SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Edna Julieth Munevar Ariza
e-mail: ejmunevara@unadvirtual.edu.co
Jeisson Chaparro Barrera
e-mail: jschaparroba@unadvirtual.edu.co
Luisa Fernanda Gómez Castelblanco
e-mail: lfgomezcas@unadvirtual.edu.co
Helber Garavito Merchán
e-mail: hgaravitom@unadvirtual.edu.co
Angie Katherine Cipamocha García
e-mail: akcipamochag@unadvirtual.edu.co

RESUMEN: *En el presente artículo se demuestra la utilización de nethserver como propuesta para la administración de servicios esenciales, otorgando un alto nivel de seguridad a una distribución GNU Linux, mediante la implementación de cinco temáticas se demuestra el uso de servicios de DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server, y VPN, en donde cada una de estas se desarrollan a través de máquinas virtuales e interfaz web de nethserver, las cuales permiten la obtención de resultados satisfactorios evidenciándose la utilidad, practicidad y facilidad de implementar estos servicios de manera segura por medio de una distribución de código abierto como lo es nethserver.*

PALABRAS CLAVE: Implementación, Nethserver, servicios, seguridad.

1 INTRODUCCIÓN

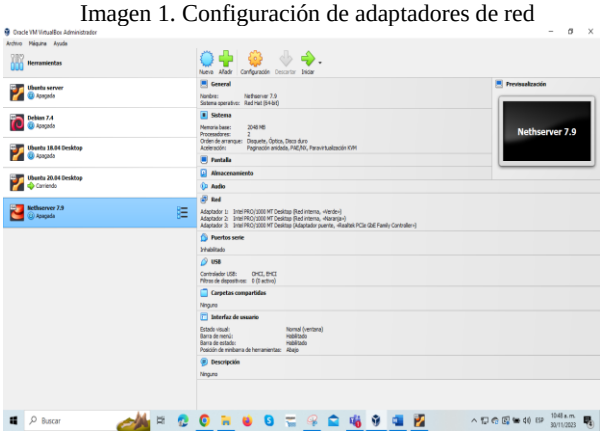
En la actualidad, la gestión eficiente de la infraestructura de red es crucial para el funcionamiento óptimo de organizaciones, empresas y entornos domésticos. La implementación de soluciones de TI flexibles, seguras y rentables se ha vuelto cada vez más relevantes, en este contexto, GNU/Linux surge como una opción poderosa y versátil para satisfacer una variedad de necesidades específicas de red, ofreciendo una serie de soluciones robustas y personalizables.

Este enfoque modular y adaptable se logra mediante el uso de distintas aplicaciones y servicios disponibles en distribuciones basadas en GNU/Linux. A continuación, se presenta una serie de soluciones destacadas para atender necesidades las cuales son DHCP Server, DNS, Proxy, Firewall, File Server, Print Server.

2 CONFIGURACIÓN DE NETHSERVER

Se descarga Nethserver y se empieza con la instalación, Definiendo las redes LAN (verde), DMZ (Naranja), y WAN (roja). Por medio, de la virtualización que ofrece la herramienta virtual Box, en la cual se tiene en cuenta el manual de uso de la misma. [1]

Imagen 1. Configuración de adaptadores de red

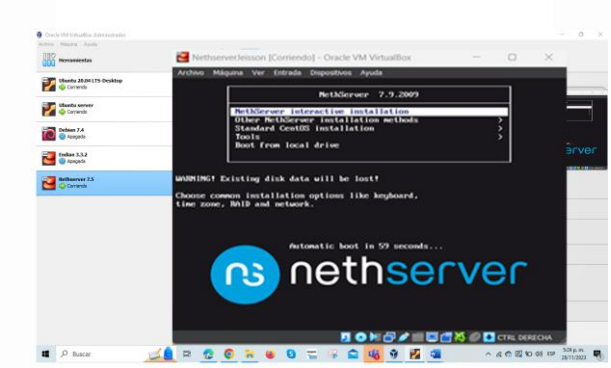


Fuente: Autoría propia

2.1 INSTALACIÓN DE NETHSERVER

Se inicia la instalación del Nethserver por medio de la su interfaz, seleccionando la opción “Nethserver interactive installation”.

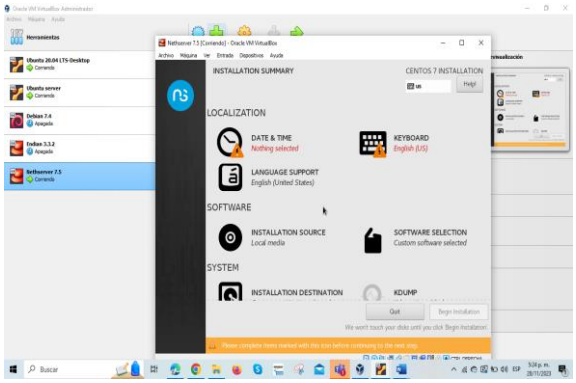
Imagen 2. Menú de inicio para la instalación de Nethserver



Fuente: Autoría propia

Se procese con la con la instalación y configuración de la zona horaria, asignación de nombre de host de la red e idioma y distribución del teclado.

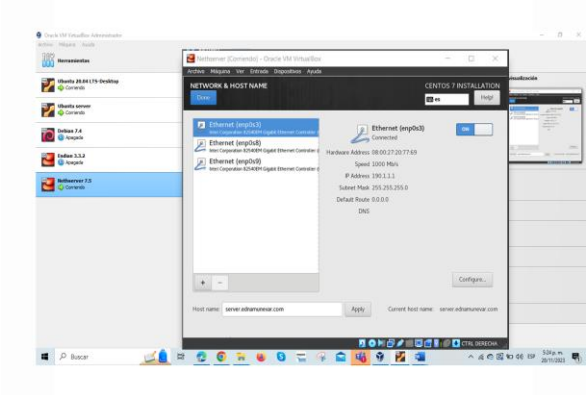
Imagen 3. Interfaz del resumen de instalación de Nethserver



Fuente: Autoría propia

Para finalizar, se establece el direccionamiento a cada adaptador de red y se asigna el hostname.

Imagen 4. Selección de los adaptadores, encendidos y asignación de hostname



Fuente: Autoría propia

3 TEMÁTICA 1: SERVIDOR DHCP, DNS Y CONTROLADOR DE DOMINIO

3.1 CARACTERÍSTICAS GENERALES

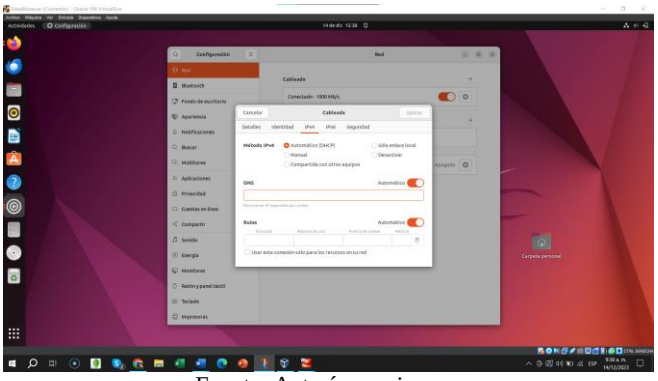
El servidor DHCP se configura con un rango de 10 equipos con asignación de IP automática conectados a la zona verde.

Imagen 5. Estableciendo rango de IP de la zona verde

Fuente: Autoría propia

Se configura el Ubuntu desktop por medio de la implementación de DHCP, con este fin es indispensable, conocer sobre la arquitectura y funcionamiento de Ubuntu desktop, por medio de la información dada en el libro “Ubuntu 22.04 LTS Desktop: Applications and Administration” [2]. De esta manera la configuración del DHCP, DNS y controladores de dominio, se pueden realizar de manera eficiente ya sea por medio de la terminal o como se muestra a continuación.

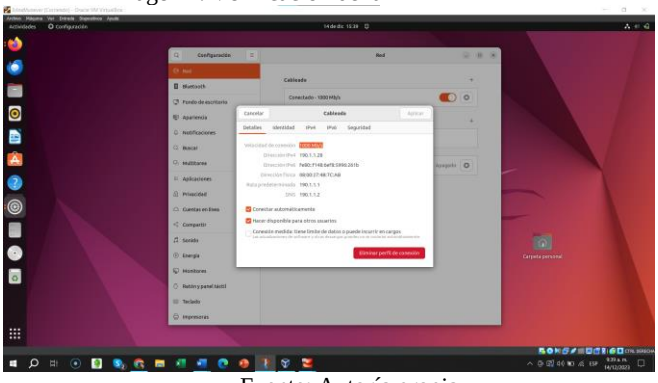
Imagen 6.Configuración del equipo desktop como DHCP



Fuente: Autoría propia

Se procede a realizar la verificaciòn de la nueva direccion IP asiganada por el DHCP

Imagen 7. Verificación de la IP

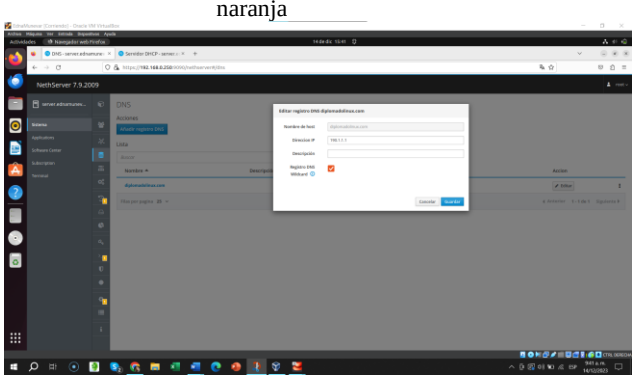


Fuente: Autoría propia

3.2 CONFIGURACIÓN DNS

Para la configuración del DNS se ingresa al Nethserver por medio de la dirección IP de la zona verde y a la vinculación de un servidor web en zona naranja.

Imagen 8. Creación del DNS conectado a la zona naranja



Fuente: Autoría propia

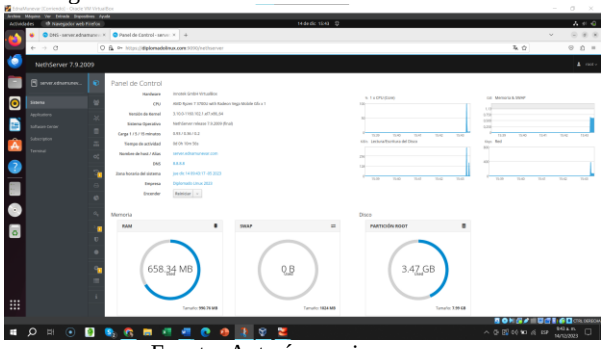
Se procede a crear el DNS, que en este caso es diplomadolinux.com.

Imagen 9. Evidencia del DNS creado

Fuente: Autoría propia

Se evidencia el acceso a la dirección diplomadolinux.com del DNS del servidor wweb en la zona naranja.

Imagen 10. Acceso a dirección del DNS del servidor

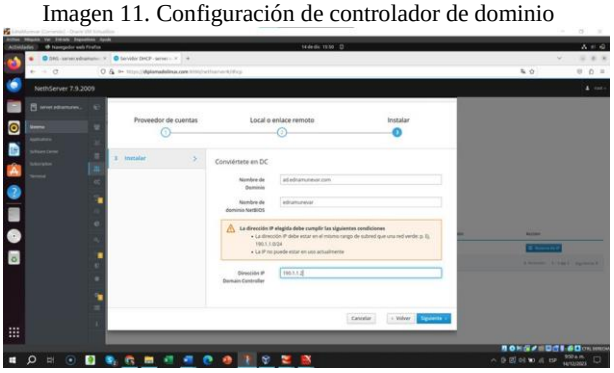


Fuente: Autoría propia

3.3 CONTROLADOR DE DOMINIO

Para esta configuración se ingresa al modúlo de usuarios y grupos, seleccionando Active Directory, etableciendo la configuracion y parametros, tal como se evidencia en la imagen.

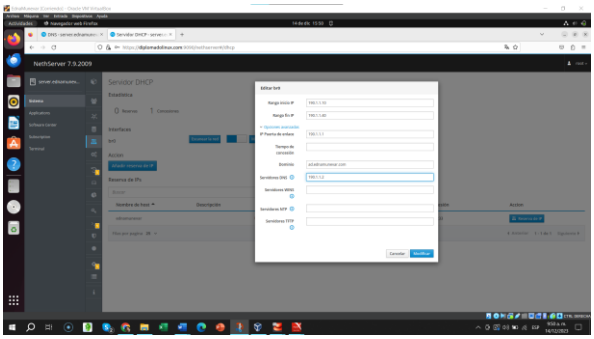
Imagen 11. Configuración de controlador de dominio



Fuente: Autoría propia

En el servidor DHCP, se especifica el nombre de dominio, direccion de dominio, la IP del dominio, donde el ultimo es asignado al adaptador de red zona verde.

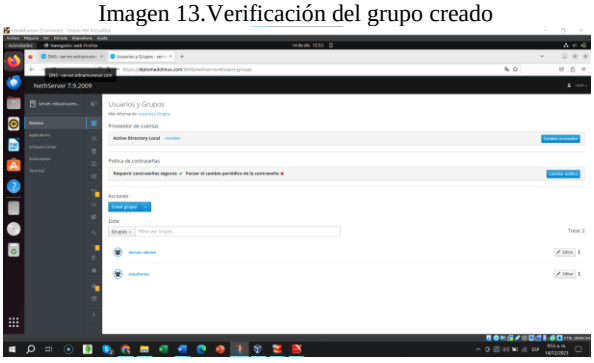
Imagen 12. Actualización del nombre dominio y la IP en DNS



Fuente: Autoría propia

Seguido a esto se procede a desbloquear las dos cuentas creadas atomaticamente, ya que estas son de gran importancia para la vinculación del ubuntu desktop al dominio.

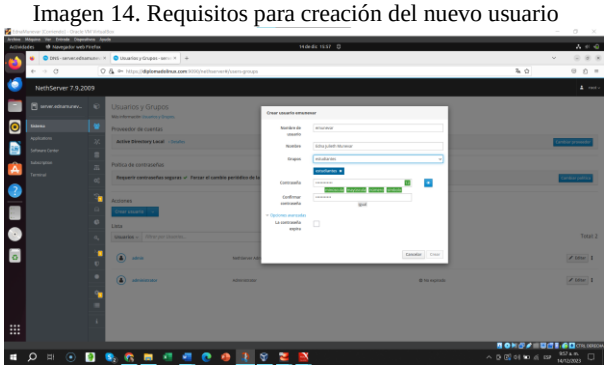
Imagen 13.Verificación del grupo creado



Fuente: Autoría propia

Se crea un grupo y usuario, estableciendo contraseña, la cual debe cumplir con los parámetros minimos de seguridad reuqueridos.

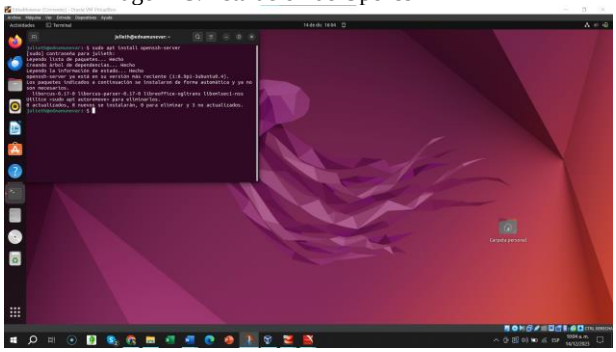
Imagen 14. Requisitos para creación del nuevo usuario



Fuente: Autoría propia

Ya creado el grupo y el usuario correspondiente se debe vincular el ubuntu desktop al dominio por medio de comando.

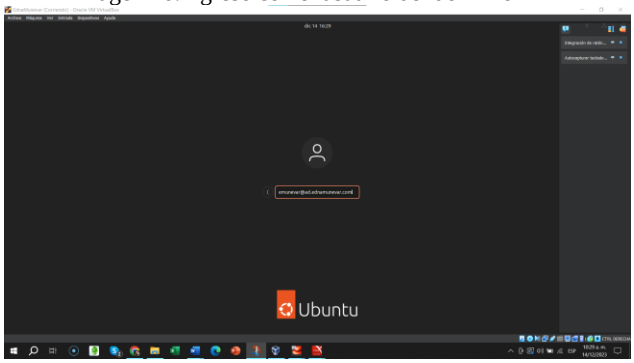
Imagen 15.Instalación de Openssh



Fuente: Autoría propia

Se procede a reiniciar la maquina desktop, digitando el nombre de usuario y el nombre de dominio con la contraseña creada.

Imagen 16.Ingreso con el usuario del dominio



Fuente: Autoría propia

Finalmente y por medio de interfaz grafica se evidencia la existencia del usuario creado.

Imagen 17. Existencia del usuario creado

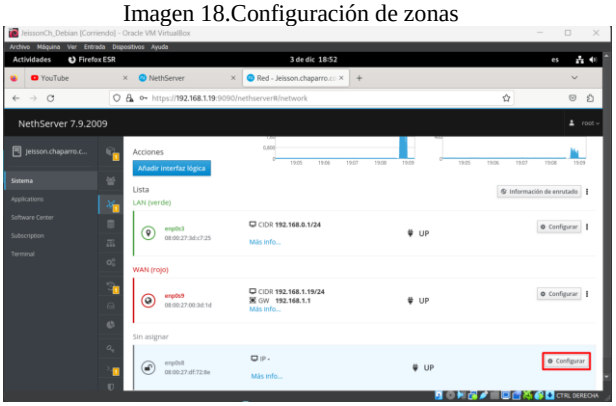
Fuente: Autoría propia

4 TEMÁTICA 2: PROXY

4.1 CONFIGURACIÓN DE LAS TARJETAS DE RED EN CADA RED

Por medio de la dirección IP se ingresa al Nethserver desde el equipo desktop. Se identifica el adaptador que dispone de conectividad a Internet con el propósito de establecer su configuración como zona roja.

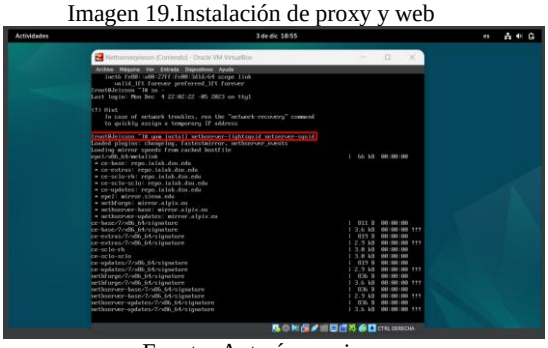
Imagen 18.Configuración de zonas



Fuente: Autoría propia

Se procede a realizar la instalación y configuración el Proxy, desde Nethserver.

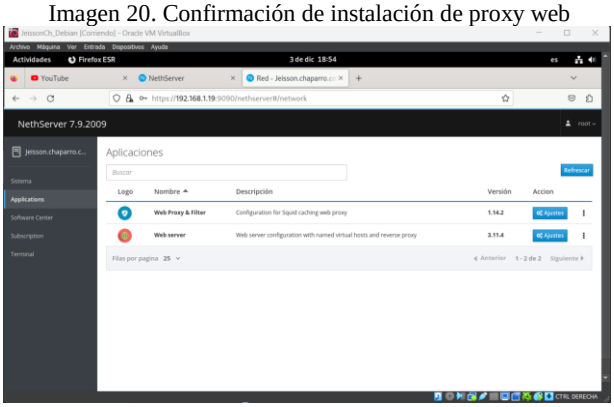
Imagen 19.Instalación de proxy y web



Fuente: Autoría propia

Posterior a la instalación de la aplicación Proxy Web mediante Nethserver, se procede a confirmar su presencia en la interfaz.

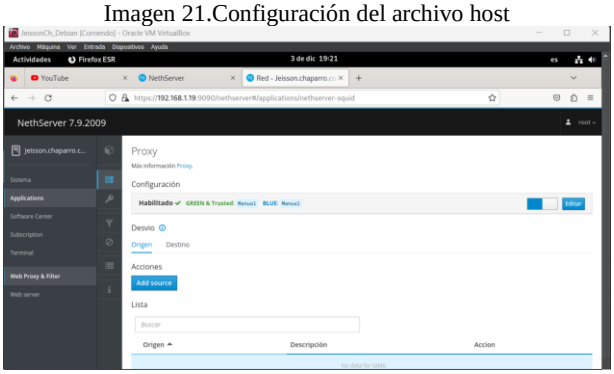
Imagen 20. Confirmación de instalación de proxy web



Fuente: Autoría propia

Se establece la configuración del archivo hosts utilizando la dirección IP 192.168.1.10, la cual corresponde a la dirección del equipo cliente.

Imagen 21.Configuración del archivo host



Fuente: Autoría propia

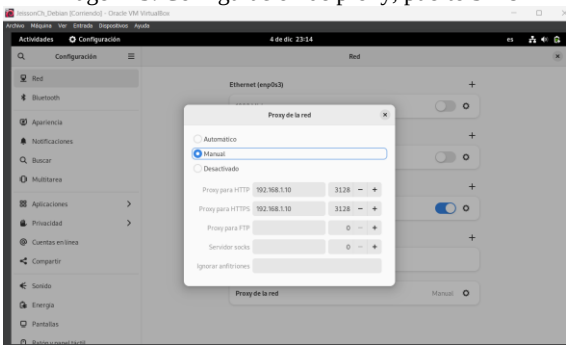
Se realizan todas las configuraciones a través de la aplicación de proxy web para definir las restricciones de las categorías que serán bloqueadas posteriormente.

Imagen 22.Elección de restricciones

Fuente: Autoría propia

Se prosigue con la configuración del proxy en la computadora cliente con el fin de filtrar la salida a través del puerto 3128.

Imagen 23. Configuración de proxy, puerto 3128



Fuente: Autoría propia

Finalmente, se procede a acceder a uno de los sitios web restringidos en el perfil, específicamente en la clasificación de "adultos", utilizando el dispositivo del usuario para visitar la página, donde el sistema de proxy se encarga de impedir automáticamente el acceso a dicho sitio.

Imagen 24. Bloqueo mediante proxy de la página

Fuente: Autoría propia

5 TEMÁTICA 3: CORTAFUEGOS

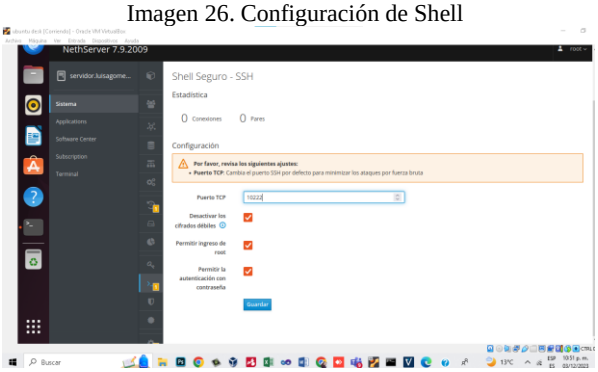
Se inicia con la configuración de las tres zonas, verde, roja y naranja.

Imagen 25.Configuración de las zonas

Fuente: Autoría propia

Se procede a ingresar al apartado de Shell seguro el corresponde a la configuración SSH, donde el puerto TCP está en 22 y se realiza el cambio por 1222.

Imagen 26. Configuración de Shell



Fuente: Autoría propia

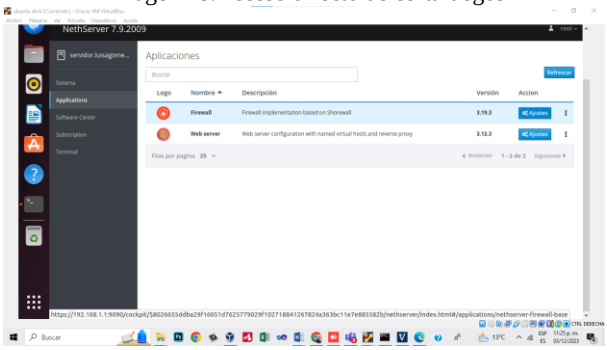
Se configura la instalación del cortafuego seleccionando Basic Firewall e iniciando su instalación. "Cortafuegos Nethserver puede actuar como firewall y puerta de enlace dentro de la red donde está instalado. Este puede instalarse desde el centro de software, en donde dentro de otras opciones permite la gestión de reglas de firewall". [3]

Imagen 27.Instalación del cortafuegos

Fuente: Autoría propia

Después de la respectiva instalación se crear un acceso directo con el fin de visualizar el firewall en el panel.

Imagen 28.Acceso directo de cortafuegos



Fuente: Autoría propia

Antes de iniciar con las restricciones se verifica que el desktop tenga acceso a redes sociales como Facebook.

Imagen 29. Verificación de funcionamiento de la página

Fuente: Autoría propia

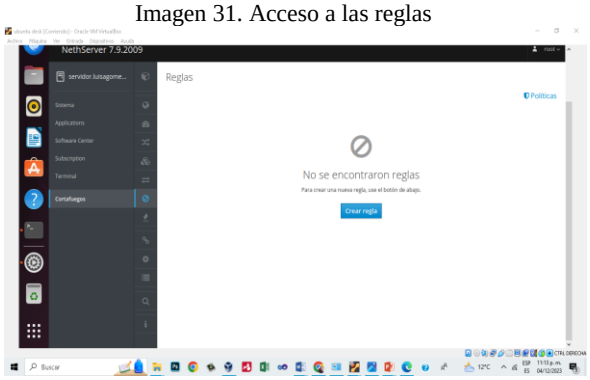
Se procede a realizar verificación desde la terminal de la IP que direcciona a Facebook para poder crear la regla y restringir el acceso. El comando usado es: $ nslookup www.facebook.com.

Imagen 30. Consulta IP Facebook

Fuente: Autoría propia

Con la IP de la red social Facebook identificada y Firewall instalado, se ingresa a crear la regla y restringir el acceso.

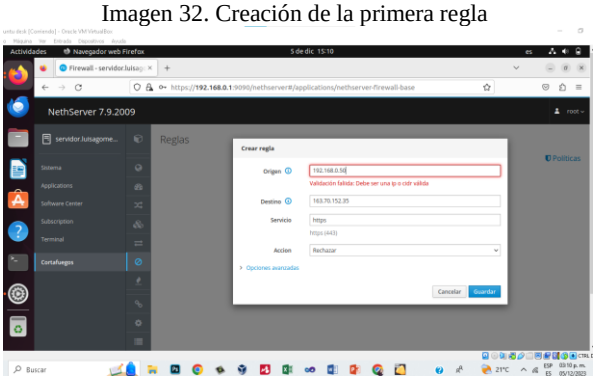
Imagen 31. Acceso a las reglas



Fuente: Autoría propia

Teniendo en cuenta que no hay ninguna restricción se procede a crear la primera regla.

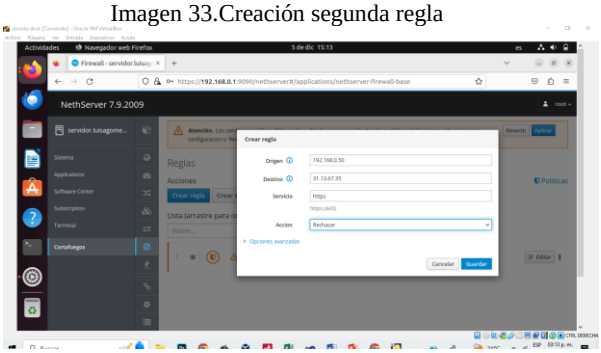
Imagen 32. Creación de la primera regla



Fuente: Autoría propia

Se ingresa al apartado de créate y se guarda la segunda regla.

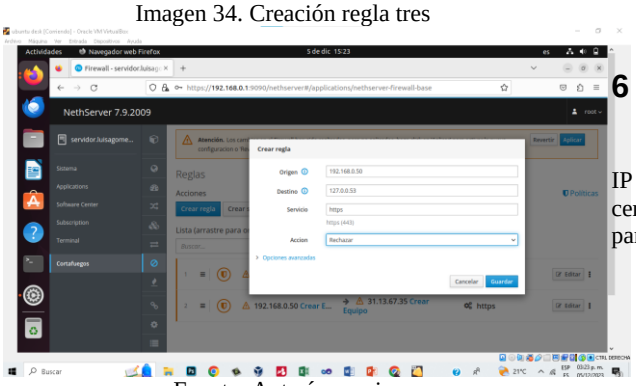
Imagen 33.Creación segunda regla



Fuente: Autoría propia

Al igual que las otras dos reglas se a crea la tercera regla con la IP correspondiente.

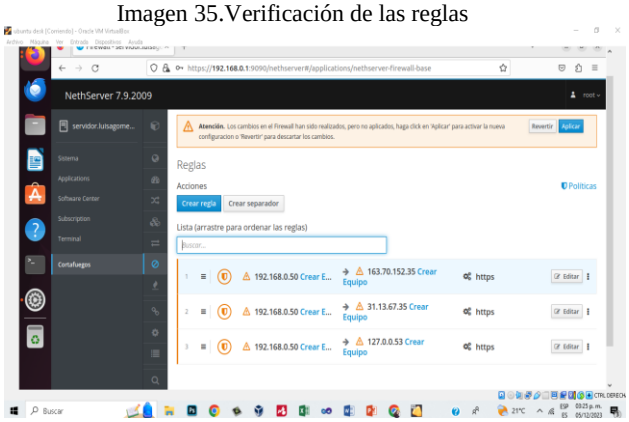
Imagen 34. Creación regla tres



Fuente: Autoría propia

Finalmente se evidencia la creación de las tres restricciones a la página de Facebook.

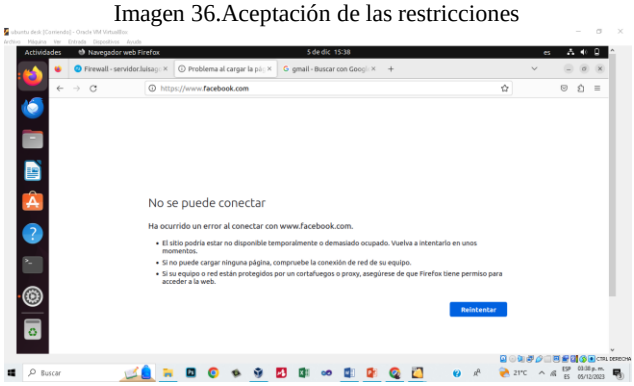
Imagen 35.Verificación de las reglas



Fuente: Autoría propia

Se procede a reiniciar el Nethserver y se vuelve a ingresar al buscador con el enlace o la página www.facebook para probar el cumplimiento de la regla.

Imagen 36.Aceptación de las restricciones

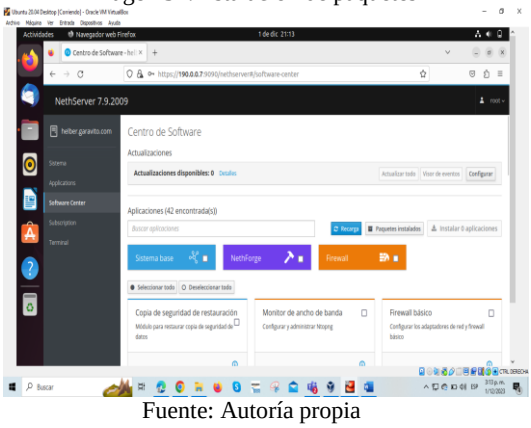


Fuente: Autoría propia

6 TEMÁTICA 4: FILE SERVER Y PRINT

Para iniciar se en entra al Nethserver haciendo uso de la IP 190.0.0.7, se digita usuario y contraseña, y en el software center se buscan los paquetes de File Server y Print Server, para realizar la instalación de las aplicaciones.

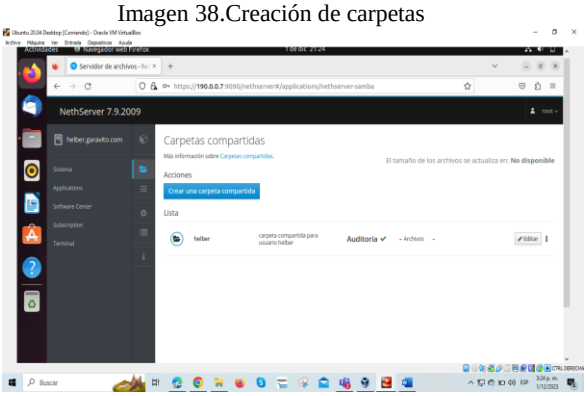
Imagen 37.Instalación de paquetes



Fuente: Autoría propia

Se verifica la correcta instalación de las aplicaciones, para ingresar a los ajustes del File Server, en el apartado de carpetas comprimidas de crear una carpeta.

Imagen 38.Creación de carpetas



Fuente: Autoría propia

En el sistema se procede a ingresar a usuarios y grupos marcando LDAP y en seguido se selecciona LDAP Local e instalar.

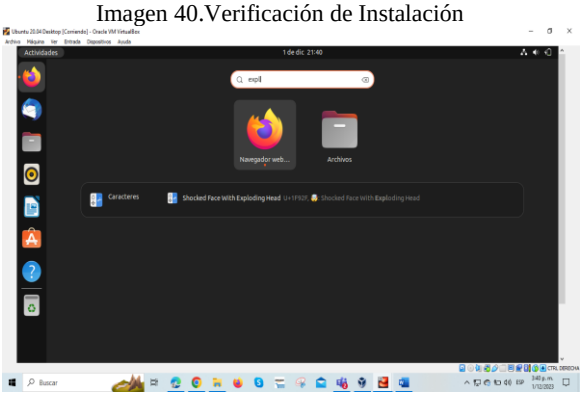
Imagen 39.Instalación de LDAP

Fuente: Autoría propia

Se evidencia la instalación de LDAP local como proveedor de cuentas y se procede a crear un usuario el cual aparece por defecto como admin.

Se ingresa al desktop y se busca expl que aparece como archivos para finalmente iniciar con un click.

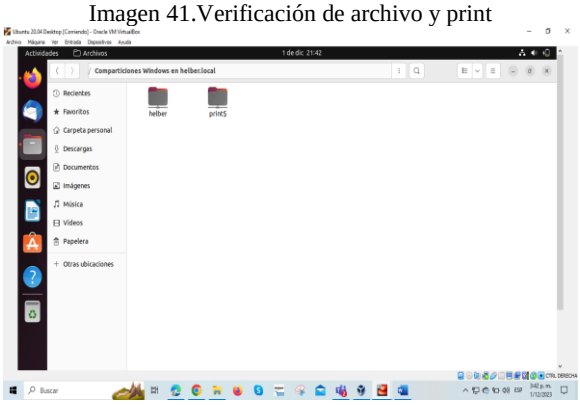
Imagen 40.Verificación de Instalación



Fuente: Autoría propia

Se ingresa al apartado de otras ubicaciones en donde se evidencia el archivo creado y el print compartido.

Imagen 41.Verificación de archivo y print



Fuente: Autoría propia

7 TEMÁTICA 5: VPN

Inicialmente, se realiza la instalación y configuración nethserver, mostrada anteriormente. Por consiguiente, se configuran las redes WAN (roja), LAN (verde) y DMZ (naranja), mediante los tres adaptadores de red definidos en nethserver.

Imagen 42. Configuración de redes

Fuente: Autoría propia

Una vez, realizada tal configuración, se continúa con la configuración del DHCP, al cual se le establece un rango de red con respecto a la red LAN (verde), donde se asigna un rango de inicio IP 192.168.11.2 y un rango fin IP 192.168.11.253. Esto permitirá ver cada vez que el equipo Ubuntu Desk (cliente), entre en contacto con la red, y además que se le asigne una IP de forma automática dentro de este rango para este equipo.

Imagen 43.Configuración DHCP

Fuente: Autoría propia

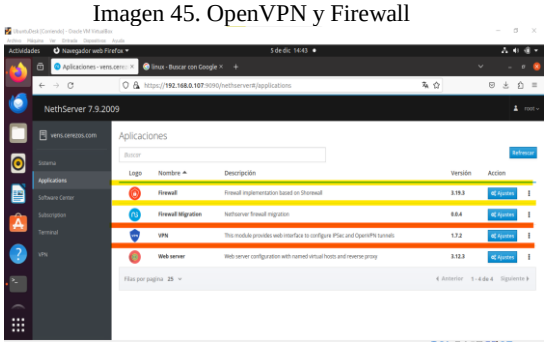
Seguidamente, se realiza la instalación de OpenVPN y de Firewall básico, por medio de software Center, donde se selecciona el paquete y se realiza la instalación.

Imagen 44.Descarga e instalación OpenVPN y Firewall

Fuente: Autoría propia

Después de que se realiza la instalación, estos aplicativos se verán reflejados en la sección aplicaciones, donde hay que dirigirse a "ajustes" con el fin de comenzar la configuración.

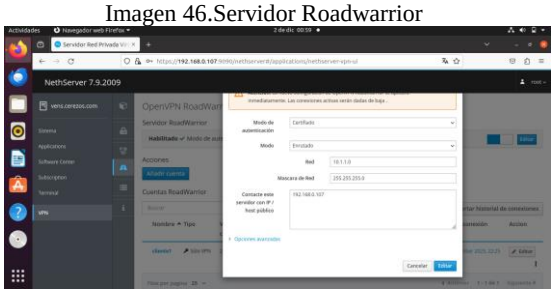
Imagen 45. OpenVPN y Firewall



Fuente: Autoría propia

Donde la principal configuración realizada es al servidor Roadwarrior, donde se selecciona: Modo de certificación: certificado, Modo: Enrutado, Red: 10.1.1.0, Máscara de subred: 255.255.255.0, Host público: 192.168.0.107 (red WAN).

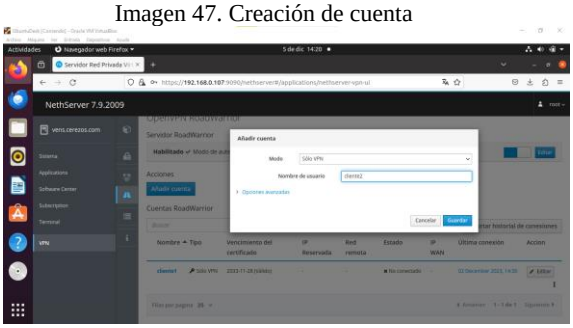
Imagen 46.Servidor Roadwarrior



Fuente: Autoría propia

Luego, en la opción de "añadir cuenta" se agrega una nueva cuenta la cual va a permitir solo VPN y se nombra como cliente2.

Imagen 47. Creación de cuenta



Fuente: Autoría propia

Posteriormente teniendo la cuenta cliente2, se realiza la descarga del certificado, el cual servirá para la activación de la red privada VPN en ubuntu Desk (cliente).

Imagen 48.Descarga configuración OpenVPN

Fuente: Autoría propia

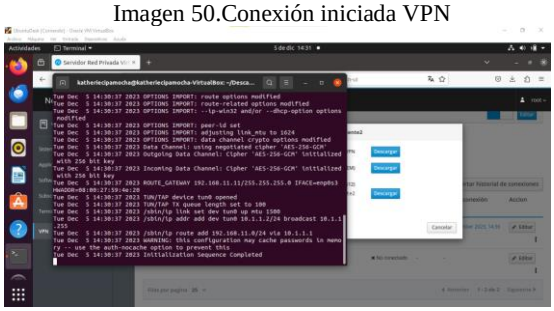
Para la configuración del firewall, solo es necesario permitir la opción de "Tráfico entre roadwarrior OpenVPN, los túneles OpenVPN y los túneles IPSec".

Imagen 49.Configuración Firewall

Fuente: Autoría propia

Acto seguido, teniendo el certificado descargado como cliente2.ovpn, por medio de la terminal se abre este archivo, ejecutando el comando sudo openvpn cliente2.ovpn, el cual permitirá la conexión y cuando esta esté conectada se mostrará el mensaje en pantalla "initialization sequence completed".

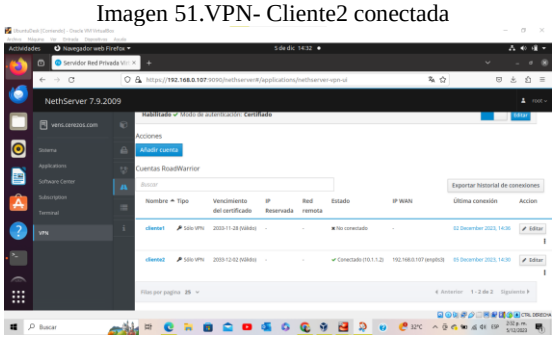
Imagen 50.Conexión iniciada VPN



Fuente: Autoría propia

Al actualizar el panel administrativo de nethserver, se puede observar que la cuenta creada cliente2 está conectada por VPN, desde el equipo Ubuntu Desk (cliente).

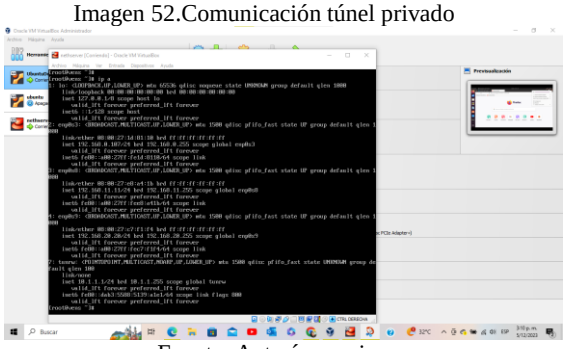
Imagen 51.VPN- Cliente2 conectada



Fuente: Autoría propia

También se verifica la creación del túnel por medio de la terminal de nethserver, ejecutando el comando IP, donde se evidencia una nueva conexión nombrada tunrw.

Imagen 52.Comunicación túnel privado



Fuente: Autoría propia

Por último, se comprueba que haya conexión a la red, desactivando la red puente (WAN) que permite el acceso a internet para Ubuntu Desk (cliente), dejando solamente activa la red LAN enp08 (verde), que anteriormente no contaba con acceso a internet y que ahora con la activación del túnel, si se tiene acceso.

Imagen 53.Conexión vía VPN

Fuente: Autoría propia

8. Conclusiones.

DHCP Server: Utilizar GNU/Linux como servidor DHCP permite una asignación dinámica de direcciones IP a dispositivos en la red de manera automatizada. Esto simplifica la gestión de direcciones IP y mejora la conectividad de los dispositivos al reducir errores de configuración manual.

Proxy: Un servidor proxy en GNU/Linux actúa como intermediario entre los usuarios y los servicios externos, mejorando la seguridad, el rendimiento y la gestión del ancho de banda al cachear contenido web, filtrar solicitudes o proteger la identidad de los usuarios.

Cortafuegos (Firewall): Con soluciones como iptables o firewalld, GNU/Linux ofrece capacidades robustas de cortafuegos, permitiendo el control y la gestión de tráfico de red para proteger la red de amenazas externas y establecer políticas de seguridad.

File Server: Implementar un servidor de archivos en GNU/Linux permite compartir recursos de almacenamiento de manera centralizada, facilitando el acceso, la gestión y la seguridad de los datos almacenados en la red. Print Server: Utilizar GNU/Linux como servidor de impresión permite centralizar y gestionar los recursos de impresión, simplificando la administración de múltiples impresoras y optimizando su uso en la red.

VPN: Configurar una red privada virtual (VPN) en GNU/Linux ofrece conexiones seguras y cifradas para acceder a la red interna desde ubicaciones externas, mejorando la seguridad y la privacidad al trabajar fuera de la red local.

8 REFERENCIAS

[1] Oracle, «Manual de usuario VirtualBox.VirtualBox» 2020. https://www.virtualbox.org/manual/

[2] R. Petersen, 22.04 LTS Desktop Applications and Administration, 2022.

[3] «DNS — NethServer 7 final,» (s.f). https://docs.nethserver.org/es/v7/dns.html.