

# IMPLEMENTACIÓN DE NETHSERVER Y CONFIGURACIÓN DE SERVICIOS DE SEGURIDAD PARA INFRAESTRUCTURA

Daniel Alberto Sarmiento Hernández  
e-mail: [dasarmiento@unadvirtual.edu.co](mailto:dasarmiento@unadvirtual.edu.co)  
Jean Carlo Castaño Millan  
e-mail: [jccastanomi@unadvirtual.edu.co](mailto:jccastanomi@unadvirtual.edu.co)  
Juan Andrés Giraldo Navarro  
e-mail: [jagiraldon@unadvirtual.edu.co](mailto:jagiraldon@unadvirtual.edu.co)  
Ricardo Andrés Penilla Muñoz  
e-mail: [rapenillam@unadvirtual.edu.co](mailto:rapenillam@unadvirtual.edu.co)  
Iván Darío Villegas Adarve  
e-mail: [iv18vil221@unadvirtual.edu.co](mailto:iv18vil221@unadvirtual.edu.co)

**RESUMEN:** El documento actual recopila el desarrollo general de las temáticas solucionadas bajo el entorno GNU/Linux, a las cuales se les aplicó sus respectivos procesos de instalación, configuración y ejecución, con el único propósito de responder a los requerimientos solicitados en la guía "Guía de actividades y rúbrica de evaluación – Paso 9 - Solucionando necesidades específicas con GNU/Linux", construyéndose una solución eficiente para infraestructura.

**PALABRAS CLAVE:** DNS, Proxy, DHCP, VPN, Firewall, LDAP.

## 1 INTRODUCCIÓN

Después de haberse llevado un proceso secuencial en cada una de las unidades programadas por el diplomado, se comprendieron los principios y herramientas necesarias en la plataforma GNU/Linux, esto hizo posible que se respondiera los requerimientos solicitados a través del servicio Nethserver basado en CentOS, plataforma base en la que se ejecutó la solución a cada una de las temáticas presentes en este artículo, entre las que se describen: temática 1: DHCP server, DNS server y controlador de dominio. Temática 2: Proxy. Temática 3: Cortafuegos. Temática 4: File Server y Print. Temática 5: VPN. Cada una de estas soluciones se encuentran debidamente evidenciadas y coherentes a su funcionamiento.

## 2 INSTALACIÓN DE NETHSERVER 7.9

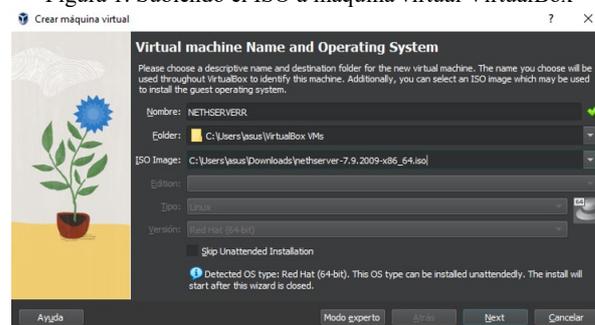
Nethserver 7.9 es una distribución estable de Linux basada en CentOS que proporciona una plataforma para servidores. Está diseñada para simplificar la administración de servidores y se brinda una variedad de

herramientas y funcionalidades para facilitar la gestión de servicios como correo electrónico, firewall, servidor web, directorio, almacenamiento, servidor proxy entre muchas más funcionalidades.

## 2.1 CONFIGURACIÓN DE MÁQUINA VIRTUAL E INSTALACIÓN DE NETHSERVER.

Se crea una máquina virtual, en donde se asigna el nombre a la máquina virtual que se instalará y se selecciona la ISO de Nethserver, seguidamente se aplican configuraciones especiales como la cantidad en memoria, CPU y disco duro, con todo esto se tendrá la máquina lista para instalar.

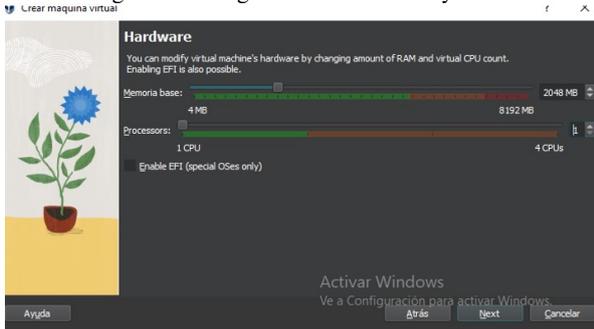
Figura 1. Subiendo el ISO a máquina virtual VirtualBox



Fuente: Autoría propia.

En este caso en particular, comenzamos montado la imagen ISO, para proceder con el proceso de instalación.

Figura 2. Configuración de memoria y CPU.



Fuente: Autoría propia.

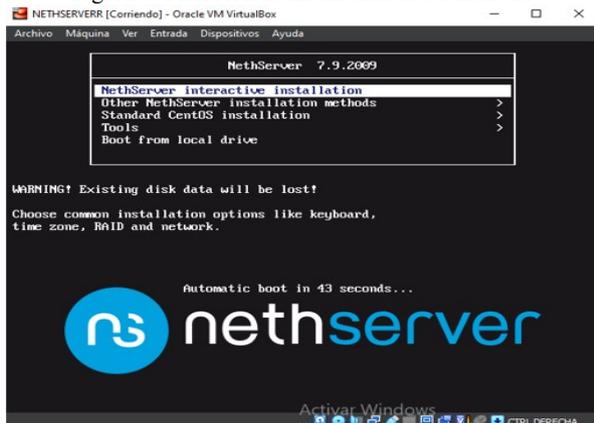
Figura 3. Configuración de capacidad del disco duro.



Fuente: Autoría propia.

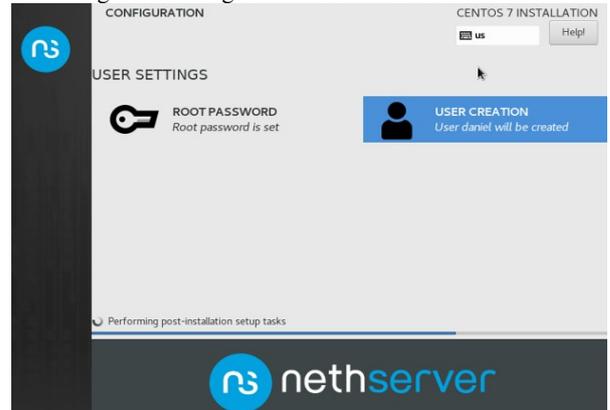
Una vez las preconfiguraciones de la máquina virtual estan listas, se procede con el inicio de la máquina virtual para proceder con la instalación de nethserver, aquí solo se realizan las preconfiguraciones básicas y el instalador hara el resto.

Figura 4. Selección de instalación de Nethserver.



Fuente: Autoría propia.

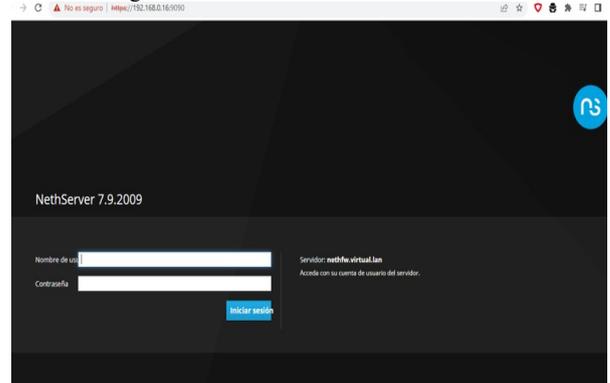
Figura 5. Configuraciones básicas de Nethserver.



Fuente: Autoría propia.

Una vez finalizada la instalación, el servicio estará activo y podrá acceder a través del puerto 9090.

Figura 6. Puesta en marcha de Nethserver.

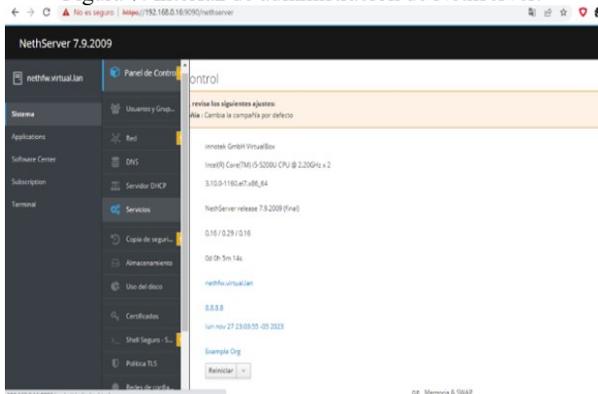


Fuente: Autoría propia.

## 2.2 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, para esto se ingresa a la interfaz de la plataforma.

Figura 7. Interfaz de administración de Nethserver.

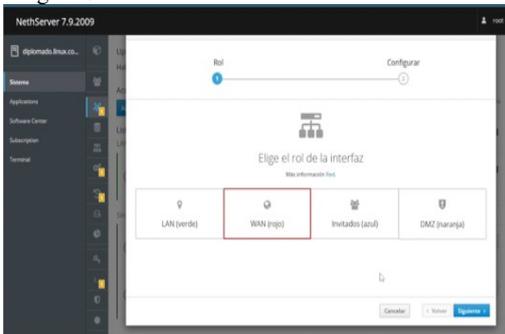


Fuente: Autoría propia.

Una vez en la interfaz, se procede con la configuración de las tres interfaces solicitadas, LAN, WAN y DMZ, con sus respectivos direccionamientos IP, esto se configura sobre el menú izquierdo en la opción de sistemas y opción red.

Sobre la sección de la figura 8, se procede con la configuración de las tres interfaces según su color y proposito.

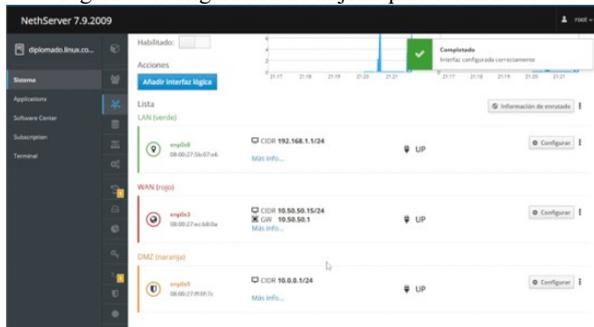
Figura 8. Interfaz de administración de Nethserver.



Fuente: Autoría propia.

Sobre la figura 9, se puede observar cada interfaz configurada, la interfaz roja es la WAN la cual dara salida a internet, la interface Verde es la LAN y la interfaz naranja es la zona DMZ para servidores.

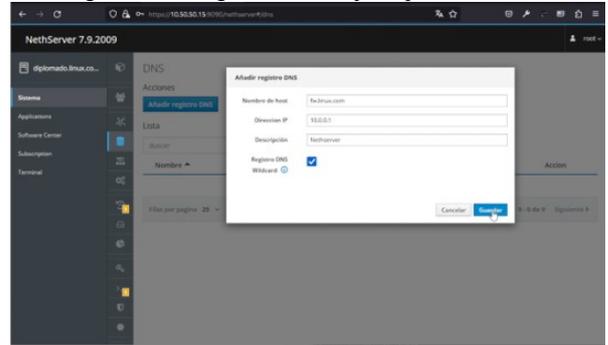
Figura 9. configuración de tarjetas para Nethserver.



Fuente: Autoría propia.

Ahora que se tienen las tres interfaces listas, se procederá con la configuración de la IP del Nethserver y un nombre de dominio en este caso fw.linux.com

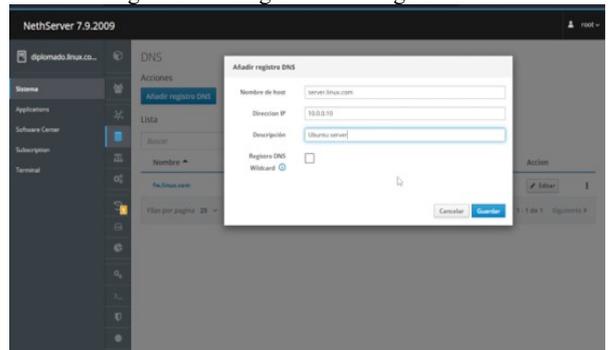
Figura 10. configuración de tarjetas para Nethserver



Fuente: Autoría propia.

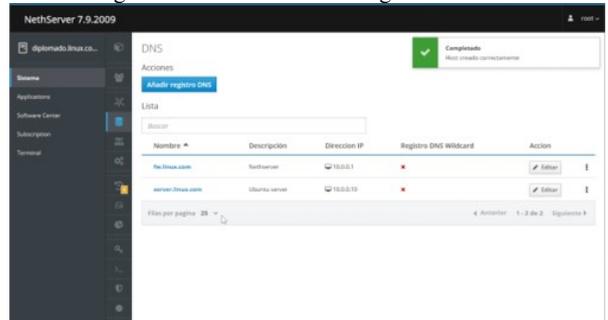
Ahora se procede con la configuración del servidor DNS, esta gestión se realiza en el menu sistemas y luego sobre la opción DNS, aquí se activa el servicio y se configura un registro DNS, llamada server.linux.com

Figura 11. configuración de registro DNS.



Fuente: Autoría propia.

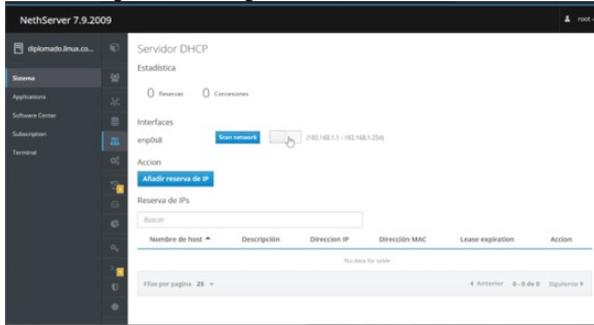
Figura 12. Confirmación de registro de DNS.



Nota: Autoría propia

Ahora se procede con la configuración del servidor DHCP, esto se realiza en la opción de sistemas y luego en la opción DHCP, donde se procede con la activación y configuración.

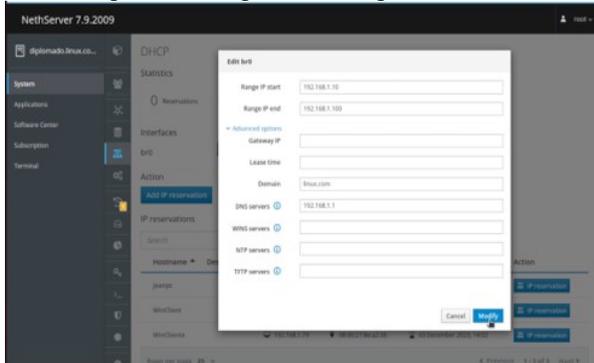
Figura 13. configuración de servidor DHCP.



Fuente: Autoría propia.

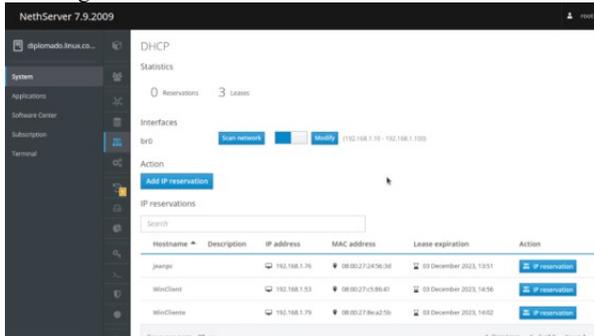
Se configura spool de red bajo el rango de red 192.168.1.0/24, con rango a la 192.168.1.10 a la 192.168.1.100.

Figura 14. configuración de segmento de red.



Fuente: Autoría propia.

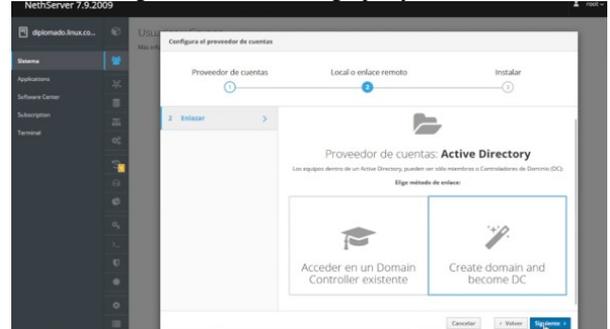
Figura 15. Evidencia del funcionamiento de DHCP.



Fuente: Autoría propia.

Ahora se procede con la configuración del servicio de controlador de dominio, en donde se deberá crear los respectivos usuarios y grupos para este fin.

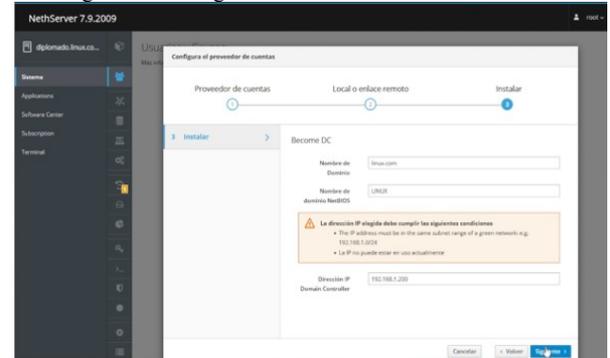
Figura 16. creación de grupos y usuarios.



Fuente: Autoría propia.

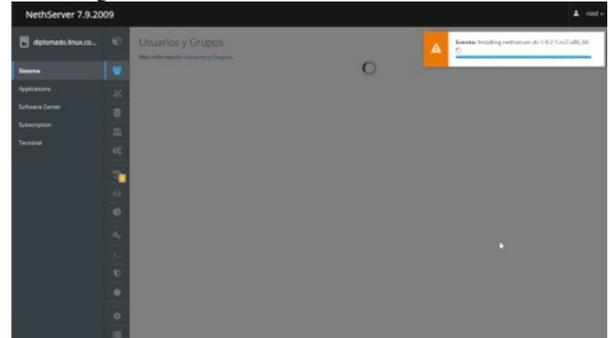
Se configura controlador de dominio, con el nombre de dominio linux.com y la dirección 192.168.1.200

Figura 17. configuración de controlador de dominio.



Fuente: Autoría propia.

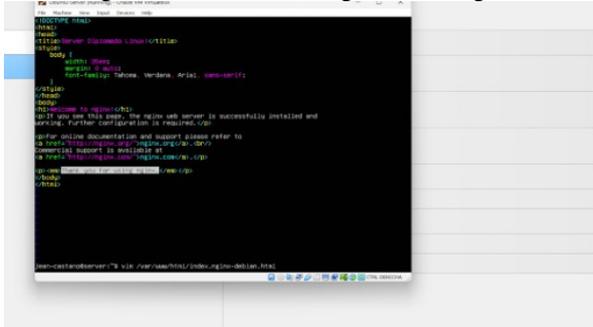
Figura 18. Instalación de controlador de dominio.



Fuente: Autoría propia.

A continuación se procede con el montaje de un servidor web nginx para un servidor ubuntu en la zona DMZ.

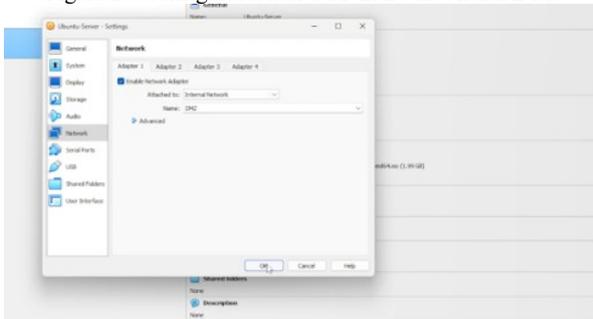
Figura 19. Instalación configuración de Nginx.



Fuente: Autoría propia.

Se configura tanto en la interface DMZ del nathserver y la interface LAN del servidor ubuntu, para que estas en la maquina Virtual Box se vean dentro de una red interna.

Figura 20. configuración de NIC LAN en Virtual Box.



Fuente: Autoría propia.

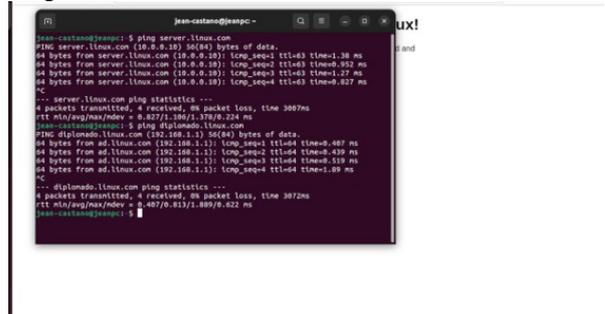
Finalmente se realizan pruebas desde un cliente linux en la interfaz verde, donde se evidencia el funcionamiento de la página desde el servidor Ngix.

Figura 21. Pruebas del servidor Ngix en el navegador.



Fuente: Autoría propia.

Figura 22. Pruebas de conexión desde el cliente a dos redes.

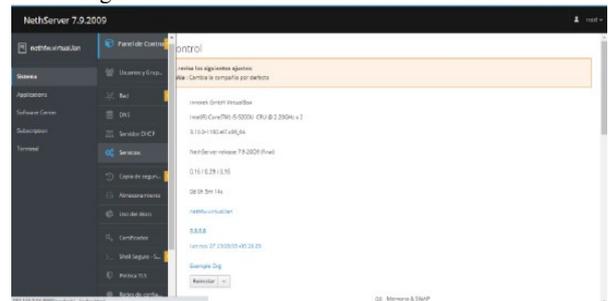


Fuente: Autoría propia.

## 2.3 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, para esto se ingresa a la interfaz de Nethserver.

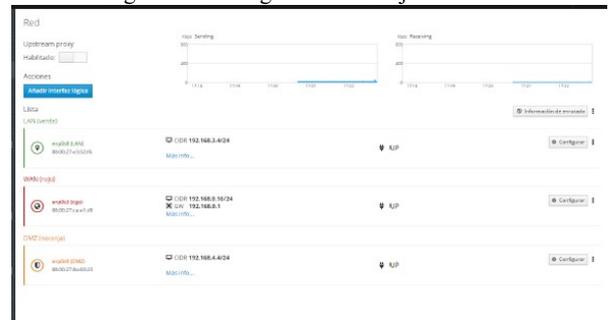
Figura 23. Interfaz administrativa de Nethserver.



Fuente: Autoría propia.

Para esta topología también se implementará la configuración de tres tarjetas de red, una verde para LAN, una roja para WAN y otra naranja para DMZ.

Figura 24. Configuración de tarjetas de red.



Fuente: Autoría propia.

En la anterior imagen se evidencia que la interface LAN verde queda bajo la red 192.168.3.0/24, la interface WAN roja

esta sobre la red 192.168.0.0/24 y finalmente la red DMZ naranja esta sobre la red 192.168.4.0/24, sobre la figura 25 se podra evidenciar las IP asignadas a cada interfaz.

Figura 25. Validación de tarjetas de red.

```

root@nethfw:~# ifconfig
[root@nethfw ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.16 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:feea:e1d9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ca:e1:d9 txqueuelen 1000 (Ethernet)
    RX packets 20972 bytes 1701967 (1.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22958 bytes 7274256 (6.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

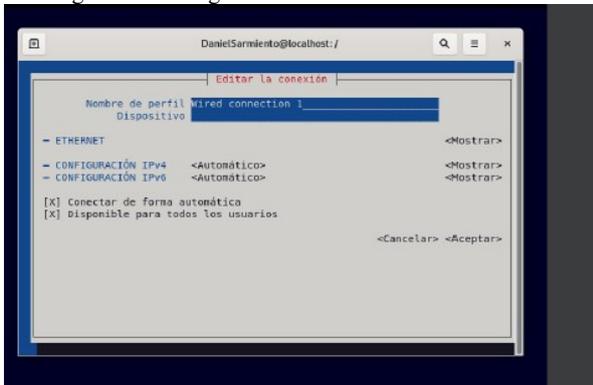
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.4 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::a00:27ff:fee3:52f6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e3:52:f6 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2032 (1.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.4 netmask 255.255.255.0 broadcast 192.168.4.255
    inet6 fe80::a00:27ff:fe8a:323 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8a:03:23 txqueuelen 1000 (Ethernet)
    RX packets 1649 bytes 100764 (98.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 151 bytes 12828 (12.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

Fuente: Autoría propia.

Sobre la interfaz LAN verde, se encuentra un Linux Debian, equipo cliente con el que se realizara pruebas de filtrado web, sobre este equipo se configura la conexión de red en DHCP.

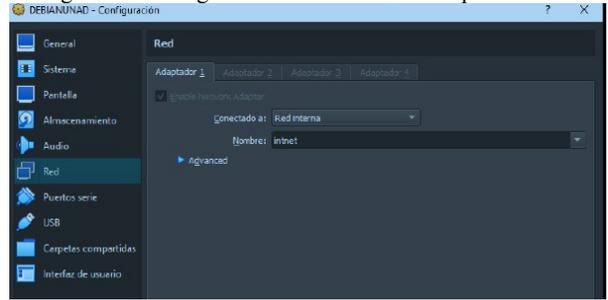
Figura 26. Configuración DHCP en nic LAN cliente.



Fuente: Autoría propia.

Se configuran la tarjeta de red LAN verde de Netserver y la tarjeta LAN del cliente linux Debian en Virtualbox. Para que ambas queden sobre la misma red local virtual.

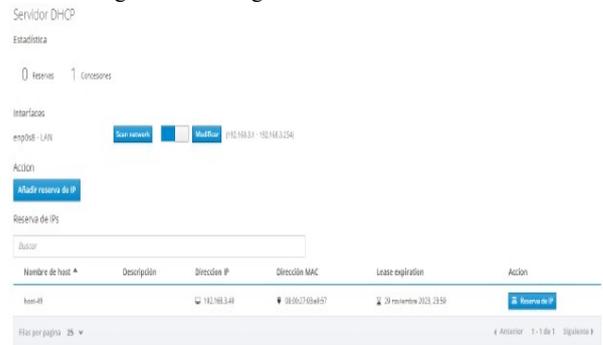
Figura 27. Configuración red internet en máquina virtual.



Fuente: Autoría propia.

Ahora que todo esta configurado adecuadamente para la red local, se procede con la activación y configuración del servidor DHCP.

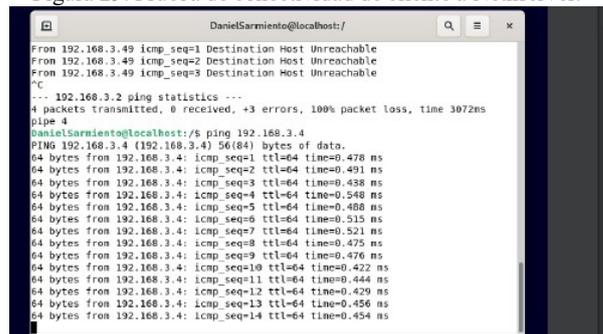
Figura 28. Configuración de servidor DHCP.



Fuente: Autoría propia.

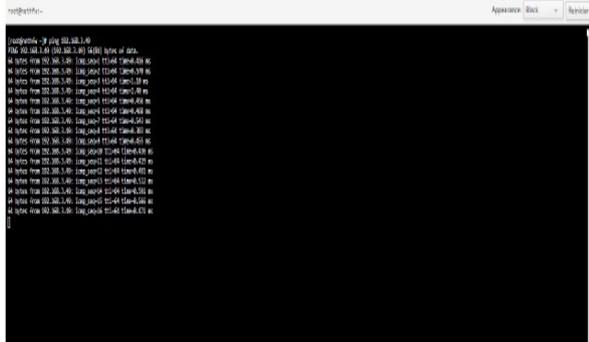
Como se puede observar el equipo cliente adquire la IP 192.168.3.49 por DHCP, esto quiere decir que ya hay conectividad local la cual se valida a continuación.

Figura 29. Prueba de conectividad de cliente a Nethserver.



Fuente: Autoría propia.

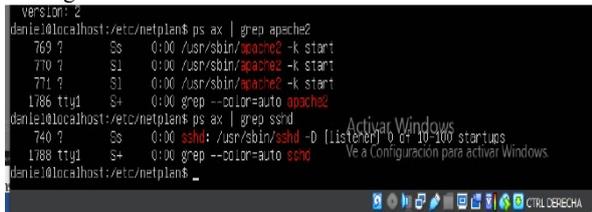
Figura 30. Prueba de conectividad desde Nethserver al cliente.



Fuente: Autoría propia.

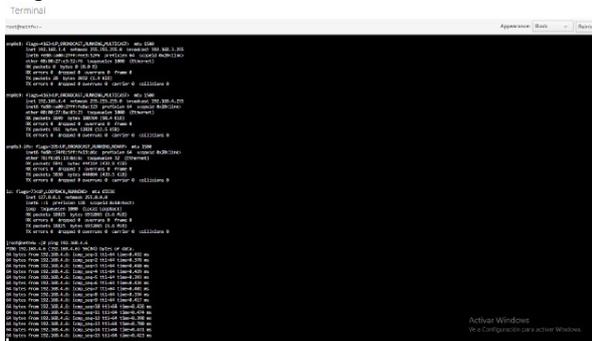
Ahora que se tiene la conectividad lista entre LAN verde y el equipo cliente, se procede con la configuración de una IP estática en el Ubuntu servidor que está en la red DMZ, para esto se configura la IP 192.168.4.6.

Figura 31. Validación de servicios de Ubuntu servidor.



Fuente: Autoría propia.

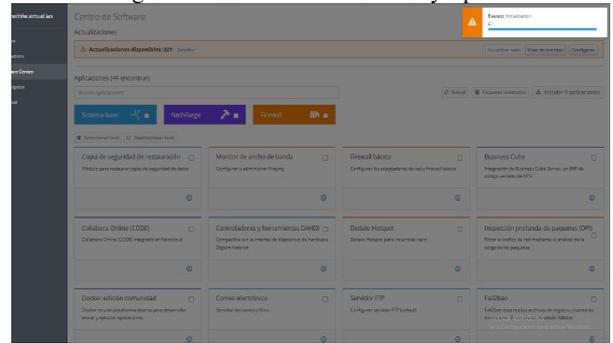
Figura 32. Conectividad desde Nethserver a Ubuntu servidor.



Fuente: Autoría propia.

Ahora se procede con la instalación del firewall y del proxy web Squid desde el centro de software de Nethserver.

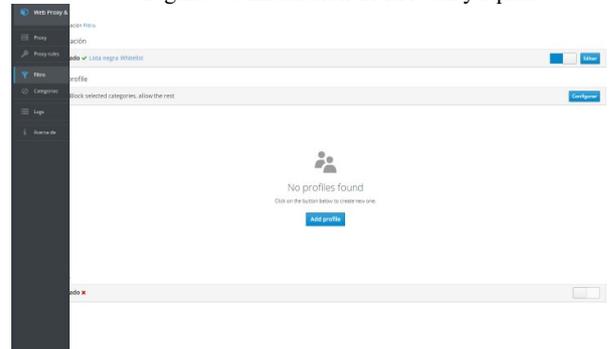
Figura 33. Instalación de firewall y squid.



Fuente: Autoría propia.

Una vez instalado el servicio, se ingresa a activar el firewall y a activar Squid para su posterior configuración.

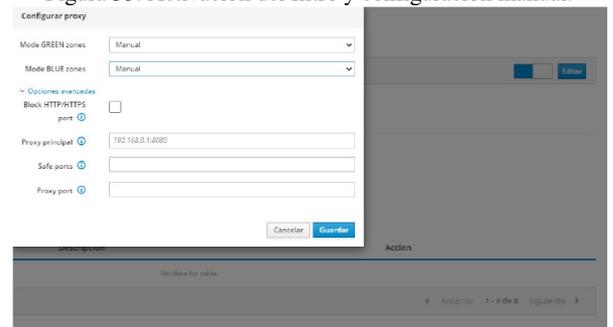
Figura 34. Instalación de firewall y squid.



Fuente: Autoría propia.

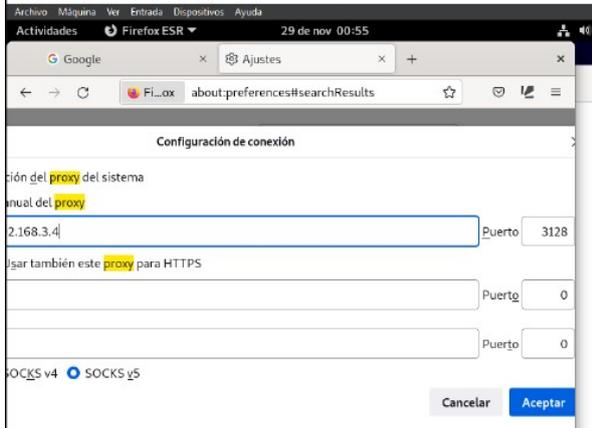
Se activa el filtro y se configura la interfaz verde LAN en modo manual.

Figura 35. Activación del filtro y configuración manual.



Fuente: Autoría propia.

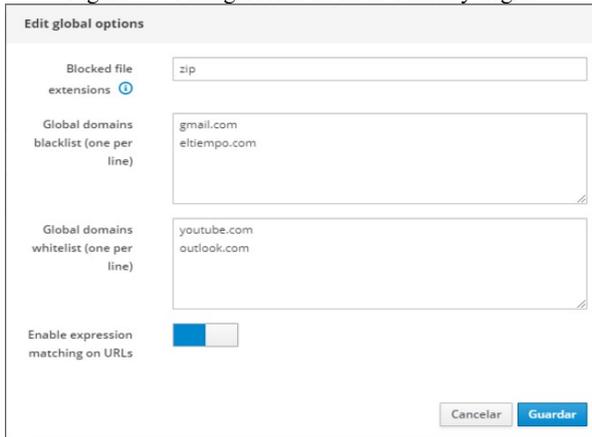
Figura 36. Activación del filtro y configuración manual.



Fuente : Autoría propia.

Se configuran reglas de filtrado, gmail.com y el tiempo.com no abrirán, pero youtube.com y outlook.com si.

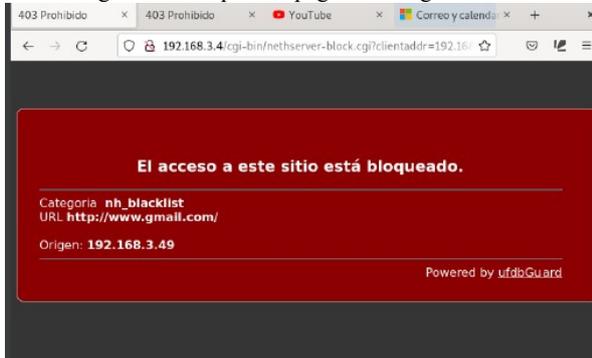
Figura 37. Configuración de listas blanca y negra.



Fuente: Autoría propia.

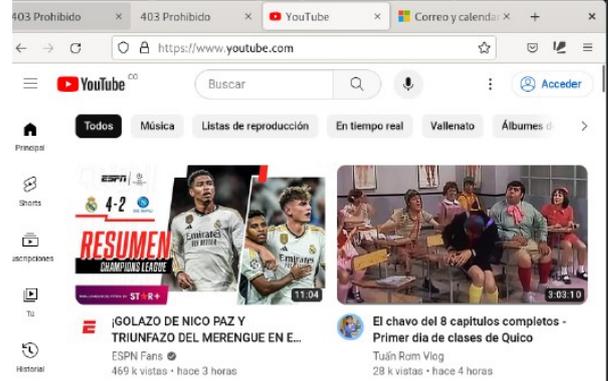
Ahora se evidencian pruebas de bloqueo desde el navegador web del cliente.

Figura 38. Bloqueo de página www.gmail.com.



Fuente: Autoría propia.

Figura 39. Página permitida por Squid.

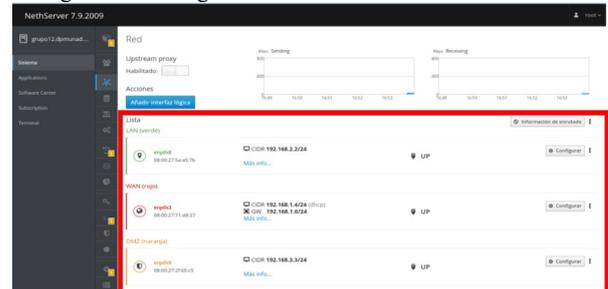


Fuente: Autoría propia.

## 2.4 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, para empezar, se abre la interfaz de Nethserver.

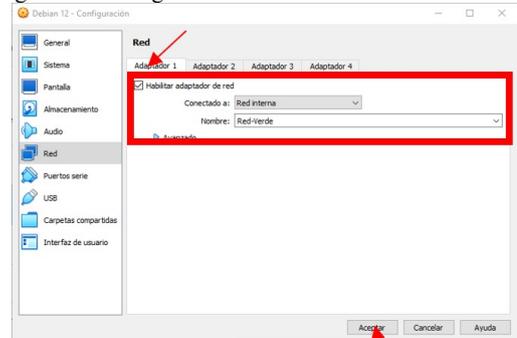
Figura 40. Configuración de las interfaces en Nethserver.



Fuente: Autoría propia.

Para que cada tarjeta de red en Nethserver funcione bien entre redes local y redes wan, se deben configurar primero sobre la configuración de Virtualbox.

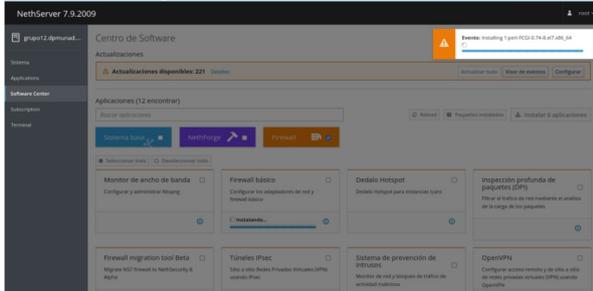
Figura 41. Configuración de las interfaces en VirtualBox.



Fuente: Autoría propia.

Para empezar a realizar la actividad con la temática planteada se procede a instalar el firewall en el centro de software de Nethserver.

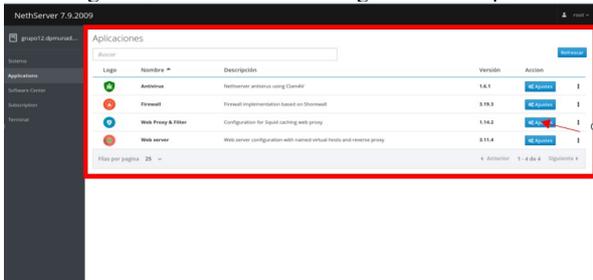
Figura 42. Instalación del firewall.



Fuente: Autoría propia.

Una vez instalado el servicio se procede con la validación de su instalación en la sección de aplicaciones.

Figura 43. Se accede a la configuración de Squid.



Fuente: Autoría propia.

Ahora se valida que la topología vaya de acuerdo a la interfaces que se implementarán desde el principio.

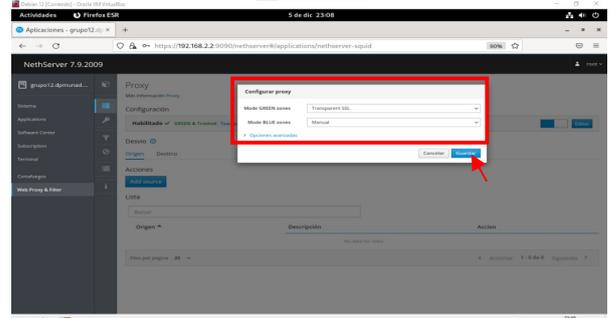
Figura 44. Se accede a la configuración de Squid.



Fuente: Autoría propia.

Se aplica la configuración del proxy web en modo transparente SSL y luego se configura el filtrado web, se aclara que al aplicar la configuración transparente, no será necesario configurar la IP y puerto del servicio en el navegador del cliente, ya que de esta manera conectaría directo contra el proxy.

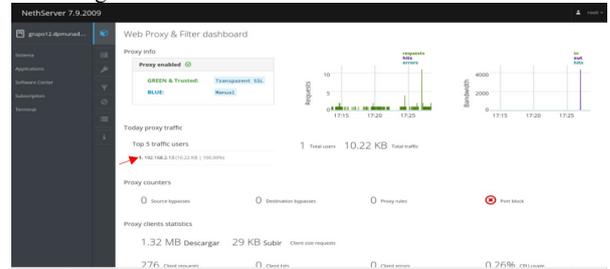
Figura 45. Se configura proxy en modo transparente.



Fuente: Autoría propia.

Ahora se evidencia que en el web proxy hay un cliente conectado al servidor con la IP 192.168.2.13

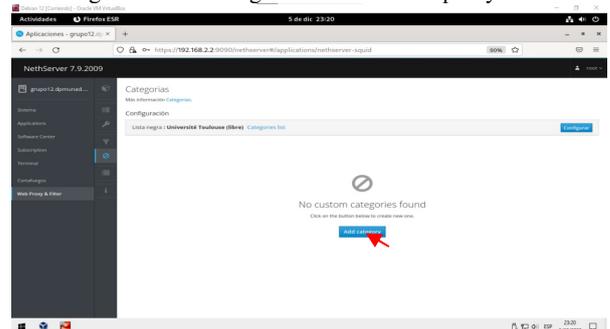
Figura 46. Se valida cliente activo en la red LAN.



Fuente: Autoría propia.

Al tener un cliente listo para enviar tráfico hacia el proxy, categorías por defecto, y en el cual no se cuenta con la restricción para sitios web de entretenimiento, por tal motivo añado una nueva categoría a través del botón denominado "Add Category".

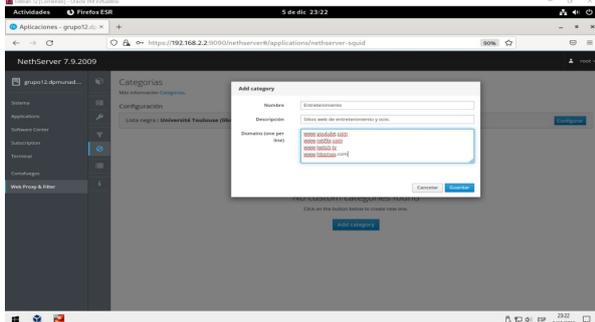
Figura 47. Se configura los filtros en el proxy web.



Fuente: Autoría propia.

A continuación se indica el nombre: Entretenimiento, se agrega una descripción si se desea y al final se agregan los sitios web que se desean restringir. Y luego se da clic en "Guardar".

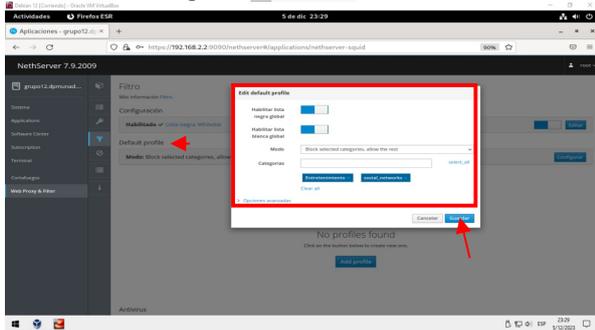
Figura 48. Añadir categoría.



Fuente: Autoría propia.

Luego se desplaza a la opción de filtro, en esta sección se puede configurar la restricción de las categorías y sitios web, se edita la opción “default profile” ya que esta opción permite agregar las categorías de los sitios web que pueden restringirse, en el caso se seleccionó “Entretenimiento” y “Social Networks” y guardó para continuar.

Figura 49. Añadir filtro web.



Fuente: Autoría propia.

Ahora se comprueba que se tenga conexión a internet.

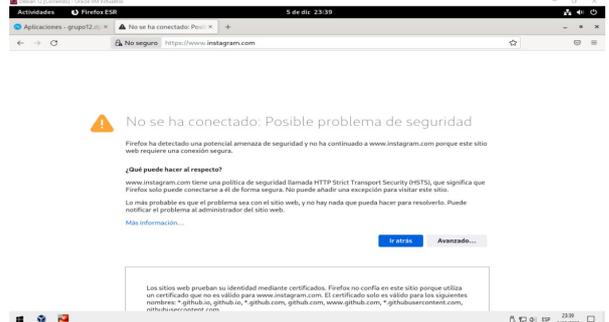
Figura 50. Conexión a internet.



Fuente: Autoría propia.

Ya que el internet funciona correctamente, se verifica el acceso a las páginas de entretenimiento y redes sociales.

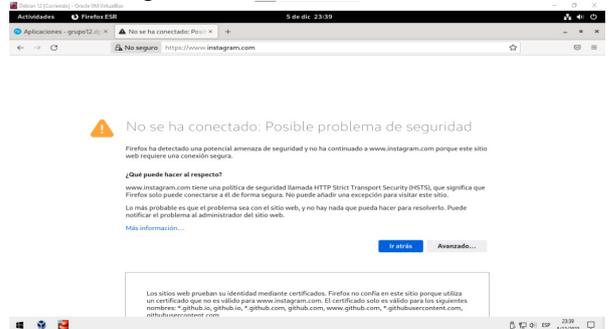
Figura 51. Restricción redes sociales.



Fuente: Autoría Propia.

Y para finalizar la verificación se comprueba el acceso a una página de entretenimiento.

Figura 52. Restricción entretenimiento.



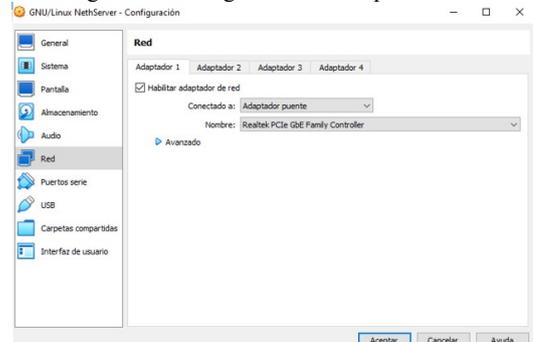
Fuente: Autoría propia.

## 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.

Lo primero en hacerse es configurar las tarjetas con las que trabajara el servidor, WAN, LAN Y DMZ.

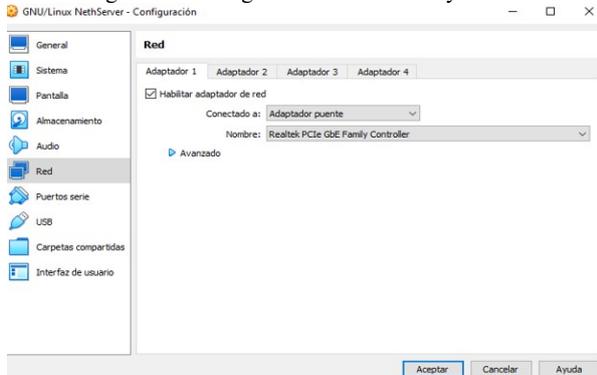
Figura 53. Configuración de nic para WAN.



Fuente: Autoría propia.

Ahora se configura las interfaces LAN Y DMZ en redes internas distintas.

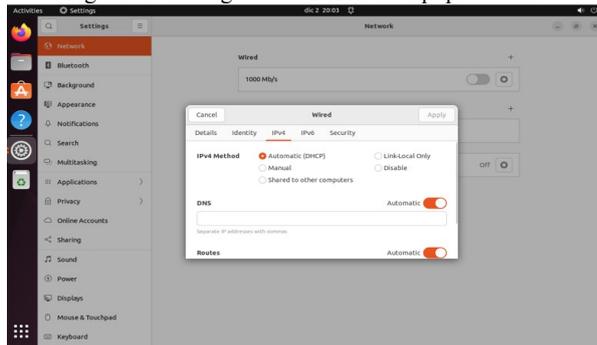
Figura 54. Configuración de nic LAN y DMZ.



Fuente: Autoría propia.

A continuación, se configura la red en DHCP en el equipo cliente que conecta la interfaz LAN.

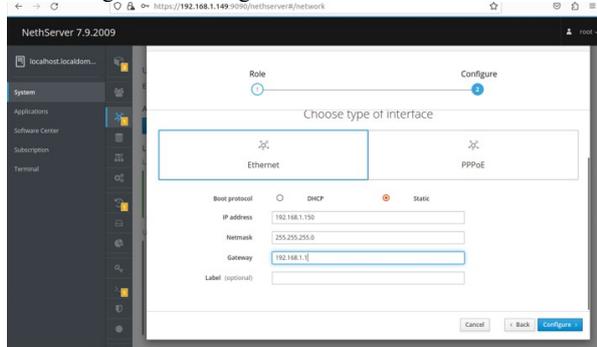
Figura 55. Configuración DHCP en equipo cliente.



Fuente: Autoría propia.

Ahora que el equipo cliente ya adquiere un direccionamiento IP bajo la red 192.168.1.0, se procede con la apertura de la página en la dirección 192.168.1.149:9090.

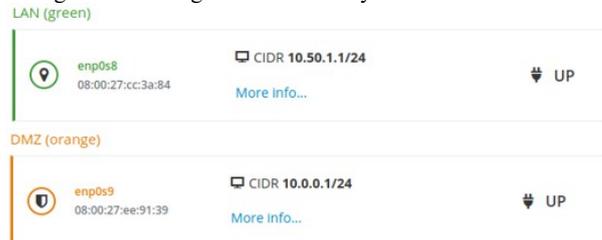
Figura 56. Configuración WAN en Nethserver.



Fuente: Autoría propia.

Ahora se procede con la configuración de las tarjetas de red LAN verde y DMZ naranja.

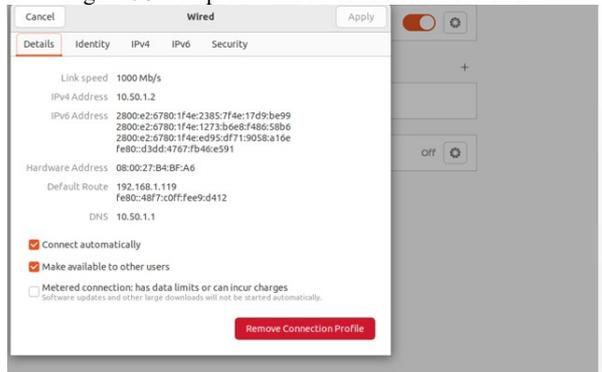
Figura 57. Configuración de LAN y DMZ en Nethserver.



Fuente: Autoría propia.

Se configura a un cliente de la red interna para que se conecte con IP estática a las interfaz lan verde.

Figura 58. comprobación de conexión de red LAN.



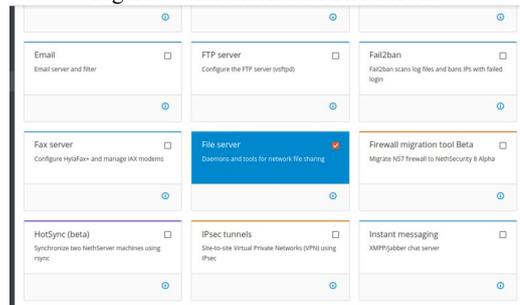
Fuente: Autoría propia.

Una vez comprobado que funcionan las conexiones, se procede a configurar el nethserver para establecer conexión por dominio LDAP y así compartir los archivos e impresoras.

Se procede a crear un grupo de usuario y un usuario, en el caso se creará el grupo file\_group\_server y el usuario ricardo.penilla. De la siguiente manera:

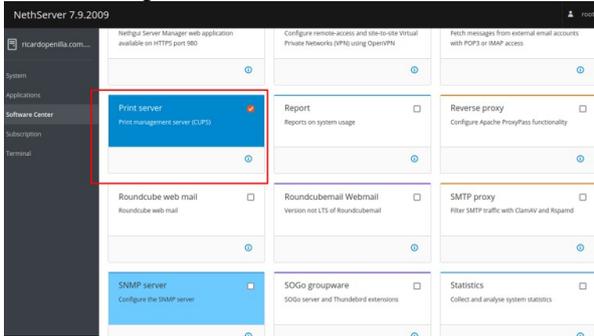
Primero se instala los paquetes requeridos para el file server y print server:

Figura 59. Instalación de File Server.



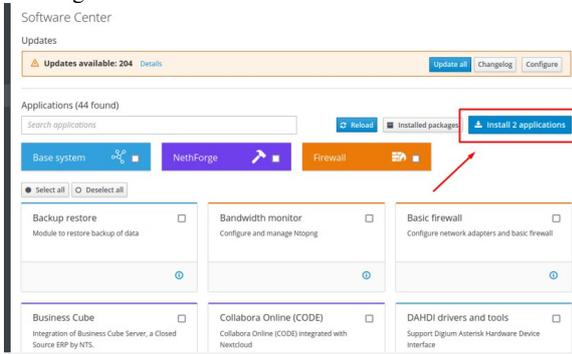
Fuente: Autoría propia.

Figura 60. Instalación de Print Server.



Fuente: Autoría propia.

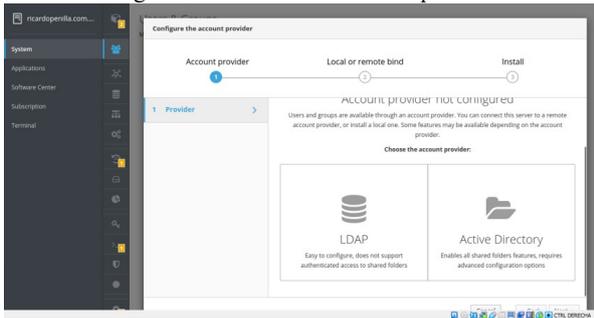
Figura 61. Se instala los dos servicios seleccionados.



Fuente: Autoría propia.

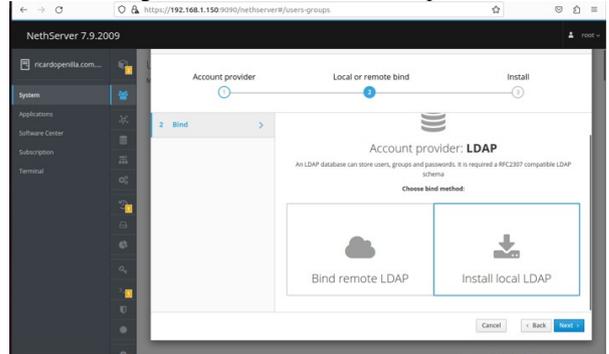
También se procede con la instalación de LDAP como se requiere en esta solución.

Figura 62. Instalación de LDAP paso 1.



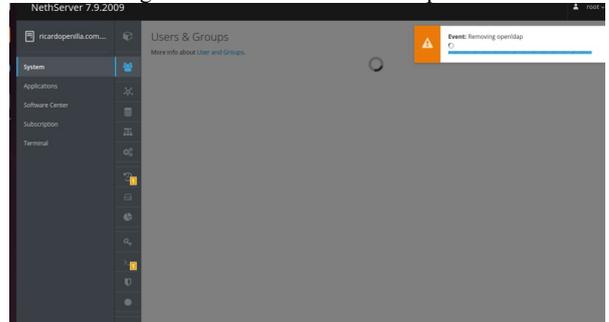
Fuente: Autoría propia.

Figura 63. Instalación de LDAP paso 2.



Fuente: Autoría propia.

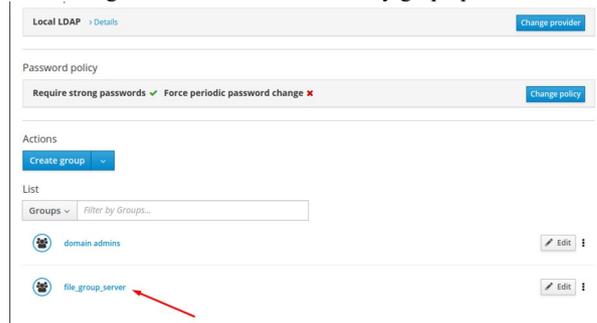
Figura 64. Instalación de LDAP paso 3.



Fuente: Autoría propia.

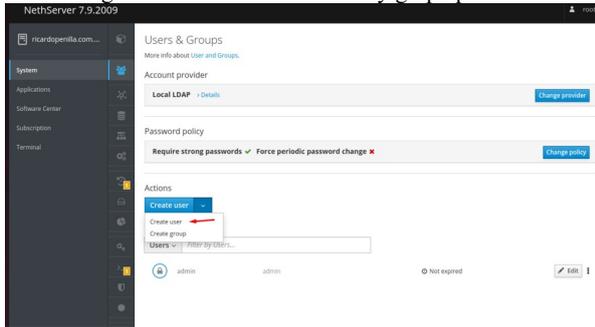
Para que LDAP funcione adecuadamente con la autenticación, se crea el usuario y el grupo, ya que con estos datos auténtica.

Figura 65. Creación de usuario y grupo paso 1.



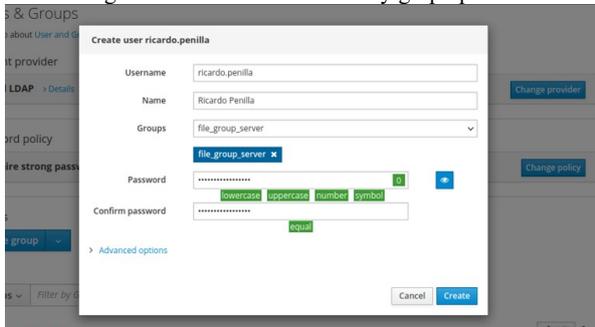
Fuente: Autoría propia.

Figura 66. Creación de usuario y grupo paso 2.



Fuente: Autoría propia.

Figura 67. Creación de usuario y grupo paso 3.

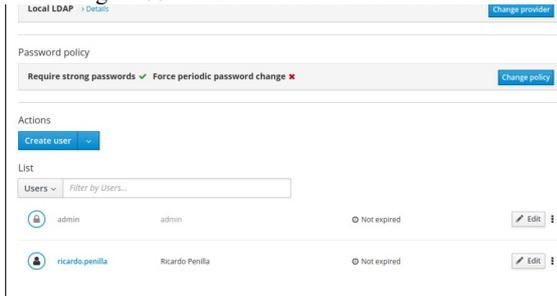


Fuente: Autoría propia.

Se procede con la creación de una carpeta compartida.

Una vez creado el usuario y grupo, se debe asegurar de que estos quedaron creados de manera adecuada.

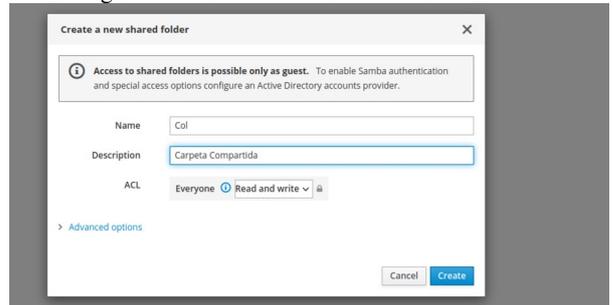
Figura 68. Validación del nuevo usuario creado.



Fuente: Autoría propia.

Ahora desde el LDAP, se crea una carpeta para que los clientes que estén en la red puedan accederla, para eso se debe poner el nombre y la descripción.

Figura 69. Validación del nuevo usuario creado.



Fuente: Autoría propia.

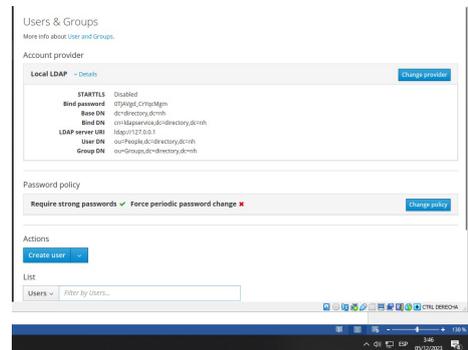
Figura 70. Creación de carpetas compartidas.



Fuente: Autoría propia.

Se revisa la información del LDAP.

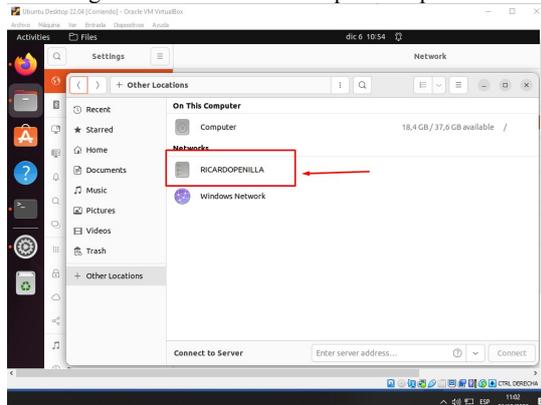
Figura 71. Validando detalles del LDAP.



Fuente: Autoría propia.

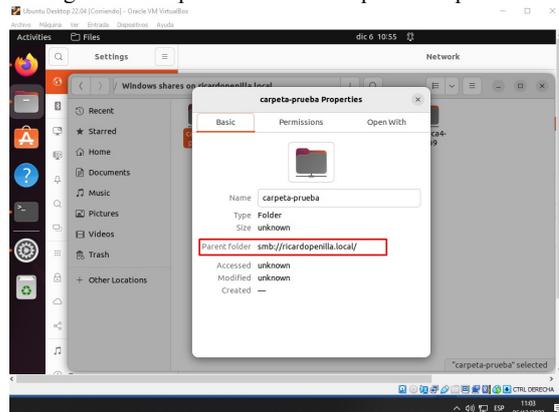
Ya una vez se tenga expuesto el LDAP compartido, se procede a probar desde el Ubuntu Cliente (Desktop)

Figura 72. Accediendo a carpeta compartida



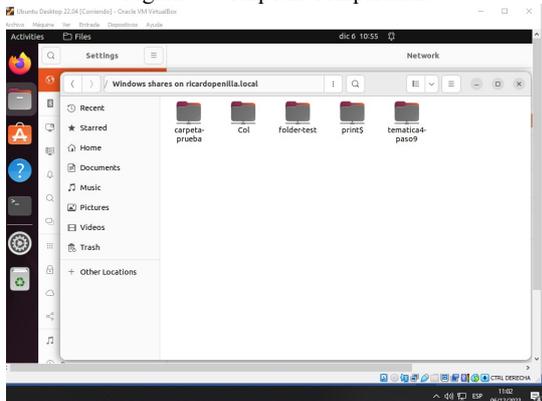
Fuente: Autoría propia

Figura 74. Propiedades de las Carpetas compartidas.



Fuente: Autoría propia

Figura 73. Carpetas compartidas.



Fuente: Autoría propia

Y se evidencia que efectivamente se tiene una carpeta compartida.

Además también se puede acceder a los servicios de las impresoras que estén agregadas y acceder. Con ello se verifica que las carpetas creadas se pueden acceder desde el cliente desktop.

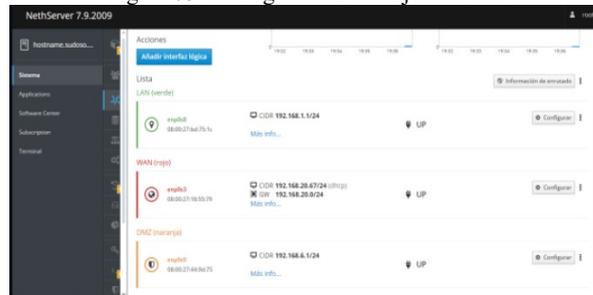
Todo esto da cuenta que en las propiedades de las carpetas se visualiza que la ruta es SMB.

## 2.5 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.

Para empezar, se procede con configuración de las tarjetas de red en Netserver, verde para LAN, roja para WAN y naranja para DMZ.

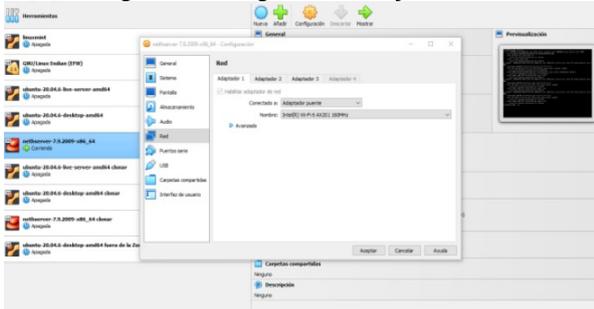
Figura 75. Configuración de tarjeta de red.



Fuente: Autoría propia.

De igual forma se procede con la configuración de estas tarjetas en las interfaces directas de la máquina virtual.

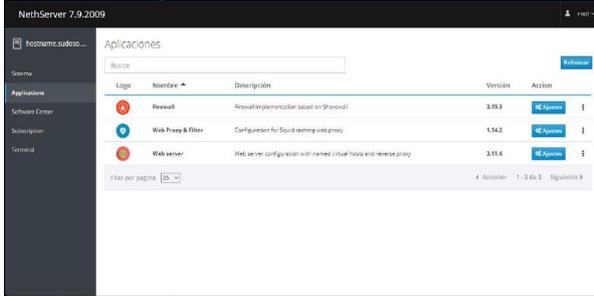
Figura 76. Configuración de tarjeta de red.



Fuente: Autoría propia.

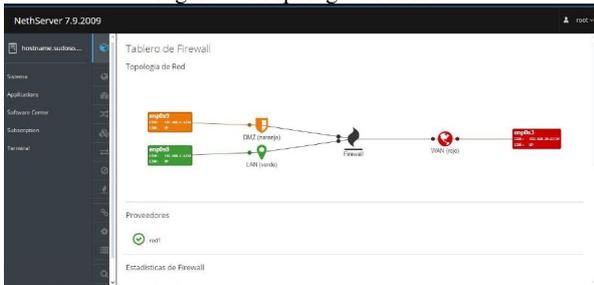
De acuerdo con lo configurado la interfaz LAN verde queda con el direccionamiento 192.168.1.1/24, la interfaz roja WAN con el direccionamiento 192.168.20.67/24 y la interfaz naranja DMZ con el direccionamiento 192.168.6.1/24, ahora se procede con la instalación de los servicios.

Figura 77. Instalación de servicios.



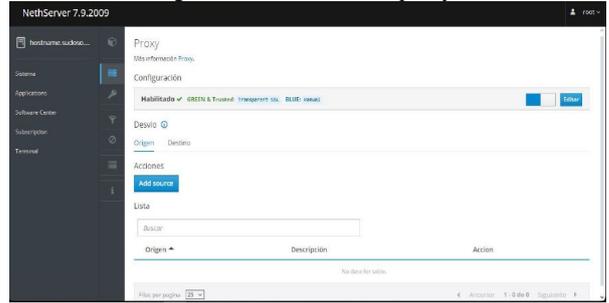
Fuente: Autoría propia.

Figura 78. Topología de la red.



Fuente: Autoría propia.

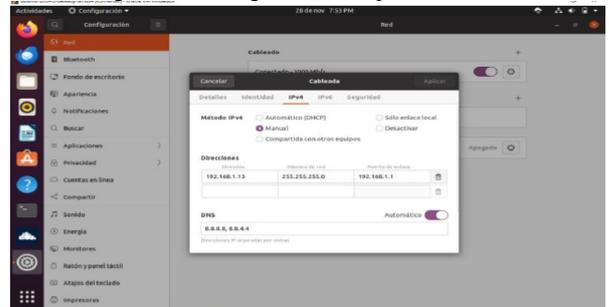
Figura 79. Activación del proxy.



Fuente: Autoría propia.

Ahora se valida la conectividad entre el equipo cliente Ubuntu y el servidor Nethserver.

Figura 80. Configuración IP fija en el cliente.



Fuente: Autoría propia.

Ahora que el equipo cliente tiene un dirección IP, se comprueba que la conectividad a internet a través del proxy este sin problemas.

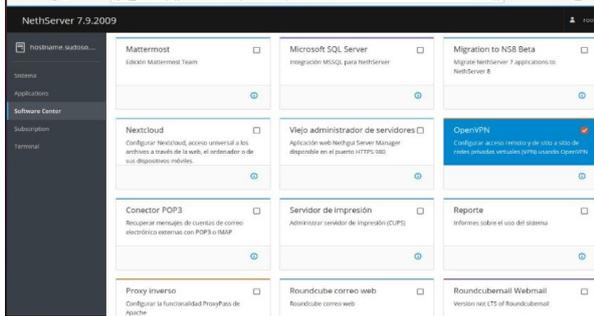
Figura 81. Navegador con conectividad a internet.



Fuente: Autoría propia.

A continuación se iniciara la instalación y configuración del servicio VPN.

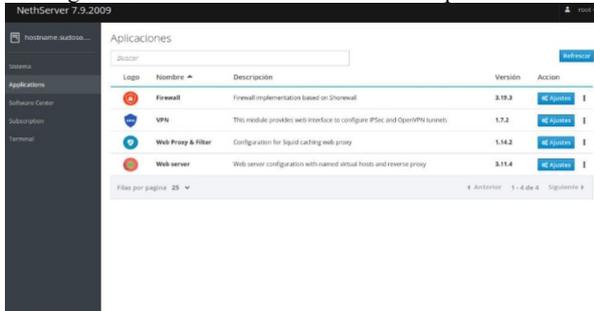
Figura 82. Instalación de VPN en el centro de software.



Fuente: Autoría propia.

Ahora se evidencia que el servicio VPN queda instalado en la sección de aplicaciones de Netserver.

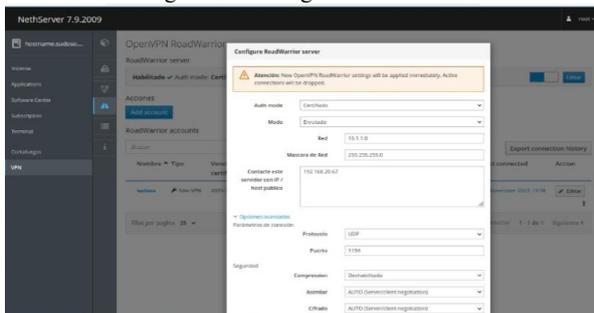
Figura 83. Servicio instalado de VPN en aplicaciones.



Fuente: Autoría propia.

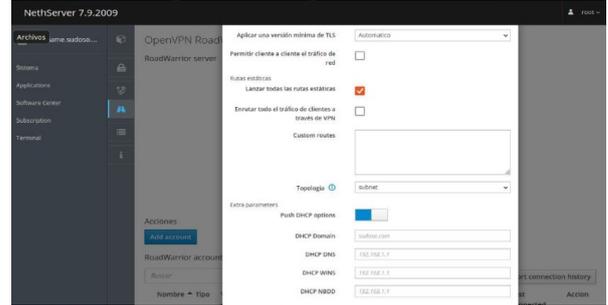
Ahora se procede con la configuración del servicio VPN.

Figura 84. Configurando la VPN.



Fuente: Autoría propia.

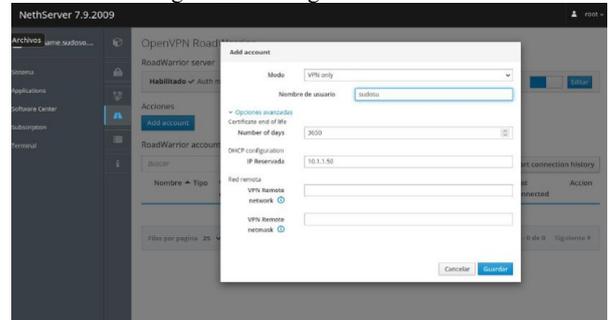
Figura 85. Configurando la VPN.



Fuente: Autoría propia.

Una vez aplicada las primeras configuraciones se procede con la creación de la cuenta,

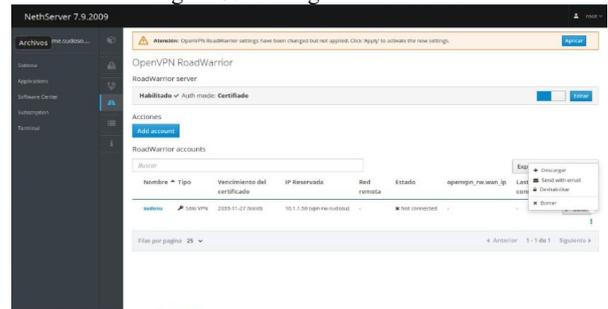
Figura 86. Configurando la VPN.



Fuente: Autoría propia.

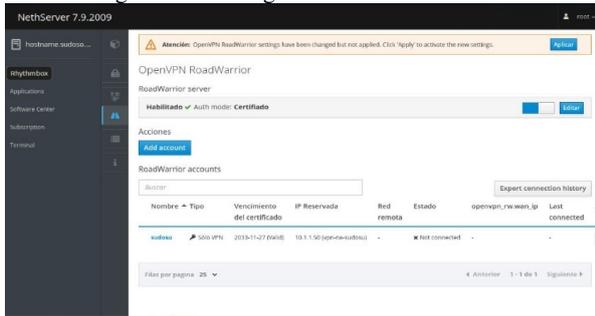
Para que un servidor VPN funcione de manera adecuada y segura se necesita de un certificado, el cual debe descargarse.

Figura 87. Configurando la VPN.



Fuente: Autoría propia.

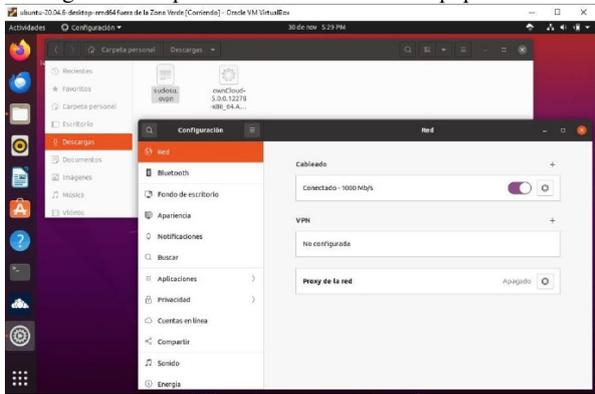
Figura 88. Descargando el certificado VPN.



Fuente: Autoría propia.

Una vez descargados los certificados en el servidor se procede a copiar estos mismos en el cliente linux que esta fuera de la zona verde.

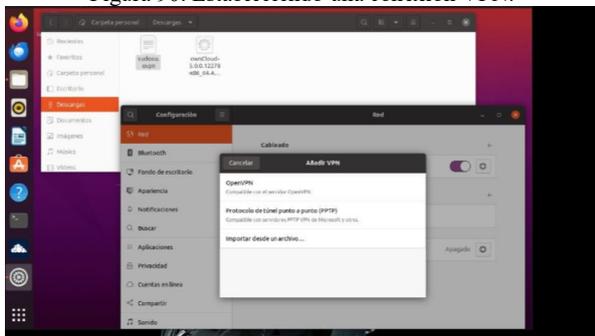
Figura 89. Copiando el certificado en el equipo cliente.



Fuente: Autoría propia.

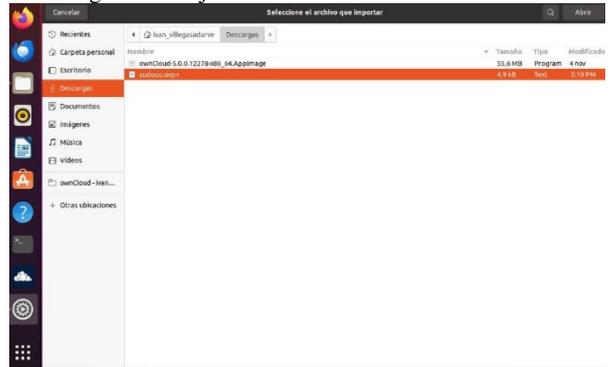
Ahora se tienen los insumos necesarios para realizar la conexión, así que desde el cliente linux se establece la conexión por vpn, al momento de hacerse, solicitará los certificados, los cuales deberán cargarse.

Figura 90. Estableciendo una conexión VPN.



Fuente: Autoría propia.

Figura 91. Adjuntándose certificado al enlace VPN.



Fuente: Autoría propia

Se valida la conexión VPN en el menu desplegable de la parte superior derecha.

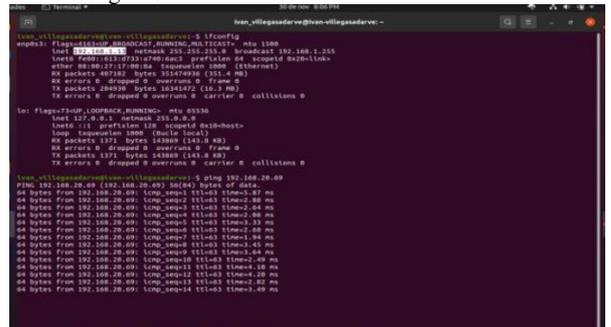
Figura 92. Validando conexión del tunel.



Fuente: Autoría propia.

Se valida que la IP de la zona verde del Netserver es la 192.168.1.13, mientras que la del desktop que esta por fuera de la zona verde tiene la IP 192.168.20.69, estas tienen conexión gracias a tunel VPN.

Figura 93. Validando conexión desde el cliente.



Fuente: Autoría propia.

