IMPLEMENTACIÓN, CONFIGURACIÓN Y APROVISIONAMIENTO DE SERVICIOS UTILIZANDO NETHSERVER

Luis Miguel Hurtado Muñoz
e-mail: lmhurtadomu@unadvirtual.edu.co
Francisco Javier Rendón Arroyave
e-mail: fjrendona@unadvirtual.edu.co
Jonh Freddy Osses Castro
e-mail: jfossesca@unadvirtual.edu.co
Edwin Yohanni Barrios Martínez
e-mail: eybarriosm@unadvirtual.edu.co
Gueynen Jhoan Mestra Florez
e-mail: gmestraf@unadvirtual.edu.co

RESUMEN: *En este trabajo, se aborda la implementación y configuración de servicios de infraestructura IT esenciales para la administración y control de una red compleja en entornos con múltiples usuarios y dispositivos. Se utiliza NethServer, una distribución de Linux basada en CentOS que ofrece una interfaz web intuitiva para la gestión de diversos servicios de red.*

Las temáticas abordadas incluyen: DHCP Server: Asignación dinámica de direcciones IP a los dispositivos de la red., DNS Server: Traducción de nombres de dominio en direcciones IP, Controlador de Dominio: Autenticación y autorización de usuarios y dispositivos en la red, Proxy: Control del acceso a Internet y filtrado de contenido, Cortafuegos: Restricción del acceso a la red y protección contra amenazas, File Server: Compartir carpetas con los usuarios de la red, Print Server: Compartir impresoras con los usuarios de la red y VPN: Creación de un túnel privado de comunicación para el acceso remoto seguro a la red..

PALABRAS CLAVE: DHCP, DNS, NETHSERVER, VPN, CORTAFUEGOS, PROXY, FILESERVER, PRINT SERVER, LDAP.

1 INTRODUCCIÓN

En el presente trabajo se abordará la implementación y configuración de diversos servicios de gestión de infraestructura IT utilizando NethServer, enfocados en mejorar la administración y seguridad de redes corporativas. Se detallarán cinco temáticas principales: la configuración de un servidor DHCP, DNS y un controlador de dominio que permitirá el acceso y registro de estaciones de trabajo GNU/Linux; la implementación de un servidor proxy para controlar el acceso a Internet filtrando el tráfico por el puerto 3128; y la configuración de un cortafuegos para restringir el acceso a sitios de entretenimiento y redes sociales desde una estación GNU/Linux.

Además, se explicará cómo configurar un servidor de archivos y de impresión, facilitando el acceso a carpetas compartidas y servicios de impresión a través de un controlador de dominio LDAP. Finalmente, se describirá la creación de una VPN para establecer un túnel de comunicación seguro entre una estación de trabajo GNU/Linux y la red corporativa, garantizando la privacidad y la integridad de los datos transmitidos. Este enfoque integral permitirá una gestión eficiente y segura de la infraestructura IT utilizando NethServer.

2 DESCARGA E INSTALACIÓN NETHSERVER

2.1 DESCARGA

Para iniciar el proceso, se debe descargar la imagen ISO desde la URL https://github.com/NethServer/dev/releases/tag/iso-7.9.2009.

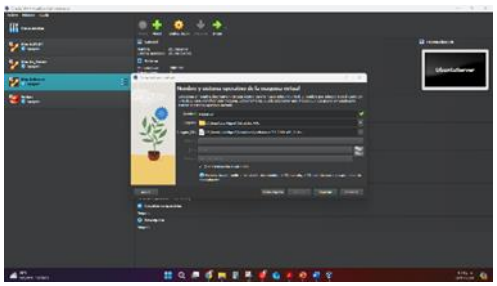
Figura 1. Descarga de imagen ISO NethServer

Fuente: Autoría propia

2.2 CONFIGURACIÓN MÁQUINA VIRTUAL

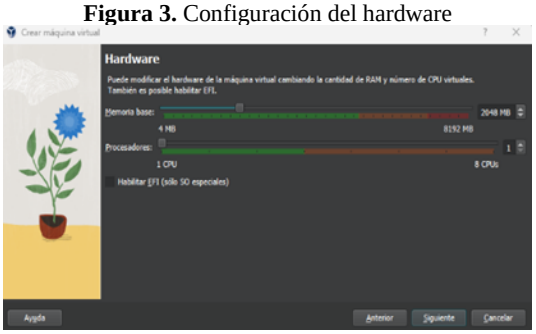
Luego, se debe configurar la máquina virtual en VirtualBox.

Figura 2. Creación de MV para NethServer



Fuente: Autoría propia

Figura 3. Configuración del hardware

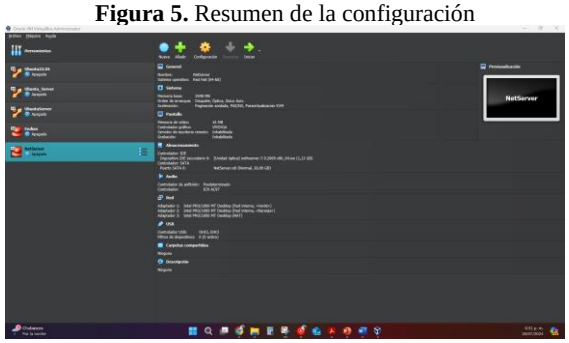


Fuente: Autoría propia

Figura 4. Configuración del Disco Duro

Fuente: Autoría propia

Figura 5. Resumen de la configuración

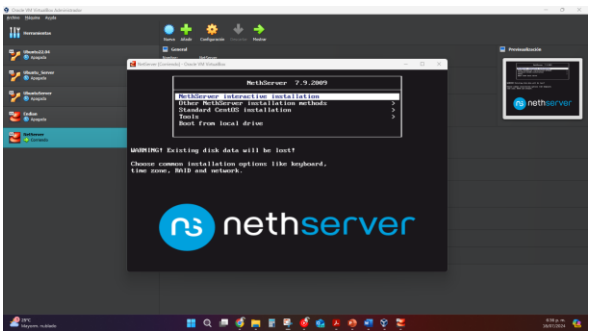


Fuente: Autoría propia.

2.3 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE NETHSERVER

A continuación, se procederá con la instalación recomendada de NethServer, siguiendo cada uno de los pasos solicitados [2].

Figura 6. Inicio de la instalación



Fuente: Autoría propia

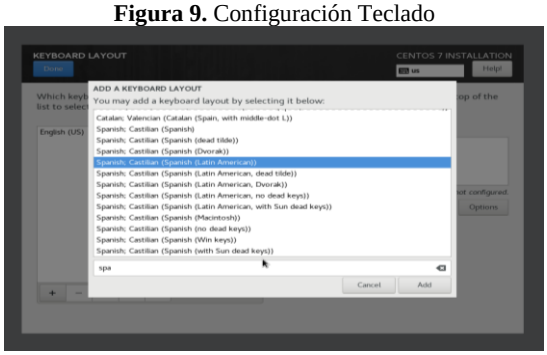
Figura 7. Configuración inicial

Fuente: Autoría propia.

Figura 8. Configuración Zona Horaria

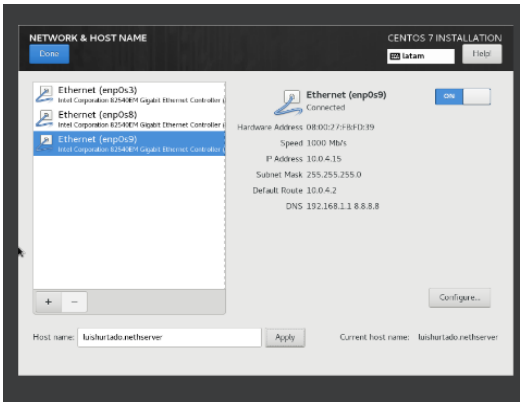
Fuente: Autoría propia.

Figura 9. Configuración Teclado



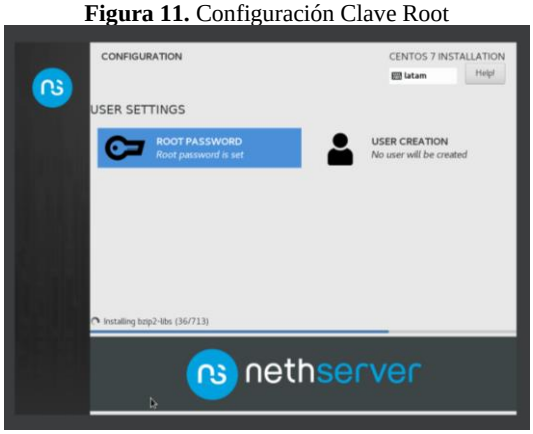
Fuente: Autoría propia.

Figura 10. Configuración Hostname



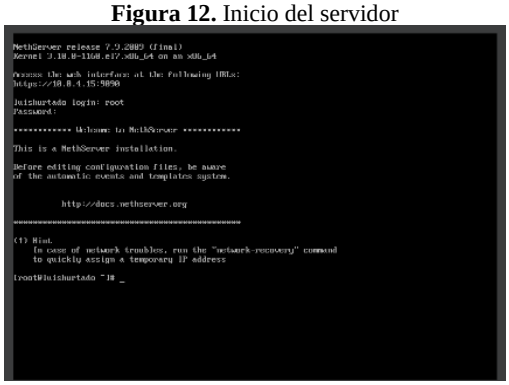
Fuente: Autoría propia

Figura 11. Configuración Clave Root



Fuente: Autoría propia.

Figura 12. Inicio del servidor



Fuente: Autoría propia.

3 TEMÁTICAS

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

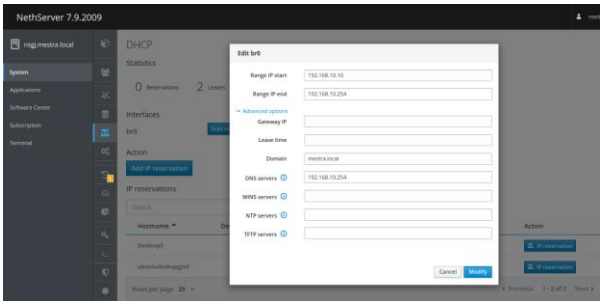
En el dinámico panorama de las redes informáticas, DHCP, DNS y controladores de dominio se erigen como pilares fundamentales que garantizan la conectividad y la gestión eficiente de los recursos [9].

El Protocolo de Configuración Dinámica de Host (DHCP) automatiza la asignación de direcciones IP, simplificando la configuración de dispositivos y evitando conflictos de direcciones.

Por su parte, el Sistema de Nombres de Dominio (DNS) traduce nombres de dominio legibles por humanos en direcciones IP numéricas, facilitando la navegación por Internet.

Los controladores de dominio, en tanto, centralizan la administración de usuarios, grupos y recursos de una red, proporcionando un punto de control único y mejorando la seguridad.

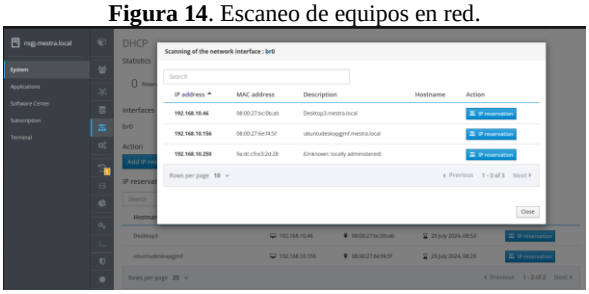
Figura 13. Configuración rango de IP**.**



Fuente: Autoría propia.

Esta configuración permite definir el rango de IP y de servidores que prestan los servicios como domino, y DNS.

Figura 14. Escaneo de equipos en red.



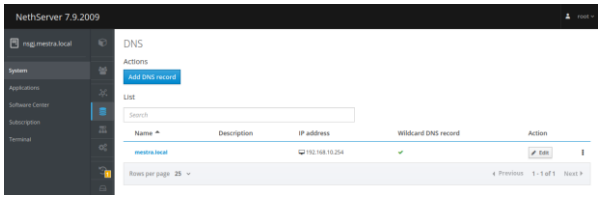
Fuente: Autoría propia.

El escaneo de red muestra todos los equipos activos del rango de ip configurado.

Figura 15. Visualización de equipos en el DHCP.

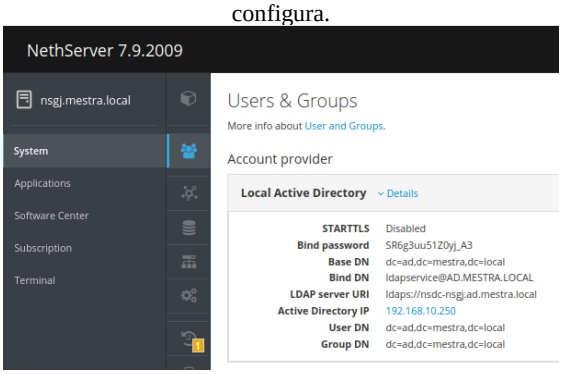
Fuente: Autoría propia.

Figura 16. Visualización de DNS configurado.



Fuente: Autoría propia.

Figura 17. Controlador de domino e información que lo configura.



Fuente: Autoría propia.

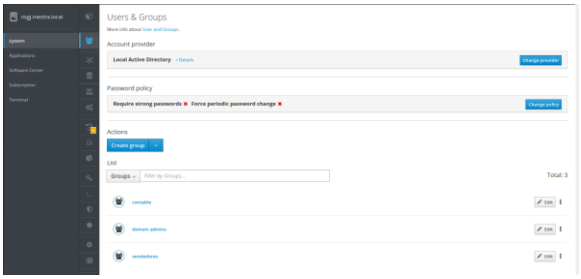
El controlador de domino se configura con LDAP el cual va a permitir el acceso de usuarios y equipos a los recursos del dominio [10].

Figura 18. Visualización de usuarios.

Fuente: Autoría propia.

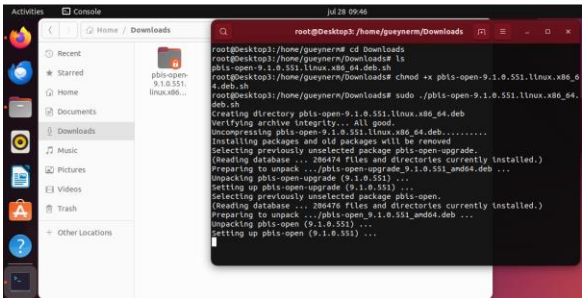
Esta herramienta del controlador de dominio permite administrar los usuarios por medio de claves, haciéndolo de forma ordenada.

Figura 19. Visualización de Grupos.



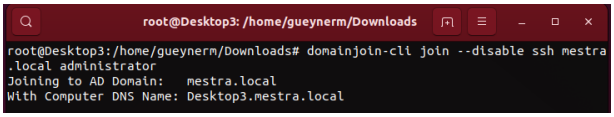
Fuente: Autoría propia.

Figura20: Instalación pbis-open para conexión del cliente.



Fuente: Autoría propia.

Figura 20. Conectando con el domino.



Fuente: Autoría propia.

El conectarse a un dominio proporciona una infraestructura de red más segura, eficiente y fácil de administrar. Es especialmente beneficioso para organizaciones de cualquier tamaño que necesiten gestionar una gran cantidad de usuarios y dispositivos.

3.2 TEMÁTICA 2: PROXY

Para lograr un control granular del acceso a internet desde una estación GNU/Linux, se implementó un esquema que involucra a NethServer como servidor central y un proxy con filtrado en el puerto 3128. El proceso se llevó a cabo de la siguiente manera:

Acceso a la interfaz web de NethServer: Se utilizó un navegador web en la máquina Ubuntu Desktop para acceder a la interfaz de administración de NethServer. Para ello, se empleó la dirección IP correspondiente a la red LAN (Verde) junto con las credenciales del usuario root [1].

Visualización del módulo del sistema: Una vez autenticado en la interfaz web, se presentó el módulo del sistema, el cual ofrece una vista general del estado y la configuración básica del servidor NethServer.

Figura 21. Ingreso con usuario root y clave

Fuente: Autoría propia.

En esta etapa, se procede a configurar las distintas redes que permitirán la conexión de los dispositivos. Se inicia con la

configuración de la red WAN (Roja), que dará acceso a internet.

Para ello, se selecciona la red WAN y se procede a asignarle una dirección IP, máscara de red y puerta de enlace. La puerta de enlace juega un rol fundamental, ya que es la que facilita el acceso a internet a los dispositivos conectados a la red.

Figura 22. Verificación de las redes

Fuente: Autoría propia.

Una vez finalizada la configuración de las redes y la asignación de direcciones IP, se procede a la etapa de configuración del Web Proxy para el filtrado de contenido web. Este proceso involucra la instalación de la aplicación "Filtro web" y el "Proxy web" desde el panel Software Center.

Para llevar a cabo la instalación, se siguen los siguientes pasos:

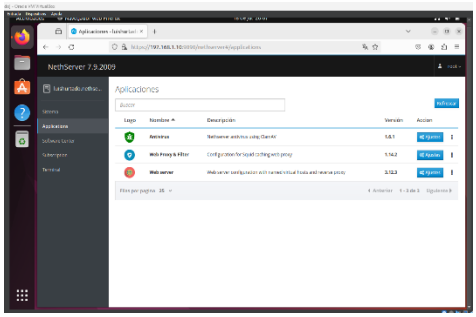
Acceso al Software Center: Se ingresa al panel Software Center ubicado en la interfaz gráfica del sistema.

Búsqueda de aplicaciones: Se procede a buscar las aplicaciones "Filtro web" y "Proxy web" utilizando la barra de búsqueda del Software Center.

Instalación de aplicaciones: Una vez localizadas las aplicaciones, se selecciona y se inicia el proceso de instalación.

Ubicación de las aplicaciones instaladas: Tras finalizar la instalación, las aplicaciones "Filtro web" y "Proxy web" estarán disponibles en el Panel Aplicaciones.

Figura 23. Verificación de instalación de Proxy web y Filtro web



Fuente: Autoría propia.

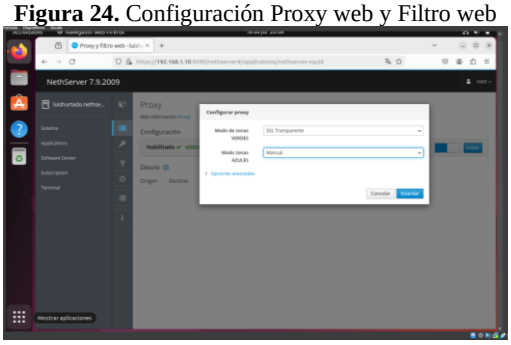
A continuación, se procede a configurar el Proxy a través del panel Web Proxy y Filter. Para ello, se deben seguir los siguientes pasos:

Acceso al panel Web Proxy y Filter: Se ingresa al panel Web Proxy y Filter desde la interfaz web de NethServer.

Configuración del Modo Zonas VERDES: En el apartado correspondiente al Modo Zonas VERDES, se selecciona la opción "SSL Transparente". Esta configuración permitirá que el tráfico web de las zonas verdes se filtre a través del proxy de manera transparente para los usuarios.

Configuración del Modo Zonas AZULES: En el apartado correspondiente al Modo Zonas AZULES, se mantiene la configuración por defecto, la cual es "Manual". Esto significa que los usuarios en las zonas azules deberán configurar manualmente su navegador para utilizar el proxy.

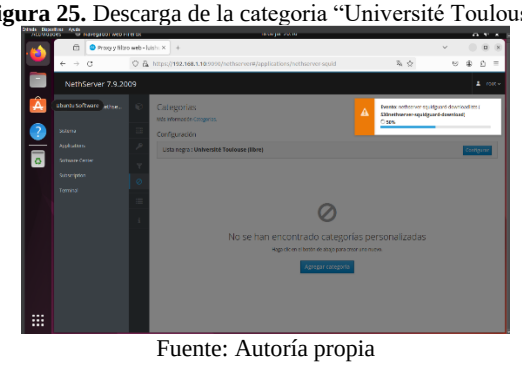
Figura 24. Configuración Proxy web y Filtro web



Fuente: Autoría propia

Posteriormente, se accede al panel Web Proxy y Filter y se dirige a la sección Categorías. Desde allí, se descarga e instala la lista de categorías deseada. En este caso, se selecciona la categoría "Université Toulouse (free)", la cual permite aplicar filtros a un conjunto de páginas web predefinidas por categorías [3].

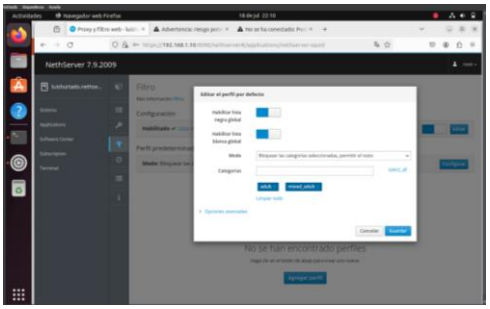
Figura 25. Descarga de la categoria “Université Toulouse”



Fuente: Autoría propia

A continuación, se accede al panel Web Proxy y Filter y se dirige a la sección Filtro. Desde allí, se selecciona las categorías que se desean bloquear y se establece el modo de filtrado que se aplicará.

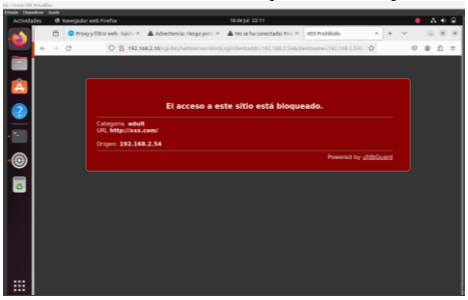
Figura 26. Configuración de los filtros



Fuente: Autoría propia

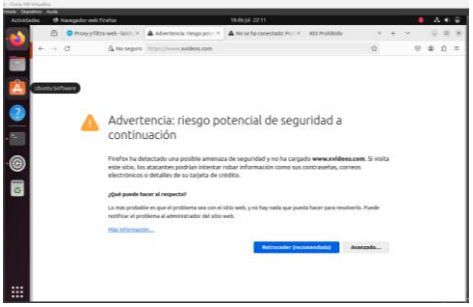
Para verificar que el proxy esté filtrando correctamente las categorías bloqueadas, se realiza una prueba de acceso desde un navegador web. Se intenta acceder a páginas web que contengan contenido para adultos o juegos de azar. Si el proxy está funcionando correctamente, estas páginas no deberían ser accesibles.

Figura 27. Verificación del bloqueo exitoso para url http



Fuente: Autoría propia

Figura 28. Verificación del bloqueo exitoso para url https



Fuente: Autoría propia.

3.3 TEMÁTICA 3: CORTAFUEGOS

Configuración y puesta en marcha detallada para limitar el acceso a sitios web de entretenimiento y redes sociales, mostrando las reglas y políticas implementadas. La comprobación de la efectividad del cortafuegos con las restricciones aplicadas se realizará desde una estación de trabajo con sistema operativo GNU/Linux (Ubuntu Desktop).

Una vez garantizado el correcto funcionamiento del sistema central en NethServer, se procederá con la configuración de las redes según la topología: WAN como Red Roja, LAN como Red Verde y DMZ como Red Naranja [2].

Figura 29. Ingreso a dashboard de NethServer

Fuente: Autoría propia.

Figura 30. Selección de configuración para red WAN

Fuente: Autoría propia

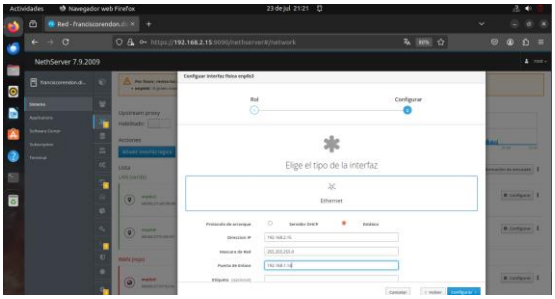
Figura 31. Asignación protocolo DHCP para red WAN

Fuente: Autoría propia.

Figura 32. Selección de configuración para red LAN

Fuente: Autoría propia

Figura 33. Asignación de dirección IP para red LAN



Fuente: Autoría propia

Figura 34. Selección de configuración para red DMZ

Fuente: Autoría propia

Figura 35. Asignación de dirección IP para red DMZ

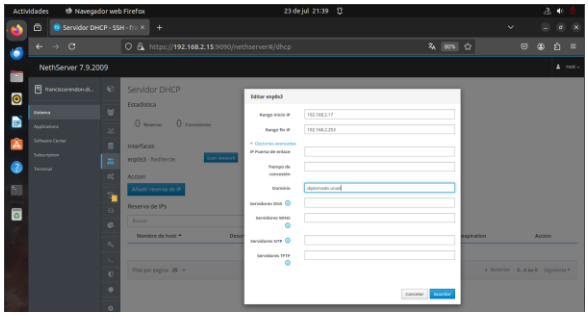
Fuente: Autoría propia.

Figura 36. Vista de configuración de redes

Fuente: Autoría propia.

Para asegurar el correcto funcionamiento del servidor DHCP, se configurarán los rangos de direcciones IP que asignará a la LAN o Red Verde [3].

Figura 37. Asignación de rango de direcciones IP en el servidor DHCP



Fuente: Autoría propia.

Después de este proceso, se reiniciará la NIC de la estación de trabajo para que el servidor DHCP realice la asignación correspondiente. Una vez asignada la dirección IP dentro del segmento de red de la LAN, se probará el acceso a cualquier página de internet. En este caso práctico, se ingresará a la red social Facebook para validar su acceso.

Figura 38. Verificación de acceso a internet y redes sociales

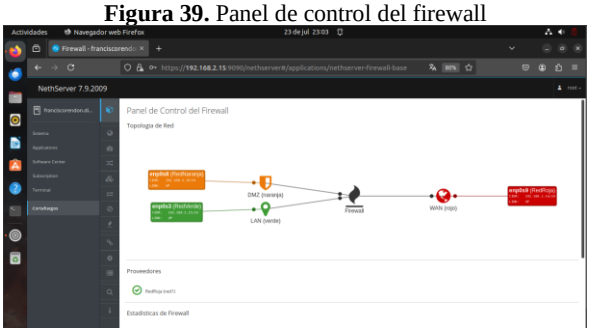
Fuente: Autoría propia.

Para comenzar la instalación del cortafuegos, se accederá al dashboard de NethServer y se dirigirá a la sección "Software Center". Allí se buscará la aplicación "Firewall Básico" y se hará clic en "Instalar" [8].

Una vez completada la instalación, desde la sección "Aplicaciones", se podrá visualizar la aplicación y, opcionalmente, crear un acceso directo.

Dentro del cortafuegos, inicialmente se verá la topología de red configurada en el panel de control, donde se representarán todas las zonas de red configuradas y, en el centro de la topología, el cortafuegos.

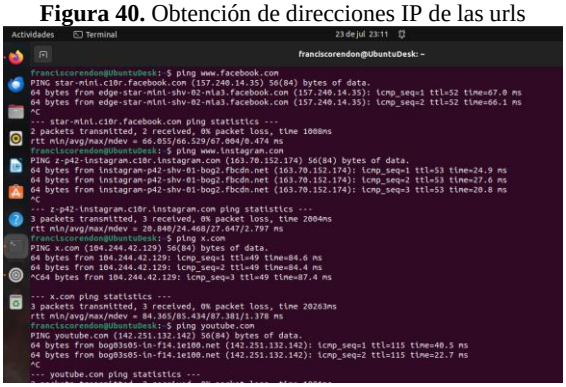
Figura 39. Panel de control del firewall



Fuente: Autoría propia.

Antes de crear las reglas de denegación de servicio, es necesario identificar las direcciones IP a las que se dirige el tráfico de los sitios web que se desean bloquear. Para ello, desde la terminal, se puede ejecutar el comando ping a cada una de las URLs.

Figura 40. Obtención de direcciones IP de las urls



Fuente: Autoría propia.

Una vez identificada la dirección IP o el segmento de red, se procederá a crear la regla desde el submenú Reglas. En esta sección, se deben especificar los siguientes parámetros:

Origen: la fuente desde la cual se realiza la petición de acceso a la URL.
Destino: la dirección IP a la que apunta el sitio.
Servicio: en este caso, se seleccionará HTTPS.
Acción: en este caso, se elegirá Rechazar.

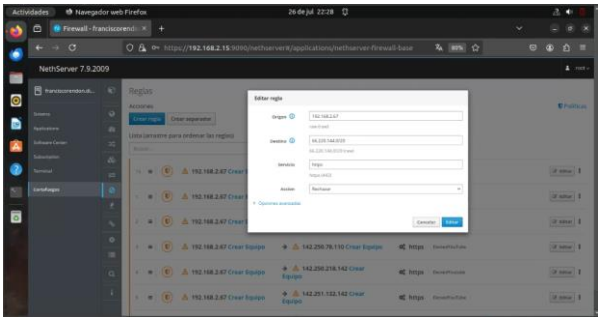
Tras configurar estos parámetros, se hará clic en el botón Guardar. Luego, se deberá hacer clic en el botón Aplicar, ubicado en la parte superior del dashboard, para que la regla surta efecto.

Es importante mencionar que algunos sitios web utilizan varias direcciones IP por motivos de redundancia, balanceo de carga, escalabilidad y disponibilidad del servicio. Para estos casos, se recomienda utilizar el comando nslookup seguido de la URL para identificar todos los segmentos de red utilizados por el sitio y así crear las reglas correspondientes [8].

Figura 41. Creación de regla para el sitio Instagram

Fuente: Autoría propia.

Figura 42. Creación de regla para el sitio Facebook

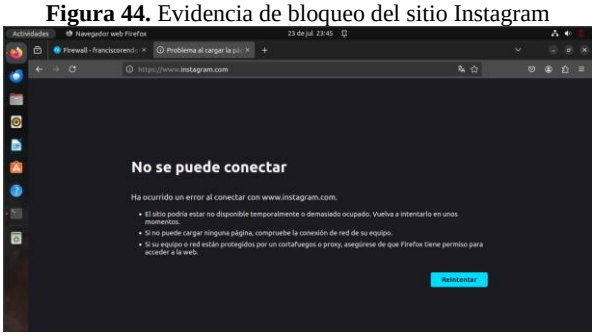


Fuente: Autoría propia.

Figura 43. Creación de regla para el sitio Spotify

Fuente: Autoría propia.

Figura 44. Evidencia de bloqueo del sitio Instagram

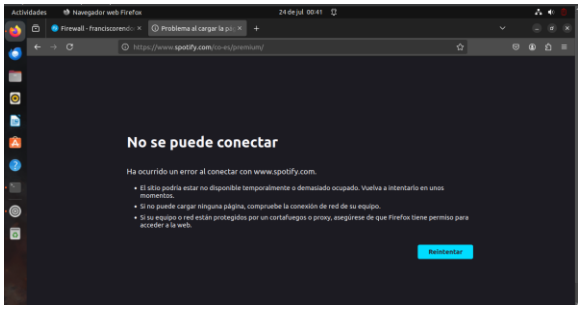


Fuente: Autoría propia.

Figura 45. Evidencia de bloqueo del sitio Facebook

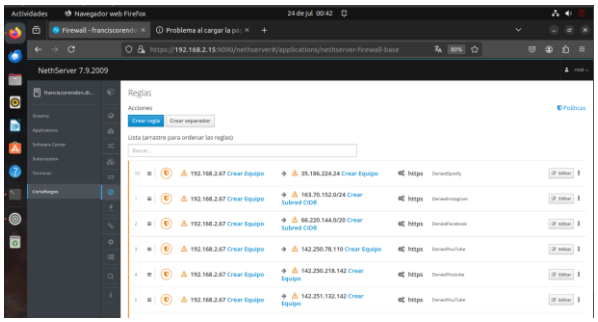
Fuente: Autoría propia.

Figura 46. Evidencia de bloqueo del sitio YouTube



Fuente: Autoría propia.

Figura 47. Evidencia de bloqueo del sitio Spotify



Fuente: Autoría propia.

Este proceso se puede repetir tantas veces como sea necesario para crear la denegación de servicio a los sitios que no estarían permitidos dentro de la organización.

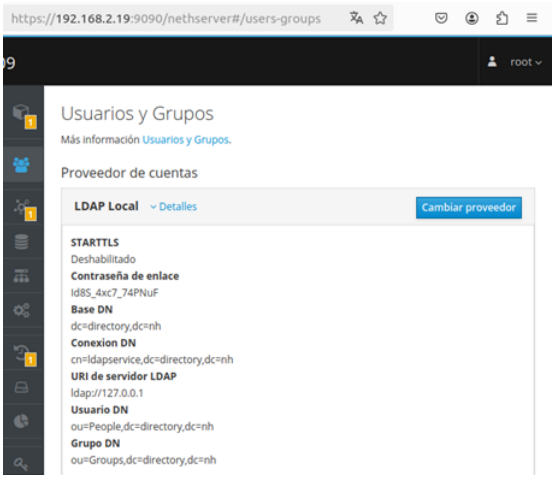
3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

A continuación, se dará a conocer el paso a paso del procedimiento realizado para configurar el servidor de archivos y el servidor de impresión a través de NethServer, distribución basada en Linux orientada específicamente a actuar como servidor en pequeñas y medianas oficinas.

Se realiza configuración del protocolo de acceso a directorios ligeros (LDAP), que permite que los usuarios encuentren información sobre las empresas y las personas, entre otros datos, y tiene como objetivos principales: almacenar estos datos en su directorio y autorizar a los usuarios para que puedan acceder a él.

Para ello vamos a la opción “Usuarios y Grupos”, seleccionamos LDAP, luego LDAL local, y finalmente aceptamos la descarga y configuración del servidor OpenLDAP.

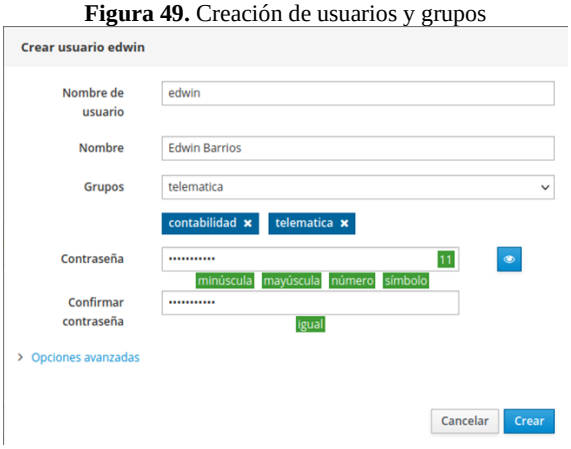
Figura 48. Configuración LDAP



Fuente: Autoría propia.

Se crean usuarios y grupos según las necesidades de la organización.

Figura 49. Creación de usuarios y grupos



Fuente: Autoría propia.

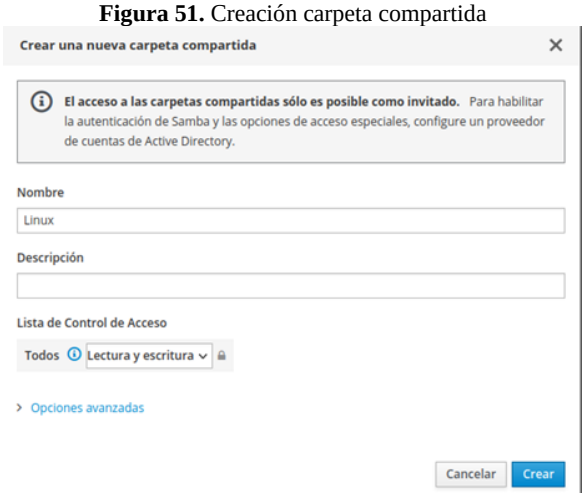
Se instalan los paquetes File Server y Print Server ubicados en la opción “Software Center”, los cuales, luego de su instalación, pueden ser verificados en la opción “Applications”.

Figura 50. Descarga de paquetes

Fuente: Autoría propia.

Para crear una carpeta compartida, se accede a la aplicación de File Server, luego Ajustes, luego Crear una carpeta compartida, se define nombre y tipo de acceso, y finalmente Crear. Para hacer seguimiento a archivos compartidos por invitados se da la opción Auditoria [11].

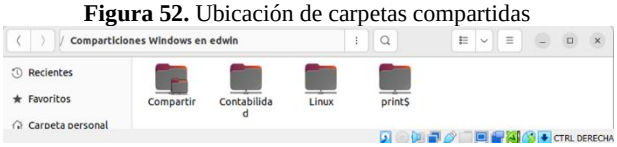
Figura 51. Creación carpeta compartida



Fuente: Autoría propia.

Para comprobar que las carpetas de archivos e impresión fueron creadas y configuradas de manera correcta, se accede al directorio del sistema operativo y en la opción "Otras ubicaciones", se pueden apreciar las carpetas.

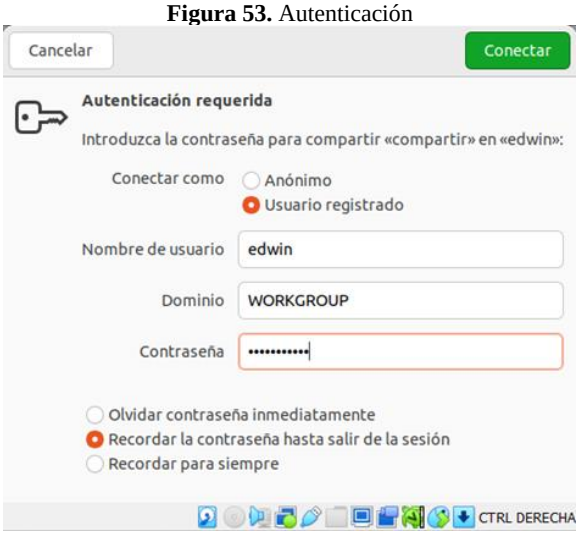
Figura 52. Ubicación de carpetas compartidas



Fuente: Autoría propia.

Al tratar de acceder a una de estas carpetas compartidas, el sistema nos solicita nos autentiquemos con usuario y contraseña.

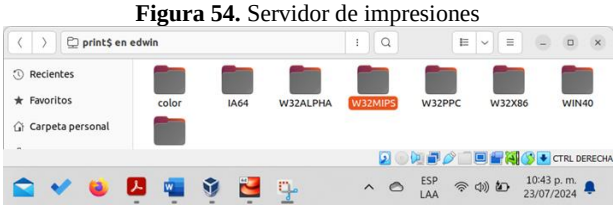
Figura 53. Autenticación



Fuente: Autoría propia.

Al acceder a la carpeta de servidor de impresiones, se aprecia que el sistema crea automáticamente carpetas con nombres preestablecidos, correspondientes al espacio generado para alojar controladores de impresoras que se pretendan instalar.

Figura 54. Servidor de impresiones



Fuente: Autoría propia.

NethServer fue configurada con diferentes adaptadores, uno de ellos para el acceso a internet, y los restantes para el acceso a la zona naranja, donde se encontraba nuestro servidor DHCP, y una zona verde para acceder a los clientes.

Dependiendo de las necesidades del usuario o de la organización, NethServer dispone de una opción para la instalación de paquetes "Software Center", que permite instalar aplicaciones que van desde bases de datos hasta mensajería instantánea.

Para compartir archivos se puede hacer de manera anónima o a través de la autenticación de uno de los usuarios creados por el controlador de dominio LDAP.

3.5 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

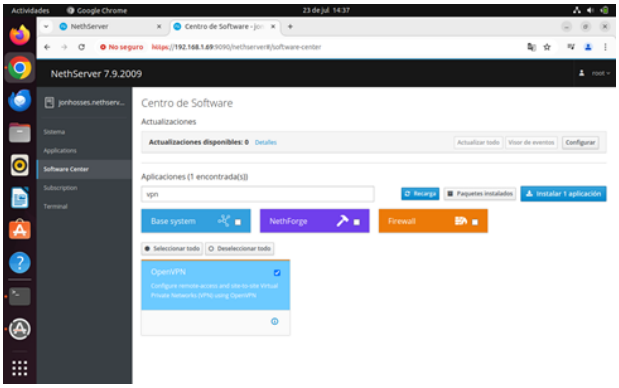
El enfoque principal es la implementación y configuración de una VPN utilizando NethServer, una distribución basada en CentOS, diseñada para gestionar servicios de red de forma sencilla y eficiente. La VPN permitirá establecer un túnel de comunicación seguro con una estación de trabajo GNU/Linux, garantizando la seguridad y facilitando el acceso remoto a los recursos internos de la organización utilizando el servidor OpenVPN en modo RoadWarrior que permite tener una conexión VPN con varios clientes [6].

Se demostrará cómo la correcta configuración de NethServer y una VPN puede resolver problemas de conectividad y seguridad en redes complejas, mejorando la productividad y la colaboración entre los usuarios.

Se iniciará con el proceso de instalación de OpenVPN en NethServer

En la sección de Software Center de NethServer, buscar la opción de VPN y seleccionar OpenVPN para realizar la instalación.

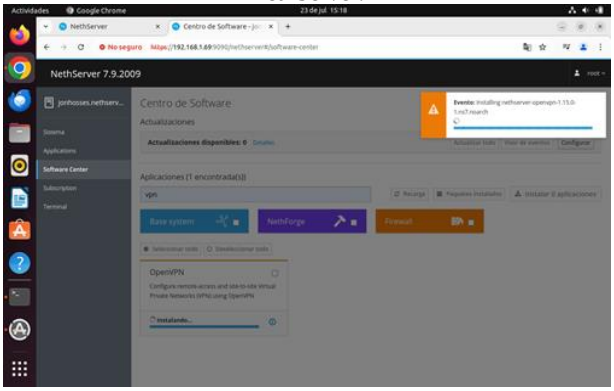
Figura 55. Búsqueda de OpenVPN en software center de NethServer



Fuente: Autoría propia.

Instalar la aplicación OpenVPN.

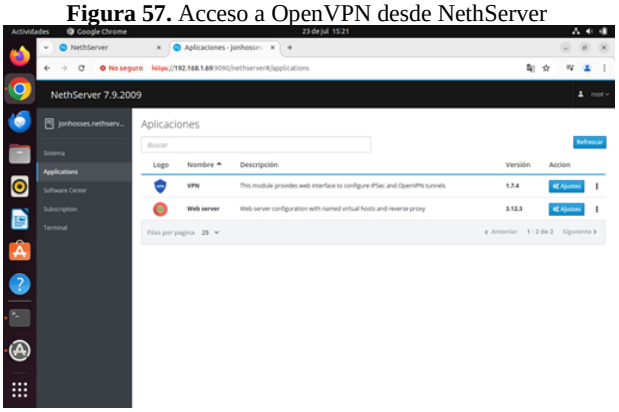
Figura 56. Instalación de OpenVPN en software center de NethServer.



Fuente: Autoría propia.

Acceder a la opción de aplicaciones y seleccionar VPN para iniciar la configuración.

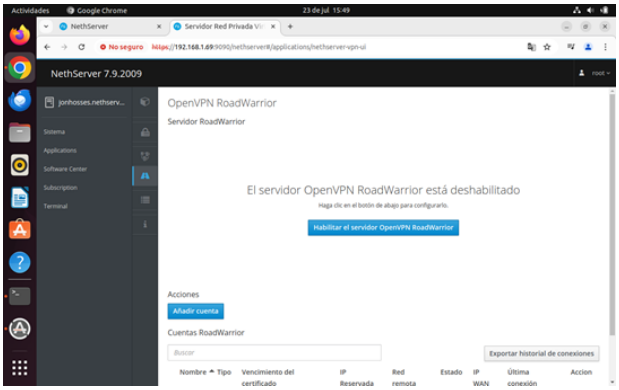
Figura 57. Acceso a OpenVPN desde NethServer



Fuente: Autoría propia.

Ingresar a la opción de OpenVPN RoadWarrior para configurar el servidor de ruta.

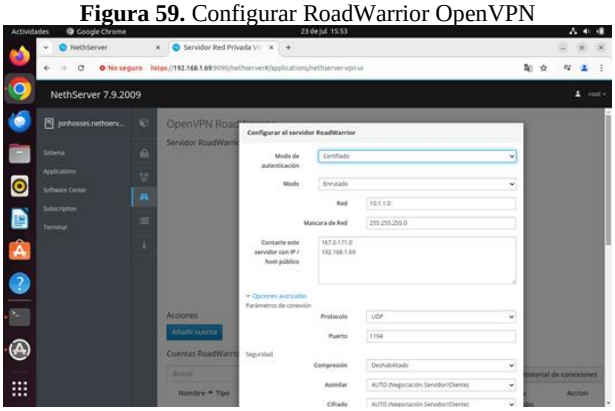
Figura 58. Configurar RoadWarrior OpenVPN



Fuente: Autoría propia.

Configurar el modo de autenticación con certificado, proporcionando mayor seguridad.

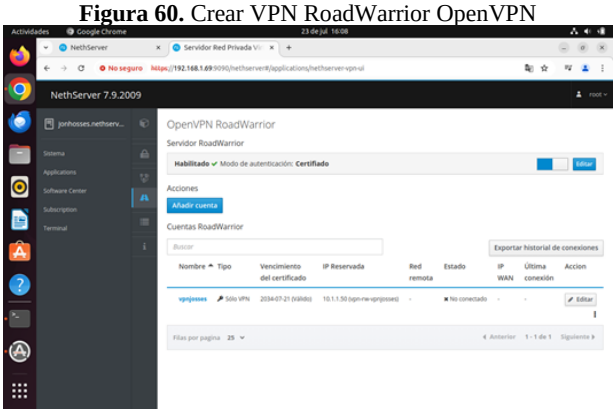
Figura 59. Configurar RoadWarrior OpenVPN



Fuente: Autoría propia.

Aplicar la configuración y verificar que la nueva VPN fue creada.

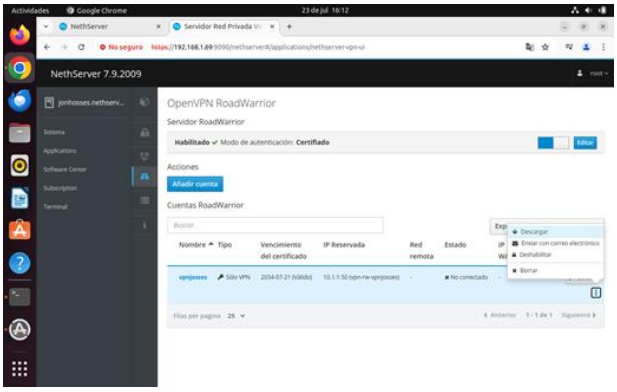
Figura 60. Crear VPN RoadWarrior OpenVPN



Fuente: Autoría propia.

Se continua con el proceso de descargar la configuración y certificado de la VPN para el cliente de OpenVPN que se instalará en las estaciones de trabajo.

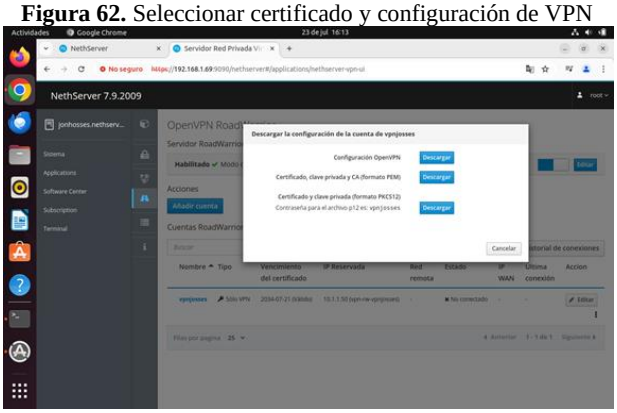
Figura 61. Descargar certificado y configuración de VPN



Fuente: Autoría propia.

Se presentan las opciones para descargar la configuración de VPN donde se encuentra la configuración de VPN, solo el certificado en formato cifrado PEM o el certificado en formato cifrado PKCS12

Figura 62. Seleccionar certificado y configuración de VPN



Fuente: Autoría propia.

Descargar el certificado en formato OVPN, para realizar una configuración completa y desde cero de la VPN de OpenVPN cliente.

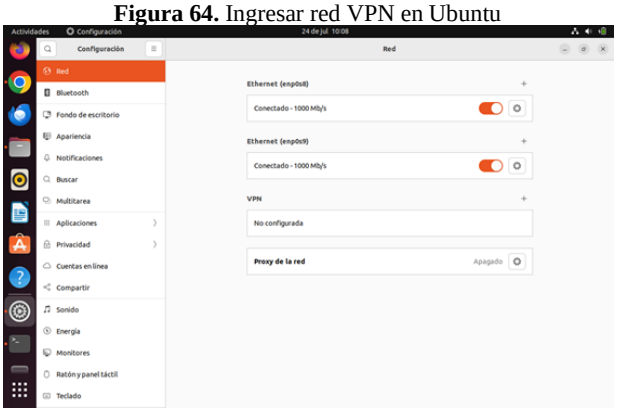
Figura 63. Certificado descargado en formato OVPN

Fuente: Autoría propia.

Se procede con la instalación y configuración del cliente VPN de OpenVPN en Ubuntu escritorio.

Ingresar a la configuración de red de Ubuntu escritorio y seleccionar la opción VPN.

Figura 64. Ingresar red VPN en Ubuntu



Fuente: Autoría propia.

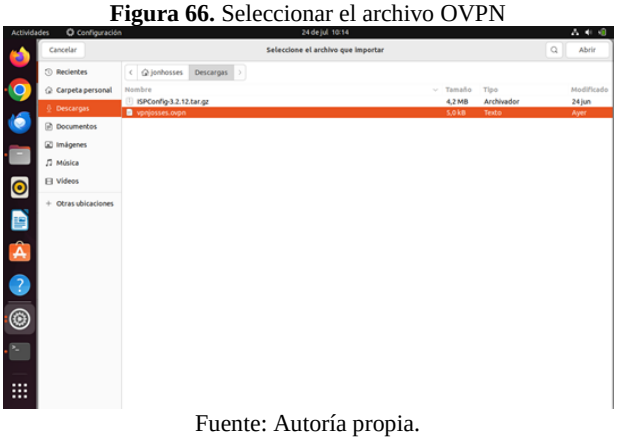
Seleccionar la opción de importar desde un archivo y usar el archivo en formato OVPN descargado previamente.

Figura 65. Importar el archivo OVPN

Fuente: Autoría propia.

Seleccionar el archivo OVPN.

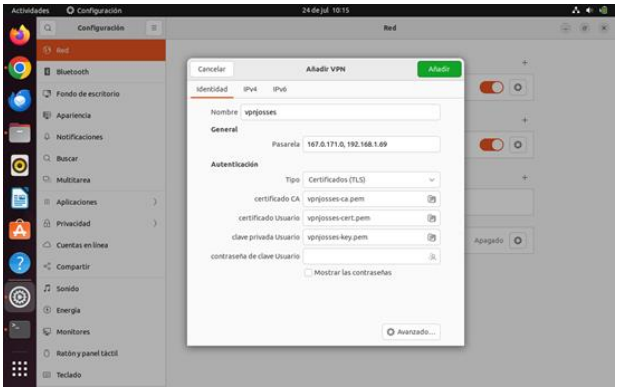
Figura 66. Seleccionar el archivo OVPN



Fuente: Autoría propia.

Importar la información de la VPN configurada en NethServer y añadirla a Ubuntu como una red VPN.

Figura 67. Cargar red vpn desde archivo OVPN



Fuente: Autoría propia.

Verificar que la nueva red VPN aparezca en la configuración de red de Ubuntu.

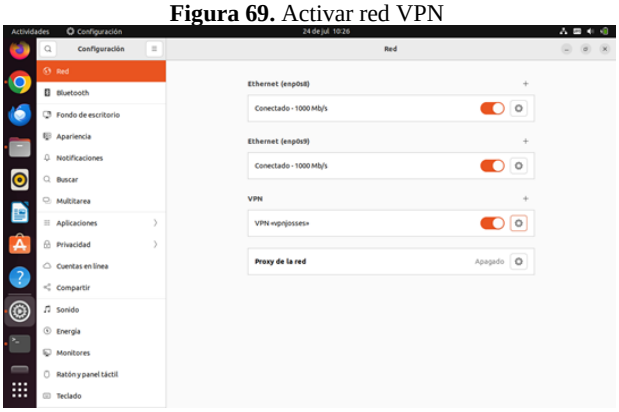
Figura 68. Red vpn añadida en ubuntu

Fuente: Autoría propia.

Finalmente se realiza las pruebas de conectividad a la VPN y el tráfico generado en la misma.

Activar la VPN recientemente configurada.

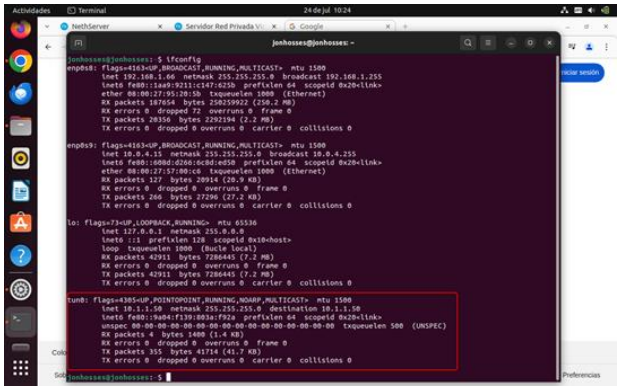
Figura 69. Activar red VPN



Fuente: Autoría propia.

Verificar que la IP configurada para la VPN corresponde a la configurada en NethServer.

Figura 70. Validar ip de la red VPN



Fuente: Autoría propia.

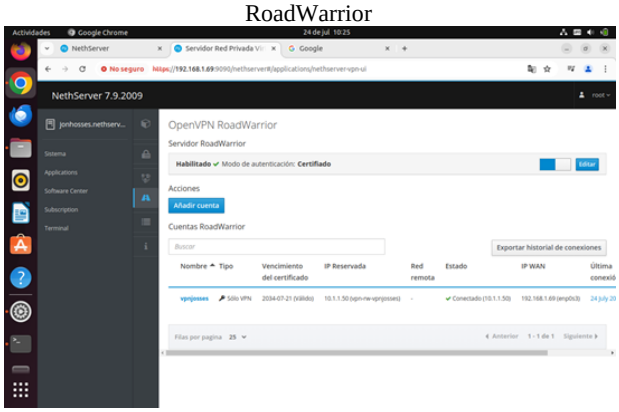
Validar en NethServer, en la opción de OpenVPN RoadWarrior, que haya tráfico en la red VPN configurada.

Figura 71. Validar tráfico de la red VPN en RoadWarrior

Fuente: Autoría propia.

Verificar que la VPN de OpenVPN en RoadWarrior esté correctamente activa y funcionando.

Figura 72. Validar estado de la conexión de la red VPN en RoadWarrior



Fuente: Autoría propia.

3.5.1 Conclusiones.

La implementación de servicios de infraestructura IT utilizando NethServer en una distribución GNU/Linux basada en Ubuntu ha demostrado ser efectiva y eficiente. Los servicios configurados aseguran un acceso controlado y seguro

a los recursos de la red, mejorando significativamente la gestión y administración de la infraestructura IT de la organización.

La implementación y configuración del servidor DHCP, servidor DNS y controlador de dominio en NethServer han resultado en una integración exitosa de estaciones de trabajo GNU/Linux a la infraestructura IT de la organización. Mediante el uso de autenticación por usuario y contraseña, se logró un acceso controlado y seguro a los recursos de la red. El registro eficiente de las estaciones de trabajo en los servicios de NethServer ha facilitado una administración centralizada, mejorando la gestión de la red y garantizando la seguridad y estabilidad del entorno corporativo.

La implementación de un proxy server en NethServer ofrece diversas ventajas para la administración y control de una red IT compleja. Permite controlar el acceso a Internet, filtrar contenido inapropiado, mejorar el rendimiento de la red y aumentar la seguridad. Sin embargo, es importante considerar las limitaciones del uso de un proxy server, como la posible degradación del rendimiento y la complejidad de la configuración y gestión.

La implementación y configuración del cortafuegos en NethServer ha permitido restringir efectivamente el acceso a sitios web de entretenimiento y redes sociales, mediante reglas y políticas bien definidas. La validación desde una estación de trabajo confirmó el correcto funcionamiento de estas restricciones, asegurando que la red corporativa opera de manera segura y alineada con las políticas organizacionales, mejorando así la seguridad y productividad en el entorno laboral.

La configuración de la VPN en NethServer ha permitido crear un túnel de comunicación seguro y privado, facilitando el acceso remoto a los recursos internos de manera eficiente y segura.

La conexión exitosa de la estación de trabajo GNU/Linux a través de la VPN ha evidenciado una mejora significativa en la accesibilidad y disponibilidad de los recursos internos, demostrando la viabilidad y funcionalidad de la solución implementada.

La configuración del servidor de archivos y del servidor de impresión utilizando NethServer, una distribución Linux especializada para pequeñas y medianas oficinas, ha sido exitosa y eficaz. A través de un procedimiento detallado, se ha implementado el protocolo LDAP para la gestión de usuarios y grupos, permitiendo una administración centralizada de datos y una autorización adecuada de accesos. La instalación de los paquetes necesarios para los servidores de archivos y de impresión se realizó sin inconvenientes, con verificación y seguimiento a través de las herramientas disponibles en NethServer.

4 REFERENCIAS

[1] NethServer. (n.d.). Web Proxy. Recuperado de https://docs.nethserver.org/en/v7/web_proxy.html

[2] [YouTube]. (2019). Nethserver Tutorial | Instalación, actualización y primeros pasos. Recuperado de https://www.youtube.com/watch?v=FNGmM-2fa_0

[3] [YouTube]. (2023). Instalar #NethServer + Configurar Web Proxy & Filtrar Contenidos Web. Recuperado de https://www.youtube.com/watch?v=cIHJbtTehKg

[4] Wikipedia. (2024, 18 de julio). Limitations of Using a Proxy Server. Recuperado de https://en.wikipedia.org/wiki/Proxy_server

[5] Administrator Manual — NethServer 7 Final. (s. f.). https://docs.nethserver.org/en/v7/

[6] VPN — NethServer 7 Final. (s. f.). https://docs.nethserver.org/es/v7/vpn.html

[7] A, D., & A, D. (2024, 2 febrero). Configurar un servidor VPN Linux con OpenVPN: conexión a dispositivos y gestión de VPN. Tutoriales Hostinger. https://www.hostinger.co/tutoriales/como-configurar-vpn-linux-con-openvpn

[8] Firewall and gateway — NethServer 6.10 Final. (n.d.). https://docs.nethserver.org/en/v6/firewall.html

[9] Manuel Cabrera Caballero. (2024, February 18). NethServer 8 Tutorial - OpenLDAP - Agregando grupos y usuarios [Video]. YouTube. https://www.youtube.com/watch?v=eHfItcrDUnQ

[10] Usuarios y grupos — NethServer 7 Final. (n.d.). https://docs.nethserver.org/es/v7/accounts.html

[11] Carpetas compartidas — NethServer 7 Final. (n.d.). https://docs.nethserver.org/es/v7/shared_folder.html