Enfoque Práctico para el Manejo de Redes y Servicios Usando Nethserver

Carlos David Marquez Valencia
e-mail: cdmarquezv@unadvirtual.edu.co
Diego Andrés Diaz Bautista
e-mail: dadiazba@unadvirtual.edu.co
Ana Lorena Alvarado Ruiz
e-mail: alalvarador@unadvirtual.edu.co
William Alberto Alvarez Campos
e-mail: walvarezc@unadvirtual.edu.co

RESUMEN: *En esta investigación se aborda la implementación y gestión de servicios IT críticos utilizando NethServer en un entorno basado en GNU/Linux, con el objetivo de atender necesidades reales de redes empresariales. Mediante configuraciones detalladas y procedimientos paso a paso. Se integraron servicios fundamentales como DHCP, DNS, Proxy, Cortafuegos, Servidores de Archivos e Impresoras, y VPN.*

Los resultados obtenidos evidencian la capacidad de NethServer para simplificar la administración de redes, mejorando el acceso, la seguridad y el control en intranets y extranets. Asimismo, se demuestra que es posible optimizar la infraestructura tecnológica de una organización de manera eficiente y segura mediante herramientas de software libre, inspirando a otros a implementar estas soluciones en sus propios entornos, utilizando NethServer en un entorno GNU/Linux, abordando necesidades reales de redes empresariales. A través de configuraciones claras y paso a paso, se lograron integrar servicios como DHCP, DNS, Proxy, Cortafuegos, Servidores de Archivos e Impresoras, y VPN.

PALABRAS CLAVE: Administración IT, GNU/Linux, NethServer, Servicios empresariales, Proxy, DNS, DCHP, Cortafuegos, File Server y Print Server, VPN.

1 INTRODUCCIÓN

NethServer es una plataforma basada en Linux diseñada para la administración centralizada de redes y servicios empresariales, ofreciendo herramientas para la gestión de firewall, correo electrónico, archivos compartidos, filtrado web, VPN y control de acceso a internet [1]. Su arquitectura modular, sumada a la facilidad de administración a través de una interfaz web intuitiva, permite a pequeñas y medianas empresas optimizar su infraestructura tecnológica sin incurrir en altos costos de licenciamiento [2]. Además, la adopción de soluciones basadas en software libre, como NethServer, promueve la flexibilidad, la escalabilidad y la seguridad en la administración de servicios IT.

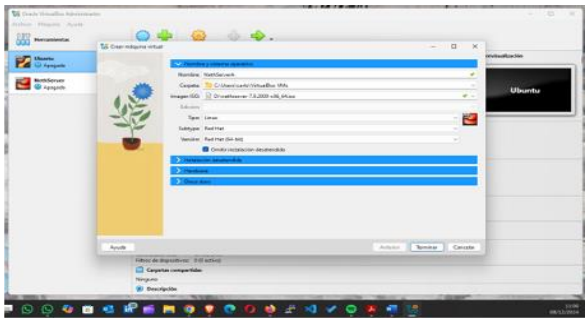
En el presente trabajo, NethServer se implementó en un entorno virtualizado mediante herramientas como VirtualBox, con el fin de explorar y aplicar configuraciones esenciales para la administración de redes y servicios de TI. Esta aproximación permitió simular escenarios prácticos en un entorno controlado, reproduciendo condiciones similares a las que podrían presentarse en contextos reales. Así, se examinaron aspectos claves de la gestión de la infraestructura, destacando la importancia de la eficiencia, la seguridad y la capacidad de respuesta frente a las demandas cambiantes del entorno tecnológico.

Los resultados obtenidos evidencian la eficacia y versatilidad de la plataforma, así como la pertinencia de las soluciones de software libre en la mejora continua de la infraestructura de TI. Este documento describe los procedimientos realizados, las configuraciones aplicadas, los resultados alcanzados y su relevancia para la gestión de redes y servicios IT.

2 INSTALACION NETHSERVER

Para iniciar con la instalación de NethServer, se utilizó VirtualBox para crear una nueva máquina virtual en la cual se montó la ISO de NethServer. En esta etapa, se configuraron las propiedades del hardware, incluyendo la memoria RAM, las CPU asignadas y el espacio de almacenamiento correspondiente al disco duro.

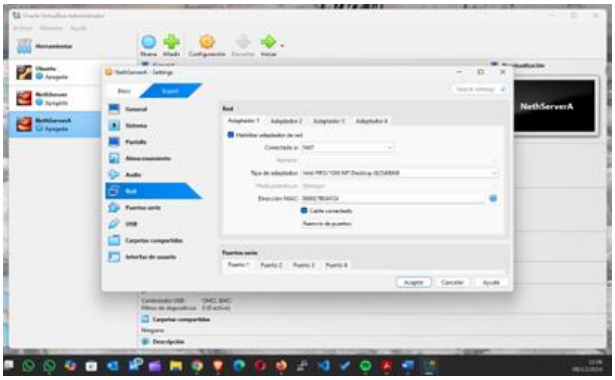
Figura 1. Creación de la máquina virtual



Fuente: Elaboración propia

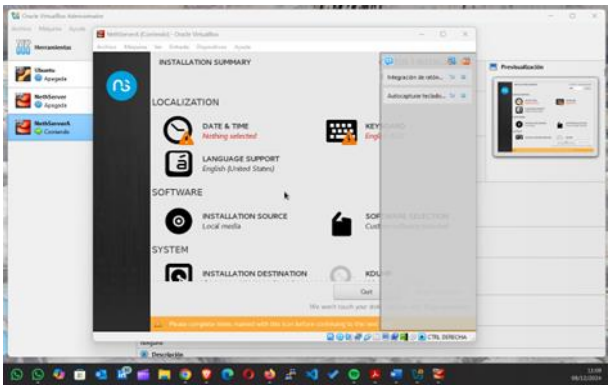
Una de las actividades más importantes a tener en cuenta durante la instalación de NethServer es la configuración de los adaptadores de red, ya que esta permite utilizar y trabajar con las direcciones IP asignadas por la red anfitriona.

Figura 2. Configuración de los adaptadores de red



Fuente: Elaboración propia

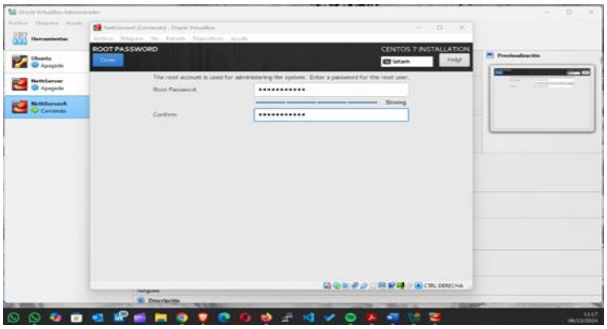
Figura 3. Configuración de la zona horaria y teclado



Fuente: Elaboración propia

En esta etapa, la configuración de la zona horaria, el teclado y la verificación previa de los adaptadores de red configurados resultan fundamentales. Es importante asegurarse de que todos estos elementos estén correctamente ajustados para garantizar el funcionamiento óptimo de NethServer.

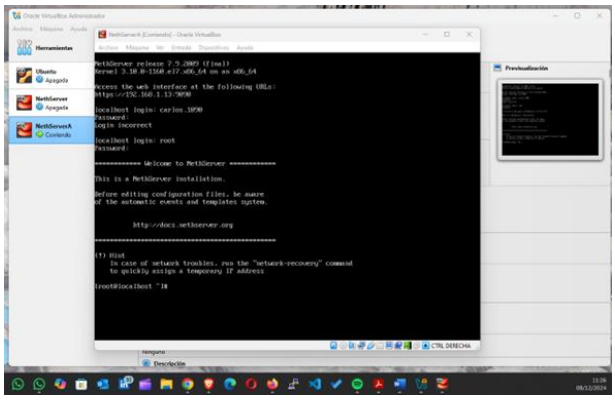
Figura 4. Creación de la Password



Fuente: Elaboración propia

Uno de los pasos importantes en la instalación de NethServer es la creación de una nueva contraseña para el usuario root, ya que esta será utilizada para acceder y gestionar la interfaz gráfica que se presenta posteriormente.

Figura 5. Login en NethServer



Fuente: Elaboración propia

En la imagen podemos ver la visa de bienvenida por consola de nuestro NethServer dónde ingresamos nuestro usuario root y la clave que creamos por medio de la interfaz.

que éste nos presentó, mostrará un mensaje de bienvenida y también una ip local con un puerto en donde se estará corriendo En NethServer, al utilizar la URL correspondiente dentro de la misma red local, es posible acceder a la aplicación de NethServer. Esto permite continuar con las temáticas, actividades y configuraciones necesarias, adaptándolas a los requerimientos de pequeñas y medianas empresas.

1 DESARROLLO DE LA PRÁCTICA

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

CONFIGURACIÓN DE DHCP, DNS Y CONTROLADOR DE DOMINIO EN NETHSERVER

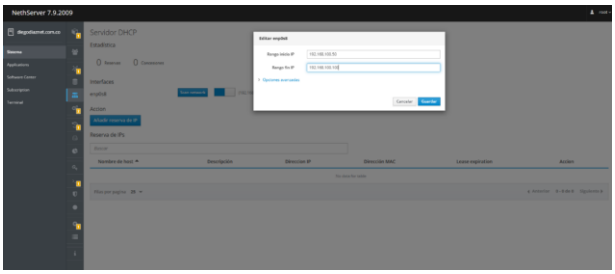
La gestión efectiva de una red empresarial se basa en varios servicios esenciales que facilitan la asignación de direcciones IP, la resolución de nombres de dominio y la administración centralizada de usuarios. NethServer, una plataforma robusta y fácil de usar, proporciona herramientas integradas para configurar y manejar servicios clave como DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System) y el Controlador de Dominio, que son vitales para el funcionamiento y la seguridad de la infraestructura de red. A continuación, se describe el proceso para configurar estos servicios en NethServer, resaltando la importancia de cada uno y su contribución a una gestión eficiente de la red.

CONFIGURACIÓN DEL SERVICIO DHCP EN NETHSERVER

El servicio DHCP es fundamental para la asignación automática de direcciones IP a los dispositivos que se conectan a una red. Este protocolo minimiza la necesidad de intervención manual al asignar dinámicamente las direcciones, lo que ayuda a evitar conflictos y simplifica la gestión de la red, especialmente en entornos donde los dispositivos se conectan y desconectan con frecuencia.

Para configurar el servicio DHCP en NethServer, primero se debe acceder a la interfaz de administración web, navegar hasta el menú Red y seleccionar la opción DHCP, donde se activa el servicio marcando la opción de habilitar. A continuación, es necesario definir el rango de direcciones IP que se asignan a los dispositivos de la red, especificando las direcciones inicial y final dentro de la subred para evitar conflictos, para este caso en concreto se asigna el rango 192.168.100.50 - 192.168.100.100 como se observa en la figura 6. Además, NethServer permite configurar parámetros adicionales como la puerta de enlace (gateway) y los servidores DNS que los dispositivos utilizarán, lo que garantiza un acceso correcto a los recursos externos sin interferencias.

Figura 6. Configuración del servicio DHCP



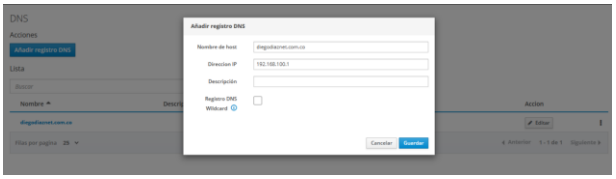
Fuente: Elaboración propia

CONFIGURACIÓN DEL SERVICIO DNS EN NETHSERVER

El servicio DNS es responsable de traducir los nombres de dominio a direcciones IP, lo que facilita la comunicación entre los dispositivos de la red. Sin un servidor DNS, los usuarios tendrían que recordar las direcciones IP de cada servidor o servicio al que deseen acceder. NethServer ofrece un servidor DNS integrado que puede configurarse fácilmente.

Para configurar el servicio DNS en NethServer, se debe acceder al menú Red desde la interfaz de administración y seleccionar la opción DNS, donde se activa el servicio y se configuran las zonas y registros necesarios. En la configuración de DNS, se pueden definir las zonas para los dominios internos de la red, creando registros A para asociar nombres de host con direcciones IP. Una correcta configuración de estas zonas y registros es fundamental para asegurar la adecuada resolución de nombres dentro de la red. En la figura 7 se observa cómo se configuran entonces para la IP del servidor 192.168.100.1 el nombre de dominio diegodiaznet.com.co

Figura 7. Configuración del servicio DNS



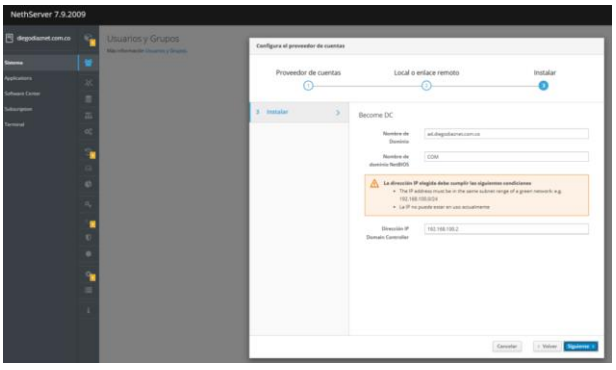
Fuente: Elaboración propia

CONFIGURACIÓN DEL CONTROLADOR DE DOMINIO EN NETHSERVER

El Controlador de Dominio es fundamental en una red empresarial, ya que permite la gestión centralizada de usuarios y dispositivos, así como el establecimiento de políticas de seguridad y acceso. En NethServer, el controlador de dominio se implementa utilizando Samba AD, que ofrece compatibilidad con protocolos de red Linux para nuestro caso, permitiendo la integración con estaciones de trabajo y otros sistemas.

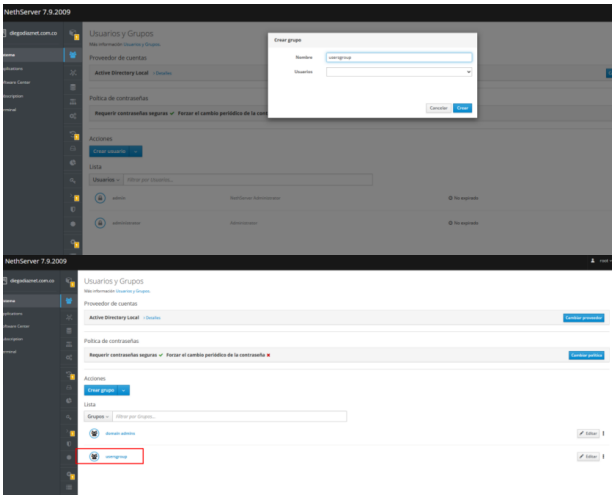
Para tener un controlador de dominio NethServer, se debe ir a aplicaciones en la interfaz de administración y elegir AD. Aquí se activa el servicio Controlador de Dominio, transformando este servidor en un punto que concentrará la autenticación y gestión de usuarios en la red. Posteriormente, debe definirse un nombre de dominio que sea único y coherente con la infraestructura empresarial (en las figuras 8 y 9 vemos cómo para este caso será ad.diegodiaznet.com.co), así como su servidor DNS que debe apuntar a sí mismo NethServer para correcta resolución de nombres dentro del dominio. Una vez configurado el controlador de dominio, se logrará incorporar los dispositivos cliente en la red mediante las credenciales de dominio, garantizando así una centralización en la administración de n permisos de acceso y posibilitando la aplicación de políticas de seguridad de forma homogénea sobre todos los dispositivos que comparten la red.

Figura 8. Configuración del servicio AD



Fuente: Elaboración propia

Figura 9. Configuración de Usuarios y Grupos



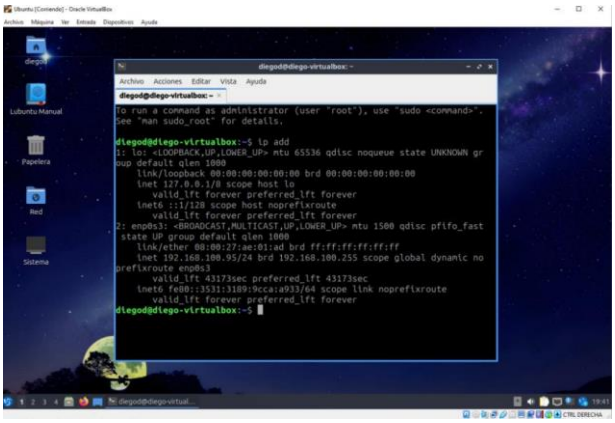
Fuente: Elaboración propia

VERIFICACIÓN Y PRUEBAS

Luego de tener configurados los servicios DHCP, DNS y Controlador de Dominio en NethServer, se procede a realizar pruebas para asegurarse de que todo esté funcionando correctamente.

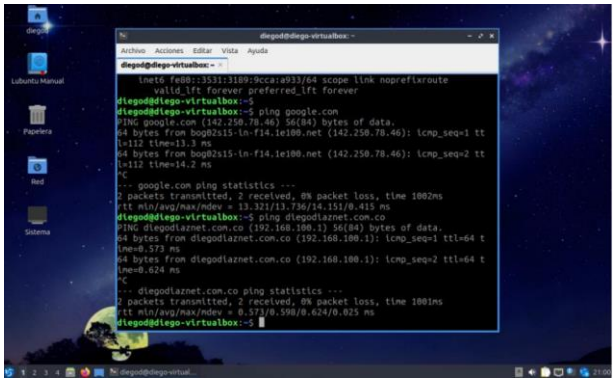
Para verificar el funcionamiento del servicio DHCP, se conecta un equipo a la red y se verifica que recibe una dirección IP dentro del rango configurado (192.168.100.50 – 192.168.100.100). Para el DNS basta con hacer ping al dominio configurado para el servidor diegodiaznet.com.co y al responder se comprueba que está correctamente configurado como se observa en la figura 10 y 11.

Figura 10. Validación del servicio DHCP operativo



Fuente: Elaboración propia

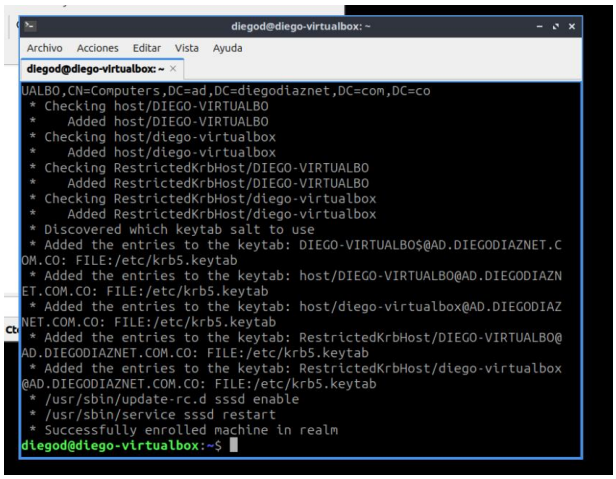
Figura 11. Configuración del servicio DHCP



Fuente: Elaboración propia

Para confirmar que el controlador de dominio está funcionando adecuadamente, se inicia sesión en el equipo cliente con las credenciales del dominio. Al ser el inicio de sesión exitoso como se observa en la figura 12, significa que el servidor está autenticando correctamente a los usuarios.

Figura 12. Validación del Inicio de usuario en el AD



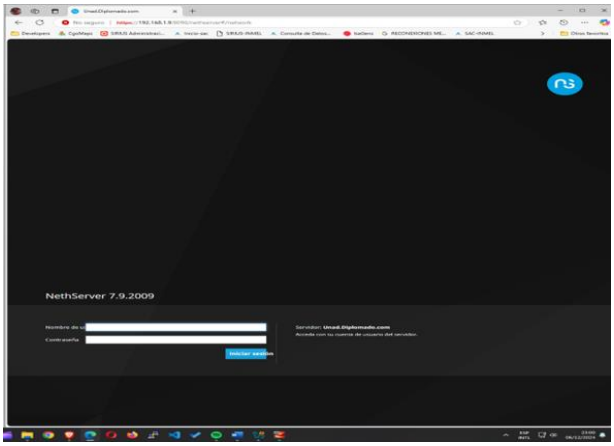
Fuente: Elaboración propia

3.2 PROXY

La configuración de un proxy en una empresa es esencial para controlar el acceso a internet, mejorando la seguridad mediante el filtrado de sitios no autorizados y el monitoreo del tráfico de red [3]. Además, la implementación de almacenamiento en caché optimiza el rendimiento, ya que reduce el uso de ancho de banda y acelera las solicitudes frecuentes [4]. La función de un proxy también protege la privacidad de los usuarios al ocultar sus direcciones IP y facilita el acceso a contenido restringido por ubicación, a la vez que permite equilibrar el tráfico entre servidores, garantizando la estabilidad de las aplicaciones empresariales [5]. En suma, un

proxy contribuye a elevar la seguridad, el rendimiento y la eficiencia en la gestión del tráfico de una red corporativa [6].

Figura 13. Ingreso a la plataforma NethServer



Fuente: Elaboración propia

En la imagen véase **figura 13** podemos observar la interfaz gráfica que el servidor ofrece para su acceso. La configuración de la red es esencial para garantizar el correcto funcionamiento de la infraestructura y cumplir con los objetivos planteados en la actividad [7]. En este caso, se accedió a un entorno que permite visualizar las diferentes redes disponibles, lo cual facilita la identificación y ajuste de parámetros críticos. A partir de esta vista, se procedió a configurar las direcciones IP y a adaptar las características de las redes según los requisitos específicos del escenario de trabajo.

En este contexto, se incluyeron configuraciones particulares para la red LAN, la red WAN y, de forma opcional, una red DMZ, asegurando así un enrutamiento y segmentación adecuados del tráfico interno y externo. Se asignaron las IP necesarias y se definió el comportamiento de las redes de acuerdo con las necesidades establecidas para la actividad, garantizando un desempeño óptimo de los servicios y una comunicación fluida entre los diferentes segmentos. Estas acciones contribuyen a una arquitectura de red más robusta, segura y eficiente, alineada con las mejores prácticas en el ámbito de la administración de redes.

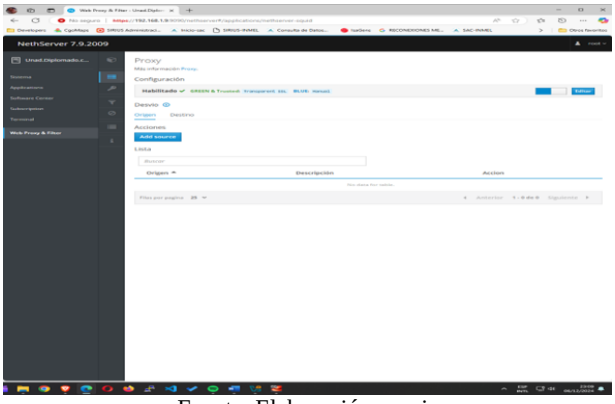
Figura 14. Configuración de las redes en NethServer

Fuente: Elaboración propia

La configuración de la red es esencial para garantizar el correcto funcionamiento de la infraestructura y cumplir con los objetivos establecidos en la actividad. Como se puede visualizar en la **Figura 14** las redes que vamos a utilizar son presentadas para su configuración. En este caso, se accedió a un entorno que permite visualizar las diferentes redes disponibles, lo que facilita la identificación de los segmentos y la preparación para ajustes específicos [1]. A partir de esta vista, se procedió a configurar las direcciones IP, así como a adaptar las características de las redes LAN, WAN y, en caso necesario, una DMZ, de acuerdo con las necesidades planteadas.

Estas acciones resultan fundamentales para asegurar un enrutamiento interno y externo eficaz, así como para establecer comunicaciones estables y seguras entre los distintos componentes de la infraestructura. La asignación de direcciones IP adecuadas y la definición del comportamiento de cada red permiten optimizar el rendimiento, la disponibilidad y la seguridad del entorno. En última instancia, la correcta configuración de la red contribuye a crear una arquitectura sólida y confiable, alineada con las prácticas recomendadas para la administración de sistemas y servicios IT.

Figura 15. Configuración e instalación de aplicaciones

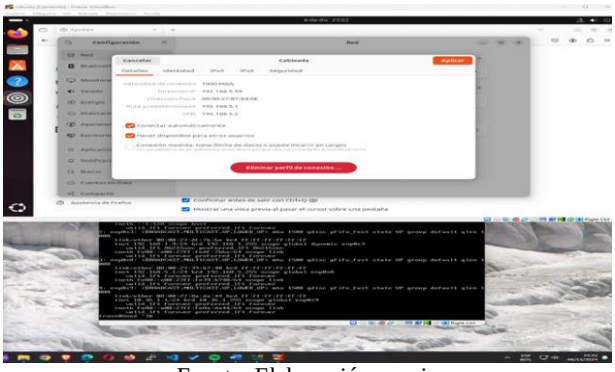


Fuente: Elaboración propia

Después de configurar las redes, el siguiente paso fue establecer el DNS y el servidor DHCP, como se observa en la **Figura 15** donde podemos acceder a los elementos críticos para la asignación dinámica de direcciones IP y la resolución de nombres en el entorno. En el servidor DHCP se definió un rango de direcciones IP acorde a la configuración previa, permitiendo que los dispositivos conectados obtuvieron automáticamente los datos de red necesarios. Estas tareas contribuyen a asegurar la disponibilidad y usabilidad de los servicios en la infraestructura, alineándose con las prácticas recomendadas en la administración de redes [14].

Además, fue necesario instalar y configurar dos aplicaciones web relacionadas con el proxy, conocidas como Web Proxy y Web Filter. A través de la plataforma de gestión, se creó un acceso directo en el menú de NethServer para simplificar su administración, brindando un control centralizado sobre el filtrado y la regulación del tráfico web. Posteriormente, se procedió a la configuración del proxy, incluyendo la creación de listas negras y listas blancas, así como la aplicación de filtros específicos destinados a restringir el acceso a ciertos sitios web según las políticas definidas en la actividad. Estas acciones complementan la arquitectura de seguridad y eficiencia en la infraestructura de TI, respaldadas por el uso de herramientas virtualizadas y entornos controlados.

Figura 16. Configuración de Proxy en los usuarios

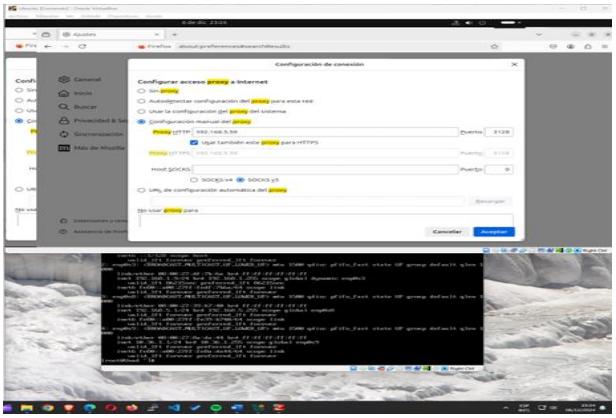


Fuente: Elaboración propia

Después de configurar los filtros y todos los elementos necesarios del proxy, el paso siguiente fue verificar la conectividad de uno de los dispositivos cliente, como se observa en la **figura 16** se tiene que utilizarían el acceso a internet a través del proxy. Para ello, se comprobó que el dispositivo estuviera correctamente conectado a la red y que el servidor DHCP estuviera asignando una dirección IP dentro del rango definido. Esta comprobación es fundamental, ya que garantiza que las configuraciones realizadas, tanto en la infraestructura de red como en el servidor proxy, están operando de manera adecuada [1].

Como se evidencia en las pruebas realizadas, el dispositivo obtuvo exitosamente una dirección IP del servidor DHCP, confirmando que la funcionalidad de asignación dinámica de direcciones, así como el enrutamiento y filtrado de tráfico, se ejecutan conforme a lo planificado. Este resultado verifica la solidez del entorno y respalda las decisiones adoptadas en el proceso de configuración, asegurando la prestación de servicios eficientes y confiables.

Figura 17. Configuración del proxy en Ubuntu.

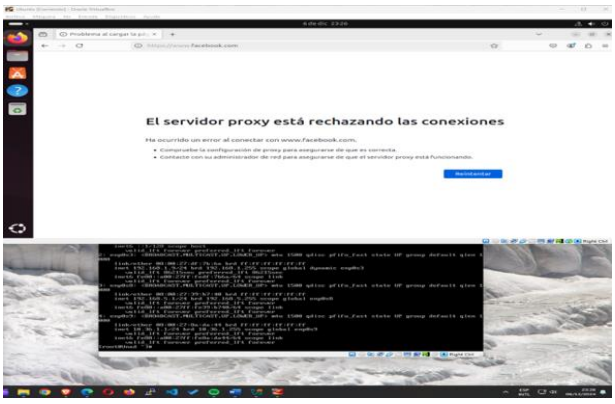


Fuente: Elaboración propia

En este paso, se configuró el proxy asignándole la dirección IP correspondiente y el puerto 3128 como se observa en la **figura 17**, previamente definidos en NethServer [1]. Tras activar su uso, se realizaron pruebas de acceso a diversas páginas y sitios web incluidos en la lista negra, con el fin de verificar que dichas restricciones fueran efectivas y que los usuarios conectados a través del proxy no pudieran acceder a contenido no autorizado.

Estas configuraciones, aplicadas al navegador en Ubuntu, permiten bloquear el acceso a aplicaciones o sitios web restringidos y garantizar el cumplimiento de las políticas de acceso establecidas. De esta forma, los dispositivos conectados a través del proxy operan bajo los lineamientos de seguridad y control definidos en la infraestructura de la red.

Figura 18. Prueba del funcionamiento del Proxy



Fuente: Elaboración propia

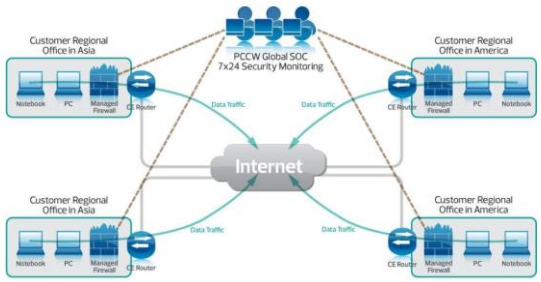
En la **figura 18 lo** siguiente es confirmar que el proxy está rechazando las conexiones hacia los sitios y páginas web incluidas en la lista negra, lo que respalda la eficacia de la configuración realizada. Este resultado demuestra que las medidas implementadas cumplen con los criterios establecidos para restringir el acceso a contenido no autorizado, garantizando así el cumplimiento de las políticas de seguridad y control definidas [4], [6].

3.3 TEMÁTICA 3 – CORTAFUEGOS

Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Un cortafuegos o firewall, es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados y la necesidad de interconexión de redes.

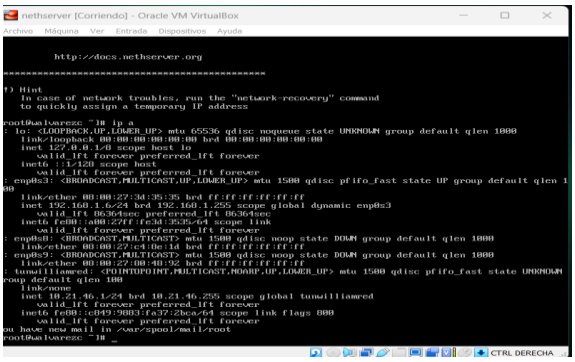
Figura 19. Esquema general de un cortafuegos



Los cortafuegos son la primera medida de seguridad que empezó a implementarse tras el nacimiento de Internet en la década de los 80, con el fin de combatir a los primeros hackers. La finalidad de los cortafuegos es la de establecer criterios de seguridad, y filtrar todas las comunicaciones que entran o salen del ordenador.

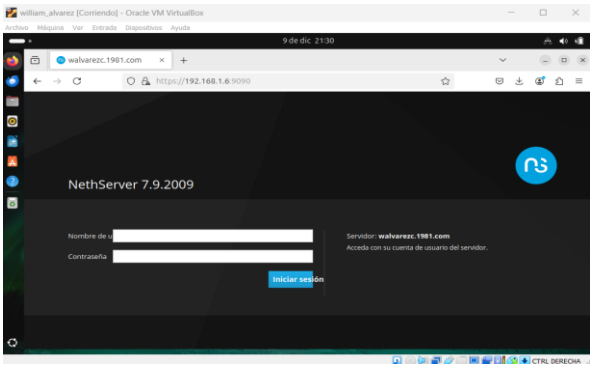
Una vez que las máquinas virtuales (NethServer y el Cliente o Desktop) estén en funcionamiento, en el Cliente abrimos el navegador Mozilla y escribimos la URL con la IP de la máquina virtual NethServer, que obtenemos al ejecutar el comando ip a en la terminal de NethServer. Esto nos permitirá acceder a la aplicación y realizar la autenticación utilizando el usuario y la contraseña correspondientes.

Figura 20. Línea de comando (ip a) en terminal de NethServer y acceso a máquina virtual de Desktop Ubuntu



Fuente: Elaboración propia

Figura 21 Inicio web del Nethserver

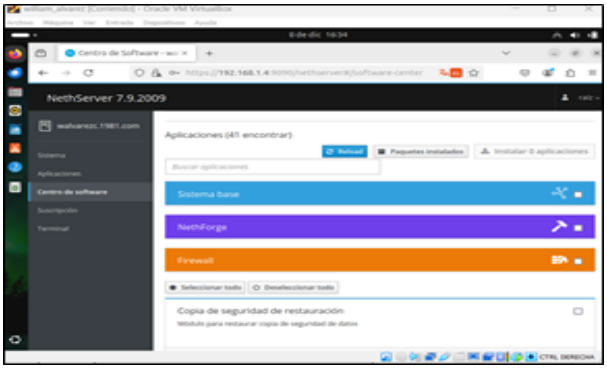


Fuente: Elaboración propia

INSTALACIÓN Y CONFIGURACIÓN

Como primera medida, accedemos al módulo Centro de Software en NethServer. Allí, activamos la casilla de Firewall - Firewall básico y procedemos con el proceso de instalación. Una vez finalizada la instalación, verificamos que la aplicación se haya instalado correctamente marcando la casilla de Aplicaciones, donde podemos confirmar que la instalación del Firewall básico se haya realizado de manera exitosa.

Figura 22. Instalación y activación de Firewall

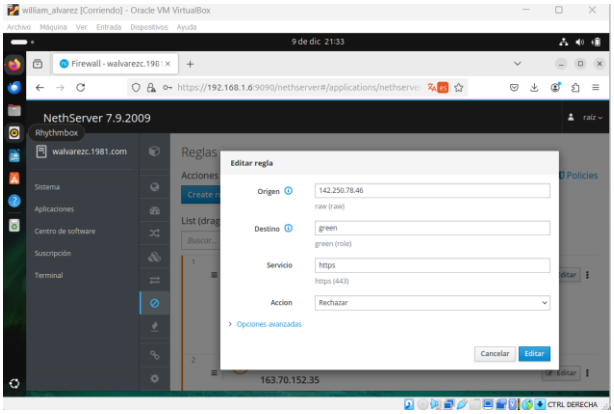


Fuente: Elaboración propia

En la casilla de Aplicaciones, seleccionamos Firewall y hacemos clic en Ajustes. En esta sección, procedemos a crear las reglas necesarias para restringir el acceso a las direcciones IP que deseamos limitar. Esto se realiza agregando las IP`s en las configuraciones de las reglas de firewall, especificando las

direcciones o rangos de IP que queremos permitir o bloquear según sea necesario.

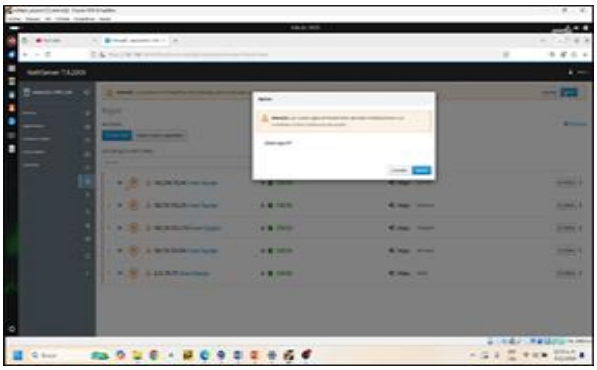
Figura 23. Configuración de las reglas



Fuente: Elaboración propia

Después de insertar cada parámetro de restricción, como las direcciones IP que deseamos bloquear o permitir, debemos hacer clic en aplicar para que cada cambio o regla que hemos configurado se guarde y se active correctamente en el firewall. Esto garantiza que las restricciones de acceso se implementen de acuerdo con lo que hemos especificado en cada parámetro.

Figura 23. Esquema final de las reglas de nuestro cortafuegos



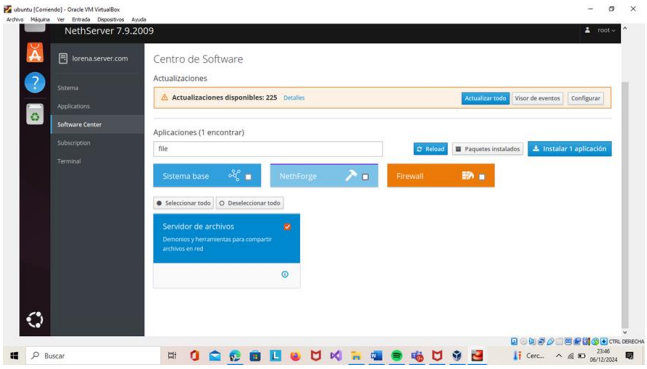
Fuente: Elaboración propia

3.4 FILE SERVER Y PRINT SERVER

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras [6]

Comienzan instalando los servicios de FILE SERVER y PRINT SERVER.

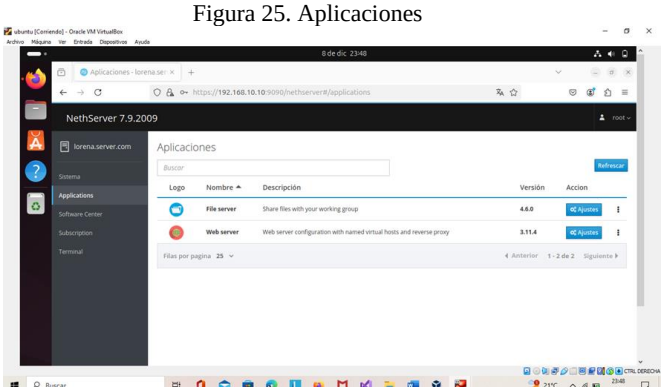
Figura 24. Instalación de servicios



Fuente: Elaboración propia

Una vez instalada, se dirigen al módulo de Aplicaciones donde encontrarán las aplicaciones descargadas.

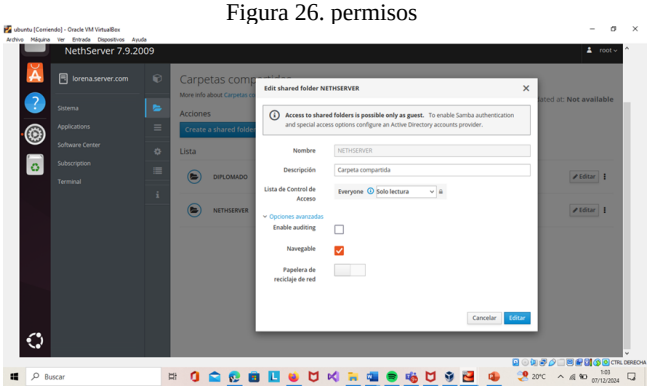
Figura 25. Aplicaciones



Fuente: Elaboración propia

En la aplicación de file server, se dirigen a los ajustes y crean una carpeta compartida. Se asigna un nombre y una ruta para la carpeta, y se configuran los permisos de acceso según sea necesario como se muestra en la figura 26.

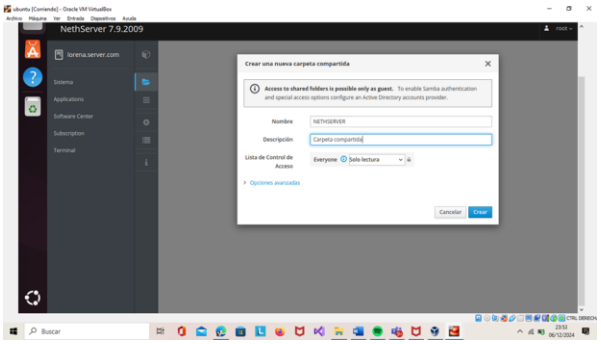
Figura 26. permisos



Fuente: Elaboración propia

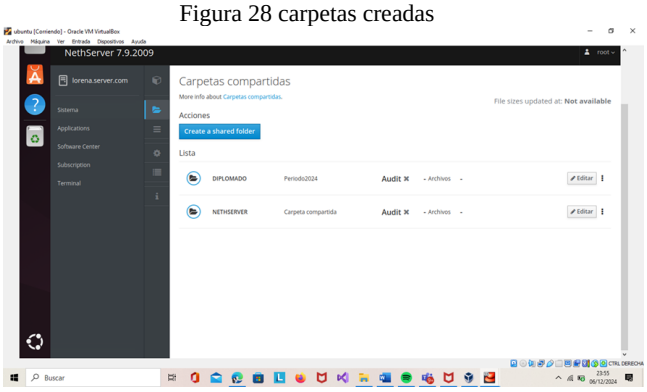
Se crean dos carpetas, una de solo lectura y una de lectura y escritura.

Figura 27 carpeta solo lectura



Fuente: Elaboración propia

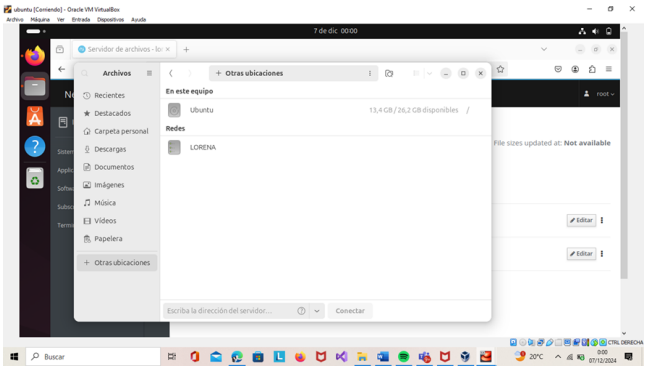
Figura 28 carpetas creadas



Fuente: Elaboración propia

Ingresan desde el cliente Ubuntu al servidor de archivos, apartado de otras ubicaciones verán una ventana donde deben ingresar la dirección IP del servidor de archivos.

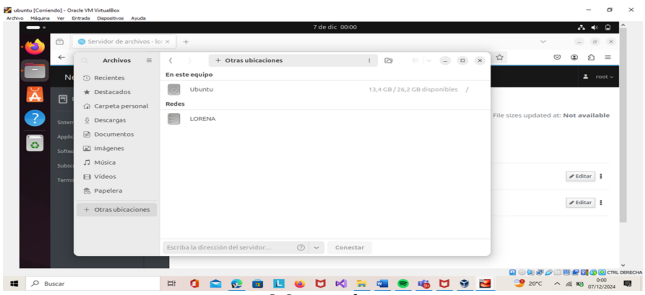
Figura 29. acceso al Servidor de Archivos - Otras Ubicaciones



Fuente: Elaboración propia

Se dirigen a otras ubicaciones y encuentran "LORENA", el servidor. Hacen clic para ingresar.

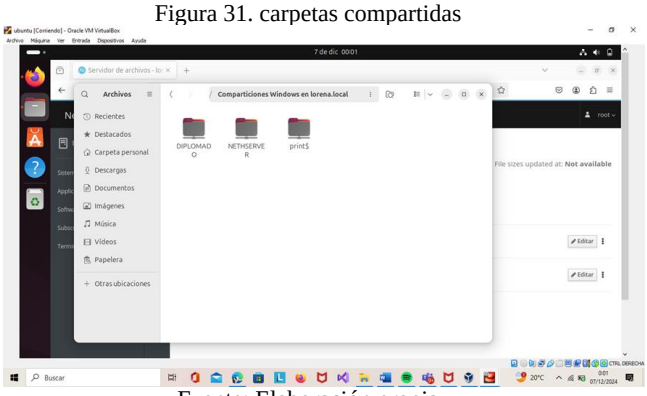
Figura 30. Acceso al Servidor LORENA



Fuente: Elaboración propia

Aquí pueden ver las carpetas compartidas y la carpeta del servidor de impresión. Hacen clic para acceder.

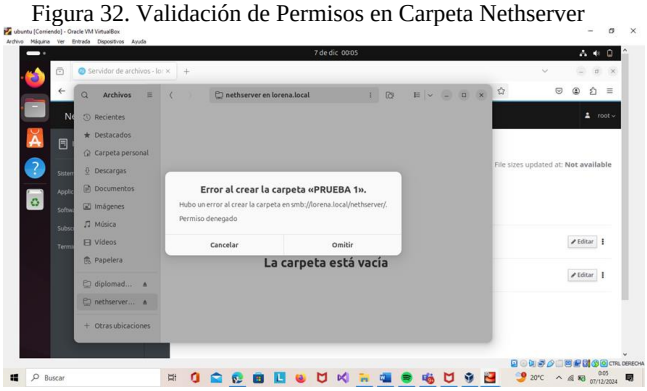
Figura 31. carpetas compartidas



Fuente: Elaboración propia

Recuerdan que la carpeta NETHSERVER es de solo lectura, mientras que la carpeta "Diplomado" permite tanto lectura como escritura. Crean una nueva carpeta dentro de "Nethserver" para verificar que los permisos de solo lectura están funcionando correctamente

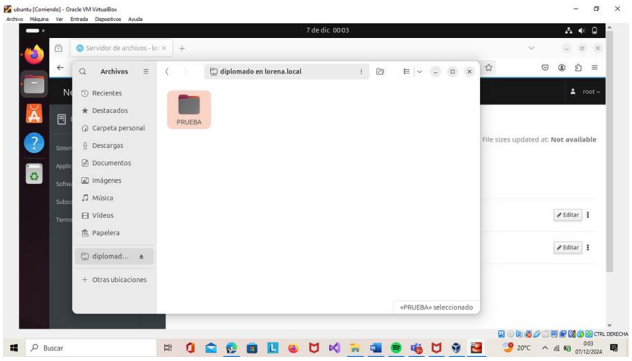
Figura 32. Validación de Permisos en Carpeta Nethserver



Fuente: Elaboración propia

Dentro de la carpeta compartida "Diplomado", crean una nueva carpeta para validar los permisos de lectura y escritura. Este paso confirma que tienen acceso adecuado para añadir y modificar contenido en dicha carpeta.

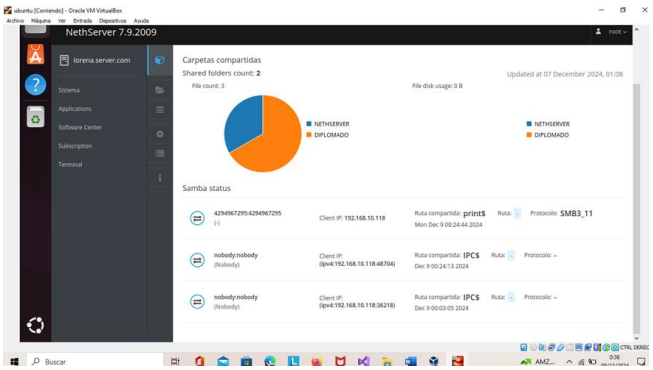
Figura 33. Acceso a Carpeta Compartida Diplomado



Fuente: Elaboración propia

En la sección del servidor de archivos, se pueden revisar las interacciones realizadas, verificando los movimientos efectuados en las diferentes carpetas.

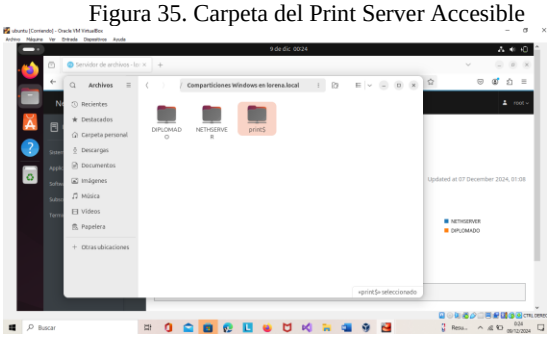
Figura 34. Verificación de Acciones en Carpetas Compartidas



Fuente: Elaboración propia

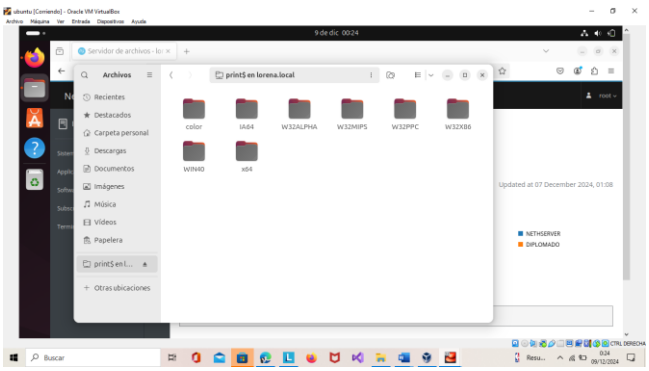
Como pueden observar, ya es posible visualizar la carpeta correspondiente al servidor de impresión. Esto indica que la conexión se ha establecido correctamente y que la carpeta está accesible para su uso.

Figura 35. Carpeta del Print Server Accesible



Fuente: Elaboración propia

Figura 36. Servicios de Impresión Activos



Fuente: Elaboración propia

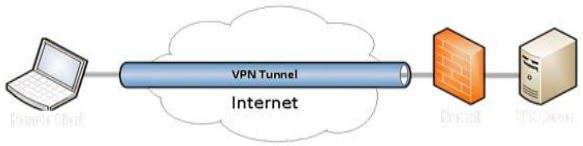
3.5 VPN

Una VPN, o red privada virtual, establece una conexión segura y privada para transmitir datos a través de redes públicas, como Internet. Su principal objetivo es proteger la privacidad del usuario, ocultando su dirección IP y cifrando los datos para evitar que sean interceptados por terceros no autorizados de privacidad, anonimato y seguridad.Una VPN permite dirigir los paquetes de datos de su máquina a otro servidor remoto antes de enviarlos a terceros a por medio del protocolo de túnel.

El servicio de VPN actúa como un filtro, lo que hace que sus datos sean ilegibles en un extremo y solo los decodifica en el otro.

En resumen, una VPN es una herramienta fundamental para quienes desean mantener su privacidad en línea y proteger sus datos mientras navegan por la web o acceden a servicios en línea.

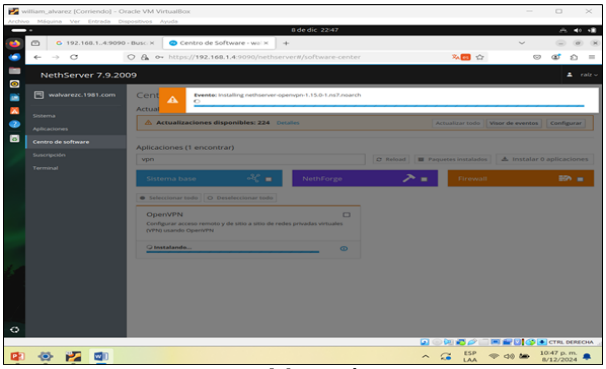
Figura 37 . Esquema gráfico de una VPN



INSTALACIÓN Y CONFIGURACIÓN

Una vez que las máquinas virtuales estén iniciadas e interconectadas, abrimos el navegador e ingresamos a la IP proporcionada por NethServer. Luego, seleccionamos la opción llamada "Centro de Software", la cual nos mostrará una barra de búsqueda. En esta barra, debemos escribir "VPN" para que el buscador localice la aplicación relacionada con la configuración (OpenVPN)

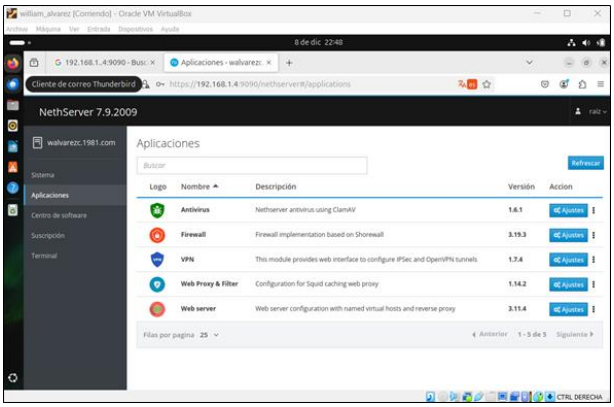
Figura 38. Instalación OpenVPN



Fuente: Elaboración propia

Ya instalada la VPN, dirígete a la pestaña de aplicaciones, donde encontrarás la confirmación de la instalación. Luego, selecciona la opción de 'Ajustes'.

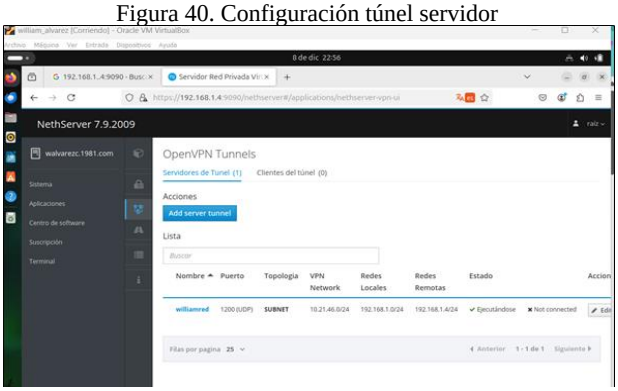
Figura 39. Verificación de la instalación de la VPN



Fuente: Elaboración propia

Debes seleccionar la pestaña 'OVPN Tunnels'. En este punto, es necesario crear el túnel entre el servidor y el cliente.

Figura 40. Configuración túnel servidor



Fuente: Elaboración propia

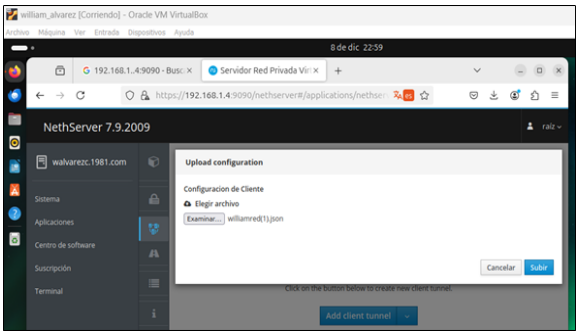
Para crear el túnel del cliente, es necesario descargar el archivo JSON, el cual deberá ser agregado posteriormente con los parámetros correspondientes a la configuración requerida.

Figura 41. Configuración túnel cliente

Fuente: Elaboración propia

En este proceso de creación de una VPN mediante un túnel de comunicación, como se observa en la imagen, el usuario accede a la interfaz del NetServer 7.9.2009 a través de una URL interna.

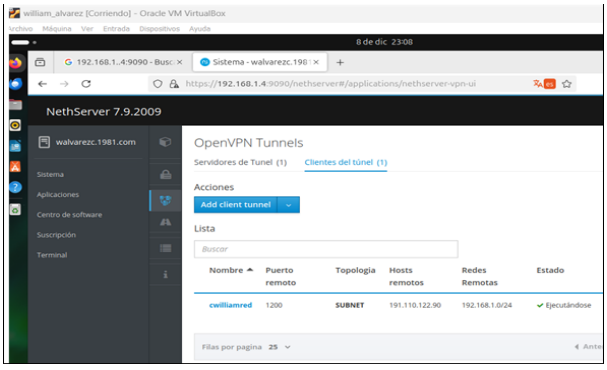
Figura 42. Anexo archivo. json



Fuente: Elaboración propia

Ahora se puede observar la creación del túnel, junto con los dos usuarios en ejecución.

Figura 43. Ejecución del túnel



Fuente: Elaboración propia

En la imagen podemos observar el túnel creado y activado para el uso, atreves de la red local, donde los usuarios que utilicen la vpn pueden acceder a los servicios configurados.

CONCLUSIONES

La configuración adecuada de DHCP, DNS y servicios de controlador de dominio en NethServer le permite administrar de manera eficiente y centralizada su infraestructura de red. Estos servicios son fundamentales para garantizar el funcionamiento adecuado de las redes empresariales al facilitar la asignación de direcciones IP, la resolución de nombres de dominio y la gestión de usuarios. Al implementar y configurar adecuadamente estos servicios, se puede optimizar el rendimiento de la red y aumentar la seguridad y el control sobre los recursos y dispositivos conectados.

La implementación de un servidor proxy con NethServer no solo se traduce en mayor control sobre el tráfico de la red, sino que también brinda un sentido de seguridad y confianza a las personas que confían en ese entorno digital. Al restringir el acceso a sitios peligrosos o inapropiados, protegemos a usuarios que, sin darse cuenta, podrían exponerse a riesgos.

Dentro de las amplias utilidades que ofrece NethServer, uno de los componentes clave es el cortafuegos o firewall. Este sistema de seguridad tiene como objetivo controlar el tráfico entre redes o servidores, estableciendo reglas para restringir el acceso según los parámetros definidos por el usuario. Las reglas de firewall pueden basarse en diversos criterios, como direcciones IP, puertos, protocolos y otras configuraciones de red.

El firewall de NethServer permite al usuario root (administrador) establecer políticas de seguridad detalladas, limitando el tráfico entrante y saliente para proteger los recursos del servidor. Al configurar estos cortafuegos, se puede permitir o bloquear el acceso a servicios específicos, mejorando así la seguridad de la infraestructura de red. Las reglas definidas en el firewall pueden ser aplicadas y modificadas en cualquier momento a través de la interfaz de administración de NethServer.

Implementar el FILE SERVER y el PRINT SERVER facilita la gestión eficiente de archivos y recursos de impresión en la red. Esto permite a los usuarios compartir, acceder y manejar archivos de forma segura y efectiva. Además, garantiza que los servicios de impresión estén siempre disponibles y operativos, lo que mejora significativamente la productividad y la colaboración en el entorno de trabajo.

La implementación de OpenVPN en NethServer demostró ser efectiva para proteger la privacidad de los usuarios al cifrar el tráfico en una red empresarial

1. REFERENCIAS

[1] NethServer. (s. f.). Documentación de NethServer. Recuperado el 6 de diciembre de 2024, de https://docs.nethserver.org/

[2] Oracle. (s.f.). Oracle VM VirtualBox User Manual. Recuperado de https://www.virtualbox.org/wiki/Documentation

[3] Cloudflare. (s.f.). *What is a Proxy Server?* Recuperado el 10 de octubre de 2024, de https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/

[4] Squid Cache. (s.f.). *Configuration Examples*. Recuperado el 10 de octubre de 2024, de https://wiki.squid-cache.org/ConfigExamples

[5] Apache Software Foundation. (s.f.). *Apache Traffic Server*. Recuperado el 10 de octubre de 2024, de https://trafficserver.apache.org/

[6] Francis, M. (2019). *Network Security: A Beginner's Guide*. Recuperado el 10 de octubre de 2024, de https://www.techrepublic.com/article/network-security-a-beginners-guide/

[7] Cisco. (s.f.). *Networking Basics*. Recuperado el 10 de octubre de 2024, de https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html

[8] Nethserver. (2022). Proxy web. [en línea] Disponible en: https://docs.nethserver.org/es/v7/web_proxy.html

[9] NethServer. (2024). File server. https://docs.nethserver.org/projects/ns8/en/latest/file_server.html