Universidad Nacional de Ingeniería

Facultad de Ingeniería Eléctrica y Electrónica

TRABAJO DE SUFICIENCIA PROFESIONAL

Implementación de un software de monitoreo de nodos de seguridad perimetral aplicando OPEN SOURCE para el Centro de Operaciones de Seguridad – SOC de una empresa de telecomunicaciones

Para obtener el Título Profesional de Ingeniero de Telecomunicaciones.

Elaborado por

Hans Nilson Solier Riveros

0009-0003-9139-5107

Asesor

MSc. Ing. Julio Teodosio Díaz Aliaga

0009-0005-5552-5319

LIMA – PERÚ

2025

Citar/How to cite	Solier Riveros [1]
Referencia/Reference Estilo/Style: IEEE (2020)	[1] H. Solier Riveros, “Implementación de un software de monitoreo de nodos de seguridad perimetral aplicando OPEN SOURCE para el Centro de Operaciones de Seguridad – SOC de una empresa de telecomunicaciones” [Trabajo de suficiencia profesional]. Lima (Perú): Universidad Nacional de Ingeniería, 2025.

Citar/How to cite	(Solier, 2025)
Referencia/Reference Estilo/Style: APA (7ma ed.)	Solier, H. (2025). *Implementación de un software de monitoreo de nodos de seguridad perimetral aplicando OPEN SOURCE para el Centro de Operaciones de Seguridad – SOC de una empresa de telecomunicaciones*. [Trabajo de suficiencia profesional, Universidad Nacional de Ingeniería]. Repositorio institucional Cybertesis UNI.

Dedicatoria

El presente trabajo se lo dedico a mis padres Agustín Solier Guevara y Haydeé Rosario Riveros Farfán, pilares fundamentales en mi vida, quienes con su amor incondicional, esfuerzo y ejemplo forjaron en mí el valor del trabajo honesto, la perseverancia y la humildad. Gracias por creer en mí incluso en los momentos más difíciles, por apoyarme sin reservas y por ser mi mayor fuente de inspiración, gracias a su guía constante he podido avanzar con firmeza en mi formación personal y profesional.

A mis abuelos, Emilio y Matilde, por ser mi raíz y mi historia. Gracias por su sabiduría, por sus consejos llenos de ternura y por el cariño silencioso que siempre me ha sostenido.

Y a mi amada hija, Madison Yoko Roxana, por ser una fuente constante de motivación y alegría asimismo recordarme cada día la importancia de avanzar con responsabilidad y compromiso. Este logro representa también el deseo de ofrecerle un futuro feliz y mejor.

Agradecimientos

Agradezco a Dios, por ser mi guía constante y darme fortaleza en los momentos difíciles.

A mis hermanos Jackelinne, Geanfranco, Kevin y Heidi, por su compañía, complicidad, apoyo incondicional y por ser una parte esencial en mi vida y en este logro.

A mi novia Karla Bonifacio, por caminar conmigo con paciencia y ternura. Gracias por tu amor incondicional, por escucharme, por animarme en los días difíciles y por hacerme sentir que no estaba solo. Tu compañía ha sido mi fuerza silenciosa.

A mi amigo y colega Luis Cárdenas Rojas, por su disposición y apoyo desinteresado. Gracias por brindarme tu ayuda en los momentos clave, por aclarar mis dudas con tus conocimientos técnicos.

Agradezco al MSc. Ing. Julio Teodosio Díaz Aliaga, por su confianza, orientación y exigencia durante este proceso. Asimismo, a la Universidad Nacional de Ingeniería, por su formación académica de calidad y por inculcarme valores de responsabilidad, excelencia y compromiso profesional.

Resumen

La demanda creciente y sostenida de servicios de gestión y seguridad de red a clientes corporativos, comprometiendo a las Empresas de Telecomunicaciones a brindar un servicio confiable y seguro de monitoreo y operatividad de los nodos de seguridad perimetral – firewall las 24 horas del día durante los 7 días de la semana, también conocido como 24/7. En la presentación del presente Informe de Suficiencia Profesional se exponen los detalles, relacionados a la instalación y operación de un Sistema de Software OPEN SOURCE que monitoree los nodos de seguridad perimetral, en el Centro de Operaciones de Seguridad (SOC por su acrónimo en inglés), de una Empresa de Telecomunicaciones.

Inicialmente se procedió a identificar los requerimientos del Centro de Operaciones de Seguridad (SOC) de la Empresa de Telecomunicaciones, considerando principalmente la escalabilidad respecto al número de sensores y nodos a monitorear, en conformidad con el protocolo SNMP a un mínimo costo de implementación, procediéndose a evaluar y comparar los softwares existentes en el mercado y finalmente elegir un software basado en OPEN SOURCE. Continuando con la implementación, configuración del software de monitoreo y, proseguir con pruebas de conectividad, transmisión de paquetes SNMP y envío de alertas.

Al concluirse la implementación del Sistema de Software de monitoreo se aseguró la supervisión y monitoreo de los nodos de seguridad perimetral gestionados por el SOC de la Empresa de Telecomunicaciones, la reducción significativa del tiempo de respuesta frente a una falla en las interfaces en los servicios que brinda. Una ventaja comparativa del software de monitoreo es su capacidad de enviar notificaciones de eventos, proporcionando a los ingenieros de soporte del SOC ejecutar las acciones correctivas.

Palabras clave —Software de Monitoreo, Seguridad perimetral, Open Source, SOC, SNMP.

Abstract

The Security Operations Center (SOC) of telecommunications companies that provide network management as well as security services to corporate customers must to bear in mind assure an uninterruptible and steady network services of perimeter security nodes—managed firewalls—24/7. Therefore, monitoring these nodes is of utmost importance. This study aims to implement an open-source software solution for monitoring perimeter security nodes within the SOC of a Telecommunications Information Enterprise.

The needs of the Security Operations Center (SOC) of the Telecommunications Enterprise were identified, focusing on key requirements such as scalability for the number of sensors and nodes to monitor, use of the SNMP protocol, and minimal implementation costs. Various software solutions were evaluated and compared, leading to the selection of an open-source-based software. Subsequently, the implementation and configuration of the monitoring software were carried out, along with connectivity tests, SNMP packet transmission, and alert notifications.

As a result, the implementation of the monitoring software ensures the supervision and monitoring of perimeter security nodes managed by the SOC of the telecommunications company, reducing response times to interface failures and the services provided by each interface. By sending event notifications, the monitoring software enables SOC engineers to take timely corrective actions.

Keywords — Monitoring Software, Perimeter Security, Open Source, SOC, SNMP.

Tabla de Contenidde o

Pág.

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Introducción

En el portafolio de soluciones que una Empresa de Telecomunicaciones ofrece a sus clientes figura el servicio de gestión de la seguridad perimetral para sus infraestructuras de red corporativas, con tal propósito cuenta con un Centro de Operaciones de Seguridad - SOC siendo uno de sus objetivos, mitigar y minimizar significativamente los tiempos fuera de servicio (TIMEOUT) provocados por fallas en los nodos de seguridad perimetral, eventos que últimamente experimenta un crecimiento exponencial dado el incremento de los nodos de seguridad perimetral a ser gestionados. Esta circunstancia ha obligado a las Empresas de Telecomunicaciones a presentar soluciones tecnológicas que ofrecen servicios de monitoreo de seguridad perimetral como de equipos de red implementando sistemas de software propietario o de tipo OPEN SOURCE, los cuales permiten recopilar información que supervisa, controla y asegura la continuidad de la operación de sus equipos.

Los Sistemas de Software de monitoreo mediante el envío de alertas y notificaciones al SOC de la Empresa de Telecomunicaciones permite a los ingenieros del SOC tomar decisiones que minimicen los tiempos fuera de servicio (TIMEOUT) de los nodos de seguridad perimetral, proporcionando de esta forma, servicios de gestión de seguridad perimetral de calidad a sus clientes corporativos. Adicionalmente el aumento de la cantidad de nodos de seguridad perimetral a ser gestionados, ha promovido la búsqueda e implementación de Sistemas de Software de monitoreo escalables.

La información contenida en el presente Informe de Suficiencia Profesional ha sido estructurada en cuatro capítulos:

El capítulo I: Introducción del Proyecto, se presentan generalidades y se describen el problema de investigación, objetivos del estudio y antecedentes.

El capítulo II: Marco teórico y conceptual, se presenta la filosofía y teoría que proporcionan un soporte conceptual al presente Informe de Suficiencia Profesional.

El capítulo III: Desarrollo del trabajo de investigación, en el cual se describe la selección e instalación del Sistema de Software de monitoreo hasta la ejecución de las pruebas de monitoreo correspondientes a los nodos de seguridad perimetral.

El capítulo IV: Análisis y discusión de resultados, en base a los objetivos propuestos y los resultados obtenidos.

Finalmente, se incluyen las conclusiones y recomendaciones que se obtuvieron al implementar el software de monitoreo y las referencias bibliográficas que sirvieron de base para el desarrollo del presente Informe de Suficiencia Profesional y sus anexos.

Capítulo I. Parte Introductoria del Trabajo

1.1 Generalidades

La gran mayoría de las Empresas han adquirido una conciencia aguda acerca que las redes de datos y la seguridad informática son componentes importantes en su quehacer diario, las cuales les brindan comunicaciones optimas y que la seguridad de la información que se transmite contribuye significativamente a la continuidad de negocio, y que minimizar los tiempos fuera de servicio de la red de datos es vital para una empresa.

La instalación de un Software de monitoreo en una red de datos proporciona la visibilidad de los componentes que constituyen la red de datos, tal como, en el caso de los nodos de seguridad perimetral o también denominado equipo firewall que presta funciones de red y brinda seguridad a la red, por lo tanto, monitorear estos componentes en cualquier momento es crítico para responder oportunamente a una falla.

1.2 Descripción del Problema de Investigación

1.2.1 Situación Problemática

El Centro de Operaciones de Seguridad - SOC de la Empresa de Telecomunicaciones, es incapaz de monitorear los nodos de seguridad perimetral de los nuevos clientes corporativos, gestionados a partir de inicios del año 2024. Lo que significa, que el SOC no supervisa ni controla en tiempo real los nodos de seguridad, es decir no dispone de la visibilidad de las interfaces de los nodos de seguridad perimetral.

La razón por la cual, los nodos de seguridad perimetral de los nuevos clientes no son monitoreados, se debe a que el software instalado tiene un límite máximo de monitoreo a 2500 nodos de seguridad perimetral, es decir, no es escalable, está limitado a un máximo de 2500 sensores, los cuales monitorean las interfaces y los servicios de los dispositivos monitoreados. Adicionalmente, otro factor limitante lo constituye, que este, no debe superar

el presupuesto del SOC de la Empresa de Telecomunicaciones destinado a la implementación de Sistema de Software de monitoreo.

Los nuevos nodos de seguridad perimetral gestionados por el SOC al no ser monitoreados, presentan el inconveniente muy serio en este caso, que ante una desconexión o que el nodo quede fuera de servicio, los tiempos de recuperación sean altos, interrumpiéndose de este modo la continuidad en las operaciones de los clientes corporativos, traduciéndose en pérdidas económicas tanto para el SOC de la Empresa de Telecomunicaciones como para el cliente corporativo.

1.2.2 Problema a Resolver

El problema radica en el factor limitante del número de nodos de seguridad perimetral que pueden ser supervisados por el Sistema de Software de monitoreo instalado en el Centro de Operaciones de Seguridad (SOC) de la Empresa de Telecomunicaciones. Esto genera riesgos de seguridad, como el surgimiento de zonas ciegas en la red, retrasos en la detección y en las respuestas ante incidentes de este tipo.

¿De qué forma se implementa un software de monitoreo de nodos de seguridad perimetral aplicando OPEN SOURCE para el Centro de Operaciones de Seguridad – SOC de una Empresa de Telecomunicaciones?

1.3 Objetivos del Estudio

1.3.1 Objetivo General

Implementar un software de monitoreo de nodos de seguridad perimetral instalando un Sistema de Software con licencia de tipo OPEN SOURCE en el Centro de Operaciones de Seguridad – SOC de una Empresa de Telecomunicaciones.

1.3.2 Objetivos Específicos

Los objetivos específicos que permiten cumplir el objetivo general son los siguientes:

- Evaluar las características de los diferentes Sistemas de Softwares de monitoreo de dispositivos de red basados en los protocolos ICMP y SNMP.
- Implementar el Sistema de Software de monitoreo con licencia de tipo OPEN SOURCE que detecte fallas en los nodos de seguridad perimetral en conformidad con los protocolos ICMP y SNMP.
- Configurar los nodos de seguridad perimetral.
- Evaluar la funcionalidad del Sistema de Software de monitoreo previamente a su puesta en operación.

1.3.3 Indicadores de Logro de Objetivos

Tabla 1

Indicadores de logro de objetivos.

Objetivos Específicos	Indicador de logro	Métrica
Evaluar las características del software de monitoreo en dispositivos de red en base a los protocolos ICMP y SNMP.	Los diferentes Sistemas de Software de monitoreo son evaluados en conformidad con los requerimientos del Centro de Operaciones de Seguridad (SOC).	Características del Sistema de Software de monitoreo.
Implementar el Sistema de Software de monitoreo con licencia OPEN SOURCE destinado a detectar fallas en los nodos de seguridad perimetral conforme a los protocolos ICMP y SNMP.	Implementación del software de monitoreo y configuración del protocolo SNMP.	Software de monitoreo OpenNMS implementado y configurado con el protocolo SNMP.
Configurar los nodos de seguridad perimetral.	Nodos de seguridad perimetral son configurados.	Porcentaje de nodos de seguridad perimetral configurados.
Evaluar la funcionalidad del Sistema de Software de monitoreo antes de su puesta en operación.	Los nodos de seguridad perimetral son monitoreados.	Porcentaje de nodos alertados.

Nota. Elaboración propia.

1.4 Antecedentes Investigativos

Respecto al tema propuesto en el presente Informe de Suficiencia Profesional, a nivel internacional y nacional, se han efectuado diversos estudios sobre la utilización de software de monitoreo con licencia OPEN SOURCE dedicado al monitoreo de, servidores, dispositivos de red como switch y router, a continuación, se detallan las investigaciones más relacionadas con el tema propuesto.

Sánchez (2022) realizó una investigación titulada "Diseño de Implementación de una Herramienta Open Source para Monitoreo de Servidores" la cual tuvo como objetivo la implementación de una herramienta de monitoreo en servidores, utilizando la plataforma Elastic2 de código abierto (open source), la cual recolectaba métricas de la infraestructura y logs, mediante un portal web era presentada esta información. La contribución de esta investigación describe el detalle de como una herramienta de monitoreo open source puede monitorear entornos de servidores con sistemas operativos como Linux y Windows, obteniendo resultados satisfactorios.

Martínez (2021) realizó una investigación titulada “Implementación de un Centro de Operaciones De Seguridad (SOC) de Código Abierto con Elementos de Red para el Control de Tráfico” cuyo objetivo fue el de implementar un centro de operaciones de seguridad con herramientas de código abierto, la implementacion de este SOC incorporo elementos de red necesarios que controlan el tráfico hasta la interfaz de usuario en donde se visualizan las alertas, estos elementos fueron integrados por correladores, herramientas de parseo de logs, dashboards, gestión de alertas. Este trabajo proporciona información y herramientas dedicadas a mejorar la seguridad de una organización que no dispone de elementos de seguridad y monitorización, debido a los altos costos de implementación.

Quispe (2019) en su investigación titulada “Implementación de un Prototipo de Monitoreo de Dispositivos de Comunicación y Usuarios Finales Utilizando el Protocolo SNMP Basada en Software Libre Para una Empresa E-Commerce” cuyo objetivo fue el desarrollo e implementacion de un prototipo que monitoree en tiempo real los dispositivos de comunicación (router, switches, acces point) y los usuarios finales (laptop,

computadoras personales, impresoras, fotocopiadoras), conforme el protocolo Simple Network Management Protocol-SNMP y software libre para una Empresa de comercio electronico (e-commerce). La solución se implementó en el sistema operativo GNU/LINUX la cual, redujo significativamente el costo del proyecto, el aprendizaje de un nuevo sistema operativo y personalizar el monitoreo con el objetivo de elevar el rendimiento de la empresa.

Oré (2019) en su investigación intitulada “Implementación de un Sistema de Monitoreo para Asegurar la Continuidad de los Servicios en un Data Center Utilizando Protocolo SNMP” con el objetivo de implementar un sistema de monitoreo que observe el comportamiento de la infraestructura de red de la empresa Netsecure Perú y asegurar la continuidad de los servicios del data center conforme al protocolo SNMP. El software de monitoreo implementado fue el PRTG NETWORK MONITOR resultando ser la herramienta indicada para la empresa Netsecure Perú, con su diseño práctico, configurable y escalable en conformidad con las necesidades de la red y los servicios brindados por Netsecure Perú.

Capítulo II. Marco teórico y conceptual

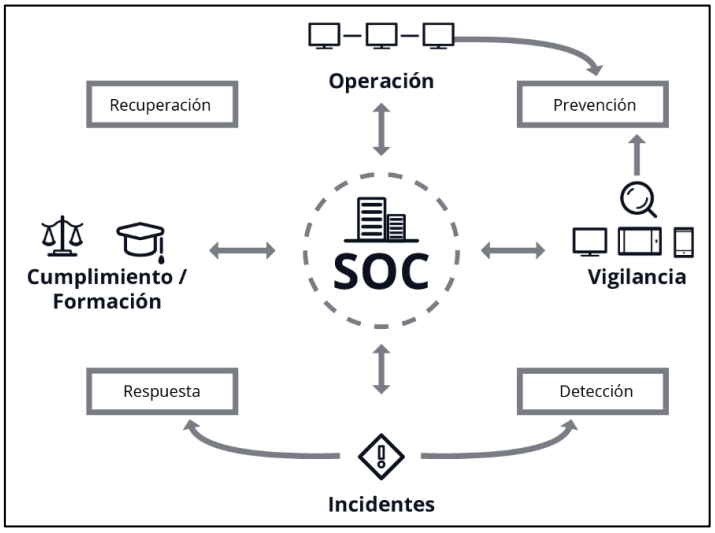
2.1 Marco teórico

2.1.1 Centro de Operaciones de Seguridad - SOC

Un Centro de Operaciones de Seguridad (SOC) es una unidad operativa diseñada para proteger la infraestructura tecnológica de una organización frente a ciber amenazas. Los equipos de un SOC supervisan redes, detectan incidentes de seguridad y responden a ellos en tiempo real. Mediante el uso de herramientas avanzadas de monitoreo y análisis, el SOC actúa como el centro neurálgico de las operaciones de ciberseguridad. Su objetivo es garantizar la integridad, confidencialidad y disponibilidad de los activos digitales de la organización (SANS Institute, 2024).

Figura 1

Diagrama de operación del SOC.



Nota: https://www.ccn.cni.es/eu/allcategories-eu-es/8-kategoria-eu-es/827-soc-eu.

2.1.2 VRF

El concepto de Virtual Routing and Forwarding (VRF) de gestión posibilita crear múltiples instancias de enrutamiento independientes dentro de un solo dispositivo de red. Esta funcionalidad es especialmente útil en entornos donde es necesario segmentar y separar el tráfico de diferentes clientes o servicios en una infraestructura compartida. Cada

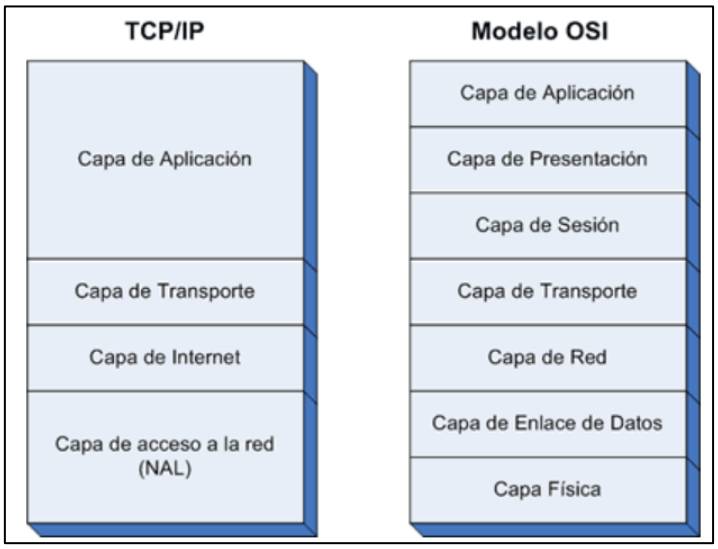
VRF tiene el comportamiento de una tabla de enrutamiento independiente, por lo que los paquetes asociados a diferentes VRF no se mezclan. Esto proporciona seguridad, optimización de recursos y simplificación de la gestión en redes complejas. Es una herramienta clave en implementaciones empresariales y en proveedores de servicios (Cisco, 2024d).

2.1.3 TCP/IP

El modelo TCP/IP es el fundamento de la comunicación en redes modernas, diseñado para garantizar la interoperabilidad entre dispositivos heterogéneos. Este modelo se compone de cuatro capas: aplicación, transporte, internet y acceso a red. Cada una con funciones específicas que incluyen la segmentación de datos, su enrutamiento a través de redes y su presentación a aplicaciones. TCP, como protocolo de transporte, asegura la entrega confiable de datos, mientras que IP proporciona direcciones únicas para cada dispositivo en la red. Su diseño modular y escalable ha permitido que TCP/IP sea el estándar predominante en redes privadas y públicas, incluyendo Internet. (Internet Society, 2023).

Figura 2

Modelo TCP/IP



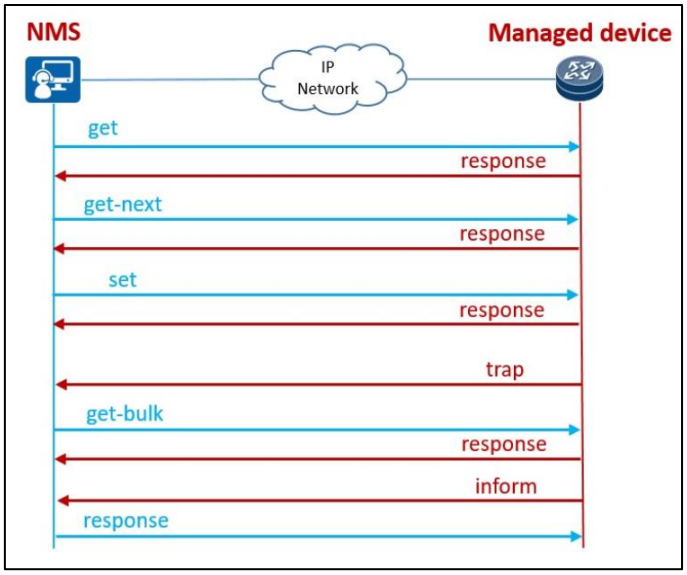
Nota: https://www.javiergarzas.com/2013/09/tcpip-se-impuso-a-osi-2.html

2.1.4 Protocolo SNMP

El Protocolo Simple de Gestión de Red (SNMP) definida en la RFC 3416, es un protocolo primordial para la supervisión y gestión de dispositivos de red como routers, switches, servidores y estaciones de trabajo. Utiliza una estructura cliente-servidor donde los "managers" (gestores) solicitan información a los "agents" (agentes) que operan en los dispositivos gestionados. Los mensajes clave incluyen "GetRequest" para obtener datos, "SetRequest" para configurar parámetros y "Trap" para notificaciones no solicitadas sobre eventos ocurridos en los dispositivos gestionados. La versatilidad de SNMP radica en su capacidad para integrarse en plataformas de monitoreo, ofreciendo una visión integral del estado de las redes. (Simple Network Management Protocol, 2023).

Figura 3

Mensajes del protocolo SNMP v2c.



Nota: https://forum.huawei.com/enterprise/es/gesti%C3%B3n-de-red-el-principio-de-funcionamiento-del-protocolo-snmp/thread/766569-100237

2.1.5 Protocolo ICMP

Los dispositivos de red utilizan ICMP (Internet Control Message Protocol) especificado en la RFC 792, para intercambiar información sobre la capa de red. ICMP es usado a menudo para generar reportes de error. Por ejemplo, al establecer una sesión HTTP, se podría producir un mensaje de error indicando “Red de destino inalcanzable”.

Este mensaje es originado por ICMP. Significa que en algún punto de la red, un router no ha encontrado una ruta hasta el host especificado en la solicitud HTTP, y dicho router ha producido el mensaje ICMP a nuestro dispositivo de red para indicarle del error (Kurose & Ross, 2017).

2.1.6 Protocolo IPv4

IPv4, o Protocolo de Internet versión 4 (IP, por sus siglas en inglés), es la primera versión de este protocolo que es ampliamente utilizado. En el modelo TCP/IP para Internet, principalmente se utiliza el protocolo IPv4. Este se definió en la RFC 791, publicada en septiembre de 1981 por el Grupo de Trabajo en Ingeniería de Internet (IETF). Este documento reemplazó a la RFC 760, que había sido publicada en enero de 1980. IPv4 es un protocolo diseñado para la transferencia de datos entre redes mediante conmutación de paquetes, como en el caso de Ethernet. Asigna una dirección única a cada sistema, permitiendo que un dispositivo en Internet identifique y se comunique con otro. Algunas de sus principales características son:

- Servicio no fiable de datagramas, también conocido como de "mejor esfuerzo".
- No garantiza que los datos enviados hayan sido recibidos.
- No hay aseguramiento de que los datos transmitidos son corregidos.
- Es posible que los paquetes lleguen duplicados o desordenados.

Las direcciones en IPv4 son únicas y se pueden generar 4,294,967,295 direcciones como máximo, debido a que cada dirección tiene un tamaño de 4 bytes (4 bits). Hay un grupo de estas direcciones que están reservadas para usos específicos, por ejemplo redes privadas o multidifusión, lo que reduce la cantidad de direcciones disponibles para uso general. Esta limitación es uno de los motivos principales que impulsaron el desarrollo de IPv6, que está destinado a reemplazar a IPv4 en los próximos años (Montañez Prieto, 2018).

2.1.7 Direcciones IPv4

En cuatro octetos (8 bits por octeto), separados por puntos y representados en formato decimal conforman una dirección IPv4. Cada bit puede ser 0 o 1 (dos opciones), lo que significa que un octeto puede tener 2 elevado a la octava potencia combinaciones posibles, es decir, 256 valores. Como se inicia la cuenta desde 0, los valores del octeto están comprendidos entre 0 y 255. Las direcciones IPv4 se dividen en cinco clases: A, B, C, D y E. La clase de una dirección se determina por el valor del primer octeto. Actualmente, solo se utilizan las clases A, B y C para la asignación y el uso práctico, mientras que las clases D y E están reservadas para investigación y estudios técnicos (Montañez Prieto, 2018).

Figura 4

Clases de direcciones IPv4.

Nota: https://lordratita.files.wordpress.com/2012/06/sin-tc3adtulo5.jpg.

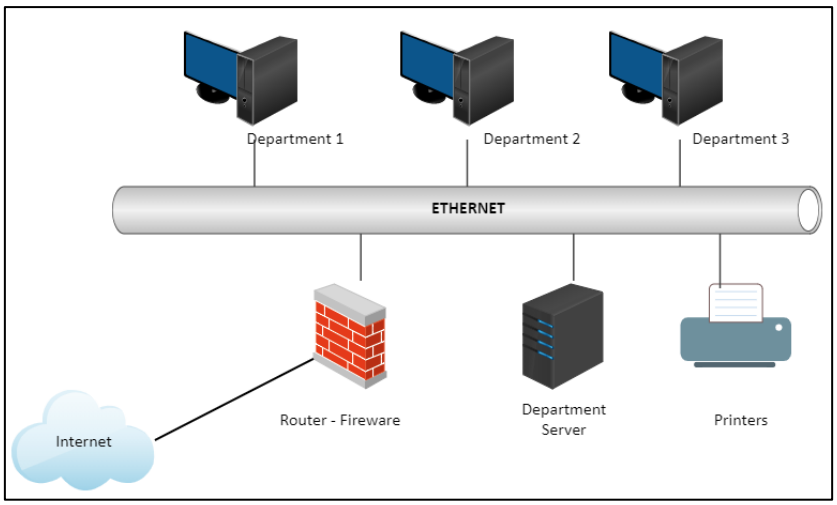
2.1.8 Red de Área Local (LAN)

Estas redes son de uso privado y abarcan una extensión limitada, generalmente de varios kilómetros. Se emplean en entornos como hogares, departamentos, oficinas, universidades o áreas específicas dentro de organizaciones. Su propósito principal es conectar dispositivos personales o estaciones de trabajo lo cual facilita la transferencia de información. Debido a su tamaño reducido, el tiempo máximo de transmisión de datos es predecible, lo que permite implementar diseños de red que serían menos efectivos en redes más grandes. Además, su gestión es más sencilla. Por lo general, estas redes utilizan un único cable al que se conectan todas las computadoras, a esto se denomina tecnología de

difusión. Funcionan a velocidades que varían entre 10 y 100 Mbps, ofreciendo un rendimiento con bajos tiempos de retardo y pocas interrupciones o fallas (Yacila, 2021).

Figura 5

Diagrama típico de una red LAN.



Nota: https://images.edrawsoft.com/articles/lan-diagram/ethernet-lan-protocol.png

2.1.9 Redes de Área Amplia (WAN)

Son aquellas redes que cubren grandes áreas geográficas, para lo cual utilizan redes de acceso público y redes de los ISP (Proveedores de Servicios de Internet). Estas redes generalmente están formadas por una serie de dispositivos de conmutación interconectados. La información transmitida por cualquier dispositivo de la red se dirige a través de estos nodos internos hasta llegar a su destino (Valarezo, 2020).

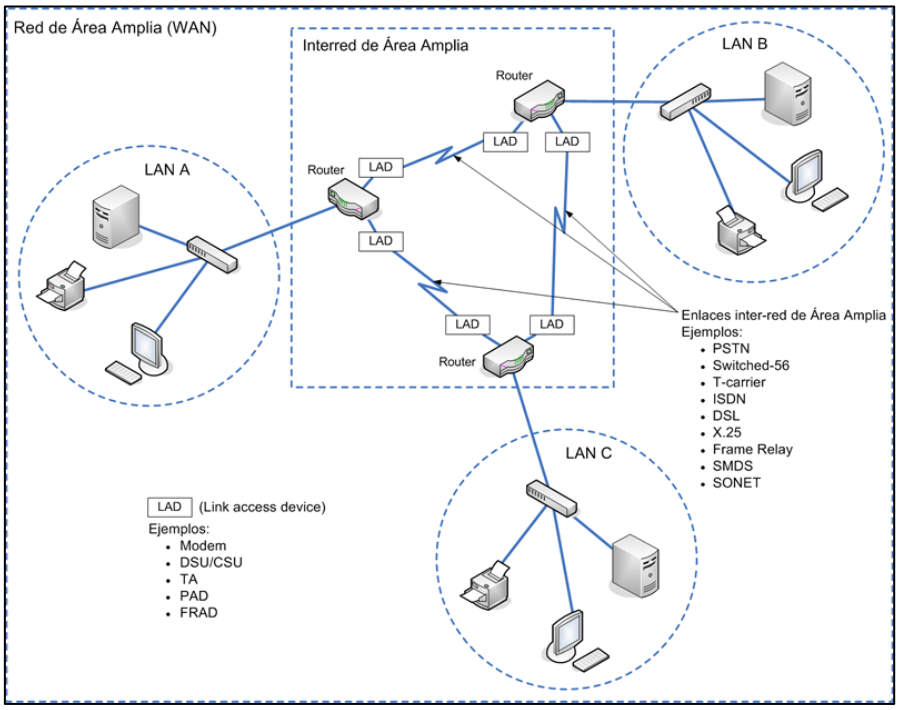
Las WAN se han implementado mediante diferentes tecnologías, entre ellas:

- Conmutación de circuitos: Este método consiste en establecer una ruta física dedicada exclusivamente a una conexión entre dos puntos de la red durante un tiempo limitado. Este tipo de conmutación es utilizado, por ejemplo, en los servicios tradicionales de telefonía fija para transmitir voz (Valarezo, 2020).
- Conmutación de paquetes: Esta tecnología divide los datos en pequeñas unidades llamadas paquetes, que se envían de manera independiente desde el origen hasta el destino a través de conmutadores y enrutadores. Cada paquete incluye información que identifica tanto al emisor como al receptor (Valarezo, 2020).

- Retransmisión de tramas (Frame Relay): Diseñada para aprovechar las altas velocidades de transmisión actuales y las bajas tasas de error, esta tecnología reduce la cantidad de información adicional utilizada para el control de errores. En lugar de depender de mecanismos redundantes, confía en la robustez del medio de transmisión y en los sistemas de destino para detectar y corregir errores. Este enfoque permite lograr mayores velocidades al minimizar la información redundante y el procesamiento asociado al control de errores (Valarezo, 2020).

Figura 6

Diagrama típico de una WAN.



Nota: https://www.textoscientificos.com/imagenes/redes/wan.png

2.1.10 Nodo de Seguridad Perimetral

La seguridad perimetral se refiere a los sistemas y herramientas diseñados para proteger redes privadas contra intrusiones, robo de información, ataques y amenazas. Su principal objetivo es reducir significativamente los riesgos asociados con la pérdida o el acceso no autorizado a los datos por parte de terceros. Además, actúa como una política de seguridad que regula la interacción entre una red privada y el internet (Espinoza, 2012, cómo se citó en Chavez, 2023).

Este enfoque de protección se basa en implementar medidas de seguridad en el perímetro exterior de la red y en sus diferentes capas. Esto permite garantizar altos niveles de confianza al mismo tiempo que proporciona un acceso controlado a servicios específicos para determinados usuarios, ya sean internos o externos, mientras se limita el acceso a otros (Espinoza, 2012, cómo se citó en Chavez, 2023).

Actualmente, existe una diversidad de herramientas de seguridad perimetral diseñadas para reducir los riesgos asociados con el uso de redes. Estas herramientas, como los firewalls, honeypots, iptables, entre otras, tienen como objetivo principal garantizar la confidencialidad e integridad de los datos, así como, prevenir cualquier posible evento que comprometa la seguridad de la información (Marín et al.,2020, tal cómo, se citó en Chavez, 2023).

2.1.11 Firewall

Un firewall, también conocido como "corta fuego", es un dispositivo o software diseñado para analizar el tráfico de red, bloquear o permitir de acuerdo a un conjunto de reglas establecidas por los administradores de red. Los firewalls operan a través de reglas de entrada y salida. Generalmente, asocian servicios de la capa 6 del modelo OSI con filtros en la capa 3 del mismo modelo. Un firewall perimetral basado en la capa 3 del modelo OSI permite gestionar el tráfico entrante y saliente mediante reglas que especifican servicios (puertos) asociados a esta capa. Estas reglas definen, por ejemplo, si se permitirá el tráfico desde o hacia una dirección IP o un servicio específico, o ambos. Este conjunto de reglas cubre todas las direcciones IP y servicios como SSH, HTTP, HTTPS, NTP, entre otros, permitiendo únicamente el acceso necesario según los requerimientos de la organización (Ruiz, 2024).

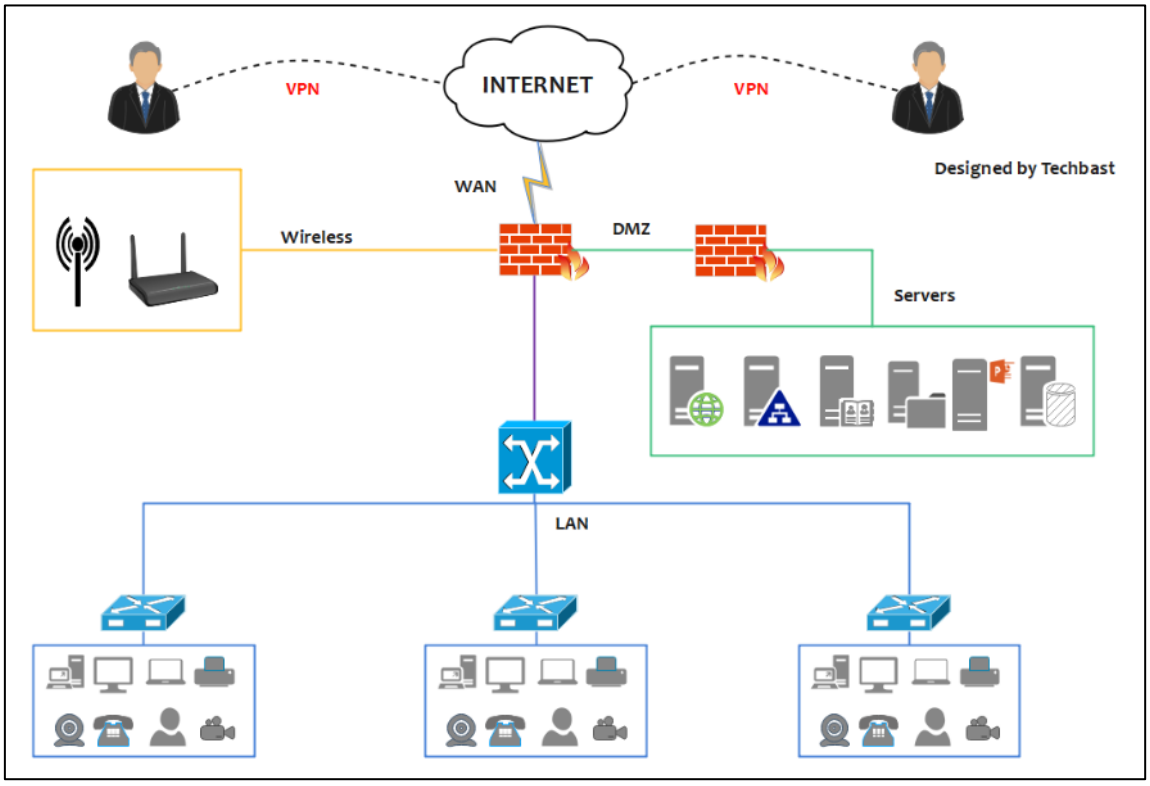
Existen dos enfoques principales para el filtrado de firewalls: los permisivos, que permiten todo el tráfico salvo las excepciones definidas en las reglas, y los restrictivos, que bloquean todo el tráfico a menos que esté específicamente permitido. Los firewalls perimetrales suelen ubicarse en la salida hacia Internet (ISP), pero también pueden estar

integrados en los sistemas operativos de los equipos de trabajo. Además, algunos dispositivos de red, como switches o puntos de acceso inalámbricos, pueden incluir funcionalidades de firewall. El filtrado que realizan abarca varias capas del modelo OSI, desde la capa física hasta la capa de aplicación (Ruiz, 2024).

Cuando se trata de hardware, un firewall se asemeja a un equipo de comunicación, como un switch, pero está equipado con un sistema operativo y hardware dedicados al filtrado de datos. Si es un software, se implementa directamente en el sistema operativo. La mayoría de los sistemas operativos, tanto de código abierto como propietarios, incluyen opciones para configurar firewalls y, por lo general, vienen con reglas predefinidas al ser instalados. Además, algunos sistemas pueden configurarse como firewalls perimetrales. Existen dispositivos especializados diseñados exclusivamente para actuar como firewalls, fabricados por marcas reconocidas como Cisco®, Fortinet®, Palo Alto®, entre otras (Ruiz, 2024).

Figura 7

Diagrama de una solución de red con firewall.



Nota: https://edrawmax.wondershare.com/article2023/firewall-network-diagram/main-pic.png

2.1.12 Tracert

El comando tracert, es una herramienta utilizada para diagnosticar redes, ya que permite en una red IP trazar la ruta desde el origen hasta el destino final que siguen los paquetes de datos. Su función principal es identificar cada nodo intermedio, como routers o gateways, por los que pasan los paquetes, proporcionando detalles sobre la ruta y los tiempos de respuesta en cada etapa. Cuando se ejecuta tracert, se envían paquetes con un valor inicial bajo en el campo TTL (Time To Live), el cual aumenta en cada intento posterior. Los routers que reciben estos paquetes disminuyen el valor del TTL en uno. Si el TTL toma un valor de cero, el router devuelve un mensaje de error ICMP al emisor. Este mecanismo permite a tracert registrar y mostrar cada punto intermedio en el trayecto hacia el destino (Microsoft, 2024).

Este comando resulta especialmente valioso para resolver problemas de conectividad, localizar posibles cuellos de botella en la red y analizar la ruta que siguen los datos hacia un servidor o dispositivo específico. En sistemas Windows, esta herramienta se conoce como tracert, mientras que en sistemas Unix y Linux se denomina traceroute (Microsoft, 2024).

2.1.13 Sniffer

Un sniffer es una herramienta tecnológica utilizada para interceptar y examinar el tráfico de datos dentro de una red. Su propósito principal es capturar los paquetes de datos en tránsito, permitiendo a los administradores de red monitorear el estado de la conexión, identificar fallos y mejorar el rendimiento de la red. No obstante, es crucial señalar que, si se utiliza con fines malintencionados, un sniffer puede emplearse para realizar actividades ilícitas, como el robo de información confidencial (Universidad VIU, 2017)

Entre los tipos de sniffers disponibles, se destacan:

- Sniffers de red: Diseñados para interceptar y analizar el tráfico general de la red.
- Sniffers de protocolo: Enfocados en la captura y análisis de datos específicos de ciertos protocolos.

- Sniffers de aplicación: Utilizados para recopilar y estudiar el tráfico generado por aplicaciones particulares.

2.1.14 Software de Monitoreo

Es una herramienta diseñada para supervisar, gestionar y optimizar el rendimiento de redes, aplicaciones y dispositivos conectados. Estos softwares ofrecen visibilidad completa de extremo a extremo, permitiendo a las organizaciones identificar y resolver problemas de conectividad, rendimiento y seguridad de manera proactiva. Estos softwares permiten a los administradores de TI supervisar redes locales y en la nube, implementar políticas, y mejorar la experiencia del usuario mediante la identificación de cuellos de botella o fallos en los servicios. Además, son fundamentales para mantener una infraestructura de red confiable, segura y optimizada, adaptándose a las necesidades específicas de cada organización. Estos softwares pueden ser propietarios o basados en open source (Cisco, 2024).

2.1.15 Open Source

Open Source hace referencia a un modelo de desarrollo de software en el que el código fuente está disponible para todos. Esto permite que cualquier persona pueda leer, editar y compartir el código, siempre que respete los términos de la licencia correspondiente. Este enfoque fomenta la colaboración, la transparencia y el perfeccionamiento continuo del software. Los proyectos de código abierto suelen ser creados y mantenidos de forma comunitaria, lo que facilita que desarrolladores de diferentes partes del mundo contribuyan con sus conocimientos y habilidades para mejorarlos (Open Source Initiative, 2024).

La Open Source Initiative (OSI) define formalmente el concepto de Open Source a través de una serie de principios, entre los cuales se encuentran (Open Source Initiative, 2024):

- Distribución gratuita: El software puede ser compartido sin restricciones.
- Acceso al código fuente: El código debe estar disponible o ser fácil de obtener.

- Permiso para modificar: Los usuarios tienen libertad para modificar el código y distribuir versiones derivadas.
- No discriminación: El uso del software no puede limitarse a ciertos grupos o personas.

2.1.16 OpenNMS Horizon

OpenNMS es una solución para el monitoreo de redes de código abierto, diseñada para proporcionar una visión completa de las actividades en redes locales y distribuidas. Ofrece funcionalidades integrales que incluyen monitoreo de fallos, rendimiento y tráfico, junto con generación de alertas centralizada. Su alta personalización, escalabilidad y capacidad de integración con aplicaciones comerciales hacen de OpenNMS una herramienta versátil y eficiente (OpenNMS Group, 2024).

Características principales de OpenNMS Horizon indicadas en el anexo 2:

- Gestión de inventario: Proporciona un sistema flexible de aprovisionamiento que facilita la interoperabilidad con herramientas de gestión de configuración (OpenNMS Group, 2024).
- Recopilación de datos amplia: Soporta múltiples protocolos estándar de la industria sin necesidad de dependencias externas, incluyendo SNMP, JSON, WinRM, XML, SQL, JMX, SFTP, FTP, JDBC, HTTP, HTTPS, VMware, WS-Management y Prometheus (OpenNMS Group, 2024).
- Gestión avanzada del tráfico: Compatible con protocolos de flujo como NetFlow (v5/v9), IPFIX y sFlow, procesando más de 300,000 flujos por segundo. También ofrece monitoreo de BGP mediante la implementación de estándares OpenBMP para métricas y mensajes, junto con análisis detallado y generación de informes empresariales (OpenNMS Group, 2024).
- Monitoreo de experiencia digital: Utiliza OpenNMS Minion para evaluar la latencia y disponibilidad de servicios desde múltiples puntos de vista (OpenNMS Group, 2024).

- Configuración avanzada: Permite configurar la mayoría de sus funciones a través de una interfaz web o scripts XML, abarcando umbrales, gestión de eventos y flujos, supervisión de servicios y medición de rendimiento (OpenNMS Group, 2024).
- Escalabilidad: Escala de manera eficiente mediante Sentinels para la persistencia de flujos, Minions para la ingesta de flujos, BMP, SNMP y Syslog, así como el uso de agentes de mensajes ActiveMQ a Kafka integrados (OpenNMS Group, 2024). Puede supervisar una gran cantidad de dispositivos y datos a través de una red distribuida organizada en niveles. Esto incluye la gestión de 1.2 millones de puntos de datos cada 5 minutos, más de 5,000 interfaces, cientos de miles de dispositivos individuales, millones de métricas de rendimiento, miles de eventos por segundo y numerosos monitores remotos, garantizando un control eficiente y detallado de toda la red (OpenNMS Group, 2021).
- Informes y visualización profesional: Ofrece paneles personalizables que se pueden exportar como PDF, gráficos de recursos, informes de bases de datos y diagramas. Además, permite definir topologías complejas en capas e integrar mapas de topología en flujos de trabajo de gestión de problemas de servicio (OpenNMS Group, 2024).
- Alertas categorizadas por severidad: Como se muestra en la figura 8 las alarmas se organizan en siete categorías, cada una identificada por un color distinto: el rojo indica una alarma crítica, el naranja corresponde a una alarma mayor que indica que un dispositivo se ha desconectado completamente y el ámbar representa una alarma menor que indica que interfaces o servicios del dispositivo se han desconectado. El amarillo señala una advertencia de peligro, mientras que el verde limón se asocia con una alarma indeterminada que indica que el evento no se asocia a una alarma, aunque es poco frecuente en el monitoreo. El verde denota un estado normal, y finalmente, el gris indica que un error previo ha sido corregido y el servicio se ha restaurado (OpenNMS Group, 2024).

Figura 8

Clasificación de alertas.

Critical	This event means numerous devices on the network are affected by the event. Everyone who can should stop what they are doing and focus on fixing the problem.
Major	A device is completely down or in danger of going down. Attention needs to be paid to this problem immediately.
Minor	A part of a device (a service, and interface, a power supply, etc.) has stopped functioning. The device needs attention.
Warning	An event has occurred that may require action. This severity can also be used to indicate a condition that should be noted (logged) but does not require direct action.
Indeterminate	No Severity could be associated with this event.
Normal	Informational message. No action required.
Cleared	This event indicates that a prior error condition has been corrected and service is restored

Nota: plataforma OpenNMS Horizon.

Por lo mencionado anteriormente, OpenNMS combina capacidades avanzadas de monitoreo con un diseño flexible y escalable, convirtiéndolo en una solución ideal para gestionar redes de cualquier tamaño o complejidad (OpenNMS Group, 2024).

2.2 Marco conceptual

Este marco teórico tiene como objetivo establecer las metodologías, herramientas y técnicas necesarias para desarrollar el trabajo de suficiencia profesional, basándose en una revisión exhaustiva de información relacionada con el tema propuesto. Para ello, se consultan diversas fuentes, como libros, manuales del fabricante, tesis de grado previas, revistas de investigación vinculadas al área de aplicación del proyecto y publicaciones en páginas web.

2.2.1 Gestión de Red

Sobre la gestion de red, Kurose y Ross (2017) citan a Saydam (1996) quien opina que “La gestión de red incluye la implantación, integración y coordinación del hardware, el software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar,

evaluar y controlar los elementos y recursos de la red, con el fin de satisfacer los requisitos de tiempo real, de rendimiento operativo y de Calidad de Servicio, a un coste razonable" (p. 348).

A continuación, en la figura 9 se indican los principales componentes de la gestion de red:

a) Servidor de Gestión. Es una aplicación, generalmente manejada por un operador y que funciona dentro de una unidad central de gestión de red ubicada en el Centro de Operaciones de Red (NOC, por sus siglas en inglés). Este servidor de gestión actúa como el núcleo de las actividades administrativas de la red, encargándose de recopilar, procesar, analizar y presentar la información relacionada con su gestión. Además, es el lugar desde donde se toman decisiones para controlar el comportamiento de la red y donde el administrador interactúa directamente con los dispositivos que la componen (Kurose & Ross, 2017).

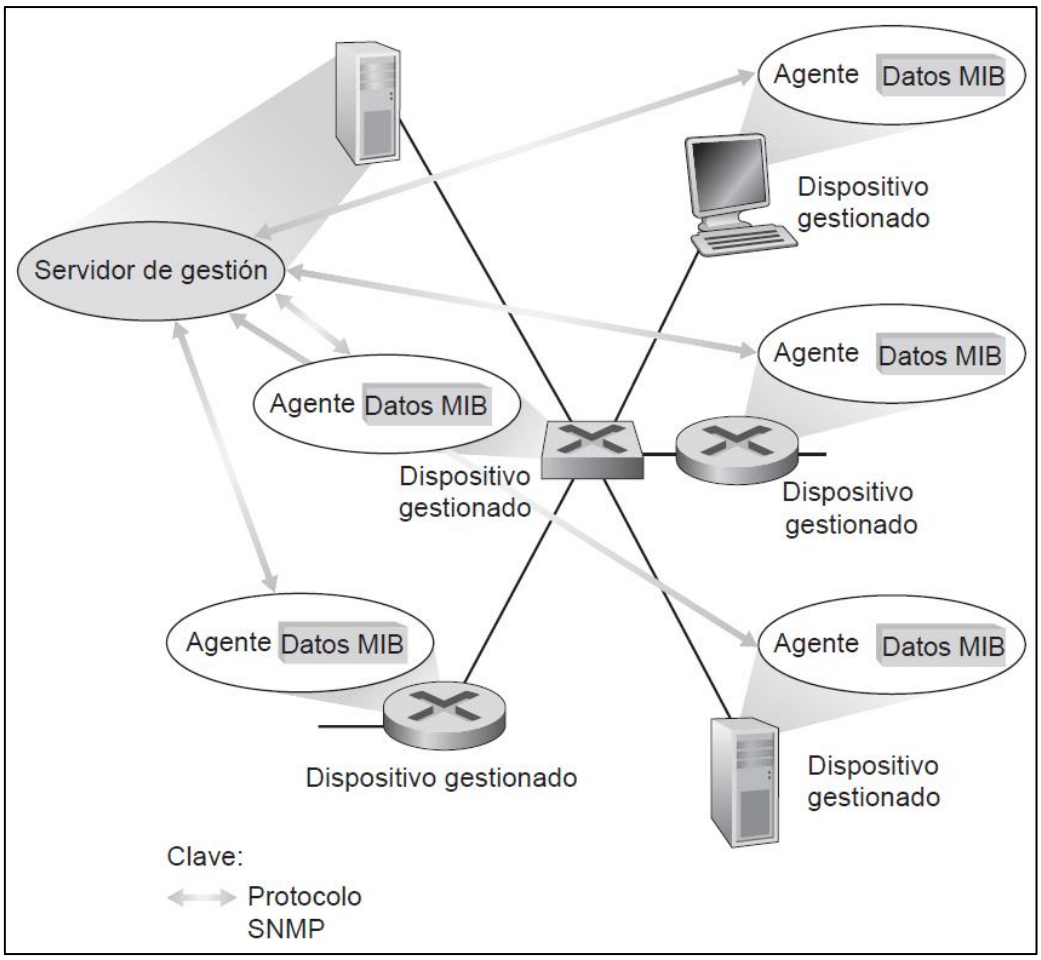
b) Dispositivo Gestionado. Es un dispositivo de red con software, que forma parte de una infraestructura gestionada. Este tipo de equipo puede ser un host, router, switch, dispositivo intermediario, módem, termómetro u otro elemento conectado a la red. Dentro de cada dispositivo gestionado existen múltiples objetos gestionados, que incluyen tanto los componentes físicos, como una tarjeta de interfaz de red (parte de un host o router), como los parámetros de configuración asociados a esos elementos de hardware y software, por ejemplo, un protocolo de enrutamiento interno como OSPF en un sistema autónomo (Kurose & Ross, 2017).

c) Base de Información de Gestión (MIB, Management Information Base). Cada objeto gestionado dentro de un dispositivo cuenta con diversos elementos de información asociados, los cuales se almacenan en una Base de Información de Gestión (MIB, por sus siglas en inglés). Estos datos están disponibles para el servidor de gestión, que, en muchos casos, también tiene la capacidad de modificarlos. Un objeto de la MIB puede representar diferentes tipos de información, como un contador (por ejemplo, el número de datagramas IP descartados en un router debido a errores en sus encabezados, o el número de

segmentos UDP recibidos por un host), datos descriptivos (como la versión del software ejecutándose en un servidor DNS), información sobre el estado de un dispositivo (indicando si está operando correctamente) o datos específicos de protocolos (como la ruta hacia un destino determinado) (Kurose & Ross, 2017).

Figura 9

Componentes de la gestión de red.



Nota. Tomado de (Kurose & Ross, 2017).

d) Agente de Gestión de Red. Es un proceso encargado de ejecutarse en el dispositivo de red. Este agente se comunica con el servidor de gestión y realiza acciones locales en el dispositivo bajo las instrucciones y supervisión de dicho servidor (Kurose & Ross, 2017).

e) Protocolo de Gestión de Red. El protocolo se encarga de la comunicación entre el servidor de gestión y los dispositivos que administra, permitiendo que el servidor pueda

revisar cómo están funcionando y dar instrucciones, todo esto a través de los agentes que los gestionan. Además, los agentes pueden usar el protocolo para notificar al servidor de gestión sobre eventos inusuales, como fallos en componentes o el incumplimiento de límites de rendimiento establecidos. Es fundamental destacar que el protocolo de gestión de red no realiza la administración de la red por sí mismo, sino que proporciona herramientas que los administradores pueden emplear para llevar a cabo tareas de monitoreo, pruebas, configuración, análisis y control de la red (Kurose & Ross, 2017).

2.2.2 Normatividad

A continuación, se presentan algunos estándares para la gestión de una red.

a) ISO/IEC 27035:2016. Esta norma ayuda a las organizaciones a saber cómo actuar y qué pasos seguir cuando ocurre un problema de seguridad con su información., adaptable a organizaciones de cualquier tamaño o industria. Sirve como una guía práctica para establecer un proceso organizado y efectivo que permita identificar, manejar y prevenir incidentes relacionados con la seguridad (International Organization for Standardization, 2016).

De acuerdo con la ISO/IEC 27035:2016 la atención de incidentes tiene 5 etapas (International Organization for Standardization, 2016):

- Planificación y Preparación. Para afrontar de manera efectiva los problemas de seguridad con la información, es clave tener reglas claras sobre cómo actuar y contar con un equipo preparado que sepa cómo responder cuando ocurre un incidente.

- Detección y Reporte. Identificar y notificar cualquier "evento" que pueda constituir o evolucionar en un incidente de seguridad.

- Evaluación y Decisión. Analizar la situación para confirmar si se trata efectivamente de un incidente de seguridad.

- Respuesta. Implementar acciones para contener, eliminar, recuperar y, cuando sea necesario, realizar un análisis forense del incidente.

- Lecciones aprendidas. En la gestión de riesgos de información se debe incorporar mejoras sistemáticas a partir de los incidentes experimentados.

b) ISO/IEC 20000. Es un estándar internacional para la gestión de servicios, se basó originalmente en una norma británica creada en el año 2000, adoptado a nivel mundial en 2005 y revisado por última vez en 2011. Aunque formalmente está compuesta por varias partes, el término ISO 20000 suele referirse a su primera sección, que establece lo que se necesita para implementar un sistema de gestión de servicios. Este estándar propone un enfoque basado en procesos integrados para garantizar que todas las etapas del servicio desde su diseño hasta su mejora continua se lleven a cabo cumpliendo con lo que se ha acordado o establecido previamente, generando valor tanto para los clientes como para los proveedores. Además, la norma promueve la aplicación de la metodología de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar) en todos los componentes del sistema de gestión y en los propios servicios, asegurando que sean diseñados, implementados, operados, evaluados y optimizados de manera constante (Cáceres, 2020).

La norma ISO 20000 establece un control riguroso sobre la gestión y el soporte de servicios de TI, asegurando que se utilicen procesos diseñados para ofrecer un servicio eficiente. Este estándar explica cómo organizar y ajustar los sistemas, así como cómo detectar y resolver los problemas que puedan surgir en el área de tecnología de la información. Una de sus principales ventajas es su capacidad de alinearse fácilmente con otras normas, lo que facilita a las organizaciones la implementación de sistemas de gestión integrados (Cáceres, 2020).

c) NIST SP 800-92. Esta guía, elaborada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, ofrece un marco para la gestión de registros de seguridad en entornos corporativos. Proporciona recomendaciones sobre la recopilación, almacenamiento y análisis de logs, con el objetivo de detectar y abordar incidentes de seguridad. Además, resalta el valor del análisis de registros para identificar amenazas de manera proactiva, optimizar la respuesta ante incidentes y facilitar investigaciones forenses. Es una herramienta esencial para establecer un monitoreo efectivo en Centros

de Operaciones de Seguridad (SOC) y sistemas de seguridad perimetral (National Institute of Standards and Technology, 2006).

d) RFC 2196 - Site Security Handbook. Este manual, desarrollado por la Internet Engineering Task Force (IETF), ofrece una guía completa para establecer políticas y procedimientos de seguridad en redes. Proporciona estrategias para configurar dispositivos de manera segura, realizar monitoreos, llevar a cabo auditorías periódicas y responder a incidentes. Además, incluye recomendaciones para gestionar vulnerabilidades específicas y salvaguardar información crítica. Es una herramienta esencial para profesionales encargados de la administración de redes y la seguridad en organizaciones tecnológicas (Fraser, 1997).

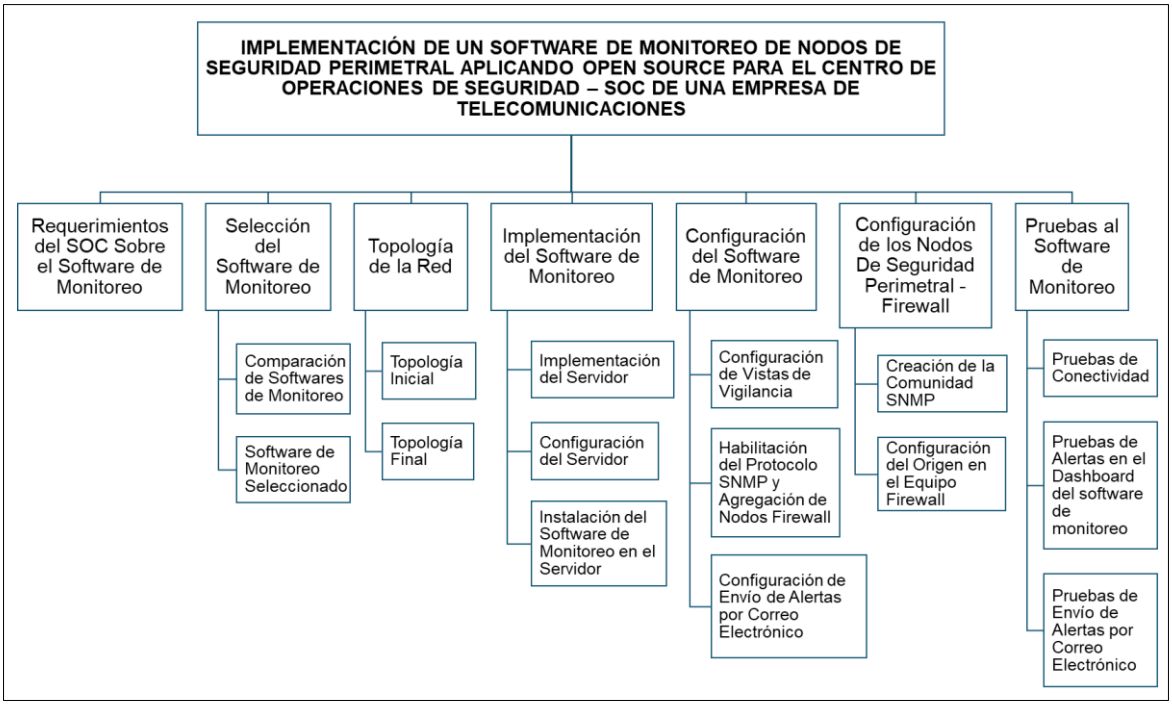
Capítulo III. Desarrollo del Trabajo de Investigación

En este capítulo se describe en detalle el Informe de Suficiencia Profesional, identificando los requerimientos del SOC de la Empresa de Telecomunicaciones con relación al software de monitoreo, con esta información se evaluó y selecciono al software de supervisión y monitoreo. Seguidamente se instaló, configuro e integro a los nodos de seguridad perimetral – firewalls los cuales se indican en el anexo 1, finalmente se procedió a ejecutar las pruebas de funcionalidad del software de monitoreo.

El software de supervisión y monitoreo fue sometido a pruebas en conformidad con la estructura de desglose trabajo (EDT) presentada en la figura 10.

Figura 10

EDT para la implementación del software de monitoreo.



Nota. Elaboración propia.

Seguidamente se presentó un cronograma de actividades como se muestra en la figura 11 en el cual se indica la secuencia de las tareas de ejecución establecidas en la EDT de la implementación del software de monitoreo.

Figura 11

Cronograma para la implementación del software de monitoreo.

Actividades / Semanas	2024					
	Enero		Febrero			
	3	4	1	2	3	4
1. Requerimientos del SOC Sobre el Software de Monitoreo						
2. Selección del Software de Monitoreo						
Comparación de Softwares de Monitoreo						
Software de Monitoreo Seleccionado						
3. Topología de la Red						
Topología Inicial						
Topología Final						
4. Implementación del Software de Monitoreo						
Implementación del Servidor						
Configuración del Servidor						
Instalación del Software de Monitoreo en el Servidor						
5. Configuración del Software de Monitoreo						
Configuración de Vistas de Vigilancia						
Habilitación del Protocolo SNMP y Agregación de Nodos Firewall						
Configuración de Envío de Alertas por Correo Electrónico						
6. Configuración de los Nodos De Seguridad Perimetral - Firewall						
Creación de la Comunidad SNMP						
Configuración del Origen en el Equipo Firewall						
7. Pruebas al Software de Monitoreo						
Pruebas de Conectividad						
Pruebas de Alertas en el Dashboard del software de monitoreo						
Pruebas de Envío de Alertas por Correo Electrónico						

Nota. Elaboración propia.

3.1 Requerimientos del SOC Sobre el Software de Monitoreo

El SOC de la Empresa de Telecomunicaciones requiere que las características y funcionalidades del software de supervisión y monitoreo, satisfaga los siguientes requerimientos:

- Capacidad de supervisar más de 2500 sensores de software de monitoreo.
- Software de monitoreo en conformidad con el protocolo SNMP para la recolección de información acerca de la operación de los nodos de seguridad perimetral.
- Niveles de alertas clasificadas según su grado de severidad.
- Visibilidad de las interfaces de los nodos de seguridad perimetral.
- Software de monitoreo escalable y personalizable gracias a la capacidad de generar gráficas de rendimiento, reportes y alertas.
- Interfaz gráfica que proporciona información para que los ingenieros de seguridad tomen decisiones oportunas.

- Envío de alertas en tiempo real por correo electrónico.
- Mínimo costo de implementación del software de monitoreo.

3.2 Selección del Software de Monitoreo

La oferta creciente y sostenida de productos de software de supervisión y monitoreo, con sus correspondientes características, funcionalidades y restricciones, tanto licenciados como los existentes en la modalidad OPEN SOURCE. En conformidad con estas características y según los requerimientos del SOC de la Empresa de Telecomunicaciones se procedió a elegir un programa de software de supervisión y monitoreo. En base a la tabla de requerimientos que debía de reunir un programa software de supervisión y monitoreo, propuesta por Casas y Sempértegui (2017), sintonizado con las características y requerimientos del SOC de la Empresa de Telecomunicaciones. El software de monitoreo ha de satisfacer los requerimientos y necesidades que se muestran en la tabla 2.

Tabla 2

Requerimientos del SOC de la empresa de telecomunicaciones.

REQUERIMIENTO	IMPACTO	VALOR MÍNIMO	VALOR MÁXIMO
Software basado en Open Source.	ALTO	0	5
Monitoreo en tiempo real de la infraestructura de red.	ALTO	0	5
Monitoreo en tiempo real de los servicios de red.	ALTO	0	5
Generación de Reportes.	ALTO	0	5
Envío de notificaciones vía correo electrónico.	ALTO	0	5
Uso del protocolo SNMP.	ALTO	0	5
Actualizaciones periódicas.	ALTO	0	5
Envío de notificaciones vía aplicaciones móviles.	MEDIO	0	3
Visualización de Topología de red.	MEDIO	0	3
Generación de gráficas de rendimiento y disponibilidad.	MEDIO	0	3
Variedad de agentes.	MEDIO	0	3
Variedad de plugins.	MEDIO	0	3
Autodescubrimiento de la red.	MEDIO	0	3
Documentación y soporte.	BAJO	0	2
TOTAL		0	50

Nota. Adaptado de Tesis “Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red para Optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo”

3.2.1 Comparación de Softwares de Monitoreo

En base a la tabla de comparación y evaluación de software de supervisión y monitoreo propuesta por Casas y Sempértegui (2017), como en la tabla 2 de requerimientos del SOC de la empresa de telecomunicaciones se elaboró una nueva tabla de evaluación la cual incluye al software de supervisión y monitoreo OpenNMS Horizon obteniéndose los resultados presentados en la tabla 3.

Tabla 3

Evaluación de los softwares de monitoreo.

REQUERIMIENTO	CACTI	COLLECTD	FREENATS	GANGLIA	ICINGA	MUNIN	NAGIOS	OpenNMS Horizon	PRTG NETWORK MONITOR	WHATSUP GOLD	ZABBIX
Software basado en Open Source	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	NO (0)	NO (0)	SI (5)
Monitoreo en tiempo real de la infraestructura de red	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Monitoreo en tiempo real de los servicios de red	SI (5)	NO (0)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Generación de Reportes	SI (5)	NO (0)	SI (5)	NO (0)	SI (5)	NO (0)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Envío de notificaciones vía correo electrónico	SI (5)	SI (5)	SI (5)	NO (0)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Uso del protocolo SNMP	SI (3)	SI (3)	NO (0)	SI (3)	SI (3)	SI (3)	SI (3)	SI (5)	SI (3)	SI (3)	SI (3)
Actualizaciones periódicas	SI (1)	SI (1)	SI (1)	SI (1)	SI (2)	SI (1)	SI (2)	SI (2)	SI (2)	SI (2)	SI (2)
Envío de notificaciones vía aplicaciones móviles	NO (0)	NO SE CONOCE	NO SE CONOCE	NO SE CONOCE	NO SE CONOCE	NO SE CONOCE	SI (3)	SI (3)	SI (3)	NO SE CONOCE	SI (3)
Visualización de Topología de red	SI (2)	NO (0)	NO (0)	SI (2)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)
Generación de gráficas de rendimiento y disponibilidad	SI (2)	NO (0)	NO (0)	SI (2)	SI (2)	SI (2)	SI (2)	SI (2)	SI (3)	SI (3)	SI (2)
Variedad de agentes	SI (2)	SI (2)	NO (0)	NO (0)	SI (3)	NO (0)	SI (3)	NO (0)	SI (3)	SI (3)	SI (3)
Variedad de plugins	SI (2)	SI (2)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (2)
Autodescubrimiento de la red	NO (0)	NO (0)	SI (3)	NO (0)	NO (0)	SI (3)	NO (0)	SI (3)	SI (3)	SI (3)	NO (0)
Documentación y soporte	SI (2)	NO (0)	SI (2)	SI (1)	SI (2)	SI (2)	SI (2)	SI (2)	SI (2)	SI (2)	SI (2)
PUNTAJE	39	23	34	27	43	37	46	48	45	42	45

Nota. Adaptado de la Tesis "Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red para Optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo"

3.2.2 Software de Monitoreo Seleccionado

Luego de comparar y evaluar las capacidades de los distintos programas de software de supervisión y monitoreo se evaluaron los resultados de la tabla 3, decidiendo por el software de monitoreo OpenNMS Horizon, el cual satisface la mayoría de los requerimientos del SOC de la Empresa de Telecomunicaciones.

Las principales características del software OpenNMS Horizon son:

- Software distribuido bajo licencia OPEN SOURCE, su licenciamiento no requiere ningún pago, en consecuencia, su costo de implementación es mínimo, adicionalmente tiene la capacidad de supervisar más de 2500 aspectos.
- El software de supervisión y monitoreo OpenNMS Horizon concurrente con el protocolo SNMP que reúne información del estado de salud de los nodos de seguridad perimetral.
- No requiere la instalación de agentes en los nodos de seguridad perimetral, por lo cual, los nodos de seguridad perimetral no experimentan interrupciones.
- Visibilidad de las interfaces de los nodos de seguridad perimetral y la categorización de las alertas por grado de severidad.

3.3 Topología de la Red

A continuación, se describe la topología inicial que requiere el monitoreo de nodos de seguridad perimetral en correspondencia con el software licenciado PRTG y la topología que implementará el software de monitoreo OpenNMS.

3.3.1 Topología Inicial

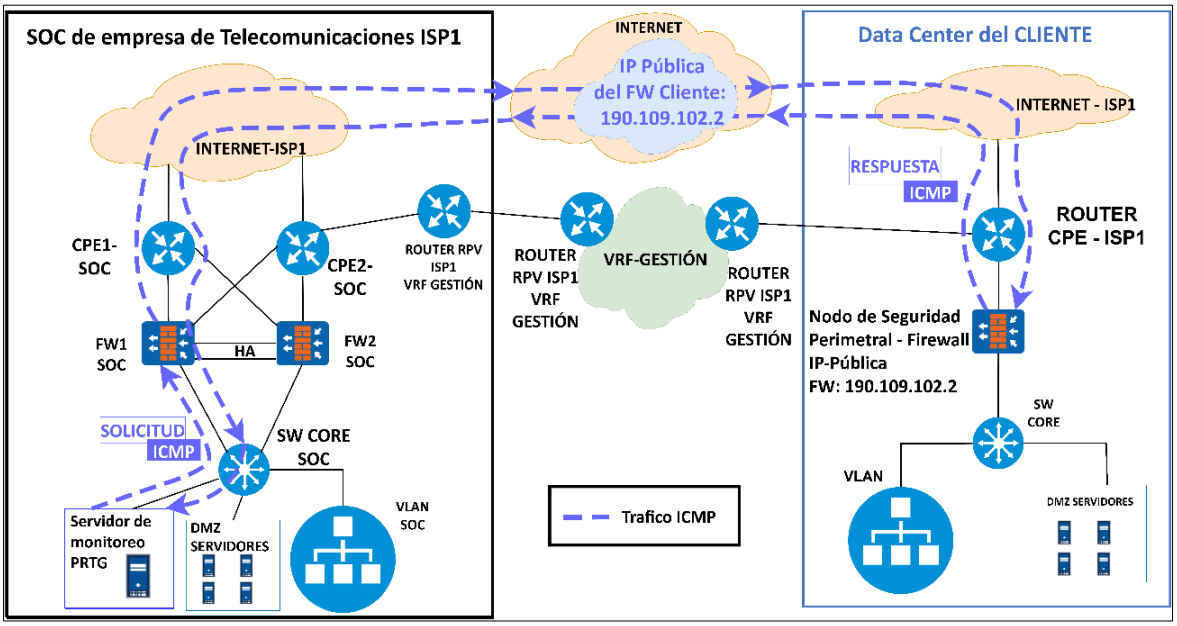
El SOC de la Empresa de Telecomunicaciones del año 2023, contaba con una topología de monitoreo de nodos de seguridad perimetral – firewall, tal como, se muestra en la figura 12, en la cual puede observarse que el diagrama de red del SOC integrada por los CPE (Equipo Local del Cliente) 1 y 2 redundantes, un router para la RPV de VRF de gestión, los dispositivos firewall FW1 y FW2 configurados para HA (Alta Disponibilidad), el dispositivo Switch Core, VLAN del SOC y la DMZ de servidores que almacenan al software

PRTG. También se muestra un típico diagrama para un cliente corporativo, constituido por CPE – ISP1, el nodo de seguridad – firewall que tiene una dirección IP pública: 190.109.102.2 y la VLAN del cliente.

El monitoreo se ejecuta de la siguiente manera, el software PRTG vía internet envía consultas de protocolo ICMP a la dirección IP pública: 190.109.102.2 de la interface WAN del nodo de seguridad perimetral del cliente, este nodo responde con un paquete ICMP indicando el estado de accesibilidad de la interface, esta forma de monitoreo, únicamente permite visualizar la interface WAN sin permitir visualizar las interfaces LAN, VRF u otra interface del firewall.

Figura 12

Topología de monitoreo de nodos de seguridad perimetral con PRTG.



Nota. Elaboración propia, basada en la arquitectura de sondeo de PRTG, White paper: Sondas remotas, https://www.paessler.com/es/learn/whitepapers/white_paper_managing_central_monitoring.

3.3.2 Topología Final

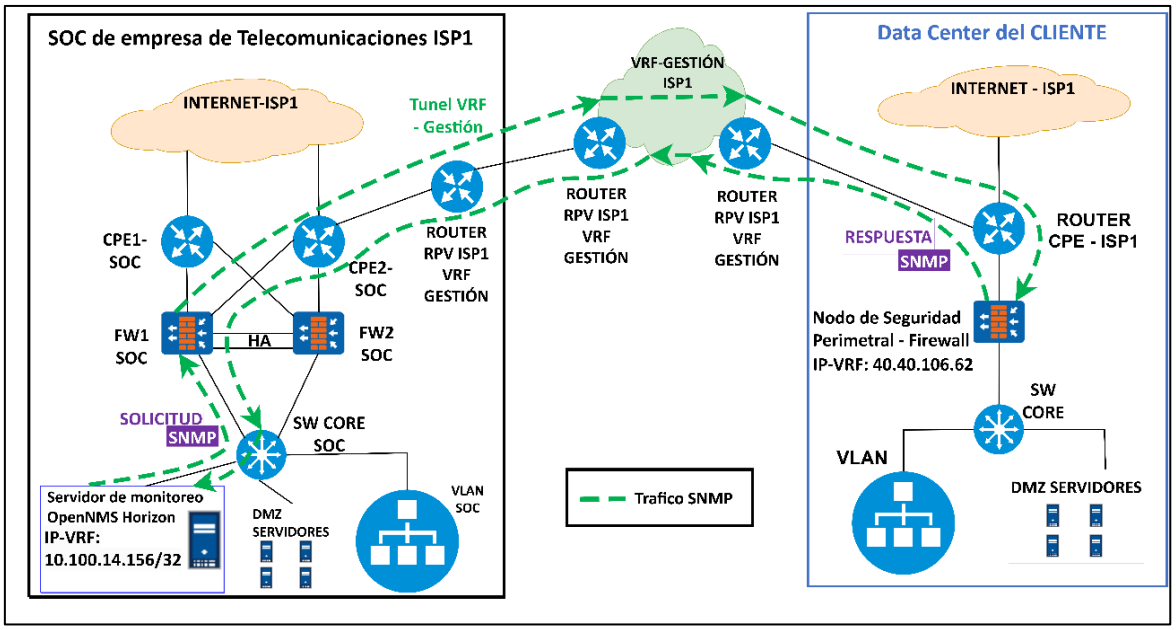
La topología de monitoreo de los nodos de seguridad perimetral con el cual se implementará el software OpenNMS Horizon, tal como, como se muestra en la figura 13, donde puede observarse el diagrama de red del SOC integrada por los CPE (Equipo Local del Cliente) 1 y 2 redundantes, un router para la RPV del VRF de gestión del ISP1, los dispositivos firewall FW1 y FW2 configurados para una prestación en HA (Alta

Disponibilidad), el dispositivo Switch Core, VLAN del SOC y la DMZ de servidores la cual se encuentra el servidor del software de monitoreo OpenNMS Horizon con la dirección IP: 10.100.14.156. Así mismo, se muestra el diagrama de red típico de un cliente corporativo, el cual está integrado por CPE – ISP1, el nodo de seguridad – firewall con una dirección IP de VRF de gestión: 40.40.106.62 y la VLAN del cliente.

El monitoreo funciona de la siguiente forma, el software OpenNMS Horizon vía la RPV de VRF de gestión envía consultas del estado del protocolo SNMP hacia la dirección IP de VRF: 40.40.106.62 de la interface VRF del nodo de seguridad perimetral del cliente para señalar a un nodo especifico, el nodo responderá con paquetes SNMP con información acerca del estado de las interfaces, servicios y parámetros que informan la integridad de dicho dispositivo. Esta topología de monitoreo proporciona la visibilidad completa del nodo de seguridad perimetral - firewall, no solo de las interfaces WAN, LAN, VRF u otra interface del firewall sino también del estado del CPU, memoria, ancho de banda y entre otros parámetros.

Figura 13

Topología de monitoreo de nodos de seguridad perimetral con OpenNMS Horizon.



Nota. Elaboración propia, basada en la arquitectura de monitoreo de OpenNMS, https://www.opennms.com/resources/security-reference-architecture/#.

3.4 Implementación del Software de Monitoreo OpenNMS

Una vez seleccionado el software de monitoreo se diseñó la topología de red del sistema de monitoreo, procediéndose con la implementación del software de monitoreo OpenNMS Horizon en conformidad con las tareas establecidas en la EDT de la figura 10.

3.4.1 Implementación del Servidor

La instalación del software de monitoreo OpenNMS Horizon requiere la puesta en operación de un servidor para instalar en el un sistema operativo compatible con OpenNMS Horizon.

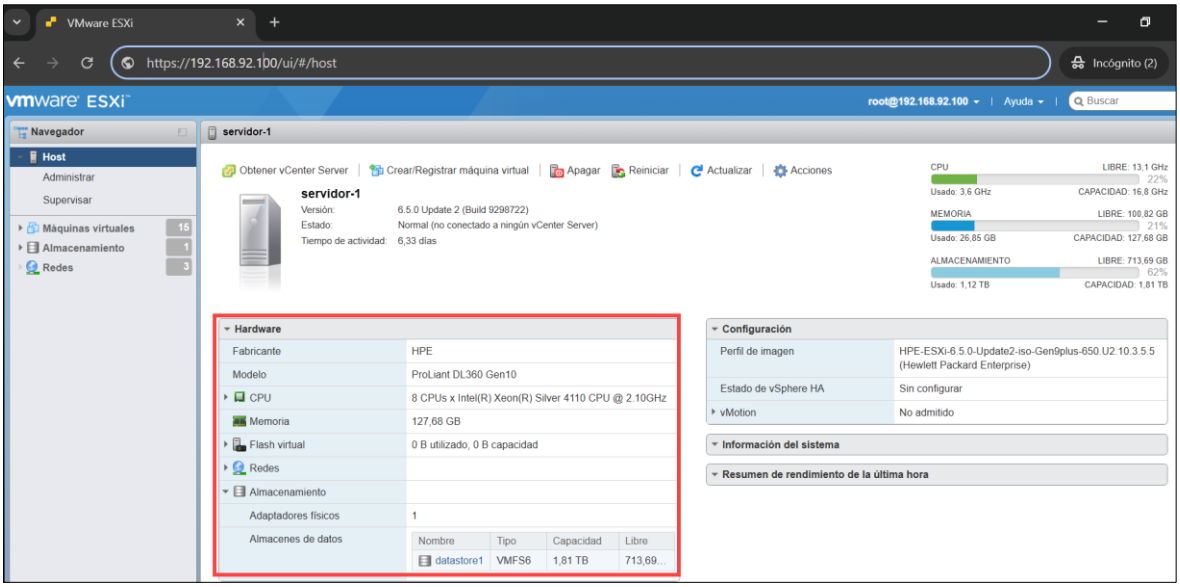
a) Requisitos del Servidor. El software OpenNMS Horizon para su correcta operación conforme al anexo 3, para tal fin, requiere una configuración mínima de hardware que reúna las siguientes especificaciones:

- CPU: 3GHz quad core x86_64 o superior
- RAM: 16 GB o superior
- Almacenamiento: 1TB con SSD o superior
- Sistema Operativo: Ubuntu 20.04 LTS o superior

El SOC de la Empresa de Telecomunicaciones debe contar con un servidor designado como servidor-1 con la configuración que se indica en el anexo 4 que supera la mínima configuración destinada a alojar a la máquina virtual del software OpenNMS Horizon. En la figura 14 se muestra la plataforma de virtualización VMware ESXi instalada en el servidor-1 indicando las especificaciones del servidor en el cual se gestionará la máquina virtual en la cual se instalará el sistema operativo Ubuntu 22.04 LTS y posteriormente el software OpenNMS Horizon.

Figura 14

Especificaciones de hardware del servidor servidor-1.

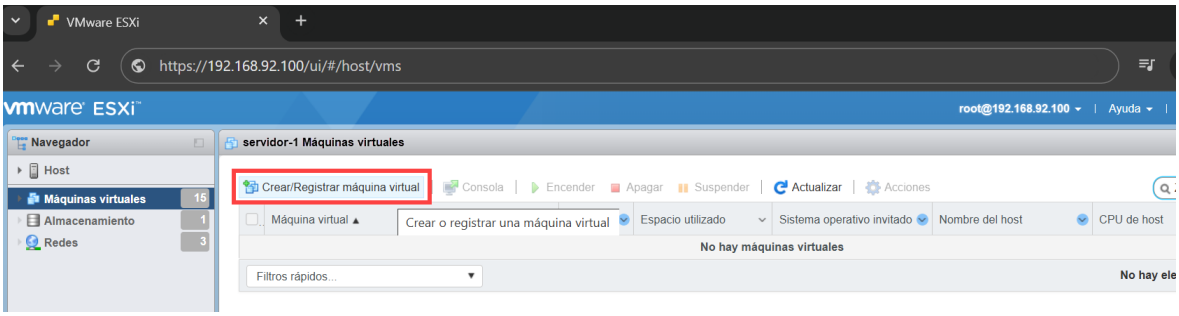


Nota: software de virtualización VMware.

b) Creación de la Máquina Virtual. En el menú de la plataforma de virtualización VMware del servidor-1 del SOC de la Empresa de Telecomunicaciones, de las Máquinas virtuales se seleccionó la opción "*Crear/Registrar máquina virtual"* tal como se indica en la figura 15, iniciando con ello la creación de la máquina virtual.

Figura 15

Selección de la opción de creación de una máquina virtual.

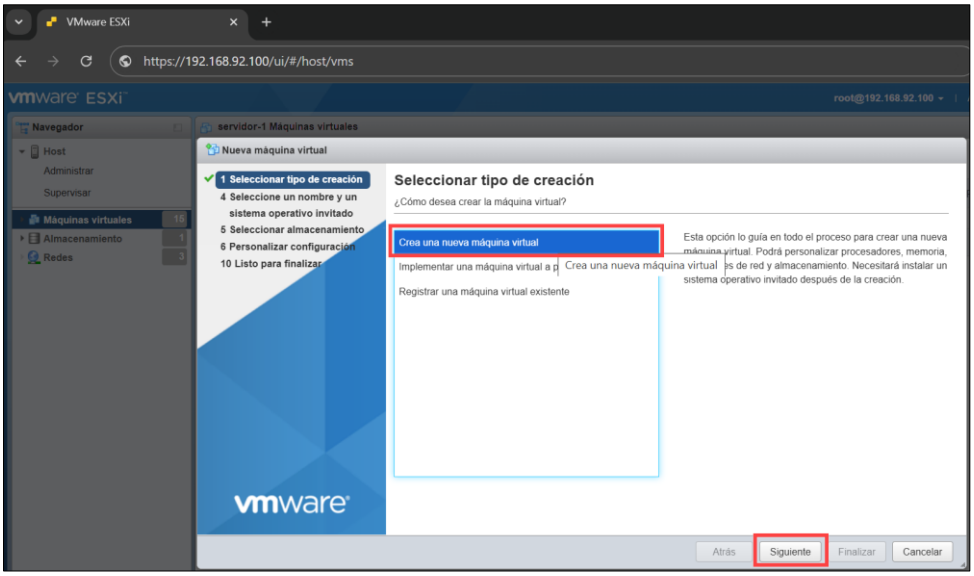


Nota: software de virtualización VMware.

En la ventana de Nueva máquina virtual en el tipo de creación se selecciona "*Crea una nueva máquina virtual*" haciendo clic en el botón Siguiente para proseguir con el proceso de creación de la máquina virtual, tal como, se indica en la figura 16.

Figura 16

Selección del tipo de creación de la maquina virtual.

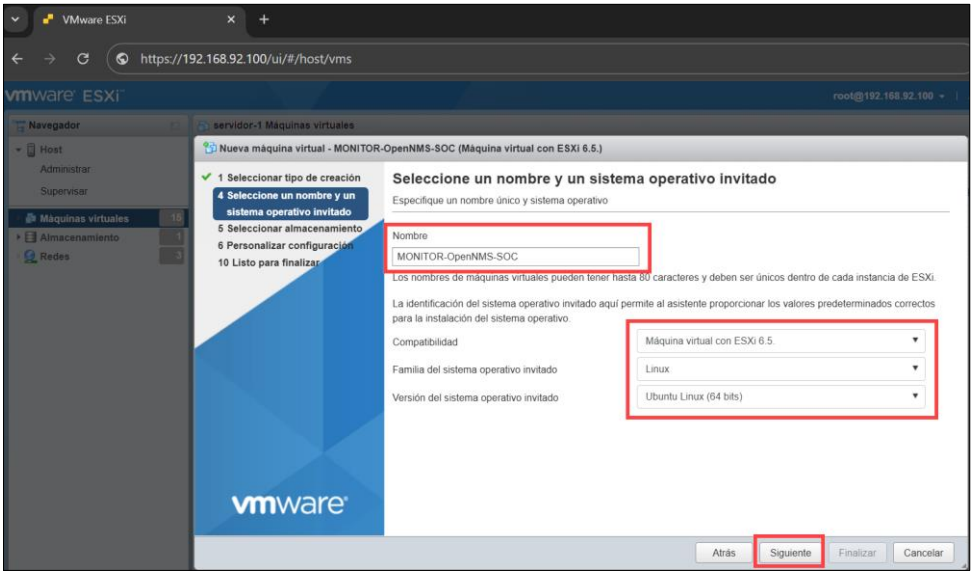


Nota: software de virtualización VMware.

Una vez elegido el tipo de creación, se agregó el nombre de la máquina virtual MONITOR-OpenNMS-SOC, seleccionándose el sistema operativo Ubuntu Linux (64 bits) a ser instalado, haciendo clic en el botón Siguiente para proseguir con el proceso de creación de la máquina virtual, tal como se indica en la figura 17.

Figura 17

Configuración del nombre y el sistema oprativo de la máquina virtual.

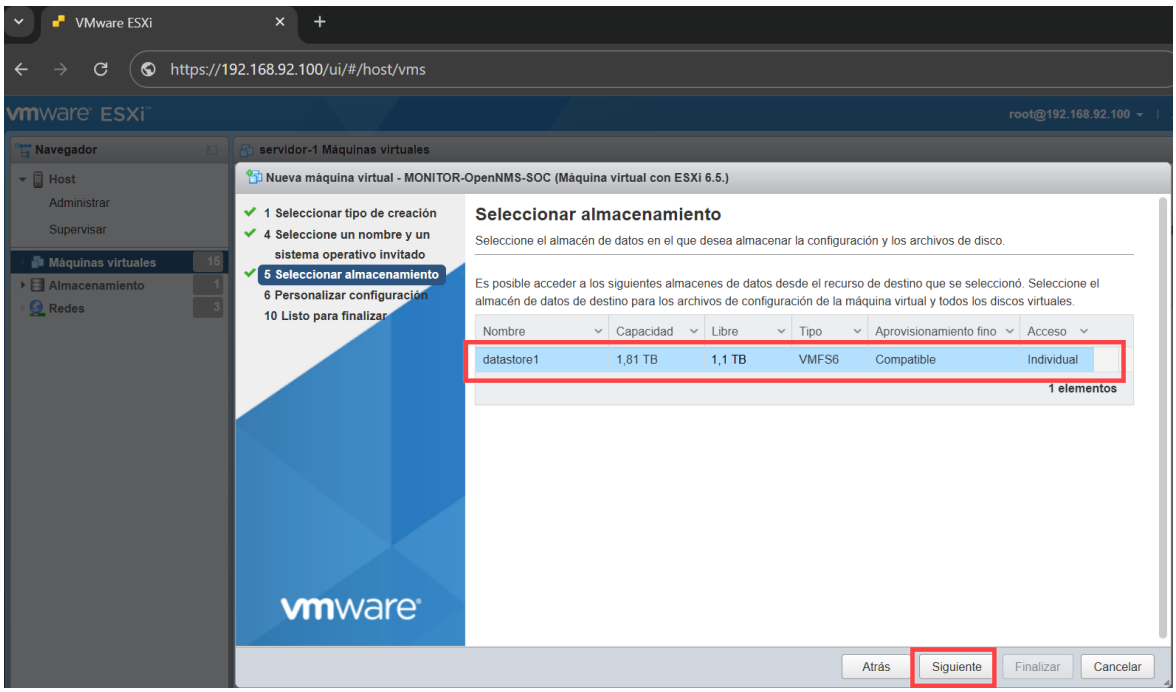


Nota: software de virtualización VMware.

Continuando con la creación, se seleccionó la unidad de almacenamiento de la máquina virtual la cual es el disco de almacenamiento del servidor-1 como se presenta en la figura 18, luego se hizo clic en el botón Siguiente para continuar con el proceso de creación.

Figura 18

Selección de la unidad de almacenamiento de la máquina virtual.

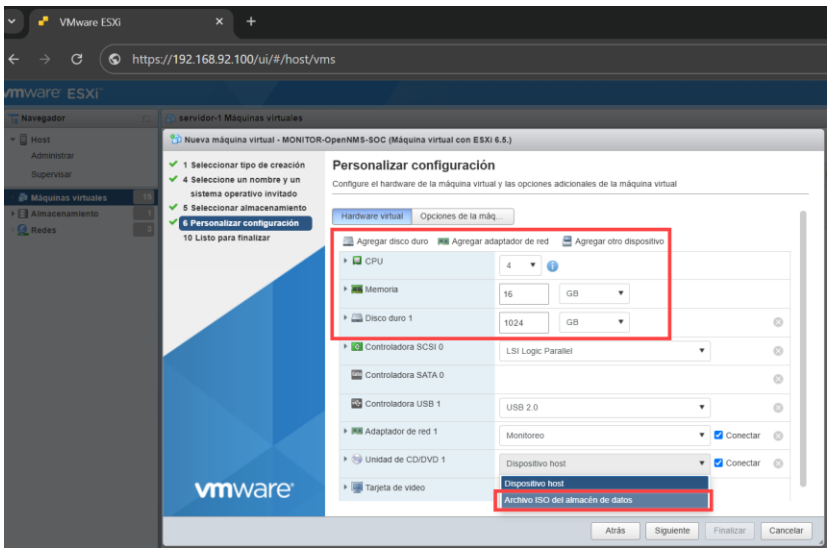


Nota: software de virtualización VMware.

Después de seleccionar el almacenamiento, se configuraron los parámetros de CPU de 4 núcleos, memoria RAM de capacidad 16 GB, tamaño del disco duro de 1024 GB seleccionándose la opción "*Archivo ISO del almacén de datos*" eligiendo un archivo de tipo ISO del almacén de datos del servidor-1, tal como, se muestra en la figura 19. Este archivo ISO es el instalador del sistema operativo.

Figura 19

Configuración del CPU, RAM y del disco duro de la máquina virtual.

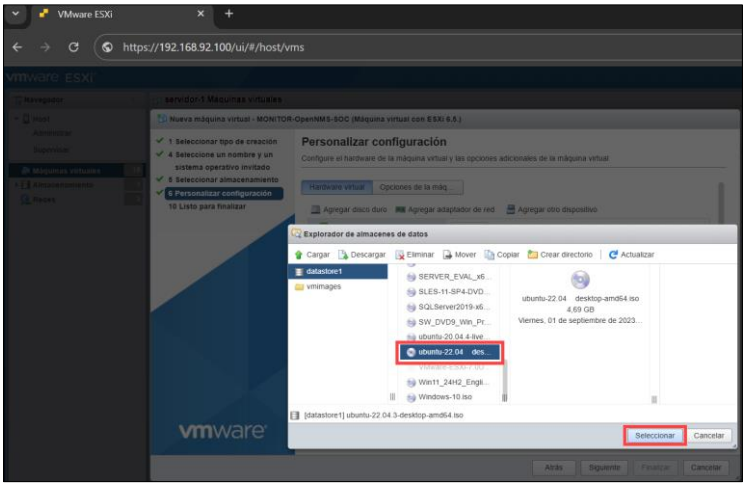


Nota: software de virtualización VMware.

Una vez seleccionada la opción "*Archivo ISO del almacén de datos*" se abre la ventana del Explorador de datos almacenados, tal como, se muestra en la figura 20, en la cual se selecciona el archivo ISO ubuntu-22.04.iso, el cual, es el instalador del sistema operativo de la máquina virtual, luego se hizo clic en el botón Seleccionar y seguidamente en el botón Finalizar para culminar con la creación de la máquina virtual MONITOR-OpenNMS-SOC.

Figura 20

Archivo de instalación del sistema operativo de la máquina virtual.

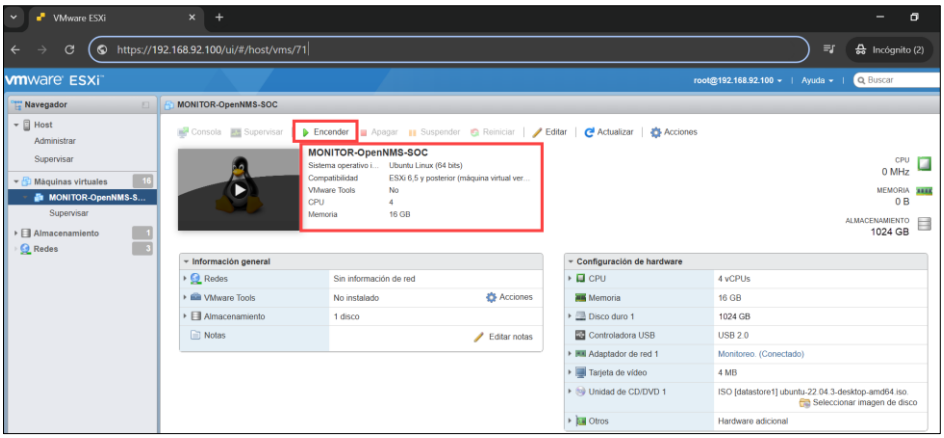


Nota: software de virtualización VMware.

Finalmente, en la plataforma del VMware, tal como, se indica en la figura 21 se comprobó que la creación de la máquina virtual fue efectuada correctamente conforme a los requerimientos de instalación mínimos del software OpenNMS Horizon, procediéndose a iniciar la operación de la máquina virtual haciendo clic en la opción Encender.

Figura 21

Verificación y encendido de la maquina virtual.

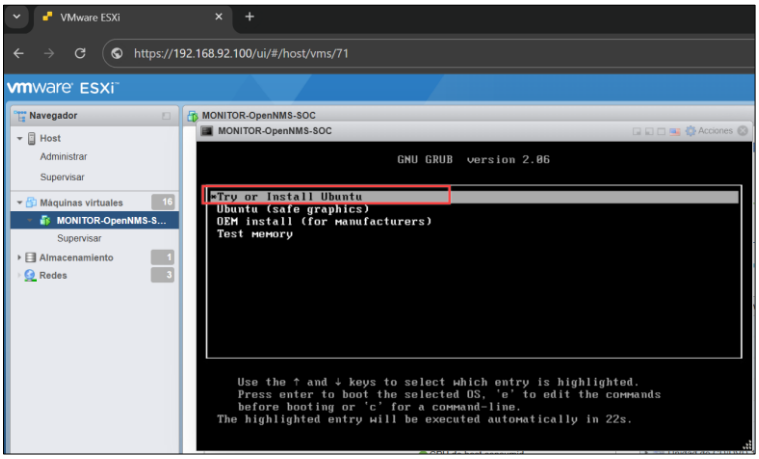


Nota: software de virtualización VMware.

c) Instalación del Sistema Operativo Ubuntu Server 22.04. Una vez iniciada la máquina virtual, se inicia automáticamente el proceso de instalación del sistema operativo Ubuntu 22.04, tal como, se muestra en la figura 22, en la ventana de instalación se seleccionó la opción "*Try or Install Ubuntu*" para iniciar la instalación de Ubuntu.

Figura 22

Ventana de inicio de la instalación de Ubuntu 22.04.

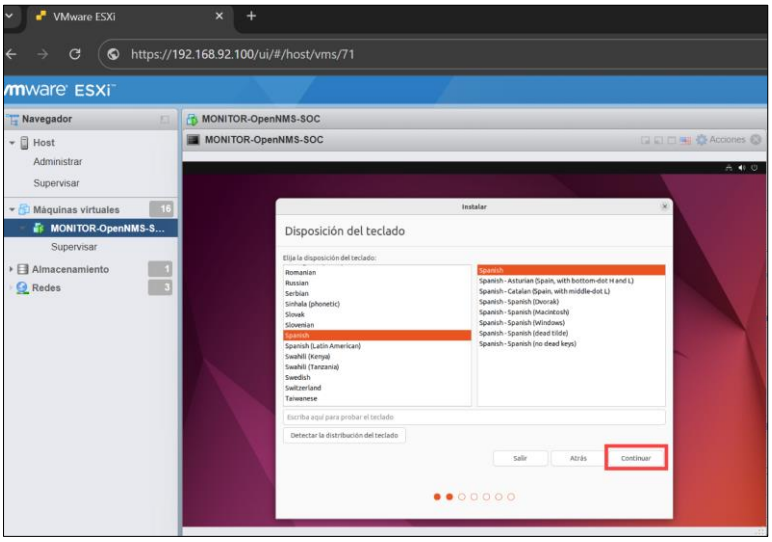


Nota: software de virtualización VMware.

Continuando con el proceso, se seleccionó el idioma de instalación del sistema operativo y la disposición del teclado, eligiéndose el idioma español, tal como, se indica en la figura 23, luego se hizo clic en el botón Continuar.

Figura 23

Selección del idioma del sistema operativo Ubuntu 22.04.

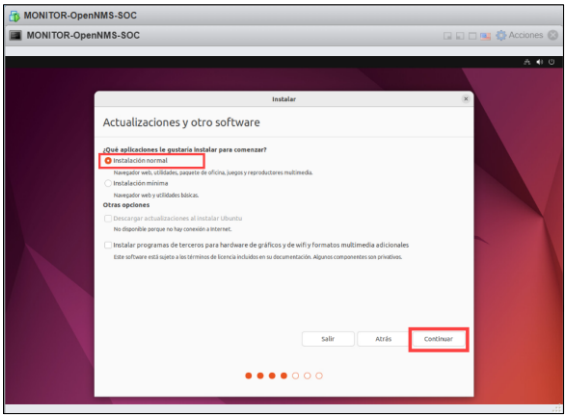


Nota: software de virtualización VMware.

En la ventana Actualizaciones y otro software se seleccionó la opción Instalación normal, tal como, se muestra en la figura 24, en esta opción se instalaron las aplicaciones necesarias para que el sistema operativo funcione correctamente, luego se hizo clic en el botón Continuar.

Figura 24

Tipo de instalación del sistema operativo Ubuntu 22.04.

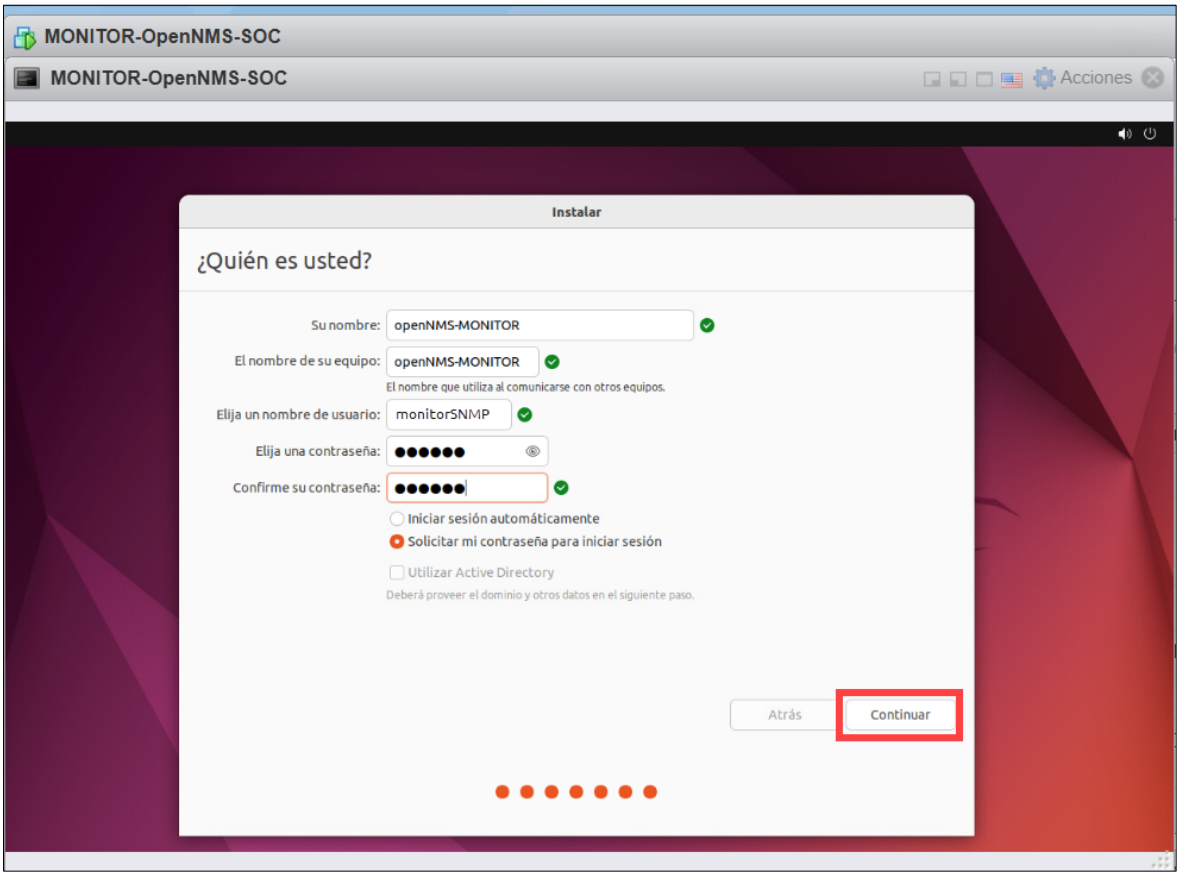


Nota: software de virtualización VMware.

En la ventana ¿Quién es usted? se configuró el nombre del equipo OpenNMS-MONITOR, el nombre de usuario monitorSNMP y una contraseña, tal como, se presenta en la figura 25, luego se hizo clic en el botón Continuar para proseguir con el proceso de instalación del sistema operativo Ubuntu, una vez, completada la instalación se seleccionó la opción Reiniciar ahora, para dar inicio a la operación del sistema operativo.

Figura 25

Configuración del usuario y nombre de equipo del sistema operativo Ubuntu.



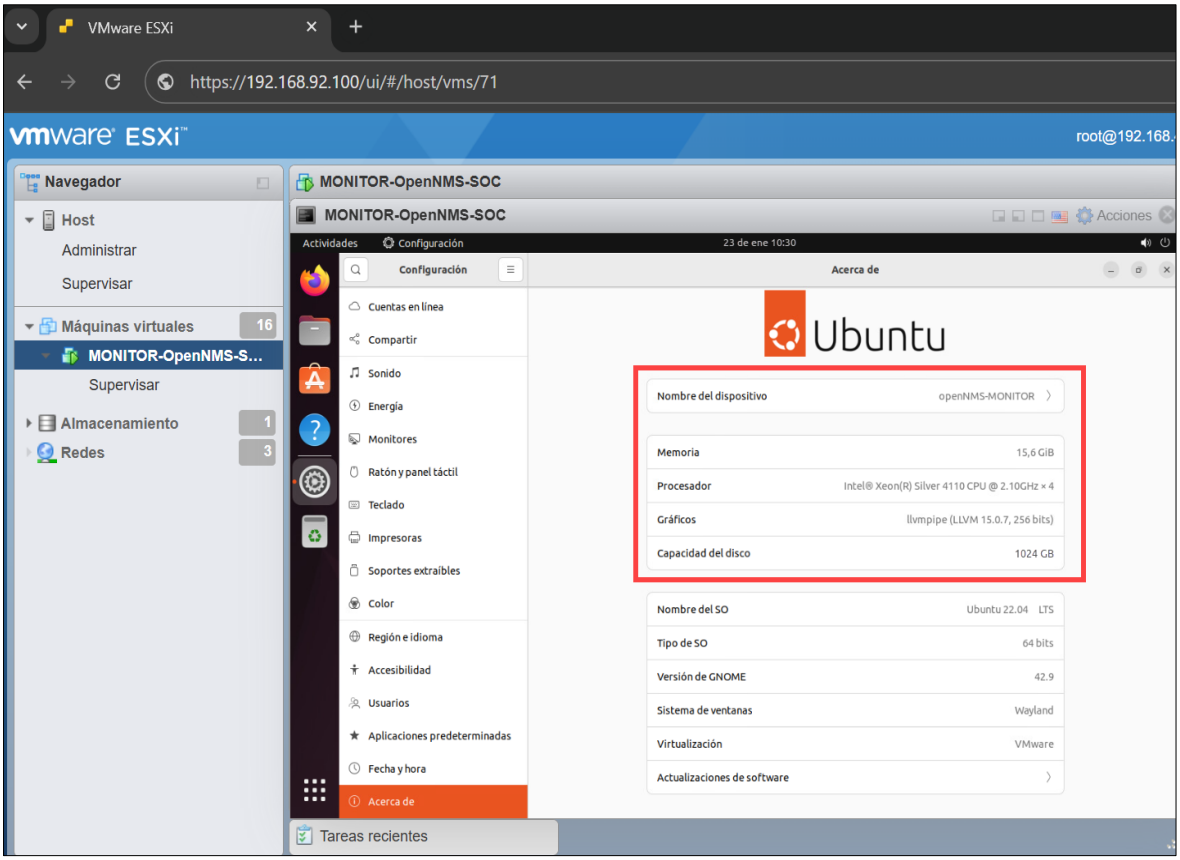
Nota: software de virtualización VMware.

Finalmente completada la instalación y reiniciada la máquina virtual, se accedió al sistema operativo Ubuntu 22.04, iniciando con la configuración de sistema operativo Ubuntu, verificándose los parámetros del sistema como procesador, memoria RAM, capacidad de almacenamiento, versión del sistema operativo y nombre del dispositivo, tal como, se indica en la figura 26, verificándose que estos parámetros sean los correctos y

satisfagan los requisitos mínimos de instalación del sistema de software de supervisión y monitoreó OpenNMS Horizon.

Figura 26

Parámetros del sistema operativo Ubuntu 22.04.



Nota: software de virtualización VMware.

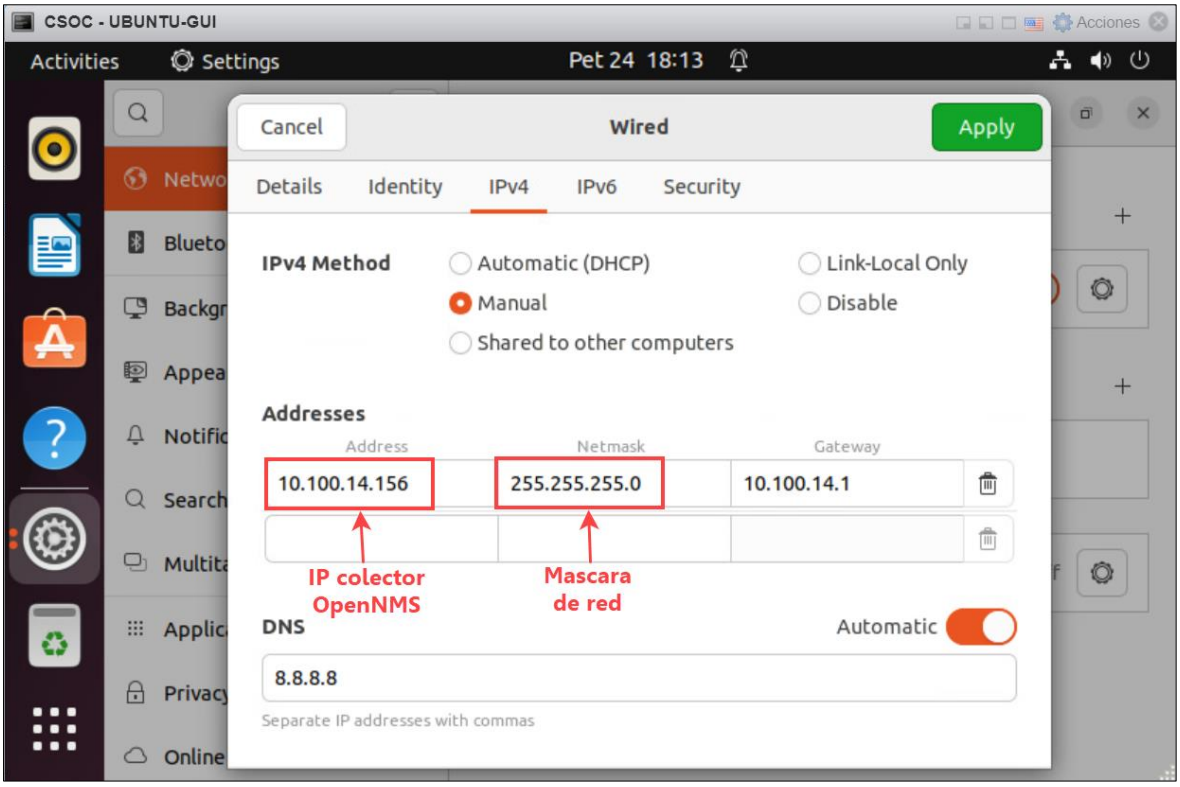
3.4.2 Configuración del Servidor Ubuntu 22.04

Con el propósito de instalar correctamente el software OpenNMS Horizon, se configuro al servidor Ubuntu 22.04 en sus diferentes prestaciones:

a) Configuración de IP Estática. Se configuró la IP: 10.100.14.156 con máscara de red 255.255.255.0 la cual pertenece al segmento de VRF de gestión de los nodos de seguridad perimetral – firewall del SOC de la empresa de telecomunicaciones, esta configuración se observa en la figura 27. Esta IP configurada es usada por el colector de logs SNMP del software OpenNMS Horizon.

Figura 27

Configuración de red en el servidor Ubuntu 22.04.

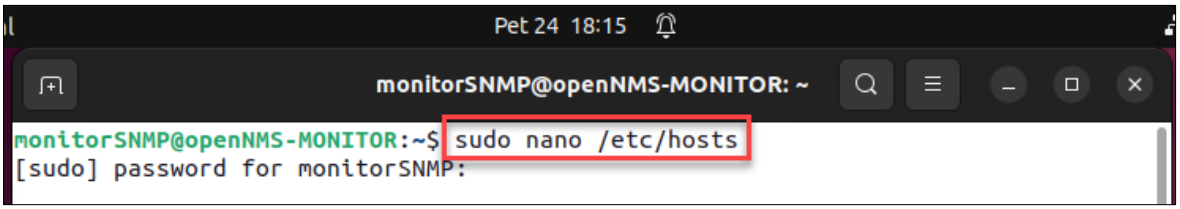


Nota: Sistema operativo Ubuntu 22.04.

b) Configuración del Nombre de Dominio. Se abrió el terminal de Ubuntu y se ejecutó el archivo de texto donde se relacionan las IP´s con los nombres de dominio, utilizando para ello el comando "*sudo nano /etc/hosts*" posteriormente se introdujo la contraseña de usuario/administrador como se observa en la figura 28.

Figura 28

Ejecución del archivo de sistema hosts.



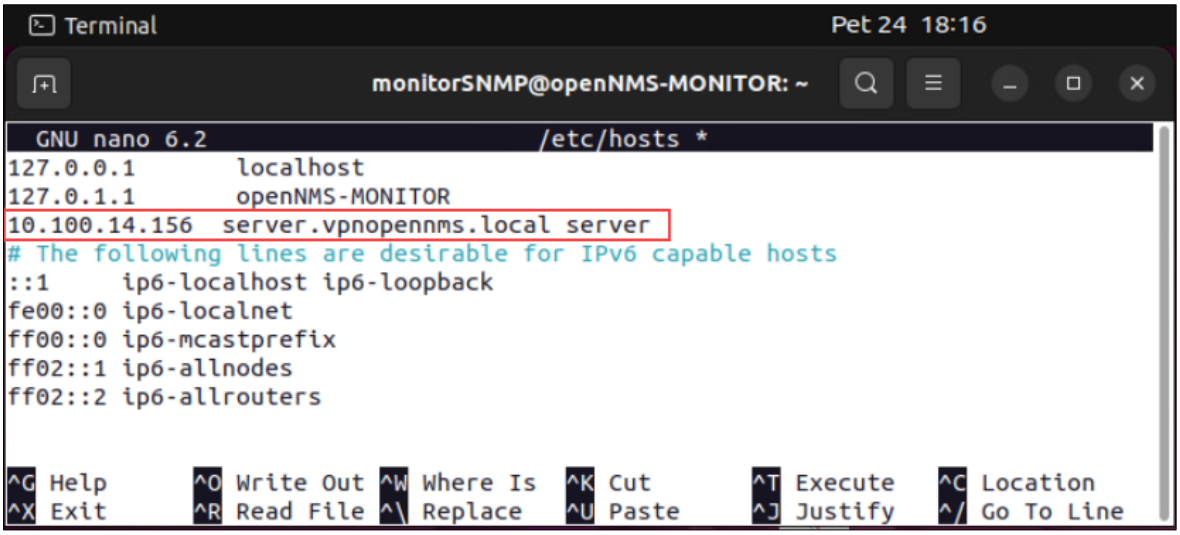
Nota: Terminal del sistema operativo Ubuntu 22.04.

Dentro del archivo de texto "*hosts*" se agregó la IP: 10.100.14.156 del colector del software OpenNMS relacionada con el nombre de dominio "server.*vpnopennms.local* " tal

como, se puede observar en la figura 29, guardandose el archivo con la combinación de teclas “*ctrl + o*”.

Figura 29

Nombre de dominio asociada a la IP del colector del software OpenNMS.

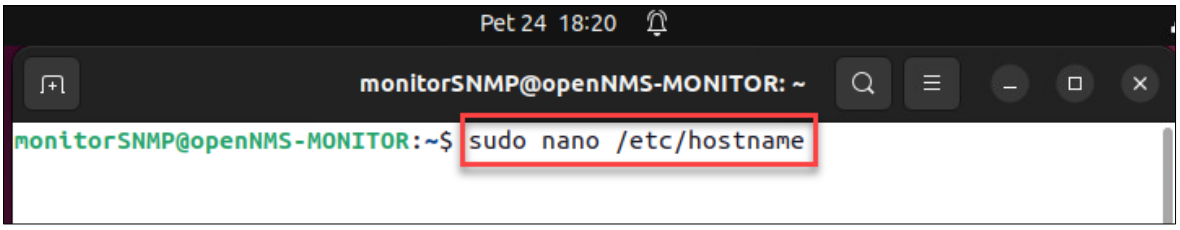


Nota: Terminal del sistema operativo Ubuntu 22.04.

c) Configuración del Hostname. En el terminal de Ubuntu se ejecutó el archivo de texto donde se encuentran los nombres del servidor, para tal fin, utilizamos el comando “*sudo nano /etc/hostname*” según la figura 30.

Figura 30

Ejecución del archivo de sistema hostname.

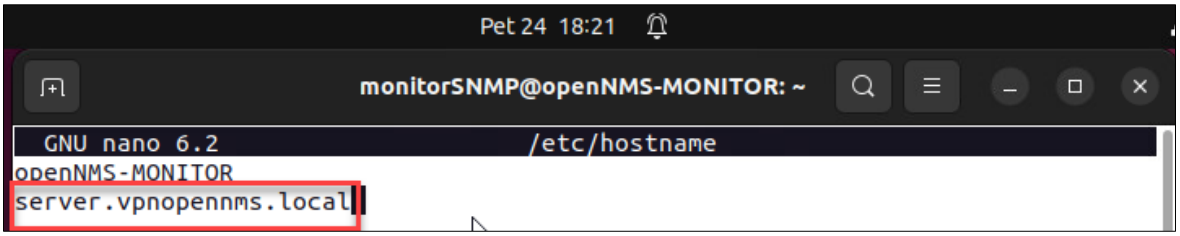


Nota: Terminal del sistema operativo Ubuntu 22.04.

Dentro del archivo de texto “*hostname*” se agregó la siguiente línea de código, “server.*vpnopennms.local* ” el cual es el nombre del servidor del software OpenNMS como puede observarse en la figura 31, guardandose el archivo con la combinación de teclas “*ctrl + o*”.

Figura 31

Nombre del servidor donde se aloja el colector del software OpenNMS.



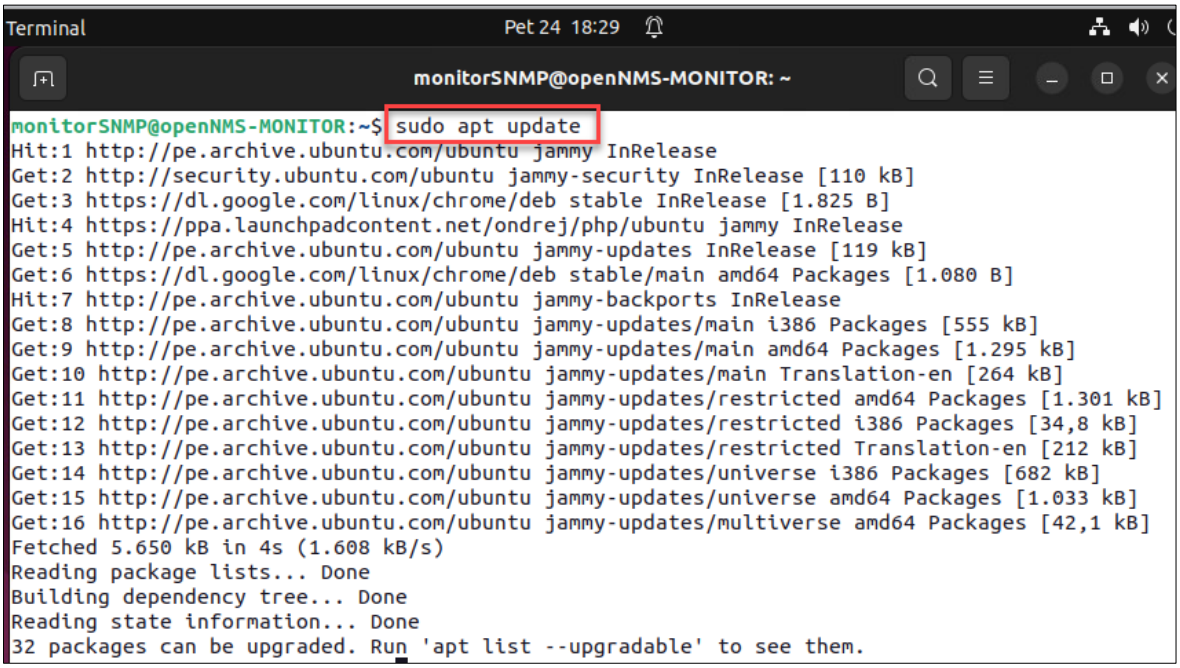
Nota: Terminal del sistema operativo Ubuntu 22.04.

d) Instalación de la Base de Datos Postgresql. Para el manejo de los datos el software OpenNMS necesita una base de datos relacional de código abierto, para ello se instaló la base de datos Postgresql.

En el terminal de Ubuntu se ejecutó el comando "*sudo apt update*" para actualizar todas las dependencias del sistema operativo Ubuntu como se puede observar en la figura 32.

Figura 32

Actualización de dependencias del sistema operativo Ubuntu.

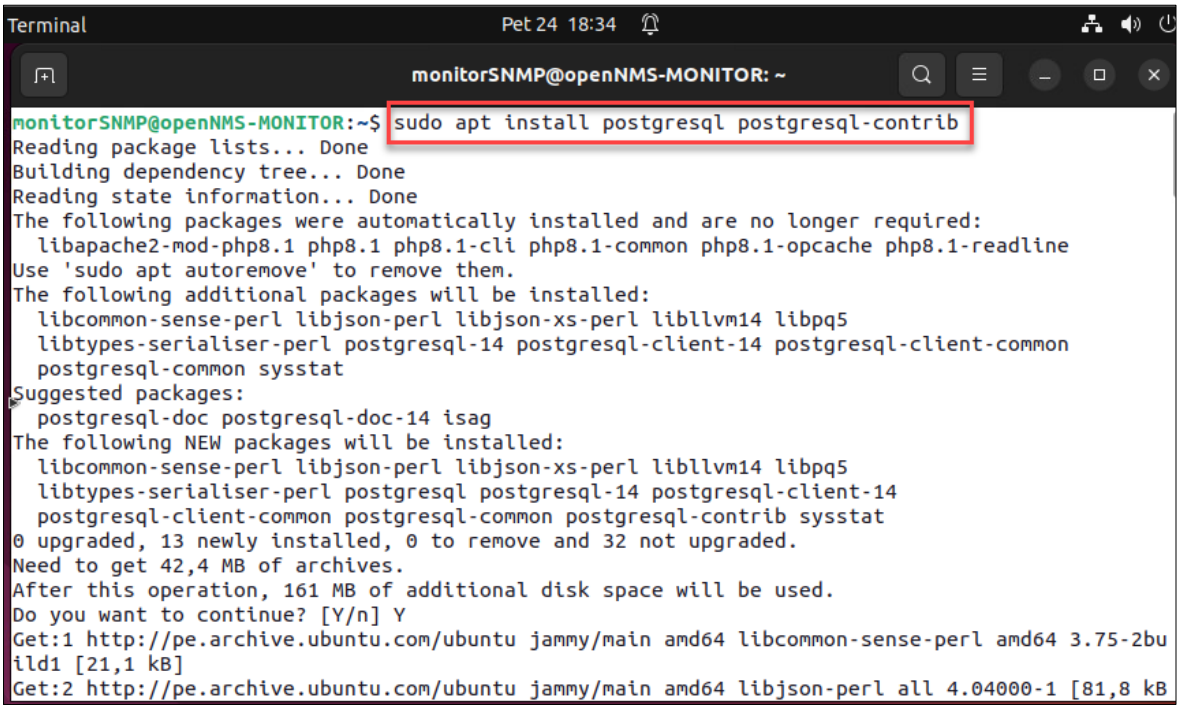


Nota: Terminal del sistema operativo Ubuntu 22.04.

Luego de la actualización de las dependencias, en el terminal de Ubuntu se ejecutó el comando "*sudo apt install postgresql postgresql-contrib*" para iniciar la instalación de la base de datos Postgresql según la figura 33.

Figura 33

Instalación de la base de datos Postgresql.

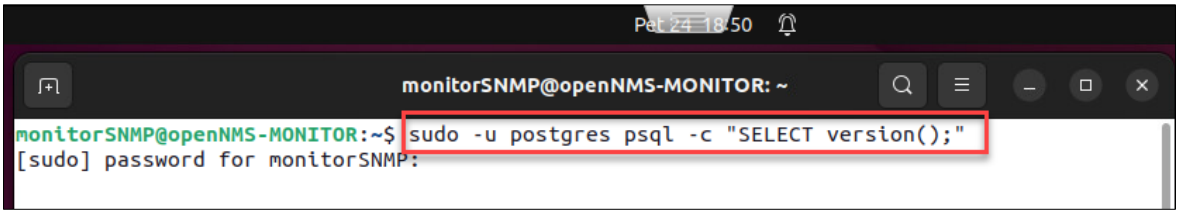


Nota: Terminal del sistema operativo Ubuntu 22.04.

Finalmente se comprobó que la versión 14.10 de la base de datos Postgresql se instaló correctamente, tal como, se puede observar en la figura 35, ejecutandose en el terminal de Ubuntu el comando "*sudo -u postgres psql -c "SELECT version();""* según la figura 34.

Figura 34

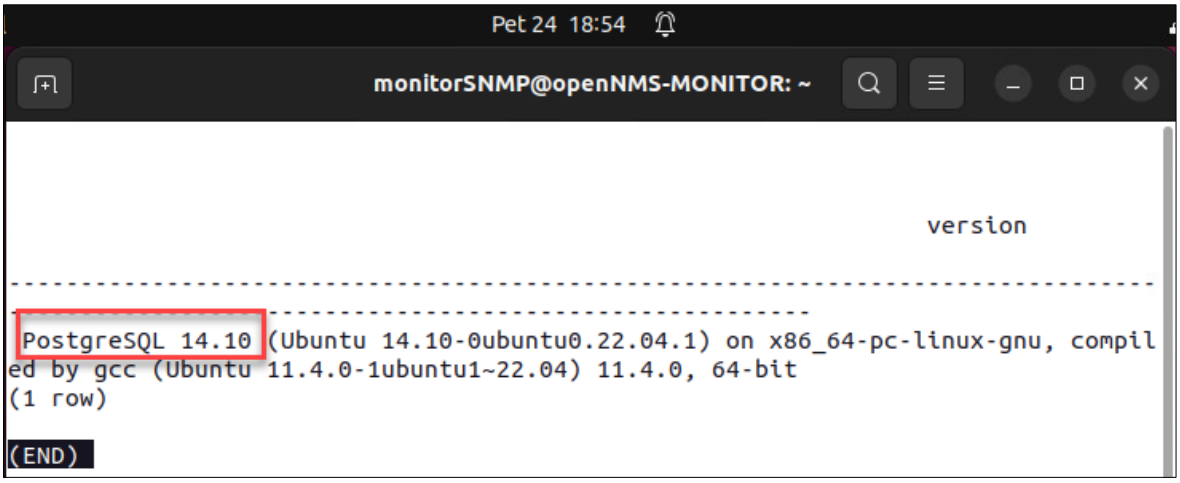
Comando que verifica la versión de la base de datos Postgresql.



Nota: Terminal del sistema operativo Ubuntu 22.04.

Figura 35

Verificación de la versión de la base de datos Postgresql.

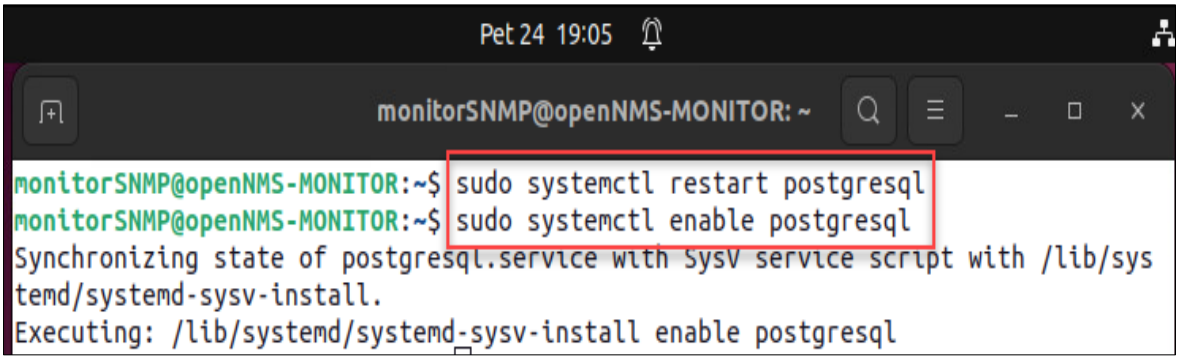


Nota: Terminal del sistema operativo Ubuntu 22.04.

e) Reinicio de la Base de Datos Postgresql. Para que la instalación se ejecute correctamente se reinició la base de datos Postgresql, para ello en el terminal de Ubuntu se ejecutaron los comandos de reinicio "*sudo systemctl restart postgresql*" y habilitación "*sudo systemctl enable postgresql*" como se observa en la figura 36.

Figura 36

Comandos para reinicio y habilitación de la base de datos Postgresql.

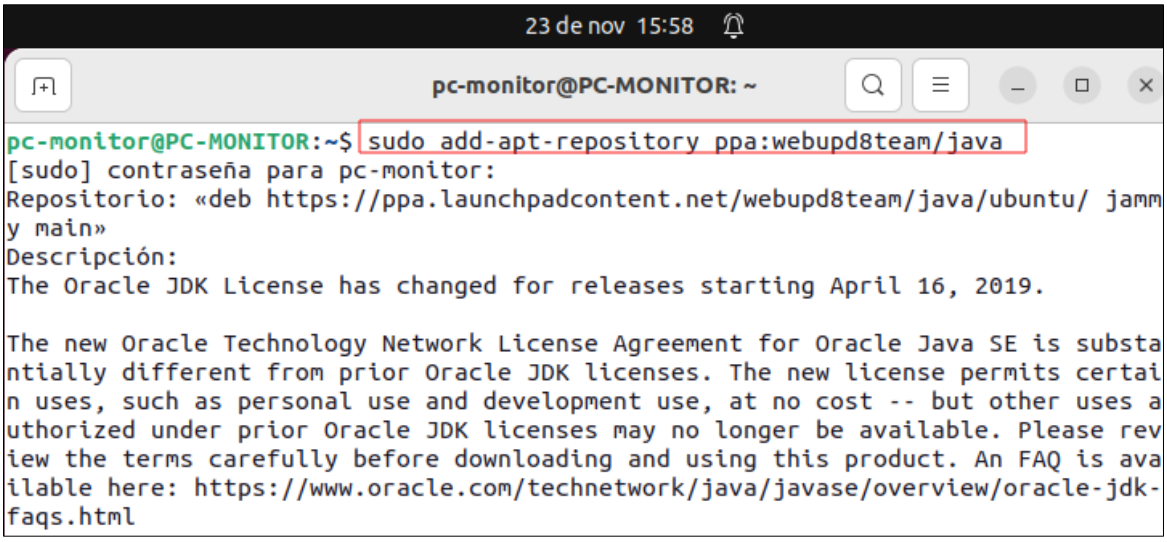


Nota: Terminal del sistema operativo Ubuntu 22.04.

f) Instalación de Java. En el terminal de Ubuntu se ejecutó el siguiente comando" *sudo add-apt-repository ppa:webupd8team/java*" para agregar en el repositorio de Ubuntu el PPA (Paquete de Archivo Personal) de Java como se indica en la figura 37.

Figura 37

Ejecución de comando para agregar el PPA de Java en el repositorio de Ubuntu.

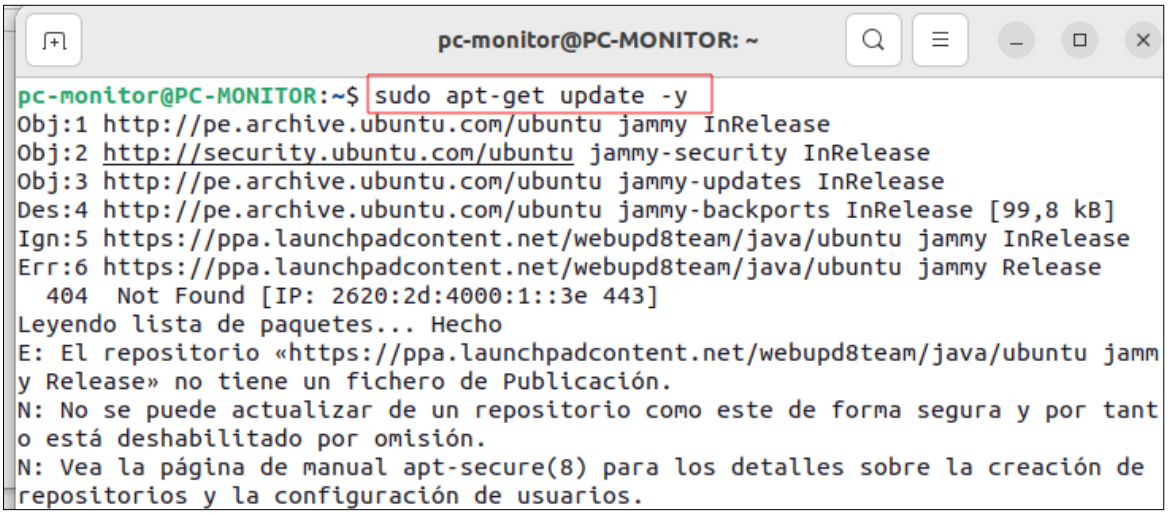


Nota: Terminal del sistema operativo Ubuntu 22.04.

Luego se procedió a actualizar los repositorios de Ubuntu, se ejecutó en el terminal el comando "*sudo apt-get update -y*" según la figura 38.

Figura 38

Actualización del repositorio de Ubuntu 22.04.

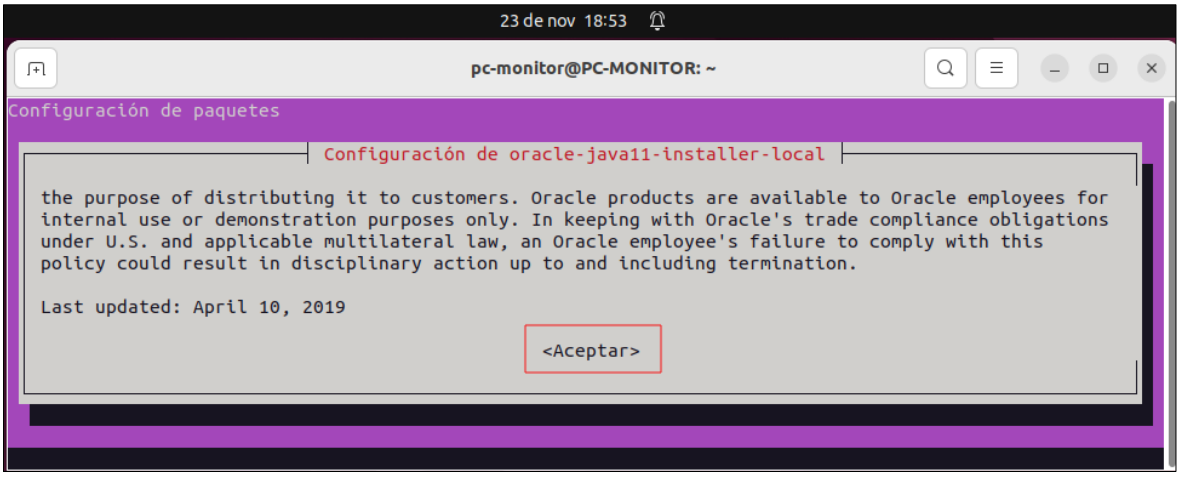


Nota: Terminal del sistema operativo Ubuntu 22.04.

Finalmente se instaló el PPA de Java para lo cual se ejecutó en el terminal el comando "*sudo apt-get install oracle-java7-installer -y*" se selecciona "Aceptar" como se observa la figura 39.

Figura 39

Instalación del paquete de Java 7.



Nota: Terminal del sistema operativo Ubuntu 22.04.

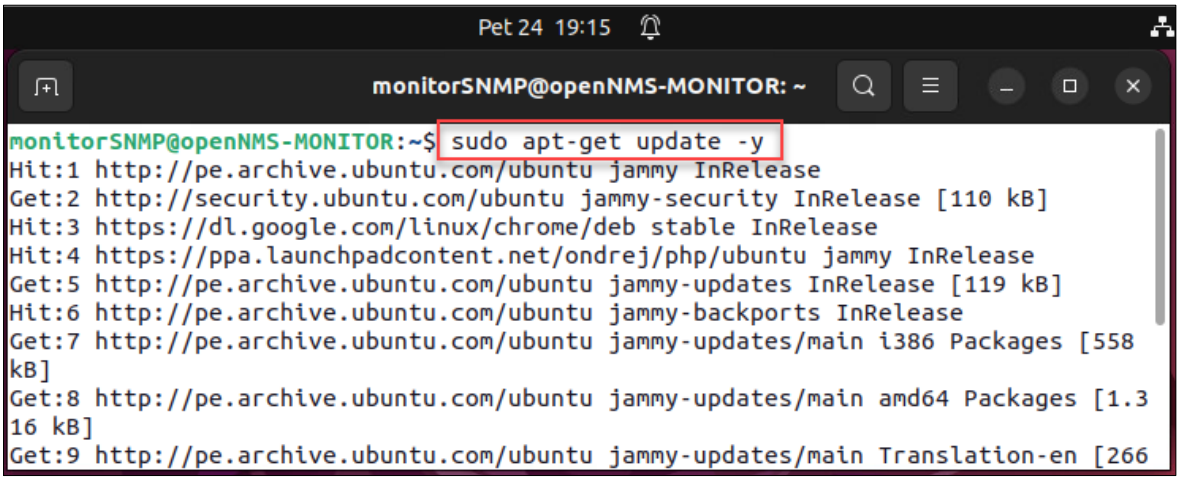
3.4.3 Instalación del Software OpenNMS HORIZON

Para llevar a cabo la instalación del software de monitoreo OpenNMS Horizon fueron ejecutados los procesos que se detallan a continuación.

a) Actualización del Servidor Ubuntu. En el terminal de Ubuntu se ejecutó el comando "*sudo apt-get update -y*" para actualizar todas las dependencias del sistema operativo Ubuntu como se puede observar en la figura 40.

Figura 40

Actualización de dependencias del sistema operativo Ubuntu 22.04.

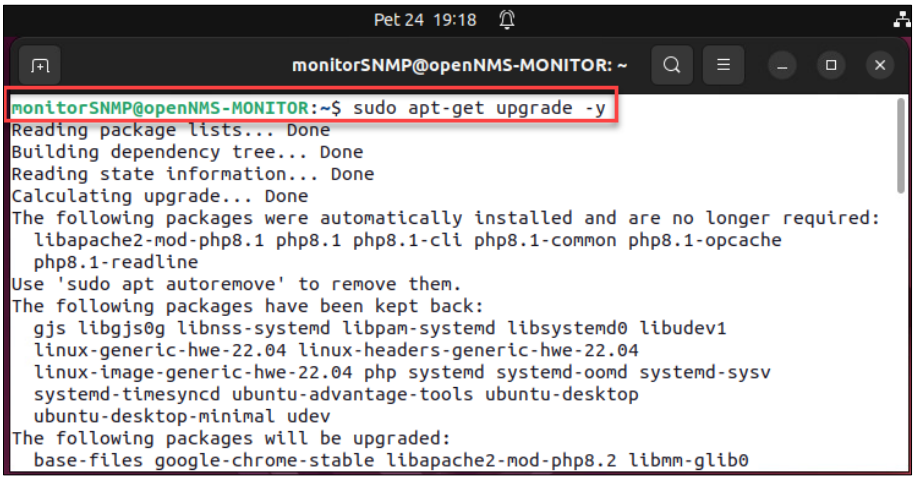


Nota: Terminal del sistema operativo Ubuntu 22.04.

Luego se realizó la actualización del sistema operativo Ubuntu de la versión 22.04 a la versión 22.04.1, para ello se ejecutó el comando "*sudo apt-get upgrade -y*" en el terminal de Ubuntu como se detalla en la figura 41.

Figura 41

Actualización del sistema operativo Ubuntu.

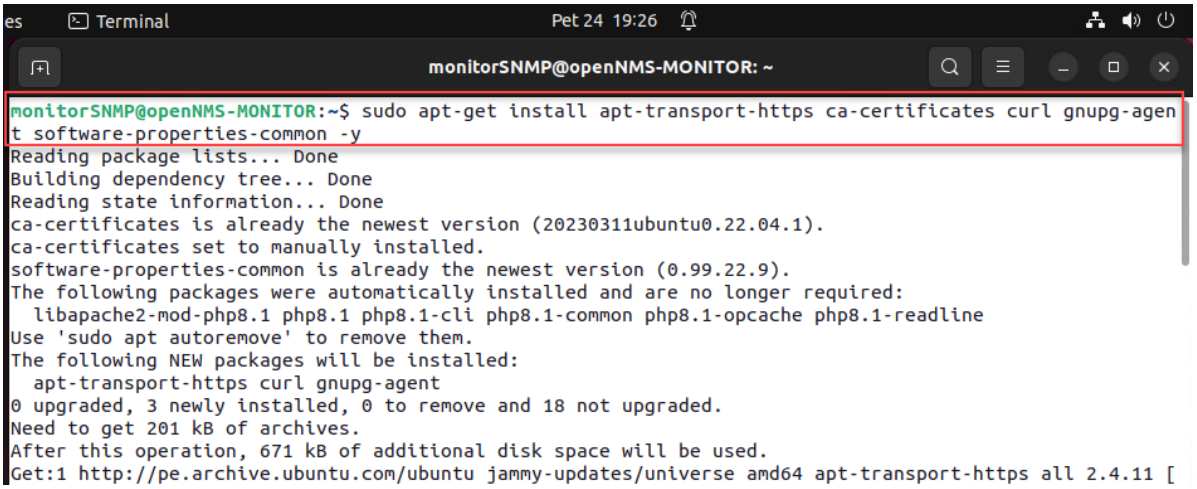


Nota: Terminal del sistema operativo Ubuntu 22.04.

Finalmente, se actualizaron algunas dependencias porque es necesaria la última versión de Ubuntu, según la figura 42 en el terminal de Ubuntu se ejecutó el comando "*sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common -y*" para ejecutar la actualización de dependencias.

Figura 42

Actualización de dependencias adicionales en Ubuntu 22.04.01.



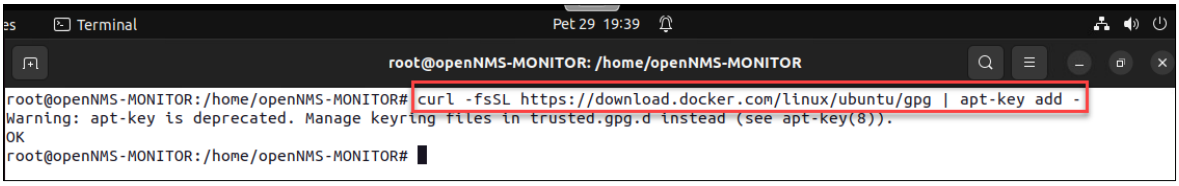
Nota: Terminal del sistema operativo Ubuntu 22.04.01.

b) Instalación de Docker Ubuntu Server. La instalación del software OpenNMS requiere una instalación previa de un organizador de contenedores que permita la ejecución del software OpenNMS a fin de disponer de todos los recursos, tal como, las herramientas de sistema y bibliotecas, por esta razón, se instaló el gestor de contenedores Docker, a continuación, se muestran los detalles del proceso de instalación de Docker.

- Adición de Repositorios de Docker. Se agregó una clave criptográfica GPG (GNU Privacy Guard) para descargar Docker desde su repositorio oficial, para ello se accedió como usuario root en el terminal de Ubuntu con el comando "*sudo su*", luego se ejecutó el comando "*curl -fsSL https://download.docker.com/linux/ubuntu/gpg | apt-key add -*" tal como, se muestra en la figura 43.

Figura 43

Adición de Clave Criptografica GPG de Docker.

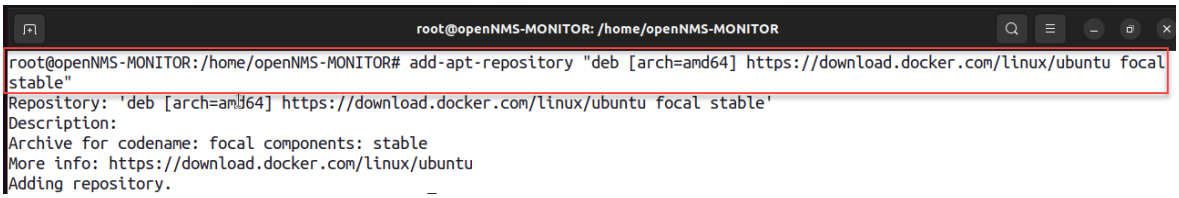


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

A continuación, como puede observarse en la figura 44 se agregó el repositorio de Docker a la lista de repositorios de Ubuntu, en el terminal se ejecutó el comando "*add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"* ".

Figura 44

Repositorio de Docker agregado a la lista de repositorios de Ubuntu.



Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Instalación de Docker y Docker Compose. Una vez actualizada la lista del repositorio de Ubuntu se instaló Docker, en el terminal de Ubuntu se ejecutó el comando " *sudo apt install docker-ce docker-compose -y* " con esto se dio inició al proceso de instalación, tal como, se ilustra en la figura 45.

Figura 45

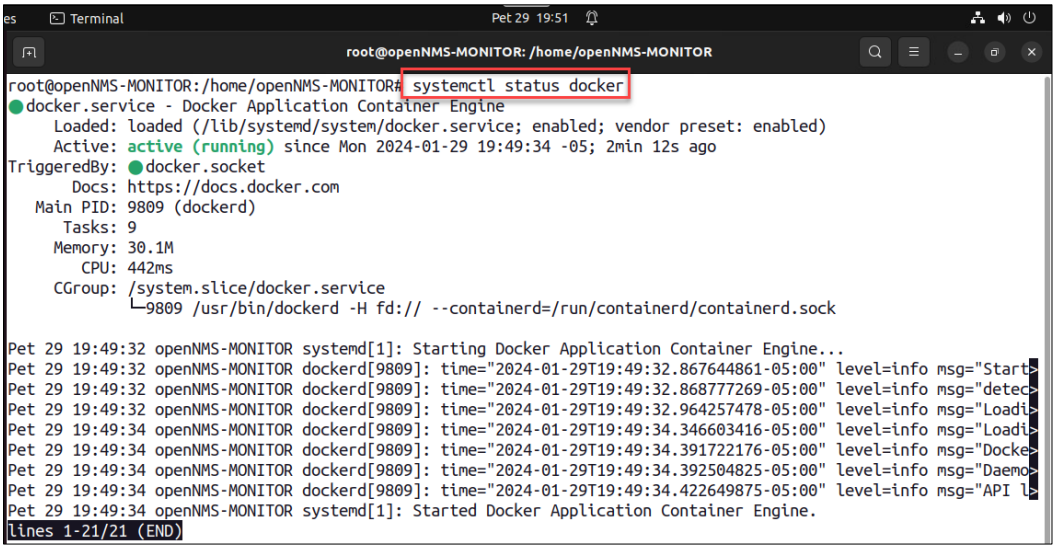
Ejecución de comando para iniciar la instalación de Docker.

Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Verificación del Estado de Docker. Finalizada la instalación de Docker y Docker Compose, lo cual, se verificó con la ejecución del comando " *systemctl status docker* " que Docker esta correctamente instalada con un estado de active (running), tal como, se ilustra en la figura 46.

Figura 46

Verificación del estado activo de Docker.



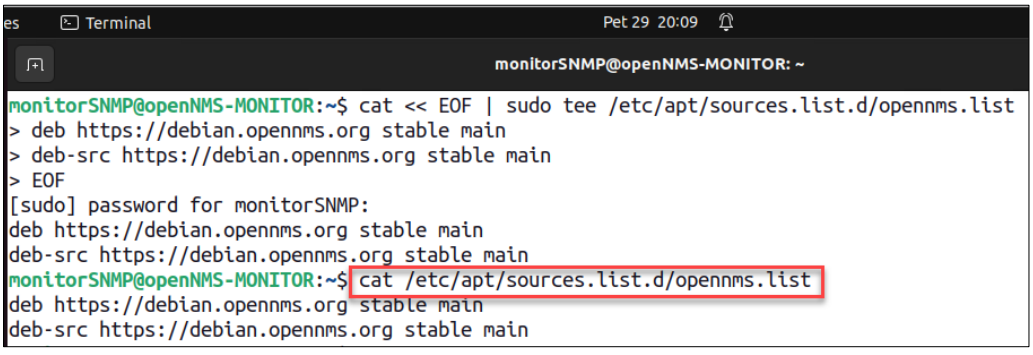
Nota: Terminal del sistema operativo Ubuntu 22.04.01.

c) Instalación del Software OpenNMS Horizon. Una vez culminada la instalación de Java y Docker se continuo con la instalación del software OpenNMS Horizon seguidamente, se detalla este proceso.

- Agregar Repositorios. En la figura 47 vemos que el repositorio de OpenNMS Horizon se agregó a la lista de repositorios de Ubuntu, ejecutando el comando " *cat << EOF | sudo tee /etc/apt/sources.list.d/opennms.list* " agregando los repositorios " > deb https://debian.opennms.org stable main " y "deb-src https://debian.opennms.org stable main ", ingresando finalmente la contraseña del usuario root.

Figura 47

Repositorio de OpenNMS Horizon agregado a los repositorios de Ubuntu.

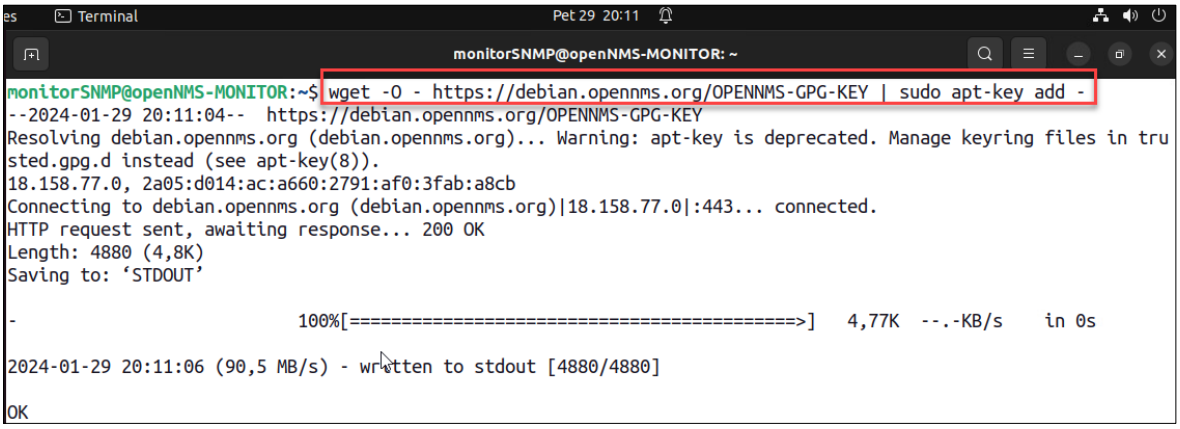


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Se agregó una clave criptográfica GPG (GNU Privacy Guard) para descargar OpenNMS desde su repositorio oficial, para ello se accedió como usuario root en el terminal de Ubuntu con el comando "*sudo su*", luego se ejecutó el comando "*wget -O - https://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -* " como se muestra en la figura 48.

Figura 48

Adición de clave Criptografica GPG de OpenNMS Horizon.

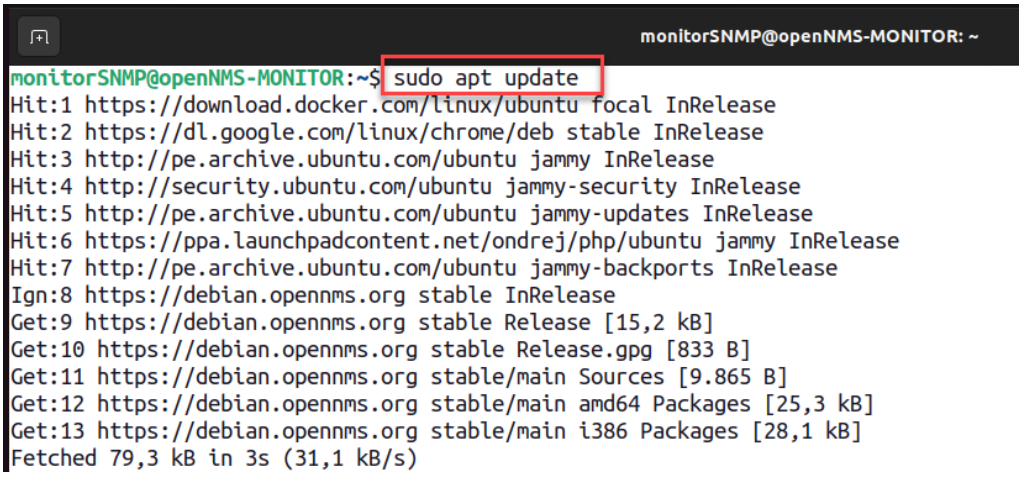


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

En el terminal de Ubuntu se ejecutó el comando "*sudo apt update* " para actualizar todas las dependencias del sistema operativo Ubuntu, tal como, puede observarse en la figura 49.

Figura 49

Actualización de dependencias en Ubuntu 22.04.01.



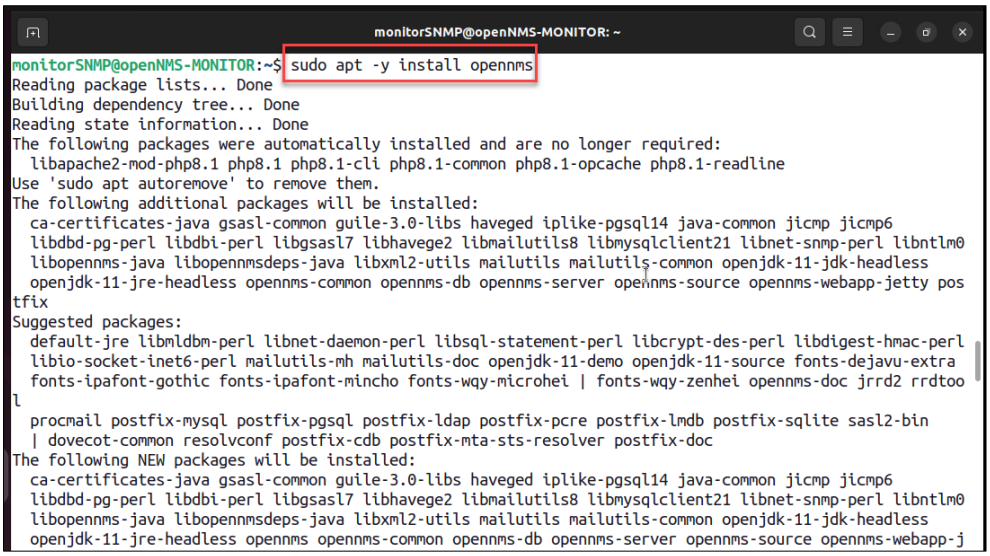
Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Instalación de OpenNMS Horizon con Todas las Dependencias Integradas.

Una vez actualizada la lista del repositorio de Ubuntu se instaló OpenNMS Horizon, en el terminal de Ubuntu se ejecutó el comando " *sudo apt -y install opennms* " dando inició al proceso de instalación, tal como, se ilustra en la figura 50.

Figura 50

Ejecución del comando que da inicio a la instalación de OpenNMS Horizon.

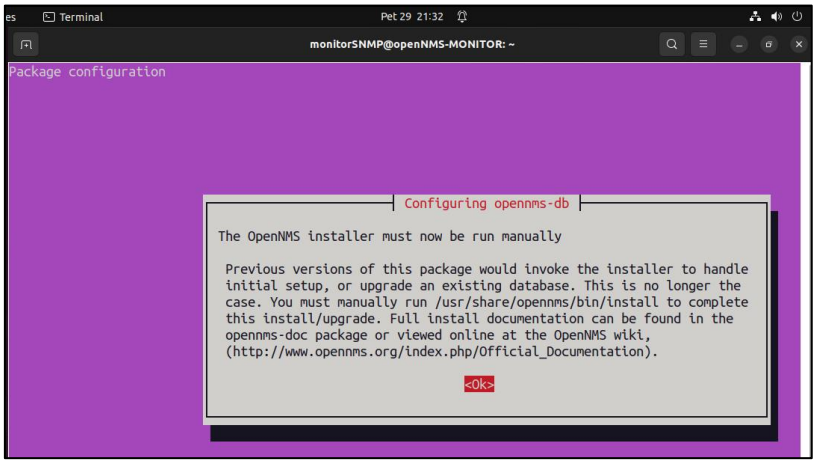


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Luego se seleccionó "OK" para finalizar la instalación de OpenNMS Horizon, tal como, se indica en la figura 51.

Figura 51

Finalización de la instalación de OpenNMS Horizon.

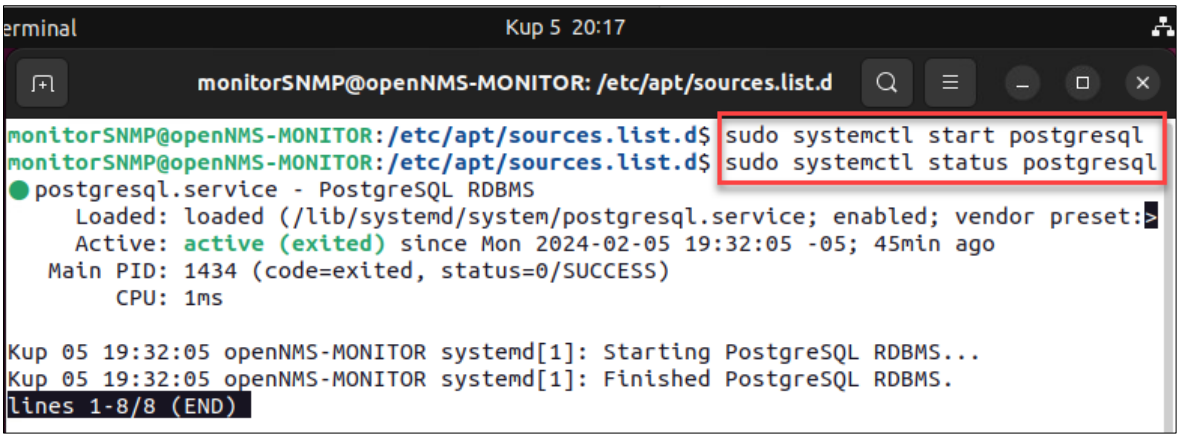


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Inicialización y Configuración de PostgreSQL. Se inició y verificó el estado de la base de datos Postgresql como se indica en la figura 52, para ello se ejecutó en el terminal de Ubuntu los comandos “sudo *systemctl start postgresql* ” y “ *sudo systemctl status postgresql* ” se verificó el estado active.

Figura 52

Inició de la base de datos Postgresql.

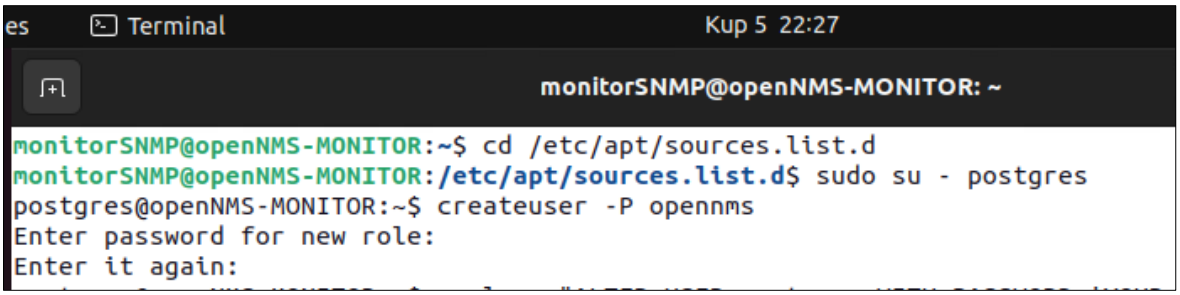


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Seguidamente se creó un usuario para la base de datos OpenNMS, tal como, se muestra en la figura 53, en el terminal de Ubuntu se ejecutaron los comandos “ *cd /etc/apt/sources.list.d/* ”,” *sudo su – postgres* ” y “ *createuser -P opennms* ” el cual contiene el nombre de usuario “ opennm ” finalmente se introdujo la contraseña elegida por el administrador.

Figura 53

Creación de usuario para la base de datos.

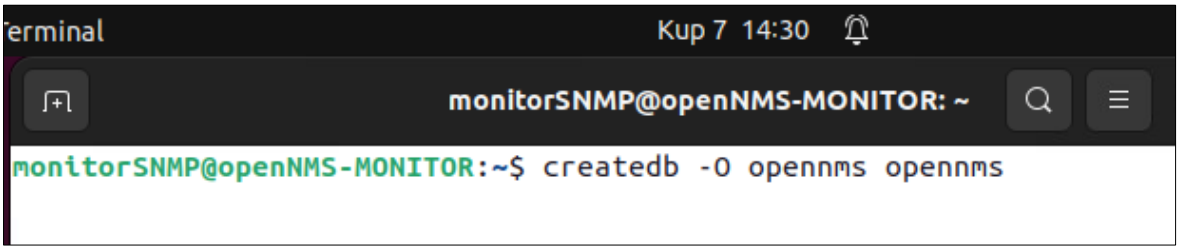


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Seguidamente, se creó una base de datos llamada “*opennms*” para el usuario “*opennms*”, para tal fin, en el terminal de Ubuntu se ejecutó el comando “createdb -0 opennms opennms”, como se muestra en la figura 54.

Figura 54

Creación de la base de datos.

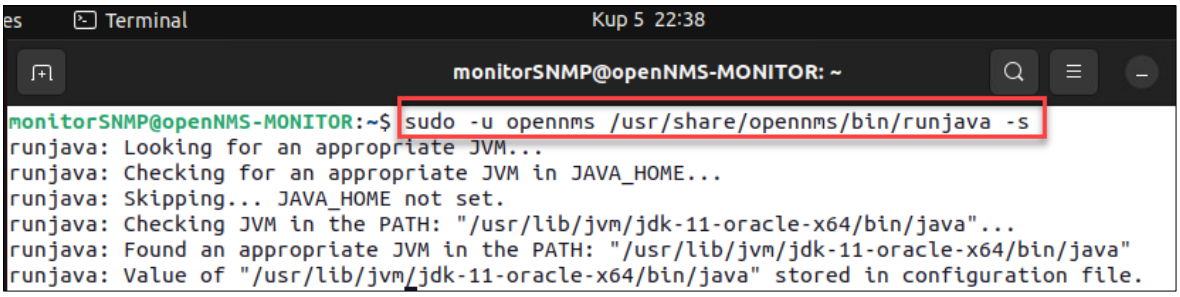


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Inicialización de OpenNMS Horizon. Antes de iniciar OpenNMS Horizon se detectó el entorno Java como se presenta en la figura 55, en el terminal de Ubuntu se ejecutó el comando “*sudo -u opennms /usr/share/opennms/bin/runjava -s*” para la realización de esta detección.

Figura 55

Detección del entorno Java.

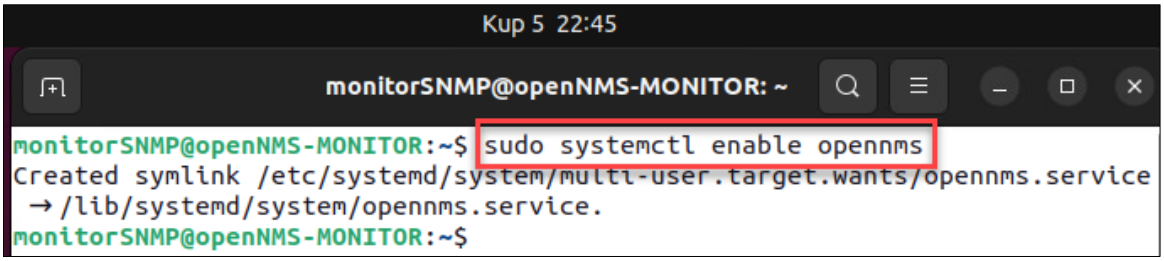


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Luego se configuró para que OpenNMS Horizon se inicie cuando arranque el sistema operativo del servidor Ubuntu, tal como, se visualiza en la figura 56, en el terminal de Ubuntu, se ejecutó el comando “sudo systemctl enable opennms ” en modo root para realizar esta configuración.

Figura 56

Configuración de inicio de OpenNMS Horizon.

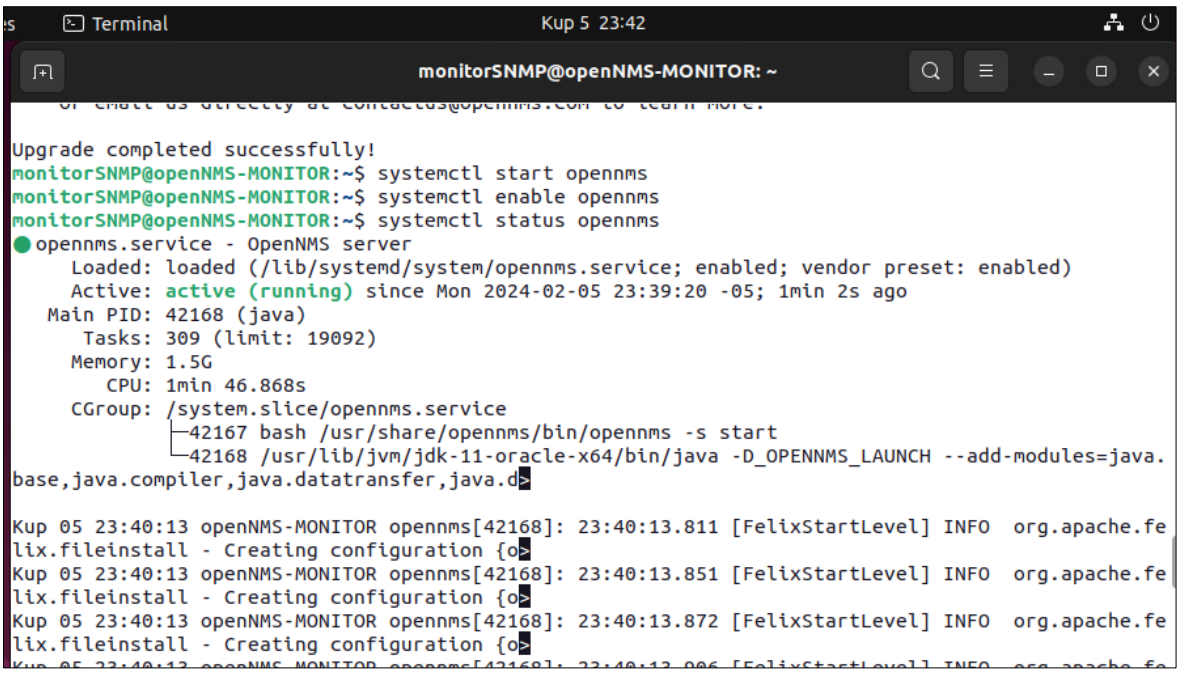


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Finalmente, como se indica en la figura 57 en el terminal de Ubuntu se ejecutan los comandos "*sudo systemctl start opennms*" y "*sudo systemctl status opennms*" para iniciar OpenNMS y verificar que se encuentra en el estado active.

Figura 57

Inicio de OpenNMS y verificación de su estado.

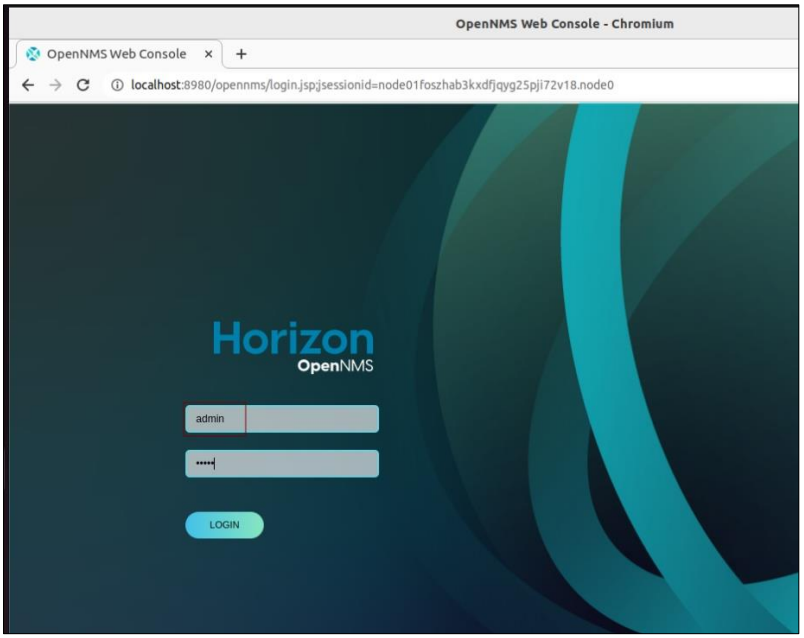


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

- Inicio de Sesión en la Plataforma OpenNMS Horizon. Inicializado el software se ingresó a la plataforma OpenNMS Horizon, como se puede visualizar en la figura 58, en el navegador de internet del servidor Ubuntu se introdujo el comando url "*http://127.0.0.1:8980/opennms/login.jsp*" para ingresar las credenciales del usuario admin.

Figura 58

Acceso a la plataforma OpenNMS Horizon.

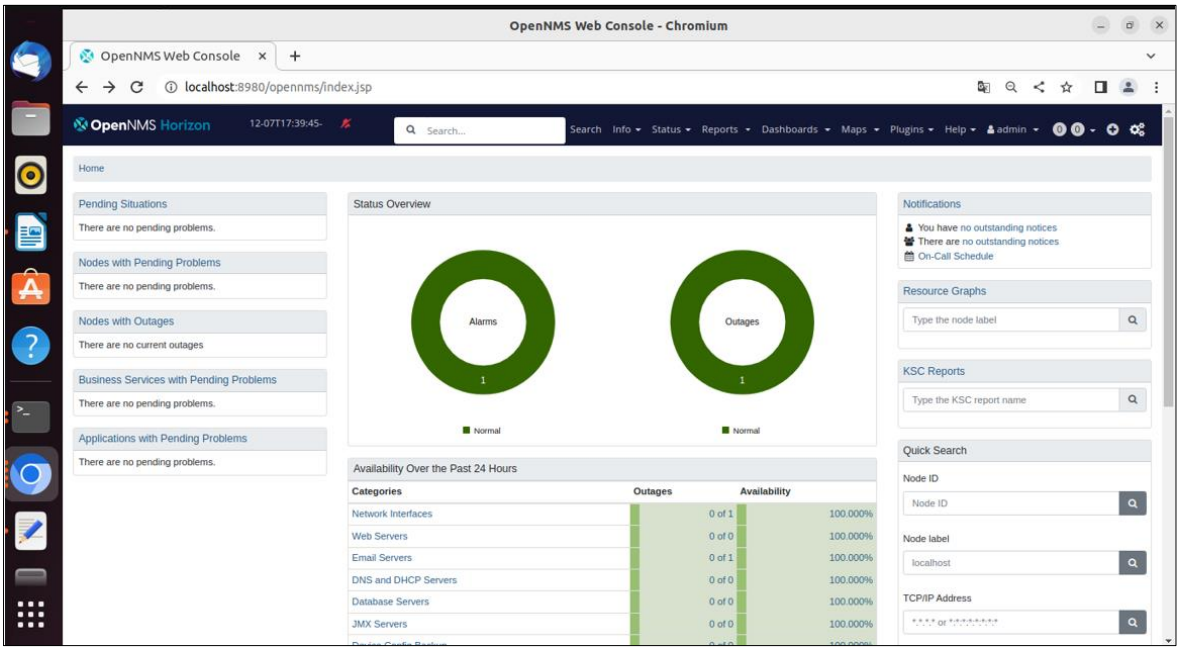


Nota: plataforma OpenNMS Horizon.

Seguidamente, en la figura 59 se muestra el dashboard de la plataforma OpenNMS Horizon.

Figura 59

Dashboard plataforma OpenNMS Horizon.



Nota: plataforma OpenNMS Horizon.

3.5 Configuración del Software de Monitoreo OpenNMS Horizon

Culminada la instalación del software OpenNMS Horizon, se configuraron las vistas de vigilancia, habilitación del protocolo SNMP, el incremento de nodos a la plataforma de OpenNMS y la configuración de alertas.

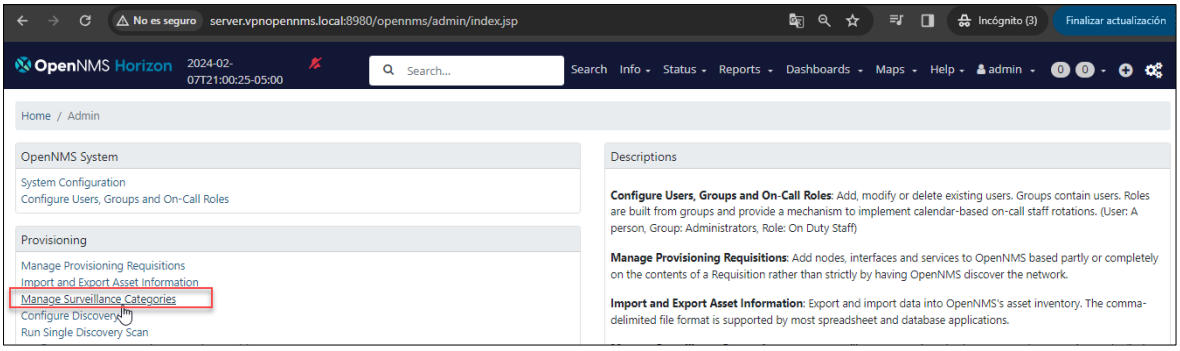
3.5.1 Configuración de Vistas de Vigilancia

Seguidamente, se muestran los detalles de configuración de la vista de vigilancia en el dashboard de la plataforma de OpenNMS Horizon, esta vista permite categorizar, organizar y tener una mejor visualización de los dispositivos de seguridad perimetral - firewall.

a) Configuración de las Categorías. Se accede a la sección de configuraciones de la plataforma OpenNMS, en el apartado "*Manage Surveillance Categories*" tal como, se indica en la figura 60.

Figura 60

Sección de administracion de vistas de vigilancia.

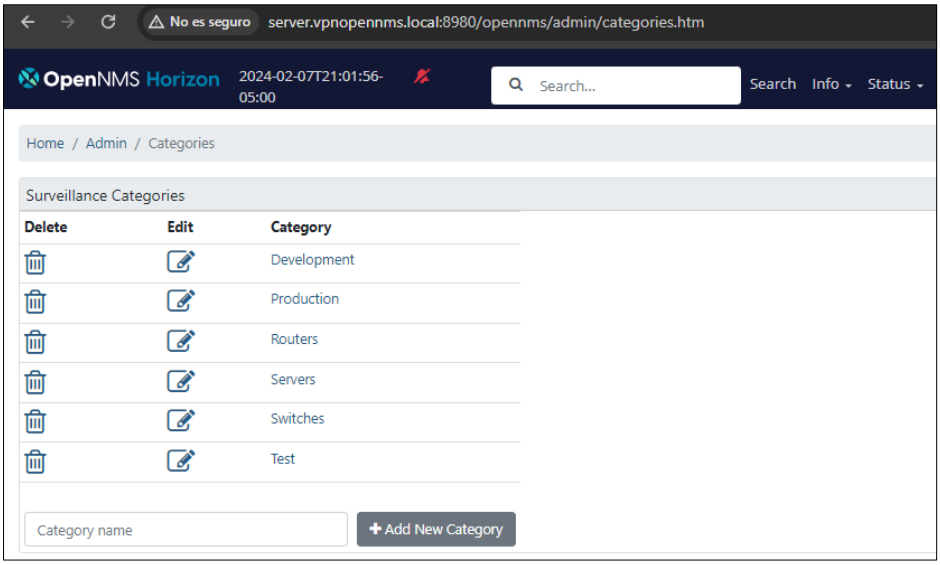


Nota: plataforma OpenNMS Horizon.

Luego se realizó la eliminación de todas las categorías que estaban por defecto, para este fin se hizo clic en los iconos de eliminación según la figura 61.

Figura 61

Eliminación de categorias por defecto.

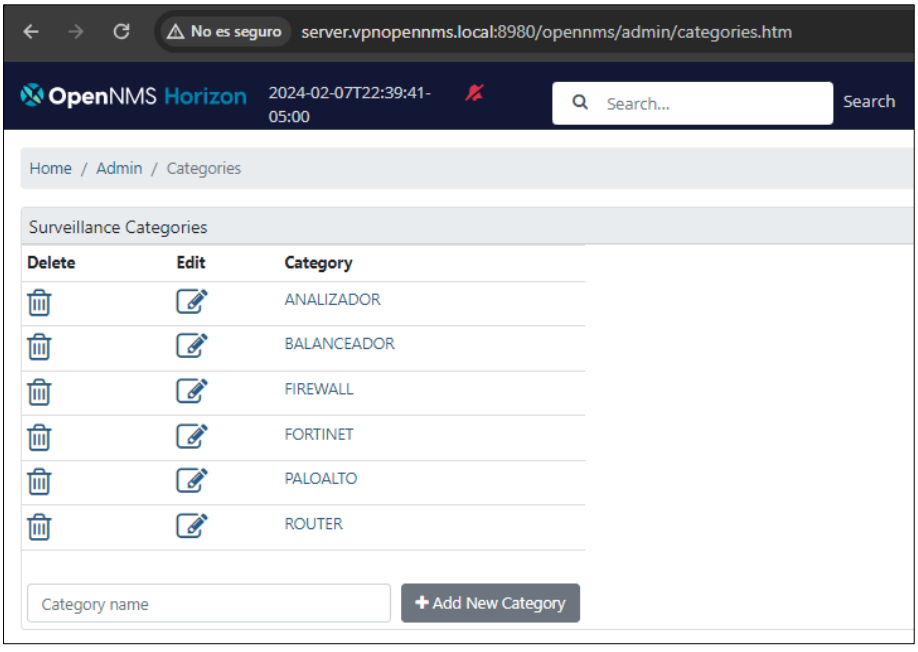


Nota: plataforma OpenNMS Horizon.

Se eliminaron las categorías por defecto, en su lugar se introdujeron los nombres de las nuevas categorías segun el tipo de dispositivo, tal como, se observa en la figura 62 seleccionándose "*Add New Category* " para guardar las categorías.

Figura 62

Configuración de las nuevas categorias.

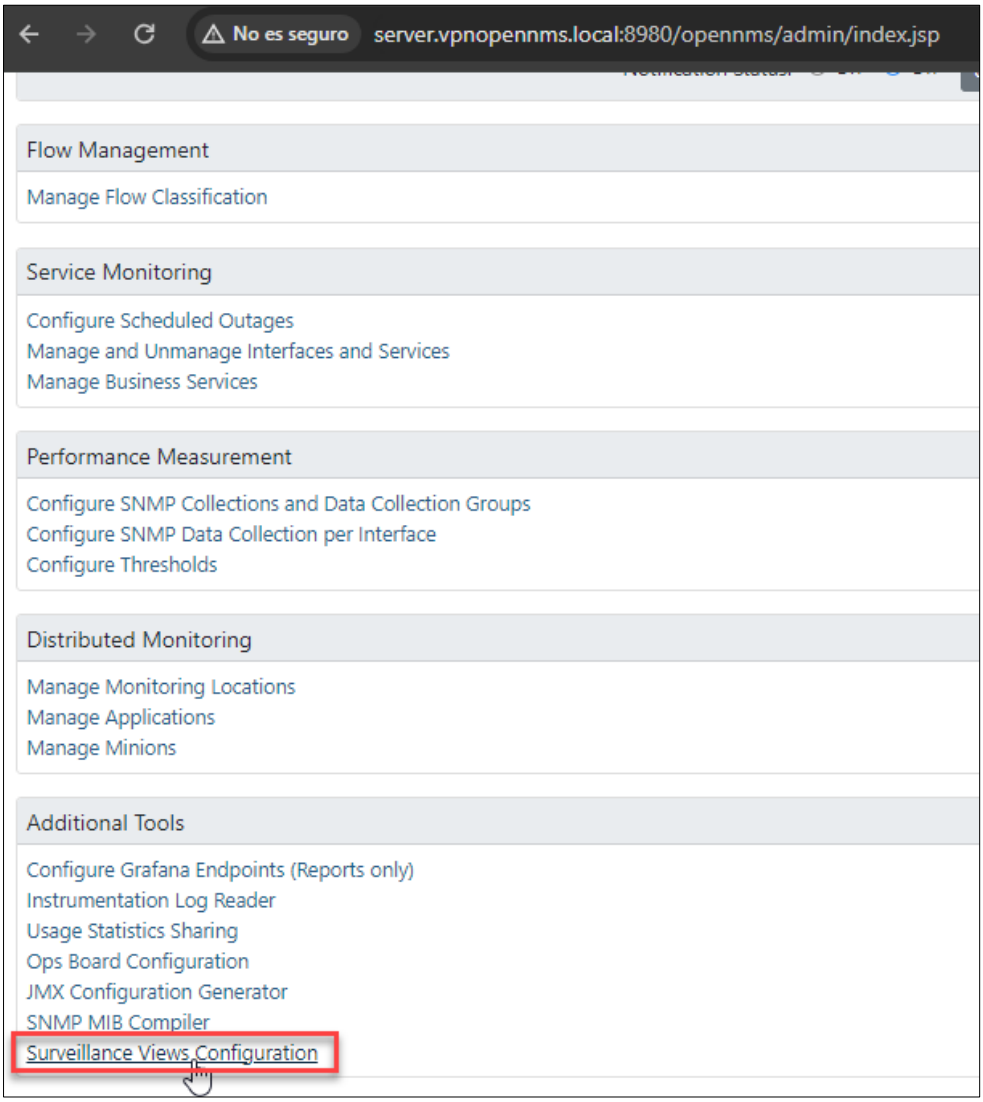


Nota: plataforma OpenNMS Horizon.

b) Creación de la Vista de Vigilancia. En la sección de configuraciones de la plataforma OpenNMS se ingresó el apartado "*Surveillance Views Configuration*", tal como, se indica en la figura 63 para iniciar la configuración.

Figura 63

Apartado de configuración de vistas de vigilancia.

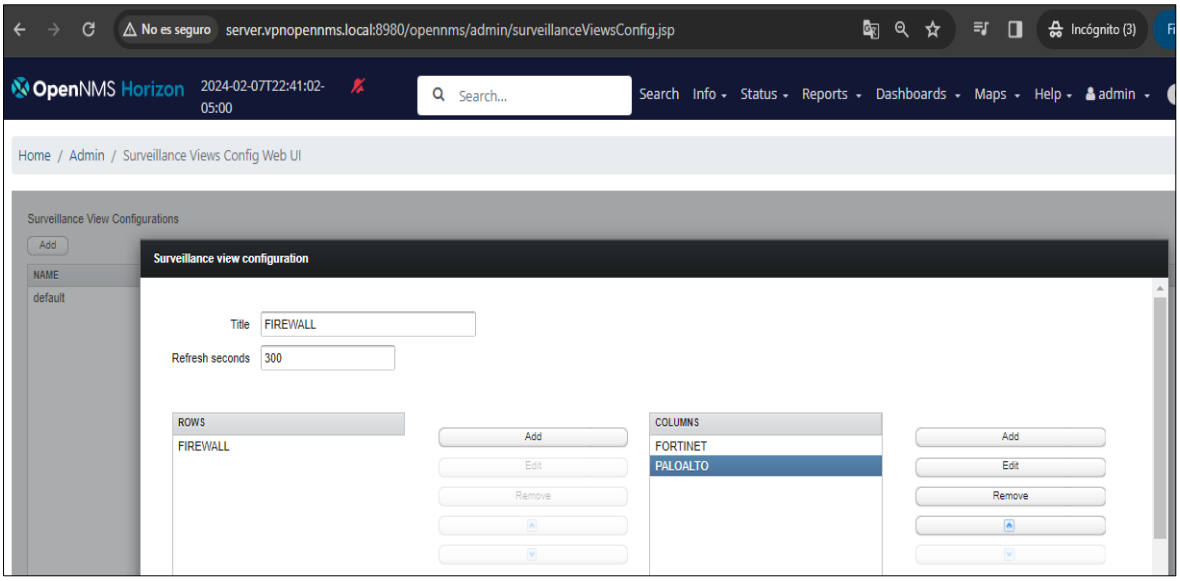


Nota: plataforma OpenNMS Horizon.

Presionando la tecla Add se configura la vista de vigilancia, tal como, se muestra en la figura 64, al introducir el nombre de la vista, se seleccionó la categoría general FIREWALL la cual contiene las dos categorías de FORTINET y PALOALTO, para finalmente guardar la configuración haciendo clic en Save.

Figura 64

Creación de la vista de vigilancia FIREWALL.

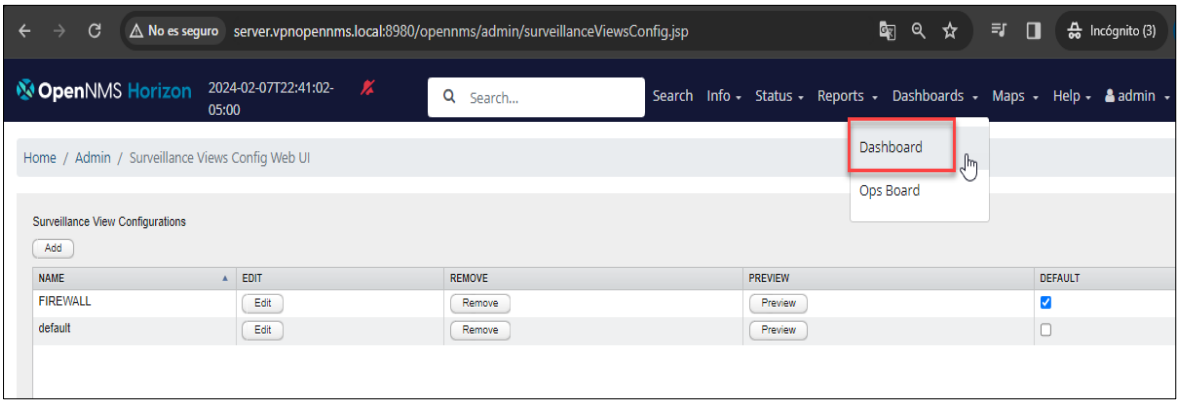


Nota: plataforma OpenNMS Horizon.

c) Verificación de la Vista de Vigilancia Creada. Al hacer clic en la sección Dashboards, seleccionándose la opción Dashboard, tal como, se indica en la figura 65.

Figura 65

Acceso al Dashboard.

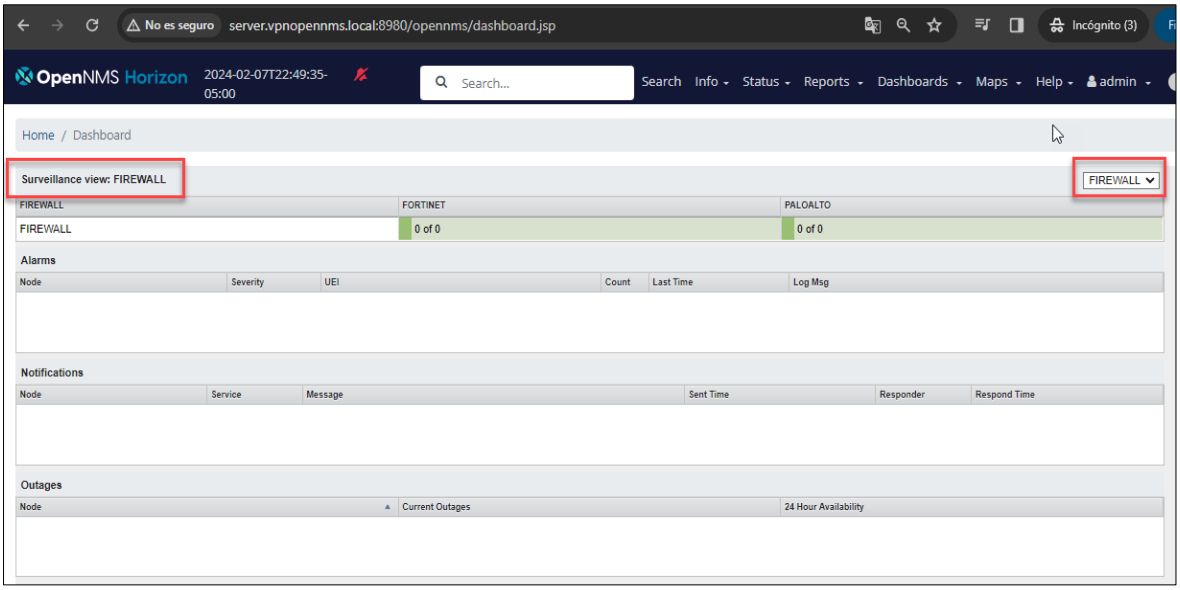


Nota: plataforma OpenNMS Horizon.

A continuación, como se presenta en la figura 66 se verifica la vista de vigilancia que se creó y sus categorías como FORTINET y PALOALTO.

Figura 66

Vista de vigilancia FIREWALL.



Nota: plataforma OpenNMS Horizon.

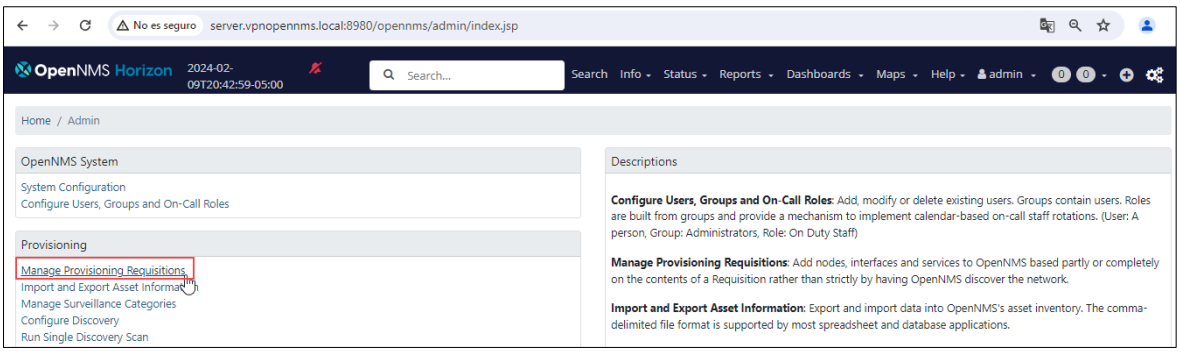
3.5.2 Habilitación del Protocolo SNMP y Agregación de Nodos Firewall

A continuación, se detalla la configuración de solicitudes de aprovisionamiento, presentación del protocolo SNMP, incremento de los nodos de seguridad perimetral – firewall a la plataforma de OpenSNMP.

a) Configuración de las Solicitudes de Aprovisionamiento. En el apartado de configuraciones de la plataforma OpenNMS se ingresó a la sección “Manage Provisioning Requisitions”, tal como, se indica en la figura 67 para iniciar la configuración.

Figura 67

Apartado de administración de solictudes de aprovisionamiento.

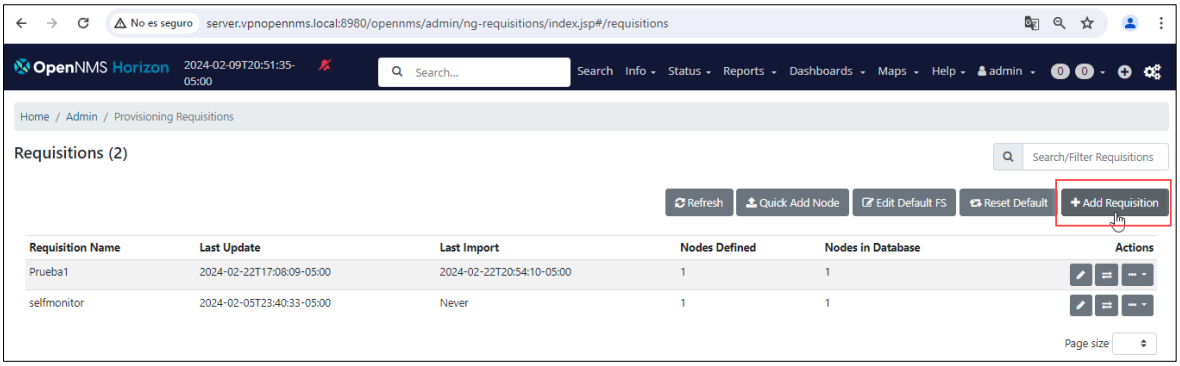


Nota: plataforma OpenNMS Horizon.

Se agregó una nueva solicitud de aprovisionamiento haciendo clic en el botón “*Add Requisition*”, tal como, se indica en la figura 68.

Figura 68

Acceso para agregar una solicitud de aprovisionamiento.

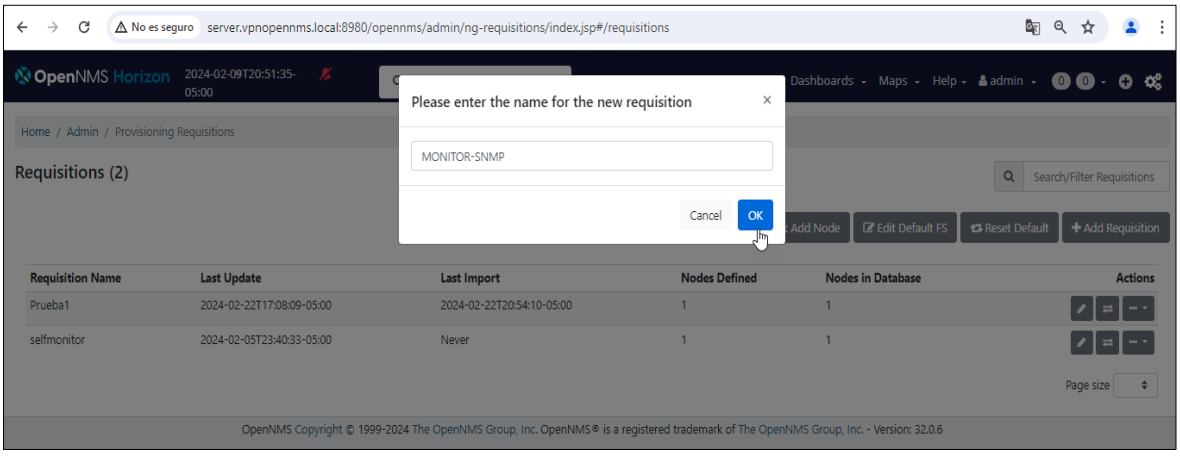


Nota: plataforma OpenNMS Horizon.

Seguidamente, se procedió a introducir el nombre de la solicitud MONITOR-SNMP, tal como, se muestra en la figura 69.

Figura 69

Nombre de la solicitud de aprovisionamiento.

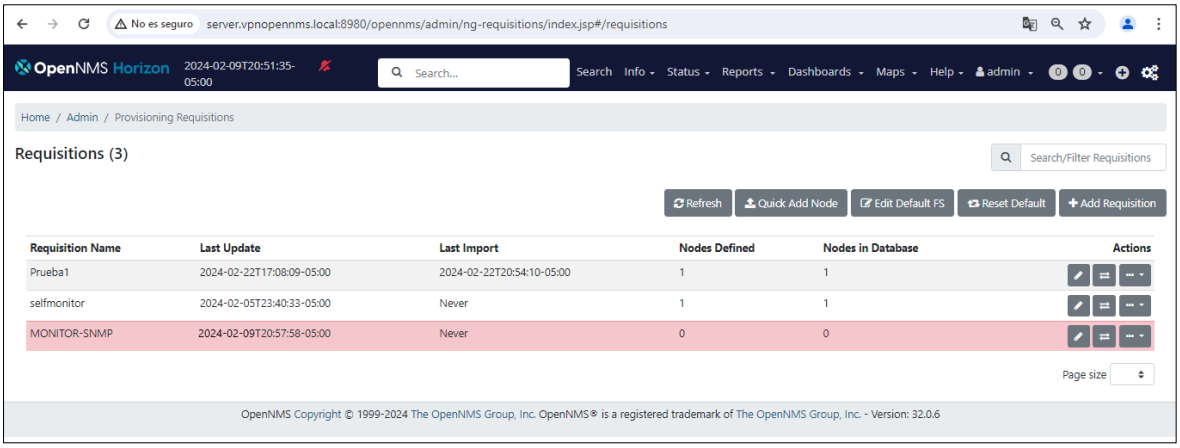


Nota: plataforma OpenNMS Horizon.

Finalmente se muestra el resultado de esta configuración como se presenta en la figura 70.

Figura 70

Solicitud de aprovisionamiento MONITOR-SNMP.

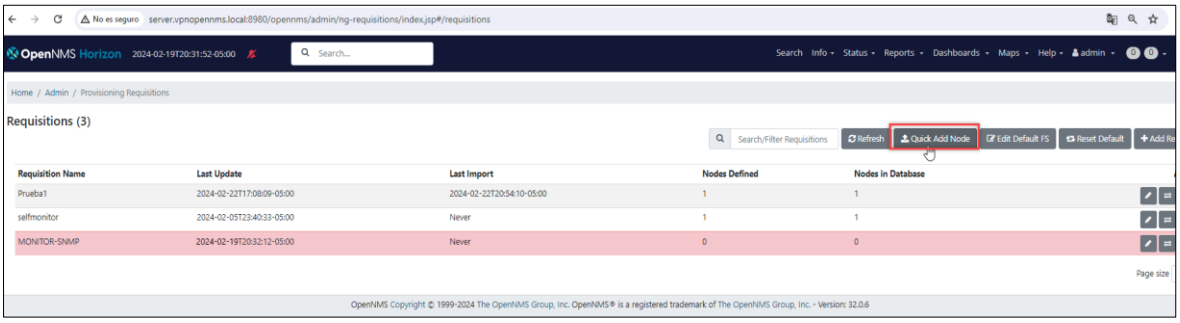


Nota: plataforma OpenNMS Horizon.

b) Adición de un Nodo de Seguridad Perimetral. Dentro del apartado “Manage Provisioning Requisitions”, se agregaron los nodos haciendo clic en el botón “Quick-*Add Node*”, tal como, se indica en la figura 71. Es necesario configurar por cada nodo que se agrega a la plataforma de OpenSNMP Horizon.

Figura 71

Acceso para agregar un nodo a la plataforma OpenNMS Horizon.

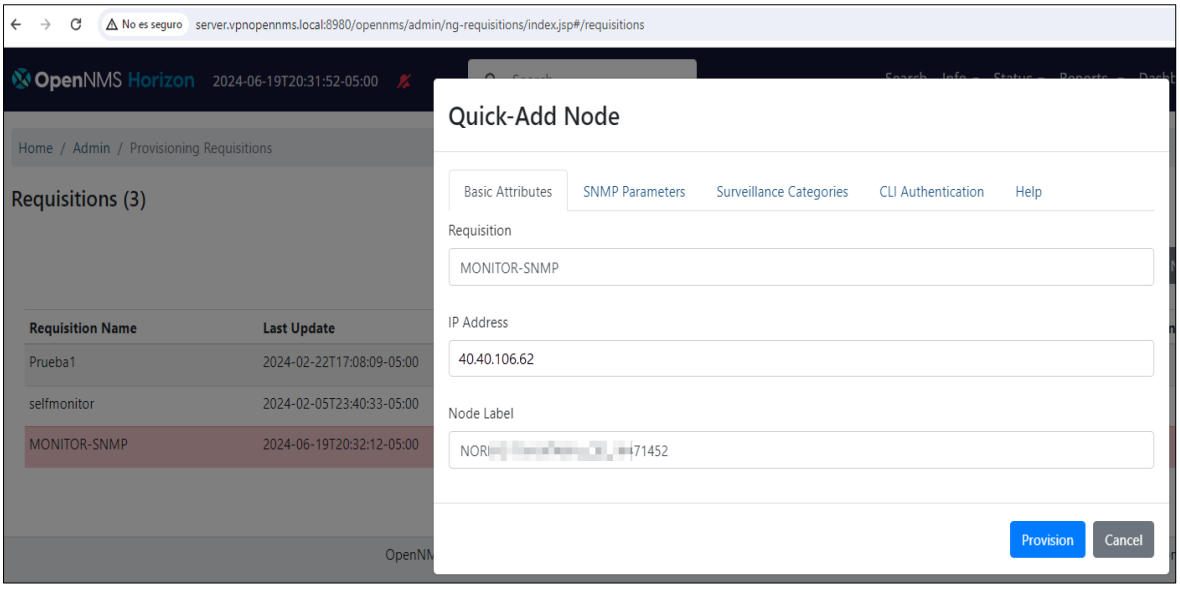


Nota: plataforma OpenNMS Horizon.

En la ventana Quick-Add Node se puede observar en la figura 72 como se configuraron los atributos básicos de solicitud de aprovisionamiento MONITOR-SNMP, la dirección IP de VRF 40.40.106.62 del nodo de seguridad perimetral y su respectiva etiqueta.

Figura 72

Configuración de atributos básicos del nodo de seguridad perimetral.

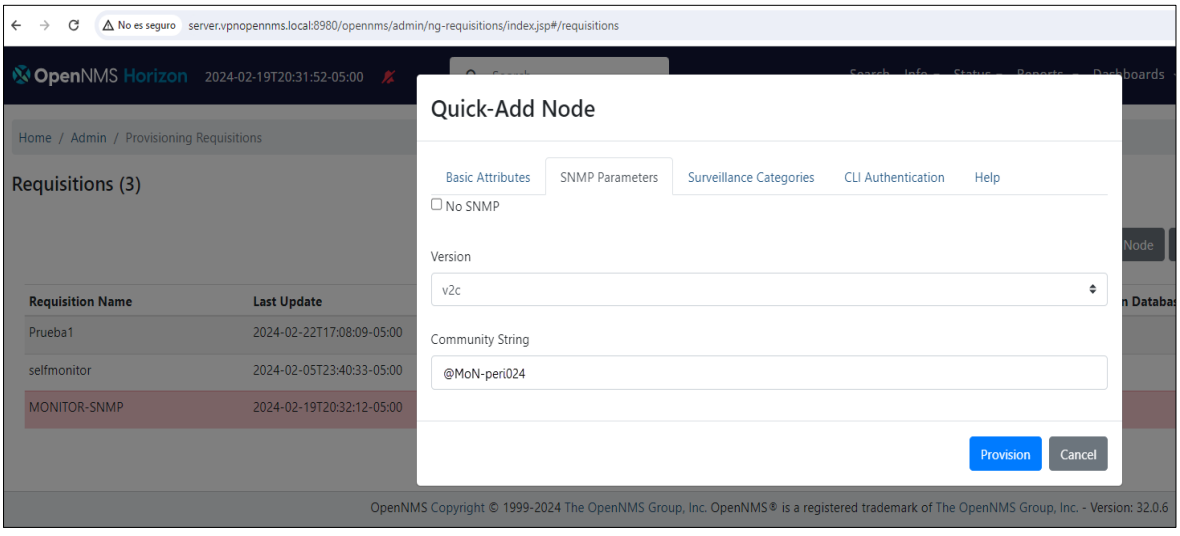


Nota: plataforma OpenNMS Horizon.

Una vez configurados los atributos básicos en la misma ventana Quic-Add Node y en el apartado SNMP Parameters como se presenta en la figura 73 se configuró los parámetros SNMP como la versión v2c del protocolo SNMP y el nombre de la comunidad SNMP la cual es "*@MoN-peri02* ".

Figura 73

Configuración de parametros SNMP.

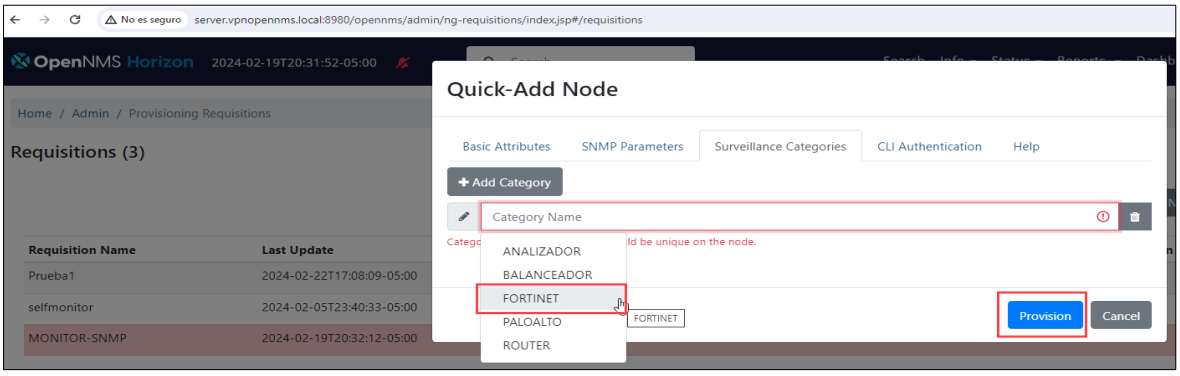


Nota: plataforma OpenNMS Horizon.

En la misma ventana Quick-Add Node y en su apartado Surveillance Categories, tal como, se indica en la figura 74 se configuró la categoría de vigilancia FORTINET después se procede a guardar la configuración haciendo clic en el botón Provision.

Figura 74

Configuración de la categoria de vigilancia para el nodo agregado.

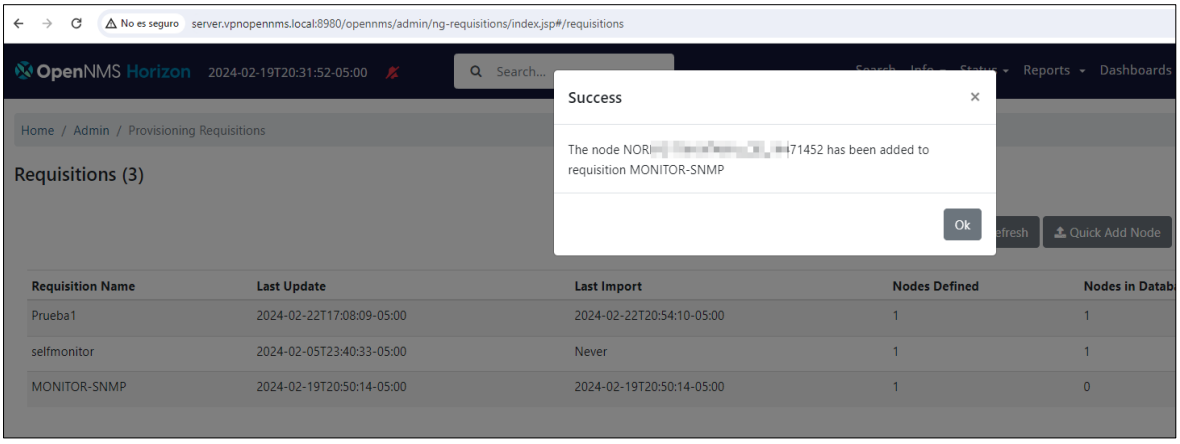


Nota: plataforma OpenNMS Horizon.

Finalmente se comprobó y verifico que la configuración guardada sea la correcta, al emitirse el mensaje mostrado en la figura 75.

Figura 75

Notificación que muestra, que el nodo agregado es el correcto.

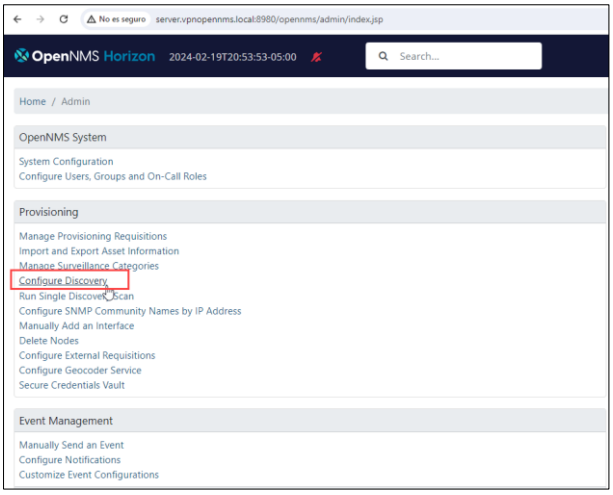


Nota: plataforma OpenNMS Horizon.

c) Configuración de Discovery. En la sección de configuraciones de la plataforma OpenNMS se ingresó al apartado "*Configure Discovery*", tal como, indica la figura 76 para dar inicio al proceso de configuración. Esta configuración fue repetida para cada nodo a ser agregado a la plataforma de OpenSNMP Horizon.

Figura 76

Acceso al apartado de configuración de descubrimiento SNMP.

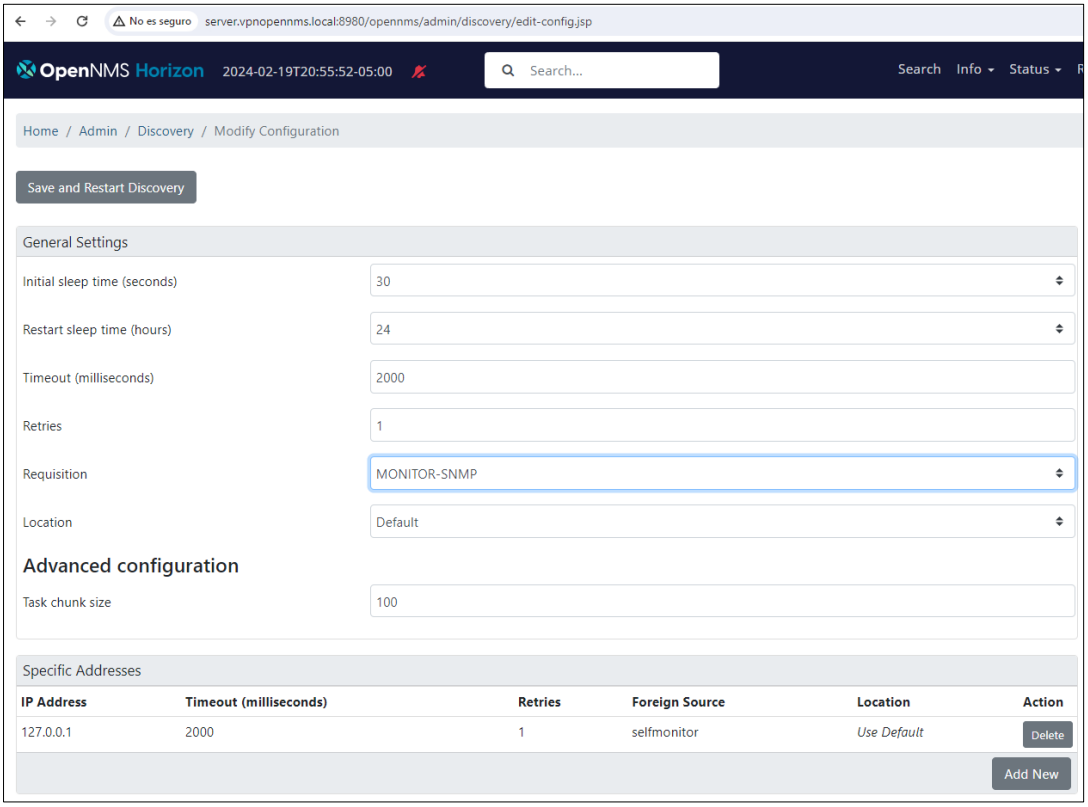


Nota: plataforma OpenNMS Horizon.

Seguidamente, en la sección General Settings se observa en la figura 77 que el campo Requisition fue seleccionado para la solicitud MONITOR-SNMP.

Figura 77

Selección de la solicitud de aprovisionamiento para el Discovery.

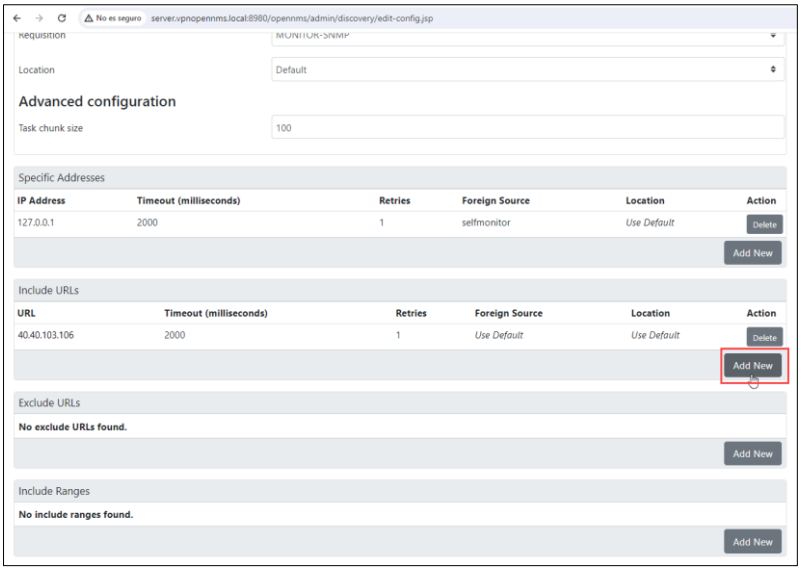


Nota: plataforma OpenNMS Horizon.

En el campo Include URLs, se agregaron las direcciones IP de los nodos de seguridad perimetral – firewall, click en el botón “Add New”, como se ve en la figura 78.

Figura 78

Acceso para agregar la IP de VRF de un nodo de seguridad perimetral.

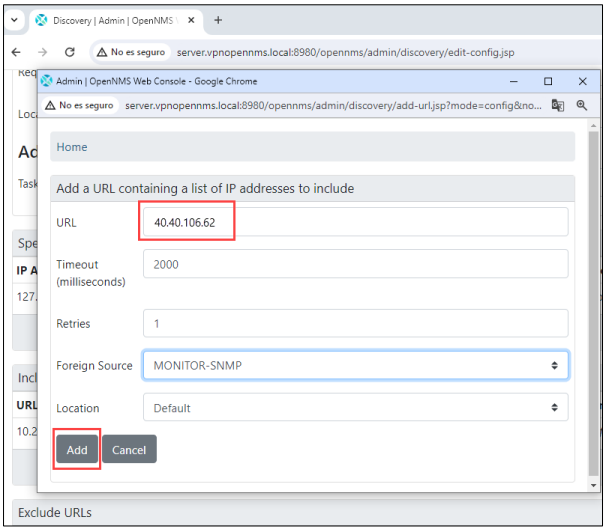


Nota: plataforma OpenNMS Horizon.

Seguidamente, se presenta la figura 79, en el campo URL se agregó la IP de VRF 40.40.106.62 del nodo de seguridad perimetral - firewall y guardar la configuración haciendo clic en el botón “*Add*”.

Figura 79

Configuración de IP de VRF del nodo de seguridad perimetral en Discovery.

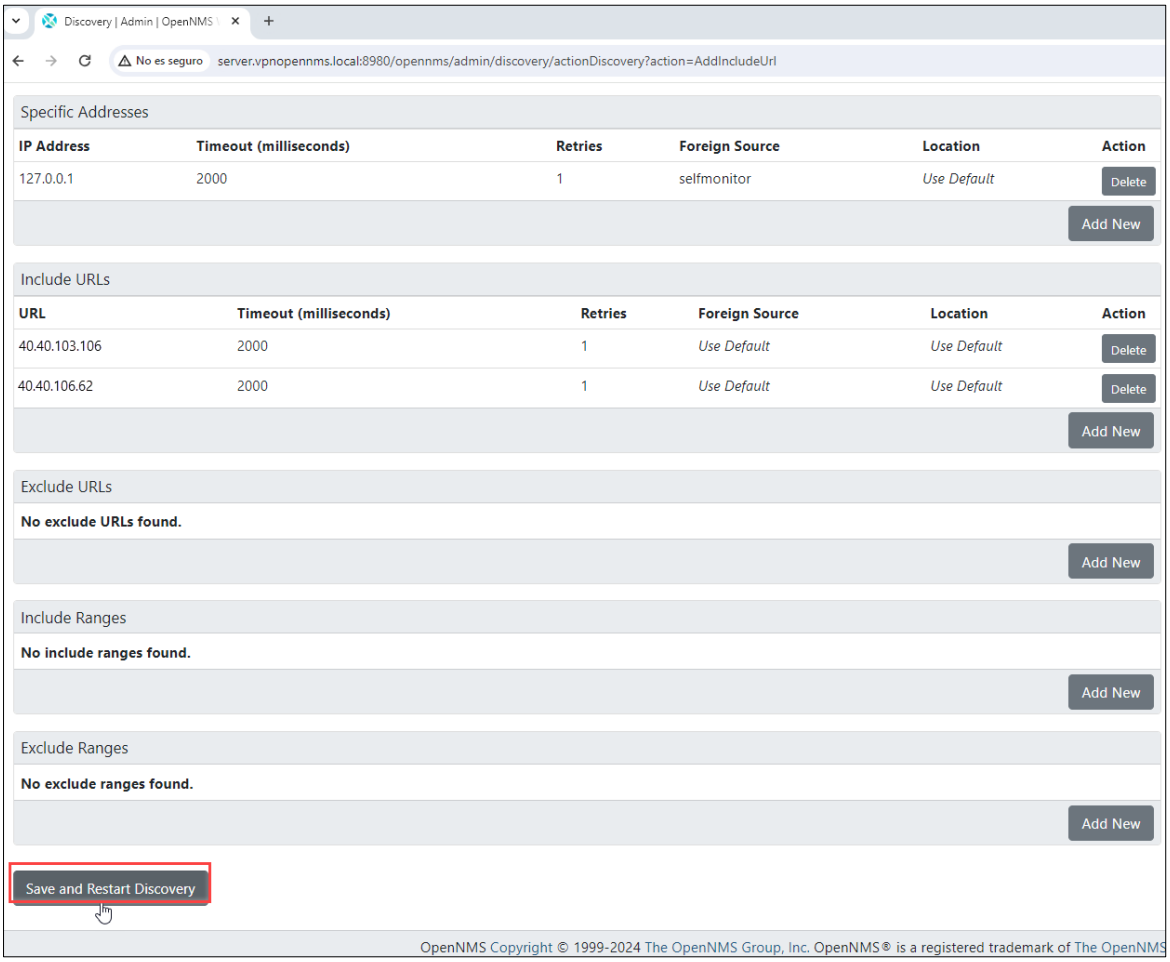


Nota: plataforma OpenNMS Horizon.

Finalmente, al hacer clic en el botón “*Save and Restart Discovery*” como se indica en la figura 80 para guardar la configuración y reiniciar con los nodos de seguridad perimetral – firewalls agregados, en correspondencia con el protocolo SNMP.

Figura 80

Guardar la configuración y reinicio del descubrimiento del Discovery.

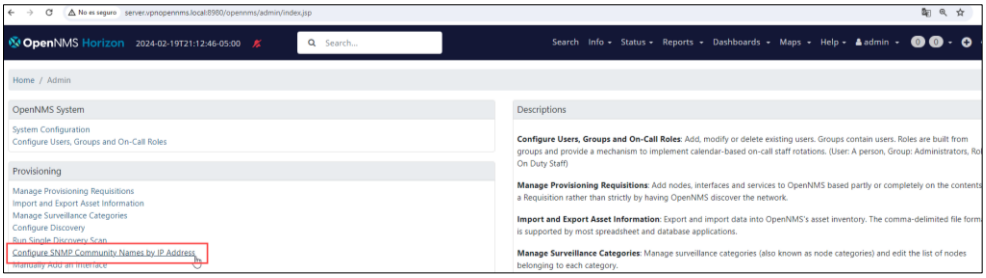


Nota: plataforma OpenNMS Horizon.

d) Configuración de la Comunidad SNMP por IP. En la sección de configuraciones de la plataforma OpenNMS al ingresar al apartado “*Configure SNMP Community Names by IP Address*”, tal como, se indica en la figura 81 se da inicio a su configuración. Efectuando estas configuraciones para cada nodo agregado a la plataforma de OpenSNMP Horizon.

Figura 81

Acceso al apartado de configuración de comunidad SNMP por IP.

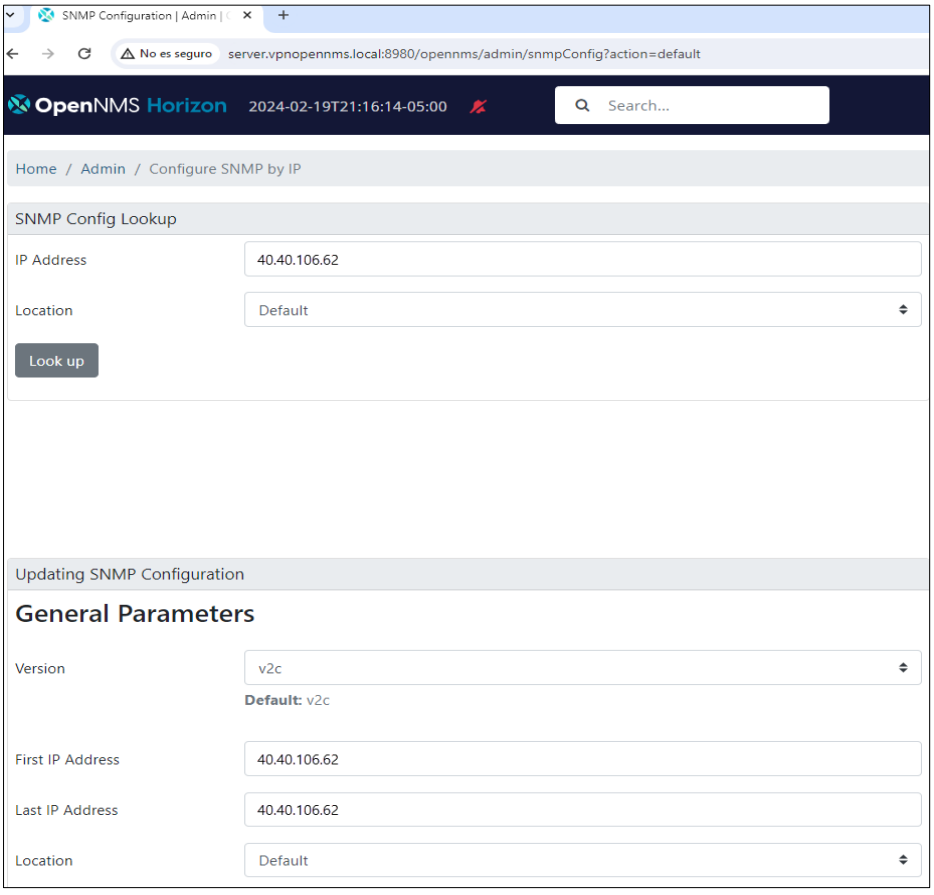


Nota: plataforma OpenNMS Horizon.

En la sección SNMP Config Lookup, se agregó la dirección IP VRF 10.249.186.62 del nodo de seguridad perimetral – firewall, tal como, se indica en la figura 82, así como, en la sección Updating SNMP Configuration se seleccionó la versión v2c agregándose la IP VRF en los campos First IP Address y Last IP Address.

Figura 82

Configuración de la comunidad SNMP por IP.

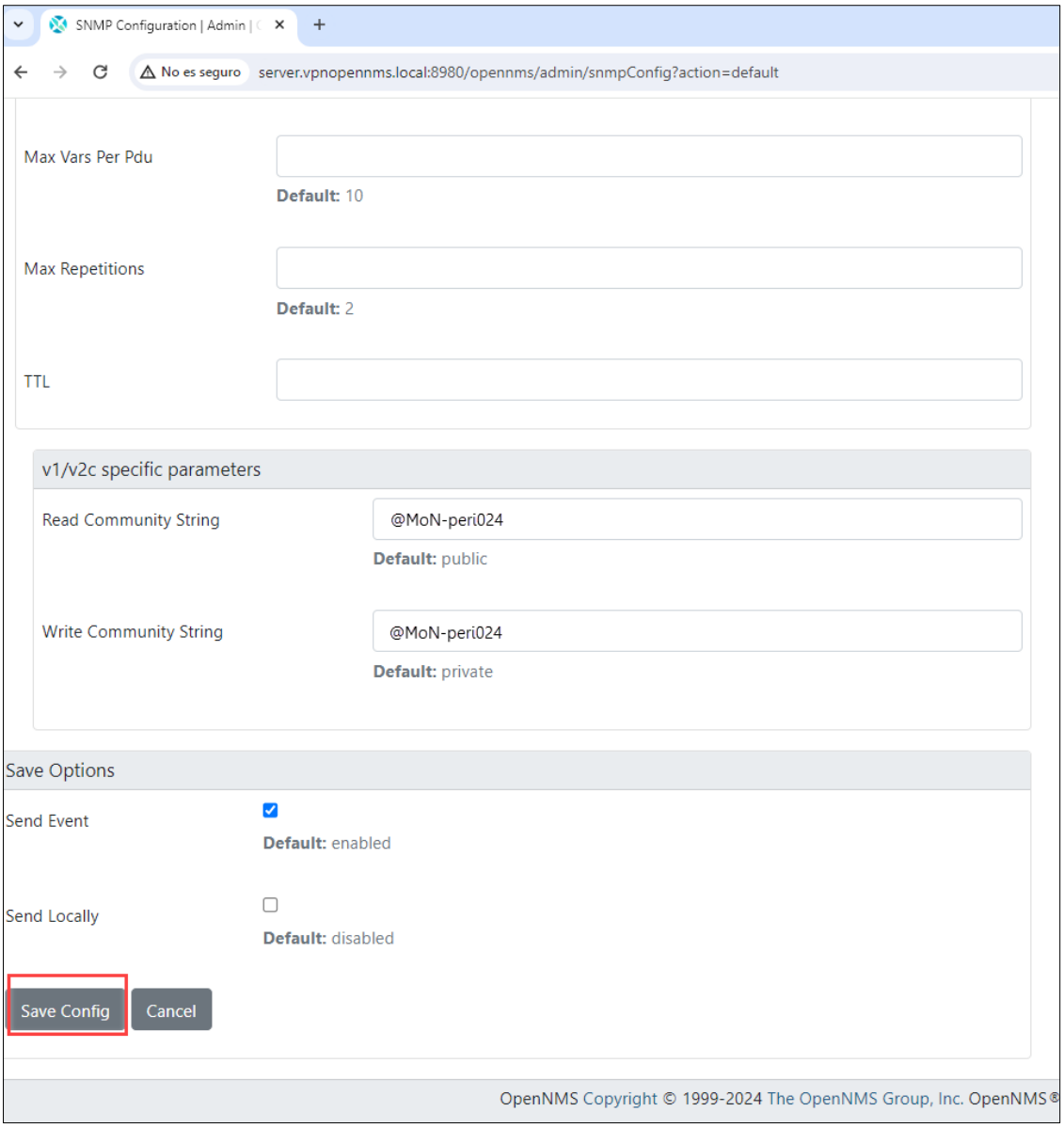


Nota: plataforma OpenNMS Horizon.

Finalmente, en la sección v1/v2c specific parameters de los campos Read Community String y Write Community String se introdujo el nombre de la comunidad SNMP "*@MoN-peri024*", tal como, se indica en la figura 83, para dar por concluida la configuración, y al hacer clic en el botón "*Save Config*" se guardó la configuración.

Figura 83

Guarda y configuración de la comunidad SNMP.

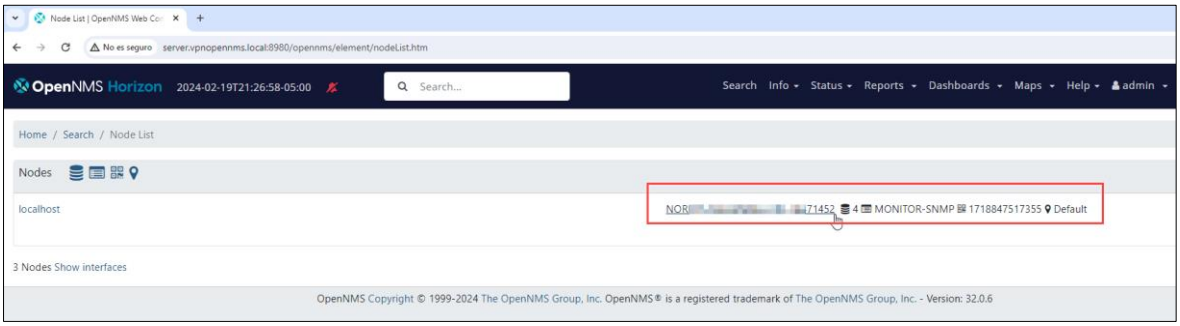


Nota: plataforma OpenNMS Horizon.

Al ingresar a la sección Info, en su apartado Node List, tal como, se presenta en la figura 84 se verificó y comprobó que el nodo de seguridad perimetral fue agregado correctamente a la plataforma OpenNMS Horizon.

Figura 84

Nodo de seguridad perimetral - firewall agregado correctamente a la plataforma OpenNMS Horizon.



Nota: plataforma OpenNMS Horizon.

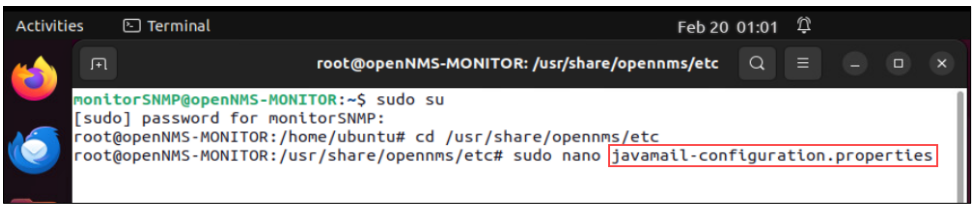
3.5.3 Configuración del Envío de Alertas por Correo Electrónico

A continuación, se detalla la configuración para él envió de alertas por correo electrónico desde el software de monitoreo OpenNMS Horizon hacia los administradores del SOC, con este fin se configuró un servidor SMTP y se efectuaron configuraciones adicionales en la plataforma OpenNMS Horizon.

a) Configuración de Servidor SMTP en el Servidor Ubuntu. El servidor SMTP fue configurado en el servidor Ubuntu 22.04, accediendo como usuario root en el terminal de Ubuntu con el comando "*sudo su*", seguidamente se ingresó con el comando "*cd /opt/opennms/etc*" a la carpeta donde se encuentra el archivo "*javamail-configuration.properties*" ejecutándose el comando "*sudo nano javamail-configuration.properties*" tal como, se presenta en la figura 85 accediendo a dicho archivo para proceder a su modificación.

Figura 85

Ejecución del archivo javamail-configuration.properties.

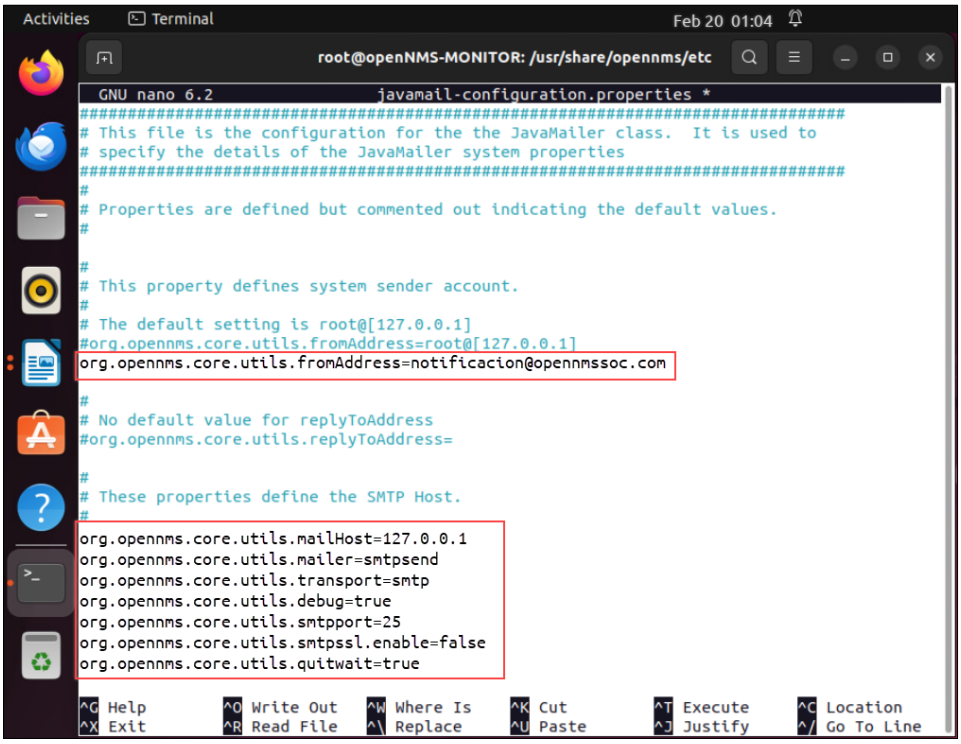


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

Dentro del archivo "*javamail-configuration.properties*" se configuraron los parámetros enmarcados en la figura 86, luego se guardó la configuración y se cerró el editor de texto.

Figura 86

Configuración del archivo javamail-configuration.properties.

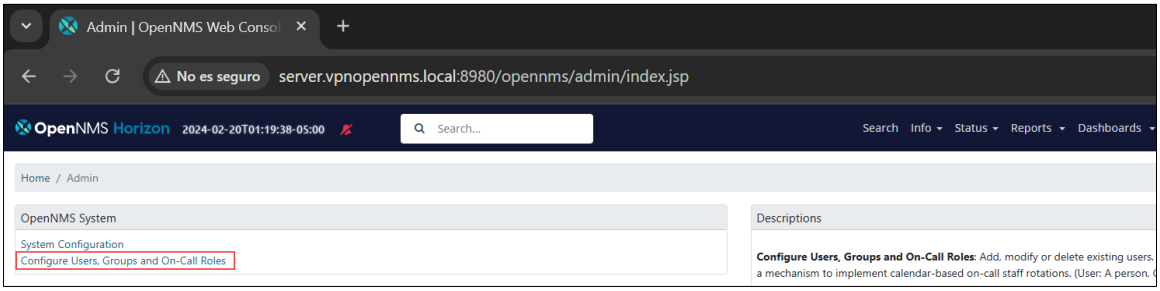


Nota: Terminal del sistema operativo Ubuntu 22.04.01.

b) Configuración de las Cuentas de Usuario. En el menú de configuraciones de la plataforma OpenNMS se ingresó al apartado "*Configure Users, Group and On-Call Roles*" tal como, se ve en la figura 87 para iniciar la configuración de cuentas de usuario.

Figura 87

Acceso a la sección de configuración de usuarios y grupos.

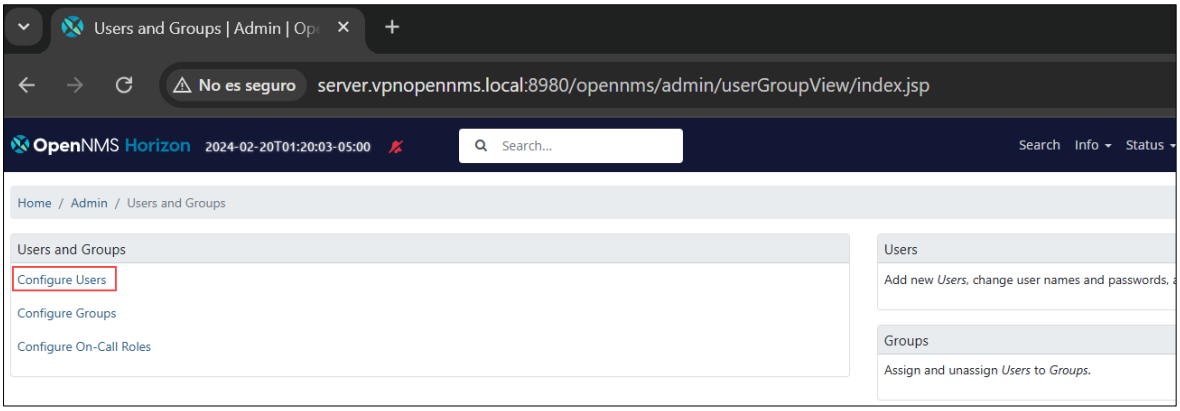


Nota: plataforma OpenNMS Horizon.

Seguidamente, en la sección Users and Groups como se ve en la figura 88 se seleccionó la opción Configure Users.

Figura 88

Acceso a la configuración de cuentas de usuario.

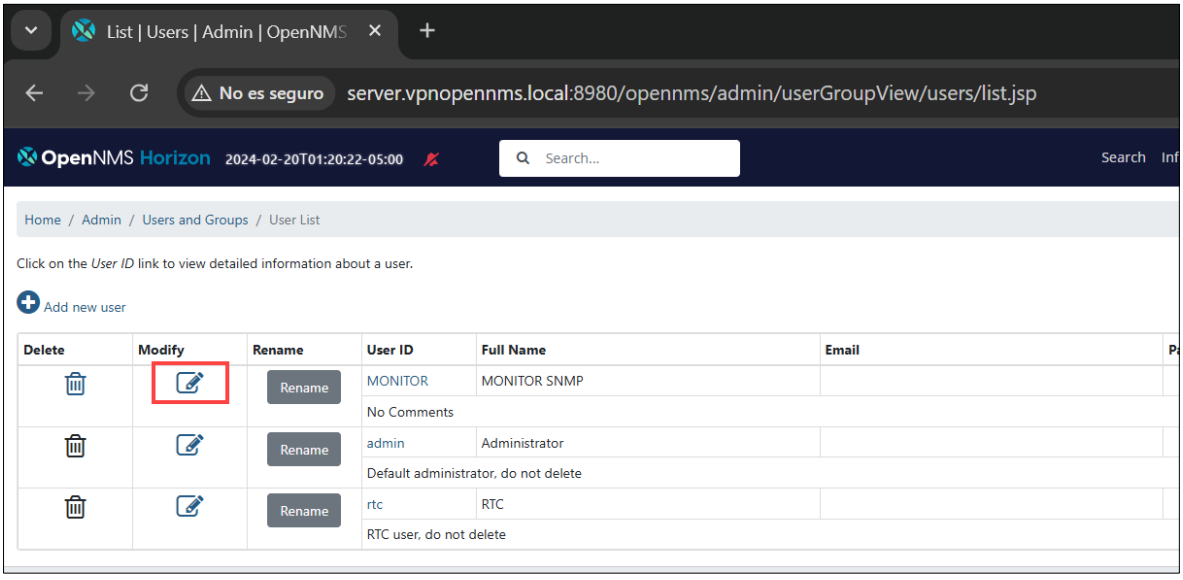


Nota: plataforma OpenNMS Horizon.

Seguidamente, aparece la ventana que se presenta en la figura 89, y en la columna Modify seleccionar el icono de edición para el usuario MONITOR y efectuar la configuración correspondiente a ese usuario.

Figura 89

Acceso a la configuración del usuario MONITOR.

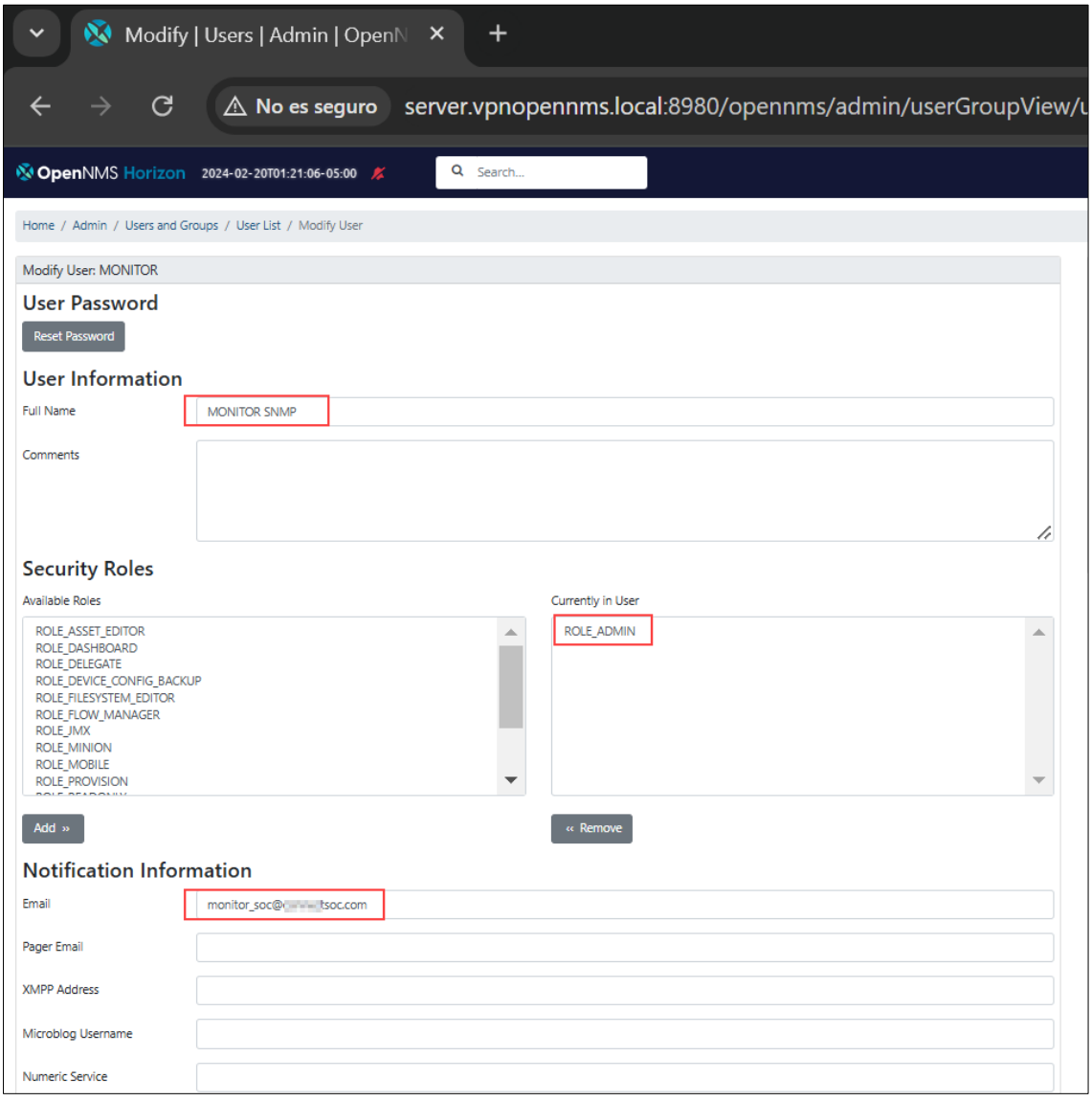


Nota: plataforma OpenNMS Horizon.

Finalmente, dentro de la sección Modify User: MONITOR se agregó en los parámetros de Full Name, Currently in User y Email los valores de MONITOR SNMP, ROLE_ADMIN y la dirección de correo electrónico monitor_so@****soc.com respectivamente, tal como, se indica en la figura 90 y para dar por concluida la configuración se hizo clic en el botón "*Save Config*" que guarda la configuración.

Figura 90

Configuración de parámetros para el usuario MONITOR.



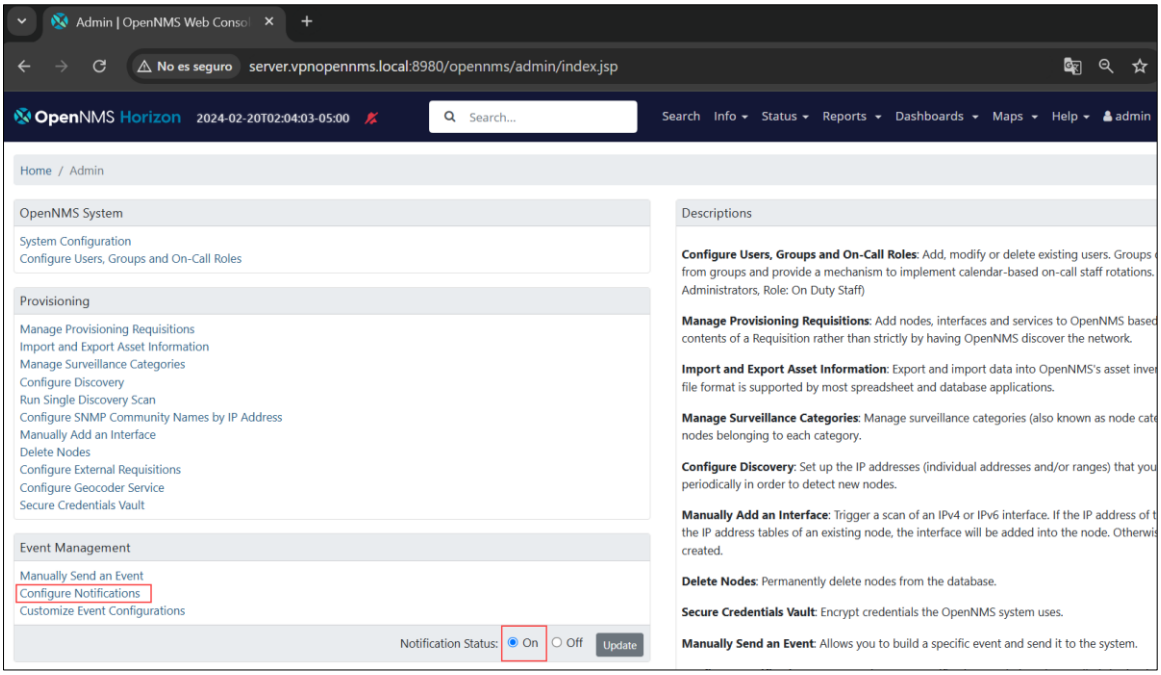
Nota: plataforma OpenNMS Horizon.

c) Configuración de la Notificación en la plataforma OpenSNMP. En el menú de configuraciones de la plataforma OpenNMS se habilitó la opción "*Notification* Status" y

luego se ingresó al apartado “*Configure Notification*”, tal como, se indica en la figura 91 para iniciar la configuración de las notificaciones.

Figura 91

Acceso al apartado de configuración de Notificaciones.

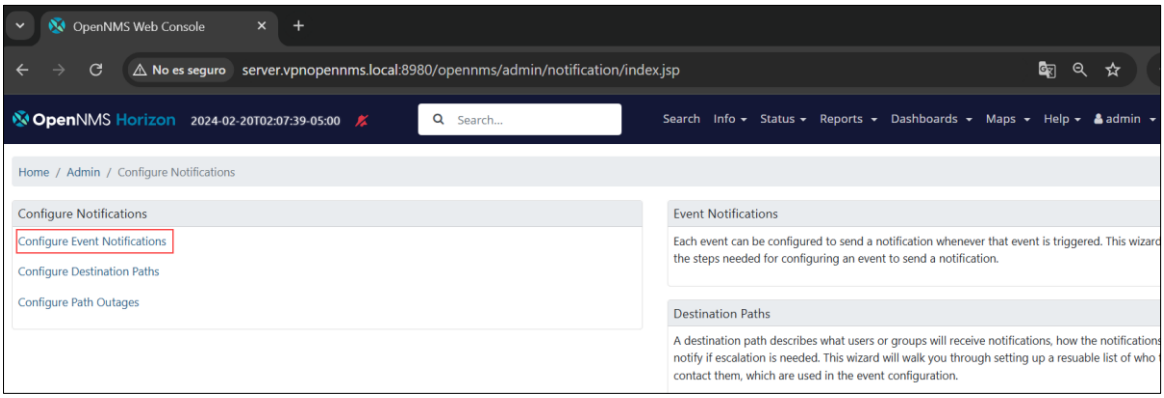


Nota: plataforma OpenNMS Horizon.

Luego en la sección Configure Event Notifications, tal como, se observa en la figura 92 se seleccionó la opción Configure Event Notifications.

Figura 92

Acceso a la configuración de notificación de eventos.

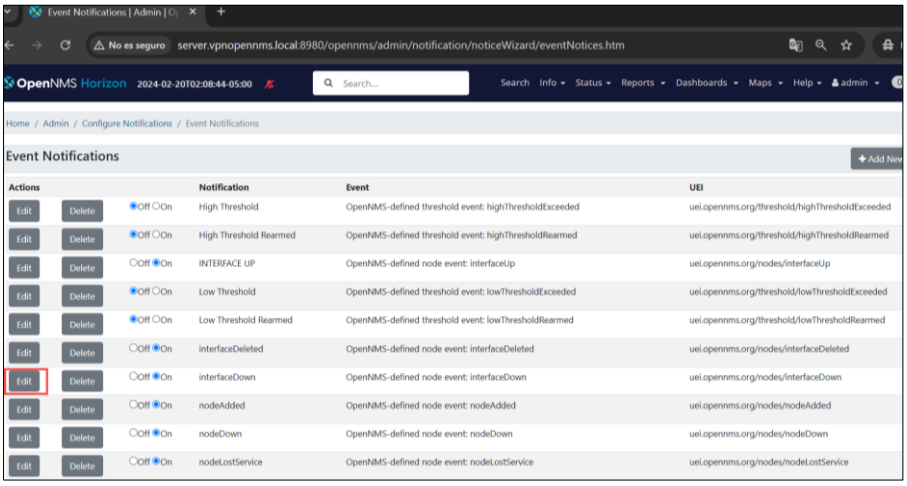


Nota: plataforma OpenNMS Horizon.

Seguidamente, aparece la ventana que se observa en la figura 93, y en la columna Actions se seleccionó Edit para efectuar la configuración en la notificación "*interfaceDown*" la cual alerta sobre una interface que se ha desconectado.

Figura 93

Acceso a la configuración de la notificación interfaceDown.

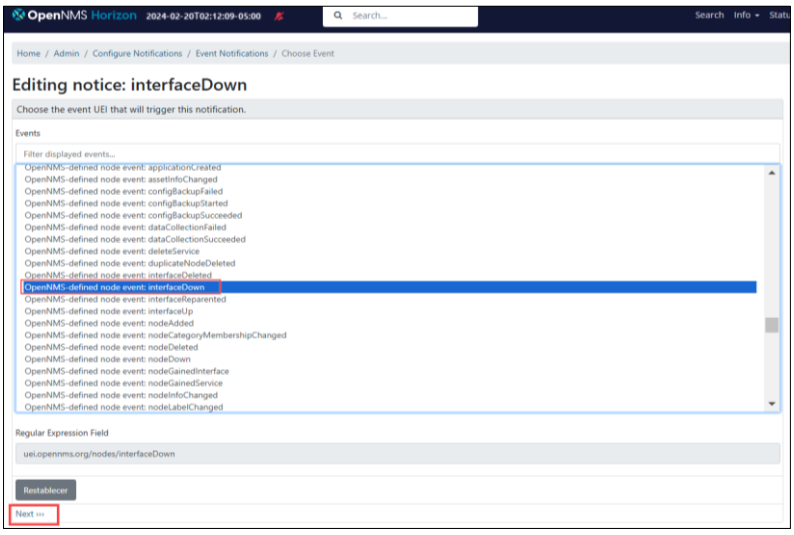


Nota: plataforma OpenNMS Horizon.

Luego en la ventana Editing notice: interfaceDown, tal como, se observa en la figura 94 se seleccionó el evento OpenNMS-defined node evento: interfaceDown haciendo clic en Next para continuar con la configuración.

Figura 94

Selección del evento interfaceDown.

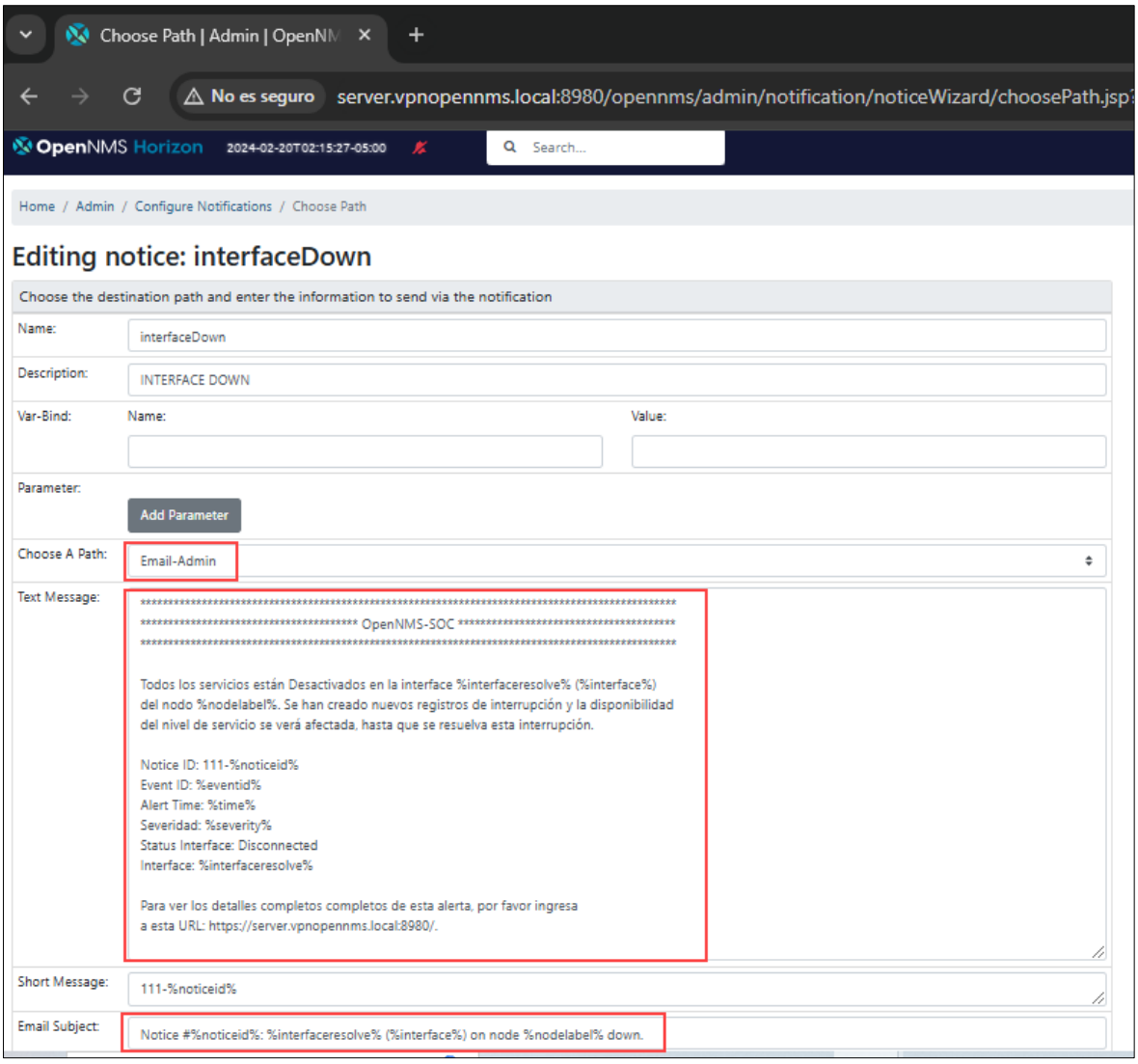


Nota: plataforma OpenNMS Horizon.

Finalmente, se agregó en los parámetros de Choose A Path, Text Message y Email Subject los valores de Email-Admin que contiene la dirección de correo del usuario MONITOR y admin, la información que indica que la interface se ha desconectado y el asunto del correo electrónico indicando que la interface está en Down respectivamente como se indica en la figura 95, para dar por terminada la configuración se hizo clic en el botón "*Save*" y guardar la configuración.

Figura 95

Configuración del contenido de la notificación interfaceDown.



Nota: plataforma OpenNMS Horizon.

3.6 Configuración de los Nodos De Seguridad Perimetral - Firewall

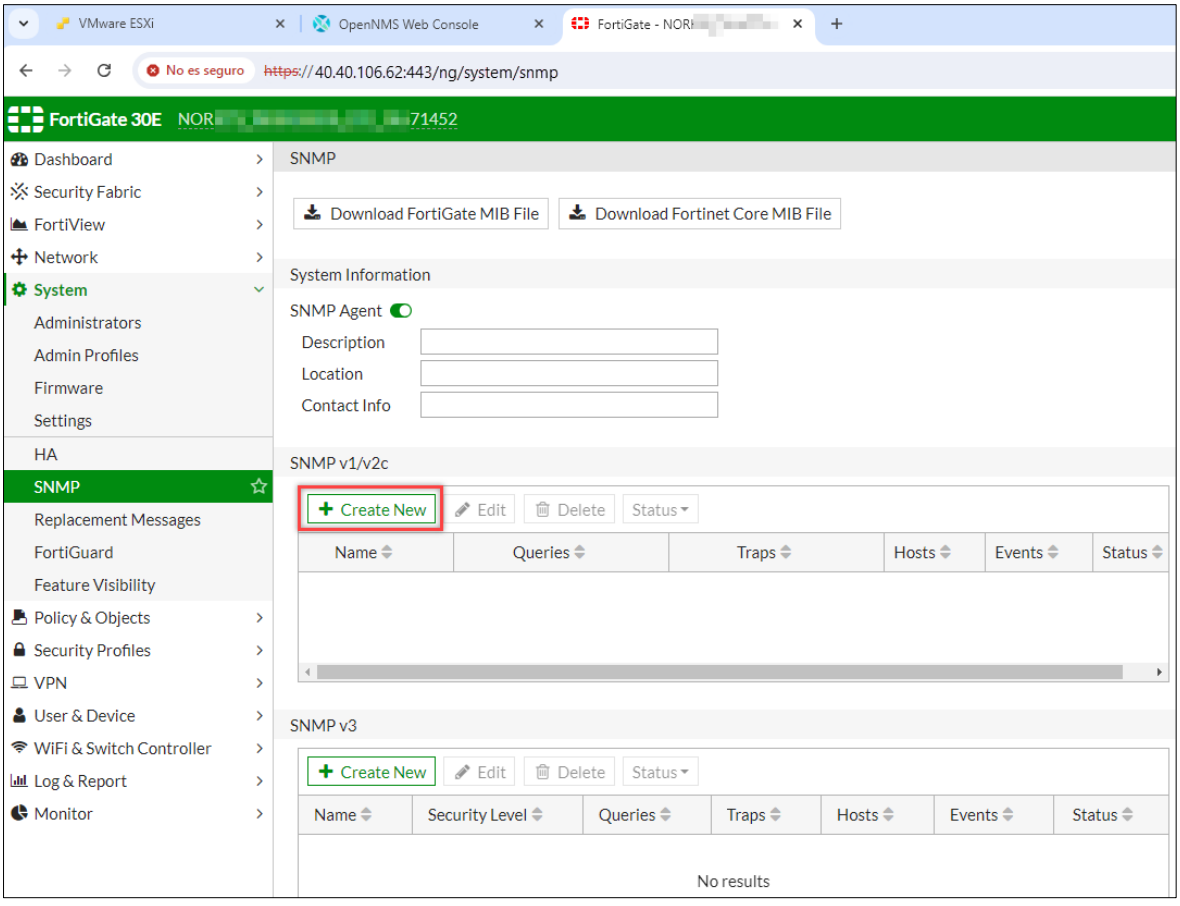
Se muestra la configuración de los nodos de seguridad perimetral, los parámetros de operación del protocolo SNMP como la comunidad SNMP, la IP del colector del software OpenNMS Horizon y la configuración del origen al nodo para el envío de paquetes SNMP.

3.6.1 Creación de la Comunidad SNMP

En la plataforma de configuración del nodo de seguridad perimetral – firewall sección System, apartado SNMP se configuran los parámetros de SNMP, tal como, se presenta en la figura 96. En el campo System Information del mismo apartado se habilitó el campo "*SNMP Agent*", así mismo, en el campo SNMP v1/v2c, haciendo clic en "*Create New*" puede crearse una nueva comunidad.

Figura 96

Ventana de configuración del apartado SNMP del nodo de seguridad perimetral - firewall.

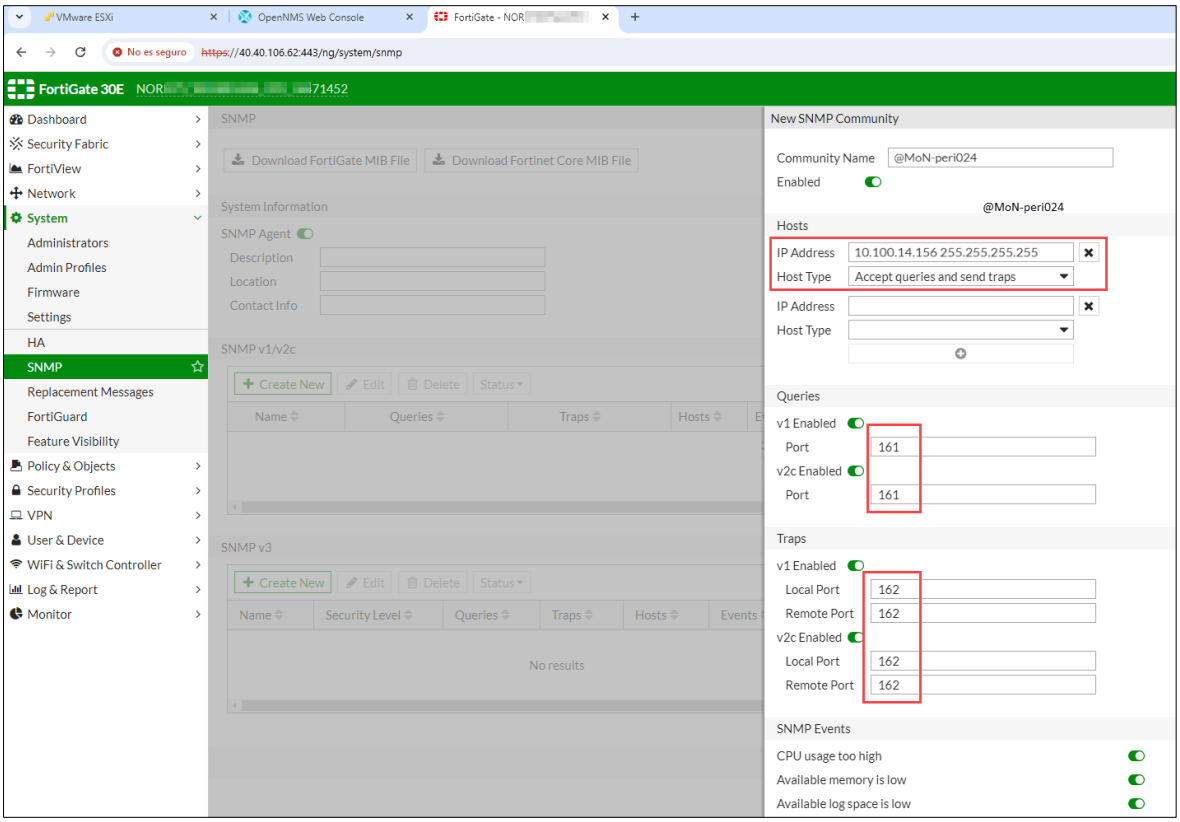


Nota: Plataforma de configuración del equipo firewall.

En la opción Create New, se configuraron los campos de Community Name introduciendo el nombre "*@MoN-peri024*" nombre con el cual también se configuró en la plataforma OpenNMS Horizon, en IP Address se introdujo la IP 10.100.14.156 con mascara de red 255.255.255.255 la cual pertenece a la IP del colector de OpenNMS, en Host Type se seleccionó "*Accept queries and send traps*", en port Queries se introdujo el valor de 161 y en port Traps se introdujo el valor de 162, tal como se ve en la figura 97. Para terminar la configuración fueron seleccionados los eventos que el nodo de seguridad perimetral envía al colector de OpenSNMP, para luego guardar la configuración.

Figura 97

Configuracion de los Parámetros del protocolo SNMP del nodo de seguridad perimetral.

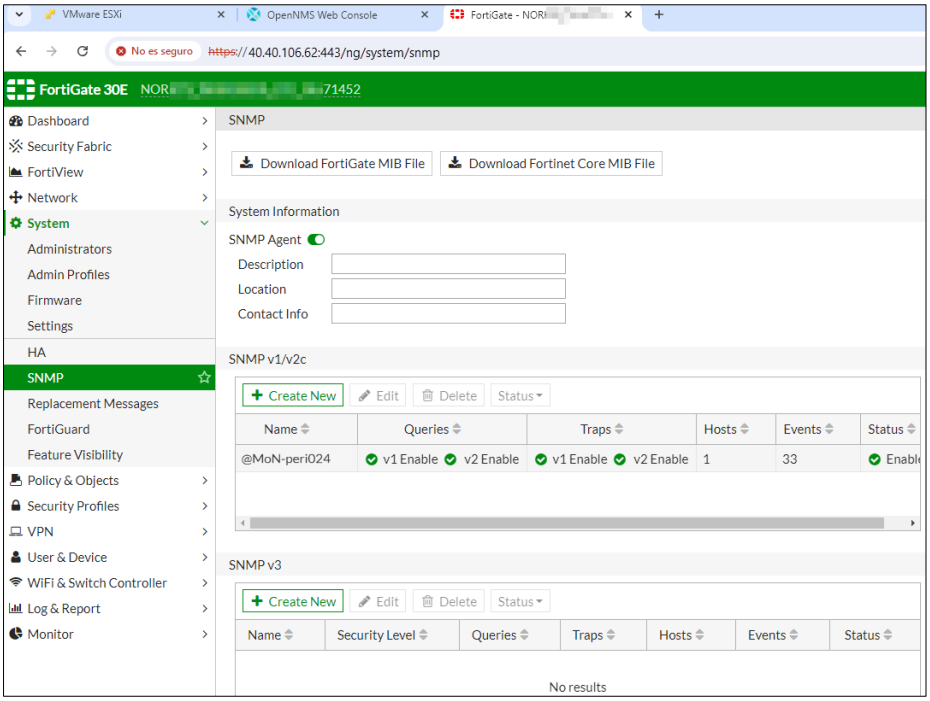


Nota: Plataforma de configuración del equipo firewall.

Finalmente se comprobó y verificó que la configuración fue efectuada correctamente, tal como, puede verse en la figura 98, donde pueden observarse que el nombre de la comunidad, los Queries y Traps han sido habilitados.

Figura 98

Configuracion del Protocolo SNMP del nodo de seguridad perimetral.



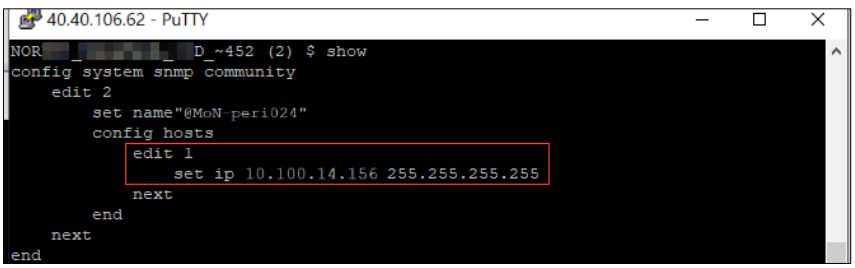
Nota: Plataforma de configuración del equipo firewall.

3.6.2 Configuración del Origen en el Equipo Firewall

Una vez creada la comunidad SNMP en el nodo de seguridad perimetral, se utilizó el cliente de SSH Putty para iniciar la configuración por línea de comandos - CLI del nodo. El comando "*config system snmp community*" permite acceder a línea de configuración de la comunidad SNMP "*@MoN-peri024*", tal como, se presenta en la figura 99.

Figura 99

Configuración de la comunidad SNMP del nodo de seguridad perimetral.



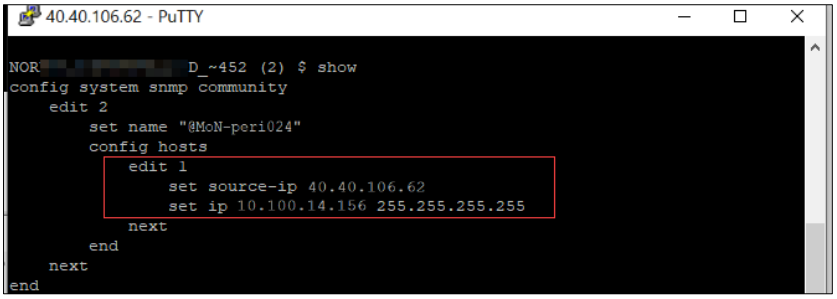
Nota: Interfaz CLI de configuración del equipo firewall.

A continuación, con el comando "*set source-ip* 40.40.106.62 255.255.255.255" se agregó el IP de origen a la comunidad SNMP, la cual es el IP VRF y la máscara de red del

nodo de seguridad perimetral – firewall. En la figura 100 se observa la configuración completa de la IP de origen.

Figura 100

Configuración de source-ip.

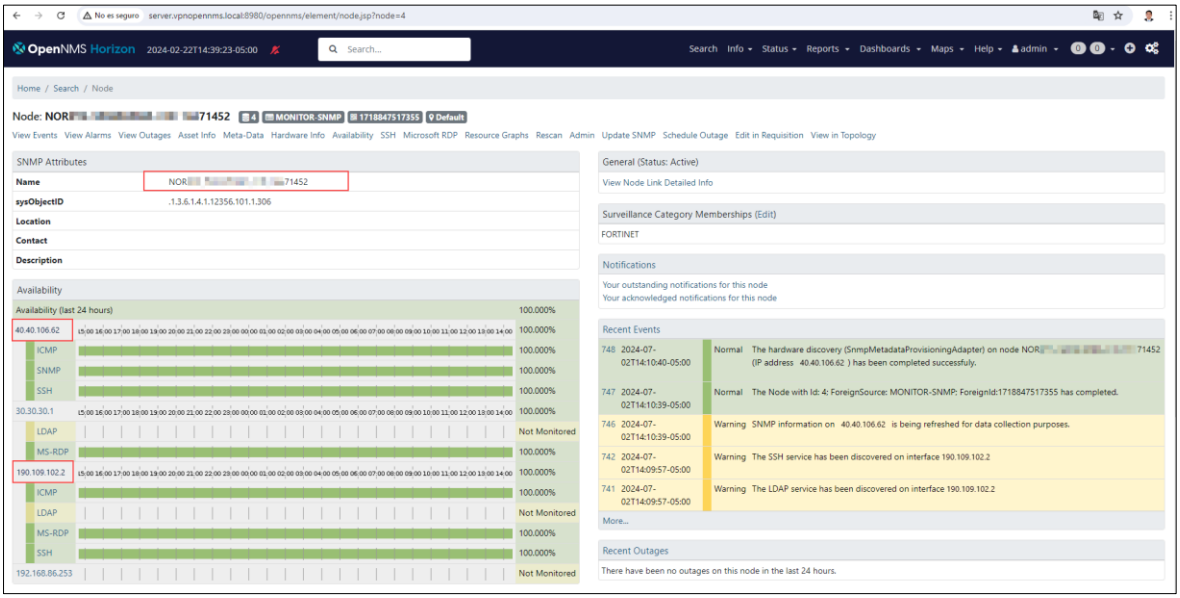


Nota: Interfaz CLI de configuración del equipo firewall.

Finalmente se verificó que el nodo de seguridad perimetral se configuró correctamente, se ingresó al apartado Node de la sección Info en la plataforma de OpenNMS Horizon y se visualizó el nodo de seguridad perimetral, monitoreando todas sus interfaces con sus respectivos protocolos de ICMP, SSH y SNMP como se puede observar en la figura 101 en la cual se ve la interface WAN con IP publica 190.109.102.2 y la IP de VRF 40.40.106.62.

Figura 101

Nodo de seguridad perimetral monitoreado por OpenNMS Horizon.



Nota: plataforma OpenNMS Horizon.

3.7 Pruebas al Software de Monitoreo OpenNMS

Una vez agregado el nodo de seguridad perimetral – firewall a la plataforma de monitoreo OpenNMS Horizon y se configuró el nodo de seguridad perimetral con los parámetros del protocolo SNMP, se realizó las pruebas de conectividad entre el colector del OpenSNMP Horizon y el nodo de seguridad perimetral, pruebas en la que en el Dashboard de la plataforma OpenNMS Horizon se alerte la caída de una interface y prueba de envío de alertas al correo del SOC de la empresa de telecomunicaciones.

Estas pruebas se realizaron en cada nodo de seguridad perimetral agregado a la plataforma de monitoreo.

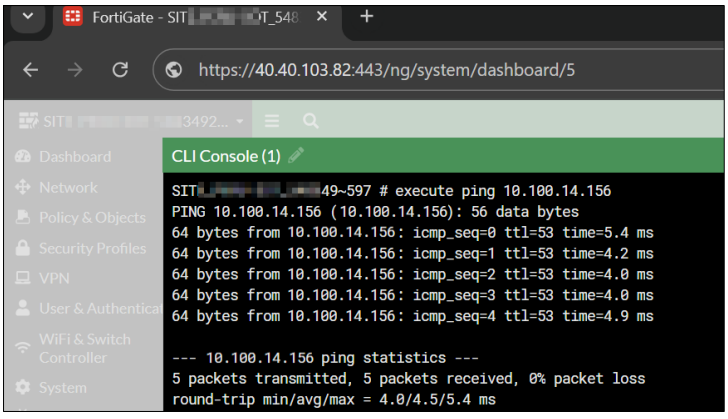
3.7.1 Pruebas de Conectividad

Se realizó las siguientes pruebas entre el nodo de seguridad perimetral – firewall y el colector de la plataforma OpenNMS Horizon.

a) Conectividad por ICMP. En la interfaz gráfica del firewall se ingresó a la configuración por CLI en la cual se ejecutó el comando "*execute ping*" para realizar consultas enviando paquetes ICMP desde el nodo de seguridad perimetral – firewall hacia la IP de VRF 10.100.14.156 del colector de OpenNMS como se presenta en la figura 102, se verificó que la latencia de 4.5 ms está dentro de los parámetros aceptables y que hay una conexión entre el colector de OpenNMS y el nodo de seguridad perimetral.

Figura 102

Envío de paquetes ICMP entre el colector OpenNMS y el dispositivo firewall.

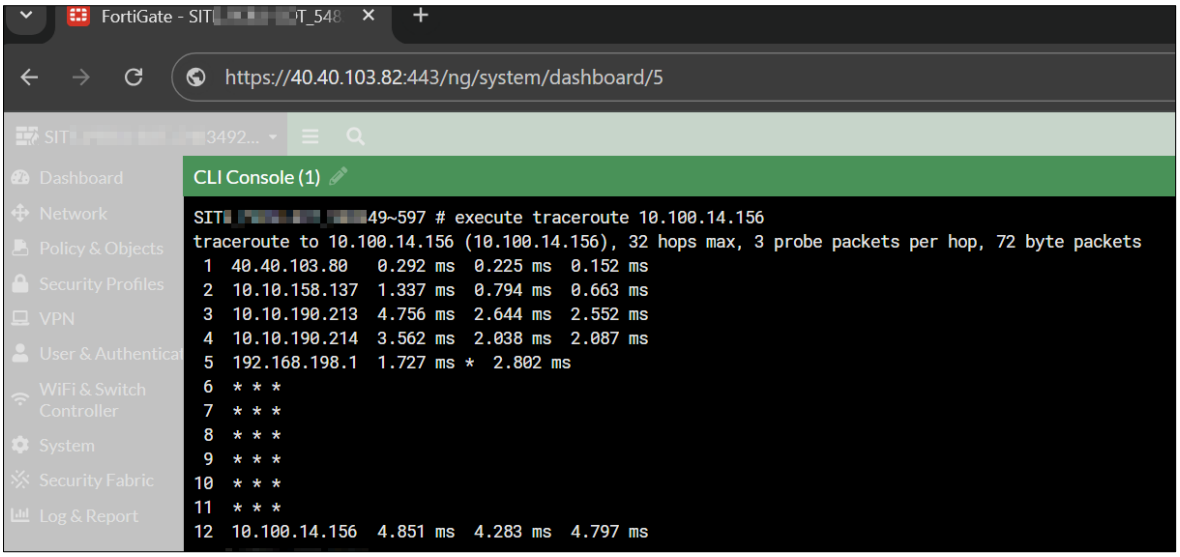


Nota: Plataforma de configuración del equipo firewall.

b) Conectividad por Traceroute. En la interfaz gráfica del firewall se ingresó a la configuración por CLI en la cual ejecutó el comando "*execute traceroute*" para saber que ruta emplea el paquete ICMP desde el nodo de seguridad perimetral – firewall hacia la IP de VRF 10.100.14.156 del colector de OpenNMS como se presenta en la figura 103, se verificó que la ruta es la correcta ya que el primer salto es a la IP 40.40.103.80 que es el Gateway de la Interface de VRF del dispositivo firewall y luego pasa por los dispositivos intermedios de la red de VRF de gestión de la empresa de telecomunicaciones hasta llegar al colector de OpenNMS instalado en un servidor del SOC.

Figura 103

Ejecución de comando Traceroute en nodo de seguridad perimetral.



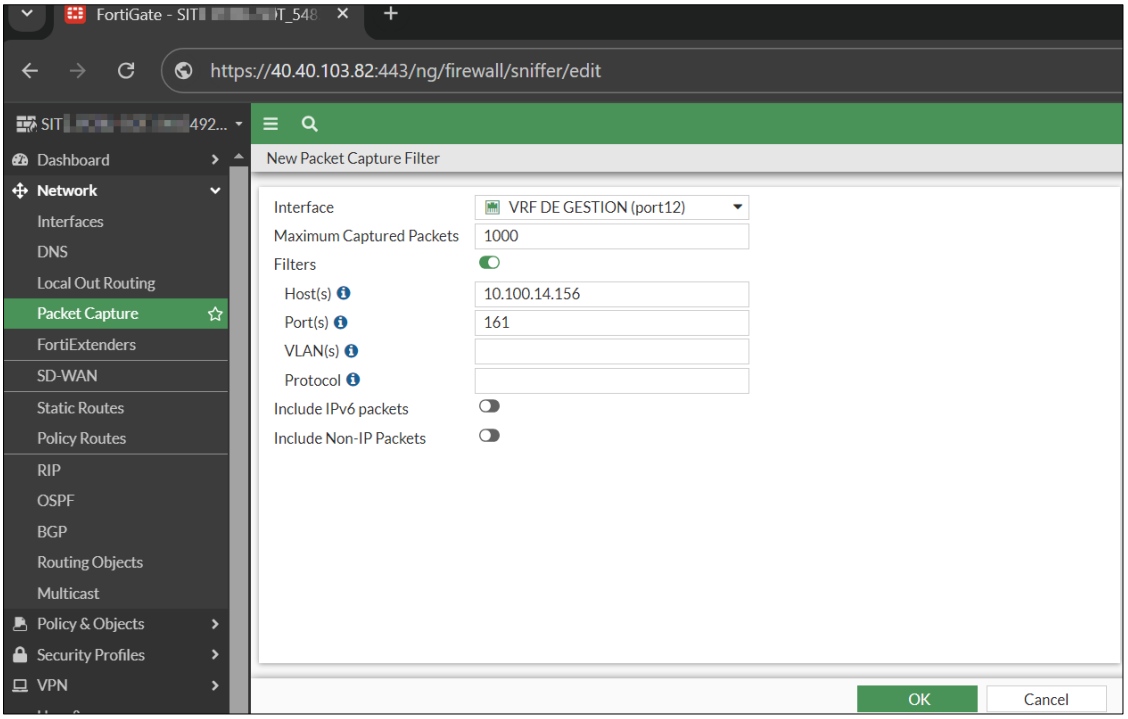
Nota: Plataforma de configuración del equipo firewall.

c) Transmisión de Paquetes SNMP. En la plataforma de configuración del nodo de seguridad perimetral – firewall se ingresó a la sección Network y luego al apartado Packet Capture, dentro de este apartado se hizo clic en "*Create New*" para crear una nueva captura y configurar los parámetros de captura de paquetes del protocolo SNMP como se presenta en la figura 104. Una vez que se ingresó a la opción Create New se configuraron los campos de Interface seleccionándose la interface de "*VRF DE GESTION (port12)*", se introdujo la captura de 1000 paquetes, se ingresó la IP destino 10.100.14.156 perteneciente al colector de OpenNMS y por último el puerto 161 que se utilizó para transmitir los

paquetes SNMP. Luego de la configuración se hizo clic en OK para guardar la configuración e iniciar la captura de paquetes.

Figura 104

Configuración para capturar paquetes SNMP.

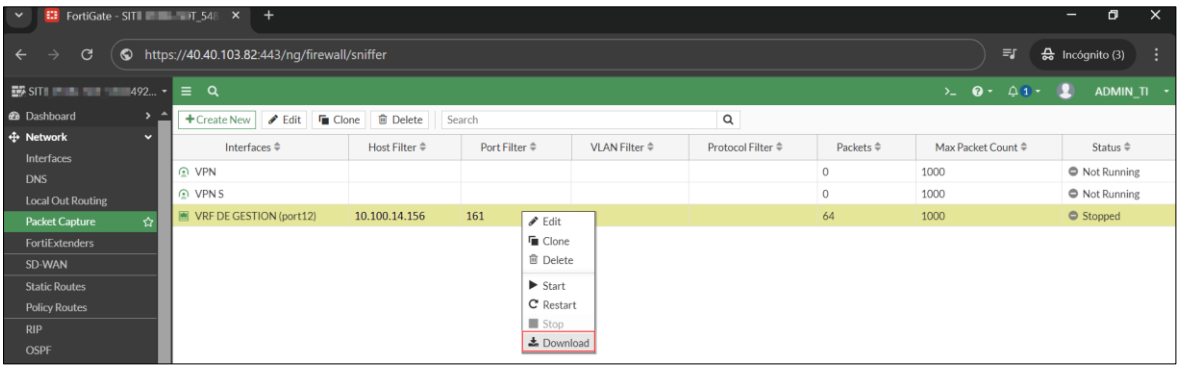


Nota: Plataforma de configuración del equipo firewall.

Luego de terminada la captura de paquetes SNMP, clic derecho en la fila donde se encuentra la interface VRF DE GESTION seleccionando "*Download*", tal como, se ve en la figura 105 para descargar de ese modo el archivo denominado "*SIT_SNMP.pcap*".

Figura 105

Descarga del archivo que contiene los paquetes capturados.

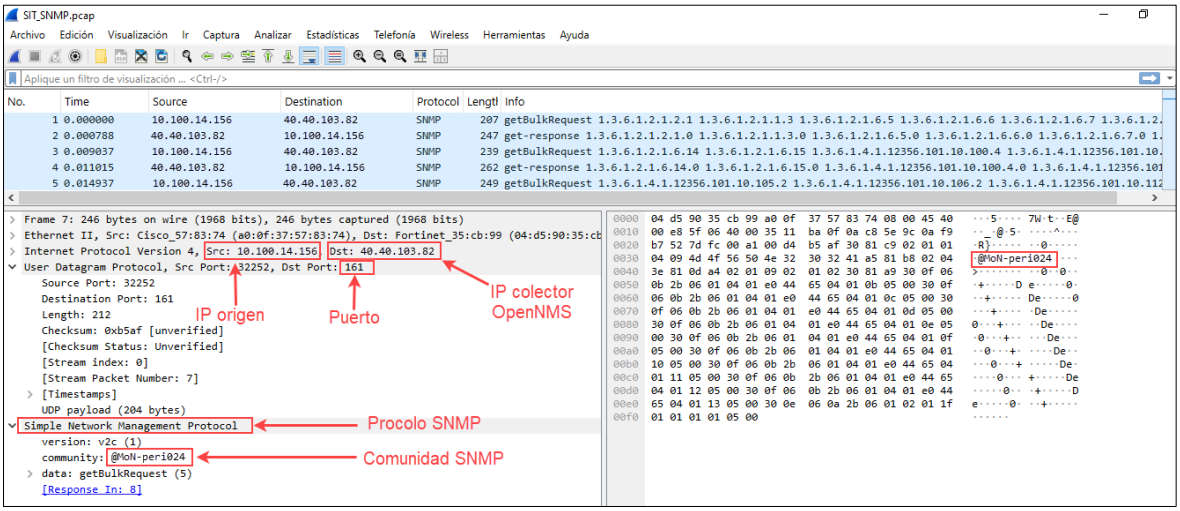


Nota: Plataforma de configuración del equipo firewall.

El archivo “*SIT_SNMP.pcap*” que contiene los paquetes SNMP se abrió con el software Wireshark para un análisis de la trama de los paquetes. De acuerdo con la figura 106, se verificaron los parámetros de configuración del SNMP del nodo de seguridad perimetral los cuales son: el protocolo SNMP, la IP del colector OpenNMS, la IP de origen la cual pertenece al firewall, la comunidad SNMP y el puerto 161 de transmisión.

Figura 106

Análisis del paquete SNMP con el software Wireshark.



Nota: software Wireshark.

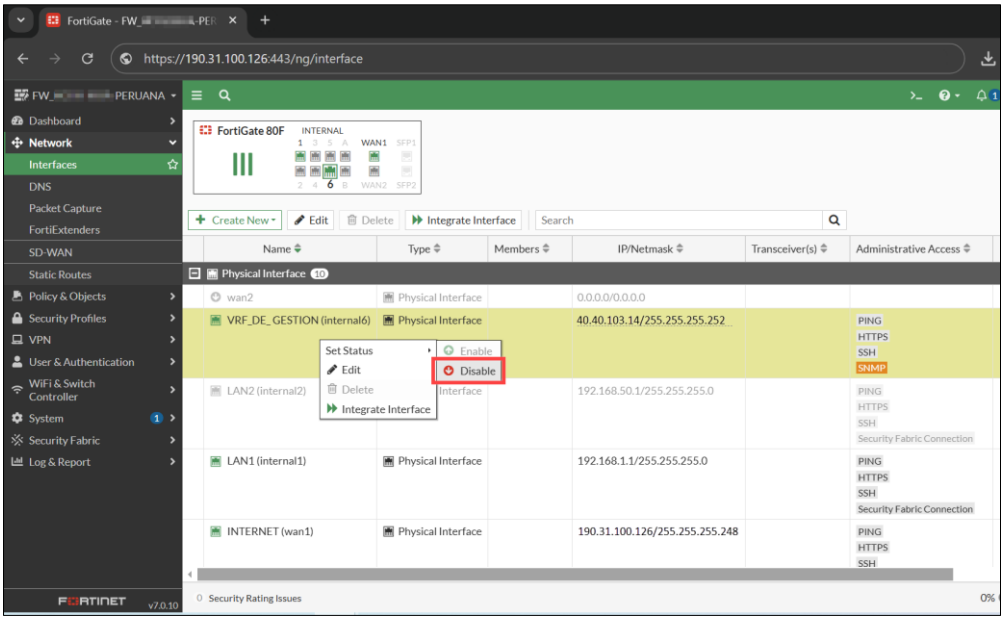
3.7.2 Pruebas de Alertas en el Dashboard de OpenNMS Horizon

Se realizó una prueba controlada, apagando y encendiendo la interface de gestión VRF del nodo de seguridad perimetral, observándose que las alertas del dashboard del OpenNMS indican los datos de la desconexión como nombre del nodo, nombre de la interfaz, dirección IP, horario de la caída, severidad, identificador del evento y un mensaje con la descripción del evento. Adicionalmente, se visualizaron gráficas que indican la conexión de los nodos de seguridad perimetral a lo largo del tiempo.

a) **Apagado de una Interface del Nodo de Seguridad Perimetral.** Se ingresó a la plataforma de configuración del nodo de seguridad perimetral – firewall luego a la sección Network y finalmente al apartado Interfaces, haciendo clic derecho en la interface VRF_DE_GESTION seleccionando la opción Disable, tal como, se ve en la figura 107 que deshabilita a la interface y dar inicio a la prueba.

Figura 107

Desconexión de la interface VRF de gestión del nodo de seguridad perimetral.

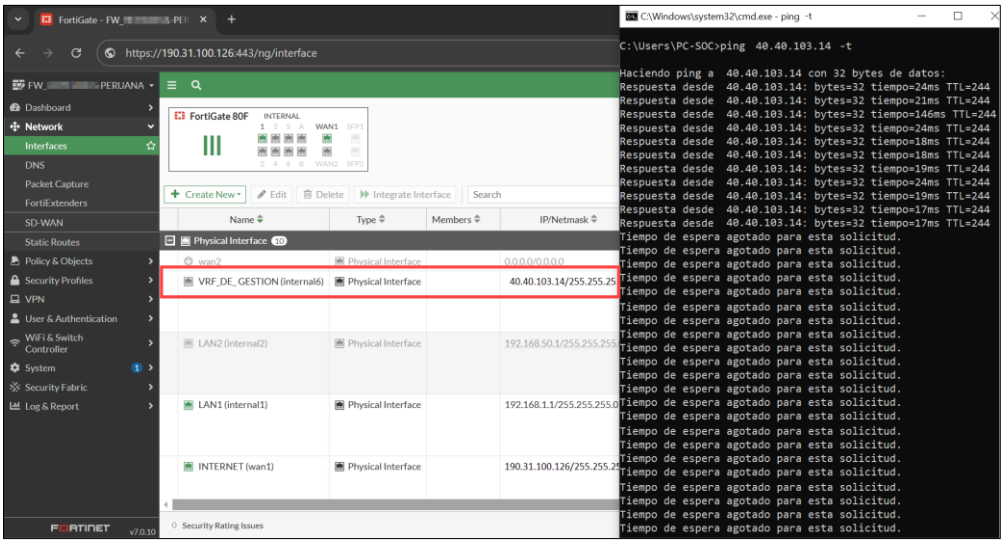


Nota: Plataforma de configuración del equipo firewall.

En la figura 108, se muestra cómo se efectúa el envío de paquetes ICMP desde un host del SOC hacia la IP 40.40.103.14 de la interface VRF, inicialmente hubo una respuesta, pero cuando se deshabilitó la interface se registró la perdida de paquetes, lo cual, es una indicación que se produjo una desconexión con la interface.

Figura 108

Perdida de paquetes ICMP debido a la desconexión de la interface de VRF de gestión.

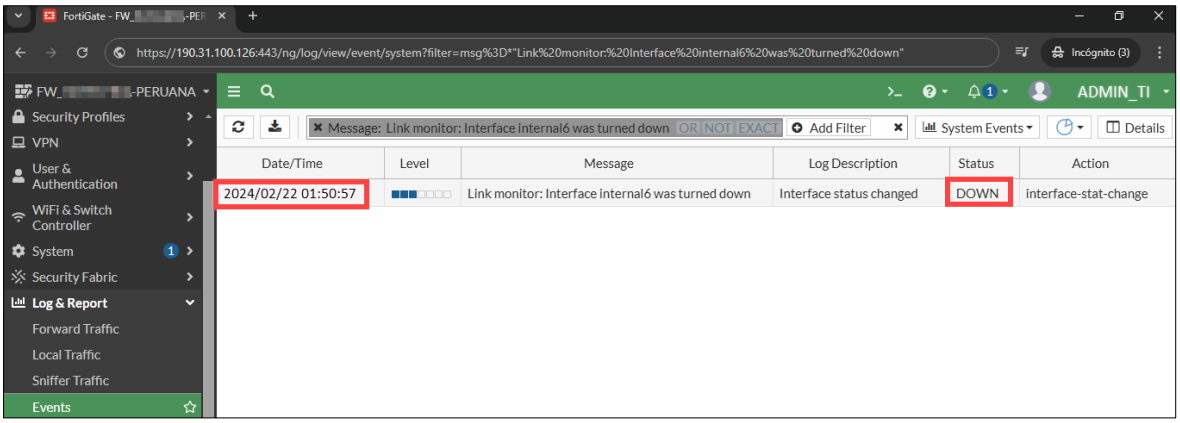


Nota: Plataforma de configuración del equipo firewall.

La hora de desconexión se registró en la sección Log & Report del nodo de seguridad perimetral, con un filtrado de la interface Internal 6, que se muestra en la figura 109, la hora y fecha, el 2024/02/22 01:50:57, indicando el estado DOWN de la interface, estos datos permiten analizar las alertas que generó la plataforma de OpenNMS Horizon.

Figura 109

Evento de desconexión en la plataforma de configuración del firewall.

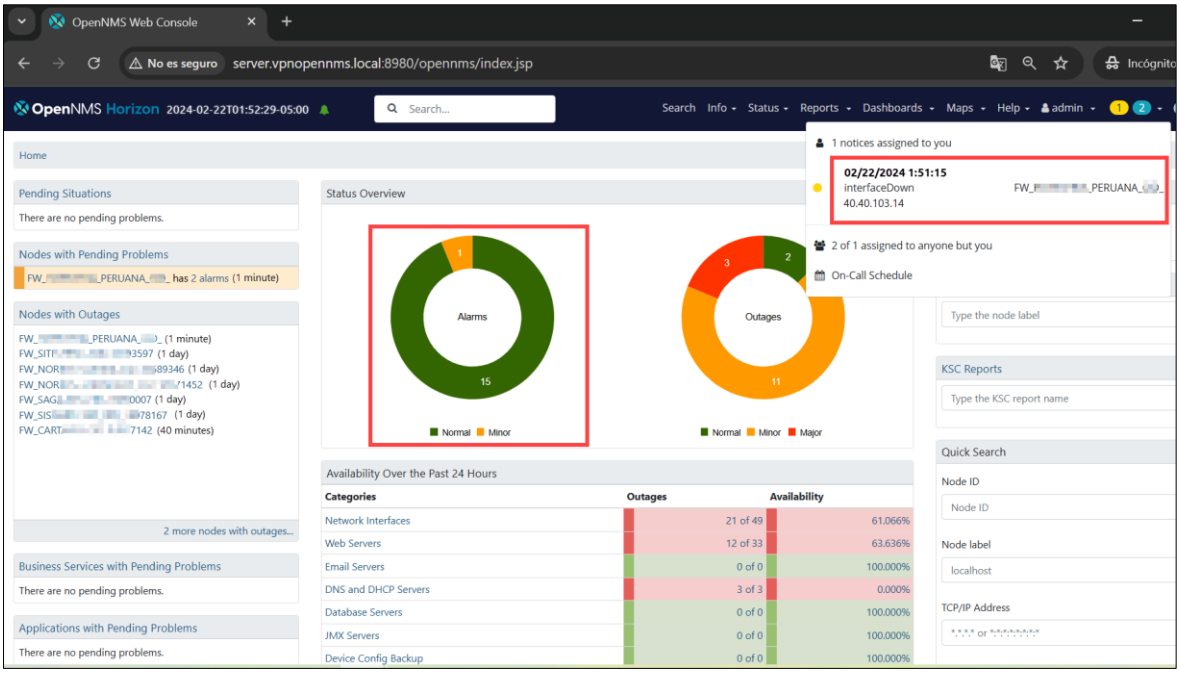


Nota: Plataforma de configuración del equipo firewall.

b) Registro de Apagado de la Interface en el Dashboard de la Plataforma OpenNMS. En la página principal de la plataforma de OpenNMS Horizon, se puede visualizar la alarma de desconexión y una notificación que indica el nombre del nodo de seguridad perimetral que se desconectó, la dirección IP de la interface, la fecha y hora, en este caso es 02/22/2024 1:51:15, tal como, se indica en la figura 110. Adicionalmente, se pudo verificar que a la plataforma OpenNMS Horizon le tomo un tiempo de respuesta de 18 segundos, para que alertara sobre la desconexión del nodo de seguridad perimetral.

Figura 110

Notificación de desconexión en la plataforma de OpenNMS.

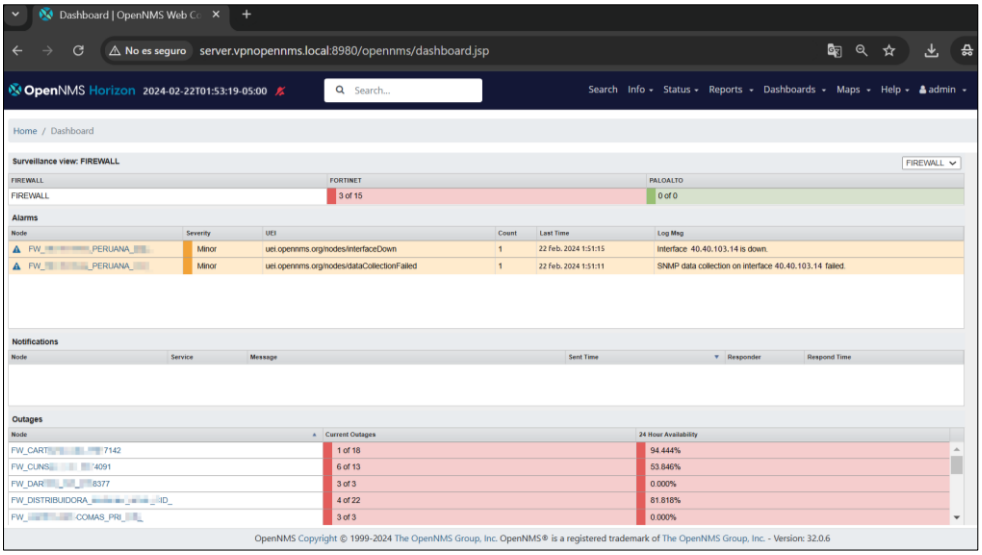


Nota: plataforma OpenNMS Horizon.

En el dashboard de la plataforma OpenNMS, en la vista de vigilancia FIREWALL se pudo verificar la alerta de desconexión del nodo de seguridad perimetral, tal como, se indica en la figura 111, donde se indica que nodos de seguridad perimetral están siendo alertados, la marca del nodo de seguridad perimetral, su severidad y el mensaje del log. En este caso, se indicó con una severidad "*Minor*" que una parte del nodo de seguridad perimetral está siendo alertada, en este caso la interface de VRF de gestión, en tanto que las otras interfaces no experimentan problemas.

Figura 111

Dashboard de la plataforma OpenNMS Horizon indicando alertas.

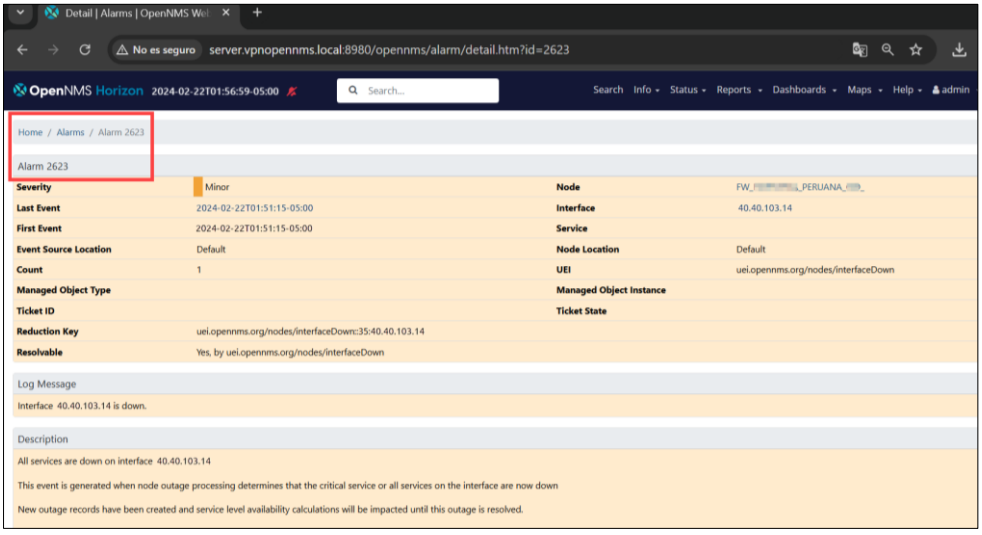


Nota: plataforma OpenNMS Horizon.

En el menú Status, sección Alarm alarma 2623, como se ve en la figura 112, donde se verifican detalles de la alarma, como nombre del nodo de seguridad perimetral, interface afectada, dirección IP de la interface, grado de severidad y una descripción que indica que todos los servicios de esta interface están desactivados y que el nodo se encuentra activo.

Figura 112

Alarma que notifica sobre la desconexión de una interface.

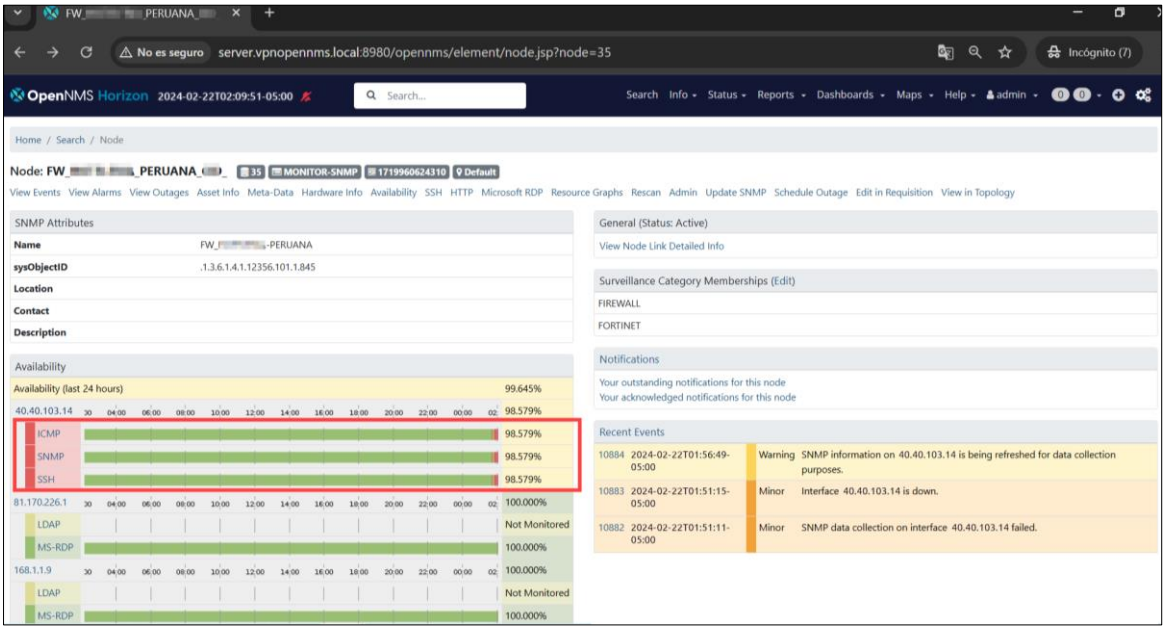


Nota: plataforma OpenNMS Horizon.

Finalmente, en el menú Search, sección Node se seleccionó el nodo de seguridad perimetral con la interface apagada, verificándose en la gráfica de línea de tiempo de las interfaces acerca de una desconexión en la interface 40.40.103.14 representada con el color rojo y que los servicios ICMP, SNMP y SSH están desconectados lo que se indica con un sombreado de color rojo, como puede verse en la figura 113. Las interfaces y servicios activos están representados por el color verde, así mismo, en esta ventana se visualizaron eventos recientes relacionados con este nodo de seguridad perimetral.

Figura 113

Gráfica de la linea de tiempo, que indica la desconexión de una interface.

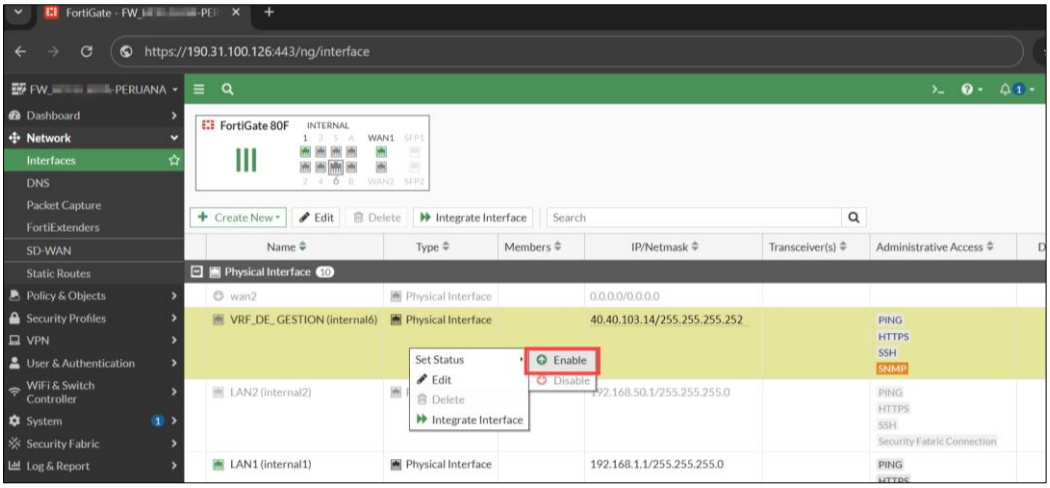


Nota: plataforma OpenNMS Horizon.

c) Encendido de la Interface del Nodo de Seguridad Perimetral. En la plataforma de configuración del nodo de seguridad perimetral – firewall, sección Network, apartado Interfaces, clic derecho en la interface VRF_DE_GESTION, seleccionando la opción Enable, como se observa en la figura 114 habilitando la interface para iniciar la prueba.

Figura 114

Conexión de la interface VRF de gestión del nodo de seguridad perimetral.

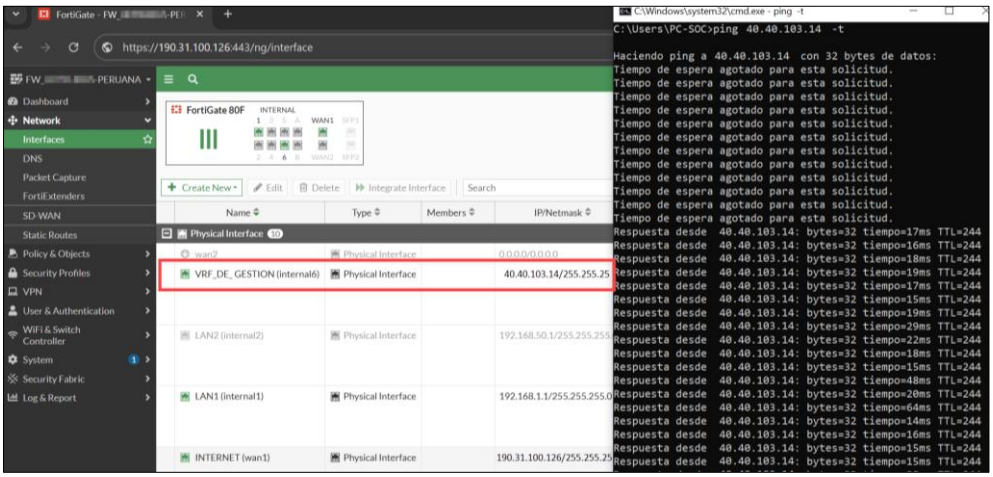


Nota: Plataforma de configuración del equipo firewall.

En la figura 115 se muestra el envío de paquetes ICMP efectuado desde un host del SOC a la dirección IP 40.40.103.14 de la interface VRF, inicialmente no hubo respuesta, pero al habilitar la interface se obtuvo la respuesta de los paquetes, indicando con ello, que se conectó a la interface.

Figura 115

Recepción de paquetes ICMP, mediante la conexión con la interface VRF de gestión.



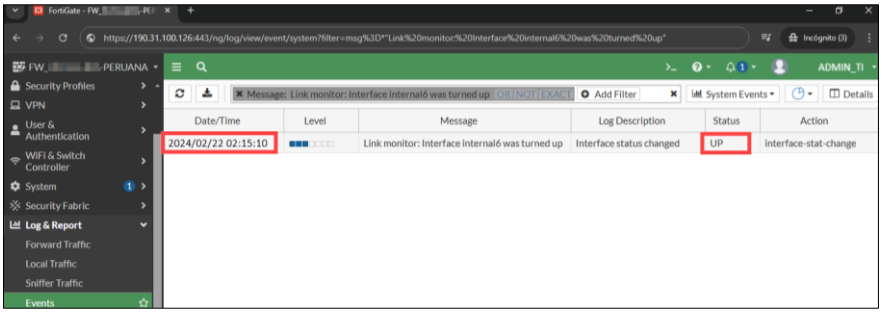
Nota: Plataforma de configuración del equipo firewall.

La hora de conexión fue registrada en la sección Log & Report del nodo de seguridad perimetral, realizándose un filtrado de la interface Internal 6, tal como, se muestra en la figura 116, verificándose la fecha y hora del evento registrado el 2024/02/22

02:15:10 que indica el estado UP de la interface, mediante estos datos se analizan las alertas generadas en la plataforma de OpenNMS Horizon.

Figura 116

Registro del evento de conexión en la plataforma de configuración del firewall.

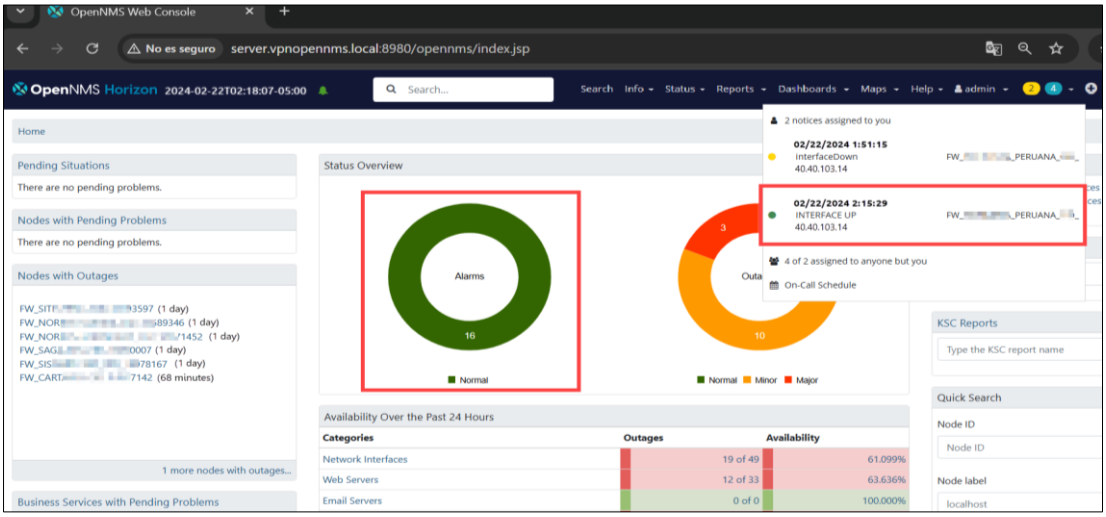


Nota: Plataforma de configuración del equipo firewall.

d) Registro del Encendido de la Interface en el Dashboard de la Plataforma OpenNMS. En la ventana principal de la plataforma de OpenNMS Horizon se visualizó la alarma de desconexión con una notificación que indica el nombre del nodo de seguridad perimetral que tuvo la desconexión, dirección IP de la interface, su fecha y hora, para este caso fue el 02/22/2024 2:15:29 como se indica en la figura 117. Se verificó que la plataforma OpenNMS Horizon tuvo un tiempo de respuesta de 19 segundos para que pueda alertar sobre la desconexión del nodo de seguridad perimetral.

Figura 117

Página principal de la plataforma de OpenNMS, notificando una conexión.

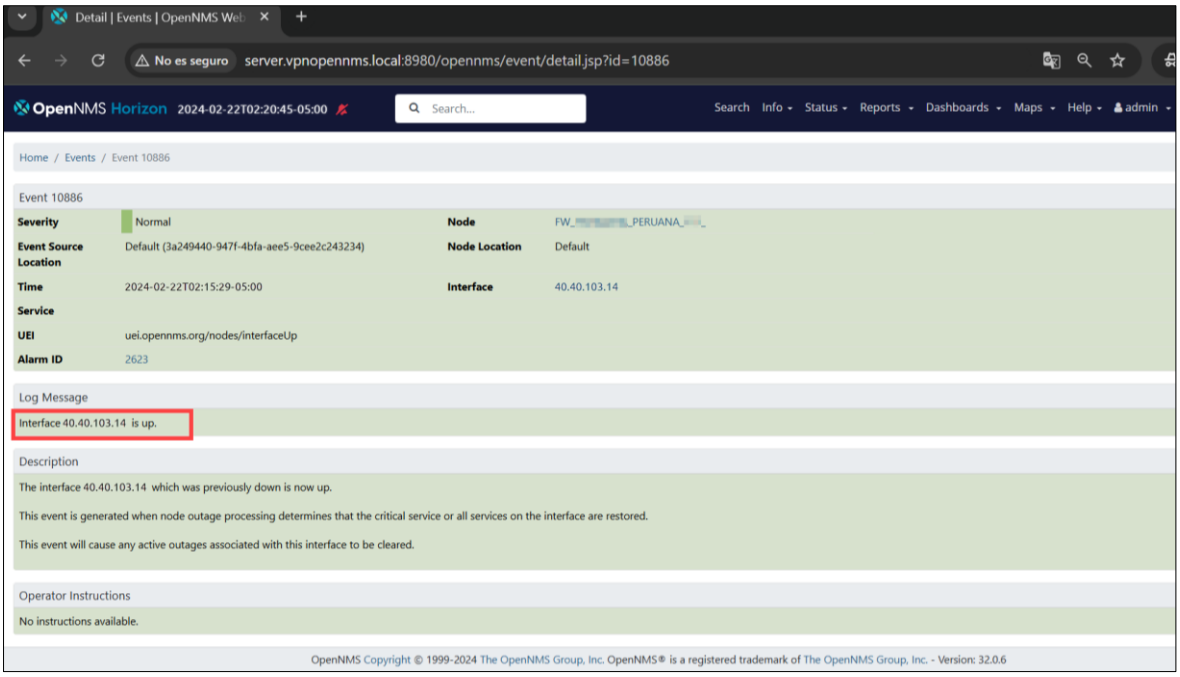


Nota: plataforma OpenNMS Horizon.

En el menú Status, sección Events evento 10886, tal como, se indica en la figura 118 verificándose los detalles del evento como el nombre del nodo de seguridad perimetral, interface afectada de la UP, dirección IP de su interface, grado de severidad del evento, descripción que indique que todos los servicios de interface están activados y si el nodo se encuentra activo.

Figura 118

Evento notificando la conexión de una interface.

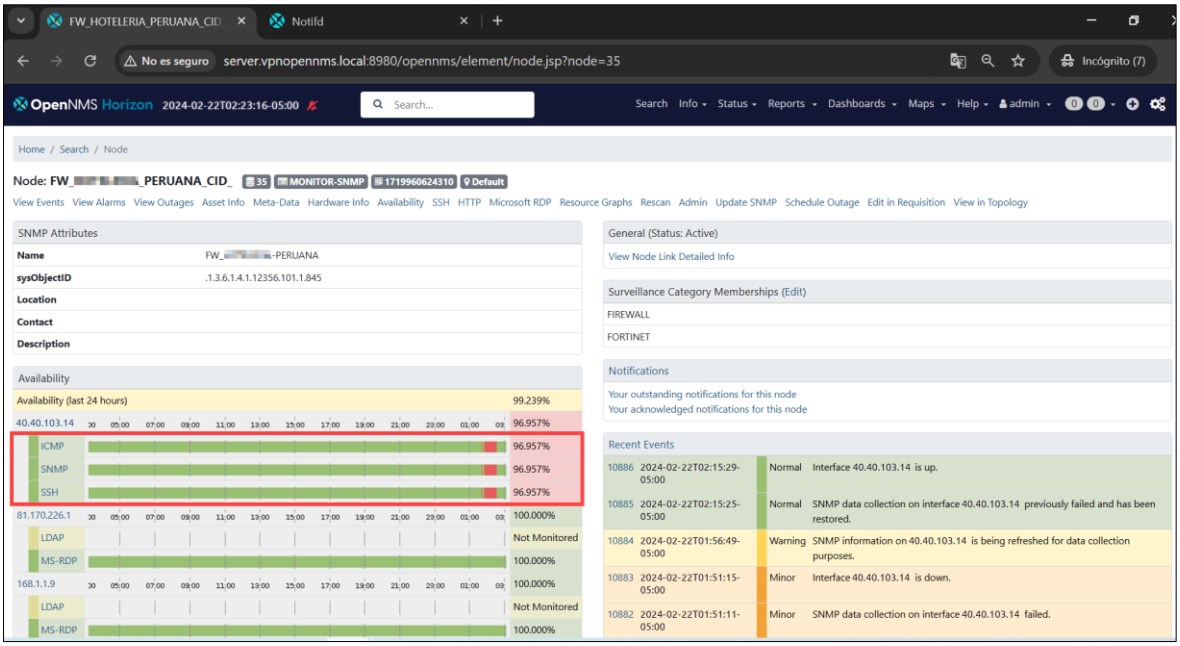


Nota: plataforma OpenNMS Horizon.

En el menú Search, sección Node seleccionándose el nodo de seguridad perimetral con la interface encendida, verificándose en la gráfica de línea de tiempo de las interfaces, conexión en la interface 40.40.103.14 representada con el color verde y la conexión de los servicios ICMP, SNMP y SSH sombreados en color verde, tal como, puede verse en la figura 119. Las otras interfaces y servicios activos están representados por el color naranja, así mismo, en esta ventana se visualizaron los últimos eventos relacionados a este nodo de seguridad perimetral.

Figura 119

Gráfica de la linea de tiempo, que indica la conexión de una interface.

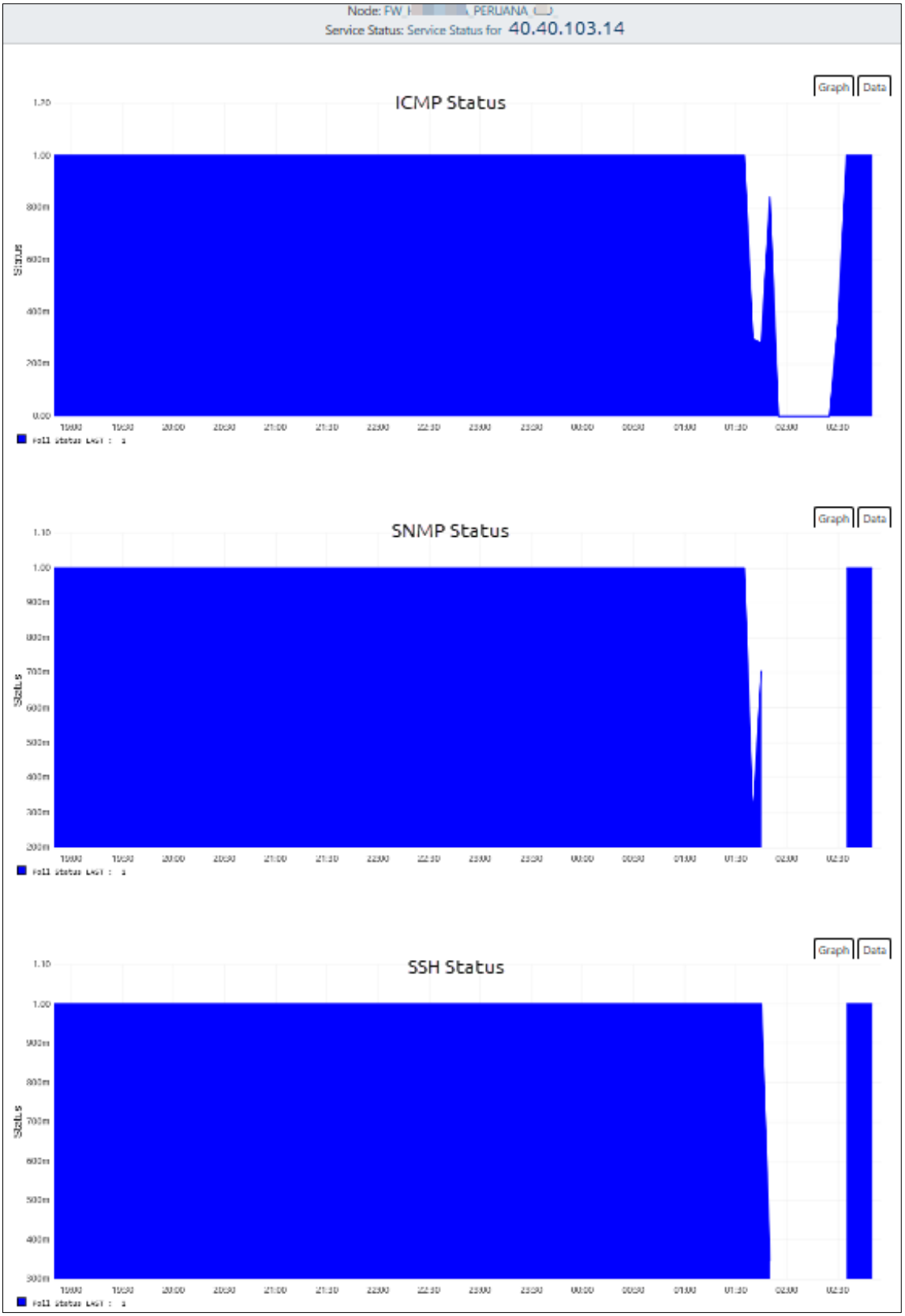


Nota: plataforma OpenNMS Horizon.

Finalmente se generó una gráfica de línea de tiempo, tal como, se visualiza en la figura 120, en la cual se observa la disponibilidad de la interface VRF como los servicios ICMP, SNMP y SSH. En el eje vertical se tuvo un valor de 1 lo cual se indica como un 100% de disponibilidad hasta que se produzca la desconexión de la interface VRF lo que se indica con el valor de 0 y cuando se logre la reconexión de la interface con el valor de 1.

Figura 120

Gráfica de disponibilidad de la interface VRF durante las pruebas.



Nota: plataforma OpenNMS Horizon.

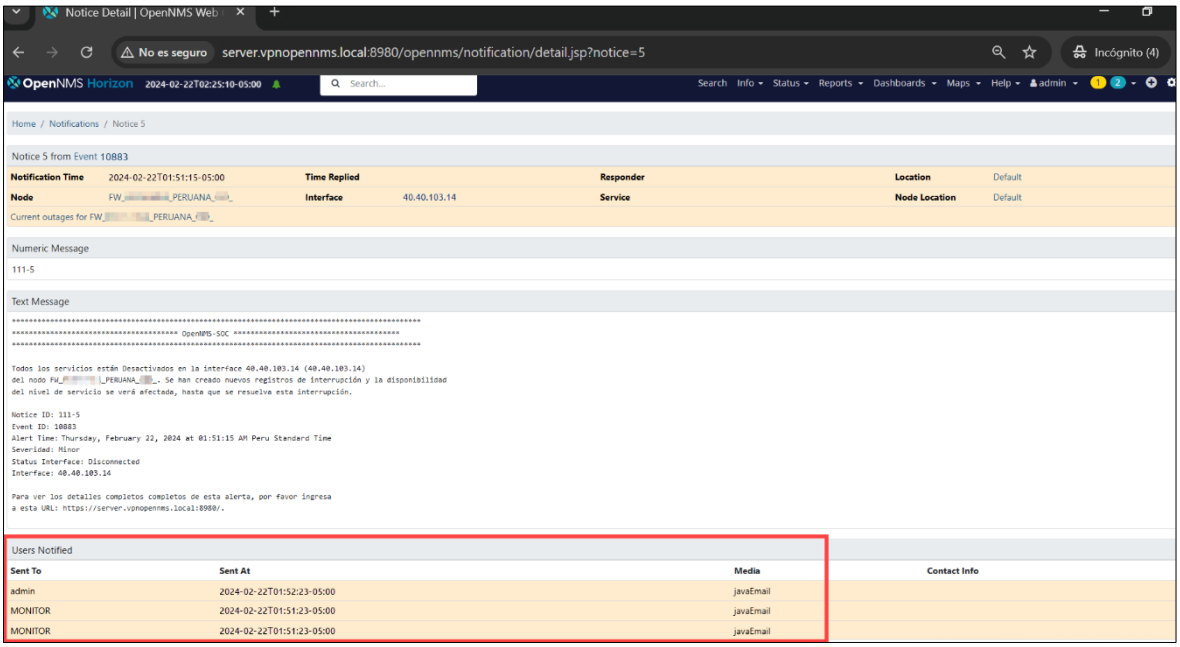
3.7.3 Pruebas de Envío de Alertas por Correo Electrónico

Para realizar estas pruebas se ejecutaron los eventos de conexión y desconexión de la interface VRF de gestión del nodo de seguridad perimetral, explicado detalladamente en el apartado 3.7.2. al producirse estos eventos, el software OpenNMS envía mensajes por correo electrónico al personal del SOC, notificando el apagado y encendido de una interface, así como, el nombre del nodo, nombre de la interfaz, dirección IP, hora de la caída, grado de severidad, identificador del evento y un mensaje que describa el evento.

a) Envío de la Notificación por Correo Electrónico de la Alerta de Desconexión de la Interface del Nodo de Seguridad Perimetral. El software OpennNMS Horizon al momento de registrar un evento de desconexión de la interface VRF de gestión (IP 40.40.103.14) procede a enviar una notificación por correo electrónico al personal del SOC, tal como, se visualiza en la figura 121 indicando los usuarios como la hora que se les envió el correo electrónico.

Figura 121

Evento que registra la desconexión de la interface y el envío del correo electrónico.



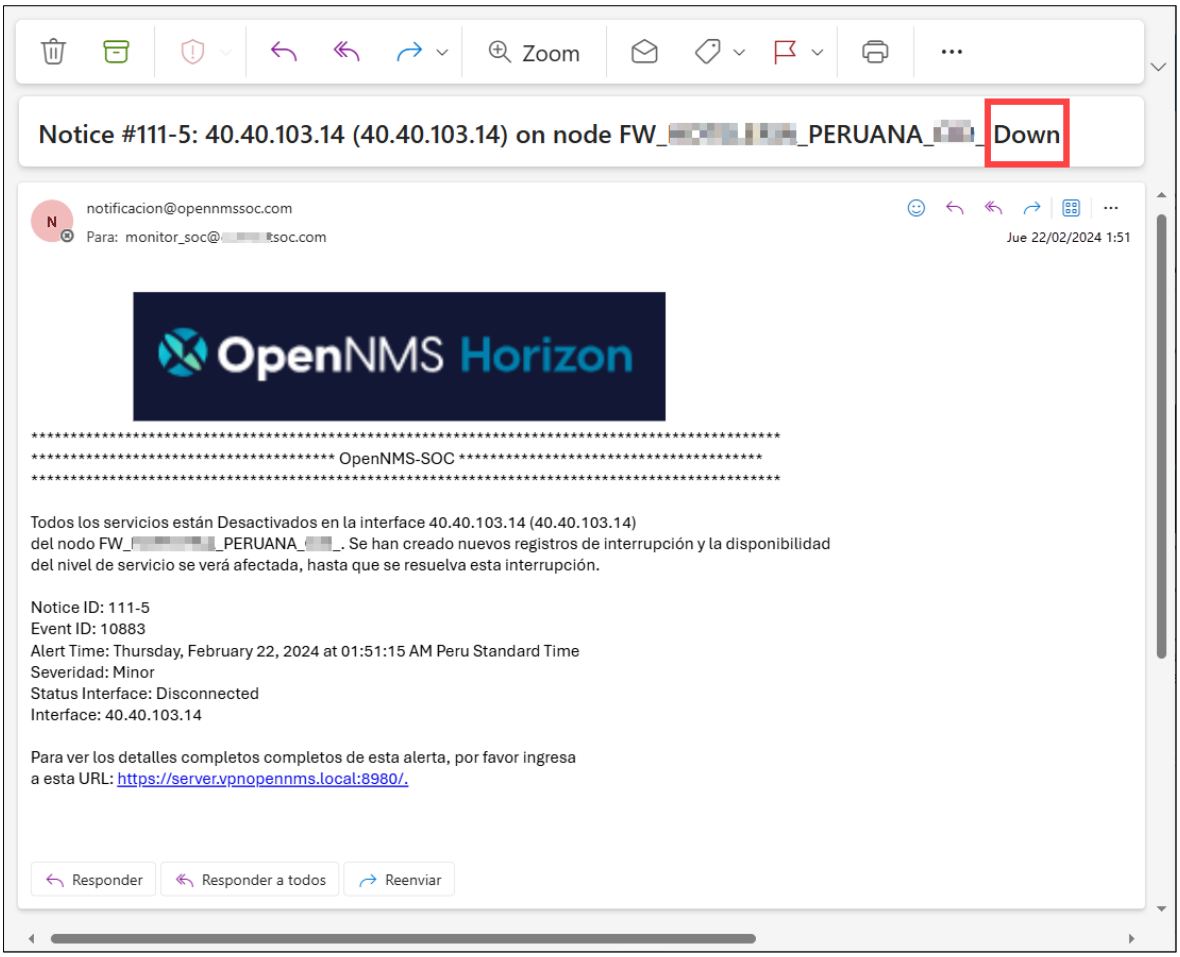
Nota: plataforma OpenNMS Horizon.

La figura 122, muestra la bandeja de entrada, de la cuenta monitor_soc@*******soc.com perteneciente al SOC de la Empresa de Telecomunicaciones

recibir un correo cuyo remitente es remitente@opennmssoc.com el cual pertenece a la plataforma OpenNMS Horizon en el cual se notifica que se ha producido una desconexión de la interface VRF de gestión (IP 40.40.103.14) del nodo de seguridad perimetral, hora en la cual se produjo el evento, severidad Minor del evento y la URL: https://server.vpnopennms.local:8980/ de la plataforma OpenNMS, información con la cual el personal del SOC analiza el evento y ejecutar las acciones correctivas pertinentes.

Figura 122

Correo electrónico acerca de la desconexión de la interface VRF de gestión del firewall.



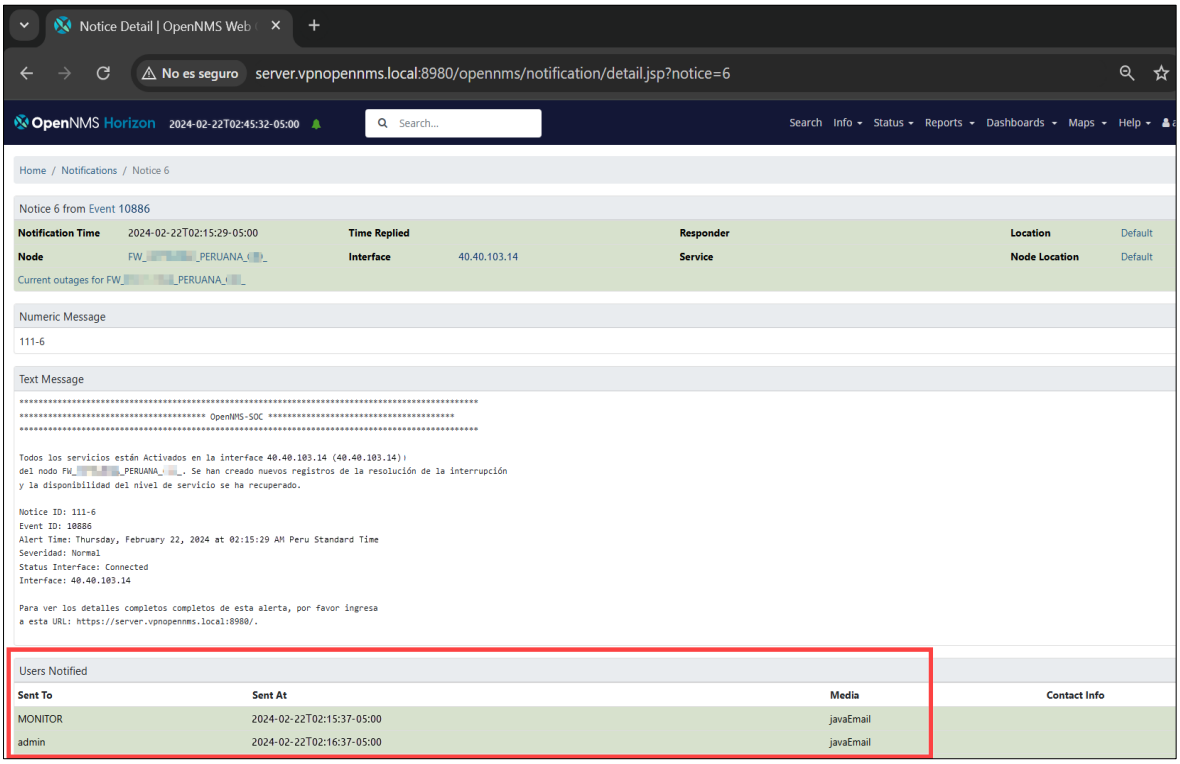
Nota: software de correo electrónico Outlook.

b) Envío de Correo Electrónico Notificando y Alertando de una Conexión de Interface del Nodo de Seguridad Perimetral. El software OpennNMS Horizon una vez que registró una conexión de la interface de VRF de gestión (IP 40.40.103.14) procede a

enviar la notificación por correo electrónico al personal del SOC, tal como, se muestra en la figura 123 indicando a los usuarios y hora que se envió del correo electrónico.

Figura 123

Evento que registra la conexión de la interface y el envío del correo electrónico.

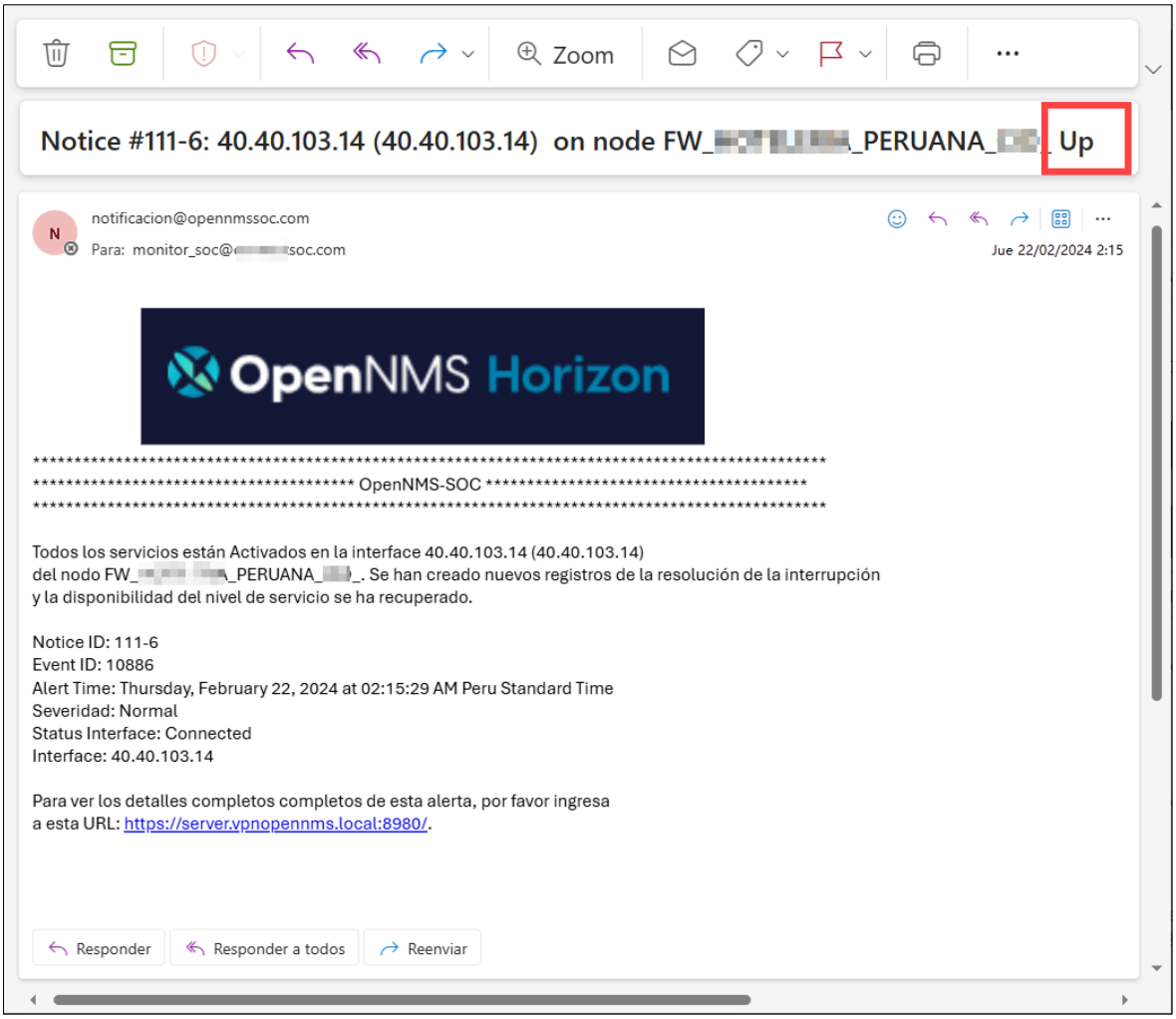


Nota: plataforma OpenNMS Horizon.

En la figura 124, se muestra haber recibido un correo electrónico en la bandeja de entrada de la cuenta monitor_soc@*******soc.com perteneciente al SOC de la Empresa de Telecomunicaciones, el remitente de este correo es notificacion@opennmssoc.com que pertenece a la plataforma OpenNMS Horizon en el cual notifica la conexión de la interface VRF de gestión (IP 40.40.103.14) del nodo de seguridad perimetral y la hora que se produjo el evento, severidad Normal del evento y la URL: https://server.vpnopennms.local:8980/ de la plataforma OpenNMS mediante el cual el personal del SOC realizó un análisis del evento.

Figura 124

Correo electrónico indicando conexión de la interface VRF de gestión del firewall.



Nota: software de correo electrónico Outlook.

Finalmente se verificó que el software OpenNMS envió notificaciones de los eventos por correo electrónico hacia el correo destino del SOC de la Empresa de Telecomunicaciones, con lo cual, indica su correcta operación.

Capítulo IV. Análisis y discusión de resultados

La implementación del software de monitoreo OpenNMS Horizon en el SOC de la Empresa de Telecomunicaciones permite monitorear los equipos de seguridad perimetral de los clientes corporativos de la Empresa, lo cual resulta en el correcto funcionamiento en las pruebas de operación.

En el presente Informe de Suficiencia Profesional, se expone como fueron cumplidos los cuatro objetivos específicos propuestos inicialmente.

4.1 Cumplimiento del Primer Objetivo Especifico

Se procedió a analizar y evaluar los distintos programas de software de monitoreo de dispositivos de red basados en los protocolos ICMP y SNMP resultando en la selección del software OpenNMS el cual cumple satisfactoriamente con las características y funcionalidades requeridas por el SOC de la Empresa de Telecomunicaciones:

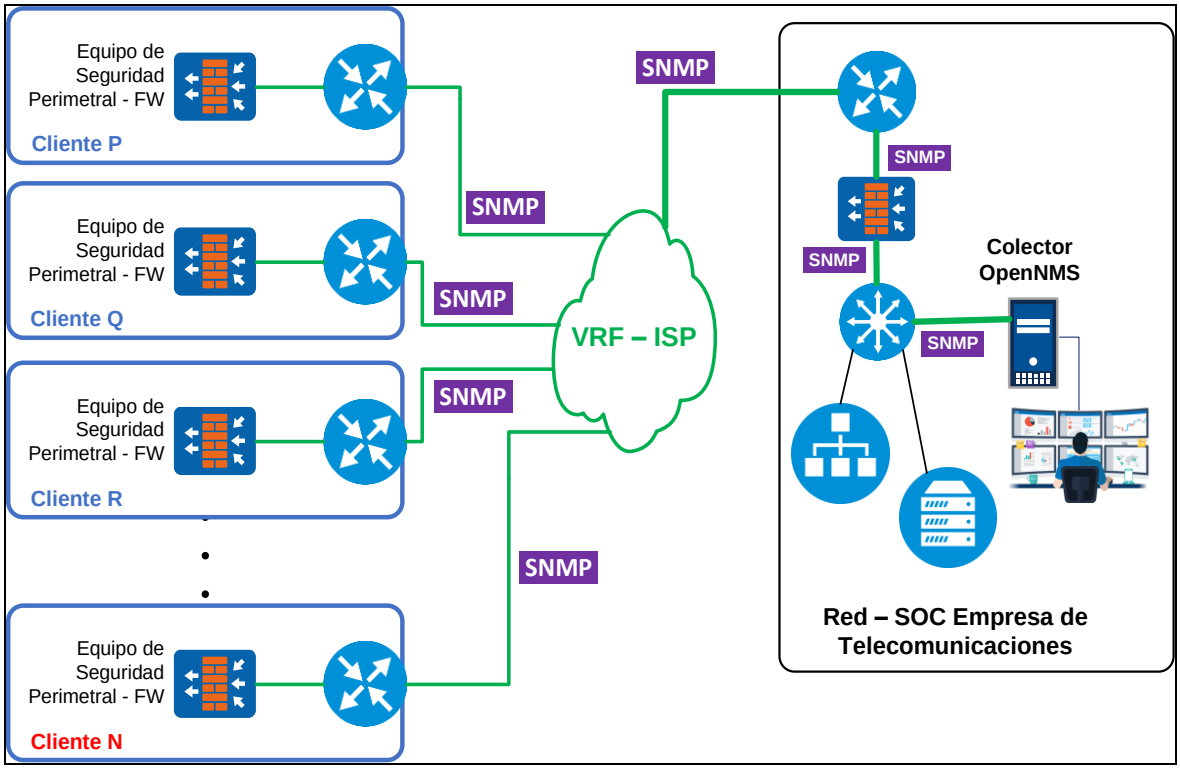
- Software de monitoreo basado en el protocolo SNMP para recolectar información acerca de la capacidad operativa de los nodos de seguridad perimetral.
- Niveles de alertas categorizadas de acuerdo al nivel de severidad.
- Visibilidad de las interfaces de los nodos de seguridad perimetral.
- Software de monitoreo escalable e individualizable acerca de las gráficas de rendimiento, reportes y alertas.
- Interfaz gráfica de fácil presentación y operación proporcionando a los ingenieros de seguridad una herramienta que les permite tomar decisiones oportunas.
- Envío de alertas por correo electrónico en tiempo real.
- Mínimo costo de implementación del software de monitoreo.
- Software escalable.

En conformidad con lo expuesto anteriormente se eligió el software OpenNMS, basado en licencia de software libre que implementa el protocoló SNMP para monitorear

los equipos de seguridad perimetral, en la figura 125 se puede visualizar el diagrama del software OpenNMS de los equipos monitoreados.

Figura 125

Diagrama de monitoreo de los nodos de seguridad perimetral con el software OpenNMS.



Nota. Elaboración propia, basada en la arquitectura de monitoreo de OpenNMS, https://www.opennms.com.

La implementación del software OpenNMS satisface el requerimiento de efectuarse a un mínimo costo de implementación, en las tablas 4, 5 y 6 se muestra detalladamente los costos parciales asociados al empleo de los recursos humanos, adquisición de equipos y licencias anuales para los softwares utilizados en la implementación del OpenNMS Horizon.

Tabla 4

Costos de los recursos humanos requeridos para implementar el OpenNMS Horizon.

Descripción	Cantidad	Tiempo (días)	Costo Unitario	Costo
Jefe del proyecto	1	6	S/. 250.00	S/. 1,500.00
Supervisor	1	15	S/. 125.00	S/. 1,875.00
Técnico de Soporte	1	24	S/. 100.00	S/. 2,400.00
Costo Total				S/. 5,775.00

Nota. Elaboración propia, basada en la estructura de costos de la empresa de Telecomunicaciones.

Tabla 5

Costos de implementar el hardware que ha de ejecutar el software OpenNMS Horizon.

Descripción	Cantidad	Costo Unitario	Costo
Servidor	1	S/. 7,500.00*	S/. 7,500.00
Costo total			S/. 7,500.00

*Nota: Elaboración propia, basada en cotizaciones de la empresa de Telecomunicaciones. * Se considera el 40% del costo del servidor, debido a que el SOC ya contaba con este equipo.*

Tabla 6

Costos de software para la implementación de OpenNMS.

Descripción	Cantidad	Costo Unitario (anual)	Costo
Licencia OpenNMS	1	S/. 0.00	S/. 0.00
Licencia Ubuntu 22.4	1	S/. 0.00	S/. 0.00
Licencia Microsoft Office 2020	1	S/. 565.00	S/. 565.00
Licencia Windows 11	1	S/. 200.00	S/. 200.00
Licencia VMware vSphere*	1	S/. 5,423.00	S/. 5,423.00
Costo Total			S/. 6,188.00

*Nota. Elaboración propia, **

https://www.deltron.com.pe/modulos/productos/items/producto.php?item_number=SWHPE8H73AAE.

En la tabla 7 se indica el costo total de la implementación del software de monitoreo OpenNMS el cual asciende a S/. 19,463.00 soles.

Tabla 7

Costo total de la implementación del software de monitoreo OpenNMS.

Concepto	Costo
Recursos Humanos	S/. 5,775.00
Costos de equipos	S/. 7,500.00
Costos de software	S/. 6,188.00
Total de Costos	S/. 19,463.00

Nota. Elaboración propia, basada en las Tablas 4, 5 y 6 del presente trabajo.

A continuación, se muestra un cuadro comparativo entre el costo total de implementación del software PRTG realizado el año 2023 y el costo de implementación del software OpenNMS, para ello se ha considerado el costo de adquisición de software en la implementación de la herramienta PRTG que se indica en la tabla 8, los costos de recursos

humanos como la adquisición de equipos que participaron en la implementación del software PRTG que tienen los mismos costos indicados en las tablas 4 y 5.

Tabla 8

Costos del software de implementación de la herramienta PRTG.

Descripción	Cantidad	Costo Unitario (anual)	Costo
Licencia PRTG (2500 sensores) *	1	S/ 30,857.19	S/ 30,857.19
Licencia Ubuntu 22.4	1	S/ 0.00	S/ 0.00
Licencia Microsoft Office 2020	1	S/ 565.00	S/ 565.00
Licencia Windows 11	1	S/ 200.00	S/ 200.00
Licencia VMware vSphere	1	S/ 5,423.00	S/ 5,423.00
TOTAL			S/ 37,045.19

*Nota. Elaboración propia, basada en * https://shop.paessler.com/shop/paessler-prtg-network-monitor-213#attr=.*

La implementación del software de monitoreo PRTG asciende a S/ 50,320.19 soles, tal como, se detalla en la tabla 9, el cual es superior al costo de implementación del software de monitoreo OpenNMS efectuado en el 2024 como se observa en la figura 126. La nueva implementación disminuye su costo en un 61.32% respecto al costo de implementación del software de monitoreo de nodos de seguridad perimetral del año 2023.

Agregado a lo anterior, su implementación superó la capacidad limitada al número relativo de equipos y aspectos a ser monitoreados, ya que el software PRTG estaba limitado a su máxima capacidad de supervisión limitada a 2500 aspectos con 2500 sensores, lo que no sucede con el software OpenNMS cuya ilimitada capacidad de supervisión y monitoreo de sus aspectos, como de sus nodos de seguridad perimetral.

Tabla 9

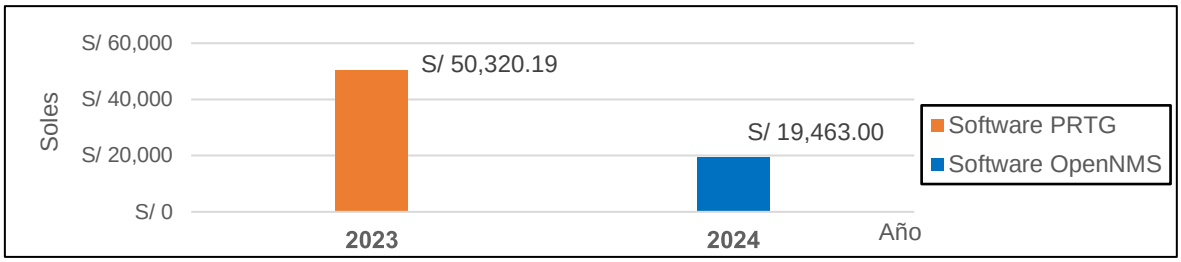
Costo total de la implementación del software de monitoreo PRTG.

Concepto	Costo
Recursos Humanos	S/ 5,775.00
Costos de equipos	S/ 7,500.00
Costos de software	S/ 37,045.19
Total de Costos	S/ 50,320.19

Nota. Elaboración propia, basada en las Tablas 4, 5 y 8 del presente trabajo.

Figura 126

Costos(en soles) de la implementación del software de monitoreo en el SOC.



Nota. El gráfico muestra los costos de implementación del software de monitoreo SOC de la Empresa de Telecomunicaciones. Elaboración propia, basada en las Tablas 7 y 9 del presente trabajo.

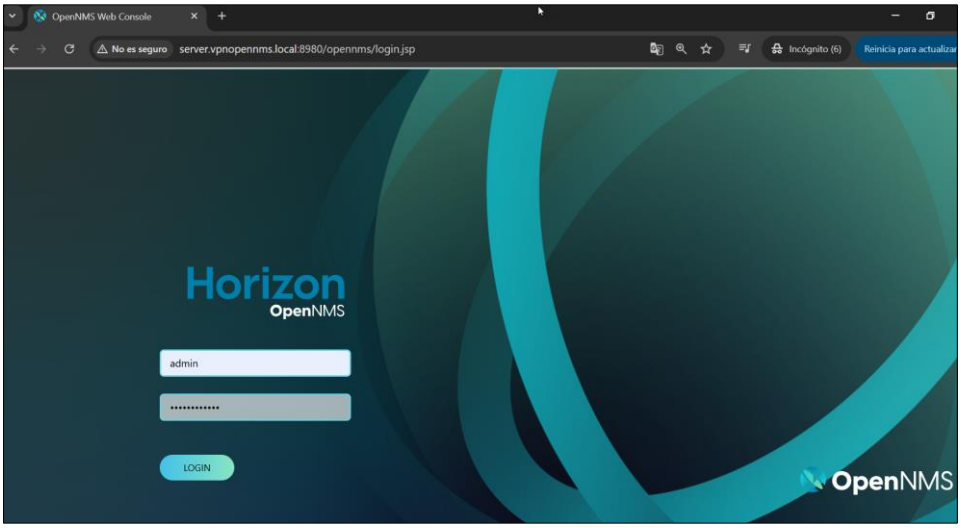
4.2 Cumplimiento del Segundo Objetivo Especifico

La implementación del software OpenNMS basado en open source en el SOC de la empresa de telecomunicaciones, se efectuó con el objetivo de monitorear los nodos de seguridad perimetral de los clientes corporativos gestionados por la Empresa.

Se accede a la plataforma de monitoreo de OpenNMS, introduciendo el enlace http://server.vpnopennms.local:8980/opennms/login.jsp en el navegador de internet de un ordenador que esté conectado a la red del NOC de la empresa, luego se deben introducir las credenciales de usuario respectivas, tal como, se puede observar en la figura 127.

Figura 127

Interfaz del software de monitoreo OpenNMS.

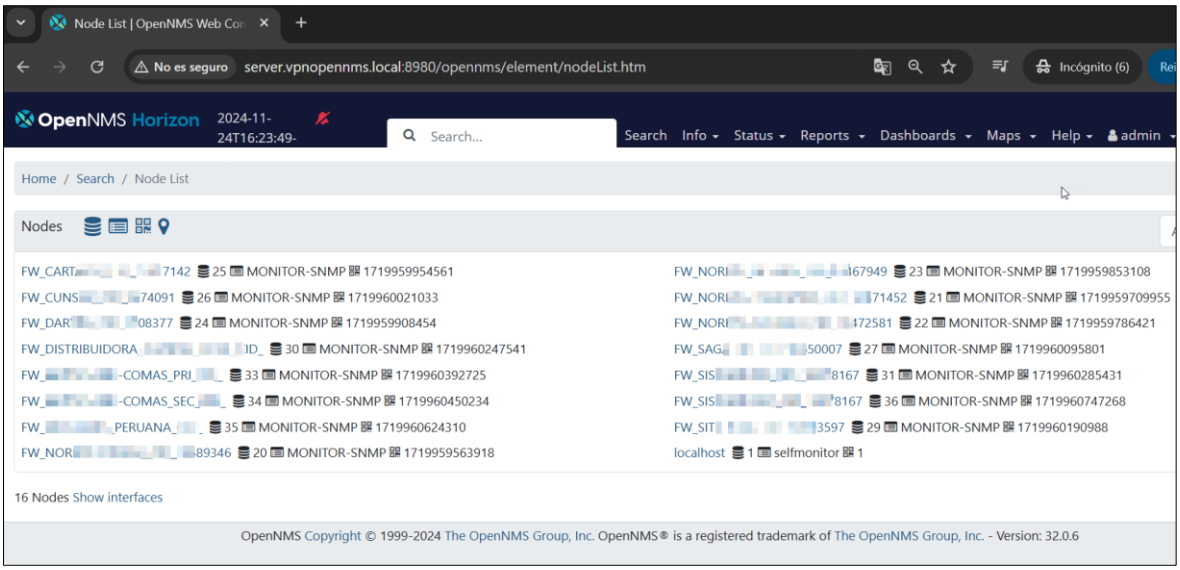


Nota: Plataforma de OpenNMS Horizon.

En la interfaz del software OpenNMS, se visualizó el dashboard como el listado de los nodos de seguridad perimetral - firewall gestionados por la empresa, los cuales se agregaron y configuraron en el OpenNMS, tal como, se muestra en la figura 128. que muestra la gestión de su rendimiento, el monitoreo de sus interfaces y que frente a cualquier caída del servicio, se tomen las acciones necesarias que recuperen el servicio.

Figura 128

Nodos de seguridad perimetral agregados a la plataforma OpenNMS.



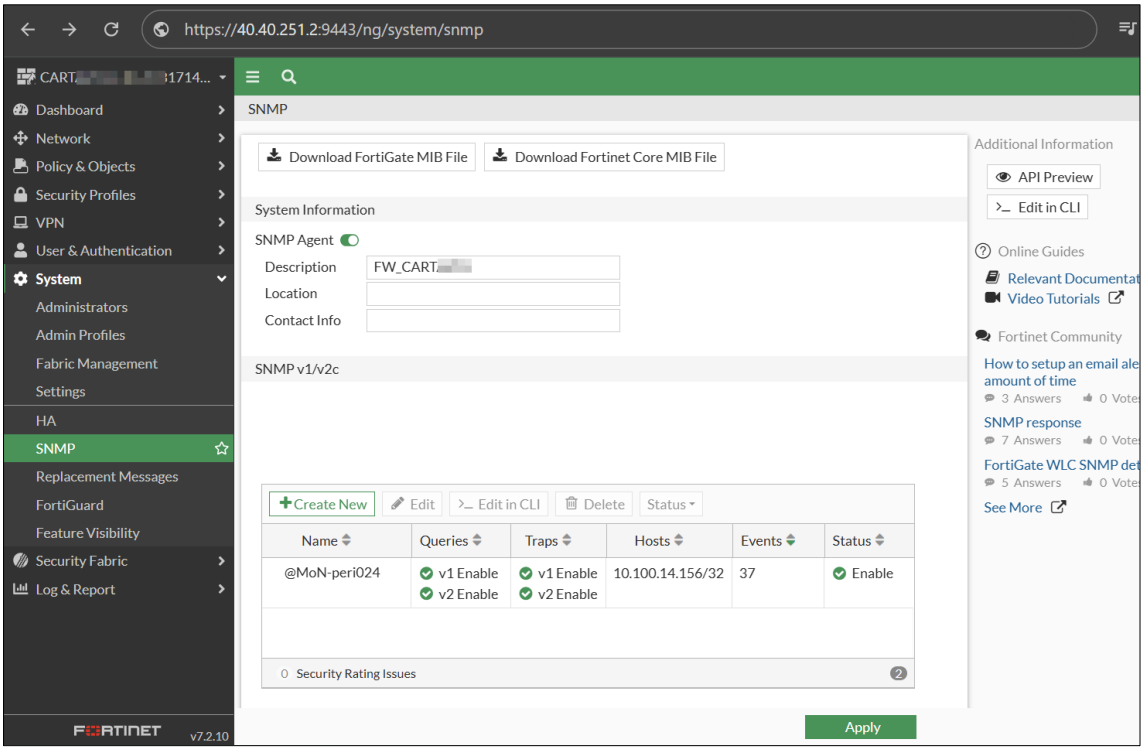
Nota: Plataforma OpenNMS.

4.3 Cumplimiento del Tercer Objetivo Especifico

Los nodos de seguridad perimetral - firewall fueron configurados con los datos del nombre de la comunidad SNMP, el IP 10.100.14.156/32 que pertenece al colector del software OpenNMS se presenta en la figura 129, mediante los cuales, los equipos firewall transmiten paquetes del protocolo SNMP v2c que contienen la información de red encaminada al colector del software OpenNMS Horizon.

Figura 129

Nodo de seguridad perimetral - firewall configurado conforme al Protocolo SNMP v2c.



Nota: Plataforma de configuración del equipo firewall.

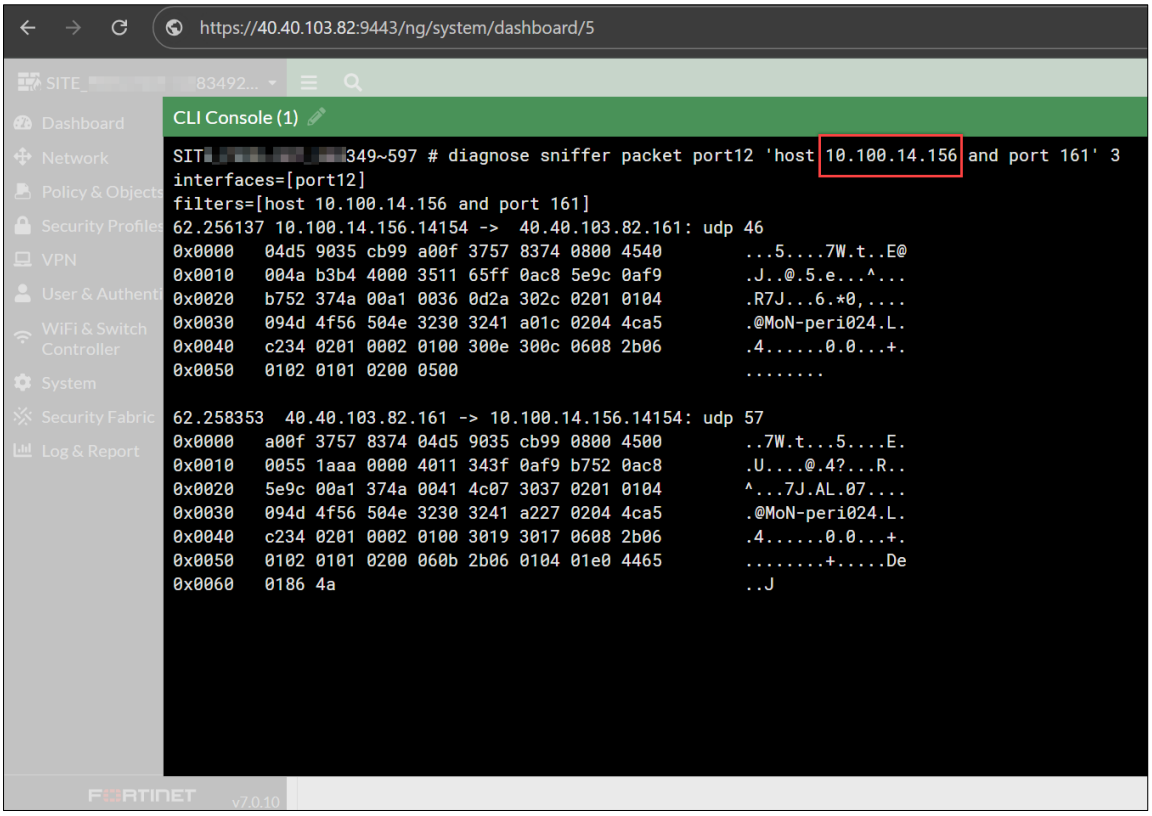
4.4 Cumplimiento del Cuarto Objetivo Especifico

Las pruebas como la supervisión efectuada al software de monitoreo OpenNMS fueron exitosas, las mismas que consistieron en:

- Pruebas de conectividad como ping, trace route, y captura de paquetes, pruebas en las cuales se verificaron los envíos de los paquetes SNMP desde un nodo de seguridad perimetral - firewall hacia el colector del software OpenNMS con IP 10.100.14.156 por el puerto 161, tal como, se observa en la figura 130, esta prueba fue efectuada en cada uno de los nodos agregados a la plataforma del OpenNMS.

Figura 130

Captura de paquetes SNMP hacia el colector del software OpenNMS.

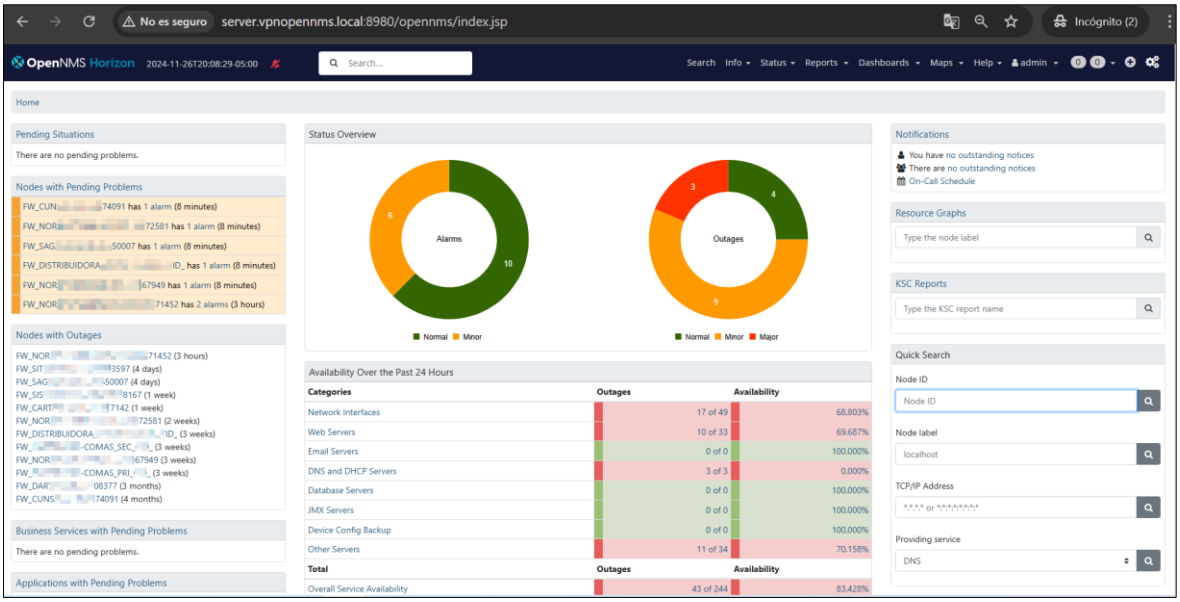


Nota: Plataforma de configuración del equipo firewall.

- Se efectuó la verificación de las alertas en el dashboard del software OpenNMS, las cuales están clasificadas según el grado de severidad, tal como, se puede apreciar en la figura 131, las alertas que tienen un grado intermedio son las que implican caída de alguna interface de un equipo firewall como se evidencia en la figura 132 donde se observa el nombre del equipo firewall, IP de gestión, interface apagada, la fecha y hora en la que ocurrió la desconexión de la interface.

Figura 131

Dashboard del OpenNMS indicando el nivel de severidad de las alarmas.

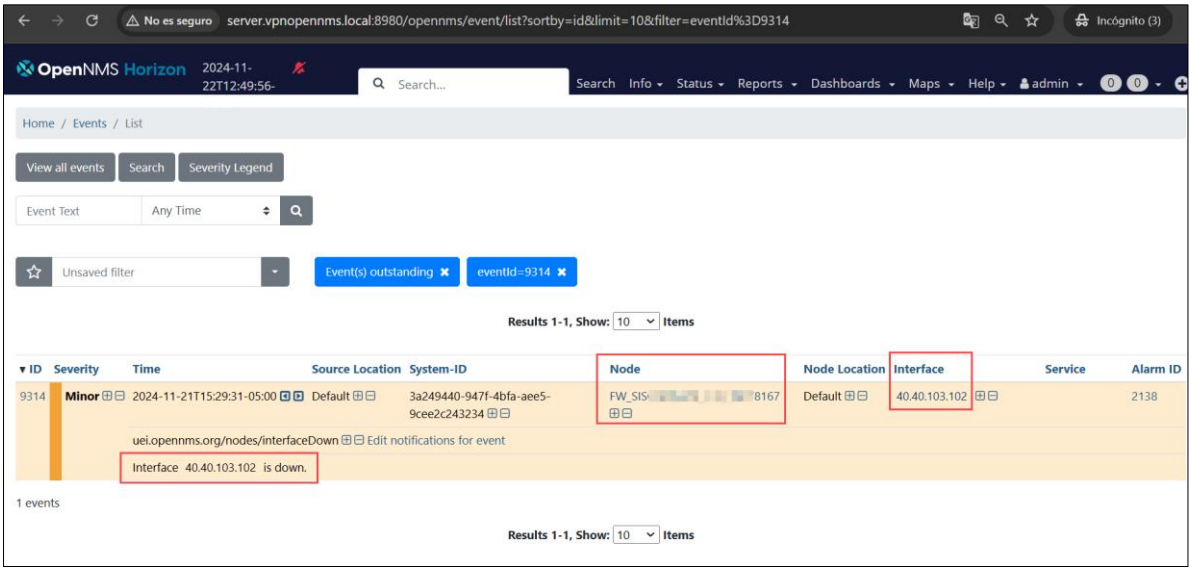


Nota: Plataforma OpenNMS Horizon.

La plataforma también permitió ejecutar filtros como se muestra en la figura 132 en la cual se ejecutaron filtros por tipo de evento, por identificador, por severidad, fecha y hora.

Figura 132

Alerta de la plataforma OpenNMS en la cual se indica el grado de severidad.

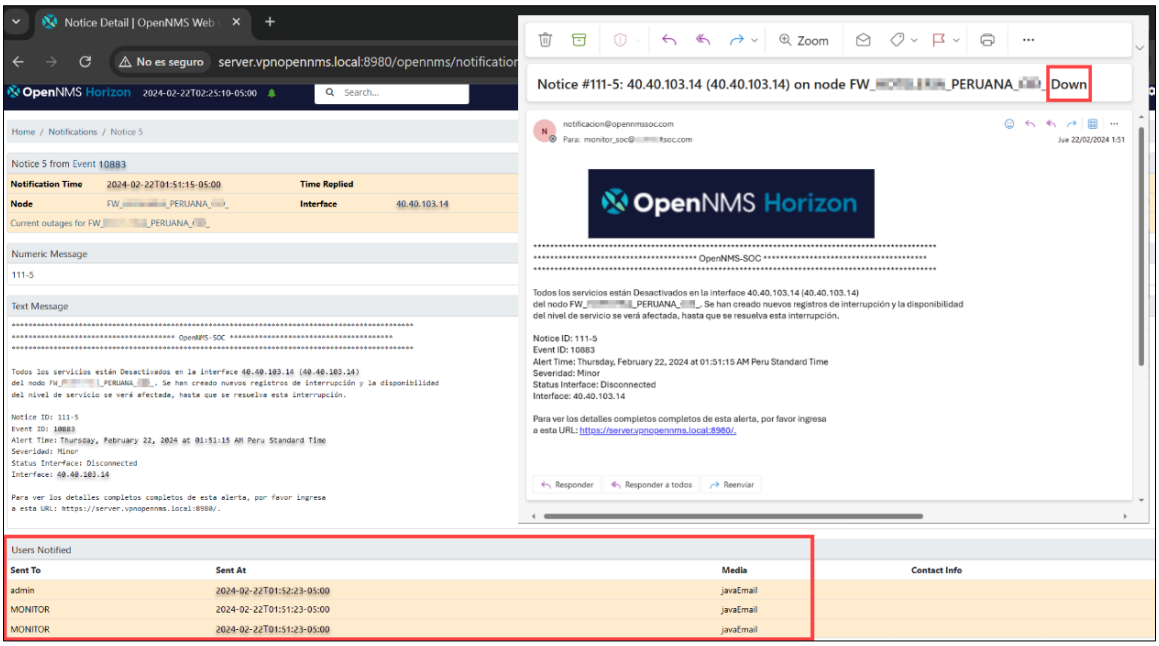


Nota: Plataforma OpenNMS Horizon.

- Adicionalmente, se verificó el envió de las alertas por correo electrónico en las cuales se indica la desconexión de la interface de un equipo firewall, a los ingenieros de soporte, para el análisis correspondiente del evento. Se adjunta la figura 133 en la cual se pone en evidencia el evento en la plataforma OpenNMS con su respectiva notificación de alerta enviada por correo electrónico.

Figura 133

Evento en la plataforma de OpenNMS y correo enviado al personal del SOC.



Nota: Plataforma OpenNMS Horizon.

- El tiempo promedio que transcurre desde el instante que se produce el evento en el nodo de seguridad perimetral hasta que la notificación llega a la bandeja de entrada del correo del SOC es de 19.4 segundos, en la tabla 10 se muestran estos tiempos registrados en las pruebas efectuadas en los 15 nodos de seguridad perimetral utilizados en las validaciones. Una tabla más detallada se muestra en el anexo 5.

Tabla 10

Tiempos promedios de llegada de la notificación al correo electrónico.

Nodo de Seguridad Perimetral	Tiempo promedio desde que se produce el evento hasta que se recibe la notificación en el correo electrónico (segundos)
FW_1719959954561	20
FW_1719960021033	19
FW_1719959908454	20
FW_1719960247541	19
FW_1719960392725	20
FW_1719960450234	18
FW_1719960624310	23
FW_1719959563918	22
FW_1719959853108	18
FW_1719959709955	18
FW_1719959786421	19
FW_1719960095801	18
FW_1719960285431	20
FW_1719960747268	22
FW_1719960190988	15
Promedio	19.4

Nota. Elaboración propia, basada en reporte de tiempos del software OpenNMS Horizon.

Como se indicó previamente, en la tabla 11 se muestran el tiempo de notificación promedio de un evento ocurrido en un nodo de seguridad perimetral antes y después de la implementación del software OpenNMS, según la tabla 11 el tiempo promedio de notificación luego de la implementación es el 6.03 % del tiempo previo a su implementación.

Tabla 11

Comparación de los tiempos promedios de notificación antes y después de la implementación del software de monitoreo OpenNMS.

Nodo de Seguridad Perimetral	Tiempo promedio de notificación de un evento generado en un Nodo de Seguridad Perimetral - Antes (Segundos)	Tiempo promedio de notificación de un evento generado en un Nodo de Seguridad Perimetral - Después (Segundos)
FW_1719959954561	327	20
FW_1719960021033	305	19
FW_1719959908454	323	20
FW_1719960247541	306	19
FW_1719960392725	322	20
FW_1719960450234	350	18
FW_1719960624310	312	23
FW_1719959563918	331	22
FW_1719959853108	341	18
FW_1719959709955	343	18
FW_1719959786421	316	19
FW_1719960095801	303	18
FW_1719960285431	313	20
FW_1719960747268	327	22
FW_1719960190988	301	15
Promedio	321.3	19.4

Nota. Elaboración propia, basada en reportes de los softwares PRTG y OpenNMS Horizon.

Una vez finalizadas estas pruebas, el software OpenNMS entró en producción para el monitoreo de los nodos de seguridad perimetral de los clientes corporativos del SOC de la Empresa de Telecomunicaciones.

Conclusiones

- El software de monitoreo OpenNMS OPEN SOURCE satisfizo los parámetros de evaluación, selección como los requerimientos del SOC de la Empresa de Telecomunicaciones, utilizando el protocolo SNMP.
- La funcionalidad de software de monitoreo es similar al de un software de monitoreo licenciado, es individualizable, escalable respecto al número de sensores y nodos, su costo de implementación ascendió al 38.68% del implementado del año 2023.
- El software de monitoreo OpenNMS activa todas sus funcionalidades, configurándose bajo el protocolo SNMP sincronizando y recolectando los registros logs de los nodos de seguridad perimetral, asegurando su funcionalidad al 100%.
- La supervisión y monitoreo de los nodos de seguridad perimetral gestionados por el SOC de la Empresa de Telecomunicaciones proporciona a los ingenieros de soporte del SOC una herramienta que les permite ejecutar acciones correctivas oportunas.
- El 100% de los nodos de seguridad perimetral admiten el protocolo SNMP v2c con el cual fueron configurados los parámetros de la comunidad SNMP y la IPv4 del colector del software OpenNMS.
- El software de monitoreo OpenNMS superó las pruebas de conectividad y transmisión de paquetes SNMP, remitiendo las alertas por e-mail cuando un nodo de seguridad perimetral experimenta desconexiones a la bandeja del SOC.
- El tiempo de notificación de un evento inesperado de conexión disminuyo al 6.03 % del tiempo registrado previo al de su implementación.

Recomendaciones

- Se recomienda efectuar un análisis serio de las necesidades y objetivos del SOC de la Empresa de Telecomunicaciones, considerando el factor de escalabilidad, costo, integración de equipos de diversa procedencia e información técnica.

- Luego de implementar el software OpenNMS, se recomienda instalar el complemento Grafana el cual permite crear paneles flexibles, visualizar e interactuar con los datos obtenidos por OpenNMS.

- Desarrollar complementos y nuevas funcionalidades para el OpenNMS Horizon utilizando OpenNMS Plugin API, recomendándose como temas de investigación futura.

- Para el envío de alertas y notificaciones, se sugiere implementar aplicaciones de mensajería de texto móviles como Telegram, Whatsapp o en su defecto implementar una aplicación móvil dedicada para él envió de alertas y notificaciones.

Referencias bibliográficas

Cáceres, J. C. (2020). *Diseño e Implementación de Mesa de Servicio Aplicando ISO 20000 para Procesos Administrativos en una Universidad Privada.* Arequipa - Perú.

Casas Reque, R. M., & Sempértegui Tocto, M. L. (2017). *Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red para Optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo.* Lambayeque-Perú.

Chavez, H. J. (2023). *Implementación de un Sistema de Seguridad Perimetral Bajo un Software Linux en una Institución Educativa de Ilo – 2021.* Moquegua - Perú.

Cisco. (2024). *Cisco DNA Center: Automatización, analítica y seguridad para redes*. Obtenido de Cisco: https://www.cisco.com/site/mx/es/products/networking/dna-center-platform/index.html

Fraser, B. (1997). *Site security handbook (RFC 2196).* Internet Engineering Task Force. Obtenido de https://www.rfc-editor.org/rfc/rfc2196.txt

International Organization for Standardization. (2016). *ISO/IEC 27035:2016 Information technology — Security techniques — Information security incident management.* Obtenido de https://www.iso.org/standard/60803.html

Kurose, J. F., & Ross, K. W. (2017). *REDES DE COMPUTADORAS. Un enfoque descendente* (Septima ed.). Madrid, España: Pearson Educación.

Martínez Gómez, M. (2021). *Implementación de un Centro de Operaciones De Seguridad (SOC) de Código Abierto con Elementos de Red para el Control de Tráfico.* Valencia - España.

Microsoft. (2024). *Descripción del comando Tracert*. Obtenido de Microsoft Learn: https://www.learn.microsoft.com/es-es/windows-server/administration/windows-commands/tracert

Montañez Prieto, J. P. (2018). *Propuesta Para la Migración del Protocolo Ipv4 a Protocolo IPv6 Para la Secretaria del SISBEN de la Alcaldia de Tunja.* Tunja.

National Institute of Standards and Technology. (2006). *Guide to computer security log management (SP 800-92).* U.S. Department of Commerce. doi:https://doi.org/10.6028/NIST.SP.800-92

Open Source Initiative. (2024). *The Open Source Definition*. Obtenido de OSI: https://www.opensource.org/osd

OpenNMS Group. (2021). *Horizon.* Obtenido de https://www.opennms.com/wp-content/uploads/2021/05/Horizon-Data-Sheet.pdf

OpenNMS Group. (2024). *OpenNMS: The open-source network monitoring and management platform*. Obtenido de OpenNMS: https://www.opennms.com

Oré Alvaro, C. (2019). *Implementación de un Sistema de Monitoreo Para Asegurar la Continuidad de los Servicios en un Data Center Utilizando Protocolo SNMP.* Lima-Perú.

Quispe Ccuno, J. R. (2019). *Implementación de un Prototipo de Monitoreo de Dispositivos de Comunicación y Usuarios Finales Utilizando el Protocolo SNMP Basada en Software Libre Para una Empresa E-Commerce.* Lima-Perú.

Ruiz, F. (2024). *Caracterización de un Firewall Perimetral Implementado Mediante Software Libre OpenBSD y CentOS.* Mexico.

Sánchez Osejo, E. R. (2022). *Diseño de Implementación de una Herramienta Open Source para Monitoreo de Servidores.* Quito - Ecuador.

Universidad VIU. (2017). *¿Qué es un Sniffer?* . Obtenido de Universidad VIU: https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-un-sniffer

Valarezo, J. R. (2020). *Desarrollo de un Prototipo de Red de Área Amplia Basado en una Arquitectura Definida por Software (SD-WAN) en una Institución Financiera.* Guayaquil - Ecuador.

Yacila, L. D. (2021). *Propuesta de Implementación de una Red LAN para la Municipalidad Distrital de Corrales – Tumbes; 2021.* Tumbes.

Anexos

Anexo 1: Detalle de los Nodos de Seguridad Perimetral.

Nodo de Seguridad Perimetral	Nombre de Firewall	Marca de Firewall	Modelo Firewall	IP de VRF
FW_1719959954561	FW_CAR[illegible]7142	FORTINET - Fortigate	FGT_60E	40.40.251.2
FW_1719960021033	FW_CUN[illegible]74091	FORTINET - Fortigate	FGT_60E	40.40.100.254
FW_1719959908454	FW_DAR[illegible]08377	FORTINET - Fortigate	FGT_200E	40.40.100.138
FW_1719960247541	FW_DISTRIBUIDORA_[illegible]_ID_	FORTINET - Fortigate	FGT_300E	40.40.106.222
FW_1719960392725	FW_[illegible]-COMAS_PRI_[illegible]_	FORTINET - Fortigate	FGT_60E	40.40.106.162
FW_1719960450234	FW_[illegible]-COMAS_SEC_[illegible]_	FORTINET - Fortigate	FGT_60E	40.40.106.163
FW_1719960624310	FW_[illegible]_PERUANA_[illegible]_	FORTINET - Fortigate	FGT_80F	40.40.103.14
FW_1719959563918	FW_NOR[illegible]89346	FORTINET - Fortigate	FGT_50E	40.40.103.106
FW_1719959853108	FW_NOR[illegible]7949	FORTINET - Fortigate	FGT_30E	40.40.106.70
FW_1719959709955	FW_NOR[illegible]71452	FORTINET - Fortigate	FGT_30E	40.40.106.62
FW_1719959786421	FW_NOR[illegible]72581	FORTINET - Fortigate	FGT_30E	40.40.106.66
FW_1719960095801	FW_SAG[illegible]50007	FORTINET - Fortigate	FGT_60E	40.40.103.254
FW_1719960285431	FW_SIS[illegible]8167	FORTINET - Fortigate	FGT_100E	40.40.103.102
FW_1719960747268	FW_SIS[illegible]8167	FORTINET - Fortigate	FGT_100E	40.40.103.103
FW_1719960190988	FW_SIT[illegible]3597	FORTINET - Fortigate	FGT_80E	40.40.103.82

Nota. Elaboración propia, basada en el direccionamiento IP del SOC de la empresa de Telecomunicaciones.

Anexo 2: Características del software de monitoreo OpenNMS Horizon.

Rapid Release, Latest Features

OpenNMS Horizon is an open-source solution that helps you visualize and monitor everything on your local and remote networks. It offers comprehensive fault, performance, traffic monitoring, and alarm generation in one place. Highly customizable and scalable, Horizon easily integrates with your core business applications and workflows.

Broadest Suite of Supported Protocols Out of the Box

SNMP	JSON	WinRM
XML	SQL	JMX
SFTP	FTP	JDBC
HTTP	HTTPS	VMware
WS-Management		Prometheus

Features

Inventory Management

Supports any type of provisioning: auto, directed, topology, interface, and service discovery. Interoperates with virtually any configuration management system.

Performance Management

Broadest suite of data collection protocols (14) means no need for third-party tools. Streaming telemetry, real-time custom thresholding, trend analysis, forecasting. Time-series performance data analysis, visual plotting and operational forecasting in real-time.

Fault Management

Service assurance via smart periodic polling. Autonomous device problem reporting. Message enrichment.

Business Service Monitoring

Monitor and model high-level business services to quickly identify the most critical problems affecting them.

Remote Data Collection

Minion provides access to the inaccessible while application perspective monitoring monitors service availability at specific locations from different perspectives.

BGP Monitoring Protocol (BMP) Support

Monitor Border Gateway Protocol (BGP) sessions and BGP routing information on the routing device. Use this information, status updates, and statistics for advanced monitoring and management.

Traffic Management

Five flow protocols. 350,000+ flows/sec. Deep-dive analysis, enterprise reporting.

Application Perspective Monitoring

Monitor a service's availability from different perspectives. Pinpoint not only where an issue occurs, but its impact on a user's or machine's digital experience.

Nota: Plataforma OpenNMS Horizon.

Anexo 3: Requerimientos técnicos del software de monitoreo OpenNMS Horizon.

Platform Solution

Configurability

Configure most features through the web UI or XML scripting. Customize Meridian to do what you want the way you want it.

Scalability

Monitor tens of thousands of devices via a distributed and tiered system: 1.2m data points every 5 minutes, 5,000+ interfaces, hundreds of thousands of discrete devices, millions of performance metrics, thousands of events per second, and thousands of remote monitors.

Enterprise Reporting and Visualization

Real-time notifications for high-priority response. Customizable Grafana dashboards. Resource graphs, database reports, charts.

Topology Maps

Define complex layered topologies. Semantics and focal point feature allow you to adjust and enhance the map quickly to customize your view and easily integrate topology maps into your service problem management workflow.

Event/Alarm Management and Correlation

Alarm and Event Management

First-class events for service assurance and performance management. Alarm workflows, ticketing integration, and flexible correlation. Customizable notifications via email, SMS, and Webhooks.

Alarm Correlation

An artificial intelligence framework logically groups related faults (alarms) into higher level objects (situations) so you can quickly detect, visualize, prioritize, and resolve situations across the entire IT infrastructure.

Technical Requirements

Minimum System Requirements	Java 8-11. Most recent version of JDK 11 recommended. PostgreSQL 10 or higher (up to and including 13) Minimum for proof-of-concept type workload: 4GB RAM 2 CPUs	
Operating System	RHEL 7.x, 8.x CentOS 7.x, 8.x	
	Proof of concept (testing)*	**Minimum server specification****
CPU	2 GHz dual core x86_64	3 GHz quad core x86_64 and above
RAM	4 GB (physical)	16 GB (physical) and above
Storage (disk space)	50 GB HDD, SSD	1 TB with SSD and above

Common Outbound Ports

OpenNMS can monitor just about any service on any device, so it is impossible to present an exhaustive list.

In the case of managing networked devices and servers, the following list covers the bulk of traffic:

ICMP	(echo-request)
SNMP	(161/udp)
SSH	(22/tcp)
HTTP	(80/tcp)
HTTPS	(443/tcp)

** You can install the packages and the services will start up*
*** Does not take into account your intended workload (e.g., network size, number of monitored metrics, flows, events, and data retention requirements).*

Nota: Plataforma OpenNMS Horizon.

Anexo 4: Especificaciones técnicas del servidor-1 del SOC.

Especificaciones técnicas	Servidor HPE ProLiant DL360 Gen10
Procesador	Intel
Familia de procesador	Intel® Xeon® escalable serie 8100/8200 - Intel® Xeon® escalable serie 3100/3200
Número de procesador	1 o 2
Núcleo de procesador disponible	De 4 a 28 núcleos, según el modelo
Caché de procesador	De 8,25 a 38,50 MB L3, según el procesador
Velocidad del procesador	3,9 GHz, máximo según el procesador
Ranuras de expansión	3, para obtener una descripción detallada, consulte las QuickSpecs
Memoria, máxima	3,0 TB con DDR4 de 128 GB 6,0 TB con kit de memoria persistente HPE 2666 de 512 GB
Memoria, estándar	LRDIMM de 3,0 TB (24 x 128 GB) memoria persistente HPE de 6,0 TB (12 x 512 GB)
Ranuras de memoria	24 ranuras DIMM
Tipo de memoria	HPE DDR4 SmartMemory y memoria persistente Intel® Optane™ serie 100 para HPE, según el modelo
Características de los ventiladores del sistema	Redundancia con conexión en caliente de serie
Controlador de red	Adaptador Ethernet 4 x 1 GbE integrado (determinados modelos) o HPE FlexibleLOM y tarjetas PCIe verticales opcionales, según el modelo
Controlador de almacenamiento	HPE Smart Array S100i, controlador HPE Essential o RAID de rendimiento, según el modelo
Medidas del producto (métrico)	Chasis de factor formato reducido: 4,29 x 43,46 x 70,7 cm, Chasis de factor formato grande: 4,29 x 43,46 x 74,98 cm
Peso	13,04 kg mínimo, 16,78 kg máximo
Administración de infraestructura	HPE iLO Standard con aprovisionamiento inteligente (integrado), HPE OneView Standard (requiere descarga) Opcional: HPE iLO Advanced y HPE OneView Advanced (requieren licencias)
Garantía	3/3/3 - La garantía del servidor incluye tres años de garantía en piezas, tres años de mano de obra y tres años de cobertura de soporte a domicilio. Información adicional sobre en la garantía limitada en todo el mundo y la asistencia técnica disponible en: http://h20564.www2.hpe.com/hpsc/wc/public/home. Puede comprar localmente cobertura de servicio y asistencia de HPE adicionales para su producto. Para obtener información acerca de la disponibilidad de las actualizaciones del servicio y su coste, visite el sitio Web de HPE en http://www.hpe.com/support
Tipo de unidad	4 SAS/SATA LFF, 8 SAS/SATA SFF + 2 NVMe, 10 SAS/SATA SFF, 10 NVMe SFF, 1 unidad trasera opcional SFF o 1 UFF doble según el modelo

Nota: Plataforma Hewlett Packard Enterprise.

Anexo 5: Medición de los tiempos de notificación del OpenNMS Horizon.

Nodo de Seguridad Perimetral	Hora de Desconexión	Hora de Alerta en el OpenNMS Horizon	Hora de Notificación en la Bandeja de Correo Electrónico	Tiempo en Notificar en el OpenNMS Horizon (segundos)	Tiempo desde que se produce el evento hasta que se recibe la notificación en el correo electrónico (segundos)
FW_1719959954561	01:05:30	01:05:48	01:05:50	18	20
FW_1719960021033	01:11:13	01:11:31	01:11:32	18	19
FW_1719959908454	01:15:39	01:15:58	01:15:59	19	20
FW_1719960247541	01:22:07	01:22:24	01:22:26	17	19
FW_1719960392725	01:29:18	01:29:37	01:29:38	19	20
FW_1719960450234	01:37:45	01:38:02	01:38:03	17	18
FW_1719960624310	01:42:26	01:42:46	01:42:49	20	23
FW_1719959563918	01:48:14	01:48:33	01:48:36	19	22
FW_1719959853108	01:55:21	01:55:36	01:55:39	15	18
FW_1719959709955	02:09:06	02:09:23	02:09:24	17	18
FW_1719959786421	02:21:27	02:21:43	02:21:46	16	19
FW_1719960095801	02:26:37	02:26:54	02:26:55	17	18
FW_1719960285431	02:35:43	02:36:01	02:36:03	18	20
FW_1719960747268	02:42:16	02:42:36	02:42:38	20	22
FW_1719960190988	02:50:03	02:50:16	02:50:18	13	15
	Promedio			17.5	19.4

Nota. Elaboración propia, basada en el reporte de tiempos del software OpenNMS Horizon.