IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT EN NETHSERVER PARA ESTACIONES GNU/LINUX

Fernando Cristancho Martínez
fcristanchom@unadvirtual.edu.co
Diana Cristina León Ramírez
dcleonr@unadvirtual.edu.co
Ivonne Dayana Perez Rincón
idperez@unadvirtual.edu.co

RESUMEN: *Este trabajo aborda la implementación y configuración de diversos servicios de infraestructura IT en Nethserver para estaciones de trabajo GNU/Linux. Se configuraron servicios como DHCP, DNS y un controlador de dominio, permitiendo a las estaciones de trabajo acceder y registrarse en la red. Además, se implementó un proxy para controlar el acceso a Internet, filtrando el tráfico a través del puerto 3128. Se configuraron reglas de cortafuegos para restringir el acceso a sitios web de entretenimiento y redes sociales. También se configuraron los servicios de archivo e impresión, facilitando el acceso a carpetas compartidas e impresoras mediante LDAP. Finalmente, se estableció una conexión VPN para asegurar la comunicación privada entre estaciones GNU/Linux. Los resultados demuestran la integración eficiente de estos servicios, mejorando la administración de red, seguridad y conectividad de las estaciones de trabajo, asegurando un entorno de TI robusto y controlado.*

PALABRAS CLAVE: Cortafuegos, DNS, Nethserver, VPN.

1 INTRODUCCIÓN

Este reporte describe el proceso de implementación y configuración de varios servicios de infraestructura IT en Nethserver para estaciones de trabajo GNU/Linux, siguiendo un enfoque basado en las mejores prácticas de administración de redes. Se abordan cinco temáticas clave: configuración de DHCP, DNS y controlador de dominio para gestionar el acceso y registro de estaciones, implementación de un proxy para controlar el acceso a Internet, configuración de un cortafuegos para restringir sitios web no deseados, habilitación de servicios de archivos e impresión mediante LDAP, y la creación de una VPN para asegurar comunicaciones privadas. La implementación de estos servicios permite mejorar la seguridad, la conectividad y la administración de la red, proporcionando un entorno de TI robusto y controlado.

2 TEMÁTICA 1: DHCP SERVER, DNS SERVER y CONTROLADOR DE DOMINIO.

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

2.1 INSTALACIÓN DE NETHSERVER

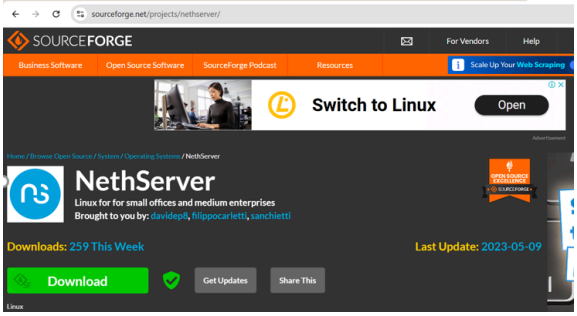
2.2.1. Descargar la imagen ISO de NethServer

Ingresamos a la página oficial para descargar el NethServer, en el siguiente link:

- https://www.nethserver.org/

Descargamos la última versión de NethServer, seleccionamos el botón Download para iniciar el proceso de descarga.

Figura 1. Página de Nethserver para iniciar la descarga

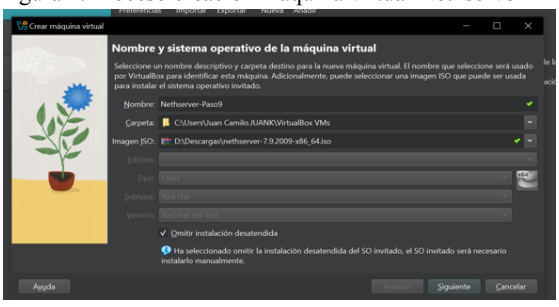


Fuente: Autoría propia

2.2.2. Crear la máquina virtual de Nethserver

Ingresamos a VirtualBox, para crear la nueva máquina virtual. Se debe usar el tipo de sistema operativo Linux y versión Red Hat (64-bit).

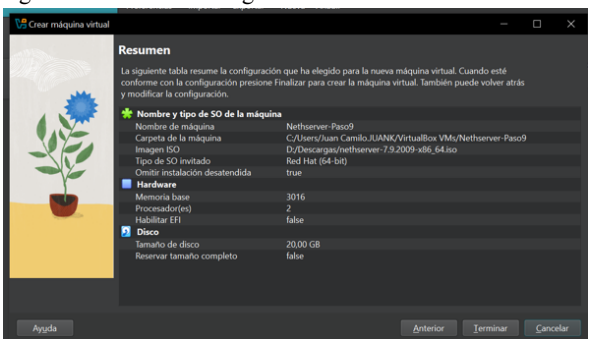
Figura 2. Proceso creación máquina virtual Nethserver



Fuente: Autoría propia

Se realiza la asignación de recursos para la memoria RAM, Procesadores y Disco Duro, como lo muestra el resumen de la figura 3.

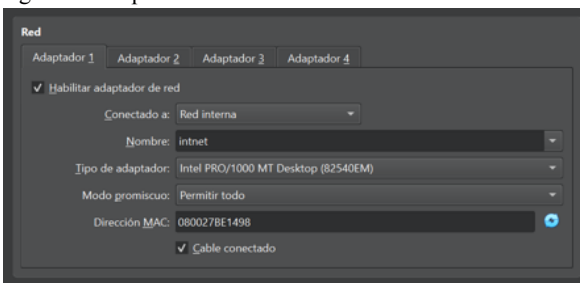
Figura 3. Resumen de asignación de recursos



Fuente: Autoría propia

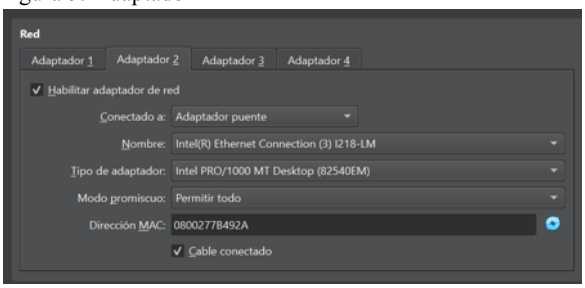
Continuamos con la configuración de los adaptadores de Red. Adaptador 1 = Red Interna y Adaptador 2 = Adaptador Puente. Como lo muestra la Figura 4 y 5 respectivamente.

Figura 4. Adaptador 1



Fuente: Autoría propia

Figura 5. Adaptador 2

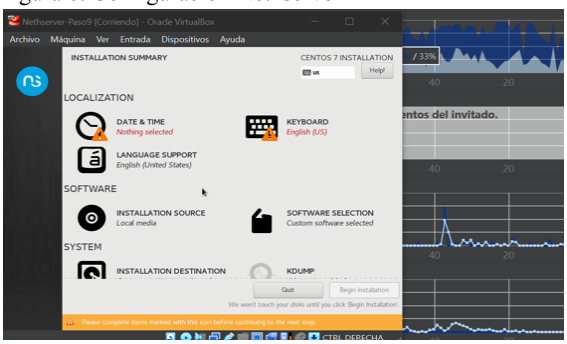


Fuente: Autoría propia

2.2.3. Configuración de Nethserver

Iniciamos la máquina virtual y esperamos que arranque. Cuando muestre el menú principal seleccionamos cada uno de los iconos para realizar la respectiva configuración. En la figura 6. nos muestra el menú, el cual se encuentra dividido por locación, software y sistema.

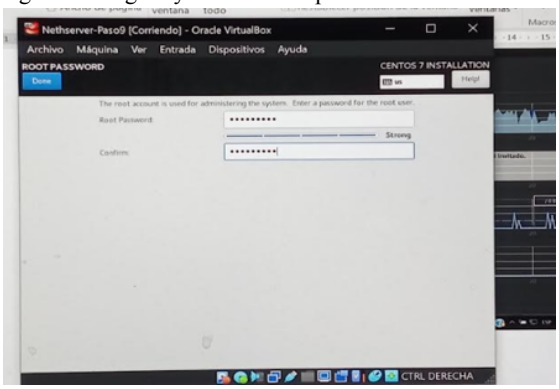
Figura 6. Configuración Nethserver



Fuente: Autoría propia

Después de finalizar la configuración del Nethserver, asignamos la contraseña del root, ingresamos a la opción ROOT PASSWORD.

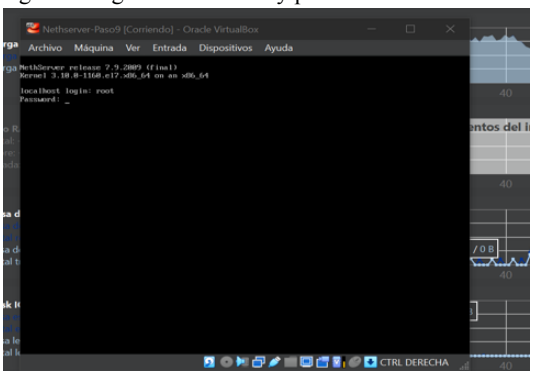
Figura 7. Asignar y confirmar el password del root



Fuente: Autoría propia

Al finalizar este proceso, se reinicia el Nethserver y nos solicita el Localhost y la contraseña que acabamos de asignar, en este caso Localhost: root y contraseña: la que acabamos de asignar en la figura 7.

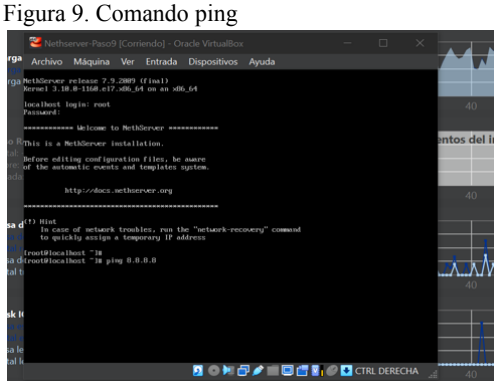
Figura 8. Ingresar Localhost y password



Fuente: Autoría propia

Ahora con el comando ping 8.8.8.8, verificamos si hay ping de internet.

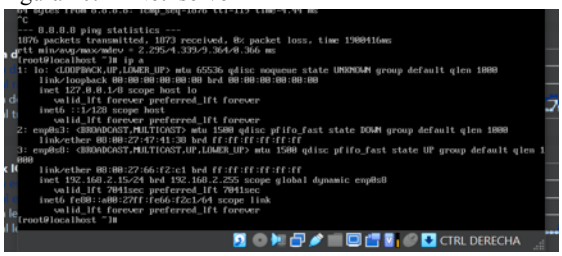
Figura 9. Comando ping



Fuente: Autoría propia

Al finalizar muestra la configuración de la IP en Nethserver.

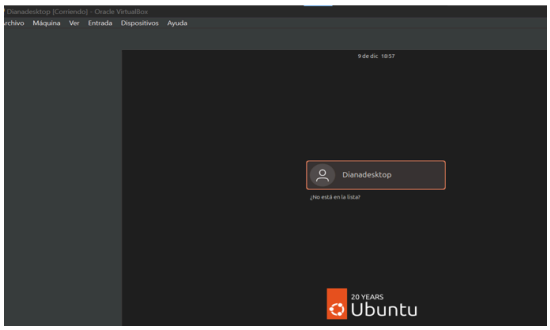
Figura 10. IP Nethserver



Fuente: Autoría propia

2.2.4. Iniciando la máquina Ubuntu Desktop

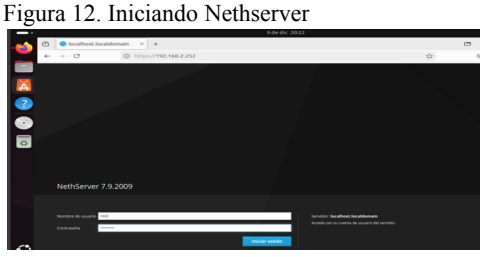
Figura 11. Iniciando la máquina desktop.



Fuente: Autoría propia

Ingresamos al navegador mozzilla escribimos la IP, e iniciamos sesión con root y la contraseña que asignamos anteriormente

Figura 12. Iniciando Nethserver



Fuente: Autoría propia

3 TEMÁTICA 2: PROXY

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

Paso 1: Descargar la ISO de Nethserver

Vamos a https://www.nethserver.org/getting-started-with-nethserver/ que es el sitio oficial de Nethserver y la descargamos, en este caso descargamos la versión 7.9.

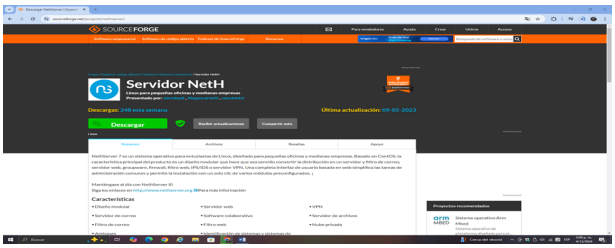


Imagen 1. Descarga ISO de Nethserver

Paso 2: Configuración e instalación de Nethserver en Virtual Box.

Seleccionamos un nombre en este caso “Nethserver”, la carpeta de destino y la imagen ISO que descargamos anteriormente de Nethserver, la edición, el tipo y la versión no la deja por defecto**.**

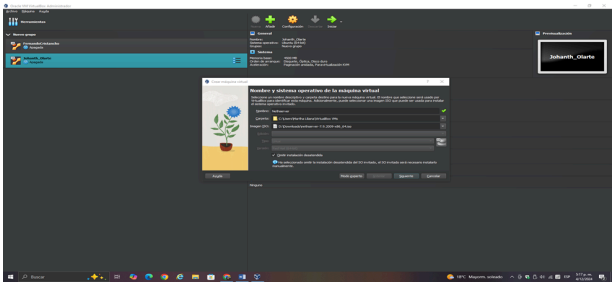


Imagen 2. Configuración de Nethserver

Modificamos la cantidad de memoria RAM en este caso 3016 MB y dos procesadores.

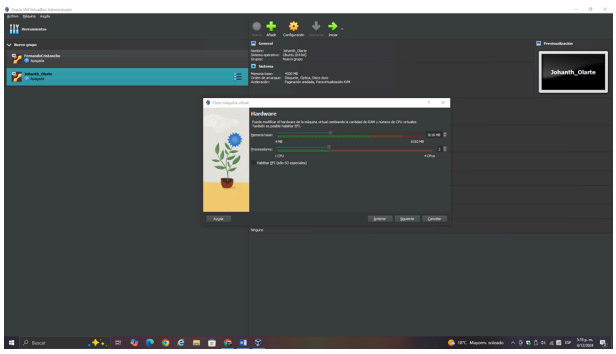


Imagen 3. Modificación memoria RAM y procesadores

Modificamos el disco duro virtual en este caso de 20 GB.

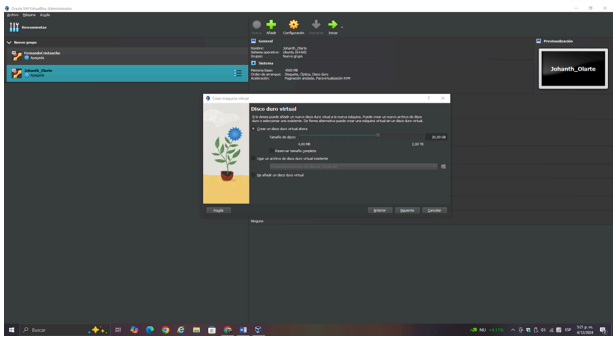


Imagen 4. Modificación disco duro virtual

Nos muestra una tabla con la configuración que acabamos de realizar.

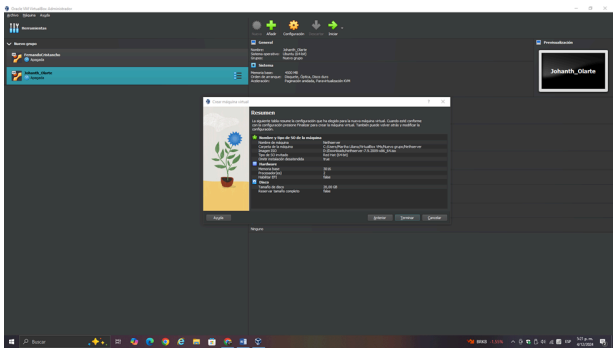


Imagen 5. Configuración de Nethserver – resumen

Configuramos los adaptadores de red, el adaptador 1 lo conectamos a la red interna.

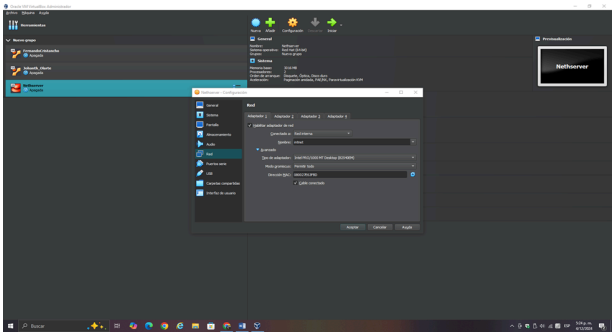


Imagen 6. Configuración - adaptador 1

El adaptador 2 lo conectamos al adaptador puente.

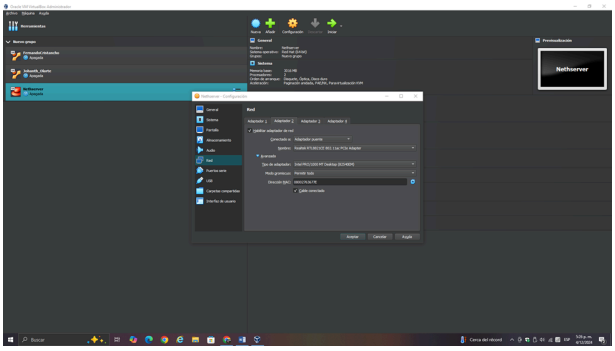


Imagen 7. Configuración – adaptador 2

Paso 3: Configuración de Nethserver

Menú de Nethserver ya instalado y funcionando en nuestra máquina virtual.

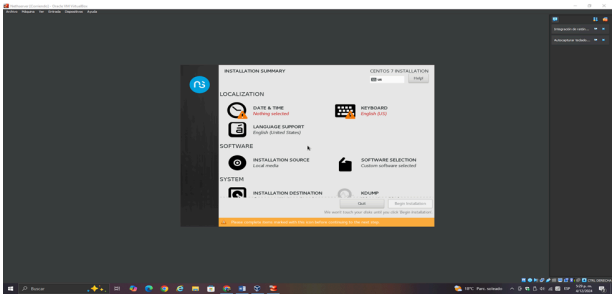


Imagen 8. Menú de Nethserver

Configuramos la zona horaria, Bogotá.

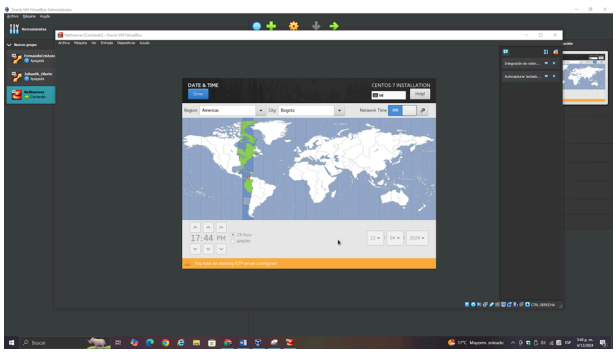


Imagen 9. Zona horaria

Configuramos el teclado en idioma español.

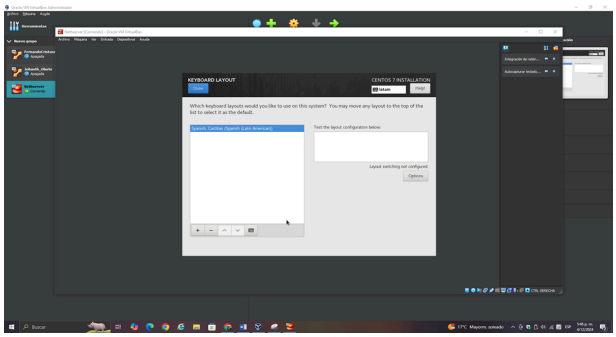


Imagen 10. Configuración del teclado

Verificamos que estén instalados nuestros adaptadores de red.

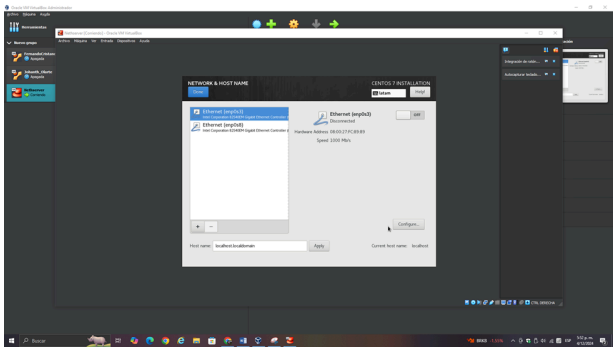


Imagen 11. Adaptadores de red

Configuramos la contraseña del root.

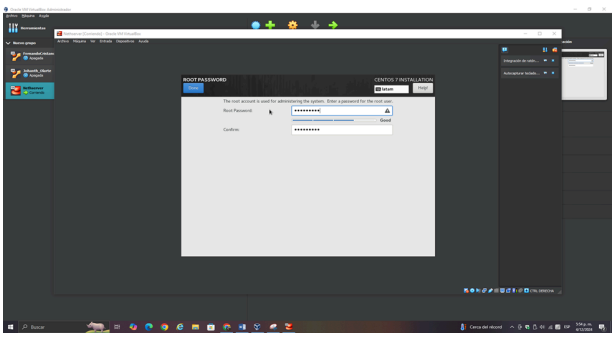


Imagen 12. Contraseña del root

Ahora ya se terminó la configuración del Nethserver, y nos aparece una IP la cual es la que nos servirá para la configuración del Nethserver desde la interfaz web es **10.0.0.36:9090**.

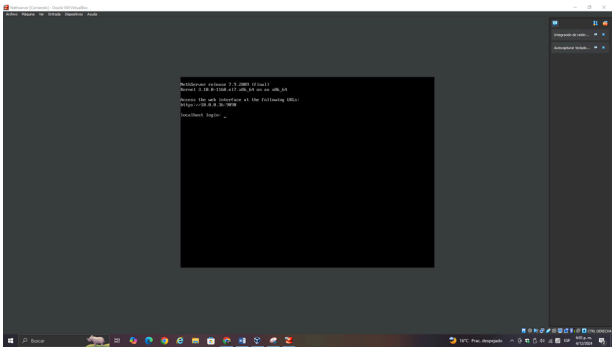


Imagen 13. IP para la configuración del Nethserver

Ahora ingresamos con la IP en nuestra interfaz web desde el navegador Firefox donde ingresamos con el root y la contraseña que proporcionamos anteriormente.

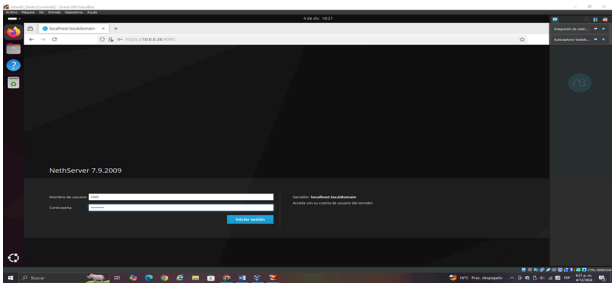


Imagen 14. Ingreso desde un navegador con la IP a Nethserver

Ahora nos pide cambiar el nombre del host, lo cambie por “paso9.unad.com”.

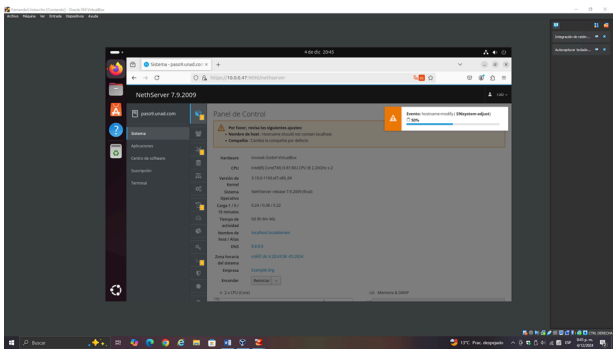


Imagen 15. Cambio nombre del host

Cambiamos la información de empresa ya que no lo piden.

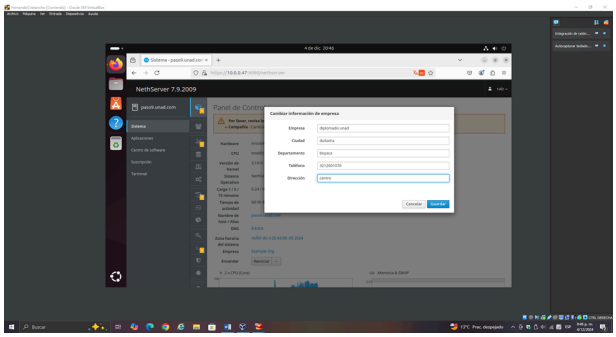


Imagen 16. Información de empresa

Configuramos la red verde y la dejamos como red roja, configuramos la dirección IP, la máscara de red y la puerta de enlace y nos desconecta de Nethserver.

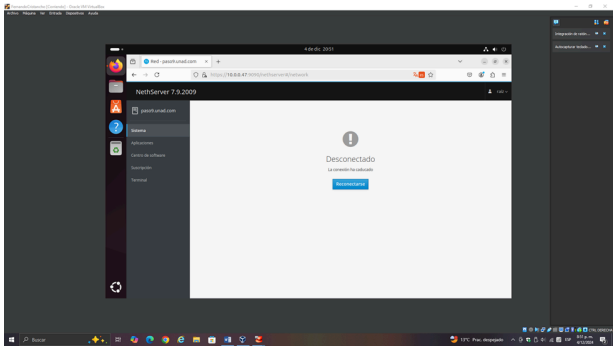


Imagen 17. Configuración de red roja

Debemos ingresar de nuevo.

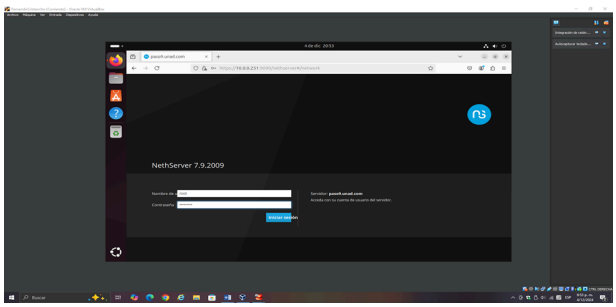


Imagen 18. Ingreso de nuevo a Nethserver

Ahora debemos configurar la red LAN verde, vamos a configuración y configuramos la dirección IP con una completamente diferente a la que tenemos.

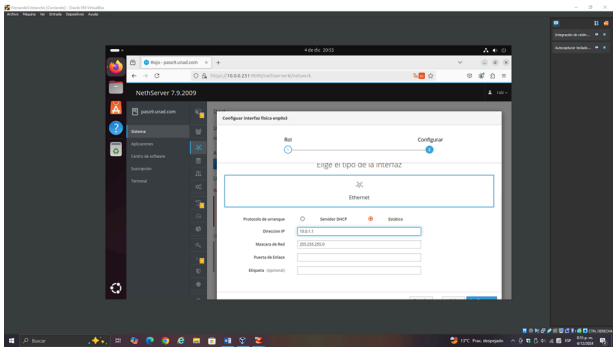


Imagen 19. Configuración red verde

Ahora configuramos los DNS, configurando el nombre de host y la dirección IP la cual es 10.0.1.1.

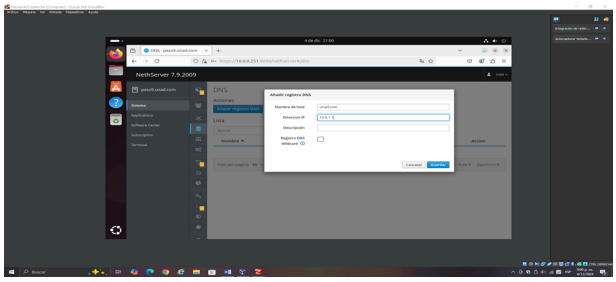


Imagen 20. Configuración de DNS

Configuramos el servidor DHCP, dando el rango de inicio desde la IP y el rango fin de la IP.

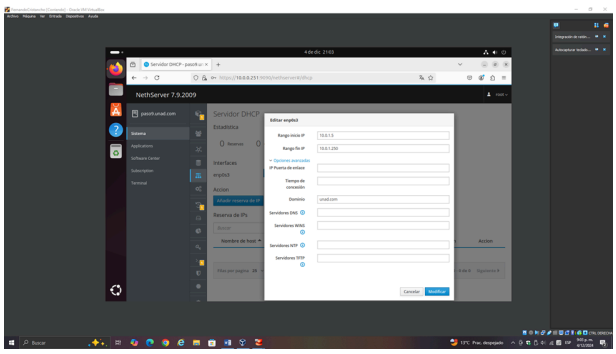


Imagen 21. Configuración del servidor DHCP

Ahora los componentes proxy los encontramos en software center y los seleccionamos Firewall básico, filtro web y proxy web, luego de esto procedemos a instalarlos.

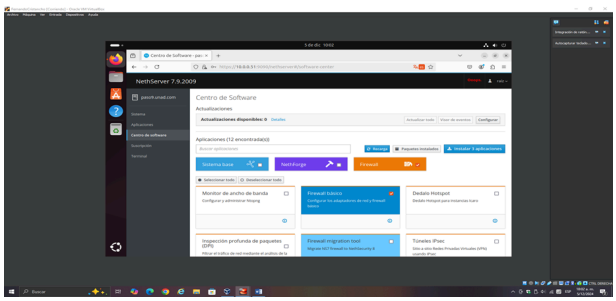


Imagen 22. Componentes proxy

Las instalaciones nos aparecen en la sección de aplicaciones, así como lo observamos en la siguiente imagen.

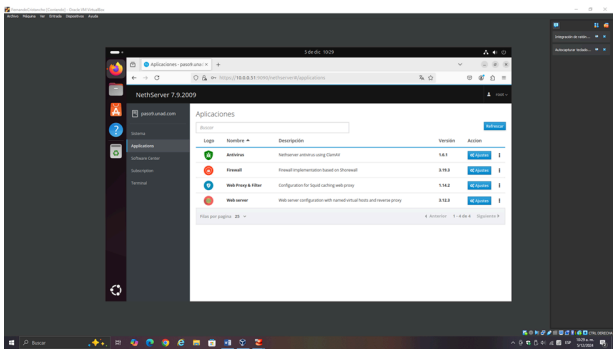


Imagen 23. Instalaciones

Ahora procedemos a crear un acceso directo para el web proxy y procedemos a configurarlo, configuramos la zona verde con la opción SSL transparente.

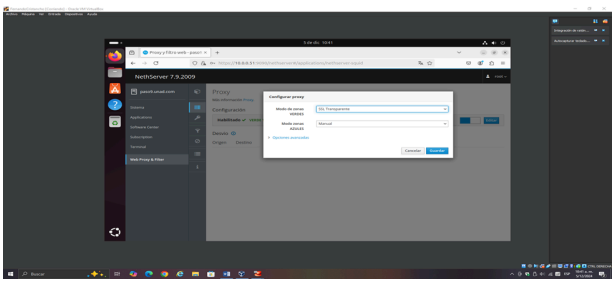


Imagen 24. Configuración proxy

Ya nos aparece habilitado.

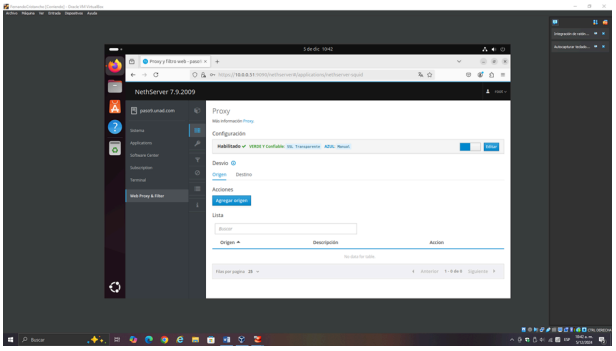


Imagen 25. Habilitado el proxy

Ahora configuramos la sección de categorías, guardamos e instalamos y esperamos a que se agreguen todos los cambios.

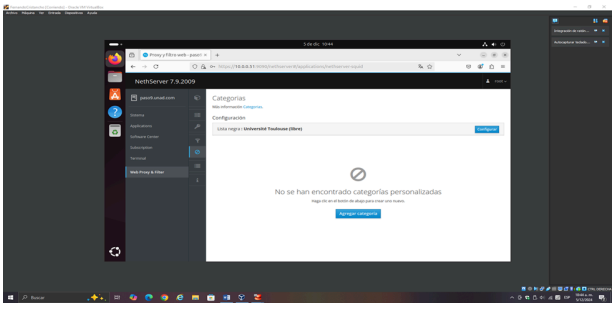


Imagen 26. Configuración sección de categorías

Ahora en la sección de “filtro” procedemos a configurar las categorías que queremos bloquear, en este casi dejamos las opciones de habilitar lista negra global y habilitar lista blanca global activadas, el modo lo ponemos en bloquear las categorías seleccionadas y permitir el resto las categorías que bloquearemos serán adult, games y mixed adult.

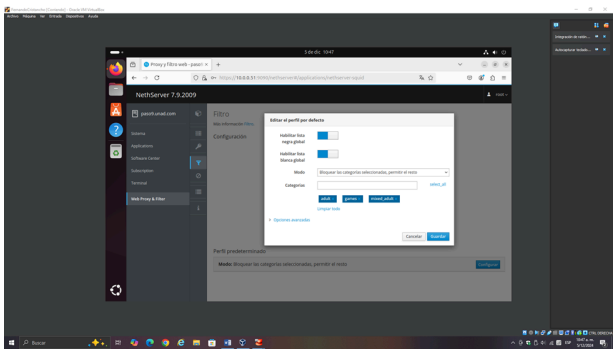


Imagen 27. Configuración de bloqueo de categorías

4 TEMÁTICA 3: CORTAFUEGOS

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Se inicia con la creación de la maquina virtual para iniciar con las respectivas configuraciones.

Imágen 1. Crear máquina virtual

Fuente: Autoría Propia

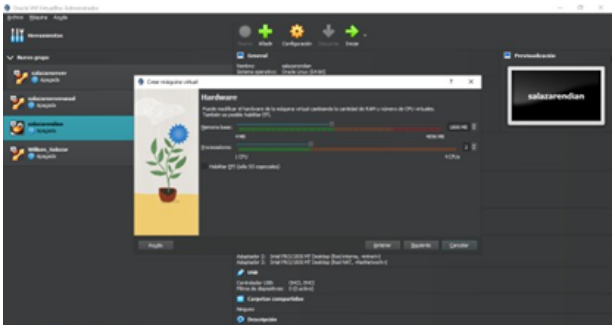
Posteriormente se realizan las respectivas configuraciones de la maquina virtual para el acceso a información.

Imágen 2. Configurar máquina virtual

Fuente: Autoría Propia

Se realizan los ajustes en la maquina virtual del hardware.

Imágen 3. Asignar el hardware de la máquina virtual



Fuente: Autoría Propia

Se verifica la funcionalidad del disco virtual para Virtual Box

Imágen 4. Disco virtual de VB

Fuente: Autoría Propia

Se validan las configuraciones para el inicio del sistema.

Imágen 5. Se verifica la configuración y se inicia

Fuente: Autoría propia

Posteriormente se verifica que la instalación del NethServer este funcionando a cabalidad y su funcionalidad sea adecuada.

Imágen 6. Se inicia instalacion de NethServer

Fuente: Autoría propia

Se realiza la adecuación del proceso de intalación de NethServer y se espera que se finalice la configuración.

Imágen 7. Proceso de instalación

Fuente: Autoría Propia

Se verifican las diferentes configuraciones para la zona horaria

Imágen 8. Configurar zona horaria

Fuente: Autoría Propia

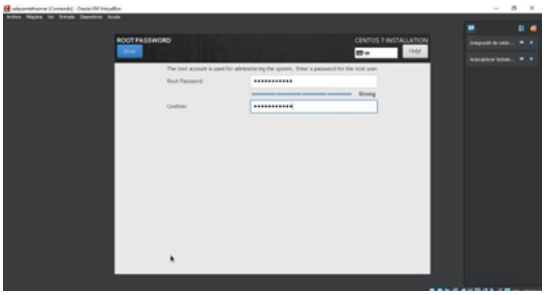
Posteriormente se configura el root y password que serán utiles para el proceso de ingreso a nuestra maquina virtual.

Imágen 9. Se configura root y password

Fuente: Autoría Propia

Se inicia nuevamente con el usuario y contraseña ya creado para que nos valide la información necesaria para el proceso.

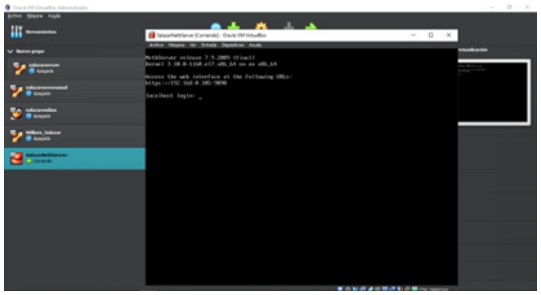
Imágen 10 Se asigna password al usuario root



Fuente: Autoría Propia

Cuando se finaliza la instalación correspondiente se procede al inicio de sesion para ejecutar el proceso.

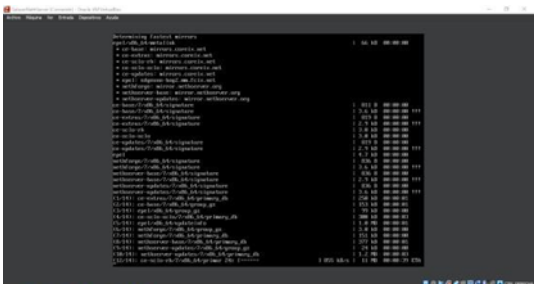
Imágen 11. Finalizada la instalación se inicia sesión



Fuente: Autoría Propia

Se ejecuta el sudo teniendo en cuenta la actualización para el inicio de procedimientos.

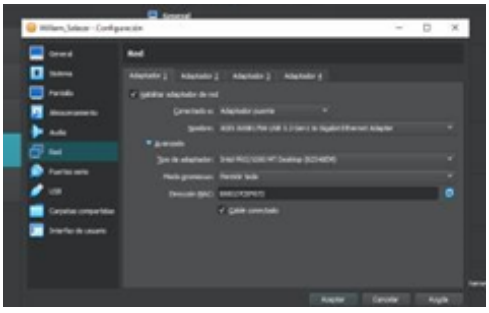
Imágen 12. Se ejecuta sudo yum update para actualizar



Fuente: Autoría Propia

Para este momento se debe configurar el adaptador 1 que funcionara para la validación del cortafuegos.

Imágen 13. Se configura el adaptador 1



Fuente: Autoría Propia

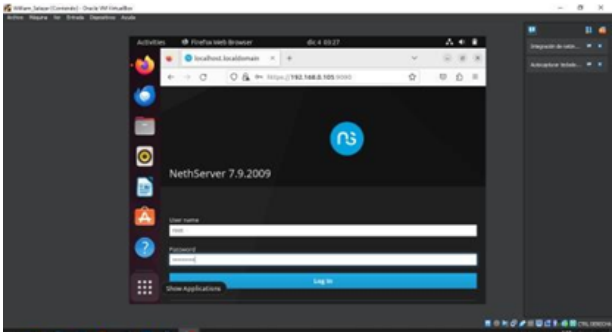
Se valida que la IP configurada este adecuada para el uso de la información de validaciones

Imágen 14. Se hace uso de ip a

Fuente: Autoría Propia

Se ingresa a la maquina virtual y se realiza el inicio del Ubuntu Desktop.

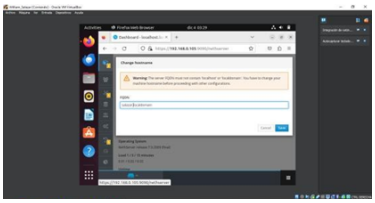
Imágen 15. Se ingresa a virtual Ubuntu Desktop



Fuente: Autoría Propia

Se realiza la asignación de un nombre en este caso se puede configurar con el nombre que se desee.

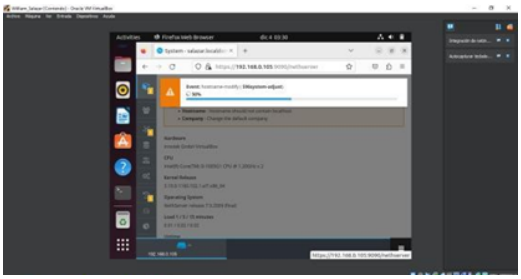
Imágen 16. Se asigna el nombre de unad.localmain.com



Fuente: Autoría Propia

Teniendo en cuanta la IP se asignan los datos adecuados para la configuración.

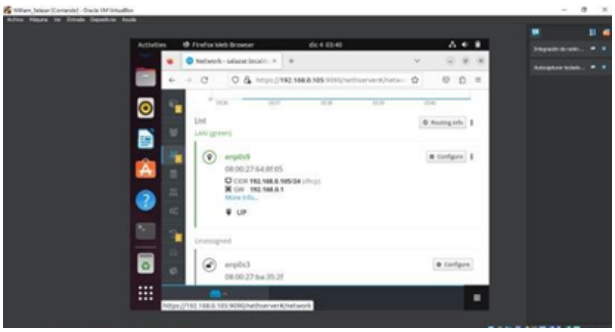
Imágen 17. Toma los datos que se asignaron en la IP



Fuente: Autoría Propia

Se configura posteriormente la LAN para que vayan conectados a un router con dispositivos cercanos para que se comparta la información adecuada.

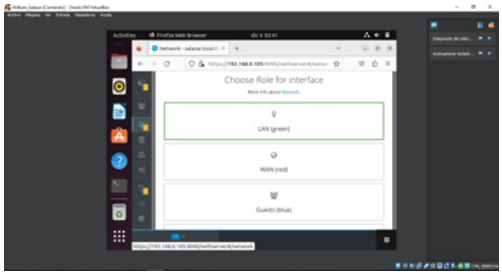
Imágen 18. Se configura LAN.



Fuente: Autoría Propia

Posteriormente se valida que la WAN por SHCP permita la conexión del router y que obtenga automaticamente una dirección IP.

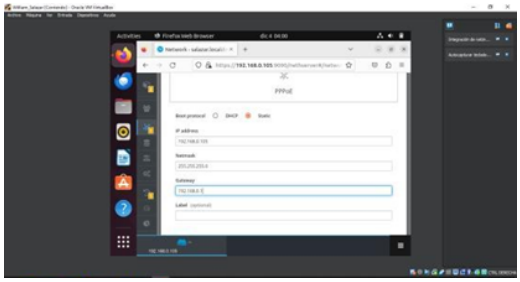
Imágen 19. Se configura WAN por DHCP.



Fuente: Autoría Propia

Posteriormente se validan que todas las funciones esten adecuadas teniendo en cuenta la IP, Mascara y Gateway que en conjunto funcionan para la conexión de redes

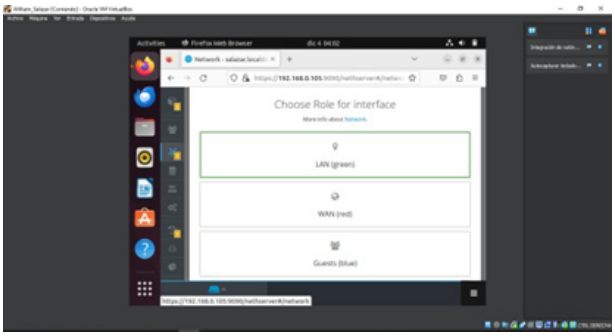
Imágen 20. Se configura Ip, Mascara, y Gateway



Fuente: Autoría Propia

Nuevamente se configura la LAN para conexion de dispositivos cercanos.

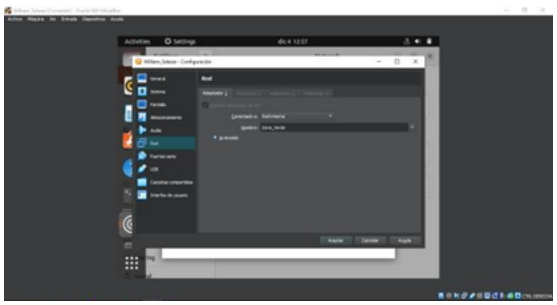
Imágen 21. Se configura LAN.



Fuente: Autoría Propia

Posteriormente se realizan los cambios de preferencia de red adecuados para la configuración del sitio y cambios en el ordenador

Imágen 22. Se realizan cambios de preferencias de red.



Fuente: Autoría Propia

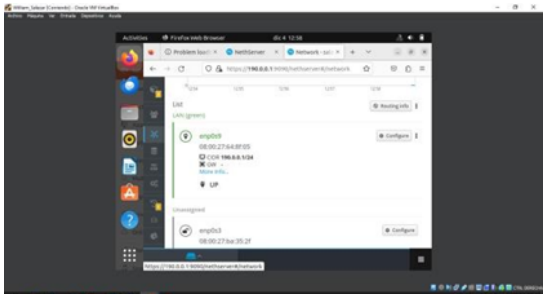
Posteriormente se utiliza un servidor de protocolo de configuración dinámica de host (DHCP) para gestionar la asignación de direcciones IP

Imágen 23. Se configura ipv4

Fuente: Autoría Propia

Se accede al NethServer teniendo en cuenta la IP.

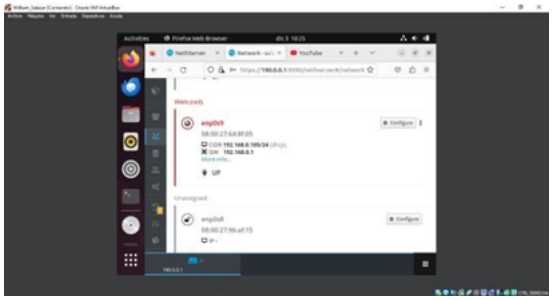
Imágen 24. Posteriormente se accede al NethServer teniendo en cuenta IP 190.0.0.1



Fuente: Autoría Propia

Se realiza la configuración de la zona WAN teniendo en cuenta especificaciones dadas.

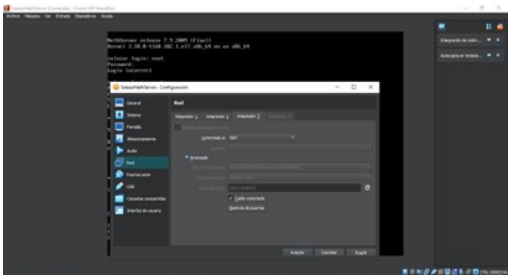
Imágen 25. Se reconfigura la zona WAN.



Fuente: Autoría Propia

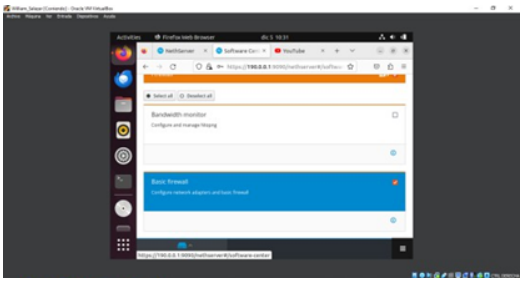
Se verifica el adaptador del Nethserver para configurar como NAT

Imágen 26. El Adaptador 3 del Nethserver se reconfigura como NAT.



Fuente: Autoría Propia

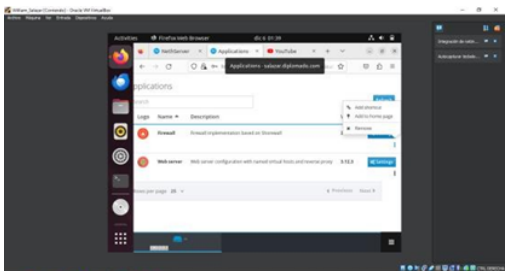
Imágen 27. Se instala Basic Firewall desde Software Center.



Fuente: Autoría Propia

Posteriormente se accede al Firewall del panel para proteger los dispositivos y datos personales de posibles amenazas en línea

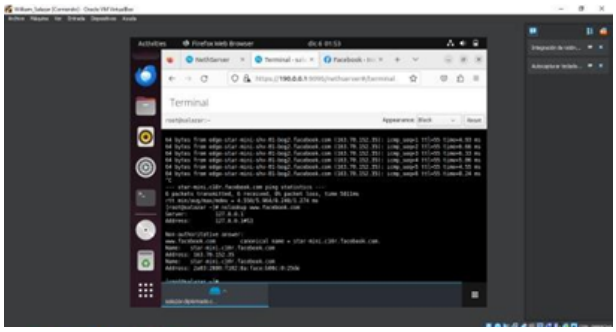
Imágen 28. Se accede al Firewall en el panel.



Fuente: Autoría Propia

Posteriormente se valida el comando nslookup lo que nos permite la restriccion de la dirección IP.

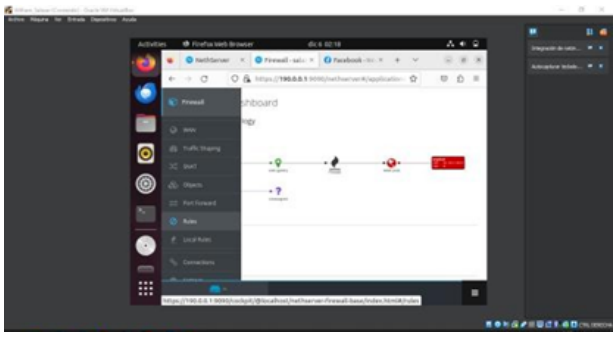
Imágen 29. Se hace uso del comando es: nslookup www.facebook.com a través de la terminal el direccionamiento IP



Fuente: Autoría Propia

Se valida el acceso al firewall. Su función es supervisar, filtrar y controlar el tráfico de red entrante y saliente, estableciendo una barrera entre una red interna y redes externas.

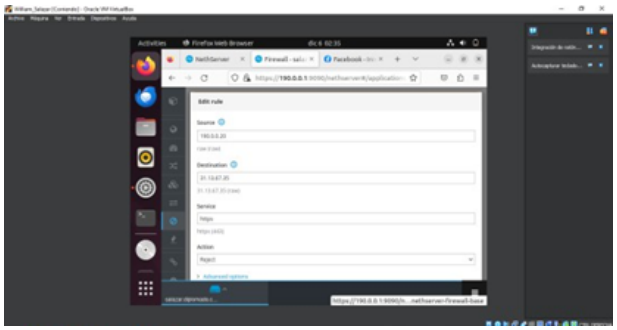
Imágen 30. Se restringe el acceso en la Firewall.

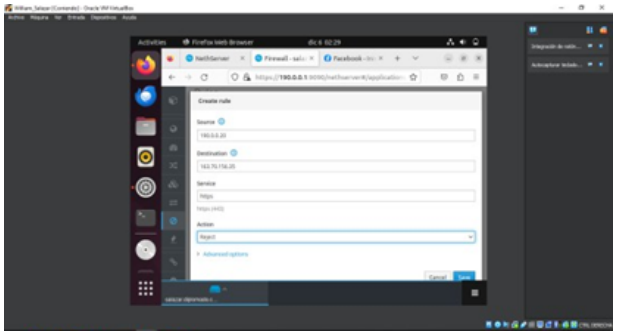


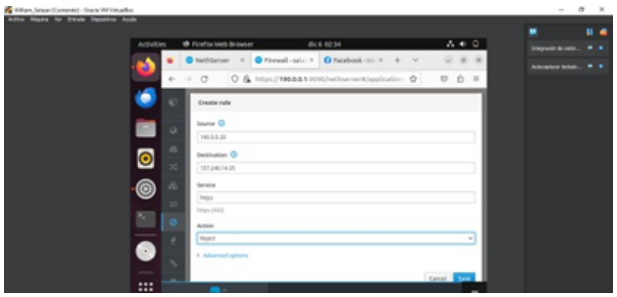
Fuente: Autoría Propia

Posteriormente se crean reglas necesarias para la restricción del proceso de restricción

Imágen 31. Se crean las reglas.



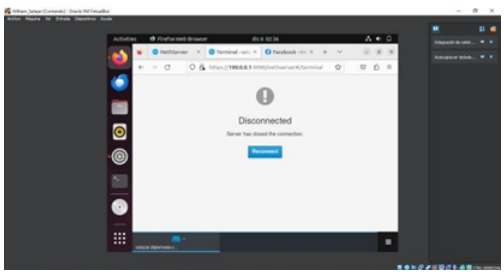




Fuente: Autoría Propia

Posteriormente validamos que los datos configurados esten funcionando a cabalidad

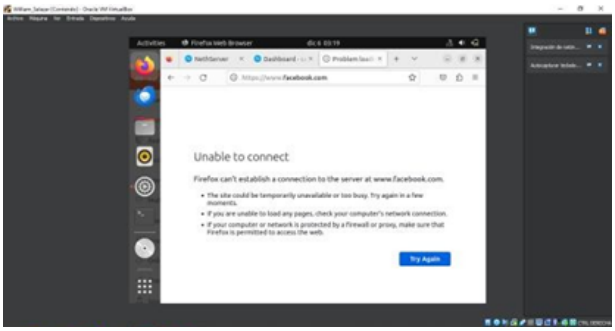
Imágen 32. Se reinicia Nethserver para aplicar cambios.



Fuente: Autoría Propia

Se comprueba iniciando en facebook y se valida que funciona la regla de configuración.

Imágen 33. Se intenta acceder a www.facebook.com para comprobar el cumplimiento de la regla.



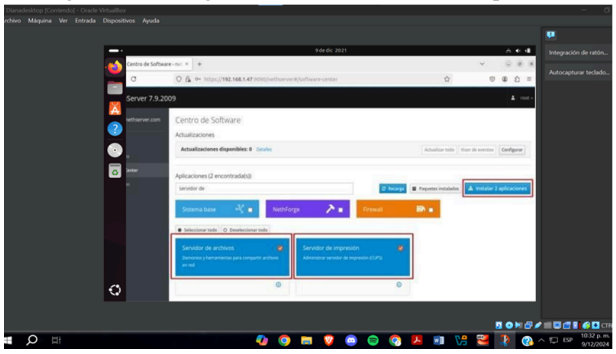
Fuente: Autoría Propia

5 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Se descarga el servidor de archivos y de impresión, ingresando al centro de software de Nethserver.

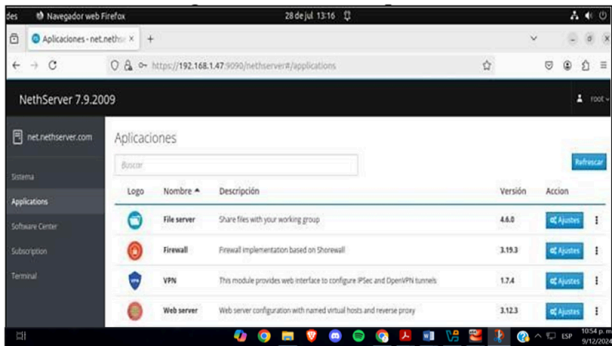
Figura 1. Descarga de servidor de archivo e impresión



Fuente: Autoría propia

Validar la instalación del file server, en el panel de aplicaciones

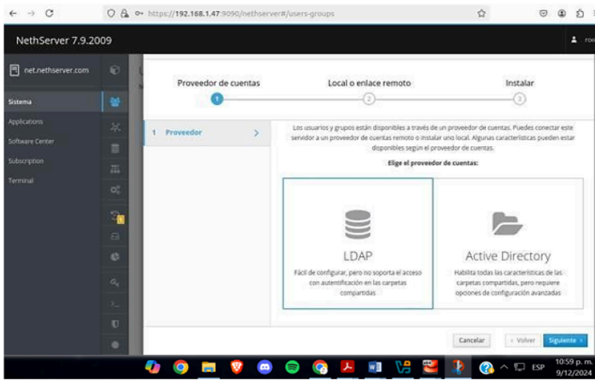
Imágen 2. Panel de aplicaciones



Fuente: Autoría propia

En NethServer, se lleva a cabo la instalación y configuración del servicio LDAP mediante el módulo Sistema, con el objetivo de establecer el proveedor de cuentas.

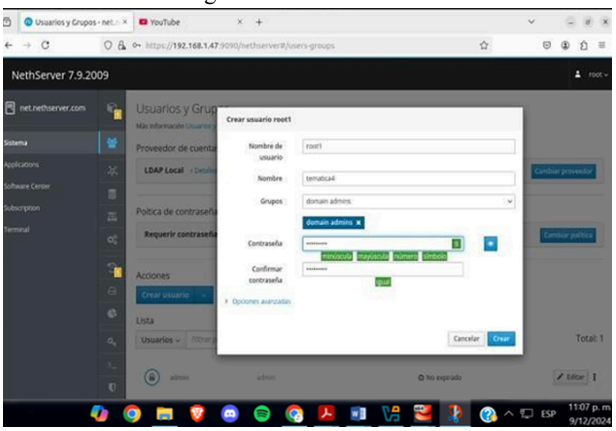
Figura 3. Instalación servicio LDAP



Fuente: Autoría propia

En la sección de usuarios y grupos, se crea el usuario que tendrá acceso a los diferentes servicios. Asimismo, se asigna el grupo correspondiente al usuario para que pueda utilizar las conexiones.

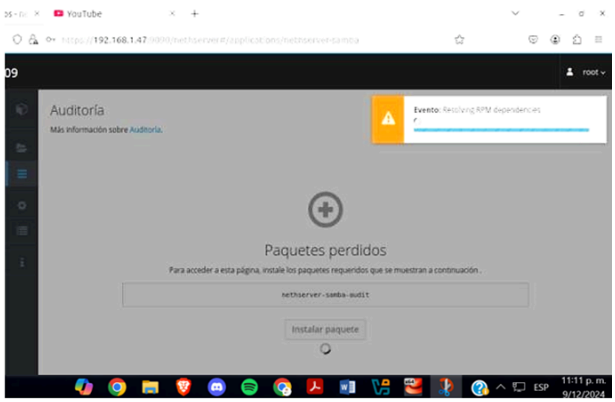
Figura 4. Usuario LDAP



Fuente: Autoría propia

Ingresamos a la configuración del servidor de archivos y se procede a instalar el paquete "nethserver-samba-audit" desde el módulo de auditoría.

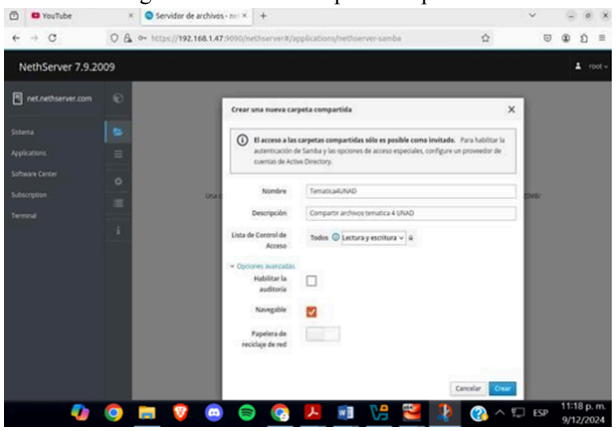
Figura 5. Instalación nethserver-samba-audit



Fuente: Autoría propia

Se configura la carpeta compartida en la red con los ajustes correspondientes en la sección de carpetas compartidas.

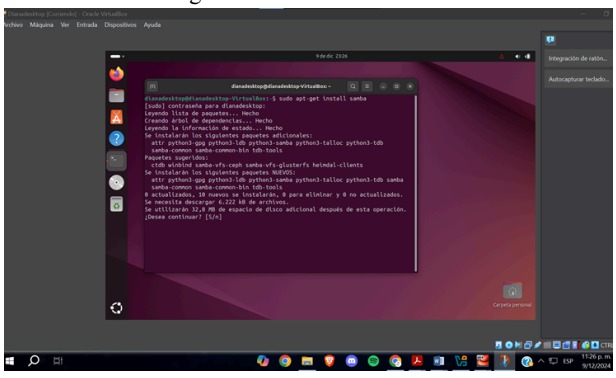
Figura 6. Creación carpeta compartida



Fuente: Autoría propia

Se ingresa a la computadora de escritorio con Ubuntu y se procede a instalar el servicio Samba utilizando el comando "sudo apt-get install samba".

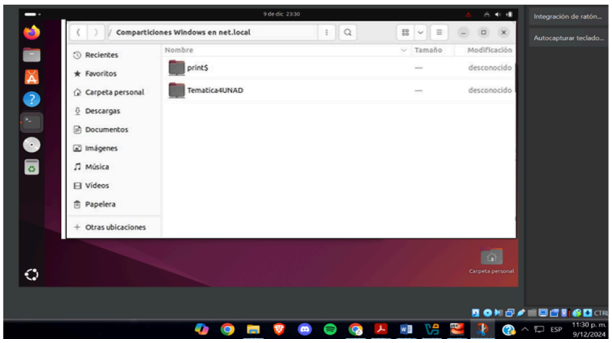
Figura 7. Instalación Samba



Fuente: Autoría propia

En la máquina de escritorio, en otras ubicaciones, se puede acceder a la red local del servidor y, dentro de esta, visualizar las carpetas compartidas de impresión y la carpeta "temática4UNAD".

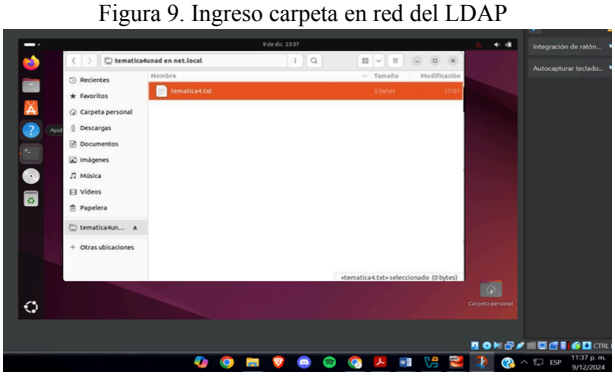
Figura 8. Carpetas compartidas



Fuente: Autoría propia

Ingresamos a la carpeta "tematica4UNAD" utilizando las credenciales del usuario registrado en LDAP y se añade un archivo, el cual queda disponible en la red compartida.

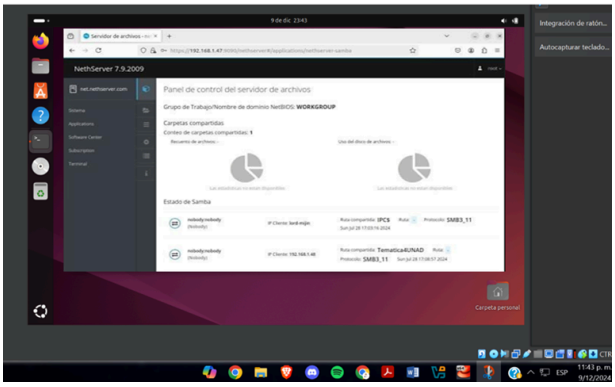
Figura 9. Ingreso carpeta en red del LDAP



Fuente: Autoría propia

Verificamos en el panel de control del servidor de archivos el registro del usuario que accedió a la carpeta compartida.

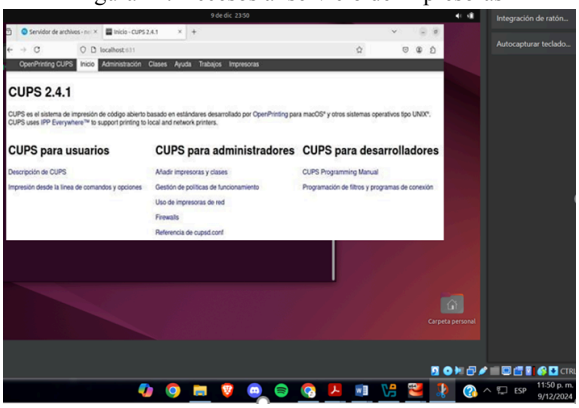
Figura 10. Accesos a la carpeta compartida



Fuente: Autoría propia

Acceder al servicio CUPS a través de la dirección localhost:631 en el navegador, el cual funciona como el administrador del servicio de impresión en NethServer.

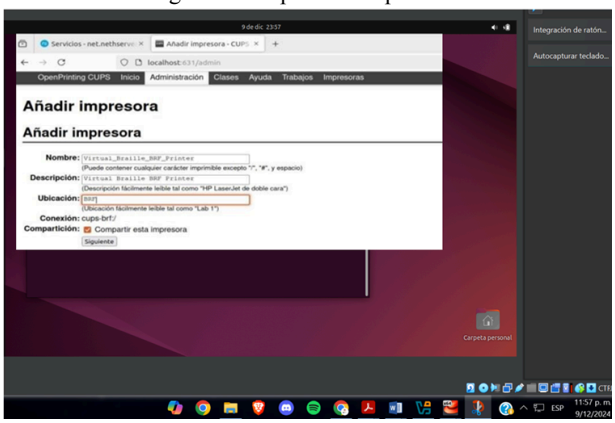
Figura 11. Accesos al servicio de impresoras



Fuente: Autoría propia

Se hace la instalación de la impresora en red, en la opción de configuración de CUPS. Al intentar imprimir un archivo la impresora que se encuentra configurada, aparece como disponible y puede ser seleccionada.

Figura 12. Impresora disponible



Fuente: Autoría propia

6 TEMÁTICA 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo

.

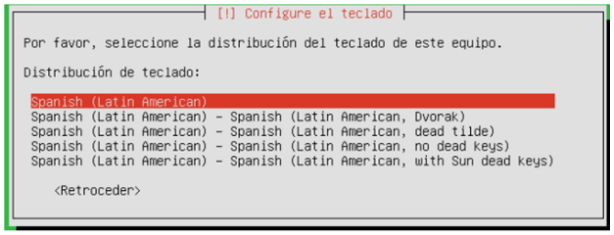
Se realiza la intalacion de Zentyal.

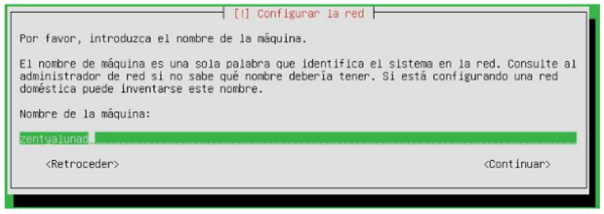
Imágen 1. Se realiza la instalación

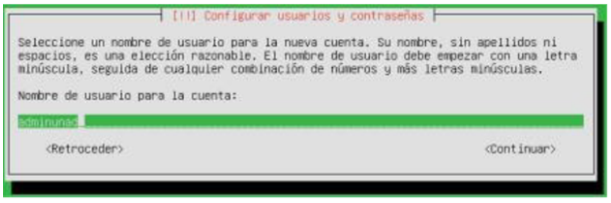
Fuente: Autoria propia.

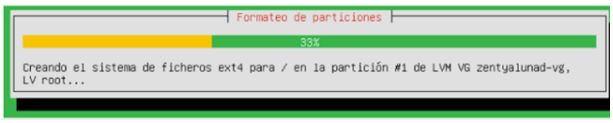
Se realizan las configuraciones correspondientes dentro del sistema.

Imágen 2. Se realizan las configuraciones correspondientes









Fuente: Autoría Propia

Se inicia la instalacion del proceso adecuado.

Imágen 3. Se inicia la instalación oficial

Fuente: Autoría Propia

Una vez finalizada la carga del sistema zentyal, se muestra lainterfaz del usuario final y se procede a abrir la consola de administración de esta plataform

Imágen 4. Programa ya abierto

Fuente: Autoría Propia

Se accede a la configuración del servidor.

Imágen 5. Posteriormente aparece la configuración final del servidor

Fuente: Autoría Propia

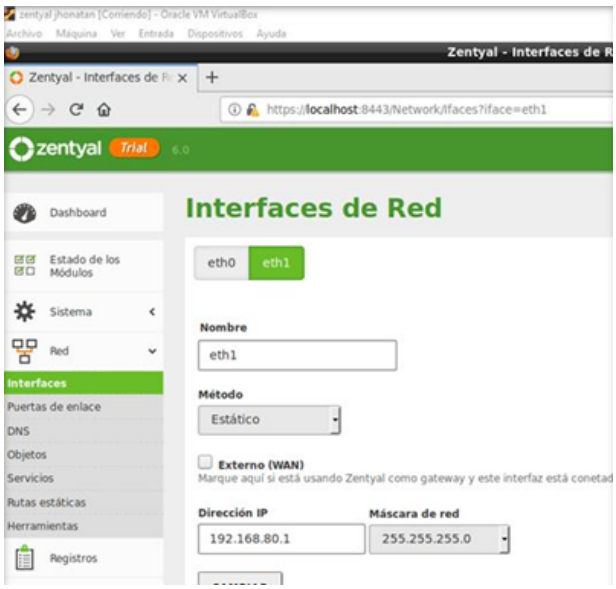
Luego se instalan los paquetes de la VPN necesarios para la instalacion adecuada del servidor.

Imágen 6. Posteriormente aparece la instalacion de los paquetes disponibles en la VPN y se da la opción de instalar.

Fuente: Autoría Propia

Posteriormente se adecua teniendo en cuenta el direccionamiento de la IP necesaria a traves del server

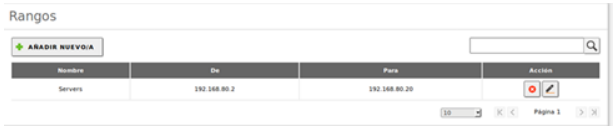
Imágen 7. Para la interfaz eth1 asignamos la ip 192.168.80.1 y a través de DHCP Server



Fuente: Autoria propia.

Luego se asignan los rangos determinados por el sistema

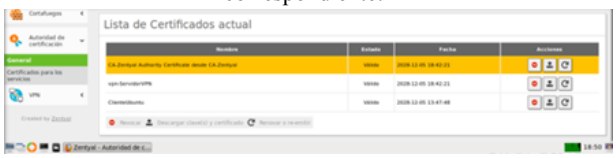
Imágen 8. Se asigna un rango desde 192.168.80.2 a 192.168.80.20



Fuente: Autoria propia.

Luego los servidores VPN se crean manualmente teniendo en cuenta el servidor del VPN.

Imágen 9. Posteriormente se tienen en cuenta los servidores VPN y posteriormente se crea manualmente el servidor VPN de manera automática para obtener el certificado correspondiente:



Fuente: Autoria propia.

Finalizando se valida la VPN del servidor que ya esta creado.

Imágen 10. Posteriormente se verifica el servidor ya creado de la VPN

Fuente: Autoria propia.

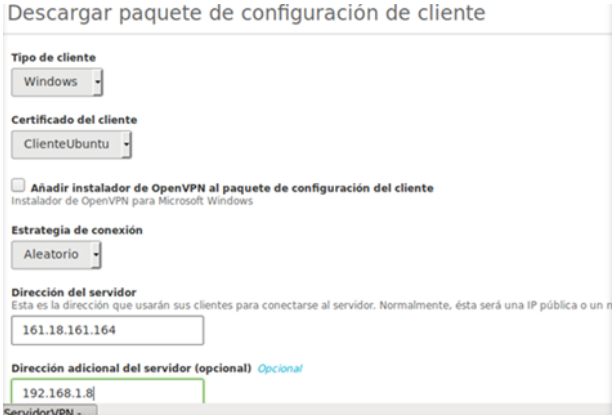
Se verifica que la configuración sea la adecuada teniendo en cuenta el servidor

Imágen 11. Se verifica la configuración del servidor.

Fuente: Autoria propia.

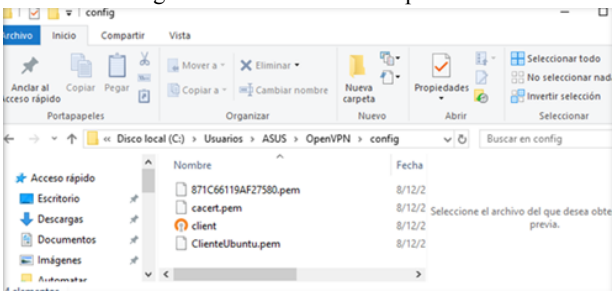
Se verifican los direccionamientos a traves de la IP.

Imágen 12. Se descarga la configuración de windows para verificar la IP



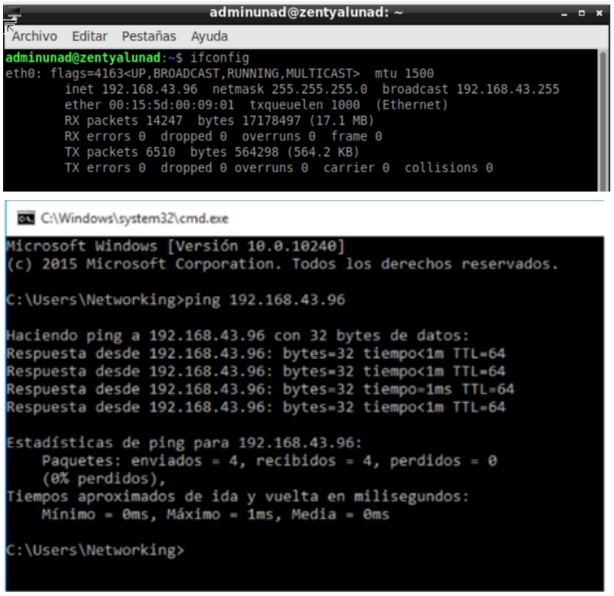
Fuente: Autoria propia.

Imágen 13. Se copia los ficheros descargados al directorio de configuración de archivos de OpenVPN



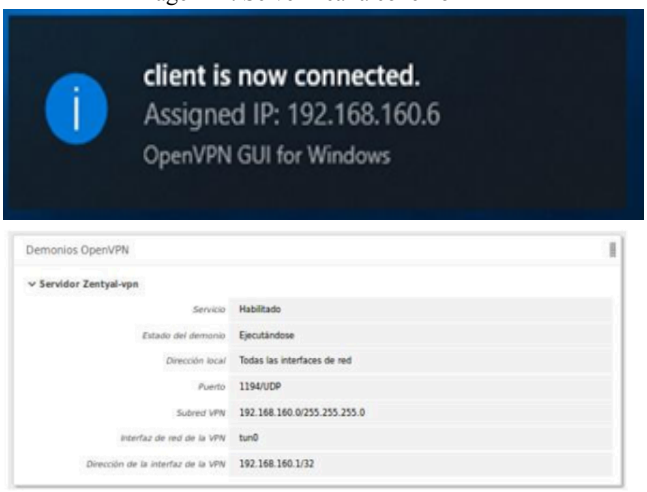
Fuente: Autoria propia.

Imágen 15. Establecida la conexión se procede a realizar la prueba, en este caso validamos la dirección ip que tiene el servidor.



Fuente: Autoria propia.

Imágen 14. Se verifica la conexión



Fuente: Autoria propia.

6.1.1 Conclusiones.

La implementación de un cortafuegos (firewall) para restringir el acceso a sitios web no deseados, como portales de entretenimiento y redes sociales, contribuye a mejorar la seguridad de la red al bloquear el tráfico no deseado. Este enfoque es eficaz para prevenir accesos no autorizados y proteger la red interna de posibles amenazas provenientes de fuentes no confiables.

Restringir el acceso a sitios web de entretenimiento y redes sociales desde una estación de trabajo GNU/Linux ayuda a mantener un entorno de trabajo más enfocado y productivo. Al bloquear el acceso a estos sitios durante el horario laboral, las organizaciones pueden asegurarse de que los recursos de la red se utilicen de manera más eficiente, reduciendo distracciones y aumentando la productividad.

La configuración detallada de reglas y políticas en el cortafuegos es esencial para garantizar que las restricciones se apliquen de manera efectiva. La creación de políticas basadas en categorías de tráfico, como la restricción de puertos específicos o direcciones URL asociadas a redes sociales y sitios de entretenimiento, permite un control granular y preciso del tráfico de la red, adaptándose a las necesidades de la organización.

La configuración del cortafuegos en GNU/Linux, utilizando herramientas como iptables o firewall, demuestra la flexibilidad y potencia del sistema operativo para administrar el tráfico de red. Aunque requiere conocimientos avanzados en la creación de reglas y políticas de acceso, GNU/Linux ofrece una plataforma robusta para implementar una solución de firewall efectiva y adaptada a los requerimientos específicos del entorno de trabajo.

La configuración de la VPN en un sistema operativo GNU/Linux demuestra la versatilidad y robustez de este entorno para manejar conexiones seguras. Herramientas como OpenVPN o IPsec permiten una implementación eficiente, aunque se requieren conocimientos específicos para ajustar adecuadamente los parámetros de seguridad y la gestión de claves.

La estabilidad de la conexión a través de una VPN depende en gran medida de la configuración adecuada tanto del cliente como del servidor. La correcta gestión de la encriptación y la optimización de la red puede asegurar que el rendimiento no se vea afectado significativamente, permitiendo el acceso sin problemas a aplicaciones y servicios de la estación de trabajo.

En conjunto, las temáticas abordadas proporcionan una solución integral para la gestión de redes seguras y eficientes. La implementación de tecnologías como **DHCP**, **DNS**, **firewalls**, **proxy**, **VPN**, y servidores de archivos e impresión no solo mejora la administración de recursos y servicios, sino que también refuerza la seguridad de la red, optimiza el uso de la infraestructura y aumenta la productividad de los usuarios. La correcta integración de estas soluciones en un entorno como **Nethserver** facilita su implementación, mientras que el uso de **GNU/Linux** como sistema operativo de base asegura una plataforma robusta y flexible para administrar y mantener la infraestructura de red.

6.1.2 CITAS Y/O REFERENCIAS

García, P. (2019). *Seguridad en redes: Implementación de proxies para control de acceso a Internet*. Editorial Seguridad y Red.

González, R. (2020). *Gestión de cortafuegos en GNU/Linux: Aplicación de políticas de seguridad en entornos corporativos*. Red Digital.

Kurtz, J. (2018). *Administración de redes con GNU/Linux: DHCP y DNS*. Editorial Tecnología y Redes.

Martínez, J. (2019). *Implementación de servidores de archivos y de impresión en redes GNU/Linux*. Editorial Tecnología y Redes.

Sánchez, A., & López, R. (2021). *Configuración avanzada de servidores de archivos e impresión con LDAP en entornos GNU/Linux*. Journal of Network Services, 14(3), 115-129.

Smith, J. (2020). *VPN: Protegiendo la privacidad en redes públicas*. Springer.

Wang, H., Zhang, L., & Liu, Y. (2022). *Fundamentos de seguridad de redes y cortafuegos: Implementación en sistemas GNU/Linux*. Wiley-IEEE Press.

Jones, R., & Adams, M. (2021). *Redes privadas virtuales en GNU/Linux: Seguridad y privacidad en la era digital*. Journal of Cybersecurity, 15(3), 45-60.