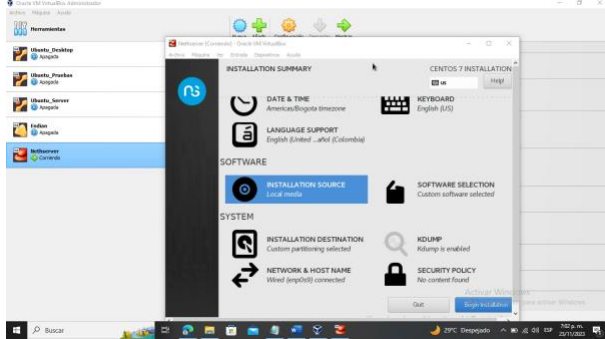




En el siguiente paso, se configuran aspectos como la selección de la zona horaria, el tipo de teclado y los idiomas preferidos para el soporte. Los demás apartados pueden mantenerse con la configuración por defecto.

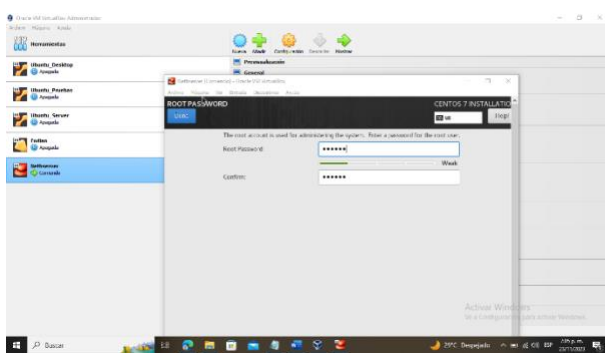
Figura. 3. Instalación NethServer



Fuente: Autoría propia

En el siguiente paso, se asigna una contraseña para el usuario root. Si se prefiere, se puede habilitar un usuario como administrador, pero en este caso únicamente se habilita el usuario root.

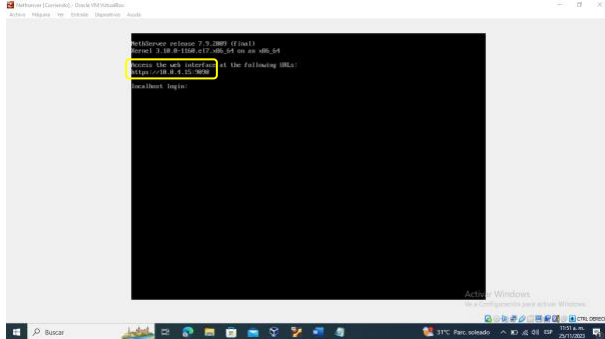
Figura. 4. Instalación NethServer



Fuente: Autoría propia

Durante esta etapa de la instalación de NethServer, se asigna una dirección IP que posibilitará el acceso desde un navegador al entorno gráfico de NethServer.

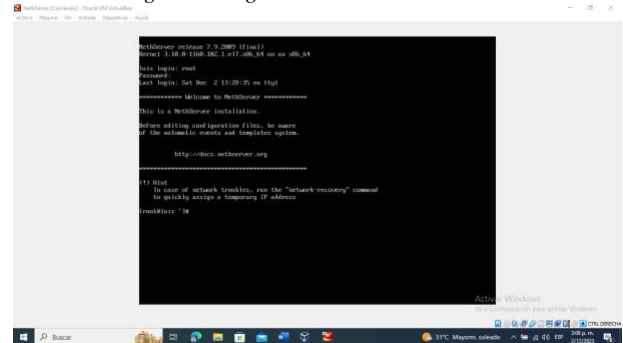
Figura. 5. Instalación NethServer



Fuente: Autoría propia

En esta fase, el proceso de instalación ha concluido y ahora es posible acceder con el usuario y contraseña previamente asignados.

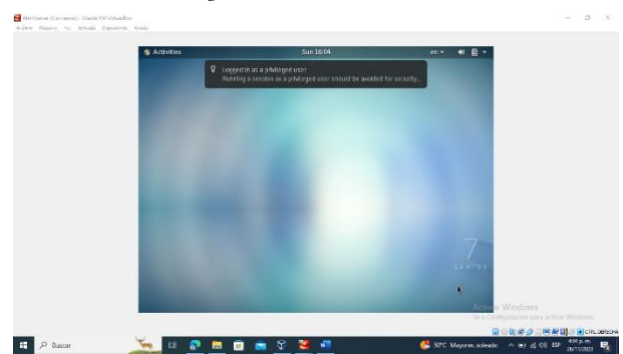
Figura. 6. Ingreso a consola NethServer



Fuente: Autoría propia

En esta sección se lleva a cabo la instalación de un entorno gráfico que facilite el acceso a través de un navegador y permita ingresar utilizando la IP asignada a nuestro NethServer.

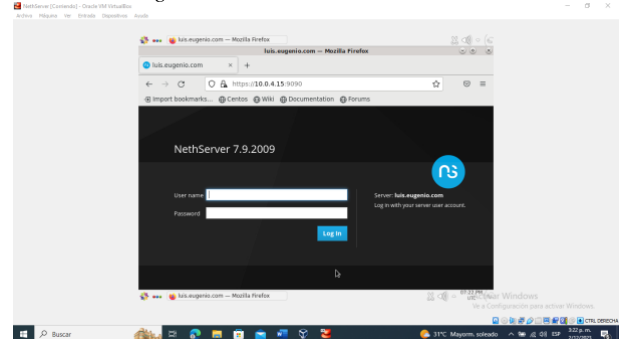
Figura. 7. Instalación DKE



Fuente: Autoría propia

Para finalizar, utilizando un navegador de preferencia, se ingresa la IP asignada durante la instalación de NethServer. Luego, se procede a la autenticación con el usuario y contraseña previamente asignados.

Figura. 8. Inicio de sesión NethServer

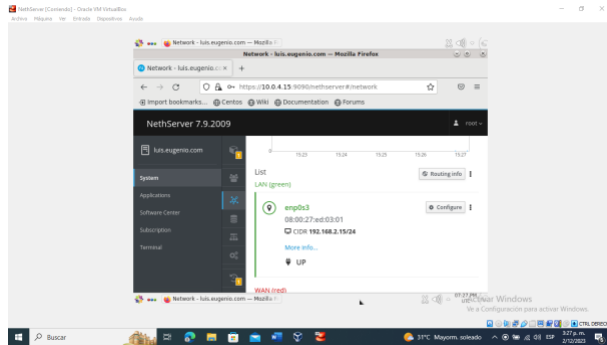


Fuente: Autoría propia

## 2.3 CONFIGURACIÓN INICIAL

En este punto de la configuración de NethServer, se procede a configurar las zonas DMZ. (García et al., 2022).

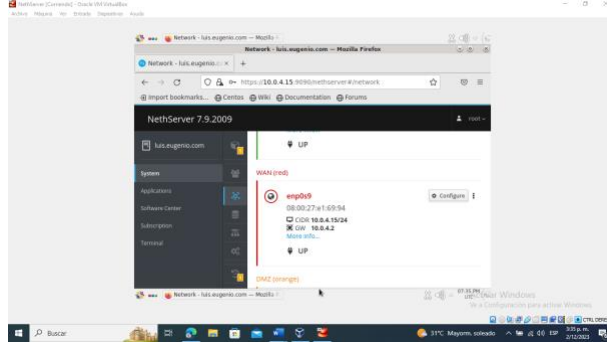
Figura. 9. Configuración Zona Verde



Fuente: Autoría propia

En el siguiente paso se configura la Zona Roja o zona desmilitarizada.

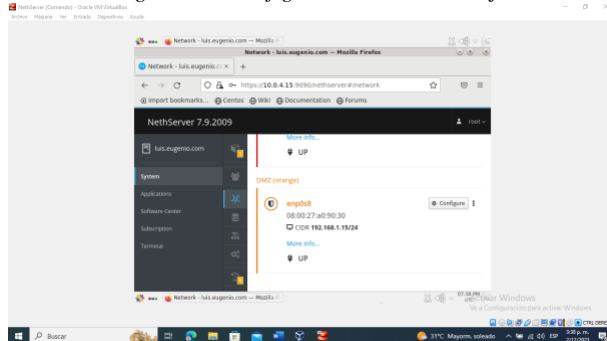
Figura. 10. Configuración Zona Roja



Fuente: Autoría propia

Finalmente, se realiza la configuración de la Zona Naranja.

Figura. 11. Configuración Zona Naranja



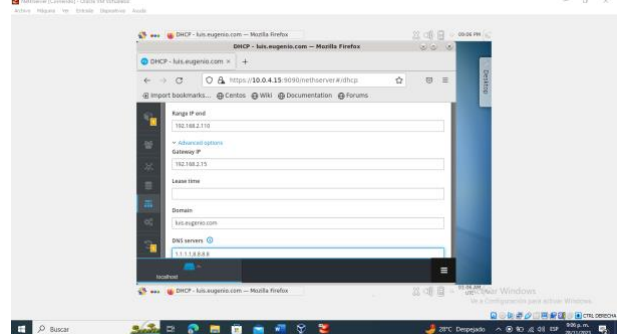
Fuente: Autoría propia

## 3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

### 3.1 SERVIDOR DHCP

En el apartado DHCP, se realiza la selección y procedemos con la configuración del servicio. Se asigna la IP 192.168.2.15 como puerta de enlace y se establece el dominio de servicio como luis.eugenio.com (Téllez & Fernanda, 2022). Además, se configura el DNS primario utilizando las direcciones 1.1.1.1 y 8.8.8.8, tal como se muestra en la Fig. 12.

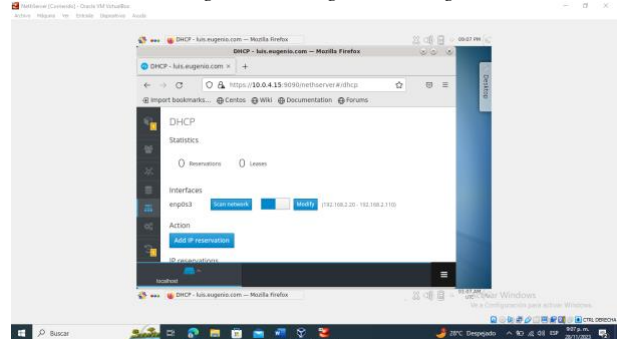
Figura. 12. Configuración servidor DHCP



Fuente: Autoría propia

Se continúa con la configuración, asignando rangos de IP que serán gestionadas por nuestro servidor. En este caso particular, se establece un rango desde la IP 192.168.2.20 hasta la 192.168.2.110, según se muestra en la Figura 13.

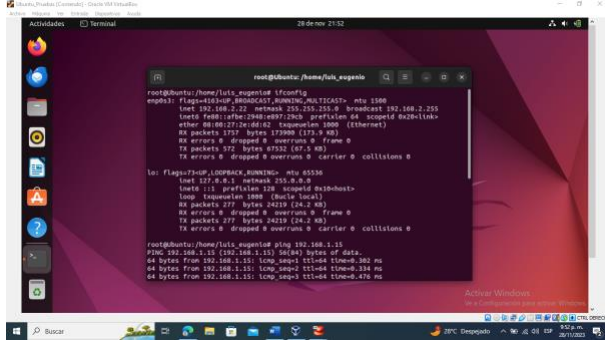
Figura. 13. Asignación rangos IP



Fuente: Autoría propia

Se procede a realizar una prueba de asignación automática de direcciones IP desde una máquina virtual con Linux Ubuntu. Tal como se muestra en la Figura 14, se confirma que la asignación de la IP corresponde al rango inicialmente parametrizado.

Figura. 14. Prueba Asignación IP

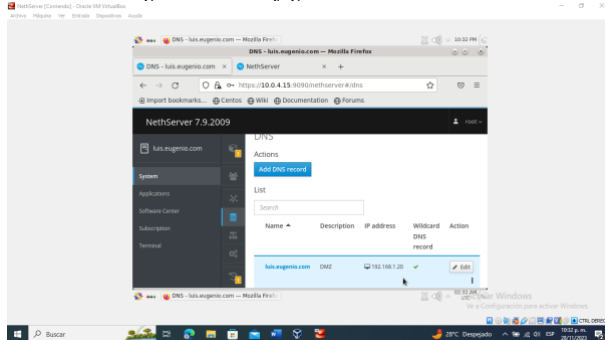


Fuente: Autoría propia

### 3.2 DNS SERVER

Mediante el DNS Server, se asegura la interpretación y reconocimiento de direcciones IP, así como el alojamiento del dominio al que se conecta, como se ilustra en la Figura 15 (Fonseca Ibáñez et al., 2022).

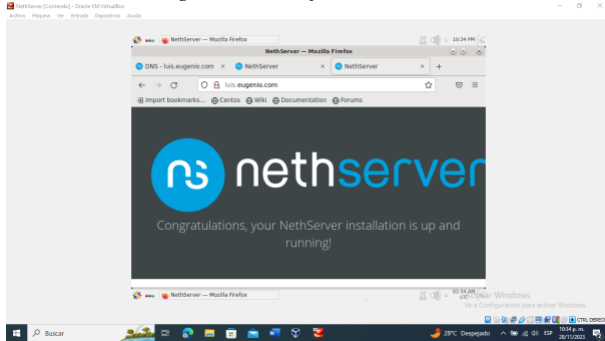
Figura. 15. Configuración DNS Server



Fuente: Autoría propia

Hacer clic en el enlace mostrado en la figura anterior y/o ingresar la dirección IP o el nombre del host del navegador.

Figura. 16. Verificación Enlace

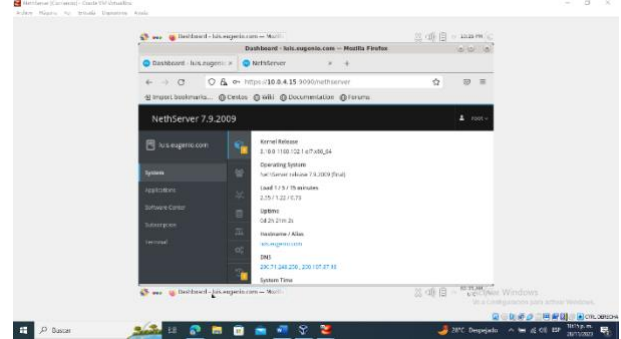


Fuente: Autoría propia

### 3.3 CONTROLADOR DE DOMINIO

La configuración de nuestro controlador de dominio asegura la correcta autenticación, autorización y aplicación de políticas de seguridad. En la Fig. 18, se muestra el enlace generado para acceder al controlador de dominio una vez configurados los parámetros necesarios (Leon Minota et al., 2022).

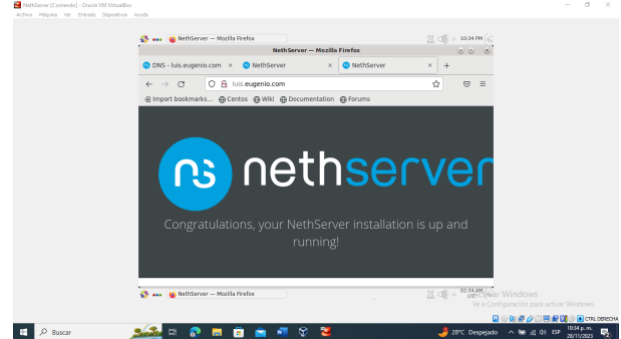
Figura. 17. Configuración Controlador Dominio



Fuente: Autoría propia

Se verifica que el controlador de dominio esté en funcionamiento y operativo.

Figura. 18. Controlador de dominio activo



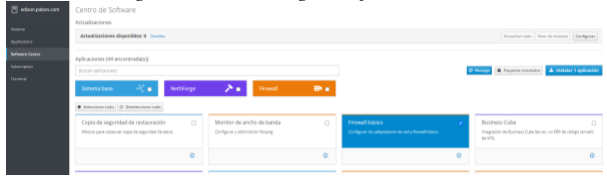
Fuente: Autoría propia

## 4 IMPLEMENTACIÓN Y GESTIÓN DEL PROXY

### 4.1 CONTROL DE ACCESO A INTERNET Y CONFIGURACIÓN DEL PROXY

Se da inicio descargando un firewall básico desde el Software Center.

Figura. 19. Descarga del firewall básico



Fuente: Autoría propia

Dentro del firewall que se instaló, en la pestaña principal, se puede visualizar información relevante sobre la arquitectura de la red actual.

Figura. 20. Interfaz de cortafuegos con arquitectura de red

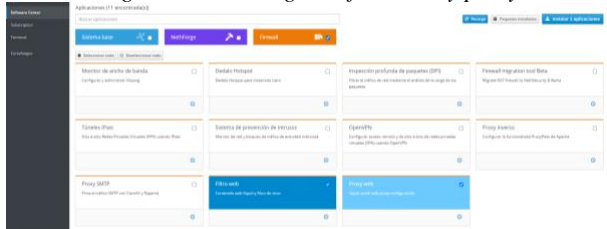


Fuente: Autoría propia

Se procede con la instalación del filtro web y un proxy web. Estas herramientas permitirán administrar y controlar el acceso a sitios web desde nuestra red.

## 4.2 DESCARGA E INSTALACIÓN DE HERRAMIENTAS DE PROXY Y FILTRO WEB

Figura. 21. Descarga del filtro web y proxy web



Fuente: Autoría propia

Dentro de las aplicaciones, se pueden visualizar las aplicaciones instaladas y crear accesos directos para facilitar su acceso y uso.

Figura. 22. Aplicaciones instaladas.



Fuente: Autoría propia

Ahora se debe ir a la sección de "Sistema" y luego a "Servicios" para verificar qué servicios están activos y cuáles no. En este punto, observamos que el servicio "Squid Proxy" no

está activado, por lo que se debe activar para su correcto funcionamiento.

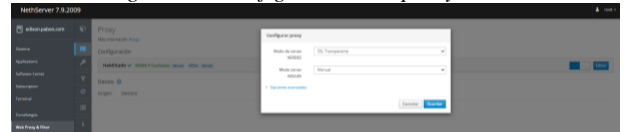
Figura. 23. Estado del Squid Proxy



Fuente: Autoría propia

Acceder a "Web Proxy and Filter" y dentro de la sección "Proxy", se debe habilitar la opción de "Filtro SSL transparente" para la red verde. Esta acción permitirá aplicar filtrado de contenido web SSL de manera transparente, mejorando la seguridad y el control en la red verde (Litardo Ordoñez & Yunda Sánchez, 2017).

Figura. 24. Configuración del proxy



Fuente: Autoría propia

Se confirma que el proxy está habilitado y configurado correctamente para su funcionamiento en la red. Esto posibilitará el filtrado y la gestión efectiva del tráfico web.

Figura. 25. Estado de configuración del proxy



Fuente: Autoría propia

Asimismo, se confirma que el Squid Proxy está habilitado y en funcionamiento al dirigirnos a la sección "Sistema" y luego a "Servicios".

Figura. 26. Estado del Squid Proxy



Fuente: Autoría propia

En la pestaña principal, se observa que el proxy SSL está habilitado, y se muestra otra información relevante. No obstante, en la parte superior, se detectan mensajes de advertencia. Es crucial revisar estos mensajes para abordar cualquier problema o configuración pendiente que pueda afectar el funcionamiento del proxy y la seguridad de la red.

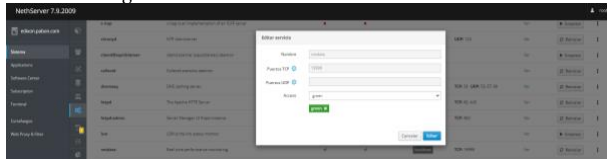
Figura. 27. Panel de control del proxy



Fuente: Autoría propia

Para resolver esto, se dirige a "Sistema" y luego a "Servicios". En la lista de servicios, se ubica "Netdata" y se hace clic en los tres puntos para acceder a la configuración. Cambiando la configuración de acceso de "localhost" a "green".

Figura. 28. Servicio de netdata



Fuente: Autoría propia

Esto posibilitará un acceso adecuado y seguro a Netdata desde la red verde, y resolverá los mensajes de advertencia mencionados anteriormente.

Figura. 29. Panel de control del proxy

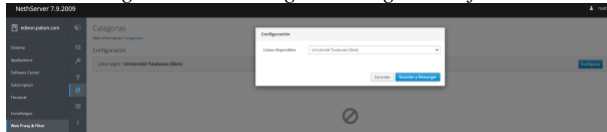


Fuente: Autoría propia

## 5 CONFIGURACIÓN DETALLADA DEL FILTRADO A TRAVÉS DEL PROXY

Para configurar las categorías, se accede a la sección de configuración del proxy. Desde allí, se puede descargar la categoría específica 'Université Toulouse' para aplicar políticas de filtrado de contenido relacionadas con esta categoría en la red.

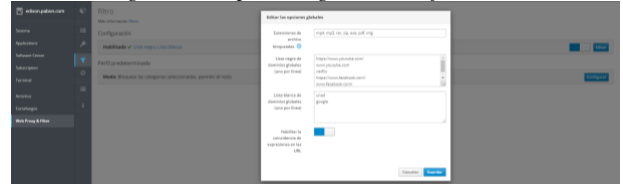
Figura. 30. Descarga de categoría de filtrado



Fuente: Autoría propia

Ahora vamos a editar las configuraciones globales del filtro web, incluyendo la filtración de extensiones, la lista negra, la lista blanca y la habilitación de coincidencias en expresiones. Estas configuraciones permitirán aplicar políticas específicas de filtrado de contenido en la red, considerando las extensiones de archivos y las páginas web definidas.

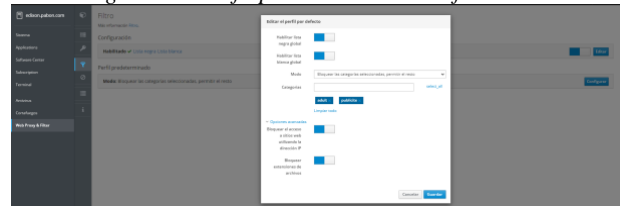
Figura. 31. Opciones globales de filtrado



Fuente: Autoría propia

Ahora se ejecuta la actividad para configurar el perfil predeterminado en el filtro web. Se bloquearán las categorías seleccionadas y se permitirá el acceso al resto. En otras palabras, el perfil predeterminado bloqueará el acceso a las categorías de contenido para adultos y publicidad, permitiendo el acceso al resto de las categorías.

Figura. 32. Perfil predeterminado del filtro web

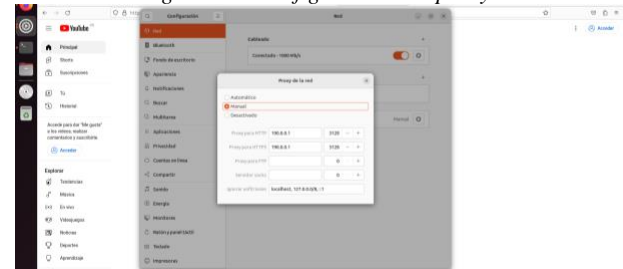


Fuente: Autoría propia

## 5.1 DEFINICIÓN, CONFIGURACIÓN Y VERIFICACIÓN DEL FILTRADO A TRAVÉS DEL PROXY

Si el servidor Squid Proxy web está escuchando en los puertos 3128, 3129 (HTTP) y 3130 (HTTPS), y está configurado para redirigir las peticiones, no es necesario configurar manualmente el proxy en el cliente. El servidor NetServer se encargará de redirigir el tráfico correctamente a través de los puertos configurados.

Figura. 33. Configuración del proxy



Fuente: Autoría propia

Ahora se verifica en el cliente que pueda acceder a una de las páginas que no tienen restricciones. Como se puede observar, el acceso se realiza exitosamente, confirmando que las configuraciones permiten el acceso a este sitio específico sin bloqueos.



Figura. 34. Página web de la UNAD

Fuente: Autoría propia

Al intentar acceder a una página para adultos, se muestra un bloqueo. Este resultado confirma que las restricciones de acceso y el filtrado de contenido están funcionando correctamente.



Figura. 35. Restricción de página web

Fuente: Autoría propia

También se intentó acceder a una página con anuncios y se observó que no se muestran, lo que indica un adecuado funcionamiento del filtro de contenido.



Figura. 36. Restricción de adultos en página web.

Fuente: Autoría propia

Ahora se intenta acceder a Facebook, sin embargo, al tratarse de una conexión segura HTTPS, se muestra un mensaje de advertencia. Aunque se intenta saltarlo yendo a la configuración avanzada y aceptando los riesgos, la restricción sigue funcionando.



Figura. 37. Acceso denegado a página web.

Fuente: Autoría propia

Si nos dirigimos a NethServer y accedemos a los registros (logs), encontraremos un listado de las peticiones realizadas. En este apartado se muestra un listado de las peticiones denegadas o las páginas a las que no se pudo acceder.



Figura. 38. Tabla de páginas filtradas.

Fuente: Autoría propia

También en la pestaña principal se puede confirmar el correcto funcionamiento del filtro de contenido. Se encuentra una gráfica que muestra las páginas permitidas y bloqueadas, además de un listado de las páginas bloqueadas y sus respectivas categorías. Esto proporciona una visión clara del funcionamiento del filtro y las restricciones aplicadas en la red.



Figura. 39. Estadísticas del proxy.

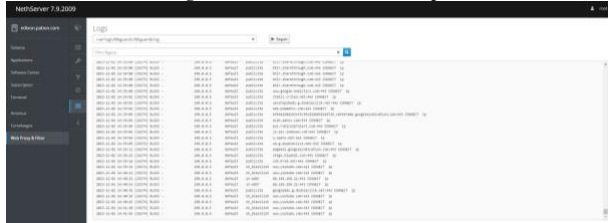
Fuente: Autoría propia

## 6 VPN

### 6.1 IMPLEMENTACIÓN Y CONFIGURACIÓN DETALLADA DE UNA VPN

Primero se realiza la instalación en el menú de aplicaciones de OpenVPN (Skendzic & Kovacic, 2017).

Figura 40. Instalación de OpenVPN

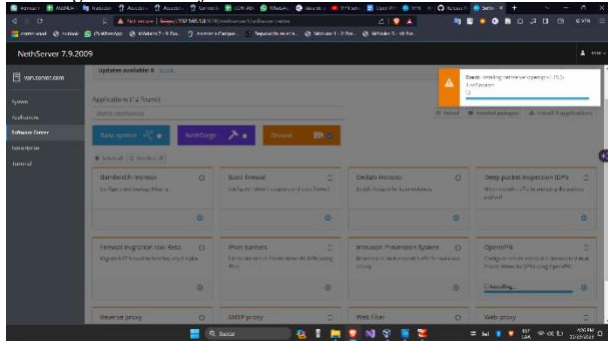


Fuente: Autoría propia

Se puede observar en la Fig. 40 que se accede al 'Software Center', donde se encuentran todas las aplicaciones disponibles para su descarga.

Después de esto se verifica en las aplicaciones instaladas;

Figura 41. Verificación de VPN instalada en servidor



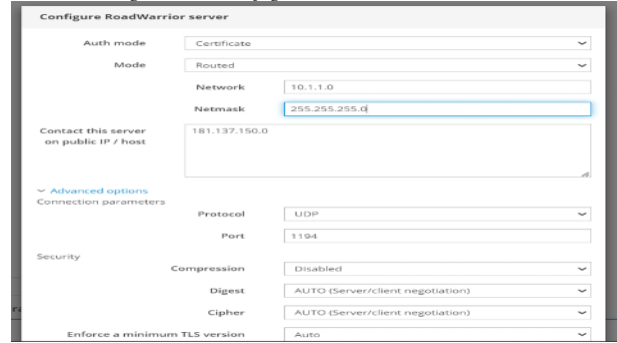
Fuente: Autoría propia

En la Fig. 41 se observa la posibilidad de configurar la VPN en el menú de aplicaciones del servidor.

### 6.2 CREACIÓN DE UN TÚNEL PRIVADO DE CONEXIÓN

La creación de este túnel privado de conexión requiere la configuración de la aplicación de VPN previamente instalada.

Figura 42. Configuración de túnel de VPN

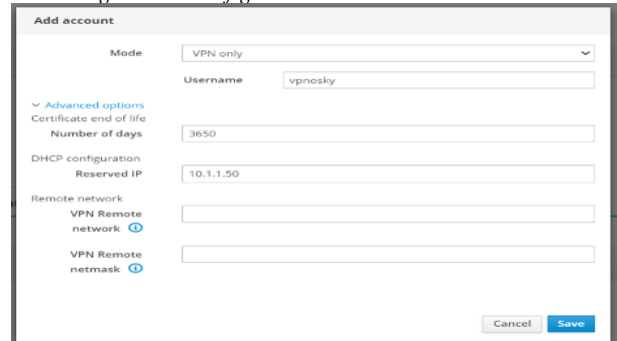


Fuente: Autoría propia

En la Fig. 42 se observa la configuración de la VPN en el servidor de NethServer.

Luego de esto, se procede a configurar las acciones de la VPN.

Figura 43. Configuración de acciones de la VPN

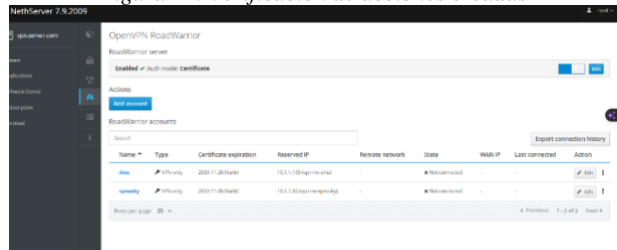


Fuente: Autoría propia

En la Fig. 43 se puede llevar a cabo la configuración de las acciones de la VPN.

Finalmente, se verifican las acciones creadas y se descarga el certificado para posterior ingreso por el túnel de VPN configurado.

Figura 44. Verificación de acciones creadas



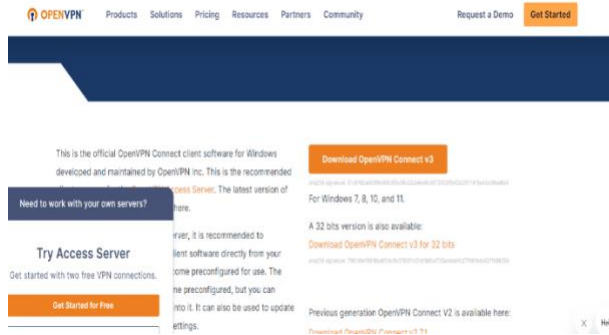
Fuente: Autoría propia

Es necesario descargar los certificados de cada una de las VPN creadas.

### 6.3 EVIDENCIA DE INGRESO A LA VPN

Para demostrar el funcionamiento de la VPN, es necesario descargar el software desde el cliente.

Figura 45. Descarga de OpenVPN cliente

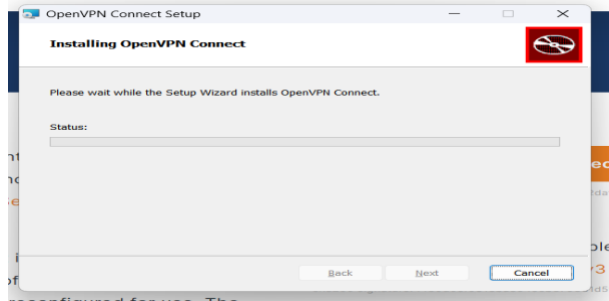


Fuente: Autoría propia

En la Fig. 45 se muestra el acceso a la página principal de OpenVPN y la opción de descarga desde el cliente.

Luego se procede con la instalación de la aplicación en el cliente de escritorio.

Figura 46. Instalación de OpenVPN cliente



Fuente: Autoría propia

Se procede con la instalación, como se puede evidenciar en la Fig. 46. Después de este proceso, la aplicación se inicia automáticamente.

Figura 47. Importación de certificado de túnel VPN



Fuente: Autoría propia.

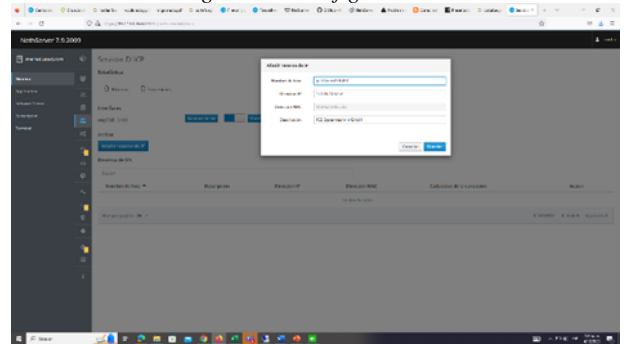
En la Fig. 47, basta con hacer clic en 'CONNECT' y el cliente se conectará a través de la VPN creada.

## 7 CONFIGURACIÓN DETALLADA DEL CORTAFUEGOS-FIREWALL

NethServer puede funcionar como cortafuegos y puerta de enlace dentro de la red donde está instalado. Todo el tráfico entre las computadoras de la red local e Internet pasa a través del servidor, el cual determina la ruta de los paquetes y las reglas a aplicar (Wang et al., 2016).

Se lleva a cabo la configuración de la IP reservada para el servidor LAN a través del enlace del Software Center desde la máquina virtual de escritorio al servidor NethServer.

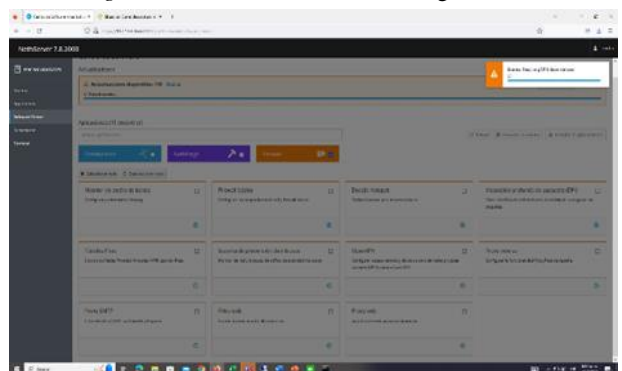
Figura 48. Configuración de IP



Fuente: Autoría propia

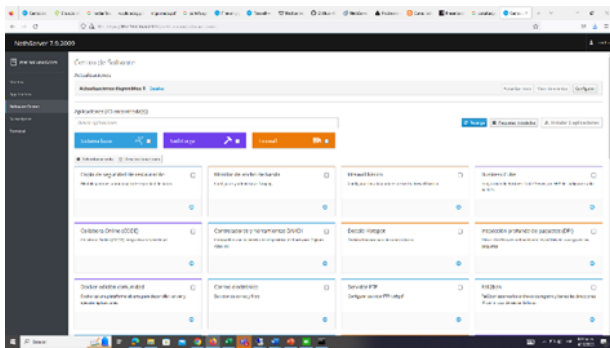
Ahora se procede a actualizar el sistema para que tome los cambios realizados.

Figura 49. Actualización de la configuración



Fuente: Autoría propia

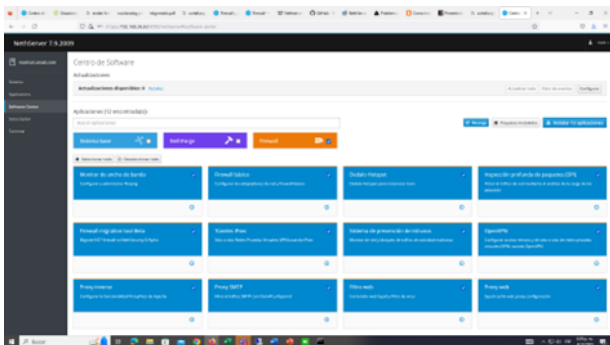
Figura. 50. Servidor Actualizado.



Fuente: Autoría propia

Después de actualizar el servidor, se procede a instalar los paquetes de Firewall.

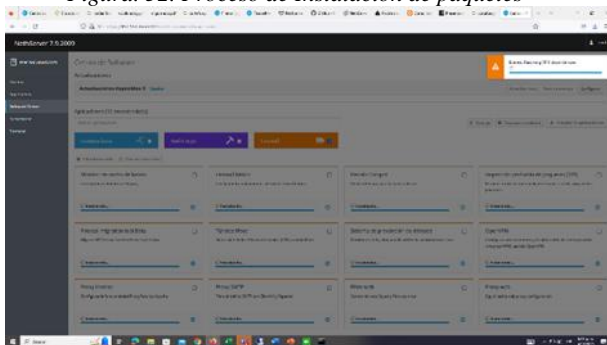
Figura. 51. Instalación de paquetes



Fuente: Autoría propia

Se inicia el proceso de instalación del Firewall desde el Software Center.

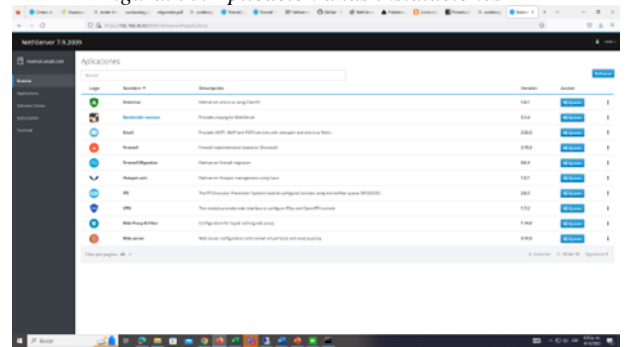
Figura. 52. Proceso de Instalación de paquetes



Fuente: Autoría propia

Se aplican y realizan los ajustes necesarios a la Firewall instalada desde el Software Center.

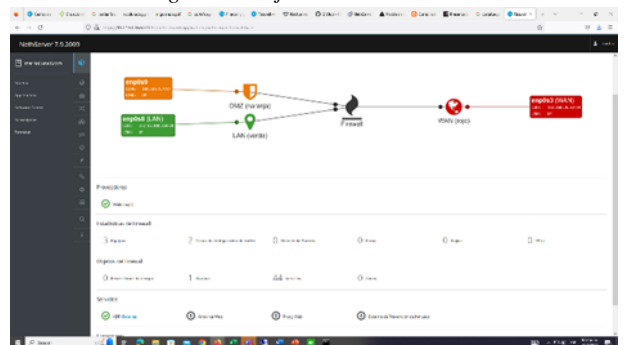
Figura. 53. Aplicación a las instalaciones



Fuente: Autoría propia

Se realizan los ajustes necesarios al Firewall de acuerdo con las instalaciones llevadas a cabo.

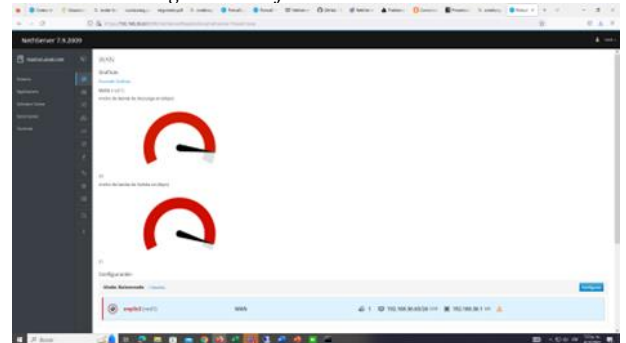
Figura. 54. Ajustes del Firewall



Fuente: Autoría propia

Igualmente, se realiza el ajuste del Firewall en la WAN.

Figura. 55. Ajustes del Firewall



Fuente: Autoría propia

Las políticas de firewall permiten el tráfico entre zonas siguiendo el esquema: GREEN -> BLUE -> ORANGE -> RED. Una regla consta de cuatro partes principales:

- Action: acción a tomar cuando se aplica la regla.
- Source: origen.
- Destination: destino.

- Service: servicio.

Las acciones disponibles son:

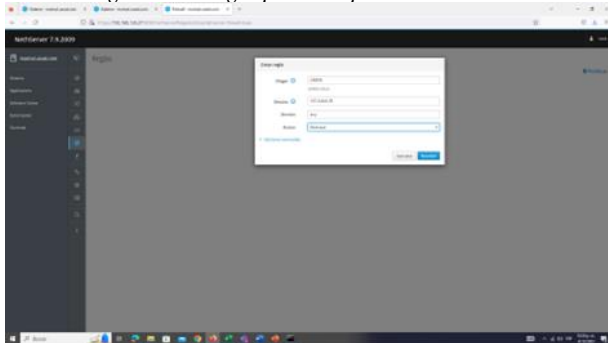
- ACCEPT: acepta el tráfico de red.
- REJECT: bloquea el tráfico y notifica al host remitente.
- DROP: bloquea el tráfico, elimina los paquetes y no envía notificación al host del remitente.
- ROUTE: enruta el tráfico al proveedor de WAN especificado.

## 7.1 EVIDENCIAS DE LA CONFIGURACIÓN Y APLICACIÓN DEL CORTAFUEGOS-FIREWALL

De acuerdo con las reglas establecidas para el Cortafuegos y puerta de enlace del servidor NethServer, se procede a configurar las siguientes reglas:

Dentro del Panel de control, se realiza la configuración de la regla para bloquear el acceso a la página Facebook.com. Para completar este proceso, es necesario conocer la IP asociada a dicha página. (IP: 152.240.6.35 para Facebook).

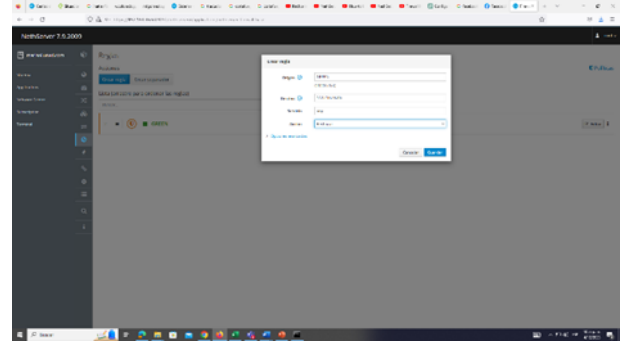
*Figura. 56. Regla para bloquear Facebook*



Fuente: Autoría propia

Igualmente, se configura la regla para bloquear el acceso a la página Youtube.com. Para llevar a cabo este proceso, es necesario conocer la IP asociada a dicha página. (IP: 142.250.78.46 para YouTube.com).

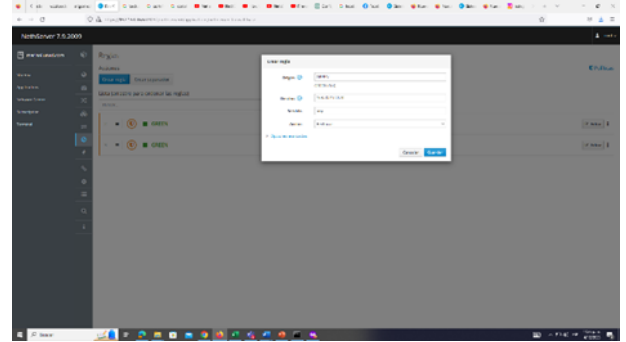
*Figura. 57. Regla para bloquear YouTube*



Fuente: Autoría propia

Asimismo, se configura la regla para bloquear el acceso a la página Instagram.com. Para llevar a cabo este proceso, es necesario conocer la IP asociada a dicha página. (IP: 142.250.78.46 para Instagram.com).

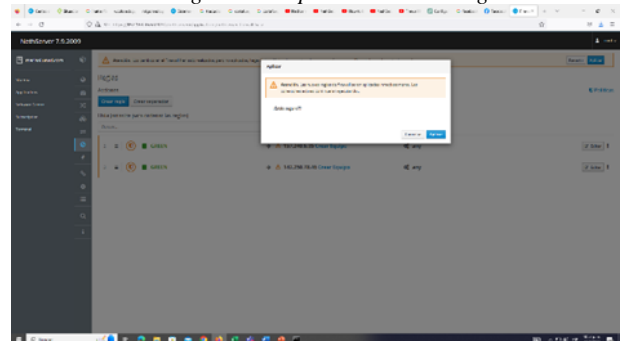
*Figura. 58. Regla para bloquear Instagram*



Fuente: Autoría propia

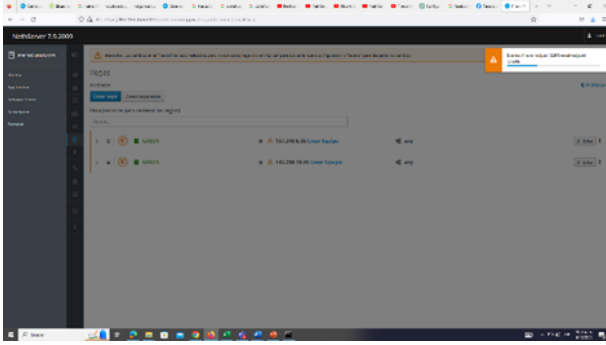
Con base en la configuración de las reglas realizadas, se procede a aplicarlas.

*Figura. 59. Aplicación de las reglas*



Fuente: Autoría propia

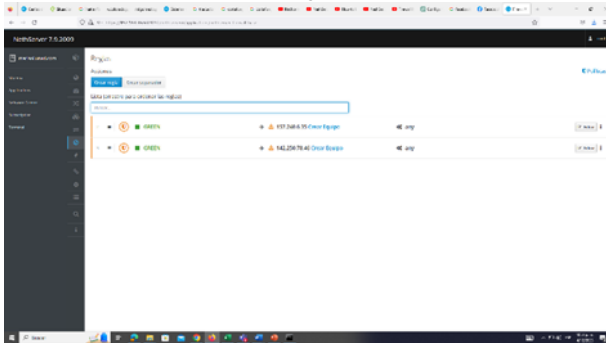
Figura 60. Aplicación de las reglas



Fuente: Autoría propia

La Fig. 59 muestra la aplicación de las reglas una vez configuradas en el servidor NethServer.

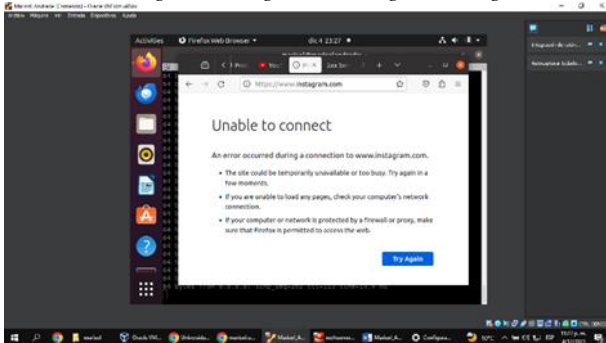
Figura 61. Reglas Aplicadas



Fuente: Autoría propia

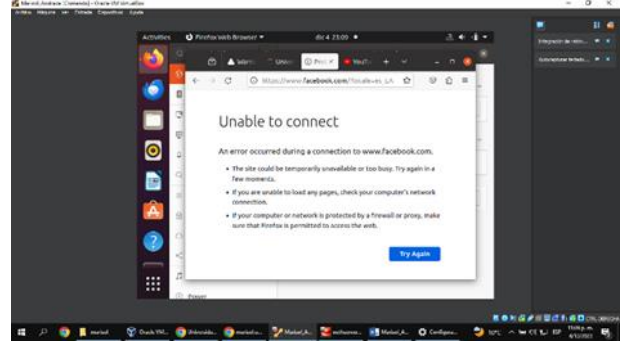
Las reglas se aplican en el explorador de la máquina cliente Desktop, lo que resulta en la restricción configurada.

Figura 62 Página de Instagram denegada



Fuente: Autoría propia

Figura 63. Página de Facebook denegada

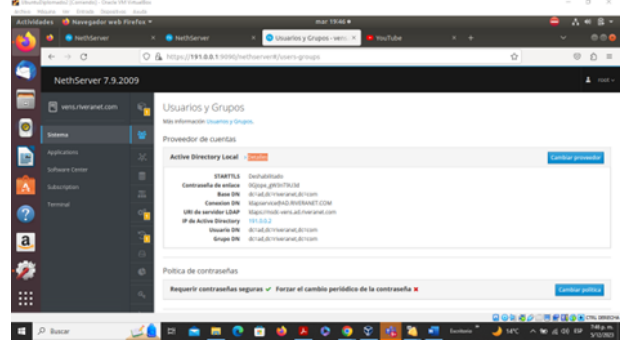


Fuente: Autoría propia

## 8. FILE SERVER Y PRINT SERVER

Para configurar el File Server y Print Server, es necesario dirigirse a la sección de 'Usuarios y Grupos' en la interfaz de NethServer, ya que estos servicios estarán destinados a los usuarios y grupos que se crearán con condiciones específicas (Amoyan et al., 2016).

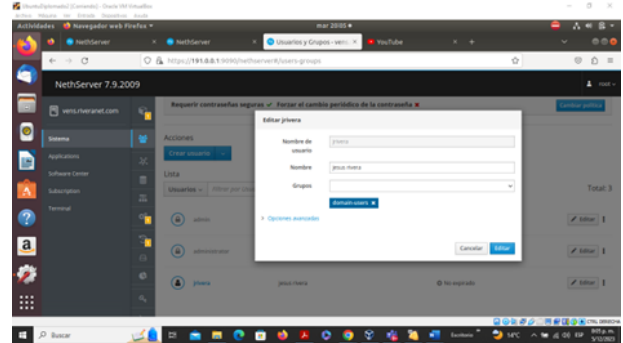
Figura 64. usuarios y grupos



Fuente: Autoría propia

Se accede a la pestaña de 'Crear Usuarios y Grupos'.

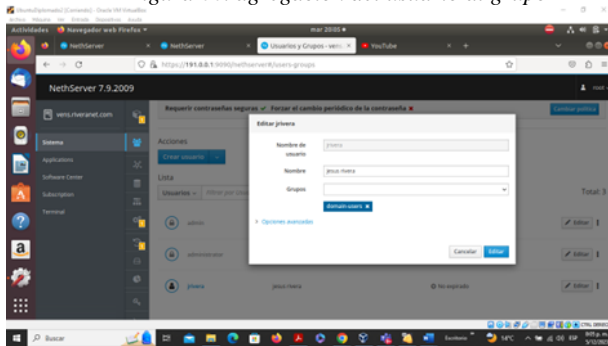
Figura 65. crear un usuario en Nethserver



Fuente: Autoría propia

Se añade un usuario al mismo grupo de dominio.

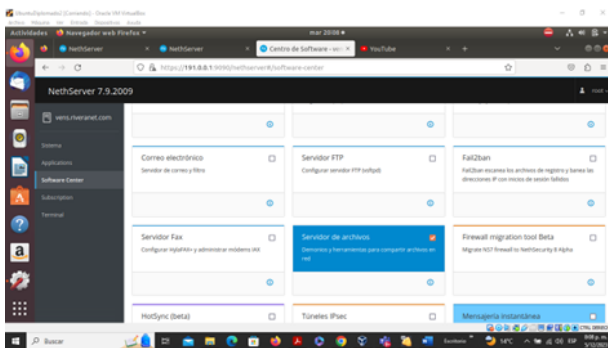
Figura 66. agregación del usuario al grupo



Fuente: Autoría propia

La instalación del módulo de File Server se realiza desde el Software Center. Este módulo se encarga de gestionar los archivos compartidos en el NethServer.

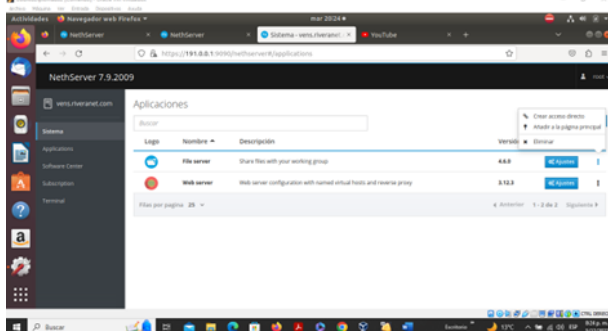
Figura 67. instalación del file server



Fuente: Autoría propia

Ahora se puede observar en el menú de aplicaciones del NethServer instalado el File Server.

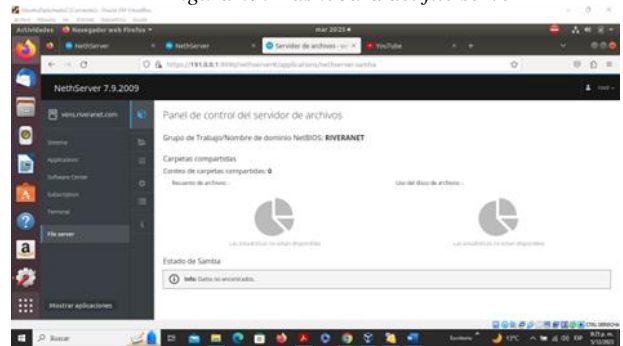
Figura 68. file server instalado



Fuente: Autoría propia

Dashboard del File Server en NethServer.

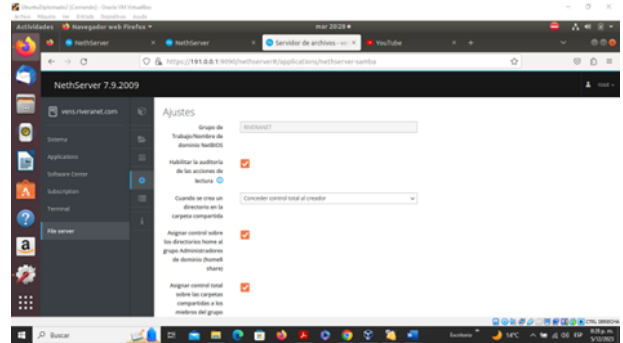
Figura 69. Dashboard del file server



Fuente: Autoría propia

Ajustes del File Server en NethServer. Dentro de los ajustes del File Server, se encuentra la opción para activar la auditoría de lectura, permitiendo el control de accesos a las carpetas compartidas.

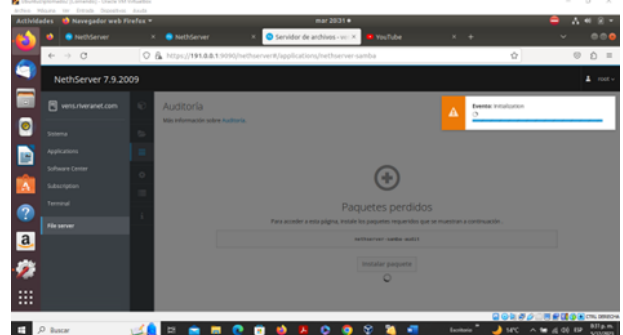
Figura 70. ajustes del file server



Fuente: Autoría propia

Se instaló el paquete 'samba-audit' para el File Server en NethServer.

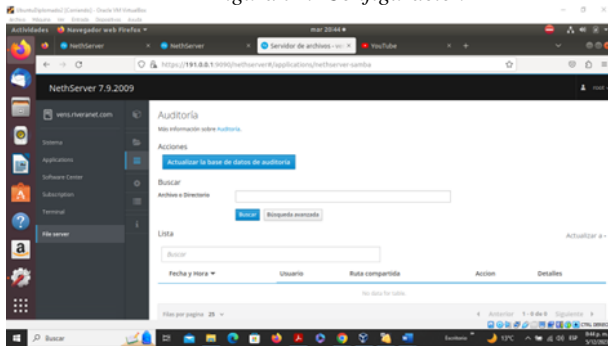
Figura 71. instalación de samba



Fuente: Autoría propia

Configuración de la auditoría del File Server.

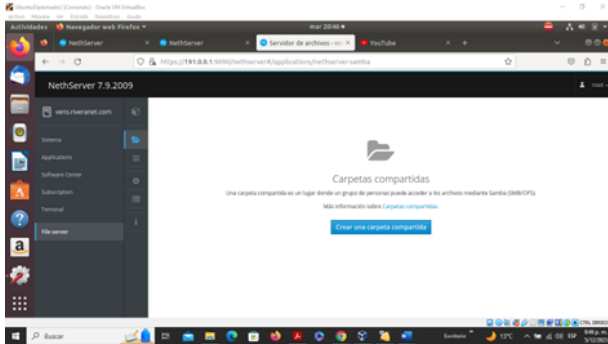
Figura 72. Configuración



Fuente: Autoría propia

Configuración de carpetas compartidas del File Server. Las carpetas compartidas emplean el servicio de Samba (SMB/CIFS).

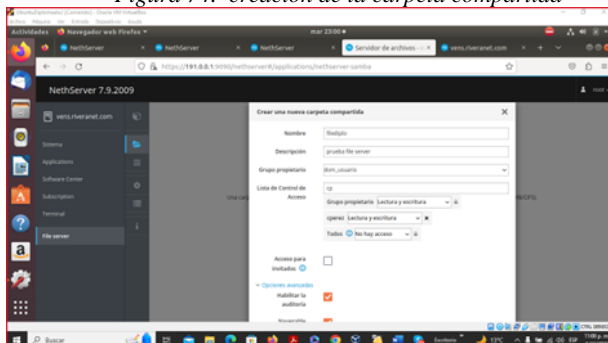
Figura 73. configuración de carpetas compartidas



Fuente: Autoría propia

Se configuró una carpeta compartida llamada 'Datos Diplomado' bajo el dominio 'domin\_users'.

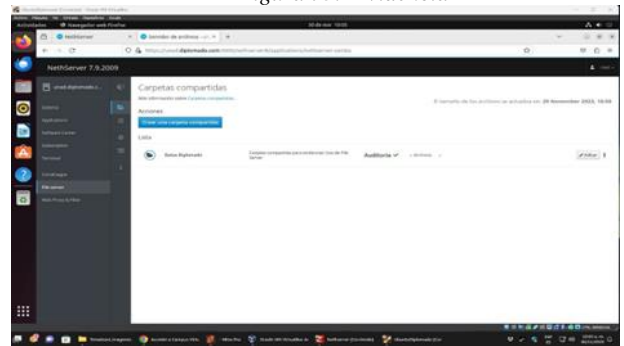
Figura 74. creación de la carpeta compartida



Fuente: Autoría propia

Evidencia de la Carpeta Compartida en NethServer.

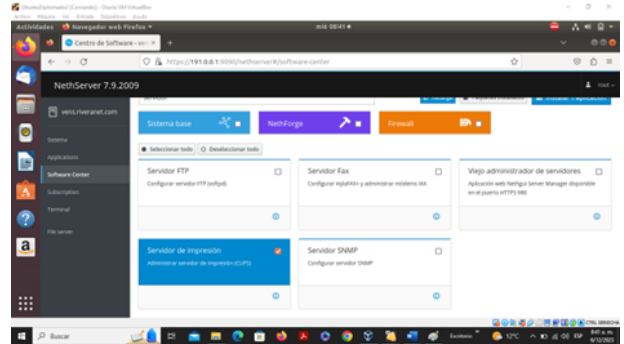
Figura 75. Evidencia



Fuente: Autoría propia

Instalación del módulo de impresión en NethServer.

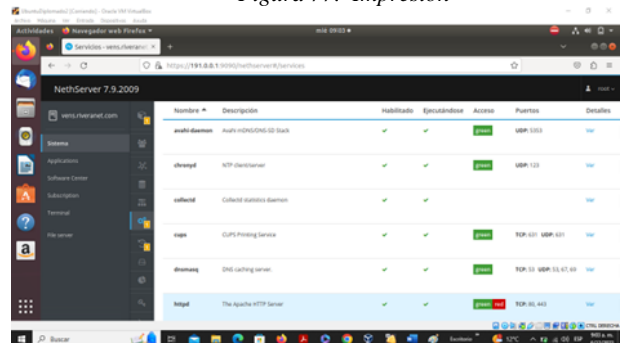
Figura 76. Instalación del print server



Fuente: Autoría propia

Servicios de impresión en NethServer.

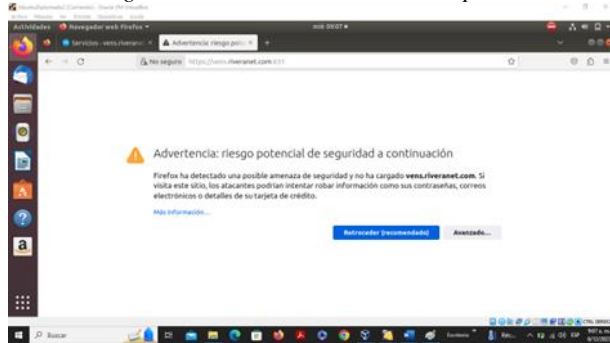
Figura 77. Impresión



Fuente: Autoría propia

Acceso a los servicios de impresión en NethServer.

Figura 78. Acceso a los servicios del print server



Fuente: Autoría propia

En el módulo de configuración CUPS se encuentran todas las opciones para configurar las impresoras destinadas al servicio de red.

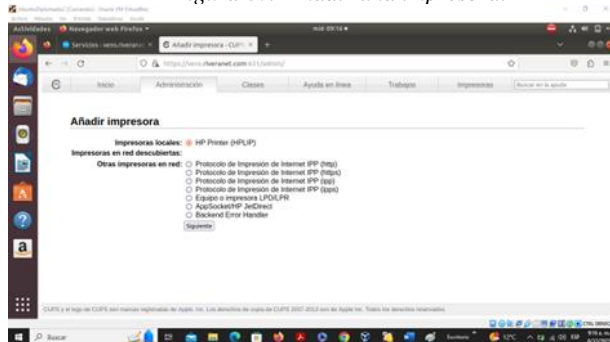
Figura 79. configurando el servicio de impresión



Fuente: Autoría propia

Procedimiento de configuración para agregar una impresora mediante un servidor de impresión.

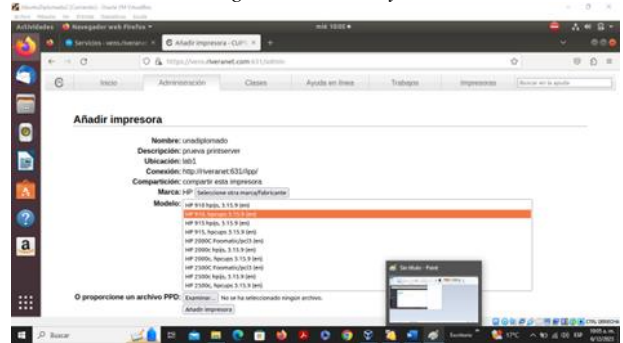
Figura 80. Añadir una impresora.



Fuente: Autoría propia

Incluir la marca y modelo de la impresora en NethServer.

Figura 81. Marca y modelo



Fuente: Autoría propia

Al acceder al servicio 'Red Prints', se encuentran las carpetas de opciones disponibles para la impresión.

Figura 82. contenido de la impresora en red



Fuente: Autoría propia

## 9. CONCLUSIONES

Una vez desarrolladas las actividades propuestas sobre la configuración de DHCP, DNS y el controlador de dominio en NethServer, se obtienen las siguientes conclusiones:

NethServer ofrece una solución integral para implementar y administrar servicios de red esenciales, como DHCP, DNS y controlador de dominio, en un entorno de servidor.

La configuración del servidor DHCP (Protocolo de Configuración Dinámica de Hosts) en NethServer permite la asignación automática de direcciones IP a los dispositivos de la red, simplificando la administración y evitando conflictos de IP. Además, permite personalizar y gestionar el rango de direcciones IP y los parámetros de red asociados.

La configuración de DNS (Sistema de Nombres de Dominio) en NethServer es fundamental para traducir nombres de dominio en direcciones IP, facilitando la navegación web y el acceso a recursos de red. NethServer utiliza la tecnología DNSMasq para proporcionar servicios completos de resolución de nombres de dominio en la red local.

El controlador de dominio en NethServer ofrece funcionalidades similares a las de un servidor de dominio de Windows Active Directory. Permite centralizar la gestión de usuarios, grupos y políticas de seguridad en una red, además de proporcionar autenticación centralizada para los usuarios.

La implementación de un sistema de proxy en NethServer ha demostrado ser una herramienta esencial para gestionar y controlar el acceso a Internet. La configuración del proxy en el puerto 3128 y el uso del filtro SSL transparente han optimizado la seguridad y eficiencia de la red. Esta experiencia destaca la capacidad de NethServer para manejar aspectos críticos de la seguridad de la red y administrar el acceso a Internet y el filtrado de contenido web.

NethServer actúa como un servidor de código abierto que incluye módulos para servidores de correo, cortafuegos, servidor web, servidor FTP, filtro web, entre otros, y puede adaptarse según las necesidades de una empresa u organización.

Las actividades de configuración de las zonas roja, verde y naranja, asignadas al DMZ, realizadas en NethServer, adquirieron habilidades y conocimientos aplicables en entornos específicos.

Las reglas aplicadas para el cortafuegos o Firewall en NethServer siguen un orden lógico e implementan los ítems establecidos con coherencia.

Las pruebas realizadas en los servidores de archivos y de impresión han arrojado resultados positivos. Además, se validó la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a los servicios de carpetas compartidas e impresoras a través del controlador de dominio LDAP. Estas pruebas demostraron la eficiencia y coherencia de la infraestructura diseñada, satisfaciendo las necesidades específicas de gestión de archivos e impresión en un entorno de red.

El procedimiento para crear una VPN con NethServer sigue un enfoque sistemático y bien definido. Inicia con la instalación de OpenVPN desde el menú de aplicaciones y se verifica su presencia en el servidor. La configuración del túnel privado de conexión se realiza a través de pasos claros, evidenciados en las figuras 6.3 y 6.4. La verificación de las acciones creadas y la descarga de certificados en la figura 6.5 aseguran la correcta implementación. La evidencia de ingreso a la VPN, demostrada en las figuras 6.6, 6.7 y 6.8, destaca la simplicidad y eficacia del proceso, permitiendo una conexión fácil para los usuarios finales.

## 10. REFERENCIAS

Amoyan, R. L., Bacomo, K., Fadol, L., Marquez, C., & Paniza, R. (2016). *Design and implementation of a cloud-based storage system for Central Philippine University College of Computer Studies*. <https://repository.cpu.edu.ph/handle/20.500.12852/2284>

Cristancho, C., & Marcela, D. (2023). *Implementación y configuración de NethServer*. <http://repository.unad.edu.co/handle/10596/54431>

Fonseca Ibáñez, B. F., Pérez Pira, F., Robles Pinza, A. M., & Calderón López, H. M. (2022). *Servidor NethServer Solución para medianas y pequeñas empresas basado en Centos*. <http://repository.unad.edu.co/handle/10596/50546>

García, E. A., Jaramillo, P. A. R., Acevedo, C. M. S., Delgado, F. N. G., & Clavijo, C. A. M. (2022). *Implementación y configuración bajo NethServer solucionando necesidades específicas con GNU/Linux*. <http://repository.unad.edu.co/handle/10596/53803>

Leon Minota, Y., Gonzales Bolivar, J., Cruz Arango, C. A., Carabali Medina, B. G., & Balanta, D. S. (2022). *Implementación de servicios de infraestructura IT usando Nethserver*. <http://repository.unad.edu.co/handle/10596/54019>

Litardo Ordoñez, Y. L., & Yunda Sánchez, J. E. (2017). *Reestructuración y optimización de los servicios de la red de datos cableada e inalámbrica mediante la implementación de un servidor Proxy en Linux en la Unidad Educativa "América del Sur"*. [bachelorThesis]. <http://dspace.ups.edu.ec/handle/123456789/14157>

Santacruz Machado, J. M., & Patricia Vasquez, L. (2022). *Instalación e implementación del sistema NethServer 7.9 para los servicios y puesta en marcha en la seguridad de la infraestructura de la red*. <http://repository.unad.edu.co/handle/10596/53963>

Skendzic, A., & Kovacic, B. (2017). Open source system OpenVPN in a function of Virtual Private Network. *IOP Conference Series: Materials Science and Engineering*, 200(1), 012065. <https://doi.org/10.1088/1757-899X/200/1/012065>

Téllez, M., & Fernanda, L. (2022). *Instalación y configuración DHCP Server, DNS Server, Controlador de Dominio, File Server Y Print Server bajo Nethserver*. <http://repository.unad.edu.co/handle/10596/54076>

Wang, B., Lu, K., & Chang, P. (2016). Design and implementation of Linux firewall based on the frame of Netfilter/IPtable. *2016 11th International Conference on Computer Science & Education (ICCSE)*, 949–953. <https://doi.org/10.1109/ICCSE.2016.7581711>