Implementación de Servicios IT Escalables y Seguros en Entornos Empresariales con NethServer

Merardo Antonio Piñeros Martínez
mapinerosm@unadvirtual.edu.co
Diego Fernando Parra Figueroa
dfparraf@unadvirtual.edu.co

RESUMEN: *Este artículo describe la implementación y configuración de servicios esenciales de infraestructura IT utilizando NethServer, integrando estaciones de trabajo GNU/Linux. Se configuraron DHCP, DNS y un controlador de dominio para gestionar usuarios y equipos en la red. Un proxy server que permitió filtrar el tráfico web a través del puerto 3128, optimizando la conectividad. Se configuro el cortafuegos para restringir el acceso a portales de entretenimiento y redes sociales mediante reglas específicas. Además, se habilitaron servicios de carpetas compartidas e impresoras utilizando LDAP, por último, se implementó una VPN para establecer un túnel seguro de comunicación con acceso remoto a contenidos y aplicaciones. El proceso incluyó configuraciones detalladas y validaciones desde estaciones GNU/Linux. Los resultados evidencian la eficacia de NethServer como una plataforma integral de gestión IT, proporcionando seguridad, conectividad y control centralizado, lo que respalda su aplicabilidad en entornos corporativos.*

PALABRAS CLAVE: Cortafuegos, infraestructura IT, NethServer, VPN.

1 INTRODUCCIÓN

La gestión eficiente de infraestructura IT en una organización requiere la implementación de servicios fundamentales que aseguren conectividad, seguridad y accesibilidad en toda la red. En este artículo, se describe la implementación de varios servicios críticos utilizando NethServer, una plataforma robusta y de código abierto, en un entorno virtualizado con VirtualBox. La configuración y administración de servicios como DHCP, DNS, controladores de dominio, proxy, cortafuegos, servidores de archivos e impresión, y redes privadas virtuales (VPN) son esenciales para optimizar el funcionamiento de la red, garantizar la seguridad de la información y mejorar la experiencia de los usuarios finales.

El primer conjunto de servicios abordados incluye la configuración de un servidor DHCP, un servidor DNS y un controlador de dominio como lo es "Active Directory Local". Estos servicios permiten centralizar la asignación de direcciones IP, la resolución de nombres de dominio y la gestión de usuarios en una red empresarial. A través de un controlador de dominio, se facilita la autenticación y autorización de usuarios, optimizando la administración de permisos y recursos en las estaciones de trabajo GNU/Linux.

Además, se configura un proxy para filtrar y controlar el acceso a Internet, lo cual es fundamental para garantizar el uso seguro y controlado de los recursos de la red. A su vez, se implementa un cortafuegos para bloquear el acceso a sitios web no deseados, como redes sociales y plataformas de entretenimiento, asegurando que la red sea utilizada de manera eficiente y sin comprometer la productividad de los usuarios. La configuración detallada de estas herramientas garantiza el control total sobre el acceso a la red y los recursos de Internet.

Finalmente, el artículo describe la implementación de servicios de File Server y Print Server, que permiten el acceso a carpetas compartidas e impresoras a través del controlador de dominio. Asimismo, se establece una VPN para asegurar comunicaciones privadas entre las estaciones de trabajo. Todo esto se lleva a cabo en un entorno virtualizado, utilizando VirtualBox, lo que proporciona un entorno controlado y seguro para la implementación de estos servicios. La virtualización permite realizar pruebas, realizar ajustes y replicar el entorno de manera eficiente, proporcionando una infraestructura IT flexible y escalable.

2 METOLOGIA

La implementación de los servicios de infraestructura IT se llevó a cabo siguiendo un enfoque sistemático dividido en etapas clave, con el objetivo de garantizar una configuración eficiente y segura. La metodología utilizada para la implementación incluyó los siguientes pasos:

Instalación y configuración de NethServer como sistema operativo base: El proceso comenzó con la instalación y configuración de NethServer como plataforma base, asegurando que todos los servicios y recursos necesarios estuvieran disponibles para su integración.

Definición y configuración de la red, continuación, se configuró las diferentes tarjetas de red. Red LAN (Zona Verde), Red WAN (Zona Roja), para el desarrollo de las temáticas no se configuro la Zona DMZ, ya que no se considera la interacción con otros servidores (Zona Naranja).

Implementación secuencial de los servicios de infraestructura IT: En esta etapa, se implementaron de manera secuencial los servicios esenciales para la infraestructura IT, incluyendo DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server y VPN. Cada uno de estos servicios fue configurado y ajustado para garantizar su integración efectiva en la red.

Integración y pruebas con estaciones de trabajo GNU/Linux: Una vez configurados los servicios, se procedió a integrar estaciones de trabajo GNU/Linux en el entorno virtualizado, utilizando VirtualBox, y se realizaron pruebas de funcionamiento para validar el acceso a los recursos y la correcta comunicación con los servicios implementados.

Aplicación de políticas de seguridad y control de acceso: Finalmente, se aplicaron políticas de seguridad y control de acceso, configurando el cortafuegos y las restricciones de acceso a servicios, con el fin de asegurar la protección de los recursos compartidos y la privacidad de la comunicación dentro de la red.

Cada uno de los servicios fue configurado de manera detallada, documentado y validado para garantizar su correcto funcionamiento dentro del entorno virtualizado, proporcionando así una infraestructura IT segura y eficiente.

3 OBJETIVO

Implementar y documentar una solución integral de servicios de infraestructura IT utilizando NethServer, optimizando la seguridad, eficiencia y administración de redes en entornos empresariales.

4 INSTALACION NETHSERVER

4.1 Descarga servidor Nethserver

Para descargar Nethserver nos podemos dirigir al sitio oficial de Nethserver y descargar la última versión estable de la imagen ISO. Esta imagen se utilizará para la instalación del sistema operativo. Sin embargo, el equipo de trabajo descargo la ISO de sitio sourceforge [1].

Los requisitos mínimos para instalar Nethserver son:

- 64-bit CPU (x86_64)
- 1 GB de RAM
- 10 GB de espacio en disco

4.2 Configurando Máquina Virtual

Crear la máquina virtual: En VirtualBox [2], seleccionamos "Nueva", nombre "NethServer", tipo "Linux" y versión "Ubuntu (64-bit)". Asignamos al menos 2 GB de RAM y 20 GB de disco duro (VDI, dinámicamente asignado).

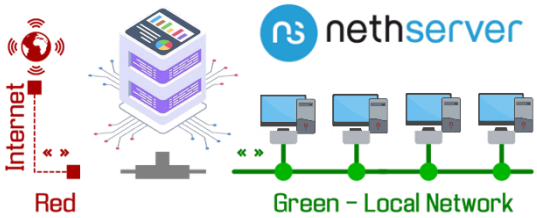
Red: Configuramos la red así: adaptador 1 "Adaptador puente" (Red Roja) y adaptador 2 "Red interna" (Red Verde) para acceso a la red LAN, aquí también podemos añadir un tercer adaptador para las zonas DMZ (Red Naranja)

Almacenamiento: En "Almacenamiento", seleccionamos la ISO de NethServer como unidad de CD/DVD para el arranque.

Configuración adicional: Asigne 2 núcleos de CPU y habilite la aceleración de hardware en "Sistema" > "Aceleración". Ajuste la memoria de video a 16 MB.

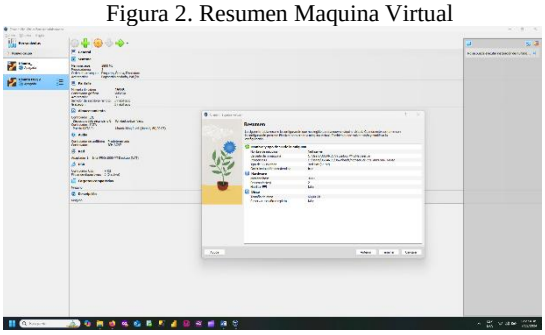
Arranque: Inicie la máquina virtual y comience la instalación de NethServer desde la ISO.

Figura 1. Diagrama de Red en zonas Nethserver



Fuente. Autoría Propia

Figura 2. Resumen Maquina Virtual

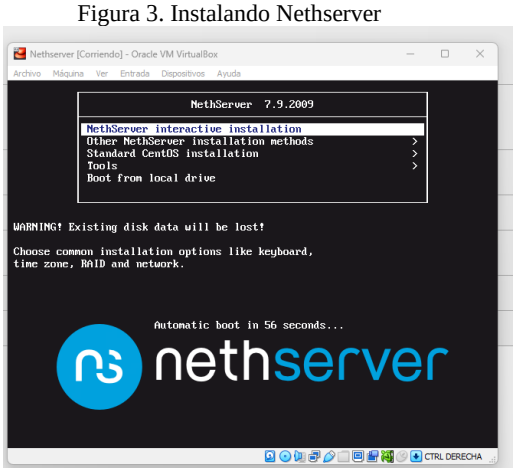


Fuente. Autoría Propia

4.3 Inciando Instalacion Nethserver

La instalación de NethServer se realizó utilizando la opción "NethServer interactive installation", una forma simplificada que facilita el proceso de configuración.

Figura 3. Instalando Nethserver

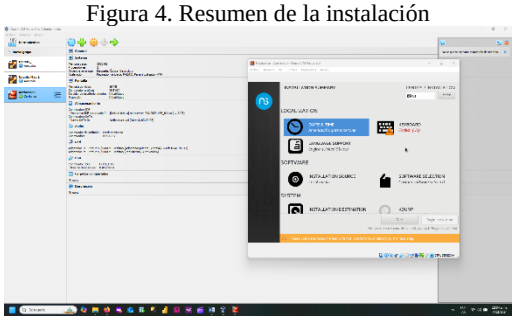


Fuente. Autoría Propia

4.3.1 Configuración inicial:

Zona horaria y teclado: La instalación no puede iniciarse hasta que se configuren la zona horaria y el teclado. Para equipos con teclado Latinoamericano, es necesario seleccionar la variante adecuada para evitar problemas al escribir comandos en la terminal (Figura 4).

Figura 4. Resumen de la instalación



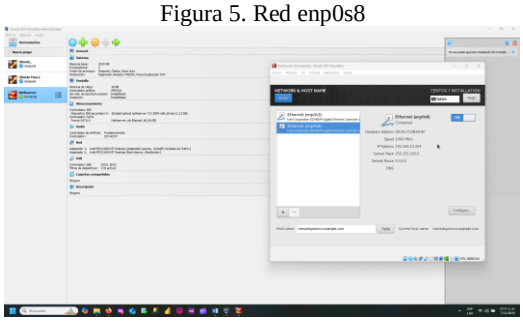
Fuente. Autoría Propia

4.3.2 Configuración de red:

Tarjeta Red enp0s3 (Adaptador 1): Para esta interfaz de red no se realizaron cambios, recordemos que la conexión es mediante DHCP.

Tarjeta de Red enp0s8 (Adaptador 2): Se configuró manualmente la red con la IP fija 192.168.10.254, asignada para la red local (Red LAN).

Figura 5. Red enp0s8



Fuente. Autoría Propia

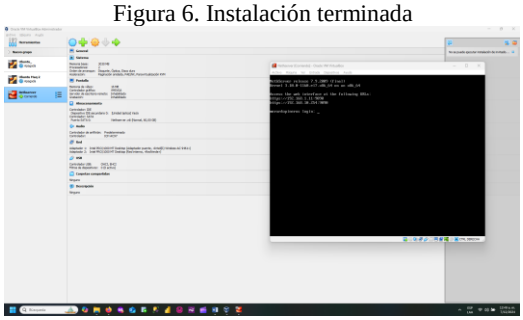
4.3.3 Proceso de instalación:

Tras configurar la red y ajustar la contraseña del usuario ROOT, procedemos a dar inició la instalación.

4.3.4 Instalación completa:

Una vez finalizada la instalación, se obtiene las direcciones es IP para acceder a la interfaz web de NethServer. La dirección IP 192.168.1.11 corresponde a la red WAN y 192.168.10.254 a la LAN "Red Verde".

Figura 6. Instalación terminada



Fuente. Autoría Propia

4.3.5 Acceso al servidor:

Se realiza el acceso al sistema con el usuario ROOT utilizando la contraseña configurada durante la instalación.

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

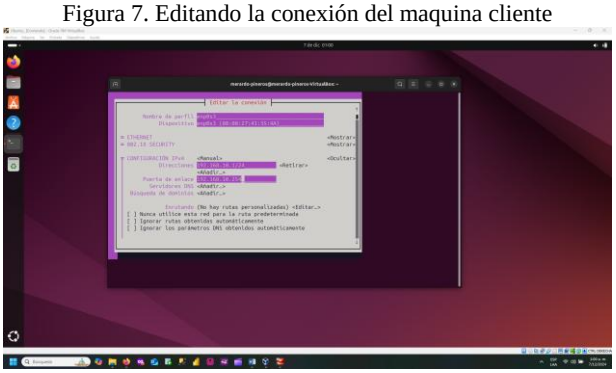
5.1 Producto esperado:

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.

5.1.1 Accediendo a la interfaz Web

Para las configuraciones iniciales, iniciamos sesión en la maquina cliente, si no es posible conectarnos de manera automática, procedemos a conectarnos de manera manual desde la maquina cliente al servidor NethServer, con el fin de realizar las configuraciones a través de la interfaz web del servidor.

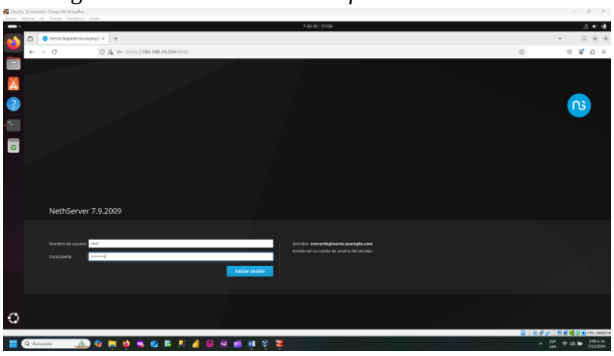
Figura 7. Editando la conexión del maquina cliente



Fuente. Autoría Propia. *Nota.* Para acceder la edición de la conexión en la terminal debemos usar el comando *nmtui*.

Una vez configurada la red, nos conectamos a el servidor Nethserver mediante la interfaz web, recordemos que la conexión la vamos a realizar a través del IP que predefinimos para la red LAN (Ver Figura 5), y el acceso a través del puerto 9090, para este caso 192.168.10.254:9090, el usuario es root y la contraseña la predefinida en la instalación.

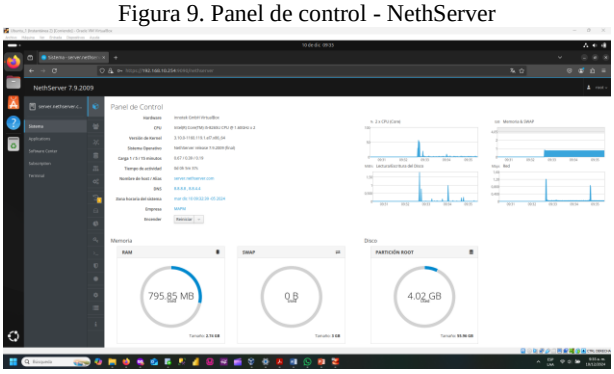
Figura 8. *Accediendo a la interfaz web de NethServer*



Fuente. Autoría Propia.

Recordemos que al intentar acceder a la interfaz web de NethServer por primera vez nos saldrá un aviso de advertencia, ya que es un certificado auto-firmado, procedemos a seleccionar “Aceptar el riesgo y continuar”, como primeros pasos procedemos a solucionar las alertas.

Figura 9. Panel de control - NethServer

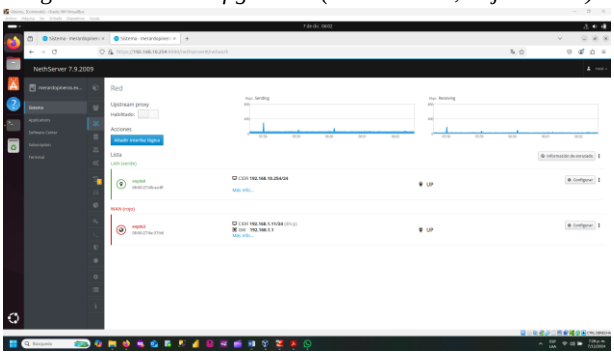


Fuente. Autoría Propia. *Nota.* Una vez accedido la primera ventana en aparecer es el panel de control.

Las dos redes de los adaptadores configurados en la máquina virtual del servidor nos aparecen en LAN (RedVerde), procedemos a configurar la red enp0s3 la cual es la que va ser la red WAN.

En el menú principal de Nethserver nos dirigimos a red, configuramos la red enp0s3, Rol WAN (Rojo), tipo de interfaz Ethernet, protocolo de arranque DHCP, una vez finalizada la configuración deberá listarnos las dos rede LAN (Verde), WAN (Rojo), recuerda que si necesitas una zona DMZ debes agregar un tercer adaptador para configura el rol DMZ (Naranja) .

Figura 10. *Redes configuradas (Verde – LAN, Rojo – WAN)*



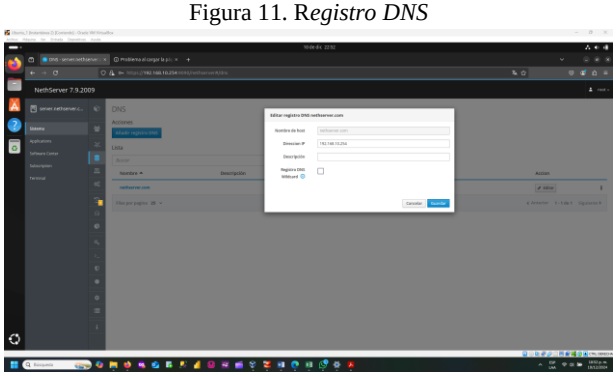
Fuente. Autoría Propia. *Nota.* Evidencia redes configuradas correctamente.

5.2 DNS Server

5.2.1 Ajustes iniciales del DNS:

En los ajustes del servidor DNS, se accede al módulo correspondiente para configurar los registros necesarios para la red local.

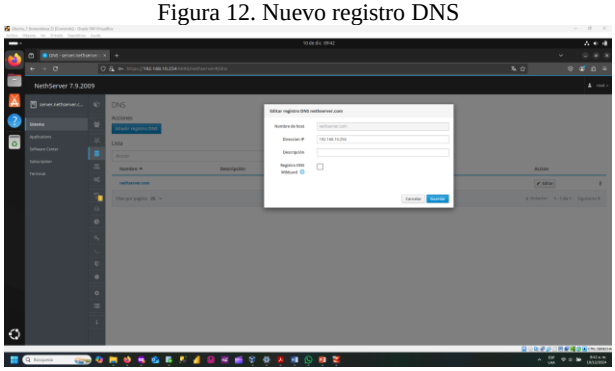
Figura 11. R*egistro DNS*



Fuente. Autoría Propia.

En el panel de control procedemos a dirigirnos a la opción DNS, así accedemos al ajuste de DNS, procedemos a dar clic en añadir registro DNS, el nombre de host será nethserver.com, y colocamos la dirección IP de la interfaz LAN que para el desarrollo de este documento se configuro la IP 192.168.10.254. con esto logramos que nuestro servidor resuelva el dominio server.nethserver.com.

Figura 12. Nuevo registro DNS



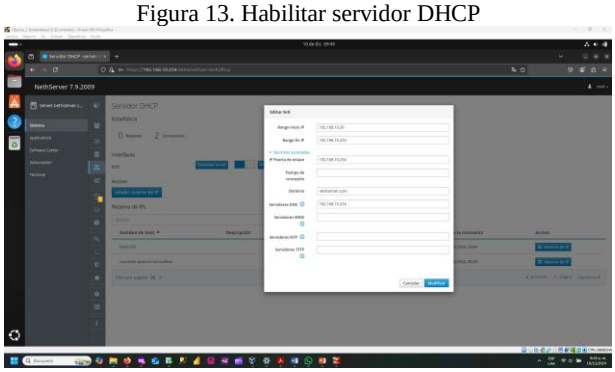
Fuente. Autoría Propia.

5.3 DHC Server

5.3.1 Habilitación del servidor DHCP:

Para esto accedemos al módulo del servidor DHCP y se habilita para la red enp0s8 (LAN). En este paso, se configura el rango de direcciones IP dinámicas, asignando el inicio en 192.168.10.10 y el final en 192.168.10.253, excluyendo la IP 192.168.10.254, que corresponde a la interfaz LAN.

Figura 13. Habilitar servidor DHCP



Fuente. Autoría Propia.

5.3.2 Problemas de conectividad inicial:

Al intentar conectar un equipo de la red LAN a Internet, puede que obtengamos problemas de conexión, debido a la falta de una regla que permita el acceso.

5.3.2.1 Configuración de la regla NAT:

Para habilitar la conexión a Internet desde la red LAN, procedemos a crear una nueva regla NAT en nuestro servidor con el siguiente comando:

- iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

Explicación del comando:

iptables: Herramienta para configurar reglas en el firewall de Linux.

-t nat: Especifica la tabla de traducción de direcciones de red.

-A POSTROUTING: Agrega una regla en la cadena POSTROUTING, aplicada antes de que los paquetes salgan del sistema.

-o enp0s3: Define la interfaz de salida (WAN).

-j MASQUERADE: Habilita el enmascaramiento, reemplazando la IP de origen con la de la interfaz de salida.

5.3.3 Verificación de la conexión:

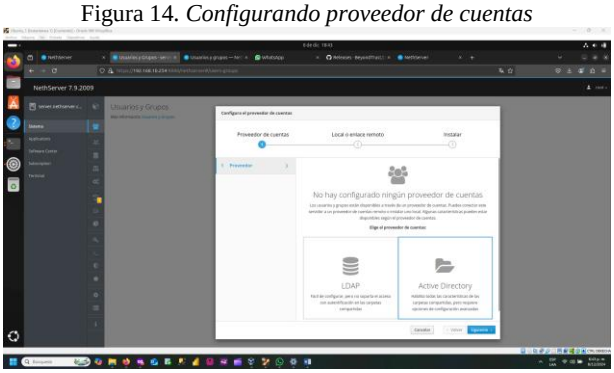
Debemos comprobar la conectividad de un equipo cliente con la dirección IP esta debe estar asignada dentro del rango configurado (Ver Figura 13).

5.4 Configuración del Controlador de Dominio

5.4.1 Configuración del Proveedor de Cuentas:

No dirigimos en el menú del sistema a la opción usuarios y grupos, se procede a configurar el controlador de dominio para el desarrollo de este laboratorio se selecciona Active Directory.

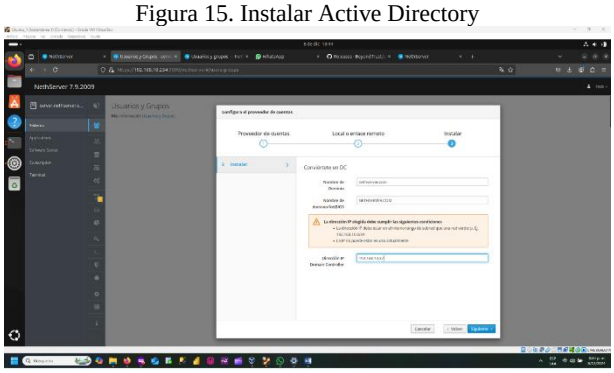
Figura 14. *Configurando proveedor de cuentas*



Fuente. Autoría Propia.

Debemos seguir los pasos guiados, la siguiente opción es local o enlace remoto, clic en crear un dominio, el último paso configuramos "Convierte en DC", para lo cual debemos proceder a colocar nuestro dominio (nethserver.com), y se le asigna una IP dentro del rango de subred en la LAN (Red Verde).

Figura 15. Instalar Active Directory

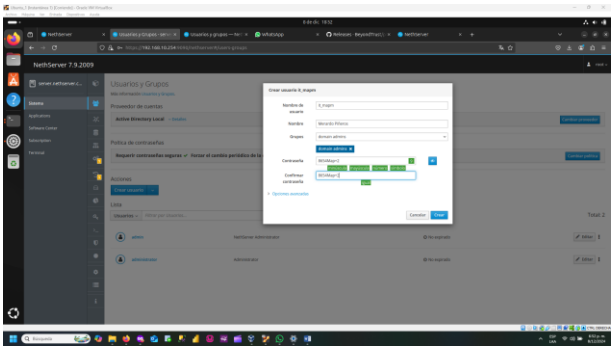


Fuente. Autoría Propia.

5.4.2 Creación de Usuarios y Grupos:

Finalizada la configuración, debemos verificar la instalación del proveedor de cuentas Active Directory Local. Se procede a crear usuarios, como it_mapm, para su posterior acceso mediante el dominio. Para activar los usuarios creados predeterminadamente por el instalador debemos actualizar la contraseña.

Figura 16. Creando Usuarios



Fuente. Autoría Propia. *Nota*. Se videncia la creación del usuario "it_mapm"

5.4.3 Configuración en Estaciones GNU/Linux:

Para vincular estaciones Ubuntu Desktop al dominio, se descargó el script "pbis-open-9.1.0.551.linux.x86_64.deb.sh" desde GitHub [3]. Antes de su ejecución, se configuraron dependencias necesarias con los comandos:

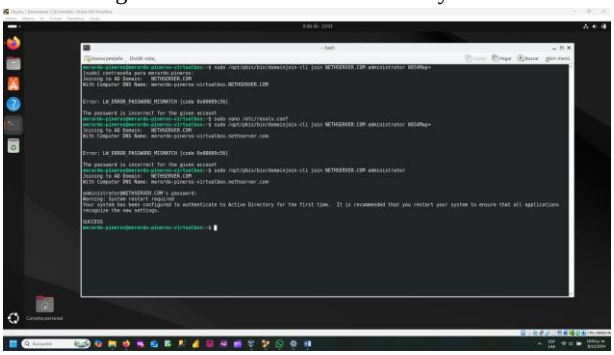
- sudo apt update
- sudo apt install lib32z1

El script se ejecutó tras otorgar permisos con chmod +x script.sh

5.4.4 Vinculación del Dominio y Resolución de Errores:

Para unir una máquina cliente al dominio, se utilizó el comando: sudo /opt/pbis/bin/domainjoin-cli join NETHSERVER.COM administrator.

Figura 17. Vinculación de dominio y cuenta

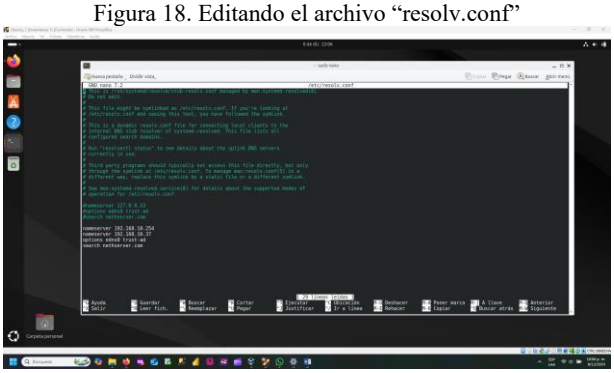


Fuente. Autoría Propia.

Una vez realizado la vinculación, es recomendable reiniciar la maquina cliente, tal como nos lo recomienda la ejecución del comando.

Si ocurre el error DNS_ERROR_BAD_PACKET, se recomienda editar el archivo /etc/resolv.conf y definir los servidores DNS correspondientes (Figura 39):

Figura 18. Editando el archivo "resolv.conf"



Fuente. Autoría Propia.

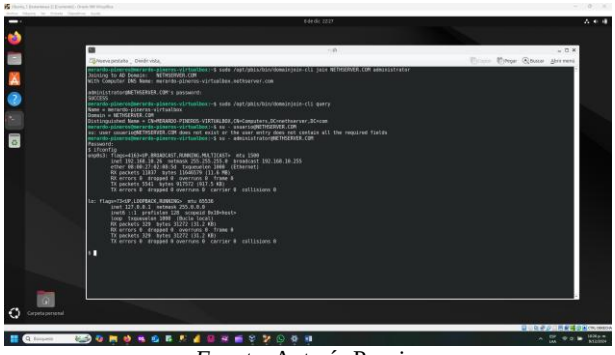
Explicación:

- nameserver 192.168.10.254: La IP corresponde a la IP de la RedVerde
- nameserver 192.168.10.254: La IP corresponde a la IP de Active Directory

5.4.5 Validación del Acceso:

Una vez reiniciado nuestra maquina cliente se validó el acceso exitoso de usuarios mediante el controlador de dominio, como el usuario administrator, desde una estación de trabajo conectada a la red LAN de Nethserver (Figura 19).

Figura 19**.** Accediendo con usuario del Proveedor de cuentas "Active Directory"



Fuente. Autoría Propia.

Con esto hemos alcanzado el producto esperado de la Temática 1.

6 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.

Un proxy [4] es un servidor intermedio que actúa como intermediario entre un cliente (como tu navegador web) y un servidor final (como un sitio web que deseas visitar)

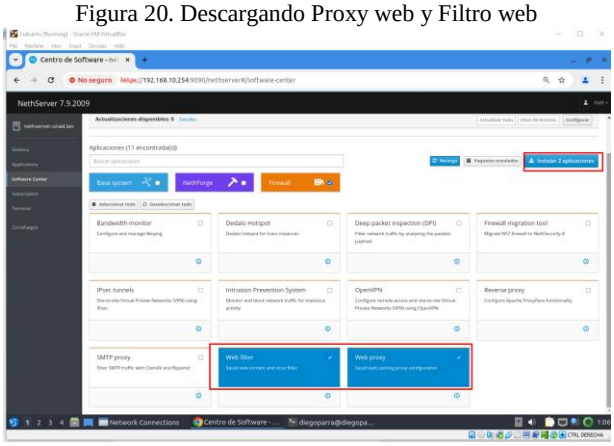
¿Cómo Funciona un Proxy?

- Petición del Cliente: El cliente (tu navegador) envía una solicitud al proxy en lugar de directamente al servidor destino.
- Proxy Recibe la Solicitud: El proxy recibe la solicitud y la evalúa.
- Proxy Envía la Solicitud al Servidor Final: Si la solicitud es válida, el proxy la reenvía al servidor final.
- Respuesta del Servidor Final: El servidor final procesa la solicitud y envía una respuesta al proxy.
- Proxy Envía la Respuesta al Cliente: El proxy recibe la respuesta del servidor final y la reenvía al cliente.

6.1 Instalación de proxy y filtro web

Procedemos a realizar la descarga de las aplicaciones Proxy web y Filtro web (Ver Figura 20), desde el centro de software de Nethserver, para esta temática y las siguientes no volveremos a mostrar los pasos de acceso al servidor nethserver, ya que se encuentra documentado anterior-mente.

Figura 20. Descargando Proxy web y Filtro web



Fuente. Autoría Propia.

Podemos validar la instalación de las aplicaciones a través del menú principal en aplicaciones, o directamente sistema – servicios (Ver Figura 21).

Figura 21. Validación de servicios instalados

6.2 Configuración de Puertos

Dentro del menú de configuración de NethServer, accedemos a la sección Sistema, específicamente a la opción Servicio. Aquí identificamos el servicio Squid y procedemos a establecer el puerto 3128, que será utilizado por el proxy web para gestionar las conexiones.

6.3 Activación del Proxy

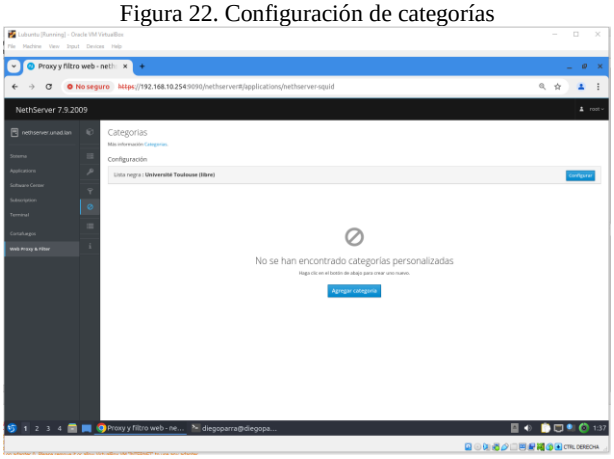
Al completar la instalación inicial del servicio de proxy en NethServer, este permanece deshabilitado de manera predeterminada. Para activarlo, seleccionamos la opción Configurar y habilitamos el modo SSL Transparente para las conexiones en las zonas verdes.

El SSL Transparente, también conocido como SSL/TLS Transparente, permite la incorporación de una capa de seguridad en las comunicaciones sin requerir configuraciones adicionales por parte de los usuarios finales. Este enfoque garantiza que todas las comunicaciones encriptadas sean manejadas de forma automática, mejorando la seguridad sin afectar la experiencia del usuario.

6.4 Descarga de Categorías

Para implementar un filtrado efectivo, es necesario descargar las listas de categorías que el proxy utilizará para identificar y restringir ciertos tipos de contenido, en este caso, utilizamos la lista negra predeterminada desarrollada por la Universidad de Toulouse, una herramienta confiable para filtrar contenido basado en categorías específicas.

Figura 22. Configuración de categorías



Fuente. Autoría Propia.

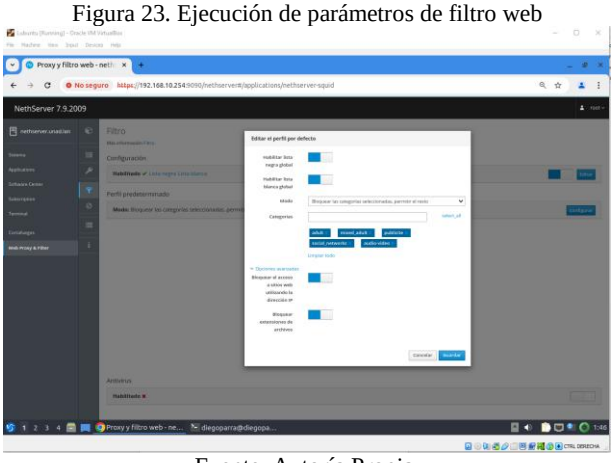
6.5 Configuración del Filtro Web

Una vez descargadas las categorías, procedemos a configurar el funcionamiento del filtro web. Para este ejemplo, seleccionamos la opción de bloquear únicamente las categorías especificadas, permitiendo el acceso al resto del contenido.

Entre las categorías bloqueadas se encuentran:

- Contenido para adultos.
- Publicidad.

Figura 23. Ejecución de parámetros de filtro web



Fuente. Autoría Propia.

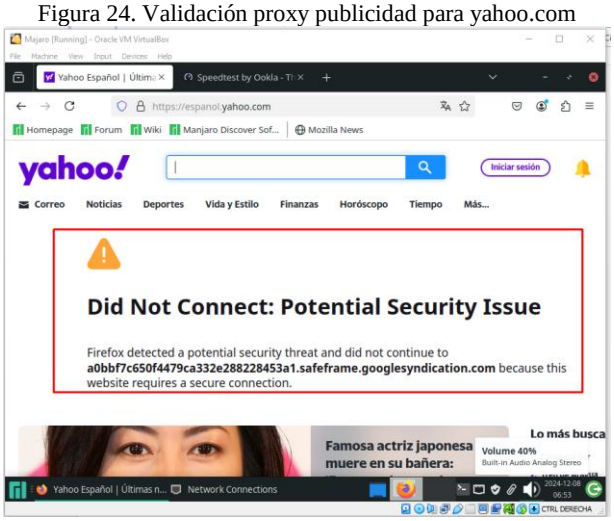
Esta configuración asegura que el acceso esté restringido a contenido no deseado mientras se permite el tráfico general hacia otros sitios web.

6.6 Validación del Funcionamiento del Proxy

Para comprobar la correcta configuración del proxy, utilizamos un equipo cliente con sistema operativo Ubuntu Desktop, previamente integrado en la red local de la zona verde, desde este equipo:

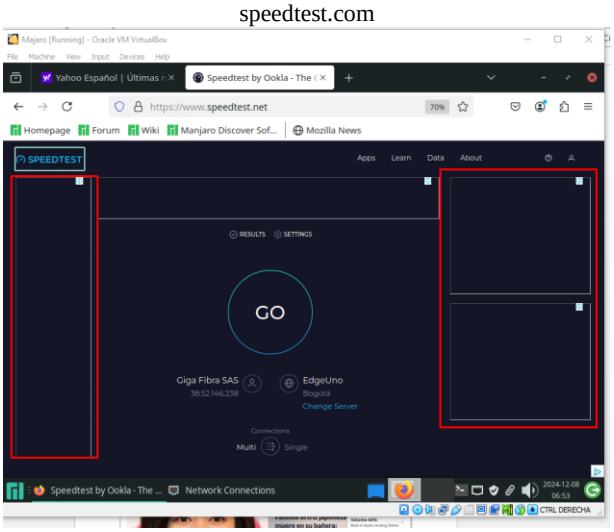
Validamos el control de tráfico para publicidad (Ver Figuras 24, 25).

Figura 24. Validación proxy publicidad para yahoo.com



Fuente. Autoría Propia.

Figura 25. Validación de publicidad para el sitio web speedtest.com

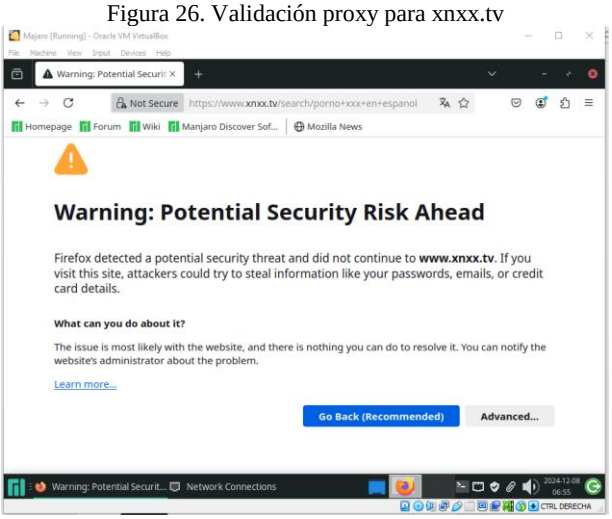


Fuente. Autoría Propia.

Estas pruebas demuestran que el proxy configurado en NethServer opera de manera efectiva, gestionando las políticas de acceso y brindando un control robusto sobre el tráfico web en la red empresarial.

Validamos el control de tráfico para sitio relacionado con contiendo para adultos (Ver Figuras 26).

Figura 26. Validación proxy para xnxx.tv

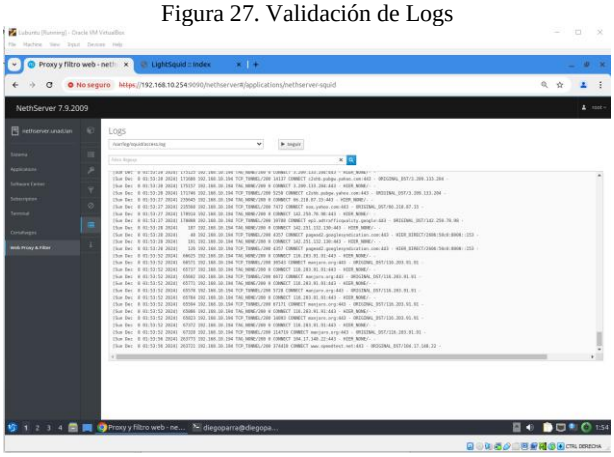


Fuente. Autoría Propia.

6.7 Validación de Logs de la Herramienta

La validación de los registros o logs es fundamental para confirmar que el proxy está operando correctamente y que las políticas de filtrado están siendo aplicadas de manera efectiva. En NethServer, los logs del proxy web se encuentran disponibles en la sección logs de la aplicación web proxy & Filter, dentro del menú de administración.

Figura 27. Validación de Logs



Fuente. Autoría Propia.

7 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.

Un firewall (o cortafuegos) [5] es un componente esencial de seguridad en redes informáticas diseñado para proteger sistemas y datos frente a accesos no autorizados, ataques o tráfico malicioso. Actúa como un filtro que controla el tráfico de red entrante y saliente según reglas predefinidas.

7.1 Instalación del Firewall

Accedemos al Software Center, procedemos a seleccionar la opción Firewall para esta temática instalamos la aplicación "Filtro Web", Esta acción descargará e instalará los componentes necesarios para activar el cortafuegos en el sistema.

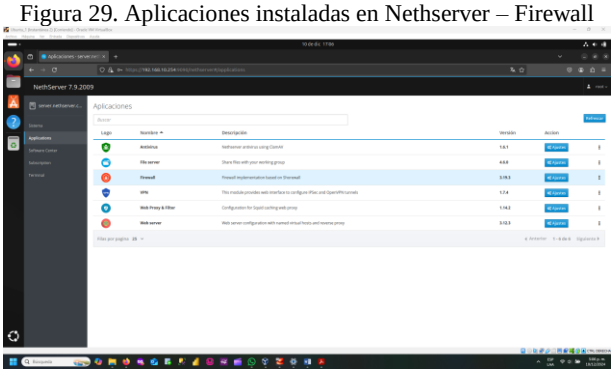
Figura 28. Descargando Filtro Web

Fuente. Autoría Propia.

7.2 Configuración Inicial

Una vez instalado, verificamos que la aplicación se instala de manera correcta en el menú de aplicaciones.

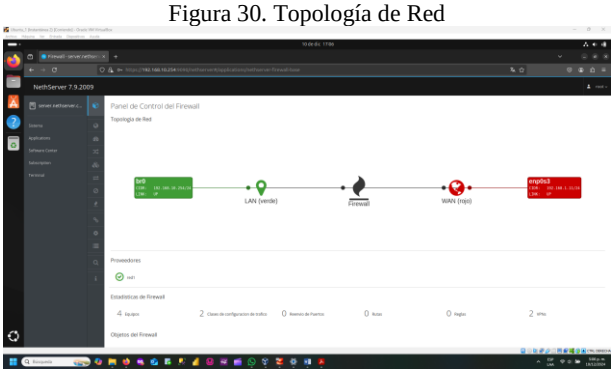
Figura 29. Aplicaciones instaladas en Nethserver – Firewall



Fuente. Autoría Propia.

Posteriormente, a través de Firewall dashboard podemos observar la topología de red configurada para el servidor Nethserver.

Figura 30. Topología de Red

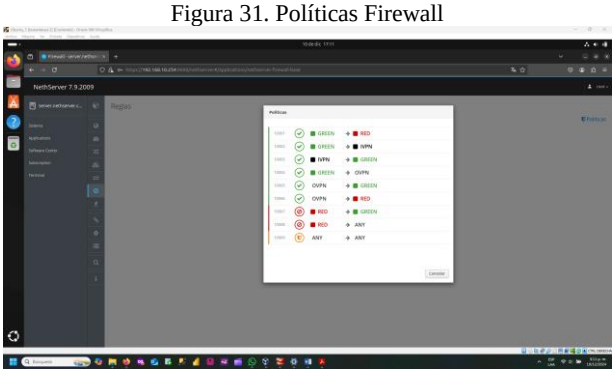


Fuente. Autoría Propia.

Recordemos que solo configuramos la red necesaria para este laboratorio, para poder activar otro adaptador de red, deberá configurarlo, por ejemplo, para la ZONA DMZ (Naranja), activa el adaptador de red en la máquina virtual y le puede dar de alta a través de comando en la terminal de Nethserver.

En el menú de la aplicación nos dirigimos a la opción reglas, en esta sección podemos ver las políticas precargadas por la aplicación.

Figura 31. Políticas Firewall

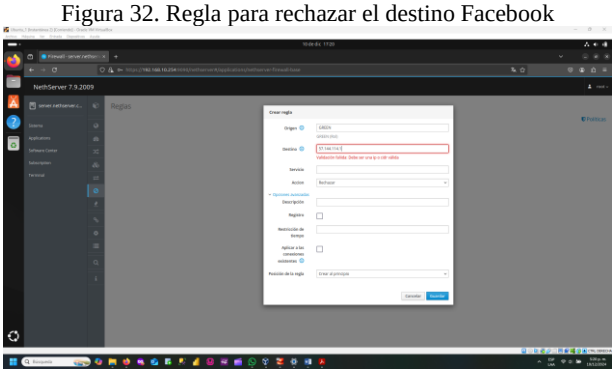


Fuente. Autoría Propia.

7.3 Creación de Reglas de Firewall

Estando en el panel de reglas, procedemos a crear nuevas reglas para bloquear el acceso a ciertas paginas como Facebook y Netflix.

Figura 32. Regla para rechazar el destino Facebook



Fuente. Autoría Propia.

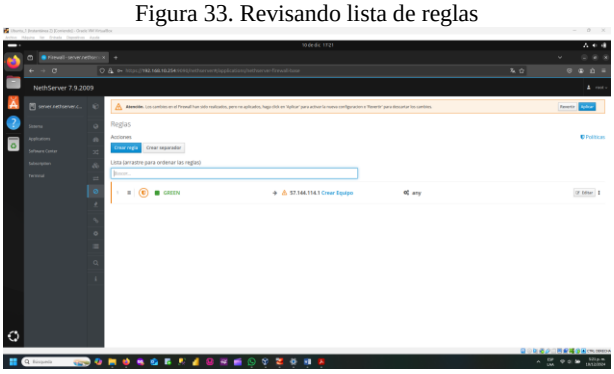
En creación de la regla probablemente no nos deja colocar el dominio a bloquear por lo que debeos hacer un ping al dominio que requerimos bloquear para obtener la IP:

Para lo cual ejecutamos el siguiente comando:

- ping dominio.com

Por ejemplo, para Facebook ping facebook.com esto devolverá la dirección IP de Facebook en el resultado, como: PING facebook.com (57.144.114.1) 56(84) bytes of data.

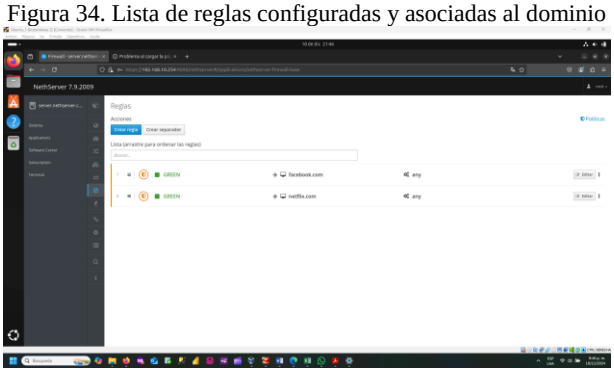
Figura 33. Revisando lista de reglas



Fuente. Autoría Propia.

En la Figura 33 podemos observar que para la red GREEN se creó la regla para rechazar la conexión a la IP de Facebook, anterior a la IP nos sale una pequeña alerta, procedemos a dar clic en la opción “Crear Equipo”, y procedemos a agregar el dominio de Facebook.

Figura 34. Lista de reglas configuradas y asociadas al dominio



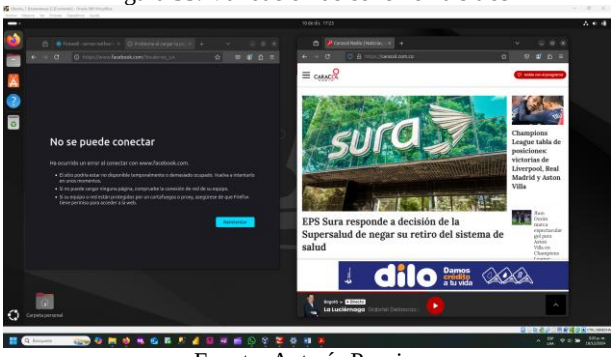
Fuente. Autoría Propia.

7.4 Validación de Configuración

Procedemos a probar las reglas configuradas desde una máquina conectada la red Lan (Zona GREEN), intentamos acceder al sitio bloqueado (Facebook.com) para confirmar que se restringe correctamente.

Verificamos la conectividad con otros sitios permitidos, como caracol.com.co, para garantizar que el acceso general a Internet sigue operativo (Ver Figura 35).

Figura 35. Validación de conexión a sitios



Fuente. Autoría Propia.

8 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

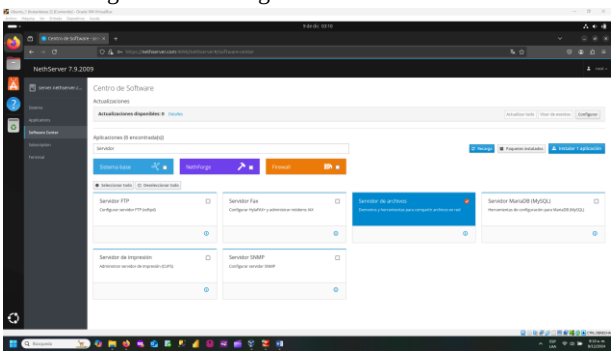
Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

File Server [6] (Servidor de Archivos) es un servidor dedicado a almacenar, administrar y distribuir archivos en una red. Actúa como un repositorio centralizado donde los usuarios pueden guardar, acceder y compartir archivos de manera eficiente, por otro lado, Print Server [7] (Servidor de Impresión) para este laboratorio podemos afirmar que es un software que gestiona una o más impresoras en una red y controla las solicitudes de impresión enviadas por los clientes (computadoras o dispositivos de la red).

8.1 Instalación de File Server en NethServer:

En NethServer, accedemos al "Centro de Software" y buscamos la aplicación "Servidor de Archivos". Hacemos clic en "Instalar" para proceder con la instalación

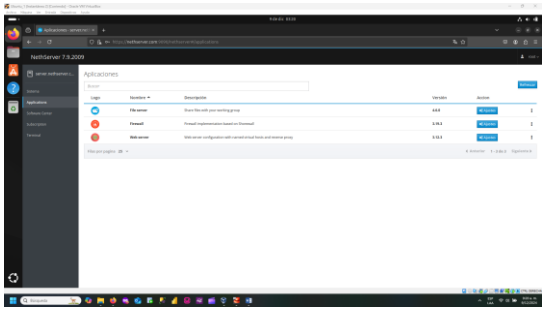
Figura 36. Descargando Servidor de Archivos



Fuente. Autoría Propia.

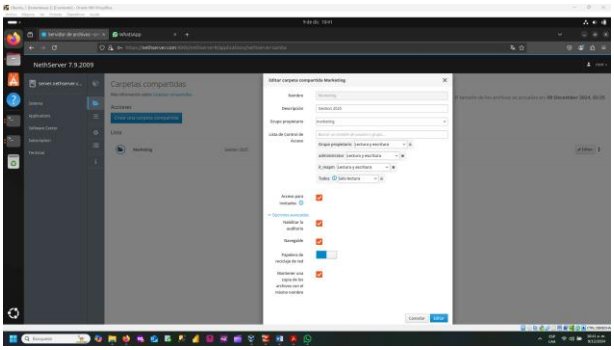
Una vez instalada la aplicación, nos dirigimos la sección aplicaciones, observamos que se haya instalado correctamente y damos click en el botón ajustes de la aplicación File Server (Ver Figura 37), en las configuraciones de File Server, vamos a la sección “Carpetas Compartidas" y seleccionamos la opción "Crear una carpeta compartida"(Ver Figura 38).

Figura 37. Aplicaciones instaladas en Nethserver



Fuente. Autoría Propia.

Figura 38. *Carpetas compartidas Nethserver*



Fuente. Autoría Propia.

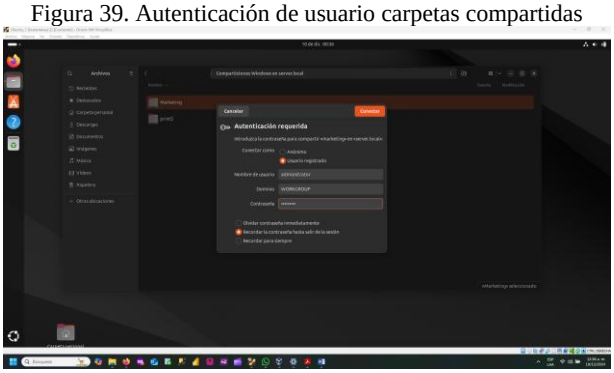
En "Lista de control de acceso", asignamos usuarios y grupos, configurando los permisos según sea necesario.

8.1.1 Acceso y validación de carpeta compartidas File Server:

Una realizado la configuración necesaria en File Server, validamos que podamos acceder desde una maquina cliente a las carpetas y archivos compartidos.

Desde la Interfax grafica del cliente, nos dirigimos a archivos – otras ubicaciones, colocamos smb://192.168.10.254 y procedemos a dar clic en conectar (Ver Figura x), si está siguiendo esta guía, recuerde que la IP es la que fue asignada a la red LAN (Red-Verde), para ingresar le pedirá usuario y contraseña, podrá ingresar con los usuarios asignados a las carpetas, recuerde que en el desarrollo de este laboratorio estamos usando el proveedor de cuentas Active Directory Local.

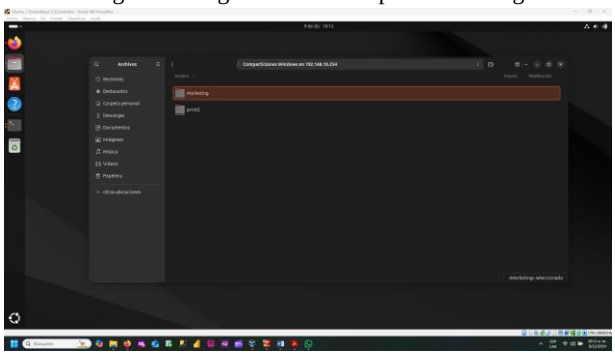
Figura 39. Autenticación de usuario carpetas compartidas



Fuente. Autoría Propia.

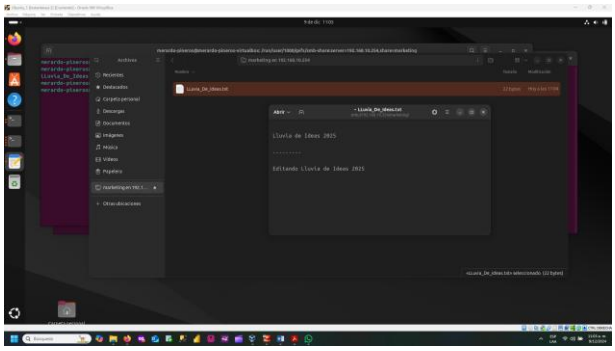
Se procede a ingresar con los usuarios y contraseñas asignadas, recuerde que podrá editar y leer archivos de acuerdo a los permisos otorgados al usuario, para este caso creamos y compartimos la carpeta Marketing.

Figura 40. Ingresando a la carpeta Marketing



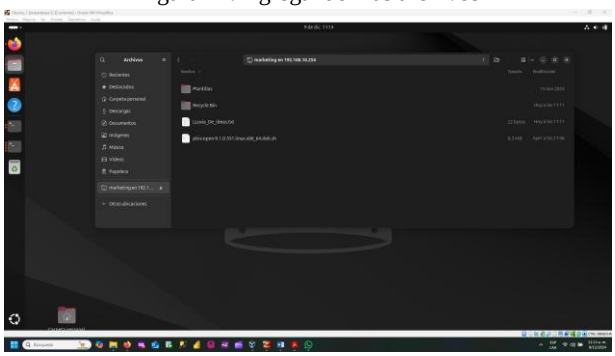
Fuente. Autoría Propia.

Figura 41. Editando un archivo compartido



Fuente. Autoría Propia. *Nota.* Se evidencia la edición de un archivo compartido.

Figura 42. Agregando más archivos

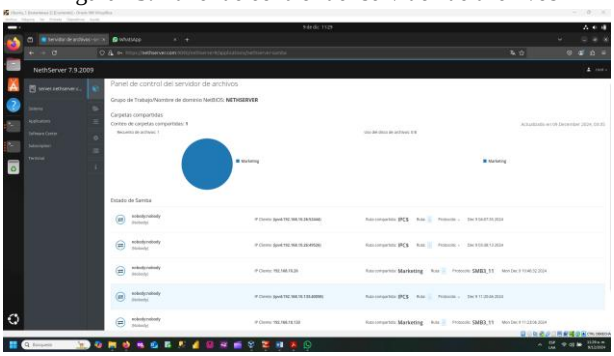


Fuente. Autoría Propia. *Nota.* Se evidencia que podemos agregar más archivos.

8.1.2 Monitoreo y auditoría:

Desde el panel de control de NethServer, en la aplicación File Server, podemos observar las máquinas cliente que se han conectado al servidor de archivos y realizar auditorías de las acciones realizados por los usuarios.

Figura 43. *Panel de control del servidor de archivos*

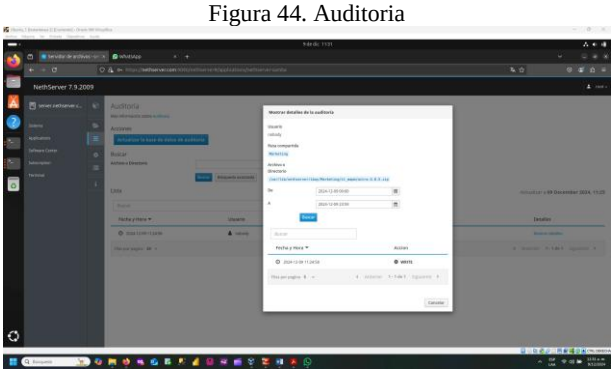


Fuente. Autoría Propia.

Como podemos observar en el panel de control del servidor de archivos, dos máquinas clientes se conectaron a través de nuestro servidor de archivos accediendo a la carpeta compartida Marketing.

En la Figura 44, podemos observar el detalle de auditorita para la ruta compartida Marketing, acción realizad por el usuario it_mapm “WRITE”; Con esto podemos afirmar y estar seguros que nuestro servidor de archivos quedo configurado correctamente.

Figura 44. Auditoria

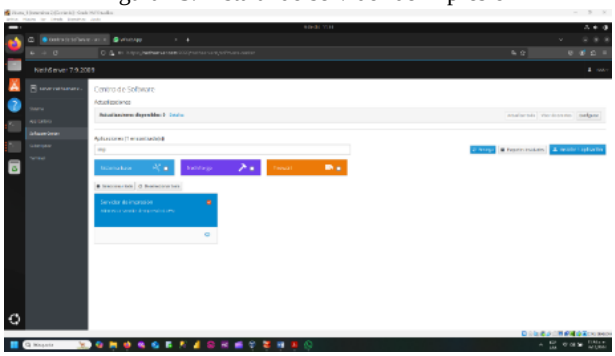


Fuente. Autoría Propia.

8.2 Servidor de Impresión

Se procede a realizar la instalación de la aplicación “Servidor de Impresión”, tenga en cuenta que esta aplicación no aparecerá en la sección aplicaciones, ya que esta se accede des la IP de la Red LAN, a través del puerto 631, para este caso 192.168.10.254:631, le pedirá autenticación de usuario, usuario root y la contraseña de acceso de root a Nethserver.

Figura 45. Instalando servidor de impresión



Fuente. Autoría Propia.

8.2.1 Acceso al Panel de Administración del Servidor de Impresión:

Para añadir una impresora en el servidor de impresión en NethServer, que utiliza CUPS (Common Unix Printing System), puedes seguir los pasos detallados a continuación:

Abre un navegador web desde cualquier dispositivo conectado a la red LAN.

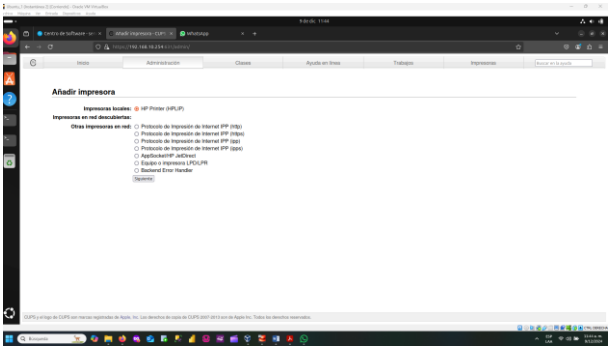
Escribe la dirección IP del servidor de impresión con el puerto de administración de CUPS, por ejemplo: http://192.168.10.254:631

Inicia sesión con las credenciales de administrador del servidor, típicamente el usuario root y la contraseña asignada.

8.2.1.1 Añadir una Impresora

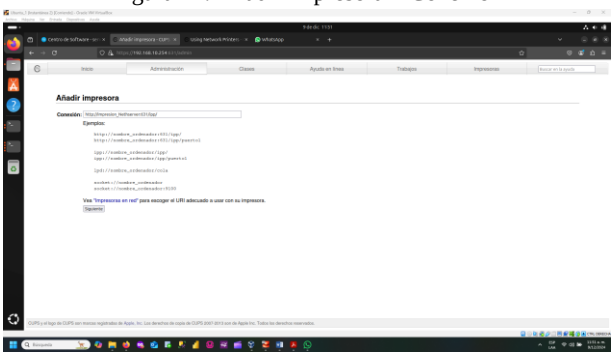
En el panel de CUPS, haz clic en la opción "Administrar", Una vez en el panel de administración del servidor de impresión se procede a dar clic en añadir impresora, Se procede a seleccionar HP Printer “HPLIP” (Ver Figura 46), establezca su conexión de acuerdo al ejemplo, lo que más se adapte su necesidad especifica (Ver Figura 47), clic en siguiente, establezca las especificaciones lo que más se adapte su necesidad específica, para este ejercicio se selecciona la marca Apple, clic en añadir impresora, establecemos el modelo de acuerdo a la necesidad específica.

Figura 46. Añadiendo impresora



Fuente. Autoría Propia.

Figura 47. Añadir impresora – Conexión



Fuente. Autoría Propia.

Con estos pasos ya queda configurada la impresora compartida en nuestro servidor de impresión.

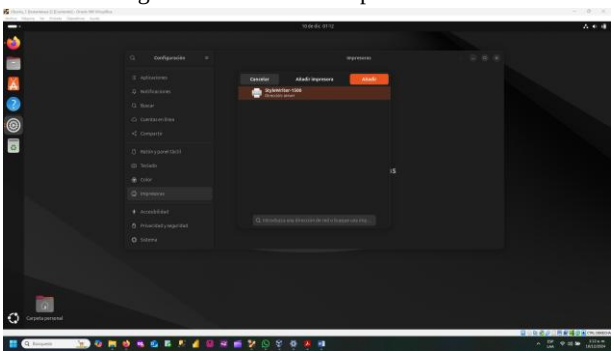
8.3 Configuración en el Cliente

Nos dirigimos a la opción de configuración de la maquina cliente, vamos a impresoras, clic en añadir impresora (Ver Figura 48), al hacer clic en añadir impresora nos saldrá la impresora configurada en el administrador de servicio de impresión (Ver figura 49), seleccionamos la impresora configurada, clic en añadir, una vez añadida correctamente la impresora, nos aparecerá listada la impresora (Ver Figura 50), con esto ya nos debe haber quedado configurada la impresora por medio de red.

Figrua 48. Añadiendo Impresoras

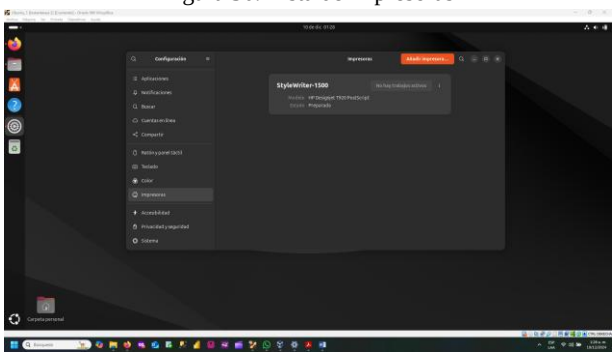
Fuente. Autoría Propia.

Figura 49. Añadiendo Impresora en red



Fuente. Autoría Propia.

Figura 50. Lista de impresoras



Fuente. Autoría Propia.

9 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.

Una VPN [8] (Virtual Private Network) es una tecnología que crea una conexión segura y cifrada entre tu dispositivo (como un ordenador, smartphone o tablet) y otra red a través de Internet, esta conexión permite que los datos transmitidos entre los puntos de conexión estén protegidos contra interceptaciones y ataques.

Elementos clave para entender qué es y cómo funciona una VPN:

Características Principales:

- Cifrado de datos
- Privacidad
- Acceso remoto
- Bypass de restricciones geográficas

Usos Comunes:

- Seguridad en redes públicas.
- Teletrabajo.
- Acceso a contenido restringido.
- Privacidad en línea.

9.1 Configuración de VPN con OpenVPN en NethServer

Desde el centro de software de NethServer, procedemos a instalar la aplicación OpenVPN para habilitar el servicio de redes privadas virtuales.

Figura 51. Descargando OpenVPN

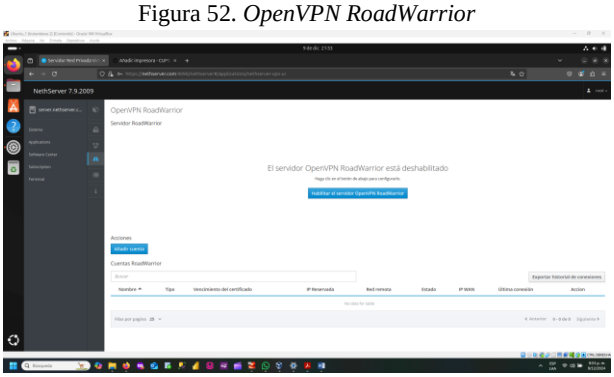
Fuente. Autoría Propia.

En el apartado de aplicaciones, confirmamos la instalación de OpenVPN, que será gestionada a través de la herramienta RoadWarrior.

9.2 Habilitación de OpenVPN RoadWarrior

Después de la instalación, accedemos a los ajustes de OpenVPN y seleccionamos la opción OpenVPN RoadWarrior, desde este menú, activamos el servidor, lo que permitirá gestionar conexiones seguras para usuarios remotos.

Figura 52. *OpenVPN RoadWarrior*



Fuente. Autoría Propia.

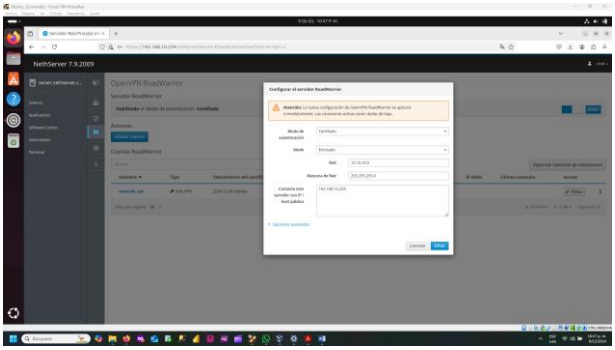
9.2.1 Configuración del servidor RoadWarrior

En la ventana de configuración del servidor se establecen los parámetros necesarios:

Modo de autenticación: Seleccione el tipo que mejor se adapte a los requerimientos (por ejemplo, certificado o contraseña).

Red VPN: Configure una red diferente a la de la LAN para evitar conflictos.

Figura 53. *Configurando el servidor RoadWarrior*



Fuente. Autoría Propia.

Para el desarrollo del laboratorio se asignaron los siguientes parámetros:

Modo de autenticación: “Certifiado”.

Este modo utiliza certificados digitales para autenticar las conexiones, garantizando un nivel elevado de seguridad.

Es especialmente útil en escenarios empresariales donde se requiere validar la identidad de los clientes sin necesidad de contraseñas adicionales.

- Modo: Enrutado

En este modo, el servidor VPN actúa como un enrutador, permitiendo que los clientes conectados accedan a redes internas específicas. Esto asegura un manejo eficiente del tráfico, ideal para configuraciones de acceso remoto.

- Red: 10.10.10.0
- Mascar de red: 255.255.255.0

Estas configuraciones definen la subred asignada a la VPN. La red 10.10.10.0 con una máscara 255.255.255.0 permite un rango de 254 direcciones IP disponibles (10.10.10.1 a 10.10.10.254), lo que es adecuado para gestionar múltiples clientes conectados al servidor.

- IP: 192.168.10.254

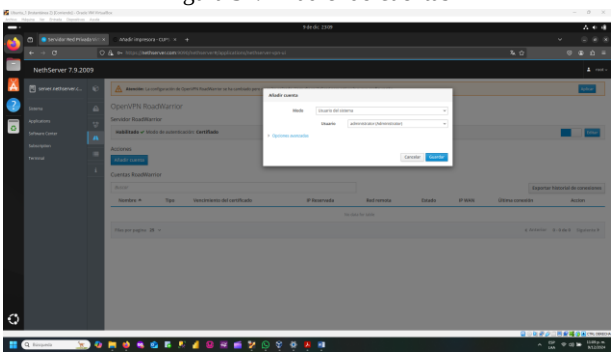
Esta es la dirección IP del servidor VPN dentro de la red local (LAN). Funciona como la puerta de enlace para las conexiones de los clientes a través de la VPN.

Estos parámetros configuran una VPN segura, flexible y compatible con múltiples clientes en una infraestructura IT empresarial.

9.2.2 Creación de cuentas de usuario

Tras configurar el servidor, es necesario añadir las cuentas de usuario que se conectarán mediante la VPN. Esto requiere que el proveedor de cuentas esté habilitado (Ver temática 1, controlador de dominio).

Figura 54. Añadiendo cuentas

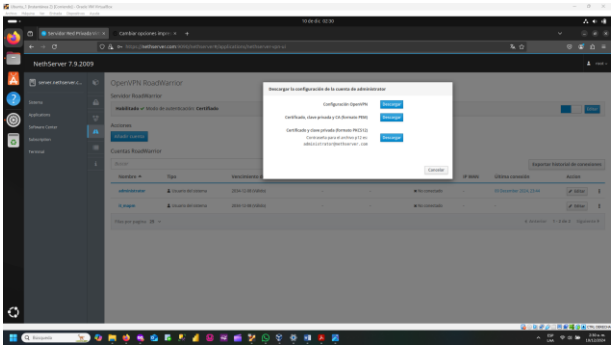


Fuente. Autoría Propia.

9.2.2.1 Descarga del archivo de configuración de usuario

Una vez añadido la cuentas con la asignación de usuarios correspondiente proceda a descargar el archivo de configuración, este lo necesitamos para la maquina cliente a conectar a través de VPN, para configurar la máquina cliente y conectarnos al servidor VPN, debemos descargar el archivo que mejor se adapte al software de cliente VPN que estemos usando.

Figura 55. Descarga de la configuración de la cuenta de usuario



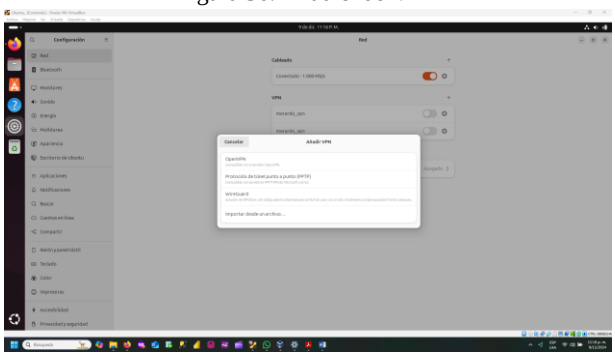
Fuente. Autoría Propia.

9.3 Configuración de la VPN en el Cliente

9.3.1 Añadiendo una VPN en el cliente

En la maquina cliente vamos a configuración – red, procedemos a añadir VPN, para el desarrollo de este documento se seleccionó la opción "Importar desde un archivo", recordemos la descarga de archivos (Ver Figura 55), debes seleccionar el archivo que tenga la extensión *.ovpn*.

Figura 56. Añadiendo VPN

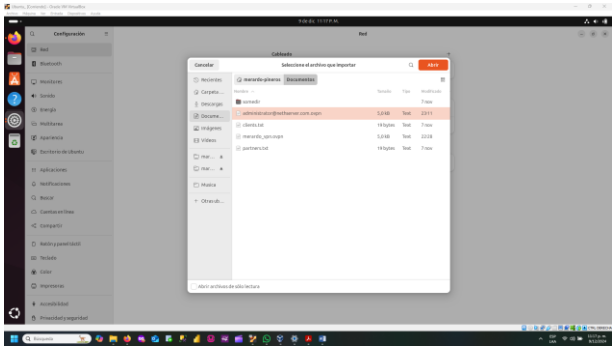


Fuente. Autoría Propia.

9.3.2 Importación del archivo de configuración

Es fundamental seleccionar correctamente el archivo con extensión .ovpn. Generalmente, este archivo lleva un nombre como usuario@dominio.com.ovpn.

Figura 57. Selección del archivo a importar

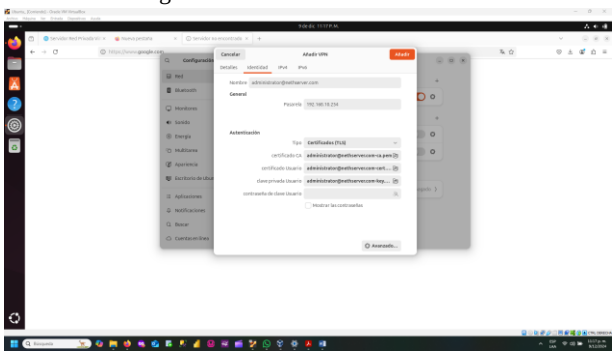


Fuente. Autoría Propia.

9.3.3 Verificación de identidad en la configuración

Tras importar el archivo, la configuración de la VPN estará disponible en la sección de identidad. Dependiendo del modo de autenticación (certificado o credenciales), puede que no sea necesario ingresar usuario y contraseña.

Figura 58. Añadir VPN – identidad

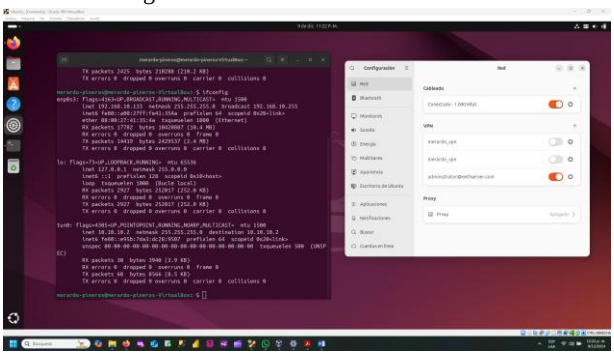


Fuente. Autoría Propia.

9.4 Verificación de la conexión VPN

Para comprobar que la conexión se ha establecido correctamente, podemos utilizar el comando ip route. Si la VPN está activa, se verá una ruta asociada a la interfaz virtual tun0, indicando que el tráfico se enruta a través de la red VPN configurada.

Figura 59. Verificando conexión VPN



Fuente. Autoría Propia

La salida del comando ip route muestra que estamos conectados a la VPN correctamente.

Conexión VPN activa (tun0):

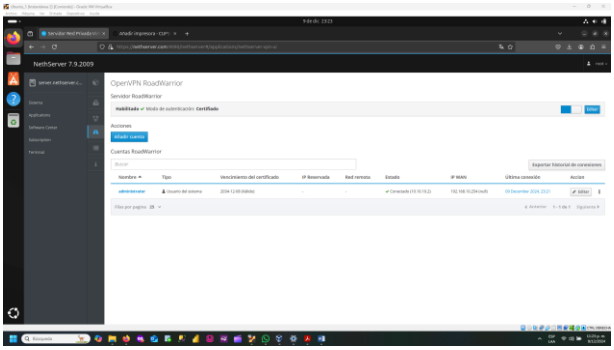
- La ruta 10.10.10.0/24 dev tun0 indica que tienes una interfaz de red virtual llamada tun0 que está enrutando tráfico hacia la red 10.10.10.0/24, lo cual corresponde a la red de la VPN.

- La ruta default via 10.10.10.1 dev tun0 muestra que el tráfico por defecto (es decir, el tráfico que no coincide con otras rutas más específicas) se enruta a través de la interfaz VPN tun0, usando la puerta de enlace 10.10.10.1, que es probablemente el servidor VPN.

9.5 Estado de cuentas VPN en el servidor

De vuelta a nuestro servidor podemos verificar que efectivamente el usuario admisitrator está conectado a través de la red VPN, estado conectado (10.10.10.2), ultima conexión “09 diciembre 2024”

Figura 60. Revisando el estado de las cuentas VPN

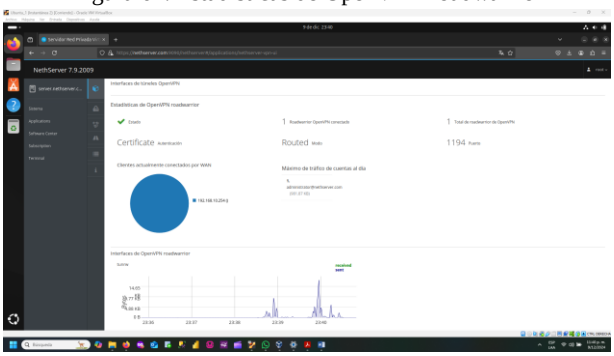


Fuente. Autoría Propia.

9.5.1 Estadísticas de OpenVPN RoadWarrior

A través de las estadísticas de OpenVPN, también podemos observar el tráfico de cuentas al día, que para nuestra conexión es 981.87 KB.

Figura 61. Estadísticas de OpenVPN roadwarrior



Fuente. Autoría Propia.

Este flujo de instrucciones de la temática VPN garantiza una implementación exitosa de OpenVPN en NethServer, habilitando una conexión segura para usuarios remotos.

10 Conclusiones

La implementación y configuración de servicios clave como DHCP, DNS y el controlador de dominio en NethServer consolidaron una infraestructura IT eficiente y segura. Se logró integrar exitosamente una estación de trabajo GNU/Linux, lo que refleja la capacidad de NethServer para centralizar la administración de recursos, optimizar procesos críticos y garantizar una experiencia funcional para el usuario. Estas configuraciones podrán ser replicables en otros entornos similares, mejorando la operatividad y la seguridad de las redes organizacionales.

El uso de herramientas como DHCP y DNS, junto con la autenticación centralizada mediante el controlador de dominio, permitió un manejo eficiente de credenciales, reducción de la carga administrativa y una experiencia de usuario final optimizada. Esto refuerza la importancia de una planificación detallada en la implementación de infraestructura tecnológica, que puede extenderse a futuras mejoras como la integración de más estaciones y políticas avanzadas de seguridad.

La experiencia adquirida en configuraciones de proxy en NethServer destacó su utilidad para controlar y optimizar el uso de recursos, mostrando cómo las mejores prácticas pueden traducirse en un uso eficiente de la infraestructura IT. Esto es esencial para implementar soluciones productivas en entornos empresariales.

La implementación y configuración de un cortafuego en GNU/Linux, como se realizó en NethServer, ha demostrado ser una solución eficaz para restringir el acceso a sitios web no deseados, como redes sociales y portales de entretenimiento. Este control se logró mediante la definición de reglas y políticas claras, validadas desde una estación de trabajo, lo que asegura un entorno de red más seguro y productivo. Esta práctica subraya la importancia de los cortafuegos como una herramienta esencial para la gestión y protección de redes empresariales.

El desarrollo de un File Server y un Print Server con autenticación LDAP demostró ser efectivo para la gestión centralizada en redes corporativas. Se estableció un sistema robusto que garantizó la seguridad y facilitó la colaboración. La integración de estos servicios en estaciones GNU/Linux evidenció su flexibilidad para adaptarse a entornos empresariales.

La implementación de una VPN mediante OpenVPN RoadWarrior en NethServer demostró ser una solución eficiente para establecer comunicaciones seguras entre servidores y estaciones de trabajo. La autenticación basada en certificados y la validación de la configuración mediante herramientas de diagnóstico reflejan la robustez y funcionalidad de la solución. Este ejercicio subraya la relevancia de las VPN en entornos corporativos y educativos, asegurando un acceso remoto confiable y seguro.

La documentación de estas prácticas proporciona una base sólida para futuras implementaciones y destaca cómo las tecnologías de código abierto, como NethServer y OpenVPN, pueden adaptarse para cumplir necesidades específicas de conectividad y seguridad. Este enfoque promueve la transformación digital en organizaciones que buscan soluciones escalables y seguras

11 REFERENCIAS

[1]. NethServer Linux para pequeñas oficinas y medianas empresas. (s. f.). Sourceforge.net. https://sourceforge.net/projects/nethserver/

[2]. Virtualbox, O. V. (2011). Oracle vm virtualbox. *Change*, *107*, 1-287. https://imagegrafix.sa/wp-content/uploads/2021/07/ImageGrafix_oracle-virtualbox-datasheet.pdf

[3]. BeyondTrust. (s. f.). Releases · BeyondTrust/pbis-open. GitHub. https://github.com/beyondtrust/pbis-open/releases

[4]. f Proxy server: Proxy server - MDN Web Docs Glossary: Definitions of Web-related terms | MDN. (2023, 8 junio). MDN Web Docs. https://developer.mozilla.org/en-US/docs/Glossary/Proxy_server

[5]. Cisco Secure Firewall: First Line of Defense. (2024, 19 octubre). [Vídeo]. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

[6]. Wright, G. (2021, 19 agosto). *file server*. Search Networking.https://www.techtarget.com/searchnetworking/definition/file-server

[7]. ACDI Latin America. (2022, 17 octubre). Cómo funciona un servidor de impresión? Linkedin. https://www.linkedin.com/pulse/c%C3%B3mo-funciona-un-servidor-de-impresi%C3%B3n-acdi-latam/

[8]. Ferguson, P., & Huston, G. (1998). What is a VPN?. http://sol.te.net.ua/www/nanog/vpn.pdf