

# NetServer: “La Vanguardia en Soluciones de Redes para un Mundo Interconectado”

Jonathan David Duarte Guzman  
e-mail: jdduarteg@unavirtual.edu.co  
José Luis Ramos Bernal  
e-mail: jlramosbe@unavirtual.edu.co  
Sergio Andres Avila Moreno  
e-mail: saavilam@unad.edu.co

**RESUMEN:** *Este artículo expone la implementación integral de NetServer en áreas fundamentales de infraestructura de red, como DHCP Server, DNS Server, Controlador de Dominio, servicios proxy, Cortafuegos, File Server, Print Server y servicios de VPN. Se detalla el proceso de configuración de cada componente, resaltando su integración para mejorar la conectividad y la seguridad de la red. Los resultados revelan una optimización notable en la eficiencia operativa, permitiendo una gestión centralizada y la entrega ágil de servicios de red. Esta implementación demuestra la versatilidad de NetServer para ofrecer soluciones completas que potencian la conectividad, la administración de recursos y la protección de datos en entornos diversos. Este estudio destaca la relevancia estratégica de NetServer en el fortalecimiento y la evolución de la infraestructura de red contemporánea.*

**PALABRAS CLAVE:** Conectividad, Eficiencia, Gestión, Seguridad.

## 1 INTRODUCCIÓN

Este artículo detalla la implementación de NetServer en áreas clave de infraestructura de red: DHCP, DNS, Controlador de Dominio, servicios proxy, Cortafuegos, File Server, Print Server y VPN. Se enfoca en la configuración específica de cada componente y su integración con NetServer para mejorar la conectividad, seguridad y eficiencia operativa. Se examinan los resultados obtenidos en cada área, destacando el impacto de NetServer en la optimización de la infraestructura de red. Este análisis exhaustivo subraya la aplicabilidad práctica y la relevancia de NetServer en entornos de infraestructura de red contemporáneos.

## 2 OBJETIVOS

Investigar la implementación de NetServer en áreas cruciales de infraestructura de red, como DHCP, DNS, Controlador de Dominio, servicios proxy, Cortafuegos, File Server, Print Server y VPN. Se busca analizar en detalle cómo NetServer contribuye a optimizar la conectividad, seguridad y eficiencia operativa en cada una de estas áreas específicas, evaluando su capacidad para simplificar la administración, fortalecer la protección de datos y mejorar el acceso a los recursos de red.

Se pretende evaluar exhaustivamente la contribución de NetServer en cada componente mencionado, resaltando su aplicabilidad práctica y relevancia en entornos contemporáneos de infraestructura de red. El objetivo principal del artículo es proporcionar una visión completa y detallada de cómo NetServer potencia y mejora la funcionalidad y la gestión en estas áreas críticas de la infraestructura de red.

## 2.1 OBJETIVOS ESPECÍFICOS

- Implementar y configurar el acceso de una estación de trabajo GNU/Linux mediante usuario y contraseña, registrándola en los servicios de Infraestructura IT de Nethserver utilizando DHCP Server, DNS Server y el Controlador de Dominio.
- Configurar un proxy que filtre el acceso a Internet desde Nethserver para una estación GNU/Linux, direccionando el tráfico a través del puerto 3128.
- Definir y configurar restricciones específicas en el cortafuego de Nethserver desde una estación de trabajo GNU/Linux, limitando el acceso a sitios de entretenimiento y redes sociales.
- Implementar y configurar el acceso de una estación de trabajo GNU/Linux a los servicios de carpetas compartidas e impresoras mediante el controlador de dominio LDAP de NetServer.

## 3 MARCO TEÓRICO

NethServer es una distribución basada en Linux que está orientada específicamente a actuar como servidor en pequeñas y medianas oficinas [1]. Ofrece una gama de servicios y funciones que abarcan diferentes aspectos de la infraestructura de red, incluyendo los elementos mencionados en las temáticas.

- DHCP y DNS
- Controlador de Dominio
- Proxy
- Cortafuegos
- File y Print Server

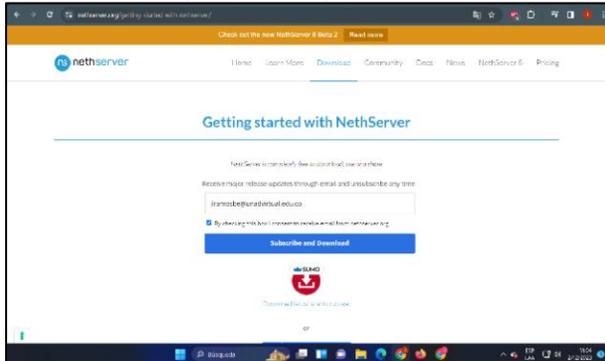
Estos elementos son fundamentales para asegurar una administración centralizada, eficiente y segura de la infraestructura de red.

## 4 INSTALACIÓN Y CONFIGURACION DE NETHSERVER

### 4.1 DESCARGA NETHSERVER

Una vez en el sitio oficial de NethServer, se inicia la descarga de la imagen ISO [2]. Una vez descargada, se procede a cargar esta ISO en la máquina destinada para la instalación, dando paso a las configuraciones requeridas para la instalación del sistema operativo.

Figura 1. Descarga nethserver

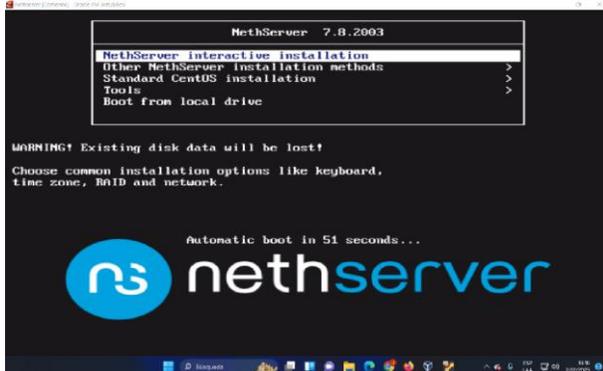


Fuente. Autoría Propia

### 4.2 CONFIGURACION NETHSERVER

Se llevará a cabo la creación de una nueva máquina virtual en VirtualBox para NethServer. Se procederá cargando la ISO descargada previamente y asignándole 2GB de RAM y 2 CPUs. Además, se configurará el espacio en disco con el valor por defecto de 20 GB. Posteriormente, se ajustarán los adaptadores 1, 2 y 3 de la máquina virtual de NethServer para su configuración óptima.

Figura 2. Consola nethserver



Fuente. Autoría Propia

### 4.3 CONFIGURACION NETHSERVER

Luego de optar por la instalación interactiva, se procederá con la configuración de la zona horaria y el idioma del teclado. Acto seguido, se realizará la configuración del Panel de Configuración Inicial de NethServer. Posteriormente, se iniciará la instalación seleccionando "Begin Installation". Durante este proceso, se accederá a la opción "ROOT PASSWORD" para establecer la contraseña del usuario root del sistema operativo.

Figura 3. Configuración zona horaria

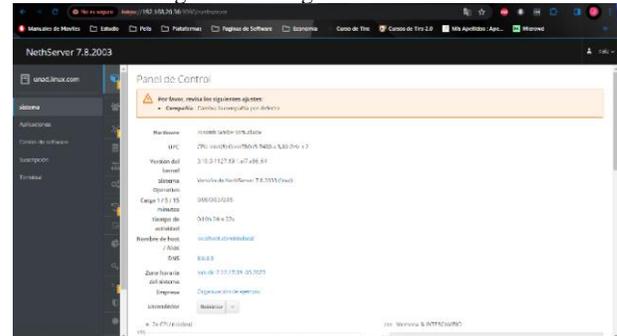


Fuente. Autoría Propia

### 4.4 PANEL DE CONTROL NETSERVER

Después de finalizar la instalación, se configurará la contraseña del usuario root en NethServer y se procederá a iniciar sesión con dicho usuario. Posteriormente, se realizará la actualización del sistema operativo mediante el comando "yum -y update" y se reiniciará el servidor. Una vez actualizado, se accede a la consola de administración de NethServer utilizando las credenciales previamente configuradas para root. Al ingresar, se solicitará la configuración de un dominio, optando por "unad.linux.com", permitiendo el acceso al panel de control.

Figura 4. Configuración realizada



Fuente. Autoría Propia

## 5 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

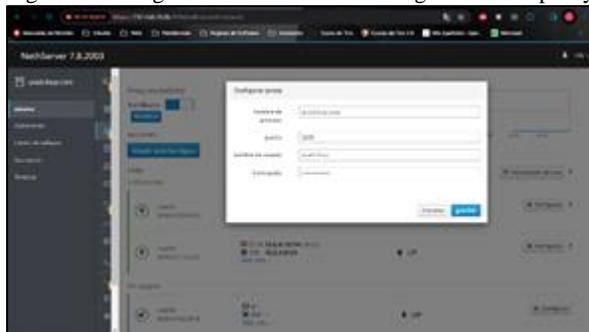
Se evidencia la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Nethserver.

Para este ejercicio debemos descargar primero la versión de Nethserver 7.8 o 7.9 para poder usar la interfaz de esta herramienta e implementar la configuración a través de la interfaz gráfica e implementar los servicios de DHCP, DNS y Domain Controller de acuerdo a las mismas configuraciones descritas al inicio, Como se menciona en [2].

### 5.1 CONFIGURACION INICIAL DE NETHSERVER

Al ingresar a los servicios web de nethserver, se realizan las configuraciones básicas de registro de información como nombre empresa, dirección teléfono y se configura el proxy.

Figura 5. Configuraciones básicas de configuración del proxy



Fuente. Autoría Propia

### 5.2 CONFIGURACIÓN DE ZONAS DE RED

Se procede a configurar la red WAN por DHCP (rojo). Esta red es la que otorga el servicio de internet. Para esto se ingresa a la opción red >> Añadir interfaz lógica

Figura 6. Configuración inicial de la WAN



Fuente. Autoría Propia

Al realizar la configuración de la red WAN esta se configura con la interfaz de puente y se selecciona la tercera tarjeta de red, Después se configura el protocolo IP al cual se dejará como Servidor DHCP ya que esta será la salida a internet.

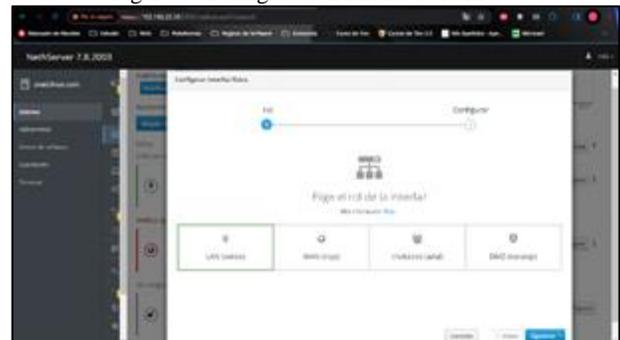
Figura 7. Configuración protocolo de la WAN



Fuente. Autoría Propia

Ahora configuraremos la red LAN en modo estático (verde). Esta red es la que permite la conexión interna.

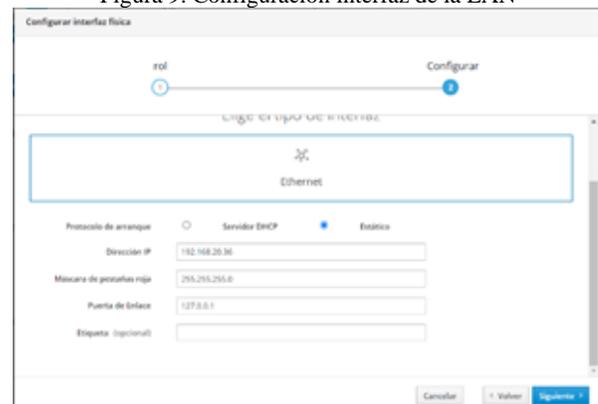
Figura 8. Configuración inicial de la LAN



Fuente. Autoría Propia

Después se configura el tipo de interfaz con una ip estática.

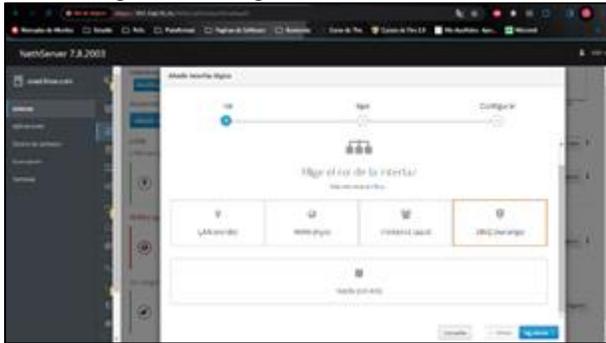
Figura 9. Configuración interfaz de la LAN



Fuente. Autoría Propia

Por último, se configura la DMZ en modo estático (naranja).

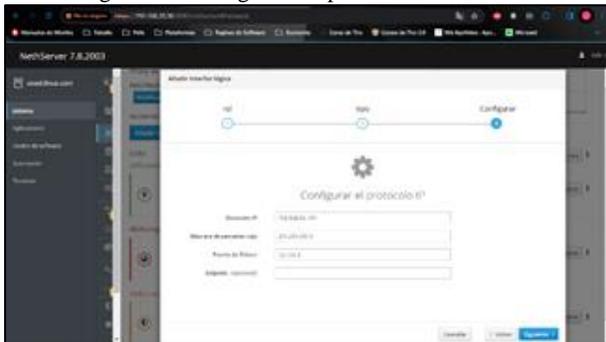
Figura 10. Configuración inicial de la DMZ



Fuente. Autoría Propia

Ahora se configura la interfaz como vínculo y se selecciona la tarjeta de red del adaptador 2 y se le da click en siguiente, por último, se configura el protocolo IP al cual se dejará con la ip estática del Ubuntu desktop.

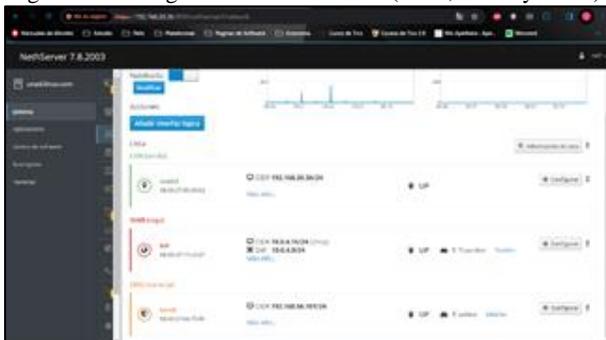
Figura 11. Configuración protocolo de la DMZ



Fuente. Autoría Propia

Ahora las 3 redes están configuradas y listas para aplicar las configuraciones.

Figura 12. Configuración de las 3 redes (LAN, WAN y DMZ)

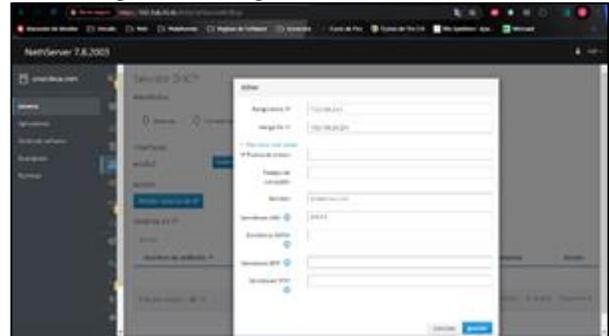


Fuente. Autoría Propia

## 5.2 CONFIGURACIÓN DEL DNS Y DHCP SERVER

Una vez se configuran las redes del punto anterior se procede a configurar el servidor DHCP, esto se hace desde la opción Servidor DHCP, se habilita la interfaz y realizaremos las configuraciones de rango de ip, dominio y DNS, guiándonos por las configuraciones descritas en [6].

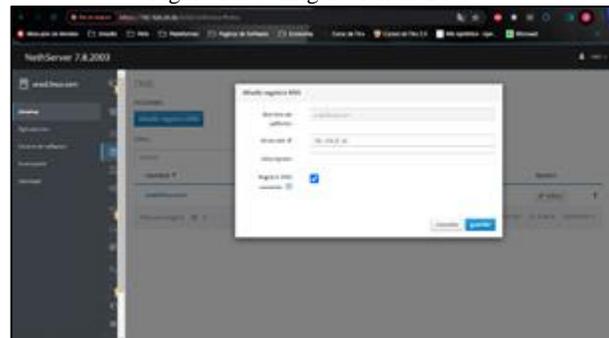
Figura 13. Configuración del servidor DHCP



Fuente. Autoría Propia

Ahora se procede a crear una reserva de direcciones ip en el servidor DHCP, se realizará la reserva de una dirección ip para la máquina Ubuntu desktop 2, para posteriormente probar el acceso desde fuera de la red LAN el cual fue exitoso ya que cargo el panel de control de nethserver. Por último, se debe la configuración del servidor DNS, para ello está la opción DNS >> Añadir registro DNS y se aplica la siguiente configuración:

Figura 14. Configuración de DNS



Fuente. Autoría Propia

Se realiza el registro en todos los servicios de infraestructura IT del nethserver en la estación de trabajo, con ello da cumplimiento a la temática

## 6 PROXY

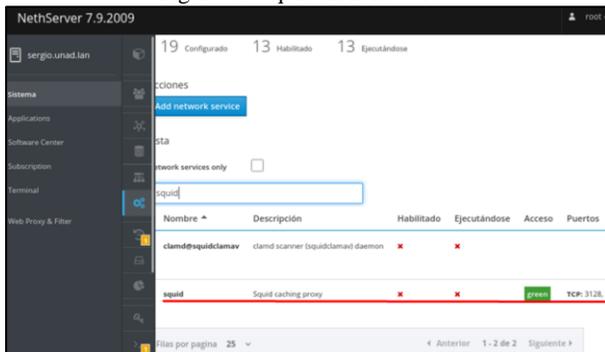
Evidenciamos la implementación de un entorno de red más seguro y eficiente mediante las configuraciones de filtro desde el panel de control del Proxy. Se espera establecer un sistema de filtrado de tráfico efectivo que permita controlar y monitorear el flujo de información dentro y fuera de la red corporativa. Además, se anticipa mejorar la protección contra amenazas externas al implementar capas adicionales de seguridad, como la filtración de contenido malicioso y la prevención de intrusiones.

Para este ejercicio debemos descargar primero la versión de Nethserver 7.8 o 7.9 para poder usar la interfaz de esta herramienta e implementar las utilidades de firewall de acuerdo a las mismas configuraciones descritas al inicio, Como se menciona en [2].

### 6.1 CONFIGURACIÓN PROXY

Después de la actualización de NetServer, se procede a buscar el módulo de la aplicación web proxy y web filter. Se observa que el servicio squid no está habilitado ni se ejecuta en el puerto TCP 3128 como se requiere. Al acceder al panel de control de NethServer y dirigirse al módulo de Proxy, se confirma que efectivamente se encuentra deshabilitado.

Figura 15. squid en zona verde

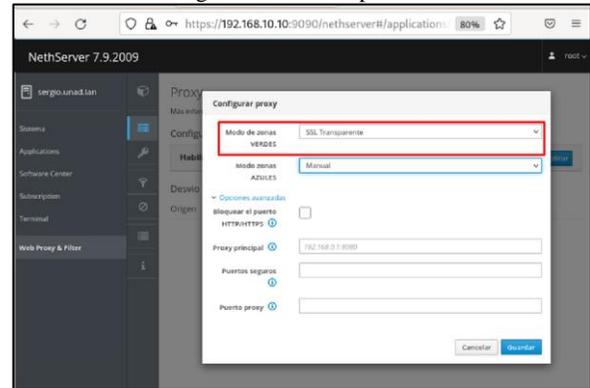


Fuente. Autoría Propia

### 6.2 PANEL DE CONTROL PROXY

Al ingresar al módulo de Proxy en el panel de control de NethServer, se observa que actualmente se encuentra deshabilitado. Se procede a configurar el campo "ssl transparente" en el modo de zona verde. Tras esta configuración, se verifica que el proxy esté habilitado y en funcionamiento. Luego, al dirigirse a la sección de Web Proxy Filter, se confirma que las configuraciones aplicadas hayan cambiado el estado a habilitado. Finalmente, para visualizar los resultados de manera gráfica, se establece la configuración de Netdata en aplicaciones y servicios, permitiendo el acceso a la zona verde.

Figura 16. Sll transparente

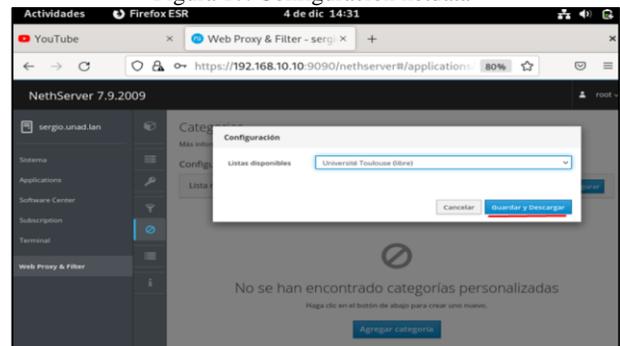


Fuente. Autoría Propia

### 6.3 CONFIGURACIÓN NETDATA

- Para obtener una representación visual de los resultados, se procede a configurar Netdata en las secciones de aplicaciones y servicios, permitiendo el acceso a la zona verde. Posteriormente, se accede a las categorías pertinentes para guardar y descargar la configuración de Netdata en el servidor, ampliando así la visibilidad y el registro de datos en tercera persona para un análisis detallado.

Figura 17. Configuración netdata



Fuente. Autoría Propia

### 6.4 FILTROS DE PROXY

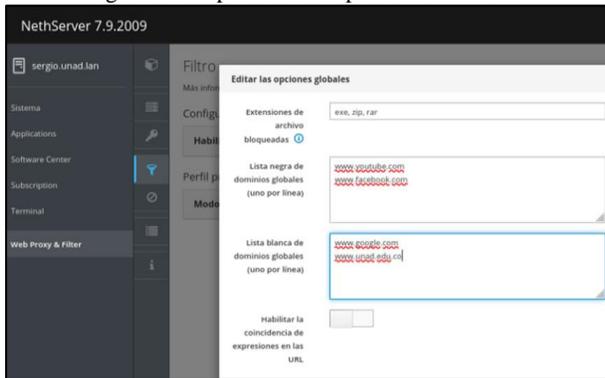
Ahora nos dirigimos a los filtros de las extensiones y dominios y editamos las opciones para permitir y denegar el alcance del host en la red corporativa mediante las reglas del proxy. De acuerdo con Nethesis Srl and the NethServer project contributors "El proxy web es un servidor que se encuentra entre las PCs de LAN y los sitios de Internet." [3].

Las reglas del proxy en NethServer se refieren a las directivas configurables que controlan y filtran el tráfico de red a través del servidor proxy. Estas reglas pueden incluir criterios como la dirección IP de origen, el destino, los puertos, el protocolo y el tipo de contenido permitido o restringido. Algunas de las reglas comunes incluyen:

- Filtrado de Contenido: Restricciones basadas en categorías, como sitios web de redes sociales, streaming de video, sitios de juegos, etc.
- Acceso Basado en Horarios: Permitir o restringir el acceso a determinados recursos durante ciertos períodos del día.
- Control de Ancho de Banda: Limitar la velocidad de descarga y carga para ciertos tipos de tráfico o usuarios.
- Filtrado por URL: Permitir o bloquear acceso a sitios web específicos basados en sus URLs.
- Listas Negras y Blancas: Crear listas para permitir o bloquear ciertos dominios o direcciones IP.

Estas reglas permiten a los administradores de red establecer políticas de acceso y seguridad para garantizar un uso adecuado de los recursos de red y proteger contra amenazas externas. La configuración de estas reglas puede realizarse a través del panel de control de NethServer, brindando flexibilidad y control sobre el tráfico de la red.

Figura 18. Implementando políticas de acceso

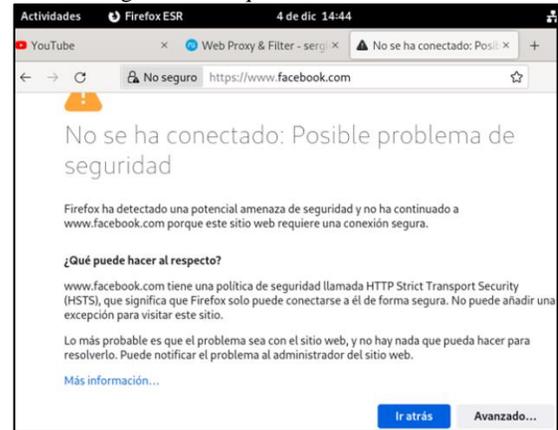


Fuente. Autoría Propia

## 6.5 POLÍTICAS DE RESTRICCIÓN

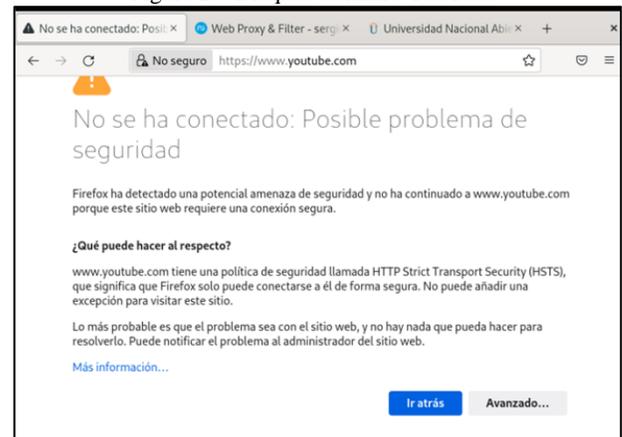
Después de establecer las restricciones de alcance, se procede a bloquear ciertas categorías de sitios web según las políticas de la empresa. Luego, se configura el equipo en modo proxy para el puerto 3128, abarcando los protocolos de host HTTP y HTTPS. Posteriormente, tras aplicar las configuraciones de restricción y activación del proxy, se verifica la efectividad de las reglas mediante el navegador, realizando búsquedas de hosts que se encuentran en la lista negra de acceso a la red corporativa, como, por ejemplo, Facebook y YouTube.

Figura 19. Bloqueo dominio Facebook



Fuente. Autoría Propia

Figura 20. Bloqueo dominio YouTube



Fuente. Autoría Propia

## 6.6 POLÍTICAS DE ACCESO PERMITIDAS

Después de aplicar la configuración de restricción y activación del proxy, se verifica a través del navegador si las reglas se han implementado con éxito, llevando a cabo la búsqueda de uno de los hosts incluidos en la lista blanca de acceso libre a la red corporativa, como, por ejemplo, Google.

Además, se valida mediante el navegador de la máquina virtual el segundo y último host modificado según las reglas del proxy, que se encuentra en la lista blanca de acceso corporativo (Unad). Esto confirma un despliegue exitoso del host configurado, cumpliendo así con los requerimientos de la temática 2: Proxy.

Figura 21. Acceso dominio google



Fuente. Autoría Propia

Figura 22. Acceso dominio google



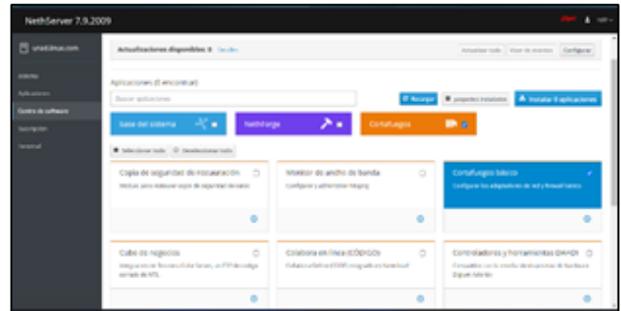
Fuente. Autoría Propia

## 7 CORTAFUEGOS

Se realiza la implementación y configuración para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas y su posterior validación del funcionamiento del cortafuego aplicando las restricciones solicitadas, esta configuración se hará desde una estación de trabajo GNU/Linux, para este ejercicio se usará la versión 7.9 y se usará la herramienta y utilidades de firewall de acuerdo a las mismas configuraciones descritas al inicio, Como se menciona en [2].

Para empezar con el desarrollo de la temática se instalarán las utilidades de firewall desde la opción centro de software:

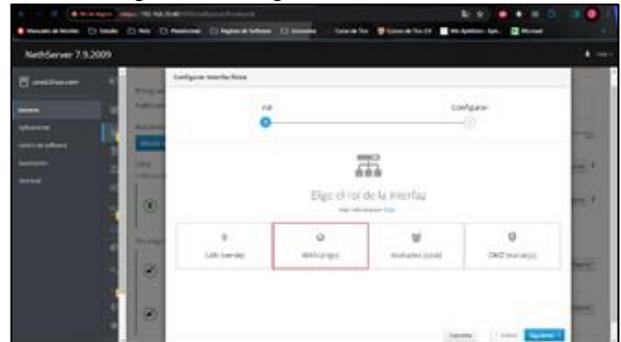
Figura 23. Instalación de los paquetes de firewall en nethserver



Fuente. Autoría Propia

Se ingresa a la plataforma y se inicia con la configuración de cada uno de los puertos, teniendo en cuenta que el verde se utilizará como red LAN, el naranja como red DMZ y finalmente el rojo como red WAN. Para la configuración de la red WAN, se hará con el puerto de la máquina virtual que se configura con adaptador puente, así se asegura que la salida a internet, y las demás redes pasarán por el Firewall.

Figura 24. Configuración de la red WAN



Fuente. Autoría Propia

Para la red WAN, su configuración de red será por protocolo DHCP y tomará la IP que brinda la red, para utilizarla como puerta de enlace de la red LAN, para la configurarla se configura el puerto de la máquina virtual que se configuró con red interna.

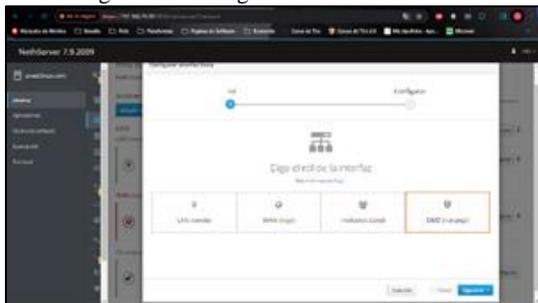
Figura 25. Configuración de la red LAN



Fuente. Autoría Propia

Ahora se procede con la configuración en el protocolo de IP estática, en el segmento que se va a utilizar para la red LAN como puerta de enlace (Gateway), se utilizará la IP que da el DHCP en la red WAN, una vez hecho esto se da click en siguiente y se procede con la configuración de la red DMZ en la cual se usará el puerto de la máquina virtual que se configura como red interna, donde se ingresaron con un segmento de red diferente al de la red LAN y la red WAN.

Figura 26. Configuración de la red DMZ

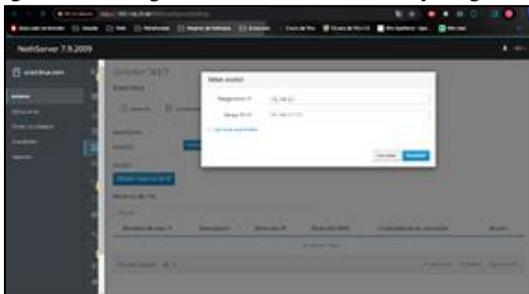


Fuente: Autoría Propia

Ahora se configura la dirección ip que se utilizará para la red DMZ, en un segmento de red diferente al de la red LAN y la red WAN para este caso se usará la ip 192.168.56.101, la cual es la ip del servidor que se está usando como DMZ.

Para asegurar que el DHCP haga su trabajo correctamente, se configura el servidor, indicando que suministre ip desde la ip siguiente a la que se utiliza en la red verde LAN.

Figura 27. Configuración de servidor DHCP y rango de ip



Fuente: Autoría Propia

Ahora desde la opción Aplicaciones >> Cortafuegos se muestra como queda configurada la topología de red a nivel gráfico, se evidencia que la configuración del firewall está aplicada de acuerdo al estándar indicado en la documentación de nethserver [7].

Figura 28. Topología de red de firewall



Fuente: Autoría Propia

Para crear la regla en el firewall y bloquear el acceso a los portales de entretenimiento y las redes sociales se gun la documentación de nethserver [8], indica que es necesario 4 elementos para crear y aplicar una regla según la documentación de nethserver:

Las reglas se aplican a todo el tráfico que pasa a través del cortafuego. Cuando un paquete de red se desplaza de una zona a otra, el sistema busca entre las reglas configuradas. Si el paquete coincide con una regla, se aplica la regla.

Nota

El orden de la regla es muy importante. El sistema siempre aplica la primera regla que coincide.

Una regla consta de cuatro partes principales:

Action: action to take when the rule applies

- Source
- Destination
- Service

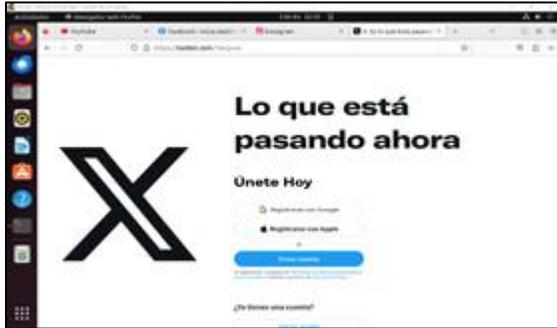
Las acciones disponibles son:

- ACCEPT: acepta el tráfico de red
- REJECT: bloquea el tráfico y notifica al host remitente
- DROP: bloquea el tráfico, los paquetes se eliminan y no se envía ninguna notificación al host del remitente
- ROUTE: enruta el tráfico al proveedor de WAN especificado.
- [8, Reglas]

Según esta definición necesitamos una acción que sería Reject o Drop según la necesidad para bloquear el tráfico, un servicio, un origen y un destino, sin embargo, al ser páginas con dominios públicos sus orígenes van a variar ya que sus ip's al ser dinámicas van a ser diferentes todo el tiempo por lo cual el concepto de regla no aplica para la temática, y la opción más aceptable es la de establecer un filtro proxy para estos dominios, según la misma documentación de nethserver [9].

Ahora vamos a bloquear la apertura de sitios o portales Web de entretenimiento y redes sociales, para esto primero se debe validar el acceso a páginas de este tipo, para este caso vamos a validar el acceso a YouTube, Facebook, Instagram y Twitter, una vez hecha esta validación desde la opción proxy >> Configurar proxy dejamos el Modo de zonas VERDES en transparente y el Modo zonas AZULES en Manual.

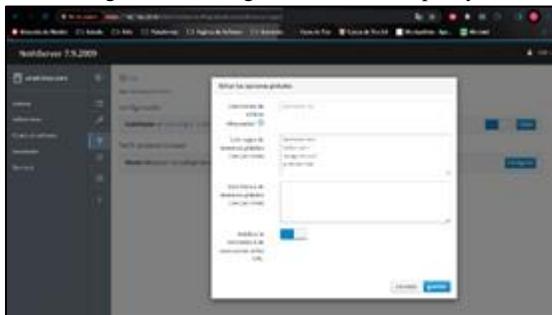
Figura 29. Validación de acceso a páginas de redes sociales



Fuente: Autoría Propia

Ahora desde la opción Filtro, desde la opción Editar las opciones globales, se agregan los dominios de las aplicaciones que se van bloquear y posteriormente se guarda la configuración.

Figura 30. Configuración del filtro proxy



Fuente: Autoría Propia

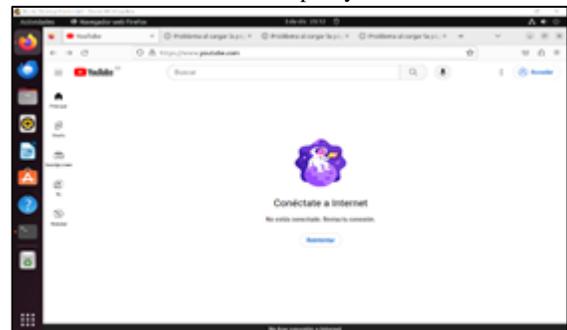
Al aplicar la política y recargar las páginas abiertas anteriormente se evidencia que ya no cargan. Sin embargo al validar el acceso a otras páginas estas sí pueden acceder sin problemas, para este caso se va a validar el acceso a la página de la UNAD y si carga pero a las otras no.

Figura 31. Página de twitter sin conexión después de aplicar el filtro proxy



Fuente: Autoría Propia

Figura 32. Página de YouTube sin conexión después de aplicar el filtro proxy



Fuente: Autoría Propia

Figura 33. Acceso a la página de la UNAD validado

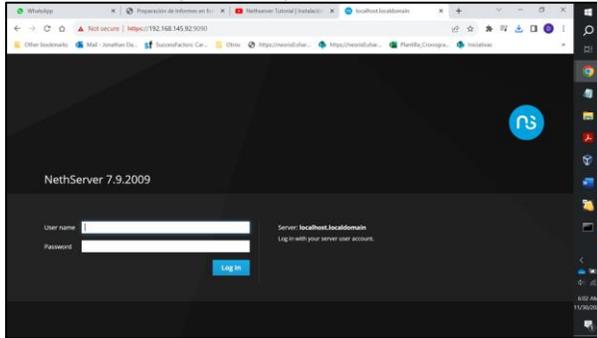


Fuente: Autoría Propia

## 8 FILE SERVER Y PRINT SERVER

### 8.1 INGRESO A NETHSERVER

Figura 34. Ingreso a nethserver



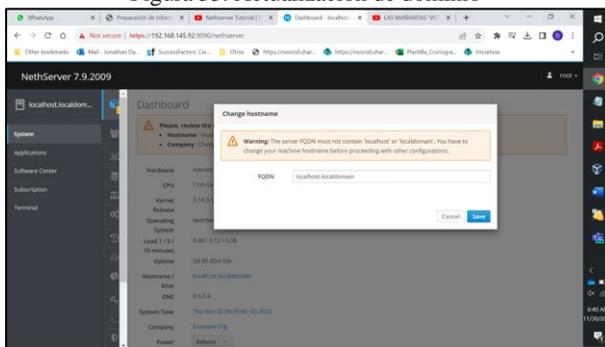
Fuente: Autoría Propia

Luego de la instalación previamente expuesta, es necesario acceder a la consola de administración de nethserver, para desde allí, poder realizar las configuraciones que tienen lugar y definir los servicios que serán ejecutados para suplir las necesidades del negocio.

### 8.2 ACTUALIZACIONES DE SISTEMA

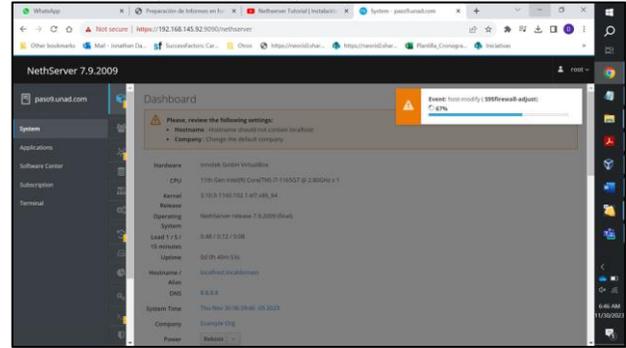
Nethserver cuenta con una interfaz intuitiva y clara que permite ejecutar las acciones requeridas; al acceder a ella, es preciso dirigirse al centro de software y buscar las herramientas a las que haya lugar, para el caso particular, se utilizará el servicio de compartido de archivos y el servicio de impresoras compartidas.

Figura 35. Actualización de dominio



Fuente: Autoría Propia

Figura 36. Configuración de dominio

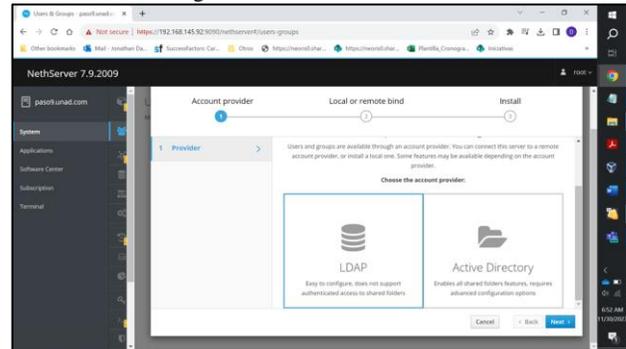


Fuente: Autoría Propia

### 8.3 CONFIGURACIÓN DE USUARIOS

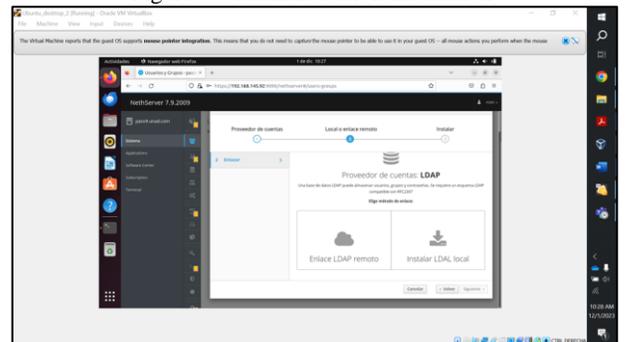
LDAP es una herramienta de software libre que permite la administración de servicios de archivos e impresoras compartidas, entre otras capacidades, incluida la de conectarse con active directory de Windows, eso habilita algunas funcionalidades extra, como compartir archivos multiplataforma que serán de gran ayuda para poder tener una red integrada y funcional.

Figura 37. Instalación LDAP



Fuente: Autoría Propia

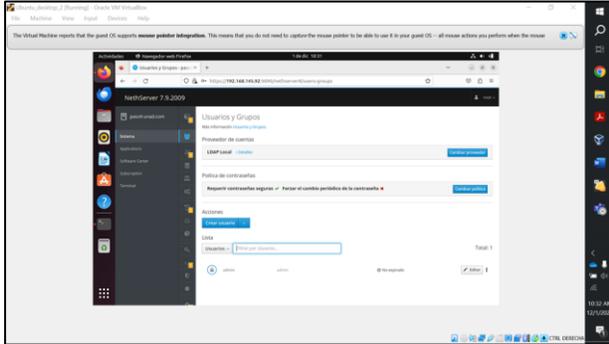
Figura 38. Administración instalación



Fuente: Autoría Propia

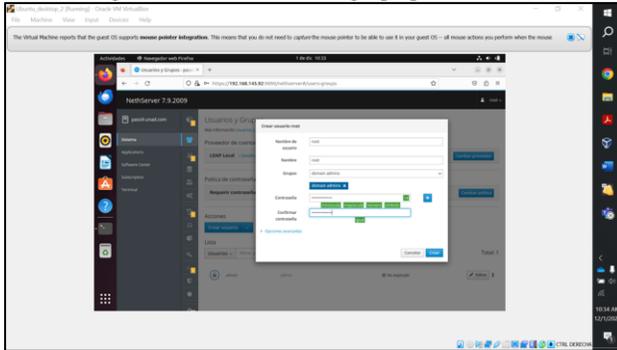
Los grupos permiten tener capacidades de administración específicas, como tener segmentos de usuarios que puedan acceder a recursos diferentes de otros, todo ello basado en permisos.

Figura 39. Administración grupos



Fuente: Autoría Propia

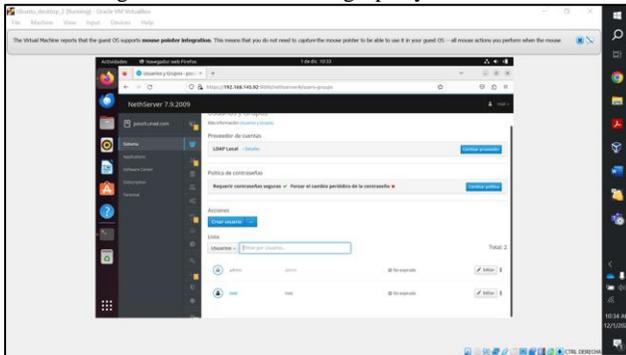
Figura 40. Administración grupo por defecto



Fuente: Autoría Propia

Luego de generados los grupos y usuarios, la consola de administración mostrará una lista de los que hayan sido creados, con sus respectivos permisos.

Figura 41. Nueva lista de grupos y usuarios

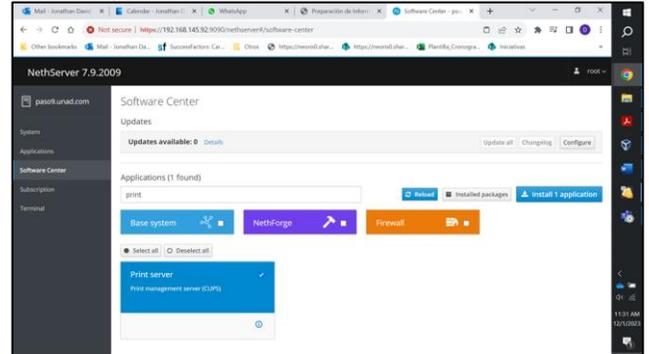


Fuente: Autoría Propia

## 8.4 INSTALACIÓN SERVICIOS

En este paso puntualmente, se realiza la instalación de las paqueterías y software necesarios que permitirán la gestión de los diferentes servicios y herramientas.

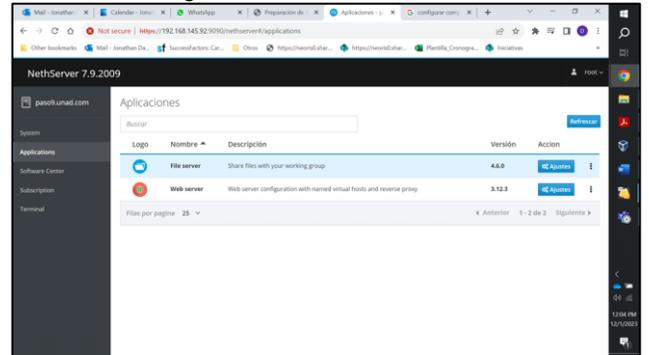
Figura 42. Instalación Print server y file server



Fuente: Autoría Propia

No solamente se cuenta con servicios de impresión y compartir archivos, la herramienta tiene una serie de habilidades como administración de dominios, administración de proxys y seguridad, lo que la hace la herramienta ideal para administración de servicios y seguridad.

Figura 43. Listado de servicios



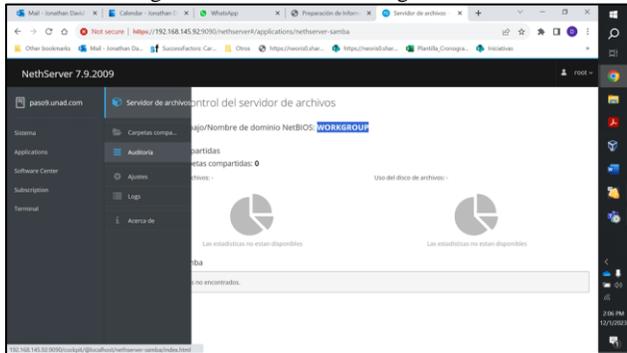
Fuente: Autoría Propia

## 8.5 CONFIGURACIÓN DE SERVICIOS

Se realiza la configuración de los servicios instalados previamente, con el fin de permitir que se genere la dinámica de red mediante herramientas para compartir archivos e impresoras.

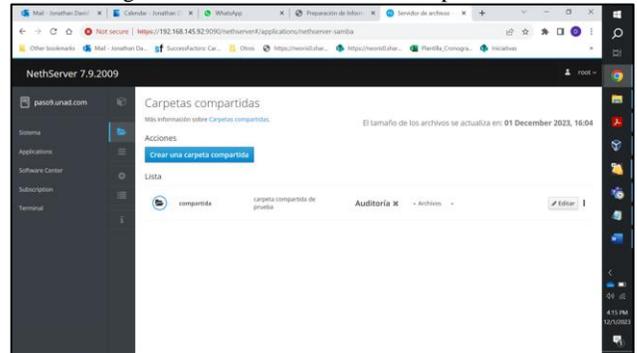
Los servicios de impresora y carpetas o recursos compartidos en red, permiten que de ser necesarios, varios equipos cliente dentro del dominio, puedan acceder a un único recurso, lo que conlleva a economizar en términos de costos y aumento en la productividad.

Figura 44. Inicio de la configuración



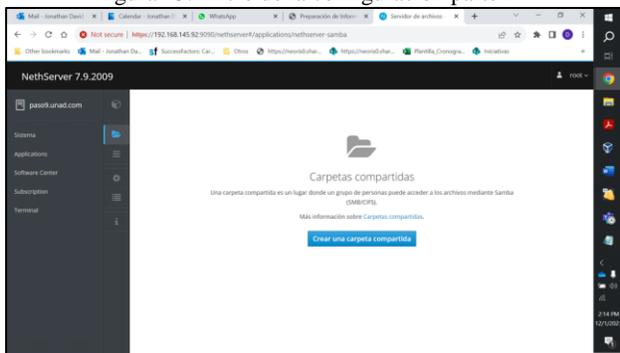
Fuente: Autoría Propia

Figura 47. Listado de archivos compartidos



Fuente: Autoría Propia

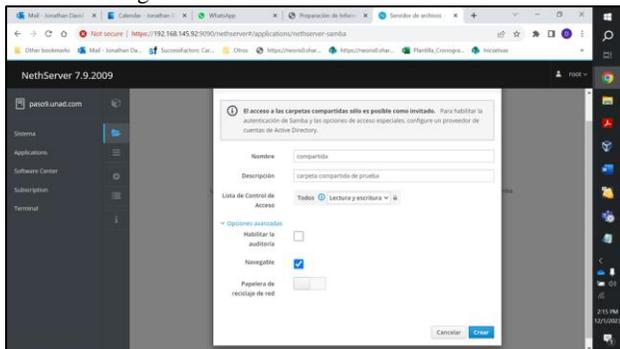
Figura 45. Inicio de la configuración parte 2



Fuente: Autoría Propia

La configuración de nethserver en términos de carpetas e impresoras compartidas, resulta ser sencilla, se trata de generar un recurso que debe contener nombre y descripción, así como una serie de permisos básicos (editar, leer).

Figura 46. Definición de características



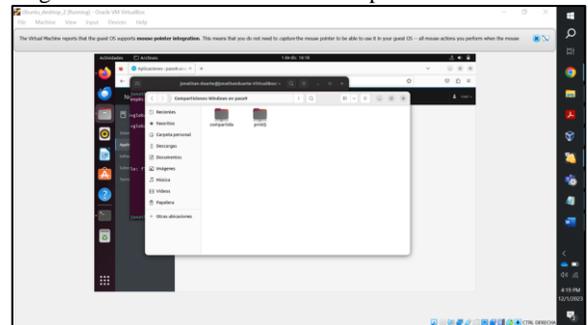
Fuente: Autoría Propia

Al finalizar con las configuraciones citadas previamente, se listan los archivos, carpetas o recursos compartidos, con sus respectivos permisos, por lo que resta verificar su adecuado funcionamiento.

## 8.6 DEMOSTRACIÓN FUNCIONAMIENTO

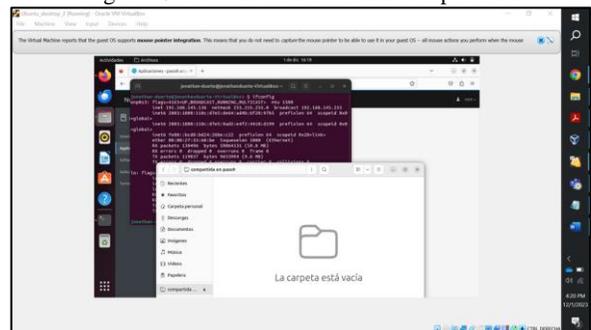
Luego de realizadas las respectivas configuraciones propias del funcionamiento de las herramientas de fileserver y printserver, se verifica el funcionamiento de los servicios y el acceso a los recursos compartidos.

Figura 48. Consulta de recursos compartidos desde cliente



Fuente: Autoría Propia

Figura 49. Acceso a los recursos compartidos



Fuente: Autoría Propia

## 9 CONCLUSIONES

La implementación del proxy y las reglas aplicadas para restringir el acceso a dominios como Facebook y YouTube revelan la capacidad integral de esta herramienta en el control de acceso web. Los resultados obtenidos no solo demuestran la efectividad en la aplicación de políticas de seguridad, sino también el poder que posee el proxy para salvaguardar la integridad y la productividad en entornos corporativos.

Al bloquear estos dominios, se garantiza la mitigación de distracciones no relacionadas con el trabajo, mejorando así el enfoque laboral y la eficiencia general. Además, el proxy no solo actúa como una barrera de seguridad, sino también como un regulador de recursos, optimizando el ancho de banda y mejorando el rendimiento de la red al limitar el acceso a contenidos no esenciales.

Se evidencia que una de las habilidades de nethserver, es permitir que tareas complejas o de administración avanzada se vuelvan sencillas y fáciles de realizar, así, el administrador del sistema luego de realizar una implementación adecuada, podrá gestionar servicios de manera oportuna y efectiva.

Son recopilados los diferentes conocimientos asociados a las temáticas de Linux (LPI) para realizar una implementación final que cubre con las necesidades del caso propuesto al inicio del diplomado.

## 10 REFERENCIAS

- [1] OpenTEC. (Jr Dos de mayo 400 Rioja-Perú). [En línea] [www.opentec.com.pe/nethserver.php](http://www.opentec.com.pe/nethserver.php)
- [2] Getting started with NethServer. [En línea] [www.nethserver.org/getting-started-with-nethserver](http://www.nethserver.org/getting-started-with-nethserver)
- [3] Nethesis Srl and the NethServer project contributors. (2023). [En línea]. Sphinx [https://docs.nethserver.org/es/v7/web\\_proxy.html](https://docs.nethserver.org/es/v7/web_proxy.html)
- [4] Nethserver - Instalación y configuración básica. (s. f.). Configura Ubuntu, Proxmox, Zabbix & NethServer para entornos de Oficina. <http://911-ubuntu.weebly.com/nethserver-instalacion/nethserver-instalacion-basica>
- [5] Tipos de instalación — NethServer 7 Final. (s. f.). <https://docs.nethserver.org/es/v7/installation.html>
- [6] "Nethserver Tutorial." [www.youtube.com, https://www.youtube.com/watch?v=GrvZutNZIRg](https://www.youtube.com/watch?v=GrvZutNZIRg) Accessed 03 Dec. 2023.
- [7] traffic default. "Firewall — NethServer 7 Final." docs.nethserver.org, May. 2018, <https://docs.nethserver.org/es/v7/firewall.html>. Accessed 03 Dec. 2023
- [8] "Firewall y gateway / Cortafuego y Puerta de enlace — NethServer 6.10 Final." docs.nethserver.org, <https://docs.nethserver.org/es/v6/firewall.html> Accessed 03 Dec. 2023.
- [9] "Proxy web — NethServer 6.10 Final." docs.nethserver.org, [https://docs.nethserver.org/es/v6/web\\_proxy.html](https://docs.nethserver.org/es/v6/web_proxy.html). Accessed 06 Dec. 2023.