SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX PARA OPENVPN EN NETSERVER Y EQUIPOS CLIENTE.

Andres Felipe Wilches Cely - 1070016603
afwilchesc@unadvirtual.edu.co

RESUMEN: Este artículo describe la instalación y configuración de NethServer en un sistema basado en GNU/Linux, con el propósito de mejorar la funcionalidad y seguridad de la red. Se detalla el proceso de implementación y optimización de OpenVPN mediante NethServer, permitiendo establecer conexiones remotas seguras a través de comunicaciones cifradas entre clientes externos y la red interna. Este enfoque garantiza la protección de datos sensibles y el acceso autorizado, además de optimizar la gestión del tráfico VPN para mantener una postura robusta de seguridad en la red. Los resultados destacan la capacidad de NethServer para satisfacer requerimientos críticos en entornos de IT.

PALABRAS CLAVE: Sistema Operativo, Gestión de redes, Conexiones seguras, VPN, Soluciones tecnológicas.

I. INTRODUCCIÓN

En el contexto actual, las empresas y organizaciones se enfrentan al reto de garantizar redes funcionales y seguras, adaptándose a las demandas tecnológicas en constante evolución. La implementación de sistemas operativos basados en GNU/Linux, como NethServer, se presenta como una solución confiable y eficiente para la administración avanzada de recursos y redes.

Este trabajo se enmarca en una actividad práctica centrada en la instalación y configuración de NethServer en un entorno GNU/Linux, con el objetivo principal de implementar OpenVPN para establecer conexiones remotas seguras. El proceso incluye la configuración de comunicaciones cifradas entre clientes externos y la red interna, asegurando la protección de datos sensibles y habilitando accesos autorizados. Asimismo, se realizaron ajustes para optimizar el tráfico VPN y reforzar la seguridad general de la red, demostrando la eficacia de NethServer para satisfacer las necesidades de conectividad y protección en entornos empresariales o institucionales.

El objetivo de este artículo es documentar, con un enfoque técnico detallado, los procedimientos y resultados obtenidos durante la instalación y configuración de NethServer, con especial atención en la implementación de OpenVPN. Cada aspecto tratado aborda elementos clave para la gestión y seguridad de redes, aplicando los conocimientos adquiridos previamente durante el proceso formativo. Este enfoque no solo busca resolver necesidades específicas de conectividad y protección, sino también explorar y demostrar las posibilidades prácticas de aplicar estas soluciones en entornos reales, destacando su relevancia en el ámbito de la infraestructura IT.

II. INSTALACIÓN DE NETHSERVER

A. CONFIGURACIÓN VIRTUALBOX

1. Dentro del proceso necesario para instalar y configurar NethServer como sistema operativo base para ofrecer servicios de infraestructura IT, es fundamental realizar una correcta asignación de recursos en el entorno virtual. Esto incluye definir parámetros como el espacio en disco, la memoria RAM y los núcleos de procesamiento, así como especificar la imagen ISO previamente descargada desde el sitio oficial de NethServer.

Aunque existen diversos hypervisores disponibles, como VMware, Hyper-V y KVM, para este caso se utilizó VirtualBox como la plataforma de virtualización. Tras la configuración inicial de la máquina virtual y la carga de la ISO de NethServer basada en CentOS 7, se completó el proceso de instalación, incluyendo la adición de claves necesarias para habilitar los servicios requeridos. (Fig. 1).

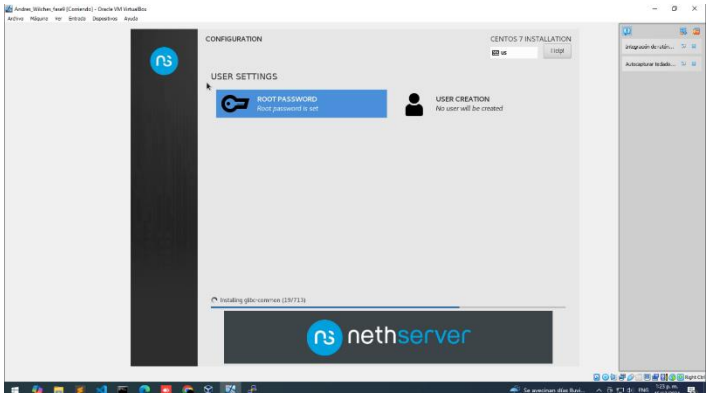

Fig 1. Fuente: Autoría Propia

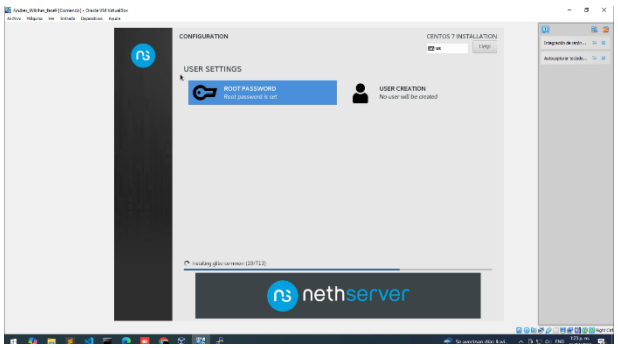

Fig 1. Fuente: Autoría Propia

B. ASIGNACIÓN DE DIRECCIONAMIENTO IP EN NETSERVER

1. Se muestra la dirección IP asignada a NethServer en la red LAN, la cual es utilizada para acceder a la consola web de administración. Esta dirección IP es un elemento fundamental para la gestión de los servicios del servidor en el entorno local. (Fig. 2)

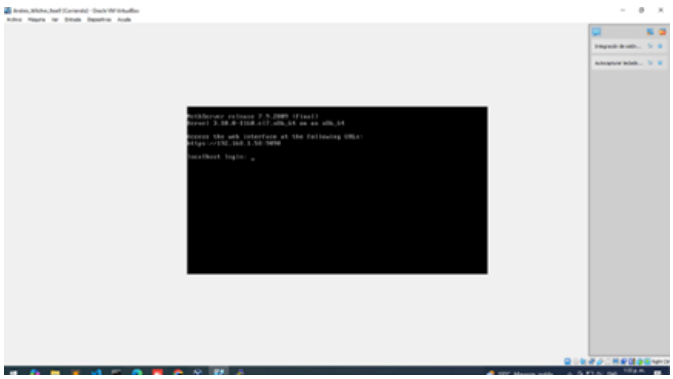

Fig. 2 Fuente: Autoría Propia

2. En la (Fig. 3), se muestra el acceso al shell de CentOS, donde se procede a modificar la configuración de la dirección IP del sistema para adaptarla a los requisitos específicos de la red.

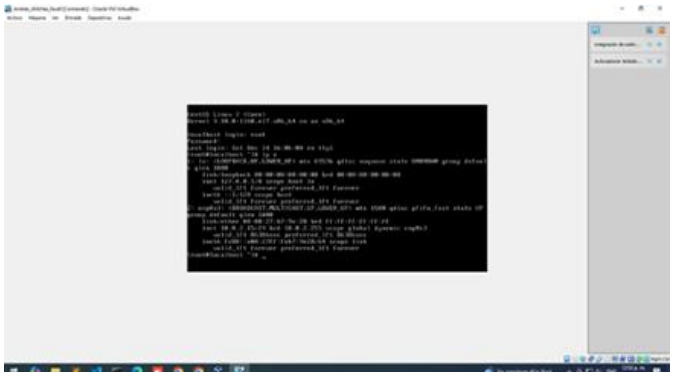

Fig. 3 Fuente: Autoría Propia

3. En el (Fig. 4), se realiza el cambio de configuración de red de NAT a modo puente, permitiendo que la máquina virtual obtenga una dirección IP dentro de la red local. Posteriormente, se reinicia la interfaz de red para aplicar los cambios y garantizar que el servidor pueda ser administrado dentro del entorno de la red configurada.

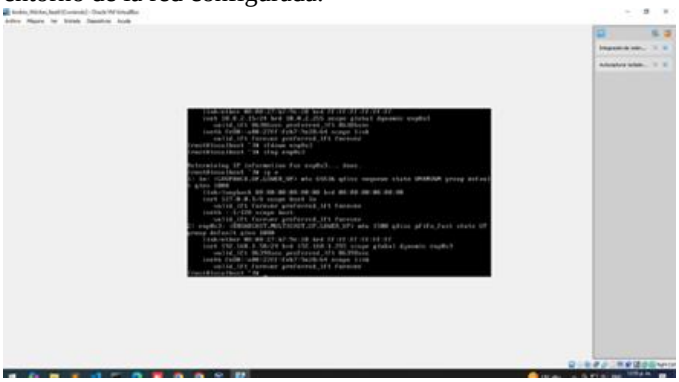

Fig. 4 Fuente: Autoría Propia

4. En la (Fig. 5), se llevan a cabo pruebas de conectividad para verificar que el servidor NethServer esté correctamente integrado a la red. Estas pruebas se realizan de manera exitosa, confirmando la comunicación efectiva entre el servidor y otros dispositivos en la red.

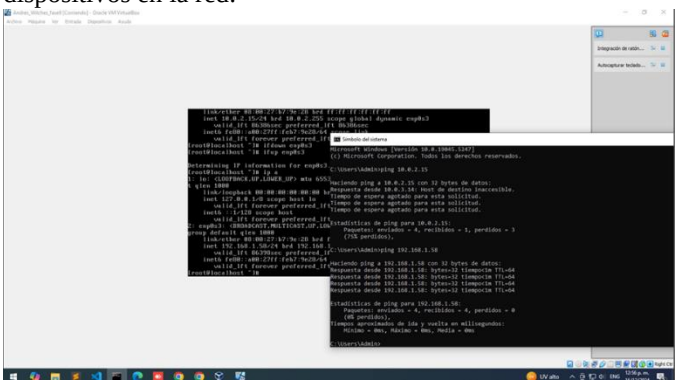

Fig. 5 Fuente: Autoría Propia

5. En la **(Fig. 6)**, se accede al panel de administración de Keycloak integrado en NethServer, a través del puerto 9090. Este panel permite gestionar usuarios, roles y configuraciones relacionadas con la autenticación y autorización del sistema.

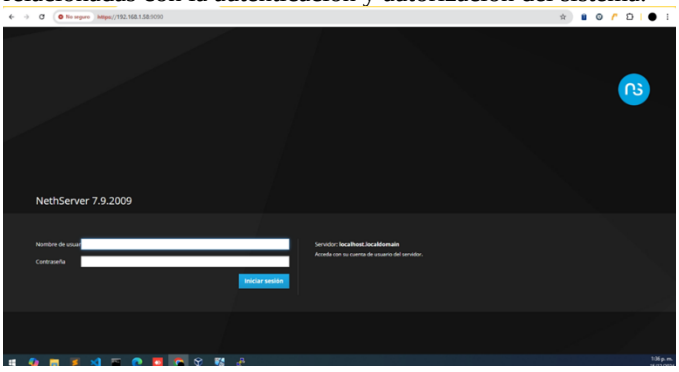

Fig. 6 Fuente: Autoría Propia

C. ENTORNO WEB NETSERVER

1. En la (Fig. 7), se realiza el ingreso al panel de administración de Keycloak utilizando el usuario root del sistema, lo que permite acceder a todas las funciones y configuraciones del sistema de autenticación.

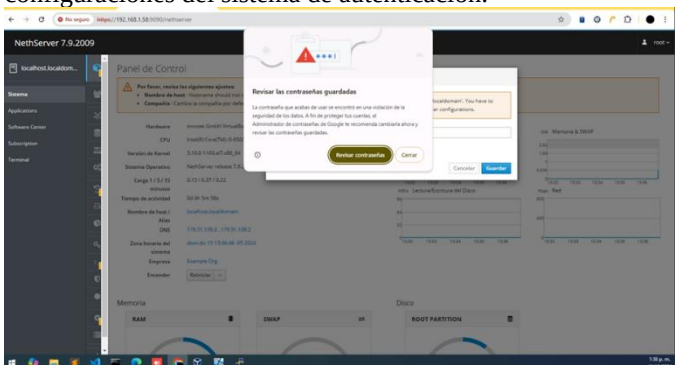

Fig. 7 Fuente: Autoría Propia

2. En la **(Fig. 8)**, se espera a que finalice el proceso de inicio del sistema, momento en el cual se completan las configuraciones iniciales y el servidor está listo para ser administrado y utilizado en el entorno de red.

Fig. 8 Fuente: Autoría Propia

3. En la **(Fig. 9)**, se procede a validar los usuarios dentro del panel de administración de Keycloak, verificando su correcta configuración y acceso en el sistema. Esto asegura que las credenciales y roles asignados sean efectivos para la gestión y seguridad de la red.

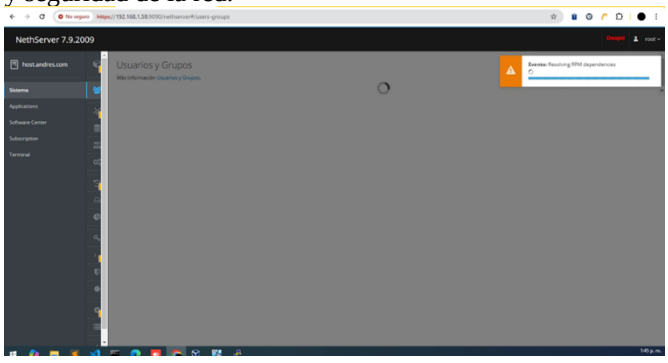

Fig. 9 Fuente: Autoría Propia

4. En la **(Fig. 10)**, se accede al *Software Center* de NethServer y se realiza una búsqueda de "VPN", lo que devuelve la opción de OpenVPN. En este caso, OpenVPN se configurará para actuar como servidor VPN, permitiendo establecer conexiones remotas seguras a la red interna.

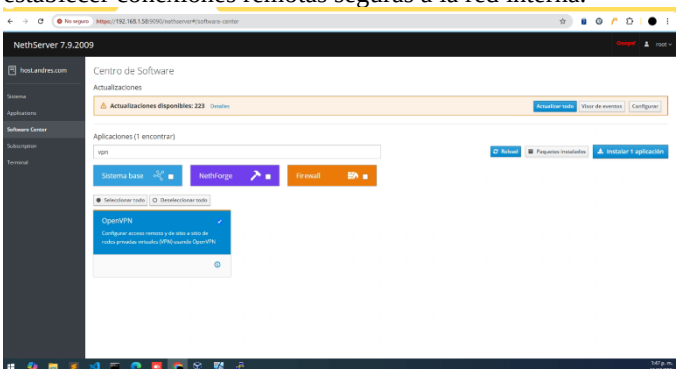

Fig. 10 Fuente: Autoría Propia

5. En la **(Fig. 11)**, se procede con la instalación de OpenVPN como servidor VPN a través del *Software Center* de NethServer. Esta instalación es crucial para habilitar las conexiones remotas seguras entre los clientes externos y la red interna del sistema.

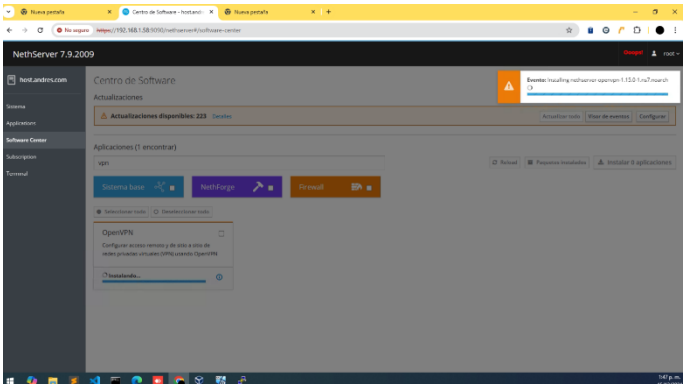

Fig. 11 Fuente: Autoría Propia

6. En la **(Fig. 12)**, después de completar la instalación de OpenVPN, se valida en la sección de aplicaciones para verificar que los servicios correspondientes se hayan instalado correctamente. Esto confirma que OpenVPN está ahora disponible y listo para ser configurado como servidor VPN.

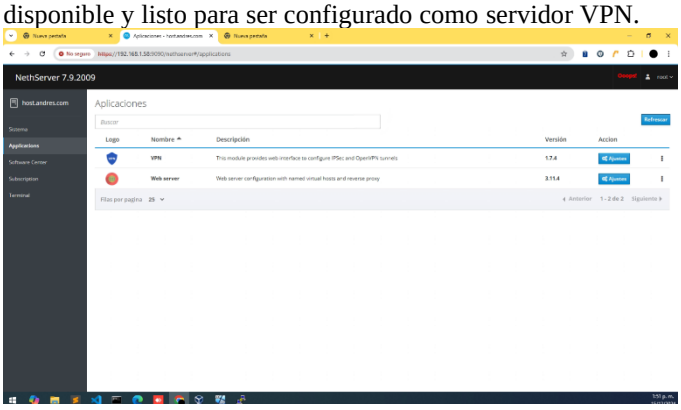

Fig. 12 Fuente: Autoría Propia

7. En la **(Fig. 13-14)**, se accede a la sección de configuración de OpenVPN dentro del panel de administración de NethServer. Aquí, se podrán ajustar los parámetros

necesarios para personalizar y habilitar el servicio VPN, garantizando conexiones remotas seguras y confiables.

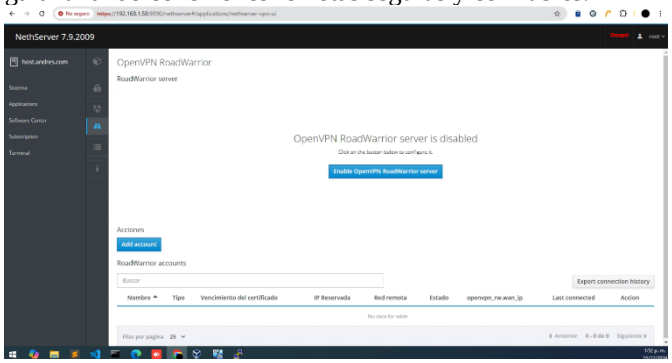

Fig. 13 Fuente: Autoría Propia

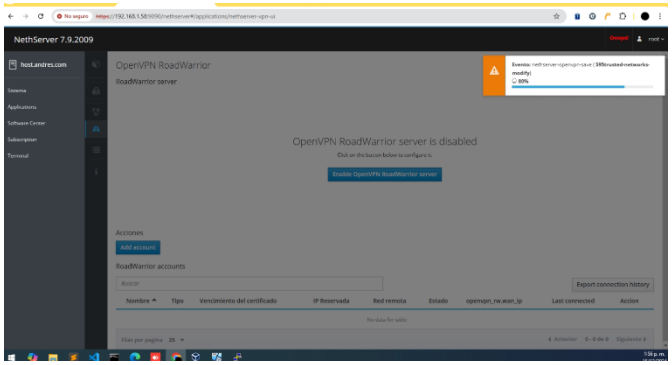

Fig. 14 Fuente: Autoría Propia

8. En la **(Fig. 15-16)**, se agrega el usuario "Admin" como un usuario de VPN. Este usuario será configurado para tener acceso a la red a través de la conexión segura proporcionada por el servidor OpenVPN.

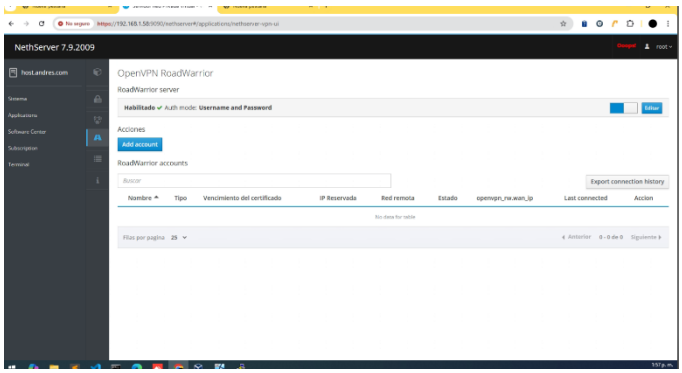

Fig. 15 Fuente: Autoría Propia

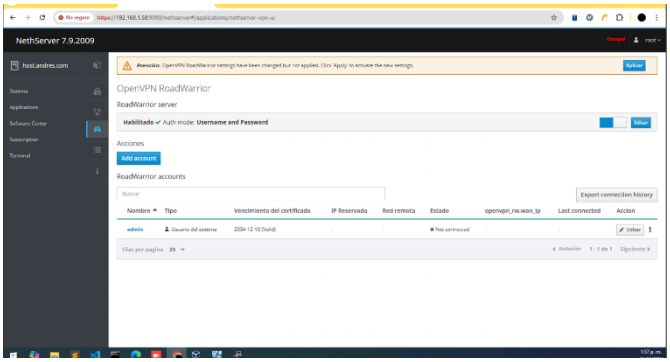

Fig. 16 Fuente: Autoría Propia

9. En la **(Fig. 17)**, además del usuario "Admin", se agrega también el usuario "vpn" para otorgarle acceso a la red a través de la conexión segura de OpenVPN. Ambos usuarios estarán configurados para acceder de manera remota a los recursos internos del sistema a través de la VPN.

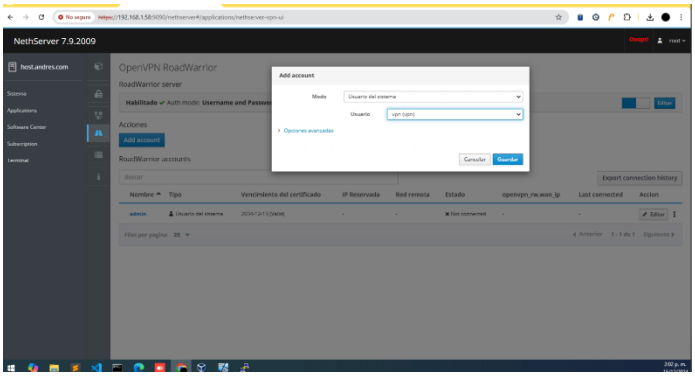

Fig. 17 Fuente: Autoría Propia

D. ENTORNO CLIENTE DE OPEN VPN

1. En la **(Fig. 18)**, después de configurar los usuarios, se procede a descargar la aplicación OpenVPN en el dispositivo cliente. Esto permitirá establecer una conexión segura entre el cliente y el servidor VPN, utilizando las credenciales previamente configuradas.

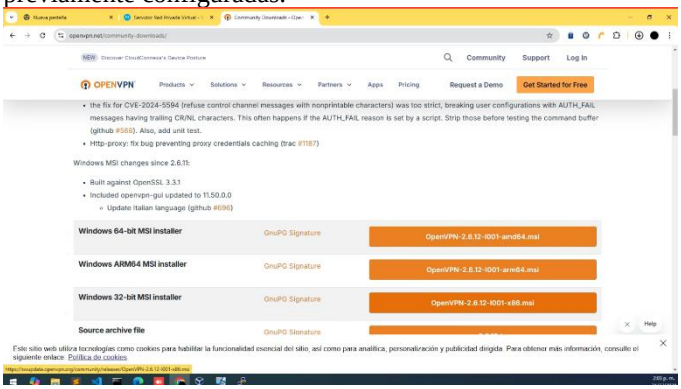

Fig. 18 Fuente: Autoría Propia

2. En la **(Fig. 19-20)**, se lleva a cabo la instalación de la aplicación OpenVPN en el dispositivo cliente, siguiendo los pasos necesarios para asegurar que el software esté listo para

conectarse al servidor VPN. Esto establece la base para que los usuarios, como "Admin" y "vpn", puedan acceder de manera segura a la red interna.

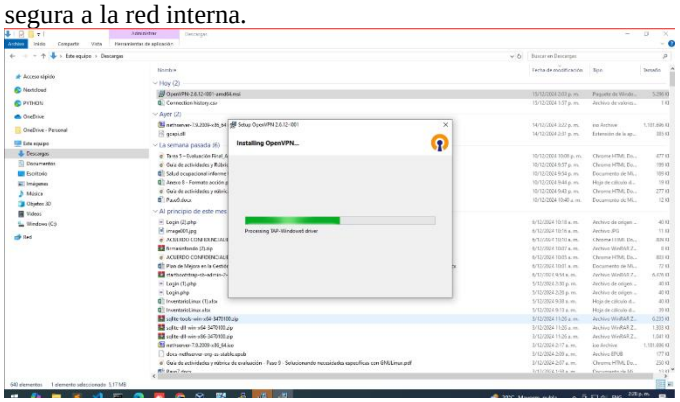

Fig. 19 Fuente: Autoría Propia

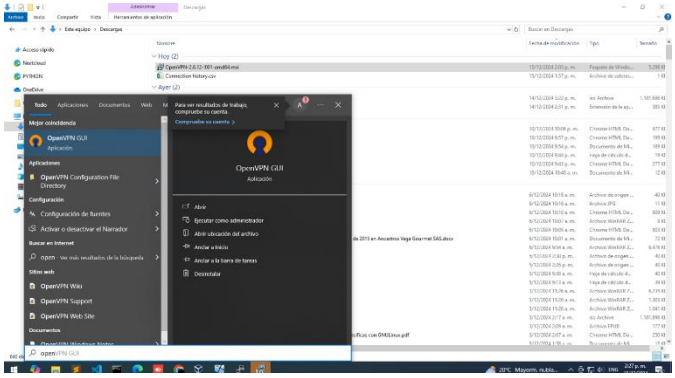

Fig. 20 Fuente: Autoría Propia

3. Después de completar la instalación de la aplicación OpenVPN en el dispositivo cliente, se procede a descargar el archivo de configuración para el usuario "vpn". Este archivo contiene los parámetros necesarios para establecer la conexión segura entre el cliente y el servidor VPN, como se muestra en la **(Fig. 21)**.

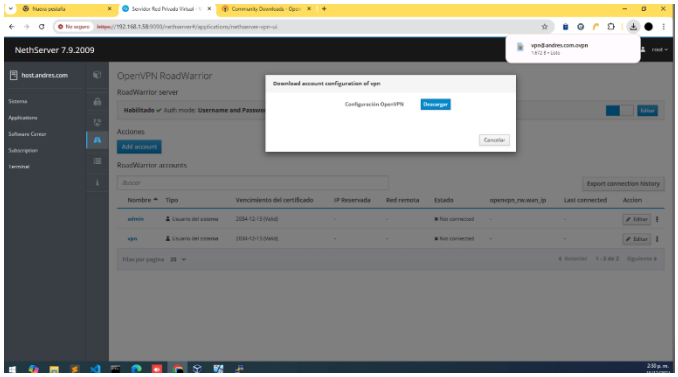

Fig. 21 Fuente: Autoría Propia

4. En la **(Fig. 22)**, se localiza el archivo de configuración descargado desde la aplicación cliente de OpenVPN. Este archivo contiene las credenciales y la configuración necesarias para conectar el dispositivo cliente al servidor VPN, asegurando una conexión segura a la red interna.

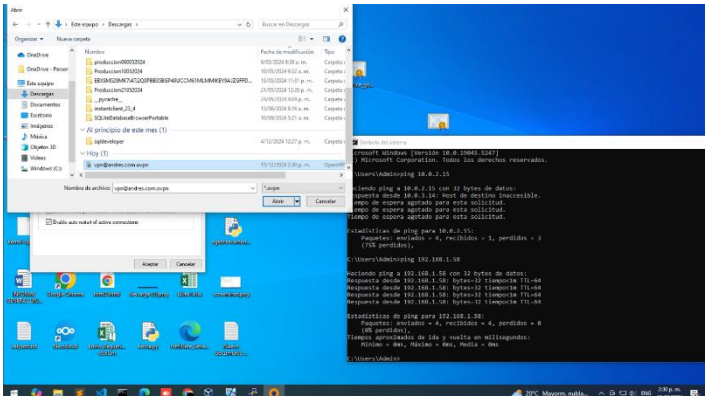

Fig. 22 Fuente: Autoría Propia

5. En la **(Fig. 23)**, podemos observar que la importación del archivo de configuración .ovpn se ha completado de manera exitosa. Este archivo ahora está integrado en la aplicación OpenVPN, permitiendo que el dispositivo cliente se conecte al servidor VPN de forma segura y efectiva.

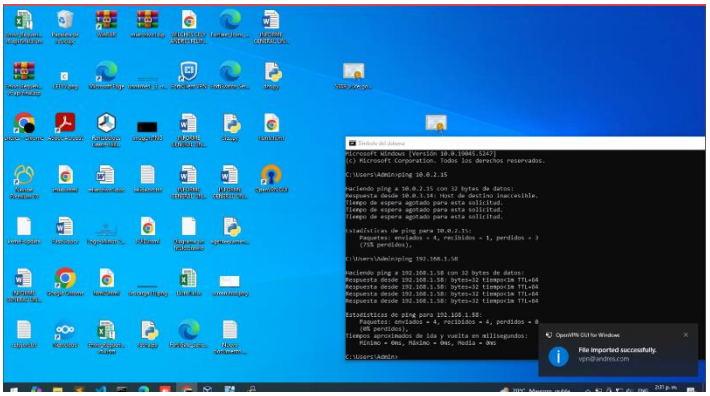

Fig. 23 Fuente: Autoría Propia

6. Después de completar la importación del archivo de configuración en la **(Fig. 23)**, procedemos a hacer clic en "Conectar", como se muestra en la **(Fig. 24)**. Posteriormente, ingresamos las credenciales del usuario "vpn" para autenticarnos y establecer una conexión segura con el servidor VPN.

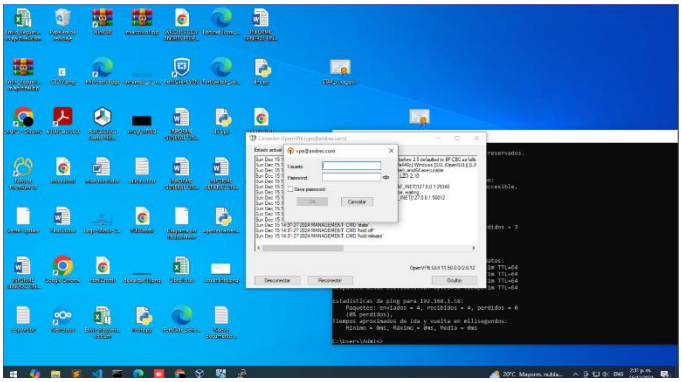

Fig. 24 Fuente: Autoría Propia

7. En la **(Fig. 25)**, se verifica la conectividad tras la autenticación exitosa. Esto confirma que el dispositivo cliente

está conectado al servidor VPN y puede acceder de manera segura a los recursos de la red interna.

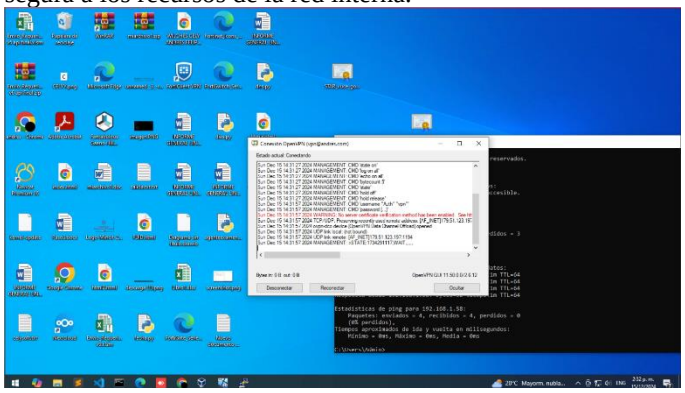

Fig. 25 Fuente: Autoría Propia

8. Por último, se accede al servicio web alojado en el servidor, utilizando la conexión establecida con el usuario "vpn". Esto permite interactuar de forma segura con la nube instalada en el servidor, aprovechando la protección y privacidad que brinda la conexión VPN. (Fig. 26).

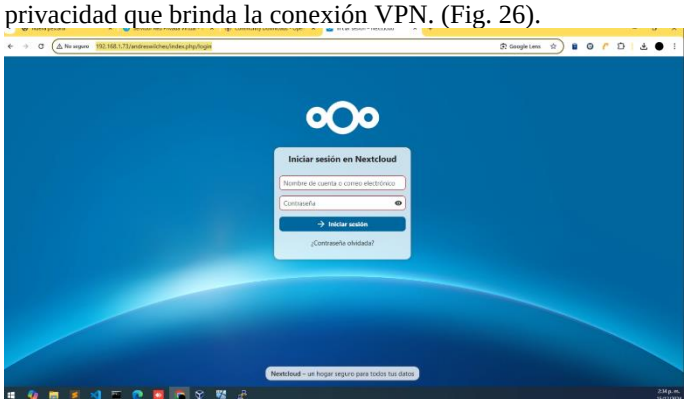

Fig. 16 Fuente: Autoría Propia

E. Conclusiones

El desarrollo de esta actividad permitió adquirir y consolidar habilidades en la instalación y configuración de servicios de red utilizando NethServer, con un enfoque particular en la implementación y gestión de OpenVPN a través de su interfaz web. Este proceso demostró ser eficiente y adecuado para proporcionar acceso remoto seguro y encriptado en un entorno controlado.

- **Instalación y configuración de NethServer:** La implementación de NethServer como sistema operativo base destacó por su interfaz web intuitiva, que facilitó la instalación y configuración de los servicios necesarios, eliminando la complejidad técnica asociada a otros métodos de gestión.
- **Configuración y gestión de OpenVPN:** La configuración de OpenVPN como servidor VPN a través de NethServer fue clave para garantizar conexiones remotas seguras. La integración de este servicio permitió establecer túneles cifrados que aseguran la integridad y confidencialidad de los datos transmitidos entre los usuarios y la red interna.
- **Gestión de usuarios para VPN:** La creación y configuración de usuarios específicos para la VPN, como "Admin" y "vpn", permitió personalizar el acceso remoto, garantizando que solo usuarios autorizados puedan conectarse al servidor y acceder a los recursos internos.
- **Validación y pruebas de conectividad:** Cada etapa del proceso, desde la instalación de la aplicación OpenVPN en los dispositivos cliente hasta la autenticación de los usuarios y las pruebas de conexión, fue validada exitosamente. Esto aseguró que el sistema estuviera completamente operativo y funcional.
- **Acceso a servicios web mediante VPN:** La actividad finalizó con el acceso exitoso al servicio web alojado en el servidor, utilizando la conexión establecida a través de OpenVPN. Este resultado reafirmó la eficacia de la solución para proporcionar acceso remoto seguro.

En conclusión, la implementación de NethServer y OpenVPN demostró ser una solución robusta y confiable para la gestión de redes y servicios remotos. La actividad subrayó la importancia de aplicar herramientas modernas y efectivas que faciliten la administración y mejoren la seguridad en entornos IT reales.

F. REFERENCIAS

[1] LPI LPIC-1 Exam 102. (2022). "Tema 106: Interfaces de usuario y escritorios". Learning LPI. Disponible en: https://learning.lpi.org/es/learning-materials/102-500/106/

[2] Canonical. (2023). "Guía del Ubuntu Desktop 20.04 LTS". Help Ubuntu. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Debian. (2023). "El manual del administrador de Debian 12.5.0". Debian. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle. (2020). "Manual de usuario VirtualBox". VirtualBox. Disponible en: https://www.virtualbox.org/manual/