SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Jaime Alberto Sánchez Tabares
jasanchezta@unadvirtual.edu.co
Diana Maria Loaiza Garcia
dmloaizaga@unadvirtual.edu.co
Luis Felipe Maturana Vergara
lfmaturanav@unadvirtual.edu.co
Federico Murillo Murillo
fmurillomu@unadvirtual.edu.co
Alexandra Salazar Zuluaga
asalazarz@unadvirtual.edu.co

RESUMEN: *La migración a sistemas operativos basados en GNU/Linux y la consolidación de servicios críticos para la infraestructura IT representan una etapa crucial en la transición tecnológica de entornos organizacionales complejos. Este proyecto aborda la fase final de dicha migración, donde estudiantes deben implementar servicios avanzados utilizando Nethserver, una distribución basada en GNU/Linux diseñada para gestionar infraestructura IT en redes Intranet y Extranet. Cada participante selecciona y desarrolla una temática específica, que abarca servicios esenciales para la gestión de redes y seguridad, con énfasis en configuraciones detalladas y documentación técnica. Los resultados de cada temática incluyen procedimientos paso a paso y evidencias prácticas, tales como capturas de pantalla, configuraciones y validaciones de funcionamiento. Este enfoque fomenta la aplicación de conocimientos adquiridos previamente, como la definición de zonas DMZ para la segmentación de redes, garantizando una implementación robusta y segura de servicios IT en infraestructuras complejas.*

PALABRAS CLAVE: GNU/Linux, Infraestructura IT, Nethserver, Servicios de red, LDAP.

1 INTRODUCCIÓN

En el paso final del diplomado de profundización en administración de sistemas operativos Open Source GNU/Linux, se han estudiado las temáticas relacionadas con la administración y puesta en marcha de una distribución basada en CentOS de Red Hat enfocada a la implementación de servicios de infraestructura IT.

EL presente artículo contiene el informe de los resultados obtenidos de la implementación del sistema operativo GNU/Linux nethserver, el cual corresponde a una distribución de servidor que cuenta con varios módulos que permiten diferentes funcionalidades enfocadas a la administración de servicios de mayor nivel para Intranet y Extranet por medio de la configuración de puertos e interfaces.

Algunas de las funcionalidades otorgadas por el nethserver, son la posibilidad de implementar cortafuegos, servidores DHCP, servicios de Proxy, servidores de archivos e impresoras y servicios de VPN.

En este documento en particular se encuentra la documentación de la instalación y puesta en marcha de Nethserver y cinco servicios, los cuales se implementan con su respectiva configuración de zona verde (LAN), que a su vez se conectará a una red WAN a través del servidor NethServer con el propósito de conectar y controlar por medio de este el tráfico y acceso a las redes LAN y WAN.

2 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR NETHSERVER

Si bien la instalación del servidor Nethserver, es responsabilidad de cada uno de los estudiantes para poder realizar la temática seleccionada, se presenta a continuación un resumen consolidado del procedimiento para la instalación y configuración.

El primer paso para poner en marcha el servidor es la descarga de la imágen iso desde el sitio oficial de nethserver, posterior a esto se realiza la creación de una máquina virtual con las especificaciones técnicas recomendadas por el distribuidor de la distribución así:

- Memoria RAM de 2048 MB
- Procesadores - 2
- Imágen de disco 50 GB reserva dinámica
- Unidad óptica para montaje de imágen ISO
- 2 Tarjetas de red habilitadas así
    - Adaptador 1 conexión NAT
    - Adaptador 2 Red interna (Verde)

Una vez se ha creado la máquina virtual con los parámetros recomendados, se procede a montar la imágen ISO previamente descargada en la unidad óptica de la máquina virtual y se enciende la máquina para dar comienzo a la instalación del sistema operativo.

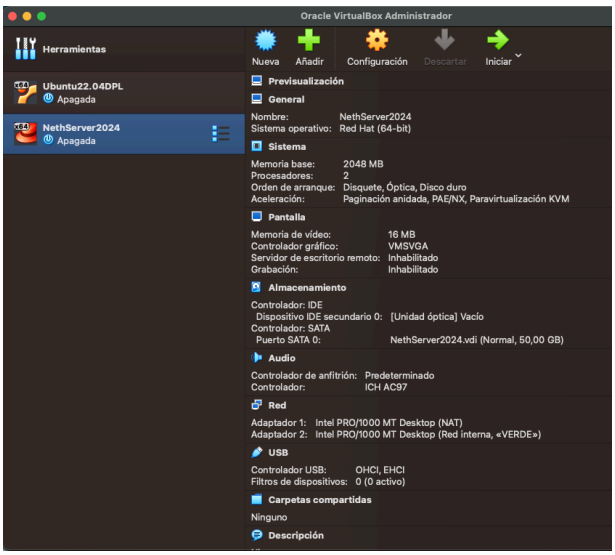

Figura 1. Creación de máquina virtual creada con los parámetros antes definidos y la configuración de sus dos tarjetas de red.

Una vez creada la máquina virtual, se da inicio al sistema para la instalación del SO.

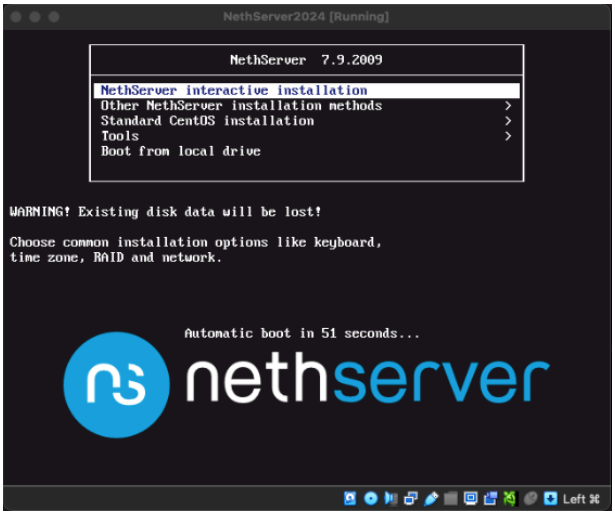

Figura 2. Inicio del proceso de instalación.

Durante el proceso de instalación se debe configurar la zona horaria, la distribución del teclado y las tarjetas de red.

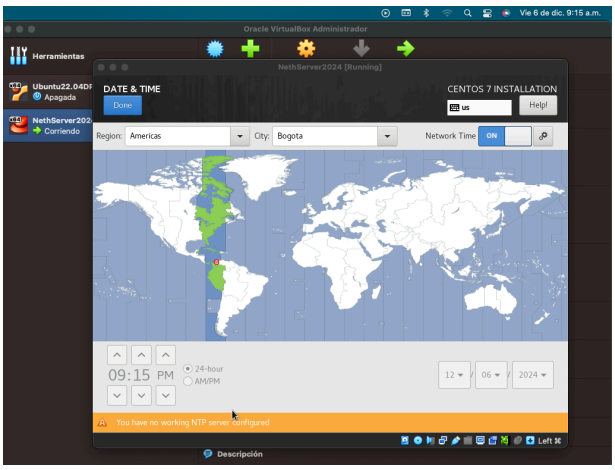

Figura 3. Configuración zona horaria.

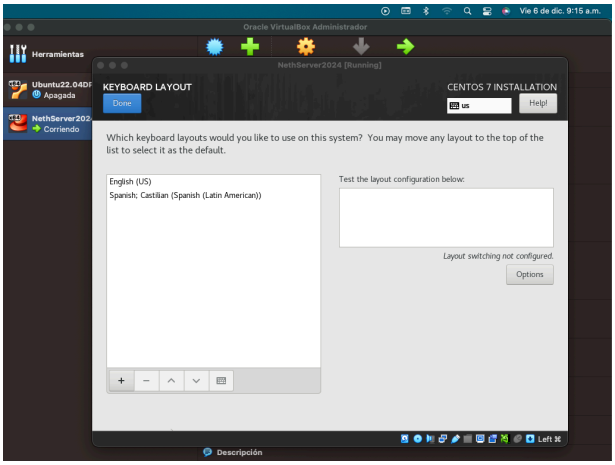

Figura 4. Configuración distribución de teclado.

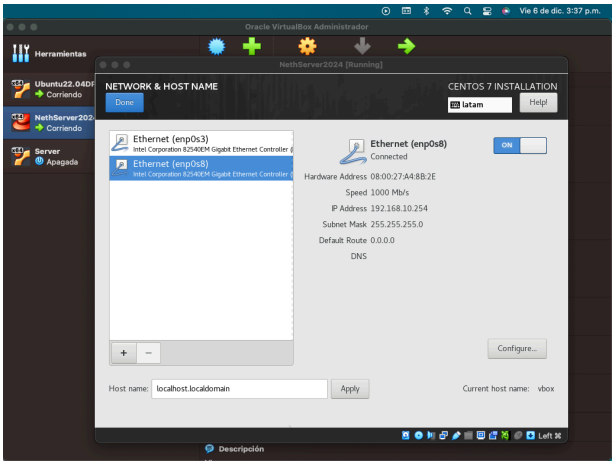

Figura 5. Configuración de las tarjetas de red.

Es importante mencionar que la tarjeta de red enp0s3 al estar configurada como red NAT, obtiene automáticamente su direccionamiento, mientras que la tarjeta de red enp0s8 debe ser configurada con una ipv4 manual que hará las veces de red LAN o zona Verde.

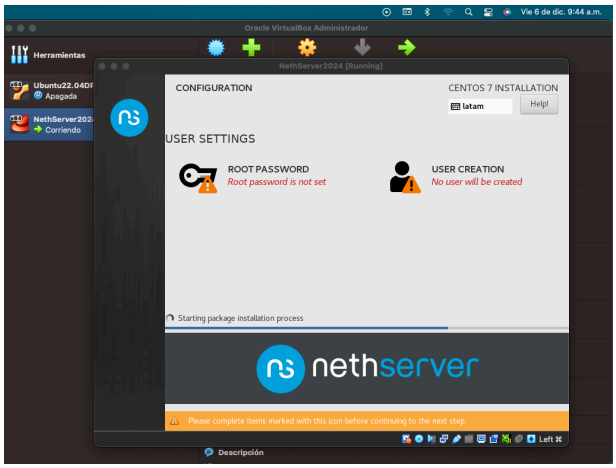

Figura 6.Configuración de contraseña para usuario root y configuración de usuario del sistema con su respectiva contraseña.

Una vez se da inicio a la instalación, el sistema pide definir una contraseña para el usuario root y la crear un usuario del sistema con su respectiva contraseña.

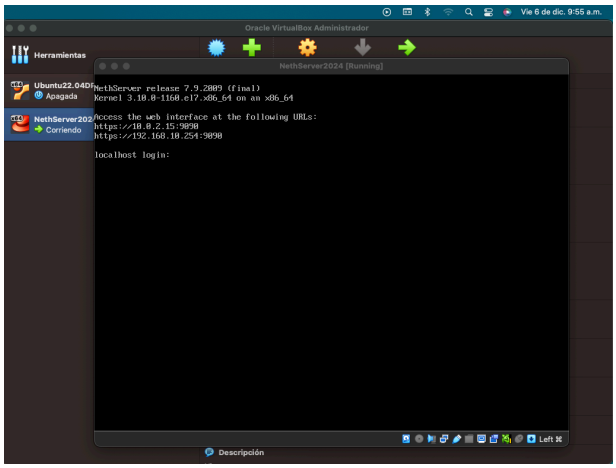

Figura 7. Finalización de la instalación.

Terminado el proceso de instalación, el sistema muestra la consola del servidor, además de el direccionamiento ip que debemos utilizar para el acceso al servidor por medio de interface web.

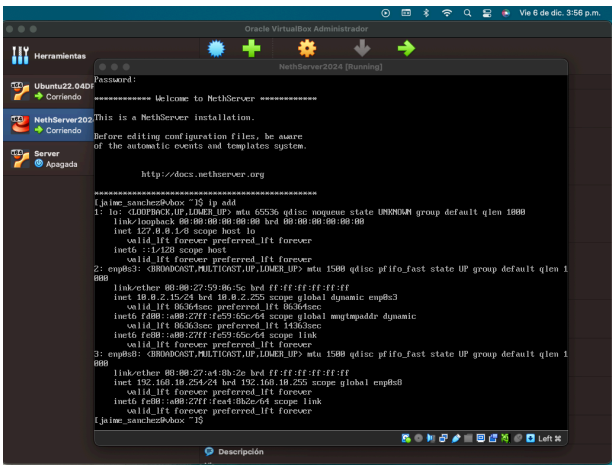

Figura 8. Comprobación de tarjetas de red.

Para garantizar que el server se ha configurado de forma adecuada, lanzamos un comando ip address para confirmar que las dos tarjetas se han habilitado y cuentan con asignación ip.

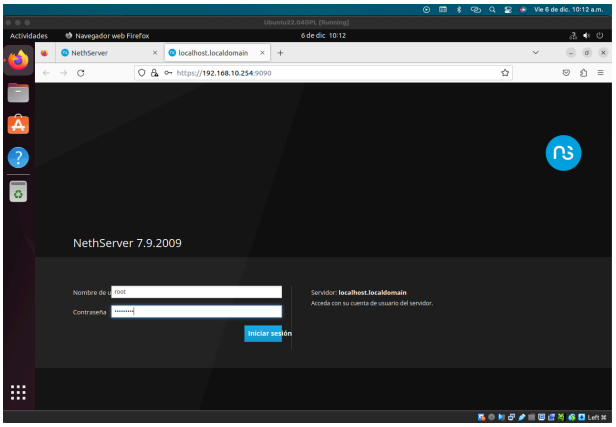

Figura 9. Conexión al server vía interface web desde el equipo cliente en la red LAN.

Finalizada la instalación accedemos al servidor vía interface web desde un equipo desktop conectado a la red interna del server por medio de la ip asignada a la red interna o zona Verde del mismo.

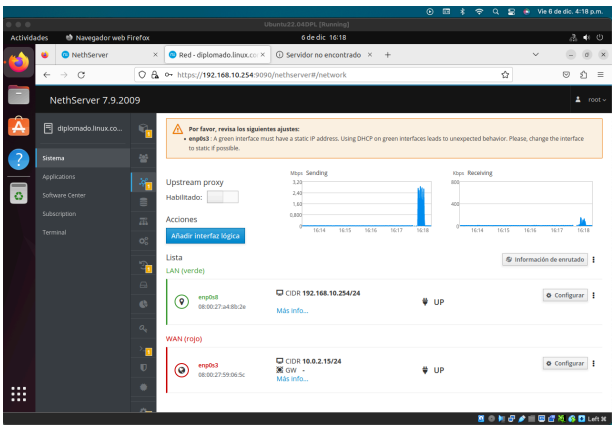

Figura 10. Configuración de tarjetas de red.

Ya dentro del dashboard del Nethserver, se deben configurar las tarjetas de red, la enp0s3 se debe cambiar a zona Roja y asignarle una puerta de enlace, mientras que a la enp0s8 solo hay que asignarle la puerta de enlace.

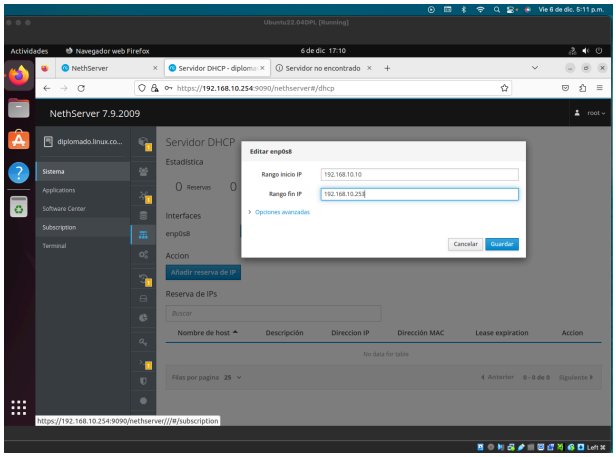

Figura 11. Configuración del servidor DHCP.

Finalmente se habilita el servidor DHCP y se le asigna un rango de direcciones ipv4 para ser asignadas de forma automática a los clientes de la red LAN.

Concluidos los pasos anteriores se tiene un servidor perfectamente configurado para continuar con el desarrollo de cada una de las temáticas solicitadas.

3 SERVICIOS CONFIGURADOS

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

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Para la instalación y configuración del servidor DHCP se ingresa por el panel de control de NethServer en el módulo de Sistema – Servidor DHCP, se habilita el enp0s8 y se realiza la asignación de rangos de direcciones IP.

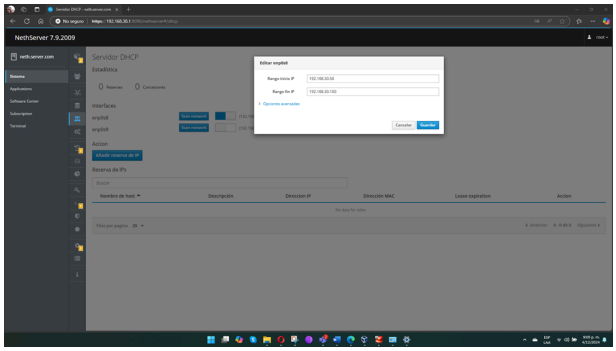

Figura 12. Asignación de rangos para la red verde del servidor DCHP.

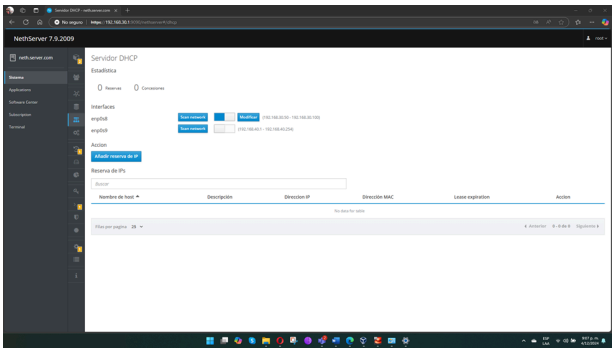

Figura 13. Captura luego de la asignación de rangos para la red verde

Se ingresa al sistema operativo Ubuntu para mirar la dirección IP, debe ser la misma de enp0s3.

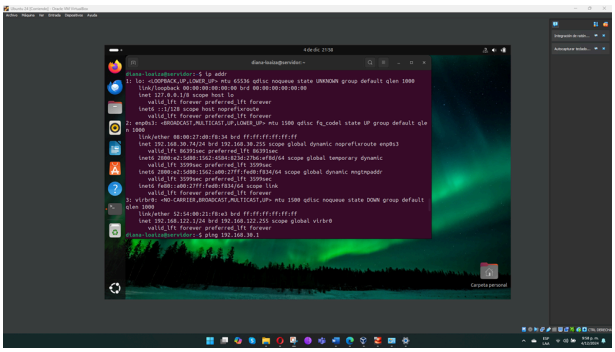

Figura 14. Captura de pantalla para validar la dirección IP de Ubuntu

Por último, se valida que se vea el equipo conectado en NethServer.

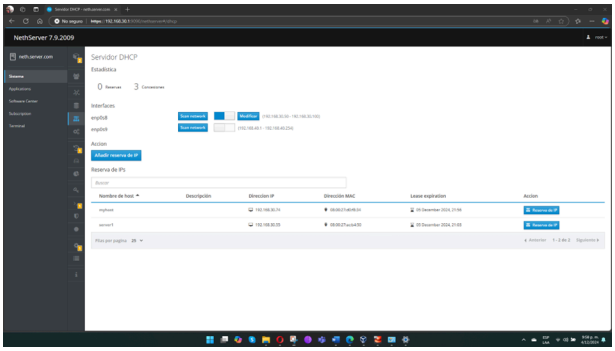

Figura 15. Captura de pantalla donde se muestra la máquina conectada

Para realizar la parametrización del DNS se ingresa por el panel de control de NethServer en el módulo de Sistema – DNS. En este caso, lo que se busca es decirle al equipo cliente con qué dirección IP se resuelve un nombre de dominio. Para este ejercicio se crea el dominio www.dimaloga.com y que salga con la dirección IP 192.168.30.1.

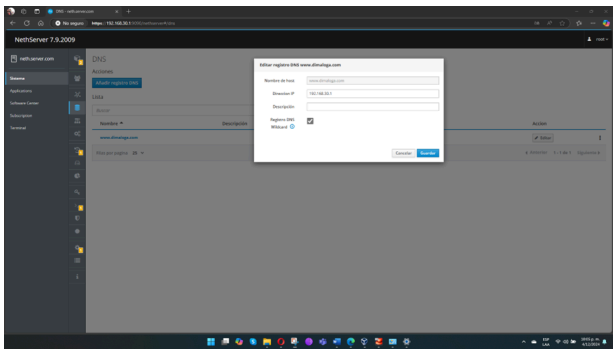

Figura 16. Captura de pantalla del registro para DNS en NethServer

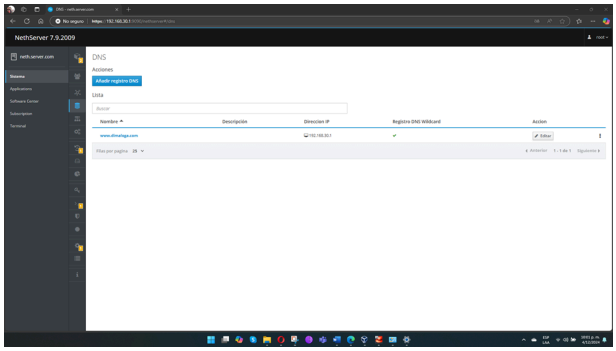

Figura 17. Captura de pantalla del nombre y dirección IP asignados del DNS

Se ingresa por la terminal de Ubuntu para validar el ping del dominio y se evidencia conexión.

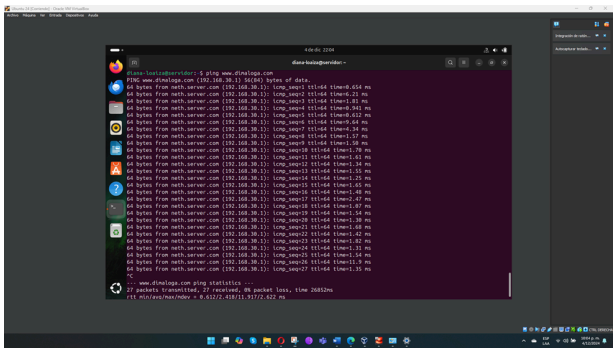

Figura 18. Captura de pantalla evidenciando ping en el dominio

3.2 PROXY

Implementación y configuración detallada del control de acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Nethserver a través de un proxy que filtra la salida por medio del puerto 3128.

El servidor proxy web se encuentra entre los clientes LAN e internet y desde allí se filtra el contenido web configurado por el administrador IT.

Se accede desde equipo desktop CentOS 9 al servidor NethServer a través de navegador web con la ip del servidor y el puerto 9090.

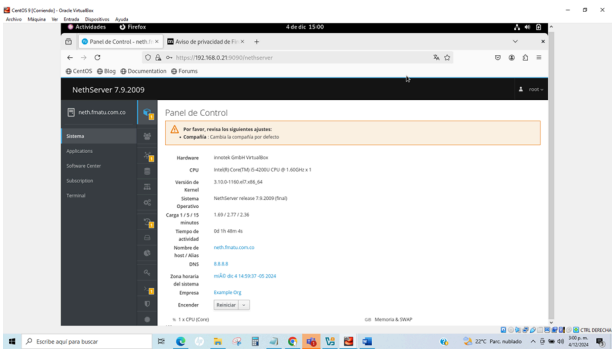

Figura 19. Acceso a NethServer

Se realiza la configuración de red con ip estática desde NethServer para la zona verde (LAN) y se descarga en la opción Software Center las aplicaciones Web Proxy & Filter, Web Server y Firewall. El proxy solo se puede configurar en zona verde y zona azul (invitados).

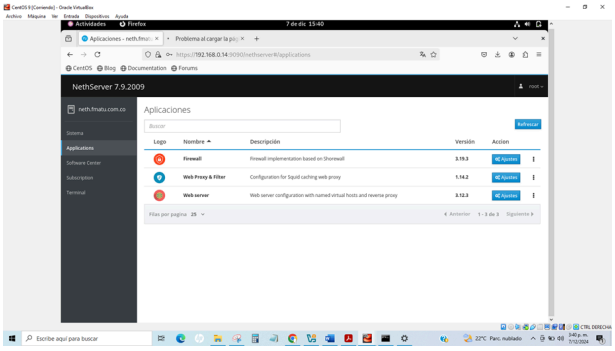

Figura 20. Instalación de aplicaciones.

Se habilita proxy desde la aplicación Web Proxy & Filter.

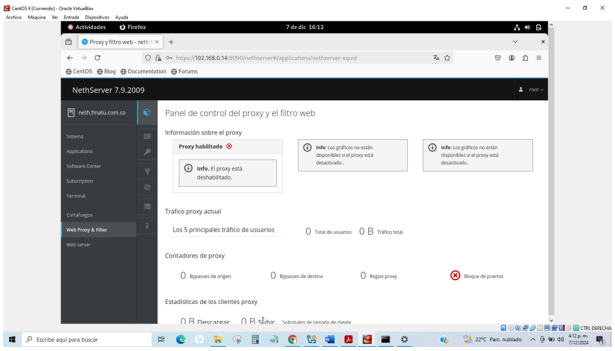

Figura 21. Panel de Control Web Proxy & Filter.

Se configura modo de las respectivas zonas. Modo SSL Transparente para la zona verde y obligar a todos los clientes a pasar por el proxy para las conexiones HTTP y HTTPS. Y para la zona azul configuramos el modo Manual para configurar manualmente todos los clientes. Adicionalmente se configura el puerto 3128 para filtrar la salida de tráfico web.

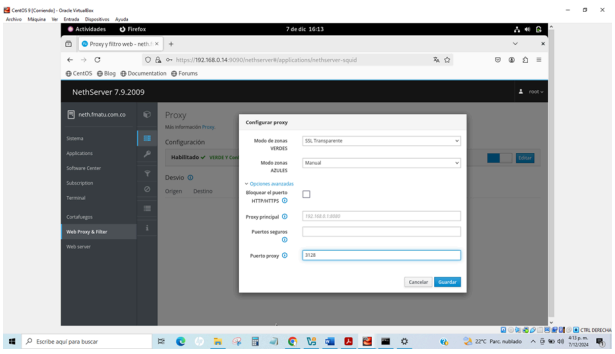

Figura 22. Configuración de modos y puertos.

Se activan opciones globales de filtro para las listas negras y las listas blancas desde la opción Filtro, con el fin de ubicar las direcciones y/o contenido web a bloquear o no.

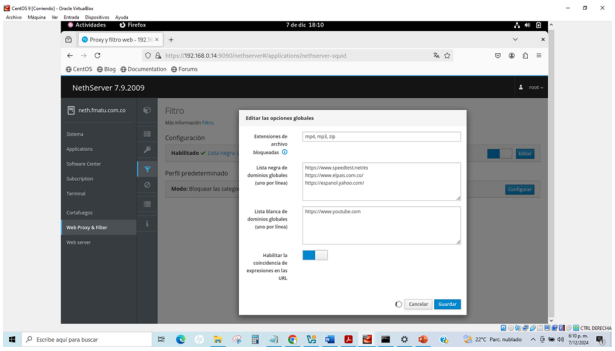

Figura 23. Configuración listas negras y blancas

Se configura el bloqueo del contenido web para las respectivas páginas web relacionadas con anterioridad.

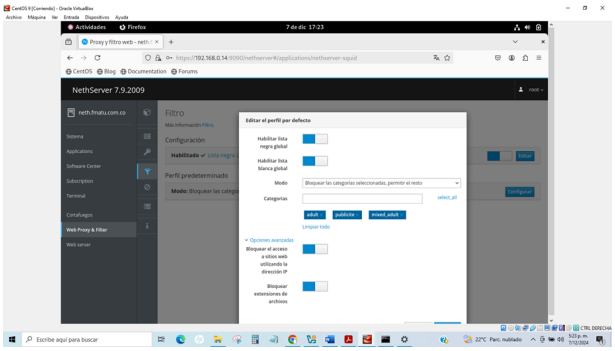

Figura 24. Configuración de contenido web.

En navegador web Mozilla Firefox se accede a la página https://www.speedtest.net/es evidenciando gran cantidad de publicidad.

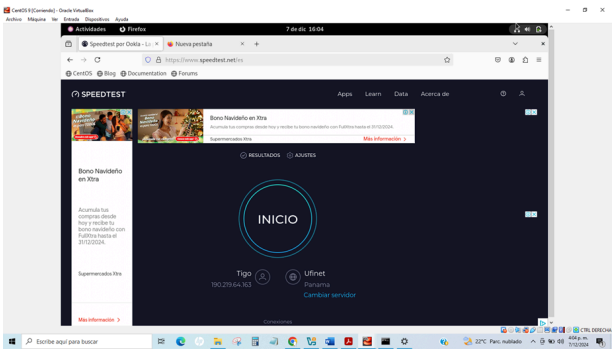

Figura 26. Página web sin proxy habilitado.

Desde el cliente se configura proxy HTTP y puerto manualmente en el navegador web Mozilla Firefox.

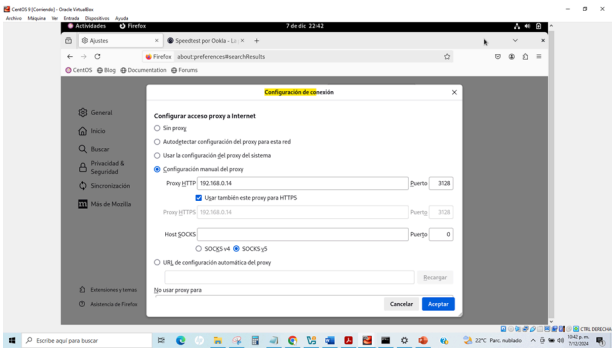

Figura 27. Configuración proxy del navegador web cliente.

Se valida bloqueo de publicidad en página web https://www.speedtest.net/es

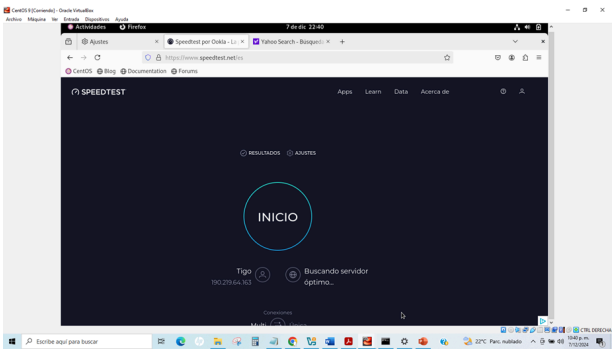

Figura 28. Página web con proxy habilitado.

3.3 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.

Cuando se utilizan cortafuegos para el filtrado de contenido web, se debe tener en cuenta que se requiere definir un conjunto de reglas o instrucciones basadas en direccionamiento de origen, puertos de comunicación, destino

del tráfico y acciones a tomar con las solicitudes, ya que a diferencia de los filtrados por proxy donde el filtrado de los contenidos se realiza por categorización de contenidos, la restricción del tráfico en los firewall, se concibe o gesta en reglas aplicables al direccionamiento.

Teniendo en cuenta lo recién mencionado, se puede resumir, que el filtrado de acceso a ciertos sitios de internet desde una red LAN administrada por un servidor con cortafuegos, se logra gracias a la creación de reglas de firewall en las cuales se debe considerar, la correcta configuración de la red LAN entre servidor y clientes, las zonas y sentido del tráfico, el origen de las solicitudes, los puertos a intervenir y las ip de destino.

Para la creación de las reglas restrictivas, las direcciones ip destino son uno de los parámetros más importantes, ya que se hace necesario tener plenamente identificadas todas las ip que apuntan al sitio objeto de ser bloqueado.

Una vez se han aclarado los puntos anteriores, y habiendo instalado el sistema operativo Nethserver en una máquina virtual y de haber configurado la red correctamente, según lo descrito en el apartado número 2 del presente artículo, se procede a realizar la instalación y configuración del cortafuegos.

Antes de realizar la instalación y configuración del cortafuegos como control de acceso a internet por parte de los clientes de la red LAN, se debe verificar la conectividad de la tarjeta de red del equipo o equipos de la red con respecto a la configuración de las tarjetas de red del servidor NetServer definidas en el apartado 2 del presente artículo y que coincide con la segmentación consultada en el Dashboard del equipo servidor y que se muestra a continuación.

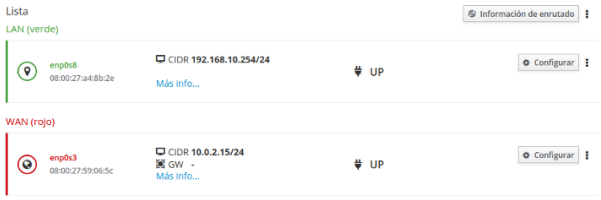

Figura 29. Configuración de tarjetas de red en el servidor.

Los equipos cliente, deben configurarse dentro de la red interna LAN o zona Verde de la red y deben utilizar como Default Gateway la misma ip asignada a la tarjeta de red LAN del servidor; la siguiente imágen da muestra de la configuración de la tarjeta de red en un cliente de la red interna LAN, esta configuración de direccionamiento se logra de forma automática por medio de un servidor DHCP configurado con anterioridad en el servidor.

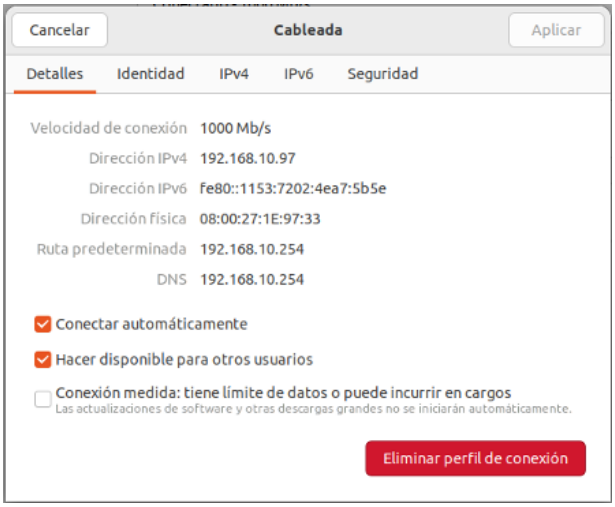

Figura 30. Configuración de tarjeta de red en equipo cliente.

Una vez se ha confirmado la correcta configuración y conexión entre cliente servidor, se procede a ingresar al dashboard del nethserver por medio de una conexión de interface web y realizar la instalación de la aplicación firewall desde el centro de software, para llevar a cabo la instalación, se debe identificar el aplicativo a instalar, seleccionarlo y dar click en el botón instalar, este proceso se realiza de forma automática; una vez se ha completado el proceso de instalación, veremos la aplicación en la sección de aplicaciones disponible para ser utilizada, ver Figuras # y #

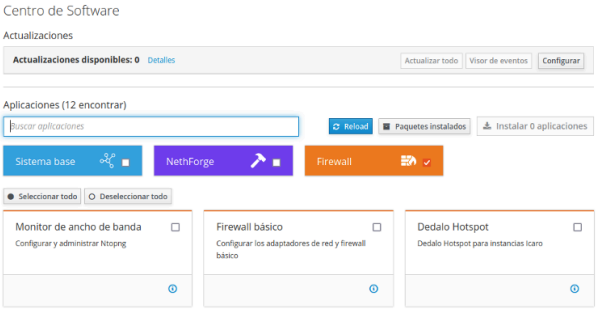

Figura 31. Centro de software.

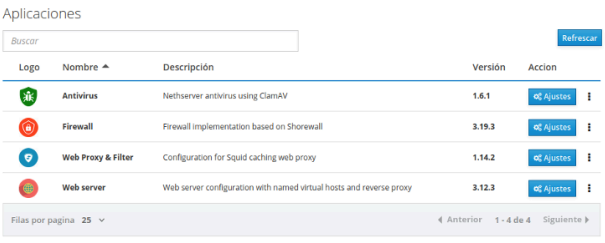

Figura 32. Aplicaciones.

Después de instalada la aplicación de firewall, se puede proceder a ingresar a su panel de control, para esto solo se debe dar click en el botón configurar que se encuentra al lado derecho de la aplicación.

Dentro del firewall se encuentra un menú de información y herramientas para la configuración bastante amplio, en la primera pestaña por ejemplo, nos encontramos con una ilustración de la topología de red; esta ilustración muestra el cortafuegos como un filtro del tráfico entre las redes LAN y WAN.

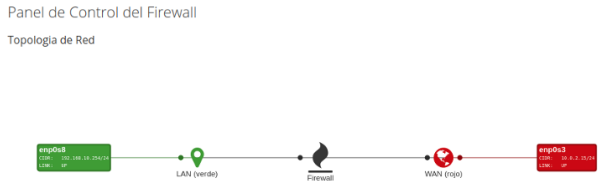

Figura 33. Topología de red.

Después de verificada la topología de red, se debe validar que el tráfico hacia internet, ping desde internet y la puerta de enlace de la capa de aplicación (ALG) se encuentren habilitadas.

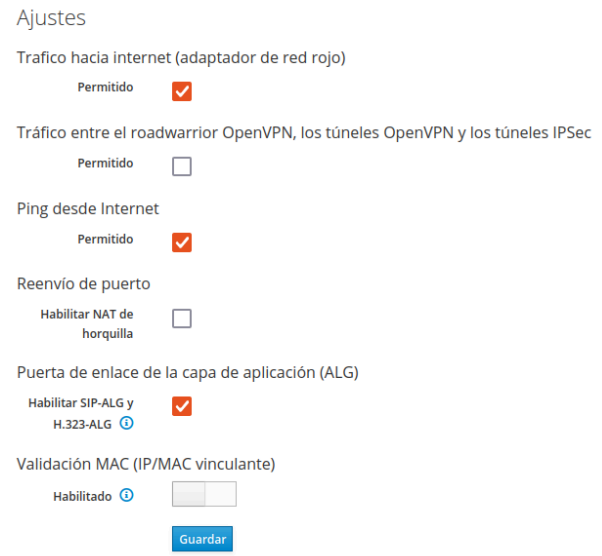

Figura 34. Ajustes de firewall.

Confirmado lo anterior se puede proceder con la configuración del control restrictivo de tráfico o solicitudes desde la red LAN hacia la WAN a los servicios de internet relacionados con redes sociales y de entretenimiento por medio de la implementación de reglas restrictivas en el módulo REGLAS del panel de control del cortafuegos.

Las reglas mencionadas, son un conjunto de parámetros ajustables en el firewall y que le indican al servidor las conexiones o solicitudes aceptadas, rechazadas o denegadas; estas reglas en resumen identifican el origen de las solicitudes, el destino, los puertos que intervienen y las acciones que el firewall debe tomar con respecto a cada solicitud.

Antes de pasar a la configuración de reglas restrictivas para un par de sitios de redes sociales y a manera de conclusión, podemos decir que el método para restringir el acceso a determinada página de internet requiere la creación de una regla en la cual se rechace toda solicitud proveniente de un equipo cliente x y que vaya dirigida hacia cierta ip de un sitio web con determinada ip, por lo que se hace necesario conocer todas las ip que apunten a un sitio para poder crear la regla.

A continuación se presentan dos ejemplos prácticos de restricción de acceso a las redes sociales Facebook e Instagram.

Para conocer las direcciones ip que apuntan a los sitios objeto de ser bloqueados,, se debe consultar estas por medio de un comando ping o nslookup directamente en la consola del servidor o de cualquier equipo con acceso a internet.

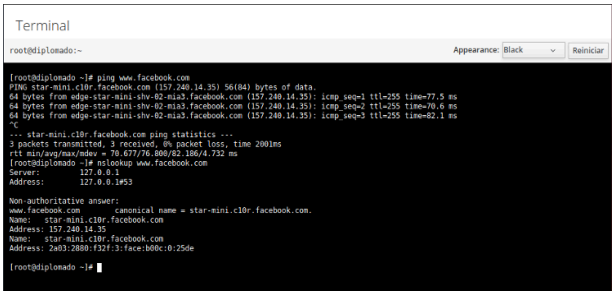

Figura 35. Comando ping y nslookup a www.facebook.com.

Se ejecutan los comandos ping y nslookup a la url de facebook y se toma nota de las ip.

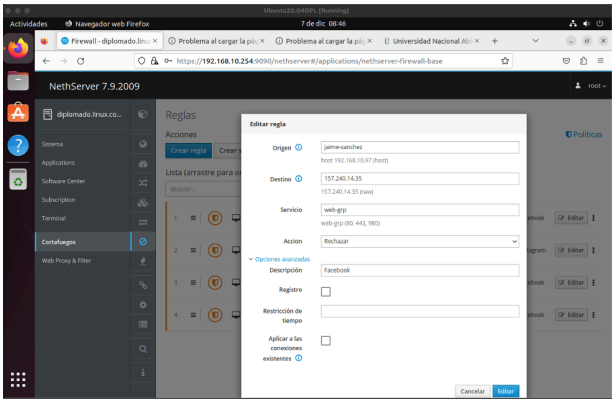

Figura 36. Creación de regla restrictiva a www.facebook.com.

Se crea una regla restrictiva en la cual el origen debe ser la ip del cliente, la zona Verde o red LAN, el destino es la dirección o direcciones ip que apuntan al sitio de facebook, el servicio o puertos a bloquear y la acción que debe tomar el cortafuegos con la solicitud.

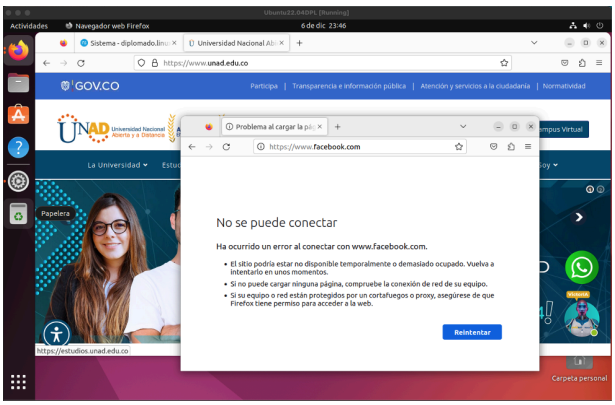

Figura 37. Validación de funcionamiento de restricción a www. facebook.com.

Se escribe en una ventana del navegador la url del sitio bloqueado para validar si la regla ha surtido efecto, en este caso, se puede observar que a pesar de que tenemos navegación en internet, la página de facebook se encuentra restringida.

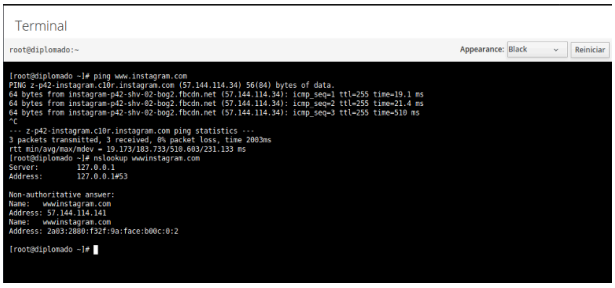

Figura 38. Comando ping y nslookup a www.facebook.com.

Se ejecutan los comandos ping y nslookup a la url de instagram y se toma nota de las ip.

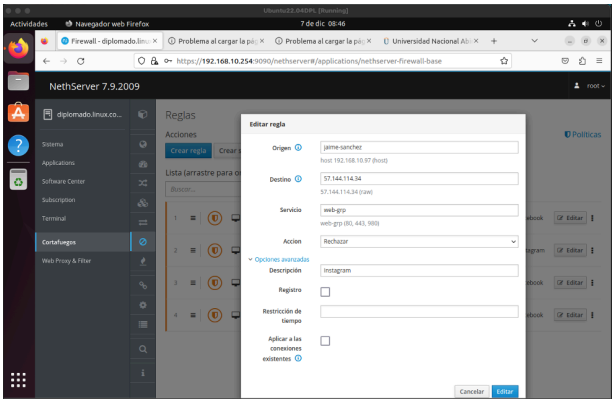

Figura 39. Creación de regla restrictiva a www. instagram.com

Se crea una regla restrictiva en la cual el origen debe ser la ip del cliente, la zona Verde o red LAN, el destino es la dirección o direcciones ip que apuntan al sitio de instagram, el servicio o puertos a bloqueary la acción que debe tomar el cortafuegos con la solicitud.

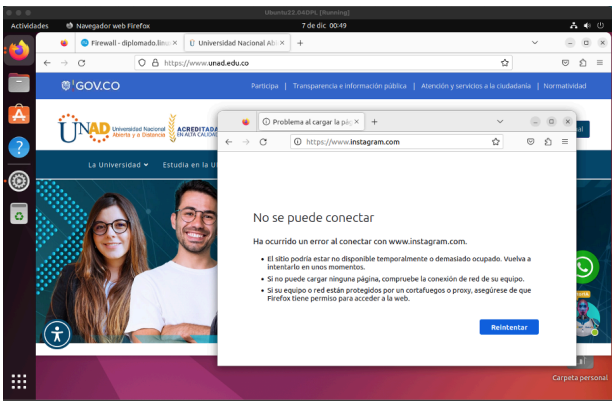

Figura 40. Validación de funcionamiento de restricción a www. instagram.com.

Se escribe en una ventana del navegador la url del sitio bloqueado para validar si la regla ha surtido efecto, en este caso, se puede observar que a pesar de que tenemos navegación en internet, la página de instagram se encuentra restringida.

Para el bloqueo de los sitios anteriores, y teniendo en cuenta que para ellos existen más de una ip que apunta al sitio, se hizo necesario definir más de una regla restrictiva por sitio; a continuación un resumen de las reglas creadas para llevar a cabo un bloqueo efectivo desde la red LAN a dichas páginas.

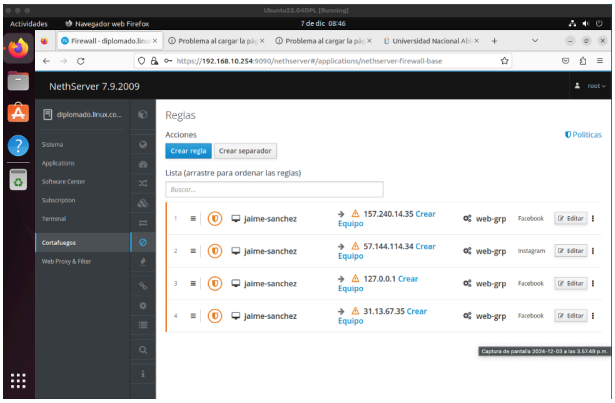

Figura 41. Resumen de reglas restrictivas para las url de los sitios www. instagram.com y www.facebook.com

3.4 FILE SERVER Y PRINT SERVER

Inicialmente se accede al servidor nethserver previamente configurado, luego se selecciona la opción sistema, usuarios y grupos y se procede a instalar el proveedor de cuentas LDAP.

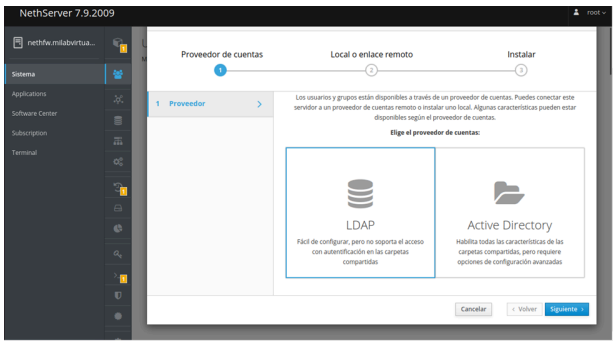

Figura 42. Instalación de proveedor de cuentas LDAP

Una vez finalizada la instalación, se accede a la configuración del proveedor LDAP y se selecciona la opción crear usuario, se carga ventana emergente donde se ingresa el nombre y grupo y se pulsa en la opción Crear.

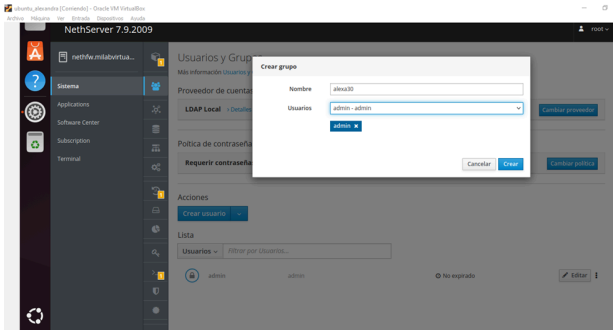

Figura 43. Creación de Grupo

Luego se selecciona la opción crear usuario, se abre ventana emergente donde se ingresa el nombre de usuario, nombre, se selecciona el grupo creado en el paso anterior y contraseña cumpliendo con los requisitos de seguridad, para finalizar se pulsa en la opción Crear.

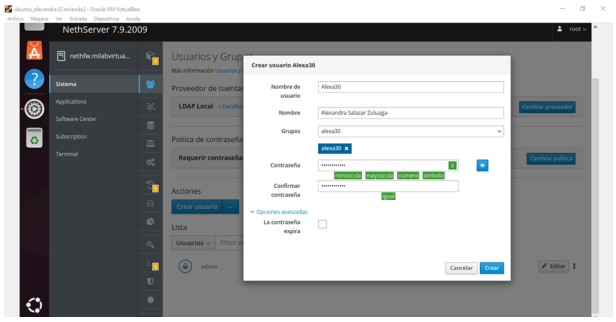

Figura 44. Creación de Usuario

Se visualiza la creación del grupo y el usuario correctamente.

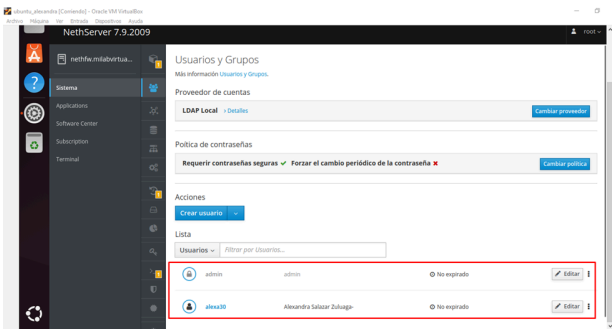

Figura 45. Visualización de Grupo y usuario creado

Se selecciona la pestaña Center Software, donde se visualizan todas las aplicaciones disponibles para instalar, se selecciona la aplicación Servidor de Archivos y Servidor de Impresión, y se pulsa clic en instalar.

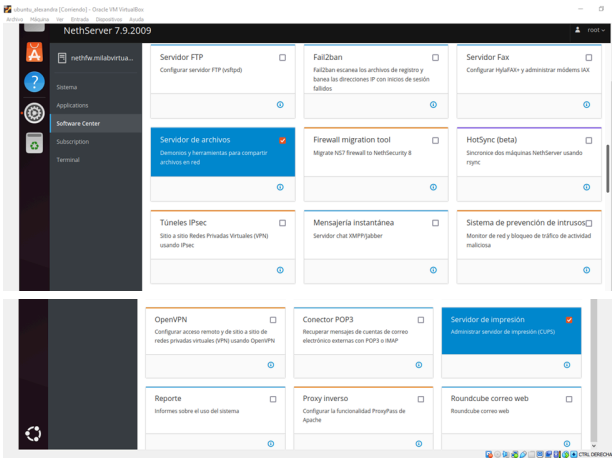

Figura 46. Instalación de Aplicaciones

Después que finaliza la instalación, se selecciona la pestaña Aplicaciones, donde se visualizan las aplicaciones instaladas en el paso anterior, en File Server seleccionamos la opción de Ajustes.

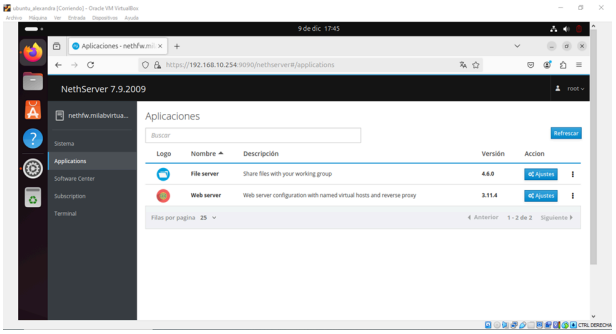

Figura 47. Aplicaciones instaladas

Se abre la pantalla Servidor de Archivos, se selecciona la pestaña Carpetas Compartidas .

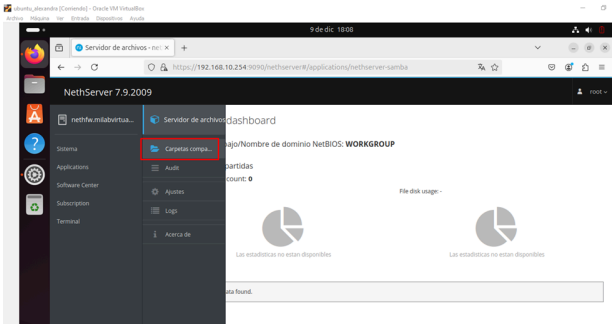

Figura 48. Carpetas Compartidas

Se selecciona la opción Crear Carpeta Compartida, y se carga ventana emergente donde se ingresa el nombre y la Descripción, y se pulsa clic en Crear.

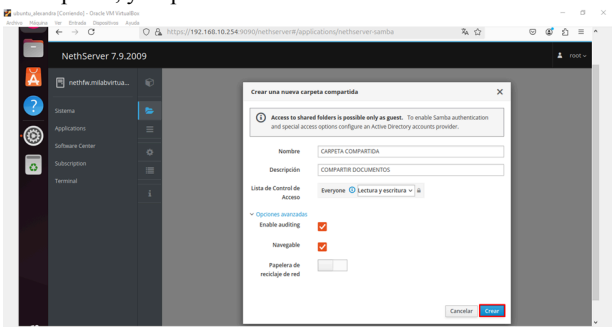

Figura 49.Ingresar Datos Carpetas Compartidas

Seleccionar la opción Auditoría, y se pulsa clic en instalar paquete

.

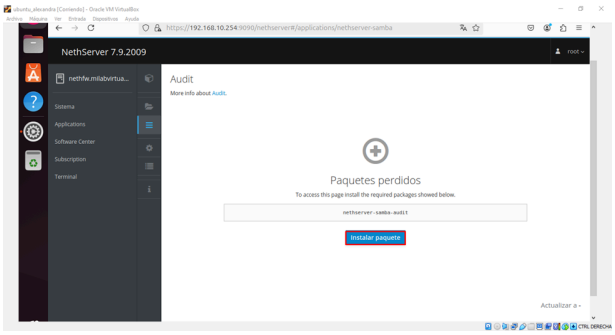

Figura 50 .Instalar paquete Auditoria

Una vez finaliza la instalación se pulsa clic en Actualizar la base de datos de Auditoría.

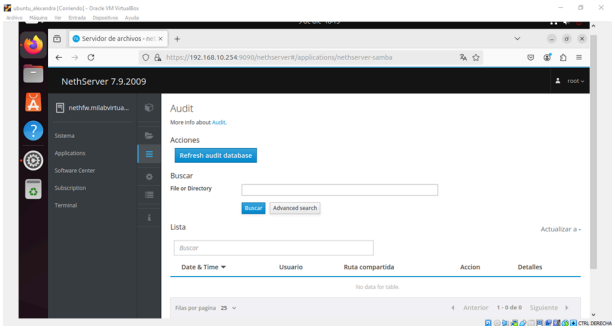

Figura 51 . Actualización de la base de datos de Auditoría

Después de actualizar la base de datos de Auditoría, se procede abrir el explorador de Archivos y se selecciona la pestaña Otras Ubicaciones, y se evidencia la carpeta compartida que se creó con anterioridad.

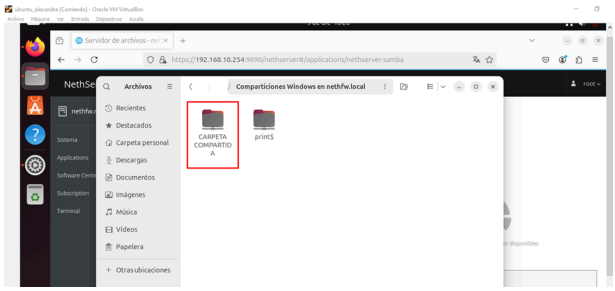

Figura 52. Otras Ubicaciones

Al pulsar doble clic en la carpeta compartida para abrirla, se debe ingresar el nombre de usuario y contraseña para poder conectarse.

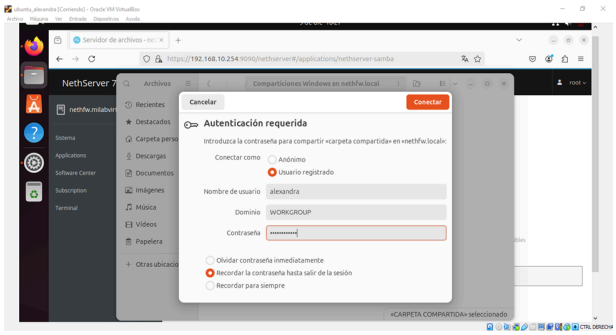

Figura 53. Autenticación

Después de ingresar a la carpeta compartida, se procede a crear dos carpetas para luego validar en el nethserver que se registren los movimientos correspondientes.

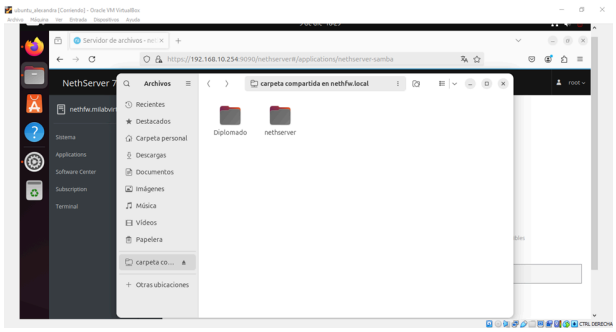

Figura 54. Creación de Carpetas

Se ingresa nuevamente al nethserver y seleccionamos la opción de Servidor de Archivos, donde se visualiza el historial de los movimientos realizados en la carpeta compartida.

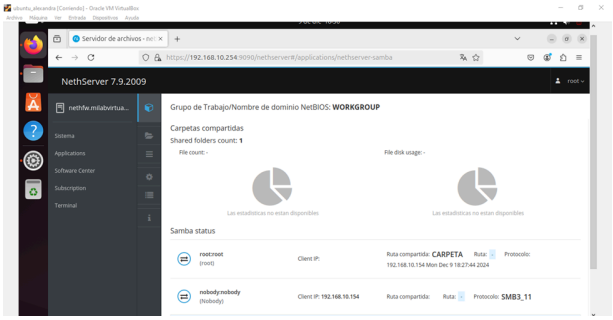

Figura 55. Historial de Movimientos de la Carpeta Compartida

Para configurar la Impresora se abre una nueva pestaña y se ingresa la dirección ip con el puerto, 192.168.10.254:631, se selecciona la pestaña Administración y se pulsa clic en la opción añadir impresora.

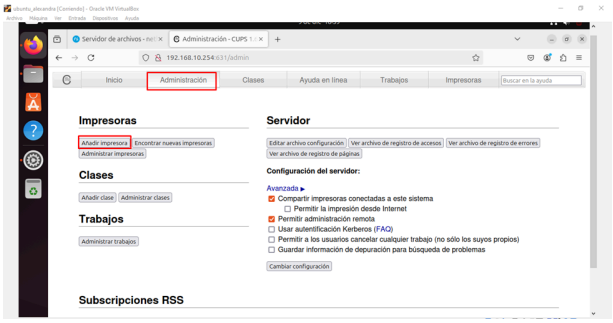

Figura 56. Añadir Impresora

Se carga pantalla donde se selecciona el tipo de impresora, en este caso seleccionamos la opción de impresoras locales y pulsamos clic en siguiente.

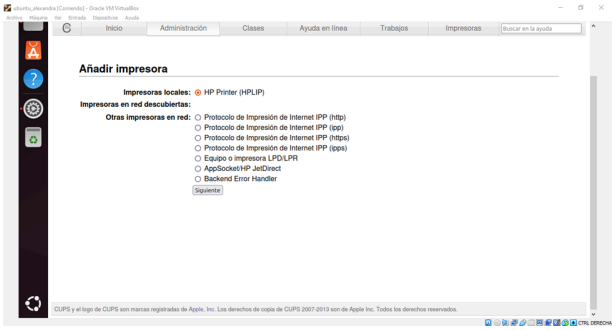

Figura 57. Tipo de Impresora

Al pulsar clic en siguiente se carga pantalla donde se configura la conexión en base al ejemplo que se muestra, se pulsa clic en Siguiente.

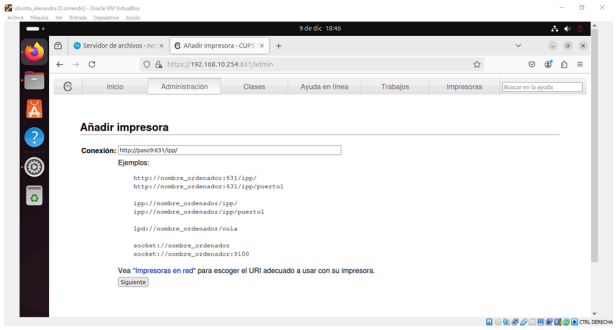

Figura 58. Conexión

Se continua con la configuración de la impresora y se ingresa el Nombre. Descripción, Marca, Modelo y para finalizar se pulsa clic en añadir impresora .

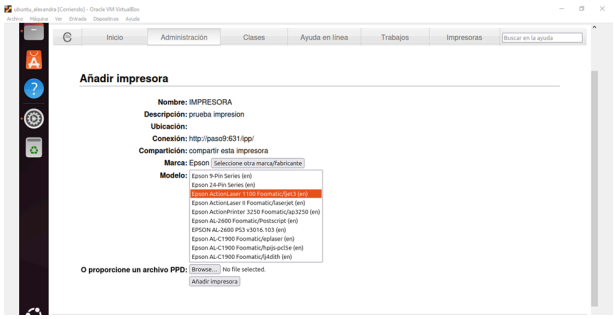

Figura 59. Configuración de Impresora

Se selecciona la pestaña impresora para validar que se cargue correctamente la impresora configurada en el paso anterior.

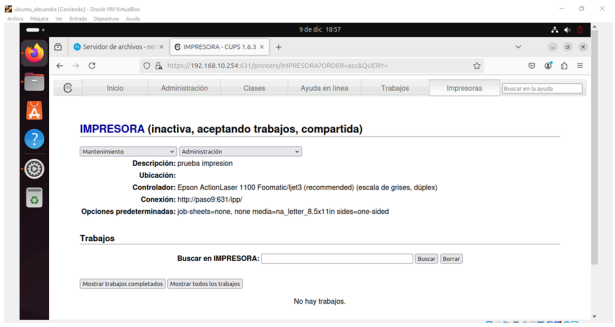

Figura 60. Detalle de la impresora creada

3.5 VPN

Por medio de NethServer, un sistema operativo basado en Linux se puede configurar fácilmente un VPN utilizando OpenVPN para crear conexiones seguras y gestionar el acceso remoto a recursos internos. NethServer permite tanto configuraciones de tipo Roadwarrior como net2net, facilitando la interconexión de redes remotas o el acceso remoto segura a una red interna.

La implementación inicia accediendo al servidor NethServer, ahí se accede al software center, se busca la aplicación OpenVPN para instalarla en NethServer.

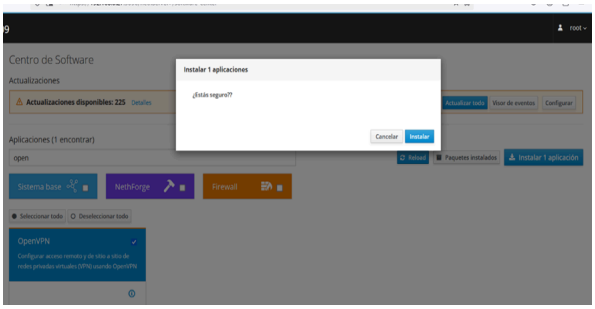

Figura 61 . Instalación de OpenVPN

Tras instalar OpenVPN, la aplicación se muestra en la sección de aplicaciones de NethServer. Para configurar la VPN, primero se crea un proveedor de cuentas LDAP en Sistemas, Usuarios y Grupos.

Figura 62 . Creación de proveedor de cuentas LDAP

Seguidamente, se selecciona la opción instalar LDAP Local. Este paso permite que NethServer gestione los usuarios y grupos necesarios para habilitar la autenticación y control de accesos en la VPN.

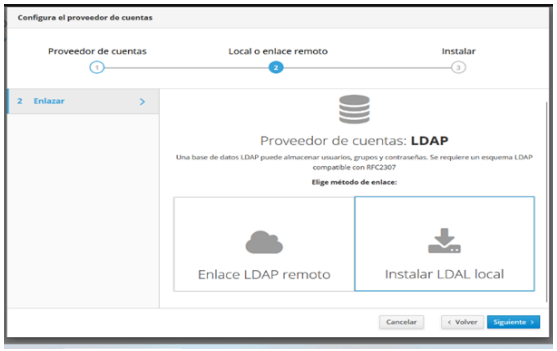

Figura 63. Instalación LDAL Local

Con el LDAP instalado, se accede a la configuración del proveedor LDAP y se selecciona crear usuario. En este paso, se define un nombre de usuario, nombre, grupo y contraseña cumpliendo con los requisitos de seguridad.

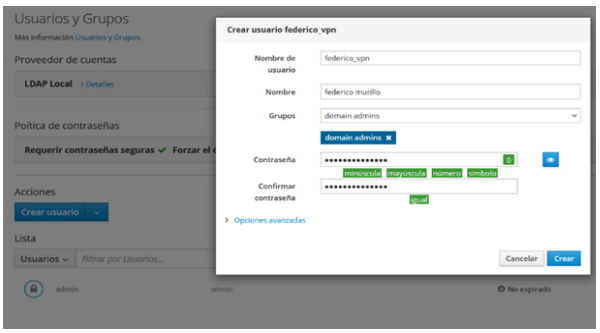

Figura 64 . Creación de un usuario LDAP

Al completar estos pasos, el nuevo usuario aparece listado en el apartado de usuarios del servidor. Para este ejemplo, se creó un usuario con el nombre federico_vpn.

Figura 65. Verificación del usuario creado

Desde la aplicación OpenVPN en NethServer, se selecciona OpenVPN RoadWarrior Server. Allí se define el modo de autenticación, red y máscara, además de configurarse para usar la IP local y que el servidor inicie automáticamente.

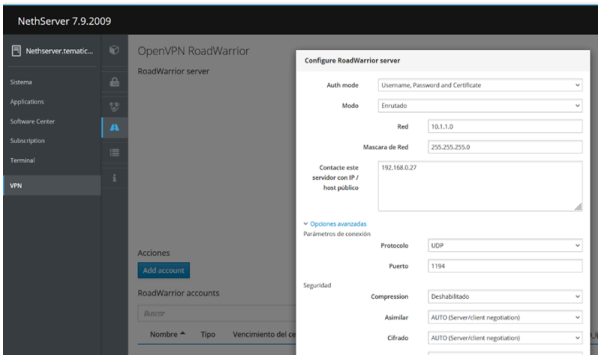

Figura 66. Configuración del servidor OpenVPN

Tras configurar el servidor, se selecciona Add Account para registrar la cuenta de usuario. Luego, se verifica que la cuenta esté correctamente registrada.

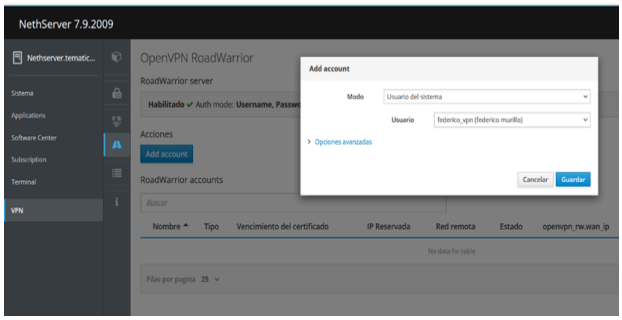

Figura 67. Creación de la cuenta de usuario en OpenVPN

En otra terminal de linux, se instala OpenVPn mediante el comando ‘sudo apt install openvpn -y’.

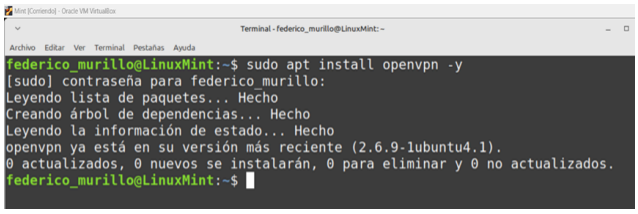

Figura 68. Instalación de OpenVPN en LinuxMint

Desde las opciones de la cuenta creada, se descarga el archivo de configuración de OpenVPN necesarios para establecer la conexión.

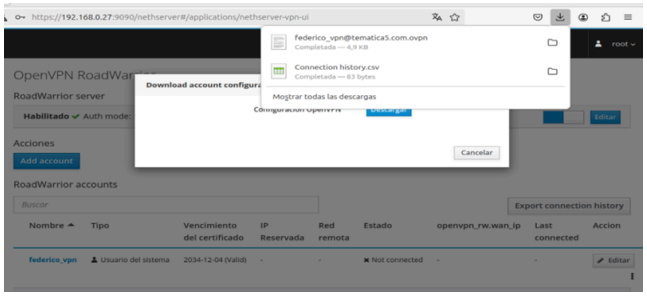

Figura 69. Descarga del archivo de configuración de OpenVPN

En LinuxMint, se accede a las conexiones de red para agregar una nueva VPN. Se selecciona la opción de importar una configuración guardada y se elige el archivo descargado previamente.

Figura 70. Configuración de la VPN

Una vez importado, se ingresan el nombre de usuario y la contraseña asociados al usuario. No se realizan modificaciones adicionales a los parámetros predeterminados.

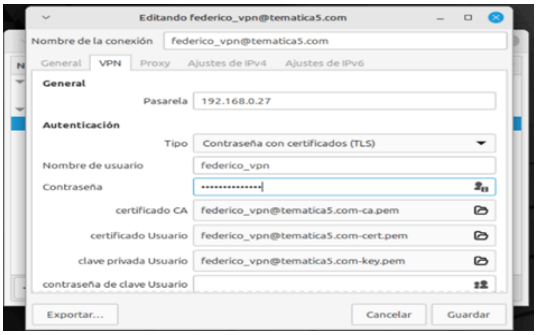

Figura 71. Modificaciones del VPN

Al completar la configuración, se visualizan dos conexiones disponibles: una cableada y una VPN. Para garantizar que la VPN se active automáticamente, se configura la conexión cableada para que inicie siempre junto con la VPN previamente creada.

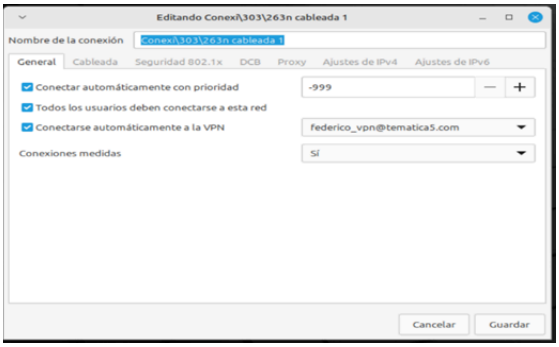

Figura 72. Verificación de conexiones

Por último, se accede nuevamente a NethServer para confirmar que el servicio VPN está activo. También se verifica que la conexión establecida sea exitosa.

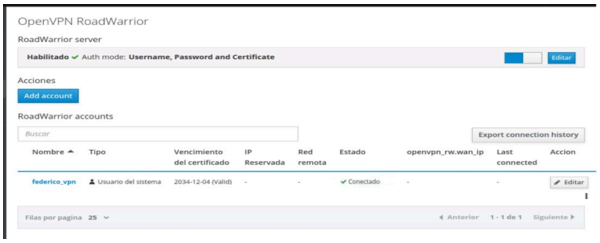

Figura 73. Verificación estado del VPN

Con esta implementación, se logra establecer una comunicación segura entre el servidor y el cliente mediante OpenVPN, garantizando acceso remoto cifrado a los recursos internos de la red.

4 CONCLUSIONES

La implementación de los servicios DHCP, DNS y Controlador de Dominio en NethServer confirma su capacidad para gestionar infraestructuras IT complejas de manera segura y eficiente, facilitando la administración centralizada de usuarios y dispositivos.

Las empresas requieren que se adopten medidas de seguridad en todos los entornos posibles para evitar ataques que la pongan en riesgo; una vulnerabilidad se produce desde el contenido proveniente de sitios de internet para lo cual las empresas adoptan el bloqueo por medio de proxy para filtrar el contenido web y obtener una capa de protección bidireccional..

Sobre la temática específica de Firewall (Cortafuegos) podemos concluir que es una gran herramienta y la primera barrera de defensa cuando de proteger nuestras redes de accesos indebidos se trata; además debemos resaltar que permite el control de uso de recursos inadecuado en el ámbito laboral, pues por medio de este podemos definir las reglas de navegación responsable enfocadas a optimizar el rendimiento no solo de la capacidad instalada en nuestras redes sino también de nuestro recurso humano.

Tanto los servidores de archivos como los de impresión, son herramientas que se utilizan para almacenar, compartir archivos y administrar impresiones en una red, son soluciones clave para una gestión eficiente y centralizada de recursos en redes empresariales, ambos servicios ofrecen fácil accesibilidad. seguridad y eficiencia.

Configurar una VPN con OpenVPN en NethServer facilita la creación de un canal seguro y cifrado para conectar usuarios remotos a la red interna de una organización. Este enfoque protege los datos sensibles durante su transmisión y garantiza un acceso confiable y controlado a los recursos internos.

5 REFERENCIAS

[1] Mil Sistemas. (2022). Administración de redes Linux con rutas IP. Recuperado de https://www.milsistemas.es

"Nethserver system requiremients". En https://www.nethserver.org. Disponible en: https://docs.nethserver.org/projects/ns8/en/latest/system_requirements.html#supported-distros-section Consultado: 03 de diciembre de 2024 10:19 am.

"Nethserver installation methods". En https://www.nethserver.org. Disponible en: https://docs.nethserver.org/projects/ns8/en/latest/install.html#pre-built-image Consultado: 03 de diciembre de 2024 10:39 am.

"Nethserver firewall". En https://www.nethserver.org. Disponible en: https://docs.nethserver.org/es/v7/firewall.html Consultado: 03 de diciembre de 2024 10:50 am.