IMPLEMENTACIÓN Y GESTIÓN DE INFRAESTRUCTURA IT EN GNU/LINUX PARA INTRANET Y EXTRANET: UN ESTUDIO DE CASO

Jorge Ernesto Gomez Giraldo
email: jegomezgi@unadvirtual.edu.co
Sergio Iván Cadavid Cadavid
e-mail: sicadavidca@unadvirtual.edu.co
Jenny Marcela Gallardo Molina
email: jmgallardom@unadvirtual.edu.co
Kristian Ferney Cruz Vaca
email: kfcruzv@unadvirtual.edu.co
Melwin Sabier Forero Ramirez
email: msforeror@unadvirtual.edu.co

RESUMEN: *Este artículo explora la configuración y administración de infraestructura IT utilizando GNU/Linux, específicamente Nethserver, para servicios de Intranet y Extranet en entornos institucionales complejos. Se detalla la implementación de servicios como DHCP, DNS, controladores de dominio, proxies, cortafuegos, servidores de archivos e impresión, y VPNs. A través de análisis prácticos y documentación técnica, se demuestra cómo GNU/Linux puede ser una solución robusta y segura para las necesidades de IT en entornos empresariales.*

PALABRAS CLAVE: GNU/Linux, Nethserver, Infraestructura IT, Intranet, Extranet, Servicios de Red, Seguridad en Red

1 INTRODUCCIÓN

En el ámbito de la administración de sistemas operativos, GNU/Linux se destaca como una plataforma poderosa y versátil para la gestión de infraestructuras IT en entornos empresariales y educativos. Este artículo aborda la implementación y gestión de infraestructuras IT con GNU/Linux, enfocándose en Nethserver, una distribución orientada a la administración de servicios de red y seguridad.

El entorno de TI moderno requiere soluciones robustas, seguras y adaptables. GNU/Linux, reconocido por su estabilidad y seguridad, proporciona un ecosistema idóneo para administrar infraestructuras IT complejas. Nethserver, con su interfaz intuitiva y herramientas de administración, facilita la configuración de servicios esenciales como DHCP, DNS, controladores de dominio, y VPNs, destacando por su eficiencia y flexibilidad.

Además, la escalabilidad y flexibilidad de GNU/Linux, combinadas con su reputación de seguridad y eficiencia, lo convierten en una elección preferente para administradores y profesionales de TI. La adaptabilidad de estas plataformas permite a las organizaciones diseñar sistemas que no solo atienden sus necesidades actuales, sino que también pueden evolucionar con el crecimiento y cambio de sus requerimientos operativos.

Este artículo busca demostrar cómo GNU/Linux, a través de Nethserver, puede ser una solución eficiente y segura para las necesidades de IT, tanto en intranets como en extranets de instituciones. Se examinarán las capacidades de GNU/Linux para configurar y mantener una variedad de servicios esenciales.

2 CONFIGURACIÓN DE NETHSERVER EN GNU/LINUX

La instalación y configuración básica de Nethserver en un entorno GNU/Linux se centra en la preparación e instalación del sistema operativo en un entorno virtualizado. Este proceso implica varios pasos clave para asegurar una implementación exitosa y funcional.

En esta fase inicial, se procede a descargar Nethserver desde su sitio web oficial. Este paso es crucial para obtener la versión más reciente y segura del sistema operativo. La descarga de Nethserver marca el comienzo de la configuración, asegurando que se cuenta con el software necesario para la implementación.

En la figura 1 se muestra la página de descarga de NethServer, con el proceso de descarga en curso. Este paso es esencial para adquirir la base del sistema operativo que se instalará en las máquinas virtuales.

Figura 1. Descarga de NethServer desde el sitio web oficial

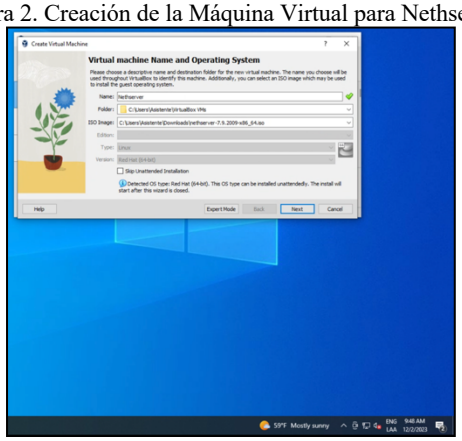
Fuente: Autoría Propia

Posteriormente en la figura 2 se preparan las máquinas virtuales necesarias para el desarrollo del ejercicio. En este

caso, se configuran dos máquinas: una que funcionará como servidor y otra como cliente. Esta división permite simular un entorno real donde el servidor Nethserver proporcionará servicios a la máquina cliente.

Se muestra en la figura 2 el proceso de creación de la máquina virtual para Nethserver en VirtualBox de Oracle. Aquí se observa la imagen ISO de NethServer lista para ser instalada en la máquina virtual, estableciendo las bases para el entorno de pruebas y operación.

Figura 2. Creación de la Máquina Virtual para Nethserver

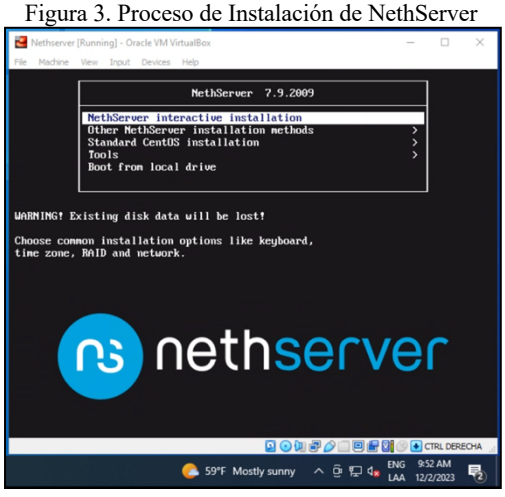


Fuente: Autoría Propia

El proceso de instalación de Nethserver es el siguiente paso crucial. Aquí, se inicia la instalación del sistema operativo en la máquina virtual preparada previamente. Este proceso es fundamental para configurar el entorno del servidor Nethserver.

Ahora, en la figura 3 tenemos la captura de la pantalla inicial de instalación de NethServer, donde se observa el inicio del proceso de instalación. Este paso es crucial para asegurar una correcta instalación y configuración del sistema operativo en el entorno virtual.

Figura 3. Proceso de Instalación de NethServer

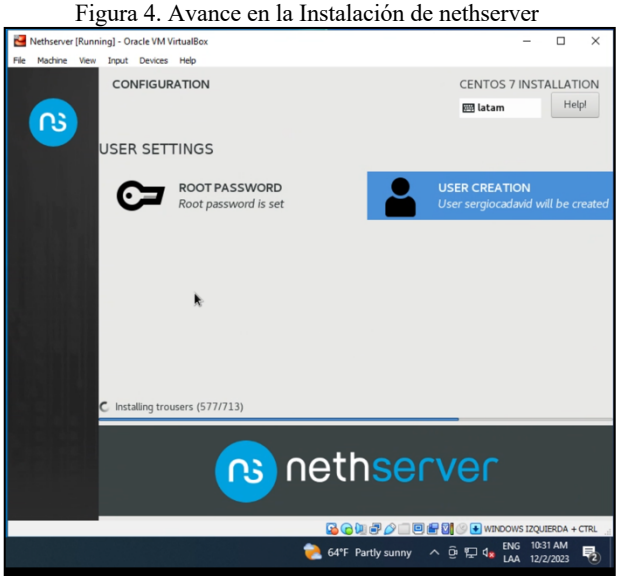


Fuente: Autoría Propia

Finalmente, el avance en la instalación de Nethserver se monitoriza hasta su conclusión. Este paso incluye la creación del usuario y contraseña del administrador, un aspecto vital para la seguridad y gestión del servidor.

En este pantallazo correspondiente a la figura 4 se visualiza el avance en la instalación del sistema operativo Nethserver en la máquina virtual. Se observa la configuración del password y del usuario administrador, asegurando que el sistema operativo esté protegido y listo para su configuración y uso.

Figura 4. Avance en la Instalación de nethserver



Fuente: Autoría Propia

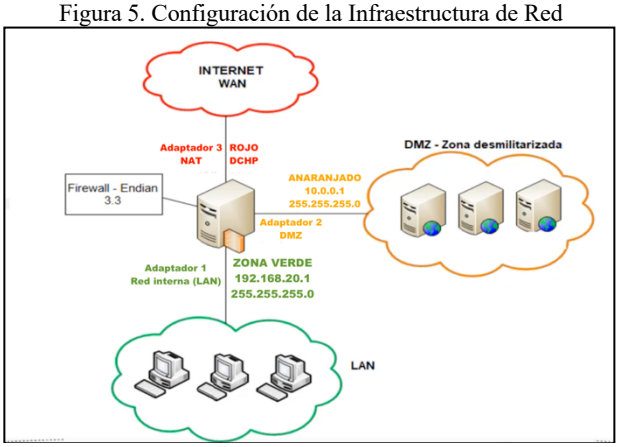
Una vez completada la instalación, la interfaz de usuario y la gestión del escritorio de Nethserver se convierten en el foco. Nethserver ofrece una interfaz gráfica intuitiva y fácil de usar, diseñada para facilitar la administración de los servicios y la configuración del sistema.

La interfaz de Nethserver permite a los administradores gestionar efectivamente la red, los servicios de seguridad, y las configuraciones del servidor sin necesidad de un profundo conocimiento en comandos de Linux. Esta accesibilidad es crucial para entornos donde la simplicidad y eficiencia en la gestión de TI son prioritarias.

En este contexto, la interfaz de usuario de Nethserver juega un papel fundamental, proporcionando un panel de control centralizado desde el cual se pueden administrar todos los aspectos del servidor. Este enfoque orientado al usuario garantiza que incluso los administradores con conocimientos limitados en GNU/Linux puedan gestionar eficientemente el servidor y sus servicios.

Para la implementación del ejercicio desarrollado, se utiliza inicialmente Endian Firewall para administrar la red. Esta herramienta se encarga de la asignación de IPs a través de DHCP y otros aspectos relacionados con la gestión de la red. En esta configuración, el servidor Nethserver se ubica en la zona DMZ (Zona Desmilitarizada), mientras que el cliente de Linux se sitúa en la zona verde, una área segura de la red. A continuación en la figura 5, podemos ver la configuración de la red.

Figura 5. Configuración de la Infraestructura de Red

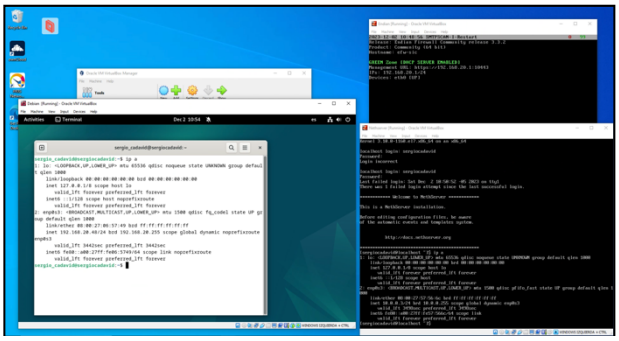


Fuente: Autoría Propia

Una representación gráfica es útil para ilustrar la distribución de las diferentes zonas, sus adaptadores de red y su configuración IP. Esto proporciona una comprensión clara de cómo se organiza la red y cómo se asignan las direcciones IP a los distintos segmentos.

Este la siguiente figura 6 se muestra que el equipo cliente ha sido configurado correctamente mediante DHCP en la zona verde, y que el servidor Nethserver está ubicado dentro del segmento de red DMZ. La visualización del correcto funcionamiento de la red es fundamental para verificar la eficacia de la configuración.

Figura 6. Evidencia del correcto funcionamiento de la red con Endian Firewall



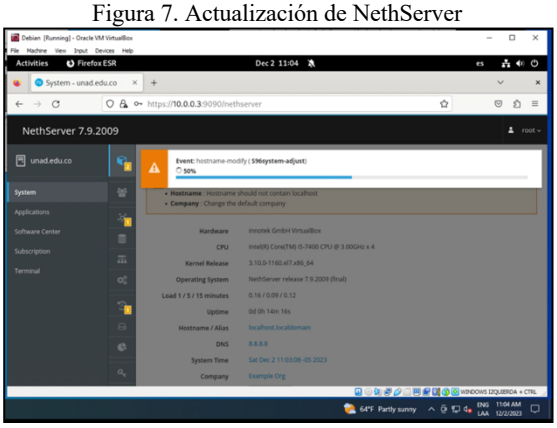
Fuente: Autoría Propia

Una vez completada la instalación de NethServer y la configuración de red de las máquinas virtuales, se procede a acceder al administrador web del servidor. Utilizando un navegador en el equipo cliente Linux Debian, se accede a NethServer mediante la dirección IP (10.0.0.3) y el puerto 9090. Este paso también incluye la actualización de los diferentes paquetes instalados en el servidor para garantizar su funcionamiento óptimo y seguridad.

Este pantallazo muestra la interfaz de configuración de red de NethServer, destacando la IP asignada al servidor. Es un aspecto crucial para asegurar que el servidor esté correctamente integrado en la red y accesible desde el cliente.

La actualización del sistema es un paso esencial en la configuración inicial. La siguiente figura 7 de la interfaz de NethServer muestra el proceso de actualización, subrayando la importancia de mantener el sistema al día para asegurar su seguridad y eficiencia.

Figura 7. Actualización de NethServer



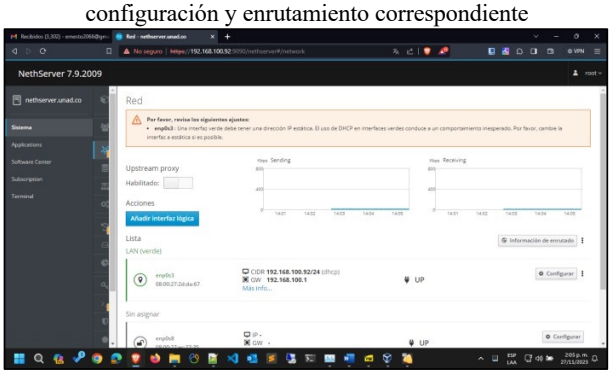
Fuente: Autoría Propia

3 IMPLEMENTACIÓN DE SERVICIOS DE RED DHCP y DNS EN NETHSERVER

La implementación eficaz de servicios de red en Nethserver es un componente crucial para una infraestructura de red robusta y eficiente, centrándose en la configuración y administración de los servicios DHCP y DNS.

Para la conectividad se realiza configuración de la red WAN para la interfaz enp0s3 por DHCP ya que esta red es la que va a brindar salida hacia internet. A continuación, se muestra la lista de interfaces que se encuentran configuradas en el hipervisor. (Figura 18) Este paso es esencial para la gestión eficiente del tráfico de red y el acceso a recursos externos.

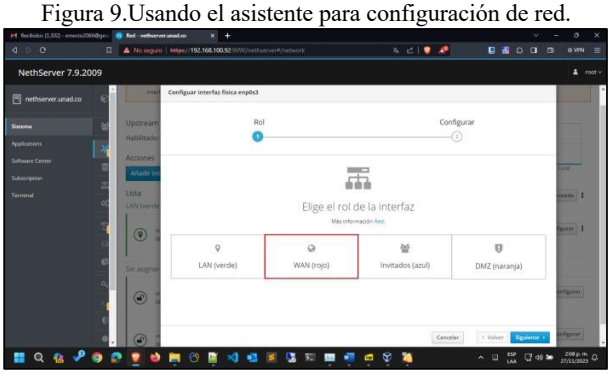
Figura 8. Listado de interfaces de red para hacer la configuración y enrutamiento correspondiente



Fuente: Autoría Propia

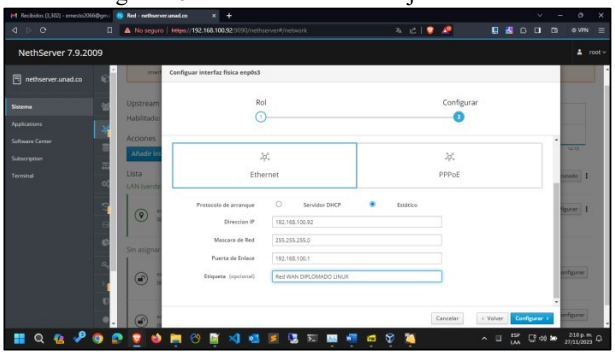
En la figura 9 y 10 se utiliza el asistente de la aplicación para hacer la configuración correspondiente en la interfaz de red.

Figura 9.Usando el asistente para configuración de red.



Fuente: Autoría Propia

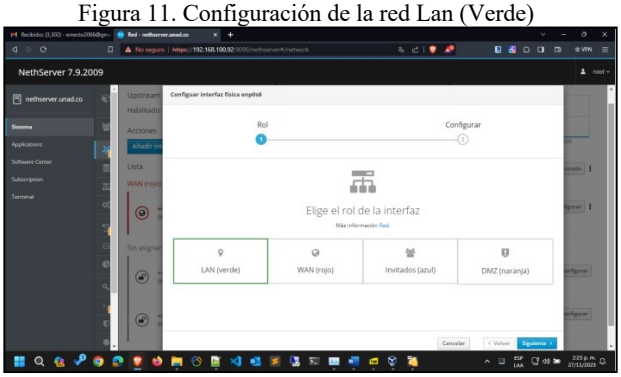
Figura 10.Enrutamiento de la tarjeta de red.



Fuente: Autoría Propia

La configuración de las demás interfaces de red sigue una estrategia codificada por colores para facilitar la identificación y gestión de las interfaces. (Figura 11)

Figura 11. Configuración de la red Lan (Verde)



Fuente: Autoría Propia

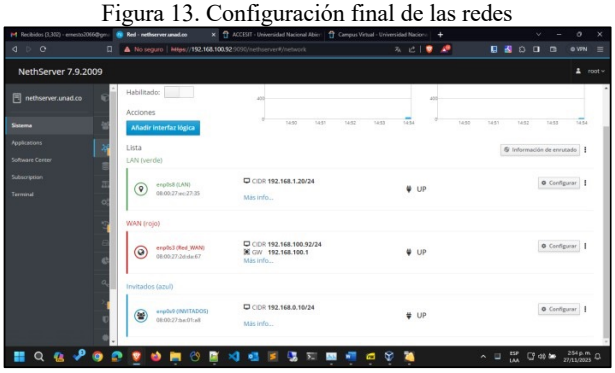
Además, se configura la red de invitados para segmentar y gestionar adecuadamente el tráfico de visitantes, esto permite una configuración de red segura y segmentada que permite tener flexibilidad en el manejo de permisos y seguridad en la gestión de red (Figura 12).

Figura 12. Configuración de la red de invitados (Azul)

Fuente: Autoría Propia

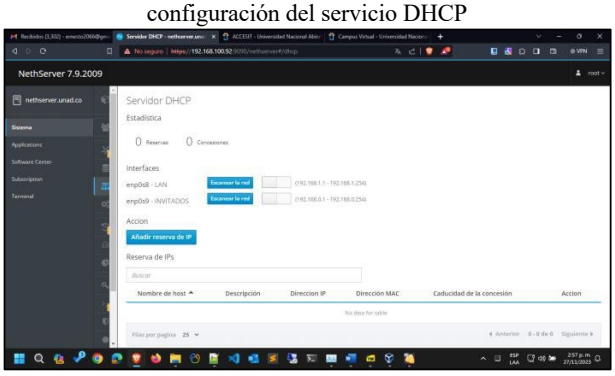
La configuración final de las redes se visualiza en la interfaz de la aplicación, confirmando la correcta configuración de los servicios de red (Figura 28).

Figura 13. Configuración final de las redes



El servidor DHCP se configura para la asignación dinámica de direcciones IP en los segmentos de red LAN e INVITADOS.

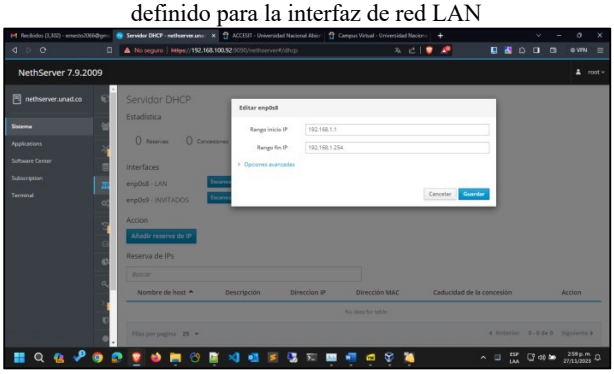
Figura 14. Validación de los segmentos de red en la configuración del servicio DHCP



Fuente: Autoría Propia

Ahora debemos activar la configuración correspondiente al segmento de red definido para la interfaz de red LAN (Verde) que se puede evidenciar en la Figura 15. Editando el rango de IPs que aplica para este.

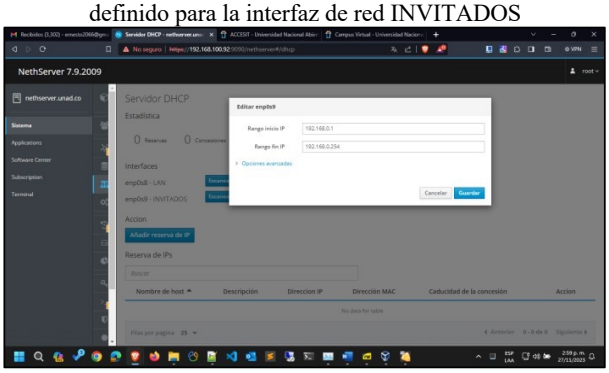
Figura 15. Activando la configuración con el segmento de red definido para la interfaz de red LAN



Fuente: Autoría Propia

Ahora debemos activar la configuración correspondiente al segmento de red definido para la interfaz de red Invitados (Azul) que se puede evidenciar en la Figura 16. Editando el rango de IPs que aplica para este.

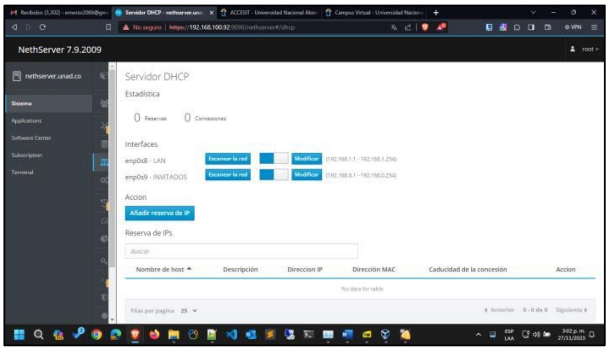
Figura 16. Activando la configuración con el segmento de red definido para la interfaz de red INVITADOS



Fuente: Autoría Propia

La correcta configuración de los segmentos de red se verifica al finalizar la configuración, aquí se puede ver la correcta configuración de los segmentos de red LAN e Invitados (Figura 17).

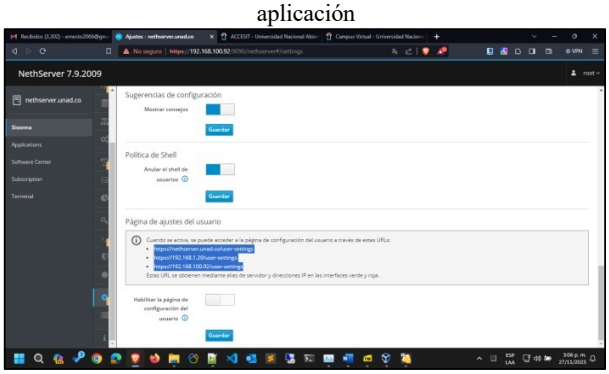
Figura 17. Segmentos de red correctamente configurados al finalizar la maniobra realizada



Fuente: Autoría Propia

En esta opción de la aplicación se puede evidenciar las páginas de configuración que genera acorde el segmento de red realizamos la prueba de comunicación con la maquina cliente para verificar que el controlador de dominio esta activo. (Figura 18)

Figura 18. Páginas de configuración de los segmentos de la aplicación

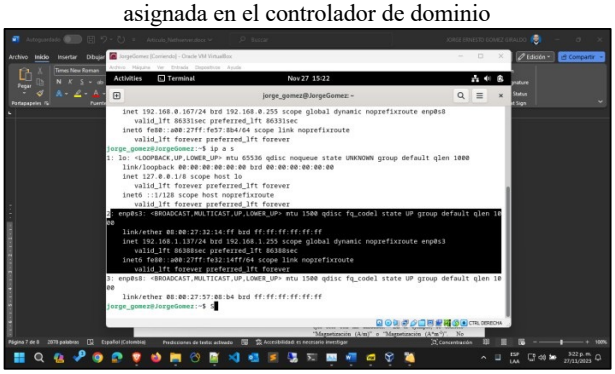


Fuente: Autoría Propia

Finalmente, se realizan pruebas de comunicación con la máquina cliente para confirmar el correcto funcionamiento del DHCP y del DNS. Para esto iniciamos una nueva máquina virtual que hará las veces de cliente.

Después de encender la maquina cliente en la red interna podemos evidenciar que se le asigna direccionamiento de manera correcta (Figura 19), esto confirma que el DHCP esta funcional ya que le fue asignada una dirección IP definida dentro del rango de configuración para esta red.

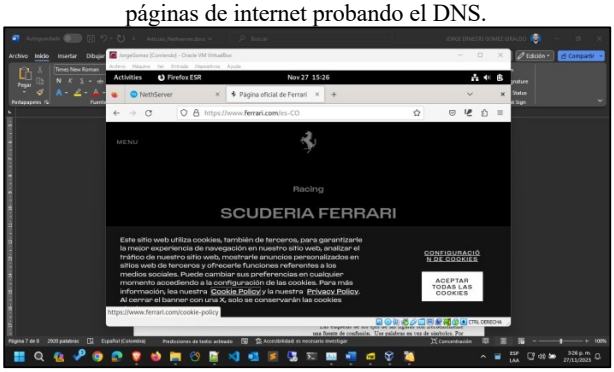
Figura 19. Maquina cliente con la configuración de red asignada en el controlador de dominio



Fuente: Autoría Propia

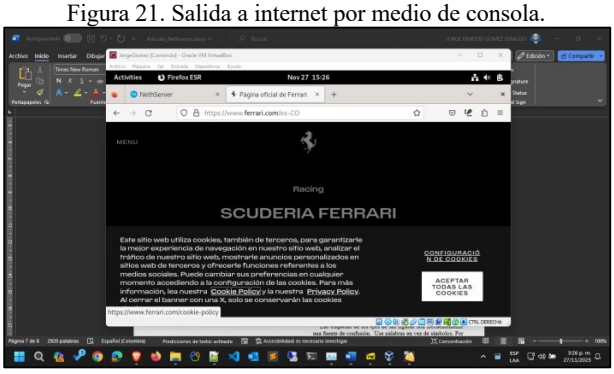
Adicional a esto podemos validar que el DNS también está funcionando ya que la maquina ha tomado automáticamente por DHCP la configuración de los servidores DNS, esto lo podemos validad ingresando al navegador y tratando de probar la conexión a internet, validando que el navegador está resolviendo de manera correcta las páginas de internet (Figura 20). También podemos validar esto por medio de un ping en la consola o terminal de Linux. (Figura 21) Incluyendo la asignación correcta de direcciones IP y la resolución de nombres de dominio

Figura 20. Verificación de salida a internet resolviendo páginas de internet probando el DNS.



Fuente: Autoría Propia

Figura 21. Salida a internet por medio de consola.

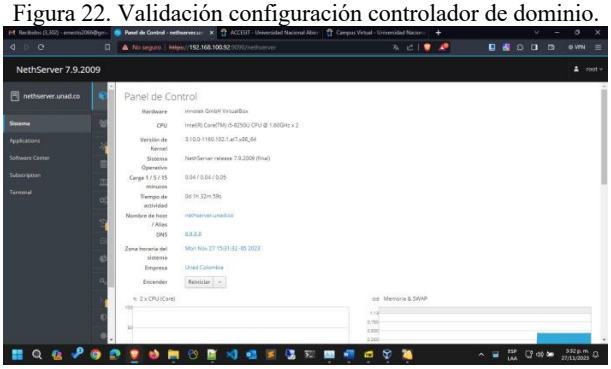


Fuente: Autoría Propia

La configuración exitosa del controlador de dominio, como se evidencia en la Figura 22, marca un hito significativo en la implementación de la infraestructura IT utilizando Nethserver en un entorno GNU/Linux. Esto demuestra la correcta integración y comunicación del controlador de dominio con las máquinas clientes en la red interna especialmente configurada para esta actividad.

La configuración detallada y precisa no solo cumple con los objetivos específicos de la temática seleccionada, sino que también subraya la eficiencia y la capacidad del sistema para gestionar de manera efectiva la autenticación y el acceso a los recursos en la red.

Figura 22. Validación configuración controlador de dominio.



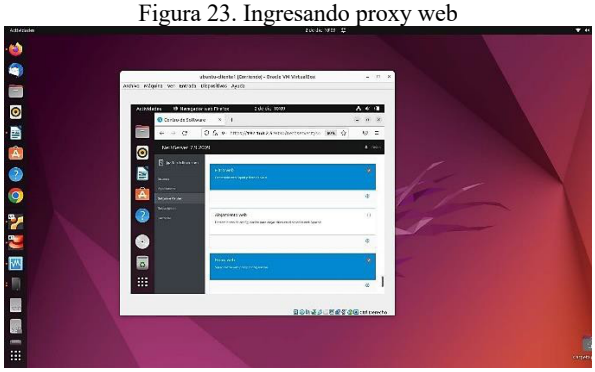
Fuente: Autoría Propia

4 SEGURIDAD EN LA RED: PROXY Y CORTAFUEGOS

4.1 INSTALACIÓN DE PROXY WEB Y WEB FILTER

En el proceso de configuración del Proxy en NethServer, se lleva a cabo la instalación de las aplicaciones "Proxy web" y "Filtro Web". Esta acción es esencial para implementar y gestionar un servidor proxy que filtra el tráfico de Internet, proporcionando un control más granular sobre el acceso a sitios web y mejorando la seguridad en la red.

Figura 23. Ingresando proxy web



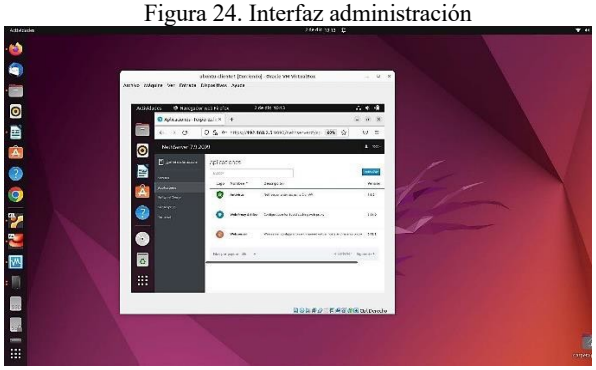
Fuente: Autoría Propia

Después de realizar la instalación de las aplicaciones "Proxy web" y "Filtro Web", procedemos a verificar el estado del servicio accediendo a la sección de "Aplicaciones" en la interfaz de administración de NethServer. Al ingresar a esta sección, confirmamos que el servicio "Web Proxy & filter" está correctamente instalado y disponible para su configuración.

4.2 ACCESO A LA SECCIÓN DE APLICACIONES

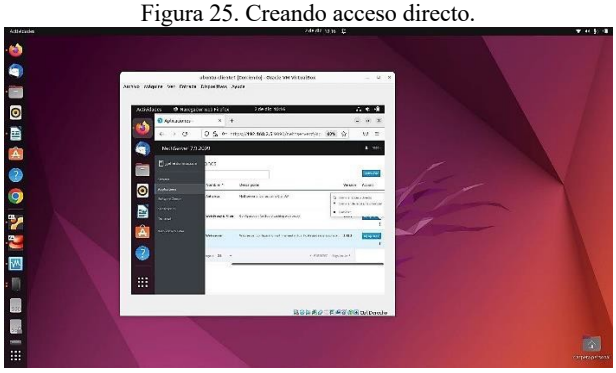
Ingresamos a la interfaz de administración de NethServer y nos dirigimos a la sección de "Aplicaciones". Esta sección proporciona una vista centralizada de las aplicaciones instaladas en el servidor, incluyendo el estado actual de cada servicio.

Figura 24. Interfaz administración



Fuente: Autoría Propia

Figura 25. Creando acceso directo.



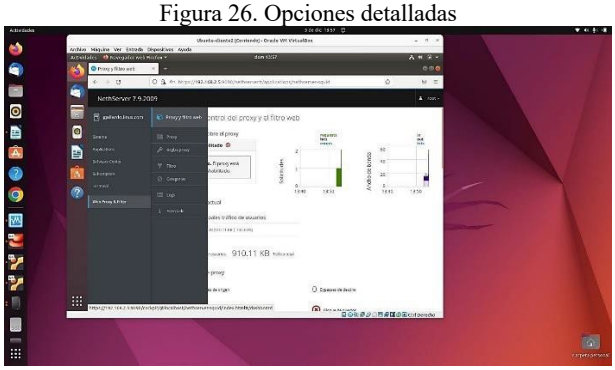
Fuente: Autoría Propia

Al seleccionar la opción "Web Proxy & filter" dentro de la sección de "Aplicaciones" en la interfaz de administración de NethServer, se despliega una ventana que presenta una variedad de acciones para configurar y administrar el servicio. Esta interfaz intuitiva proporciona a los administradores un conjunto completo de herramientas para adaptar el comportamiento del proxy web y el filtro según las necesidades específicas de la red.

4.3 CONFIGURACIÓN DETALLADA

Al hacer clic en "Web Proxy & filter", se accede a una pantalla que ofrece opciones detalladas para la configuración del servicio. Aquí, los administradores pueden definir reglas de acceso, establecer políticas de filtrado, y ajustar parámetros relacionados con el rendimiento y la seguridad del servicio.

Figura 26. Opciones detalladas



Fuente: Autoría Propia

Una vez dentro de la interfaz de configuración de "Web Proxy & filter", al hacer clic en el botón correspondiente, se despliega una serie de opciones avanzadas. Entre estas opciones, elegimos "SSL Transparente" para habilitar la inspección de tráfico seguro (SSL/TLS) de manera transparente. Este paso es significativo para mejorar la visibilidad y el control sobre el tráfico cifrado, contribuyendo a la seguridad y al cumplimiento de políticas en la red.

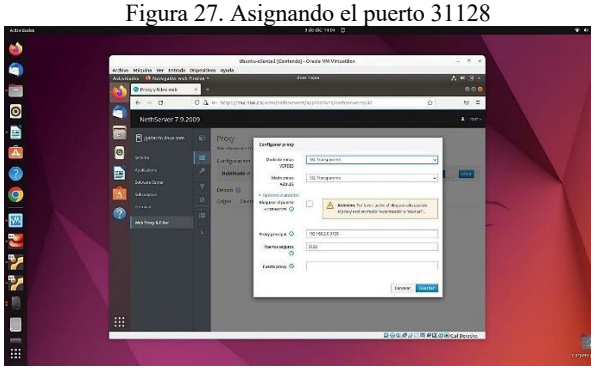
4.4 SELECCIÓN DE SSL TRANSPARENTE

La opción "SSL Transparente" permite al proxy web inspeccionar y filtrar el tráfico cifrado sin que los usuarios finales tengan que realizar ajustes manuales en sus configuraciones. Esto es esencial para aplicar políticas de seguridad y filtrado de manera efectiva, incluso en el caso de conexiones cifradas.

4.5 CONFIGURACIÓN DEL PUERTO 3128

En conjunto con la selección de "SSL Transparente", asignamos el puerto "3128" para la gestión del tráfico SSL/TLS. Este puerto específico se utiliza para la comunicación segura entre el cliente y el servidor proxy, asegurando que las interacciones relacionadas con SSL/TLS se manejen de manera eficiente y segura.

Figura 27. Asignando el puerto 31128



Fuente: Autoría Propia

Guardamos y tenemos configurado nuestro proxy en el servidor NethServer:

Figura 28. Validando proxy

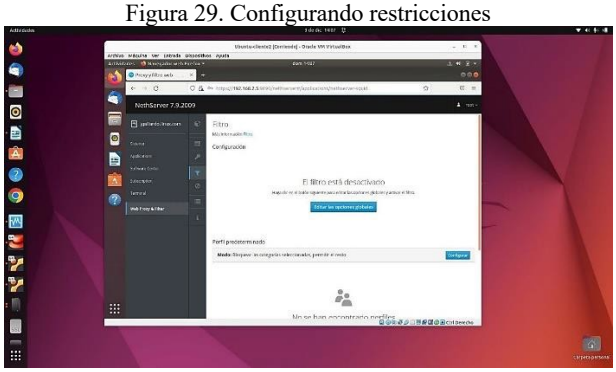
Fuente: Autoría Propia

Dentro de la interfaz de configuración de "Web Proxy & filter", procedemos a la sección de "Filtro" y establecemos las restricciones que el proxy deberá controlar. Esta etapa es esencial para la aplicación de políticas de filtrado web que regulan el acceso a determinadas categorías de sitios y contenido en línea.

4.6 CONFIGURACIÓN DE RESTRICCIONES EN LA SECCIÓN DE FILTRO

Al seleccionar la opción de "Filtro", se despliega un conjunto de configuraciones que permiten definir las restricciones y políticas de acceso a sitios web. Aquí, los administradores pueden especificar las categorías que desean bloquear o permitir, estableciendo así las pautas para el comportamiento del filtro web.

Figura 29. Configurando restricciones



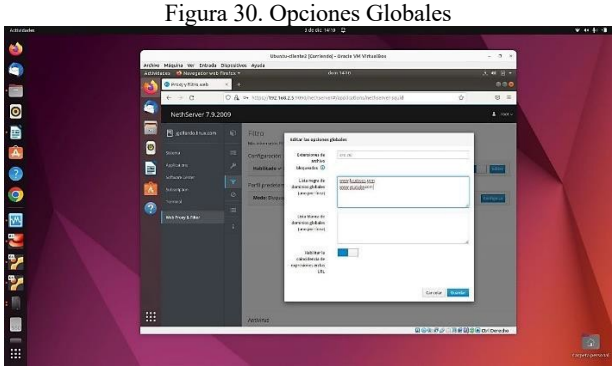
Fuente: Autoría Propia

En la interfaz de configuración de "Web Proxy & filter", accedemos a la sección de "Opciones Globales" para editar las configuraciones globales del proxy web. En esta ventana, se nos brinda la capacidad de limitar ciertas acciones, como el acceso a determinadas páginas web y la descarga de archivos, estableciendo así restricciones globales que afectan a todo el tráfico a través del proxy.

4.7 EDICIÓN DE OPCIONES GLOBALES

Al seleccionar la sección de "Opciones Globales", se despliega una ventana que ofrece configuraciones a nivel global que afectan el comportamiento del proxy web para todo el tráfico que pasa a través de él. Aquí, los administradores pueden editar diversas opciones que impactan directamente en cómo se gestionan y controlan las acciones de los usuarios en la red.

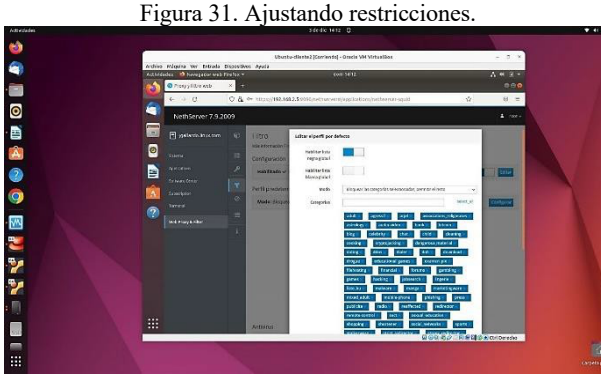
Figura 30. Opciones Globales



Fuente: Autoría Propia

Dentro de la configuración de "Web Proxy & filter", nos dirigimos a la sección de "Modo" para ajustar las restricciones y controlar con mayor precisión el acceso a ciertas páginas en Internet. En esta opción, se presenta la capacidad de aplicar restricciones adicionales, brindando a los administradores la flexibilidad de personalizar las políticas de filtrado web para cumplir con los requisitos específicos de seguridad y uso de la red.

Figura 31. Ajustando restricciones.



Fuente: Autoría Propia

Entramos a uno de nuestros clientes y verificamos que tenga acceso a internet, de esta manera verificaremos el correcto funcionamiento de las configuraciones anteriormente realizadas:

Figura 32. Verificando acceso a internet.

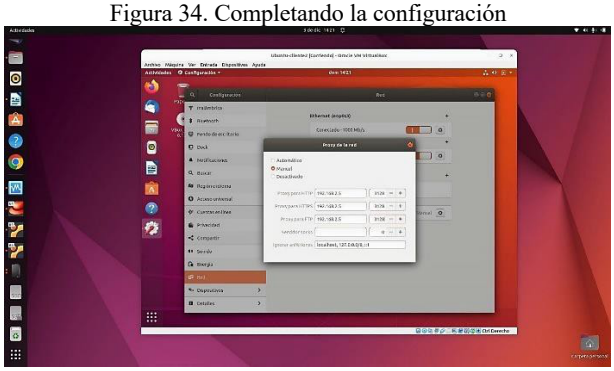
Fuente: Autoría Propia

En el cliente, procedemos a la configuración de redes y activamos el servicio de Web Proxy que previamente hemos configurado en NethServer. Esta acción es fundamental para dirigir el tráfico de Internet del cliente a través del servidor proxy, aprovechando las políticas y restricciones establecidas en NethServer para mejorar la seguridad y el control de acceso a la red.

Figura 33. Activando servicio Web Proxy

Fuente: Autoría Propia

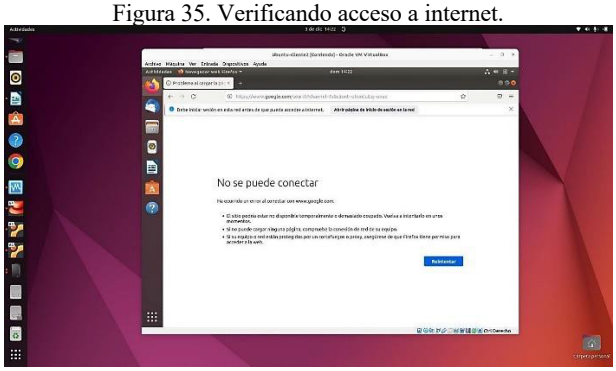
Figura 34. Completando la configuración



Fuente: Autoría Propia

Ingresamos nuevamente al navegador y verificamos que ya no tenemos acceso a internet:

Figura 35. Verificando acceso a internet.



Fuente: Autoría Propia

El proceso integral de implementación y configuración del sistema de Proxy en una estación de trabajo GNU/Linux, basada en NethServer, ha culminado con éxito, ofreciendo una solución robusta para el control efectivo del acceso a los servicios de conectividad a Internet.

5 SERVICIO DE CORTAFUEGOS

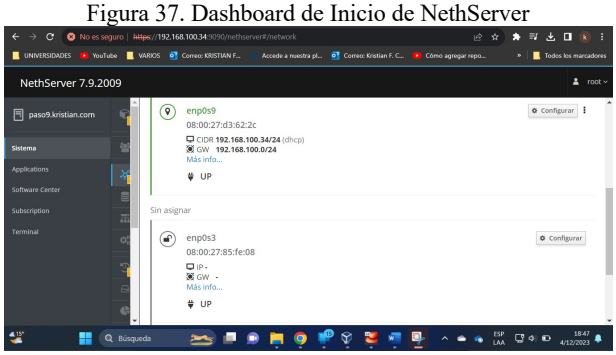
5.1 CONFIGURACIÓN INICIAL DEL CORTAFUEGOS

Al iniciar el NethServer, es posible acceder a la interfaz de usuario a través de la URL https://192.168.100.34:9090/ utilizando las credenciales de usuario y contraseña 'root'. Este acceso nos lleva directamente al 'Dashboard' de NethServer, donde se pueden observar y gestionar las diferentes configuraciones.

Figura 36. Interfaz URL de NethServer

Fuente: Autoría Propia

Figura 37. Dashboard de Inicio de NethServer

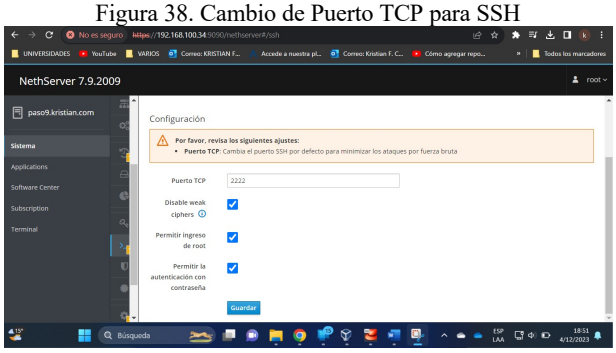


Fuente: Autoría Propia

5.2 CONFIGURACIÓN DEL SHELL SEGURO Y PUERTOS

Dentro de la configuración del sistema, se localiza la opción "Shell seguro". Aquí, se modifica el número de puerto, que por defecto es el 22, cambiándolo al 2222. Este cambio es una medida de seguridad adicional para evitar accesos no autorizados.

Figura 38. Cambio de Puerto TCP para SSH



Fuente: Autoría Propia

5.3 CONFIGURACIÓN DE REDES LAN, WAN Y DMZ

El siguiente paso involucra la configuración de las direcciones IP de las redes LAN, WAN y DMZ. Se ajustan las configuraciones en cada una de las tarjetas de red, asignando los segmentos y métodos de direccionamiento adecuados para las redes 'naranja', 'roja' y 'verde'.

Figura 39. Configuración de Redes

Fuente: Autoría Propia

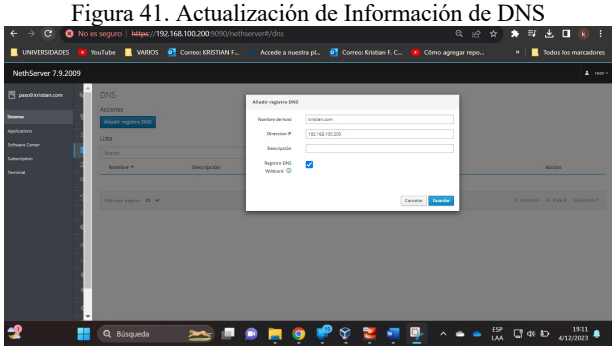
Figura 40. Redes Configuradas

Fuente: Autoría Propia

5.4 CONFIGURACIÓN DE DNS Y DHCP

En el apartado de DNS, se crea un nuevo servidor DNS, asignando los datos correspondientes y guardando los cambios. Posteriormente, se selecciona el apartado de DHCP para definir el rango de direcciones IP que se entregarán en la red LAN.

Figura 41. Actualización de Información de DNS



Fuente: Autoría Propia

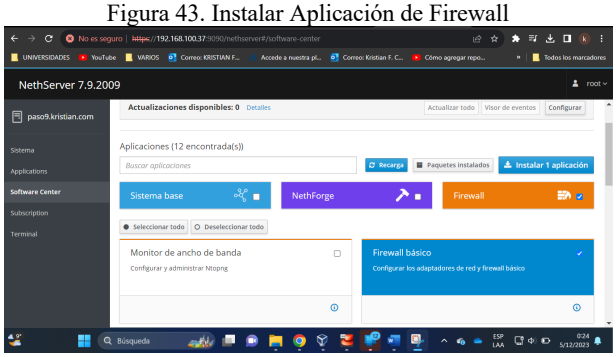
Figura 42. Configuración de DHCP

Fuente: Autoría Propia

5.5 INSTALACIÓN Y CONFIGURACIÓN DEL CORTAFUEGOS

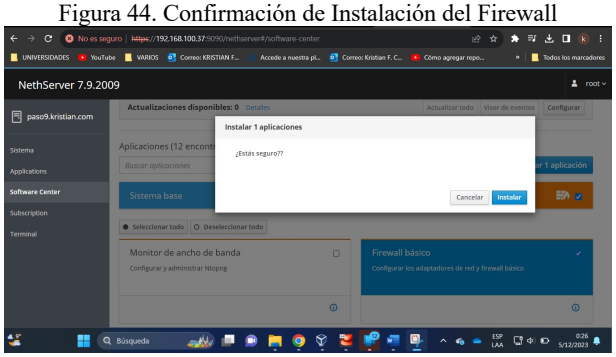
A continuación, se accede al 'Software Center', donde en la sección de aplicaciones se ubica y selecciona la opción de 'Firewall'. Se procede a instalar la aplicación de cortafuegos.

Figura 43. Instalar Aplicación de Firewall



Fuente: Autoría Propia

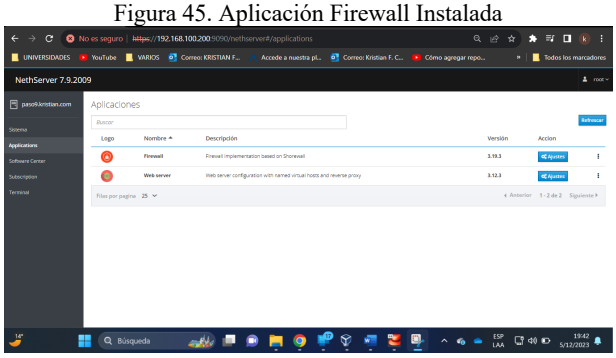
Figura 44. Confirmación de Instalación del Firewall



Fuente: Autoría Propia

Una vez finalizada la instalación, el firewall estará disponible en la sección de "Aplicaciones".

Figura 45. Aplicación Firewall Instalada

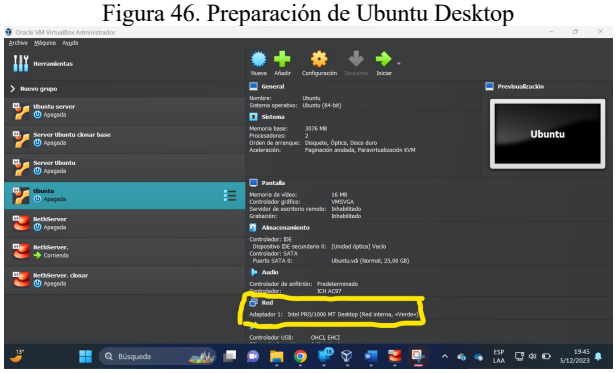


Fuente: Autoría Propia

5.6 PREPARACIÓN DE CLIENTE UBUNTU DESKTOP

Se prepara una máquina con Ubuntu Desktop configurando su tarjeta de red para conectar con la red interna en el segmento 'verde'.

Figura 46. Preparación de Ubuntu Desktop



Fuente: Autoría Propia

5.7 CONFIGURACIÓN DEL FILTRO WEB

Se agrega también la aplicación de filtro web desde el Software Center. Dentro de la opción de filtro, se configura el perfil predeterminado eligiendo las categorías que se desean permitir y bloquear.

Figura 47. Agregar Filtro Web

Fuente: Autoría Propia

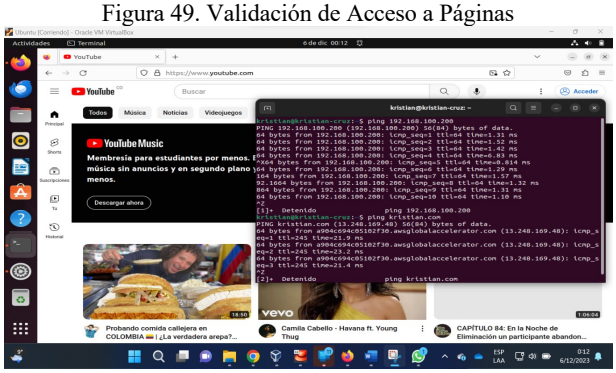
Figura 48. Configuración de Categorías en el Filtro Web

Fuente: Autoría Propia

5.8 VALIDACIÓN DE ACCESO Y USO DEL CORTAFUEGOS

Se verifica que el cliente Ubuntu Desktop tenga conexión a Internet y acceso a páginas como YouTube, Facebook y otras, sobre un segmento diferente al creado en NethServer.

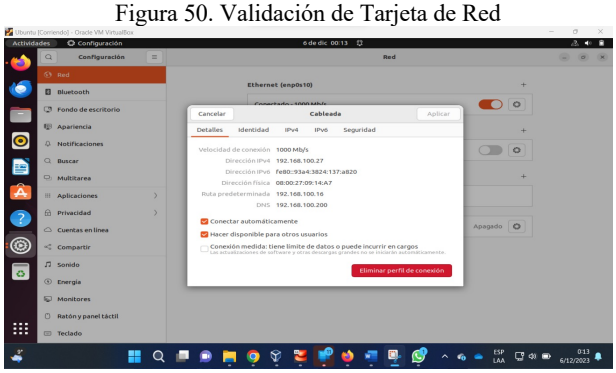
Figura 49. Validación de Acceso a Páginas



Fuente: Autoría Propia

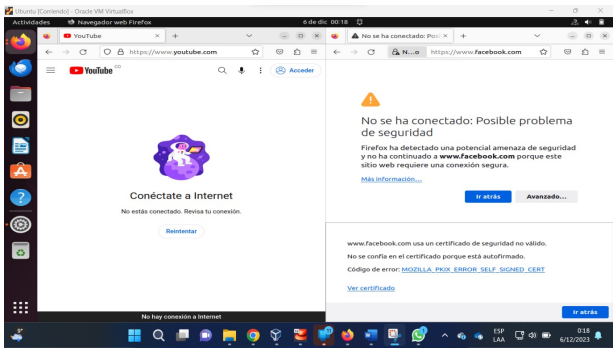
Posteriormente, se configura la tarjeta de red en DHCP para que tome el direccionamiento configurado en NethServer. Al intentar acceder a páginas de redes sociales y de videos, se observa que el cortafuegos está bloqueando correctamente el acceso.

Figura 50. Validación de Tarjeta de Red



Fuente: Autoría Propia

Figura 51. Validación de Denegación de Páginas por el Firewall



Fuente: Autoría Propia

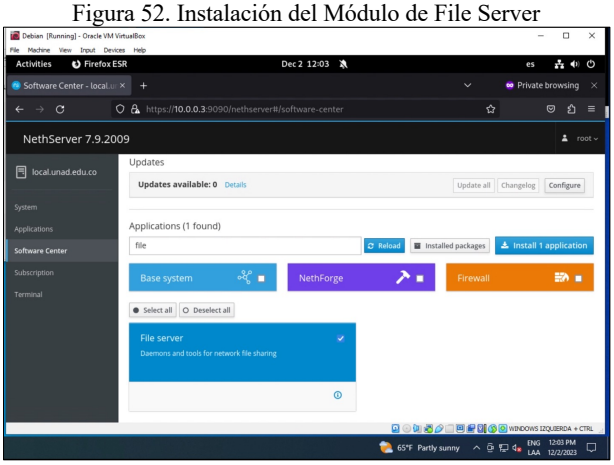
6 SERVICIOS DE ALMACENAMIENTO Y ACCESO: FILE Y PRINT SERVER

6.1 CONFIGURACIÓN DE FILE SERVER

Un File Server, o servidor de archivos, es una entidad crucial en cualquier red que permite almacenar, gestionar y acceder a archivos desde múltiples clientes. Su función es centralizar recursos de almacenamiento en un solo lugar, facilitando la administración y el acceso compartido de archivos. [1]

Antes de la instalación, es necesario actualizar los paquetes de la instalación base de NethServer. Posteriormente, en el "Software Center" de NethServer, se selecciona e instala el módulo File Server. Este paso es fundamental para habilitar la función de almacenamiento y compartición de archivos en la red. (Figura 52)

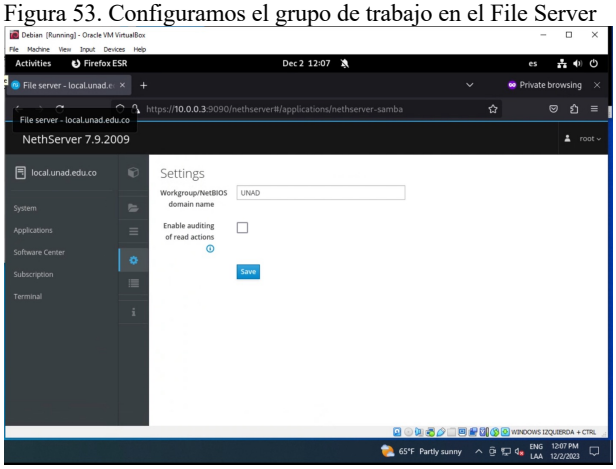
Figura 52. Instalación del Módulo de File Server



Fuente: Autoría Propia

Tras la instalación, se procede a configurar el grupo de trabajo para el servidor de archivos, en este caso, UNAD. Esta configuración es crucial para la organización y el acceso correcto en una red de dominio. (Figura 53)

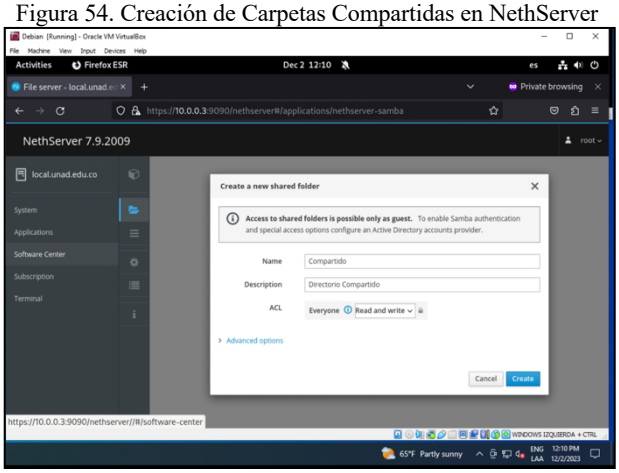
Figura 53. Configuramos el grupo de trabajo en el File Server



Fuente: Autoría Propia

Finalmente, se configuran las carpetas compartidas en el File Server, asignando los permisos adecuados. Este paso asegura que los usuarios autorizados puedan acceder y modificar los archivos compartidos, manteniendo la seguridad y la integridad de los datos. (Figura 54)

Figura 54. Creación de Carpetas Compartidas en NethServer



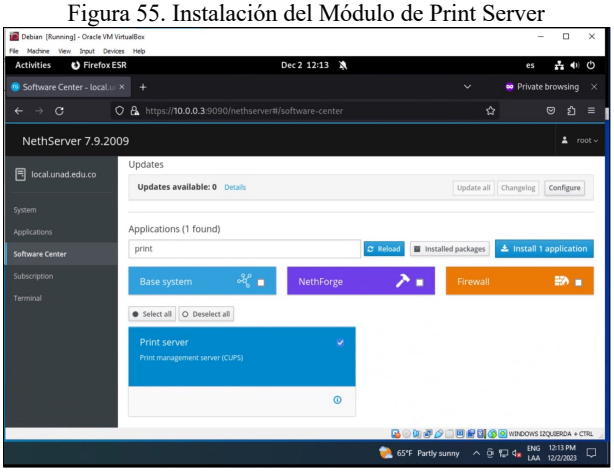
Fuente: Autoría Propia

6.2 CONFIGURACIÓN DE PRINT SERVER

Un Print Server, o servidor de impresión, administra las impresoras en una red y centraliza las tareas de impresión. [2] Esta es una pieza esencial en la infraestructura de TI de cualquier organización, facilitando la gestión centralizada de tareas de impresión. Su importancia radica en su capacidad para administrar eficientemente múltiples impresoras y solicitudes de impresión de diversos usuarios en una red. Al centralizar la gestión de impresoras, un Print Server reduce la carga de trabajo en los equipos individuales, optimiza el tráfico de red y mejora la seguridad de la información impresa.

Este paso comienza con la instalación del Print Server en NethServer a través del "Software Center". Este proceso integra el servidor de impresión en la red. (Figura 55)

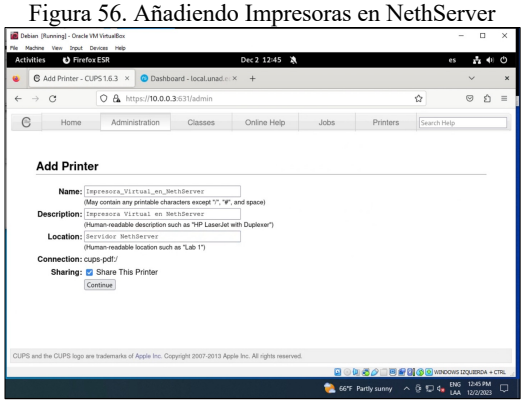
Figura 55. Instalación del Módulo de Print Server



Fuente: Autoría Propia

Después de instalar el Print Server, se procede a configurar una impresora virtual de PDF. Este paso demuestra la capacidad del Print Server de NethServer para gestionar diferentes tipos de impresoras, adaptándose a las necesidades específicas de la red. (Figura 56)

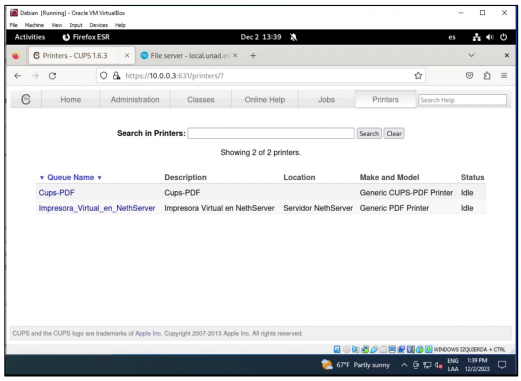
Figura 56. Añadiendo Impresoras en NethServer



Fuente: Autoría Propia

Posterior a la creación de la impresora, podemos desplegar la lista de dispositivos para ver su correcta configuración. (Figura 57).

Figura 57. Impresoras en NethServer



Fuente: Autoría Propia

6.3 CONFIGURACIÓN DEL CONTROLADOR DE DOMINIO LDAP

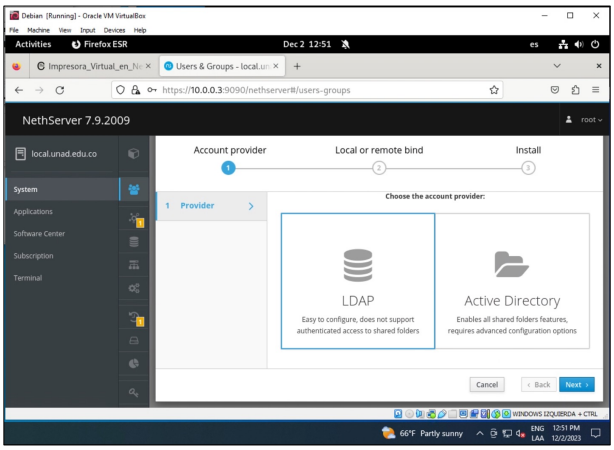
El controlador de dominio LDAP en un entorno NethServer es un componente crucial para la gestión de la seguridad y el acceso a los recursos en una red corporativa o educativa. [3] LDAP (Lightweight Directory Access Protocol) es un protocolo estandarizado para la administración de información relacionada con usuarios y servicios en una red.

La implementación de un controlador de dominio LDAP en NethServer facilita la administración de cuentas de usuario, grupos, políticas de acceso y otros datos de directorio de manera eficiente y segura. Este sistema es esencial para garantizar la autenticación y autorización adecuadas de los usuarios, permitiendo un control detallado sobre quién puede acceder a qué recursos en la red.

Además, el uso de LDAP mejora la escalabilidad y la flexibilidad de la infraestructura de TI, ya que permite integrar fácilmente con otros servicios y aplicaciones, manteniendo al mismo tiempo un alto nivel de seguridad y coherencia en la gestión de identidades y accesos.

Como primer paso para su implementación, se instala y configura el servicio LDAP en NethServer, lo cual es esencial para administrar grupos de usuarios y políticas de acceso en la red. (Figura 58)

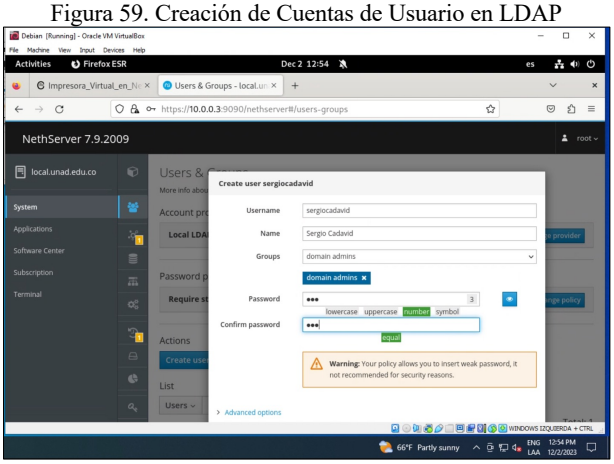
Figura 58. Instalación y Configuración de LDAP en NethServer



Fuente: Autoría Propia

Tras configurar LDAP, se crean cuentas de usuario. Este paso es crucial para el control de acceso y la autenticación en la red, permitiendo a los usuarios acceder a los recursos compartidos y las impresoras. (Figura 59)

Figura 59. Creación de Cuentas de Usuario en LDAP

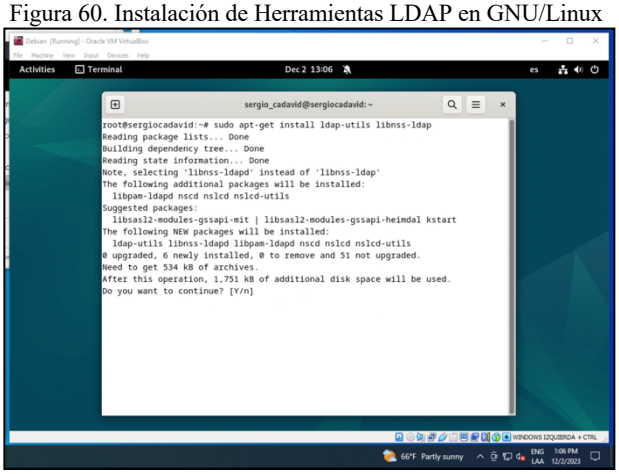


Fuente: Autoría Propia

6.4 CONFIGURACIÓN Y COMPROBACIÓN DE ACCESO DESDE ESTACIÓN DE TRABAJO GNU/LINUX

Para acceder a los recursos de NethServer desde un cliente GNU/Linux, se instalan las herramientas LDAP en el cliente GNU/Linux y se configura el acceso al servidor LDAP usando el gestor de paquetes apt-get de Linux Debian. Este paso permite al cliente acceder a los recursos compartidos de NethServer. (Figura 60)

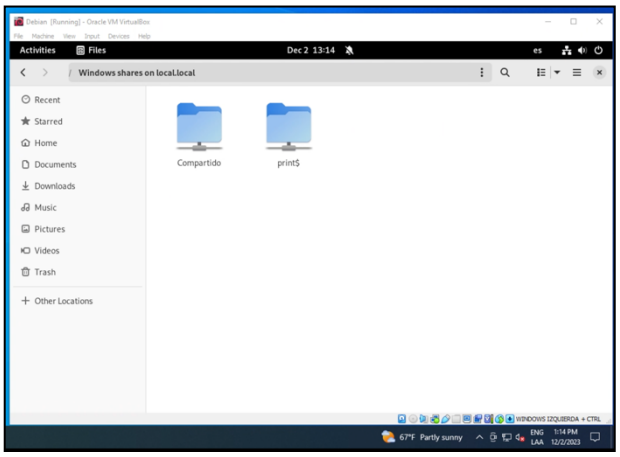
Figura 60. Instalación de Herramientas LDAP en GNU/Linux



Fuente: Autoría Propia

Finalmente, como parte crucial del proceso de configuración, se lleva a cabo la verificación del acceso a las carpetas compartidas desde el cliente GNU/Linux. Este paso es esencial para confirmar que la configuración realizada en el servidor Nethserver ha sido exitosa y que los recursos compartidos son plenamente accesibles en la red. Durante esta fase de verificación, se comprueba la capacidad de los usuarios en la estación de trabajo GNU/Linux para acceder a las carpetas compartidas, abrir archivos y, dependiendo de los permisos asignados, modificar o añadir nuevos contenidos.

Figura 46. Listado de recursos compartidos en el servidor NethServer

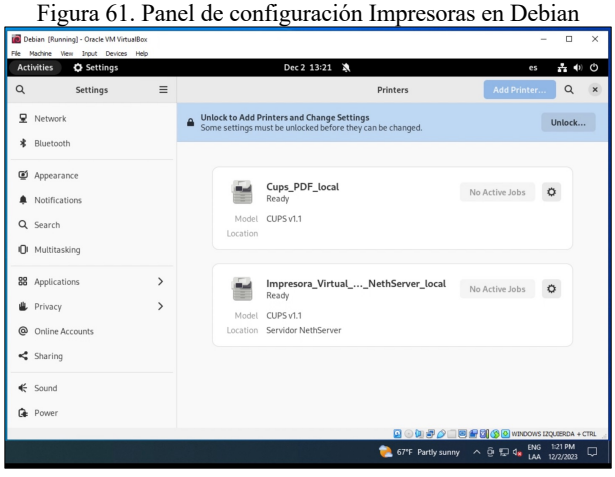


Fuente: Autoría Propia

6.5 COMPROBACIÓN DE ACCESO A LA IMPRESORA COMPARTIDA DESDE GNU/LINUX

Como último paso, se accede al gestor de impresoras en Debian para confirmar la visibilidad y configuración de la impresora virtual instalada en el servidor NethServer. (Figura 61)

Figura 61. Panel de configuración Impresoras en Debian



Fuente: Autoría Propia

En resumen, la configuración y gestión de servicios de almacenamiento, acceso e impresión en NethServer representa un componente vital para el mantenimiento de una infraestructura de TI eficiente y segura. A lo largo de este artículo, hemos detallado cómo la implementación de un File Server y un Print Server en NethServer puede centralizar y simplificar el manejo de recursos compartidos y tareas de impresión en una red, ofreciendo soluciones escalables y accesibles para organizaciones de cualquier tamaño. Además, la integración del controlador de dominio LDAP en NethServer demuestra la importancia de una gestión de identidades y accesos eficiente, asegurando un alto nivel de seguridad y un control detallado sobre los recursos de la red.

Estos servicios no solo mejoran la eficiencia operativa y la seguridad de la red, sino que también ofrecen una flexibilidad y escalabilidad significativas, lo que es esencial en el dinámico entorno tecnológico actual. La facilidad de configuración y gestión de estos servicios en NethServer, como se ha demostrado a través de los pasos y pantallazos presentados, subraya la viabilidad de GNU/Linux y NethServer como una opción robusta para la administración de sistemas en diversos entornos empresariales y educativos.

Al concluir, este artículo no solo proporciona una guía práctica para configurar estos servicios esenciales en NethServer, sino que también refuerza la idea de que la adopción de soluciones basadas en GNU/Linux puede resultar en una infraestructura de TI más eficiente, segura y adaptable, alineada con las necesidades cambiantes de las organizaciones modernas.

7 ESTABLECIMIENTO DE REDES PRIVADAS VIRTUALES (VPN)

7.1 INTRODUCCIÓN A LAS VPNS

Una VPN (Red Privada Virtual) es una tecnología de red que permite una extensión segura de una red local sobre una red pública o no controlada, como Internet. Proporciona la funcionalidad necesaria para enviar y recibir datos a través de redes públicas o compartidas como si estuvieran directamente interconectadas a una red privada. Las VPNs son ampliamente utilizadas tanto en entornos corporativos como individuales para asegurar conexiones y proteger datos sensibles.

7.2 PRINCIPALES CARACTERÍSTICAS Y BENEFICIOS DE LAS VPNS

Cifrado de Datos: La VPN utiliza protocolos de cifrado avanzados para asegurar que los datos transmitidos permanezcan inaccesibles e ilegibles para los usuarios no autorizados.

Anonimato: Ofrece a los usuarios la capacidad de navegar con una identidad oculta y desde una ubicación geográfica diferente, lo que es crucial para la privacidad en línea.

Acceso Remoto Seguro: Permite a los empleados acceder a la red corporativa de forma segura desde ubicaciones remotas, lo que es esencial para el trabajo a distancia.

Bypass de Restricciones Geográficas: Posibilita el acceso a contenido en línea que puede estar restringido en ciertas regiones.

Seguridad en Redes Públicas: Protege los datos de los usuarios cuando se conectan a redes Wi-Fi públicas, que son más vulnerables a los ataques.

7.3 DESCARGA E INSTALACIÓN DE ZENTYAL

Se procede a realizar la descarga del Zentyal desde la web configuración y enrutamiento correspondiente; Zentyal es una distribución de servidor Linux que se centra en proporcionar soluciones integrales para pequeñas y medianas empresas (PYMES). Está diseñado para ser una alternativa fácil de usar y asequible a otras soluciones de servidor más complejas. Zentyal combina varios servicios y aplicaciones comunes en un único paquete, lo que facilita la administración y el mantenimiento de servidores para usuarios con menos experiencia técnica.

Figura 62. Descarga de Zentyal

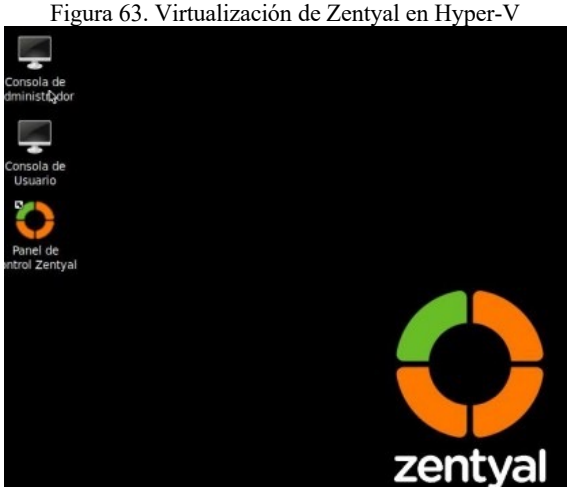
Fuente: Autoría Propia

7.4 CONFIGURACIÓN DE ZENTYAL Y VIRTUALIZACIÓN CON HYPER-V

Se utiliza Hyper-V para la virtualización del sistema, montando la ISO de Zentyal en una máquina virtual.

El término "Hypervisor" se refiere a un software de virtualización que permite la ejecución de múltiples sistemas operativos en una misma máquina física. En el contexto de Windows, hay dos tipos principales de hipervisores: el "Hypervisor de Tipo 1" y el "Hypervisor de Tipo 2".

Figura 63. Virtualización de Zentyal en Hyper-V



Fuente: Autoría Propia

7.5 INSTALACIÓN Y CONFIGURACIÓN DEL MÓDULO VPN EN ZENTYAL

La instalación del módulo VPN en Zentyal representa un paso fundamental en la configuración de una infraestructura de red segura y eficiente. Este módulo es crucial para establecer conexiones seguras y cifradas, que son vitales para proteger los datos durante su tránsito a través de la red. Al habilitar la VPN, Zentyal crea un "túnel" virtual, en el cual la información se transmite encriptada, protegiéndola así contra interceptaciones no autorizadas o accesos malintencionados.

Este nivel de seguridad es particularmente importante en un mundo donde la transferencia de datos sensibles y confidenciales es una constante, especialmente en entornos corporativos o educativos donde la privacidad y la seguridad de la información son de máxima prioridad.

Figura 64. Instalación del Módulo VPN en Zentyal

Fuente: Autoría Propia

7.6 CONFIGURACIÓN DEL SERVIDOR VPN Y CERTIFICADOS

Un servidor es una computadora o sistema de hardware y software que proporciona servicios, recursos o funcionalidades a otros dispositivos, conocidos como clientes. Estos servicios pueden variar desde la administración de archivos y la gestión de impresiones hasta el alojamiento de sitios web, el procesamiento de correos electrónicos, la gestión de bases de datos, la ejecución de aplicaciones específicas y mucho más.

La configuración del servidor VPN incluye la generación y administración de certificados digitales, que son fundamentales para la autenticación y seguridad en las conexiones VPN.

En el contexto de una conexión VPN, un certificado es un componente esencial que facilita la autenticación y la seguridad de la comunicación entre el cliente y el servidor. Los certificados digitales son archivos electrónicos que contienen información sobre la identidad de una entidad, como una organización o un individuo, y se utilizan para establecer la confianza en línea.

Figura 65. Configuración de Servidor VPN y Certificados

Fuente: Autoría Propia

Instalación y Configuración de OpenVPN en la Estación de Trabajo GNU/Linux

Se instala OpenVPN en la estación de trabajo GNU/Linux, importando el certificado necesario para establecer una conexión segura con el servidor VPN.

Figura 66. Instalación de OpenVPN en GNU/Linux

Fuente: Autoría Propia

7.7 ESTABLECIMIENTO Y VERIFICACIÓN DE LA CONEXIÓN VPN

Una vez establecida la conexión VPN, se realiza una prueba para verificar la conectividad y la dirección IP asignada al servidor, confirmando el correcto funcionamiento de la VPN.

Figura 67. Verificación de la Conexión VPN

Fuente: Autoría Propia

La implementación de una VPN utilizando Zentyal y OpenVPN en una estación de trabajo GNU/Linux ofrece un método seguro y eficiente para establecer un túnel privado de comunicación. Esta configuración asegura que la información transmitida entre la estación de trabajo y la red esté cifrada y protegida, proporcionando una solución vital para la seguridad y privacidad en entornos de red modernos.

8 CONCLUSIONES

La implementación y configuración de una infraestructura de TI utilizando GNU/Linux y Nethserver han proporcionado valiosas lecciones y destacado varias características clave de esta combinación.

La configuración de servicios DHCP y DNS en Nethserver ha resultado eficaz para la administración de la conectividad y resolución de nombres en la red. Su gestión centralizada y la interfaz intuitiva facilitan la administración del tráfico de red y la información de dominio, resaltando la eficiencia y simplicidad de Nethserver en la gestión de infraestructuras de TI.

La implementación del controlador de dominio LDAP subraya la fortaleza de Nethserver en la gestión de identidades y accesos. Este sistema es crucial para garantizar la autenticación y autorización adecuadas en la red, demostrando la capacidad de Nethserver para mantener un alto nivel de seguridad y coherencia en la gestión de accesos.

La instalación y configuración del Proxy y el Filtro Web en Nethserver han mejorado significativamente el control sobre el acceso a Internet. Esta configuración permite una gestión más granular del tráfico web, mejorando la seguridad y facilitando el cumplimiento de políticas de uso de Internet en la red.

El establecimiento del cortafuegos en Nethserver ha reforzado la seguridad de la red. La facilidad de configuración y la integración con el sistema operativo demuestran la eficacia de Nethserver como una herramienta poderosa para la gestión de la seguridad de la red, permitiendo un control detallado del acceso a los recursos.

La implementación de un File Server y un Print Server en Nethserver ha centralizado y simplificado la gestión de recursos compartidos y tareas de impresión en la red. Esta centralización ofrece soluciones escalables y accesibles para organizaciones de cualquier tamaño, mejorando la eficiencia operativa y la colaboración.

La implementación de una VPN utilizando Zentyal y OpenVPN en una estación de trabajo GNU/Linux ha ofrecido un método seguro y eficiente para establecer un túnel privado de comunicación. Esta configuración asegura que la información transmitida entre la estación de trabajo y la red esté cifrada y protegida, destacando la importancia de la VPN en la protección de datos sensibles y en la facilitación del trabajo remoto seguro.

La utilización de GNU/Linux y Nethserver para la implementación de una infraestructura de TI demuestra ser una solución eficiente, segura y adaptable. Esta combinación facilita la gestión de una variedad de servicios esenciales de red, desde la seguridad hasta la compartición de recursos, adecuándose a las necesidades cambiantes de las organizaciones modernas. La facilidad de configuración y la flexibilidad inherente a estas plataformas resaltan su viabilidad como opciones robustas para la administración de sistemas en diversos entornos empresariales y educativos.

9 REFERENCIAS

[1] Chowdhury, M. R., & Gupta, A. (2021). *Advanced Linux Networking and Storage*. O'Reilly Media.

[2] Miller, M. (2020). File and Print Servers in Linux Environments. *Linux Journal*, 15(7), 48-55.

[3] Singh, R. (2022). *LDAP and Domain Controller Integration in GNU/Linux. Journal of Network Administration*, 17(3), 89-102.

Adminso.es. (2017). Iptables - guía rápida - ASO. Recuperado de http://www.adminso.es/index.php/Iptables_-_gu%C3%ADa_r%C3%A1pida

Anónimo. (2017). Recuperado de http://www.it-docs.net/ddata/67.pdf

Béjar, H (2015). *Selección, instalación, configuración y administración de los servidores de transferencia de archivos (UF1275)*. Madrid, ES: IC Editorial. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=150&docID=11148772&tm=1480301092468

Comandos de iptables. Recuperado de https://pabloyela.files.wordpress.com/2013/08/manual-de-uso-de-iptables-jorge-kleinerman.pdf

Coyote linux. Recuperado de https://www.ecured.cu/Coyote_Linux

De, E., & Tecnológica, F. (s/f). ESCUELA POLITÉCNICA NACIONAL. Recuperado el 4 de diciembre de 2023 de https://bibdigital.epn.edu.ec/bitstream/15000/1309/1/CD-0609.pdf

Deyimar, A. (2019, diciembre 30). Configurar un servidor VPN de Linux con OpenVPN - Guía paso a paso. *Tutoriales Hostinger*. Recuperado de https://www.hostinger.co/tutoriales/como-configurar-vpn-linux-con-openvpn

Endian Firewall. (2017). Recuperado de http://www.i-t-m.com/productos-servicios/seguridad/endian-firewall

Fernández, Y. (2019, 1 de mayo). Primeros pasos para empezar tras instalar tu primera distribución Linux. *Xataka*. Recuperado de https://www.xataka.com/basics/primeros-pasos-linux

Firewall — NethServer 7 Final. (s. f.). Recuperado de https://docs.nethserver.org/es/v7/firewall.html

García, J. & Perramont, X. (2007). Aspectos avanzados de seguridad en redes. *Universidat Oberta de Catalunya – UOC*. Recuperado de http://hdl.handle.net/10609/204

Getting started with NethServer. (s. f.). Recuperado de https://www.nethserver.org/getting-started-with-nethserver/

Gupta, A. (2023). Efficient Network Administration with Nethserver. *International Journal of Open Source Software and Systems, 14*(2), 80-95.

Josep, J. E., & Remo, S. B. (2007). Administración avanzada de GNU/Linux. *Universitad Oberta de Catalunya – UOC*. Recuperado de http://hdl.handle.net/10609/226

Katerine, J., & Remolina, R. (s/f). IMPLEMENTACIÓN Y CONFIGURACIÓN DETALLADA DE LA CREACIÓN DE UNA VPN BAJO ZENTYAL SERVER. Recuperado el 4 de diciembre de 2023 de https://repository.unad.edu.co/bitstream/handle/10596/49419/jkrojasre.pdf?sequence=1

Lee, S. H. (2021). Comparative Analysis of Network Security in GNU/Linux and Windows Systems. *Network Security, 29*(6), 22-29.

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux: A Practical Guide to Implementing Penetration Testing Strategies on Websites, Web Applications, and Standard Web Protocols with Kali Linux*. Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=644345&lang=es&site=ehost-live

NethServer. (s. f.). La instalación y configuración de Nethserver es una buena manera de aprender sobre la administración de sistemas GNU/Linux. Recuperado de https://docs.nethserver.org/es/v7/

NethServer. (s. f.). NethServer/docs: NethServer documentation. Recuperado de https://github.com/NethServer/docs

Patel, K. R., & Mehta, D. (2018). The Role of Linux in Modern IT Infrastructure: An Industry Perspective. *Journal of Systems and Software, 99*, 97-109.

Perpiñán, A. (2008). Seguridad de Sistemas GNU/LINUX. *Fundación Código Libre Dominicano*. Recuperado de http://www.mclibre.org/descargar/docs/manual-fcld/perpinan-gnu-linux-seguridad-200804.pdf

Quasarbi.com. (2017). ¿Qué es Endian? OpenSource UTM (Gestión Unificada de Amenazas), Bogota - Colombia. Recuperado de http://www.quasarbi.com/endian.html

Rivera, J. G., Barrera, A. H., Reina, N. Y. R., & Amaya, J. S. (s/f). Evaluación final Diplomado de profundización en Linux. Recuperado el 4 de diciembre de 2023 de https://repository.unad.edu.co/jspui/bitstream/10596/23417/1/nruizre.pdf

Rodríguez, P. (2022). DHCP and DNS Configuration in GNU/Linux Systems. *Linux Networking Magazine, 12*(4), 30-35.

Rodríguez, P., & Fernández, G. (2019). Nethserver as a Scalable Solution for Small and Medium Enterprises. *International Journal of Open Source Software and Processes, 11*(4), 45-60.

Romo, F. M. (s/f). ESTUDIO E IMPLEMENTACIÓN DE LA RED VPN ARKA S.A. Recuperado el 4 de diciembre de 2023 de https://red.uao.edu.co/bitstream/handle/10614/1099/T0003582.pdf?sequence=1&isAllowed=y

Singh, A. (2013). *Instant Kali Linux*. Birmingham [UK]: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=656227&lang=es&site=ehost-live

Smith, J. A., & Johnson, L. M. (2020). GNU/Linux in Enterprise Environments: A Comprehensive Overview. *Journal of Information Technology, 35*(2), 115-130.

Smith, J., & Lee, K. (2021). Fundamentals of Network Management in Linux Environments. *Networking and Systems Journal, 15*(3), 45-60.

Solucionando necesidades específicas con Gnu/Linux. Recuperado el 4 de diciembre de 2023 de https://1library.co/document/ynegeely-solucionando-necesidades-especificas-con-gnu-linux.html

Thompson, H., & Davis, R. J. (2022). Open Source Software in Education: Case Studies with GNU/Linux. *Education and Information Technologies, 27*(1), 333-350.

Web.mit.edu. (2017). Opciones usadas en comandos iptables. Recuperado de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-iptables-options.html

Fernández, Y. (2019). Primeros pasos empezar tras instalar tu primera distribución Linux. *Xataka*. Recuperado de https://www.xataka.com/basics/primeros-pasos-linux.