PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

MONITOREO DE REDES Y MÁQUINAS VIRTUALES CON HERRAMIENTAS OPEN SOURCE UTILIZANDO EL EMULADOR DE REDES GNS3.

AUTOR:

ALISSON MICHELLE ORTIZ BARROS

DIRECTOR: MGTR. CHARLES ESCOBAR

QUITO DM, 2022

DEDICATORIA

Mi Padre Patricio Ortiz por educarme para ser lo que ahora soy, por enseñarme a creer más en mí y por guiar mis pasos desde el cielo.

Mi madre Patricia Barros por su apoyo constante e incondicional y por ser la mejor que me ha dado la vida.

Mi hermana Gabriela Ortiz por ser mi mejor amiga y la razón de mi existencia.

Mis abuelitos Teresa Bohórquez y Angel Barros por el apoyo incondicional y estar ahí siempre para mí.

Todas las personas que creyeron siempre en mí.

AGRADECIMIENTO

A Dios por ubicarme en el sitio y momento preciso

A la vida que con sus momentos buenos que me ha dado recuerdos gratos y con sus momentos no tan buenos me que me ha permitido adquirir madurez y experiencia.

A mis padres por brindarme su amor, enseñarme a soñar, ayudarme a creer y enfocarme en luchar para conseguir lo que quiero.

A mi hermana por su apoyo, paciencia, ejemplo y amor.

A la Pontificia Universidad Católica del Ecuador por enseñarme de ciencias para hacerle frente a la vida.

A mis maestros por impartirme sus conocimientos.

A todas las personas que han contribuido para alcanzar mis sueños.

Alisson

RESUMEN

El presente proyecto de titulación busca brindar un monitoreo de redes y máquinas virtuales con herramientas Open Source utilizando el emulador de redes GNS3, empleando diferentes tipos de configuraciones Firewall y gestión de configuraciones de Windows con requerimientos para cada situación. En el primer capítulo se describe la problemática existente en la actualidad sobre el monitoreo de redes y su implicación en el costo al utilizar herramientas diferentes al emulador de redes GNS3 para posteriormente en el segundo capítulo hacer énfasis en la gestión teórica de la investigación, detallando de forma precisa las variables de la investigación y los protocolos concernientes para el desarrollo, de la misma manera los modelos implícitos para poder alcanzar los objetivos planteados. Posteriormente se explica el funcionamiento y los componentes de ICINGA2, desde el modelado del monitoreo mediante una topología de estrella, la preparación e instalación de los dispositivos, el análisis correspondiente, procesos de instalación y los análisis de resultados mediante la simulación implícita, con lo cual se concluye que la implementación de un monitoreo de redes y máquinas virtuales con herramientas Open Source es favorable y beneficiosa al utilizar el emulador de redes GNS3 por su bajo costo.

Palabras clave: Desarrollo, control, redes, monitoreo, telecomunicaciones

ABSTRACT

This degree project seeks to provide monitoring of networks and virtual machines with Open Source tools using the GNS3 network emulator, using different types of Firewall configurations and Windows configuration management with requirements for each situation. The first chapter describes the current problems on network monitoring and its implication in the cost when using tools other than the GNS3 network emulator, and later, in the second chapter, emphasis is placed on the theoretical management of the research, detailing Precisely the variables of the investigation and the protocols concerning the development, in the same way the implicit models to be able to reach the established objectives. Subsequently, the operation and components of ICINGA2 are described, from the modeling of monitoring through a star topology, the preparation and installation of the devices, the corresponding analysis, installation processes and the analysis of results through implicit simulation, with which It is concluded that the implementation of network and virtual machine monitoring with Open Source tools is favorable and beneficial when using the GNS3 network emulator due to its low cost.

Keywords: Development, control, networks, monitoring, telecommunications

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TEMA:

MONITOREO DE REDES Y MÁQUINAS VIRTUALES CON HERRAMIENTAS OPEN SOURCE UTILIZANDO EL EMULADOR DE REDES GNS3.

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. JUSTIFICACIÓN

En la actualidad, cualquier red de datos puede ser susceptible a varios intentos de intrusos que quieran ingresar a un sistema o dado el caso a ataques cibernéticos o informáticos, en este contexto es fundamental contar con un sistema que pueda detectar actividad sospechosa, generar alarmas y registrar eventos en tiempo real. Con el monitoreo en redes y máquinas virtuales mediante el Software GNS3 (Graphic Network Simulation), se podrá conocer las ventajas y beneficios que brinda esta tecnología, ya que se estudiará y se analizará esta nueva arquitectura en la red y a su vez logrará optimizar y simplificar los recursos, haciendo las redes más seguras y dinámicas.

Existen diversas formas para el control de una red moderna y cumpla estándares internacionales de funcionamiento, las herramientas que se utilizan para el monitoreo o la supervisión están diseñadas con el objetivo de supervisar el tráfico los tiempos de respuesta y el tráfico en la red. Si una empresa tiene una red activa, se necesita del monitoreo de las redes para asegurarse que no es vulnerable a algún ataque. Por lo tanto, es estudio se centra en el análisis de herramientas de monitoreo de nodos y aplicaciones individuales.

Esta investigación trata de analizar los diversos servicios en el ámbito tecnológico a través del emulador de redes GNS3 en las empresas y relacionándolas con todos los requerimientos por

medio de la plataforma Icinga2, de la misma manera se trata de determinar la criticidad de los servicios tecnológicos para el desarrollo de la topología en GNS3.

1.2. PLANTEAMIENTO DEL PROBLEMA

En la actualidad el monitoreo de redes es una de las actividades principales dentro de un proceso tecnológico y monitorear los sistemas conectados de una empresa se transforma en una tarea fundamental para el mantener una red funcionando idónea. Estas actividades han hecho que las industrias, corporaciones, instituciones, empresas grandes y medianas, incrementen sus recursos en sistema de monitoreo, de comunicación, lo que produce varias acciones decisivas que tomar, sobre todo en los tiempos de respuesta y disponibilidad de las redes y sus dispositivos, como routers, switches, firewalls, servidores, etc.

Sin embargo, el aumento de inversiones en este tema de monitoreo de redes puede generar tráfico y puede llegar a saturarse, produciendo la pérdida del enlace o la degradación de la señal. Por estas razones el monitoreo se vuelve clave en una empresa y se debe tener la debida preparación técnica y herramientas tecnológicas suficientes para cumplir con las necesidades mínimas de diferentes empresas. Debido al alto costo de la infraestructura de red tradicional, se sugieren alternativas como el monitoreo de redes y servidores para facilitar la gestión, flexibilidad y escalabilidad del entorno. Por lo tanto, esta investigación se centra en identificar las diferentes formas de monitorear una red a través de código abierto utilizando el emulador de redes GNS3 y la herramienta de monitoreo Icinga2.

1.3.OBJETIVOS

1.3.1. OBJETIVO GENERAL

Analizar el monitoreo de una empresa de tecnología a través de los servicios tecnológicos utilizando el emulador de redes GNS3 por medio de la plataforma Icinga2.

1.3.2. OBJETIVOS ESPECÍFICOS

1. Modelar el monitoreo de una topología de red para una empresa de tecnología
2. Describir los beneficios y servicios que brinda una red de accesos utilizando topología en GNS3.
3. Analizar los recursos que contiene la tecnología Icinga2 para el monitoreo de redes.
4. Analizar los resultados del monitoreo de dispositivos de red con la herramienta Icinga2

1.4.METODOLOGÍA DE LA INVESTIGACIÓN

La metodología para este estudio inicia con el método exploratorio de las redes tomando en cuenta las herramientas señaladas en el marco teórico como es Icinga2 como código abierto, además se utiliza el método descriptivo con el objetivo de detallar las topologías de la tecnología GNS3 que se pueden considerar al momento de desarrollar el diseño de una red de acceso utilizando esta tecnología, por lo tanto, es de tipo analítico y experimental, ya que necesita realizar un análisis de los beneficios que la tecnología traerá a la empresa a través de simulaciones.

El proyecto presentado por (López, 2020) en la ciudad de Quito buscó realizar un examen de red de área amplia definida por procedimientos (SD-WAN) en el programa GNS3 y utilizando aparatos de tecnología FORTINET. El Capítulo 1 narra el trabajo y los dispositivos tecnológicos de conmutación de etiquetas multiprotocolo (MPLS). La teoría básica de Redes Definidas por Software (SDN) da paso luego a un análisis de SD-WAN, sus conceptos, arquitectura, ventajas, etc., con una explicación del programa GNS3 y la tecnología FORTINET. El título 2 detalla el desempeño Hybrid SD-WAN. Se especifican seguridades, política, ingeniería de tráfico, etc. Además, se cubre en detalle el control centralizado y la investigación a través de FortiManager y FortiAnalyzer, y el capítulo concluye con la

configuración. El tercer capítulo confirma los resultados de la simulación mediante la ejecución de pruebas, pruebas de seguridad y pruebas de monitoreo.

En el trabajo desarrollado por Alcívar (2019) para la Escuela Superior Politécnica Agropecuaria de Manabí se compara el paradigma tradicional de redes con un modelo de red definido por (SDN) en el entorno de red en un espacio determinado con traducción. Se implementan dos marcos de simulación, uno es una red tradicional, y el otro es una red SDN con un diseño similar, pero con las cualidades semejantes de este modelo. Estos entornos se implementan en el emulador de red GNS3. Para añadir servidores web y aulas virtuales, VirtualBox y VMware están integrados en el emulador. Para obtener los resultados se implementa una máquina virtual en el emulador, realizando aclaraciones a redes locales y externas. De estas pruebas se alcanzaron el estado latente, cambio de latencia y extravío de paquetes.

1.5. ALCANCE

El monitoreo y supervisión de redes es un elemento importante dentro de la estrategia de toda empresa en lo que tiene que ver en la administración de redes puesto que brinda información de primera mano para solucionar problemas tecnológicos sobre todo relacionados con la red y si no se toma correctivos a tiempo pueden causar graves daños a una organización.

Cuando se tiene una planificación y estrategia definida para este ámbito se mitiga los riesgos como redes con sobrecarga, problemas con el router, delitos cibernéticos o la perdida de datos, en definitiva, el monitoreo permite identificar los elementos de red utilizados o subutilizados, solucionar fallas en la red que son mínimos, identificar amenazas de ciberseguridad y de manera especial proteger los datos. A esto se suma la posibilidad de analizar el rendimiento de la red y evitar las interrupciones en la red.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. MARCO TEÓRICO

2.1 Marco Teórico

GNS3 es un simulador que se basa en IOS Cisco por lo que puede diseñar topología avanzadas de red y probar el funcionamiento antes de alguna implementación tecnológica. Este tipo de herramienta es muy útil y sobre todo amigable para el simular soluciones e implementar escenarios de pruebas. Para el buen funcionamiento de la GNS3 en un PC se debe contar con una capacidad mayor a 8G de memoria y que el programa pueda ejecutarse sin ningún problema. (Vera, 2014).

Esta herramienta que sirve a los profesionales que trabajan en redes y también a los estudiantes en la ejecución de laboratorios, en la estructuración de proyectos cuyo objetivo es la simulación de escenarios de pruebas para solucionar algún tipo de problemas. (Vera, 2014).

Al ser una aplicación tecnológica de código abierto tiende a tener ciertas dificultades sobre todo en la simulación de equipos más robustos como usados en el CORE de un Service Provider.

Icinga2 es una herramienta que facilita también el monitoreo de red de código abierto y que tiene mucha aceptación a nivel mundial. Está basada en los estudios y trabajos realizados por Nagios Core. Se conforma por un API RESTful flexible con lo que se puede ingresar configuraciones propias e identificar datos de rendimiento on line, en vivo en un tablero. En esta herramienta también se puede establecer panales personalizados, por lo tanto, se puede escoger la información que se requiere monitorear (Opensource, 2020)

El visualizar un área en donde se implementa esta herramienta funciona bien, es decir, tiene un soporte para Graphite e Influx DB, que puede transformar los datos de los rendimientos en gráficos con todas las funciones para analizar los rendimientos de manera más precisa (Opensource, 2020).

Icinga2 permite además el monitoreo de datos de rendimientos históricos y on line, tiene un sistema de alertas para el seguimiento en vivo y se configura para que envíe notificaciones de los problemas de rendimiento ya sea por mensajes de texto o correo electrónico. Es una herramienta gratuita (Opensource, 2020).

La topología de una red se define como ciertas disposiciones que tiene la misma, que incluye los nódulos y los enlaces. Están dos procedimientos de delimitar la arquitectura de red: la topología lógica y física. La topología física de una red se consiste en el diseño real de las estaciones de trabajo, en este sentido, existen varias tipológicas que se mencionan a continuación (Computerweekly, 2019)

La topología de red en estrella, que se caracteriza por que se encuentra un computador base al que las estaciones de trabajo se conectan en forma directa, sin embargo, cada puesto laboral se encuentra conectadas indirectamente por medio de la computadora central (Computerweekly, 2019).

Otra topología física es la denominada de red de bus, que se define porque cada puesto de trabajo se conecta por un cable llamado bus, por lo cual algún puesto de trabajo se conecta claramente a otro puesto de la red (Computerweekly, 2019).

La topología de red de malla usa dos diseños, la red completa y la red parcial, en la de red completa, cada puesto de trabajo se conecta de manera directa a los otros puestos de trabajo y en la red parcial no todos los puestos están conectados a los demás y algunos están conectados

a otras por medio de nodos con los que comparten información específica (Computerweekly, 2019).

Otra topología es la denominada red de árbol que usa múltiples redes con estrella interconectadas. Los computadores o PCs centrales de las redes se conectan a través de un bus principal (Computerweekly, 2019).

Finalmente, se pude señalar la topología lógica que identifica la naturaleza que tienen las señales de nodo a nodo, por ejemplo, algunas redes se estructuran en estrella y funciona como redes de bus (Computerweekly, 2019).

Para complementar este ámbito, para el buen manejo de la información empresarial es necesario contar con redes de comunicación que sean apropiadas y sobre todo efectivas para compartir y proteger los datos e información. Hay otro tipo de clasificación de las redes que pueden ser centralizadas y descentralizadas, en las redes centralizadas la comunicación gira sobre una persona que es la responsable de liderar los procesos y funciona como eje de otros funcionarios de una empresa y en la descentralizada, la comunicación fluye entre todos los funcionarios de una empresa sin tener un líder o un jefe (Computerweekly, 2019).

Además, existe la red en cadena, que usan las empresas que requieren el procesamiento de la información tomando en cuenta la organización institucional por lo cual el intercambio de información se da entre los usuarios más cercano y por otro lado se tiene la red en estrella que se utilizan en empresas con una dinámica de mando vertical, es decir el usuario ocupa lo central y los funcionarios están a su alrededor (Computerweekly, 2019).

Otra red que se puede describir es la de en círculo, que permite intercambiar la información de un usuario a otro hasta llegar al origen. La desventaja es que cada uno de los usuarios de la red posee contactos directos (Computerweekly, 2019).

La implicación de las zonas de red LAN, DMZ y SERVIDORES privados guardan una relación directa en la topología de estrella, debido a que pueden canalizar y centralizar información a partir de un nodo, el cual guarda relación con las partes a través de un firewall de seguridad establecido por zonas. Los elementos que forman parte de la topología son:

- **Routers**: Enrutan los datos de la red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transferencias simples, como interacciones web.(Cumbal et al., 2021).
- **Switches:** Facilita conectar distintos equipos y nodos en la red, siempre cableados, y es notable tener en cuenta. En cambio, un conmutador siempre conectará dispositivos a la red de área local, ya sabes, lo llamamos LAN (La Red & Peláez, 2020).
- **Servidores:** En lenguaje informático, un servidor o server es una computadora y sus programas que sirven a otras computadoras. El servidor participa y responde a las solicitudes de otras computadoras. Otras computadoras que le hacen solicitudes se convierten en "clientes" del servidor (Alcívar, 2019).

2.2.1. Networking

La repartición de direccionamiento a nivel WAN para Inaquiza (2019) habla que la red de datos sobre MPLS, permite la intercomunicación entre los PEs y Ces, por cuanto se deben determinar distintos esquemas de direccionamientos con máscara /30 en base a la subred para establecer la primera IP es el PE y la segunda IP es el CE, como estándar. Para la red de datos se establecen dos tipos de subredes las cuales son para el enlace primario y de backup, lo que permite establecer conexiones con diferentes PEs sobre el protocolo dinámico BGP Inaquiza (2019).

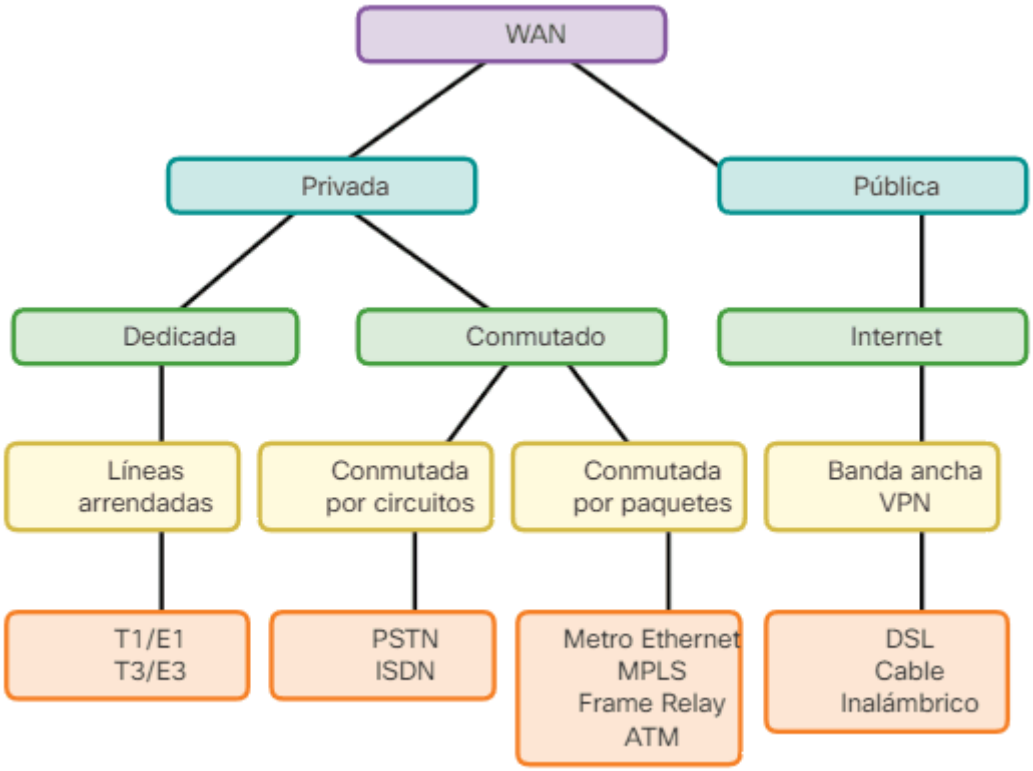

Figura 1: *Opciones de conexión de enlaces WAN*

Nota: La imagen fue obtenida de: **(CCNA, 2020)**

Generalmente se utiliza una red WAN cuando se tiene un área geográfica grande, se debe recordar que se paga al proveedor por el servicio incurrido.

2.2.2. Direccionamiento de la Red

Es una compilación de mecanismos que transmiten recursos con cada dispositivo, los cuales deben estar definidos con una dirección IP que puedan interconectarse entre sí.

Las direcciones IP se representan en formato binario, es decir, un conjunto de 32 bits, que a su vez se dividen en 4 conjuntos de 8 bits, denominados octetos, para la comodidad del cliente, las direcciones IP se representan en el formato decimal. Un cierto número de bits plantear la parte de la red, y otro conjunto de bits representa la parte del host; es la máscara de red la que realiza esta separación. Los dispositivos en una red igual pueden informar sin colocar una puerta de enlace o puerta de entrada. Una entrada que sirve para enlazar es un aparato que sabe cómo acceder a una red remota. En la actualidad se manipula subredes con máscaras de

longitud variable VLSM, las cuáles pueden destinar el número de host adecuado a la red sin perder tiempo en su direccionamiento.

2.2.3. Software de redes GNS3

GNS3 es un software que le permite simular, diseñar y construir topologías o escenarios de red en un entorno controlado antes de la implementación, lo que le permitirá configurar su red sin comprometer su red en funcionamiento. Este software es una herramienta de simulación avanzada que permite simular redes de acceso utilizando tecnología SD-WAN (Díaz Saravia, 2017).

En otras es un simulador de redes que tiene por objetivo diseñar topologías complejas de redes y poner a prueba las simulaciones, teniendo la posibilidad de escoger los elementos indispensables de las redes diseñadas.

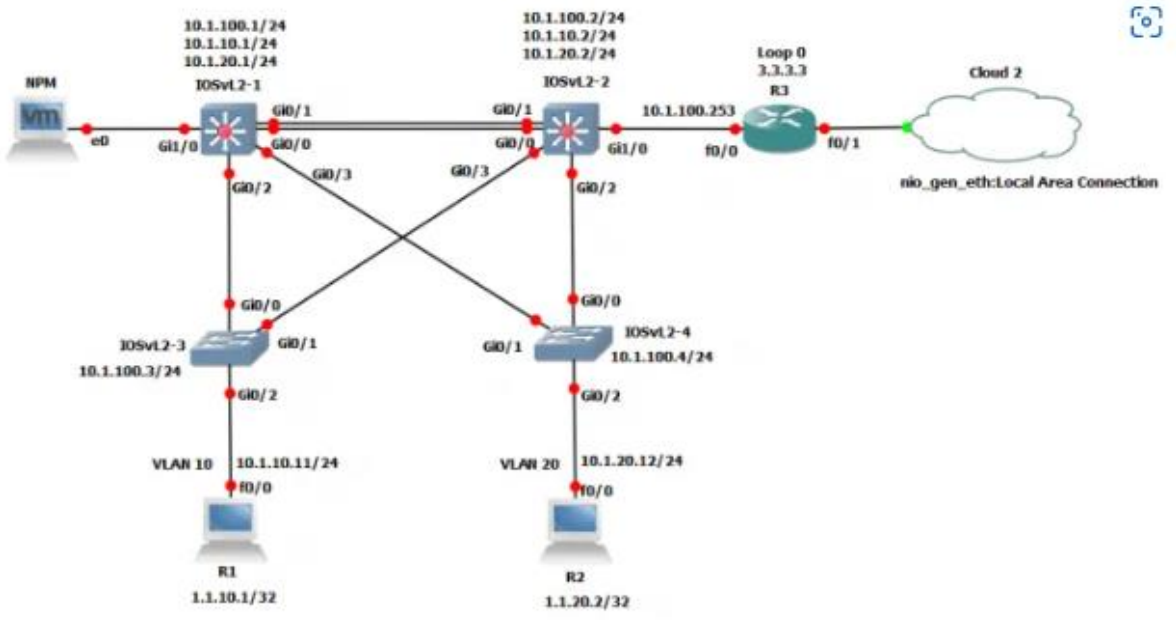

Figura 2: *Topología de entorno GNS3*

La imagen fue obtenida de: (Telectrónika, 2018)

El software tiene varias funciones que lo distinguen de otros programas similares, este software admite dispositivos simulados y emulados:

- **Emulación:** GNS3 emula el hardware de la máquina y ejecuta la imagen real en la máquina virtual.
- **Simulación:** Características y funciones de dispositivos como los interruptores analógicos NS3. No está ejecutando un sistema operativo real, sino un dispositivo emulado desarrollado por GNS3.

La instalación de este software, requiere una serie de requisitos que se muestran en la siguiente tabla:

Tabla 1. *Requisitos Mínimos del GNS3*

Requerimientos Mínimos	
Sistema Operativo	Sistema (Windows 7 o posterior), IOS (Maverick 10.9 o posterior), Distribución Linux, Debian, Ubuntu
Procesador	Procesador con 2 o más núcleos / extensión de virtualización
Memoria	Mínimo de 4 GB de RAM
Almacenamiento	Espacio mínimo de 200 MB – Recomendado 1 GB
Adicionales	El almacenamiento de imágenes, requiere más espacio en el equipo (disco duro)

Fuente: (Díaz Saravia, 2017)

2.2.4. Máscara de la Subred

Una máscara de subred, como una dirección IP, es una serie de números binarios de 32 bits dividido en octetos de 8 bits, cada octeto se encuentra separado por un punto, razón por la cual hay 4 octetos; la tarea principal de la máscara es interpretar cuál es la red y la parte del host de una determinada dirección IP.

Según Luke (2019) las máscaras de subred de longitud variable permiten ajustar el tamaño en bits de la parte host al número de hosts que se desean alojar en cada red. Esto,

consecuentemente, lleva también a un ajuste del tamaño en bits del prefijo de la subred, de ahí el nombre: Máscara de subred de longitud variable [RFC 1519],[RFC 1878]. Lo que se persigue es paliar el desperdicio de direcciones IP que se produce debido al método de generar las subredes y para paliar los efectos del reparto ineficiente. (p. 6)

Al aplicar VLSM, la dirección de red debe agregarse con la máscara de red, la cual indica qué parte es el prefijo y qué parte corresponde al host. Por lo tanto, se ha introducido una nueva notación para las máscaras de red, lo que hace que sea más fácil trabajar con ellas CIDR. El símbolo solo está representado por la dirección de red que lo acompaña y números separados por / que representan la longitud del prefijo o el mismo número de bit "1" en la máscara de red.

2.2.5. VLSM y CIDR

Históricamente el tratar de redes con clase, esto es, siempre direcciones IP pertenecientes a la clase A, B o C, y las máscaras para estas clases son fijas: /8, /16, /24 de manera respectiva.Esta problemática con las redes clásicas es que las direcciones IP se desperdician, tal es el caso que, se requieren 10 direcciones, se debe usar una red de clase C, la misma que dispone de 254 direcciones disponibles.

CIDR significa Class Inter Domain Routing, es sinónimo de resumen, el cual crea por lo general superredes. Después de que el marco llega al enrutador, se debe verificar la tabla de enrutamiento, que muestra un mejor trayecto para llevar el paquete a origen, verificando el formulario del desarrollo, el enrutamiento consume recursos informáticos, por lo que es más representativo si su latencia es baja.

2.2.6. Dynamic Host Configuration Protocol (DHCP)

Representa el protocolo de configuración dinámica de host, admite los terminales conectados a la red se puedan realizar dinámicamente los parámetros de red como dirección IP, máscara

de subred, puerta de enlace o sistema de nombres de dominio. Existe un modelo cliente/servidor en el servicio DHCP, como se puede observar en el diagrama, el usuario emite una solicitud de difusión (a todo dispositivo de red), el servidor responde a la petición del cliente.

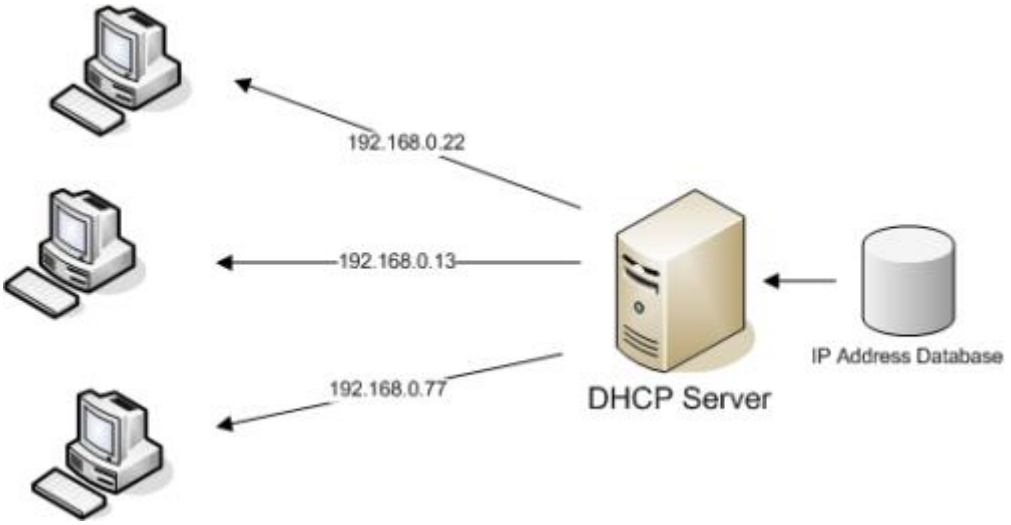

Figura 3: *Funcionamiento de DHCP*

Nota: La imagen fue obtenida de: **(Berrocal, 2018)**

La ventaja es que puede controlar, a la vez que se puede asignar direcciones, en la red, las direcciones IP ya no se pueden repetir, lo que causará inconvenientes y no podrá usar los recursos de la red en algunas de las máquinas establecidas.

2.2.7. Protocolo SMTP

La suplantación de correo electrónico es posible porque el (SMTP) que en sus siglas se traduce en protocolo simple de transferencia de correos, es principalmente el protocolo utilizado para enviar correo electrónico no incluye un mecanismo establecido para verificación. (Molina et al., 2019) consideran que esto permite que los clientes SMTP puedan comunicarse con servidores de correo, aunque no siempre se toma esta precaución. Por lo general, una persona con los conocimientos necesarios puede tomar las precauciones adecuadas. A través de conectarse al servidor y utilizarlo para remitir mensajes a través del envío de correos

electrónicos, entre los cuales los objetivos también pueden estar la suplantación de identidad, en la que el remitente inserta el comando en el encabezado del mensaje para cambiar y alterar el destino implícito de la comunicación.

El protocolo SMTP según Montúfar (2021) es responsable de transformar las alertas del servidor de monitoreo recibidas a través de SMTP, en llamadas telefónicas, llamadas VoIP, SMS o correo de retransmisión. Las cuales están destinadas para realizar llamadas y enviar SMS, los dispositivos de forma general suelen utilizar módulos USB a UART los cuales intercambian información con el resto de los módulos a través de la utilización de comandos AT. En SMS, solo está involucrada la utilización de comandos AT, mientras que, durante las llamadas telefónicas, los comandos AT se utilizan para marcar el número de teléfono especificado y de esta manera poder monitorear el estado de la llamada.

2.2.8. TCP/IP

Es importante considerar que existen diversas formas para la detección de presencia Conexiones TCP activas entre cualquier red de clientes y servidores Linux remotos que usan mensajería a través de canales presentes en la implementación del kernel de Linux cuyos valores IPID IPv4 globales se realizan por conexión. Para lo cual los requisitos de ataque son los siguientes:

– El servidor es una máquina Linux que ejecuta el kernel 4.0 o posterior.

– Acceso a múltiples direcciones IPv4 para usar como atacante dirección.

Para (Geoffrey et al., 2019) el ataque explota el comportamiento RST de Linux en respuesta a SYN/ACK "no solicitados". Este es el comportamiento predeterminado del kernel de Linux, y Descrito en RFC como el comportamiento correcto para manejar SYN/ACK "no solicitados".

Un "no invitado" SYN/ACK es el SYN/ACK para ningún SYN enviado, y Entonces no representa una conexión potencial.

Al detectar cuando el kernel de Linux cambia usando uno de sus 2048 contadores IPID globales para usar el contador IPID TCP por conexión, el ataque es capaz de deducir el puerto IP correspondiente a 4 una conexión TCP activa, no un observador en la ruta. La tupla de 4 puertos IP que representa el TCP activo de la conexión es la dirección de origen, el puerto de origen, la dirección de destino y el puerto de destino en comunicación TCP.

2.2.9. Modelo OSI

Con la Industria del internet 4.0 (inteligencia artificial, big data, aprendizaje automático, entre otros) y su impacto en la sociedad. El tema de la seguridad en la red para (Chaparro et al., 2021) ha comenzado a tomarse de forma más importante y se ha convertido en una prioridad para las organizaciones que han implementado políticas, procedimientos y técnicas enfocadas en mitigar los riesgos cibernéticos. Pero cuando se trata de seguridad red, todavía hay muchas deficiencias, porque el principal problema de las organizaciones es que la jerarquización, es decir el nivel superior del modelo OSI se centra en dejar las capas inferiores en segundo plano en lo que respecta a la generación de un desfase que es la seguridad de la infraestructura interna de la organización, ya que esto podría ser un vector de ataque ciberdelincuentes.

El estándar OSI de siete capas es un modelo conceptual para describir y estandarizar la comunicación de redes de datos y telecomunicaciones para la interoperabilidad. (Rivera, 2019) considera que después de las décadas de 1960 y 1970, nacieron muchos protocolos de comunicación, muchas veces incompatibles y heterogéneas patrocinados por diferentes proveedores, allí surgió la necesidad de estandarizar modelos, diseñar, establecer estándares, para después de varios años de arduo trabajo y ardua labor por parte de diversas organizaciones internacionales como ISO, ITU-T, IEEE, etc., pueden publicar y alojar un documento marco

denominado "Modelo de referencia OSI Modelo de referencia de interconexión de sistemas abiertos)" usando ISO/IEC 7498- 1:1994 o ITU-T X.200.

2.2.10. Enrutamiento estático

El enrutamiento estático admite a los jefes de red optar un camino para cada enlace de red de origen y de destino. (Romero, 2019, p. 27) Cuando los usuarios de la red aplican dichas rutas, configuran manualmente rutas estáticas para llegar a una red específica mediante la determinación de la dirección de la red vecina, la máscara y la dirección IP del próximo salto, que es diferente de los protocolos de enrutamiento dinámico. Intercambian sus caminos internamente con otras redes con diferentes direcciones IP. Las rutas estáticas no se cambian automáticamente y deben reconfigurarse manualmente cuando cambia la topología de la red.

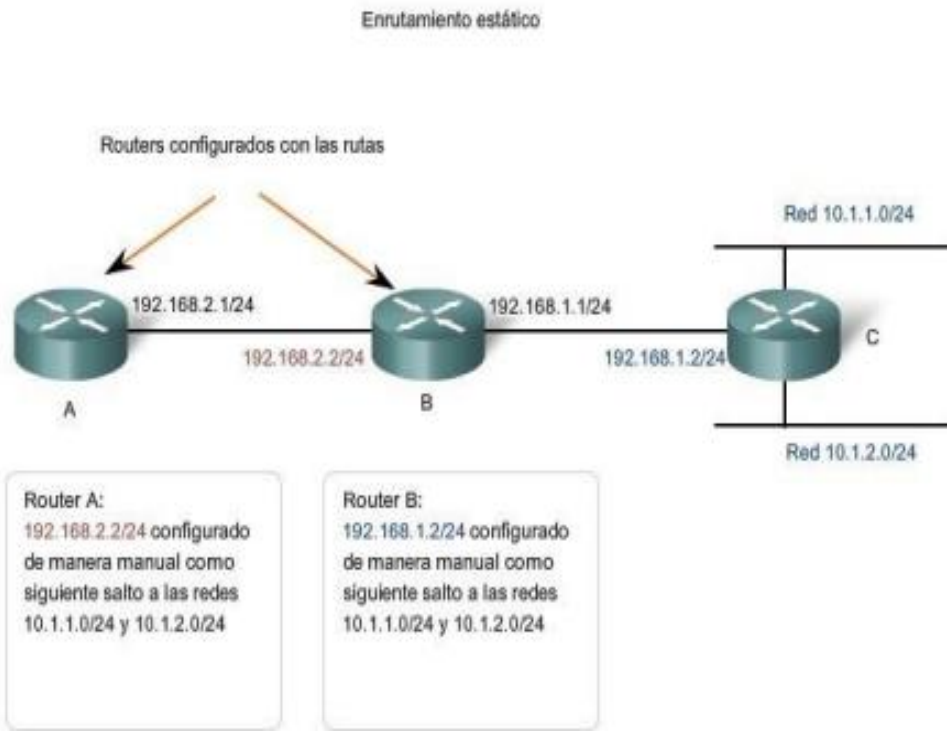

Figura 4: *Enrutamiento estático*

Nota: Obtenida de **(Romero, 2019)**

2.2.11. Enrutamiento Dinámico OSPF

Es el protocolo de enrutamiento más manejado en la actualidad, el cual está destinado para redes de datos ya que presta simplicidad, adaptabilidad y un rendimiento eficaz frente a cambios de topología. En las redes de datos cotidianos, los protocolos de enrutamiento se ejecutan en cada enrutador y los administran allí a través del plano de datos y plano de control.

La lógica existente en cada nodo cuando falla un enlace de red los enrutadores deben actualizarse, lo que da como resultado que el tráfico de control inunde la red, a través de anuncios de estado de enlace (LSA) esto sigue pasando para mantener la tabla de enrutamiento siempre actualizada.

Con la llegada de las redes definidas por software (SDN), las actualizaciones de la tabla de enrutamiento son más flexibles porque SDN separa el plano de datos y de control lo que permite que se gestionen los dos planos respectivamente. (González & López, 2019) consideran que este nuevo modelo de gestión combina el controlador, el nodo principal de la red, la cual es responsable de gestionar y mantener una comunicación continua con todos los conmutadores de red para obtener una visión centralizada y global de la red.

2.2.12. Monitoreo de redes

Bayas (2015) el monitorio de redes lo describe como el proceso de capturar, procesar y analizar paquetes de datos transmitidos o recibidos a través de una red informática. Se pueden analizar varias métricas de estos paquetes, como la utilización del ancho de banda, la tasa de pérdida de paquetes, la cantidad de desconexiones, etc.

Para el monitoreo se utilizan software especializado que recopila los datos de la red, los analiza y proporciona información sobre el rendimiento. Se puede utilizar para una variedad de propósitos, como:

- Ayudar a operadores a diagnosticar y solucionar problemas
- Detectar problemas de rendimiento en redes
- Supervisar el rendimiento de las redes
- Alertar a operadores sobre ocurrencia de problemas

Para el monitoreo de las redes se utilizan varios protocolos que verifican el funcionamiento normal de las redes, para Junco & Rabelo (2018) un protocolo es un conjunto de reglas para que los mecanismos de red se compartan entre sí. Los sistemas de monitoreo de red utilizan protocolos para identificar y reportar problemas de rendimiento de la red. Los tipos de protocolos son:

- SNMP: protocolo simple de administración, en capa de aplicaciones, usada para llamada y respuesta de dispositivos switches hasta impresoras.
- ICMP: protocolo utilizado para enviar información y operaciones de IP en dispositivos.
- Protocolo de Detección de Cisco: protocolo que detecta la administración de dispositivos, utilizando diferentes protocolos de capa de red.

2.2.13. Diseño de servicio

Es diseñar un servicio transformado para su introducción en el mundo real, incluida su arquitectura, procesos, políticas y documentación, para cumplir con las obligaciones comerciales, funcionales y de calidad acordados. (Casanova & Saavedra, 2018) Algunos de los requisitos que se deben tener en consideración para la implementación del diseño son:

- **Gestión del catálogo de servicios:** en este apartado se gestiona la información referente a los servicios de operación que necesitan ser ejecutados.

- **Gestión de niveles de servicio:** se utiliza una escala para medir el nivel de ejecución de los servicios actuales y se deja establecida una medida para futuras referencia de este tipo.
- **Gestión de la capacidad:** como su nombre lo indica en esta actividad se administra la capacidad del sistema TI para asegurar el costo de todas las áreas estudiadas.
- **Gestión de la disponibilidad:** se gestiona toda actividad y su disponibilidad para futuras referencias, sean para recursos, medición u objetividad.
- **Gestión de la continuidad de los servicios:** Es una evaluación y control total de los servicios TI, se realizan procesos de guía continua a todo.
- **Gestión de la seguridad de la información:** En este apartado se alinea todo lo referente a los servicios de TI y el negocio a evaluar.
- **Gestión de proveedores:** Aquí se asegura que toda actividad relacionada con los proveedores sea utilizada por la empresa y de igual forma sea acordada para cumplir con los objetivos de esta.

2.2.14. Transición de servicio

Facilita orientación para desarrollar y mejorar la capacidad de convertir servicios nuevos y cambiados en operaciones. Brinda orientación sobre cómo ejecutar de manera efectiva las circunstancias de una estrategia de servicio en las operaciones de servicio, al mismo tiempo que controla el riesgo de fallas e interrupciones.

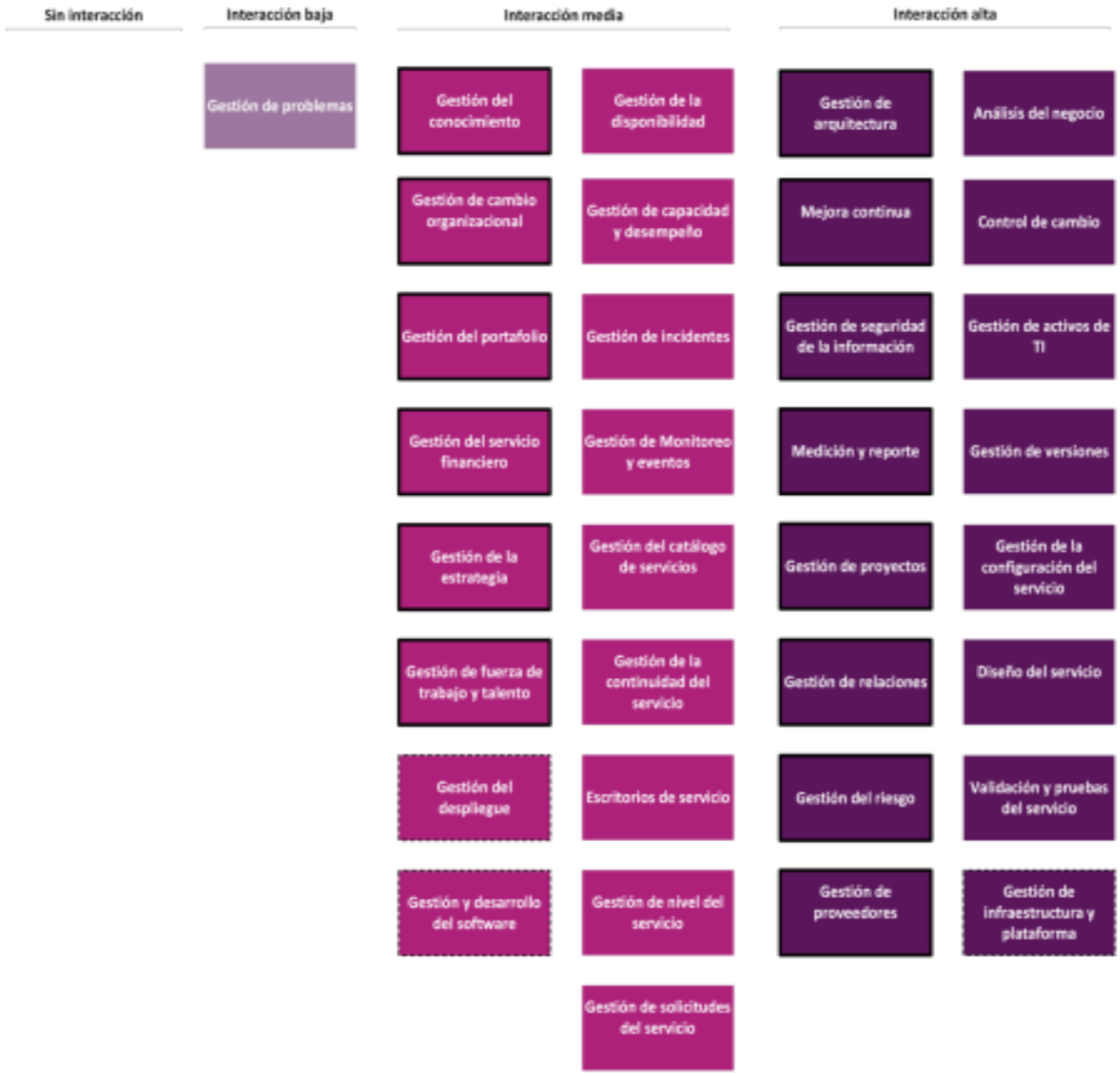

Figura 5: *Plantilla para la actividad de transición de servicios*

Nota: Obtenida de **(Salamanca, 2019)**

2.2.15. Mejora continua de servicio

El objetivo principal del mejoramiento en el servicio es disponer constantemente los servicios de TI con los requisitos comerciales es identificar oportunidades de mejora para respaldar los procesos comerciales, encontrando formas de aumentar la eficiencia y reducir los costos.

La mejora continua de los servicios no puede entenderse como una fase separada. Sus actividades deben ejecutarse durante todo el ciclo de vida. Cada etapa del ciclo de vida produce

salidas que sirven como entradas para la siguiente etapa. Una estrategia de servicio informa la visión empresarial, los servicios que necesita la organización y los requisitos identificados para nuevos servicios o cambios en los servicios existentes. (Cestari et al., 2015)

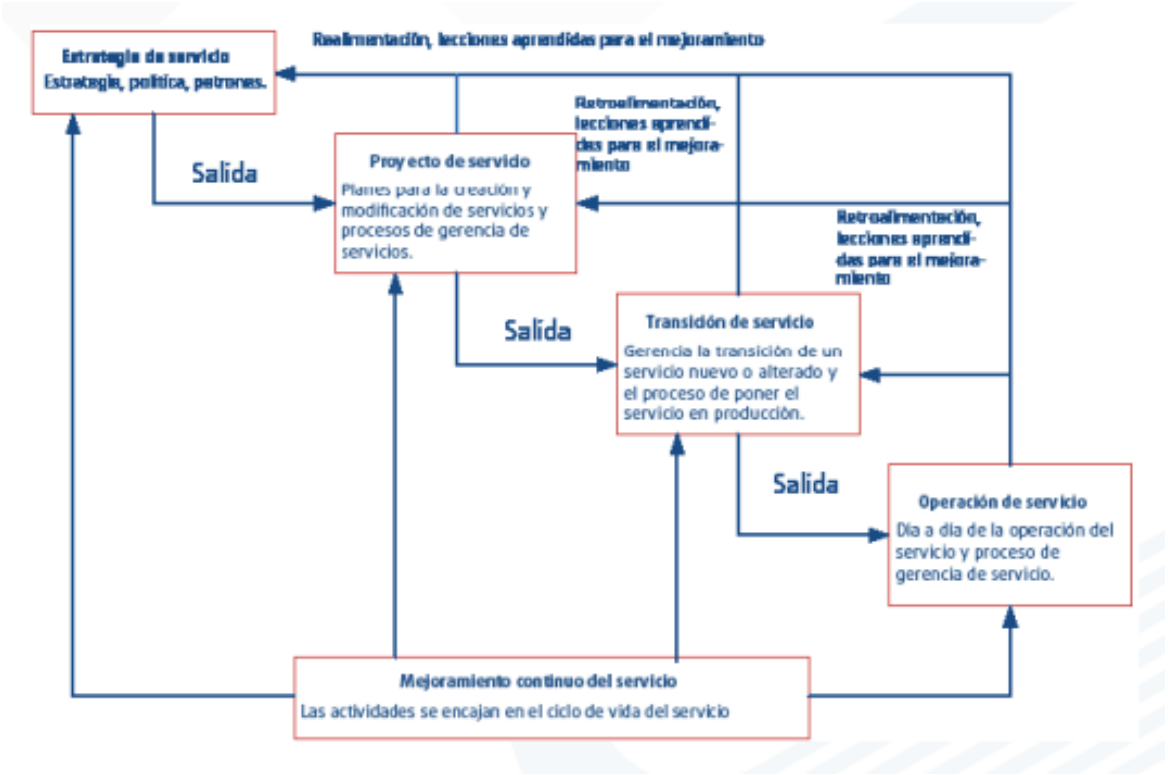

Figura 6: *Diagrama del proceso de mejoramiento continuo*

Nota: Obtenida de **(Cestari et al., 2015)**

Básicamente, en este método se verifica el logro de los parámetros del proyecto, lo que significa que, si no se ha logrado, es necesario realizar algunas tareas que no se completaron o se realizaron en su totalidad en la fase anterior (Pérez T. , 2021, p. 71)

Los parámetros de calidad se cuantifican para que se puedan hacer los ajustes pertinentes cuando corresponda o notificar al área semejante en corregir cualquier deficiencia. En este período, también debe haber mecanismos establecidos para monitorear constantemente los datos y elementos más sensibles del sistema para evadir desequilibrios o desviaciones del propósito subyacente.

2.2.16. Topología Estrella

Se refiere al camino a través del cual siguen las señales por medio de la topología física, a partir de la forma en que los sitios se comunican a través del medio físico. Estas estaciones permiten la comunicación entre sí, de forma directa o indirectamente, siguiendo una ruta determinada a través de las condiciones de cada momento. De acuerdo a las características de los equipos desplegados en la entidad, y las correspondientes condiciones estructurales descritas, se definen al utilizar la estrella como topología. De forma general en una red LAN que utilice esta topología, en cada estación están directamente conectadas a un nodo central, de forma general por medio de dos enlaces punto a punto. El cual se centra en uno para enviar y otro para recibir.

Una topología de tipo estrella extendida es lo equiparable o lo mismo que una topología en estrella, excepto en que cada nodo conectado a un nodo central de forma seguida también es el medio de otra estrella. Normalmente, el nodo base está ocupado por un conmutador, y los nodos esclavos están siendo utilizados por un concentrador. La topología en estrella es considerada una de las más utilizadas ya que su simplicidad al momento de implementar y su correspondiente flexibilidad a la escala de la red. (Mendoza, 2021)

La adaptabilidad de la topología en estrella a la configuración de las empresas depende de la arquitectura de la red, la cual se basa en una topología en estrella. En cuyo módulo central XBee se conecta al puerto COM virtual de la PC. En una PC, se ejecuta la interfaz de usuario desarrollada en C# utilizando el entorno Visual Studio basado en interfaz Gráficos de Windows Forms (Cerezuela et al., 2021).

CAPÍTULO 3

3. Análisis y monitoreo a través de los servicios tecnológicos utilizando el emulador de redes gns3 por medio de la plataforma Icinga2.

3.1. Modelado del monitoreo de una topología en red para empresas tecnológicas

Es una topología que consta de un nodo central de donde salen otros enlaces a otros nodos a través del cableado. El nodo central cumple la función de hacer circular toda la información en la red. Cabe señalar que esta red diseñada en base a este enfoque no realiza ningún tipo de interconexión de computadora a computadora ya que toda la información pasa a través de un nodo central. (Cumbal et al., 2021)

Por lo tanto, la topología propuesta a este trabajo de investigación es una topología en estrella, que se detalla a continuación, y que consta de tres zonas:

- Zona de SERVIDORES
- Zona DMZ
- Zona de res LAN 1

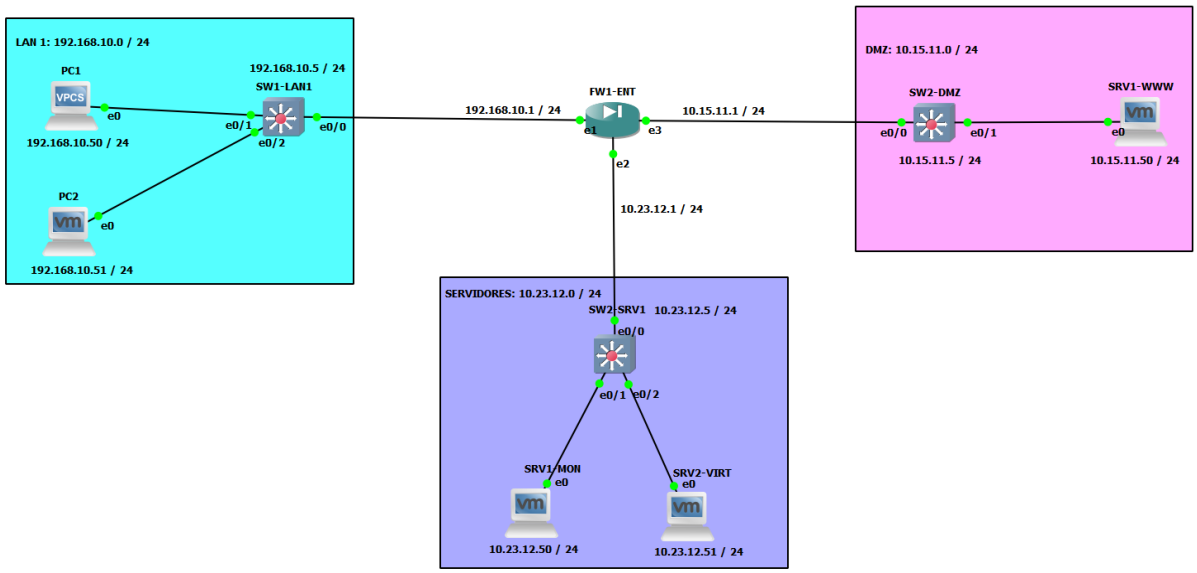

Figura 7: *Topología en Estrella*

Para descargar se utilizar a https://www.gns3.com/ donde se encuentra el botón “Free Download”, se pulsa él botón click para continuar, optar entre Windows, Mac o Linux:

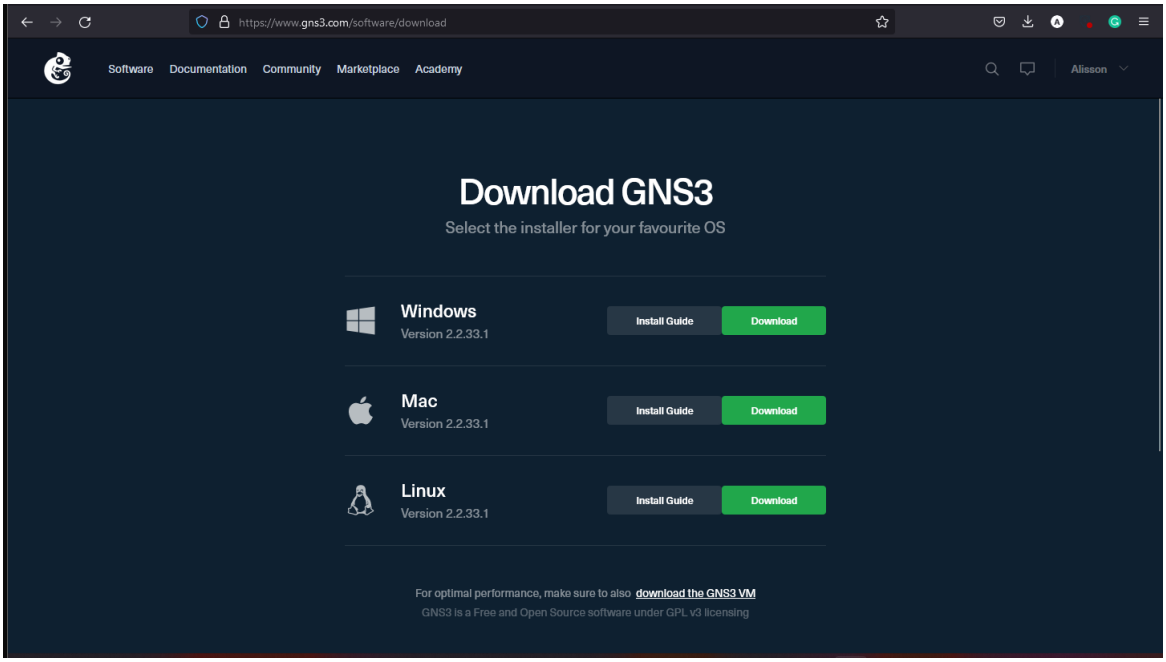

Figura 8: *Análisis de la tecnología GNS3 para la emulación de redes*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Cuando se complete la descarga, el archivo se ejecutará, luego solicitará derechos de administrador, presione aceptar y se obtiene la siguiente pantalla como se muestra en la Figura, esto indica el acuerdo de licencia para que se realice la instalación de GNS3. Haga clic en I Agree:

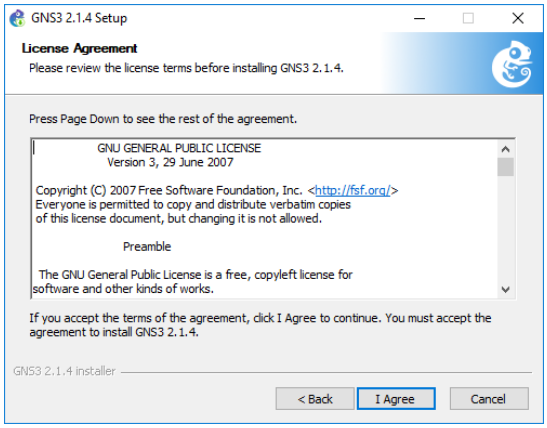

Figura 9: *Análisis de la tecnología GNS3 para la emulación de redes a*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

El acceso directo va a ser direccionado en el menú de inicio, va a hacer la forma predeterminada:

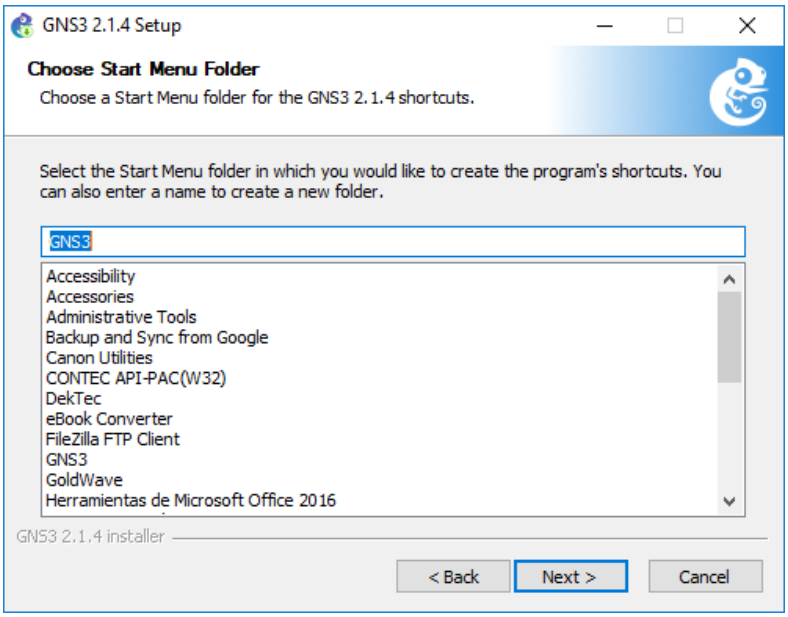

Figura 10: *Análisis de la tecnología GNS3 para la emulación de redes b*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Selección de componentes para la instalación GNS3:

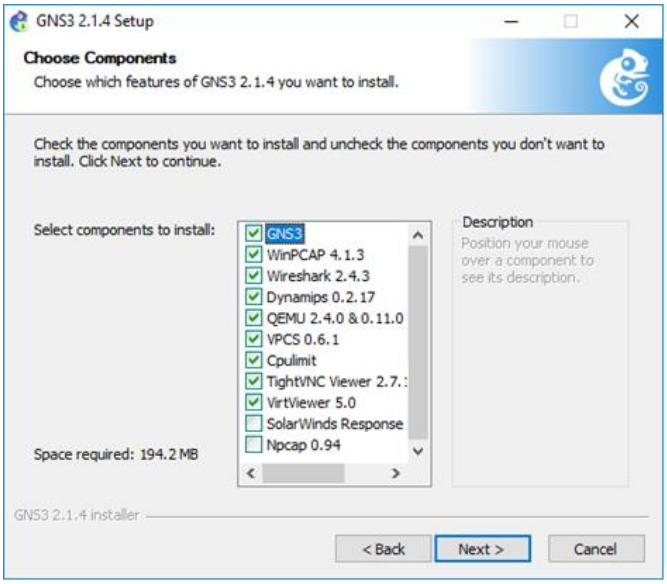

Figura 11: *Análisis de la tecnología GNS3 para la emulación de redes c*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Especifique el directorio donde se instalará la aplicación, en cuyo caso se ha dejado el directorio predeterminado:

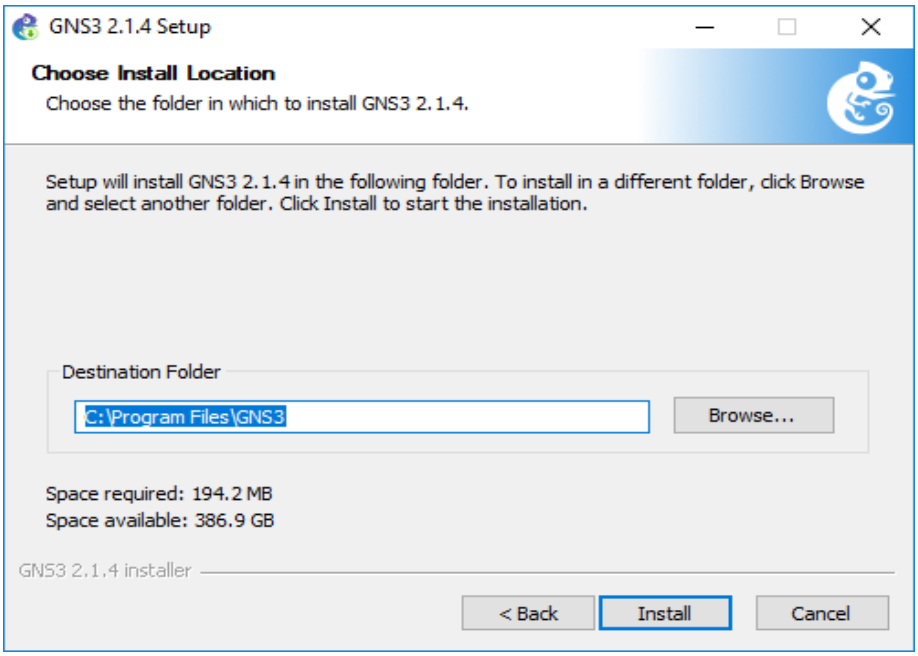

Figura 12: *Análisis de la tecnología GNS3 para la emulación de redes d*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Instalación de aplicaciones adicionales, accesos para que la aplicación funcione sin ningún conflicto:

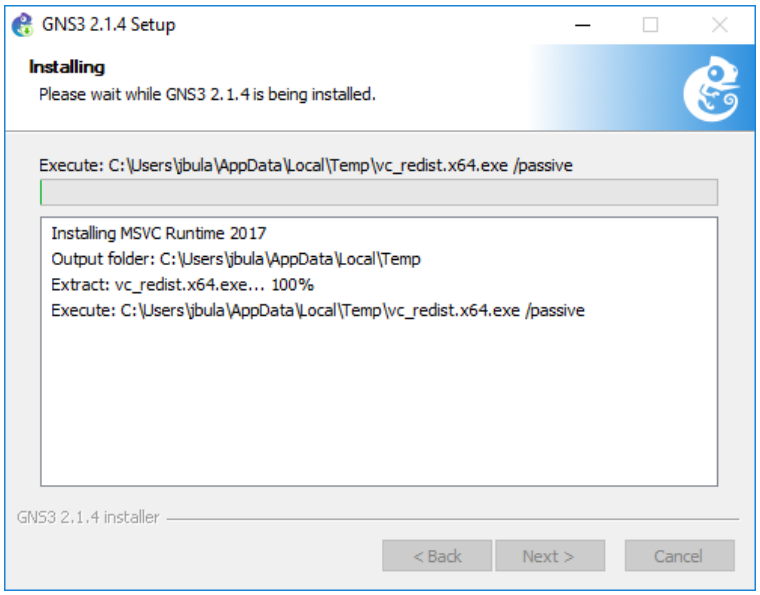

Figura 13: *Análisis de la tecnología GNS3 para la emulación de redes e*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Se requiere la instalación de una conexión a Internet para la descarga de la aplicación Wireshark:

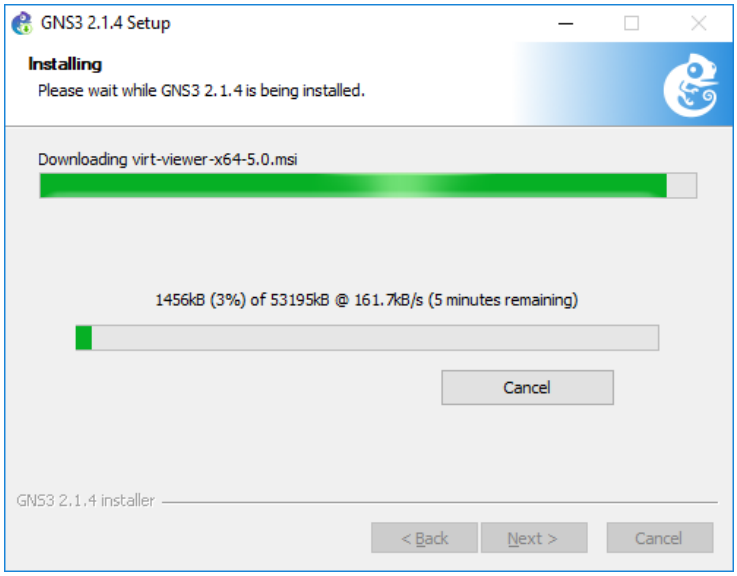

Figura 14: *Análisis de la tecnología GNS3 para la emulación de redes f*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Presionar en el botón Next para la siguiente pantalla:

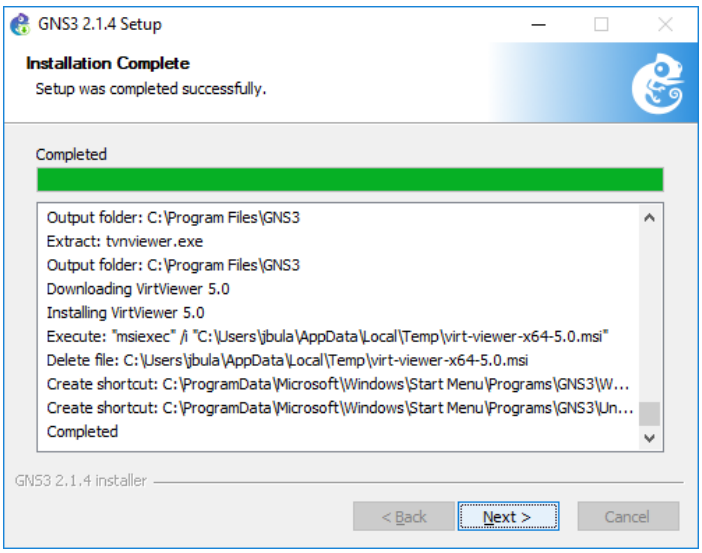

Figura 15: *Análisis de la tecnología GNS3 para la emulación de redes g*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

A continuación, aparece una pantalla que solicita instalar Solarwinds Standard Toolset, admite tareas de administración, gestión y monitoreo de redes. Por lo que se ha dejado en defecto NO y seleccionar opción Next:

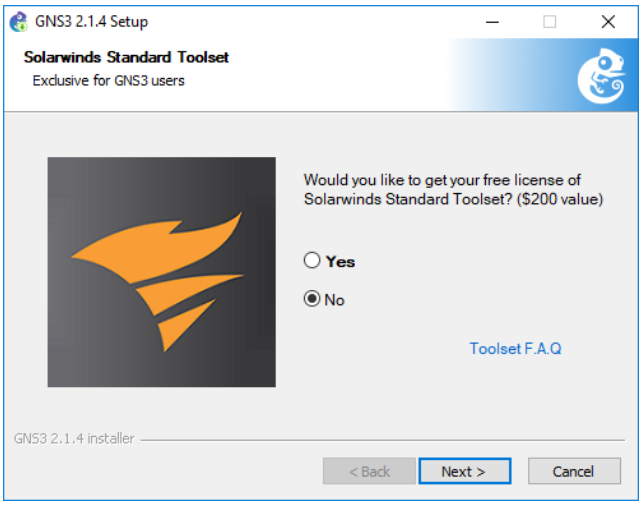

Figura 16: *Análisis de la tecnología GNS3 para la emulación de redes h*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Al final terminó instalando GNS3. Seleccione Start GNS3:

Figura 17: *Análisis de la tecnología GNS3 para la emulación de redes i*

Nota: La imagen fue obtenida en el desarrollo de la investigación mediante la descarga de GNS3

Tabla 2 *Topología Estrella Dispositivos*

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway Predeterminado
SW1-LAN1	VLAN 1	192.168.10.5	255.255.255.0	192.168.10.1
SW2-SRV1	VLAN 1	10.23.12.5	255.255.255.0	10.23.12.1
SW2-DMZ	VLAN 1	10.15.11.5	255.255.255.0	10.15.11.1
PC1	IPV4	192.168.10.50	255.255.255.0	192.168.10.1
PC2	IPV4	192.168.10.51	255.255.255.0	192.168.10.1
SRV1-MON	IPV4	10.23.12.50	255.255.255.0	10.23.12.1
SRV2-VIRT	IPV4	10.23.12.51	255.255.255.0	10.23.12.1
SRV1-WWW	IPV4	10.15.11.50	255.255.255.0	10.15.11.1
FW1-ENT	LAN 1	192.168.10.1	255.255.255.0	N/D
	SERVIDORES	10.23.12.1	255.255.255.0	N/D
	DMZ	10.15.11.1	255.255.255.0	N/D

Switches:

Los switches utilizados en la topología tienen las siguientes características, mismas que han sido tomadas de GNS3:

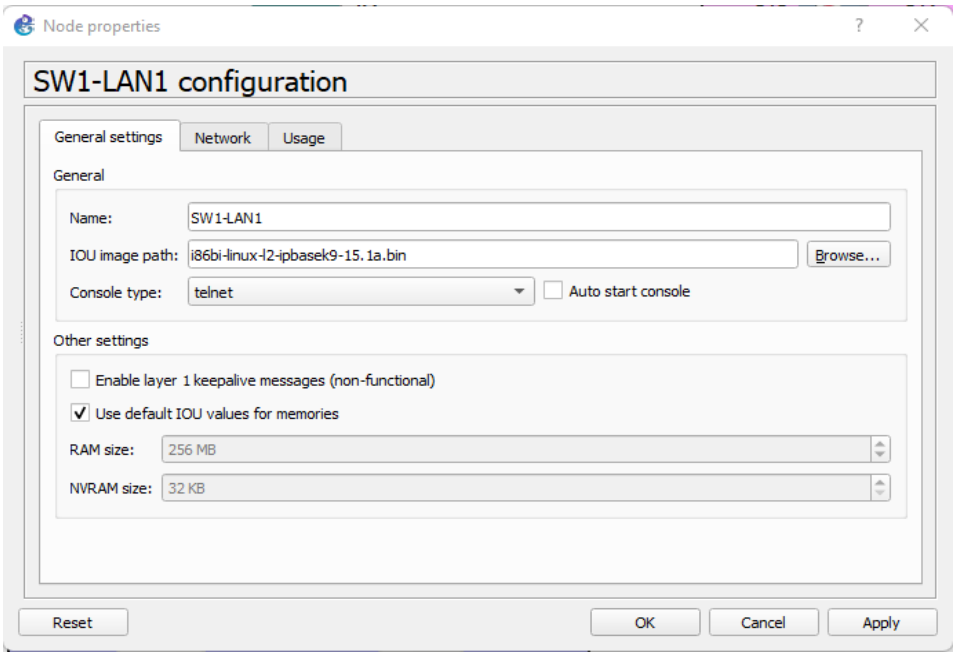

Figura 18 *Sw1-LAN1*

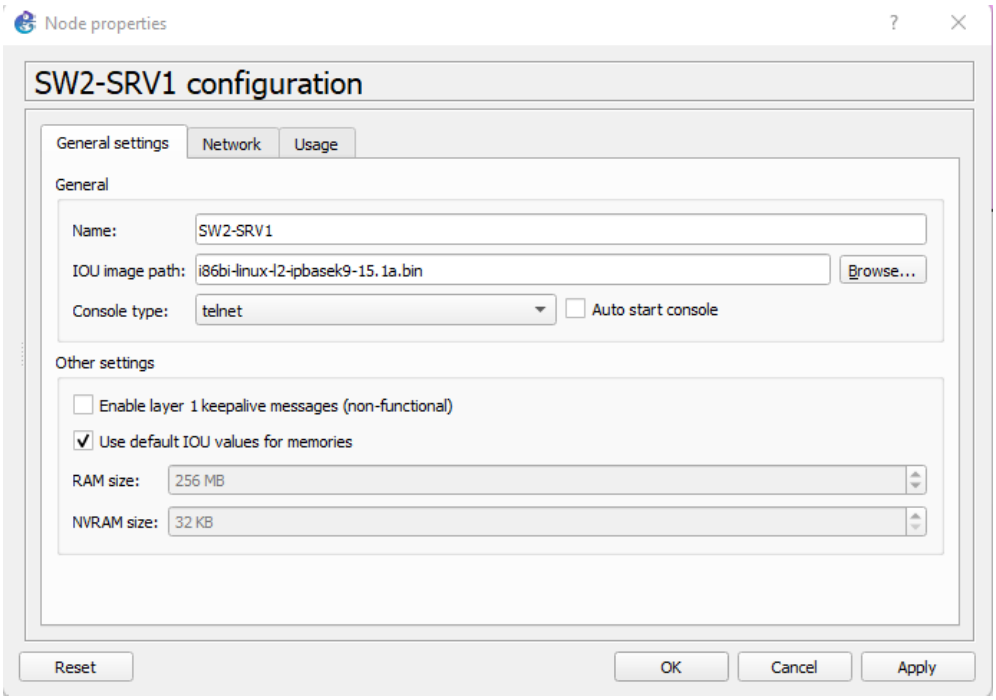

Figura 19 *SW2-SRV1*

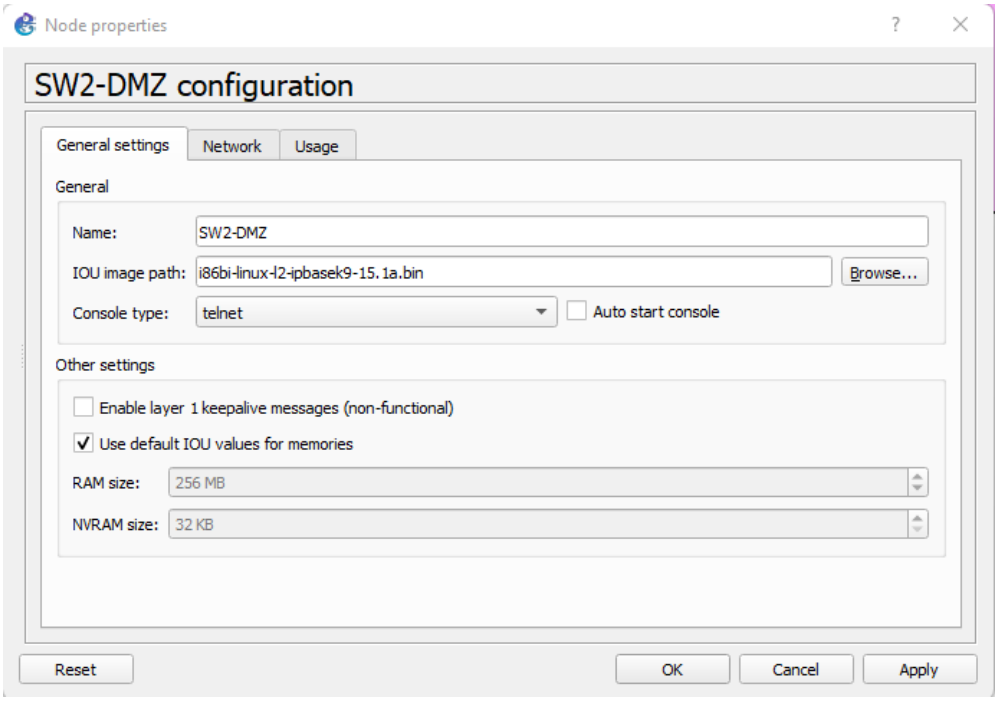

Figura 20 *SW2-DMZ*

PC's

La PC's utilizadas en la topología tienen las siguientes características, mismas que han sido tomadas de GNS3 y VMWare Workstation:

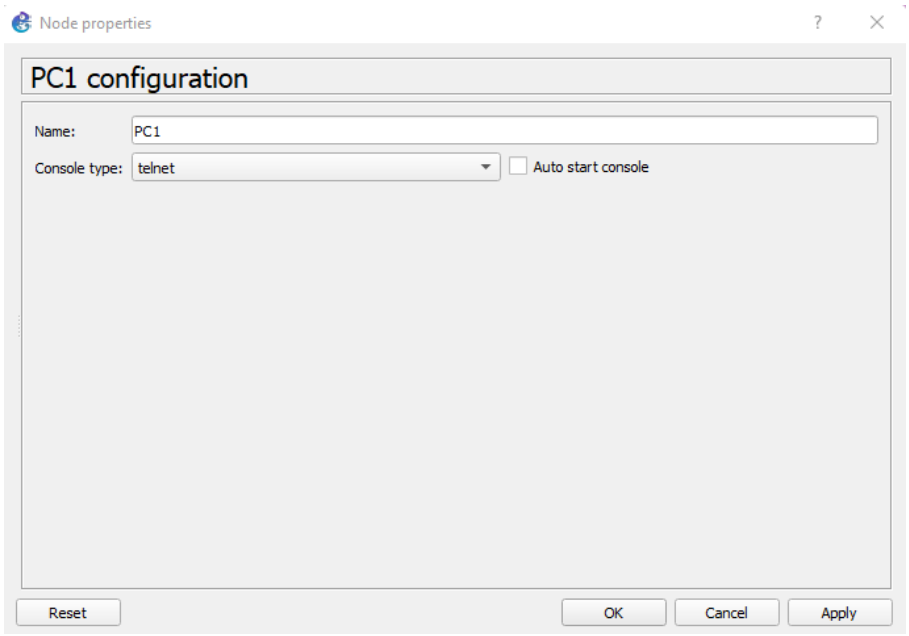

Figura 21 *PC1*

Tabla 3 *Requerimientos Mínimos*

Sistema Operativo	Sistema (Windows 7 o posterior), IOS (Maverick 10.9 o posterior), Distribución Linux, Debian, Ubuntu
Procesador	Procesador con 2 o más núcleos / extensión de virtualización
Memoria	Mínimo de 4 GB de RAM
Almacenamiento	Espacio mínimo de 200 MB – Recomendado 1 GB
Adicionales	El almacenamiento de imágenes, requiere más espacio en el equipo (disco duro)

Fuente: (Díaz Saravia, 2017)

PC2: Windows 10 con las siguientes características

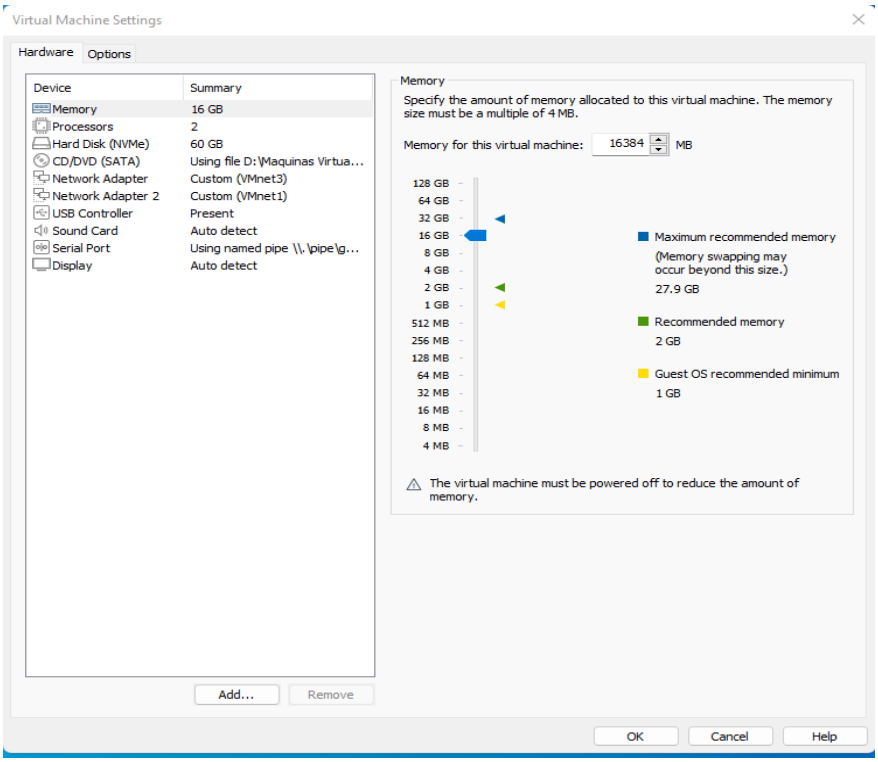

Figura 22 *PC2*

SRV1-MON: Servidor de monitoreo con sistema operativo CentOs8 con las siguientes características:

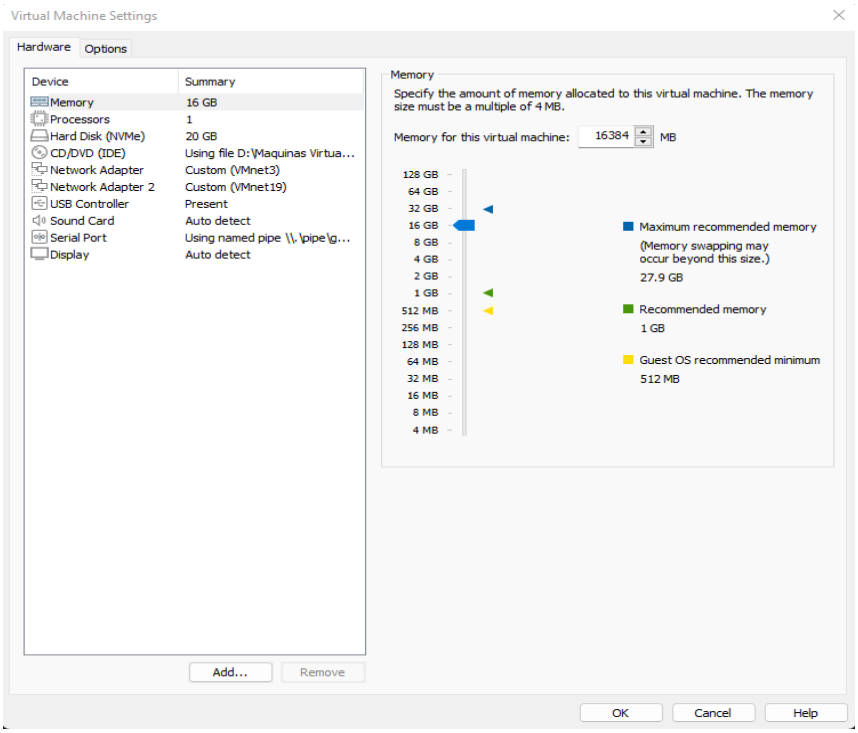

Figura 23 *SRV1-MON*

SRV2-VIRT: CentOs8 con las siguientes características

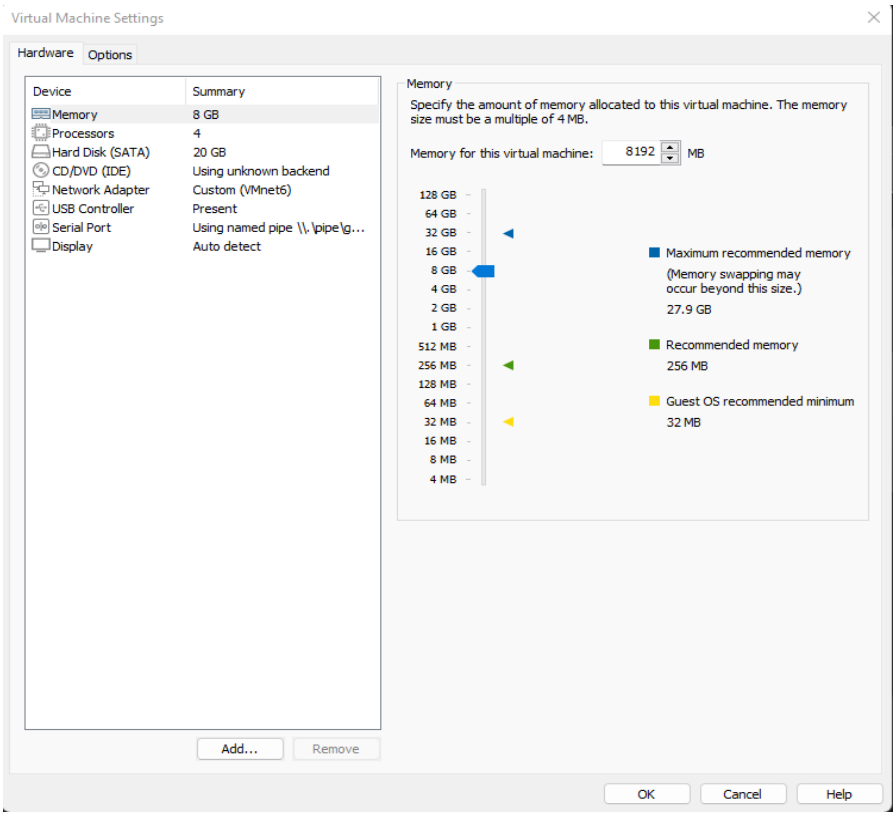

Figura 24 *SRV2-VIRT*

SRV1-WWW: CentOs8 con las siguientes características

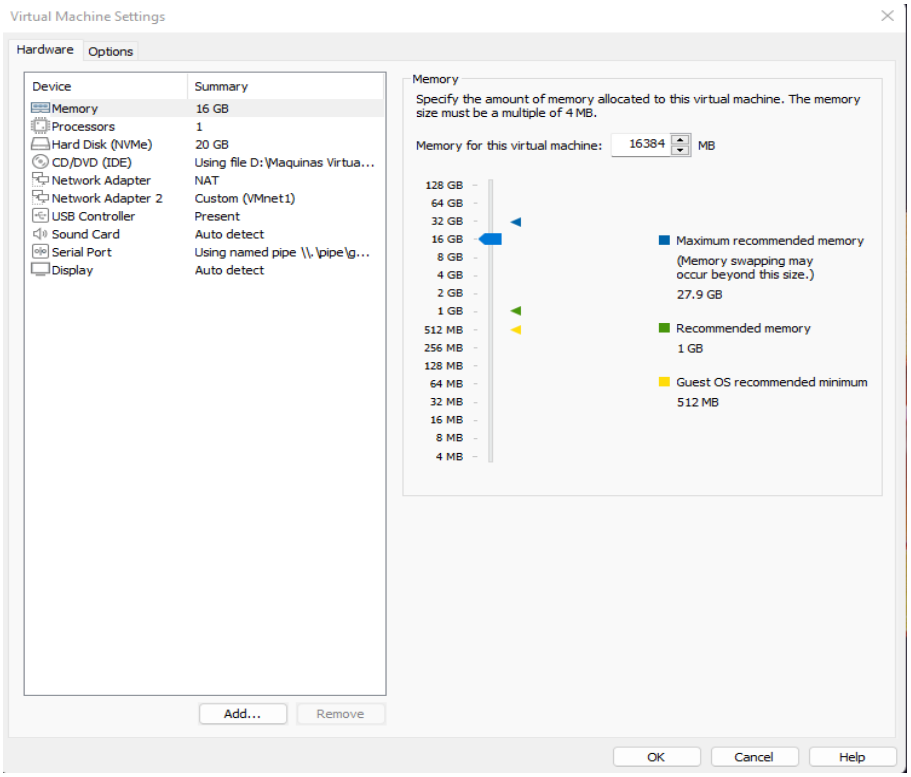

Figura 25 *SRV1-WWW*

FIREWALL

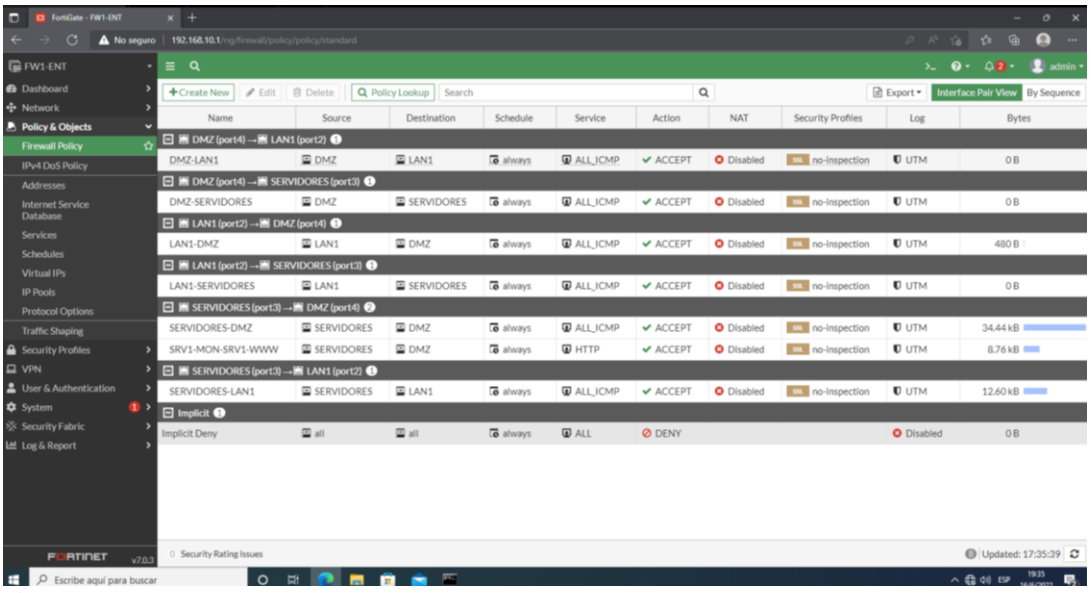

Figura 26 *FW1-ENT*

FW1-ENT: Servidor de monitoreo con sistema operativo FIREWALL con las siguientes características

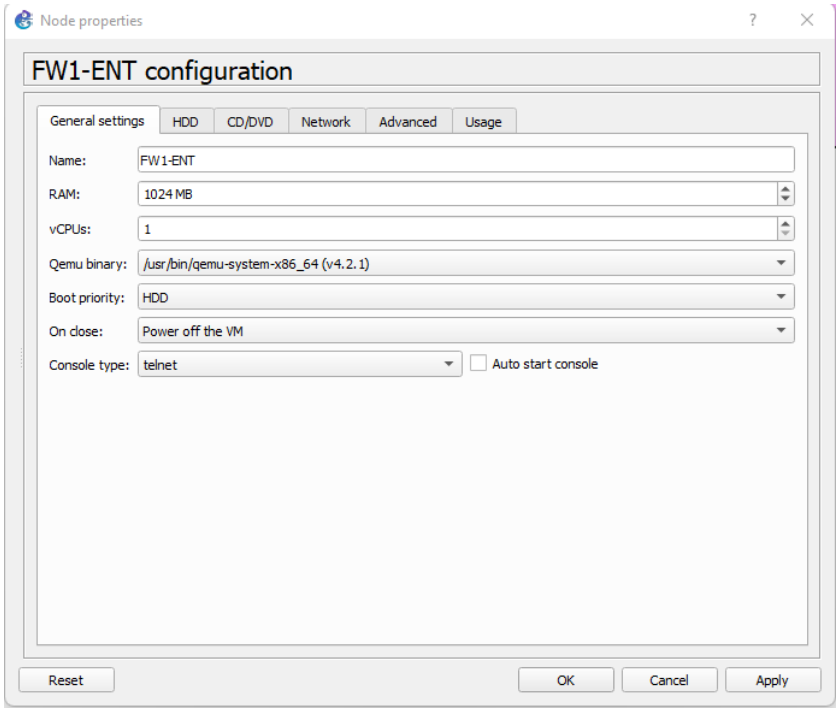

Figura 27 *FW1-ENT a*

El proceso a seguir, parte de añadir la dirección IP en la Vlan1 para el SW1-LAN1:

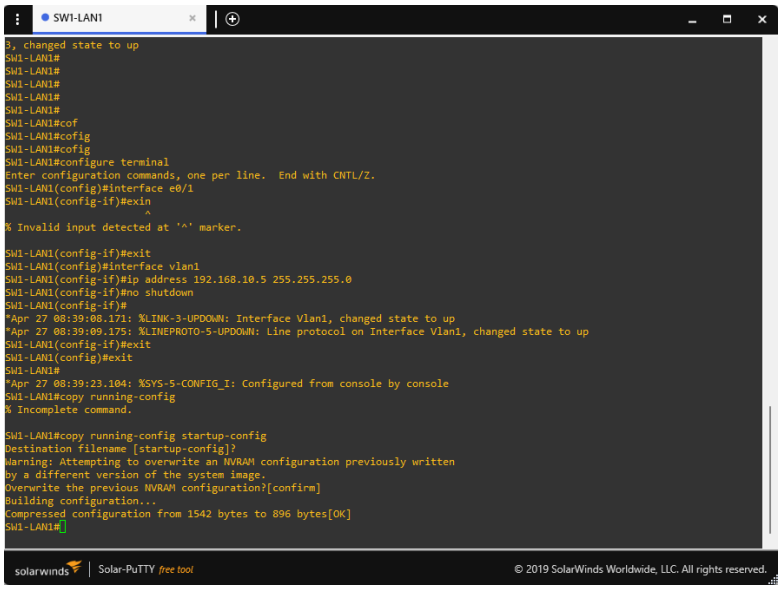

Figura 28 *Añadir dirección IP en VLAN1*

El proceso siguiente es la verificación de la conectividad en la PC1 haciendo ping al SW1-LAN1:

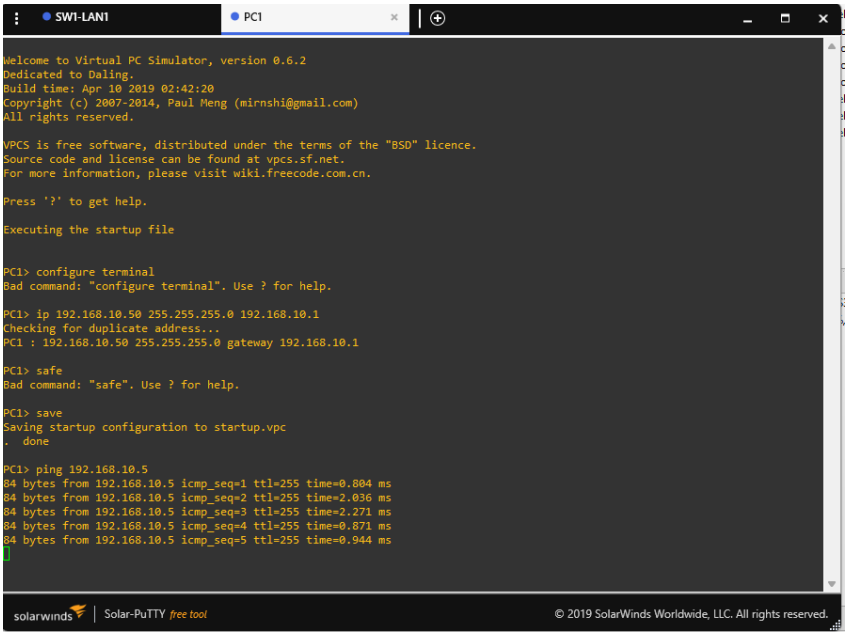

Figura 29 *Verificación de conectividad PC1*

Es por ello que se hace necesario la configuración IP en la máquina PC2:

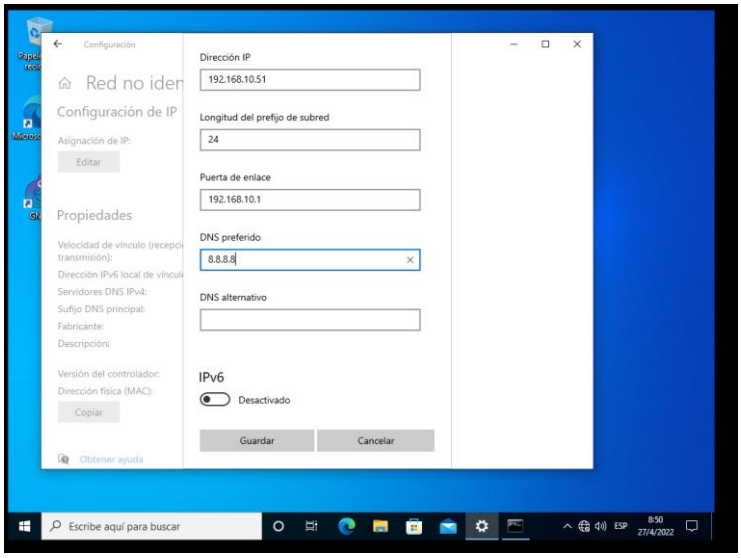

Figura 30 *Configuración IP PC2*

Para luego proceder a guardar los cambios y se verifica si hay conectividad:

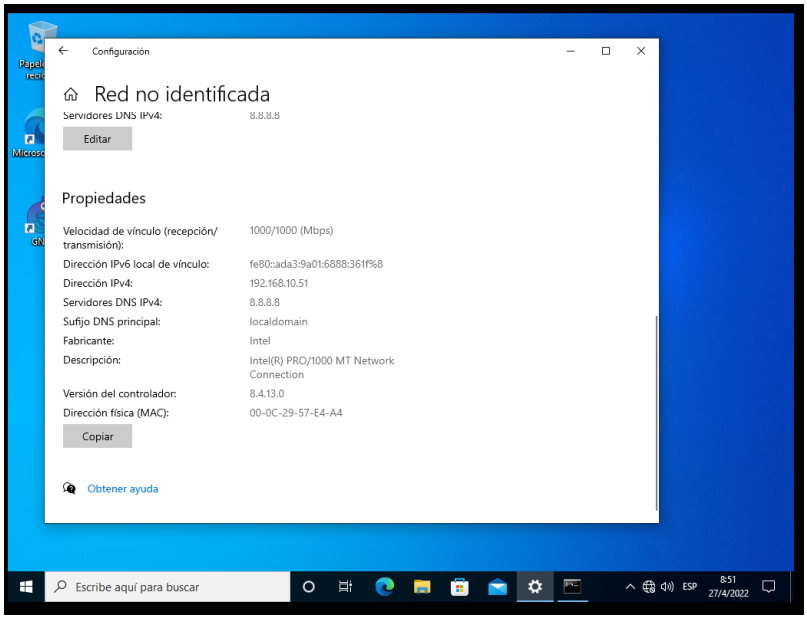

Figura 31 *Verificación de conectividad*

Es indispensable el poder verificar la conectividad en la PC2 haciendo ping al SW1-LAN1:

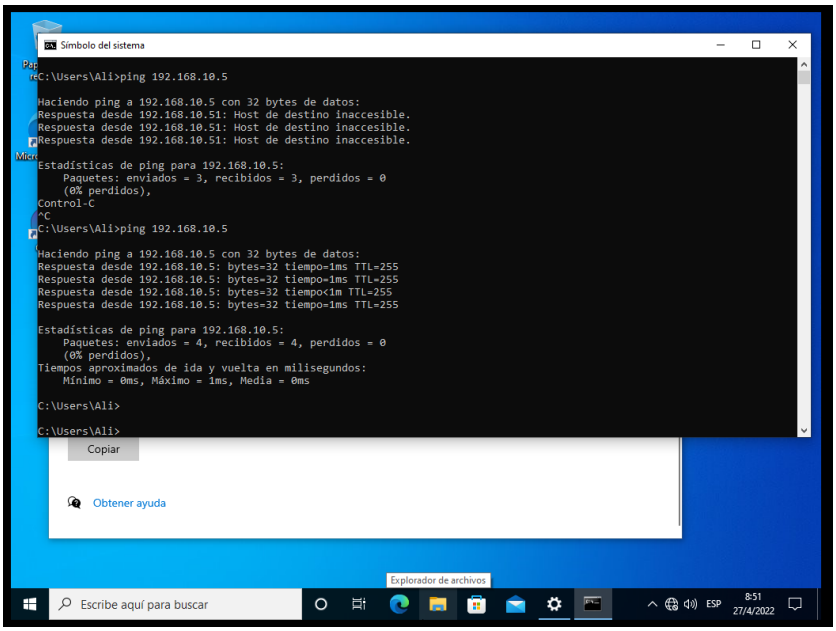

Figura 32 *Ping al SW1-LAN1*

Sin embargo, se hace imprescindible el añadir la dirección IP en la Vlan1 para el SW2-DMZ:

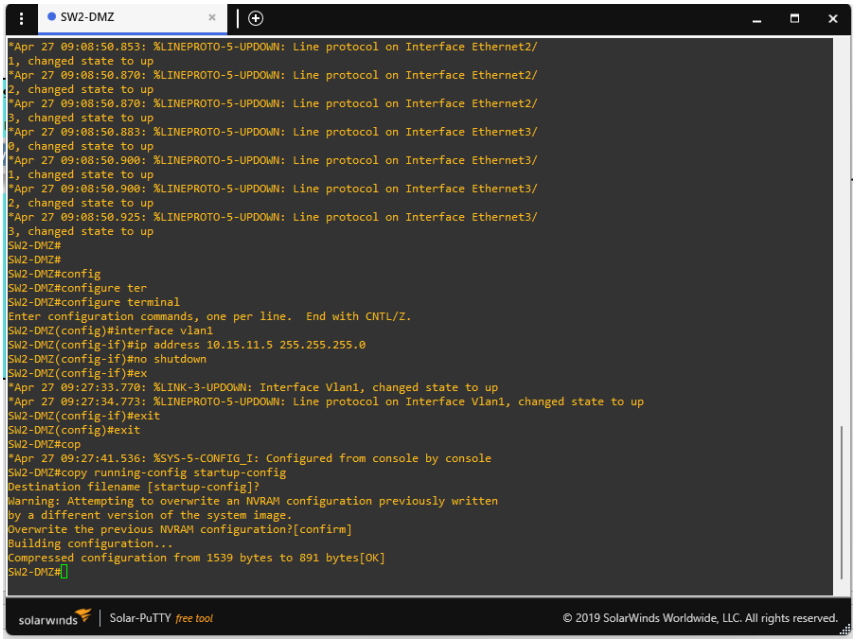

Figura 33 *Añadir direcciones IP al VLAN1*

Para de esta manera poder proceder con la configuración IP en la máquina SRV1-WWW:

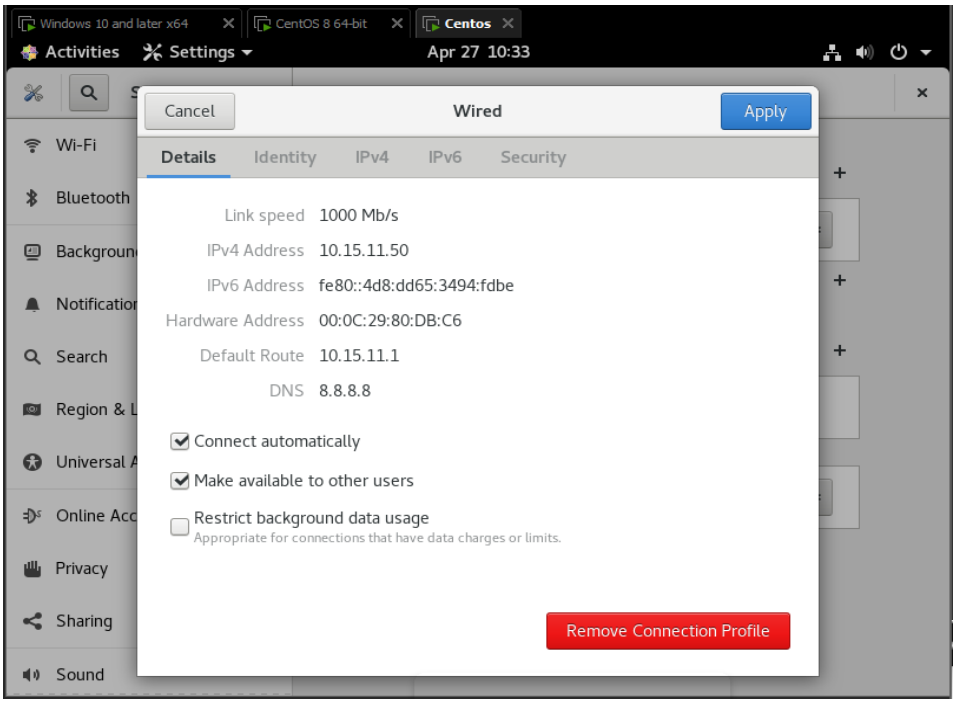

Figura 34 *Configuración IP máquina SRV1-WWW*

Y así verificar la conectividad en la SRV1-WWW haciendo ping al SW2-DMZ:

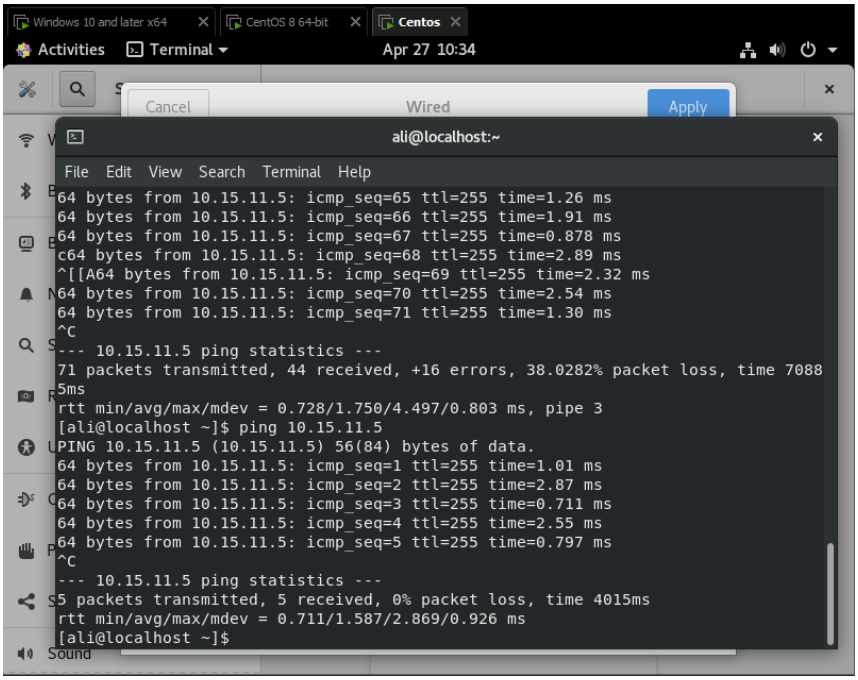

Figura 35 *Verificación de conectividad SRV1-WWW*

Añadiendo de forma adecuada la dirección IP en la Vlan1 para el SW2-SRV1:

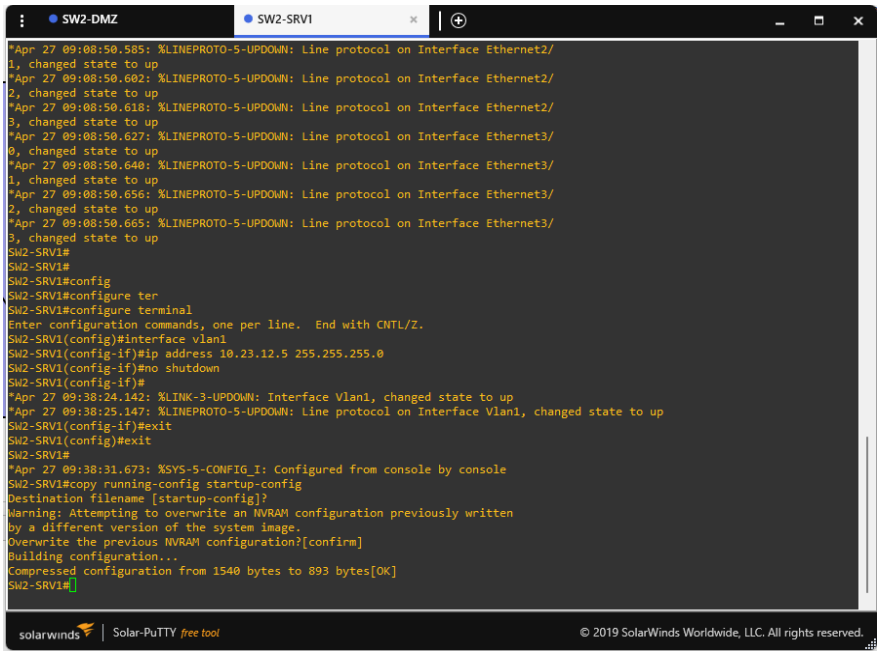

Figura 36 *Añadir direcciones IP a VLAN 1*

Y así configurar IP en la máquina SRV1-MON:

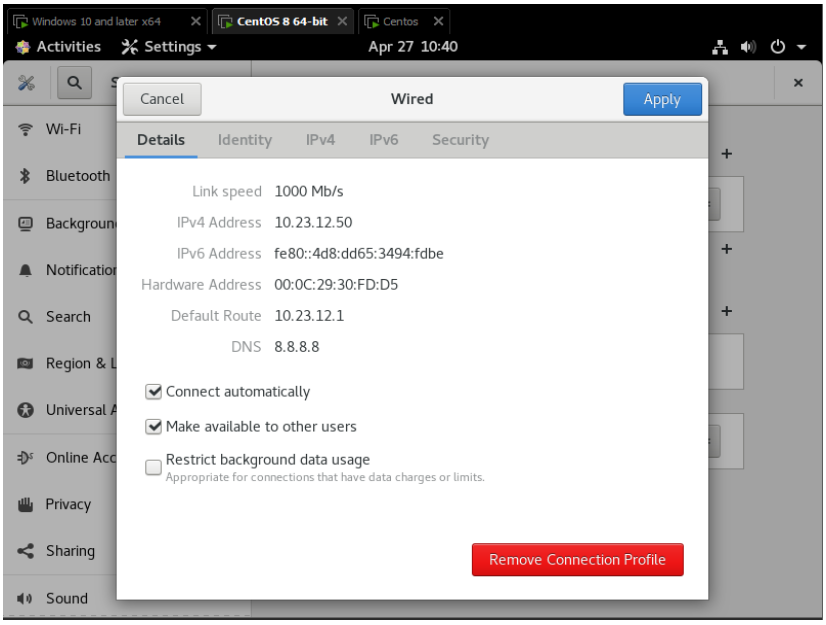

Figura 37 *Configuración IP en SRV1-MON*

El proceso de verificación de la conectividad en la SRV1-MON haciendo ping al SW2-SRV1 es necesario según el procedimiento establecido:

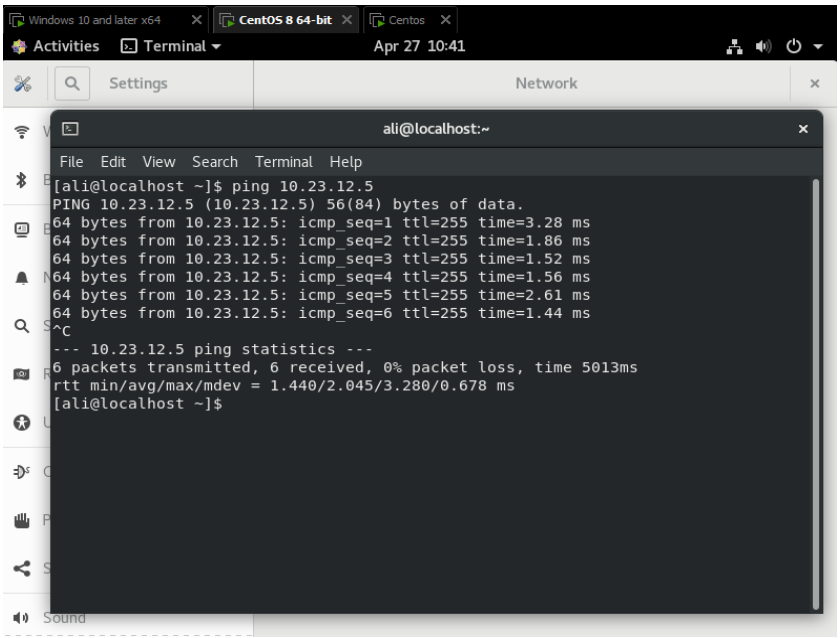

Figura 38 *Verificación de conectividad SRV1-MON*

Es por lo que se procede con la configuración IP en la máquina SRV2-VIRT:

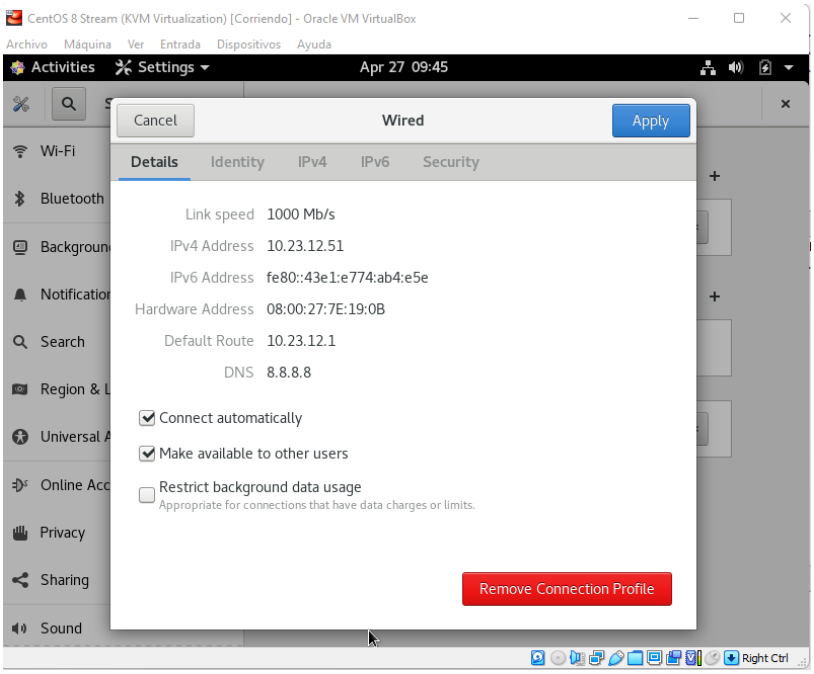

Figura 39 *Configuración IP SRV2-VIRT*

Para luego verificar la conectividad en la SRV2-VIRT haciendo ping al SW2-SRV1:

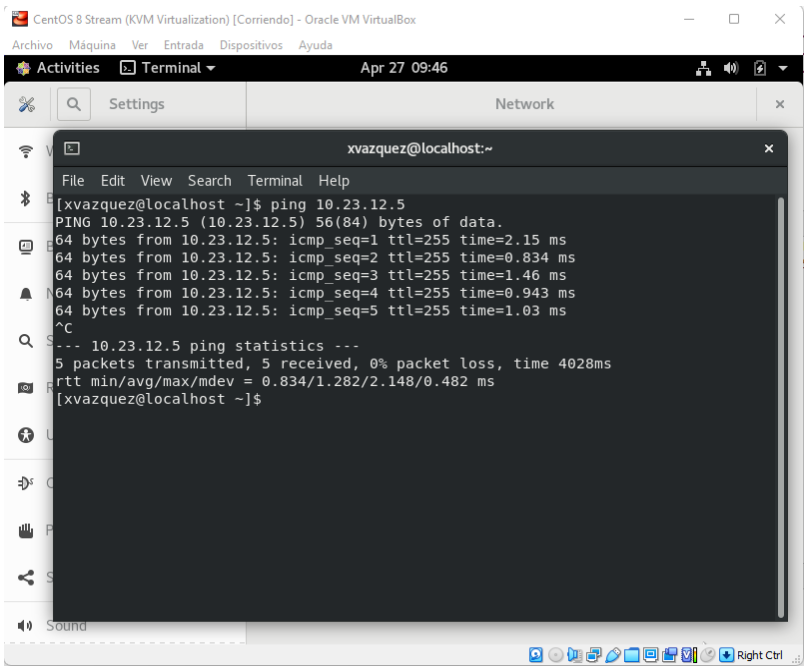

Figura 40 *Verificación de conectividad SRV2-VIRT*

Icinga2 es un instrumento de monitoreo de código abierto para verificar la disponibilidad en los recursos de TI (red, servidores, etc.) e informar interrupciones cuando fallan los recursos. También genera datos de rendimiento con fines informativos (Bayas, 2015)

Tiene varios subprocesos y puede ejecutar miles de comprobaciones por segundo sin afectar a la CPU. También al configurar clústeres de alta disponibilidad para Icinga2 y proporcionar configuraciones distribuidas para entornos grandes/complejos (Bayas, 2015).

Instalación de Icinga2:

Primero, actualizar y mejorar el CentOS Linux.

```
dnf -y update && dnf -y upgrade
```

Seguido, Instalar el repositorio Icinga.

```
dnf install -y https://packages.icinga.com/epel/icinga-rpm-release-8-latest.noarch.rpm
```

Habilitar al repositorio EPEL y Obtener el repositorio EPEL. Adicionalmente se necesita el repositorio de PowerTools (herramientas de software) para EPEL.

```
dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

dnf install -y epel-release

dnf config-manager --set-enabled ol8_codeready_builder
```

Se Obtendrán algunas herramientas que serán necesarias posteriormente para la instalación y configuración de Icinga2 e Icinga Web 2 (red 2 de Icinga).

```
dnf install -y git curl make gcc wget nano vim net-tools tar unzip zip
```

Usar comando abajo para instalar Icinga2:

```
dnf install -y icinga2
```

Iniciar y Habilitar el servicio Icinga2.

```
systemctl enable icinga2

systemctl start icinga2

systemctl status icinga2
```

Instalar las conexiones requeridas para Icinga2.

```
dnf install -y nagios-plugins-all
```

Ejecutar el siguiente comando para confirmar que los archivos de Icinga son correctos antes de querer cambiar alguno de estos archivos de Icinga.

```
icinga2 daemon -C
```

Si se quiere usar SELinux con Icinga2 entonces, necesita instalar los siguientes paquetes y establecer reglas de firewall (red de sistema de seguridad) para el puerto 80 y 443.

```
dnf install -y icinga2-selinux
firewall-cmd --add-service=http && firewall-cmd --permanent --add-ser-
vice=http
firewall-cmd --reload
```

Después de completar los pasos mencionados, ahora se Instala y configura MYSQL ó MariaDB como base de datos para Icinga2.

```
dnf install -y mysql-server

Or

dnf install -y mariadb-server mariadb
```

Iniciar, habilitar y situar MYSQL.

```
systemctl start mysqld
systemctl enable mysqld
systemctl status mysqld
```

Asegurar el MYSQL

```
mysql_secure_installation
```

Después de Ingresar el comando anterior el sistema solicitará una contraseña raíz. Presionar Enter ya que no se tiene una. Luego el sistema preguntará si se quiere añadir una clave raíz presionar “y”, colocar 0 y establecer una contraseña raíz. Por favor presionar “y” por cada vez que el sistema pregunta sobre alguna configuración.

Contraseña raíz: linux5171

Instalando los módulos de IDO para MySQL

El siguiente paso es instalar el paquete icinga2-ido-mysql usando el gestor de paquetes de distribución.

```
dnf install -y icinga2-ido-mysql
```

Configurar MySQL

Configurar una base de datos MySQL para Icinga 2, ingresar a la base de datos MySQL como cuenta raíz y crear una base de datos nombrada como icinga.

```
mysql -u root -p
Enter password:
mysql> CREATE DATABASE icinga;
mysql> create user 'icinga' identified by 'Icinga123!';
mysql> grant SELECT, INSERT, UPDATE, DELETE, DROP, CREATE VIEW, INDEX, EXE-
CUTE on icinga.* to 'icinga';
mysql> FLUSH PRIVILEGES;
mysql> quit
```

Después de configurar la base de datos MySQL, importar el esquema Icinga 2 IDO usando el siguiente comando.

```
mysql -u root -p icinga < /usr/share/icinga2-ido-mysql/schema/mysql.sql
Enter password:
```

Habilitando el módulo IDO MySQL

El archivo de configuración está localizado en /etc/icinga2/features-available/ido-mysql.conf file. Puede actualizarse una vez ya configurado.

```
nano /etc/icinga2/features-available/ido-mysql.conf

object IdoMysqlConnection "ido-mysql" {
  user = "icinga"
  password = "Icinga123!"
  host = "localhost"
  database = "icinga"
}
```

Habilitar IDO y reiniciar el servicio de Icinga para que la configuración anterior pueda resultar.

```
icinga2 feature enable ido-mysql
systemctl restart icinga2.service
```

Instalación de Icinga Web 2:

Primero, instalar el servidor de red.

```
dnf install -y httpd

systemctl enable httpd

systemctl start httpd

systemctl status httpd
```

Ingresar a mysql al digitar el siguiente comando:

```
mysql -u root -p
```

Crear la siguiente base de datos para icinga web 2:

```
mysql> CREATE DATABASE icingaweb;
mysql> create user 'icingaweb' identified by 'Icinga123!';
mysql> GRANT ALL PRIVILEGES ON icingaweb.* TO 'icingaweb';
mysql> FLUSH PRIVILEGES;
mysql> quit
```

Configurar Icinga2 Rest API User (apoyo API usuario):

```
icinga2 api setup
```

Editar el archivo "/etc/icinga2/conf.d/api-users.conf" con nano editor.

```
nano /etc/icinga2/conf.d/api-users.conf
```

Agregar las siguientes líneas:

```
object ApiUser "icingaweb2" {
password = "Wijsn8Z9eRs5E25d"
permissions = [ "status/query", "actions/*", "objects/modify/*", "ob-
jects/query/*" ]
}
```

Ahora, Reiniciar el servicio de Icinga2 para aplicar la configuración anterior.

```
systemctl restart icinga2
```

Instalar repositorio SCL, es requerido para Icinga Web 2.

```
dnf -y group install "Development Tools"
dnf -y install gcc-c++ gcc make mysql-devel.x86_64
```

Instalar PHP

En este punto, el sistema está listo para la instalación. PHP 7.4 es la última versión estable disponible para la instalación. Así que se puede usar la última versión para los servidores de producción. Se puede usar otras versiones de PHP según sean los requisitos deseados.

```
dnf module reset php
dnf module enable php:7.4
```

Instalar Icinga Web 2 e Icinga CLI usando el siguiente comando:

```
dnf install -y icingaweb2 icingacli
```

Si se necesita SELinux para Icinga Web 2 instalarlo usando el siguiente comando:

```
dnf install -y icingaweb2-selinux
```

Instalar PHP FPM y otros módulos PHP que serán necesarios para Icinga web 2.

```
dnf install –y php-json php-ldap
dnf install -y php-mysqlnd php-fpm php-ldap php-pgsql php-xmlrpc php-intl
php-gd php-pdo php-soap php-posix php-cli
```

Iniciar y habilitar el servicio.

```
systemctl enable php-fpm.service
systemctl start php-fpm.service
systemctl restart httpd
systemctl restart php-fpm.service
```

Instalar ImageMagick y PHP Imagick

```
dnf install ImageMagick ImageMagick-devel ImageMagick-perl
```

Instalar php Imagick asegurando que se necesita instalar bajo los paquetes en el sistema.

```
dnf install php-devel php-pear make
```

Ahora instalar php Imagick con pecl.(Pecl es un repositorio para Extensiones Php) como se muestra abajo

```
pecl install imagick
```

Añadir extensión php al archivo php.ini

```
echo "extension=imagick.so" > /etc/php.d/20-imagick.ini
```

Seguido, reiniciar el sistema para efectuar toda la configuración

```
reboot
```

Ahora, crear la ficha para terminar la configuración de Icinga Web 2 a través de la interfaz de red:

```
icingacli setup token create
```

Abrir Icinga Web 2 Usando el siguiente url en el navegador web:

```
http://192.168.171.136/icingaweb2/setup
```

Remplazar el IP arriba del url con el sistema IP.

Configuración Icinga Web 2

Solicitará la ficha generada, pegarla y seleccionar en siguiente

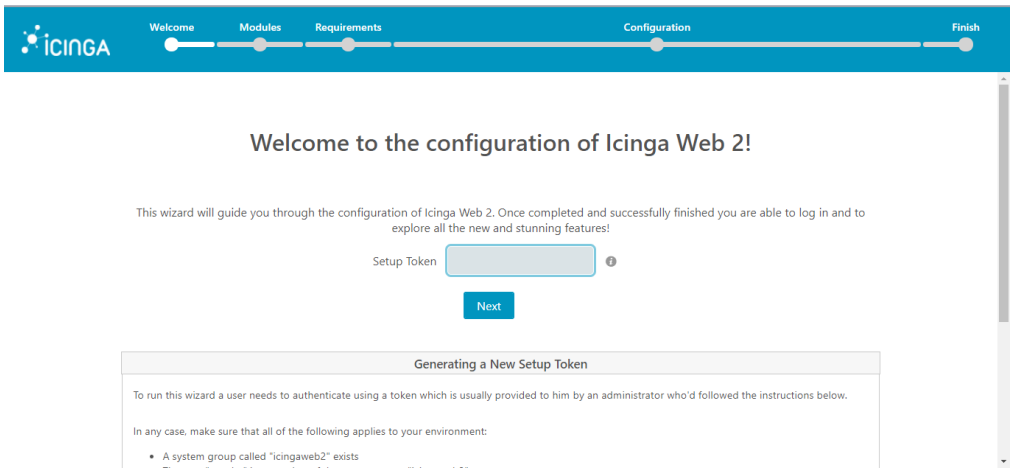

Figura 41 *Icinga Web 2 Configuration*

Los módulos de monitoreo están habilitados por defecto, se puede habilitar Doc, Migrar y Traducir opcionalmente y después seleccionar siguiente.

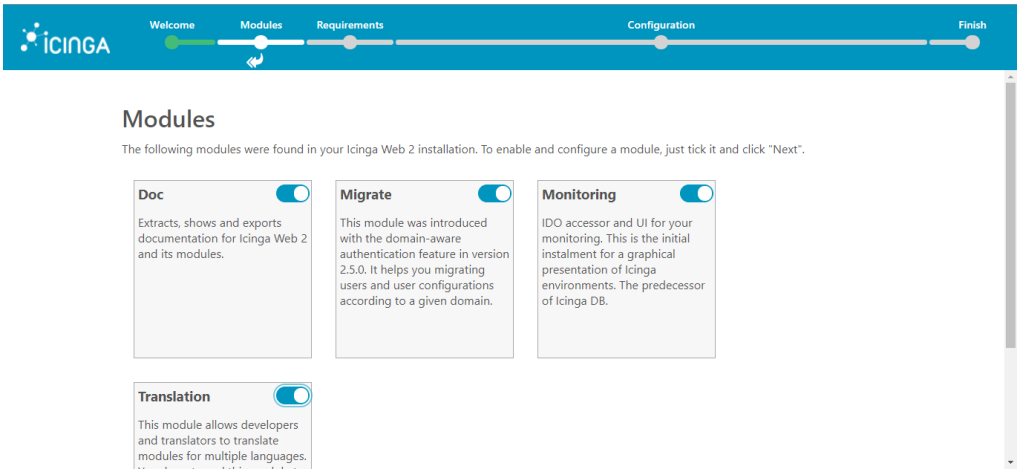

Figura 42 *Icinga Web 2 Configuration Modules*

Ahora todos los módulos PHP deben ser de color verde, en caso de haber nos e color amarillo, se recomienda arreglarlo antes de continuar, si todos se encuentran verdes, seleccionar siguiente.

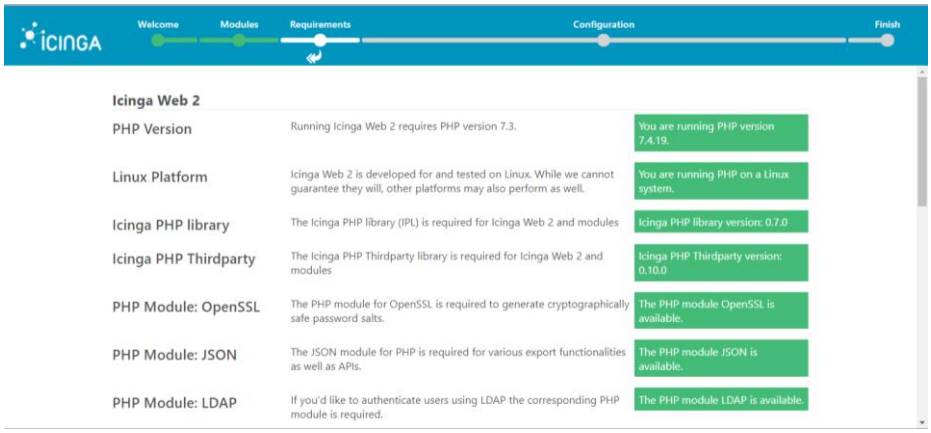

Figura 43 *Icinga Web 2 Configuration Modules II*

Por defecto se usa la autenticación de base de datos.

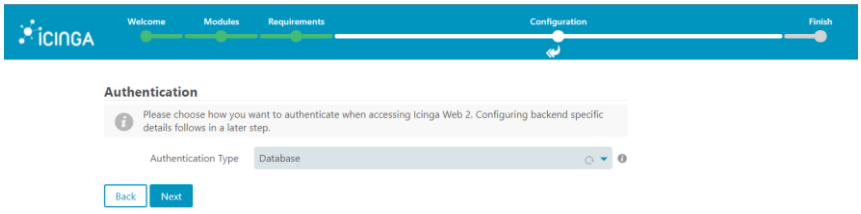

Figura 44 *Icinga Web 2 Configuration Authentication*

Configure el recurso de la base de datos, aquí se usarán las credenciales creadas por la base de datos de icingaweb. Se necesita configurar los parámetros de servidor local, la base de datos, cliente y clave. Antes de presionar siguiente, puede hacer click en Validar Configuración en orden de validar que las credenciales estén trabajando correctamente.

- Anfitrión: sevidor local
- Nombre de Base de Datos: icingaweb
- Usuario: icingaweb
- Contraseña: Icinga123!

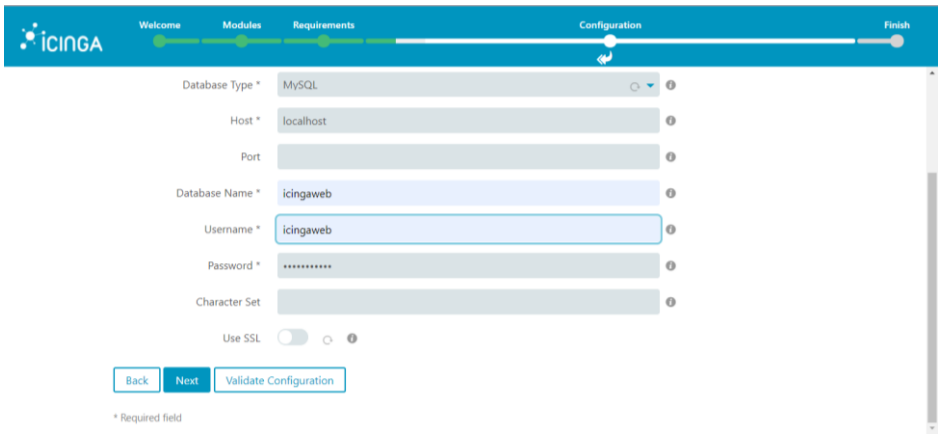

Figura 45 *Icinga Web 2 Configuration Database*

Configurar la Autenticación de Backend, este fue definido en el archivo de api-users.conf, solo seleccione siguiente.

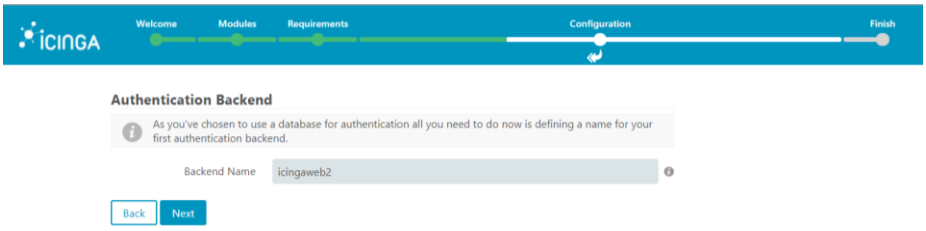

Figura 46 *Icinga Web 2 Configuration Authetication Backend*

En la pantalla de administración se define el usuario y contraseña para ingresar en la interfaz de Icinga Web.

- Nombre de Usuario: admin
- Contraseña: linx5171
- Repetir conraseña: linux5171

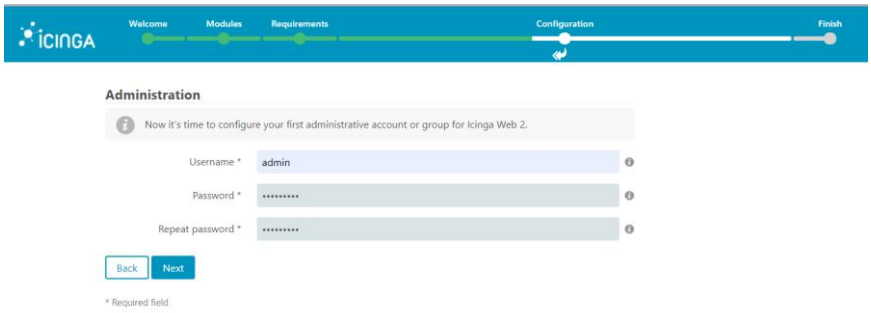

Figura 47 *Icinga Web 2 Configuration Administration*

En la pantalla de configuración de la aplicación de debe hacer click en siguiente, se puede cambiar ajustándolo acorde a lo que se necesite, pero no afectan los defectos.

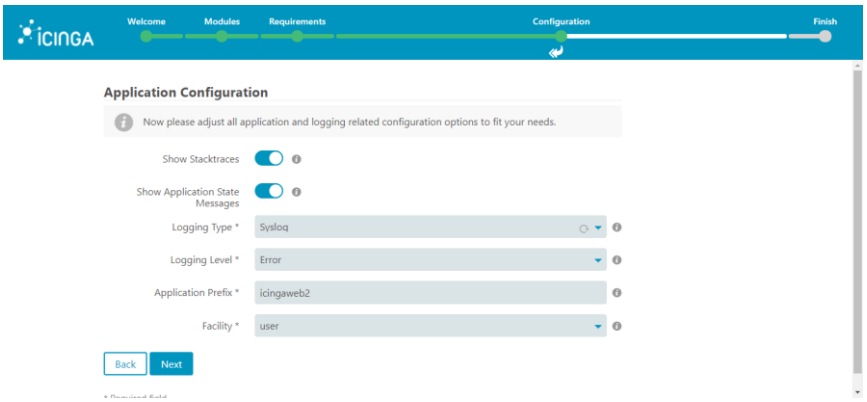

Figura 48 *Icinga Web 2 Configuration Application Configuration*

Se tiene una pantalla de resumen, aquí solo seleccione siguiente.

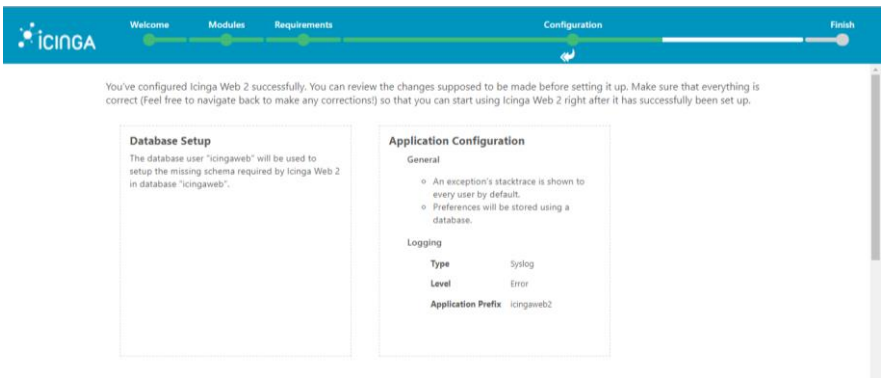

Figura 49 *Icinga Web 2 Configuration Application Configuration II*

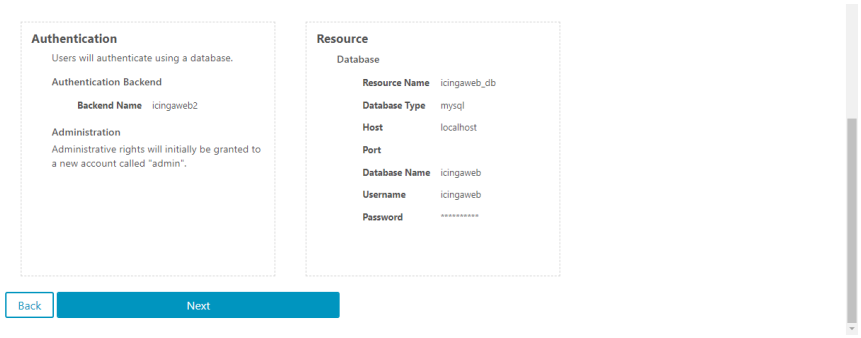

Figura 50 *Icinga Web 2 Configuration Application Configuration III*

Ahora, se puede configurar el módulo de monitoreo por Icinga Web 2, solo seleccione siguiente.

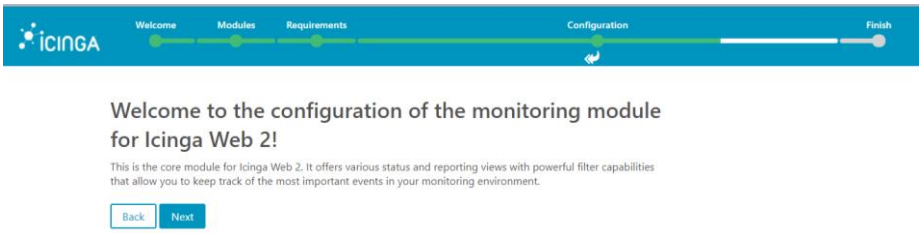

Figura 51 *Icinga Web 2 Configuration Application Configuration IV*

Ahora, se configura el Recurso IDO de monitoreo, aquí se usan las credenciales creadas previamente para la base de datos de Icinga. Aquí se necesita preparar los parámetros de servidor local, la base de datos, cliente y clave. Antes de presionar en Validar Configuración en orden de validar que las credenciales están trabajando correctamente.

- Anfitrión: localhost
- Base de Datos: icinga
- Usuario: icinga
- Contraseña: Icinga123!

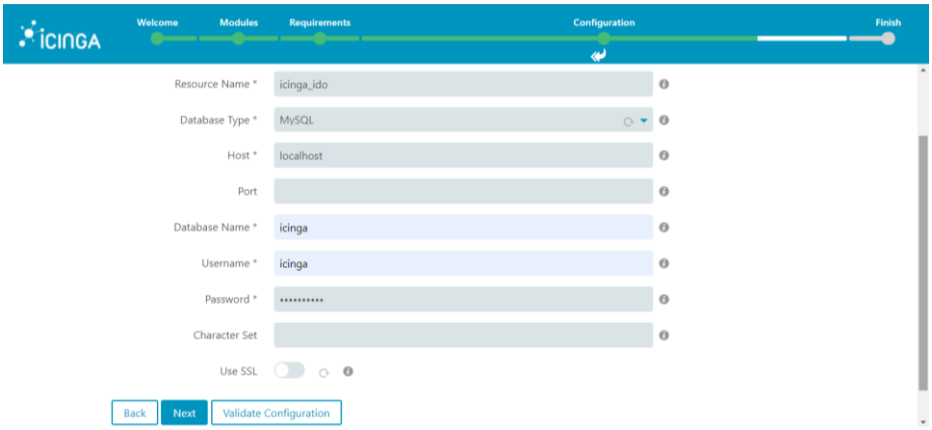

Figura 52 *Icinga Web 2 Configuration Application Configuration Localhost*

Seleccionar Comando de Transporte:

Ahora seleccione el comando transporte. Se configura el Recurso IDO de monitoreo, aquí se usan las credenciales creadas previamente para la base de datos de Icinga. Aquí se necesita preparar los parámetros de servidor local, nombre de base de datos, cliente y clave. Antes de presionar en Validar Configuración en orden de validar que las credenciales están trabajando correctamente.

- Anfitrión: localhost
- Nombre de Usuario de API: icingaweb2
- Contraseña de API: Wijsn8Z9eRs5E25d

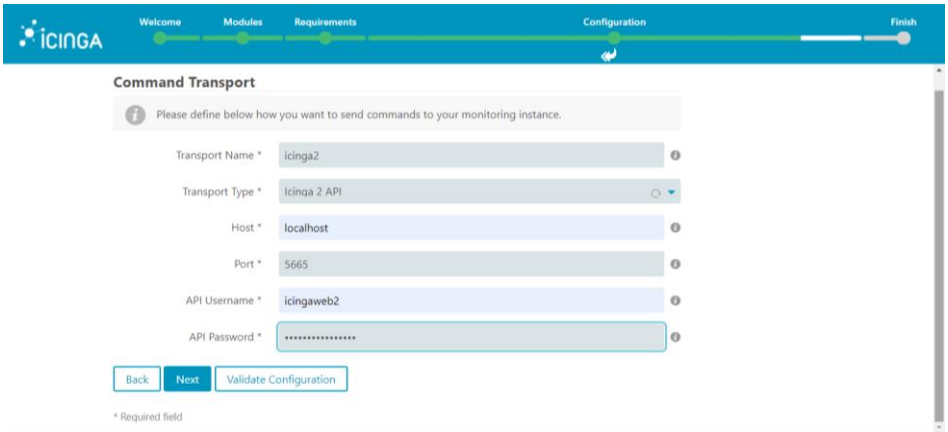

Figura 53 *Icinga Web 2 Configuration Application Command Transport*

En la pantalla de monitoreo de seguridad solo dar click en siguiente

Figura 54 *Icinga Web 2 Configuration Application Monitoring Security*

Ahora se tiene una pantalla exitosa de Icinga Web 2, solo se necesita presionar en Terminar.

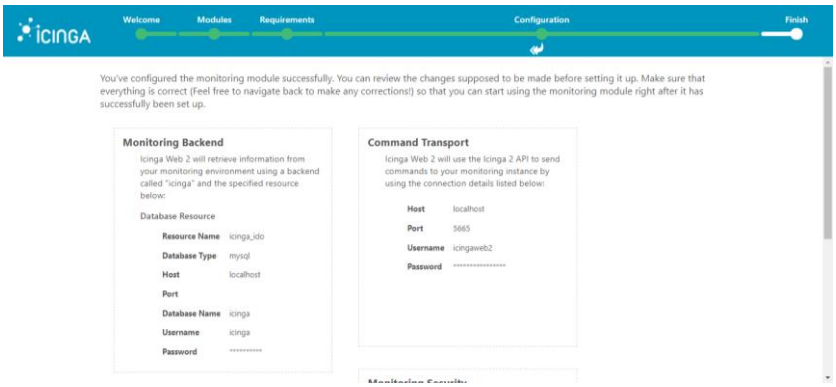

Figura 55 *Icinga Web 2 Configuration Application Monitoring Security II*

Se debería tener una pantalla de felicitaciones con la sección de Ingresar a Icinga Web disponible, solo seleccionar en ese botón para ingresar en Icinga Web 2.

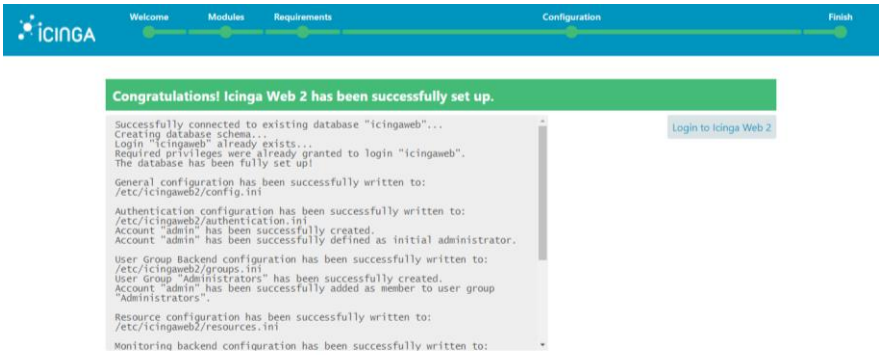

Figura 56 *Icinga Web 2 Configuration Application Monitoring Security III*

- Nombre de Usuario: admin
- Contraseña: linux5171

Figura 57 *Icinga Web 2 Configuration Application Dashboard*

Añadir Director Icinga para Icinga2 e Icinga Web 2

Después de completar la instalación de Icinga2 e Icinga Web 2 crear la Base de Datos y el permiso para Director.

```
mysql -u root -p
```

Ahora, Ingresar la contraseña que estaba configurado en la instalación de Icinga Web 2.

Ingresar ahora en el DB, Crear la base de datos y determinar el cliente y sus permisos.

```
mysql> CREATE DATABASE director CHARACTER SET 'utf8';
mysql> create user 'director' identified by 'Icinga123!';
mysql> GRANT ALL PRIVILEGES ON director.* TO 'director';
mysql> FLUSH PRIVILEGES;
mysql> quit
```

Crear guion base y lograr ejecutarlo. Usarlo e instalar Icinga director y sus dependencias. Mover a un archivo personal para crear el guion.

```
nano create_icinga_director.sh
```

Añadir la siguiente línea en el guion:

```
#!/bin/bash
MODULE_VERSION="1.8.1"
ICINGAWEB_MODULEPATH="/usr/share/icingaweb2/modules"
REPO_URL="https://github.com/icinga/icingaweb2-module-director"
TARGET_DIR="${ICINGAWEB_MODULEPATH}/director"
```

```
useradd -r -g icingaweb2 -d /var/lib/icingadirector -s /bin/false icingadi-
rector
install -d -o icingadirector -g icingaweb2 -m 0750 /var/lib/icingadirector
git clone "${REPO_URL}" "${TARGET_DIR}" --branch v${MODULE_VERSION}
cp "${TARGET_DIR}/contrib/systemd/icinga-director.service" /etc/sys-
temd/system/

icingacli module enable director
systemctl daemon-reload
systemctl enable icinga-director.service
```

Guardar y abandonar el archivo de guion.

Dar derecho de ejecutar usando el siguiente comando:

```
chmod +x create_icinga_director.sh
```

Hacer arrancar el guion ase usando el siguiente comando:

```
bash create_icinga_director.sh
```

Crear un guion base y hacerlo ejecutable. Usarlo para instalar un incubador para Icinga director.

```
nano create_icinga_incubator.sh
```

Añadir la siguiente línea en el guion:

```
#!/bin/bash
MODULE_NAME=incubator
MODULE_VERSION=v0.11.0
REPO="https://github.com/Icinga/icingaweb2-module-${MODULE_NAME}"
MODULES_PATH="/usr/share/icingaweb2/modules"
git clone ${REPO} "${MODULES_PATH}/${MODULE_NAME}" --branch "${MODULE_VER-
SION}"
icingacli module enable "${MODULE_NAME}"
systemctl start icinga-director.service
```

Guardar y abandonar el archivo de guion.

Dar derecho de ejecutar usando el siguiente comando:

```
chmod +x create_icinga_incubator.sh
```

Hacer Correr el guion base usando el siguiente comando:

```
bash create_icinga_incubator.sh
```

Cargar el esquema para Base de Datos de Director usando abajo el comando mencionado:

```
mysql -u root -p director < /usr/share/icingaweb2/modules/direc-
tor/schema/mysql.sql
```

Reiniciar módulo de Director.

```
systemctl restart icinga-director.service
```

Configurar archivo ApiUsuario en /etc/icinga2/conf.d/api-users.conf

```
nano /etc/icinga2/conf.d/api-users.conf

object ApiUser "director" {
        password = "Wijsn8Z9eRs5E25d"
        permissions = [ "*" ]
}
```

Reiniciar servicio Icinga2..

```
systemctl restart icinga2
```

Creando un Nuevo Recurso

Se necesita ahora cargar en Icinga Web, y crear un nuevo recurso. Ir a Configuración – Aplicación – Recursos. Luego presionar en Crea Nuevo Recurso, se necesita configurar un Nombre de Recurso, Nombre de Base de Datos, Contraseña y Carácter (dígito) de configuración. Después de dar click en Validar Configuración, y si todo está bien, presionar en Guardar Cambios. Durante el proceso inicial Kickstart de Icinga Director se necesitará proveer las credenciales para un Usuario de Api, puede usarse el usuario raíz (base) definido en api-users.conf.

Nombre de Recurso: director_db

Anfitrión: localhost

Nombre de Base de Datos: director

Cliente: director

Clave: Icinga123!

Configuración de Carácter: utf8

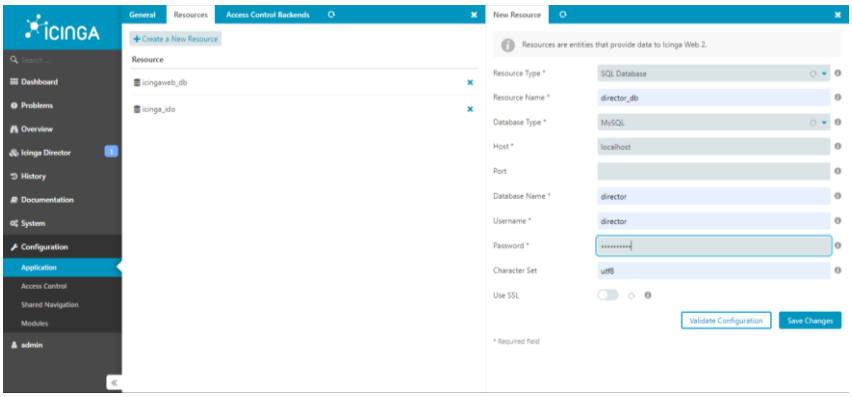

Figura 58 *Icinga Web 2 Configuration Application Creating New Resource*

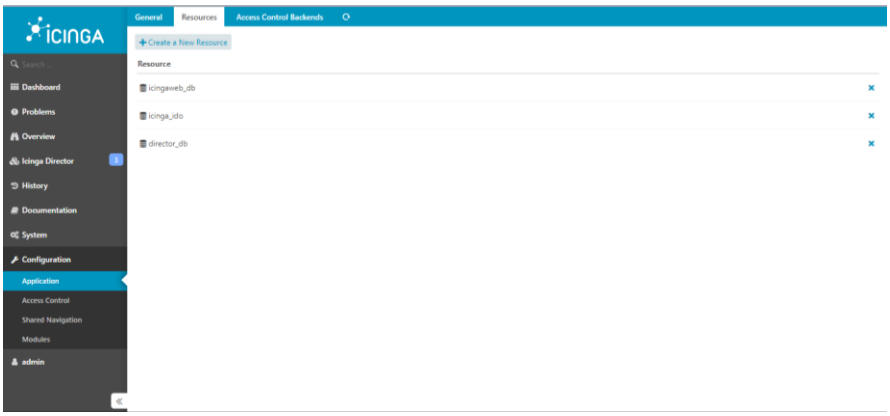

Figura 59 *Icinga Web 2 Configuration Application Creating New Resource II*

Ir a Icinga Director en Icinga Web y escoger el nuevo recurso: director_db

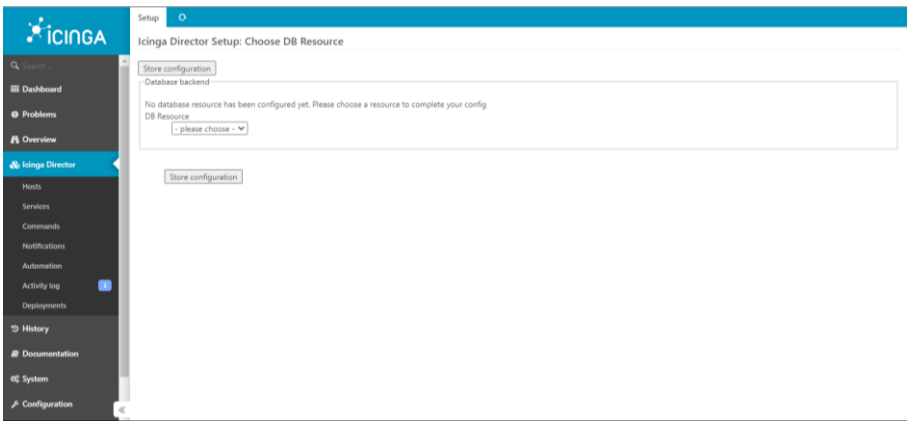

Figura 60 *Icinga Web 2 Configuration Application Creating New Resource III*

Reiniciar módulo Director.

```
systemctl restart icinga-director.service
```

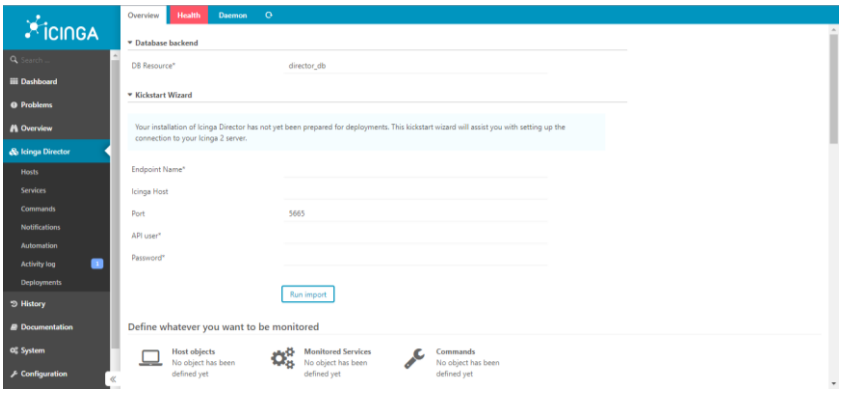

Figura 61 *Icinga Web 2 Configuration Application Restart Director Module*

Ingresar los siguientes valores para el Asistente de Kickstart:

- Endpoint Name: localhost.localdomain
- Icinga host: localhost
- Port: 5665
- API User: director
- Password: Wijsn8Z9eRs5E25d

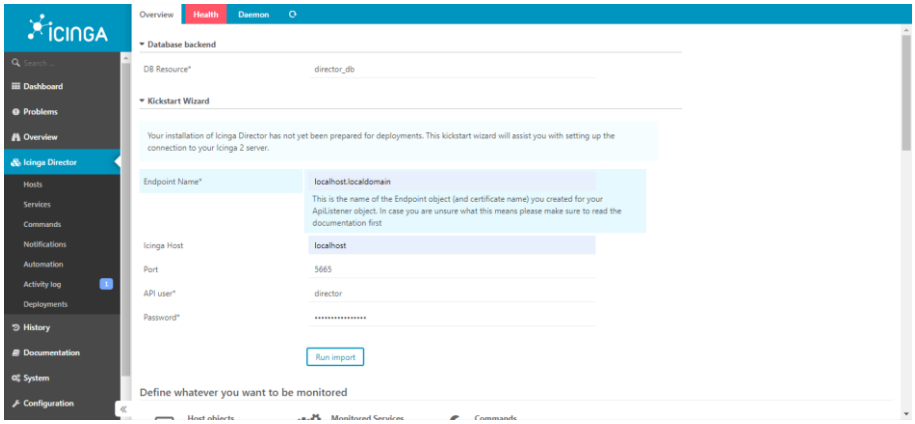

Figura 62 *Icinga Web 2 Configuration Application Asistente de Kickstart*

Ahora se puede ver la Actividad de Ingreso en la opción del menú de Director de Icinga que serán alertas en color naranja. Cuando se hace click ahí, se puede ver en el centro de la pantalla un mensaje Desplegar los cambios pendientes solo presionar en el enlace de desplegaros.

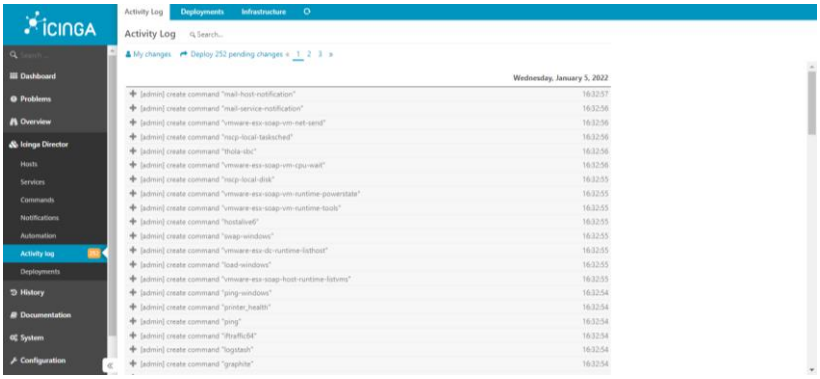

Figura 63 *Icinga Web 2 Configuration Application Asistente de Kickstart II*

Presionar en el enlace de no hay cambios pendientes.

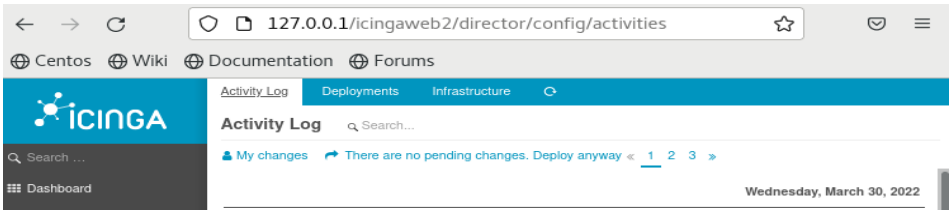

Figura 64 *Icinga Web 2 Configuration Application Activity Log*

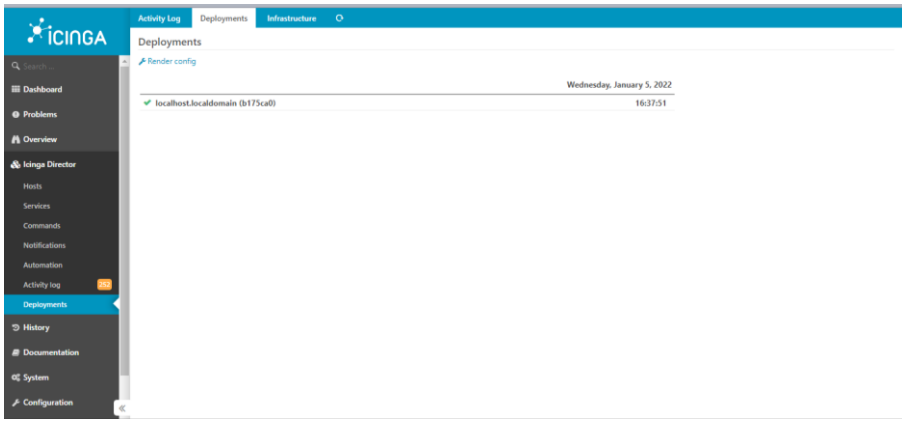

Figura 65 *Icinga Web 2 Configuration Application Activity Log II*

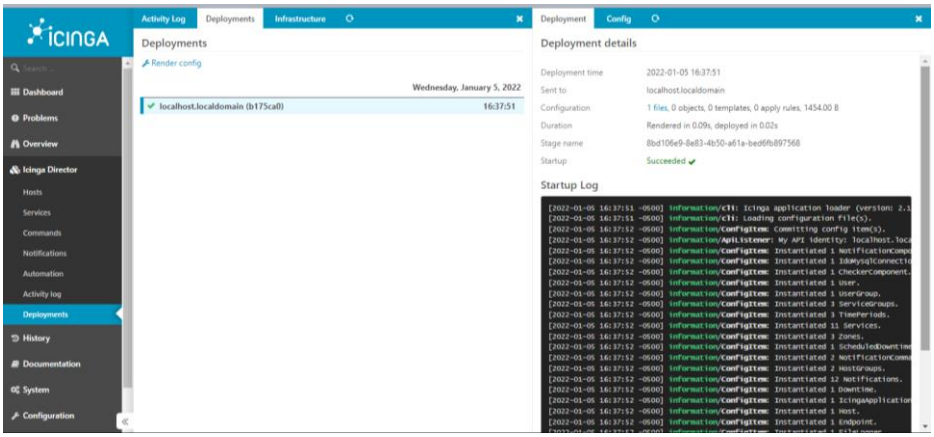

Figura 66 *Icinga Web 2 Configuration Application Activity Log III*

Los servidores que se van a monitorear en ping, servicio web:

Por medio del protocolo ICMP se van a monitorear los siguientes dispositivos de red:

- SW1-LAN1 está ubicado en la zona LAN 1
- SW2-SRV1 está ubicado en la zona de SERVIDORES
- SW2-DMZ está ubicado en la zona de DMZ
- SRV2-VIRT está ubicado en la zona de SERVIDORES
- FW1-ENT está ubicado en el Firewall

Por medio del protocolo HTTP se van a monitorear el servicio web de los siguientes servidores:

- SRV1-MON está ubicada en la zona de SERVIDORES
- SRV1-WWW está ubicado en la zona de DMZ

Proceso de Instalación

Configuración de políticas de seguridad:

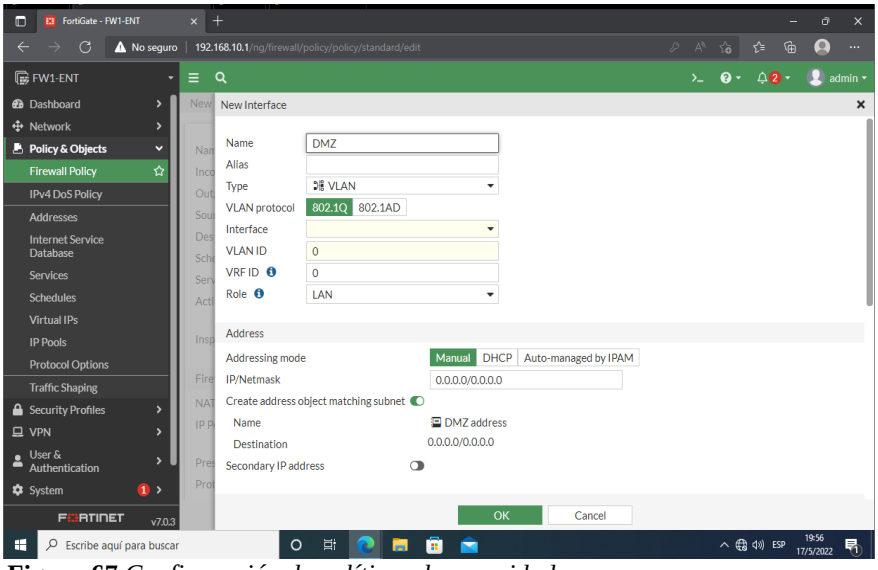

Figura 67 *Configuración de políticas de seguridad*

Políticas de seguridad entre la zona de SERVIDORES y zona DMZ

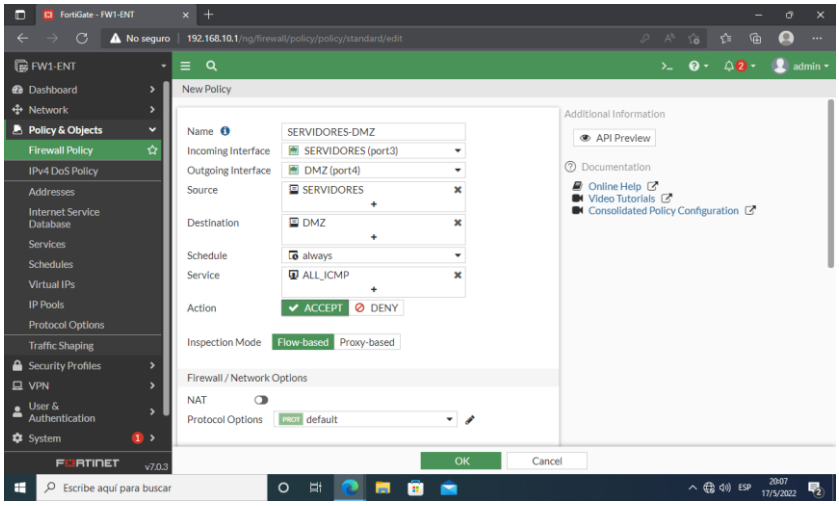

Figura 68 *Políticas de seguridad Servidores y DMZ*

Políticas de seguridad entre la zona de DMZ y zona SERVIDORES

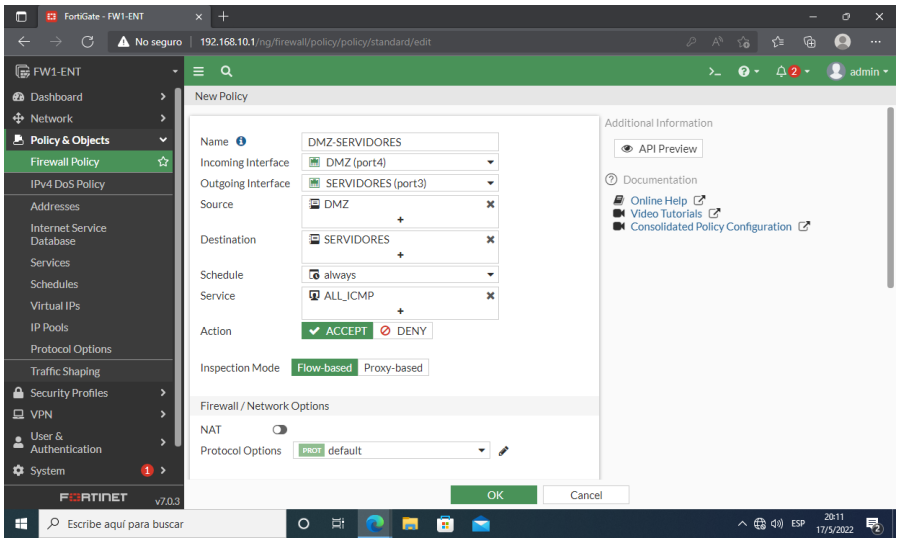

Figura 69 *Políticas de seguridad DMZ y Servidores*

Políticas de seguridad entre la zona de DMZ y zona LAN1

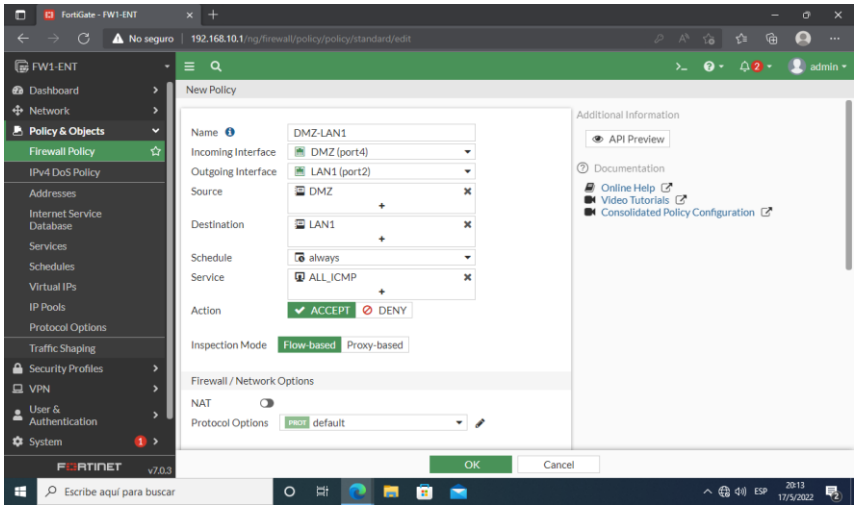

Figura 70 *Políticas de seguridad DMZ y LAN1*

Políticas de seguridad entre la zona de LAN1 y zona DMZ

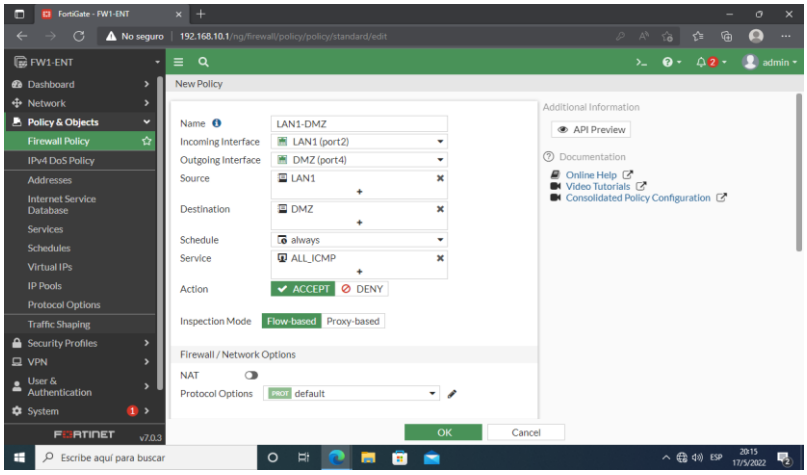

Figura 71 *Políticas de seguridad LAN1 y DMZ*

Resumen de políticas de seguridad

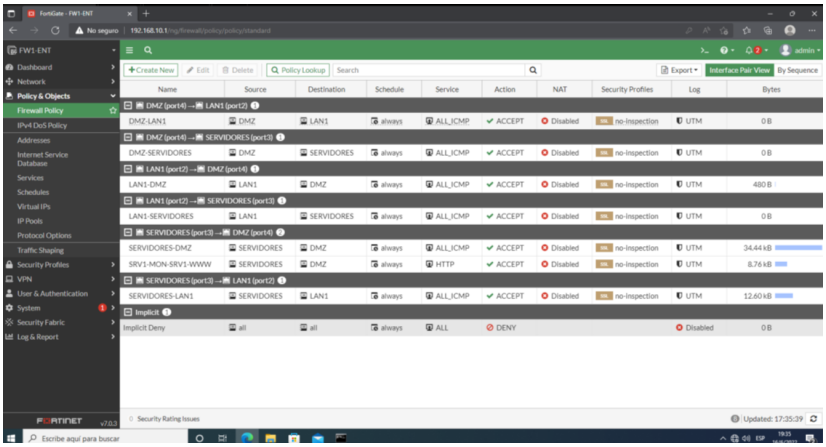

Figura 72 *Resumen de políticas de seguridad*

Configuración de Icinga 2 para monitoreo de equipos de red según topología

Configuración de monitoreo de Switches

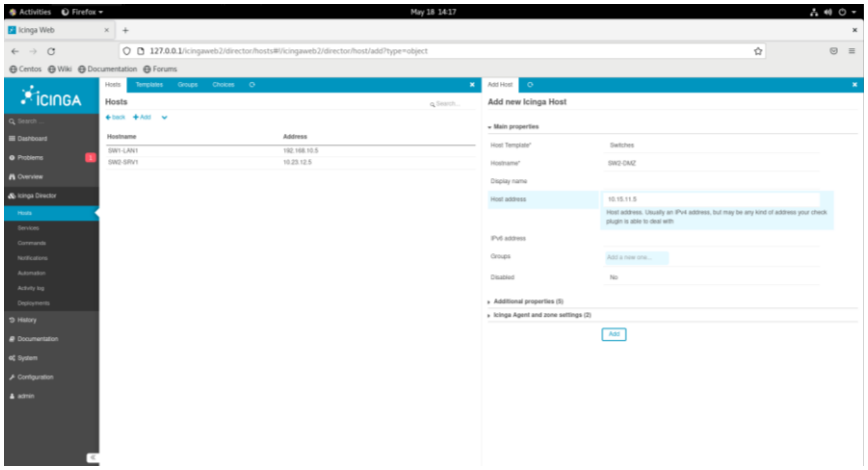

Figura 73 *Configuración de monitoreo de Switches*

Despliegue de equipos configuración para inicio de monitoreo

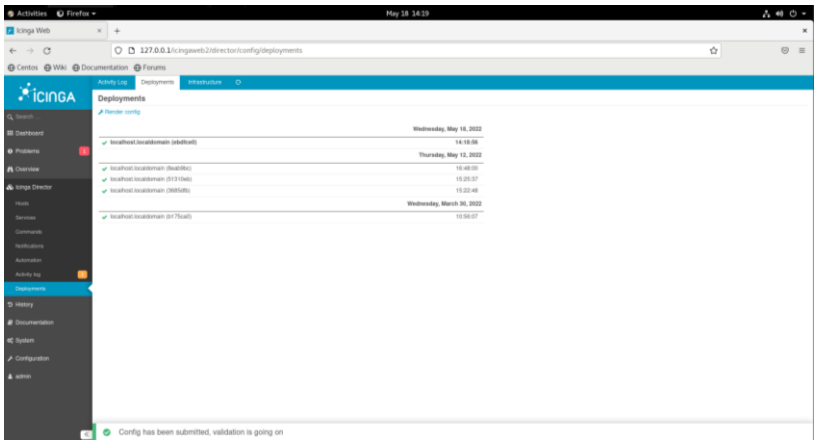

Figura 74 *Despliegue de equipos configurados 1*

Despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados:

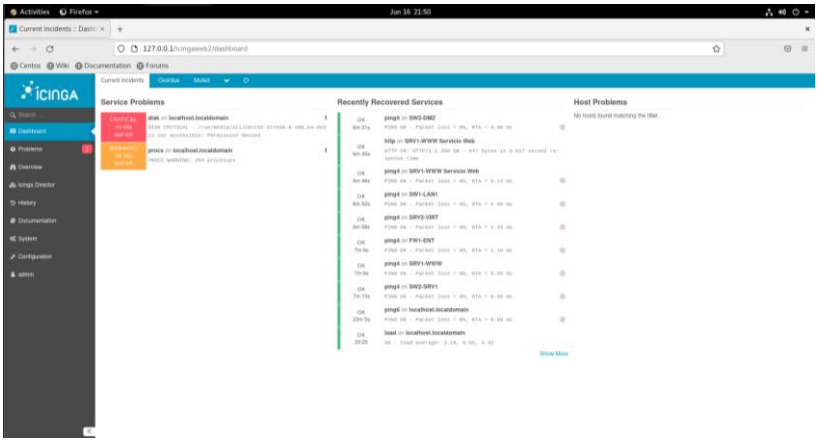

Figura 75 *Despliegue de equipos configurados 2*

Configuración en Icinga Director en Hosts:

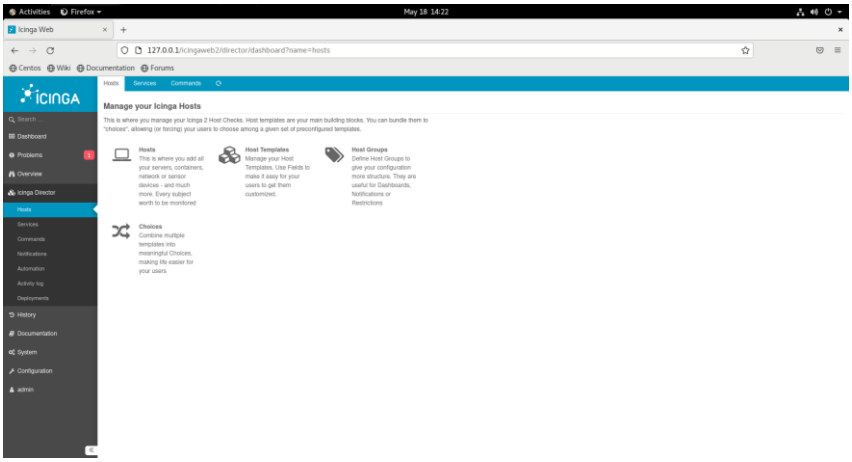

Figura 76 *Despliegue de equipos configurados 3*

Configuración de Servidores:

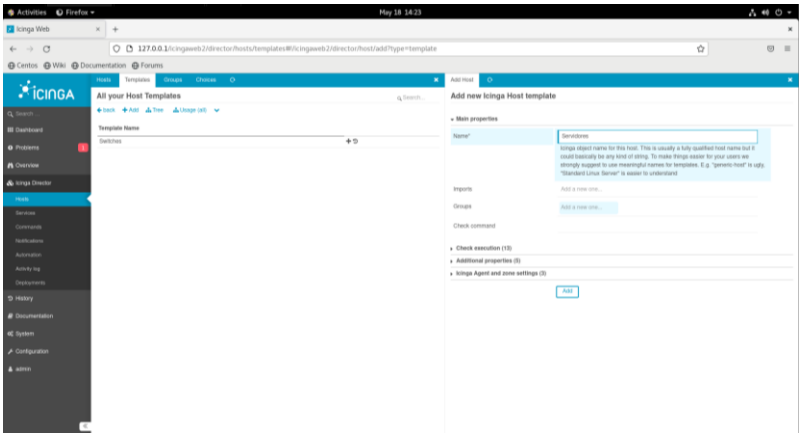

Figura 77 *Despliegue de equipos configurados 4*

Despliegue de la configuración de Servidores correcta:

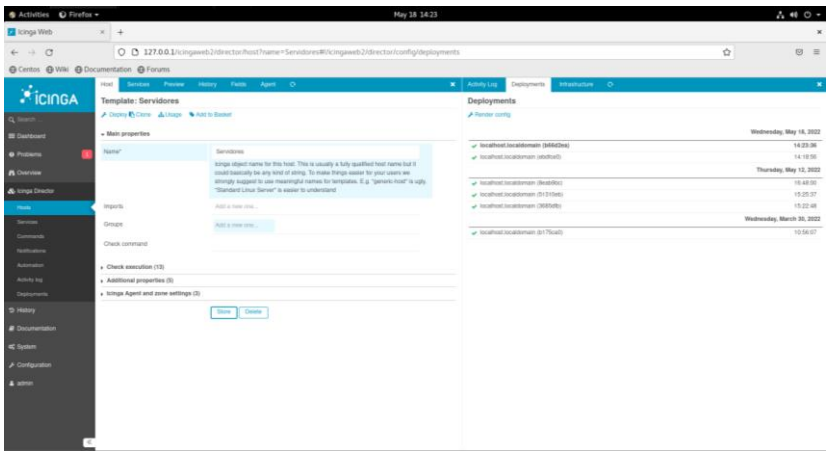

Figura 78 *Despliegue de equipos configurados 5*

Despliegue de la configuración de Servidores correcta:

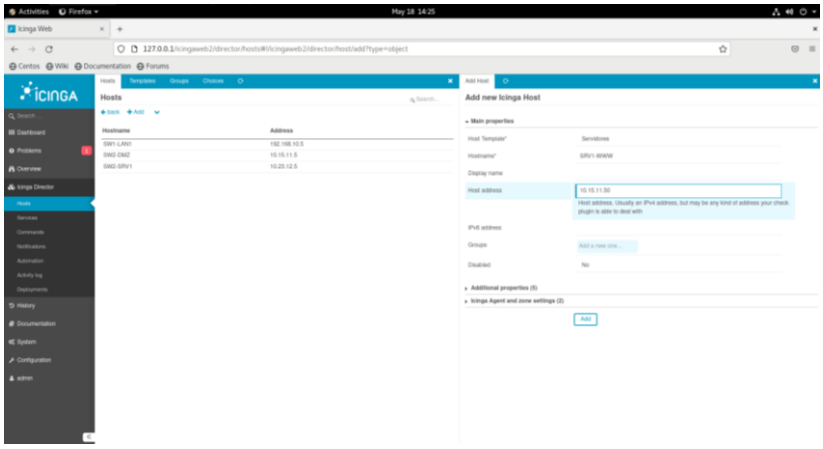

Figura 79 *Despliegue de equipos configurados 6*

Despliegue de la configuración de Servidores en SRV1-WWW:

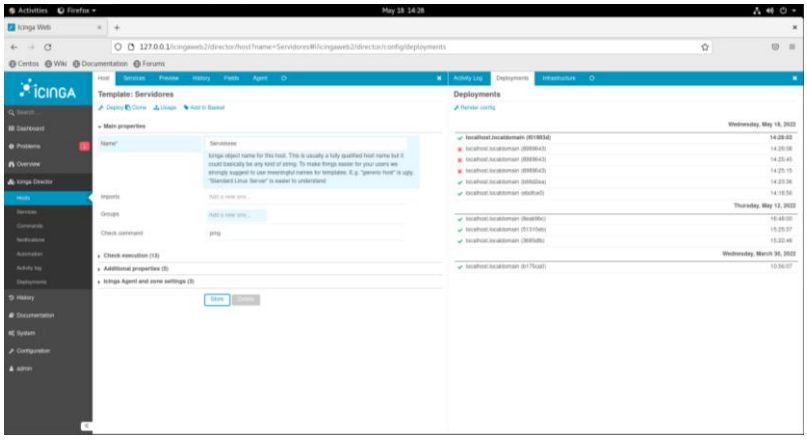

Figura 80 *Despliegue de equipos configurados 7*

Instalación del HTTPD en servicio web:

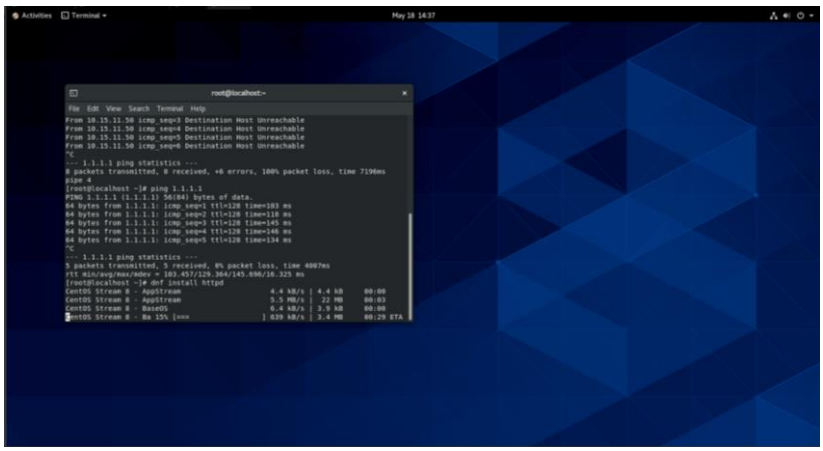

Figura 81 *Despliegue de equipos configurados 8*

Instalación del HTTPD en servicio web:

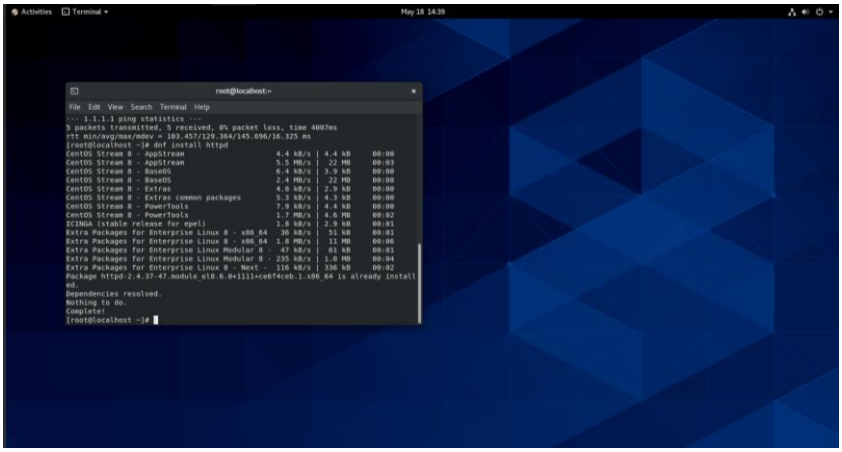

Figura 82 *Despliegue de equipos configurados 9*

Verificación de Iniciar y Habilitar el servicio HTTPD:

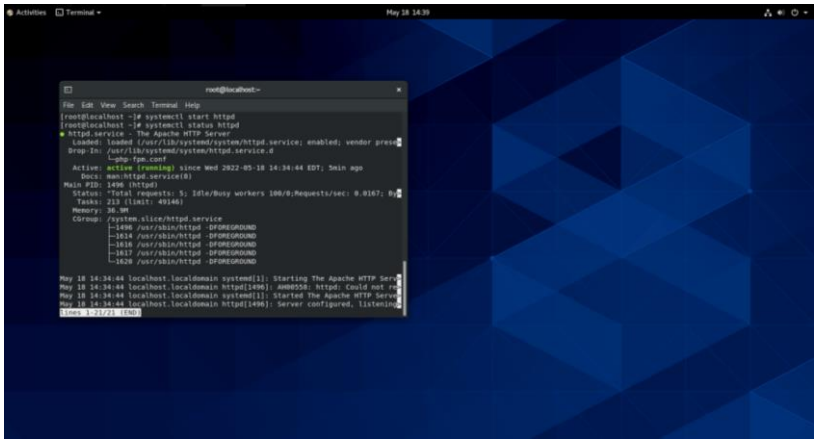

Figura 83 *Despliegue de equipos configurados 10*

Configuración de políticas de seguridad web en el firewall:

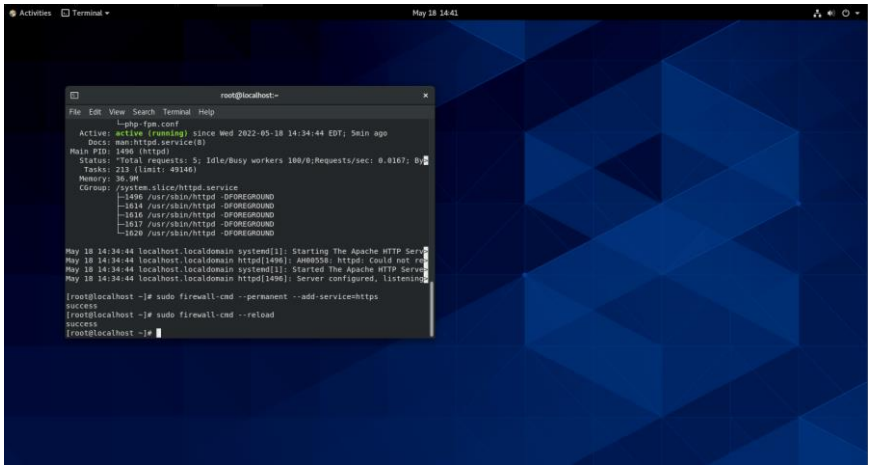

Figura 84 *Despliegue de equipos configurados 11*

Políticas de seguridad entre la zona de SERVIDORES y zona DMZ e Monitoreo de servidor web:

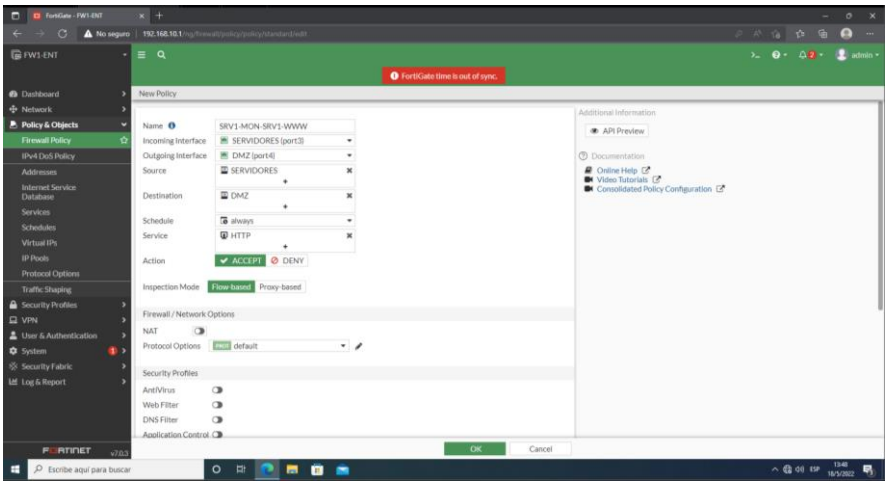

Figura 85 *Despliegue de equipos configurados 12*

Resumen de políticas de seguridad

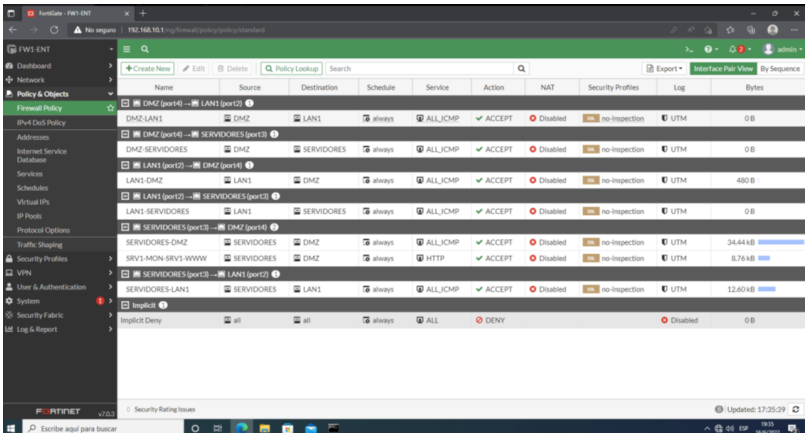

Figura 86 *Despliegue de equipos configurados 13*

Verificación del servicio HTTPD en servicio web con la IP 10.15.11.50:

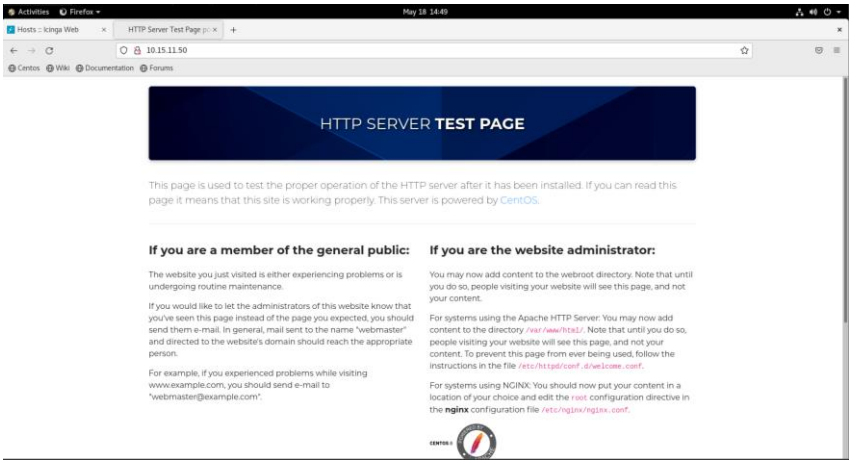

Figura 87 *Despliegue de equipos configurados 14*

Configuración de SRV1-WWW:

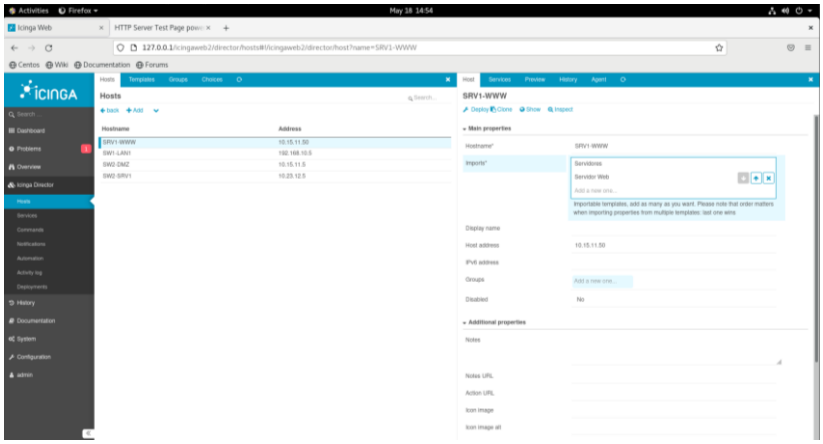

Figura 88 *Despliegue de equipos configurados 15*

Configuración de SRV1-WWW Servicio Web y despliegue de la configuración correcta:

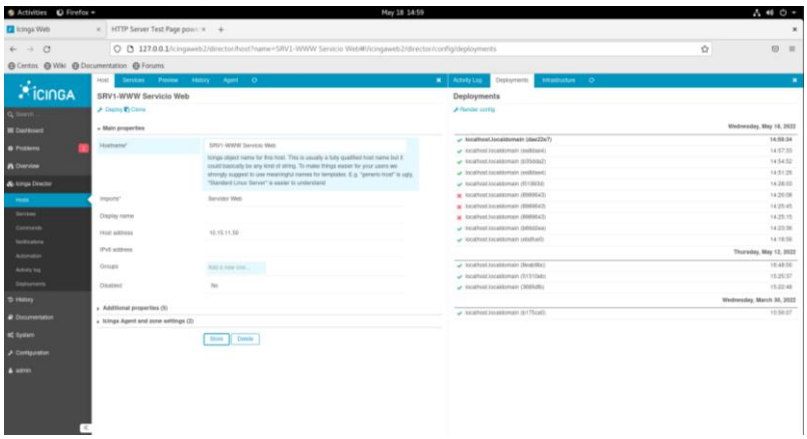

Figura 89 *Despliegue de equipos configurados 16*

Creación en Hostgroup del grupo Switches:

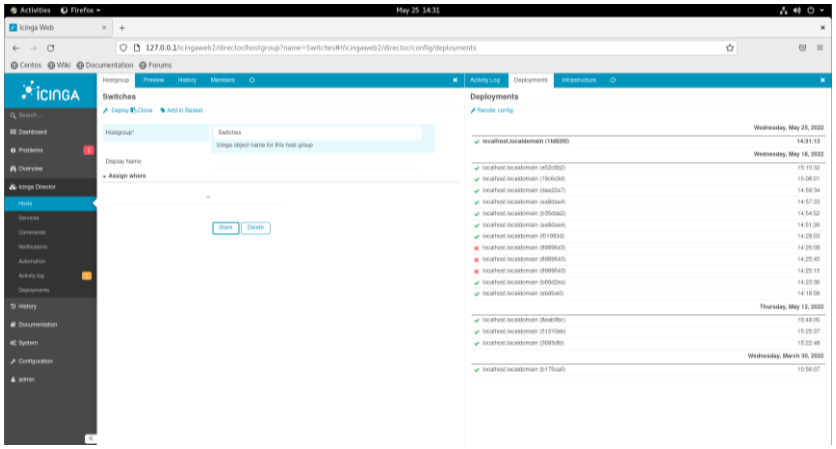

Figura 90 *Despliegue de equipos configurados 17*

Asignación del grupo Switches en la SW1-LAN1:

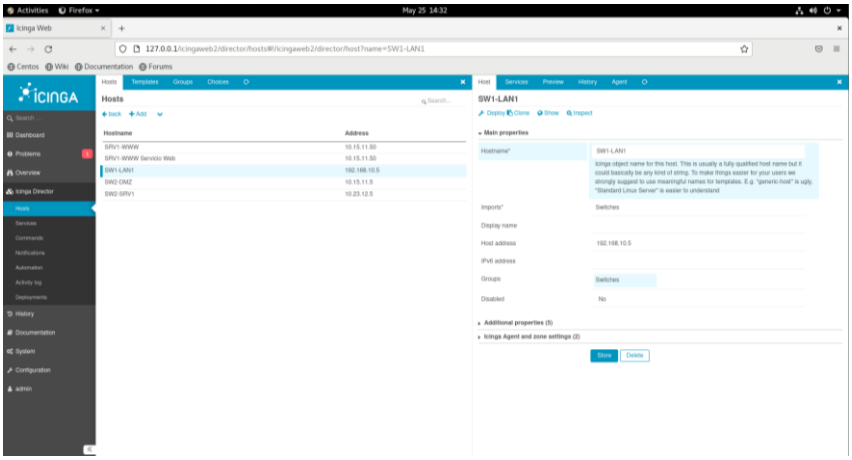

Figura 91 *Despliegue de equipos configurados 18*

Despliegue de la configuración de SW1-LAN1 en grupo Switches correcta:

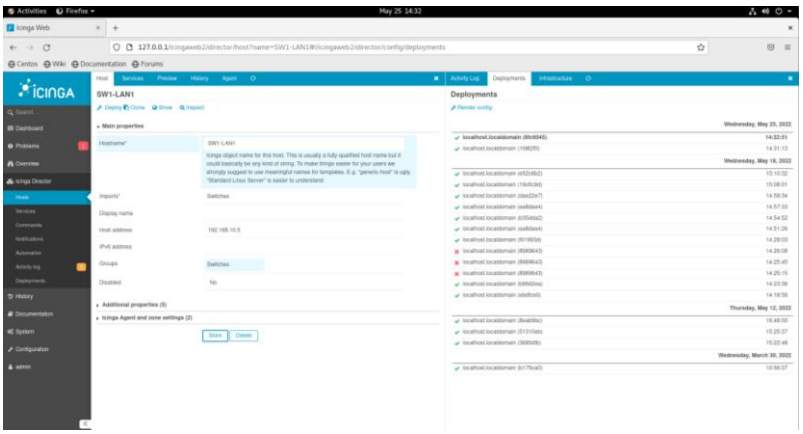

Figura 92 *Despliegue de equipos configurados 19*

Asignación del grupo Switches en la SW2-DMZ:

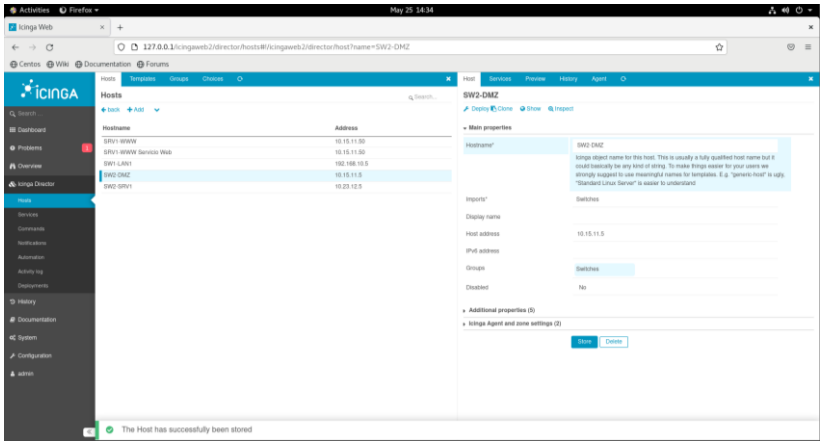

Figura 93 *Despliegue de equipos configurados 20*

Despliegue de la configuración de SW2-DMZ en grupo Switches correcta:

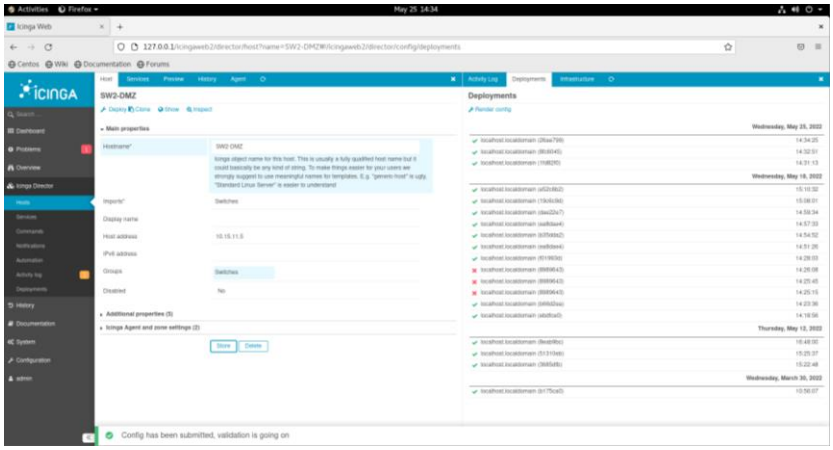

Figura 94 *Despliegue de equipos configurados 21*

Asignación del grupo Switches en la SW2-SRV1:

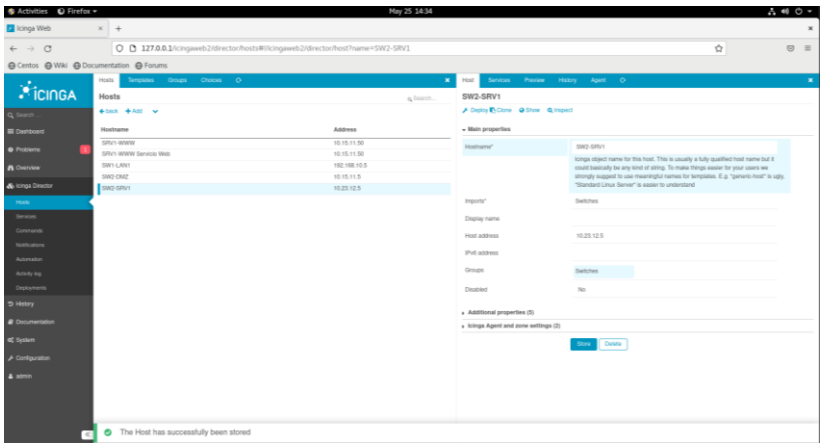

Figura 95 *Despliegue de equipos configurados 22*

Despliegue de la configuración de SW2-SRV1 en grupo Switches correcta:

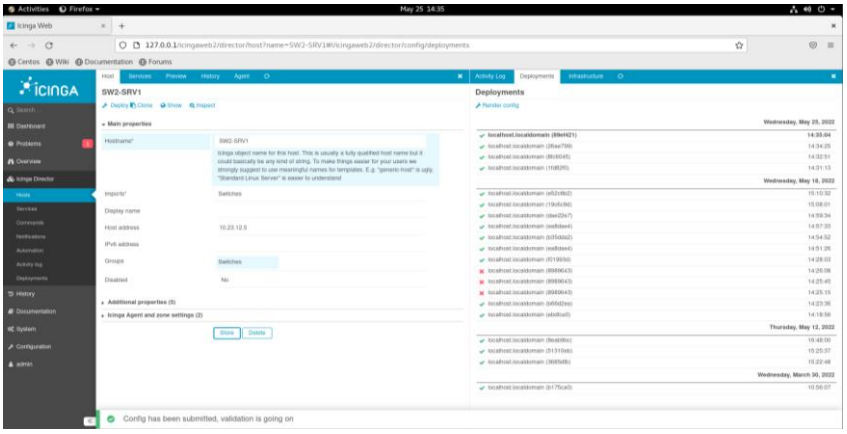

Figura 96 *Despliegue de equipos configurados 23*

Creación en Hostgroup del grupo Servidores Linux:

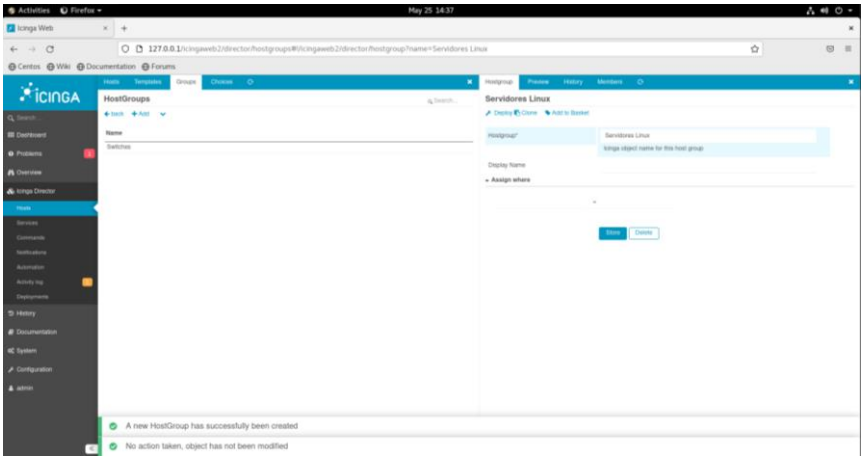

Figura 97 *Despliegue de equipos configurados 24*

Despliegue de la configuración de Servidores Linux:

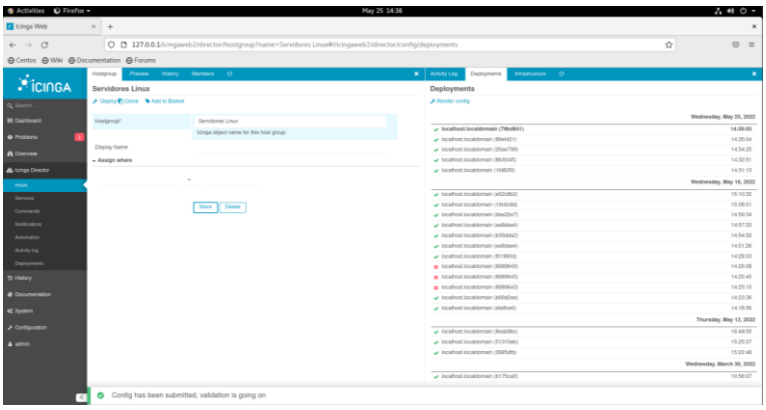

Figura 98 *Despliegue de equipos configurados 25*

Asignación del grupo Servidores Linux en la SRV1-WWW:

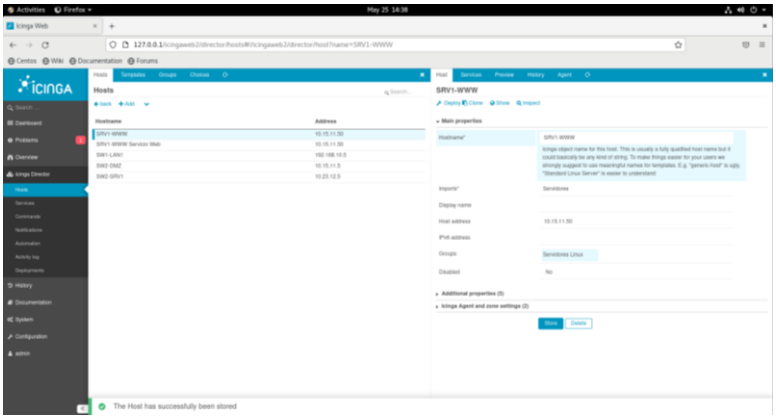

Figura 99 *Despliegue de equipos configurados 26*

Asignación del grupo Servidores Linux en la SRV1-WWW:

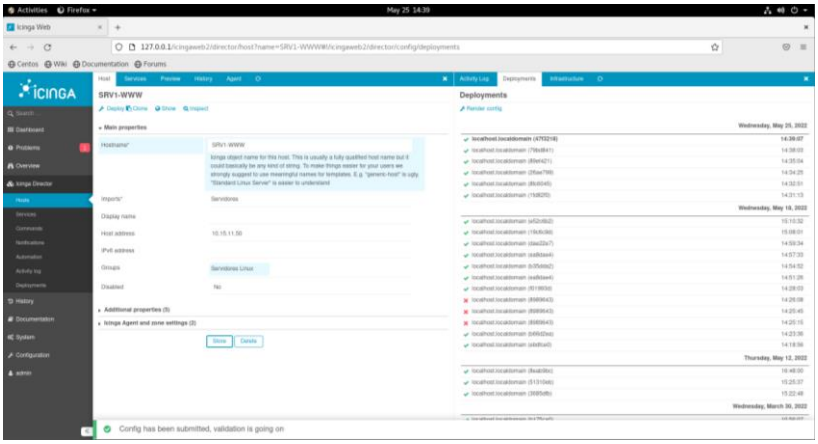

Figura 100 *Despliegue de equipos configurados 27*

Asignación del grupo Servidores Linux en la SRV2-VIRT:

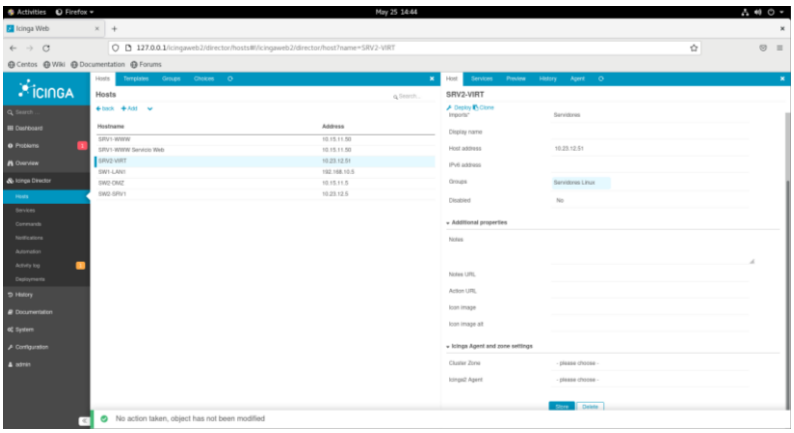

Figura 101 *Despliegue de equipos configurados 28*

Despliegue de la configuración de SVR2-VIRT en el grupo Servidores Linux:

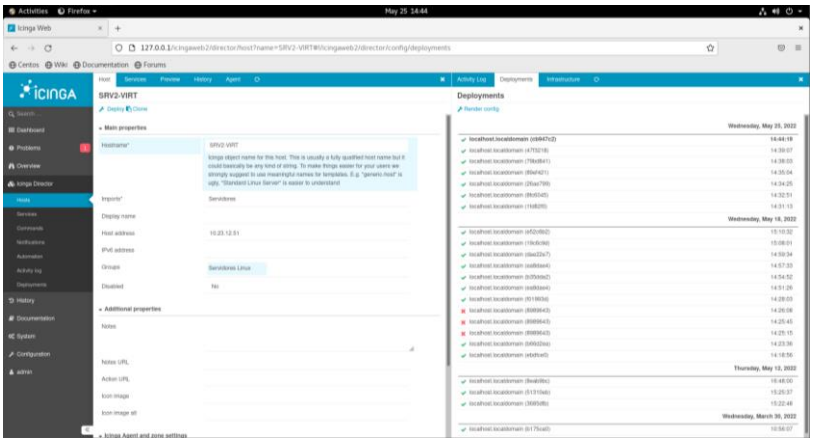

Figura 102 *Despliegue de equipos configurados 29*

Despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados mediante la asignación de los grupos de Switches, Servidores Linux:

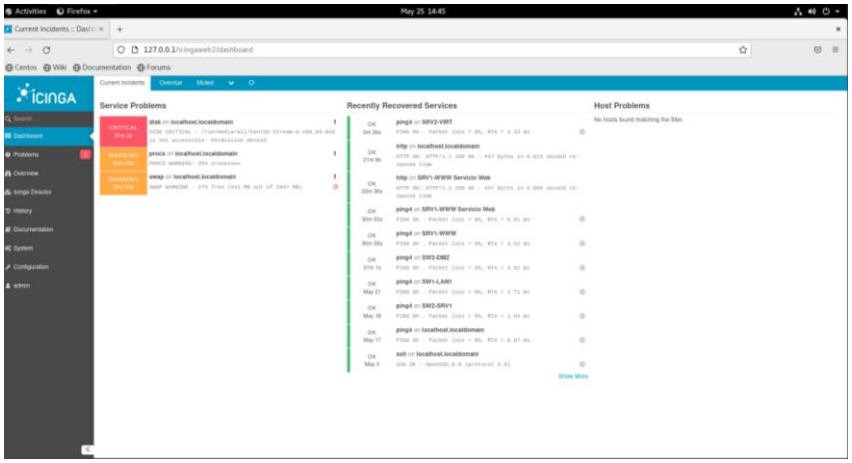

Figura 103 *Despliegue de equipos configurados 30*

Configuración de Firewalls:

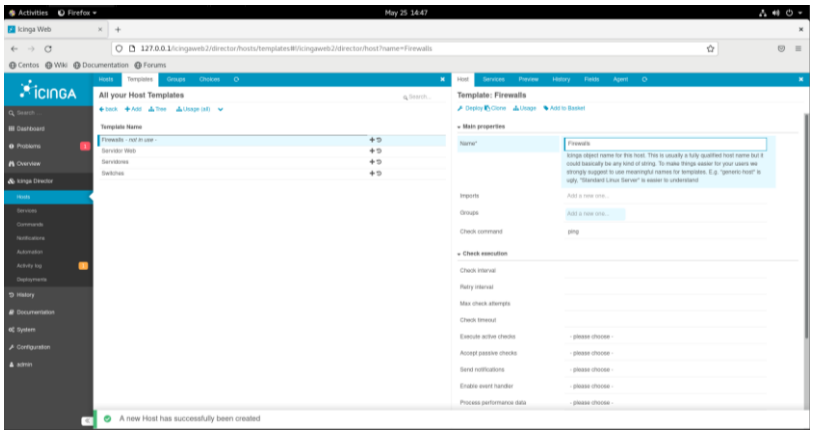

Figura 104 *Despliegue de equipos configurados 31*

Despliegue de la configuración de Firewalls correcta:

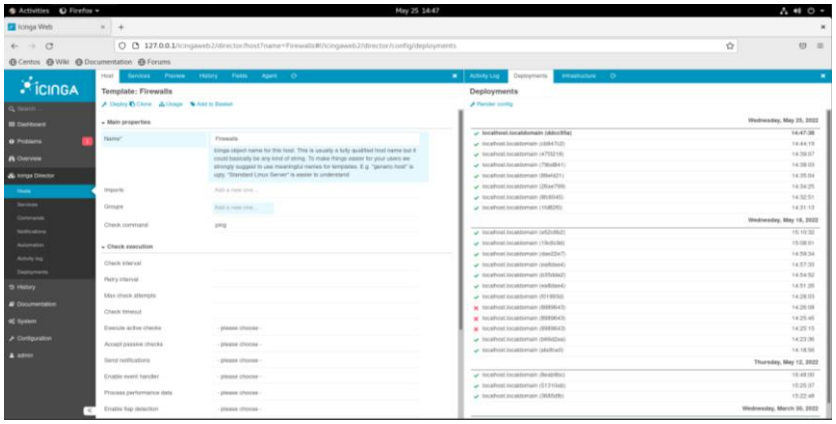

Figura 105 *Despliegue de equipos configurados 32*

Configuración de FW1-ENT en Hosts:

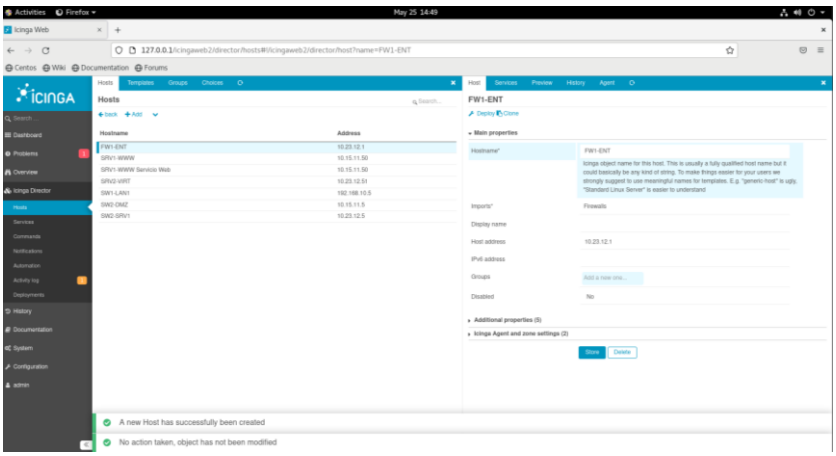

Figura 106 *Despliegue de equipos configurados 33*

Despliegue de la configuración de FW1-ENT correcta:

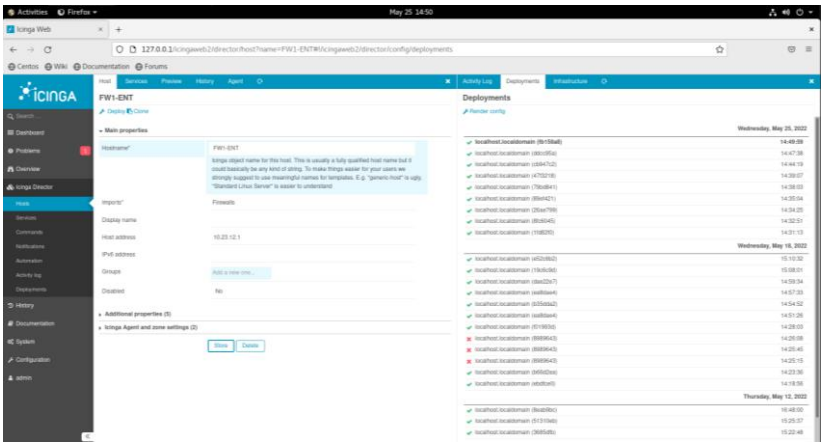

Figura 107 *Despliegue de equipos configurados 34*

Creación en Hostgroup del grupo Firewalls:

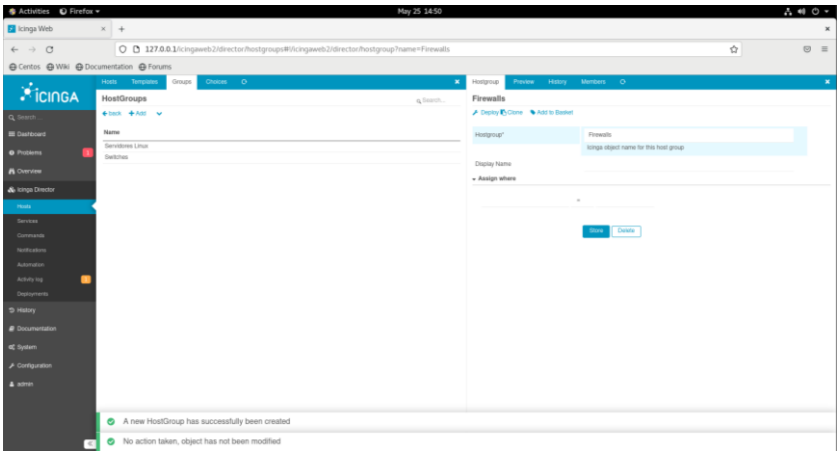

Figura 108 *Despliegue de equipos configurados 35*

Despliegue de la configuración del grupo Firewalls correcta:

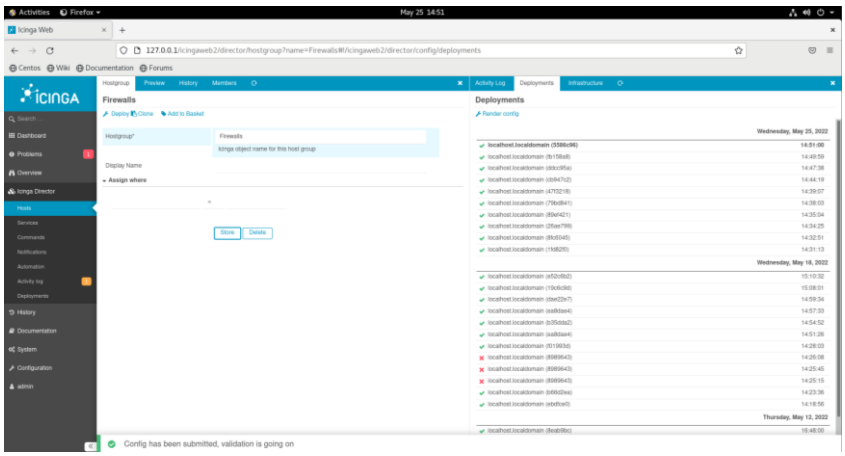

Figura 109 *Despliegue de equipos configurados 36*

Asignación del grupo Firewalls en la FW1-ENT:

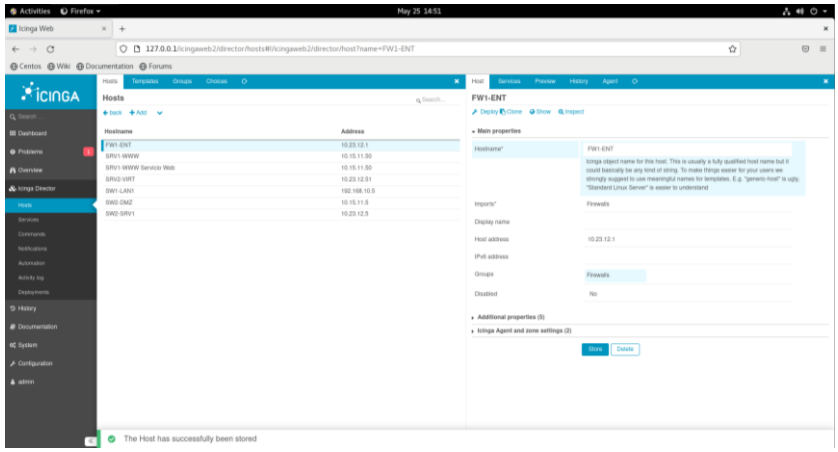

Figura 110 *Despliegue de equipos configurados 37*

Despliegue de la configuración de FW1-ENT en grupo Firewalls correcta:

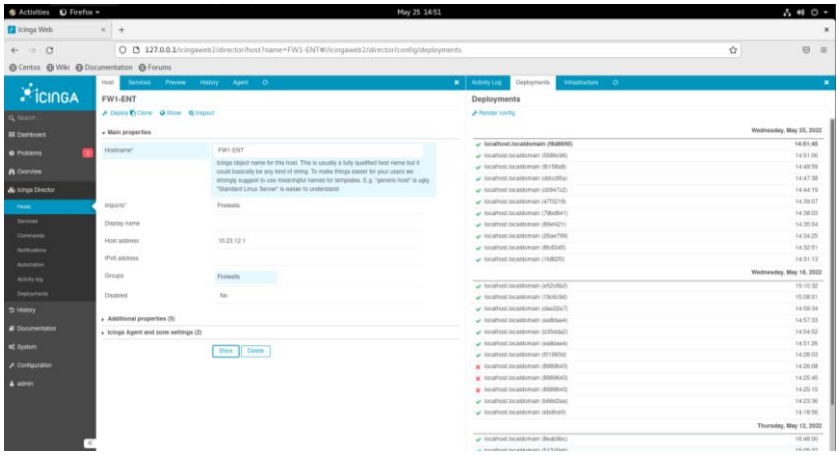

Figura 111 *Despliegue de equipos configurados 38*

Finalmente se muestra la topología completa y la descripción de sus elementos con las herramientas habilitadas:

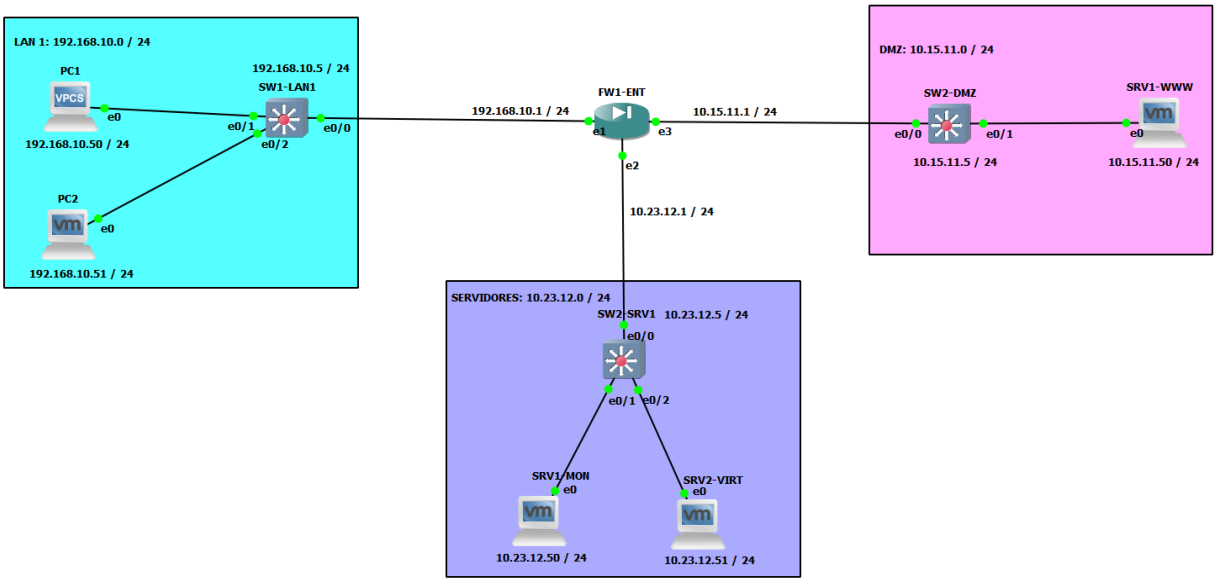

Figura 112 *Despliegue de equipos configurados 39*

Finalmente, como se especificó en la figura 112 se detalló la topología propuesta, a continuación, se hace una descripción más detallada de cada una de las zonas:

- La zona de LAN 1 tiene una conexión directa al firewall FW1-ENT en la interface Ethernet e1. El direccionamiento IP utilizado en la zona de LAN 1 es 192.168.10.0 / 24 en esta zona hay 3 dispositivos:

    - El switch SW1-LAN1 es un switch CISCO IOU L2 con imagen i86bi-linux-l2-ipbasek9-15.1a.bin con las siguientes características memoria RAM 256 MB, memoria NVRAM 32 KB, adaptadores Ethernet 4.
    - La PC1 consta de requerimientos mínimos como el sistema operativo: Sistema (Windows 7 o posterior), IOS (Maverick 10.9 o posterior), Distribución Linux,

Debian, Ubuntu, Procesador: Procesador con 2 o más núcleos / extensión de virtualización, Memoria: Mínimo de 4 GB de RAM, Almacenamiento: Espacio mínimo de 200 MB – Recomendado 1 GB, Adicionales: El almacenamiento de imágenes, requiere más espacio en el equipo (disco duro).

- La PC2 consta de un sistema operativo Windows 10 en una máquina virtual VMware Workstation Pro configurada con las siguientes características Memory: 16 GB, Processors; 2, Hard Disk (NVMe): 60 GB, CD/DVD (SATA): D:\Maquinas Virtuales\Windows\Win10.iso, Network Adapter: Custom (VMnet3), Network Adapter (VMnet1), USB Controller: Present, Sound Card: Auto detect, Serial Port: Using named pipe \\.\pipe\gns3_vmware\0912b7ce-906b-4c9e-b2c7-0837d1b00001, Display: Auto detect.

- La zona de SERVIDORES tiene una conexión directa al firewall FW1-ENT en la interface Ethernet e2. El direccionamiento IP utilizado en la zona de SERVIDORES es 10.23.12.0 / 24 en esta zona hay 3 dispositivos:

  - El switch SW2-SRV1 es un switch CISCO IOU L2 con imagen i86bi-linux-l2-ipbasek9-15.1a.bin con las siguientes características memoria RAM 256 MB, memoria NVRAM 32 KB, adaptadores Ethernet 4.
  - El servidor SRV1-MON este servidor CentOs 8 Stream en una máquina virtual VMware Workstation Pro configurada con las siguientes características Memory: 16 GB, Processors: 1, Hard Disk (NVMe): 20 GB, CD/DVD (IDE): D:\Maquinas Virtuales\centos\CentOS-Stream-8-x86_64-latest-dvd1.iso, Network Adapter: Custom (VMnet13), Network Adapter: Custom (VMnet19), USB Controller: Present, Sound Card: Auto detect, Serial Port: Using named

pipe \\.\pipe\gns3_vmware\01fb60fd-60ab-4f4b-81ae-41c01b3a3412, Display: Auto detect. Dentro de este servidor está instalado ICINGA2

- El servidor SRV2-VIRT este servidor CentOs 8 Stream en una máquina virtual VMware Workstation Pro configurada con las siguientes características Memory: 8 GB, Processors: 4, Hard Disk (NVMe): 20 GB, CD/DVD (IDE): Using unknown backend, Network Adapter: Custom (VMnet6), USB Controller: Present, Sound Card: Auto detect, Serial Port: Using named pipe \\.\pipe\gns3_vmware\3753afd5-04c8-403e-90ec-0df0302810c4, Display: Auto detect. Dentro de este servidor está instalado un servidor web APACHE

- La zona de DMZ tiene una conexión directa al firewall FW1-ENT en la interface Ethernet e3. El direccionamiento IP utilizado en la zona de DMZ es 10.15.11.0 / 24 en esta zona hay 2 dispositivos:

  - El switch SW2-DMZ es un switch CISCO IOU L2 con imagen i86bi-linux-l2-ipbasek9-15.1a.bin con las siguientes características memoria RAM 256 MB, memoria NVRAM 32 KB, adaptadores Ethernet 4.
  - El servidor SRV1-WWW este servidor CentOs 8 Stream en una máquina virtual VMware Workstation Pro configurada con las siguientes características Memory: 16 GB, Processors: 1, Hard Disk (NVMe): 20 GB, CD/DVD (IDE): D:\Maquinas Virtuales\centos\CentOS-Stream-8-x86_64-latest-dvd1.iso, Network Adapter: Custom (VMnet4), Network Adapter: Custom (VMnet1), USB Controller: Present, Sound Card: Auto detect, Serial Port: Using named

pipe \\.\pipe\gns3_vmware\4d3cad4c-7962-4f53-8628-f3956a8f7d6e, Display: Auto detect. Dentro de este servidor está instalado Servicio Web.

- Finalmente, las tres zonas interconectan por medio de un FIREWALL FW1-ENT versión FortiGate VM64-KVM v7.0.3 build0237 (GA) con imagen Quemu binary: /usr/bin/quemu-system-x86_64 (v4.2.1), RAM: 1024 MB, vCPUs: 1, Adapters; 4

3.2. Describir los beneficios y servicios que brinda una red de accesos utilizando topología en GNS3.

En el caso de este proyecto la descripción de los beneficios se centra en un modelo de red de acceso cableada.

Las redes de acceso por cable se configuran donde un cliente se conecta a una ubicación específica a través de la terminal de su proveedor de servicios le brinda conexión a través del medio cableado. El medio de acceso puede ser par de cobre, string coextensive o fibra óptica. Entre los beneficios que se aplican a este tipo de red se pueden mencionar:

- Capacidad para simular escenarios de distintos tipos de capa física.
- Capacidad para virtualizar los sistemas operativos o firmware de los dispositivos de red.
- Capacidad de virtualizar dispositivos de red de la línea Cisco® reales
- Herramienta Open Source estándar de mercado y de amplio uso.

3.2.1. Capacidad para simular escenarios de distintos tipos de capa física

GNS3 permite modelar la capa física con par de cobre o fibra óptica de acuerdo a las necesidades del proyecto, así en este caso para la topología de red de acceso desarrollada se utilizó una capa física de par de cobre cuya velocidad está determinada por las características de la capa de enlace de los IOS usados durante la virtualización de los mismos. Como se muestra en la Figura 112 es una topología estrella.

3.2.2. Capacidad para virtualizar los sistemas operativos o firware de los dispositivos de red

GNS3 permite virtualizar los IOS reales de los dispositivos de red, lo que facilita que el modelamiento proporcione comportamientos similares a la implementación física, adicionalmente se puede interactuar con virtualizadores de sistemas operativos como Oracle Virtual Box® y similares, para esto GNS3 usa Dynamips, Dynagen, Quemu, Pemu, VirtualBox y VMware Workstation Pro.

En el caso del proyecto se usó el virtualizador Oracle Virtual Box® para los servidores o equipos de escritorio mientras que los dispositivos de red se configuraron con los respectivos IOS como se muestra en la siguiente tabla:

Dispositivo	Firmware / SO
Switch SW1-LAN1	CISCO IOU L2
Switch SW2-SRV1	CISCO IOU L2
Switch SW2-DMZ	CISCO IOU L2
PC1	Máquina por defecto en GNS3
PC2	Máquina Windows 10
SRV1-MON	Máquina CentOs 8 Stream
SRV2-VIRT	Máquina CentOs 8 Stream
SRV1-WWW	Máquina CentOs 8 Stream

FW1- ENT	FortiGate VM64-KVM v7.0.3

Nota: Elaborado por Ortiz, 2022

3.2.3. Capacidad para virtualizar dispositivos de red de la línea Cisco® reales

GNS3 permite modelar una red eficiente y rentable para los usuarios, también permite simular los dispositivos de red de esta marca, como switchs, enrutadores, etc. Estos deben ser descargados para poder usar el software. Se debe tener cuidado con las licencias de uso. Como ejemplo se puede mencionar Cisco c3600.

Para el modelado de la red de acceso de este proyecto se usaron los siguientes dispositivos:

- Switch SW1-LAN1 - CISCO IOU L2
- Switch SW2-SRV1 - CISCO IOU L2
- Switch SW2-DMZ - CISCO IOU L2
- PC1 – Máquina por defecto en GNS3
- PC2 – Máquina Windows 10 a través de VMware.
- SRV1-MON – Máquina CentOs 8 Stream a través de VMware, instalación de ICINGA2.
- SRV2-VIRT - Máquina CentOs 8 Stream a través de VMware, instalación de un servidor web APACHE.
- SRV1-WWW - Máquina CentOs 8 Stream a través de VMware, instalación de Servicio Web.
- FW1- ENT – Firewall versión FortiGate VM64-KVM v7.0.3

Se puede personalizar en la propia plataforma. No se requiere interacción con la línea de comandos, lo cual es un gran problema. GNS3 bloquea todos los niveles de dificultad que permiten controlar y realizar.

3.2.4. Herramientas Open Source estándar de mercado y amplio uso

GNS3 es una de las mejores simulaciones de red disponibles actualmente en el mercado. La herramienta no solo es de código abierto, también es utilizado en el foro que es grande y funcional. Con los últimos avances en tecnología, el software de identificación de redes se considera el próximo gran avance para sus clientes.

3.3. Analizar los recursos que contiene la tecnología Icinga 2 para el monitoreo de redes.

Icinga proporciona métodos de exportación (en tiempo real) donde los datos del usuario se recuperan para un procesador externo (en términos de Idea). Además, la posición mental se puede desarrollar con módulos. Es uno de los más útiles en los gráficos. Como sugiere el nombre, es solo para un módulo.

Los informes en forma de gráficos sólidos (el usuario puede definir plantillas de gráficos, tipos de conjuntos, etc.). De esta forma, recopila datos de rendimiento en una base de datos separada utilizando un servicio de recopilación gráfica. De esta manera, un usuario reflexivo puede analizar el historial de procesamiento de datos. El plugin de comprobación sin agentes en lo servicios y sistemas de destino es:

- Protocolo de Gestión de la Plataforma Inteligente para obtener información del Baseboard Management Controller de la placa del sistema (sensores que proporcionan velocidades de los ventiladores y eventos del sistema - eventos de arranque del sistema, errores de hardware, etc.)

También se encuentran los recursos de Icinga2 los cuales son:

- Sistema para monitorización de redes

- Herramientas para control de los recursos de la red,
- Sistema de notificación de errores al usuario
- Sistema de reporte de rendimiento y estado de los recursos.
- Flexibilidad para ser escalable y extensible,
- Capacidad para controlar entornos complejos y grandes a través de lugares dispersos.

3.4. Análisis los resultados del monitoreo de dispositivos de red con la herramienta Icinga2.

Una vez realizada la implementación de la topología de red en estrella estructurada con GNS3 y monitoreada con ICINGA2 se evaluarán los siguientes resultados:

- Interface Web
- Visualización de los equipos configurados
- Monitorización de servicios de red (HTTP, SSH, ping)
- Monitorización de componentes de los equipos (switches, pcs)
- Notificación a usuarios por correo electrónico
- Nivel de alertas

Para analizar los resultados descritos previamente serán necesarias las acciones que se muestran en la siguiente tabla:

Tabla 4 *Acciones a seguir*

Item	Descripción del resultado	Acciones a realizarse
1	Interface Web	Captura interfaces de Icinga2
2	Visualización de los equipos configurados	Mostrar en el panel de Icinga2 el listado de equipos configurados con sus características.
3	Monitorización de servicios de red (HTTP, SSH, ping)	Generación de trafico de los distintos protocolos para capturarlos y mostrarlos a través de la interface de Icinga2

4	Monitorización de componentes de los equipos	Mostrar en el panel de Icinga2 el listado de componentes de red configurados con sus características
5	Notificación a usuarios por correo electrónico	Validación de la recepción de correos de notificación a los usuarios
6	Nivel de alertas	Se ejecutarán actividades que disparen las alertas en el monitoreo y mostrarlas en el panel de ICINGA2

Nota: Elaborado por Ortiz, 2022

3.4.1. Interface Web

A continuación, se muestra la interface de Icinga2:

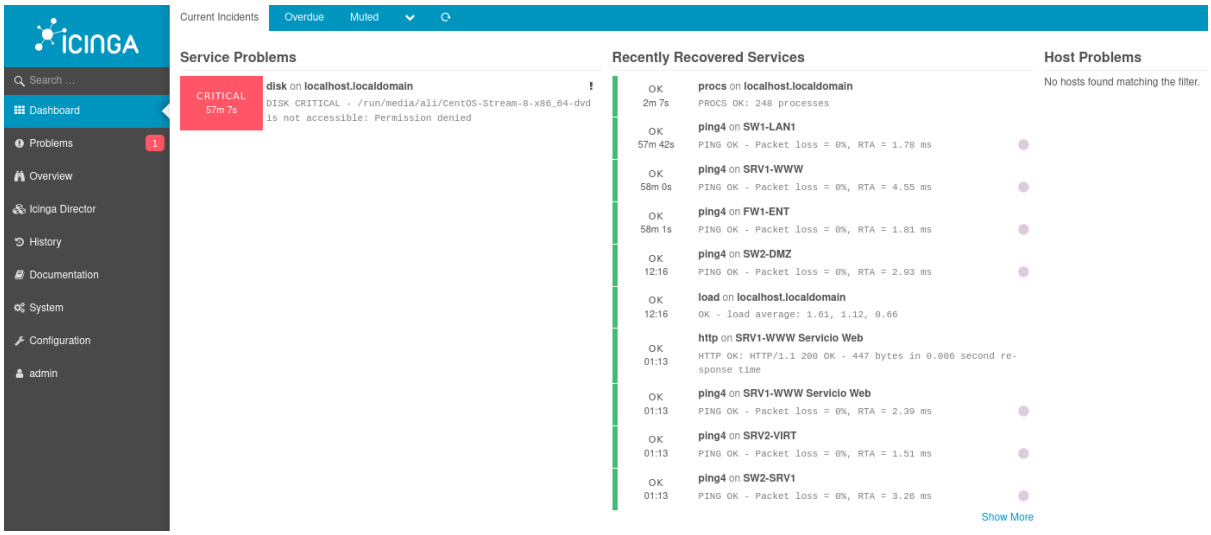

Figura 113 *Despliegue de equipos configurados 40*

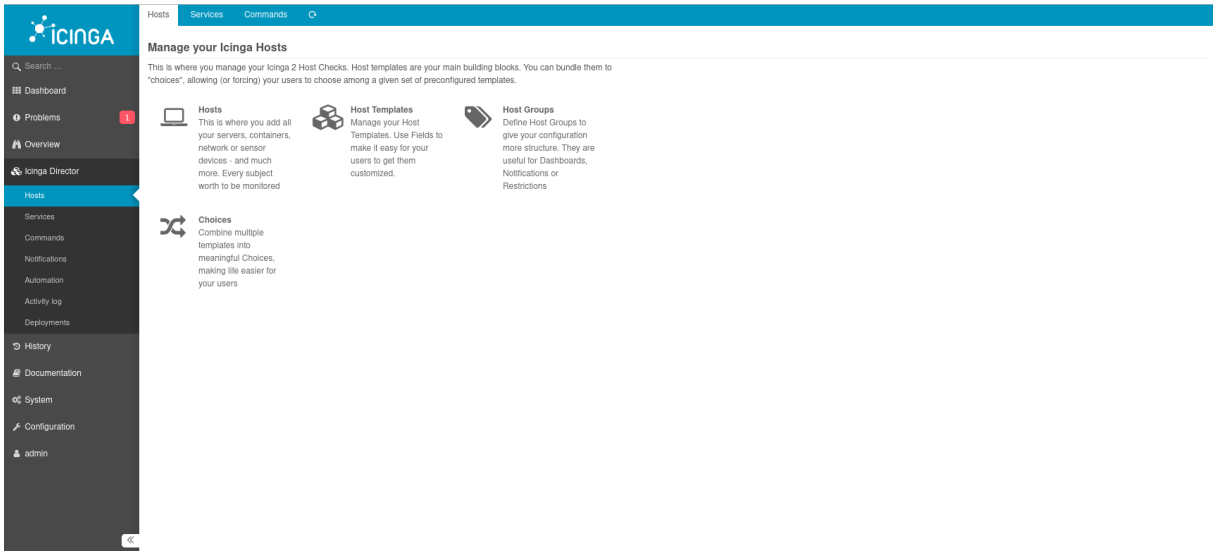

Figura 114 *Despliegue de equipos configurados 41*

3.4.2. Visualización de los equipos configurados

A continuación, se muestra el panel de Icinga2 con el listado de equipos configurados con sus características:

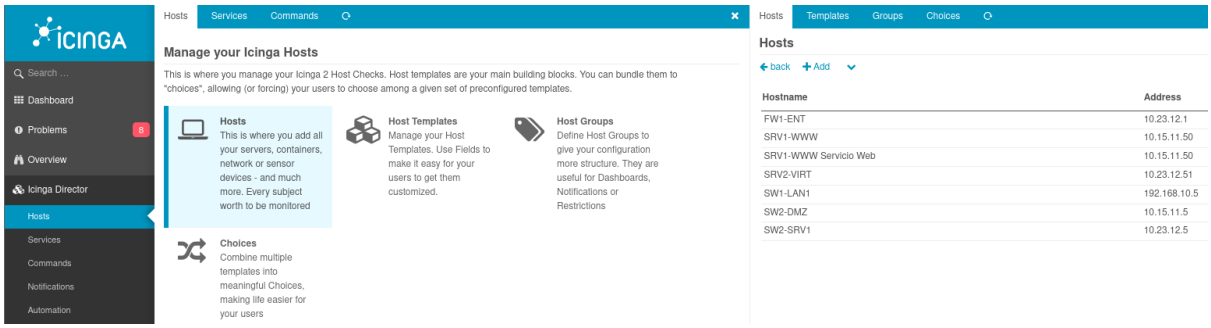

Figura 115 *Despliegue de equipos configurados 42*

3.4.3. Monitorización de servicios de red (HTTP, SSH, ping)

Para analizar este resultado fue necesario generar tráfico de los distintos protocolos para capturas y mostrarlos a través de la interfaz de Iginga2:

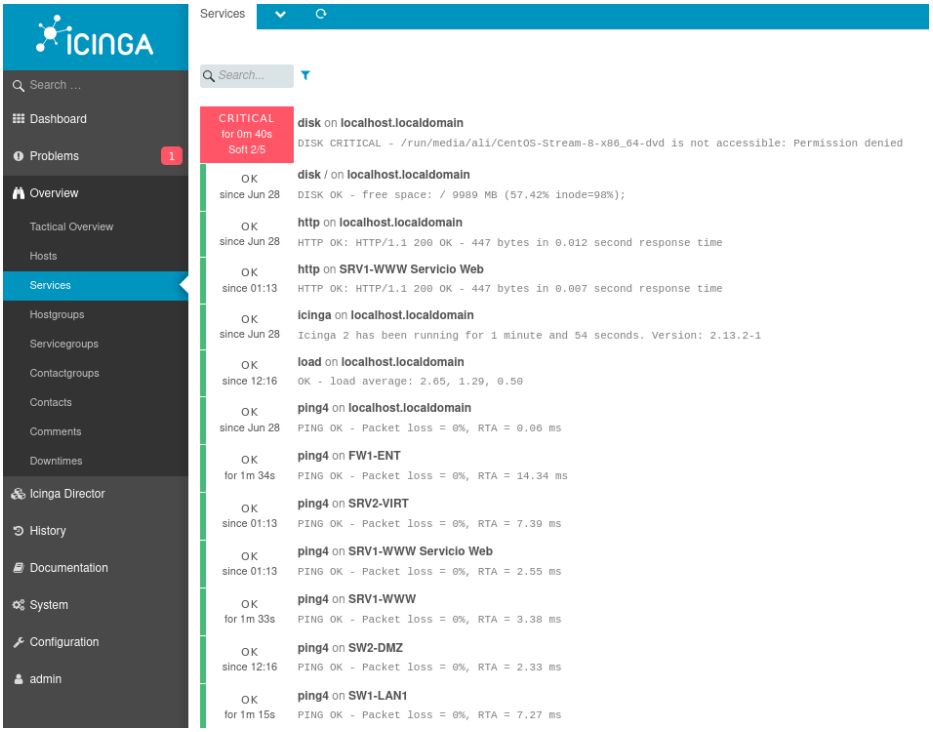

Figura 116 *Despliegue de equipos configurados 43*

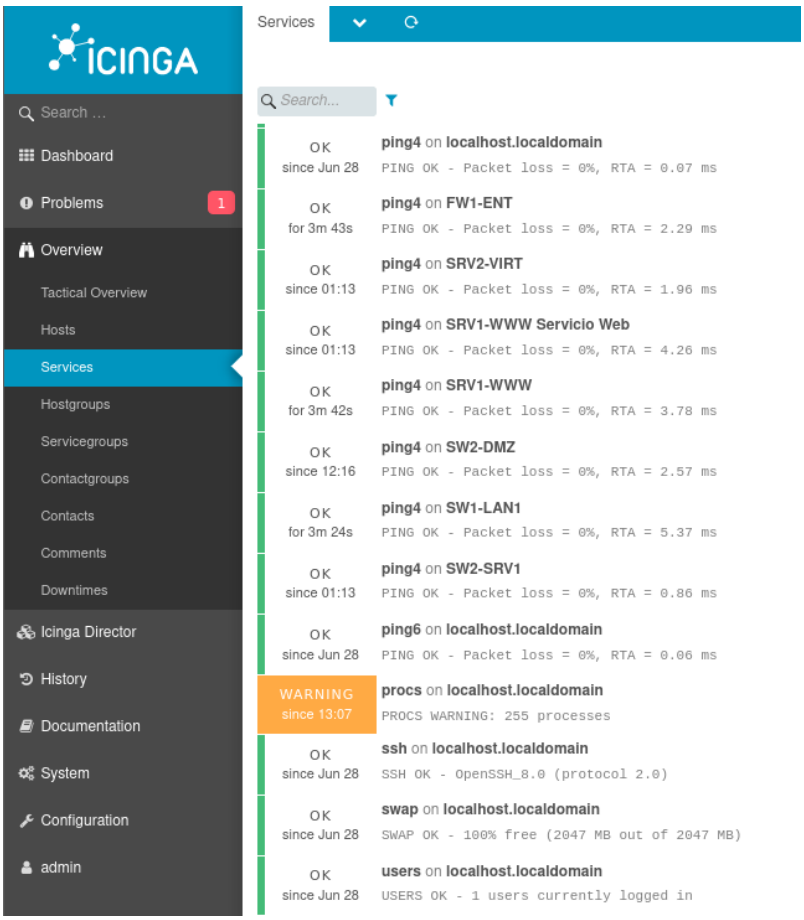

Figura 117 *Despliegue de equipos configurados 44*

3.4.4. Monitorización de componentes de los equipos

Mostrar en el panel de Icinga2 el listado de componentes de red configurados con sus características:

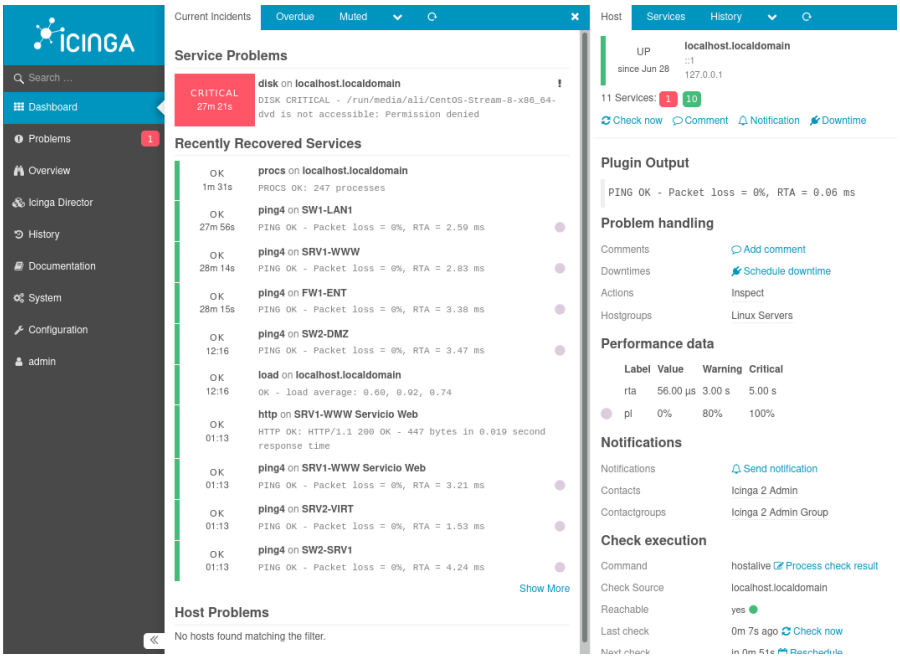

Figura 118 *Despliegue de equipos configurados 45*

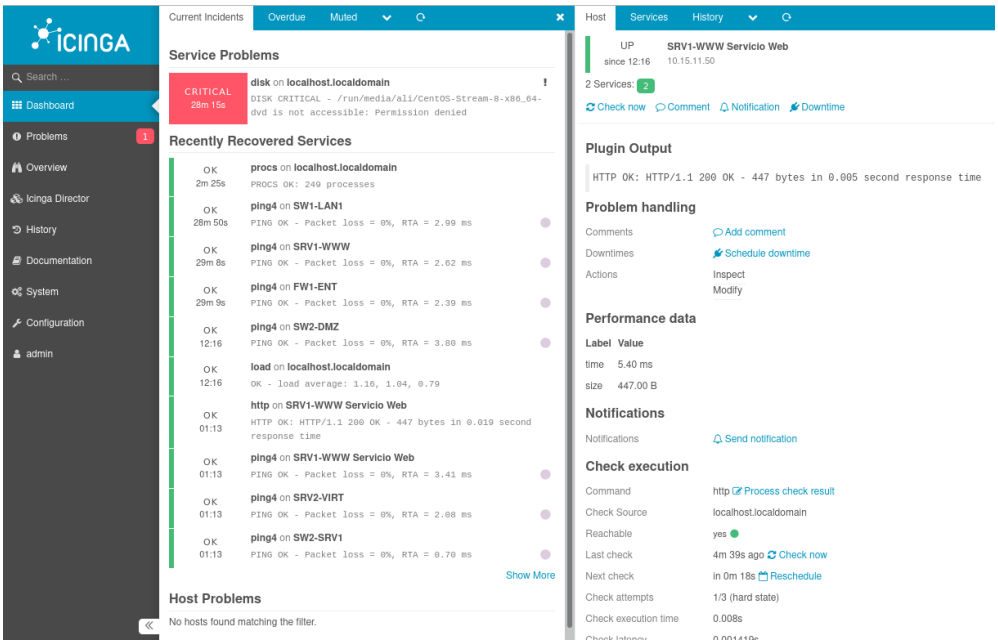

Figura 119 *Despliegue de equipos configurados 46*

3.4.5. Notificación a usuarios por correo electrónico

Se configuraron correos genéricos pero dado que no está conectado a internet y no cuenta con una red interna de correo, no se envían los correos:

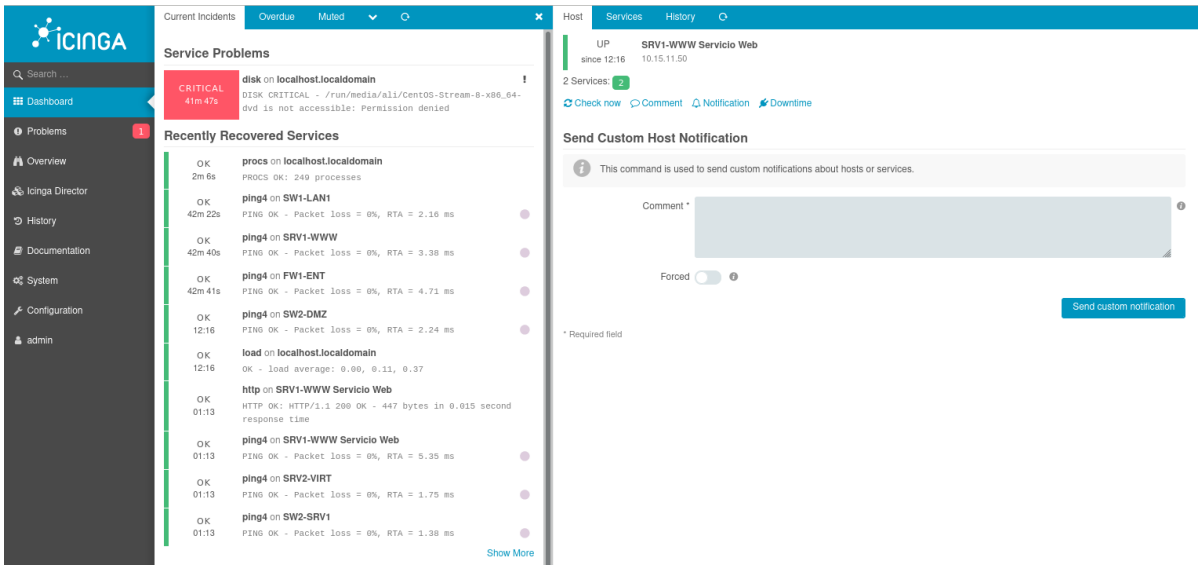

Figura 120 *Despliegue de equipos configurados 47*

3.4.6. Nivel de alertas

Nivel de alertas:

- DOWN
- UP
- WARNING

Para el monitoreo de los servicios se van a realizaron 5 simulaciones:

- Simulación 1 Operación de la red – Condiciones Normales
- Simulación 2 Operación de la red – Caída de red de la Zona LAN 1
- Simulación 3 Operación de la red – Caída de red de la Zona DMZ
- Simulación 4 Operación de la red – Caída de red de la Zona SERVIDORES

- Simulación 5 Operación de la red – Caída general del FIREWALL

Simulación 1 Operación de la red – Condiciones Normales:

Despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados:

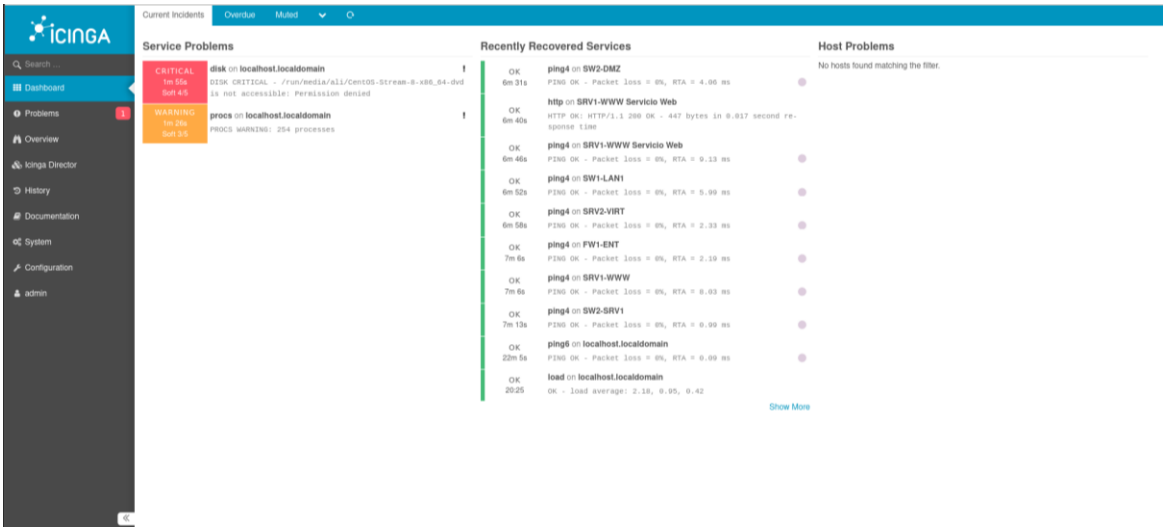

Figura 121 *Despliegue de equipos configurados 48*

Simulación 2 Operación de la red – Caída de red de la Zona LAN 1

Lo que se hizo para simular la caída fue desconectar la Zona LAN 1 con el FIREWALL como se muestra en la topología y se muestra el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados.

Como se muestra en el grafico a continuación se desconectó el switch SW1-LAN1 del firewall FW1-ENT para simular la caída del enlace de la zona LAN 1 con el FIREWALL:

Simulación de caída de la zona LAN1

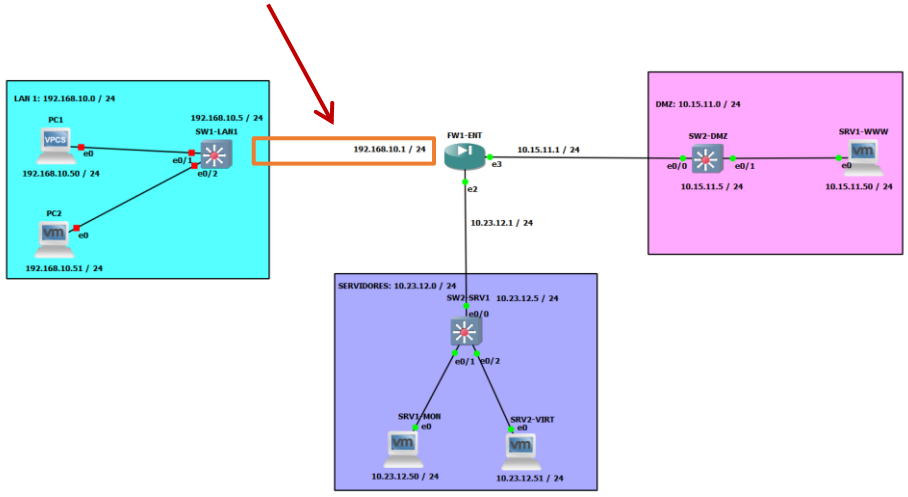

Figura 122 *Despliegue de equipos configurados 49*

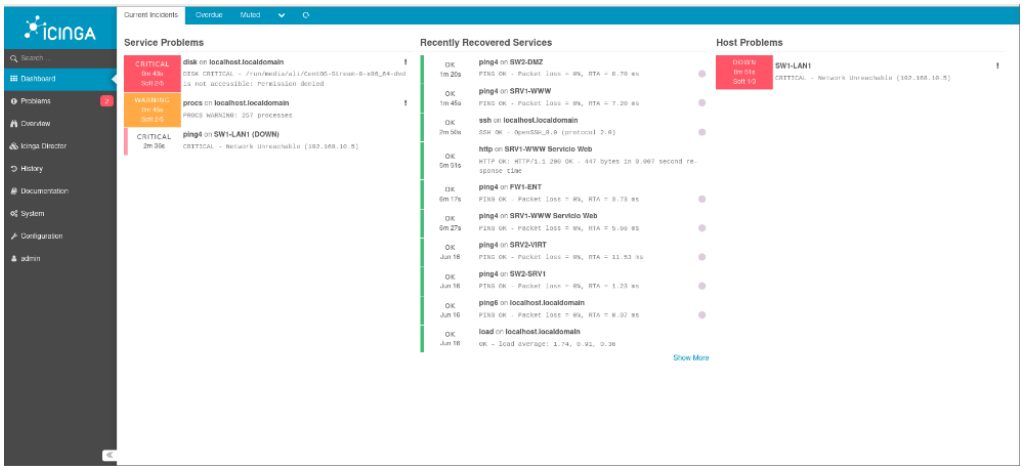

Figura 123 *Despliegue de equipos configurados 50*

Verificación del levantamiento de la zona LAN 1 en el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados. Nuevamente se restable en el enlace entre el switch SW1-LAN1 con el firewall FW1-ENT en condiciones normales y la topología queda de la siguiente manera:

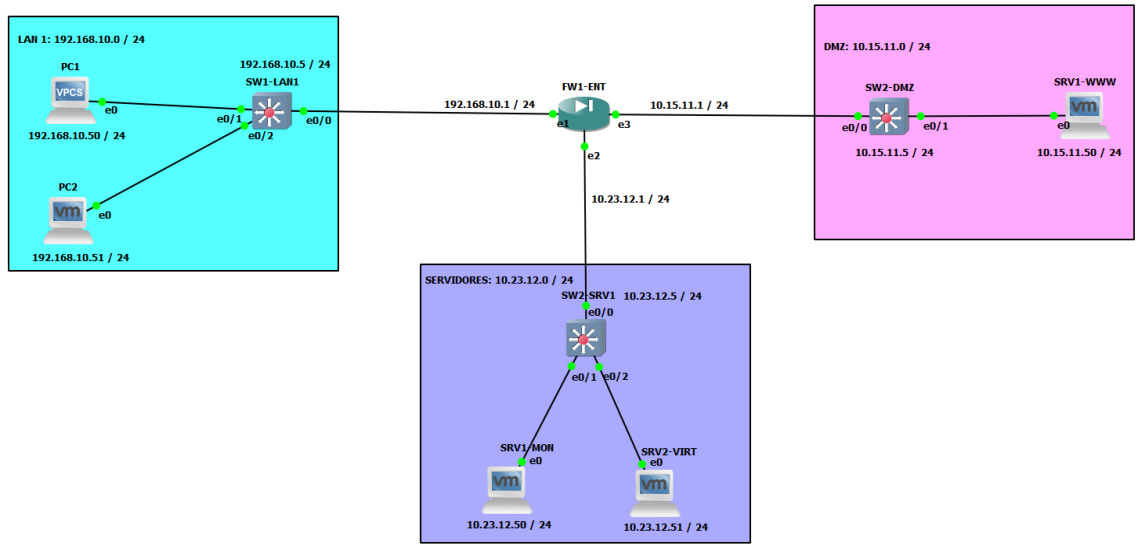

Figura 124 *Despliegue de equipos configurados 51*

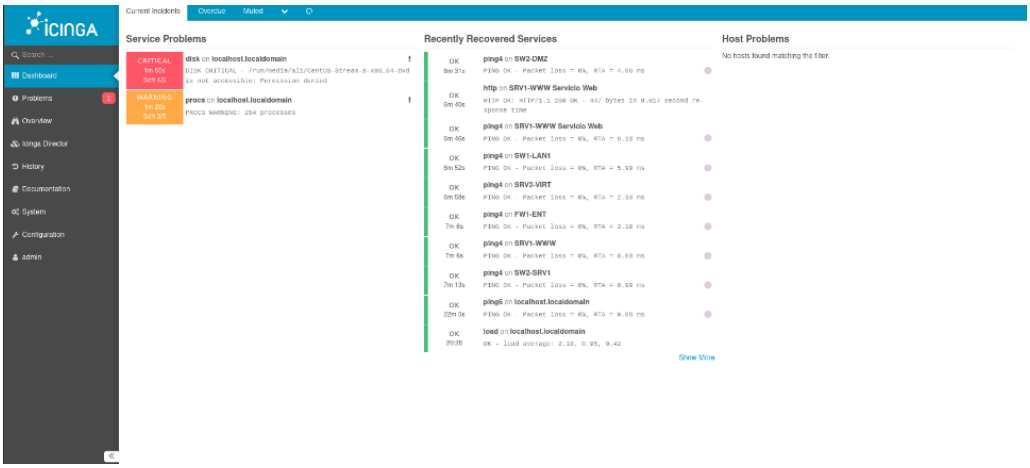

Figura 125 *Despliegue de equipos configurados 52*

Simulación 3 Operación de la red – Caída de red de la Zona DMZ

Lo que se hizo para simular la caída fue desconectar la Zona DMZ con el FIREWALL como se muestra en la topología y se muestra el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados.

Como se muestra en el grafico a continuación se desconectó el switch SW2-DMZ del firewall FW1-ENT para simular la caída del enlace de la zona DMZ con el FIREWALL:

Simulación de caída de la zona DMZ

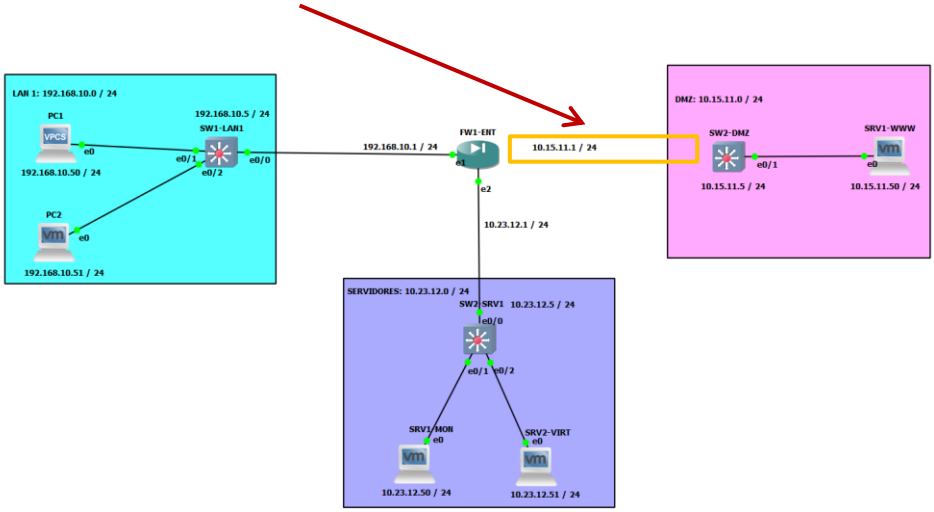

Figura 126 *Despliegue de equipos configurados 41a*

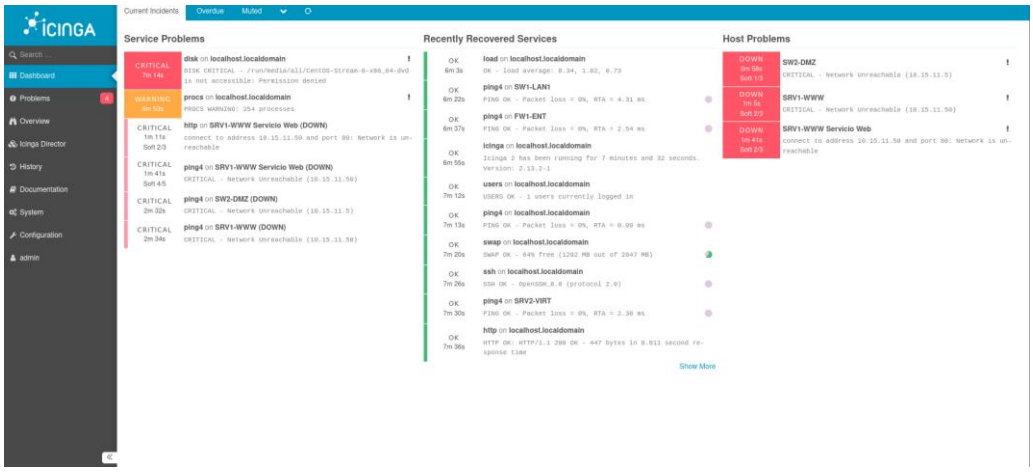

Figura 127 *Despliegue de equipos configurados 41b*

Verificación del levantamiento de la zona DMZ en el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados. Nuevamente se restable en el enlace entre el switch SW2-DMZ con el firewall FW1-ENT en condiciones normales y la topología queda de la siguiente manera:

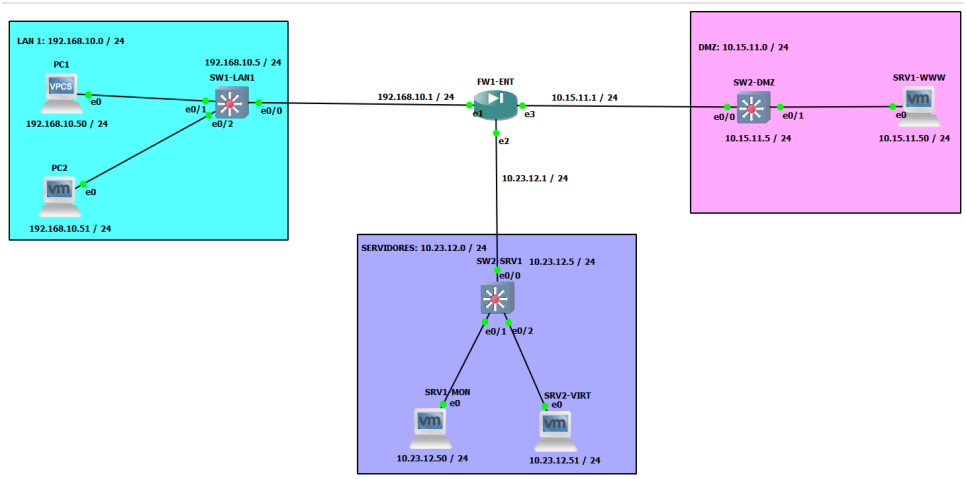

Figura 128 *Despliegue de equipos configurados 41c*

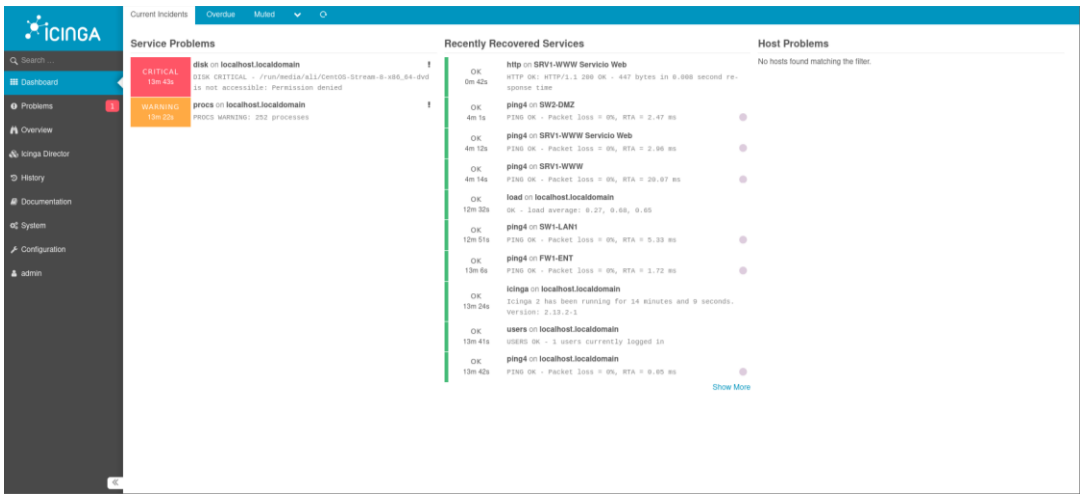

Figura 129 *Despliegue de equipos configurados 41d*

Simulación 4 Operación de la red – Caída de red de la Zona SERVIDORES

Lo que se hizo para simular la caída fue desconectar la Zona SERVIDORES con el FIREWALL como se muestra en la topología y se muestra el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados.

Como se muestra en el grafico a continuación se desconectó el switch SW2-SVR1 del firewall FW1-ENT para simular la caída del enlace de la zona SERVIDORES con el FIREWALL:

Simulación de caída de la zona SERVIDORES

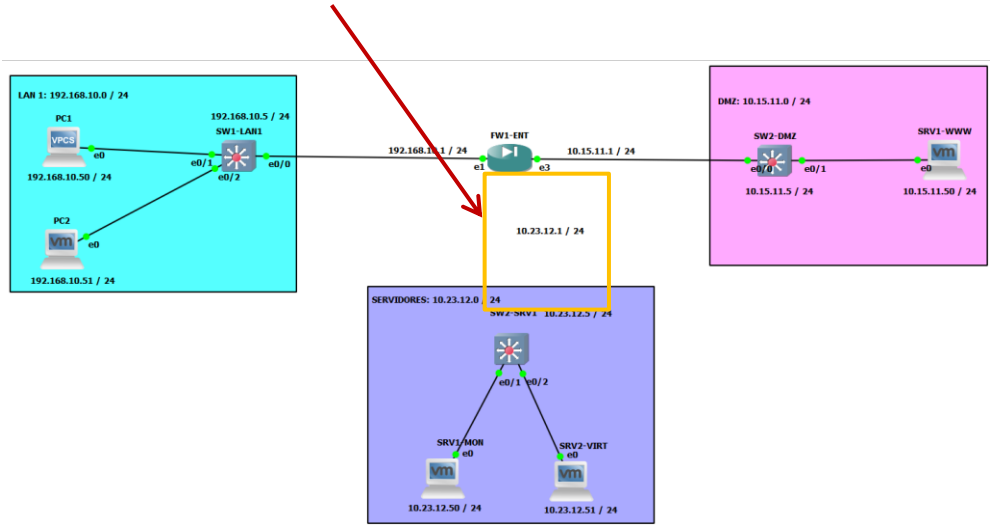

Figura 130 *Despliegue de equipos configurados 41e*

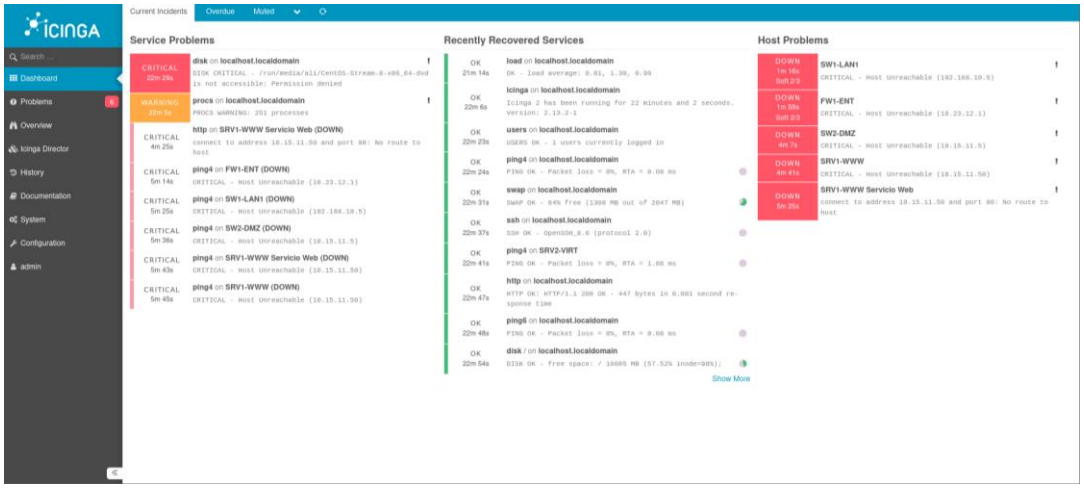

Figura 131 *Despliegue de equipos configurados 41f*

Verificación del levantamiento de la zona SERVIDORES en el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados. Nuevamente se restable en el enlace entre el switch SW2-SRV1 con el firewall FW1-ENT en condiciones normales y la topología queda de la siguiente manera:

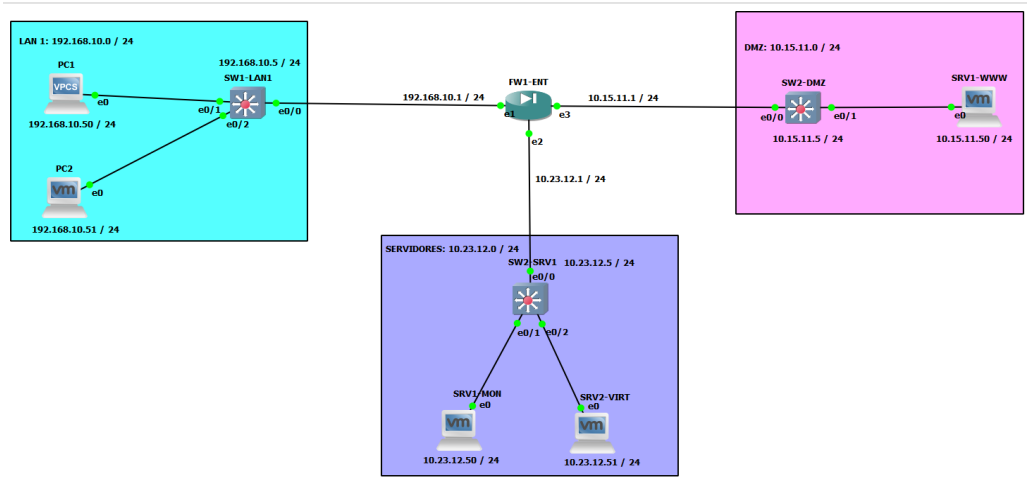

Figura 132 *Despliegue de equipos configurados 41g*

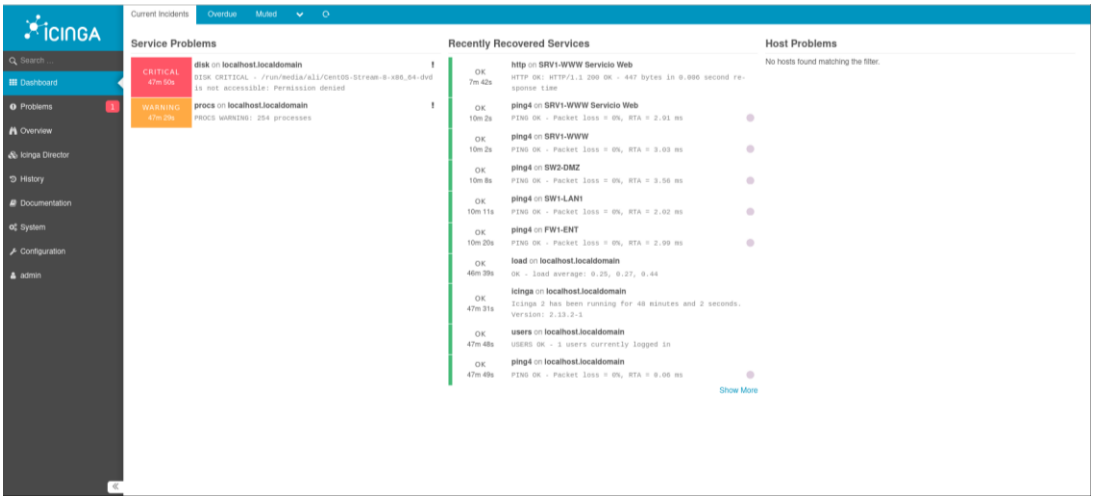

Figura 133 *Despliegue de equipos configurados 41h*

Simulación 5 Operación de la red – Caída general del FIREWALL

Lo que se hizo para simular la caída fue desconectar el FIREWALL como se muestra en la topología y se muestra el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados.

Como se muestra en el grafico a continuación se desconectó el firewall FW1-ENT para simular la caída del FIREWALL:

Simulación de caída del FIREWALL

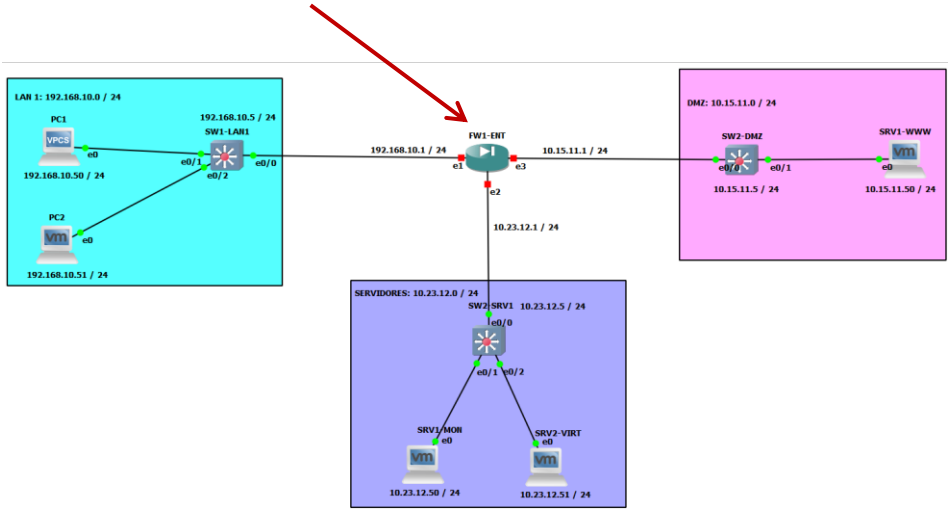

Figura 134 *Despliegue de equipos configurados 41ha*

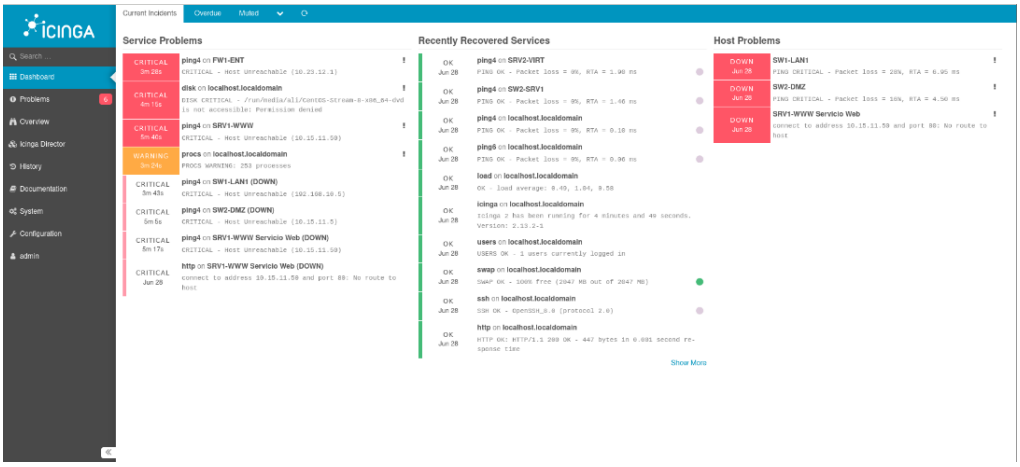

Figura 135 *Despliegue de equipos configurados 41hb*

Verificación del levantamiento del FIREWALL en el despliegue de historial de Problemas de Servicio y Servicios Recientemente Recuperados. Nuevamente se restable en el enlace entre el firewall FW1-ENT en condiciones normales y la topología queda de la siguiente manera:

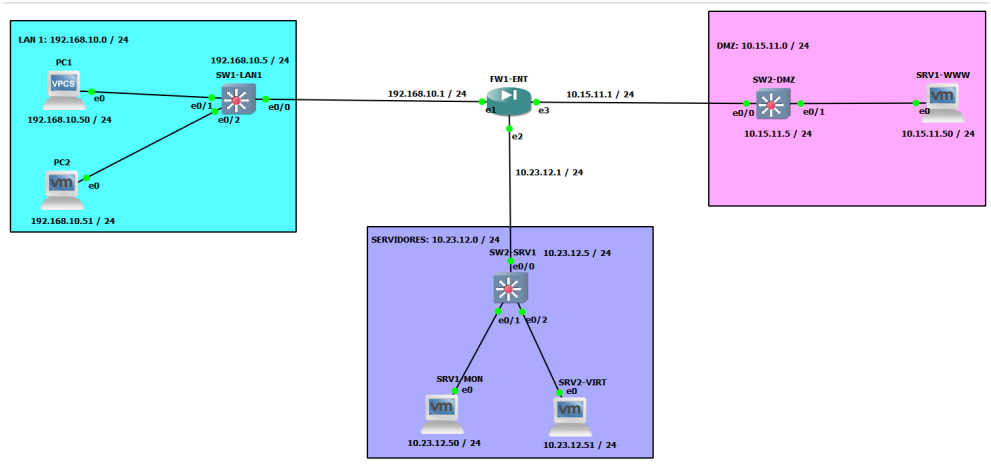

Figura 136 *Despliegue de equipos configurados 41hc*

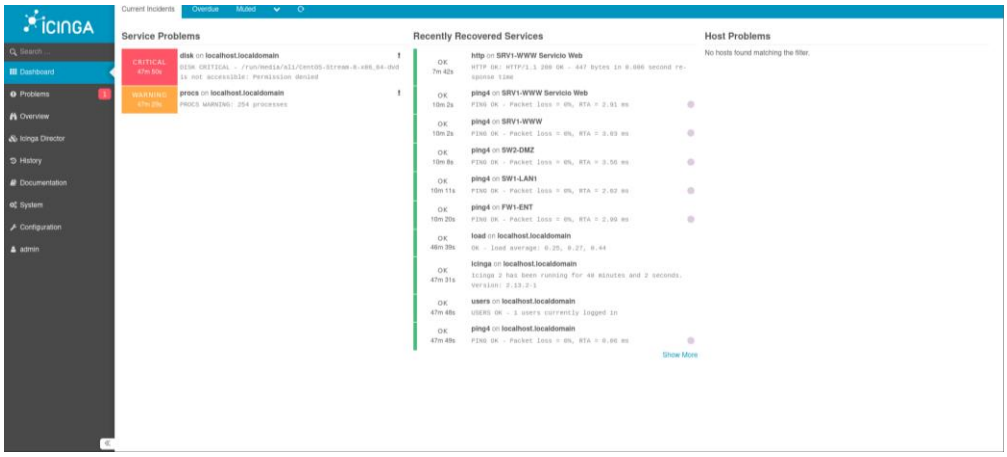

Figura 137 *Despliegue de equipos configurados 41hd*

Tabla de Resultados

De las simulaciones hechas en los puntos anteriores los resultados obtenidos son los siguientes:

Tabla 5 *Tabla de resultados*

		Protocolo de Monitoreo ICMP						Protocolo de monitoreo WWW		Resultado
Operación de la red	Zona	Switch	Estado	Servidor	Estado	Firewall	Estado	Servicio	Estado	
Condiciones Normales	LAN 1	**SW1-LAN1**	OK	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-LAN1 SÍ responde al monitoreo
	DMZ	**SW2-DMZ**	OK	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-DMZ SÍ responde al monitoreo
		N/A	N/A	**SRV1-WWW**	OK	N/A	N/A	**SRV1-WWW**	OK	El servidor SRV1-WWW SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
	Servidores	N/A	N/A	**SRV1-MON**	OK	N/A	N/A	**SRV1-MON**	OK	El servidor SRV1-MON SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
		N/A	N/A	**SRV2-VIRT**	OK	N/A	N/A	N/A	N/A	El servidor SRV1-VIRT SÍ responde al monitoreo
	Firewall	N/A	N/A	N/A	N/A	**FW1-ENT**	OK	N/A	N/A	El firewall FW1-ENT SÍ responde al monitoreo
Caida de red de la Zona LAN1	LAN 1	**SW1-LAN1**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-LAN1 NO responde al monitoreo
	DMZ	**SW2-DMZ**	OK	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-DMZ SÍ responde al monitoreo
		N/A	N/A	**SRV1-WWW**	OK	N/A	N/A	SRV1-WWW	OK	El servidor SRV1-WWW SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
	Servidores	N/A	N/A	**SRV1-MON**	OK	N/A	N/A	**SRV1-MON**	OK	El servidor SRV1-MON SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
		N/A	N/A	**SRV2-VIRT**	OK	N/A	N/A	N/A	N/A	El servidor SRV1-VIRT SÍ responde al monitoreo
	Firewall	N/A	N/A	N/A	N/A	**FW1-ENT**	OK	N/A	N/A	El firewall FW1-ENT SÍ responde al monitoreo
Caida de red de la Zona DMZ	LAN 1	**SW1-LAN1**	OK	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-LAN1 SÍ responde al monitoreo
	DMZ	**SW2-DMZ**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-DMZ NO responde al monitoreo
		N/A	N/A	SRV1-WWW	DOWN	N/A	N/A	**SRV1-WWW**	DOWN	El servidor SRV1-WWW NO responde al monitoreo y el servicio WWW NO responde al monitoreo
	Servidores	N/A	N/A	**SRV1-MON**	OK	N/A	N/A	**SRV1-MON**	OK	El servidor SRV1-MON SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
		N/A	N/A	**SRV2-VIRT**	OK	N/A	N/A	N/A	N/A	El servidor SRV1-VIRT SÍ responde al monitoreo
	Firewall	N/A	N/A	N/A	N/A	**FW1-ENT**	OK	N/A	N/A	El firewall FW1-ENT SÍ responde al monitoreo
Caida de red de la Zona Servidores	LAN 1	**SW1-LAN1**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-LAN1 NO responde al monitoreo
	DMZ	**SW2-DMZ**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-DMZ NO responde al monitoreo
		N/A	N/A	SRV1-WWW	DOWN	N/A	N/A	**SRV1-WWW**	DOWN	El servidor SRV1-WWW NO responde al monitoreo y el servicio WWW NO responde al monitoreo
	Servidores	N/A	N/A	**SRV1-MON**	OK	N/A	N/A	**SRV1-MON**	OK	El servidor SRV1-MON SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
		N/A	N/A	**SRV2-VIRT**	OK	N/A	N/A	N/A	N/A	El servidor SRV1-VIRT SÍ responde al monitoreo
	Firewall	N/A	N/A	N/A	N/A	**FW1-ENT**	DOWN	N/A	N/A	El firewall FW1-ENT NO responde al monitoreo
Caida de general del Firewall	LAN 1	**SW1-LAN1**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-LAN1 NO responde al monitoreo
	DMZ	**SW2-DMZ**	DOWN	N/A	N/A	N/A	N/A	N/A	N/A	El switch SW1-DMZ NO responde al monitoreo
		N/A	N/A	SRV1-WWW	DOWN	N/A	N/A	**SRV1-WWW**	DOWN	El servidor SRV1-WWW NO responde al monitoreo y el servicio WWW NO responde al monitoreo
	Servidores	N/A	N/A	**SRV1-MON**	OK	N/A	N/A	**SRV1-MON**	OK	El servidor SRV1-MON SÍ responde al monitoreo y el servicio WWW SÍ responde al monitoreo
		N/A	N/A	**SRV2-VIRT**	OK	N/A	N/A	N/A	N/A	El servidor SRV1-VIRT SÍ responde al monitoreo
	Firewall	N/A	N/A	N/A	N/A	**FW1-ENT**	DOWN	N/A	N/A	El firewall FW1-ENT NO responde al monitoreo

NOTA: La caida general del Firewall no significa que los equipos de la Zona LAN1 y DMZ esten caidos, lo que significa es que el servidor de monitoreo SRV1-MON perdió conectividad con dichas zonas, es por eso que Sí se siguen monitreando los equipos de la Zona de servidores ya que la conectividad en esta zona no está caida.

La caida general del SERVIDORES no significa que los equipos de la Zona LAN1 y DMZ esten caidos, lo que significa es que el servidor de monitoreo SRV1-MON perdió conectividad con dichas zonas, es por eso que Sí se siguen monitreando los equipos de la Zona de servidores ya que la conectividad en esta zona no está caida.

Conclusiones

La herramienta de análisis Icinga2 es un recurso que se utiliza para el monitoreo de redes, servidores, etc.; luego del análisis de la información sobre esta herramienta, se puede determinar que ayuda a la comprobación de las necesidades de seguridad en línea de las empresas, que utiliza los recursos, de comunicación por medio de una API (interfaz REST) por HTTP mediante un servidor web o estación de trabajo y con CPE vía SNMP. A través de HTTP se configuran, sirven, modifican todos los servicios redundantes dentro del servidor y encuestados a través de SNMP. Todos estos recursos son utilizados para el monitoreo de redes de las empresas.

El modelado de la red de topología para empresas tecnológicas comienza con la estructuración de la red, para esto, es necesario contar con Routers, Switches, Workstation, Firewall, mediante un servidor LINUX, después se instala el software GSN3 y se verifica el funcionamiento de los componentes, luego se instala el servicio Icinga Web 2, además de los módulos IDO, MySQL, PHP y se configura los componentes para que funcionen de igual forma, luego de esto finalmente, se agregan los directores (usuarios) del programa para comenzar a utilizar el monitoreo. Esta topología se basa en el esquema estrella para empresas.

A través de la infraestructura y a los puntos críticos registrados, es necesario verificar el mantener una plataforma de red orientada a brindar el rendimiento y la escalabilidad adecuada para poder contar con una infraestructura receptiva, es por ello que es conveniente eliminar conexiones innecesarias para disminuir tiempos elevados en la respuesta. Al respecto de las caídas generales que se produjeron en el modelado de las simulaciones se considera que pese a que el Firewall o el servidor hayan estado caídos en ciertas zonas, lo que ocasionó que hayan perdido conectividad, sin embargo, se mantuvieron monitoreando los equipos de las otras zonas.

El software GNS3 es recomendado para las empresas que deseen mejorar su sistema de redes, ya que a través de su interfaz, es posible la simulación, diseño e implementación de conjunto de redes y determinar las fallas que puede acarrear en el proceso de montaje o errores de instalación, además luego de la investigación realizada, otro de los beneficios es la gestión de tiempos de latencia, de equipos, inclusive la gestión de conmutación para así de forma gráfica observar a través de curvas los rendimientos totales o parciales de la red.

Recomendaciones

La implementación de la topología Icinga2 en las empresas, es un aliciente para que toda corporación aumente su seguridad en redes, desde el punto de vista de los recursos que utilizan, este programa optimiza los recursos utilizados, para determinar las fallas o agujeros de seguridad que se encuentran en las empresas.

De forma general de acuerdo con los resultados obtenidos y las herramientas Open Source se recomienda a las empresas el uso de las mismas para obtener un alto nivel de monitoreo a bajo costo, sin embargo, el principal beneficio del análisis de esta plataforma radica en evitar que los clientes, los cuales, aun teniendo interferencias en sus enlaces, en situaciones concretas puedan estar con los servicios caídos debido a no estar trabajando con procesos redundantes.

Es importante considerar que para el proceso de la implementación de un proyecto direccionado a la simulación en GNS3 se debe tomar en consideración la capacidad que tiene la RAM de la PC, los recursos de seguridad que necesita la empresa o cliente, la capacidad de la empresa donde se va a estructurar el software y que tipo de firewall necesita, así optimizando recursos.

Se recomienda que toda empresa, estructure su plataforma de monitoreo para asegurar la integridad de sus sistemas, pues la simulación GNS3, brinda apoyo al departamento tecnológico para evitar gastos innecesarios en el futuro y evaluar la seguridad de la estructura de red utilizada. Es preciso realizar un estudio de la infraestructura de red a través de la realización de mantenimientos programados, los cuales permitirán la determinación y diagnóstico de posibles inconvenientes futuros.

Bibliografía

Alcívar, P. (2019). Análisis comparativo entre red de computadoras tradicional y red definida por software: caso de estudio ESPAM MFL. *Repositorio Digital ESPAMMFL*. https://repositorio.espam.edu.ec/handle/42000/1031

Asencios Silva, K. L. (2019). *Implementacion de buenas practicas para la gestion de servicios de TI basado en ITIL V3 para la Unidad de Tecnologia de la Informacion de la zona registral N°VII-sede Huaraz,2016.* Huaraz, Ancash, Perú: Universidad Nacional Santiago Antúnez De Mayolo.

Baca Dueñas, Y., & Vela De la Cruz, G. (2015). *DISEÑO E IMPLEMENTACIÓN DE PROCESOS BASADOS EN ITIL V3 PARA LA GESTIÓN DE SERVICIOS DE TI DEL ÁREA DE SERVICE DESK DE LA FACULTAD DE INGENIERÍA Y ARQUITECTURA – USMP.* Lima,Perú: Universidad San Martin de Porres.

Bayas, J. I. (2015). Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en CELEC. *Universidad Técnica de Ambato,* 1-184. https://repositorio.uta.edu.ec/bitstream/123456789/13063/1/Tesis_t1035ec.pdf

Berrocal, J. (20 de Abril de 2018). *Microinformática*. Prácticas del curso de microinformática: https://josemberrocal.wordpress.com/2018/04/20/servidores-dhcp-y-dns/

Bon, J. V., De Jong, A., & Kolthof, A. (2008). *Estrategia del servicio basado en ITIL*. Holanda: Van Haren publishing.

Bravo, L., & Andrade, M. (2020). ITIL V4 en la gestión de solicitudes e incidentes de la mesa de ayuda de la Universidad Nacional de Loja. *Dominio de las Ciencias*, *6*(4), 1510-1534.

https://docs.google.com/viewerng/viewer?url=https://www.dominiodelasciencias.com/ojs/index.php/es/article/viewFile/1564/2947

Cali, F. (2018). Implementación del algoritmo de protocolo de direccionamiento para redes de sensores inalámbricos con el estándar IEEE 802.15.4. *Repositorio Digital de la EPN*. https://bibdigital.epn.edu.ec/handle/15000/19061

Carate, B., & Pozo, D. (2019). Diseño de un sistema de detección de intrusos (NIDS) para una red simulada PYMES en GNS3, implementada en un módulo Raspberry Pi portátil. *Repositorio Digital Universidad Politécnica Salesiana*. https://dspace.ups.edu.ec/handle/123456789/17546

Casanova, M., & Saavedra, A. (2018). Implementación de la mesa de servicio aplicando ITIL 4 para mejorar la calidad del servicio en la oficina de sistemas de información de la universidad privada de la selva peruana. *Universidad Privada de la Selva Peruana*, 1-165. http://repositorio.ups.edu.pe/bitstream/handle/UPS/42/Tesis%20ITIL.pdf

CCNA. (12 de Octubre de 2020). *CCNA Desde 0*. CCNA Desde 0: https://ccnadesdecero.es/eleccion-de-tecnologia-wan/

Cerezuela, E., Durán, L., Gutiérrez, D., Domínguez, J., Ríos, A., & Jiménez, Á. (2021). Práctica de desarrollo de una red de sensores basada en la programación de microprocesadores para sistemas en tiempo real. *Jenui, 6*, 303-306. http://jenui2021.hola-mundo.info/EC0055.pdf

Cestari, F., Pfeifer, L., César, A., & Dimmit, J. (2015). Gerencia de servicios TI. *Escuela superior de redes RED CEDIA*, 1-338. https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI3.pdf

Chaparro, S., González, S., Miranda, N., & Páez, R. (2021). Seguridad en la capa de enlace del modelo OSI. *Pontificia Universidad Javeriana de Colombia*. https://exploitland.com/wp-content/uploads/2021/07/seguridad-capa-de-enlace.pdf

Computerweekly. (2019). *https://www.computerweekly.com/es/definicion/Topologia-de-red*. https://www.computerweekly.com/es/definicion/Topologia-de-red: https://www.computerweekly.com/es/definicion/Topologia-de-red

Cumbal, R., Buestán, J., & Domínguez, J. (2021). Implementación de una red IoT con GPRS para monitorear los parámetros en un vehículo en tiempo real. *Revista de Investigación en Tecnologías de la Información RITI, 9*(17), 66-76. https://doi.org/10.36825/RITI.09.17.007

Desconocido. (2020). *Instituto Vasco de estadistica*. https://www.eustat.eus/documentos/opt_0/tema_133/elem_3468/definicion.html

Días Sobrinho, J. (2007). Acreditación de la educación superior en America latina y el Caribe. *Universitat Politécnica de Catalunya*, 287.

Díaz Saravia, M. W. (2017). Simulación de redes de computadoras con GNS3 e integración de máquinas virtuales. *Revista de la Escuela Especializada en Ingeniería ITCA-FEPAD, 1*(1), 15-23. http://www.redicces.org.sv/jspui/bitstream/10972/1734/1/PARTE%203.pdf

Enreda. (8 de Septiembre de 2011). *Blog Enreda*. https://blog.enreda.coop/icinga-herramienta-para-monitorizar-sistemas-basada-en-nagios/#:~:text=Icinga%20es%20un%20sistema%20de,del%20estado%20de%20los%20recursos

García , A. (2007). *HERRAMIENTAS TECNOLÓGICAS PARA MEJORAR LA DOCENCIA.* España: Universidad de Salamanca.

García , F. (2010). Docencia. *Universidad de Salamanca*, 29.

Geoffrey, A., Espinoza, A., & Jedidiah, C. (2019). Detecting TCP/IP Connections via IPID Hash Collisions. *Sciendo*, 311–328. https://sciendo.com/downloadpdf/journals/popets/2019/4/article-p311.pdf

González, J., & López, F. (2019). Evaluación de Convergencia del Protocolo OSPF en Redes Definidas por Software. *Facultad de Politécnica. Universidad Nacional de Asunción*. http://sedici.unlp.edu.ar/bitstream/handle/10915/91137/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Inaquiza, E. (2019). Diseño e implementación de la red WAN para la empresa Fairis C.A. Sobre la red MPLS de Puntonet. *Universidad Politécnica Salesiana*. https://dspace.ups.edu.ec/bitstream/123456789/16898/1/UPS-ST003908.pdf

International Business Machines Corporation. (12 de 04 de 2021). *IMB.* Subsitema del protocolo PPP: https://www.ibm.com/docs/es/aix/7.2?topic=communications-asynchronous-point-point-protocol-subsystem

Junco, G., & Rabelo, S. (2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica*, *10*(1), 76-83. http://scielo.sld.cu/pdf/rcim/v10n1/rcim09118.pdf

La Red, D., & Peláez, J. (2020). Los niveles de Servicio en la Ingenieria de Software. *Universidad Nacional del Nordeste*, 3.

López, J. (2020). Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el software GNS3. *Repositorio Digital Escuela Politécnica Nacional*. https://bibdigital.epn.edu.ec/handle/15000/21163

Luke, J. (2019). Guía sobre direccionamiento IP, subredes y enrutamiento. *Creative Commons*. https://193.145.118.245/xmlui/bitstream/handle/915/14702/Guia_sobre_direccionamiento_IP__subredes_y_enrutamiento.pdf?sequence=1&isAllowed=y

Mendoza, D. (2021). Diseño e implementación de una red LAN para Tecnoimport. *UNESUM-Ciencias: Revista Científica Multidisciplinaria*, 185-196. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/592/382

Molina , L., Auquilla, A., & Espín, H. (2019). Análisis de los Mecanismos de Defensa Contra el Ciberataque SMTP Spoofing en la Infraestructura de Red IPV4 de la Universidad Nacional de Chimborazo. *Repositorio Digital Universidad Nacional de Chimborazo*. http://dspace.unach.edu.ec/handle/51000/5576

Montúfar, J. (2021). Proyecto de implementación de servidor para la conversión de alertas recibidas mediante el protocolo SMTP a llamada por VOIP, llamada telefónica, envío de SMS y/o envío de correo. *Universidad de San Carlos de Guatemala*, 8. http://www.repositorio.usac.edu.gt/16249/1/Juan%20Fernando%20Mont%C3%BAfar%20Juarez.pdf

Navarro , V. (2009). *Calidad en el servicio para le personal docente de la UTCN*. El cid editor.

Opensource. (2020). *https://opensource.com/article/19/2/network-monitoring-tools*. https://opensource.com/article/19/2/network-monitoring-tools: https://opensource.com/article/19/2/network-monitoring-tools

Parrilla, J. (2020). La capa de red, direccionamiento, máscaras de longitud variable, mecanismos de transición de IPV6, ICMP E IGMP. *Centro de estudios de posgrado de la Universidad de Jaén*. https://tauja.ujaen.es/bitstream/10953.1/13543/1/PARRILLA_MARTNEZ_JOSANTONIO_TFM_INFORMTICA.pdf

Pérez, M. (2018). Aplicación de la metodología ITIL para impulsar la gestión de TI en empresas del norte de Santander (Colombia): revisión del estado del arte. *Revista Espacio, 39*(09), 117. https://www.revistaespacios.com/a18v39n09/a18v39n09p17.pdf

Pérez, T. (2021). Estudio de las metodologías ITIL y Lean Six Sigma para ubicación y uso de las tecnologías 2G, 3G y 4G en la actualidad en Colombia. *Universidad Snto Tomás*. https://repository.usta.edu.co/jspui/bitstream/11634/33628/1/2021sofiaperez.pdf

Pina, A. B. (2008). ENTORNOS DE APRENDIZAJE MIXTO EN EDUCACIÓN SUPERIOR. *Universitat de Barcelona*, 1.

Rivera, J. (2019). Un sistema multi-agente para la autoconfiguración de las operaciones de red en la subcapa MAC del modelo OSI. *Universidad Nacional de Colombia*. https://repositorio.unal.edu.co/bitstream/handle/unal/63721/tesis%20MSc-Juan%20Carlos%20Rivera.pdf?sequence=1&isAllowed=y

Rodríguez, R., & Pinto, M. (2014). *Servicio de referencia virtual.* Asturias: Trea.

Romero, J. (2019). Análisis de la infraestructura tecnológica de la empresa Mapfre Atlas compañia de seguros SA. diseño de rede para mejorar la calidad de servicios actuales. *Universidad de Guayaquil*. http://repositorio.ug.edu.ec/bitstream/redug/39341/1/B-CINT-PTG-N.393%20Romero%20Caicedo%20Johnny%20%20%C3%81ngel.pdf

Saavedra, C. (2017). CONTROL DE SERVICIOS DE RED Y SERVIDORES BASADO EN HERRAMIENTAS DE ADMINISTRACIÓN DE RED Y POLÍTICAS DE GESTIÓN DE CALIDAD. *PUCE Esmeraldas*. https://181.39.85.171/bitstream/123456789/1463/1/SAAVEDRA%20DROUET%20CESAR.pdf

Salamanca, J. (2019). Guia de implementación para la gestión de servicios incorporando principios ágiles en el marco de trabajo ITIL. *Universidad ICESI*, 1-109. https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/87070/1/T02148.pdf

Sánchez, D. (2015). Evaluación del rendimiento de aplicaciones en línea a través de redes Wan sobre OPNET. *Universidad Católica de Santiago de Guayaquil*, 1-62. http://repositorio.ucsg.edu.ec/bitstream/3317/3932/1/T-UCSG-PRE-TEC-ITEL-104.pdf

Sánchez, J., Chávez , J., & Mendoza, J. (Enero de 2018). La calidad en la eduación superior: Una mirada al proceso de evaluación y acreditación de universidades del Ecuador. *Revista caribeña de ciencias sociales*, 5.

Sánchez, S. (2021). Diseño de la interfaz PCI para la tarjeta HDLC-4M. *Instituto Tecnológico de Costa Rica*, 1-218. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/6320/dise%c3%b1o-interfaz-tarjeta.pdf?sequence=1&isAllowed=y

Telectrónika. (2018). *GNS3 Guía Introductoria: Características y Requerimientos Mínimos*. https://www.telectronika.com/articulos/ti/que-es-gns3/

Van Bon, J., Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T. (2010). *Fundamentos de ITIL V3.* Holanda: Van Haren Publishing.

Vera, C. (2014). *https://prezi.com/q6tpwsk5nrcw/simulador-de-redes-gns3/*. https://prezi.com/q6tpwsk5nrcw/simulador-de-redes-gns3/: https://prezi.com/q6tpwsk5nrcw/simulador-de-redes-gns3/

Ziggaf, Z. (2018). Diseño y despliegue de un sistema de monitorización de red para gestión de fallos y rendimiento. *Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación*. https://oa.upm.es/53093/1/TFG_ZAKARIAE_ZIGGAF_KANJAA.PDF

Características de la arquitectura de GNS3. (s. f.). Library. Recuperado 8 de julio de 2022, de https://1library.co/article/caracter%C3%ADsticas-de-la-arquitectura-de-gns.zwvwp41q