

CONFIGURACION, PUESTA EN MARCHA Y APLICACIONES DE NETHSERVER EN GNU/LINUX

Liliana Maria Restrepo Ayala
e-mail: lmrestrepoay@unadvirtual.edu.co
James Arley Ramírez Gómez
e-mail: jaramirezgo@unadvirtual.edu.co
Carlos Mario Sánchez Toro
e-mail: cmsanchezt@unadvirtual.edu.co
Víctor Aldrin Mena Arias
e-mail: vamenaa@unadvirtual.edu.co
Víctor Manuel García Hurtado
e-mail: vmgarciah@unadvirtual.edu.co

RESUMEN: El propósito de este proyecto es abordar una problemática a nivel corporativo mediante la implementación práctica del sistema operativo GNU/Linux NethServer. Se inicia desde cero, configurando tanto el sistema de seguridad como la infraestructura de red. El trabajo resaltaré el conocimiento adquirido durante el diplomado, abarcando la implementación, configuración y desarrollo del sistema operativo Linux, destacando su gran utilidad en el entorno corporativo

PALABRAS CLAVE: Nethserver, DHCP, Proxy, VPN, Cortafuegos.

1 INTRODUCCIÓN

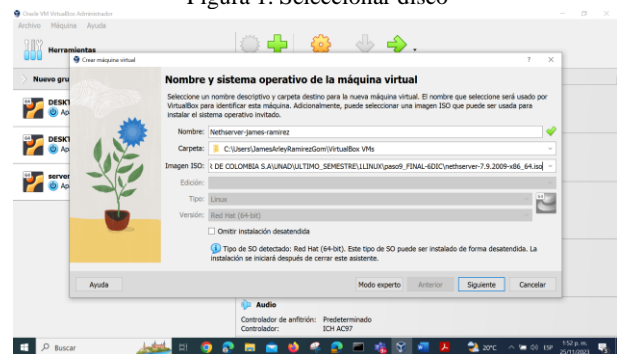
En este proyecto, se compilarán las soluciones desarrolladas a lo largo del curso con el propósito de potenciar las habilidades y el criterio profesional necesarios para enfrentar desafíos asociados con la migración de datos en sistemas operativos Linux. Asimismo, se destacará la creación de infraestructuras de red reales mediante la implementación de la distribución Ubuntu Linux. El objetivo último es adquirir conocimientos prácticos y competencias para poder brindar soluciones efectivas en este ámbito.

2 DESARROLLO DE CONTENIDOS

2.1 INSTALACION DE NETHSERVER

Para llevar a cabo la instalación, se procede a descargar el archivo ISO desde la página oficial. Posteriormente, se realizaron los ajustes necesarios en la máquina virtual para asegurar el acceso desde los clientes.

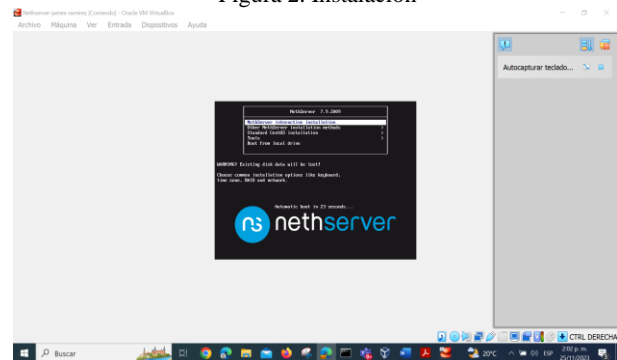
Figura 1. Seleccionar disco



Fuente: Autoría Propia

Entre las diversas opciones proporcionadas por el sistema, se optó por la instalación interactiva de Nethserver. En este caso, se procederá a instalar la versión 7.9.2009 de Nethserver.

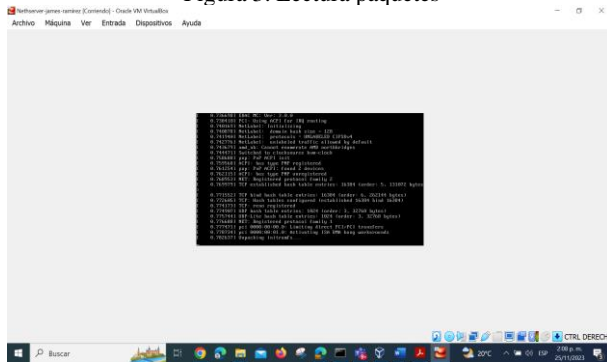
Figura 2. Instalación



Fuente: Autoría Propia

Al seleccionar la primera opción se da inicio a la instalación de los respectivos paquetes.

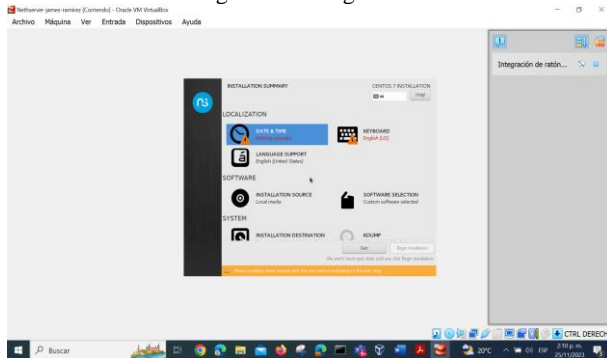
Figura 3. Lectura paquetes



Fuente: Autoría Propia

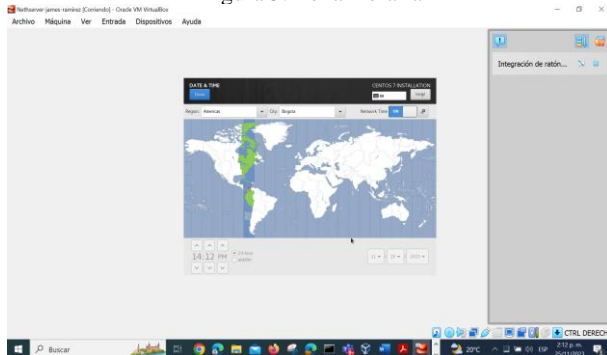
En las siguientes pantallas, se pide ajustar la zona horaria y el tipo de lenguaje en el cual se realizará la instalación.

Figura 4. Configuración



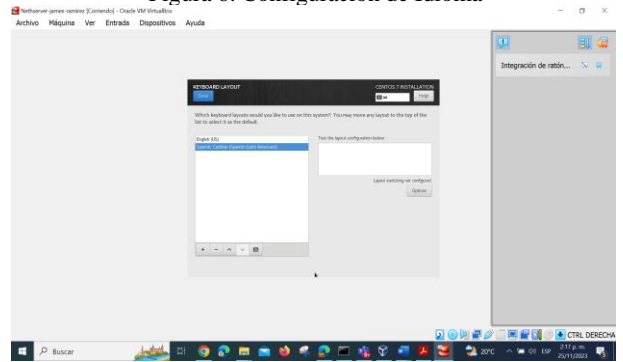
Fuente: Autoría Propia

Figura 5. Zona Horaria



Fuente: Autoría Propia

Figura 6. Configuración de Idioma



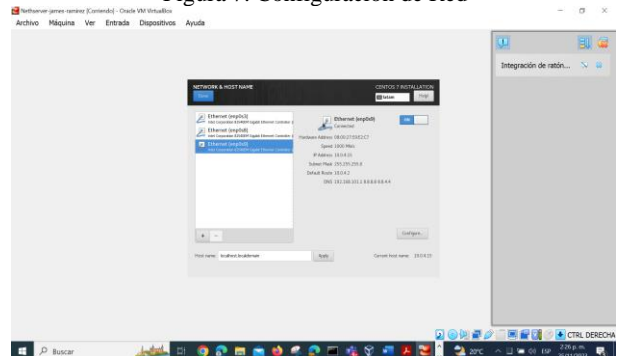
Fuente: Autoría Propia

En las opciones de red, se verifican las tarjetas de red que se encuentran disponibles.

Si se desea, se le asigna el nombre de dominio.

Si se opta por omitirlo en el momento de la instalación, se puede configurar más adelante, una vez haya finalizado la instalación.

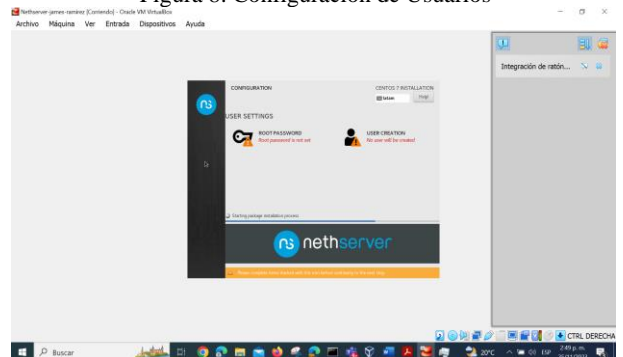
Figura 7. Configuración de Red



Fuente: Autoría Propia

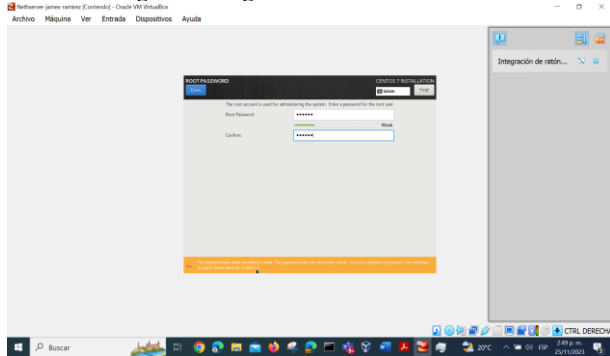
Si se desea, se puede crear una cuenta de usuario nueva, pero para este ejercicio solo se asignará la contraseña al usuario root y se continua con la instalación.

Figura 8. Configuración de Usuarios



Fuente: Autoría Propia

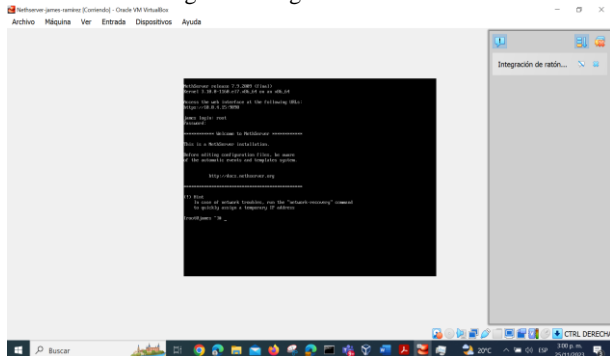
Figura 9. Asignación de contraseña root.



Fuente: Autoría Propia

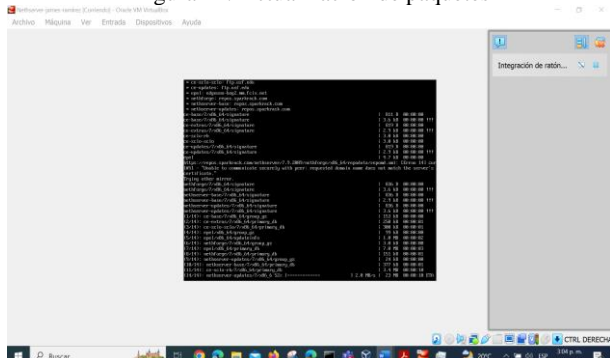
Una vez instalado y reiniciado el sistema, se confirma la IP y el puerto con el que se puede acceder a la configuración del sistema y se ingresa con el usuario root y la contraseña.

Figura 10. Ingreso a el sistema



Fuente: Autoría Propia

Figura 11. Actualización de paquetes

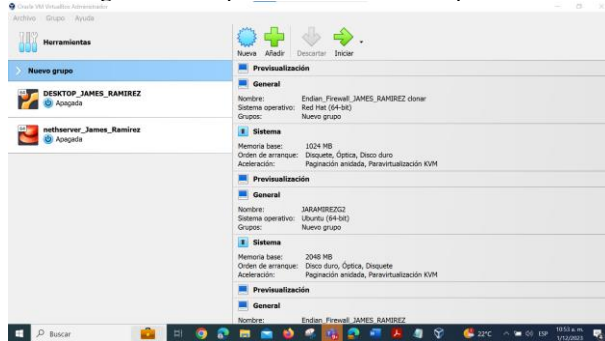


Fuente: Autoría Propia

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

Para validar el funcionamiento de estos servicios, se hará uso de una máquina con UBUNTU desktop, desde la cual se accederá a las configuraciones del Nethserver, la cual estará conectada a la red LAN (verde).

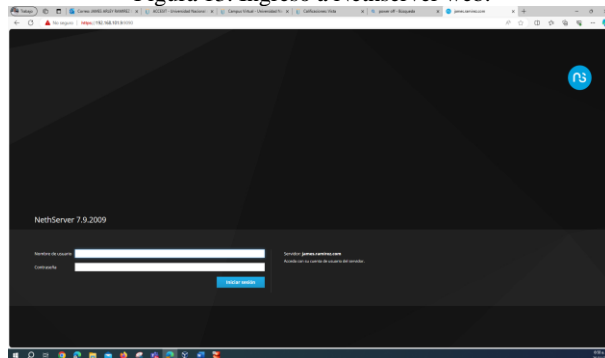
Figura 12 Comprobación de sistemas operativos



Fuente: Autoría Propia

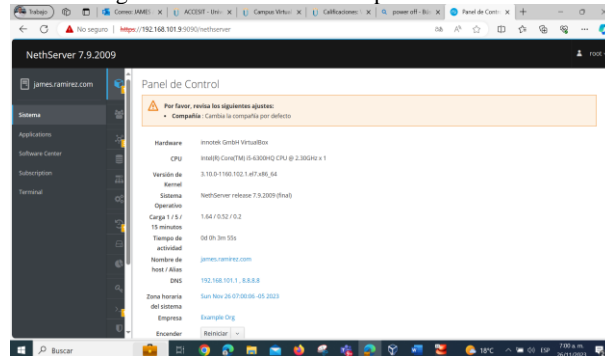
Desde la máquina con Ubuntu, se accede al servidor por medio del navegador y se valida que esté instalado y su actual versión.

Figura 13. Ingreso a Nethserver web.



Fuente: Autoría Propia

Figura 14. Visualización del panel de control

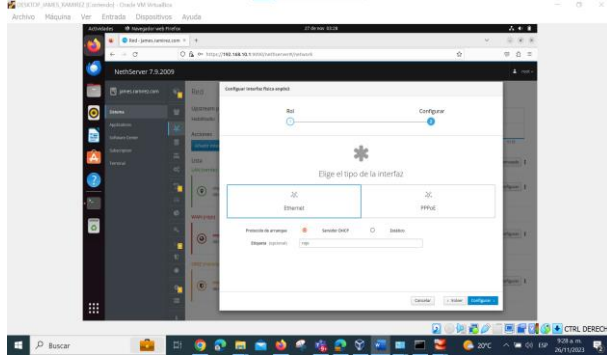


Fuente: Autoría Propia

Se procede a configurar las diferentes redes para las conexiones de los dispositivos.

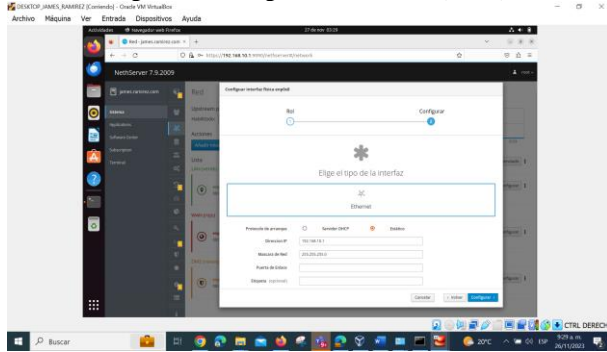
Primero se configura la red WAN (Roja) para dejarla con acceso a Internet.

Figura 15. Configuración de WAN (roja)



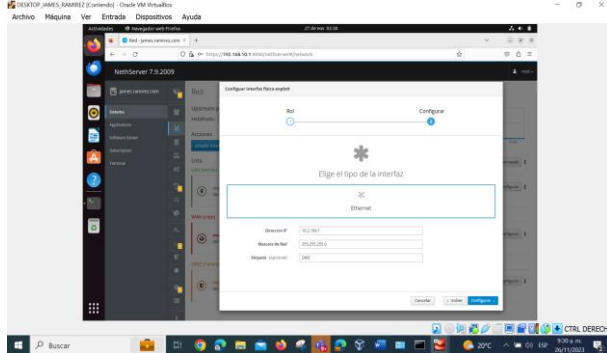
Fuente: Autoría Propia

Figura 16. configuración de LAN (verde)



Fuente: Autoría Propia

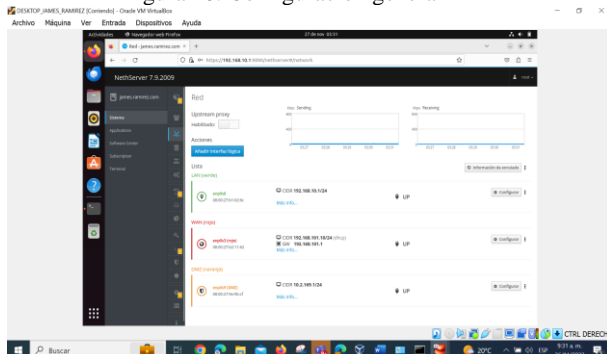
Figura 17. Configuración de DMZ (naranja)



Fuente: Autoría Propia

Se validan las nuevas configuraciones realizadas en las redes.

Figura 18. Configuración general RED

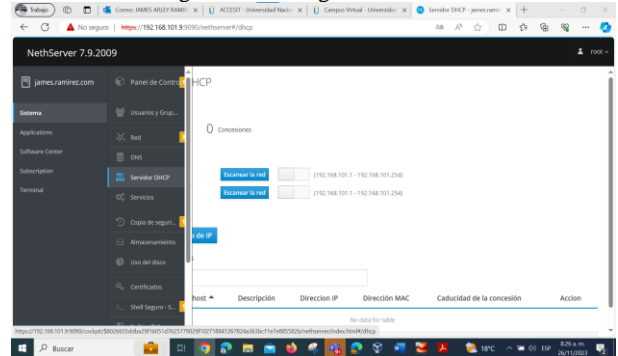


Fuente: Autoría Propia

2.2.1 DHCP SERVER

Para habilitar el DHCP, ir a Sistema / Servidor DHCP

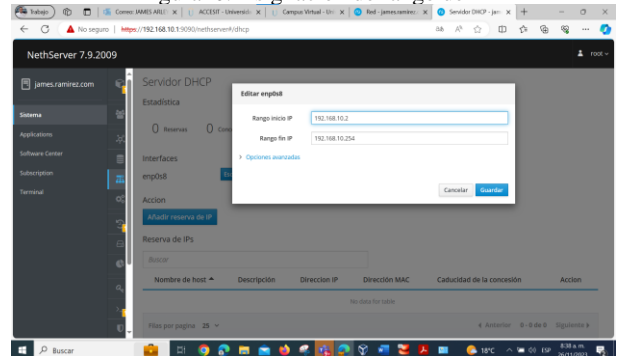
Figura 19. Configuración DHCP



Fuente: Autoría Propia

Se hace una asignación de direcciones IP para habilitar un rango para 253 máquinas.

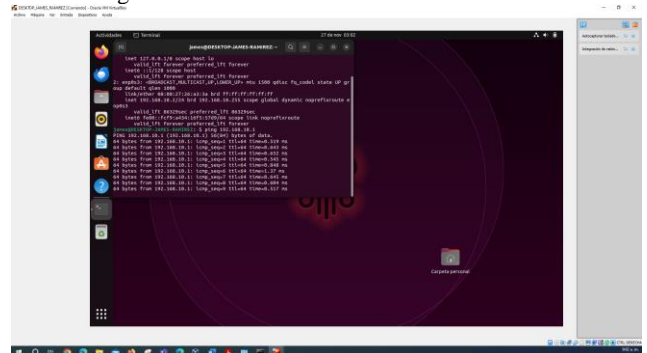
Figura 20. Asignación de rango de IP



Fuente: Autoría Propia

Para verificar que todo esté funcionando correctamente, se procede a iniciar la máquina con Ubuntu desktop, la cual había sido configurada previamente para conectarse a la red local (verde). Una vez iniciada, se le asignó una dirección IP y se pudo observar en el panel que se encontraba conectada como uno de los equipos activos en la red.

Figura 21. Validación funcionamiento DHCP

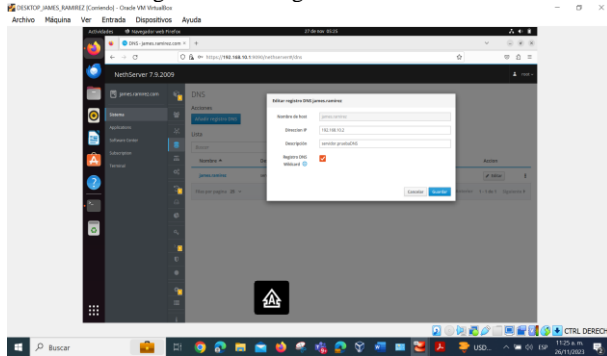


Fuente: Autoría Propia

2.2.2 DNS SERVER

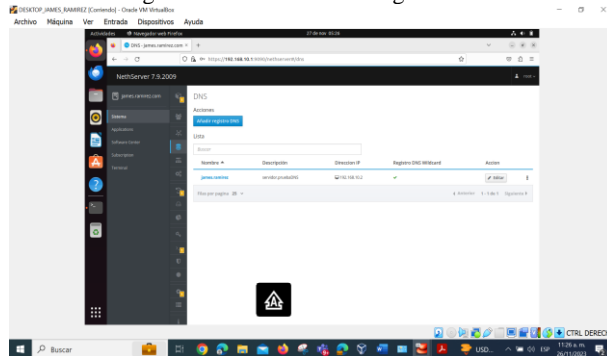
Para habilitarlo, se realiza por la opción Sistema / DNS.
Se define un nombre de Dominio y para este ejercicio se le asigna la IP 192.168.10.2

Figura 22. Configuración de dominio



Fuente: Autoría Propia

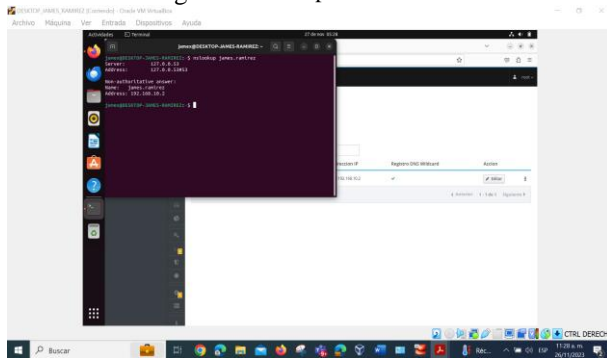
Figura 23. Validación del registro DNS



Fuente: Autoría Propia

Desde el GNU/Linux Desktop se ejecutan comandos que involucren la resolución de nombres de dominio como por ejemplo Nslookup que se encarga de consultar los servidores de nombres de Internet usando un método interactivo.

Figura 24. Comprobación DNS

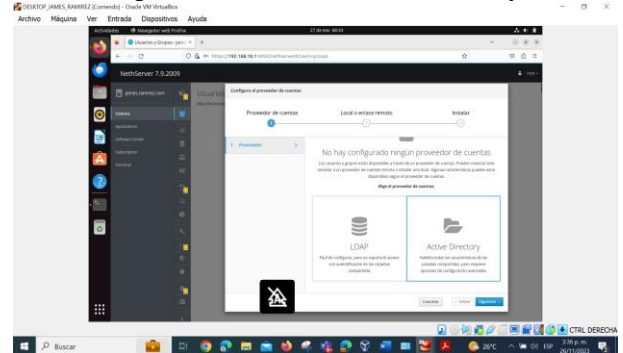


Fuente: Autoría Propia

2.2.3 CONTROLADOR DE DOMINIO

Active Directory - ir a la opción de usuarios y grupos para configurar.

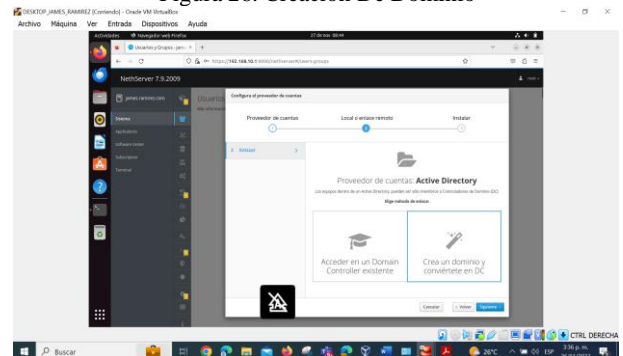
Figura 25. Instalación de Active Directory



Fuente: Autoría Propia

Se crea un nuevo controlador.

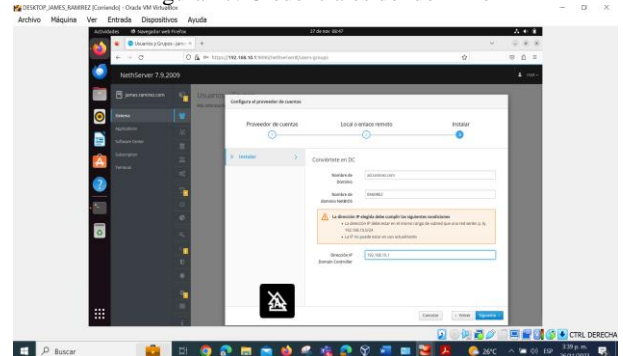
Figura 26. Creación De Dominio



Fuente: Autoría Propia

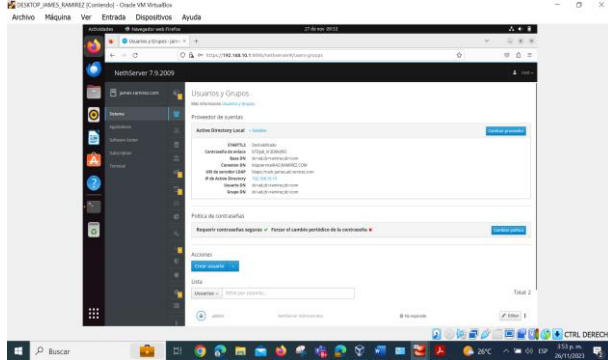
Se definen los parámetros del dominio.

Figura 27. Credenciales del dominio



Fuente: Autoría Propia

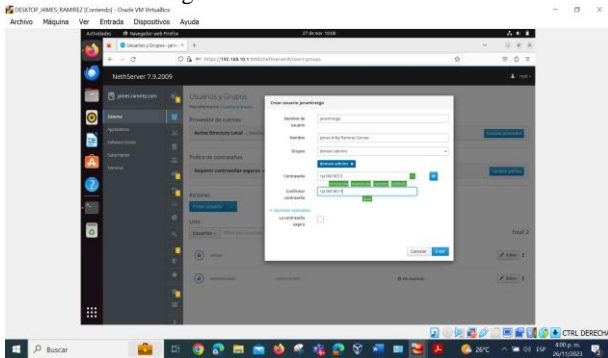
Figura 28. Validación de configuración



Fuente: Autoría Propia

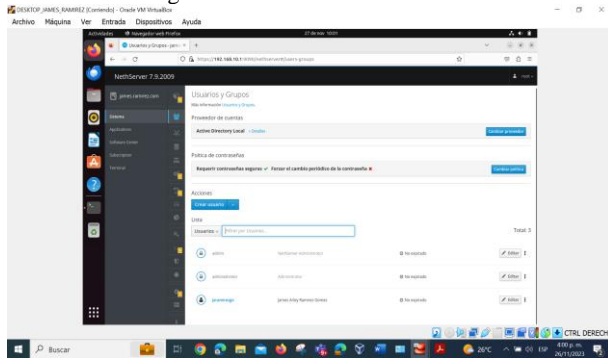
Se crea un usuario de dominio para logueo, el cual se agrega a el grupo de administradores del dominio.

Figura 29. Creación de usuario



Fuente: Autoría Propia

Figura 30. Validación de usuarios



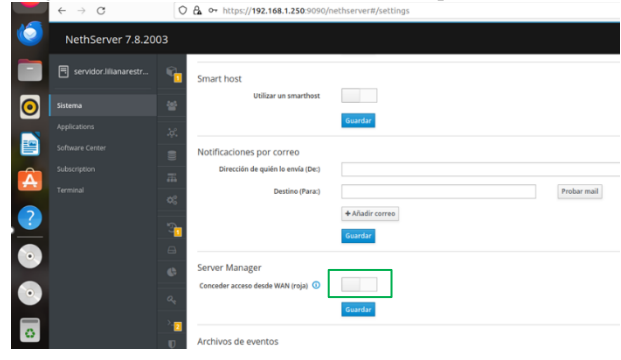
Fuente: Autoría Propia

2.3 DESARROLLO TEMÁTICA 2: PROXY.

2.3.1 CONFIGURACIÓN DE PROXY EN NETHSERVER

El objetivo de esta actividad es redirigir el tráfico por el puerto 3128, no obstante, para iniciar con este proceso se realiza unos ajustes de seguridad como lo es la restricción del acceso a internet directamente por la zona WAN, ya que el equipo Desktop debe ingresar a internet únicamente por la zona verde, a la que se encuentra conectado.

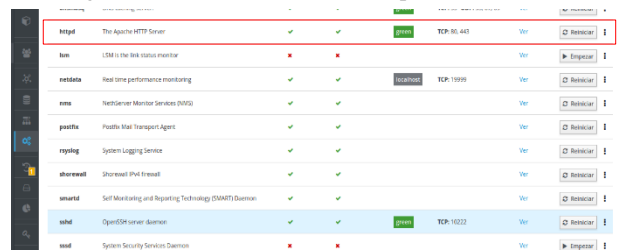
Figura 31. Restricción de acceso a internet por la zona WAN



Fuente: Autoría Propia

Se verifica la lista de servicios que se encuentran en ejecución de NethServer, con el fin de ubicar el servicio HTTPD, el cual es el servidor web y por defecto se encuentra habilitado en las zonas verde y roja, por lo tanto, se procede a habilitar su acceso únicamente a la zona verde.

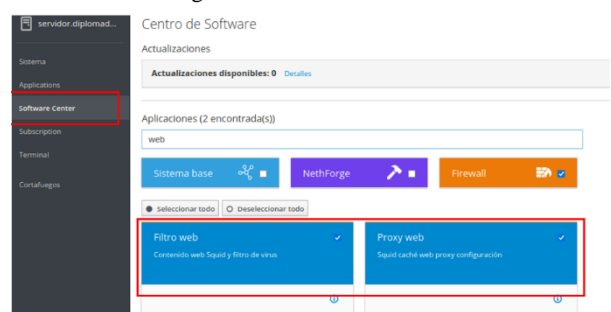
Figura 32. Acceso al servidor web por la zona verde



Fuente: Autoría Propia

Mediante el Software Center se procede a instalar dos servicios esenciales para desarrollar esta temática que son el web proxy y filtro web, y que permite definir los puertos por los cuales se redirecciona el tráfico.

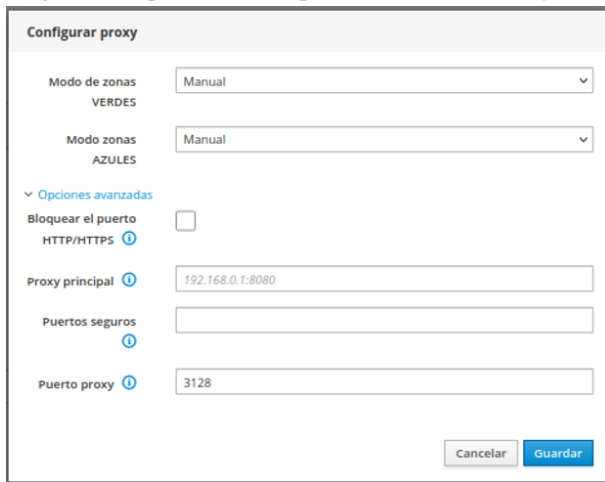
Figura 33. Validación de usuarios



Fuente: Autoría Propia

Una vez instalado, se realiza la activación del proxy, especificando el puerto 3128 mediante el modo manual de la zona verde, aunque es de aclarar que esta misma configuración por defecto se aplicará a los equipos que se encuentren conectados a la zona azul en caso de haberse configurado esta zona.

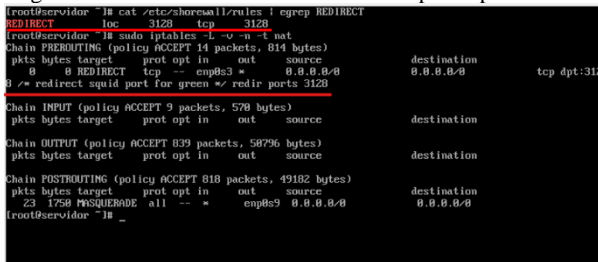
Figura 34. Especificación de puerto 3128 zonas verde y azul



Fuente: Autoría Propia

Directamente en el servidor se ejecutan los comandos `cat /etc/shorewall/rules | egrep REDIRECT` y `sudo iptables -L -v -n -t nat`, con el fin de verificar si el puerto 3128 es el único puerto disponible para el redireccionando el tráfico.

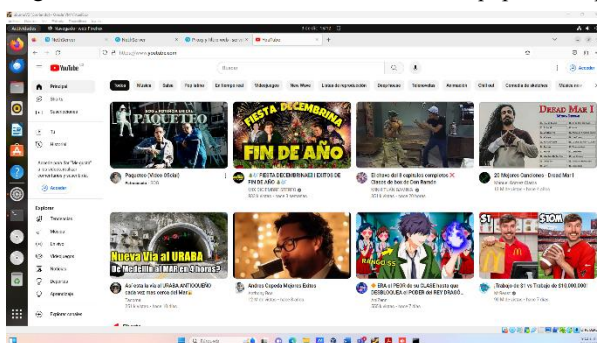
Figura 35. Redireccionamiento del tráfico por el puerto 3128



Fuente: Autoría Propia

Una vez se haya comprobado el redireccionamiento, se verifica el acceso a internet por medio del equipo desktop conectando en la red interna de la zona verde.

Figura 36. Verificando acceso a internet desde equipo desktop

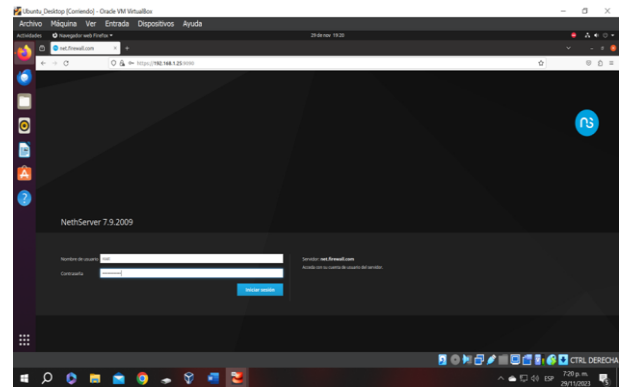


Fuente: Autoría Propia

2.4 DESARROLLO TEMÁTICA 3: FIREWALL.

Para ingresar al nethserver se debe acceder con usuario y contraseña.

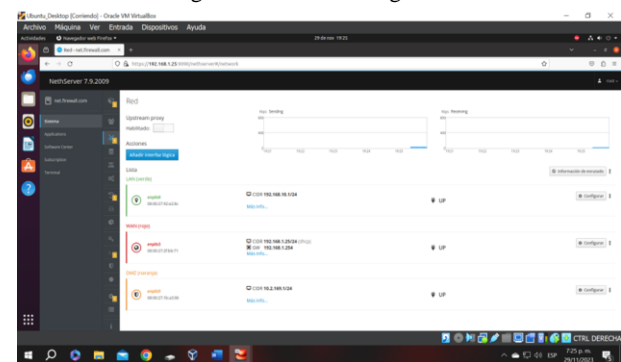
Figura 37. Ingreso al NethServer



Fuente: Autoría Propia

Se configuran las 3 redes con las que se va a trabajar.

Figura 38. Redes configuradas

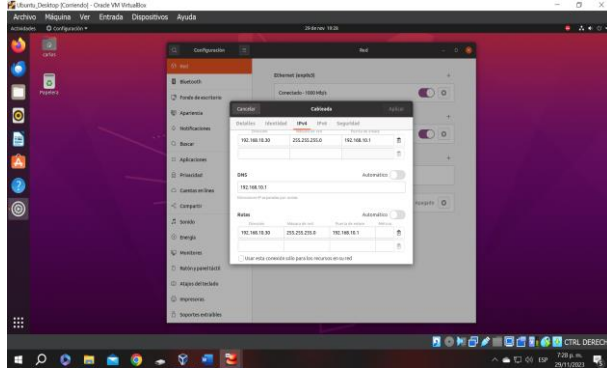


Fuente: Autoría Propia

En el desktop ingresar a la configuración de red cableada, seleccionar IPv4, marcar el modo manual, ingresar una dirección IP que corresponda a la red verde, ingresar la máscara de red e ingresar la dirección de la puerta de enlace, para este caso es la dirección IP de la zona verde configurada en el nethserver, para el DNS ingresar la dirección IP de la zona verde y deshabilitar automático, en rutas colocar los mismos datos ingresados anteriormente, por ultimo deshabilitar la opción de “usar esta conexión solo para los recursos de su red”.

Con esta configuración se garantiza que el desktop va a tener internet suministrado por la zona verde a la cual el desktop hace parte de su red.

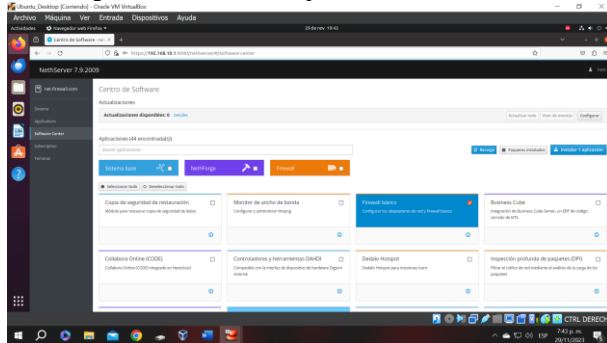
Figura 39. Configuración Red en Desktop Zona Verde



Fuente: Autoría Propia

En el menú principal seleccionar Software Center, luego seleccionar Firewall, seleccionar Firewall básico y por último dar clic al botón instalar aplicación.

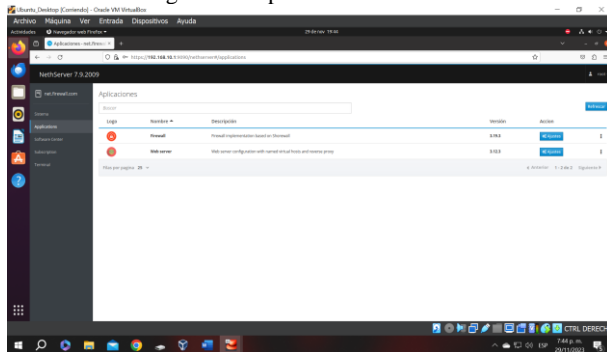
Figura 40. Instalación Aplicación Firewall Básico



Fuente: Autoría Propia

En el menú Aplicaciones se encuentran las aplicaciones instaladas, dar clic en los ajustes de firewall.

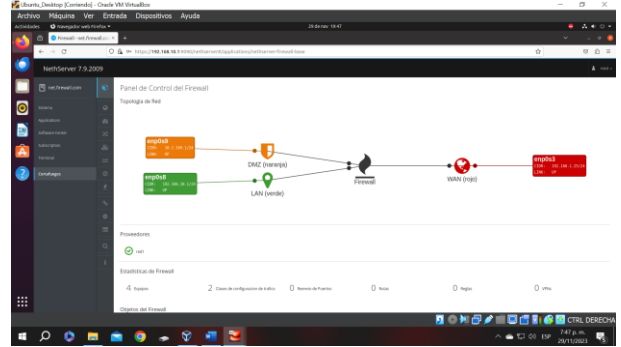
Figura 41. Aplicaciones Instaladas



Fuente: Autoría Propia

En el panel de control del firewall se observa la topología de red configurada.

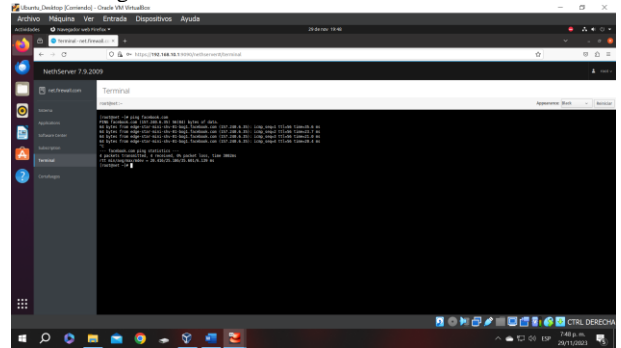
Figura 42. Topología de Red



Fuente: Autoría Propia

Se realiza un ping a la página de Facebook para validar la dirección IP.

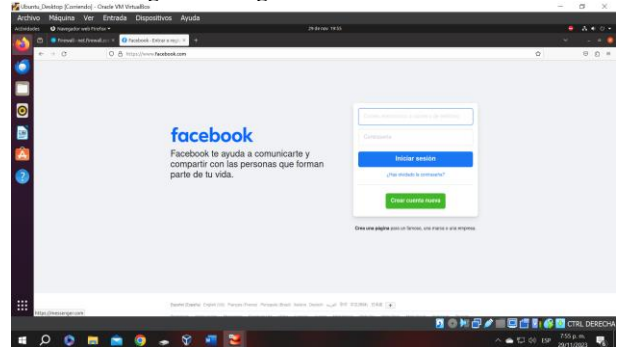
Figura 43. Validación Dirección IP Facebook



Fuente: Autoría Propia

Se verifica que la página de Facebook está habilitada.

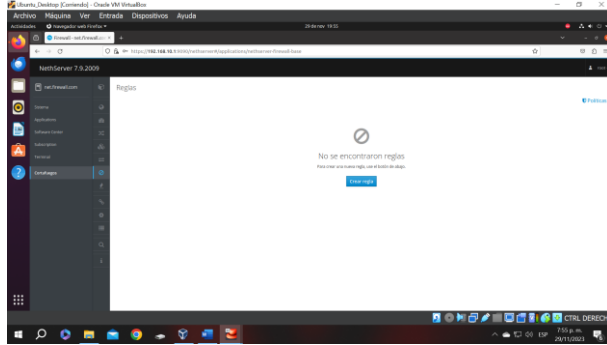
Figura 44. Página Facebook Habilitada



Fuente: Autoría Propia

Se ingresa a las configuraciones del firewall y se escoge la opción de reglas.

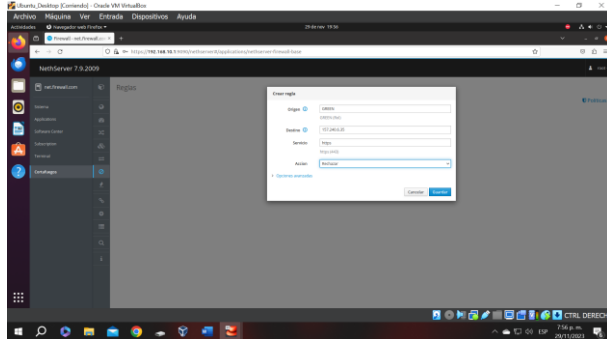
Figura 45. Crear Regla



Fuente: Autoría Propia

En el campo de origen se ingresa la zona verde, en el campo destino se ingresa la dirección IP de la página que se quiere bloquear, en este caso es la página de Facebook, en servicio se escoge https, en acción se escoge rechazar y se pulsa guardar.

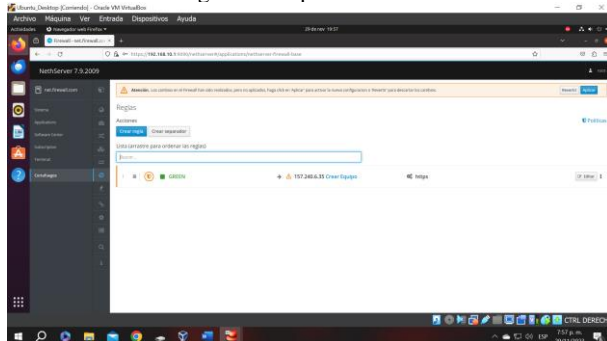
Figura 46. Creación de una Regla



Fuente: Autoría Propia

Pulsar en Aplicar para que los cambios se realicen.

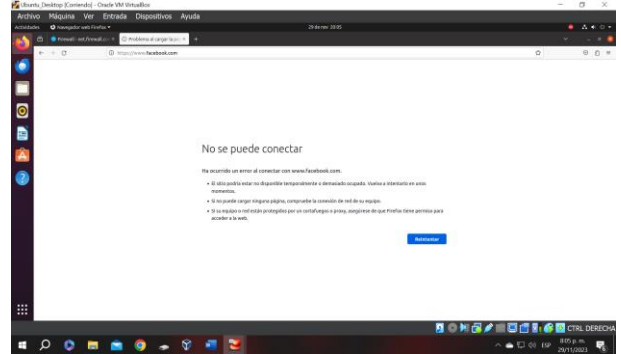
Figura 47. Aplicar Cambios



Fuente: Autoría Propia

Al ingresar a la página de Facebook esta se encuentra bloqueada.

Figura 48. Página Facebook Rechazada



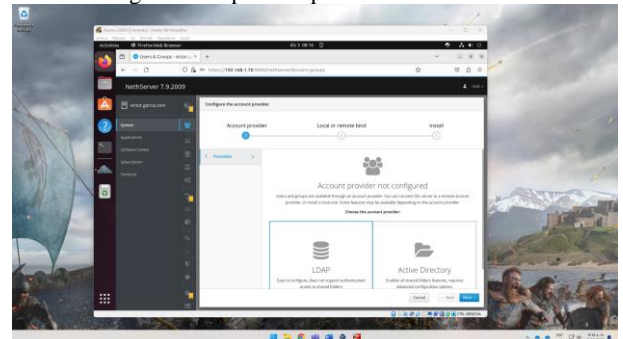
Fuente: Autoría Propia

2.5 DESARROLLO TEMÁTICA 4: FILE SERVER Y PRINT SERVER.

2.5.1 INSTALACION DE LDAP

En el módulo de Sistema seleccionamos la opción de Usuarios y Grupos, dar clic en LDAP y luego en siguiente.

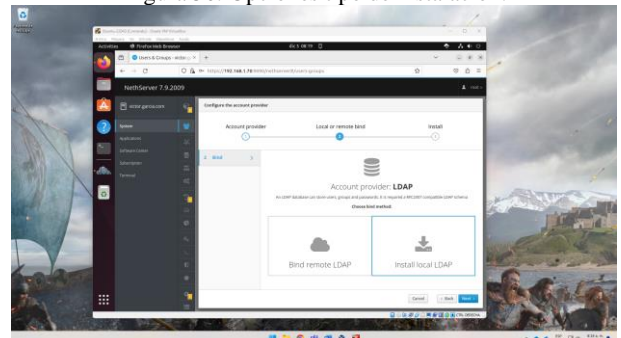
Figura 49. Opciones proveedor de cuenta



Fuente: Autoría propia

Seleccionar la opción de instalación de forma local y dar clic en siguiente para que comience la descarga.

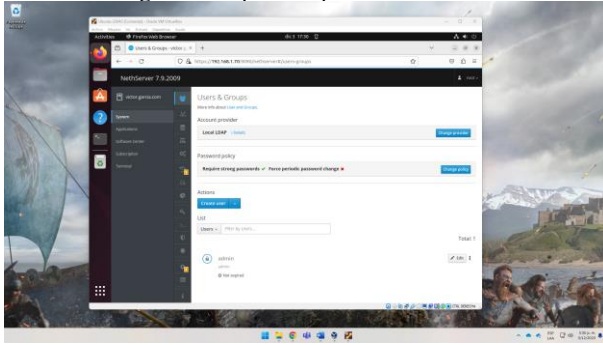
Figura 50. Opciones tipo de instalación.



Fuente: Autoría propia

Termina la descarga e instalación, proceder a crear un usuario en el módulo de Usuarios y Grupos.

Figura 51. Opciones proveedor de cuenta

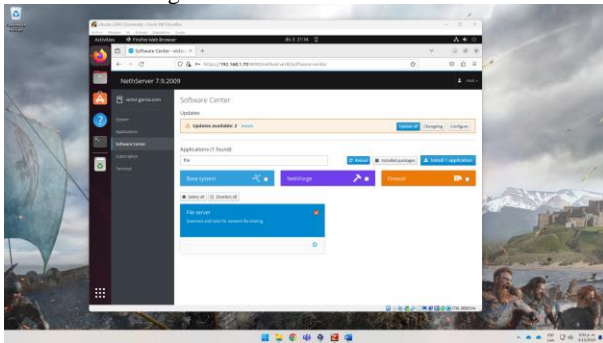


Fuente: Autoría propia

2.5.2 INSTALACION DE FILE SERVER

Dirigirse al módulo de Software Center, buscar el instalador del file server y luego en instalar.

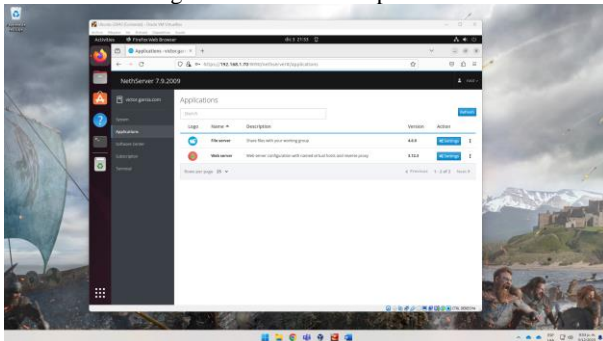
Figura 52. Instalador del file server



Fuente: Autoría propia

Verificar la adición del file server en el panel de aplicaciones.

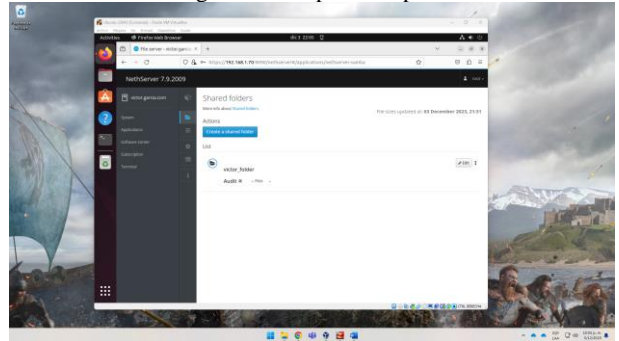
Figura 53. Módulo de aplicaciones



Fuente: Autoría propia

En el módulo de Aplicaciones, en la opción de file server dar clic en configuración, buscar el módulo de Carpetas Compartidas y crear una nueva carpeta.

Figura 54. Carpeta compartida

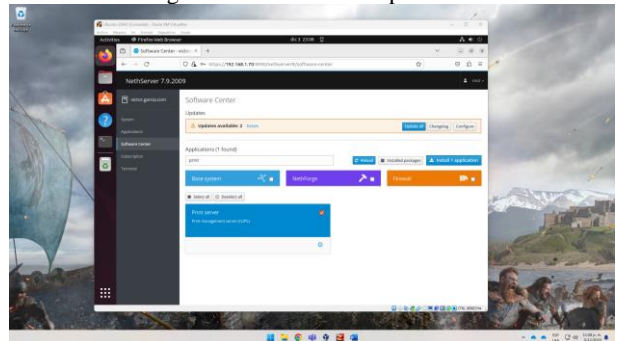


Fuente: Autoría propia

2.5.3 INSTALACION DE PRINT SERVER

Dirigirse al módulo de Software Center, buscar el instalador del print server y luego en instalar.

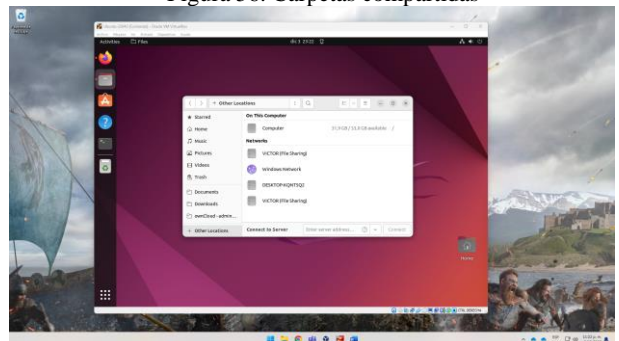
Figura 55. Instalador del print server



Fuente: Autoría propia

Dirigirse al explorador de archivos del cliente para visualizar las carpetas compartidas.

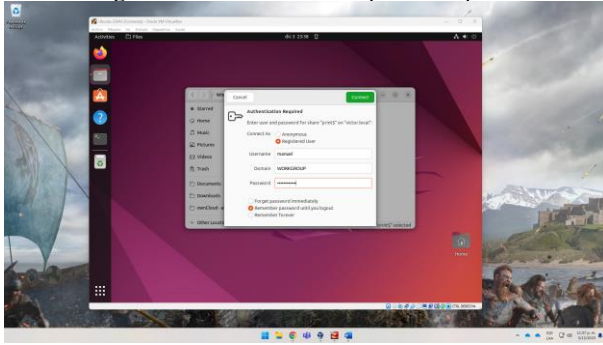
Figura 56. Carpetas compartidas



Fuente: Autoría propia

Autenticarse e ingresar a las carpetas con las credenciales del usuario anteriormente creado.

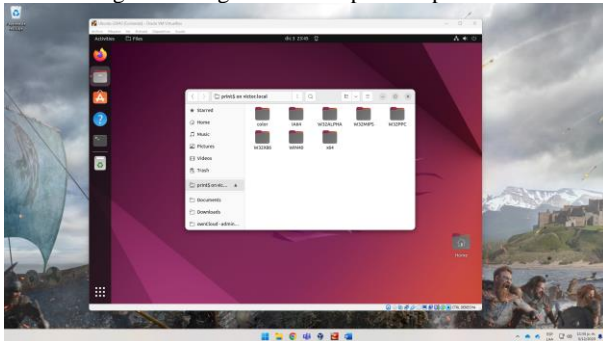
Figura 57. Autenticación carpetas compartidas



Fuente: Autoría propia

Ingresar a la carpeta del print server.

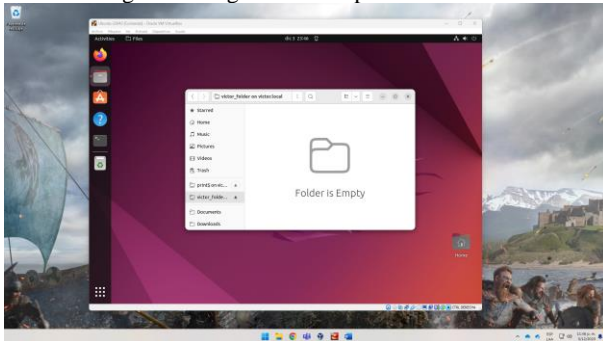
Figura 58. Ingreso a la carpeta del print server



Fuente: Autoría propia

Ingresar a la carpeta del file server.

Figura 59. Ingreso a la carpeta del file server



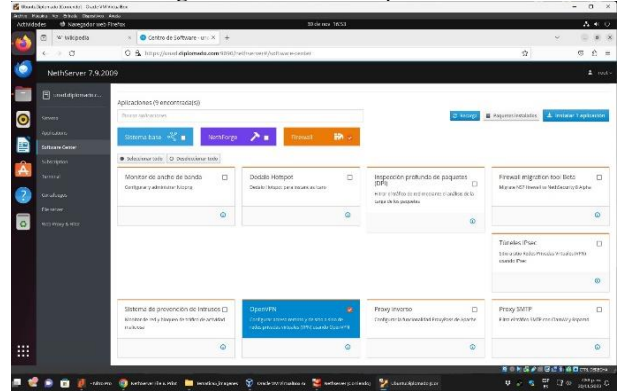
Fuente: Autoría propia

2.6 DESARROLLO TEMÁTICA 5: VPN.

2.6.1 CONFIGURACIÓN DE VPN EN NETHSERVER

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

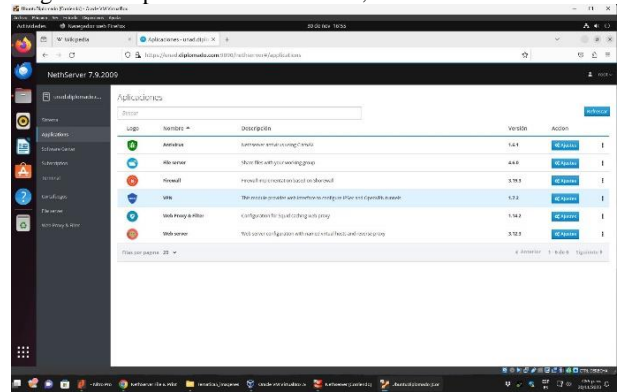
Figura 60. El módulo OpenVPN.



Fuente: Autoría propia

Este módulo es el encargado de implementar el VPN en Nethserver.

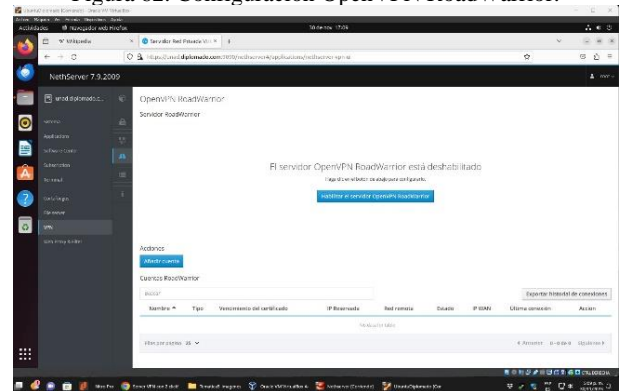
Figura 61. Aplicaciones Nethserver, observa el módulo VPN.



Fuente: Autoría Propia

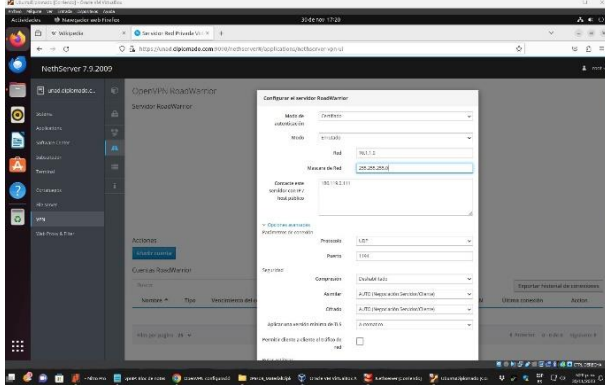
Este módulo provee de servicio como IPSec y OpenVPN.

Figura 62. Configuración OpenVPN RoadWarrior.



Fuente: Autoría Propia

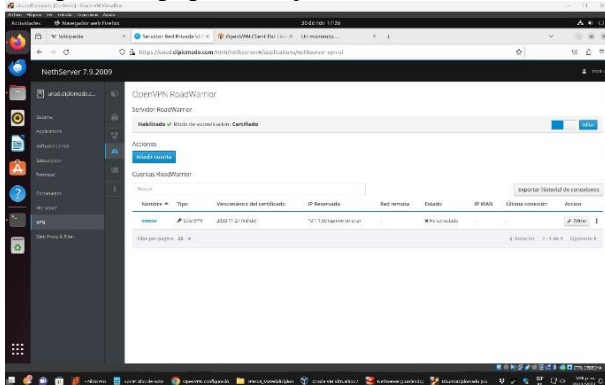
Figura 63. Aplicaciones Nethserver, observa el módulo VPN.



Fuente: Autoría Propia

Es esta configuración se genera el Certificado y el protocolo de conexión, para este ejemplo se emplea la IP 10.1.1.0 y de host publico 186.119.0.111.

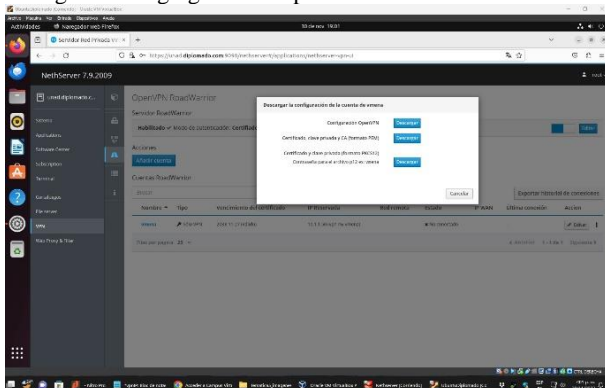
Figura 64. Agregar cuenta para el servidor RoadWarrior.



Fuente: Autoría Propia

Para este ejemplo práctico se emplea el nombre “vmena” y de tipo “Solo VPN”.

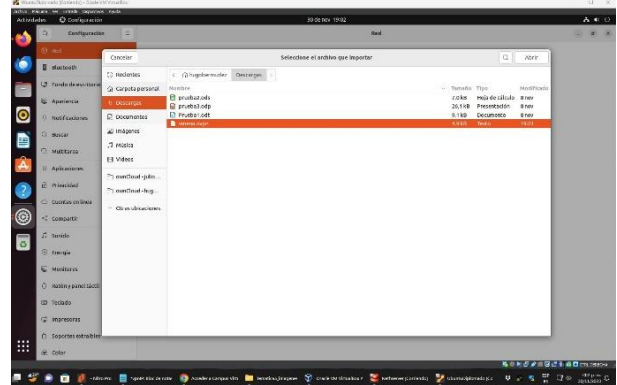
Figura 65. Agregar cuenta para el servidor RoadWarrior.



Fuente: Autoría Propia

En el módulo principal de OpenVPN RoadWarrior se encontrará la opción de descarga para los certificados del VPN en dos formatos, PEM y PXCS12.

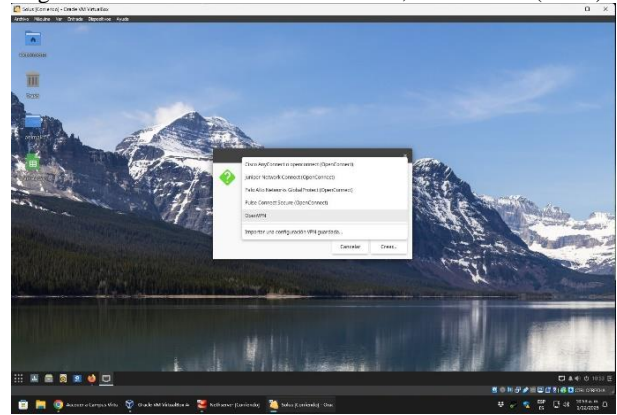
Figura 66. Certificado para VPN el archivo “vmena.ovpn”.



Fuente: Autoría Propia

La configuración para el VPN se puede almacenar en un archivo para su rápida implementación.

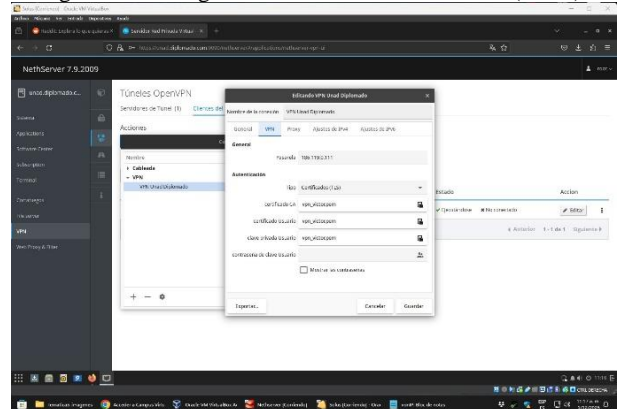
Figura 67. Prueba en un sistema Cliente, distribución (Solus).



Fuente: Autoría Propia

En este sistema también se encuentra la opción de OpenVPN en su configuración de red.

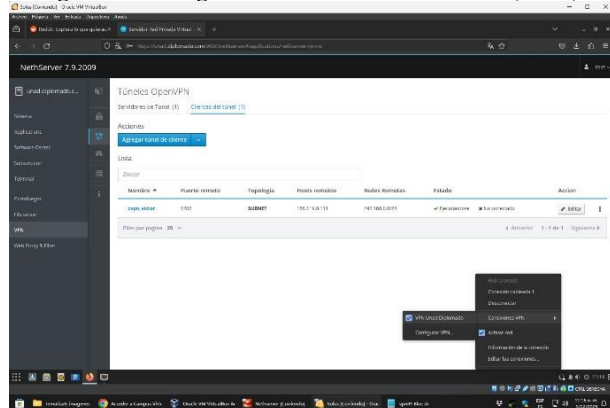
Figura 68. Configurando VPN en usuario cliente (Solus).



Fuente: Autoría Propia

Para este ejemplo práctico, la conexión VPN recibe el nombre de “VPN Unad Diplomado”.

Figura 69. Configurando VPN en usuario cliente (Solus).



Fuente: Autoría Propia

En la barra de tareas, se comprueba la conexión al VPN.

3 CONCLUSIONES

La implementación y configuración exitosa de un DHCP Server, DNS Server y Controlador de Dominio son elementos cruciales para la administración eficiente de redes en entornos GNU/Linux. Estos componentes no solo facilitan la asignación dinámica de direcciones IP, sino que también optimizan la resolución de nombres y la gestión centralizada de usuarios y recursos a través del Controlador de Dominio. La conclusión resalta la importancia de estas herramientas en la creación de redes robustas y fácilmente gestionables en el ecosistema Linux.

La implementación de un Proxy en entornos GNU/Linux se revela como una medida esencial para gestionar y optimizar el tráfico web. Este componente no solo mejora el rendimiento al almacenar en caché recursos, sino que también proporciona un control avanzado sobre el acceso a la web y la seguridad. La conclusión subraya la importancia del Proxy como una herramienta versátil para mejorar la eficiencia y la seguridad en el acceso a Internet en sistemas basados en Linux.

La configuración de un Cortafuegos en sistemas GNU/Linux es crucial para garantizar la seguridad de la red al controlar el tráfico de entrada y salida. La conclusión destaca la importancia de diseñar reglas precisas y gestionar adecuadamente las políticas de seguridad para proteger el sistema contra amenazas externas. La implementación exitosa de un Cortafuegos fortalece la postura de seguridad del sistema operativo, salvaguardando la integridad y confidencialidad de los datos.

El desarrollo de un File Server y Print Server en entornos GNU/Linux se revela como un componente esencial para la gestión eficiente de archivos y recursos de impresión en redes. La conclusión destaca la importancia de estos servicios al facilitar el intercambio de archivos y la administración centralizada de impresoras. La implementación exitosa de estas temáticas contribuye a una mayor productividad y organización en el entorno Linux.

La implementación de una VPN en entornos GNU/Linux emerge como una solución esencial para garantizar la seguridad

de las comunicaciones en redes, especialmente en entornos donde la privacidad y la integridad de los datos son prioritarias. La conclusión subraya la importancia de establecer conexiones seguras y cifradas, proporcionando a los usuarios una vía segura para acceder a recursos de red de forma remota.

4 REFERENCIAS

Pizarro Galán, A. M. y Pizarro Galán, A. M. (2017). Linux para usuarios. Madrid, Spain: Ministerio de Educación de España. (Páginas. 99 - 126). eLibro. <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/49434?page=99>

RedesZone (2016). NethServer: conoce esta distro basada en CentOS/RHEL. <https://www.redeszone.net/2016/09/26/nethserver-conoce-estadistro-basada-centosrhel-crear-propio-servidor-casa-u-oficina/>

Gómez López, J. (2015). Administración de sistema operativos. Madrid, Spain: RA-MA Editorial. (Páginas. 242 - 249). eLibro. <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=242>

Pizarro Galán, A. M. y Pizarro Galán, A. M. (2017). Linux para usuarios. Madrid, Spain: Ministerio de Educación de España. (Páginas.307 - 320). eLibro. <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/49434?page=307>

Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial. eLibro. <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92>