“SOLUCIÓN INTEGRAL DE SERVICIOS DE REDES CON NETHSERVER”

Diego Hernando Marín Suárez
e-mail: dhmarins@unadvirtual.edu.co
Rosa Carrillo Riaño
e-mail: rcarrillor@unadvirtual.edu.co
Fabian Andrés Suarez Guerrero
e-mail: fasuarezgu@unadvirtual.edu.co
Cristian Andrés Collazos Ariza
e-mail: cacollazosa@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación y puesta en marcha de un servidor para centralizar servicios de IT con NethServer en fase de prototipado. En base a una topología de red segmentada en red LAN, DMZ y WAN, se implementa el servicio DHCP para el direccionamiento dinámico, DNS para la resolución de nombres de dominio y conectividad, directorio activo para la gestión de usuarios. Además, se implementa un firewall para agregar seguridad a través del cortafuegos, servidor de archivos e impresoras para compartir información y recursos así servicio VPN para conectar clientes de forma remota segura a una red privada. Finalmente, este artículo permite evidenciar la funcionalidad y como a través del uso de herramientas Open Source se puede implementar una infraestructura completa de servicios de tecnología aplicable a diferentes entornos productivos.*

PALABRAS CLAVE: NethServer, DHCP, DNS, controlador de dominio, proxy. firewall, servidor de archivos, servidor de impresión, VPN, LDAP, Samba y Samba Client, LAN, Virtual Box, Ubuntu, WAN, IP, Software Center.

1 INTRODUCCIÓN

En un mundo cada vez versátil y digitalizado, la necesidad que las organizaciones enfrentan en la optimización de sus recursos e infraestructura tecnológica se hace cada vez más esencial para mantener y asegurar sus operaciones haciéndolas eficientes, escalables y seguras. En este contexto, las herramientas de código abierto son una alternativa económicamente viable en comparación con las soluciones propietarias, ofreciendo escalabilidad, personalización y una amplia comunidad de soporte.

Este artículo presenta la implementación de NethServer, una plataforma Open Source basada en CentOS, como una solución integral para la gestión de servicios críticos de infraestructura de TI. NethServer permite la configuración y administración centralizada de múltiples servicios, tales como servidor DHCP, DNS, directorio activo, firewall, servidor de archivos, servidor de impresión y VPN, los cuales se abordarán en el presente artículo.

2 NETHSERVER

2.1 CARACTERÍSTICAS GENERALES

NethServer es una herramienta que permite gestionar servicios de IT de fácil configuración y administración. Es una distribución de Linux, basada en CentOS. Permite la administración por medio de una consola WEB y gestiona servicios como: DNS, DHCP, VPN, firewall, Proxy, servidor WEB, servidor de archivos samba, correo electrónico, entre otros.

2.2 INSTALACIÓN

Se ingresa al repositorio de NethServer en GitHub a través del siguiente link *https://github.com/NethServer/dev/releases* y se descarga la versión .iso más reciente disponible en este formato: *nethserver-7.9.2009-x86_64.iso*. Luego, se crea una máquina en virtual box para ejecutar la imagen y se le crea tres adaptadores de red: uno para la red verde (LAN), otra para la red Naranja (DMZ) y la otra para la red Roja (WAN) o red de internet:

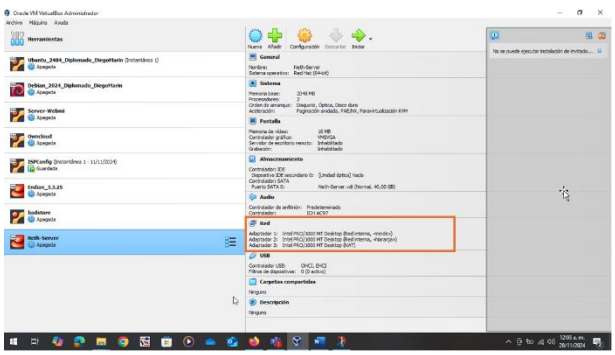

Imagen 1. Resumen máquina para NethSever

Una vez configurada la máquina virtual, se ejecuta para iniciar la instalación:

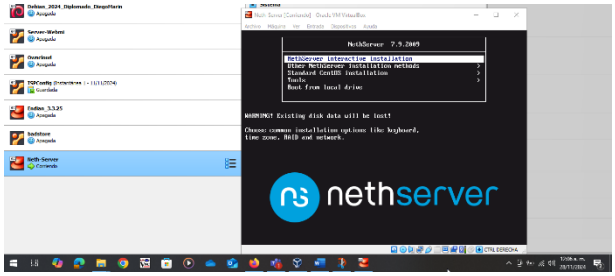

Imagen 2. Ejecutar instalación NethServer

Durante el proceso se siguen las instrucciones del instalador y finalmente así se ve la máquina instalada con Nethserver y accedida desde consola:

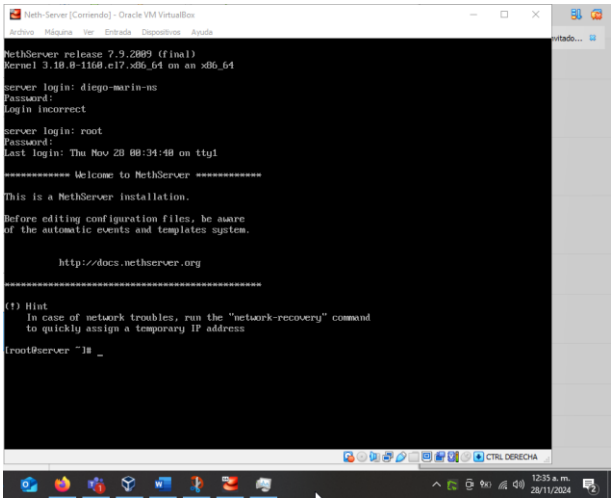

Imagen 3. Nethserver instalado

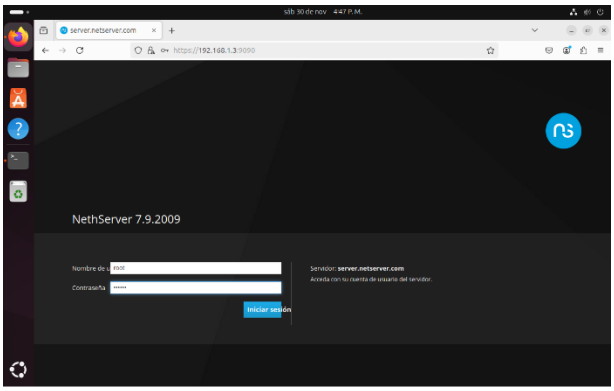

Imagen 4. Acceder a través de consola web desde un equipo cliente

3 TEMÁTICA 1: DHCP, DNS Y CONTROLADOR DE DOMINIO

Antes de iniciar las configuraciones, es importante asignar el nombre de host, cambiar la información de empresa y asignar DNS que permitan la navegación a internet en Sistema > Panel de control:

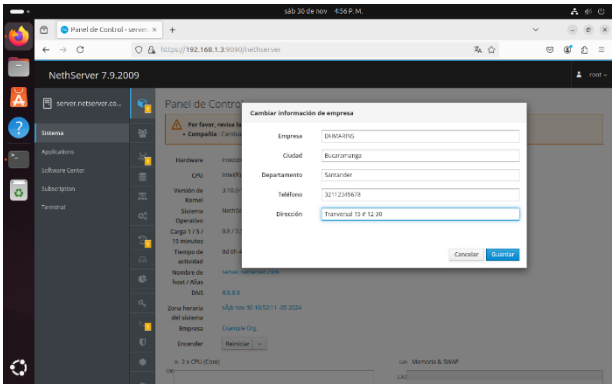

Imagen 5. Modificar parámetros necesarios en panel de control

Además, se deben configurar los tres adaptadores de las redes *Verde, Naranja y Roja*:

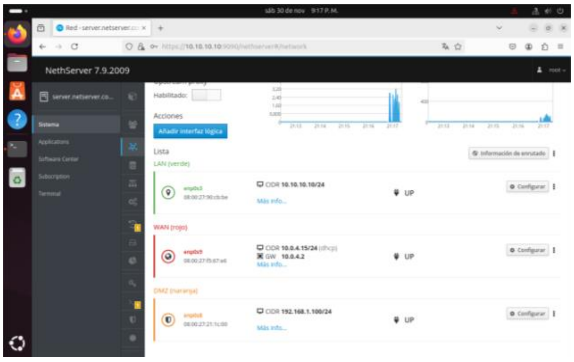

Imagen 6. Red verde, naranja y roja

3.1 DHCP

En Sistema > DHCP se establece el rango de direccionamiento dinámico para la red verde:

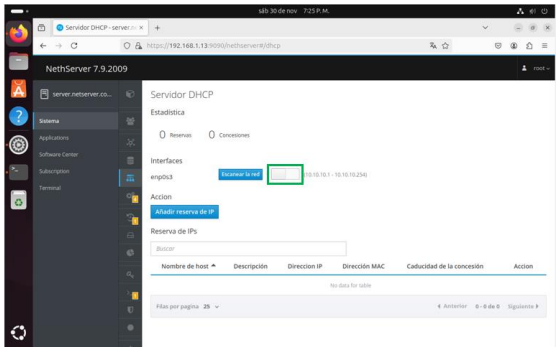

Imagen 7. Activar DHCP en interfaz de red verde

Se establece el rango y el dominio:

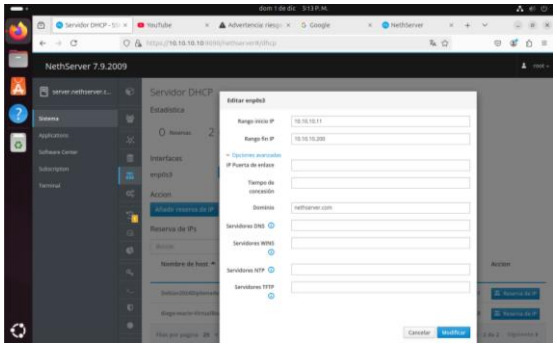

Imagen 8. Rango DHCP

Finalmente, en el equipo cliente se establece el adaptador de red en red interna “verde” y configurado por DHCP se valida que reciba direccionamiento:

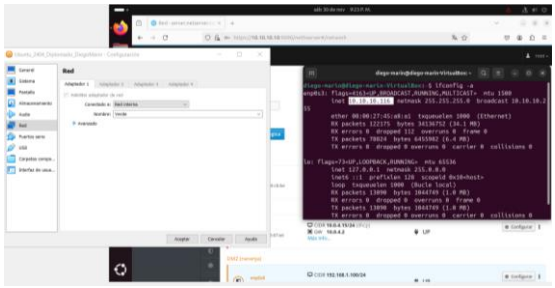
Imagen 9. Prueba de conexión

De esta forma ya queda establecido el servicio DHCP por la red verde.

3.2 DNS

En Sistema > DNS se ingresa para añadir un nuevo registro DNS:

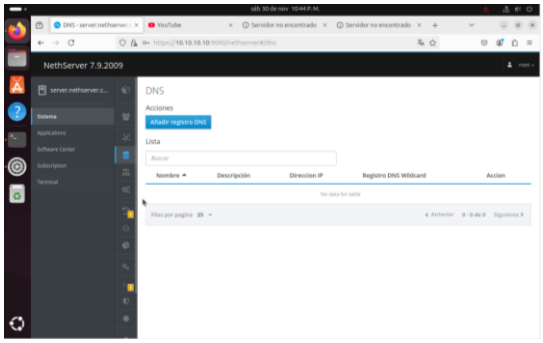

Imagen 10. Añadir registro DNS

Se establece el nombre de host y la dirección IP por la cual va a resolver nombres de dominio (la misma de la interfaz verde):

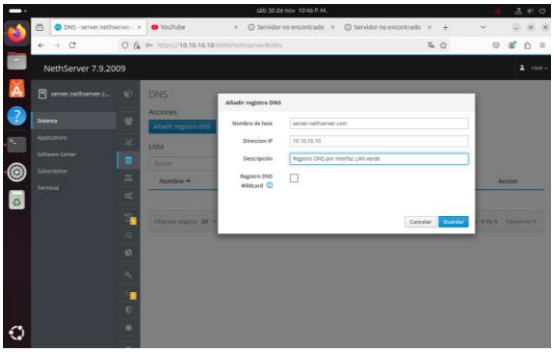

Imagen 11. Añadir parámetros de registro DNS

Una vez configurado, se valida desde el cliente que resuelva el dominio y servicios de internet:

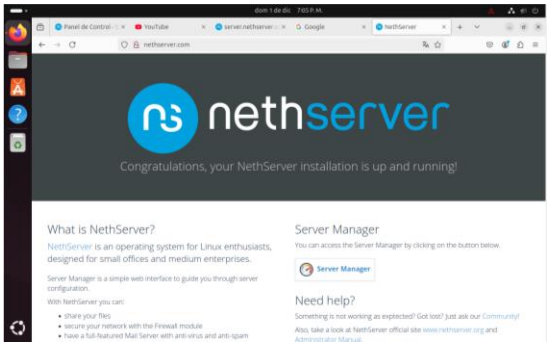

Imagen 12. Validar resolución de DNS

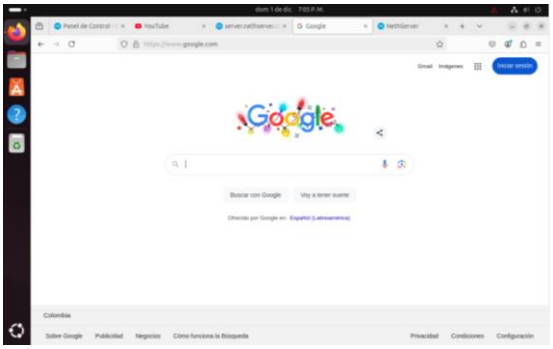

Imagen 13. Validar navegación en internet

De esta forma se valida que la configuración DNS surge efecto.

3.3 CONTROLADOR DE DOMINIO

Para agregar el Dominio, se ingresa por Sistema > Usuarios y Grupos, y se crea un nuevo proveedor de cuentas. Se selecciona Active Directory:

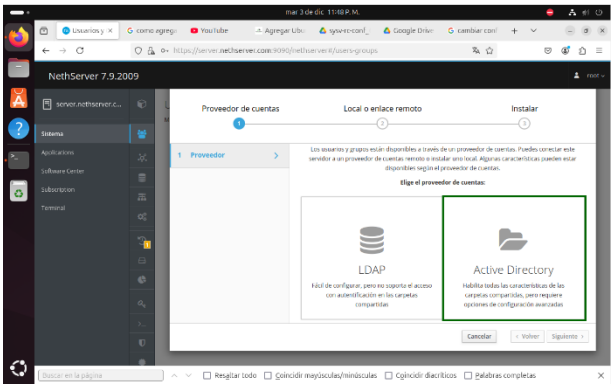

Imagen 14. Seleccionar proveedor de cuentas

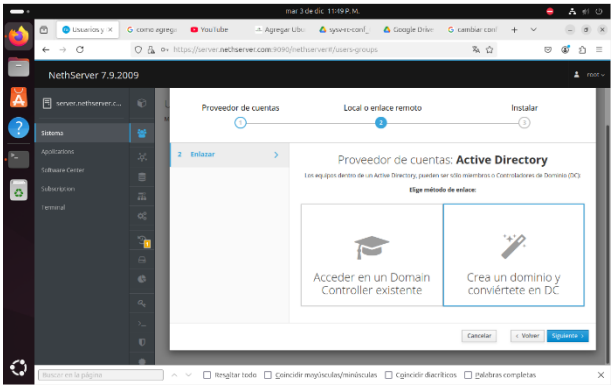

Imagen 15. Crear dominio

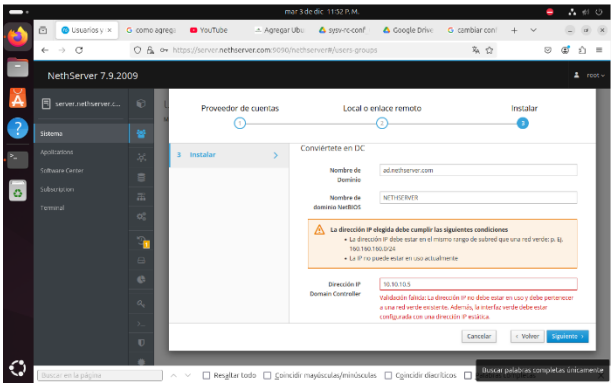

Imagen 16. Configuraciones de DC

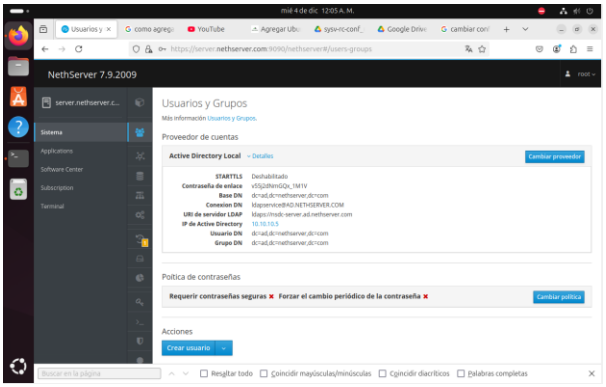

Imagen 17. Información de directorio activo creado

Luego, se habilitan usuarios y se crea un usuario nuevo:

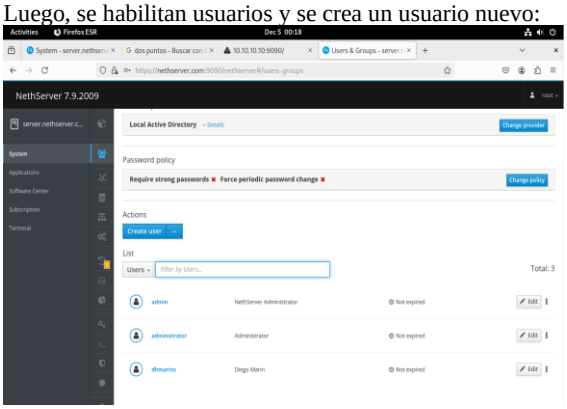

Imagen 18. Usuarios existentes

3.3.1 Configurar equipo cliente para unir al dominio

Antes de iniciar, se debe validar que la tarjeta de red del servidor para la red verde que permita el modo promiscuo:

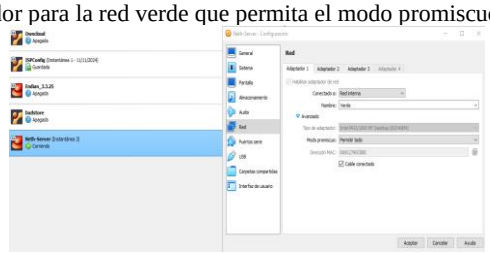

Imagen 19. Permitir modo promiscuo

Luego, en el equipo cliente se debe descargar la librería pbis que permite y facilita la integración con el directorio activo:

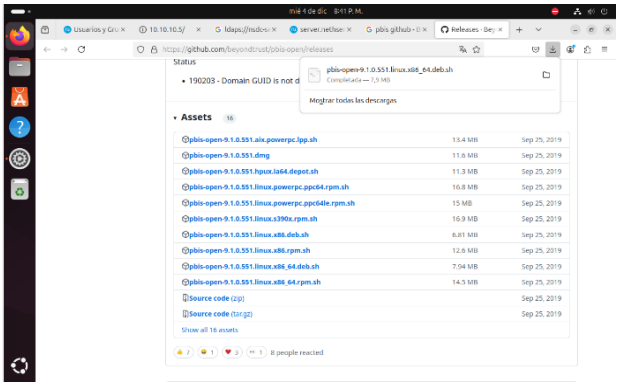

Imagen 20. Descargar librería pbis

Una vez descargada, por terminal, en la ubicación de descarga, se ejecuta el comando *chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh* y luego de eso se ejecuta el paquete con el comando *sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh*. Cuando finaliza la instalación se muestra de la siguiente forma:

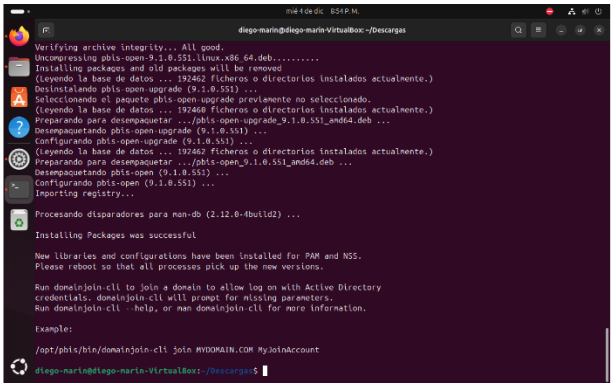

Imagen 21. Instalación de paquete pbis

Luego se une al dominio con el siguiente comando, especificando el dominio del directorio activo y un usuario administrador:

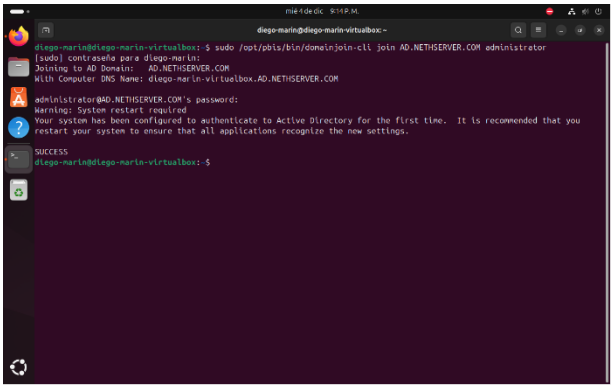

Imagen 22. Comando para unir al dominio

3.3.2 Prueba de conexión a Dominio

Luego se reinicia el equipo cliente y se accede por otro usuario para ingresar con un usuario de dominio:

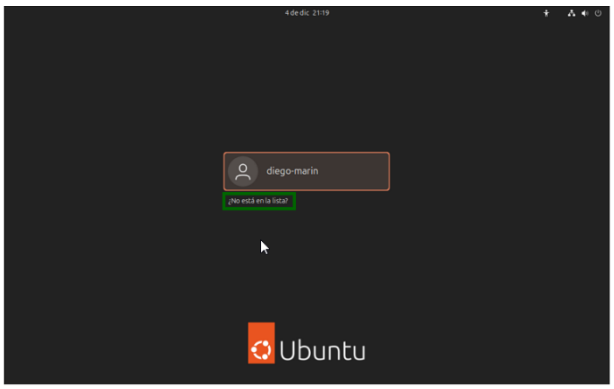

Imagen 23. Seleccionar *¿No está en la lista?*

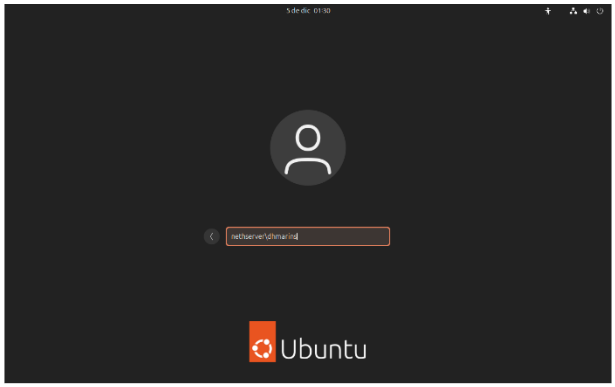

Imagen 24. Ingresar nombre de usuario de dominio

Luego se ingresa la contraseña asignada cuando se creó el usuario y puede iniciar sesión. Finalmente se comprueba el acceso:

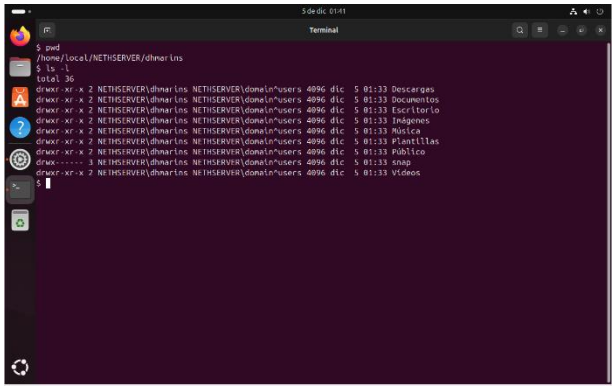

Imagen 25. Validación login usuario *dhmarins*

4 TEMATICA 2: PROXY

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 ingreso a la interfaz web de NethServer se realiza desde un navegador web en la máquina Ubuntu Desktop utilizando la dirección IP de la red LAN (Verde), el usuario root y la contraseña. Una vez se ingresa, se muestra el módulo del sistema con el estado y la configuración básica.

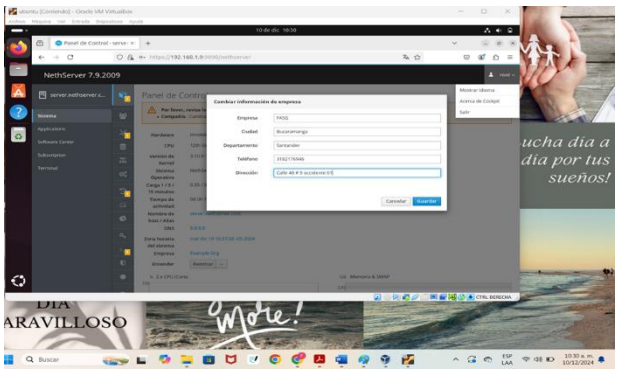

Imagen 26. Información básica de la empresa.

Se configuran las diferentes redes para las conexiones de los dispositivos. Primero se configura la red WAN (Roja) para dejarla con acceso a Internet.

Para realizarlo, se selecciona y se realiza la asignación de la dirección IP, máscara de red y puerta de enlace. Esta última es la que permite acceso a internet.

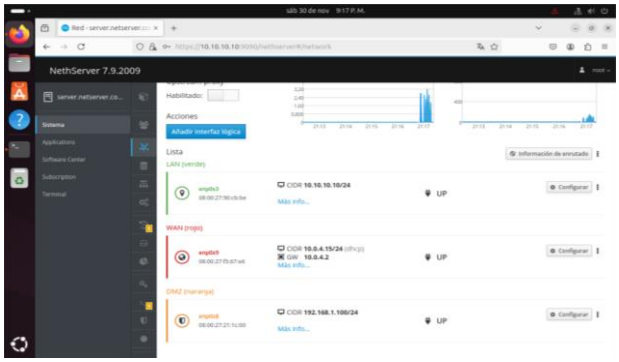

Imagen 27. Redes LAN, WAN y DMZ

Finalizada la configuración y asignación de direcciones IP a cada una de las redes, se inicia el proceso de configuración del Web Proxy para filtrar el contenido web mediante un servidor proxy.

Para esto, se instala la aplicación Filtro web y el Proxy web desde el panel Software Center. Una vez finalice instalación, las aplicaciones se localizan en el Panel Aplicaciones.

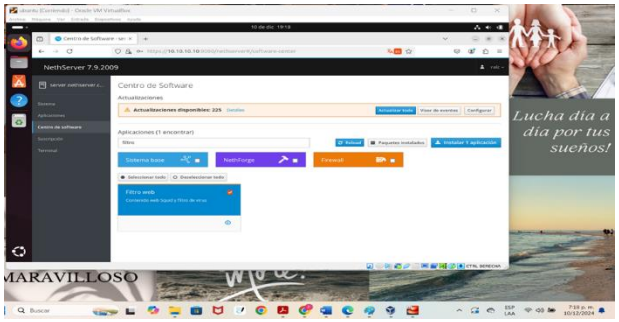

Imagen 28. Filtro web

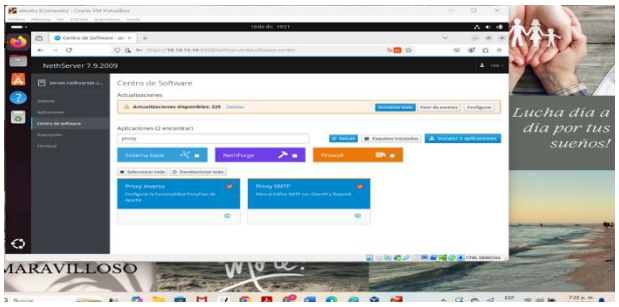

Imagen 29. Proxy web.

Posteriormente se puede configurar los DNS y el Servidor DHCP desde el panel Sistemas.

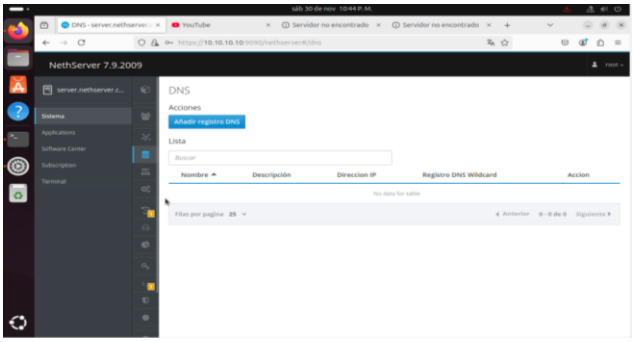

Imagen 30. Añadir registro DNS

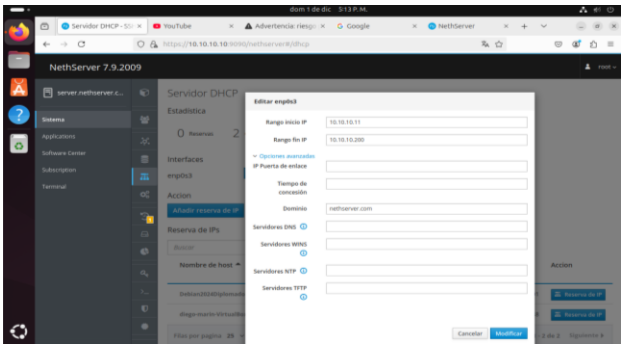

Imagen 31. Configuración Servidor DHCP

Ahora, se procede a configurar el Proxy desde el panel Web Proxy y Filter. Para ello, en el Modo de zonas VERDES se selecciona SSL Transparente. El modo zonas AZULES se deja en Manual.

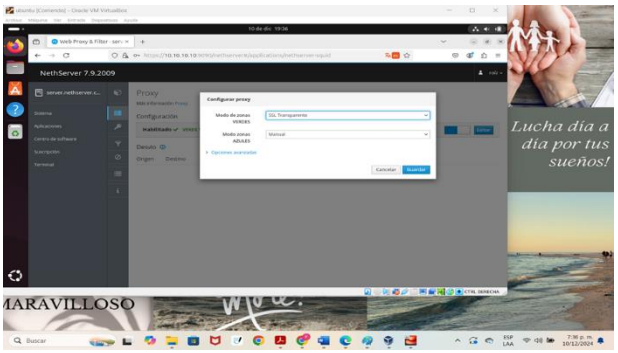

Imagen 32. Configuración proxy.

Desde el panel Web Proxy y Filter y la sección Categorías, se descarga y configura la lista de categorías. Para este caso "Université Toulouse (free)" esta categoría ayuda aplicar los filtros a un grupo de páginas definidas por categorías.

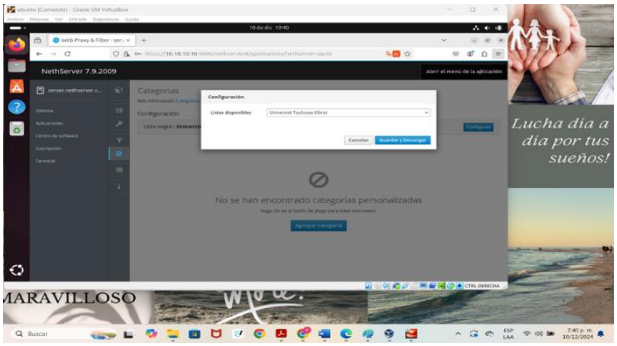

Imagen 33. Descargar lista de Categorías.

Desde la sección Filtro del panel Web Proxy y Filter, se seleccionan las Categorías y el modo en que se desea aplicar el filtrado.

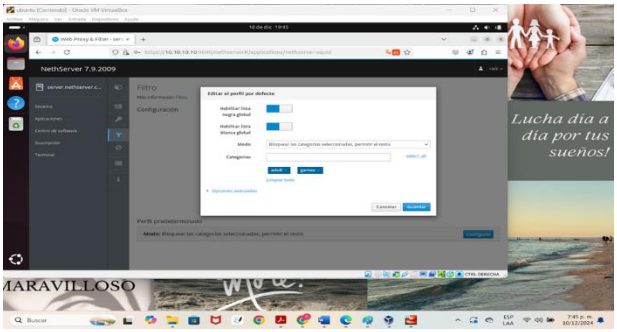

Imagen 34. Categorías y Modo de Filtrado.

Para este caso se aplica filtro a las categorías adult y games. Esto permitirá bloquear sitios web para adultos y sitios de juegos.

Para comprobar que el proxy está filtrando las categorías que se han bloqueado, se procede a acceder desde un navegador a algunas páginas de contenido para adulto y con contenido para juegos.

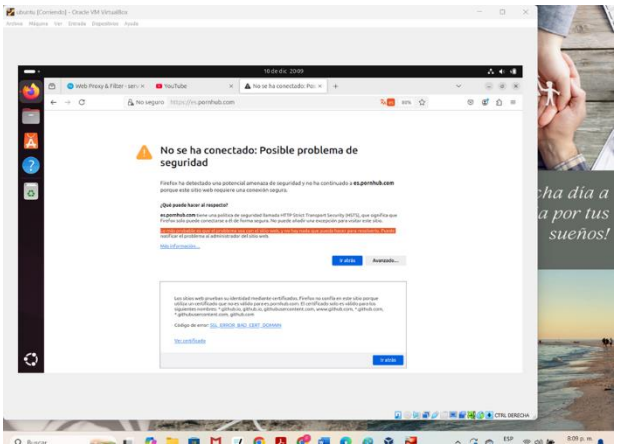

Imagen 35. Sitio Web adultos bloqueado.

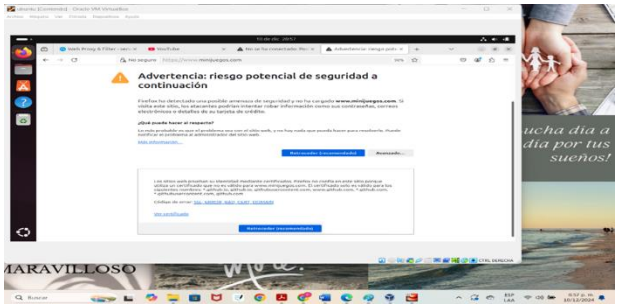

Imagen 36. Sitio Web juegos bloqueado.

5 TEMÁTICA 3 FIREWALL - 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.

Ahora bien, para iniciar la configuración del Firewall en NethServer, se debe primero tener en cuenta que se deben realizar unas configuraciones especiales, como lo son las LAN y la WAN de la red para que se tomen y se puedan aplicar respectivamente todos los cambios. Para ellos, se debe dar clic en Red para realizar estas configuraciones.

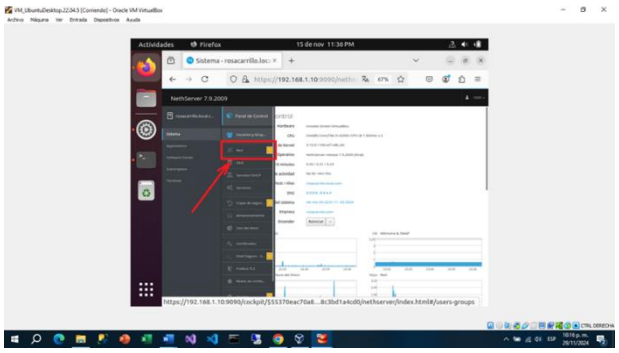

Figura 37. Configuración Red

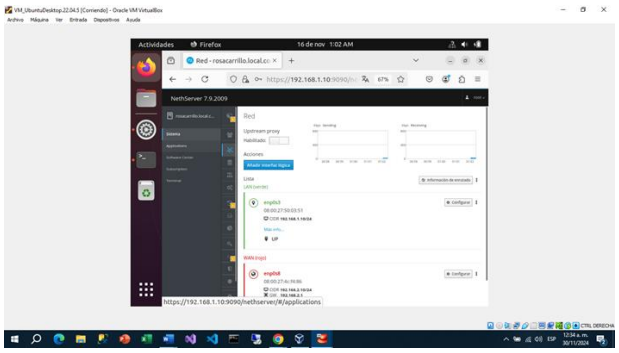

Figura 38. Configuración Red.

Cuando se realiza la configuración de la WAN, se debe colocar en modo DHCP para que le asigne dinámicamente el direccionamiento IP a la máquina de Escritorio en Ubuntu.

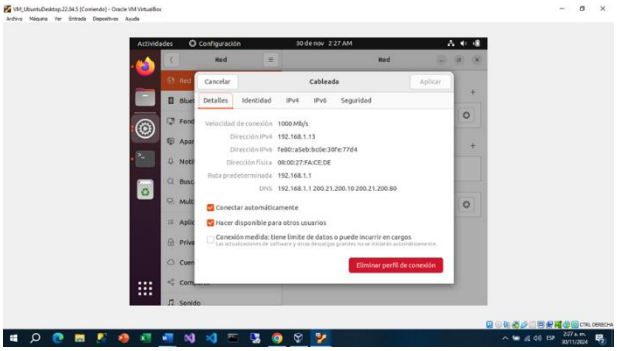

Figura 39. DHCP

Una vez configurado el paso anterior, se procede a realizar la instalación del Firewall, desde el Software Center, sin embargo, se debe revisar que no existan actualizaciones pendientes por aplicar, si existen, se deben aplicar antes de realizar la instalación del firewall, que en este caso se evidencia que existen por ende se procederá a realizar estas actualizaciones.

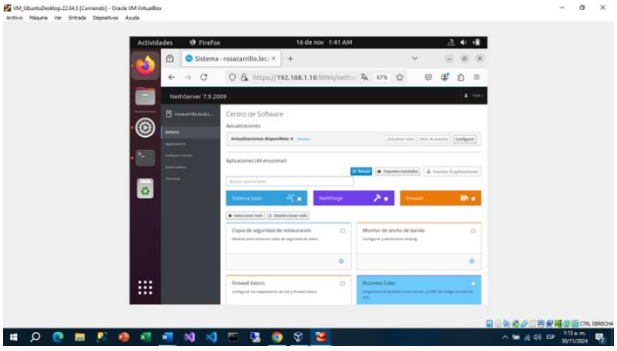

Figura 40. Firewall

Ahora sí, una vez actualizadas todas las aplicaciones, se debe habilitar el firewall, dando clic en “Firewall Básico” después se debe dar clic en “Instalar 1 Aplicación” y seguir el proceso de instalación.

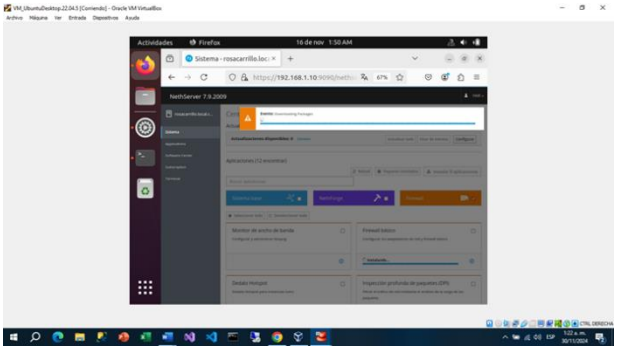

Figura 41. Firewall.

Una vez se realiza la instalación, de esta aplicación, se debe dirigir al menú de aplicaciones y acto seguido se debe dar clic en los 3 puntos de la opción de firewall, esto con el fin de tener la configuración por acceso directo en la interfaz.

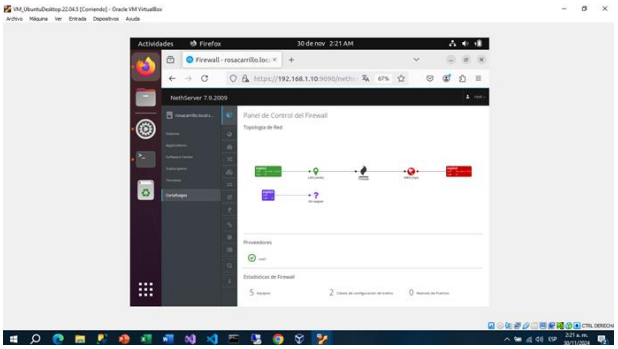

Figura 42 Firewall

Antes de realizar la creación de las reglas se debe realizar una verificación de que desde la máquina de escritorio se acceda correctamente a redes sociales y portales de entretenimiento, entre otros.

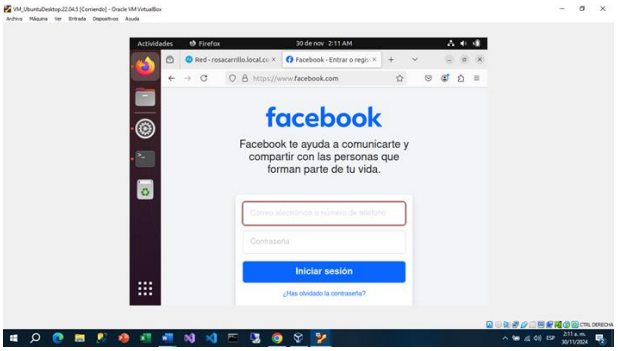

Figura 43 Creación de Reglas.

Acto seguido, se debe proceder a la configuración de las reglas de bloqueo en el Firewall, dando clic en “Reglas” y después en “Agregar Reglas” y seguir el instructivo, también se debe verificar la IP de la Máquina a la que se le van a aplicar las distintas reglas para probar y así mismo se debe realizar un nslookup a los dominios que se quieren bloquear para tener el listado de ips respectivas, (www.facebook.com, www.youtube.com, www.whatsapp.com, www.vanguardia.com).

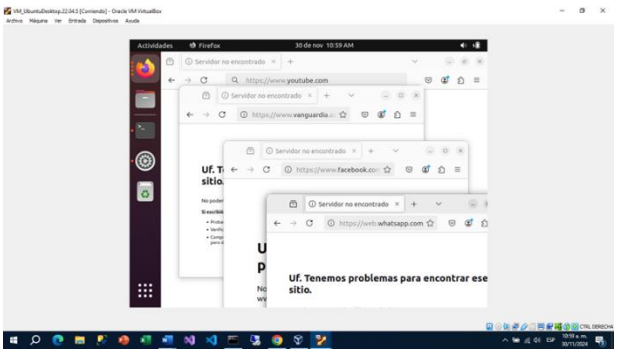

Figura 44. Reglas de Bloqueo

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Para realizar la configuración del File Server y Print Server se debe instalar en el NetServer las aplicaciones de “Servidor de Archivos” y “Servidor de Impresión”.

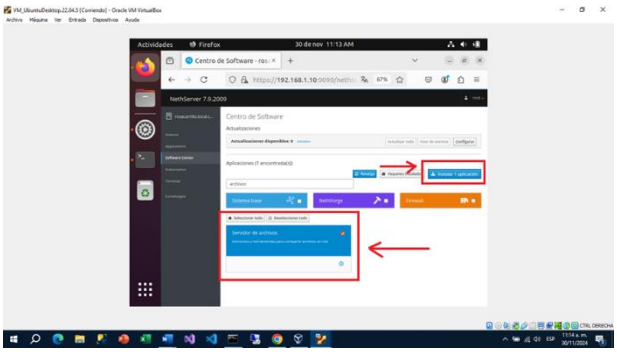

Figura 45. File Server y Print Server

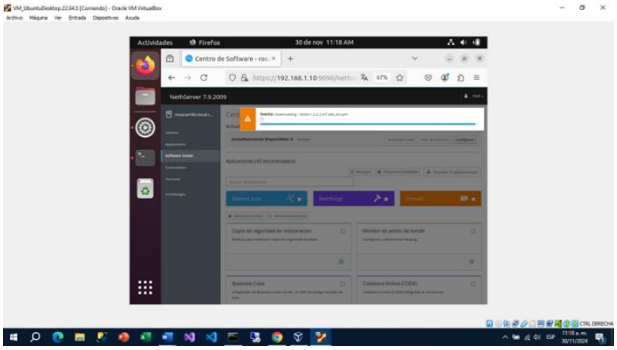

Figura 46. File Server y Print Server.

Una vez realizada, la instalación se deben crear accesos directos para tener más fácil la configuración de estos servicios.

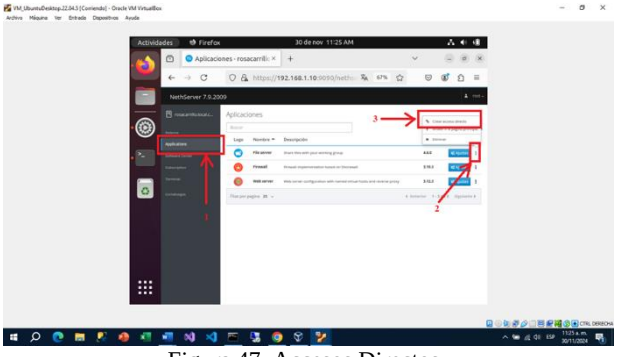

Figura 47. Accesos Directos.

Ahora se debe configurar el LDAP, para realizar la autenticación, autorización y perfilamiento de los usuarios para acceder a los diferentes recursos compartidos tanto de archivos como dispositivos de impresión. Para ello se debe configurar esta característica instándola y siguiendo el instructivo respectivo.

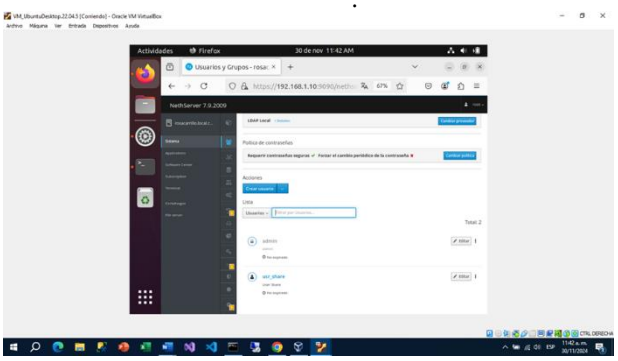

Figura 47. Configuración LDAP.

Ahora se debe dar clic en “File Server” y acto seguido en “Auditoria” para realizar las diferentes configuraciones, en las que se incluye la instalación de los paquetes asociados.

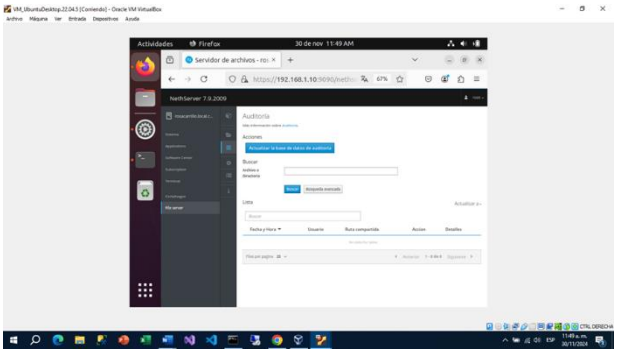

Figura 49. File Server.

Ahora bien, si se realizara la configuración de las carpetas a compartir y otras configuraciones relacionadas, como lo es la configuración del lado del cliente del “SAMBA Y SAMBA CLIENT” para poder conectarse al servidor de archivos y de impresión a través de este protocolo y poder setear la configuración necesaria, que en este caso no sería ninguna, pero hay que tener en cuenta que si se desea configurar un WorkGroup distinto al de por defecto hay que configurar en el cliente ese mismo WorkGroup para que se puedan conectar adecuadamente.

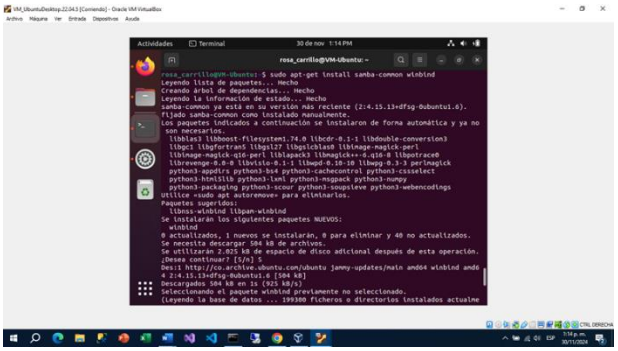

Figura 50. SAMBA Y SAMBA CLIENT.

7 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.

Una vez instalado, obtén la IP asignada al servidor con el comando *ip a*:

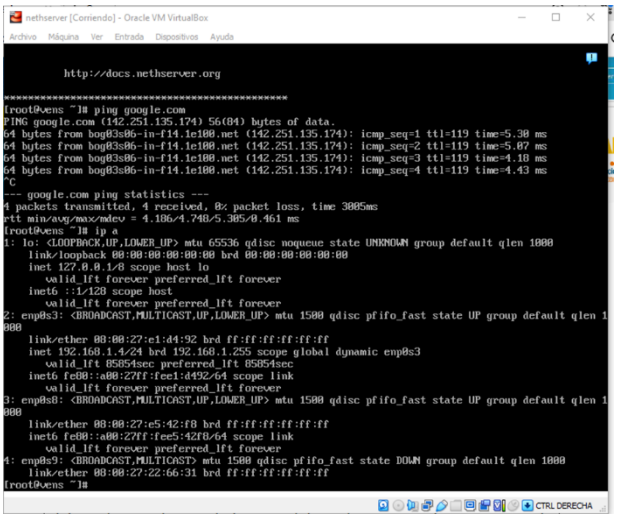

Imagen 51. Configuración IP

Abre un navegador en otro dispositivo y accede a:

https://<IP_DEL_SERVIDOR>:980

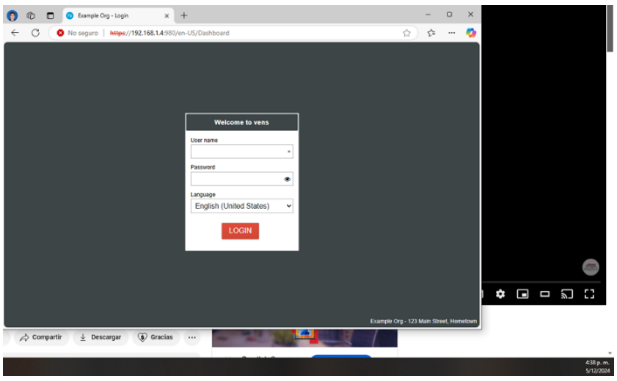

Imagen 52. Acceso plataforma

Inicia sesión con el usuario `root` y su contraseña.

Define las interfaces de red:
LAN: Red interna.
WAN: Conexión a Internet.
DMZ: Para servicios expuestos.

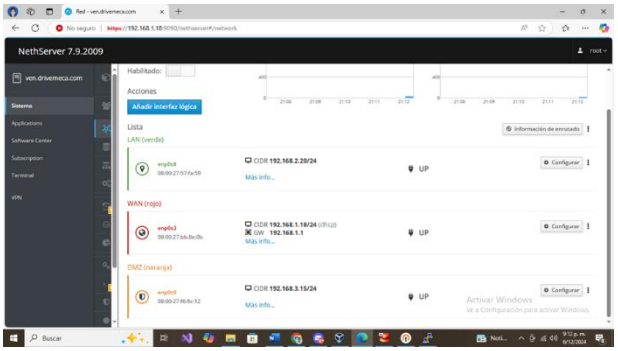

Imagen 53. Interfaz

Cambia el puerto por defecto (22) a otro más seguro, como 2222, desde la interfaz de NethServer.

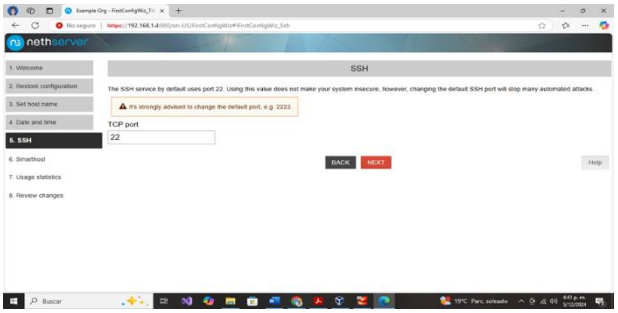

Imagen 54. Cambio de puerto

Descarga el archivo .ovpn generado y transfiérelo a la estación de trabajo GNU/Linux.

Imagen 55. Descarga de OPENVPN

En la estación de trabajo, instala OpenVPN:

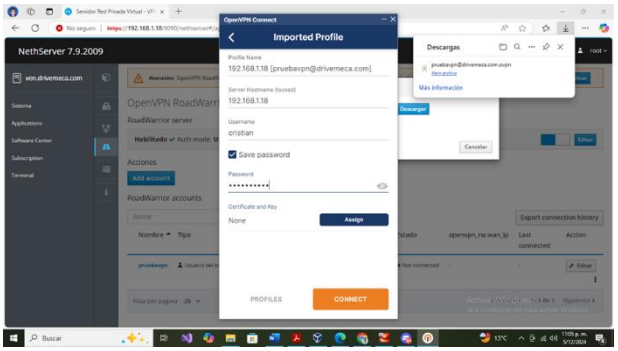

Imagen 56. OPENVPN

Colocamos de grupo LDAP local para poder visualizar los grupos de manera local en el servidor y poder genera un grupo para los usuarios

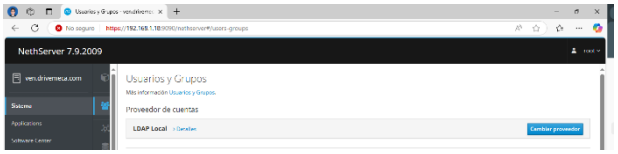

Imagen 57. Grupos

Conéctate con el archivo de configuración:

En este paso creamos creación usuario con usuario nombre de usuario y agregamos el grupo al que tenemos creado además de una contraseña para poder ingresar con usuario y contraseña al túnel de VNP

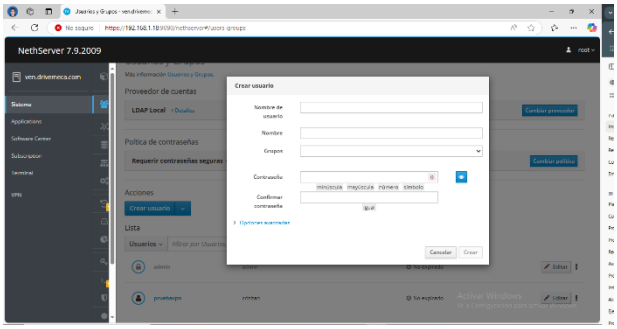

Imagen 58. Usuarios

Imagen 59. Importación de archivo

Damos en BROWSE para poder descargar el archivo creado desde usuarios de vpn

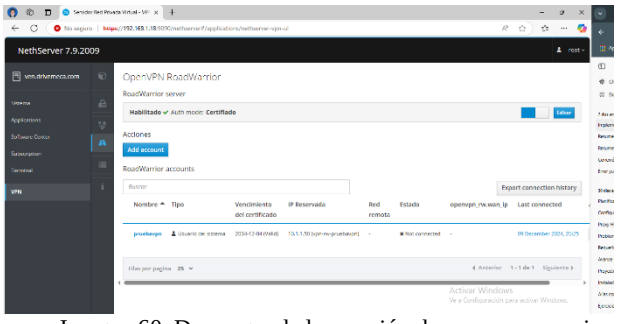

Imagen 60. Descargar de la creación de open vpn warrior

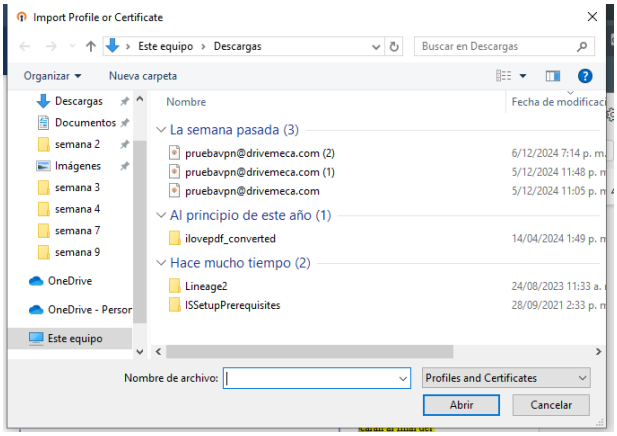

Imagen 61. Búsqueda de archivo de descarga de usuario

Asegúrate de que la VPN esté activa y operativa desde el panel de administración de NethServer.

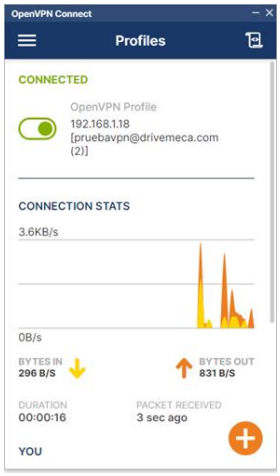

Imagen 62. VPN activa

Con la VPN conectada, accede a recursos de la red interna, como:

Servidores web.

Compartición de archivos.

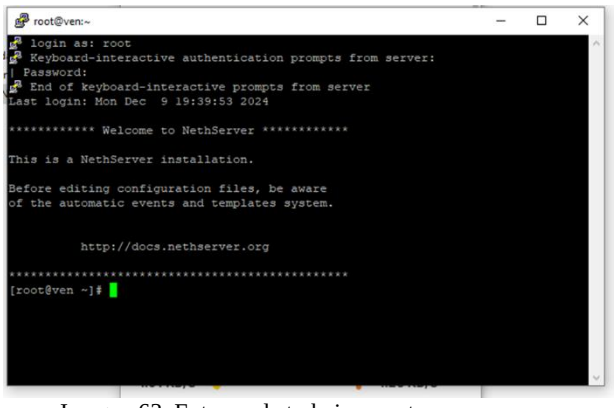

Imagen 63. Entorno de trabajo remoto

8 CONCLUSIONES

Con la implementación de NethServer y puesta en marcha de la solución a las temáticas planteadas, se puede concluir:

1. El servicio DHCP, DNS y servidor de dominio son fundamentales para cualquier implementación tecnológica dentro de una organización. La gestión de direccionamiento IP dinámico, conexión a internet y políticas de directorio activo para la centralización de usuarios y servicios en NethServer facilita su gestión y administración.
2. Configurar un proxy desde Nethserver es una herramienta valiosa para mejorar tu conexión a internet. Además, nos puede ayudar a acceder a contenido restringido, realizar pruebas, depuración de aplicaciones web, monitorear y analizar el tráfico de red.
   Sin embargo, es importante tener en cuenta que los proxies pueden tener sus propias limitaciones y riesgos, como la posibilidad de interceptación de datos o la exposición a malware. Por lo tanto, es fundamental elegir un proxy confiable, seguro y utilizarlo de manera responsable y ética.

3. Se realizó la configuración de interfaces de usuario a través de tareas administrativas con servicios esenciales obteniendo un óptimo nivel de seguridad en el sistema operativo GNU/Linux.

4. Teniendo en cuenta las temáticas escogidas se solucionó gran parte de la problemática planteada, que consistía en la migración de sistemas operativos, servicios y puestas en marcha de los sistemas de seguridad de la infraestructura de red.
   En el desarrollo de esta última fase de la migración y puesta en marcha, se enfatiza en la administración y control de las distribuciones GNU/Linux basada en Ubuntu, implementando servicios de infraestructura IT para intranet y Extranet.

5. La implementación de una VPN utilizando NethServer demuestra la capacidad de esta plataforma open-source para gestionar servicios avanzados de infraestructura IT de manera segura, eficiente y económica. Este proyecto resalta cómo una VPN garantiza la protección de datos y comunicaciones, permitiendo el acceso remoto a recursos internos desde ubicaciones externas a través de un canal encriptado.

9 REFERENCIAS

[1] De Luz, S. (26 de 09 de 2016). RZ redes zone. Obtenido de RZ redes zone: https://www.redeszone.net/2016/09/26/nethserver-conoce-esta-distro-basada-centosrhel-crear-propio-servidor-casa-u-oficina/

[2] Murillo, R. (6 de 11 de 2024). Youtube. Obtenido de Youtube: https://www.youtube.com/watch?v=R7qNw06qOPs

[3] NethServer. (s.f.). Obtenido de NethServer: https://docs.nethserver.org/en/v7/upgrade.html

[4] Red-orbita. (7 de 11 de 2016). Obtenido de Red-orbita: https://red-orbita.com/?p=7494

[5] Forge, S. (09 de 05 de 2023). Source Forge. Obtenido de https://sourceforge.net/projects/nethserver/

[6] LPI. (2022). LPI . Obtenido de https://learning.lpi.org/es/learning-materials/102-500/110/

[7] Canonical. (2018). Help Ubuntu. Obtenido de https://help.ubuntu.com/20.04/ubuntu-help/index.html

[8] Debian. (2020). Debian. Obtenido de https://www.debian.org/releases/stable/amd64/index.es.html

[9] Debian. (2023). Debian. Obtenido de https://www.debian.org/releases/stable/amd64/index.es.html

[10] Documentation, U. (2023). Canonical. Obtenido de https://help.ubuntu.com/20.04/ubuntu-help/index.html