DE LA CONFIGURACIÓN A LA CONEXIÓN: USO DE NETHSERVER PARA RESOLVER DESAFÍOS DE REDES

Angie Agudelo Rojas
e-mail: agagudelor@unadvirtual.edu.co
Jefferson Sick Bohorquez Velasquez
e-mail: jsbohorquezve@unadvirtual.edu.co
Luisa Fernanda Quintero Ariza
e-mail: lfquinteroar@unadvirtual.edu.co
Michel Viviana Hernández Rojas
e-mail: mvhernandezr@unadvirtual.edu.co
Steffany Johana Rojas Comas
e-mail: sjrojasco@unadvirtual.edu.co

RESUMEN:

Este artículo aborda la implementación de soluciones específicas para la administración de sistemas a través de NethServer, una plataforma basada en GNU/Linux diseñada para simplificar la gestión de servidores. El desarrollo incluye la configuración de servicios clave, como VPN para comunicaciones privadas seguras, Samba para compartir recursos entre sistemas heterogéneos, y DNS para garantizar la resolución eficiente de nombres de dominio. Además, se exploran funciones avanzadas de seguridad mediante cortafuegos, gestión de usuarios y grupos, y herramientas de monitoreo. Este trabajo demuestra cómo NethServer centraliza y facilita la administración de infraestructura tecnológica, ofreciendo un enfoque robusto y accesible para la resolución de necesidades organizacionales.

PALABRAS CLAVE: AWS, DHCP, DNS, Firewall, Linux, Nethserver, Proxy, servidor, VPN.

3 INTRODUCCIÓN

En la actualidad, las organizaciones enfrentan la necesidad de gestionar entornos tecnológicos cada vez más complejos, donde la seguridad, conectividad y disponibilidad de recursos son fundamentales. Este trabajo presenta una implementación práctica utilizando NethServer, una plataforma basada en GNU/Linux que permite administrar servicios críticos de manera centralizada y sencilla. Ofrece una interfaz intuitiva y modular que permite implementar servicios esenciales como proxy, firewall, servidor de correo, VPN, y más, con configuraciones centralizadas y fáciles de manejar. Su flexibilidad y enfoque en la seguridad hacen de NethServer una solución robusta para optimizar y proteger infraestructuras de TI.

Complementando esta solución, se utilizó la infraestructura de Amazon Web Services (AWS) para alojar y desplegar los servidores, aprovechando su escalabilidad y flexibilidad.

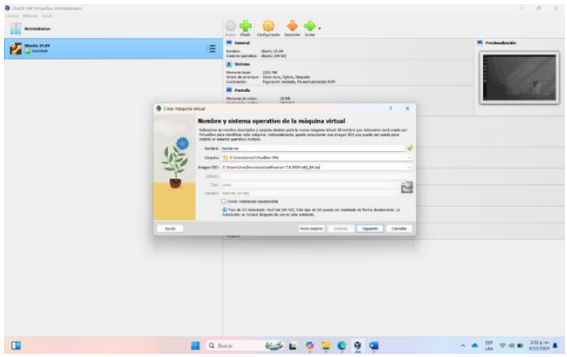
Las actividades incluyeron la configuración de un servidor VPN para establecer túneles seguros de comunicación, el uso de Samba para compartir recursos entre sistemas heterogéneos como GNU/Linux, Windows y macOS, y la implementación de servicios DNS para garantizar la resolución eficiente de nombres de dominio. Adicionalmente, se configuraron políticas de seguridad a través de cortafuegos, y se utilizaron herramientas de monitoreo para supervisar la infraestructura.

La integración de NethServer con AWS demuestra cómo es posible abordar necesidades específicas de administración de sistemas, combinando soluciones de software libre con servicios en la nube. Este enfoque no solo garantiza la flexibilidad y escalabilidad requeridas por las organizaciones, sino que también simplifica la administración y mejora la seguridad del entorno tecnológico.

4 INSTALACIÓN DE NETHSERVER

Para instalar Nethserver se requiere ir al sitio oficial https://www.nethserver.org/getting-started-withnethserver/ y descargar el archivo ISO de instalación. Posteriormente se abre VirtualBox (Previamente instalado) y se crea una nueva máquina virtual, esto siguiendo la guía y asignando la configuración deseada y requerida (cantidad de memoria RAM recomendada mínimo 1 GB y disco duro virtual con al menos 20 GB de espacio).

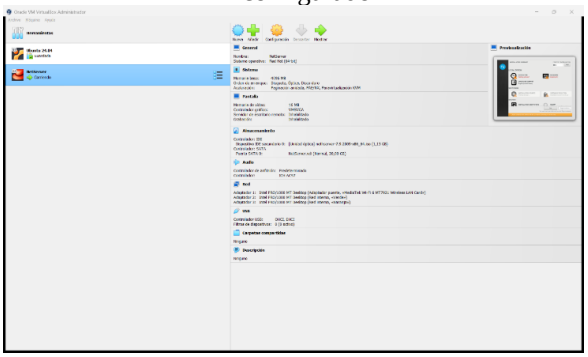
Figura 1. Creación de máquina virtual con NethServer



Fuente. Autoría Propia

Al finalizar la configuración se puede evidenciar en la interfaz de VirtualBox, como la máquina ya está lista para ejecutarse y con la configuración de las redes (Adaptador 1: adaptador puente; Adaptador 2: red interna verde; adaptador 3: red interna naranja) que se utilizarán para la implementación de los servicios en Nethserver.

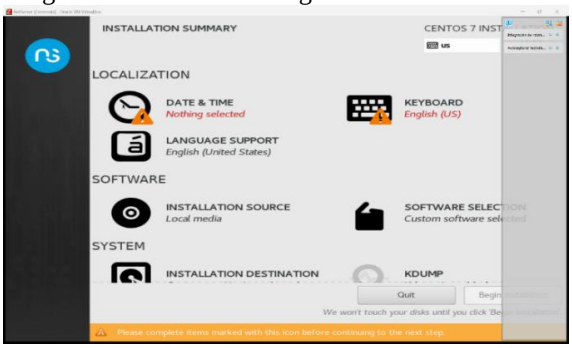
Figura 2. Interfaz de VirtualBox con NethServer configurado



Fuente. Autoría Propia

Al iniciar la máquina por primera vez, se ve una guía rápida para poder configurar el entorno de Nethserver, donde nos pide especificar la fecha y hora por medio de la ubicación geográfica, definir el lenguaje del teclado y configurar el usuario root y otro usuario si se desea.

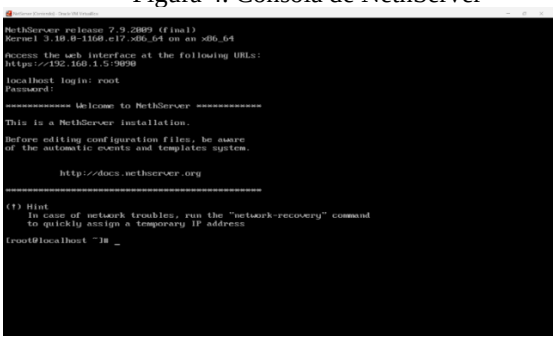
Figura 3. Interfaz de configuración de NethServer



Fuente. Autoría Propia

Una vez finalizada la configuración del entorno de Nethserver, se observa la inicialización del sistema operativo y la consola nos muestra la versión de Nethserver, la dirección IP asignada 192.168.1.5, el puerto 9090, y pide iniciar sesión con las credenciales previamente establecidas, como se evidencia en la siguiente imagen se inicia sesión con el usuario root, y así ya se tiene acceso a la línea de comandos donde se podrá interactuar con el sistema operativo.

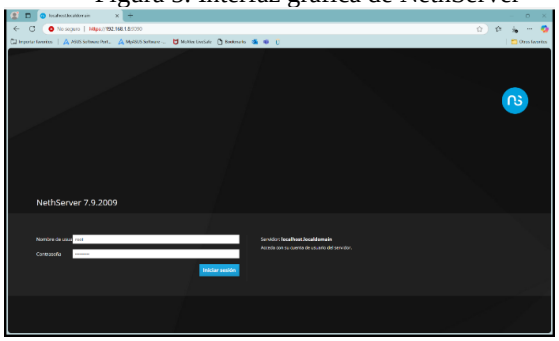
Figura 4. Consola de NethServer



Fuente. Autoría Propia

Mientras está corriendo el servidor de NethServer en la máquina virtual de VirtualBox, se puede acceder a la interfaz gráfica de administración de NethServer desde cualquier navegador web en el equipo anfitrión o en cualquier dispositivo conectado a la misma red. Esto se logra ingresando la dirección IP del servidor NethServer seguida del puerto específico de acceso, en este caso, 192.168.1.8:9090.

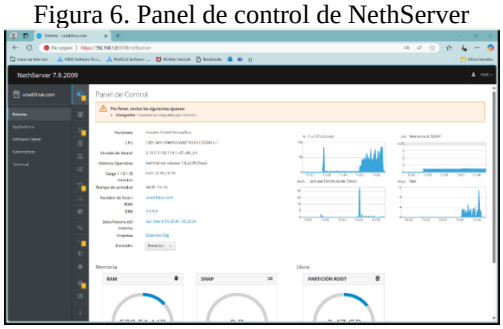
Figura 5. Interfaz gráfica de NethServer



Fuente. Autoría Propia

Una vez ingresado en el entorno NethServer, se visualiza el panel de control, una interfaz web intuitiva y centralizada desde la cual se pueden manipular y gestionar los diferentes servicios que ofrece NethServer. Este panel de control es esencial para la administración efectiva del servidor y es el punto de partida para la implementación y configuración de varios servicios clave.

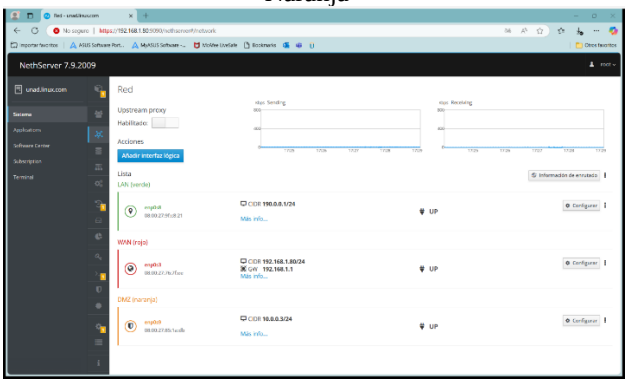
Figura 6. Panel de control de NethServer



Fuente. Autoría Propia

En el menú desplegable que ofrece el entorno, en el apartado de “Red” se gestionan los adaptadores, como se evidencia en la siguiente imagen NethServer tiene configurado 3 adaptadores, adaptador verde con la IP 190.0.0.1/24 que corresponde a el equipo Desktop, este adaptador está configurado como la red local (LAN), la red verde se considera segura y está destinada a dispositivos internos de la organización., adaptador rojo con la ip 192.168.1.80/24, este adaptador está configurado como la red externa (WAN) y se encarga de la conexión a Internet y adaptador naranja con la ip 10.0.0.3/24, este adaptador está configurado como la Zona Desmilitarizada (DMZ), se utiliza para servicios que deben ser accesibles desde fuera de la red local, como servidores web, servidores de correo, etc.

Figura 7. Configuración de las Zonas Verde, Roja, Naranja



Fuente. Autoría Propia

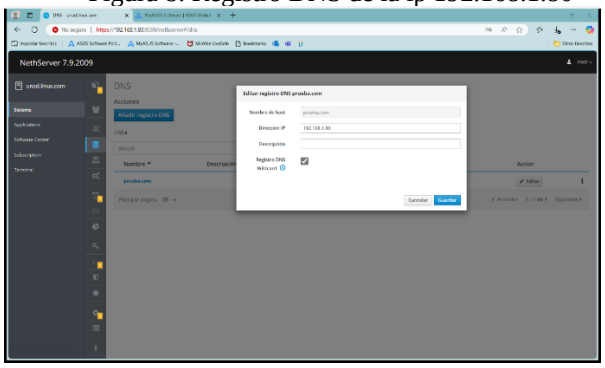
5 DESARROLLO DE TEMATICAS

5.3 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

5.3.1 IMPLEMENTACIÓN DE DNS SERVER

Para realizar la implementación del servicio de DNS se requiere ir al módulo “DNS” de NethServer, en donde se podrá añadir el nombre del host, dirección ip y una descripción, en la siguiente imagen se ve la configuración de la dirección ip 192.168.1.80, la cual corresponde a la interfaz de NethServer, sin embargo, se agrega el dominio prueba.com para que desde este se puede ingresar. Configurar un DNS local en NethServer permite la resolución rápida y eficiente de nombres de host dentro de la red local, mejorando el rendimiento de la red.

Figura 8. Registro DNS de la ip 192.168.1.80



Fuente. Autoría Propia

Una vez realizado el registro del dominio deseado, se procede a realizar la prueba desde el navegador de nuestra máquina virtual correspondiente a la zona verde, en la siguiente imagen se ve el resultado de dicha prueba, donde se evidencian la conexión correspondiente con el DNS Y cómo ingresando en el buscador “prueba.com”, se accede a la IP 192.168.1.80 correspondiente a la interfaz de NethServer.

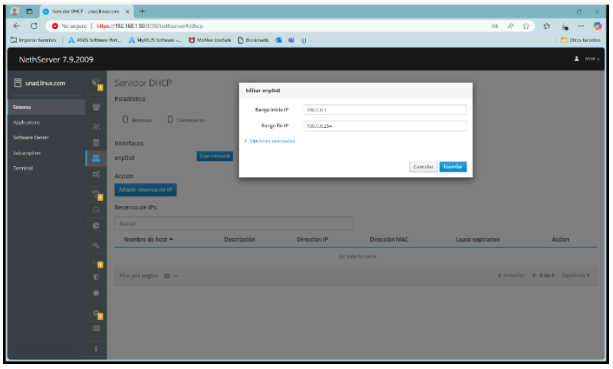
Figura 9. Prueba de acceso a DNS

Fuente. Autoría Propia

5.3.2 IMPLEMENTACIÓN DE DHCP SERVER

Para realizar la implementación del servicio de DHCP se requiere ir al módulo “DHCP” de NethServer, en esta interfaz podemos evidenciar que reconoce automáticamente la interfaz enp0s8, la cual corresponde a la zona verde, ahí se selecciona la opción de “modificar” y tal como se evidencia en la siguiente imagen, permite definir el rango en el que se asignaran las IP de la zona verde.

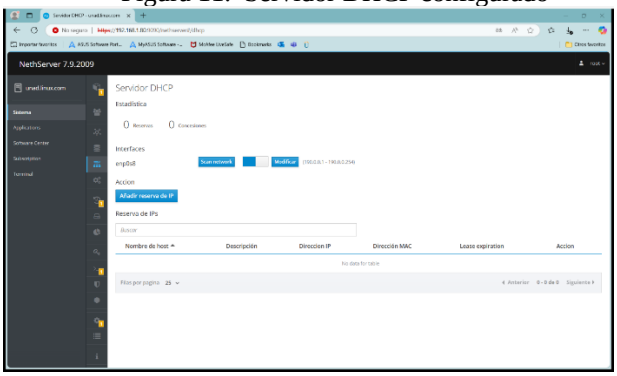
Figura 10. Asignación de rango IP para servidor DHCP



Fuente. Autoría Propia

Una vez seleccionado el rango y activado el servicio se puede hacer uso del servicio, en el mismo módulo de “DHCP” se puede evidenciar la opción “Añadir reserva de IP”, la cual permite asignar siempre la misma dirección IP al dispositivo seleccionado asociada a la dirección MAC y que ningún otro equipo pueda tomarla.

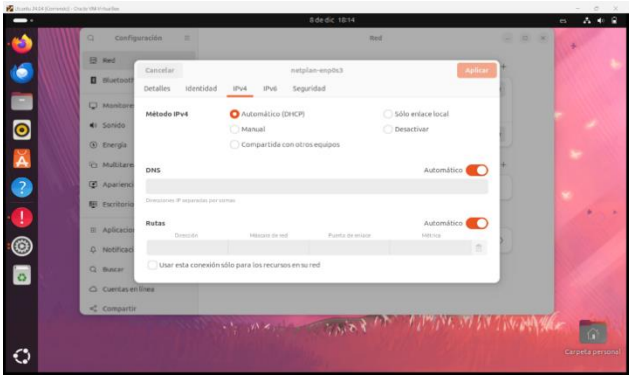
Figura 11. Servidor DHCP configurado



Fuente. Autoría Propia

Es importante tener en cuenta que desde la máquina virtual configurada como el cliente, ubicada en la zona verde (LAN), se debe activar la asignación de direcciones IP en modo automático (DHCP). Esto asegura que el cliente reciba una dirección IP válida de manera automática del servidor NethServer, lo cual simplifica la gestión y evita conflictos de IP, como se evidencia en la siguiente imagen.

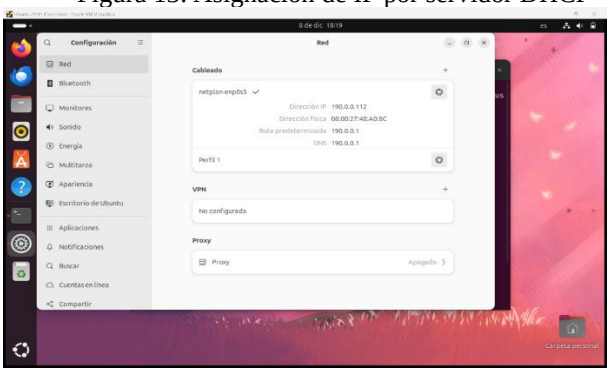
Figura 12. Activación de DHCP en la máquina virtual cliente



Fuente. Autoría Propia

Una vez activado el método IP en modo DHCP, la máquina cliente en la zona verde comenzará automáticamente a solicitar una dirección IP al servidor DHCP configurado en NethServer, que para este caso es la ip 190.0.0.112.

Figura 13. Asignación de IP por servidor DHCP

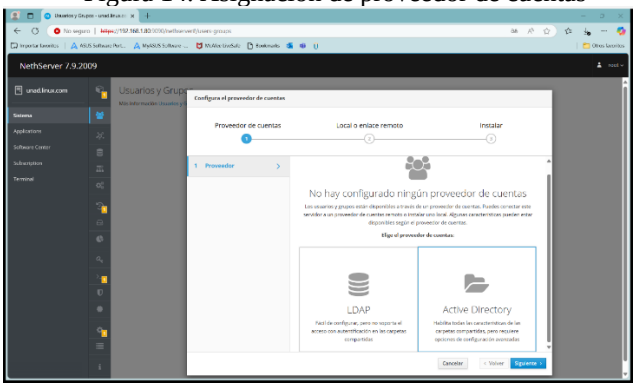


Fuente. Autoría Propia

5.3.3 SERVICIO DE CONTROLADOR DE DOMINIO

Para realizar la implementación del servicio de Controlador de Dominio en NethServer, es necesario seguir una serie de pasos específicos dentro del módulo "Usuario y Grupos". Este proceso incluye la selección de Active Directory como proveedor de cuentas, que permite una gestión centralizada y segura de usuarios y grupos.

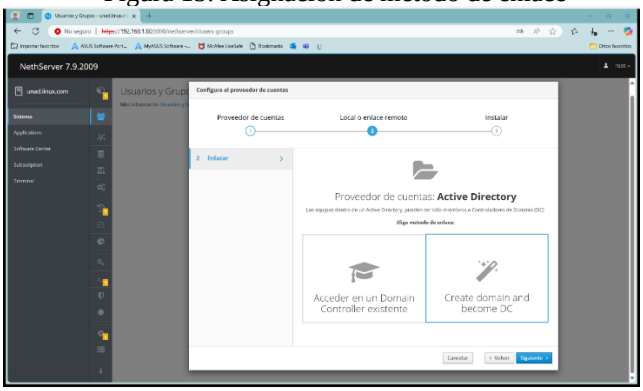
Figura 14. Asignación de proveedor de cuentas



Fuente. Autoría Propia

Posteriormente se escoge el método de enlace, para este caso será "Create domain and become DC", este proceso transformará a NethServer en un Controlador de Dominio (DC), permitiendo gestionar centralmente usuarios y dispositivos en la red.

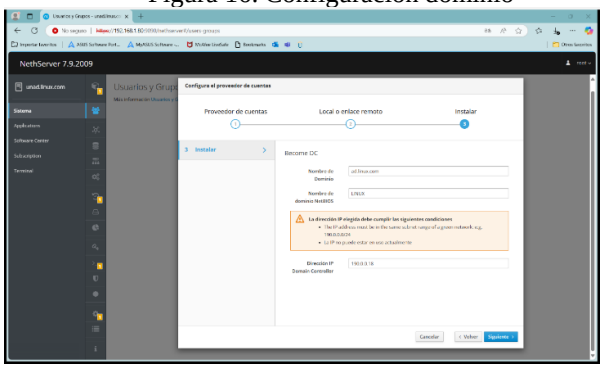
Figura 15. Asignación de método de enlace



Fuente. Autoría Propia

Seguidamente se define el nombre de dominio, ad.linux.com, nombre del dominio netbios, Linux, y la dirección ip del controlador del dominio, 190.0.018, es importante destacar que el nombre de dominio debe ser único y representativo de la organización o propósito del dominio.

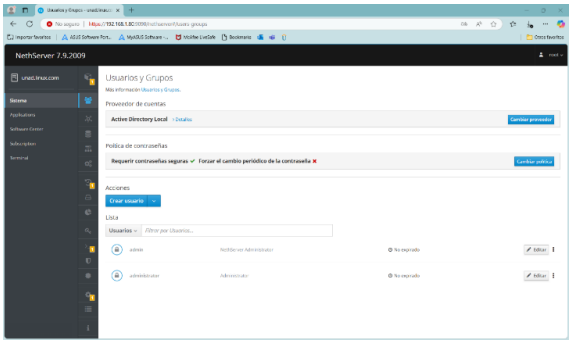
Figura 16. Configuración dominio



Fuente. Autoría Propia

El siguiente paso es gestionar los usuarios predeterminados que vienen ya creados en el sistema. Estos usuarios son "admin" y "administrator". Activar y asignar contraseñas a estos usuarios es crucial para asegurar el acceso y la administración efectiva del dominio y sus recursos.

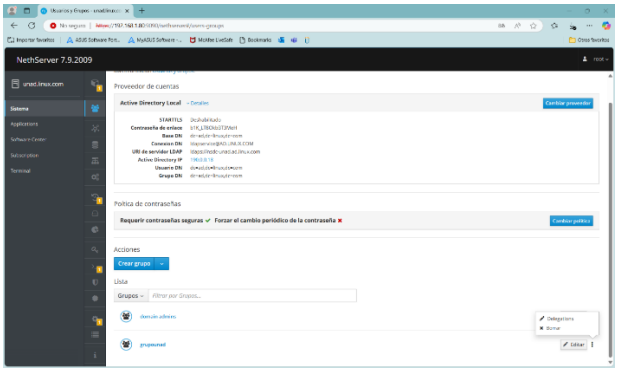
Figura 17. Configuración de usuarios del controlador de dominio



Fuente. Autoría Propia

En la siguiente interfaz, una vez que el dominio y el Controlador de Dominio han sido configurados correctamente, se crea el grupo "grupounad" y se asignan los usuarios ya creados "admin" y "administrator". En este punto observamos que el directorio activo ya está configurado con dirección ip y dominio, grupos y usuarios.

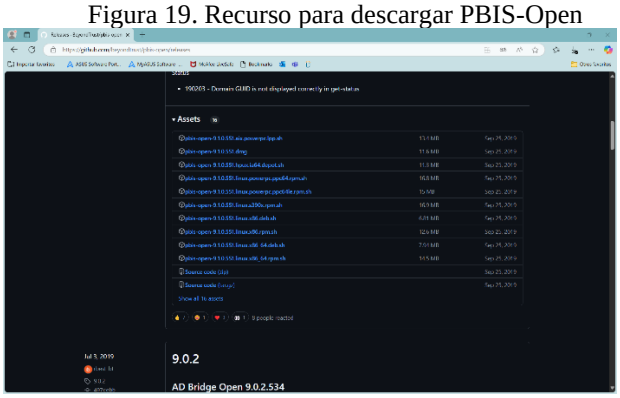
Figura 18. Configuración de grupos del controlador de dominio



Fuente. Autoría Propia

Para conectar una máquina virtual con el directorio activo, es necesario utilizar la herramienta PBIS-Open (BeyondTrust AD Bridge Open), la cual se encuentra disponible para descargar en https://github.com/beyondtrust/pbis-open/releases. Esta herramienta permite integrar Active Directory con sistemas Unix y Linux, facilitando la autenticación y el inicio de sesión único

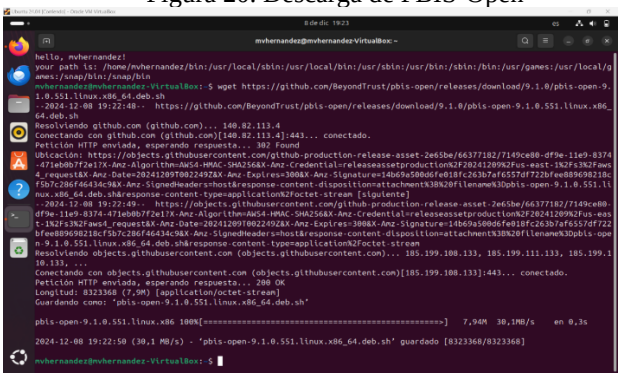
Figura 19. Recurso para descargar PBIS-Open



Fuente. Autoría Propia

Se identifica la versión de PBIS-Open que sea compatible con el sistema operativo donde se va a instalar y se ejecuta el comando wget para descargar el recurso.

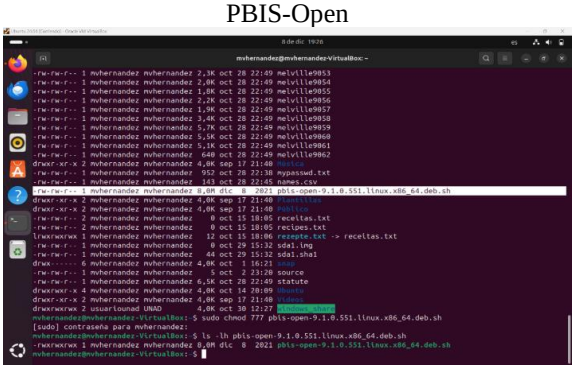
Figura 20. Descarga de PBIS-Open



Fuente. Autoría Propia

Cuando se descarga un archivo, especialmente de una fuente externa como GitHub, es posible que este no tenga los permisos necesarios para ser ejecutado. En la siguiente imagen se evidencia que el archivo efectivamente no tiene permisos de ejecución, por lo que se le asignan los permisos correspondientes por medio del comando chmod -R 777, -R indica que se aplicará recursivamente (en caso de que sea un directorio con subarchivos).

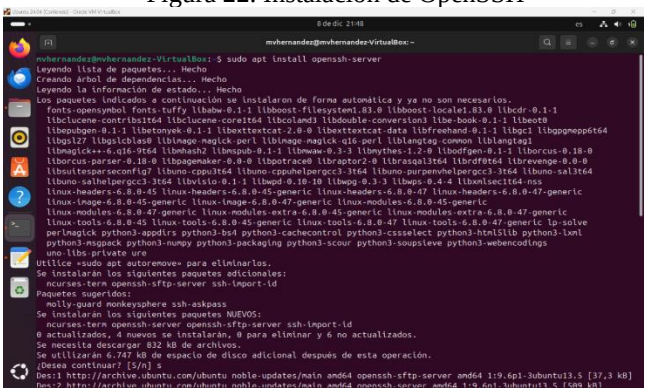
Figura 21. Asignación de permisos de ejecución a PBIS-Open



Fuente. Autoría Propia

Antes de finalizar la instalación de PBIS-Open, se instala OpenSSH, el cual proporciona una forma segura de acceder de manera remota al servidor. Esto se realiza por medio del comando sudo apt install openssh-server, como se evidencia en la siguiente imagen.

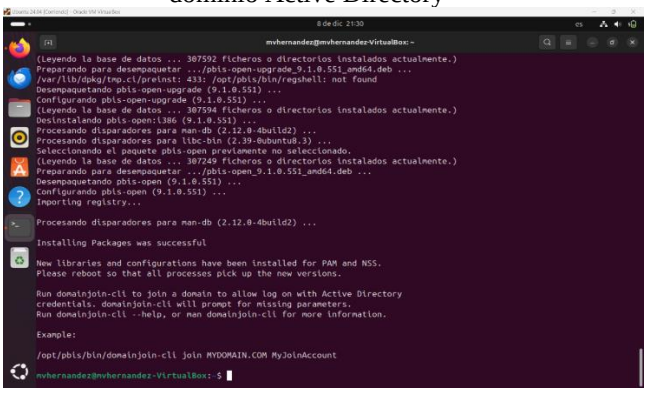
Figura 22. Instalación de OpenSSH



Fuente. Autoría Propia

Una vez instalado PBIS-Open, se procede a utilizar la herramienta para conectar la máquina Linux al dominio Active Directory por medio del comando: sudo /opt/pbis/bin/domainjoin-cli join ad.linux.com administrator

Figura 23. Conexión de la máquina Linux al dominio Active Directory



Fuente. Autoría Propia

Después de unir la máquina al dominio ya hay una configuración funcional que permite a los usuarios del dominio autenticarse y acceder a los recursos de la máquina Linux. Esto facilita la administración centralizada y la integración de sistemas Linux en entornos basados en Active Directory

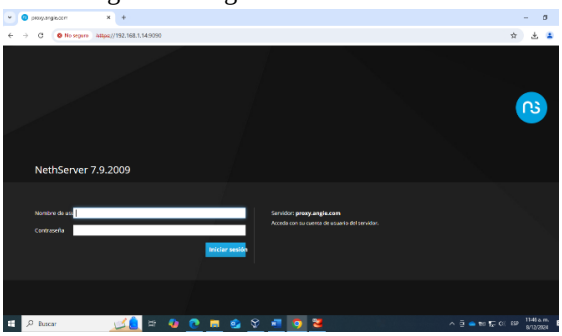
3.2 TEMÁTICA 2: PROXY

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Nethserver a través de un proxy que filtra la salida por medio del puerto 3128.

El uso de un proxy en redes empresariales permite gestionar de manera eficiente el acceso a Internet, ofreciendo capacidades de filtrado, seguridad, y anonimato. En este caso, se implementó un proxy en NethServer para controlar el tráfico generado por una estación GNU/Linux, configurándolo en modo no transparente y aplicando políticas específicas para listas negras y blancas. Este enfoque facilita la administración de accesos y mejora la seguridad de la red.

Antes de comenzar, el servidor NethServer debe estar correctamente instalado y configurado dentro de la zona DMZ. Esto asegura una separación de las redes internas y externas, minimizando riesgos de seguridad. Una vez en funcionamiento, se accede al servidor desde un navegador, utilizando la dirección IP de la red LAN y el puerto 9090.

Figura 24. Ingreso a consola

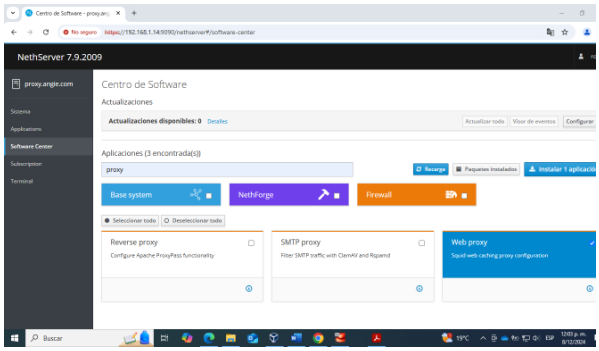


Fuente. Autoría Propia

Después de ingresar y realizar las configuraciones iniciales de NethServer, en el apartado de Software Center se seleccionan los paquetes necesarios para la actividad:

- Web proxy

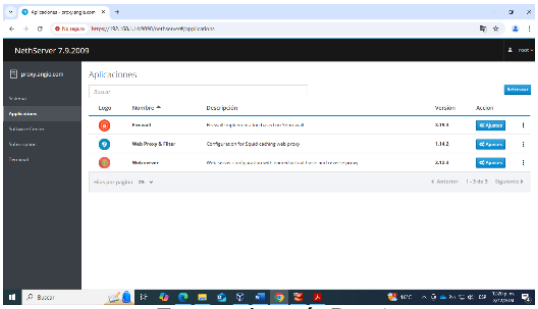
Figura 25. Instalación de aplicaciones



Fuente. Autoría Propia

Una vez instalados, estos módulos se visualizan en la sección de Applications

Figura 26. Aplicaciones instaladas

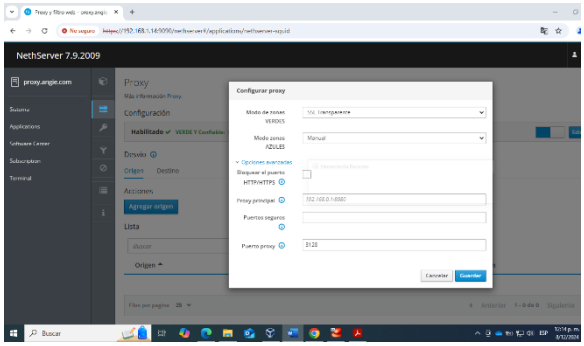


Fuente. Autoría Propia

El primer paso en la configuración del proxy fue habilitar el servicio y configurarlo en modo no transparente, estableciendo el puerto 3128 para el

tráfico HTTP/HTTPS. Este modo requiere que las estaciones cliente configuren manualmente el uso del proxy, lo que proporciona mayor control sobre las conexiones.

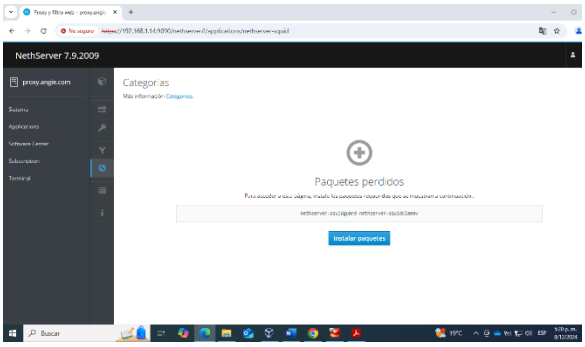
Figura 27. Activación de proxy



Fuente. Autoría Propia

En la configuración del proxy en el módulo de categorías del proxy, se activaron los paquetes predefinidos de páginas web agrupadas por temas. Estas categorías permiten simplificar la configuración del filtrado, al aplicar reglas específicas según los criterios establecidos.

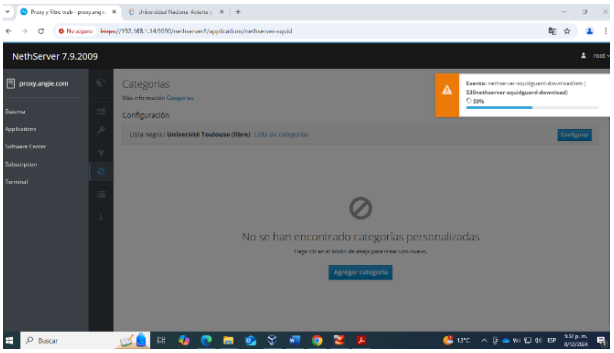
Figura 28. Instalación de Categorías



Fuente. Autoría Propia

Se utilizó la categoría por defecto "Université Toulouse (libre)", que agrupa un conjunto de páginas web para filtrar contenido automáticamente.

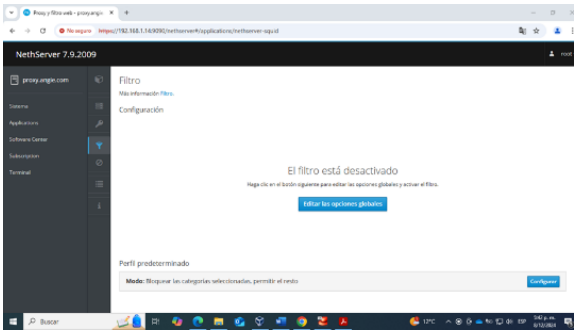
Figura 29. Instalación de Categorías



Fuente. Autoría Propia

Se dejó activado el perfil predeterminado, que bloquea las categorías seleccionadas y permite el acceso al resto del contenido.

Figura 30. Perfil Categorías



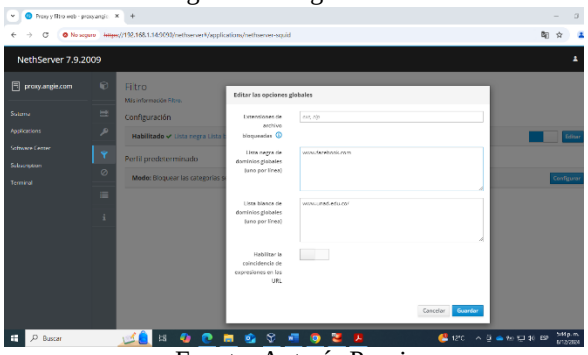
Fuente. Autoría Propia

Para la configuración de las reglas de filtrado se ingresan al módulo de filtros y se añadieron dos reglas específicas:

- Lista negra: Bloqueo del acceso a la página www.facebook.com, que representa una política para restringir el uso de redes sociales.

- Lista blanca: Permiso para acceder a la página www.unad.edu.co, asegurando que los usuarios puedan consultar contenido académico.

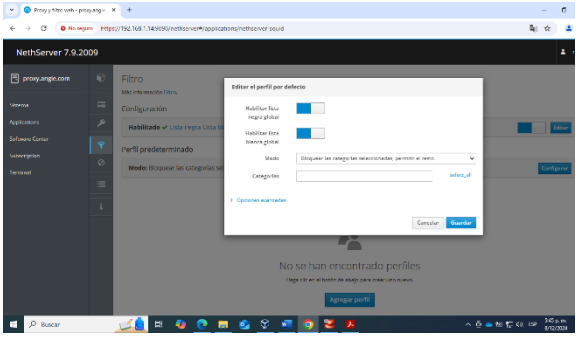
Figura 31. Reglas de Filtrado



Fuente. Autoría Propia

Posteriormente, se verificó que ambas listas estuvieran habilitadas correctamente en el perfil predeterminado del proxy.

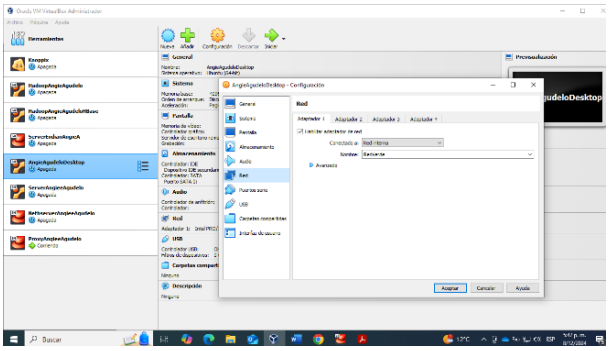
Figura 32. Perfil de filtrado



Fuente. Autoría Propia

Para verificar el funcionamiento correcto del proxy se ingresa a otra maquina la cual se encuentra configurada a la red interna “verde” de tal forma se garantiza que esté relacionada a la misma red del servidor.

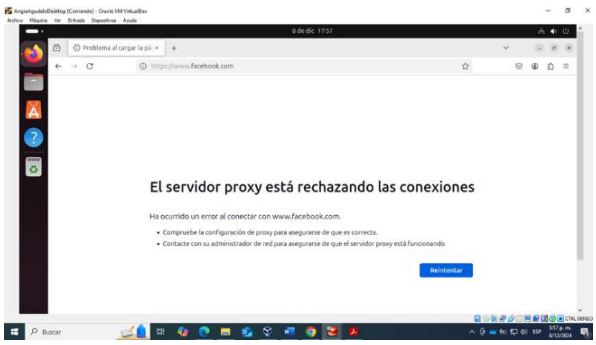
Figura 33. Configuración Máquina Virtual



Fuente. Autoría Propia

Se intentó acceder a la página registrada en la lista negra (www.facebook.com), confirmando que el acceso fue bloqueado por las políticas del proxy.

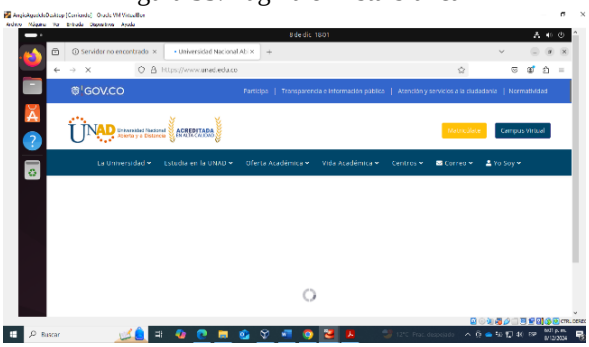
Figura 34. Página en lista negra



Fuente. Autoría Propia

Se intentó acceder a la página registrada en la lista blanca (www.unad.edu.co), verificando que el acceso fue permitido sin restricciones.

Figura 35. Página en lista blanca



Fuente. Autoría Propia

El proxy configurado en NethServer gestionó eficazmente el tráfico de la estación GNU/Linux conectada a la red interna verde. Las pruebas demostraron que las políticas de acceso definidas se aplicaron correctamente, bloqueando el contenido no autorizado y permitiendo el acceso a servicios específicos. Esto valida la utilidad de NethServer como una solución robusta para la gestión de proxies en entornos empresariales.

5.4 TEMÁTICA 3: 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

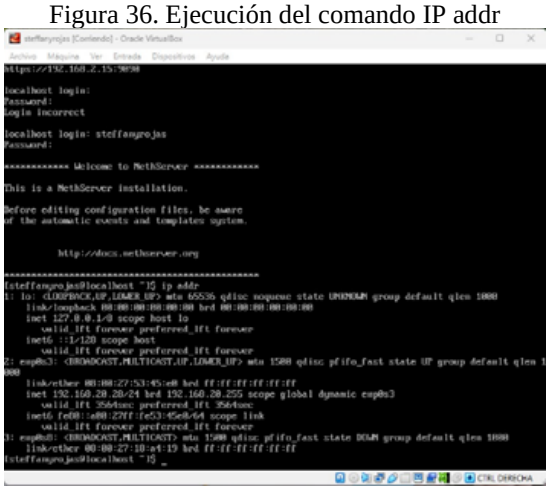
restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

1. Configuración del cortafuegos.

Posteriormente a la instalación, utilizaremos una máquina virtual con el GNU Linux Ubuntu para ejecutar el portal de firewall de Nethserver y probar su efectividad.

a. Se ejecutó el comando ip addr para desplegar las configuraciones de IP address y poder accederlo desde la máquina virtual de Ubuntu.

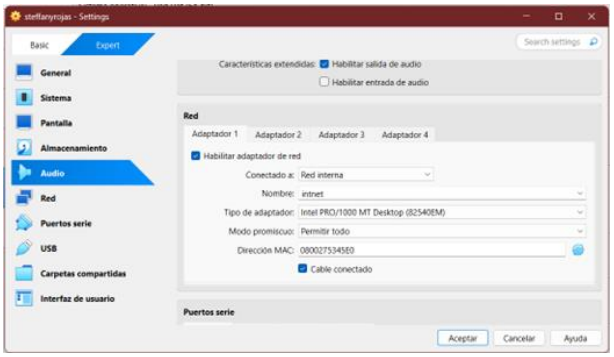
Figura 36. Ejecución del comando IP addr



Fuente. Autoría Propia

b. Una vez se halla localizado la dirección IP, se procederá a abrir la página de configuración en la máquina virtual Ubuntu. Como parte importante de la conexión de este firewall, el acceso a internet va a venir solamente de el cortafuegos, de forma que la máquina virtual solo debe tener configurada la red interna que le permita conectarse a la máquina virtual que ejecuta Nethserver.

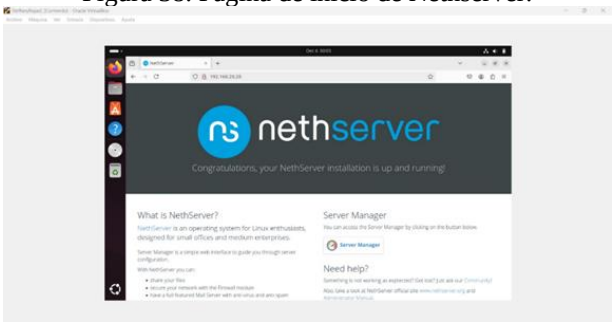
Figura 37. Configuración de red en máquina virtual de Ubuntu.



Fuente. Autoría Propia

c. Una vez las redes internas sean configuradas de manera satisfactoria, abriremos Firefox o el navegador instalado en la máquina virtual Ubuntu y accederemos a la dirección IP configurada en la red interna de conexión entre Ubuntu y Nethserver.

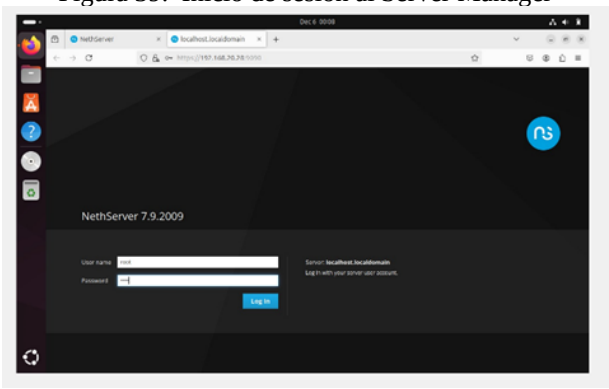
Figura 38. Página de inicio de Nethserver.



Fuente. Autoría Propia

d. En la página previamente desplegada, abriremos el Server manager, e iniciaremos sesión con la contraseña de root previamente establecida.

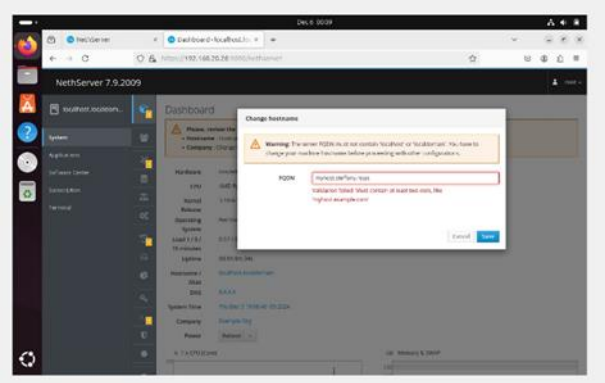
Figura 39. Inicio de sesión al Server Manager



Fuente. Autoría Propia

e. Una vez se despliegue el dashboard de Nethserver, pedirá configurar el hostname, siga los pasos de nueva configuración. En este caso se asignó el hostname: myhost.steffany.rojas.

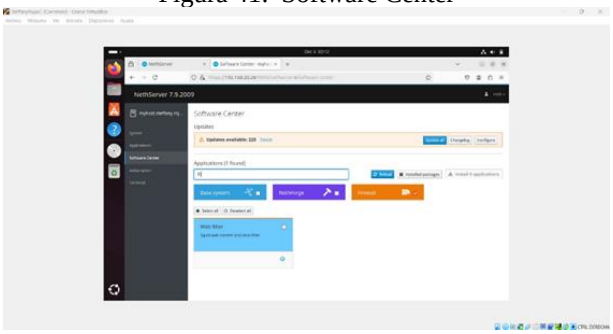
Figura 40. Configuración del Hostname



Fuente. Autoría Propia

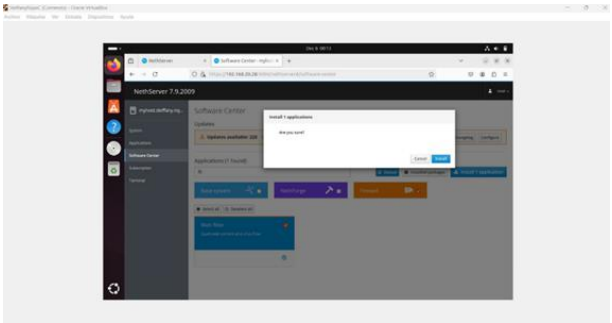
f. Una vez el hostname sea configurado con éxito, se desplegó el software center y se realizó la instalación de la aplicación Web filter.

Figura 41. Software Center



Fuente. Autoría Propia

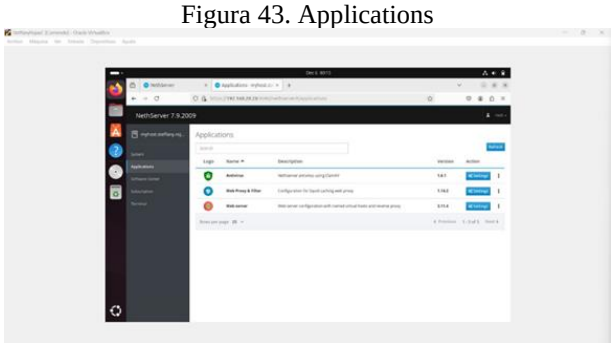
Figura 42. Confirmación para la instalación del web filter



Fuente. Autoría Propia

g. Ahora desplegaremos la sección de applications y abriremos las configuraciones de Web Proxy & Filter.

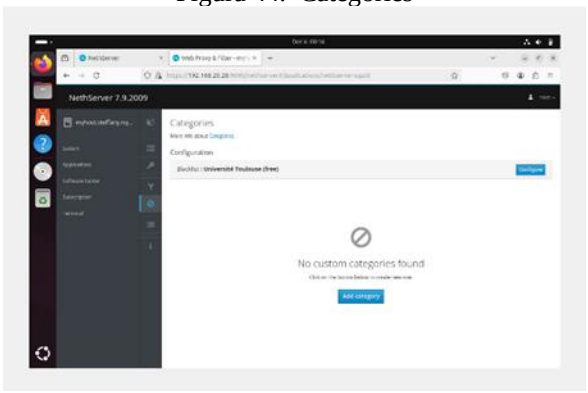
Figura 43. Applications



Fuente. Autoría Propia

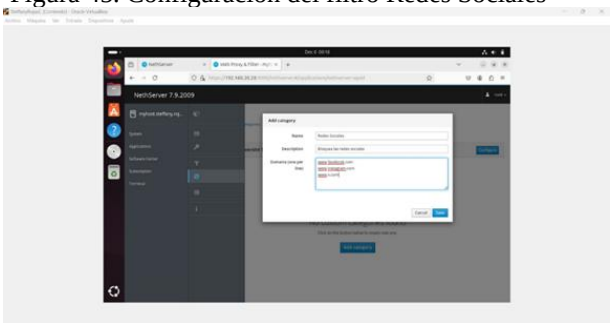
h. Una vez las configuraciones se desplegaron, se accedió a las categorías y se agregaron las secciones de redes sociales y de entretenimiento.

Figura 44. Categories



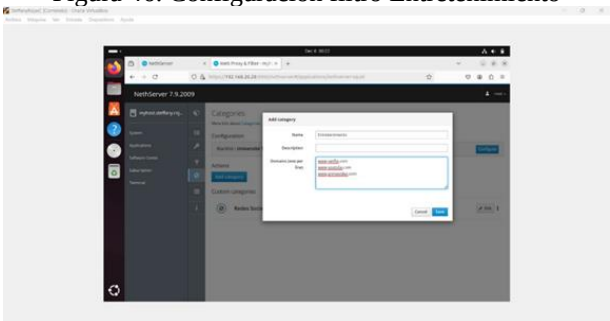
Fuente. Autoría Propia

Figura 45. Configuración del filtro Redes Sociales



Fuente. Autoría Propia

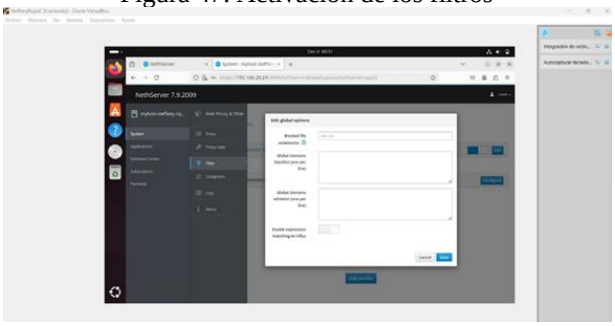
Figura 46. Configuración filtro Entretenimiento



Fuente. Autoría Propia

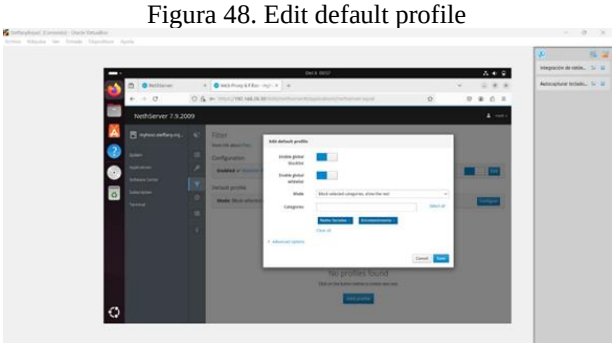
i. Posteriormente se hizo la activación de los filtros para que el cortafuegos empezara con su bloqueo a los sitios web agregados a las categorías previamente agregadas.

Figura 47. Activación de los filtros



Fuente. Autoría Propia

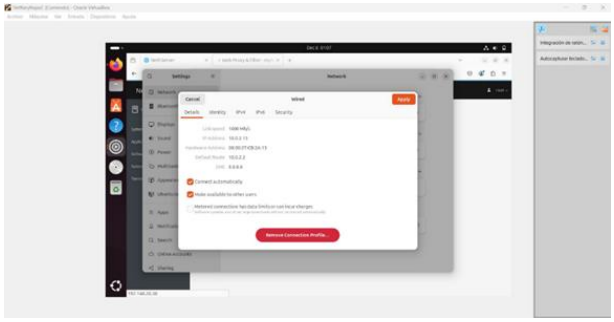
Figura 48. Edit default profile



Fuente. Autoría Propia

j. Finalmente, se hace la configuración del DNS a 8.8.8.8 que es conectado con el firewall, para asegurar que la conexión va a darse a través del cortafuegos.

Figura 49. configuración de DNS en máquina virtual Ubuntu



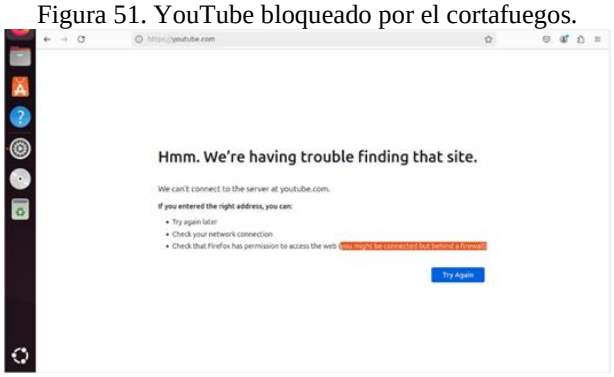
Fuente. Autoría Propia

k. Las pruebas con algunas páginas configuradas en el cortafuegos se pueden evidenciar a continuación.

Figura 50. Facebook bloqueado por el cortafuegos.

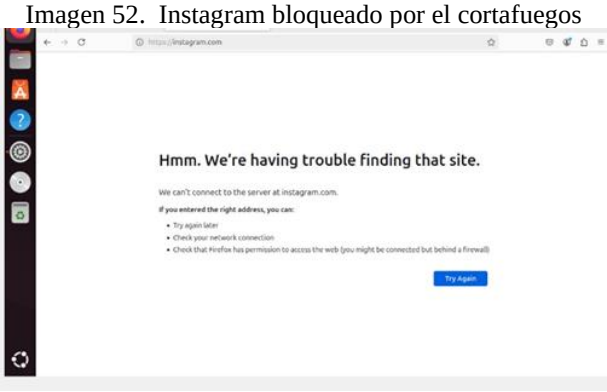
Fuente. Autoría Propia

Figura 51. YouTube bloqueado por el cortafuegos.



Fuente. Autoría Propia

Imagen 52. Instagram bloqueado por el cortafuegos



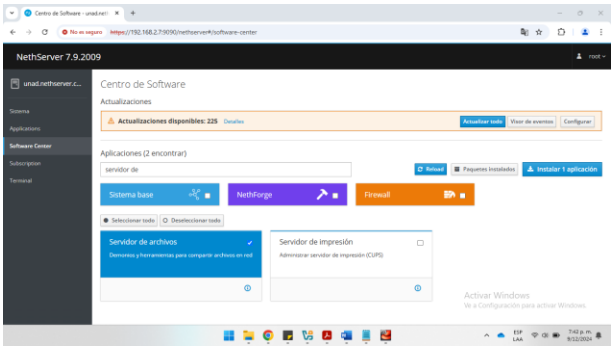
Fuente. Autoría Propia

5.5 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: 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

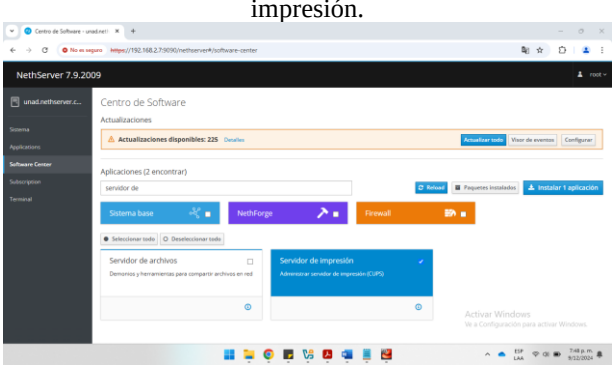
Para el inicio de esta temática daremos con el paso de descargar los paquetes requeridos en el servidor esto por medio de NethServer desde la opción de Software Center

Figura 53. Descarga del paquete de servidor de archivos.



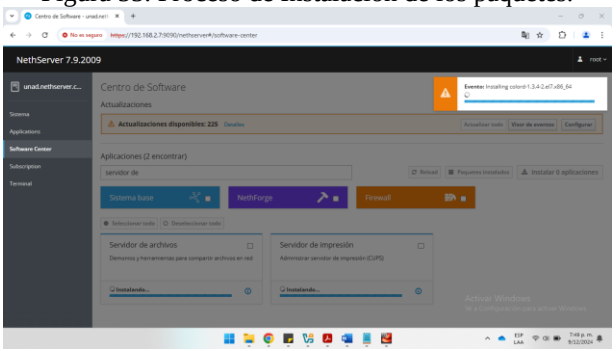
Fuente: Autoría Propia

Figura 54. Descarga del paquete de servidor de impresión.



Fuente: Autoría Propia

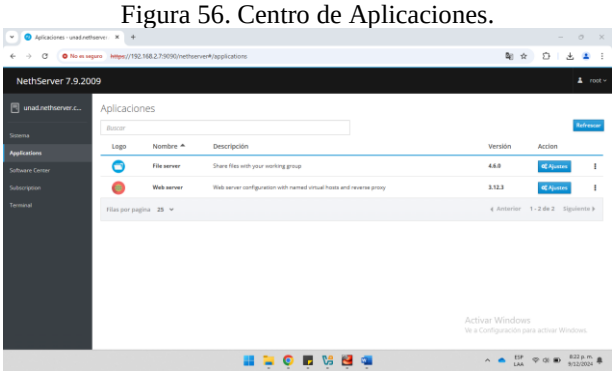
Figura 55. Proceso de Instalación de los paquetes.



Fuente: Autoría Propia

Ingresamos al centro de aplicaciones y seleccionamos configurar Filer Server:

Figura 56. Centro de Aplicaciones.



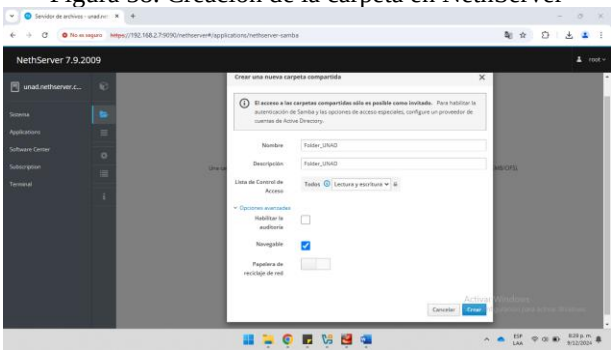
Fuente: Autoría Propia

Ingresamos en la aplicación de FileServer para dar con la creación de la carpeta compartida

Figura 57. Configuración carpeta compartida.

Fuente: Autoría Propia

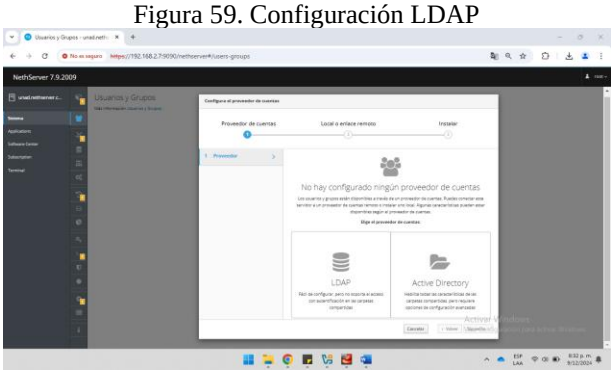
Figura 58. Creación de la carpeta en NethServer



Fuente: Autoría Propia

Para que las carpetas compartidas puedan ser visualizadas desde los usuarios conectados a la red LAN, debemos configurar el controlador de dominio LDAP, pasos que se desarrollan ingresando en los ajustes de la aplicación:

Figura 59. Configuración LDAP



Fuente: Autoría Propia

Figura 60. Configuración de Dominio LDAP remoto

Fuente: Autoría Propia

Ingresamos a él Desktop de Linux una vez terminada la configuración, esto para proceder con la conexión de la carpeta compartida

Figura 61. VM Ubuntu Desktop

Fuente: Autoría Propia

Procedemos con la conexión del folder compartido por medio del FileServer de NethServer

Figura 61. Conexión de Folder

Fuente: Autoría Propia

Procedemos con la validación de la explosión de las impresoras, desde el print$

Figura 63. Conexión de Folder

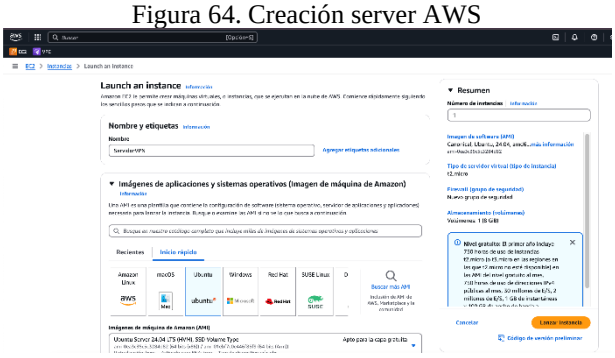
Fuente: Autoría Propia

5.6 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.

Para la realización de esta temática se trabajará en AWS, y con esto se debe crear una instancia de Ubuntu Server 22.04 LTS:

Figura 64. Creación server AWS



Fuente: Autoría Propia

Luego de esto se deben configurar los grupos de seguridad y abrir los puertos necesarios (22 para SSH desde mi IP origen y 1194 para OpenVPN).

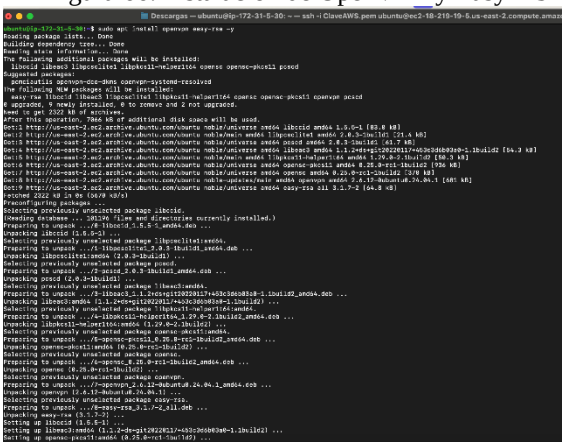
Figura 65. Creación grupos de seguridad AWS

Fuente: Autoría Propia

Seguido de esto se debe instalar OpenVPN en el servidor y Easy-RSA:

OpenVPN es una solución de red privada virtual (VPN) altamente flexible y de código abierto que permite establecer conexiones seguras y cifradas entre dispositivos. Es ampliamente utilizado por su robustez, adaptabilidad y capacidad para operar en diversas plataformas.

Figura 66. Instalación de OpenVPN y Easy-RSA



Fuente: Autoría Propia

Cuando esto se instala, se deben cambiar los parámetros de configuración para que se pueda ir estableciendo adecuadamente la VPN: Cambiar valores como KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, etc.

Figura 67. Edición del archivo vars para definir parámetros básicos

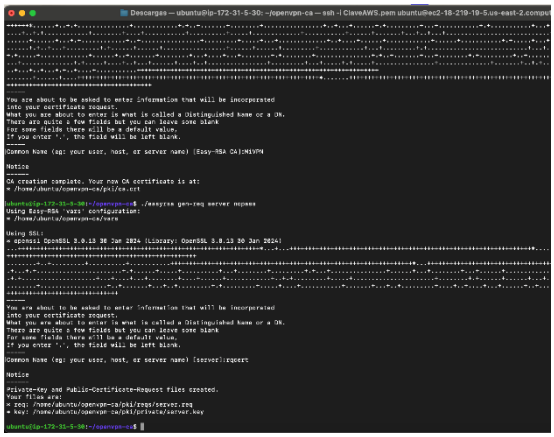
Fuente: Autoría Propia

Teniendo todos estos pasos se deben crear los entornos de Easy-RSA, crear la Autoridad Certificadora (CA), generar los certificados y las claves.

Figura 68. Creación de la autoridad certificadora

Fuente: Autoría Propia

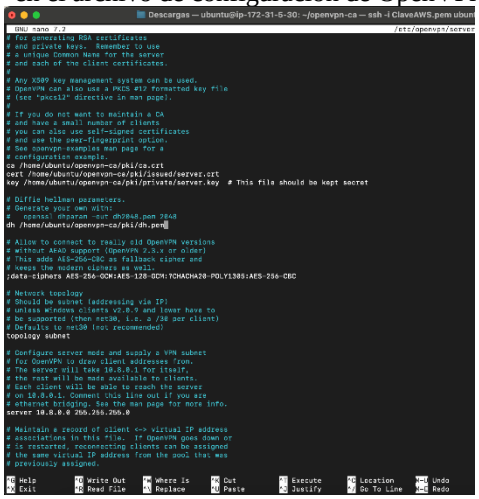
Figura 69. Generación de un certificado para el servidor



Fuente: Autoría Propia

Después de estos pasos tan importantes es necesario configurar el OpenVPN con todas las rutas adecuadas donde se encuentran los certificados y claves, si esto no se realiza no vamos a tener una conexión de VPN exitosa.

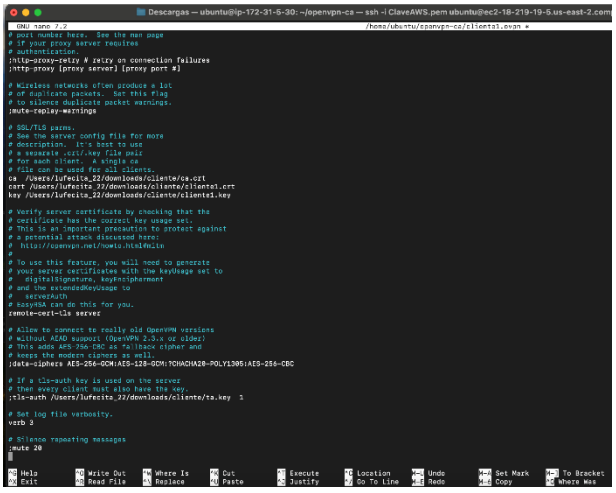
Figura 70. Cambio de las rutas de los certificados en el archivo de configuración de OpenVPN



Fuente: Autoría Propia

Así como se desarrolló la generación de certificados para el servidor AWS, se deben generar para el cliente en este caso un MacOS, donde se deben alojar los archivos para que la conexión site to site sea exitosa:

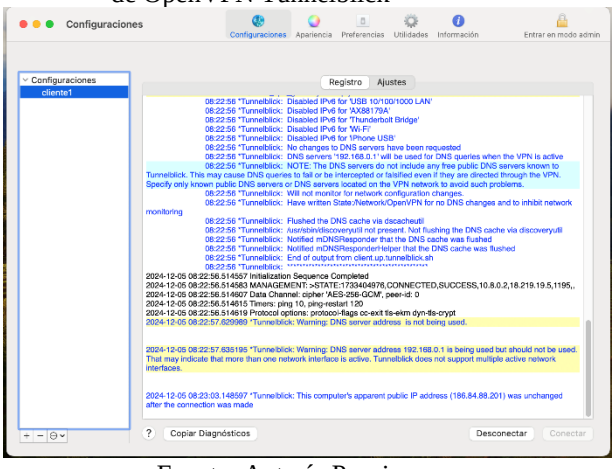
Figura 71. Generación de un certificado para el cliente



Fuente: Autoría Propia

Ya por último se deben realizar las respectivas conexiones y para esto se descarga un cliente OpenVPN Tunnelblick, que va a permitir la conexión de la VPN desde mi MacOS y poder consumir el servicio Apache que se creó allí.

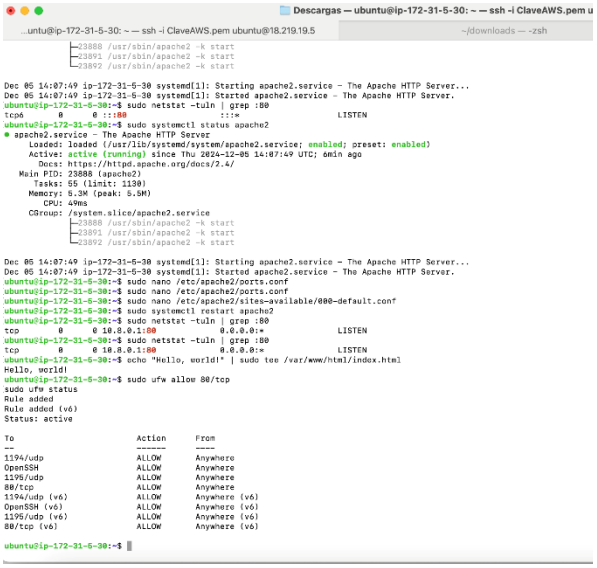
Figura 72. Conexión establecida de la VPN a través de OpenVPN Tunnelblick



Fuente: Autoría Propia

Para la validación se crea un archivo en el index y se verifica el FW. Para confirmar que el puerto 80 este habilitado.

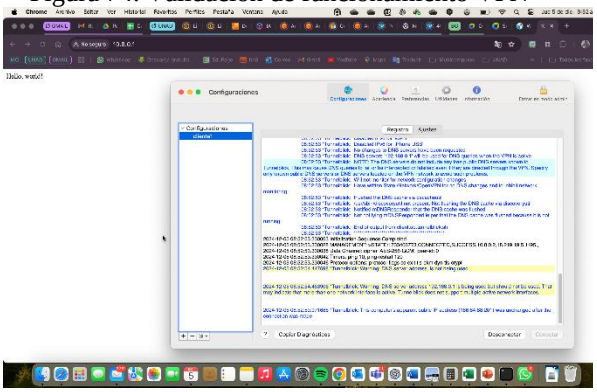
Figura 73. Creación de un archivo en el index y verificación del FW



Fuente: Autoría Propia

Se confirma desde el navegador a la IP asignada donde está expuesto el servicio y se valida que está el mensaje creado para el index “Hello, world”

Figura 74. Validación de funcionamiento VPN



Fuente: Autoría Propia

6 CONCLUSIONES

La implementación de servicios base en NethServer, como los abordados en esta guía, son fundamentales para establecer una infraestructura de TI robusta, segura y eficiente. A través de la configuración de DNS, DHCP y la creación de un Controlador de Dominio, se ha logrado centralizar la gestión de la red y mejorar la seguridad y la operatividad del sistema, también mejora la capacidad de la organización para crecer y adaptarse a nuevas necesidades, posicionando empresas y generando confianza ante los clientes.

La implementación de una VPN permitió establecer un túnel seguro entre una estación de trabajo GNU/Linux y un cliente macOS, demostrando su efectividad para garantizar la integridad y confidencialidad de los datos en redes públicas. Este proyecto resalta la importancia de las VPN como solución clave para el acceso remoto seguro, enfrentando desafíos técnicos que fueron superados mediante ajustes configurativos, consolidando una infraestructura robusta y adaptable a entornos académicos y empresariales.

La configuración de servicios de red con NethServer demuestra su eficiencia y flexibilidad para gestionar recursos en redes locales. Este proyecto permitió reforzar conocimientos prácticos y técnicos en temas como FileServer y PrintServer, destacando el potencial de las herramientas Open Source.

Se puede asegurar que luego de realizar esta configuración la protección de una infraestructura de red limitando el acceso a contenido no deseado es apropiada y eficiente, comprobando que la implementación del cortafuego de software libre es una solución eficiente y efectiva que restringe el acceso a sitios web de entretenimiento y redes sociales dentro de una organización, ya que tiene tiene un gran potencial al ser una solución de costo reducido y alta fiabilidad.

Nethserver, a través de su servicio de proxy, proporciona una gestión eficiente y segura del acceso a internet, permitiendo la implementación de políticas adaptables a diferentes entornos. Su facilidad de configuración y capacidad de filtrado optimizan el uso de recursos tecnológicos, fortaleciendo la seguridad y productividad en la red.

7 REFERENCIAS

[1] *NethServer - https://docs.nethserver.org/es/v7/release_notes.html*

[2] *%20 en%20un%20solo%20dispositivo*

[3] *NethServer.org. (2023). NethServer.org. Obtenido de https://docs.nethserver.org/en/v7/dhcp.html#dhcp-configuration*

[4] *NethServer.org. (2023). NethServer.org. Obtenido de https://docs.nethserver.org/en/v7/dns.html*

[5] *OpenVPN Technologies Inc. (n.d.). OpenVPN: Secure networking solutions. Retrieved from https://openvpn.net*

[6] *Oracle. (s.f). Oracle VM VirtualBox [En línea]. Disponible en: https://www.oracle.com/co/virtualization/virtualbox/#:~:text=Oracle%20VM%20VirtualBox%2C%20el%20software,operativos*

[7] “Oracle VirtualBox: User Guide for Release 7.1,” (C) Copyright 2024. https://www.virtualbox.org/manual/

[8] “Firewall y gateway / Cortafuego y Puerta de enlace — NethServer 6.10 Final.” https://docs.nethserver.org/es/v6/firewall.html

[9] https://docs.nethserver.org/es/v7/web_proxy.html