IMPLEMENTACIÓN DE LOS SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT BAJO EL SERVIDOR GNU/LINUX NETHSERVER

Mireya Carrillo Delgado
e-mail: mcarrillodel@unadvirtual.edu.co
Rubén Darío Capacho Rico
e-mail: rdcapachor@unadvirtual.edu.co
Sergio Mauricio Mantilla Serrano
e-mail: smmantillas@unadvirtual.edu.co
Libardo Gómez Patiño
e-mail: lgomezpa@unadvirtual.edu.co
Ingrith Yurley Mosquera Vargas
e-mail: iymosquerav@unadvirtual.edu.co

RESUMEN: *En el presente artículo se evidencia la instalación y configuración como sistema operativo base a la distribución NethServer versión 7.9.2009, la cual fue instalada en una máquina virtual implementada en VirtualBox. Luego, se realiza la implementación de los servicios de gestión de infraestructura IT DHCP Server, DNS Server y Controlador de Dominio, Proxy, Cortafuegos, File Server y Print Server y VPN. Por lo anterior, el presente documento es construido con el paso a paso de la Implementación y configuración detallada de cada uno de los servicios descritos evidenciando el funcionamiento de los mismos.*

PALABRAS CLAVE: Cortafuegos, DHCP, Nethserver, VPN.

1 INTRODUCCIÓN

Linux es un sistema operativo bastante versátil con una gran variedad de distribuciones para la gestión y administración de servidores. Nethserver es una de estas distribuciones. Este sistema operativo es muy modular, y se le pueden incorporar fácilmente nuevos plugins y software adicional para aumentar sus opciones predeterminadas. Gracias a la interfaz gráfica de usuario, se podrá gestionar todos los servicios y su configuración de forma fácil y rápida, no se tendrá que editar ficheros de texto para configurar los diferentes servicios, ni tampoco meterse en la terminal del sistema vía SSH o Telnet para administrarlo, todo se podrá hacer a través de su interfaz vía web [1]. En el presente trabajo, se establecen los resultados obtenidos al realizar el montaje de una máquina virtual con Nethserver sobre el cual se realizó la configuración de una gran variedad de servicios de gestión de infraestructura IT como es el caso de DHCP y DNS server, controlador de dominio, proxy, cortafuegos, file server y VPN.

2 INSTALACIÓN DE NETHSERVER

Se procedió a realizar el montaje de un servidor con Nethserver. Como primera medida se realizó la descarga de la imagen ISO de la página oficial de Nethserver, y se realizó el montaje de la respectiva máquina virtual partiendo de esta imagen ISO. La versión descargada fue la 7.9.2009. [2]

Posteriormente, se procedió a realizar el montaje de una máquina virtual con las siguientes características:

- 3 GB de RAM
- 10 GB de disco duro
- 2 Cpus

Figura 1. Máquina virtual del Nethserver.

Fuente: Autoría Propia

Una vez definida la máquina virtual, se procedió a definir los 3 adaptadores de red para la zona verde, naranja y roja. Estas se presentan en la tabla 1.

Tabla 1. Ips para los adaptadores de red.

Zona	Ip	Mascara de red	MAC
Zona verde	192.168.100.107	255.255.255.0	08002742BAF8
Zona naranja	10.0.4.15	255.255.255.0	08002738A88F
Zona roja	DCHP		080027A457D7

Fuente: Autoría Propia

Una vez definidos estos adaptadores, se procedió a asignarlos a la máquina virtual y a iniciarla. Acá es importante resaltar, que para la DMZ y la red LAN se usaron dos máquinas virtuales con Linux Debian, a las cuales, se le asignaron los adaptadores de red de la zona verde y naranja.

Figura 2. Inicio de la máquina virtual con el Nethserver.

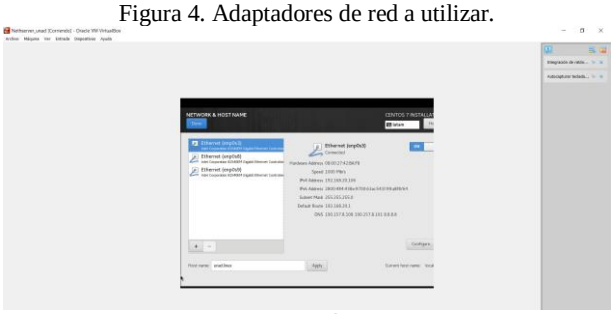
Fuente: Autoría Propia

En el resumen de la instalación se procedió a definir el hora y fecha de la máquina, así como, el idioma del teclado a usar. Adicionalmente, se verificaron los 3 adaptadores de red.

Figura 3. Resumen de la instalación.

Fuente: Autoría Propia

Figura 4. Adaptadores de red a utilizar.



Fuente: Autoría Propia

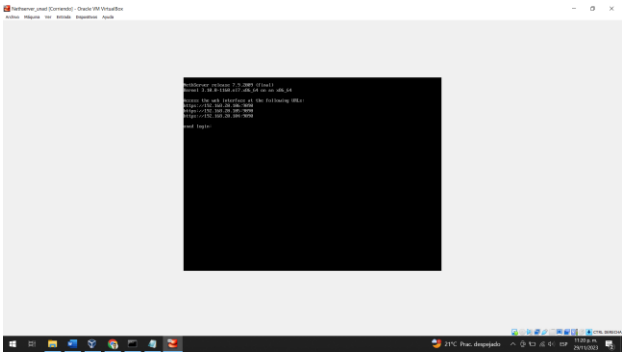
Se procede a iniciar con el proceso de instalación y la definición de la contraseña root.

Figura 5. Asignación de la contraseña del usuario root.

Fuente: Autoría Propia

Una vez se finaliza la instalación se puede apreciar las ips asignadas y el puerto a utilizar para acceder a la interfaz gráfica del Nethserver, en este caso, el puerto asignado fue el 9090.

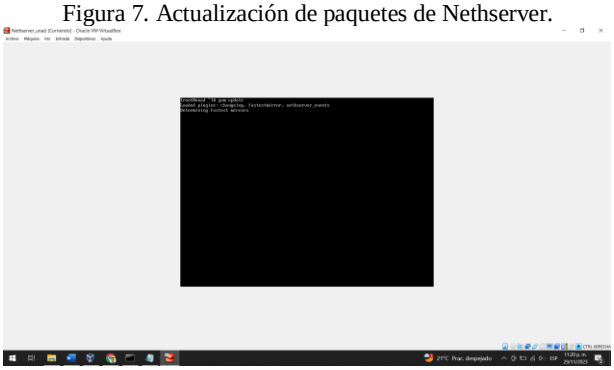
Figura 6. Ips asignadas para los adaptadores de red del Nethserver.



Fuente: Autoría Propia

Antes de iniciar la configuración desde la interfaz gráfica, se precio a realizar la actualización de los paquetes del sistema operativo. En este caso, se ejecutó el comando yum update.

Figura 7. Actualización de paquetes de Nethserver.



Fuente: Autoría Propia

Para abrir la interfaz gráfica, se utilizó la máquina virtual de la LAN utilizando el navegador predefinido. En primera medida, se aceptaron los riesgos de los certificados auto firmados y se procedió a realizar la autenticación.

Figura 8. Autenticación en la interfaz gráfica.

Fuente: Autoría Propia

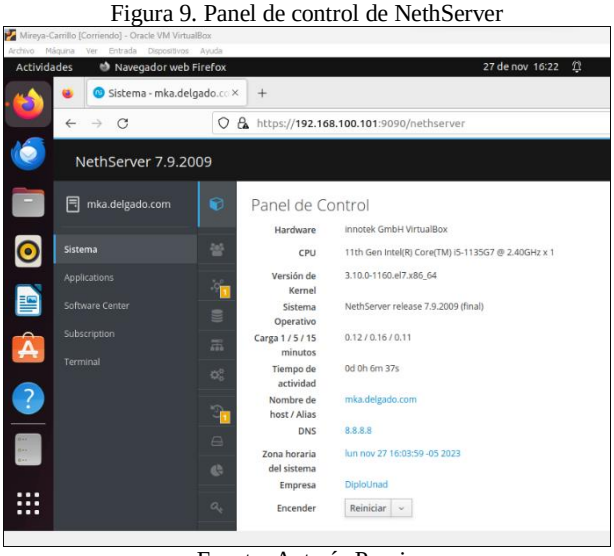
Dentro del Nethserver se cuentan con una gran variedad de funcionalidades para configurar los diferentes servicios que esta distribución de Linux ofrece. Partiendo de esto, se procedió a realizar el montaje de un DHCP Server, un proxy, un cortafuegos, un file server y una VPN.

3 DESARROLLO DE LA TEMÁTICA

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

Una vez instalado el Nethserver en el VirtualBox, se procede a ingresar desde el navegador del equipo cliente a la interfaz de Nethserver para registrar la información básica de la empresa. [3]

Figura 9. Panel de control de NethServer



Fuente: Autoría Propia

Posteriormente se debe realizar la configuración de la red donde cada tarjeta de red será para una zona, la tarjeta enp0s8 se destinó para la zona verde (LAN) con una IP estática 192.168.5.1, la tarjeta enp0s3 para la zona roja (WAN) con una IP por DHCP y por último la tarjeta enp0s9 se definió para la zona naranja (DMZ) con una IP estática 10.36.1.1.

Figura 10. Lista de asignación de redes por zonas

Fuente: Autoría Propia

3.1.1 DHCP SERVER

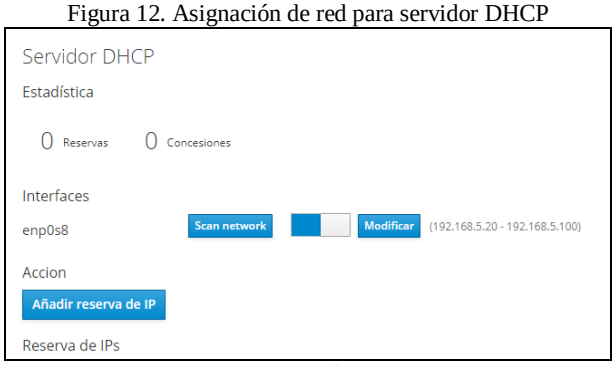
En el módulo DHCP se procede a modificar las opciones para ser ajustados en NethServer, asignándole 80 IP como rango (192.168.5.20 – 192.168.5.100) dentro del segmento de la red Verde. [4]

Figura 11. Asignación de red para servidor DHCP

Fuente: Autoría Propia

Guardada la configuración se evidencia que tomó el rango de IP establecido anteriormente.

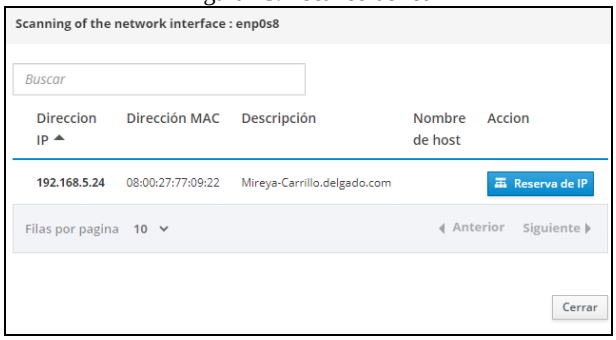
Figura 12. Asignación de red para servidor DHCP



Fuente: Autoría Propia

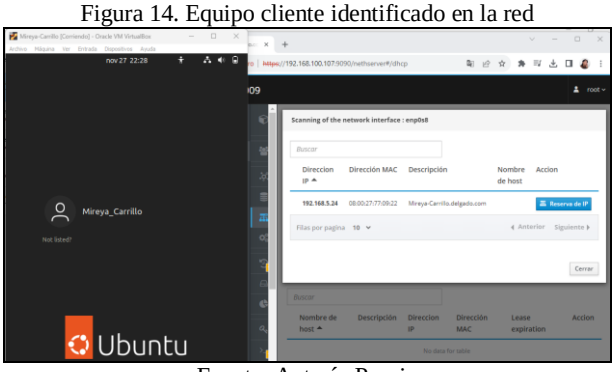
Al realizar un escaneo a la red, el servidor identifica un equipo (equipo cliente utilizado) al cual le asigna la IP 192.168.5.24 que está dentro del rango configurado en el servidor DHCP

Figura 13. Escaneo de red



Fuente: Autoría Propia

Figura 14. Equipo cliente identificado en la red

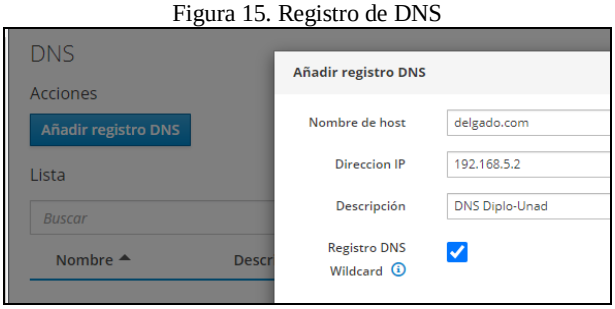


Fuente: Autoría Propia

3.1.2 DNS SERVER

En el módulo DNS se añade lo correspondiente al registro DNS.

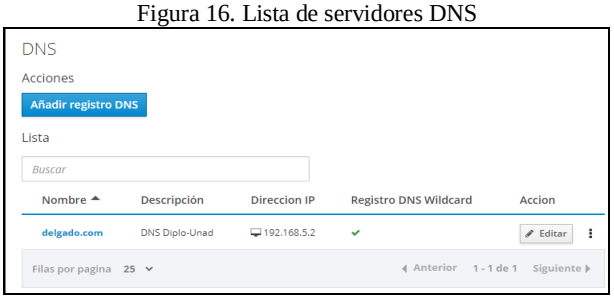
Figura 15. Registro de DNS



Fuente: Autoría Propia

Completado el proceso de registro se listan los registros de DNS realizados.

Figura 16. Lista de servidores DNS



Fuente: Autoría Propia

Para verificar el funcionamiento del DNS, se ingresa al navegador del equipo cliente, en este caso una maquina con Ubuntu desktop y se digita delgado.com donde se evidencia que reconoce el DNS registrado.

Figura 17. Reconociendo el DNS registrado

Fuente: Autoría Propia

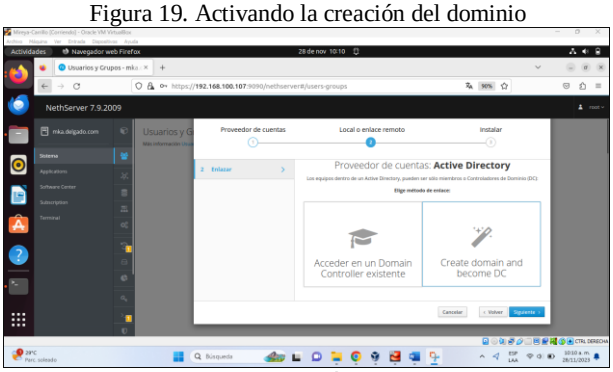
3.1.3 ACTIVE DIRECTORY

En NethServer se ingresa al módulo de usuarios y grupos para realizar el active directory y posteriormente realizar el créate domain and become DC. [5]

Figura 18. Habilitando el directorio activo

Fuente: Autoría Propia

Figura 19. Activando la creación del dominio



Fuente: Autoría Propia

Para la creación del dominio se utilizaron los siguientes datos:

Nombre de dominio: delgado.com
Nombre de dominio NetBIOS: DELGADO
Dirección IP Domain Controller: 192.168.5.2

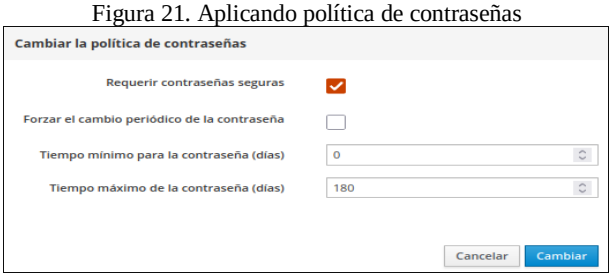
Como resultado del registro se obtiene un detalle del active directory local

Figura 20. Resumen detallado del active directory local

Fuente: Autoría Propia

A continuación se ajusta la política de contraseñas para que estas sean seguras en los usuarios y grupos que posteriormente se crearan.

Figura 21. Aplicando política de contraseñas



Fuente: Autoría Propia

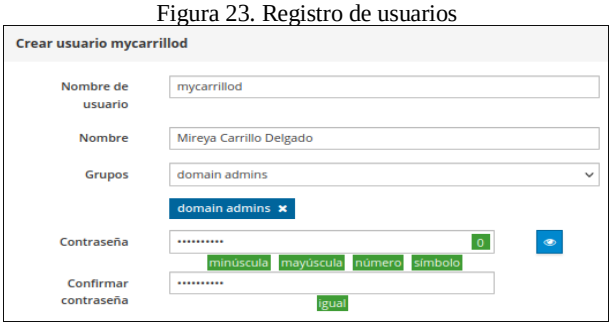
Se procede a la creación de los grupos y se evidencia que el grupo domain admins fue creado automáticamente por el sistema.

Figura 22. Lista de grupos registrados

Fuente: Autoría Propia

Ahora se hace la creación de los usuarios donde se pueden vincular a alguno de los grupos creados.

Figura 23. Registro de usuarios



Fuente: Autoría Propia

Al empezar la creación de usuarios el sistema crea los usuarios admin y administrator automáticamente y para estos solo se hizo cambio de la contraseña.

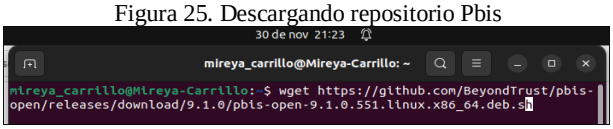
Figura 24. Lista de usuarios registrados

Fuente: Autoría Propia

3.1.4 AGREGAR EQUIPO AL CONTROLADOR DE DOMINIO

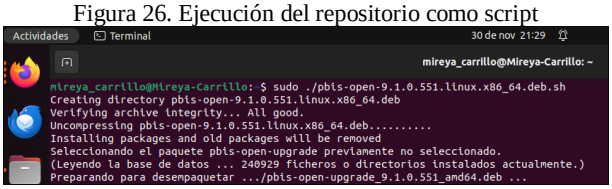
En la terminal del equipo cliente se descarga el repositorio pbis al que se le debe dar permisos de ejecución para poder ser ejecutado como un script y de esta manera poder unir la maquina cliente al dominio creado. [6]

Figura 25. Descargando repositorio Pbis



Fuente: Autoría Propia

Figura 26. Ejecución del repositorio como script



Fuente: Autoría Propia

Con el comando sudo apt install openssh-server se instala aplicación para la comunicación en la red usando a ssh como protocolo.

Figura 27. Instalando Openssh-server

Fuente: Autoría Propia

Al ejecutar el repositorio como script, el resultado de la última línea fue un ejemplo de la línea de comando a utilizar para terminar la unión del dominio en el equipo usando la línea de comando sudo /opt/pbis/bin/domainjoin-cli join DELGADO.COM administrator reemplazando el nombre del dominio y el nombre de la cuenta.

Figura 28. Unión exitosa del equipo al dominio

Fuente: Autoría Propia

Cerrada la sesión actual de la cuenta del equipo cliente, se ingresa por la opción no listed para poder digitar el usuario creado en el active directory al que se le agrega el dominio @delgado.com y se ingresa con credenciales de acceso.

Figura 29. Ingreso exitoso al sistema con usuario mycarrillod

Fuente: Autoría Propia

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.

Para la actividad ya se tiene el servidor Nethserver instalado y configurado dentro de la zona DMZ, donde arranca desde la web de administración y se accede desde el navegador.

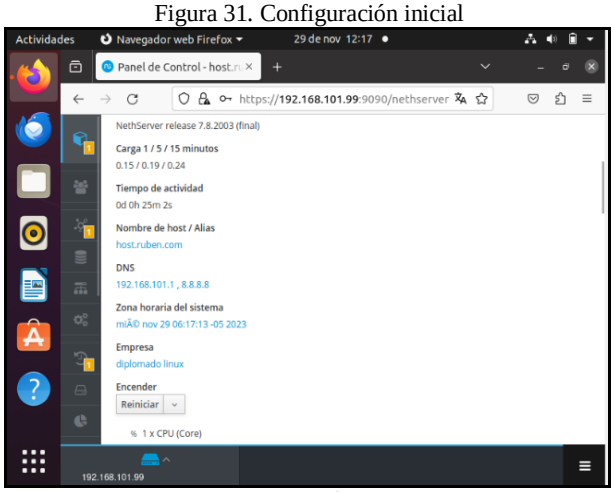
Al primer inicio se deben realizar algunas configuraciones previas.

Figura 30. Login Nethserver

Fuente: Autoría Propia

Se debe configurar el control del Nethserver, donde se debe de asignar el usuario el cual se le coloca host.ruben.com e igualmente se configura el nombre de la compañía, para este caso quedo Diplomado Linux

Figura 31. Configuración inicial

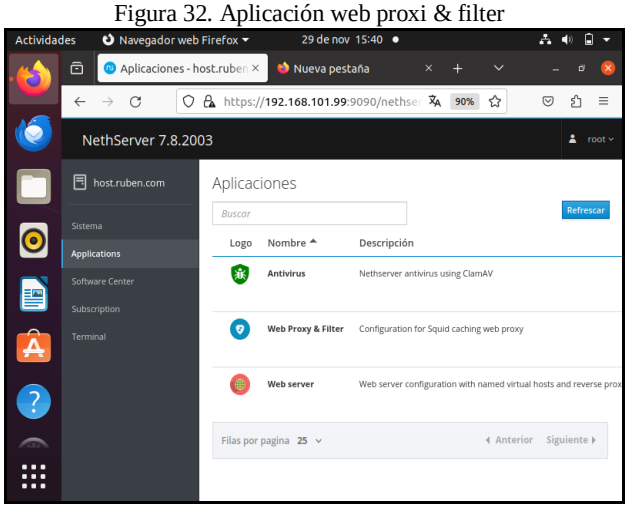


Fuente: Autoría Propia

Después de haber actualizado el sistema y el Nethserver se debe instalar las aplicaciones necesarias para llevar a cabo la práctica y el correcto funcionamiento de la temática.

*Aplicaciones filtro web y proxi web

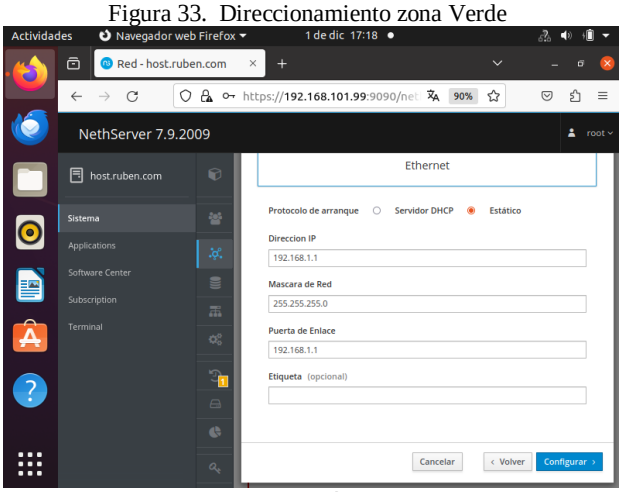
Figura 32. Aplicación web proxi & filter



Fuente: Autoría Propia

Se realiza la Configuración de la LAN (verde) ubicada enp0s8 192.168.1.1 con máscara 24, esta configuración se realiza de manera estática.

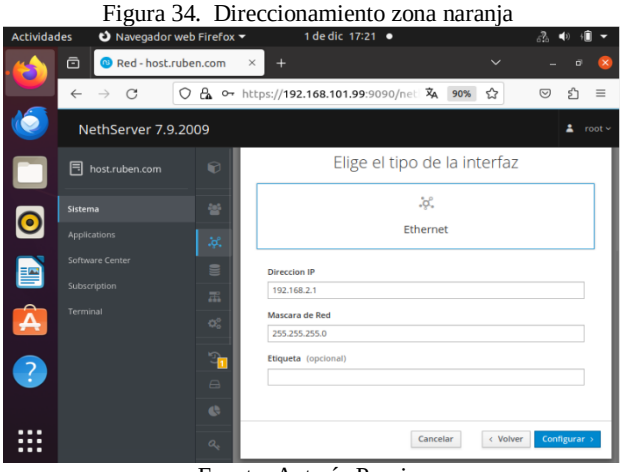
Figura 33. Direccionamiento zona Verde



Fuente: Autoría Propia

Se realiza la configuración de la zona DMZ (Naranja). Ubicada en el enp0s9 192.168.2.1 con mascara 24.

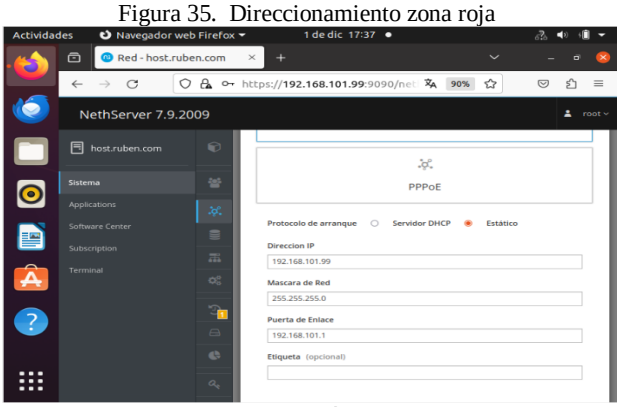
Figura 34. Direccionamiento zona naranja



Fuente: Autoría Propia

Se realiza la configuración de la WAN (Roja) ubicada en enp0s3 IP estática 192.168.101.99 mascará 24 y puerta de enlace 192.168.101.1.

Figura 35. Direccionamiento zona roja



Fuente: Autoría Propia

Figura 36. Activación categorías

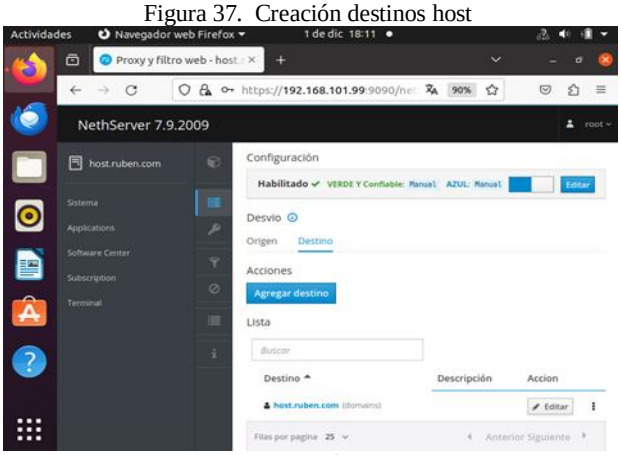
Fuente: Autoría Propia

Se activa la categoría, en donde se utiliza la que trae por defecto, la cual ayudara aplicar los filtros a unas páginas definidas y categorías.

Se debe hacer dos filtros, el primero bloqueara algunas páginas donde están las categorías que viene por defecto y el segundo son las que se aplicara a un host que se le permitirá todas las categorías y se bloqueara las demás páginas.

Creación destino para aplicar los filtros.

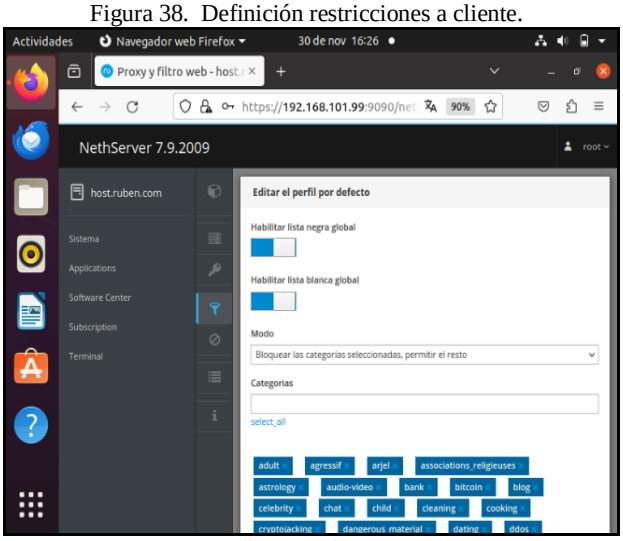
Figura 37. Creación destinos host



Fuente: Autoría Propia

Configuración de filtrado al cliente host.ruben.com con IP 192.168.1.1 se les dan los permisos a todas las categorías seleccionadas.

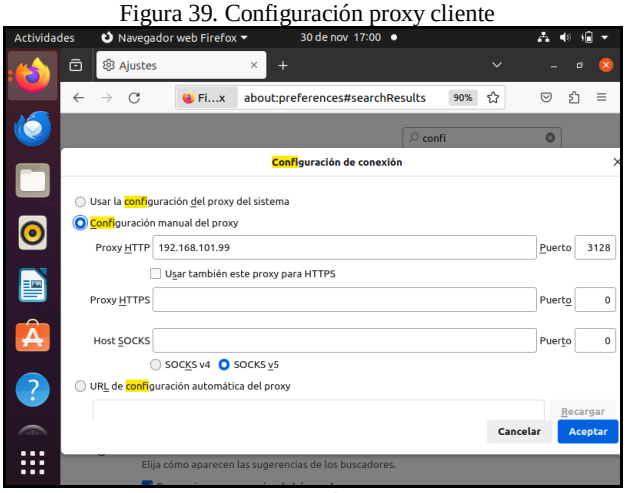
Figura 38. Definición restricciones a cliente.



Fuente: Autoría Propia

Configuración del proxy en equipo cliente

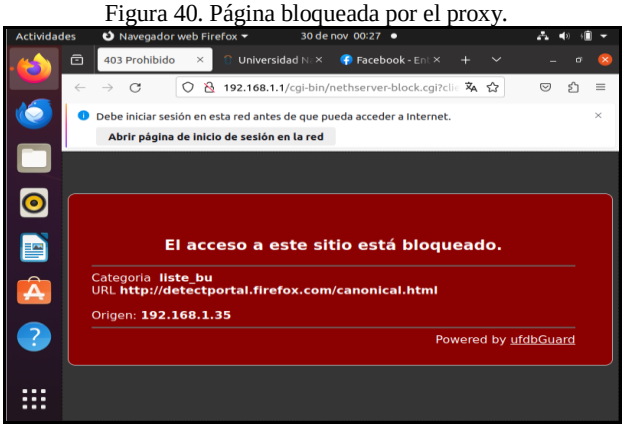
Figura 39. Configuración proxy cliente



Fuente: Autoría Propia

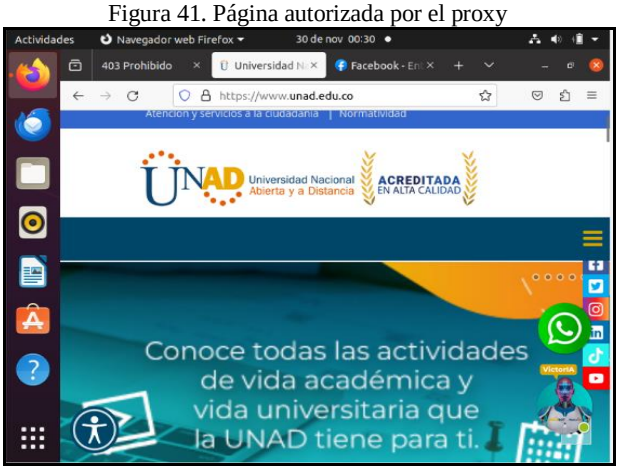
Se ingresa al equipo y se ingresa a páginas y esta página está fuera de las categorías definidas y la bloquea.

Figura 40. Página bloqueada por el proxy.



Fuente: Autoría Propia

Figura 41. Página autorizada por el proxy



Fuente: Autoría Propia

3.3 TEMÁTICA 3: CORTAFUEGOS

Un cortafuegos o firewall es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados [7]. En este caso, se realizó el montaje de un cortafuegos para realizar el bloqueo a unos sitios web particulares relacionados con redes sociales y sitios de entretenimiento. Para ello, se inició con la configuración de las redes asignando las IPs predefinidos en la tabla 1.

Figura 42. Configuración de la red roja.

Fuente: Autoría Propia

Figura 43. Configuración de la red naranja.

Fuente: Autoría Propia

Figura 44. Configuración de la red verde.

Fuente: Autoría Propia

Posteriormente se procedió a instalar el firewall desde el centro de software y a configurar las reglas de bloqueo de los sitios definidos.

Figura 45. Instalación del firewall desde el centro de software.

Fuente: Autoría Propia

Una vez instalado, se procedió a abrir esta aplicación desde el menú de aplicaciones. Entre las primeras cosas importantes a ver, es la forma en que esta concebidos los adaptadores de red y como la red naranja y verde pasan a través del firewall para acceder a la WAN. En este punto, es importante resaltar que cada petición hacia internet será validad por el firewall, el cual, va a permitir o restringir el acceso.

Figura 46. Apertura del firewall.

Fuente: Autoría Propia

Figura 47. Configuración de la red.

Fuente: Autoría Propia

Para poder tener acceso a internet desde la red verde, se procedió a crear un DHCP con el rango de ips posibles. Este rango estuvo entre las ips 192.168.100.1 y la 192.168.100.254.

Figura 48. Configuración del DHCP.

Fuente: Autoría Propia

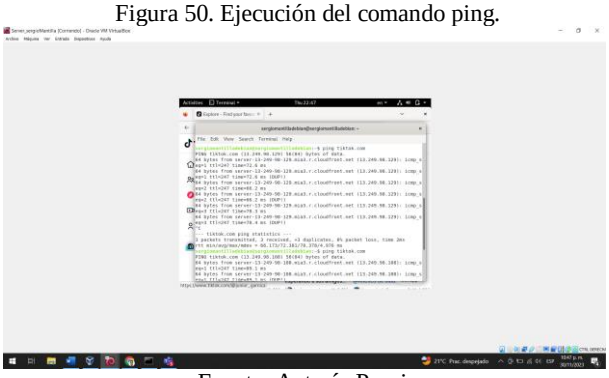
Los sitios web a restringir son tiktok.com y vanguardia.com. Se inicio con el bloqueo de tiktok para ello, se verifico en primera medida que se tuviera conexión con el sitio.

Figura 49. Verificación de acceso a tiktok.

Fuente: Autoría Propia

Una vez confirmada la navegación se procedió a verificar las ips que maneja este sitio web y proceder a bloquearlas, para ello, se usó el comando ping. En esta ejecución se pudo apreciar que las ips usadas por tiktok son variables, por ende, se procede a crear un rango de ips y usarlo para la creación de la regla.

Figura 50. Ejecución del comando ping.



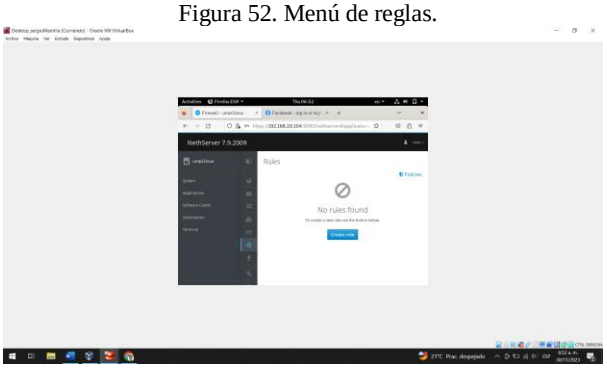
Fuente: Autoría Propia

Figura 51. Rango de IPs a bloquear.

Fuente: Autoría Propia

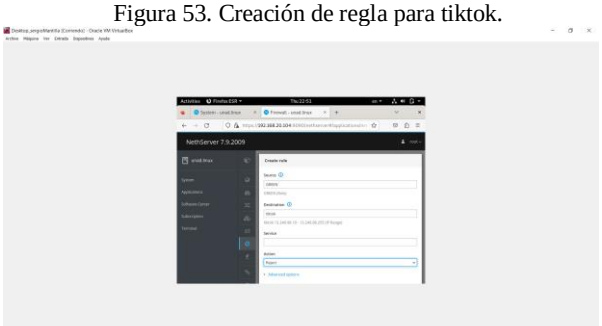
Teniendo el rango de IP configurado se procedió a acceder al menú de reglas y configurar la respectiva regla de bloqueo para estas IP.

Figura 52. Menú de reglas.



Fuente: Autoría Propia

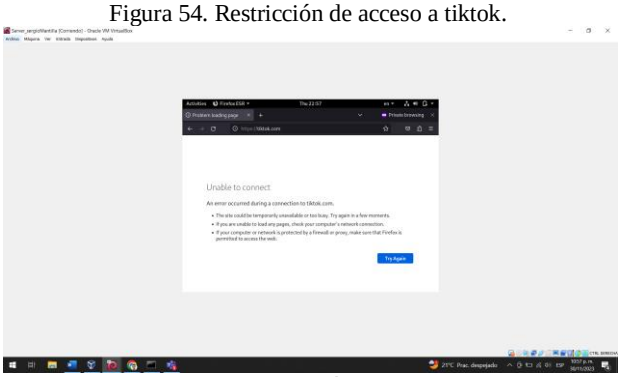
Figura 53. Creación de regla para tiktok.



Fuente: Autoría Propia

Una vez creada la regla se procede a verificar el acceso al sitio web y confirmar su respectiva restricción.

Figura 54. Restricción de acceso a tiktok.



Fuente: Autoría Propia

Posteriormente, se realizó el mismo proceso con el sitio web de vanguardia liberal. En este caso, la IP usada por este portal de noticias no es variable por ende no se creó un rango de IP.

Figura 55. Verificación de acceso a vanguardia.

Fuente: Autoría Propia

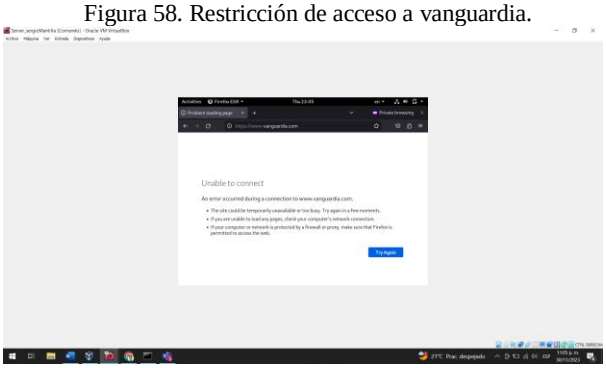
Figura 56. Ejecución del comando ping al sitio de vanguardia.

Fuente: Autoría Propia

Figura 57. Configuración de regla de bloqueo.

Fuente: Autoría Propia

Figura 58. Restricción de acceso a vanguardia.



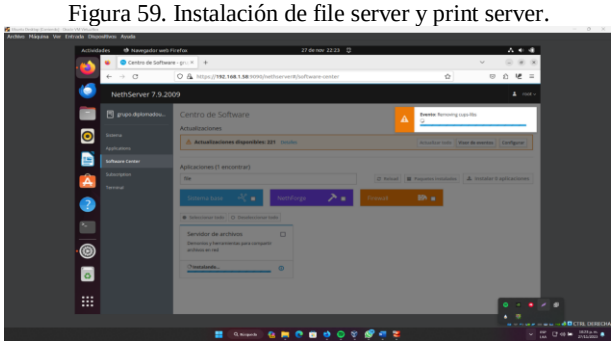
Fuente: Autoría Propia

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Un file server es un servicio que permite por medio de la red acceder a archivos, carpetas y programas ubicados en el sistema, este servicio brinda una capa de seguridad ya que estos elementos además de estar protegidos por un servicio de autenticación también están protegidos por permisos de lectura y escritura para archivos o carpetas. El print server es un servicio que permite a diferentes usuarios conectarse a impresoras compartidas en la red y así procesar de manera más eficiente este trabajo, es decir el print server actúa como el intermediario entre el computador del usuario y la impresora como tal. Para este caso se realizó la implementación de un file server y un print server usando la herramienta nethserver, en VirtualBox y haciendo las pruebas desde una máquina de Ubuntu desktop conectada a la misma red y desde donde se evidencia el funcionamiento de las implementaciones.

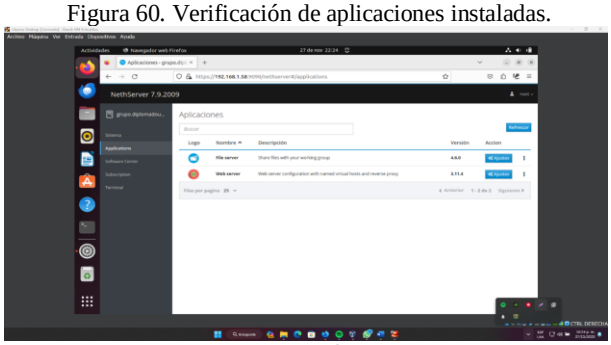
Lo primero que se realizo fue desde la interfaz gráfica de nethserver instalar la aplicación de file server y print server. [8]

Figura 59. Instalación de file server y print server.



Fuente: Autoría Propia

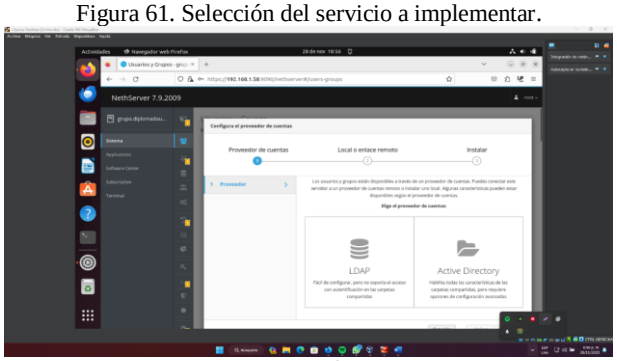
Figura 60. Verificación de aplicaciones instaladas.



Fuente: Autoría Propia

Posteriormente se realizó la instalación del servicio LDAP para el control de acceso de los usuarios a los directorios compartidos

Figura 61. Selección del servicio a implementar.

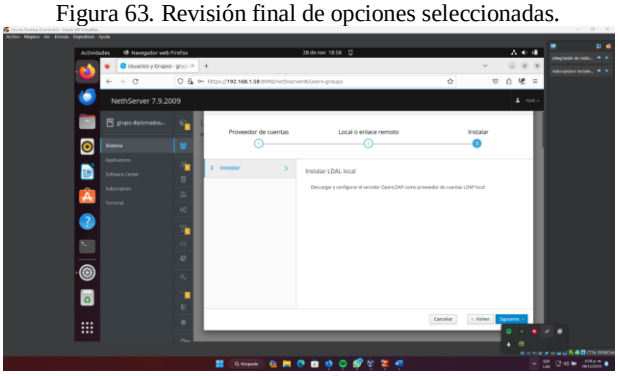


Fuente: Autoría Propia

Figura 62. Selección del tipo de implementación.

Fuente: Autoría Propia

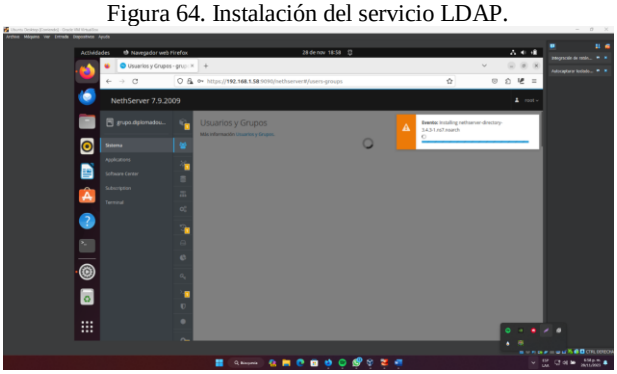
Figura 63. Revisión final de opciones seleccionadas.



Fuente: Autoría Propia

Luego de revisadas las opciones seleccionadas se procede con la instalación del servicio.

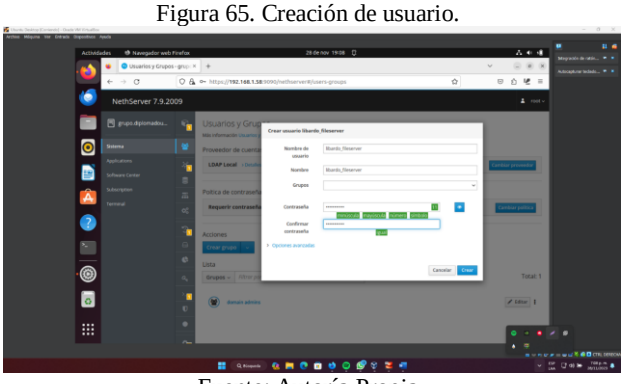
Figura 64. Instalación del servicio LDAP.



Fuente: Autoría Propia

Una vez implementado el servicio se procede a realizar la creación del usuario que se usara para el acceso a las carpetas compartidas, al cual se le asigna el nombre de libardo_fileserver y se le asigna una contraseña que cumpla con los requisitos de seguridad.

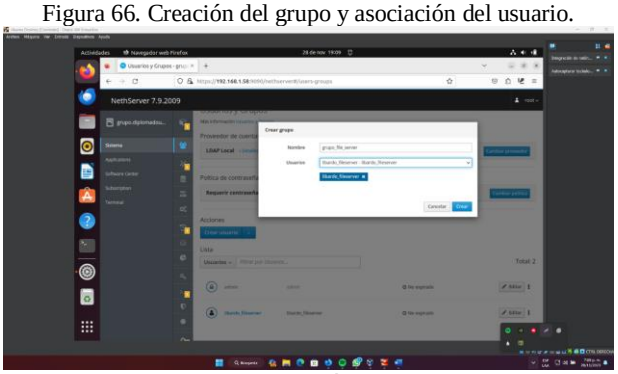
Figura 65. Creación de usuario.



Fuente: Autoría Propia

Posteriormente se realiza la configuración del grupo y la asociación del usuario al grupo creado para su posterior uso

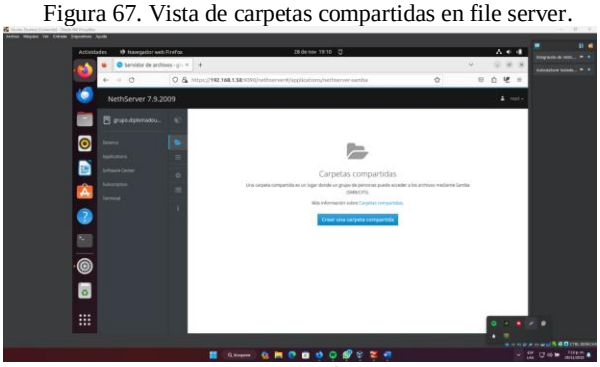
Figura 66. Creación del grupo y asociación del usuario.



Fuente: Autoría Propia

Posterior a la creación del usuario ya se puede acceder al file server y luego a la sección de carpetas compartidas donde se realizará la creación de la misma para realizar las pruebas correspondientes. [9]

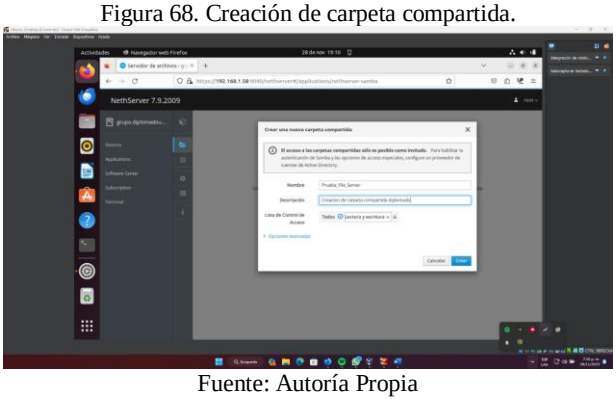
Figura 67. Vista de carpetas compartidas en file server.



Fuente: Autoría Propia

Ahora se procede a realizar la creación de la carpeta compartida a la cual se le asigna el nombre de Prueba_File_Server y se establecen permisos de lectura y escritura para la misma.

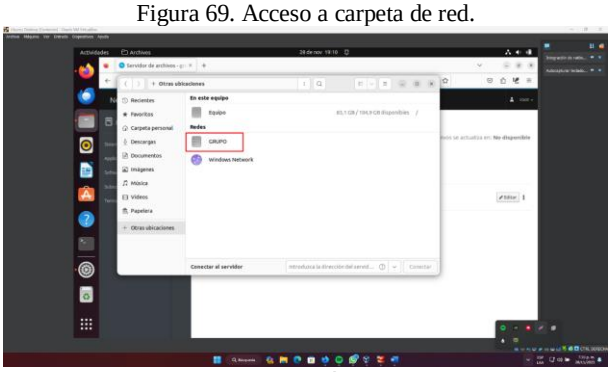
Figura 68. Creación de carpeta compartida.



Fuente: Autoría Propia

Desde la máquina de Ubuntu desktop usando el gestor de archivo se procede a acceder a la carpeta generada por nethserver la cual se encuentra disponible en la sección de redes.

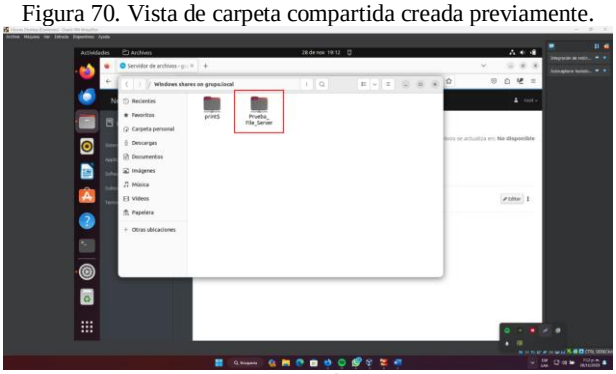
Figura 69. Acceso a carpeta de red.



Fuente: Autoría Propia

Dentro de esta se puede evidenciar la carpeta creada anteriormente desde el file server.

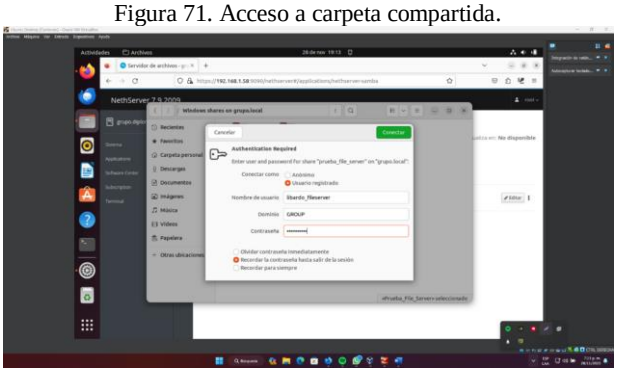
Figura 70. Vista de carpeta compartida creada previamente.



Fuente: Autoría Propia

Ahora al intentar acceder a dicha carpeta solicita la autenticación la cual se procede a realizar con las credenciales del usuario anteriormente creado.

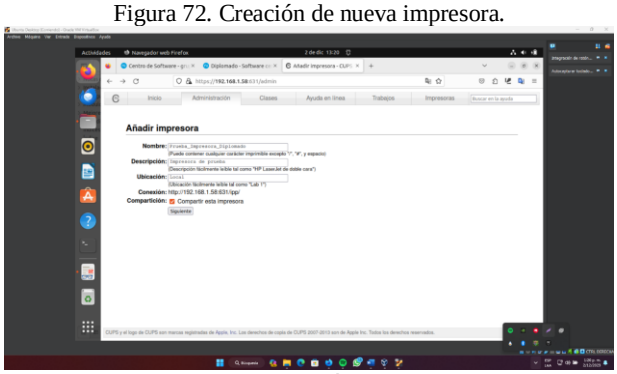
Figura 71. Acceso a carpeta compartida.



Fuente: Autoría Propia

Ahora se procede a realizar la configuración del print server, para el cual se debe acceder desde el puerto 631, desde el cual se va a iniciar agregando una nueva impresora, y a esta se le asigna el nombre de Prueba_impresora_diplomado y se continua con el proceso de creación. [10]

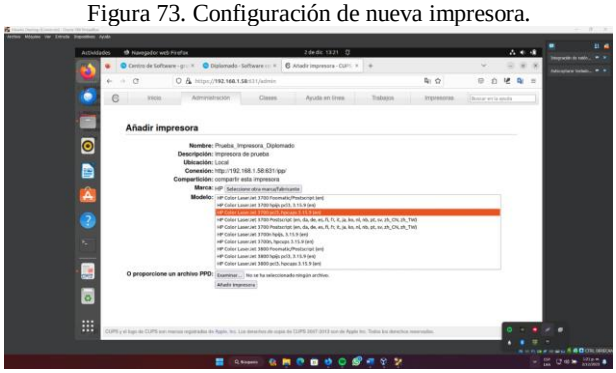
Figura 72. Creación de nueva impresora.



Fuente: Autoría Propia

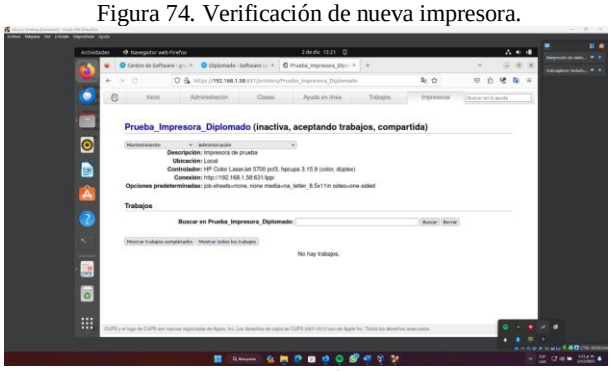
Posteriormente se procede a configurar la marca y el modelo de la impresora para terminar con la configuración de esta desde el print server.

Figura 73. Configuración de nueva impresora.



Fuente: Autoría Propia

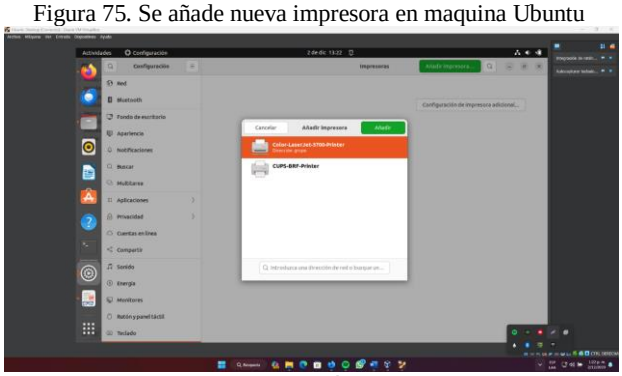
Figura 74. Verificación de nueva impresora.



Fuente: Autoría Propia

Por ultimo y para verificar que la impresora haya quedado correctamente configurada se procede a agregar desde la máquina de Ubuntu desktop.

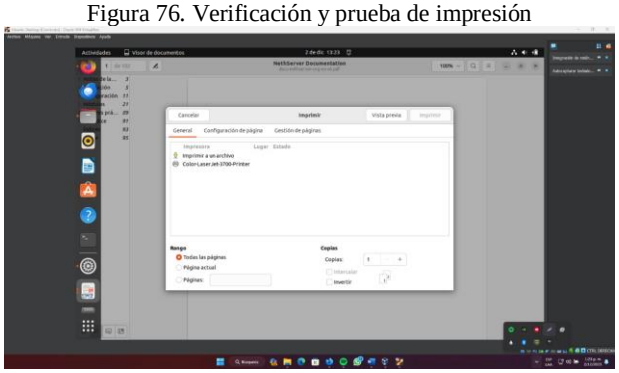
Figura 75. Se añade nueva impresora en maquina Ubuntu



Fuente: Autoría Propia

Luego de añadir la impresora a la maquina y para finalizar con las pruebas requeridas se procede a hacer una prueba de impresión desde un archivo pdf, desde donde se va a poder evidenciar la impresora disponible para realizar la impresión del documento.

Figura 76. Verificación y prueba de impresión



Fuente: Autoría Propia

3.5 TEMÁTICA 5: VPN

Las VPN son una herramienta que permite crear una conexión segura y encriptada entre un dispositivo y una red privada a través de Internet. Se utiliza para proteger la privacidad en línea, permitiendo a los usuarios navegar por la web de manera anónima y segura al ocultar su dirección IP y encriptar sus datos, permitiendo proteger datos, mantener privacidad y acceder a contenido de manera segura. Así también, OpenVPN es un protocolo VPN, actualmente es uno de los más populares. Es uno de los únicos de código abierto que también tiene su propia aplicación de código abierto. Es responsable de manejar las comunicaciones cliente-servidor. Básicamente, ayuda a establecer un "túnel" seguro entre el cliente VPN y el servidor VPN. [11]

Para dar inicio a la configuración de la VPN , desde la opción sistema y luego red se configuran la red LAN (verde), WAN (roja) y DMZ (naranja).

Figura 77. Configuración redes NethServer

Fuente: Autoría Propia

Luego desde la opción software center se realiza la instalación de la VPN, realizando la búsqueda de la aplicación OpenVPN y seguidamente se selecciona instalar 1 aplicación.

Figura 78. Instalación VPN en NethServer

Fuente: Autoría Propia

Figura 79. Instalación OpenVPN en NethServer

Fuente: Autoría Propia

Después, se verifica en la opción aplications que la aplicación VPN se encuentre instalada, después se selecciona opciones de la aplicación VPN para dar inicio a la configuración.

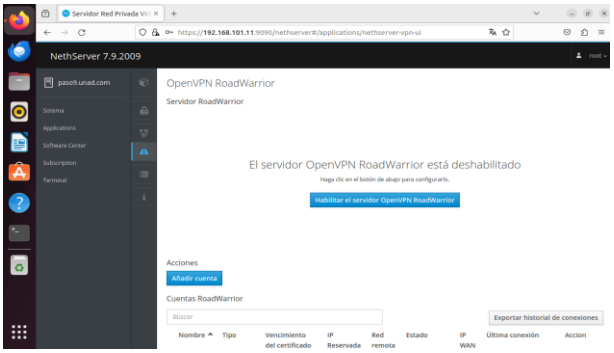
Figura 80. Configuración VPN en NethServer

Fuente: Autoría Propia

3.5.1 CONFIGURACIÓN VPN

Se inicia con la configuración del OpenVPN RoadWarrior, para ello se selecciona habilitar el servidor OpenVPN RoadWarrior. [12]

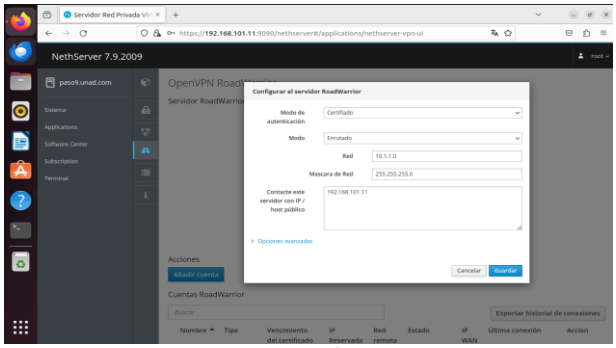
Figura 81. Configuración OpenVPN RoadWarrior en NethServer



Fuente: Autoría Propia

Para la configuración del RoadWarrior se debe tener en cuenta que en el modo de autenticación se debe seleccionar certificado, en modo se selecciona enrutado, se asigna una red, una máscara de red y se escribe la IP que en este caso corresponde a la asignada en el servidor nethserver dentro de la red WAN, luego se da en guardar.

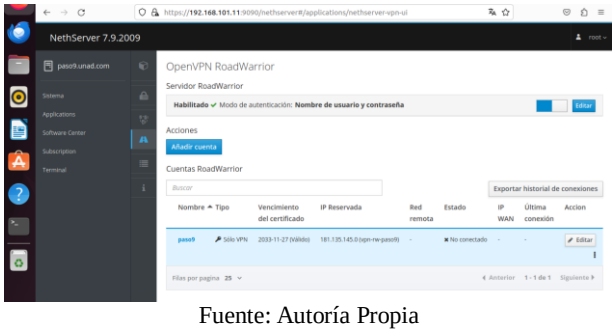
Figura 82. Configuración OpenVPN RoadWarrior en NethServer



Fuente: Autoría Propia

Luego, se debe dar clic en añadir cuenta, allí se selecciona solo VPN y se asigna un nombre de usuario y luego se da en guardar.

Figura 83. Configuración de la cuenta RoadWarrior en NethServer



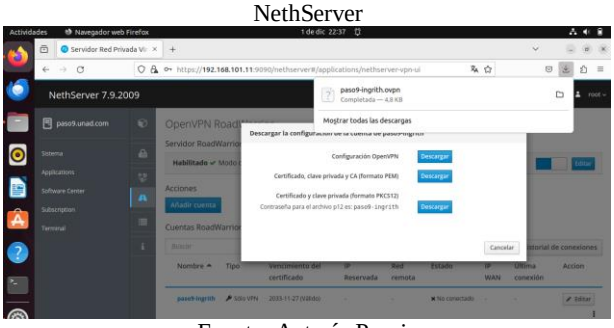
Fuente: Autoría Propia

Figura 84. Configuración de la cuenta RoadWarrior en NethServer

Fuente: Autoría Propia

Una vez creada la cuenta y aplicados los cambios realizados se procede a realizar la descarga de la configuración OpenVPN.

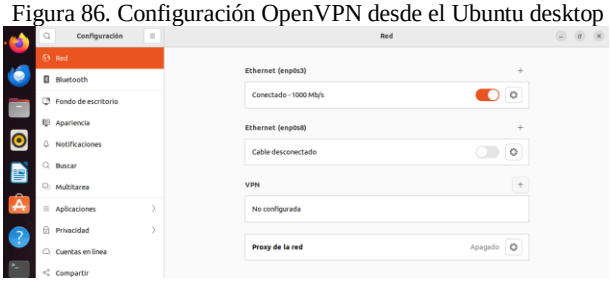
Figura 85. Descarga configuración OpenVPN RoadWarrior en NethServer



Fuente: Autoría Propia

Luego que termine la descarga, hay que dirigirse a configuración al apartado VPN y se selecciona en el símbolo + para añadir la VPN.

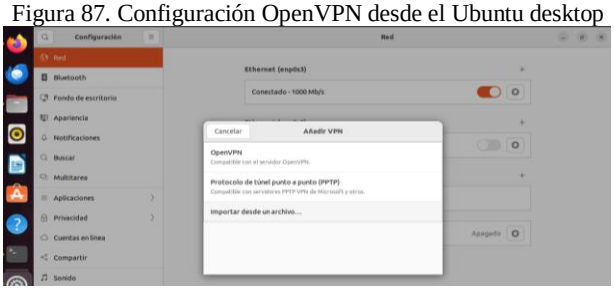
Figura 86. Configuración OpenVPN desde el Ubuntu desktop



Fuente: Autoría Propia

Cuando se abra la pestaña para añadir la VPN se selecciona la opción importar desde un archivo.

Figura 87. Configuración OpenVPN desde el Ubuntu desktop



Fuente: Autoría Propia

Luego se selecciona el archivo descargado de NethServer y se da en abrir.

Figura 88. Importación archivo OpenVPN desde el Ubuntu desktop

Fuente: Autoría Propia

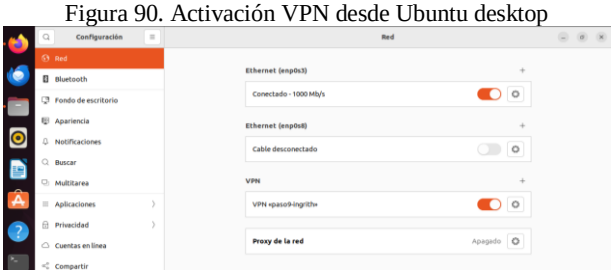
Una vez aparezcan cargados los archivos importados se selecciona añadir.

Figura 89. Configuración OpenVPN desde el Ubuntu desktop

Fuente: Autoría Propia

Luego se conecta la VPN añadida.

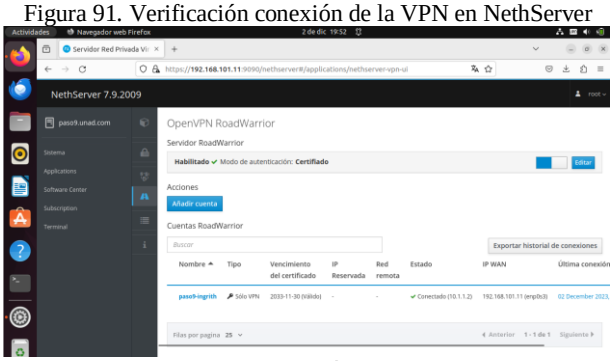
Figura 90. Activación VPN desde Ubuntu desktop



Fuente: Autoría Propia

Finalmente hay que regresar al NethServer para verificar la conexión de la VPN.

Figura 91. Verificación conexión de la VPN en NethServer

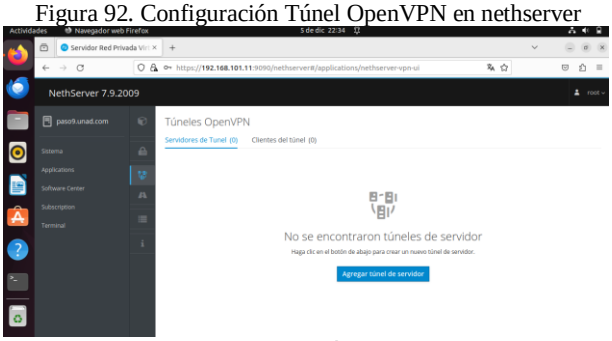


Fuente: Autoría Propia

3.5.2 CONFIGURACIÓN TÚNEL OPENVPN

Se inicia con la configuración del Túnel OpenVPN, para ello se selecciona Agregar túnel de servidor, ingresando a la opción túnel OpenVPN.

Figura 92. Configuración Túnel OpenVPN en nethserver



Fuente: Autoría Propia

Para la configuración del Túnel OpenVPN se debe asignar un nombre y se deben tener en cuenta las redes configuradas. De este modo, en la opción red Direcciones públicas se debe escribir la IP de la red WAN, en redes locales va la red LAN y en redes remotas la red DMZ. Luego, se da en la opción guardar.

Figura 93. Configuración Túnel OpenVPN en nethserver

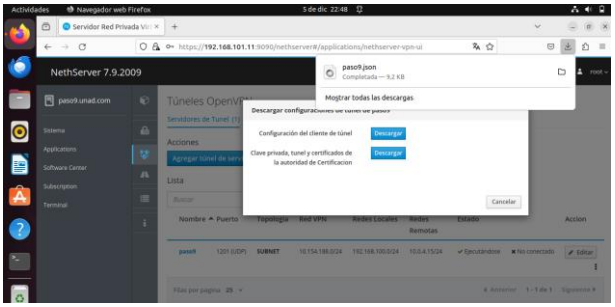
Fuente: Autoría Propia

Figura 94. Configuración Túnel OpenVPN en nethserver

Fuente: Autoría Propia

Una vez guardados los cambios se procede a realizar la descarga de la configuración del cliente de túnel.

Figura 95. Descarga configuración Túnel OpenVPN en nethserver



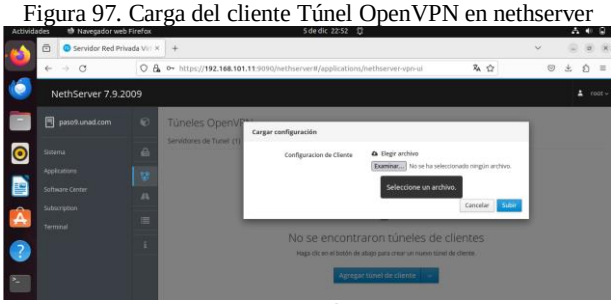
Fuente: Autoría Propia

Luego, hay que dirigirse a la opción clientes del túnel, allí se cargara el archivo descargado en el item agregar túnel del cliente – cargar configuración.

Figura 96. Carga del cliente Túnel OpenVPN en nethserver

Fuente: Autoría Propia

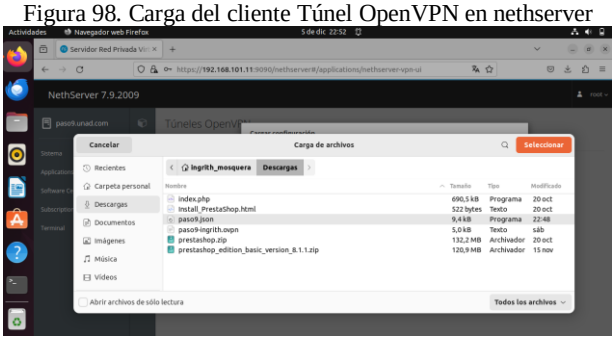
Figura 97. Carga del cliente Túnel OpenVPN en nethserver



Fuente: Autoría Propia

Se selecciona el archivo descargado y luego da en la opción subir.

Figura 98. Carga del cliente Túnel OpenVPN en nethserver



Fuente: Autoría Propia

Figura 99. Carga del cliente Túnel OpenVPN en nethserver

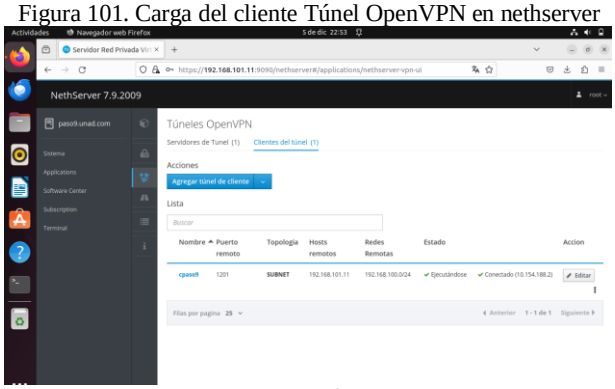
Fuente: Autoría Propia

Figura 100. Carga del cliente Túnel OpenVPN en nethserver

Fuente: Autoría Propia

Una vez finalice la carga del archivo se evidencia la correcta conexión realizada.

Figura 101. Carga del cliente Túnel OpenVPN en nethserver



Fuente: Autoría Propia

4 CONCLUSIONES

Para finalizar, se pudo establecer una ruta de análisis e investigación sobre la instalación y el uso de NethServer, evidenciando que ofrece una gran variedad de servicios como lo es el servidor DHCP el cual es indispensable en las redes, aparte de que permite la comunicación entre estaciones de trabajo, ya que la asignación de IP para conectarse es por solicitud al DHCP Server y este recurra a sus bases de datos para verificar la configuración de redes asignadas y así dentro de ese rango asignar de forma automática la IP.

El Servidor DNS tiene su reconocimiento como servidor de nombres, ya que su servicio permite interpretar la dirección IP proporciona por un nombre de dominio dado, teniendo en cuenta sus bases de datos realiza el proceso de traducir la información, pues para el usuario es más fácil memorizar el nombre del dominio que la IP.

Para configurar un controlador de dominio se debe hacer una active directory en la interfaz de Nethserver para que funcione como un servidor que almacenara la información de las cuentas tanto de usuarios como grupos y la información de seguridad del dominio creado, y finalmente desde la terminal del equipo cliente unir el equipo con el dominio.

Una vez realizada la actividad se procede a dar solución a las problemáticas de migración del sistema operativo Nethserver, donde se realizó la instalación del servidor con sus respectivas configuraciones y lograr el objetivo general de la 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.

El desarrollo de la actividad permitió profundizar en una nueva distribución de Linux útil para la administración de servidores y poner rápidamente en funcionamiento una variedad de servicios. En este caso, Nethserver fue útil para darle seguridad a la red verde y naranja usando cortafuegos, los cuales, permitieron controlar los permisos que se tienen sobre los sitios web que se visitan.

La actividad permitió poner un funcionamiento un firewall o cortafuegos, lo cual fue bastante interesante, ya que este concepto es muy usado en el monto tecnológico. Este tipo de sistemas de seguridad permiten restringir el acceso a diversas actividades cuando se navegue por una red particular.

Se puede concluir que la implementación del file server y el print server utilizando NethServer brinda flexibilidad al momento de gestionar estos servicios, esto por supuesto facilita y asegura el intercambio de información de manera segura, ya que se cuenta con capas de autenticación para acceder a los diferentes recursos configurados. Esta seguridad no sólo protege los datos almacenados en el servidor de datos, sino que también protege la integridad de toda la red.

La capacidad de administrar fácilmente el acceso ayuda a cumplir con los requisitos de privacidad y seguridad asegurando el acceso solo a usuarios autorizados previamente. En resumen, utilizar NethServer para manejar dichos servicios no sólo es una opción optima, sino también una buena opción que beneficia a la escalabilidad de la infraestructura donde se implemente.

Debido a la simplicidad y la administración centralizada hace que configurar y gestionar una VPN en nethserver sea más sencillo. Las VPN son herramientas importantes para la seguridad y la privacidad en línea, permitiendo a los usuarios acceder a una red privada de forma remota a través de una conexión segura. Con NethServer, se puedo implementar OpenVPN. Por lo anterior, con el desarrollo de este trabajo se evidencia la instalación e implementación de los servicios de la VPN OpenVPN a través de NethServer, verificando el funcionamiento de la VPN creada, dando así soluciones óptimas a la problemática planteada.

5 REFERENCIAS

[1] "NethServer: Conoce esta distro basada en CentOS/RHEL para crear tu propio servidor en casa u oficina". RedesZone. Accedido el 2 de diciembre de 2023. [En línea]. Disponible: https://www.redeszone.net/2016/09/26/nethserver-conoce-esta-distro-basada-centosrhel-crear-propio-servidor-casa-u-oficina/

[2] "Getting Started With Nethserver". Nethserver. Accedido el 2 de diciembre de 2023. [En línea]. Disponible: https://www.nethserver.org/getting-started-with-nethserver/

[3] Manuel Cabrera Caballero. (2018, 16 octubre). NethServer tutorial | Instalación, actualización y primeros pasos [Vídeo]. YouTube. https://www.youtube.com/watch?v=FNGmM-2fa_0

[4] Manuel Cabrera Caballero. (2018, octubre 22). Nethserver Tutorial. | Configurando DHCP Server [Vídeo]. YouTube. https://www.youtube.com/watch?v=GrvZutNZIRg

[5] Nethserver Controlador Primario de Dominio (PDC). (s. f.-b). Configura Ubuntu, Proxmox, Zabbix & NethServer para entornos de Oficina. http://911-ubuntu.weebly.com/nethserver-pdc/nethserver-como-pdc-primary-domain-controller

[6] Harold Achipiz. (2022, 15 febrero). Unir clientes Ubuntu y Windows a Zentyal [Vídeo]. YouTube. https://www.youtube.com/watch?v=hQn4tvIaHJc

[7] Y. Fernández. "Firewall: qué es un cortafuegos, para qué sirve y cómo funciona". Xataka - Tecnología y gadgets, móviles, informática, electrónica. Accedido el 2 de diciembre de 2023. [En línea]. Disponible: https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

[8] "Carpetas compartidas — NethServer 7 Final". Administrator Manual — NethServer 7 Final. Accedido el 3 de diciembre de 2023. [En línea]. Disponible: https://docs.nethserver.org/es/v7/shared_folder.html#shared-folders-section

[9] "Shared folders — NethServer 7 Final". Administrator Manual — NethServer 7 Final. Accedido el 3 de diciembre de 2023. [En línea]. Disponible: https://docs.nethserver.org/en/v7/shared_folder.html

[10] "The old Server Manager — NethServer 7 Final". Administrator Manual — NethServer 7 Final. Accedido el 3 de diciembre de 2023. [En línea]. Disponible: https://docs.nethserver.org/es/v7/base_system.html

[11] Tim Mocan. (2019) ¿Qué Es OpenVPN y Cómo Funciona OpenVPN? . https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-openvpn/

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