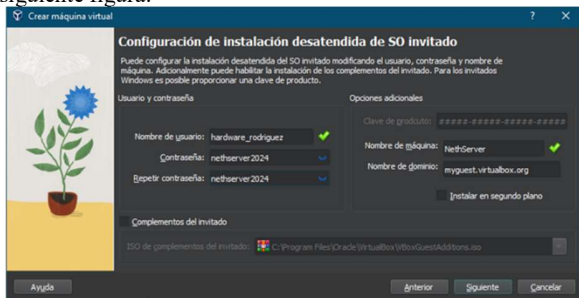


Posterior a ello continuamos con la asignación del nombre de usuario, nombre de maquina y de dominio y la contraseña de la máquina virtual

Figura 2. Asignación de usuario VirtualBox

Aquí asignamos el usuario y el nombre de la máquina virtual en VirtualBox, permitiendo identificar y gestionar la instancia específica del servidor NethServer. Esta configuración es crucial para organizar y diferenciar varias máquinas virtuales en un entorno de pruebas o producción, como se observa en la siguiente figura:

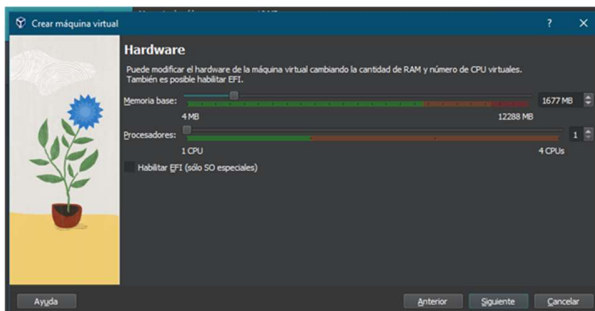


Fuente: Autoría Propia

En este paso asignamos las capacidades para la memoria y la cantidad de procesadores que ocuparía nuestra máquina virtual, en este caso nuestro NethServer.

Figura 3. Asignación de RAM y CPU

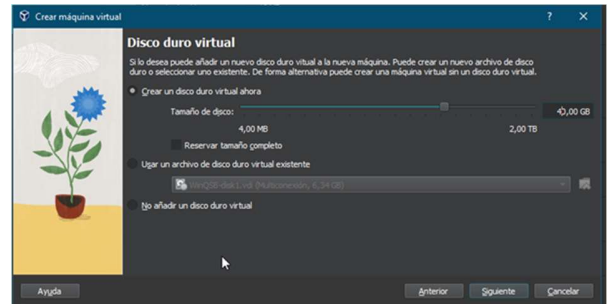
Asignamos los recursos de memoria RAM y CPU para la máquina virtual de NethServer. Esta configuración asegura que el servidor virtual disponga de los recursos necesarios para operar eficientemente, como se detalla en la siguiente figura:



Fuente: Autoría Propia

Procedimos en esta sección asignar el disco y la capacidad den disco que deseamos para nuestra máquina virtual.

Definimos el espacio en disco para la máquina virtual de NethServer. Este paso es esencial para garantizar que el servidor tenga suficiente capacidad de almacenamiento para su operación y para los datos que gestionará, como se muestra en la siguiente figura:

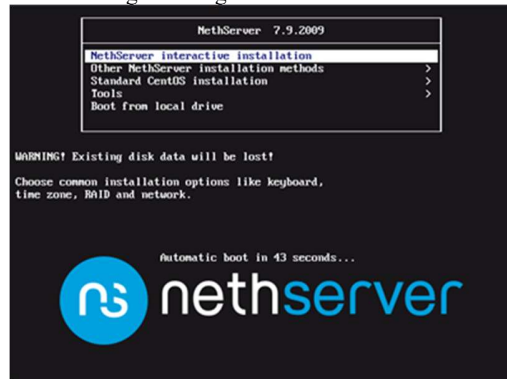


Fuente: Autoría Propia

Una vez realizadas estas configuraciones arrancamos la máquina virtual la cual nos mostrará el asistente de instalación de NethServer

Figura 5. Selección de inicio de NethServer

En esta imagen ilustramos cómo se selecciona la opción de inicio de NethServer desde VirtualBox, marcando el comienzo del proceso de instalación del sistema operativo, como se evidencia en la siguiente figura:

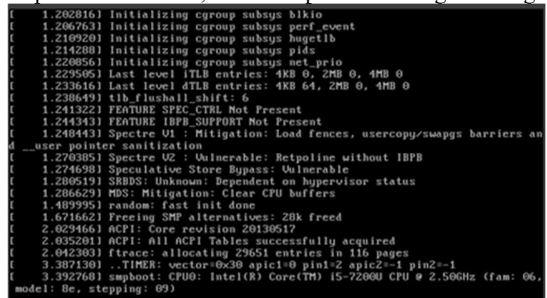


Fuente: Autoría Propia

Arrancamos seleccionando NethServer y este empieza a correr realizando las primeras acomodaciones para permitimos rápidamente configurarlo.

Figura 6. Arranque de NethServer

Se documenta el proceso de arranque de NethServer, una fase crítica donde se cargan los componentes iniciales del sistema operativo. Esta fase es vital para verificar que el servidor arranque correctamente, como se aprecia en la siguiente figura:



Fuente: Autoría Propia

Una vez ha terminado, nos muestra una interfaz gráfica donde debemos cambiar la zona horaria y la configuración del teclado, también podemos hacer otras configuraciones de red, por ejemplo, instalar recursos.

Figura 7. Configuraciones iniciales

Esta figura nos muestra cómo se configura el idioma del teclado en NethServer, un paso importante para asegurar que el sistema reconozca correctamente las entradas del usuario, especialmente en configuraciones regionales específicas, como se observa en la siguiente figura .



Fuente: Autoría Propia

Aquí seleccionamos la zona horaria y indicamos si queremos establecer la hora global por defecto.

Figura 8. Configuración zona horaria

En esta etapa se configura la zona horaria en NethServer, asegurando que el servidor opere en la zona horaria correcta para registros precisos de tiempo y eventos. Este paso es esencial para la sincronización de tiempo en aplicaciones y servicios que dependen de la hora correcta, como se evidencia en la siguiente figura:

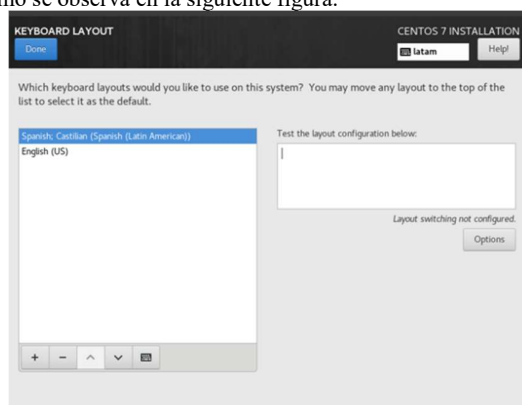


Fuente: Autoría Propia

Configuramos el idioma del teclado lo cual es muy importante para poder establecer una comunicación efectiva a través del teclado con la consola de NethServer.

Figura 9. Configuración de idioma de teclado

Esta figura muestra cómo se configura el idioma del teclado en NethServer, un paso importante para asegurar que el sistema reconozca correctamente las entradas del usuario, especialmente en configuraciones regionales específicas. Configurar el idioma correcto del teclado es crucial para evitar errores de entrada y facilitar la administración del sistema, como se observa en la siguiente figura:

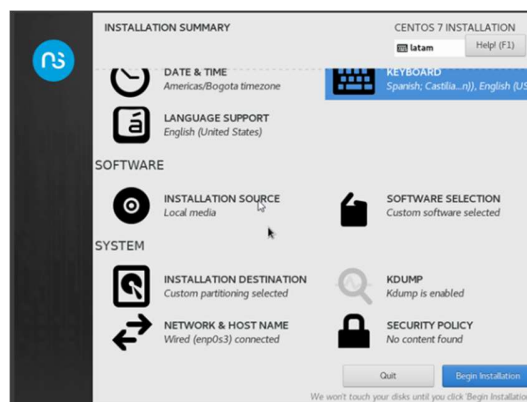


Fuente: Autoría Propia

Una vez realizado esto podemos continuar con la instalación y las advertencias desaparecen.

Figura 10. Continuación de la configuración

Continuando con la instalación, esta figura muestra los siguientes pasos de configuración, donde se establecen opciones adicionales del sistema. Estos pasos son cruciales para personalizar el servidor según las necesidades específicas del usuario, como se evidencia en la siguiente figura:



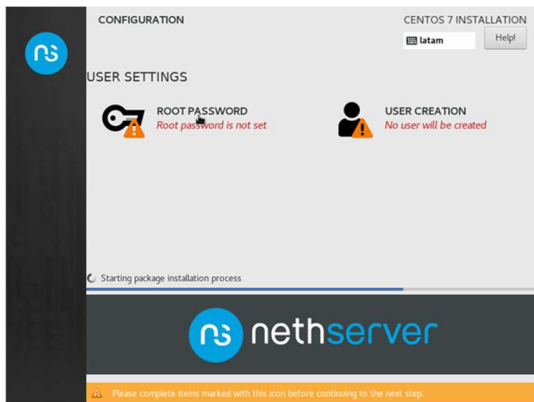
Fuente: Autoría Propia

Al continuar nos presenta otra interfaz en la cual nos indica que debemos asignar el password a el usuario root y que podemos crear otro usuario.

Figura 11. Configuración de cuenta root

En esta etapa se asigna una contraseña para la cuenta root en NethServer, asegurando que solo usuarios autorizados puedan

acceder al sistema con privilegios de administrador, como se muestra en la siguiente figura:

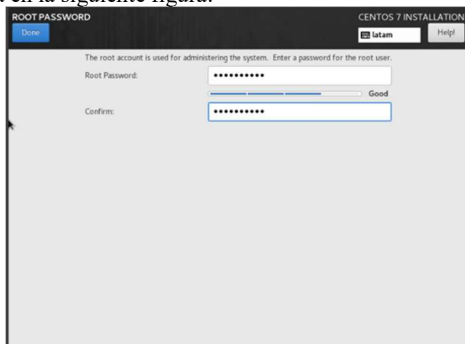


Fuente: Autoría Propia

Asignamos al root la contraseña damos click en Done y esperamos a que termine la instalación.

Figura 12. Asignación de contraseña al usuario root

Esta figura ilustra la asignación de la contraseña al usuario root en NethServer, un paso fundamental para la seguridad del servidor. La correcta configuración de la contraseña es esencial para proteger el acceso administrativo, como se detalla en la siguiente figura:

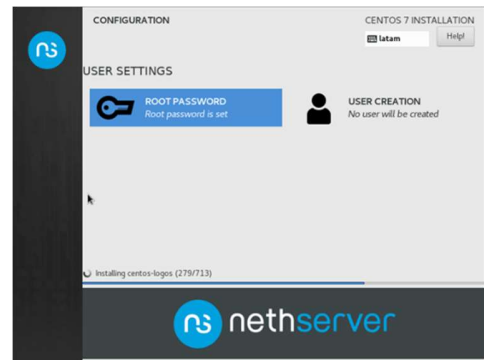


Fuente: Autoría Propia

Una vez realizado esto las advertencias son retiradas y nos queda esperar a que termine la instalación.

Figura 13. Últimos momentos de instalación de NethServer

Se documentan los últimos momentos de la instalación de NethServer, destacando la finalización del proceso y la preparación del sistema para su uso operativo. Esta fase confirma que el servidor está listo para su configuración final y puesta en marcha, como se observa en la siguiente figura:

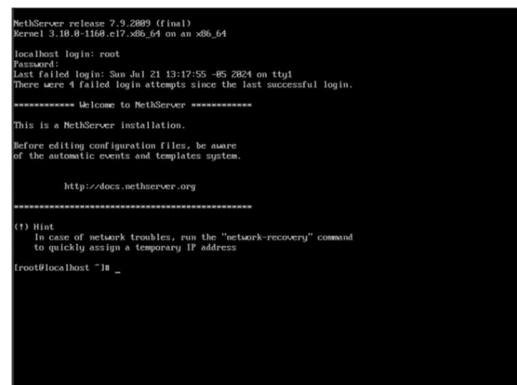


Fuente: Autoría Propia

Una vez terminada la instalación ya tenemos nuestro servidor de NethServer listo para trabajar, aquí nos pide realizar login podemos hacerlo con la cuenta root y con la contraseña previamente asignada, con ello ya podemos actualizar paquetes obtener la IP y conectarnos desde un navegador a la IP de nuestro servidor y poder trabajar NethServer de forma gráfica.

Figura 14. Ingreso con root al servidor

Se muestra el ingreso al servidor NethServer con la cuenta root, permitiendo al administrador acceder al entorno de configuración y gestión del sistema, como se evidencia en la siguiente figura:

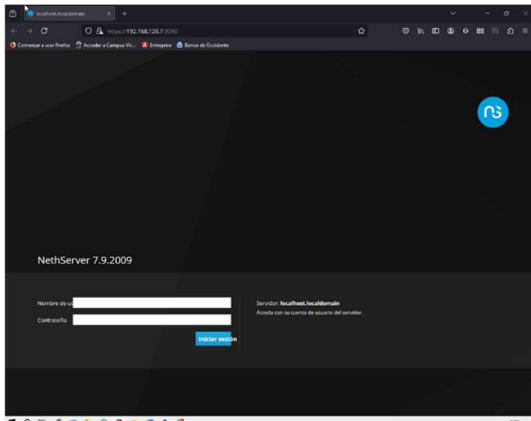


Fuente: Autoría Propia

Obtenida la ip de nuestro servidor podremos conectarnos y trabajar desde un entorno web nuestro servidor con las diferentes herramientas y servicios que provee este potente servidor.

Figura 15. Interfaz web de NethServer

Aquí se presenta la interfaz web de NethServer después del inicio de sesión, una herramienta esencial para la gestión y configuración del servidor a través de un navegador web, como se muestra en la siguiente figura:



Fuente: Autoría Propia

Este documento es un ejemplo del formato con los márgenes, la colocación del texto, éste está disponible en formato de WORD. Contiene las líneas y los párrafos con los márgenes y área de impresión.

3. RESULTADOS

Los resultados obtenidos fueron muy positivos, cumpliendo eficazmente con los objetivos establecidos para la implementación de los diferentes servicios. Cada servicio ha sido configurado y probado minuciosamente para asegurar su correcto funcionamiento y su capacidad para satisfacer las necesidades específicas planteadas al inicio del proyecto.

A lo largo de este trabajo, detallaremos las diversas implementaciones realizadas, comenzando con una descripción exhaustiva de cada servicio, los pasos seguidos para su configuración y las pruebas realizadas para verificar su operatividad. Cada sección incluirá capturas de pantalla que ilustran el proceso, proporcionando una comprensión clara y detallada de las acciones llevadas a cabo.

Además, abordaremos los desafíos encontrados durante la implementación y cómo fueron superados, ofreciendo una perspectiva completa sobre el proceso de desarrollo. Los resultados de las pruebas serán presentados de manera sistemática, destacando la eficacia y eficiencia de cada servicio, así como su integración con otros componentes del sistema.

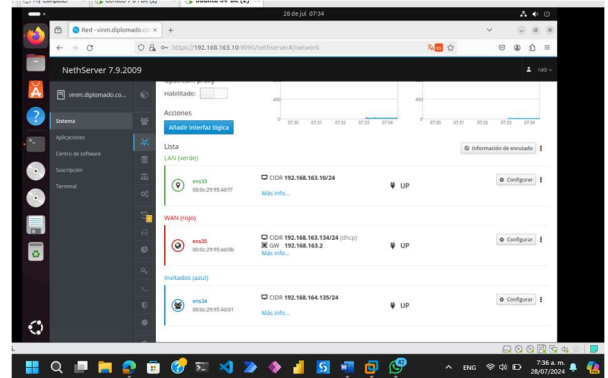
3.1 CONFIGURACION DE SERVICIOS

En esta sección veremos como realizamos la implementación de cada uno de los servicios propuestos para este laboratorio

PROXY

Figura 16. Redes Configuradas, red azul, Red Roja y Red Verde

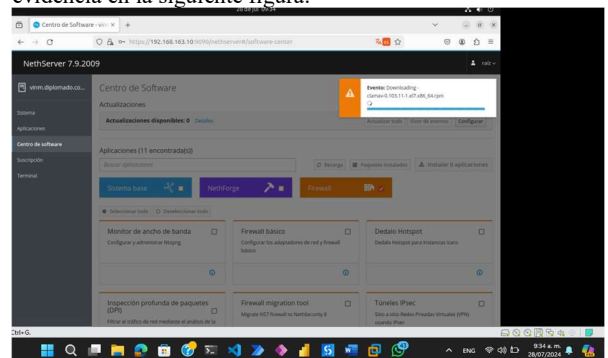
Se documenta la configuración de las redes en NethServer, estableciendo diferentes zonas de red (azul, roja y verde) para gestionar el tráfico y la seguridad de la red. Esta configuración es crucial para segmentar y proteger diferentes tipos de tráfico de red, como se observa en la siguiente figura:



Fuente: Autoría Propia

Figura 17. Instalación de los paquetes web proxy y filtro web

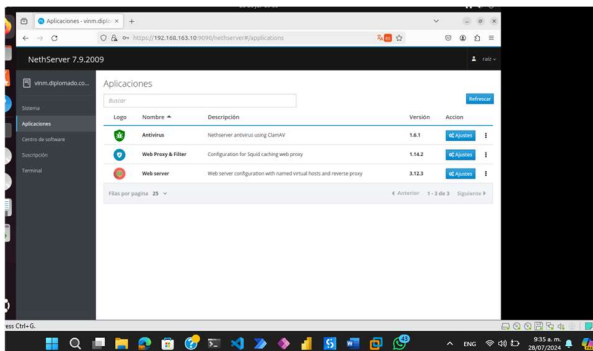
En esta imagen ilustramos el proceso de instalación del controlador de dominio LDAP en NethServer, permitiendo la gestión centralizada de usuarios y autenticación en la red. La instalación de LDAP es fundamental para la administración eficiente de los recursos de red y la seguridad, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 18. Sección de aplicaciones, paquetes instalados

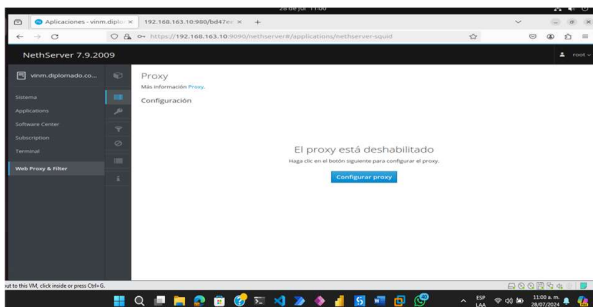
Esta figura muestra la instalación del paquete de File Server en NethServer, habilitando el servidor para compartir archivos en la red. La configuración del File Server permite a los usuarios acceder, compartir y colaborar en documentos y otros recursos, optimizando la gestión de archivos en un entorno corporativo, como se observa en la siguiente figura:



Fuente: Autoría Propia

Figura 19. Sección de configuración y habilitación de proxy

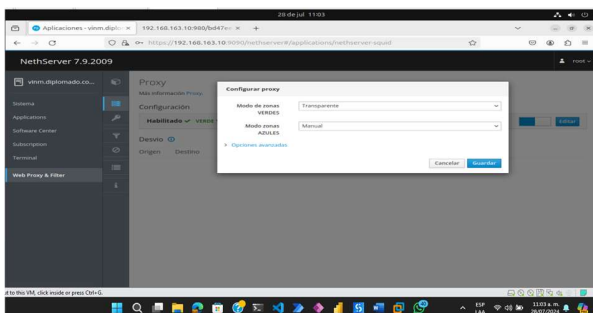
Se presenta la creación de una carpeta compartida en NethServer, una función esencial para facilitar el acceso compartido a archivos entre diferentes usuarios en la red. La correcta configuración de carpetas compartidas es crucial para la colaboración y el flujo de trabajo en equipos de trabajo, como se muestra en la siguiente figura:



Fuente: Autoría Propia

Figura 20. Habilitación de proxy red verde transparente y azul manual

En esta figura se muestra la habilitación del proxy en la red verde de forma transparente y en la red azul de forma manual, permitiendo controlar y monitorear el tráfico de red de manera eficiente. Configurar adecuadamente el proxy es vital para la seguridad y el rendimiento de la red, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 21. En la siguiente imagen vemos el proxy habilitado

Aquí se presenta la sección de configuración del proxy en NethServer, donde se detalla cómo habilitar y ajustar las opciones del proxy para adaptarse a las necesidades de la red. Esta configuración permite un control granular del acceso a Internet y la filtración de contenido, como se observa en la siguiente figura:

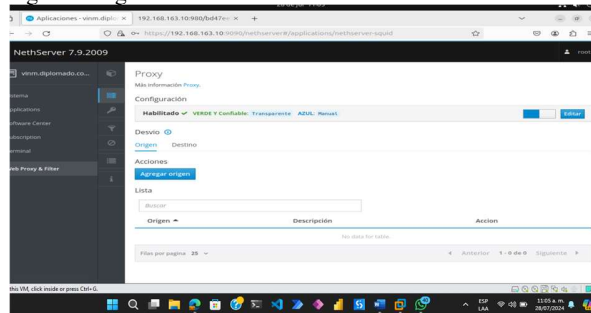


Figura 22. Habilitamos el servicio netdata y le asignamos la red verde para habilitar las graficas

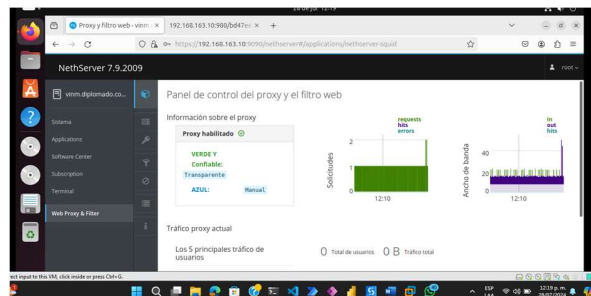
Esta imagen muestra los pasos para configurar y habilitar el proxy en NethServer, incluyendo las opciones de filtrado y control de acceso. El correcto ajuste del proxy es esencial para la seguridad y la gestión del tráfico de red, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 23. Visualización de las graficas

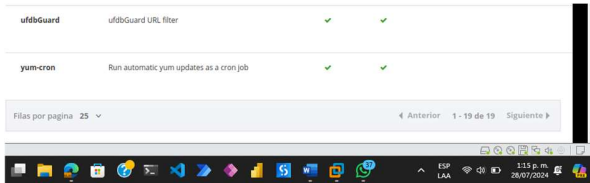
Para obtener un análisis detallado del tráfico de red y el rendimiento del sistema, hemos habilitado el servicio netdata y configurado las gráficas correspondientes. Esta herramienta nos proporciona una visualización en tiempo real del uso de recursos del sistema, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 24. Habilidad del servicio ufwGuard, para filtrar las páginas web

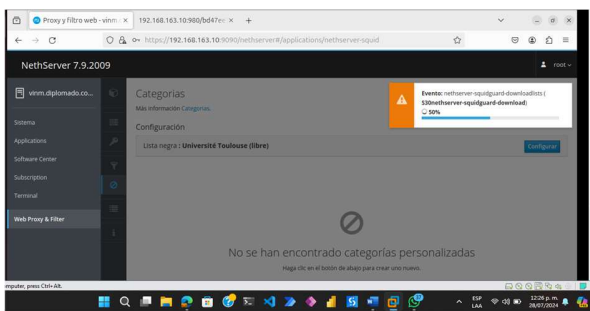
El siguiente paso en nuestra configuración de seguridad es la habilitación del servicio ufwGuard. Este servicio es crucial para filtrar y controlar el acceso a sitios web inapropiados o no deseados. A continuación, se muestra la pantalla de configuración del ufwGuard:



Fuente: Autoría Propia

Figura 25. Creación de categorías para filtrar

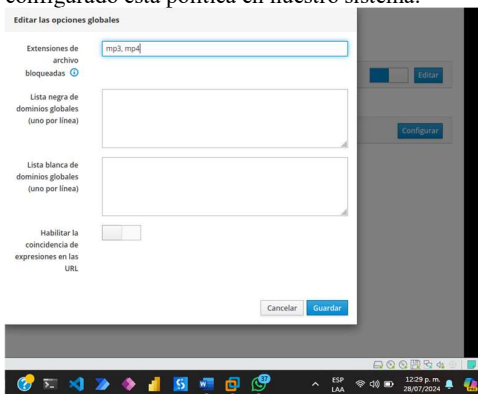
Para una gestión más eficaz del filtrado web, hemos creado diversas categorías que nos permiten organizar y controlar el acceso a diferentes tipos de contenido. Este paso es fundamental para personalizar las políticas de acceso según las necesidades específicas, como se observa en la siguiente figura:



Fuente: Autoría Propia

Figura 26 Configuración de extensiones de archivo bloqueadas

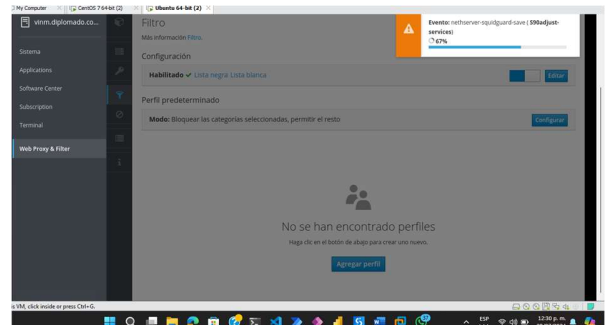
Además del filtrado de contenido web, es importante bloquear ciertas extensiones de archivo que pueden representar un riesgo de seguridad. La siguiente figura muestra cómo hemos configurado esta política en nuestro sistema:



Fuente: Autoría Propia

Figura 27. Creación y habilitación de filtros

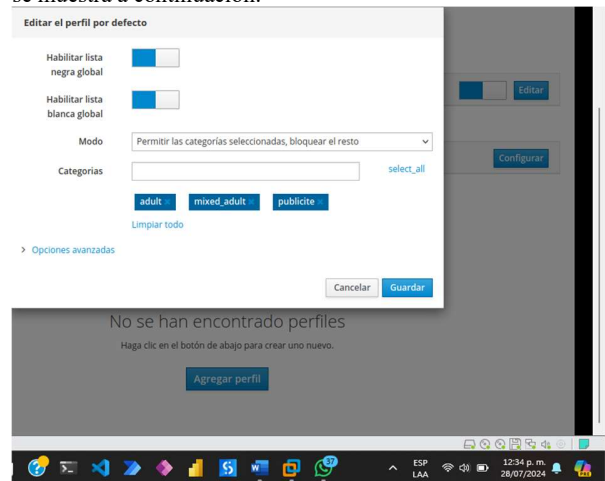
La creación y habilitación de filtros específicos nos permite aplicar reglas de seguridad precisas para el tráfico de red. Estos filtros son esenciales para garantizar que solo se permita el acceso a contenido seguro y aprobado, como se ilustra en la siguiente figura:



Fuente: Autoría Propia

Figura 28. Se filtra las categorías que se van a filtrar en proxy, que es la publicidad y acceso a paginas inadecuadas

Para mejorar la experiencia de navegación y la seguridad, hemos configurado el proxy para filtrar categorías específicas como publicidad y páginas inapropiadas. Esta configuración ayuda a reducir distracciones y riesgos para los usuarios, como se muestra a continuación:



Fuente auditoria propia

Figura 29. Desde el panel visualizamos que ya se consumen recursos de descarga nuestro cliente

Una vez implementadas las políticas de filtrado y seguridad, es vital monitorear el consumo de recursos para asegurar un

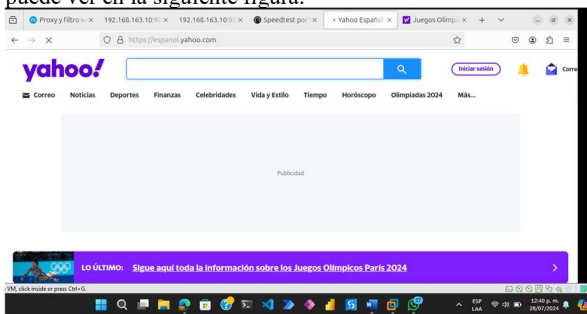
rendimiento óptimo. Desde el panel de control, podemos observar cómo se están utilizando los recursos del sistema, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 30. Accedimos a la página yahoo donde sale publicidad y por el proxy, ya no sale publicidad

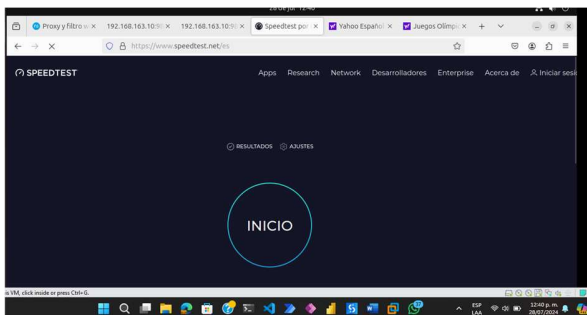
Para verificar la efectividad del filtrado de publicidad, hemos accedido a la página de Yahoo y comprobado que el proxy bloquea correctamente los anuncios. Este paso asegura una navegación más limpia y segura para los usuarios, como se puede ver en la siguiente figura:



Fuente: Autoría Propia

Figura 31. Se accede a la página speedtest, donde también se ven las publicidad a los lados y no se ve

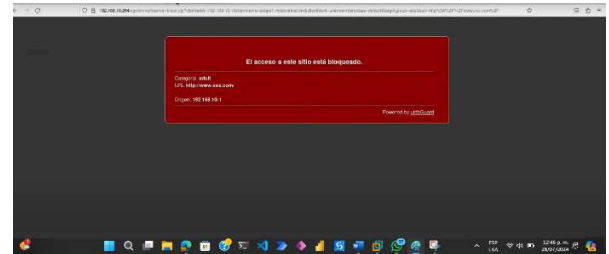
Se presenta la prueba de acceso a la página Speedtest, donde inicialmente se visualizaban anuncios publicitarios. Tras la configuración del proxy, se observa la ausencia de estos anuncios, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 32. Página para adultos, no se puede visualizar por el proxy

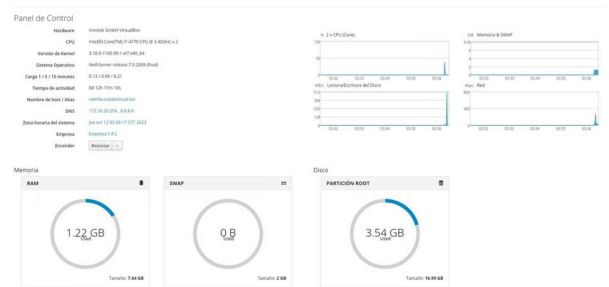
Se intenta acceder a una página para adultos, sin embargo, gracias a la configuración del proxy, el acceso es bloqueado, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 33. Panel principal donde se visualiza los recursos consumidos desde el servidor proxy

El panel principal muestra un resumen detallado de los recursos consumidos desde el servidor proxy. Este monitoreo es crucial para garantizar un rendimiento óptimo, como se evidencia en la siguiente figura:



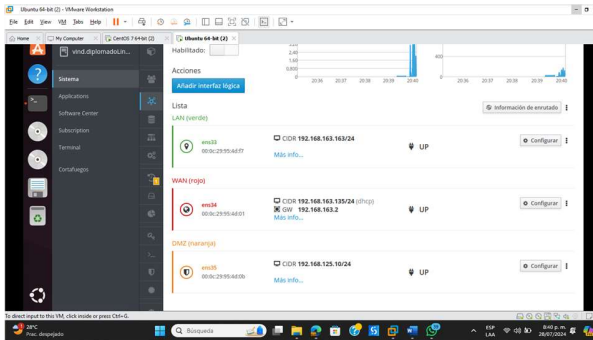
Fuente: Autoría Propia

3.2 CORTAFUEGOS

En la siguiente imagen se realizó la configuración de las redes, para la arquitectura, donde se estableció una red, verde, para la red LAN, una red roja para la wan y otra red naranja para la configuración de cortafuegos

Figura 34. Se realiza la configuración de las redes

La configuración de las redes se lleva a cabo para establecer una arquitectura eficiente, dividiendo la red en diferentes zonas (verde, roja y naranja). Esta configuración es esencial para la seguridad y gestión del tráfico, como se evidencia en la siguiente figura:

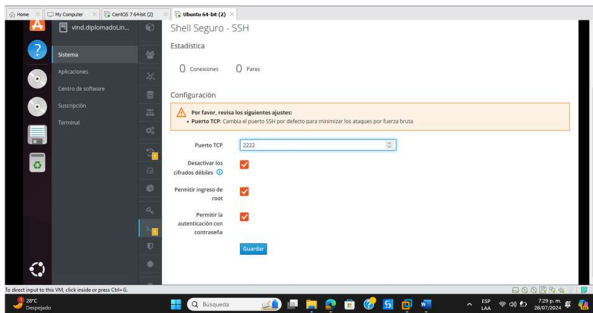


Fuente: Autoría Propia

En la siguiente imagen se establece la configuración del SSH, colocando el puerto de red 2222

Figura 35. Establecer el puerto SSH

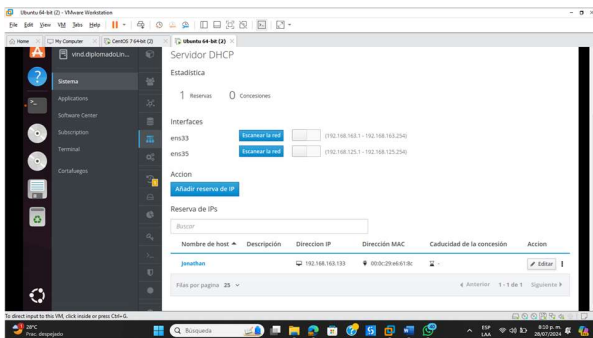
Se configura el puerto SSH, estableciéndolo en 2222 para mejorar la seguridad del acceso remoto al servidor. Esta práctica reduce la vulnerabilidad a ataques, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 36. Se añade la configuración DHCP para la red LAN

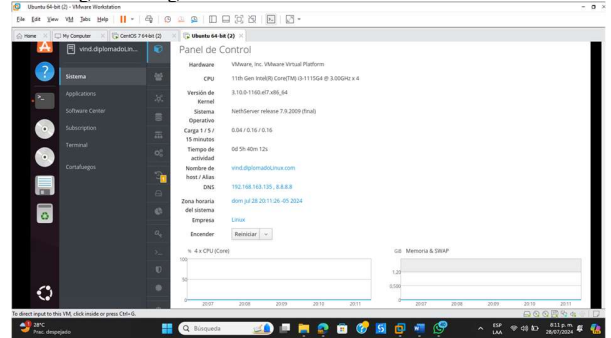
Se añade la configuración DHCP para la red LAN, lo que facilita la asignación automática de direcciones IP a los dispositivos conectados. Esta configuración es fundamental para la gestión eficiente de la red, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 37. Se visualiza que se modificó el DNS y el nombre de la empresa colocándolo Linux

Se modifica el DNS y se cambia el nombre de la empresa a 'Linux', lo que mejora la identificación y resolución de nombres dentro de la red. Esta actualización es crucial para la organización y el funcionamiento de la red, como se evidencia en la siguiente figura:

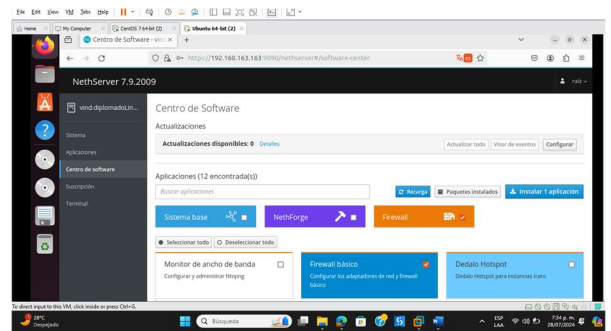


Fuente: Autoría Propia

En la sección de centro de software, se filtra el componente firewall básico, seleccionando firewall, después aparece, firewall básico, se selecciona y se da clic en instalar aplicación.

Figura 38. Instalación firewall básico

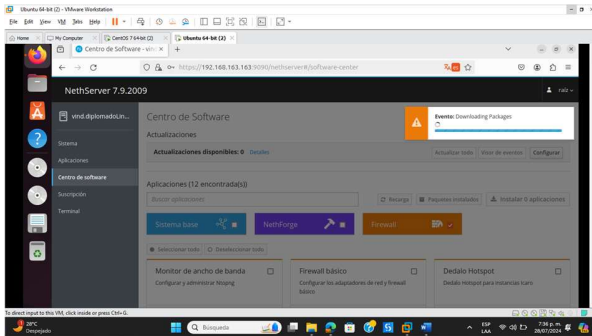
Se procede a la instalación del firewall básico, que es esencial para proteger la red de accesos no autorizados y ataques externos. Este paso es fundamental para la seguridad de la infraestructura, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 39. Se encuentra instalando firewall básico

El proceso de instalación del firewall básico se muestra en esta etapa. Es importante asegurarse de que el firewall esté correctamente instalado y configurado para garantizar una defensa eficaz, como se evidencia en la siguiente figura:

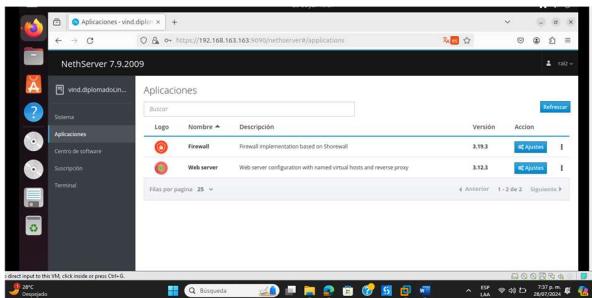


Fuente: Autoría Propia

En la sección de aplicaciones, podemos acceder al firewall que se instaló

Figura 40. Sección de aplicaciones

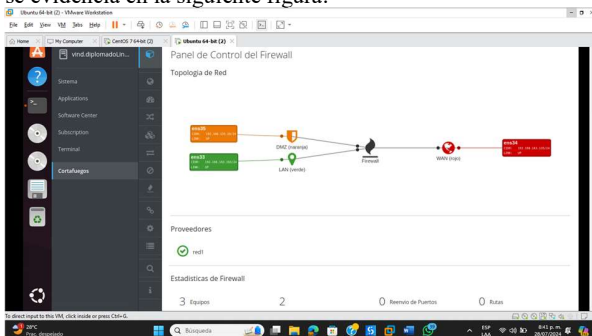
En la sección de aplicaciones, se puede acceder al firewall recién instalado. Esta interfaz permite gestionar y configurar las reglas de seguridad, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 41. Topología de la red desde el panel de control de firewall

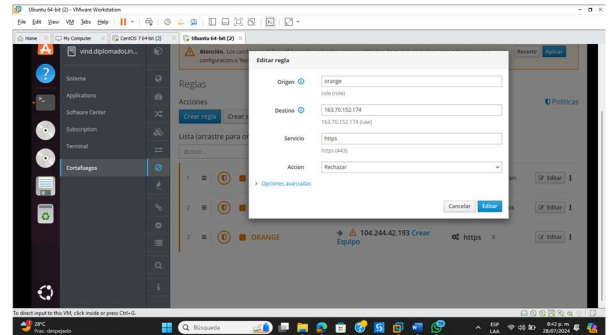
La topología de la red se visualiza desde el panel de control del firewall, proporcionando una vista clara de la estructura de la red y las conexiones entre los dispositivos. Esta visualización es crucial para la administración de la red, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 42. Se añade las reglas de filtro para no acceder a las redes sociales de facebook, instagram y X

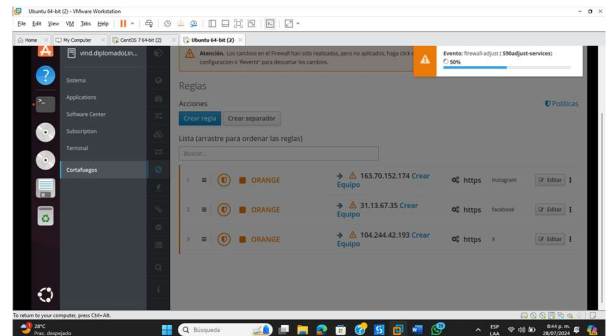
Se añaden las reglas de filtro para bloquear el acceso a redes sociales como Facebook, Instagram y X. Esta medida es útil para controlar el uso de la red y evitar distracciones, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 43. Se está guardando las reglas

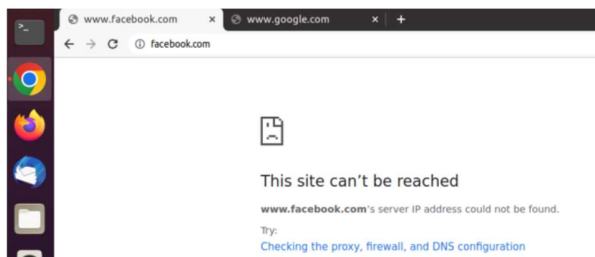
Para asegurar que las nuevas reglas de filtrado se apliquen correctamente, se procede a guardar todas las configuraciones realizadas en el firewall, como se evidencia en la siguiente figura:



Fuente: Autoría Propia

Figura 44. Se prueba el acceso a la red social Facebook

Se realiza una prueba para verificar que las nuevas reglas de filtrado estén funcionando, intentando acceder a la red social Facebook, como se muestra en la siguiente figura:



Fuente: Autoría Propia

3.3 FILE SERVER Y PRINT SERVER

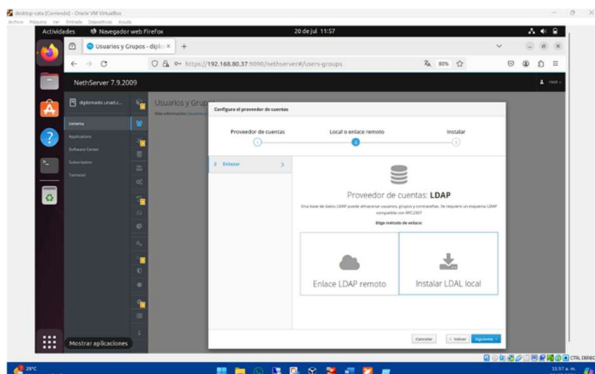
Implementación y configuración del acceso a una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

3.4 INSTALACION DEL CONTROLADOR DE DOMINIO LDAP

Se realiza la instalación del LDAP en NethServer

Figura 45. Instalación LDAP

A continuación, se muestra el proceso de instalación del servicio LDAP en NethServer, el cual es crucial para la gestión de usuarios y grupos en la red, como se evidencia en la siguiente figura:

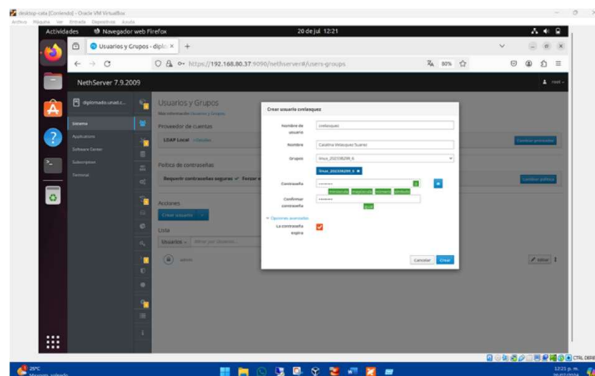


Fuente: Autoría Propia.

Se crea un grupo llamada "linux_202338299_6" y un usuario "cvelasquez" para acceso y se asigna la contraseña.

Figura 46. Configuración usuario y contraseña LDAP

Una vez instalado el LDAP, se procede a la creación de un usuario y un grupo, configurando las credenciales necesarias para su acceso, como se puede observar en la siguiente figura:



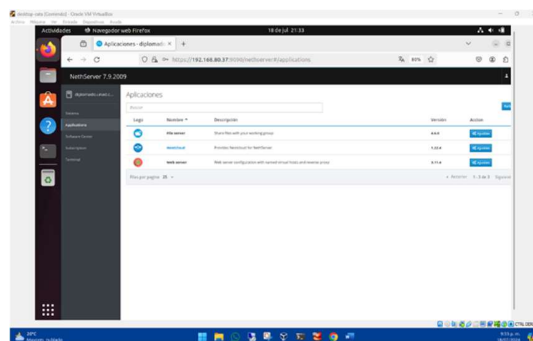
Fuente: Autoría Propia.

FILE SERVER

Desde el NethServer realizamos la instalación del paquete llamado file server.

Figura 47. Instalación del paquete file server

Se realiza la instalación del paquete File Server en NethServer, permitiendo así la creación y gestión de carpetas compartidas en la red, como se muestra en la siguiente figura:

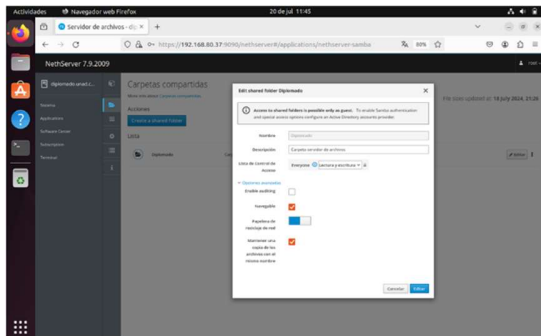


Fuente: Autoría Propia.

Abrimos el paquete que acabamos de instalar y creamos la carpeta compartida llamada "diplomado" con permisos de lectura y escritura.

Figura 48. Creación de carpeta compartida

Posteriormente, se crea una carpeta compartida llamada "diplomado", asignando permisos de lectura y escritura para los usuarios autorizados, como se evidencia en la siguiente figura:

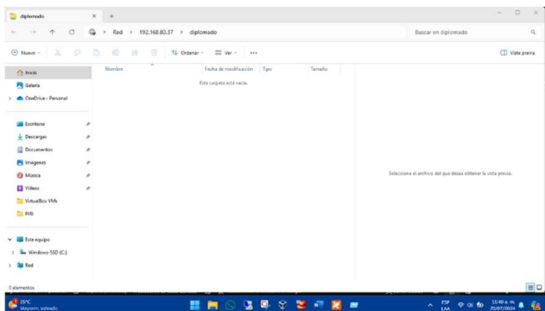


Fuente: Autoría Propia.

Ingresamos a la carpeta compartida en Windows y accedemos a la carpeta compartida de manera correcta.

Figura 49. Carpeta compartida desde Windows

Se verifica el acceso a la carpeta compartida desde un equipo con sistema operativo Windows, asegurando la correcta integración y funcionalidad, como se muestra en la siguiente figura:

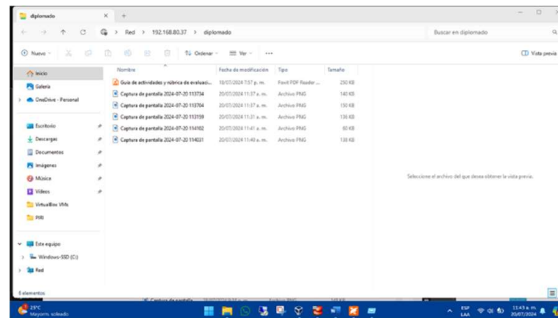


Fuente: Autoría Propia.

Validamos el envío de archivos a la carpeta compartida y los permisos de lectura y escritura.

Figura 50. Visualización de archivos en carpeta compartida

Se valida el envío y acceso a archivos dentro de la carpeta compartida, comprobando los permisos de lectura y escritura establecidos, como se puede observar en la siguiente figura:



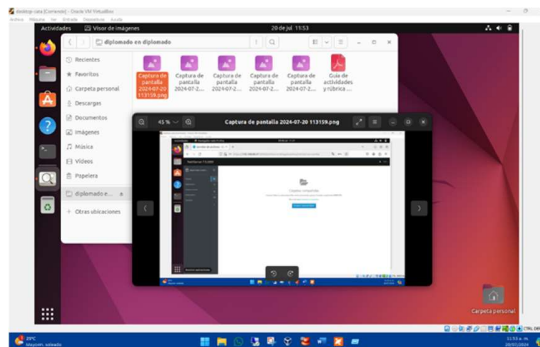
Fuente: Autoría Propia.

3.5 RESULTADO OBTENIDO DEL FILE SERVER

Se comprobó que, ingresando desde otro equipo conectado a la red verde, evidenciamos que los archivos se enviaron de manera correcta para todos los usuarios de la LAN.

Figura 51. Visualización de carpeta compartida en Ubuntu

Para comprobar la visualización, accedimos a la carpeta compartida desde un equipo con sistema operativo Ubuntu, como se muestra en la siguiente figura:



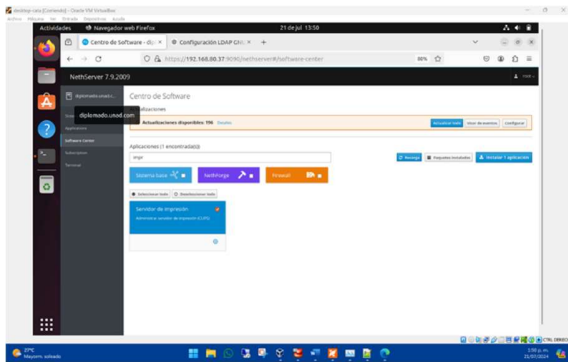
Fuente: Autoría Propia.

3.6 PRINT SERVER.

Desde el NethServer realizamos la instalación del paquete Print Server para administración de impresoras (CUPS).

Figura 52. Instalación de paquere Print Server

Procedemos con la instalación del paquete Print Server en NethServer, el cual es fundamental para la administración de impresoras en la red, como se evidencia en la siguiente figura:

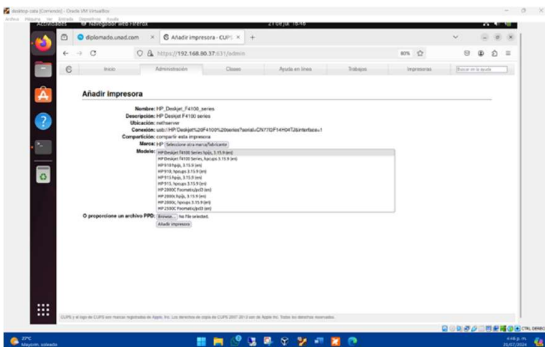


Fuente: Autoría Propia.

Desde el servidor NethServer ingresamos de manera local usando la IP 192.168.80.37 puerto 631 y configuramos la impresora HP_Deskjet_f4100.

Figura 53. Selección e instalación de la impresora

Desde la interfaz del servidor NethServer, se selecciona e instala una impresora específica, configurando sus parámetros de funcionamiento, como se puede observar en la siguiente figura:

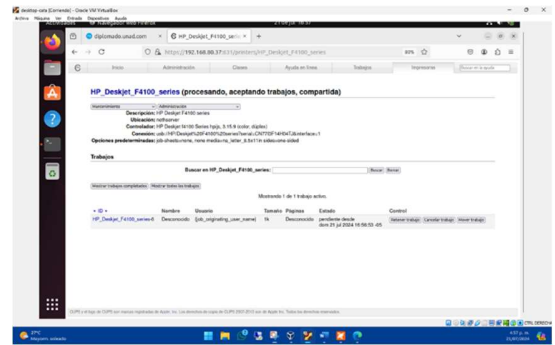


Fuente: Autoría Propia.

Después de la configuración de la impresora se evidencia que la misma envía trabajos para impresión y la misma se puede ver tanto en el servidor con en los demás equipos conectados a la red.

Figura 54. Configuración de la impresora

Una vez configurada la impresora, se verifica que esta pueda recibir y procesar trabajos de impresión desde diferentes equipos de la red, como se muestra en la siguiente figura:



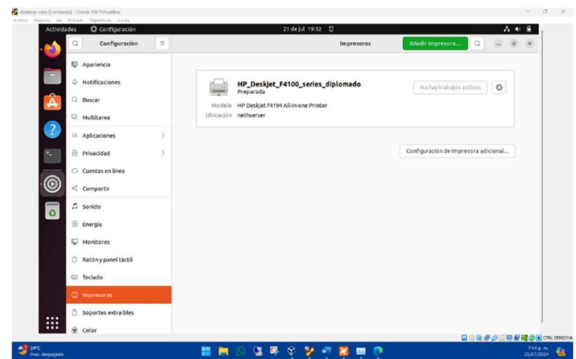
Fuente: Autoría Propia.

RESULTADO OBTENIDO DEL PRINT SERVER

Se comprueba que la impresora fue configurada en el servidor de manera correcta usando los CUPS y evidenciando que se la impresora se comparte con otros equipos.

Figura 55. Funcionalidad de la impresora compartida

Se comprueba que la impresora fue configurada en el servidor de manera correcta usando los CUPS y evidenciando que la impresora se comparte con otros equipos, como se evidencia en la siguiente figura:

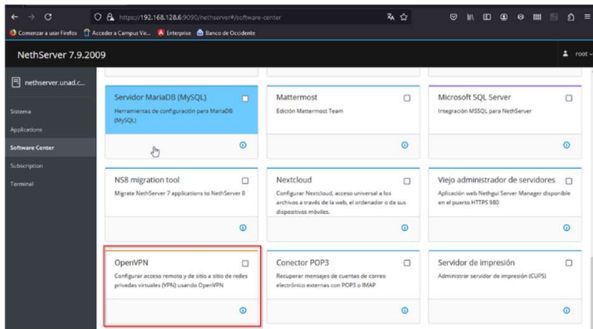


3.7 VPN

Inicialmente para la configuración de este servicio se procede a instalar OpenVPN el cual se puede instalar ingresando como root a la interfaz web de NethServer en el menú Software Center.

Figura 56. Selección de servicio a instalar

Inicialmente para la configuración de este servicio se procede a instalar OpenVPN el cual se puede instalar ingresando como root a la interfaz web de NethServer en el menú Software Center, como se evidencia en la siguiente figura:

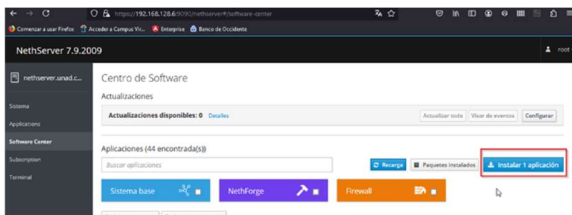


Fuente: Autoría Propia.

Una vez seleccionados los servicios a instalar se indica que se desea instalar la aplicación

Figura 57. Instalación de servicios seleccionados

Una vez seleccionados los servicios a instalar se indica que se desea instalar la aplicación, como se evidencia en la siguiente figura:

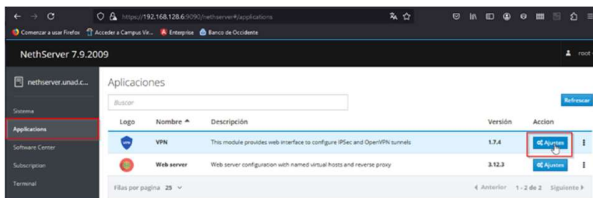


Fuente: Autoría Propia.

Posterior a la instalación nos dirigimos al módulo aplicaciones donde encontramos la VPN y podemos dar clic en ajuste.

Figura 58. Ajustar Aplicación VPN

Posterior a la instalación nos dirigimos al módulo aplicaciones donde encontramos la VPN y podemos dar clic en ajuste, como se evidencia en la siguiente figura:

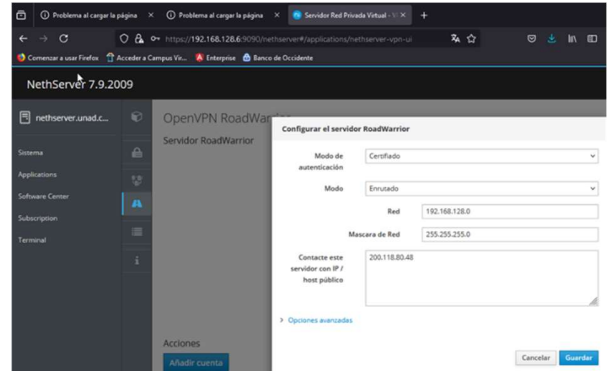


Fuente: Autoría Propia.

Encontrándonos en la configuración procedemos a configurar una VPN RoadWarrior

Figura 59. Configuración de VPN RoadWarrior

Encontrándonos en la configuración procedemos a configurar una VPN RoadWarrior, como se evidencia en la siguiente figura:

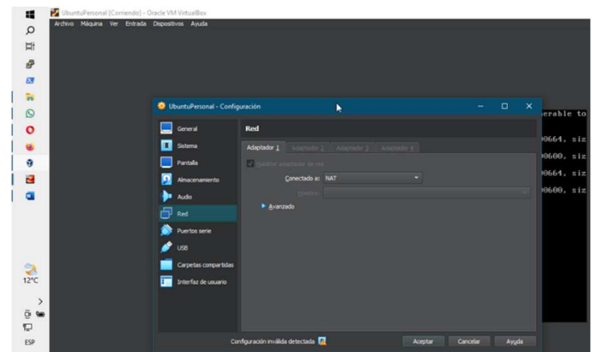


Fuente: Autoría Propia.

Una vez realizado este proceso ya tenemos nuestra VPN creada y procedemos a iniciar una maquina Ubuntu para comprobar configuramos en NAT la red

Figura 60. Configuración de tarjeta de red Ubuntu

Una vez realizado este proceso ya tenemos nuestra VPN creada y procedemos a iniciar una máquina Ubuntu para comprobar configuramos en NAT la red, como se evidencia en la siguiente figura:

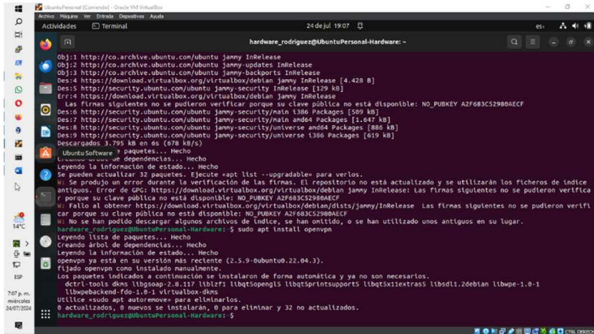


Fuente: Autoría Propia.

Se procede a instalar el cliente de OpenVPN en Ubuntu

Figura 61. Instalación de OpenVPN cliente

Se procede a instalar el cliente de OpenVPN en Ubuntu, como se evidencia en la siguiente figura:

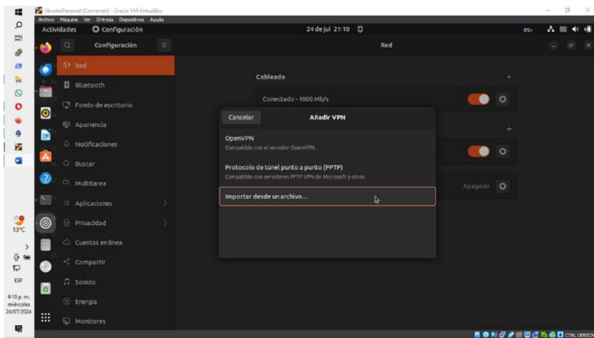


Fuente: Autoría Propia.

Desde NethServer se procede a descargar el archivo de configuración .ovpn el cual me permite configurar rápidamente mi VPN en un cliente, en Ubuntu procedemos a importar este archivo.

Figura 62. Importar archivo .ovpn

Desde NethServer se procede a descargar el archivo de configuración .ovpn el cual permite configurar rápidamente la VPN en un cliente en Ubuntu, procedemos a importar este archivo, como se evidencia en la siguiente figura:

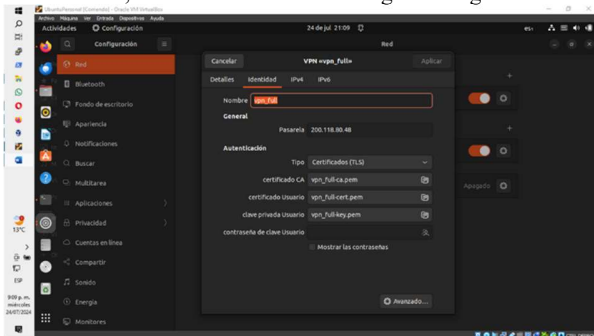


Fuente: Autoría Propia.

Una vez cargado el archivo .ovpn tenemos la configuración de nuestra VPN

Figura 63. Configuración de VPN cliente

Una vez cargado el archivo .ovpn tenemos la configuración de nuestra VPN, como se evidencia en la siguiente figura:

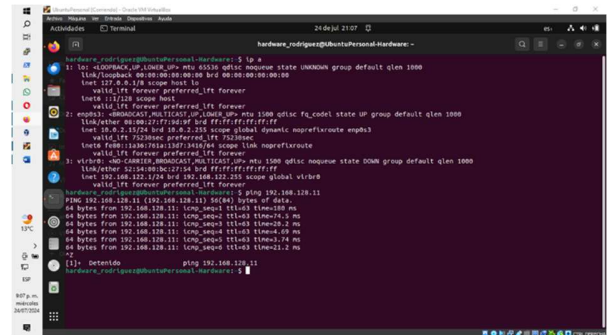


Fuente: Autoría Propia.

Después de configurar la VPN en el cliente comprobamos realizando un ping al servidor Debian que está en otra red que responde con éxito.

Figura 64. Verificación de conexión a servidor en otra red

Después de configurar la VPN en el cliente comprobamos realizando un ping al servidor Debian que está en otra red, obteniendo una respuesta exitosa, como se evidencia en la siguiente figura:

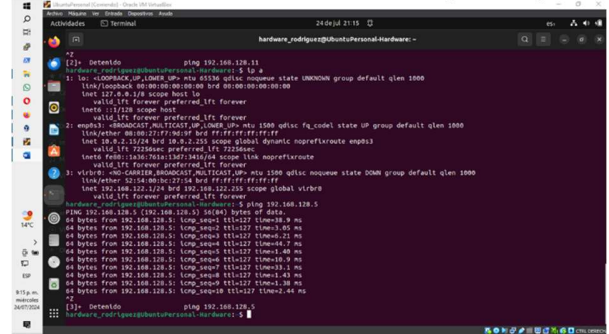


Fuente: Autoría Propia.

También realizamos ping a la maquina local la cual responde con éxito encontrándose en otra red, pero conectándose otra vez de la VPN.

Figura 65. Verificación de conexión a equipo en otra red

También realizamos ping a la máquina local, obteniendo una respuesta exitosa, encontrándose en otra red pero conectándose a través de la VPN, como se evidencia en la siguiente figura:



Fuente: Autoría Propia.

4. CONCLUSIONES

La implementación de soluciones como VPN, cortafuegos y proxies nos proporciona una capa robusta de seguridad y control en la gestión de redes. Una VPN garantiza la confidencialidad y la integridad de los datos durante la transmisión, permitiendo el acceso remoto seguro a los recursos corporativos. El cortafuegos, por su parte, actúa como una barrera esencial contra accesos no autorizados y amenazas externas, filtrando el tráfico y aplicando políticas de seguridad estrictas. Los proxies complementan estas medidas al actuar como intermediarios en la comunicación de red, mejorando el rendimiento y ofreciendo capacidades adicionales de filtrado y caché. Juntas, estas tecnologías fortalecen la seguridad de la red y protegen los datos contra amenazas internas y externas.

Los servidores de archivos y de impresión son fundamentales para la optimización de recursos y la eficiencia operativa en una red. Un servidor de archivos centraliza el almacenamiento y la gestión de datos, facilitando el acceso compartido y mejorando la organización y seguridad de la información. Por otro lado, un servidor de impresión simplifica la administración de dispositivos de impresión, permitiendo el acceso compartido y reduciendo la necesidad de impresoras individuales. Esta centralización no solo mejora la eficiencia operativa al reducir costos y simplificar el mantenimiento, sino que también asegura un uso más controlado y responsable de los recursos de impresión y almacenamiento.

En conclusión, la integración de VPN, proxies, cortafuegos, servidores de archivos y de impresión proporciona una solución integral para la gestión y protección de redes. La VPN asegura una comunicación cifrada y segura entre usuarios remotos y la red corporativa, mientras que el cortafuegos protege contra amenazas externas y controla el tráfico de red. Los proxies optimizan el rendimiento y controlan el acceso, y los servidores de archivos e impresión facilitan la colaboración y gestión eficiente de recursos. Juntas, estas tecnologías no solo refuerzan la seguridad y el rendimiento de la red, sino que también contribuyen a una operación más fluida y eficiente en el entorno corporativo.

5. REFERENCIAS

- [1] Triana Lopez, G. A. (2018) Instalación y configuración un cortafuegos bajo sistemas GNU/Linux con NethServer.
- [2] Pickard, A. S., & Knight, S. J. (2005). Proxy evaluation of health-related quality of life: a conceptual framework for understanding multiple proxy perspectives. *Medical care*, 43(5), 493-499.
- [3] Crist, E. F., & Keijsers, J. J. (2015). *Mastering OpenVPN*. Packt Publishing Ltd.
- [4] Bellovin, S. M., & Cheswick, W. (1998). Así funciona la seguridad informática: Cortafuegos. *Investigación y ciencia*, (267), 70-71.
- [5] Valladares Cueva, D. F. (2013). Análisis, desarrollo y construcción de un sistema para la administración y gestión

de documentos digitales levantados en un servidor de archivos (Bachelor's thesis).

- [6] Alshalan, A., Pisharody, S., & Huang, D. (2015). A survey of mobile VPN technologies. *IEEE Communications Surveys & Tutorials*, 18(2), 1177-1196
- [7] Mosquera, C. A. H., Ortiz, I. D. J. O., Eslava, A. G., Neita, J. E. R., & Montes, (2018) F. A. C. NETHSERVER SIMPLIFICA LA ADMINISTRACIÓN DE SERVIDORES. GUÍA RÁPIDA PARA PRINCIPIANTES IMPLEMENTADA EN VIRTUALBOX.