Implementación y Configuración Integral de Servicios de Red: DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos, Servidor de Archivos, Impresiones y VPN en un Entorno IT

Wilson Daniel Benítez
e-mail: Wdbenitezo@unadvirtual.edu.co
Ana Carolina Cifuentes
e-mail: accifuentesc@unad.edu.co
Sandra Valentina Páez González
e-mail: svpaezg@unadvirtual.edu.co
Yenny Marcela Pérez
e-mail: ymperezam@unadvirtual.edu.co
Dannia Julissa Quevedo Mahecha
e-mail: djquevedom@unadvirtual.edu.co

RESUMEN: *Este documento detalla el proceso de instalación y configuración de una variedad de servicios de red, con el objetivo de aplicar prácticas avanzadas de administración en un entorno de red utilizando NethServer 7.9. Se abordan los servicios de DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos, Servidor de Archivos, Servidor de Impresiones y VPN, así como la integración y gestión de estaciones de trabajo GNU/Linux. El proceso se estructura en tres fases principales: instalación, configuración y puesta en funcionamiento de cada servicio, proporcionando una guía exhaustiva para la implementación efectiva en un entorno IT.*

PALABRAS CLAVE: Nethserver, DHCP, Proxy, DNS, VPN.

1 INTRODUCCIÓN

La gestión eficiente de una infraestructura de red en entornos empresariales requiere una integración armoniosa de múltiples servicios y tecnologías. NethServer, una distribución de Linux basada en CentOS, este ofrece una solución robusta y accesible para la administración de servicios de red esenciales. Su interfaz gráfica intuitiva facilita la configuración y el mantenimiento de una variedad de servicios, desde DHCP y DNS hasta servidores de archivos e impresión, lo que lo convierte en una herramienta valiosa para pequeñas y medianas empresas.

En este contexto, la integración y gestión de estaciones de trabajo GNU/Linux en la infraestructura de red exige una comprensión detallada de cómo estos sistemas interactúan con los servicios configurados. Los administradores deben considerar aspectos como la compatibilidad del software, la configuración de políticas de seguridad y el manejo de accesos, para optimizar la interoperabilidad y la eficiencia operativa.

Este documento proporciona un análisis detallado del proceso de instalación y configuración de NethServer y sus servicios asociados, abordando específicamente la

configuración de servicios clave y la integración con estaciones de trabajo GNU/Linux. La estructura del documento se enfoca en la implementación de cada componente, proporcionando una guía técnica y analítica para la optimización de la infraestructura de red.

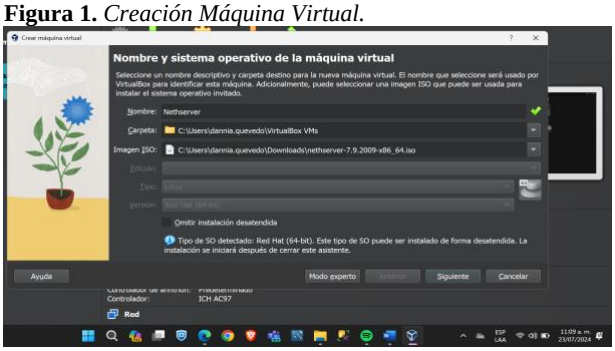
2 CONFIGURACIÓN DE UNA MÁQUINA VIRTUAL PARA LA INSTALACIÓN DE NETHSERVER

La implementación de NethServer en un entorno virtualizado ofrece flexibilidad y eficiencia en la administración de servicios de red. La primera etapa en este proceso es la configuración de una máquina virtual adecuada. Para ello, se utiliza un hipervisor, como VirtualBox o VMware, que permite la creación y gestión de máquinas virtuales en un entorno controlado.

2.1 CREACIÓN DE LA MÁQUINA VIRTUAL

El primer paso consiste en crear una nueva máquina virtual a través del hipervisor seleccionado. Se debe asignar un nombre descriptivo a la máquina virtual, como "NethServer-VM", para facilitar su identificación. A continuación, se configura el tipo y versión del sistema operativo; en este caso, se selecciona "Linux" y "Other Linux (64-bit)" debido a que NethServer se basa en CentOS. Este ajuste garantiza la correcta asignación de recursos y la compatibilidad del sistema operativo invitado.

Figura 1. *Creación Máquina Virtual.*

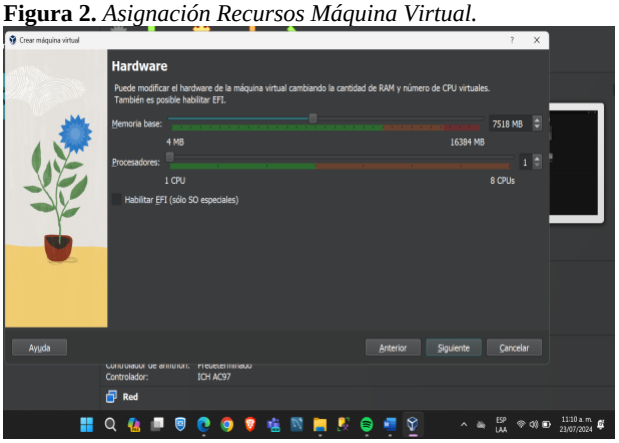


Fuente. Autoria Propia.

2.2 ASIGNACIÓN DE RECURSOS

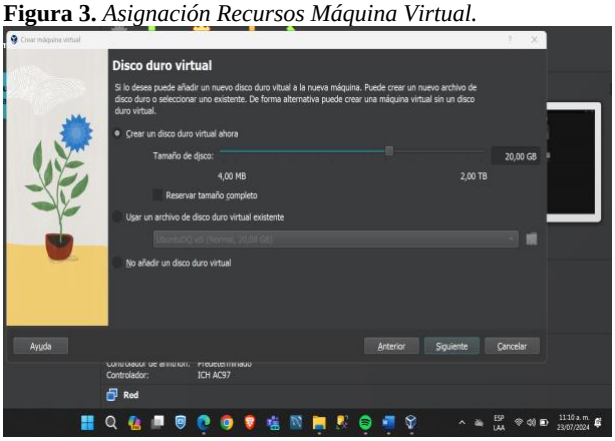
La asignación de recursos a la máquina virtual es crucial para su rendimiento. Se debe especificar la cantidad de memoria RAM, recomendando un mínimo de 2 GB para asegurar un funcionamiento fluido. En cuanto al almacenamiento, se debe crear un disco duro virtual con un tamaño suficiente para la instalación y operación de NethServer; se recomienda al menos 20 GB para permitir la instalación de paquetes y el almacenamiento de datos. Además, es necesario configurar el tipo de disco duro como "Dynamically allocated" para gestionar eficientemente el espacio en disco.

Figura 2. *Asignación Recursos Máquina Virtual.*



Fuente. Autoria Propia.

Figura 3. *Asignación Recursos Máquina Virtual.*

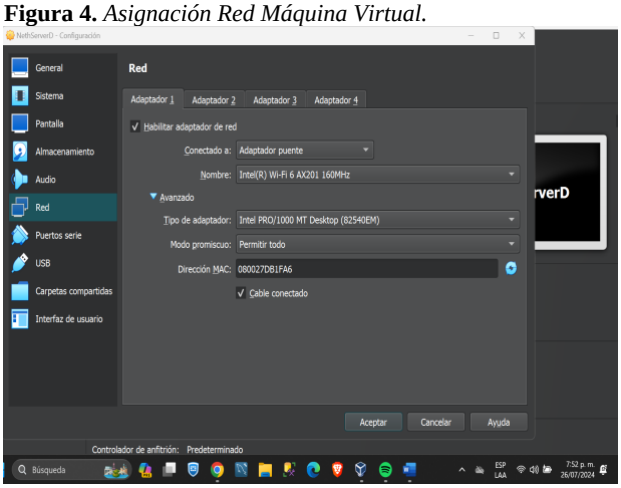


Fuente. Autoria Propia.

2.3 CONFIGURACIÓN DE RED

La configuración de la red es otro aspecto fundamental. Se debe ajustar la interfaz de red de la máquina virtual para que esté en modo "Bridged Adapter" o "NAT" según las necesidades de red del entorno de prueba. El modo "Bridged Adapter" permite que la máquina virtual obtenga una dirección IP en la misma red que el host, facilitando la comunicación directa con otros dispositivos. Alternativamente, el modo "NAT" permite que la máquina virtual comparta la conexión de red del host, lo que es útil para entornos aislados.

Figura 4. *Asignación Red Máquina Virtual.*

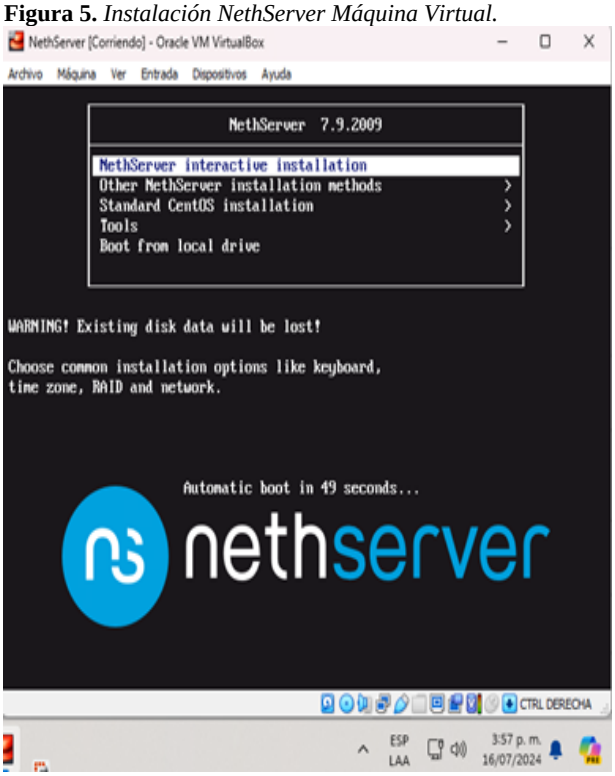


Fuente. Autoria Propia.

2.4 INSTALACIÓN DEL SISTEMA OPERATIVO

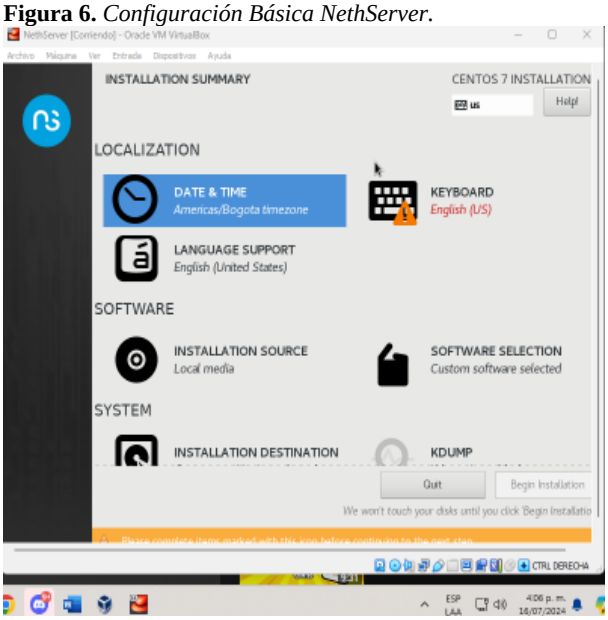
Una vez configurada la máquina virtual, se debe iniciar y montar la imagen ISO de NethServer en la unidad óptica virtual. La imagen ISO puede descargarse desde el sitio web oficial de NethServer. Al iniciar la máquina virtual, el proceso de instalación de NethServer comenzará automáticamente desde la imagen ISO. Se debe seguir el asistente de instalación, que guiará a través de la configuración inicial del sistema, incluyendo la partición del disco, la configuración de red y la selección de paquetes.

Figura 5. *Instalación NethServer Máquina Virtual.*



Fuente. Autoria Propia.

Figura 6. *Configuración Básica NethServer.*



Fuente. Autoria Propia.

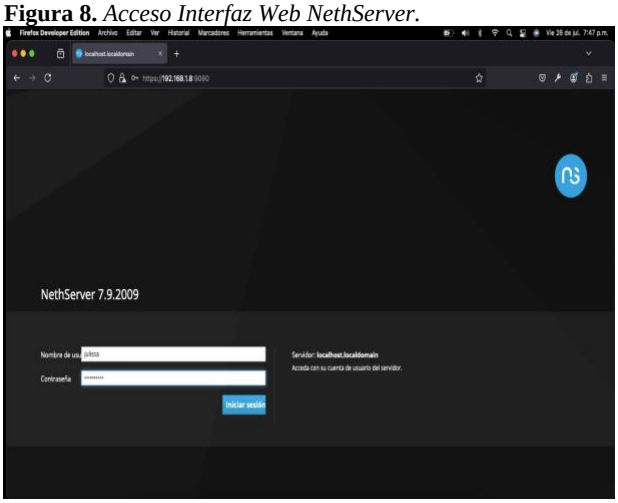
Figura 7. *Configuración Usuario NethServer.*

Fuente. Autoria Propia.

2.5 CONFIGURACIÓN INICIAL DE NETHSERVER

Tras completar la instalación, la máquina virtual se reiniciará y se deberá realizar la configuración inicial de NethServer a través de su interfaz web. Accediendo a la dirección IP asignada a la máquina virtual desde un navegador web, se puede configurar el servidor, estableciendo parámetros como la zona horaria, el nombre del servidor y la configuración de servicios iniciales.

Figura 8. *Acceso Interfaz Web NethServer.*



Fuente. Autoria Propia.

3 CONFIGURACIÓN INTEGRAL DE SERVICIOS DE RED Y SEGURIDAD

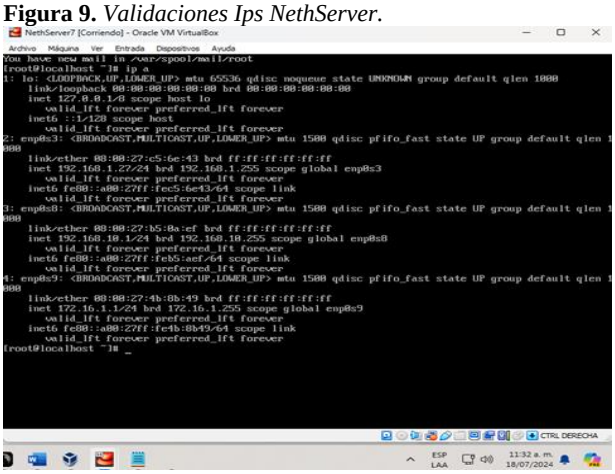
En el ámbito de la administración de redes y seguridad, la configuración integral de servicios críticos es esencial para garantizar una infraestructura IT robusta y segura. Este artículo explora el proceso de implementación y configuración de servicios fundamentales como DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos, Servidor de Archivos, Servidor de Impresiones y VPN. Cada uno de estos componentes desempeña un papel crucial en la gestión eficiente de redes y la protección de datos. La correcta configuración y administración de estos servicios aseguran la integridad, disponibilidad y confidencialidad de la información en un entorno de red, optimizando el rendimiento y la seguridad general del sistema.

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

El proceso de configuración de la máquina virtual se inicia con la importación de la imagen ISO de Nethserver. En este contexto, al primer adaptador de red se le asigna un adaptador en modo puente, lo que permite la comunicación directa con la red física subyacente. Para el segundo adaptador, se establece una red interna etiquetada como 'RVERDE', destinada a la segmentación de tráfico interno. Adicionalmente, un tercer adaptador es configurado para una red interna denominada 'RNARANJA', con el objetivo de aislar segmentos específicos de la red para aplicaciones o servicios diferenciados.

Una vez completada la instalación, se accede al sistema utilizando comandos para validar la configuración de las interfaces de red y verificar las direcciones IP asignadas a cada adaptador. Esto se realiza típicamente mediante comandos como ip addr o ifconfig, proporcionando información sobre la conectividad de red y la asignación de IPs.

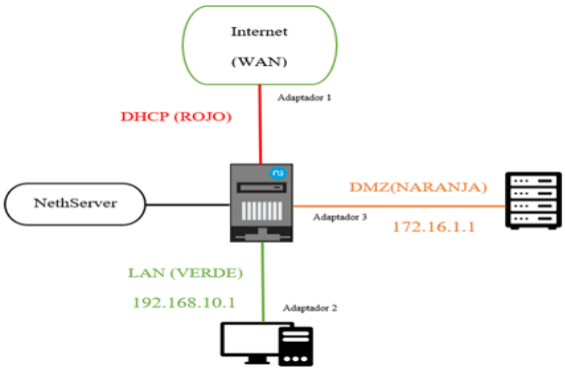
Figura 9. *Validaciones Ips NethServer.*



Fuente. Autoria Propia, Wilson Benitez.

Las ips anteriormente configuradas se asignaron de acuerdo con el diagrama de red.

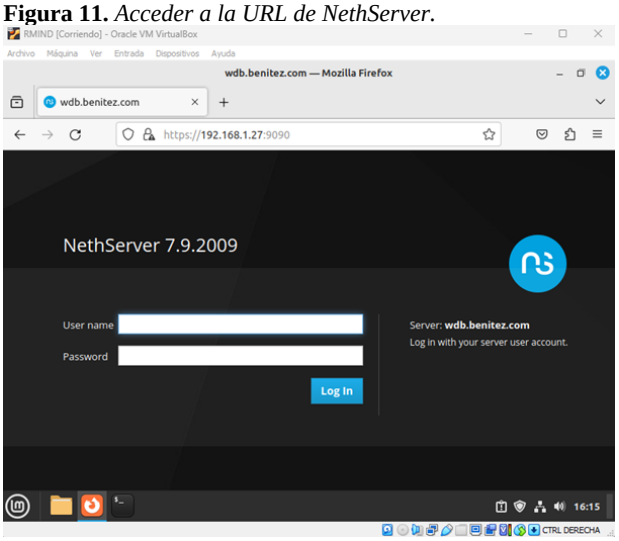
Figura 10. *Diagrama de Red.*



Fuente. Autoria Propia, Wilson Benitez.

Posteriormente, se abre un navegador web e ingresa la URL del servidor NethServer.

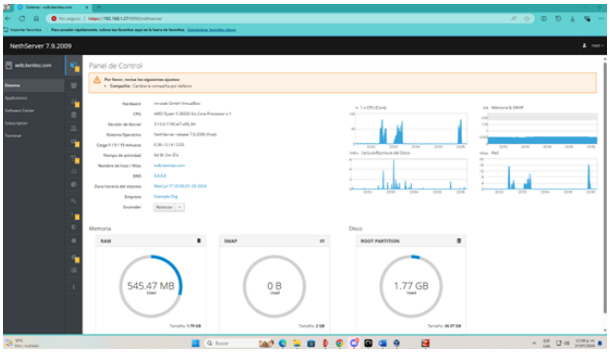
Figura 11. *Acceder a la URL de NethServer.*



Fuente. Autoria Propia, Wilson Benitez.

Se inicia sesión con el usuario ROOT, lo cual proporciona acceso administrativo al panel de control del NethServer.

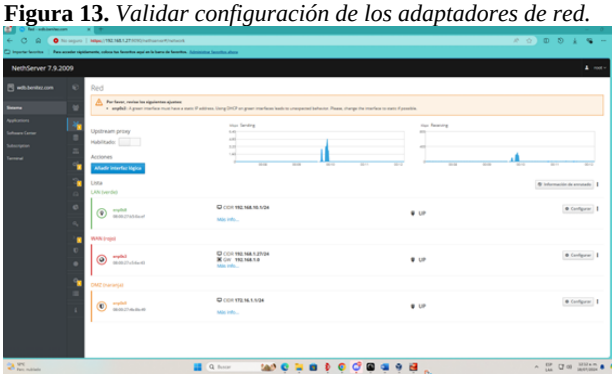
Figura 12. *Inicio de Sesión en el panel gráfico de NethServer.*



Fuente. Autoria Propia, Wilson Benitez.

En el panel de control, se selecciona la opción 'Red' para revisar las interfaces de red previamente configuradas, permitiendo la visualización y verificación de las redes identificadas como verde (RVERDE), roja (WAN) y naranja (RNARANJA). Esta sección permite la supervisión y ajuste de la configuración de red de acuerdo con las necesidades operativas.

Figura 13. *Validar configuración de los adaptadores de red.*



Fuente. Autoria Propia, Wilson Benitez.

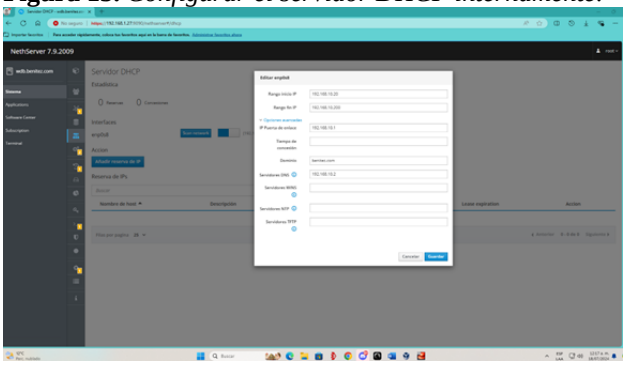
En la sección 'Servidor DHCP', se selecciona la opción 'Scan network' para realizar un escaneo de la red y configurar los parámetros del servicio DHCP.

Figura 14. *Configurar el servidor DHCP.*

Fuente. Autoria Propia, Wilson Benitez.

Se define el rango de direcciones IP que el servidor DHCP asignará automáticamente, así como la puerta de enlace predeterminada, el dominio y los servidores DNS. Esta configuración facilita la administración dinámica de direcciones IP en la red.

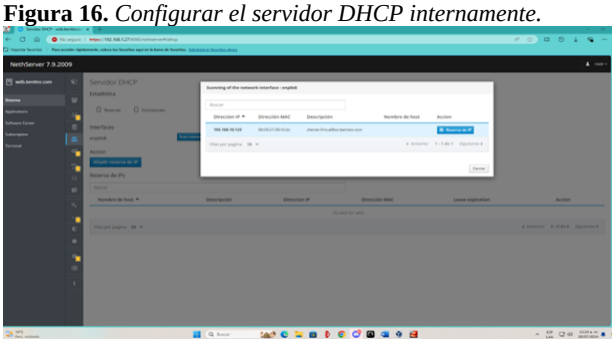
Figura 15. *Configurar el servidor DHCP internamente.*



Fuente. Autoria Propia, Wilson Benitez.

Se establece una reserva de IP para la red LAN (RVERDE), asegurando que ciertos dispositivos o servicios reciban una dirección IP específica dentro de la red.

Figura 16. *Configurar el servidor DHCP internamente.*



Fuente. Autoria Propia, Wilson Benitez.

En la sección 'DNS' del panel, se selecciona 'Añadir registro DNS' para configurar registros DNS adicionales. Se introduce el nombre del dominio y la dirección IP asociada, permitiendo que el servidor resuelva nombres de dominio a direcciones IP correspondientes, lo que es crucial para la resolución de nombres y la comunicación de servicios dentro y fuera de la red.

Figura 17. *Configurar el servidor DNS.*

Fuente. Autoria Propia, Wilson Benitez.

Finalmente, en la sección 'Usuarios y Grupos', bajo la opción 'Active Directory', se configura el nombre del Active Directory (AD) y la IP asociada. Esto permite que el servidor se integre con el dominio Active Directory existente, facilitando la gestión de usuarios y políticas de red dentro del entorno corporativo.

Figura 18. *Configurar Usuarios y Grupos (Directorio Activo).*

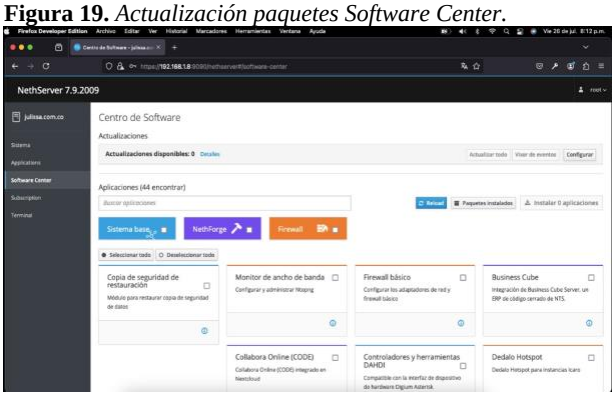
Fuente. Autoria Propia, Wilson Benitez.

3.2 PROXY

Un servidor proxy actúa como intermediario entre un cliente y un servidor, permitiendo a los usuarios acceder a recursos de red de manera indirecta. Los proxies se utilizan ampliamente para mejorar la seguridad, gestionar el tráfico de red y proporcionar funciones de caché para acelerar el acceso a los datos. Además, los proxies pueden filtrar contenido y controlar el acceso a sitios web, lo que resulta especialmente útil en entornos corporativos e institucionales. La implementación de un proxy eficiente es fundamental para optimizar el rendimiento de la red y asegurar la integridad de los datos.

En la interfaz web de NethServer, se debe navegar al Software Center para garantizar que todos los paquetes estén actualizados. Este procedimiento es crucial para mantener la seguridad y el rendimiento del sistema. En la sección de Software Center, se pueden revisar y aplicar las actualizaciones disponibles para todos los componentes instalados, asegurando así que el sistema opere con las versiones más recientes y seguras de los paquetes.

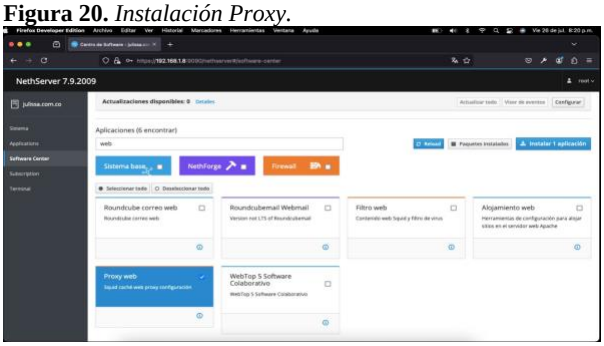
Figura 19. *Actualización paquetes Software Center.*



Fuente. Autoria Propia, Dannia Quevedo.

En la interfaz web de NethServer, se debe navegar al **Software Center**, donde se realiza una búsqueda del paquete **Web Proxy**. Una vez localizado, se procede con la instalación de dicho paquete para habilitar las funcionalidades de proxy en el servidor. Este paso es esencial para configurar y gestionar adecuadamente el acceso y control del tráfico de red a través del proxy.

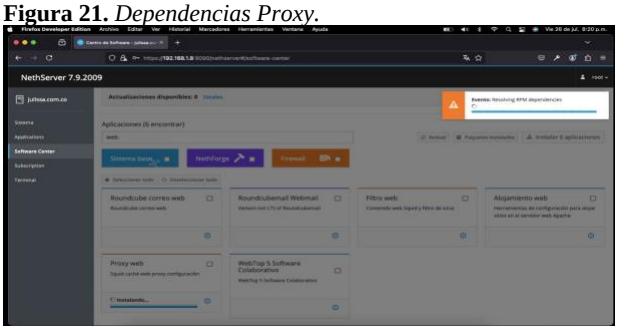
Figura 20. *Instalación Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

Es fundamental asegurar que la descarga del paquete **Web Proxy** se haya completado con éxito y que todas las dependencias necesarias se hayan instalado correctamente. Este paso garantiza que el sistema funcione de manera óptima y sin errores, permitiendo que el proxy desempeñe su función de manera efectiva en la gestión y control del tráfico de red.

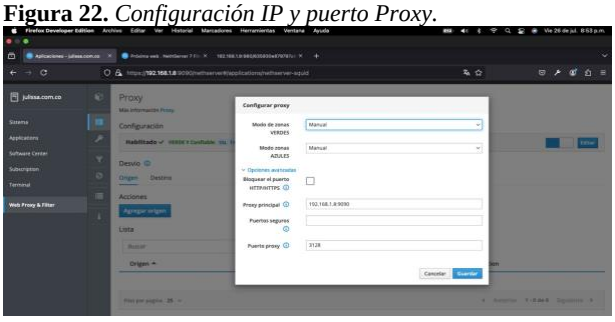
Figura 21. *Dependencias Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

En la configuración general del proxy, se habilita la opción de configuración manual. Específicamente, se define la IP del proxy principal y se establece el uso del puerto 3128 para la comunicación del proxy. Esta configuración es crucial para asegurar que el tráfico de red sea dirigido correctamente a través del proxy, permitiendo un control eficiente y una administración adecuada del acceso a los recursos de la red.

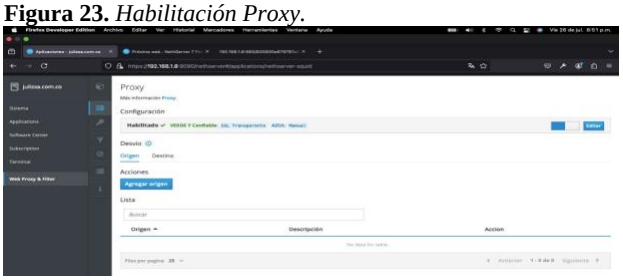
Figura 22. *Configuración IP y puerto Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

Luego de guardar la configuración, se verifica que la configuración establecida se visualice como **Habilitada**. Esta confirmación es esencial para asegurar que los cambios realizados en la configuración del proxy se han aplicado correctamente y que el sistema está preparado para gestionar el tráfico de red de acuerdo con las nuevas directrices establecidas.

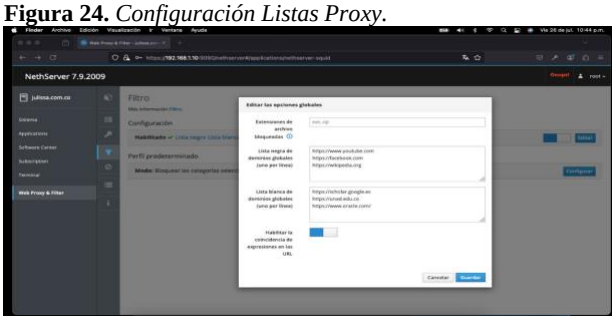
Figura 23. *Habilitación Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

En las opciones de **Filtro** de la configuración del proxy, se definen las **Listas Negras** para bloquear el acceso a sitios específicos y las **Listas Blancas** para permitir el acceso a sitios autorizados. Esta configuración permite un control granular sobre el contenido accesible a través de la red, mejorando la seguridad y asegurando que los usuarios solo puedan acceder a recursos aprobados mientras se restringe el acceso a contenido no deseado o potencialmente peligroso.

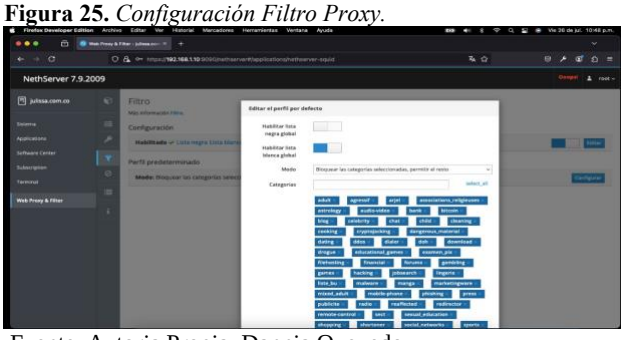
Figura 24. *Configuración Listas Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

También, en las opciones de **Filtro** de la configuración del proxy, se configuran categorías para sitios inapropiados o que puedan representar un riesgo en la administración de datos. Esta medida asegura una navegación segura y controlada, protegiendo a los usuarios y la integridad de la red al evitar el acceso a contenido que podría comprometer la seguridad de los datos o exponer a los usuarios a riesgos innecesarios.

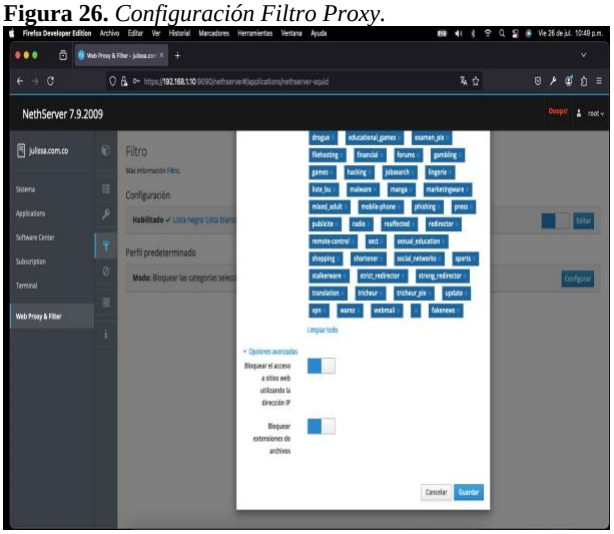
Figura 25. *Configuración Filtro Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

Adicionalmente, en las opciones avanzadas del proxy, se habilitan las funciones para bloquear el acceso a sitios web utilizando la dirección IP y para bloquear extensiones de archivos específicas. Estas configuraciones fortalecen la seguridad de la red y previenen la descarga de contenido potencialmente peligroso, protegiendo así a los usuarios y a la infraestructura de posibles amenazas y vulnerabilidades.

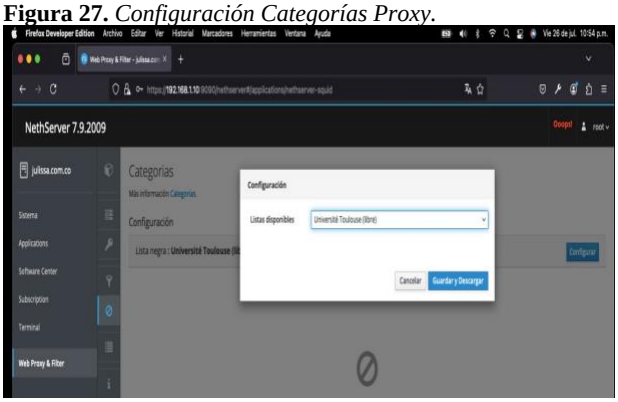
Figura 26. *Configuración Filtro Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

En las categorías de configuración del proxy, se selecciona **"Université Toulouse (libre)"** debido a que ofrece reglas predefinidas optimizadas para instituciones académicas. Esta selección permite equilibrar el acceso a recursos educativos con la seguridad y el control del tráfico de red, proporcionando un entorno seguro y eficiente para el uso de internet en contextos académicos.

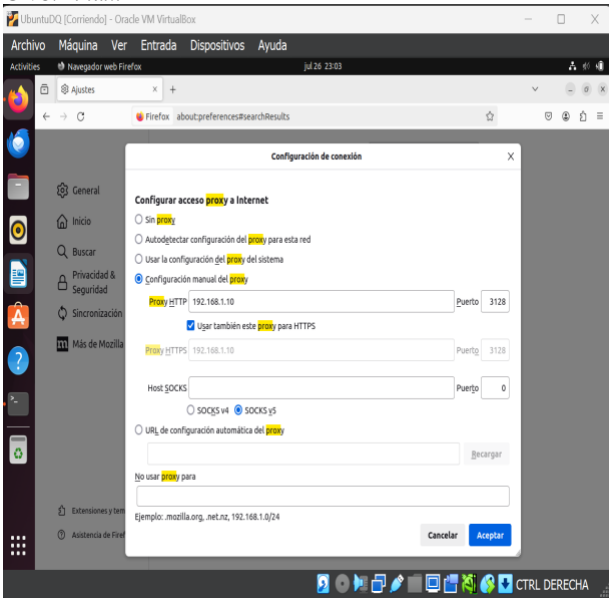
Figura 27. *Configuración Categorías Proxy.*



Fuente. Autoria Propia, Dannia Quevedo.

Una vez configurado el proxy, se ajusta una estación GNU/Linux (Ubuntu) para que se comunique con NethServer a través del puerto 3128, asegurando una correcta integración del servicio. En Ubuntu, se configura Firefox para usar el proxy en la dirección IP de NethServer (192.168.1.10) y el puerto 3128. Esta configuración garantiza que todo el tráfico web de la estación pase a través del proxy, permitiendo la aplicación de las políticas de filtrado y seguridad definidas en NethServer.

Figura 28. *Configuración Navegador Firefox estación GNU/Linux.*



Fuente. Autoria Propia, Dannia Quevedo.

Además, se configura a nivel del sistema el uso de los datos del proxy de NethServer editando el archivo de configuración del proxy en /etc/environment. Esta configuración asegura que todas las aplicaciones y servicios que requieran acceso a la red en la estación GNU/Linux utilicen el proxy configurado, proporcionando una capa adicional de control y seguridad en la comunicación de red.

Figura 29. *Configuración Sistema Estación GNU/Linux.*

Fuente. Autoria Propia, Dannia Quevedo.

Para aplicar estos cambios, se ejecuta el comando source /etc/environment y se reinicia la estación GNU/Linux con el comando reboot. Esto garantiza que todas las aplicaciones y servicios del sistema utilicen la configuración del proxy definida, asegurando una integración completa y efectiva con el servidor NethServer.

Figura 30. *Ejecución Comando.*

Fuente. Autoria Propia, Dannia Quevedo.

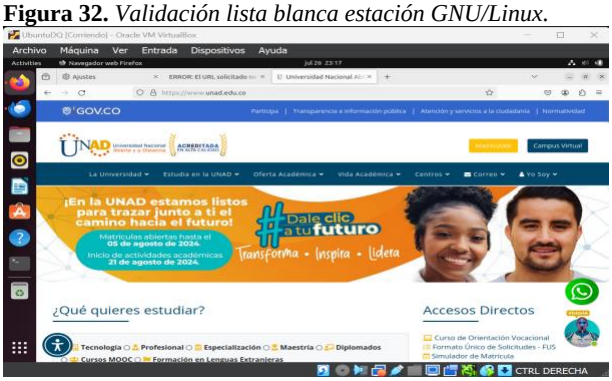
Se accede a Internet desde la estación GNU/Linux y se verifica que el tráfico pasa a través del proxy. Para confirmar que las reglas de filtrado están funcionando correctamente, se realiza una prueba de lista negra intentando acceder a un sitio bloqueado, como https://www.youtube.com. En un caso exitoso, el acceso es denegado, validando así que las políticas de restricción implementadas en el proxy están operando de manera efectiva.

Figura 31. *Validación lista negra estación GNU/Linux.*

Fuente. Autoria Propia, Dannia Quevedo.

También, en un caso exitoso de lista blanca, se accede a un sitio permitido, como https://unad.edu.co, y se verifica que el acceso es concedido. Esto asegura que el proxy está operando según lo configurado, permitiendo el acceso a los sitios autorizados mientras bloquea aquellos que están en la lista negra. Esta verificación confirma la correcta implementación y funcionamiento de las políticas de filtrado del proxy.

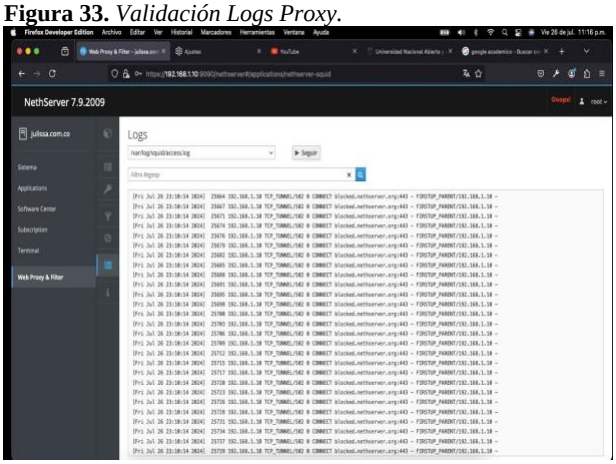
Figura 32. *Validación lista blanca estación GNU/Linux.*



Fuente. Autoria Propia, Dannia Quevedo.

Finalmente, desde la interfaz web de NethServer, se pueden revisar los logs del proxy para evidenciar la actividad de las pruebas y validaciones. Esta revisión permite confirmar que el tráfico se está manejando correctamente a través del puerto 3128, de acuerdo con la configuración del proxy. La verificación de los logs es crucial para asegurar que todas las políticas de filtrado y control de acceso están operando como se espera, proporcionando una capa adicional de seguridad y control en la gestión del tráfico de red.

Figura 33. *Validación Logs Proxy.*

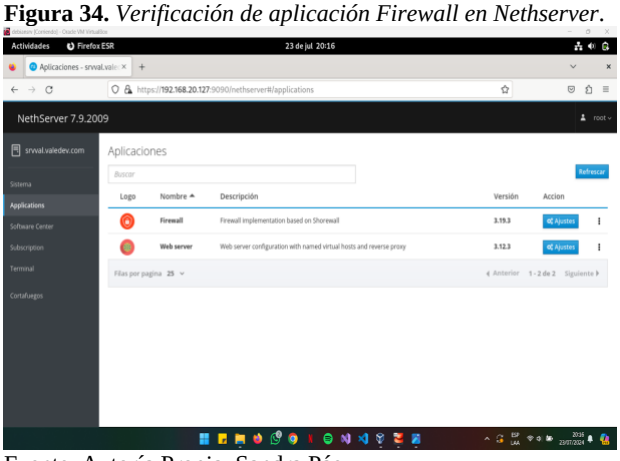


Fuente. Autoria Propia, Dannia Quevedo.

3.3 CORTAFUEGOS

Se realiza configuración de restricciones de sitios web de ocio y entretenimiento como Facebook o YouTube, para esto se requiere de las configuraciones de IP en zona verde, naranja y roja, con ello realizar las validaciones de acceso. posteriormente de Nethserver se instalará el software de firewall básico el cual permitirá anexar las reglas que se desean implementar.

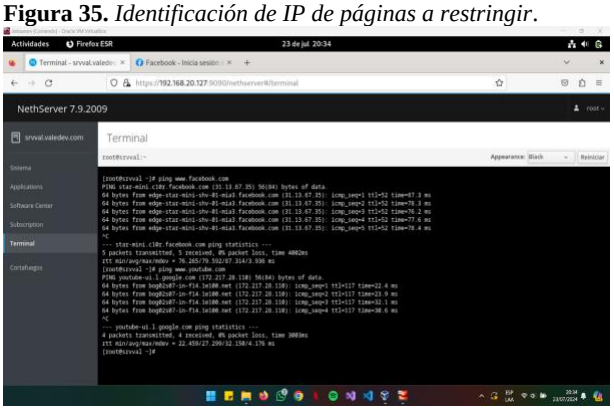
Figura 34. *Verificación de aplicación Firewall en Nethserver.*



Fuente. Autoría Propia, Sandra Páez.

Posteriormente se realiza la ubicación de la IP de las páginas que se desean bloquear mediante el uso del comando Ping en la terminal. Esto, además de identificar la IP nos permite validar que la página que deseamos restringir está activa en la red global.

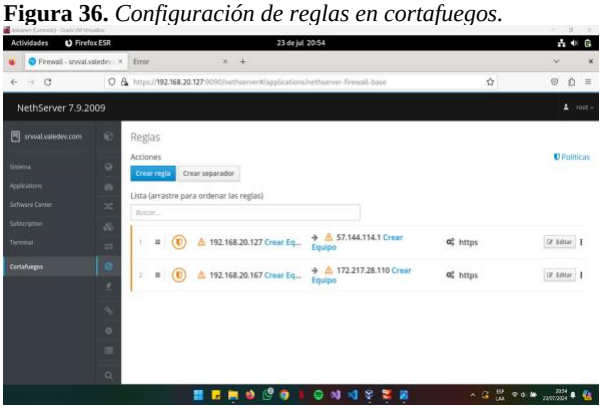
Figura 35. *Identificación de IP de páginas a restringir.*



Fuente. Autoría Propia, Sandra Páez.

Al tener identificadas las IP se realiza el proceso de restricción de páginas para lo cual en la aplicación cortafuegos se ingresa al apartado “Reglas”, en el cual se debe ingresar la IP de origen que es la IP del equipo desde el cual se va a realizar la restricción, y la IP de destino, la cual es la página que se va a restringir, se realiza la restricción en servicios https y se selecciona la acción que ejecutará la regla, en este caso se bloquea el acceso a estos sitios.

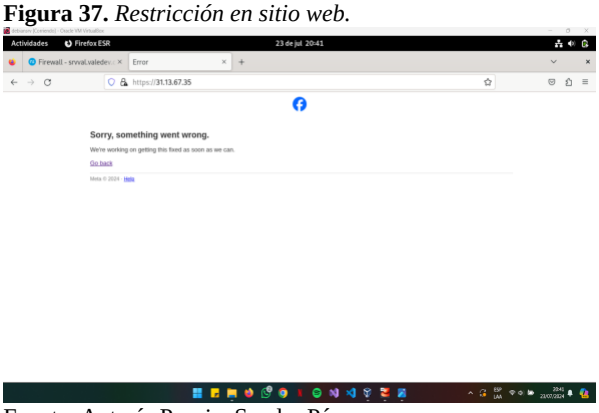
Figura 36. *Configuración de reglas en cortafuegos.*



Fuente. Autoría Propia, Sandra Páez.

Al acceder a las páginas web restringidas nos mostrará un mensaje de error ya que desde esta IP tenemos un acceso denegado a la página.

Figura 37. *Restricción en sitio web.*

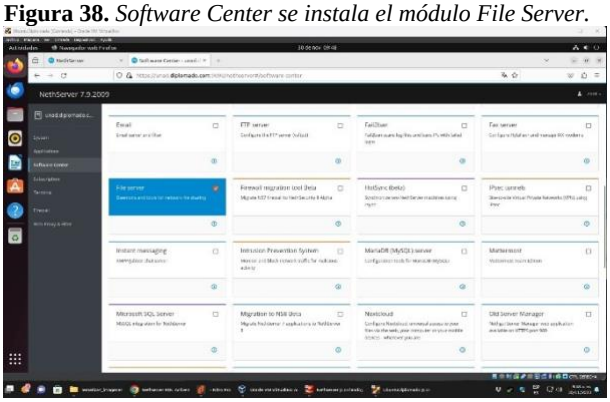


Fuente. Autoría Propia, Sandra Páez.

3.4 FILE SERVER Y PRINT SERVER

Configuración e implementación detallada para permitir que una estación de trabajo GNU/Linux acceda a servicios de carpetas compartidas e impresoras mediante un controlador de dominio LDAP.

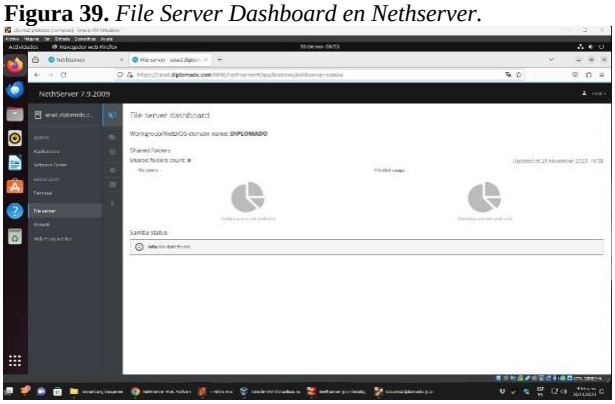
Figura 38. *Software Center se instala el módulo File Server.*



Fuente. Autoría Propia, Yenny Perez.

El módulo de Servidor de Archivos es responsable de administrar los archivos compartidos en Nethserver.

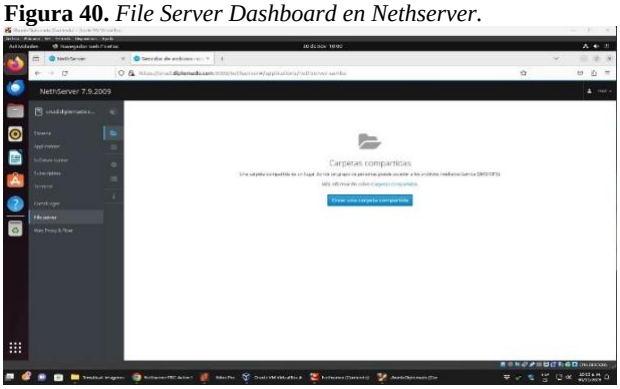
Figura 39. *File Server Dashboard en Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

En el panel de control del servidor de archivos, observamos el grupo de trabajo, que en este caso se llama "DIPLOMADO".

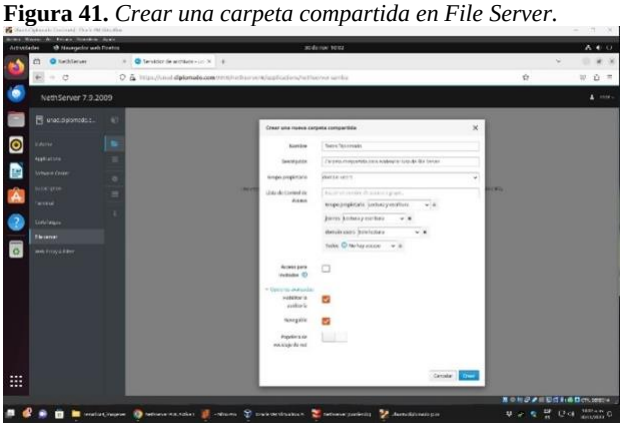
Figura 40. *File Server Dashboard en Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

Las carpetas compartidas usan los servicios de samba (SMB/CIFS).

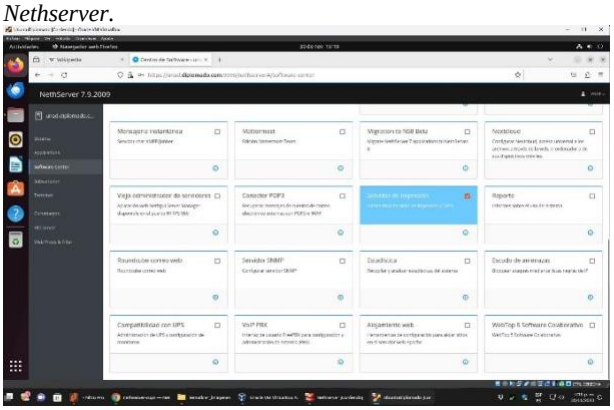
Figura 41. *Crear una carpeta compartida en File Server.*



Fuente. Autoría Propia, Yenny Perez.

Para este ejercicio práctico, se configura una carpeta compartida denominada "Datos Diplomado" y el dominio domain_users, activando la Auditoría.

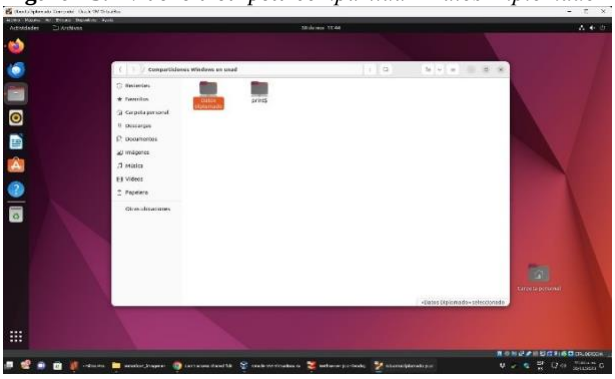
Figura 42. *Instalación del módulo de impresión en Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

El módulo de gestión de impresión en Nethserver se encarga de la administración del servicio de impresión de documentos.

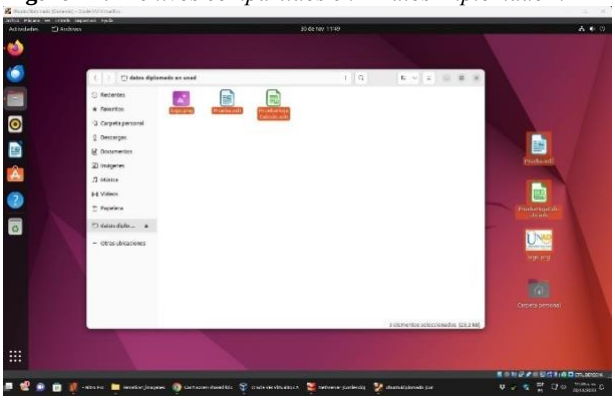
Figura 43. *Evidencia carpeta compartida "Datos Diplomado"*



Fuente. Autoría Propia, Yenny Perez.

La carpeta denominada "Datos Diplomados" se encuentra accesible a través de la red utilizando el protocolo LDAP.

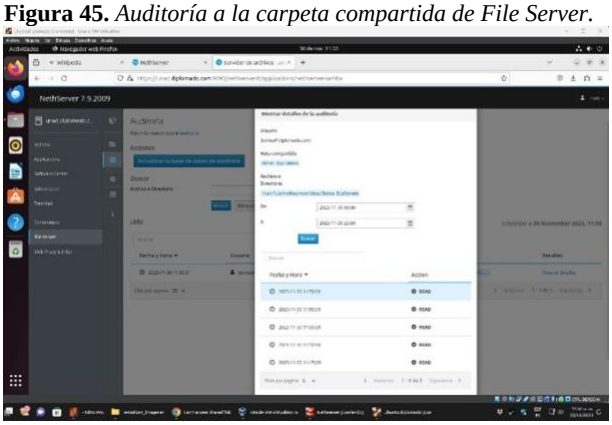
Figura 44. *Archivos compartidos en "Datos Diplomado".*



Fuente. Autoría Propia, Yenny Perez.

En este ensayo, se demuestra que la carpeta puede contener archivos de diversos formatos. En este caso, se incluyeron imágenes, un documento de texto y una hoja de cálculo.

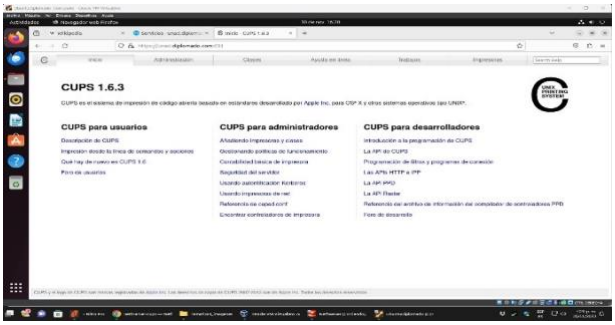
Figura 45. *Auditoría a la carpeta compartida de File Server.*



Fuente. Autoría Propia, Yenny Perez.

El registro muestra la fecha y hora del acceso, la ruta de red utilizada por el usuario y la acción ejecutada, que puede ser READ o WRITE.

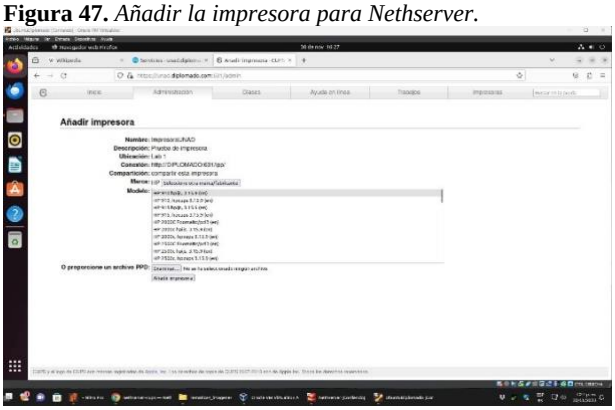
Figura 46. *Configurando servicio de impresión en Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

En el módulo de configuración de CUPS, se encuentran todas las opciones necesarias para ajustar las impresoras para su utilización en la red.

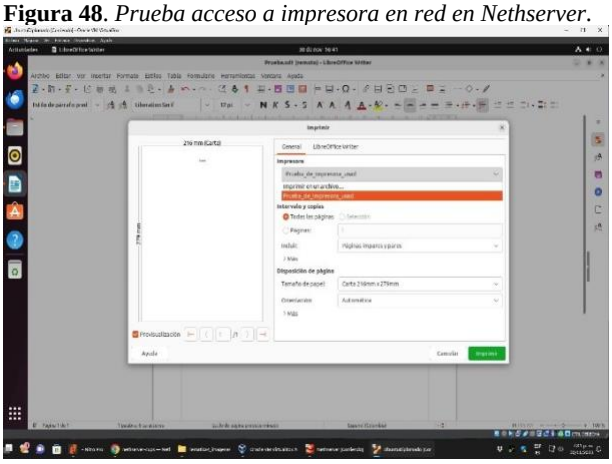
Figura 47. *Añadir la impresora para Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

El menú de configuración del servidor de impresión abarca una variedad de modelos y marcas de impresoras disponibles en el mercado.

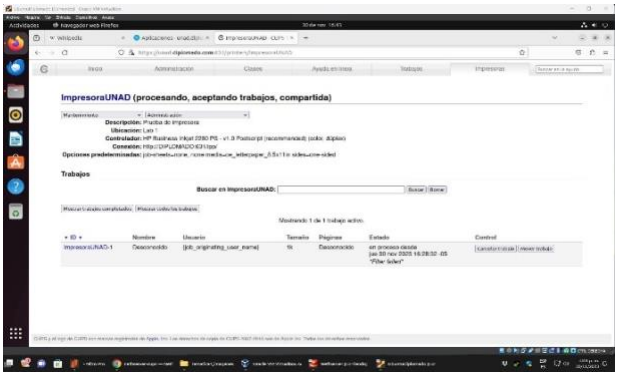
Figura 48. *Prueba acceso a impresora en red en Nethserver.*



Fuente. Autoría Propia, Yenny Perez.

En esta demostración práctica, se realiza una impresión de un documento y se observa la impresora en red desde el usuario de Desktop (Red Verde).

Figura 49. *Evidencia cola de impresión en Nethserver.*



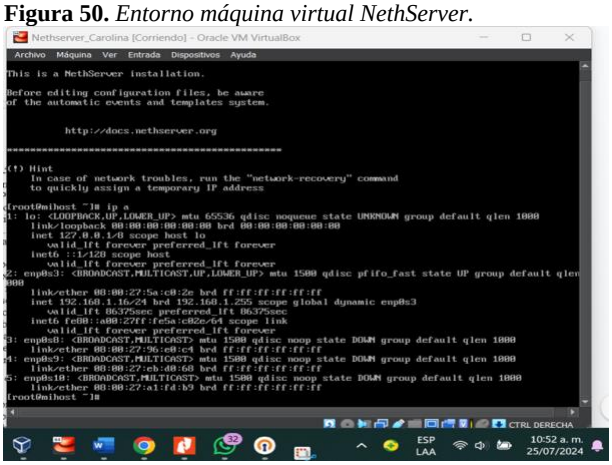
Fuente. Autoría Propia, Yenny Perez.

Al acceder a la configuración de impresoras en Nethserver, se puede observar la impresión que se envió desde el usuario Desktop a través del servicio de Print Server.

3.5 VPN

Se lleva a cabo la implementación y configuración detallada de una VPN para establecer un túnel de comunicación privado con una estación de trabajo GNU/Linux, demostrando el acceso a contenido o aplicaciones en la estación. Tras instalar NethServer en una máquina virtual, se verifica la dirección IP asignada, en este caso 192.168.1.16, para asegurar la correcta integración en la red.

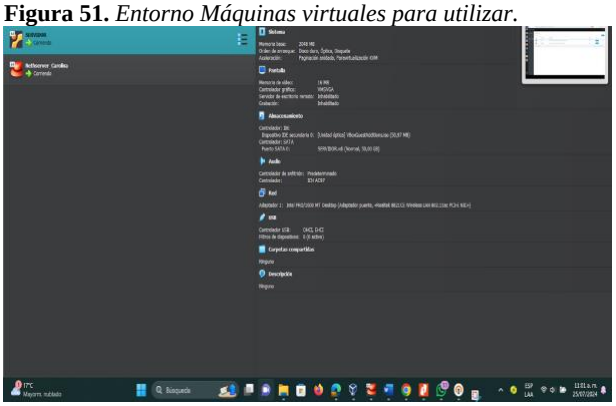
Figura 50. *Entorno máquina virtual NethServer.*



Fuente. Autoría Propia, Ana Cifuentes.

Con el objetivo de continuar con el proceso de configuración y pruebas, se utiliza una máquina virtual adicional con Ubuntu, denominada "servidor". Esta máquina complementa la infraestructura existente y permite realizar las configuraciones y pruebas necesarias de manera eficiente.

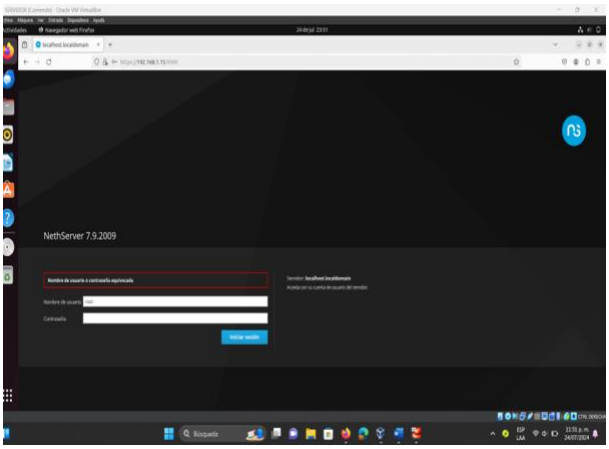
Figura 51. *Entorno Máquinas virtuales para utilizar.*



Fuente. Autoría Propia, Ana Cifuentes.

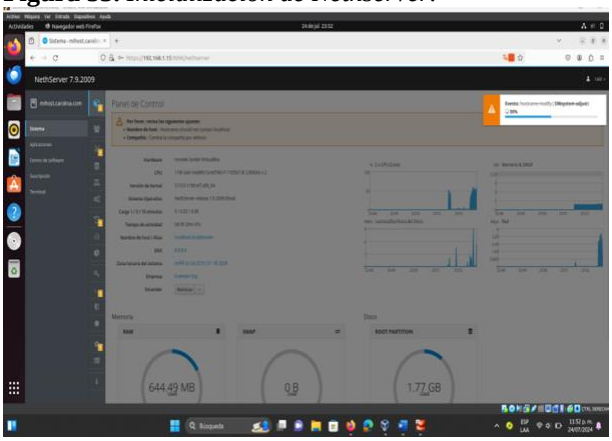
Una vez que la máquina virtual de Ubuntu está en funcionamiento, se abre el navegador web y se accede a la interfaz de NethServer mediante la dirección 192.168.1.16:9090. A continuación, se requiere ingresar el nombre de usuario y la contraseña establecidos durante la instalación de NethServer para acceder al entorno administrativo.

Figura 52. E*ntorno de inicio de Nethserver.*



Fuente. Autoría Propia, Ana Cifuentes.

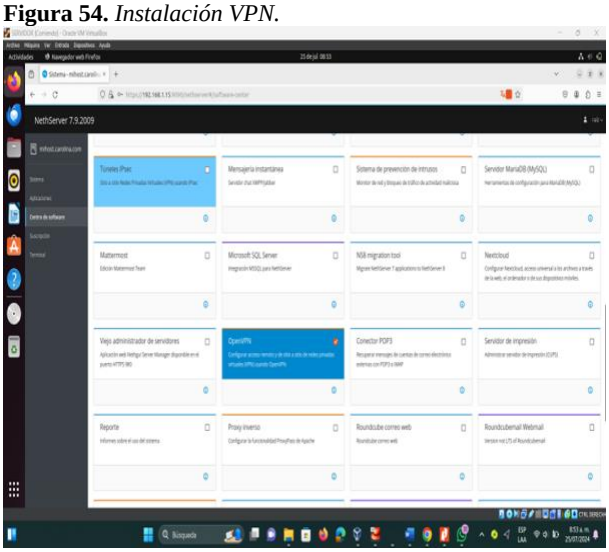
Figura 53. *Inicialización de Nethserver.*



Fuente. Autoría Propia, Ana Cifuentes.

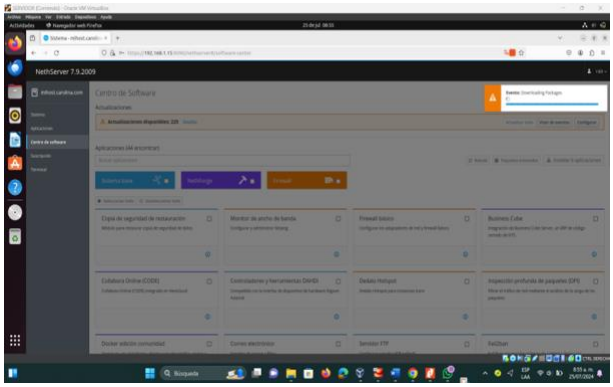
A continuación, se procede con la instalación de OpenVPN desde el menú "Centro de Software". Se busca la aplicación VPN y se selecciona para su instalación.

Figura 54. *Instalación VPN.*



Fuente. Autoría Propia, Ana Cifuentes.

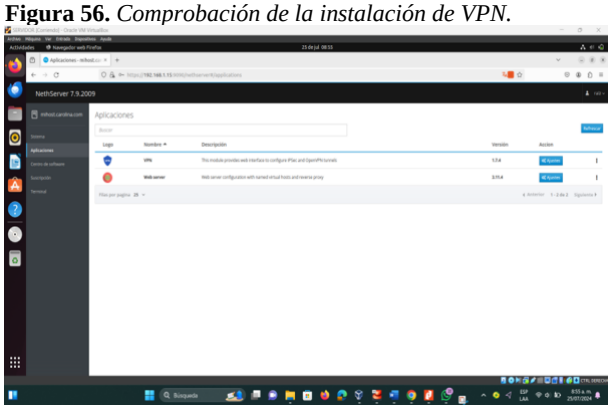
Figura 55. *Instalación VPN.*



Fuente. Autoría Propia, Ana Cifuentes.

En el menú, bajo el apartado de aplicaciones, se verifica la correcta instalación de la aplicación VPN.

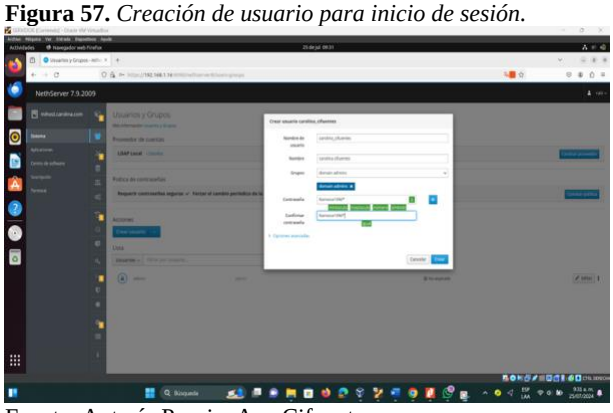
Figura 56. *Comprobación de la instalación de VPN.*



Fuente. Autoría Propia, Ana Cifuentes.

Se configura el túnel de la VPN creando un nuevo usuario. Para ello, se accede al menú "Sistema", seleccionando "Usuarios", y se elige la opción "Crear nuevo usuario". Este usuario será utilizado para el proceso de inicio de sesión en la VPN.

Figura 57. *Creación de usuario para inicio de sesión.*



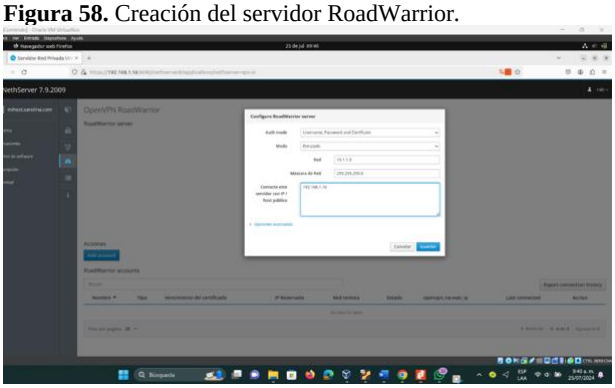
Fuente. Autoría Propia, Ana Cifuentes.

A continuación, se accede al apartado de "Aplicaciones", seleccionando "VPN" y luego "Ajustes" para configurar un servidor OpenVPN RoadWarrior. Este servidor permitirá establecer la conexión VPN.

En la sección de autenticación, se seleccionan las opciones: "nombre de usuario", "contraseña" y "certificado".

En el modo de red, se elige "enrutado". Se establece la dirección IP como 10.1.1.0 y se configura la máscara de red correspondiente a los requisitos del entorno. Finalmente, se configura el host público con la IP de la configuración inicial, asignada como WAN.

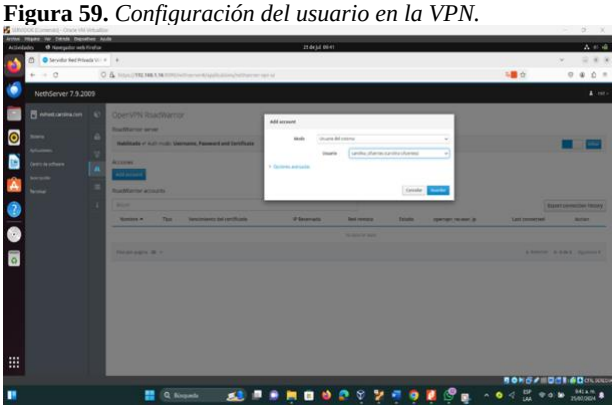
Figura 58. Creación del servidor RoadWarrior.



Fuente. Autoría Propia, Ana Cifuentes.

Se añade el usuario previamente creado, **carolina_cifuentes**, al servidor VPN, otorgándole los permisos necesarios para su correcto funcionamiento.

Figura 59. *Configuración del usuario en la VPN.*



Fuente. Autoría Propia, Ana Cifuentes.

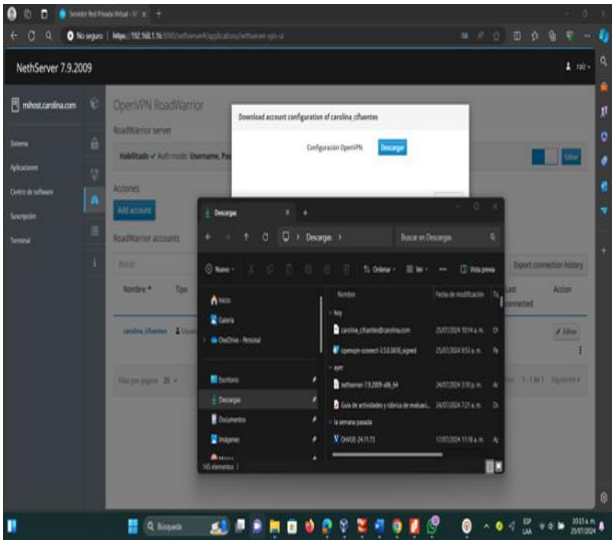
Se procede a instala OpenVPN Connect en el servidor local, que en este caso es una máquina con Windows.

Figura 60. *Descarga e instalación de OpenVPN Connect.*

Fuente. Autoría Propia, Ana Cifuentes.

Desde el sistema operativo local, fuera de VirtualBox, se descarga el archivo de configuración de la VPN. Para ello, se accede al navegador web y se dirige a la siguiente dirección: https://192.168.1.16:9090/nethserver.

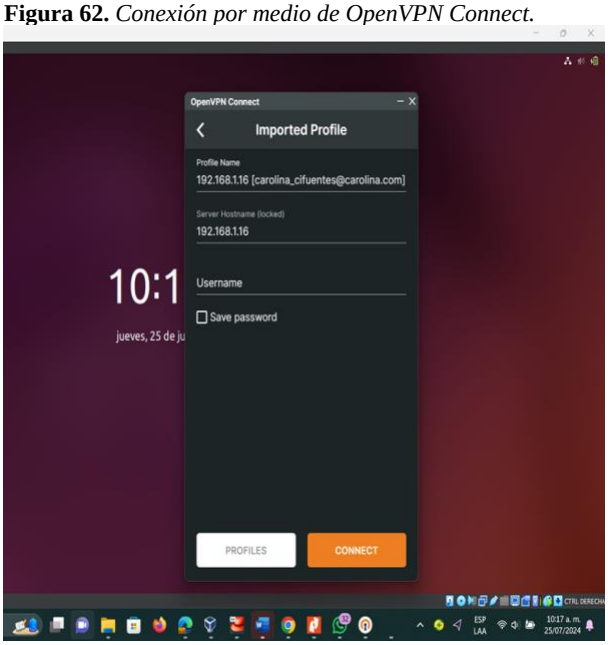
Figura 61. *Descarga del archivo VPN en nuestro servidor local.*



Fuente. Autoría Propia, Ana Cifuentes.

Se importa el archivo descargado, denominado carolina_cifuentes@carolina.com, a la aplicación OpenVPN Connect. Para completar el proceso, se ingresan las credenciales de usuario y contraseña previamente configuradas en NethServer.

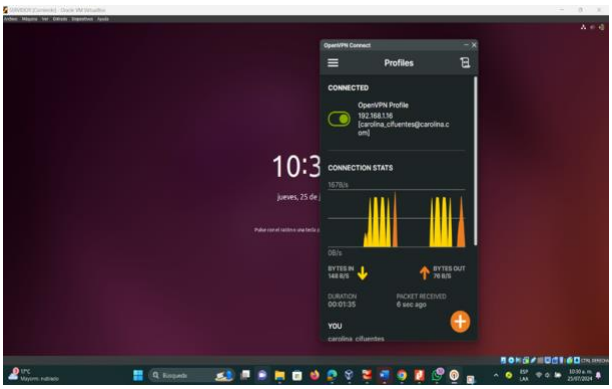
Figura 62. *Conexión por medio de OpenVPN Connect.*



Fuente. Autoría Propia, Ana Cifuentes.

Una vez cargado el archivo en OpenVPN Connect, se selecciona la opción "Conectar". Al hacerlo, se puede verificar que la conexión se ha establecido con éxito.

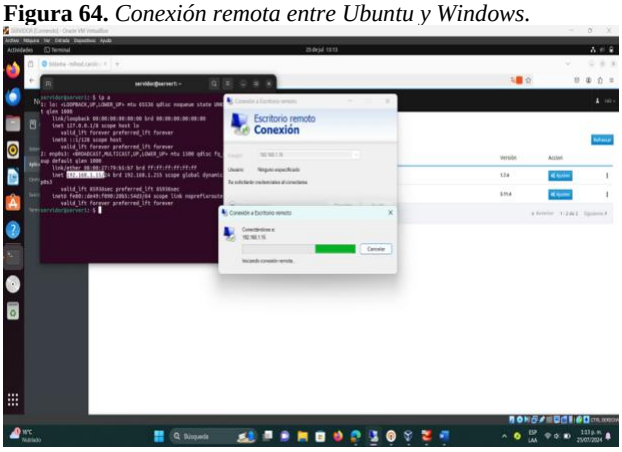
Figura 63. *Conexión exitosa de la VPN.*



Fuente. Autoría Propia, Ana Cifuentes.

Se realiza la conexión remota desde el escritorio remoto de Windows hacia el servidor Ubuntu utilizando la dirección IP 192.168.1.15.

Figura 64. *Conexión remota entre Ubuntu y Windows.*



Fuente. Autoría Propia, Ana Cifuentes.

4 CONCLUSIONES

La implementación y configuración integral de servicios de red en un entorno IT utilizando NethServer y estaciones de trabajo GNU/Linux demuestran la viabilidad y eficacia de gestionar una infraestructura compleja con herramientas de código abierto.

NethServer, derivado de CentOS, ha demostrado ser una plataforma robusta y flexible para la gestión de servicios de red en pequeñas y medianas empresas. Su interfaz gráfica de usuario amigable permite a los administradores, incluso con poca experiencia, configurar y administrar múltiples servicios de red de manera eficiente.

La configuración de servicios críticos como DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos, Servidor de Archivos y Servidor de Impresiones en un entorno unificado reduce significativamente la complejidad de la gestión de la red. Cada servicio configurado en NethServer interactúa de manera armoniosa, proporcionando una solución integral que mejora la eficiencia operativa y la seguridad de la red.

Las pruebas realizadas han evidenciado la estabilidad y el rendimiento de NethServer bajo diferentes cargas de trabajo y configuraciones. La capacidad del sistema para manejar múltiples servicios sin degradar su rendimiento es un testimonio de su diseño optimizado y eficiente.

La interfaz de administración de NethServer simplifica la gestión de usuarios y permisos, permitiendo una administración centralizada de todos los servicios de red. Además, la capacidad de NethServer para escalar y adaptarse a las crecientes demandas de la red hace que sea una solución adecuada para entornos en constante evolución.

La integración de estaciones de trabajo GNU/Linux con NethServer se realizó de manera fluida, demostrando la interoperabilidad y compatibilidad del sistema con diferentes plataformas. Esta característica es esencial para organizaciones que utilizan una combinación de sistemas operativos en su infraestructura de TI.

La utilización de software de código abierto como NethServer y GNU/Linux representa una significativa optimización de recursos y reducción de costos para las organizaciones. La ausencia de licencias costosas y la posibilidad de personalización del software permiten a las empresas destinar recursos a otras áreas críticas.

En resumen, la implementación y configuración de servicios de red mediante NethServer proporciona una solución integral y eficiente para la gestión de infraestructuras IT en entornos empresariales. La combinación de seguridad, facilidad de administración, estabilidad y escalabilidad posiciona a NethServer como una herramienta valiosa para cualquier organización que busque optimizar su infraestructura de red

5 REFERENCIAS

[1] E. De Benedetto, M. Cicognani, and A. Natale, “An open-source approach for network services management: The NethServer case,” in 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, Oct. 2020, pp. 3003-3008. doi: 10.1109/SMC42975.2020.9283095.

[2] R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities,” in 2008 IEEE 10th International Conference on High Performance Computing and Communications, Dalian, China, Sep. 2008, pp. 5-13. doi: 10.1109/HPCC.2008.113.

[3] W. Stallings, “Operating system support for virtual machines,” in Operating Systems (7th ed.). Upper Saddle River, NJ, USA: Prentice Hall, 2005, ch. 7, sec. 2, pp. 331-367.

[4] S. Williamson, “Deploying VPNs: IPsec, SSL, and MPLS,” in The Essentials of Computer Organization and Architecture (4th ed.). Burlington, MA, USA: Jones & Bartlett Learning, 2014, ch. 8, sec. 4, pp. 492-517.

[5] M. E. Russinovich, D. A. Solomon, and A. Ionescu, Windows Internals (6th ed.), Part 1. Redmond, WA, USA: Microsoft Press, 2012.

[6] C. Kim and J. Choi, “Implementation of secure VPN system using OpenVPN,” in 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, South Korea, Oct. 2014, pp. 376-378. doi: 10.1109/ICTC.2014.6983196.

[7] E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Boston, MA, USA: Addison-Wesley, 2001.

[8] T. Anderson, D. Culler, and D. Patterson, “A case for NOW (Networks of Workstations),” in 1995 IEEE International Symposium on High Performance Distributed Computing, Washington, DC, USA, Aug. 1995, pp. 24-26. doi: 10.1109/HPDC.1995.518674.

[9] D. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture (5th ed.). Upper Saddle River, NJ, USA: Prentice Hall, 2006.

[10] F. Adelstein, S. K. Gupta, and G. Richard, “UNIX System Security Tools,” in Fundamentals of Network Security. New York, NY, USA: Springer, 2008, ch. 9, sec. 3, pp. 247-269.

[11] R. A. Day, “A practical guide to securing and optimizing Squid proxy,” in 2004 IEEE International Conference on Networks (ICON), Singapore, Nov. 2004, pp. 241-245. doi: 10.1109/ICON.2004.1409140.

[12] R. P. Goldberg, “Survey of virtual machine research,” Computer, vol. 7, no. 6, pp. 34-45, Jun. 1974. doi: 10.1109/MC.1974.6323581.

[13] C. E. Landwehr, “Formal models for computer security,” ACM Computing Surveys (CSUR), vol. 13, no. 3, pp. 247-278, Sep. 1981. doi: 10.1145/356850.356852.

[14] J. Howard and T. Longstaff, “A common language for computer security incidents,” Sandia National Labs., Albuquerque, NM, USA, Tech. Rep. SAND98-8667, Oct. 1998. doi: 10.2172/663998.

[15] D. Brent Chapman and E. D. Zwicky, Building Internet Firewalls (2nd ed.). Sebastopol, CA, USA: O'Reilly Media, 2000.

[16] M. Steen and P. Hatcher, “Secure and scalable file services for distributed environments,” in 2011 IEEE 7th International Conference on e-Science, Stockholm, Sweden, Dec. 2011, pp. 296-303. doi: 10.1109/eScience.2011.40.

[17] W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols. Reading, MA, USA: Addison-Wesley, 1994.

[18] G. Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems: Concepts and Design (5th ed.). Boston, MA, USA: Addison-Wesley, 2011.

[19] L. Cheng, D. Schwabe, and T. V. Le, “Implementing DHCP for efficient IP address management,” in 2002 IEEE International Conference on Communications (ICC), New York, NY, USA, Apr. 2002, pp. 1661-1665. doi: 10.1109/ICC.2002.997478.

[20] E. G. Amoroso, Fundamentals of Computer Security Technology. Upper Saddle River, NJ, USA: Prentice Hall, 1994.