Diego Alexander Zambrano Alayon – **Temario 1**
e-mail: Dazambranoa@unadvirtual.edu.co
Diego Alexander Zambrano Alayon – **Temario 2**
e-mail: Dazambranoa@unadvirtual.edu.co
Diego Alexander Castañeda Lizcano – **Temario 3**
e-mail: dacastanedali@unadvirtual.edu.co
Mario Osorio Torres – **Temario 4**
e-mail: mosoriotor@unadvirtual.edu.co
Juan Carlos Guerrero Ballen – **Temario 5**
e-mail jcguerrerob@unadvirtual.edu.co

1. RESUMEN

Este trabajo tiene como objetivo la implementación y configuración de servicios esenciales en una infraestructura de red basada en GNU/Linux, utilizando Nethserver como plataforma principal. A través de la selección de temáticas como servidores DHCP, DNS, proxis, cortafuegos, servidores de archivos e impresión, y VPN, se busca dotar a los participantes de las habilidades necesarias para gestionar y asegurar una red en entornos corporativos complejos. Cada miembro del equipo trabajará en una de estas temáticas, documentando los procedimientos, configuraciones y resultados obtenidos. El enfoque será colaborativo, con retroalimentación constante entre los integrantes para optimizar las soluciones implementadas. El trabajo culminará con la elaboración de un informe técnico en formato IEEE, que consolidará los hallazgos y soluciones implementadas en cada área, destacando los aprendizajes adquiridos a lo largo del proceso.

2. OBJETIVO 1

Desarrollar la capacidad de configurar y administrar servicios clave de infraestructura IT, como el servidor DHCP, el servidor DNS y el controlador de dominio en un entorno basado en GNU/Linux, utilizando Nethserver. A través de este proceso, se profundizará en la asignación dinámica de direcciones IP, la resolución de nombres dentro de la red y el control de acceso a recursos mediante autenticación centralizada, garantizando una gestión eficiente y segura de las estaciones de trabajo en una red corporativa o institucional.

3. OBJETIVO

Adquirir competencias en la implementación y configuración de un servidor Proxy en Nethserver, destinado a gestionar el acceso a Internet desde estaciones de trabajo GNU/Linux. Este objetivo permitirá al estudiante comprender y aplicar técnicas de filtrado de tráfico web, utilizando reglas específicas para controlar el acceso a ciertos contenidos y servicios en línea. Este aprendizaje contribuirá a optimizar la seguridad, la eficiencia y el rendimiento de la red, asegurando que las políticas de uso de Internet se apliquen de manera efectiva.

4. OBJETIVO

Desarrollar habilidades para la configuración y gestión de una red privada virtual (VPN) en Nethserver, con el objetivo de establecer un túnel seguro de comunicación entre estaciones de trabajo GNU/Linux. A través de la implementación de la VPN, se adquirirá un conocimiento profundo sobre la creación de canales de comunicación cifrados que protejan la integridad y confidencialidad de los datos transmitidos, facilitando el acceso remoto seguro a los recursos de la red institucional o corporativa.

5. PALABRAS CLAVE

GNU/Linux, Nethserver, Infraestructura de red, Servicios IT, Seguridad en redes, DHCP, DNS, Proxy, Cortafuegos, VPN, Servidor de archivos, Servidor de impresión, Configuración de servicios, Administración de sistemas, Redes corporativas, Trabajo colaborativo, Documentación técnica, Formato IEEE, Optimización de red.

6. TEMARIOS DE DESARROLLO DE EJERCICIO

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

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Nethserver.

DESARROLLO DEL TEMARIO 1

DHCP Server, DNS Server y Controlador de Dominio.
Aquí descargamos el ISO del Netserver en su paguina oficial https://sourceforge.net/projects/nethserver/

.

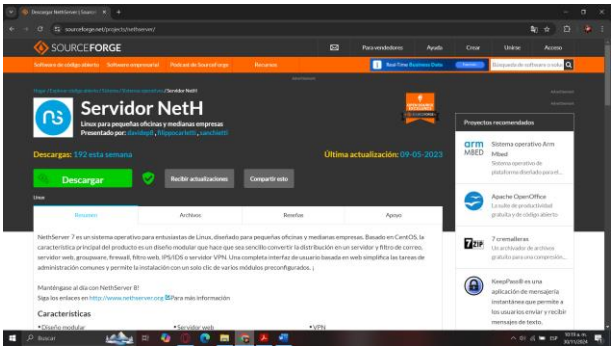

Fig. 1 -. Página de descarga

Configuramos la máquina para la instalación del NethServer

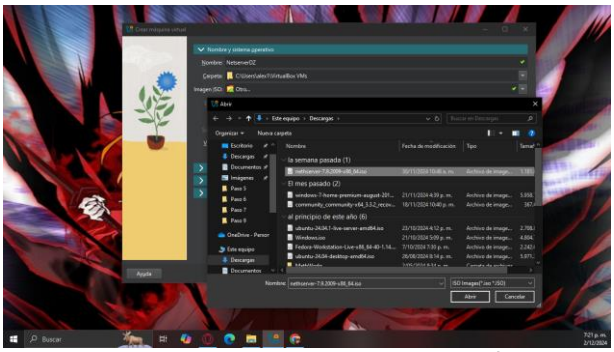

Fig. 1 - instalación del servidor

Iniciamos la maquina esperamos que nos arroje el menú de instalación e iniciamos en el la primera opción

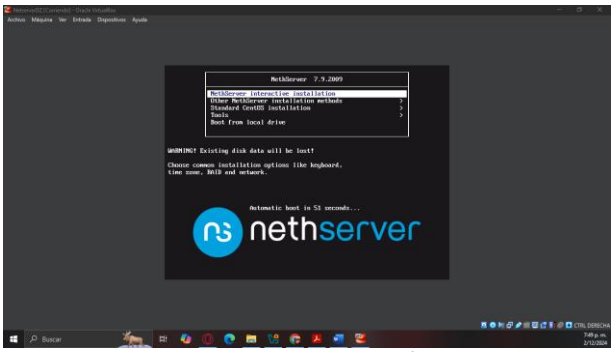

Fig. 3 - inicio de instalación interactiva NethServer

Seleccionamos fecha, hora y teclado y también si se quiere el lenguaje

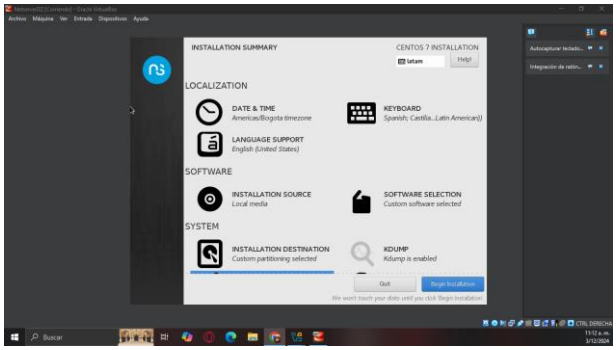

Fig. 2 - menú de instalación

Configuramos la clave del super usuario ROOT

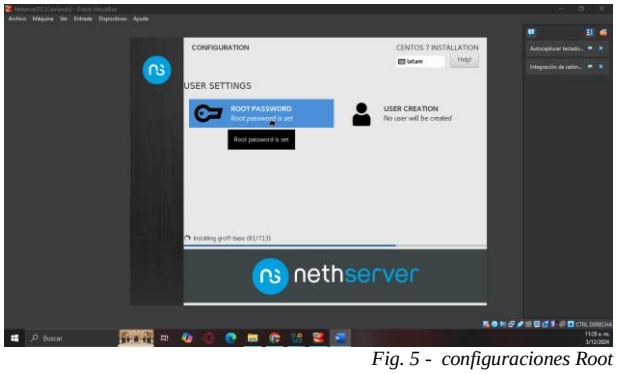

Fig. 5 - configuraciones Root

Este ya es el inicio de pantalla del servidor NethServer

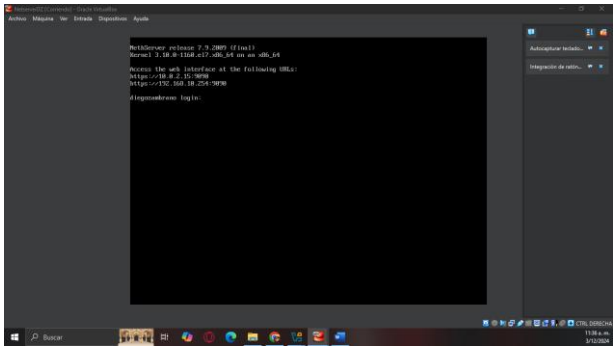

Fig. 6 - pantalla principal del servidor

Nos toca ajustar manualmente la red para poder acceder al servidor desde el escritorio grafico de fedora

.

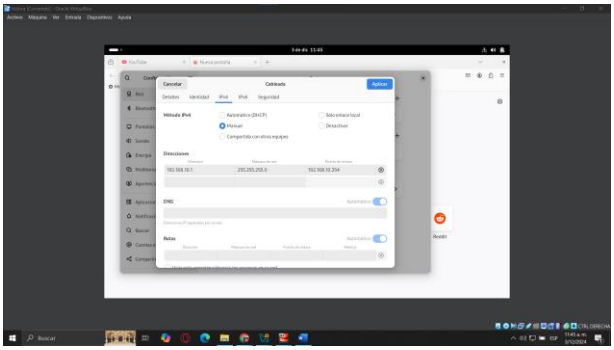

Fig. 7 - ajuste de IP

Inicio de sesión, se coloca la dirección configurada que sería 192.168.10.254 y usamos el: 9090 tenemos en cuenta que se debe de colocar de la siguiente manera https//192.168.10.254:9090 (en el caso del ejemplo) esto para que nos arroje el inicio de logeo del NethServer seria Root y la clave asignada

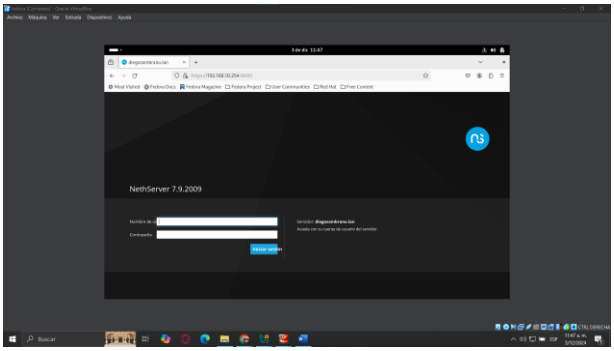

Fig. 8 - inicio de root

Después de las credenciales nos arroja el menu de inico

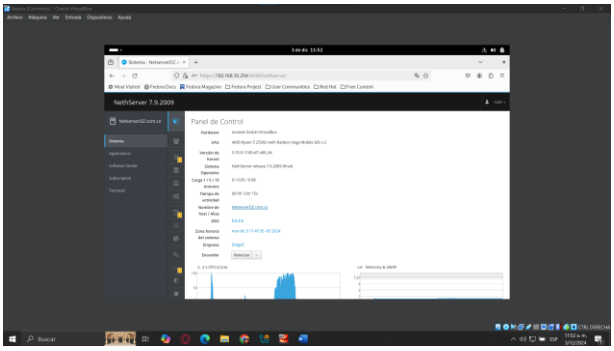

Fig. 9 - panel principal

Cambiamos una de las redes de verde a roja para el WAN

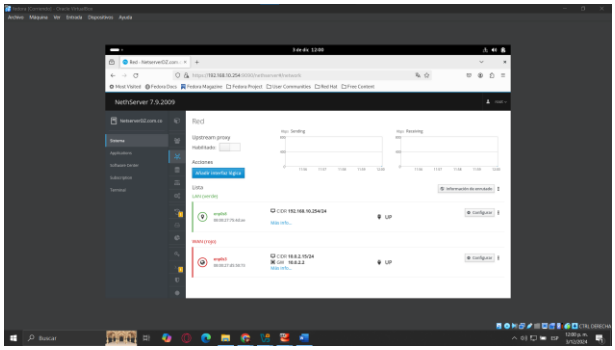

Fig. 10 - configuración de red

Después de configurar se configura la red en automatico ya que antes no nos arrojaba intenet

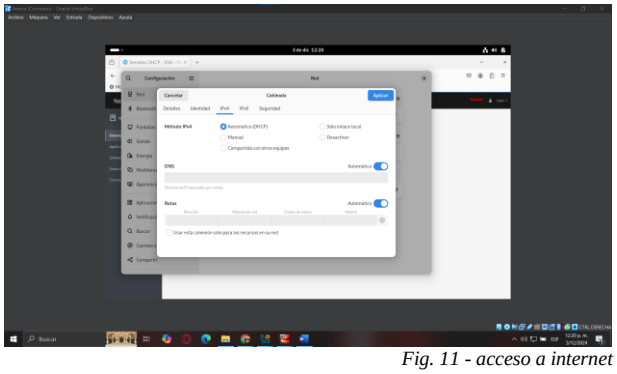

Fig. 11 - acceso a internet

Comprobamos que ahora si nos está dando internet

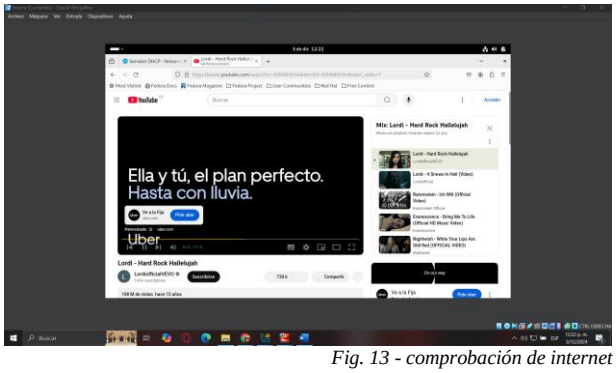

Fig. 13 - comprobación de internet

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.

DESARROLLO DEL TEMARIO 2

Seleccionamos las aplicaciones a usar para configurar el proxy

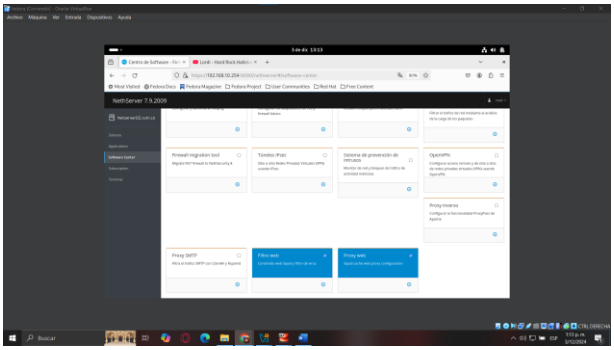

Fig. 13 - instalación de aplicaciones

Configuramos el proxy en SSL transparente

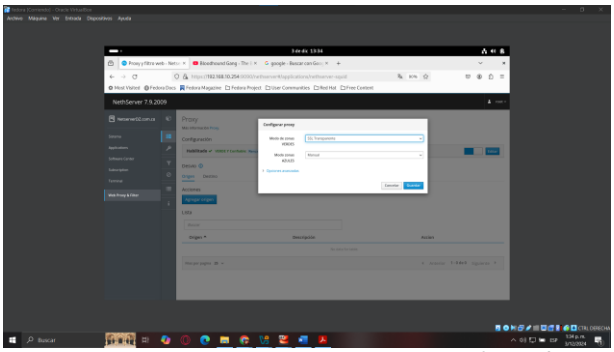

Fig. 14 - configuración proxy

Despuesde la configuración vemos que ya esta encendido el proxy y esta en funcionamientio

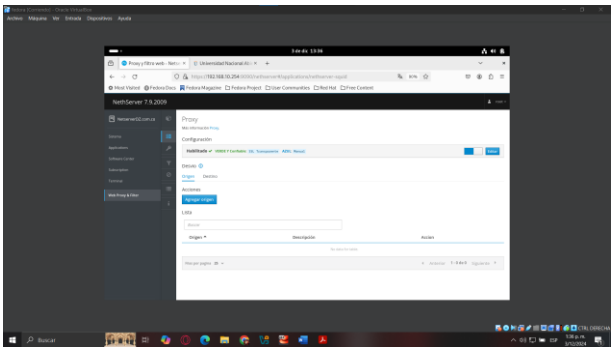

Fig. 15 - proxy funcionando

Aquí nos damos cuenta de que el puerto solicitado 3128 está activo y corriendo

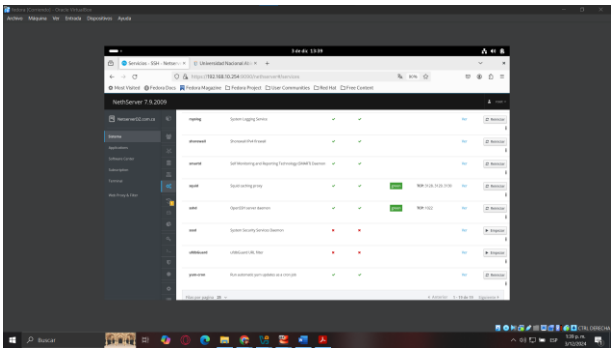

Fig. 16 - comprobación Puerto 3128

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.

DESARROLLO DEL TEMARIO 3

El temario se llevará a cabo la configuración de una red simulada utilizando la herramienta GNS3 para estudiar y comprender las funcionalidades y servicios proporcionados por un servidor de firewall. En este caso, se utiliza NethServer, una distribución basada en Linux diseñada para proporcionar servicios de red, seguridad y administración a pequeña y mediana escala. A lo largo del proceso, se integran diversas máquinas virtuales y se configuran distintos servicios de red, incluyendo el acceso a Internet, control de tráfico y filtrado de contenido web.

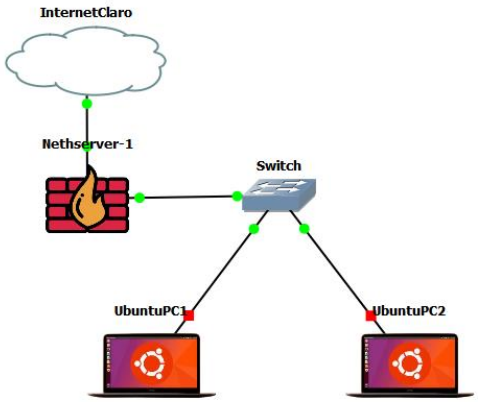

Fig. 17 – Topología de red

La arquitectura de red diseñada para este proyecto es sencilla pero funcional, e incluye los siguientes artefactos:

- *Internet: Simulado como un proveedor externo de conectividad.*
- *Servidor de Firewall: NethServer, que actuará como un cortafuegos y servidor de gestión de red.*
- *Switch de Acceso o Distribución: Encargado de la interconexión de dispositivos dentro de la red.*
- *UbuntuPC1 y UbuntuPC2: Máquinas con Ubuntu que actúan como clientes dentro de la red simulada.*

se procede con la instalación de NethServer en una máquina virtual, con el objetivo de configurar una plataforma que sirva como servidor de firewall y administración de la red.

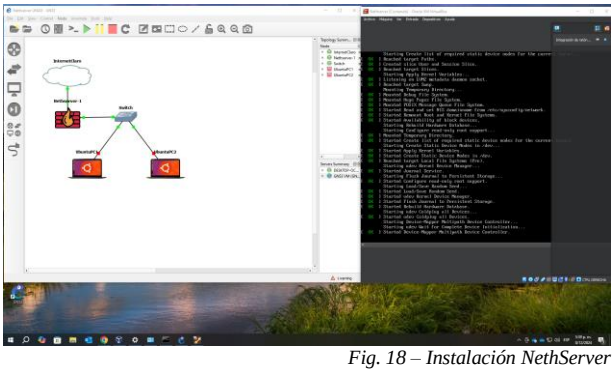

Fig. 18 – Instalación NethServer

La instalación se realiza mediante una imagen ISO de NethServer, y durante el proceso se asignan los recursos necesarios a la máquina virtual (como CPU, RAM y almacenamiento). Al iniciar la máquina virtual, NethServer solicita la configuración básica del sistema.

Durante los primeros pasos de la configuración, se deben ajustar los parámetros de fecha, hora y la disposición del teclado para adecuarlo al entorno local. Estos parámetros son cruciales para la correcta sincronización de logs y administración remota del sistema.

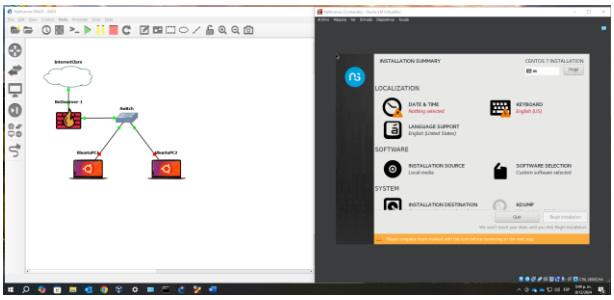

Fig. 19 – Con figuración NethServer

Una de las primeras tareas en la configuración de NethServer consiste en definir las interfaces de red para permitir la conectividad con otras máquinas en la red.

Configuración de la Primera Interfaz (enp0s3): para obtener automáticamente una dirección IP mediante DHCP desde el simulador de Internet. Esta configuración permite que NethServer acceda a la red externa, facilitando la conexión a Internet. Se asigna el FQDN (Fully Qualified Domain Name) de ***nethserver.unad.lan*** *para identificar de manera única al servidor dentro de la red local.*

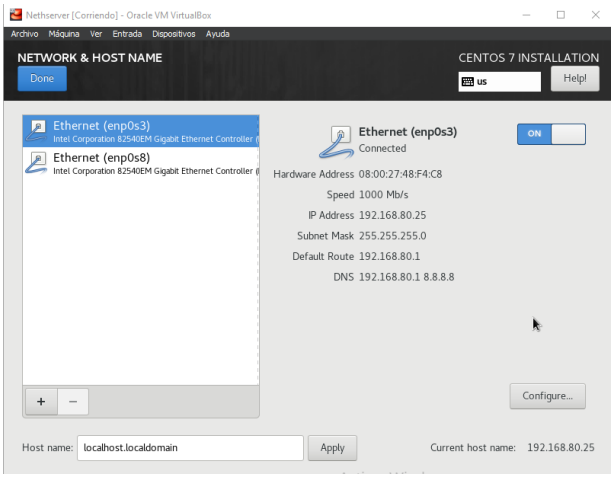

Fig. 20 – Configuración Adaptador de red

Configuración de la Segunda Interfaz (enp0s8, se configura de manera estática con la dirección IP 192.168.10.254 y la máscara de subred 255.255.255.0 (o /24). Esta interfaz actuará como la puerta de enlace interna de la red local, permitiendo la comunicación con los clientes dentro de la red.

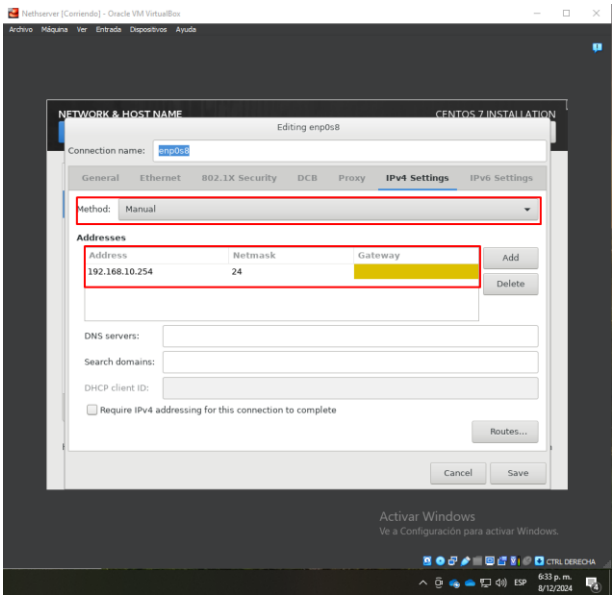

Fig. 21 – Configuración Adaptador de red

Una vez configurado el servidor NethServer, se procede con la configuración de los equipos clientes. En este caso, se utiliza ***UbuntuPC1****, que se conecta al servidor NethServer para acceder a la interfaz web de administración.*

La tarjeta de red de UbuntuPC1 se configura para obtener una dirección IP automáticamente a través del servicio DHCP proporcionado por NethServer. Esto se logra ajustando los parámetros de la tarjeta de red a Automático (DHCP) en la configuración de red de UbuntuPC1.

Fig. 22 – Configuración Adaptador de red PC1

*Al obtener la dirección IP, **UbuntuPC1** se configura para acceder a la interfaz de administración web de NethServer mediante la URL **https://192.168.10.254**. Al aceptar el certificado no seguro del servidor, se accede a la interfaz de administración de NethServer.*

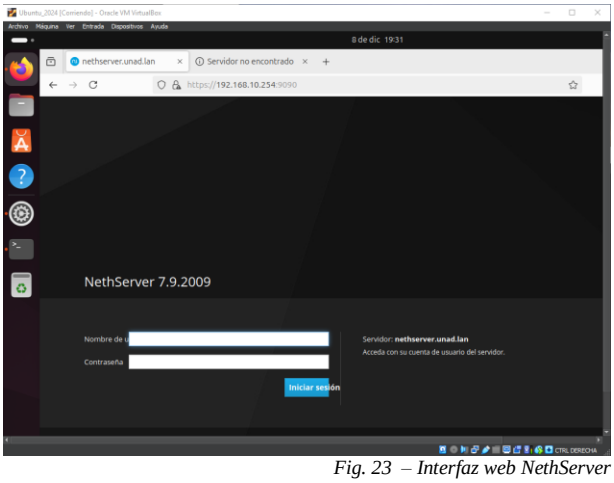

Fig. 23 – Interfaz web NethServer

En la interfaz web de NethServer, se configuran los roles de las interfaces de red para definir su comportamiento dentro de la red.

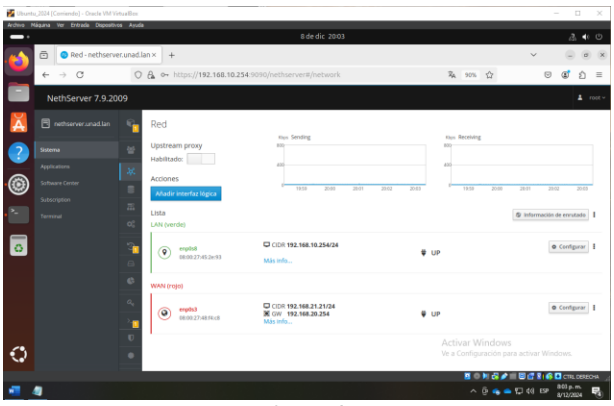

Fig. 24 – Configuración Adaptador de red - NethServer

*Se configura la interfaz **enp0s3** como **WAN** (Wide Area Network), asignándole una dirección IP estática de **192.168.80.30**, con máscara de subred **255.255.255.0** y puerta de enlace **192.168.80.1**, que corresponde a la IP de la red externa.*

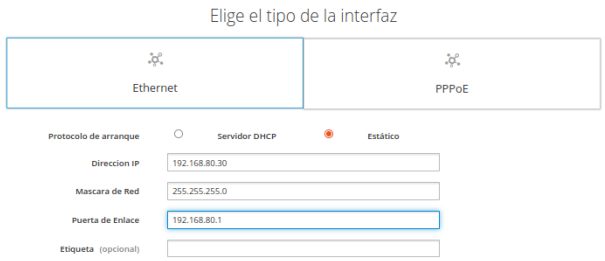

Fig. 25 – Adaptador de red WAN

*La interfaz **enp0s8** se configura con el rol **LAN**. Se mantiene la dirección IP **192.168.10.254** con la máscara de subred **255.255.255.0**.*

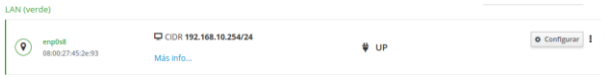

Fig. 26 – Adaptador de red LAN

*Se configura el servidor DNS para **NethServer**. El primer servidor DNS se establece en **192.168.80.1** (servidor de DNS interno) y como secundario se configura **8.8.8.8**, el servidor DNS público de Google.*

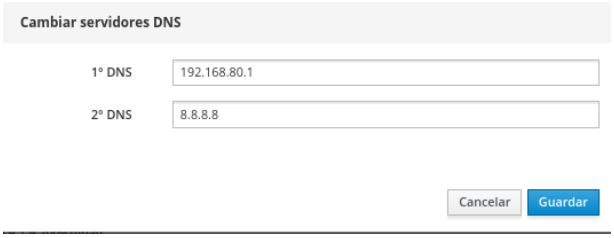

Fig. 27 – Configuración DNS

Se configura el servicio DHCP en la interfaz LAN de NethServer. El rango de direcciones IP permitidas está delimitado entre 192.168.10.10 y 192.168.10.254. Este rango se utilizará para asignar dinámicamente direcciones IP a los dispositivos que se conecten a la red interna.

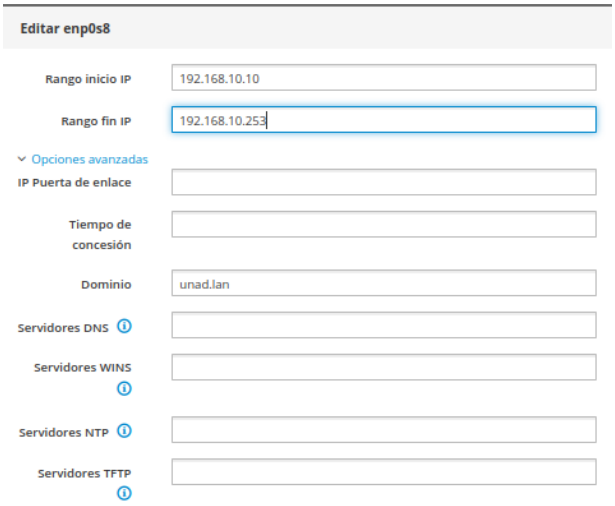

Fig. 28 – Configuración DHCP

*Se verifica que **UbuntuPC1** obtenga una dirección IP dentro del rango configurado por el servidor DHCP y que pueda acceder a los servicios proporcionados por NethServer, incluyendo el acceso a Internet y la interfaz de administración web.*

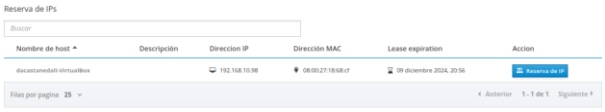

Fig. 29 – Asignación de IP al PC1

Al ejecutar esta configuración el equipo toma el siguiente direccionamiento automático con la IP 192.168.10.98 y los DNS del servidor 192.168.10.254

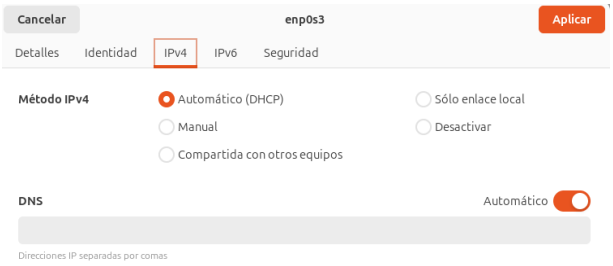

Fig. 30 – Adaptador de red DHCP

*Para garantizar la seguridad y el control del tráfico de red en la infraestructura simulada, se procede a la instalación y configuración del firewall en **NethServer**. El servidor NethServer cuenta con una herramienta integrada llamada **Shorewall**, que permite definir políticas y reglas de tráfico para gestionar la comunicación entre las distintas interfaces de red.*

Para comenzar, es necesario instalar el paquete de firewall básico, que se encuentra disponible en el Software Center de NethServer. Este paquete habilita el servicio de Shorewall, que permite aplicar políticas de control de acceso y filtrado en las interfaces de red configuradas previamente.

Para instalar el paquete, se accede al Software Center y se selecciona la opción correspondiente para instalar el Firewall Básico. Este paquete incluye las herramientas necesarias para configurar el firewall, así como las reglas predeterminadas que pueden ser personalizadas según las necesidades del entorno de red.

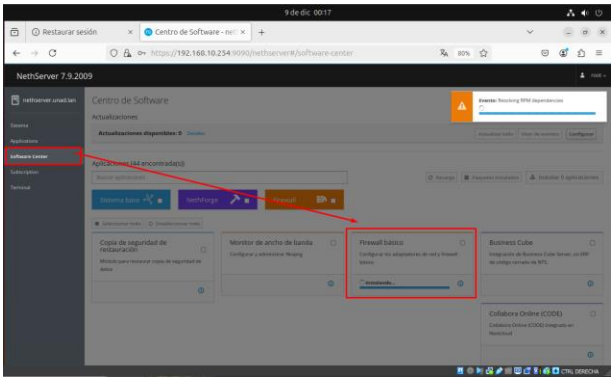

Fig. 31 – Modulo Firewall Básico

*Una vez instalado el servicio de firewall, se accede a la interfaz de administración de **Shorewall** desde la plataforma web de NethServer. Al iniciar el servicio, se visualiza la topología de la red, junto con estadísticas detalladas sobre el tráfico que atraviesa las interfaces de red. Esta información es crucial para monitorear el rendimiento del firewall y verificar que las políticas se apliquen correctamente.*

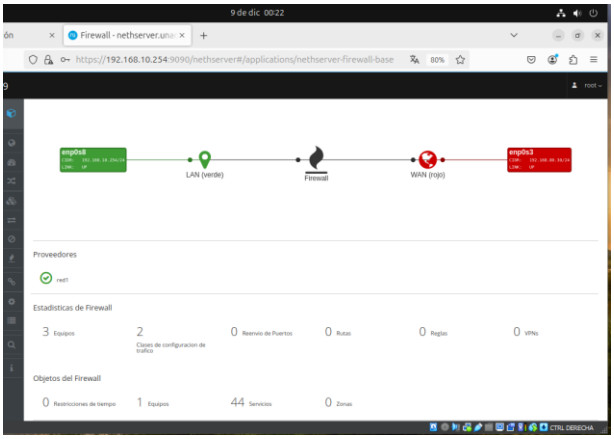

Fig. 32 – Topología de Red

*Para complementar la seguridad y el control de la red, se implementa un sistema de filtrado de contenido web. NethServer permite configurar un servicio de **proxy web** y un sistema de **filtrado de URLs** para gestionar el acceso a páginas web, bloqueando contenido no deseado o potencialmente peligroso.*

- *Proxy Web: Este servicio actúa como intermediario entre los clientes de la red interna y los servidores externos en Internet. Al habilitar el proxy, se puede controlar el tráfico HTTP y HTTPS, además de permitir la implementación de políticas de filtrado y control de acceso.*

- *Filtrado de Contenido Web: Este servicio se encarga de bloquear o permitir el acceso a determinadas páginas web en función de su contenido. Para esto, se utiliza el servicio UFDBGuard (URL Filter Database), que emplea una base de datos actualizada para identificar sitios web que deben ser filtrados.*

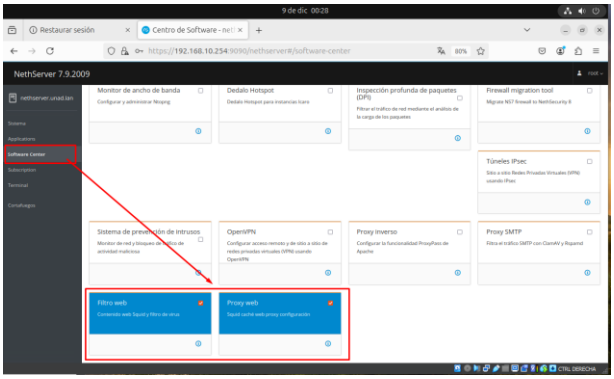

Fig. 33 – Proxy Web

La activación del proxy permite comenzar a monitorear las solicitudes web que los clientes internos realicen a través del servidor, proporcionando estadísticas detalladas sobre el tráfico y las peticiones realizadas.

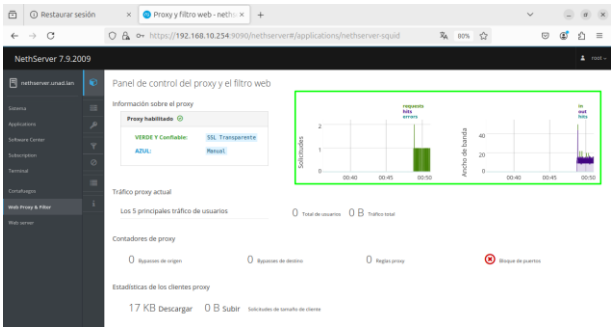

Fig. 34 – Estado del Trafico Web

Para habilitar el servicio de filtrado de contenido, se debe activar UFDBGuard, que utiliza una base de datos de URLs clasificadas por categorías. Esta base de datos se actualiza regularmente para reflejar los cambios en la web y mejorar la efectividad del filtrado.

*El servicio de **filtrado de contenido web** permite configurar diferentes categorías de sitios web que pueden ser bloqueados o permitidos.*

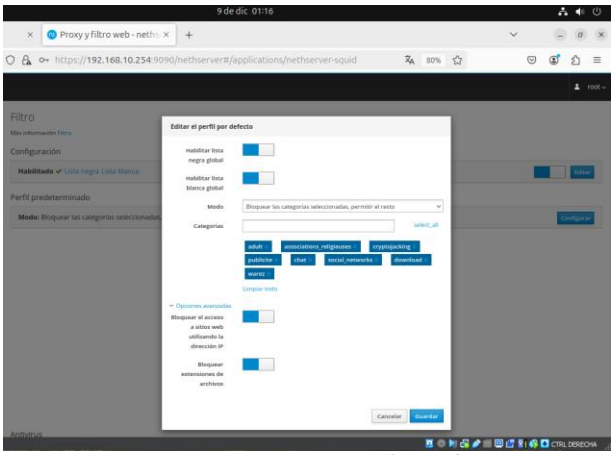

Fig. 35 – Configuración del Filtrado Web

Se finaliza ingresando a la pagina y no se visualiza el ingreso a la pagina

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

DESARROLLO DEL TEMARIO 4

*El uso de un servidor LDAP (Lightweight Directory Access Protocol) permite centralizar la gestión de usuarios, grupos y recursos en una red. En este caso, se configurará **OpenLDAP**, una implementación de código abierto ampliamente utilizada para gestionar directorios basados en LDAP. A continuación, se detallan los pasos necesarios para instalar y configurar un servidor LDAP en un sistema basado en **Ubuntu**.*

- *Instalación y configuración del servidor LDAP*
- *Instalar el servidor LDAP, como OpenLDAP:* ***sudo apt install slapd ldap-utils***
- *Configurar el dominio LDAP durante la instalación: Nombre del dominio:* ***dc=servidor-unad,dc=edu,dc=co.***

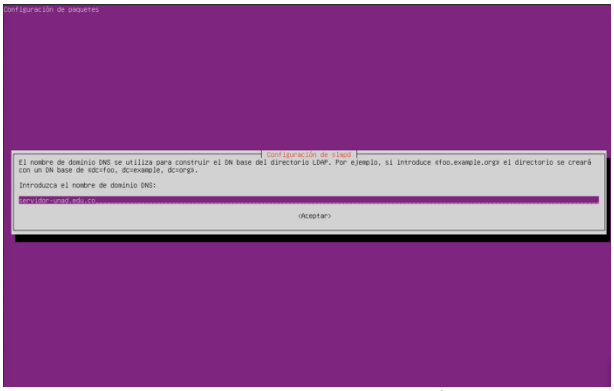

Fig. 36 – Instalación del Servidor LDAP

Una vez instalado, se puede verificar que el servidor LDAP esté funcionando correctamente con el siguiente comando:

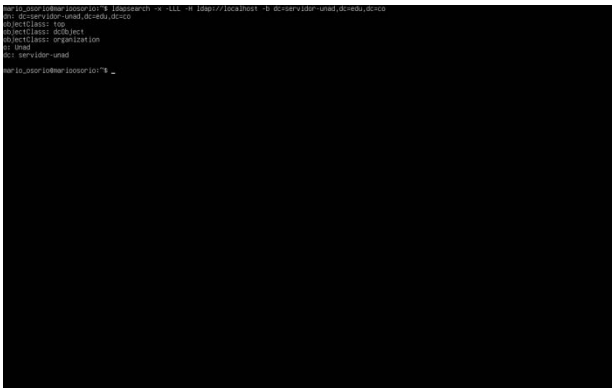

Fig. 37 – Instalación del Servidor LDAP II

Este comando realiza una búsqueda simple en el directorio LDAP en la base de ***dc=servidor-unad,dc=edu,dc=co.***

- *ldapsearch -x -LLL -H ldap://localhost -b dc=servidor-unad,dc=edu,dc=co*
- *Configuración de nombre de dominio y base de datos*

Fig. 38 – Configuración de Dominio

Creación de Usuarios y Grupos con LDIF los usuarios y grupos se crean mediante archivos LDIF, que contienen las definiciones de las entradas a añadir al directorio LDAP. Un archivo LDIF para crear un usuario y un grupo.

Para añadir este archivo al servidor LDAP, se usa el comando:

- *sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/core.ldif*

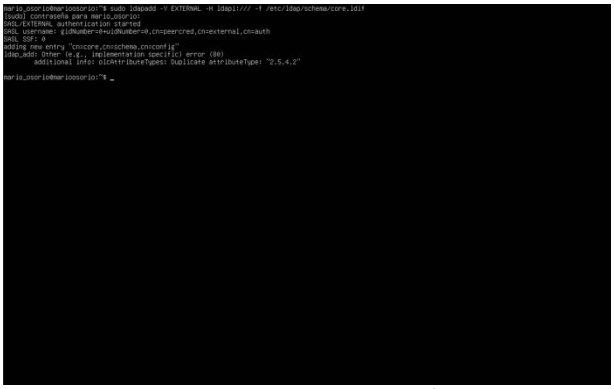

Fig. 39 – Ejecución de comandos LDPA

Este comando añade las entradas de usuario y grupo definidas en el archivo ***LDIF****.*

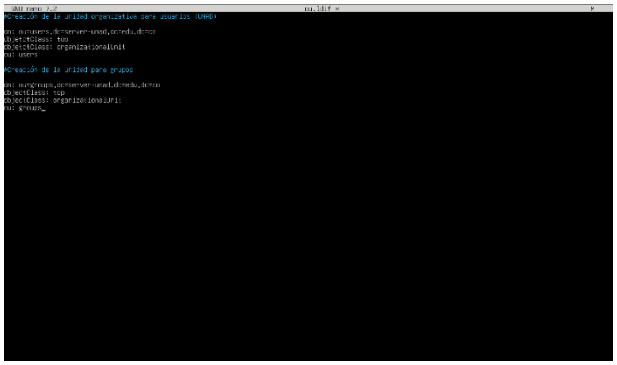

Fig. 40 – Ejecución de comandos LDIF

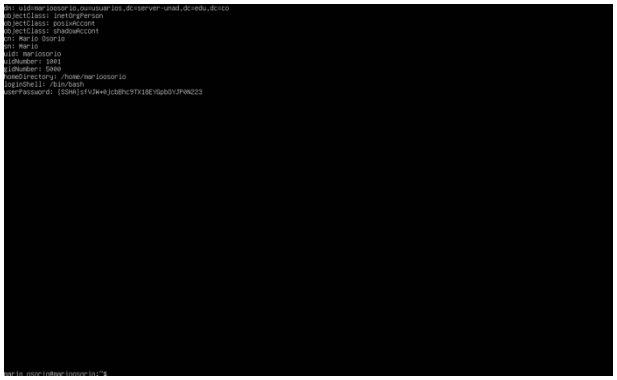

Fig. 41 – añadirlos con ldapadd.

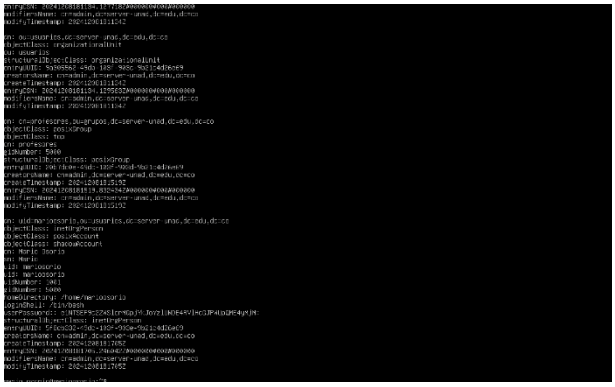

Fig. 42 – Resultado.

Configuración del Servidor de Archivos (File Server): Samba *es una implementación del protocolo SMB/CIFS que permite compartir archivos e impresoras entre sistemas Linux. En este caso, se configurará Samba para utilizar* ***LDAP*** *como backend para la autenticación y gestión de usuarios.*

Para instalar Samba en un sistema Ubuntu, se utiliza el siguiente comando:

.

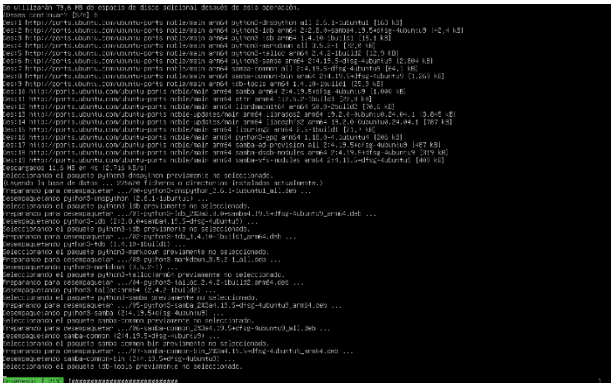

Fig. 43 – Instalador del servidor samba

- *sudo apt install samba*

*La configuración de Samba se realiza editando el archivo /etc/samba/smb.conf. Para integrar **LDAP** como backend de autenticación, se añaden las siguientes líneas en la sección [global]*

- *workgroup = UNAD*
- *security = user*
- *passdb backend = ldapsam:ldap://servidor-unad*
- *ldap suffix = dc=servidor-unad,dc=edu,dc=co*
- *ldap admin dn = cn=admin,dc=servidor-unad,dc=edu,dc=co*
- *ldap user suffix = ou=usuarios*
- *ldap group suffix = ou=grupo*
- *ldap machine suffix = ou=computers*

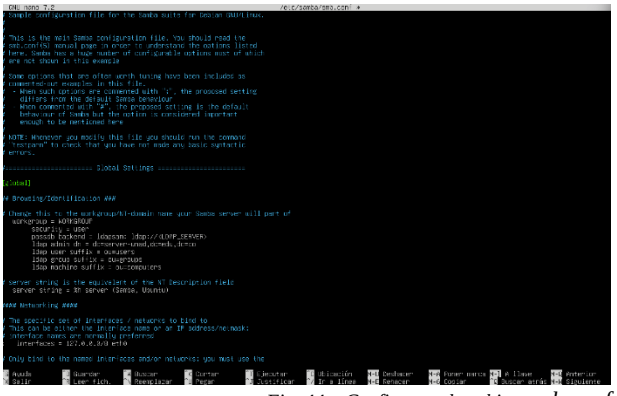

Fig. 44 – Configurar el archivo smb.conf

Definir carpetas compartidas en el archivo de configuración de Samba, también es necesario definir las carpetas que se compartirán en la red. Para ello, se añade una sección como la siguiente:

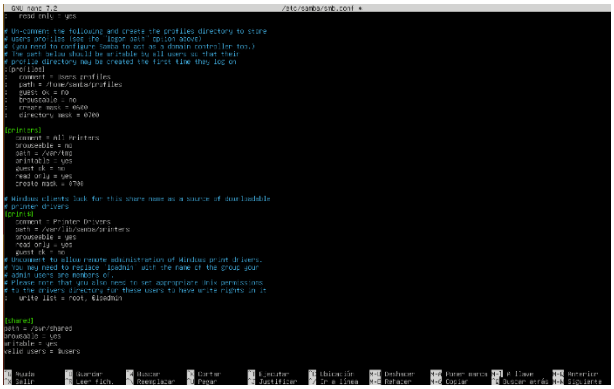

Fig. 45 – Editar el archivo smb.conf

- *ini*
- *[shared]*
- *path = /srv/shared*
- *browseable = yes*
- *writable = yes*
- *valid users = @users*

Una vez configurado el archivo smb.conf, se crea el directorio compartido y se ajustan los permisos adecuados para garantizar que los usuarios puedan acceder y modificar los archivos según sea necesario.

*Estos comandos crean la carpeta compartida, asignan el grupo **users** y establecen permisos de lectura y escritura para los miembros del grupo.*

Fig. 45 – Creación de Grupos

Pruebas del servidor de archivos, Después de configurar Samba, es necesario reiniciar el servicio para que los cambios en la configuración surtan efecto.

Fig. 46 – Reinicio del servicio

- *sudo systemctl restart smbd nmbd*

Una vez configurado el servidor de archivos con Samba, es importante verificar que otros dispositivos en la red puedan acceder correctamente al recurso compartido.

*Se abre el **gestor de archivos** (como Nautilus en Ubuntu) y en la barra de direcciones se escribe la dirección del servidor Samba, precedida de smb://: Si todo está configurado correctamente, el recurso compartido debe ser accesible*

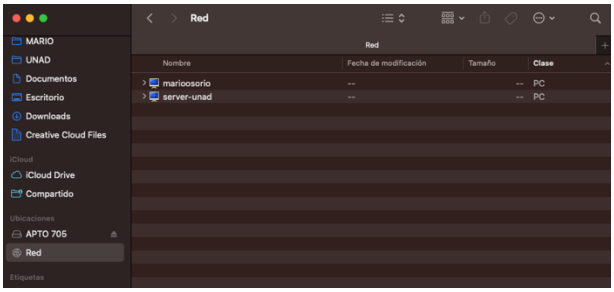

Fig. 47 – Gestor de Archivos

El Common UNIX Printing System (CUPS) es un sistema de impresión que permite compartir impresoras en una red, ya sea local o a través de Samba. Aquí se describen los pasos para instalar y configurar un servidor de impresión con CUPS.a. Instalación de CUPS.

- *sudo apt install cups*

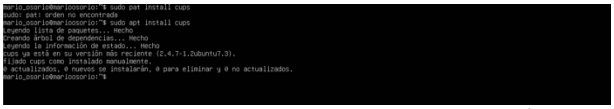

Fig. 48 – Instalación de Cups

Para permitir que las impresoras sean accesibles desde la red local, se debe editar el archivo de configuración de CUPS /etc/cups/cupsd.conf y habilitar el acceso desde la red local.conf, Se edita el archivo con un editor de texto:

Agrega o modifica las siguientes líneas en la configuración:

- *Listen *:631*
- *<Location />*
- *Order allow,deny*
- *Allow @LOCAL*
- *</Location>*

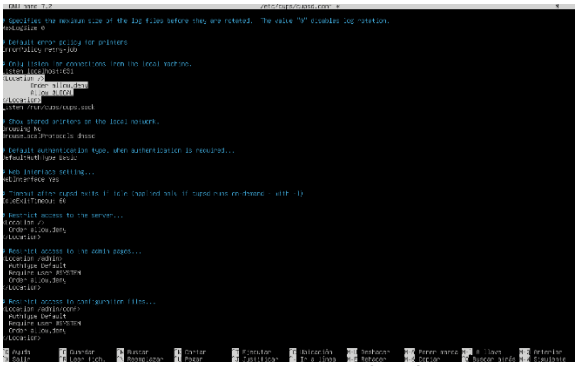

Fig. 46 – Modificación de archivo cupsd.conf

Para agregar impresoras al servidor CUPS, puedes hacerlo a través de la interfaz web de CUPS. Accede a la interfaz de administración de CUPS abriendo un navegador web y dirigiéndote a http://localhost:631 Desde aquí, podrás agregar impresoras locales o de red y configurar sus opciones de compartición.
*Para compartir impresoras a través de **Samba** y permitir que los usuarios de Linux accedan a ellas, es necesario configurar Samba. **Editar el archivo de configuración de Samba** (/etc/samba/smb.conf) para incluir la sección de impresoras:*

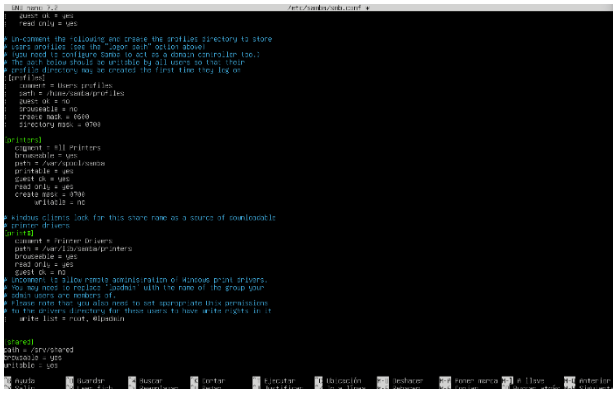

Fig. 47 – Modificación de archivo /smb.conf

- *ini*
- *[printers]*
- *comment = All Printers*
- *path = /var/spool/samba*
- *browseable = yes*
- *guest ok = yes*
- *writable = no*
- *printable = yes*

*Después de realizar las configuraciones, es necesario reiniciar los servicios de **Samba** y **CUPS** para aplicar los cambios:*

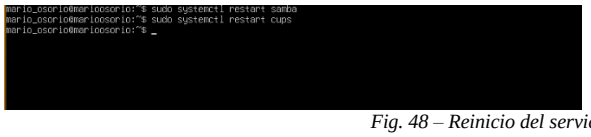

Fig. 48 – Reinicio del servicio

- *sudo systemctl restart smbd nmbd cups*

Para que una estación de trabajo GNU/Linux pueda integrarse al dominio LDAP y acceder a los recursos centralizados (como usuarios y grupos), se deben instalar los paquetes necesarios y configurar la conexión LDAP.

Fig. 49 – Instalación Librerias

- *sudo apt install libnss-ldap libpam-ldap ldap-utils*

*Durante la instalación de los paquetes anteriores, se te pedirá que configures la conexión **LDAP**. Debes ingresar la siguiente información:*

- *(ldap://servidor-unad), la base DN (dc=servidor-unad,dc=edu,dc=co) y el usuario admin.*

*Para que la estación de trabajo GNU/Linux pueda utilizar **LDAP** para la resolución de usuarios y grupos, es necesario modificar el archivo de configuración /etc/nsswitch.conf.*

*Se edita el archivo /etc/nsswitch.conf para habilitar el acceso a **LDAP** para las bases de datos de usuarios, grupos y contraseña*

- *sudo nano /etc/nsswitch.conf*

Dentro de este archivo, busca las siguientes líneas y cámbialas de esta forma:

- *passwd: compat ldap*
- *group: compat ldap*
- *shadow: compat ldap*

*Esto configura el sistema para que busque información de usuarios, grupos y contraseñas en **LDAP**, además de en los archivos locales del sistema.*

*Se deben instalar las herramientas necesarias para acceder a recursos compartidos utilizando el protocolo **SMB/CIFS**:*

- *sudo apt install cifs-utils*

Fig. 50 – Instalación cifs-utils

Para montar una carpeta compartida de Samba en el sistema, ejecuta el siguiente comando, reemplazando <samba_server> por la IP o nombre de host del servidor Samba, <ldap_user> por el nombre de usuario LDAP, y <password> por la contraseña correspondiente:

- *sudo mount -t cifs //<samba_server>/shared /mnt/shared -o username=<ldap_user>,password=<password>,domain=UNAD*

*Este comando monta la carpeta compartida **shared** desde el servidor Samba en el directorio /mnt/shared del sistema local.*

Para que el montaje de la carpeta compartida sea permanente y se monte automáticamente al arrancar el sistema, edita el archivo /etc/fstab:

- *sudo nano /etc/fstab*

Se añade la siguiente línea al final del archivo, reemplazando <samba_server> con la IP o nombre del servidor Samba y <ldap_user> con el nombre del usuario LDAP:

- *fstab*
- *//<samba_server>/shared /mnt/shared cifs credentials=/etc/smbcredentials,iocharset=utf8,sec=ntlmssp 0 0*

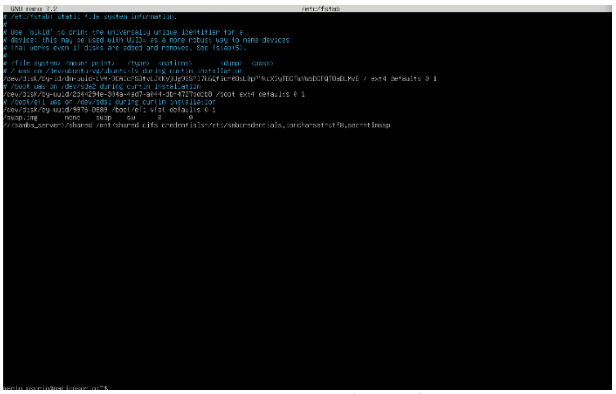

Fig. 51 – Configuración del archivo ldap_user

Para acceder a las impresoras compartidas a través de CUPS desde una estación de trabajo GNU/Linux, Se debe instalar el cliente de CUPS para permitir que la estación de trabajo acceda a las impresoras compartidas.

Fig. 52 – install cups-client

- *sudo apt install cups-client*

Una vez instalado CUPS, puedes configurar la impresora utilizando la interfaz gráfica de CUPS o desde la línea de comandos.

Para agregar la impresora desde la línea de comandos, ejecuta el siguiente comando, reemplazando Printer_Name por el nombre de la impresora y servidor-unad por la dirección del servidor CUPS.

– *lpadmin -p Printer_Name -E -v ipp://servidor-unad:631/printers/Printer_Name -m everywhere*

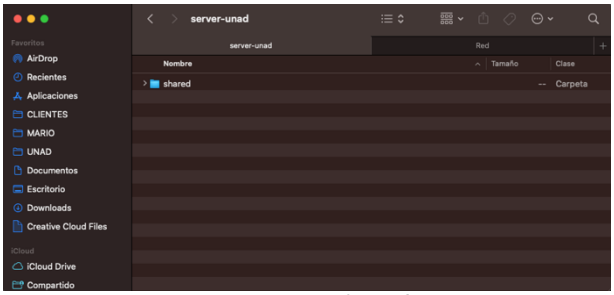

Fig. 53 – Confirmación de Carpeta compartida

Este comando añade la impresora Printer_Name al sistema y la habilita para su uso. La opción -v especifica la URL del servidor CUPS, y -m everywhere indica que se utilizará un controlador genérico para la impresora.

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.

DESARROLLO DEL TEMARIO 5

El primer paso en la implementación de la VPN fue la creación de una máquina virtual (VM) que alojaría el servidor NethServer. Esta máquina virtual se configuró utilizando un software de virtualización como VirtualBox o VMware.

El primer paso en la implementación de la VPN fue la creación de una máquina virtual (VM) que alojaría el servidor NethServer. Esta máquina virtual se configuró utilizando un software de virtualización como VirtualBox.

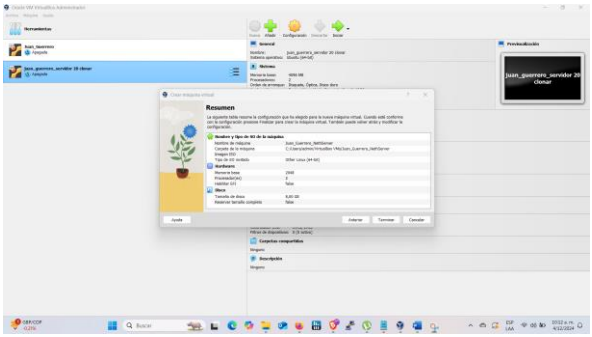

Fig. 54 – Configuración de la máquina virtual

Se eligió un sistema operativo Linux de 64 bits para instalar NethServer. La asignación de recursos fue de al menos 2 GB de RAM y 20 GB de espacio en disco duro, para asegurar que el servidor pudiera manejar las conexiones y el tráfico generado por la VPN.

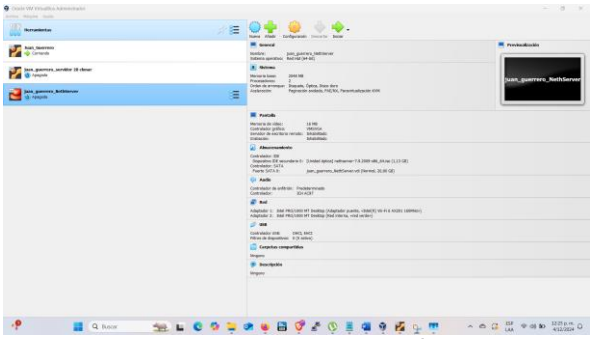

Fig. 55 – Validación de la maquina virtual

Una vez que la máquina virtual fue creada, el siguiente paso fue instalar el sistema operativo NethServer. Para ello, se utilizó una imagen ISO descargada desde la página oficial de NethServer.

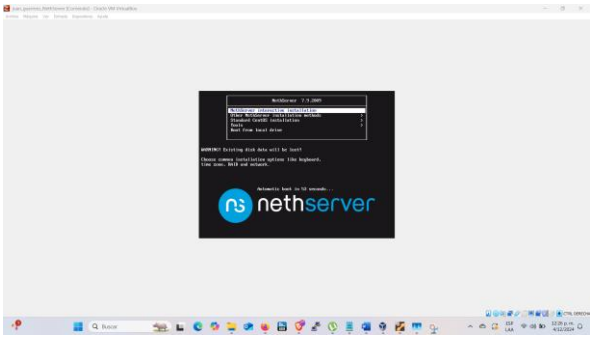

Fig. 56 – Instalación del sistema NethServer

Se montó la imagen ISO en la máquina virtual y se inició el proceso de instalación. Durante la instalación, se seleccionaron el idioma y la región adecuada, y se configuraron los parámetros básicos de red.

En este paso, se asignó una dirección IP estática a la interfaz LAN de NethServer, garantizando que el servidor tuviera una dirección IP fija dentro de la red local.

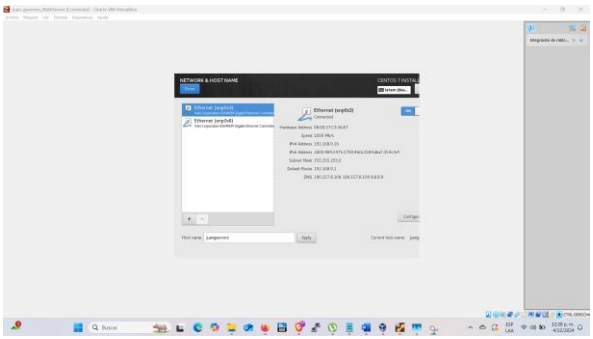

Fig. 57 – Configuración de Adaptador de red

*Durante la instalación, se configuró la contraseña del usuario **root**, quien es el administrador del sistema. Es fundamental que esta contraseña sea segura, ya que el acceso al sistema y sus configuraciones depende de ella.*

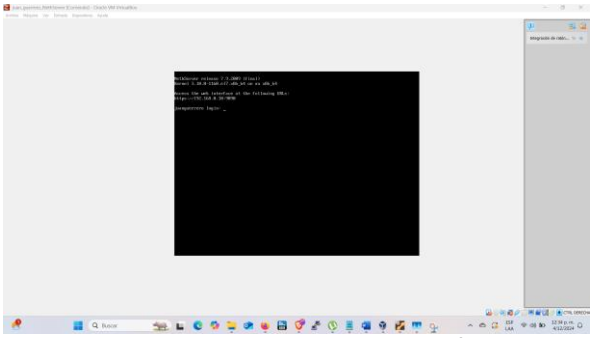

Fig. 58 – Finalización de la instalación

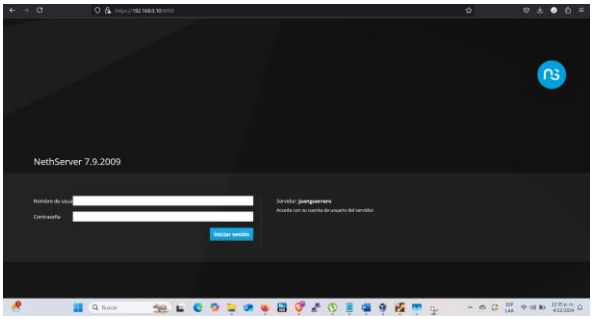

Fig. 59 – Inicio de sección.

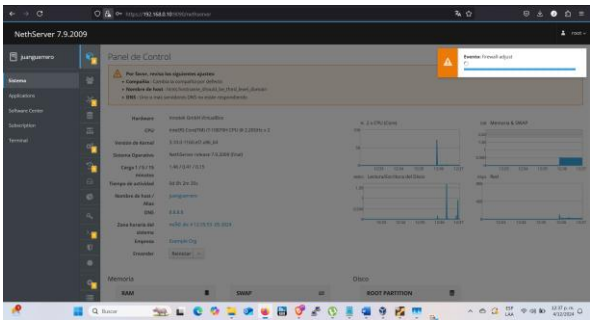

Fig. 60 – Panel de control de Netserver

Una vez instalado NethServer, se procedió a la configuración de la red desde la interfaz web de administración del sistema, accesible a través de un navegador web.

*En la interfaz web de NethServer, se accedió a la sección de configuración de redes y se asignó la interfaz **enp0a3** como la interfaz **WAN**, lo que le permitió conectarse a Internet*

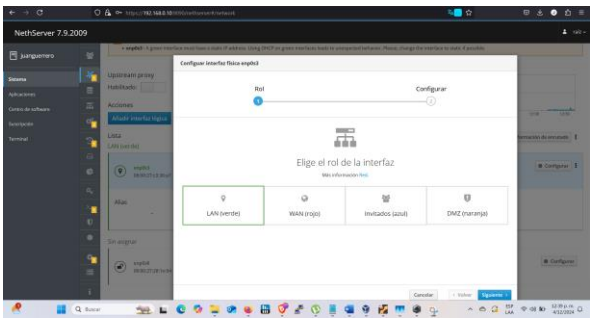

Fig. 61 – Configuración del acceso WAN

*Después de aplicar la configuración, se verificó que la red **enp0a3** estuviera correctamente configurada como la interfaz de acceso WAN y que la red LAN estuviera configurada adecuadamente para la comunicación interna. Este proceso se completó con éxito y la máquina estaba lista para recibir conexiones externas*

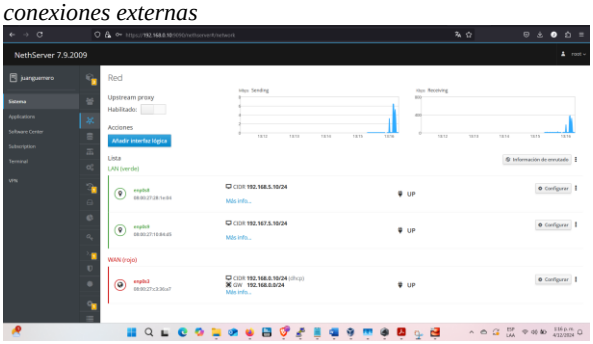

Fig. 62 – Estado de la tarjeta de WAN

*NethServer incluye un **Software Center** que permite buscar, instalar y gestionar aplicaciones. Para configurar la VPN, se accedió a esta herramienta desde el panel de administración web*

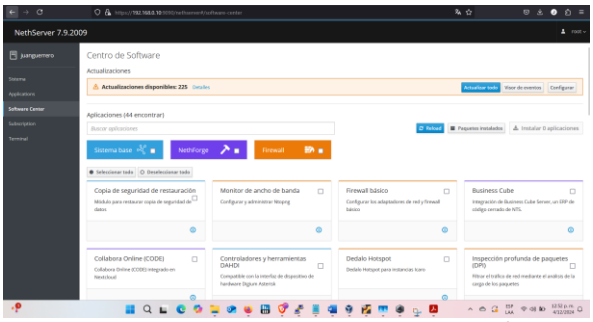

Fig. 63 – Software Center

*A través del **Software Center**, se buscó e instaló el paquete correspondiente para gestionar conexiones VPN, en este caso **OpenVPN**. Este paquete proporciona las herramientas necesarias para configurar y gestionar una red privada virtual segura en el servidor.*

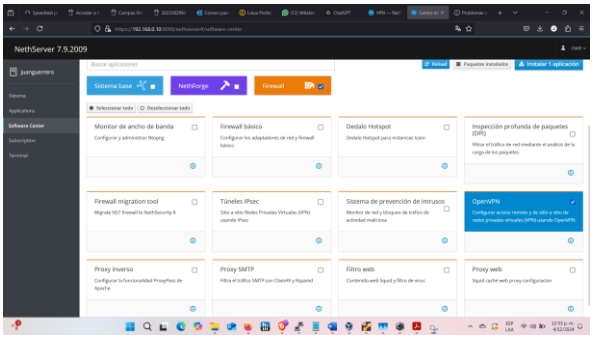

Fig. 64 – Modelo de Instalación OpenVPN

Vemos que está instalando la aplicación que acabamos a elegir en el Software Center.

*Buscamos el paquete para **Tuneles IPSec** y procedemos a instalarlo. Este complemento permite la creación de túneles de comunicación segura utilizando el protocolo IPSec, una opción comúnmente utilizada en redes empresariales para garantizar la privacidad y la integridad de los datos transmitidos.*

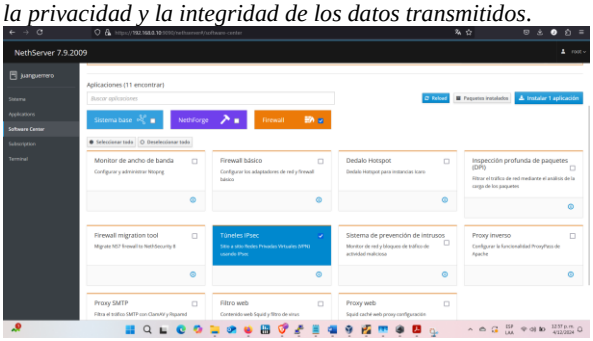

Fig. 65 – Modulo de Instalación Tuneles IPSec

Una vez que el complemento IPSec está instalado, podemos ver en la interfaz de NethServer que las herramientas VPN están disponibles y configurables.

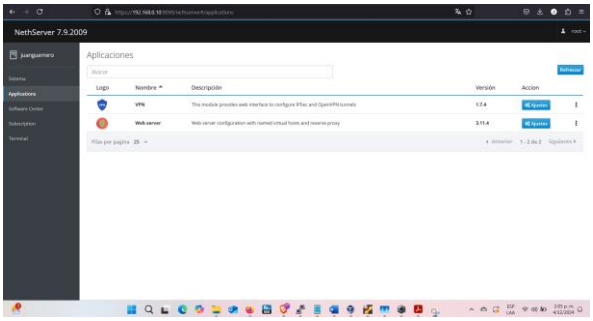

Fig. 66 – Aplicaciones

*Esto se valida revisando la sección de aplicaciones instaladas en el **Panel de Control** de NethServer, donde aparece la opción para configurar túneles IPSec.*

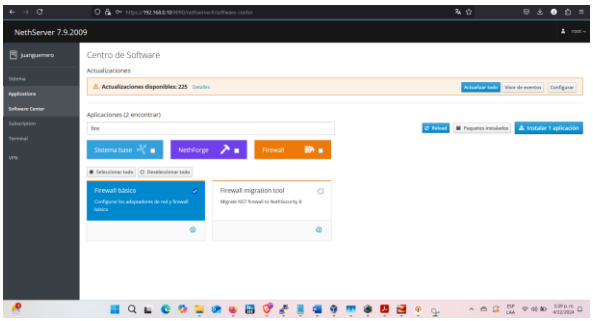

Fig. 67 – Confirmación de Aplicaciones Instaladas

*El primer paso en la configuración es asegurarse de que el servidor tiene el **nombre de host** adecuado, lo que facilitará la identificación de la máquina dentro de la red*

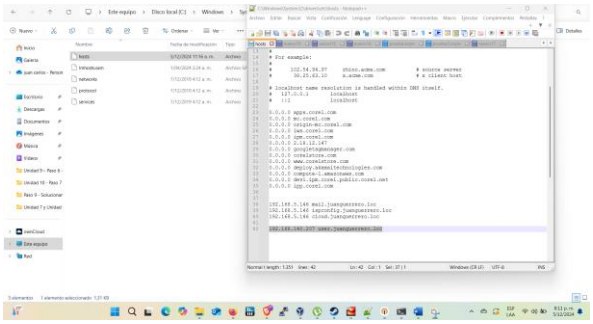

Fig. 68 – Configuración de Host

*En la interfaz de administración de NethServer, se accede a la sección de **Redes** y se configura una nueva subnet con la dirección IP **192.168.5.10**. Esta dirección se asigna a la interfaz que se utilizará para las conexiones VPN, asegurando que los clientes de VPN puedan comunicarse con la red interna del servidor.*

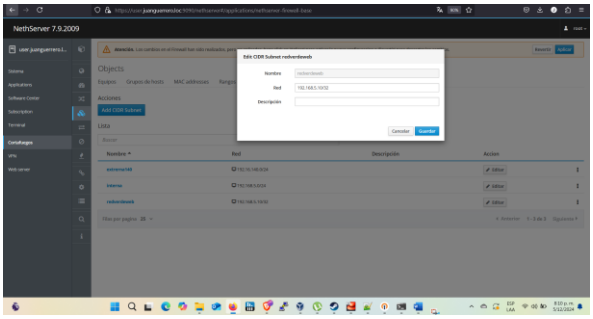

Fig. 69 – redes subnet.

*Para permitir que cualquier cliente pueda acceder a la red interna de la VPN, se configura la subnet con la dirección **0.0.0.0/0**. Esto significa que cualquier dirección IP de cliente dentro del rango de la red privada podrá acceder a la red interna a través del túnel VPN. Esta configuración es útil en escenarios donde se desea habilitar el acceso a toda la red interna sin restricciones adicionales.*

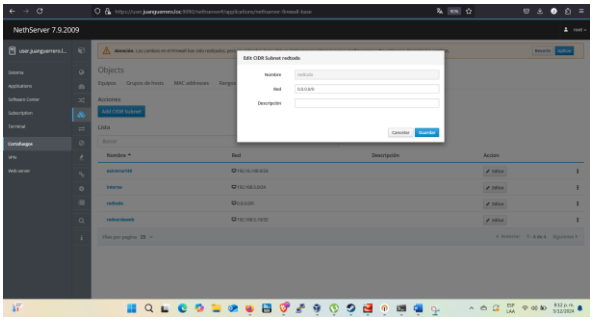

Fig. 70 – Configuración de la VPN

*Después de configurar las subredes, podemos verificar que las redes creadas estén correctamente configuradas. En la pantalla de **Redes**, las subredes previamente creadas se muestran como parte de la infraestructura de red de NethServer, lo que indica que la configuración es correcta.*

.

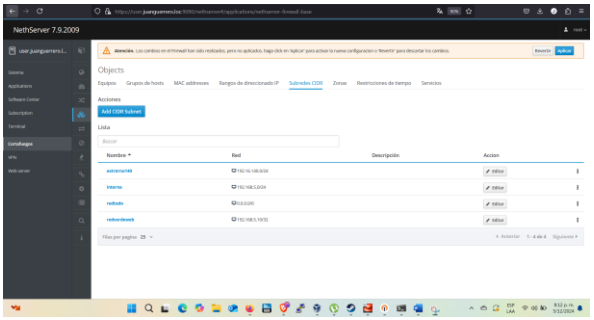

Fig. 71 – Redes subnet creadas.

*Desde la interfaz web de NethServer, se accede a la sección **Túneles IPSec**..*

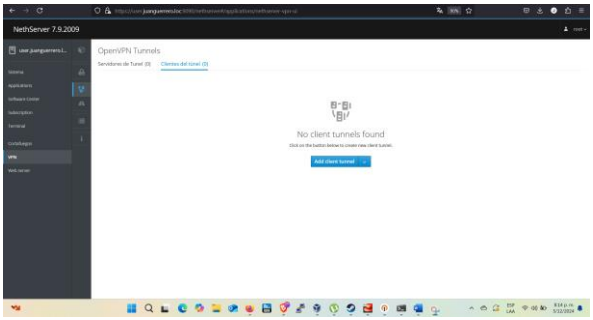

Fig. 72 – creación de VPN

*En esta pantalla, se configura un nuevo túnel para permitir la conexión de los clientes VPN. La dirección de la red interna que se define para este túnel es **192.168.5.10/24**, lo que indica que toda la red **192.168.5.x** estará accesible para los clientes VPN.*

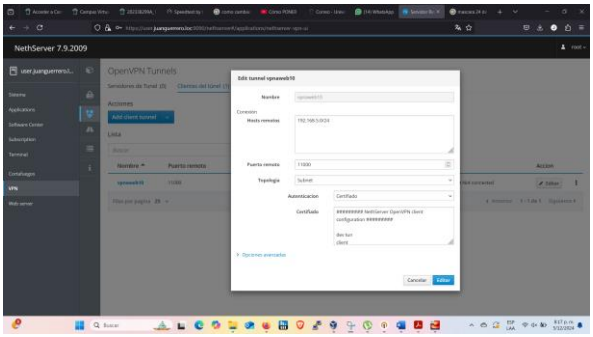

Fig. 73 – Creación de Tunnel.

Podemos ver el túnel que hemos creado.

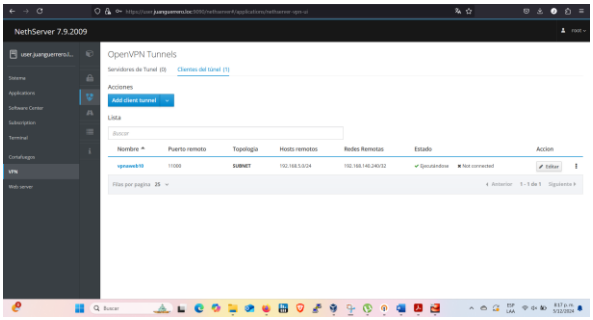

Fig. 74 – Tunnel creado.

Vamos a configurar la regla de la VPN.

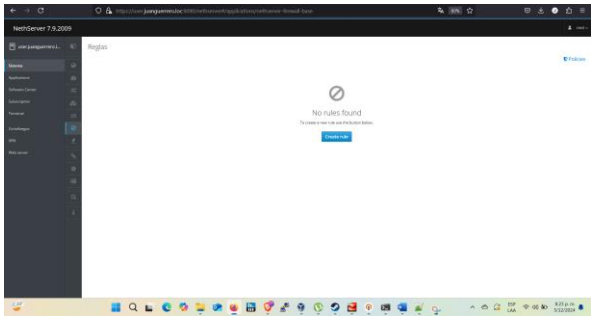

Fig. 75 – creación reglas

*La regla se configura de manera que cualquier tráfico proveniente de clientes VPN sea permitido para acceder a la red **192.168.5.10**. Además, se configura para que el tráfico sea permitido por todos los puertos, asegurando que los clientes puedan acceder a cualquier recurso dentro de la red.*

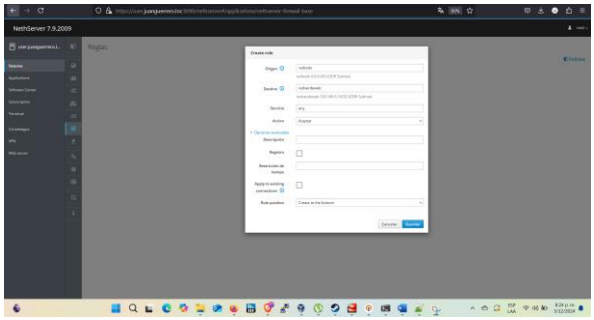

Fig. 76 – Creando reglas

*En la interfaz de administración de NethServer, podemos visualizar la regla de acceso creada previamente para la VPN. En esta sección, se define el **origen** y **destino** del tráfico que se permitirá a través del túnel IPSec..*

Una vez que las reglas de acceso están configuradas, el siguiente paso es crear un certificado para el usuario de la VPN. vamos a asignar las siguientes IP´s.

Nombre de usuario: Vpnreal
IP Reservada: 192.168.5.15
VPN Remote: 192.168.5.16
VPN netmask: 255.255.255.0

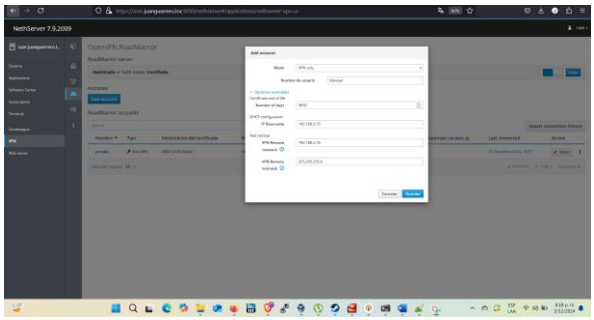

Fig. 77 – Configuración usuario de VPN

*Después de configurar el usuario, se puede visualizar que la VPN, llamada **vpnreal**, está configurada correctamente y lista para ser utilizada.*

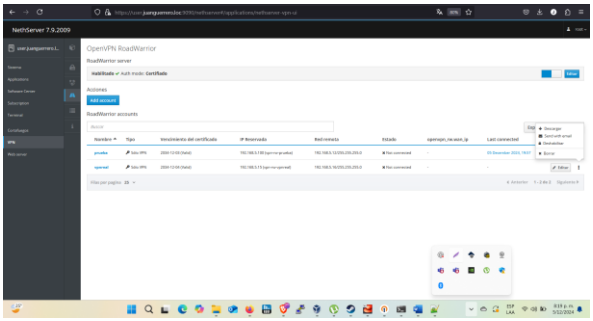

Fig. 78 – VPN creadas.

*El siguiente paso es descargar el certificado generado para el usuario **Vpnreal**, el cual se utilizará para la autenticación y la conexión a la VPN.*

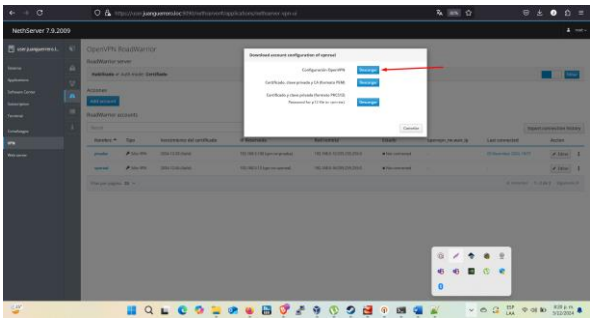

Fig. 79 – Descargar certificado de VPN

Una vez descargado el certificado, podemos evidenciar que el archivo ha sido correctamente descargado en el equipo local. Este archivo será utilizado en la configuración del OpenVPN para establecer la conexión segura.

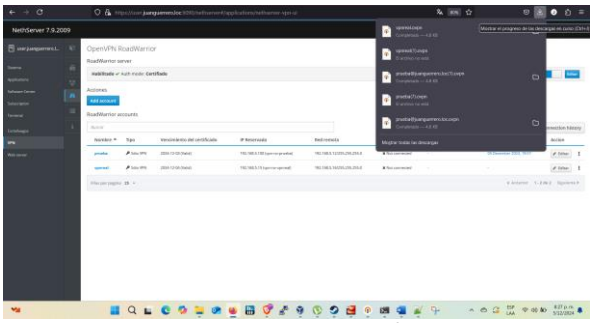

Fig. 80 – Certificado de VPN descargado

*El archivo de certificado descargado se abre con un editor de texto para realizar las modificaciones necesarias. En este caso, se cambia la **IP** por el **nombre de host** previamente asignado al servidor en NethServer, que simula una IP pública para la conexión remota.*

Fig. 81 – Modificación de Certificado.

*Se sustituye la dirección IP de la VPN por el nombre **user.juanguerrero.loc**, el cual fue establecido previamente como el nombre del host del servidor.*

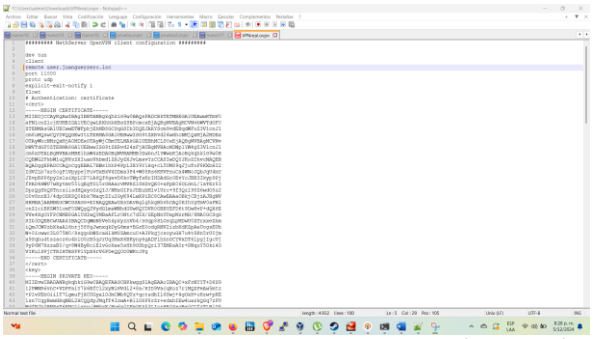

Fig. 82 – Certificado Modificado.

Después de realizar las modificaciones, el certificado queda listo para ser utilizado en el cliente VPN. La configuración con el nombre de host simula el uso de una IP pública, facilitando la conexión remota.

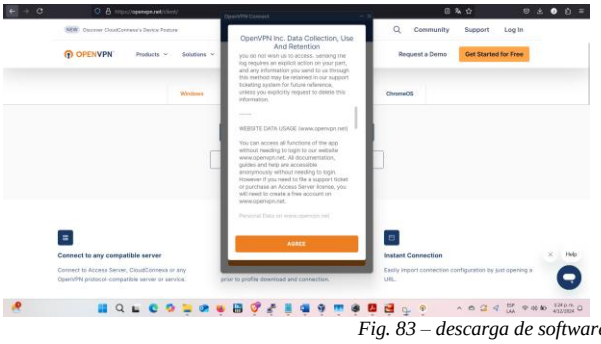

Fig. 83 – descarga de software.

Una vez que el certificado está modificado y listo, el siguiente paso es instalar el software cliente OpenVPN en la estación de trabajo y cargar el certificado para completar la configuración de la conexión.

.

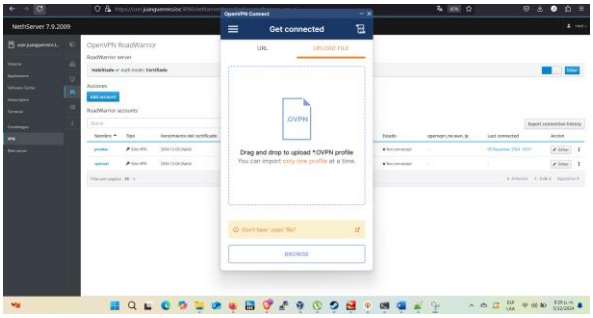

Fig. 84 – certificado de VPN

Después de la instalación, se inicia el cliente OpenVPN y se carga el certificado previamente modificado. Este certificado contiene la configuración necesaria para que el cliente se autentique y se conecte al servidor VPN de manera segura.

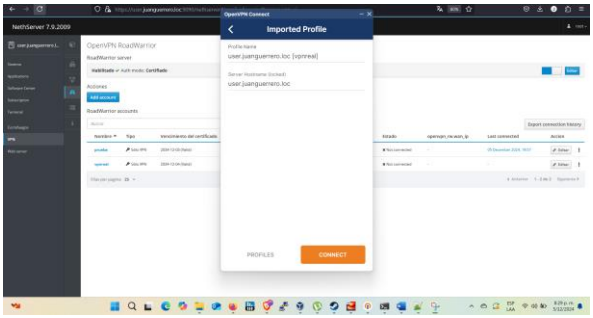

Fig. 85 – VPN cargado

Podemos ver que ya estamos conectado a la VPN.

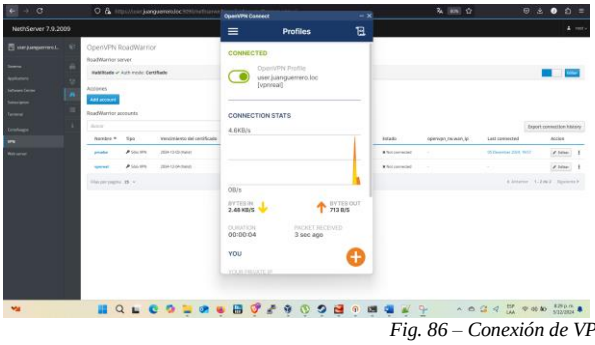

Fig. 86 – Conexión de VPN

*Desde una máquina cliente que está conectada a la VPN, se realiza un **ping** a la dirección IP **192.168.5.10**. Dado que las reglas de firewall configuradas previamente permiten todo el tráfico hacia esta IP (por la configuración de la regla de acceso con **any**), el ping debe ser exitoso y responder sin problemas, lo que indica que la conexión VPN está operativa y la red interna es accesible.*

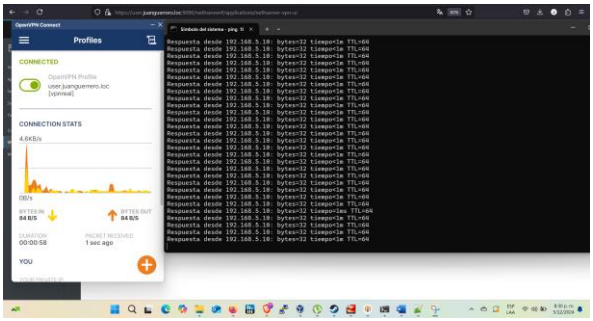

Fig. 87 – Prueba de funcionamiento de VPN.

Otra prueba que se realiza es desconectar la VPN y verificar que la ip 192.168.5.10 nos dejo de responder esto con el fin de verificar que realmente es por la VPN que estamos llegando a la ip 192.168.5.10.

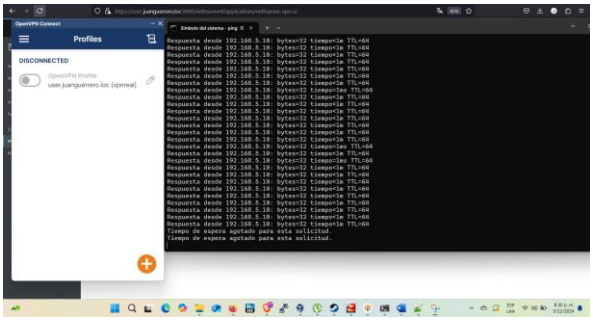

Fig. 88 – Prueba de funcionamiento de VPN.

Nos volvemos a conectar a la VPN para seguir haciendo pruebas a la IP 192.168.5.10 que fue a la que le aplicamos las reglas y permisos en el anterior proceso en este caso la prueba fue hacer una conexión por SSH que es el puerto 22 y evidenciamos que está en funcionamiento.

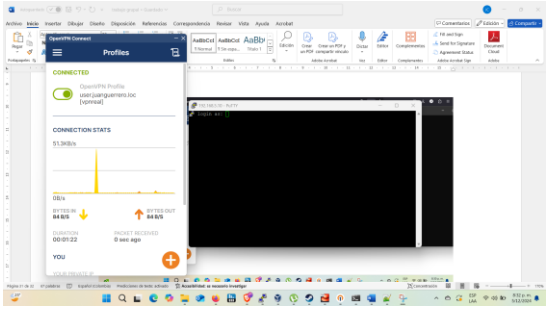

Fig. 89 – Resultado Exitoso

La prueba de SSH debe ser exitosa, lo que confirma que el puerto 22 está abierto y que el tráfico a través de la VPN se maneja correctamente según las reglas configuradas.

7. SUSTENTACIÓN DEL TRABAJO FINAL

Alumno	*Asignación*	*Video*
Diego Alexander	*Temario 1*	*https://youtu.be/VA5PZQOhQe4*

Zambrano Alayon		
Diego Alexander Zambrano Alayon	*Temario 2*	
Diego Alexander Castañeda Lizcano	*Temario 3*	*https://youtu.be/94DRRrsNIAk*
Mario Osorio Torres	*Temario 4*	*https://youtu.be/QSsR8JYatPc*
Juan Carlos Guerrero Ballen	*Temario 5*	*https://youtu.be/CZavsyLFZJE*

8. CONCLUSIONES

Temario 1 y Temario 2: *La actividad nos permite aplicar los conocimientos adquiridos durante las fases anteriores del proyecto, enfocándose en la implementación de servicios avanzados de infraestructura TI mediante NethServer en un entorno GNU/Linux basado en Ubuntu. Al trabajar en áreas específicas como DHCP, DNS, Controlador de Dominio y Proxy, se logró consolidar competencias clave en la configuración y administración de redes, servicios y sistemas operativos.*
El enfoque práctico y colaborativo facilitó el aprendizaje progresivo, integrando conceptos de redes, seguridad y administración de sistemas en un entorno realista. Además, la documentación técnica desarrollada como producto final refuerza la importancia de un diseño bien estructurado y la resolución efectiva de problemas en entornos de infraestructura TI. En resumen, la actividad no solo alcanzó su objetivo técnico, sino que también fortaleció habilidades críticas para enfrentar desafíos en sistemas complejos de Intranet y Extranet.

Temario 3: *La actividad demuestra la importancia de una configuración detallada en servidores de red, como NethServer, para asegurar una conectividad adecuada y segura. La asignación de direcciones IP, la configuración de DHCP y el establecimiento de un firewall son esenciales para gestionar el tráfico y la seguridad de la red, lo que garantiza una infraestructura eficiente y controlada.*

La implementación de servicios como el firewall Shorewall y el filtrado web con UFDBGuard refuerza la seguridad de la red, permitiendo controlar el acceso a internet y bloquear contenido inapropiado. Esto muestra cómo se pueden aplicar medidas efectivas para proteger la red interna y mejorar la navegación controlada.

Temario 4: *La implementación de un servidor LDAP con Samba es efectiva para la gestión centralizada de usuarios y recursos en redes.*

- *Permite gestionar credenciales, accesos a archivos e impresoras desde una única ubicación, simplificando la administración en redes grandes o distribuidas.*
- *La integración de LDAP con Samba crea un entorno seguro para que usuarios de estaciones de trabajo accedan a recursos compartidos.*
- *Ofrece flexibilidad y ventajas significativas en interoperabilidad entre distintos sistemas operativos en una red.*
- *Las medidas de seguridad implementadas aseguran accesos controlados y protegidos, reduciendo riesgos de accesos no autorizados y mejorando la confiabilidad del sistema.*

Temario 5*: La implementación de la VPN en NethServer fue exitosa, configurando adecuadamente la máquina virtual, las interfaces de red y los servicios de VPN (OpenVPN e IPSec), lo que permitió una conexión segura y eficiente para usuarios remotos.*

Las pruebas realizadas confirmaron el correcto funcionamiento de la VPN, con accesos seguros a la red interna mediante ping y SSH. La configuración de subredes, reglas de firewall y autenticación garantizó una comunicación protegida y estable.

9. REFERENCIAS

Roberto Murillo. (n.d.). https://www.youtube.com/watch?v=R7qNw06qOPs

Samba.org. (2023). Samba: Sitio Oficial. Recuperado de https://www.samba.org

OpenLDAP. (2023). El Proyecto OpenLDAP. Recuperado de https://www.openldap.org

Comunidad de Ayuda de Ubuntu. (2022). Autenticación Samba/LDAP. Recuperado de https://help.ubuntu.com/community/Samba/LDAPAuthentication

The Linux Documentation Project. (2021). Guía de LDAP. Recuperado de https://tldp.org/HOWTO/LDAP-HOWTO/

El Proyecto de Documentación de FreeBSD. (2020). Configuración de Samba con Backend LDAP. Recuperado de https://www.freebsd.org/doc/handbook/network-servers.html

UNAD. (2023). Manual de Administración de Red de la Universidad Nacional Abierta y a Distancia (UNAD). Recuperado de https://www.unad.edu.co

Linux Mint. (2021). Cómo Configurar un Servidor de Archivos Samba. Recuperado de https://linuxmint.com

Proftpd.org. (2022). Autenticación y Autorización LDAP. Recuperado de https://www.proftpd.org

.

NethServer descarga ISO
https://sourceforge.net/projects/nethserver/