

IMPLEMENTACIÓN Y CONFIGURACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT EN NETHSERVER

Integrante 1 Eliana Sandrith Jimenez Cruz – cc 1045525915

e-mail: esjimenezc@unadvirtual.edu.co

Integrante Diana Marcela Plaza Berrio – cc 1041268904

e-mail: dmplazab@unadvirtual.edu.co

Integrante 3 Stiben Rodriguez Rojas – cc 1017218384

e-mail: srodriguezroj@unadvirtual.edu.co

Integrante 4 Maria Camila Patino Alzate – cc 1092915616

e-mail: mcpatinoa@unadvirtual.edu.co

Integrante 5 Yefferson Mena Mena - cc1077452046

e-mail: ymenamen@unadvirtual.edu.co

RESUMEN: Se realizó la implementación y configuración integral de servicios de infraestructura IT utilizando NethServer como sistema operativo base. Las actividades incluyeron la instalación y ajuste de múltiples servicios: DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server y VPN. Cada uno de estos servicios fue configurado para garantizar la autenticación, conectividad y control de accesos en estaciones de trabajo GNU/Linux, asegurando el cumplimiento de los requerimientos técnicos y de seguridad. Se realizaron pruebas específicas para validar la funcionalidad de cada servicio, evidenciando su correcto desempeño en entornos de Intranet y Extranet. Este trabajo refleja la viabilidad de NethServer como solución robusta para la administración de servicios críticos en redes empresariales complejas.

PALABRAS CLAVE: GNU/Linux, NethServer, servicios IT, administración de redes.

1 INTRODUCCIÓN

La gestión eficiente de servicios de infraestructura IT es fundamental para el funcionamiento de instituciones con redes complejas, tanto en entornos de Intranet como de Extranet. En este contexto, NethServer se presenta como una solución robusta basada en GNU/Linux, capaz de integrar y administrar múltiples servicios esenciales para la operación de redes empresariales.

Este informe detalla la implementación y configuración de un conjunto integral de servicios en NethServer, incluyendo DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server y VPN. Cada servicio fue configurado con base en las mejores prácticas y aplicando los conocimientos adquiridos en actividades previas, asegurando así la correcta integración y funcionalidad con estaciones de trabajo GNU/Linux.

El objetivo principal de este trabajo es demostrar la capacidad de NethServer para administrar de manera eficiente los servicios críticos de IT, validando su desempeño mediante

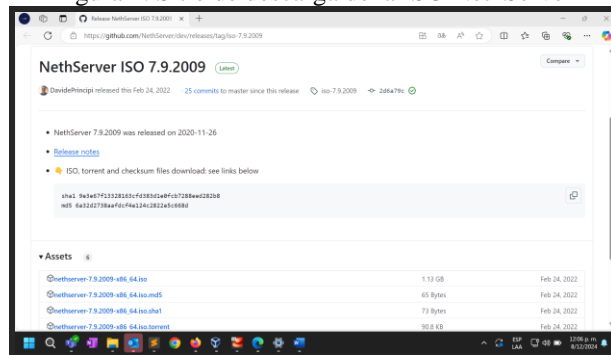
pruebas específicas y garantizando el cumplimiento de los requerimientos técnicos y de seguridad. Este proceso refleja la importancia de utilizar herramientas confiables y configuraciones personalizadas para responder a las necesidades de redes institucionales complejas.

2 CONFIGURACIÓN E INSTALACIÓN DE NETHSERVER

2.1 DESCARGA DE LA ISO NETHSERVER

Para llevar a cabo la implementación de los servicios de infraestructura IT, se procedió a la descarga de la imagen ISO de NethServer en su versión 7.9.2009. Este archivo se obtuvo desde el repositorio oficial en GitHub, accesible a través del enlace: <https://github.com/NethServer/dev/releases/tag/iso-7.9.2009>.

Figura 1. Sitio de descarga de la ISO NethServer



Fuente: Autoría Propia

2.2 REQUISITOS MÍNIMOS DEL SISTEMA

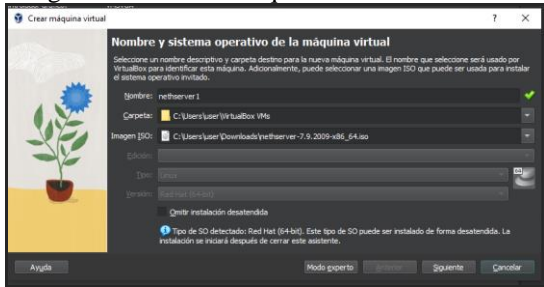
Para la instalación y ejecución de NethServer 7.9.2009, se requiere un sistema que cumpla con los siguientes requisitos mínimos: un procesador de 64 bits compatible, 1 GB de memoria RAM como mínimo, 8 GB de espacio en disco para una instalación básica, y una tarjeta de red. Sin embargo, para configuraciones que incluyan servicios adicionales o múltiples usuarios conectados, se recomienda disponer de al menos 2

GB de RAM y 20 GB de almacenamiento. Estos requerimientos aseguran un desempeño óptimo del sistema y la capacidad de manejar servicios críticos de infraestructura IT.

2.3 CREACIÓN DE MÁQUINA VIRTUAL

Se creó una máquina virtual en VirtualBox para la instalación de NethServer 7.9.2009.

Figura 2. Creación máquina virtual NethServer

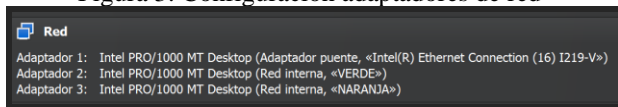


Fuente: Autoría Propia

2.4 CONFIGURACIÓN DEL ADAPTADOR DE REDES

En la máquina virtual de NethServer se configuraron tres adaptadores de red: el primero en modo puente para la red WAN (roja), asegurando la conectividad con Internet; el segundo como red interna para la LAN (verde), destinada a la comunicación con dispositivos locales; y el tercero también como red interna, asignado a la DMZ (naranja), utilizado para servicios expuestos de forma segura.

Figura 3. Configuración adaptadores de red

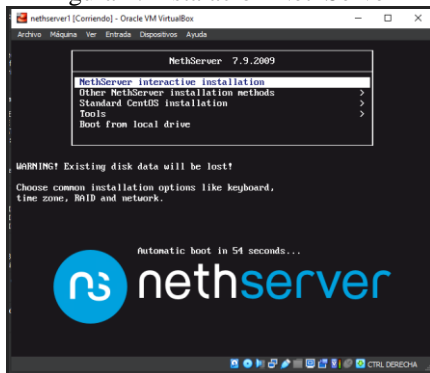


Fuente: Autoría Propia

2.5 INSTALACIÓN NETHSERVER

Se inicia la instalación de NethServer en la máquina virtual desde la imagen ISO previamente descargada.

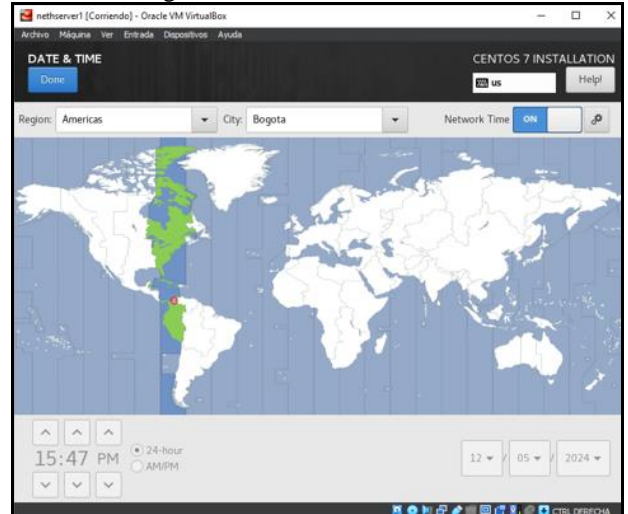
Figura 4. Instalación NethServer



Fuente: Autoría Propia

Se seleccionó la zona horaria ajustando el país correspondiente en el mapa interactivo.

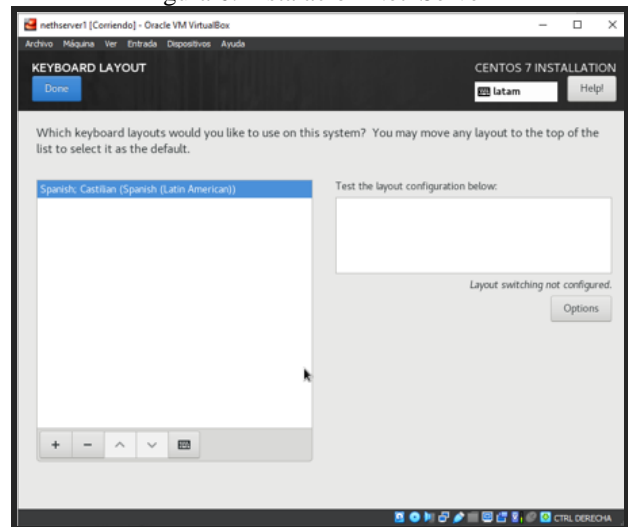
Figura 5. Instalación NethServer



Fuente: Autoría Propia

Se configuró el idioma del teclado, eligiendo la opción de español latinoamericano para mayor compatibilidad.

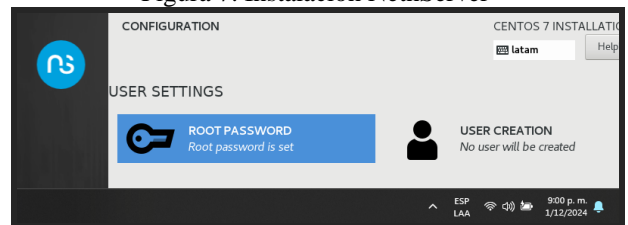
Figura 6. Instalación NethServer



Fuente: Autoría Propia

Se crea contraseña de usuario root para garantizar el acceso controlado al sistema.

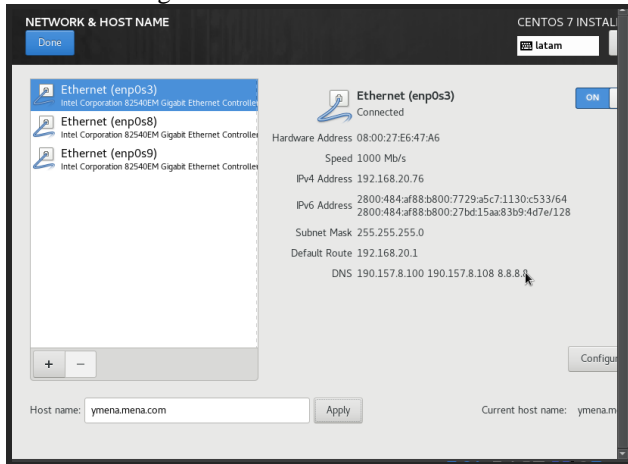
Figura 7. Instalación NethServer



Fuente: Autoría Propia

Se configuraron las interfaces de red, asignando cada adaptador a las zonas WAN, LAN y DMZ según los requisitos establecidos.

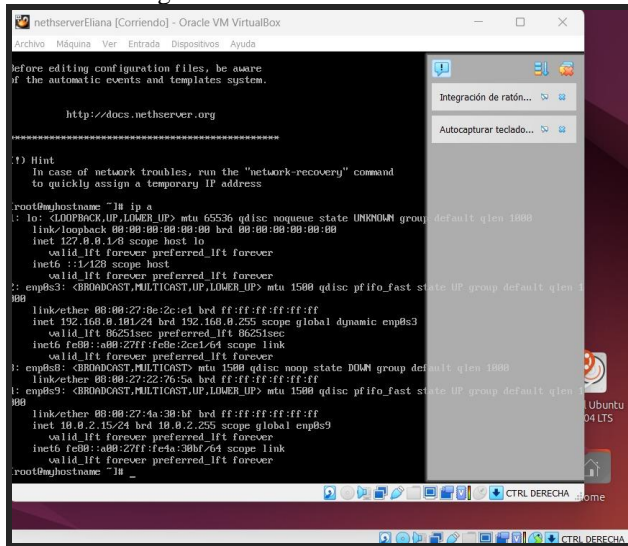
Figura 8. Instalación NethServer



Fuente: Autoría Propia

Se verifica que NethServer está instalado y en ejecución, con las redes correctamente configuradas según lo definido durante el proceso de instalación.

Figura 9. Instalación NethServer



Fuente: Autoría Propia

de dicha estación en los servicios de Infraestructura IT de NethServer.

3.1.1 INTRODUCCIÓN

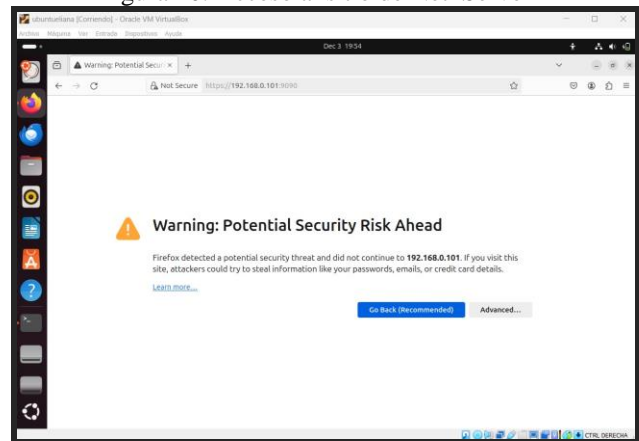
Los servicios de DHCP, DNS y Controlador de Dominio son esenciales para la gestión eficiente y segura de la infraestructura de red.

- DHCP Server: Este servicio asigna direcciones IP dinámicamente a los dispositivos de la red, lo que permite una gestión automatizada y sin necesidad de configuración manual en cada estación de trabajo.
- DNS Server: El servidor DNS se encarga de traducir nombres de dominio en direcciones IP, facilitando la navegación dentro de la red y en Internet.
- Controlador de Dominio: Ofrece servicios de autenticación centralizada, gestionando usuarios y permisos dentro de un entorno de red, garantizando seguridad y organización.

3.1.2 ACCESO A NETHSERVER

Se asignó la IP 192.168.0.101 a la red LAN. A continuación, se abrió esta dirección IP en un navegador utilizando el protocolo HTTPS, lo que redirige al panel de administración web de NethServer.

Figura 10. Acceso al sitio de NethServer



Fuente: Autoría Propia

3.1.3 AUTENTICACIÓN

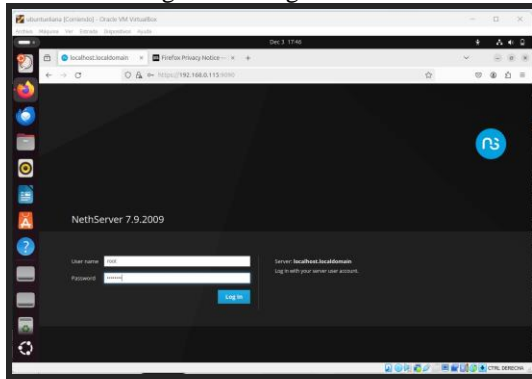
Al ingresar a la interfaz de NethServer, se presentó una pantalla de inicio de sesión donde se introdujeron las credenciales (usuario root y la contraseña asignada previamente).

3 TEMÁTICAS DESARROLLADAS

3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Producto esperado: 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

Figura 11. Login de NethServer

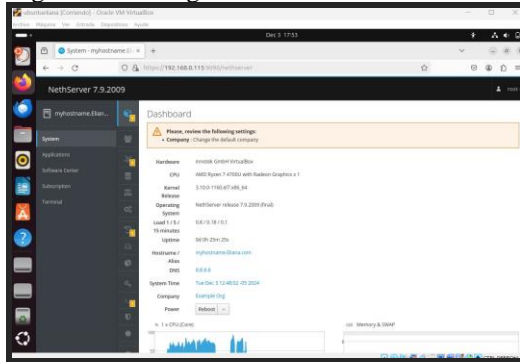


Fuente: Autoría Propia

3.1.4 INICIO DE NETHSERVER

Una vez iniciado sesión, se procedió a configurar los servicios correspondientes a la red y a los servidores que se iban a utilizar.

Figura 12. Configuración inicial de los servicios

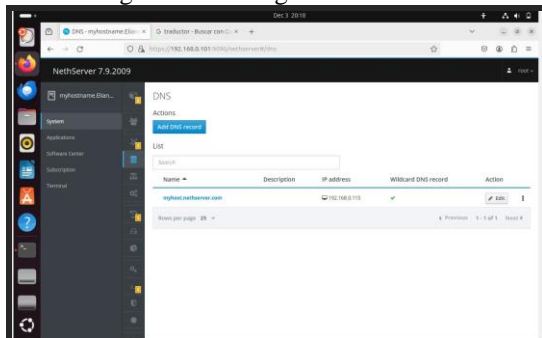


Fuente: Autoría Propia

3.1.5 CONFIGURACIÓN DEL SERVIDOR DNS

Se configuró el servicio de DNS para la resolución de nombres de dominio dentro de la red local, asegurando que las estaciones de trabajo puedan acceder a los recursos internos de manera eficiente. (Descripción de los detalles específicos de la configuración aquí).

Figura 13. Configuración servidor DNS

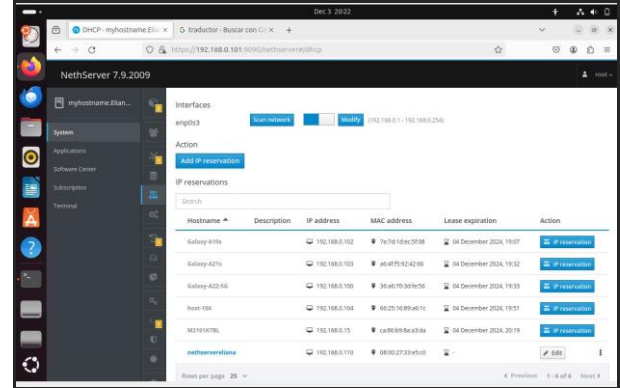


Fuente: Autoría Propia

3.1.6 CONFIGURACIÓN DEL SERVIDOR DHCP

En la interfaz de NethServer, se accedió a la opción de configuración de DHCP, donde se asignaron los rangos de IP disponibles para la red LAN.

Figura 14. Configuración servidor DHCP

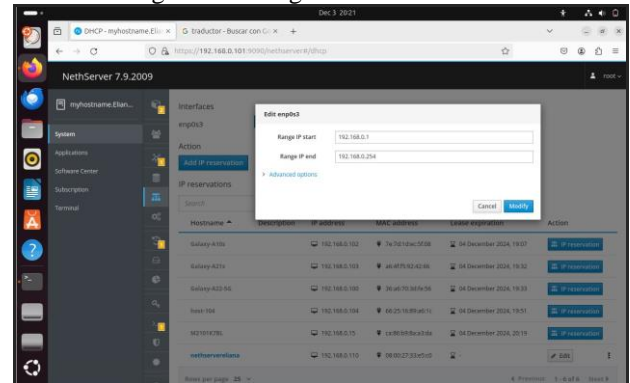


Fuente: Autoría Propia

3.1.7 ASIGNACIÓN DE DIRECCIONES IP

Al encender el servidor y acceder a la opción de configuración DHCP, se asignaron los rangos de direcciones IP a las interfaces de red.

Figura 15. Rango de direcciones IP

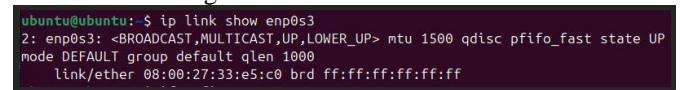


Fuente: Autoría Propia

3.1.8 BÚSQUEDA DE MAC ADDRESS

Para asegurarse de que los dispositivos correctos recibieran las direcciones IP adecuadas, se configuraron reservas de direcciones basadas en las direcciones MAC de cada dispositivo.

Figura 16. MAC Address

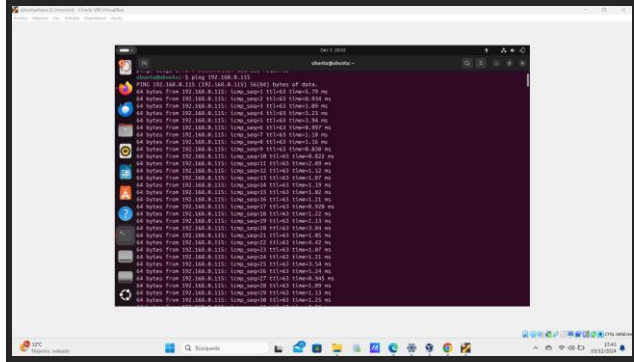


Fuente: Autoría Propia

3.1.9 CONEXIÓN CON UBUNTU A NETHSERVER

Se verificó la conexión entre el servidor NethServer y una estación de trabajo Ubuntu mediante el comando ping, confirmando que la estación de trabajo podía comunicarse correctamente con el servidor.

Figura 17. Ping desde desktop a NethServer



Fuente: Autoría Propia

3.1.10 COMPROBACIÓN DE DHCP Y DNS

Finalmente, se validó que el servidor DHCP estuviera funcionando correctamente al verificar que la estación de trabajo recibiera su dirección IP automáticamente. También se verificó la resolución de nombres mediante el servidor DNS configurado.

3.2 TEMÁTICA 2: PROXY

Producto esperado: Implementación y configuración detallada del control del 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.

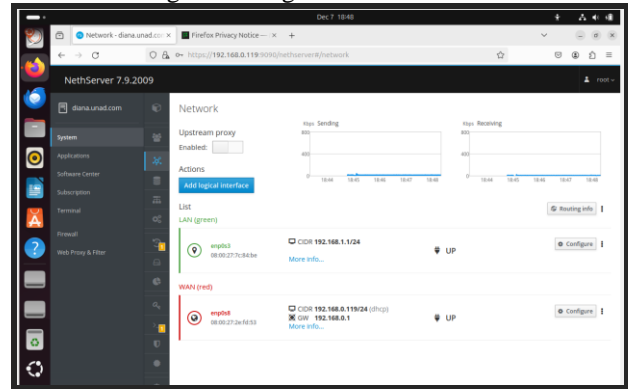
3.2.1 INTRODUCCIÓN

La implementación de un servidor proxy en NethServer es fundamental para controlar el acceso a Internet desde la red interna, aplicando filtros que restrinjan el acceso a ciertos contenidos. Esto se logra mediante la configuración de un servidor proxy que utiliza el puerto 3128 para filtrar el tráfico y bloquear ciertos sitios web o tipos de archivos. A continuación, se describe el proceso de configuración y los pasos realizados.

3.2.2 ACCESO A LA RED

Se ingresa a la red para configurar la lista de servidores de cada interfaz de red en NethServer. Esto permite establecer la comunicación entre las diferentes redes (LAN, WAN, DMZ) y configurar adecuadamente el proxy.

Figura 18. ingreso a NethServer



Fuente: Autoría Propia

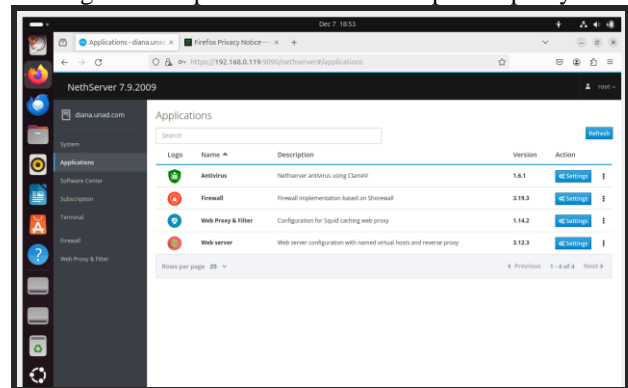
3.2.3 INSTALACIÓN DEL PROXY

Seguidamente, se procede a la instalación del proxy web en NethServer. Este servicio permite gestionar y controlar el tráfico de Internet, asegurando que las conexiones de salida se filtren de acuerdo con las políticas establecidas.

3.2.4 APLICACIONES INSTALADAS

Se evidencia que las aplicaciones necesarias para el funcionamiento del proxy han sido instaladas correctamente, permitiendo que se realice el filtrado de contenido y control de acceso.

Figura 19. Aplicaciones instaladas para el proxy

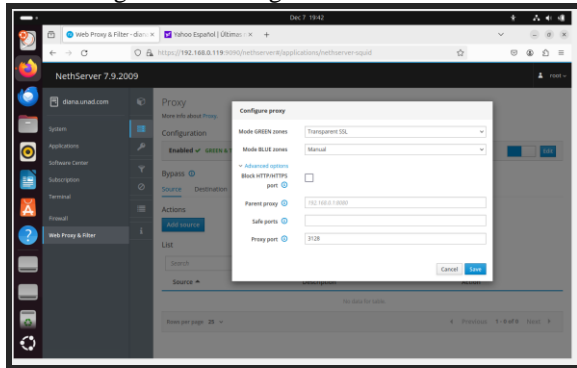


Fuente: Autoría Propia

3.2.5 CONFIGURACIÓN DE ZONAS DE RED

Se configura la zona verde como transparent SSL para permitir que el tráfico cifrado también pase a través del proxy. La zona azul se configura como manual, y se asigna el puerto 3128, que es el puerto predeterminado utilizado por el proxy para la filtración de tráfico.

Figura 20. Configuración de las zonas

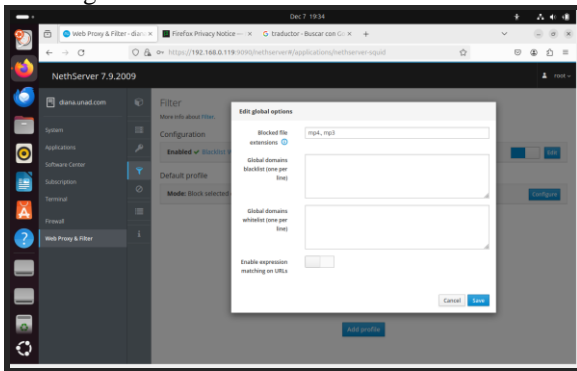


Fuente: Autoría Propia

3.2.6 FILTRO DE EXTENSIONES DE ARCHIVOS

Se configura un filtro para bloquear ciertas extensiones de archivos como .mp4 y .mp3, restringiendo el acceso a contenidos multimedia que no estén permitidos por las políticas establecidas.

Figura 21. Filtro de extensiones de archivos

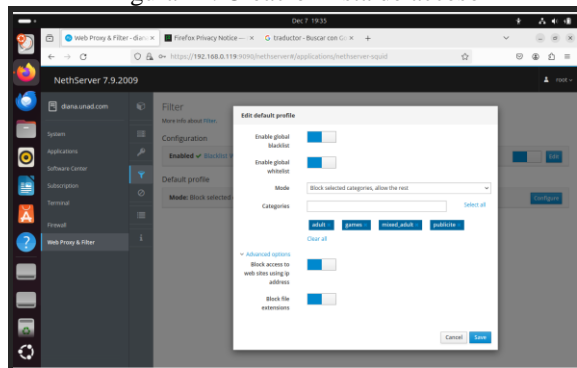


Fuente: Autoría Propia

3.2.7 CREACIÓN DE LISTAS DE ACCESO

Se configura una lista de sitios web que no serán permitidos para los usuarios, bloqueando sitios de publicidad y páginas para adultos. Se habilitan las listas negras y blancas globales, lo que permite gestionar de manera más eficiente el control del acceso a Internet.

Figura 22. Creación lista de acceso

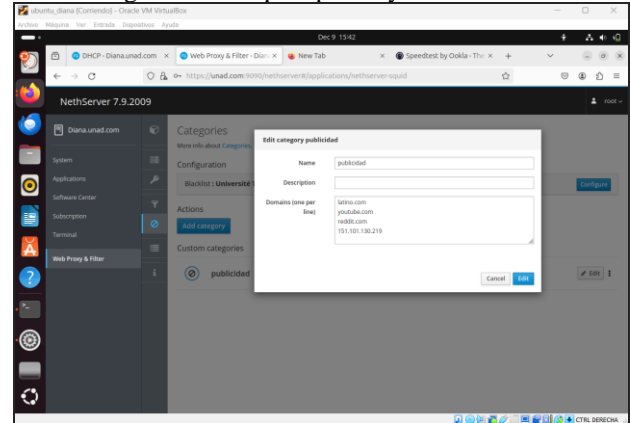


Fuente: Autoría Propia

3.2.8 BLOQUEO POR IP Y EXTENSIONES

Además de las listas de URLs, se configura el bloqueo mediante la dirección IP de los sitios y las extensiones de archivos que no deben ser accesibles desde la red interna.

Figura 23. Bloqueo por IP y extensiones



Fuente: Autoría Propia

3.2.9 VERIFICACIÓN DEL FUNCIONAMIENTO DEL PROXY

Una vez completada la configuración, se realiza una prueba de acceso a Internet desde una estación de trabajo para asegurarse de que el proxy esté funcionando correctamente y aplicando los filtros establecidos.

Figura 24. verificación funcionamiento proxy

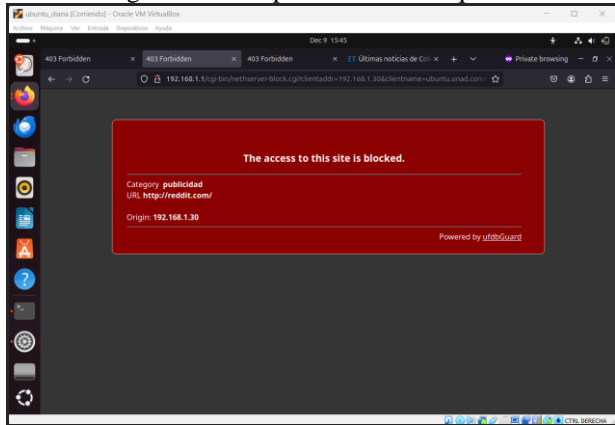


Fuente: Autoría Propia

3.2.10 COMPROBACIÓN DE BLOQUEOS Y RESTRICCIONES

Se verifica que los filtros estén aplicando correctamente las restricciones de contenido, como el bloqueo de ciertas extensiones de archivos y sitios web, según lo configurado previamente.

Figura 25. Comprobación de bloqueos



Fuente: Autoría Propia

3.3 TEMÁTICA 3: CORTAFUEGOS

Producto esperado: 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.

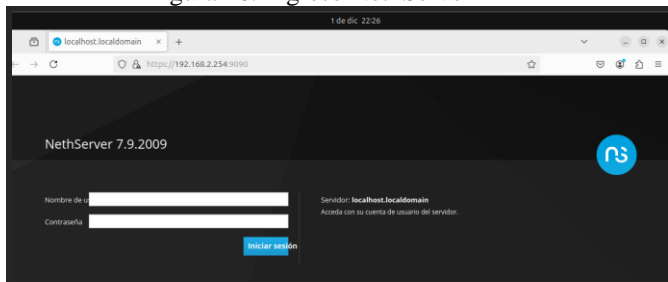
3.3.1 INTRODUCCIÓN

El cortafuegos de NethServer es una herramienta fundamental para gestionar la seguridad de la red al permitir la creación de políticas y reglas específicas que restringen el acceso a contenido no autorizado. En esta temática, se implementó un control detallado del tráfico web mediante configuraciones específicas de firewall y proxy. Esto incluyó la instalación de las aplicaciones necesarias, la creación de categorías de bloqueo, la configuración de reglas en el firewall y la validación del correcto funcionamiento de las restricciones desde una estación de trabajo GNU/Linux.

3.3.2 INGRESO A NETHSERVER

El primer paso consistió en acceder al sistema NethServer desde un navegador web utilizando la dirección IP asignada al servidor. Una vez cargada la interfaz de administración, se procedió a realizar el inicio de sesión con las credenciales configuradas previamente.

Figura 26. Ingreso NethServer

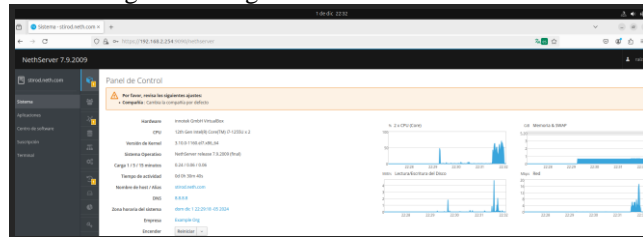


Fuente: Autoría Propia

3.3.3 INICIO DE SESIÓN EN NETHSERVER

Una vez dentro de la interfaz de NethServer, se llevaron a cabo las configuraciones iniciales necesarias para personalizar el servidor y preparar las herramientas requeridas para la gestión del tráfico web.

Figura 27. Pagina inicial de NethServer

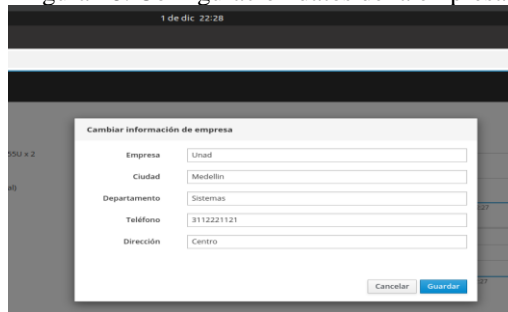


Fuente: Autoría Propia

3.3.4 DATOS DE LA EMPRESA

Se actualizaron los datos predeterminados de la empresa con información más realista, adecuada para el contexto de la actividad. Esta configuración permite identificar correctamente la organización en la interfaz y los registros del servidor.

Figura 28. Configuración datos de la empresa



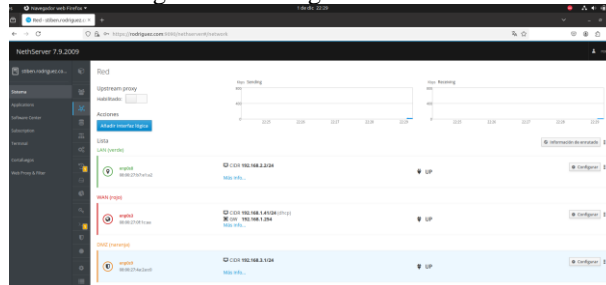
Fuente: Autoría Propia

3.3.5 CONFIGURACIÓN DE REDES

Se configuraron las diferentes redes disponibles en el servidor según las necesidades del entorno:

- Verde (LAN): Red interna de la organización.
- Naranja (DMZ): Zona desmilitarizada para servicios públicos.
- Roja (WAN): Conexión a internet.

Figura 29. Configuración de redes

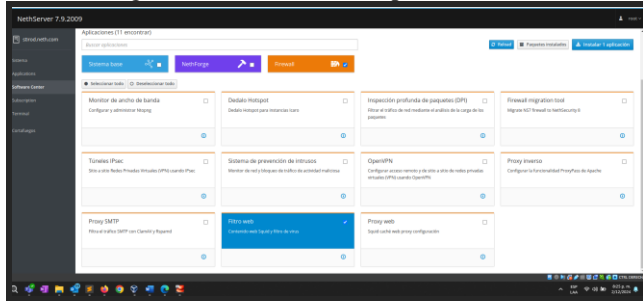


Fuente: Autoría Propia

3.3.6 INSTALACIÓN DE APLICACIONES

Para garantizar un control completo del tráfico web, se instalaron y configuraron las herramientas necesarias, incluyendo el firewall y el filtro web. Esto permitió establecer reglas específicas de acceso y restricciones según las políticas definidas.

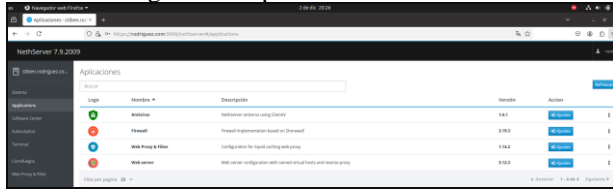
Figura 30. Instalación de aplicaciones



Fuente: Autoría Propia

Se descargaron e instalaron las aplicaciones de firewall y filtro web desde la interfaz de administración de NethServer. Esto permitió habilitar las herramientas necesarias para el control del tráfico.

Figura 31. Aplicaciones instaladas



Fuente: Autoría Propia

3.3.7 CONFIGURACIÓN DEL FIREWALL

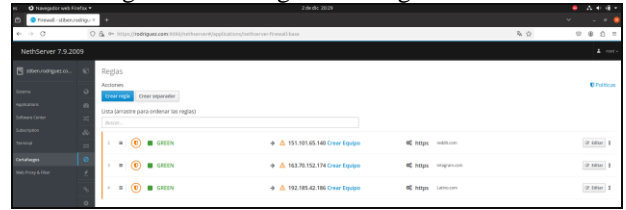
Desde la sección de configuración del firewall, se establecieron las reglas necesarias para restringir el acceso a sitios de entretenimiento y redes sociales. Las reglas se diseñaron para bloquear tanto dominios específicos como direcciones IP asociadas a dichos sitios.

Figura 32. Configuración firewall



Fuente: Autoría Propia

Figura 33. Configuración reglas firewall



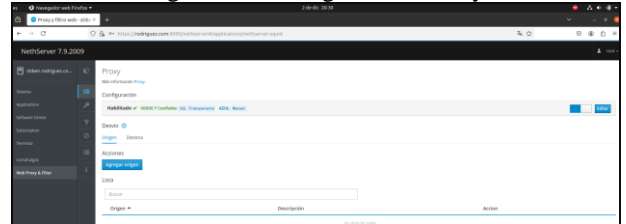
Fuente: Autoría Propia

3.3.8 CONFIGURACIÓN DEL PROXY

El proxy se habilitó como una herramienta adicional para filtrar y restringir el acceso a contenido web. A través del proxy, se establecieron categorías específicas de bloqueo, como sitios de entretenimiento y redes sociales.

Desde la interfaz de NethServer, se activó el proxy como un componente crítico para el control del tráfico web.

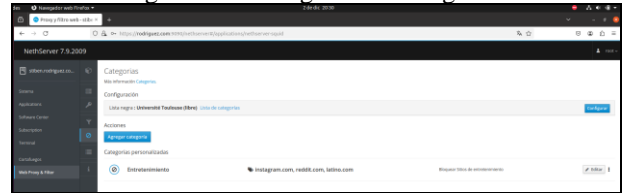
Figura 34. Configuración Proxy



Fuente: Autoría Propia

Se configuraron categorías personalizadas para bloquear sitios específicos. Esto incluyó la creación de una categoría dedicada a sitios de entretenimiento y la asignación de dominios e IP a dicha categoría.

Figura 35. Configuración categorías

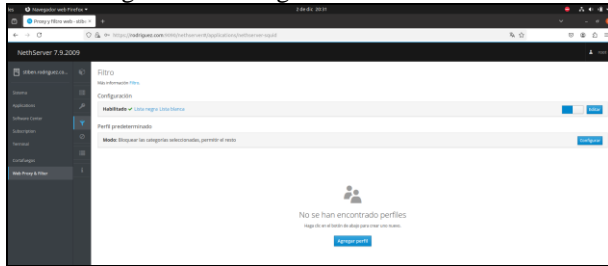


Fuente: Autoría Propia

3.3.9 FILTRO DEL PROXY

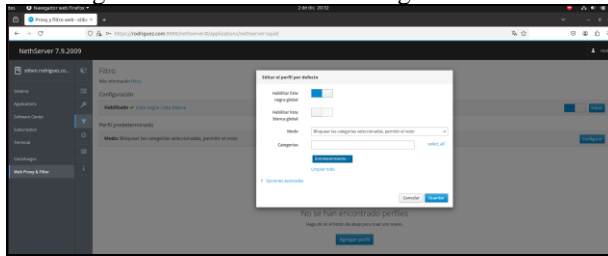
Con las categorías configuradas, se establecieron filtros que aplicaban dichas restricciones al tráfico web. Esto aseguró que las políticas definidas se aplicaran correctamente a los usuarios de la red.

Figura 36. Configuración del filtro web



Fuente: Autoría Propia

Figura 37. Habilitando las categorías creadas

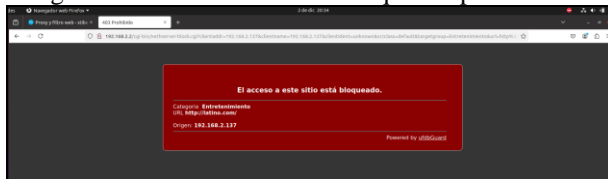


Fuente: Autoría Propia

3.3.10 VALIDACIÓN DEL FUNCIONAMIENTO

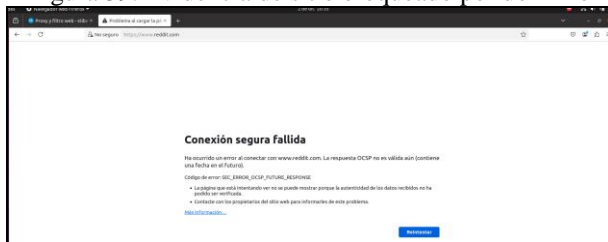
Finalmente, se realizó la validación de las restricciones configuradas. Desde una estación de trabajo GNU/Linux, se comprobó el bloqueo de sitios tanto por dominio como por IP. Las pruebas confirmaron que las políticas configuradas se aplicaron correctamente, restringiendo el acceso a contenido no autorizado.

Figura 38. Evidencia de sitio bloqueado por dominio



Fuente: Autoría Propia

Figura 39. Evidencia de sitio bloqueado por dominio



Fuente: Autoría Propia

Figura 40. Evidencia de sitio bloqueado por IP



Fuente: Autoría Propia

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: 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.

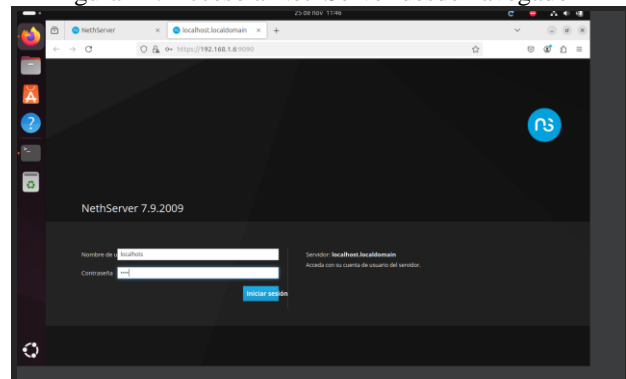
3.4.1 INTRODUCCIÓN

La implementación de un servidor de archivos (File Server) y servidor de impresoras (Print Server) permite a los usuarios acceder y gestionar archivos y recursos de impresión de manera centralizada a través de un servidor. En esta actividad, se configuró NethServer para habilitar los servicios de acceso a carpetas compartidas e impresoras mediante el uso de LDAP.

3.4.2 ACCESO A TRAVÉS DEL NAVEGADOR

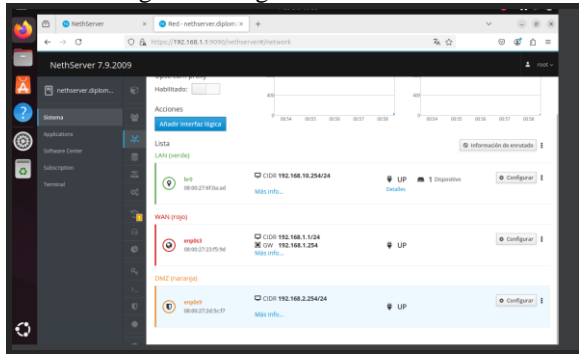
El proceso se inicia accediendo a la interfaz de NethServer mediante el navegador desde una estación de trabajo Linux Desktop, utilizando la dirección IP correspondiente.

Figura 41. Acceso a NethServer desde navegador



Fuente: Autoría Propia

Figura 42. Ingreso en NethServer

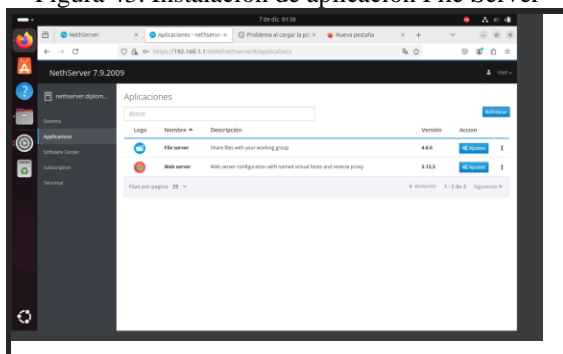


Fuente: Autoría Propia

3.4.3 INSTALACIÓN DE LA APLICACIÓN FILE SERVER

Se instala la aplicación de servidor de archivos (File Server) en NethServer, lo que habilita la funcionalidad de compartir carpetas entre los usuarios de la red.

Figura 43. Instalación de aplicación File Server

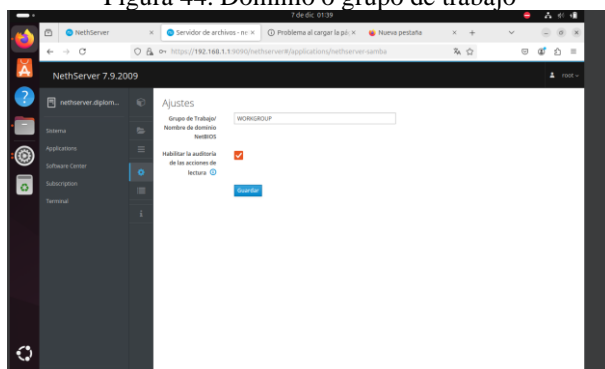


Fuente: Autoría Propia

3.4.4 CONFIGURACIÓN DEL DOMINIO O GRUPO DE TRABAJO

Se configura NethServer para ser parte de un dominio o grupo de trabajo, lo que permite la integración con un entorno LDAP para la autenticación y gestión de usuarios.

Figura 44. Dominio o grupo de trabajo

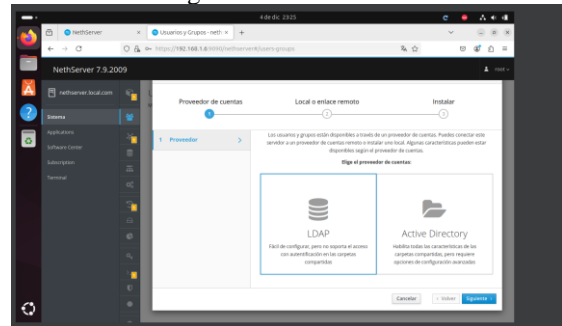


Fuente: Autoría Propia

3.4.5 CONFIGURACIÓN DE LDAP LOCAL

Se configura el servicio LDAP local en NethServer para gestionar de manera centralizada los usuarios y grupos que tendrán acceso a los recursos compartidos en el servidor.

Figura 45. LPDA local

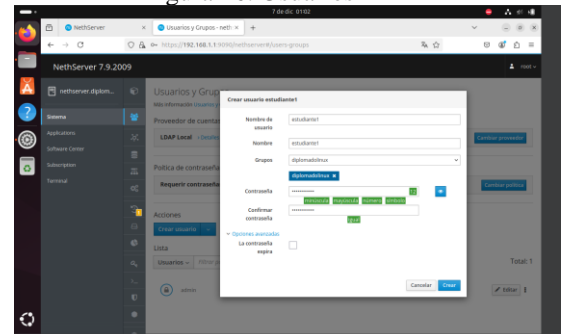


Fuente: Autoría Propia

3.4.6 CREACIÓN DE USUARIOS EN LDAP

Se procede a crear un usuario dentro del servicio LDAP, lo que permitirá que los usuarios se autentiquen en el servidor para acceder a los recursos compartidos.

Figura 46. Usuarios LPDA

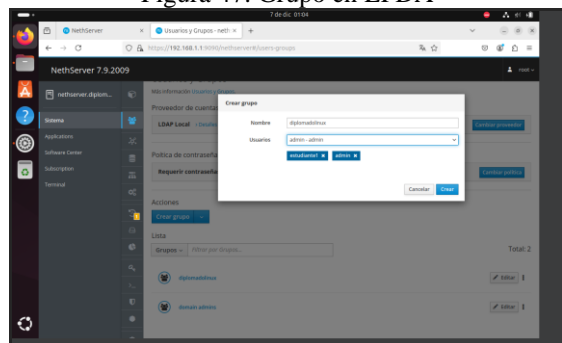


Fuente: Autoría Propia

3.4.7 CREACIÓN DE GRUPO EN LDAP

Se crea un grupo de usuarios en el servicio LDAP para organizar y gestionar de manera eficiente el acceso a los recursos del servidor.

Figura 47. Grupo en LPDA

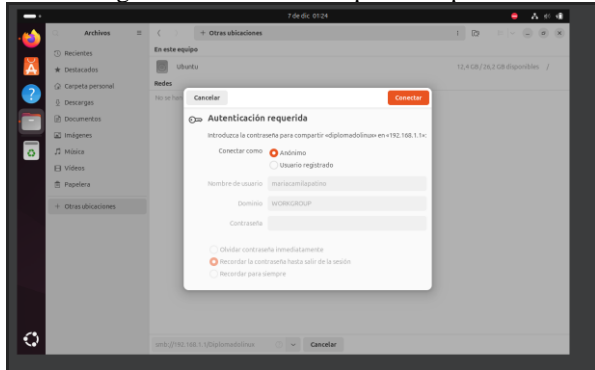


Fuente: Autoría Propia

3.4.8 CONEXIÓN A LA CARPETA COMPARTIDA DESDE LINUX DESKTOP

Se verifica el acceso desde la estación de trabajo Linux Desktop a la carpeta compartida configurada en NethServer. El acceso se realiza utilizando el usuario autenticado a través de LDAP.

Figura 48. Conexión carpeta compartida

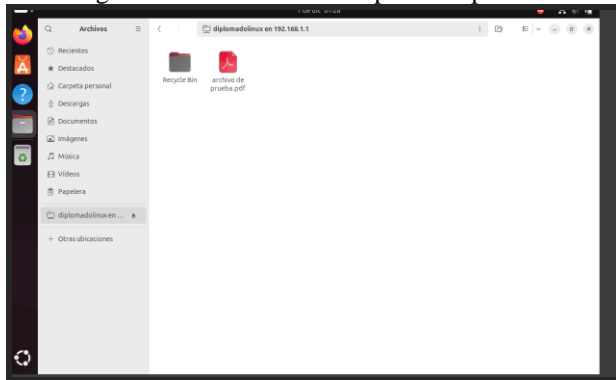


Fuente: Autoría Propia

3.4.9 ANEXADO DE ARCHIVO A LA CARPETA COMPARTIDA

Una vez realizada la conexión, se anexa un archivo a la carpeta compartida para confirmar que los usuarios pueden almacenar y gestionar archivos dentro del recurso compartido.

Figura 49. Archivo en la carpeta compartida

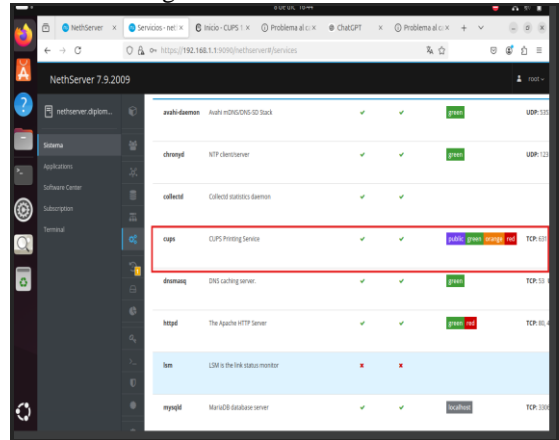


Fuente: Autoría Propia

3.4.10 VALIDACION DEL SERVICIO CUPS PARA LA INSTALACION DE IMPRESORAS

Una vez instalado el servicio de server Printer se valida el servicio de CUPS para acceder a la administración de impresoras

Figura 47. Servicios CUPS

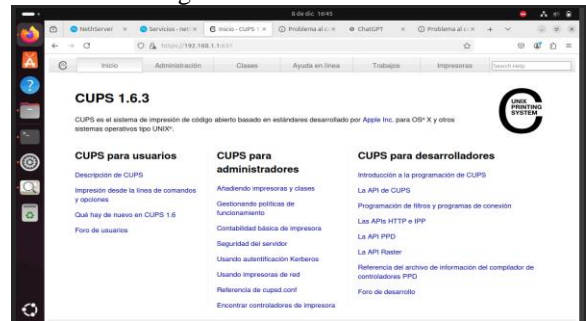


Fuente: Autoría Propia

3.4.11 ACCESO A LA URL WEB DE CUPS

Una vez configurad el server printer se accede mediante la ip del servidor apuntado al puerto 631 el cual es predeterminado para el administrador de impresoras.

Figura 48. Acceso a CUPS

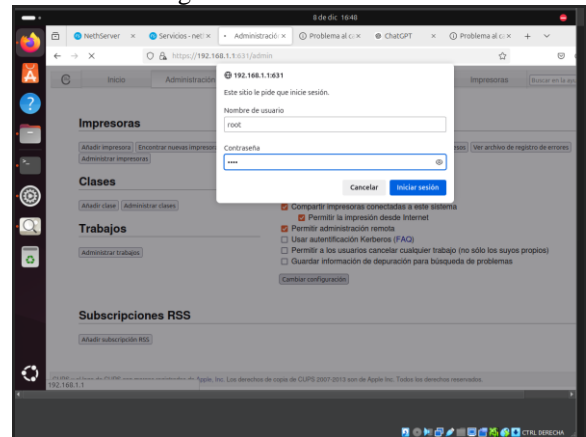


Fuente: Autoría Propia

3.4.12 CREDENCIALES DE ACCESO

Para la administración de impresora de debe acceder con el usuario y contraseña establecida en el servidor

Figura 49. Acceso a CUPS



Fuente: Autoría Propia

3.4.13 INSTALACION DE SERVICIO DE IMPRESORA VIRTUAL PARA LA EJECUCION DEL TEMATICA

se instala el servicio de cups para la impresora virtual y para ello acceder la terminal desde la web del nethserver y ejecutamos el comando: yum install cups-pdf



Figura 50. Instalación de cups-pdf

Fuente: Autoría Propia

3.4.14 INSTALACION DE LA IMPRESORA VIRTUAL

Desde al web cups se selecciona el en impresoras locales el cups-pdf

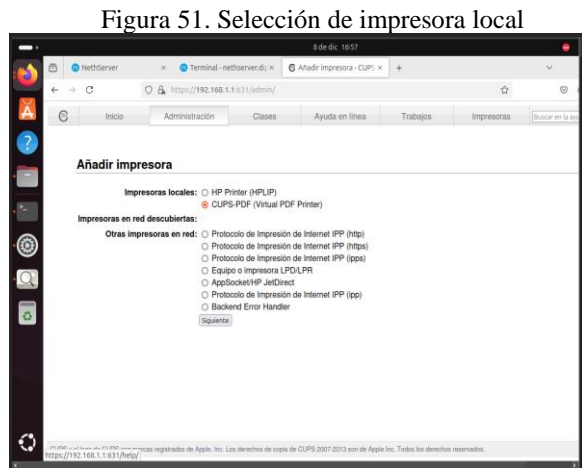


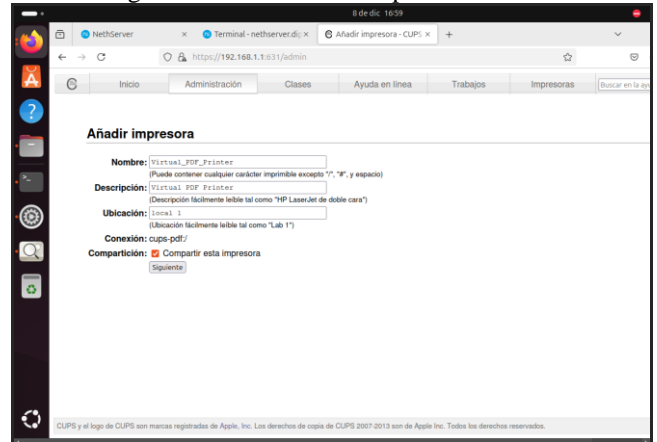
Figura 51. Selección de impresora local

Fuente: Autoría Propia

3.4.15 INSTALACION DE LA IMPRESORA VIRTUAL

Se configura la información principal de la impresora y se permite la conexión remota para que se pueda instalar desde ubuntu desktop

Figura 52. Selección de impresora local

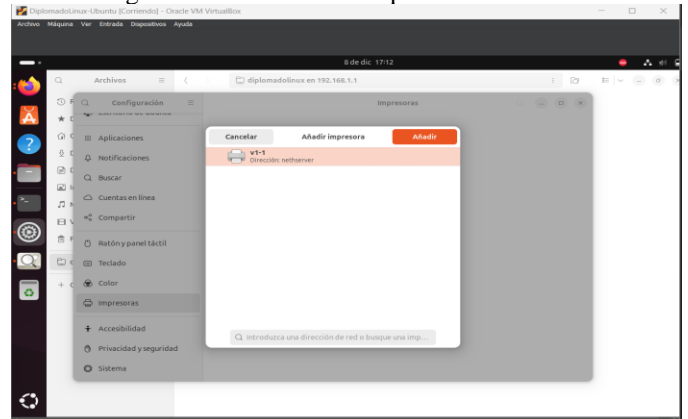


Fuente: Autoría Propia

3.4.16 INSTALACION DE LA IMPRESORA EN EL EQUIPO CLIENTE

Desde la configuración de impresoras del Ubuntu Desktop se busca el impreso y se añade.

Figura 53. Selección de impresora local

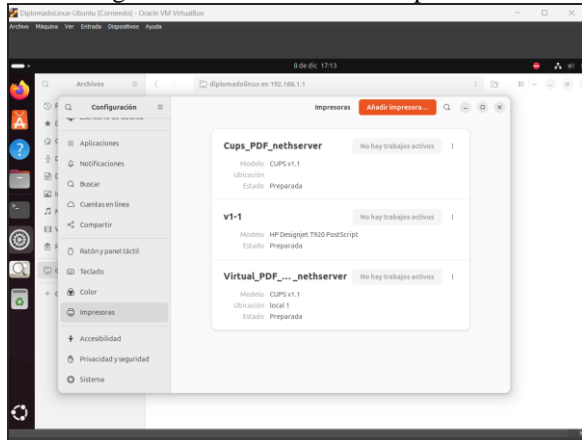


Fuente: Autoría Propia

3.4.17 VISUALIZACION DE LA IMPRESORA INSTALADA Y CON SU RESPECTIVA PRUEBA DE IMPRESIÓN

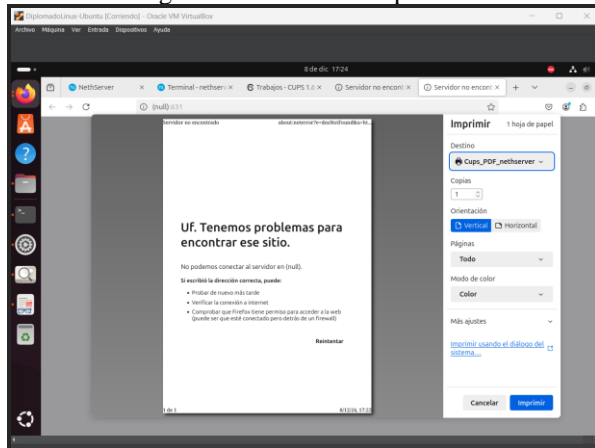
Una vez instalada la impresora se puede visualizar des el panel de configuración de las impresoras del Ubuntu desktop además se hace la prueba imprimiendo desde el navegador.

Figura 54. visualización de impresoras



Fuente: Autoría Propia

Figura 53. Prueba de impresión



Fuente: Autoría Propia

3.5 TEMÁTICA 5: VPN

Producto esperado: 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

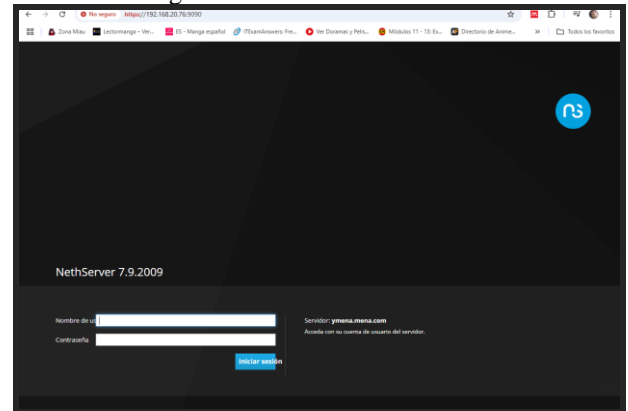
3.5.1 INTRODUCCIÓN

La configuración de una red privada virtual (VPN) permite establecer una conexión segura entre redes o estaciones de trabajo a través de Internet. En este caso, se configuró una VPN en NethServer para permitir el acceso a una estación de trabajo GNU/Linux mediante un túnel privado. A continuación, se detallan los pasos realizados para su configuración.

3.5.2 ACCESO A LA INTERFAZ DE ADMINISTRACIÓN

Una vez terminado el proceso de configuración inicial de NethServer, se accede a la interfaz de administración a través de HTTPS en la dirección <https://192.168.20.76:9090>.

Figura 54. Acceso a NethServer

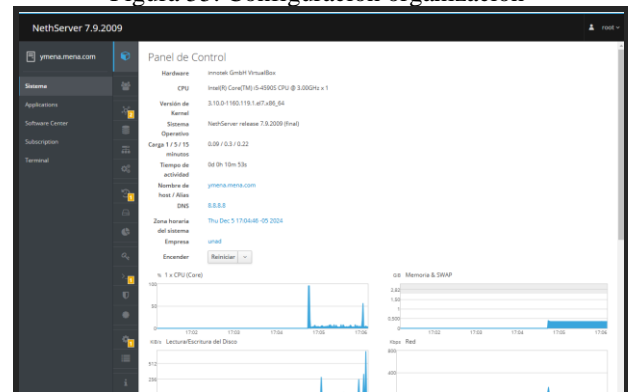


Fuente: Autoría Propia

3.5.3 CONFIGURACIÓN DEL NOMBRE DE LA ORGANIZACIÓN

En la pestaña Sistema, se configura el nombre de la organización, que en este caso se asignó como UNAD.

Figura 55. Configuración organización

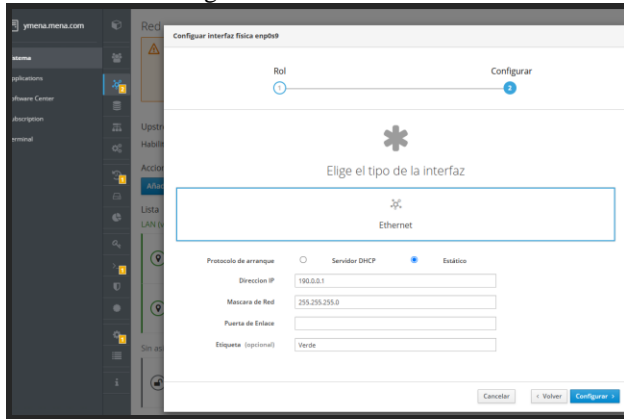


Fuente: Autoría Propia

3.5.4 CONFIGURACIÓN DE REDES (VERDE, ROJA Y NARANJA)

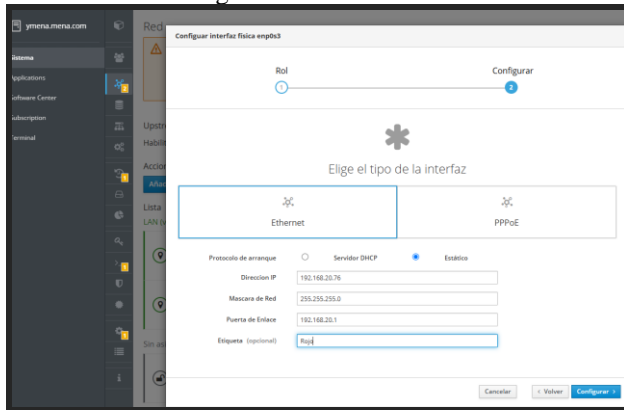
Se configuran las interfaces de red para las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), asignando direcciones IP estáticas:

Figura 56. Red VERDE



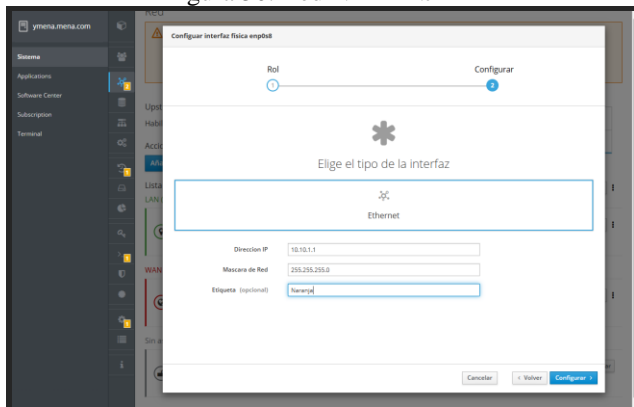
Fuente: Autoría Propia

Figura 57. Red ROJA



Fuente: Autoría Propia

Figura 50. Red NARANJA

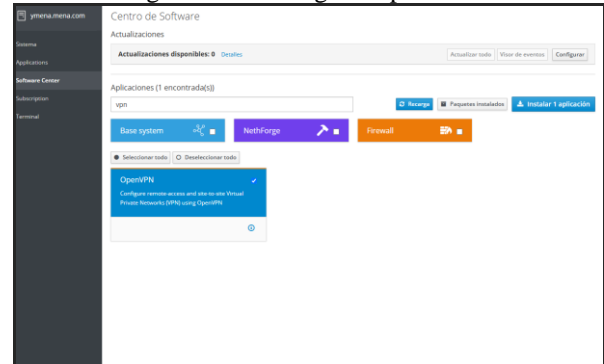


Fuente: Autoría Propia

3.5.5 DESCARGA DE APLICACIONES

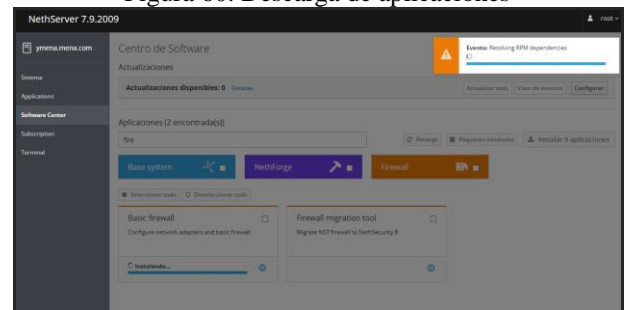
Se procede a la descarga de las aplicaciones necesarias para la configuración de la VPN, como OpenVPN y Basic Firewall.

Figura 59. Descarga de aplicaciones



Fuente: Autoría Propia

Figura 60. Descarga de aplicaciones

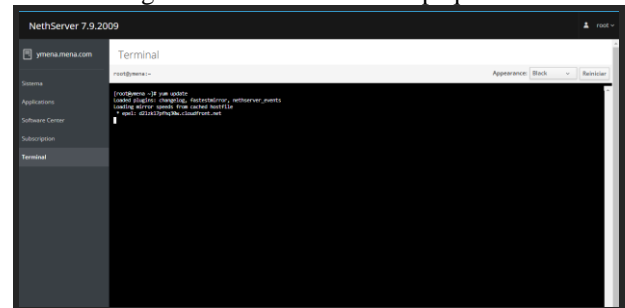


Fuente: Autoría Propia

3.5.6 ACTUALIZACIÓN DE PAQUETES

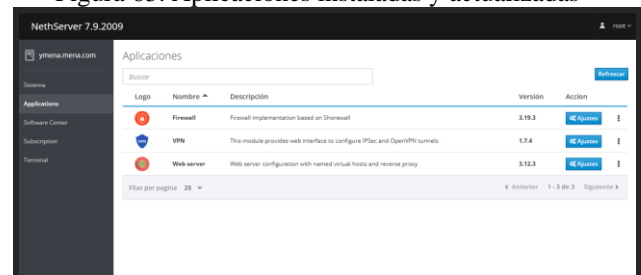
Una vez instaladas las aplicaciones, se actualizan los paquetes mediante el comando yum update. En este caso, no se presentaron actualizaciones disponibles.

Figura 62. Actualización de paquetes



Fuente: Autoría Propia

Figura 63. Aplicaciones instaladas y actualizadas

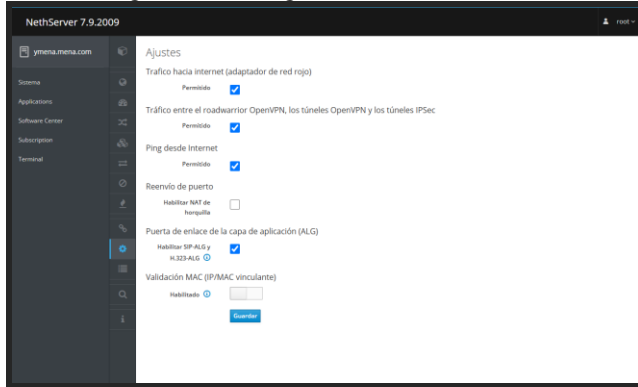


Fuente: Autoría Propia

3.5.7 CONFIGURACIÓN DEL FIREWALL

En la aplicación Firewall, nos dirigimos a la pestaña de ajustes y se selecciona la opción de Tráfico entre el road warrior OpenVPN, los túneles OpenVPN y los túneles IPsec, permitiendo que las conexiones VPN sean gestionadas por el firewall.

Figura 64. Configuración del Firewall

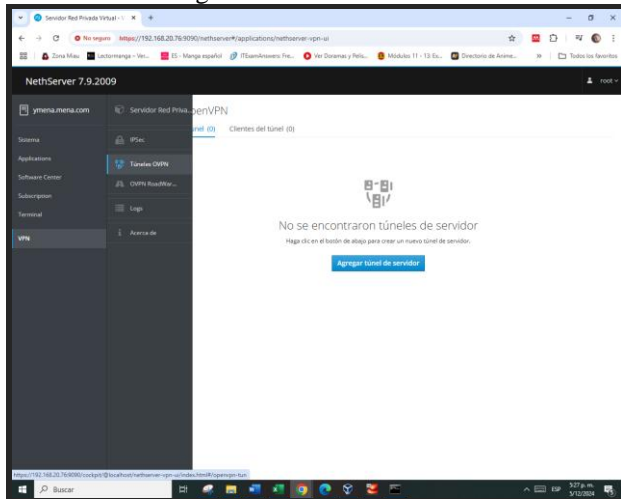


Fuente: Autoría Propia

3.5.8 CREACIÓN DE UN TÚNEL VPN

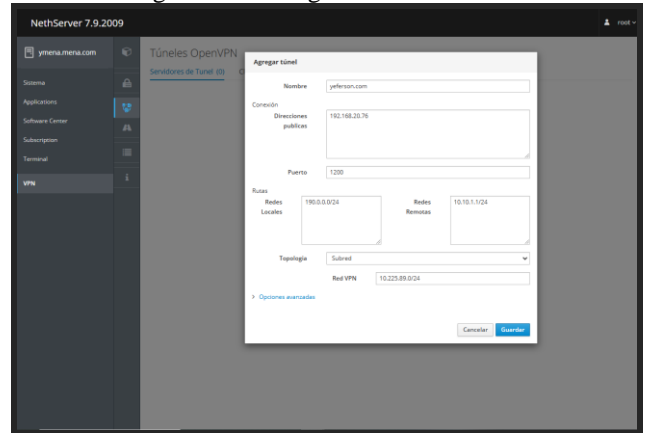
Se procede con la creación de un túnel VPN. Se asigna un nombre al túnel, se agrega la IP de conexión en Direcciones públicas y se definen las rutas remotas. Después de verificar todos los parámetros, se guarda la configuración.

Figura 65. Creación túnel



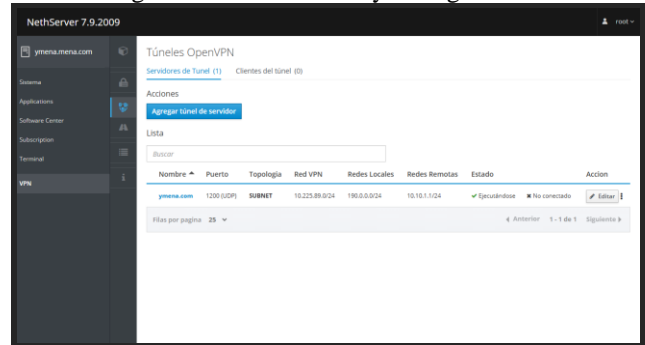
Fuente: Autoría Propia

Figura 66. Configuración del túnel



Fuente: Autoría Propia

Figura 67. Túnel creado y configurado

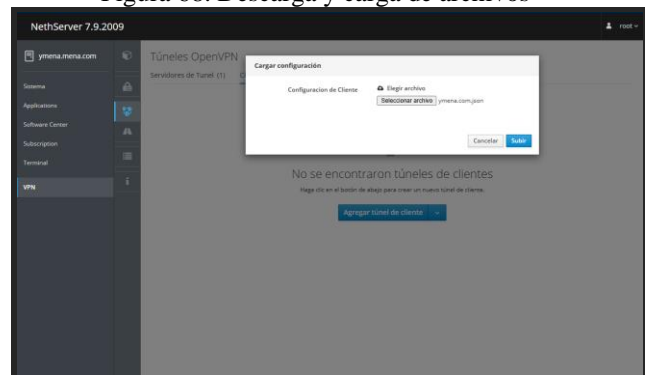


Fuente: Autoría Propia

3.5.9 DESCARGA Y CARGA DEL ARCHIVO DE CONFIGURACIÓN

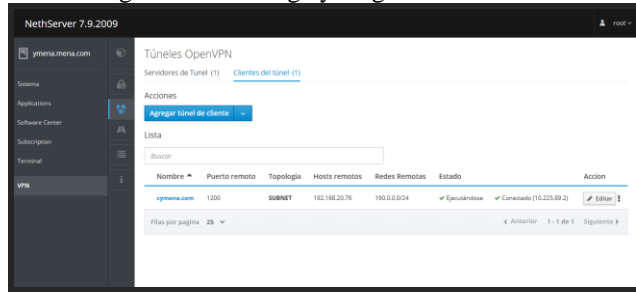
Una vez creado el túnel, se descarga y carga el archivo de configuración correspondiente para el cliente VPN. Si todo está correcto, se muestra que la conexión es exitosa.

Figura 68. Descarga y carga de archivos



Fuente: Autoría Propia

Figura 69. Descarga y carga de archivos

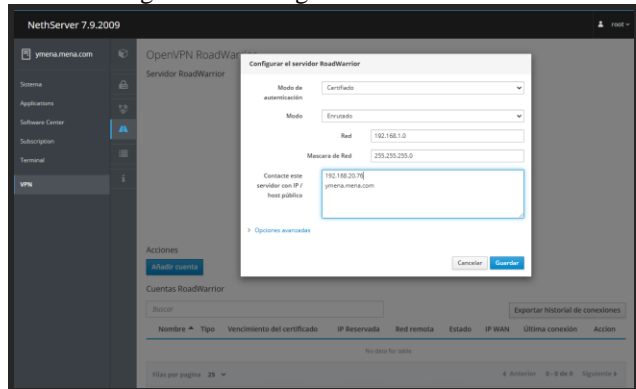


Fuente: Autoría Propia

3.5.10 CONFIGURACIÓN DEL CLIENTE

Se configura el cliente VPN, seleccionando el modo de autenticación, asignando una IP y máscara de red, y configurando la IP de conexión a NethServer (192.168.20.76) junto con su DNS.

Figura 70. Configuración del cliente

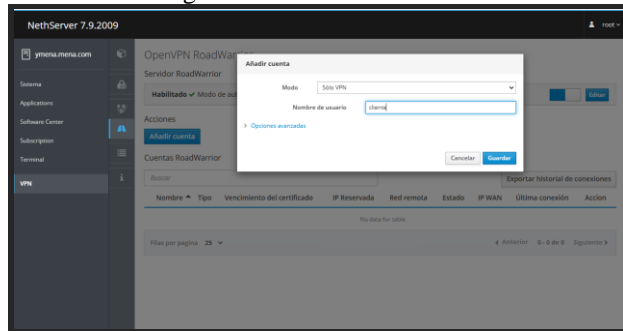


Fuente: Autoría Propia

3.5.11 AÑADIR CUENTA CLIENTE

Se añade una cuenta cliente en la configuración de NethServer.

Figura 71. Cuenta de cliente

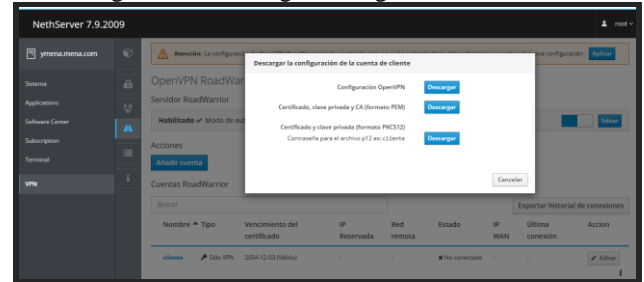


Fuente: Autoría Propia

3.5.12 DESCARGA DE LA CONFIGURACIÓN DEL CLIENTE

Se descarga el archivo de configuración del cliente, permitiendo que el cliente se conecte a NethServer.

Figura 72. Descargar configuración cliente

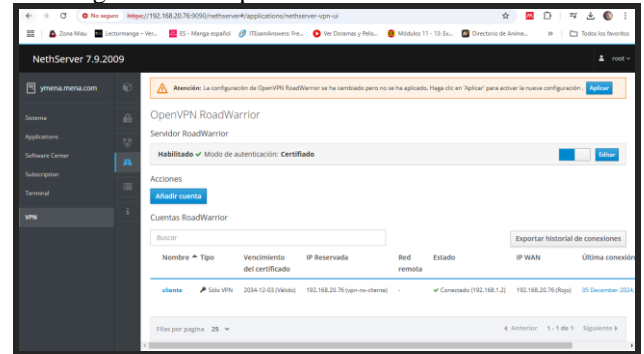


Fuente: Autoría Propia

3.5.13 COMPROBACIÓN DE LA CONEXIÓN

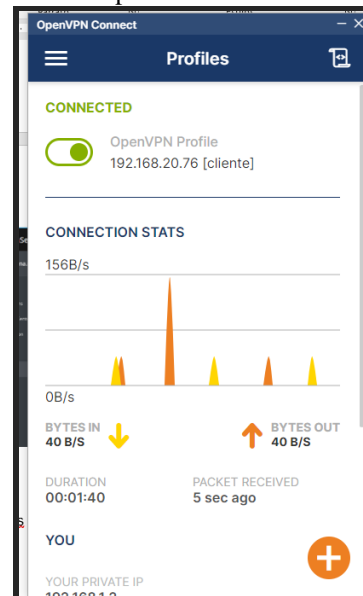
Se verifica que la conexión VPN sea exitosa desde el PC cliente. En la interfaz de NethServer, se muestra el estado de la conexión como "conectado" junto con la fecha de la última conexión.

Figura 73. Comprobación de conexión exitosa



Fuente: Autoría Propia

Figura 74. Comprobación de conexión exitosa



Fuente: Autoría Propia

4 Conclusiones.

Se logró implementar y configurar de manera exitosa los servicios de DHCP, DNS y el Controlador de Dominio en NethServer, lo que permitió una administración más eficiente de la infraestructura de red. Con el DHCP, se automatizó la asignación de direcciones IP a los dispositivos de la red, evitando la necesidad de configuración manual. El servidor DNS optimizó la resolución de nombres, facilitando el acceso a recursos tanto internos como externos. Además, la implementación del Controlador de Dominio centralizó la autenticación de usuarios y la gestión de permisos, mejorando la seguridad y organización de la red.

La configuración del servidor proxy en NethServer permitió un control más riguroso sobre el acceso a Internet desde la red interna. Al establecer filtros a través del puerto 3128, se consiguió bloquear el acceso a sitios no deseados y proteger la red de posibles amenazas. Esto se tradujo en un manejo eficiente del tráfico saliente, restringiendo el acceso a contenidos no autorizados y ayudando a mantener un entorno de trabajo seguro y optimizado en términos de ancho de banda.

La implementación y configuración del cortafuegos en NethServer permitió aplicar reglas precisas para bloquear el acceso a sitios web de entretenimiento y redes sociales, lo que mejoró notablemente la seguridad de la red. Las políticas de control de tráfico fueron establecidas de forma detallada y validadas correctamente desde una estación de trabajo GNU/Linux. Gracias a estas medidas, se garantizó que solo el tráfico autorizado pudiera ingresar a la red, protegiéndola de accesos no deseados y fortaleciendo la infraestructura contra posibles amenazas externas.

La configuración de los servicios de servidor de archivos y servidor de impresoras en NethServer facilitó la centralización del acceso a recursos compartidos y dispositivos de impresión en la red. Mediante el uso de LDAP para la autenticación, los usuarios pudieron acceder de forma segura a las carpetas y a las impresoras de manera centralizada, optimizando los flujos de trabajo. Esta implementación no solo mejoró la colaboración entre los miembros de la red, sino que también redujo la dependencia de recursos locales, haciendo más eficiente la administración de los recursos compartidos.

La configuración de una VPN en NethServer permitió establecer una conexión segura y privada entre la red interna y las estaciones de trabajo remotas. Esto facilitó el acceso a recursos de la red mediante un túnel cifrado, garantizando la confidencialidad y seguridad de las comunicaciones. La implementación de la VPN permitió a los usuarios acceder a aplicaciones y contenido de la red de manera remota, protegiendo la información y manteniendo la integridad de los datos a través de una conexión segura.

5 REFERENCIAS

- [1] LPI LPIC-1 Exam 102. (2022). Tema 110: Seguridad. Linux Professional Institute. <https://learning.lpi.org/es/learning-materials/102-500/110/>
- [2] Canonical. (2018). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>

- [3] Debian. (2020). El manual del administrador de Debian 12.5.0. Debian. <https://www.debian.org/releases/stable/amd64/index.es.html>
- [4] Oracle. (2020). Manual de usuario VirtualBox. VirtualBox. <https://www.virtualbox.org/manual/>
- [5] Gómez-Marí, I., & Pedrosa-Sáez, A. (2023). La educación en la era del metaverso. ¿Está la comunidad educativa preparada?: Análisis de las actitudes y el conocimiento del alumnado, docentes y familias hacia la inclusión del metaverso en la educación. EducaT: Educación Virtual, Innovación Y Tecnologías, 4(1), 3-44. <https://hemeroteca.unad.edu.co/index.php/educat/article/view/6571/6473>
- [6] NethServer. (2020, septiembre 9). ISO 7.9.2009 release. GitHub. <https://github.com/NethServer/dev/releases/tag/iso-7.9.2009>
- [7] Cabrera Caballero, M. (2018, septiembre 12). NethServer tutorial | Instalación, actualización y primeros pasos [Video]. YouTube. https://www.youtube.com/watch?v=FNGmM-2fa_0&ab_channel=ManuelCabreraCaballero
- [8] LPI LPIC-1 Exam 102. (2022). Tema 107: Tareas administrativas. Linux Professional Institute. <https://learning.lpi.org/es/learning-materials/102-500/107/>