PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de
Magíster en Tecnologías de Información mención Gestión y Administración de TI

SIMULACIÓN DE UNA RED SDWAN ADVPN PARA EL DESARROLLO DE PROYECTOS EMPRESARIALES

Autor: Juan Andres Solis Poveda
Director: Juan francisco Chafla

Quito, 10 de mayo de 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, JUAN ANDRÉS SOLIS POVEDA, con CI 1720235876, autor del trabajo de graduación intitulado: "SIMULACIÓN DE UNA RED SDWAN ADVPN PARA EL DESARROLLO DE PROYECTOS EMPRESARIALES", previa la obtención del título profesional de Magíster en Tecnologías de la Información con mención en Gestión y Administración de TI, en la Facultad de Ingeniería

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENECYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de información de la Educación Superior del Ecuador para su difusión pública respetando los derechos del autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: "SIMULACIÓN DE UNA RED SDWAN ADVPN PARA EL DESARROLLO DE PROYECTOS EMPRESARIALES", presentado por el maestrante JUAN ANDRES SOLIS POVEDA, titular de la Cédula de Identidad Nº 1720235876 para optar al Grado de Magíster en Tecnologías de Información mención Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ciencias de la Educación.

En la ciudad de Quito, a los 10 días de mayo de 2023

JUAN FRANCISCO CHAFLA ALTAMIRANO C.I. 0603003609

jchafla390@puce.edu.ec

NRO TELEFONO: 0984691990

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 9% índice de similitud con otras fuentes.

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

TesisSolisv2

INFORME DE ORIGINALIDAD

9%	8%	3%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Trabajo del estudiante	2%
2	repositorio.ucsg.edu.ec Fuente de Internet	1%
3	repositorio.espe.edu.ec Fuente de Internet	<1%
4	repositorio.ug.edu.ec Fuente de Internet	<1%
5	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%
6	Submitted to Liberty University Trabajo del estudiante	<1%
7	es.slideshare.net Fuente de Internet	<1%
8	vietnetdisti.freshdesk.com Fuente de Internet	<1%
9	www.lareferencia.info Fuente de Internet	

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo JUAN ANDRÉS SOLIS POVEDA, con cédula de identidad # 1720235876, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; se ha consultado las referencias bibliográficas que se incluyen en el presente documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a esté trabajo, a la PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Juan Andrés Solis Poveda

C.C.: 1720235876

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

SIMULACIÓN DE UNA RED SDWAN ADVPN PARA EL DESARROLLO DE PROYECTOS EMPRESARIALES

Autor: Juan Andrés Solis Poveda

Director -Tutor: Juan Francisco Chafla

Fecha: 10 de mayo del 2023

RESUMEN

El presente trabajo de titulación permite diseñar y simular sobre GNS3 y VMware, una arquitectura SDWAN ADVPN; la redes basadas en túneles Dinámicos ADVPN permiten simplificar el proceso de configuración y solución de problemas e incidentes en las redes empresariales ya que se crean túneles bajo demanda y permite tener una topología full mesh; por otro lado, las redes SDWAN permiten la utilización simultánea de los diferentes canales de comunicación que puedan entregar los ISPs, de esta manera cada enlace de Internet puede transmitir un tráfico definido con la tranquilidad de que se está ocupando el ancho de banda contratado y existe redundancia en el caso de fallas. La combinación de ambas tecnologías ofrece una solución para que las sucursales pueden comunicarse entre sí cuando lo necesiten y permanezcan en standby cuando no se requiera, optimizando así recursos de la red.

Palabras clave: ADVPN, SDWAN, GNS3, VMware

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

SIMULATION OF AN ADVPN SDWAN NETWORK FOR THE DEVELOPMENT OF BUSINESS PROJECTS

Autor: Juan Andrés Solis Poveda

Director -Tutor: Juan Francisco Chafla

Fecha: 10 de mayo del 2023

ABSTRACT

The present titling work allows to design and simulate on GNS3 and VMware, a SDWAN ADVPN architecture; networks based on ADVPN Dynamic tunnels allow to simplify the process of configuration and solution of problems and incidents in business networks since tunnels are created on demand and allows to have a full mesh topology; On the other hand, SDWAN networks allow the simultaneous use of the different communication channels that ISPs can deliver, in this way each Internet link can transmit a defined traffic with the peace of mind that the contracted bandwidth is being used and there is redundancy in case of failures. The combination of both technologies offers a solution so that branches can communicate with each other when they need to and remain on standby when not required, thus optimizing network resources.

Keywords: ADVPN, SDWAN, GNS3, VMware

INTRODUCCIÓN

El crecimiento acelerado de las comunicaciones a nivel global crea un desafío constante para que los proveedores de servicios y las empresas busquen desplegar nuevos métodos de conexión entre sus concentradores y cada una de las sucursales; para ello, la aplicación tecnologías que permitan simplificar la implementación y la solución de problemas durante su uso se hace más evidente. La utilización de SDWAN ADVPN permite que mediante túneles dinámicos y bajo demanda las sucursales puedan comunicarse entre ellas y hacia Matriz, utilizando los canales de Internet de cada ISP.

El trabajo inicia con el planteamiento del problema en el se explica la formulación del problema, objetivos generales y específicos y la justificación de la investigación.

Los estudios previos de investigación en el capítulo dos permiten desde varios autores mantener una referencia de estudio; además se aborda el desarrollo de los fundamentos teóricos necesarios para el presente proyecto, tales como el estudio de la red de área extendida que luego será utilizada y definida mediante software llamado SDWAN, la descripción de los túneles VPN dinámicos y herramientas de software que forman parte el diseño y simulación del proyecto.

El tipo de investigación se presentan en el capítulo tres, en el que permite enfocar el desarrollo del proyecto en una metodología específica para la solución del problema planteado, las técnicas de análisis que ayudan a organizar y estructurar el trabajo.

Finalmente, se expone el diseño y simulación de una red SDWAN ADVPN con un enfoque práctico en las arquitecturas empresariales debido a que sus características se basan en una topología dinámica y escalable en el tiempo.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

Actualmente, se plantea múltiples escenarios de cambio a nivel tecnológico, permitiendo a las empresas mejorar tanto en su desempeño como en su productividad, este nuevo enfoque se traduce en buscar proveedores de servicios que cumplan con todos los estándares actuales de seguridad y nuevos esquemas de conectividad.

Los protocolos de comunicación tradicionales, utilizan generalmente mecanismos de redundancia con uno o dos proveedores de servicios de Internet ISP, teniendo respaldada la conexión de las sucursales hacia Matriz ante cualquier desastre, esta es una forma de asegurar que la información pueda ser transmitida sin mayor interrupción con el modelo denominado principal y backup, la limitación que tiene este esquema es que no se aprovecha correctamente el envío de tráfico por la segunda última milla, ya que es pasiva y solo funciona como respaldo, en el modelo activo – activo se puede enviar y balancear la carga de información por los dos enlaces, configurando cada regla bajo un diseño especifico según las necesidades del cliente.

Las empresas requieren una mayor velocidad de respuesta en conectividad para consumir los recursos de los servidores alojados en Matriz y para comunicarse entre sucursales, para ello se opta por diseñar una arquitectura descentralizada para que las comunicaciones se realicen de manera dinámica y lleguen a sus destinos sin dar saltos innecesarios que ocasionas lentitud en los servicios, esto se lleva a cabo mediante la conexión ADVPN SDWAN que permite el uso de dos interfaces WAN que componen una interfaz virtual, la cual administrará toda la ed.

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

- Realizar una simulación de una red SDWAN ADVPN utilizando un software de entorno grafico de equipos Firewalls de próxima generación NGFW para desarrollar proyectos empresariales.

1.2.2. Objetivos Específicos

- Presentar los fundamentos teóricos de SDWAN ADVPN y exponer las ventajas del presente proyecto.
- Analizar la arquitectura SDWAN ADVPN, parámetros y características de sus componentes para la simulación del proyecto.
- Realizar pruebas experimentales de una red SDWAN ADVPN en un entorno de simulación.
- Analizar los resultados obtenidos, luego de la simulación de la red SDWAN ADVPN realizada.

1.3. Justificación de la Investigación

Las empresas requieren de servicios que les permita simplificar y administrar sus recursos de manera más ágil y simplificada, uno de los requisitos más importantes es poder aprovechar todos los recursos de conectividad que puedan brindar sus proveedores de servicios de Internet ISP, esto se lo logra teniendo una arquitectura tecnológica que permita a la red de área extendida estar bajo un software definido por una interfaz virtual, permitiendo tener tiempos menores de conexión entre sucursales y hacia Matriz, mejorando el

rendimiento de la comunicación de los datos.

La arquitectura Hub and Spoke es muy utilizada ya que se centraliza todos los servicios en Matriz y las sucursales deben viajar hacia el concentrador para consumir sus recursos, este esquema está cambiando debido a que muchos los servidores están siendo migrados a la nube ya sea pública o hibrida y además las sucursales requieren comunicarse entre ellas debido a que la información ya no se encuentra agrupada en un solo punto, por lo que la necesidad de descentralizar los servicios es cada vez más alta, esto implica cambiar de topología lógica para que las sucursales disminuyan sus tiempos de conexión y puedan comunicarse entre ellas.

Para permitir la comunicación entre sucursales y disminuir los tiempos de respuesta se utilizará el establecimiento de túneles VPN de manera dinámica, esto permitirá que las agencias puedan tener una conectividad directa bajo demanda y ya no tendrá la necesidad de llegar hasta Matriz, parea ello, se utilizará tules seguros con autodescubrimiento ADVPN dentro de un servicio SDWAN.

El nuevo esquema de configuración permitirá dinamizar la comunicación y mejorará el rendimiento y disponibilidad de los servicios ya que se simplificará y aprovechará los recursos tecnológicos, una de las ventajas de SDWAN es tener un modelo activo – activo entre las interfaces WAN permitiendo utilizar las rutas de salida hacia Internet y consumir el ancho de banda de cada recurso organizando el tráfico según las necesidades y prioridades que tenga la información.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Para el estudio planteado, se consideraron cuatro casos de estudio como antecedentes y referentes de investigación para el desarrollo del proyecto, a continuación, se detallan los trabajos indicados:

Bustos Sánchez (2019), en su tema de tesis *Análisis de factibilidad técnico y económico entre una red MPLS Traffic Engineering (TE) con IPSEC y una red Sd-Wan moderna*, realizó una comparación entre el desempeño de una red MPLS con Traffic Engineer TE y túneles IPsec con una red MPLS configurada en un entorno de SDWAN que es el software defino por la WAN.

La comparación que se realizó tuvo como objetivo encontrar niveles de jitter, seguridad, latencia, BW (ancho de banda) y calidad de Servicio (QoS) para realizar un análisis acerca de cuál es la mejor tecnología que se puede utilizar tanto por el costo total de implementación como el beneficio que lleva tener una de las dos redes configuradas e instaladas en los proveedores de servicios ISP.

Se concluyó que las redes configuradas con SDWAN brindan flexibilidad, disponibilidad y la posibilidad de configurar y administrar de manera centralizada las redes simplificando las tareas de los administradores de red; además de disminuir los tiempos de conectividad y los costos de implementación. SDWAN ofrece balanceo de cargas entre múltiples rutas que pueden ser enlaces de Internet o Datos permitiendo así que se puedan independizar los servicios.

Carrasco Cabrera (2020), en su proyecto *Diseño y simulación de una red de accesos en GNS3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador*, plantea

el diseño de una red de accesos con la tecnología SDWAN para el uso en medianas empresas en el Ecuador, mediante la utilización del software de simulación gráfica de redes GNS3, logrando evidenciar los beneficios y aplicaciones de dicha tecnología, ya que este software permite simular entornos reales de redes de alta disponibilidad y tolerante a fallas, a partir de los modos de configuración y características propias de los equipos.

Carrasco, en su propuesta de investigación identifica todas las mejoras en cuanto a la disponibilidad, uso efectivo de anchos de banda de los enlaces en la infraestructura, optimización de tráfico en contraste con las redes tradicionales; adicionalmente, un punto muy importante que aporta es la administración centralizada que disminuye los tiempos de ejecución de cambios e implementación.

Entre los principales aspectos que concluye en su trabajo está la flexibilidad y adaptabilidad a los cambios que se puedan requerir en el crecimiento de una empresa, esto implica que las redes sean más seguras y su presupuesto para los proyectos disminuyan económicamente.

Rodríguez Limones (2021) en su proyecto *DISEÑO DE IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD GESTIONADA CON SD-WAN PARA UNA RED MPLS QUE PROVEE SERVICIOS DE INTERNET Y DATOS PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA*, plantea el diseño del servicio de Seguridad Gestionada para la Universidad Politécnica Salesiana y su implementación mediante Red de Área Extendida Definida por Software (SDWAN), tanto para los servicios de Internet como para los servicios de Datos en la red MPLS.

Uno de los objetivos específicos de este trabajo es aprovechar todos los recursos físicos y lógicos que proporcionan dos proveedores de Servicios ISP contratados en un esquema activo – activo para utilizar no solo como contingencia sino para poder ocupar el

ancho de banda contratado mediante el balanceo de cargas y la calidad de servicio que se puede configurar en el SDWAN.

El resultado de este trabajo expone las ventajas de la utilización de SDWAN frente a las redes tradicionales, ya que se puede configurar las reglas en las que analice de manera autónoma cual es el mejor camino por calidad de servicio para que se enrute el tráfico, con ello se genera mayor estabilidad, confiabilidad y disponibilidad en el servicio de Internet y Datos.

Marín Santamaría (2021), en su proyecto de tesis *Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos*, plantea la necesidad de buscar un nuevo diseño de red que sea escalable y que permita la conectividad remota de todos sus usuarios a los recursos de la empresa, esto enmarcado en el ámbito de la pandemia del COVID-19, puesto que se tuvo que cambiar la ubicación geográfica del lugar de trabajo de los colaboradores, para lo que se plantea el uso de reglas de SDWAN.

Otro punto muy importante es configurar mediante las reglas del Firewall los permisos que tiene cada usuario como un tema de seguridad. Con la configuración de SDWAN se actualiza automáticamente para siempre se tome el mejor camino en la red, esta capacidad que tiene el Firewall permite que se pueda crear un proceso de identificación para permitir o bloquear el tráfico mediante los grupos de las políticas de seguridad que tiene el equipo.

A través de la simulación en GNS3, de la red propuesta por el autor, en este trabajo se concluye que las redes SDWAN permite centralizar toda la administración de los equipos en un solo lugar, además de que este tipo de redes cuentan con la capa de protección de Firewall para la seguridad ante cualquier amenaza, mejora la disponibilidad de servicio debido a que

es tolerante a fallas y por ende permite disminuir o mantener el presupuesto destinado al área de TI.

2.2. Bases Teóricas.

2.2.1. Wide Area Network WAN

Las Redes de Área Amplias llamadas en inglés WAN, permiten la conectividad entre distas redes de área local LAN y redes metropolitanas MAN; para ello se han utilizado grandes infraestructuras físicas implementadas con altos recursos económicos, que, en sus inicios, no permitían velocidades de trasmisión de datos altos, sin embargo, hoy en día, con los avances tecnológicos se ha podido lograr conectividad de extremo a extremo alcanzando velocidades muy altas y amplios anchos de banda en el tráfico de datos, no solo a través de redes cableadas sino también a través de redes inalámbricas (Sheng, Bai, & Sun, 2021).

Dentro del modelo OSI, las redes WAN trabajan en capa física que es la capa 1 y capa de enlace de datos que es la capa 2; los protocolos de la capa 1 describen los mecanismos de conexión eléctrica, mecánica y operativa en la que los datos se transmiten en su unidad de medida que es el bit, es decir 1(s) y 0(s) eléctricos; por otro lado, los protocolos de la capa de enlace del modelo OSI, detalla la forma en la que los bits son encapsulados para ser transmitidos; su unidad de medida dentro de este modelo es la trama (Sheng, Bai, & Sun, 2021).

Generalmente, las empresas públicas y privadas contratan a los proveedores de Internet (ISP) para las interconexiones que se requieren a nivel de WAN, con el objetivo lograr una comunicación entre las sucursales, matriz, servidores o cualquier servicio que se requiera y que estén separadas en diferentes ubicaciones geográficas; los costos de arrendamiento siempre van a depender del tipo de tecnología que se utilice. La calidad de

servicio y los costos son propios de cada proveedor (Sheng, Bai, & Sun, 2021).

2.2.2. Redes empresariales tradicionales

Las redes tradicionales se refieren a un esquema de conectividad centralizado y estático, en donde todas las sucursales se conectan hacia la matriz para solicitar sus recursos y servicios; y es en estas conexiones en las que se generan posibles puntos de falla como la degradación del servicio debido a latencia, jitter, paquetes perdidos y saturación de los enlaces, debido al ineficiente dimensionamiento del ancho de banda contratado el cual se ve afectado por la cantidad de usuarios y sucursales que están trabajando al mismo tiempo; todo esto será percibido por el usuario como lentitud en sus servicios (Sheng, Bai, & Sun, 2021).

Como redes tradicionales, las redes WAN requiere de una infraestructura que puede ser muy compleja y costosa, por lo que generalmente las empresas no construyen su propia infraestructura, sino que optan por el alquiler de esta a proveedores de servicios locales o internacionales. Las topologías de las redes tradicionales presentan desafíos en la actualidad que constantemente está cambiando, como el uso de velocidades más altas, servicios en la nube, entre otros, a continuación, se presenta un listado de los problemas más relevantes que tienen las redes tradicionales:

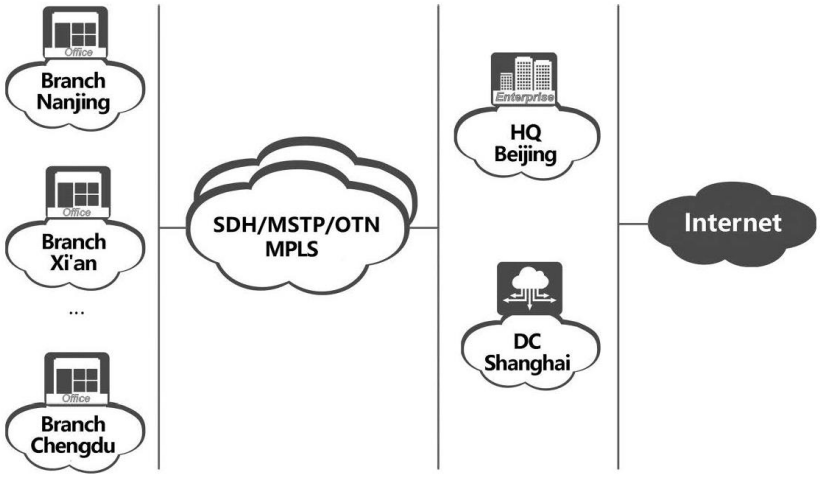
- Problema de interconexión entre servicios de nube debido a que las arquitecturas son cerradas.
- Interconexión cada vez más compleja.
- Operación y mantenimiento de redes complejas.
- Configuraciones manuales propensas a errores en las implementaciones y soluciones.

(Leng, 2021).

Para disminuir los problemas descritos anteriormente, se puede configurar parámetros como la calidad de servicio QoS que prioriza el tráfico de voz y video, considerado que al ser un tráfico en tiempo real es más susceptible a degradaciones; también se puede limitar el ancho de banda dependiendo la importancia y complejidad que demande cada usuario; es así que, los administradores de red deben encargarse de enrutar correctamente el tráfico y configurar los parámetros que se requieran para un correcto funcionamiento dentro de la red (Sheng, Bai, & Sun, 2021).

Figura 1

Esquema de una red tradicional



Nota. De *Software-Defined Wide Area Network Architectures and Technologies*, por Sheng, C., Bai, J., & Sun, Q., 2021

Para dar respuesta a la modernización de los cambios tecnológicos, con la llegada de la transformación digital, la migración de servicios en la nube, la virtualización de las redes, la descentralización de los servicios en un solo punto, la necesidad de reducir costos de operación y mantenimiento, aprovechar los recursos de ancho de banda e infraestructura de cada uno de los enlaces de datos e Internet que provee los ISP, entre otros retos, se creó la tecnología SDWAN, que se refiere a redes de área extendida definidas por software (Fordham, 2021).

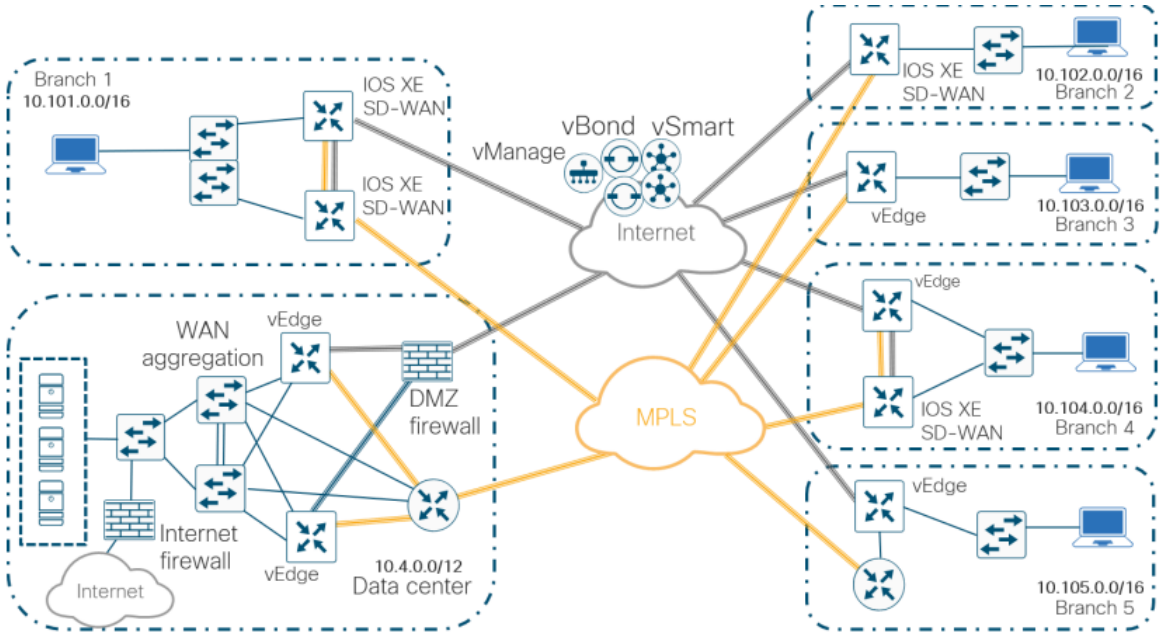
2.2.3. Software Defined Wide Area Network SDWAN

Las Redes de Área Extendida Definidas por Software, conocidas por sus siglas en inglés como redes SDWAN, son redes que interconectan a largas distancias la oficina central y las sucursales de una organización, logrando transmitir todo tipo de información, recursos y aplicaciones a través de la red (Cisco, 2019).

Con los constantes desarrollos tecnológicos, las empresas y organizaciones están migrando sus servicios, aplicaciones y su infraestructura a los servicios de la nube, como es en el caso de IaaS que es Infraestructura como servicio, SaaS que es el Software como servicio, PaaS que es la Plataforma como servicio, para ello las comunicaciones requieren tener una mayor estabilidad y una topología de red más escalable hacia todo tipo de comunicación (Cisco, 2019).

Figura 2

Redes SDWAN



Nota. De *Cisco SD-WAN End-to-End Deployment*, por Cisco, 2019.

Las redes SDWAN fueron propuestas y presentadas por primera vez en el 2014, por

parte de la ONUG (Open Networking User Gruop), en una conferencia en la que se expuso que la tecnología de las redes definidas por software por sus siglas en ingles SDN pueden ser aplicadas a las WAN empresariales, esto permite aprovechar el control centralizado de SDN, la configuración automatizada de WAN, alto nivel de capacidad de programación, entre otras ventajas (Leng, 2021).

Dentro de las definiciones que tiene SDWAN se destaca la de Gartner, empresa de consultoría y de investigación más grande del mundo que abarca todas las ramas de TI. Gartner define a la redes SDWAN como una solución que llega para evolucionar y reemplazar los equipos enrutadores que administran las WAN tradicionales, pudiendo trabajar de manera independiente a la tecnología de transporte que se esté utilizando en las WAN y permitiendo tener rutas dinámicas que se basen en políticas que gestionan múltiples conexiones de redes de áreas extendidas. En este contexto Gartner presenta tres características principales de las redes SDWAN (Leng, 2021):

- Enlaces Híbridos.
- Selección de rutas dinámicas.
- Servicios Adicionales (Leng, 2021).

Otra definición muy aceptada en la industria de las Telecomunicaciones es la de la organización sin fines de lucro que promover estándares de redes nuevas y vigentes, procedimientos, pruebas técnicas y desarrollo de servicios Ethernet, llamado MEF (Metro Ethernet Forum), que publicó el primer estándar para el servicio de SDWAN que es el MEF 70 (MEF Standard 70, 2019).

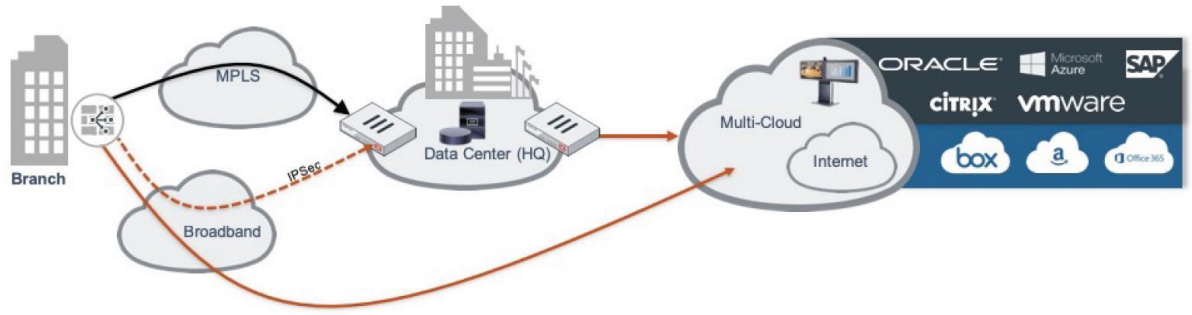
En dicho estándar se define que SDWAN es un servicio que permite la conectividad mediante el uso de políticas y aplicaciones que se basan en una red superpuesta IP, que es

independiente del método de transporte que usen las múltiples WAN y que permite la administración mediante el orquestador centralizado para dar calidad de servicio, balanceo de carga y priorización de tráfico (MEF Standard 70, 2019).

SDWAN en definitiva aprovecha las múltiples conexiones a Internet por medio de las WAN corporativas, en las que decide cual es el mejor camino o el más apropiado para aplicaciones y servicios configurados en sus reglas, con el objetivo de garantizar un correcto rendimiento y disponibilidad (Leng, 2021).

Figura 3

Arquitectura SDWAN Moderna



Nota. De *Fortinet Secure SD-WAN Reference Architecture*, por Fortinet, 2019.

2.2.4. SDWAN ADVPN

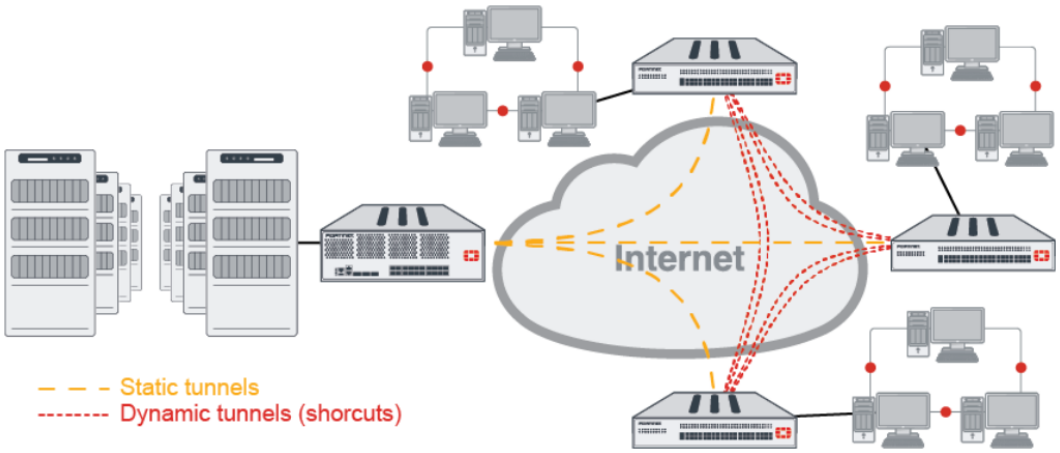
Uno de los avances tecnológicos que presenta SDWAN es la utilización de ADVPN. que son las siglas en ingles de Red Privada Virtual con Detección Automática. ADVPN es una tecnología IPsec que permite que las redes tradicionales Hub and Spoke puedan evolucionar y pasen de un modelo centralizado hacia un modelo en el que las sucursales puedan comunicarse entre sí directamente de manera dinámica y bajo demanda, mejorando el rendimiento de la red (Fortinet, 2019).

La ventaja más importante que presenta es que pasa de un esquema Hub and Spoke a

una topología en malla completa, permitiendo reducir los tiempos de conexión entre todos los puntos y que la red sea mucho más escalable que las tradicionales. Los beneficios que aporta ADVPN a SDWAN, consolida a esta tecnología como una solución segura, escalable, íntegra y que permite estar a la vanguardia de los cambios de la Transformación Digital (Fortinet, 2021).

Figura 4

SDWAN ADVPN



Nota. De *Administration Guide - 6.4.2, FortiOS, por Fortinet, 2021*

2.2.5. Herramientas de Simulación

Para el desarrollo del proyecto es necesaria la utilización de programas que permitan simular una red SDWAN ADVPN empresarial, en un entorno que tenga las herramientas adecuadas y con los equipos que se utilizarían en un proyecto de implementación, para ello se considera la aplicación de VMware como hipervisor de escritorio y GNS3 como emulador de hardware; los cuales se describen a continuación:

2.2.5.1. VMware Workstation.

VMware Workstation es un producto de VMware en su versión para escritorio, el cual

es un hipervisor que permite a los usuarios crear máquinas virtuales con los recursos que tiene la maquina física sobre la que ha sido instalado. Una VM (máquinas virtuales) contará con características de CPU, RAM, discos de almacenamiento, interfaces de red, entre otros; puede ser compatible diferentes Sistemas Operativos como Windows, Linux, M Windows, Linux, Mac OS X, OS X y macOS. (VMware, 2022).

2.2.5.2. GNS3.

El software GNS3 (Graphical Network Simulator 3) es una herramienta que permite emular diferentes topologías de red con diversas marcas de equipos; además permite configurar los equipos en un ambiente de prueba controlado y puede ser utilizado para tecnologías como SDN, NFV, Linux, etc, por lo que GNS3 ha sido de gran ayuda para el desarrollo de proyectos estudiantiles y profesionales (GNS3, 2022).

CAPÍTULO III: METODOLOGÍA

3.1. Tipo de Investigación

SDWAN es una tecnología que permite el desarrollo empresarial a gran escala ya que simplifica la comunicación entre todas las sedes y servicios de una organización mediante la administración inteligente de las WAN, esto ayuda a que cumplan una de las metas para estar a la vanguardia de la transformación digital. La presente investigación no generará nuevos conceptos teóricos ni definiciones, sino que entregara una propuesta practica para las soluciones que se pueden ofrecer a empresas corporativas y gubernamentales, mediante el uso de redes de área extendida definidas por software con ADVPN; por tanto, el tipo de investigación es cualitativa ya que permite proporcionar información de un tema específico tal manera de estudio de casos (Echaverría, 1999).

Dentro del tipo de investigación Cualitativo se encuentra el método aplicado que permite resolver problemas que aquejan a una parte de la sociedad en el sector productivo, generando un conocimiento práctico y mejorando los procesos en el espacio de la tecnología. La técnica de investigación apropiada para el desarrollo del presente trabajo es la técnica de observación a través de la cual se analizará el objeto de estudio y se plantearán las ventajas de utilizar una nueva tecnología para la optimización de recursos en las organizaciones que aún mantienen instaladas y operando redes tradicionales (Echaverría, 1999).

3.2. Diseño de Investigación

Para el presente proyecto, cuyo objetivo principal es la simulación de una red SDWAN ADVPN, se realiza el diseño de investigación que señala las actividades principales para alcanzar el objetivo, estas son:

1) Exponer los fundamentos teóricos de las redes tradicionales y la migración hacia redes WAN definidas por software en las organizaciones.

2) Identificación de herramientas de software para la simulación del proyecto.

3) Análisis de los componentes y equipamientos necesarios para el diseño de una red SDWAN ADVPN.

4) Diseño de un esquema de red SDWAN ADVPN para ser simulado.

5) Simulación de una red SDWAN ADVPN.

6) Análisis y presentación de resultados.

(Echaverría, 1999)

3.3. Técnicas e instrumentos de recolección de datos

Considerando el enfoque cualitativo por el que se ha optado para el desarrollo del trabajo, es la aplicación de la técnica documental la que permitirá seleccionar información de documentos, libros y revistas científicas, a través de la cual se podrá plantar la solución y definir los componentes que se requieren para ello, y será el input necesario para el análisis de las características y ventajas de la propuesta, en contraste con las redes tradicionales (Echaverría, 1999).

Adicionalmente, con la técnica documental se logrará determinar las herramientas de software óptimas que permiten generar una simulación de un entorno de red empresarial real, en el que se pueda identificar requisitos técnicos y configuración para el desarrollo del proyecto (Echaverría, 1999).

3.4. Técnica de Análisis de Datos

Un estudio de tipo cualitativo proporciona datos de tipo descriptivo, por lo que el análisis se basará en la organización de la información obtenida relacionada a los fabricantes de equipos con tecnología SDWAN, tal como, especificaciones técnicas de equipos, tipos de tecnologías que utilizan, tipos de conexión y las especificaciones de modelos y configuración que se requiere para simular este proyecto. Adicionalmente, se realiza consultas bibliográficas de varios autores con el objetivo de identificar la estructura de la topología física y lógica para el desarrollo de redes empresariales en el que se busca identificar los fundamentos teóricos de la tecnología SDWAN, así como sus ventajas al momento de implementar en las nuevas redes de datos como parte del desarrollo y modernización de las telecomunicaciones (Echaverría, 1999).

CAPÍTULO IV: PRESENTACIÓN DE LA PROPUESTA

4.1. Introducción

Para el desarrollo del proyecto, se maneja GNS3 como emulador de hardware de todos los dispositivos a utilizar, el cual permite tener un ambiente realista del proceso de configuración y desarrollo. Para la configuración SDWAN ADVPN se seleccionan las máquinas virtuales marca Fortinet, las cuales están disponibles en la plataforma de Forticloud de manera libre.

De manera general, la propuesta se desarrolla con cuatro pasos; como primer paso se realiza el diseño de una red con un modelo Hub and Spoke compuesto por un equipo matriz y dos sucursales; como segundo paso se instala las VMs y los componentes de red en GNS3; el tercer paso consiste en configurar los equipos Fortigate para finalmente realizar las pruebas de funcionamiento.

4.2. Topología de red

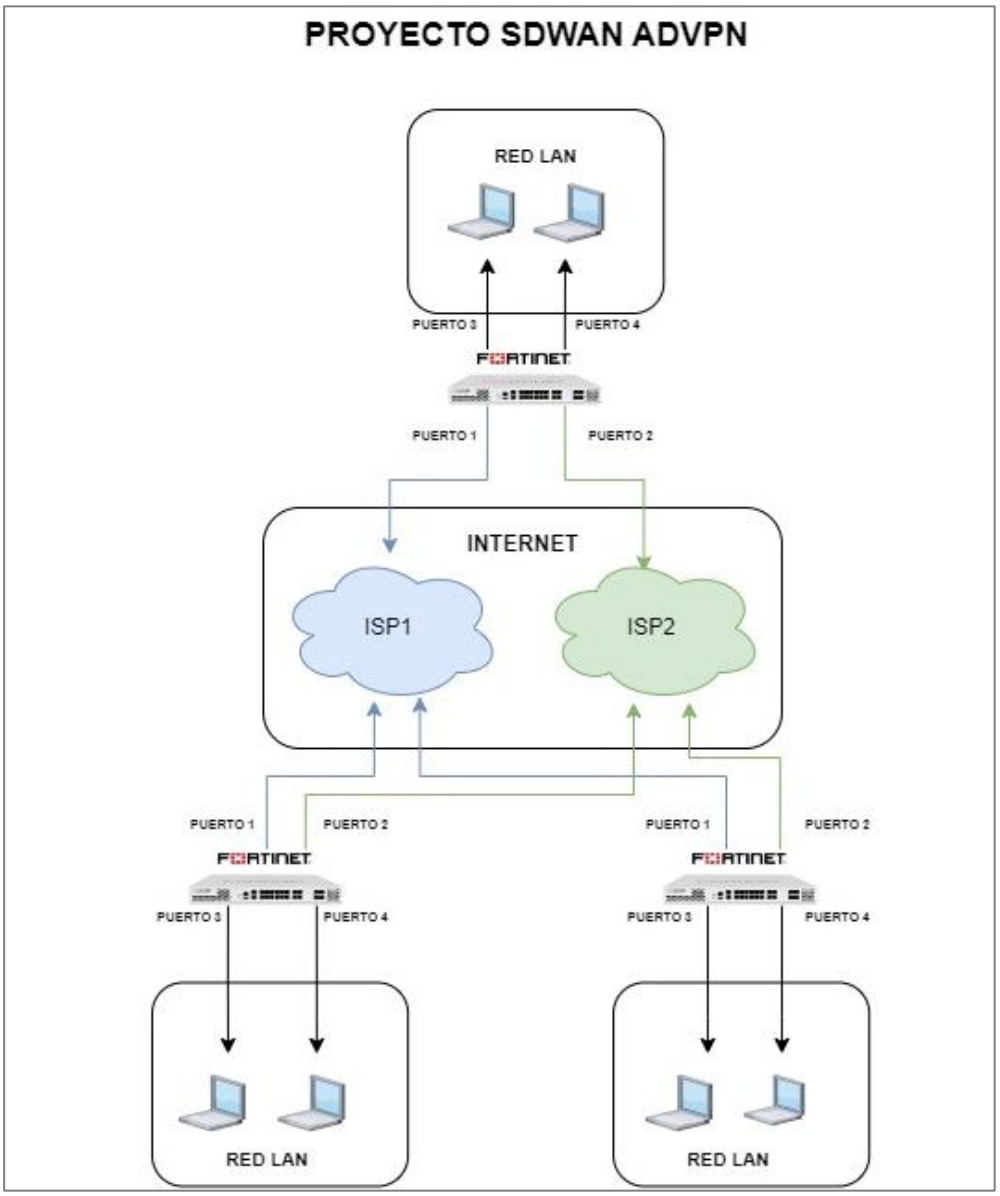
La topología de red de propuesta está compuesta de 3 equipos Fortinet, de los cuales dos son las sucursales y un equipo es la matriz, en donde las empresas ubican los servidores y servicios para toda la red. Para este proyecto, se ha dimensionado que tenga dos salidas a Internet, es decir, tiene dos proveedores de servicio de Internet que estarán identificados como ISP1 e ISP2, estos permitirán que cada sucursal o matriz tenga redundancia en su comunicación interna y hacia Matriz, con ello se garantiza la alta disponibilidad en la conectividad de los servicios, ya que, si un proveedor pierde su comunicación, todo el tráfico podrá ser enrutado hacia el segundo proveedor, permitiendo que el flujo de datos sea continuo.

Para la validación del correcto funcionamiento se ha colocado dos equipos finales, el

primero permitirá las pruebas de conectividad y el segundo la navegación hacia Internet.

Figura 5

Topología general de red propuesta



4.3. Descripción de Puertos

Para la implementación del proyecto, en la Tabla 1 se describe las interfaces utilizadas:

Tabla 1

Lista de interfaces equipos Fortigate

	FORTIGATE MATRIZ	FORTIGATE GYE	FORTIGATE LOJA
ISP1	192.168.50.200	192.168.50.210	192.168.50.220
ISP2	192.168.121.4	192.168.121.6	192.168.121.8
ADVPN1	172.16.100.1	172.16.100.254	172.16.100.253
ADVPN2:	172.16.200.1	172.16.200.254	172.16.200.253
LAN	10.10.100.0/24	10.10.150.0/24	10.10.200.0/24
Loopback	14.14.14.1	-	-

4.4. Simulación de la red SDWAN ADVPN

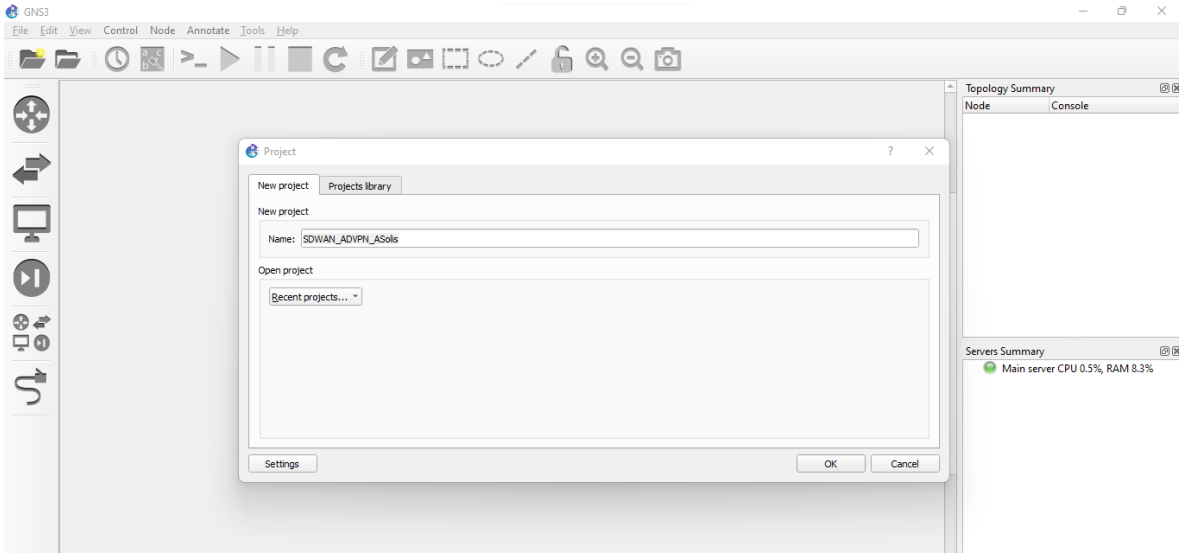
Para la simulación del proyecto, previamente se debe instalar un hipervisor de escritorio, el cual permite que se desplieguen máquinas virtuales sobre él; en este caso se utiliza VMware Workstation. El emulador seleccionado es el GNS3 (Simulador de Graficas de Red) y, adicionalmente, se utiliza imágenes oficiales de máquinas virtuales de equipos Fortinet que fueron descargadas de la plataforma Forticloud como se detalla en el Anexo I.

A continuación, se detalla el procedimiento realizado:

- Se crea un nuevo proyecto dentro de GNS3 llamado SDWAN_ADVPN_ASolis:

Figura 6

Ventana de creación un nuevo proyecto en GNS3

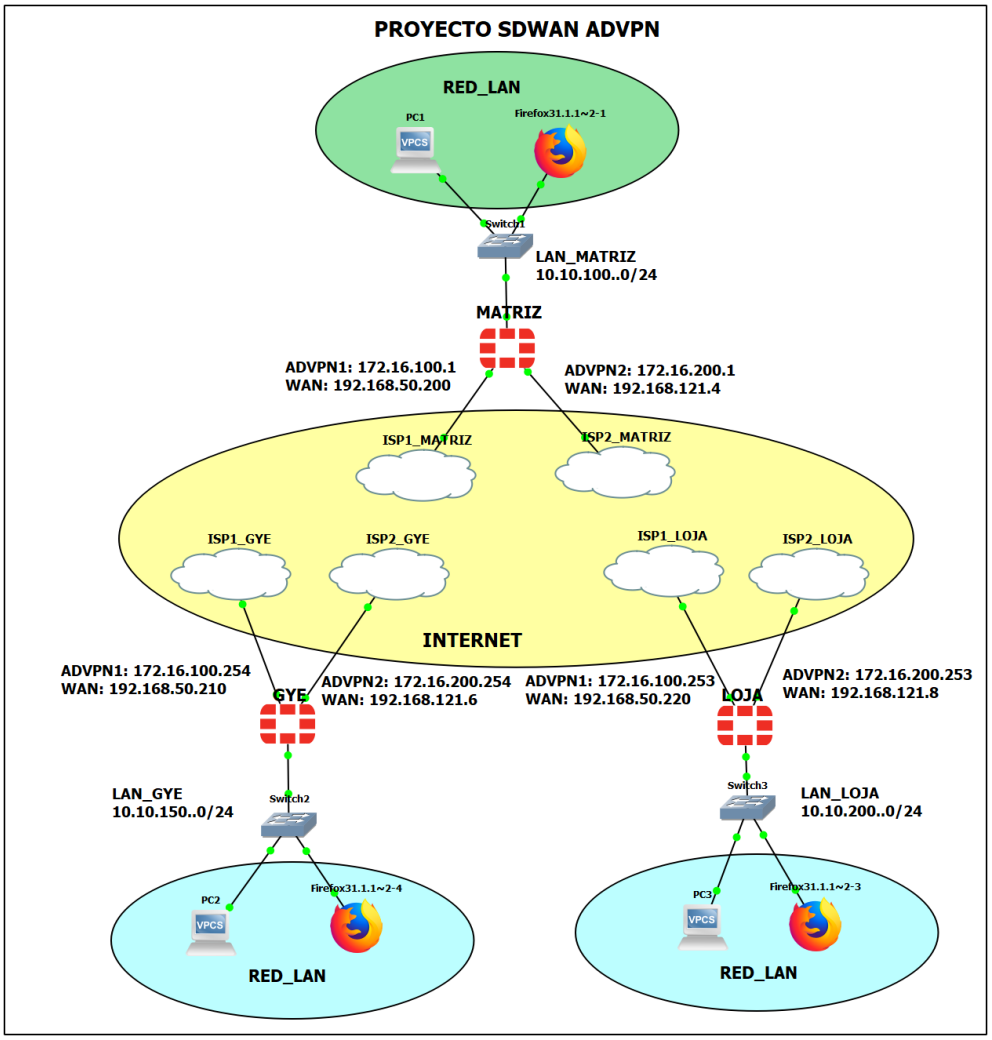


- Para la topología propuesta, se agregan los siguientes equipos en el emulador GNS3:

    - 1 equipo Fortigate Matriz.
    - 2 equipos Fortigate para las sucursales de Guayaquil, Loja.
    - 3 quipos PC´s, una para cada equipo Fortinet que representarán la red LAN.
    - 3 imágenes del navegador Mozila Firefox para validar la navegación de Internet en la LAN.

Figura 7

Topología detallada de la red propuesta



4.5. Configuraciones equipos Fortigate

A continuación, se presenta las configuraciones de los equipos Fortigates en Matriz y las sucursales:

4.5.1. Configuración Base de Equipos Fortigates

4.5.1.1. Fortigate Matriz.

Como parte de las configuraciones base se establece el puerto de la ISP1, ISP2 y el puerto LAN:

- Puerto1: ISP1 = 192.168.50.200
- Puerto2: ISP2 = 192.168.121.4
- Puerto3: LAN_MATRIZ= 10.10.100.1/24

Figura 8

Configuración Fortigate MATRIZ

```
MATRIZ # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.50.200 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP1"
        set alias "ISP1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.121.4 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP2"
        set alias "ISP2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 10.10.100.1 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "LAN_MATRIZ"
        set alias "LAN_MATRIZ"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 3
    next
```

4.5.1.2. Fortigate Guayaquil (GYE).

Como se especifica tanto la Matriz como las sucursales tienen dos proveedores de servicio de Internet descrito de la siguiente manera:

- Puerto1: ISP1 = 192.168.50.210
- Puerto2: ISP2 = 192.168.121.6
- Puerto3: LAN_GYE= 10.10.150.1/24

Figura 9

Configuración Fortigate GYE

```
GYE # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.50.210 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP1"
        set alias "ISP1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.121.6 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP2"
        set alias "ISP2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 10.10.150.1 255.255.255.0
        set allowaccess ping
        set type physical
        set description "LAN_GYE"
        set alias "LAN_GYE"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 3
    next
```

4.5.1.3. Fortigate Loja.

Para la sucursal de Loja se estable los siguientes puertos WAN y LAN:

- Puerto1: ISP1 = 192.168.50.220
- Puerto2: ISP2 = 192.168.121.8
- Puerto3: LAN_LOJA= 10.10.200.1/24

Figura 10

Configuración Fortigate LOJA

```
LOJA # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.50.220 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP1"
        set alias "ISP1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.121.8 255.255.255.0
        set allowaccess ping https http
        set type physical
        set description "ISP2"
        set alias "ISP2"
        set lldp-reception enable
        set role wan
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 10.10.200.1 255.255.255.0
        set allowaccess ping
        set type physical
        set description "LAN_LOJA"
        set alias "LAN_LOJA"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 3
    next
```

4.5.2. Configuración ADVPN

Para establecer las comunicaciones dinámicas por túneles directos con ADVPN entre las sucursales y Matriz, se debe configurar en cada equipo dos túneles IPsec que cifran y

autentican la información de extremo a extremo permitiendo que el tráfico viaje de manera segura; para ello se establece dos fases en el túnel IPsec, la Fase 1 permite establecer la autenticación entre los pares, así como la negoción de los parámetros de criptografía y claves de inicio de sesión, la Fase 2 es la negociación del túnel IPsec para el tráfico que fluirá por los túneles con base en las claves proporcionadas en la Fase 1; las dos fases se configuran para cada enlace de Internet que proporcionan los ISP´s.

4.5.2.1. Fortigate Matriz.

Como parte de la Fase 1 se establecen los siguientes parámetros:

- Tipo de interfaz
- Interfaz a la que se establece la VPN
- Tipo de par para la conexión.
- Dispositivo Kernel para los túneles.
- Tipo de cifrado para los túneles.
- Habilitación de envío de mensajes de accesos directo para la detección automática de los túneles.
- Habilitación del siguiente salto de túnel.
- Clave de secreta para el cifrado de los túneles.
- Intervalo de detección de pares.

Figura 11

Configuración ADVPN - Fortigate MATRIZ Fase 1

```
MATRIZ # sh vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "ADVPN_1"
        set type dynamic
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set psksecret ENC CqlpuqlOXltHr4oXlhPx/DOQdlp7/emg2WjqS7VGYbDrCy
xWaLlirlqXcL8CdByUpJ/TAJBKUX5Fd6qRAqcXeD+IvRJNgrsrX+tQ6w==
        set dpd-retryinterval 60
    next
    edit "ADVPN_2"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set psksecret ENC MGNyQcCW7WM/wLVQ717B/AuYOjb+UmKRRRDlN91JsdjQF9
hxdIRsgM+hRcdAHgogrI0jj9qZfi9yZ+DQcH/BYtP0/YItXcAfc/Xsxg==
        set dpd-retryinterval 60
    next
end
```

Para la configuración de la Fase 2 se establecen los siguientes parámetros:

- Se crea la Fase 2 con el nombre del túnel.
- La Fase 1 determina las opciones requeridas para la Fase 2.
- Tipo de cifrado para los túneles.

Figura 12

Configuración ADVPN - Fortigate MATRIZ Fase 2

```
MATRIZ # sh vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "ADVPN_1"
        set phaselname "ADVPN_1"
        set proposal des-sha256
    next
    edit "ADVPN_2"
        set phaselname "ADVPN_2"
        set proposal des-sha256
    next
end
```

4.5.2.2. Fortigate GYE y LOJA.

Para la configuración de la Fase 1 en el establecimiento de los túneles dinámicos ADVPN se establecen los siguientes parámetros:

- Tipo de Interfaz
- Interfaz a la que se establece la VPN.
- Tipo de par para la conexión.
- Dispositivo Kernel para los túneles.
- Tipo de cifrado para los túneles.
- Habilitación de recepción de mensajes de accesos directo para la detección automática de los túneles.
- Habilitación del siguiente salto de túnel.
- Determinación del Gateway remoto, es decir la IP WAN del Hub.
- Clave de secreta para el cifrado de los túneles.

Figura 13

Configuración ADVPN - Fortigate GYE Fase 1

```
GYE # sh vpn ipsec phasel-interface
config vpn ipsec phasel-interface
    edit "ADVPN_1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set auto-discovery-receiver enable
        set remote-gw 192.168.50.200
        set tunnel-search nexthop
        set psksecret ENC PTUl3GdPqQb6PmyTbEz4xVEej+HbOWAI2
JsHB8GrgFGJGEzlT6X2ig04JH7FFl6F8nwalrjUKqBFlzdgfDQpMOeRw==
    next
    edit "ADVPN_2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set remote-gw 192.168.121.4
        set tunnel-search nexthop
        set psksecret ENC lqLrDPccmZ3FTcBFjJ38aEOPlbsDV56yn
vA+3+530WOi5li/lZnoBim9TxcrBU6YhI/fhYIfdYLtsySKjoZzvyuzw==
    next
end
```

Figura 14

Configuración ADVPN - Fortigate LOJA Fase 1

```
LOJA # sh vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "ADVPN_1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set remote-gw 192.168.50.200
        set tunnel-search nexthop
        set psksecret ENC WrWg2ekcy7Lod+qeSz9Ml47v22ON18tY7S
ycnuFxjjrifcWHhK8U4V0vuyUNgXtLqEWbYNV1DLEeBbK1w3X0c1Jaow==
    next
    edit "ADVPN_2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-sha256
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set remote-gw 192.168.121.4
        set tunnel-search nexthop
        set psksecret ENC aw5FU7cjIDIltvepYn6Dd07AD43B8TO9Dj
A4Kk6JP64QcP8UyM65Mftiut4O8Fj54nbRwbaMp9MrKbIqW6bXmrkmmQ==
    next
end
```

Para la configuración de la Fase 2 en las sucursales se establecen los siguientes parámetros:

- Se crea la Fase 2 con el nombre del túnel.
- La Fase 1 determina las opciones requeridas para la Fase 2.
- Tipo de cifrado para los túneles.

Figura 15

Configuración ADVPN - Fortigate GYE Fase 2

```
GYE # sh vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "ADVPN_1"
        set phaselname "ADVPN_1"
        set proposal des-sha256
    next
    edit "ADVPN_2"
        set phaselname "ADVPN_2"
        set proposal des-sha256
    next
end
```

Figura 16

Configuración ADVPN - Fortigate LOJA Fase 2

```
LOJA # sh vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "ADVPN_1"
        set phaselname "ADVPN_1"
        set proposal des-sha256
    next
    edit "ADVPN_2"
        set phaselname "ADVPN_2"
        set proposal des-sha256
    next
end
```

4.5.3. Configuración BGP

El protocolo BGP (Protocolo de puerta de enlace de Frontera) permite intercambiar información del enrutamiento hacia todos los miembros que tengan el mismo sistema autónomo permitiendo tener una topología de malla, cada equipo se configura vecinos uno por cada ISP, además se propagar la red LAN de cada punto.

4.5.3.1. Fortigate Matriz.

En matriz se configura una interfaz adicional llamada Loopback con la IP 14.14.14.1/32, que permite a las sucursales censar constantemente los túneles ADVPN para

validar si están o no con servicio, con lo cual las sucursales podrán establecer las prioridades en los regalas de conmutación o preferencia del SDWAN:

Figura 17

Configuración Interfaz Loopback - Fortigate MATRIZ

```
MATRIZ # sh system interface Loopback
config system interface
    edit "Loopback"
        set vdom "root"
        set ip 14.14.14.1 255.255.255.255
        set allowaccess ping
        set type loopback
        set role lan
        set snmp-index 15
    next
end
```

Para BGP en Matriz se configura los siguientes parámetros:

- Se configura el sistema autónomo
- Se da un identificativo al Router
- Se habilita ibgp-multipath para permitir la instalación de multiples rutas BGP hacia el mismo destino, en las tablas de enrutamiento.
- Se habilita la selección de rutas adicionales IPv4 BGP.
- Se crean 2 grupos de vecinos para cada uno de los túneles ADVPN1 y ADVPN2.
- Se configura las redes de cada túnel:
    - ADVPN1: 172.16.100.0 255.255.255.0
    - ADVPN2: 172.16.200.0 255.255.255.0
- Se configura la red LAN de Matriz y la Loopback:
    - Red LAN: 10.10.100.0 255.255.255.0
    - Loopback: 14.14.14.1 255.255.255.255

Figura 18

Configuración BGP - Fortigate MATRIZ

```
MATRIZ # sh router bgp
config router bgp
    set as 65501
    set router-id 172.16.100.1
    set ibgp-multipath enable
    set additional-path enable
    config neighbor-group
        edit "ADVPN_1"
            set remote-as 65501
            set route-reflector-client enable
        next
        edit "ADVPN_2"
            set remote-as 65501
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 172.16.100.0 255.255.255.0
            set neighbor-group "ADVPN_1"
        next
        edit 2
            set prefix 172.16.200.0 255.255.255.0
            set neighbor-group "ADVPN_2"
        next
    end
    config network
        edit 1
            set prefix 10.10.100.0 255.255.255.0
        next
        edit 2
            set prefix 14.14.14.1 255.255.255.255
        next
    end
```

4.5.3.2. Fortigate GYE y LOJA.

En cada una de las sucursales se configura la red LAN de cada punto y dos vecinos hacia Matriz; a continuación, se describe los parámetros configurados:

- Se configura el sistema autónomo para BGP.
- Se da un identificativo al Router.
- Se configura los dos vecinos hacia Matriz:
    - 172.16.100.1

- 172.16.200.1

- Se configura la red LAN de Matriz y la Loopback:
  - Red LAN: 10.10.150.0 255.255.255.0

Figura 19

Configuración BGP - Fortigate GYE

```
GYE # sh router bgp
config router bgp
    set as 65501
    set router-id 172.16.100.254
    config neighbor
        edit "172.16.100.1"
            set remote-as 65501
        next
        edit "172.16.200.1"
            set remote-as 65501
        next
    end
    config network
        edit 1
            set prefix 10.10.150.0 255.255.255.0
        next
    end
```

Figura 20

Configuración BGP - Fortigate LOJA

```
LOJA # sh router bgp
config router bgp
    set as 65501
    set router-id 172.16.100.253
    config neighbor
        edit "172.16.100.1"
            set remote-as 65501
        next
        edit "172.16.200.1"
            set remote-as 65501
        next
    end
    config network
        edit 1
            set prefix 10.10.200.0 255.255.255.0
        next
    end
```

4.5.4. Configuración SDWAN

4.5.4.1. Fortigate Matriz.

Para la configuración de Matriz se debe agregar los miembros que van a formar parte del SDWAN, para ello se agrupa en la interfaz virtual llamada virtual-wan-link las interfaces virtuales ADVPN1 y ADVPN2 en una sola zona como se muestra en la Figura 21:

- Zona virtual-wan-link:
    - ADVPN1
    - ADVPN2

Figura 21

Configuración SDWAN - Fortigate MATRIZ

```
MATRIZ (sdwan) # show
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 3
            set interface "ADVPN_1"
        next
        edit 4
            set interface "ADVPN_2"
        next
    end
```

Luego, se crea la regla SDWAN que permite que el tráfico de Matriz pueda llegar a cada una de las sucursales, para ello se indica que la primera prioridad sea por la interfaz virtual ADVPN1 y en caso de falla conmute por la interfaz virtual ADVPN; a continuación, se presenta en la configuración a través de formato CLI (Figura 22) y GUI (Figura 23):

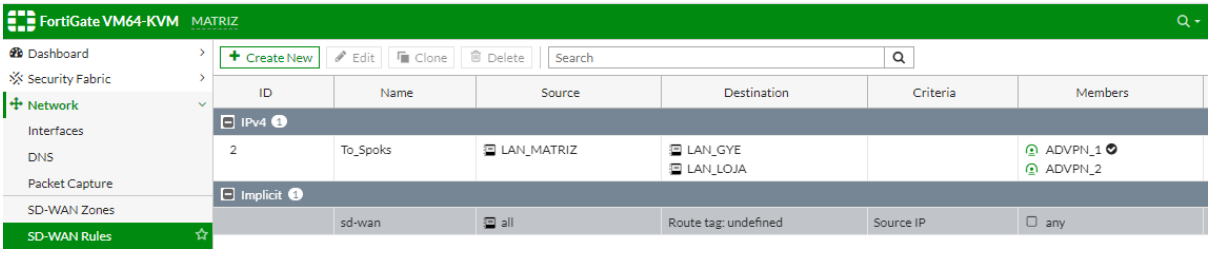
Figura 22

Creación de regla SDWAN CLI - MATRIZ

```
    config service
        edit 2
            set name "To_Spoks"
            set dst "LAN_GYE" "LAN_LOJA"
            set src "LAN_MATRIZ"
            set priority-members 3 4
        next
    end
end
```

Figura 23

Creación de regla SDWAN GUI - MATRIZ



4.5.4.2. Fortigate GYE y LOJA.

Para la configuración de SDWAN en las sucursales es necesario agrupar en la misma zona de la interfaz virtual a las dos interfaces físicas, en las que se identifica el Gateway de cada uno de los dos proveedores de servicios y las dos interfaces de los túneles ADVPN1 y ADVPN2.

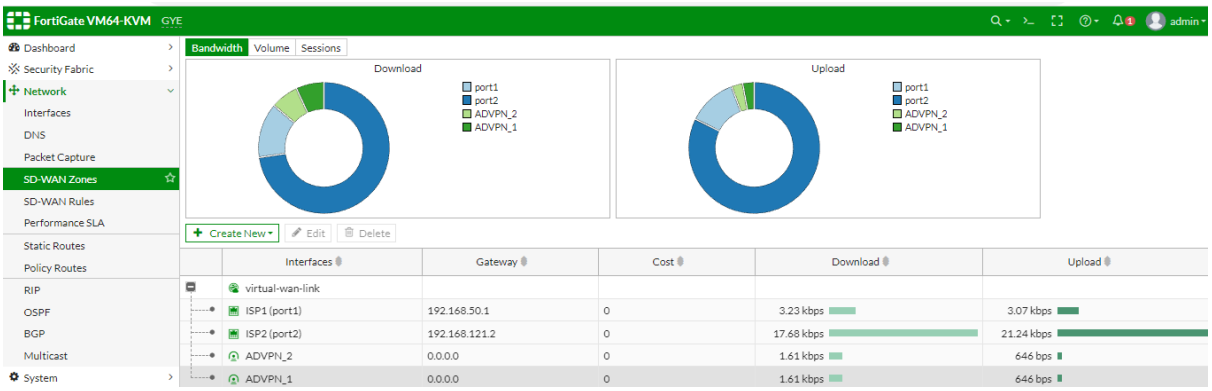
Figura 24

Agrupación de interfaces en la zona SDWAN CLI- Fortigate GYE

```
GYE # sh system sdwan
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port1"
            set gateway 192.168.50.1
        next
        edit 2
            set interface "port2"
            set gateway 192.168.121.2
        next
        edit 4
            set interface "ADVPN_2"
        next
        edit 5
            set interface "ADVPN_1"
        next
    end
```

Figura 25

Agrupación de interfaces en la zona SDWAN GUI- Fortigate GYE



Para crear las reglas de SDWAN, primero se debe generar un SLA (Acuerdo de Nivel de Servicio) en el cual se especifique un destino específico con el que cada interfaz mantenga un ping constante mediante el protocolo ICMP y se pueda identificar cuando un servicio este caído y se deba conmutar de manera automática hacia el otro proveedor; se describe a continuación el SLA para Internet y el SLA para la conexión de los túneles ADVPN hacia

Matriz:

SLA hacia Internet: se especifica como servidor destino al DNS de Google 8.8.8.8 en el cual las dos interfaces físicas ISP1 e ISP2 estarán censando constantemente por ICMP el destino, para ello se especificará que para que conmute de un proveedor al otro se debe tener una pérdida del 10% de paquetes en un intervalo de 500 milisegundos por 5 veces consecutivas y, para restaurar la comunicación por el ISP inicial se debe validar por 5 veces el mismo intervalo.

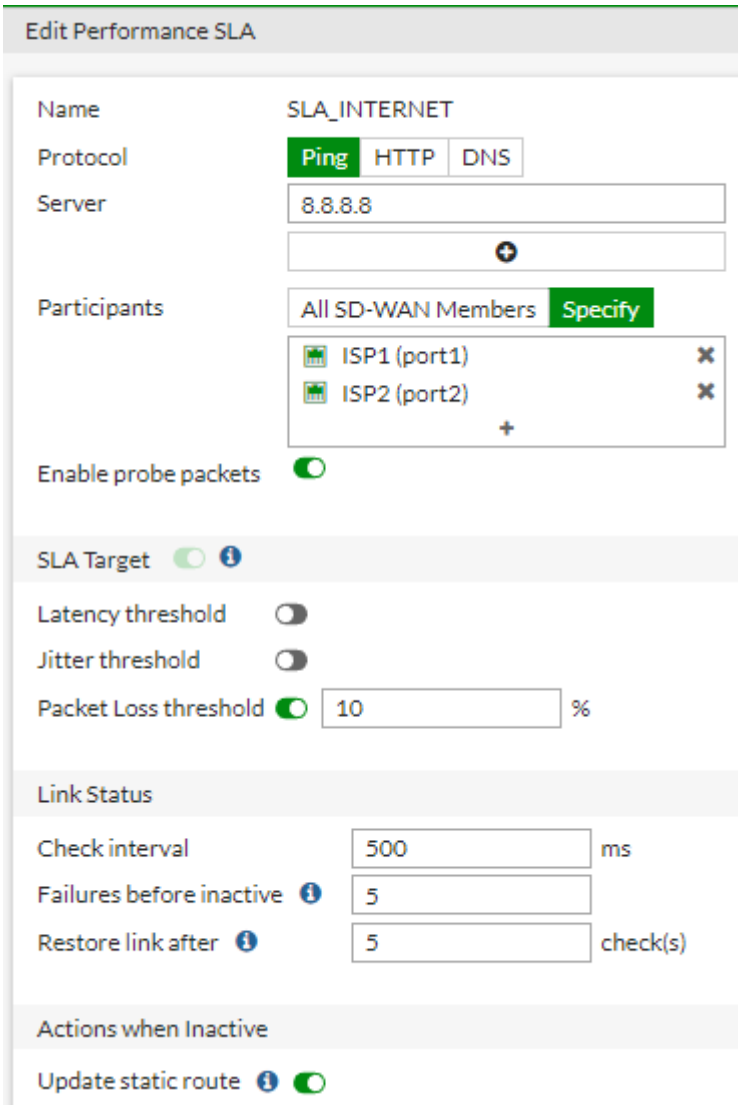
Figura 26

Configuración SLA hacia internet CLI

```
config health-check
    edit "SLA_INTERNET"
        set server "8.8.8.8"
        set members 1 2
        config sla
            edit 1
                set link-cost-factor packet-loss
                set packetloss-threshold 10
            next
        end
    next
```

Figura 27

Configuración SLA hacia internet CLI



SLA VPN: se configura con las dos interfaces lógicas ADVPN1 y ADVPN2 con destino hacia la interfaz Loopback 14.14.14.1, creada en Matriz con el objetivo de validar que cada uno de los túneles estén operativos; como en el caso anterior, se especifica el SLA con un umbral del 10% de perdida de paquetes para conmutar al siguiente proveedor en caso de falla de servicio, esta configuración se la realiza en las dos sucursales.

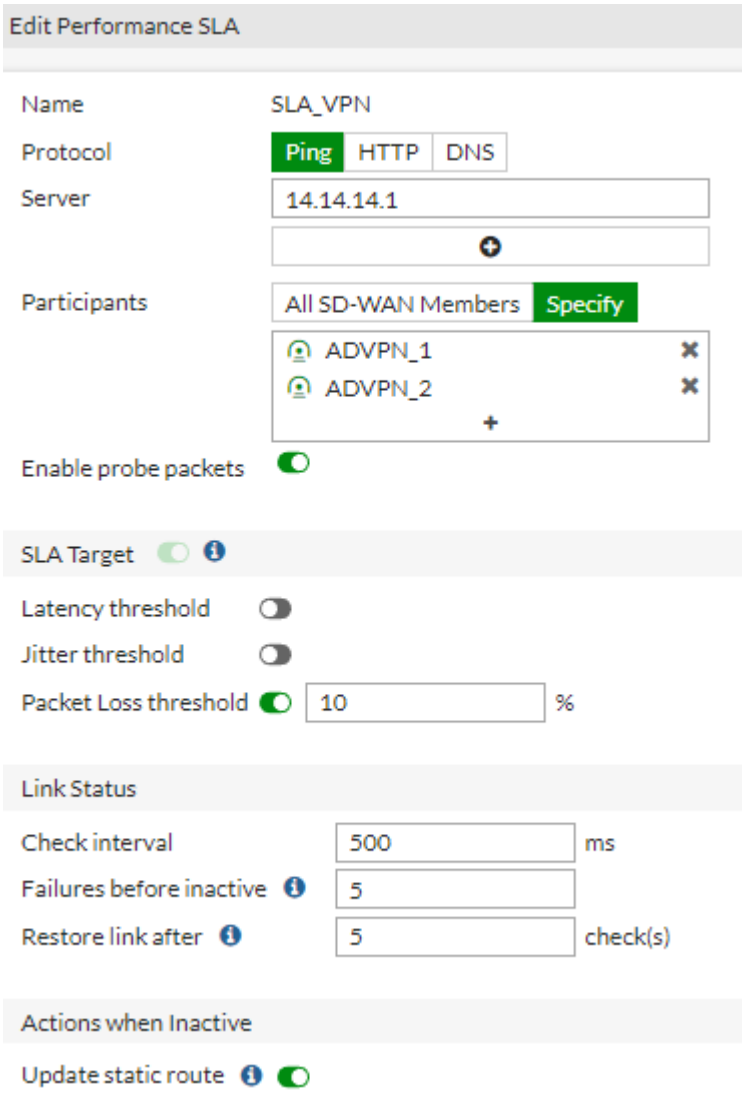
Figura 28

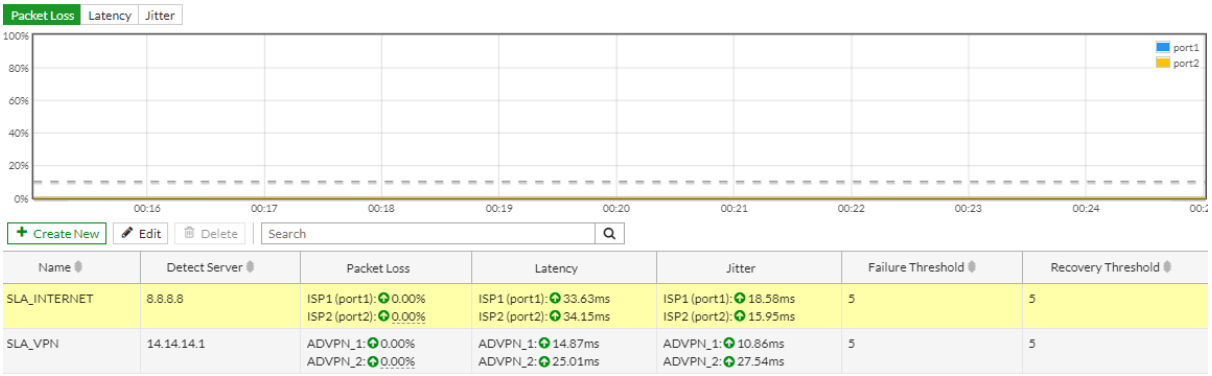
Configuración SLA VPN CLI

```
    edit "SLA_VPN"
        set server "14.14.14.1"
        set members 4 5
        config sla
            edit 1
                set link-cost-factor packet-loss
                set packetloss-threshold 10
            next
        end
    next
end
```

Figura 29

Configuración SLA VPN GUI





Finalmente se debe crear las reglas de SDWAN para que se especifique la ruta prioritaria para el envío de tráfico:

- Regla SDWAN hacia Matriz: se configura con el SLA hacia la Loopback; se va a permitir que el tráfico de la red LAN de las sucursales tengan como destino Matriz y su sucursal vecina, se especifica como ruta prioritaria el ADVPN1 y luego el ADVPN2 (Figura 30).
- Regla SDWAN hacia Internet; permite que todo el tráfico de navegación de la red LAN de las sucursales tenga como destino Internet y se coloca como prioridad el ISP2 y como secundario el ISP1 (Figura 31):

Figura 30

Regla SDWAN hacia MATRIZ CLI

```
    config service
        edit 1
            set name "TO_MATRIZ"
            set mode sla
            set dst "LAN_LOJA" "LAN_MATRIZ" "LOOPBACK"
            set src "LAN_GYE"
            config sla
                edit "SLA_VPN"
                    set id 1
                next
            end
            set priority-members 5 4
        next
        edit 2
            set name "TO_INTERNET"
            set mode sla
            set dst "all"
            set src "LAN_GYE"
            config sla
                edit "SLA_INTERNET"
                    set id 1
                next
            end
            set priority-members 2 1
        next
    end
end
```

Figura 31

Regla SDWAN hacia MATRIZ GUI

IPv4 2					
1	TO_MATRIZ	LAN_GYE	LAN_LOJA LAN_MATRIZ LOOPBACK	SLA	ADVPN_1 ADVPN_2
2	TO_INTERNET	LAN_GYE	all	SLA	ISP2 (port2) ISP1 (port1)
Implicit 1					
	sd-wan	all	Route tag: undefined	Source IP	any

Figura 32

Regla SDWAN hacia Internet CLI

```
    config service
        edit 3
            set name "TO_MATRIZ"
            set mode sla
            set dst "LAN_GYE" "LAN_MATRIZ" "LOOPBACK"
            set src "LAN_LOJA"
            config sla
                edit "TO_MATRIZ"
                    set id 1
                next
            end
            set priority-members 3 4
        next
        edit 2
            set name "TO_INTERNET"
            set mode sla
            set dst "all"
            set src "LAN_LOJA"
            config sla
                edit "SLA_INTERNET"
                    set id 1
                next
            end
            set priority-members 2 1
        next
    end
end
```

Figura 33

Regla SDWAN hacia Internet GUI

IPv4 2

3	TO_MATRIZ	LAN_LOJA	LAN_GYE LAN_MATRIZ LOOPBACK	SLA	ADVPN_1 ADVPN_2
2	TO_INTERNET	LAN_LOJA	all	SLA	ISP2 (port2) ISP1 (port1)

4.5.5. Configuración Firewall Policy

4.5.5.1. Fortigate Matriz.

Para la configuración de las políticas de Firewall en Matriz es muy importante conocer que estas son jerárquicas, es decir, se ejecutan de manera descendente, por lo que se debe validar que estén colocadas de manera correcta, a continuación, se detalla las políticas configuradas:

- Matriz_Sucursales:
    - From: LAN_Matriz.
    - To: virtual-wan-link.
    - Source: LAN_Matriz
    - Destination: LAN_GYE, LAN_LOJA.
    - Service: All
- Sucursales_Matriz:
    - From: virtual-wan-link.
    - To: LAN_Matriz.
    - Source: LAN_GYE, LAN_LOJA.
    - Destination: LAN_Matriz
    - Service: All
- LAN_LAN:
    - From: virtual-wan-link.
    - To: virtual-wan-link.
    - Source: LAN_GYE, LAN_LOJA.
    - Destination: LAN_GYE, LAN_LOJA.
    - Service: All.
- VPN_LOOPBACK:
    - From: virtual-wan-link.
    - To: Loopback
    - Source: LAN_GYE, LAN_LOJA, ADVPN1, ADVPN2.
    - Destination: Loopback address
    - Service: All.

- LAN_MATRIZ-INTERNET_ISP1:
    - From: LAN_MATRIZ
    - To: ISP1
    - Source: LAN_MATRIZ
    - Destination: all
    - Service: All.
    - NAT: Enable.
- LAN_MATRIZ-INTERNET_ISP2:
    - From: LAN_MATRIZ
    - To: ISP2
    - Source: LAN_MATRIZ
    - Destination: all
    - Service: All.
    - NAT: Enable.

Figura 34

Configuración Firewall Policy Matriz

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
MATRIZ_SUCURSALES	LAN_MATRIZ (port3)	virtual-wan-link	LAN_MATRIZ	LAN_GYE LAN_LOJA	always	ALL	ACCEPT	Disabled
SUCURSALES_MATRIZ	virtual-wan-link	LAN_MATRIZ (port3)	LAN_GYE LAN_LOJA	LAN_MATRIZ	always	ALL	ACCEPT	Disabled
LAN_LAN	virtual-wan-link	virtual-wan-link	LAN_GYE LAN_LOJA	LAN_GYE LAN_LOJA	always	ALL	ACCEPT	Disabled
VPN_LOOPBACK	virtual-wan-link	Loopback	LAN_GYE LAN_LOJA ADVPN1 ADVPN2	Loopback address	always	ALL	ACCEPT	Disabled
LAN_MATRIZ - INTERNET_ISP1	LAN_MATRIZ (port3)	ISP1 (port1)	LAN_MATRIZ	all	always	ALL	ACCEPT	Enabled
LAN_MATRIZ - INTERNET_ISP2	LAN_MATRIZ (port3)	ISP2 (port2)	LAN_MATRIZ	all	always	ALL	ACCEPT	Enabled

4.5.5.2. Fortigate GYE y LOJA.

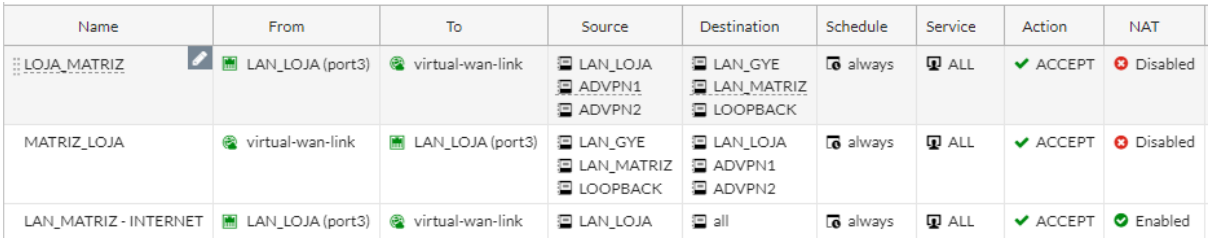
Las configuraciones de las políticas de Firewall para las sucursales usan la interfaz

virtual SDWAN en la que tiene como miembros las dos interfaces físicas y los túneles ADVPN; a continuación, se detallan las políticas configuradas en cada sucursal:

- LOJA_MATRIZ
    - From: LAN_LOJA
    - To: virtual-wan-link.
    - Source: LAN_LOJA, ADVPN1, ADVPN2.
    - Destination: LAN_GYE, LAN_MATRIZ, LOOPBACK.
    - Service: All.
- MATRIZ_LOJA
    - From: virtual-wan-link.
    - To: LAN_LOJA.
    - Source: LAN_GYE, LAN_MATRIZ, LOOPBACK.
    - Destination: LAN_LOJA, ADVPN1, ADVPN2.
    - Service: All.
- LAN_MATRIZ-INTERNET:
    - From: LAN_LOJA
    - To: virtual-wan-link.
    - Source: LAN_LOJA
    - Destination: all
    - Service: All.
    - NAT: Enable.

Figura 35

Configuración Firewall Policy LOJA



Name	From	To	Source	Destination	Schedule	Service	Action	NAT
LOJA_MATRIZ	LAN_LOJA (port3)	virtual-wan-link	LAN_LOJA ADVPN1 ADVPN2	LAN_GYE LAN_MATRIZ LOOPBACK	always	ALL	ACCEPT	Disabled
MATRIZ_LOJA	virtual-wan-link	LAN_LOJA (port3)	LAN_GYE LAN_MATRIZ LOOPBACK	LAN_LOJA ADVPN1 ADVPN2	always	ALL	ACCEPT	Disabled
LAN_MATRIZ - INTERNET	LAN_LOJA (port3)	virtual-wan-link	LAN_LOJA	all	always	ALL	ACCEPT	Enabled

- GYE_MATRIZ
    - From: LAN_GYE
    - To: virtual-wan-link.
    - Source: LAN_GYE, ADVPN1, ADVPN2.
    - Destination: LAN_LOJA, LAN_MATRIZ, LOOPBACK.
    - Service: All.
- MATRIZ_GYE
    - From: virtual-wan-link.
    - To: LAN_GYE.
    - Source: LAN_LOJA, LAN_MATRIZ, LOOPBACK.
    - Destination: LAN_GYE, ADVPN1, ADVPN2.
    - Service: All.
- LAN_GYE-INTERNET:
    - From: LAN_GYE
    - To: virtual-wan-link.
    - Source: LAN_GYE
    - Destination: all
    - Service: All.
    - NAT: Enable.

Figura 36

Configuración Firewall Policy GYE

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
GYE_MATRIZ	LAN_GYE (port3)	virtual-wan-link	LAN_GYE ADVPN1 ADVPN2	LAN_LOJA LAN_MATRIZ LOOPBACK	always	ALL	ACCEPT	Disabled
MATRIZ_GYE	virtual-wan-link	LAN_GYE (port3)	LAN_LOJA LAN_MATRIZ LOOPBACK	LAN_GYE ADVPN1 ADVPN2	always	ALL	ACCEPT	Disabled
LAN_GYE - INTERNET	LAN_GYE (port3)	virtual-wan-link	LAN_GYE	all	always	ALL	ACCEPT	Enabled

4.6. Pruebas de funcionamiento

Para las pruebas de funcionamiento se valida la conectividad desde los equipos finales y los equipos Fortigate. A continuación, se describe las pruebas de comunicación entre Matriz y sucursales, la conectividad entre sucursales en donde se generan dinámicamente los túneles bajo demanda ADVPN y finalmente la validación del failover mediante las reglas configuradas del SDWAN y las políticas de Firewall.

4.6.1. Pruebas de conectividad Matriz – Sucursales

Como primer paso se valida que las sesiones BGP de las dos sucursales estén activas desde Matriz; deben tener 4 vecinos, dos por cada sucursal:

Figura 37

Validación de sesiones BGP activas

```
MATRIZ # get router info bgp summary
VRF 0 BGP router identifier 172.16.100.1, local AS number 65501
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 11 seconds

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.100.253 4      65501     191     194        3    0    0 00:00:20        1
172.16.100.254 4      65501       6       9        2    0    0 00:00:22        1
172.16.200.253 4      65501     192     197        3    0    0 00:00:20        1
172.16.200.254 4      65501     195     196        1    0    0 00:00:23        1

Total number of neighbors 4
```

Los equipos Fortigates tanto en Matriz como en las sucursales tienen habilitado DHCP para los segmentos LAN, a continuación, se especifica la IP asignada:

- Red LAN MATRIZ: 10.10.100.0/24
    - PC LAN MATRIZ: 10.10.100.2
- Red LAN GYE 10.10.150.0/24
    - PC LAN GYE 10.10.150.2
- Red LAN LOJA 10.10.200.0/24
    - PC LAN LOJA 10.10.200.2

Figura 38

Red LAN MATRIZ

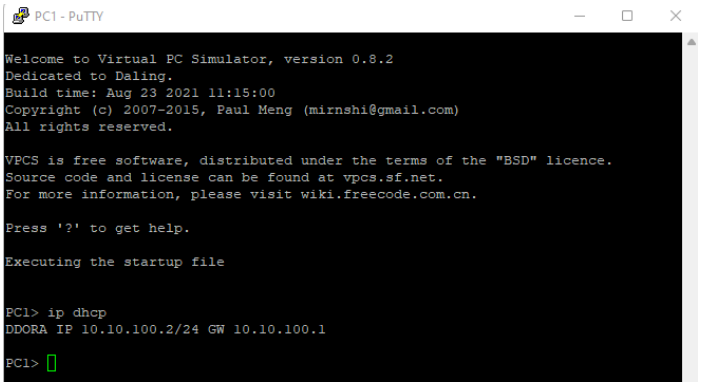


Figura 39

Red LAN GYE

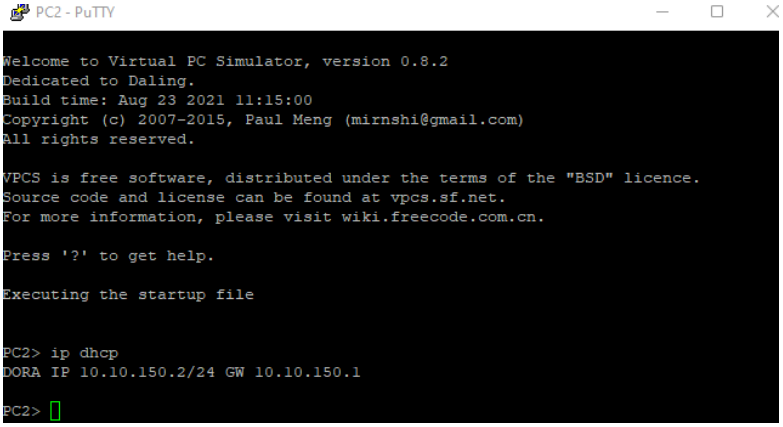
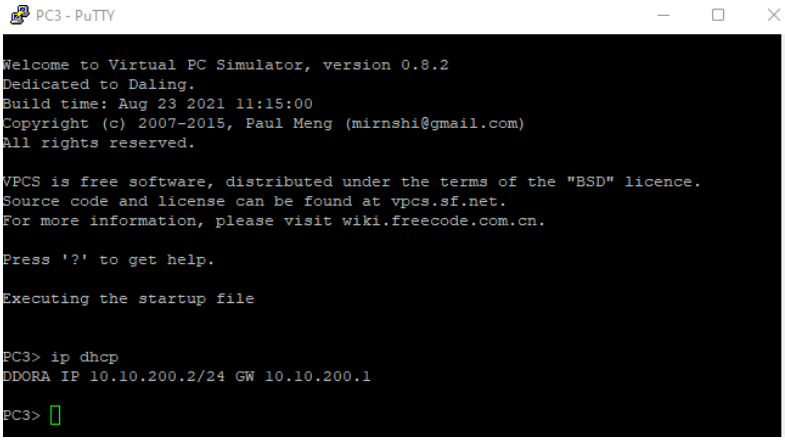


Figura 40

Red LAN LOJA



Para las pruebas de conectividad entre Matriz y las sucursales se utiliza el protocolo ICMP desde el equipo final, con ello se valida que desde la LAN de las sucursales puedan comunicarse a Matriz y viceversa, en estado inicial las reglas SDWAN tiene al proveedor IPS1 como principal y al ISP2 como secundario en el caso de fallo:

Figura 41

Conectividad MATRIZ - GYE y MATRIZ - LOJA

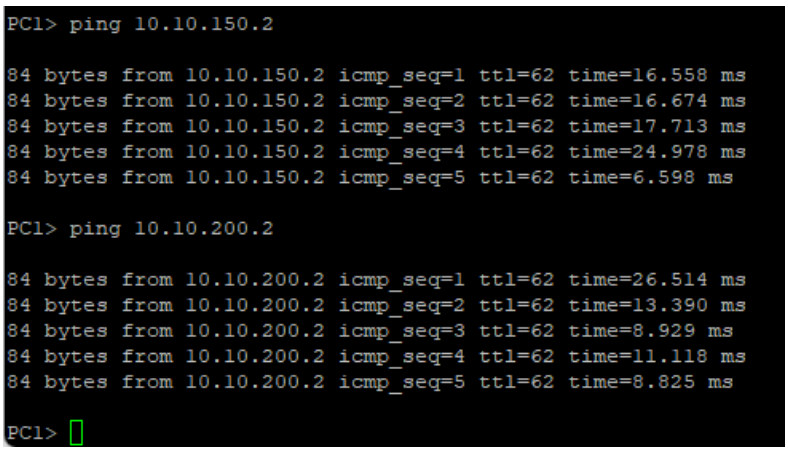


Figura 42

Traza MATRIZ - GYE a través de ISP1

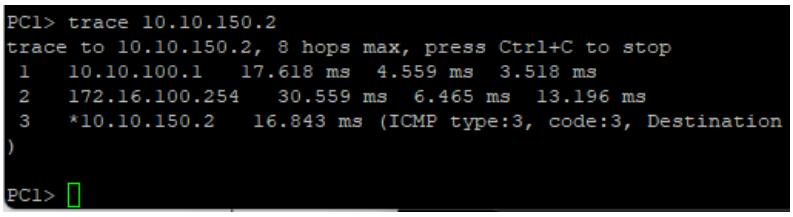


Figura 43

Conectividad GYE - MATRIZ

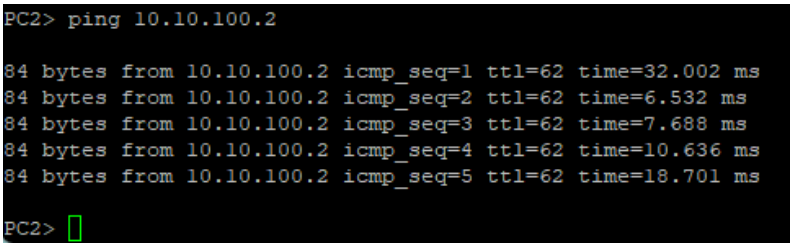


Figura 44

Traza GYE – MATRIZ a través de ISP1

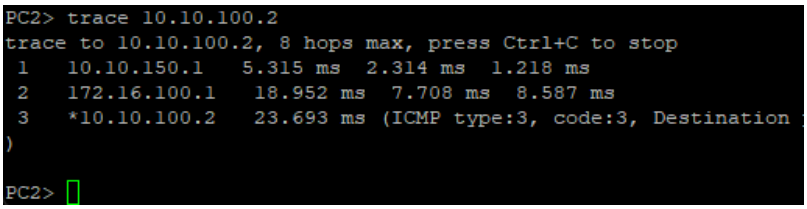


Figura 45

Conectividad LOJA - MATRIZ

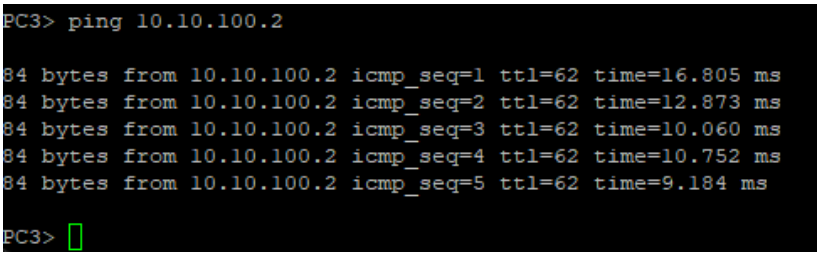
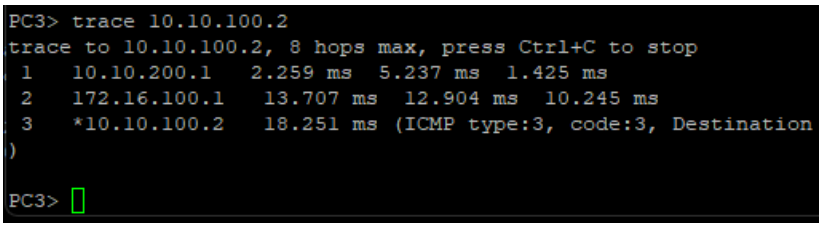


Figura 46

Traza LOJA - MATRIZ a través de ISP1



4.6.2. Pruebas de conectividad hacia Internet

En Matriz y en las sucursales se tiene un esquema de doble enlace de Internet con dos proveedores de servicio; una de las ventajas que permite SDWAN es configurar sus reglas para que los dos enlaces estén trabajando, es decir, que siempre estén en modo activo-activo para la comunicación entre sucursales y Matriz. Se usa como prioridad el IPS1 y para la salida a Internet el ISP2. A continuación, se valida la conexión con el protocolo ICMP hacia Google.

- WAN Matriz:
    - ISP1: 192.168.50.200
    - ISP2: 192.168.121.4
- WAN GYE:
    - ISP1: 192.168.50.210
    - ISP2: 192.168.121.6
- ISP2: 192.168.121.6 WAN Matriz:
    - ISP1: 192.168.50.220
    - ISP2: 192.168.121.8

Para el caso de Matriz se colocó en las políticas de Firewall como primera prioridad al ISP1:

Figura 47

Prueba de conectividad MATRIZ - Internet

```
PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=112 time=33.440 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=112 time=23.092 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=112 time=22.183 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=112 time=23.437 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=112 time=30.381 ms

PC1>
```

Figura 48

Traza MATRIZ – Internet a través de ISP1

```
PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   10.10.100.1   7.736 ms  1.679 ms  1.318 ms
 2   192.168.50.1   9.618 ms  6.752 ms  6.918 ms
```

Figura 49

Verificación de conectividad en el navegador

Para el caso de las sucursales GYE y LOJA, la salida a Internet es por el ISP2, como se muestra a continuación:

Figura 50

Prueba de conectividad GYE - Internet

```
PC2> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=30.252 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=22.592 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=25.634 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=35.777 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=27.816 ms

PC2>
```

Figura 51

Traza GYE – Internet a través de ISP2

```
PC2> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   10.10.150.1   8.581 ms  2.725 ms  1.435 ms
 2   192.168.121.2   9.409 ms  11.628 ms  4.388 ms
```

Figura 52

Prueba de conectividad GYE – Internet desde navegador sucursal GYE

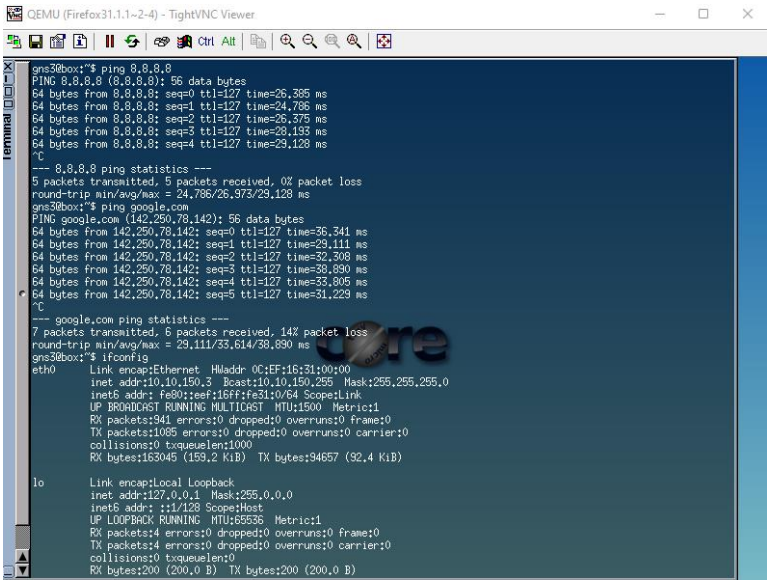


Figura 53

Prueba de conectividad LOJA – Internet

```
PC3> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=23.534 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=23.835 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=23.185 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=30.269 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=24.403 ms

PC3>
```

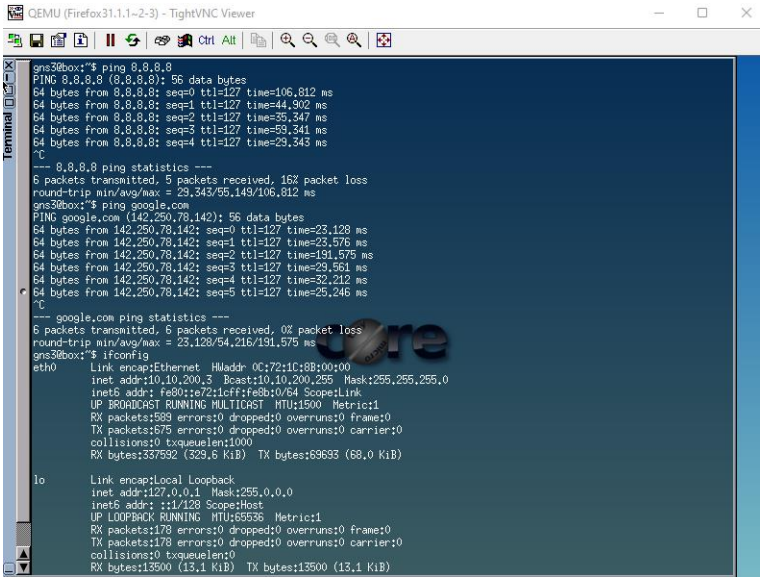
Figura 54

Traza LOJA – Internet a través de ISP2

```
PC3> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   10.10.200.1   2.547 ms  5.078 ms  7.210 ms
 2   192.168.121.2   15.390 ms  20.587 ms  6.628 ms
```

Figura 55

Prueba de conectividad LOJA – Internet desde navegador sucursal LOJA



4.6.3. Pruebas de conectividad entre sucursales

Para validar la creación de los túneles dinámicos bajo demanda ADVPN se presenta el primer escenario en el que solo existen dos túneles activos, los cuales son configurados de manera manual:

Figura 56

Validación de túneles ADVPN GYE hacia MATRIZ

```
GYE # get ipsec tunnel list
NAME         REMOTE-GW        PROXY-ID-SOURCE          PROXY-ID-DESTINATION     STATUS TIMEOUT
ADVPN_1      192.168.50.200:0 0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25502
ADVPN_2      192.168.121.4:0  0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25501
```

Figura 57

Validación de túneles ADVPN LOJA hacia MATRIZ

```
LOJA # get ipsec tunnel list
NAME         REMOTE-GW         PROXY-ID-SOURCE          PROXY-ID-DESTINATION     STATUS TIMEOUT
ADVPN_1      192.168.50.200:0  0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25462
ADVPN_2      192.168.121.4:0   0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25466
```

Cuando se solicita la comunicación entre sucursales se crea un túnel dinámico que permite la conexión sin necesidad de configurar túneles adicionales, con ello se puede disminuir el tiempo de configuración, la complejidad del despliegue del proyecto y facilitar en la resolución de problemas.

Figura 58

Conexión ADVPN GYE - LOJA

```
PC2> ping 10.10.200.2

84 bytes from 10.10.200.2 icmp_seq=1 ttl=62 time=13.380 ms
84 bytes from 10.10.200.2 icmp_seq=2 ttl=62 time=12.615 ms
84 bytes from 10.10.200.2 icmp_seq=3 ttl=62 time=18.549 ms
84 bytes from 10.10.200.2 icmp_seq=4 ttl=62 time=11.831 ms
84 bytes from 10.10.200.2 icmp_seq=5 ttl=62 time=9.945 ms

PC2>
```

Figura 59

Conexión ADVPN LOJA - GYE

```
PC3> ping 10.10.150.2

84 bytes from 10.10.150.2 icmp_seq=1 ttl=62 time=16.278 ms
84 bytes from 10.10.150.2 icmp_seq=2 ttl=62 time=10.826 ms
84 bytes from 10.10.150.2 icmp_seq=3 ttl=62 time=11.886 ms
84 bytes from 10.10.150.2 icmp_seq=4 ttl=62 time=12.064 ms
84 bytes from 10.10.150.2 icmp_seq=5 ttl=62 time=10.272 ms

PC3>
```

Figura 60

Creación de túnel dinámico ADVPN GYE – LOJA

```
GYE # get ipsec tunnel list
NAME         REMOTE-GW        PROXY-ID-SOURCE          PROXY-ID-DESTINATION     STATUS TIMEOUT
ADVPN_1      192.168.50.200:0 0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25099
ADVPN_2      192.168.121.4:0  0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25099
ADVPN_1_0    192.168.50.220:0 0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     42833

GYE #
```

Figura 61

Creación de túnel dinámico ADVPN GYE – LOJA

```
LOJA # get ipsec tunnel list
NAME         REMOTE-GW        PROXY-ID-SOURCE          PROXY-ID-DESTINATION     STATUS TIMEOUT
ADVPN_1      192.168.50.200:0 0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25078
ADVPN_2      192.168.121.4:0  0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     25081
ADVPN_1_0    192.168.50.210:0 0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0          up     43093

LOJA #
```

4.6.4. Pruebas de Failover entre proveedores

Para validar la conmutación entre proveedores de servicios cuando pierde comunicación uno de los ISP en los equipos Fortigate, se realiza un apagado de la interfaz WAN en matriz, específicamente la interfaz ISP1:

Figura 62

Apagado de interfaz WAN en MARIZ

```
MATRIZ (port1) # set status down

MATRIZ (port1) # show
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.50.200 255.255.255.0
        set allowaccess ping https http
        set status down
        set type physical
        set description "ISP1"
        set alias "ISP1"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
end
```

Luego de la falla en el proveedor ISP1 se valida que en Matriz las sesiones BGP se establecen solo con un vecino hacia cada sucursal:

Figura 63

Sesiones BGP MATRIZ - Sucursales

```
MATRIZ # get router info bgp summary
VRF 0 BGP router identifier 172.16.100.1, local AS number 65501
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 34 seconds

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.100.253 4      65501     350     358        0    0    0    never Active
172.16.100.254 4      65501     164     173        0    0    0    never Active
172.16.200.253 4      65501     356     361        1    0    0 00:00:03        1
172.16.200.254 4      65501     360     365        1    0    0 00:00:02        1
```

Se realizan las pruebas de conectividad entre Matriz y las sucursales para demostrar que su comunicación es mediante el ISP2:

Figura 64

Conectividad MATRIZ – GYE y MATRIZ – LOJA

```
PC1> ping 10.10.150.2

84 bytes from 10.10.150.2 icmp_seq=1 ttl=62 time=24.202 ms
84 bytes from 10.10.150.2 icmp_seq=2 ttl=62 time=9.108 ms
84 bytes from 10.10.150.2 icmp_seq=3 ttl=62 time=10.027 ms
84 bytes from 10.10.150.2 icmp_seq=4 ttl=62 time=9.589 ms
84 bytes from 10.10.150.2 icmp_seq=5 ttl=62 time=10.210 ms

PC1> ping 10.10.200.2

84 bytes from 10.10.200.2 icmp_seq=1 ttl=62 time=33.818 ms
84 bytes from 10.10.200.2 icmp_seq=2 ttl=62 time=17.205 ms
84 bytes from 10.10.200.2 icmp_seq=3 ttl=62 time=7.785 ms
84 bytes from 10.10.200.2 icmp_seq=4 ttl=62 time=23.536 ms
84 bytes from 10.10.200.2 icmp_seq=5 ttl=62 time=6.994 ms
```

Figura 65

Traza MATRIZ - Sucursales a través de ISP2

```
PC1> trace 10.10.150.2
trace to 10.10.150.2, 8 hops max, press Ctrl+C to stop
 1   10.10.100.1   8.029 ms  2.395 ms  12.821 ms
 2   172.16.200.254   19.162 ms  6.228 ms  8.955 ms
 3   *10.10.150.2   15.860 ms (ICMP type:3, code:3, Destination
)

PC1> trace 10.10.200.2
trace to 10.10.200.2, 8 hops max, press Ctrl+C to stop
 1   10.10.100.1   1.921 ms  2.035 ms  4.206 ms
 2   172.16.200.253   12.547 ms  6.161 ms  12.498 ms
 3   *10.10.200.2   13.258 ms (ICMP type:3, code:3, Destination
)
```

La arquitectura ADVPN SDWAN permite no solo la simplificación en los despliegues a gran escala de sucursales, sino también el aprovechamiento de todos los enlaces contratados con los proveedores de servicios permitiendo tener una alta disponibilidad a nivel de conectividad.

CAPÍTULO V: CONCLUSIONES

5.1. Conclusiones

- Con la implementación de una arquitectura ADVPN se logra simplificar el despliegue de las configuraciones, ya que solo se necesitan crear los túneles entre Matriz y las sucursales y, para la conectividad entre sucursales los túneles se crearán de manera dinámica y bajo demanda.

- En el despliegue de un esquema activo – activo para la utilización de todos los enlaces de los proveedores de servicios se maneja una arquitectura WAN definida por software SDWAN, en él se configuran las reglas para el enrutamiento del tráfico especifico por las diferentes interfaces físicas o lógicas; además, permite que en caso de caída o degradación de la última milla de uno de los ISP´s se pueda conmutar de manera automática el tráfico por medio de los parámetros de control de reglas y SLA configurados en el SDWAN, dando como resultado un diseño tolerante a fallas.

- Para el análisis y configuración de una arquitectura empresarial en un ambiente de pruebas se puede utilizar GNS3, el cual permite simular un entorno real; en este caso Fortinet permite descargar máquinas virtuales con su sistema operativo.

- Con el desarrollo del presente proyecto se demuestra que la arquitectura SDWAN ADVPN es una solución dinámica, segura, escalable en el tiempo y de alta disponibilidad, con ello las empresas pueden robustecer sus esquemas de conectividad.

5.2. Recomendaciones

- Se recomienda que para la implementación de una arquitectura en GNS3 se debe analizar el espacio en memoria RAM que requiere cada uno de los dispositivos virtualizados, ya que puede ser un limitante si se necesita desplegar una topología amplia y almacenarla en el computador físico.

- Para proyectos empresariales se recomienda que siempre se maneje luego del diseño un ambiente de pruebas, esto permitirá validar los posibles puntos de falla en configuración para que al momento de implementar los servicios sean mínimamente afectados con el cambio.

- Para implementar SDWAN ADVPN se recomienda siempre utilizar diferentes proveedores de servicios, con ello se puede garantizar que la alta disponibilidad tendrá un mayor rango de efectividad ya que se garantiza rutas distintas.

REFERENCIAS

Referencias

Bustos Sánchez, C. S. (2019). *Repositorio de la Universidad de Fuerzas Armadas ESPE* . Obtenido de http://repositorio.espe.edu.ec/handle/21000/15877

Carrasco Cabrera, F. A. (06 de 11 de 2020). *Repositorio Digital UCSG.* Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/15699

Cisco. (07 de 2019). *Cisco SD-WAN End-to-End Deployment.* Obtenido de https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/SD-WAN-End-to-End-Deployment-Guide.pdf

Fordham, S. (2021). *Learning SD-WAN with Cisco, Transform Your Existing WAN.* Bedfordshire: Apress.

Fortinet. (03 de 12 de 2019). *Fortinet Secure SD-WAN Reference Architecture.* USA: Fortinet.

Fortinet. (27 de 08 de 2021). FortiOS - Administration Guide. Fortinet.

Fortinet. (27 de 08 de 2021). *FortiOS - Administration Guide - 6.4.2.* Obtenido de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4dcf9363-d124-11ea-8b7d-00505692583a/FortiOS-6.4.2-Administration_Guide.pdf

GNS3. (2022

GNS3. Obtenido de https://www.gns3.com/

Hamelin, S. (2020). *FORTINET, Fortinet Auto Discovery VPN (ADVPN).* Obtenido de https://kb.fortinet.com/kb/documentLink.do?externalID=FD39360

Leng, T. (2021). *SD-WAN SOLUTION.* Huawei Technologies Co.

Marín Santamaría, L. A. (13 de 08 de 2021). *Repositorio Digital UCSG.* Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/16888

MEF Standard 70. (july de 2019). *SD-WAN Service Attributes and Services.* Obtenido de https://www.mef.net/wp-content/uploads/2019/07/MEF-70.pdf

Rodríguez Limones, M. F. (10 de 11 de 2021). *Repositorio Digital UCSG.* Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/17647

Roncero Hervás, Ó. (20 de 05 de 2014). *Universidad Politécnica de cataluña.* Obtenido de https://upcommons.upc.edu/bitstream/handle/2099.1/21633/Memoria.pdf

Sheng, C., Bai, J., & Sun, Q. (2021). *Software-Defined Wide Area Network Architectures and Technologies.* POSTS&TELECOM PRESS.

VMware. (2022). *VMwate* . Obtenido de https://www.vmware.com/

Apéndice: Manual de Instalación de Herramientas de Simulación y Virtualización

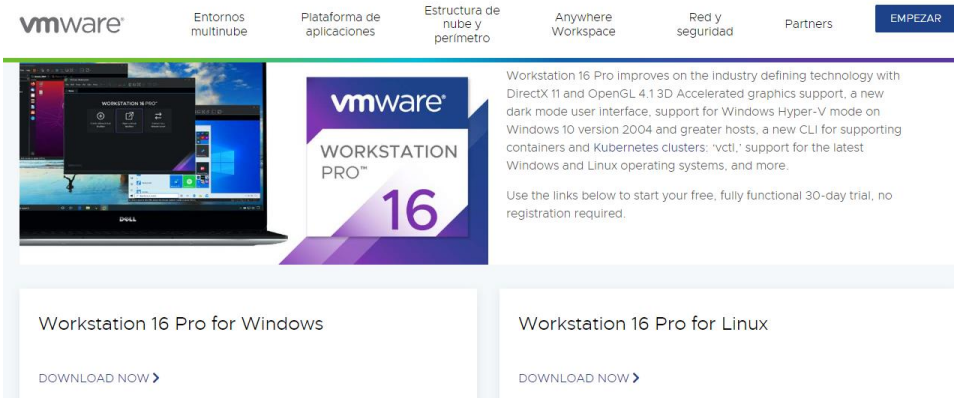
1. SOFTWARE REQUERIDO:

Para la implementación del presente proyecto se descarga tres softwares base, los cuales son VMware Workstation Pro, GNS3 para Windows y VM GNS3 VMware Workstation.

a) VMware Workstation Pro: permite la virtualización de la VM GNS3. Se descarga de la página oficial de VMware.

Figura 66

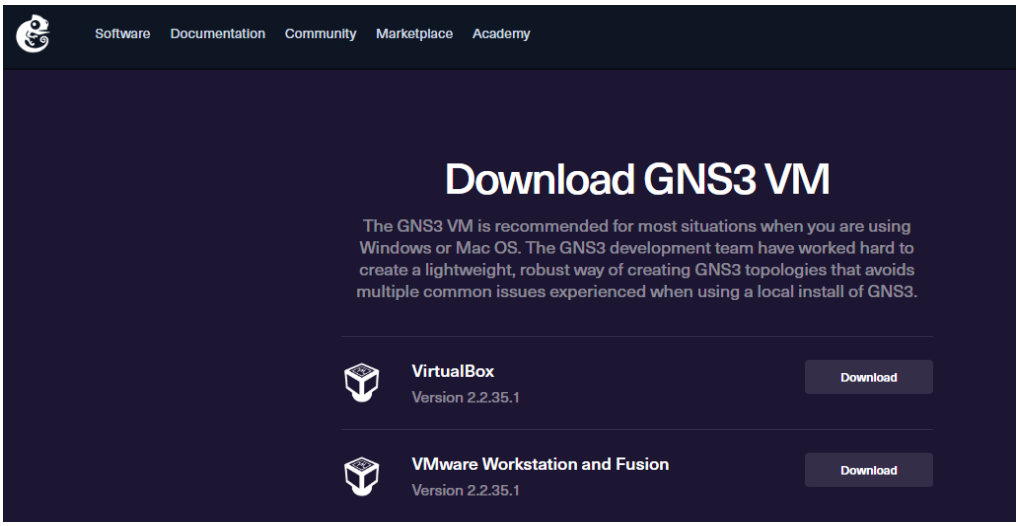
Página de descarga VMware



b) VM GNS3 VMware Workstation: trabaja como el servidor de GNS3.

Figura 67

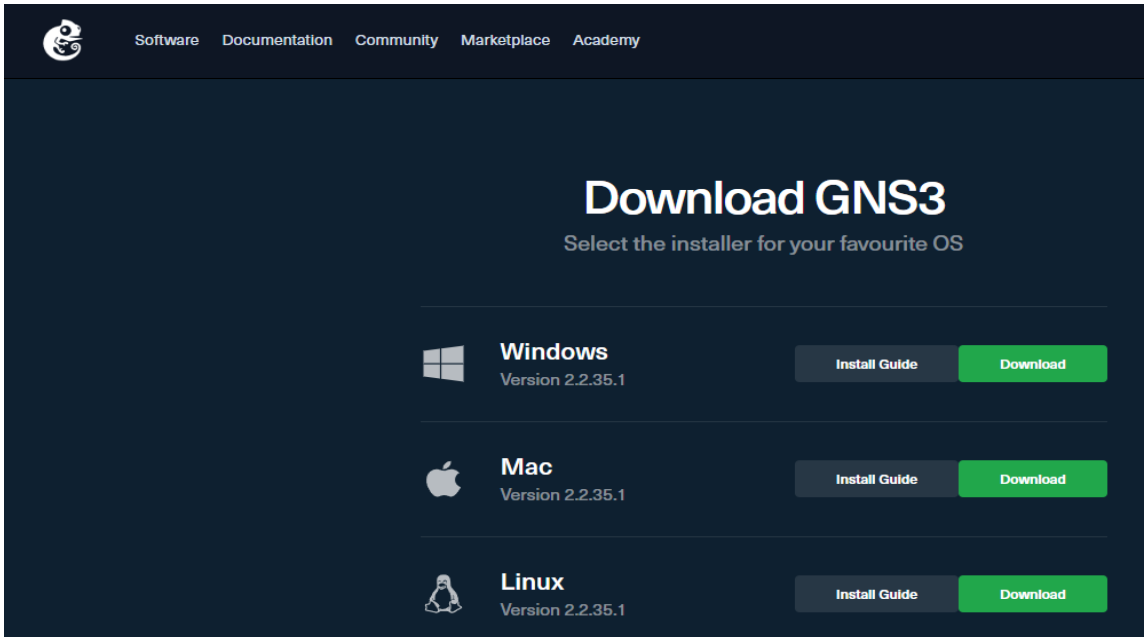
Página de descarga VM GNS3 VMware Workstation



c) **GNS3 para Windows:** será el simulador en el que se desplegará las imágenes de los equipos a utilizar en la arquitectura SDWAN ADVPN. Se descarga de la página de GNS3:

Figura 68

Página de descarga GNS3



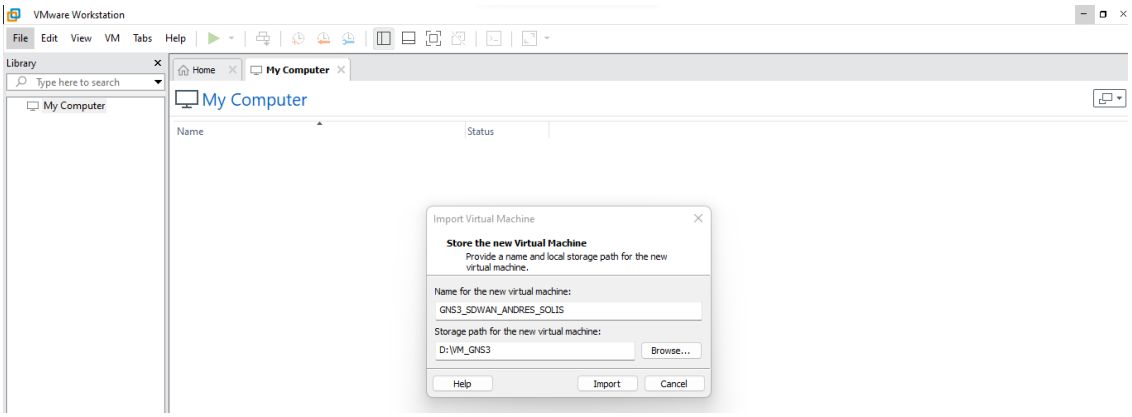
2. INSTALACIÓN

a) Para la instalación de GNS3 VM en VmWare Workstation:

- Se coloca el nombre de la máquina virtual y la ubicación de almacenamiento en el equipo físico:

Figura 69

Creación de la máquina virtual



- Se importa VM GNS3 en VMware Workstation:

Figura 70

Importación de VM GNS3 en VMware Workstation

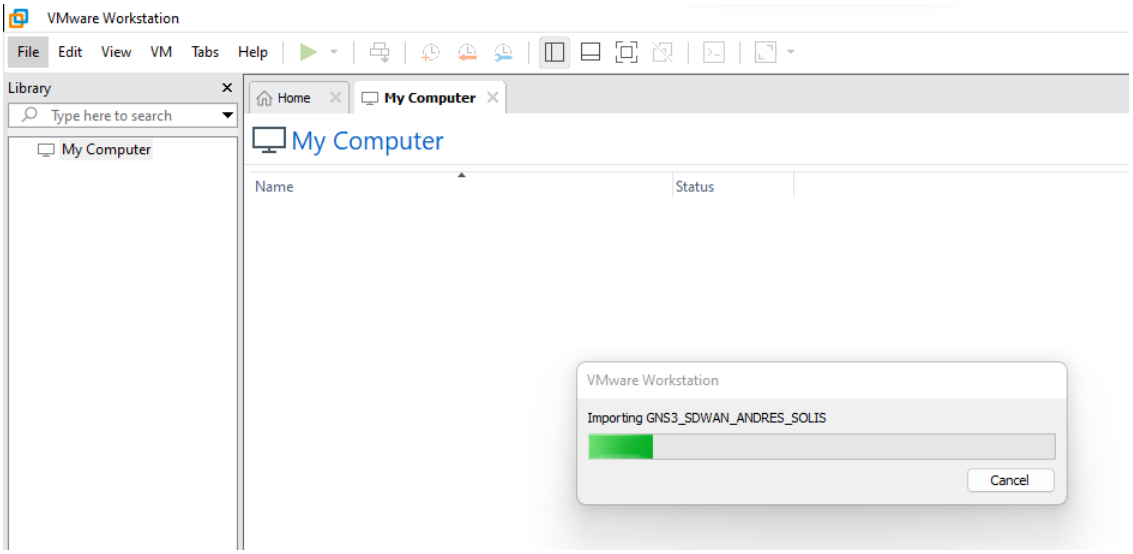
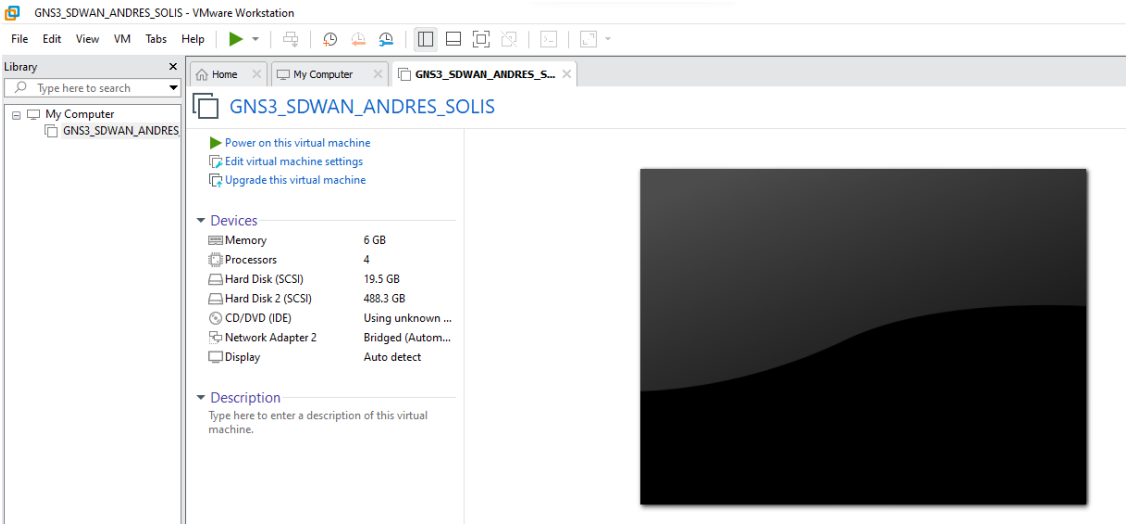


Figura 71

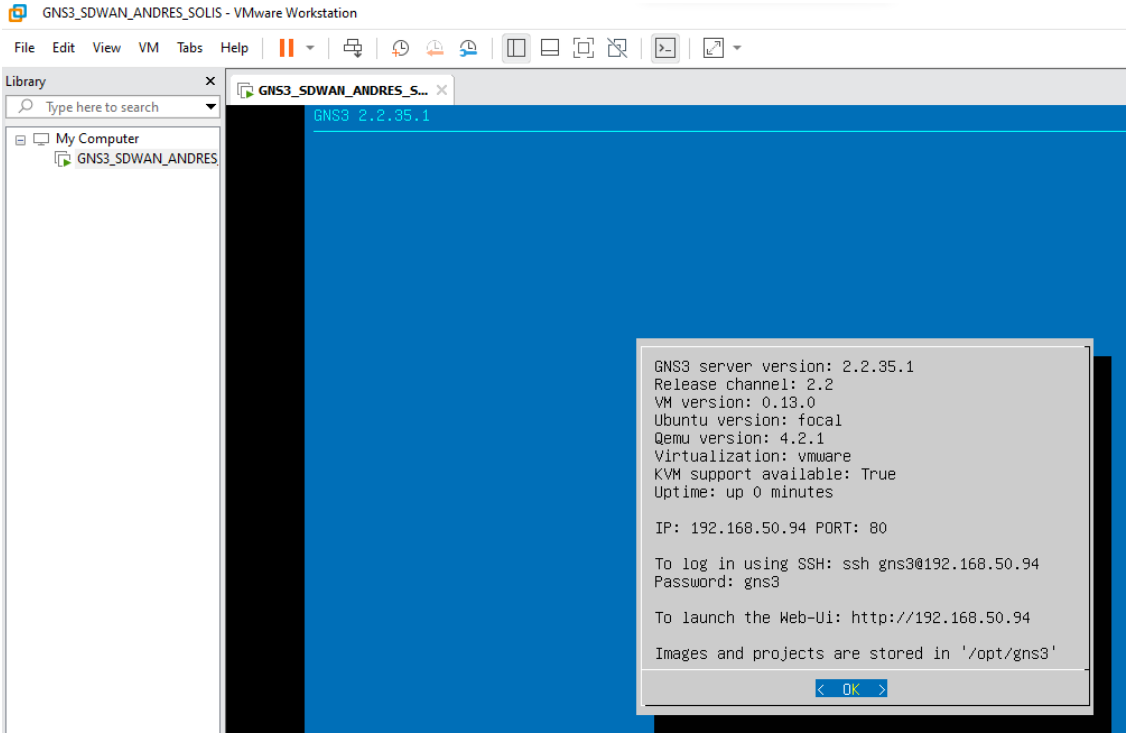
Visualización de los recursos configurados para la VM GNS3



- La VM GNS3 se encuentra sobre un sistema operativo UBUNTU, esta VM será el servidor del cliente GNS3 instalado en Windows:

Figura 72

VM GNS3

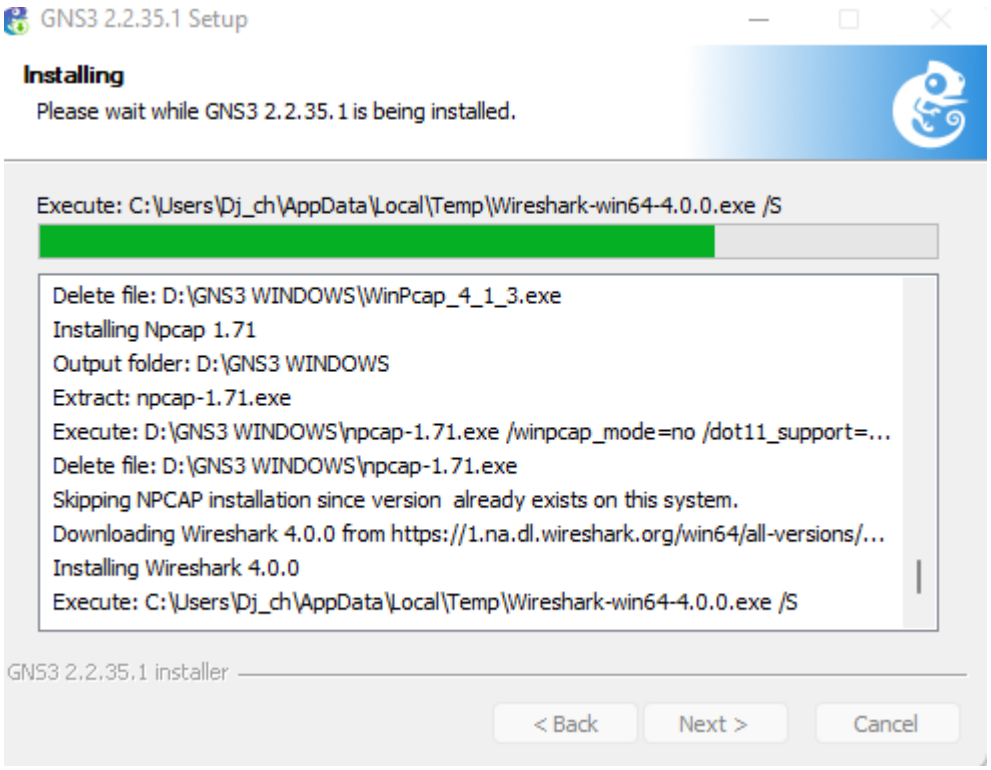


b) Instalación de GNS3 para Windows:

- Se ejecuta el instalador con los parámetros por defecto:

Figura 73

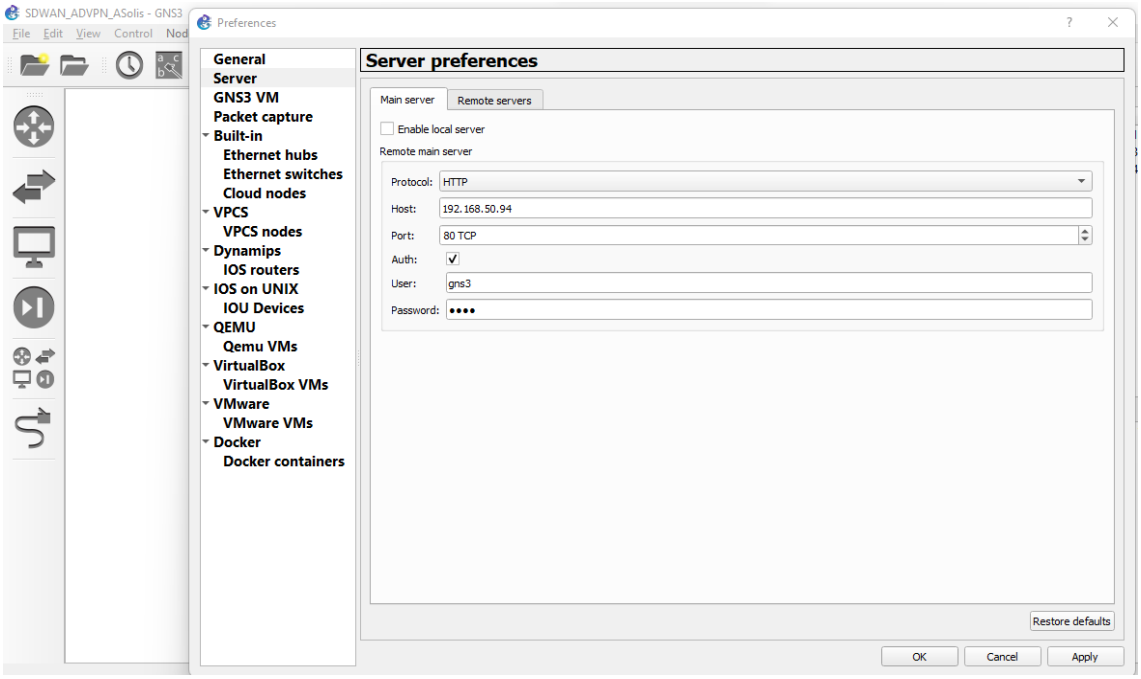
Ejecución del instalador GNS3 para Windows



- Para que se sincronice con el servidor se coloca la IP, usuario y password, esta información se extrae del servidor VM GNS3 sobre Ubuntu, con ello ya podemos disponer de la ventana de trabajo de GNS3 en Windows:

Figura 74

Ventana de trabajo GNS3 para Windows

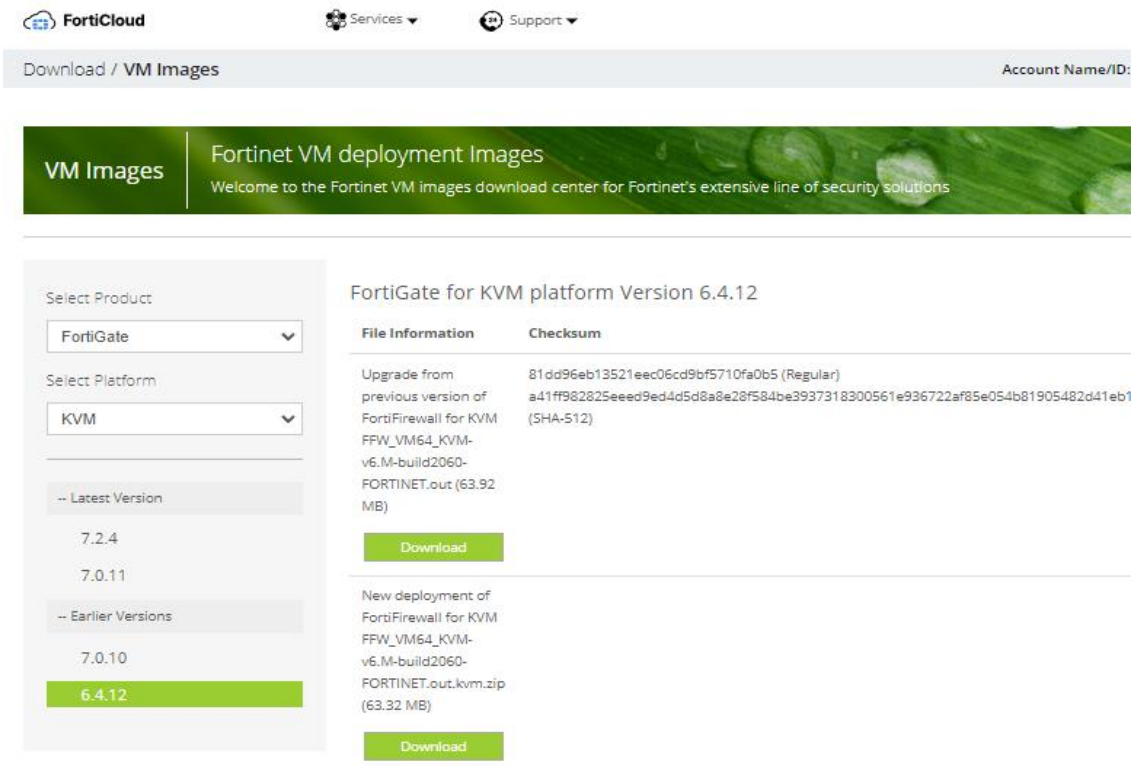


c) Instalación de Fortigate en GNS3 para Winsdows

- Para descargar la máquina virtual de Fortigate compatible con GNS3 es necesario crear un usuario en Forticloud; con las credenciales de acceso ya establecidas se puede descargar KVM Fortigate para instalar en GNS3 Windows:

Figura 75

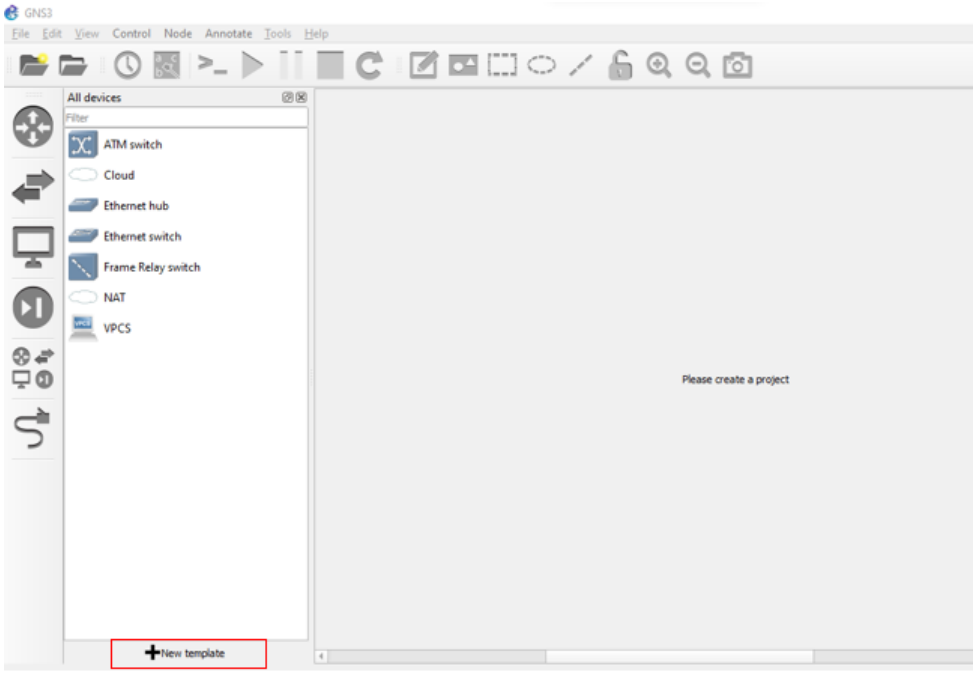
Página de descarga de Fortigate



- Para la instalación de Fortigate en GNS3 se debe agregar un nuevo template:

Figura 76

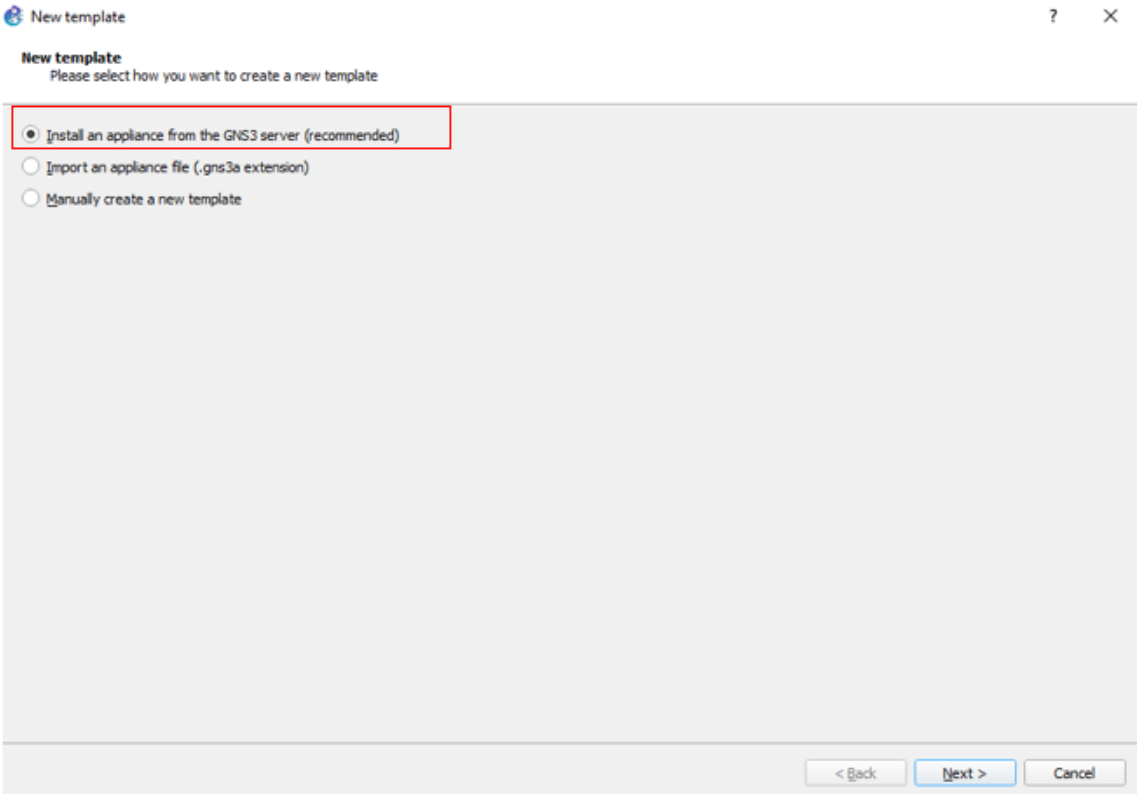
Creación de Template Fortigate



- Se selecciona la opción para que la instalación se ejecute desde el servidor virtualizado de GNS3 figura:

Figura 77

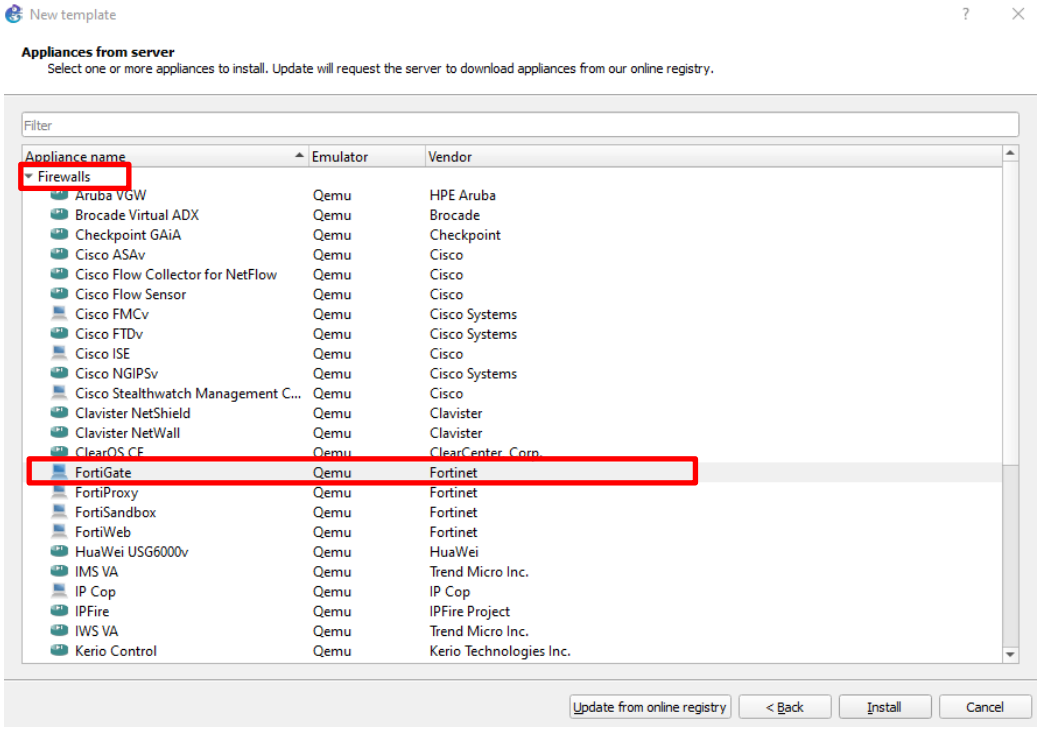
Instalación en Servidor GNS3



- Se selecciona el tipo y marca del dispositivo a utilizar en la simulación, que en este caso será un Firewall marca Fortigate:

Figura 78

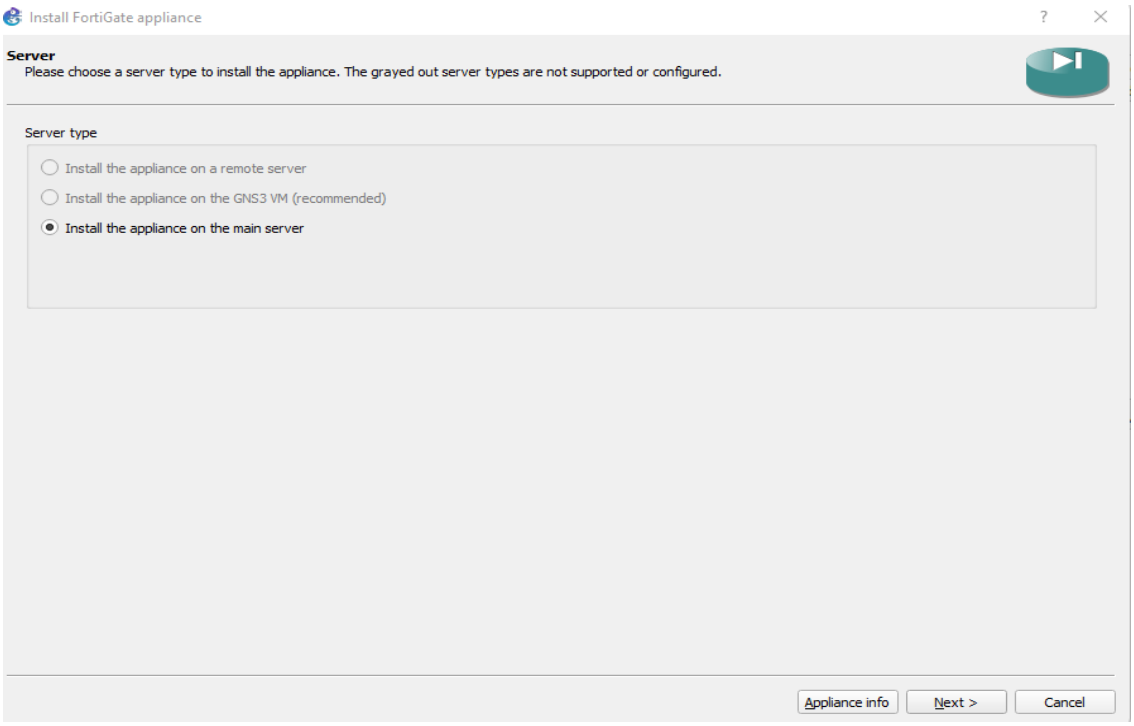
Selección de tipo y marca de dispositivo



- Se instala el equipo Firewall Fortigate en el servidor principal:

Figura 79

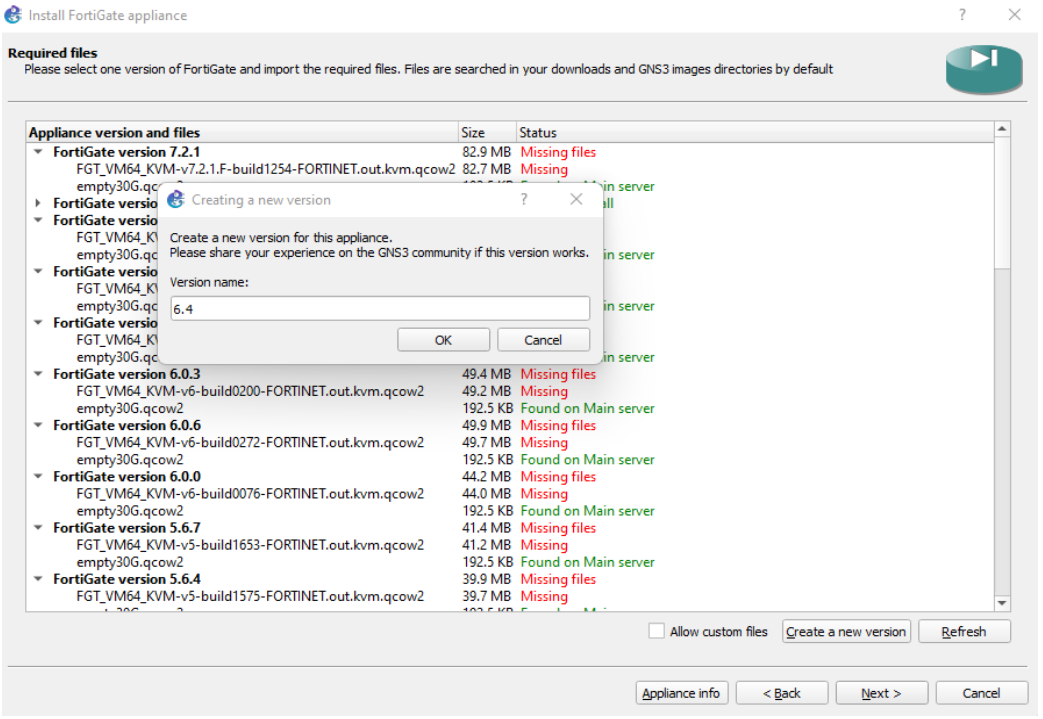
Instalación de equipo Forigate en Servidor principal



- Se crea una nueva versión de Fortigate, en este caso será la versión 6.4:

Figura 80

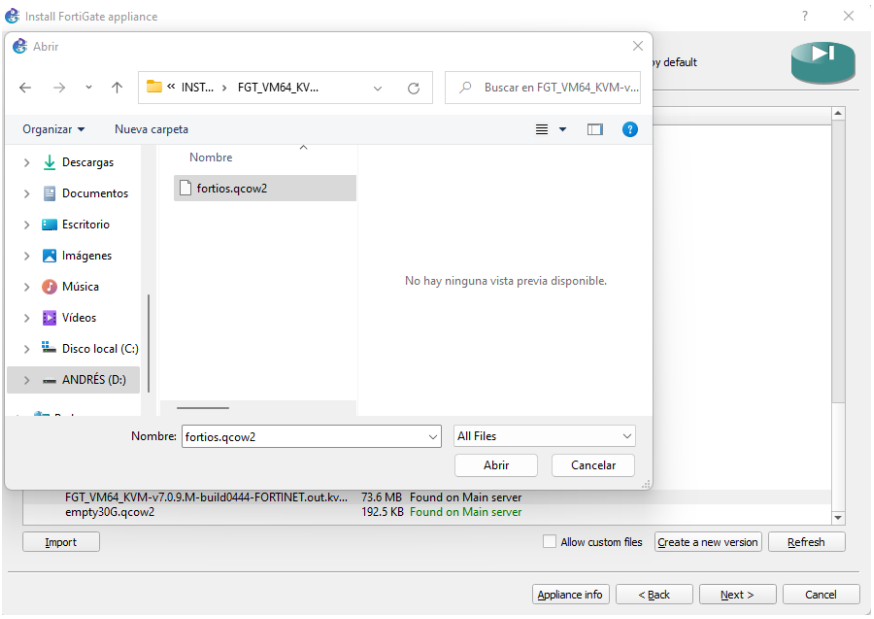
Creación de versión 6.4 de Fortigate



- Se importa el KVM Fortigate virtual descargado previamente en Forticloud:

Figura 81

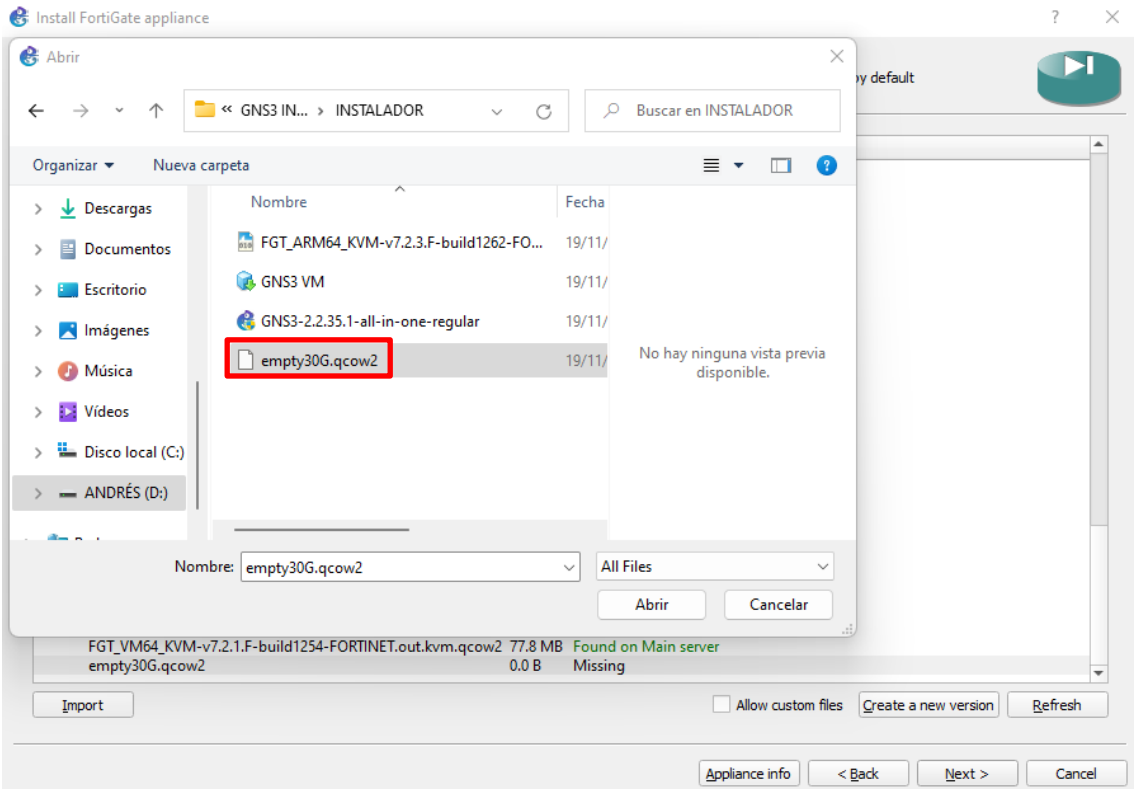
Importación de KVM Fortigate



- A continuación, se descargar e importa la imagen para una plantilla de disco de almacenamiento en el repositorio de GNS3:

Figura 82

Imagen para una plantilla de disco de almacenamiento



- Finalmente se instala y se agrega en el grupo de dispositivos. Por defecto el equipo Fortigate tiene como credenciales de acceso usuario *admin* y no tiene password:

Figura 83

Uso de equipo Fortigate