IMPLEMENTACIÓN AVANZADA DE SERVICIOS DE INFRAESTRUCTURA IT EN GNU/LINUX: UN ENFOQUE INTEGRAL HACIA LA ADMINISTRACIÓN Y CONTROL DE NETHSERVER

Nicolás Rivas Díaz
e-mail: nrivasd@unadvirtual.edu.co
David Aníbal Vásquez Beltrán
e-mail: davasquezb@unadvirtual.edu.co
Wilson Possos Piñeros
e-mail: wpossosp@unadvirtual.edu.co
Ricardo López Gómez
e-mail: rlopezgome@unadvirtual.edu.co
Leidy Viviana Quintero Saavedra
e-mail: lvquinteros@unadvirtual.edu.co

RESUMEN: *El presente artículo documenta la implementación detallada de servicios avanzados en infraestructura IT utilizando GNU/Linux y Nethserver. Se describe el proceso completo, desde la instalación inicial hasta la configuración y pruebas exhaustivas de servicios clave, como DHCP, DNS, Proxy, Cortafuegos, File Server, Print Server y VPN. Cada paso se ejecutó con precisión, aplicando conocimientos previos, y se realizaron pruebas rigurosas para validar el correcto funcionamiento. Los resultados revelan una administración eficiente y control robusto de la infraestructura IT en entornos complejos basados en GNU/Linux. Este enfoque práctico proporciona una guía integral y significativa para implementar servicios avanzados con Nethserver en entornos de red.*

PALABRAS CLAVE: Infraestructura IT, GNU/Linux, Nethserver.

1 INTRODUCCIÓN

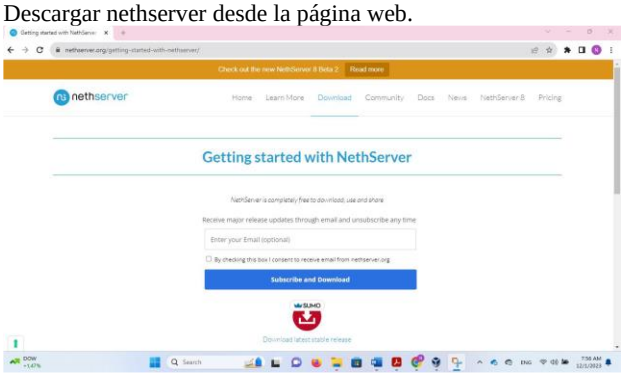
En el ámbito actual de la administración de infraestructura IT, la implementación eficiente de servicios avanzados en entornos GNU/Linux se ha vuelto esencial. Este artículo detalla un enfoque integral basado en Nethserver, una distribución de GNU/Linux centrada en la administración y control de servicios. A lo largo de este informe, exploraremos la implementación paso a paso de servicios clave, como DHCP, DNS, Proxy, Cortafuegos, File Server, Print Server y VPN. Cada proceso se ha llevado a cabo meticulosamente, aplicando conocimientos previos y sometiendo cada implementación a pruebas exhaustivas. Estas prácticas se centran en ofrecer una guía detallada para la administración avanzada de servicios en entornos complejos basados en GNU/Linux, destacando la importancia de una infraestructura IT robusta y eficaz.

2 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

2.1 INSTALACIÓN NETHSERVER

Inicialmente se procede con la descarga del nethserver; el cual es una distribución para servidores basado en Linux. Lo primero es acceder a la página oficial y desde allí realizar la descarga de la imagen ISO.

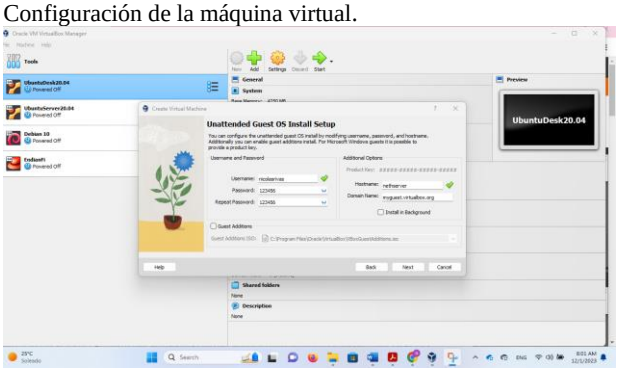
Figura 1
Descargar nethserver desde la página web.



Fuente: Página oficial nethserver

Se realiza la configuración inicial con ayuda de la ISO descargada en el paso anterior; con esta creamos la máquina virtual.

Figura 2
Configuración de la máquina virtual.



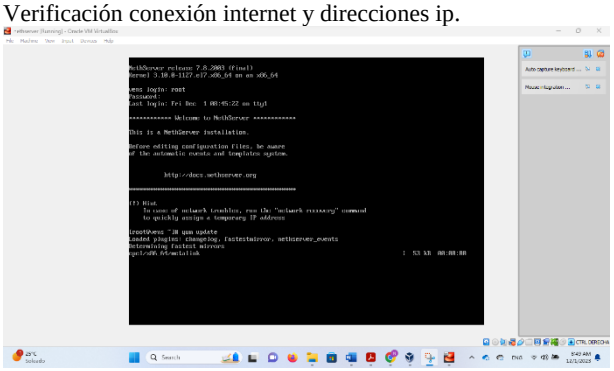
Fuente: Elaboración propia

Luego de configurar la máquina virtual y configurar la hora, fecha, zona horaria, idioma del teclado y las terminales se procede a verificar que tenga acceso a internet. En este caso se verifica con el comando ping e ip a. Estos se usan para verificar conexión y las ip del sistema respectivamente.

Figura 3
Configuración nethserver en interfaz gráfica.

Fuente: Elaboración propia

Figura 4
Verificación conexión internet y direcciones ip.



Fuente: Elaboración propia

Ahora se accede al panel de control en el que ingresan las credenciales de contraseña y usuario, esto se debe realizar en el equipo cliente o desktop seleccionado; para este caso se trabajara bajo la distribución Ubuntu 20.04 y por medio del navegador se accede a nethserver directamente con la ip configurada. La dirección usada para este caso es 192.168.1.24.

Luego, se debe realizar la configuración del nombre del servidor, el cual se denominó vens.drivemeca.com. También se coloca como puerto SSH el 2222 por temas de seguridad, y, finalmente, se deben verificar los puertos. Todas estas configuraciones se pueden verificar en el dashboard del nethserver.

Figura 5
Verificación configuraciones del servidor

Fuente: Elaboración propia

2.2 Temática 1: DHCP Server, DNS Server y Controlador de Dominio

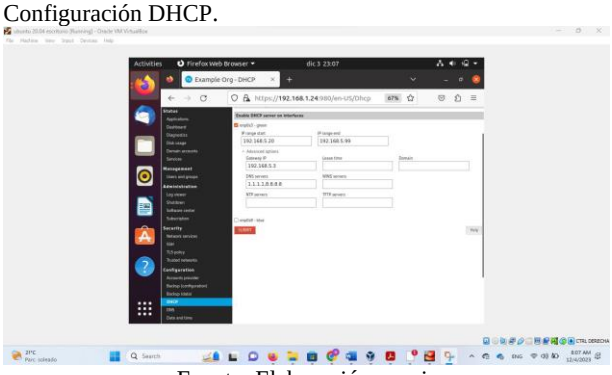
En primera instancia se ingresa a nethserver y se evidencia que no está habilitado el DHCP server y DNS server como se observa en la siguiente figura.

Figura 6
Verificación de configuración DHCP y DNS.

Fuente: Elaboración propia

Para configurarlo se debe ir a la ficha DHCP, la cual muestra 2 tarjetas y es necesario seleccionar cual será la DHCP, para este caso se opta por la verde (Green) y se configura el rango deseado de las IP.

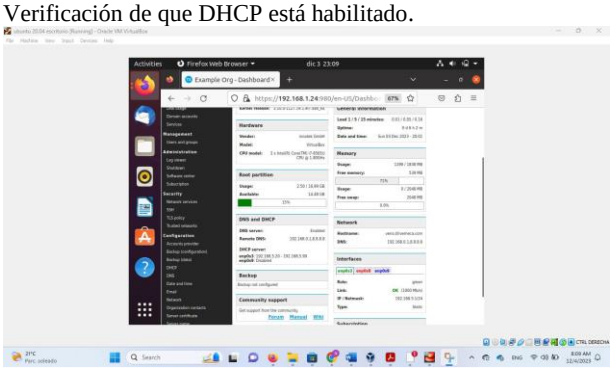
Figura 7
Configuración DHCP.



Fuente: Elaboración propia

A continuación, se valida en el dashboard que ya está habilitado DHCP Server.

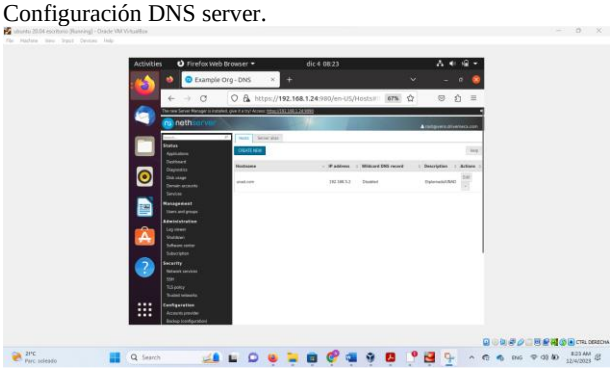
Figura 8
Verificación de que DHCP está habilitado.



Fuente: Elaboración propia

Ahora, se procede a configurar el DNS server como se ve en la siguiente figura.

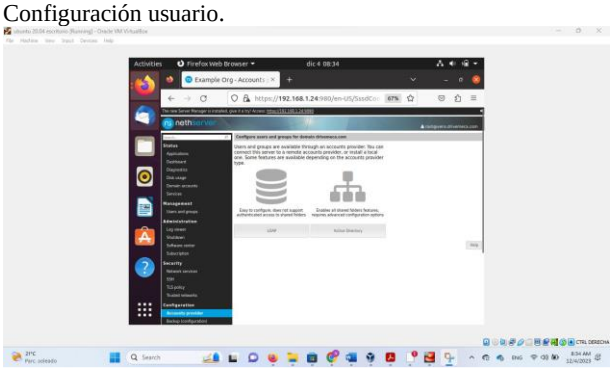
Figura 9
Configuración DNS server.



Fuente: Elaboración propia

El siguiente paso es configurar los usuarios y grupos como es solicitado en la guía, en la siguiente imagen se puede ver dicha configuración.

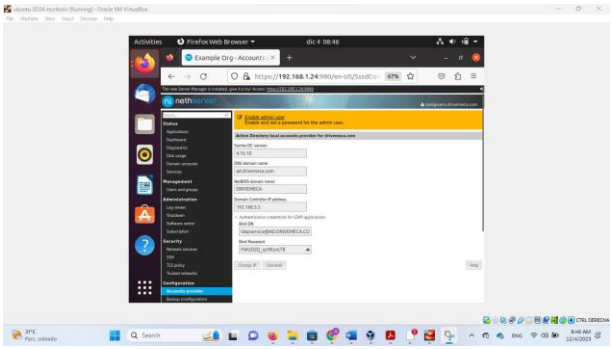
Figura 10
Configuración usuario.



Fuente: Elaboración propia

Se procede con la activación del directorio, con la finalidad de poder configurar los usuarios.

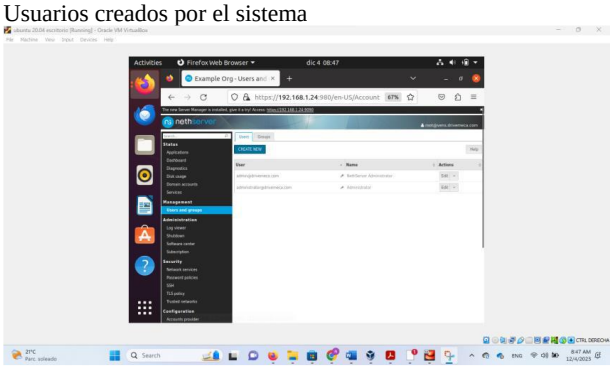
Figura 11
Activación del directorio



Fuente: Elaboración propia

Se validan los usuarios creados por el sistema, los cuales serían admin y administrador respectivamente.

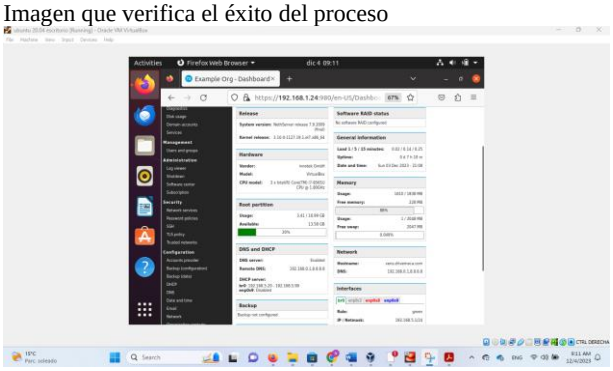
Figura 12 .
Usuarios creados por el sistema



Fuente: Elaboración propia

Finalmente, se valida que se tenga activado el DNS y DHCP, así como la creación de la interfaz br0; lo que indica que todo quedo bien.

Figura 13.
Imagen que verifica el éxito del proceso



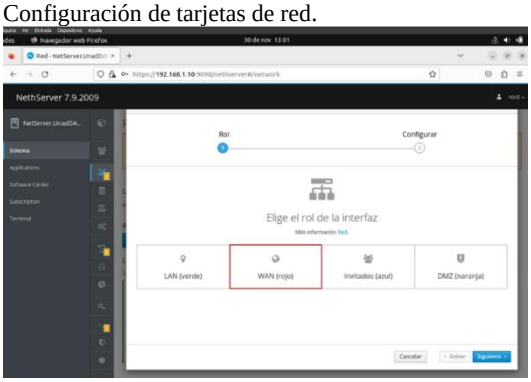
Fuente: Elaboración propia

3 Temática 2: PROXY

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.

Se procede a ingresar a la configuración de red en donde se evidencia que las dos tarjetas se encuentran definidas como LAN, por ende, se cambia el color de la tarjeta enp0s3 a WAN.

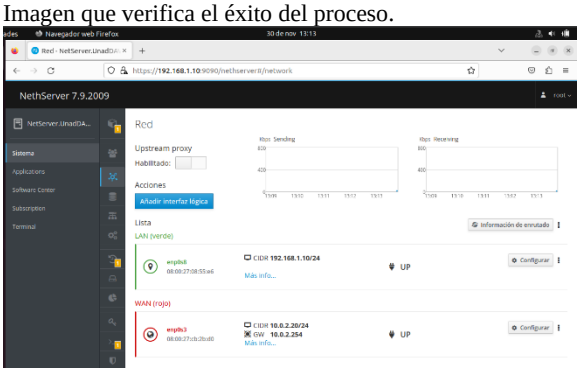
Figura 14
Configuración de tarjetas de red.



Fuente: Elaboración propia

Con ello, se puede observar que ya se encuentran correctamente configuradas las redes LAN y WAN.

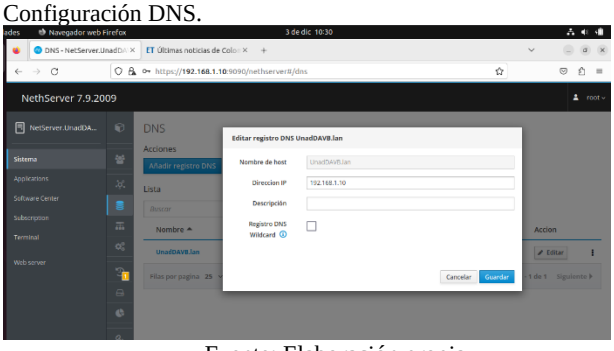
Figura 15
Imagen que verifica el éxito del proceso.



Fuente: Elaboración propia

Ahora en la opción de DNS se añade un nuevo registro y se procede a definir el nombre de host con el mismo dominio otorgado previamente y la dirección ip del servidor Nethserver.

Figura 16
Configuración DNS.



Fuente: Elaboración propia

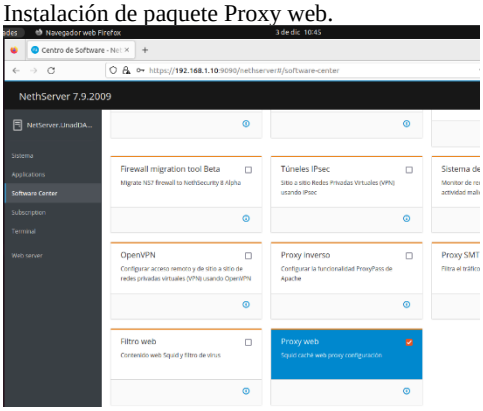
Luego, al ingresar al menú lateral en la opción de Software Center se procede a instalar el paquete de nombre “Firewall básico”.

Figura 17
Instalación del paquete de aplicación

Fuente: Elaboración propia

De la misma forma se procede a instalar el paquete de proxy web.

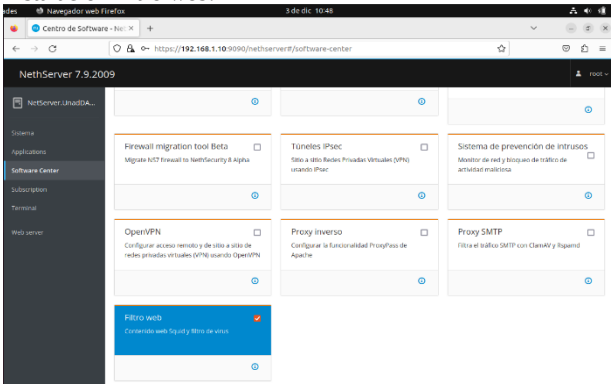
Figura 18
Instalación de paquete Proxy web.



Fuente: Elaboración propia

Finalmente, se realiza el mismo procedimiento para instalar el filtro web.

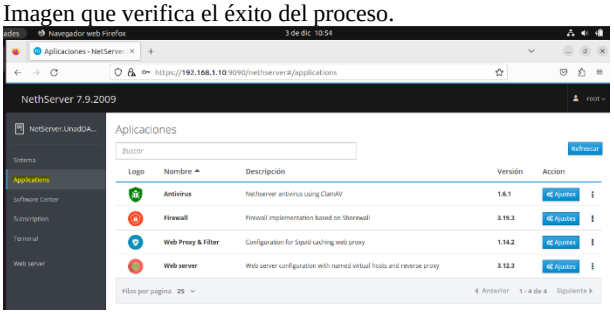
Figura 19
Instalación filtro web.



Fuente: Elaboración propia

Se puede evidenciar que, al ingresar al apartado de aplicaciones, ya se encuentran instalados estos paquetes de aplicación.

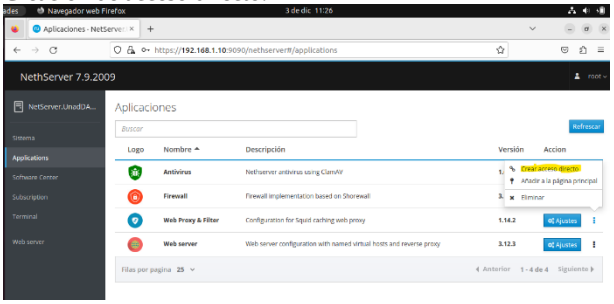
Figura 20
Imagen que verifica el éxito del proceso.



Fuente: Elaboración propia

Ahora se procede a configurar el proxy, por lo tanto, se ingresa a la opción Web Proxy Filter, creando un acceso directo el cual se mostrará en la parte del menú de navegación.

Figura 21
Creación de acceso directo.



Fuente: Elaboración propia

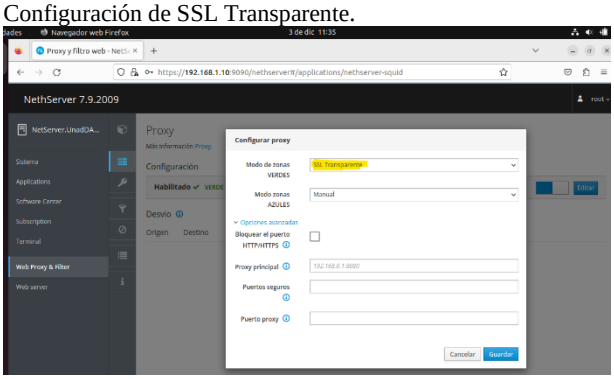
Al ingresar en la opción de Web Proxy & Filters, se observa que este se encuentra deshabilitado, por ende, se inicia el proceso de configuración desde la opción "Configurar proxy".

Figura 22
Configuración de proxy.

Fuente: Elaboración propia

A continuación, en el modo de zonas verdes se elige el "SSL Transparente" el cual se escucha por el puerto 3128.

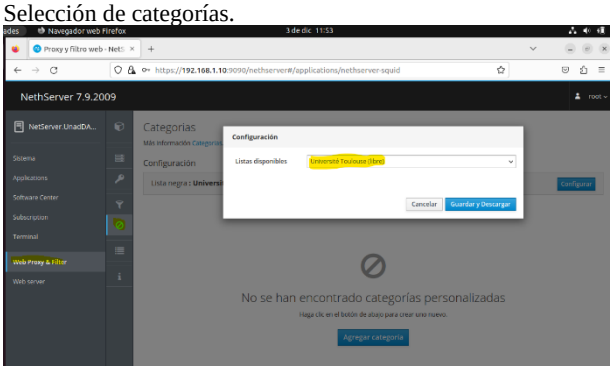
Figura 23
Configuración de SSL Transparente.



Fuente: Elaboración propia

A continuación, se ingresa al apartado de categorías y se selecciona la lista "Université Toulouse (libre)", la cual viene por defecto y contiene categorías de páginas web, por lo que se oprime en guardar y descargar para continuar.

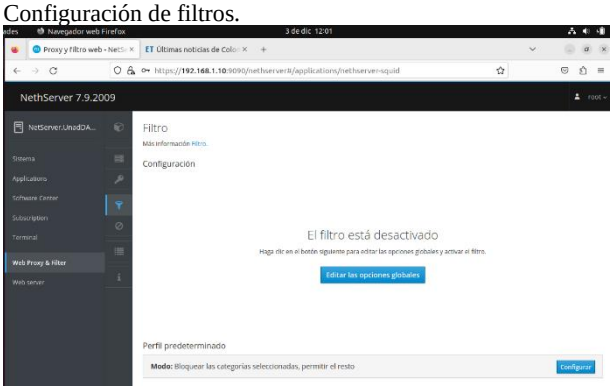
Figura 24
Selección de categorías.



Fuente: Elaboración propia

Ahora se procede a ingresar al aparatado de filtro en donde se observa que se encuentra desactivado, por lo cual se inicia su configuración desde la opción de "Editar as opciones globales".

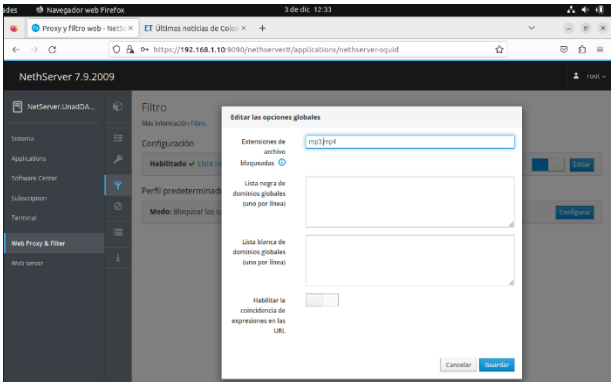
Figura 25
Configuración de filtros.



Fuente: Elaboración propia

Seguido a esto, se agregan las extensiones de archivo a bloquear, en este caso se coloca mp3 y mp4, las cuales pertenecen a formato de video.

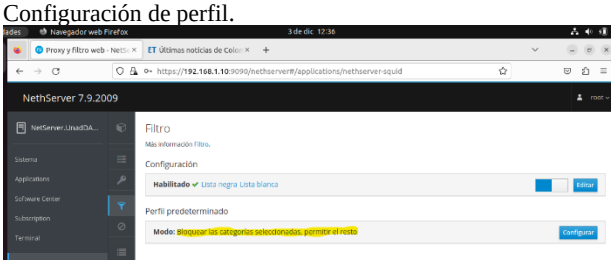
Figura 26
Selección de extensión de archivos.



Fuente: Elaboración propia

Ahora se procede a configurar el perfil determinado el cual como se observa indica que bloqueará todas las categorías seleccionadas y permitirá el resto.

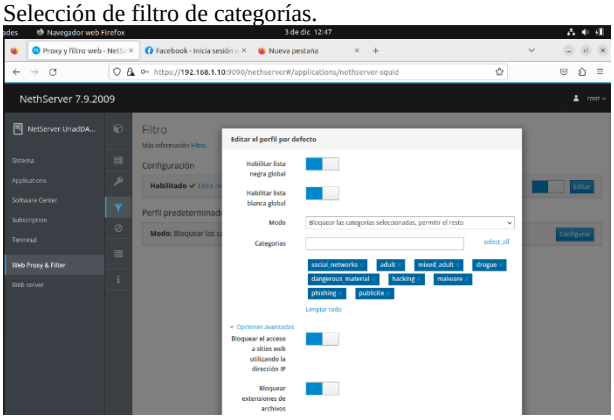
Figura 27
Configuración de perfil.



Fuente: Elaboración propia

A continuación, se elige el modo “bloquear las categorías seleccionadas y permitir el resto”, con el fin de definir cuáles son las categorías a las cuales no se podrá acceder mediante el filtrado de proxy, en este caso, se eligen 9 categorías entre las cuales se encuentran algunas como redes sociales, contenido para adultos, hacking, entre otras.

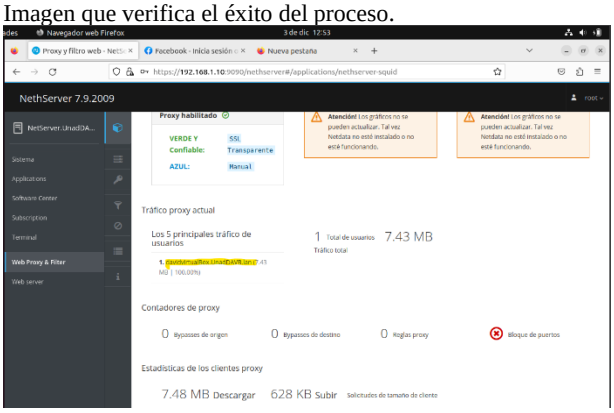
Figura 28
Selección de filtro de categorías.



Fuente: Elaboración propia

Luego de esto, al regresar a el panel de control del web proxy se puede evidenciar que el equipo desktop ya se está filtrando dentro la configuración establecida.

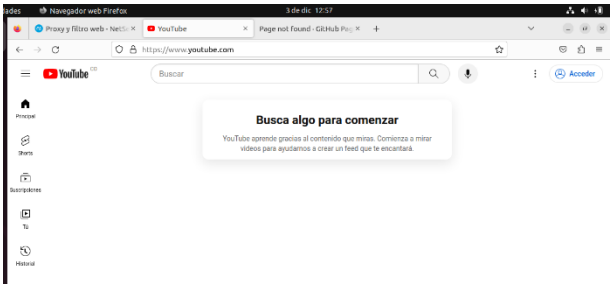
Figura 29
Imagen que verifica el éxito del proceso.



Fuente: Elaboración propia

A continuación, se procede a realizar una última validación en donde se evidencia que al ingresar a www.youtube.com, esta web no muestra videos ya que previamente se bloqueó este tipo de formatos de archivo y tampoco muestra algún tipo publicidad.

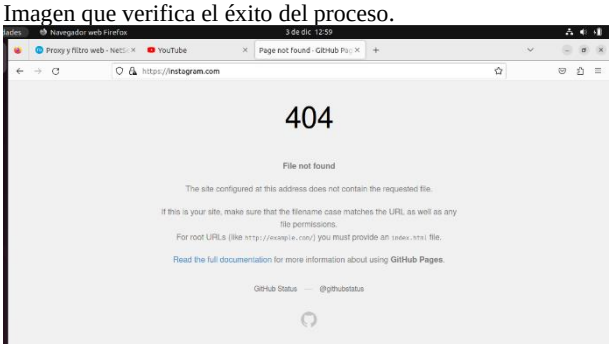
Figura 30
Validación de filtrado web.



Fuente: Elaboración propia

Finalmente, si se quiere ingresar a una red social como lo es Instagram, se observa que su acceso se encuentra bloqueado por las políticas establecidas en el web proxy.

Figura 31
Imagen que verifica el éxito del proceso.



Fuente: Elaboración propia

4 Temática 3: CORTAFUEGOS

Esta temática busca brindar seguridad de la información local, así como restringir el acceso a sitios web específicos bajo unas reglas de seguridad.

Por lo tanto, para implementar y configurar un firewall usando el sistema operativo Nethserver y lograr restringir la apertura de portales o sitios web de entretenimiento, así como redes sociales se requiere la realización de los siguientes pasos:

Primero, se debe crear una nueva máquina usando VirtualBox, como se evidenció anteriormente y en la cual se instalará el sistema operativo Nethserver.

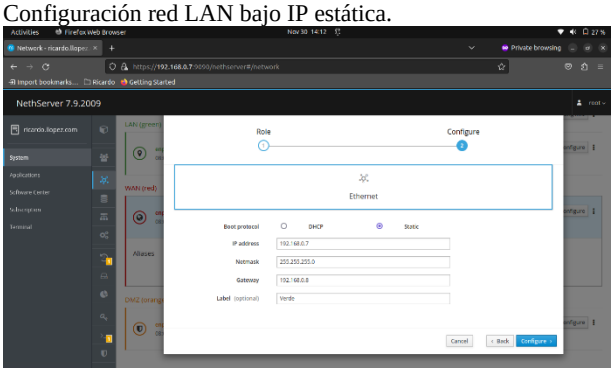
Después es necesario configurar cada una de las redes, LAN, WAN, DMZ así:

Figura 32
Configuración de red WAN bajo protocolo DHCP.

Fuente: Elaboración propia

Para esta configuración solamente se requiere la selección de DHCP y editar el label en rojo.

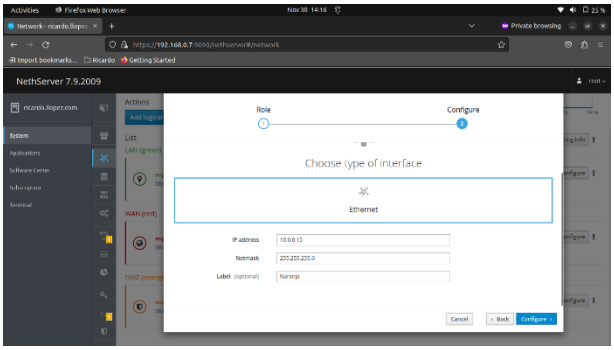
Figura 33
Configuración red LAN bajo IP estática.



Fuente: Elaboración propia

Para esta configuración se requiere que la IP sea estática y el label este en verde.

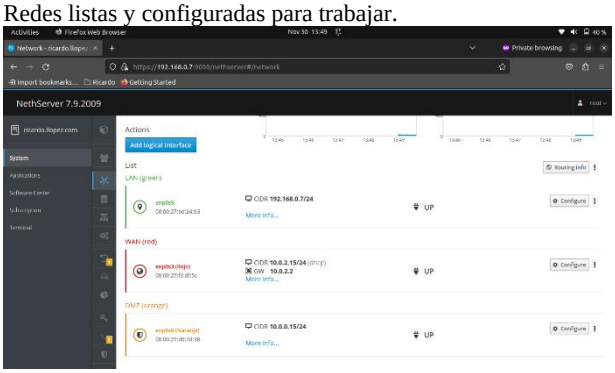
Figura 34
Configuración red DMZ bajo IP privada.



Fuente: Elaboración propia

Para esta configuración se asigna la red privada por defecto con router funcionando y se define el label como naranja.

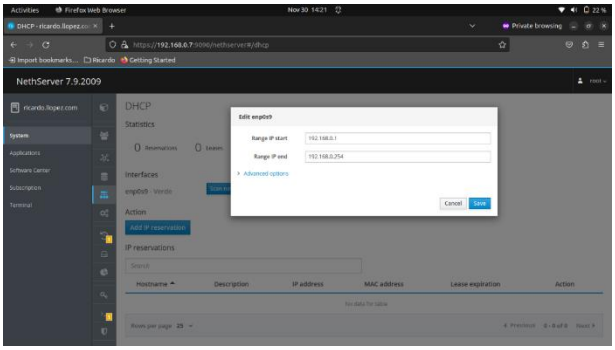
Figura 35
Redes listas y configuradas para trabajar.



Fuente: Elaboración propia

Al realizar la configuración correcta, se puede continuar con la instalación del firewall, y para ello es necesario verificar el rango de direcciones IP para asegurar que todo esté funcionando.

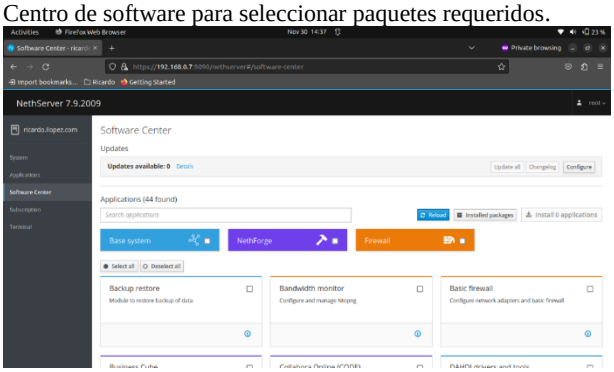
Figura 36
Validación del rango de direcciones IPs para iniciar a trabajar con el Firewall.



Fuente: Elaboración propia

Una vez realizado esto, se procede a instalar el firewall Shorewall desde el centro de software. Este es el punto medular de la temática

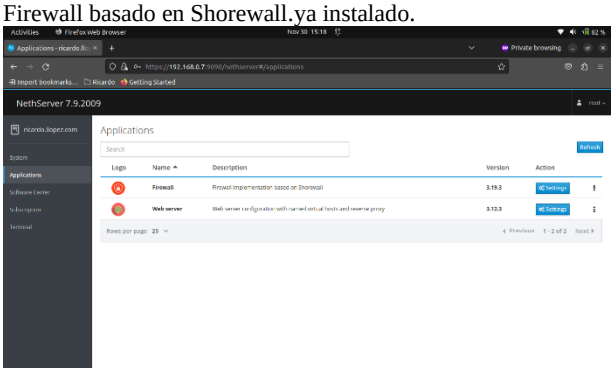
Figura 37
Centro de software para seleccionar paquetes requeridos.



Fuente: Elaboración propia

Para la búsqueda se filtra por la palabra clave Firewal y se da clic en instalar.

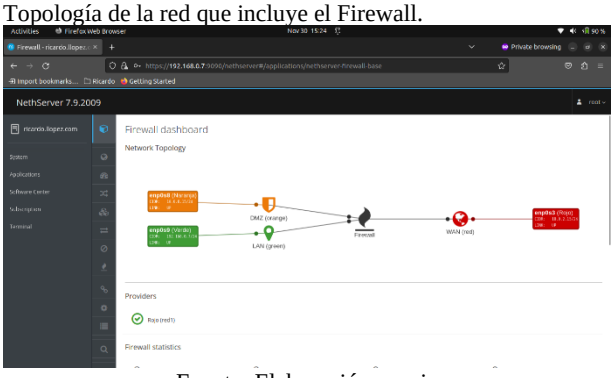
Figura 38
Firewall basado en Shorewall,ya instalado.



Fuente: Elaboración propia

Ahora se procede a verificar que la red incluye el cortafuegos; esto se puede evidenciar en la topología de red.

Figura 39
Topología de la red que incluye el Firewall.



Fuente: Elaboración propia

Una vez se ha corroborado e instalado el paquete necesario se procede a comprobar que el equipo cliente cuenta con acceso normal a cualquier red social; para este caso se eligió la red social Instagram.

Figura 40
Ingreso exitoso y sin restricción al sitio web de Instagram.

Fuente: Elaboración propia

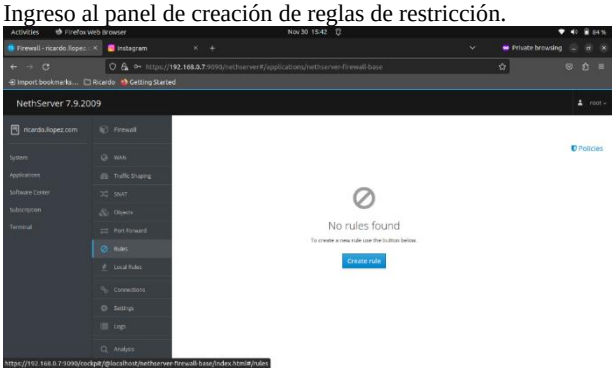
Se verifica por terminal cuál es la dirección IP correspondiente a Instagram a través del comando ping. Esto debido a que se requiere para una posterior asignación de las reglas de seguridad.

Figura 41
Verificación de la IP de Instagram a través de la terminal

Fuente: Elaboración propia

Una vez hecho esto, se procede a crear las reglas de restricción con el fin de denegar el acceso a la red social de Instagram. Esto se hace desde el ítem Firewall en el menú Rules.

Figura 41
Ingreso al panel de creación de reglas de restricción.

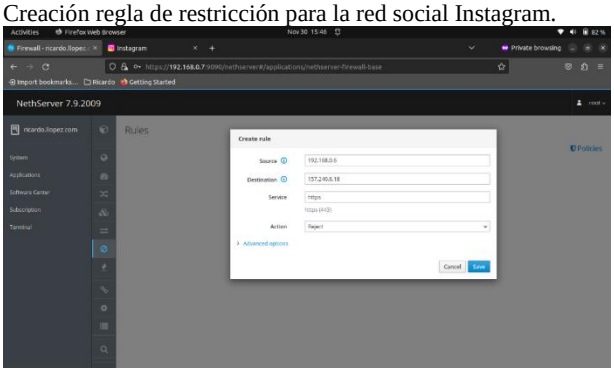


Fuente: Elaboración propia

Teniendo las direcciones IP definidas se colocan en los campos de fuente y destino respectivamente y se establece la

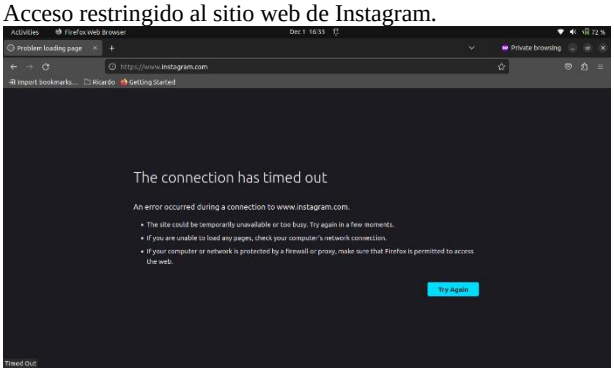
regla Reject (rechazar); esto permite que no sea posible usar la red social de Instagram.

Figura 42
Creación regla de restricción para la red social Instagram.



Fuente: Elaboración propia

Después de crear esta regla, se ingresa nuevamente al sitio web con el fin de corroborar si la restricción es correcta.
Figura 43
Acceso restringido al sitio web de Instagram.



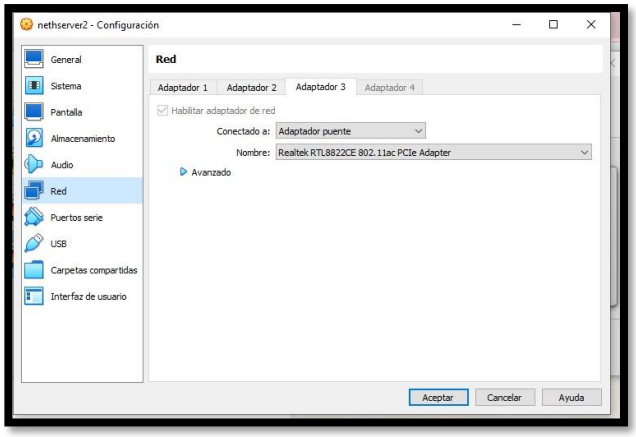
Fuente: Elaboración propia

Finalmente, se puede evidenciar que el firewall o cortafuegos basado en Shorewall está funcionando acorde con las reglas establecidas. El mismo proceso se debe llevar a cabo si se desea restringir el acceso a cualquier sitio web que se desee en la red especifica de trabajo, de esta manera, se podrá contar con un mayor control y seguridad de la información.

5 Temática 4 File server y Print server

En esta temática se demuestra el cómo a través del controlador de dominio LDAP permite el acceso de una estación de trabajo GNU/LINUX a los servicios de impresoras y archivos compartidos. Se debe realizar primero la instalación de Nethserver, desde la máquina virtual se procede a instalar y en la sección de red en el adaptador uno se configura como red interna verde con el fin de tener una conexión Ubuntu. En el adaptador dos se colocará red interna como “naranja”, En el adaptador tres se deja adaptador puente

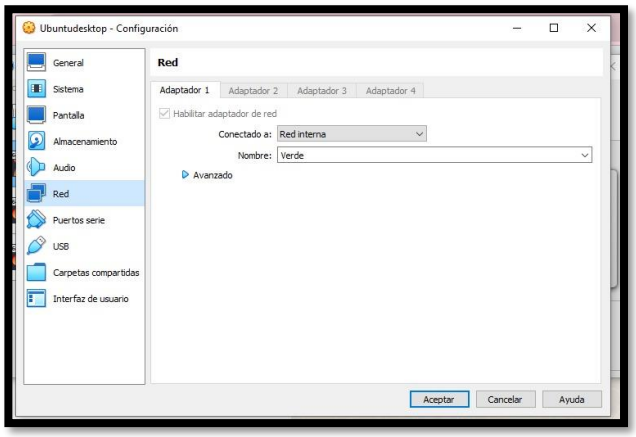
Figura 44
Configuración de red Nethserver.



Fuente: Elaboración propia

En Ubuntu en la configuración de la red se deja red interna como “verde” para la conexión con Nethserver

Figura 45
Configuración de red Ubuntu.



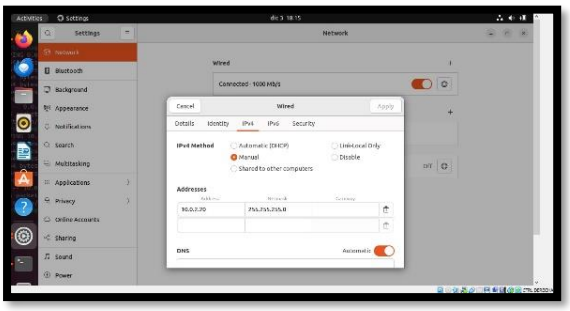
Fuente: Elaboración propia

Se procede a realizar ping 0.0.0.0 para verificar que tiene red, se ingresa la “ip a” para ver las ips de las conexiones, tal como se ve a continuación.
Figura 46

Luego al ingresar a Ubuntu se revisa la Ip Se procede a realizar la modificación de la ip cambiando el último número en base a enp0s8.

Figura 47

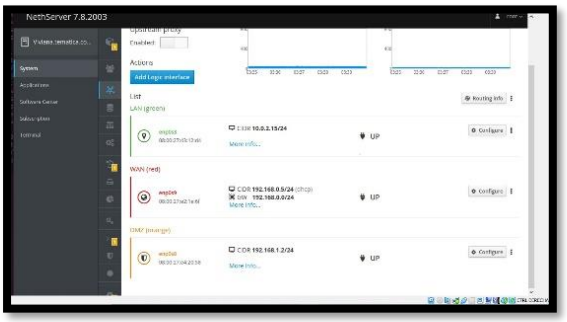
Configuración de red Ubuntu.



Fuente: Elaboración propia

Luego al ingresar a Ubuntu en Firefox se ingresa la ip de enp0s3 más el puerto 9090 con el fin de poder tener acceso al Nethserver, al realizarlo se procede a configurar la red en system, con LAN, WAN y DMZ respectivamente.

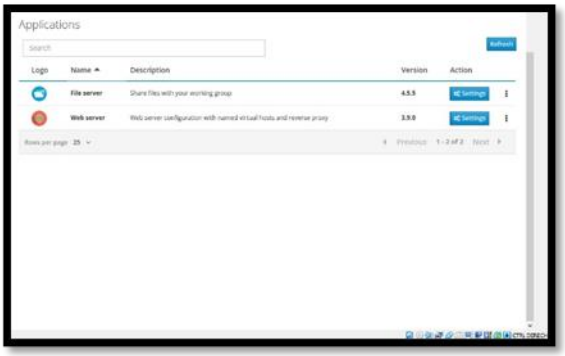
Figura 48
Configuración de red Ubuntu



Fuente: Elaboración propia

En la terminal se confirma si tiene conexión entre Ubuntu y Nethserver luego se procede a realizar las instalaciones de paquetes, para esto se usa el filtro de Base system y desde allí se instala File server y Print Server.

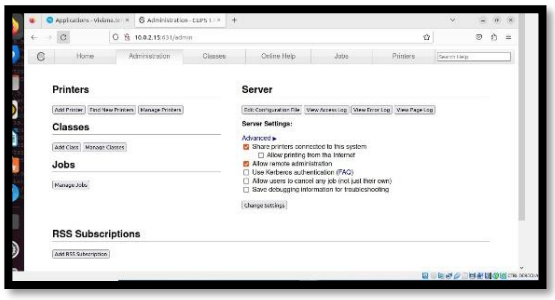
Figura 49
Instalación de FileServer y PrintServer



Fuente: Elaboración propia

Luego se verifica que el servicio de impresora esté disponible ingresando la IP 10.0.2.15 por el puerto 631 y se ingresa en la opción “adding printers and clases”, se inicia sesión y se evidencia el acceso al servicio a impresora.

Figura 50
Servicio de impresora.



Fuente: Elaboración propia

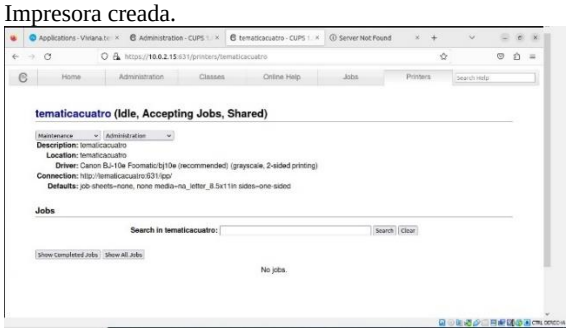
Se ingresa agregar impresora y se escoge la que se desea compartir si una local o de red Se ingresa el enlace según como se desee que quede para la conexión de impresora, Se ingresa el nombre, la descripción, como se desea encontrar la impresora y se activa la opción de compartir

Figura 51
Servicio de impresora.

Fuente: Elaboración propia

Se procede a escoger la marca, el modelo de la impresora y se agrega la impresora. En la siguiente imagen se evidencia la creación de la impresora con sus características

Figura 52
Impresora creada.



Fuente: Elaboración propia

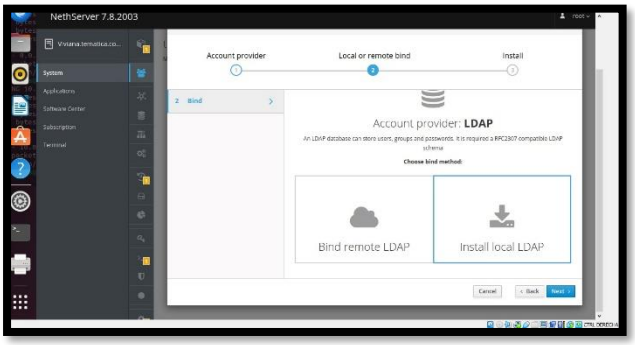
Se ingresa a la configuración de Ubuntu en la sección de impresoras, donde se puede confirmar que la impresora fue compartida

Figura 53
Impresora creada.

Fuente: Elaboración propia

Desde NethServer se ingresa a System y a Users and Groups, para ingresar a proveedor de cuenta se escoge LDAP para tener acceso a carpetas compartidas A continuación se realiza la instalación local LDAP

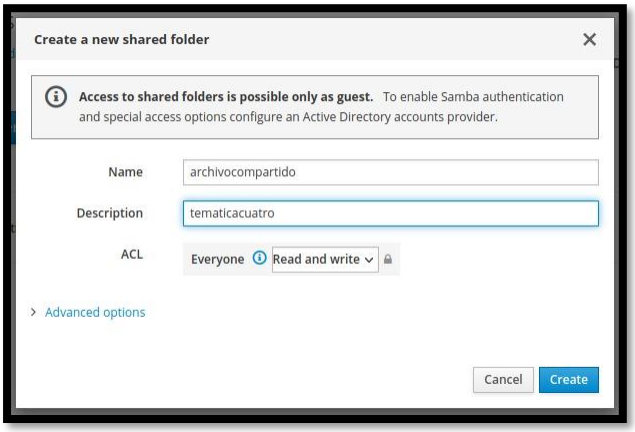
Figura 54
Impresora creada.



Fuente: Elaboración propia

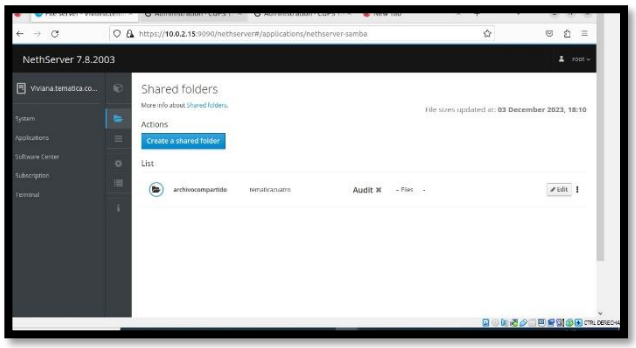
Luego se ingresa a aplicaciones en configuración para crear una carpeta nueva compartida desde Nethserver a Ubuntu En la siguiente imagen se evidencia la creación de la carpeta, se ingresa el nombre de la descripción.

Figura 55
Impresora creada



Fuente: Elaboración propia

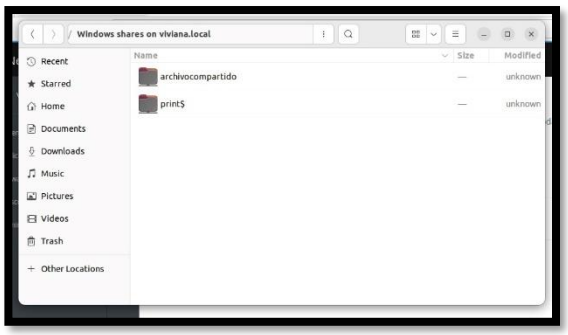
Figura 56
Evidencia de la carpeta creada



Fuente: Elaboración propia

Para verificar que se haya compartido la carpeta, se ingresa al archivo en Ubuntu, tal como se visualiza en la imagen, aparece la carpeta compartida

Figura 57
Impresora creada



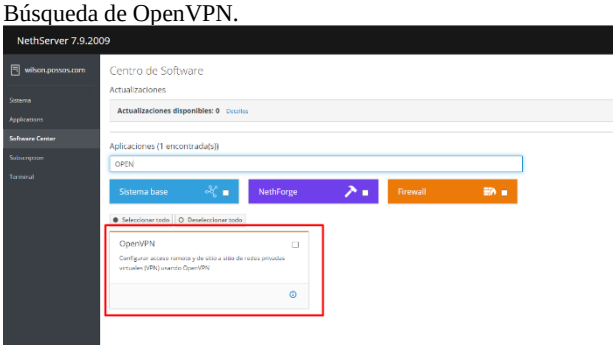
Fuente: Elaboración propia

6 Temática 5 VPN CONNET SERVER

En esta temática se realizará una 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.

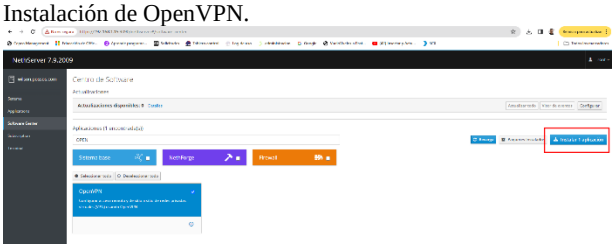
En primer lugar, debe ingresar a nethserver al centro de software en donde se va a descargar e instalar OpenVPN.

Figura 58
Búsqueda de OpenVPN.



Fuente: Elaboración propia

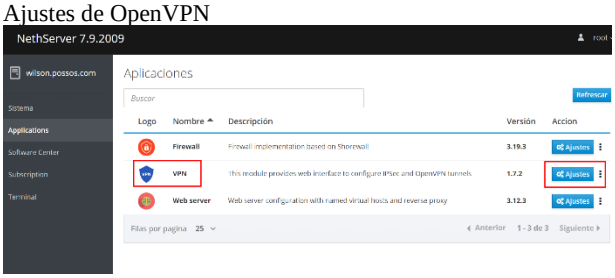
Figura 59
Instalación de OpenVPN.



Fuente: Elaboración propia

Una vez instalada la aplicación OpenVPN se debe dirigir al módulo de aplicaciones y allí la podremos encontrar para realizar la configuración en el botón de ajustes.

Figura 60
Ajustes de OpenVPN



Fuente: Elaboración propia

Se ingresa a la opción de OpenVpn RoadWarrior ya que está diseñado para proporcionar acceso remoto a usuarios móviles o trabajadores remotos. Es ideal para situaciones en las que los usuarios necesitan acceder a la red de la empresa desde ubicaciones externas. En este caso es la ideal para la aplicación que se requiere.

Para realizar la configuración se habilitará OpenVPNWarrior.

Figura 61
Habilitar OpenVPNWarrior.

Fuente: Elaboración propia

A continuación, se configuran las siguientes opciones:

1. Modo de autenticación: Se deja como certificado, vamos a descargar un certificado el puede enviarse viacorreo electronio u otro medio para realizar la conexión.

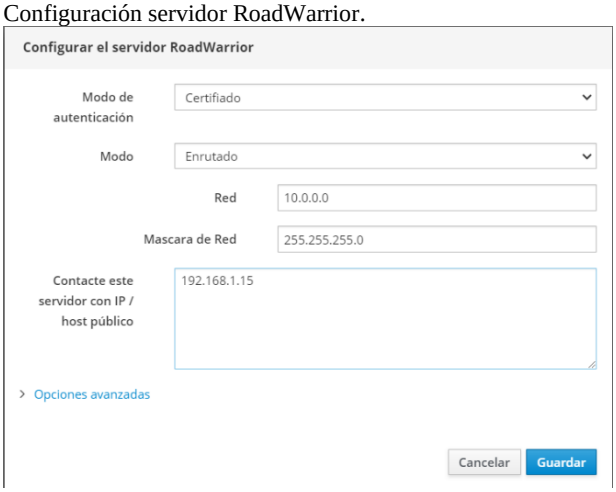
2. Modo: Se deja el modo como enrutado ya que las redes en los extremos de la VPN pueden estar en subredes IP diferentes, y el enrutador VPN se encarga de enrutar los paquetes entre estas subredes.

3. Red: Se asigna una ip de red diferentes a las usadas para que sobre este segmento de red se asigne a los equipos conectados a la VPN.

4. Mascara dered: Se asigna una mascara de red para asegurar que el enrutamiento de los paquetes se realice correctamente.

5. Servidor IP: Se asigna la IP a la cual se va a conectar nuestra VPN, en este caso asignamos la IP del NethServer.

Figura 62
Configuración servidor RoadWarrior.

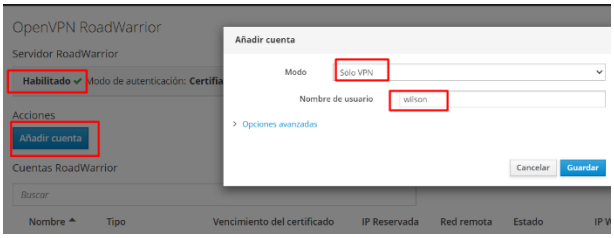


Fuente: Elaboración propia

Al validar que el servidor se encuentra habilitado se añade una cuenta, con la cual se va a realizar la conexión por VPN el cliente.

En este caso se crea un usuario de solo VPN, esta opción se usa cuando el usuario no está sincronizado con ningún otro servicio. Se asigna un nombre de usuario, en este caso; Wilson.

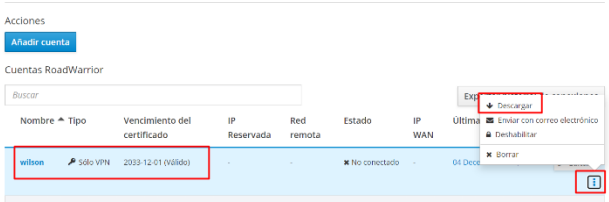
Figura 63
Cuenta Usuario VPN



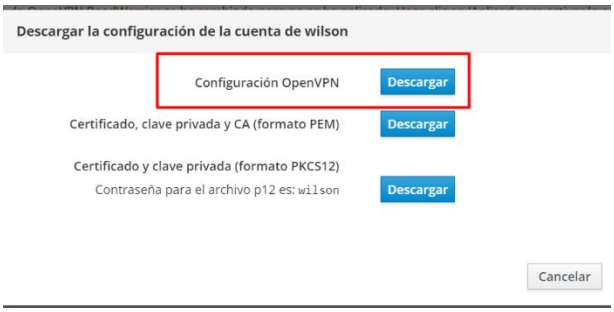
Fuente: Elaboración propia

Ahora se debe descargar el certificado el cual es el archivo con el que se va a conectar con el cliente. Se da click en el usuario que fue creado y en las opciones en los tres puntos damos clic en descargar.

Figura 64
Descarga Certificado de conexión



Fuente: Elaboración propia



Fuente: Elaboración propia

Ahora se carga el certificado en el cliente para la conexión.

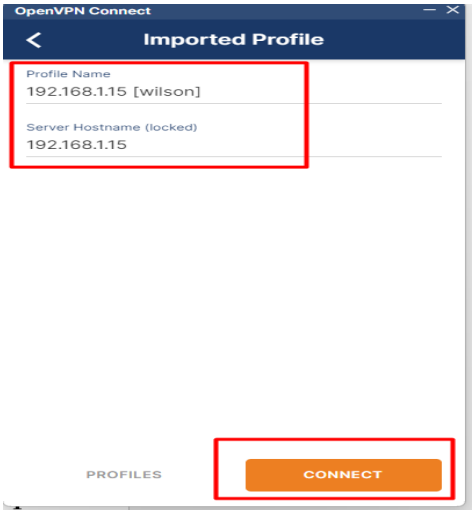
Se descarga el cliente de OpenVPN directamente de la página en el cliente que se va a conectar, se instala y se configura la VPN por medio del archivo certificado descargado.

Figura 65
Configuración cliente VPN en OpenVPN

Fuente: Elaboración propia

Se valida que la información de conexión coincida con la configurada en el NethServer y le damos conectar.

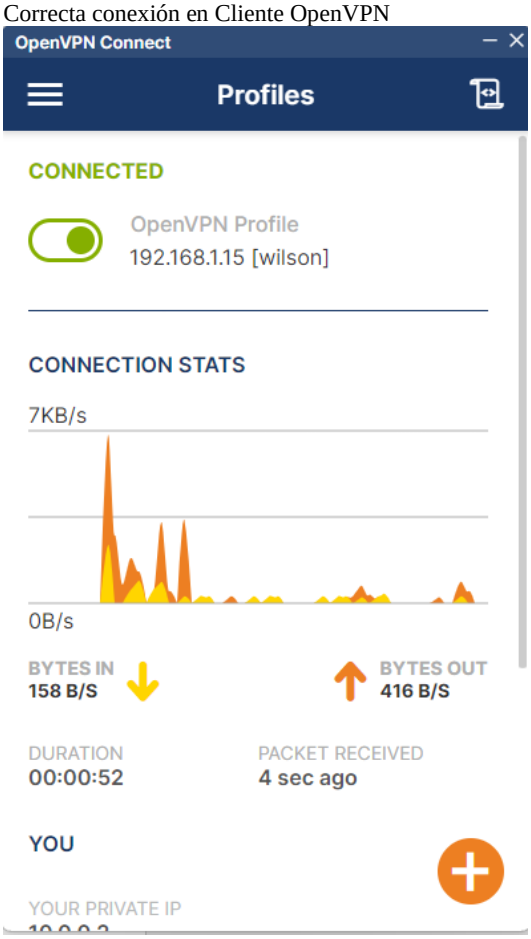
Figura 66
Configuración de VPN Cliente Windows



Fuente: Elaboración propia

Se valida la conexión por VPN se ejecute de manera correcta tanto en el cliente como en el servidor.

Figura 67
Correcta conexión en Cliente OpenVPN



Fuente: Elaboración propia

Por último, se valida la correcta conexión en el servidor.

Figura 68
Conexión en el servidor NethServer por OpenVPN Cliente.

Fuente: Elaboración propia

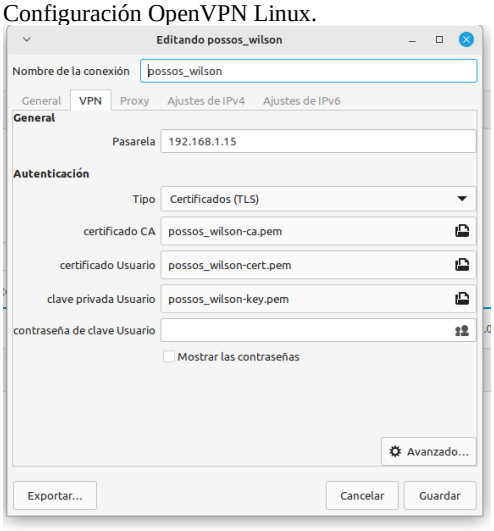
De la misma manera, se realiza la conexión en GNU/ Linux.

Figura 69
Conexión OpenVPN Linux

Fuente: Elaboración propia

Se confirma que la información de conexión coincida con la del servidor.

Figura 70
Configuración OpenVPN Linux.



Fuente: Elaboración propia

7 Conclusiones

La instalación y configuración del servidor NethServer, incluyendo la activación de DHCP Server, DNS Server y el Controlador de Dominio, ha sido exitosa. Las figuras proporcionadas muestran el proceso paso a paso, desde la descarga e instalación inicial hasta la verificación de la configuración de DHCP y DNS. Además, se ha llevado a cabo la configuración de usuarios y grupos, la activación del directorio, y se ha validado la existencia de usuarios creados por el sistema. Se verifica el éxito del proceso al mostrar la activación de DNS y DHCP, así como la creación de la interfaz br0. En resumen, la implementación parece haber sido realizada de manera exitosa y se espera que el entorno esté listo para su uso.

Se observa un enfoque consciente en la seguridad durante el proceso de configuración. Esto se evidencia en la selección de un puerto SSH diferente al predeterminado (2222 en lugar de 22) para mejorar la seguridad del servidor. Además, se ha llevado a cabo la verificación de la conexión a Internet y las direcciones IP, lo que indica una preocupación por la conectividad inicial. Se muestra la verificación de las configuraciones del servidor en el dashboard, lo que sugiere un monitoreo activo de las configuraciones realizadas. Esta atención a los detalles y la seguridad es esencial para garantizar un entorno de servidor robusto y protegido contra posibles amenazas.

La implementación de una conexión VPN utilizando NethServer como servidor y OpenVPN como cliente ofrece una solución segura y flexible para interconectar redes o proporcionar acceso remoto a usuarios. La combinación de OpenVPN como cliente permite un acceso remoto seguro, mientras que NethServer simplifica la gestión centralizada y proporciona una interfaz amigable para la configuración y supervisión de la VPN. Esta configuración ofrece ventajas significativas en términos de seguridad, accesibilidad remota y flexibilidad, pero requiere una configuración precisa.

Conocer cómo funcionan cada una de las zonas y segmentos de redes locales o redes de internet permite comprender la importancia del uso de firewalls para la protección de dispositivos personales, así como mantener seguro los datos e información personal de posibles intrusos externos.

Es fundamental reconocer la importancia de diferentes lenguajes de programación, por esto como se evidencia con Linux es importante tener un buen dominio de los comandos con el fin de poder realizar diferentes tareas, como por ejemplo el compartir archivos, administrar permisos, usuarios, tener manejo en las redes, todo esto con el fin de poder realizar diferentes tareas que pueden ayudar en la elaboración y el buen desarrollo de proyectos como Ingeniera de sistemas.

8 BIBLIOGRAFÍA

[1] LPI LPIC (2022). https://learning.lpi.org/es/learning-materials/
[2] Canonical (2018). Guía del Ubuntu desktop 18.04 LTS. Help Ubuntu. https://help.ubuntu.com/18.04/ubuntu-help/index.html.
[3] Debian (2020). El manual del administrador de Debian 10.04. Debian https://www.debian.org/doc/manuals/debian-handbook/index.es.html

[4] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/
[5] Cómo configurar un firewall para su pequeña empresa en 6 pasos. Cisco. Accedido el 27 de noviembre de 2023. [En línea]. Disponible: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/security/how-to-setup-a-firewall.html
[6] What is a firewall? Definition and explanation. www.kaspersky.com. Accedido el 26 de noviembre de 2023. [En línea]. Disponible: https://www.kaspersky.com/resource-center/definitions/firewall.
[7] 7 Different Types of Firewalls | securitywing. securitywing. Accedido el 27 de noviembre de 2023. [En línea]. Disponible: https://securitywing.com/types-of-firewall/
[8] Understanding Firewalls for Home and Small Office Use | CISA. Cybersecurity and Infrastructure Security Agency CISA. Accedido el 28 de noviembre de 2023. [En línea]. Disponible: https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use#:~:text=Firewalls%20provide%20protection%20against%20outside,or%20network%20via%20the%20internet.
[9] R. Sheldon. "What is stateful inspection in networking?" Networking. Accedido el 25 de noviembre de 2023. [En línea]. Disponible: https://www.techtarget.com/searchnetworking/definition/stateful-inspection#:~:text=Stateful%20inspection,%20also%20known%20as,to%20allow%20through%20the%20firewall.
[10] What Is a Proxy Firewall and How Does It Work? | Fortinet. Fortinet. Accedido el 28 de noviembre de 2023. [En línea]. Disponible: https://www.fortinet.com/resources/cyberglossary/proxy-firewall