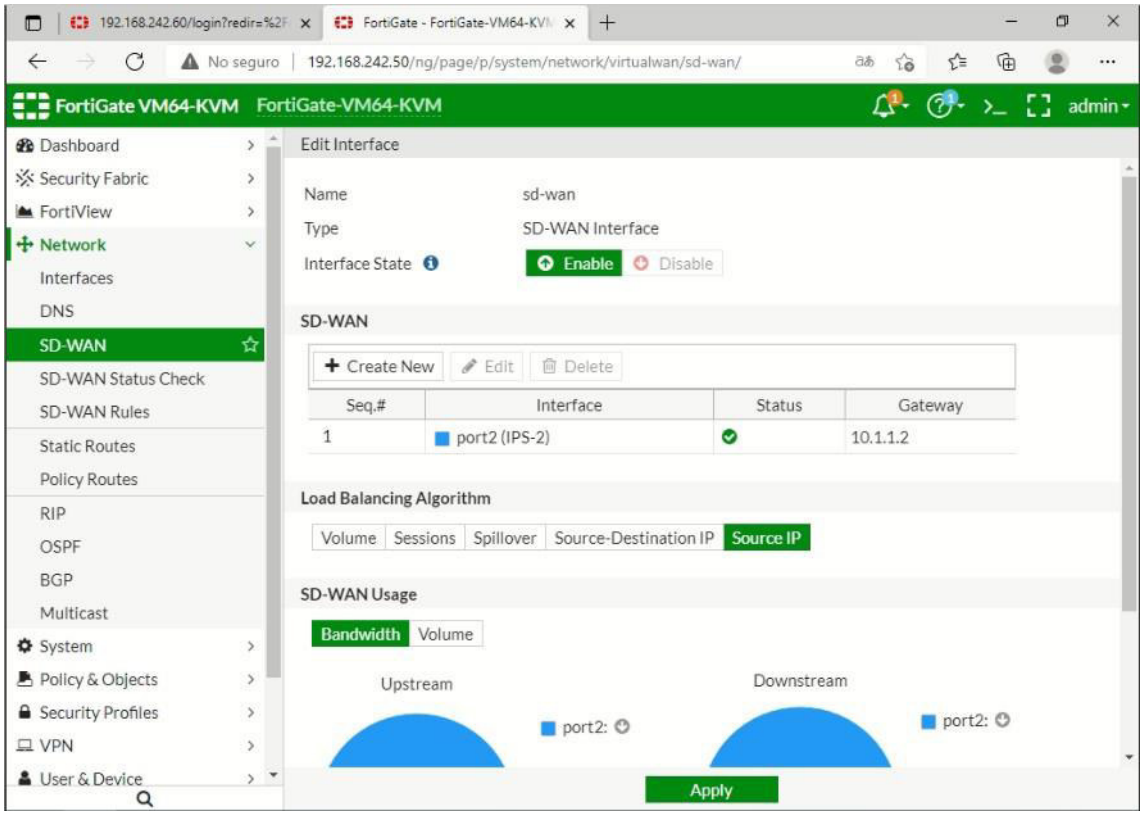


Figura 3.164 Configuración de enlace SDWAN en la red 2

Con la interfaz de SDWAN definida se procede a configurar una ley para mantener un correcto monitoreo de todo el tráfico que circula en la red para ello se modifican los siguientes parámetros:

- Name: Voice
- Server: 1.1.1.2
- Timeout: 10 seconds

Con la ley configurada se procede a la implementación de la regla que permitirá que se reconozca el tráfico dentro de la red SDWAN. Para ello se modifican los siguientes parámetros vistos en la Figura 3.165.

- Name: VOice
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 1.1.1.1
- Status Check: voice

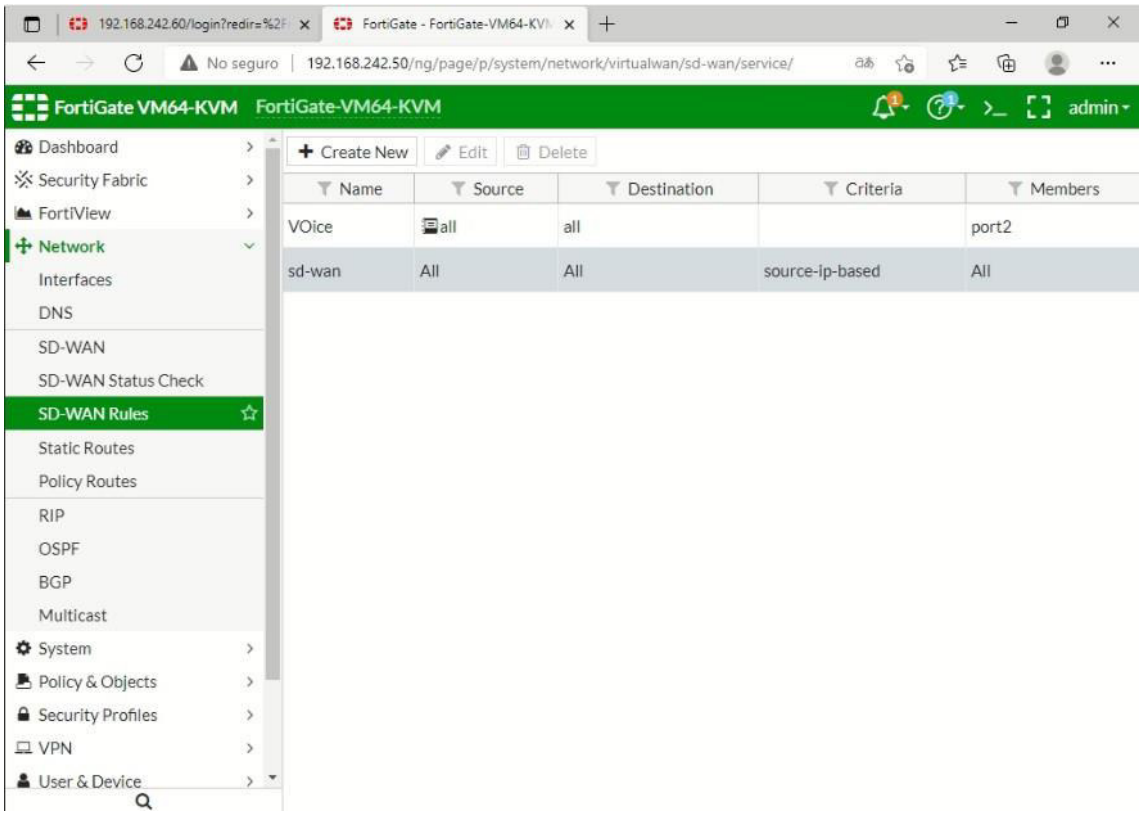


Figura 3.165 Configuración de reglas SDWAN en la red 2

Para poder tener una conexión a internet de parte de los equipos se procede a configurar una ruta por defecto accediendo al apartado *"Network > Static Routes*" y modificando los siguientes parámetros como se muestra en la Figura 3.166.

- Destination: 0.0.0.0/0.0.0.0
- Device: Port3
- Gateway: 192.168.242.2

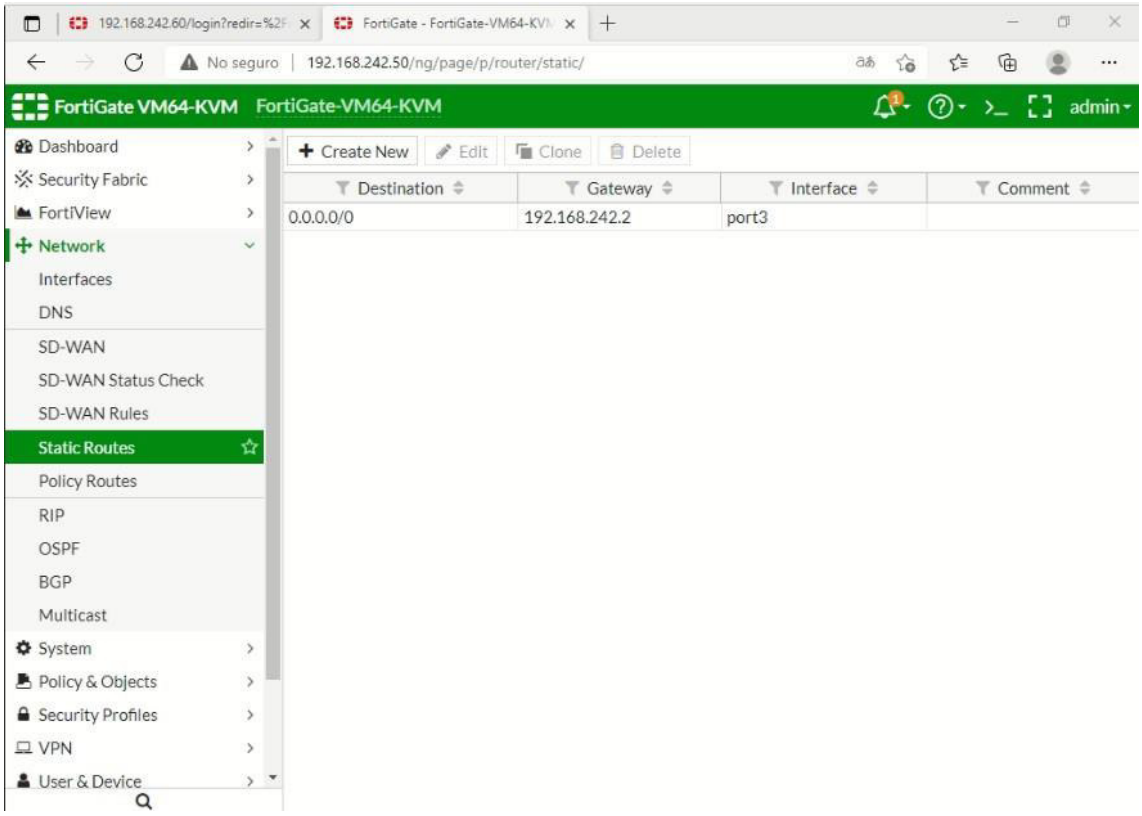


Figura 3.166 Configuración de una ruta por defecto en la red 2

Del mismo modo que en la red pasada se procede a configurar las direcciones IP dentro de las configuraciones para poder ser seleccionadas más adelante. Para realizar estos cambios se accede a "*Policy & Objects* > *Addresses*" y se establecen los siguientes parámetros los mismos que se muestran en la Figura 3.167.

VLAN 1

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.40.0/24
- Interface: LAN

VLAN 2

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.50.0/24
- Interface: LAN

VLAN 3

- Name: LAN
- Type: IP/Netmask
- Subnet/IP Range: 192.168.60.0/24
- Interface: LAN

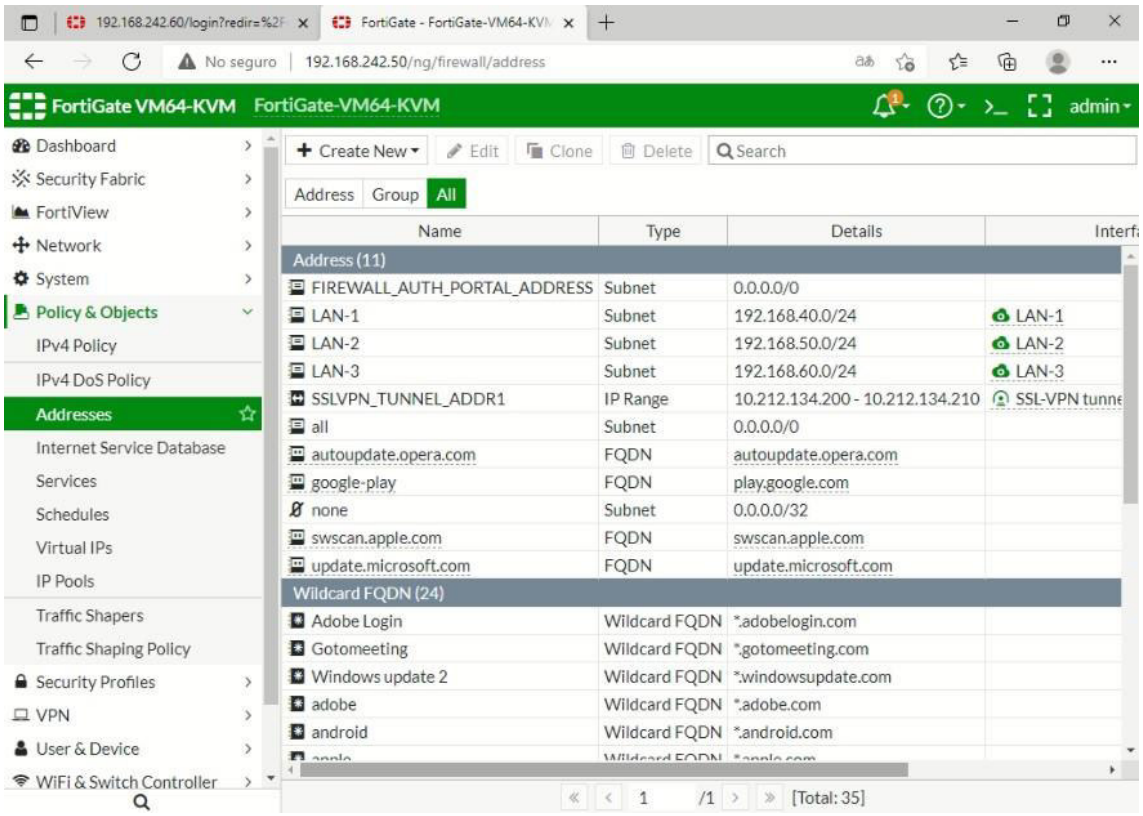


Figura 3.167 Configuración de una dirección para políticas en la segunda red

Con las direcciones establecidas se procede a configurar las políticas tanto como para la salida a internet como para tener comunicación entre vlans. Entre redes y hacia internet estas políticas se detallan a continuación:

Política de salida a internet

- Name: WAN
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

Política de salida a red por interfaz *loopback*

- Name: loopback
- Incoming Interface: loopback
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política de salida a red por interfaz LAN

- Name: LAN
- Incoming Interface: LAN-1
- Outgoing Interface: sd-wan
- Source: ALL
- Destination: ALL
- Service: ALL

Política de retorno a la red por interfaz SDWAN

- Name: LAN.1
- Incoming Interface: sd-wan
- Outgoing Interface: LAN
- Source: ALL
- Destination: ALL
- Service: ALL

Política de conexión entre vlans

- Name: LAN TO LAN 1&2
- Incoming Interface: LAN 1
- Outgoing Interface: LAN 2
- Source: ALL
- Destination: ALL
- Service: ALL

Se debe comprobar que todas las políticas se configuraron correctamente accediendo al apartado de "*Policy & Objects"* como se muestra en la Figura 3.168.

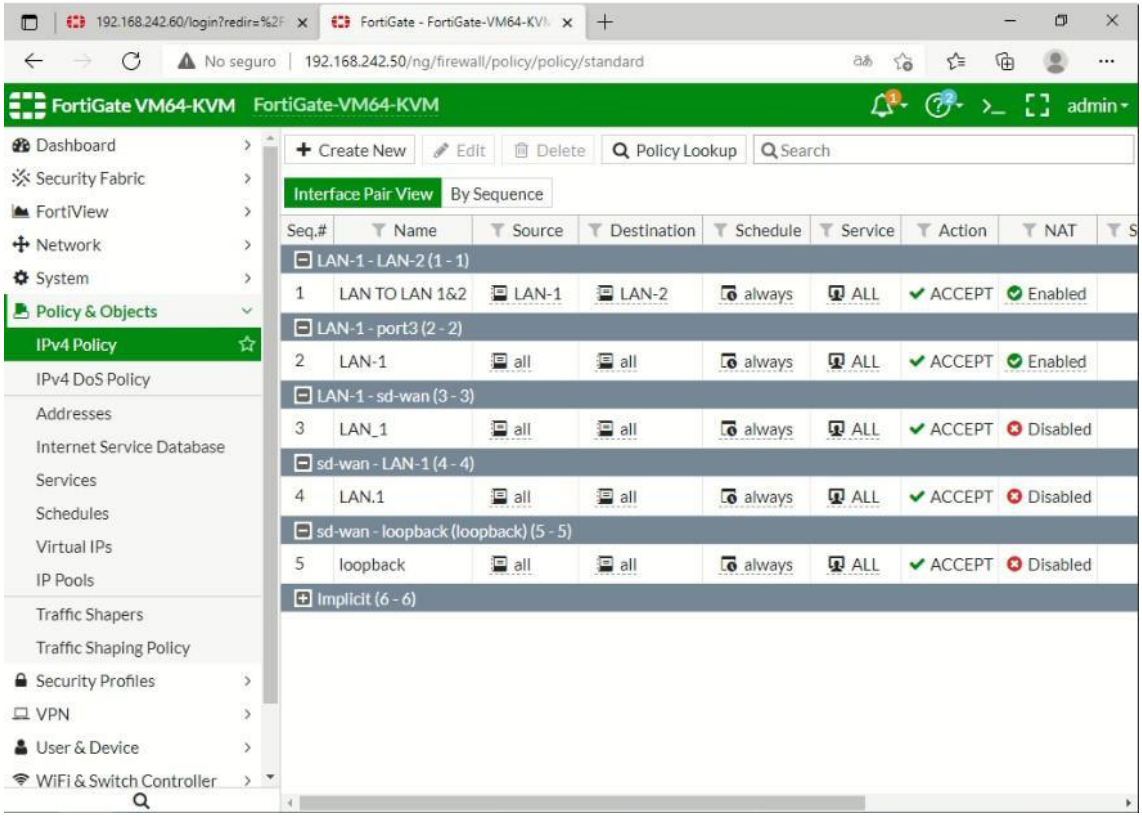


Figura 3.168 Políticas para acceso en la red 2

El último paso a configurar dentro de esta interfaz gráfica es el protocolo de enrutamiento dinámico OSPF. La interfaz de *router* que se utilizará en este caso es 1.1.1.2 y el área por defecto será la 0.0.0.0, la interfaz por donde debe circular el tráfico es la interfaz de SDWAN y las redes que debe conocer son las siguientes. Como se muestra en la Figura 3.169.

- 1.1.1.2/255.255.255.255
- 10.1.1.0/255.255.255.252
- 192.168.40.0/255.255.255.0
- 192.168.50.0/255.255.255.0
- 192.168.60.0/255.255.255.0

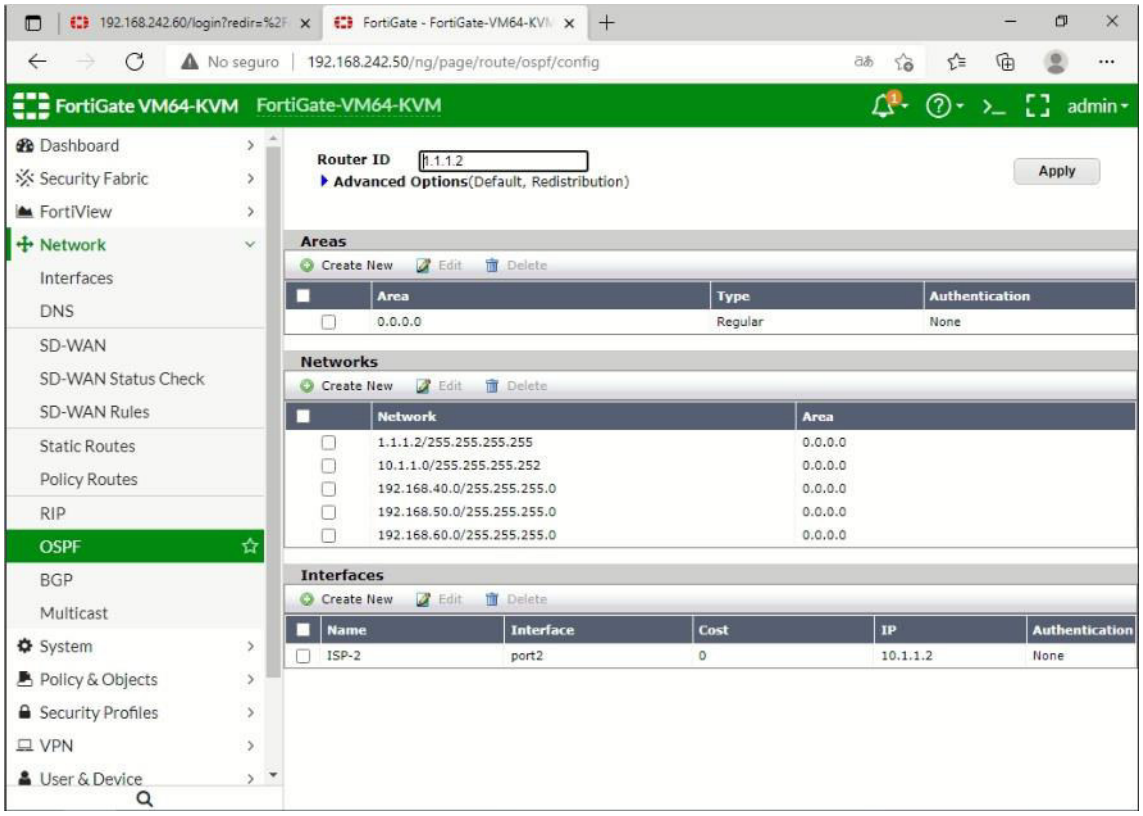


Figura 3.169 Configuración de protocolo OSPF en la red 2

Para comprobar que todo el procedimiento se llevó a cabo correctamente, se verifica en el apartado de "*Network > Interfaces"* que todas las interfaces, así como los servicios se ejecuten correctamente como se muestra a continuación en la Figura 3.170 y la Figura 3.171.

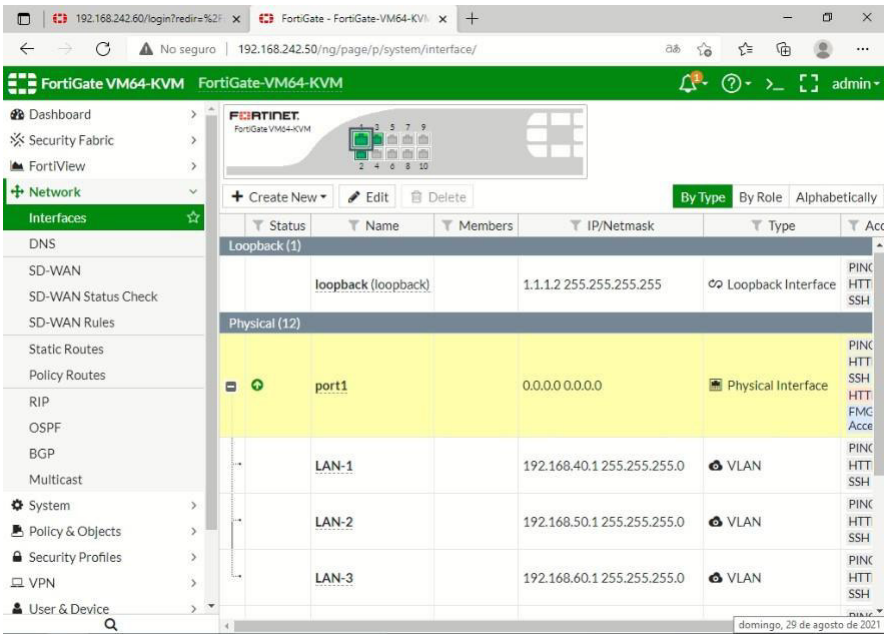


Figura 3.170 Interfaces en la red 2

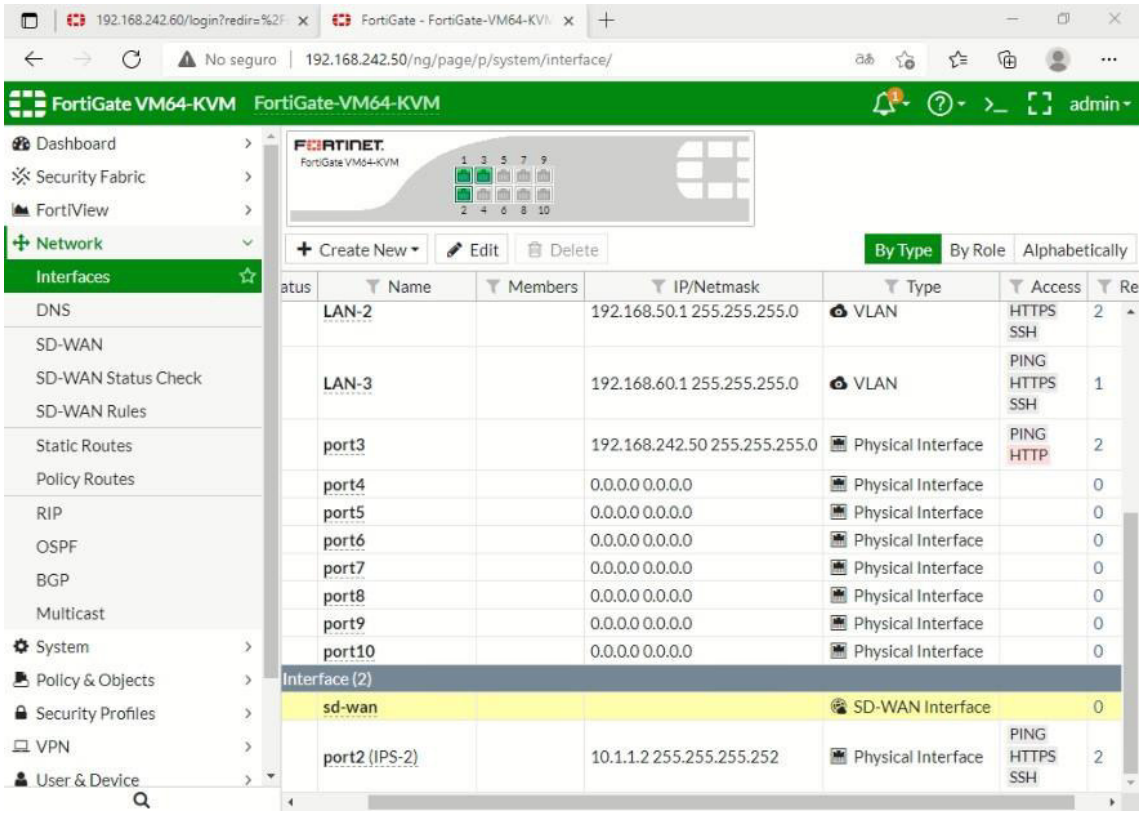


Figura 3.171 Interfaces SDWAN en la red 2

Para concluir con la configuración de esta red se procede al establecimiento de las vlans dentro del *switch* en la red 2. La primera acción a llevarse a cabo es la asignación de nombres de los usuarios a las VLANs para ello se accede a las configuraciones del equipo por medio del uso del comando "*configure terminal*" y se implementan los siguientes comandos:

- Vlan 2
- Name user 1
- Vlan 3
- Name user 2
- Vlan 4
- Name user 3

Una vez configurados estos comandos se procede a establecer un enlace de tipo troncal para que todas las comunicaciones viajen hacia el exterior. Del mismo modo se concede el acceso a las vlans mediante cada una de las interfaces *ethernet* a las cuales estén conectadas respectivamente mediante la aplicación de los siguientes comandos:

- Interface Ethernet 0/3
- Swtichport trunk encapsulation dot1q
- Switchport mode trunk
- Interface Ethernet 0/0
- Switchport mode access
- Switchport access vlan 2
- Interface Ethernet 0/1
- Switchport mode access
- Switchport access vlan 3
- Interface Ethernet 0/2
- Switchport mode access
- Switchport access vlan 4

Finalmente, mediante el uso del comando "*show vlan brief*" se verifican que todas las vlans se encuentren activas y en correcto funcionamiento como se muestra en la Figura 3.172.

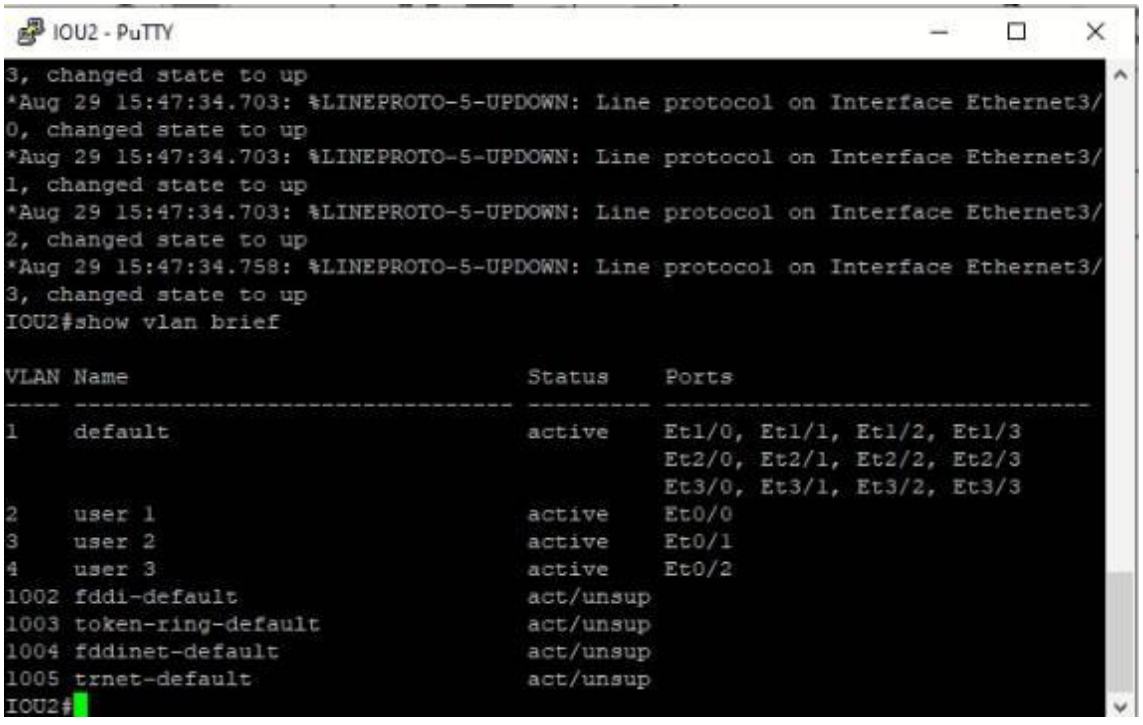


Figura 3.172 Comprobación de Vlans en switch de la red 2

Red SDWAN-IPSEC

La siguiente red consta de conexiones mediante enlaces SDWAN y conexiones por medio de túneles VPN, para ello se requiere de los siguientes dispositivos:

- 4 equipos FortiGate 5.6.1
- 8 equipos switch propietarios de Cisco
- 6 computadores VPCS
- 2 nubes de conexión hacia Internet

De igual manera que en las redes pasadas ya se conoce el *Gateway* por defecto de las redes NAT a Internet motivo por el cual se colocarán las direcciones de los equipos dentro del rango de direcciones de 192.168.242.0/24. El direccionamiento utilizado para esto se detalla en la Tabla 3.5 a continuación.

Tabla 3.5 Direccionamiento RED SDWAN-IPSEC

TIPO	DIRECCIÓN
SERIAL 1 CENTRAL	10.1.1.1/30
SERIAL 2 CENTRAL	10.1.1.2/30
SERIAL 3 SUCURSAL	10.1.1.1/30
SERIAL 4 SUCURSAL	10.1.1.2/30
RED 1	192.168.60.0/24
RED 2	192.168.70.0/24
RED 3	10.70.16.0/24
RED 4	10.60.16.0/24
GATEWAY INTERNET CENTRAL 1	192.168.242.70/24
GATEWAY INTERNET CENTRAL 2	192.168.242.90/24
GATEWAY INTERNET SUCURSAL 1	192.168.242.80/24
GATEWAY INTERNET SUCURSAL 2	192.168.242.100/24

Una vez que se tiene las direcciones IP establecidas se procede con la formación de la topología la cual se observa en la Figura 3.173.

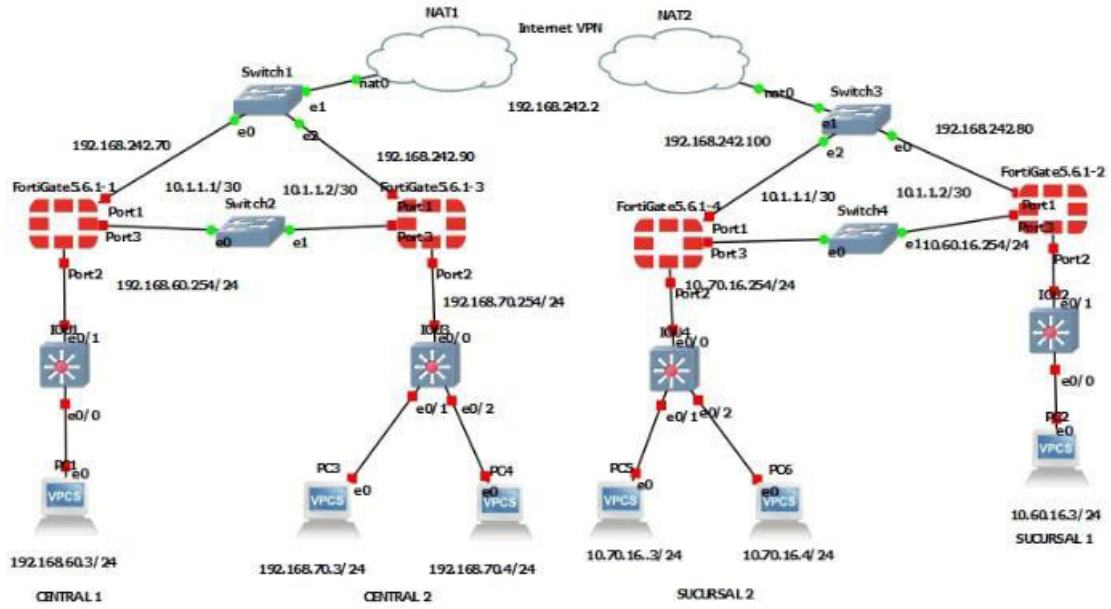


Figura 3.173 Topología Red SDWAN-IPSEC

El primer paso en la configuración de esta topología es asignar las direcciones IP a los distintos equipos FortiGate respectivamente. Estas direcciones deben encontrarse en el rango del *Gateway* definido por la red NAT y para ellos se llevan a cabo los siguientes comandos:

Fortigate Central 1

- config system interface
- edit port1
- set ip 192.168.242.70/24
- set allowaccess http ping telnet
- end
- show system interface

Fortigate Central 2

- config system interface
- edit port1
- set ip 192.168.242.90/24
- set allowaccess http ping telnet
- end
- show system interface

Fortigate Sucursal 1

- config system interface
- edit port1
- set ip 192.168.242.80/24
- set allowaccess http ping telnet
- end
- show system interface

Fortigate Sucursal 2

- config system interface
- edit port1
- set ip 192.168.242.100/24
- set allowaccess http ping telnet
- end
- show system interface

Un aspecto importante a considerar es que se debe adicionar el servicio de telnet a cada una de estas interfaces ya que esto permitirá la comunicación por túneles IPSEC entre equipos FortiGate a través de Internet. Estos procedimientos se detallan en la Figura 3.174, Figura 3.175, Figura 3.176 y Figura 3.177 respectivamente.

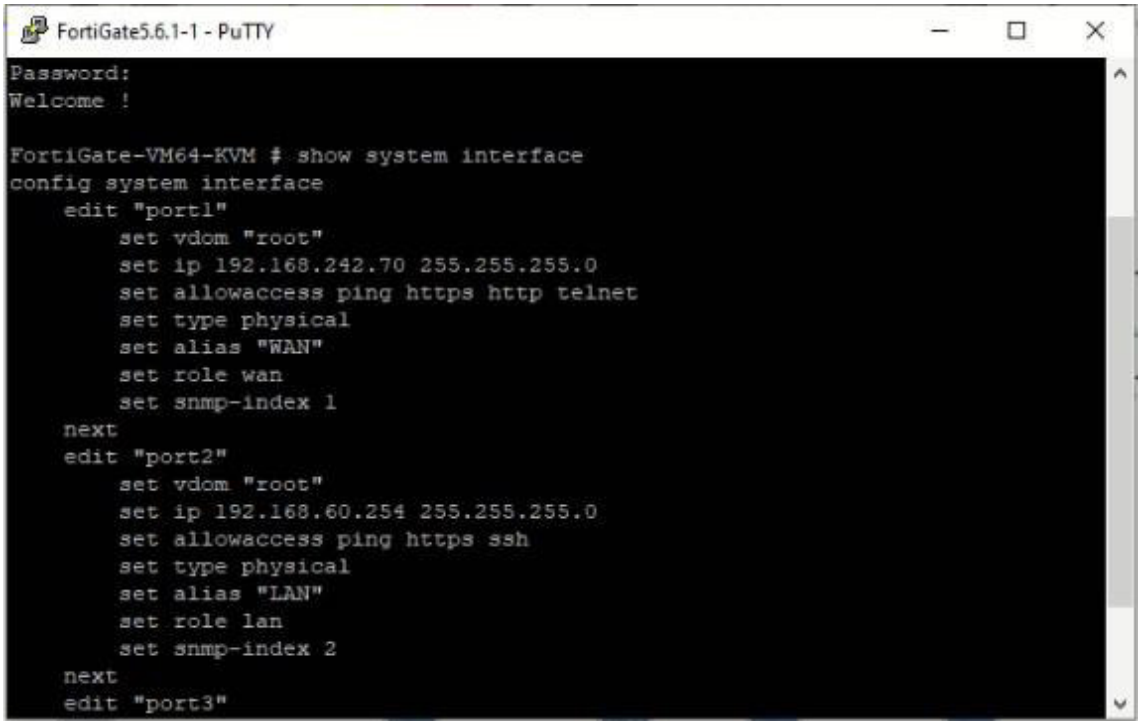


Figura 3.174 Configuración de equipo CENTRAL 1

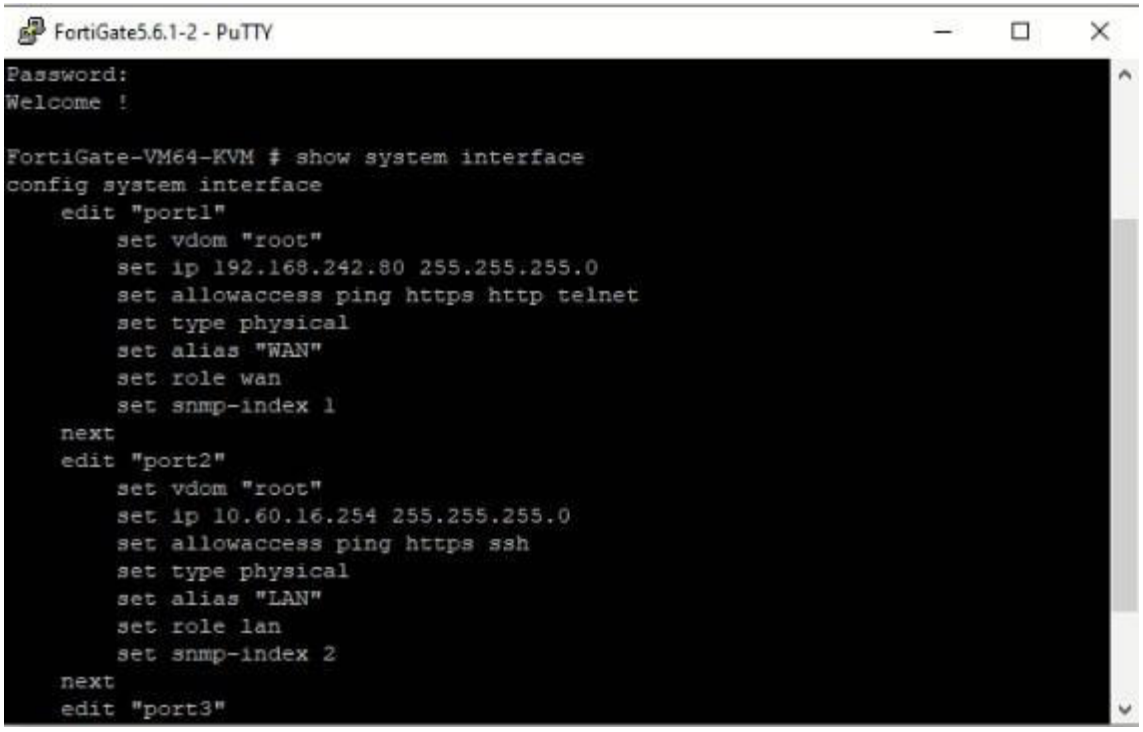


Figura 3.175 Configuración de equipo SUCURSAL 1

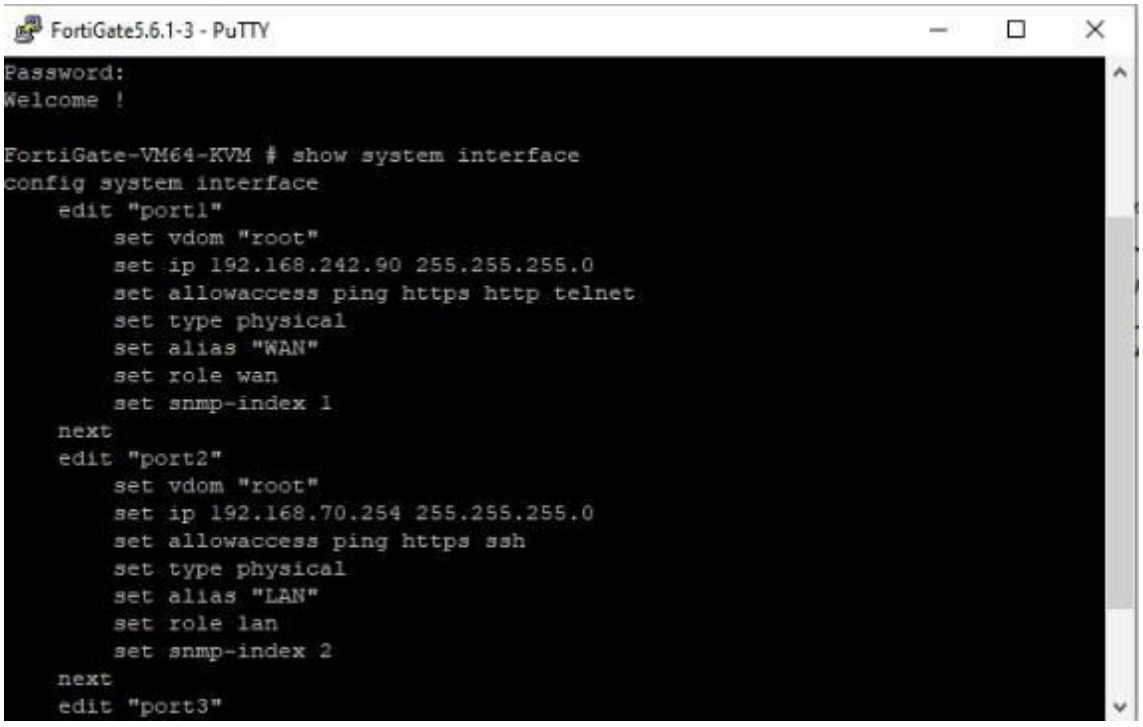


Figura 3.176 Configuración de equipo CENTRAL 2

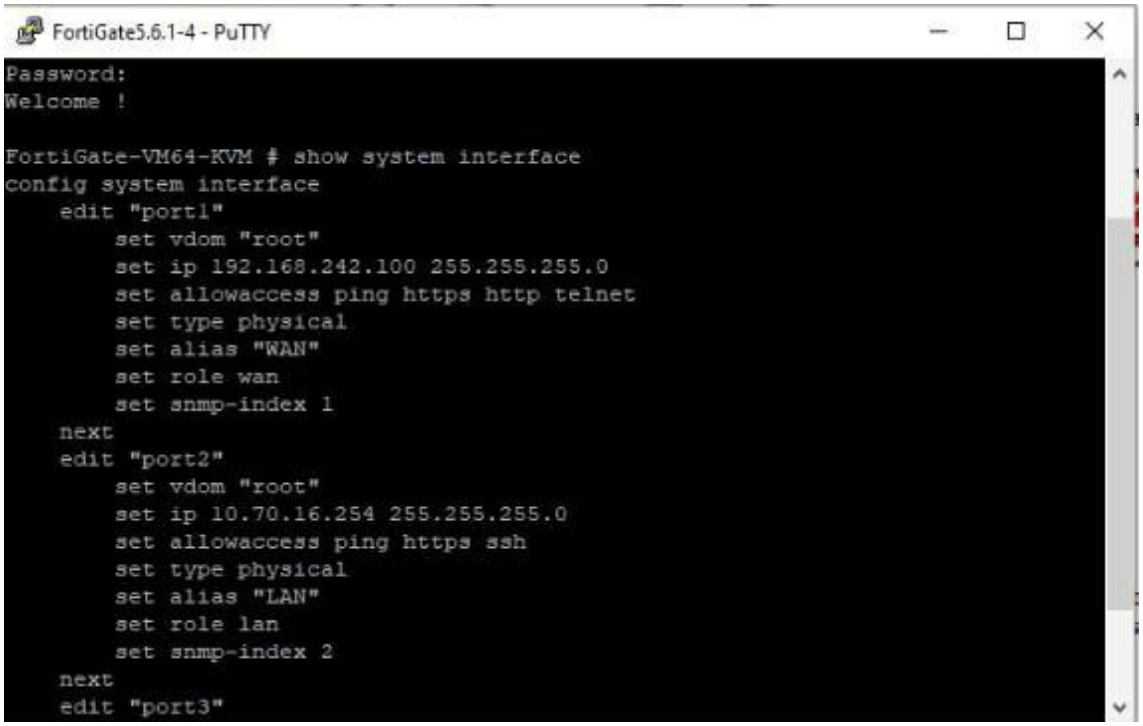


Figura 3.177 Configuración de equipo SUCURSAL 2

Una vez que se han establecido las direcciones para el funcionamiento de los equipos FortiGate se procede a configurar las direcciones de los diferentes equipos VPCS en la red como se observa en la Tabla 3.6.

Tabla 3.6 Direcciones y Gateways VPCS SDWAN-IPSEC

VPCS	DIRECCIÓN	GATEWAY
PC1	192.168.60.3/24	192.168.60.254/24
PC2	10.60.16.3/24	10.60.16.254/24
PC3	192.168.70.3/24	192.168.70.254/24
PC4	192.168.70.4/24	192.168.70.254/24
PC5	10.70.16.3/24	10.70.16.254/24
PC6	10.70.16.4/24	10.70.16.254/24

Configuración Central 1

Para configurar correctamente la red se debe acceder a la interfaz gráfica del equipo FortiGate para ello se escribe la dirección 192.168.242.70 en el buscador de preferencia y se accede mediante las credenciales por defecto en el sistema. La primera interfaz a configurar será la de salida a Internet la misma que debe constar con los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.70/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING, TELNET

La siguiente interfaz a modificar es el enlace serial por medio del cual se establece un enlace ISP hacia la segunda central en esta primera red. Para realizarlo se modifican los siguientes parámetros:

- Alias: ISP
- Role: WAN
- IP/Network Mask: 10.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH

A continuación, se procede a modificar los parámetros de la interfaz LAN acorde a lo mostrado a continuación:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 192.168.60.254/24
- Administrative Access: HTTPS, HTTP, PING, SSH

Una vez terminadas estas configuraciones se procede a verificar las mismas como se muestra en la Figura 3.178.

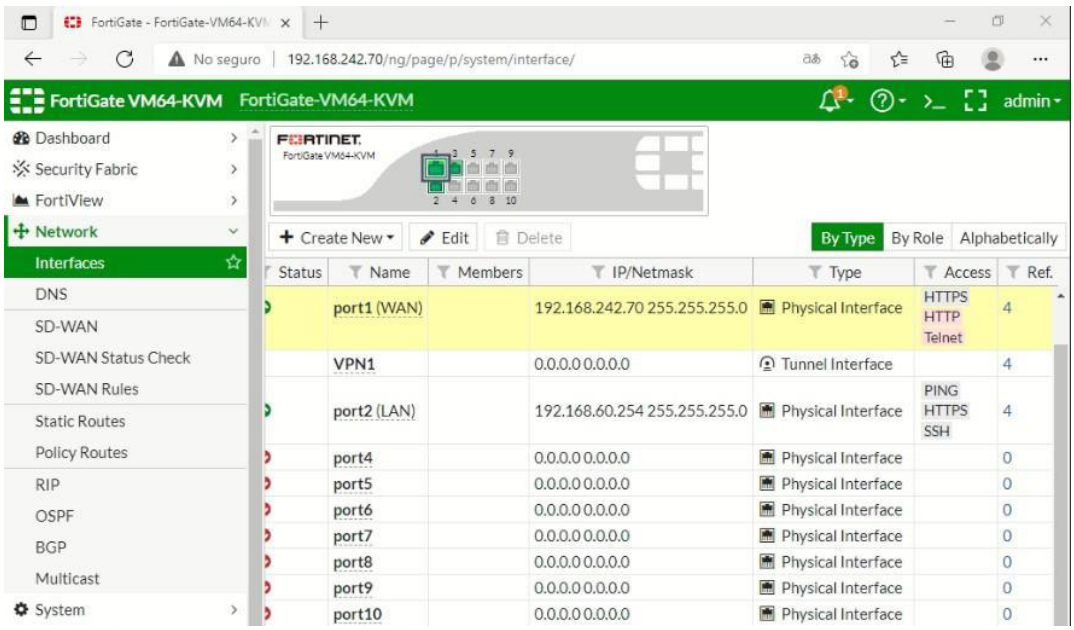


Figura 3.178 Interfaces en Fortigate CENTRAL 1

Al igual que en casos previos se debe asignar un *Gateway* para la salida de una interfaz que opere con SDWAN. Para ello se asigna el *Gateway* de la interfaz de ISP como se muestra en la Figura 3.179.

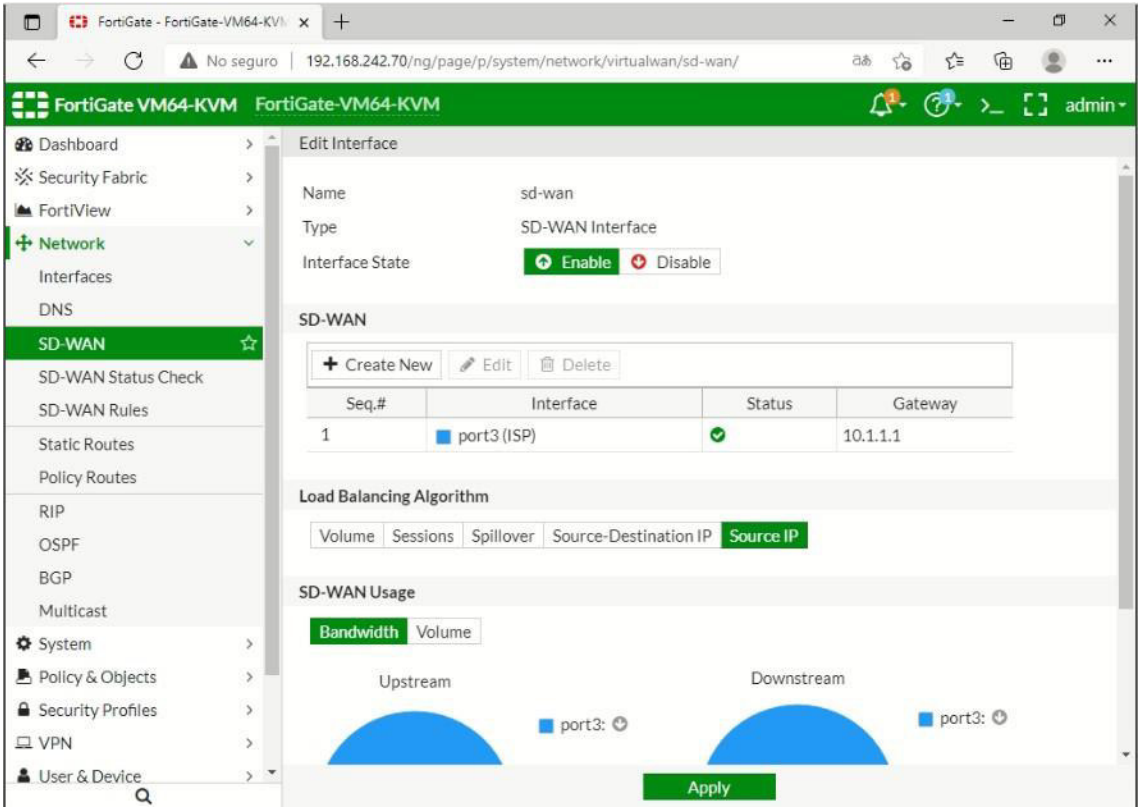


Figura 3.179 Configuración de SDWAN CENTRAL 1

A continuación, se procede a configurar la ley respectiva para que pueda operar el enlace SDWAN y del mismo modo lograr monitorear el enlace y todo el tráfico que viaje sobre él, para hacerlo se modifican los siguientes parámetros.

- Name: LEY1
- Server: 10.1.1.1
- Timeout: 10 seconds

Posteriormente se procede a configurar una regla para dicha ley esto con el objetivo de poder proteger el enlace SDWAN y para ello se modifican los parámetros presentados a continuación:

- Name: ley1
- Source Address: All
- Destination Address: All

- Interface Members: Gateway 10.1.1.1
- Status Check: LEY1

Estas modificaciones se pueden analizar en la Figura 3.180 a continuación.

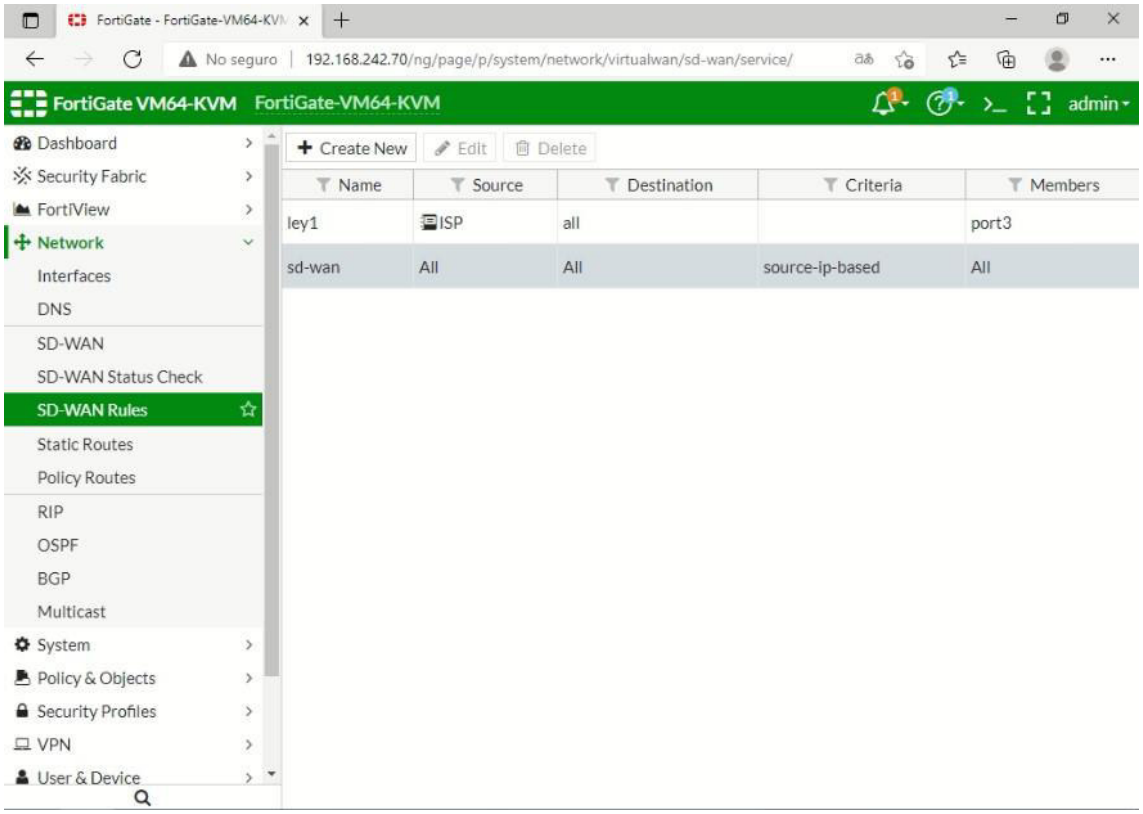


Figura 3.180 Configuración de reglas SDWAN CENTRAL 1

El siguiente paso a configurar es el túnel VPN; para realizar esto se accede al parámetro "*VPN > IPsec Wizard",* dentro del mismo se puede encontrar los pasos necesarios para configurar un túnel VPN, los parámetros a configurar se muestran a continuación:

- Name: VPN-1
- Type: site to site
- Remote: Fortigate
- Nat: no nat
- Ip: 192.168.242.80
- Outgoing interface: WAN (port1)
- Pre-shared key: tesis12345
- Local interface: LAN
- Local subnets: 192.168.60.0/24
- Remote subnets: 10.60.16.0/24

EL procedimiento consiste en establecer primero el tipo de túnel que se desea realizar. Para este caso es un túnel de tipo *site to site* es decir comunicación por medio de internet, existen otros tipos de túneles VPN disponibles en los equipos Fortigate sin embargo por problemas en las licencias de prueba solo se puede realizar la comunicación por *site to site*. Uno de los aspectos importantes es que Fortigate permite la conexión VPN por otros equipos de otras marcas por ejemplo Cisco por lo que se debe seleccionar el tipo de equipo, así como el fabricante del mismo. Es importante desactivar la conexión mediante NAT ya que esto podría interferir con el *Gateway* NAT proporcionado por el sistema previamente. Acto seguido se procede a la implementación de la dirección del *Gateway* de internet del equipo al cual se desea llegar es decir la sucursal 1 y se especifican tanto la interfaz por la que saldrá el tráfico que en este caso es la interfaz WAN y una clave de acceso. Para entablar la comunicación misma clave que debe coincidir al realizar el mismo procedimiento en la sucursal 1. Finalmente se establece la red local a la cual se encuentra conectado el equipo, así como la red local remota a la cual se desea acceder. Para comprobar que funcionó se comprueba en el apartado "*VPN > IPsec Tunnels*" como se muestra en la Figura 3.181.

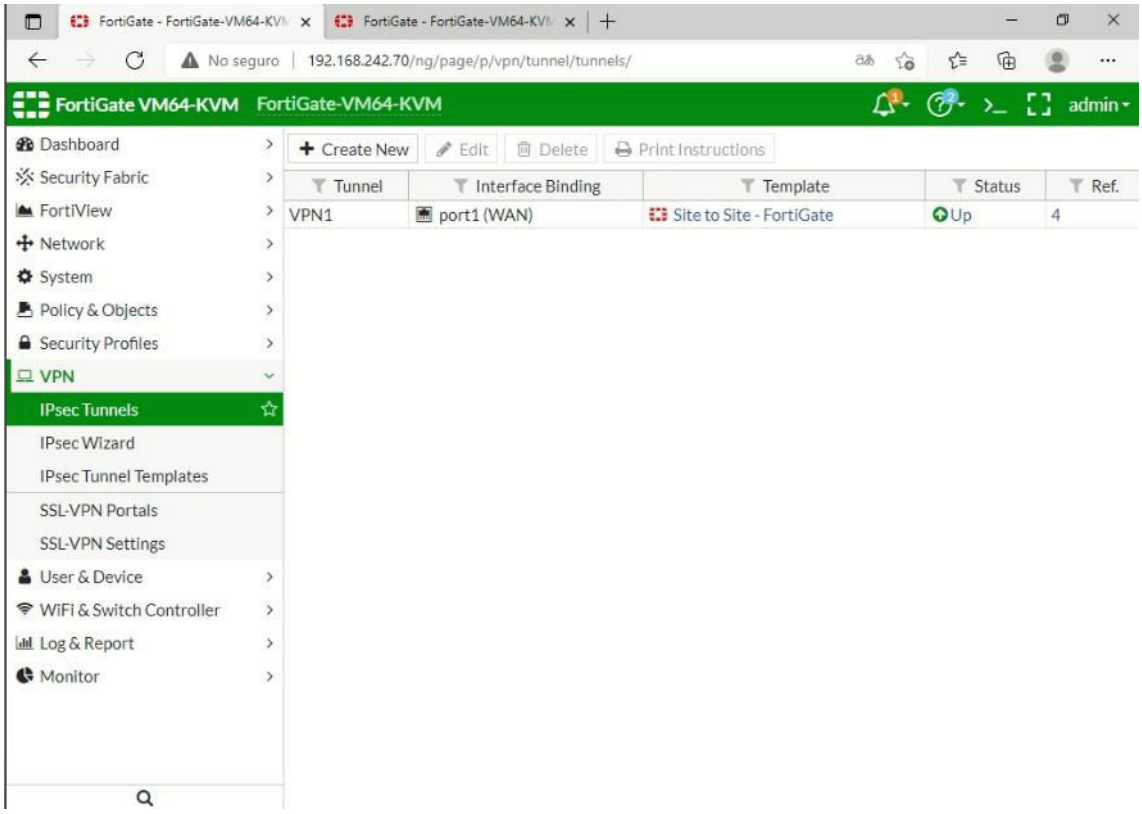


Figura 3.181 Configuración de VPN en CENTRAL 1

Con el procedimiento previamente realizado, se crean automáticamente las políticas definidas para la transmisión de datos por medio de túneles de tipo VPN. Por lo que solo es necesario configurar una política extra para poder realizar la transmisión hacia internet por lo cual se modifican los siguientes parámetros. Las políticas y su correcto funcionamiento se aprecia en la Figura 3.182.

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

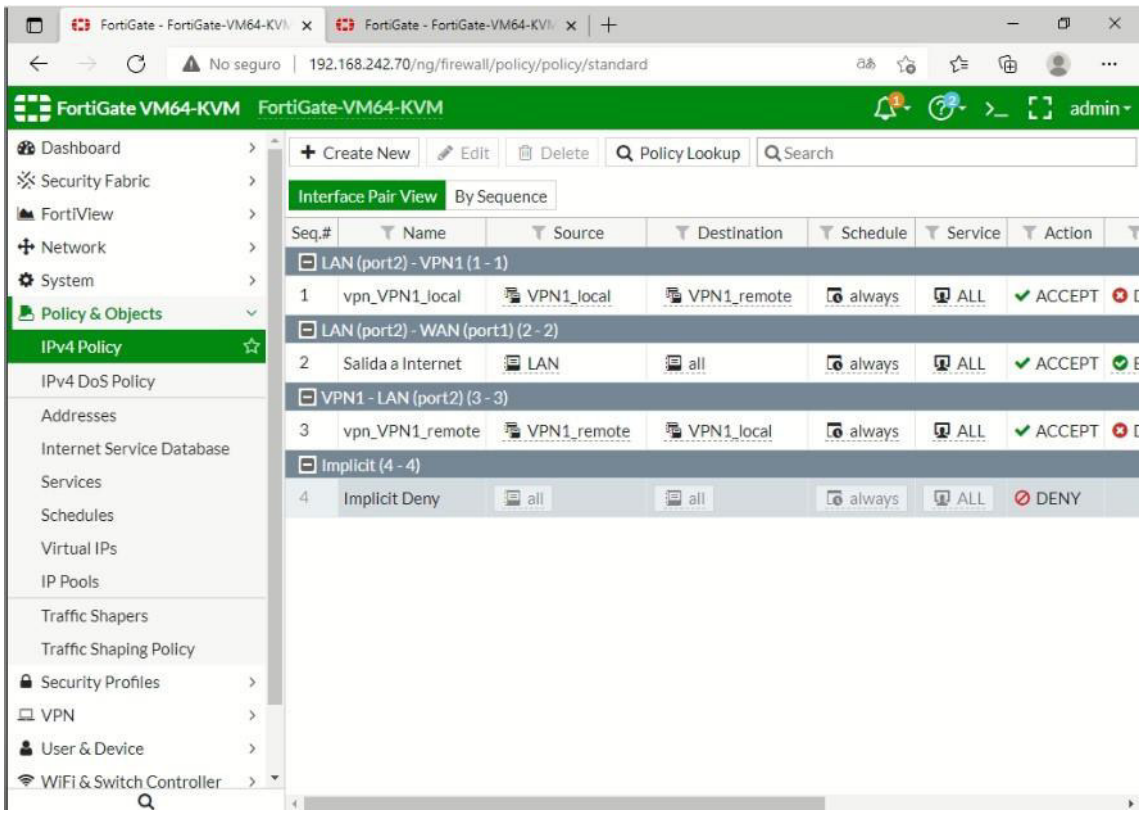


Figura 3.182 Políticas para acceso CENTRAL 1

Del mismo modo se establecen las direcciones automáticamente en el sistema como se aprecia en la Figura 3.183.

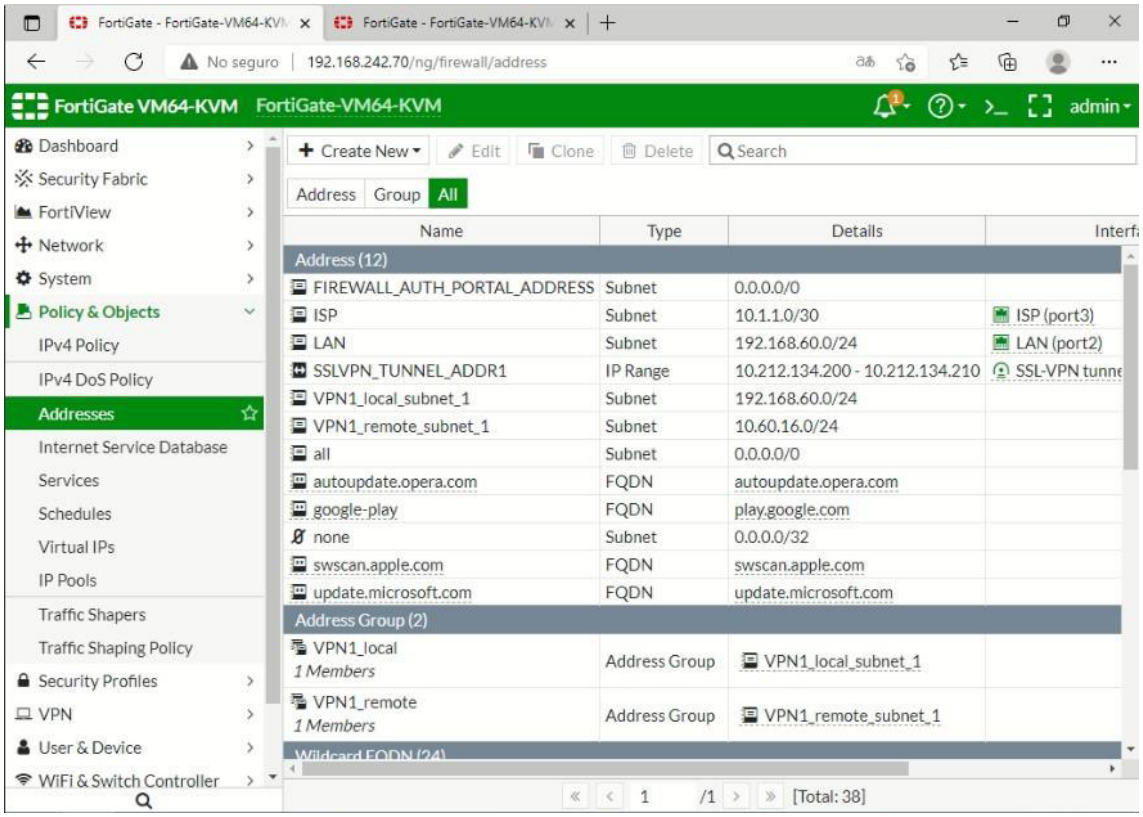


Figura 3.183 Configuración de dirección para políticas CENTRAL 1

Finalmente, se procede al establecimiento de una ruta por defecto para completar el procedimiento para obtener comunicación por medio de Internet. Para ello se modifican los siguientes parámetros los cuales se aprecian en la Figura 3.184.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

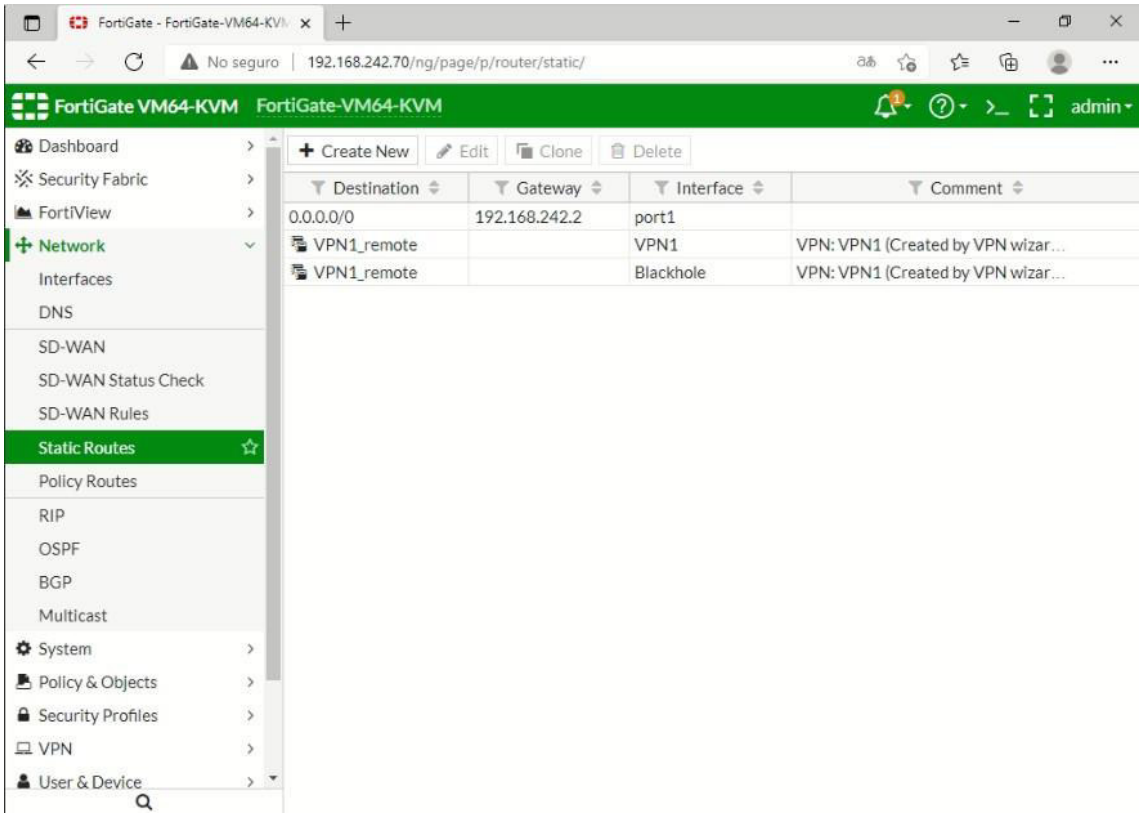


Figura 3.184 Configuración de una ruta por defecto Central 1

Finalmente, para completar con la configuración de esta central se verifica en el apartado de "*Network* > *Interfaces"* todas las interfaces. Así como el túnel VPN creado previamente como se muestra en la Figura 3.185.

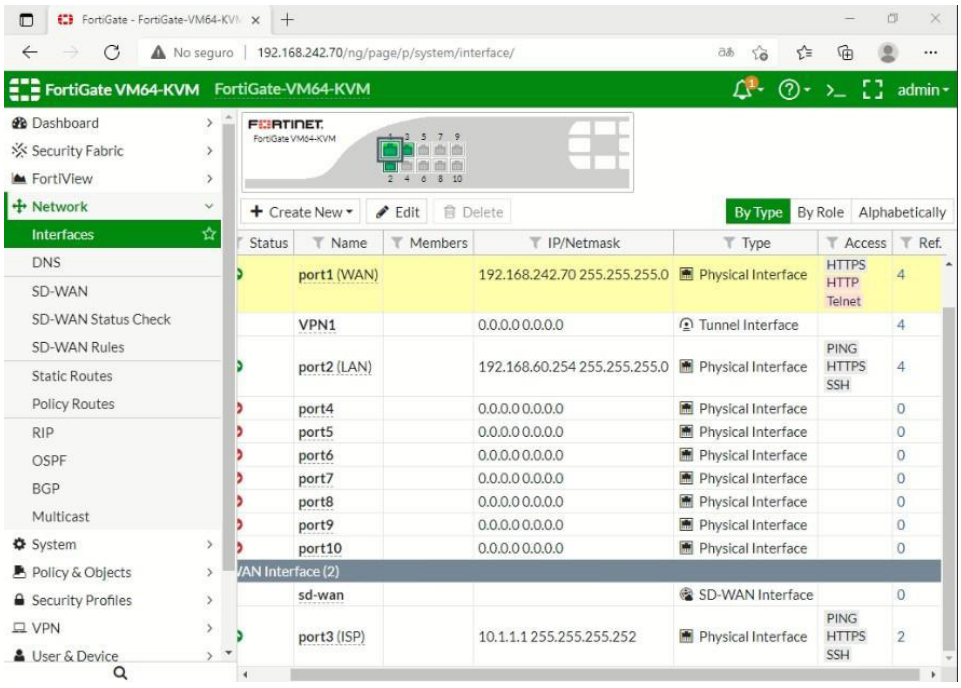


Figura 3.185 Configuración de interfaces en CENTRAL 1

Configuración Central 2

Para la correcta configuración de la siguiente central es necesario acceder a la interfaz gráfica del equipo FortiGate designado para ello se escribe la dirección 192.168.242.90 y se accede mediante las credenciales respectivas. De igual manera que en la central 1 se procede a modificar la interfaz de salida a Internet aplicando los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.90/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING, TELNET

Adicionalmente, se procede a configurar la interfaz serial por medio de la cual se configurará posteriormente un enlace SDWAN para obtener comunicación entre ambas centrales; para hacerlo se modifican los siguientes parámetros:

- Alias: ISP
- Role: WAN
- IP/Network Mask: 10.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING, SSH

Acto seguido se procede a configurar la red LAN a la cual está conectado el equipo FortiGate por medio de la aplicación de los siguientes parámetros:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 192.168.70.254/24
- Administrative Access: HTTPS, HTTP, PING, SSH

Finalmente se verifican las interfaces respectivas como se muestra en la Figura 3.186.

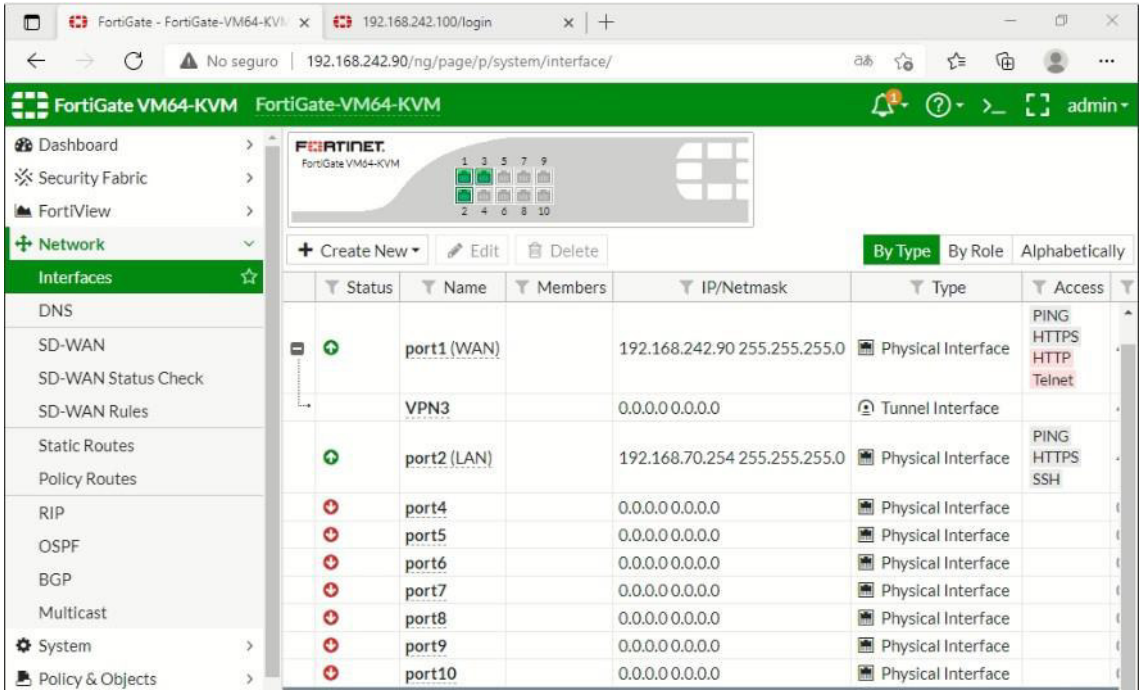


Figura 3.186 Interfaces en Fortigate CENTRAL 2

Del mismo modo que la central 1 se procede a asignar el *Gateway* del enlace ISP al enlace SDWAN como se muestra en la Figura 3.187.

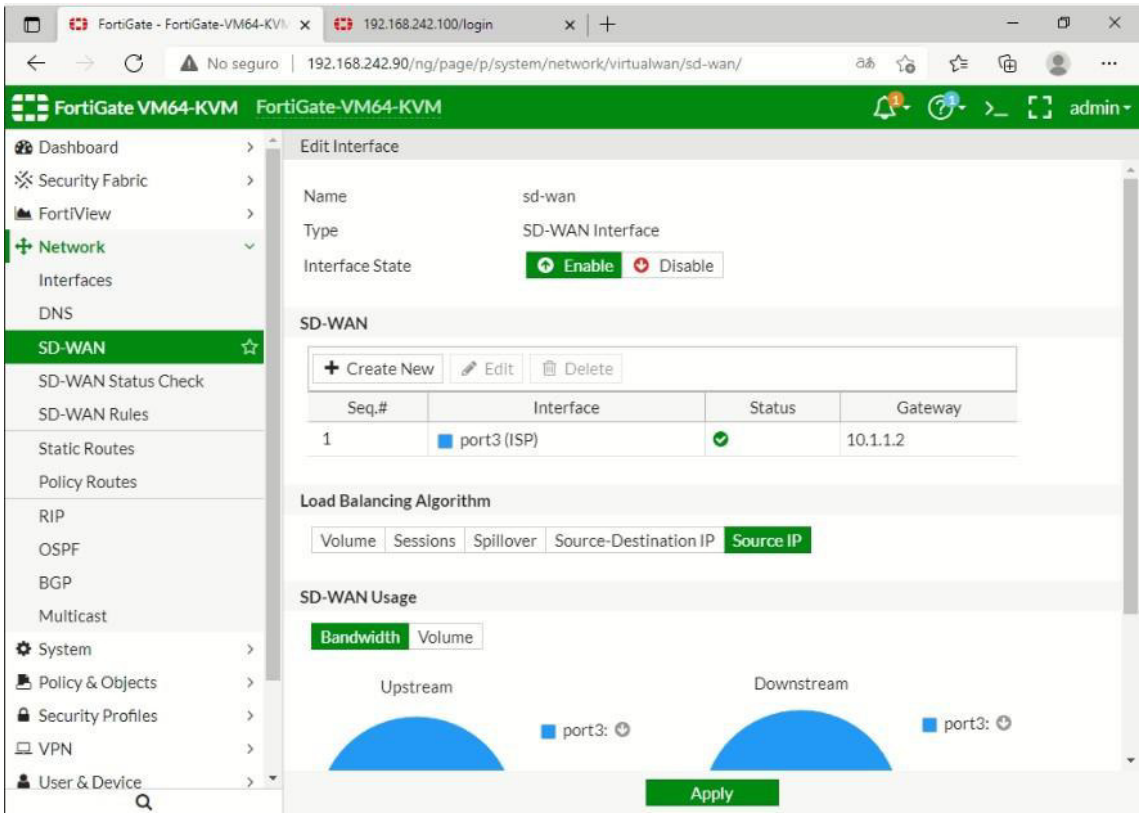


Figura 3.187 Configuración de SDWAN CENTRAL 2

De igual manera se procede a la configuración de la ley respectiva para el enlace de SD-WAN para lo cual se siguen los parámetros que se muestran a continuación:

- Name: LEY3
- Server: 10.1.1.2
- Timeout: 10 seconds

A continuación, se procede a la configuración de una regla que facilite el monitoreo de todo el tráfico que circule por medio del enlace SD-WAN; para ello se realizan las siguientes modificaciones. Mismas que se pueden observar en la Figura 3.188.

- Name: ley3
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 10.1.1.2
- Status Check: LEY3

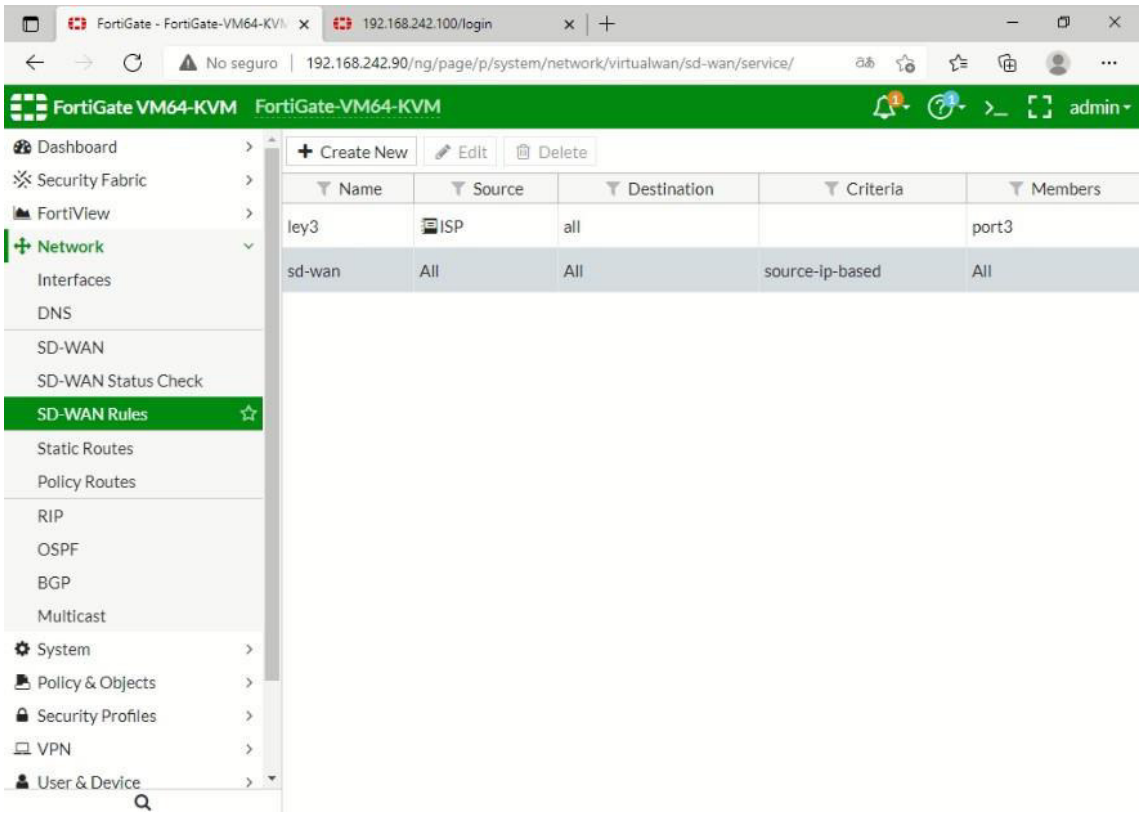


Figura 3.188 Configuración de reglas SDWAN CENTRAL 2

De igual manera que en la red pasada se procede a configurar un túnel VPN en este equipo para ello se modifican los siguientes parámetros:

- Name: VPN-3
- Type: site to site
- Remote: Fortigate
- Nat: no nat
- Ip: 192.168.242.100
- Outgoing interface: WAN (port1)
- Pre-shared key: clave12345
- Local interface: LAN
- Local subnets: 192.168.70.0/24
- Remote subnets: 10.70.16.0/24

Como se aprecia; la clave de ingreso para esta central es distinta; esto se debe a que se encuentra en otra red. Pero es importante conocer que se debe hacer coincidir esta clave con la de la sucursal 2 para que exista un correcto establecimiento de la comunicación. La creación de este túnel se puede apreciar en el apartado de "*VPN > IPsec Tunnels"* como se muestra en la Figura 3.189.

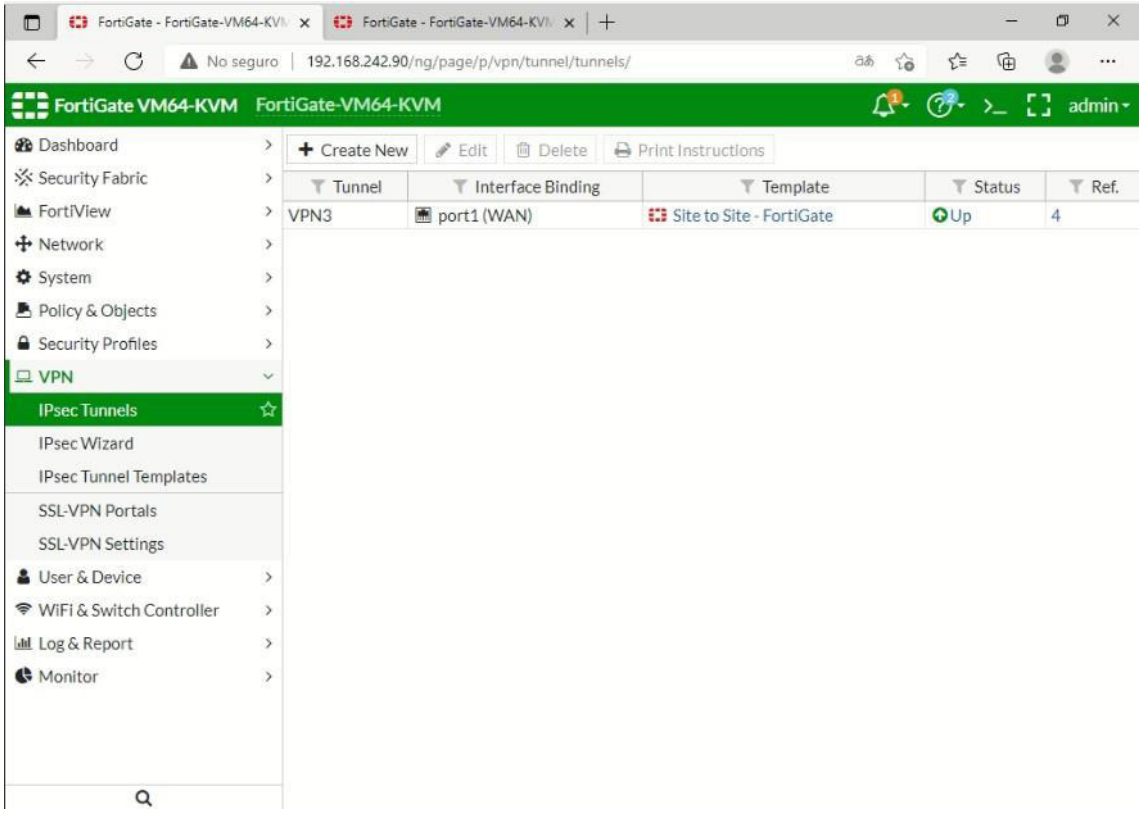


Figura 3.189 Configuración de VPN en CENTRAL 2

De igual manera, las políticas se generan automáticamente por lo que únicamente se debe configurar la política de salida a Internet; para ello se configuran los siguientes parámetros. Mismos que se aprecian en la Figura 3.190.

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

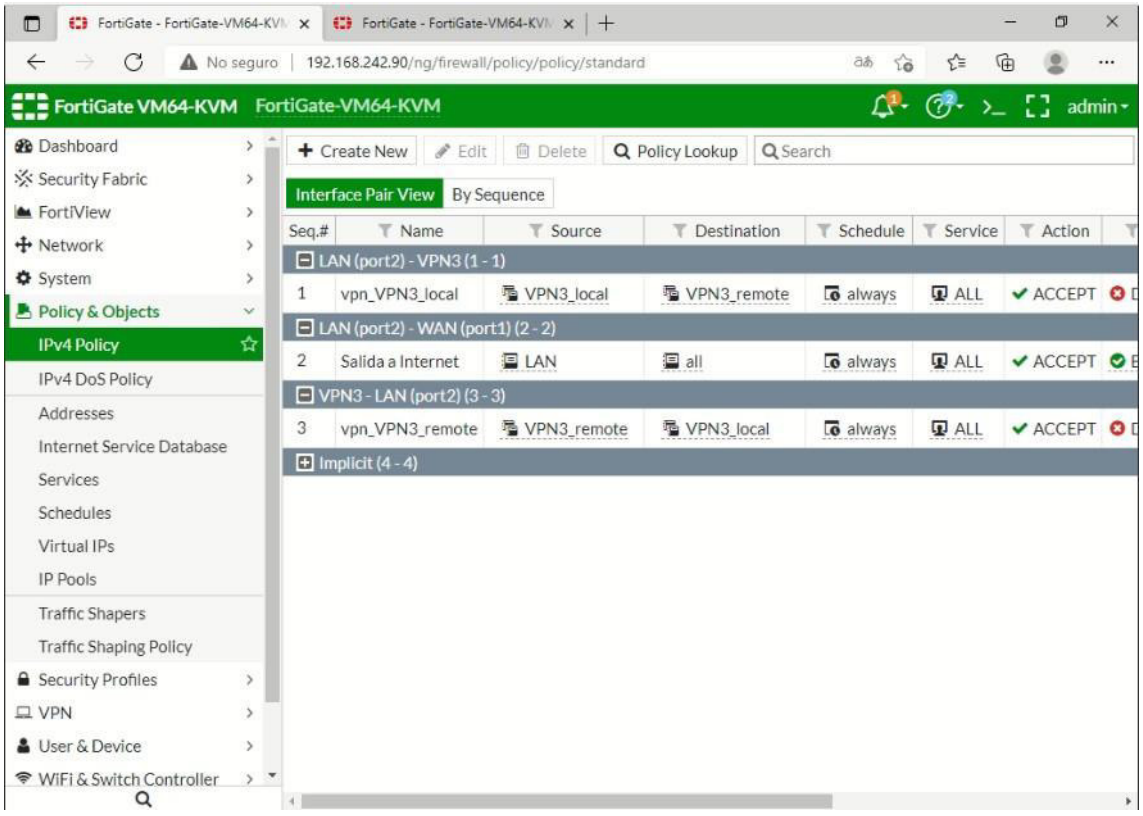


Figura 3.190 Políticas para acceso CENTRAL 2

Posteriormente, se procede a revisar las direcciones creadas automáticamente para verificar que tanto las direcciones como los permisos coinciden con lo configurado previamente como se muestra en la Figura 3.191.

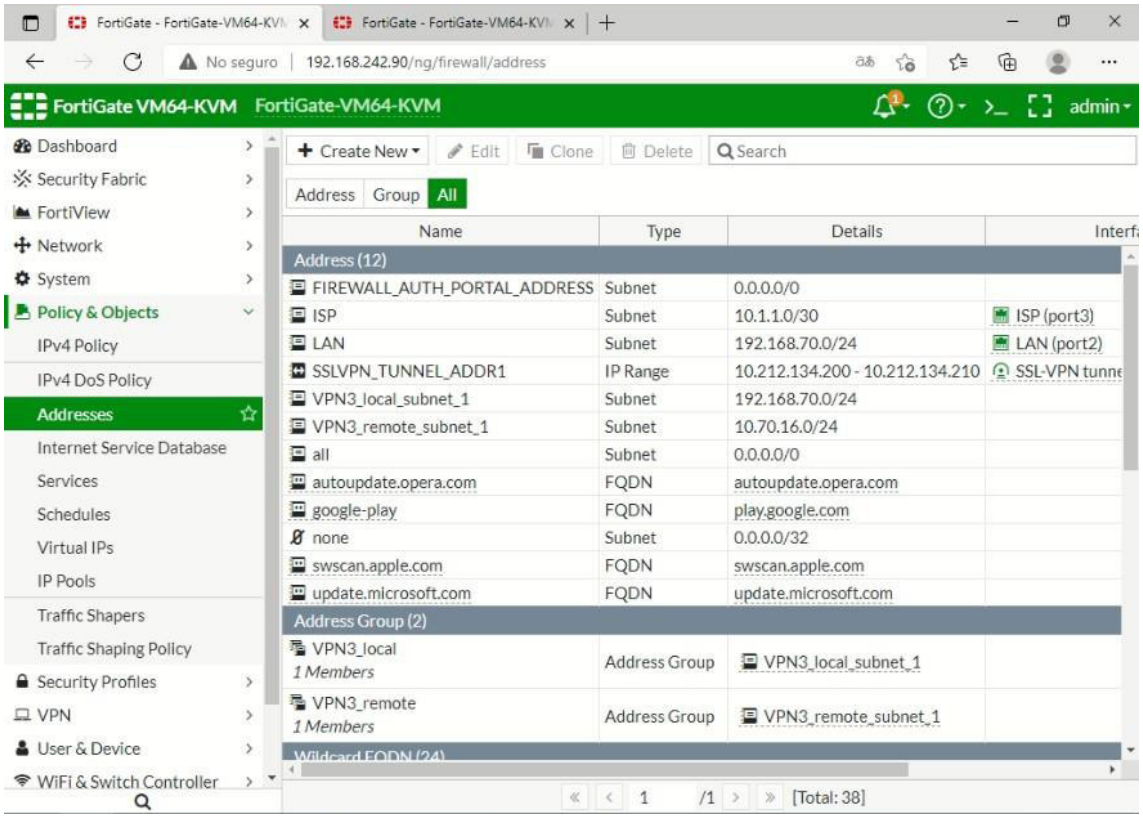


Figura 3.191 Configuración de una dirección para políticas CENTRAL 2

Al igual que en la central 1, para que exista comunicación con las sucursales, se debe implementar una ruta por defecto; para ello se modifican los siguientes parámetros. Mismos que se aprecian en la Figura 3.192.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

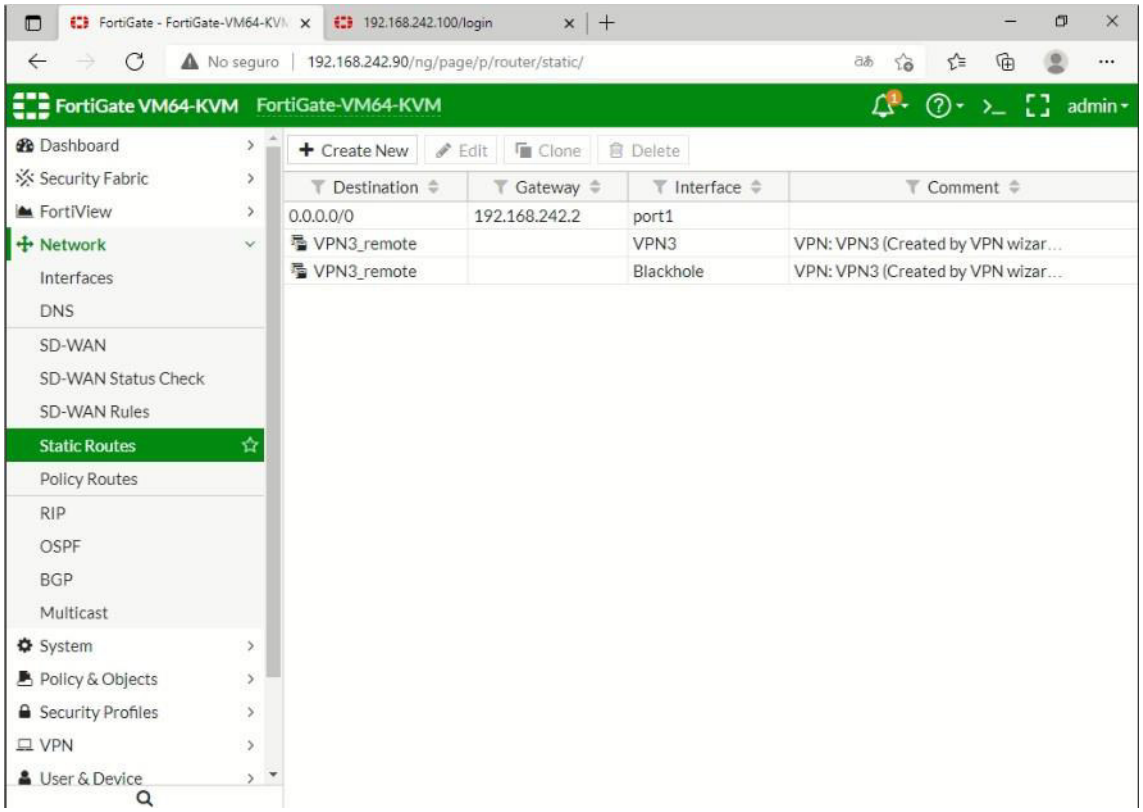


Figura 3.192 Configuración de una ruta por defecto Central 2

Finalmente, se procede a verificar las interfaces en el apartado de "*Network > Interfaces"* como se muestra en la Figura 3.193.

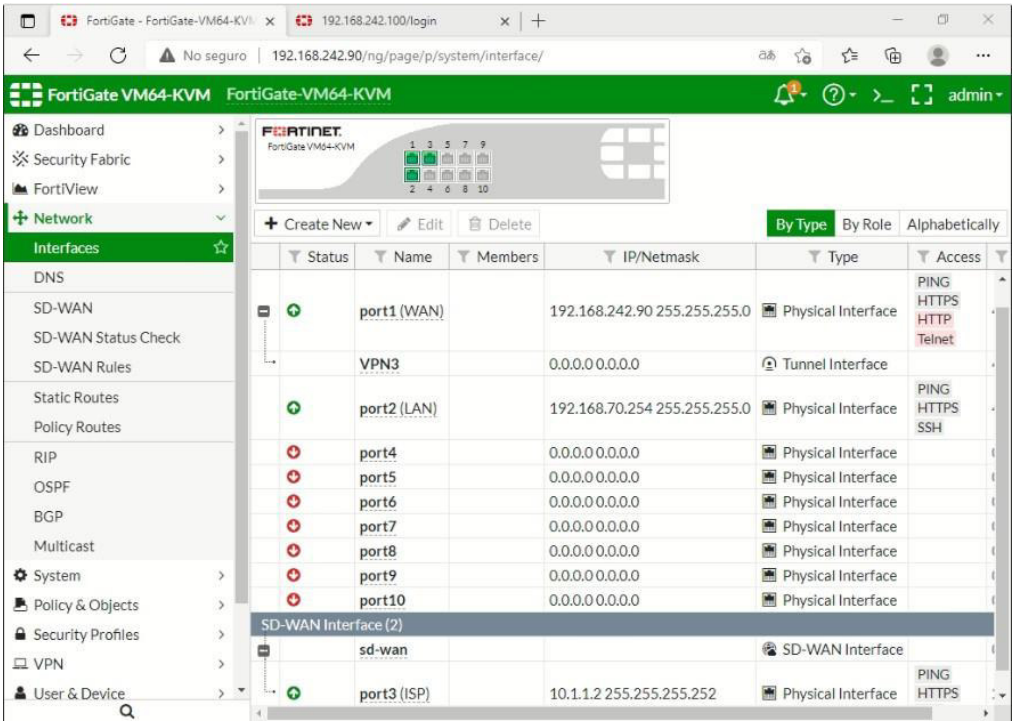


Figura 3.193 Configuración de interfaces en CENTRAL 2

Configuración Sucursal 1

El primer paso es acceder a la interfaz gráfica del equipo Fortigate para lo cual se procede a escribir la dirección 192.168.242.80 en el buscador de preferencia y se accede con las credenciales por defecto. La primera interfaz a configurar es la de conectividad a internet modificando los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.80/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING, TELNET

A continuación, se procede a configurar la interfaz del enlace serial denominada ISP como se muestra a continuación:

- Alias: ISP-1
- Role: WAN
- IP/Network Mask: 10.1.1.2/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Finalmente, se procede a configurar la interfaz LAN mediante la aplicación de los siguientes parámetros:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 10.60.26.254/24
- Administrative Access: HTTPS, HTTP, PING, SSH

El procedimiento previamente mencionado se puede observar en la Figura 3.194.

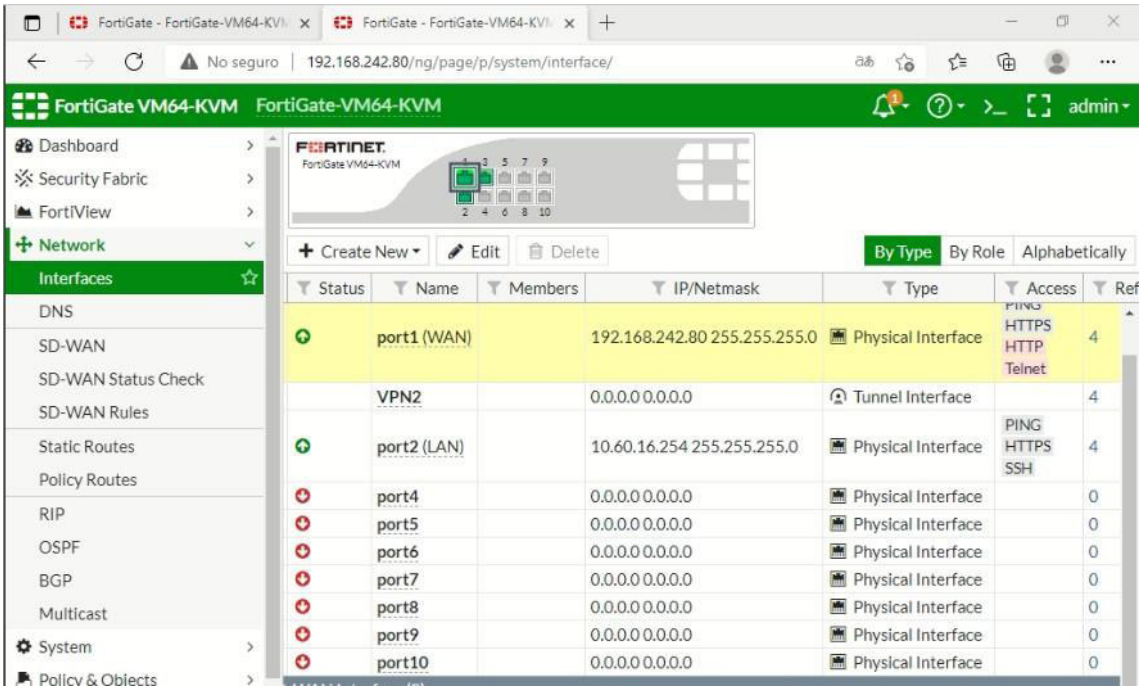


Figura 3.194 Interfaces en Fortigate SUCURSAL 1

Posteriormente se procede a configurar el *Gateway* para el enlace SDWAN en la red este *Gateway* será el utilizado para la interfaz ISP como se muestra en la Figura 3.195.

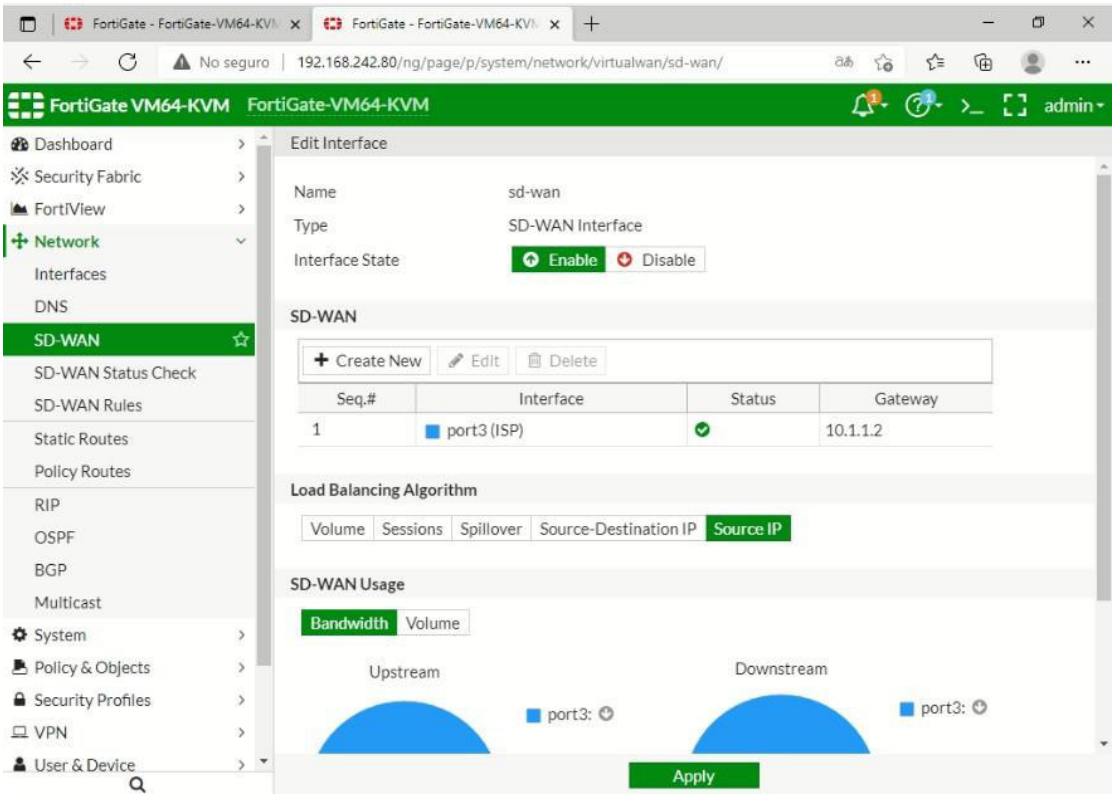


Figura 3.195 Configuración de SDWAN SUCURSAL 1

Una vez definido este enlace SD-WAN se procede a configurar la ley respectiva, Así como la regla para poder mantener un monitoreo efectivo sobre todo el tráfico que circule dentro de la red SDWAN. Este procedimiento se detalla a continuación y se lo puede observar en la Figura 3.196.

Establecimiento de una ley SD-WAN

- Name: LEY2
- Server: 10.1.1.2
- Timeout: 10 seconds

Establecimiento de una regla SD-WAN

- Name: ley2
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 10.1.1.2
- Status Check: LEY2

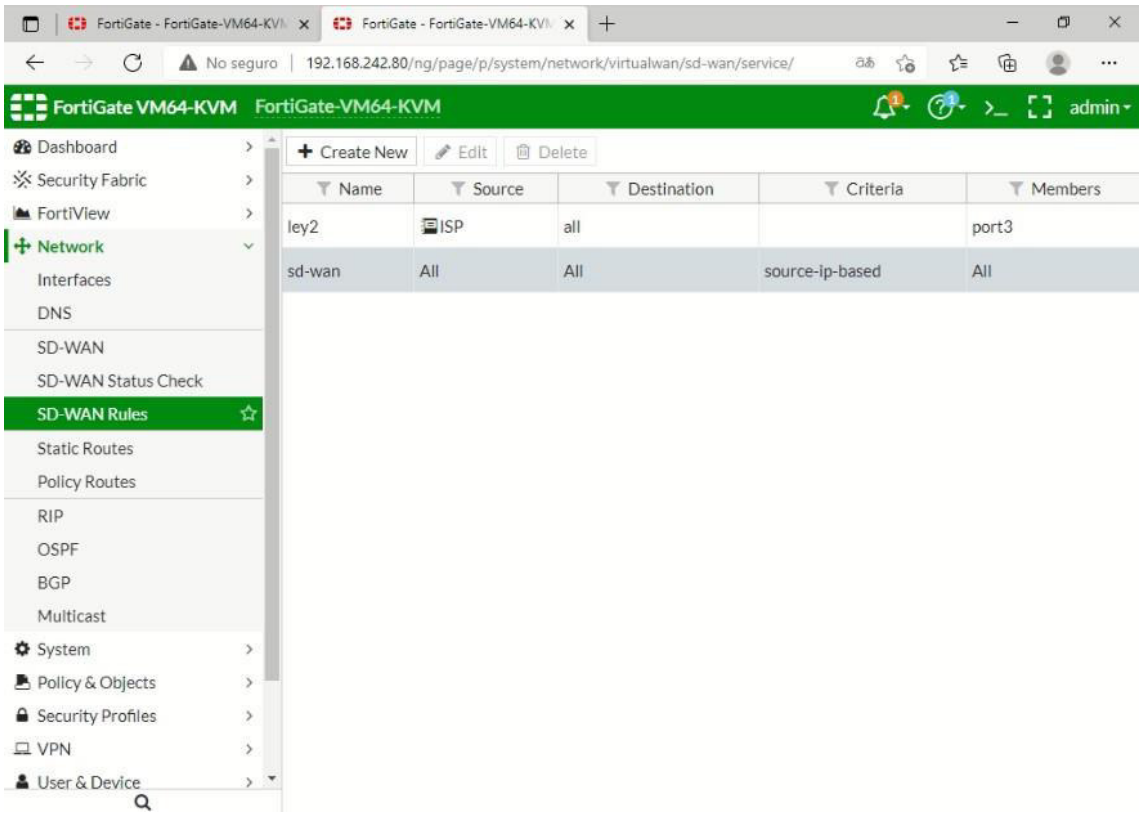


Figura 3.196 Configuración de reglas SDWAN SUCURSAL 1

De igual manera que en las centrales se debe configurar los túneles VPN respectivos para obtener comunicación por medio de este medio con las centrales respectivas para cada sucursal. Los parámetros que se deben modificar son los siguientes:

- Name: VPN-2
- Type: site to site
- Remote: Fortigate
- Nat: no nat
- IP: 192.168.242.70
- Outgoing interface: WAN (port1)
- Pre-shared key: tesis12345
- Local interface: LAN
- Local subnets: 10.60.16.0/24
- Remote subnets: 192.168.60.0/24

Como se había mencionado previamente se debe hacer coincidir las contraseñas para este caso las contraseña que se colocó en la central 1 debe ser la misma que se coloque en este apartado para de este modo se pueda obtener una correcta comunicación entre la central 1 y la sucursal 1. Una vez establecido este procedimiento se procede a revisar el estado de esta conexión que se encuentre arriba en el apartado de "*VPN > IPsec Tunnels",* como se aprecia en la Figura 3.197.

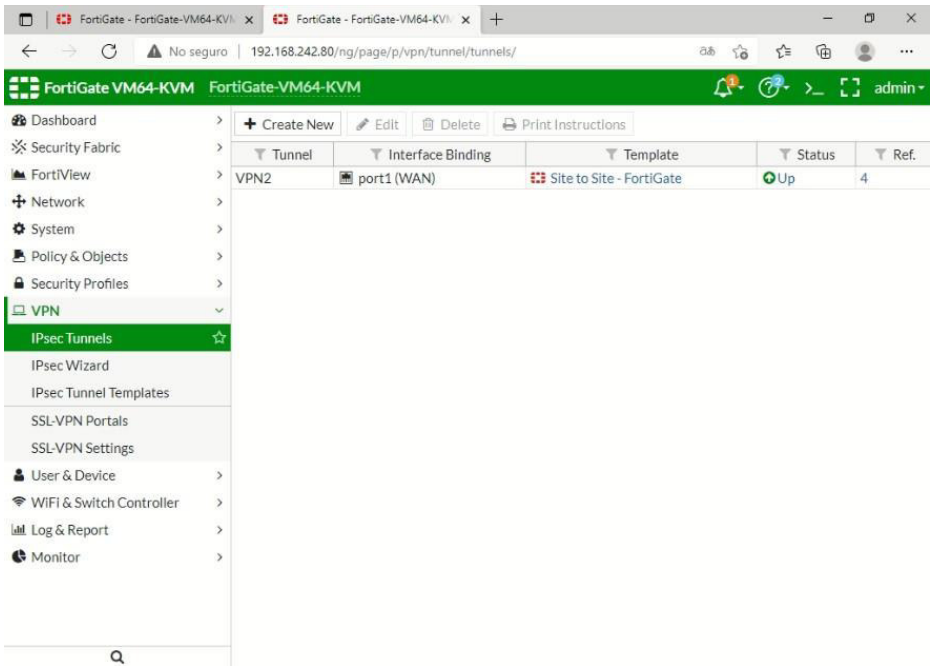


Figura 3.197 Configuración de VPN en SUCURSAL 1

Del mismo modo que en casos previos, se procede a configurar una política de salida a internet mediante la implementación de los siguientes parámetros. Esta política junto con las políticas generadas automáticamente con la configuración de túneles VPN se puede observar en la Figura 3.198.

- Name: Salida a Internet
- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

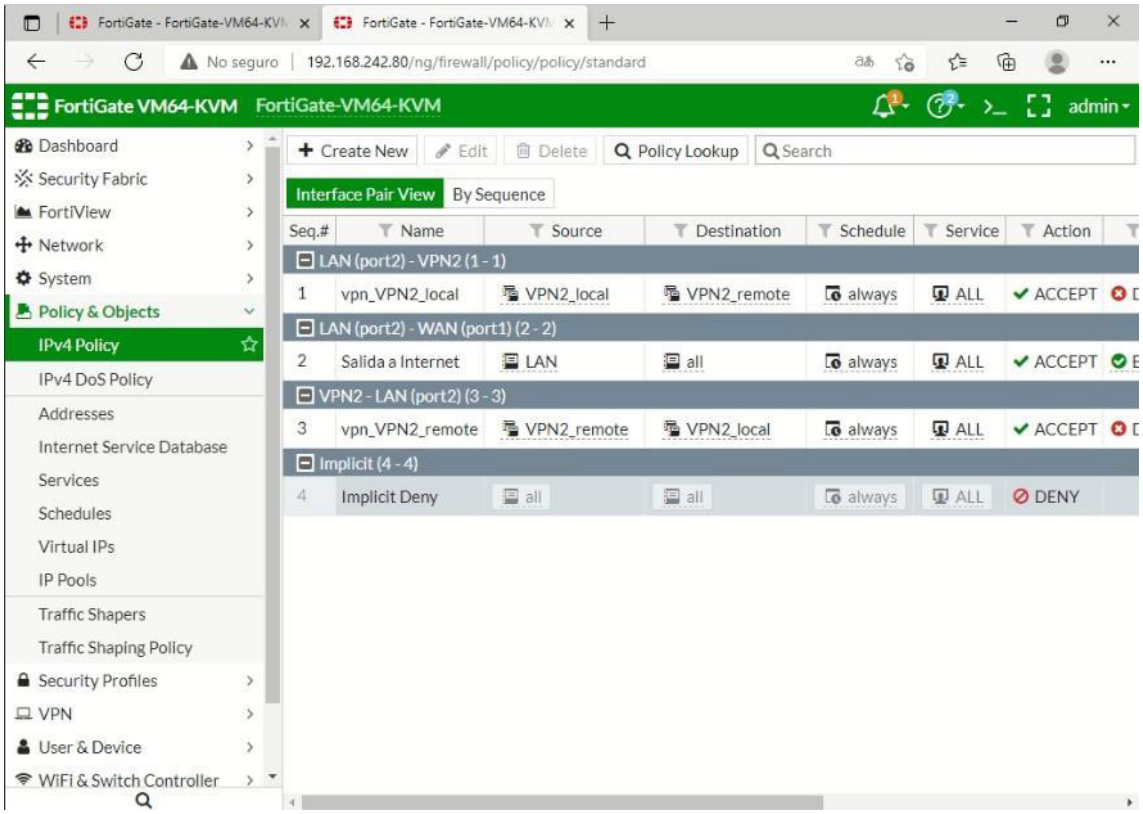


Figura 3.198 Políticas para acceso SUCURSAL 1

Adicionalmente, se procede a verificar que tanto las direcciones de la red LAN locales como remotas se configuraron correctamente como se muestra en la Figura 3.199.

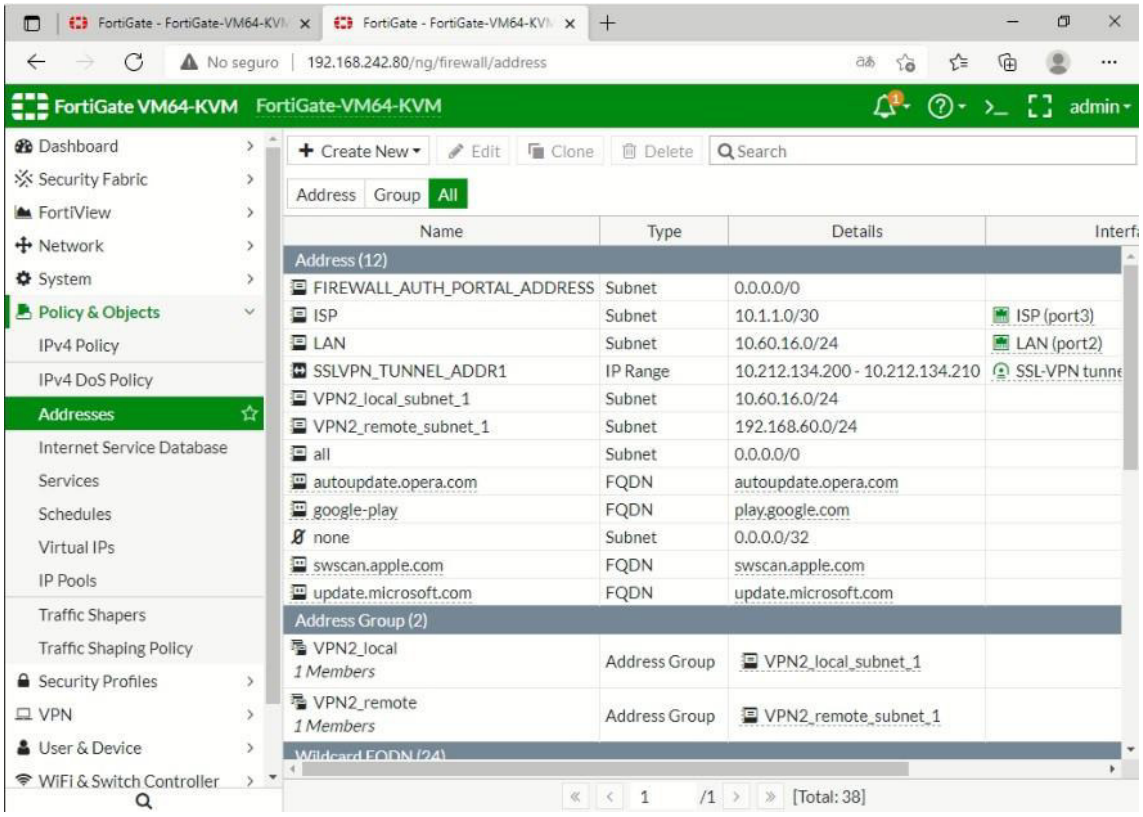


Figura 3.199 Configuración de dirección para políticas SUCURSAL 1

Como último paso para configurar esta sucursal se procede a configurar una ruta estática por defecto siguiendo estos parámetros. Mismos que se aprecian en la Figura 3.200.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

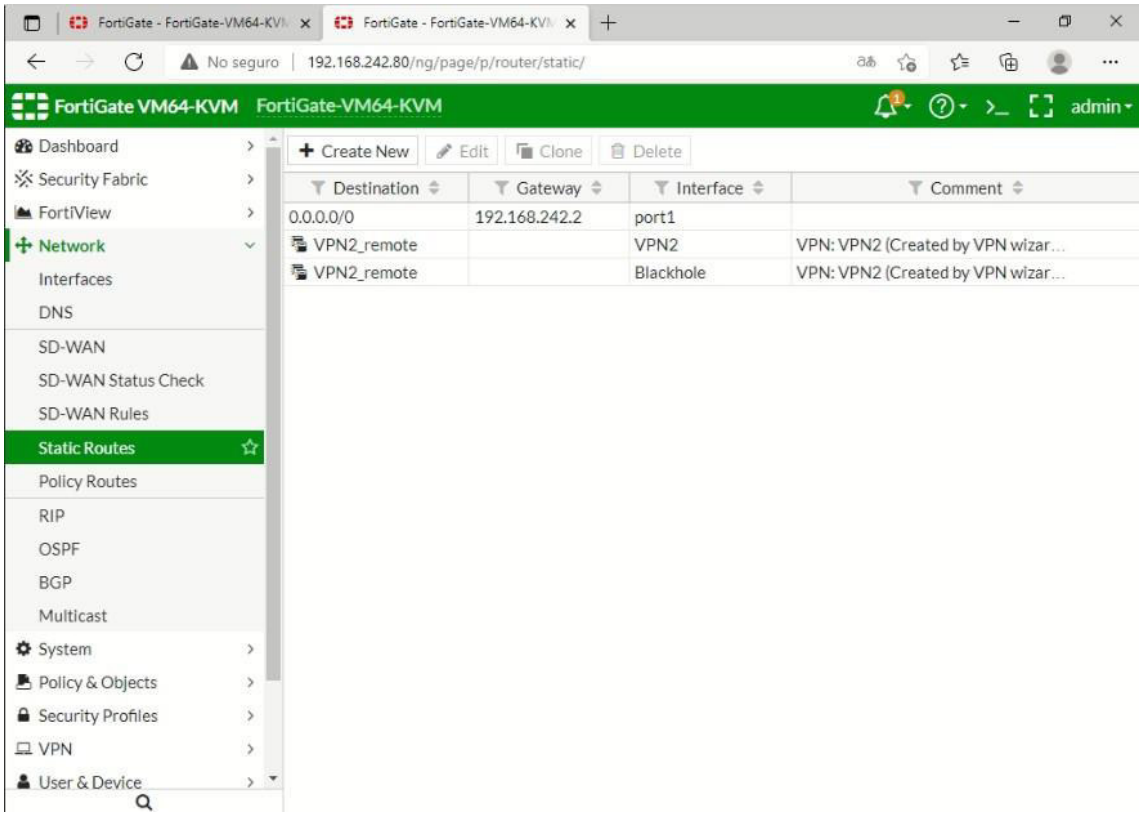


Figura 3.200 Configuración de una ruta por default Sucursal 1

Finalmente, se procede a la comprobación de las interfaces accediendo al apartado de *"Network > Interfaces",* como se muestra en la Figura 3.201.

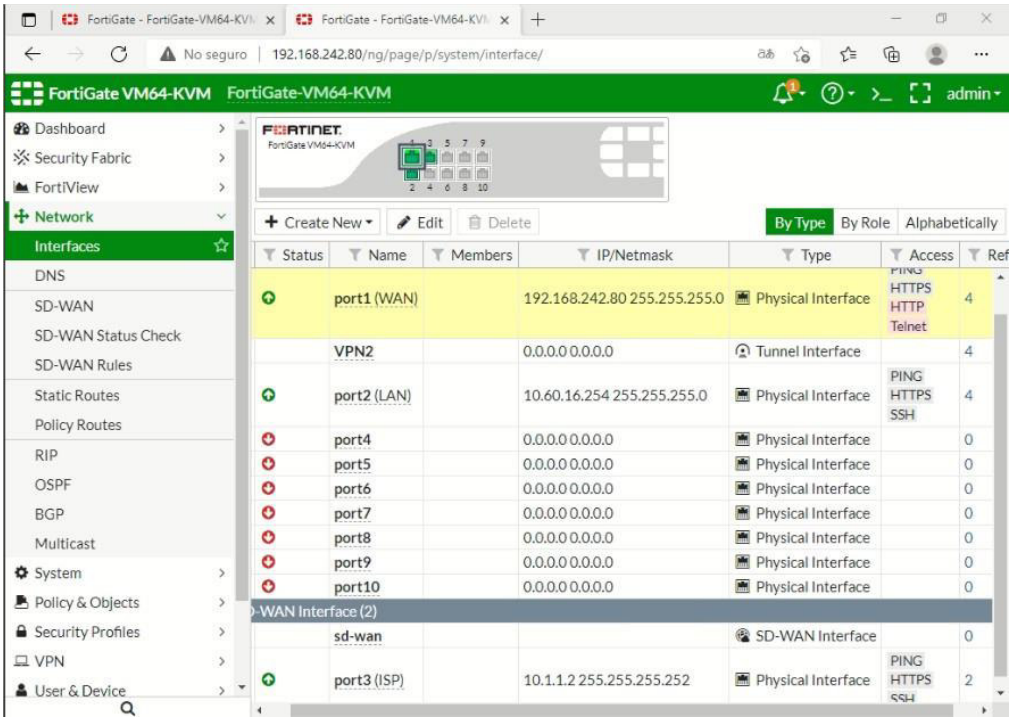


Figura 3.201 Configuración de interfaces en SUCURSAL 1

Configuración Sucursal 2

Para concluir con la configuración de la red se accede a la interfaz gráfica de este equipo para ello se escribe la dirección 192.168.242.100 en el buscador de preferencia y se accede con las credenciales previamente mencionadas. Primero se debe configurar la interfaz de salida a Internet mediante la aplicación de los siguientes parámetros:

- Alias: WAN
- Role: WAN
- IP/Network Mask: 192.168.242.70/255.255.255.0
- Administrative Access: HTTPS, HTTP, PING, TELNET

Adicionalmente, se configura la interfaz serial respectiva como ISP como se muestra en el procedimiento a continuación:

- Alias: ISP
- Role: WAN
- IP/Network Mask: 10.1.1.1/30
- Administrative Access: HTTPS, HTTP, PING,SSH

Con estos parámetros configurados se procede a configurar los parámetros de la red LAN con el siguiente procedimiento:

- Alias: LAN
- Role: LAN
- IP/Network Mask: 10.70.16.254/24
- Administrative Access: HTTPS, HTTP, PING, SSH

Estos cambios se pueden observar en la Figura 3.202 a continuación.

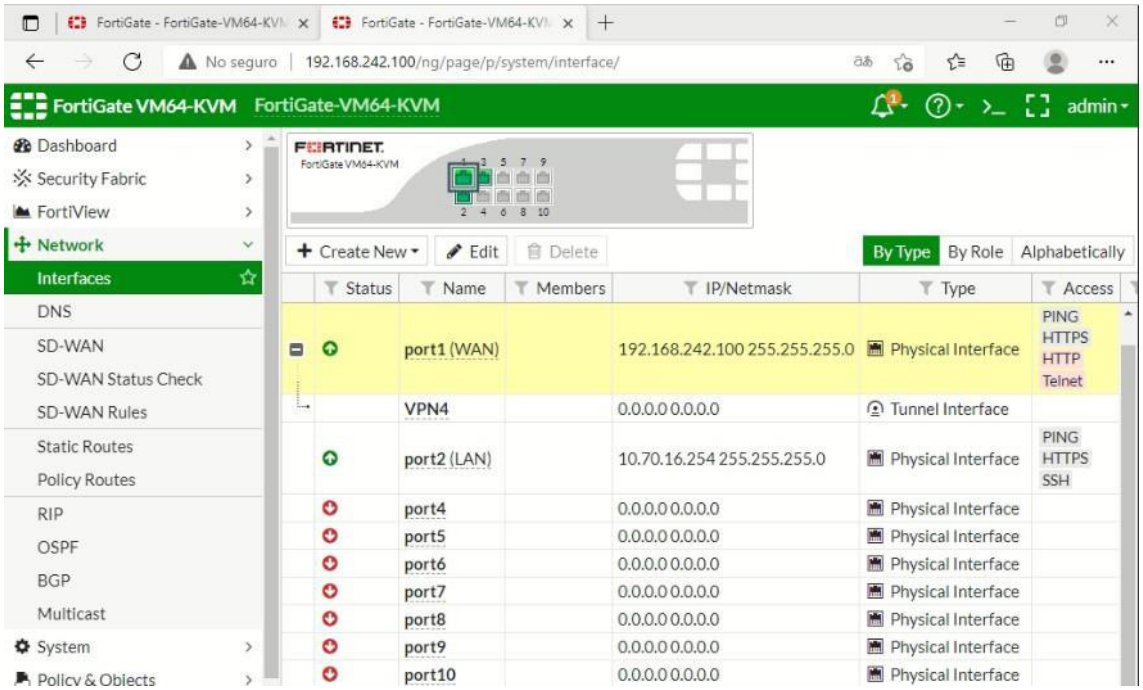


Figura 3.202 Interfaces en Fortigate SUCURSAL 2

A continuación, se procede a asignar el *Gateway* que deberá funcionar con un enlace de SD-WAN, el *Gateway* utilizado para este caso será la interfaz de ISP como se muestra en la Figura 3.203.

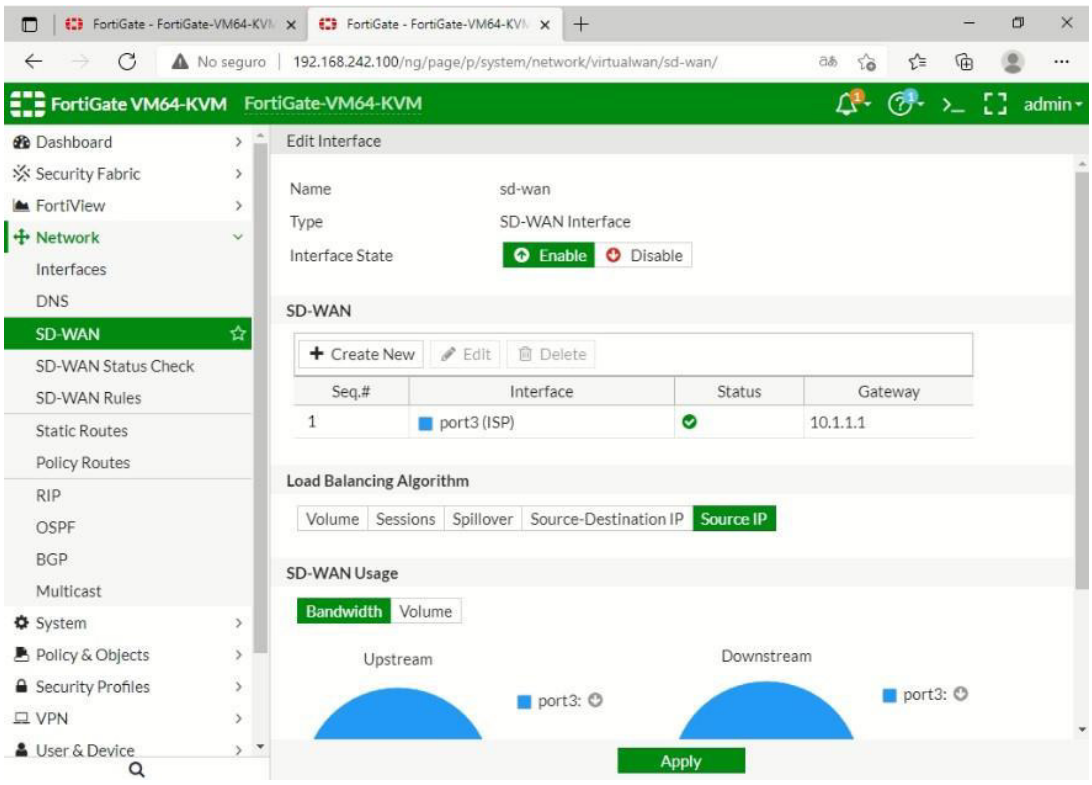


Figura 3.203 Configuración de SDWAN SUCURSAL 2

Acto seguido se procede a configurar la ley respectiva para poder monitorear el tráfico que circule en el enlace de SD-WAN. Los procedimientos necesarios para configurar tanto la ley como la regla respectiva se detallan a continuación, mismos que se pueden observar en la Figura 3.204.

Establecimiento de una ley SD-WAN

- Name: LEY4
- Server: 10.1.1.1
- Timeout: 10 seconds

Establecimiento de una regla SD-WAN

- Name: ley4
- Source Address: All
- Destination Address: All
- Interface Members: Gateway 10.1.1.1
- Status Check: LEY4

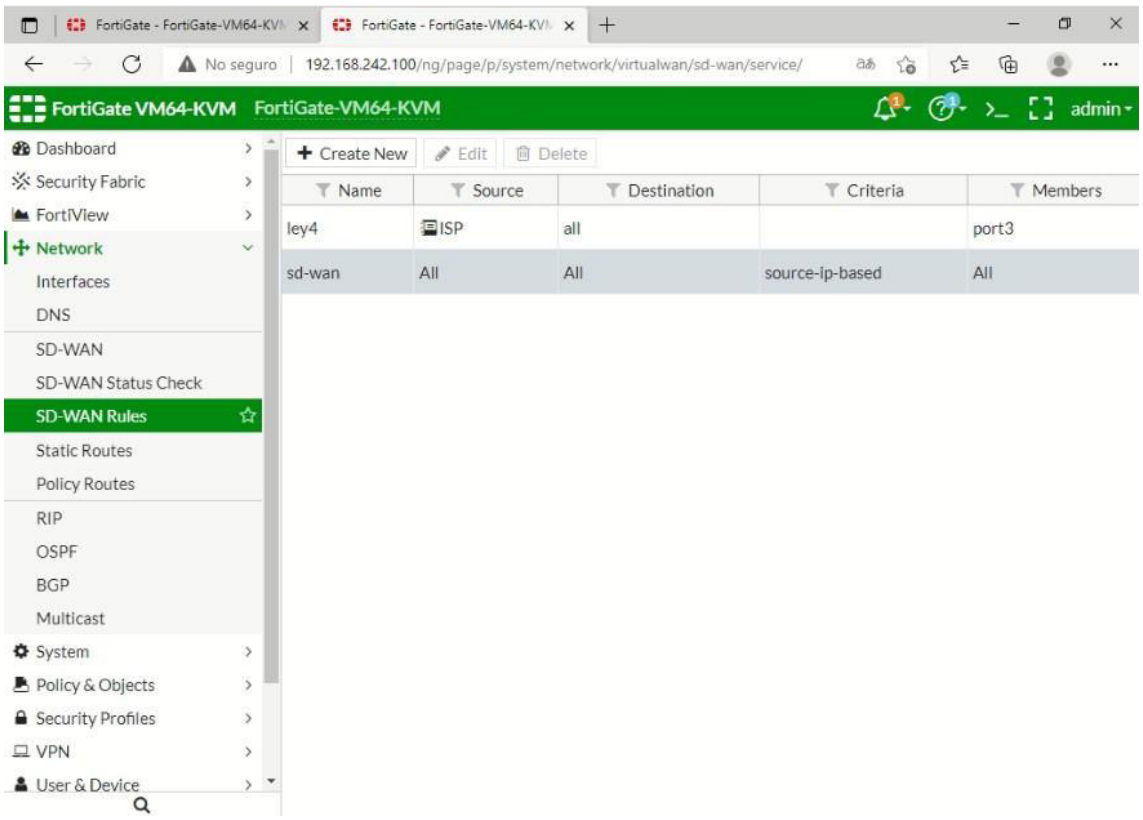


Figura 3.204 Configuración de reglas SDWAN SUCURSAL 2

A continuación, se procede a configurar un túnel de tipo VPN para establecer comunicación de esta forma con la central 2, para esto es necesario conocer la calve

que se escribió con antelación en la central 1. Para lograr esto se modifican los parámetros detallados a continuación, mismos que se aprecian en la Figura 3.205.

- Name: VPN-4
- Type: site to site
- Remote: Fortigate
- Nat: no nat
- IP: 192.168.242.90
- Outgoing interface: WAN (port1)
- Pre-shared key: tesis12345
- Local interface: LAN
- Local subnets: 10.70.16.0/24
- Remote subnets: 192.168.70.0/24

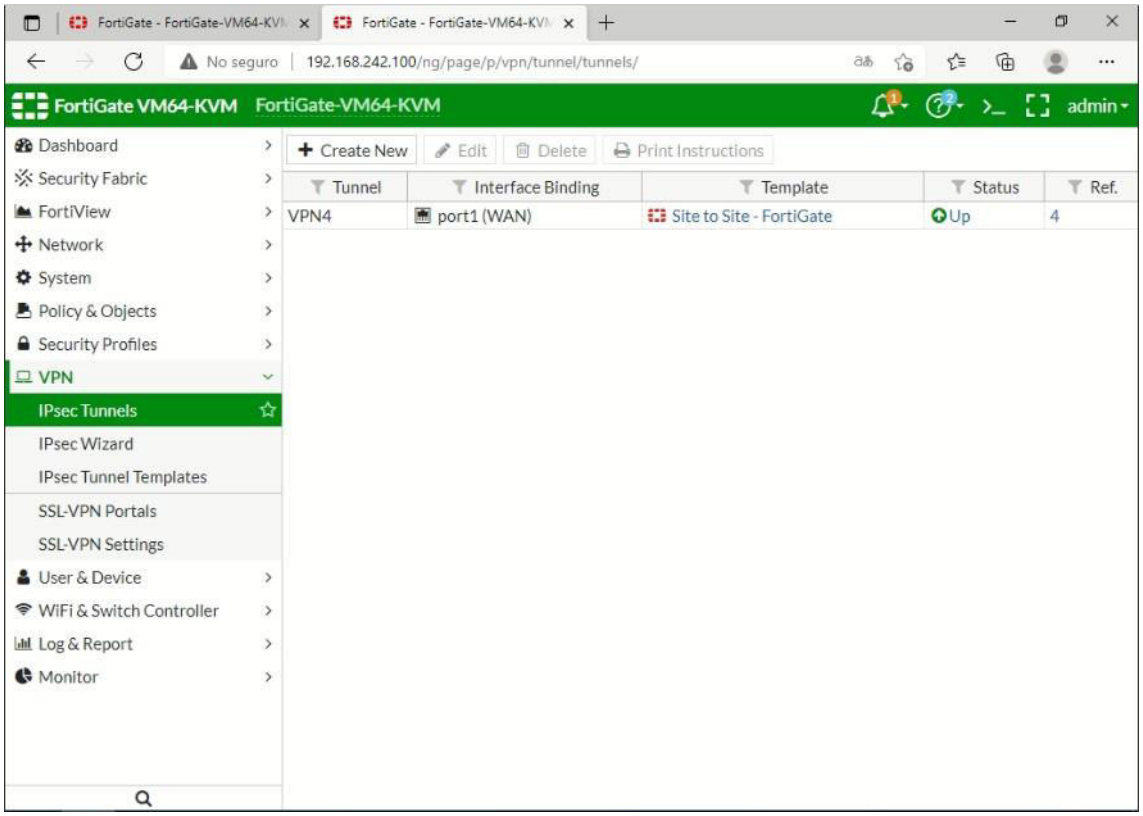


Figura 3.205 Configuración de VPN en SUCURSAL 2

Del mismo modo que en las redes pasadas se procede a configurar la política para acceso a Internet y a confirmar las mismas en el apartado de *"Policy & Objects > IPv4 Policy".* como se detalla a continuación y se observa en la Figura 3.206.

- Name: Salida a Internet
- Incoming Interface: LAN

- Outgoing Interface: WAN
- Source: LAN
- Destination: ALL
- Service: ALL

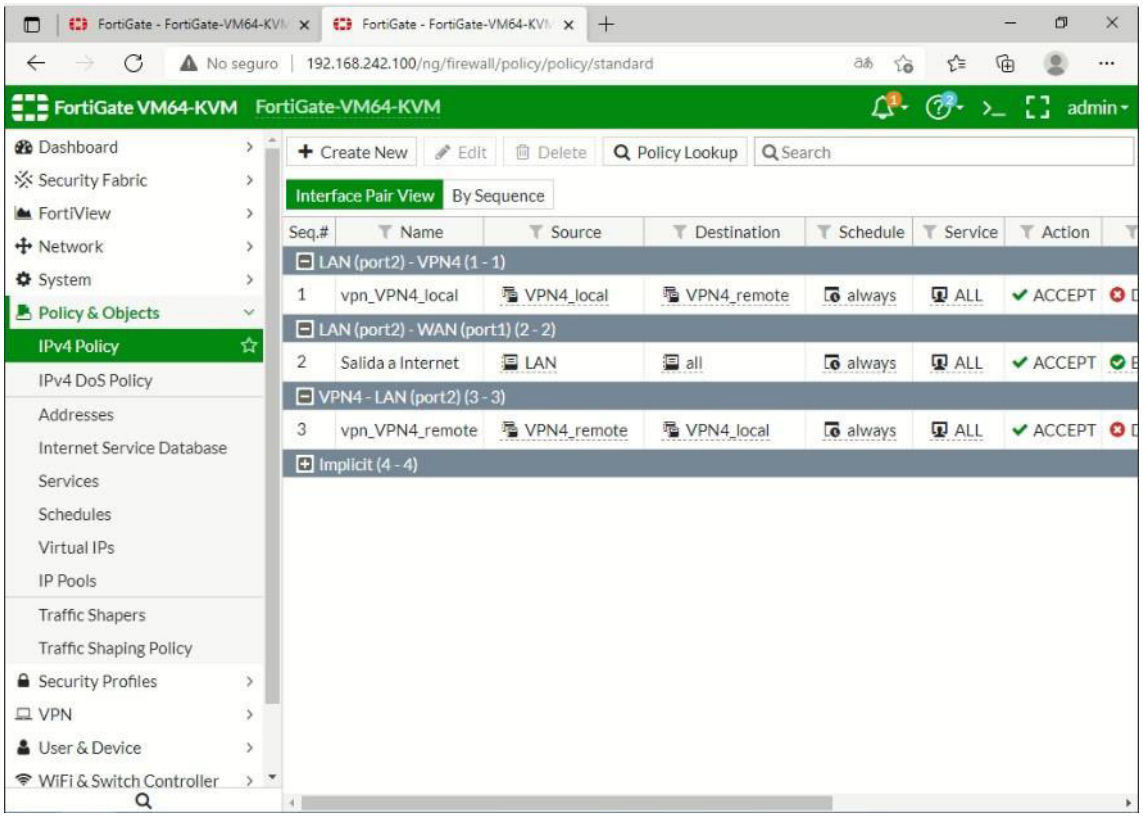


Figura 3.206 Políticas para acceso SUCURSAL 2

Para comprobar que las direcciones se generaron de forma automática se procede a ingresar al apartado de "*Policy & Objects* > *Addresses"* como se muestra en la Figura 3.207.

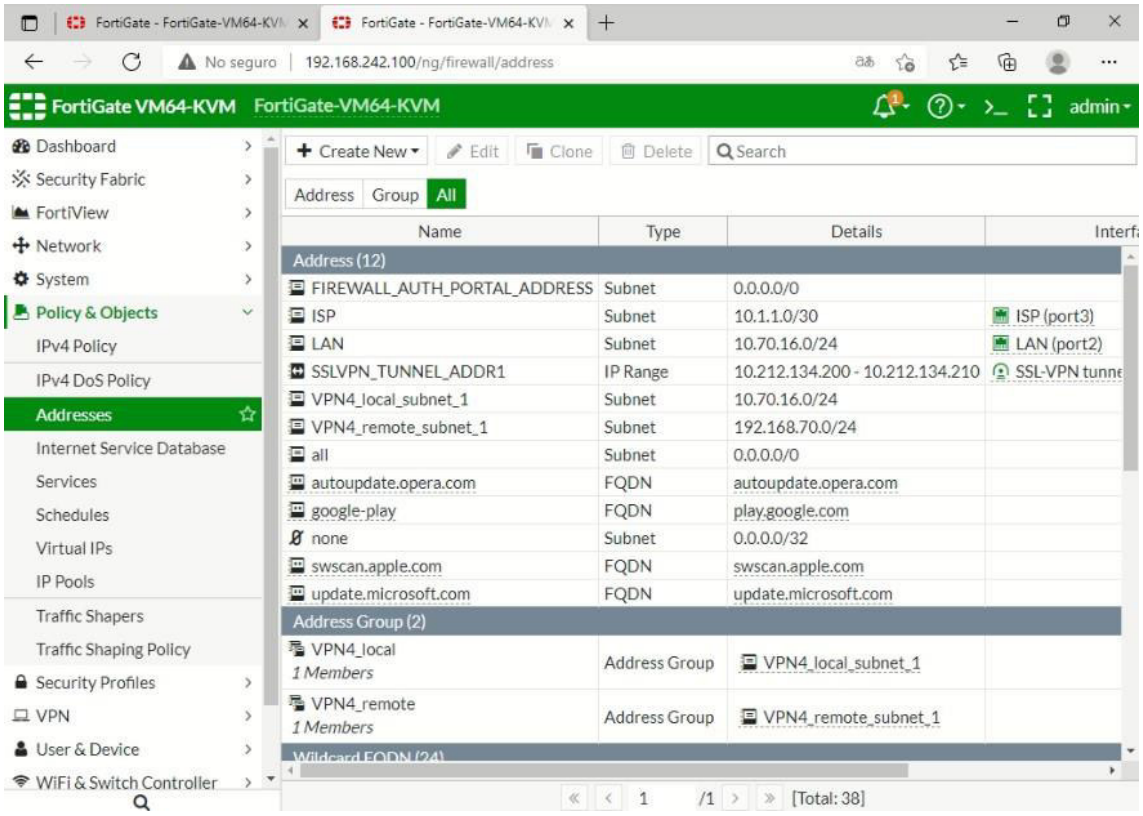


Figura 3.207 Configuración de dirección para políticas SUCURSAL 2

Para terminar con la configuración de esta red se procede a configurar una ruta estática por *default* la misma que permitirá la conexión por medio de la Internet y para realizar esta acción se procede a implementar los siguientes parámetros. Los mismos que se aprecian en la Figura 3.208.

- Destination: 0.0.0.0/0.0.0.0
- Device: WAN
- Gateway: 192.168.242.2

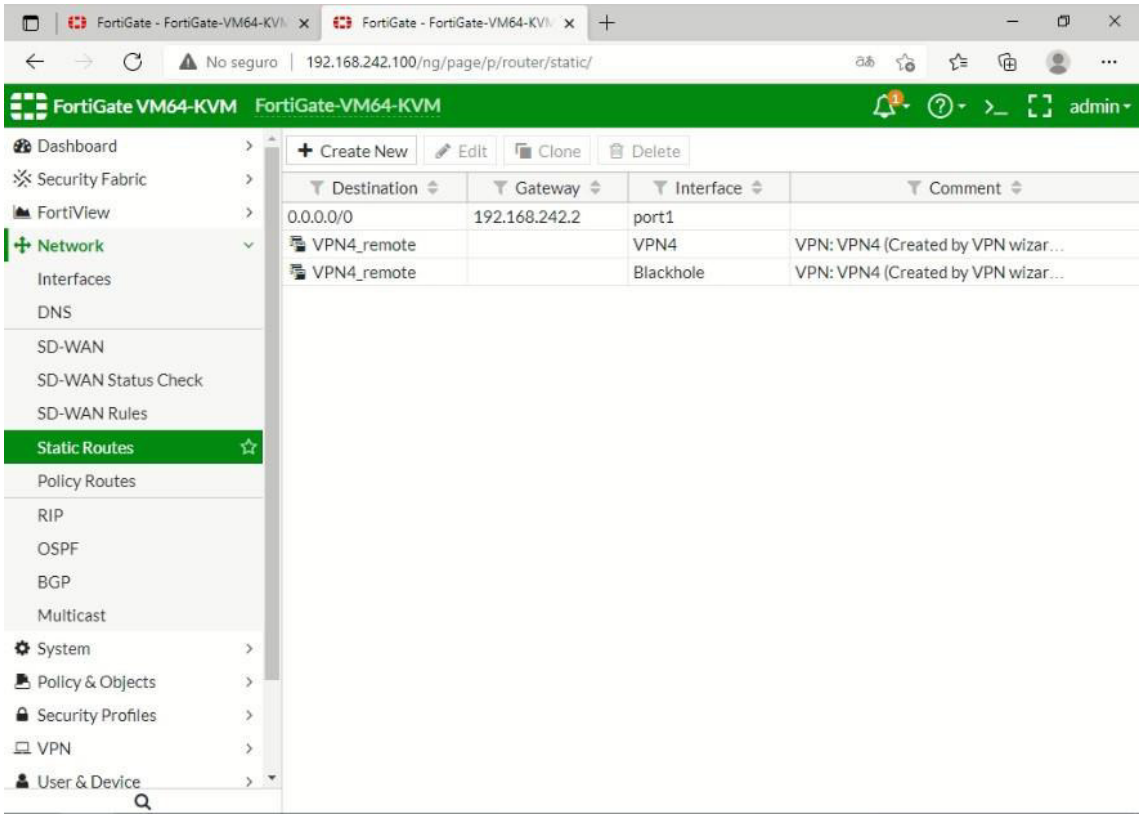


Figura 3.208 Configuración de una ruta por default Sucursal 2

Finalmente, se procede a revisar en el apartado de "*Network > Interfaces*" que tanto las interfaces como los servicios que se están ejecutando lo hagan de manera satisfactoria como se muestra en la Figura 3.209.

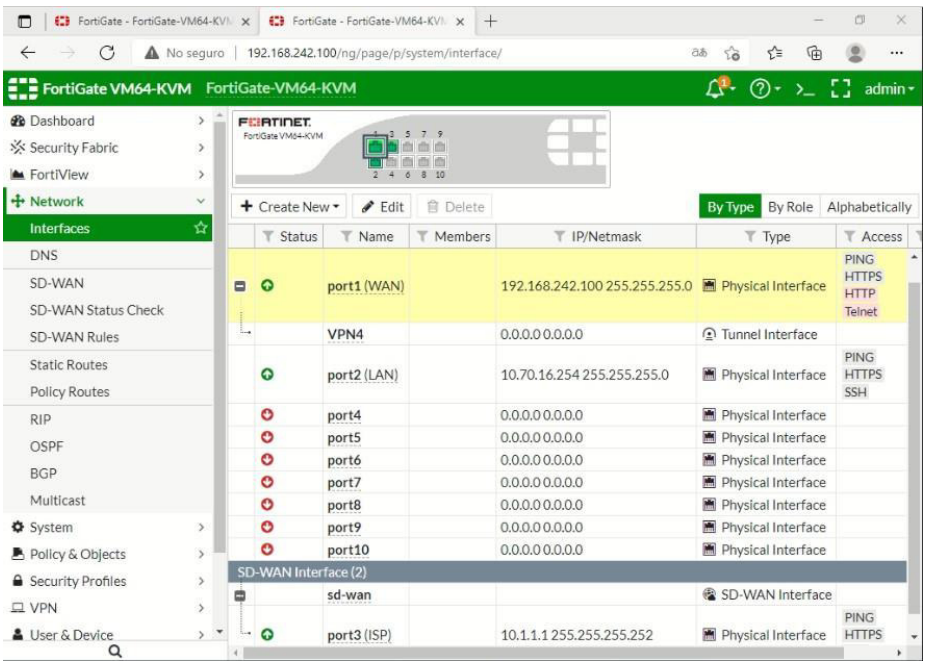


Figura 3.209 Configuración de interfaces en SUCURSAL 2

3.4 Realizar pruebas sobre la red virtualizada SD-WAN en GNS3

Pruebas Red SDWAN-CISCO

Para la realización de las pruebas se utilizan diferentes comandos en los equipos, el primer comando utilizado es el "*show control local-properties*" este comando desplegará información sobre el equipo analizado. Así como las conexiones que tiene el mismo, Los equipos analizados fueron el nodo central *vManage*, el enrutador *vSmart* y el equipo *vBond*. El apartado de "*certificate-status"* debe encontrarse instalado para validar que el equipo se encuentra operativo en su totalidad, para ello se puede analizar diferentes parámetros, como el número de serie o la fecha de validez de los certificados instalados. Adicionalmente, se muestran todas las direcciones a las cuales el equipo se encuentra conectado y por medio de qué interfaz está saliendo el tráfico y si las conexiones se encuentran activas o no, en nuestro caso se aprecia que los equipos conocen las direcciones de los equipos vecinos con lo cual se puede apreciar que existe conexión en la red SD-WAN visto la Figura 3.210, la Figura 3.211 y la Figura 3.212.

```
vmanage# show control local-properties
personality                     vmanage
sp-organization-name            sd-wan-lab
organization-name               sd-wan-lab
root-ca-chain-status            Installed

certificate-status              Installed
certificate-validity            Valid
certificate-not-valid-before    Sep 14 03:04:42 2021 GMT
certificate-not-valid-after     Mar 07 03:04:42 2027 GMT

dns-name                        200.1.1.1
site-id                         503
domain-id                       0
protocol                        dtls
tls-port                        23456
system-ip                       50.3.0.2
chassis-num/unique-id           347e81d8-bb39-402b-88b1-bc06e66f954a
serial-num                      B6948B4A5B09634D
cloud-hosted                    no
token                           -NA-
retry-interval                  0:00:00:15
no-activity-exp-interval        0:00:00:20
dns-cache-ttl                   0:00:02:00
port-hopped                     FALSE
time-since-last-port-hop        0:00:00:00
number-vbond-peers              1

INDEX   IP                                      PORT
------------------------------------------------------
0       200.1.1.1                               12346

number-active-wan-interfaces    4

                                PUBLIC          PUBLIC PRIVATE        PRIVATE                                 PRIVATE                                 LAST
INSTANCE            INTERFACE   IPv4            PORT   IPv4           IPv6                                    PORT    VS/VM  COLOR            STATE CONNECTION
-------------------------------------------------------------------------------------------------------------------------------------------------------------
0       eth0        200.1.1.2       12346  200.1.1.2       ::                                      12346   1/0    default          up    0:00:00:10
1       eth0        200.1.1.2       12446  200.1.1.2       ::                                      12446   0/0    default          up    0:00:00:09
2       eth0        200.1.1.2       12546  200.1.1.2       ::                                      12546   0/0    default          up    0:00:00:09
3       eth0        200.1.1.2       12646  200.1.1.2       ::                                      12646   0/0    default          up    0:00:00:09

(END)
```

Figura 3.210 Información y conectividad de vManage

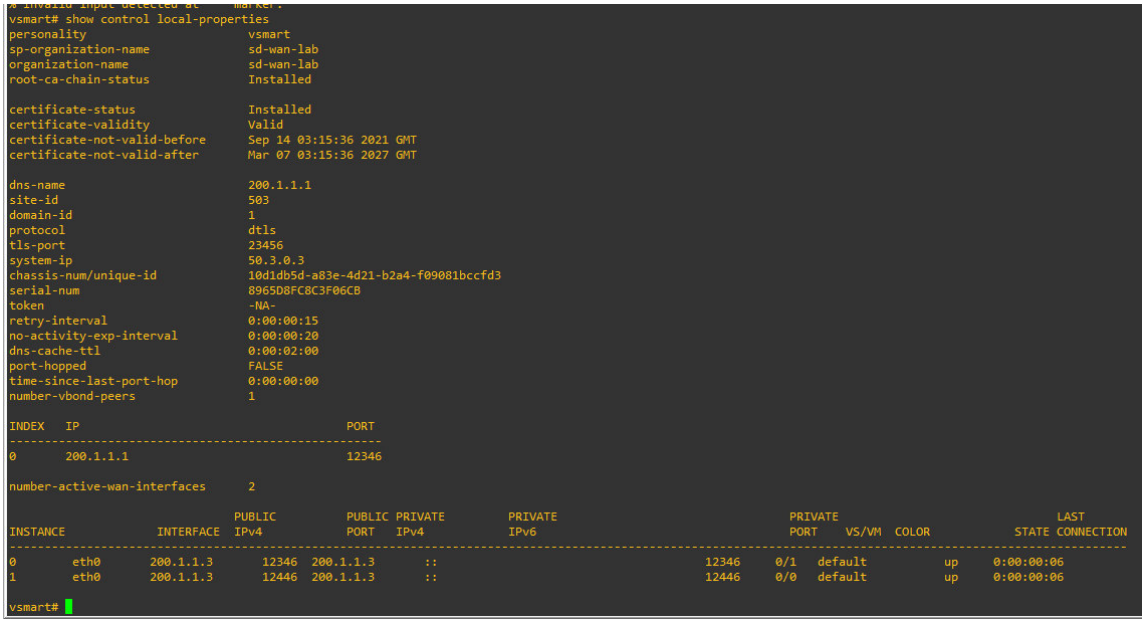


Figura 3.211 Información y conectividad de vSmart

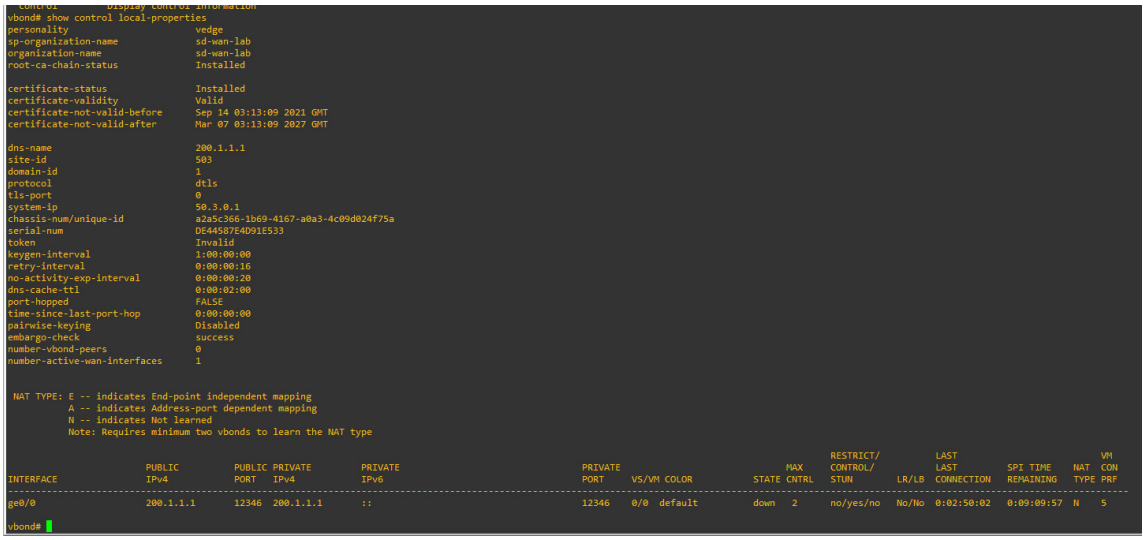


Figura 3.212 Información y conectividad de vSmart

El segundo comando utilizado para verificar el funcionamiento de la red es "*show control connections*". Este comando permitirá verificar el estado de todas las conexiones hacia el resto de controladores de la red como se aprecia en la Figura 3.213.

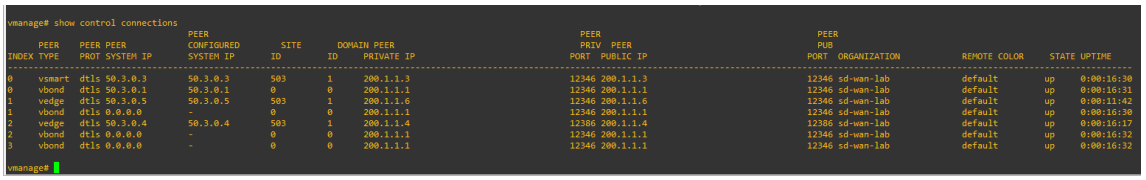


Figura 3.213 Conexiones a los controladores

El siguiente comando que se utiliza para verificar la información del controlador y también para conocer cuántos equipos se están conectado es "*show orchestrator summary*" el mismo que se muestra en la Figura 3.214.

```
vbond# show orchestrator summary
orchestrator summary 0
 vmanage_counts          4
 vsmart_counts           2
 vedge_counts            2
 protocol                dtls
 listening_ip            0.0.0.0
 listening_ipv6          ::
 listening_port          12346
 valid_controller_counts 2
vbond#
vbond#
vbond# show orchestrator summary
orchestrator summary 0
 vmanage_counts          4
 vsmart_counts           2
 vedge_counts            2
 protocol                dtls
 listening_ip            0.0.0.0
 listening_ipv6          ::
 listening_port          12346
 valid_controller_counts 2
vbond#
```

Figura 3.214 Información de vBond

El siguiente comando a utilizar es "*show orchestrator connections*" este comando permite saber las conexiones que se encuentran disponibles dentro del equipo vBond. Adicionalmente se observan los nombres de los controladores y sus respectivas direcciones, así como la organización a la cual pertenecen como se observa en la Figura 3.215.

```
vbond# show orchestrator connections
                                                                    PEER                      PEER
         PEER     PEER     PEER               SITE     DOMAIN   PEER             PRIVATE  PEER             PUBLIC                                    ORGANIZATION
INSTANCE TYPE     PROTOCOL SYSTEM IP          ID       ID       PRIVATE IP       PORT     PUBLIC IP        PORT    REMOTE COLOR     STATE           NAME                    UPTIME
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
0        vedge    dtls     50.3.0.4           503      1        200.1.1.4        12386    200.1.1.4        12386   default          up              sd-wan-lab              0:00:19:08
0        vedge    dtls     50.3.0.5           503      1        200.1.1.6        12346    200.1.1.6        12346   default          up              sd-wan-lab              0:00:14:19
0        vsmart   dtls     50.3.0.3           503      1        200.1.1.3        12346    200.1.1.3        12346   default          up              sd-wan-lab              0:00:19:09
0        vsmart   dtls     50.3.0.3           503      1        200.1.1.3        12446    200.1.1.3        12446   default          up              sd-wan-lab              0:00:19:09
0        vmanage  dtls     50.3.0.2           503      0        200.1.1.2        12346    200.1.1.2        12346   default          up              sd-wan-lab              0:00:19:08
0        vmanage  dtls     50.3.0.2           503      0        200.1.1.2        12446    200.1.1.2        12446   default          up              sd-wan-lab              0:00:19:08
0        vmanage  dtls     50.3.0.2           503      0        200.1.1.2        12546    200.1.1.2        12546   default          up              sd-wan-lab              0:00:19:08
0        vmanage  dtls     50.3.0.2           503      0        200.1.1.2        12646    200.1.1.2        12646   default          up              sd-wan-lab              0:00:19:08
```

Figura 3.215 Controladores disponibles en vBond

Finalmente, se procede a comprobar la conexión mediante el envío de paquetes ICMP hacia el resto de los controladores de la red. Así como la salida a internet de cada uno de los equipos que van hacia los clientes denominados vEdges como se observa en la Figura 3.216 y la Figura 3.217.

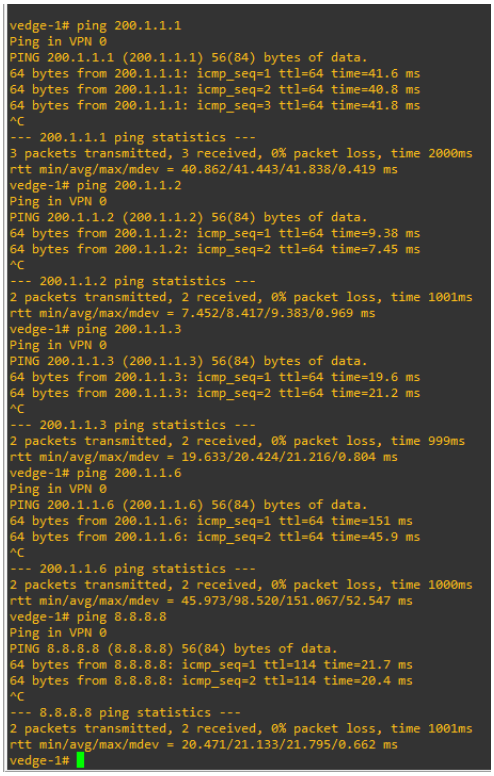


Figura 3.216 Envío de paquetes ICMP vEdge

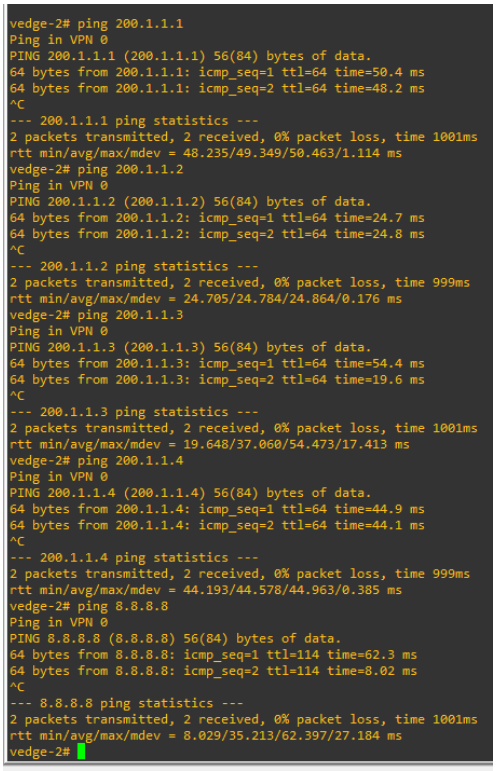


Figura 3.217 Envío de paquetes ICMP vEdge2

Pruebas Red SDWAN-FORTINET

Las pruebas que se van a llevar a cabo dentro de este apartado son para verificar el funcionamiento de las diferentes conexiones realizadas por medio de la aplicación del protocolo de enrutamiento dinámico OSPF, así como las salidas a internet. Las conexiones entre VLANs y la comunicación por medio de túneles IPSEC, uno de los principales inconvenientes para la realización completa de estas redes son las licencias que manejan los equipos Fortigate pertenecientes a la empresa Fortinet. Para la realización del presente proyecto se utilizaron licencias de prueba con una duración de 1 mes. Mismas que cuentan con varias restricciones entre las que más afectan al rendimiento de las redes es la incapacidad de usar más de 6 políticas para el permitir el establecimiento de conexiones limitando de este modo el uso extendido de los equipos.

Otro de los inconvenientes presentados al momento de la realización de diferentes topologías es el uso de equipos Fortigate más actualizados. Los equipos utilizados fueron de la versión 5.6 los cuales funcionan correctamente pero no disponen de muchas de las aplicaciones disponibles en versiones como la 6.0 o superiores. Uno de los inconvenientes quizá mucho más relevantes es la incapacidad de poder trazar una ruta de un paquete por medio del uso del comando "*trace".* Esto se debe principalmente a que cuando el paquete viaja en la red llega al equipo Fortigate y por restricción de las licencias se bloquea de este modo incapacitando al usuario saber la ruta exacta del paquete hacia la red destino.

El motivo anteriormente mencionado obliga a que en la realización de pruebas para este apartado conste de los siguientes parámetros:

- Verificaciones de conexión mediante el uso del comando "ping".
- Verificaciones de conexión por medio del monitoreo presente en los equipos Fortigate.

Red SDWAN-OSPF

Uno de los principales inconvenientes el cual ya fue mencionado previamente es la incapacidad de realizar las conexiones completas por motivo de las licencias. Sin embargo, en las tablas de enrutamiento del protocolo dinámico OSPF se tiene que todos los equipos FortiGate conocen todas las redes.

El primer equipo a analizar será el equipo correspondiente a la red 192.168.242.10, el comando que se utiliza para la obtención de la tabla de enrutamiento tanto para este

como para los equipos siguientes se detalla a continuación y se aprecia en la Figura 3.218.

Get router info routing-table all

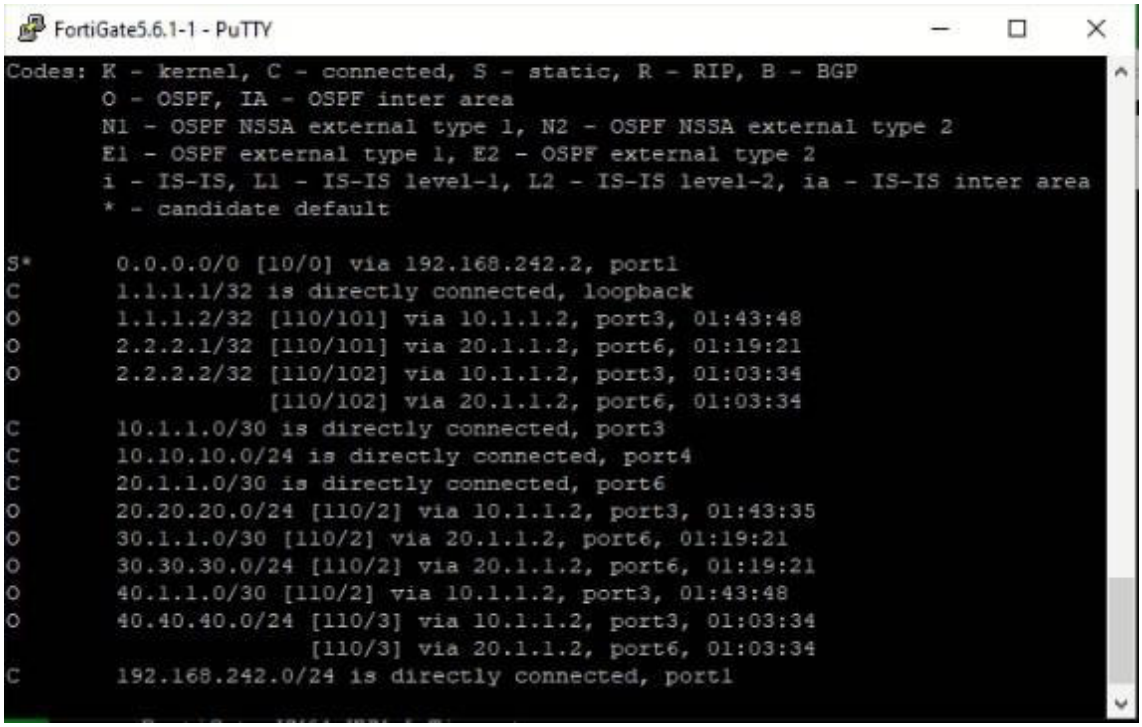


Figura 3.218 Tabla de enrutamiento primer equipo Fortigate

Como se aprecia en la Figura 3.218 se conoce tanto las redes directamente conectadas como la ruta estática por *default* y adicionalmente conoce todas las rutas de la red. Así como las interfaces seriales configuradas mediante enlaces SD-WAN, esto indica que se podrá realizar ping hacia cualquiera de las 4 redes y se tendrá la comunicación efectiva.

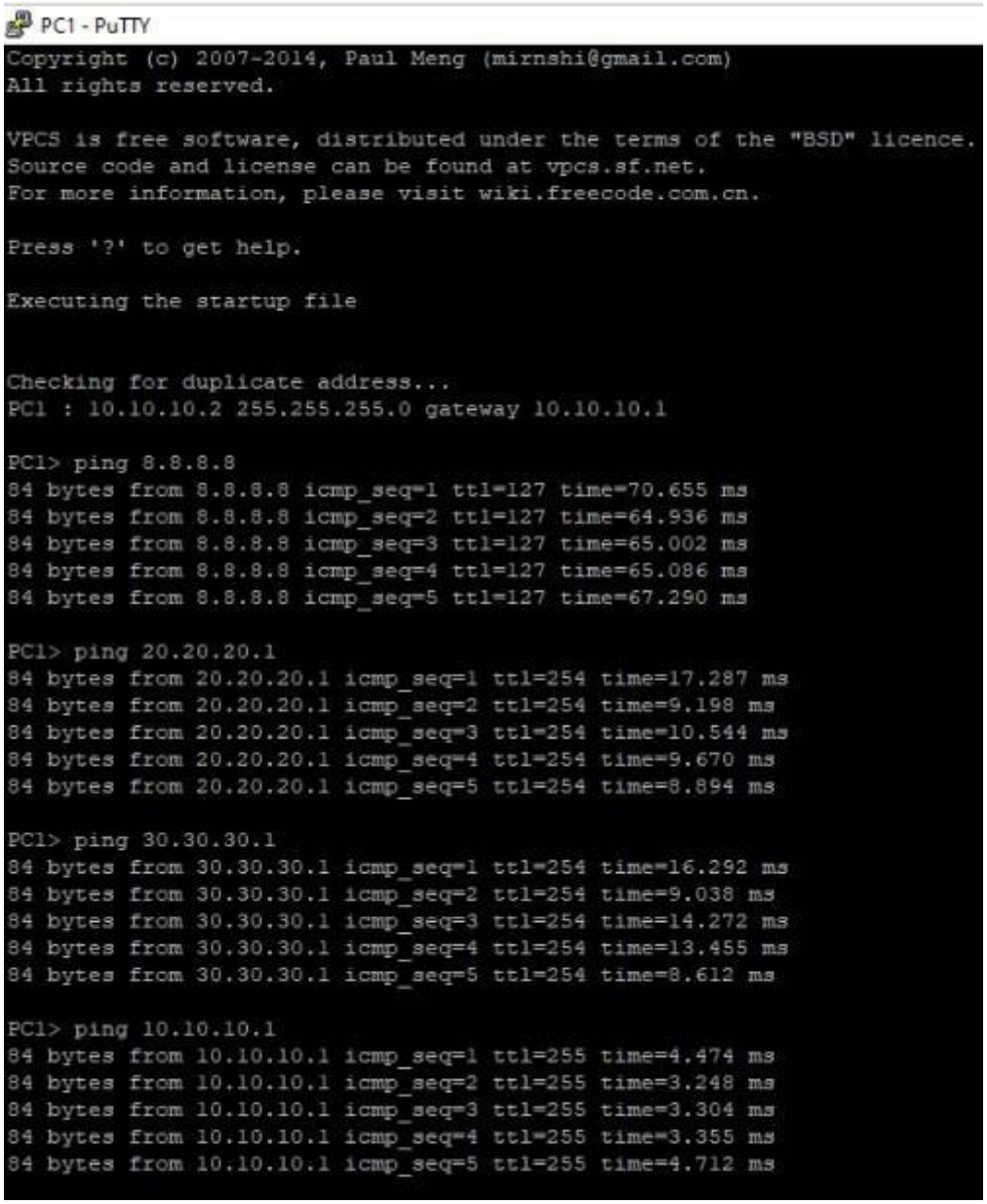


Figura 3.219 Verificación de conexión mediante ping

Como se aprecia en la Figura 3.219 se tiene conexión hacia el internet y hacia las redes que conforman la topología sin embargo debido a problemas de licencias no se permite el ping hacia la red 40.40.40.1. Con respecto a los tiempos en los que viajan los paquetes se observa que tienen un leve retardo debido a la conexión a Internet del servidor en físico.

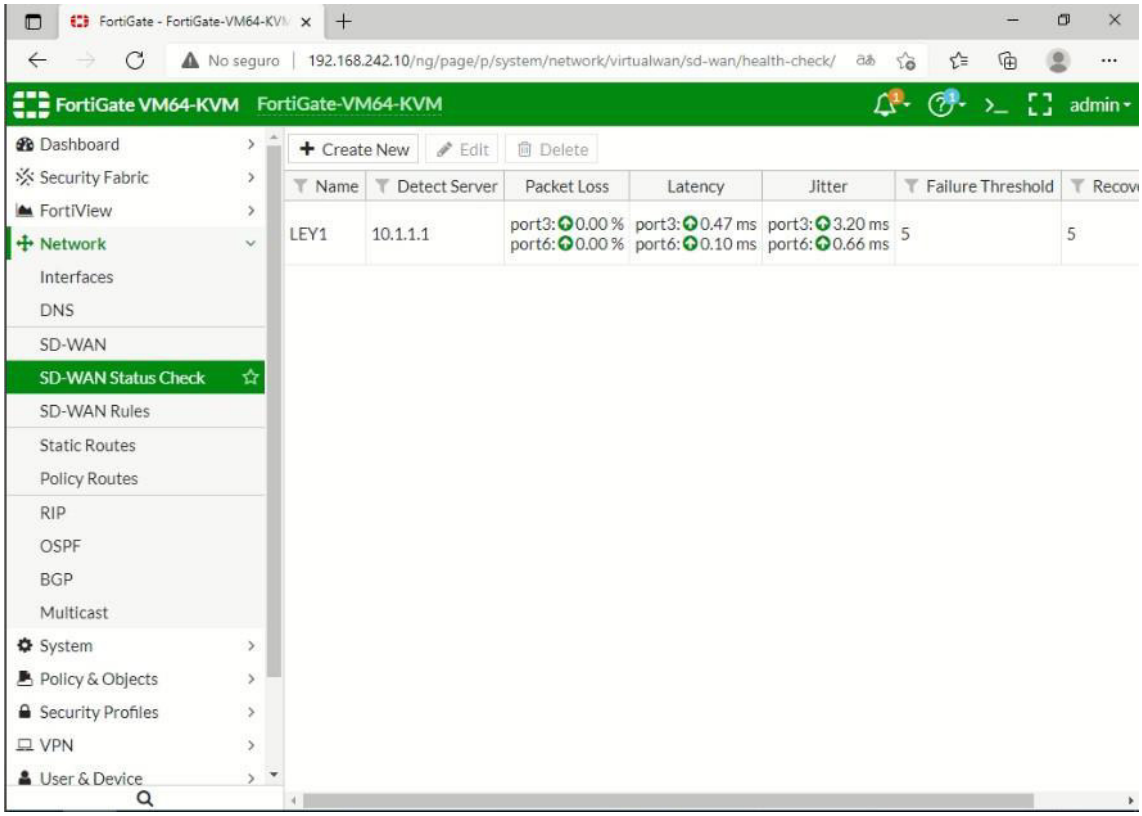


Figura 3.220 Monitoreo del funcionamiento del enlace SDWAN

En la Figura 3.220 se observa el monitoreo de ambos enlaces de SD-WAN que se llevan ejecutando se tienen 3 parámetros importantes los cuales se detallarán a continuación:

- Paquetes perdidos. – Este es uno de los parámetros más importantes ya que indica el porcentaje de paquetes perdidos en el enlace SD-WAN, para este caso no existen paquetes perdidos lo que indica que el enlace está operando de forma correcta.
- Latencias. – Este parámetro determina el tiempo en el que un paquete se tarda en transmitirse este aspecto va muy ligado a la velocidad de Internet que se disponga en la red, es decir en este caso dependerá mucho de la velocidad de internet del servidor en la EPN. En este caso debido a que los paquetes están eligiendo un camino por defecto la latencia en este enlace será mayor para solucionar este problema es recomendable que se ejecute balanceo de carga en el sistema.
- Fluctuación de retardo. – Este parámetro determina la variabilidad del tiempo en el que se envían los paquetes, por la misma razón previamente mencionada los paquetes eligen un camino por defecto motivo por el cual en un puerto será mayor esta cantidad. El mejor camino para solucionar este inconveniente es realizar balanceo de carga.

El segundo equipo a analizar es el perteneciente a la dirección 192.168.242.20. El primer parámetro a analizar es la tabla de enrutamiento obtenida mediante el comando previamente mencionado dando como resultado lo siguiente:

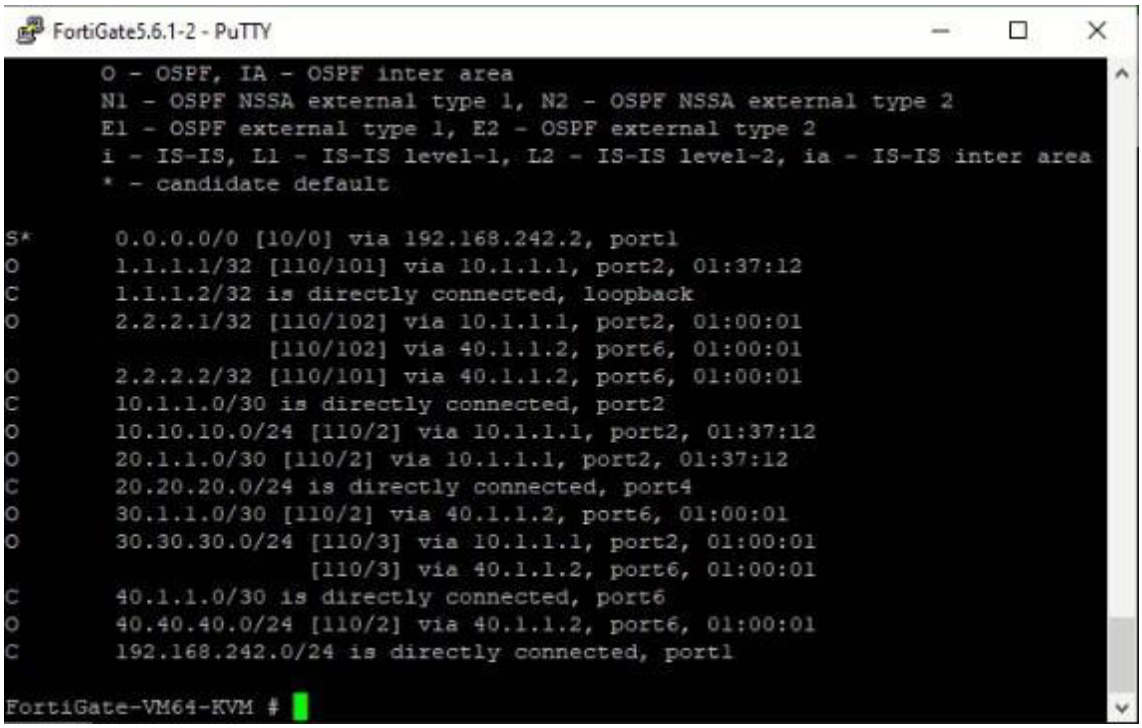


Figura 3.221 Tabla de enrutamiento segundo equipo Fortigate

En la Figura 3.221 se observa de igual manera que en el equipo anterior este conoce todas las redes disponibles. Es decir, puede enviar un paquete hacia cualquier red mientras se encuentre en la tabla de enrutamiento. Adicionalmente se cuenta con una ruta por default para obtener salida a Internet y adicionalmente se tiene las interfaces *loopback* para poder realizar un enrutamiento por medio de OSPF.

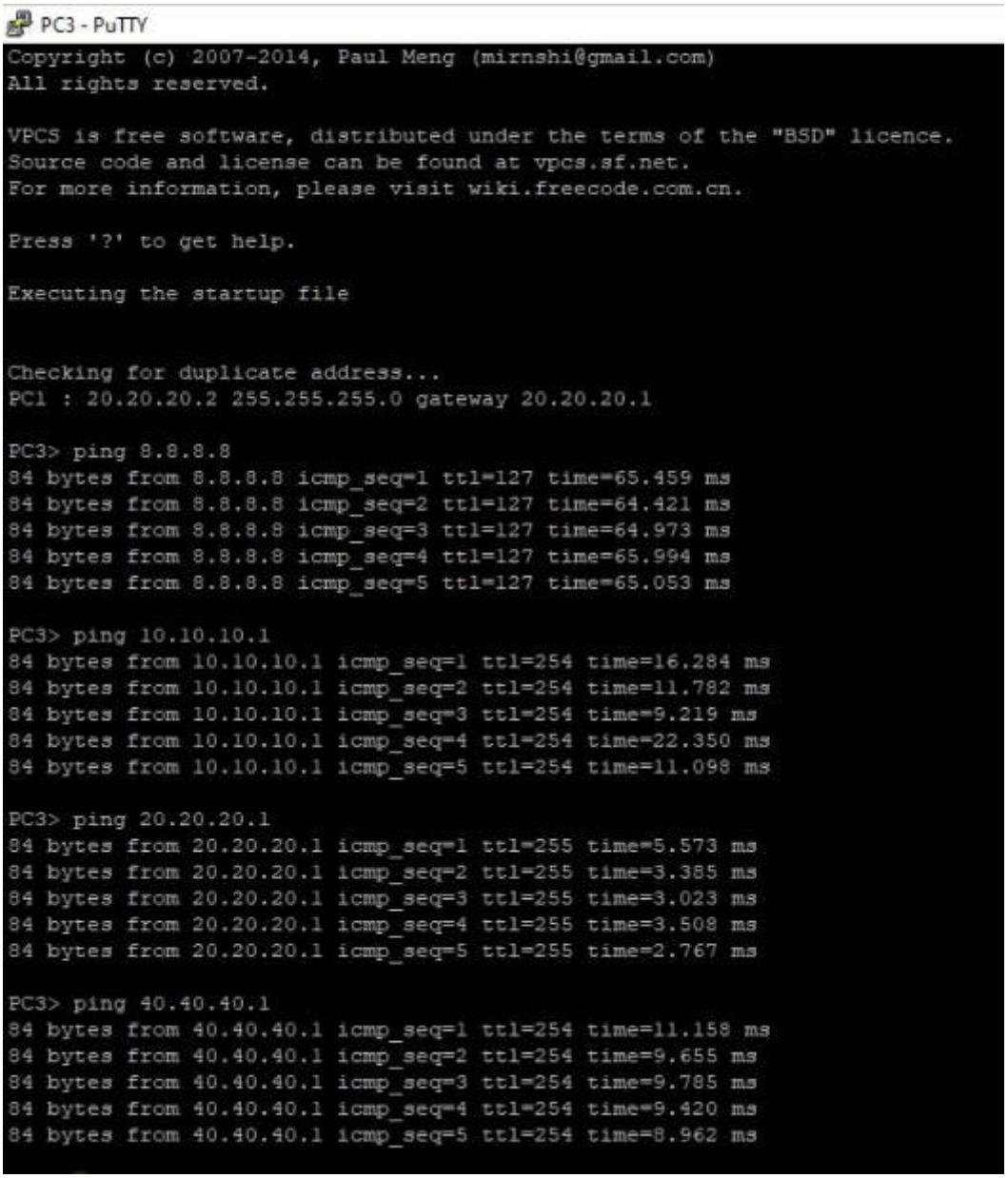


Figura 3.222 Verificación de conexión mediante ping segundo equipo

En la Figura 3.222 se observa que realmente existe conectividad hacia todas las redes remotas. Sin embargo, por problemas de licencias de los equipos no se puede realizar esta prueba hacia una de las redes establecidas, las latencias de los mensajes dependen de la velocidad de internet del servidor en físico.

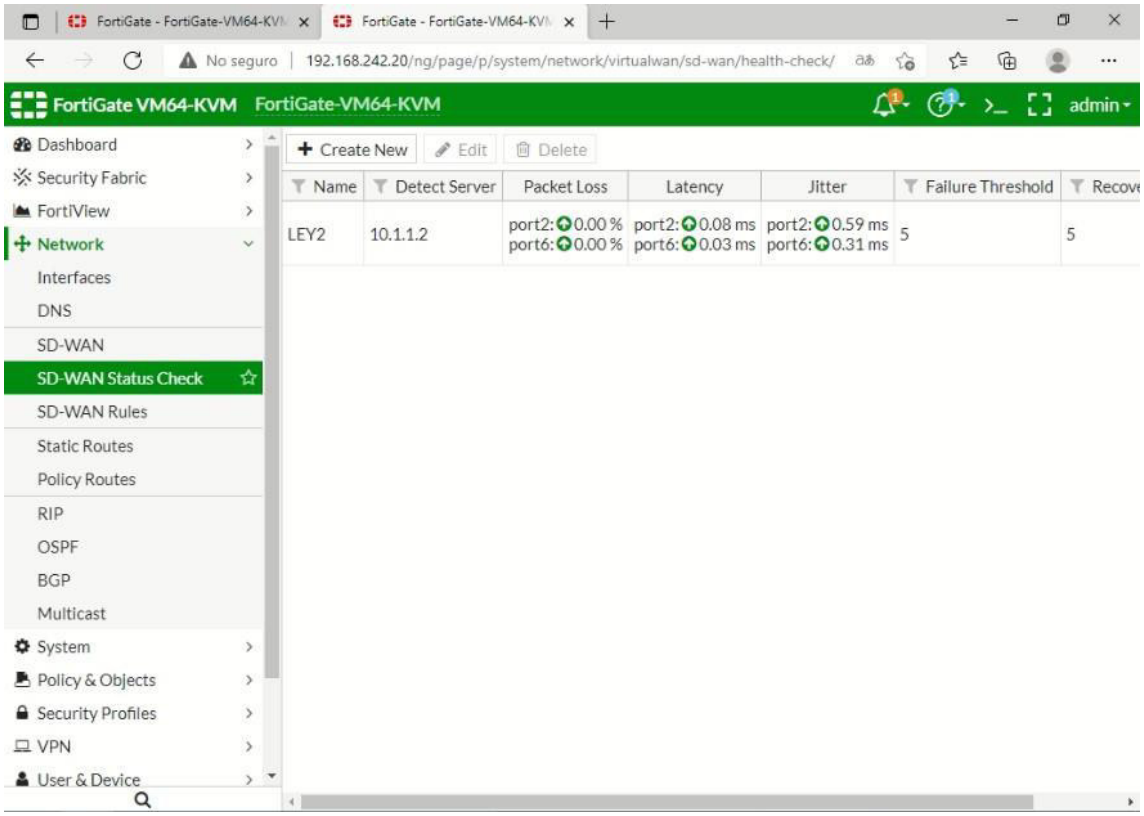


Figura 3.223 Monitoreo del funcionamiento del enlace SDWAN segundo equipo

En la Figura 3.223 se observa el monitoreo de los enlaces que operan mediante SD-WAN. Como ya se detalló previamente se tiene que no existen paquetes perdidos lo que indica que el enlace SD-WAN funciona correctamente la latencia de estos enlaces es muy similar en tiempo esto indica que para los paquetes no existe un camino pre definido. Pero podría optimizarse de mejor manera realizando un balanceo de carga, aunque para esta parte de la red no es muy necesario.

El tercer equipo a analizar es el perteneciente a la dirección 192.168.242.30 el cual por medio del uso del comando para obtención de la tabla de enrutamiento la misma que se presenta en la Figura 3.224.

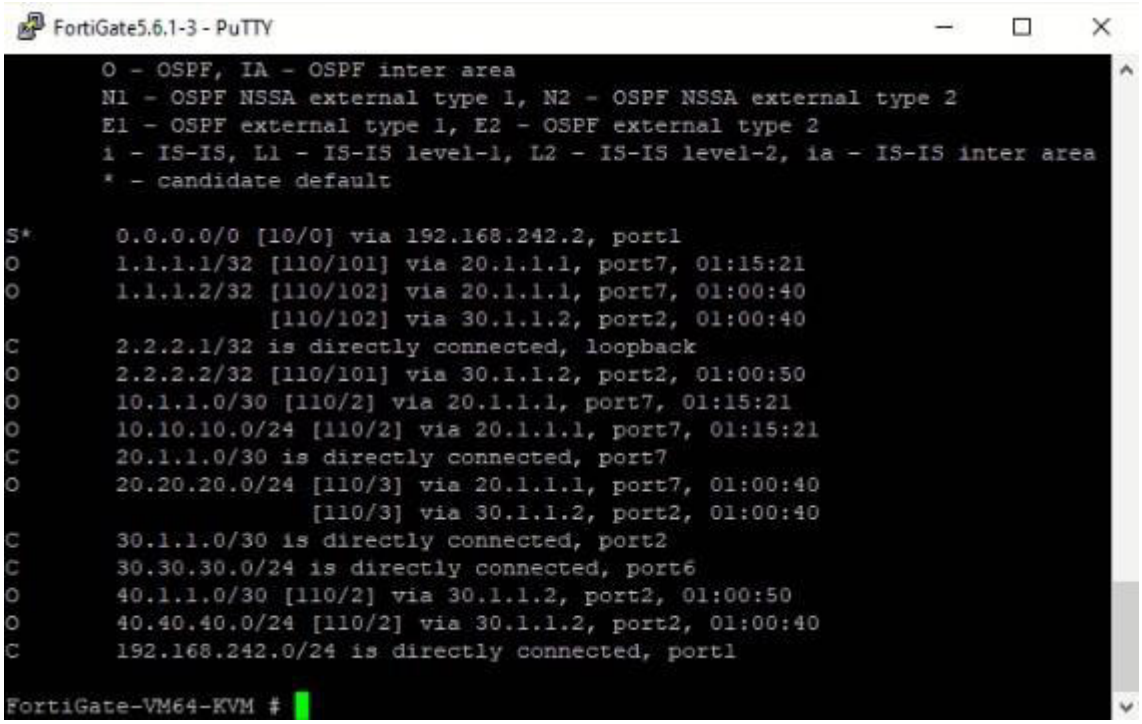


Figura 3.224 Tabla de enrutamiento tercer equipo Fortigate

Del mismo modo que en los demás equipos este también conoce todas las rutas que se encuentran disponibles en la red por lo que se puede enviar un paquete ICMP hacia cualquier destino de la red como se detalla en la Figura 3.225 y en la Figura 3.226 pertenecientes a ambas VPCS dentro de la red respectivamente

Figura 3.225 Verificación de conexión mediante ping tercer equipo VPCS 6

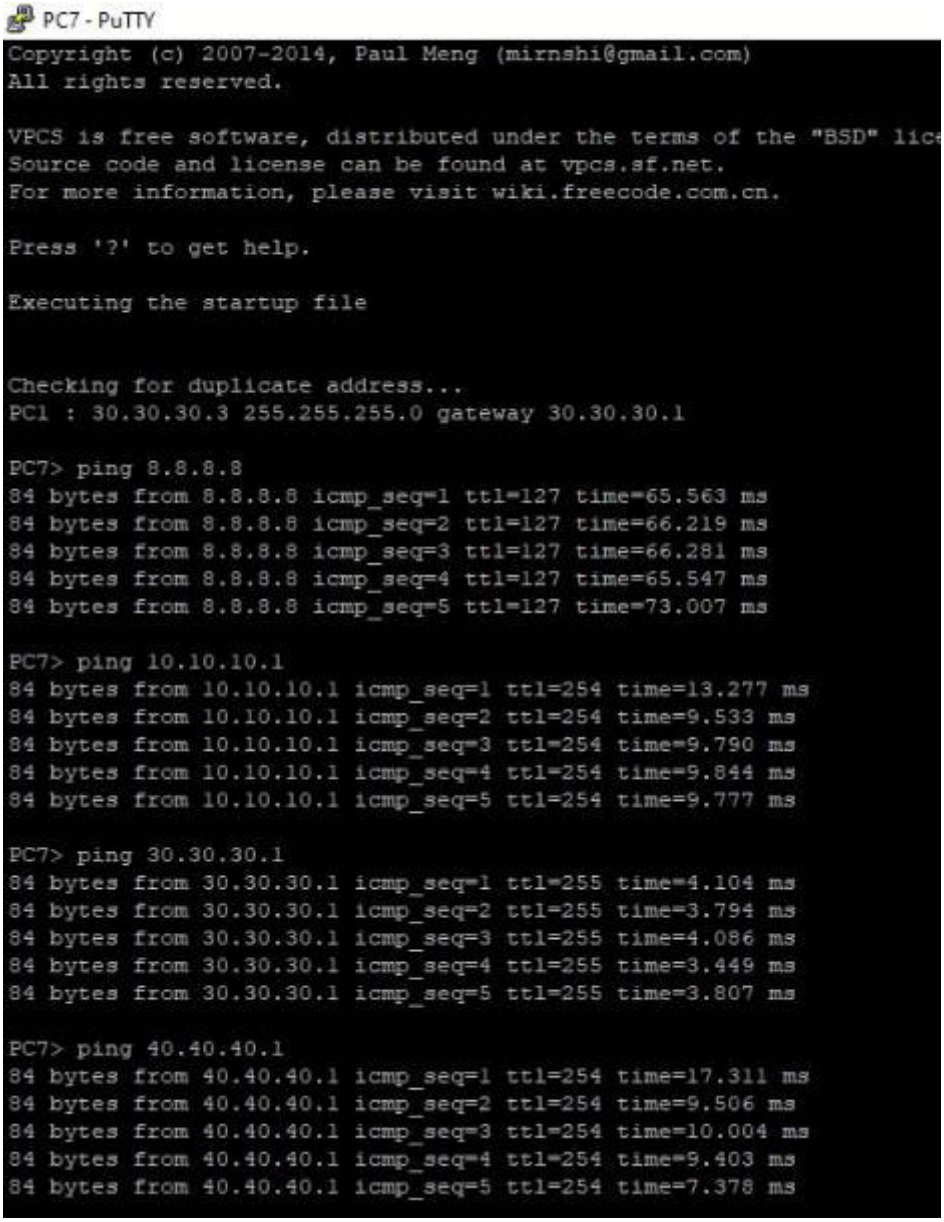


Figura 3.226 Verificación de conexión mediante ping tercer equipo VPCS 7

Como se puede apreciar la comunicación se está llevando a cabo correctamente, cada una de las VPCS posee de conectividad hacia la internet como a las diferentes redes dentro de la topología. Como se puede notar los tiempos de envío de los paquetes ICMP es muy similar al tiempo que se toma en las otras partes de la topología.

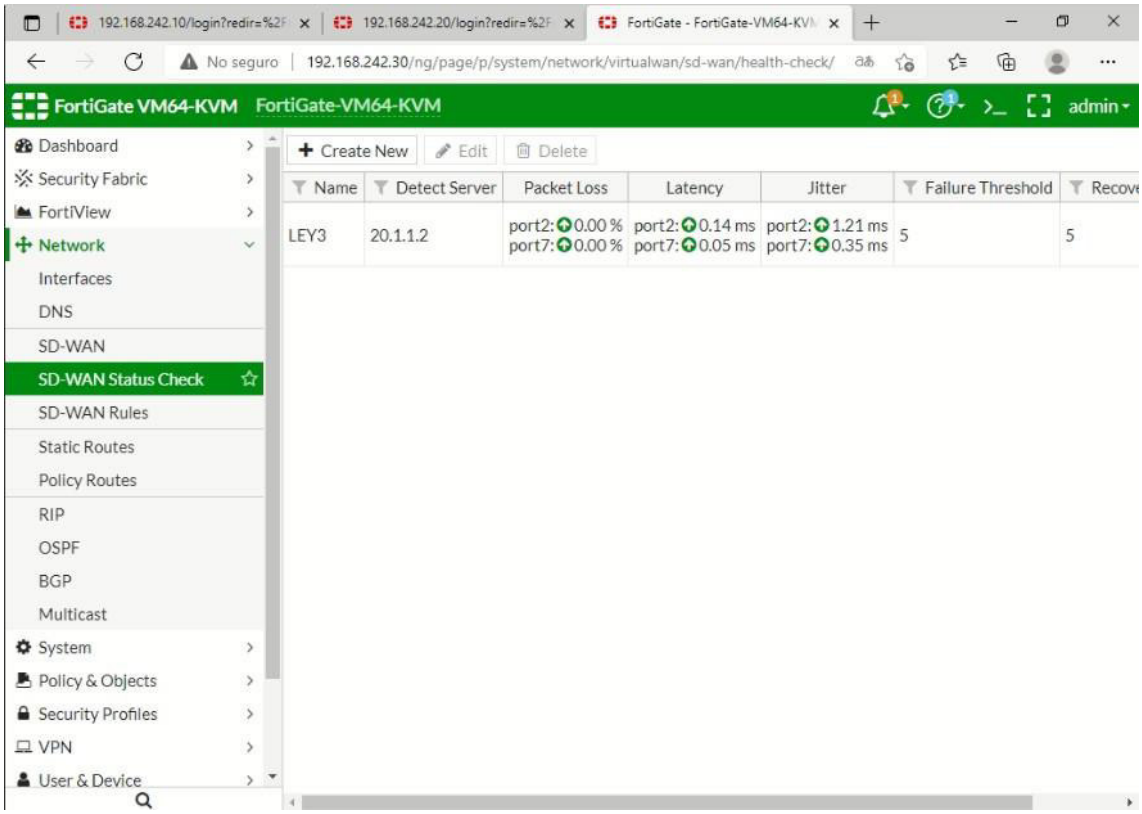


Figura 3.227 Monitoreo del funcionamiento del enlace SDWAN tercer equipo

En la Figura 3.227 se observa el monitoreo de los enlaces que se encuentran configurados para SD-WAN, para comprobar que el enlace funciona correctamente se verifica el apartado de paquetes perdidos si el valor es de 0 el funcionamiento de SD-WAN es el adecuado. De la misma manera que en el segundo equipo aquí no sería necesario aplicar un balanceo de carga puesto que las latencias en ambas interfaces es la adecuada en base a los parámetros visualizados previamente. El retardo en cambio se observa que es considerablemente mayor en un enlace que en el otro esto puede deberse a que el paquete tomó un camino más largo en la red para llegar al destino.

Finalmente, el ultimo equipo a analizar es el perteneciente a la red 192.168.242.40 el mismo que presenta una tabla de enrutamiento que se presenta a continuación.

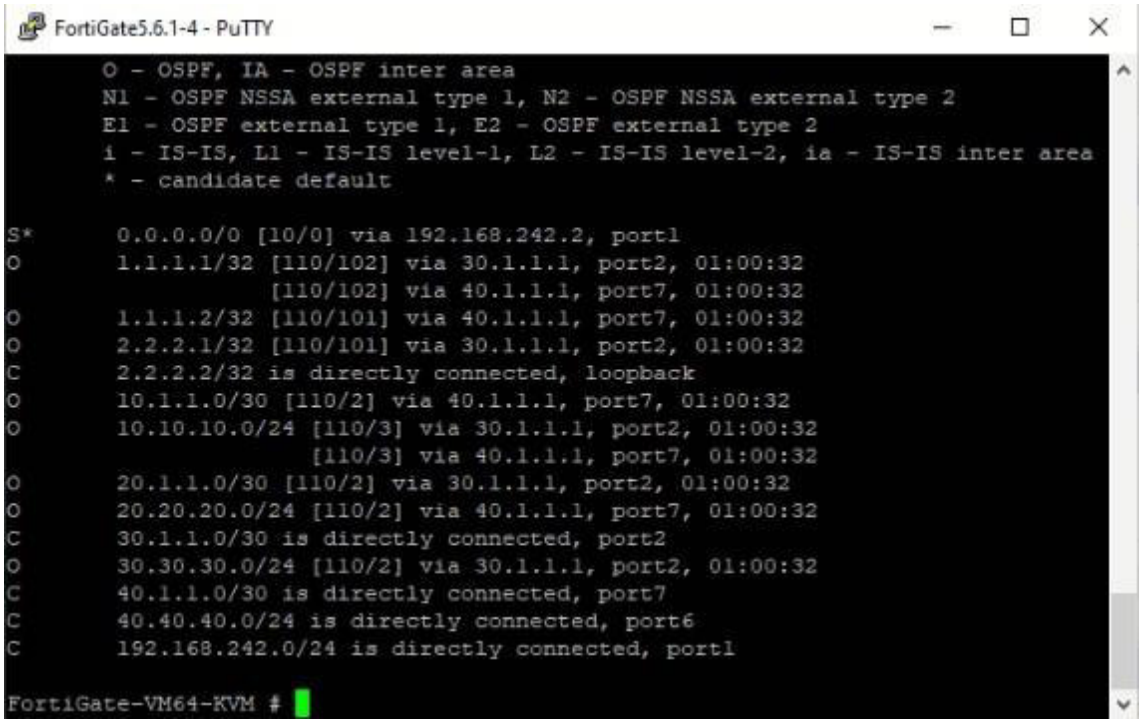


Figura 3.228 Tabla de enrutamiento cuarto equipo Fortigate

Como se observa en la Figura 3.228 el equipo conoce todas las direcciones de la red. Del mismo modo que los demás equipos se puede realizar el envío de un paquete ICMP hacia el resto de la red.

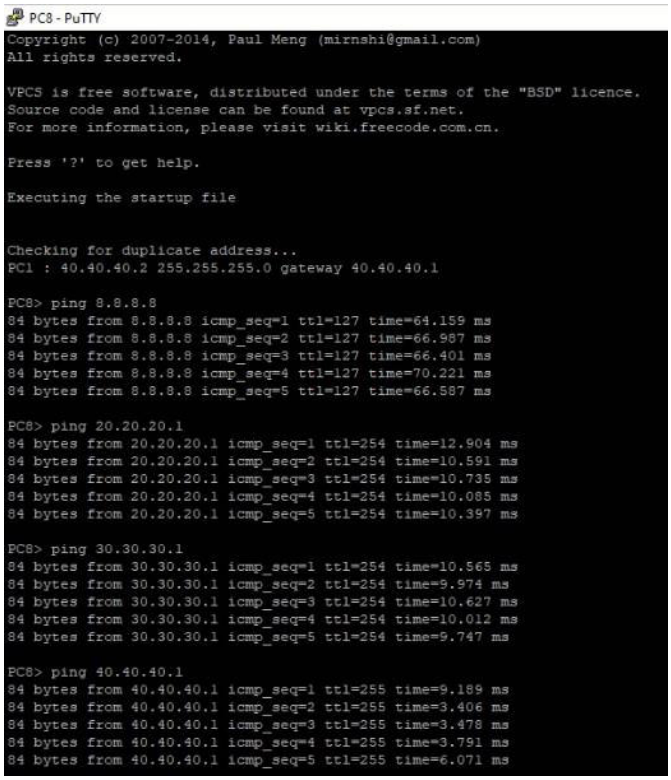


Figura 3.229 Verificación de conexión mediante ping VPCS 8

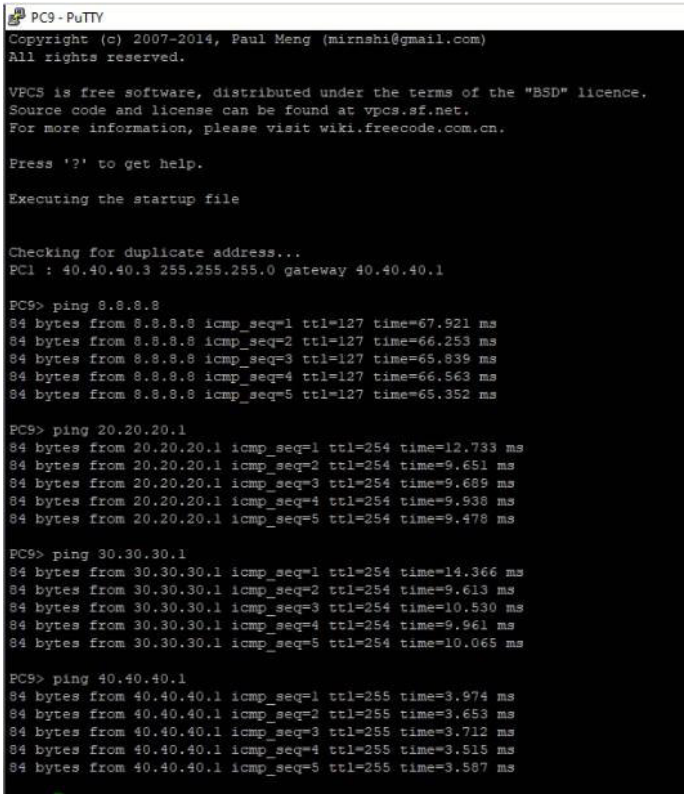


Figura 3.230 Verificación de conexión mediante ping VPCS 9

Como se aprecia en la Figura 3.229 y la Figura 3.230 se aprecia el envío de paquetes de tipo ICMP hacia el resto de la red. Completándose de esta manera satisfactoriamente la comunicación por enlaces SDWAN haciendo uso del protocolo de enrutamiento dinámico OSPF.

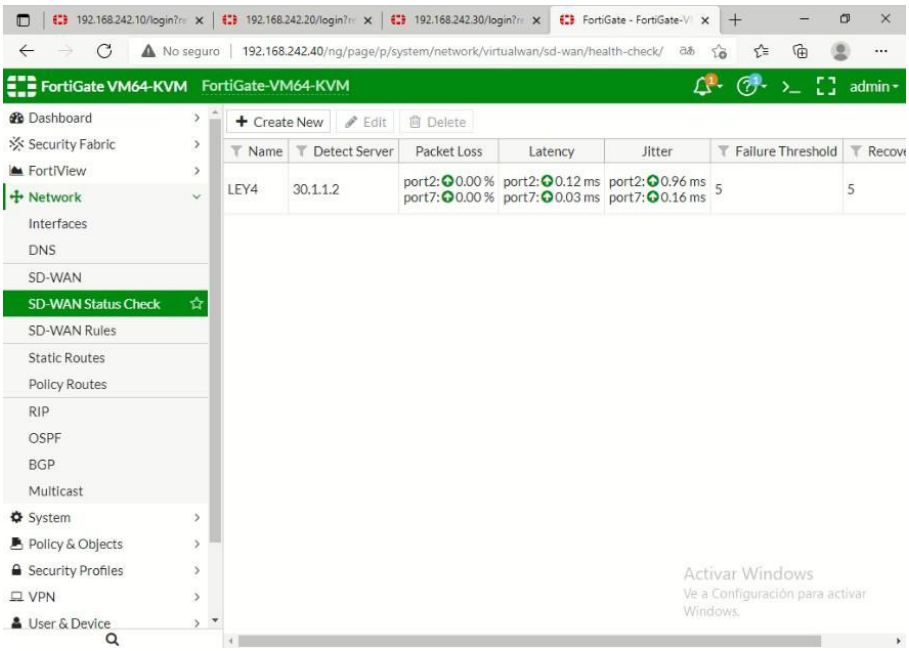


Figura 3.231 Monitoreo del funcionamiento del enlace SDWAN cuarto equipo

Finalmente, en la Figura 3.231 se tiene el monitoreo de los enlaces SD-WAN y de igual forma que en los equipos pasados estos enlaces están funcionando correctamente ya que el porcentaje de pérdida de paquetes es 0. Adicionalmente se puede notar que tanto las latencias como el retardo tiene valores muy similares por lo que se puede concluir que de toda la red estos enlaces operan en un balanceo de carga para ambas interfaces ISP de tipo SD-WAN obteniendo de este modo el máximo rendimiento en la red.

Red SDWAN-VLAN-OSPF

Para las pruebas de esta red debido a la restricción de políticas se tuvo acceso solo desde el primer equipo VPCS1 hacia el resto de la red motivo por el cual la salida a la red por medio de mensajes ICMP de las VPCS restantes no pudo llevarse a cabo.

Como primera parte se procede a obtener las tablas de enrutamiento tanto del primer equipo Fortigate como del segundo por medio de la aplicación del comando "*get router info rounting-table all",* estas tablas pueden ser revisadas en la Figura 3.232 y la Figura 3.233 respectivamente.

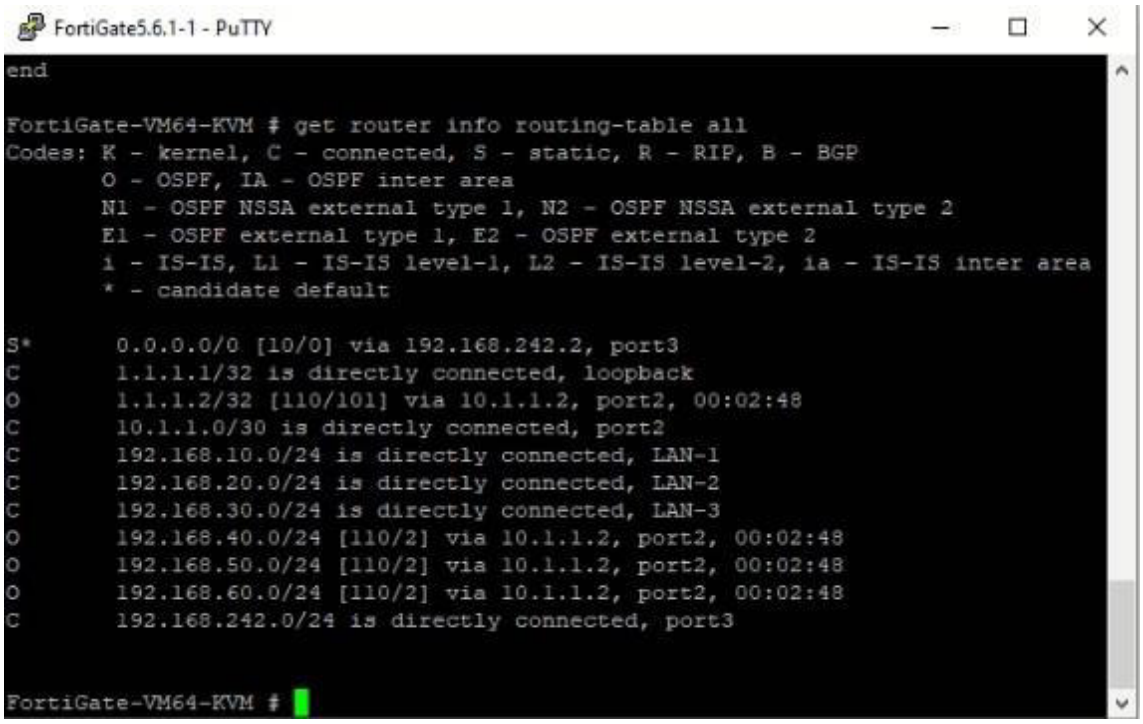


Figura 3.232 Tablas de enrutamiento primer equipo Fortigate

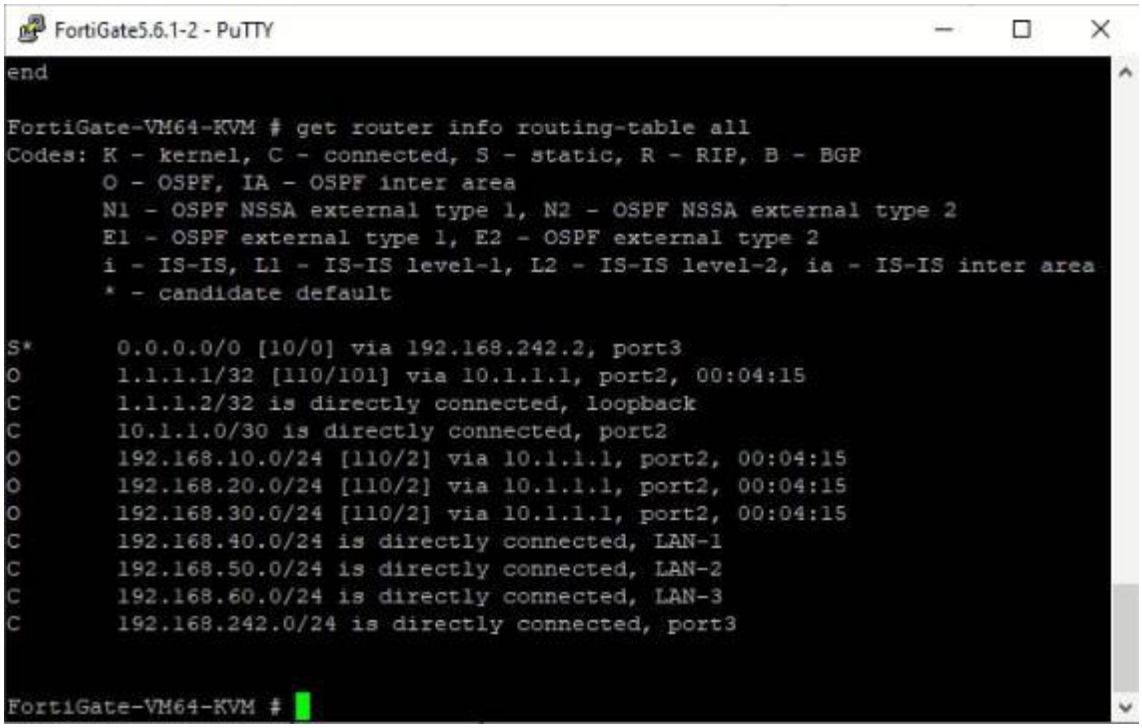


Figura 3.233 Tablas de enrutamiento segundo equipo Fortigate

Como se puede apreciar tanto en el primer equipo como en el segundo se conocen todas las rutas que se encuentran disponibles tanto las directamente conectadas como las rutas aprendidas por medio del protocolo dinámico OSPF. Adicionalmente se observa que se tiene una ruta estática por default la cual ayudará al envío de paquetes hacia Internet. Un parámetro importante a notar es que también se conoce las rutas de tipo *loopback* que ayudan a que se pueda establecer comunicación entre VLANs de una red hacia la otra.

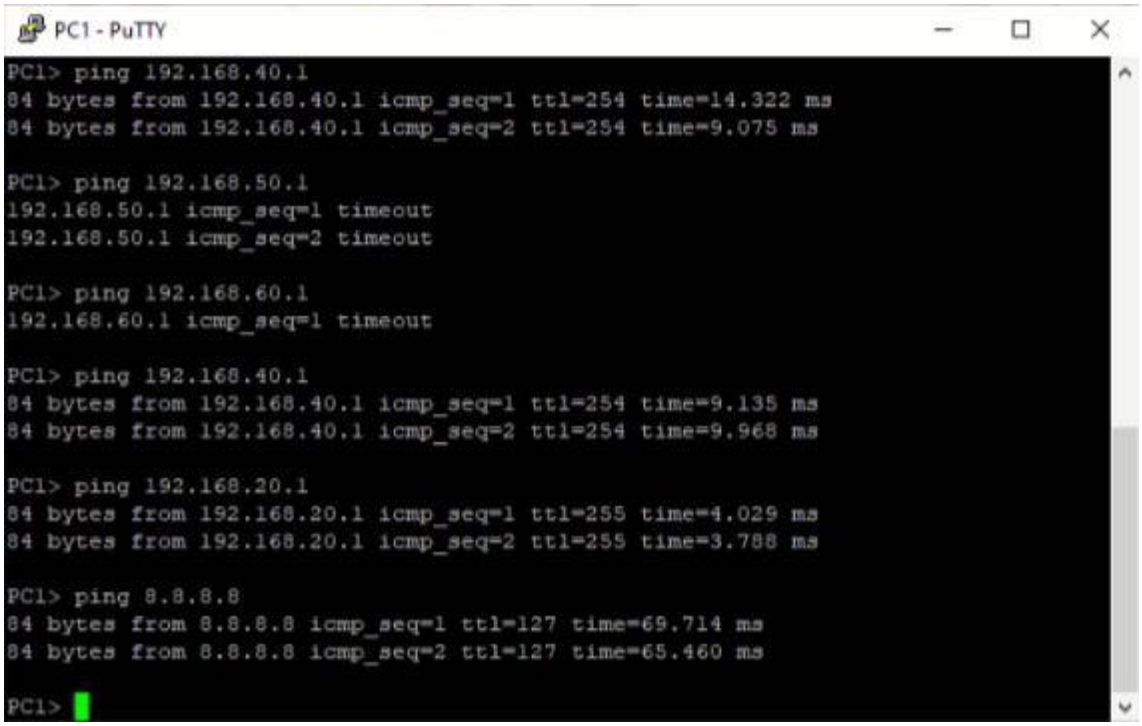


Figura 3.234 Verificación de recepción de paquetes ICMP hacia la segunda red

Como se aprecia en la Figura 3.234 se tiene comunicación con la red remota, sin embargo, como se mencionó previamente no se puede acceder a las demás redes por motivo de las licencias de los equipos. Adicionalmente se tiene comunicación entre VLANs de la misma red lo que indica que tanto el protocolo OSPF, el enlace de tipo troncal, así como los enlaces SDWAN presentes funcionan de manera correcta. En cuanto al tiempo de envío de los paquetes ICMP está dentro del rango de lo permitido en base a la velocidad de trasmisión de los datos del servidor en físico.

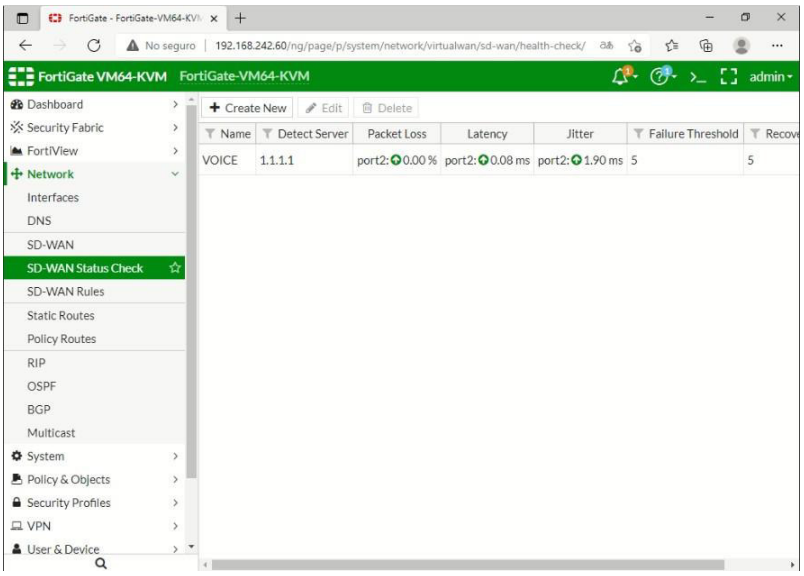


Figura 3.235 Comprobación del estado del enlace SDWAN en la primera red

Como se aprecia en la Figura 3.235 el porcentaje de paquetes perdidos en el enlace SDWAN en la red 192.168.242.60 es de 0, es decir, el enlace SDWAN está operando adecuadamente en la transmisión de paquetes. Del mismo modo la latencia refleja un valor dentro de los parámetros normales en base a la velocidad de transmisión lo que se ve reflejado finalmente en el retardo que experimenta el enlace.

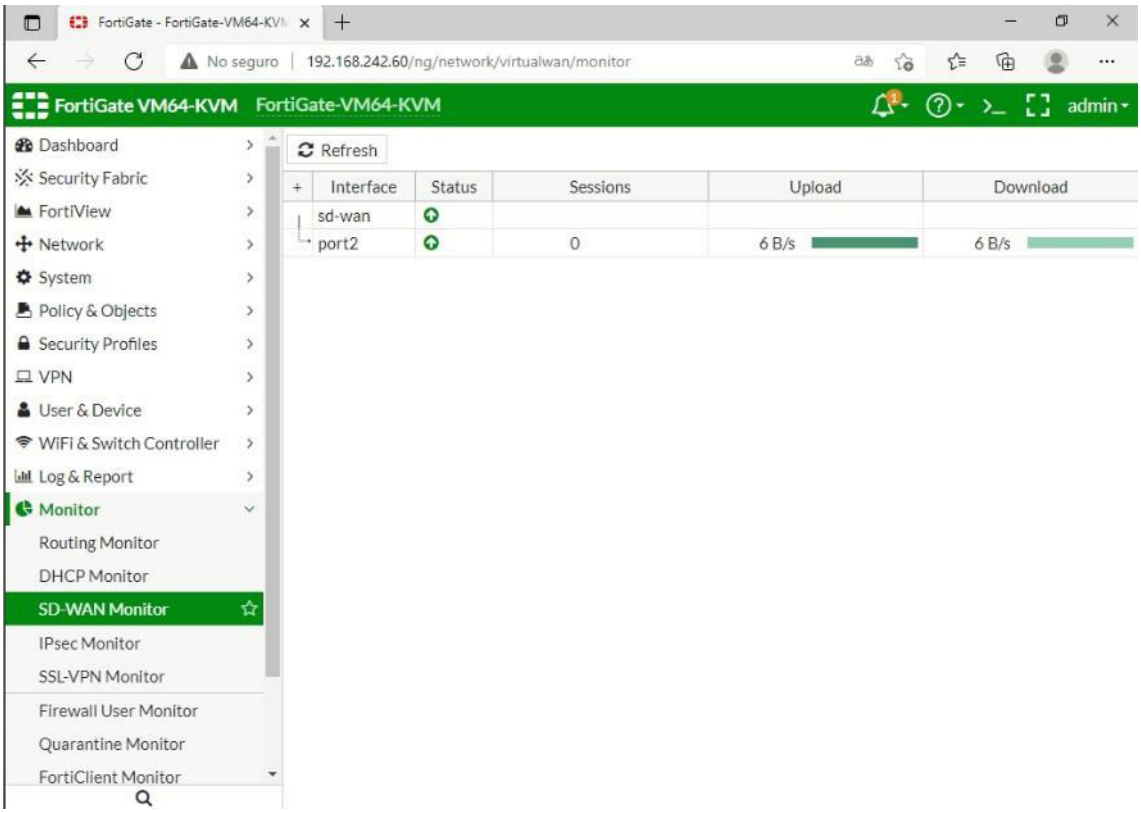


Figura 3.236 Monitoreo del enlace SDWAN en la primera red

En la Figura 3.236 se observa el modo de funcionamiento del enlace SDWAN, así como las velocidades de subida y bajada que experimenta el mismo. Esta velocidad está medida en bits/segundo, para comprobar que el enlace funciona correctamente ambas velocidades deben coincidir o no ser muy diferentes entre sí. Mientras mejor sea la velocidad de transmisión mayor será la eficacia del enlace SDWAN pudiendo enviar una mayor cantidad de paquetes optimizando de este modo la red. Para este caso en particular se tiene una velocidad de 6 B/s tanto de subida como de bajada lo que indica nuevamente que el enlace está funcionando correctamente.

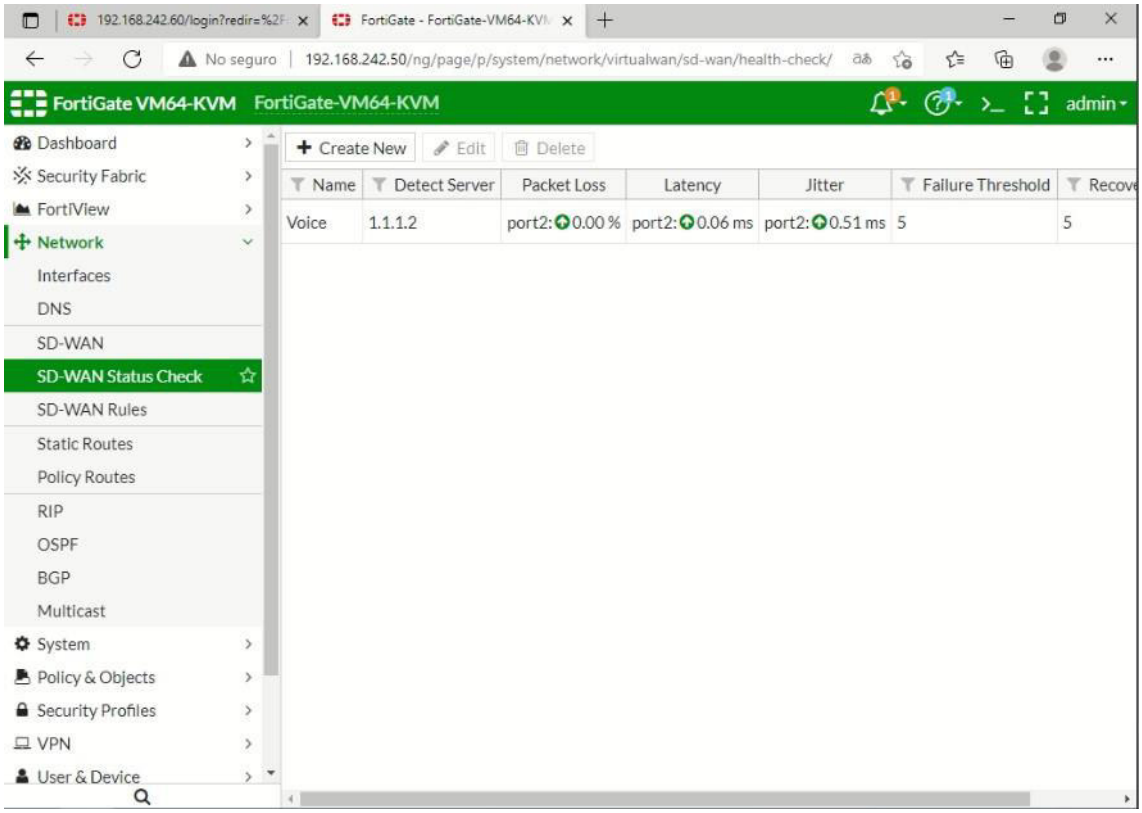


Figura 3.237 Comprobación del estado del enlace SDWAN en la segunda red

En la Figura 3.237 se observa que se tiene un porcentaje de pérdidas de 0 volviendo a este enlace completamente funcional. En este caso se tiene tanto en la latencia como en el retardo valores similares lo que significa que el camino por SDWAN se encuentra optimizado, esto se verá reflejado en la capacidad de enviar y recibir tráfico hacia redes externas.

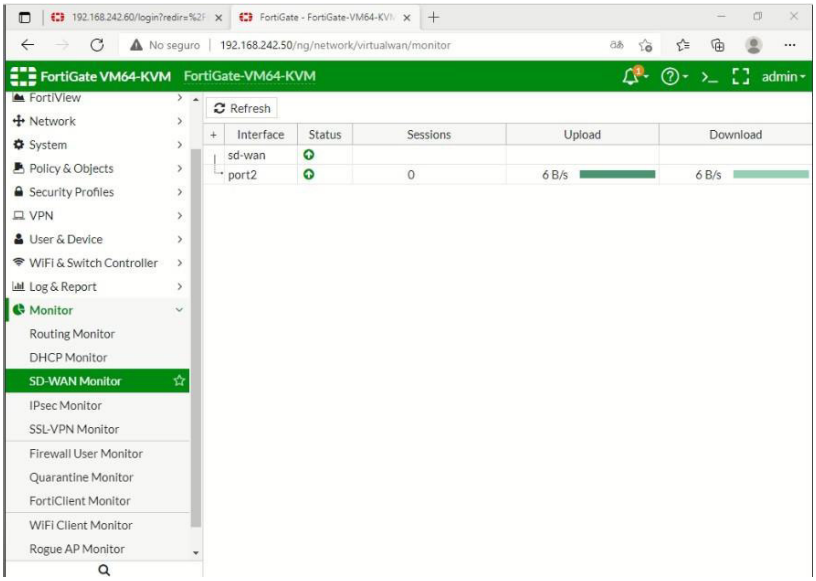


Figura 3.238 Monitoreo del enlace SDWAN en la segunda red

Del mismo modo que en la primera red en la Figura 3.238 se detalla las velocidades que se están manejando tanto de subida como de bajada. Como estos valores coinciden se puede concluir que el enlace se encuentra operando perfectamente y con cierta optimización en el mismo. Un dato importante es saber que cuando el enlace SDWAN falla por algún motivo el estado del enlace cae generando de este modo un aviso en la interfaz gráfica para que el administrador de la red tome las acciones respectivas para solventar el problema.

Red SDWAN-IPSEC

Esta red cuenta con una comunicación desde centrales hacia sucursales por medio de internet, esta red es una representación simulada sobre el funcionamiento e implementación de redes SDWAN mediante equipos FortiGate. la comunicación mediante túneles IPSEC proporciona una comunicación segura entre entes de una misma organización por este motivo es fundamental conocer el correcto funcionamiento de estas comunicaciones. A continuación en la Figura 3.239 se puede observar que existe transmisión de paquetes de tipo ICMP entre la central 1 y la sucursal 1. Posteriormente en la Figura 3.240 se observa la comunicación por medio de la transmisión de paquetes ICMP entre la sucursal 1 y la central 1 verificando de este modo el correcto funcionamiento de los túneles IPSEC.

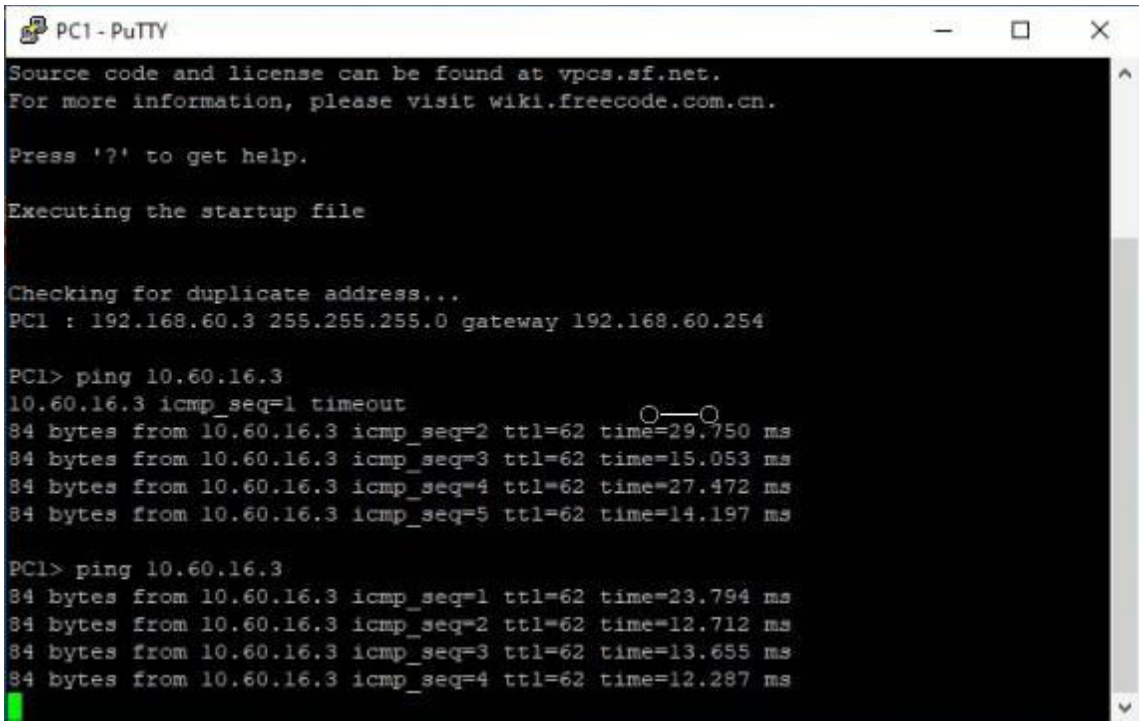


Figura 3.239 Verificación de conexión por medio de ICMP Central 1 – Sucursal 1

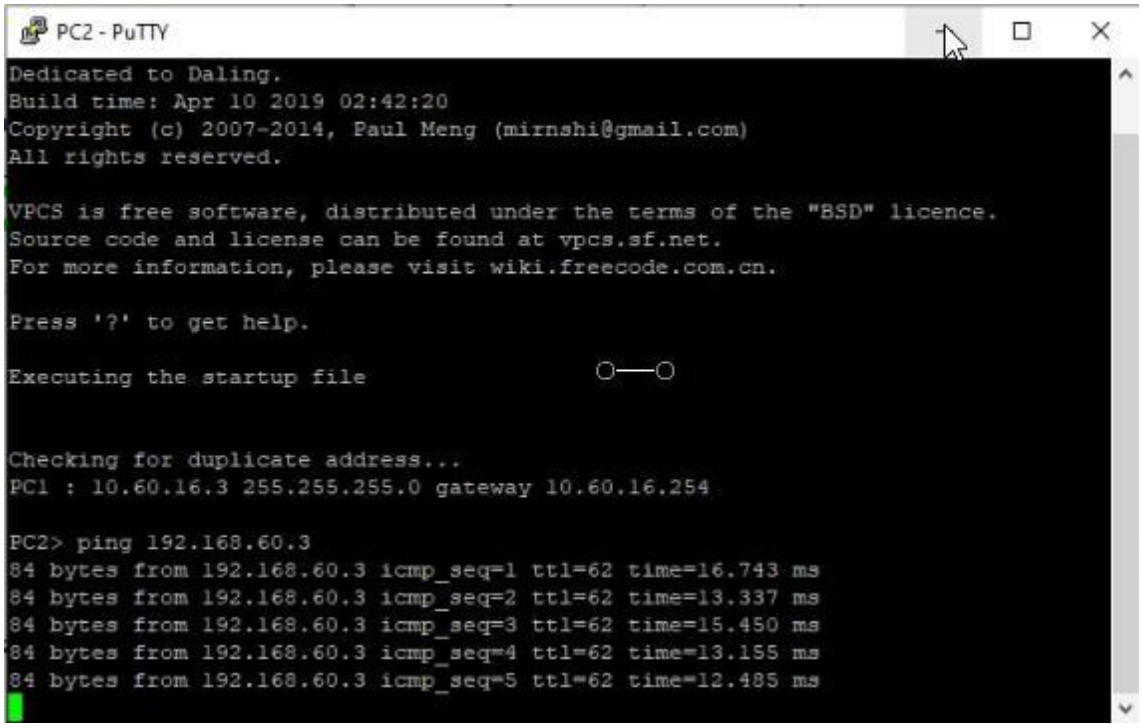


Figura 3.240 Verificación de conexión por medio de ICMP Sucursal 1 – Central 1

De igual manera se procede a verificar el envío de paquetes ICMP desde la central 2 hacia la sucursal 2 desde ambas VPCS pertenecientes a la central 2 hacia las 2 VPCS en la sucursal 2 como se muestra en la Figura 3.241 en la Figura 3.242. En la Figura 3.243 y en la Figura 3.244 respectivamente.

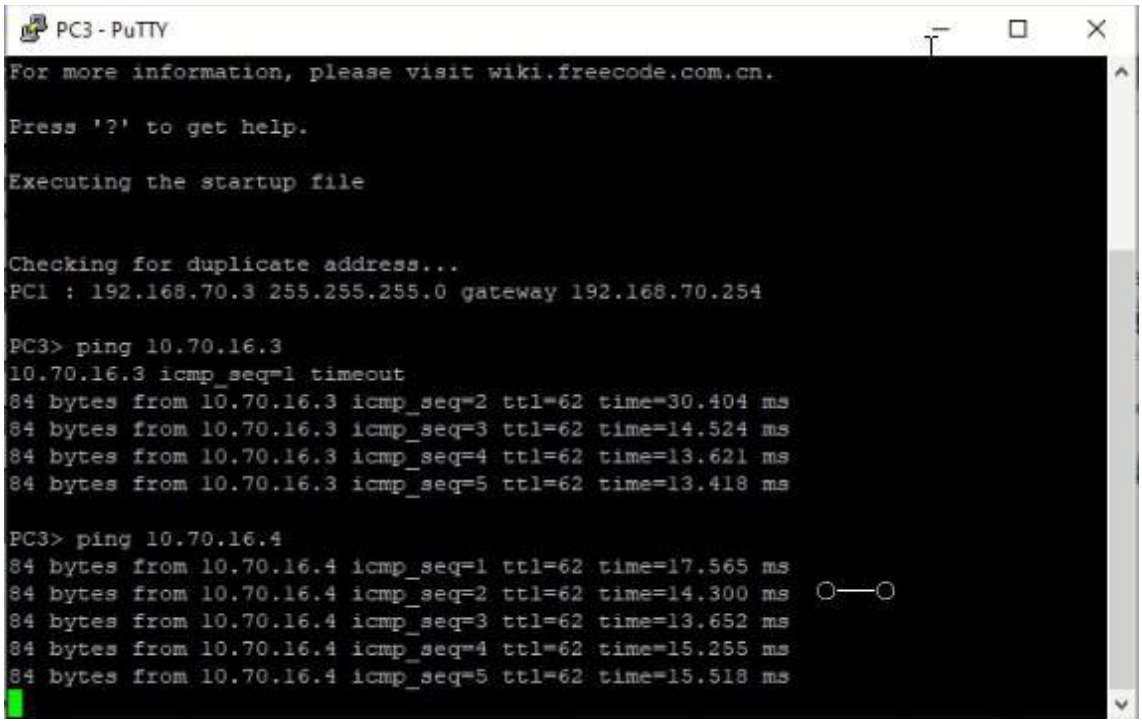


Figura 3.241 Envío de mensajes ICMP Central 2 – Sucursal 2 VPCS 3

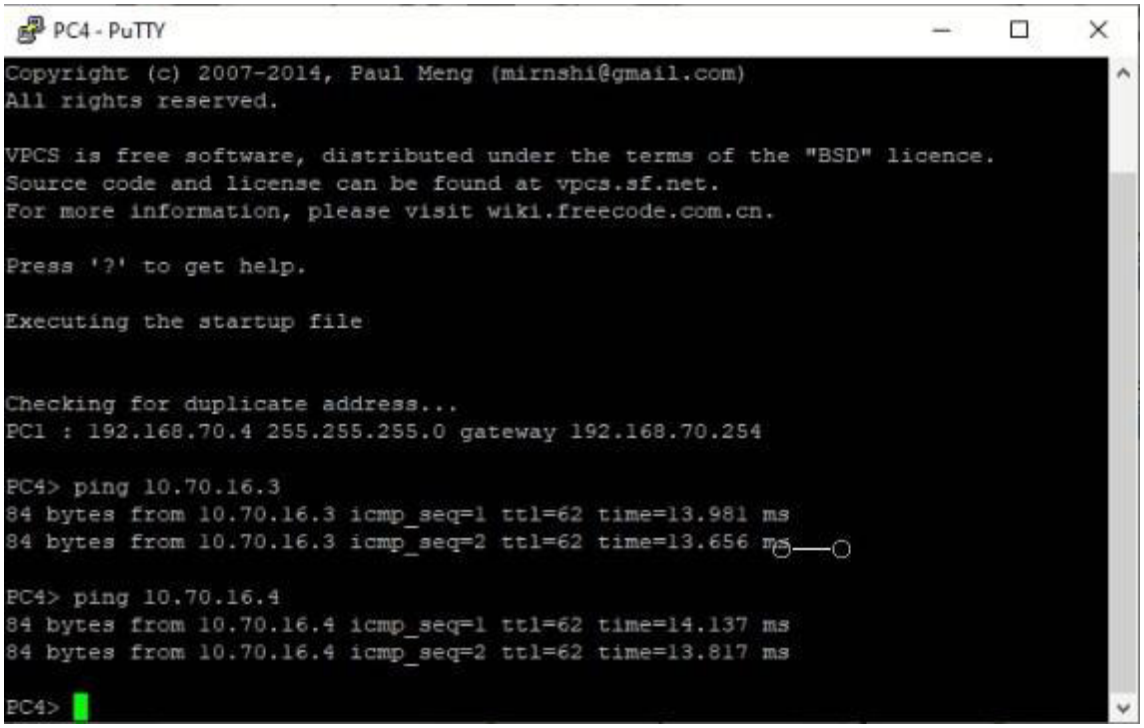


Figura 3.242 Envío de mensajes ICMP Central 2 – Sucursal 2 VPCS 4

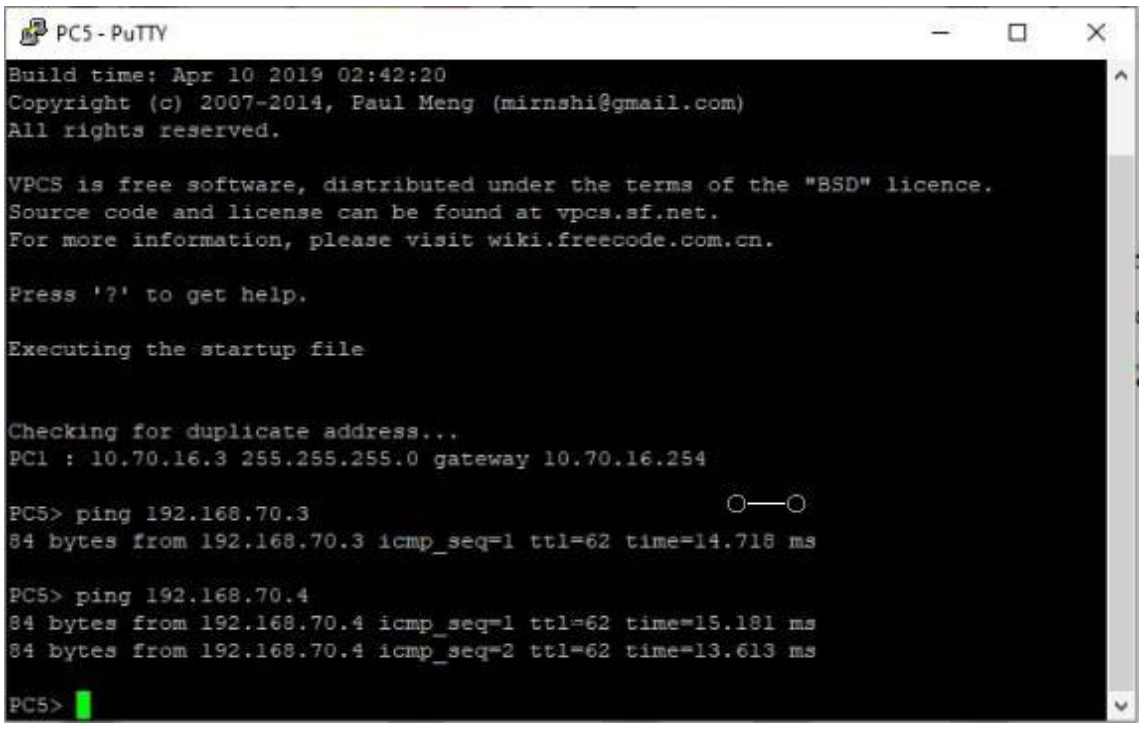


Figura 3.243 Envío de Mensajes ICMP Sucursal 2 – Central 2 VPCS 5

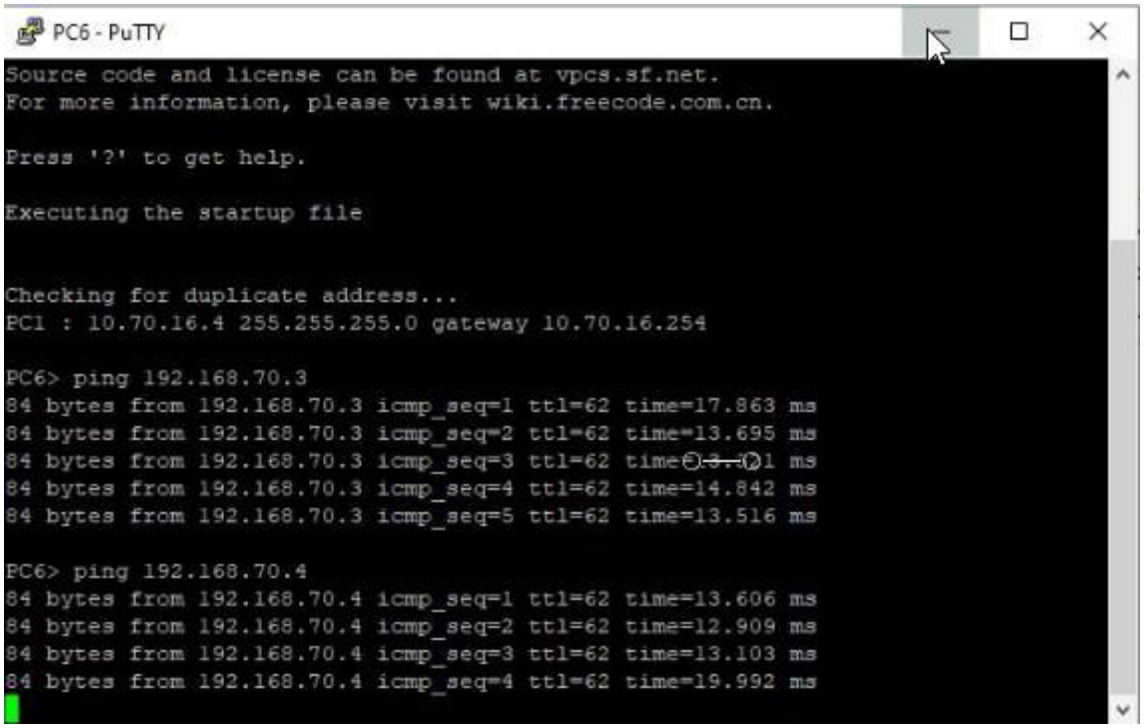


Figura 3.244 Envío de mensajes ICMP Sucursal 2 – Central 2 VPCS 6

En la Figura 3.245 se observa el monitoreo del enlace SDWAN creado, el parámetro correspondiente a la pérdida de paquetes dentro del enlace es de 0 indicando que el enlace funciona correctamente. Además de presentar una optimización de la comunicación esto debido a que los parámetros de latencia y retardo son relativamente similares dando como resultado a un envío de paquetes uniforme a través de la red.

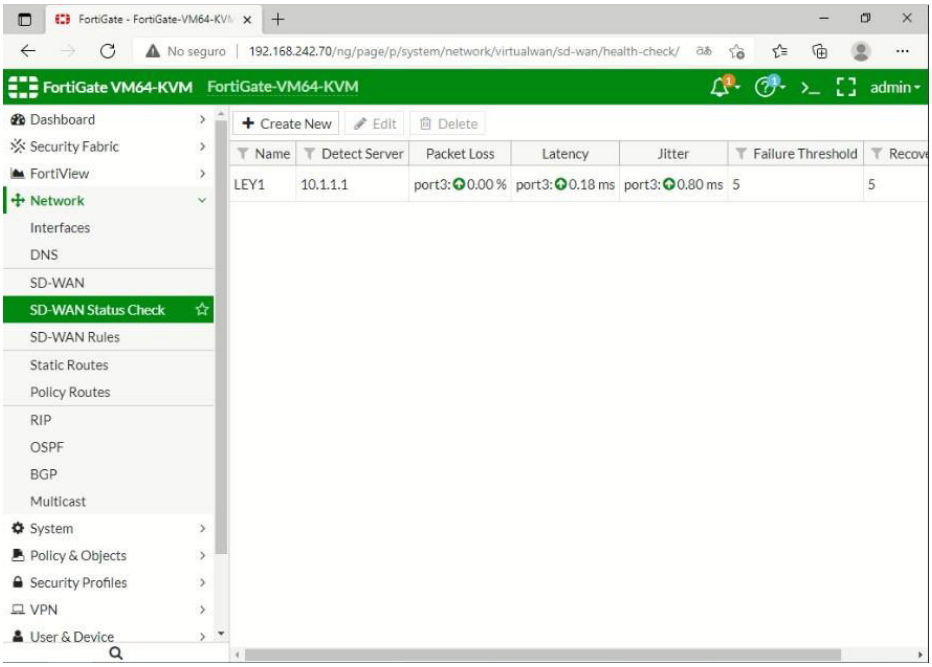


Figura 3.245 Monitoreo del enlace SDWAN en Central 1

Del mismo modo en la Figura 3.246 se observa el estado del enlace SDWAN en la sucursal 1 donde se va a experimentar parámetros similares en la transmisión de información teniendo que el porcentaje de pérdidas es de 0. Se concluye que el enlace opera de forma correcta y que se deben tomar medidas alternas ya que el enlace presenta un mayor valor de retardo que de latencia esto es corregible mediante la aplicación de balanceo de carga.

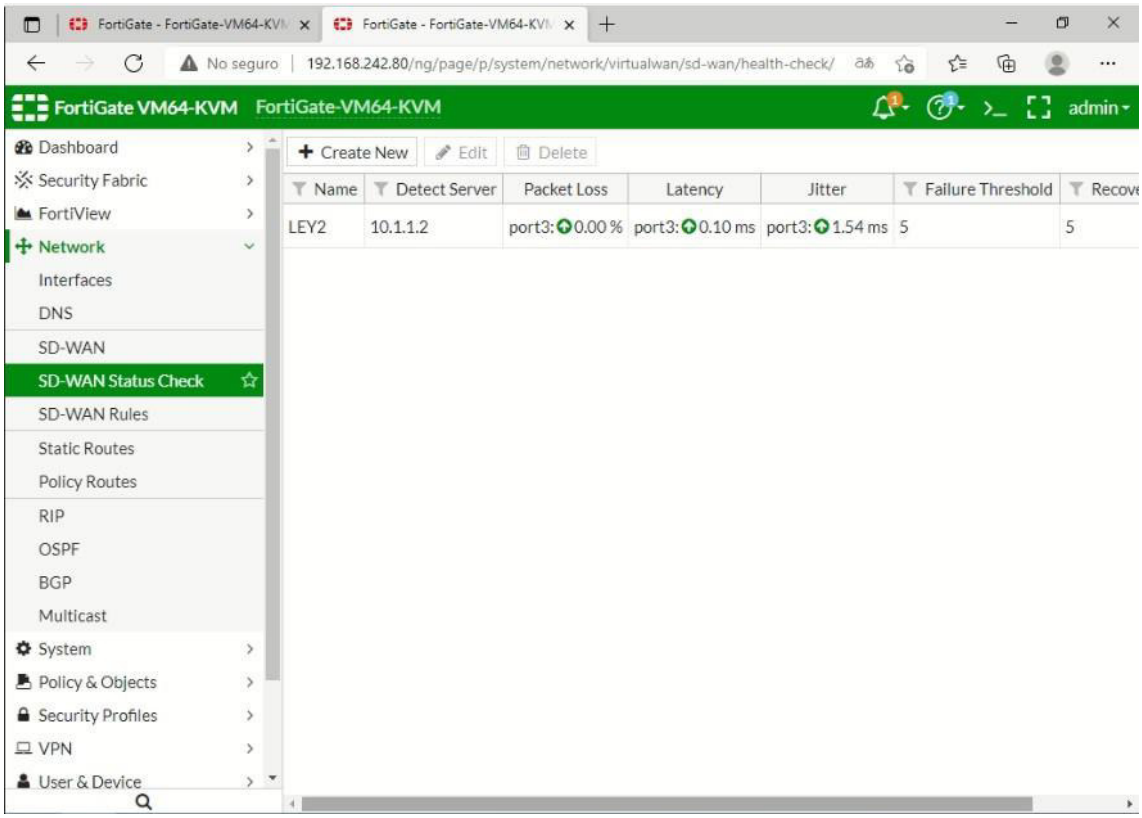


Figura 3.246 Monitoreo del enlace SDWAN en Sucursal 1

En la Figura 3.247 se analiza los parámetros para la segunda central la misma que está operando correctamente es sus enlaces SDWAN debido a que el porcentaje de pérdidas de los paquetes es 0. Sin embargo, se requiere de la aplicación de balanceo de carga para poder optimizar la comunicación debido a las diferencias de los valores de latencia y retardo.

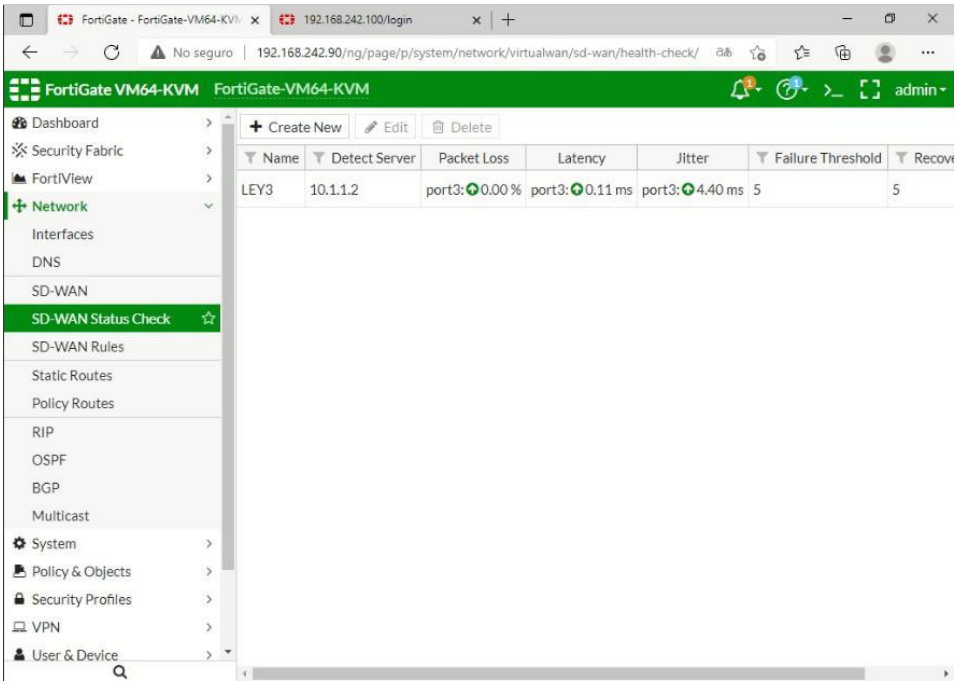


Figura 3.247 Monitoreo del enlace SDWAN en Central 2

Finalmente, se procede al monitoreo de la sucursal 2 al igual que los enlaces pasados se encuentra operando correctamente SDWAN ya que el porcentaje de pérdidas de los paquetes es de 0. De igual manera es necesario aplicar balanceo de carga para optimizar la comunicación esto debido al valor de retardo que se está presentando como se observa en la Figura 3.248.

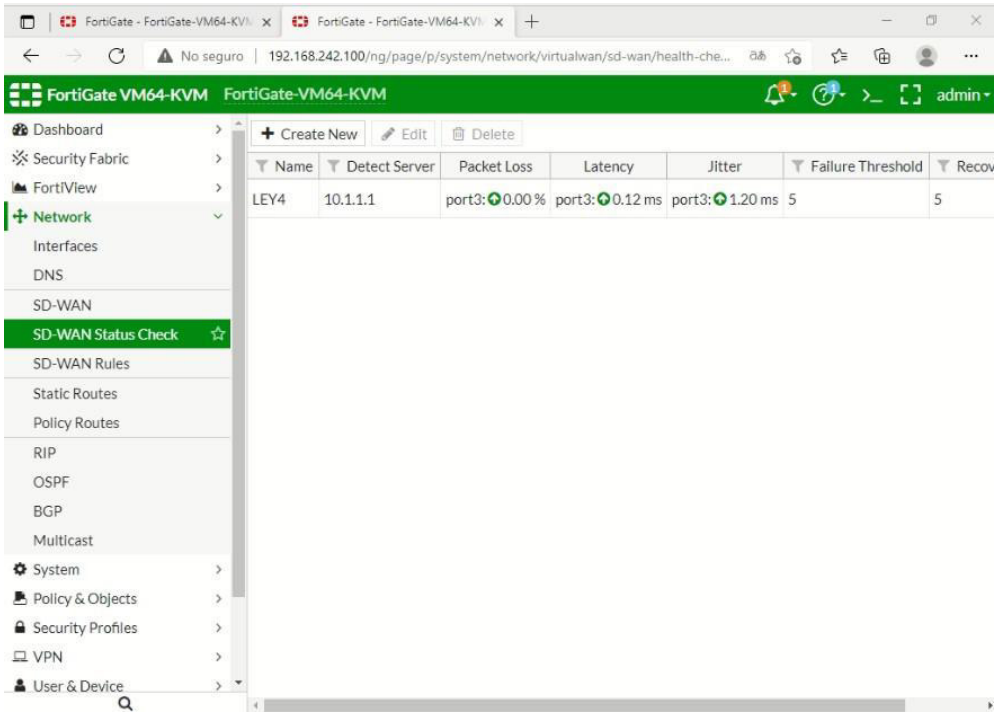


Figura 3.248 Monitoreo del enlace SDWAN en Sucursal 2

Posteriormente, se analiza el estado de la comunicación IPSEC, dentro de la cual se pueden verificar parámetros como el tipo de comunicación que se presenta, en este caso un túnel VPN y el tipo de equipo al cual se accede con la comunicación. Adicionalmente se presenta el estado del túnel, es decir, si se encuentra activo o se encuentra inactivo esto permitirá conocer al administrador de red el estado del servicio y en caso de una pérdida saber que procedimientos son los adecuados a tomar como se aprecia en la Figura 3.249, Figura 3.250, Figura 3.251 y la Figura 3.252 respectivamente.

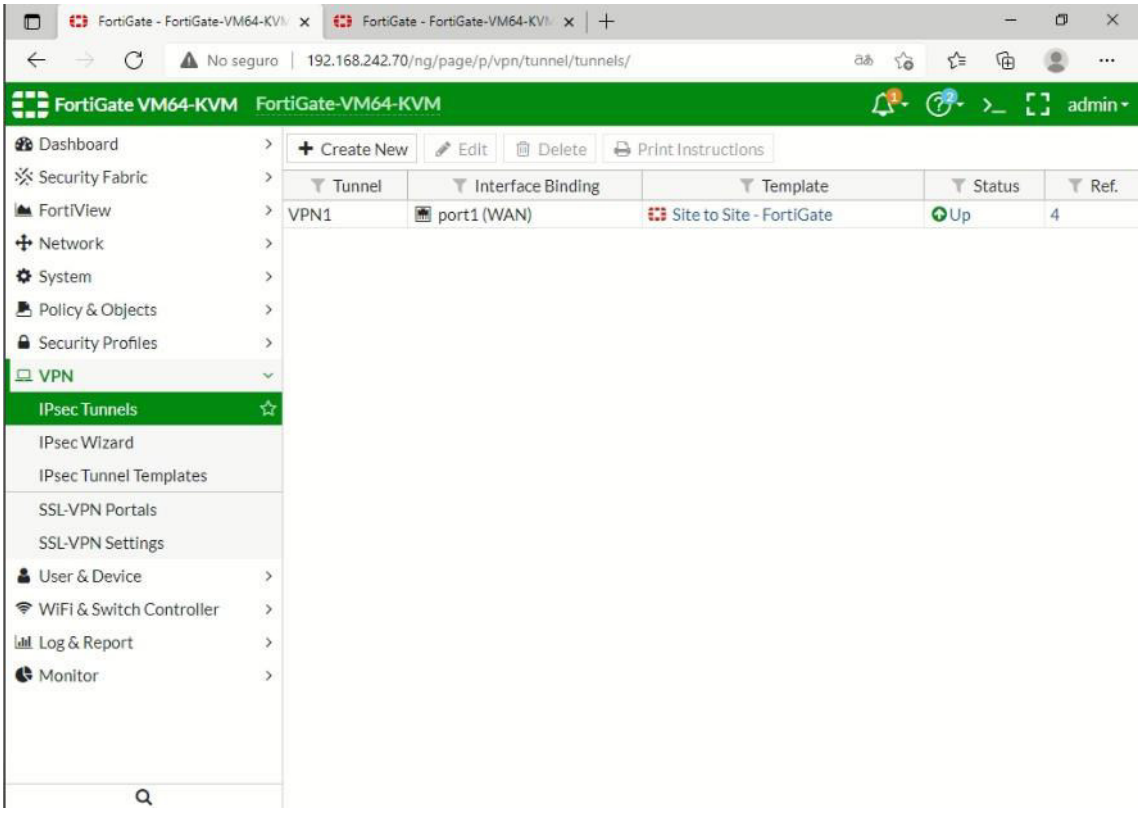


Figura 3.249 Monitoreo de túnel VPN-IPSEC en la Central 1

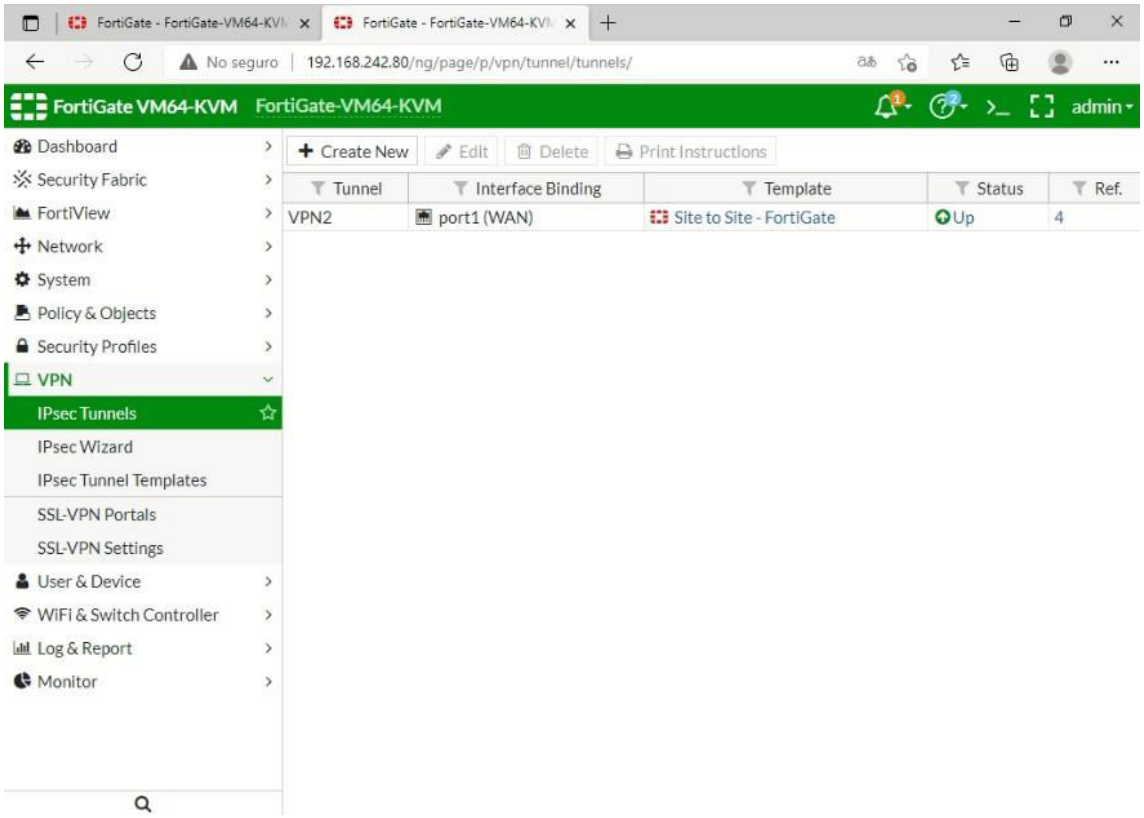


Figura 3.250 Monitoreo de túnel VPN-IPSEC en la Sucursal 1

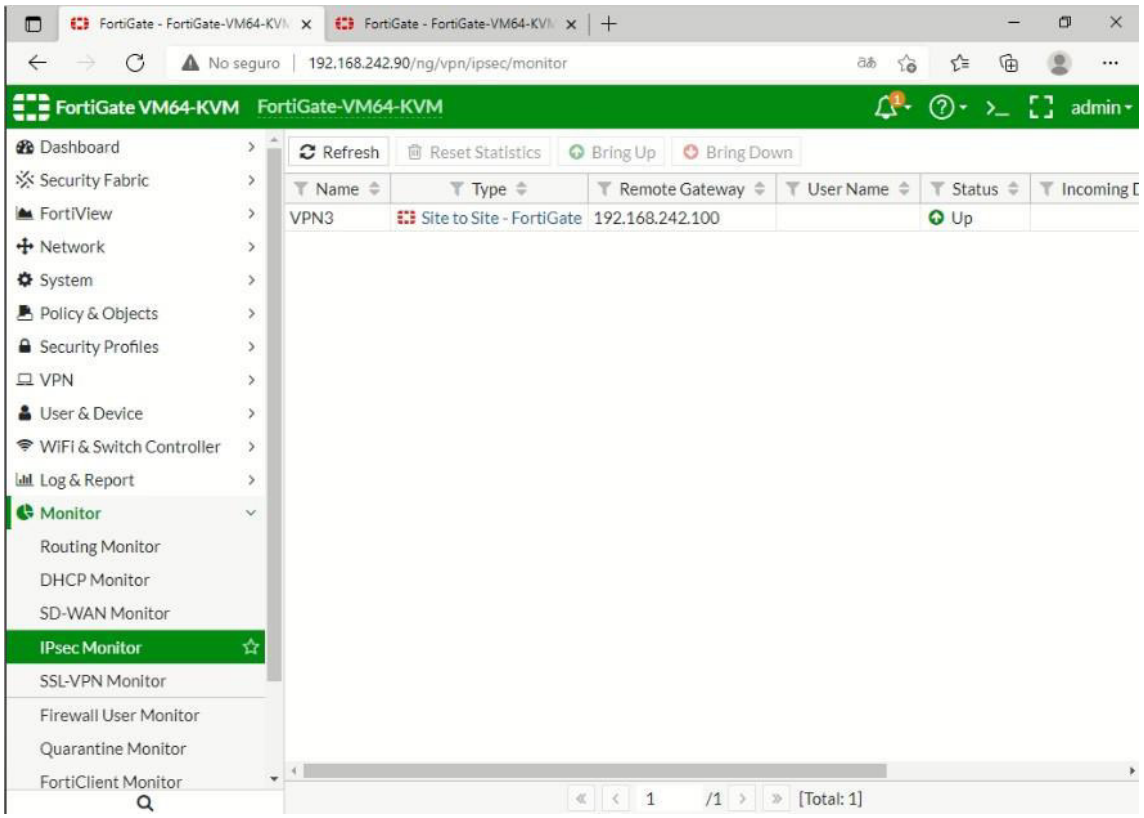


Figura 3.251 Monitoreo de túnel VPN-IPSEC en la Central 2

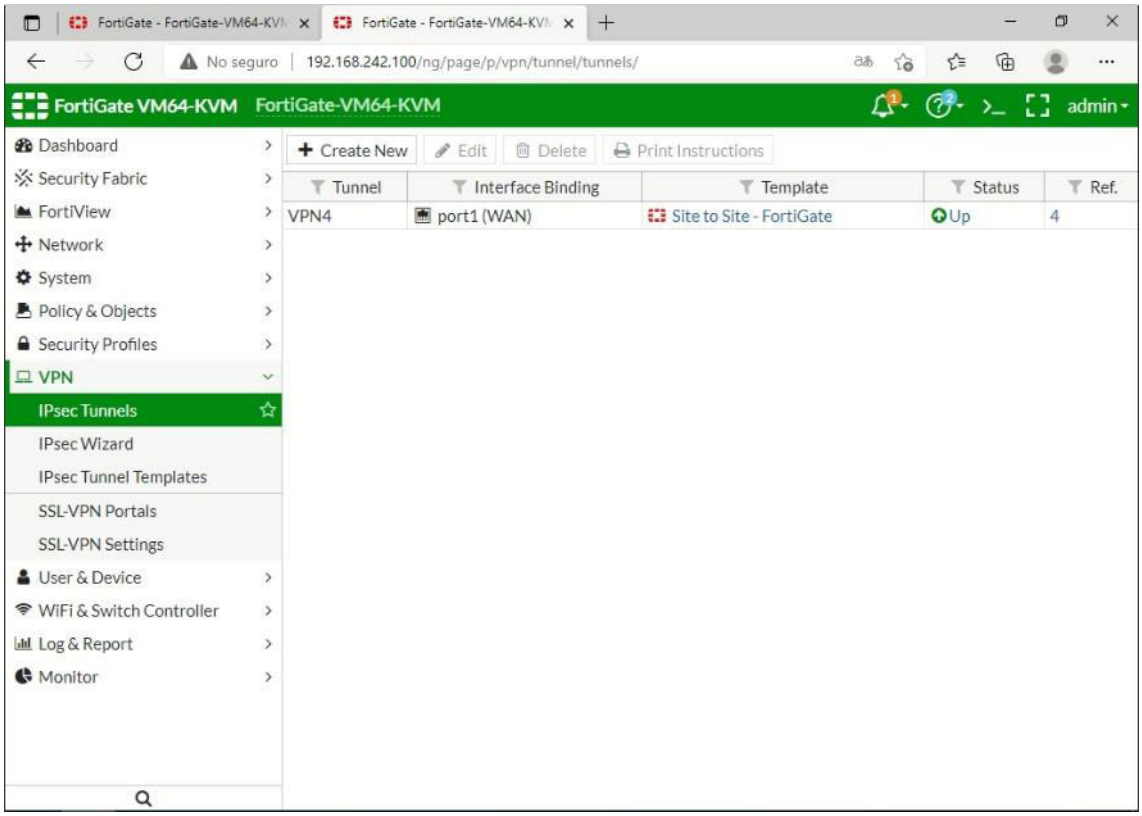


Figura 3.252 Monitoreo de túnel VPN-IPSEC en la Sucursal 2

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Para la configuración de redes de tipo SD-WAN, dentro de equipos Fortigate los cuales son propietarios de la empresa Fortinet, se deben tener varias consideraciones. Pero la más importante es el uso limitado de los equipos a causa de las licencias de prueba, estas limitaciones impiden la realización de redes amplias, sin embargo, se pudo realizar un análisis completo sobre el funcionamiento de estos enlaces en las distintas topologías previamente presentadas.
- En la red que opera mediante enlaces SD-WAN y enrutamiento dinámico de tipo OSPF se puede observar que tanto los tiempos de envío de paquetes, así como las latencias son los adecuados. Estos valores pueden llegar a cambiar en casos reales puesto que están ligados a la velocidad de transmisión de información en internet, otro aspecto a considerar es que para la correcta operación del protocolo de enrutamiento dinámico OSPF se debe contar con una dirección *loopback* caso contrario los paquetes no podrán salir del equipo remitente.
- Con el conocimiento adquirido, la red que opera mediante enlaces SD-WAN y enrutamiento por VLANS posee una gran cantidad de limitaciones en cuanto a políticas. Estas políticas ayudan al administrador de la red a tener un mejor control del tráfico que circula en la misma, sin embargo, de no configurarse correctamente toda la operación de la red se vería comprometida.
- Uno de los aspectos más importantes dentro de los servicios que se pueden implementar en los equipos Fortigate es el uso de comunicaciones mediante túneles VPN y comunicación IPSEC. Si bien es cierto en los equipos Cisco se tiene esta opción Fortinet ofrece un entorno mucho más amigable para la configuración de este tipo de comunicación entre centrales y sucursales. Pero quizá el inconveniente más grande que se presentó en esta red es la incapacidad para poder realizar enlaces de tipo SD-WAN hacia la internet sin haber adquirido la licencia del producto por completo. Sin embargo, esto no limita la capacidad de mantener comunicación con otros equipos Fortigate dentro de la misma red es decir entre centrales y entre sucursales.
- Al momento de realizar una simulación de SD-WAN Cisco hay que verificar que los equipos sean de una misma versión, ya que al momento de realizar la simulación pueden existir errores de conectividad debido a esto. Lo mismo

sucede con el nombre de la organización, que debe ser el mismo en todos los equipos y en caso de no ser el mismo la conexión entre equipos no se podrá realizar.

- Para la elaboración de la simulación se tomó en cuenta los requerimientos mínimos de los equipos, por ello se procedió a utilizar un servidor y al no ser suficiente se tuvo que realizar el uso de *Google Cloud,* ya que el número de procesadores del servidor no eran los adecuados. Hay que considerar que el equipo que más requerimientos tiene es el vManage debido a que es el equipo central y en el cual se va a centralizar la red, tiene una interfaz gráfica y se encarga de las configuraciones remotas.
- Las redes SD-WAN proporcionan seguridad al momento de enviar la información, debido a la creación de túneles entre dispositivos siendo transparente para el cliente el transporte de los paquetes. Además, que la implementación de una red SD-WAN reduce costos, pero se debe tomar en cuenta el tipo de tráfico que se va enviar por la red, debido a que utiliza internet para el envío de la información.
- Después de investigar las soluciones SD-WAN de varios proveedores se ha concluido en realizar la configuración y estudio de las soluciones de Cisco y Fortinet, debido a que todas las soluciones necesitan de licencias para el uso de los equipos y la información de los comandos es limitada en ciertos casos. Cisco proporciona información y cursos sobre las soluciones SD-WAN, el curso de preparación para la certificación CCNP SD-WAN en comparación con los demás cursos es accesible, además que en curso se proporcionó las licencias de los equipos para las practicas. Por ello se escogió Cisco. Fortinet proporciona demos de los equipos con lo cual no se deben pagar licencias.

4.2 Recomendaciones

- Después de la realización de las diferentes topologías tanto en Cisco como en Fortinet se puede decir que ambas tienen sus ventajas y desventajas, sin embargo, es recomendable usar equipos Fortigate para la elaboración de redes con enlaces SD-WAN, esto porque brinda un entorno más amigable con el usuario para la configuración de las redes y las licencias que se brindan permiten el análisis del comportamiento de las redes, esto si se desea realizar una simulación. Por otra parte, si se desea realizar una implementación es recomendable usar equipos Cisco por su amplia gama de servicios que se pueden implementar y la fiabilidad de sus enlaces.

- Para realizar simulaciones es recomendable que se utilice versiones 5.6 en adelante de los equipos, puesto que las versiones más actuales de Fortigate no son compatibles aún con algunas de las configuraciones realizadas previamente, como lo es el caso de los túneles de tipo IPSEC.
- Se recomienda tener la versión 20 del software de simulación GNS3, esto debido a que los equipos Fortigate suelen presentar problemas en versiones previas del sistema, adicionalmente se recomienda tener las últimas versiones de los equipos Cisco para las simulaciones de equipos como *switches* o *routers* en caso de que se desee realizar una topología mixta.
- Se recomienda el uso de *Google Cloud* para las simulaciones de SD-WAN Cisco, debido a que los equipos requieren altos recursos. El uso de *Google Cloud* puede ayudar al momento de realizar prácticas que necesitan de grandes recursos además de que su mayor beneficio es que tienen una etapa de prueba de 90 días gratis y un crédito de 300 dólares.
- Se recomienda usar SD-WAN Cisco para el tráfico que no requiera de grandes velocidades o que no sean de tiempo real. Esto debido a que la solución SD-WAN va a pasar a través de internet y dependerá del mismo para la entrega de los datos. Para el tráfico de tiempo real se recomienda utilizar una red MPLS ya que cumplirá en todo momento con las velocidades requeridas para el transporte de ese tipo de tráfico.
- Se debe tener conocimientos de Linux para la instalación de las máquinas virtuales y las configuraciones de los equipos. En la creación de las instancias en el *Google Cloud* se instala un SO de Linux por lo cual ayudará de gran manera saber los comandos básicos. Además, que al momento de montar certificados y firmar los mismos se ingresa en la vshell de los equipos donde se utiliza comandos de Linux. Para la configuración inicial de los equipos casi nunca existe una interfaz gráfica, estos equipos utilizan una CLI para su configuración inicial por lo cual lo mínimo que se debe conocer es: configuración de interfaces, asignación de IP y levantar interfaces.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] Z. Yang, «Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities,» 9 May 2019. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/8847124. [Último acceso: 24 April 2021].

[2] CISCO, «CISCO,» [En línea], 12 03 2018. [En línea]. Available: https://www.cisco.com/c/es_es/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html.. [Último acceso: 12 01 2021].

[3] «IEEE 2014 International Science and Techonolofy Conference (Modern Networking Technologies),» MoNeTec, 28 10 2014. [En línea]. Available: http://libgen.rs/scimag/10.1109%2Fmonetec.2014.6995604. [Accessed: 14- Jan- 2021].. [Último acceso: 14 01 2021].

[4] «IEEE 2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC) - Moscow, Russia,» MoNeTec, 28 10 2014. [En línea]. Available: http://libgen.rs/scimag/10.1109%2Fmonetec.2014.6995604. . [Último acceso: 14 01 2021].

[5] H. Xiaolan, «Multi-controller deployment algorithm in hierarchical architecture for SDWAN,» Yifeng, 2019. [En línea]. [Último acceso: 2021].

[6] Y. Kongzhe, «Multi-Controller Placement for Load Balancing in SDWAN,» Zhao Bing, 2019. [En línea]. [Último acceso: 2021].

[7] A. Khaled, « A simulation framework for interconnecting distributed datacenters over Software-Defined Wide Area Network (SD-WAN),» IoTSim-SDWAN, 2020. [En línea]. [Último acceso: 2021].

[8] S. Hua, «Automated Traffic Engineering in SDWAN: Beyond Reinforcement Learning, Toronto,» INFOCOM , 2020. [En línea]. [Último acceso: 2021].

[9] I. Lakatos, «Metodologia de los programas de investigacion cientifica,» 12 junio 2007. [En línea]. Available: Available: http://libgen.rs/book/index.php?md5=21B4561D543B55F9201FD6D30E60CC7A. [Último acceso: 2 Marzo 2021].. [Último acceso: 2021].

[10] Ю. Лисецкий, «Особенности SDN-технологии от Cisco Systems,» 16 marzo 2020. [En línea]. Available: https://e-archivo.uc3m.es/handle/10016/29330. [Último acceso: 7 marzo 2021].

[11] A. Iorguta, «Cisco SD-WAN. Incorporación de controladores.,» Cisco, 13 junio 2018. [En línea]. Available: https://pocvlab.com/cisco-sd-wan-controllers-onboarding/. [Último acceso: 07 marzo 2021].

[12] D. Y. D. S. J. C. J. Gooley, «Redes de área amplia definidas por software de Cisco: diseño, implementación y protección de su WAN de próxima generación con Cisco SD-WAN,» 07 marzo 2021. [En línea]. Available: http://library.lol/main/3CB8F68E70BAEC73F9268F2ACB98AE08.. [Último acceso: 19 mayo 2021].

[13] J. Lemus, «Vertical-iberica,» 19 02 2020. [En línea]. Available: https://vertical-iberica.com/que-es-fortinet-y-como-funciona/. [Último acceso: 2021].

[14] «Fortinet,» 16 mayo 2016. [En línea]. Available: https://drive.google.com/file/d/0B3ERI4p-nn66dHc4MFZWU3dGdFk/view?resourcekey=0-LSi4iThvXtmKRomng7YccQ. [Último acceso: 2021].

[15] Fortinet, «FortiOS 5.6,» [En línea]. Available: https://files.eetgroup.com/MStronic/FortiOS%205_6%20Data%20Sheet%20-%20APRIL%202017%20FINAL_pptx.pdf. [Último acceso: 19 mayo 2021].

[16] H. Enterprise, «Support Huawei,» 3 June 2021. [En línea]. Available: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100164637&id=EN-US_TOPIC_0194319490&lang=en. [Último acceso: 12 November 2021].

[17] J. SUPPORT, «Juniper Solutions,» 12 January 2021. [En línea]. Available: https://www.juniper.net/content/dam/www/assets/solution-briefs/us/en/routers/connect-thousands-of-branch-offices-with-session-smart-sd-branch.pdf. [Último acceso: 12 November 2021].

ANEXOS

ANEXO 1: CERTIFICADO DE FUNCIONAMIENTO

ESCUELA POLITECNICA NACIONAL
Campus Politécnico "J. Rubén Orellana R

Quito, 22 de septiembre de 2021

CERTIFICADO DE FUNCIONAMIENTO DE PROYECTO DE TITULACIÓN

Yo, Fernando Vinicio Becerra Camacho, docente a tiempo completo de la Escuela Politécnica Nacional y como director de este trabajo de titulación, certifico que he constatado el correcto funcionamiento de la simulación de redes SD-WAN las cuales fueron implementadas por los estudiantes Adrián Pérez y Jefferson Gualoto.

DIRECTOR

Ing. Fernando Vinicio Becerra Camacho

Ladrón de Guevara E11-253, Escuela de Formación de Tecnólogos, Oficina 28. EXT: 2729
email: pablo.proano@epn.edu.ec Quito-Ecuador

ANEXO 2: VIDEO DE FUNCIONAMIENTO