

# Optimización y Eficiencia: Soluciones Específicas con GNU/Linux NethServer

Angelica Maria Otorora Ramirez  
e-mail: amotalorar@unadvirtual.edu.co

Brayan Leonel Tovar Jimenez  
e-mail: bltovarj@unadvirtual.edu.co

Diana Marcela Leon Borda  
e-mail: dmleonbo@unadvirtual.edu.co

Diego Andres Marroquin Rengifo  
e-mail: damarroquinr@unadvirtual.edu.co

Tania Ximena Losada Rubiano  
e-mail: txlosadar@unadvirtual.edu.co

**RESUMEN:** A continuación se muestran la ejecución de varios servicios como DHCP Server, DNS Server y Controlador de Dominio, servidor de Proxy, cortafuegos o Firewall, File Server y Print server, y por último el VPN. Estos gestionados por una gran plataforma llamada Nethserver, que es una distribución de GNU/Linux, que se erige como una opción eficaz para ofrecer servicios. Los resultados satisfactorios son un indicio del gran potencial que tiene, ofreciendo beneficios como la seguridad y el control del acceso a internet y facilitar la compartición de archivos en la red.

**PALABRAS CLAVE:** DNS, DCHP, firewall, Nethserver, print, proxy, VPN.

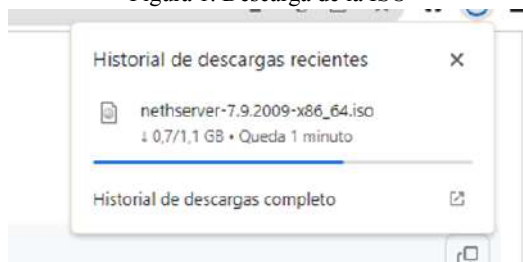
## 1 INTRODUCCIÓN

Se busca implementar las soluciones para la problemática dada a partir del desarrollo de la creación de varios servicios usando como herramienta principal el sistema operativo GNU/Linux, centrándose en instalarlos y configurarlos de una manera óptima para el beneficio de alguna empresa sin importar su tamaño, dándole seguridad y respaldo a su sistema tecnológico.

## 2 INSTALACIÓN DE NETHSERVER

Primeramente, se debe realizar la descarga de la ISO a través de la página oficial de NethServer, <https://www.nethserver.org/getting-started-with-nethserver/>

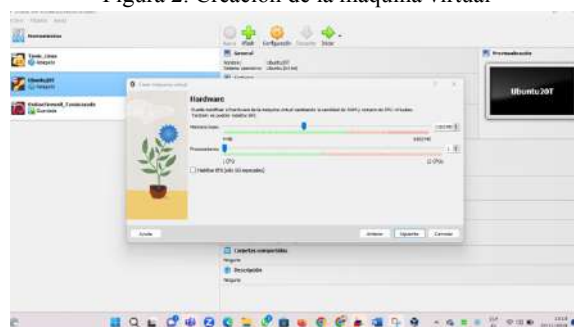
Figura 1. Descarga de la ISO



Fuente: Autoría propia

Cuando este se encuentre descargado, se procede a crear una nueva máquina virtual en el programa VirtualBox, allí se configura tamaño de disco, uso de procesador y se incluye la ISO descargada.

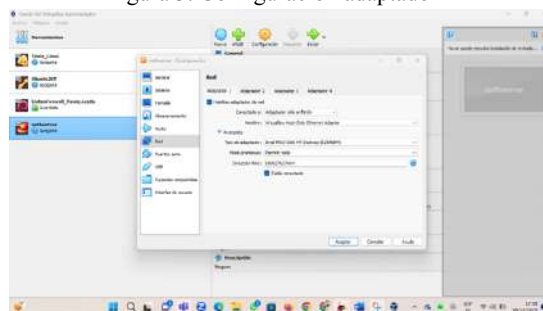
Figura 2. Creación de la máquina virtual



Fuente: Autoría propia

Al finalizar las características de la máquina, se procede a dirigirse a configuraciones de la misma, en esta ocasión se configura la red, el adaptador 1 se lo deja como NAT y se da en "Permitir todo"

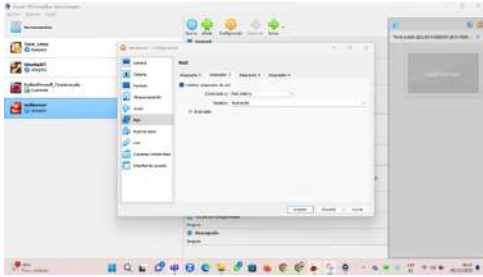
Figura 3. Configuración adaptador 1



Fuente: Autoría propia

Adicionalmente, se configuran dos adaptadores más, en este caso el adaptador 2 estará conectado a la red interna y se lo renombra "RedVerde", el adaptador 3 de igual manera conectado a la red interna y será llamado "RedAzul" o "RedNaranja" dependiendo de la red que se vaya a conectar.

Figura 4. Configuración adaptador 2



Fuente: Autoría propia

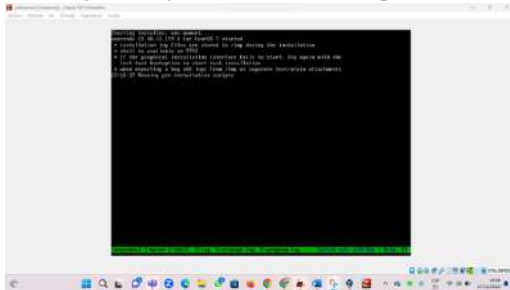
Figura 5. Configuración adaptador 3



Fuente: Autoría propia

Se inicia el sistema operativo, donde primeramente se escoge el NethServer y este automáticamente iniciará sus configuraciones. En el root se debe colocar una clave la cual permite ingresar al sistema como también crear un usuario.

Figura 6. Ejecución del sistema operativo



Fuente: Autoría propia

Después de finalizar la configuración del sistema operativo, se comprueba que este permita la conexión remota a través de otro sistema operativo, para esto se empieza con el usuario que se creó y se ejecuta el comando "ifconfig", este arroja la IP del sistema.

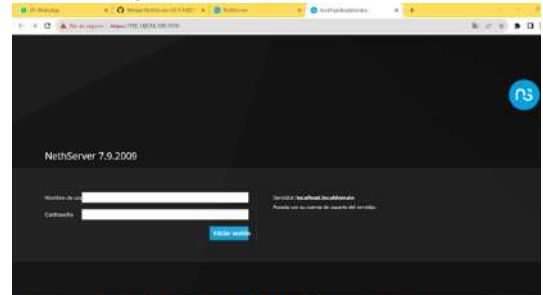
Figura 7. Verificación de IP



Fuente: Autoría propia

Se realiza la conexión desde el otro sistema operativo haciendo uso de un navegador y escribiendo en la URL "<https://192.168.56.105:9090>", con esto se ingresa a la interfaz web de NethServer, se debe escribir el usuario y clave, para este el nombre de usuario será root y la clave que se le haya asignado.

Figura 8. Interfaz web NethServer

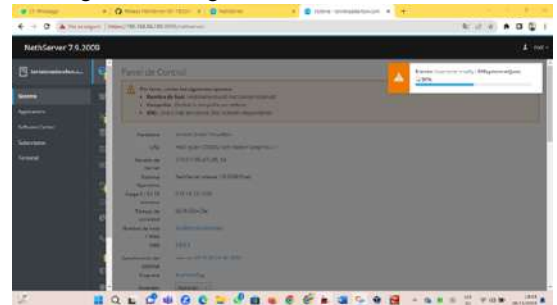


Fuente: Autoría propia

### 3 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Finalizada la configuración de NethServer, se empieza la misma con el usuario root, al iniciar se actualiza el hostname, por el nombre de usuario que se generó.

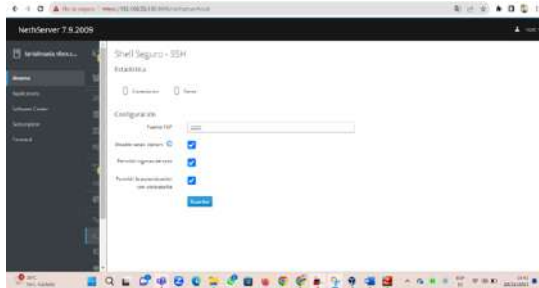
Figura 9. Configuración del hostname



Fuente: Autoría propia

Se ejecuta la configuración del Shell, haciendo cambio del puerto 22 por el 2222 u otro que sea indicado.

Figura 10. Configuración del Shell



Fuente: Autoría propia

Para poder tener una conexión, se inicia la configuración de los adaptadores de red, iniciando por el WAN, que es el rojo, este solamente se lo dejará como DHCP, dejando la IP y máscara de red como se encuentra.

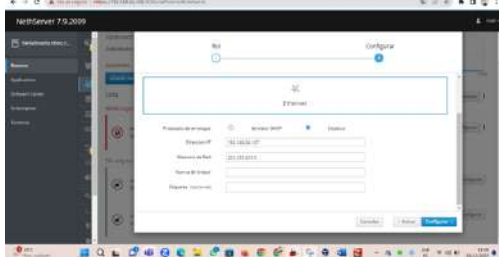
Figura 11. Adaptación del adaptador rojo



Fuente: Autoría propia

Se configura seguidamente la red LAN, que es la Verde, se deja esta por medio de IP estática y se le asigna la IP 192.168.55.107.

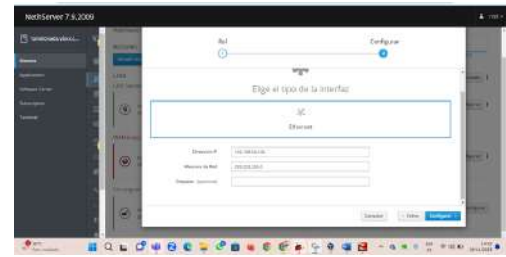
Figura 12. Adaptación del adaptador verde



Fuente: Autoría propia

Se ejecuta la configuración de la red azul o naranja, de igual manera se la ajusta como estática y en este caso se le asigna la IP 192.168.54.108.

Figura 13. Adaptación del adaptador azul o naranja



Fuente: Autoría propia

En consola se verifica que efectivamente los cambios hayan quedado procedidos.

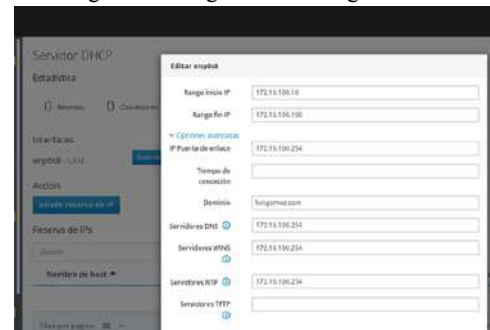
Figura 14. Comprobación de redes en consola



Fuente: Autoría propia

Se realiza la configuración del rango de red para activar el DHCP, en esta ocasión se activa el enp0s8.

Figura 15. Asignación de rango de red



Fuente: Autoría propia

Se valida que este quede activado.

Figura 16. Activación de interfaz enp0s8

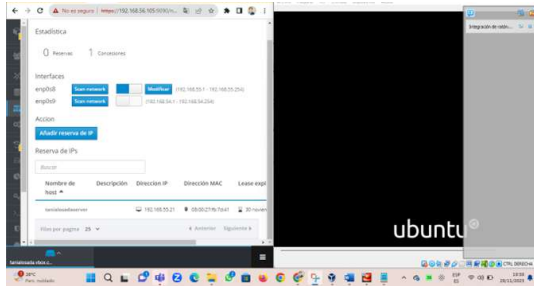


Fuente: Autoría propia

Para comprobar que efectivamente se puede proceder la conexión en otros sistemas operativos, se ejecuta el sistema operativo Ubuntu Desktop y allí se configura el adaptador 1 con la conexión de red verde. Se visualiza que

efectivamente se presenta una conexión en NethServer conforme se ejecuta el sistema operativo.

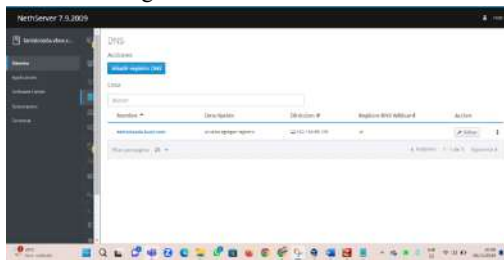
Figura 17. Conexión con enp0s8



Fuente: Autoría propia

En el proceso final se ejecuta la configuración de las DNS, se ingresa a este apartado y desde allí se crea el host, se le asigna un nombre el cual será tanialosada.local.com y la IP será con la que se ingresa a la interfaz web de NethServer, por último se agrega una descripción.

Figura 18. Creación de DNS



Fuente: Autoría propia

Se verifica la conexión en un servidor donde no se tiene establecida la conexión directa con las IP de NethServer y se visualiza que efectivamente no se puede conectar a la DNS establecida.

Figura 19. Confirmación conexión con DNS



Fuente: Autoría propia

En este caso se realiza la conexión con un servidor que tenga una configuración con NethServer y efectivamente se visualiza conexión directa a la DNS.

Figura 20. Confirmación conexión con DNS



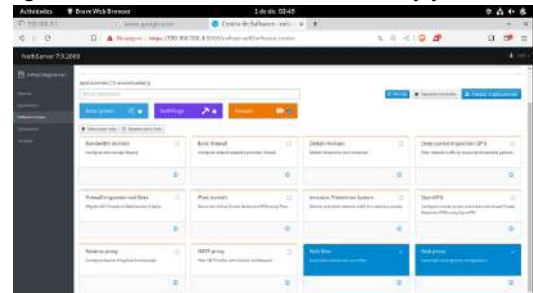
Fuente: Autoría propia

## 4 TEMÁTICA 2: PROXY

La configuración del servidor Proxy se ejecutó entre la red WAN y la red LAN, lo que corresponde a la interfaz roja con la verde, este servidor permitirá actuar como un filtro donde se negará la navegación a las páginas web que se desean.

Al tener conocimiento de esto y siguiendo con el proceso anterior, se procede con la instalación de los servicios Proxy y el filtro web desde NethServer, usando una máquina Linux en la red LAN.

Figura 21. Instalando los servicios de Proxy y filtro web

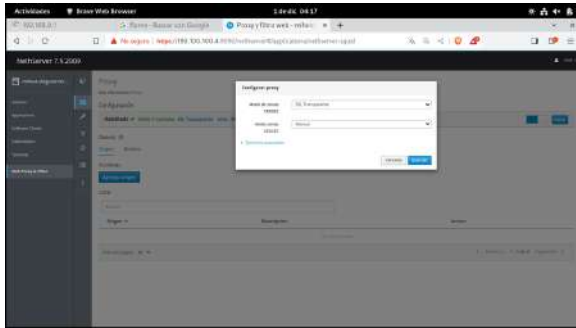


Fuente: Autoría propia

Estando en el Software Center se procede con la búsqueda de los servicios Proxy y el de filtro web, estos dos son necesarios para proceder correctamente el servidor Proxy.

Si se desea navegar más fácil se puede ajustar la aplicación de proxy, que es Squid, como acceso directo en el menú lateral.

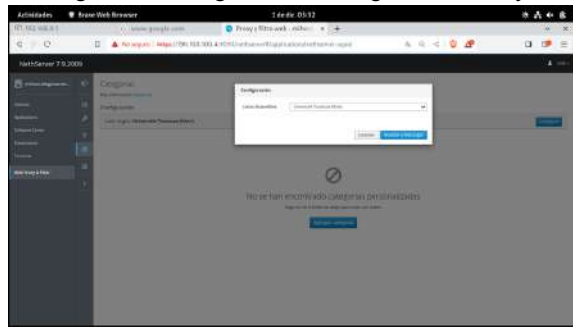
Figura 22. Primera configuración del Proxy



Fuente: Autoría propia

Se debe dirigir a “Configurar Proxy”, donde se ajusta la opción de “Modo de zonas VERDES” y para que sea efectivo el servidor Proxy se lo ajusta en “SSL Transparente” donde usa no solo el puerto 3128, sino también el 3129 que corresponde a sitios con “HTTPS”

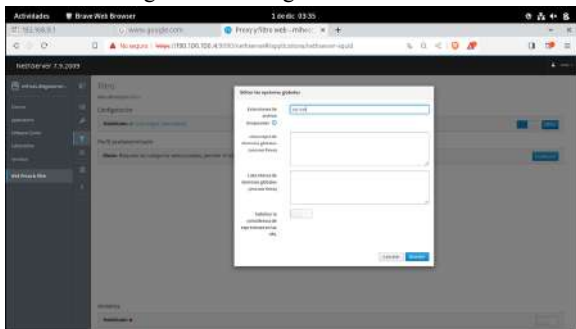
Figura 23. Configurando las categorías del Proxy



Fuente: Autoría propia

Estando en el apartado de “Configuración” del Proxy, se puede observar que tiene una lista negra y que ya tiene una por defecto, ante esto es por importante ajustarla con el botón que dice “Guardar y Descargar”

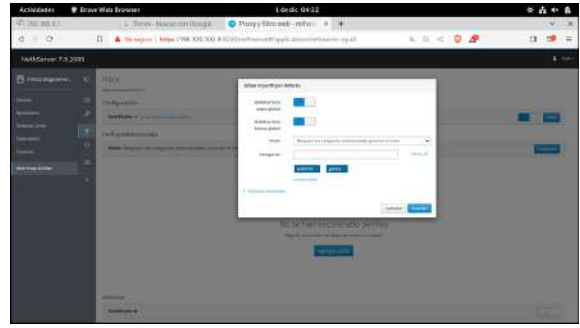
Figura 24. Configurando los filtros



Fuente: Autoría propia

En el apartado de “Filtros” es muy importante digitar las extensiones de archivo, para este caso se desea evitar archivos ejecutables y de videos AVI.

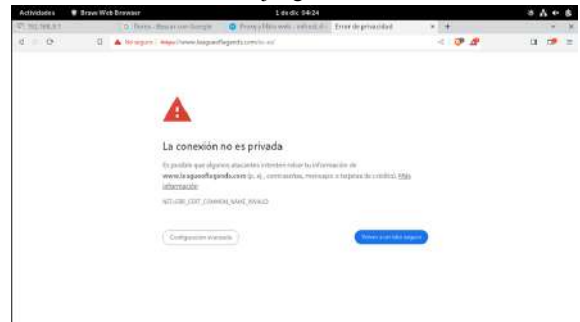
Figura 24. Seleccionado las categorías



Fuente: Autoría propia

Luego de habilitar el filtro con las extensiones, se sigue con las categorías, donde se escoge “publicite” para evitar anuncios y “games” para no dejar ingresar a sitios web de videojuegos.

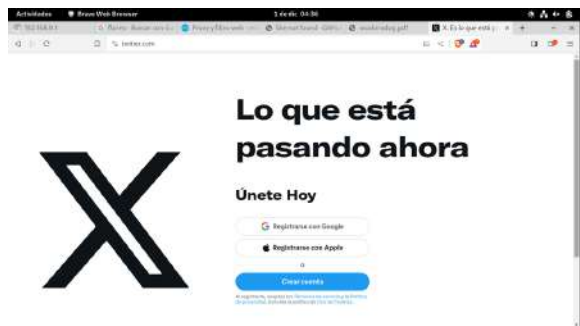
Figura 25. Corroborando el servidor Proxy en la página de juegos



Fuente: Autoría propia

Se ingresa a una página de un videojuego muy popular y se puede observar como el servidor Proxy entra en acción.

Figura 26. Corroborando acceso a páginas que no están dentro del filtro



Fuente: Autoría propia

En el caso de las redes sociales, al no estar bloqueadas por el Proxy, se puede ingresar sin problemas.

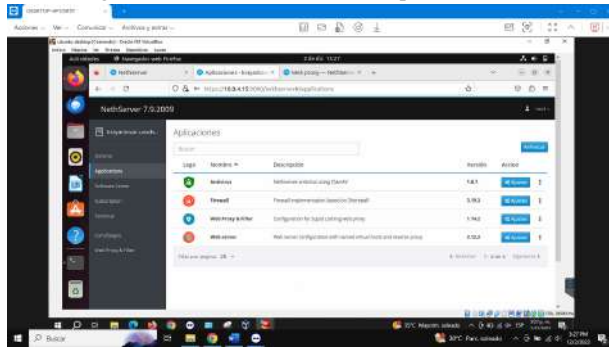
## 5 TEMÁTICA 3: CORTAFUEGOS

Una vez concluido el procedimiento de instalación de nethserver, se habilita la gestión del sistema a

través de una terminal con conectividad a la red del servidor. Es crucial ejecutar una actualización de los paquetes mediante el comando "yum update" que permita garantizar un rendimiento óptimo y la incorporación de las últimas mejoras y correcciones.

A través de Software Center, se lleva a cabo la descarga e instalación de los aplicativos de Firewall Básico, es fundamental prestar atención a la correcta configuración de la red que se realiza inicialmente, como también a cada uno de los demás procesos de configuración y de gestión del sistema, ya que un procedimiento incorrecto impediría la descarga de los respectivos paquetes, provocando una serie de errores en los procesos de actualización del sistema. Así las cosas, si cada uno de los procedimientos se realiza de la manera correcta, la disponibilidad del Firewall estará garantizada para descarga e instalación en la sección de aplicaciones de Software Center.

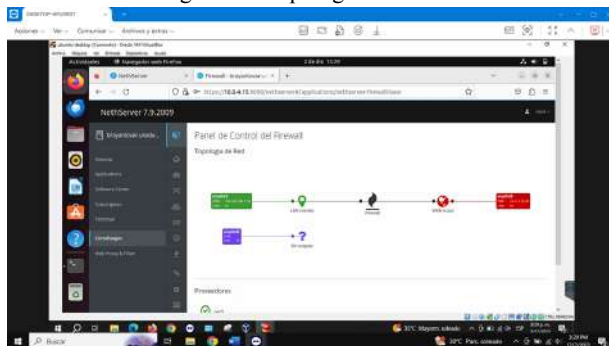
Figura 27. Interfaz Nethserver - aplicaciones



Fuente: Autoría propia

En el ámbito de la gestión de redes, se implementan cambios de asignación de direcciones IP de dinámicas a estáticas, así como la configuración de zonas de red. Esto permite establecer listas blancas y negras, definiendo qué sitios web pueden o no ser accedidos desde terminales protegidas por el cortafuegos. Esta medida no solo optimiza la estabilidad de la red, sino que también refuerza la seguridad al tener un control preciso sobre el acceso a recursos digitales, mejorando la respuesta ante posibles amenazas.

Figura 28. Topología de red

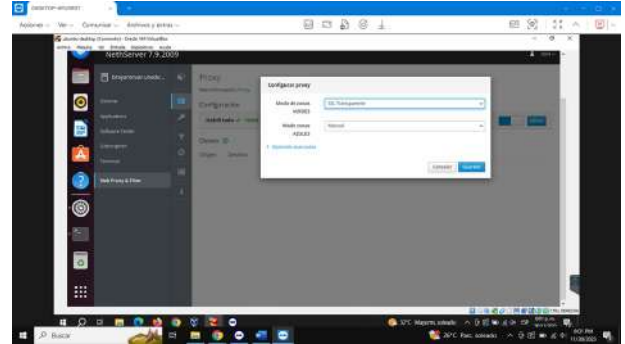


Fuente: Autoría propia

En la configuración del Proxy establecemos para el modo de zonas VERDES "SSL Transparente", el anterior

ajuste hace referencia a una configuración en la que el cifrado SSL (Secure Sockets Layer) se implementa de manera transparente, es decir, sin que el usuario o la aplicación sean conscientes de ello. SSL es un protocolo de seguridad que garantiza la privacidad y la integridad de la comunicación entre dos sistemas, como un navegador web y un servidor web.

Figura 29. Interfaz nethserver - Web Proxy & Filter - Proxy

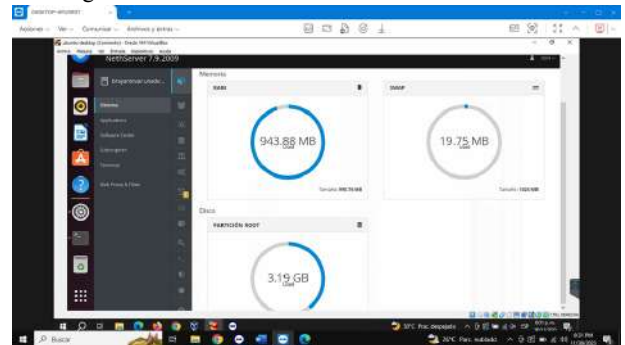


Fuente: Autoría propia

Es necesario señalar que las aplicaciones de firewall requieren significativos recursos de hardware, específicamente en cuanto a la memoria RAM. Por lo tanto, es de suma importancia tener en consideración este aspecto durante la fase de planificación para la implementación de un sistema de esta índole.

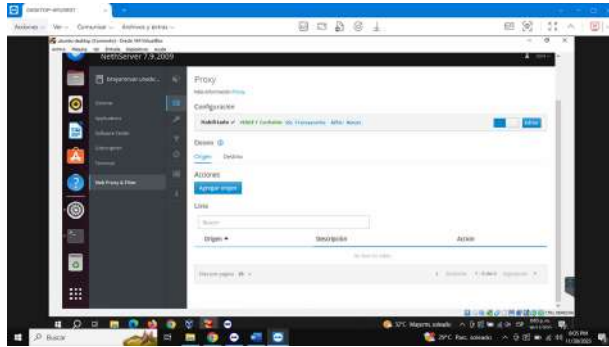
Se recomienda asignar un mínimo de 8 GB de memoria RAM al hardware. Esta asignación específica es crucial para asegurar la capacidad adecuada de procesamiento y respuesta del sistema, permitiendo así una implementación robusta y eficiente de las funciones de seguridad del firewall.

Figura 30. Interfaz Nethserver - Panel de Control



Fuente: Autoría propia

Figura 31. Interfaz Nethserver - Web Proxy & Filter - Proxy

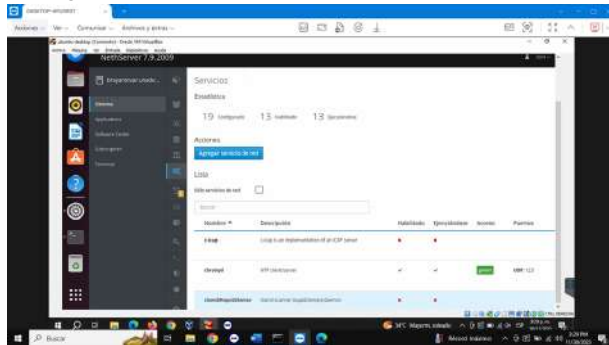


Fuente: Autoría propia

Una vez que las aplicaciones Firewall Básico son descargadas e instaladas desde el Software Center, la extensión de los servicios de NethServer se incrementa. Esto se debe a que, con las nuevas aplicaciones instaladas, la capacidad de NethServer se amplía considerablemente en cuanto a sus funcionalidades de firewall.

Es importante destacar que estas nuevas funcionalidades necesitan ser configuradas adecuadamente para entrar en operación de manera efectiva.

Figura 32. Interfaz Nethserver - Sistema - Servicios



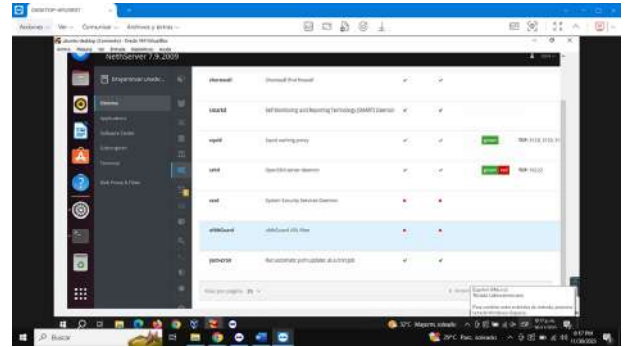
Fuente: Autoría propia

Al igual que ciertos servicios que se activan automáticamente al realizar ajustes en las respectivas aplicaciones descargadas e instaladas, existen otros servicios esenciales que demandan una activación manual para su puesta en marcha.

En este caso específico, es el servicio de *ufdbGuard*, entre otros, los cuales necesitan ser activados manualmente. Estos servicios no son obligatorios, pero son opcionales y, al mismo tiempo, indispensables para la implementación personalizada e idónea del sistema deseado.

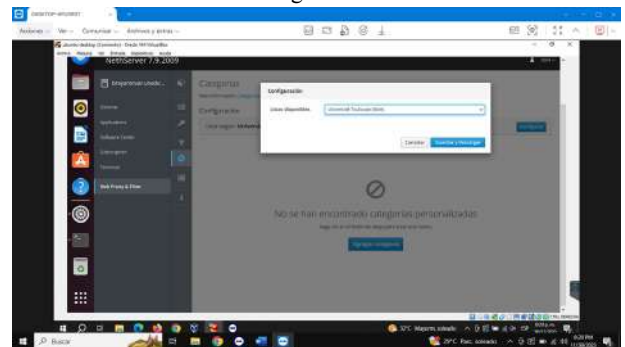
*ufdbGuard* es como un guardián digital que ayuda a filtrar lo que ves en internet y controla quién tiene acceso. Es muy útil en entornos donde necesitas decidir qué sitios web pueden visitar las personas, según reglas predefinidas. Finalmente, se puede decir que es una herramienta confiable para mantener la seguridad y el control en la web.

Figura 33. Interfaz Nethserver - Sistema - Servicios



Fuente: Autoría propia

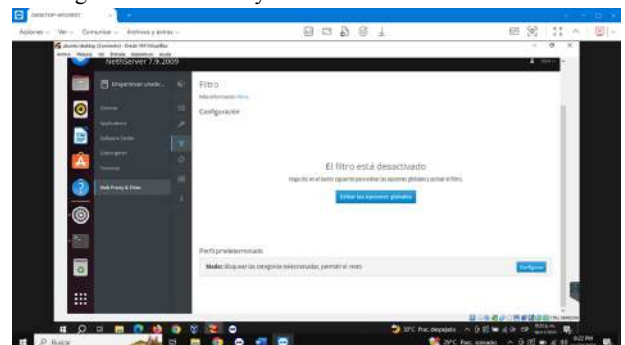
Figura 34. Interfaz Nethserver - Web Proxy & Filter - Categorías



Fuente: Autoría propia

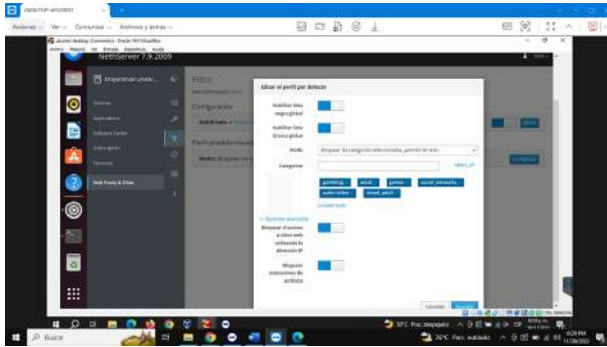
El filtro de contenido es una herramienta que analiza el tráfico web en busca de determinados patrones o categorías. Su objetivo principal es aplicar políticas de filtrado para controlar el acceso a ciertos tipos de contenido en línea. Esto puede incluir la prohibición de sitios web específicos, la restricción de ciertas categorías de contenido (como contenido para adultos o redes sociales) y la prevención de amenazas en línea al bloquear sitios maliciosos.

Figura 35. Web Proxy & Filter - Filtro desactivado



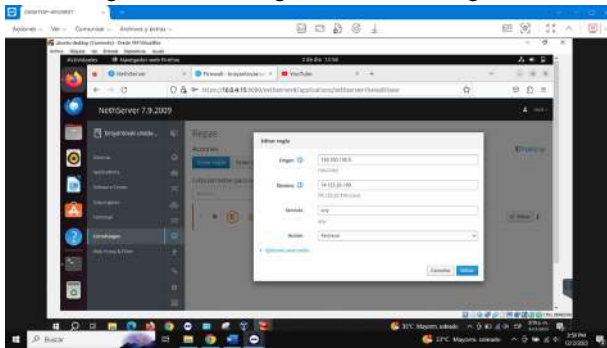
Fuente: Autoría propia

Figura 36. Web Proxy & Filter - Filtro



Fuente: Autoría propia

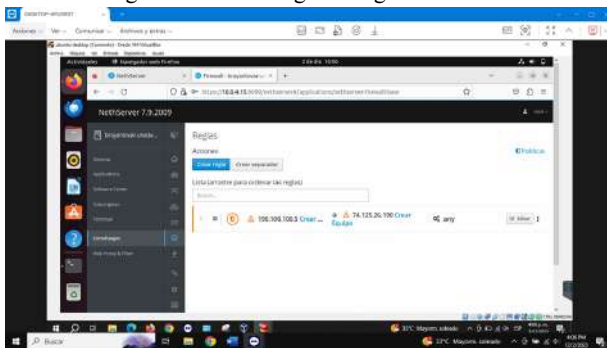
Figura 37. Cortafuegos - Creación de regla



Fuente: Autoría propia

El cortafuegos es una barrera de seguridad que regula el tráfico de datos entre la red interna y externa, protegiendo contra accesos no autorizados y amenazas cibernéticas al filtrar y controlar las comunicaciones.

Figura 38. Cortafuegos - Regla Creada

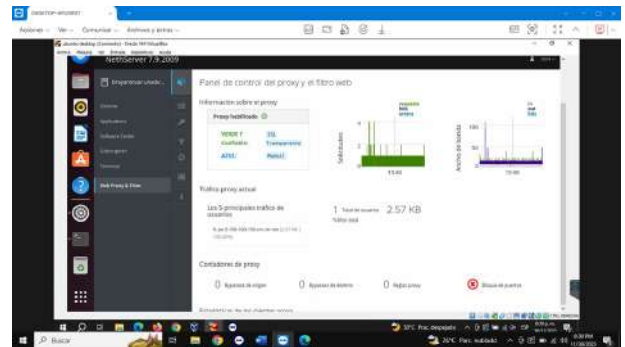


Fuente: Autoría propia

En esta fase, se está en la etapa final del desarrollo de la temática. Se han llevado a cabo los procedimientos esenciales que posibilitan la implementación de restricciones en el acceso a contenidos y portales web relacionados con entretenimiento y redes sociales.

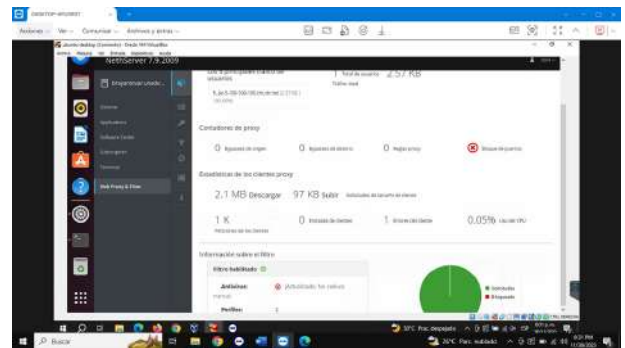
En este punto, se puede observar que las métricas y estadísticas ya han comenzado a registrar actividad.

Figura 39. Panel de Control de Web Proxy & Filter - Métricas



Fuente: Autoría propia

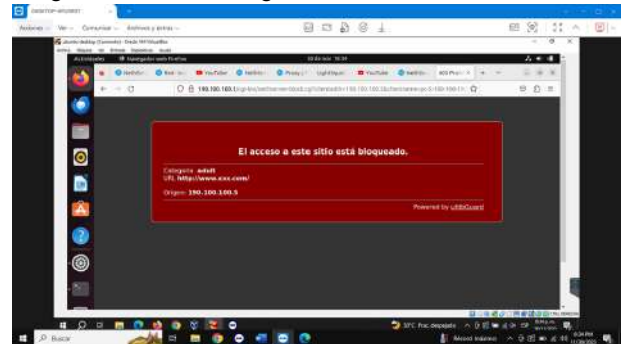
Figura 40. Panel de Control de Web Proxy & Filter - Métricas



Fuente: Autoría propia

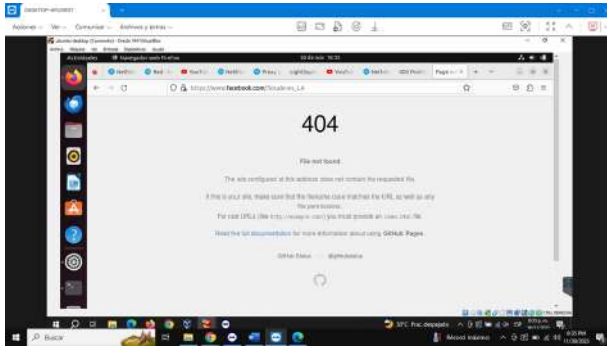
En pocas palabras, agregar un firewall en NethServer resultó ser muy importante para hacer más segura la red. Los resultados que se obtuvieron muestran claramente que mejoró la protección y el manejo de las comunicaciones. Cumplió eficazmente con las expectativas de tener un entorno más seguro y bajo control. Estos resultados confirman que instalar el cortafuegos en NethServer es una medida crucial para proteger la integridad del sistema.

Figura 41. Interfaz navegador - Restricción web exitosa



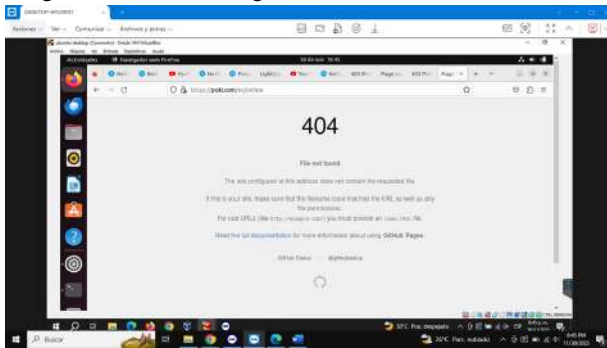
Fuente: Autoría propia

Figura 42. Interfaz navegador - Restricción web Exitoso



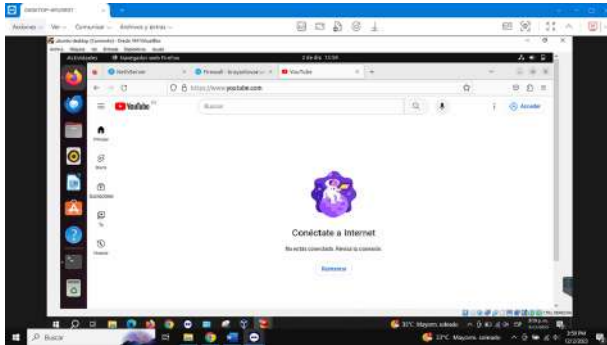
Fuente: Autoría propia

Figura 43. Interfaz navegador - Restricción web Exitoso



Fuente: Autoría propia

Figura 44. Interfaz navegador - Restricción web Exitoso

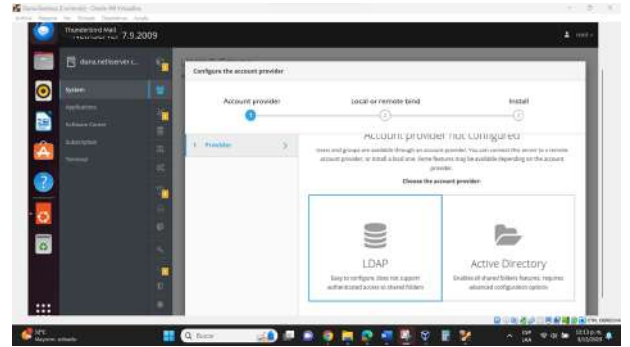


Fuente: Autoría propia

## 6 TEMÁTICA 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.

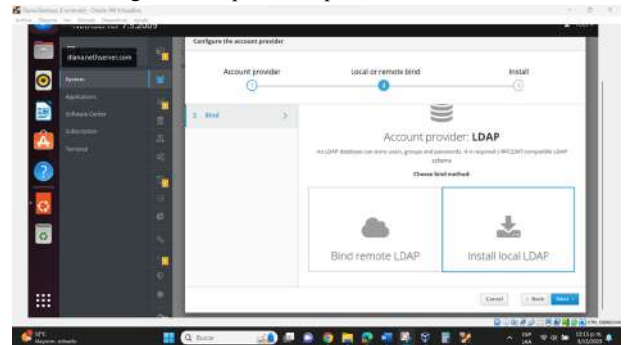
Figura 45. Menú opciones Usuarios y Grupos



Fuente: Autoría propia

Se ingresa a la opción Instalar LDAP, Luego de la instalación, se entra al módulo para gestionar usuarios y grupos. Panel de Usuarios y Grupos LDAP.

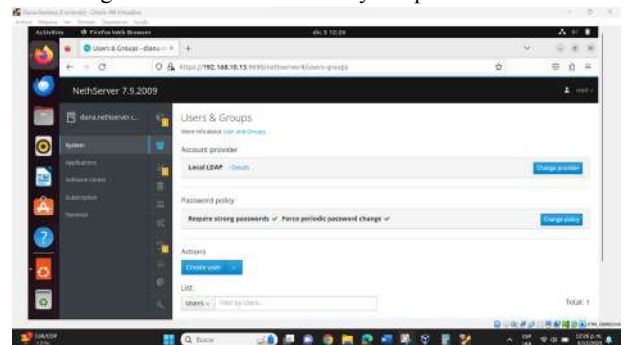
Figura 46. Opciones tipo de instalación



Fuente: Autoría propia

Luego de la instalación, se ingresa al módulo para gestionar usuarios y grupos. Panel de Usuarios y Grupos LDAP.

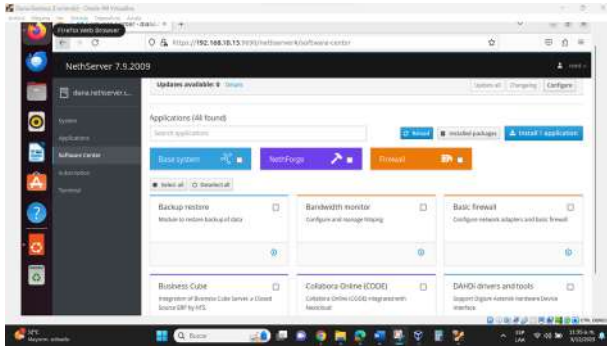
Figura 47. Panel de usuarios y Grupos LDAP



Fuente: Autoría propia

En el menú Software Center, se busca y se selecciona la aplicación de "File Server", luego se escoge la opción "Instalar aplicación", e inicia el proceso de descarga e instalación.

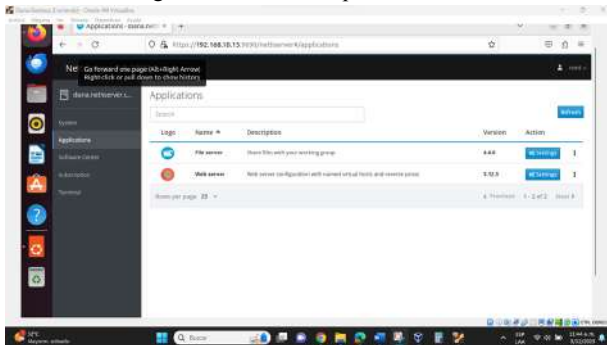
Figura 48. Panel Software Center



Fuente: Autoría propia

Al terminar la instalación se ingresa al módulo de “Aplicaciones” donde se observa la aplicación de “File Server”

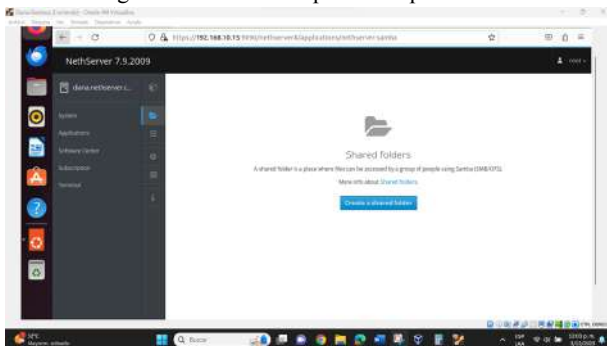
Figura 49. Panel de Aplicaciones



Fuente: Autoría propia

Se ingresa a los ajustes, luego al panel de configuración de “File Server”. En el submódulo carpetas compartidas.

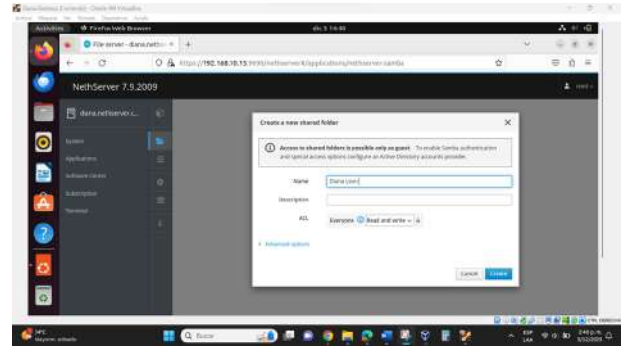
Figura 50. Módulo carpetas compartidas



Fuente: Autoría propia

Al ingresar al panel de configuración de “File Server”, en el submódulo carpetas compartidas, se crea la carpeta con el nombre “Diana Leon”

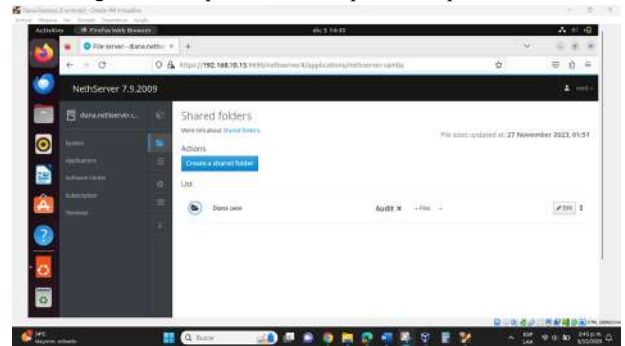
Figura 51. Configuración carpeta



Fuente: Autoría propia

En el submódulo de carpetas compartidas, se evidencia la creación de la carpeta.

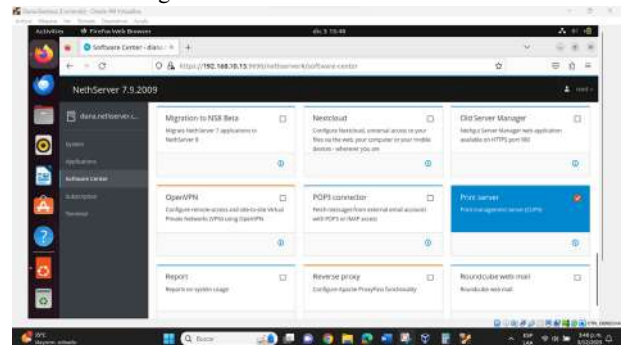
Figura 52. Explorador de carpetas compartidas



Fuente: Autoría propia

Se realiza el mismo proceso con la instalación del “File Server”, se ingresa a Software Center, se busca la aplicación “Print Server”

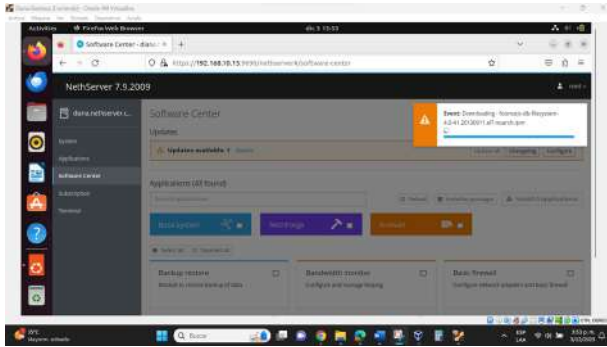
Figura 53. Panel Software Center



Fuente: Autoría propia

Se selecciona la opción instalar, se evidencia el proceso de descarga e instalación.

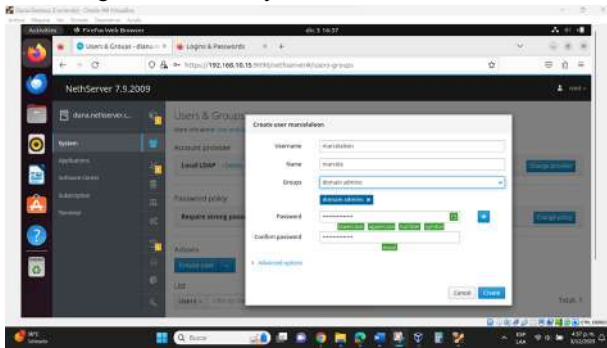
Figura 54. Instalación Print Server



Fuente: Autoría propia

En el módulo de Usuarios y Grupos, se crea el usuario “marcelaleon”, con su contraseña establecida.

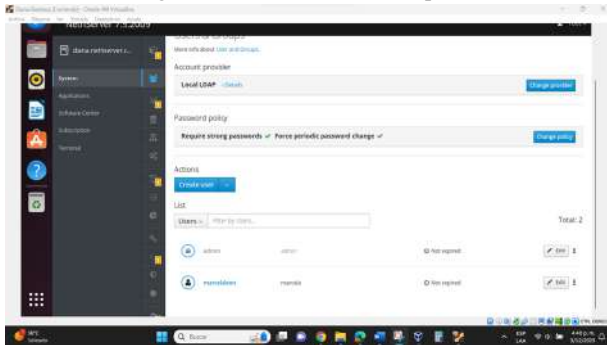
Figura 55. Usuario y credenciales de acceso.



Fuente: Autoría propia

En el módulo de Usuarios y Grupos, se evidencia la creación del usuario “marcelaleon”

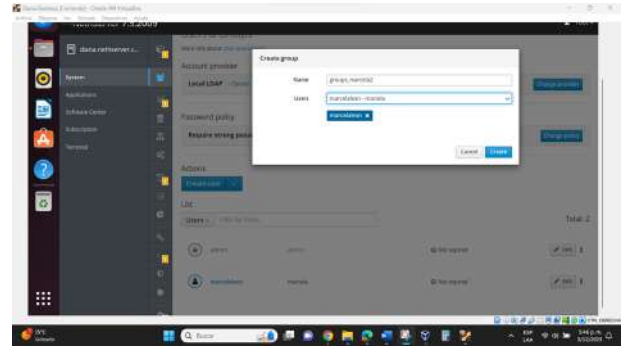
Figura 56. Panel User & Groups



Fuente: Autoría propia

En el módulo Usuarios y grupos, se crea el grupo llamado “groups\_marcela2”, se relaciona con el usuario “marcelaleon”

Figura 57. Configuración Grupo.



Fuente: Autoría propia.

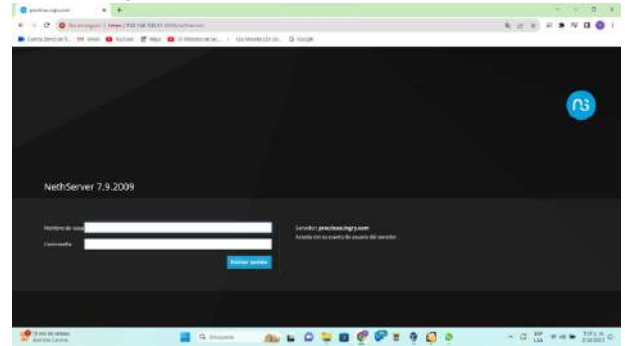
## 7 TEMÁTICA 5: VPN

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux.

En esta actividad se creó el servidor en plataforma NetServer, donde se realizó la configuración de la red (LAN, WAN, DMZ)

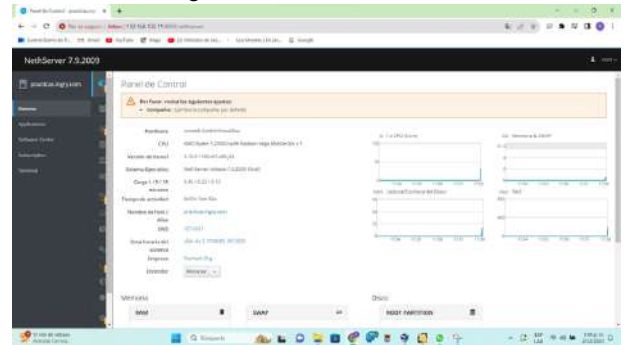
El primer paso es ingresar con el usuario y contraseña root para acceder inmediatamente al módulo del sistema, donde se visualiza el estado y las configuraciones.

Figura 58. Inicio de sesión en el servidor



Fuente: Autoría propia

Figura 59. Panel de control

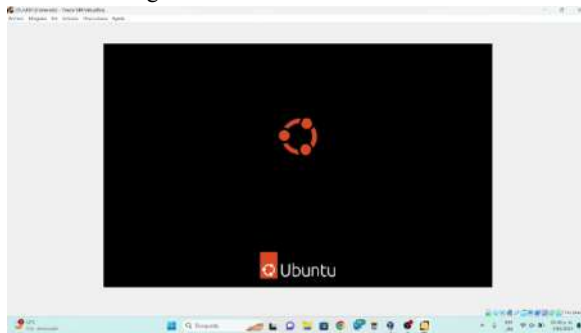


Fuente: Autoría propia

Se realiza la configuración de las redes para la conexión de los diferentes dispositivos, donde la red WAN (roja) 10.0.4.15/24 para que tenga acceso al internet. Posteriormente asignamos una IP y configuramos la red LAN (verde) 190.100.1/24.

Como se había instalado una máquina virtual en otras dos plataformas que se comportan como, los usuarios que se conectan al servidor, se inicia sesión en la máquina virtual Ubuntu con el acceso ya proporcionado, aquí actual el equipo como si estuviera conectada por una red local (LAN Verde).

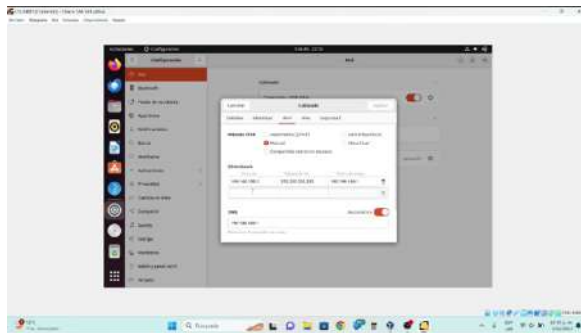
Figura 60. Inicio de sesión Ubuntu



Fuente: Autoría propia

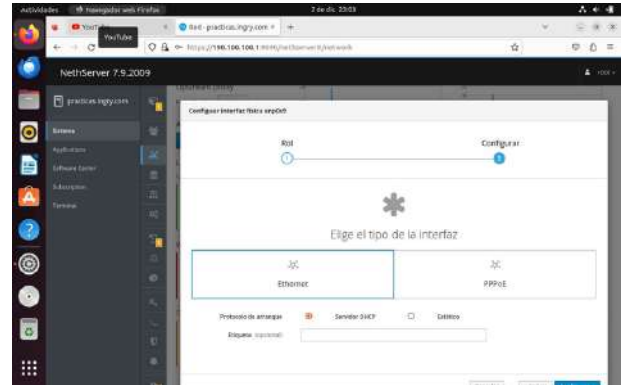
Aquí se da el acceso, con la IP fija y estática dentro de los rangos de la máscara de LAN Y WAN.

Figura 61. Configuración de la red en Ubuntu



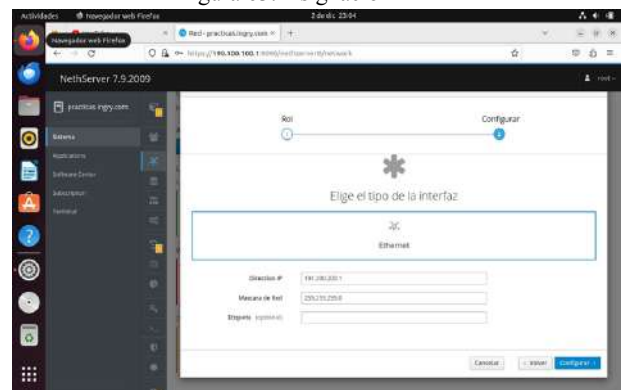
Fuente: Autoría propia

Figura 62. Configuración de WAN



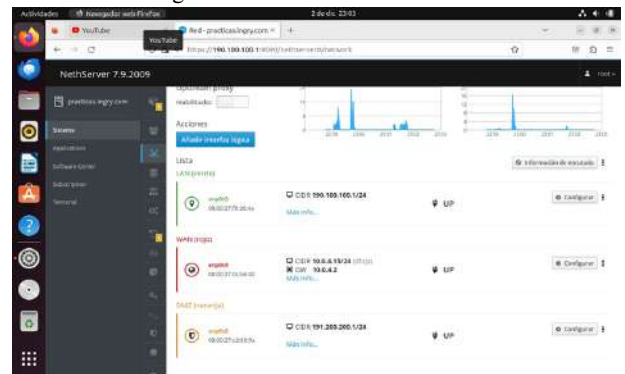
Fuente: Autoría propia

Figura 63. Asignación IP



Fuente: Autoría propia

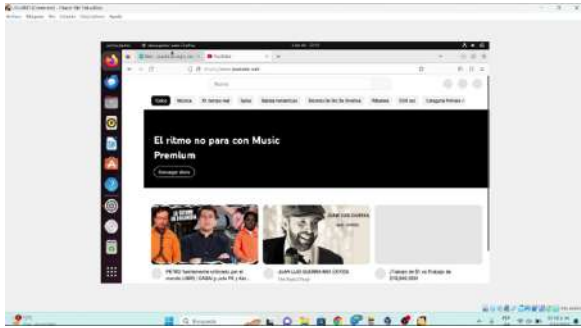
Figura 64. Conexión de la red.



Fuente: Autoría propia.

Se evidencia que tiene acceso a internet ingresando por el navegador.

Figura 65. Ingreso al navegador

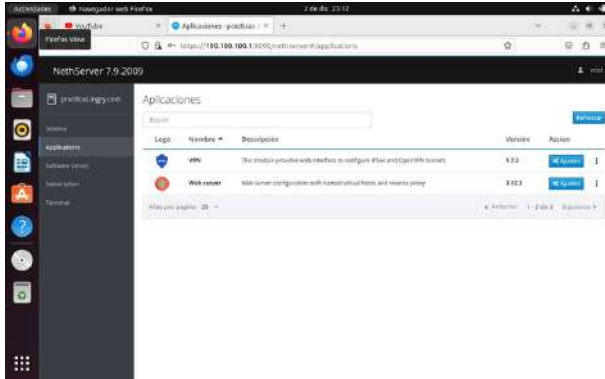


Fuente: Autoría propia

Este paso es muy importante, ya que cuando se ingrese a la máquina virtual sin importar la distribución identifique el equipo conectado a la red.

Para el siguiente paso se procederá a descargar y agregar las aplicaciones.

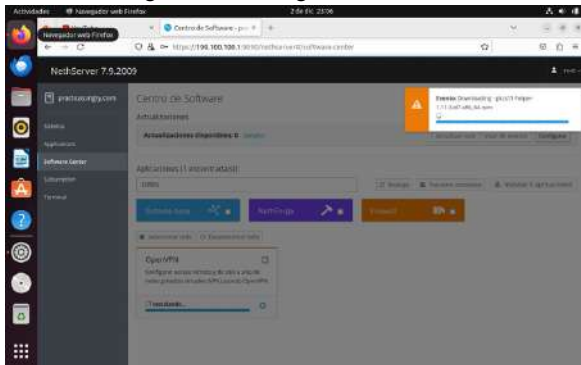
Figura 66. Aplicaciones



Fuente: Autoría propia

Aquí se descarga el paquete de configuraciones donde viene los certificados y por ende se carga el certificado en la aplicación OPENVPN.

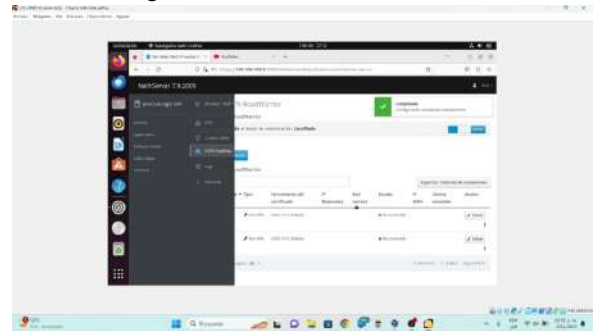
Figura 67. Descargar el certificado



Fuente: Autoría propia

Se evidencia la conexión del OPENVPN en la plataforma Ubuntu.

Figura 68. Conexión de OPENVPN



Fuente: Autoría propia

Para evidenciar que sirve en cualquier plataforma y/o sistema operativo, también se instaló en la máquina virtual Windows 10, se inicia sesión en la máquina virtual y procedemos a ingresar al servidor NethServer

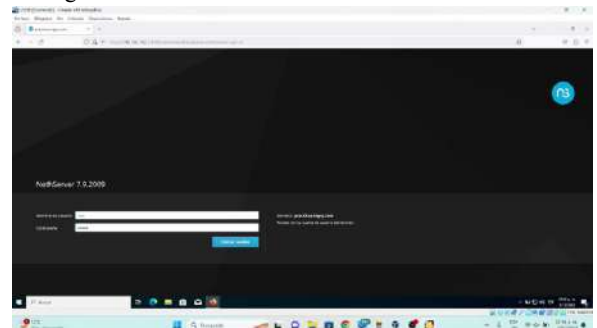
Figura 69. Inicio de sesión Windows 10



Fuente: Autoría propia

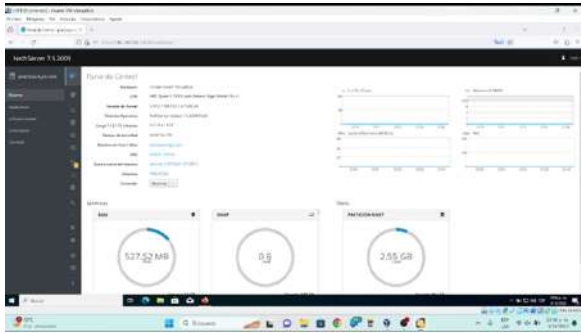
Se ingresa con el usuario root y se realiza la configuración por IP fija dentro del rango.

Figura 70. Inicio de sesión en el servidor NethServer



Fuente: Autoría propia

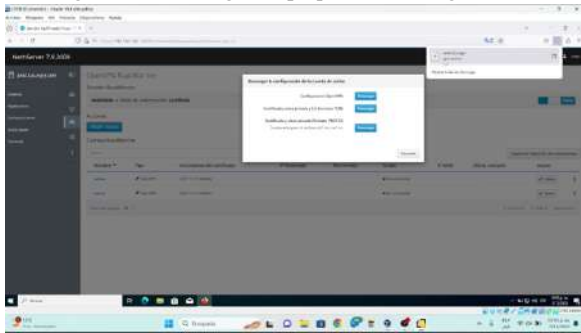
Figura 71. Panel de control del servidor



Fuente: Autoría propia

Aquí se procede a realizar la descarga del paquete de configuración donde incluye el certificado.

Figura 72. Descarga del paquete de configuración



Fuente: Autoría propia

Para el siguiente paso se procede a realizar la descarga e instalación de la aplicación “OPENVPN”

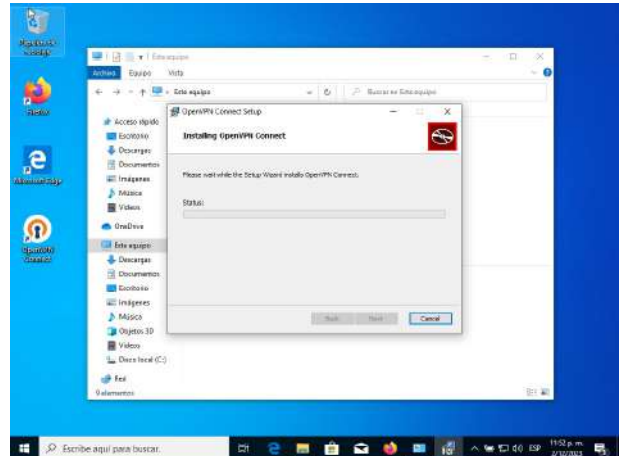
Figura 73. Descarga del OPENVPN



Fuente: Autoría propia

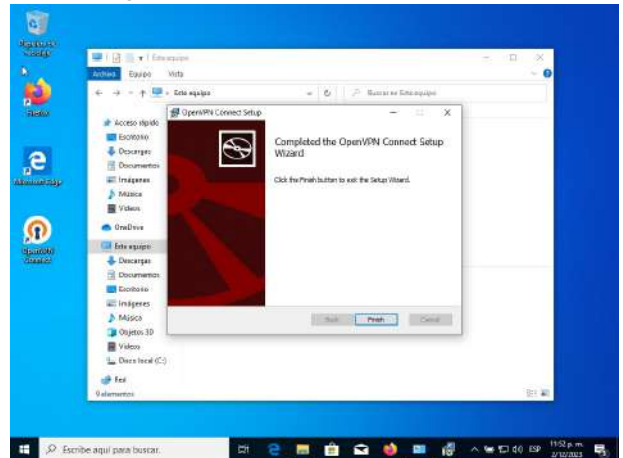
Después de la descarga se procede a instalar la aplicación.

Figura 74. Instalación de OPENVPN



Fuente: Autoría propia

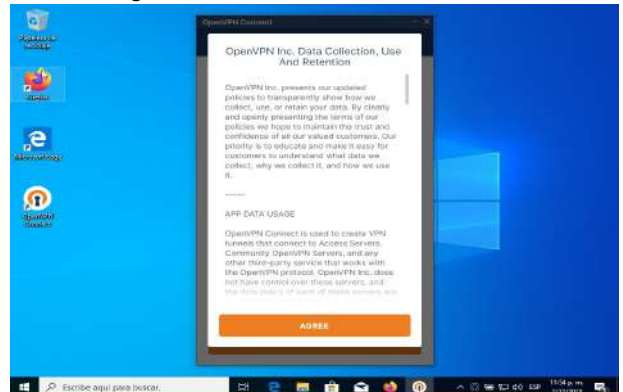
Figura 75. Finalización de la instalación



Fuente: Autoría propia

Una vez culminada la descarga y la configuración del servidor VPN y también se ejecutó la descarga del paquete que contiene los certificados necesarios para la conexión.

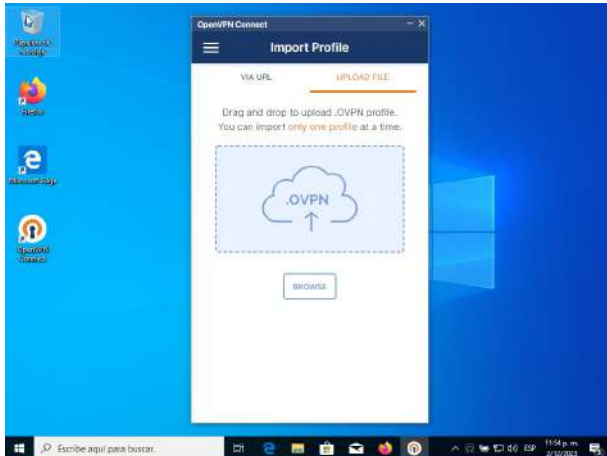
Figura 76. Inicio sesión de OPENVPN



Fuente: Autoría propia

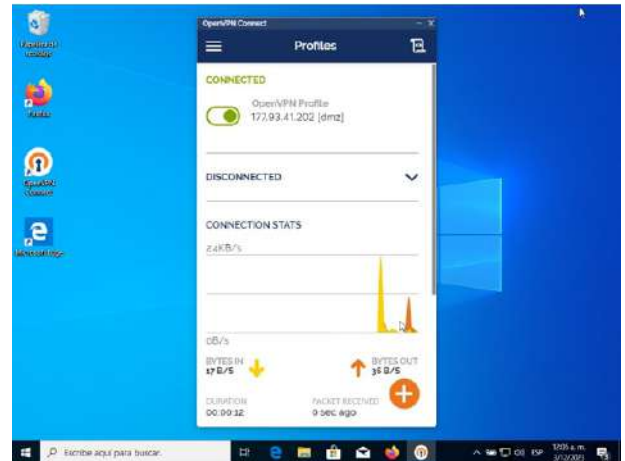
Como ya se tiene el certificado, se adjunta para que haya una conexión exitosa.

Figura 77. Importar el certificado



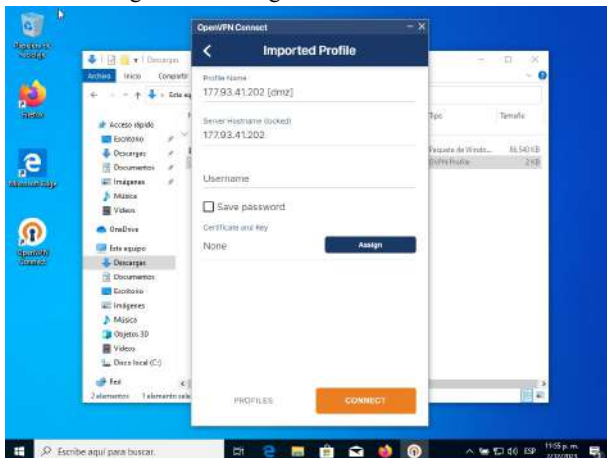
Fuente: Autoría propia

Figura 78. Conexión



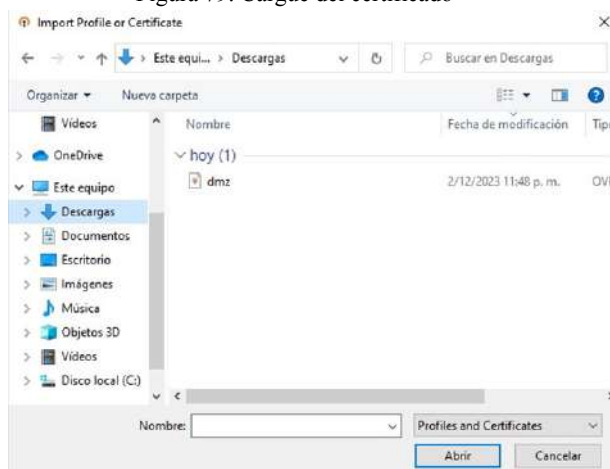
Fuente: Autoría propia

Figura 78. Configuración del servidor



Fuente: Autoría propia

Figura 79. Carga del certificado



Fuente: Autoría propia

## 8 CONCLUSIONES

La adopción de GNU/Linux NethServer para resolver necesidades específicas destaca por su eficacia y versatilidad. La combinación de la robustez de este sistema operativo con las funciones específicas de esta distribución ofrece una solución integral, proporcionando eficiencia, adaptabilidad y satisfacción precisa de los requerimientos particulares.

El uso de un cortafuegos o firewall en Nethserver es esencial para garantizar la seguridad de la red. Al implementar un firewall, se establece una barrera defensiva que controla el tráfico de red, protegiendo así los sistemas contra posibles amenazas externas. Además, facilita la administración de reglas para permitir o bloquear ciertos tipos de tráfico, brindando de esta forma un mayor control sobre la seguridad.

La implementación de un entorno de red eficaz está ligado a la configuración adecuada de servicios clave como el DHCP Server, DNS Server y el Controlador de Dominio, estos elementos en conjunto constituyen la columna vertebral de una infraestructura de red bien estructurada.

Un servidor Proxy garantiza la eficiencia para negar el ingreso a sitios con categorías que se ha escogido bloquear, muy útil para el ámbito educativo u organizaciones con estos requisitos.

Mediante la implementación y configuración, del controlador de dominio LDAP, el cual permite el acceso a los servicios de carpetas compartidas e impresoras, como resultado brinda seguridad a la información almacenada.

Se evidenció en esta actividad que la implementación del VPN es una de las mejores herramientas, ya que transmite los datos de las redes públicas de forma anónima y segura porque oculta las direcciones IP, como también realiza un cifrado de datos para que el que no esté autorizado no los visualiza.

## 9 REFERENCIAS

- [1] Caballero, M. C. [@DriveMeca]. (2018, octubre 22). *Nethserver Tutorial 🔥 | Configurando DHCP Server*. Youtube. <https://www.youtube.com/watch?v=GrvZutNZIRg>
- [2] Lab Virtuales Servidores. (2023, 12 de octubre). *Instalar #NethServer + Configurar Web Proxy & Filtrar Contenidos Web*. [video]. Youtube. <https://youtu.be/cIHJbtTehKg?si=us42cKe-zq4DXNjk>
- [3] Sistemas Italianos. (2020, 14 de marzo). *Centos. OpenVPN Server con NethServer e LDAP*. [video]. Youtube. <https://youtu.be/3Fv11F93Jac?si=ZWH307iyP89ihxCM>
- [4] Fandiño, B. (2023, 29 de noviembre). *Zonas de Red en NethServer*. [video]. Youtube. <https://youtu.be/KoluHFwFiOY?si=lpjinEUpiGn0BTIm>
- [5] Antonio J. (2020, 14 de marzo). *NethServer | Configuración e instalación de aplicaciones*. [video]. Youtube. <https://www.youtube.com/watch?v=aNAbGaayx2Y&t=1037s>