UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA
TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

"INGENIERO ELECTRÓNICO"

TITULO DEL PROYECTO TÉCNICO:

"DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL"

AUTORES

VERA VÉLEZ ERICK ÁLVARO
LLAMBO VERA OSCAR OMAR

DIRECTOR

PhD. BREMNEN VÉLIZ NOBOA

GUAYAQUIL – ECUADOR

2021

CERTIFICADOS DE RESPONSABILIDAD Y AUTORÍA

Nosotros, Vera Vélez Erick Álvaro y Llambo Vera Oscar Omar permitimos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su respectiva trascripción sin fines de lucro. También, exponemos que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Vera Velez Erick Álvaro

CI: 0930497151

Llambo Vera Oscar Omar

CI: 0923652903

Guayaquil,15 de marzo de 2021

CERTIFICADO DE CESIÓN DE DEREECHOS DE AUTOR

Nosotros, Erick Álvaro Vera Vélez con documento de identificación N° 0930497151 y Oscar Omar Llambo Vera con documento de identificación N° 0923652903, declaramos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación titulado "DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL ", mismo que ha sido desarrollado para optar por el título de "INGENIERO ELECTRÓNICO", en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil, quedando la Universidad autorizada para ejercer plenamente los derechos aprobados anteriormente.

Vera Velez Erick Álvaro
CI: 0930497151

Llambo Vera Oscar Omar
CI: 0923652903

Guayaquil,15 de marzo de 2021

CERTIFICADO DE DIRECCIÓN DE TRABAJO DE TITULACIÓN

Yo PhD. Bremnen Véliz, expresó que bajo mi dirección y asesoría fue desarrollado el proyecto técnico de titulación “DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL”, realizado por los estudiantes VERA VÉLEZ ERICK ÁLVARO con cédula ciudadanía 0930497151 y LLAMBO VERA OSCAR OMAR con cedula de ciudadanía 0923652903 obteniendo un producto que cumple con los objetivos del diseño de aprobación, informe final y además los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Guayaquil,15 de marzo de 2021

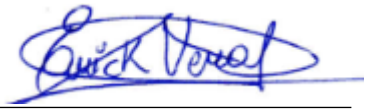
_____

Tutor del Trabajo de titulación
Docente Ing. Bremnen Véliz Noboa, PhD.
CI: 0703865139

DECLARATORIA DE RESPONSABILIDAD

Nosotros, Erick Álvaro Vera Vélez portador de la cédula de identidad N° 0930497151 y Oscar Omar Llambo Vera portador de la cedula de identidad N° 0923652903, estudiantes de la Universidad Politécnica Salesiana con sede Guayaquil, expresamos que la responsabilidad del contenido de este proyecto de titulación pertenece meramente y es propiedad intelectual de la Universidad Politécnica Salesiana sede Guayaquil.

Guayaquil,15 de marzo de 2021



Vera Velez Erick Álvaro
CI: 0930497151

Llambo Vera Oscar Omar
CI: 0923652903

DEDICATORIA

Este proyecto de titulación va dedicado inicialmente a Dios y a mis padres, quienes me han conducido y apoyado durante todo este tiempo en mis estudios para culminarlos y ser un profesional.

Agradezco a mi padre el Ab. Rolando Vera por su ayuda constante y esfuerzo para lograr este objetivo también a mi madre la Sra. Digna Vélez por sus consejos que me dio durante toda la vida desde que. fui un niño a hasta ahora a ellos le dedico cada logro personal y profesional que he alcanzado.

Erick Álvaro Vera Vélez

DEDICATORIA

La presente tesis esta dedicada a mis padres ya que sin ellos no sabia posible lograr concluir mis proyectos profesionales. También quiero dedicar este proyecto a mis hermanos que creyeron en mi y me apoyaron para que persista en mis objetivos y por ultimo a mis compañeros que estuvieron desde el principio y a lo que se unieron en el camino y fueron de gran compañía en todos estos años.

Oscar Omar Llambo Vera

.

AGRADECIMIENTO

Agradezco a Dios primeramente por haberme dado la vida, salud y sabiduría para llegar a esta etapa de mi vida que es mi titulación como profesional logrando superar cada uno de los obstáculos que se presentan, gracias a mi familia y a mi hija Emma Vera que fueron el motor principal para obtener hoy esta alegría y por apoyarme en cada decisión de este proyecto también me gustaría agradecer a los docentes de la carrera por sus enseñanzas en el aula y sus experiencias que nos compartían durante toda mi carrera universitaria porque todos han aportado con un granito de arena a mi formación como profesional.

Erick Álvaro Vera Vélez

AGRADECIMIENTO

En primera instancia quiero agredecer a Dios, a mis padres ya que me supieron inculcar el trabajo e integridad, a mis compañero tesista ya que sin ellos no había sido posible este proyecto. Deseo expresar mis mas sinceros agradecimiento hacia la Universidad Politécnica Salesiana sede Guayaquil, a sus directivos y docentes por haberme formado como profesionales a lo largo de estos años

Oscar Omar Llambo Vera

RESUMEN DEL PROYECTO

La presente tesis: “DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON REDES DEFINIDAS POR SOFTWARE (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL”, se basa en la necesidad de contar con un banco de prueba virtualizado para REDES DEFINIDAS POR SOFTWARE, MPLS, FRAME RELAY, BGP, ENRUTAMIENTO ESTÁTICO,SWTICHES ADMINISTRABLES y para diferentes tipos de tecnologías de routers, firewall, switches que se encuentran en las empresas donde los estudiantes y los docentes podrán configurar estos dispositivos, observar el comportamiento y la fiabilidad de la red viendo que dispositivo es más seguro en el momento de implementación para la proteger la información de los usuarios finales y aprender de ellos.

El estudio de esta nueva tecnología se fundamenta en controlar la demanda de servicios, ancho de banda, menor ping para mejorar la optimización de la capacidad de la red donde la redes definidas por software escogen el enlace WAN con menor fluctuación. Para la simulación de esta tecnología se virtualizo un servidor DELL R210 II que se encuentra en el laboratorio de telecomunicaciones el cual se optimizó en memorias ram y disco duros SSD para mejor rendimiento en el momento de la simulación .

El objetivo de este proyecto es constuir un banco de pruebas virtualizado para ayudar a los estudiante y docentes de la universidad para simular ROUTERS, SWITCH, FIREWALL de diferentes marcas comerciales, los estudiantes no cuentan con un infraestructura donde se pueda simular estas nuevas tecnologías de redes para realizar las configuraciones de estos dispotivos, el laboratorio de telecomunicaciones cuenta con el programa CISCO PACKET TRACER que solo permite simular los dispositivos que vienen en su software permitiendo una configuración restringida en el momento de diseñar una topología de una red por ejemplo al configurar una red MPLS las versiones actuales no permiten la configuración de esta tecnología .

ABSTRACT

This thesis: "DESIGN AND IMPLEMENTATION OF A VIRTUALIZED TEST BANK WITH NETWORKS DEFINED BY SOFTWARE (SD-WAN) IN THE TELECOMMUNICATIONS LAB FOR THE UNIVERSIDAD POLITÉCNICA SEDE GUAYAQUIL", is based on the test of having a virtualized NETWORK DEFINED BY SOFTWARE, MPLS, FRAME RELAY, BGP, STATIC ROUTING, ADMINISTRABLE SWTICHES and for different types of technologies of routers, firewall, switches found in companies where students and teachers can configure these devices, observe the behavior and the network reliability seeing that the device is more secure at the time of deployment to protect the information of the end users and learn from them.

The study of this new technology is based on controlling the demand for services, bandwidth, lower ping to improve the optimization of network capacity where software-defined networks choose the WAN link with the least fluctuation. For the simulation of this technology, it was virtualized on a DELL R210 II server that is in the telecommunications laboratory, which was optimized in ram memories and SSD hard drives for better performance at the time of simulation.

The objective of this project is to build a virtualized test bed to help university students and teachers to simulate ROUTERS, SWITCH, FIREWALL of different commercial brands, the students do not have an infrastructure where these new network technologies can be simulated To configure these devices, the telecommunications laboratory has the CISCO PACKET TRACER program that only allows simulating the devices that come in its software allowing a restricted configuration when designing a network topology, for example when configuring a network MPLS current versions do not allow the configuration of this technology.

Tabla de contenido

Tabla de ilustraciones

INTRODUCCIÓN

La presente investigación se refiere al tema de diseño e implementación de un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN).

Una red SD-WAN se define como una sustitución del hardware de redes WAN tradicional como los enrutadores configurados mediante de línea de comandos (CLI) con administración centralizada al aplicar redes definidas por software (SDN) a conexiones de red de área amplia (WAN) para ofrecer de manera más eficaz aplicaciones a usuarios en largas distancias.

La característica principal de este tipo de red es que no depende de amplia cantidad de equipos físicos, lo que brinda una flexibilidad y eficacia en la administración, enrutando dinámicamente el tráfico a través de enlaces privados y públicos, tales como enlaces MPLS arrendados y banda ancha, Long Term Evolution (LTE) y/o inalámbricos.

La realización de este proyecto se basa que al no contar con un laboratorio donde se pueda implementar las nuevas tecnologías de manera virtualizada con emuladores Gns3 en el cual se pueda realizar simulaciones, modificaciones, configuraciones de redes físicas y virtuales, sea capaz de satisfacer las necesidades de los estudiantes y se puedan preparar para la incorporación de nuevas tecnologías y formas de uso.

Asimismo percibiremos en los siguientes capítulos como virtualizar un servidor,repotenciar su hadware a través de las especificaciones del equipo y la elección del software para virtualizar y crear el ambiente virtual para el desarrollo de las diez prácticas que se diseño de redes definidas por software para redes de área amplias.

El actual documento se ejecuta en el diseño e implementación de un banco de pruebas virtualizado para redes definidas por software para redes de área amplia (SD-WAN) empleada en la Universidad Politécnica Salesiana sede Guayaquil la cual cumple con la formación académica de los estudiantes.

CAPÍTULO I

EL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

La tecnología para la comunicación global va evolucionando con el transcurso del tiempo, surgiendo nuevas formas para comunicarse que demanda más dispositivos en la red. Llegará un punto en el cual no podremos seguir conectados restringiendo el acceso a la conexión de dispositivos a nuestra red local o empresarial generando cuellos de botellas, banda ancha limitada, ataques de información causando retrasos al momento de transferir información. Actualmente encontramos en el mercado hardware que va a permitir solucionar este tipo de inconvenientes dentro la red o para enlaces WAN, pero suelen ser costosa.

En la nube encontramos software que nos permiten de una manera virtual emular dispositivos como routers, switches, firewall y sistemas operativos, usando recursos físicos de nuestros equipos informáticos en disco duro, CPU y memoria RAM, los estudiantes de las carreas de Ingeniería Electrónica e Ingeniería en Telecomunicaciones podrán realizar estas simulaciones.

El laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil no cuenta con el hardware necesario para efectuar simulaciones de redes definidas por software para redes de áreas amplias de forma virtualizada donde los estudiantes obtendrán las prácticas para la conexión de estas redes, para cifrar y segmentar el tráfico de la red, permitir identificar problemas para una solución rápida, lograr un mayor rendimiento de las aplicaciones, para conseguir una experiencia optima y garantizar la disminución de latencia en la red.

1.2. ANTECEDENTES

El laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil actualmente no consta con una plataforma para virtualizar o emular redes de datos por lo cual se ha considerado desarrollar este proyecto, al ser una tecnología nueva que no se encuentra implementada en la Universidad Politécnica Salesiana. Las practicas propuestas permitirán de manera virtualizada hacer la conexión de redes WAN, cifrar y segmentar el tráfico de la red, identificar problemas de red, lograr un mayor rendimiento de las aplicaciones, conseguir una experiencia optima y garantizar la disminución de latencia en la red.

El desarrollo de este proyecto será de gran beneficio, principalmente a los estudiantes y los docentes que imparten las materias de redes de computadores y redes de comunicaciones permitiendo el desarrollo e investigación de nuevas tecnologías donde se podrá cambiar el

comportamiento de una red dinámica, mejorar el rendimiento de las redes actuales, los cuales aportaran al entendimiento de este nuevo tipo de arquitectura.

1.3. IMPORTANCIA Y ALCANCES

Este proyecto tiene como propósito ser de impacto e innovación como resultado la preparación y conocimiento para enfrentarse a los cambios que se presentarán a futuro en diferentes empresas de telecomunicaciones que deseen implementar las nuevas soluciones de conectividad abaratando costos de implementación lo cual reduce la intervención de técnicos y la probabilidad de errores.

1.4. DELIMITACIÓN

1.4.1. ESPACIAL

El proyecto técnico para la obtención del título de ‘‘Ingeniero Electrónico mención Telecomunicaciones”, fue implementado en la Universidad Politécnica Salesiana sede Guayaquil.

1.4.2. ACADÉMICA

Orientado a las materias de Redes de Computadoras 1, Redes de Computadoras II y Redes de Comunicación.

1.4.3. TEMPORAL

El presente proyecto técnico se realizó durante en el período 2020-2021.

1.5. OBJETIVOS

1.5.1 OBJETIVO GENERAL

Diseñar e implementar un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN) para el laboratorio de telecomunicaciones de la Universidad Politécnica salesiana sede Guayaquil.

1.5.2 OBJETIVOS ESPECIFICOS

- Comparar los diferentes tipos de tecnologías de virtualización.
- Generar un escenario virtual para el acceso remoto a los estudianes al servidor.
- Analizar el funcionamiento de los protocolos TCP/IP con la tecnología SD-WAN.
- Diseñar e implementar diez prácticas con diversos protocolos de red para pruebas de conectividad.

1.5.2 METODOLOGÍA

Se usa la metodología experimental porque es el instrumento principal debido a que los estudiantes podrán manipular, configurar, diseñar y comparar redes definidas por software de manera virtual obtenido resultados positivos y acertados estas pruebas fueron desarrolladas con el fin de demostrar el enlace de comunicación consiguiendo sacar terminaciones sobre los resultados de las prácticas llevando a cabo los conocimientos técnicos y teóricos aprendidos a lo largo de nuestra vida universitaria.

1.5.2 BENEFICIARIOS DE LA PROPUESTA E INTERVENCIÓN

Los alumnos de las carreras de Ingeniería Electrónica e Ingeniería en Telecomunicaciones son los principales beneficiarios en la elaboración de este proyecto.

CAPÍTULO II

MARCO TEÓRICO

2.1. VIRTUALIZACIÓN

La virtualización es la forma que se complementa el hardware y software de los sistemas operativos que se van a utilizar. Nos permite ejecutar varios sistemas operativos de manera concurrente en un solo servidor físico, donde podemos provisionar alcamenamiento de discos duro, memoria RAM y CPU para las diferentes maquinas virtuales dependiendo la necesidad de los beneficiarios o empresa.(Fernández & García, 2011).

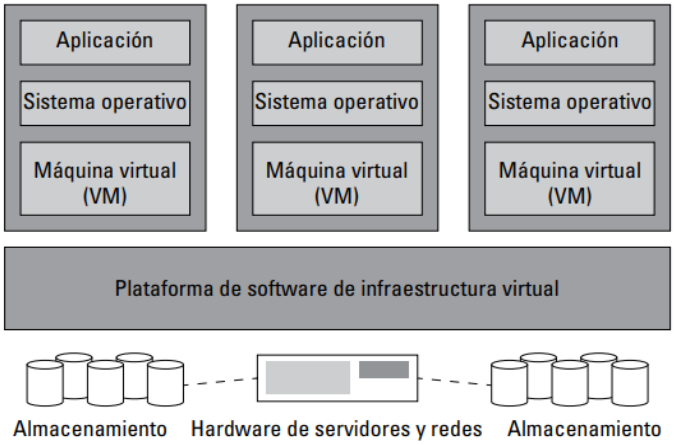


Figura 1 Vista de una virtualización
Fuente: Seguridad para la nube y la virtualización FOR DUMMIES [DANIEL Reis, 2013]

2.2.1. TIPOS DE VIRTUALIZACIÓN

En la actualidad encontramos diversos ejemplos de virtualización:

- Virtualización por servidores.
- Virtualización de memorias.
- Virtualización de Almacenamiento (Storage).
- Virtualización de Escritorio (Desktop).
- Virtualización de redes (network)

2.2.2. VIRTUALIZACIÓN POR SERVIDORES

Esta manera de virtualizar a través de servidores es un entorno que está constituido en hardware mediante un software propietario que representa un

ambiente computacional. El software invitado, que habitualmente es un SO completo comienza a iniciar como si fuera un hardware independiente.

Las diversas máquinas virtuales son simuladas por un servidor físico para que esto funcione se asigna los recursos tales como memoria RAM, CPU y almacenamiento del servidordor y estos recursos ser determinados primeramente por un árbitro (hypervisor). (Fernández & García, 2011).

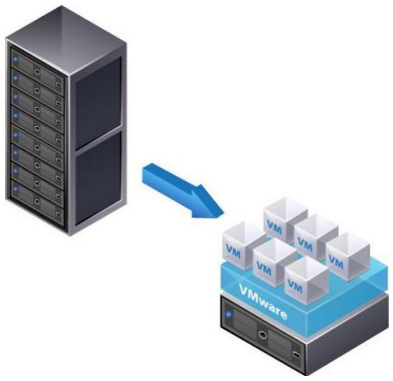


Figura 2 Virtualización de un servidor
Fuente. Virtualización de servidores por Alex Marquez.Universidad Politécnica de Catalunya (UPC)[Alex Márquez, 2011]

2.2.3. VIRTUALIZACIÓN POR MEMORIAS

Este tipo de virtualización por memorias sirve de un modo diferente tienendo como recurso a las diversas restricciones que imputa la memoria física, siendo el motivo de los cuellos de botella para el funcionamiento de las aplicaciones o servicios.

Debemos tener en cuenta los siguientes objetivos en el instante de virtualizar por memoria:

- Asignar los recursos suficentes de memoria RAM a diferentes aplicaciones y sistemas operativos teniendo en cuenta la demanda.
- Aumentar la eficacia y disminuir en el tiempo de ejecución de aplicaciones de los servidores que usan un intenso consumo de memoria. (Fernández & García, 2011).

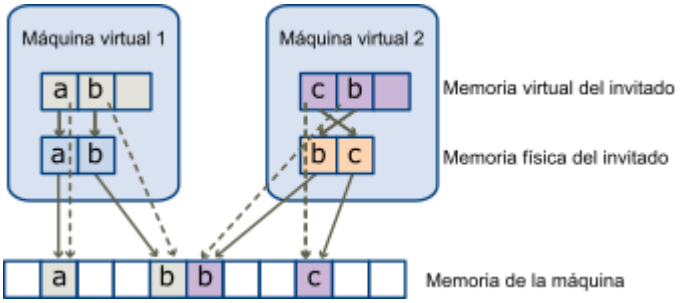


Figura 3. Virtualizacon de memoria
Fuente. Virtualización..Yenisleidy Fernández Romero1, Karen García Pombo2 [Fernandez & Garcia, 2011]

2.2.4. VIRTUALIZACIÓN DE ALMACENAMIENTO (STORAGE)

La representación de virtualización por almacenamiento se describe como el método de utilizar el almacenamiento físico en almacenamiento lógico. Su principal objetivo es el ahorro de recursos de almacenamiento en los servidores su función es en dirigir, administar y gestionar los espacios de almacenamiento físico..(Fernández & García, 2011).

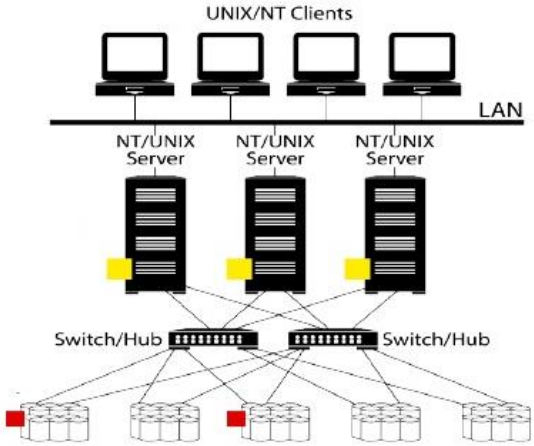


Figura 4. Virtualizacon de Almacenamiento
Fuente. https://sites.google.com/site/wwwvirtualizacioneducom/

2.2.5. VIRTUALIZACIÓN DE ESCRITORIO (DESKTOP)

Este método refiere a elaborar un entorno de cliente-servidor este se guarda en un servidor principal o central, con sus funciones, servicios y aplicaciones para acceder mediante uan conexión remota desde el escritorio virtual. (Fernández & García, 2011).

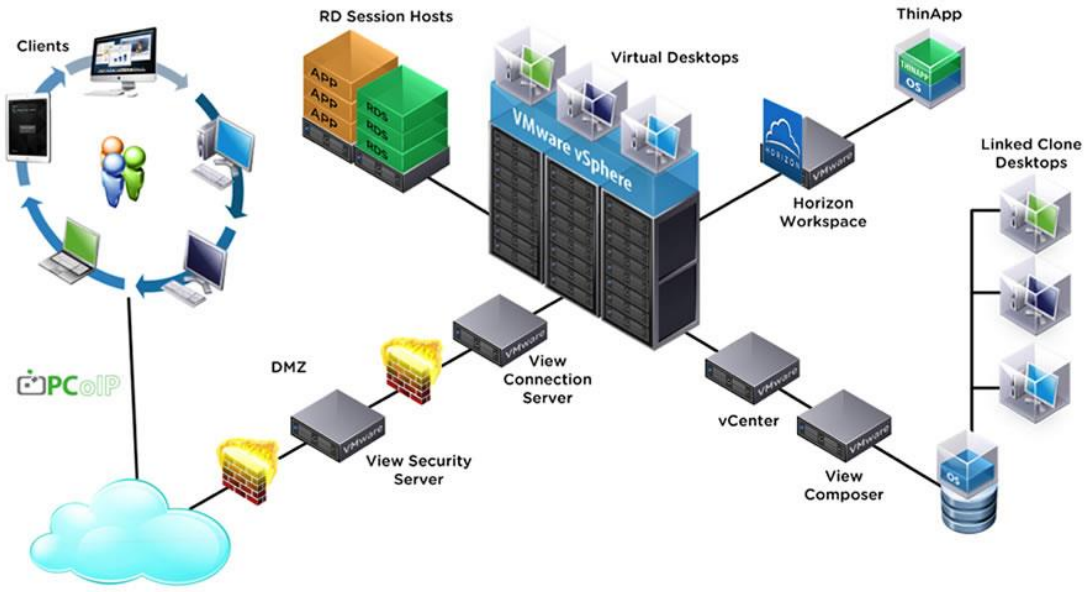


Figura 5. Virtualizacion de Escritorio
Fuente. http://www.vsolutionsvs.com/site/index.php/soluciones/virtualizacion-de-escritorios

2.2.6. VIRTUALIZACIÓN DE REDES (NETWORK)

Este método se refiere a fusionar los recursos entre el software y hardware y funcionalidades de red de datos en una sola identidad establecida en software, siendo nombrada como una red virtual. Al realizar la implementación facilita y provee el asunto de gestión, ofreciendo a los administradores de red en conservar un control preciso sobre los recursos de la red que gestiona.

Las VLANs permiten a los encargados de gestionar la red acoplar elementos de redes a comodidad, proporcionando la eventualidad de inspeccionar todo lo que ocurre en la red. (Fernández & García, 2011).

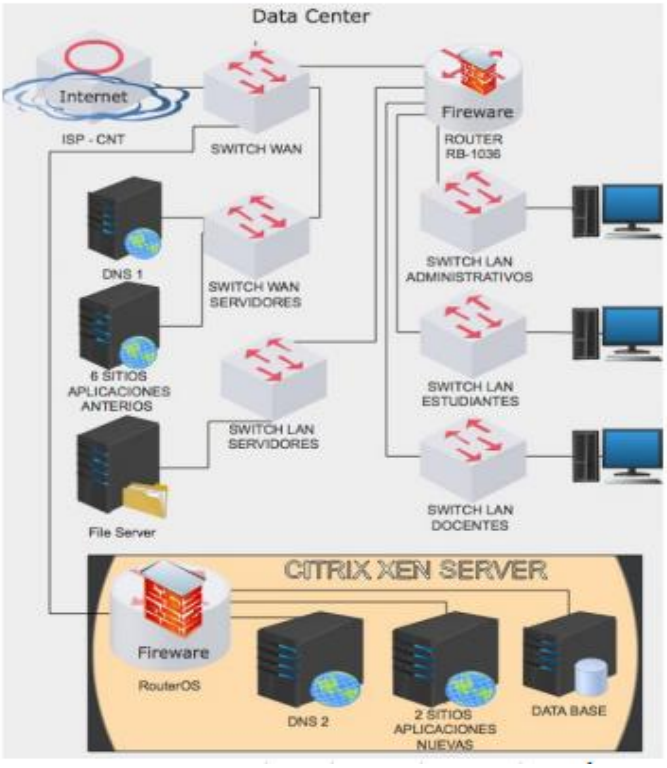


Figura 6

Fuente.Virtualizacion de redes y servidores emulando infrestructura tecnológica [Casierra Cavada, J., Quiñonez Ku, X., Herrera Izquierdo, L., Egas Acosta, C, (2018]

2.3. TIPOS DE REDES

Las redes de computadoras consiguen atender a variadas clasificaciones en ocupación de los elementos que se hayan tenido en mente, las redes de datos se especifican de esta manera:

2.3.1. SEGÚN SU EXTENSIÓN

En función del recorrido físico en la que se encuentra conectados los diferentes nodos se puede decir la siguiente clasificación:

- Red de área personal (PAN): son redes de computadoras que son utilizadas para la comunicacion entre dispositivos por ejemplo impresoras, laptop y scanner su alcance consigue llegar a 10 metros son generalmente por cable USB.

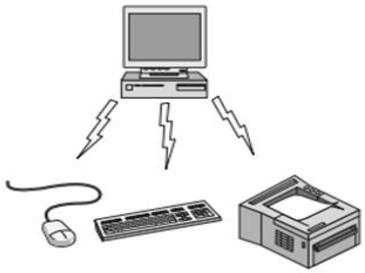


Figura 7. Red Pan

Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

- Red de área local (LAN):Esta red es de uso doméstico como una oficina o lugar de un centro comercial sirve para compartir recursos, imágenes o NAS y es un red de clase C.

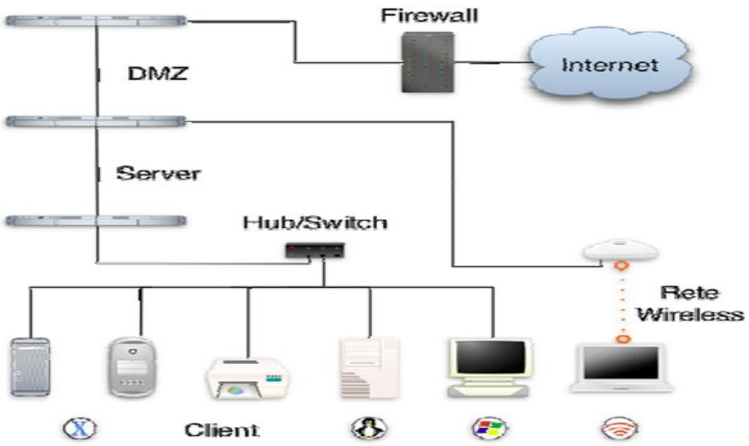


Figura 8. Red Lan

Fuente. Introduccrion a las Redes de Computadores [Alvarez & Monsalve, 2008]

- Red de área metropolitana (MAN): Tiene como objetivo en ofrecer una cobertura de internet geográfica a través de fibra óptica este ejemplo de red logra ser privada o pública igualmente cuenta una banda ancha extensa y su alcance es máximo de 50 km.

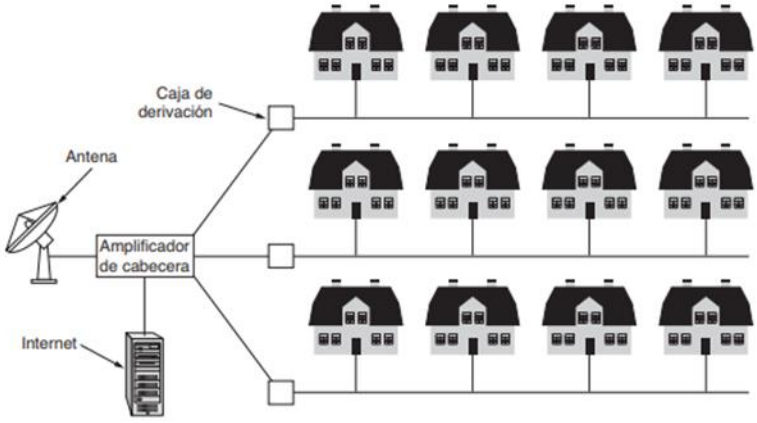


Figura 9. Red Metropolitana
Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

- Red de área extensa (WAN): Enlaza ciudades y países alrededor del planeta entre sí. Regularmente son implantadas por las empresas de servicios de Internet (ISP). (Castaño & López, 2013).

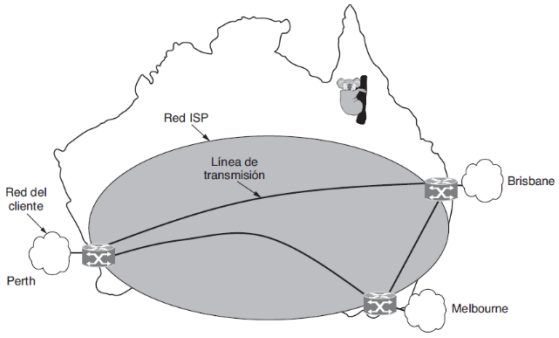


Figura 10. Red Wan
Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

2.3.2. SEGÚN SU TOPOLOGÍA

Constan dos diferentes ejemplos de topología:

- Topología física: Representa la red de datos en los medios de transmisión.
- Topología lógica: Se específica cómo se conecta las computadoras a la red de datos.

- **Topología física de la red**

Las topologías físicas de redes de datos más manejadas son:

- Topología de bus: Esta topología tiene como fin usar un único segmento de cable permitiendo que todos los equipos se acoplen de manera inmediata.

Figura 11. Topologia en Bus
Fuente. Teccnologia de la información [Daniel Kohen, Enrique Asin]

- Topología de anillo: Domina una sola conexión de entrada y salida una de sus desventajas es que posee una trasmisión más lenta que las otras topologías.

Figura 12.Topologia en Anillo
Fuente. Teccnologia de la información [Daniel Kohen, Enrique Asin]

- Topología de estrella: Cada computadora va conectada a cada puerto del dispositivo central de concentración por lo habitual puede ser un hub o un switch.

Figura 13. Topología en Estrella

Fuente. Tecnología de la información [Daniel Kohen, Enrique Asin]

- Topología jerárquica: Una red jerárquica agrupa las características de una red estrella extendida.

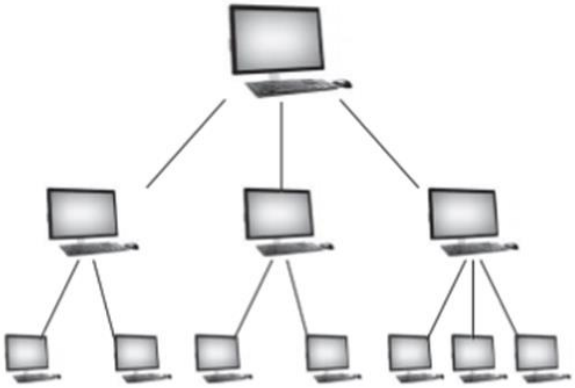


Figura 14. Topología Jerárquica
Fuente. Tecnología de la información [Daniel Kohen, Enrique Asin]

- Topología de malla: Esta topología surge en encaminar los datos y voz no requiere de un servidor central o nodo. (Castaño & López, 2013).

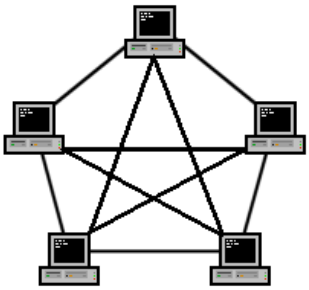


Figura 15. Topología de Malla
Fuente. https://sites.google.com/site/topologiasdered708/home/topologia-de-red-de-maya

Topología lógica de la red

La topología de la red lógica se detalla en la manera que las computadoras y dispositivos se participan internamente en la red de datos. (Castaño & López, 2013).

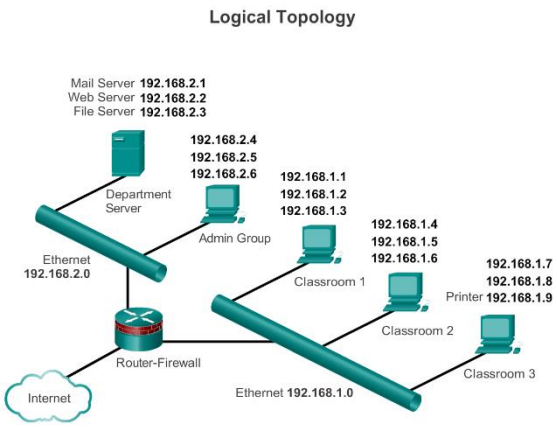


Figura 16. Topologia de red lógica
Fuente. Cisco CCNA v5

2.3.3. SEGÚN EL TIPO DE ACCESO A LA RED

Los dispositivos, servidores y computadoras de una red de datos se enlazan con otras redes usando una dirección IP. Se especifican de la siguiente forma:

- Red pública: Enlazan una red de datos usando una dirección IP única que les ortoga su distribuidor de servicio para internet (ISP).(Castaño & López, 2013).

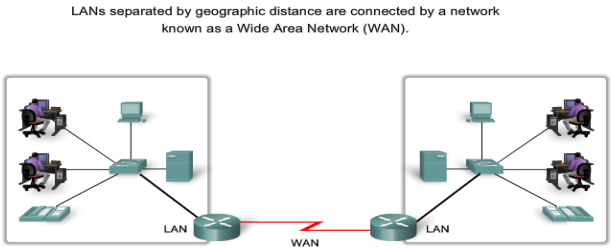


Figura 17. Red pública
Fuente. Cisco CCNA v5

- Red privada: Es una red que usa direcciones IP privadas de clase C y debe ser nateada y enmascarada con la red pública para lograr tener acceso a internet.

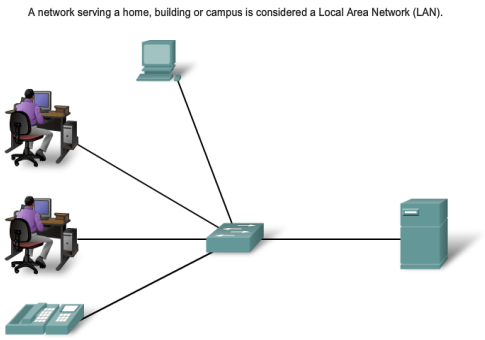


Figura 18. Red privada
Fuente. Cisco CCNA v5

2.3.4. SEGÚN EL MEDIO DE TRANSMISIÓN

El canal maneja una red de datos o de voz para transmitir y recibir información, y se pueda formar la sucesiva clasificación:

- Red cableada: Las computadoras o servidores se enlazan a la red a través de un cable de red o patchcord. Este cable de red puede ser de diferentes tipos según la velocidad de la NIC.

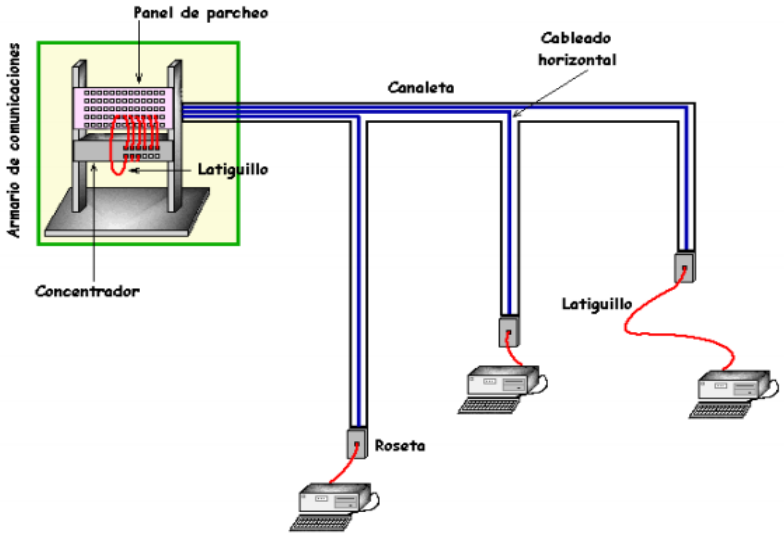


Figura 19. Red cableda
Fuente.Universidad de Cadiz, Facultad de ciencia sociales y de la comunicacion, Redes de datos [M Fernandez]

- Red inalámbrica: comunica y toma información a través de transmisiones electromagnéticas. Las ondas son enviadas y recibidas a través de las antenas que tienen los ordenadores y como los celulares o laptop que se conectan a la red WIFI. (Castaño & López, 2013).

Figura 20. Red inalambrica
Fuente.Universidad de Cadiz, Facultad de ciencia sociales y de la comunicacion, Redes de datos

2.4. DISPOSITIVOS DE INTERCONEXIÓN DE REDES

Sirven para comunicar los equipos terminales y la conexión que va a Internet conoceremos diferentes dispositivo mencionados en la vida cotidiana que son los siguientes:

- Concentradores o hubs: sirven para restablecer el pulso eléctrico de transmisión cada cierto tiempo, por que la señal va sufriendo perdidas en una determinada distancia.

Figura 21. HUB
Fuente.Redes Locales. Alfredo Abad Domingo

- Conmutadores o switches: es un dispositivo que logra fraccionar la red en múltiples segmentos dependiéndo la cantidad de puertos que posea el switch alcanzando que nunca se produzca una colisión en el envío de paquetes.

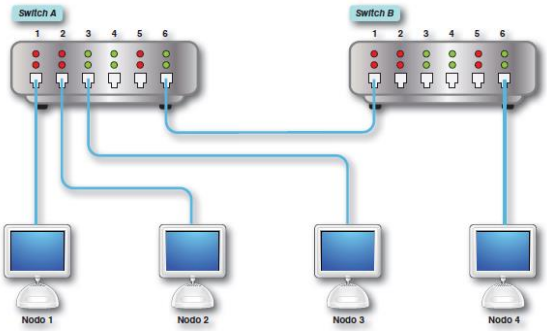


Figura 22. Conmutadores o switches
Fuente.Redes Locales. Alfredo Abad Domingo

- Enrutadores o routers: son utilizados para enviar y recibir el tráfico de la red. Se aprovecha cuando queremos acoplar diferentes LAN a través de enrutamiento estáticos o dinámicos.

Figura 23. Enrutadores o routers
Fuente.Redes Locales. Alfredo Abad Domingo

- Cortafuegos o firewall: es un dispositivo que tiene como función gestionar y administar la seguridad de la red a través de reglas que son declaras en el equipo.

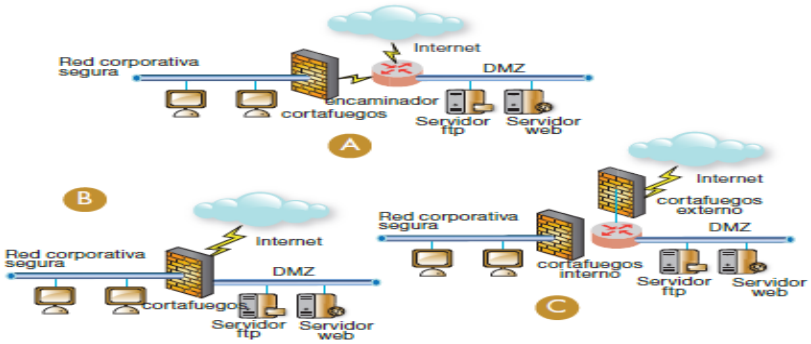


Figura 24. Enrutadores o routers
Fuente.Redes Locales. Alfredo Abad Domingo

- Módem: es un aparato usado para transmitir señales de datos por medio de cables de teléfono.

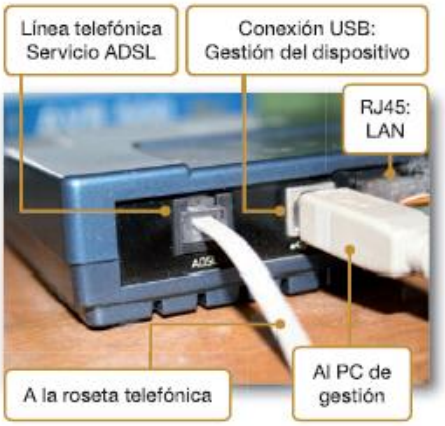


Figura 25. Módem
Fuente.Redes Locales. Alfredo Abad Domingo

- Cable módem: es similar al módem, pero remite datos por medio de patchcord de coaxial. También logra trasladar señales de televisión. (Castaño & López, 2013).

Figura 26. Cable módem
Fuente.Redes Locales. Alfredo Abad Domingo

2.5. CABLEADO ESTRUCTURADO

El estándar de cableado estructurado nos describe cómo podemos realizar un montaje del cableado de comunicaciones en instituciones públicas, instituciones privadas u edificios . El estándar explica de forma breve los diferentes tipos de cables utp que se vayan a manejar, terminales, distancias máximas,distribución de elementos de interconexión, se debe seleccionar el tipo de cable dependiendo la instalación que se vaya a realizar. (Bellido ,2013).

2.5.1. CONJUNTO DE CABLEADO ESTRUCTURADO

La agrupación del cableado estructurado debe estar constituido en distintas partes, cada uno contiene un subsistema. Son los siguientes:

- Cableado de campus: Interconecta los distintos edificios de una organización o institución. Se sugiere utilizar fibra óptica para no tener pérdida de paquetes.

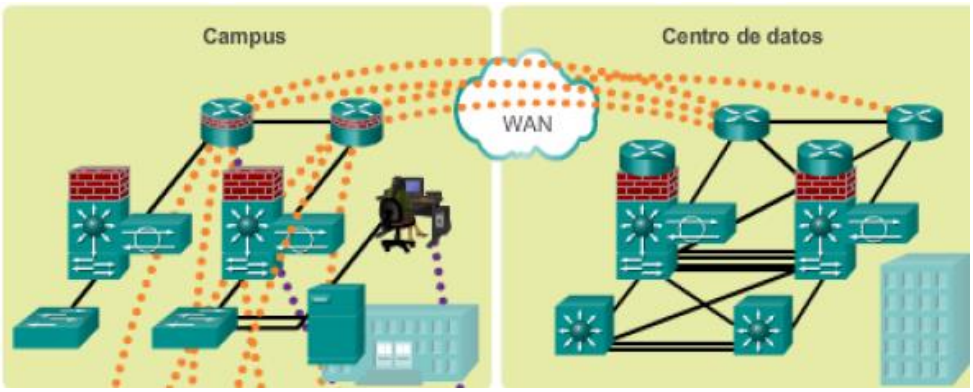


Figura 27. Cableado Campus
Fuente.Cisco CNNA v5

- Sala de equipamiento: Lugar en el que coinciden todas las conexiones y enlaces del edificio.

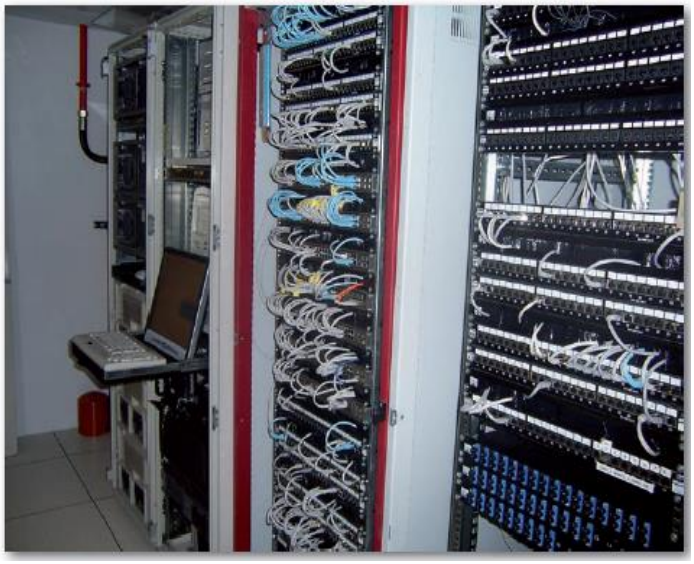


Figura 28. Sala de Equipamiento
Fuente.Redes Locales. Alfredo Abad Domingo

- Cableado troncal: Este se encarga de llevar a cabo todas las conexiones través del cableado vertical. (Molina, 2014).

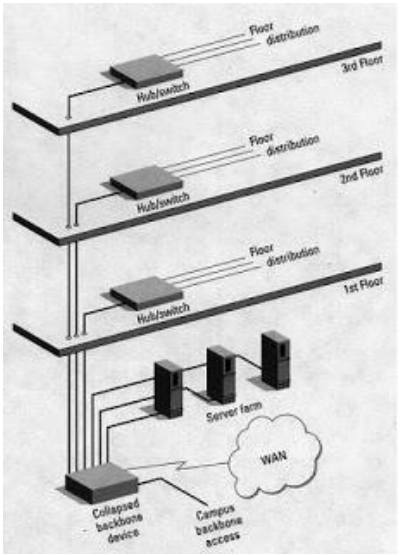


Figura 29. Cableado Troncal
Fuente. https://sites.google.com/site/stigestionydesarrollo/recuperacion/desarrollo-1/tema10/3

- Sala de Telecomunicaciones: Es una espacio centralizado adentro de una institución, colegio o edificio que alberga los dispositivos del sistema de cableado de telecomunicaciones.

Figura 30. Sala de Equipamiento
Fuente.Redes Locales. Alfredo Abad Domingo

- Cableado horizontal: Proviene desde las conexiones de pared llamadas rosetas o faceplate por los caneles telecomunicacionesde hasta los rack de comunicaciones.

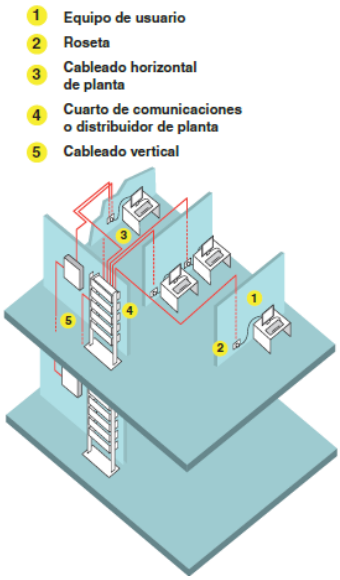


Figura 31. Cableado Horizontal
Fuente.Redes Locales. Alfredo Abad Domingo

- Área de trabajo: Se llama área de trabajo al lugar donde se encuentra una sala de telecomunicaciones que proporciona o ofrece un determinado servicio. (Bellido ,2013).

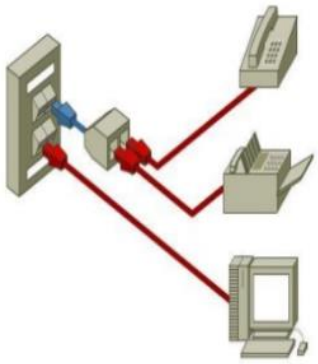


Figura 32. Área de trabajo
Fuente. https://es.slideshare.net/lismark93/cableado-estructurado-36423999

2.5.2 ESTÁNDARES DE CABLE UTP/STP

El siguiente estándar ANSI/EIA/TIA-568 queda separado en diferentes procesos técnicos que constituyen los elementos de transmisión. Estos son:

- TSB36: Detalla el uso del cableado de par trenzado.
- TSB40: Define la querencia del conector RJ-45 y los procesos que se ejecutan en los empalmes de cableado.
- TSB53: Describe el manejo de cableado de par trenzado apantallado.

Los estándares de cableado estructurado ANSI/EIA/TIA 568 e ISO/IEC 11808:2002 aceptan diferentes tipos de cableado: UTP/FTP para las instalaciones de cobre y cable multimodo (50/125 µ m o 62.5/125 µ m) y monomodo para las instalaciones de fibra óptica. En el caso del cable trenzado de cobre, las diferentes calidades existentes, es decir, la categoría (según ANSI/EIA/TIA-568) o clase (según ISO/IEC 11801), determinarán la rapidez máxima de entrega y el trayecto máximo entre las conexiones. La categoría del cable depende de la cantidad de trenzado por metro (cuanto mayor es este valor, mayor es su inmunidad al ruido) y la existencia o no de una pantalla protectora. (Molina, 2014).

2.5.3 TIPOS DE CABLES

El par trenzado es un cable muy manejado en pequeñas y grandes instalaciones. Su uso es debido a su facilidad de instalación, su reducido coste y su buen rendimiento, además de que se trata de una tecnología muy desarrollada actualmente. El cableado de par trenzado está disponible en varias versiones.

- Par trenzado no apantallado (UTP): este cableado dispone de una mayor flexibilidad, por lo que suele instalarse como latiguillos en los paneles de parcheo y las conexiones del área de trabajo entre los enchufes de pared y los equipos, donde además su longitud suele ser bastante reducida. Tiene una impedancia característica de 100 Ω y está formado por cuatro pares: blanco-azul y azul, blanco-naranja y naranja, blanco-verde y verde, y blanco-marrón y marrón.

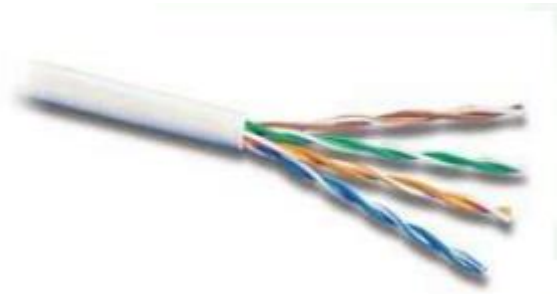


Figura 33. Par tranzado no apantallado
Fuente.
http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/recursos/tiposcablesRed.pdf?i=1

- Par trenzado apantallado (STP, S/STP, FTP, S/FTP o S/UTP): este tipo de cable está formado por cuatro pares apantallados par a par o globalmente por una malla conductora. Debido a su pantalla, se trata de un cable más rígido y de mayor coste, pero permite una mayor protección frente a interferencias. Tiene una impedancia característica de 150 Ω y su espesor no es significativamente superior que el cable no apantallado.

Figura 34. Par tranzado apantallado
Fuente.
http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/recursos/tiposcablesRed.pdf?i=1

- Cable multipar: Se trata de un cable de par trenzado que puede ir apantallado o no y que incluye una gran cantidad de pares. En los estándares de cableado estructurado aparece normalmente definido por 25 pares. Hay que tener en cuenta que en este tipo de cable no deben circular señales incompatibles que puedan producir diafonía.

Figura 35. Cable multipar
Fuente.
http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/recursos/tiposcablesRed.pdf?i=1

Los cables de par trenzado, al igual que otros cables de cobre, están caracterizados por el diámetro del núcleo conductor. Cuanto mayor es este diámetro, mayor grosor tendrá el cable y menor resistencia tendrá al paso de la corriente eléctrica. Esto quiere decir que un cable de cobre de mayor grosor tendrá unas características de atenuación mejores con respecto a cables de menor grosor, por lo que serán capaces de cubrir distancias más largas. La mayoría de los fabricantes utilizan la medida del AWG (American Wire Gauge o Calibre del Cable Americano) para indicar el grosor del cable. El valor más común para el par trenzado es 24 AWG, que se corresponde con un diámetro del cobre de 1/24 de pulgada. El valor del AWG puede variar en los cables trenzados actuales de 9 a 26 AWG.

2.6. TIPOS DE SOFTWARE PARA EMULAR REDES INFORMÁTICAS

Existen diferentes software para emular redes informáticas se nombran las mas usadas por los usuarios son las siguientes:

- Cisco Packet Tracer
- GNS3
- NetSim

- CISCO PACKET TRACER.- Es una herramienta desarrollada por Cisco sirve para emular redes informáticas, donde ellos ofrecen en su software routers, switches de la marca y es fácil de utilizar una de sus desventajas solo se puede emular equipos CISCO.

Figura 36.. Cisco Packet Tracer
Fuente. http://net4dd.com/guia-de-implementacion-de-cisco-packet-tracer-en-windows/

- GNS3 .- Es un simulador grafico para redes informáticas de código abierto sirve para realizar una simlacion de redes informáticas complejas como se trabajaría, se comportaría la red en tiempo real una de sus ventajas se puede cargar Qemu y KVM de dififerentes fabricantes como CISCO,HP.FORTINET,SOPHOS y siendo una herramienta usada por

todos los ingenieros y personas que se van a certificar en dichos equipos.

Figura 37. GNS3

Fuente. https://www.gns3.com/

- NETSIM.- Este simulador es usado especialmente en investigación y también en desarrollos de redes y aplicaciones de defensas.

Figura 38. NETSIM
Fuente. https://www.comsnets.org/archive/2015/demos_exhibits.html

2.7. SERVIDORES

Los servidores son computadoras potentes que tienen un profundo rendimiento usadas en empresas y organizaciones ,los servidores también ofrecen servicios a varios beneficiarios clientes y servicios.

El hadware del servidor se perfecciona y logra un tiempo de contestación optimo para diversas peticiones dentro de la red de datos. Los servidores poseen distintas unidades de procesamiento central (CPU) y hilos , bastante capacidad de memorias (RAM) y diferentes unidades de almacenamiento como discos HDD y SSD de alta capacidad que admiten hallar información de forma tremendamente rápida. (Bellido ,2013).

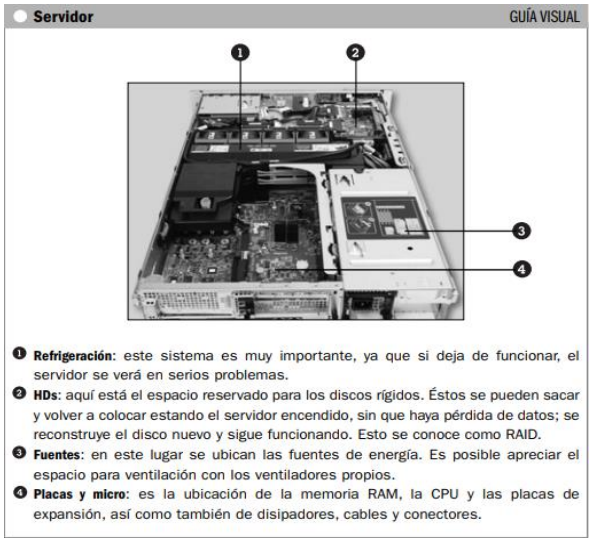


Figura 39. Parte interna de un servidor
Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

2.7.1. TIPOS DE DISEÑOS DE SERVIDORES

Constan diversos diseños de servidores como una torre independiente, estos pueden ser acoplados en bastidores, o bien, pueden poseer un diseño en blade. Estos servidores pueden tomar la función de NAS ,Streaming, servidor de datos y dispositivos para usuarios finales.(Bellido ,2013).

- Servidor Blade :Entregan la máxima concentración de potencia de computo y escalabilidad.
- Servidor acoplado en bastidor: Son excelentes para poseer mas espacios libres.
- Servidores independientes: Se usan en pequeñas empresas y proveen felixibilidad para escoger componentes internos. (Bellido ,2013).

2.7.2. SISTEMAS RAID SERVIDORES

Un array de RAID (Redundant Array of Independent Disk) esta formado por varios conjunto de discos que funcionan de manera colectiva como un único sistema de almacenamiento los sistemas RAID son los siguientes:
RAID 0. Son discos con bandas sin tolerancia al error. El nivel 0 de RAID no es redundante, así que no se incumbe puntualmente al acrónimo es fragmentada logrando un unidad de mayor volumen . (Gómez, 2014).

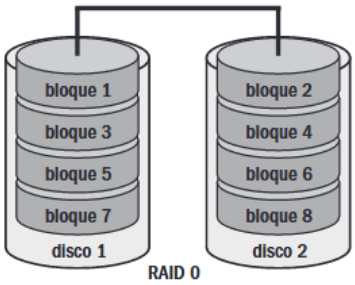


Figura 40. RAID 0
Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

- RAID 1 o disco espejo. El RAID 1 provee redundancia al plagiar todos los datos de disco a otr. El beneficio de un array 1 es un poco superior que cuando se posee una sola unidad para cumplir esta función se necesita 2 discos siempre deben ser pares.

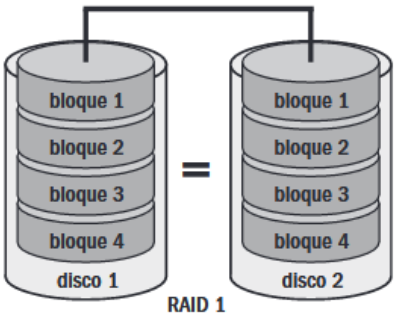


Figura 41. RAID 1
Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

- RAID 5. Para utilizar array 5 se neceita minimo 3 unidades de discos duros estos trabajan diferentes con bloques de paridad distribuidos. El RAID 5 en vez de reproducir totalmente los datos del disco duro se utilizan los bits de paridad para que en estos asunto se rompa un disco duro poder reformar la información del mismo. (Gómez, 2014).

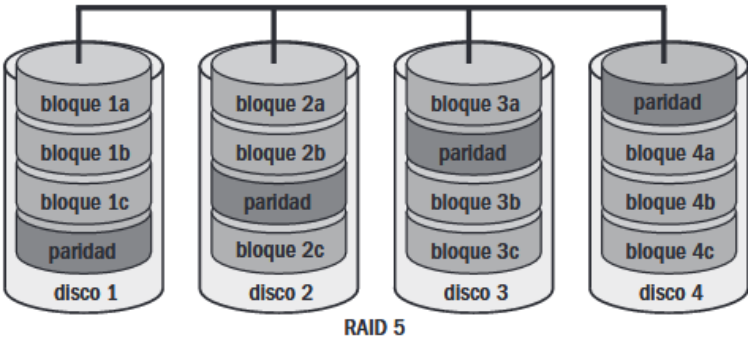


Figura 42. RAID 5
Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

2.7.3. SOFTWARE DEL SERVIDOR

Primariamente constan dos grandiosos alternativas al momento de preferir un SO: los asentados en UNIX (o su homólogo Linux) o Windows. Linux es un sistema de código abierto, Windows es un producto comercial propiedad de Microsoft la selección de estas dos alternativas no está libre de controversia. (Gómez, 2014).

Ambos sistemas operativos consiguen actuar como cliente o servidor (Gómez, 2014).

EMPRESA	SOLUCIÓN	WEB
VMware	Vsphere	**www.vmware.com/products/vsphere**
Microsoft	Hyper-V	**www.microsoft.com/hyper-v-server**
Citrix	XenServer	**www.citrix.com/xenserver**
Oracle	Oracle VM	**www.oracle.com/us/technologies/virtualization**
Oracle Solaris	Oracle Solaris Containers	**www.oracle.com/us/products/servers-storage/solaris/virtu**
Red Hat	Enterprise Virtualization	**www.latam.redhat.com/rhel/virtualization**
Parallels	Parallels Server	**www.parallels.com/virtualization/server**
Novell	Suse Linux Enterprise Server	**www.novell.com/es-es/products/server/virtualization.html**

Figura 43. Software de Virtualización
Fuente. Administrador de Servidores [Marchionni, Enzo Augusto 2011]

2.7.4. ESTRUCTURA CLIENTE/SERVIDOR

La estructura cliente/servidor está compuesta por servicios alojados en servidores y clientes que son los que realizan peticiones de servicios al servidor; para que esto sea viable, cliente y servidor tienen de estar en redes semejantes. (Carvajal,2017).

El cliente es el que establece haciendo la petición al servidor y el servidor es quien soluciona la petición una vez admitida.El servidor toma una multitud de peticiones de los clientes y éste inmediatamente las procesa. Dependiendo del número de clientes simultáneos que se vaya a atender, tendremos que seleccionar un servidor con unas características, tanto de software como de hardware. (Carvajal,2017).

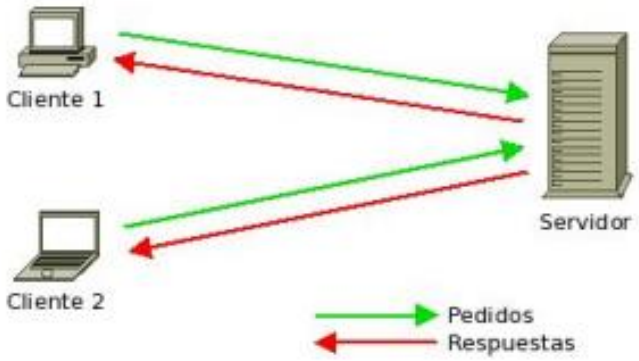


Figura 44. Modelo Cliente-Servidor
Fuente.El modelo Cliente / Servidor [E Marini 2012]

CAPÍTULO III

DISEÑO E IMPLEMENTACION DEL BANCO DE PRUEBAS

3.1. PROPOSITO DEL DISEÑO

El propósito de este diseño e implementación del banco de pruebas virtualizado se lo plasma con la finalidad de dar conocer las redes definidas por software para redes de áreas amplias para la administración de tráfico, control centralizado de la red a través de diversos enlaces, permitiendo a los estudiantes programar este de tipo de redes de comunicación sujetando tiempos de abastecimiento y restando o separando la necesidad de configurar manualmente routers o firewall habituales, optimizando la conectividad del servicio de la oficina central y la nube.

Para este diseño e implementacion del banco de prueba se utilizo la topología estrella para la comunicación de las computadoras hacia el servidor que esta conectado a un punto de red en el laboratorio de telecomunicaciones y para la simulacion de redes definidas por software se virtualizo el servidor Dell R210II con el software EXSI 6.5 UPDATE 3, se instalo GNS3 – SERVER dentro del servidor y se añadio todos los QEMU y KVM para la realización de las prácticas.

El banco de prueba o entorno virtual se diseñó para abastecer las computadoras que se encuentran en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil.

En la siguente figura se describe la topoligía de red y la conexión de comunicación del banco de prueba:

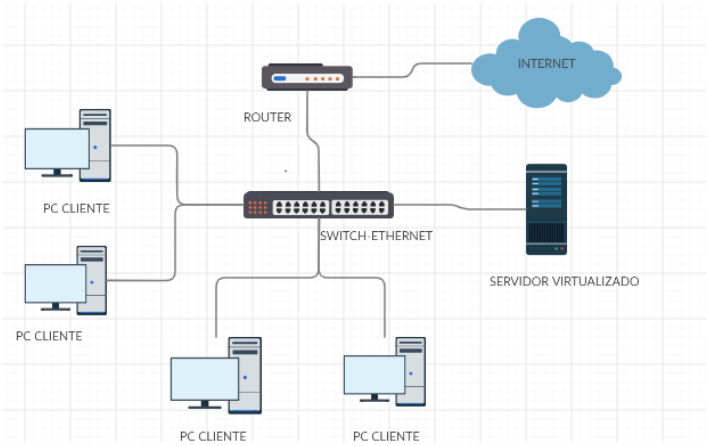


Figura 45. Diseño del banco de prueba
Fuente: Los autores

3.2. CONSTRUCCIÓN DEL BANCO DE PRUEBA

Para la parte inicial del proceso de elaboración del banco de pruebas se realizó en los siguientes pasos:

1. Proceder a desarmar el servidor Dell R210 II para mantenimiento correctivo.

Figura 46. Desmontar Dell R210 II
Fuente: Los autores

2. Limpieza del Servidor Dell R210 II.

Figura 47 Mantenimiento Correctivo Dell R210 II
Fuente: Los autores

3. Desarmar disipador y aplicar pasta térmica para la CPU del servidor Dell R210 II

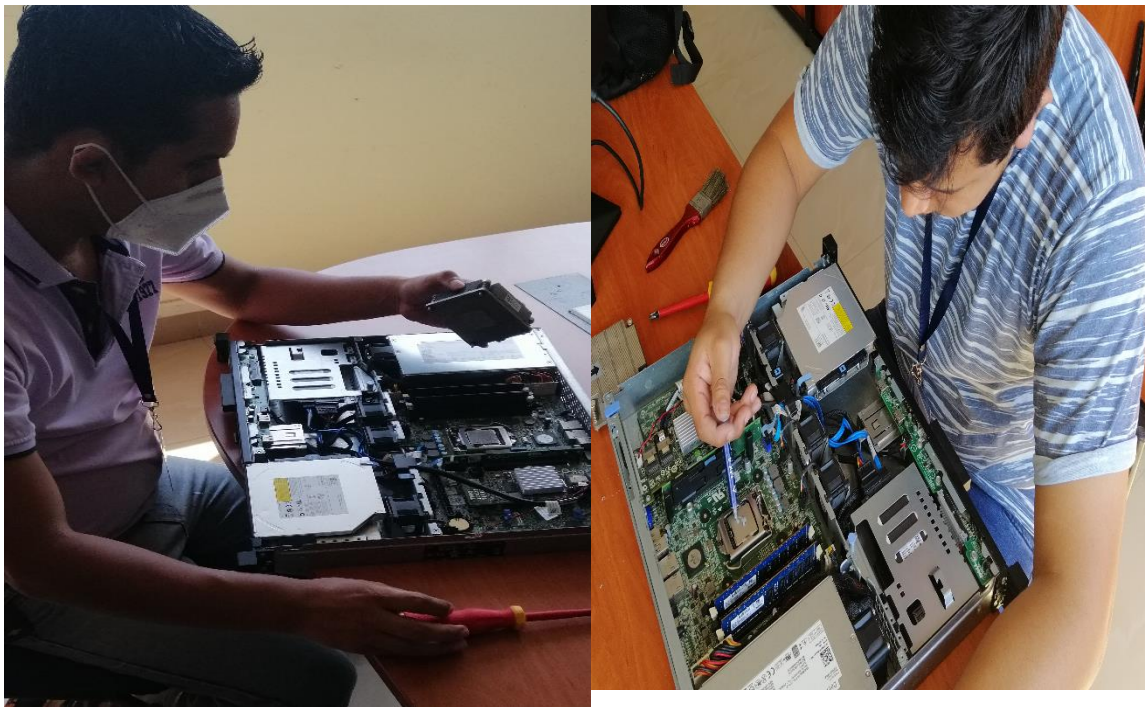


Figura 48. Desmontaje del disipador y aplicación de pasta térmica Dell R210 II
Fuente: Los autores

4. Instalación de discos duros y memorias RAM.

Figura 49. Instalación SSD Dell R210 II y memorias ram
Fuente: Los autores

3.3. CONFIGURACIÓN DE DISCO DUROS DEL SERVIDOR DELL R210 II

Para la instalación de sistemas operativos de virtualización se procedió primero a configurar los discos duro en RAID 1 y se lo detalla en los siguientes pasos.

1. Realizar la configuración de disco duros dentro del servidor Dell R210 II

   tecleamos la combinación Ctrl+C.

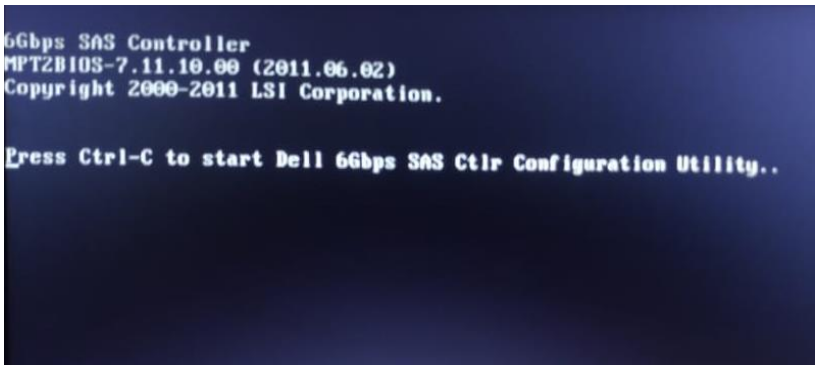


Figura 50. Configuración de los discos duros Dell R210 II
Fuente: Los autores

2. Seleccionar SAS Controller a configurar

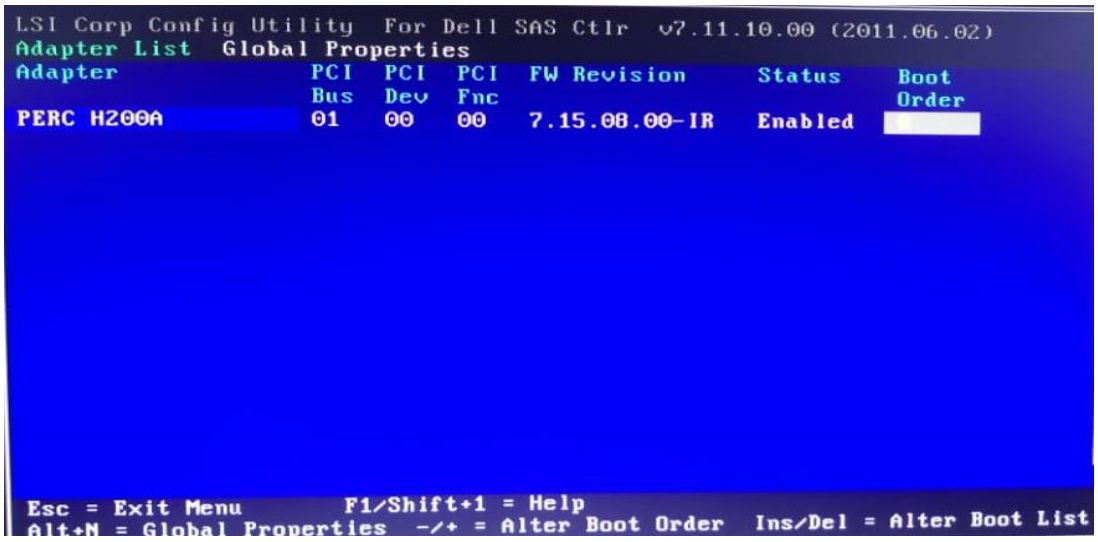


Figura 51. SAS controller PERC H200A Dell R210 II
Fuente: Los autores

3. Vamos a la opción RAID PROPERTIES.

Figura 52. Raid propiedades Dell R210 II
Fuente: Los autores

4. Seleccionar RAID 1

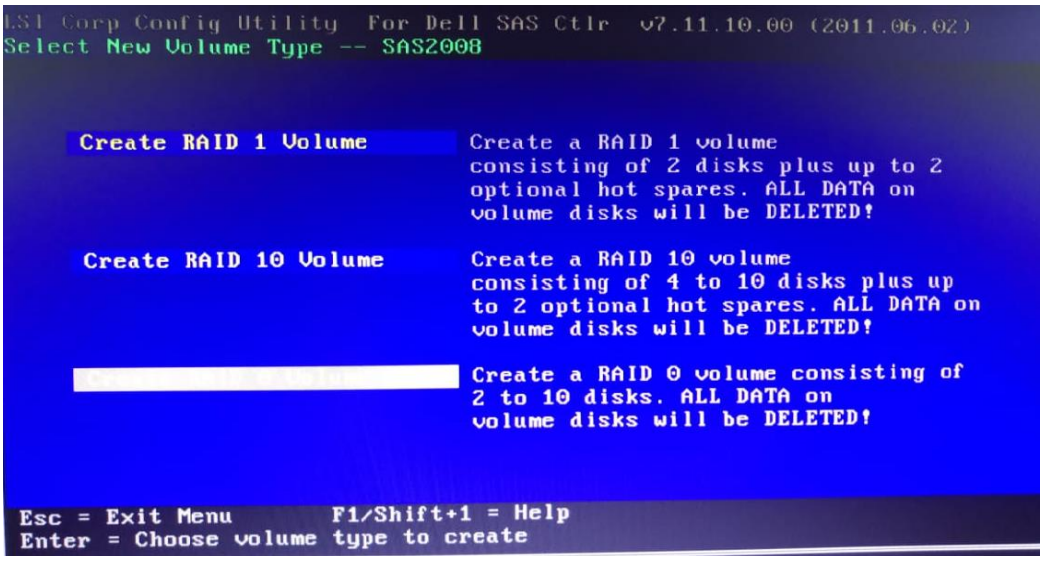


Figura 53. Selección del RAID 1 Dell R210 II
Fuente: Los autores

5. Seleccionar disco primario y disco secundario o espejo, tecleamos C para crear el volumen del RAID.

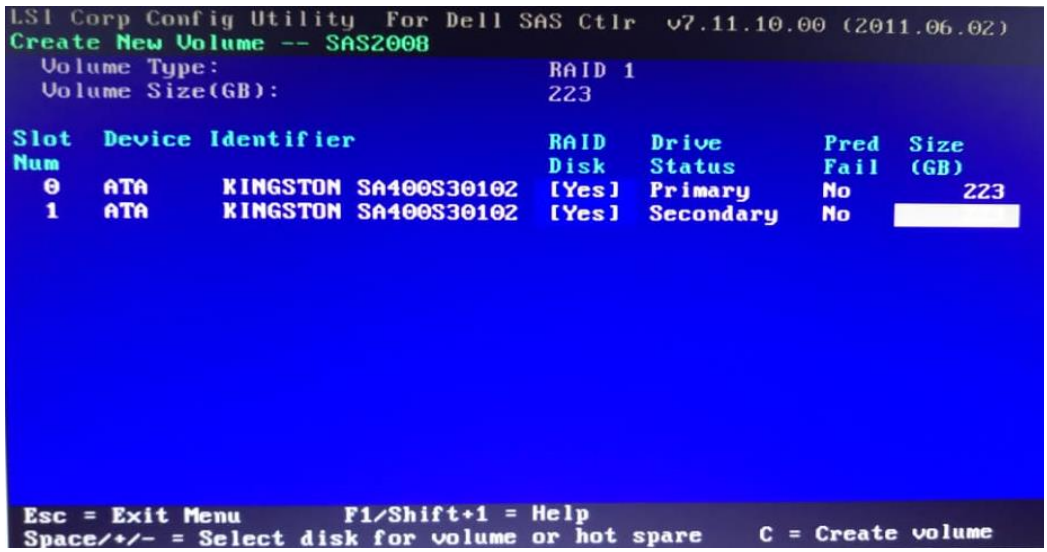


Figura 54. Selección de disco duros Dell R210 II
Fuente: Los autores

6. Creación del Volumen RAID 1

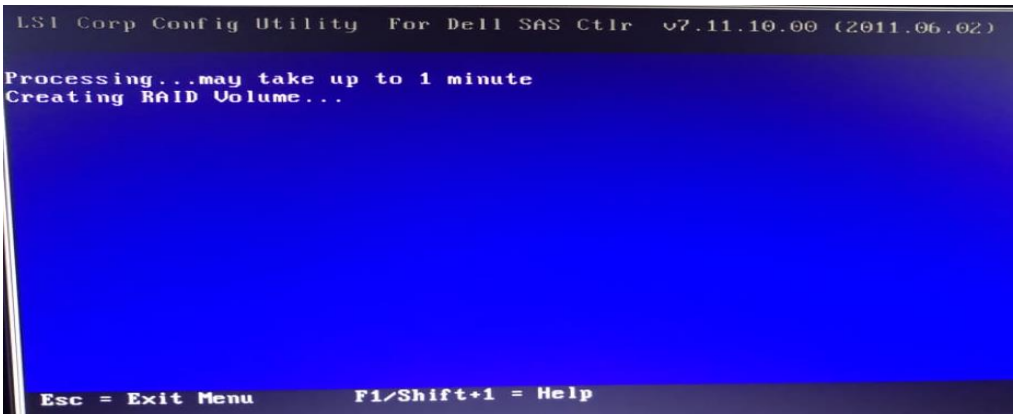


Figura 55. Selección del RAID 1 Dell R210 II
Fuente: Los autores

3.1.3. COMPARACIÓN DE LOS DIFERENTES TIPOS DE SOFTWARE PARA VIRTUALIZAR SERVIDOR

Para la virtualización de servidores tenemos varios sistemas operativos que son usados en diferentes empresas detallaremos sus características de cada uno de ellos.

Estos son los principales proveedores en el espacio de virtualización del servidor mas usados. Ver Anexo A

- VMware vSphere
- Red Hat Virtualization
- Proxmox VE
- Microsoft Hyper-V

Para la virtualización del proyecto técnico se escogio el sistema de WMware ESXi 6.5 es un sistema que permite instalar, administar y configurar maquinas virtuales que se encuentan en el servidor de forma rápida y flexible ayudando asi la incorporación de la virtualización.

3.4. INSTALACIÓN DEL SISTEMA OPERATIVO EXSI 6.5 U3 EN EL SERVIDOR DELL R210 II

La instalación del sistema operativo del servidor Dell R210 II se consideró el sistema de EXSI 6.5 U3 porque nos permite una rápida instalación y administración de las maquinas virtuales en el servidor también es un software que la mayoría de las empresas lo utilizan para gestionar sus servicios por su alta disponibilidad en producción ,se tenia previsto instalar PROXMOX un sistema operativo de código abierto para la virtualización del equipo pero presentaba el problema en cargar los archivos ova y con EXSI 6.7 U3 problemas con el CPU que no soportaba el sistema.

1. Botear el servidor con la tecla F11 Boot Manager

Figura 56. Boot Manager Dell R210 II
Fuente: Los autores

2. Seleccionar el medio de instalación del sistema CD-ROM.

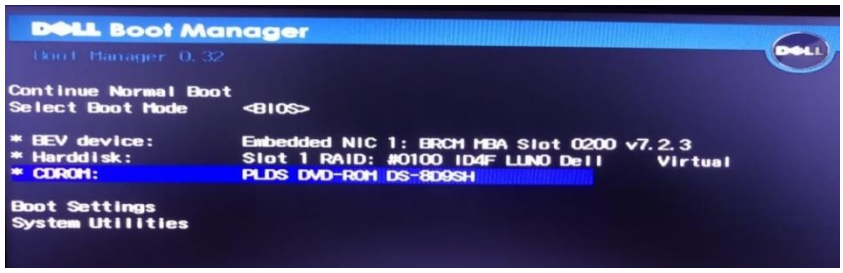


Figura 57. Boot CD-ROM 1 Dell R210 II
Fuente: Los autores

3. Seleccionar en el Boot Menu Dell EXSI 6.5.

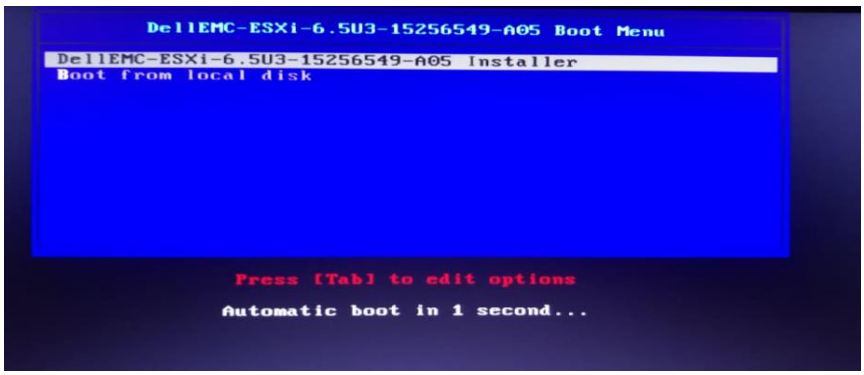


Figura 58. Boot Menu Dell R210 II
Fuente: Los autores

4. Carga del sistema operativo EXSI 6.5 U3.

Figura 59. Loading Exsi 6.5.0
Fuente: Los autores

5. Bienvenida a la instalación de EXSI 6.5 U3 en el servidor Dell R210 II.

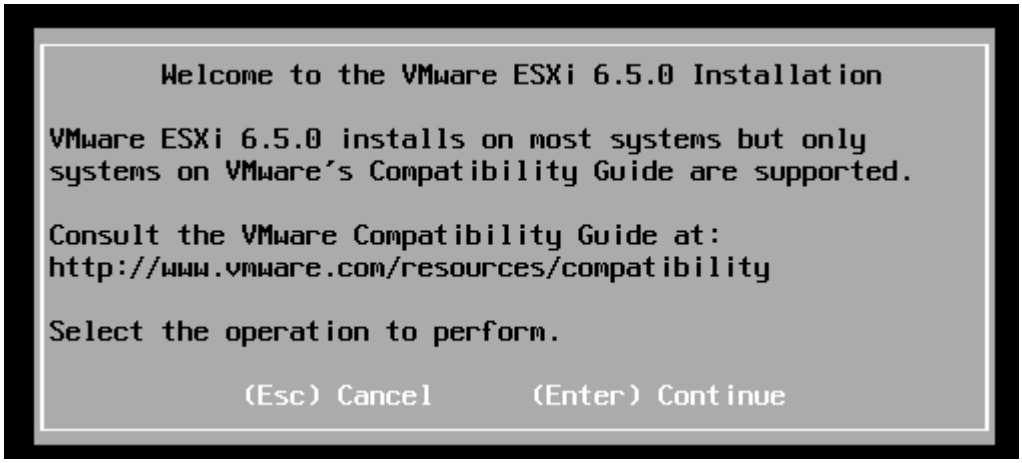


Figura 60. Welcome Exsi 6.5
Fuente: Los autores

6. Aceptación de términos y licencia EXSI 6.5 U3.

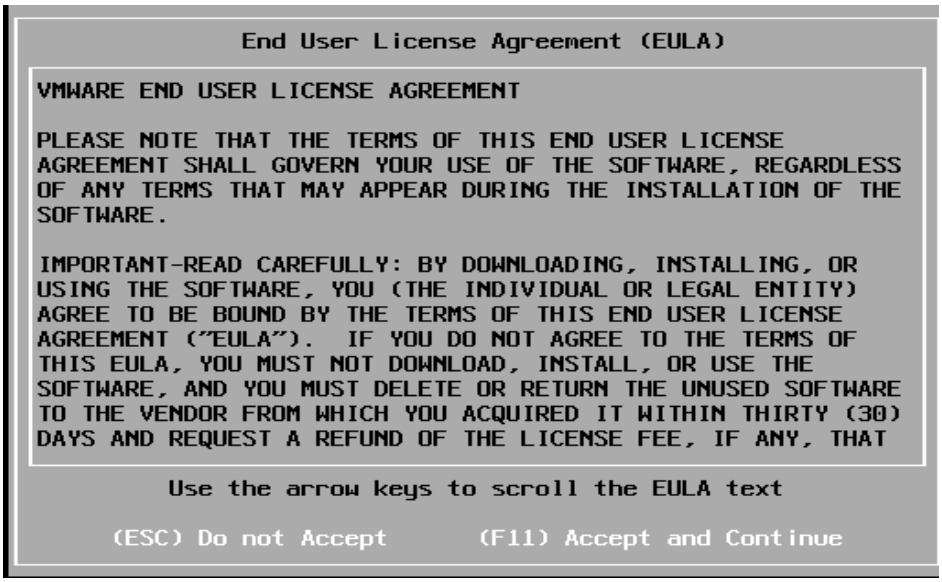


Figura 61. Términos y Condiciones Exsi 6.5
Fuente: Los autores

7. Instalación de EXSI 6.5 U3 en los discos duros del servidor Dell R210 II.

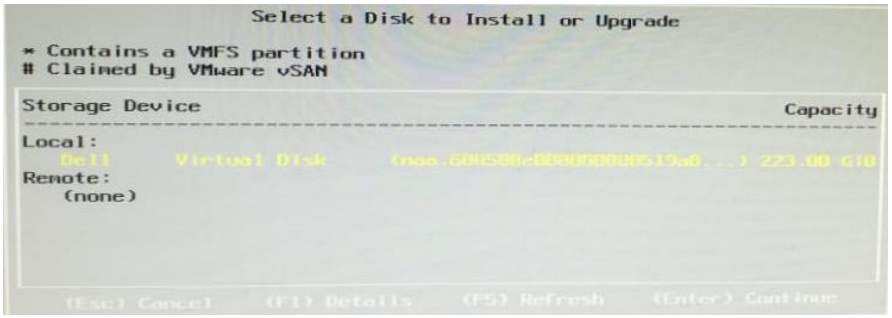


Figura 62 Instalación Exsi 6.5
Fuente: Los autores

8. Configuración de idioma del teclado.

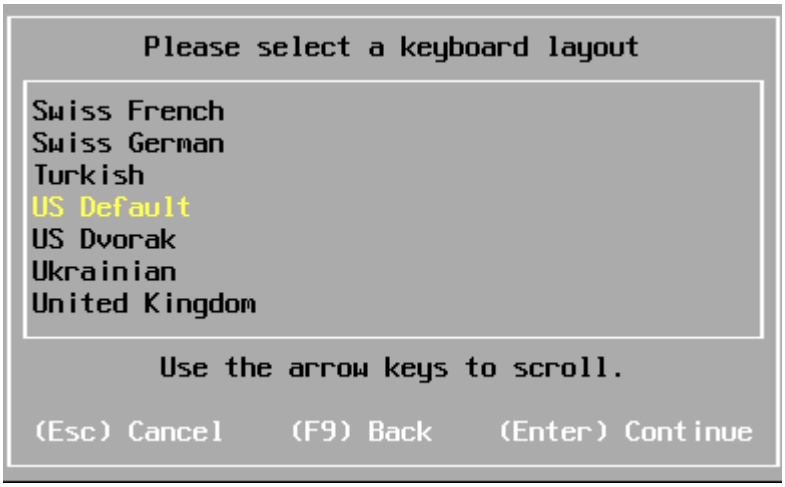


Figura 63.Configuración del idioma del teclado Exsi 6.5
Fuente: Los autores

9. Configuraciòn de contraseña del EXSI 6.5 U3.

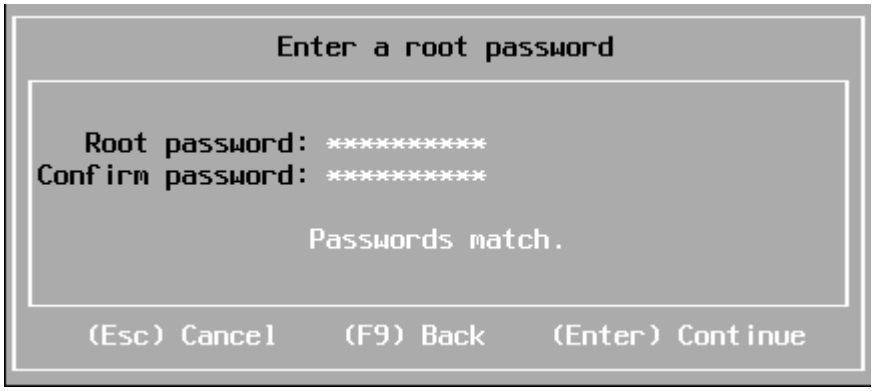


Figura 64 Contraseña del Exsi 6.5

Fuente: Los autores

10. Sistema operativo EXSI 6.5 U3 instalandose en el servidor Dell R210 II.

Figura 65.Contraseña del Exsi 6.5
Fuente: Los autores

11. Sistema operativo EXSI 6.5 U3 instalado.

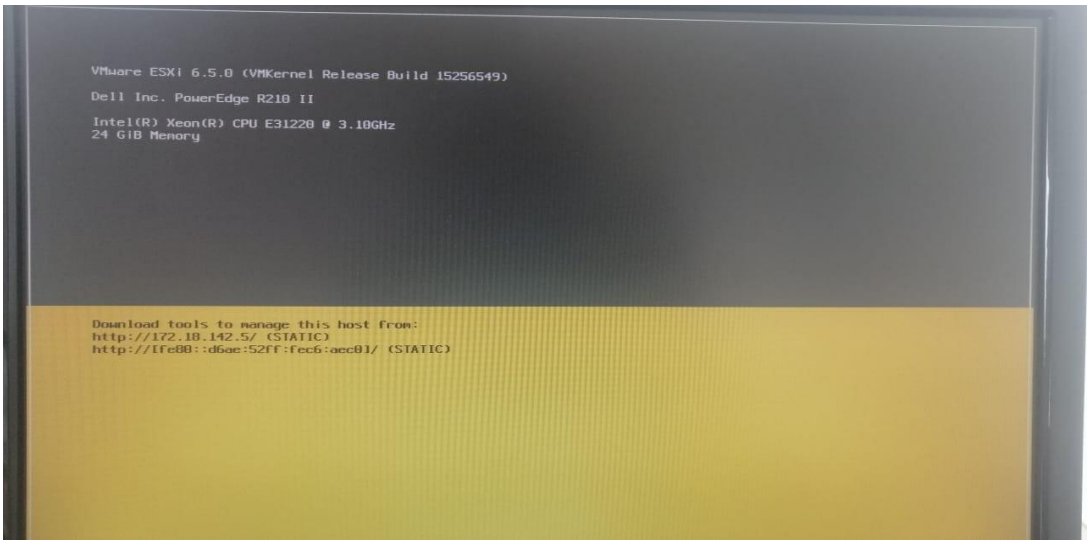


Figura 66. SO EXSI 6.5
Fuente: Los autores

12. Para acceder al modo de configuración presionamos F2 y se nos aparece el siguiente cuadro donde colocaremos las credenciales que se configuro en el proceso de instalación.

    Login name:root
    Password:Up$Gye2o2o

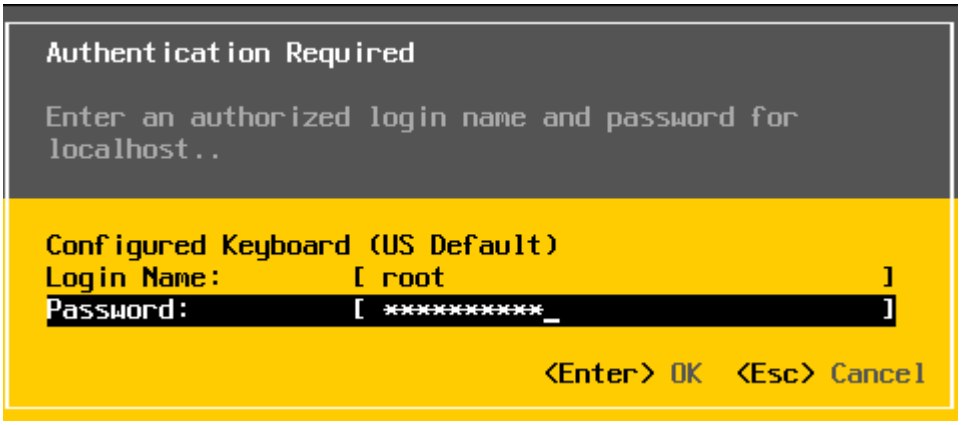


Figura 67.Autenticación del Exsi 6.5
Fuente: Los autores

13. Configuración de IP estática para el servidor Dell R210 II.

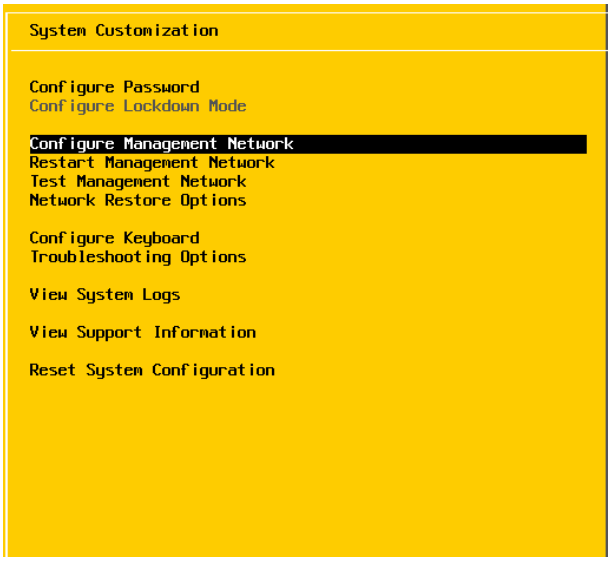


Figura 68.Configure Network Exsi 6.5
Fuente: Los autores

13.1. Seleccionar IPv4 Configuración.

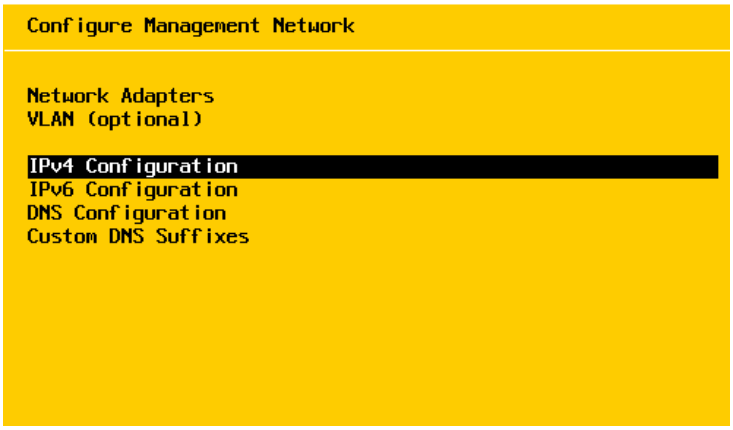


Figura 69.Configurar ipv4
Fuente: Los autores

13.1.2 Asignar la siguiente IP de manera estática al servidor 172.18.142.5/24, no se añade ninguna IP al Gateway porque no se requiere salida a internet el servidor

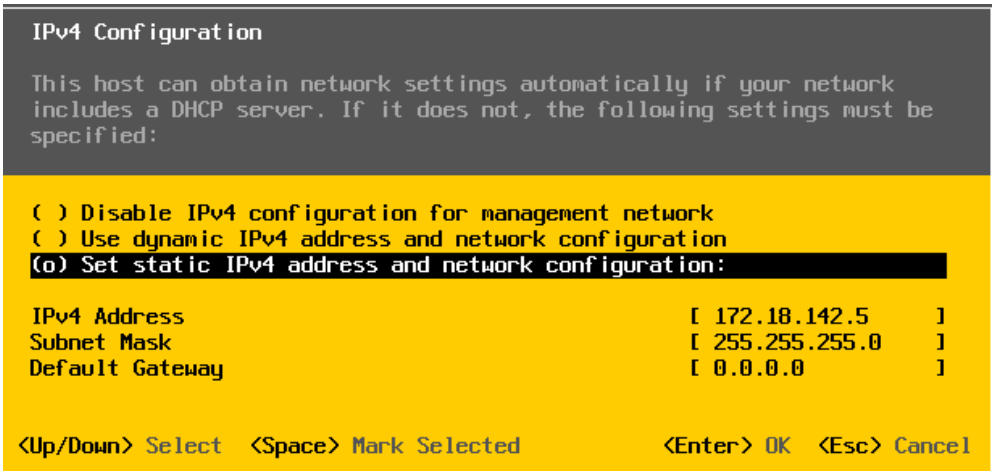


Figura 70. Configurar IP estática
Fuente: Los autores

13.1.3 Aceptar cambios de configuración.

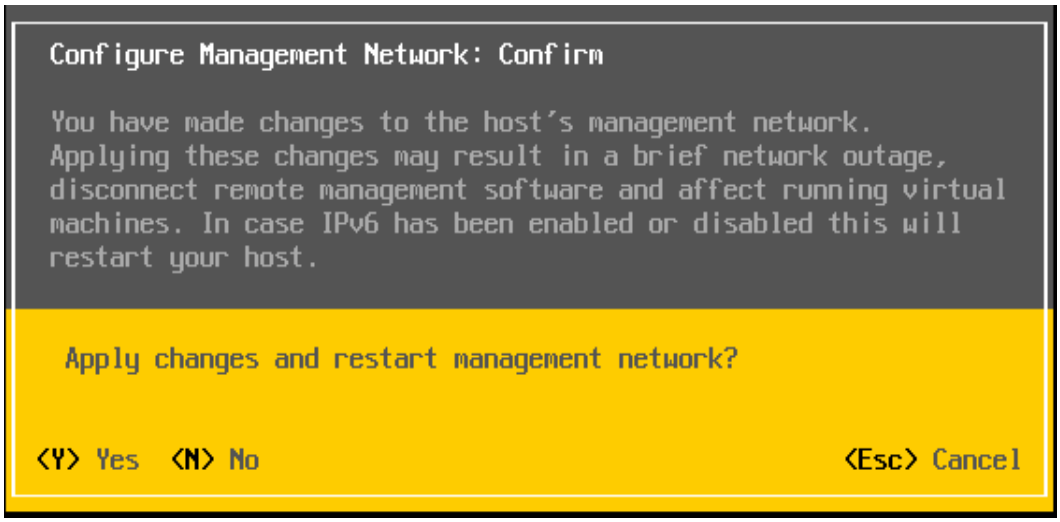


Figura 71. Confirmación de cambios en la tarjeta de red
Fuente: Los autores

3.5. CONFIGURACIÓN DE GNS3-SERVER EN EL SERVIDOR

1. Para la instalación de GNS3 SERVER se procede la descarga en la siguiente dirección https://www.gns3.com/software/download-vm y se seleccionamos GNS3 EXSI.

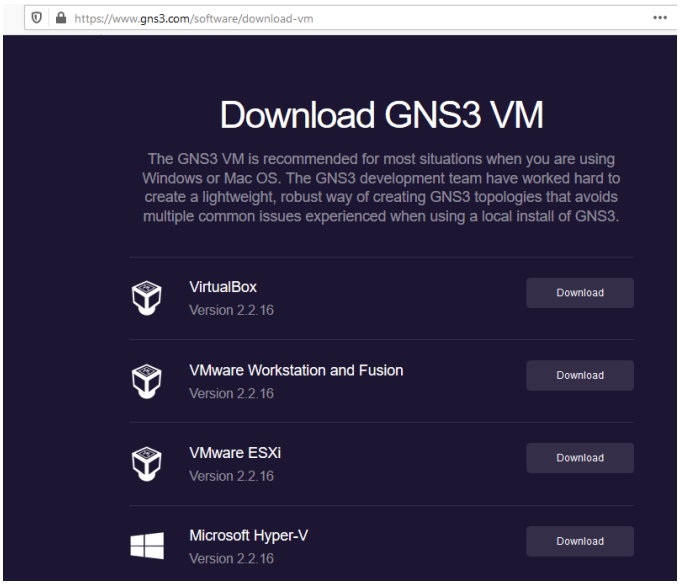


Figura 72.Descarga VMware ESXi 2.2.16
Fuente: Los autores

2. Descomprimir el archivo GNS3.VM.VMware.ESXI.2.2.16

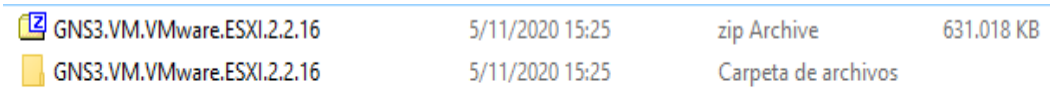


Figura 73. Descomprimir archivo zip Exsi 2.2.16
Fuente: Los autores

3. Entrar al browser y ingresamos al servidor exsi con la dirección ip 172.18.142.5, las credenciales administrativas son:

Nombre del usuario: root
Password: Up$Gye2o2o

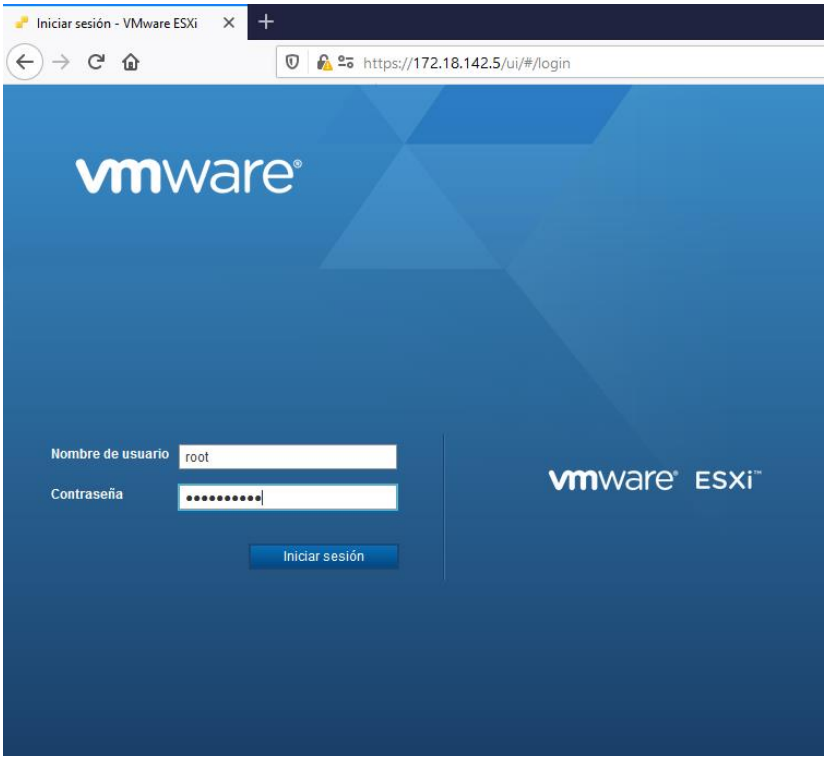


Figura 74.Login Exsi 6.5 Browser
Fuente: Los autores

4. Ingresamos al sistema de administración para escoger la opción de máquinas virtuales.

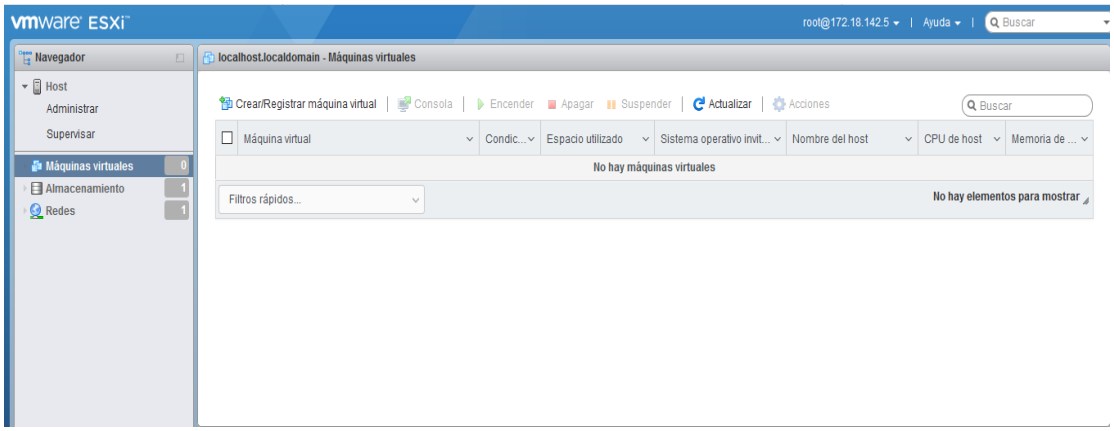


Figura 75.Máquina Virtual Exsi 6.5
Fuente: Los autores

5. Damos clic en crear/registrar máquina virtual y se nos muestra la siguiente ventana, se selecciona implementar una maquinar virtual a partir de un archivo existente OVF u OVA.

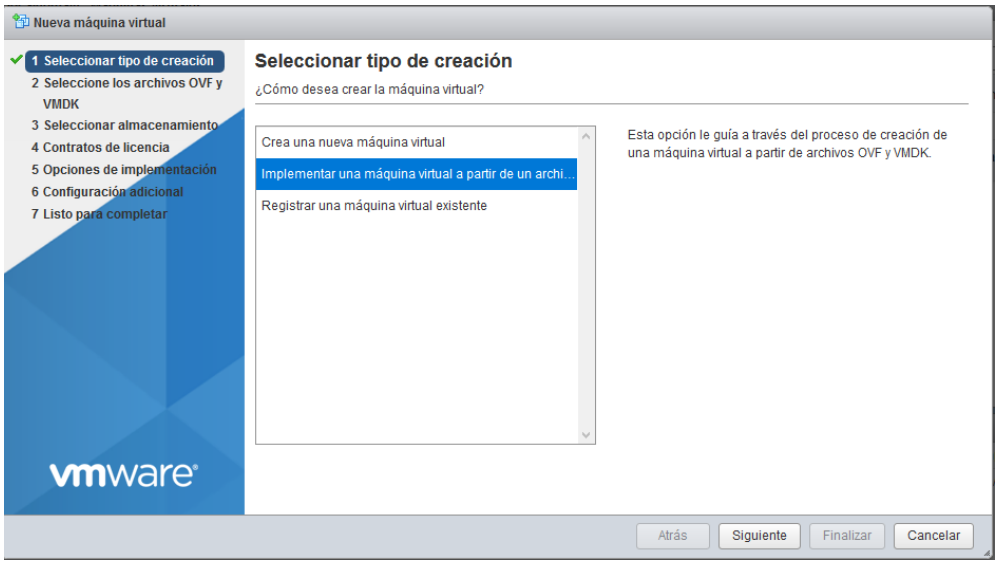


Figura 76.Creación de la máquina virtual
Fuente: Los autores

6. Introducir el nombre de la máquina virtual y seleccionamos el archivo OVF descargado.

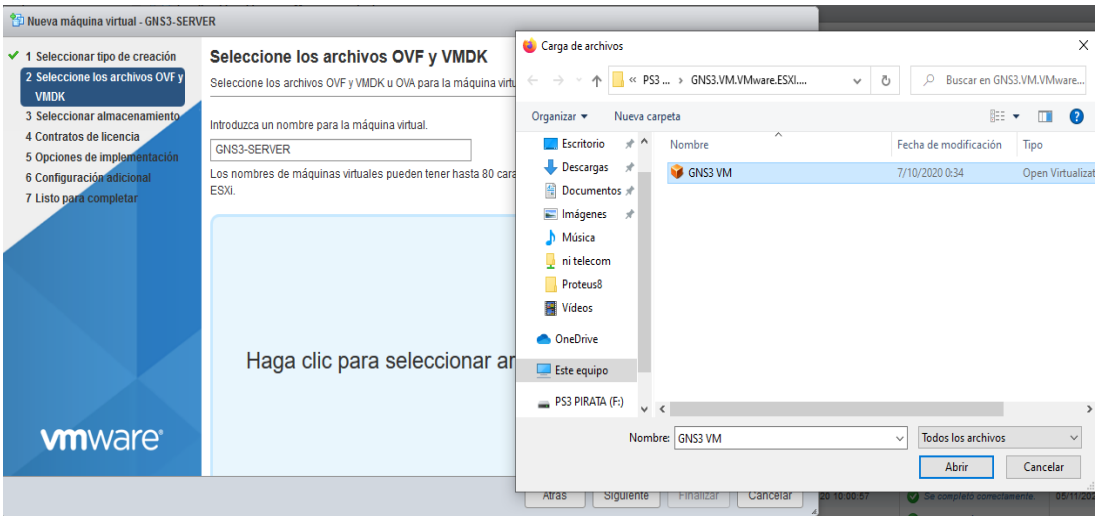


Figura 77.Instalación de la máquina Virutal
Fuente: Los autores

7. Seleccionar el almacenamiento donde se va alojar la máquina en nuestro servidor.

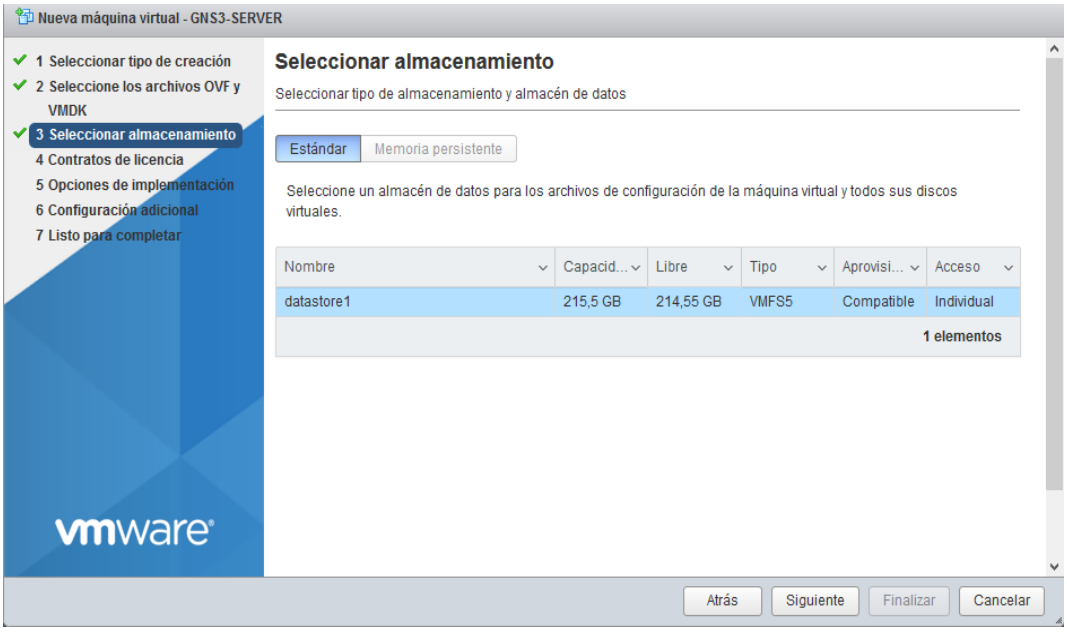


Figura 78.Selección de almacenamiento
Fuente: Los autores

8. Seleccionar la opción aprovisionamiento fino.

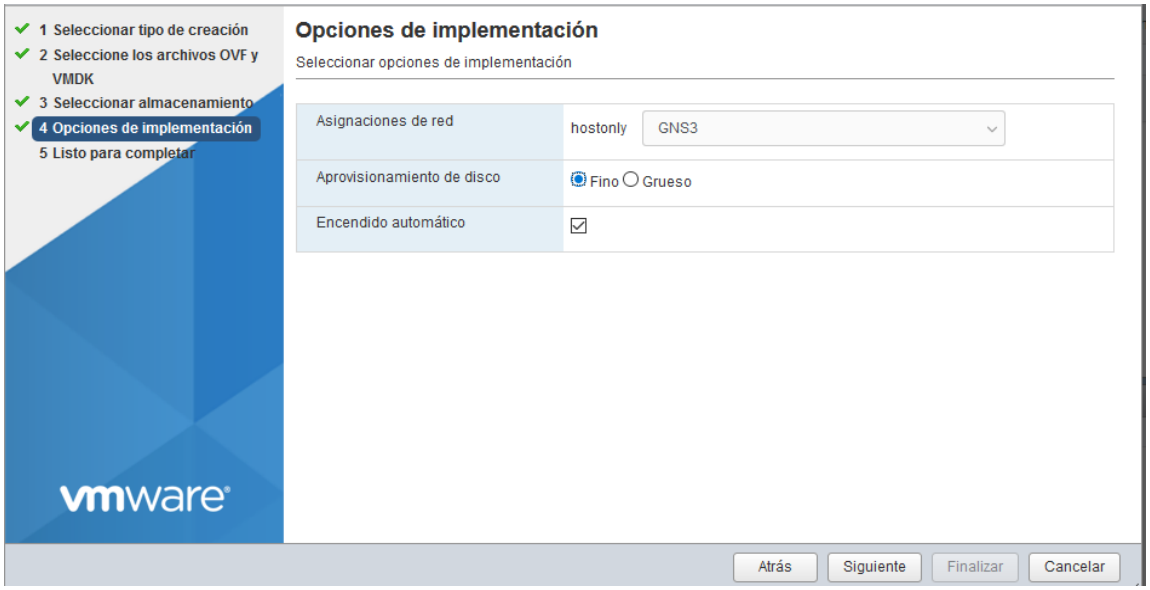


Figura 79.Aprovisionamiento fino máquina virtual
Fuente: Los autores

9. Esperar que se cargue la implementación de la máquina virtual.

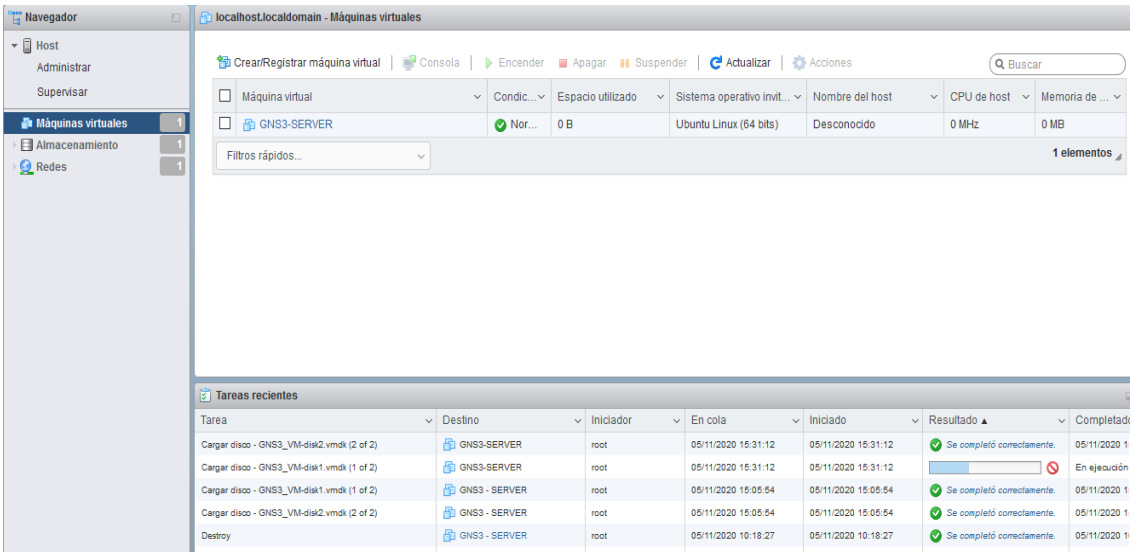


Figura 80.Instalación OVF GNS3
Fuente: Los autores

10. Performance de la máquina virtual GNS3-SERVER.

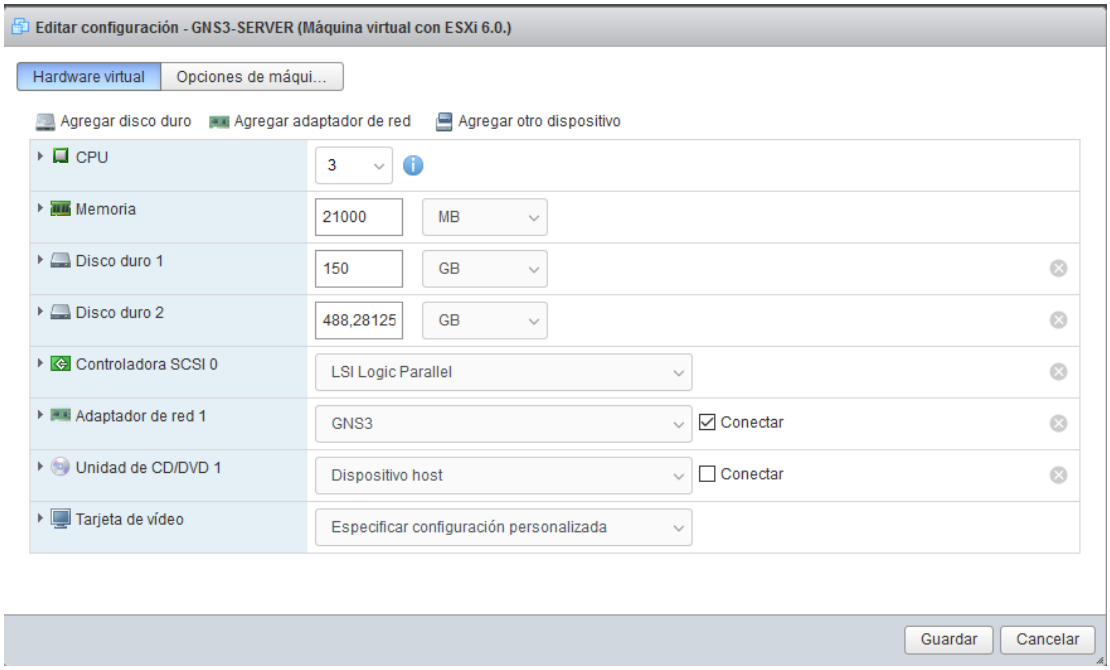


Figura 81.Performance de la máquina virtual
Fuente: Los autores

11. Encender nuestra máquina virutal GNS3-SERVER.

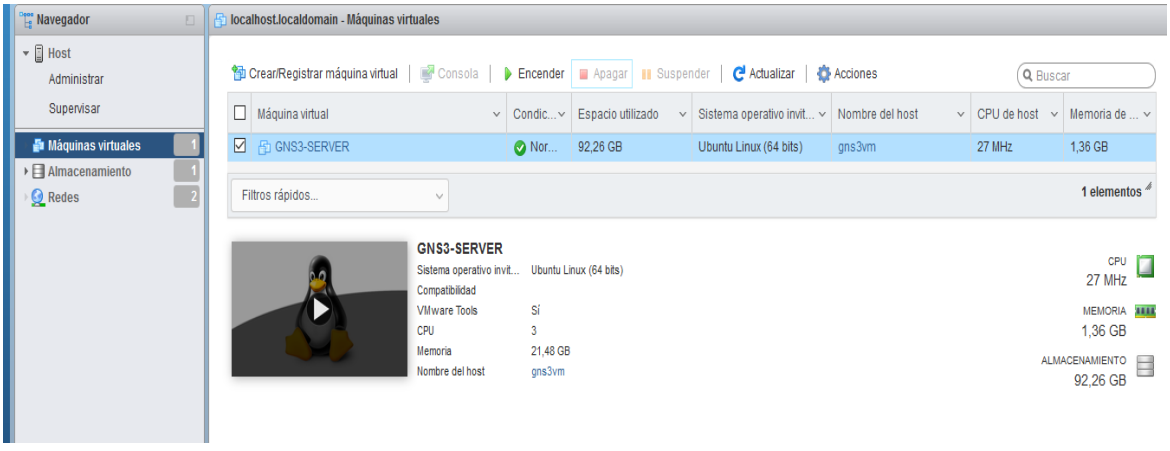


Figura 82.Encendido de la máquina virtual
Fuente: Los autores

12. Ventana de nuestra máquina virtual encendida .

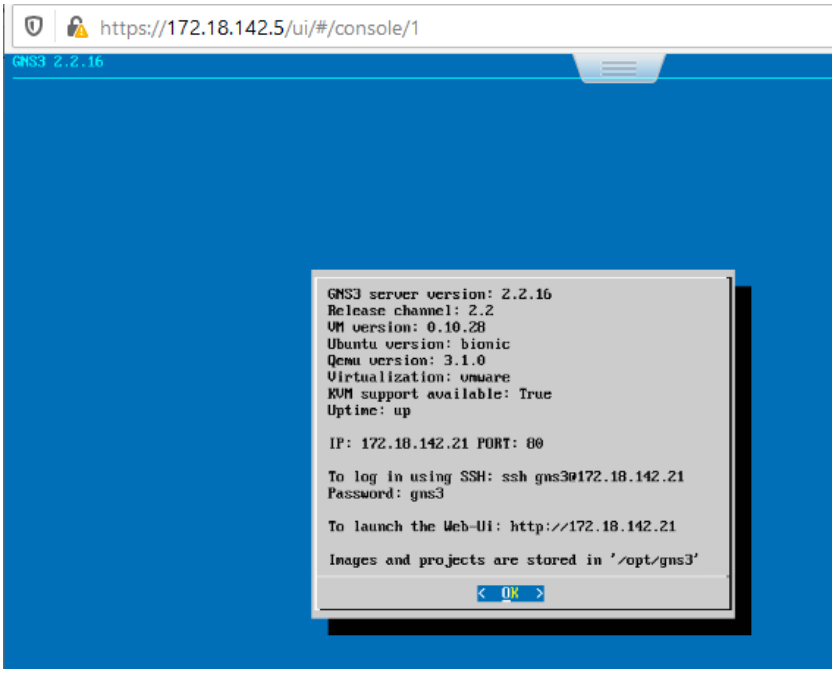


Figura 83.GNS3-SERVER encendida
Fuente: Los autores

12.1 Entrar en las configuraciones de GNS3 2.2.16 para dejar definida la ip estática de la máquina virtual, damos enter en OK.

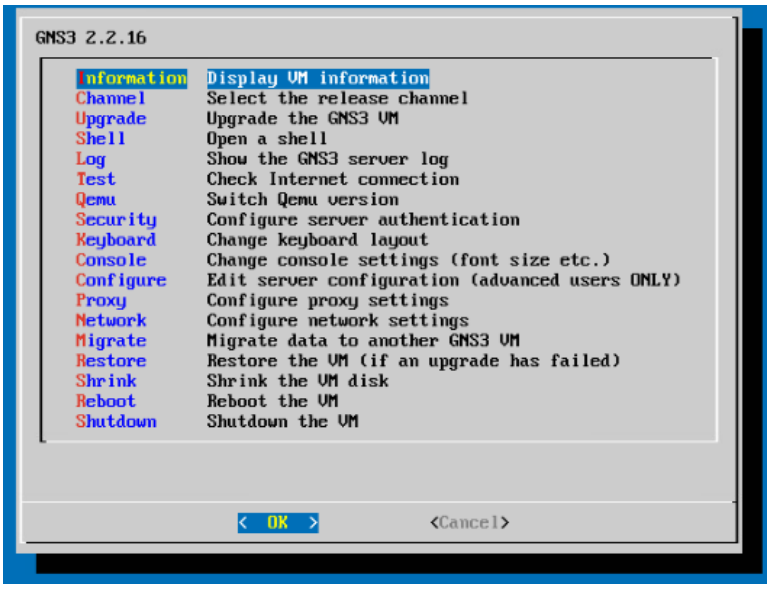


Figura 84.Ventana de configuración GNS3 2.2.16
Fuente: Los autores

12.2 Para acceder a las configuraciones de red, vamos a la opción Network.

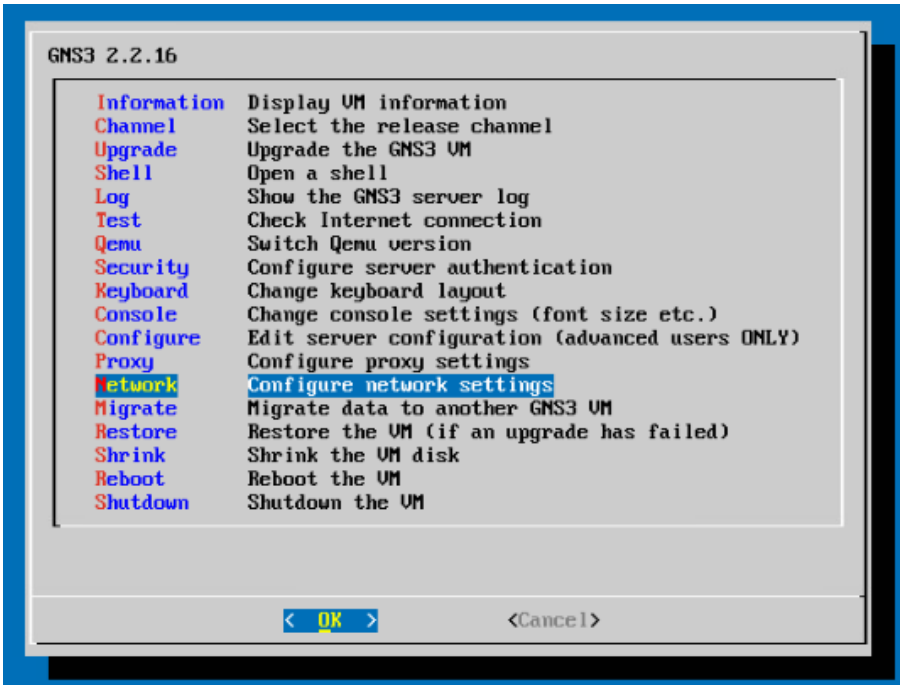


Figura 85.Network GNS3 2.2.16
Fuente: Los autores

12.2 Configuración de la IP estática para GNS3 2.2.16, una vez asignada la dirección IP tecleamos Crtl+O para guardar los cambios.

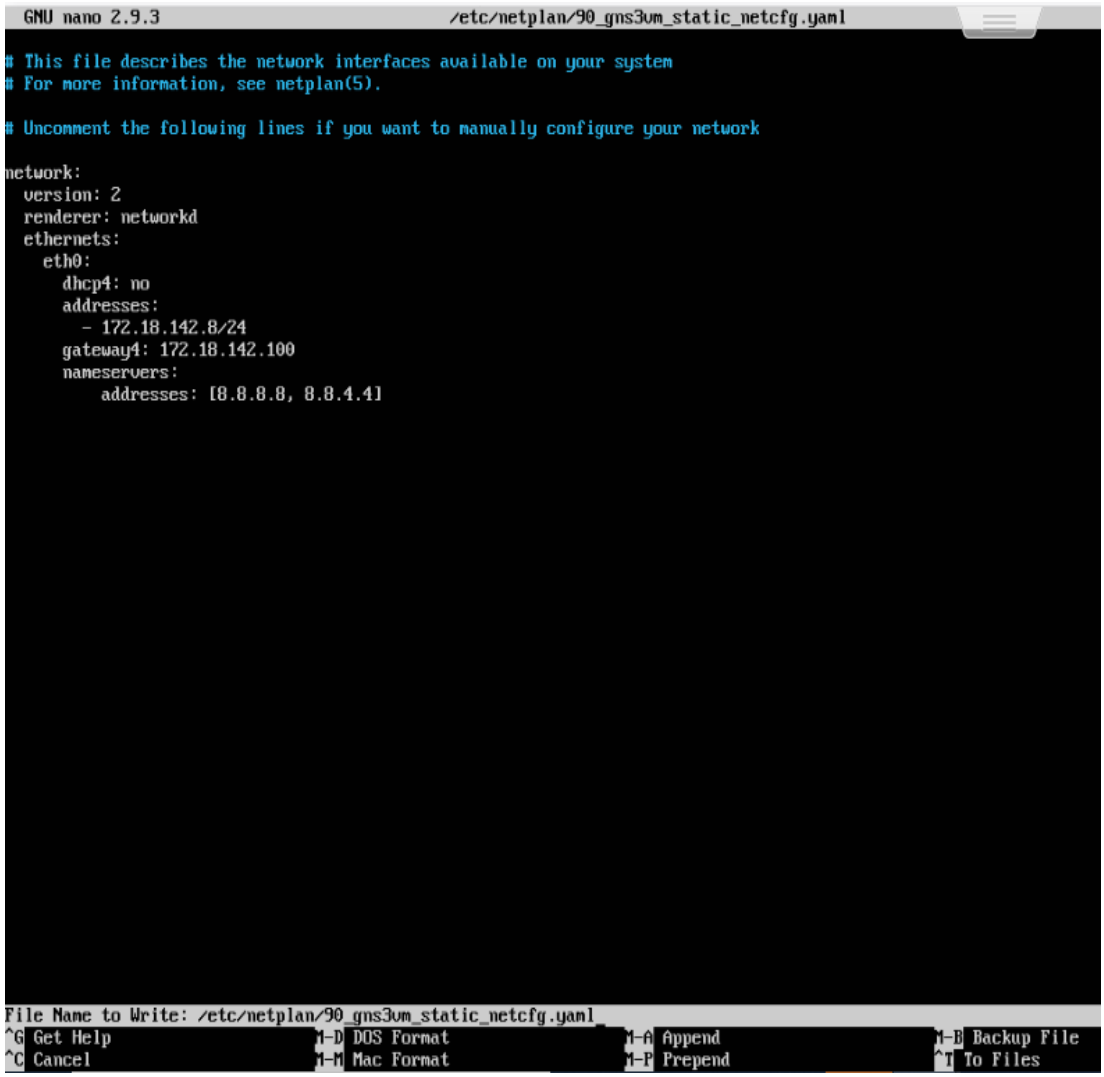


Figura 86. Configuración IP estática GNS3 2.2.16
Fuente: Los autores

13. Ventana de GNS3 2.2.16 con la nueva dirección IP.

Figura 87. GNS3 2.2.16
Fuente: Los autores

3.6. INSTALACIÓN DE LOS IOS EN EL SERVIDOR GNS3.

Para elaboración de las prácticas de redes definidas por software se instaló routers, switches, firewall y sistemas operativos de Windows que se detallan a continuación:

ROUTERS

SERIE C1700, SERIE C2600, SERIE C3620, SERIE C3660, SERIE C2691,SERIE C3725 SERIE C7200, ROUTERBOARD MIKROTIK Y HPE VSR1001.

SO WINDOWS

WINDOWS7, WINDOWS 10.

FIREWALL

FORTIGATE, SOPHOS XG, CHECKPOINT FIREWALL, PALO ALTO Y JUNIPER FIREWALL Y PFSENSE.

SWITCHES

CISCO Lv2.

Se detalla los pasos a seguir para la instalación de los IOS en el servidor GNS3-SERVER.

1. Buscar el archivo gns3a para la instalación de la aplicación de Windows

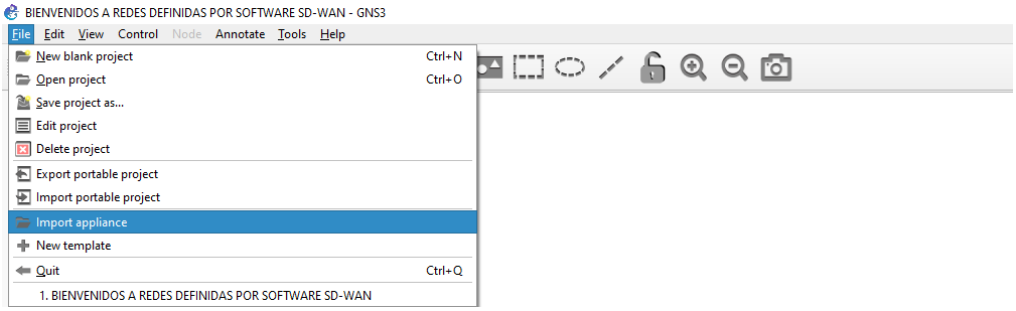


Figura 88.Import appliance GNS3 2.2.16
Fuente: Los autores

2. Abrir archivo Gns3a donde se encuentra ubicado.

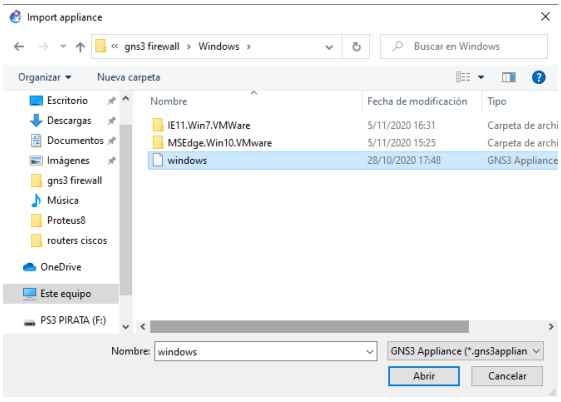


Figura 89.Ubicación del archivo Gns3
Fuente: Los autores

3. Seleccionar donde se va a guardar la aplicación de Windows 7.

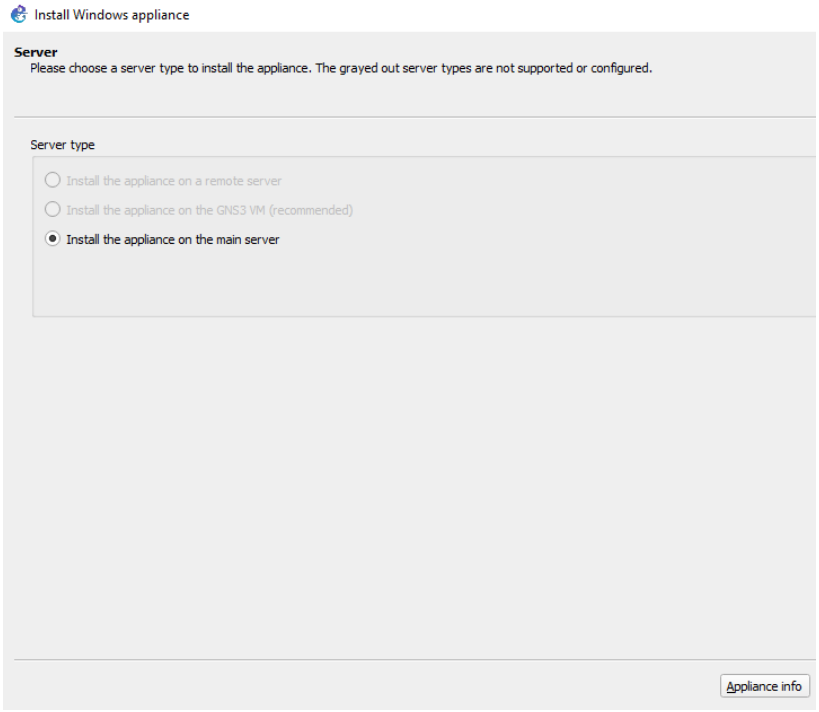


Figura 90.Selección de instalación
Fuente: Los autores

4. Elegir la versión de Windows en este caso es Windows 7.

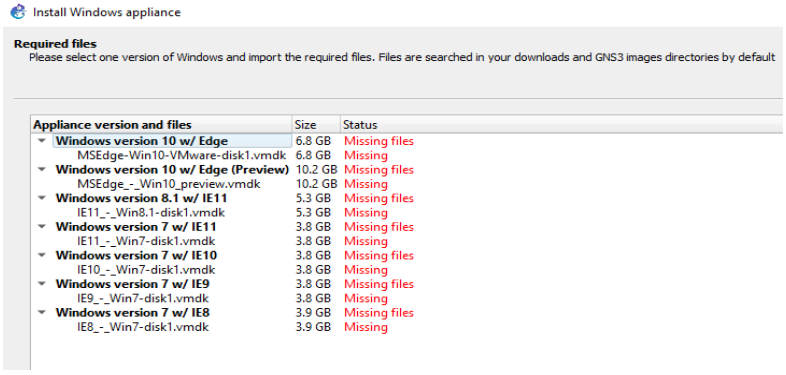


Figura 91.Selección de instalación
Fuente: Los autores

5. Cargar los archivos VMware disk del sistema seleccionado que va a ser almacenado en el servidor.

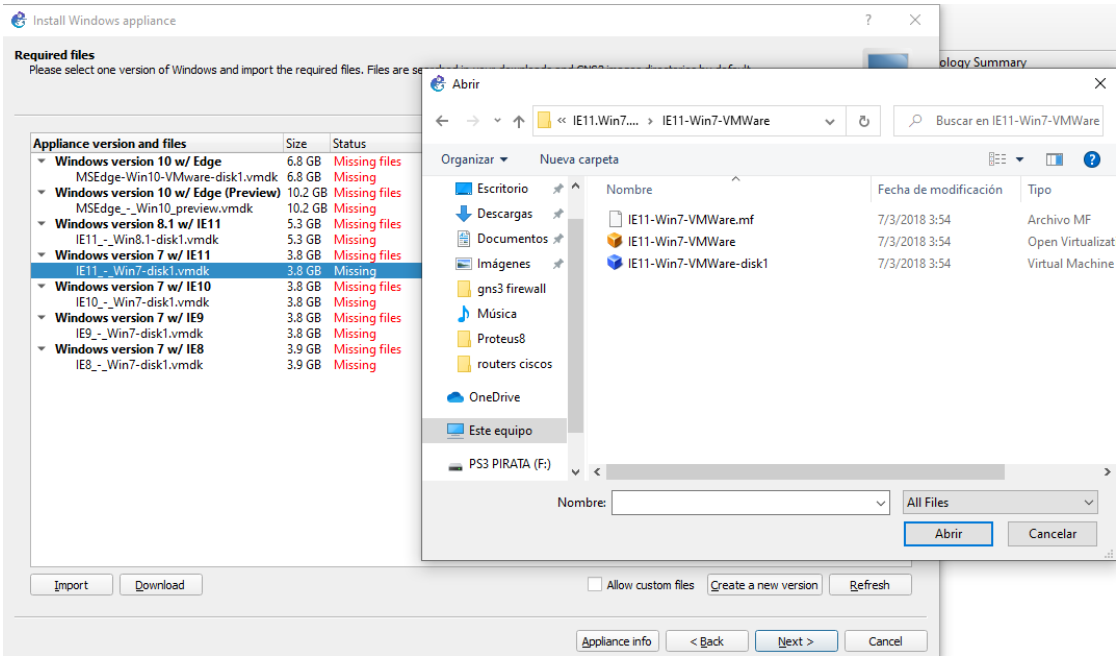


Figura 92.Selección del archivo vmware disk
Fuente: Los autores

6. Esperar que el archivo se transfiera al servidor, depende del tamaño del archivo esto demorar en cargar.

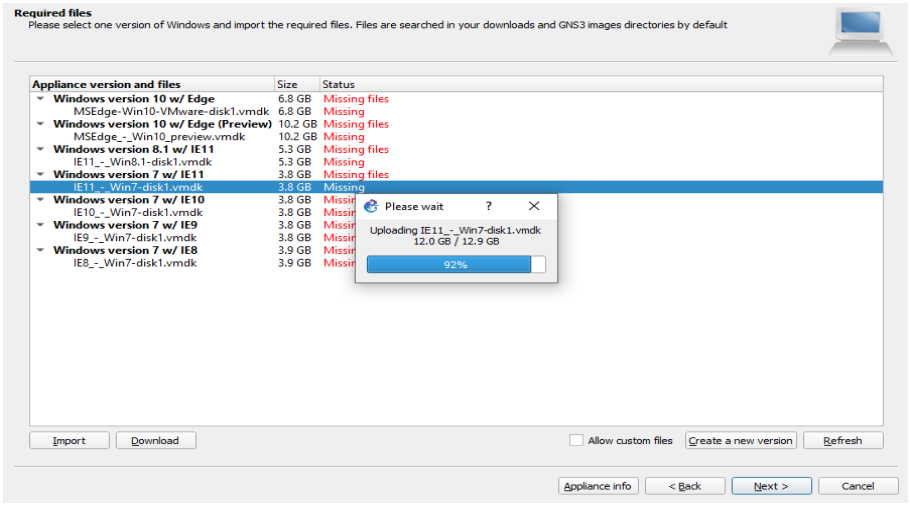


Figura 93. Selección del archivo vmware disk
Fuente: Los autores

7. Una vez finalizada la transferencia del archivo le aparece el siguiente mensaje.

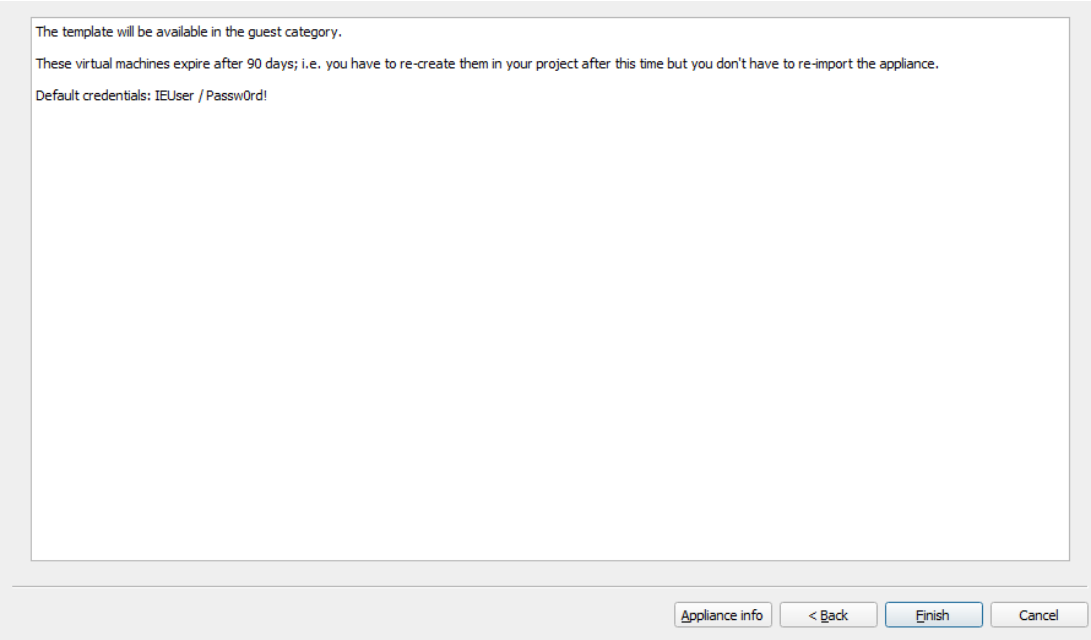


Figura 94.Finalización del archivo
Fuente: Los autores

Nota:

Para la instalación de los archivos restante como es firewall,routers y switch seguir los pasos anteriores.

3.7. DESCRIPCIÓN TÉCNICA DE LOS DISPOSITIVOS DEL BANCO

Los dispositvos del banco de pruebas de redes definidas por software para redes de área amplia (SD-WAN), fueron seleccionados para sastifacer la necesidad de recursos faltante en el momento de simular este tipo de tecnología orientado para los estudiantes y docentes que imparten las materias de redes de computadoras y redes de comunicación que van hacer uso de este banco de pruebas siendo asi que la mayoría de estos dispositivos informáticos se encuentra en nuestro mercado local y son fácil de adquision en caso llegaran a averiarse.

A continuación detallamos los elementos incluidos en el banco de prueba.

3.8. Dell PowerEdge R210 II

El R210 II se puede implementar en prácticamente cualquier entorno, tiene la potencia que se necesita para que su empresa funcione y brinda la escalabilidad para ayudarla a crecer.Comparta, administre y proteja sus datos, todo con un solo sistema. (DELL,2012).

Dentro de sus características técnicas:

- Valor empresarial: rendimiento y funciones para facilitar la colaboración, el uso compartido y la protección de datos y la fácil escalabilidad.
- Fácil de administrar: controladora del ciclo de vida de Dell™ y conjunto completo OpenManage™ para una administración remota simplificada.
- Tecnología flexible y segura: discos duros redundantes integrados, cifrado, opciones de seguridad y protección de datos. Ver Anexo C

Figura 95. Dell R210 II

Fuente: https://www.dell.com/ec/empresas/p/poweredge-r210-2/pd

3.9. KINGSTON A400 SSD SATA de 2,5"

La unidad A400 de estado sólido de Kingston brinda formidables mejoras en la velocidad de respuesta, sin actualizaciones agregadas del hardware. Ofrece tiempos de arranque, carga y de transmisión de archivos extraordinariamente más transitorios en comparación con las unidades de disco duro mecánico. Ver Anexo D

Figura 96.SSD Kingston A400

Fuente: https://www.kingston.com/es/ssd/a400-solid-state-drive

CAPÍTULO IV

MANUAL DE PRÁCTICAS DEL LABORATORIO

Se realiza el desglose de practicas a implementar en el banco de pruebas virtualizado para redes definidas por software para redes de área amplia (SD-WAN) para la ejecución de estas practicas los estudiantes deben tener conocimiento de las materias de redes de computadoras I y redes de computadoras II teniendo en cuenta los dispositivos que van para configurar para fortalecer sus destrezas técnicas en el momento de realizar las simulaciones.

4.1. GUIA DE PRÁCTICAS PARA PRUEBAS DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN)

PRÁCTICA 1: Conexión remota al servidor virtual con el software GNS3.

PRÁCTICA 2: Configuración de una red SD-WAN con Fortigate 6.2.0.

PRÁCTICA 3: Configuración de una red SD-WAN con perfomance SLA en fortigate 6.4.2.

PRÁCTICA 4: Configuración de una red SD-WAN con prioridad de servicios con sd-wan rules.

PRÁCTICA 5: Configuración de una red SD-WAN con fortigate y enlazados con dispositivos mikrotik.

PRÁCTICA 6: Configuración de una red VPN IPSEC fortigate a fortigate.

PRÁCTICA 7: Configuración de una red VPN IPSEC con balanceo sd-wan.

PRÁCTICA 8: Configuración de un failover con mikrotik para un enlace SD-WAN

PRÁCTICA 9: Configuración de un mangle con mikrotik para el enlace SD-WAN.

PRÁCTICA 10: Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik.

4.1.1. PRÁCTICA 1

Conexión remota al servidor virtual con el software de GNS3.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA** Nº 1
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO QUERIDO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Conexión de acceso remota al servidor virtual con el software de GNS3.

OBJETIVOS

General

Establecer conexión de manera remota para seguir la realización de las prácticas de laboratorio para redes definidas por software para redes de área amplia (SD-WAN).

Específicos

- Descargar, instalar en la computadora GNS3.
- Conectar remotamente la computadora al servidor virtual.

GLOSARIO

GNS3 .- GNS3 es un software manejado por ingenieros de redes para emular, configurar, experimentar y solucionar dificultades de redes virtuales y reales.

SD-WAN.- Las redes de área amplia definidas por software o SD-WAN (software-defined networking area network), tienen como enfoque el diseño empresarial , instituicional y corporativo para mejorar el uso de recursos en las redes internas de empresas en la red, para optimizar el desempeño y concretar el tráfico de nuestra red, sea de Internet o interconexión de sedes.

CONEXIÓN REMOTA. - Tiene como hecho de conectarse a servicios, aplicaciones o datos de TI desde un sitio diferente a la sede central o una establecimiento más cercana al centro de datos. Esta conexión consiente a los usuarios acceder a una red o una computadora de forma remota por medio de una conexión a Internet.

IP.- La internet protocol address se fundamenta en el protocolo de Internet, que es, también, la base del funcionamiento de Internet. Se trata de la dirección inequívoca de un dispositivo (por ejemplo, una computadora,un servidor de streaming o de una impresora) dentro de una red interna o externa.

MARCO PROCEDIMENTAL

1. Descargar e instalar el software GNS3 para conexión remota al servidor virtualizado, desde el siguiente link.

   https://www.gns3.com/software/download

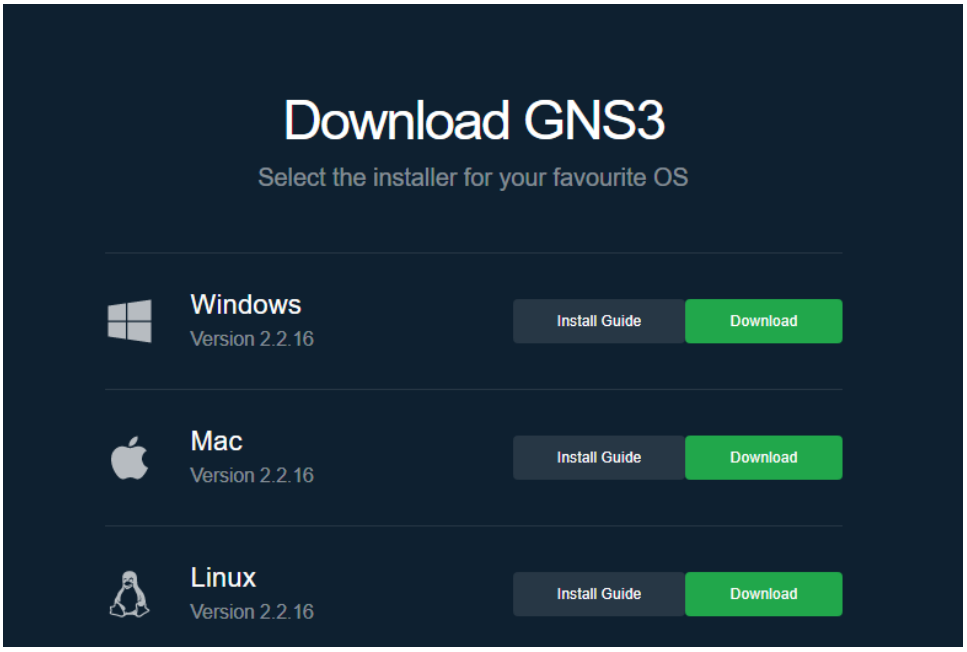


Figura 97. Descargar Gns3
Fuente: Los autores

2. Conectar de manera remota nuestra computadora a través de TCP/IP al servidor virtualizado.

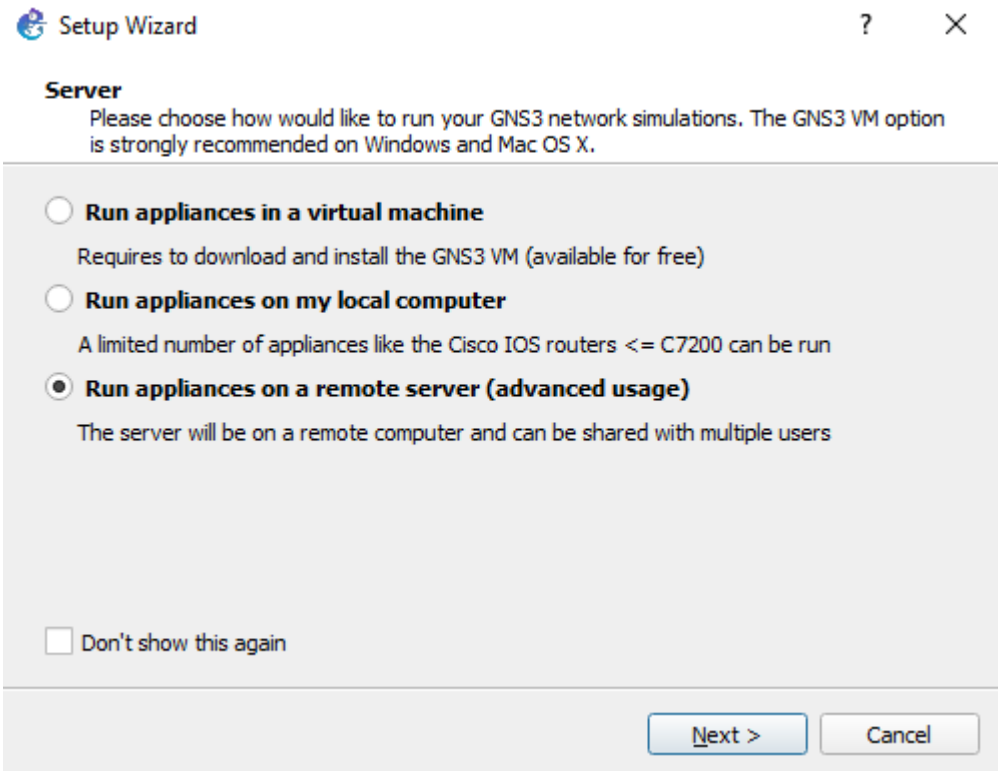


Figura 98. Conexión al servidor
Fuente: Los autores.

3. Escribir la dirección IP que se encuentra en la imagen y colocamos en usuario y contraseñas la palabra gns3.

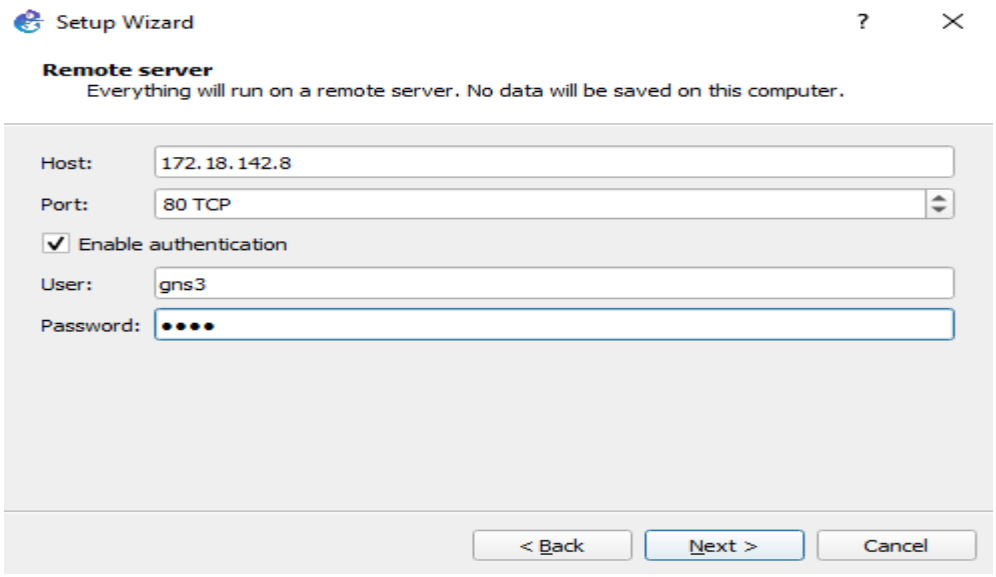


Figura 99. Datos de conexión al servidor.
Fuente: Los autores.

4. Conexión existosa al servidor

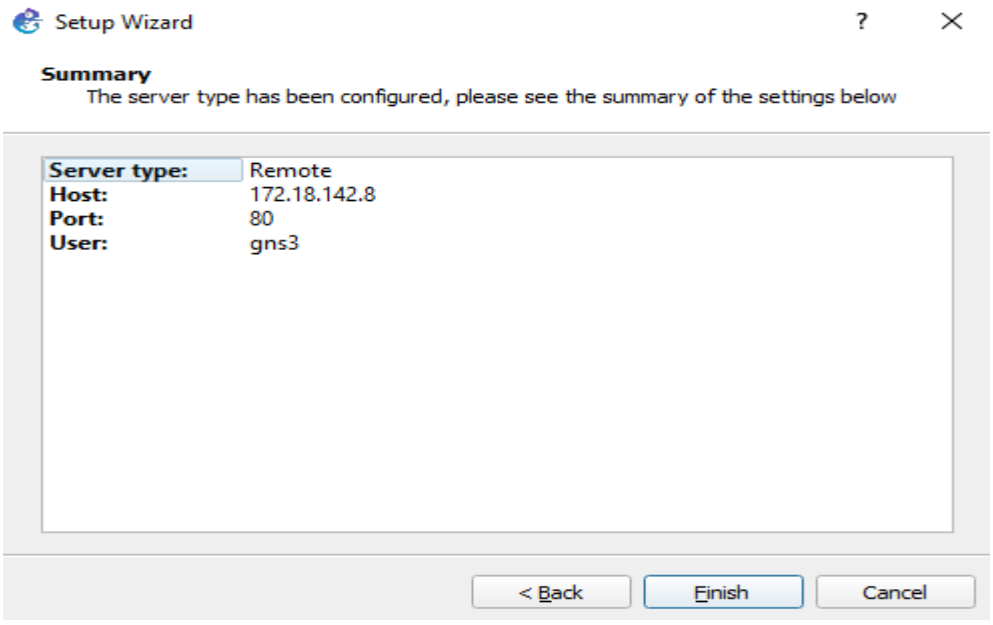


Figura100. Conexión establecida a gns3 server
Fuente: Los autores

5. Seleccionar el proyecto o crear nuevo proyecto.

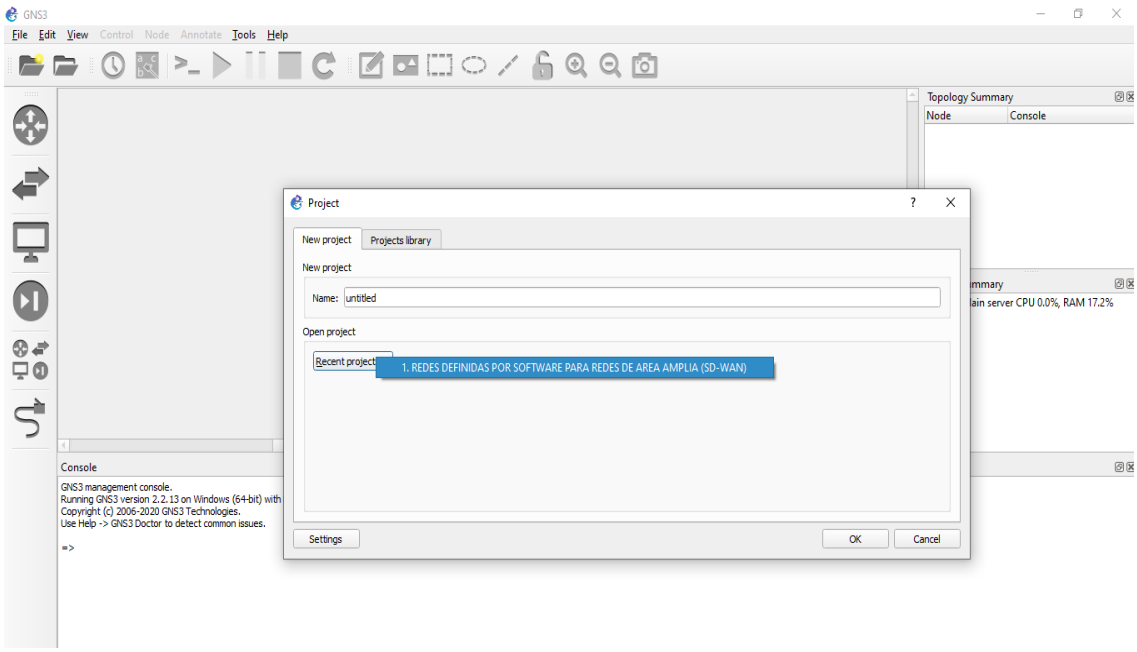


Figura101. Proyecto en Gns3
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)

CRONOGRAMA/CALENDARIO

De acuerdo con la planificación de cada docente

4.1.2. PRÁCTICA 2

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 2**
- **NUMERO DE COMPUTADORAS:** 16
- **TIEMPO CONSIDERADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con Fortigate 6.2.0

OBJETIVOS

General

Configurar punto a punto con redes definidas con software para redes de área amplia SD-WAN para acceso a internet.

Específicos

- Realizar uso más efectivo de conexiones de internet.
- Configurar Vlans para administración de la red.
- Programar interfaces SD-WAN para los enlaces a internet.

GLOSARIO

SD-WAN.- Las redes de área amplia definidas por software o SD-WAN (software-defined networking area network), tienen como enfoque el diseño empresarial , instituicional y corporativo para mejorar el uso de recursos en las redes internas de empresas en la red, para optimizar el desempeño y concretar el tráfico de nuestra red, sea de Internet o interconexión de sedes.

VLANS.- Una Virtual Local Area Network (VLAN) o red de área local virtual es un conjunto flexible de dispositivos que se hallan en diferente sitio de una red de área local pero se notifican como si existieran en el mismo segmento físico.

SWITCH O CONMUTADOR.- Es un dispositivo de interconexión utilizado para enlazar equipos en una redde datos estableciendo lo que se conoce como una red de área local (LAN).

MARCO PROCEDIMENTAL

1. Crear nuevo proyecto para realizar la práctica 2.

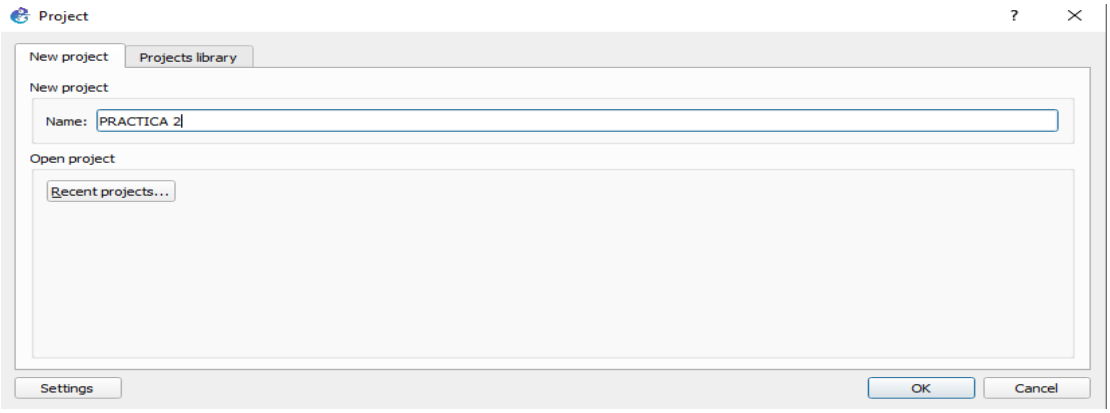


Figura102. Nuevo proyecto
Fuente: Los autores

2. Diseñar la topología de la práctica 2 donde las sucursales son los dispositivos de firewall fortigate.

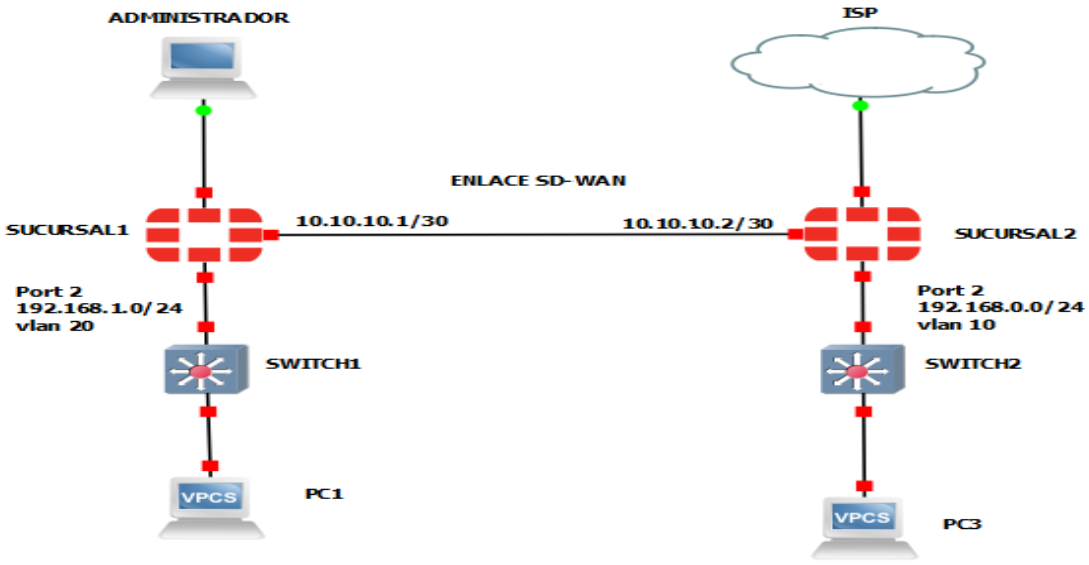


Figura103. Diseño de la red práctica Nº2
Fuente: Los autores

3. Encender sucursal 1 y sucursal 2.

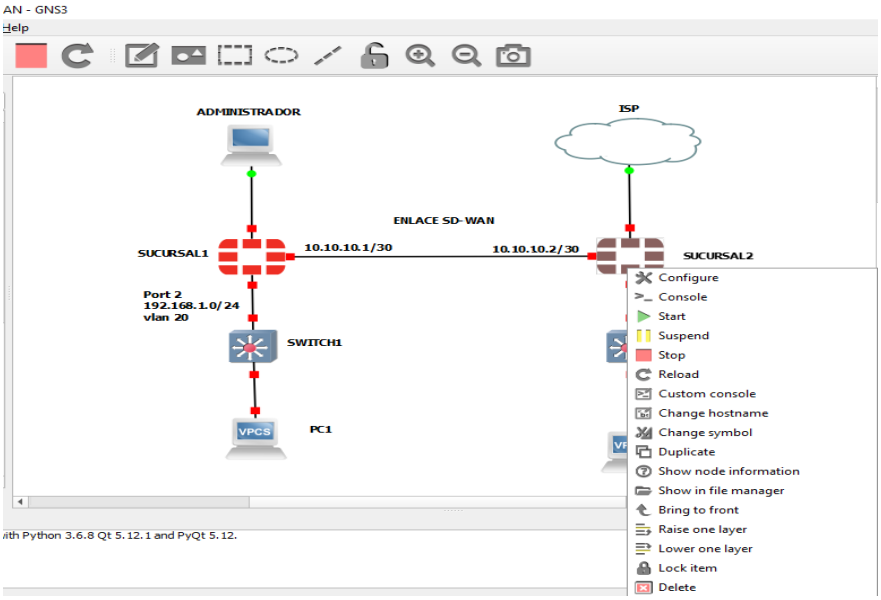


Figura104. Encendido de sucursales fortigate 6.2.0
Fuente: Los autores

4. Iniciar por modo console en sucursal 2

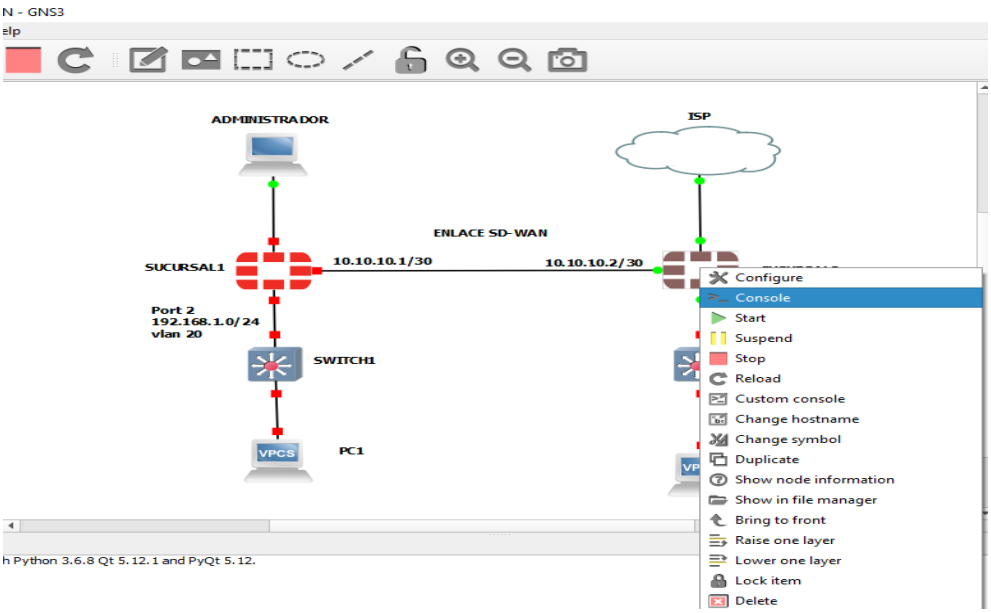


Figura105. Ingresar CLI Sucursal 2
Fuente: Los autores

5. Escribir en el login la palabra admin y la contraseña en blanco en esta versión de fortigate 6.2.0, te permite ingresar a la configuración sin realizar el cambio de contraseña a la administración del equipo comenzaremos a configurar sucursal 2.

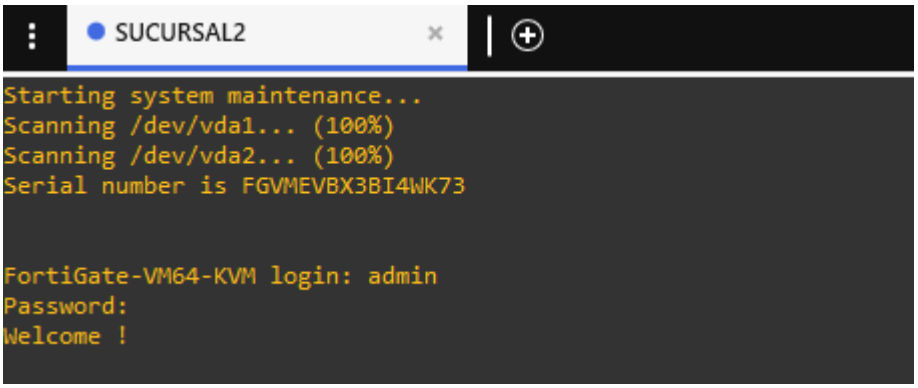


Figura106. Visualización del CLI
Fuente: Los autores

6. Para mostrar la IP del fortigate de sucursal1 debemos ingresar el siguiente comando: get system interface – donde en port1 nos muestra la dirección IP que obtuvo de muestro router.

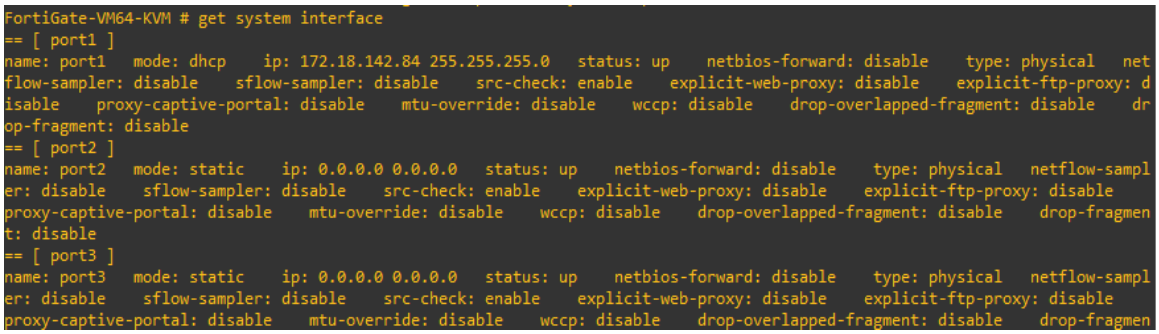


Figura107. Dirección IP sucursal 2 del Fortigate 6.2.0
Fuente: Los autores

7. Ingresar al fortigate por navegador con la dirección la dirección IP que obtuvo de nuestro router.

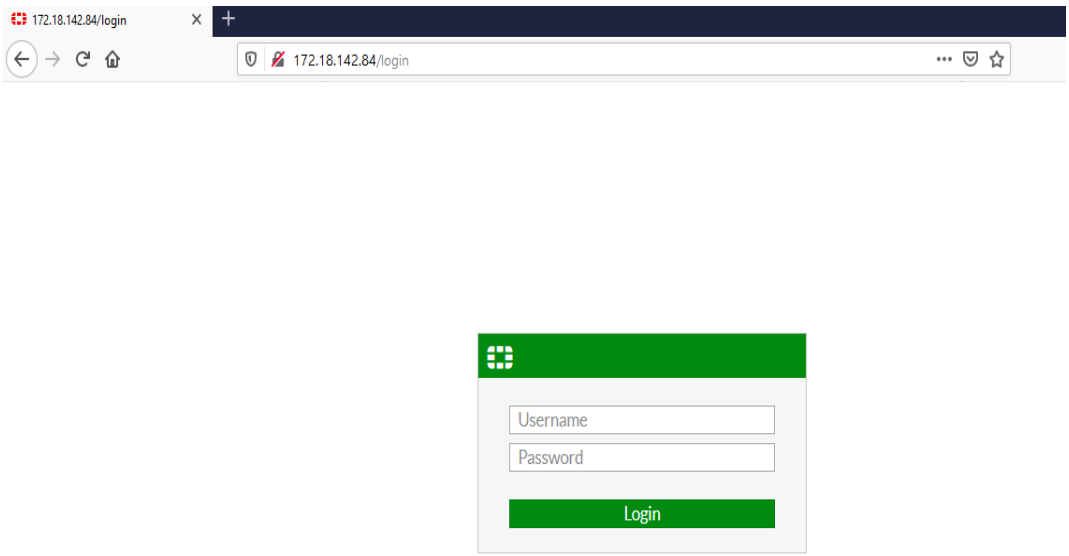


Figura108. Interfaz Web Fortigate
Fuente: Los autores

8. Configurar la dirección ip para la red SD-WAN, damos en click en la interface port2.

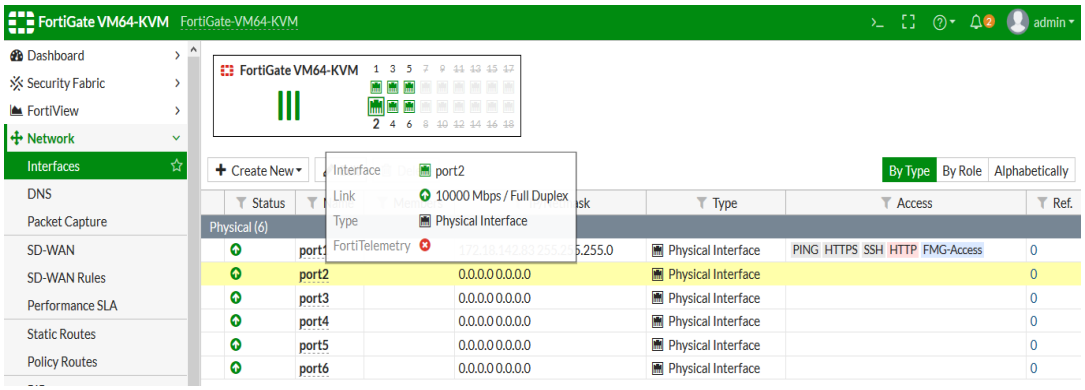


Figura109. Selección del port2 sucursal 2
Fuente: Los autores

9. Ingresar nombre de la interfaz y su respectiva dirección de red.

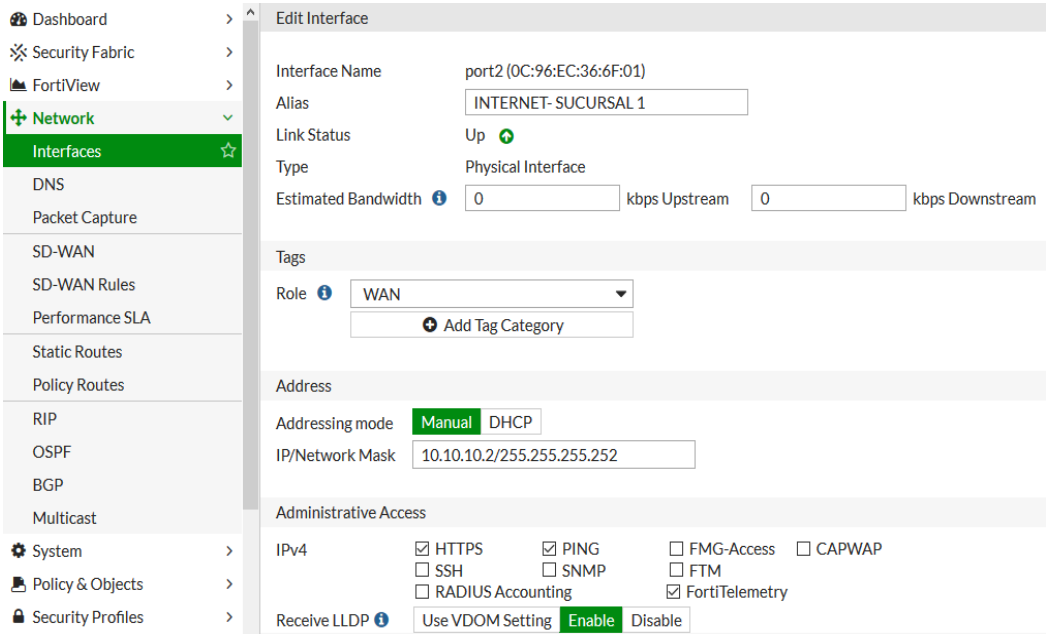


Figura110. Configuración del port2
Fuente: Los autores

10. Ingresar a create new para la configuración de la interface VLAN 10

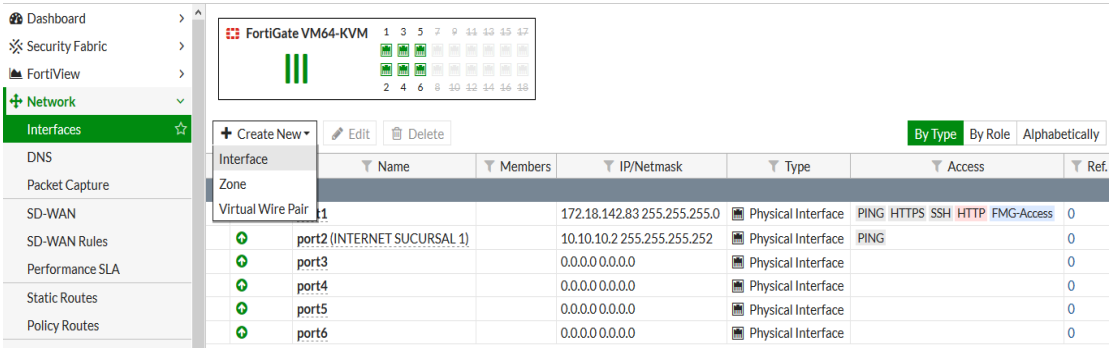


Figura111. Interface Virtual
Fuente: Los autores

11. Configurar la interfaz VLAN 10 para la red local.

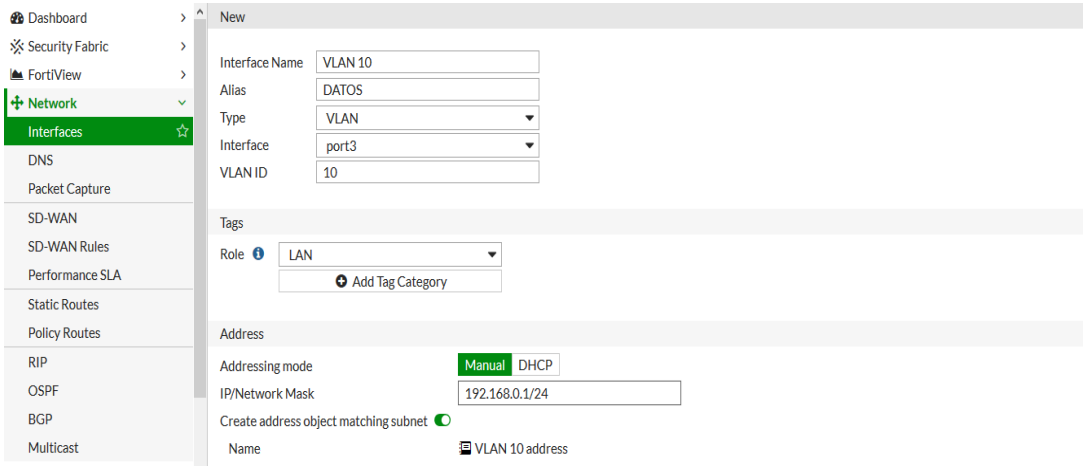


Figura112. Configuración de interfaz VLAN-IP
Fuente: Los autores

12. Configurar DHCP server para la red local de la interfaz vlan 10

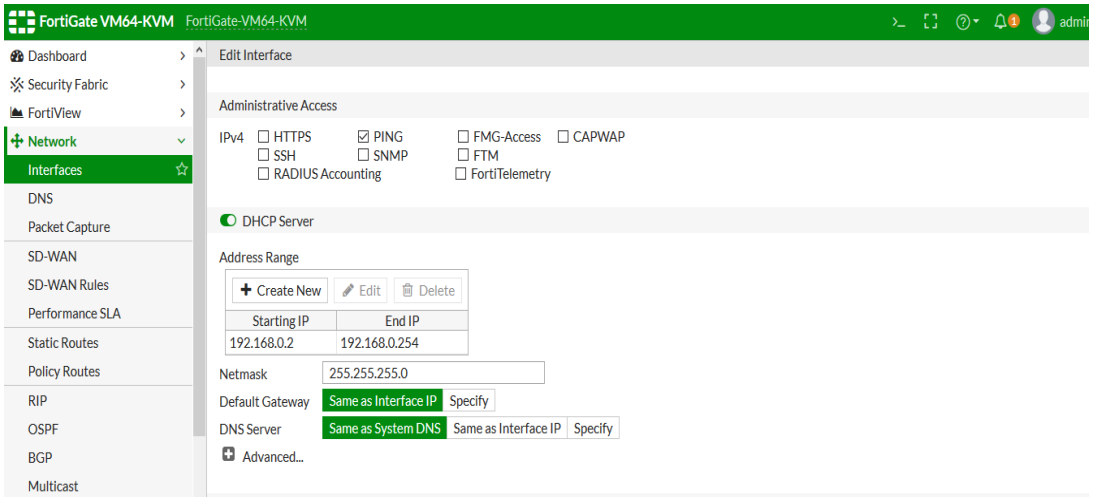


Figura113. Configuración de DHCP interfaz VLAN 10
Fuente: Los autores

13. Visualización de todas las interfaces de red configuradas.

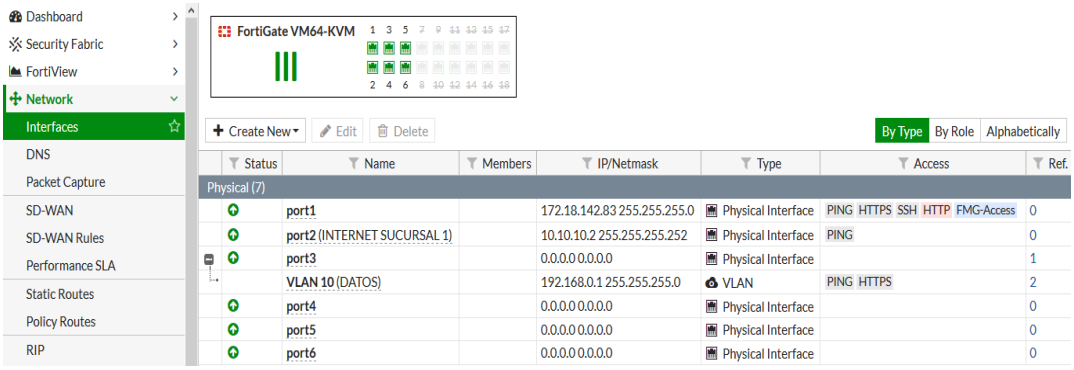


Figura114. Interfaces Configuradas Fortigate Oficina Central
Fuente: Los autores

14. Seleccionar static route para salida a internet.

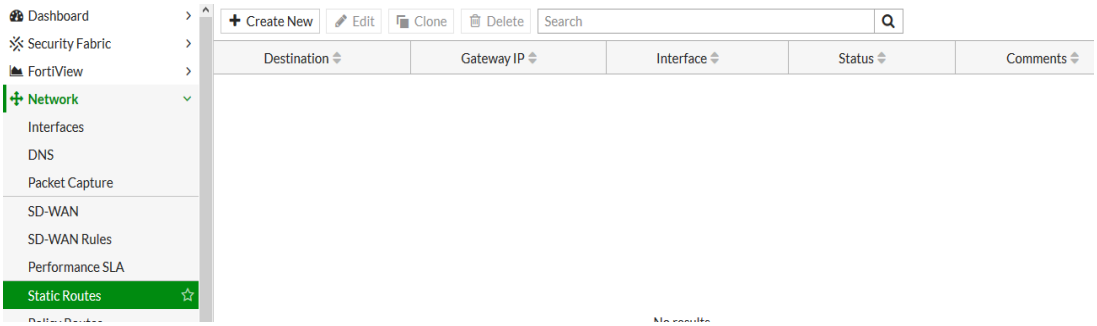


Figura115. Módulo de static routes
Fuente: Los autores

15. Configurar la por cual interfaz tendremos salida internet en este caso es por el port1 donde se asignará automáticamente la IP del Gateway de nuestro router, también se le puede asignar de manera manual.

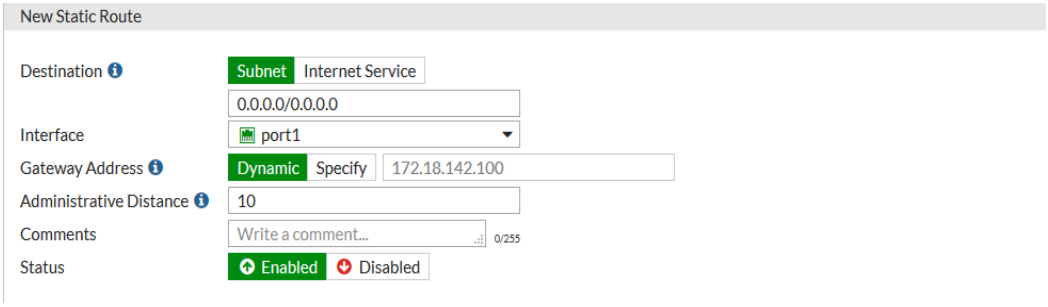


Figura116. Configuración static routes
Fuente: Los autores

16. Realizaremos un ping a la siguiente dirección 8.8.8.8 para verificar la salida de internet del dentro del fortigate de sucursal 2.

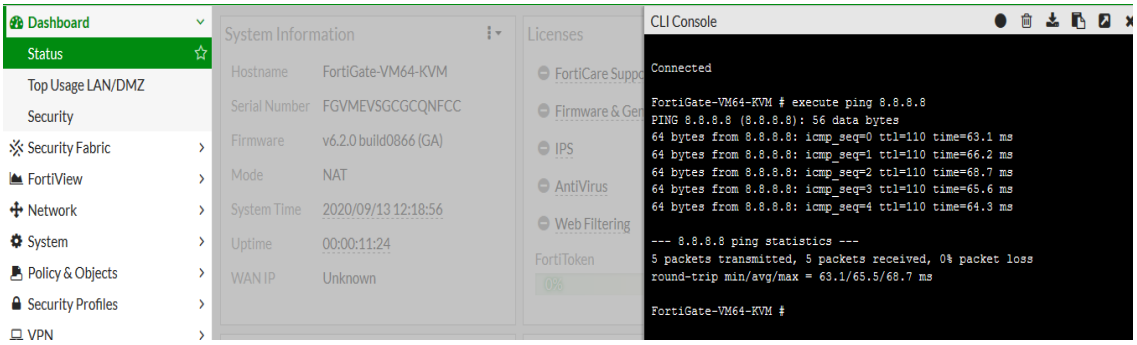


Figura117. Ping a Google
Fuente: Los autores

17. Configurar la política para tener todos los servicios de navegación para nuestra red de la sucursal 1 y la red local de la VLAN 10, solo se puede crear máximo 5 políticas en este entorno virtual.

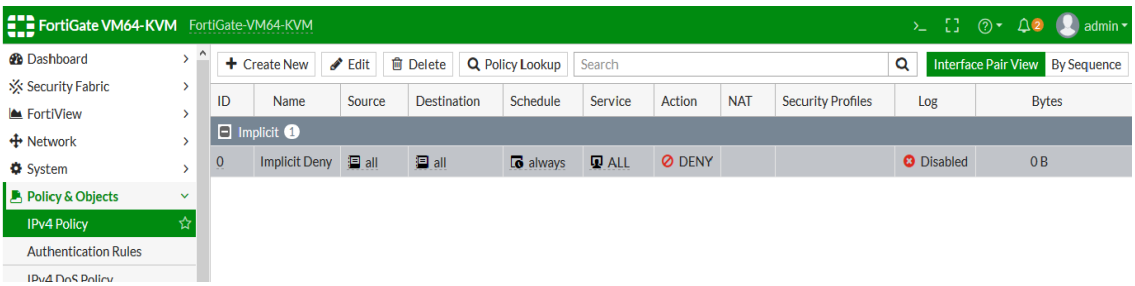


Figura 118. Ipv4 Policy Sucursal 2
Fuente: Los autores

18. Realizar la configuración de la política para navegación sin restricción para la red local.

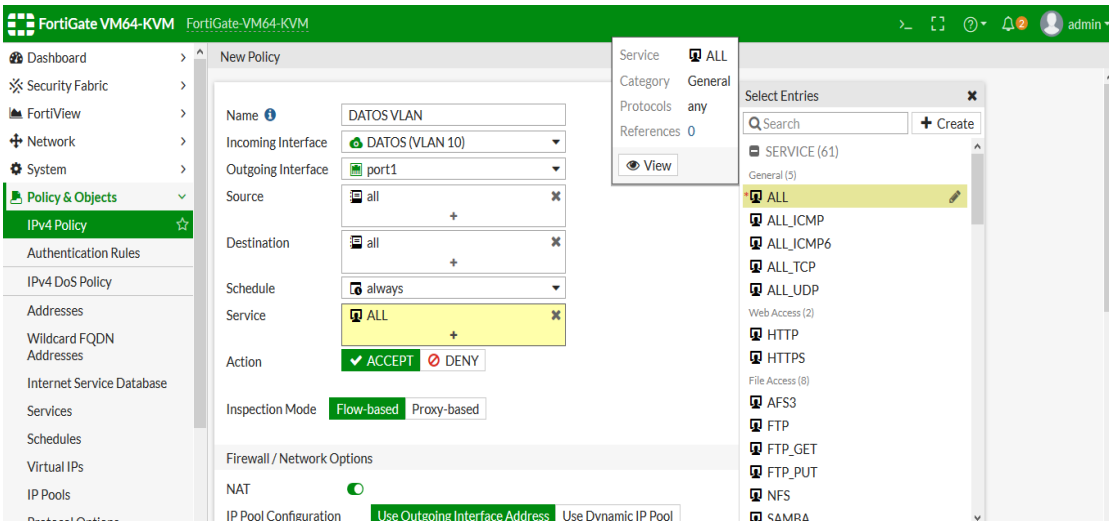


Figura119.Configuración de los servicios Sucursal 2
Fuente: Los autores

19. Políticas creadas para la VLAN 10 de red local

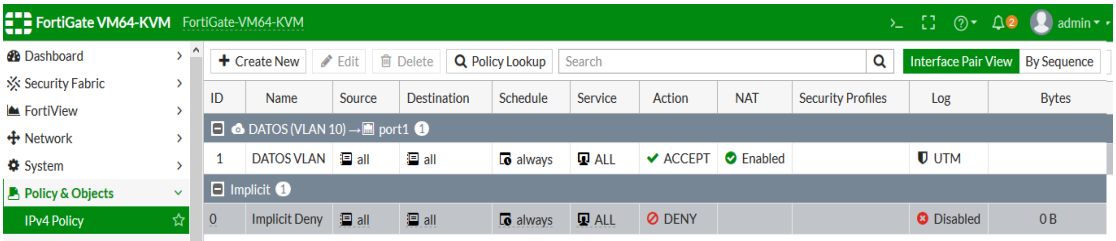
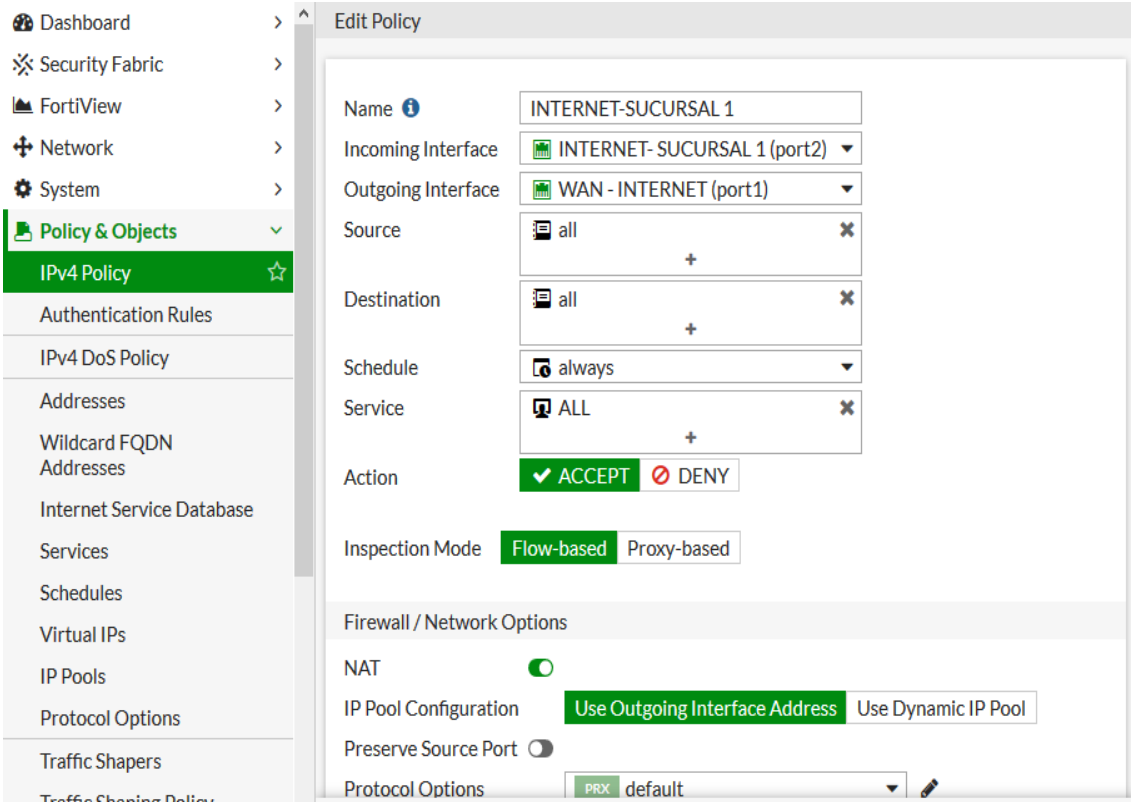


Figura120. Políticas Vlan 10
Fuente: Los autores

20. Realizar la configuración de la política de navegación para la red de la



sucursal

Figura121.Configuración de las políticas para Sucursal 1
Fuente: Los autores

21. Iniciar Switch 2 para la configuración de la VLAN 10.

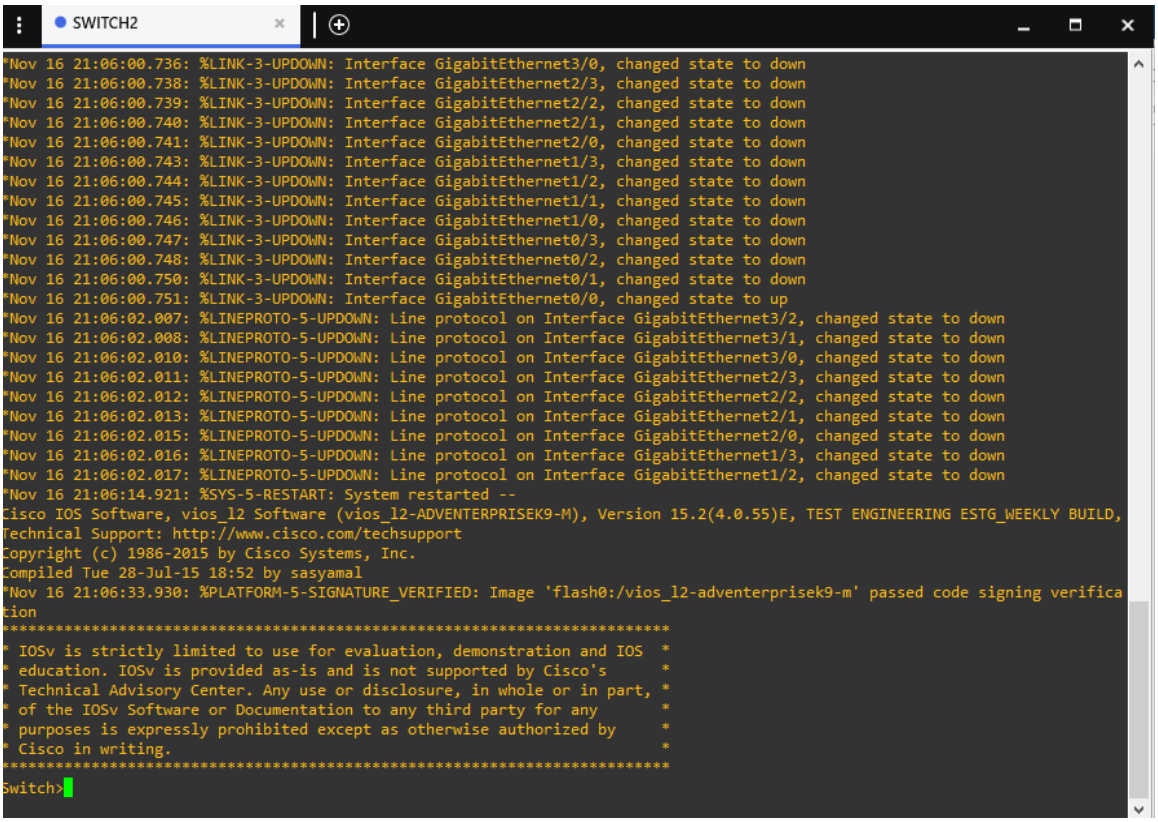


Figura122. Iniciando Switch
Fuente: Los autores

22. Configurar la VLAN 10 en el switch.

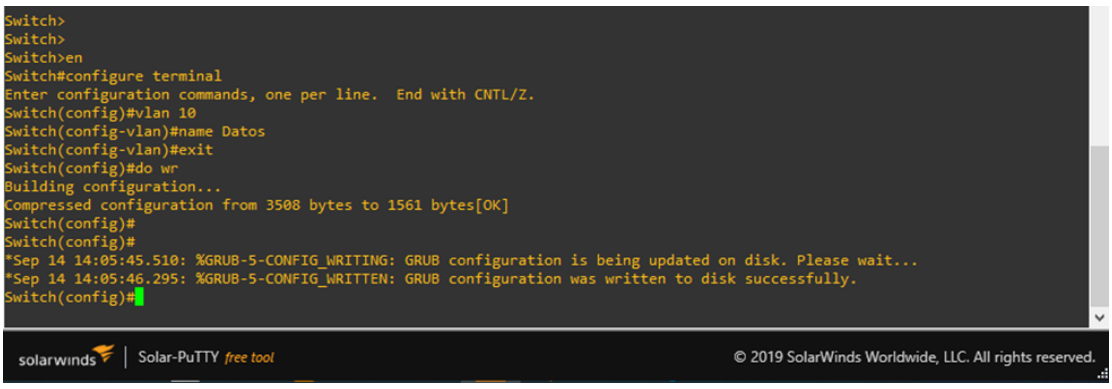


Figura123. Creación VLAN-10 Datos
Fuente: Los autores

23. Configurar puerto troncal switch 2.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 3/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 3569 bytes to 1600 bytes[OK]
Switch(config-if)#
*Sep 14 14:24:32.499: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Sep 14 14:24:33.267: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config-if)#exit
Switch(config)#
```

Figura124. Puerto Trunk VLAN
Fuente: Los autores

24. Asignar VLAN la 10 a los puertos que vamos usar.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range gigabitEthernet 0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do wr
Building configuration...
Compressed configuration from 3722 bytes to 1671 bytes[OK]
Switch(config-if-range)#
*Sep 14 14:31:23.223: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Sep 14 14:31:23.985: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config-if-range)#exit
Switch(config)#
```

Figura125. Puerto Access VLAN 10
Fuente: Los autores

25. Iniciar las VPCS ,teclear DHCP para obtener dirección IP y realizamos un ping a la siguiente dirección para verificar la salida a internet.

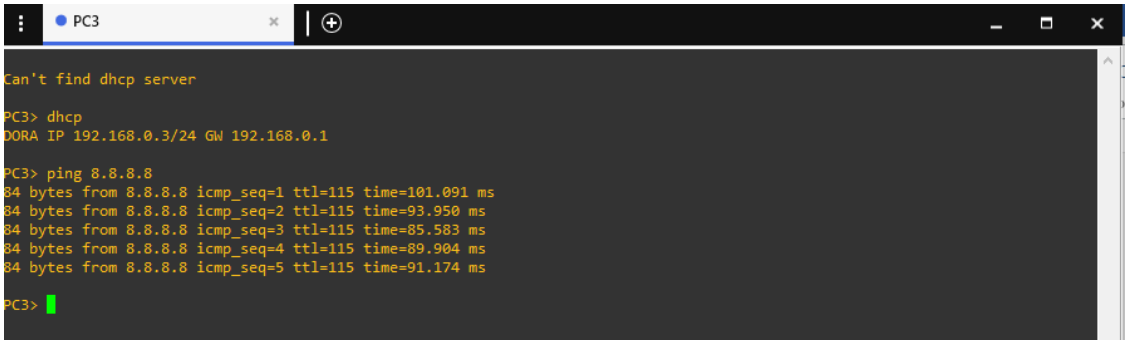


Figura126. Comprobación de internet PC3 Sucursal 2
Fuente: Los autores

26. Entrar por console al fortigate sucursal 1 para obtener la dirección IP que obtuvo de nuestro router local escribimos el siguiente comando get system interface.

.

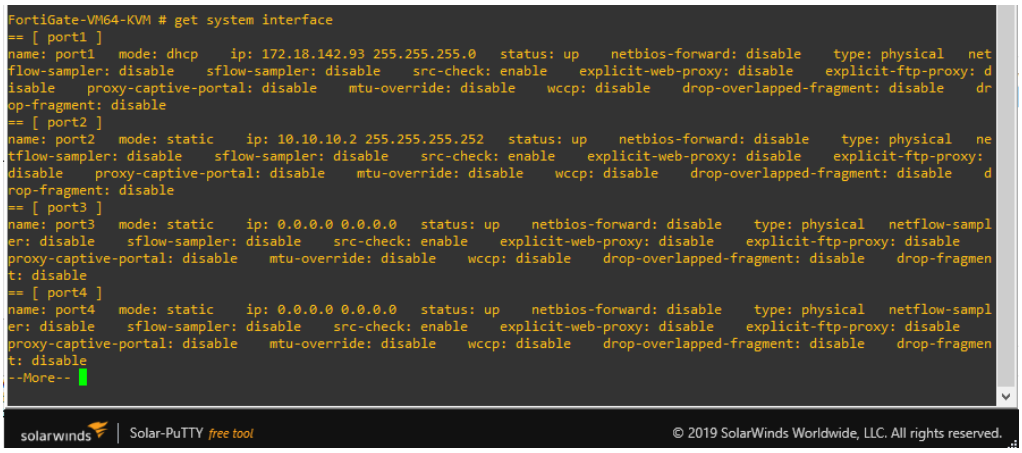


Figura127. Comprobación de internet PC3 Sucursal 2
Fuente: Los autores

27. Entrar via browser con la IP asignada.

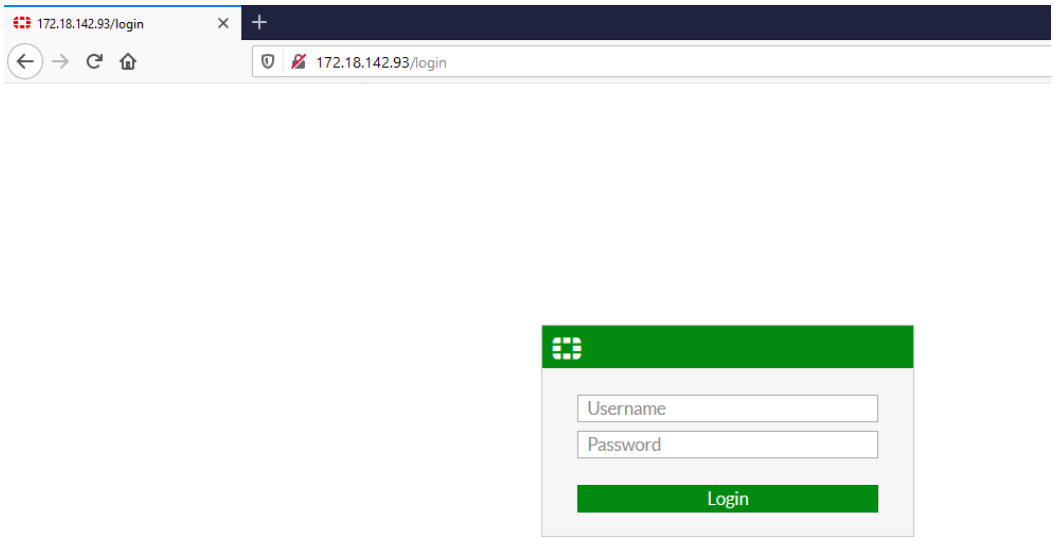


Figura128. Browser Fortigate Sucursal 2
Fuente: Los autores

28. Configurar la interface port2 fortigate sucursal 1.

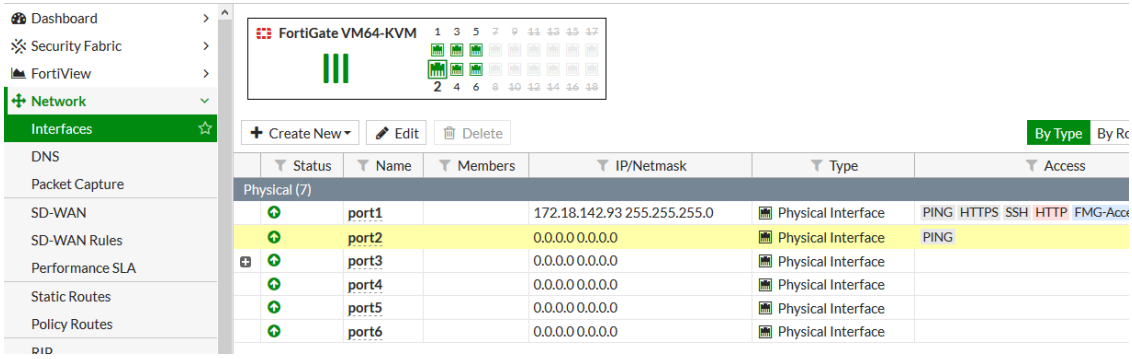


Figura 129. Port2 Fortigate Sucursal 2
Fuente: Los autores

29. Configuracion del port2 para la red SD-WAN del fortigate sucursal 1.

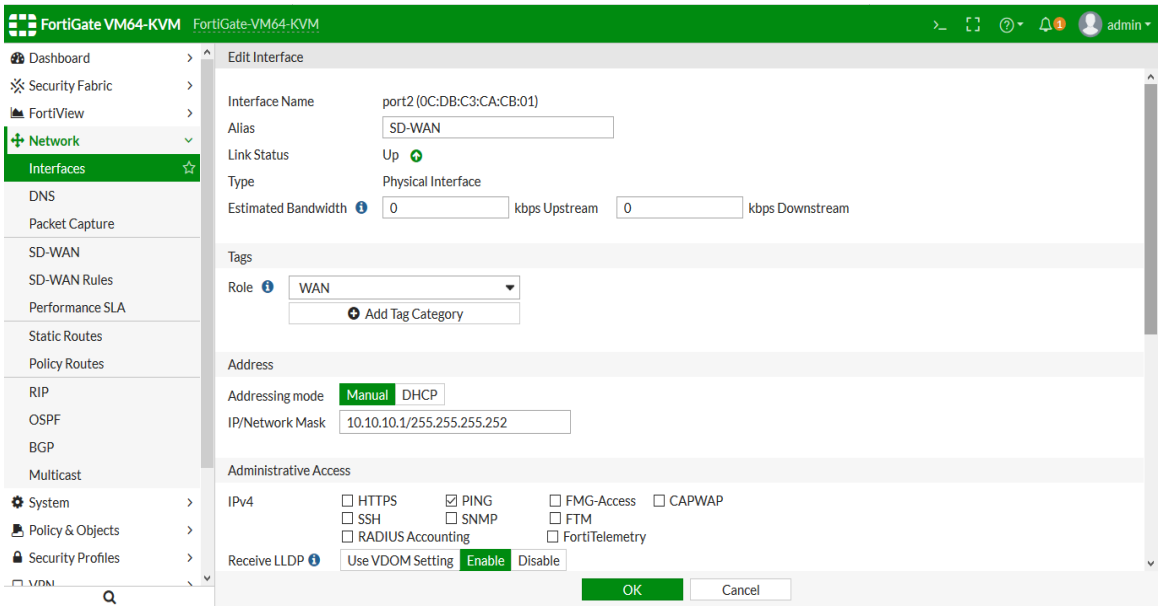


Figura130.Configuración del port2 sucursal 1
Fuente: Los autores

30. Configurar interface VLAN 20 en el fortigate sucursal 1.

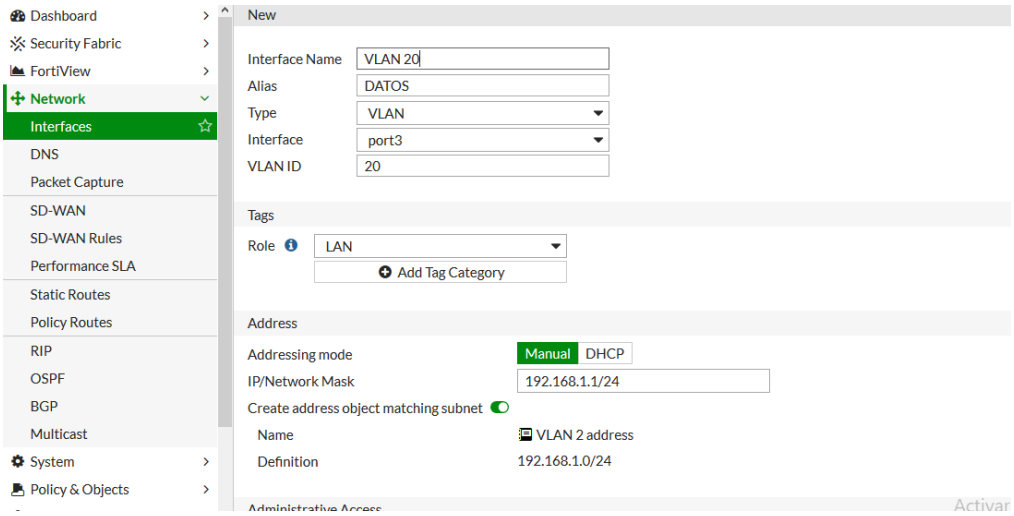


Figura131.Interfaz Vlan Sucursal 1
Fuente: Los autores

31. Activar DHCP Server para la interfaz VLAN 20.

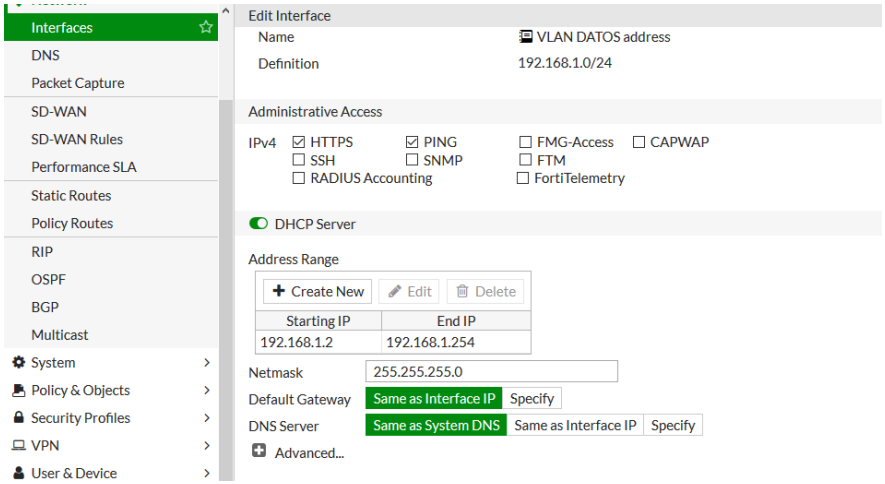


Figura132. DHCP VLAN Sucursal 1
Fuente: Los autores

32. Configuracion de la SD-WAN, le damos enable para activar la interfaz.

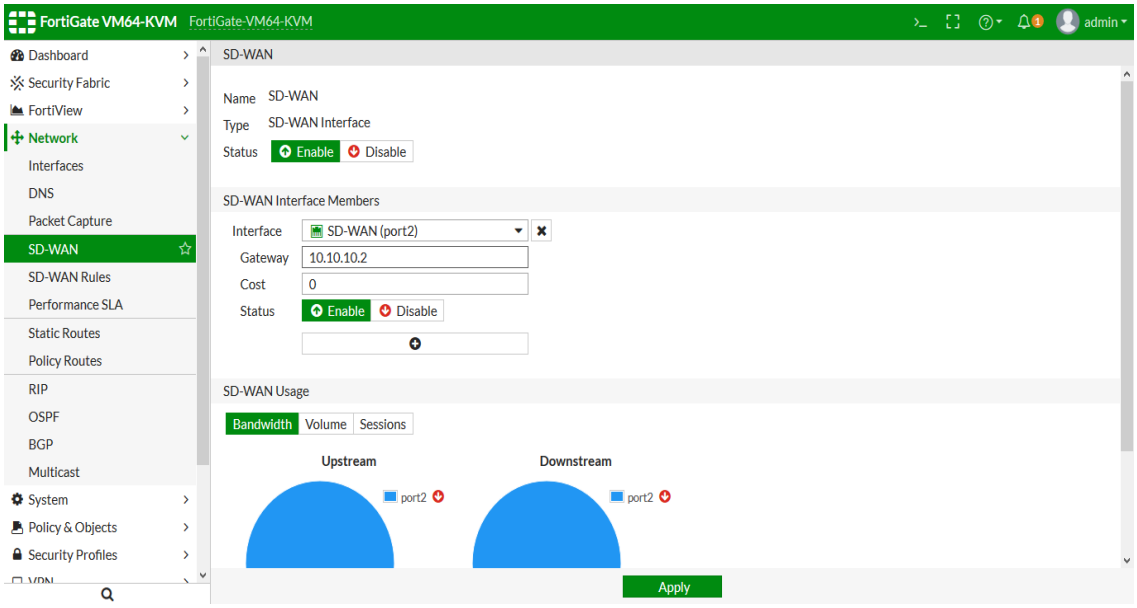


Figura133.SD-WAN Sucursal 1
Fuente: Los autores

33. Configurar static routes para salida a internet del enlace SD-WAN.

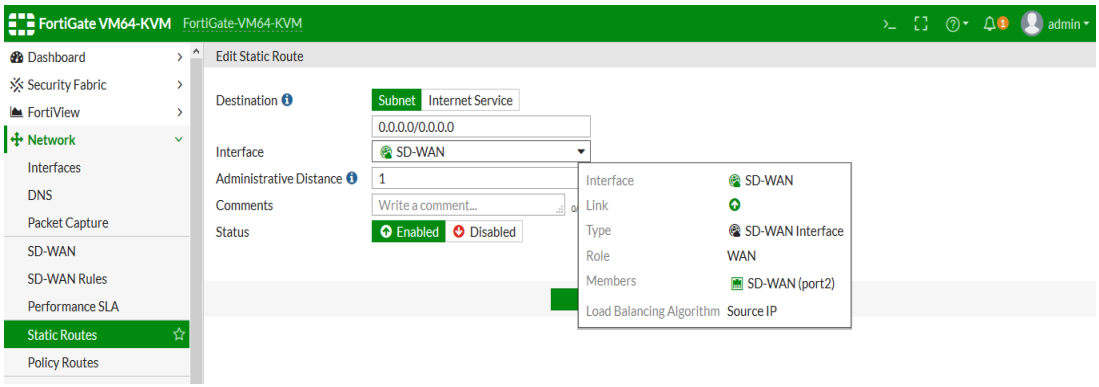


Figura134.Configuracion Static Routes Sucursal 1
Fuente: Los autores

34. Configurar IPv4 policy donde direccionaremos la salida a internet por el enlace SD-WAN a nuestra red local.

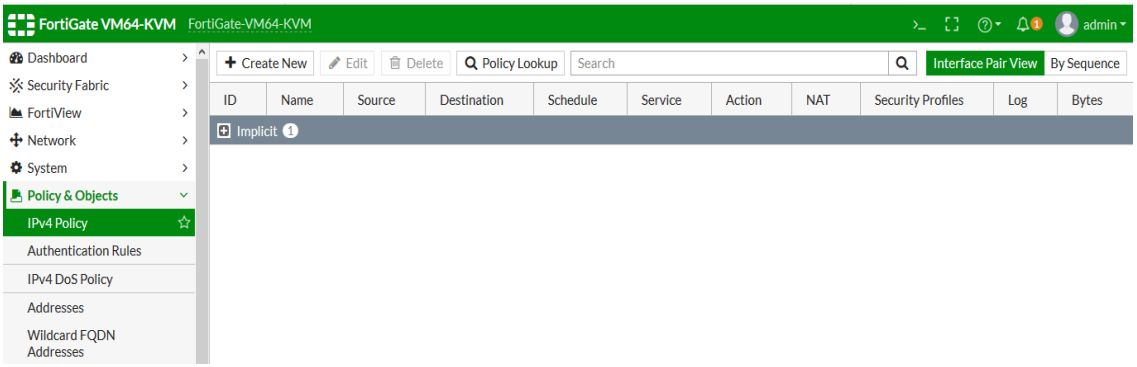


Figura135.Interfaz IPv4 Policy Sucursal 1
Fuente: Los autores

35. Configuración de la regla para internet.

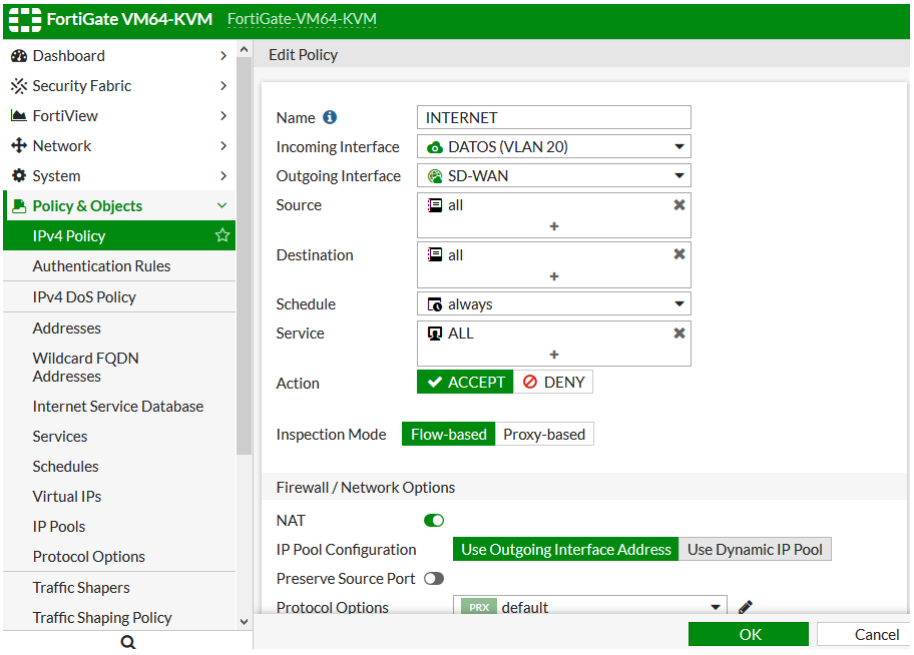


Figura136.Configuracíon IPv4 Policy Sucursal 1
Fuente: Los autores

36. Realizar un ping a la siguiente dirección 8.8.8.8 para verificar la salida de internet del fortigate Sucursal 1.

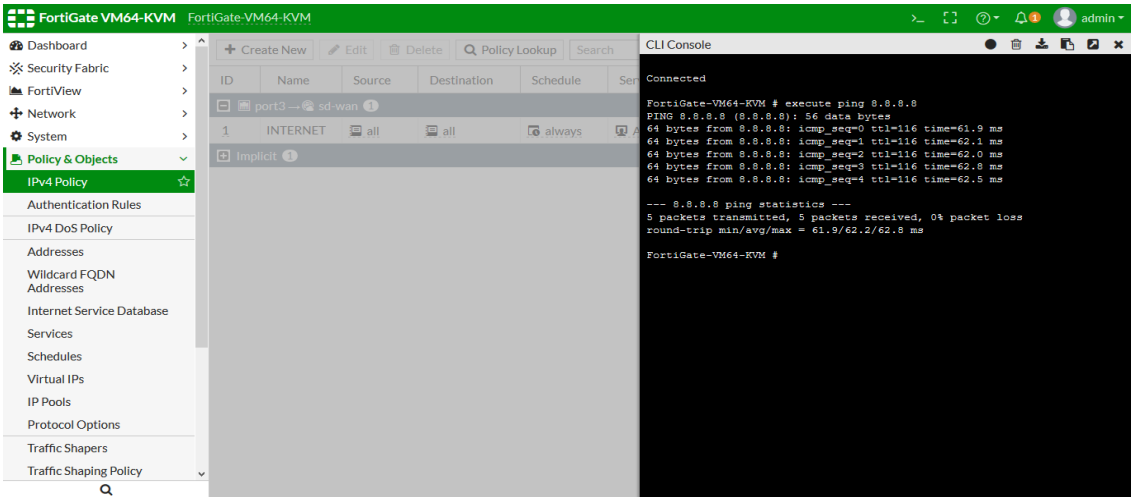


Figura137.Ping Google Fortigate Sucursal 1
Fuente: Los autores

37. Configurar switch con la VLAN 20 para nuestra red local.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name Datos
Switch(config-vlan)#do wr
Building configuration...
Compressed configuration from 3508 bytes to 1558 bytes[OK]
*Sep 17 17:57:02.679: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Sep 17 17:57:03.415: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config-vlan)#exit
Switch(config)#
```

Figura 138. Configuración VLAN 20
Fuente: Los autores

38. Configurar el puerto troncal del switch.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 3/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 3569 bytes to 1596 bytes[OK]
Switch(config-if)#
*Sep 17 18:04:59.721: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Pl
ease wait...
*Sep 17 18:05:00.477: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successf
ully.
Switch(config-if)#exit
Switch(config)#
```

Figura139. Puerto Trunk switch Sucursal 1
Fuente: Los autores

39. Asignar la VLAN 20 a los puertos que vamos usar.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
Compressed configuration from 3620 bytes to 1629 bytes[OK]
Switch(config)#
*Sep 17 18:10:31.058: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Sep 17 18:10:31.813: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config)#
```

Figura 140. Puerto Access VLAN 20
Fuente: Los autores

40. Para asignación de IP de manera automática tecleamos en el CLI la palabra dhcp, show para que nos muestre que IP nos entrega y realizamos un ping a google.

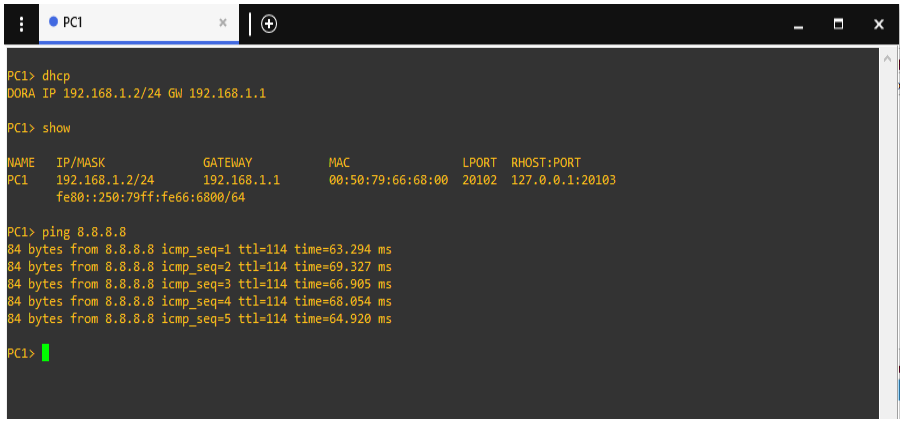


Figura 141. Verificacion de red local y navegación Sucursal 1
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.3. PRÁCTICA 3

Configuración de una red SD-WAN con perfomance SLA en fortigate 6.4.2.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA** Nº 3
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO CONSIDERADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN para el equilibrio de carga con SLA.

OBJETIVOS

General

Configurar equilibrio de carga con SLA.

Específicos

- Configruar la red SD-WAN.
- Configurar preformance SLA.
- Seleccionar la conexiones que tenga menos ping o jitter.

GLOSARIO

PING.- Ping es un instrucción o una herramienta de diagnóstico que consiente realizar una verificación del estado de una determinada conexión o host local.

JITTER.- Jitter es la diferencia de velocidad entre los paquetes más lentos y más rápidos. Esencialmente, es una variación en el retraso. En aplicaciones que son sensibles a los paquetes retrasados, como la transmisión, VoIP o juegos, esto podría afectar negativamente la experiencia del usuario si es demasiado alta.

LACTENCIA.- Es cuando en una red se presenta retardo dentro del tiempo estimado de trasmisión.

PACKET LOSS.- Es cuando en una red se en envían o reciben paquetes de datos y este no llegan a su destino.

SLA.- Se define como un conjunto de condicionamiento que se utiliza para especificar el nivel de servicio que un cliente podría esperar de su proveedor de servicio.

HTTPS.- Es un protocolo que se lo utiliza para la transferecia de datos entre el host y un sevidor utilizando un cifrado ssl para una conexión segura.

DNS.- (acrónimo de Domain Name System) Es un protocolo el cual relaciona el nombre de dominio de una pagina web con su dirección ip publica.

MARCO PROCEDIMENTAL

1. Diseñar la topología de la red para la práctica 3.

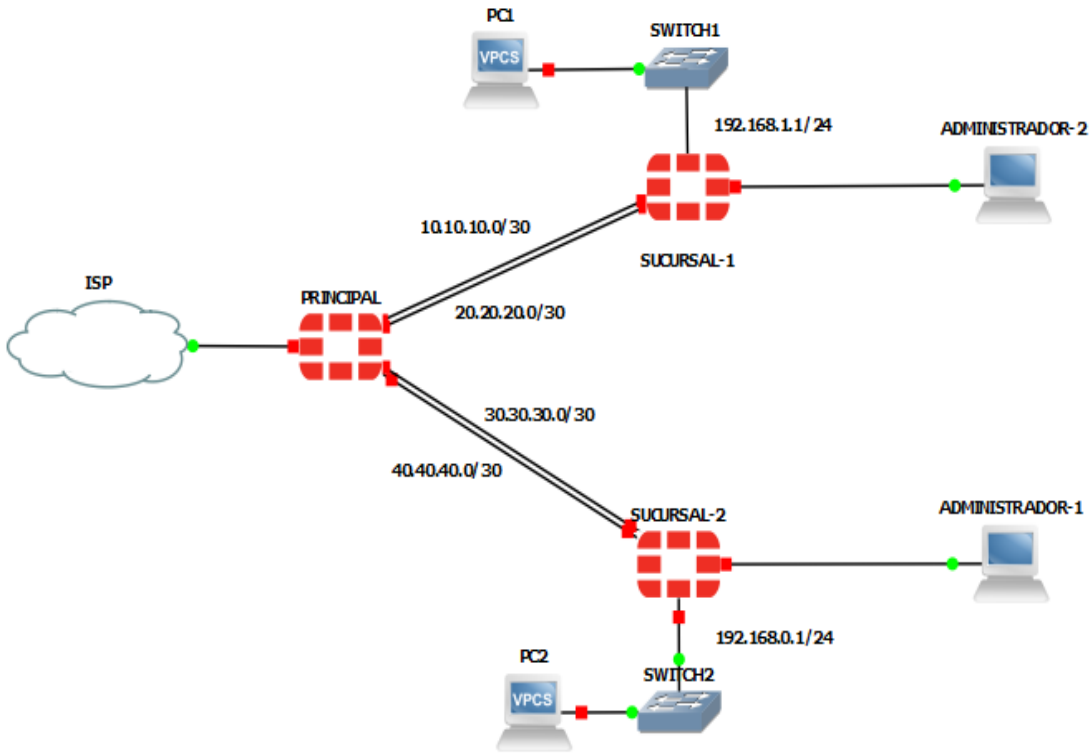


Figura 142. Diseño de la red práctica Nº3
Fuente: Los autores

2. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

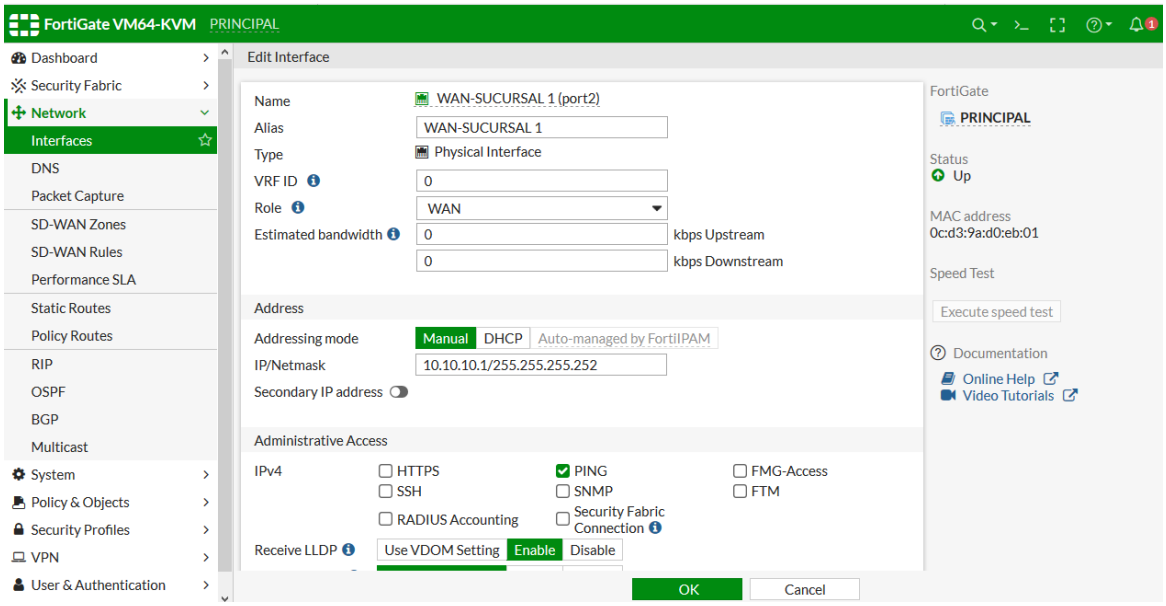


Figura 143.Configuracion IP fortigate principal port2
Fuente: Los autores

3. Configurar la dirección IP en puerto 3 en el fortigate principal para el enlace wan para el fortigate sucursal 1.

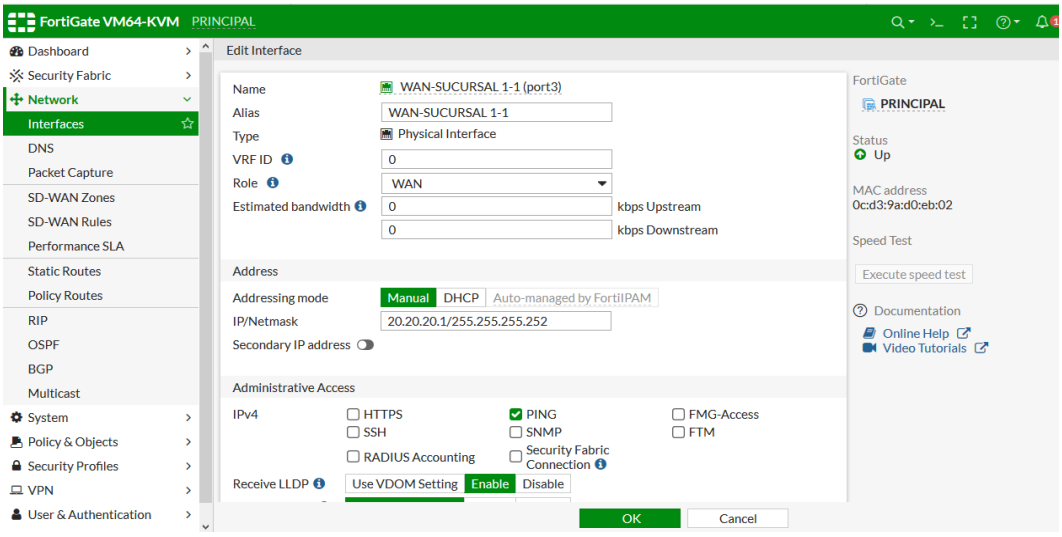


Figura 144.Configuracion IP fortigate principal port3
Fuente: Los autores

4. Configurar la dirección ip en el puerto 4 en el fortigate principal para el enlace wan para el fortigate sucursal 2.

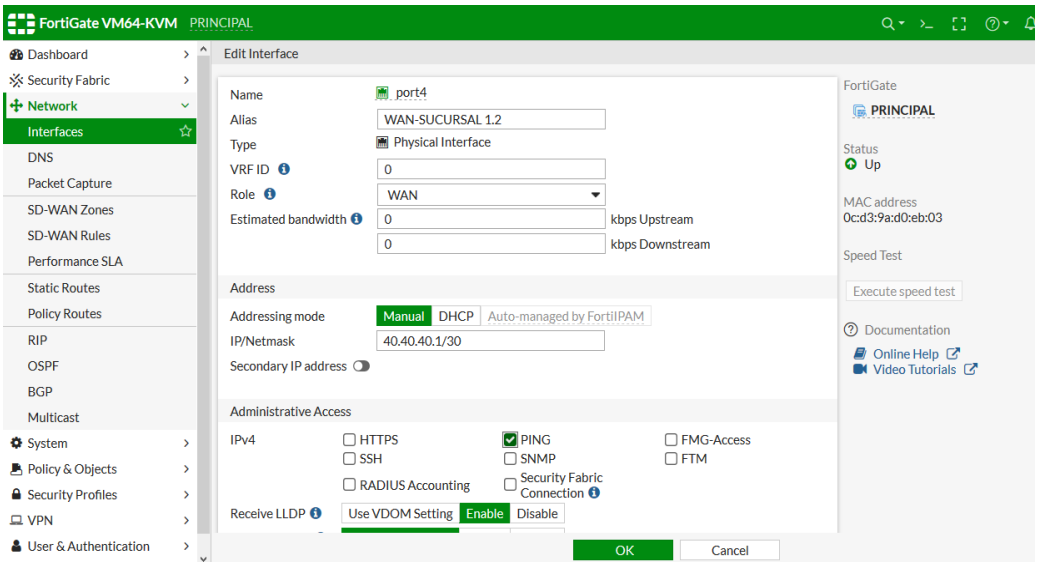


Figura 145.Configuracion IP fortigate principal port4
Fuente: Los autores

5. Configurar la dirección IP en el puerto 5 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

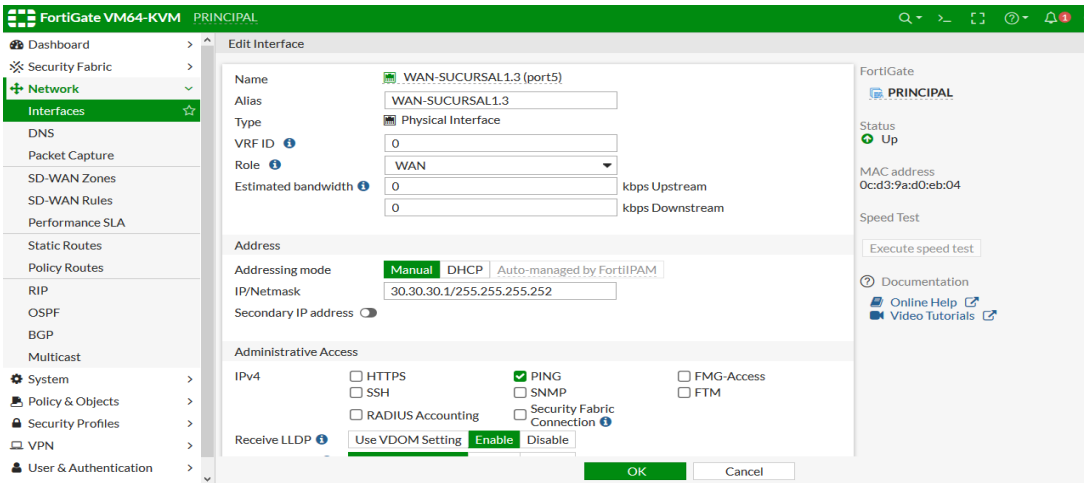


Figura 146.Configuracion IP fortigate principal port5
Fuente: Los autores

6. Crear una zona de interfaces para añadir una sola regla en el policy IPv4 en el fortigate principal.

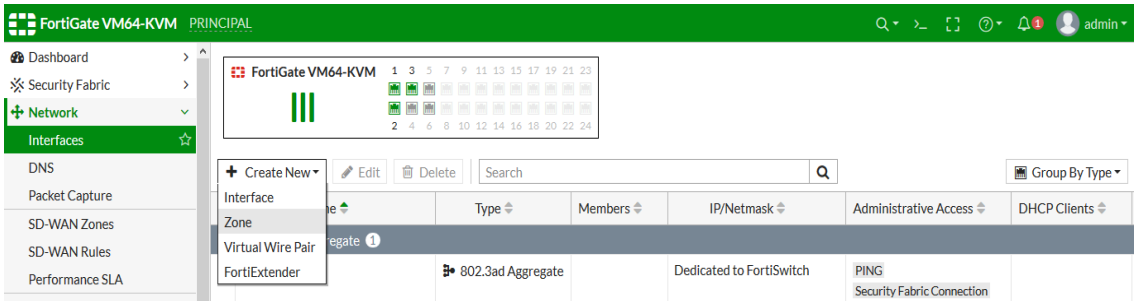


Figura 147. Crear zonas de interfaces
Fuente: Los autores

7. Damos nombre a la zone y arrastar las interfaces a que van unir en la interface para el fortigate surcusal 1.

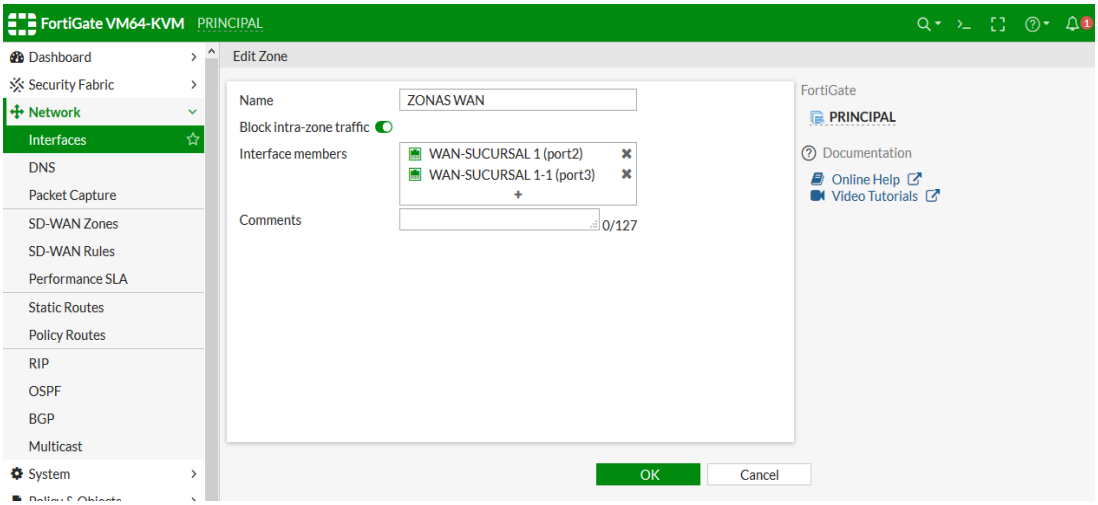


Figura 148. Interface members fortigate principal
Fuente: Los autores

8. Damos nombre a la zone y arrastar las interfaces a que van unir en una la interface para el fortigate sucursal 2.

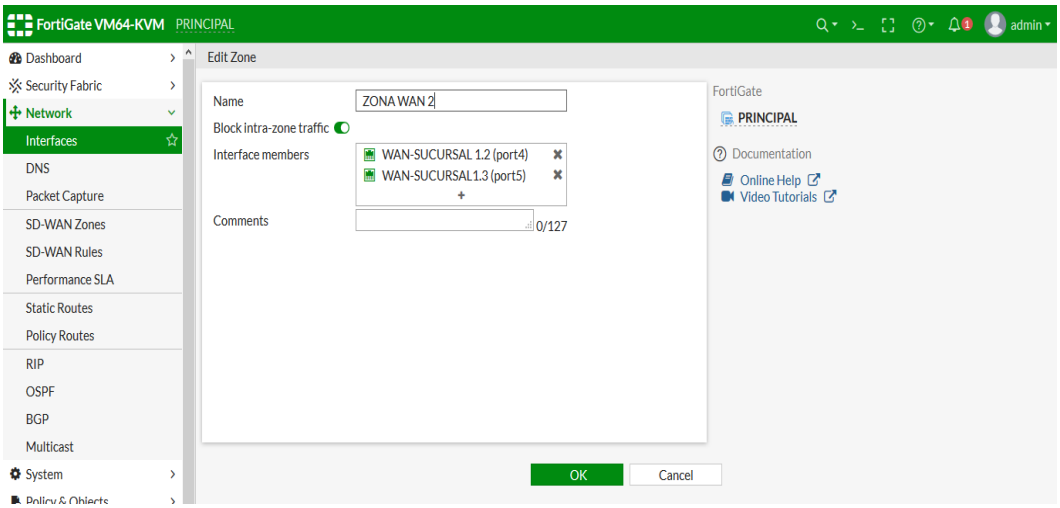


Figura 149. Interface members fortigate principal
Fuente: Los autores

9. Configurar static routes para el fortigate principal, le damos click en la opción dynamic y obtendrá el Gateway del router principal.

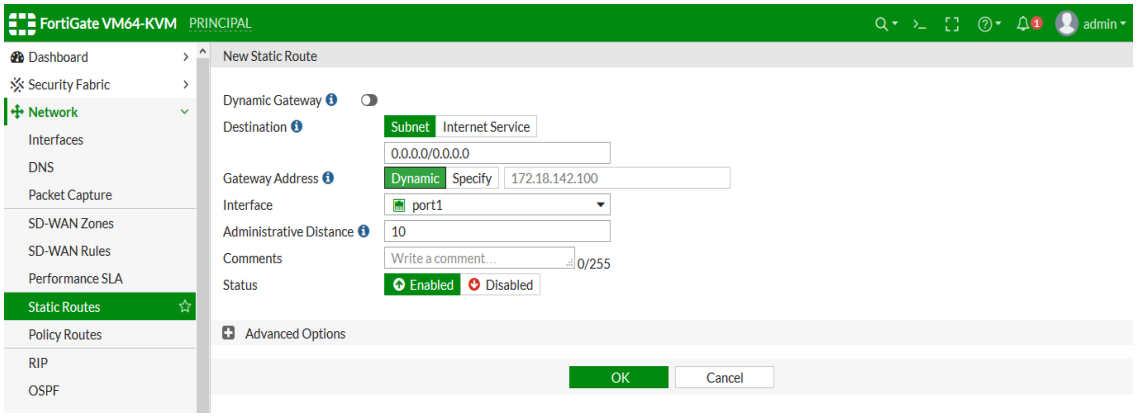


Figura 150. Static routes fortigate principal
Fuente: Los autores

10. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 1.

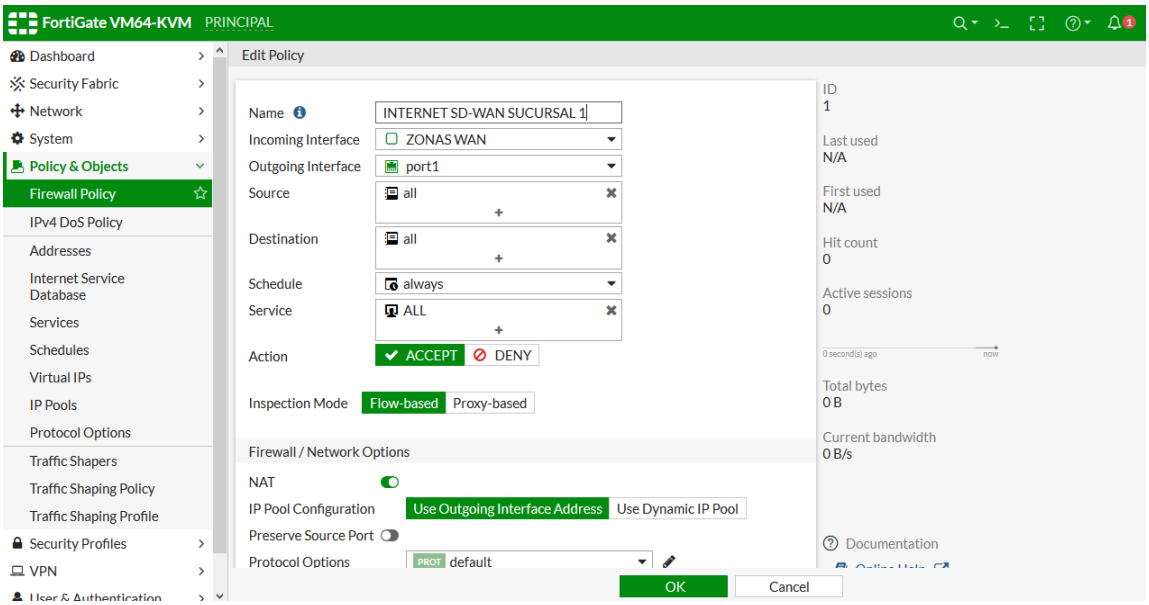


Figura 151. Regla de internet para el fortigate sucursal 1
Fuente: Los autores

11. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 2.

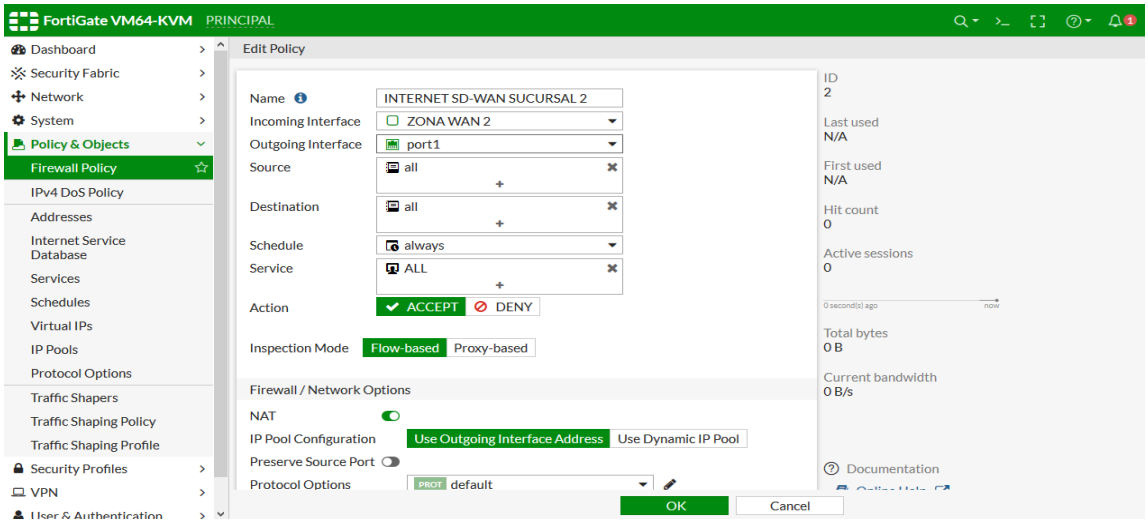


Figura 152. Regla de internet para fortigate sucursal 2
Fuente: Los autores

12. Configurar la dirección IP al port2 del fortigate de la sucursal 1.

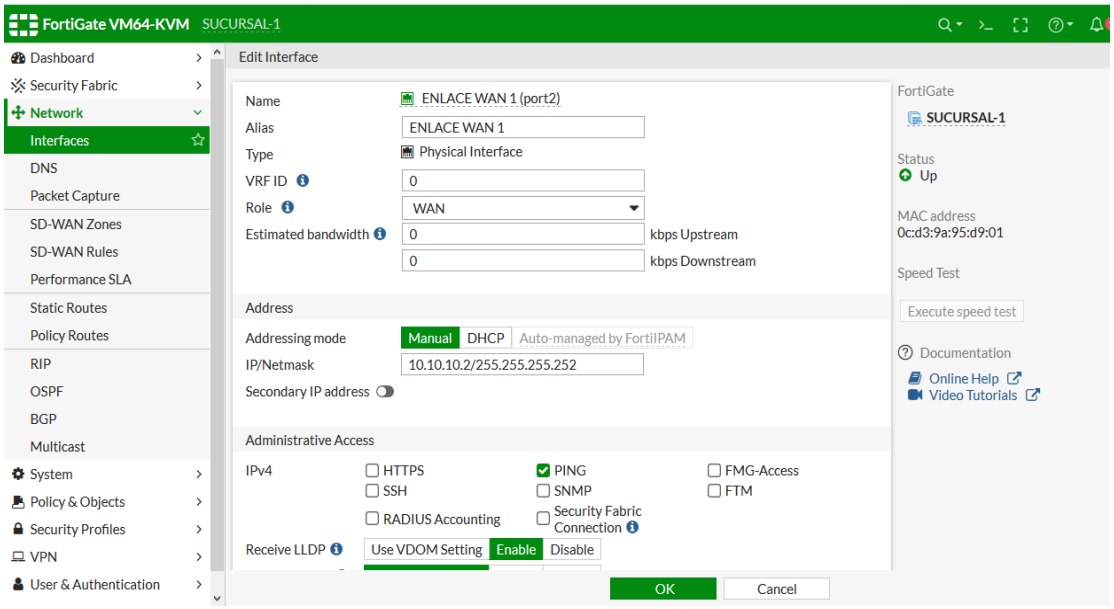


Figura 153. Dirección IP port2 fortigate sucursal 1
Fuente: Los autores

13. Configurar la dirección IP al port3 del fortigate de la sucursal 1.

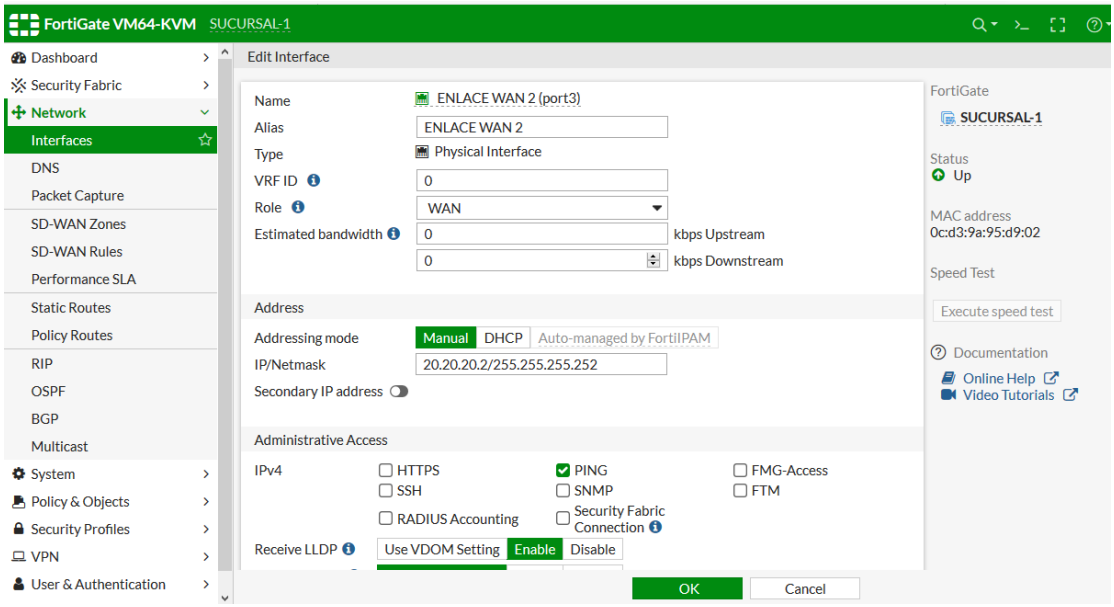


Figura 154. Dirección IP port3 fortigate sucursal 1
Fuente: Los autores

14. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal.

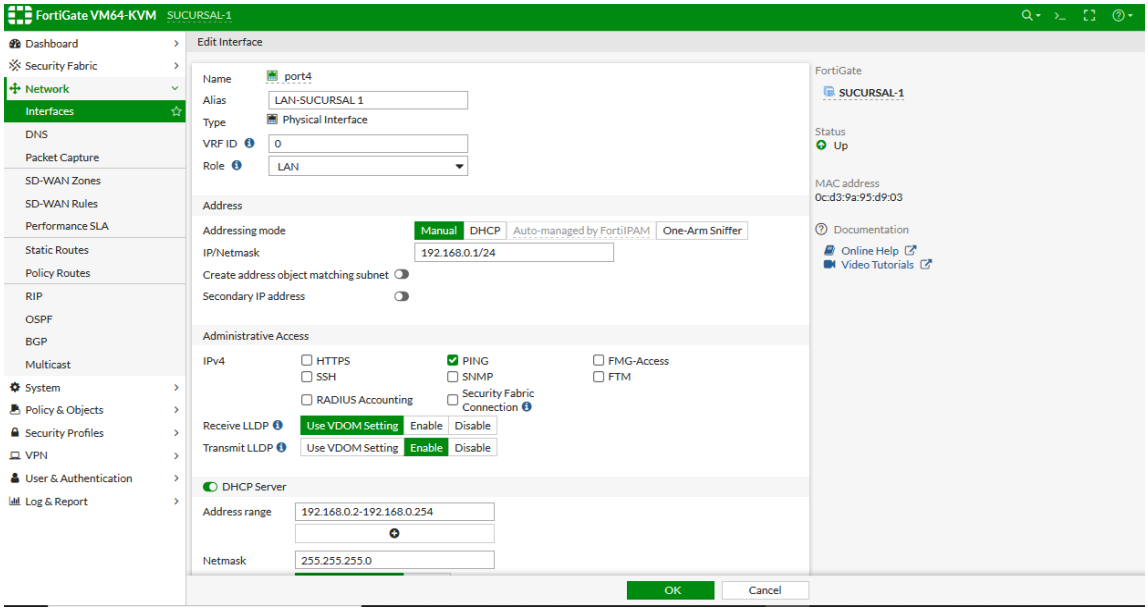


Figura 155. Configuración red local del fortigate
Fuente: Los autores

15. Crear SD-WAN Member en la sucursal 1.

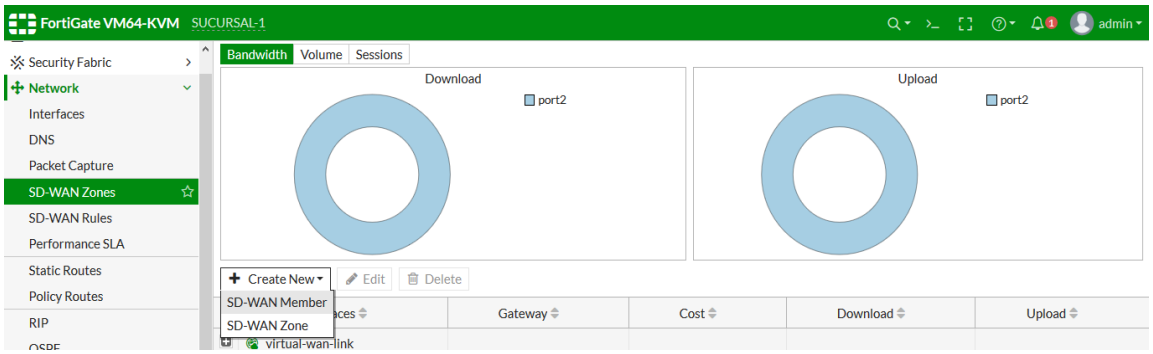


Figura 156. SD-WAN zone fortigate sucursal 1
Fuente: Los autores

16. Crear SD-WAN para la interface enlace WAN 1.

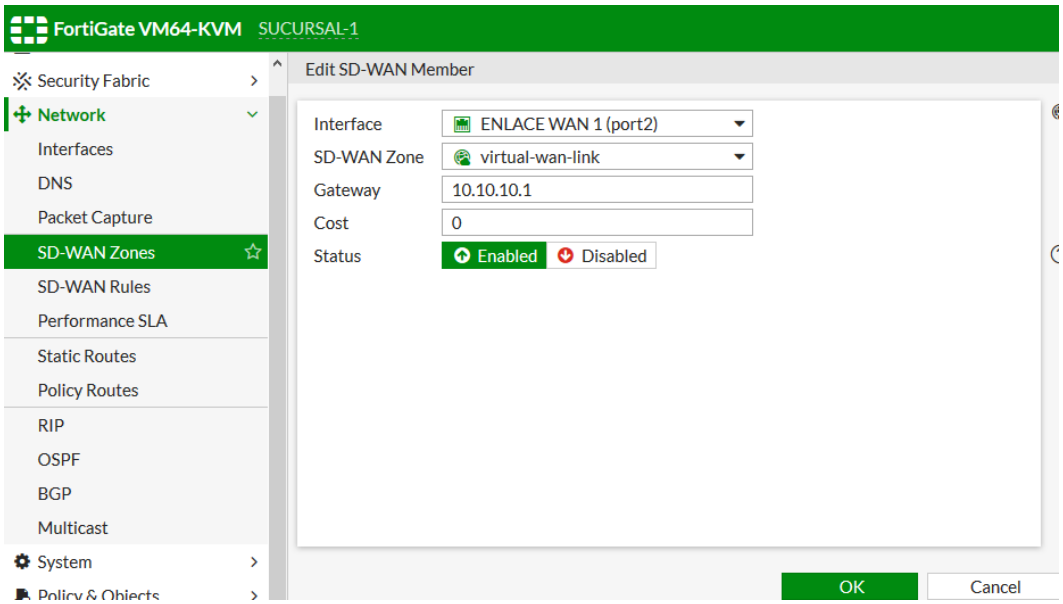


Figura 157. SD-WAN enlace wan 1
Fuente: Los autores

17. Crear SD-WAN para la interface enlace WAN 2.

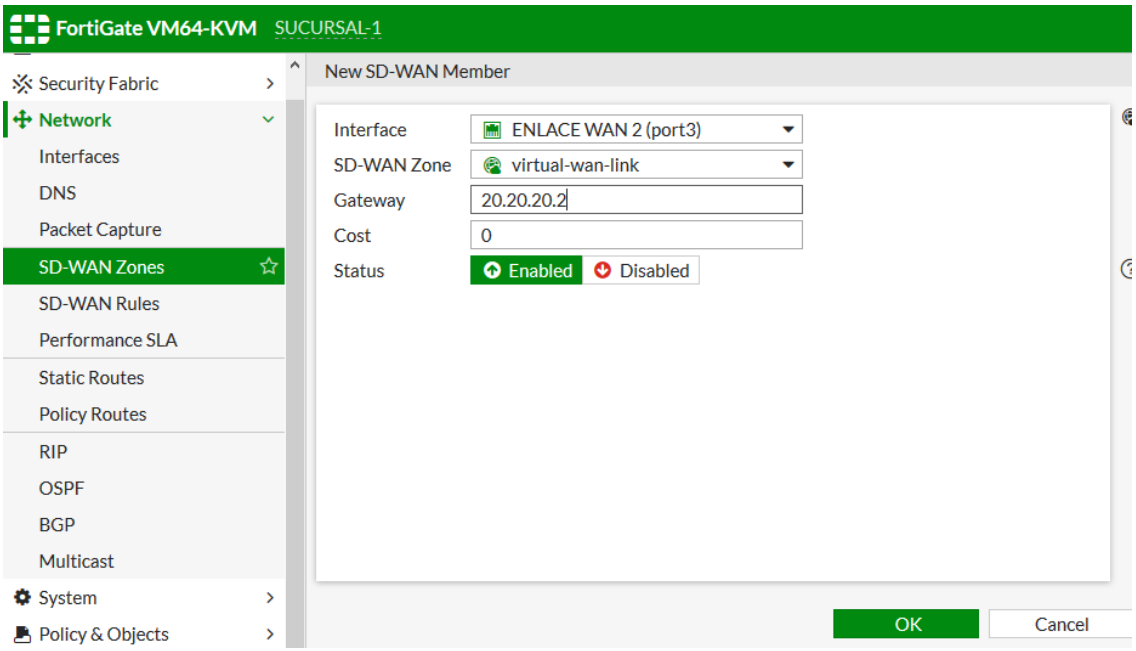


Figura 158. SD-WAN enlace WAN 1
Fuente: Los autores

18. Configurar static routes para la SD-WAN.

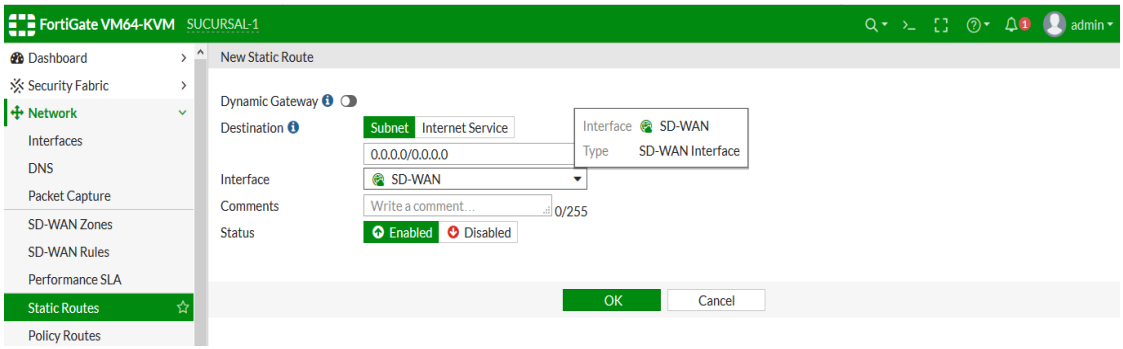


Figura 159. Static routes para SD-WAN fortigate sucursal 1
Fuente: Los autores

19. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 1.

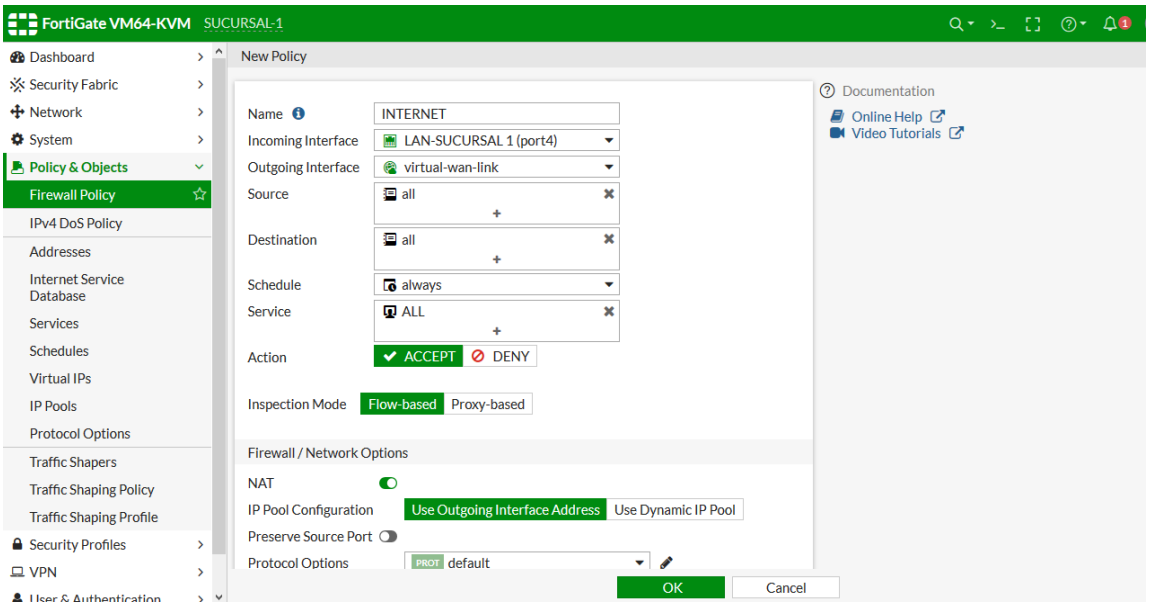


Figura 160. Static routes para SD-WAN fortigate sucursal 1
Fuente: Los autores

20. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos ping o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new.

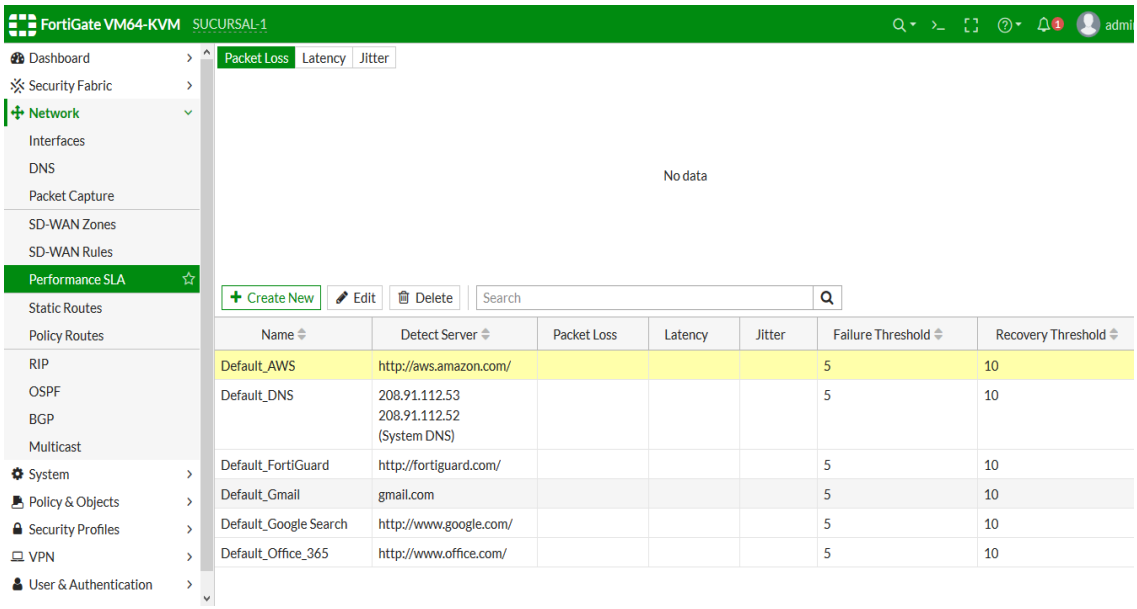


Figura 161. Configuración de static routes SD-WAN del fortigate
Fuente: Los autores

21. Realizar un SLA a travez de ping a google salga a travez de la SD-WAN.

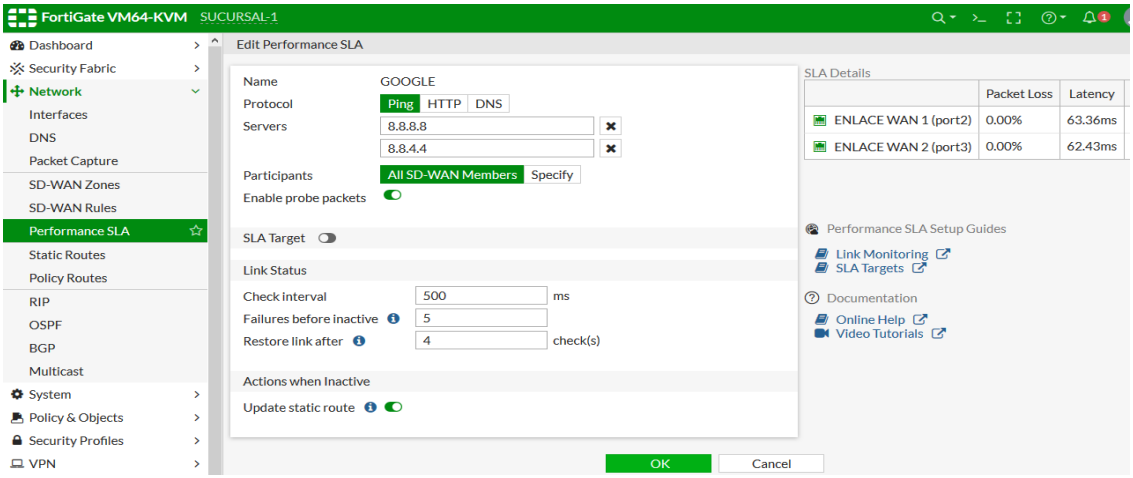


Figura 162. Configuración de static routes SD-WAN del fortigate
Fuente: Los autores

22. Veremos que tenemos menos ping y jiptter en una de las interfaces configuradas donde sd-wan eligue en enlace con mejor calidad de servicios.

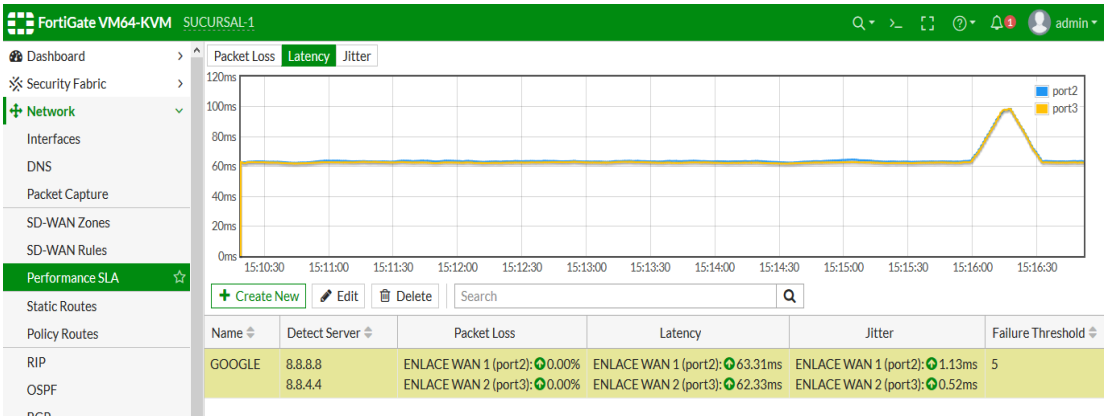


Figura 163. Diagrama de calidad de sevicio de sucrusal 1
Fuente: Los autores

23. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

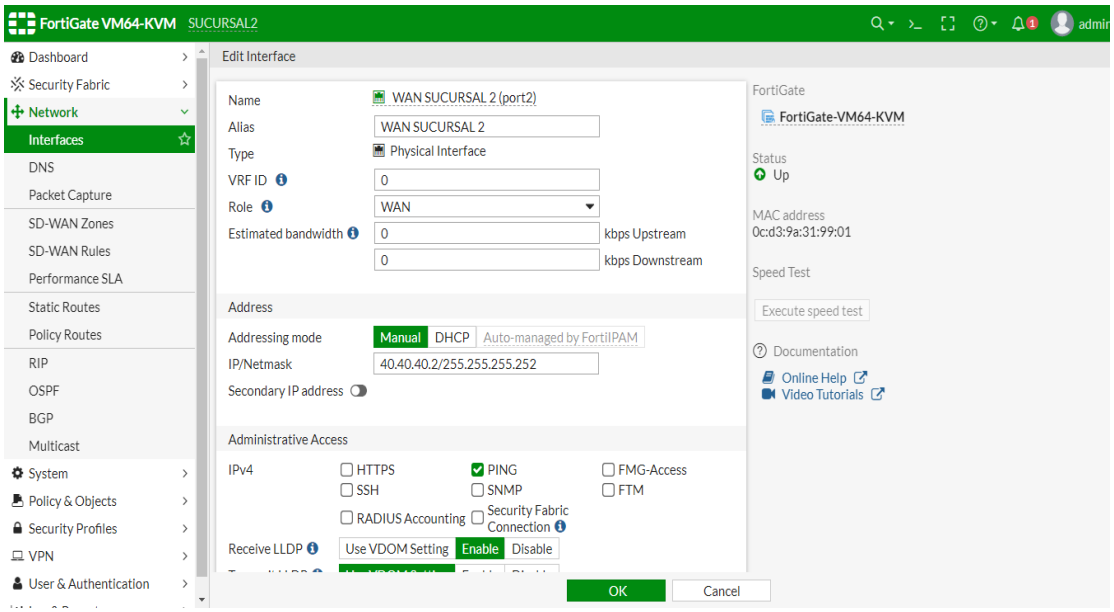


Figura 164. Configuracion IP fortigate WAN sucrsal 2
Fuente: Los autores

24. Configurar la dirección IP en puerto 3 en el frotigate principal para el enlace wan para el fortigate sucursal 2.

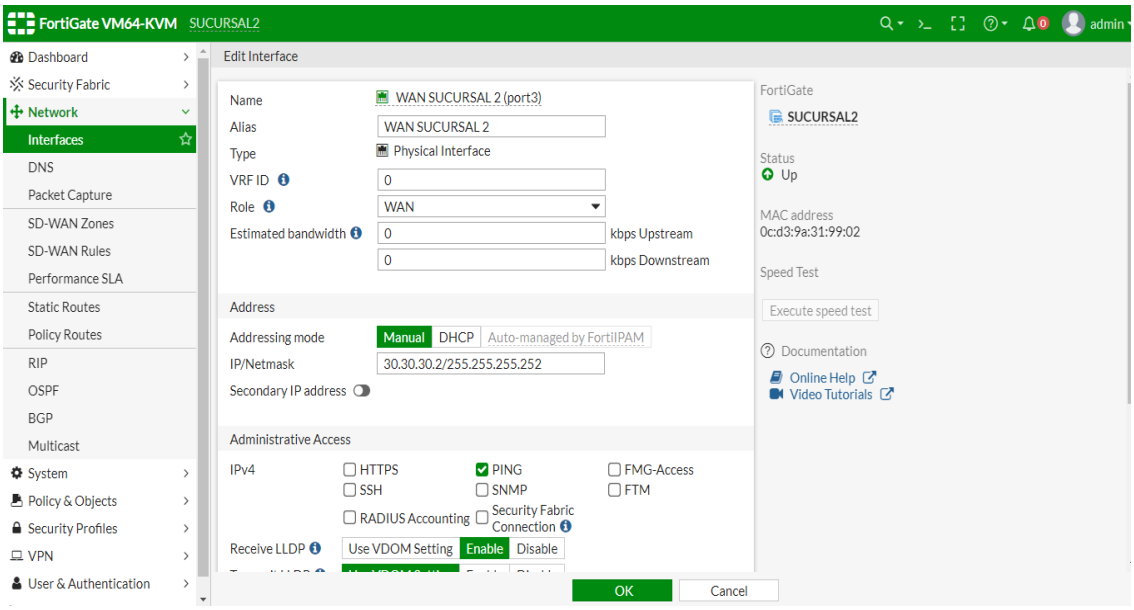


Figura 165. Configuracion IP fortigate WAN sucursal 2
Fuente: Los autores

25. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal 2.

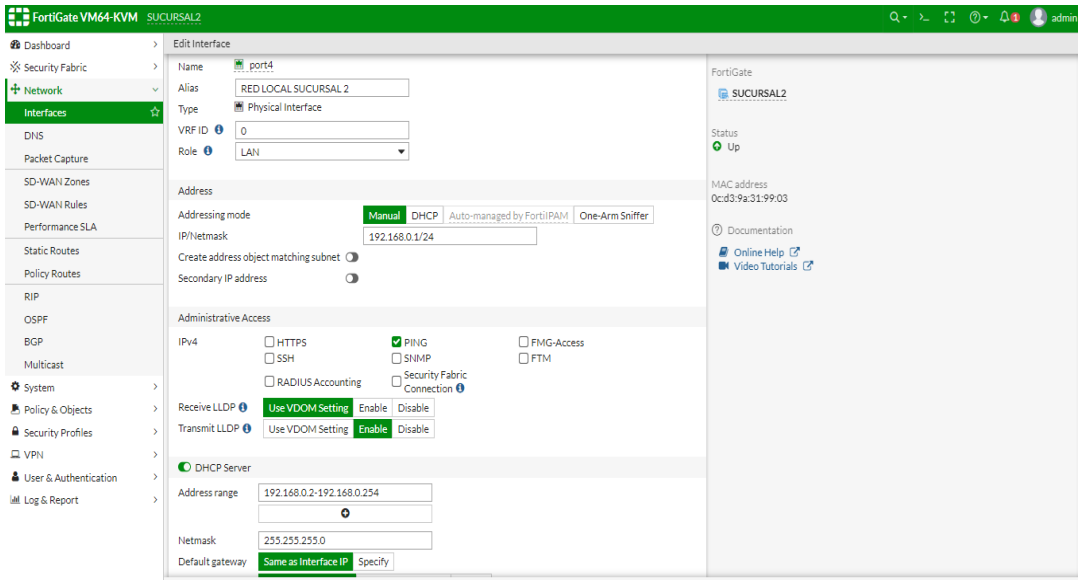


Figura 166. Configuración red local del fortigate
Fuente: Los autores

26. Crear SD-WAN Member en la sucursal 2.

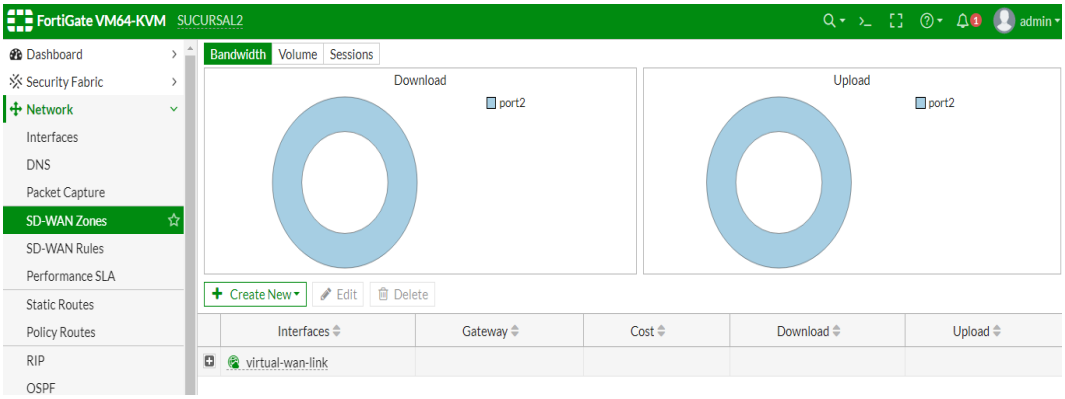


Figura 167.SD-WAN zone fortigate sucursal 2
Fuente: Los autores

27. Crear SD-WAN para la interface sucursal 2.

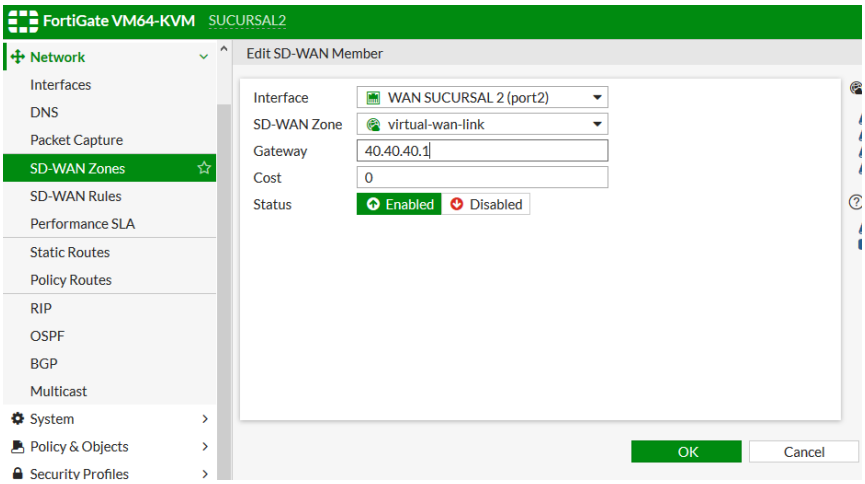


Figura 168. SD-WAN sucursal 2 para puerto 2
Fuente: Los autores

28. Crear SD-WAN para la interface sucursal 2.

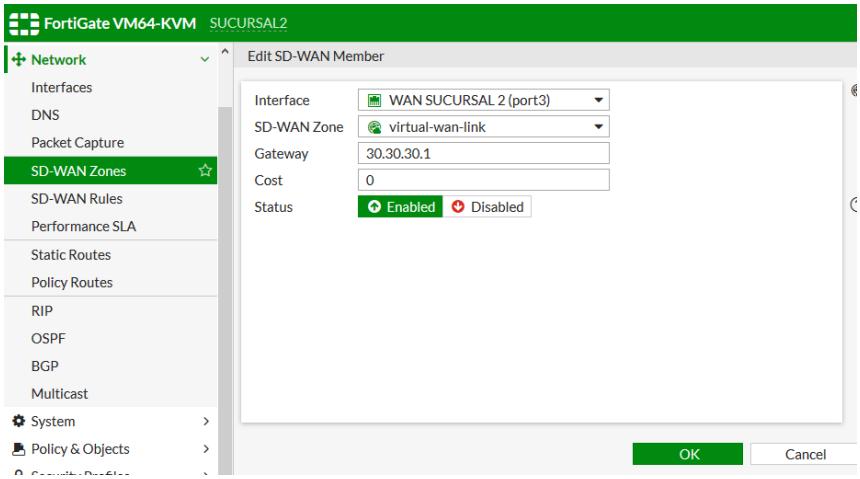


Figura 169. SD-WAN sucursal 2 para puerto 3
Fuente: Los autores

29. *C*onfigurar static routes para la SD-WAN sucursal 2.

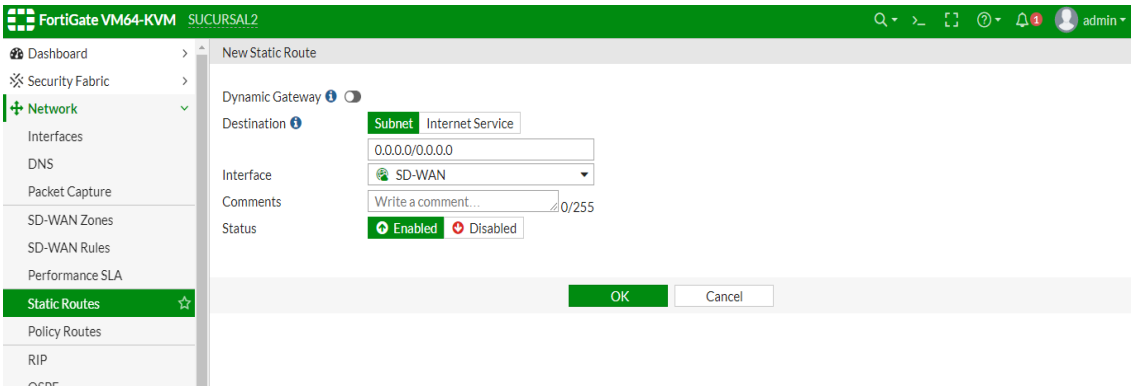


Figura 170. Static routes para SD-WAN fortigate sucursal 2
Fuente: Los autores

30. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 2.

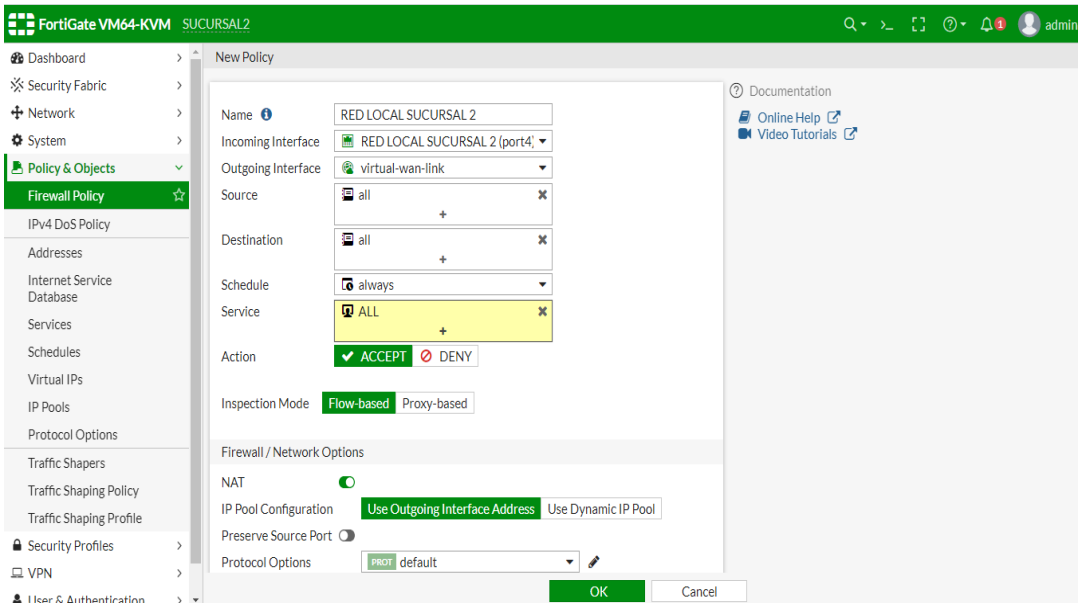


Figura 171. Static routes para sd-wan fortigate sucursal 2
Fuente: Los autores

31. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos ping o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new para sucursal 2.

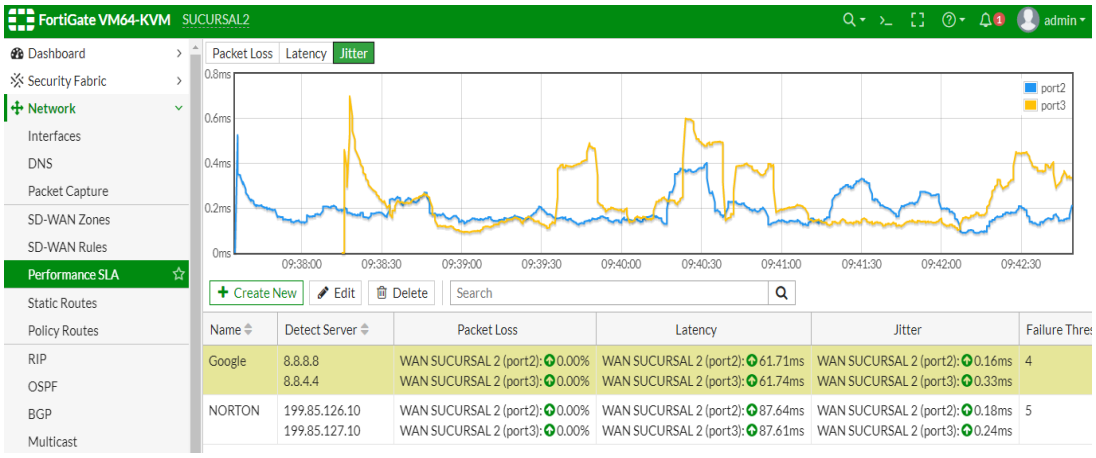


Figura.172 Gráficas la sucursal 2

Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA

- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.4. PRÁCTICA 4

Configuración de una red SD-WAN con prioridad de servicios con sd-wan rules.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA** Nº 4
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con prioridad de servicios con sd-wan rules.

OBJETIVOS

General

Configurar el balanceo de carga con SD-WAN rules

Específicos

- Configurar uan red SD-WAN.
- Establecer configuraciones de SD-WAN rules.
- Calidad de servicios al enlace SD-WAN.

GLOSARIO

SD-WAN RULES.- Son reglas que se utilizan para examinar como se divide las sesiones a los miembros de SD-WAN

PING.- Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión o host local**.**

JITTER.- Jitter es la diferencia de velocidad entre los paquetes más lentos y más rápidos. Esencialmente, es una variación en el retraso. En

aplicaciones que son sensibles a los paquetes retrasados, como la transmisión, VoIP o juegos, esto podría afectar negativamente la experiencia del usuario si es demasiado alta.

LACTENCIA.- Es cuando en una red se presenta retardo dentro del tiempo estimado de trasmisión.

PACKET LOSS.- Es cuando en una red se en envían o reciben paquetes de datos y este no llegan a su destino.

MAXIMIZE BANDWIDTH (SLA).- El tráfico se distribuye entre todos los enlaces disponibles según el algoritmo de equilibrio de carga seleccionado.

LOWEST COST (SLA).- A las interfaces se les asigna una prioridad en función de la configuración de SLA seleccionada.

BEST QUALITY.- A la interfaz se le asigna una prioridad basada en el factor de costo de enlace de la interfaz

MARCO PRODECIMENTAL

1. Diseñar la topología de la red para la prática 4.

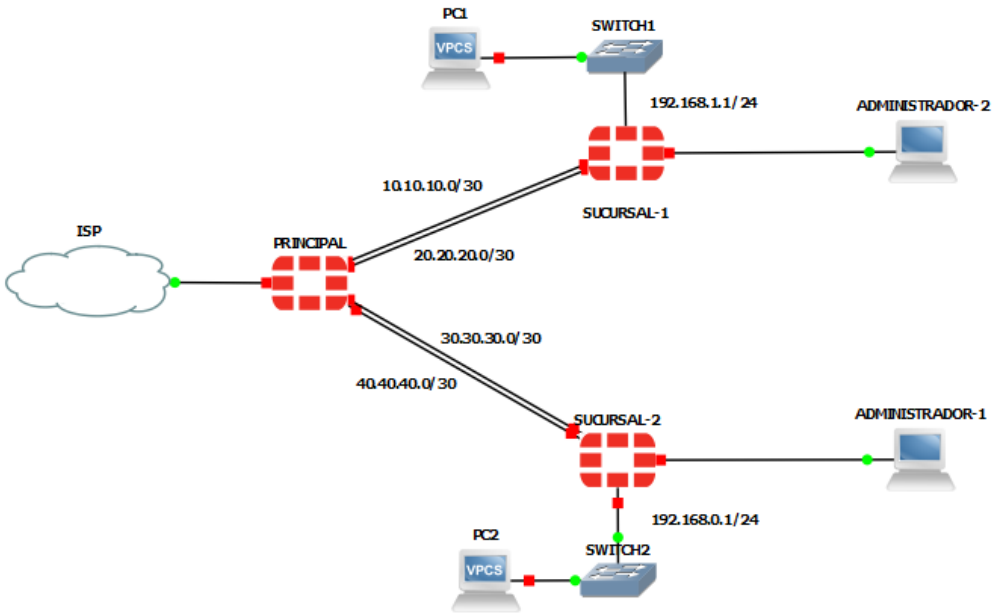


Figura 173. Diseño de la red práctica Nº4
Fuente: Los autores

2. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

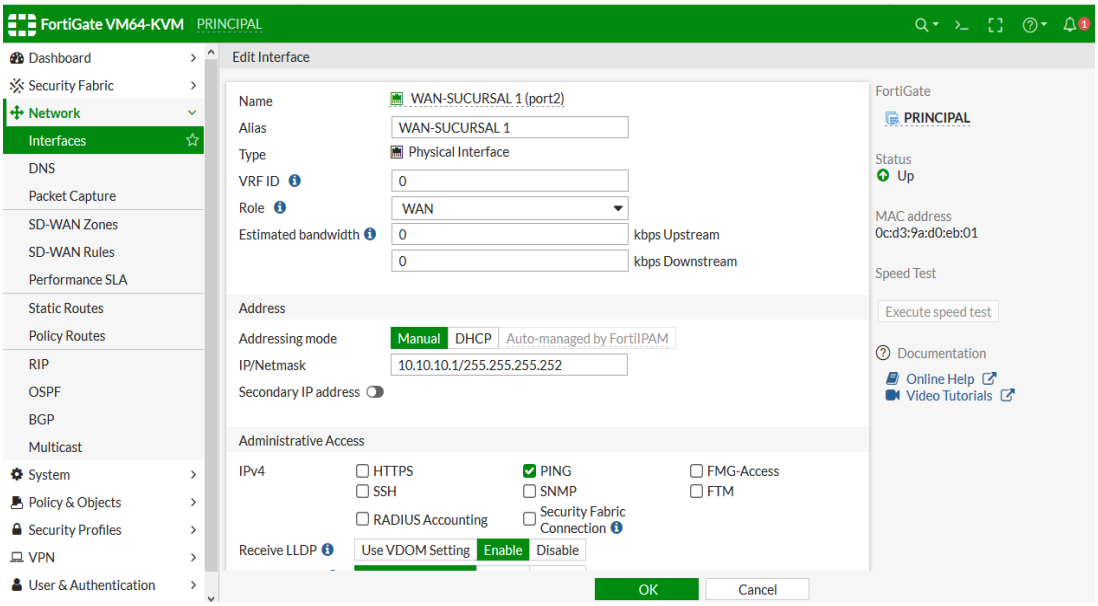


Figura 174.Configuracion IP fortigate principal port2
Fuente: Los autores

3. Configurar la dirección IP en puerto 3 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

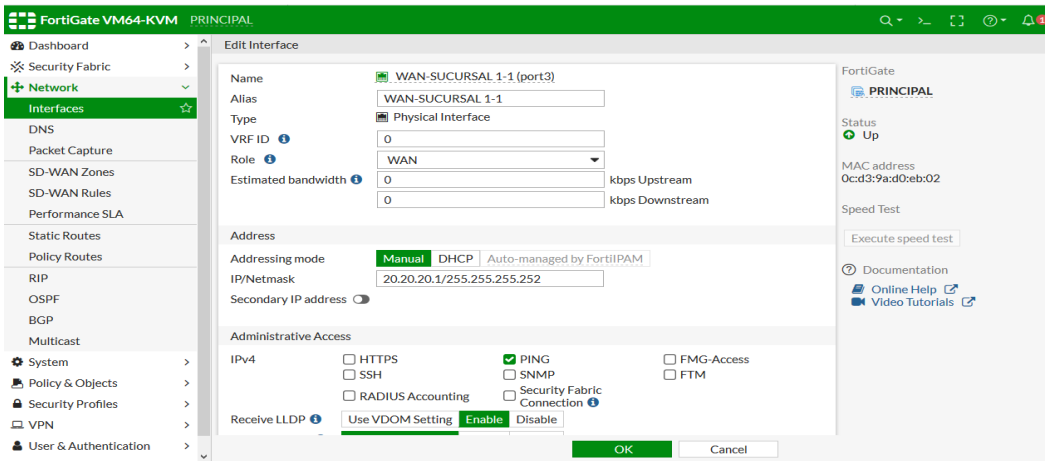


Figura 175.Configuracion IP fortigate principal port3
Fuente: Los autores

4. Configurar la dirección IP en el puerto 4 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

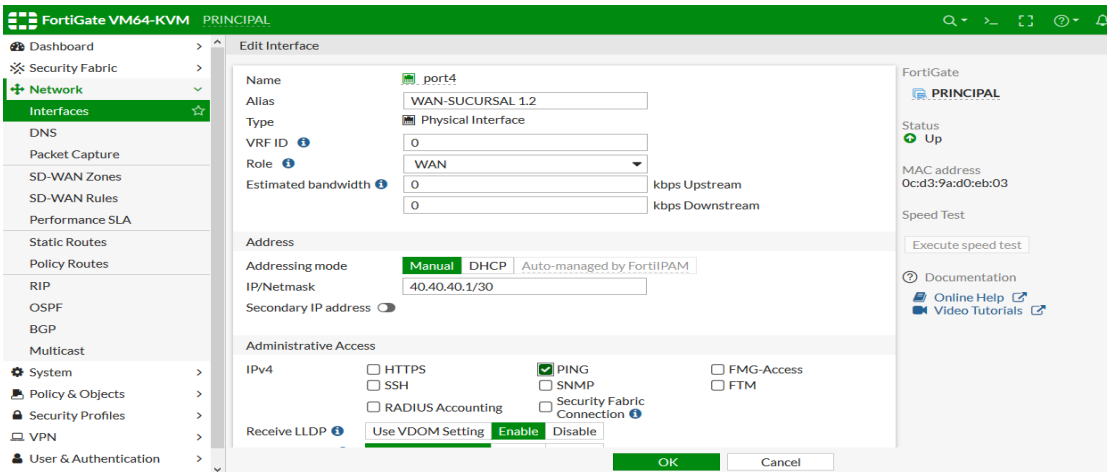


Figura 176.Configuracion IP fortigate principal port4
Fuente: Los autores

5. Configurar la dirección IP en el puerto 5 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

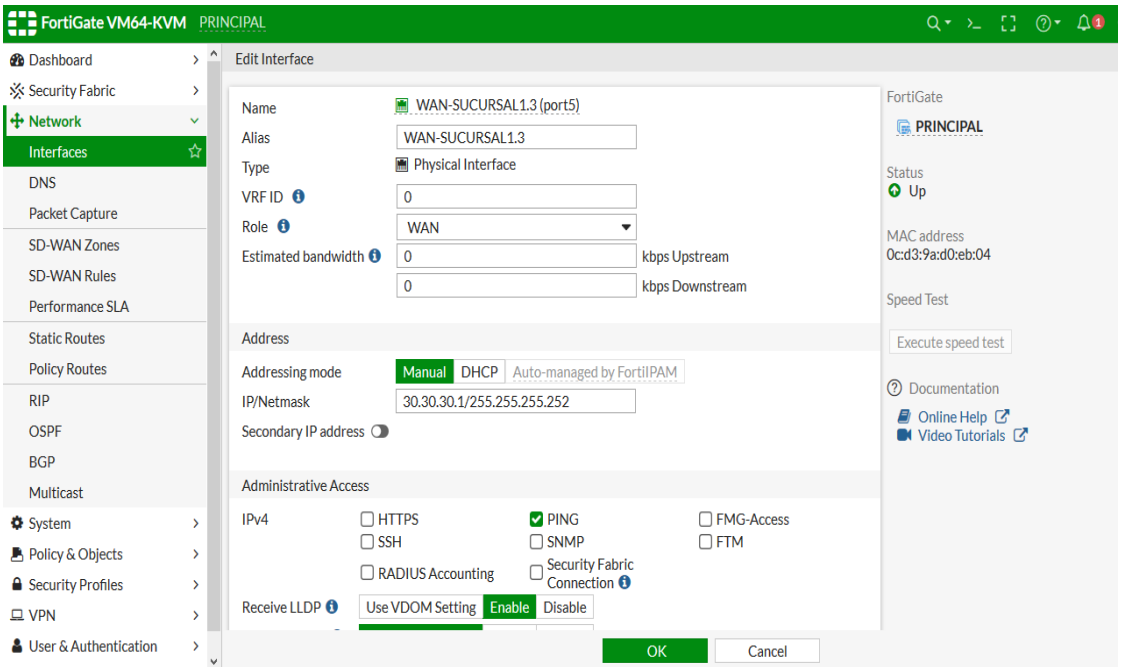


Figura 177.Configuracion IP fortigate principal port5
Fuente: Los autores

6. Crear una zona de interfaces para añadir una sola regla en el policy IPv4 en el fortigate principal.

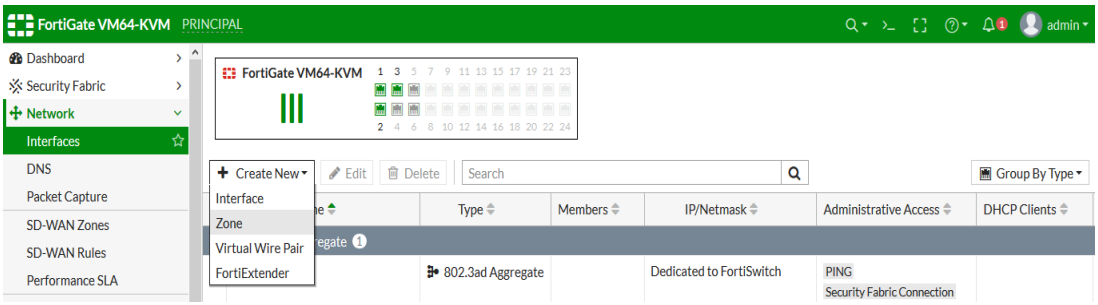


Figura 178. Crear zonas de interfaces
Fuente: Los autores

7. Damos nombre a la zone y arrastar las interfaces a que van unir en la interface para el fortigate surcusal 1.

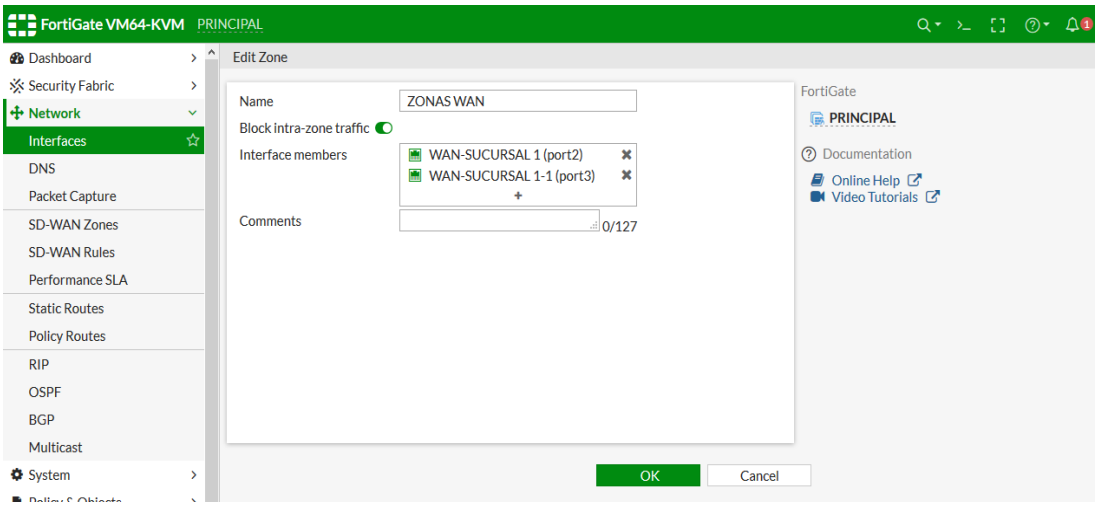


Figura 179. Interface members fortigate principal
Fuente: Los autores

8. Damos nombre a la zone y arrastar las interfaces a que van unir en una la interface para el fortigate sucursal 2.

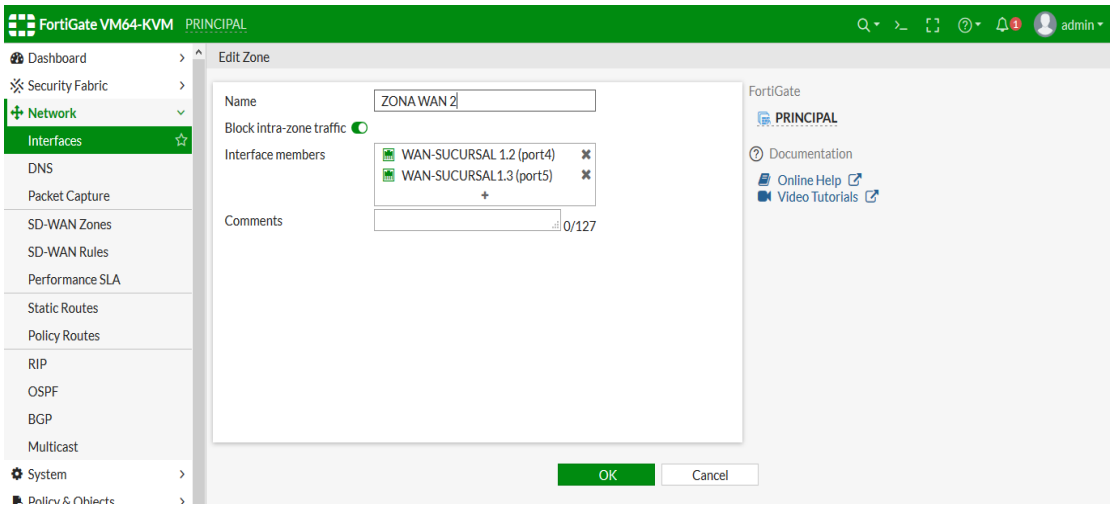


Figura 180. Interface members fortigate principal
Fuente: Los autores

9. Configurar static routes para el fortigate principal, le damos click en la opción dynamic y obtendrá el dns del router principal.

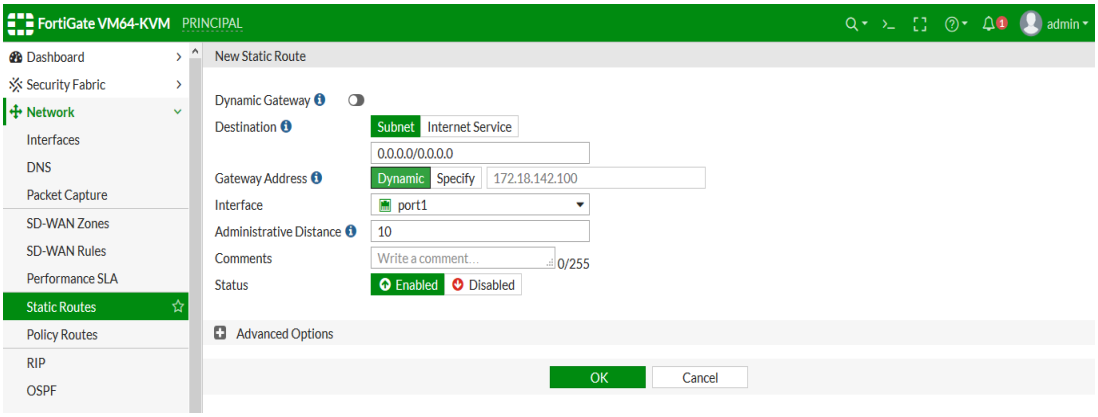


Figura 181. Static routes fortigate principal
Fuente: Los autores

10. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 1.

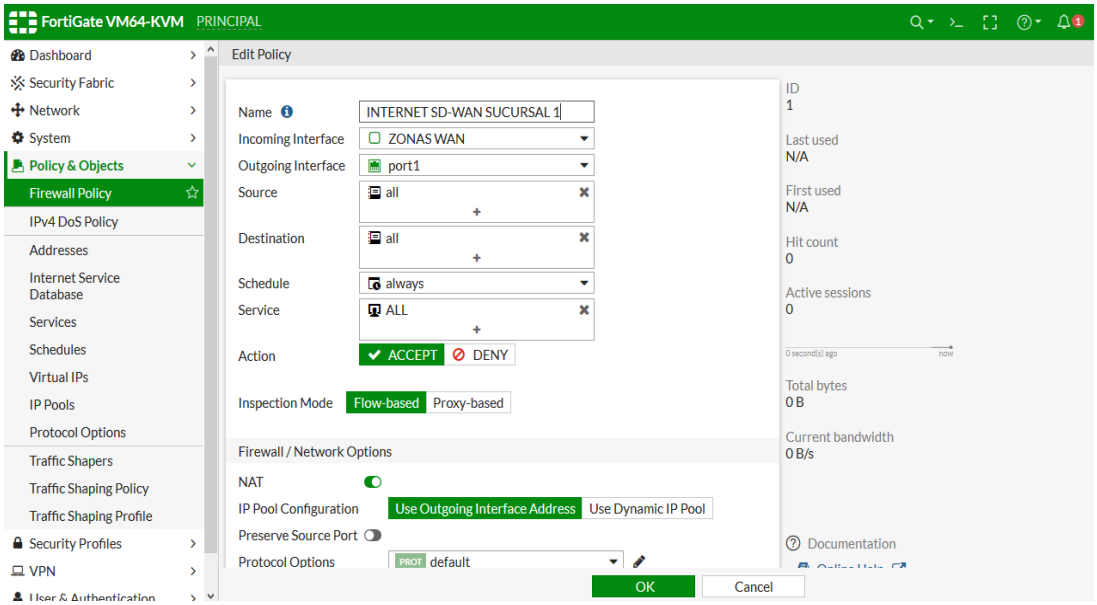


Figura 182. Regla de internet para el fortigate sucursal 1
Fuente: Los autores

11. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 2.

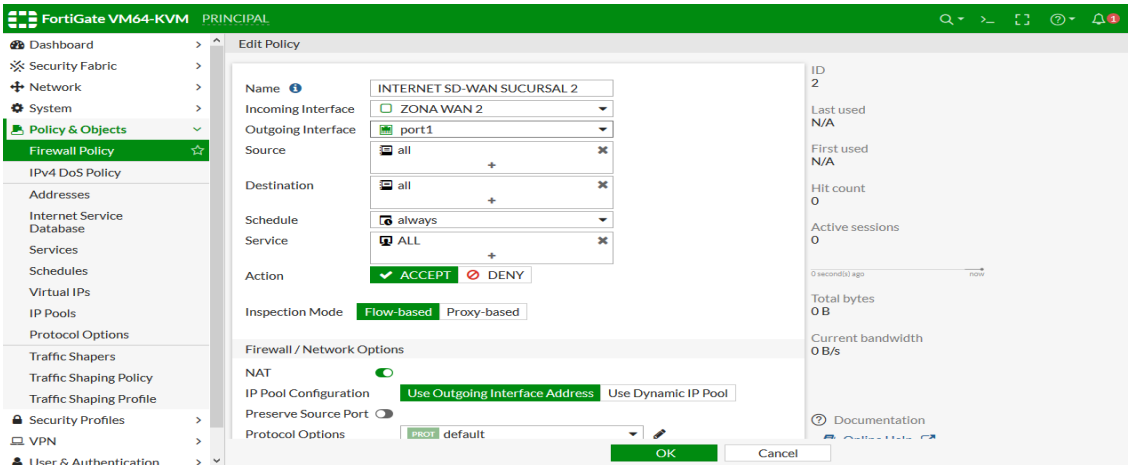


Figura 183. Regla de internet para fortigate sucursal 2
Fuente: Los autores

12. Configurar la dirección IP al port2 del fortigate de la sucursal 1.

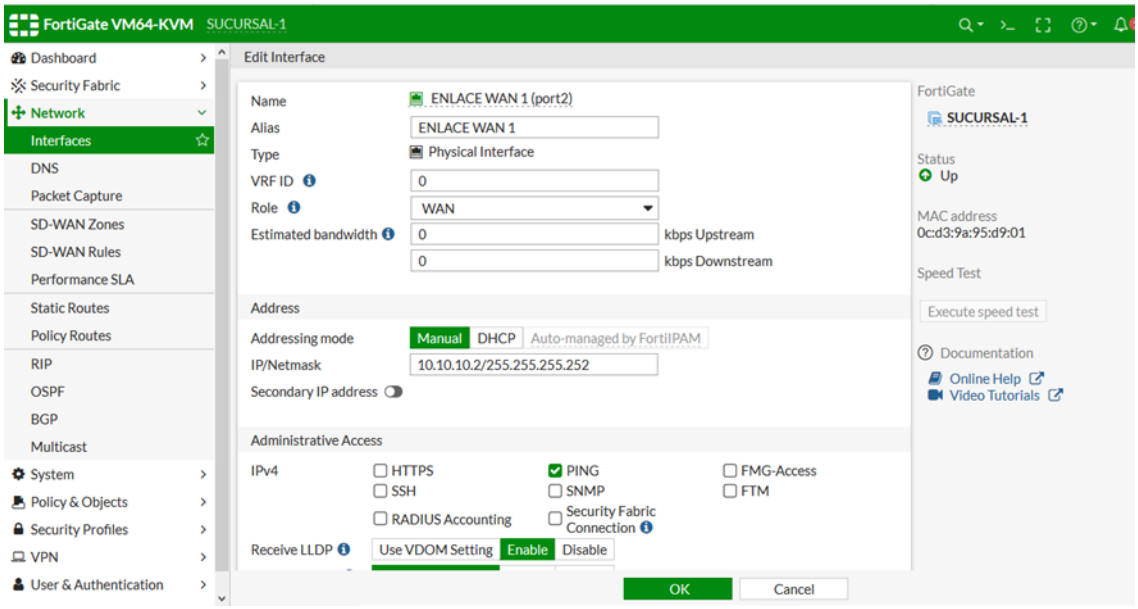


Figura 184. Dirección IP port2 fortigate sucursal 1
Fuente: Los autores

13. Configurar la dirección IP al port3 del fortigate de la sucursal 1.

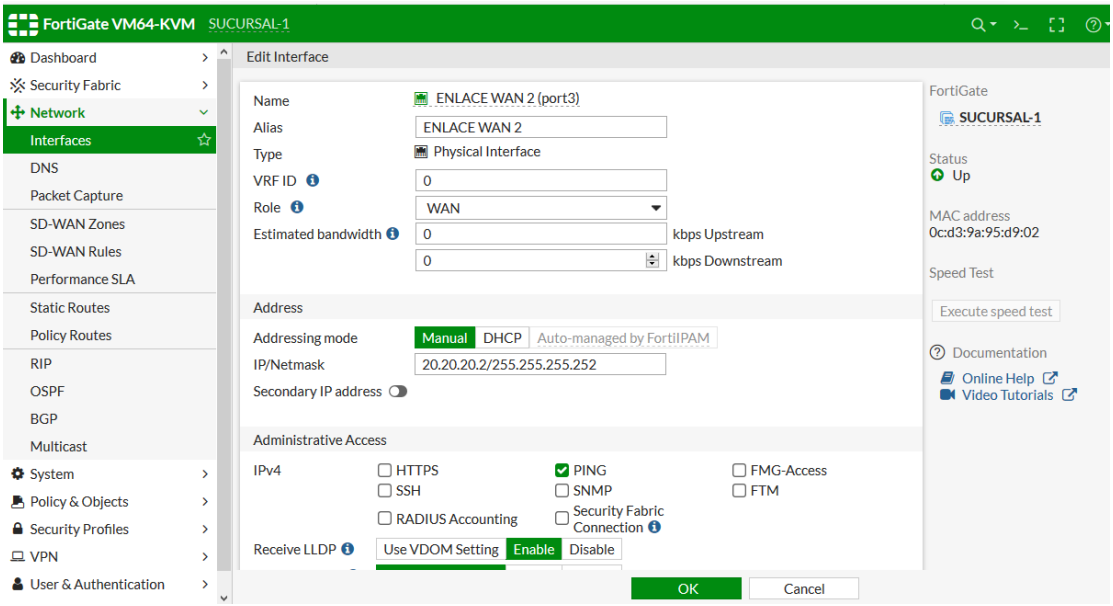


Figura 185. Dirección IP port3 fortigate sucursal 1
Fuente: Los autores

14. Configurar la interface port4 para la red local con su dhcp del fortigate sucursal.

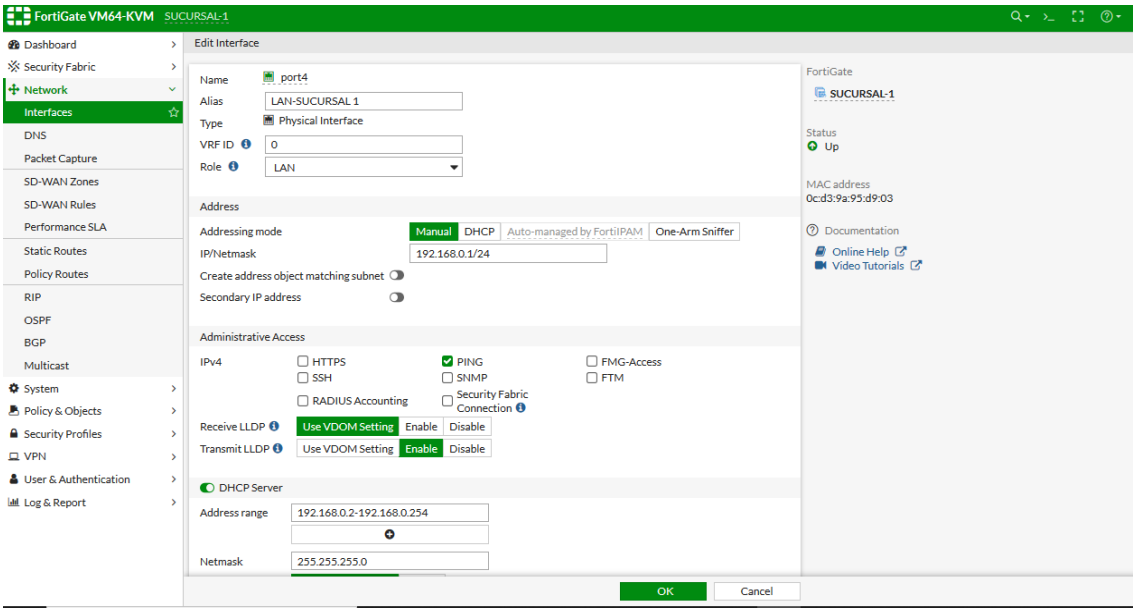


Figura 186. Configuración red local del fortigate
Fuente: Los autores

15. Crear SD-WAN Member en la sucursal 1.

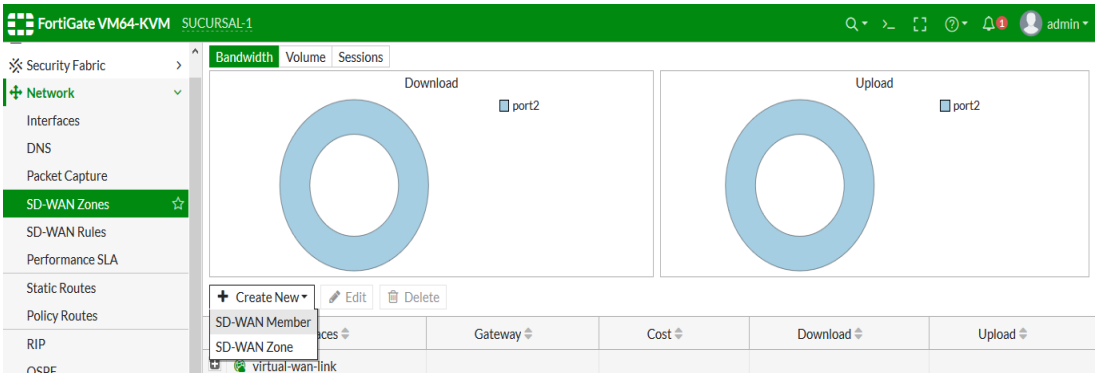


Figura 187. Sd-wan zone fortigate sucursal 1
Fuente: Los autores

16. Crear SD-WAN para la interface enlace wan 1.

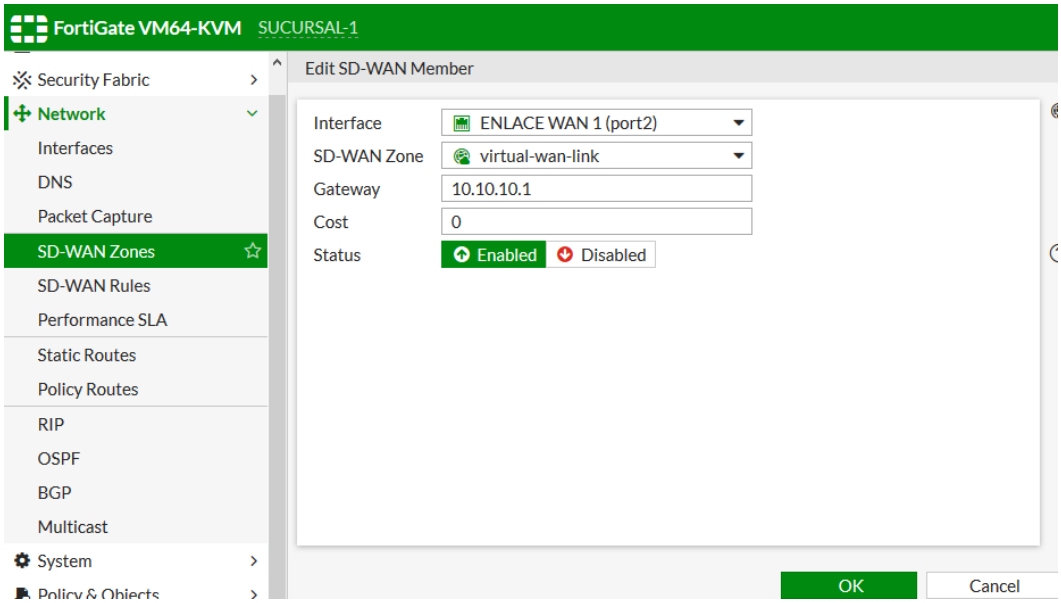


Figura 188. Sd-wan enlace wan 1
Fuente: Los autores

17. Crear SD-WAN para la interface enlace wan 2.

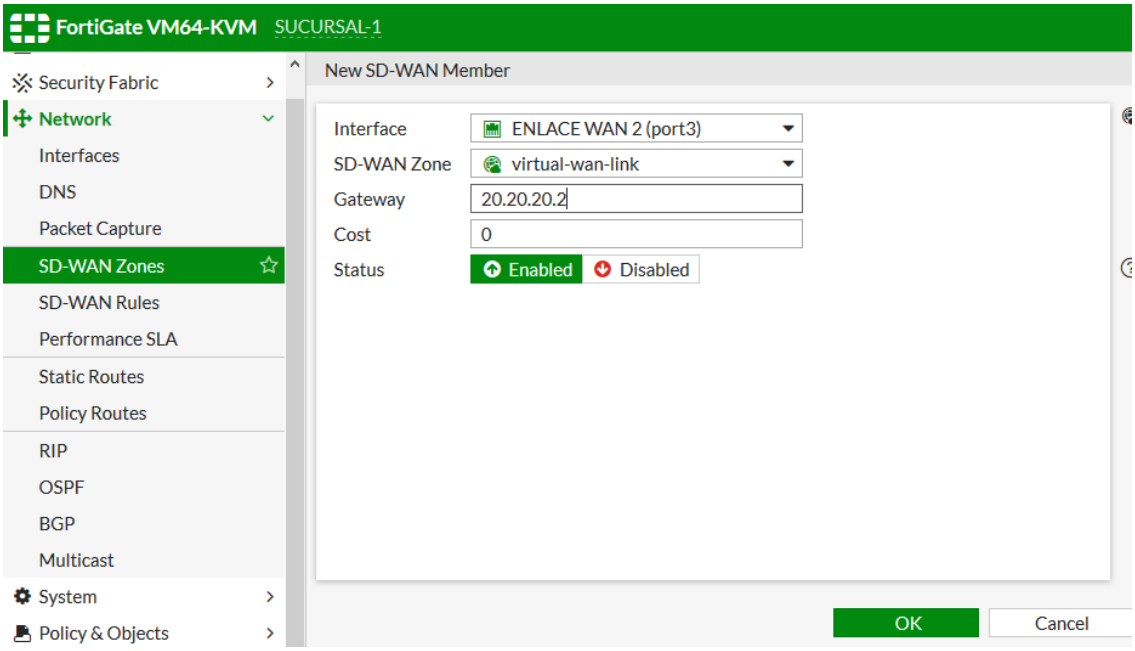


Figura 189. Sd-wan enlace wan 1
Fuente: Los autores

18. Configurar static routes para la SD-WAN.

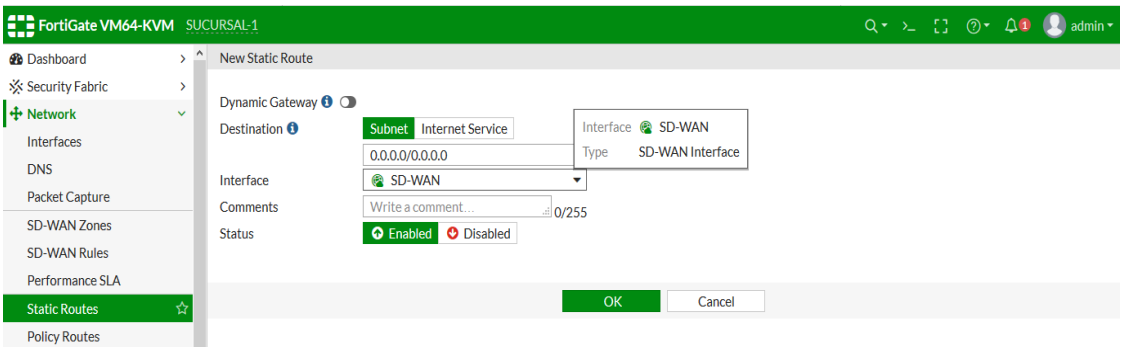


Figura 190. Static routes para sd-wan fortigate sucursal 1
Fuente: Los autores

19. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 1.

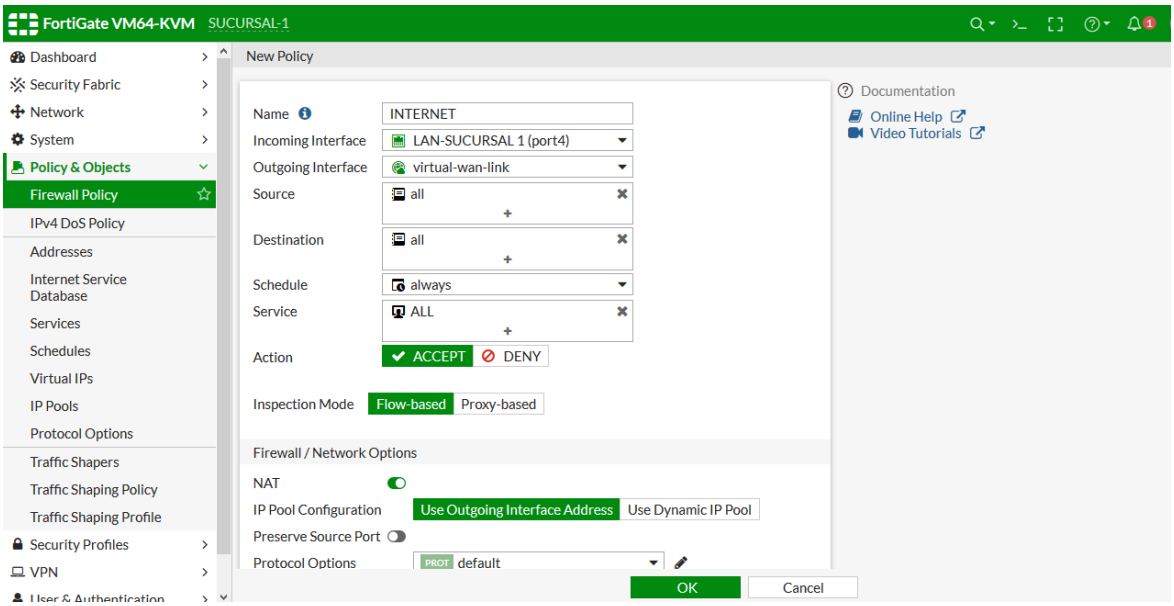


Figura 191. Static routes para sd-wan fortigate sucursal 1
Fuente: Los autores

20. Configurar SD-WAN Rules en sucurasal 1 para controlar como se distribuye las sesiones a los miembros de SD WAN dames click en créate new y nombramos nuestra primera regla que se llamara Faceboox.

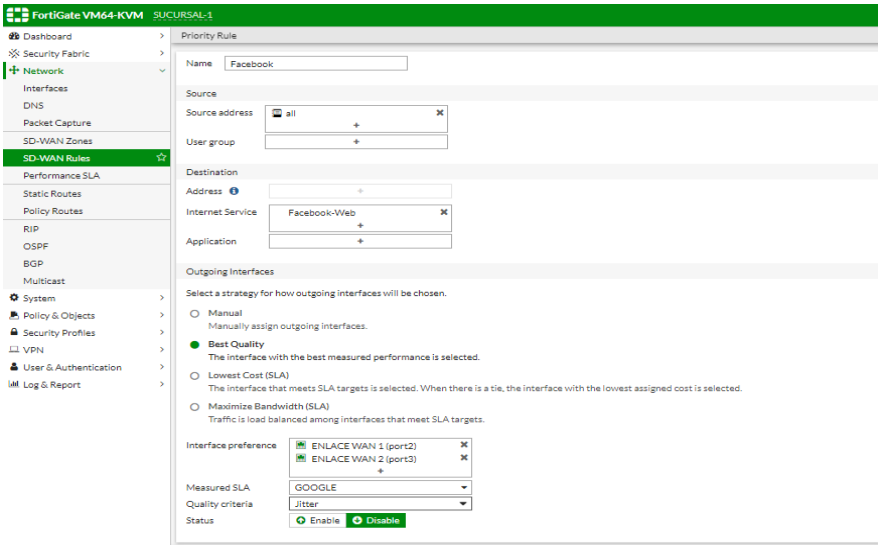


Figura 192. SD-WAN Rules para Faceboox- fortigate sucursal 1
Fuente: Los autores

21. Creamos una nueva regla llamada TeamViewer y llenamos los campos mostrados.

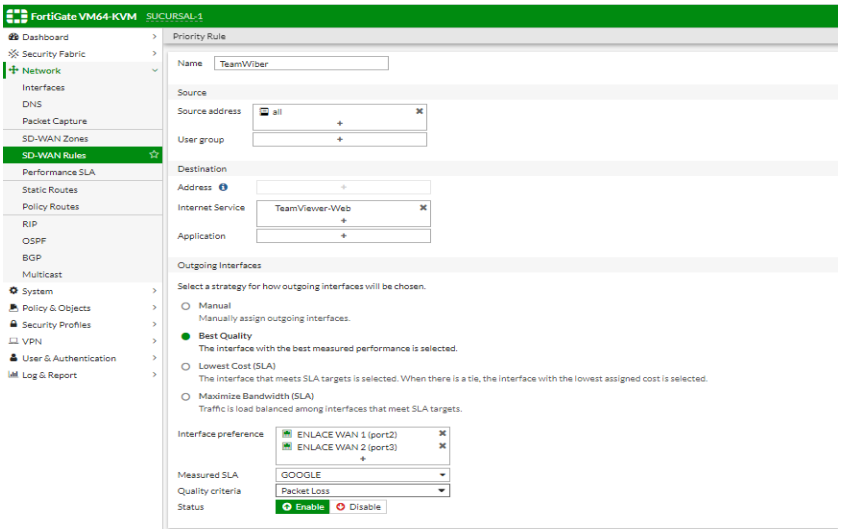


Figura 193. SD-WAN Rules para TeamViewer- fortigate sucursal 1
Fuente: Los autores

22. Por ultimo nuestra ultima regla se llamara Adobe y llenamos los campos mostardos.

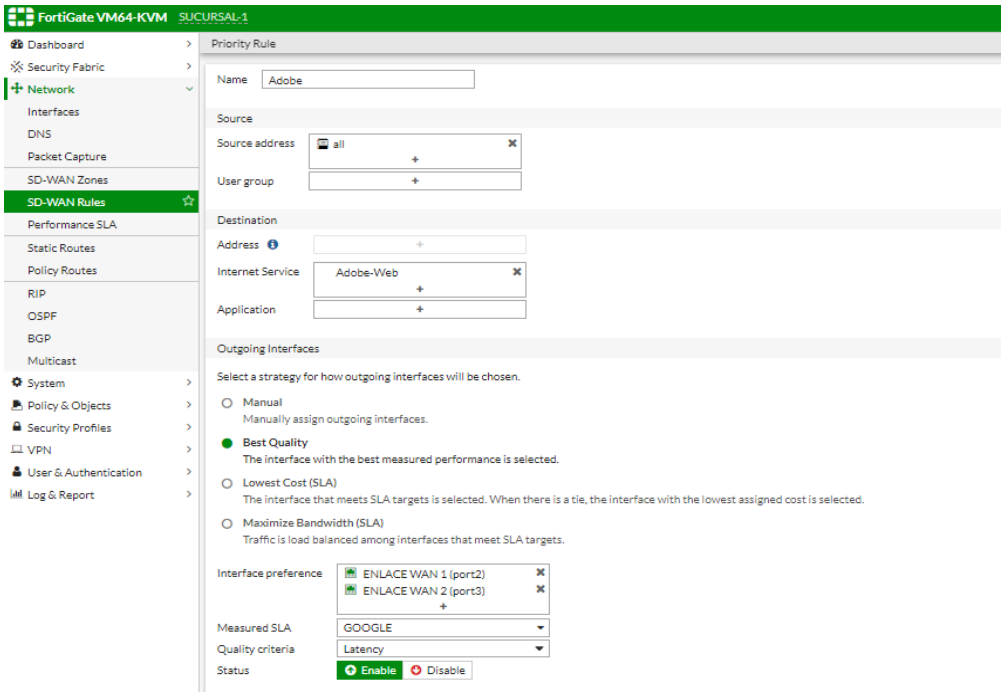


Figura 194. SD-WAN Rules para Adobe- fortigate sucursal 1
Fuente: Los autores

23. Mostramos todas las SD-WAN Rules el cual indica porque enlace va a navegar nuestra regla y cual criterio tomara en cuenta para poder hacerlo.

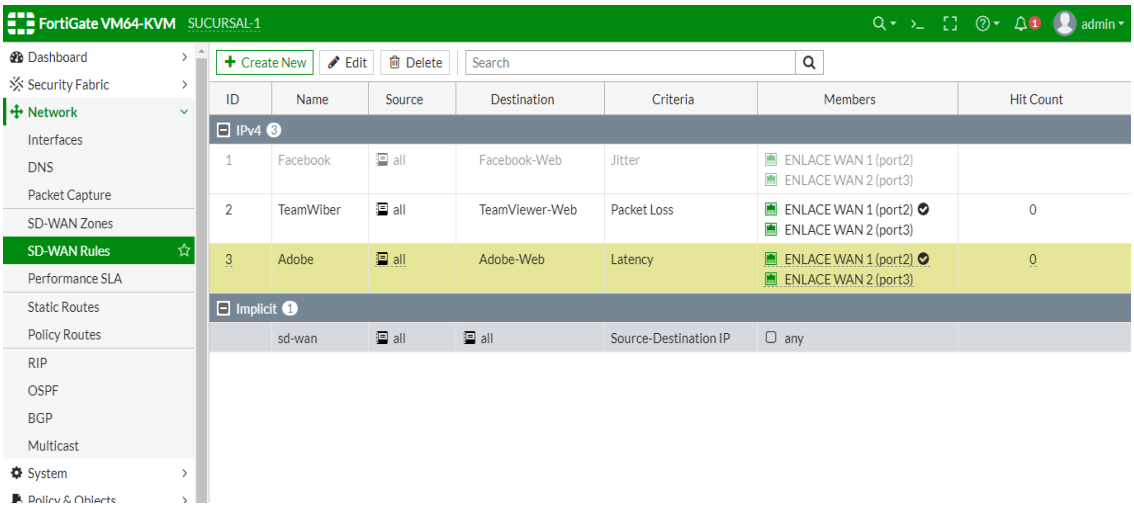


Figura195. SD-WAN Rules para fortigate sucursal 1
Fuente: Los autores

24. Configurar SD-WAN Rules en sucurasal 2 para controlar como se distribuye las sesiones a los miembros de SD-WAN dames click en créate new y nombramos nuestra primera regla que se llamara Amazon.

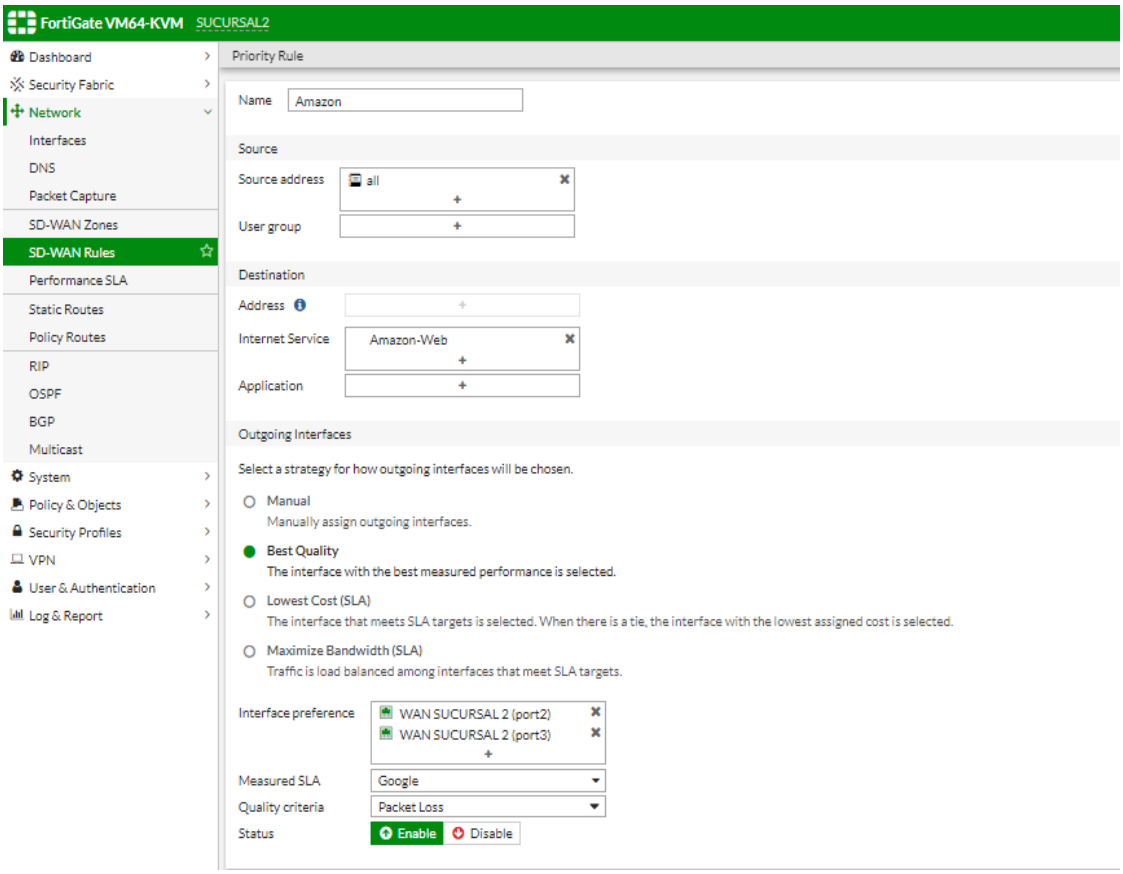


Figura 196. SD-WAN Rules para Amazon- fortigate sucursal 2
Fuente: Los autores

25. Del mismo modo creamos otra nueva SD-Rules la cual nombraremos Likendin y llenamos los campos mostrados.

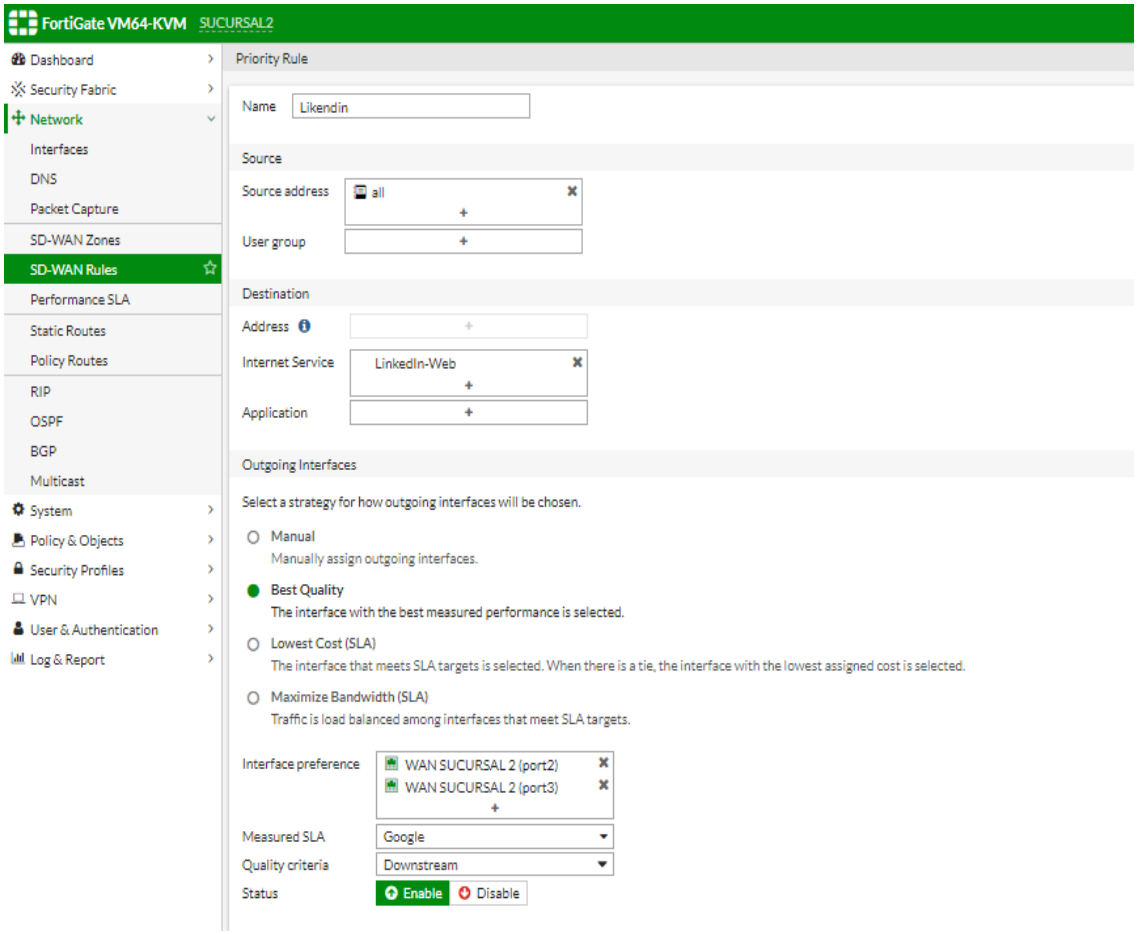


Figura 197. SD-WAN Rules para Likendin- fortigate sucursal 1
Fuente: Los autores

26. Mostramos todas las SD-WAN Rules el cual indica porque enlace va a navegar nuestra regla y cual criterio tomara en cuenta para poder hacerlo.

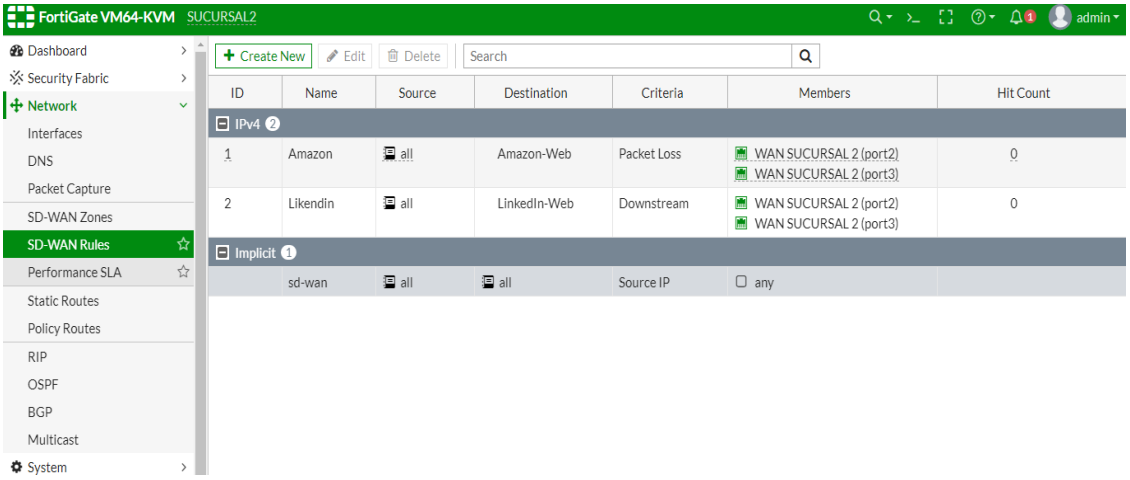


Figura.198 SD-WAN Rules - fortigate sucursal 2
Fuente: Los autores

27. Realizar un SLA a travez de PING a google salga a travez de la SD-WAN.

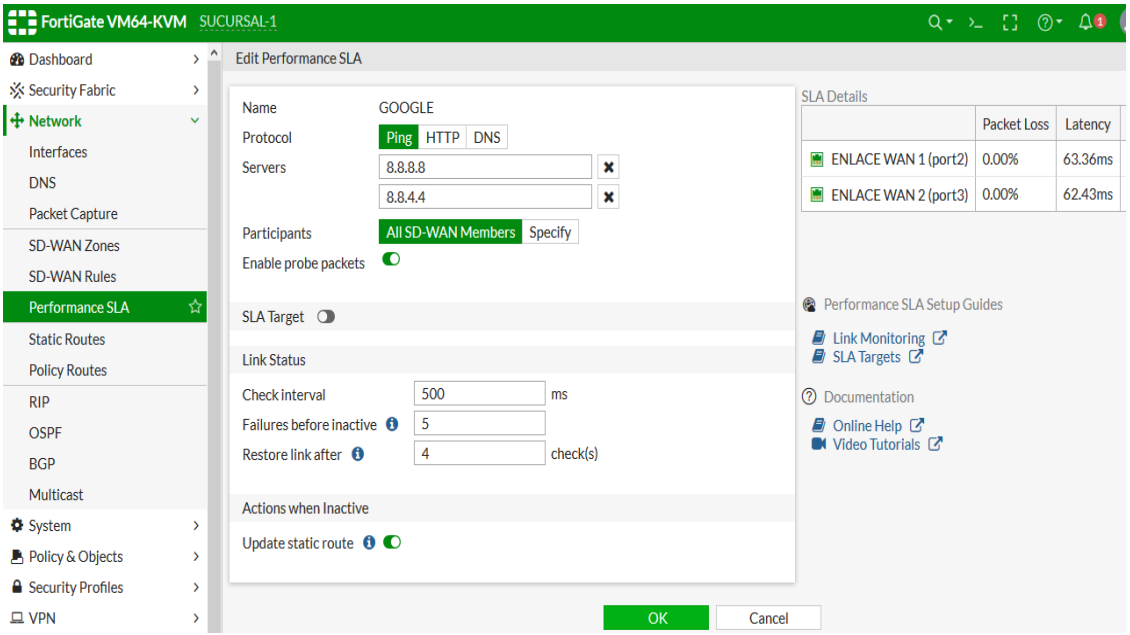


Figura 199. Configuración de static routes SD-WAN del fortigate
Fuente: Los autores

28. Veremos que tenemos menos PING y JIPTTER en una de las interfaces configuradas donde SD-WAN eligue en enlace con mejor calidad de servicios.

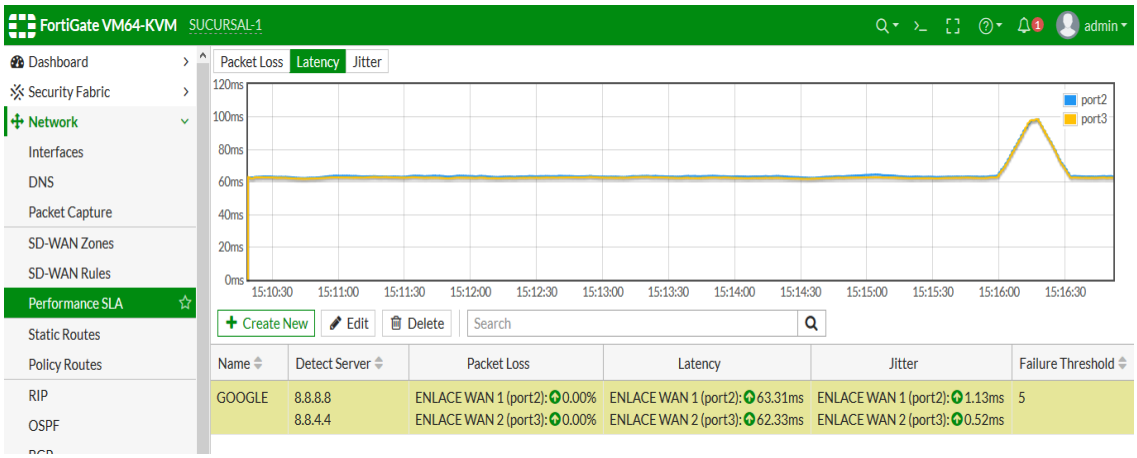


Figura 200. Diagrama de calidad de sevicio de sucrusal 1

Fuente: Los autores

29. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

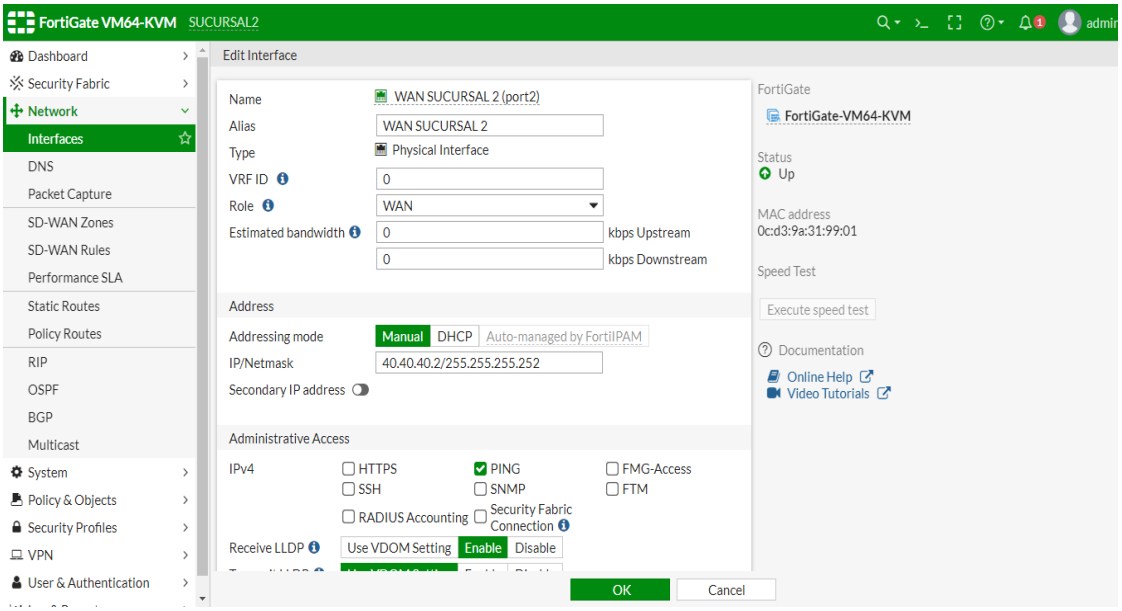


Figura 201. Configuracion IP fortigate wan sucrsal 2
Fuente: Los autores

30. Configurar la dirección IP en puerto 3 en el frotigate principal para el enlace WAN para el fortigate sucursal 2.

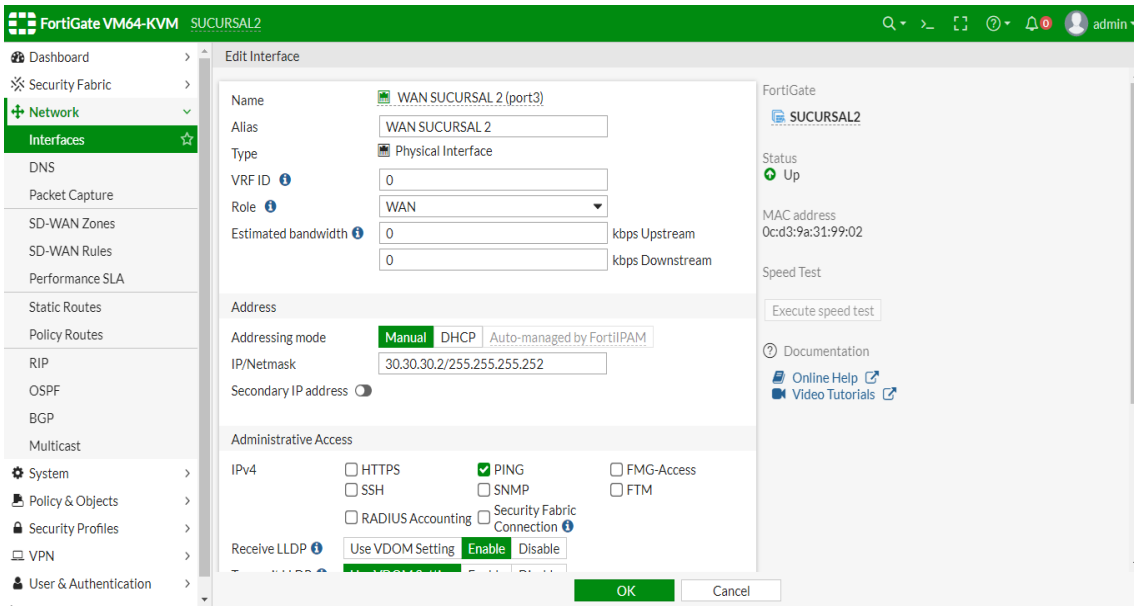


Figura 202. Configuracion IP fortigate wan sucursal 2
Fuente: Los autores

31. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal. 2.

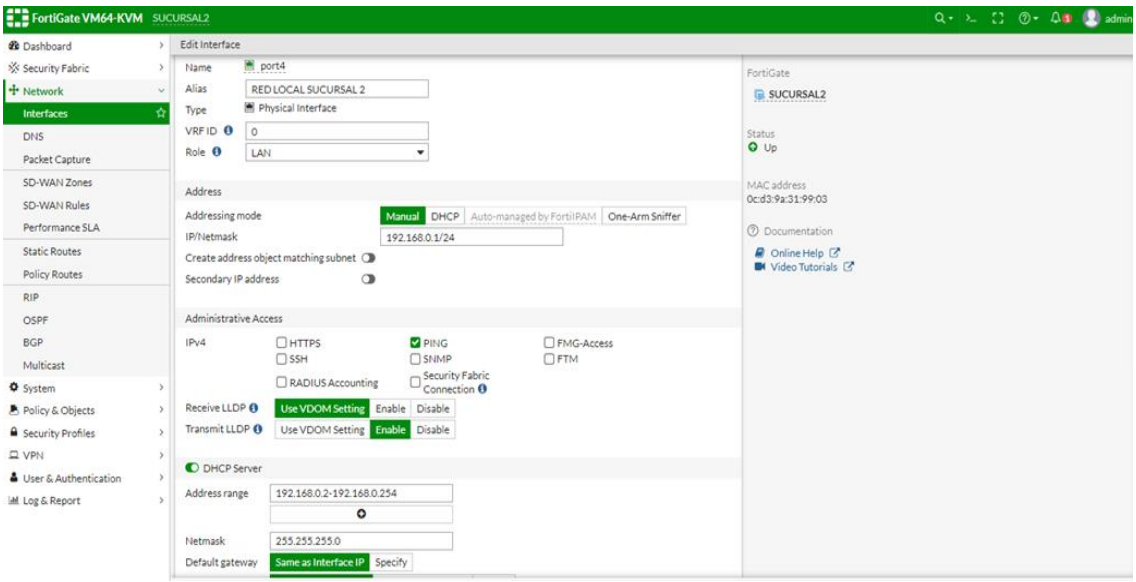


Figura 203. Configuración red local del fortigate
Fuente: Los autores

32. Crear SD-WAN Member en la sucursal 2.

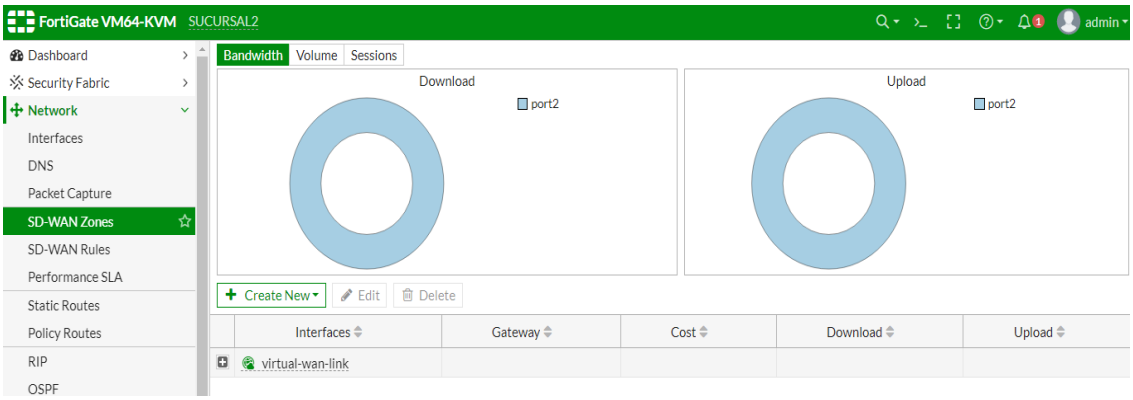


Figura 204. Sd-wan zone fortigate sucursal 2
Fuente: Los autores

33. Crear SD-WAN para la interface sucursal 2.

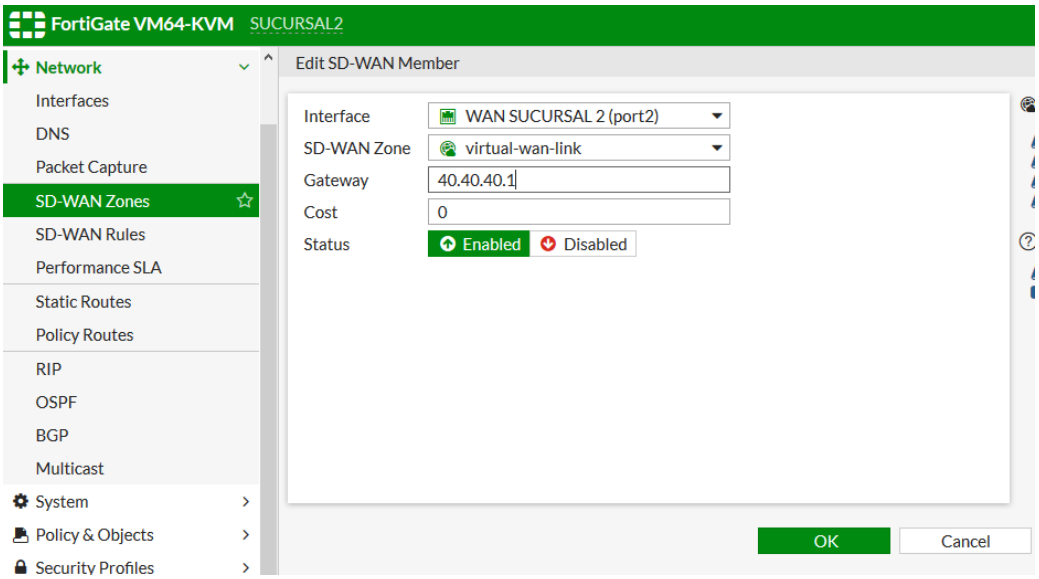


Figura 205 Sd-wan sucursal 2 para puerto 2
Fuente: Los autores

34. Crear SD-WAN para la interface sucursal 2.

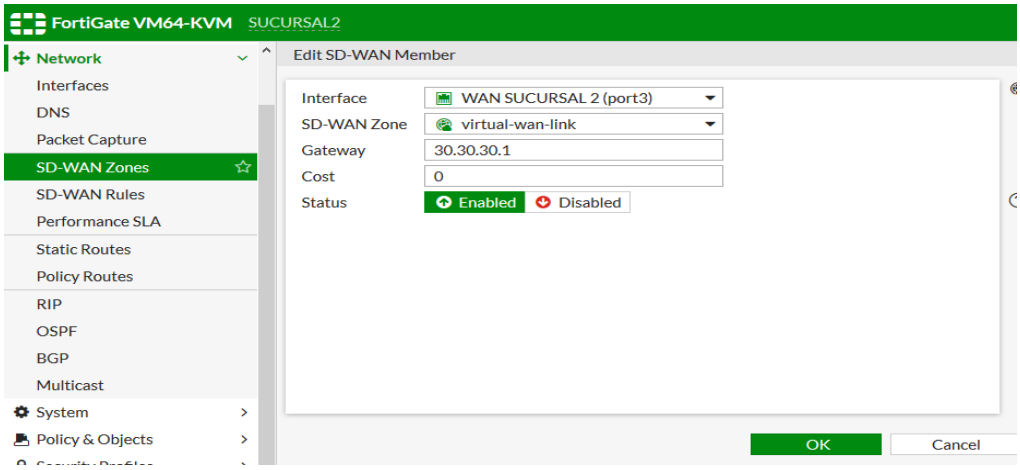


Figura 206. Sd-wan sucursal 2 para puerto 3
Fuente: Los autores

35. Configurar static routes para la SD-WAN sucursal 2

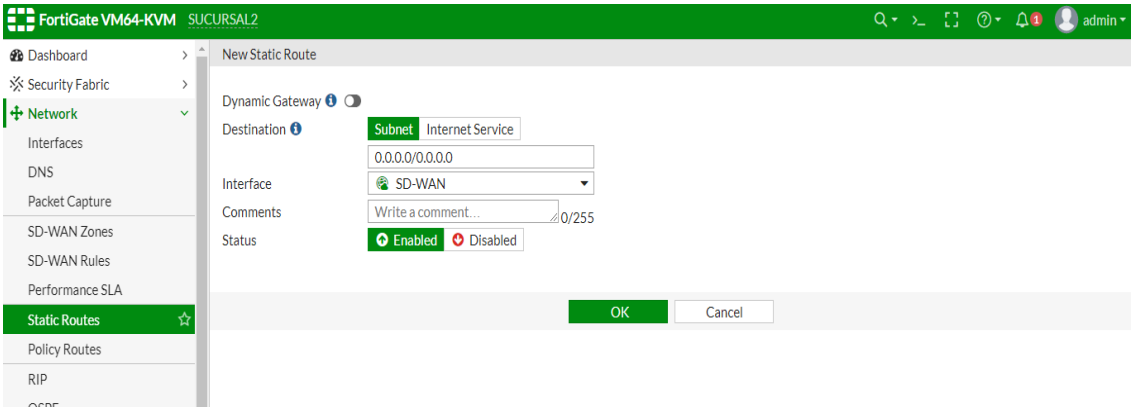


Figura 207. Static routes para sd-wan fortigate sucursal 2
Fuente: Los autores

36. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 2.

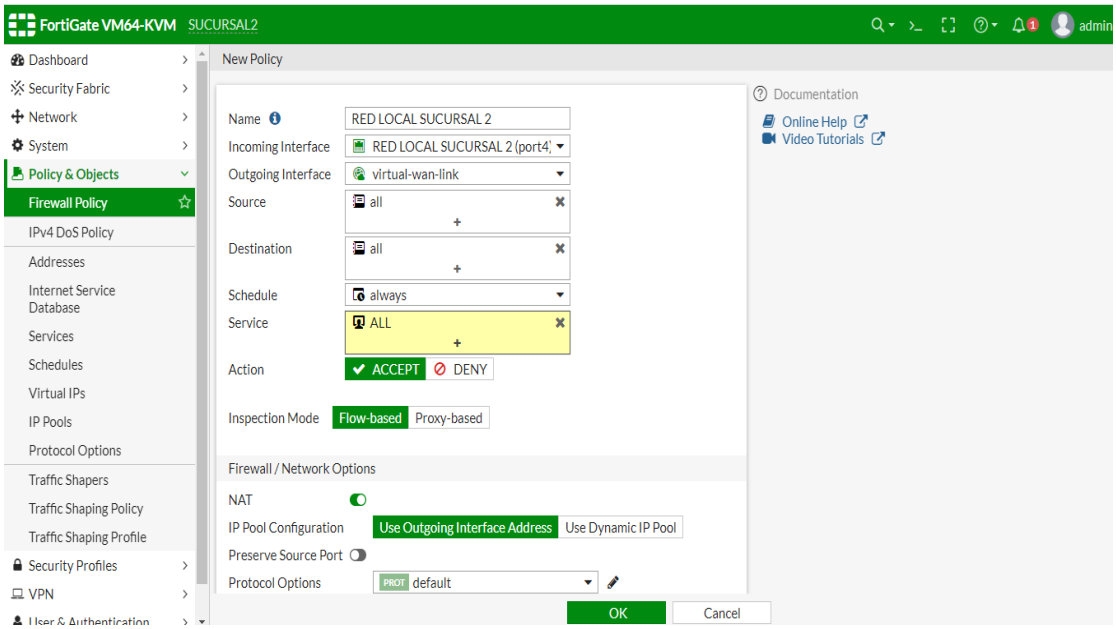


Figura 208. Static routes para sd-wan fortigate sucursal 2
Fuente: Los autores

37. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos PING o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new para sucursal 2.

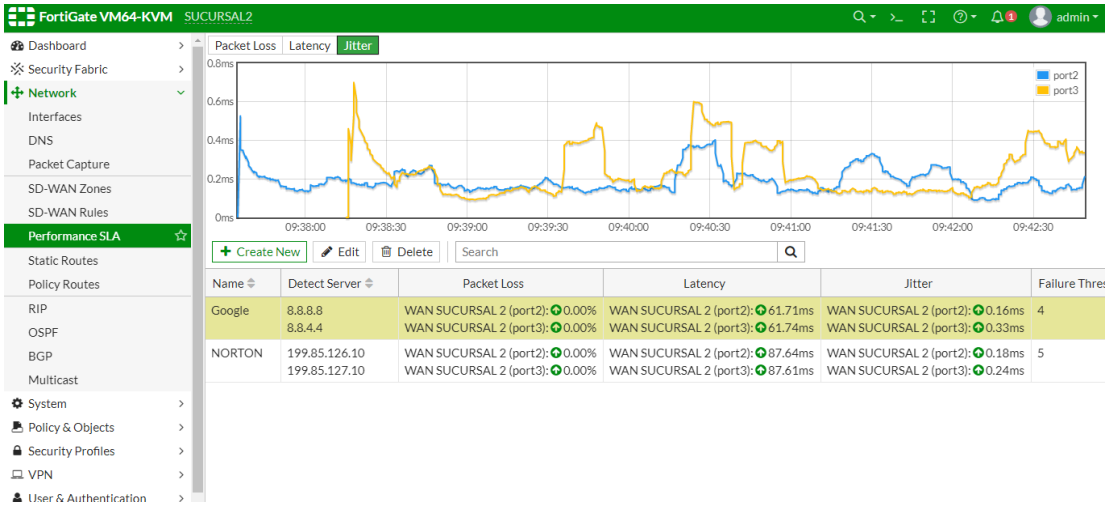


Figura 209. Configuración de static routes sd-wan del fortigate
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.5. PRÁCTICA 5

Configuración de una red SD-WAN con fortigate y enlazados con dispositivos mikrotik.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 5**
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con fortigate y enlazarlos con dispositivos mikrotik.

OBJETIVOS

General

Configurar la red sd-wan y enlazarlos con enrutamiento estático.

Específicos

- Configurar enrutamiento estático en los mikrotik.
- Configurar dispositivos mikrotik para salida a internet.
- Comprobar compatibilidad de los enlaces finales.

GLOSARIO

MIKROTIK.- Mikrotik es un fabricante de hardware y software de routers su kernel esta basado en Linux 2.6.

DHCP.- Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP determina dinámicamente una dirección IP a un dispotivo dentro de la red de datos por ejemplo celulares y computadoras.

DHCP-CLIENT.- El cliente aceptará una dirección, máscara de red, puerta de enlace predeterminada y dos direcciones de servidor DNS de su proveedor de internet ISP.

NAT.- Es manejado por los routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles, NAT es usada por las redes IPv4.

WINBOX.- Es una herramienta que permite la administración de equipos mikrotik manejando una GUI rápida y sencilla.

MARCO PROCIDEMENTAL.

1. Diseñar la topología de la red para la práctica 5

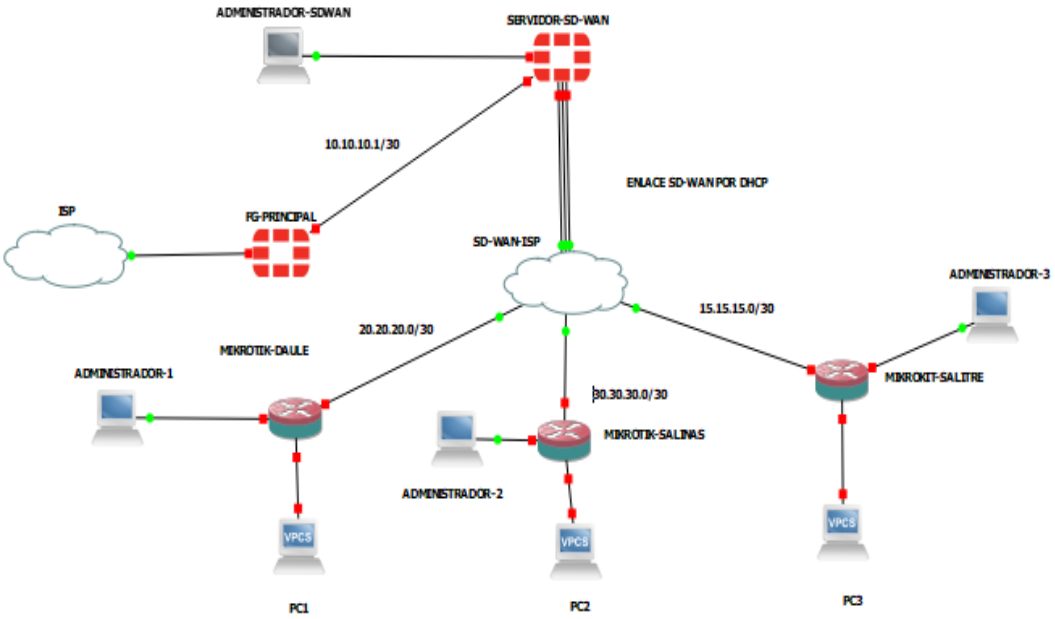


Figura 210. Diseño de la red práctica Nº5
Fuente: Los autores

2. Configurar la red del enlace WAN en el fortigate principal para el fortigate servidor sd-wan.

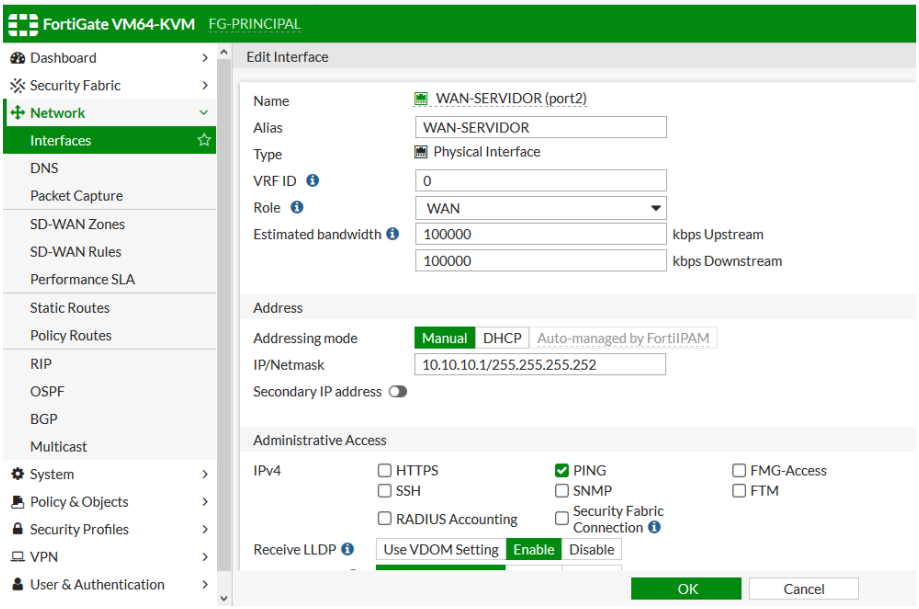


Figura 211. Interfaz port2 FG-principal
Fuente: Los autores

3. Configurar ruta estática para el fortigate principal para la salida a internet,damos click en dynamic para obtener la configuración del ISP.

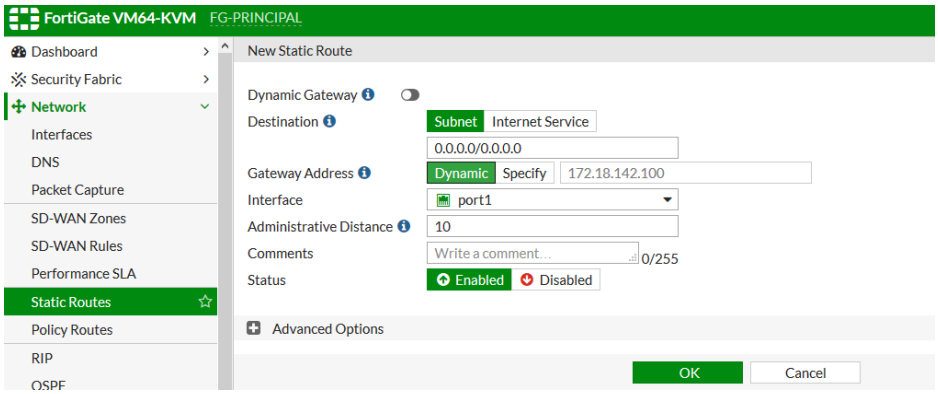


Figura 212. Interfaz port2 FG-principal
Fuente: Los autores

4. Configurar la regla en el firewall que permitirá la salida a internet al servidor SD-WAN.

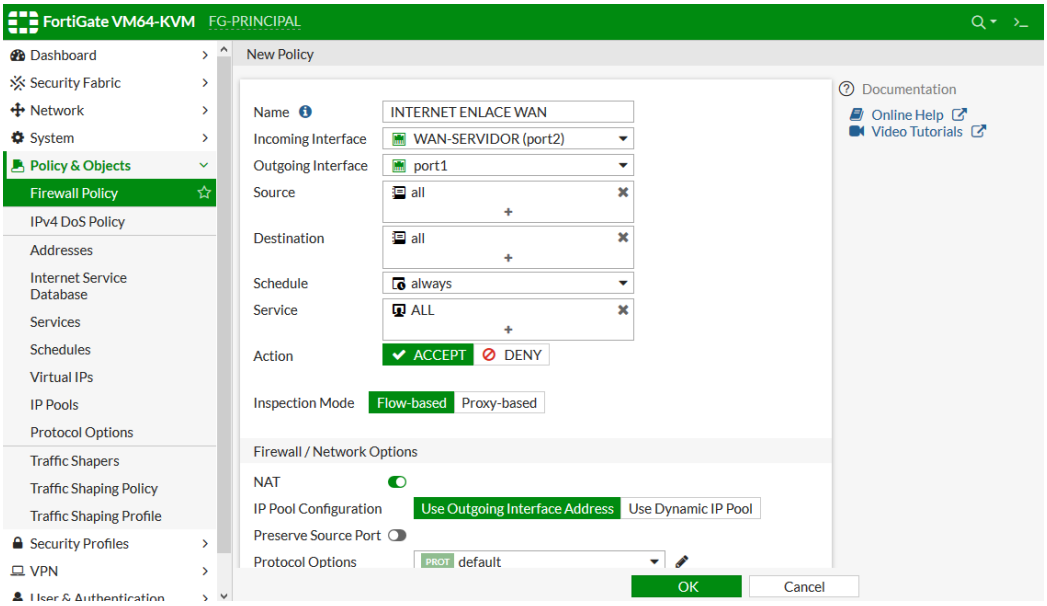


Figura 213. Firewall Policy port2
Fuente: Los autores

5. Configurar la red del enlace principal en el fortigate servidor SD-WAN.

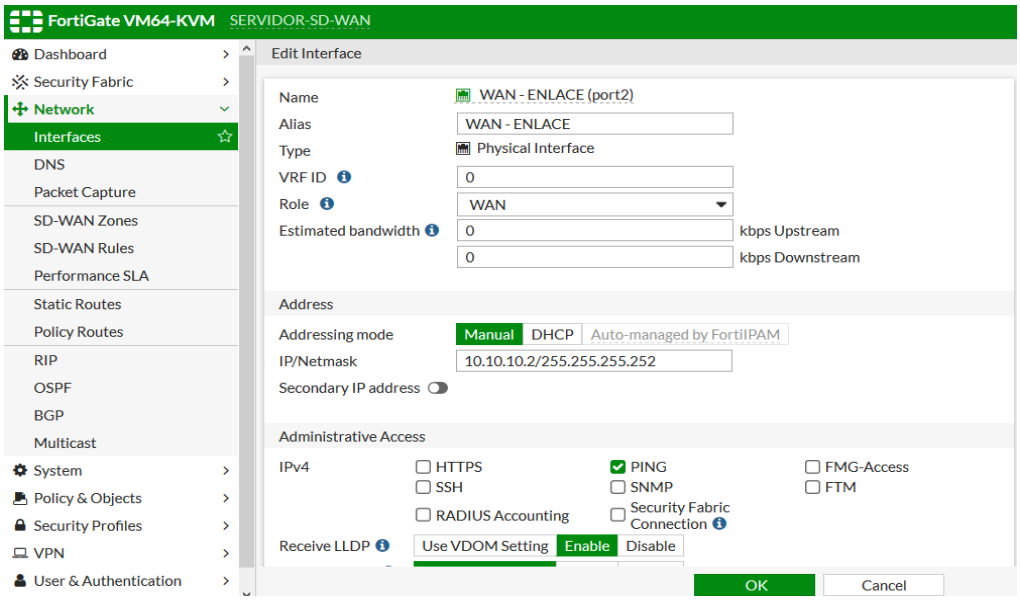


Figura 214. Servidor sd-wan port2
Fuente: Los autores

6. Configurar las interfaces port3 en el servidor SD-WAN que se comunicara con el mikrotik-daule.

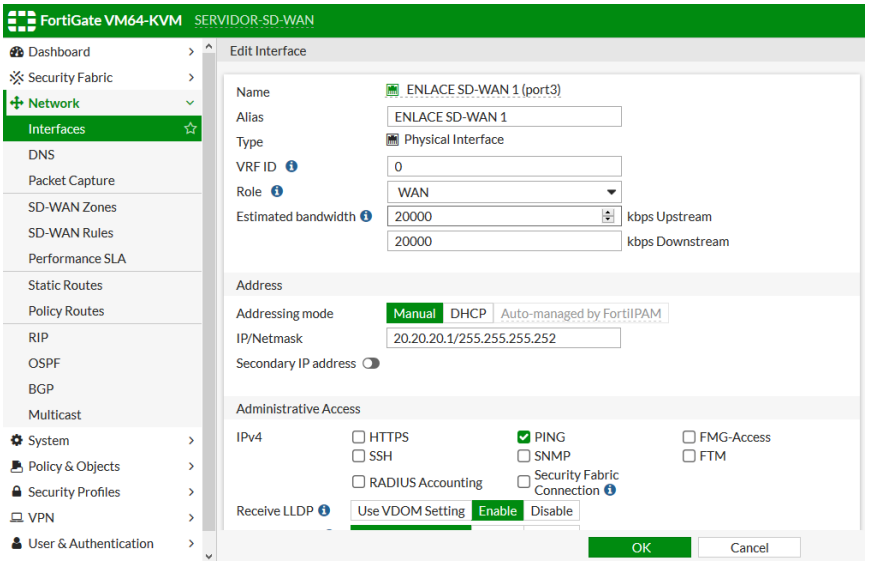


Figura 215. Servidor sd-wan port3
Fuente: Los autores

7. Configurar la interface port4 en el servidor SD-WAN que se comunicara con el mikrotik-salinas.

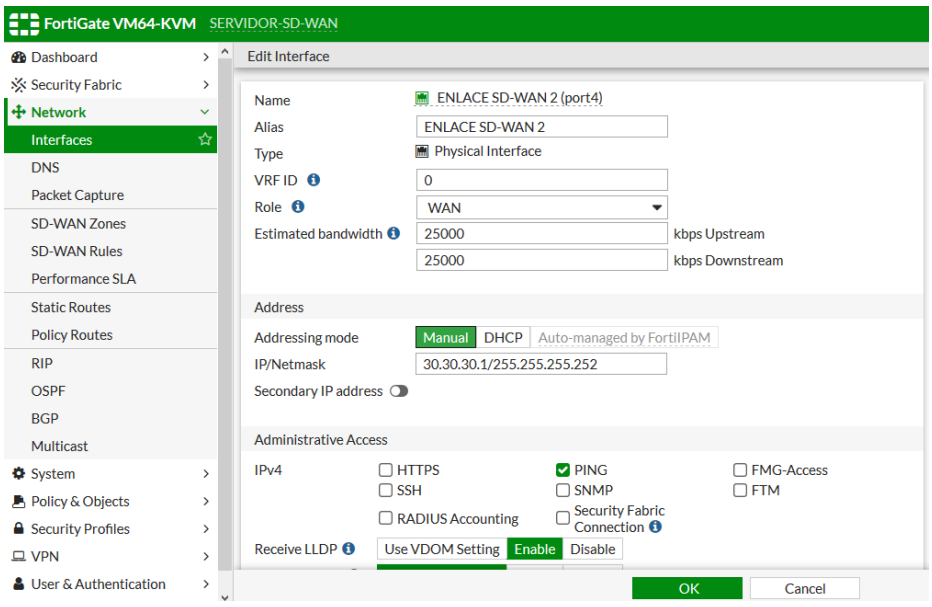


Figura 216. Servidor sd-wan port4
Fuente: Los autores

8. Configurar port5 en el servidor SD-WAN que se comunicara con el mikrotik-salitre.

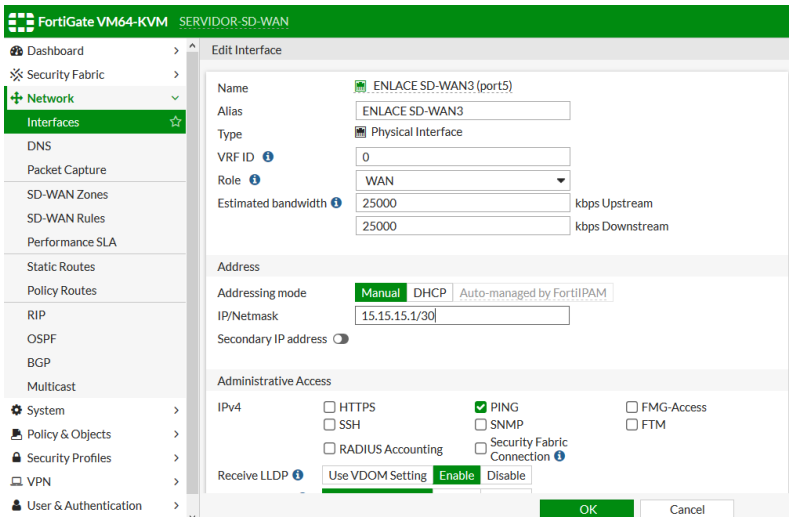


Figura 217. Servidor sd-wan port5
Fuente: Los autores

9. Configurar la interfaz port3 en SD-WAN MEMBER para el enlace con mikrotik-daule.

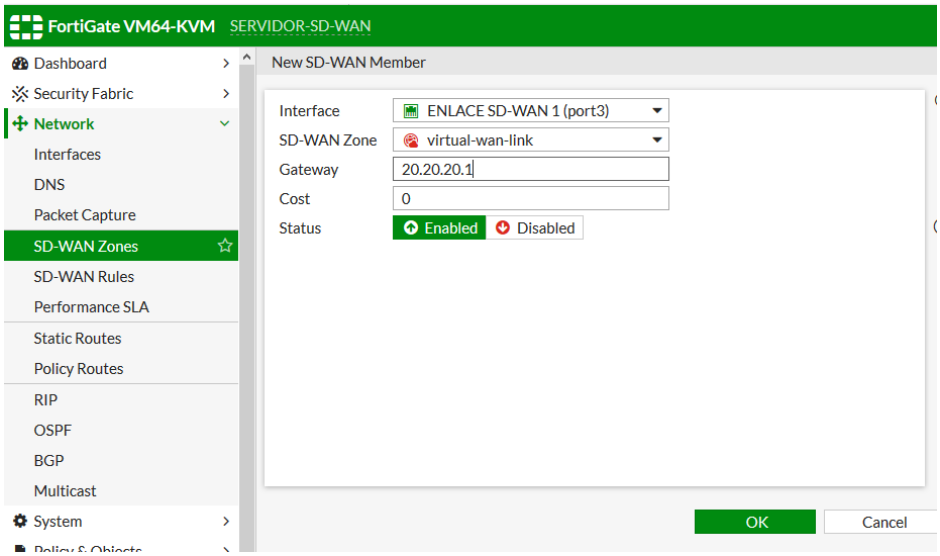


Figura 218. Interfaz sd-wan port3 servidor
Fuente: Los autores

10. Configurar la interfaz port4 en SD-WAN MEMBER para el enlace con mikrotik-salinas.

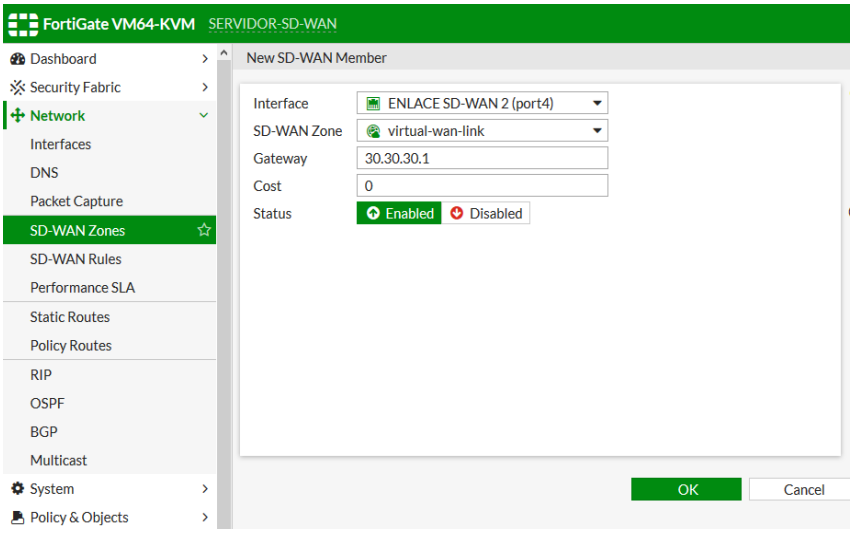


Figura 219. Interfaz sd-wan port4 servidor
Fuente: Los autores

11. Configurar la interfaz port5 en SD-WAN member para el enlace con mikrotik-salitre.

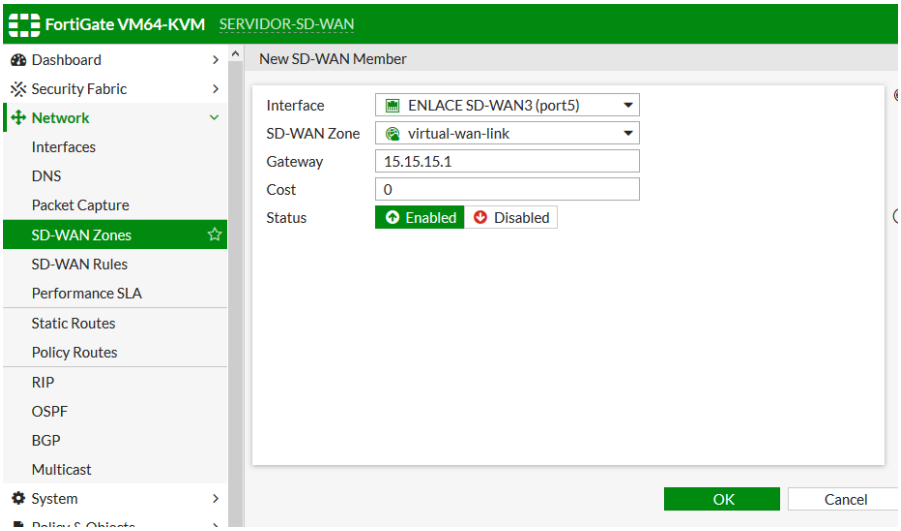


Figura 220. Interfaz sd-wan port5 servidor
Fuente: Los autores

12. Configurar la interfaz port2 en SD-WAN MEMBER que dara paso a la nube SD-WAN ISP a internet.

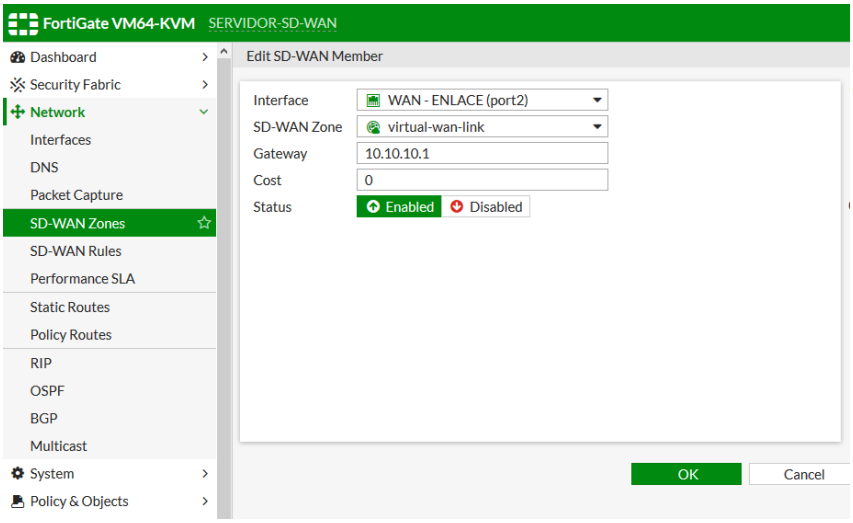


Figura 221. Interfaz sd-wan port2 servidor
Fuente: Los autores

13. Configurar la static routes para el servidor SD-WAN.

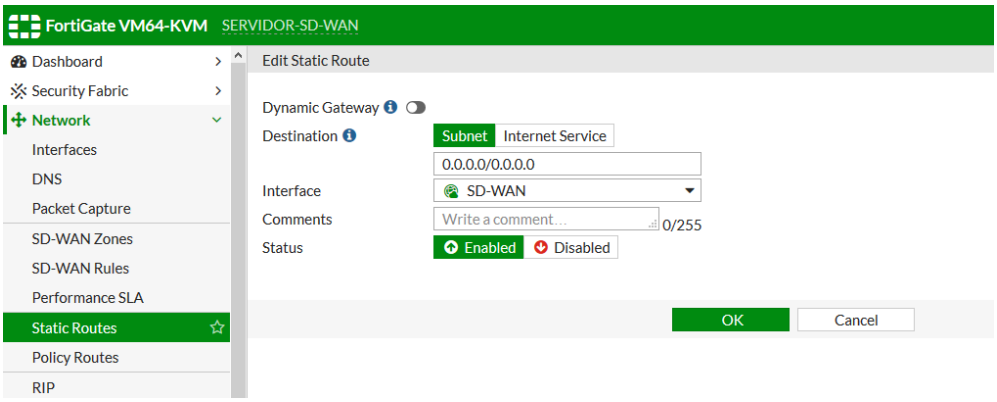


Figura 222. Static routes servidor-sd wan
Fuente: Los autores

14. Configurar regla para la salida a internet a las sucursales atrevez del enlace SD-WAN.

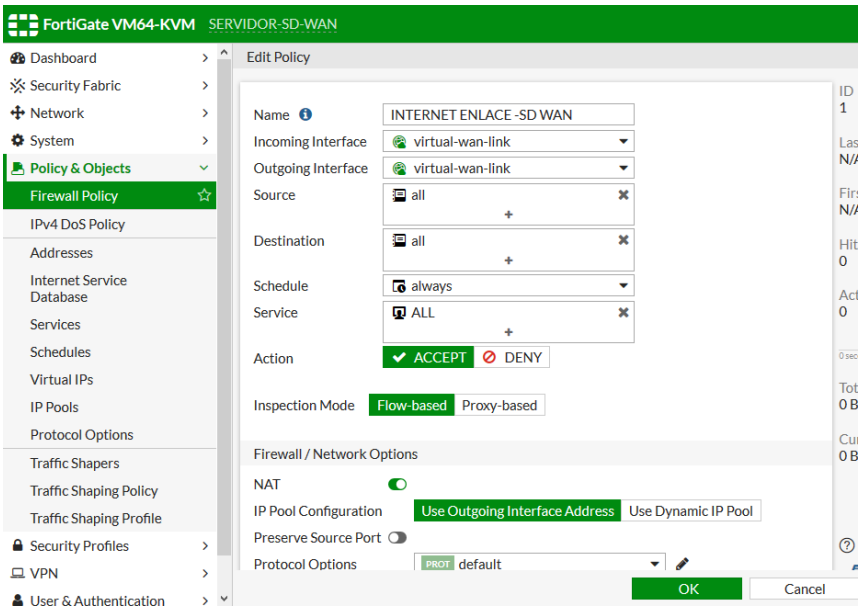


Figura 223. Static routes servidor-sd wan
Fuente: Los autores

15. Vemos que tenemos ya tráfico en la interfaz SD-WAN en el servidor.

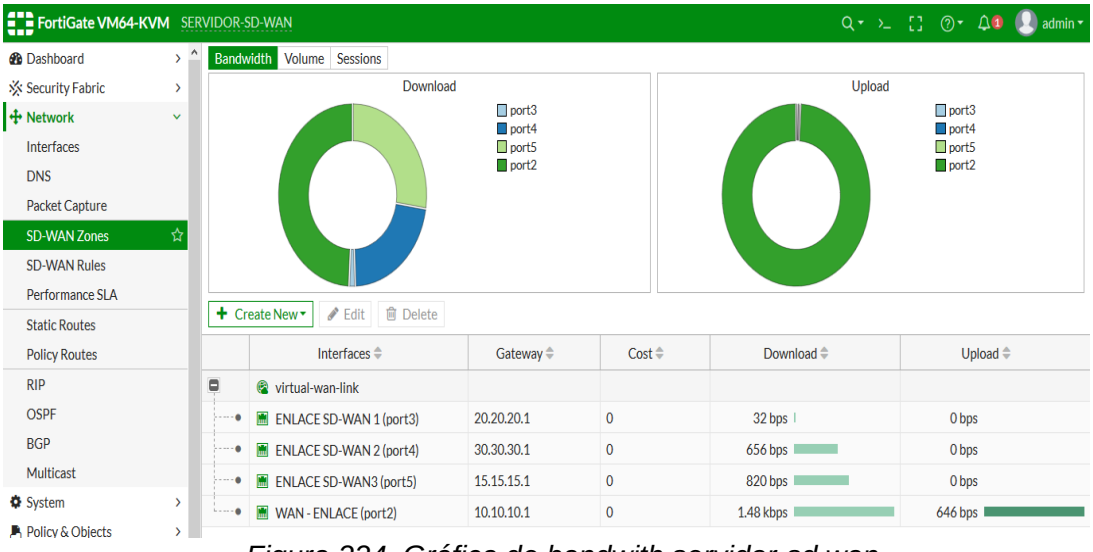


Figura 224. Gráfica de bandwith servidor-sd wan

Fuente: Los autores

16. En la nube SD-WAN vemos que están configurada los puertos con sus respectiva VLAN´S para la comunicación con los dispositivos.

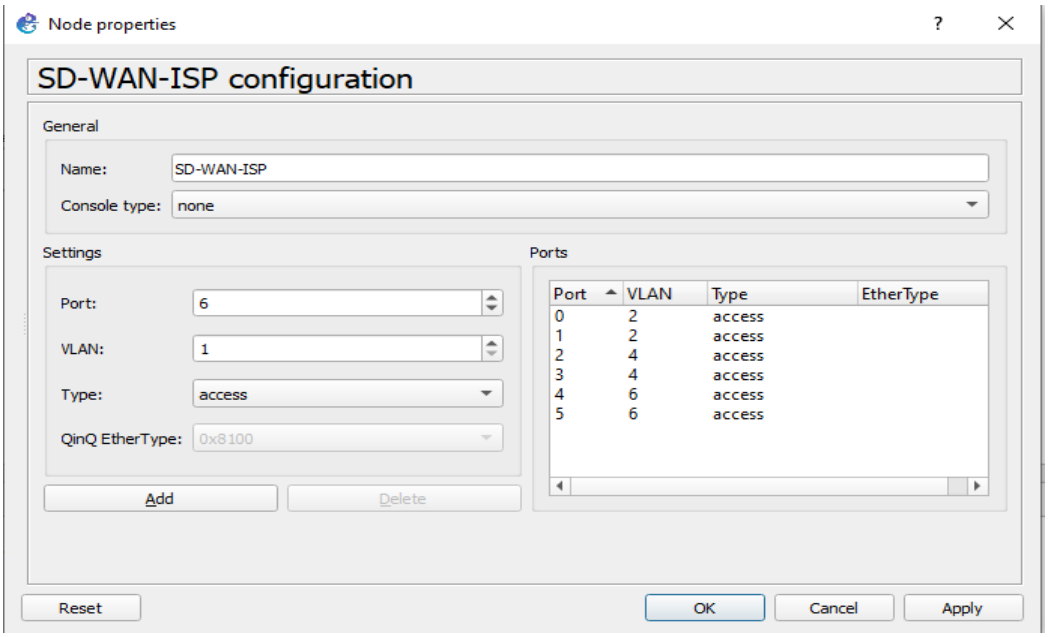


Figura 225. Sd-wan ISP
Fuente: Los autores

17. Descargar Winbox para configurar los mikrotik para la red SD-WAN.

Link de descargar: https://mikrotik.com/download

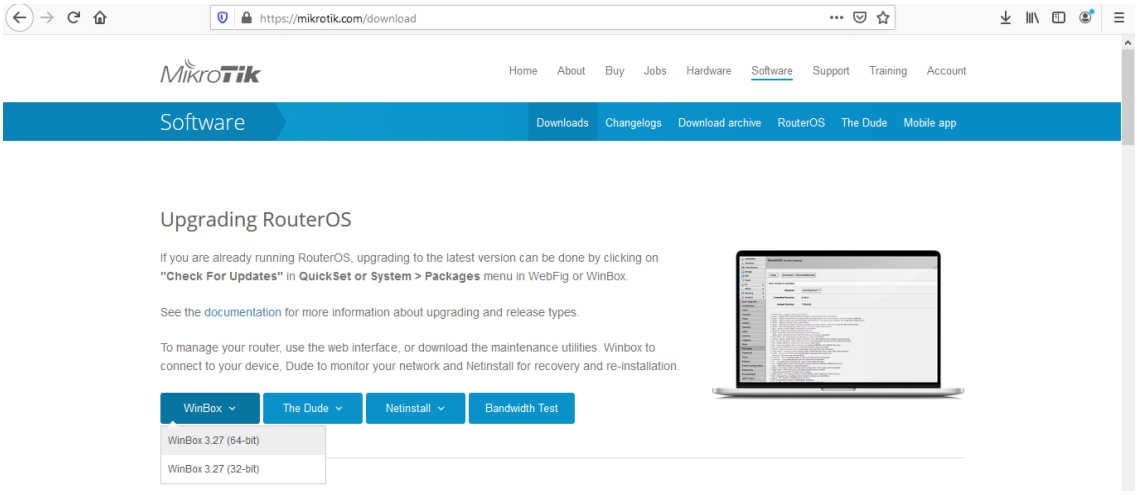


Figura 226. Descarga de winbox
Fuente: Los autores

18. Abrir Winbox y nos aparecerá la mac address del mikrotik Daule.

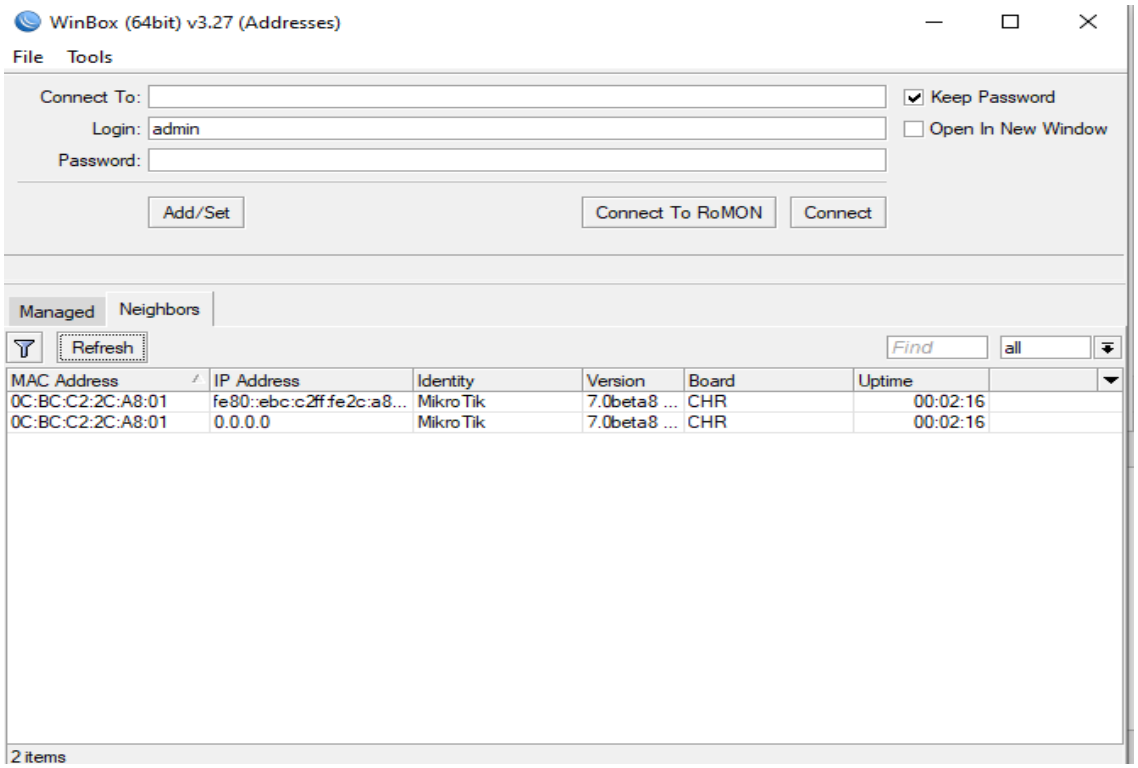


Figura 227.Neighbors Winbox
Fuente: Los autores

19. Damos click en la MAC ADDRESS y en connect para ingresar a la interfaz del mikrotik-DAULE.

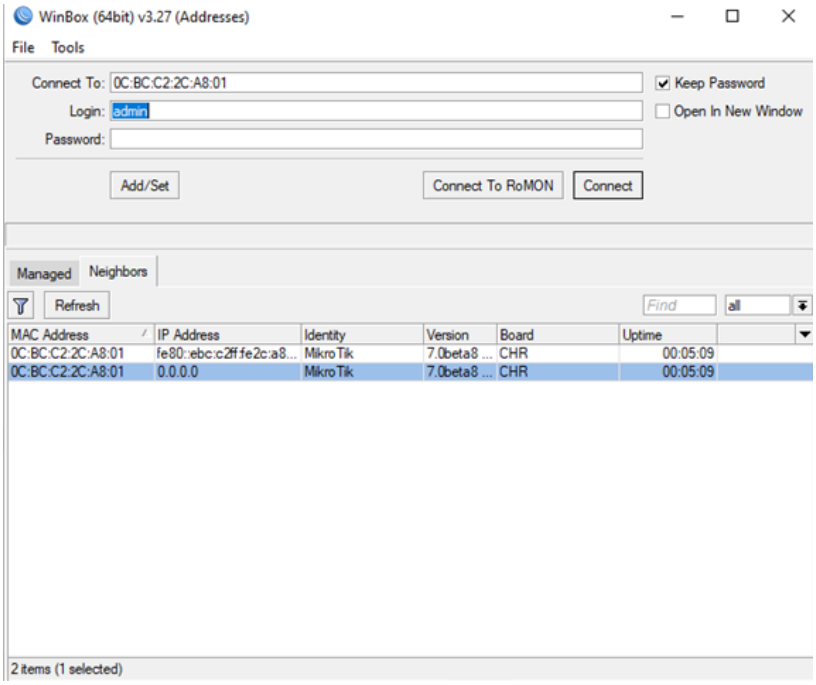


Figura 228.Seleccionar mikrotik a configurar
Fuente: Los autores

20. Cambiar el nombre del dispositivo system y seleccionamos identity.

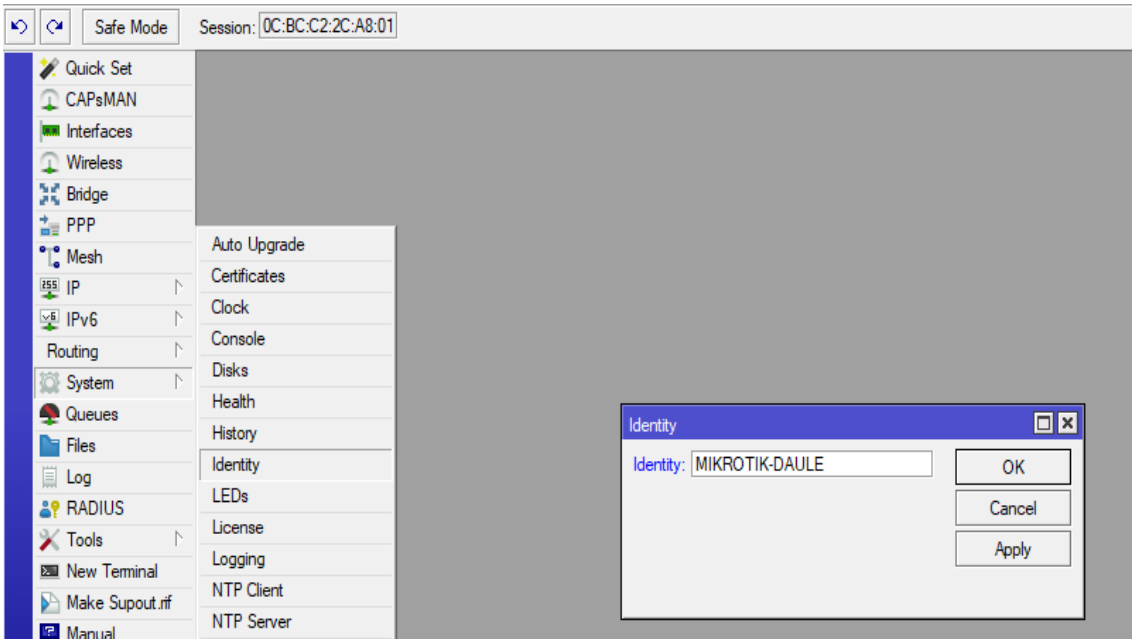


Figura 229.Cambiar nombre al mikrotik
Fuente: Los autores

21. Configurar la dirección IP a la interfaz del mikrotik-DAULE.

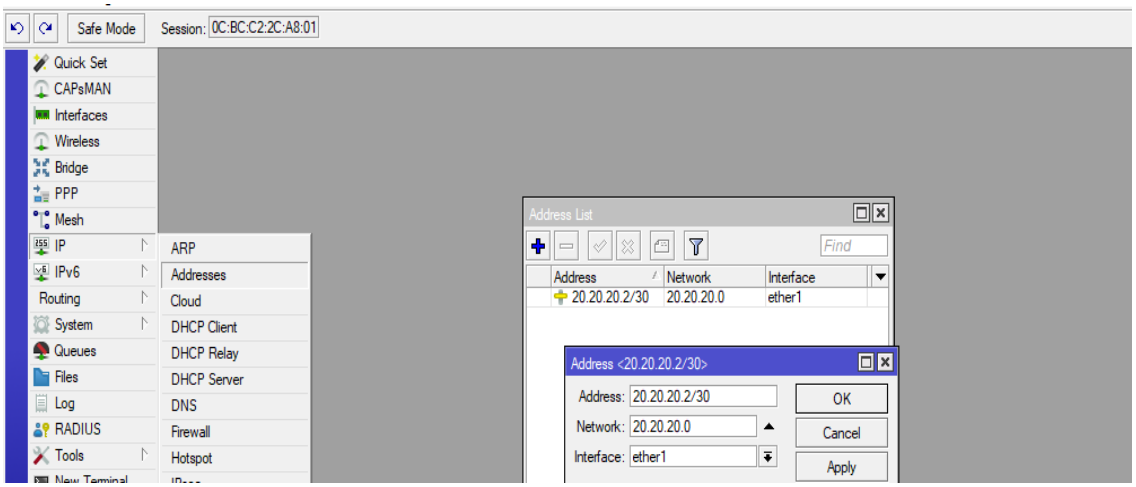


Figura 230.Ip addresses mikrotik-daule
Fuente: Los autores

22. Configurar el DNS del mikrotik se ingresa el Gateway de la red SD-WAN.

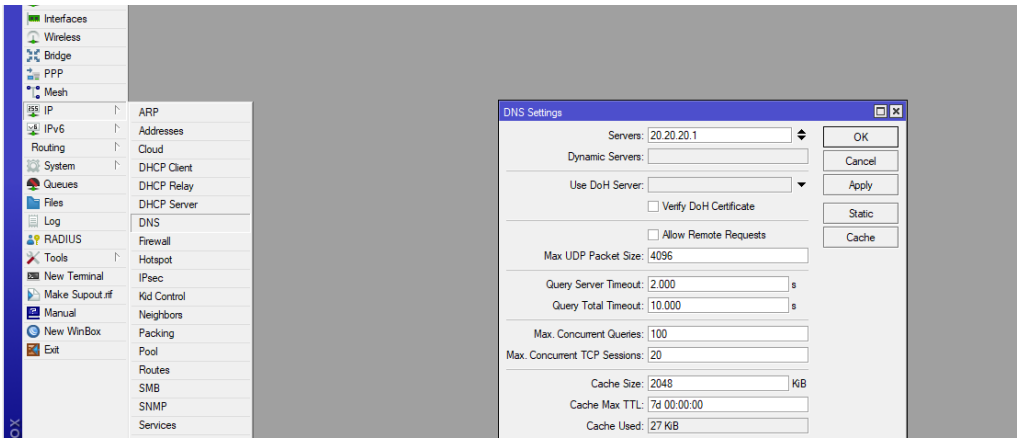


Figura 231.DNS mikrotik-daule
Fuente: Los autores

23. Configurar la routes para la salida a internet por el enlace SD-WAN.

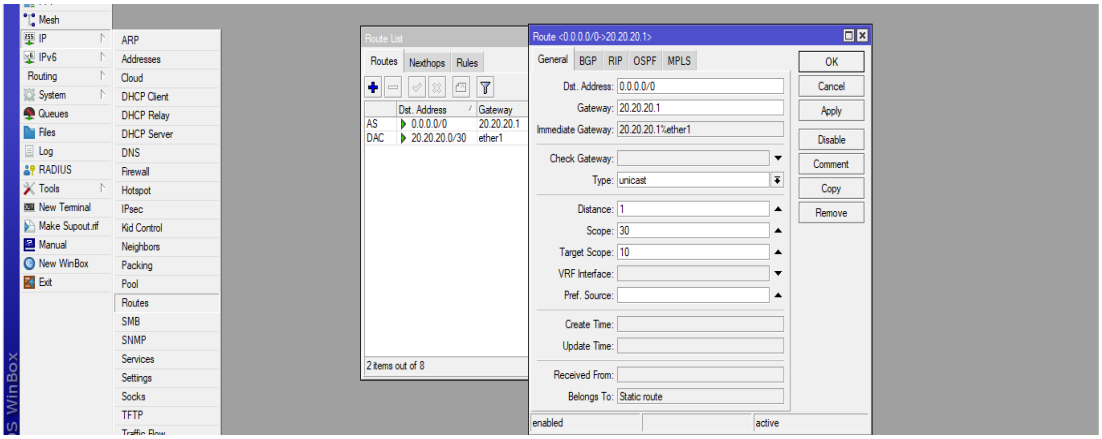


Figura 232. Static routes mikrotik-daule
Fuente: Los autores

24. Hacer un ping a udemy para comprobar si tenemos internet dentro del router.

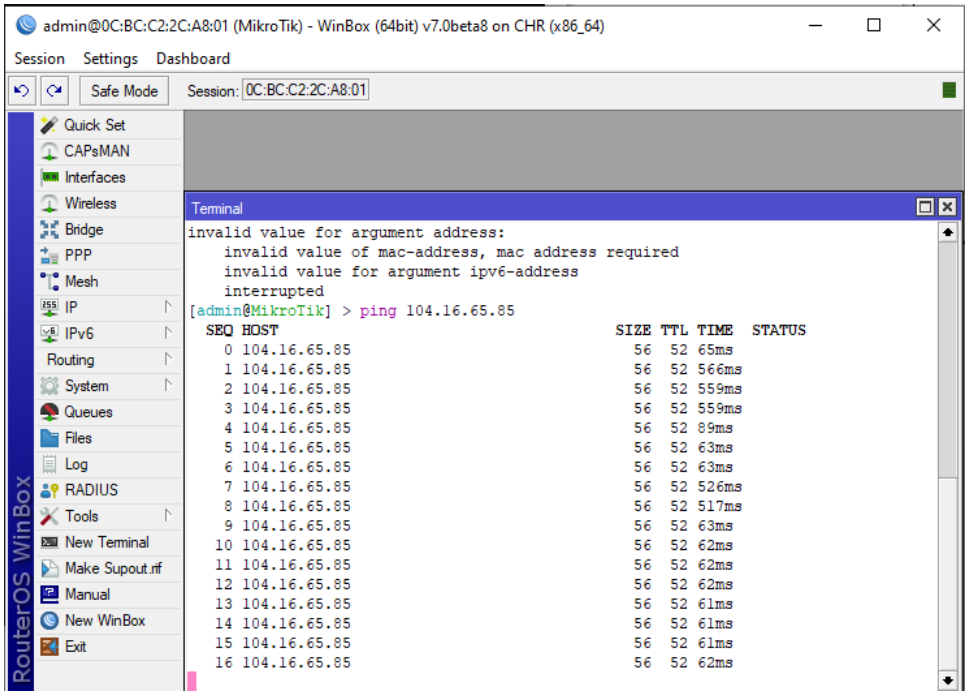


Figura 233. Ping a udemy mikrotik-daule
Fuente: Los autores

NOTA: Para la configuración de los siguientes sucursales realizar los pasos anteriores.

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.6. PRÁCTICA 6

Configuración de una red vpn ipsec fortigate a fortigate.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 6**
- **NUMERO DE COMPUTADORAS**: 10
- **TIEMPO CONSIDERADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de una red vpn ipsec fortigate a fortigate.

OBJETIVOS

General

Configurar vpn´s en fortigate

Específicos

- Configurar vpn ipsec
- Configurar fortigates firewall.
- Realizar ping entre subredes.

GLOSARIO

VPN.- Red virtual privada es una tecnología que usa Internet para conectarse a un sitio determinado y de esta forma poder permitir conexión a ciertos servicios.

IPSEC.- Es un framework o colección de protocolos que operan en la capa de Red del modelo OSI y que juntos establecen una de las tecnologías más seguras y soportadas, utilizada regularmente para instaurar túneles a través de redes IP, las llamadas Redes Privadas Virtuales (VPN).

NAT.- Es manejado por los routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles, NAT es usada por las redes IPv4.

MARCO PROCIDEMENTAL

1. Diseño de la topología de la red para la práctica 6

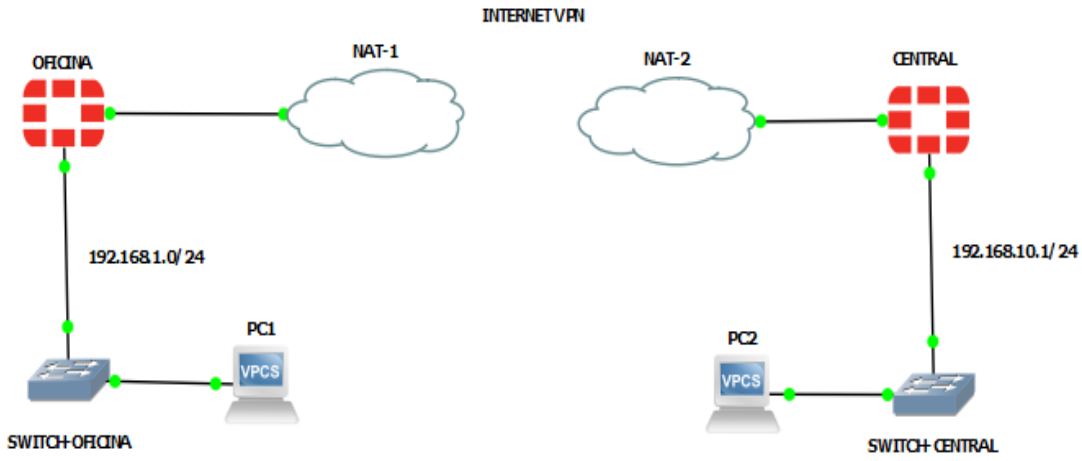


Figura 234. Diseño de la red práctica n°6
Fuente: Los autores

2. Configurar la red local del fortigate oficina en el port2 por DHCP.

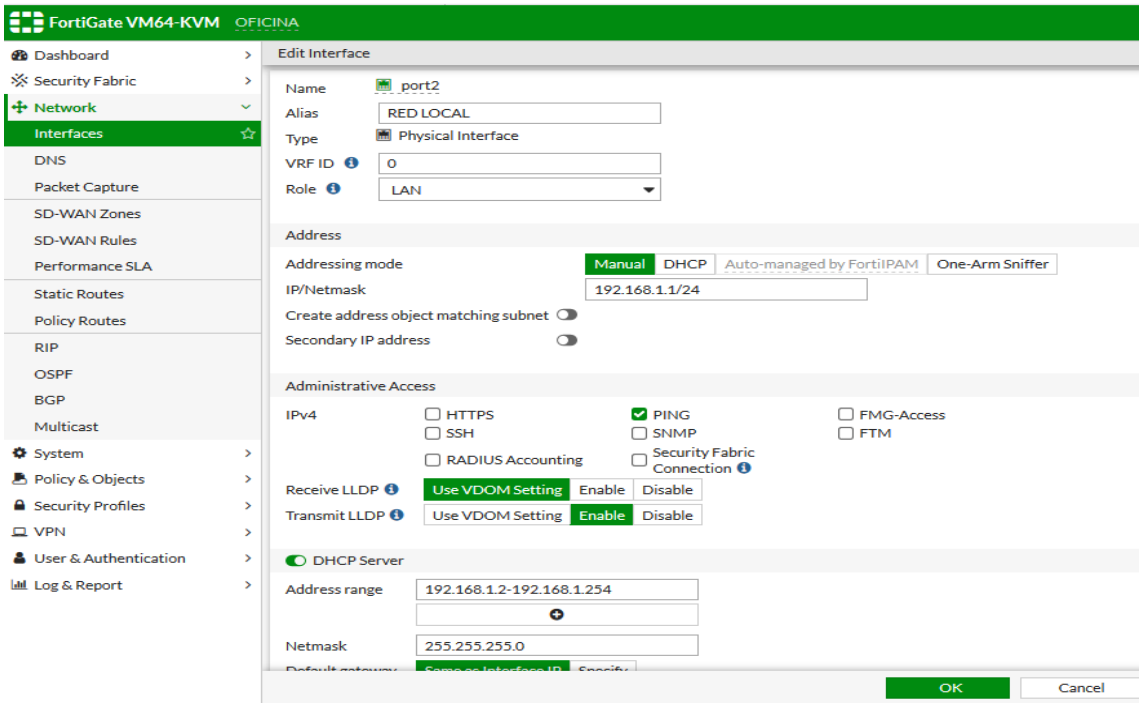


Figura 235. Configuración del port2 oficina
Fuente: Los autores

3. Configurar la red local del fortigate central en port2 por DHCP.

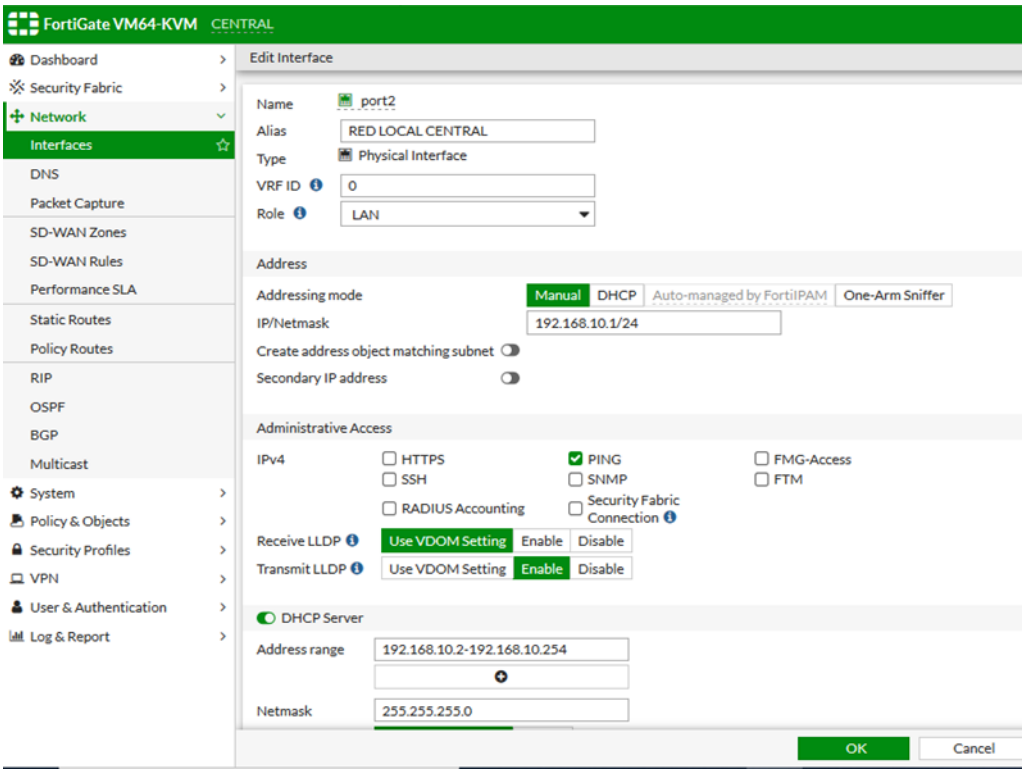


Figura 236. Configuración del port2 central

Fuente: Los autores

4. Configurar static routes para el fortigate-oficina.

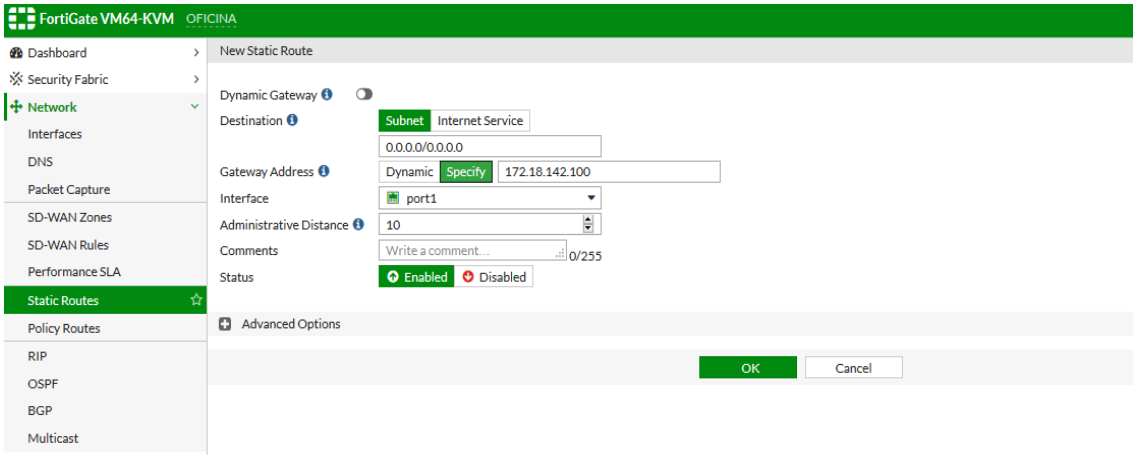


Figura 237. Configuración static routes Oficina
Fuente: Los autores

5. Configuración static routes fortigate central.

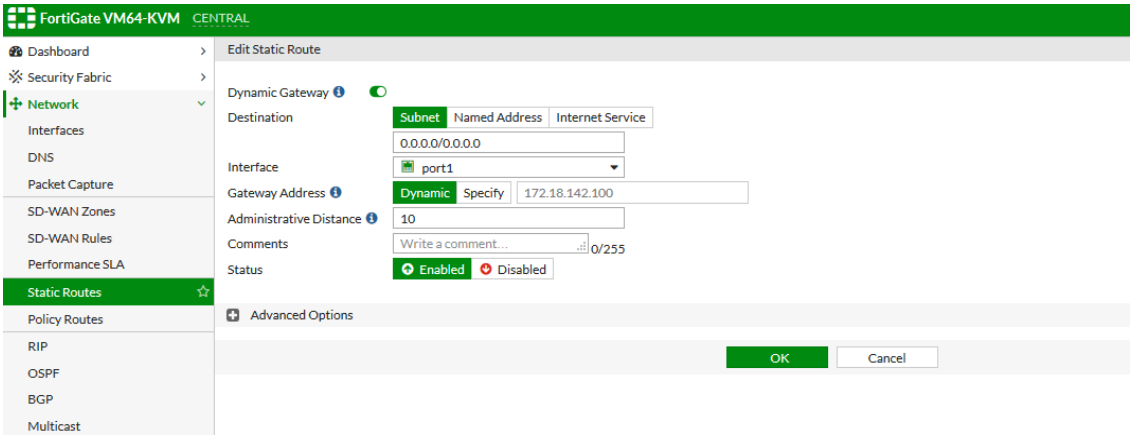


Figura 238. Configuración static routes Central
Fuente: Los autores

6. Configuracion de salida a internet a la red local.

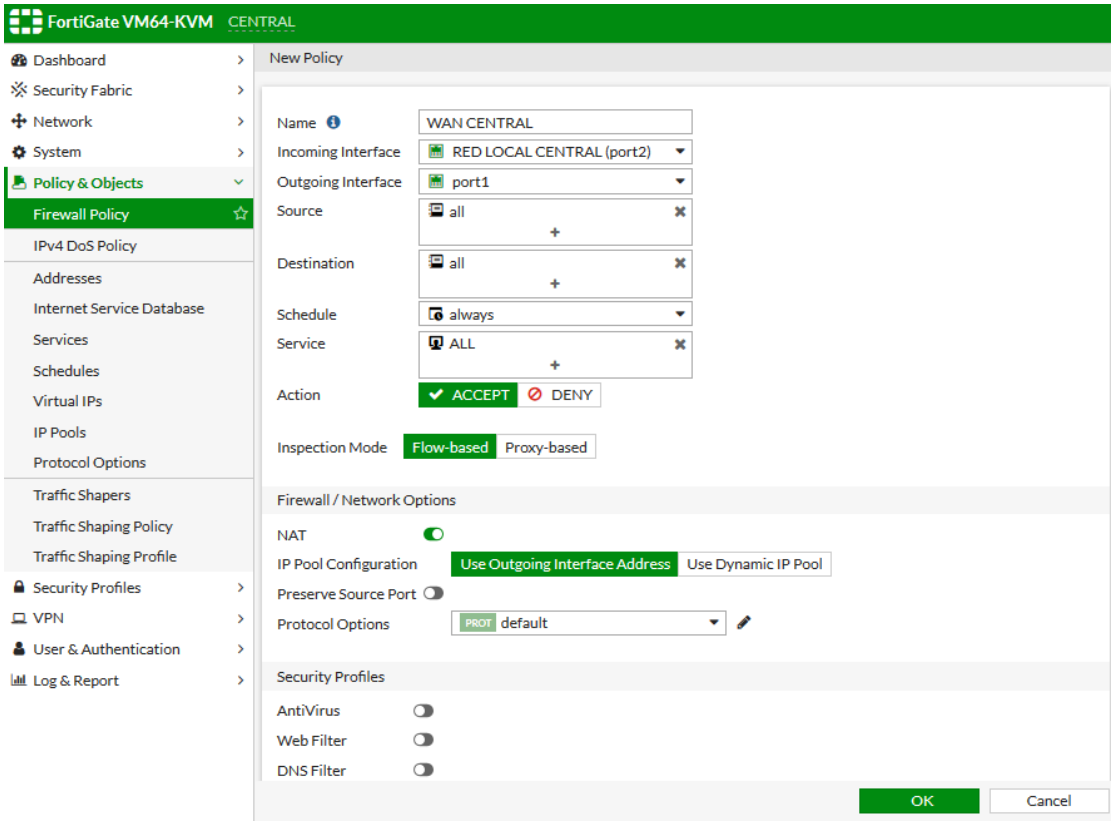


Figura 239. Regla de internet para el fortigate Central
Fuente: Los autores

7. Configurar la regla para salida a internet atravez de nuestra red local.

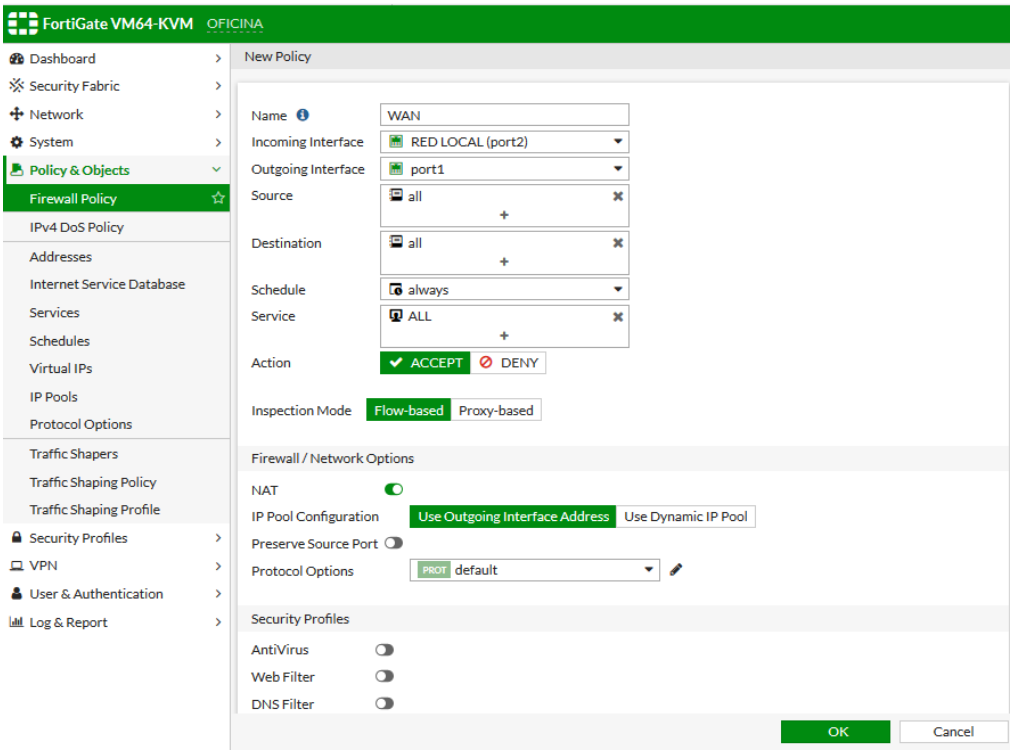


Figura 240. Regla de internet para el fortigate Oficina
Fuente: Los autores

8. Configurar la VPN que nos permitirá la conexión virtual al fortigate central.

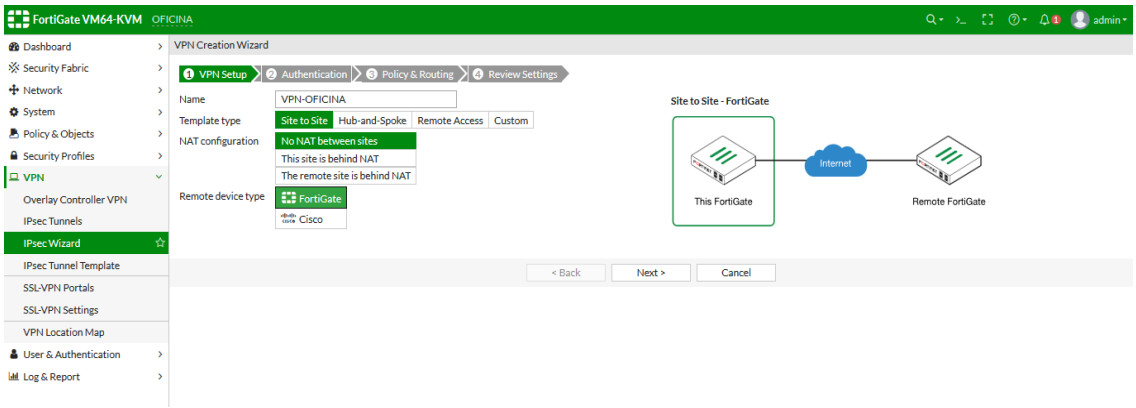


Figura 241. VPN Setup en el fortigate Oficina
Fuente: Los autores

9. Agregar la IP del fortigate central en remote IP address en el fortigate oficina y agregamos un cifrado siguiente ups2020.

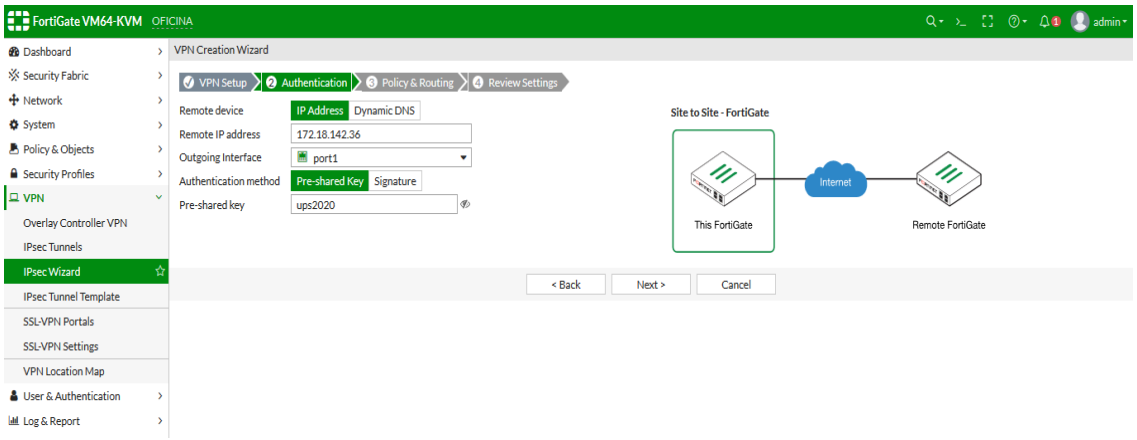


Figura 242. Remote IP address en el fortigate Oficina
Fuente: Los autores

10. Agregar la IP de red local del fortigate oficina que permitirá la comunicación y en remote subnets el Gateway de la red local del fortigate central.

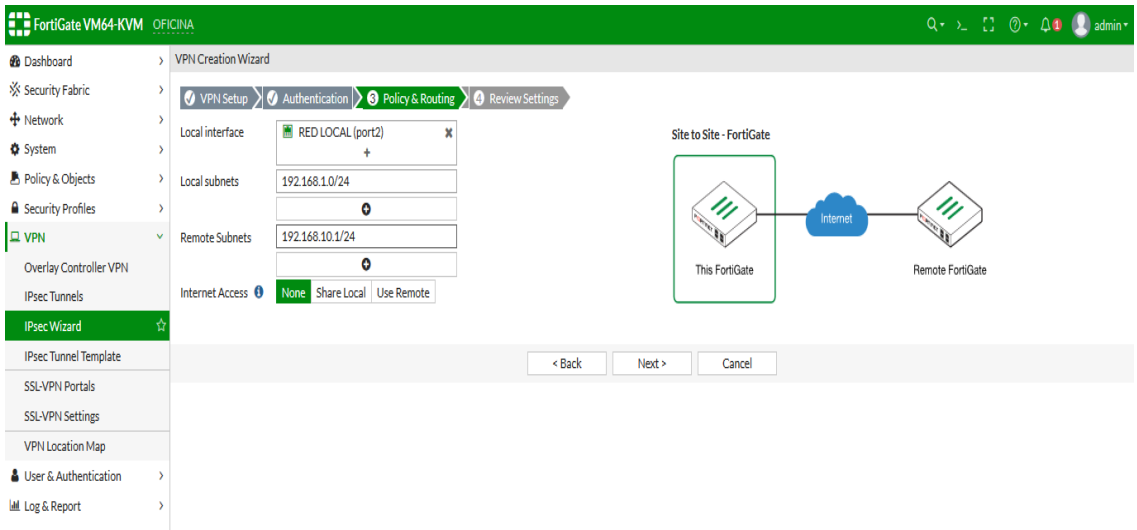


Figura 243.Policy & Routing para el fortigate Oficina
Fuente: Los autores

11. Tunel ipsec fortigate oficina configurado.

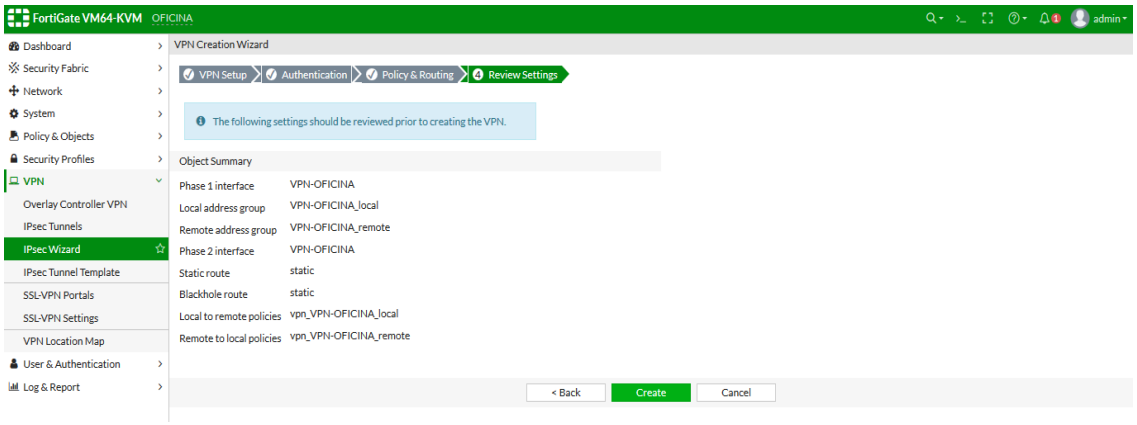


Figura 244.. Review Settings para el fortigate Oficina
Fuente: Los autores

12. Entrar en VPN tunels para ver si esta activo y nos mostrara en estado rojo.

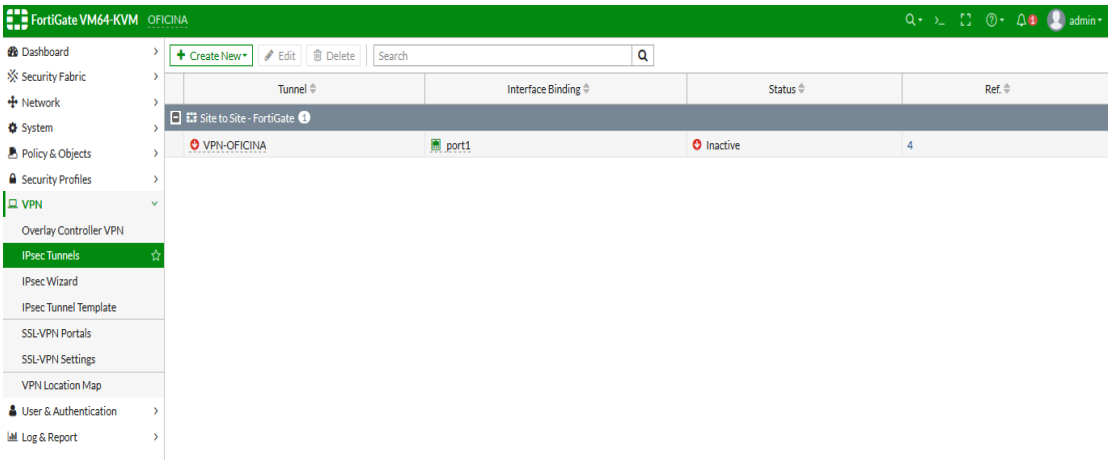


Figura 245. Review Settings para el fortigate Oficina
Fuente: Los autores

13. En static routes se configurara automáticamente.

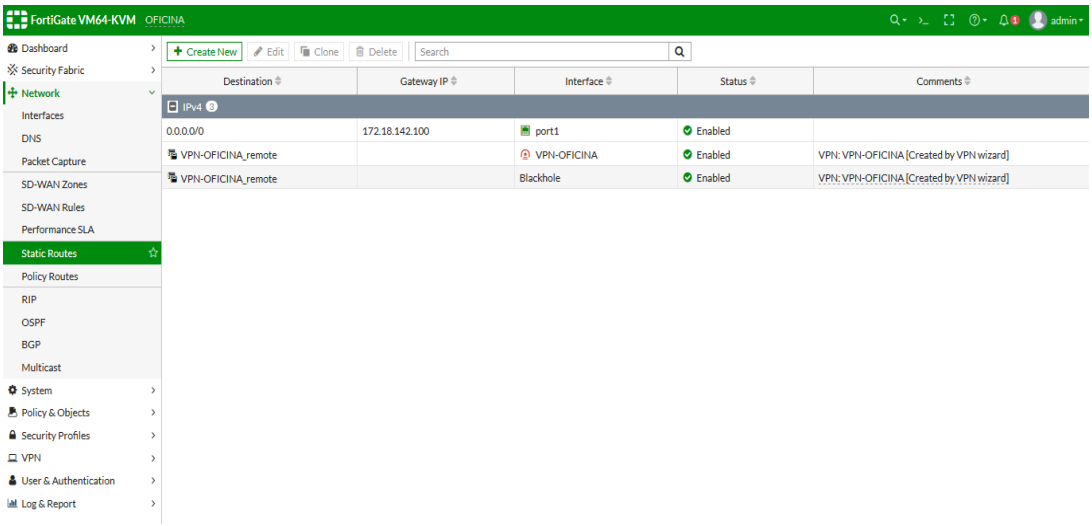


Figura 246. Review Settings para el fortigate Oficina
Fuente: Los autores

14. Se crea las policy automáticamente en el fortigate oficina.

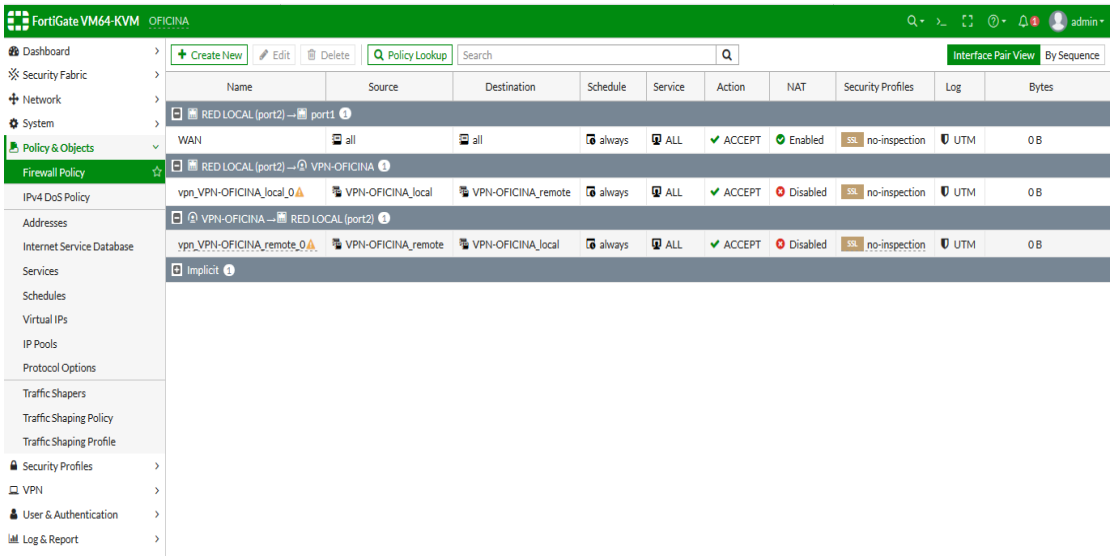


Figura 247. Review Settings para el fortigate Oficina
Fuente: Los autores

15. Configuración de la red VPN del fortigate central.

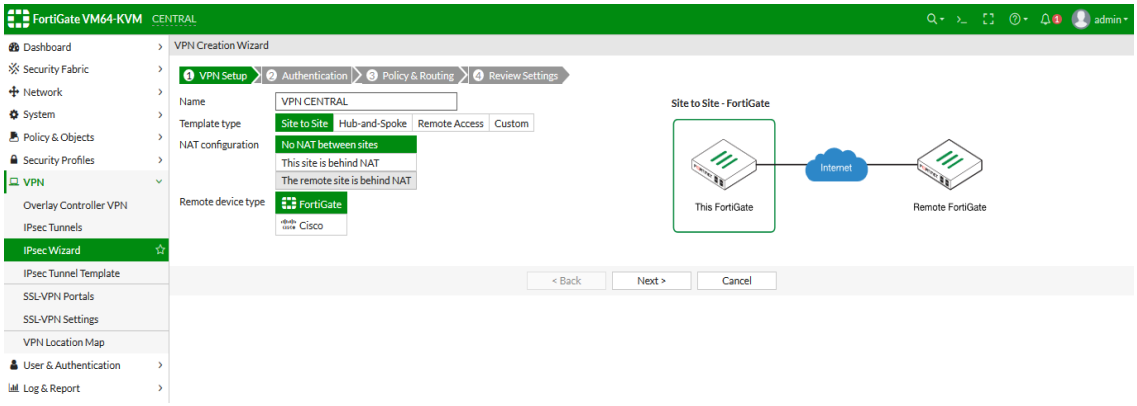


Figura248.VPN Setup en el fortigate Central
Fuente: Los autores

16. Configurar la red remota del fortigate central.

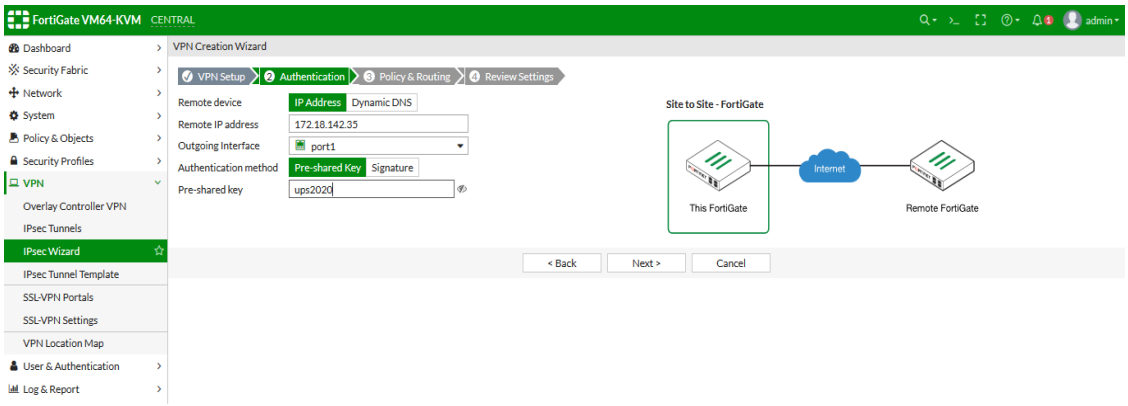


Figura 249. Remote IP address en el fortigate Central
Fuente: Los autores

17. Agregar la IP de red local de l fortigate central que permitirá la comunicación y en remote subnets el Gateway de la red local del fortigate oficina.

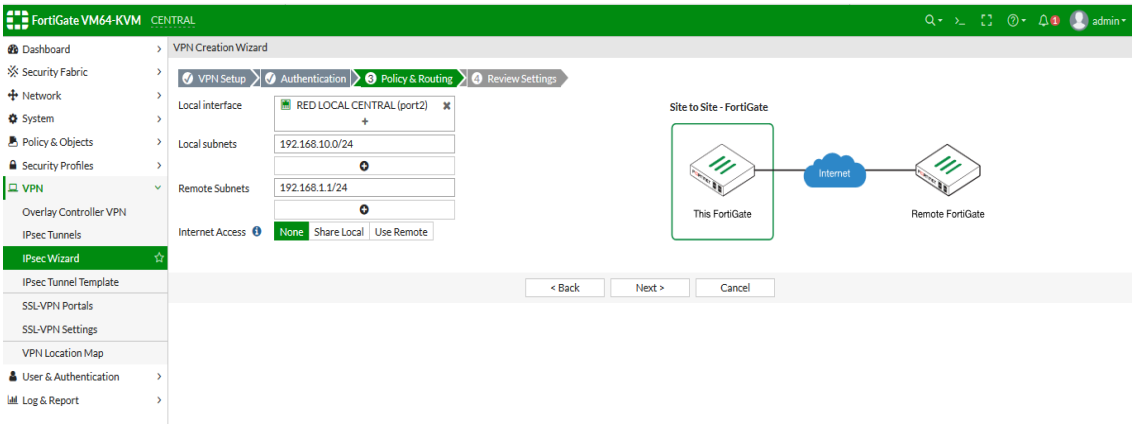


Figura 250. IPSEC para el fortigate Central

Fuente: Los autores

18. Tunel IPSEC fortigate central configurado.

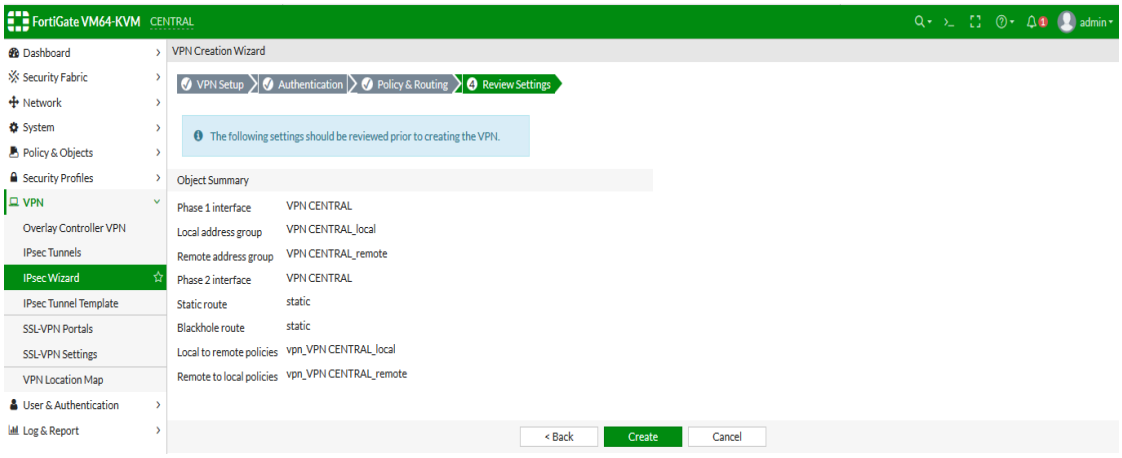


Figura 251. Review Settings para el fortigate Central
Fuente: Los autores

19. Activar VPN el fortigate oficina.

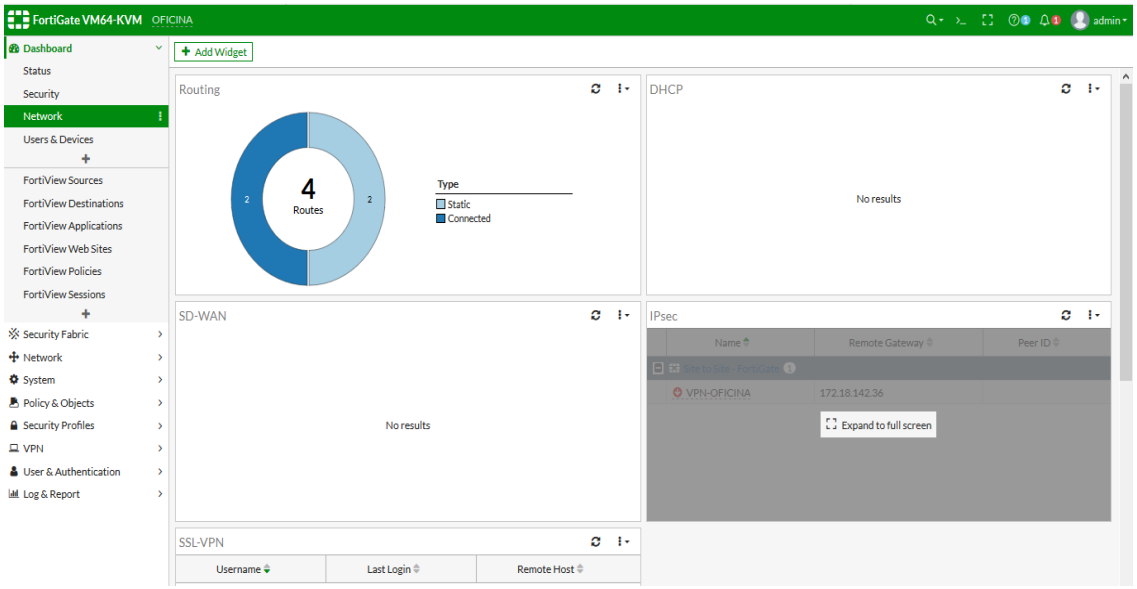


Figura 252 Revisar configuraciones para el fortigate Central
Fuente: Los autores

20. Activar VPN en el fortigate oficina bring up.

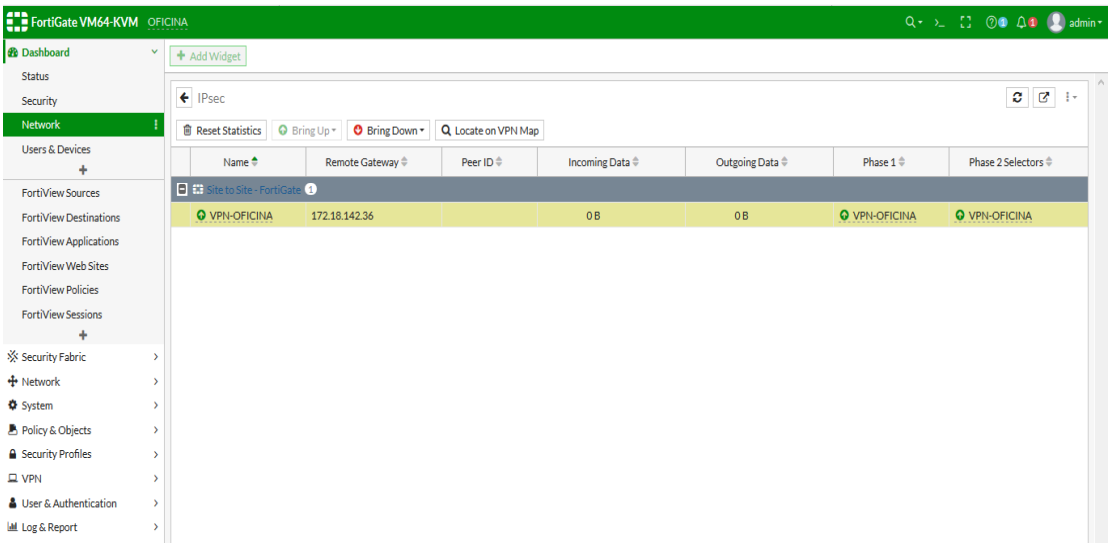


Figura 253. Bring up en el fortigate Oficina
Fuente: Los autores

21. En el fortigate central bring up.

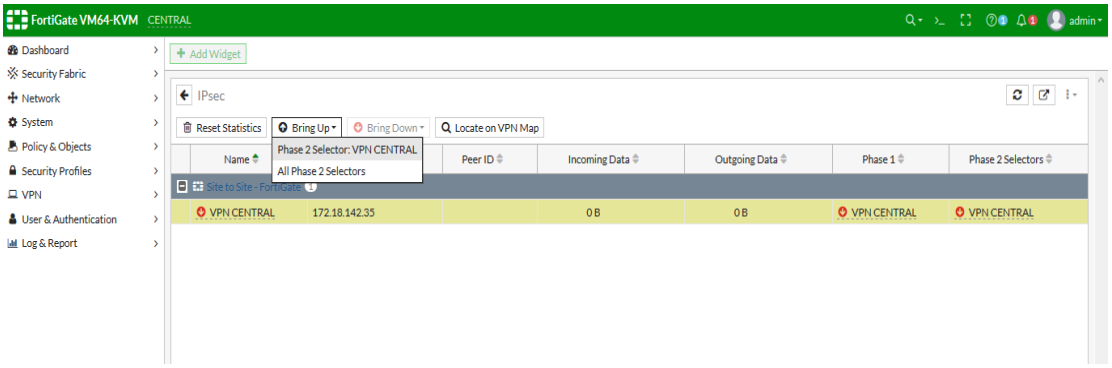


Figura 254. Bring up en el fortigate Central
Fuente: Los autores

22. Realizar ping a la red local del fortigate central.

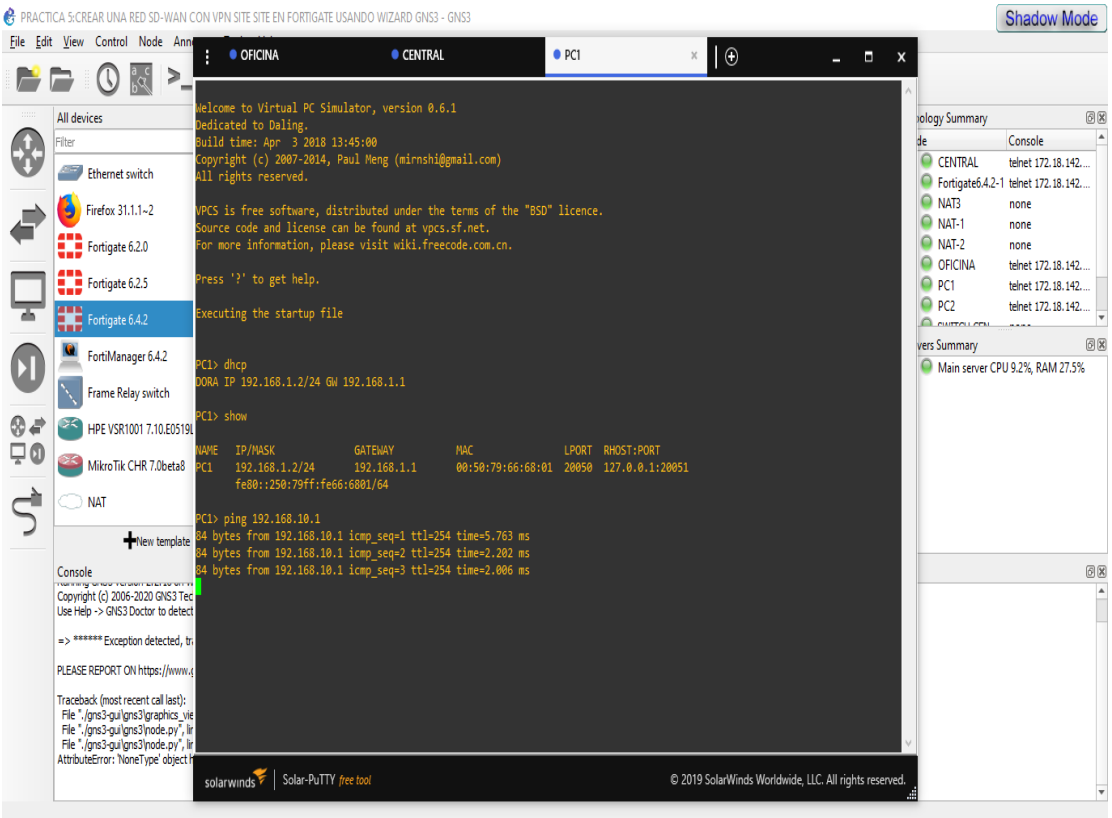


Figura 255. Ping en el fortigate Oficina y Central
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.7. PRÁCTICA 7

Configuración de una red vpn ipsec con balanceo sd-wan.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 7**
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de una red vpn ipsec con balanceo sd-wan.

OBJETIVOS

General

Configurar balanceo SD-WAN atravez de VPN

Específicos

- Configurar vpn ipsec con fortigate.
- Realizar balanceo de la red SD-WAN con VPN.
- Comprobar comunicación entre las subredes.

GLOSARIO

VPN.- Red virtual privada es una tecnología que usa Internet para conectarse a un sitio determinado y de esta forma poder permitir conexión a ciertos servicios.

IPSEC.- Es un framework o colección de protocolos que operan en la capa de Red del modelo OSI y que juntos establecen una de las tecnologías más seguras y soportadas.

SUBREDES.- Una subred es una categoría de direcciones lógicas. cuando una red se vuelve muy extensa, concierta dividirla en subredes.

MARCO PROCEDIMENTAL

1. Diseñar la topología de la red para la práctica 7.

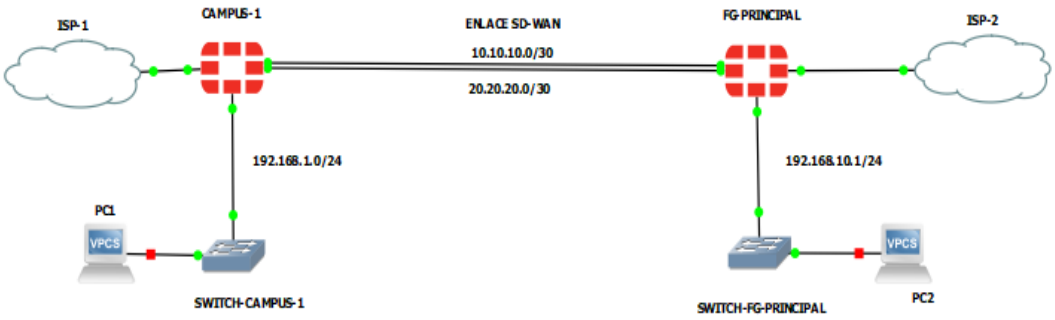


Figura 256. Diseño de la red práctica Nº7
Fuente: Los autores

2. Configurar la dirección IP en el port2 de la interfaz en el fortigate campus-1 que se usara para la SD-WAN y la VPN.

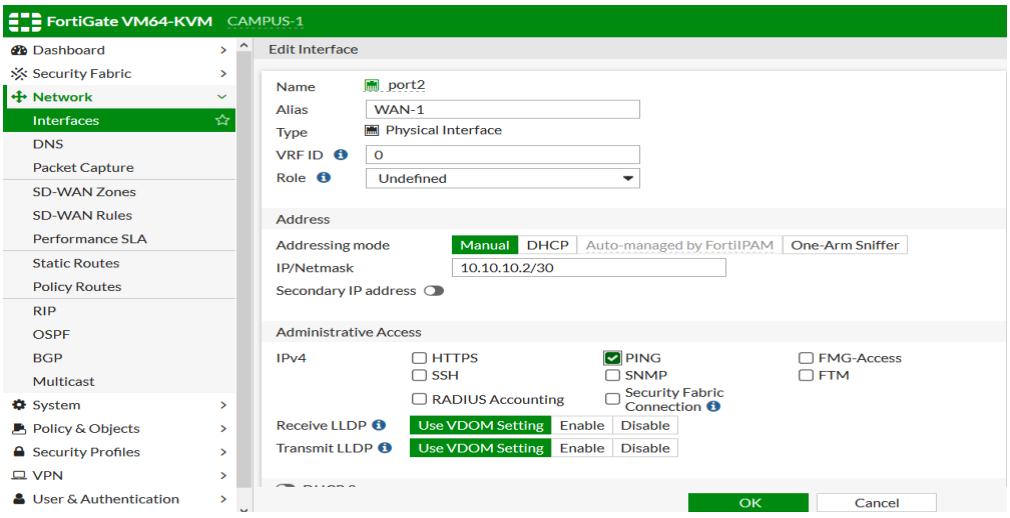


Figura 257.Configuracion IP fortigate campus1 port2
Fuente: Los autores

3. Configurar la dirección IP en el port3 de la interfaz en el fortigate campus-1 que se usara para la SD-WAN y la VPN.

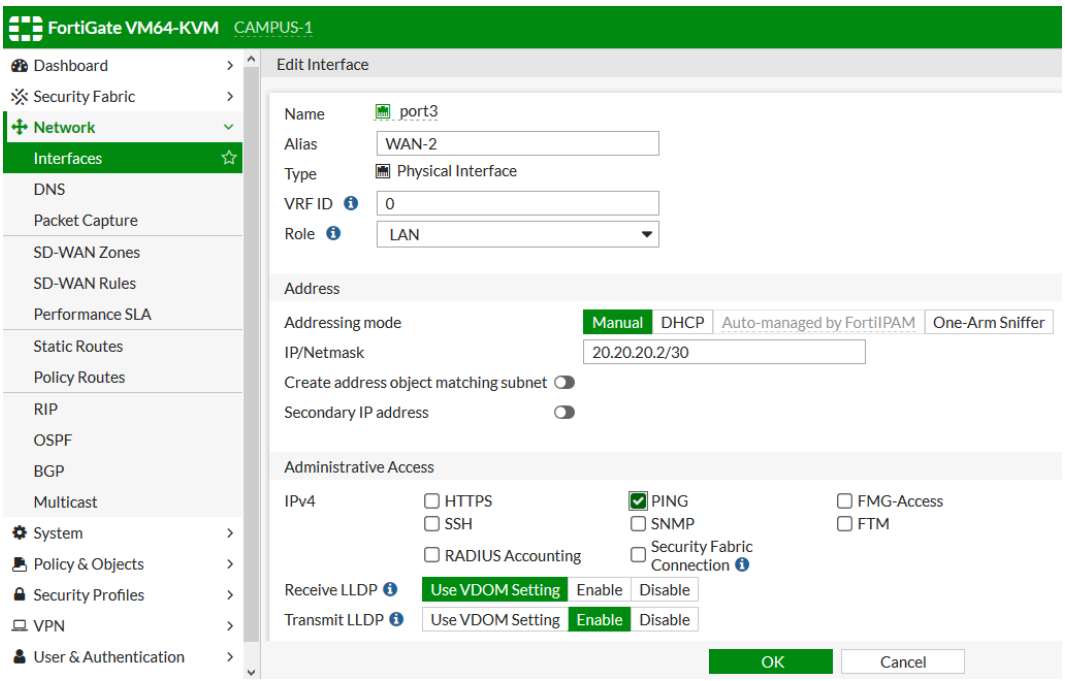


Figura 258.Configuracion IP fortigate campus1 port3
Fuente: Los autores

4. Configurar la red local en el port4 del campus-1.

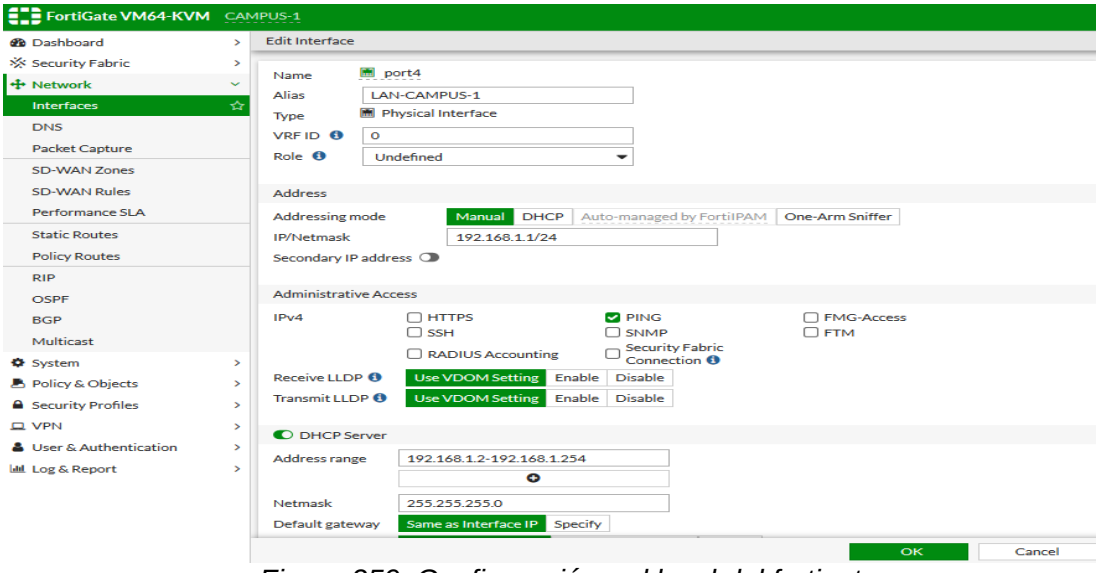


Figura 259. Configuración red local del fortigate
Fuente: Los autores

5. Configurar la VPN dentro del módulo SD-WAN.

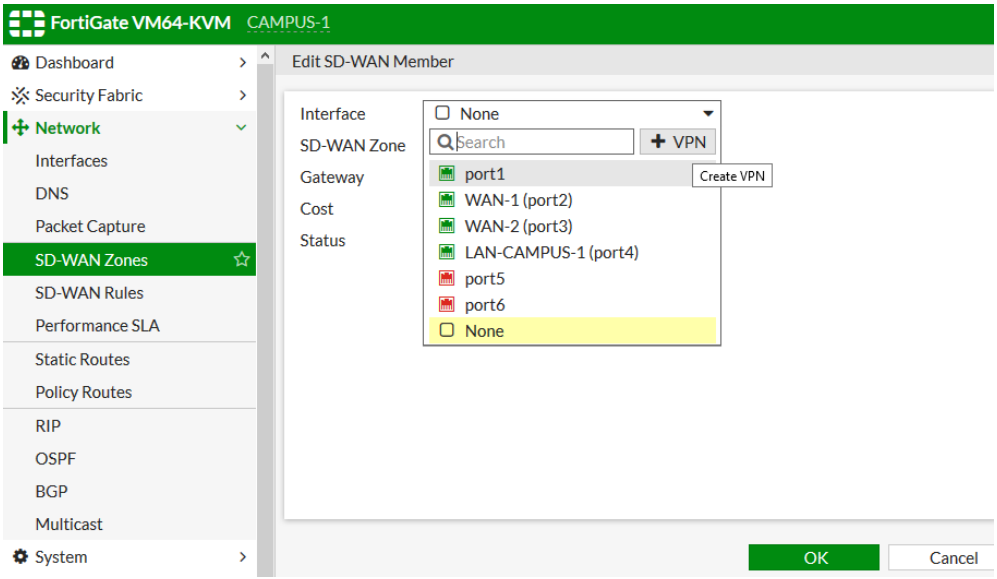


Figura 260. Interfaz SD-WAN port 1 campus 1
Fuente: Los autores

6. Configurar la VPN para WAN-1.

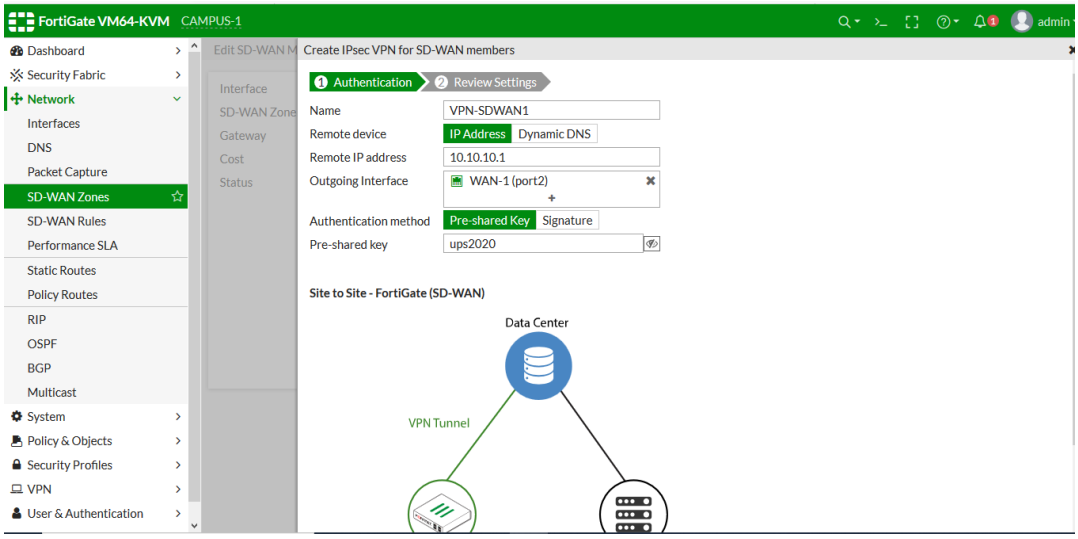


Figura 261. Configuracion VPN WAN 1 campus 1
Fuente: Los autores

7. Configurar la VPN para la WAN 2.

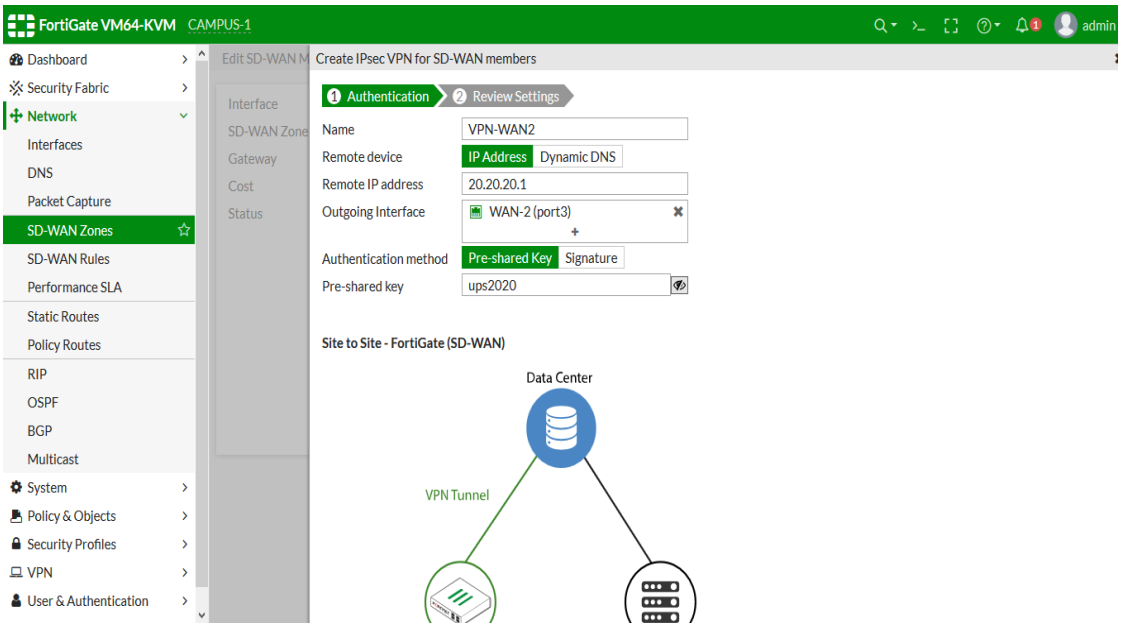


Figura 262. Configuracion VPN WAN 2 campus 1
Fuente: Los autores

8. Seleccionar las interfaces VPN configuradas en la SD-WAN.

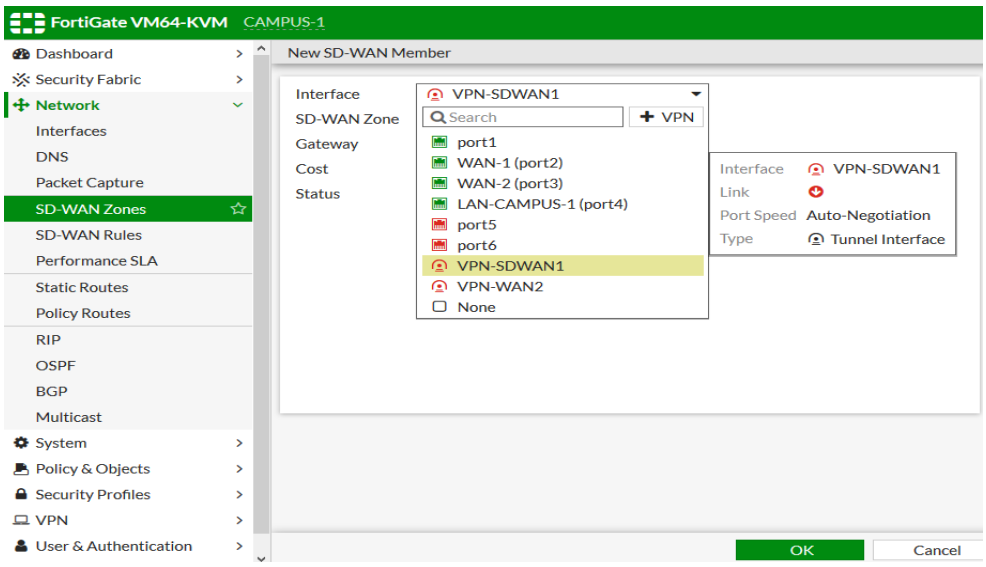
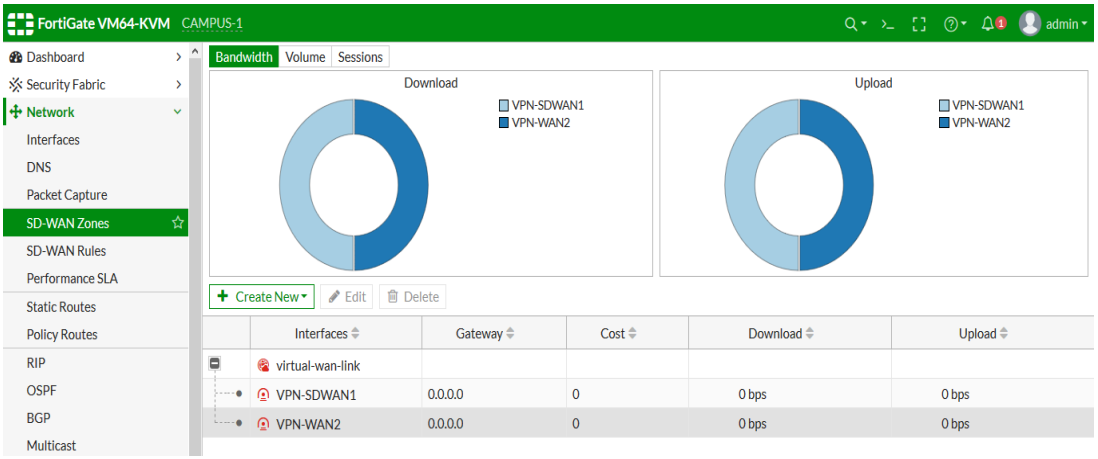


Figura 263. Interfaz VPN SDWAN1 campus 1
Fuente: Los autores

9. Visualización de las interfaces VPN dentro de la sd-wan del fortigate



campus-1.

Figura 264 SD-WAN Zones Campus 1
Fuente: Los autores

10. Activar las vpn para comunicación con el fg-principal.

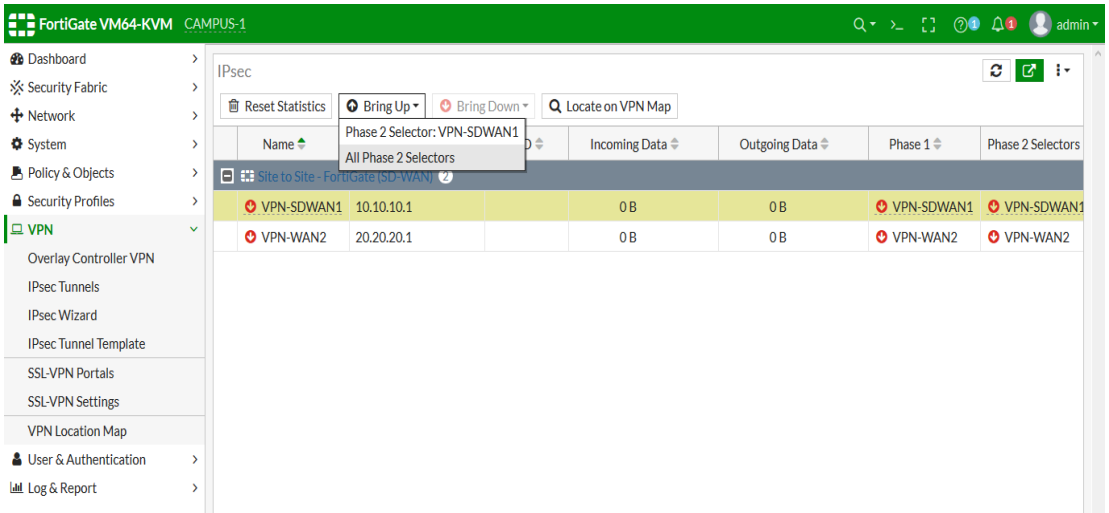


Figura 265Bring up VPN `S
Fuente: Los autores

11. Crear la static routes con la dirección de red local del fg-principal.

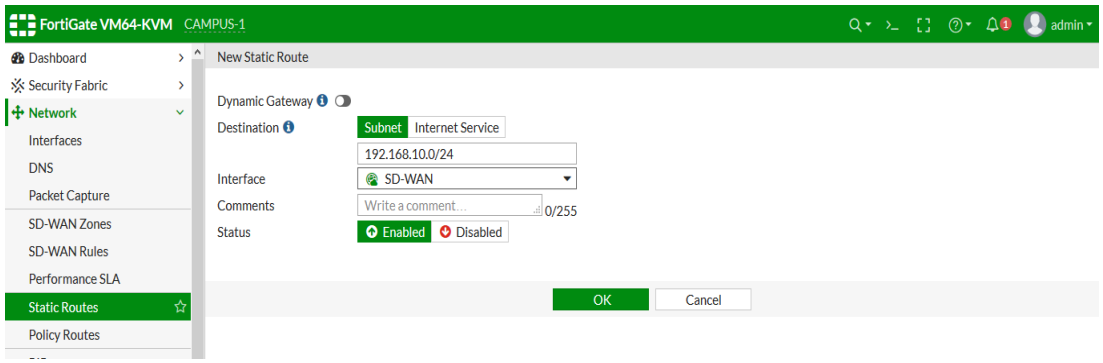


Figura 266. Stattc routes para SD-WAN fortigate campus 1
Fuente: Los autores

12. Crear las políticas para la comunicación entre VPN´S en fortigate campus-1.

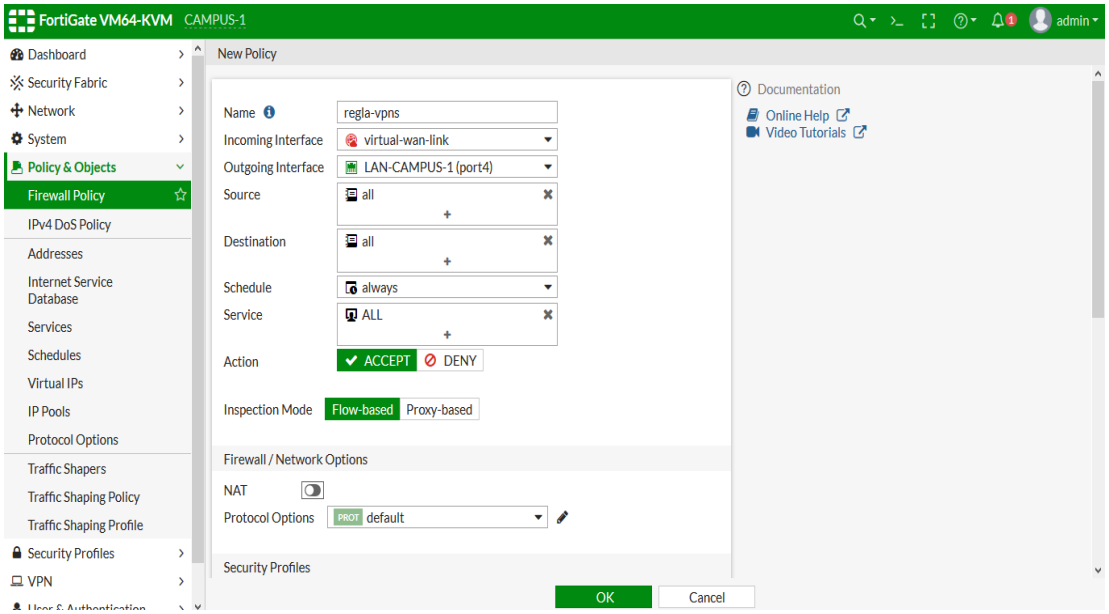


Figura 267. Firewall Policy SD-WAN fortigate campus 1
Fuente: Los autores

13. Política para la salida a internet de la red local del campus-1.

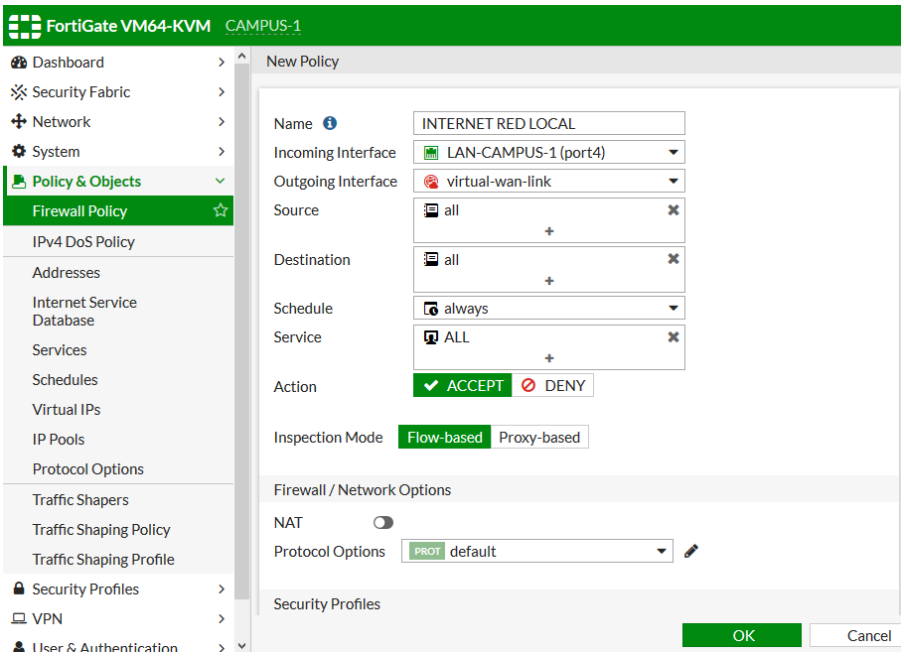


Figura 268. Firewall Policy Intternet red local fortigate campus 1
Fuente: Los autores

14. Configurar la interfaz port2 en el fg-principal.

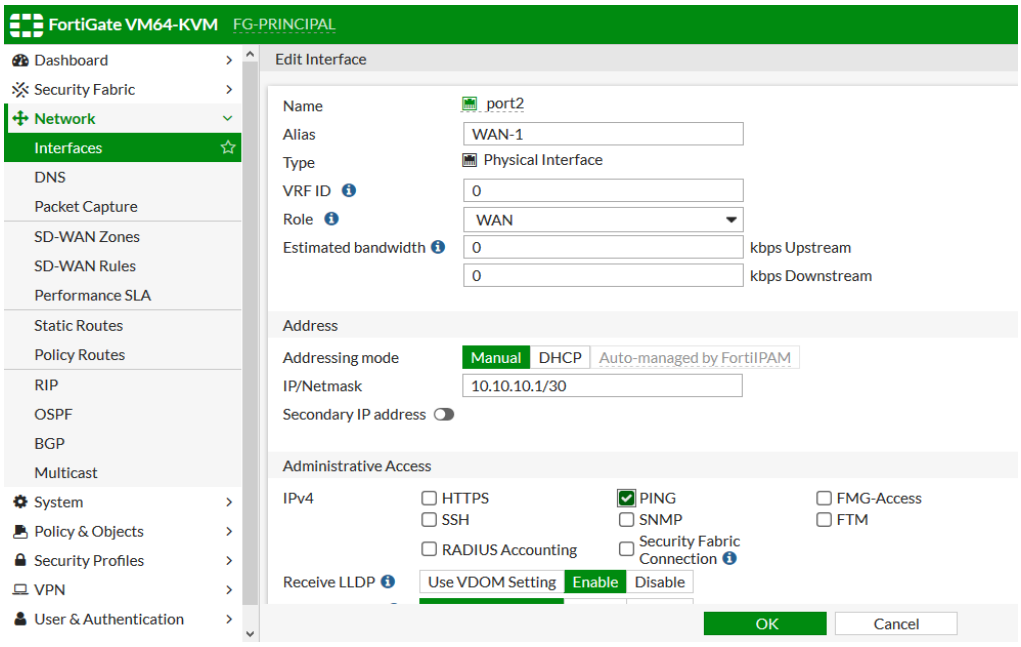


Figura 269.Configuracion interfaz port2 fortigate fg-principal
Fuente: Los autores

15. Configurar port3 en el fg-principal para la WAN-2.

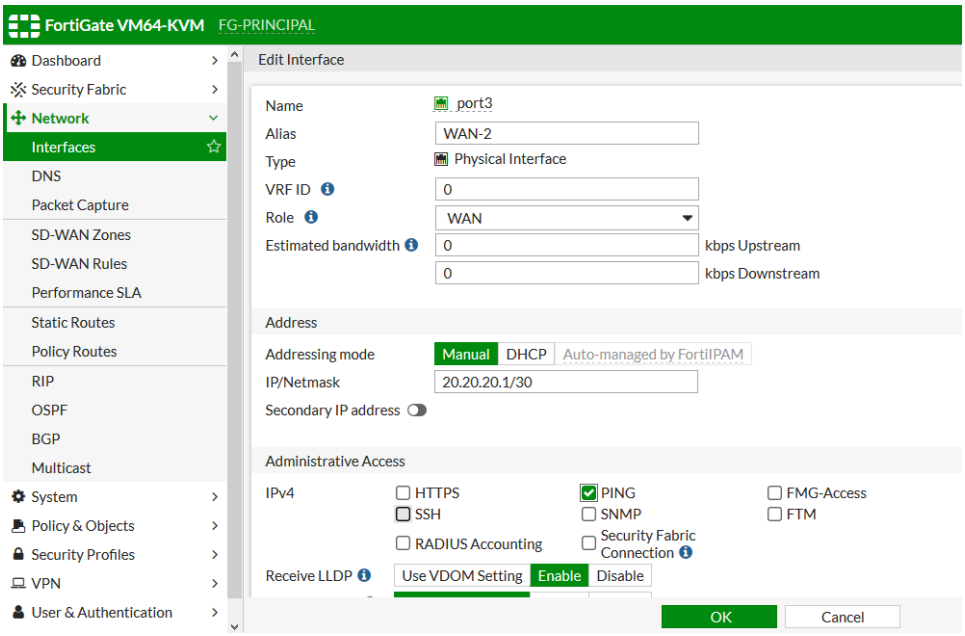


Figura 270.Configuracion IP fortigate principal port3
Fuente: Los autores

16. Configurar el port4 para la red local del fg-principal.

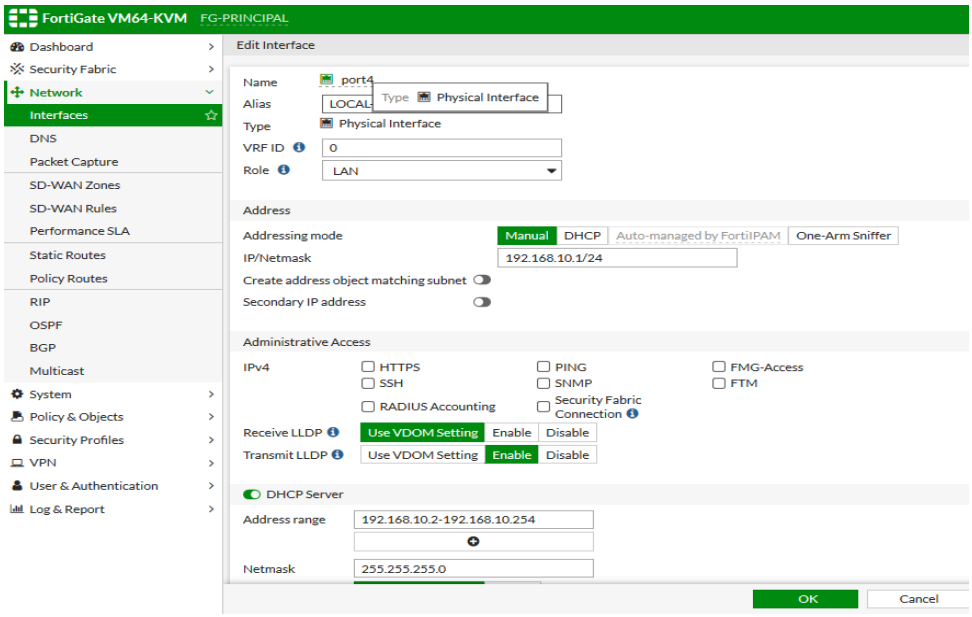


Figura 271.Configuracion IP fortigate principal port4
Fuente: Los autores

17. Configurar la VPN que pertnece a la WAN-1.

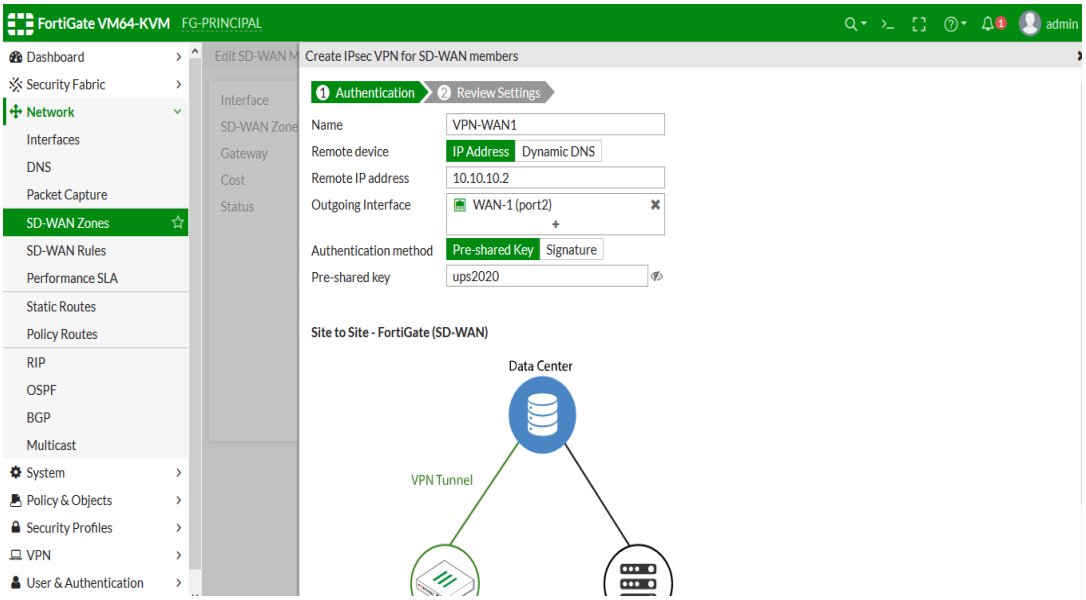


Figura 272. Configuracion VPN WAN 1 principal
Fuente: Los autores

18. Configurar la VPN que pertenece a la WAN-2.

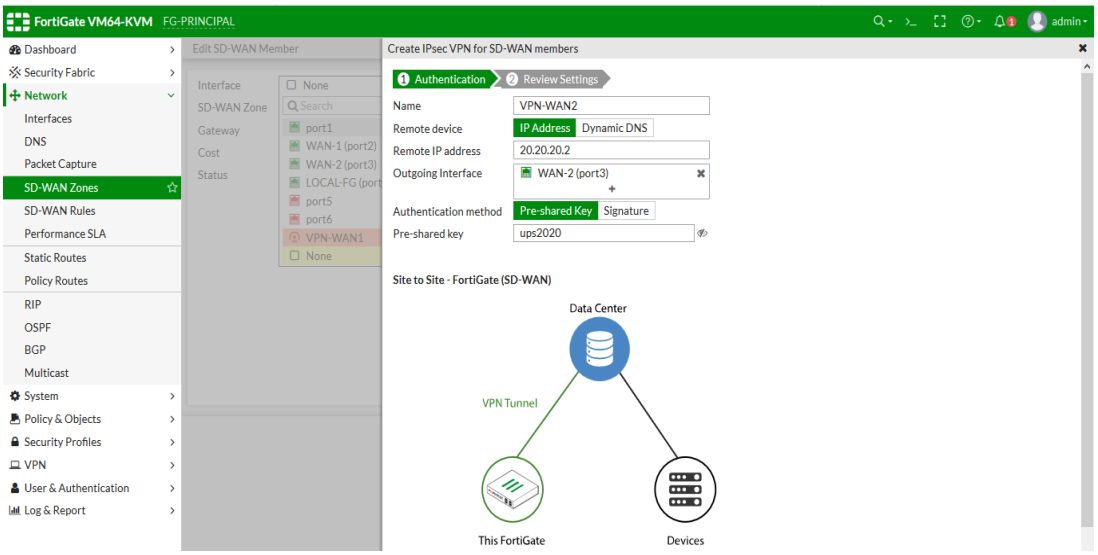


Figura 273. Configuracion VPN WAN 2 principal
Fuente: Los autores

19. Asignar las VPN a la SD-WAN

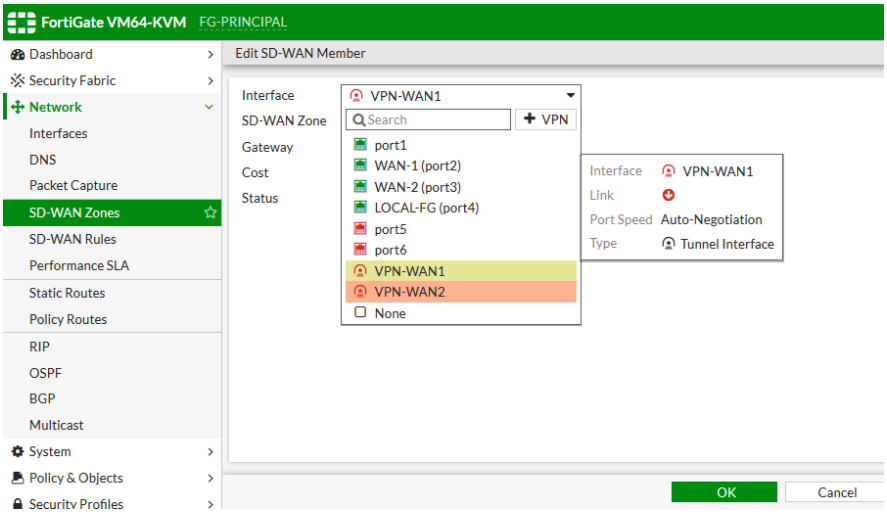


Figura 274. Interfaz VPN SDWAN1 princpal
Fuente: Los autores

20. Visualizar las VPN configuradas en la sd-wan del fg-principal.

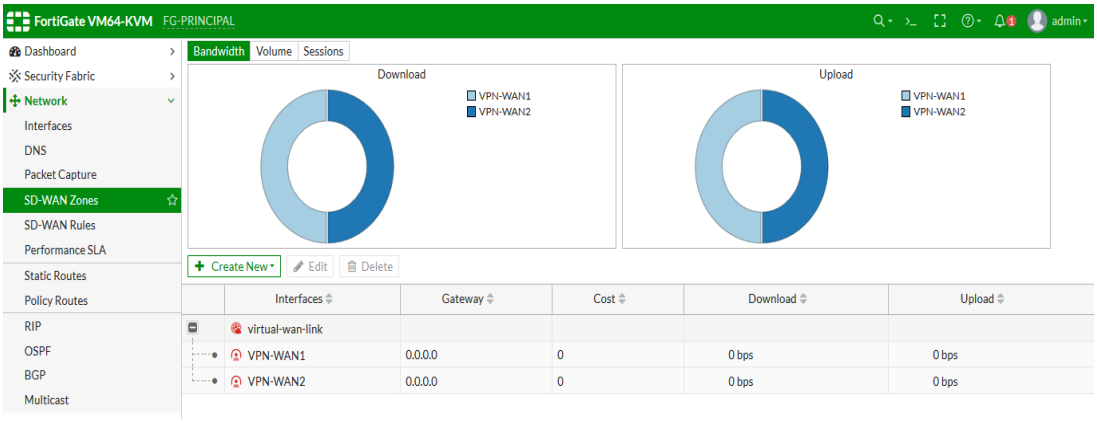


Figura 275. SD-WAN Zones Principal
Fuente: Los autores

21. Activar las VPN´S para comunicación entre las interfaces.

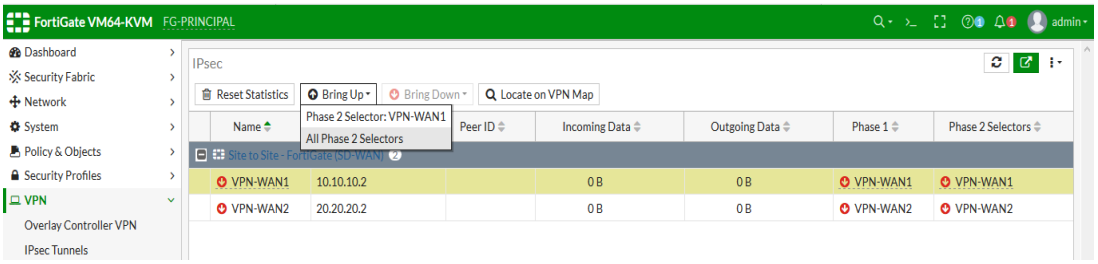


Figura 276 Bring up VPN `S principal
Fuente: Los autores

22. Gráfico de VPN´S activadas.

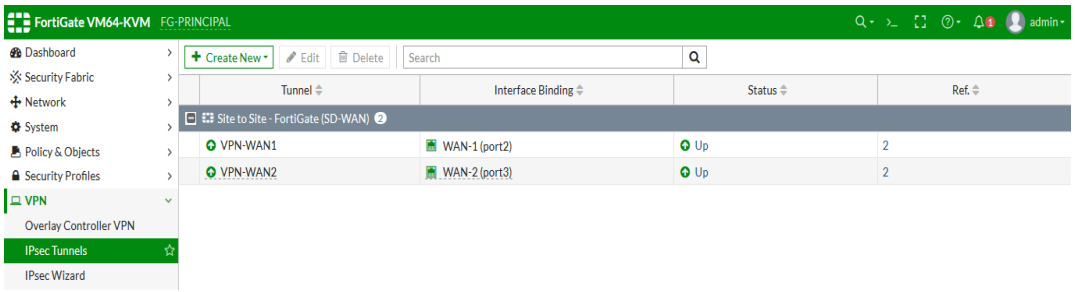


Figura 277 VPN `S principal activadas
Fuente: Los autores

23. Crear static routes para la comuniacion de la red local del fg-principal con el campus-1.

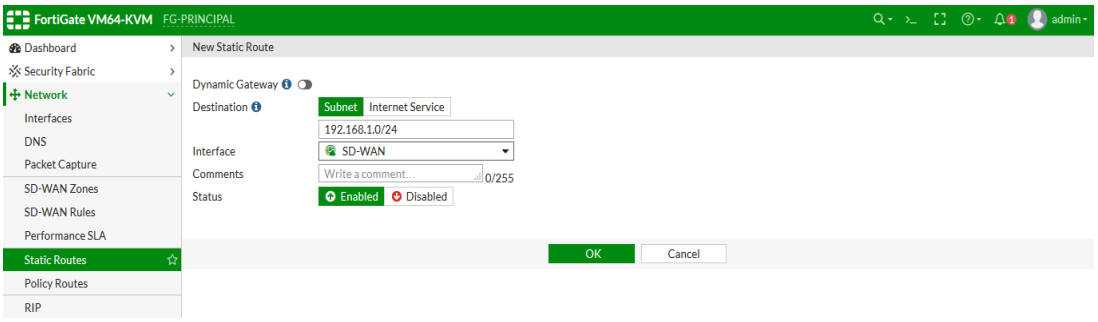


Figura 278. Stattc routes para SD-WAN fortigate fg-principal
Fuente: Los autores

24. Crear políticas para la comunicación entre VPN´S.

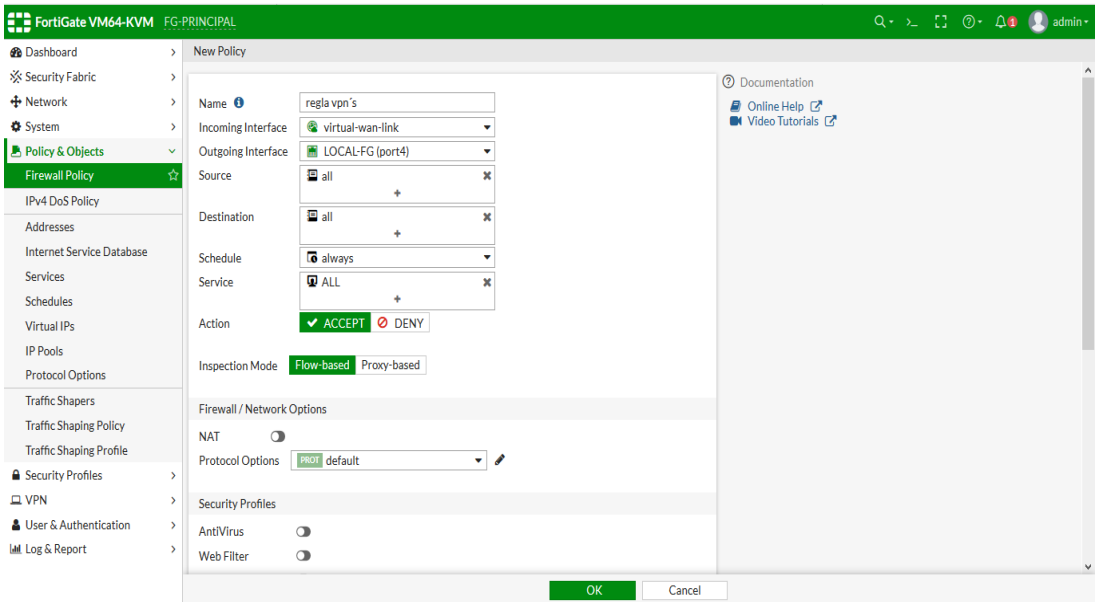


Figura 279. Firewall Policy SD-WAN fortigate fg-principal 1
Fuente: Los autores

25. Politica para salida a internet red local.

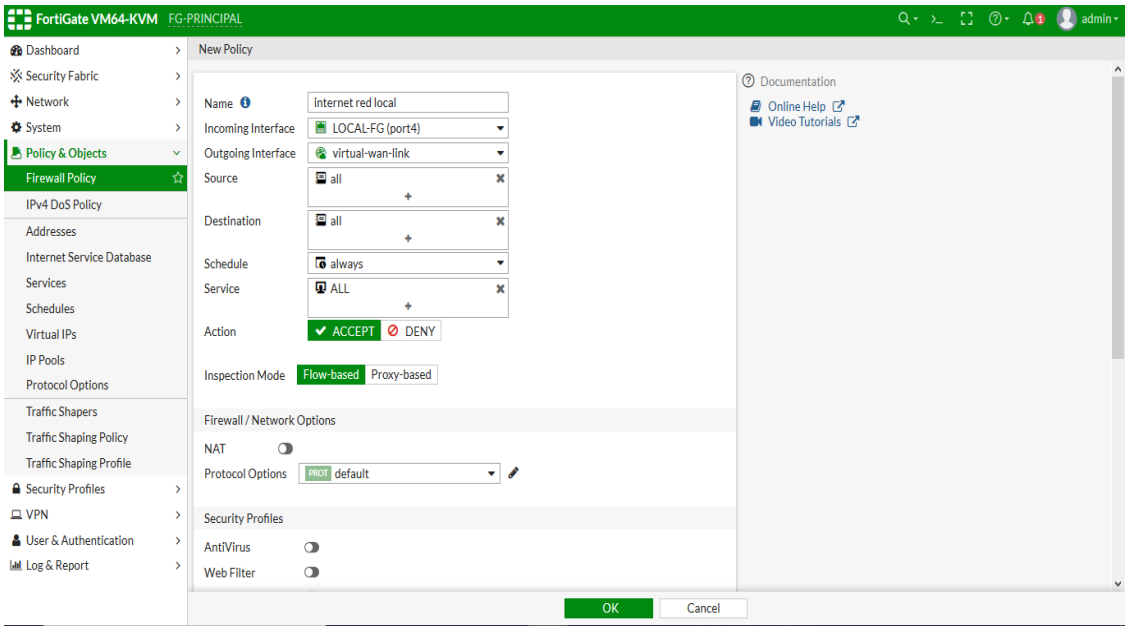


Figura 280. Firewall Policy Intternet red local fortigate fg-principal
Fuente: Los autores

26. Politica para navegación de internet para la SD-WAN.

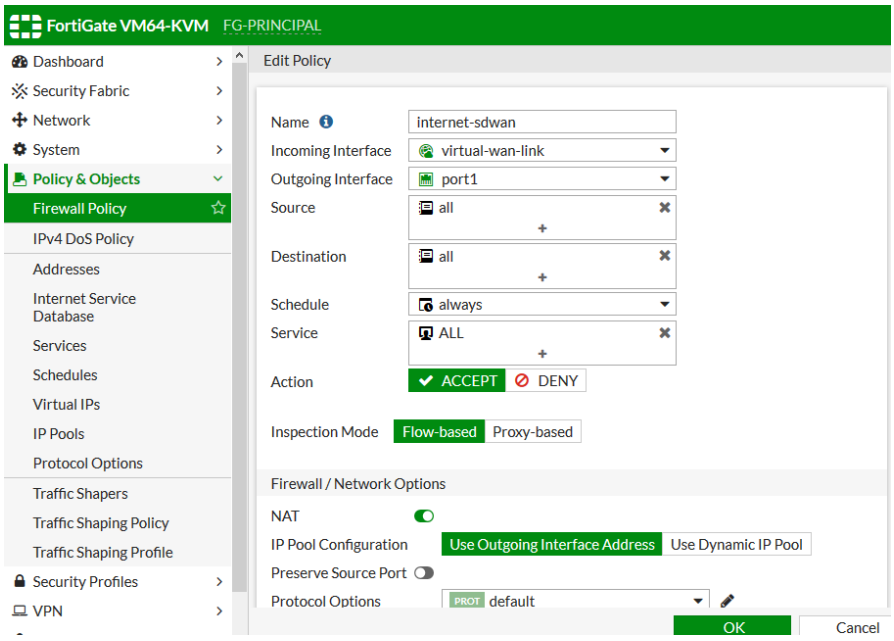


Figura 281. Firewall Policy Intternet SD-WAN fortigate fg-principal
Fuente: Los autores

27. Configurar static routes de la SD-WAN en el fortigate campus-1.

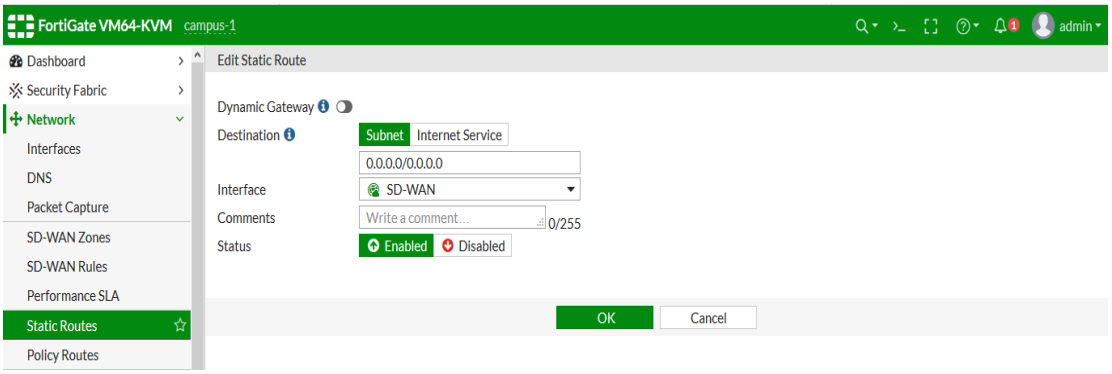


Figura 282. Configuracion static routes SD-WAN campus1
Fuente: Los autores

28. Ping entre red locales de cada fortigate y google.

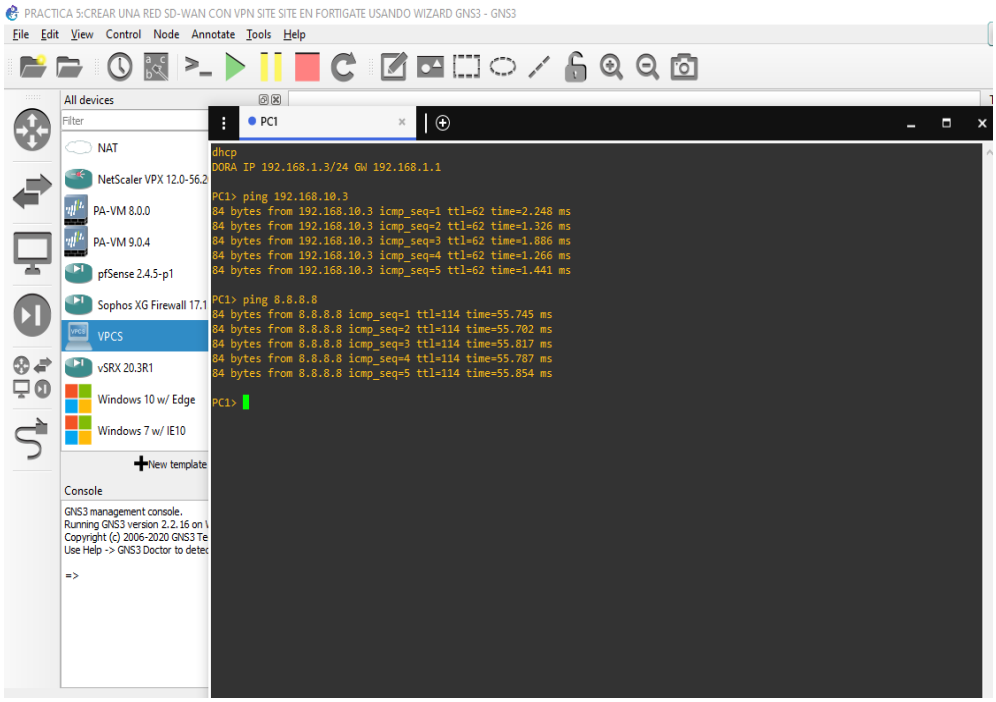


Figura 283 Ping en el fortigate campus y fg-primcipal
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.8. PRÁCTICA 8

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 8**
- **NUMERO DE COMPUTADORAS**: 10
- **TIEMPO CONSIDERADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de un failover con mikrotik para un enlace SD-WAN.

OBJETIVOS

General

Configurar un failover con mikrotik para un enlace SD-WAN.

Específicos

- Configurar Failover con mikrotik.
- Establecer un fortigate WAN.
- Comprobar la comunicación del Failover.

GLOSARIO

FAILOVER.- También llamada conmutacion por error el cual funciona como un respaldo, cuando se presenta un fallo en unas de nuestras redes WAN este entra a funcionar de manera automática, asi no se vera afectado nuestros dispositivos finales.

WAN.- Se la conoce también como red de área amplia, se compone de varias redes LANS ubicadas alrededor del globo terráqueo.

ISP.- Son siglas usadas en telecomunicaciones y su definición es Internet Service provider el cual prorpociona de una compañía servicio de internet como por ejemplo Claro, Telconet, Telefonica.

MARCO PROCEDIMENTAL

1. Diseñar la topología de la red para la práctica 8.

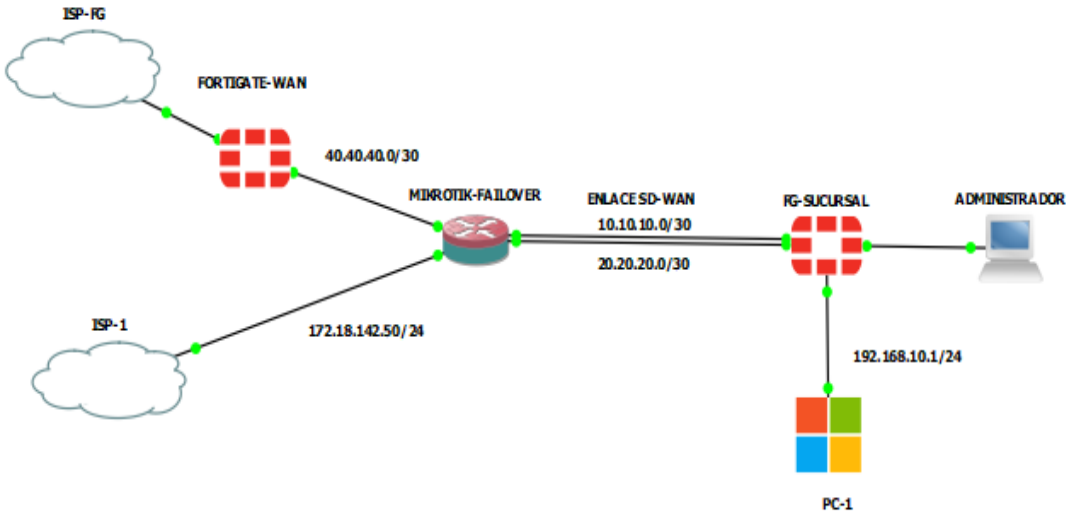


Figura 284. Diseño de la red práctica Nº8
Fuente: Los autores

2. Configurar el port2 del fortigate WAN para el enlace FAILOVER al mikrotik.

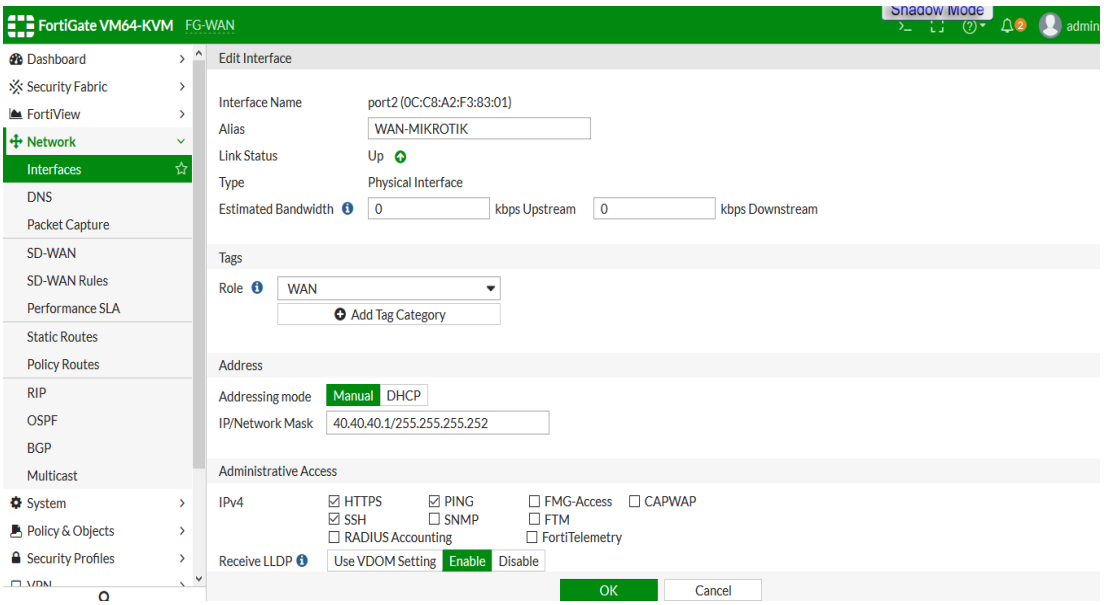


Figura 285.Configuracion IP fortigate FG-WAN port2
Fuente: Los autores.

3. Configurar la static routes al FG-WAN.

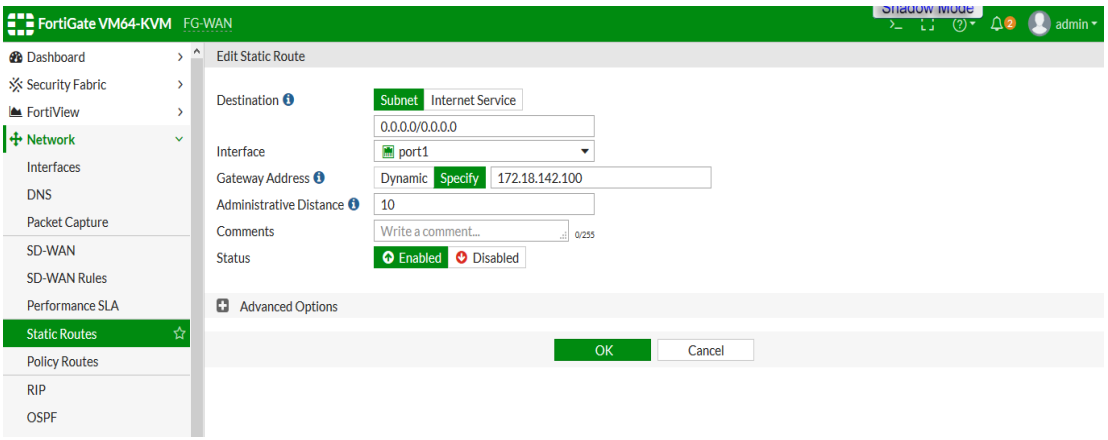


Figura 286. Configuración static routes FG-WAN port 1
Fuente: Los autores

4. Configurar la regla en el firewall para salida de internet a la WAN para mikrotik.

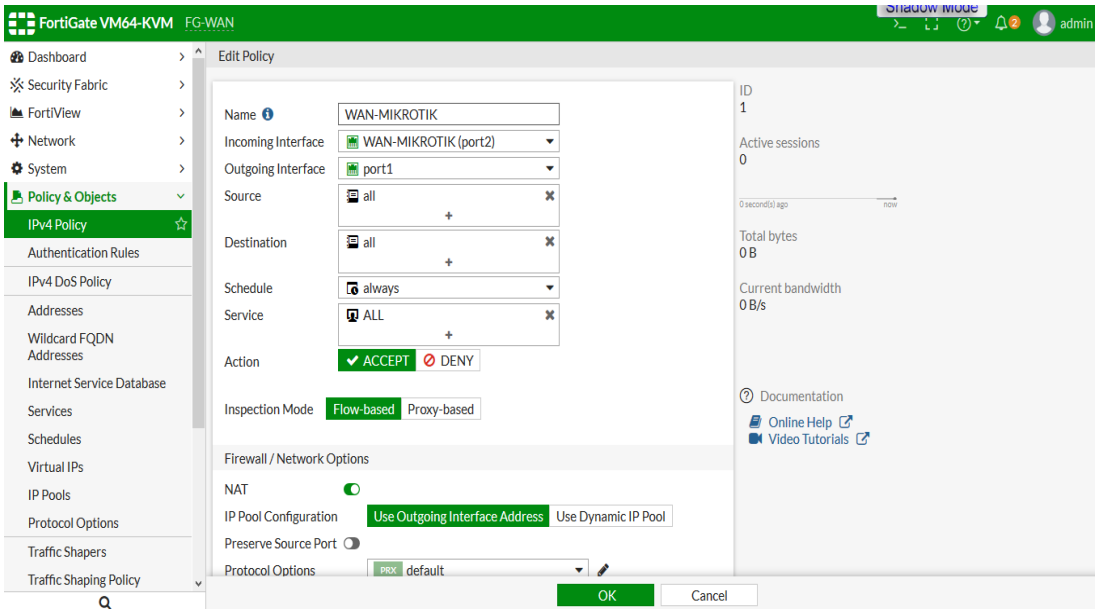


Figura 287. Configuracion Policy FG-WAN port1
Fuente: Los autores

5. Abrir winbox y seleccionar el routerboards que vamos a configurar el faiolver.

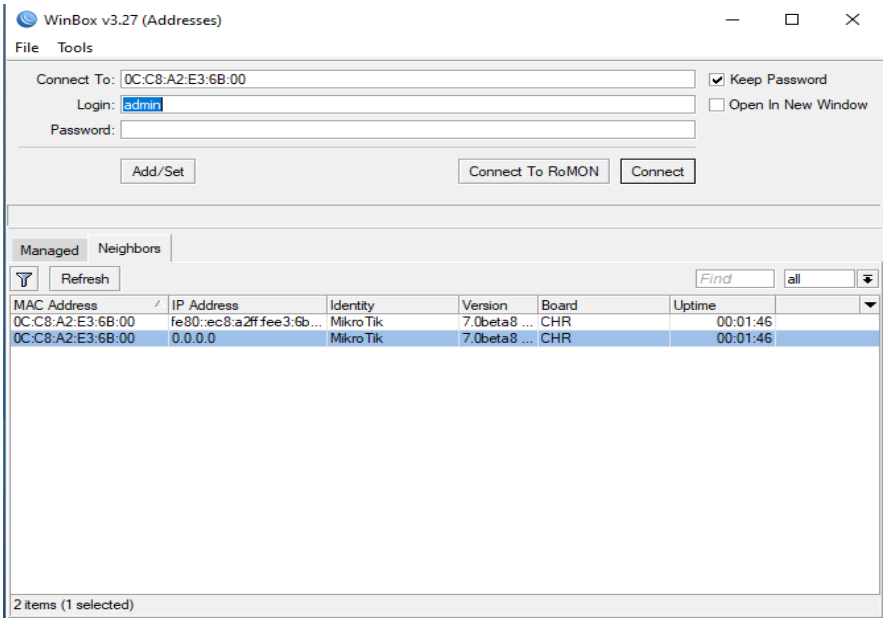


Figura 288. Elección del Routerboard para failover
Fuente: Los autores

6. Damos click en IP- ADDRESS y en la cruz azul agregamos la IP del ISP-1 a la eth1.

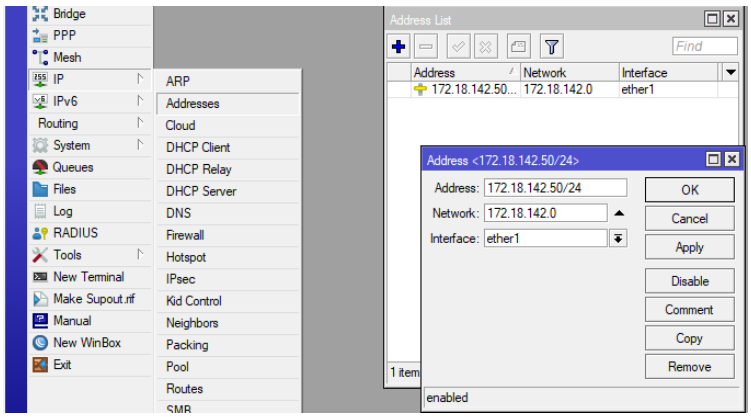


Figura 289.Añadir IP para ISP1-ethe1
Fuente: Los autores

7. Agregar la IP a la eth2 del fortigate WAN que nos simulara de ISP.

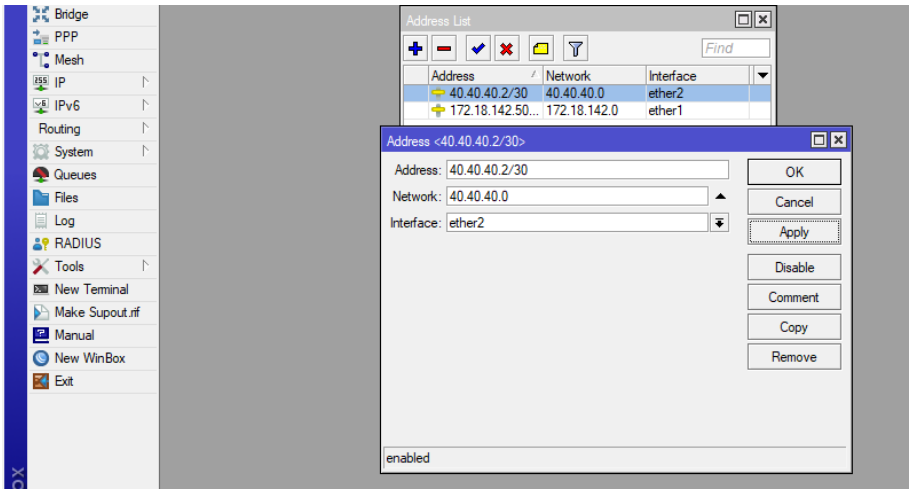


Figura 290.Añadir IP para ISP1-ethe2
Fuente: Los autores

8. Agregar los DNS al router mikrotik se puede usar los de google o del router local.

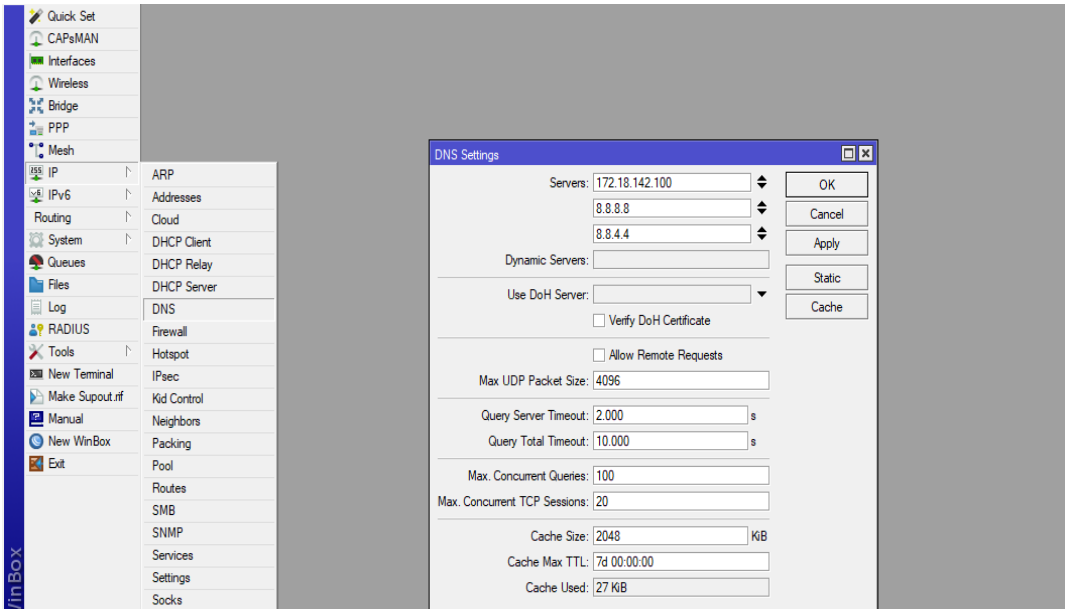


Figura 291. Añadir DNS a router Mikrotic
Fuente: Los autores

9. Configurar en FIREWALL opción NAT para la salida de internet del eth1.

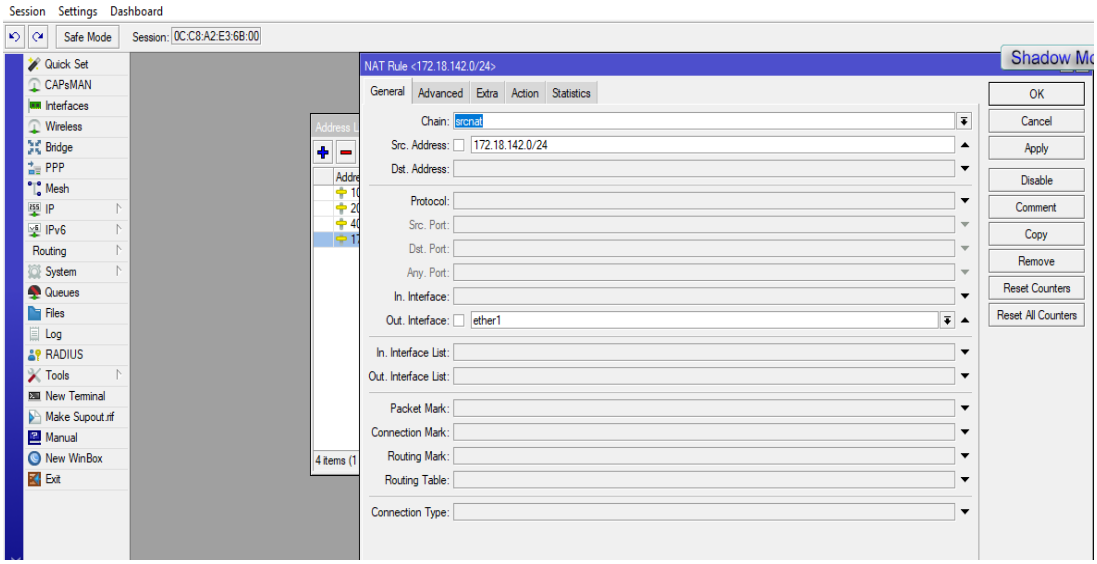


Figura 292.Configuracion de Firewall ethe 1 (a)
Fuente: Los autores

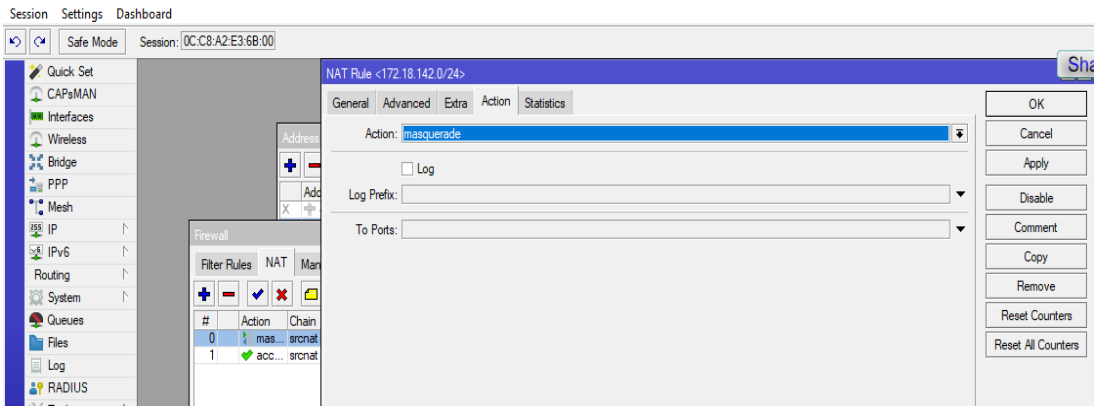


Figura 293.Configuracion de Firewall ethe 1 (b)
Fuente: Los autores

10. Configurar en FIREWALL opción NAT para la salida de internet del eth2.

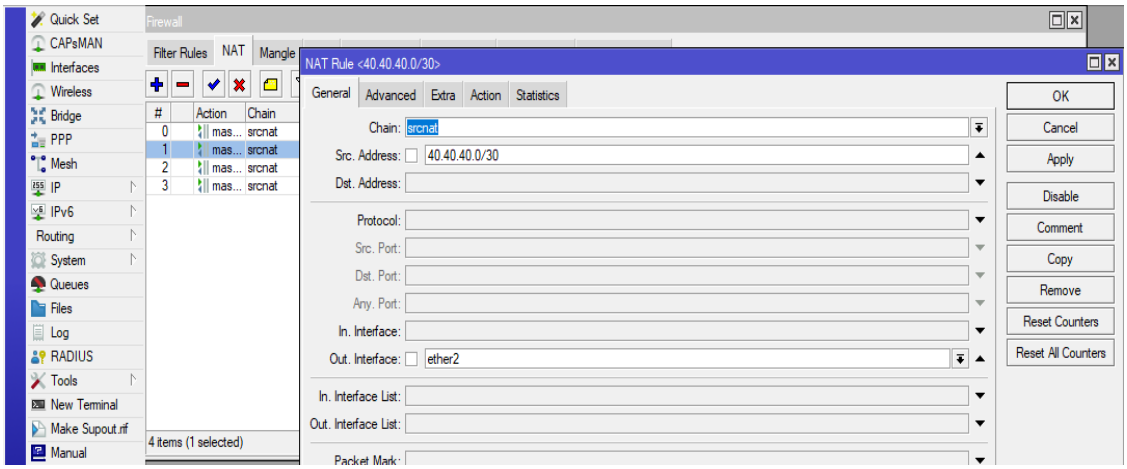


Figura 294.Configuracion de Firewall ethe 2 (a)
Fuente: Los autores

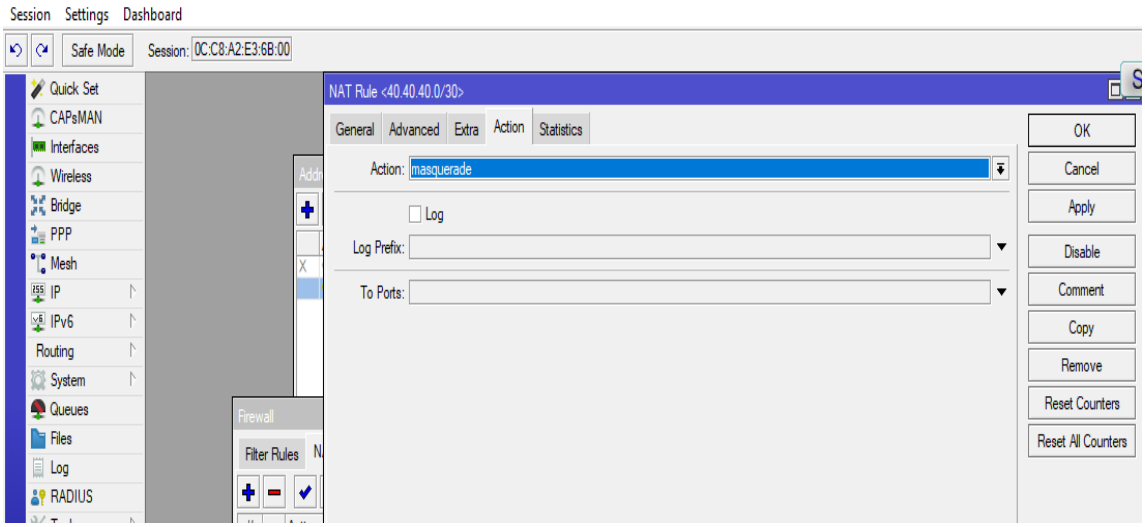


Figura 295.Configuracion de Firewall ethe 2 (b)
Fuente: Los autores

11. Configurar la NAT para la WAN-1 para los enlaces SD-WAN.

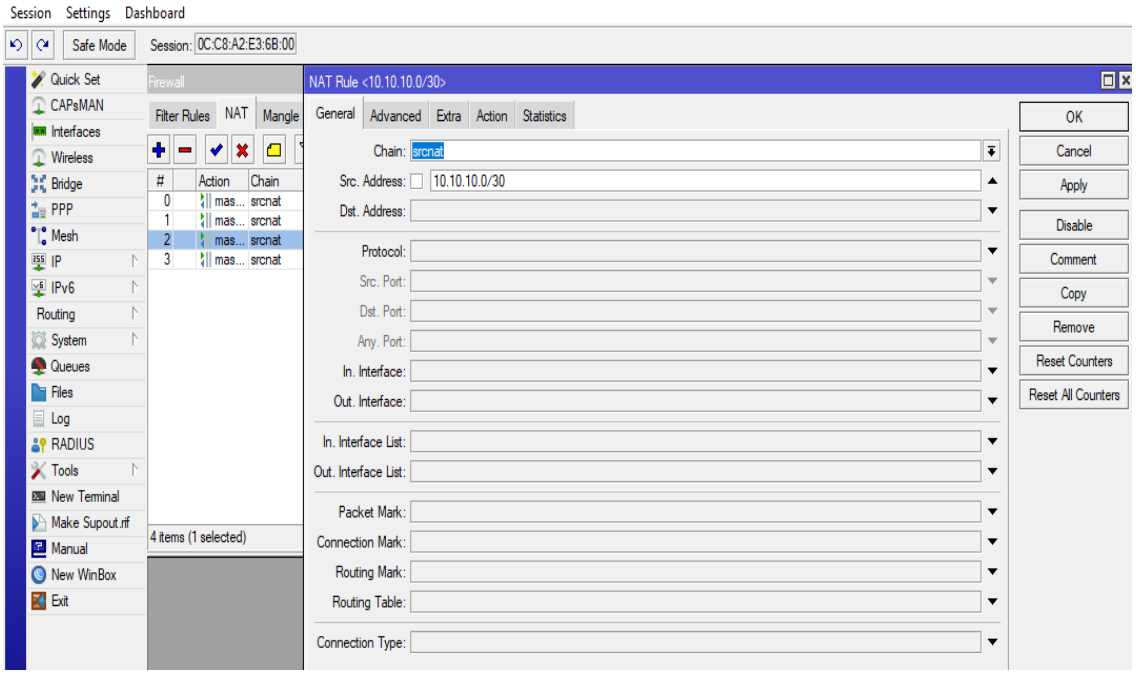


Figura 296. Configuracion NAT para WAN 1 (a)
Fuente: Los autores

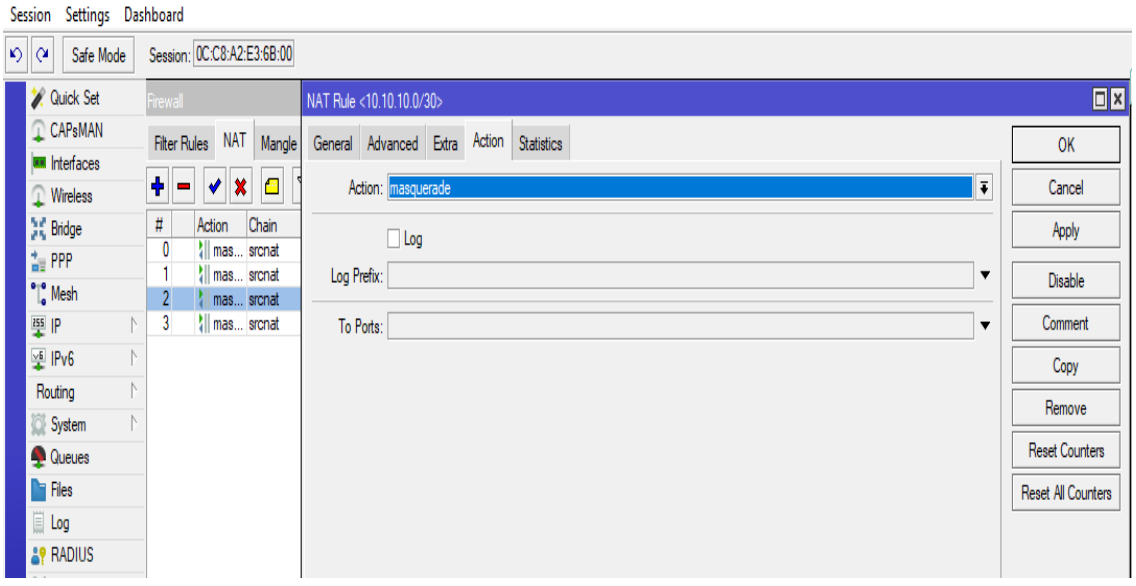


Figura 297. Configuracion NAT para WAN 1 (b)
Fuente: Los autores

12. Configurar la NAT para la WAN-2 para los enlaces SD-WAN.

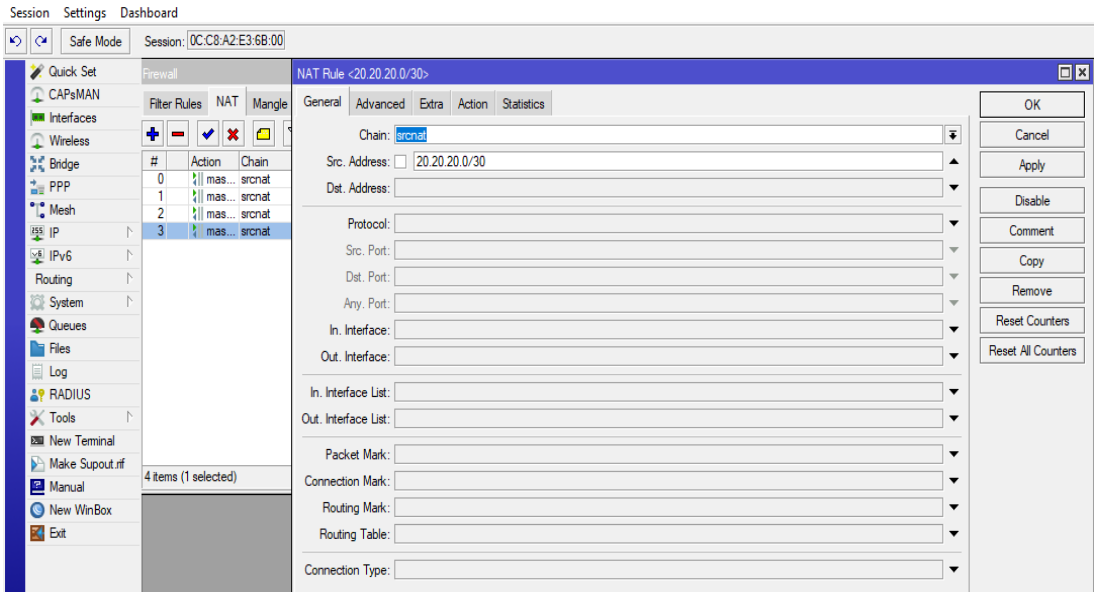


Figura 298.Configuracion NAT para WAN 2 (a)
Fuente: Los autores)

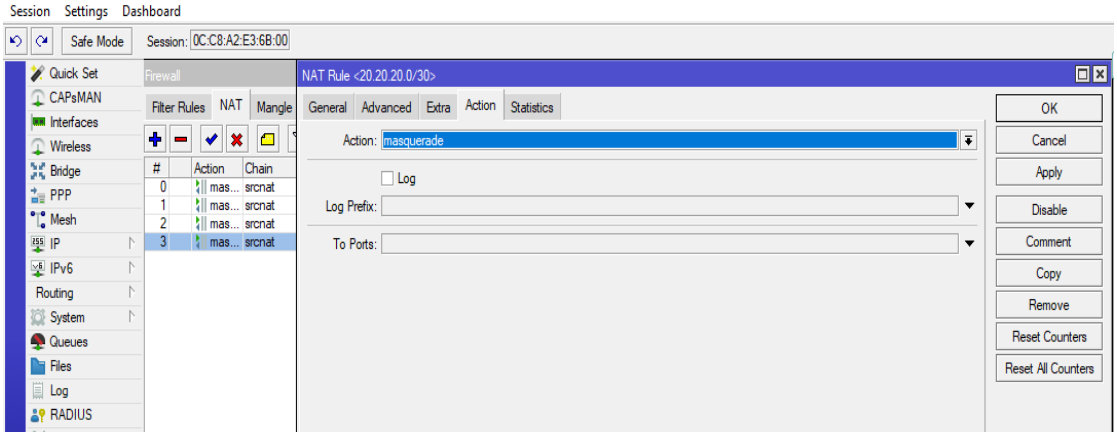


Figura 299.Configuracion NAT para WAN 2 (b)
Fuente: Los autores

13. Configurar la routes para la WAN ISP-1 donde se agregra la menor distancia a la WAN que tenga mejor banda ancha en casos reales.

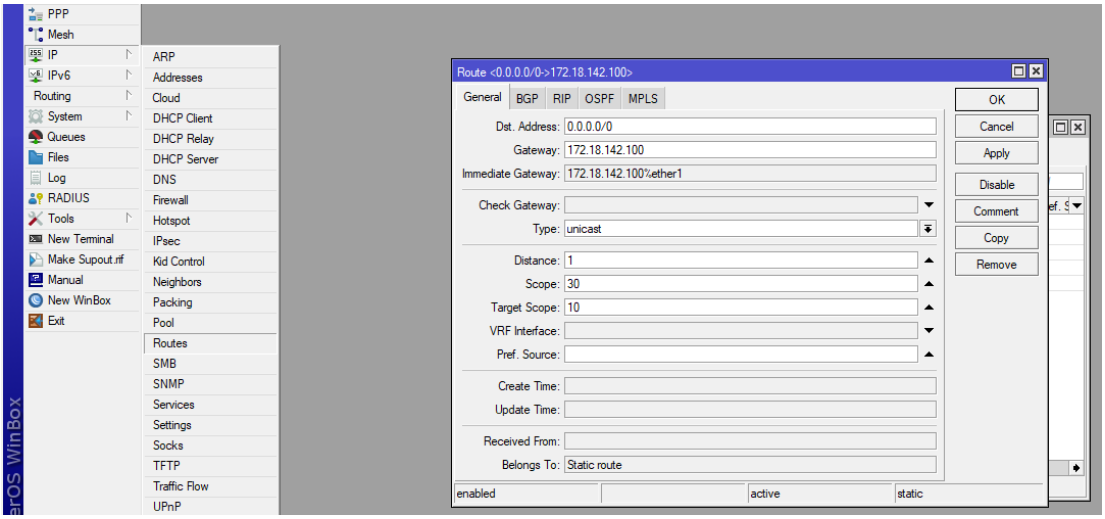


Figura 300.Configuracion WAN IPS 1 para distancia
Fuente: Los autores

14. Configurar la routes para la ISP-2.

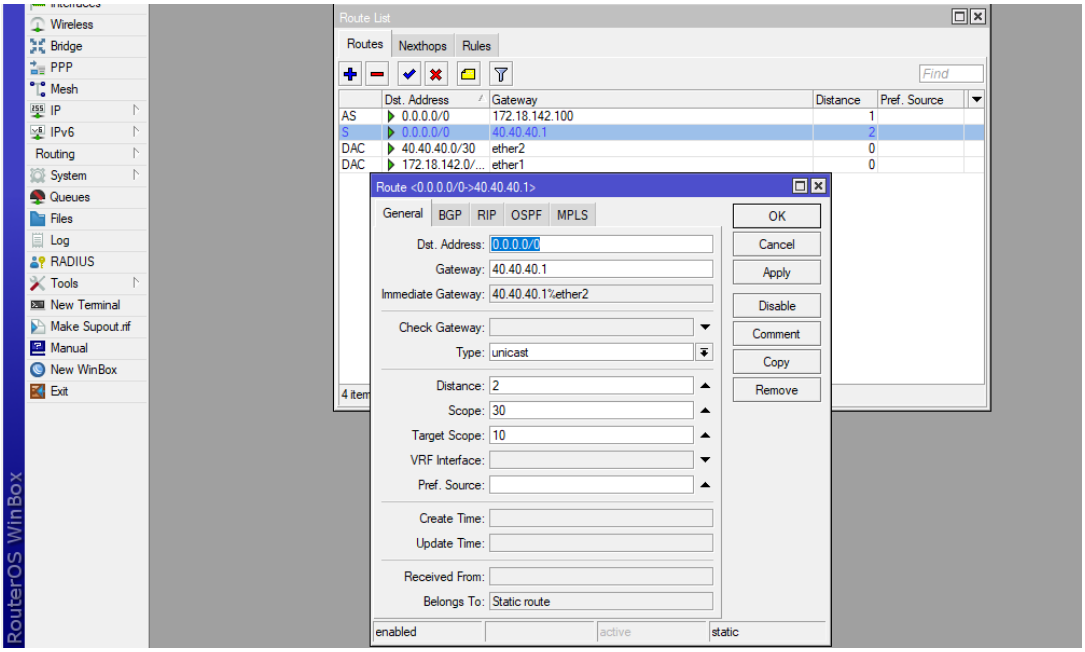


Figura 301.Configuracion WAN IPS 2 para distancia
Fuente: Los autores

15. Realizar la prueba de FailOver se desconectara la eth1 y automáticamente el ping se debe restablecer por la eth2 tal como se observa en la imagen.

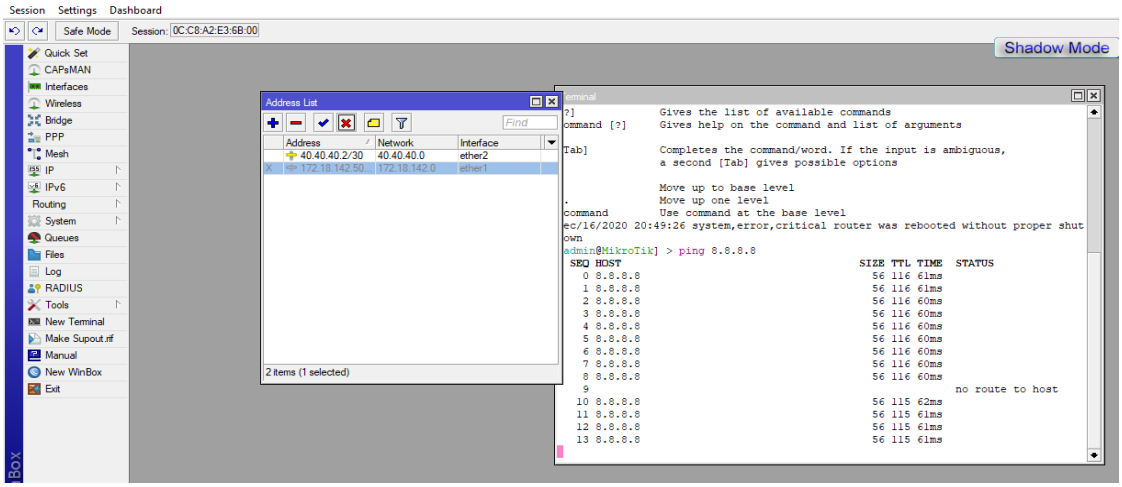


Figura 302. Test Failover

Fuente: Los autores

16. Configurar la ETH3 para la WAN-1 del fg-sucursal.

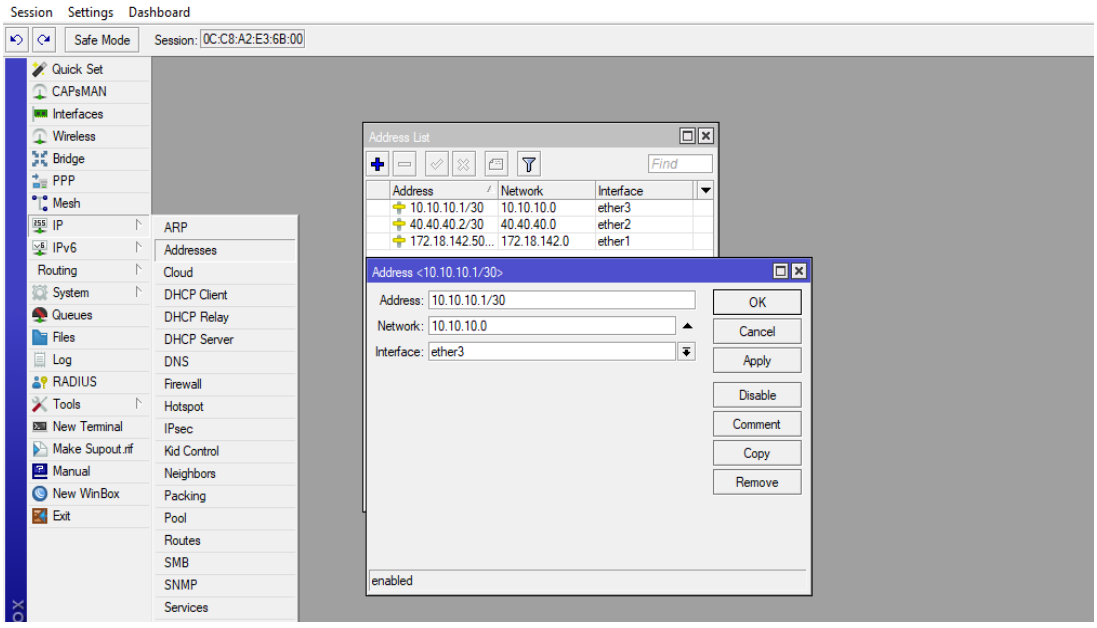


Figura 303.Configuracion eth3 para la WAN1 FG-SUCURSAL
Fuente: Los autores

17. Configurar la eth4 para la WAN-2 del fg-sucursal.

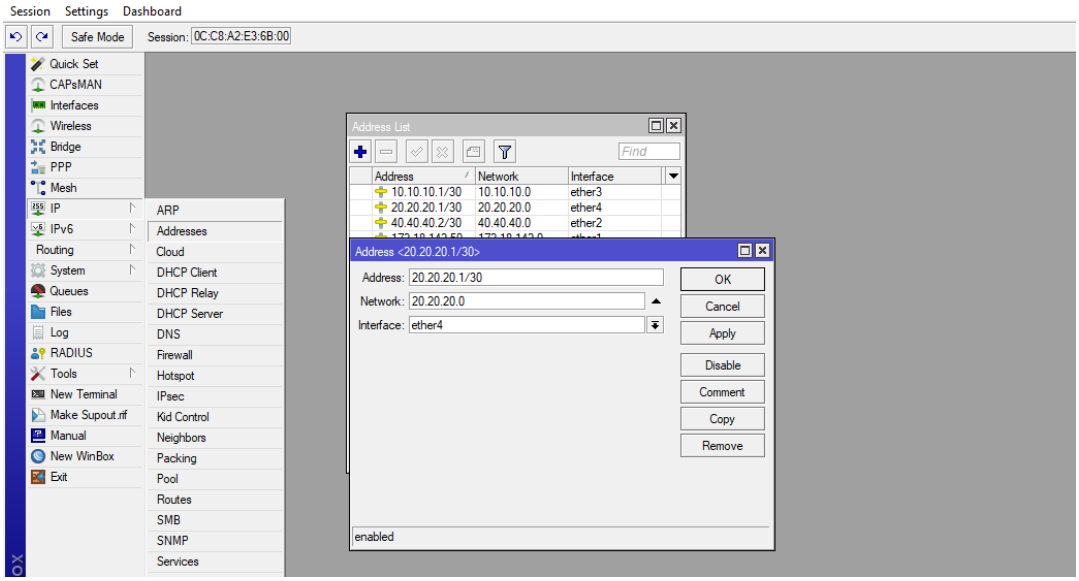


Figura 304.Configuracion eth4 para la WAN2 FG-SUCURSAL
Fuente: Los autores

18. Configurar el port2 en fg-sucursal para la WAN-1.

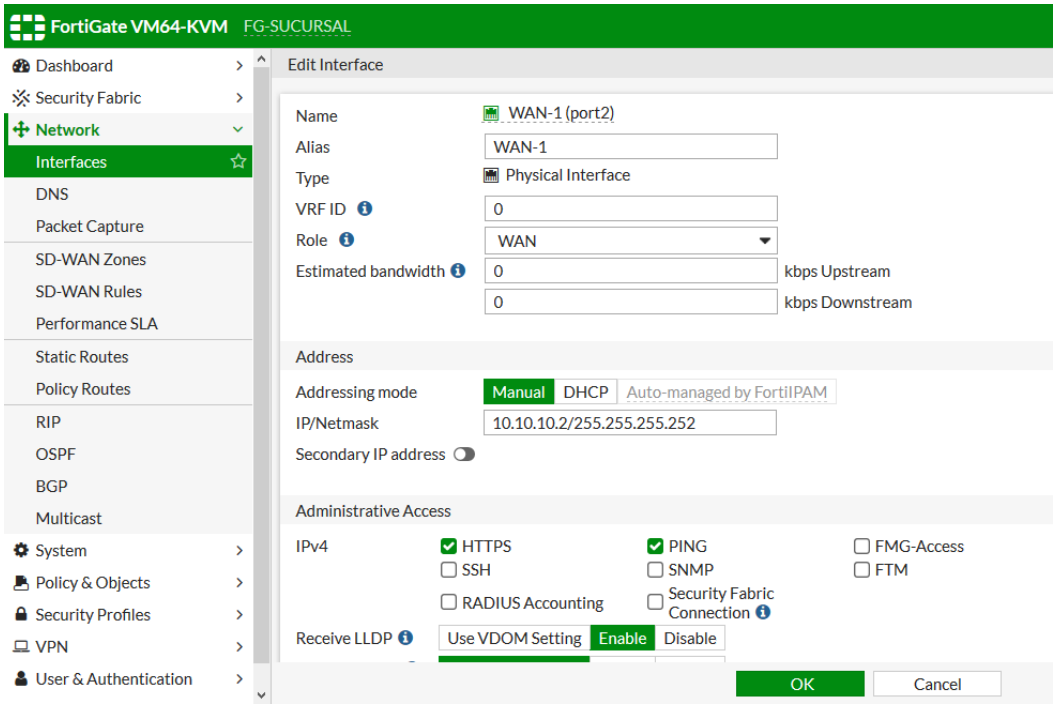


Figura 305. Configuracion port 2 FG-SUCURSAL para la WAN 1
Fuente: Los autores

19. Configurar el port3 para WAN-2 del fg-sucursal.

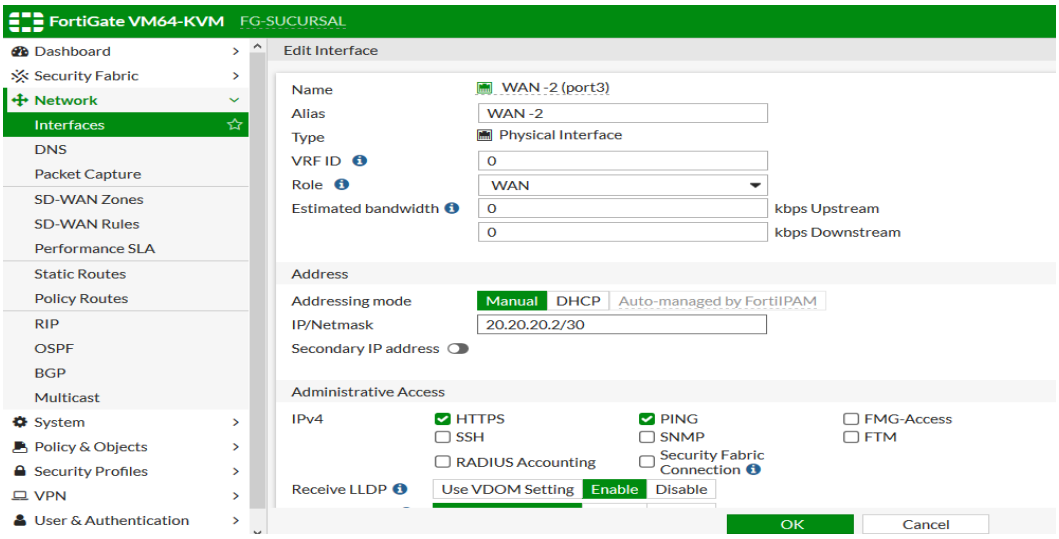


Figura 306.Configuracion port 3 FG-SUCURSAL para la WAN 2
Fuente: Los autores

20. Configurar el port4 para la red local del fg-sucursal.

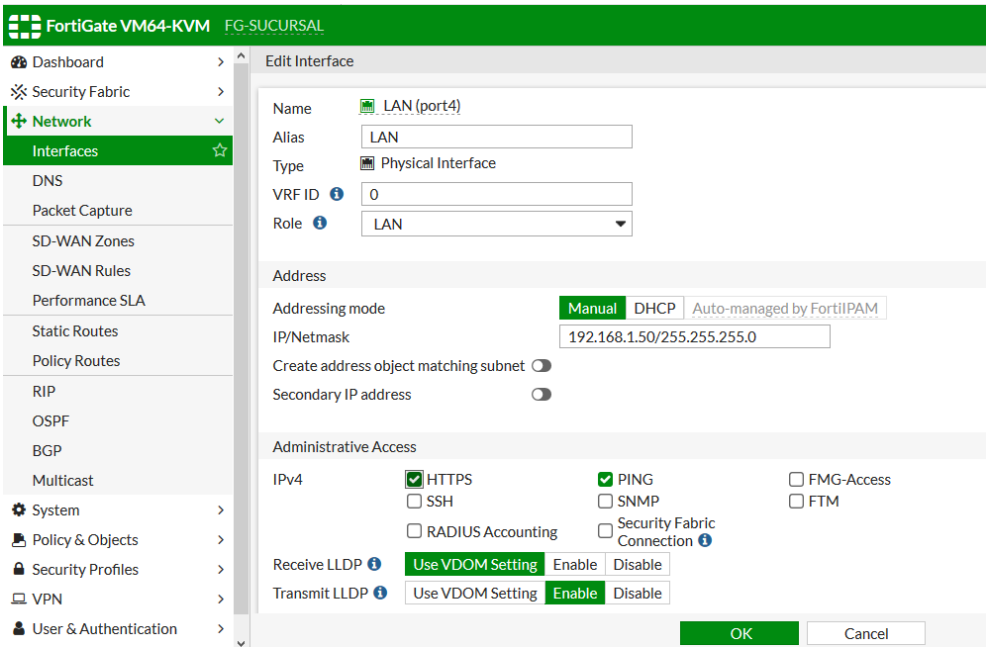


Figura 307.Configuracion port 4 red local FG-SUCURSAL
Fuente: Los autores

21. Configurar las interface WAN-1 para la SD-WAN.

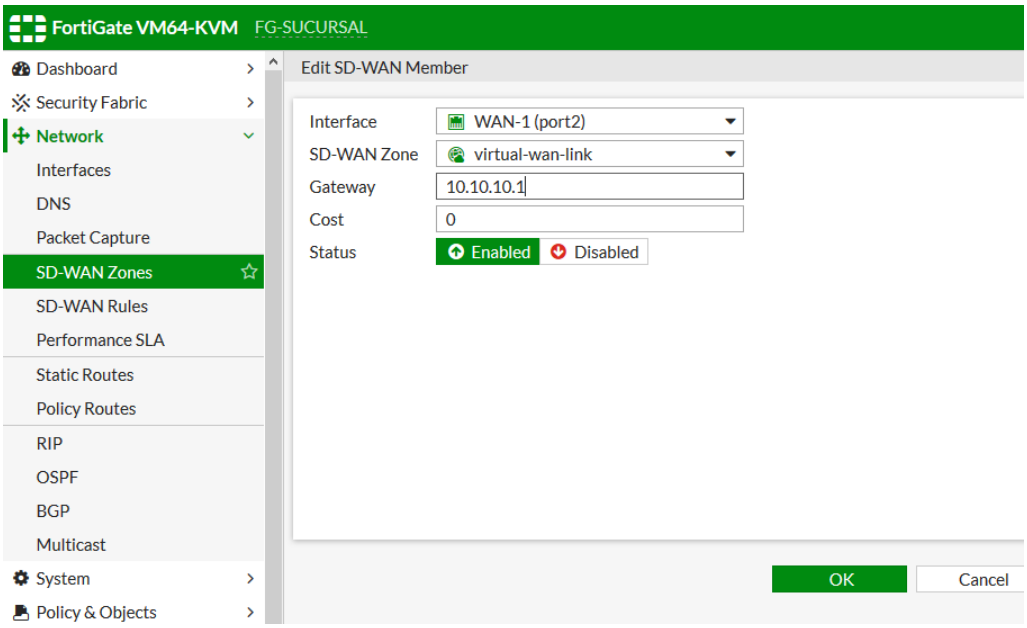


Figura 308.Configuracion interface WAN 1 FG-SUCURSAL

Fuente: Los autores

22. Configurar la interface WAN-2 para la SD-WAN.

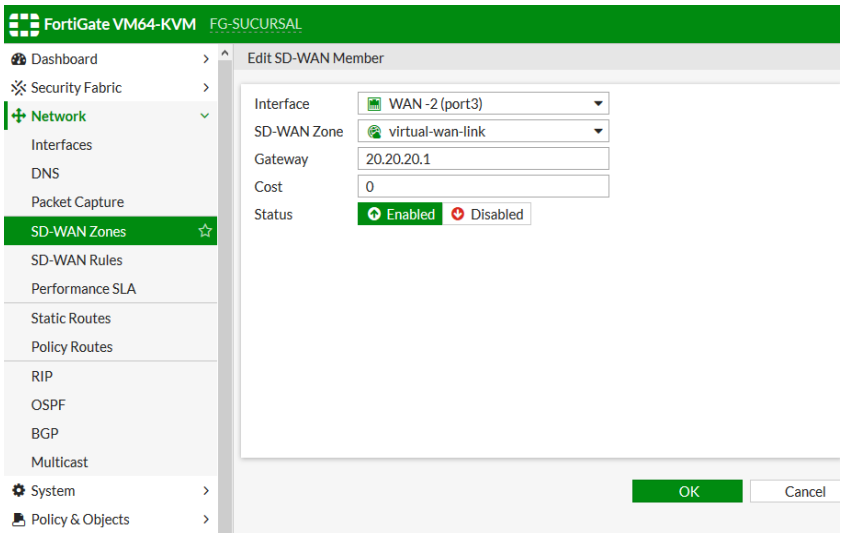


Figura 309.Configuracion interface WAN 2 FG-SUCURSAL
Fuente: Los autores

23. Configurar la static routes para el enlace SD-WAN.

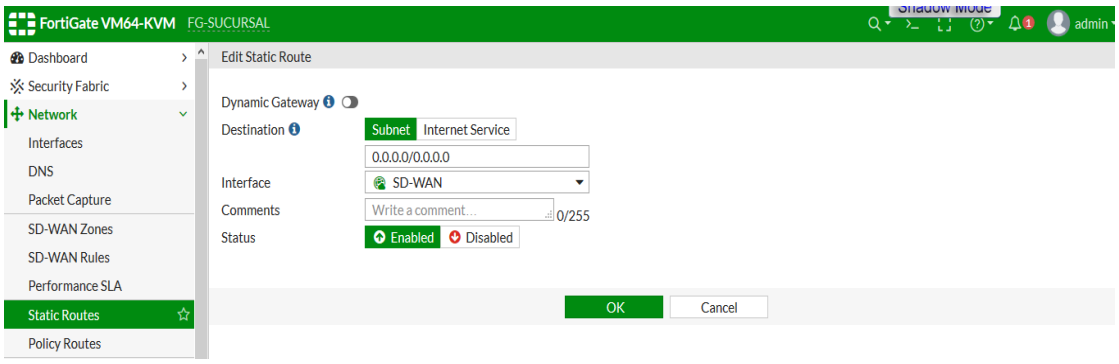


Figura 310.Configuracion static routes SD-WAN FG-SUCURSAL
Fuente: Los autores

24. Configurar los DNS en el fg-sucursal.

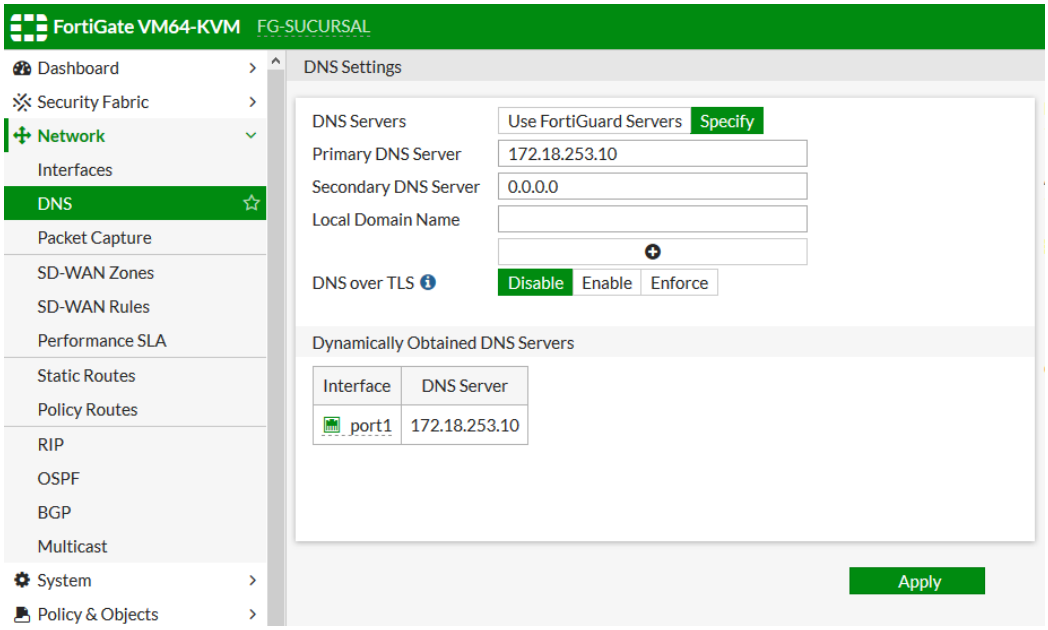


Figura 311.Configuracion DNS FG-SUCURSAL
Fuente: Los autores

25. Configurar la política para salidad de internet para la red local.

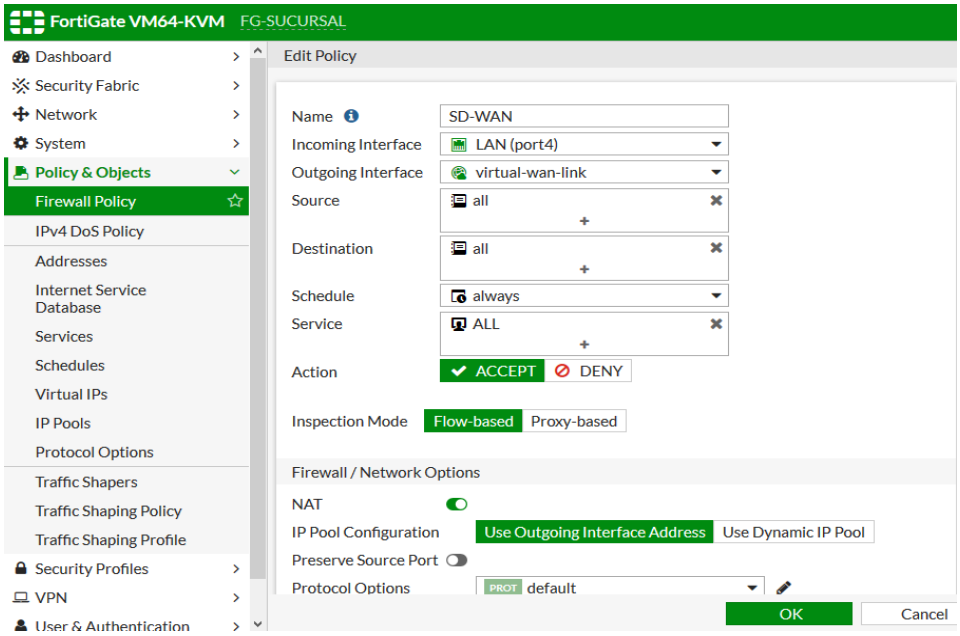


Figura 312.Configuracion firewall policy para la red local FG-SUCURSAL
Fuente: Los autores

26. Configurar la perfomance SLA para ver los jitter de las WAN´S.

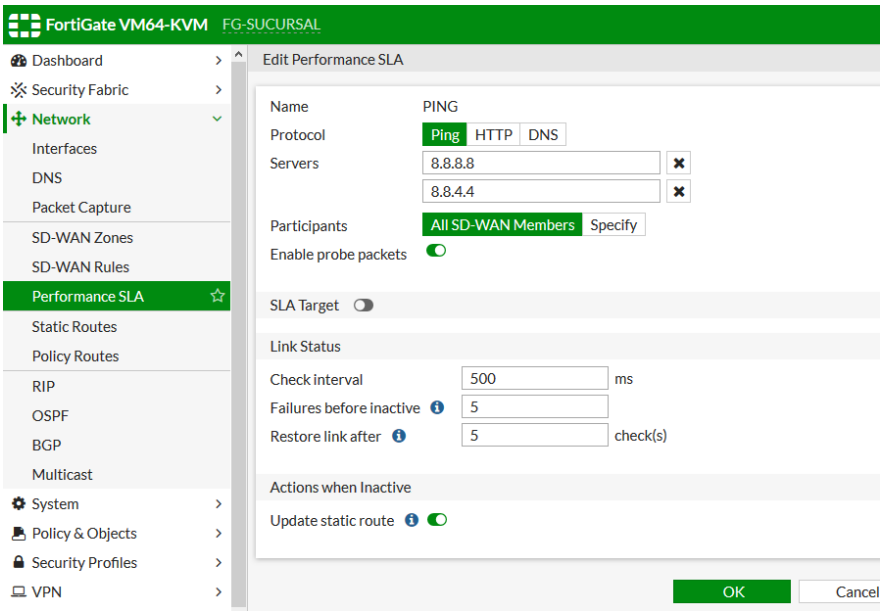


Figura 313.Configuracion perfomance SLA FG-SUCURSAL
Fuente: Los autores

27. Se desactivara todas las WAN´S ISP que van al fg-sucursal y obversamos en perfomance SLA caído .

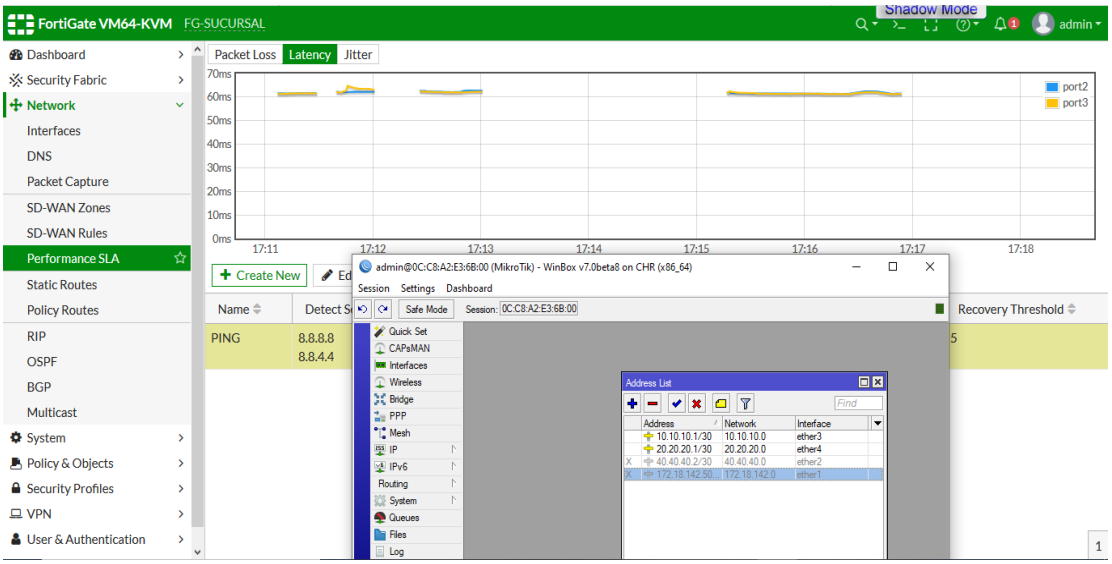


Figura 314.Observacion Perfomance SLA
Fuente: Los autores

28. Activar una interfaz de la WAN´S que van al fg-sucursal y veremos como se activan las 2 activan automáticamente las interfaces.

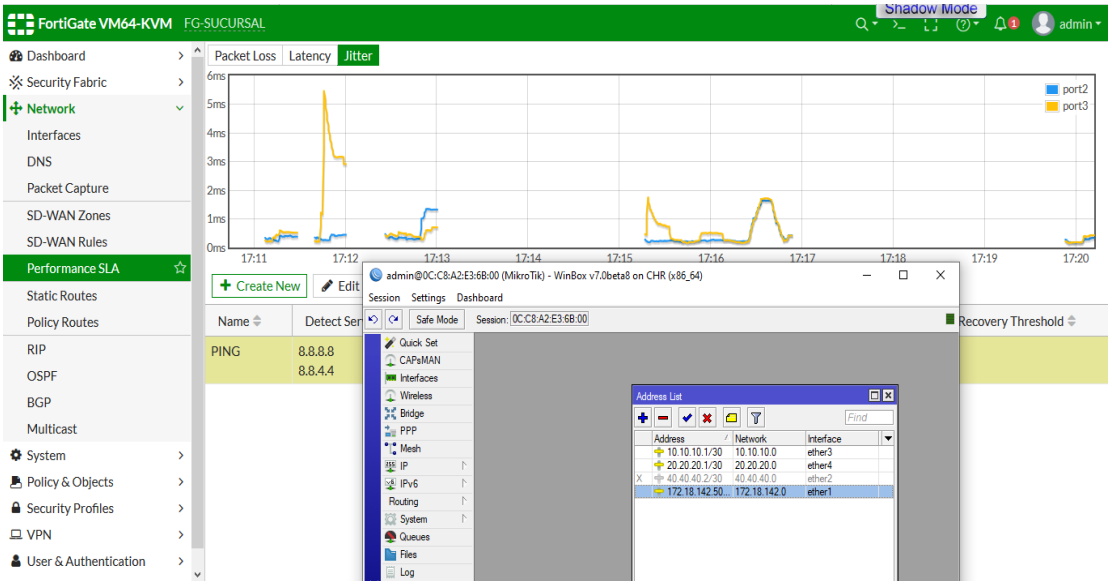


Figura 315.Activacion interfaz WAN´S
Fuente: Los autores

29. FailOver actuando en la red local del fg-sucursal.

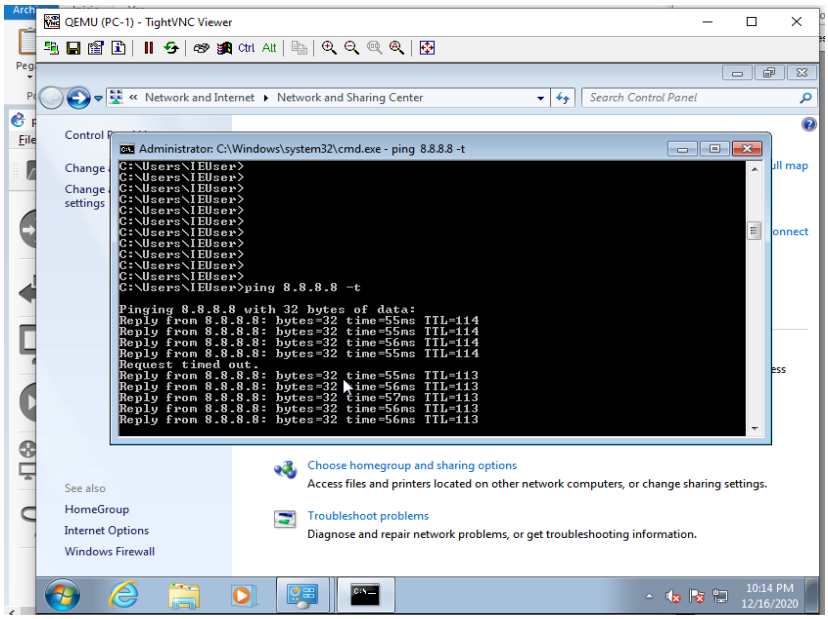


Figura 316.Ping failover conectando FG-SUCURSAL
Fuente: Los autores

30. FailOver actuando desconectando unos de los WAN que van al fg-sucursal.

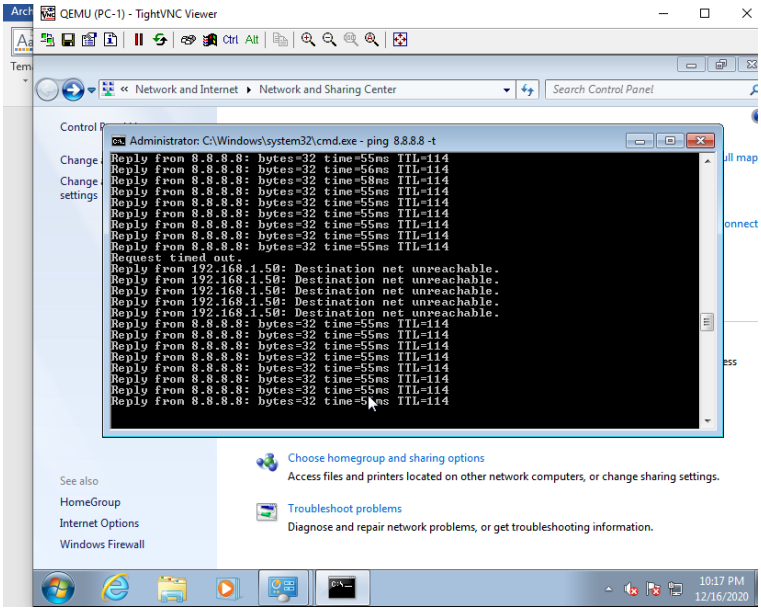


Figura 317.Ping failover desconectando FG-SUCURSAL
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente.

4.1.9. PRÁCTICA 9

Configuración de un mangle con mikrotik para el enlace sd-wan.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 9**
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO ESTIMADO:** 2 Horas.

DATOS DE LA PRÁCTICA

TEMA: Configuración de un mangle con mikrotik para el enlace SD-WAN.

OBJETIVOS

General

Configurar un mangle con mikrotik para el enlace sd-wan.

Específicos

- Configurar mangle para el enlace SD-WAN.
- Realizar una red SD-WAN
- Marcar paquetes del enlace SD-WAN.

GLOSARIO

MANGLE.- Es una especie de marcador que marca los paquetes para el procesamiento futuro con marcas especiales estas marcas se las puedes realizar en el NAT, QUEUE TREES y en el enrutamiento.

ROUTEROS.- Es el sistema operativo del hardware RouterBOARD tiene todas las características necesarias para un ISP.

MARCO PROCEDIMENTAL

1. Diseñar la topología de red para la práctica 9.

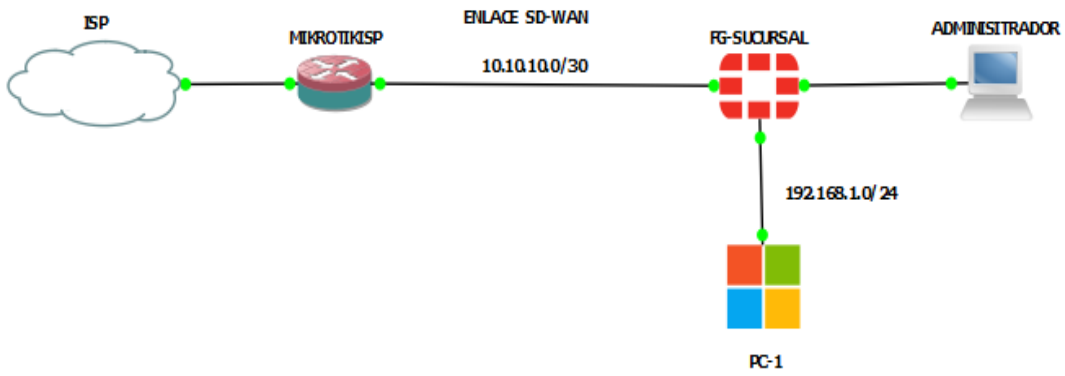


Figura 318. Diseño de la red práctica Nº9
Fuente: Los autores

2. Configurar la eth2 en el mikrotik para la WAN-1 del fg-sucursal.

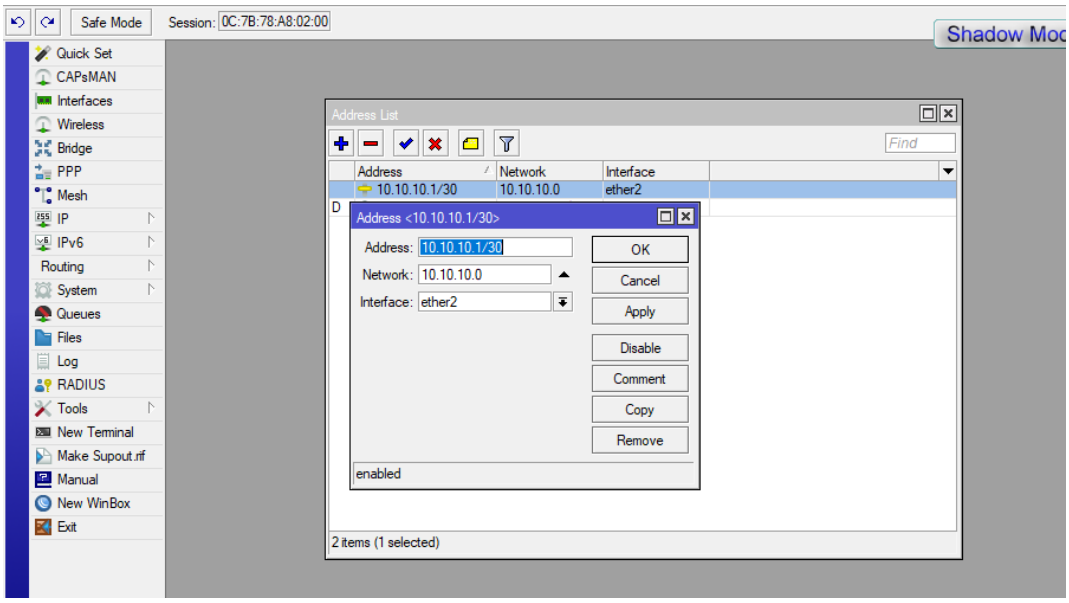


Figura 319. Diseño de la red práctica Nº9
Fuente: Los autores

3. Configurar DNS para el mikrotik-ISP.

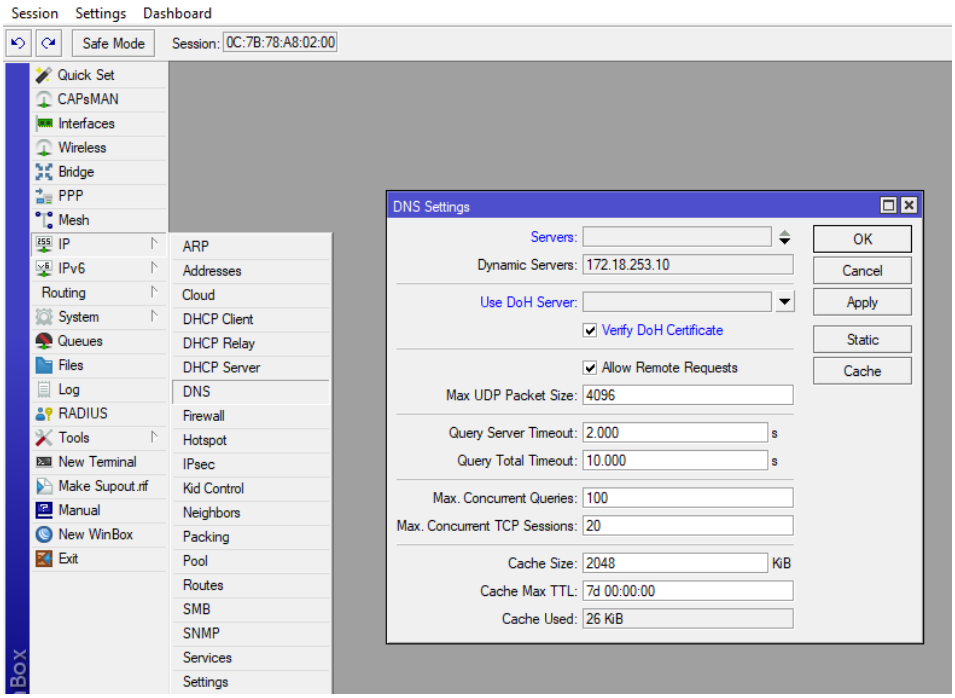


Figura 320. Configuracion DNS Mikrotik ISP
Fuente: Los autores

4. Configurar la NAT para la red de la WAN-1.

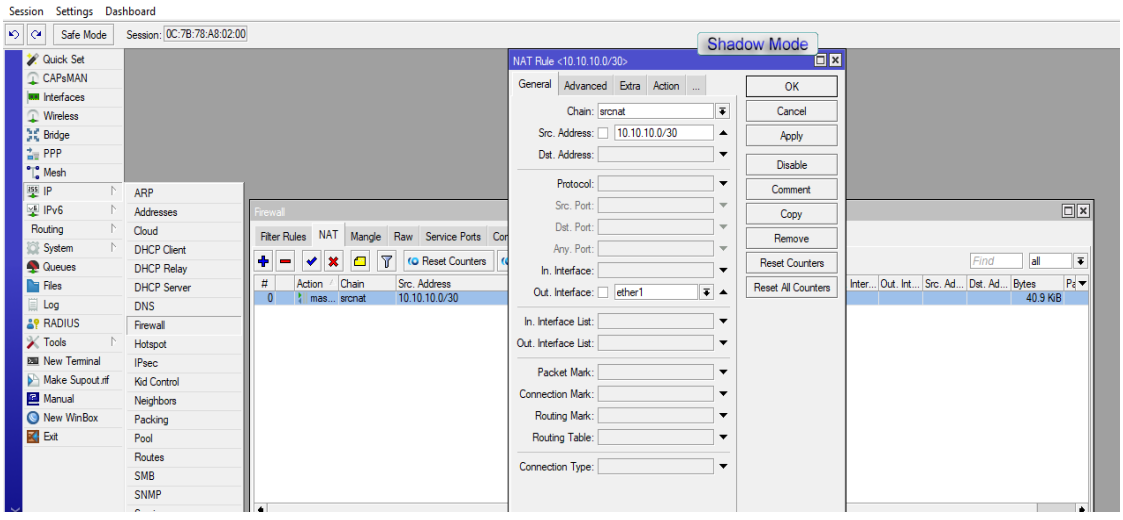


Figura 321. Configuracion NAT mikrotik ISP (a)
Fuente: Los autores

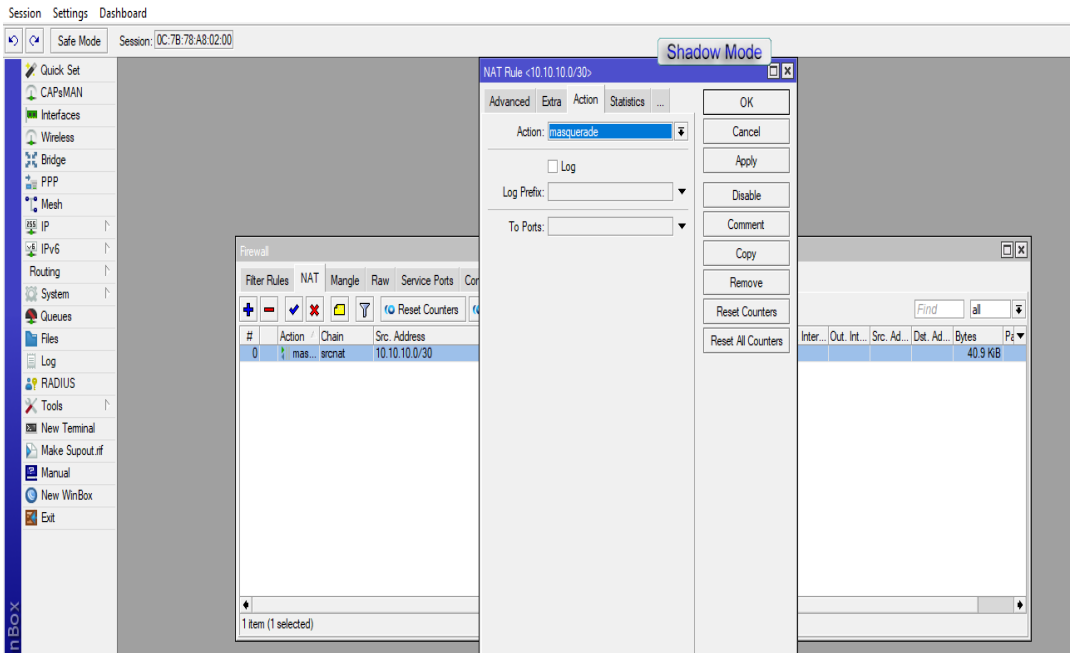


Figura 322. Configuracion NAT masquerade mikrotik ISP (b)

Fuente: Los autores

5. Configurar la IP para el port2 del fg-sucursal.

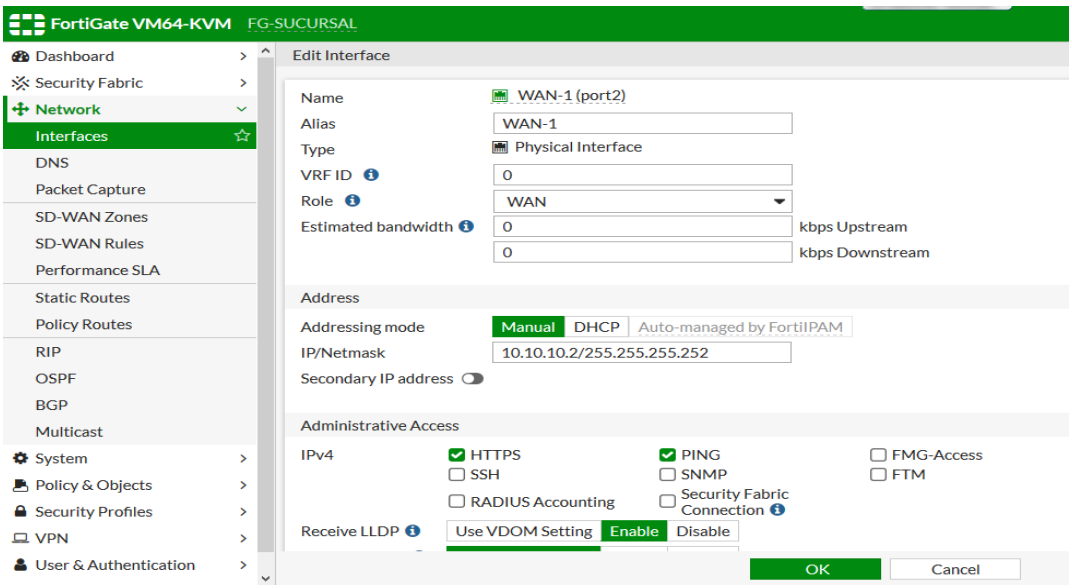


Figura 323. Configuracion IP port 2 FG-SUCURSAL
Fuente: Los autores

6. Configurar el port4 para la red local del fg-sucursal.

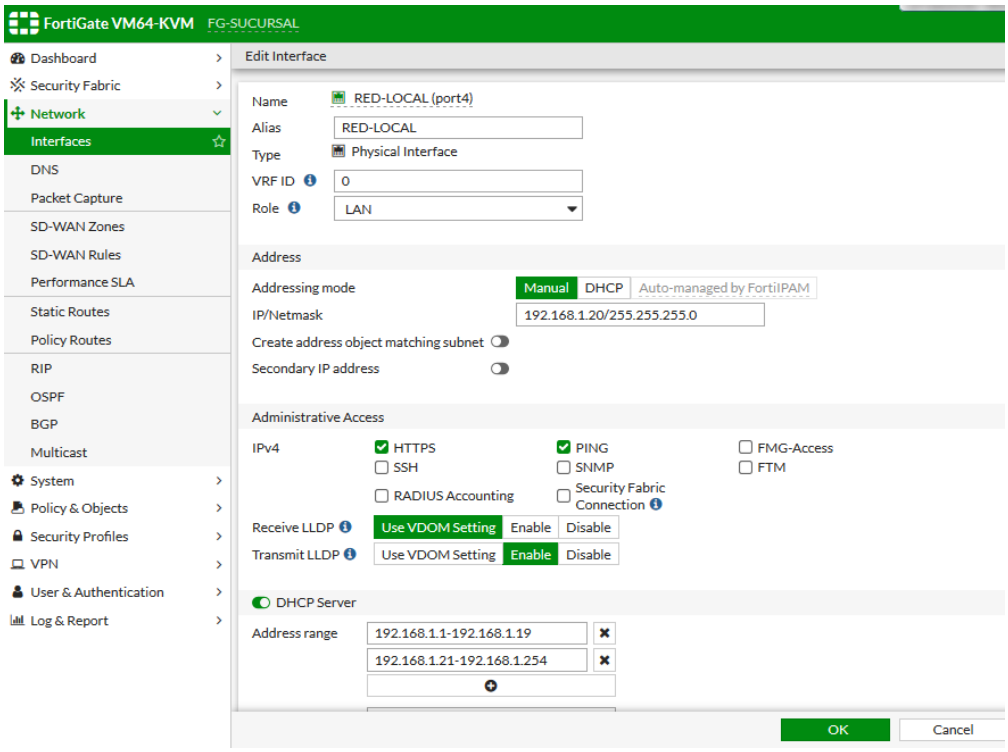


Figura 324. Configuracion red local port 4 FG-SUCURSAL
Fuente: Los autores

7. Configurar DNS al fg-sucursal.

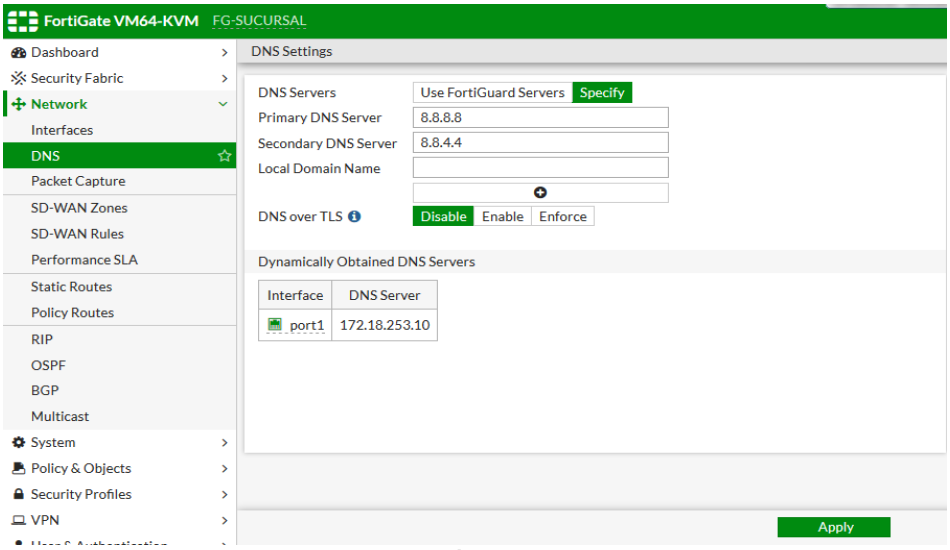


Figura 325. Configuración DNS FG-SUCURSAL
Fuente: Los autores

8. Configurar la interfaz que va a pertenecer a la SD-WAN.

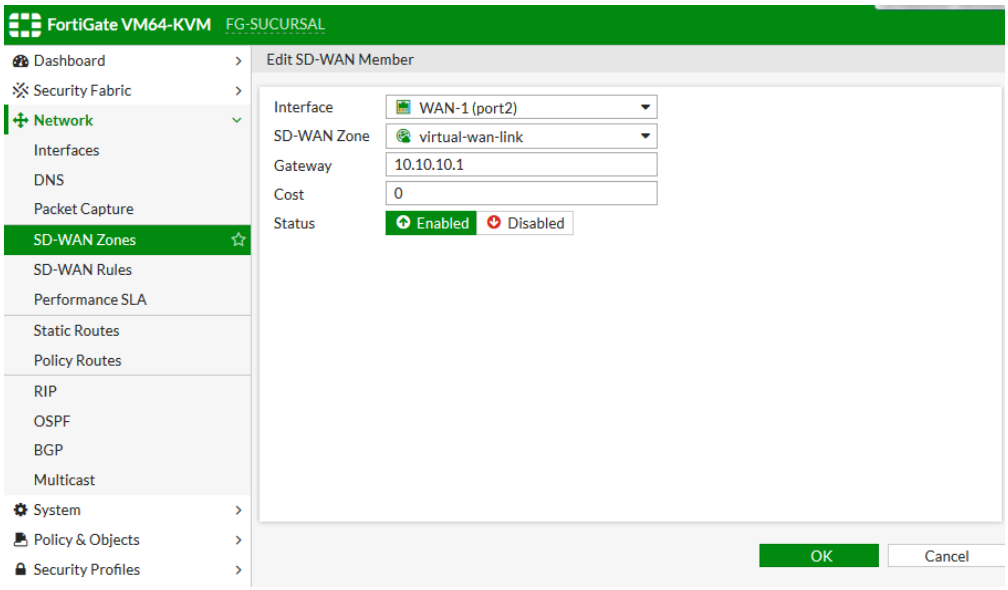


Figura 326. Configuración SD-WAN Zones FG-SUCURSAL
Fuente: Los autores

9. Configurar la static routes para la SD-WAN.

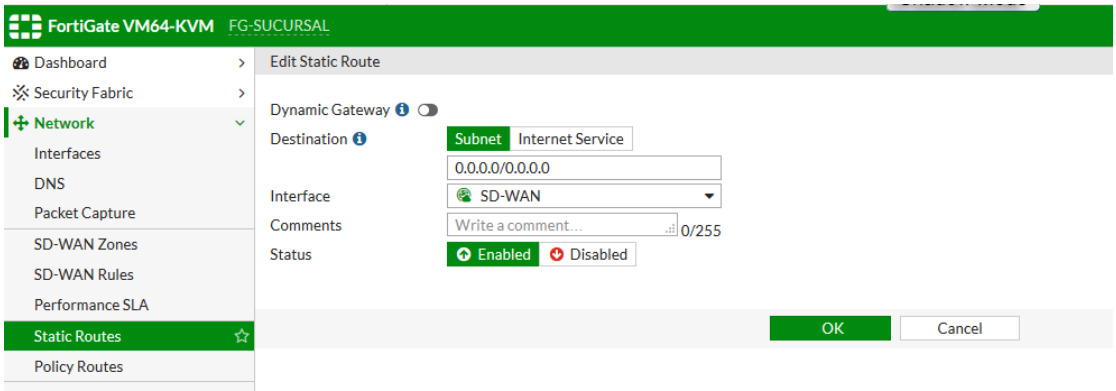


Figura 327. Configuración Static routes FG-SUCURSAL

Fuente: Los autores

10. Configurar la regla para la salida a internet a la red loca del fg-sucursal.

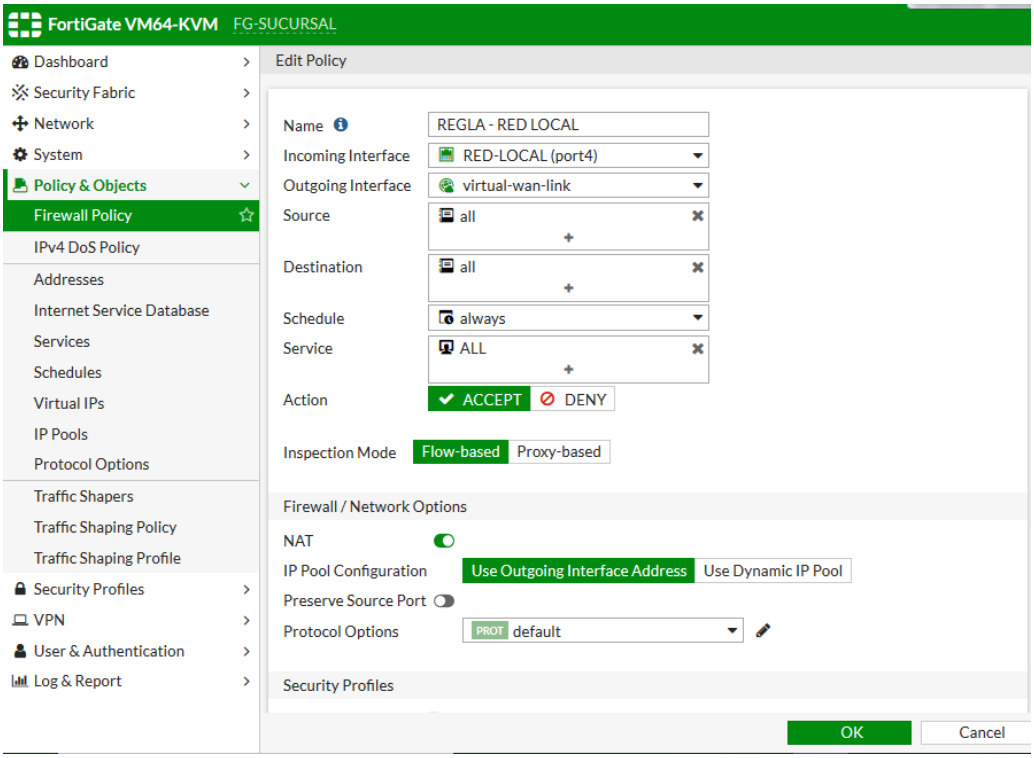


Figura 328. Configuración firewall policy FG-SUCURSAL
Fuente: Los autores

11. Configurar un marcado de conexiones para los puertos 80 y 443 .

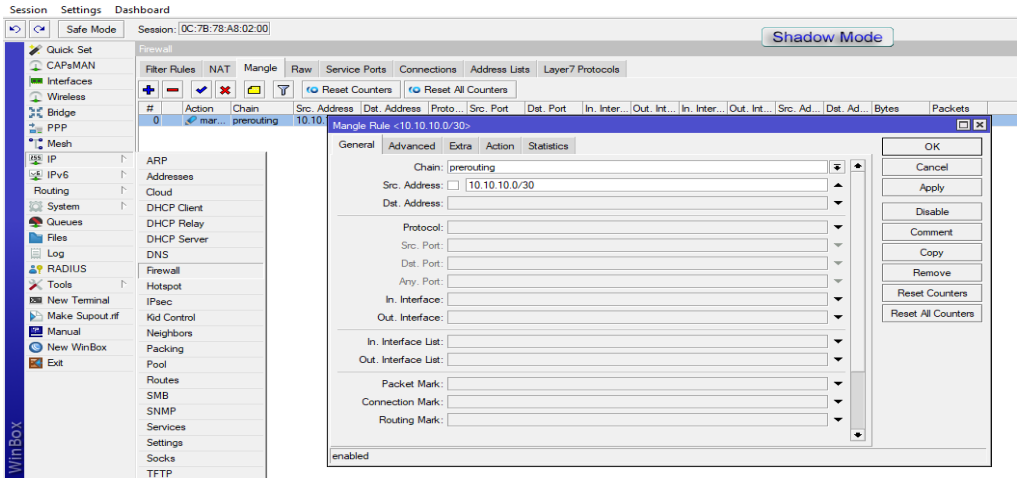


Figura 329. Configuración marcado de conexiones a la redpuerto 80 y 443 (a)
Fuente: Los autores

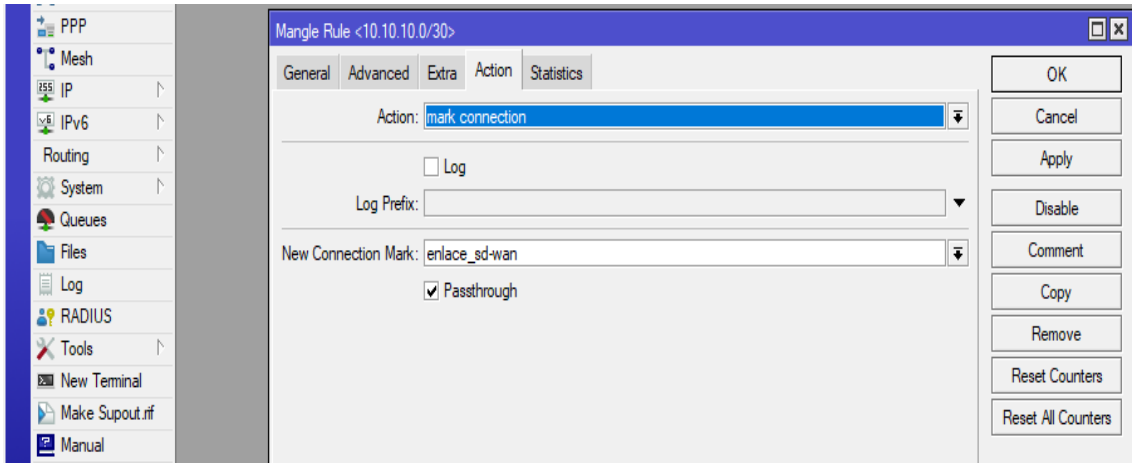


Figura 330. Configuración marcado de conexiones puerto 80 y 443 (b)

Fuente: Los autores

12. Configurar un marcado de paquetes para los puertos 80 y 443

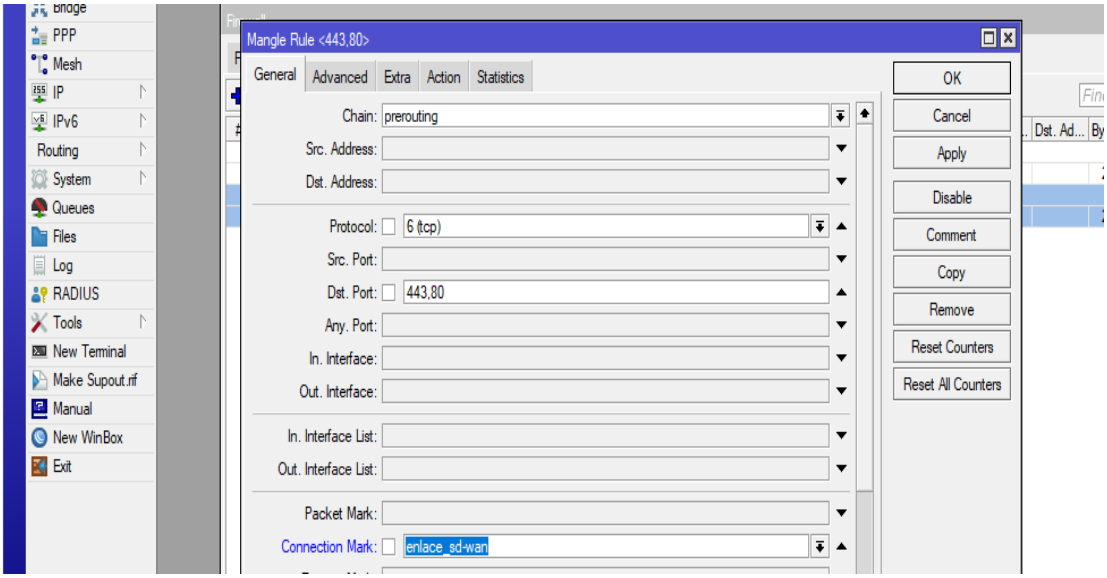


Figura 331. Configuración marcado de paquetes puerto 80 y 443 (a)
Fuente: Los autores

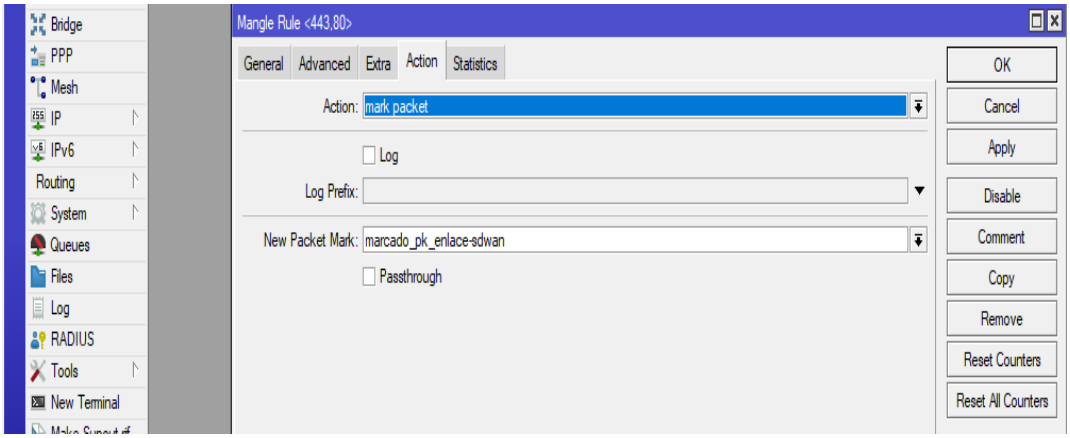


Figura 332. Configuracion marcado de paquetes puerto 80 y 443 (b)
Fuente: Los autores

13. Visulización de los marcados de nuestro enlace SD-WAN desde la red local fg-sucursal.

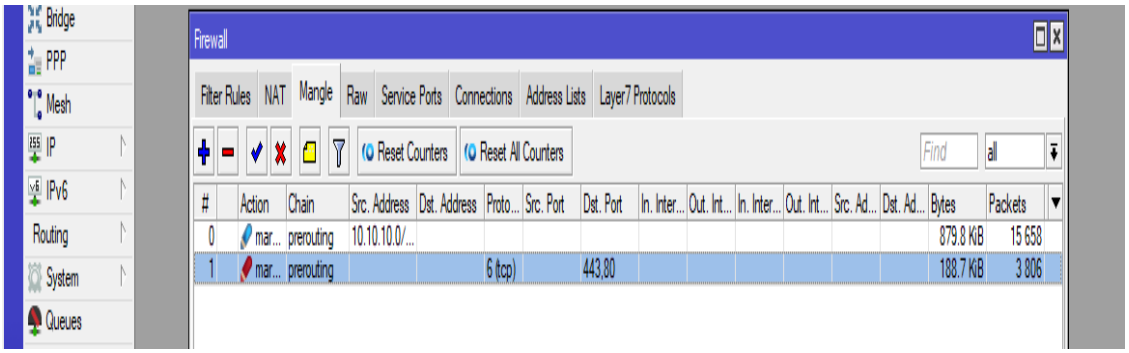


Figura 333. Visualizacion marcado de paquetes SD-WAN FG –SUCURSAL
Fuente: Los autores

14. Configurar marcado de paquetes a DNS.

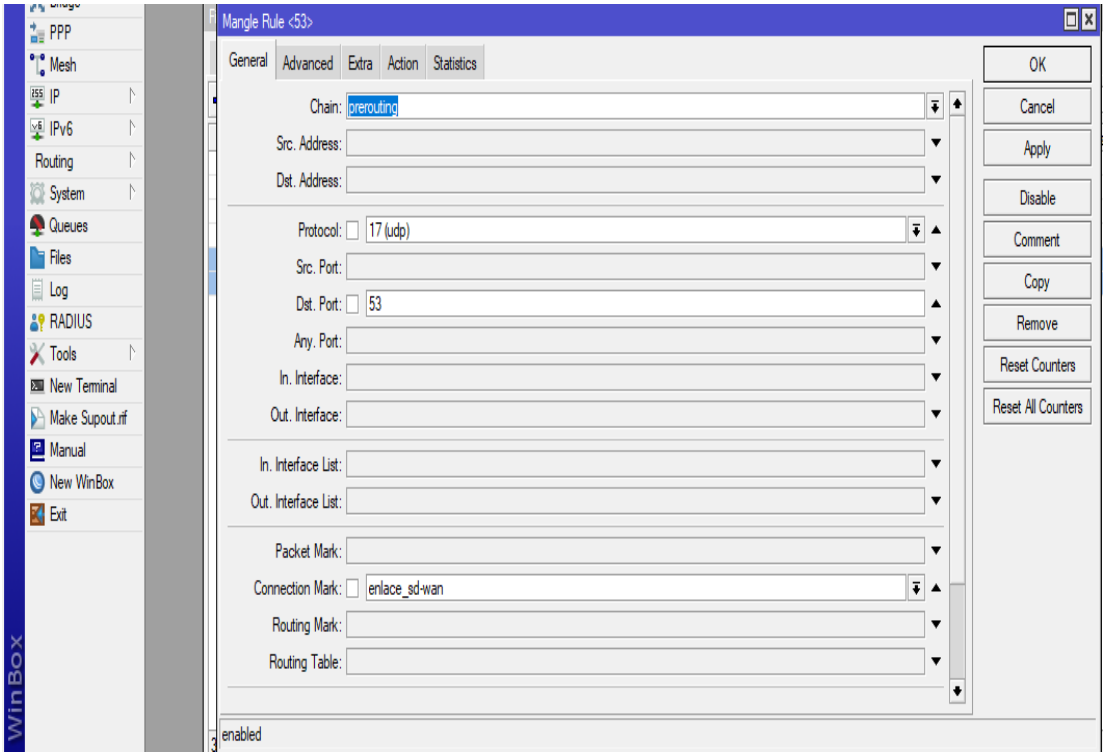


Figura 334. Configuracion marcado de paquetes DNS (a)
Fuente: Los Autores

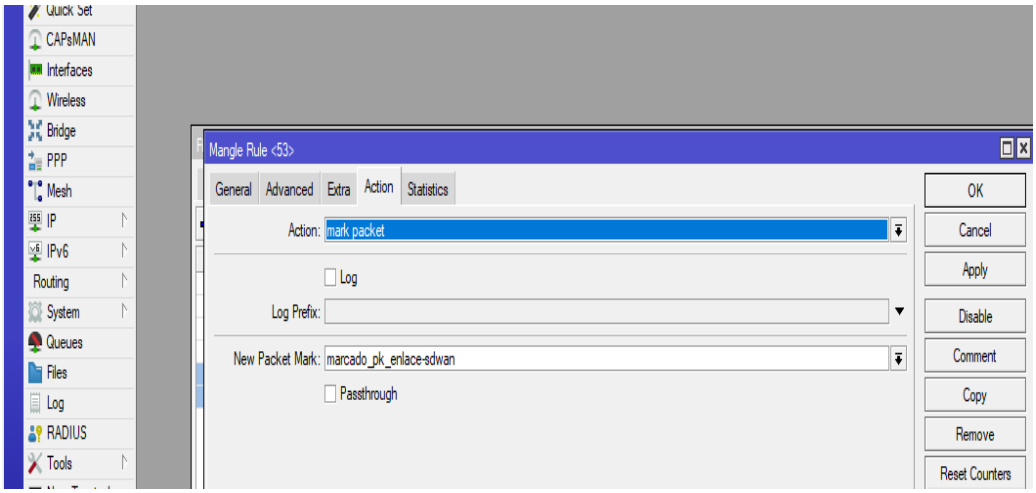


Figura 335. Configuracion marcado de paquetes DNS (b)
Fuente: Los Autores

15. Agregar un address-list para el marcado de paquetes para youtube.

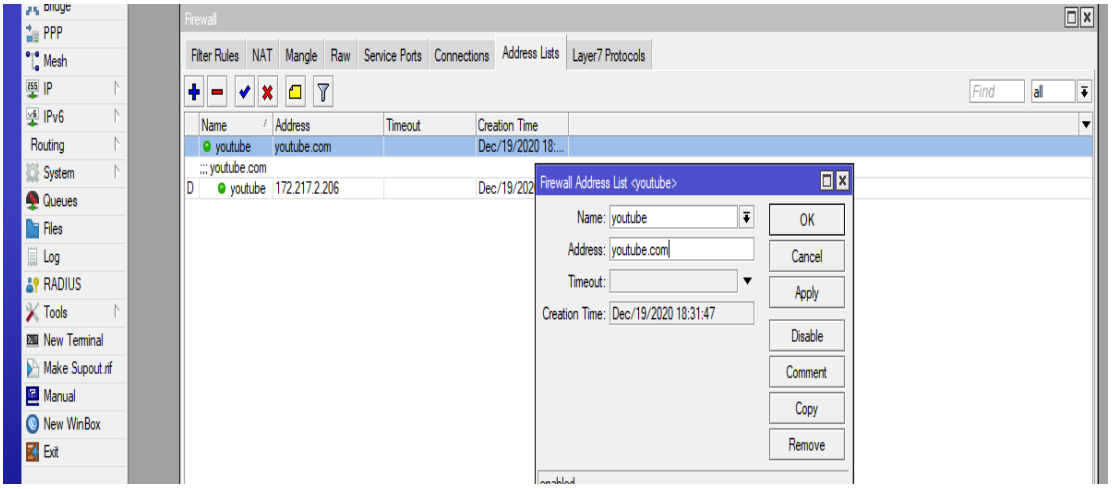


Figura 336. Agregando address-list para marcado
Fuente: Los Autores

16. Configurar el marcado de paquetes para youtube para el enlace sd-wan.

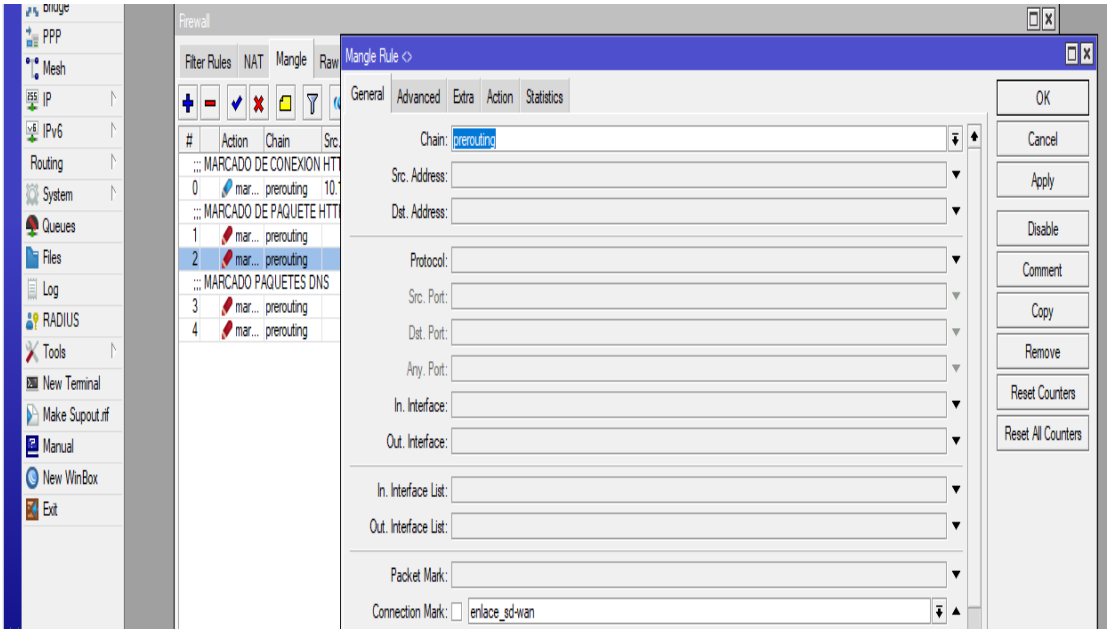


Figura 337. Configuracion marcado de paquetes SD-WAN (a)
Fuente: Los Autores

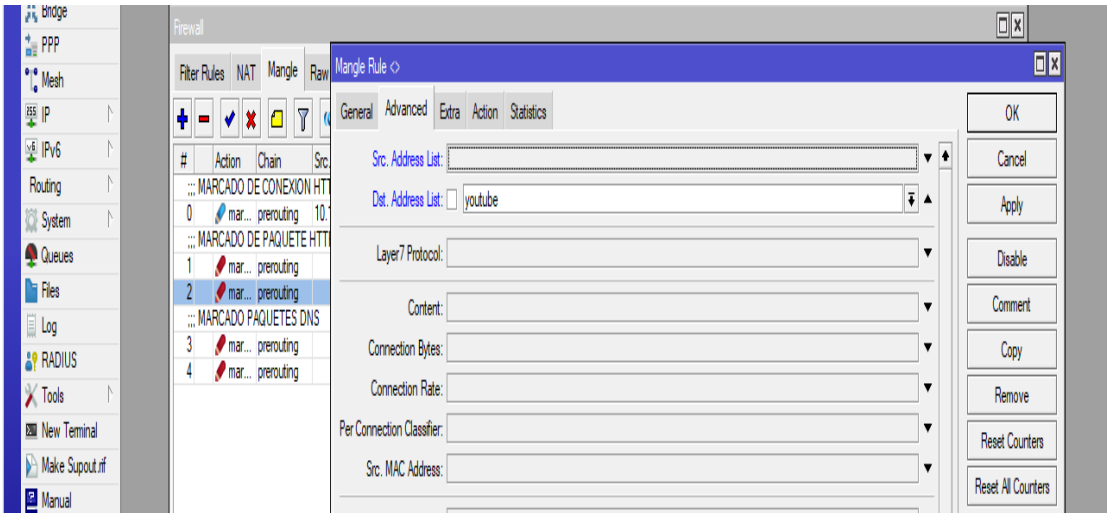


Figura 338. Configuracion marcado de paquetes SD-WAN (b)
Fuente: Los Autores

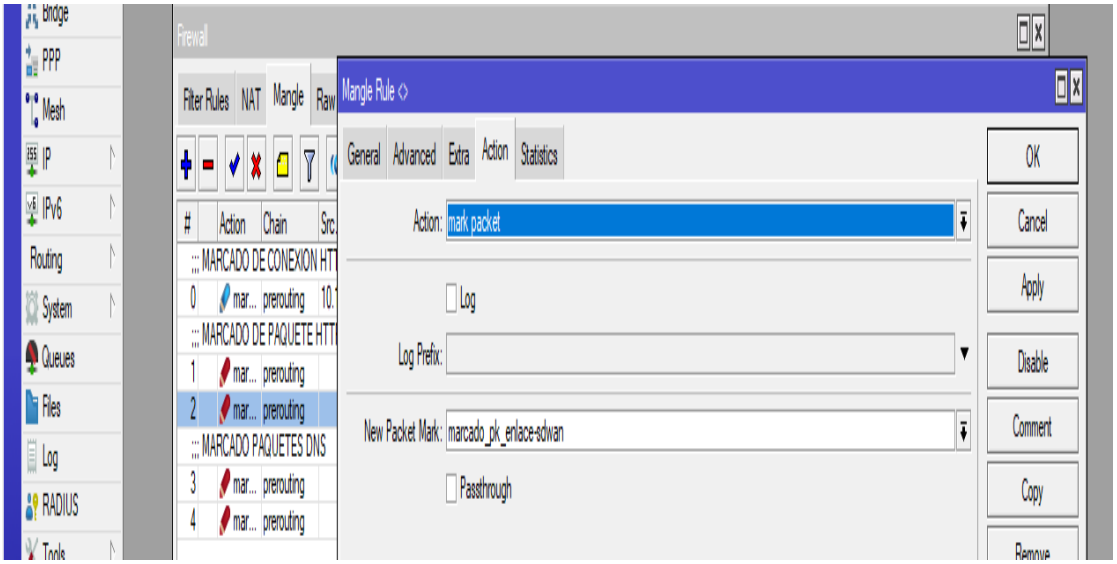


Figura 339. Configuracion marcado de paquetes SD-WAN (c)
Fuente: Los Autores

17. Visualizacion de los marcados de paquetes del enlace sd-wan.

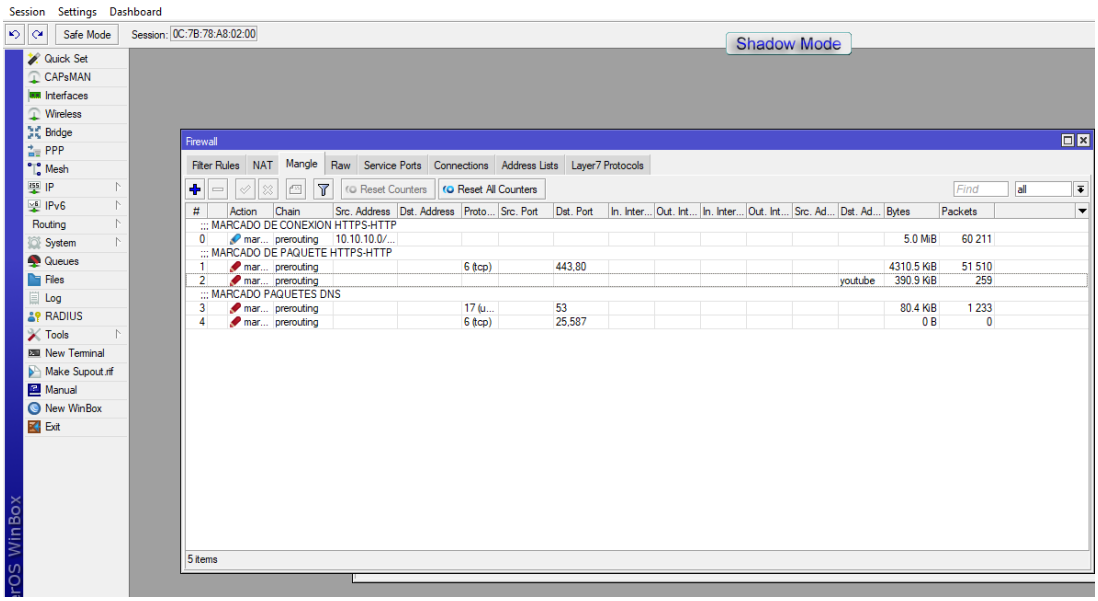


Figura 340. Visualizacion marcado de paquetes SD-WAN
Fuente: Los Autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.10. PRÁCTICA 10

Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik.

DATOS INFORMATIVOS

- **MATERIA:** Redes de comunicación
- **PRÁCTICA Nº 10**
- **NUMERO DE COMPUTADORAS:** 10
- **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik.

OBJETIVOS

General

Configurar layer 7 con mikrotik para el enlace SD-WAN

Específicos

- Configurar layer 7 en mikrotik
- Realizar un marcado de paquetes y conexiones.
- Elaborar un simple queues a los servicios y marcados de conexión.

GLOSARIO

MANGLE.- Es una especie de marcador que marca los paquetes para el procesamiento futuro con marcas especiales estas marcas se las puedes realizar en el NAT, QUEUE TREES y en el enrutamiento.

ROUTEROS.- Es el sistema operativo del hardware RouterBOARD tiene todas las características necesarias para un ISP.

LAYER 7.- Es un método de búsqueda de patrones en flujos ICMP / TCP / UDP.

QUEUE.- Las colas se utilizan para limitar y priorizar el tráfico.

MARCO PRODECIMENTAL

1. Diseñar la topología de red para la práctica 10.

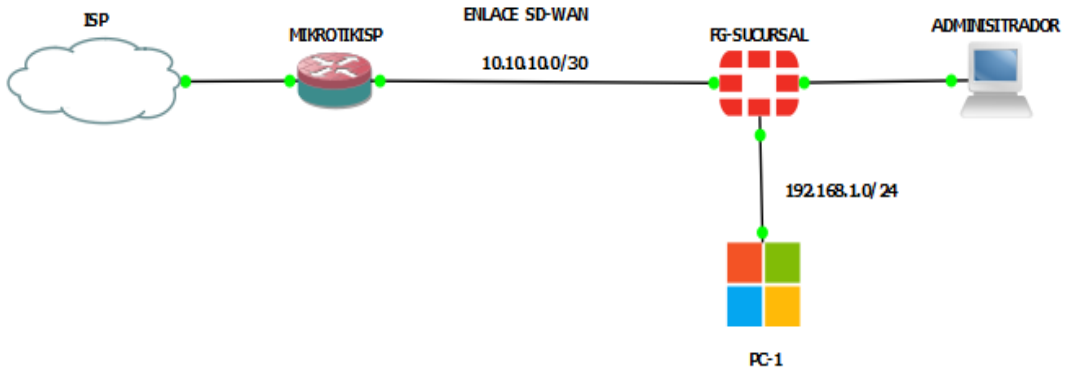


Figura 341. Diseño de la red práctica Nº 10
Fuente: Los autores

2. Configurar la eth2 en el mikrotik para la WAN-1 del fg-sucursal.

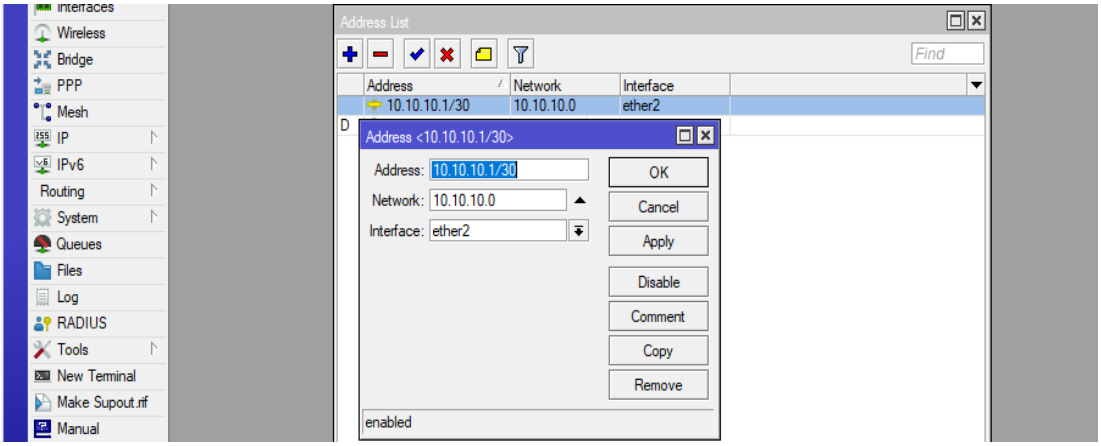


Figura 342. Configuración eth2 mikrotik
Fuente: Los autores

3. Configurar DNS para el mikrotik-ISP.

.

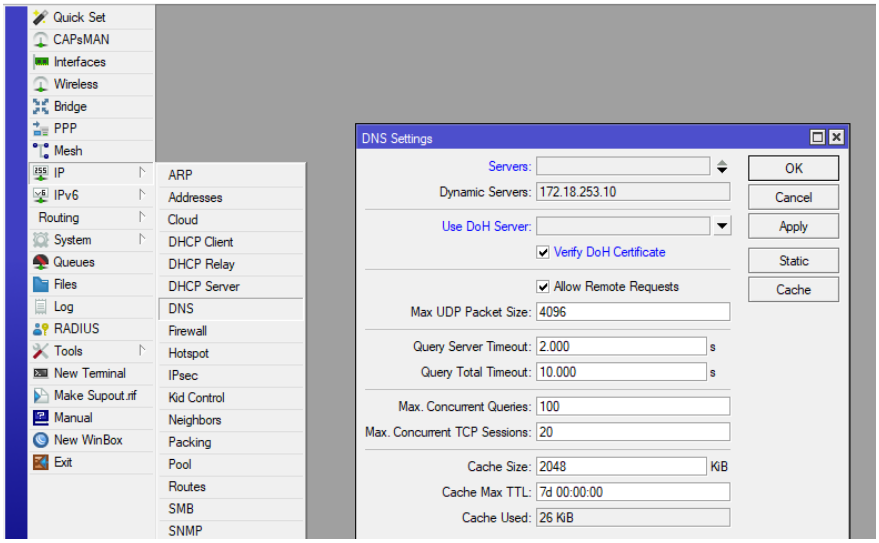


Figura 343. Configuracion DNS mikrotik
Fuente: Los autores

4. Configurar la NAT para la red de la WAN-1.

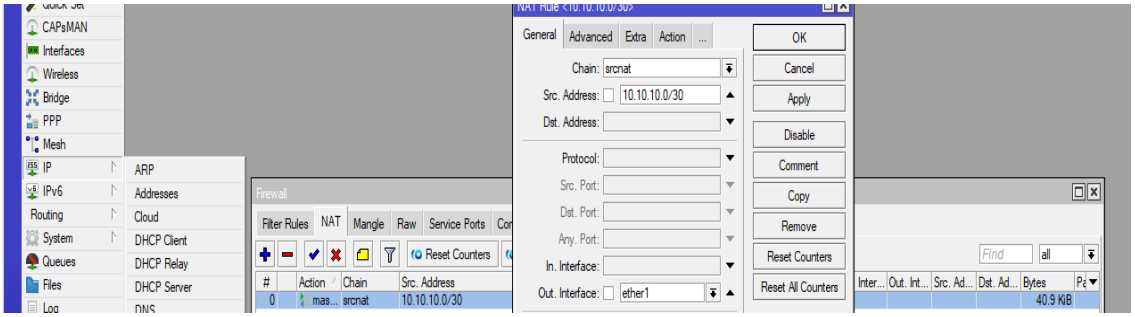


Figura 344. Configuración del NAT mikrotik (a)
Fuente: Los autores

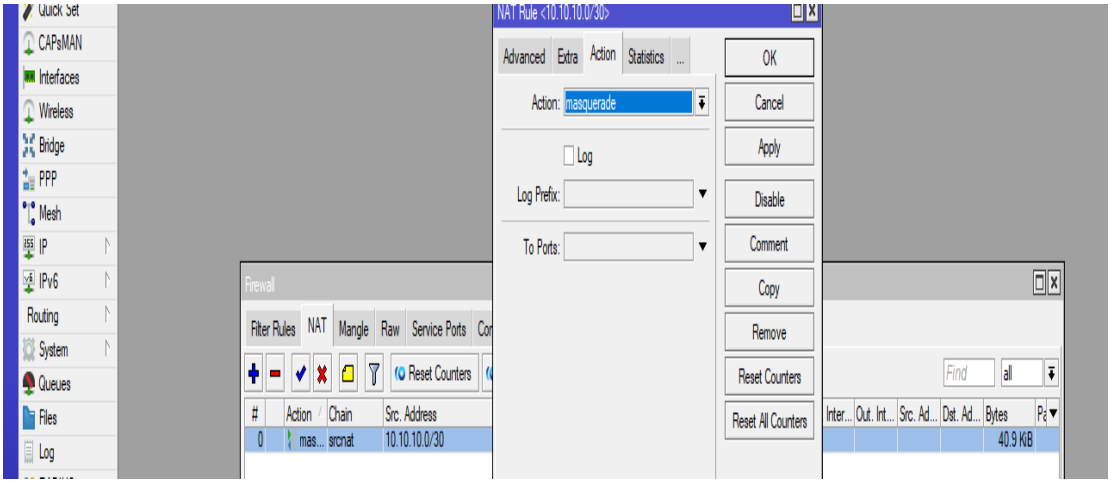


Figura 345. Configuración del NAT masquerade (b)

Fuente: Los autores

5. Configurar la IP para el port2 del fg-sucursal.

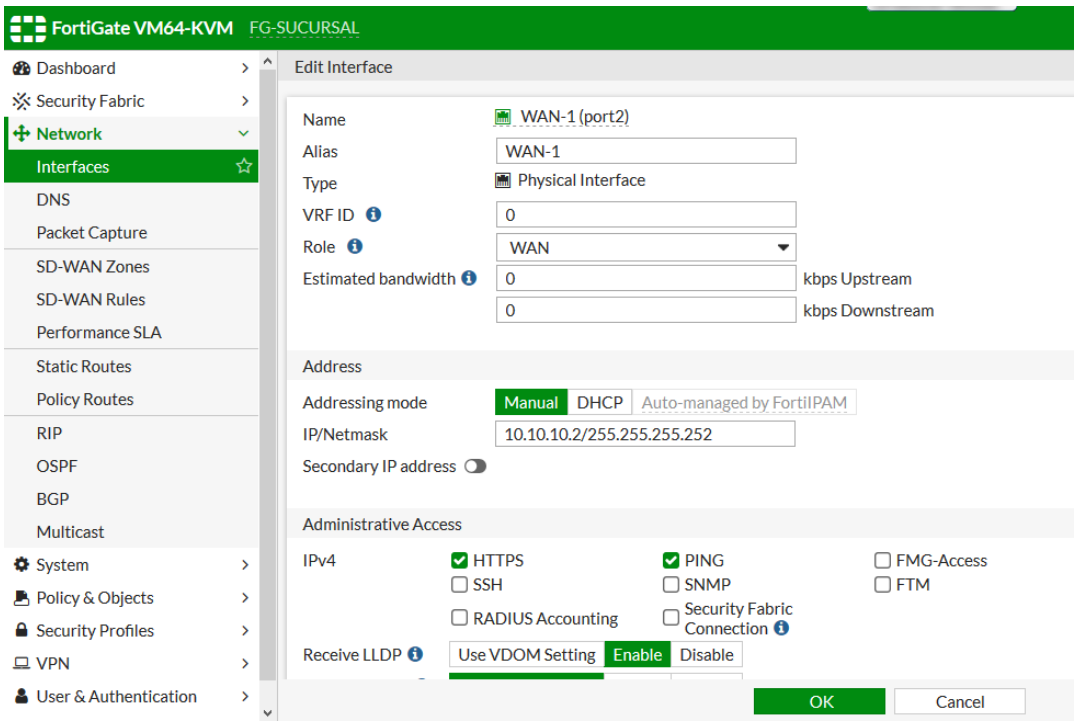


Figura 346. Configuracion IP port 2 FG-SUCURSAL
Fuente: Los autores

6. Configurar el port4 para la red local del fg-sucursal.

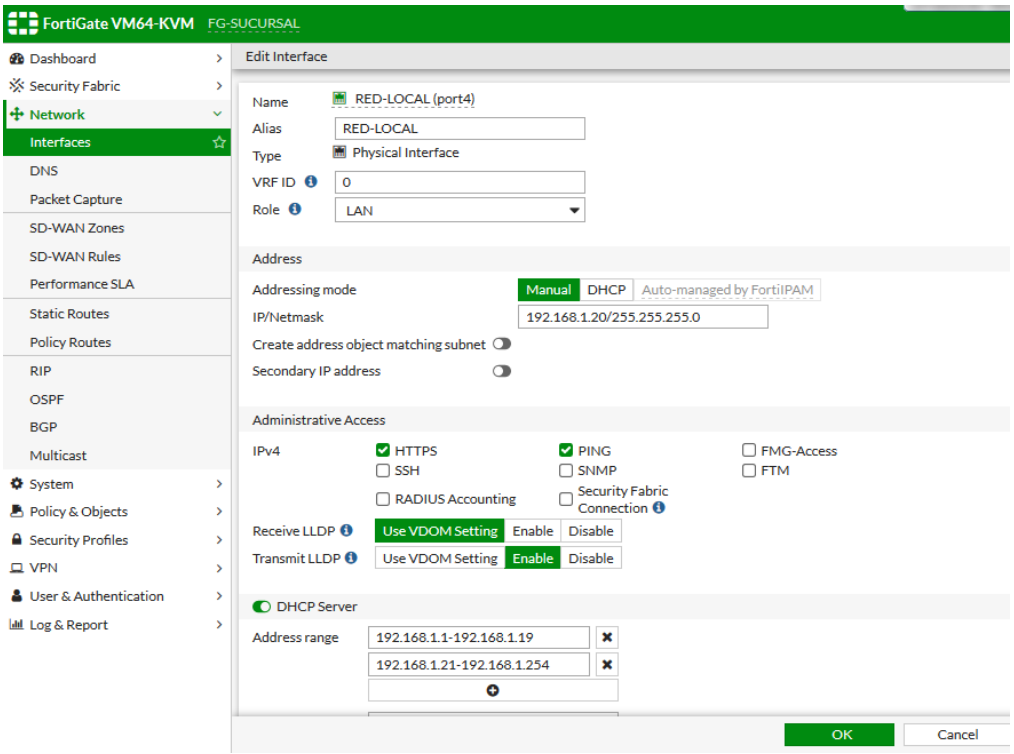


Figura 347. Configuracion red local port 4 FG-SUCURSAL
Fuente: Los autores

7. Configurar DNS al fg-sucursal.

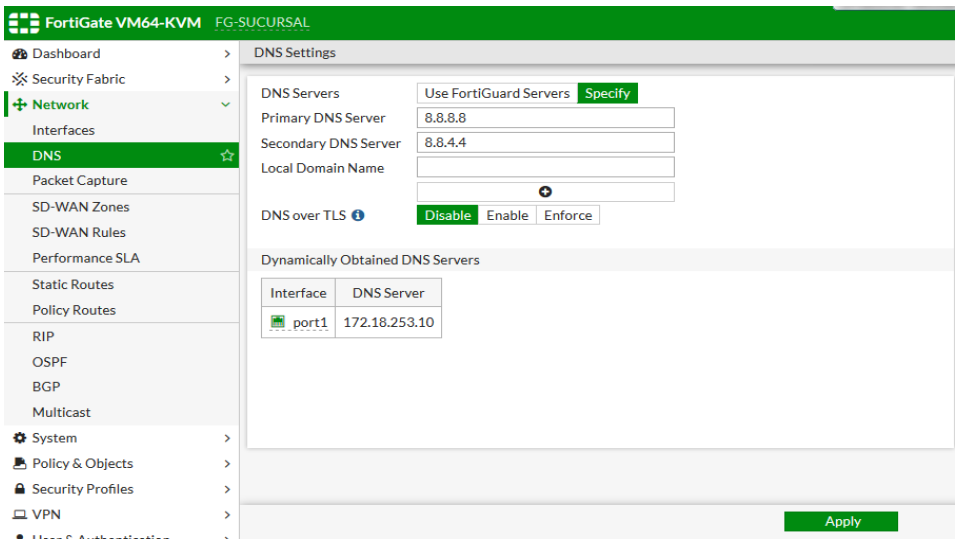


Figura 348. Configuracion DNS FG-SUCURSAL
Fuente: Los autores

8. Configurar la interfaz que va a pertenecer a la SD-WAN.

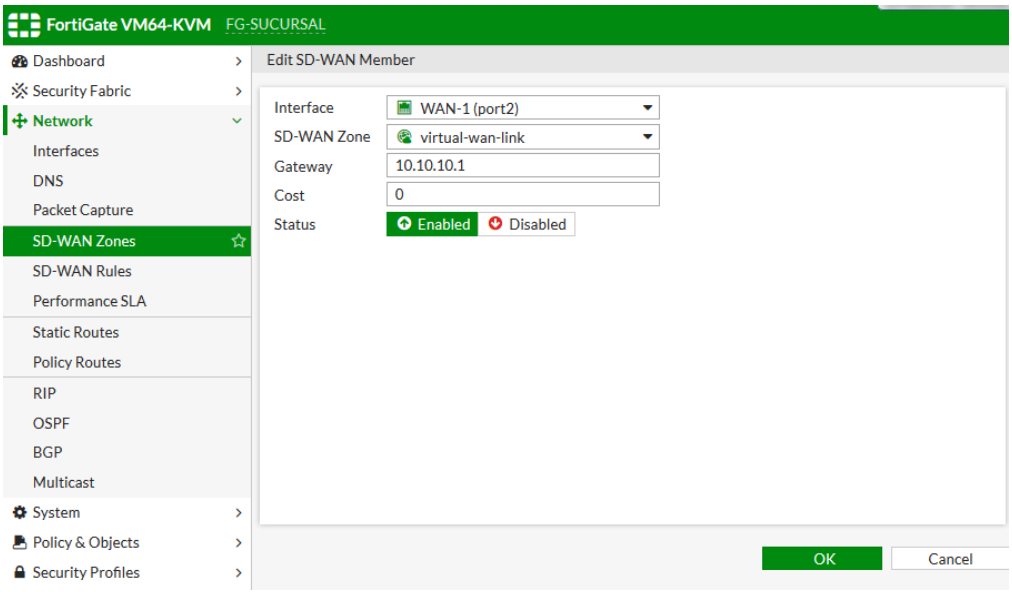


Figura 349. Configuracion SD-WAN Zones FG-SUCURSAL
Fuente: Los autores

9. Configurar la static routes para la SD-WAN.

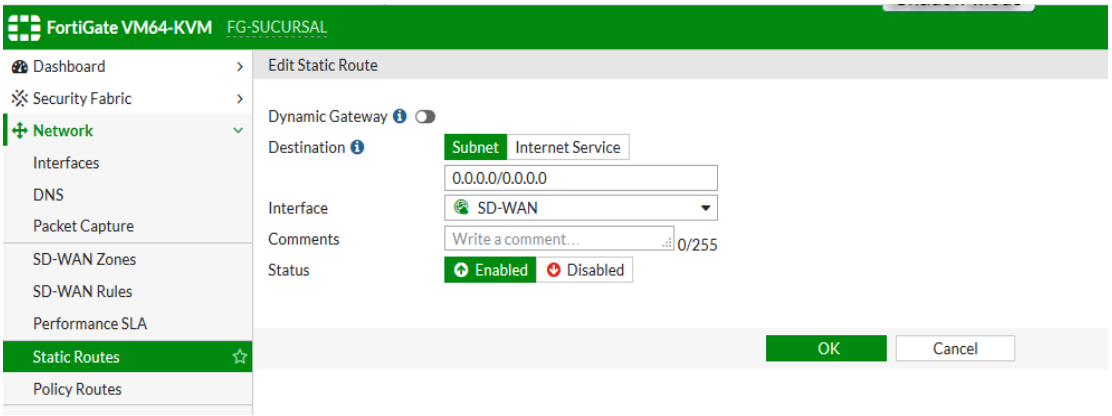


Figura 350. Configuracion Static routes FG-SUCURSAL
Fuente: Los autores

10. Configurar los layer 7 en el mikrotik de redes sociales.

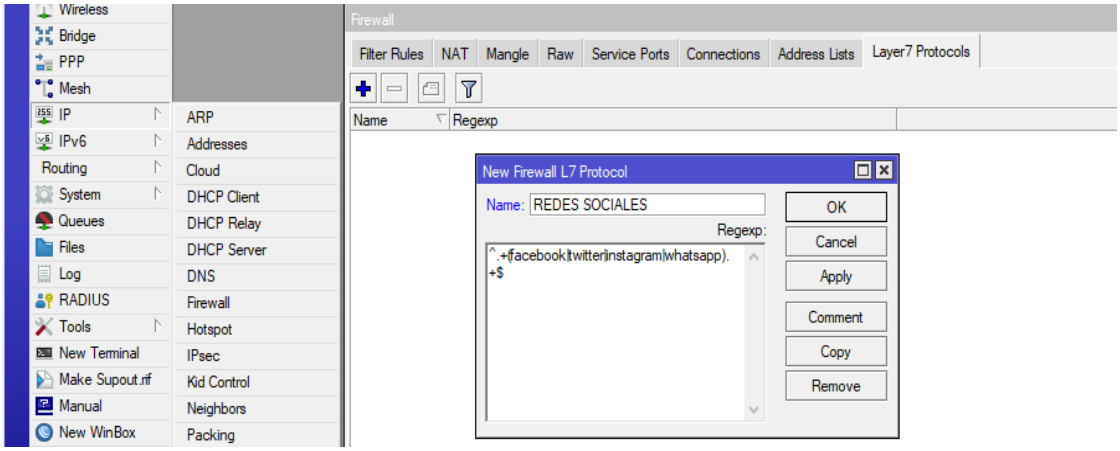


Figura 351. Configuracion layer 7 redes sociales.
Fuente: Los autores

11. Configurar layer 7 para youtube.

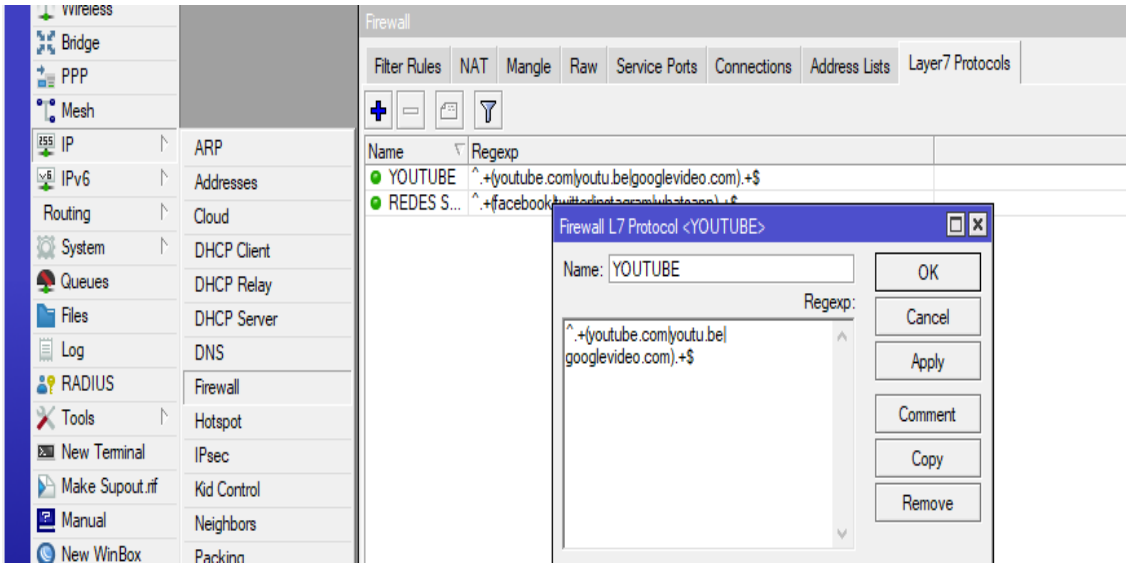


Figura 352. Configuracion layer 7 youtube.
Fuente: Los autores

12. Configurar un marcado de conexión para la red del enlace SD-WAN.

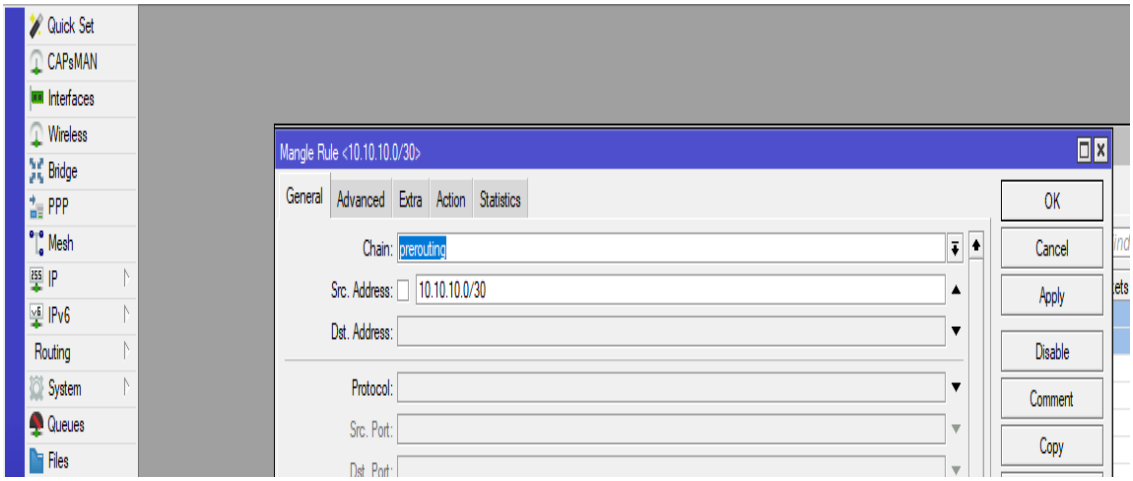


Figura 353. Marcado de conexión enlace sd-wan.(a)
Fuente: Los autores

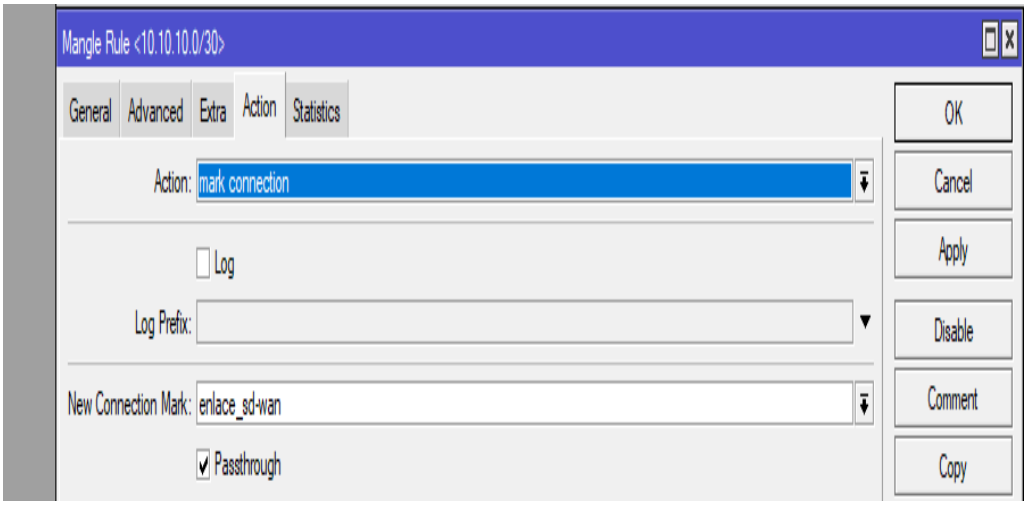


Figura 354. Marcado de conexión enlace sd-wan. (b)
Fuente: Los autores

13. Configurar un marcado de paquetes para redes sociales.

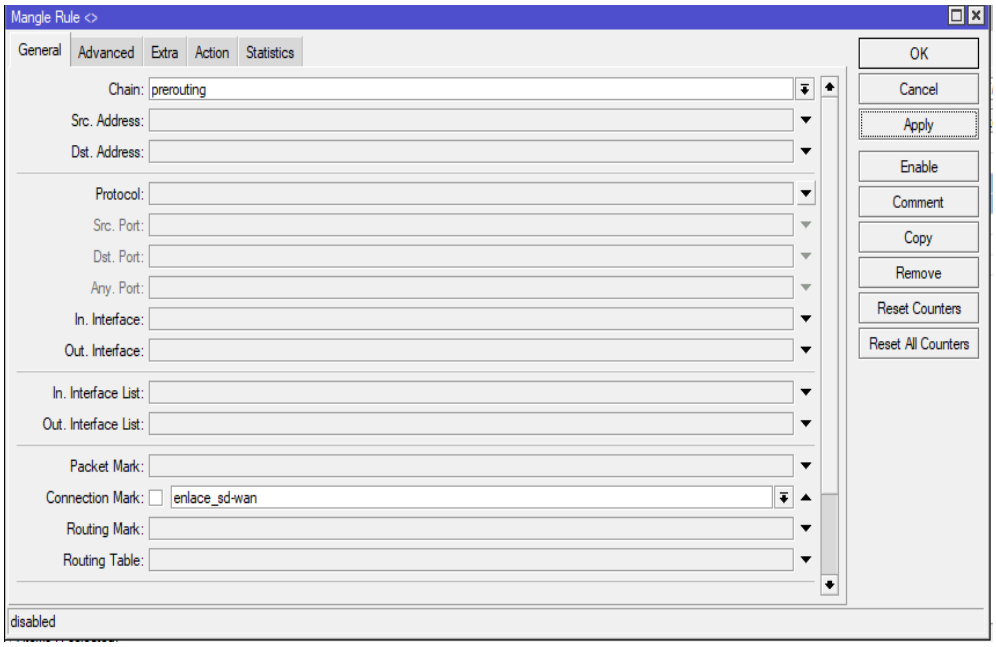


Figura 355. Marcado de redes sociales. (a)
Fuente: Los autores

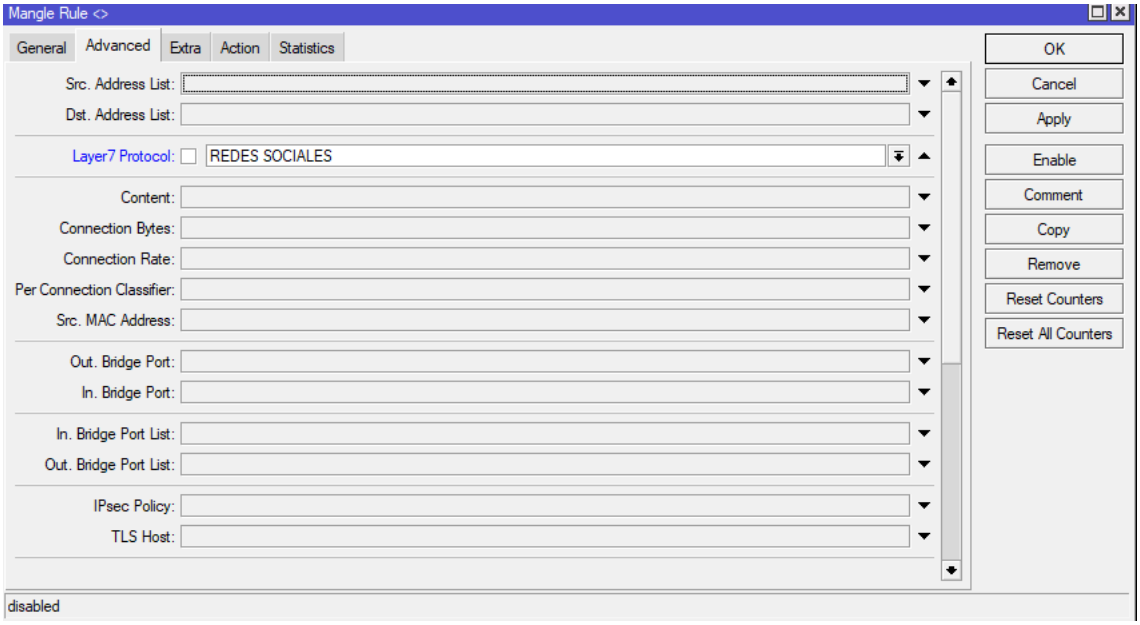


Figura 356. Layer 7 redes sociales. (b)
Fuente: Los autores

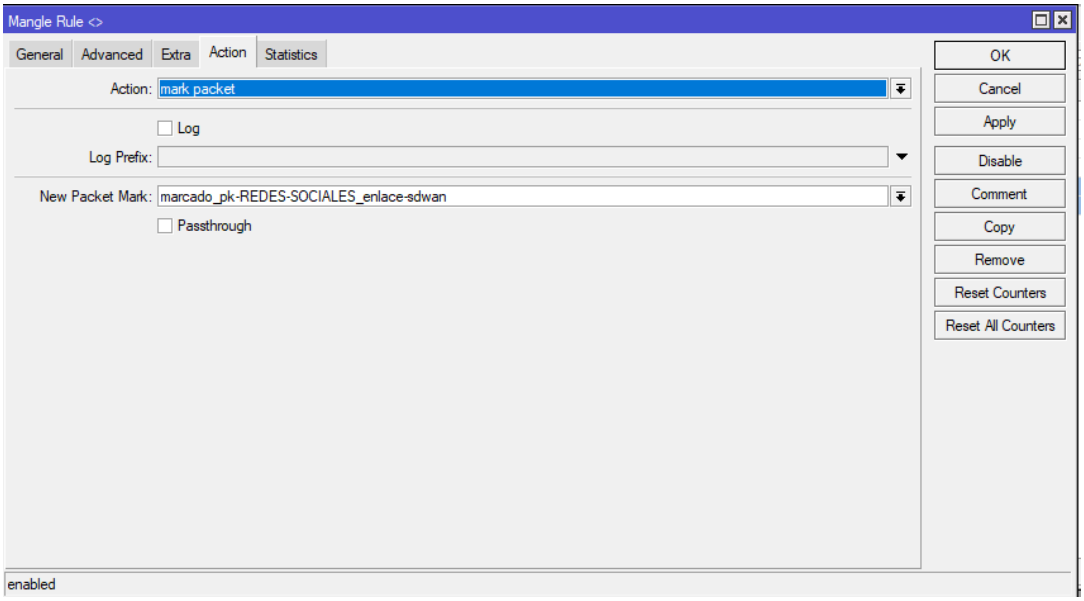


Figura 357. Configuración del packet mark redes sociales. (c)
Fuente: Los autores

6. Configurar marcado de paquetes para youtube.

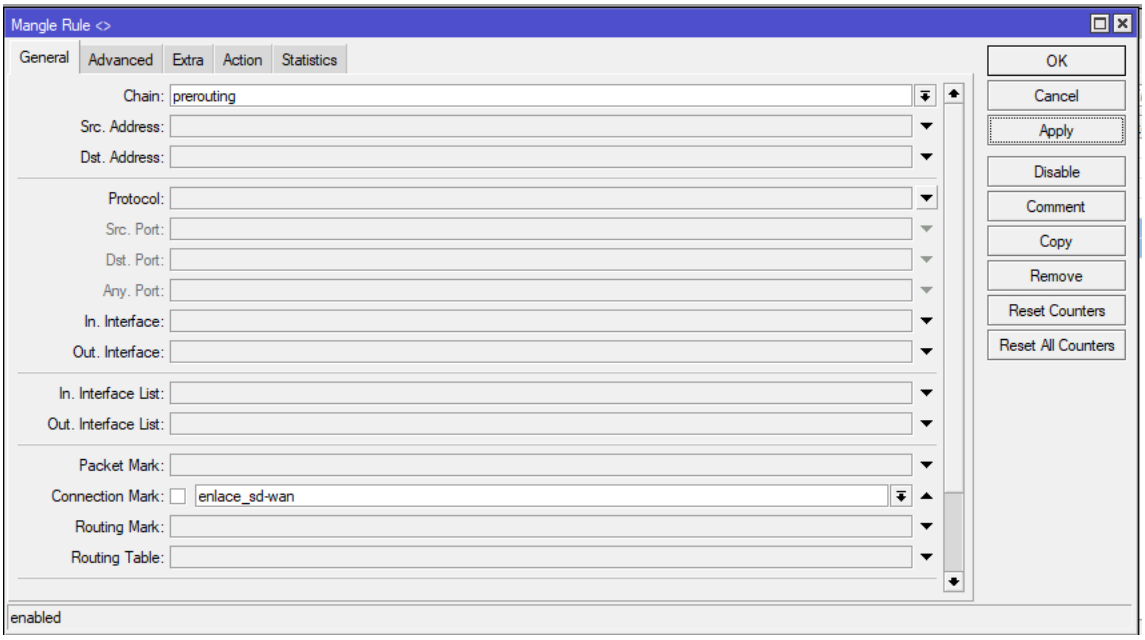


Figura 358. Marcado de paquetes youtube. (a)
Fuente: Los autores

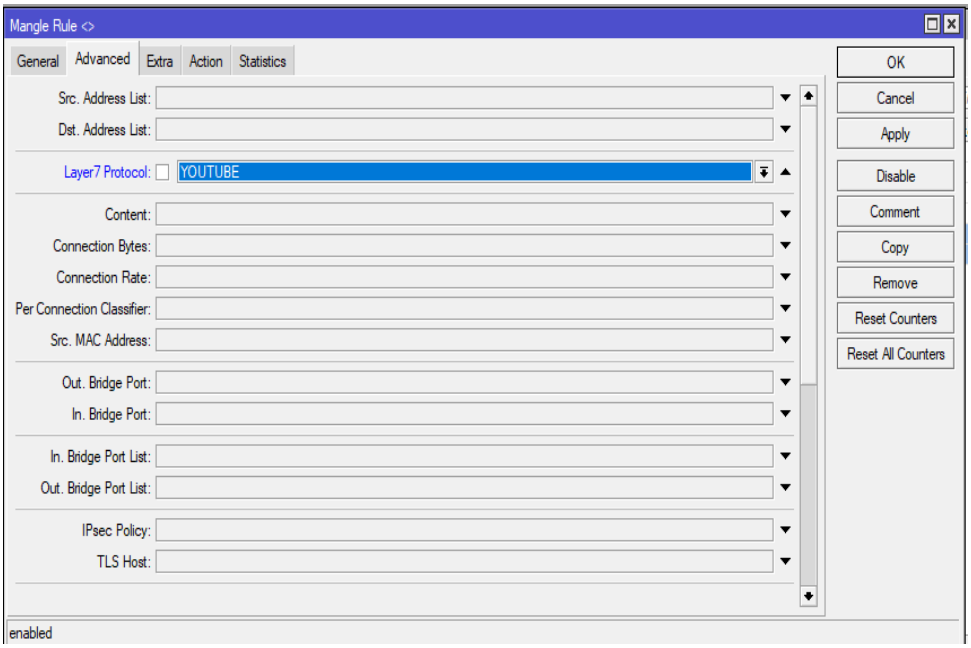


Figura 359. Layer 7 youtube. (b)
Fuente: Los autores

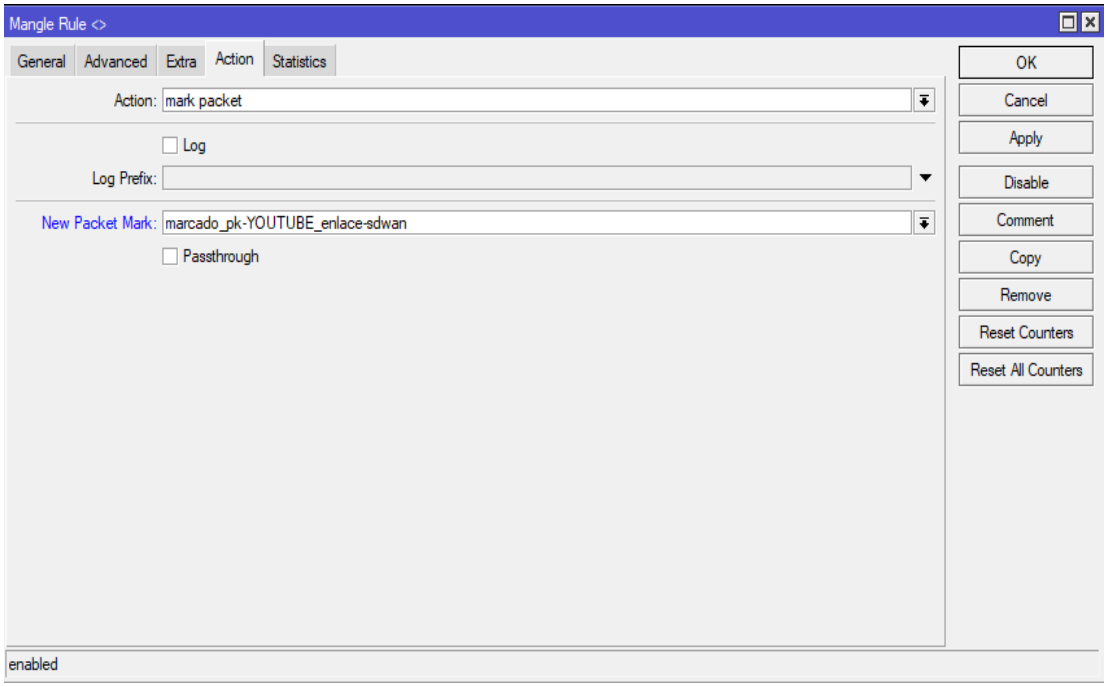


Figura 360. Configuración del packet mark youtube. (c)
Fuente: Los autores

7. Entrar a youtbe o alguna red social configurada en el layer 7 del mikrotik y vemos que genera paquetes.

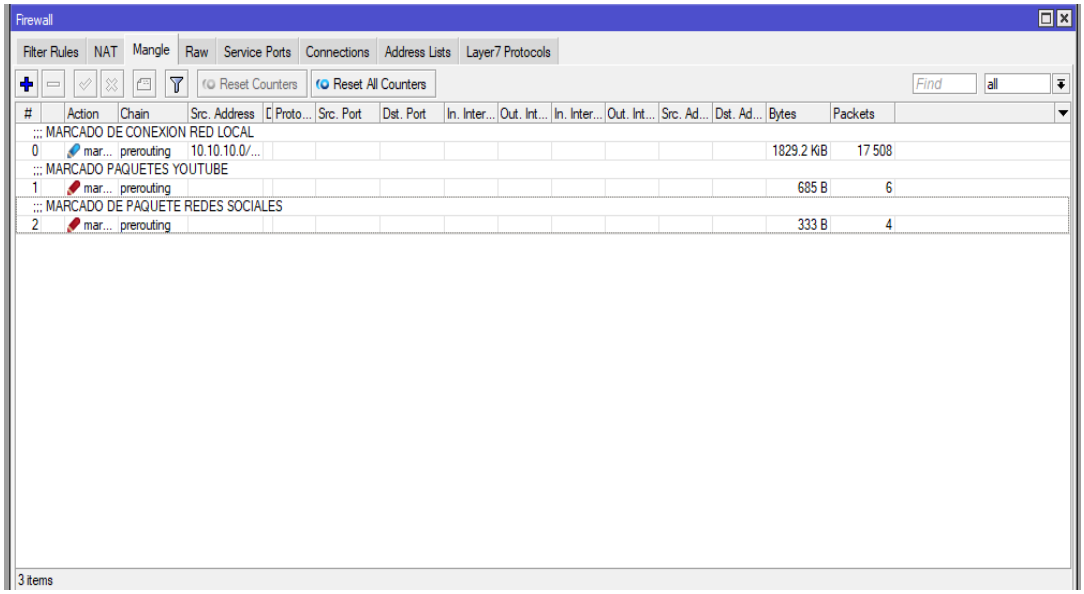


Figura 361. Visualización marcado de paquetes layer 7.
Fuente: Los autores

8. Crear una calidad de servicio para el enlace SD-WAN se le asignara upload 10MB y download 10MB.

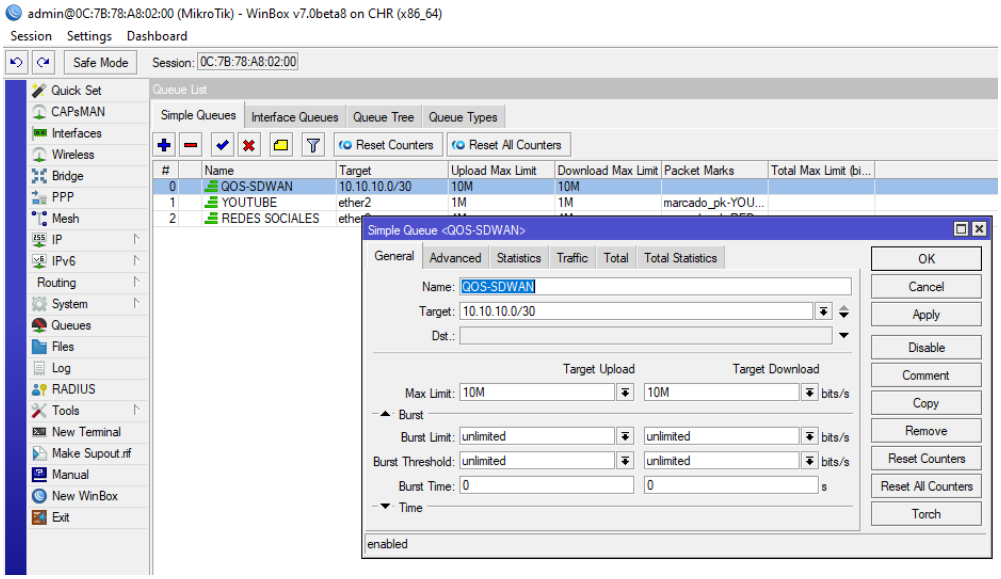


Figura 362. QOS enlace SD-WAN.
Fuente: Los autores

9. Configurar QOS para youtube 4MB/4MB.

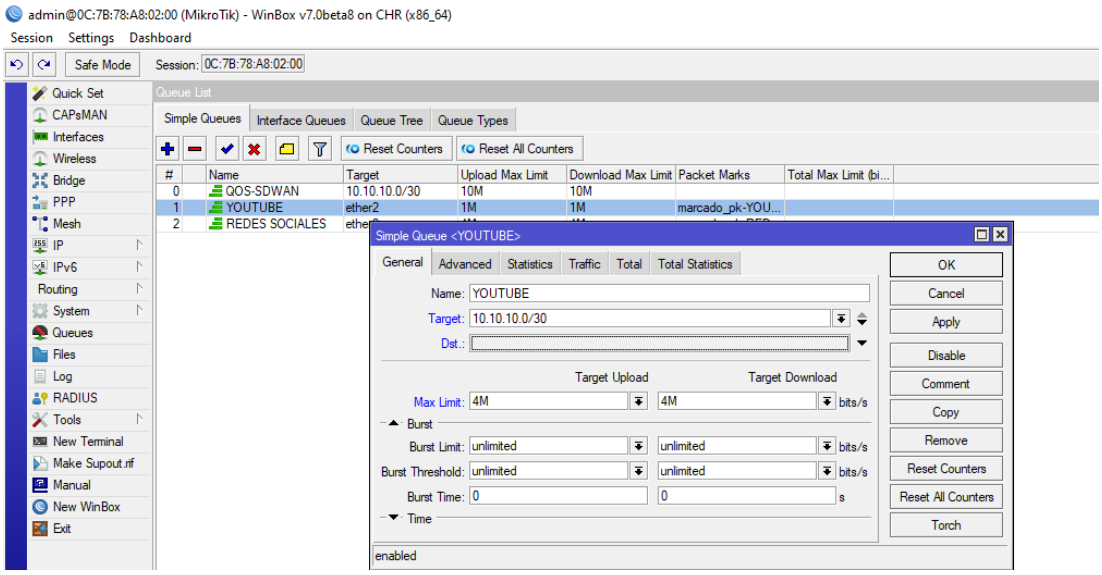


Figura 363. QOS youtube

Fuente: Los autores

10. Configurar al marcado de paquetes de youtube 3MB/3MB

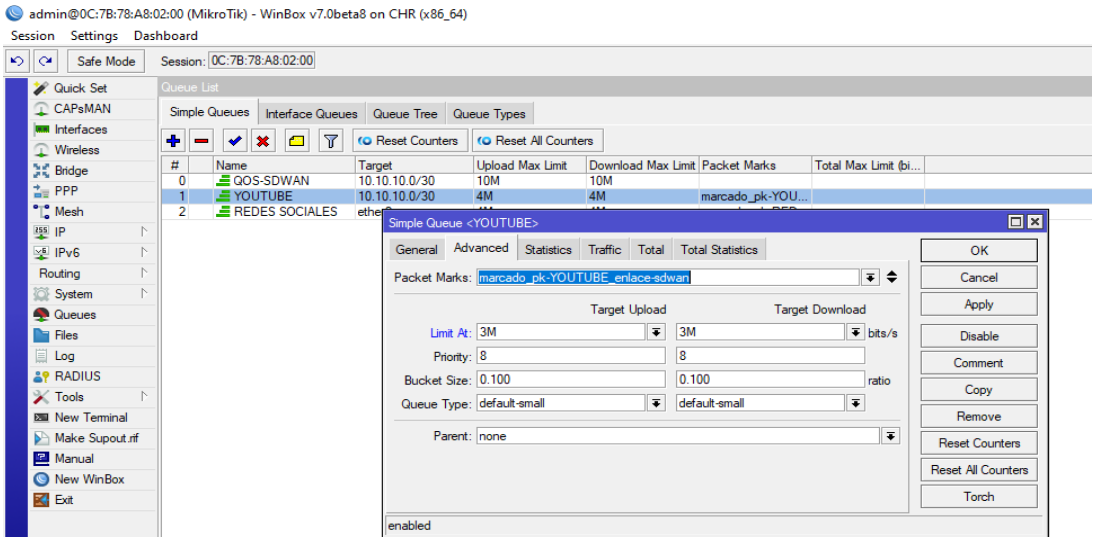


Figura 364. QOS marcado de paquetes youtube
Fuente: Los autores

11. Configurar QOS para redes sociales.

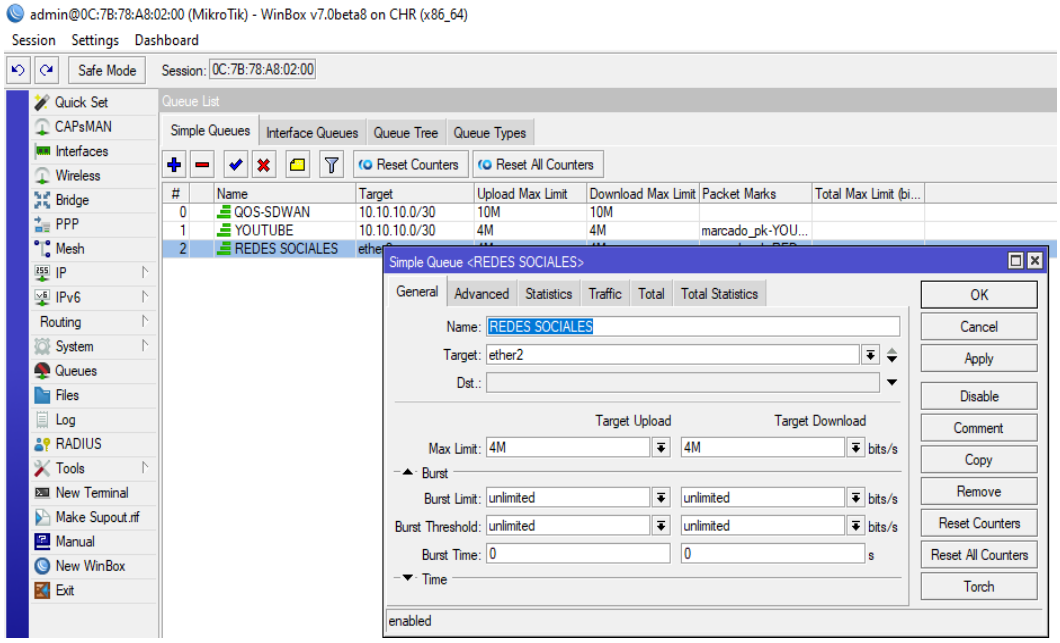


Figura 365. QOS redes sociales.
Fuente: Los autores

12. Configurar QOS al marcado de paquetes para redes sociales.

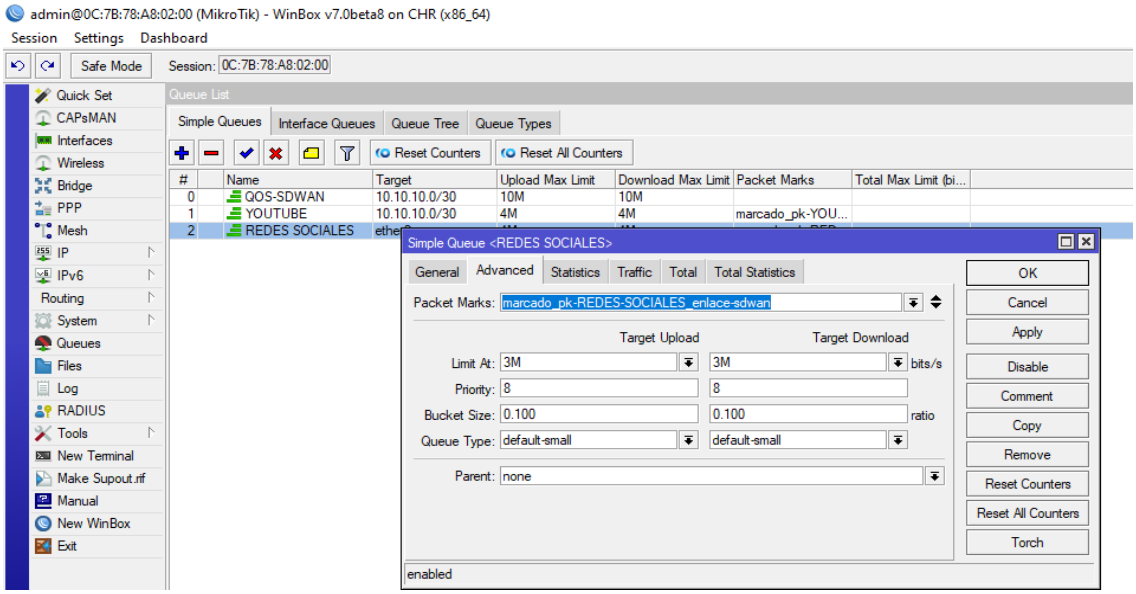


Figura 366. QOS marcado de paquetes redes sociales.
Fuente: Los autores

RECURSOS UTILIZADOS

- COMPUTADORA
- CABLE DE RED (PATCHCORD)
- GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

CAPÍTULO V

ANÁLISIS DE RESULTADOS

5.1. Análisis del proyecto

Se realizó la respectiva verificación que el proyecto cumpla los objetivos preliminarmente determinados y además se comprobó el funcionamento correcto del servidor DELL R210 II y el uso de aplicación cliente de GNS3 al instante de ejecutar la conexión al GNS3-SERVER donde utilizara los recursos de memoria RAM y CPU que le suministrara el servidor.

5.2. Comunicación de las computadoras clientes al servidor

Mediante conexión Ethernet, el servidor y las computadoras clientes deben estar conectadas a un mismo switch y pertenecer al mismo segmento de red, para la conexión al ambiente virtual para ejecutar las simulaciones de redes definidas por software se debe encender la máquina virtual que se halla instalada en el servidor accediendo a el a tráves de la dirección IP se que configuro, una vez iniciada la máquina virtual de GNS3-SERVER se instala la aplicación de GNS3 cliente y se enlaza mediante la dirección IP del GNS3-SERVER .

5.3. Elaboración del banco de prueba y prácticas.

Se realiza diez prácticas de redes definidas por software para redes de área amplias utilizando el ambiente virtual de GNS3 con sus respectivos dispositivos como routers,firewall y switch para la simulación además en este proyecto se manifiesta la instalación de virtualización con EXSI, GNS3 SERVER, memorias RAM, disco duros de estado sólidos SSD este banco de prueba sirve para simular diferentes protocolos de redes y nuevos equipos de seguridad , routers ,switches y sistemas operativos que vayan surgiendo a tráves del tiempo.

5.4. Pruebas realizadas

Se ejecuta la verificación que las computadoras clientes del laboratorio de telecomunicaciones de la Universdidad Politécnica Salesiana sede Guayaquil tengan conexión con el servidor a través de la aplicación de GNS3 cliente.

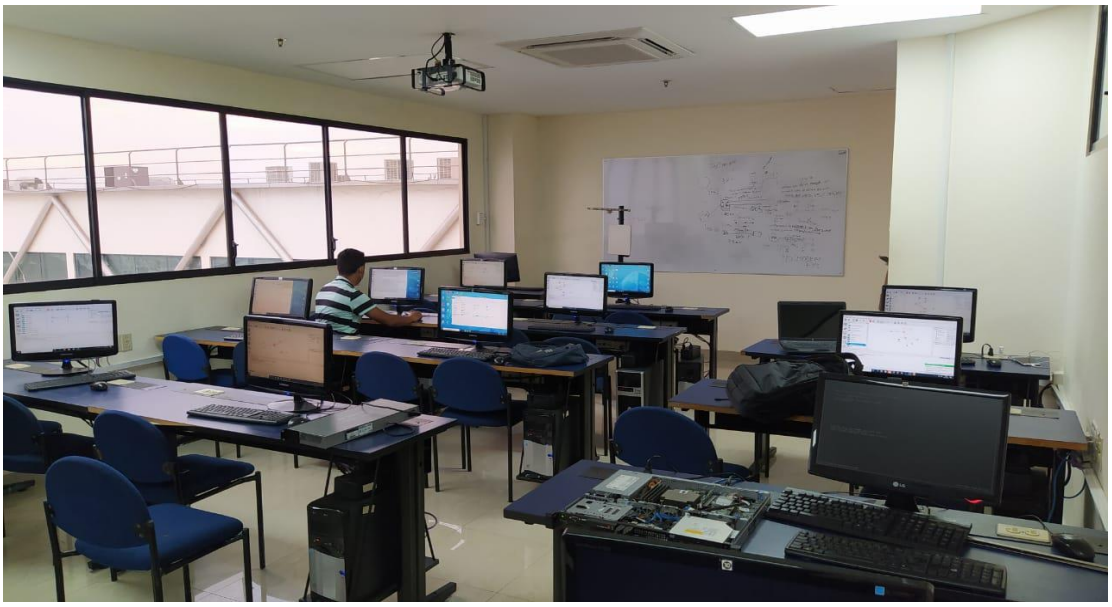


Figura 367. Verificación de conexión al servidor
Fuente. Los autores

Una vez realizada la conexión al servidor ingresamos automáticamente al ambiente virtual donde se encuentran elaboradas las prácticas.

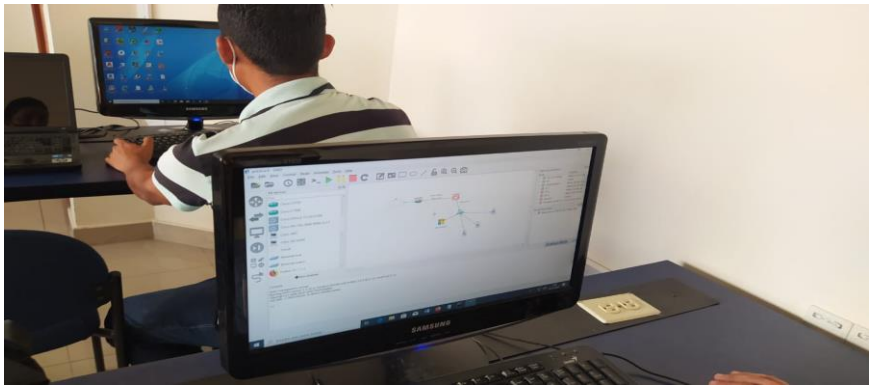


Figura 368. Verificación de conexión al servidor
Fuente. Los autores

Adicional antes de instalar GNS3 o al conectarse a través de la aplicación desactivar el antivirus o firewall del sistema operativo que se utilizando le mostrara en letras amarillas que esta siendo bloqueada la conexión al servidor.

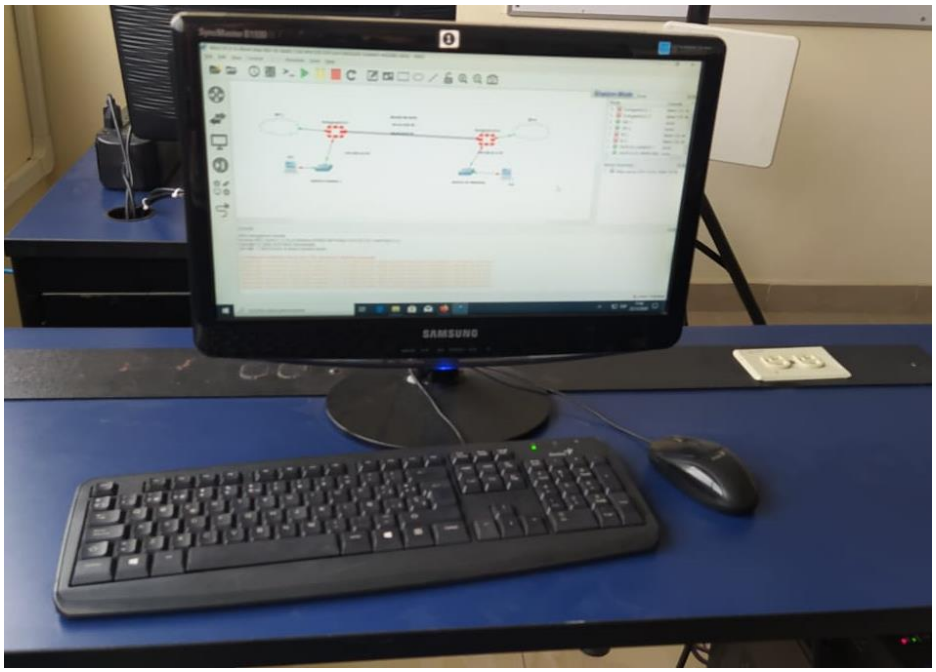


Figura 369. Firewall bloqueando conexión
Fuente. Los autores

CAPÍTULO VI

CONCLUSIONES

El objetivo principal de este proyecto técnico de un banco de pruebas para redes definidas por software de una manera virtualizada es que el estudiante consiga trabajar, configurar y diseñar redes de última generación, diseños de redes complejos con CISCO, Mikrotik, Palo Alto solo añadiendo el KVM de cualquier dispositivo al servidor utilizando los recursos de CPU y memoria RAM donde solo con la aplicación de GNS3 cliente podrá conectarse al servidor, se lo puede realizar con cualquier equipo sea PC o laptop alta y baja gama.

Para la elaboración del banco de pruebas se mejoró los recursos del servidor instalando adicionalmente 16GB de memoria RAM, el servidor constaba con 8GB de memoria y asimismo se incrementó dos unidades de estado sólido de 240GB cada uno sustituyendo el HDD mecánico.

Cabe resaltar que en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil constan computadoras de baja gama para la actualidad y frena desarrollar prácticas de simulaciones de redes informáticas en la actualidad se utiliza CISCO PACKET TRACER obteniendo una limitante en el momento de diseñar una red de datos complejas permitiendo solo simular sus dispositivos que aparecen incluidos en el software.

El resultado de este proyecto técnico es que los estudiantes ensayen como configurar equipos que en la actualidad son costosos en obtener , una de las ventajas de este proyecto que los estudiantes lograrán defenderse en el momento de efectuar sus pasantías pre-profesionales simulando equipos que constan instalado en las empresas asi obteniendo conocimiento para futuros proyectos.

Al instante de terminar la instalaciones de los discos SSD, memorias RAM, software de virtualización y la creación de la maquina virtual para el ambiente de desarrollo para las prácticas se realizó la conexión de todas las computadoras del laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil al servidor, obteniendo un resultado satisfactorio.

Para el desarrollo de este proyecto se realizo diez prácticas **PRÁCTICA 1:** Conexión remota al servidor virtual con el software GNS3, **PRÁCTICA 2:** Configuración de una red SD-WAN con Fortigate 6.2.0,**PRÁCTICA 3:** Configuración de una red SD-WAN con perfomance SLA en fortigate 6.4.2, **PRÁCTICA 4:** Configuración de una red SD-WAN con prioridad de servicios

con sd-wan rules, **PRÁCTICA 5:** Configuración de una red SD-WAN con fortigate y enlazados con dispositivos mikrotik, **PRÁCTICA 6:** Configuración de una red VPN IPSEC fortigate a fortigate, **PRÁCTICA 7:** Configuración de una red VPN IPSEC con balanceo sd-wan, **PRÁCTICA 8:** Configuración de un failover con mikrotik para un enlace SD-WAN,**PRÁCTICA 9:** Configuración de un mangle con mikrotik para el enlace SD-WAN, **PRÁCTICA 10:** Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik, donde los estudiantes pondrán los recursos suficientes para las prácticas y nuevos KVM para simular diferentes equipos.

CAPÍTULO VII

RECOMENDACIONES

Verificar que todas las conexiones eléctricas que se conectan al servidor estén en perfecto estado.

Actualizar el ambiente virtual del GNS3-SERVER cada vez que surja una nueva versión a través de la configuración del software de la máquina virtual.

Antes de actualizar realizar un backup a la máquina virtual.

Cambiar el servidor por uno más actual para realizar multiples conexiones de usuarios finales y poder realizar simulaciones de alto rendimiento en CPU y memoria RAM.

Instalar software libre de virtualización se recomienda PROXMOX.

El servidor debe estar conectado en un punto de red del laboratorio de telecomunicaciones.

Para la administración del servidor y sus configuraciones se pide que tenga conocimiento en EXSI.

CAPÍTULO VIII

REFERENCIAS BIBLIOGRAFÍA

Yenisleidy Fernández, Karen García. (2011). *Virtualización*. Cuba: Revista Digital De Las Tecnologías De La Información Y Las Comunicaciones. Obtenido de http://revistatelematica.cujae.edu.cu/index.php/tele/issue/view/4

Andrew.S. Tanenbaum & David Wetherall. (2012).*Redes de computadoras.* México: Pearson Educación. Obtenido de https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Francisco Molina.(2014). *Redes Locales*.Madrid:RA-MA,S.A. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=3228517

Rafael Castaño, Jesús López.(2013*). Redes Locales*.España: MacMillan Iberia,S.A.Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=3217345&query=redes+locales

Enrique Bellido.(2013). *Implementanción de los elementos de la red local*. Madrid:Editorial CEP,S.L. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=4499051&query=red+local

Julio Gómez López.(2014).*ADMINISTRACIÓN DE SISTEMAS OPERATIVOS*.MADRID:RA-MA EDITORIAL. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=5758899&query=administracion+de+sistemas

Francisco Carvajal Palomares.(2017). Instalación y configuración del software del servidor Web.Madrid: Editorial CEP S.L. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=5214031&query=Instalaci%C3%B3n+y+configuraci%C3%B3n+del+software+de+servidor+Web

Alfredo Abad Domingo.(2012).*Redes Locales*. McGraw-Hill/Interamericana de España, S.L. Obtenido de https://juanantonioleonlopez.files.wordpress.com/2017/11/redes-locales.pdf

CAPÍTULO IX

ANEXOS

ANEXO A. CRONOGRAMA DE DURACIÓN DEL PROYECTO

CRONOGRAMA DEL PROYECTO						
DURACION DE EJECUCION DEL PROYECTO	6 MESES					
ACTIVIDADES	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
BUSCAR SOFTWARE DE VIRTUALIZACION						
BUSCAR EL HADWARE NECESARIO						
REPOTENCIAR SERVIDOR						
INSTALAR SISTEMA OPERATIVO DE VIRTUALIZACION						
INSTALAR PLATAFORMA DE GNS3						
DESARROLLO DE LAS PRÁCTICAS						
ELABORACION DE LA DOCUMENTACIÓN						

Tabla 1. Cronograma del proyecto técnico

ANEXOS B. Sistemas Operativos de virtualización

SOFTWARE DE VIRTUALIZACIÓN	CARACTERISTICAS	VENTAJAS	DESVENTAJAS
VMware Sphere	Consolidar el hadware para mejorar la utilización de la capacidad. Aumentar el rendimiento para logar una ventaja competitiva. Reducir la inversión en capital y los gastos operativos,	Eficiencia gracias a la utilización y a la automatización. Reducción drástica de los costes de TI.	El precio de una solución paga de vSphere puede llegar entre $4000y $8000. No es compatible con una gran lista de hardware domestico.
Red Hat Virtualization	Basado en Linux. Colaboración open source.	Virtualizacion abierta permite ahorrar dinero. Rendimiento mejorado de las cargas de trabajo.	Acceder a un soporte completo y adecuado. Regimen de pago o suscripción.

		Configuración sencilla.	
Proxmox VE	Código abierto. Permite la migración. Plantillas SO.	Aprovechamiento de recursos. Flexibildiad para testing. Clustering. Alta disponibilidad (HA).	RAID (desventaja en relación a la necesidad de tener discos iguales. Requiere hardware costoso. Mayor probabilidad a fallas fatales.
Microsoft Hyper-V	Memoria dinámica. Migración en vivo. Migración de almacenamiento.	Ahorro en costes de hardware. Facilitación de creación de backup. Establece o amplia un entorno de nube privado.	Aplicaciones mas lentas. Requiere licencia de software. Es utilizado generalmente para Windows.

Tabla 2. Comparación de sistemas operativos de virtualización

ANEXO C. DELL R210 II

Procesadores	Familia de productos del procesador E3-1200 de cuatro núcleos Intel® Xeon® Familia de productos del procesador i3-2100 de dos núcleos Intel Core™ Series G600 y G800 de dos núcleos Intel Pentium® Series G400 y G500 de dos núcleos Intel Celeron®
Chipset	Intel C202
Memoria	Hasta 32 GB (4 ranuras DIMM): DDR3 de 1 GB/2 GB/4 GB/8 GB hasta de 1333 MHz
Opciones de virtualización	Citrix® XenServer® VMware® vSphere® ESX™ y ESXi™ Red Hat Enterprise Virtualization®
Sistemas operativos	Microsoft® Windows Server® 2012 Microsoft Windows Server 2012 Essentials

	Microsoft Windows® Small Business Server 2011 Microsoft Windows Small Business Server 2008 Microsoft Windows Server 2008 R2 Foundation SP1 Microsoft Windows Server 2008 SP2, x86/x64 (x64 incluye Hyper-V®) Microsoft Windows Server 2008 R2 SP1, x64 (incluye Hyper-V v2) Microsoft Windows HPC Server 2008 Novell® SUSE® Linux Enterprise Server Red Hat® Enterprise Linux®
Opciones de almacenamiento	Unidad de estado sólido de 2,5" SATA, SAS (10.000 RPM) SAS (15.000 RPM) de 3,5", SAS nearline (7.200 RPM), SATA (5.400 RPM, 7.200 RPM).
Capacidad máxima de almacenamiento interno	Hasta 6 TB
Controladora integrada de red	Una Broadcom BCM 5716 de dos puertos
Controladoras RAID	PERC S100 (basada en software) PERC S300 (basada en software) PERC H200 (6 Gb/s)

Tabla 3 .Especificaciones del Servidor Dell PowerEdge R210 II

ANEXO D. Disco Solido SSD

Factor de forma	2,5" y M.2 2280
Interfaz	SATA Rev. 3.0 (6 Gb/s), retrocompatible con SATA Rev. 2.0 (3 Gb/s)
Capacidades[2]	120GB, 240GB, 480GB, 960GB, 1,92 TB
NAND	3D
Consumo eléctrico	0,195 W en reposo / 0,279 W promedio / 0,642 W (máx) lectura / 1,535 W (máx) escritura
Dimensiones	100,0 mm x 69,9 mm x 7,0 mm (2,5”) 80 mm x 22 mm x 1,35 mm (M.2)
Peso	40g
Temperatura de servicio	0°C~70°C
Temperatura de almacenamiento	-40°C~85°C
Vibraciones en funcionamiento	2,17 G máxima (7-800 Hz)
Vibración en reposo	20 G máximo (10-2000 Hz)
Vida útil	1 millón de horas MTBF
Bytes escritos en total (TBW)[4]	240GB: 80TB

Tabla 4: KINGSTON A400 SSD SATA de 2,5"

ANEXO E. LISTADO DE MATERIALES

EQUIPO	VALOAR
MEMORIAS RAM	125 $
DISCO DUROS SSD	85 $

Tabla 4: Materiales del proyecto técnico