GNU/Linux Nethserver (Instalar y configurar como sistema operativo base para disponer de los servicios de Infraestructura IT)

Giovani Alfonso Caicedo barrera
gacaicedob@unadvirtual.edu.co
Darcy Elena Rios
deriose@unadvirtual.edu.co
Juan Sebastián Higuita
jshiguitag@unadvirtual.edu.co
Anyi Yulieth Valencia Reyes
ayvalenciar@unadvirtual.edu.co

RESUMEN: Este trabajo se centra en la instalación y configuración de NethServer, una plataforma de código abierto para la gestión de servidores, y en el desarrollo de temáticas específicas relacionadas con la administración de redes. Las temáticas abordadas incluyen la configuración de un DHCP Server, un DNS Server, un Controlador de Dominio, un Proxy, un Cortafuegos y una VPN. Estos elementos son esenciales para garantizar un entorno de red seguro y eficiente.

PALABRAS CLAVE: controlador de dominio, DHCP server, file server, nethserver.

1 INTRODUCCIÓN

En el contexto de la creciente importancia de la infraestructura de red en entornos empresariales y académicos, la implementación adecuada de servicios de red se vuelve crucial. Este trabajo se enfoca en el uso de NethServer, una solución robusta y versátil, para abordar diversas temáticas que contribuyen al correcto funcionamiento y seguridad de una red.

2 INSTALACION DE NETHSERVER

NethServer es una distribución basada en Linux que está orientada específicamente a actuar como servidor en pequeñas y medianas oficinas. Esta distribución está basada en las populares distribuciones CentOS y Red Hat Enterprise Linux, Cuenta con variedad de funciones como lo son MailServer and Filter, WebServer, Groupware, Firewall, Web Filter, IPS/IDS, VPN.

2.1 ENLACE DE DESCARGA

https://www.nethserver.org/getting-started-with-nethserver/

2.2 CONFIGURACIÓN DE MÁQUINA VIRTUAL

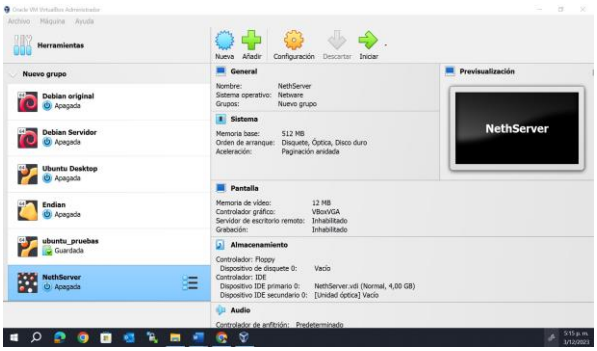

Ilustración 1. Configuración máquina virtual

Se inicia con la instalación recomendada de nethserver.

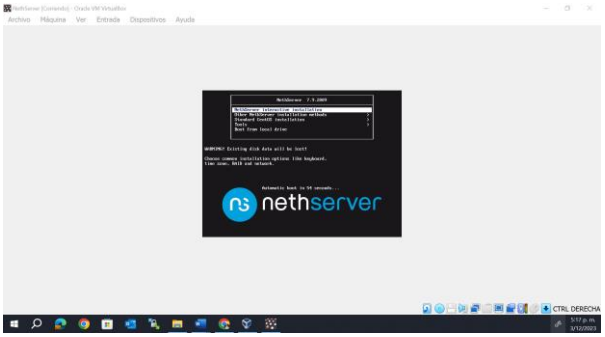

Ilustración 2. Instalación

Se realiza la configuración básica de inicio de la instalación del NethServer.

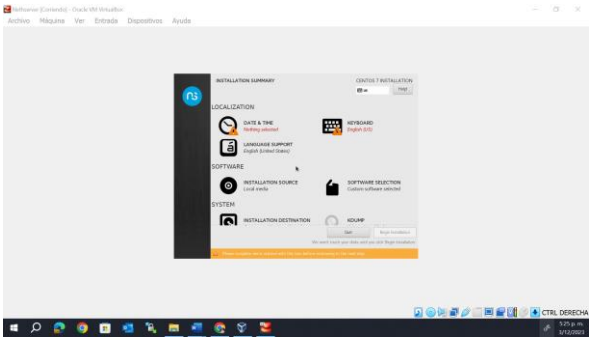

Ilustración 3. Configuración inicial - hora

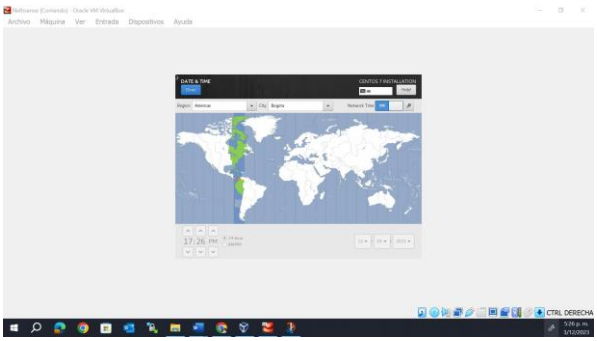

Ilustración 4. Configuración inicial - ubicación

Selección de idioma y sincronización de hora y fecha.

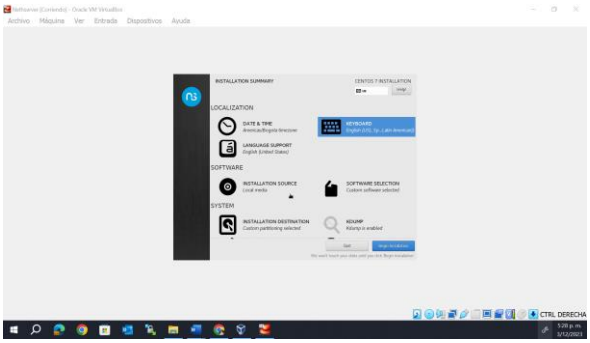

Ilustración 5. Configuración inicial - teclado

Instalación Nethserver

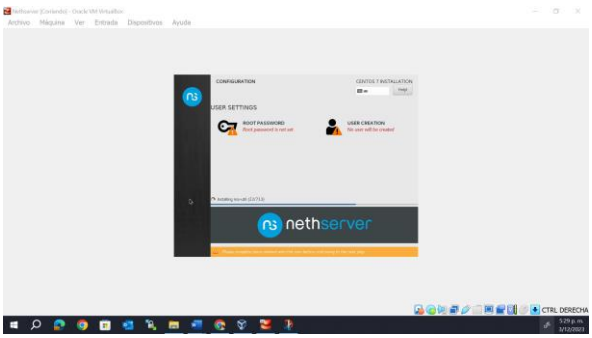

Ilustración 6. Configuración inicial. Autor propio - usuarios

Creación de la contraseña para el usuario root.

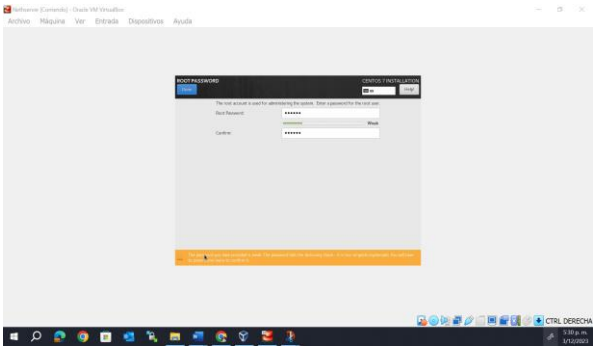

Ilustración 7. Configuración inicial - credenciales

Se realiza la validación de ingreso de la otra máquina virtual Ubuntu.

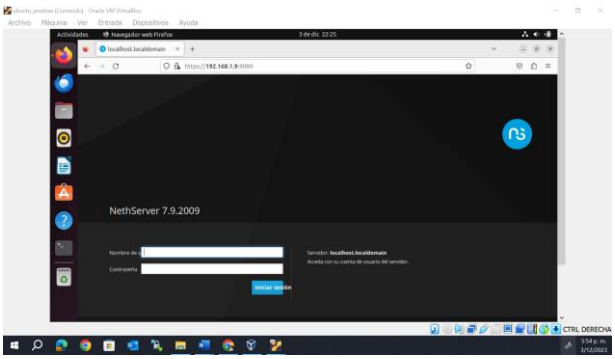

Ilustración 8. Configuración inicial

3 DESARROLLOD E LAS TEMATICAS

3.1 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.

Se ingresa a los servicios de nethserver, y se realizan las configuraciones de registro y proxy.

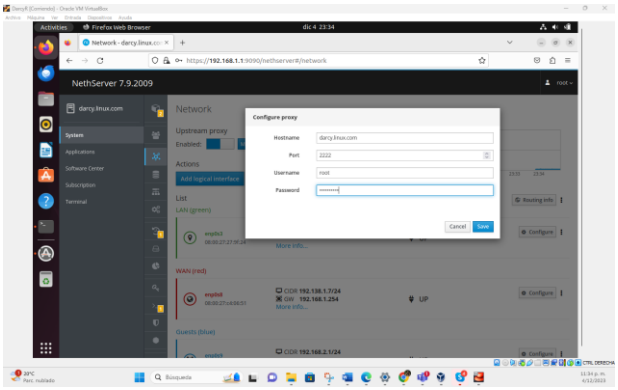

Ilustración 9. Configuración inicial

Primeramente, se configura la red de invitados como azul estático.

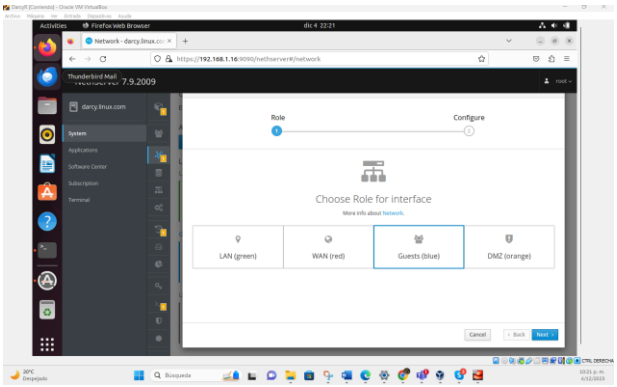

Ilustración 10. Configuración Red invitados.

Luego se configuran las interfaces emp0s3 LAN-Verde Emp0s8 WAN-Roja.

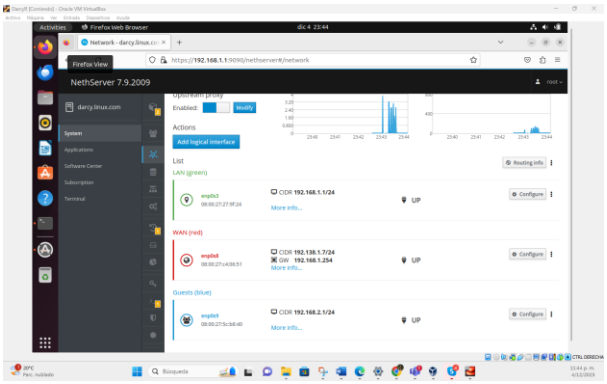

Ilustración 11. Configuración interfaces Verde, Roja y Azul

Se realiza la configuración en el servidor DHCP. Para enp0s3 LAN.

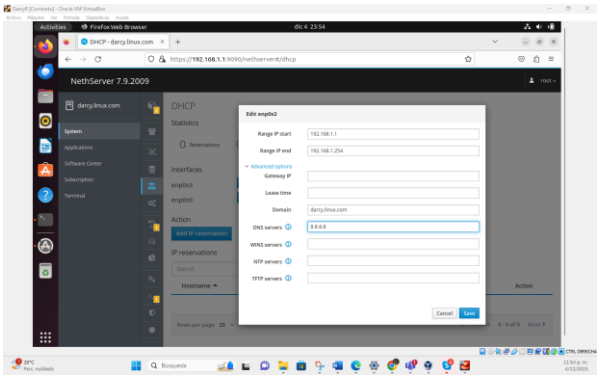

Ilustración 12. Configuración servidor DHCP, LAN.

Se registra en emp0s3 desde 191.168.1.1-192.168.1.254 y la reserva de direcciones IP en el servidor DHCP que se usaran por las diferentes estaciones de trabajo.

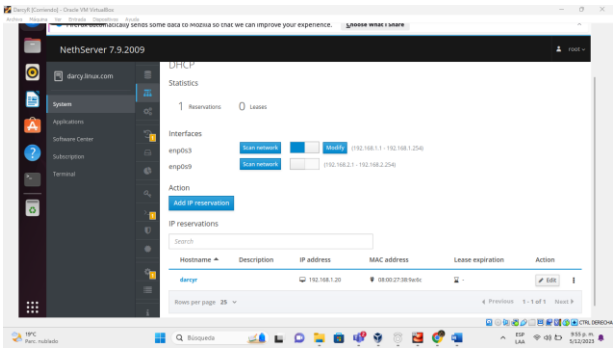

Ilustración 13. Creación reserva de direcciones IP en DHCP

Se comprueba iniciando sesión en Ubuntu. Así se garantiza que el controlador está activo.

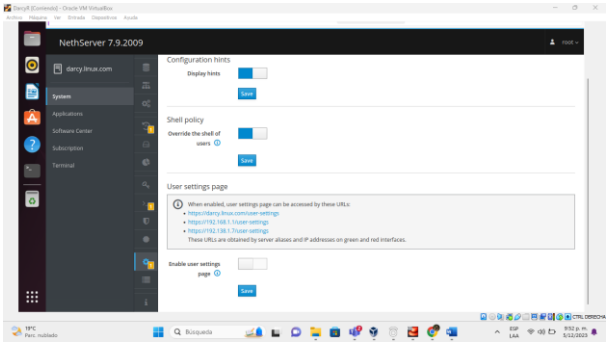

Ilustración 14. Comprobación de la creación del servicio. Autor propio

Evidencia de acceso desde fuera de la LAN a la red.

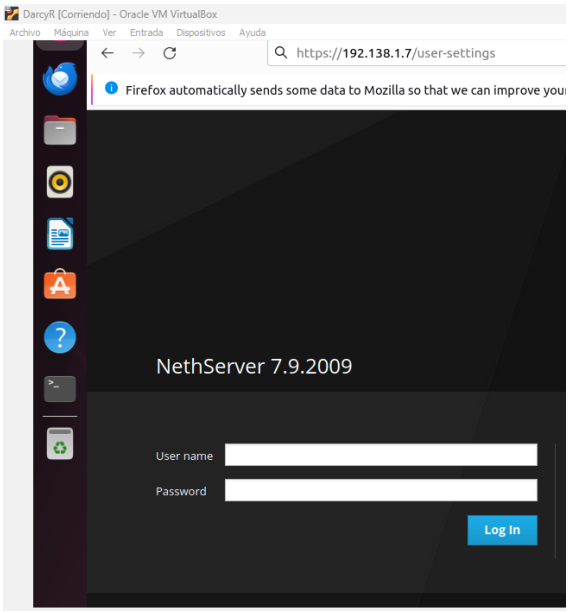

Ilustración 15. Validación acceso fuera de la LAN

Se realiza la configuración del servidor DNS.

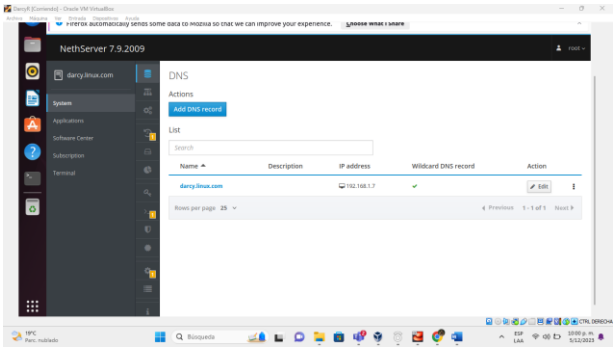

Ilustración 16. Configuración servidor DNS

Y por último se evidencia el registro en nethserver de los servicios de infra TI.

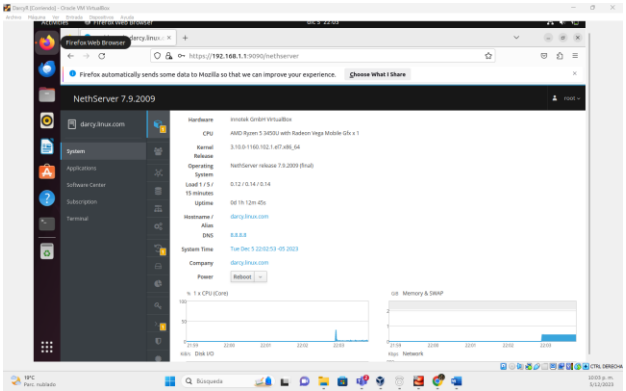

Ilustración 17. Evidencia Nethserver con servicios de infraestructura

3.2 TEMÁTICA 2: PROXY

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

Para el desarrollo de la temática se cuenta con el servidor ya instalado y configurado dentro de una zona DMZ, se arranca desde la web de administración a la cual se puede acceder de manera local y remotamente con el empleo de un navegador.

Al primer inicio se deben realizar algunas configuraciones previas.

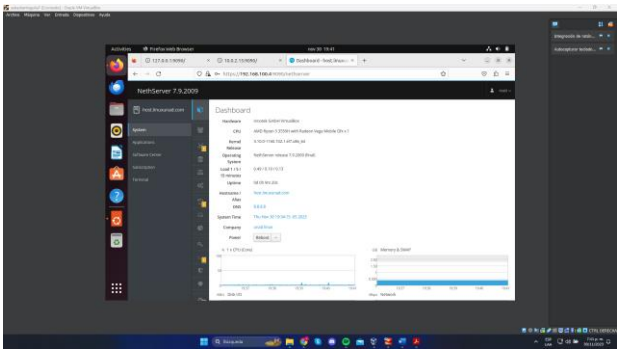

Ilustración 18- configuración inicial

Se instalan los componentes de firewall y proxy.

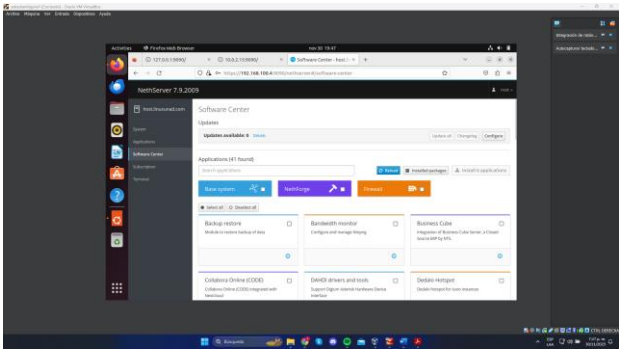

Ilustración 19 – instalación de aplicaciones

Se seleccionan los servicios necesarios para la práctica y su correcto funcionamiento.

- Web Proxy & filter.
- Firewall.

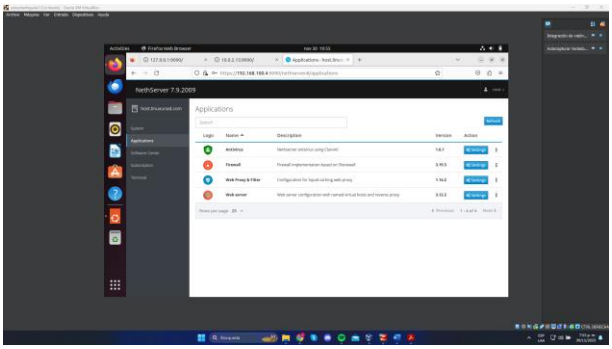

Ilustración 20- configuración de aplicaciones

Configuración zona verde, enp0s8 192.168.1.1 con máscara 24, esta configuración se realiza de manera estática.

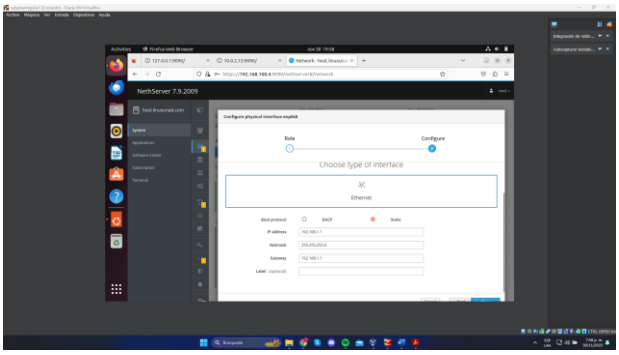

Ilustración 21 – configuraciones de red verde

Configuración zona roja, enp0s3 192.168.100.4 con máscara 24, esta configuración se realiza de manera estática.

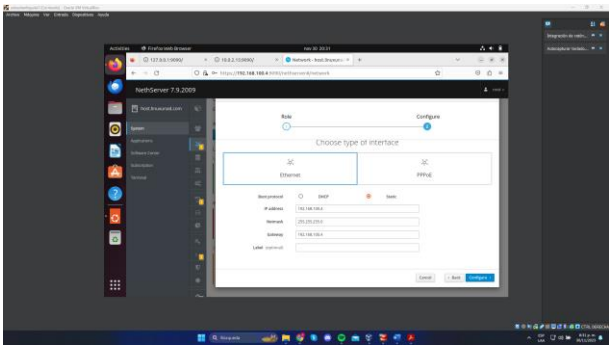

Ilustración 22- configuraciones de red roja

Configuración zona naranja, enp0s9 192.168.2.1 con máscara 24, esta configuración se realiza de manera estática.

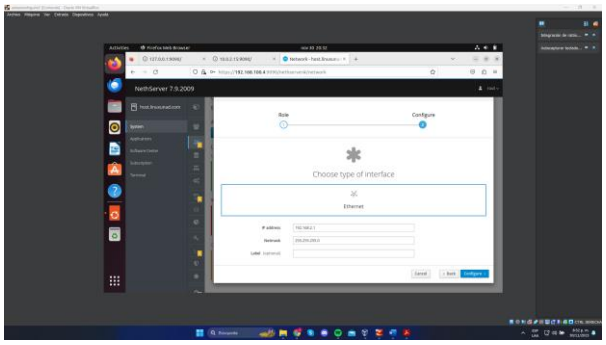

Ilustración 23 - configuraciones de red verde

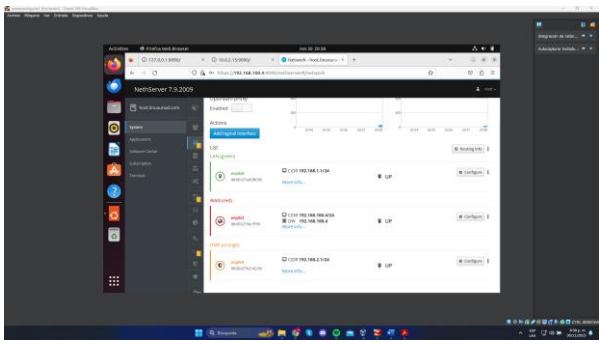

Ilustración 24- configuraciones de red

Configuración servicios DHCP para la tarjeta interna, definiendo un rango (192.168.1. - 192.168.1.254) a las que los clientes se van a conectar permitiendo el acceso a internet.

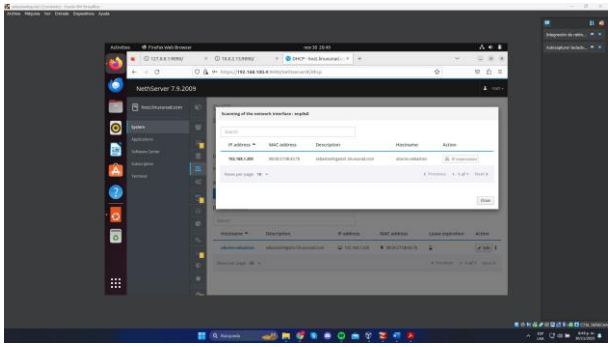

Ilustración 25- configuración dhcp

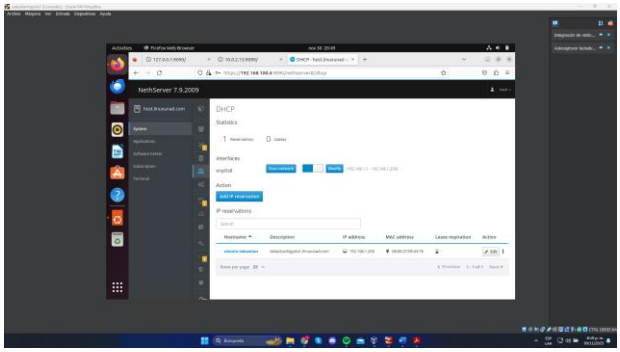

Ilustración 26- configuración proxy dhcp

Se realizan pruebas de conectividad hacia internet y una traza de la ruta que toma los paquetes y se evidencia que pasa por el servidor configurado.

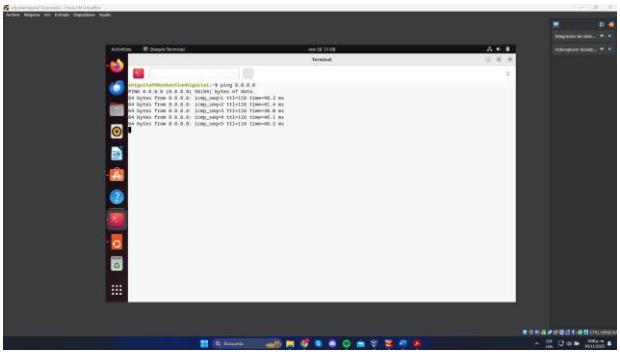

Ilustración 27-Verificacion de conexión

Configuración Equipo DMZ con dirección estática 192.168.2.2 con puerta de enlace 192.168.2.1

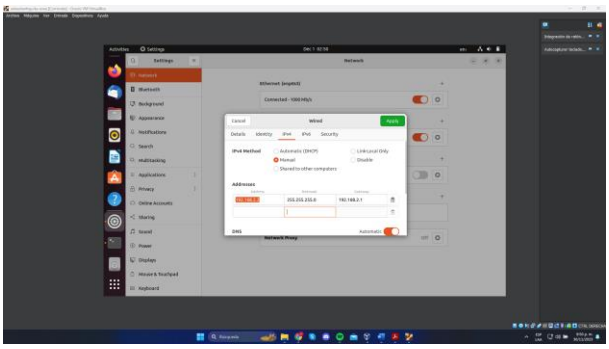

Ilustración 28 – configuración zona dmz

Pruebas de acceso al servidor apache instalado con resultado satisfactorio, ya se tenía el apache2 instalado con sus dependencias.

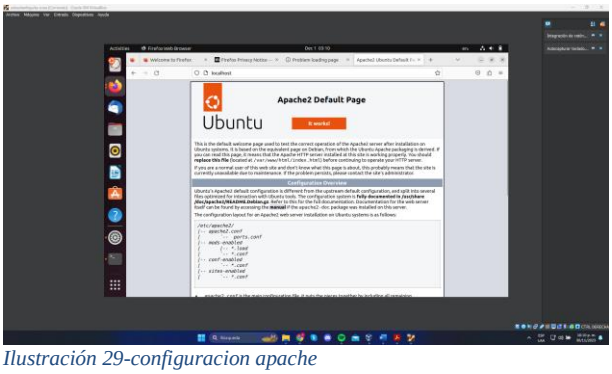

Ilustración 29-configuracion apache

Se habilita el proxy para la zona verde, Transparent SSL donde se habilitará y deshabilitara algunas categorías que agrupan páginas en internet, el proxy siempre escucha por el puerto 3128.

Se activa la categoría, las categorías propuestas para este caso “Université Toulouse (free)” esta categoría ayuda a aplicar los filtros a un grupo de páginas definidas por categorías.

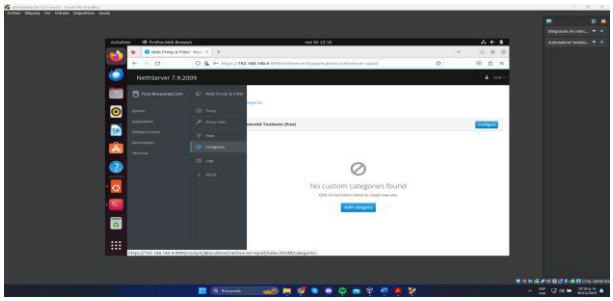

Ilustración 30- configuración de filtros

Para el ejercicio se realiza un filtrado que bloqueara todas las páginas incluidas dentro de todas las categorías ya instaladas.

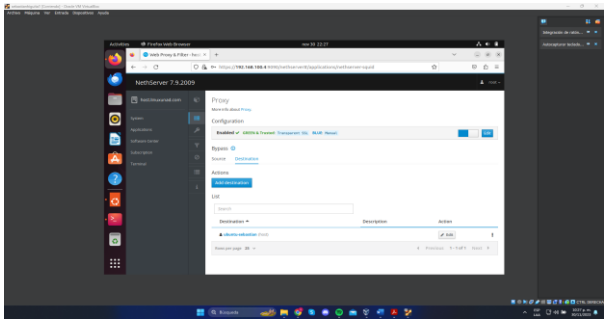

Ilustración 31- creación de filtros

Configuración de filtrado al cliente con ip 192.168.1.119 se les dan los permisos a todas las categorías seleccionadas.

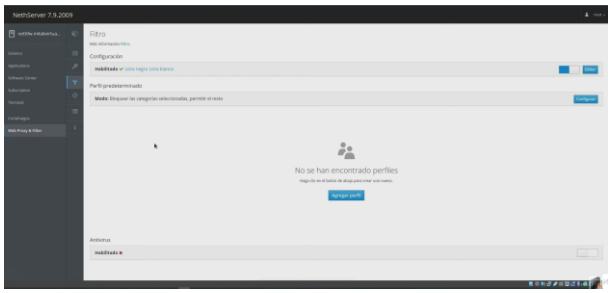

Ilustración 32- configuración de listas

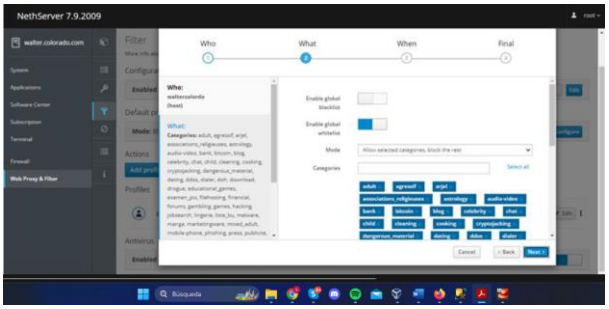

Ilustración 33- importación de listas

Con ayuda el squid se valida los registros de acceso.

Ilustración 34 – registros de squid

Configuración del proxy en equipo cliente donde se indica el host que se configuro y el puerto indicado 3128.

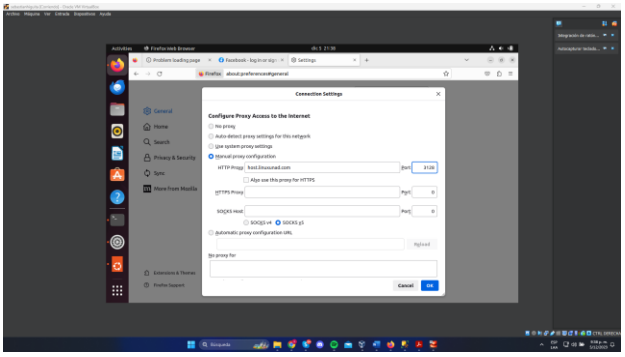

Ilustración 35 - configuración proxy en cliente

Se ingresa al equipo y se ingresa a páginas http://app.virtusys.com.br esta página está fuera de las categorías definidas y la bloquea.

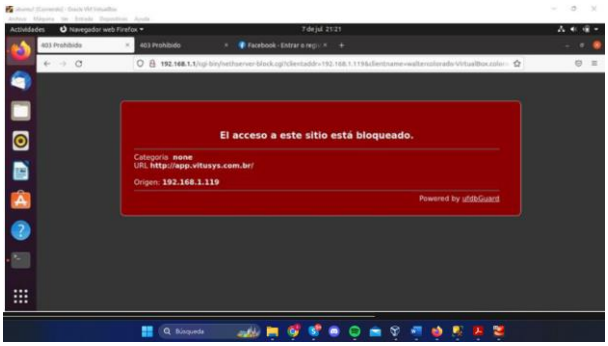

Ilustración 36 - validación de acceso

Seguido se realiza la prueba de una página autorizada incluida dentro del filtrado por categoría.

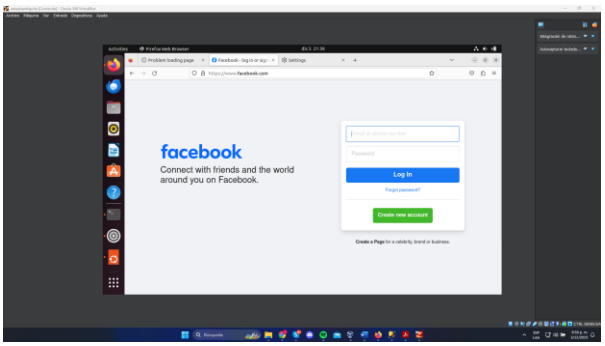

Ilustración 37- validación de acceso

3.3 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.

Como primero se ingresa a las propiedades del NethServer y se procede a la instalación del Firewall, así como sus componentes básicos.

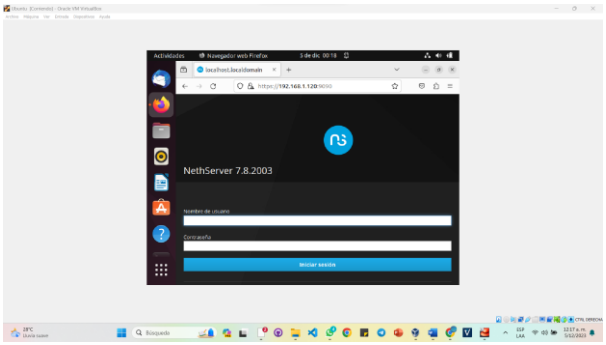

Ilustración 38-ingreso nethserver

Se ingresa a la plataforma y se inicia con la configuración de cada uno de los puertos, sabiendo que el verde se usará como red LAN, el naranja como red DMZ y el rojo como red WAN.

En la configuración de la red roja – WAN, se escoge el puerto de la máquina virtual que ya se había configurado con el adaptador puente, así se asegura que se tiene salida a internet y las demás pasarán por el Firewall.

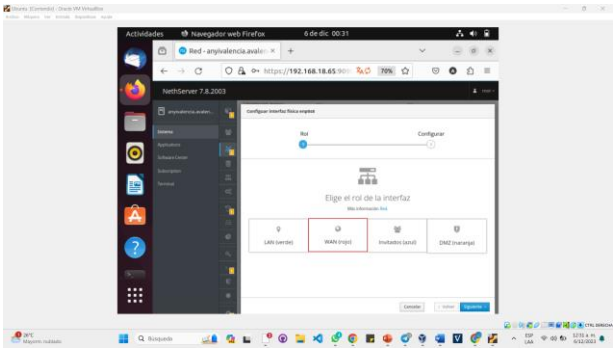

Ilustración 39-configuracion de red roja

Se tiene la red roja – WAN, se indica que la configuración de red sea por protocolo DHCP y se toma la IP que brinde la red, para utilizarla como puerta de enlace de la red verde – LAN.

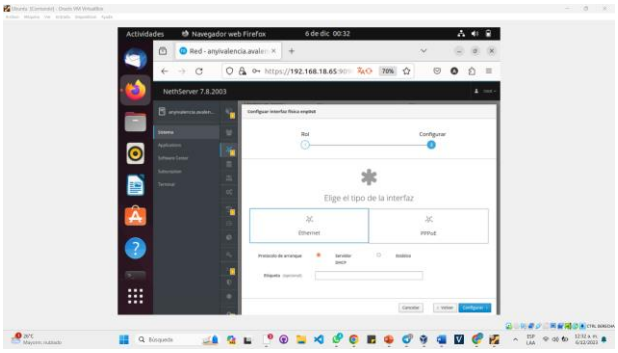

Ilustración 40-Configuacion de red verde

Configuración de la red verde – LAN, se escoge el puerto de la máquina virtual configurada con la red interna.

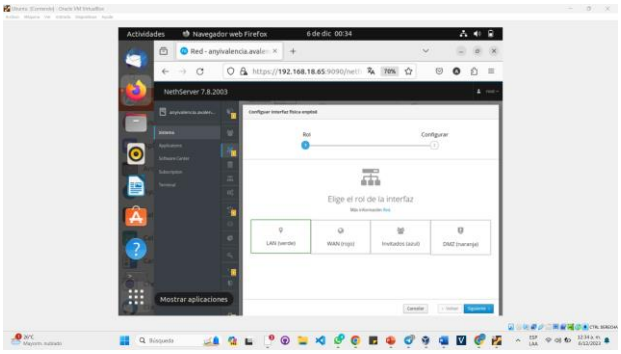

Ilustración 41-configuracion de red naranja

Configuración del protocolo de la IP estática, en el segmento que se decida utilizar para la red verde LAN y se utiliza uno de los puertos de la máquina virtual que se eligió en la red interna. Como puerta de enlace (Gateway), se usa la IP que asignó el DHCP en la red roja – WAN.

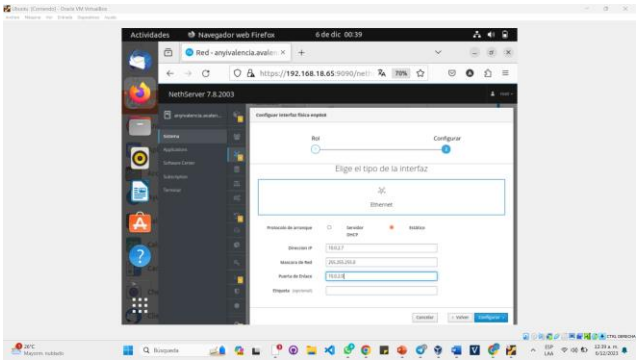

Ilustración 42- configuración dhcp – LAN

Configuración de la red Naranja – DMZ, en la cual se usará el puerto de la máquina virtual que se configure como red interna, donde la ingresaron con un segmento de red diferente al de la red LAN y la red WAN

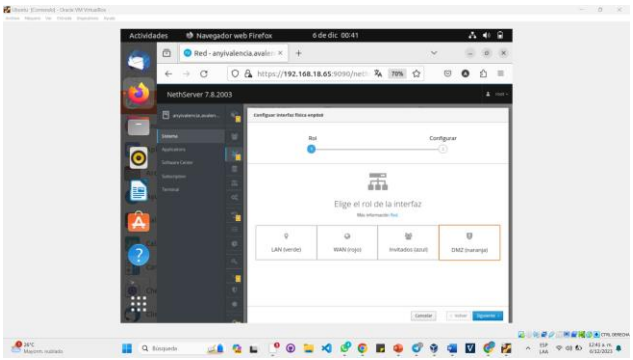

Ilustración 43- configuración DMZ

En esta red, en la siguiente figura se colocará la dirección IP que se decida utilizar para la red Naranja – DMZ, con un segmento de red diferente al de la red LAN y red WAN.

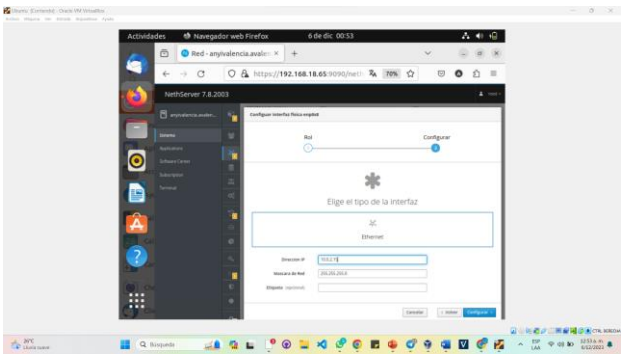

Ilustración 44- configuración WAN

Se asegura que el DHCP esté funcionando correctamente, se configura el servidor, indicando que suministre IP desde la IP siguiente a la que se usará en la red verde – LAN.

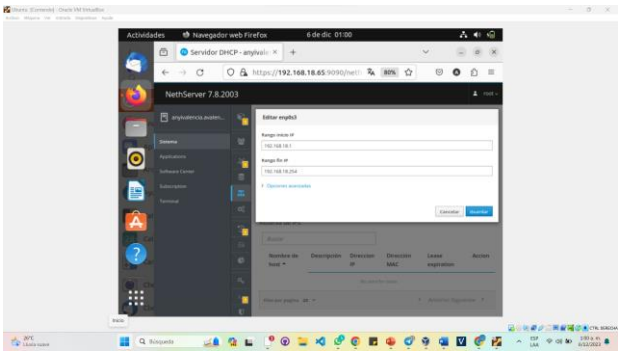

Ilustración 45-Condiguracion IP red verde

Se procede a observar al servidor del Firewall y se muestra como quedó la topología de red a partir de una gráfica.

Ilustración 46-Verioficacion diagrama firewall

Ahora, para la configuración de la máquina Ubuntu Desktop, ya se tiene instalada la versión 20-04 y se revisó que esta máquina si puede ingresar a redes sociales.

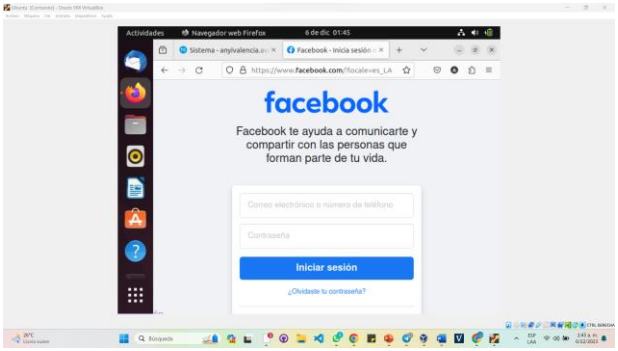

Ilustración 47-Verificacion de acceso

Ya se tiene conexión a Facebook, se procede a revisar por terminal hacía qué IP direcciona dicha página para poder crear la regla y restringir el acceso.

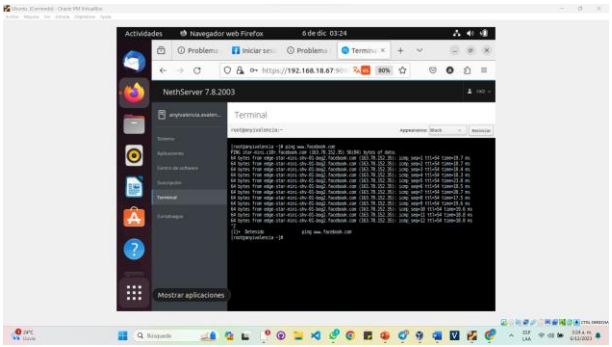

Ilustración 48-Verificacion de conexión

Al tener la IP identificada, se procede a ingresar al Firewall y crear la regla, para que se vaya a restringir el acceso.

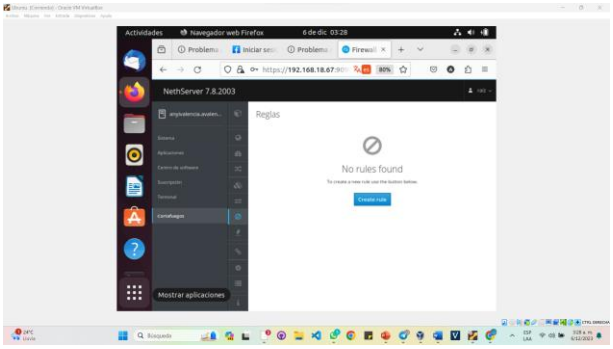

Ilustración 49- Configuración de regla

Se procede entonces a ingresar los datos ya conocidos y se presiona en el botón crear regla y se procede con dicho proceso.

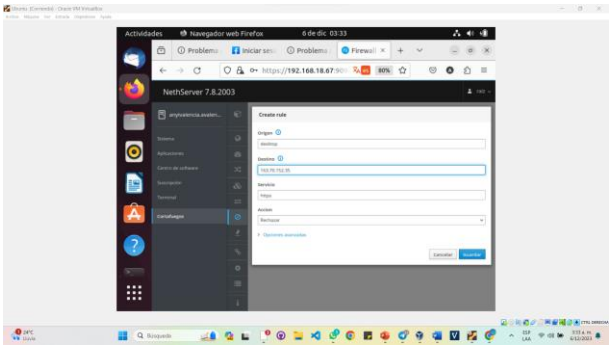

Ilustración 50 – Creación de reglas

Se selecciona el equipo que ya se tiene como desktop, en el Destino seleccionar la IP a la que me apunta Facebook, en el Servicio se selecciona https y ya por último en Acción se selecciona rechazar, se presiona el botón Guardar y posteriormente el botón Aplicar ubicado en la parte superior del aplicativo.

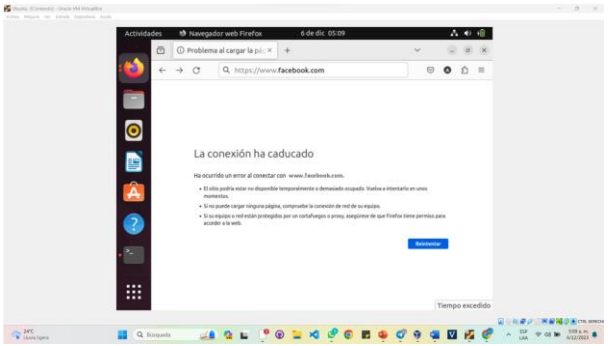

Ilustración 51 – Verificación de firewall

3.4 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.

Producto esperado: ser realizara la configuración para la creación de una VPN que permita establecer un túnel privado de comunicación entre un equipo de trabajo y/o estación de trabajo con GNU/Linux

Una vez realizado el procedimiento de instalación de nethserver se debe configurar por lo mínimo 3 tarjetas de red de red las cuales serán asignadas para la red LAN, WAN y DMZ.

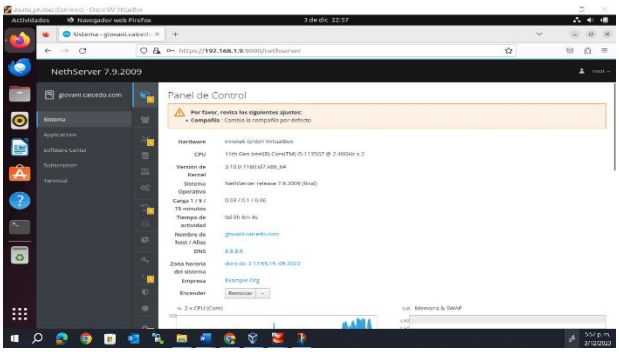

Ilustración 52- Configuración de inicio

Se continua con la creación del servidor DHCP el cual permite la asignación del direccionamiento IP por DHCP para los equipos que se van a conectar a la red LAN.

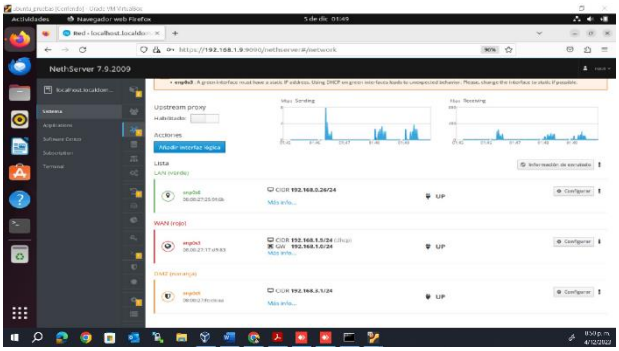

Ilustración 53- Configuración de red

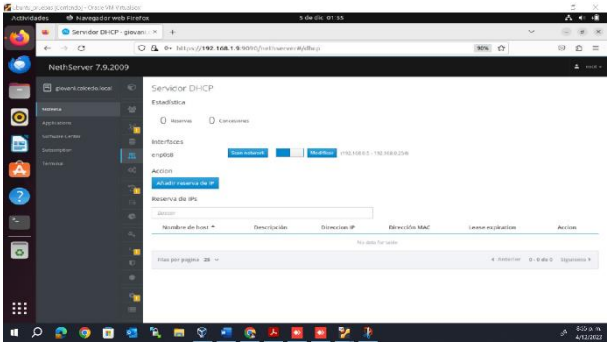

Ilustración 54 - Configuración dhcp

Se asigna direccionamiento IP de la red LAN a el equipo cliente con sistema operativo UBUNTU

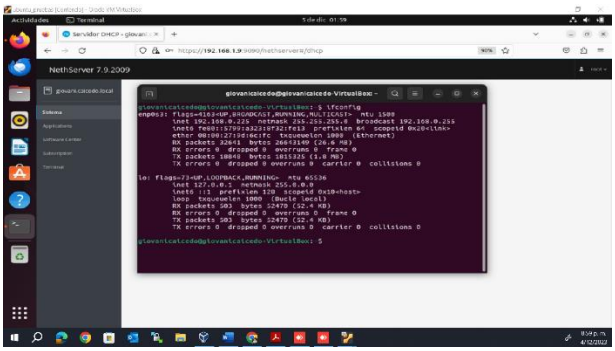

Ilustración 55- validación de ips

Se realiza descarga de Open VPN utilizando el panel de administración del nethserver y se instala en la aplicación web de nethserver.

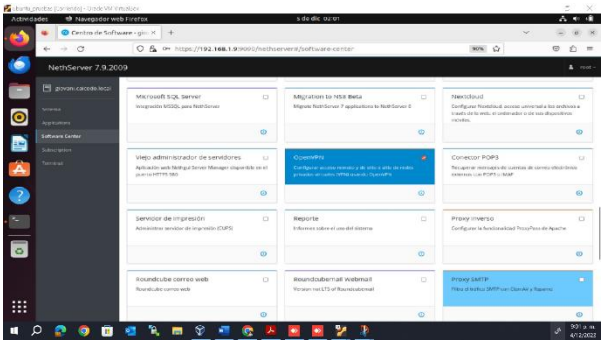

Ilustración 56- Instalación de aplicaciones

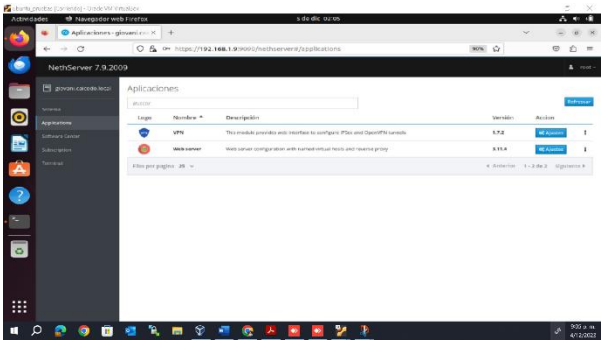

Ilustración 57- Configuración de aplicaciones

Por medio de la opción Sistema -> Usuarios y Grupos, se selecciona el proveedor de cuentas LDAP (Protocolo Ligero de Acceso a Directorio) y se crea usuario.

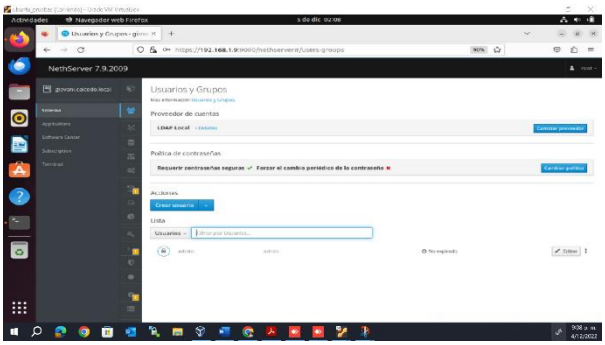

Ilustración 58- Configuración de usuarios

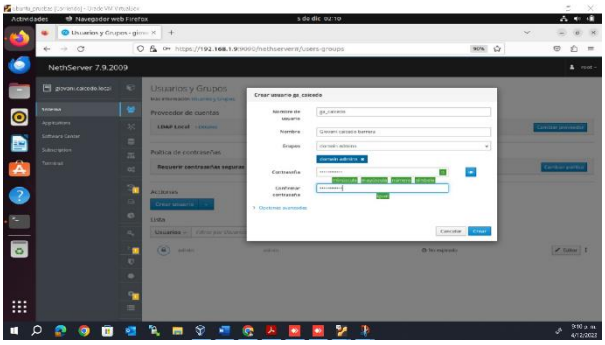

Ilustración 59 - Configuración de grupos

Se continua con la configuración del aplicativo instalado para la VPN en este caso el OpenVPN, se configura en servidor OpenVPN RoadWarrior, la opción de modo de autenticación por Nombre de usuario, contraseña y certificado, después se asigna una dirección IP a la red de la VPN, y se repisa la IP de la red WAN como salida para comunicarse entre equipos.

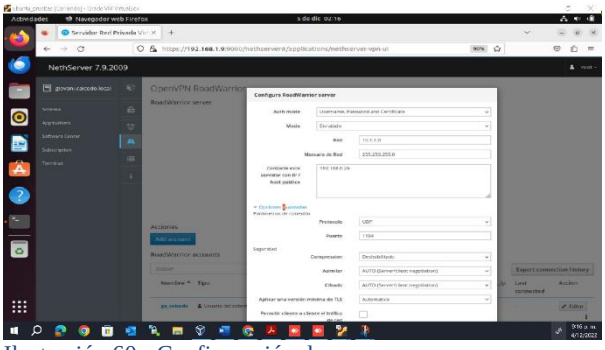

Ilustración 60 - Configuración de vpn

Se crean los usuarios que tendrán los permisos de acceso a la VPN, en este caso los usuarios que fueron creados con anterioridad a través de LDAP local

.

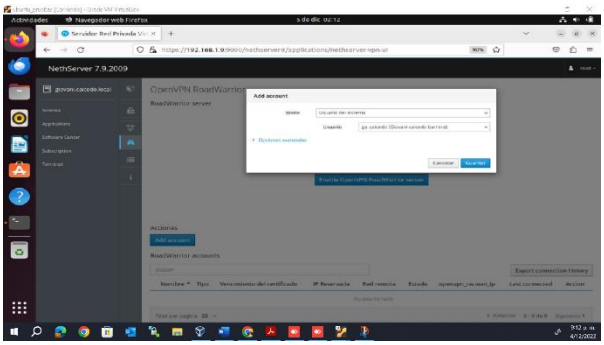

Ilustración 61- Configuración de usuario a vpn

Después de adicionadas las cuentas se procede a descargar los certificados para ingresar a través del cliente de VPN en los respectivos sistemas operativos de las estaciones de trabajo.

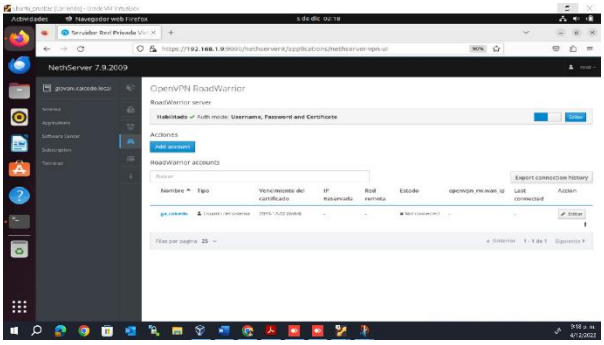

Ilustración 62- Descargar certificados

Se debe realizar la instalación del software OpenVPN al equipo cliente de Windows, realizar conexión autenticando con el certificado de cada usuario

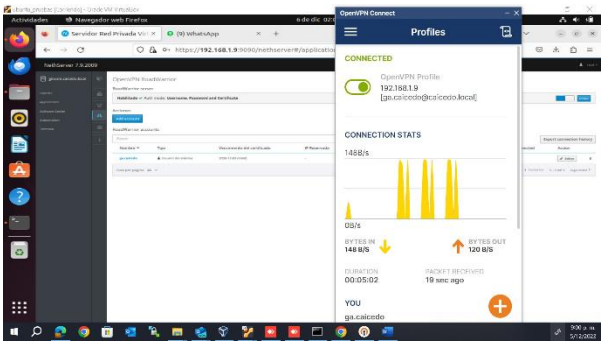

Ilustración 63- Configuración de cliente

Evidencia ingreso por la terminal de Windows se puede acceder por SSH a la base de datos de maríadb.

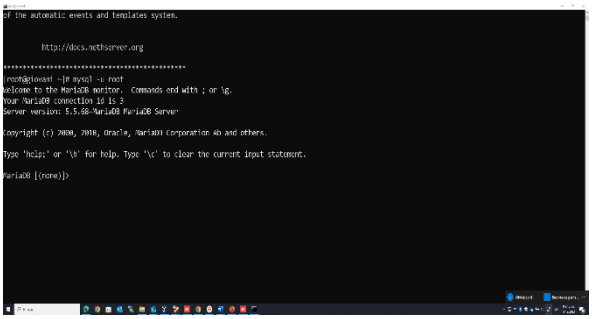

Ilustración 64- Validación de acceso

CONCLUSIONES

La implementación de NethServer y el desarrollo de las temáticas abordadas han demostrado ser fundamentales para la creación de un entorno de red robusto y seguro. La integración de servicios como DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos y VPN proporciona una infraestructura integral que optimiza la conectividad y garantiza la protección contra amenazas potenciales. Este enfoque ofrece beneficios significativos en términos de eficiencia operativa y seguridad de la red.

Se evidencia un sencillo proceso de instalación y configuración de un servidor ayudados con Nethserver. Este, junto con su conjunto de servicios, nos proporciona una herramienta potente y de fácil configuración, teniendo en cuenta las respectivas reglas de redireccionado, configuradas en sus respectivas redes.

A nivel individual, cada estudiante adquirido la destreza técnica necesaria para la administración, instalación y la operabilidad de la plataforma Nethserver con cada uno de sus diferentes servicios que ofrece, y así lograr ampliar el portafolio de servicios por la empresa a la web, dado que se cuenta con una robusta plataforma que garantiza la seguridad de la información.

CITAS Y/O REFERENCIAS

[1] NethServer Documentation. Disponible en: https://docs.nethserver.org

[2] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Prentice Hall

[3] Cisco. (2018). Cisco Firewalls. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/index.html

[4] Doherty, P., & Doherty, D. (2009). VPNs: A Beginner's Guide (2nd ed.). McGraw-Hill Education.