Implementación de cortafuegos y servicios en infraestructura IT con GNU/Linux Nethserver para restringir el acceso a sitios de entretenimiento y redes Sociales

Jhon Jairo Contreras Castillo
Cod: 1.072.259.309
Grupo No. 202338299_1
jjcontrerac@unadvirtual.edu.co

RESUMEN: *En el marco del Diplomado de Profundización en Administración de Sistemas Operativos Open Source con Certificación en Linux, se abordó la temática de cortafuegos en GNU/Linux NethServer. El objetivo fue implementar y configurar un sistema de restricciones para bloquear el acceso a sitios web de entretenimiento y redes sociales, garantizando la seguridad y funcionalidad del sistema operativo. La metodología incluyó la instalación y configuración de servicios esenciales, así como la aplicación de reglas y políticas de cortafuegos desde una estación de trabajo basada en GNU/Linux. Como resultado, se definieron políticas de seguridad efectivas, implementando una zona DMZ y validando el correcto funcionamiento del cortafuegos. Este trabajo demuestra la capacidad del sistema para satisfacer necesidades específicas de infraestructura IT y subraya la importancia de las herramientas Open Source en la administración de redes seguras.*

PALABRAS CLAVE: administración de redes, cortafuegos, GNU/Linux, redes seguras, *restricción de acceso*

1 INTRODUCCIÓN

El presente informe documenta el desarrollo y resultados obtenidos en la configuración y administración de un cortafuegos basado en GNU/Linux NethServer, como parte del Diplomado de Profundización en Administración de Sistemas Operativos Open Source. En este contexto, se seleccionó la temática de cortafuegos, cuyo propósito fue restringir el acceso a sitios web específicos mediante reglas y políticas avanzadas, asegurando un entorno controlado y seguro. La implementación incluyó la definición de una zona DMZ acorde con la red administrable y la validación del funcionamiento del cortafuegos desde una estación de trabajo. Este proyecto refleja la aplicación práctica de conocimientos adquiridos en los pasos anteriores del diplomado, resaltando la importancia de una correcta administración de sistemas Open Source para satisfacer necesidades específicas en infraestructuras IT modernas.

2 DESARROLLO DE LAS ACTIVIDADES

2.1 Instalación y Configuración de NethServer en VirtualBox

Para llevar a cabo la instalación y configuración de NethServer, comencé creando una nueva máquina virtual en VirtualBox y configurando las interfaces de red de acuerdo con los requisitos del proyecto.

2.2 Crear una nueva máquina virtual NethServer

Abrí VirtualBox y seleccioné la opción Nueva

Asigné el nombre **Nethserver Jhon Contreras** y seleccioné los parámetros:

- **Tipo:** Linux.
- **Versión:** Red Hat (64-bit).

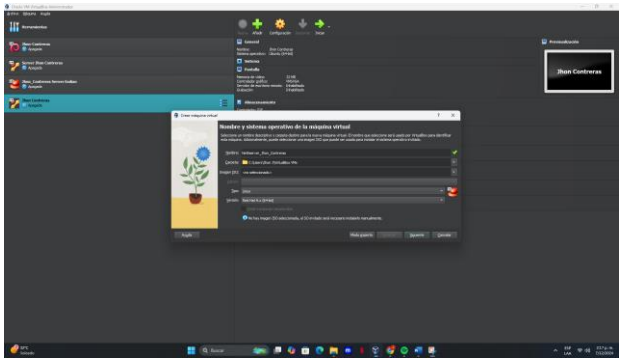

Ilustración 12.2 Creacion de una nueva máquina virtual - Autoría Propia

Se configuro la memoria RAM en 2048 MB y le asigné 2 procesadores para garantizar un rendimiento adecuado.

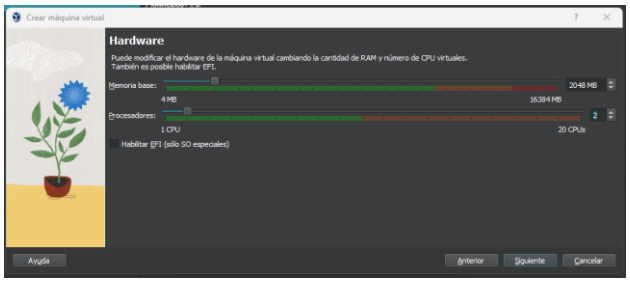

Ilustración 2 Configuración de Ram y Procesador para NethServer - Autoría Propia

Seleccioné la opción de crear un disco duro virtual (VDI) y configuré un tamaño dinámico de 25 GB.

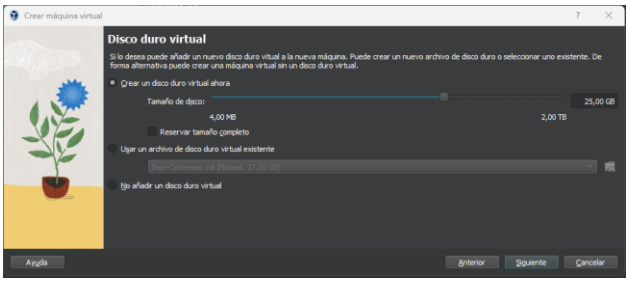

Ilustración 3 Configuración disco duro virtual - Autoría Propia

Luego de haber configurado el tamaño del disco virtual y a ver dado clic en siguiente nos mostrara un resumen de como ha quedado la maquina configurada

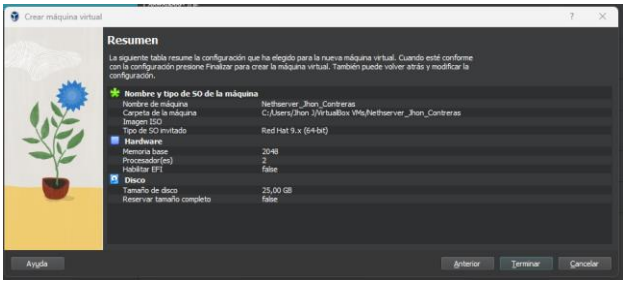

Ilustración 4 Resumen de la configuración realizada - Autoría Propia

2.3 Configuración de la máquina virtual NethServer

Entré en las configuraciones de la máquina virtual recién creada.

Configuré los adaptadores de red:

Adaptador 1 (Adaptador Puente): Este adaptador permite que la máquina tenga acceso a internet. No requiere cambios adicionales.

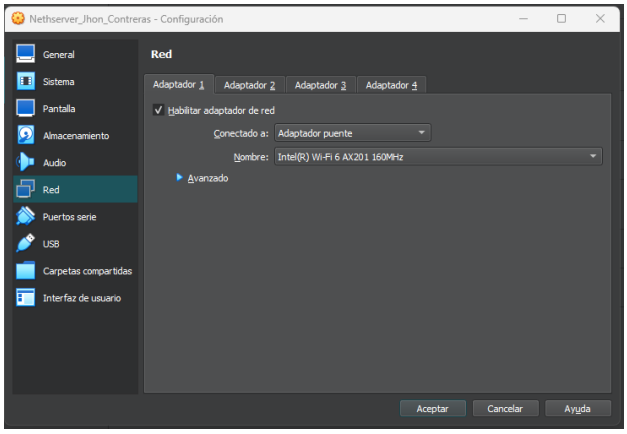

Ilustración 5 Adaptador 1 (Adaptador Puente) - Autoría Propia

Adaptador 2 (Red Interna - LAN Verde): Lo nombré como **Verde** para que sirva como la red de acceso principal a NethServer.

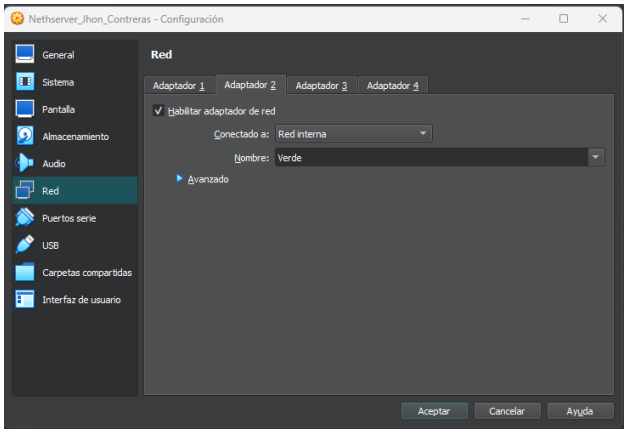

Ilustración 6 Adaptador 2 (Red Interna - LAN Verde) - Autoría Propia

Adaptador 3 (Red Interna - DMZ Naranja): Se nombré como **Naranja** para configurar la zona desmilitarizada.

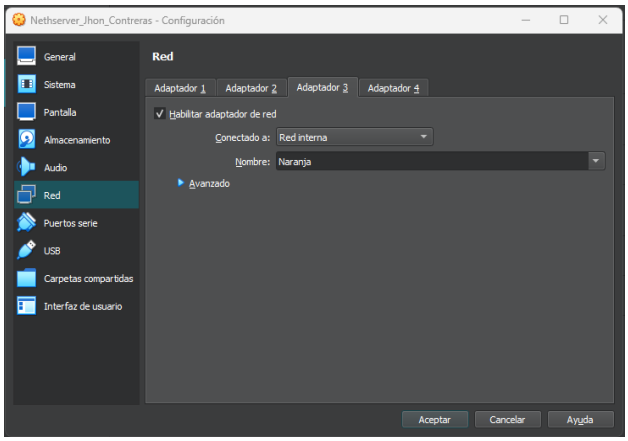

Ilustración 7 Adaptador 3 (Red Interna - DMZ Naranja) Autoría Propia

A continuación se procedió a Agregar la ISO de NethServer

Descargué la ISO oficial de NethServer desde su página web.

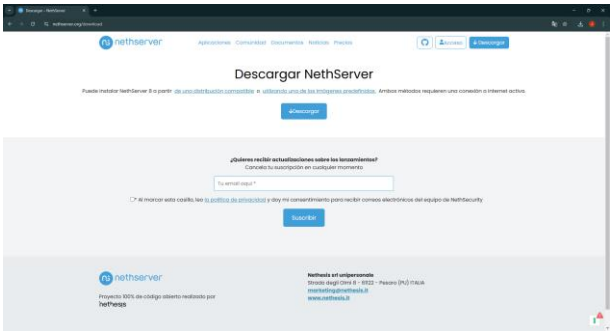

Ilustración 8 Descarga NethServer desde su página web Autoría Propia

En las configuraciones de la máquina virtual, seleccioné la pestaña Almacenamiento y agregué la ISO como disco óptico al controlador.

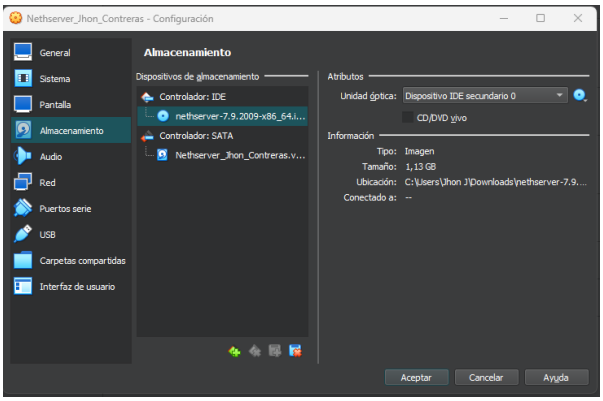

Ilustración 9 ISO como disco - Autoría Propia

2.4 Instalación de NethServer

Después de haber agregado la ISO de NethServer y haber iniciado la máquina virtual, llegué a la pantalla inicial del instalador

En la pantalla inicial, seleccioné la opción NethServer interactive installation y presioné **Enter**.

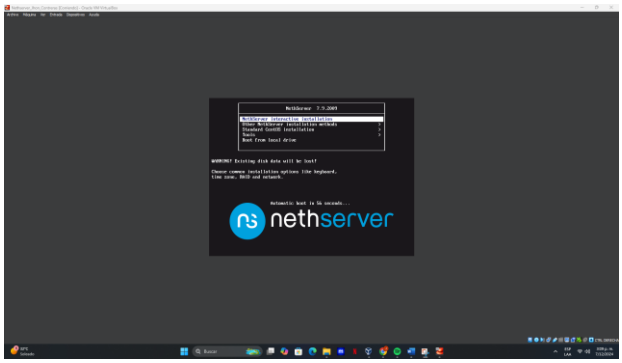

Ilustración 10 Inicio 2.4 Instalación de NethServer - Autoría Propia

2.5 Configuración básica durante la Instalación de NethServer

A continuación el instalador me guio para configurar los siguientes parámetros:

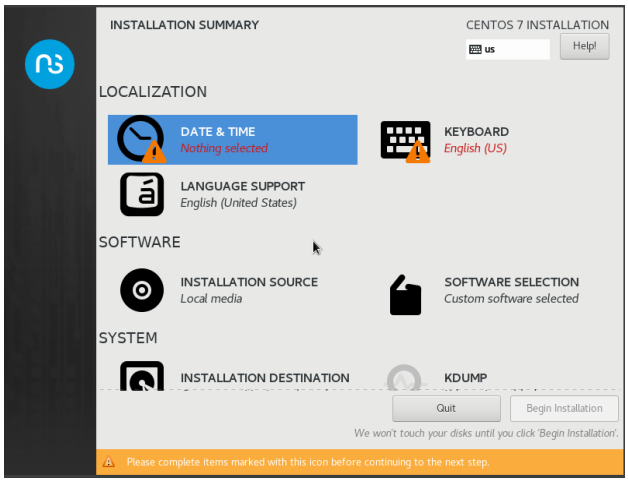

Ilustración 11 2.5 Configuración básica Instalación de NethServer - Autoría Propia

Zona horaria: Elegí la correspondiente a mi ubicación (America/Bogota)

Ilustración 12 Configuración Zona horaria - Autoría Propia

Teclado: Seleccioné es (Español Latin america) para el idioma del teclado.

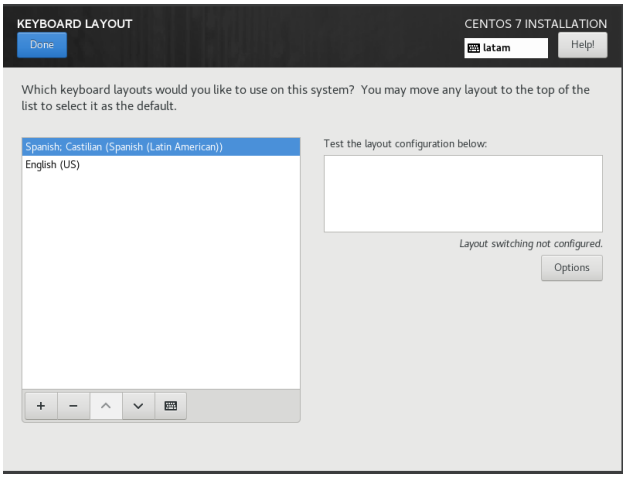

Ilustración 13 Configuración Teclado - Autoría Propia

Idioma: Seleccioné es (Español - Colombia) para el idioma del NethServer.

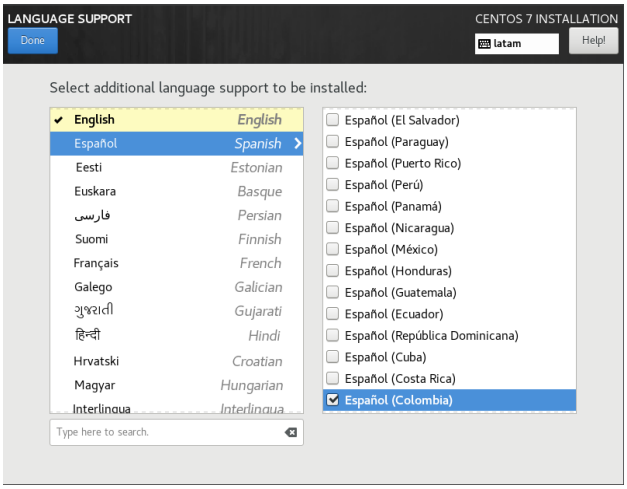

Ilustración 14 Configuración Idioma - Autoría Propia

2.6 Configuración de las interfaces de red NethServer

A continuación, se procedió a configurar las interfaces de red y el nombre del host durante la instalación de NethServer. Esta configuración es fundamental para establecer la conectividad y asignar las zonas correspondientes (WAN, LAN y DMZ) que utilizaré en la implementación del cortafuegos.

Configuración de la interfaz enp0s3 (Red WAN)

La interfaz enp0s3 quedó configurada automáticamente como la red WAN (por defecto). Esta interfaz proporcionará acceso a Internet y fue preconfigurada con los siguientes parámetros:

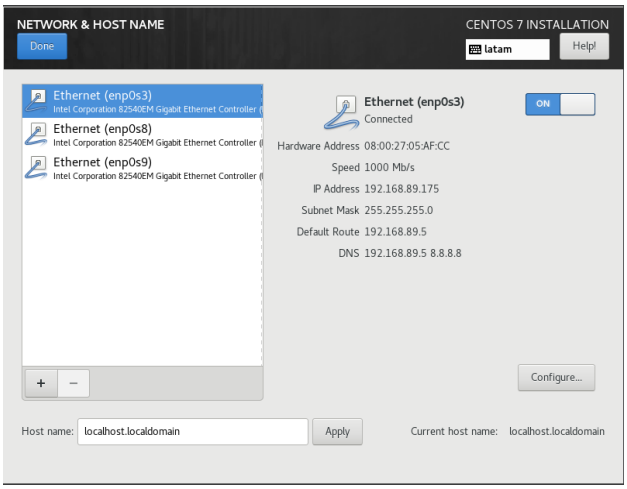

Ilustración 15 Configuración de la interfaz enp0s3 (Red WAN - Adaptador Puente) - Autoría Propia

- **IP Address:** 192.168.89.175.
- **Subnet Mask:** 255.255.255.0.
- **Default Route:** 192.168.89.5 (puerta de enlace para la conexión externa).
- **DNS:** 192.168.89.5, 8.8.8.8

No se realizaron cambios en esta interfaz, ya que cumple su propósito como red externa.

Configuración de la interfaz enp0s8 (Red LAN)

La interfaz **enp0s8** fue asignada manualmente como la red **LAN**, encargada de gestionar la comunicación interna entre los dispositivos de la red local. Sus parámetros fueron configurados de la siguiente manera:

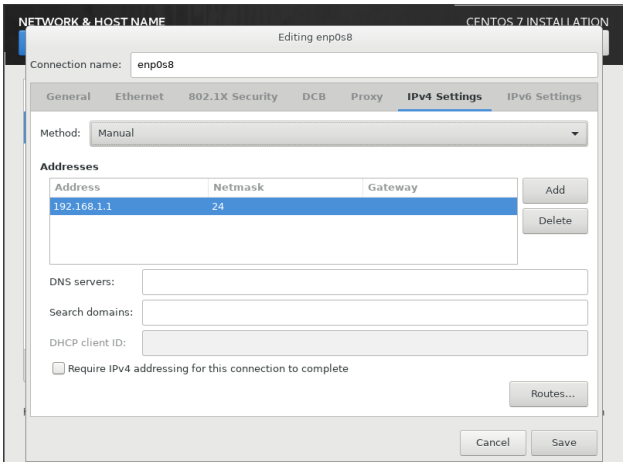

Ilustración 16 Configuración de la interfaz enp0s8 (Red Interna - LAN Verde) - Autoría Propia

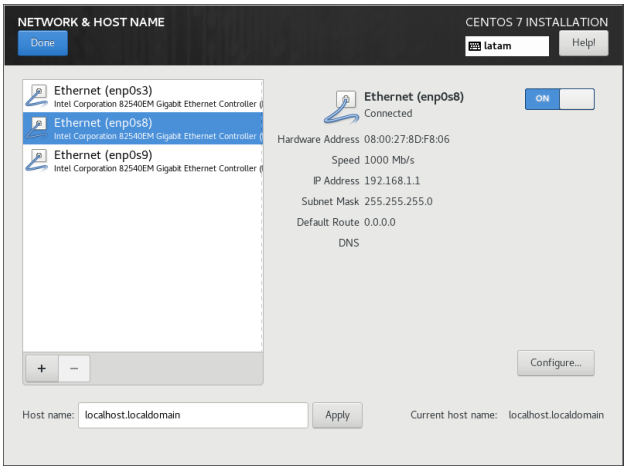

Ilustración 17 Configuración de la interfaz enp0s8 (Red Interna - LAN Verde) - Autoría Propia

- **Dirección IP:** 192.168.1.1
- **Máscara de subred:** 255.255.255.0
- **Puerta de enlace predeterminada:** 0.0.0.0
- **Servidores DNS:** Ninguno

Esta interfaz permite a los dispositivos internos acceder a los servicios proporcionados por el servidor y comunicarse de manera segura dentro de la red local.

Configuración de la interfaz enp0s9 (Red Interna - DMZ Naranja)

La interfaz **enp0s9** fue configurada como la red **DMZ**, destinada a alojar servicios públicos como servidores web, servidores FTP u otros recursos expuestos a Internet. Su configuración es la siguiente:

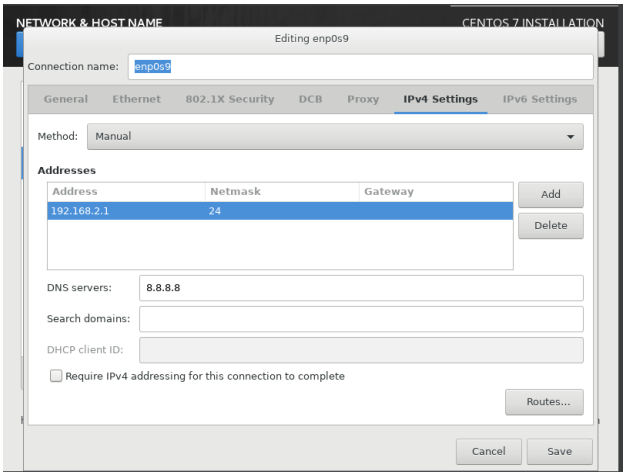

Ilustración 18 Configuración de la interfaz enp0s9 - Autoría Propia

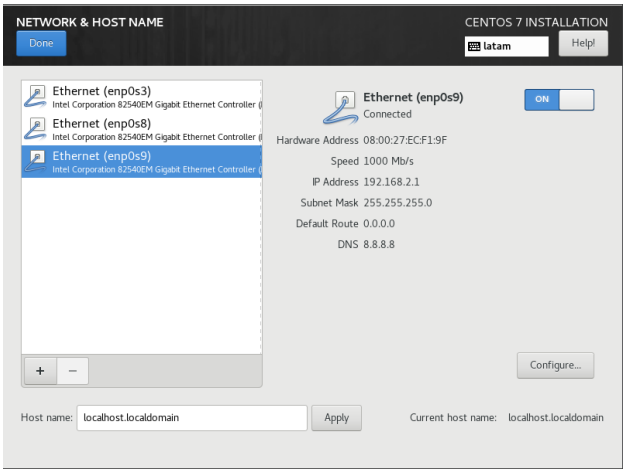

Ilustración 19 Ilustración 18 Configuración de la interfaz enp0s9 (red DMZ Naranja) - Autoría Propia

- **Dirección IP:** 192.168.2.1
- **Máscara de subred:** 255.255.255.0
- **Puerta de enlace predeterminada:** 0.0.0.0
- **Servidores DNS:** 8.8.8.8

Esta configuración asegura que los servicios públicos permanezcan aislados de la red interna, garantizando así un mayor nivel de seguridad.

Además, configuré el nombre del host del sistema como jhon.contreras.unad, para personalizar y facilitar su identificación en la red. Este nombre sustituirá al predeterminado localhost.localdomain una vez aplicado.

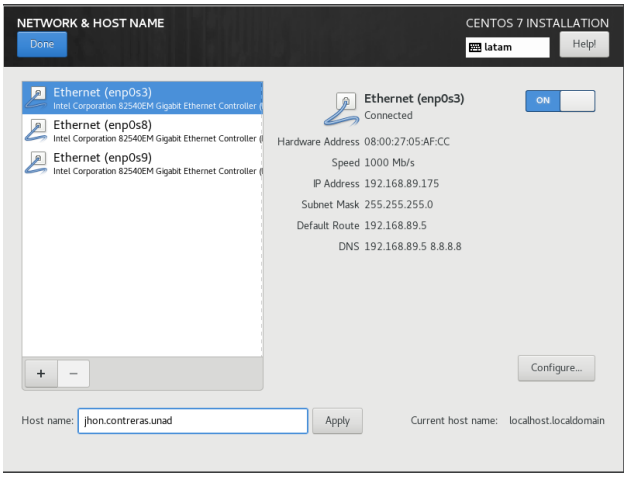

Ilustración 20 Configuración nombre del host del sistema - Autoría Propia

2.7 Configuración Root Password NethServer

En este paso de la instalación de NethServer, el sistema nos está indicando dos configuraciones importantes que debemos completar antes de continuar: como lo son

Contraseña del Root (Root Password): también la Creación de un Usuario

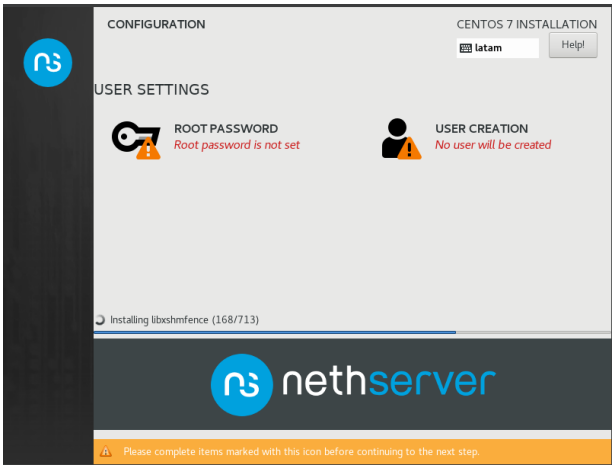

Ilustración 21 Configuración Root Password y Usuario - Autoría Propia

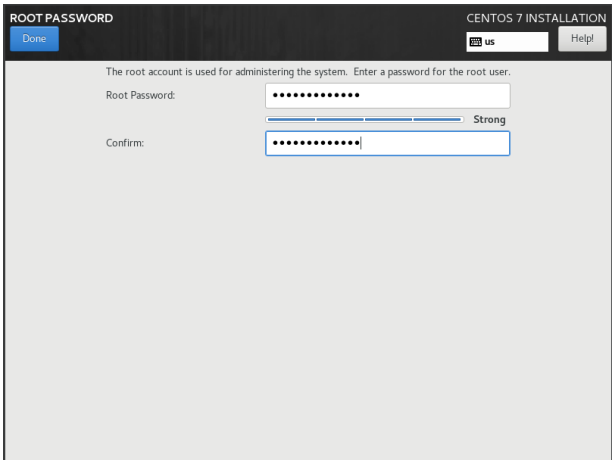

Ilustración 22 Configuración Root Password - Autoría Propia

este paso es crucial para garantizar la seguridad y funcionalidad del sistema. La configuración de la contraseña root es obligatoria, mientras que la creación de un usuario adicional es una buena práctica recomendada. Una vez completadas estas configuraciones, podemos proceder con el resto de la instalación.

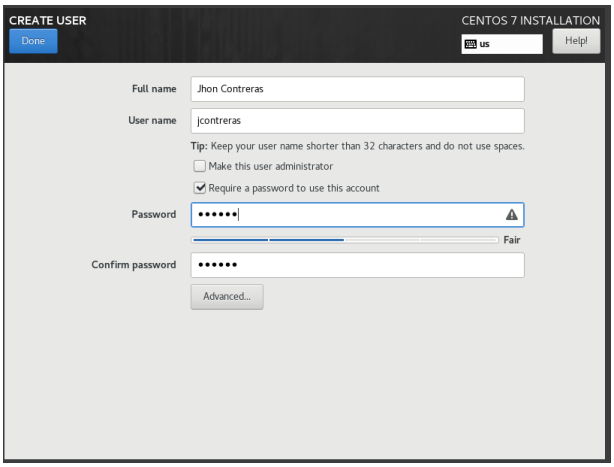

Ilustración 23 Creación de un Usuario Estándar - Autoría Propia

2.8 Verificación de la configuración de red en NethServer

Una vez completada la instalación inicial de NethServer, accedí al sistema para verificar que las configuraciones de red realizadas previamente estuvieran aplicadas correctamente.

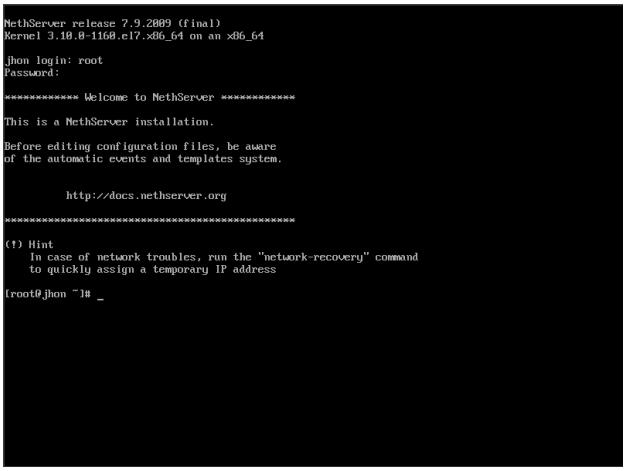

Ilustración 242.7 Verificación de la configuración de red en NethServer - Autoría Propia

Utilicé el comando ip a para listar las interfaces de red y sus configuraciones.

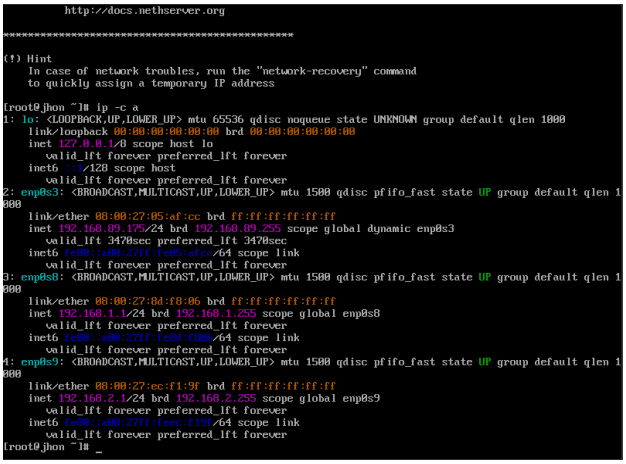

Ilustración 25 2.7 Verificación de la configuración de red en NethServer - Autoría Propia

2.9 Acceso a la configuración de NethServer desde el navegador

Con la configuración de las interfaces de red completa y la conectividad del servidor asegurada, el siguiente paso fue acceder a la interfaz gráfica de administración de NethServer desde un navegador web. Este acceso es esencial para realizar la gestión avanzada del servidor de forma más intuitiva.

abrí el navegador (en mi caso, **Firefox**, aunque puede ser cualquier otro navegador compatible). Este equipo tenía acceso a la interfaz LAN del servidor, cuya dirección IP es **192.168.89.175**. ingresé la siguiente URL: https://192.168.89.175:9090, Es importante especificar el protocolo **HTTPS** y el puerto **9090**, ya que este último es el predeterminado para acceder a la interfaz gráfica de NethServer.

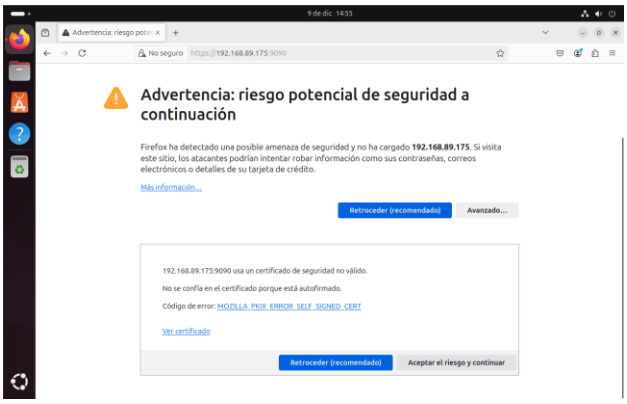

Ilustración 26 Inicio del navegador - Autoría Propia

Como era de esperarse, el navegador mostró un mensaje de advertencia sobre el certificado de seguridad. Esto sucede porque NethServer utiliza un certificado SSL/TLS autogenerado, que no está firmado por una autoridad certificadora reconocida. En el caso de Firefox, apareció el mensaje "Advertencia: Posible riesgo de seguridad". Seleccioné la opción "Avanzado" y luego hice clic en "Aceptar el riesgo y continuar".

Pantalla de inicio de sesión de NethServer

Después de aceptar la advertencia, el navegador me redirigió a la pantalla de inicio de sesión de NethServer. Aquí ingresé las credenciales del administrador, que son las siguientes:

- **Usuario:** root
- **Contraseña:** la definida durante la instalación del servidor.

Este paso asegura que solo personal autorizado pueda acceder al sistema

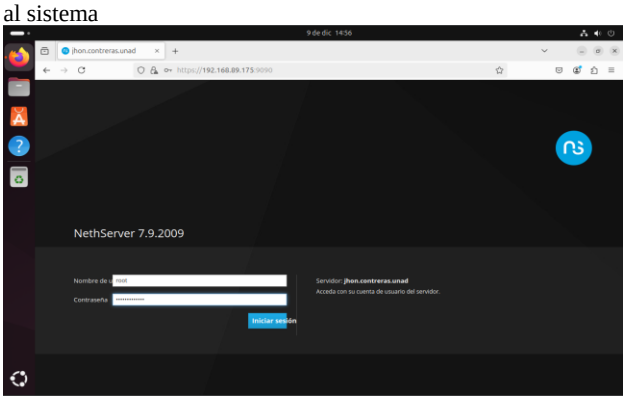

Ilustración 27 Acceso a la interfaz de administración - Autoría Propia

Este paso asegura que solo personal autorizado pueda acceder al sistema.

2.10 Acceso al panel de administración

Al iniciar sesión correctamente, se desplegó el panel principal de administración de NethServer. Este panel está diseñado para facilitar la gestión del servidor, ofreciendo una interfaz amigable para configurar servicios, gestionar usuarios, supervisar el estado del sistema, y mucho más.

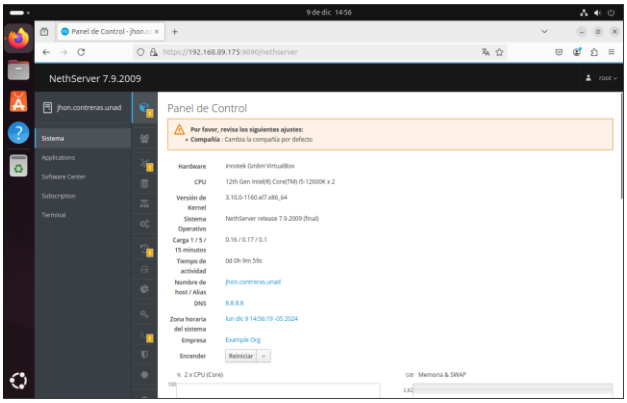

Ilustración 28 Panel de administración - Autoría Propia

Cambio de la compañía por defecto en el sistema

el sistema sugiere realizar algunas configuraciones adicionales para personalizarlo según las necesidades de la organización.

Una de estas configuraciones incluye el cambio de la **compañía por defecto**.

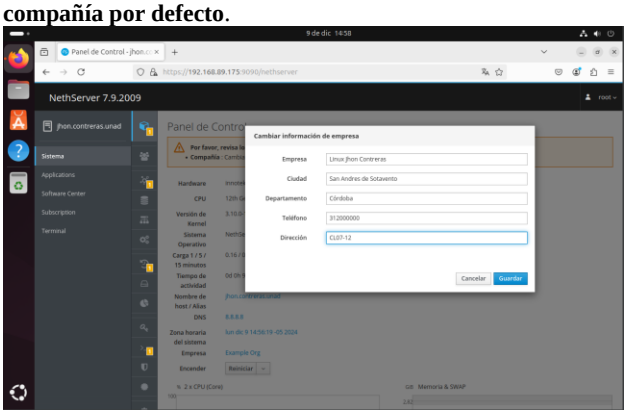

Ilustración 29 Cambio compañía por defecto - Autoría Propia

Después de ingresar los datos de la compañía, hice clic en el botón "Guardar" o "Aplicar". Una vez guardados los cambios, volví a la pantalla principal para confirmar que el nombre de la compañía actualizado aparecía reflejado en las secciones donde se menciona la organización

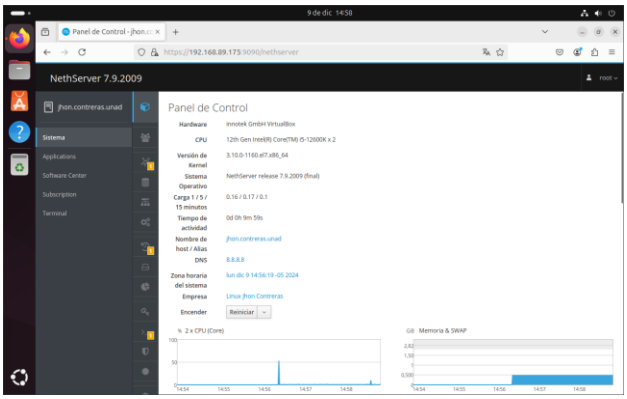

Ilustración 30 nombre de la compañía actualizado - Autoría Propia

2.11 Configuración de las interfaces de red

Una vez que ingresamos al panel de control de NethServer, debemos asegurarnos de que las interfaces de red estén configuradas correctamente para las tres zonas principales que mencionamos: WAN, LAN y DMZ. En este caso, se te solicita configurar IP estática para cada interfaz y se visualizan colores que indican el estado de estas interfaces.

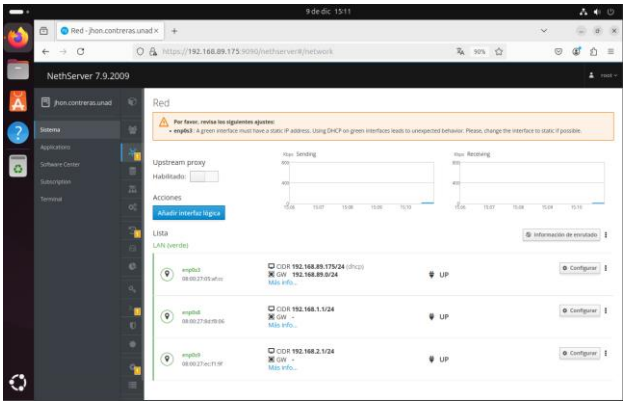

Ilustración 31 2.10 Configuración de las interfaces de red - Autoría Propia

Una vez dentro del panel, navegamos al módulo de configuración de red para identificar las interfaces físicas disponibles. El sistema detectó las siguientes:

- **enp0s3**: Se usará como la interfaz WAN (Roja), para la conexión a Internet.
- **enp0s8**: Se configurará como la interfaz LAN (Verde), para la red interna.
- **enp0s9**: Será utilizada como la interfaz para la DMZ (Naranja), para servicios expuestos a Internet.

Configuración de la interfaz WAN (Roja - enp0s3)

Para configurar cada interfaz, seguimos un proceso sistemático.

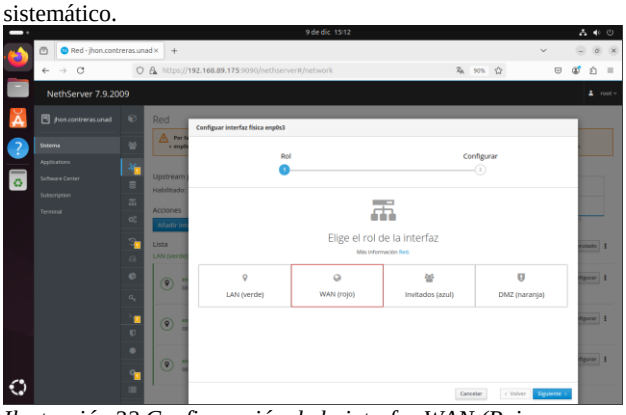

Ilustración 32 Configuración de la interfaz WAN (Roja - enp0s3) - Autoría Propia

Seleccionamos la interfaz enp0s3 en el módulo de red.
La configuramos como Zona Roja (WAN).

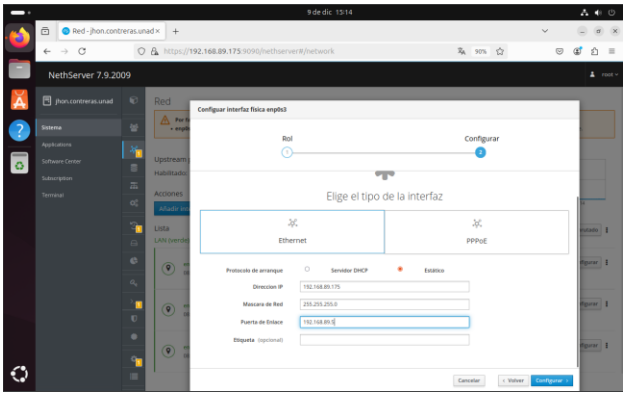

Ilustración 33 Configuración de la interfaz WAN (Roja - enp0s3) - Autoría Propia

Optamos por la obtención de una dirección IP dinámica mediante **DHCP**, proporcionada por el router o ISP. En este caso, con el tipo de interfaz (Ethernet) estático y se asignó automáticamente la IP 192.168.0.197, Mascara de red: 255.255.255.0 y con Puerta de Enlace: 192.168.89.5.

La zona Roja (WAN) representa la conexión a Internet. Usar DHCP es útil para simplificar la configuración inicial y adaptarse automáticamente a la red del proveedor. Este paso asegura que el servidor tenga acceso a recursos externos y pueda gestionar el tráfico entrante y saliente.

Configuración de la interfaz LAN (Verde - enp0s8)

Seleccionamos la interfaz enp0s8 y la configuramos como **Zona Verde (LAN)**.

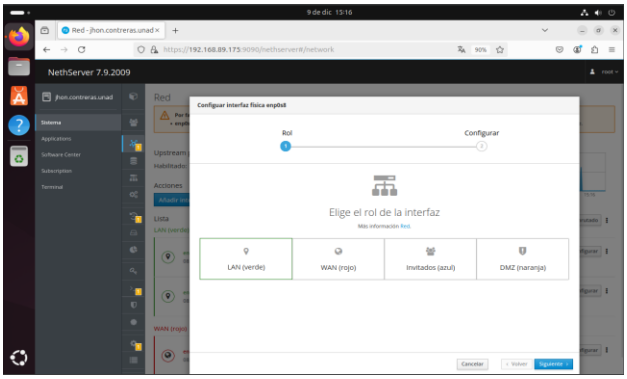

Ilustración 34Configuración de la interfaz LAN (Verde - enp0s8) - Autoría Propia

Asignamos la dirección IP estática 192.168.1.1/24.

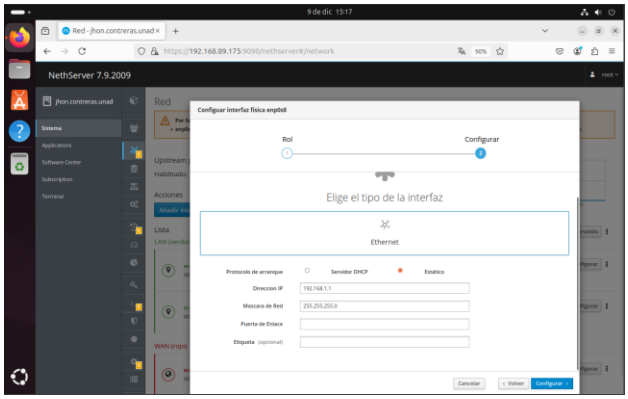

Ilustración 35 Configuración de la interfaz LAN (Verde - enp0s8) - Autoría Propia

La zona Verde (LAN) es esencial para la red interna, ya que conecta a los usuarios locales con el servidor. La dirección IP 192.168.1.1 es una elección estándar, ya que también se utiliza como puerta de enlace para los dispositivos conectados a esta red. Usar una IP estática garantiza la estabilidad y evita conflictos de direccionamiento.

Configuración de la interfaz DMZ (Naranja - enp0s9)

Seleccionamos la interfaz enp0s9 y la configuramos como **Zona Naranja (DMZ)**.

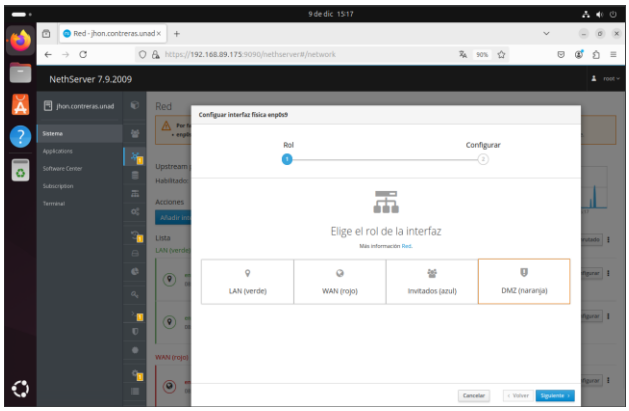

Ilustración 36 Configuración de la interfaz DMZ (Naranja - enp0s9) - Autoría Propia

Asignamos la dirección IP estática 192.168.2.1/24.
Guardamos los cambios.

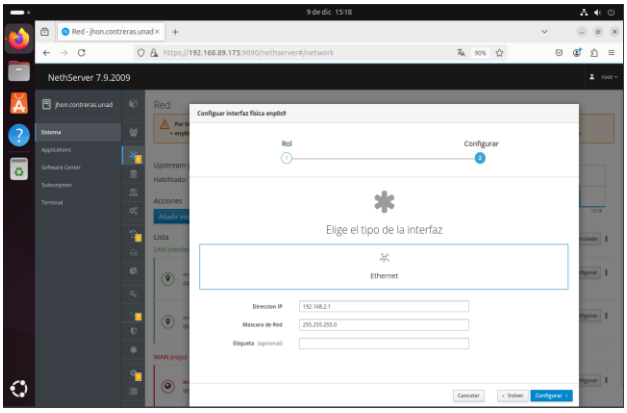

Ilustración 37 Configuración de la interfaz DMZ (Naranja - enp0s9) - Autoría Propia

La zona Naranja (DMZ) está destinada a alojar servicios que deben estar disponibles desde Internet, como servidores web o de correo. Asignar una dirección IP estática permite una gestión precisa de los servicios expuestos y asegura su aislamiento de la red interna (LAN), mejorando la seguridad.

Verificación del estado de las interfaces

Luego de configurar las interfaces, revisamos en el módulo de red que cada una estuviera activa y correctamente asignada:

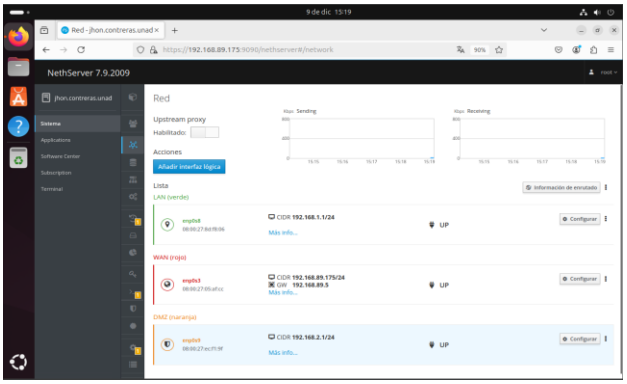

Ilustración 38 Estado de las interfaces - Autoría Propia

- **enp0s3 (Roja - WAN):** Dirección IP dinámica 192.168.0.197, obtenida vía DHCP.
- **enp0s8 (Verde - LAN):** Dirección IP estática 192.168.1.1/24.
- **enp0s9 (Naranja - DMZ):** Dirección IP estática 192.168.2.1/24.

Las interfaces aparecen en estado **UP**, lo que confirma que están funcionando correctamente.

Este paso es crucial para garantizar que las configuraciones se hayan aplicado correctamente.

Acontinuacion se realizan pruebas para validar el funcionamiento de cada interfaz:

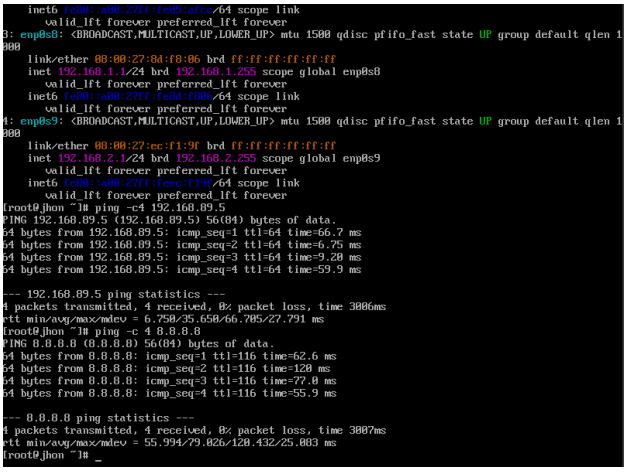

Ilustración 39 Pruebas de conectividad - Autoría Propia

LAN (Verde): Desde un equipo conectado a la red local, confirmamos que era posible acceder al servidor mediante la dirección 192.168.1.1 y que los dispositivos podían comunicarse entre sí.

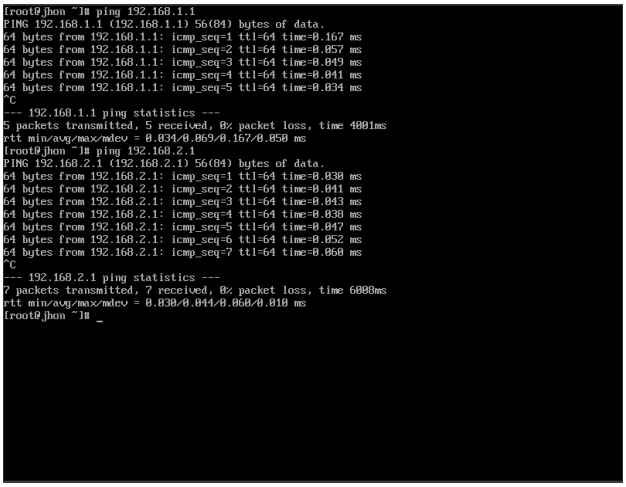

Ilustración 40 Pruebas de conectividad ping - Autoría Propia

2.12 Configuración del apartado de Shell Seguro - SSH en NethServer

En este paso, procedemos a configurar el servicio **SSH (Secure Shell)** en NethServer, lo cual es esencial para garantizar un acceso remoto seguro al servidor.

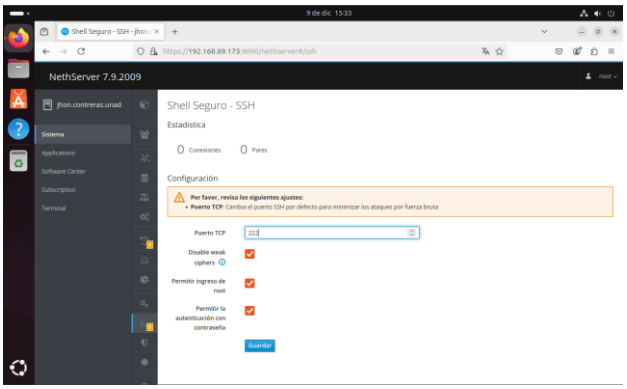

Ilustración 41 2.11 Configuración del apartado de Shell - Autoría Propia

Dentro del apartado de configuración del servicio SSH:

1. Identificamos la opción que define el **puerto TCP** utilizado por el servicio.
2. Reemplazamos el valor actual por el puerto **222**, que es el puerto estándar para conexiones SSH.
3. Guardamos los cambios realizados.

2.13 Configuración de un nuevo registro DNS en NethServer

En este paso, configuramos un nuevo registro DNS en el servidor NethServer. Este registro permitirá resolver el nombre del host contreras.unad a la dirección IP 192.168.1.1, asegurando que los dispositivos de la red interna puedan acceder al servidor utilizando su nombre en lugar de la dirección IP.

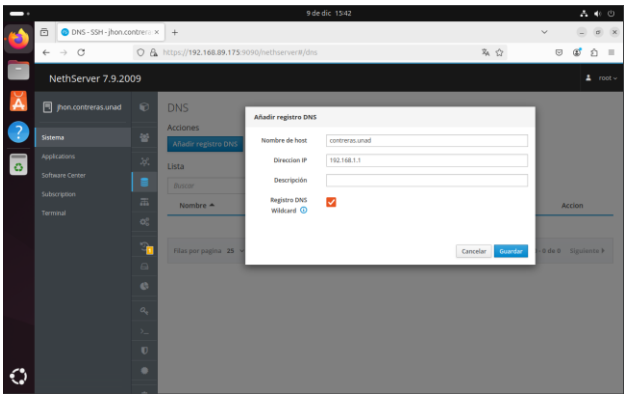

Ilustración 42 2.12 Configuración de un nuevo registro DNS- Autoría Propia

Dentro del módulo DNS, realizamos los siguientes pasos:

1. Hacemos clic en la opción **Añadir Registro DNS**.
2. Completamos los campos requeridos:
   - **Nombre del host:** contreras.jj
   - **Dirección IP:** 192.168.1.1
3. Marcamos la casilla de **Registro DNS** para confirmar que este registro se incluirá en la base de datos DNS gestionada por NethServer.
4. Guardamos los cambios.

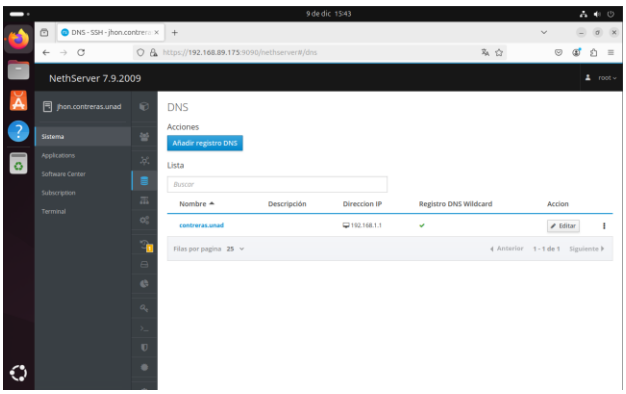

Ilustración 43 nuevo registro DNS en NethServer- Autoría Propia

El registro DNS **contreras.unad** fue configurado correctamente para apuntar a la dirección IP **192.168.1.1**.

2.14 Configuración del servicio DHCP en NethServer

El siguiente paso consiste en habilitar y configurar el servicio DHCP (Protocolo de Configuración Dinámica de Host) en el servidor NethServer

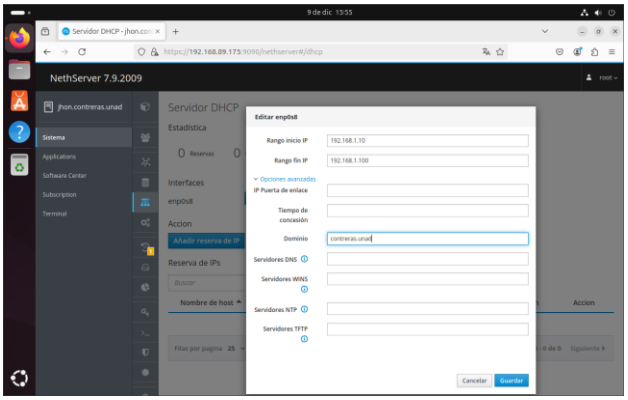

Ilustración 44 servicio DHCP- Autoría Propia

En la interfaz de configuración del servicio DHCP:

1. Activamos el servicio DHCP para la interfaz de la zona Verde (LAN) **enp0s8**.
2. Establecemos el rango de direcciones IP que el servidor asignará automáticamente:
   - **Rango de inicio:** 192.168.1.10
   - **Rango de fin:** 192.168.1.100
3. Configuramos el dominio interno de la red como **contreras.unad**.
4. Guardamos los cambios.

Definir un rango de direcciones (192.168.1.10 - 192.168.1.100) evita conflictos con la dirección estática del servidor (192.168.1.1) y permite reservar direcciones para dispositivos que requieren configuraciones fijas. El dominio interno (**contreras.unad**) proporciona una identidad clara para la red y facilita la resolución de nombres en la red local.

Validación de la conexión desde la consola

Nos dirigimos a la consola de NethServer para realizar pruebas de conectivida

Prueba de resolución de nombres (DNS interno)

Validamos que el dominio interno contreras.unad resuelve correctamente al servidor:

ping contreras.unad

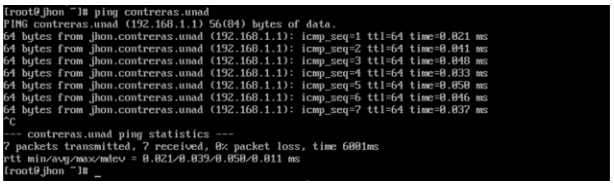

Ilustración 45 Prueba de conectividad contreras.unad- Autoría Propia

El dominio interno **contreras.unad** resuelve correctamente al servidor

Prueba de conectividad externa con Google DNS (8.8.8.8)

Probamos la conectividad externa al realizar un ping al servidor público de Google

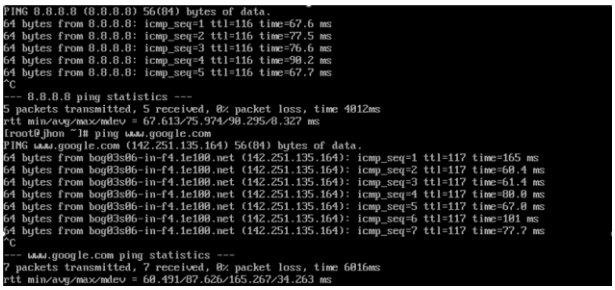

Ilustración 46 Prueba de conectividad Google DNS (8.8.8.8) - Autoría Propia

Esto confirma que el servidor puede resolver nombres de dominio externos mediante su configuración de DNS.

2.15 Instalación y configuración del Firewall en NethServer

En esta sección, procederemos a instalar y configurar el **Firewall** en NethServer. Este componente es esencial para garantizar la seguridad de la red, ya que permite gestionar el tráfico entrante y saliente, definiendo reglas específicas que protejan los servicios y dispositivos conectados al servidor.

Instalación del Firewall básico

1. **Acceso al Centro de Software:**
   - **Desde el panel de control de NethServer, navegamos al apartado Centro de Software.**
   - **Aquí se encuentran disponibles diversos módulos y aplicaciones adicionales para personalizar y ampliar las capacidades del servidor.**

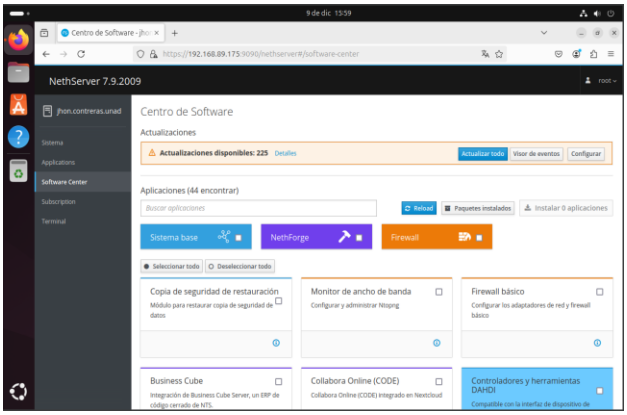

Ilustración 47 Instalación del Firewall básico- Autoría Propia

Selección del módulo Firewall:

- Localizamos la opción **Firewall básico** dentro de la lista de aplicaciones disponibles.
- Marcamos esta opción y hacemos clic en **Instalar Aplicación**.

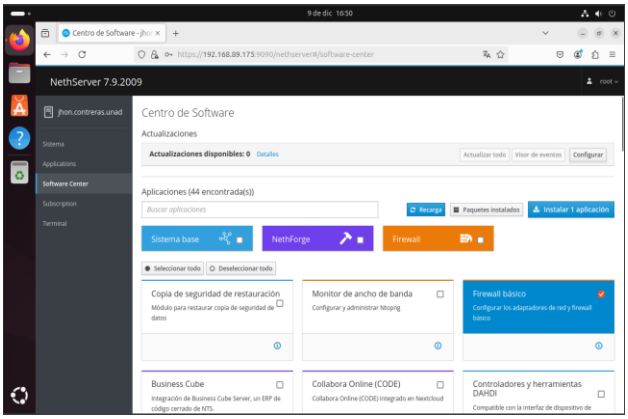

Ilustración 48 2.14 Instalación del Firewall en NethServer- Autoría Propia

Verificación de la instalación

Nos dirigimos al apartado Aplicaciones del panel de control.

En esta sección, verificamos que el Firewall aparece como instalado junto con otras aplicaciones esenciales como el Web Server.

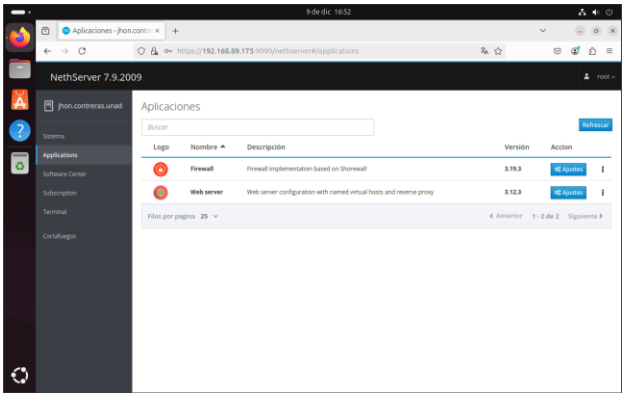

Ilustración 49 Verificación de la instalación- Autoría Propia

confirmamos que el Firewall está instalado asegura que las herramientas necesarias para su configuración estén disponibles y que el servidor pueda comenzar a implementar reglas de control de tráfico.

Visualización de la Topología de Red en el Panel de Control del Firewall

Al acceder al módulo Cortafuegos en NethServer, se nos presenta una representación gráfica de la Topología de Red del servidor. Esta vista es fundamental para entender cómo se han configurado y organizado las interfaces de red, así como la relación entre las zonas de la red y el Firewall

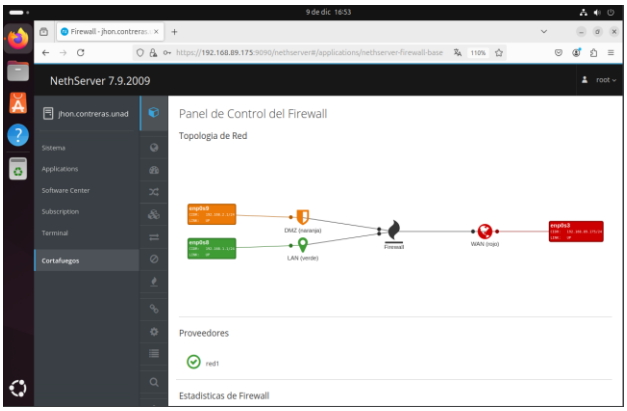

Ilustración 50 Topología de Red - Autoría Propia

La topología ilustra cómo el tráfico fluye entre las distintas zonas:

- **Desde WAN (Rojo):** Todo el tráfico entrante desde Internet pasa primero por el Firewall, donde se aplican las reglas configuradas para filtrar accesos no autorizados.
- **Desde LAN (Verde):** Los dispositivos internos conectados a esta red tienen acceso a Internet a través del Firewall. También pueden acceder a los servicios públicos alojados en la DMZ.
- **Desde DMZ (Naranja):** Los servicios públicos en esta zona están disponibles para conexiones desde Internet, pero no tienen acceso directo a la LAN, lo que protege los dispositivos internos.

Firewall:

- Representado como el núcleo de la topología, gestionando el tráfico entre las tres zonas principales.
- **Función:** Controla y filtra el tráfico entre las zonas WAN, LAN y DMZ, según las reglas configuradas.

Proveedor de red:

- En la parte inferior, se muestra el proveedor de red configurado (en este caso, **red1**), que representa la conexión externa activa.

Instalación de Filtro Web y Proxy Web en NethServer

Continuando con la configuración de NethServer, se procede a instalar las aplicaciones de **Filtro Web** y **Proxy Web**, herramientas que son esenciales para la gestión del acceso a Internet, control de contenido y seguridad en la red.

Acceso al Centro de Software:

- Ingresamos nuevamente al **Centro de Software** desde el panel de control de NethServer.
- Localizamos las opciones **Filtro Web** y **Proxy Web** en la lista de aplicaciones disponibles.
- Marcamos ambas aplicaciones y hacemos clic en **Instalar**.

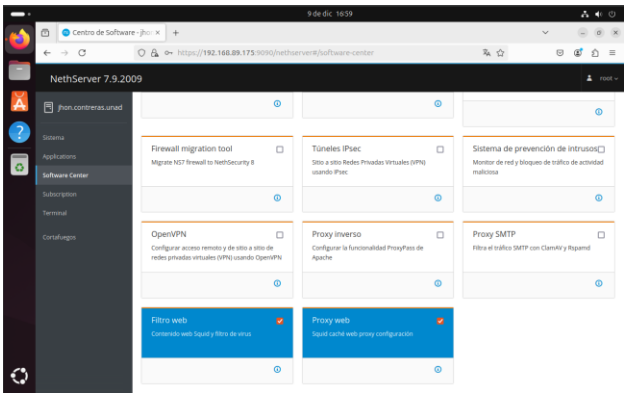

Ilustración 51 Instalación de Filtro Web y Proxy Web- Autoría Propia

Verificación de la instalación

acceso al Panel de Aplicaciones:

- Una vez completada la instalación, nos dirigimos al apartado de Aplicaciones en el panel de control de NethServer.

Verificamos que las siguientes aplicaciones están ahora instaladas y disponibles:

- **Web Proxy & Filter:** Herramienta combinada para control de contenido y gestión del tráfico web.
- **Antivirus:** Instalado automáticamente como complemento para mejorar la seguridad.

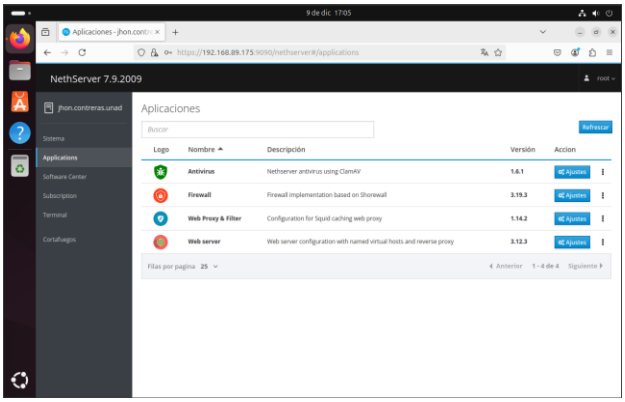

Ilustración 52 Verificación de la instalación Filtro Web y Proxy Web - Autoría Propia

Configuración del Web Proxy & Filter en NethServer

En este paso, procedemos a habilitar y configurar el servicio de Web Proxy & Filter, una herramienta clave para el control del tráfico web, la supervisión de solicitudes y la gestión del ancho de banda en la red.

Acceso y Habilitación del Proxy Web

1. **Ingreso al módulo Web Proxy & Filter:**
   - Desde el panel de aplicaciones en NethServer, seleccionamos **Web Proxy & Filter**.
   - Inicialmente, observamos que el servicio está **deshabilitado**.
   - Hacemos clic en la opción **Configurar Proxy** para ingresar a los ajustes.

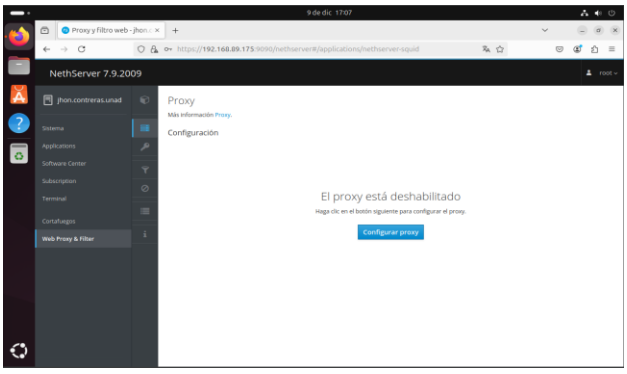

Ilustración 53 Habilitación del Proxy Web - Autoría Propia

Configuración del Proxy

1. **Modo para Zonas Verdes (LAN):**
   - Configuramos el proxy en modo **SSL Transparente** para la red verde (LAN).
   - **Justificación:** Este modo intercepta y supervisa el tráfico HTTPS, proporcionando mayor control sobre las conexiones seguras sin requerir configuración manual en los dispositivos cliente.
2. **Modo para Zonas Azules:**
   - Para la red azul, dejamos el modo **Manual**.

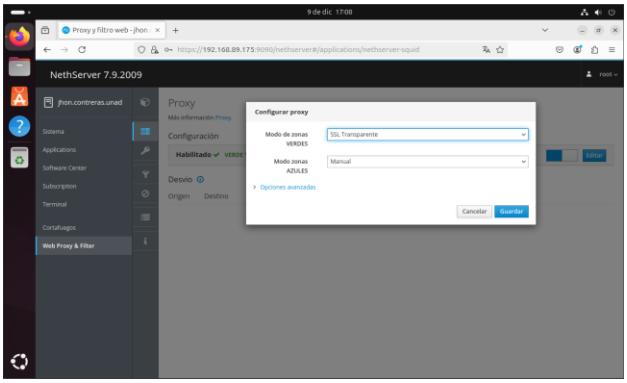

Ilustración 54 Configuración del Proxy - Autoría Propia

Al aplicar y guardar la configuración, el servicio Web Proxy & Filter se habilita automáticamente.

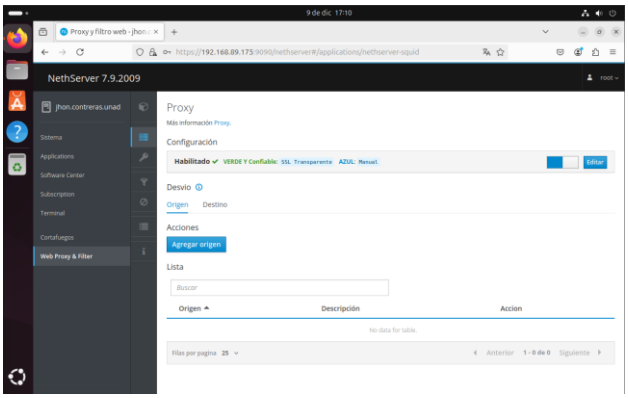

Ilustración 55servicio Web Proxy & Filter habilitado automáticamente. - Autoría Propia

Revisión del servicio Squid

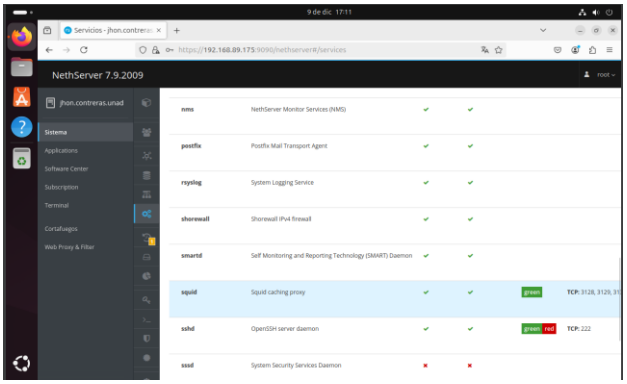

Ilustración 56 servicio Squid - Autoría Propia

Nos dirigimos al apartado de Servicios y buscamos el servicio Squid, que es el motor del proxy.

Verificamos que el servicio está habilitado y escuchando para la red verde (192.168.1.0/24).

Verificación de la Configuración del Proxy y Reglas de Firewall

En este paso, se ha ejecutado una serie de comandos para verificar y monitorear la configuración del proxy y las reglas de firewall en el servidor NethServer.

Al ejecutar el comando : cat /etc/shorewall/rules | egrep REDIRECT

- El comando muestra varias entradas relacionadas con **REDIRECT** para los puertos TCP 3129 y 3138. Esto indica que el tráfico en esos puertos se está redirigiendo al proxy, que es responsable de gestionar el tráfico web:
    - **Puerto 3129 TCP**: Generalmente asociado con HTTP.
    - **Puerto 3138 TCP**: Generalmente asociado con HTTPS.

Estos valores indican que el proxy está configurado para interceptar el tráfico web y redirigirlo a través del proxy.

```
[root@jhon ~]# cat /etc/shorewall/rules | egrep REDIRECT
REDIRECT        loc     3129    tcp     80      -       !192.168.89.175,192.168.1.1,192.168.2.1
REDIRECT        loc     3138    tcp     443     -       !192.168.89.175,192.168.1.1,192.168.2.1
[root@jhon ~]#
```

Ilustración 57 Verificación de las Reglas de Firewall para el Proxy - Autoría Propia

Comprobación de las Cadenas de Firewall

En Este apartado se muestran las reglas activas en las cadenas OUTPUT y POSTROUTING del firewall.

```
Chain OUTPUT (policy ACCEPT 724 packets, 43690 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 713 packets, 42882 bytes)
 pkts bytes target     prot opt in     out     source               destination
   11   808 MASQUERADE  all  --  *      enp0s3  0.0.0.0/0            0.0.0.0/0

Chain loc_dnat (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ~excl0     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
/* transparent proxy on green for port 80 */
    0     0 ~excl1     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
 /* transparent proxy on green for port 443 */

Chain ~excl0 (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.89.175      /* transpar
ent proxy on green for port 80 */
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.1.1         /* transpar
ent proxy on green for port 80 */
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.2.1         /* transpar
ent proxy on green for port 80 */
    0     0 REDIRECT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           /* transpar
ent proxy on green for port 80 */ redir ports 3129

Chain ~excl1 (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.89.175      /* transpar
ent proxy on green for port 443 */
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.1.1         /* transpar
ent proxy on green for port 443 */
    0     0 RETURN     all  --  *      *       0.0.0.0/0            192.168.2.1         /* transpar
ent proxy on green for port 443 */
    0     0 REDIRECT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           /* transpar
ent proxy on green for port 443 */ redir ports 3138
[root@jhon ~]# _
```

Ilustración 58 Cadenas de Firewall - Autoría Propia

Las verificaciones realizadas confirman que el proxy web está correctamente configurado y funcionando de acuerdo con las reglas establecidas. El tráfico HTTP y HTTPS está siendo redirigido a través del proxy en los puertos correctos (3129 y 3138). Las reglas de firewall aseguran que este tráfico se maneje de forma segura y transparente.

2.16 Configuración de Filtros de Contenido Web y Listas de Categorías en el Proxy

En este paso, se realiza la configuración de filtros de contenido web y la habilitación de listas de categorías para bloquear o permitir ciertos sitios según su clasificación.

Configuración de Categorías de Filtro en Web Proxy & Filter

Accedemos al módulo **Web Proxy & Filter** en el panel de NethServer y nos dirigimos a la sección de **Categorías**.

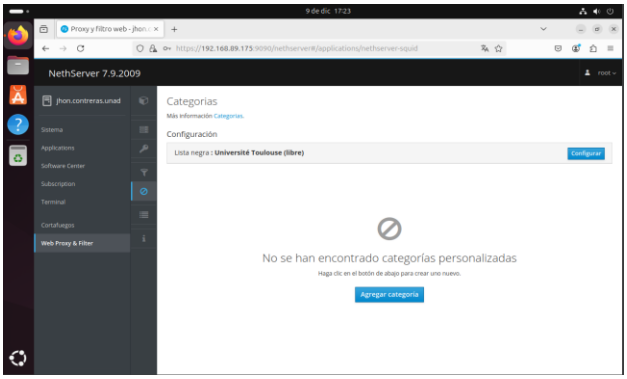

Ilustración 59 Categorías de Filtro en Web - Autoría Propia

Al principio, el sistema nos muestra que **no se ha encontrado ninguna categoría**. Esto significa que no hay categorías de filtro preconfiguradas o descargadas en el servidor.

En la parte superior de la página, encontramos una categoría predeterminada denominada Lista negra: Université

Toulouse (libre). Esta categoría es una lista pública que contiene dominios o sitios web que deben ser bloqueados.

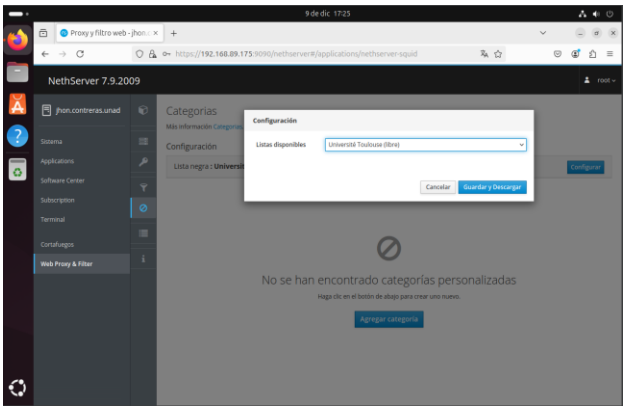

Ilustración 60 descargar las listas de categorías - Autoría Propia

Procedemos a **descargar** las listas de categorías disponibles, lo que permite añadir categorías adicionales de filtrado. Guardamos los cambios para asegurarnos de que las listas se actualicen correctamente.

Habilitación del Filtro de Contenido Web

Nos dirigimos a la sección de Filtros dentro del módulo de Web Proxy & Filter. Aquí podemos observar que el filtro está inicialmente deshabilitado.

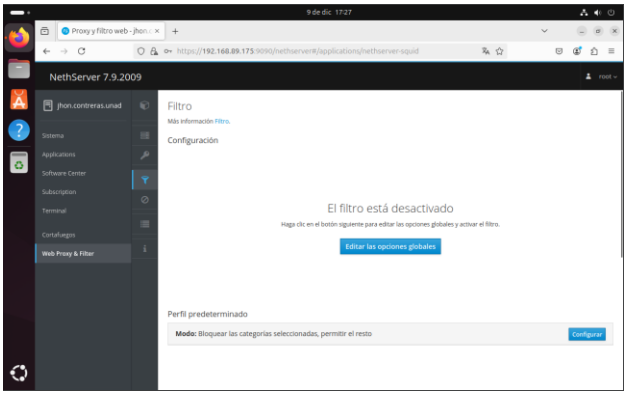

Ilustración 61 Habilitación del Filtro de Contenido Web - Autoría Propia

Hacemos clic en la opción **Editar las opciones globales** para configurar el filtro según nuestras necesidades.

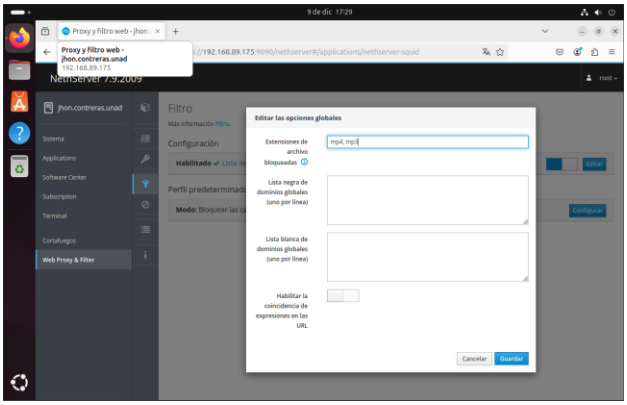

Ilustración 62 Editar las opciones globales - Autoría Propia

Dejamos las opciones predeterminadas tal cual están, asegurándonos de que el filtro quede **habilitado** correctamente, y luego guardamos los cambios.

Configuración del Perfil Predeterminado de Filtrado

A continuación, nos dirigimos a la sección de Perfil Predeterminado para editar las configuraciones específicas de los perfiles de usuario que utilizarán el servicio de filtrado web.

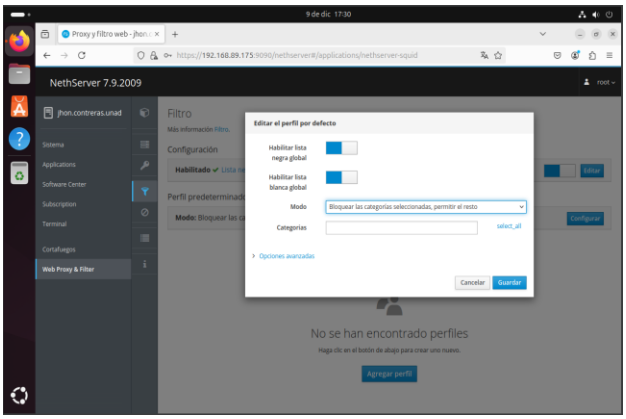

Ilustración 63 Configuración del Perfil Predeterminado de Filtrado - Autoría Propia

- En el perfil predeterminado, habilitamos la **Lista negra global**. Esto asegura que se aplique la lista negra a todos los usuarios que utilicen el servicio de proxy y filtrado web.

- Habilitamos también la **Lista blanca global**, lo que permite permitir ciertos sitios web a pesar de estar en las categorías bloqueadas.

- Configuramos el filtro en **modo "Bloquear las categorías seleccionadas"**, lo que significa que se bloquearán las categorías específicas que seleccionemos (como contenido para adultos, redes sociales, etc.).

- Para todas las demás categorías que no estén seleccionadas en la lista, se permitirá el acceso. Esta configuración asegura que solo los sitios clasificados en las categorías bloqueadas serán restringidos, mientras que el resto se mantendrá accesible.

Después de configurar las opciones anteriores, procedemos a **guardar los cambios**.

Procedimiento para Bloquear Sitios Web Usando Filtros en NethServer

En este paso, se procederá a bloquear los sitios web relacionados con contenido pornográfico utilizando las categorías de filtrado definidas en el perfil predeterminado.

Acceso al Perfil Predeterminado de Filtro

Nos dirigimos nuevamente al Perfil Predeterminado dentro del módulo Web Proxy & Filter para editar las configuraciones de filtrado. Dentro del perfil predeterminado, buscamos la sección de Categorías. Aquí se encuentran las diferentes categorías de sitios web que podemos controlar.

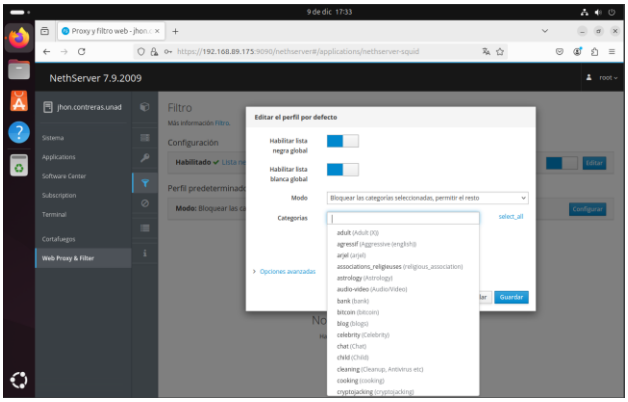

Ilustración 64 Bloquear Sitios Web Usando Filtros en NethServer - Autoría Propia

Buscamos y seleccionamos las categorías **adul** (contenido para adultos) y **mixed_adul**

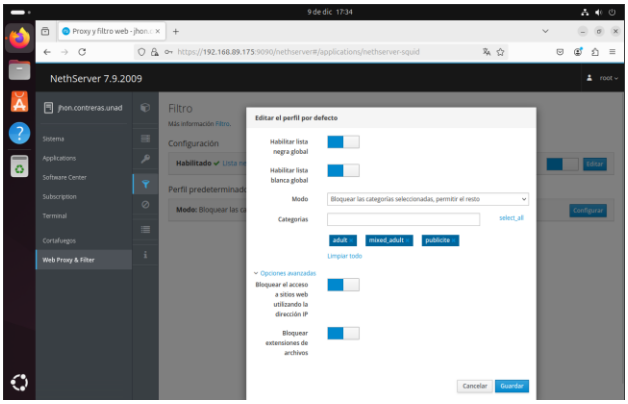

Ilustración 65 Bloquear Sitios Web Usando Filtros en NethServer - Autoría Propia

A continuación, configuramos el **modo de filtrado**. Como se mencionó previamente, se debe habilitar el modo **"Bloquear las categorías seleccionadas"**.

Al seleccionar las categorías **adul** y **mixed_adul**, NethServer bloqueará los sitios web que caen dentro de estas categorías.

Descripción del Panel de Control del Proxy y el Filtro Web en NethServer

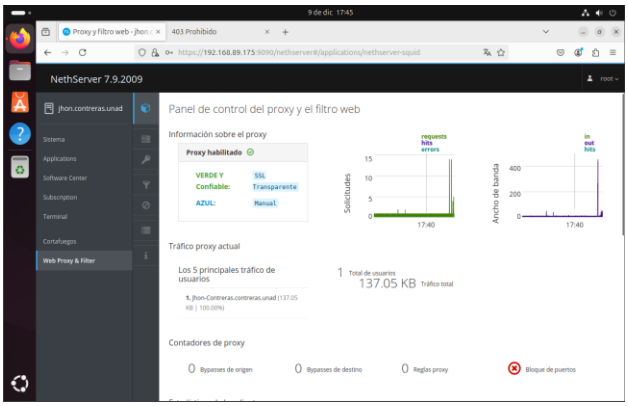

Ilustración 66 del Panel de Control del Proxy y el Filtro Web - Autoría Propia

A continuación, como podemos observar en el Panel de control del proxy y el filtro web, se nos presenta información clave sobre el funcionamiento del proxy:

1. **Estado del Proxy:** En la parte superior, se muestra que el proxy está habilitado. Además, se detalla el tipo de configuración:
   - VERDE Y SSL indica que el proxy admite conexiones seguras.
   - Confiable - Transparente, que significa que no requiere configuración manual en los dispositivos de los usuarios.
   - AZUL - Manual, opción que no está activa en este momento.
2. **Tráfico Proxy Actual:** En la sección central, podemos observar el tráfico generado por los usuarios conectados al proxy. En este caso, solo hay

un usuario registrado: *jhon.contreras.unad*, quien ha generado un tráfico total de 137.05 KB.

3. **Gráficas de Actividad:**
    - En la gráfica de solicitudes (requests), podemos observar la cantidad de peticiones procesadas por el proxy en tiempo real, con un registro de hits (solicitudes exitosas) y posibles errores.
    - La gráfica de ancho de banda muestra el flujo de datos de entrada y salida del proxy.

Reporte de Acceso de Usuarios Squid

se muestra un informe generado por Squid sobre el acceso de usuarios correspondiente al periodo de trabajo de diciembre de 2024. En este reporte se puede analizar la actividad del proxy en detalle:

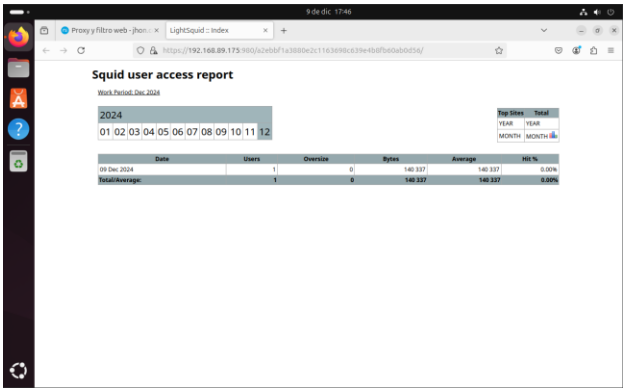

Ilustración 67 Reporte de Acceso de Usuarios Squid - Autoría Propia

El informe indica que el día 9 de diciembre de 2024 Este tipo de reportes es muy útil para monitorear el uso del proxy, analizar el tráfico generado por los usuarios y ajustar la configuración del sistema según las necesidades de la red.

Verificación de la Funcionalidad del Bloqueo

Para verificar que el bloqueo esté funcionando correctamente, intentamos acceder a un sitio web que pertenezca a las categorías adul o mixed_adul para ello ingresamos a www.xxx.com.

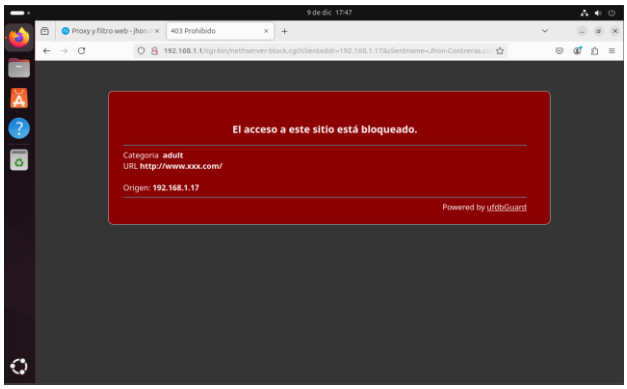

Ilustración 68 Verificación de la Funcionalidad del Bloqueo - Autoría Propia

La prueba de acceso a **www.xxx.com** nos confirma que la configuración de bloqueo para las categorías **adul** y **mixed_adul** está funcionando correctamente, garantizando que los sitios pornográficos estén bloqueados, tal como se esperaba.

Procedimiento para Bloquear Redes Sociales (Facebook y Twitter)

A continuación, se explica el proceso para bloquear sitios web de redes sociales como Facebook y Twitter utilizando el filtro de contenido en NethServer,

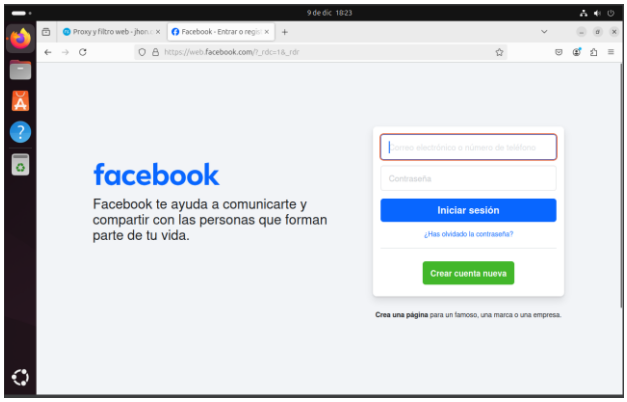

Ilustración 69 Sitio web Facebook - Autoría Propia

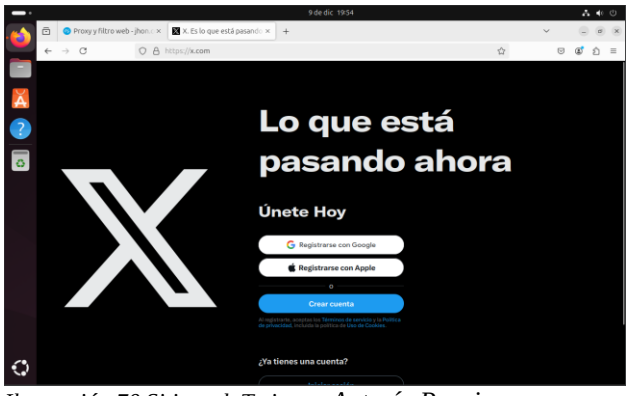

Ilustración 70 Sitio web Twitter - Autoría Propia

Creación de una Nueva Categoría para Redes Sociales

Nos dirigimos a Web Proxy & Filter y seleccionamos la opción Categorías.

Hacemos clic en Agregar Categoría. En el campo de nombre, colocamos R. Sociales para identificar esta nueva categoría como relacionada con redes sociales.

En el campo de dominios, colocamos las URL de los sitios web que queremos bloquear, como www.facebook.com (y también podemos agregar www.twitter.com si deseamos bloquear Twitter).

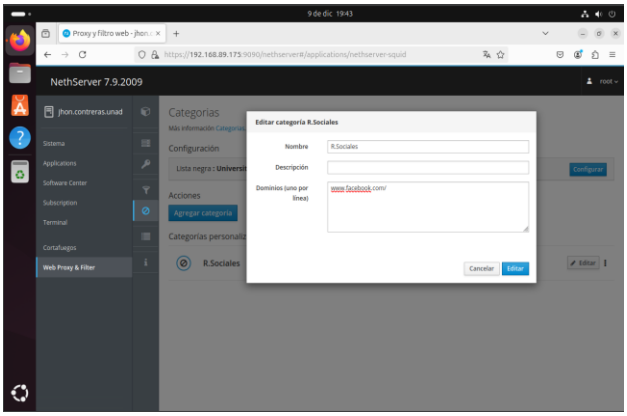

Ilustración 71 Creación de una Nueva Categoría - Autoría Propia

Finalmente, hacemos clic en **Editar** para confirmar la creación de la categoría **R. Sociales**.

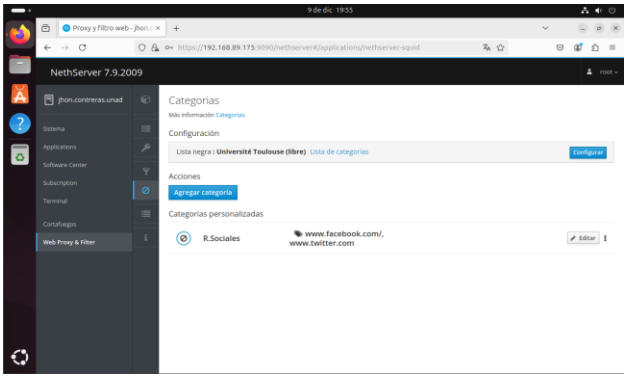

Ilustración 72 Creación de una Nueva Categoría R.Sociales. - Autoría Propia

Configuración del Filtro de Redes Sociales

Ahora, nos dirigimos a la opción de **Filtro** dentro de **Web Proxy & Filter** y seleccionamos **Editar perfil por defecto**.

En la sección de **Categorías**, buscamos la nueva categoría que hemos creado, **R. Sociales**, y la habilitamos para ser bloqueada.

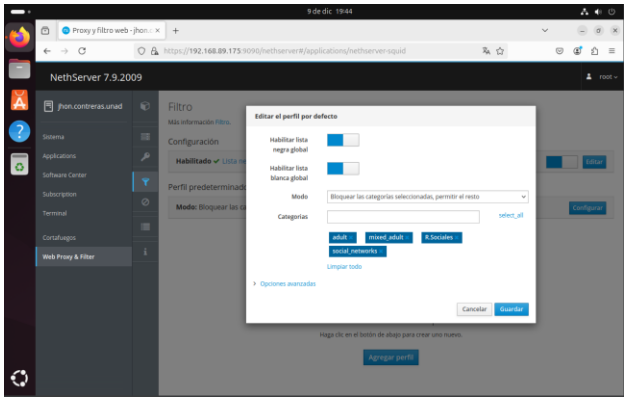

Ilustración 73 Configuración del Filtro de Redes Sociales - Autoría Propia

Después de habilitarla, hacemos clic en **Guardar** para aplicar los cambios al perfil predeterminado.

Confirmación del Bloqueo de Sitios Web de Redes Sociales

Para verificar que el bloqueo ha sido exitoso, intentamos acceder a www.facebook.com desde un dispositivo dentro de la red gestionada por NethServer.

Al ver el mensaje de bloqueo, podemos confirmar que el filtro está funcionando correctamente y que **Facebook** ha sido bloqueado según la categoría **R. Sociales**.

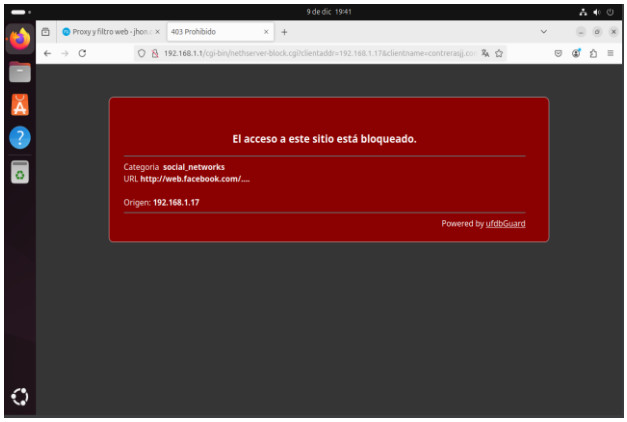

Ilustración 74 Confirmación del Bloqueo de Sitios Web Facebook - Autoría Propia

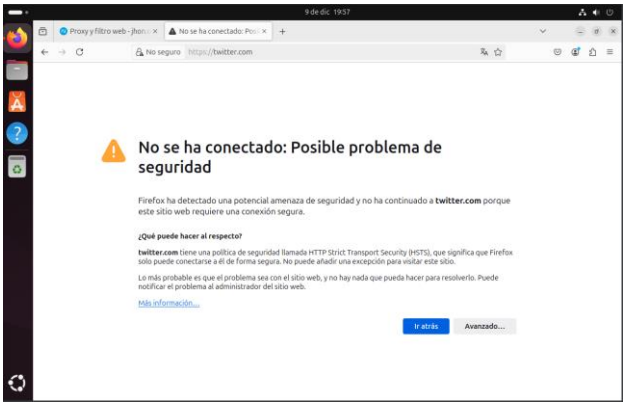

Ilustración 75 Confirmación del Bloqueo de Sitios Web Twitter - Autoría Propia

El proceso de bloqueo de redes sociales se ha completado con éxito. La creación de la categoría **R. Sociales**, junto con la configuración del filtro para bloquear dicha categoría, ha dado como resultado el bloqueo efectivo de **Facebook** y **Twitter**, impidiendo que los usuarios accedan a estos sitios desde la red gestionada por NethServer. La verificación a través del mensaje de **"Acceso denegado"** confirma que el filtro está funcionando correctamente.

2.16.1 Conclusiones.

La implementación del cortafuegos en GNU/Linux NethServer permitió cumplir con el objetivo de restringir el acceso a sitios web de entretenimiento y redes sociales, garantizando un entorno seguro y funcional para la red administrada. Las reglas y políticas configuradas se validaron exitosamente, evidenciando su efectividad en el cumplimiento de las restricciones solicitadas.

Este estudio muestra cómo las herramientas de código abierto se pueden usar para administrar sistemas informáticos, especialmente en lo que se refiere a la seguridad.Además, al configurar la zona DMZ y seguir buenas prácticas en la gestión de sistemas, se refuerza el control y la protección en las redes de las empresas.

Este proyecto nos muestra la importancia de combinar teoría y práctica al resolver problemas en sistemas operativos Open Source.

3 REFERENCIAS

(102., 2022) (Canonical, 2018) (Debian, 2020) (Oracle, 2020) (Gómez-Marí, 2023) (nethserver, 2024)

4 Bibliografía

102., L. L.-1. (2022). *Tema 110: Seguridad*. Obtenido de https://learning.lpi.org/es/learning-materials/102-500/110/

Canonical. (2018). *Guía del Ubuntu desktop 20.04 LTS*. Obtenido de https://help.ubuntu.com/20.04/ubuntu-help/index.html

Debian. (2020). *El manual del administrador de Debian 12.5.0. Debian*. Obtenido de https://www.debian.org/releases/stable/amd64/index.es.html

Gómez-Marí, I. &.-S. (2023). *La educación en la era del metaverso.* Obtenido de https://hemeroteca.unad.edu.co/index.php/educat/article/view/6571/6473

nethserver. (2024). Obtenido de https://www.nethserver.org/

Oracle. (2020). *VirtualBox*. Obtenido de https://www.virtualbox.org/manual/