

“IMPLEMENTACIÓN DE SERVICIOS EN NETHSERVER “

Anyi Tatiana Noscue Otela
e-mail: atnoscueo@unadvirtual.edu.co
Yony Alfredo Ortega Solarte
e-mail: yaortegas@unadvirtual.edu.co
Luis Antonio Almeida Paz
e-mail: laalmeidap@unadvirtual.edu.co
Angie Katherine Achicanoy Guevara
e-mail: akachicanoyg@unadvirtual.edu.co
Wilson Josimar Angulo Domínguez
e-mail: wjangulod@unadvirtual.edu.co

RESUMEN: El propósito de este documento es presentar la instalación y configuración de NethServer como medida técnica para avanzar hacia la plataforma de administración de infraestructura de tecnologías de la información. A través de esta implementación, se busca proporcionar soluciones integrales para cada una de las temáticas planteadas, teniendo en cuenta los aspectos relacionados con el funcionamiento de DHCP, DNS, controlador de dominio, proxy, cortafuegos, file server y Print server, así como los servicios VPN. En última instancia, el objetivo principal de esta actividad es implementar con éxito, bajo el entorno GNU/Linux, una infraestructura técnica capaz de cumplir con las necesidades particulares del cliente.

PALABRAS CLAVE: DHCP, DNS, NethServer, Proxy

INTRODUCCIÓN

NethServer es un sistema operativo de código abierto para los entusiastas de Linux, diseñado para oficinas pequeñas y medianas empresas [1]. Es muy sencillo, seguro y flexible [1]. Está listo para entregar mensajes, para proteger la red con el servidor de seguridad incorporado, compartir archivos y mucho más, todo en el mismo sistema [1]. Esto implica la implementación detallada de servicios esenciales como DHCP, DNS y Controlador de Dominio, con configuración es específicas para proxy, seguridad y control preciso del cortafuegos. También permite una configuración detallada para el acceso a estaciones de trabajo mediante File Server y Print Server, demostrando compromiso con la optimización. Además, posibilita la configuración de VPN para crear un túnel privado seguro, mejorando la privacidad y seguridad en las comunicaciones a través de Internet u otra red pública.

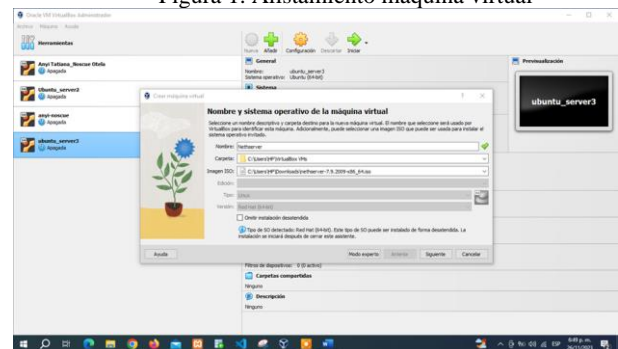
INSTALACIÓN NETHSERVER

1.1 URL DE DESCARGA

Ingresar al sitio oficial de NethServer y descargar la imagen ISO <https://www.NethServer.org/>

En la Figura 1. Se puede ver que primero hay que crear una nueva máquina virtual llamada NethServer ajustar los parámetros necesarios, asignar el tamaño de memoria RAM de acuerdo a las necesidades y recursos del sistema y agregar la imagen ISO.

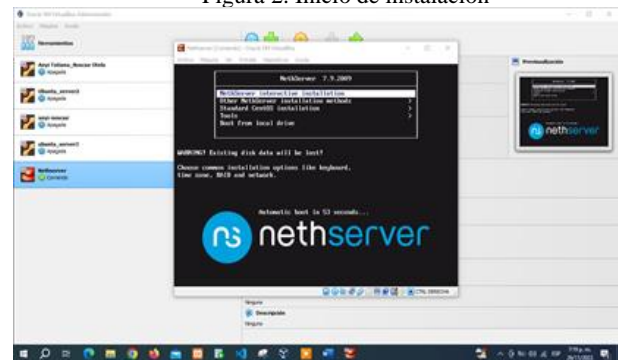
Figura 1. Alistamiento máquina virtual



Fuente: Autoría propia

En la Figura 2. Se puede ver que después de iniciar la maquina debe aparecer la primera pantalla de NethServer en la máquina virtual donde hay que seleccionar la primera opción y presionar la tecla intro para continuar con la instalación.

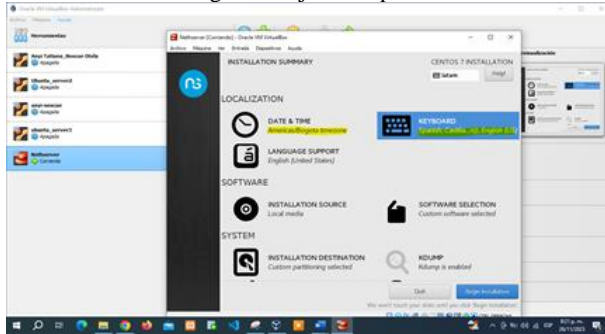
Figura 2. Inicio de instalación



Fuente: Autoría propia

En la Figura 3. Se puede ver que hay que configurar los parámetros de localización en este caso es (América-Bogotá) así como también ajustar la distribución del teclado al idioma español.

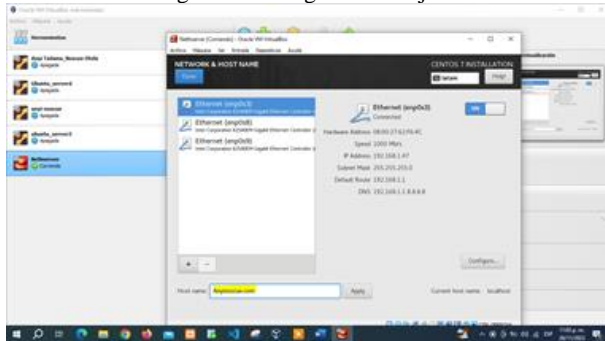
Figura 3. Ajuste de parámetros



Fuente: Autoría propia

En la Figura 4. Se puede ver que están activas tres tarjetas de red en el equipo donde una es para la WAN, otra para la LAN y una tercera para invitados. También se ajusta un nombre para el equipo en este caso es Anyinoscue.com

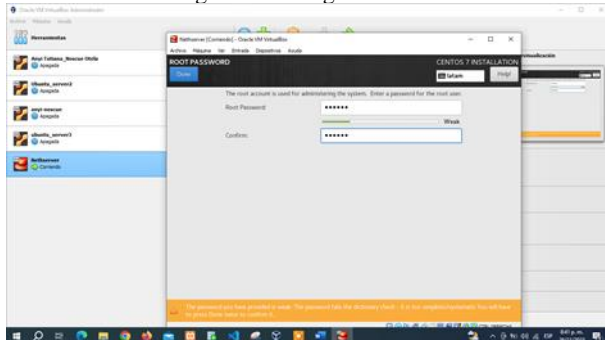
Figura 4. Configuración tarjeta de red



Fuente: Autoría propia

En la Figura 5. Se puede ver que hay que asignar una contraseña al administrador de cuenta NethServer la cual debe ser lo suficientemente fuerte para garantizar la seguridad de la información.

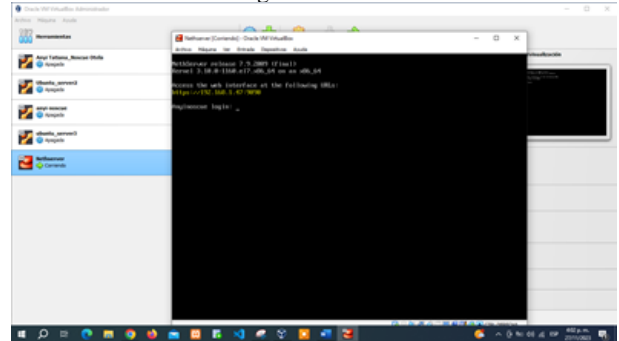
Figura 5. Configurar usuario root.



Fuente: Autoría propia

En la Figura 6. Se muestra que luego de realizar la instalación, el sistema se reiniciara y después da una dirección IP de acceso con el puerto 9090 para que los datos puedan ser dirigidos correctamente a su destino y con ello se ingresa de manera correcta al NethServer.

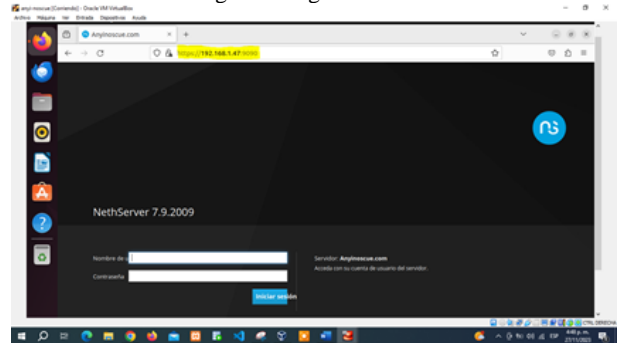
Figura 6. IP de acceso



Fuente: Autoría propia

En la Figura 7. Se muestra el ingreso a NethServer por medio del navegador Mozilla desde la maquina Ubuntu Anyi_Noscue validando que esté instalado y en la versión actual por medio de la dirección IP 192.168.1.47:9090

Figura 7. Ingreso a NethServer



Fuente: Autoría propia

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

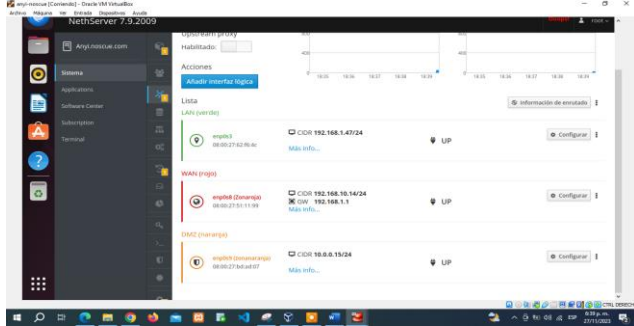
Para iniciar con el desarrollo de la temática primero se da una breve descripción de los servicios a implementar.

Los servicios de DHCP facilitan el uso de red o el Internet [2]. Mientras que el DNS se utiliza para convertir el nombre de un sitio web como FS.com a su dirección IP y viceversa [2]. Por otra parte, el controlador de dominio es un servidor que responde a las solicitudes de "Autenticación de Seguridad" dentro de un Dominio [3].

DHCP server

En la Figura 8. Se muestra la configuración de las interfaces de las zonas verdes, naranja y roja donde a cada una se le agrega una IP diferente para evitar conflictos.

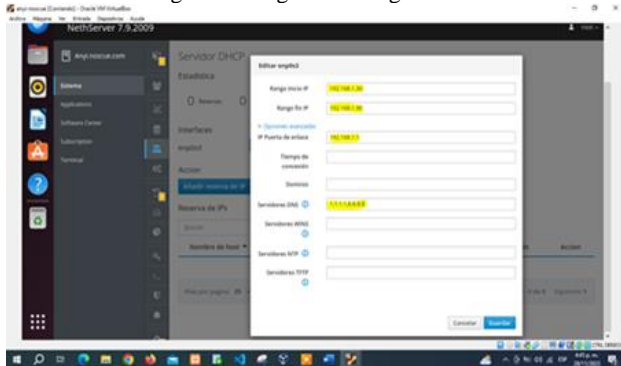
Figura 8. Configuración de interfaces



Fuente: Autoría propia

En la Figura 9. Se muestra el rango DHCP el cual se establece dentro de la red correspondiente a la red asociada en este caso la enp0s3 zona verde con una IP 192.168.1.47 donde el rango que se estableció es la 192.168.1.30 a 192.168.1.90.

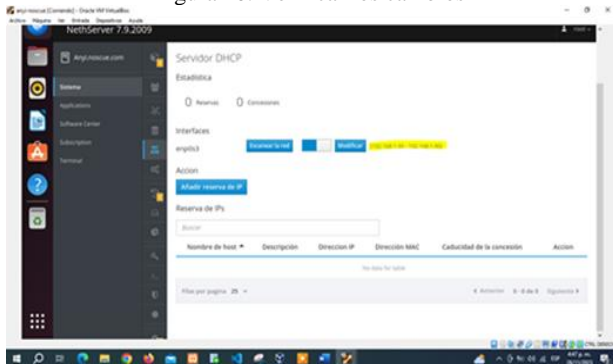
Figura 9. Asignación rango de IP



Fuente: Autoría propia

En la Figura 10. Se muestra que el servidor DHCP quedo habilitado y que los cambios fueron tomados correctamente lo que genera la conexión para un rango de 90 equipos.

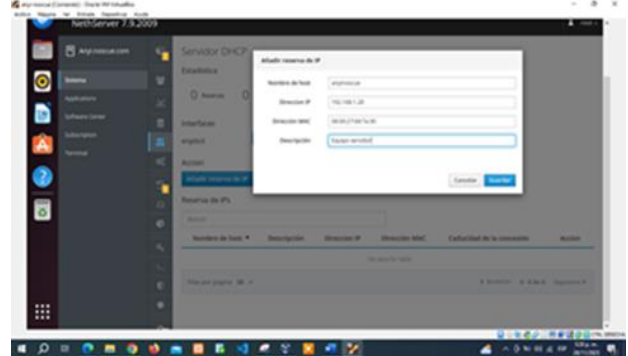
Figura 10. Verificar los cambios



Fuente: Autoría propia

En la Figura 11. Se muestra la configuración de la maquina Ubuntu server3 en DHCP para que se conecte a través de la red LAN verde conectada a la IP asignada bajo el rango de direcciones que se estableció.

Figura 11. Configurar maquina Ubuntu_server3

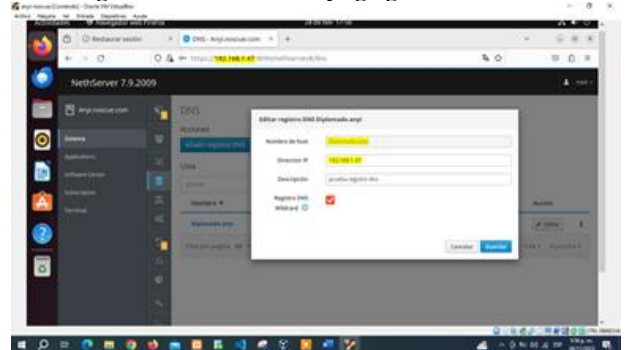


Fuente: Autoría propia

DNS Server

En la Figura 12. Se muestra como habilitar el DNS y agregar un nuevo registro para facilitar la comunicación y acceso a los servicios de la red que solo está disponible dentro de la red LAN (zona verde) a su vez se añade un nombre de dominio.

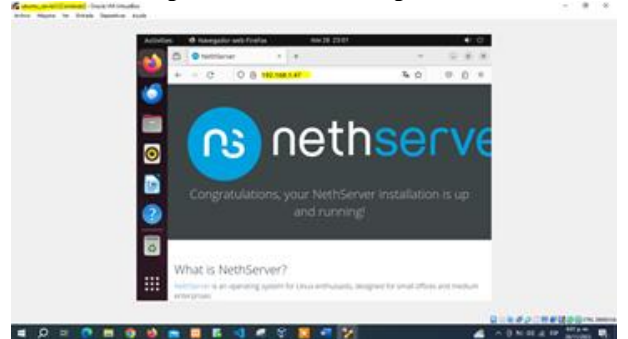
Figura 12. Habilitar DNS y agregar nombre de dominio



Fuente: Autoría propia

En la Figura 13. Se muestra que el servidor DNS haya quedado configurado correctamente y esto se evidencia al ingresar a la maquina Ubuntu_Server con la dirección IP 192.168.1.47 y este cumple con la petición.

Figura 13. Verificar configuración DNS



Fuente: Autoría propia

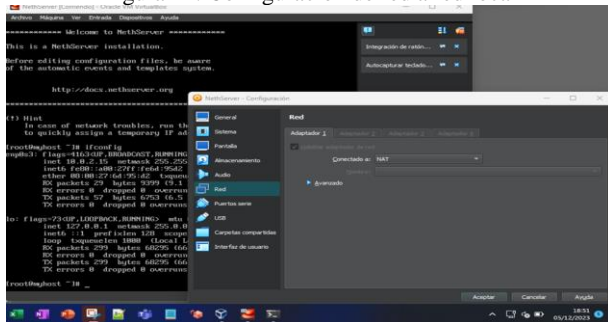
TEMÁTICA 2: PROXY

Un servidor proxy actúa como intermediario entre los usuarios y los servidores de destino [4]. Cuando un usuario solicita un recurso, como un archivo, página web u otro recurso, el servidor proxy intercepta la solicitud y la envía al servidor de destino en nombre del usuario [4]. El servidor de destino envía luego la respuesta al servidor proxy, que, a su vez, la reenvía al usuario [4]. Los proxis se utilizan para varios propósitos, incluyendo la mejora de la seguridad, el control de acceso a Internet, la aceleración del rendimiento y el filtrado de contenido [4].

En la figura 14. Se muestra la configuración actual de la red, la cual está establecida en el modo de Traducción de direcciones de red de manera predeterminada. No obstante, debido a ciertas circunstancias o necesidades específicas, se procede a realizar un cambio en la configuración. Este cambio implica la transición al modo de adaptador puente. La razón detrás de esta modificación radica en la intención de asignar una dirección IP perteneciente a la red local.

En la Figura 14. Se muestra Configuración actual de red es NAT por defecto, sin embargo, dado que no se la alcanza, se hará el cambio a Adaptador de puente para que se le asigne una IP de la red local.

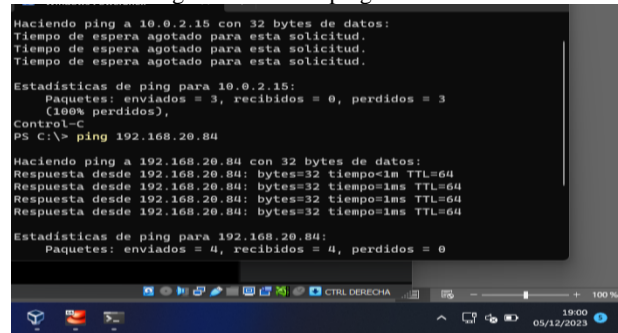
Figura 14. Configuración de red a red local



Fuente: Autoría propia

En la Figura 15. Se muestra la realización de prueba ping, para observar que ahora ya se alcanza la máquina. En este contexto específico, la prueba de ping se lleva a cabo después de haber realizado el cambio en la configuración de red, específicamente la transición al modo adaptador puente. La finalidad de esta prueba es confirmar que la máquina ahora puede ser alcanzada o accedida desde otros dispositivos en la misma red local. Si la prueba de ping es exitosa, esto indicará que la máquina responde adecuadamente a las solicitudes de red, confirmando así la efectividad del cambio realizado en la configuración.

Figura 15. Prueba ping dirección IP

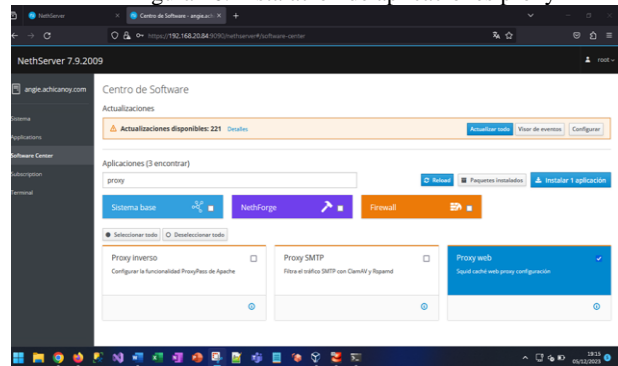


Fuente: Autoría propia

En la Figura 16. Se muestra la instalación de las aplicaciones del proxy después de haber ingresado a NethServer con usuario y contraseña. Una vez que el usuario ha iniciado sesión en NethServer, el cual es un sistema operativo de servidor basado en Linux, se procede a instalar las aplicaciones relacionadas con el proxy. Estas aplicaciones son esenciales para gestionar y controlar el tráfico de red, especialmente cuando se busca mejorar la seguridad, la eficiencia y la monitorización del uso de Internet en una red específica.

La instalación de estas aplicaciones involucra la selección de opciones específicas, la configuración de parámetros relevantes y posiblemente la descarga e instalación de paquetes de software adicionales. Es posible que en la figura 16 se muestren interfaces gráficas o comandos de terminal que reflejen este proceso de instalación.

Figura 16. Instalación de aplicaciones proxy

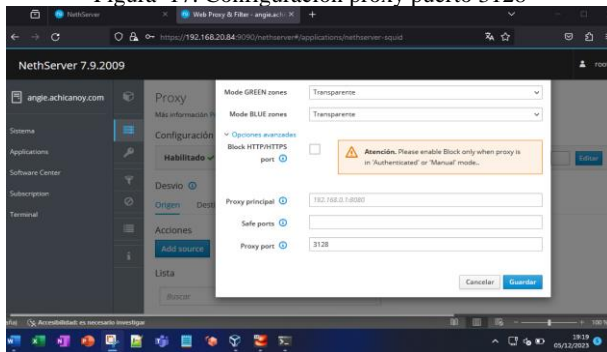


Fuente: Autoría propia

En la Figura 17. Se muestra la configuración de los modos de las zonas como "transparent" para que permitan el tráfico sin restricciones y en opciones avanzadas, se configura el puerto del proxy como 3128, todo esto a través de NethServer en la opción de sistema. Además, en las opciones avanzadas, se lleva a cabo una configuración adicional al establecer el puerto del proxy como 3128.

Este paso indica que el servidor proxy está escuchando en el puerto 3128 para las solicitudes de tráfico. La selección específica de este puerto es una decisión estratégica que puede estar basada en estándares comunes o en los requisitos particulares del entorno de red.

Figura 17. Configuración proxy puerto 3128



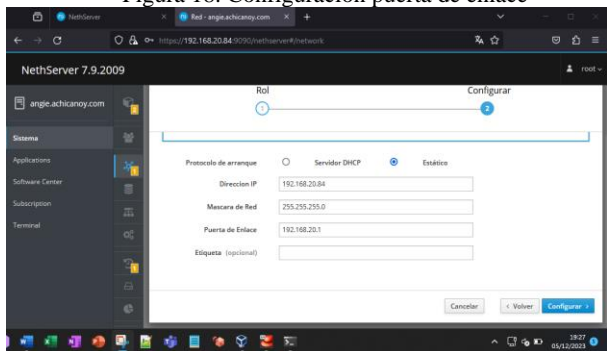
Fuente: Autoría propia

En la Figura 18. Se muestra la configuración realizada correspondiente a la puerta de enlace utilizada, esto a través de NethServer. Este paso es crítico, ya que la puerta de enlace (Gateway) juega un papel fundamental en la dirección del tráfico de red entre la red local y redes externas, como Internet.

La figura muestra interfaces gráficas o ajustes específicos que permiten al usuario o administrador de red especificar la puerta de enlace que utilizará el sistema. La configuración de la puerta de enlace es esencial para garantizar que el tráfico de red se dirija de manera eficiente y efectiva a través de la conexión adecuada.

En entornos de red, la puerta de enlace suele ser la dirección IP del dispositivo que actúa como el punto de acceso a otras redes, como un enrutador [5]. Configurar correctamente la puerta de enlace es vital para asegurar una conectividad fluida y un enrutamiento eficiente de los datos [5].

Figura 18. Configuración puerta de enlace



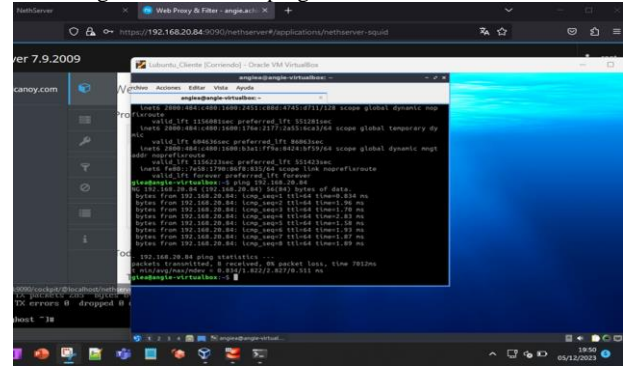
Fuente: Autoría propia

En la Figura 19. Se muestra la prueba realizada a través de Ubuntu haciendo ping a la dirección IP configurada en NethServer. Esta prueba es crucial para validar que la configuración realizada en NethServer, incluyendo la asignación de direcciones IP, la configuración de la puerta de enlace y otros ajustes de red, se haya llevado a cabo correctamente.

Además, sirve para confirmar que el sistema Ubuntu puede comunicarse adecuadamente con NethServer a través de la red, lo cual es esencial para el funcionamiento correcto de la

infraestructura de red configurada. La figura 19, al mostrar visualmente los resultados de esta prueba, proporciona una confirmación práctica de la conectividad exitosa entre Ubuntu y NethServer.

Figura 19. Prueba ping desde la terminal de Ubuntu

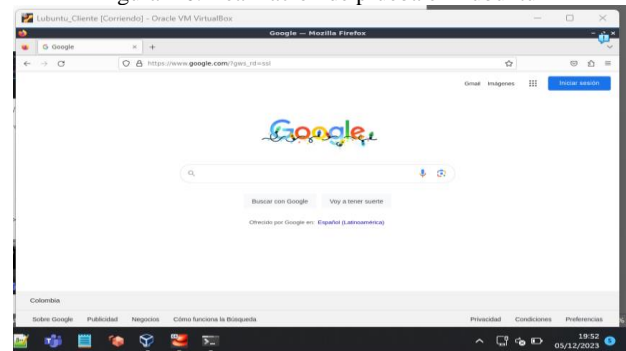


Fuente: Autoría propia

En la Figura 20. Se muestra la realización de la prueba ejecutada, con el fin de verificar el acceso a internet sin realizar la configuración en el proxy dentro del navegador de internet ingresando desde la máquina virtual de Ubuntu, tal como se evidencia a continuación.

La realización de esta prueba es fundamental para evaluar cómo se comporta la red en ausencia de configuraciones específicas en el proxy. En este contexto, la prueba podría implicar intentar acceder a sitios web o recursos en línea desde la máquina virtual de Ubuntu sin haber realizado configuraciones previas en el navegador para redirigir el tráfico a través del servidor proxy.

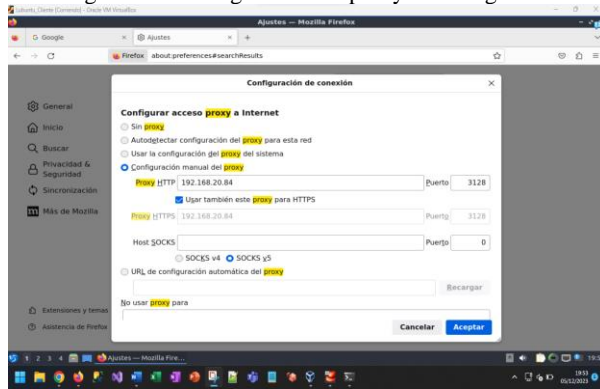
Figura 20. Realización de prueba en Ubuntu



Fuente: Autoría propia

En la Figura 21. Se muestra el proceso realizado en la configuración de proxy en el navegador abierto en la máquina virtual del cliente Ubuntu.

Figura 21. Configuración de proxy en navegador

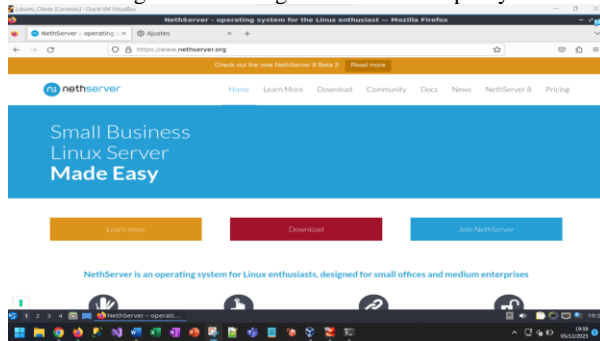


Fuente: Autoría propia

En la Figura 22. Se muestra la navegación realizada a través del proxy configurado previamente. Esta figura refleja una captura de pantalla de un navegador web que indica la navegación que ha sido interceptada o gestionada por el proxy configurado en el entorno de red.

Se observan detalles como la dirección web visitada, la hora de la navegación y otra información relevante que permita monitorear y evaluar el tráfico web a través del proxy. La figura 22 es valiosa para los administradores de red, ya que proporciona una visualización práctica de cómo el servidor proxy está gestionando el acceso a Internet y qué sitios web están siendo solicitados por los usuarios en la red.

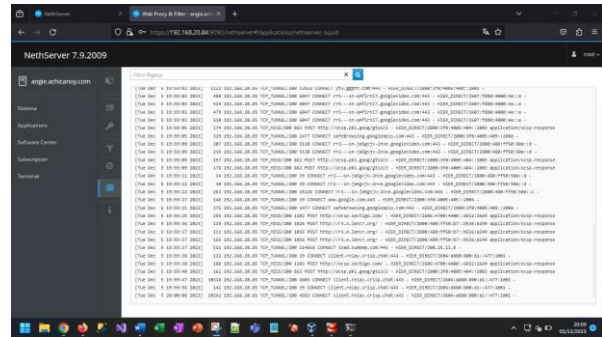
Figura 22. Navegación a través de proxy



Fuente: Autoría propia

En la Figura 23. Se evidencia que a través del log de NethServer, los diferentes sitios en donde se ha realizado navegación. Esta representación gráfica o captura de pantalla probablemente incluya información detallada sobre las actividades de navegación registradas por el servidor, como las direcciones URL visitadas, las horas de acceso y posiblemente otros detalles relevantes.

Figura 23. Verificación de navegación a través del log de NethServer

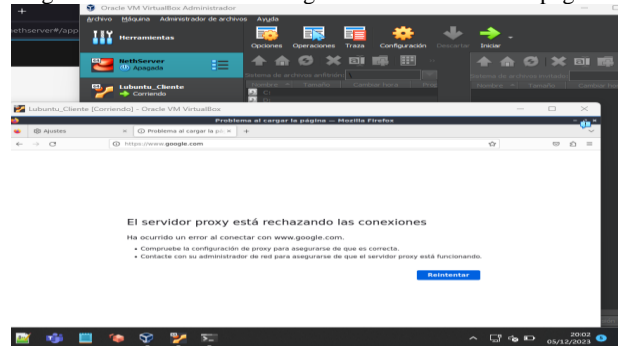


Fuente: Autoría propia

En la Figura 24. Se muestra claramente el impacto de apagar el servidor proxy en el entorno de red. La captura de pantalla o representación visual posiblemente destaca la falta de conexión y el acceso limitado o nulo a los servicios de Internet una vez que el servidor proxy ha sido apagado.

Este escenario indica que el servidor proxy, al ser un componente central en la gestión del tráfico de red, desempeña un papel crucial en la conectividad a Internet. Cuando se apaga, las solicitudes de los usuarios para acceder a sitios web y servicios externos ya no son gestionadas por el proxy, lo que puede resultar en una pérdida de conectividad o en una restricción significativa del acceso a Internet.

Figura 24. Verificación navegación con NethServer apagado



Fuente: Autoría propia

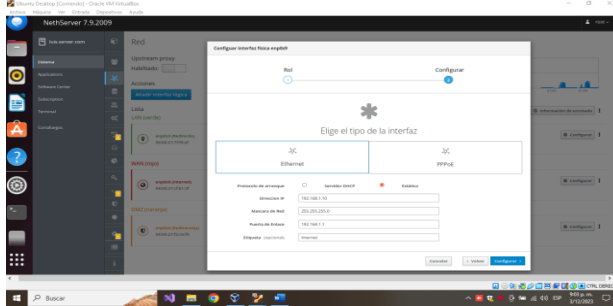
TEMÁTICA 3: CORTAFUEGOS

Firewall o cortafuegos: Es un elemento informático que controla el tráfico entrante y saliente de un dispositivo o una red privada [6] con la finalidad de bloquear la entrada de datos que no cumplan con algunos criterios de seguridad [6].

Implementación de cortafuegos, con la ayuda de NethServer se crea las reglas y políticas de navegación para los diferentes usuarios que quieran acceder a la red DMZ, o WAN. La verificación se hace con un sistema operativo Ubuntu desktop 22.04 y como servidor se usa NethServer 7.9 2009.

En la Figura 25. Se muestra la configuración de la IP estática 192.168.1.10/24 de la red WAN para salir a internet, y la puerta de enlace se establece como 192.168.1.1 que es el DNS de nuestro ISP (Proveedor de servicios de internet).

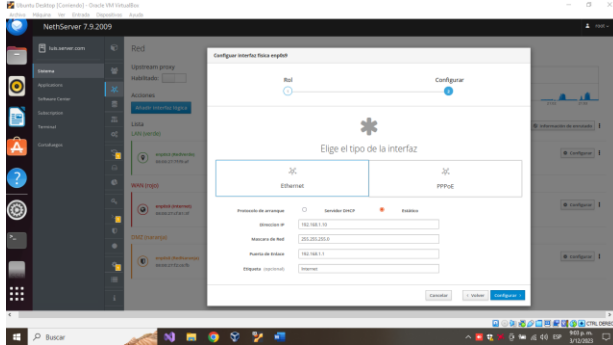
Figura 25. Configuración de red WAN



Fuente: Autoría propia

En la Figura 26. Se muestra la configuración de la IP estática 192.168.80.1/24 de la red LAN, y la puerta de enlace se establece como 192.168.1.10 que es la dirección IP de la red WAN de este modo podemos restringir tráfico como el de las redes sociales.

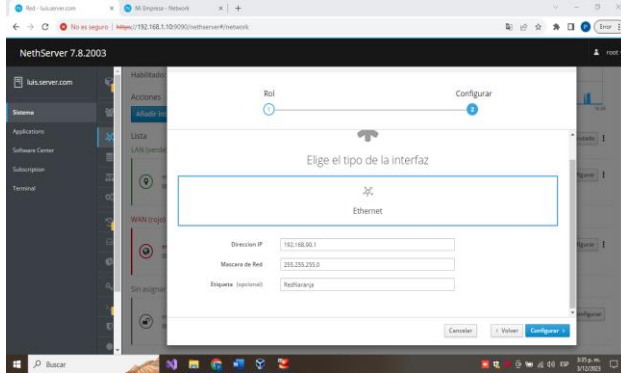
Figura 26. Configuración de red LAN



Fuente: Autoría propia

En la Figura 27. Se muestra la configuración de la red Naranja o DMZ en la que se establece la IP estática 192.168.90.1/24.

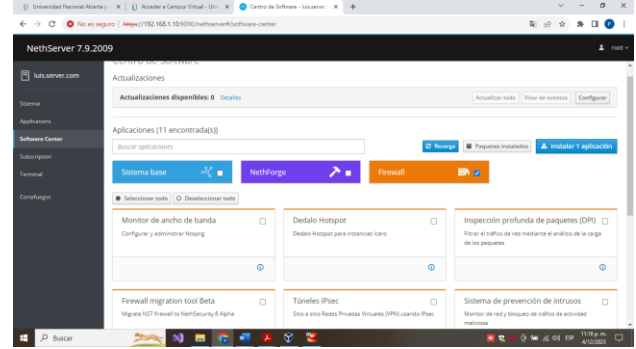
Figura 27. Configuración de red DMZ



Fuente: Autoría propia

En la Figura 28. Se muestra la instalación del Firewall desde el centro de software, elegimos firewall básico en este caso llamado Shorewall.

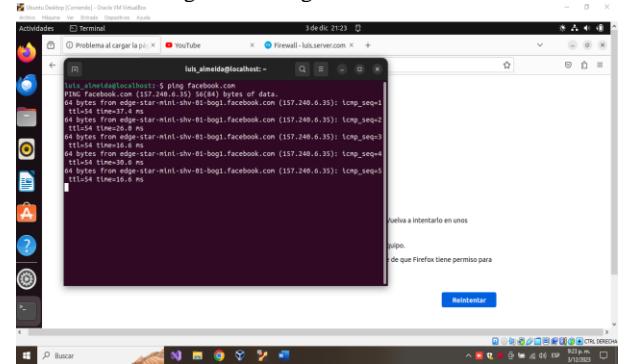
Figura 28. Instalación de Firewall



Fuente: Autoría propia

En la Figura 29. Se muestra la verificación de la IP de la plataforma Facebook.com realizando un ping desde la terminal al dominio Facebook.com, con el fin de poderla bloquear en este caso la IP es 157.240.6.35.

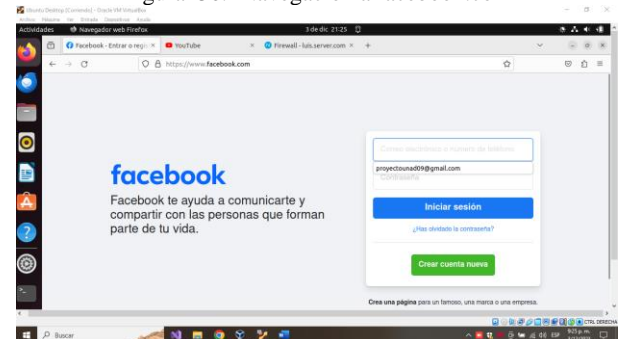
Figura 29. Ping a facebook.com



Fuente: Autoría propia

En la Figura 30. Se muestra la verificación de la navegación a la URL de Facebook desde el navegador web Firefox.

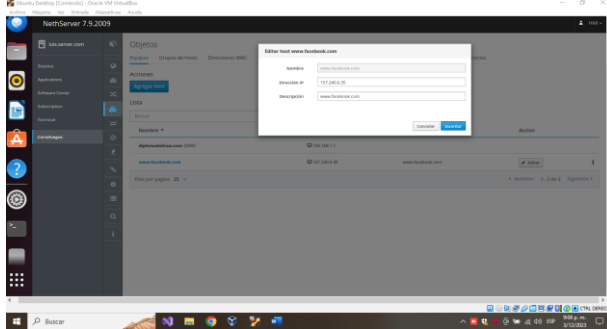
Figura 30. Navegación a facebook.com



Fuente: Autoría propia

En la Figura 31. Se muestra la evidencia de la creación del objeto www.facebook.com, el cual se utilizará más adelante en la creación de la regla del firewall.

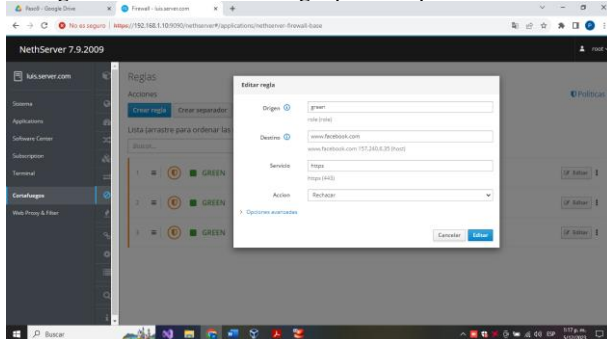
Figura 31. Creación objeto facebook



Fuente: Autoría propia

En la Figura 32. Se muestra la creación de la regla para toda la red GREEN o red LAN y se añade el objeto de Facebook y se rechaza todas las solicitudes realizadas por el puerto 443 (https).

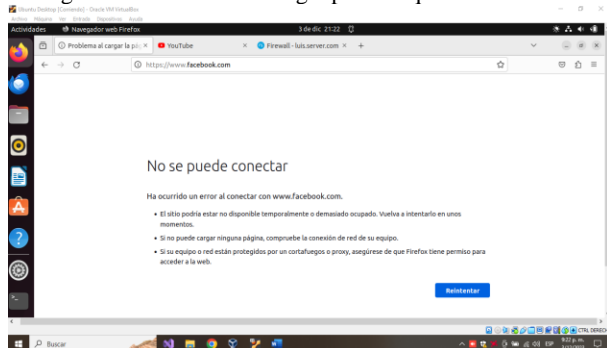
Figura 32. Creación de regla para bloqueo de facebook



Fuente: Autoría propia

En la Figura 33. Se muestra que en el navegador de Firefox no se tenga acceso a la plataforma de Facebook.

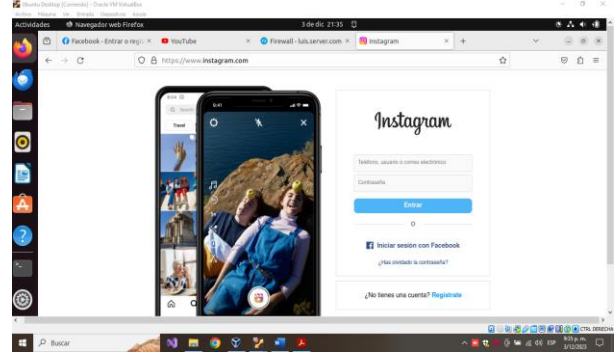
Figura 33. Creación de regla para bloqueo de facebook



Fuente: Autoría propia

En la Figura 34. Se muestra la navegación a la plataforma de Instagram.

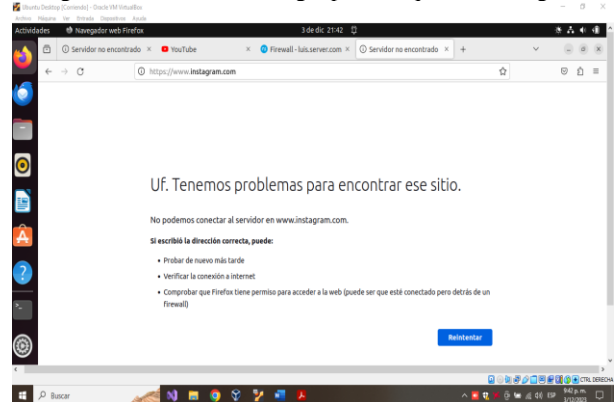
Figura 34. Navegación a www.instagram.com



Fuente: Autoría propia

En la Figura 35. Se muestra la creación de la regla para toda la red GREEN, se añade el objeto de Instagram y se rechaza todas las solicitudes realizadas por el puerto 443.

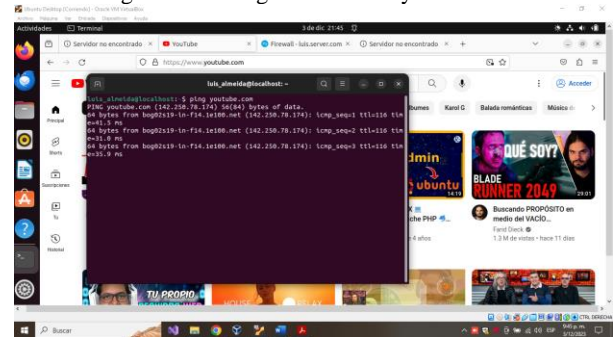
Figura 35. Creación de regla para bloqueo de Instagram



Fuente: Autoría propia

En la Figura 36. Se muestra la evidencia de la navegación a la plataforma de Youtube.com.

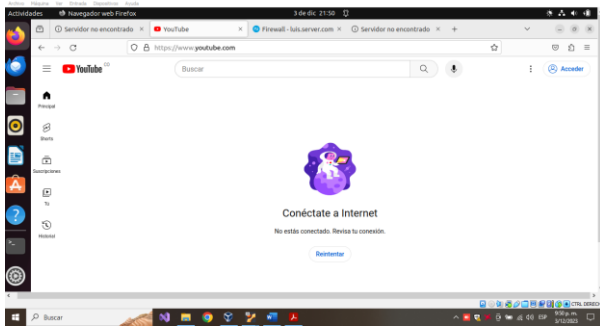
Figura 36. Navegación a www.youtube.com



Fuente: Autoría propia

En la Figura 37. Se muestra la creación de la regla para toda la red GREEN, añadimos el objeto de youtube.com y se rechaza todas las solicitudes realizadas por el puerto 443.

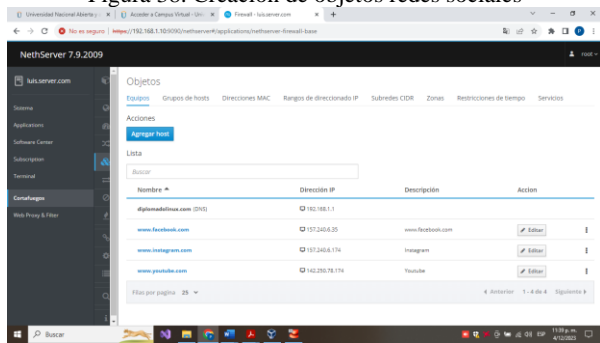
Figura 37. Creación regla para bloqueo de ww.youtube.com



Fuente: Autoría propia

En la Figura 38. Se muestra todos los objetos creados para bloquear las plataformas de YouTube, Facebook e Instagram.

Figura 38. Creación de objetos redes sociales



Fuente: Autoría propia

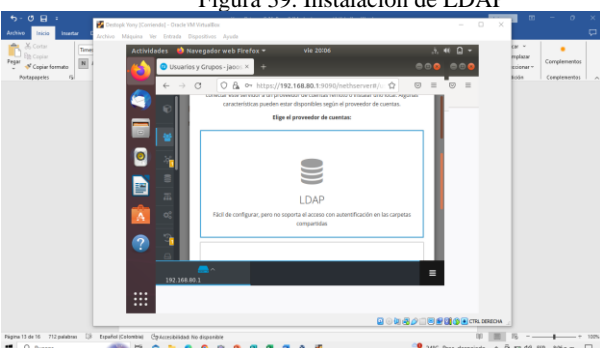
TEMÁTICA 4: FILE SERVER Y PRINT SERVER.

File server: Es un sistema informático que almacena y comparte archivos de datos para que los usuarios autorizados puedan acceder a ellos a través de una red [7].

Print server: Dispositivo utilizado en redes de área local (LAN) [8] la cual interconecta un grupo de computadoras cercanas entre sí por medio de cables.

En la figura 39. Se muestra cómo se debe proceder a la instalación done se ingresa a la opción de usuarios y grupos e instala LDAP.

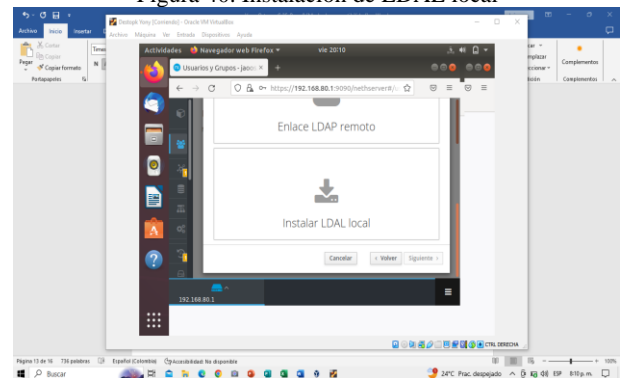
Figura 39. Instalación de LDAP



Fuente: Autoría propia

En la Figura 40. Se muestra la configuración de proveedor de cuentas y se selección la instalación de LDAP local.

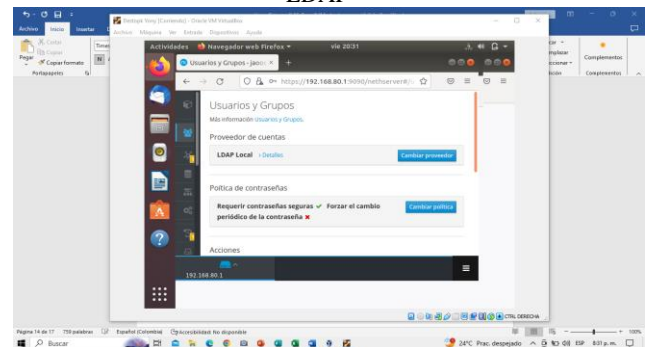
Figura 40. Instalación de LDAP local



Fuente: Autoría propia

En la Figura 41. Se muestra el siguiente escenario para saber que se ha instalado correctamente.

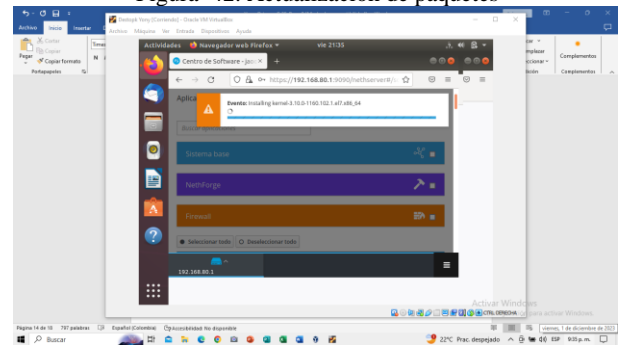
Figura 41. Correcta instalación del proveedor de cuentas LDAP



Fuente: Autoría propia

En la Figura 42. Se muestra la actualización y se instala los paquetes necesarios del sistema.

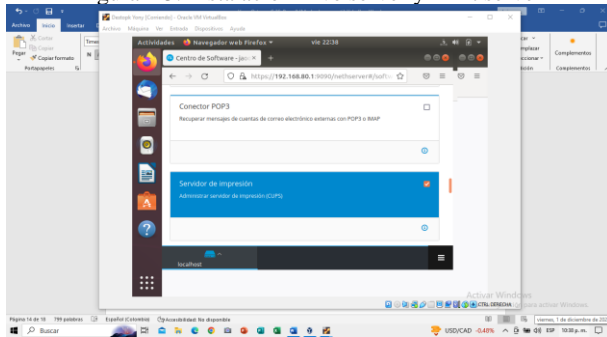
Figura 42. Actualización de paquetes



Fuente : Autoría propia

En la Figura 43. Se muestra como se debe seleccionar e instalar las aplicaciones de servidor de impresión y el servidor de archivos.

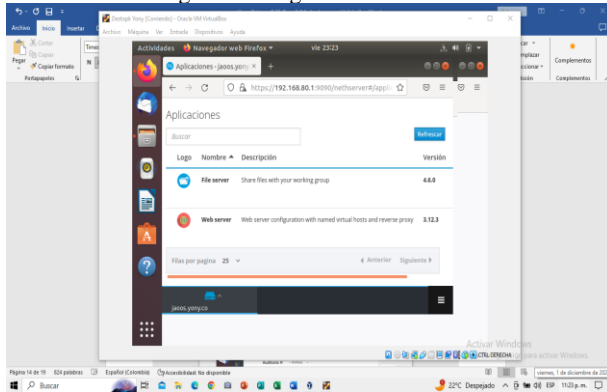
Figura 43. Instalación Live server y Print server



Fuente: Autoría propia

En la Figura 44. Se muestra el ingreso al servidor de archivo, se va ajustes para la creación de carpetas compartidas.

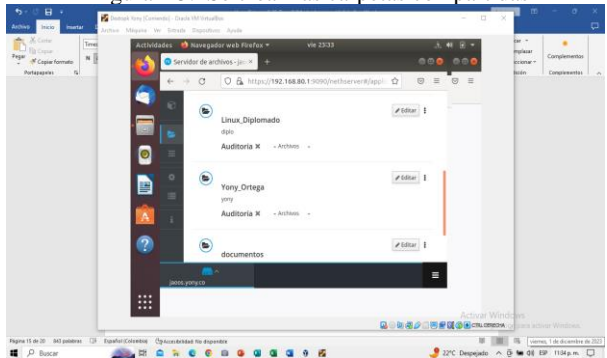
Figura 44. Ingreso a file server



Fuente: Autoría propia

En la Figura 45. Se muestra como se deben crear las carpetas compartidas en la opción para tal fin.

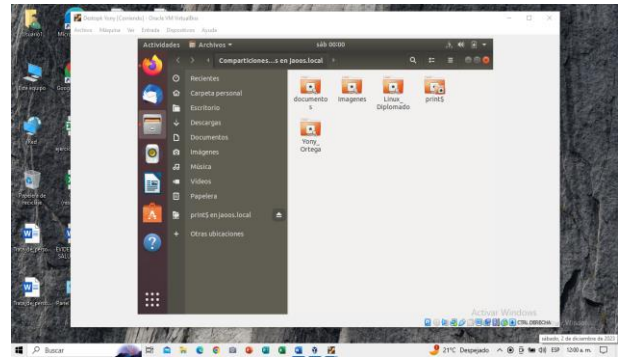
Figura 45. Se crean las carpetas compartidas



Fuente: Autoría propia

En la Figura 46. Se muestra la verificación de las carpetas compartidas que fueron creadas en el dashboard de NethServer desde los archivos del desktop del equipo cliente.

Figura 46. Verificación de carpetas compartidas



Fuente: Autoría propia

En la Figura 47. Se muestra la creación del acceso de Print server en el escritorio del equipo cliente.

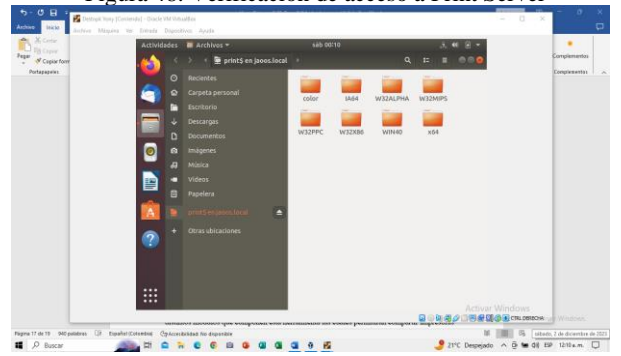
Figura 47. Acceso a Print server



Fuente: Autoría propia

En la Figura 48. Se muestra el acceso al servicio de la impresora a través de Print server por medio del desktop del equipo cliente, antes solicita el login de acceso para poder hacer a la conexión con el servidor de impresión y mostrar la impresora en red.

Figura 48. Verificación de acceso a Print Server



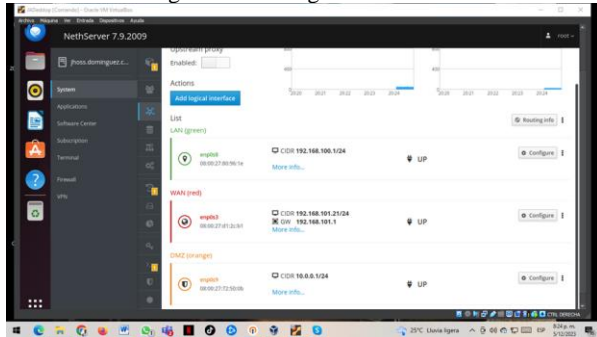
Fuente: Autoría propia

TEMÁTICA 5 VPN

VPN: Significa Red Privada Virtual, por sus siglas en inglés [9]. Uno de estos softwares VPN de código abierto es OpenVPN y puede funcionar como un servidor VPN de Linux [9].

En la Figura 49. Se muestra el ingreso a la opción del sistema para la configuración de las interfaces de las zonas verdes (LAN), roja (WAN) y naranja (DMZ) con sus respectivas direcciones IP

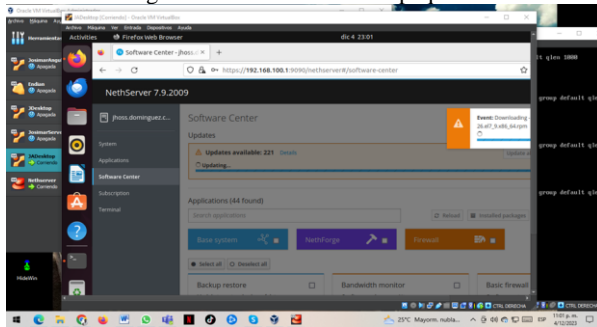
Figura 49. Configuración de interfaces



Fuente: Autoría propia

En la Figura 50. Se muestra el ingreso a la opción centro de software para realizar las respectivas actualizaciones y la instalación de los paquetes necesarios del sistema.

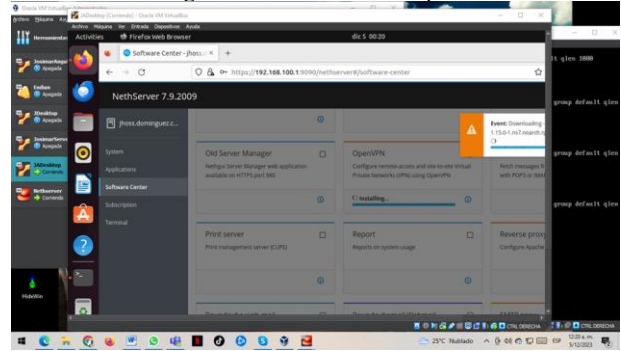
Figura 50. Actualización de paquetes



Fuente: Autoría propia

En la Figura 51. Se muestra el ingreso a la opción centro de software para realizar la respectiva descarga e instalación de OpenVPN y así realizar el acceso remoto a la VPN.

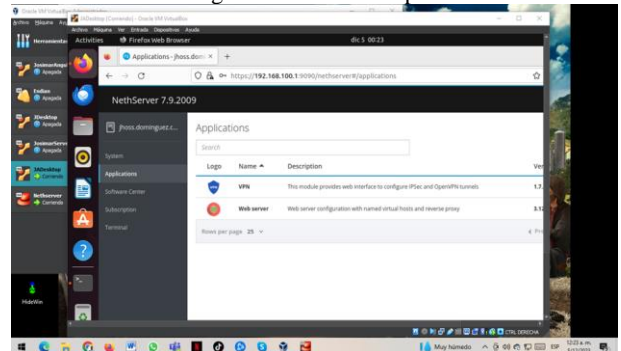
Figura 51. Instalación de Open VPN



Fuente: Autoría propia

En la Figura 52. Se muestra el ingreso a la opción de aplicaciones y se evidencia el programa OpenVPN instalado, después se va ajustes para la creación de la VPN.

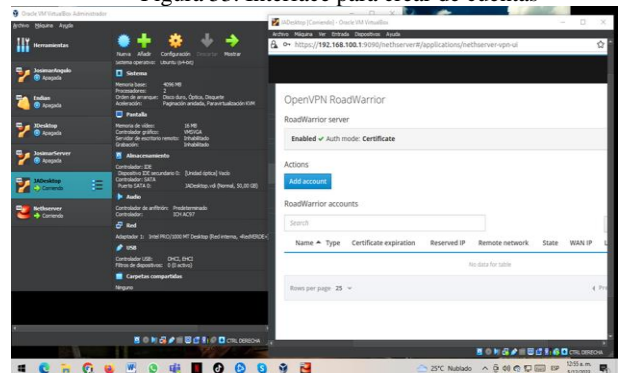
Figura 52. Interface OpenVPN



Fuente: Autoría propia

En la Figura 53. Se muestra el ingreso a la opción VPN y después se ingresa a la interface OpenVPN RoadWarrior para la creación de Cuentas, se evidencia que está habilitado.

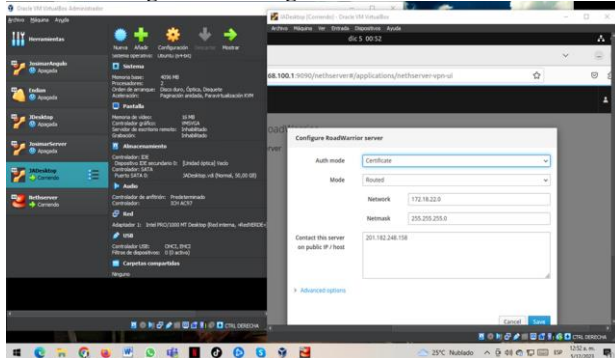
Figura 53. Interface para crear de cuentas



Fuente: Autoría propia

En la Figura 54. Se muestra el ingreso a la opción VPN y después se ingresa a la interface OpenVPN RoadWarrior, se añade una cuenta y luego se realiza la configuración del túnel VPN por medio del Servidor RoadWarrior.

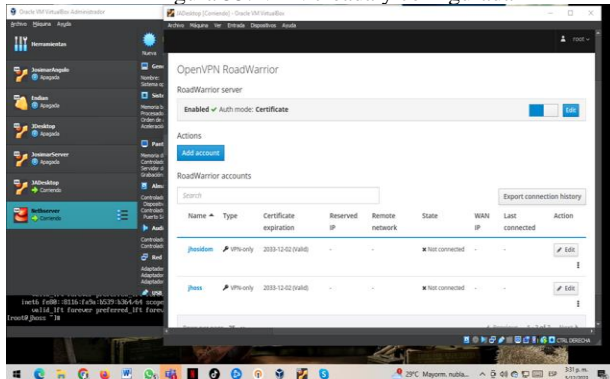
Figura 54. Configuración del servicio VPN



Fuente: Autoría propia

En la Figura 55. Se muestra el ingreso a la opción VPN y después se ingresa a la interface OpenVPN RoadWarrior, se verifica y se evidencia las acciones VPN creadas con el servidor RoadWarrior.

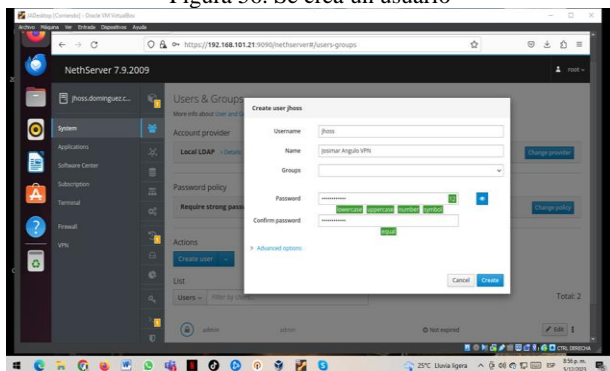
Figura 55. VPN creada y configurada



Fuente: Autoría propia

En la Figura 56. Se muestra el ingreso al sistema y después a la opción usuarios y grupos para la instalación de LDAP local y así poder realizar la creación de los usuarios.

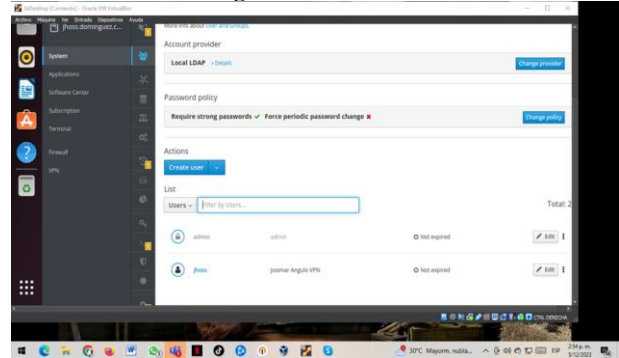
Figura 56. Se crea un usuario



Fuente: Autoría propia

En la Figura 57. Se muestra el ingreso al sistema y después a la opción usuarios y grupos, ya se evidencia que el usuario esta creado y así obtener los permisos en la VPN.

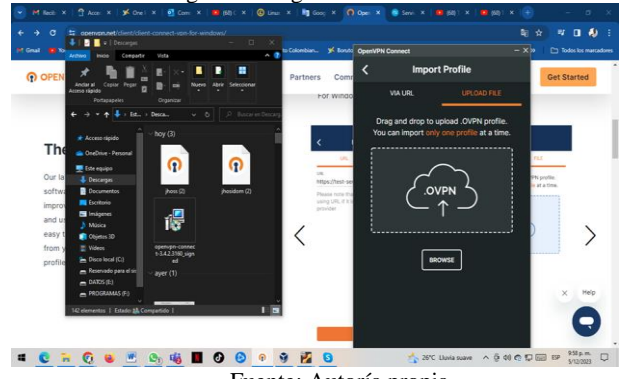
Figura 57. Usuario creado



Fuente: Autoría propia

En la Figura 58. Se muestra el ingreso a la aplicación cliente VPN y el ingreso del certificado a la aplicación OpenVPN Connect para realizar la conexión con el servidor OpenVPN RoadWarrior.

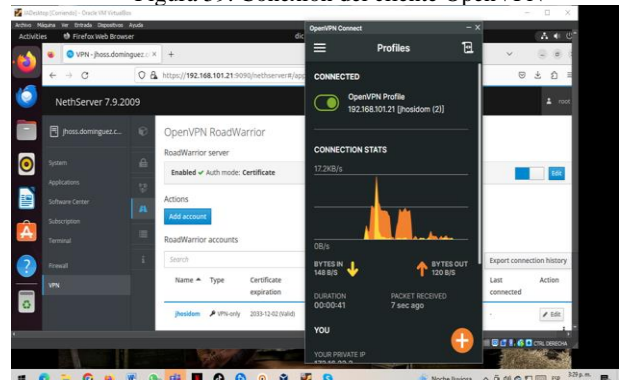
Figura 58. Ingreso de cliente a VPN



Fuente: Autoría propia

En la Figura 59. Se muestra que se realizó la conexión entre el cliente de OpenVPN Connect y la VPN (jhosidom) en el entorno del servidor OpenVPN RoadWarrior.

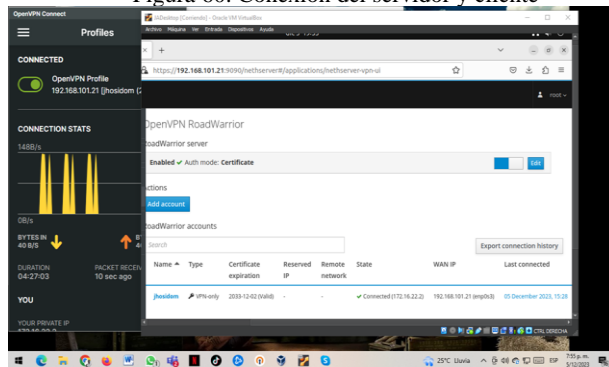
Figura 59. Conexión del cliente OpenVPN



Fuente: Autoría propia

En la Figura 60. Se muestra la conexión remota realizada desde el cliente OpenVPN Connect y el entorno servidor RoadWarrior, esto nos permite que la información viaje de forma segura y protegida, cifrada y anónima, protegiendo nuestros datos y la confiabilidad [10].

Figura 60. Conexión del servidor y cliente



Fuente: Autoría propia

1.1.1 CONCLUSIONES.

La implementación de un proxy en entornos como NethServer y Ubuntu puede aportar beneficios significativos en términos de seguridad, control de acceso y optimización del rendimiento.

La implementación efectiva de unos cortafuegos en NethServer contribuye a fortalecer la seguridad de la infraestructura informática y a mantener la integridad y confidencialidad de los datos.

La VPN en NethServer proporciona un nivel adicional de seguridad al cifrar las comunicaciones entre el cliente y el servidor, lo que ayuda a proteger la información sensible de posibles amenazas externas.

Los servicios DHCP y DNS son elementos fundamentales que simplifican la administración y supervisión de la infraestructura tecnológica en cualquier organización.

La combinación de un File Server robusto y un Print Server eficiente proporciona a las empresas las herramientas necesarias para optimizar sus operaciones, mejorar la colaboración entre los usuarios y garantizar la seguridad y disponibilidad de los recursos compartidos.

1.1.2 REFERENCIAS

- [1] Flores, R. (2020). Instalación Básica de NethServer. <https://mundo.openit.com.bo/?p=2406>
- [2] John. (2020). ¿Qué son DHCP y DNS y cuáles son las diferencias entre ellos? <https://community.fs.com/es/article/dhcp-and-dns-difference.html>
- [3] Hernández, J. E. (2019). NethServer controlador primario de dominio (PDC). <http://911-ubuntu.weebly.com/NethServer-pdc/NethServer-como-pdc-primary-domain-controller>
- [4] Boettner, F. A. (2022). Mejoras en la seguridad web del usuario mediante el uso de un proxy local (Doctoral dissertation,

- [5] Basurto Dávila, J. C. (2010). Análisis comparativo de la implementación de voz sobre IP en Wireless Mesh Networks y Wireless LAN tradicionales tomando en consideración parámetros de calidad de servicio y problemas de movilidad ocasionados por Handoffs (Bachelor's thesis, ESPOL). <https://www.dspace.espol.edu.ec/handle/123456789/10778>
- [6] Gómez, J. A. (2022). ¿Qué es un firewall y cómo funciona? <https://www.deltaprotect.com/blog/que-es-un-firewall>
- [7] Heddi. (2022). Servidor de archivos. <https://techlib.net/techedu/servidor-de-archivos/>
- [8] Cerón, D. (2015). Print server. <https://certificacionsistemasoperativos.wordpress.com/2015/06/06/print-server/>
- [9] Deyimar, A. (2023). Configurar un servidor VPN de Linux con OpenVPN – Guía paso a paso. https://www.hostinger.co/tutoriales/como-configurar-vpn-linux-con-openvpn#Como_probar_un_servidor_VPN_de_Linux_con_Open_VPN
- [10] De Luz, S. (2023). Cómo conectarte a una VPN con OpenVPN. <https://www.redeszone.net/tutoriales/vpn/openvpn-instalacion-configuracion/>