IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT EN NETHSERVER PARA ESTACIONES DE TRABAJO GNU/LINUX: UNA SOLUCIÓN INTEGRAL DE RED, SEGURIDAD Y GESTIÓN DE RECURSOS

Dilson Lazaro-Ospino
e-mail: djlazaroo@unadvirtual.edu.co
Jose Alberto Salcedo Campo
e-mail: jasalcedoca@unadvirtual.edu.co
Jesus Alberto Maestre
e-mail: jamaestre@unadvirtual.edu.co
Luis Alfredo Berna López
e-mail: labernal@unadvirtual.edu.co
Eduar Gamez De La Hoz
e-mail: eegamezd@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de servicios de infraestructura IT en Nethserver para estaciones de trabajo GNU/Linux, abordando cinco temáticas clave: DHCP Server, DNS Server y Controlador de Dominio, Proxy, Cortafuegos, File Server y Print Server, y VPN. Se detalla la configuración y gestión de servicios esenciales como asignación de direcciones IP dinámicas, resolución de nombres, control de acceso a internet mediante un proxy y filtrado de contenido, así como la creación de reglas de firewall para restringir sitios no deseados. Además, se implementa un servidor de archivos e impresión accesible mediante un controlador de dominio LDAP. Finalmente, se configura una VPN para permitir la conexión segura de estaciones de trabajo. Este enfoque integral mejora la administración de redes, seguridad y gestión de recursos en entornos corporativos, proporcionando una solución robusta y escalable para la infraestructura IT.*

PALABRAS CLAVE: GNU/Linux, Infraestructura IT, Nethserver, Seguridad de red.

1 INTRODUCCIÓN

En el contexto actual de la educación y la tecnología, la integración de nuevas herramientas digitales ha transformado la forma en que se enseñan y aprenden los contenidos. El uso del metaverso en la educación es uno de los avances más recientes, y según Gómez-Marí y Pedrosa-Sáez (2023), es crucial analizar las actitudes y conocimientos de los estudiantes, docentes y familias para comprender si la comunidad educativa está preparada para su inclusión. Por otro lado, el uso de software libre y sistemas operativos como GNU/Linux es una alternativa creciente en el ámbito de la administración de sistemas y la gestión de recursos tecnológicos. En este sentido, Hernández y Sánchez (2022) y Vargas (2020) abordan la importancia de implementar y gestionar sistemas Linux en el entorno educativo. Asimismo, herramientas y objetos virtuales de aprendizaje, como los presentados por Guzmán Arévalo (2017) y Hernández (2022), ofrecen una excelente base para la formación en tecnologías abiertas y la administración de infraestructuras IT. Este artículo tiene como objetivo explorar cómo la implementación de servicios en Nethserver para estaciones de trabajo GNU/Linux puede optimizar la infraestructura educativa, mejorando la seguridad, la gestión de recursos y la conectividad en entornos académicos.

2 NETHSERVER

NethServer es una distribución de Linux basada en CentOS, diseñada principalmente para facilitar la administración de servicios de red en pequeñas y medianas empresas. Es una solución integral que permite configurar y gestionar diversos servicios de infraestructura de red.

2.1 ASPECTOS IMPORTANTES A DESTACAR SOBRE NETHSERVER

Aunque NethServer es reconocido por su simplicidad y versatilidad, existen varios aspectos que a menudo no se mencionan y que son relevantes para una evaluación completa de su implementación en entornos corporativos.

En primer lugar, aunque NethServer es de código abierto y recibe actualizaciones periódicas, la comunidad detrás de su desarrollo no siempre es tan activa como en otras distribuciones populares, lo que puede generar retrasos en actualizaciones críticas. Además, aunque la plataforma está diseñada para ser fácil de usar, las configuraciones avanzadas, como la gestión de VPN o cortafuegos, requieren un conocimiento técnico más profundo.

Otro aspecto importante es la dependencia de su interfaz web para la administración, lo que puede ser limitante para usuarios avanzados acostumbrados a trabajar con la línea de comandos. A pesar de su flexibilidad, NethServer presenta ciertas limitaciones en cuanto a personalización avanzada en comparación con otras distribuciones más genéricas, lo que podría no satisfacer las necesidades de entornos altamente especializados. Además, aunque es adecuado para pequeñas y medianas empresas, puede no ser la mejor opción para organizaciones de gran escala debido a restricciones en el rendimiento.

Por último, la documentación de NethServer, aunque útil, no es tan extensa como la de otras soluciones más populares, lo que podría complicar la resolución de problemas complejos. Estos factores deben ser considerados al evaluar NethServer como una opción para la gestión de redes empresariales.

3 DHCP, DNS Y CONTROLADOR DE DOMINIO

El servidor *Dynamic Host Configuración Protocol* (DHCP) agrupa la misión de la distribución de red local para cualquier terminal conectado a ella, cuando un computador (o un dispositivo como una impresora, un teléfono inteligente, etc.) se vinculan a la red local, puede requerir los parámetros de configuración de red mediante la formalidad DHCP, el servidor DHCP responde, suministrando el IP, DNS y otras cuantificaciones de red notables.

3.1 CONFIGURACIÓN DHCP

El servidor DHCP se puede encargar en todas las interfaces verde y azul NethServer fijará una dirección IP libre dentro de la configuración rango DHCP en la página DHCP > Servidor DHCP. El rango DHCP debe precisar dentro de la red de la interfaz asociada, por ejemplo, si la interfaz verde tiene IP/netmask 192.168.1.6/24 .255.255.0 el rango debe ser 192.168.1.7 - 192.168.1.254.

3.2 OPCIONES AVANZADAS

Hay siete elecciones desarrolladas para DHCP, obtiene una asignación cero iniciativas, una opción o las siete opciones. Para los servidores - DNS, se consigue asignar cero, uno o más para cada servidor; si pone más de uno, esgrima una coma entre cada servidor sin espacio.

3.3 RESERVA IP DEL HOST

El servidor DHCP otorga una dirección IP a un terminal durante una fase de lapso limitado si un conector solicita tener siempre la misma dirección IP, se le puede conceder una reserva IP coligada a su dirección MAC.

La página DHCP> IP reservation lista las direcciones IP actualmente asignadas:

- Una línea con botón IP reservation iguala un host con un alquiler estacional (color gris).
- Una línea con el botón Edit identifica un host con una IP reservada (color negro). Un pequeño icono de dos saetas adyacente al alias del host muestra que la concesión DHCP ha declinado y es un estado estándar para los hosts con configuración IP estática, ya que jamás se colocan en relación con el servidor DHCP.

3.4 INICIO DE INSTALACIÓN DE NETHSERVER

En la imagen observamos el inicio de instalación de NethServer.

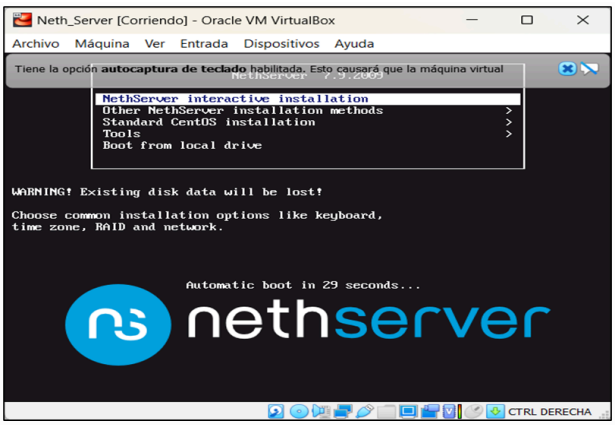


Imagen 1: creación propia – VirtualBox

En la siguiente imagen observamos la localización, idioma, conexión de las tarjetas y el usuario root con su contraseña.

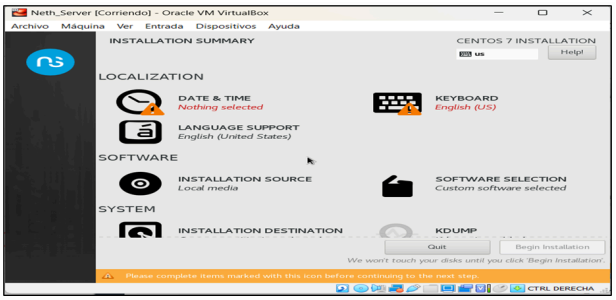


Imagen 2: creación propia – VirtualBox

En la siguiente imagen observamos el usuario root y la contraseña que le vamos a poner para ingresar al NethServer.

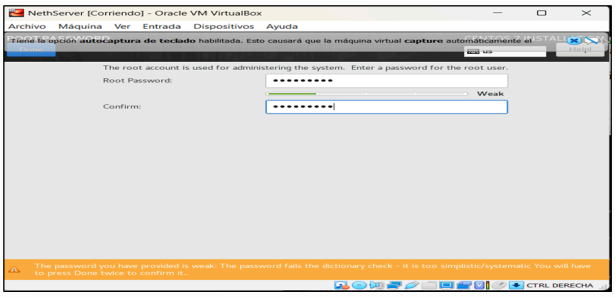


Imagen 3: creación propia – VirtualBox

En esta imagen observamos que NethServer se instaló correctamente y nos arroja la ip de ingreso como se observa.

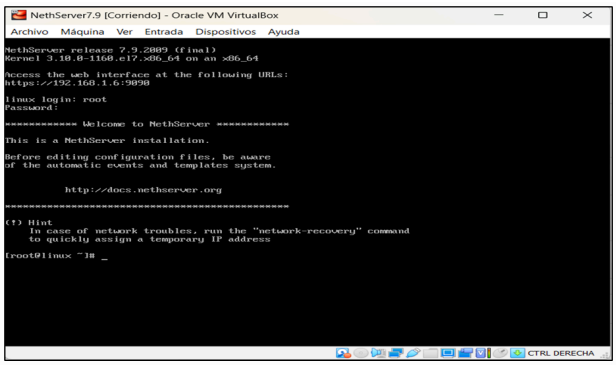


Imagen 4: creación propia – VirtualBox

3.5 INICIO DE LA CONFIGURACIÓN DE LAS TARJETAS DE RED EN NETHSERVER.

En esta imagen observamos la interfaz de NethServer con la ip que nos generó la instalación, ingresamos con el usuario root y la contraseña que previamente creamos en la configuración.

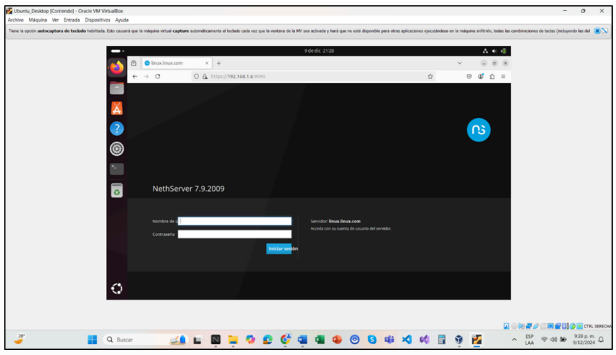


Imagen 5: creación propia – VirtualBox

En la siguiente imagen nos muestra el inicio de sesión y como primera medida se debe hacer el cambio de nombre de la empresa y posterior a ello seguimos con las configuraciones según la temática propuesta.

Los datos de la empresa que solicita el sistema son:

- Nombre
- Ciudad
- Departamento
- Teléfono
- Dirección

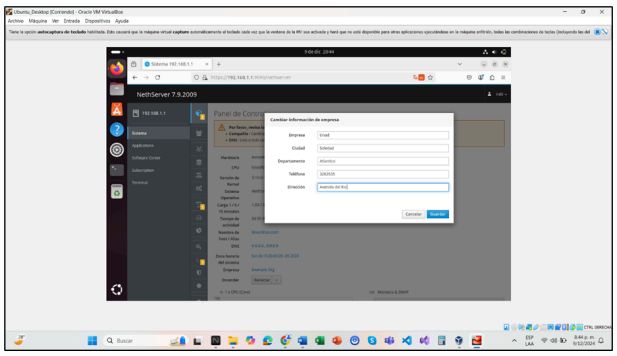


Imagen 6: creación propia – VirtualBox

En la siguiente imagen observamos las tres tarjetas de red creadas para la actividad como la red LAN (verde), WAN (rojo) y DMZ (naranja), las cuales están configuradas con sus respectivas ip.

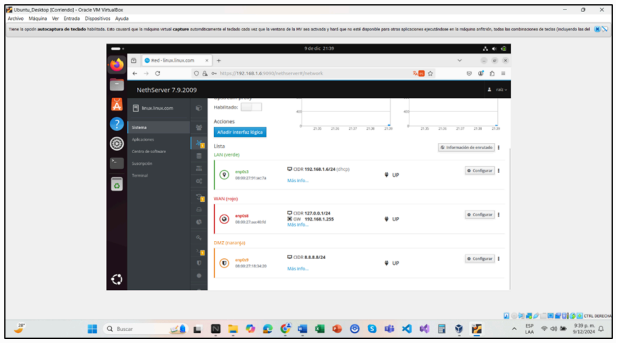


Imagen 7: creación propia – VirtualBox

En esta imagen observamos la configuración del servidor DHCP con la red verde LAN y el rango de las ip.

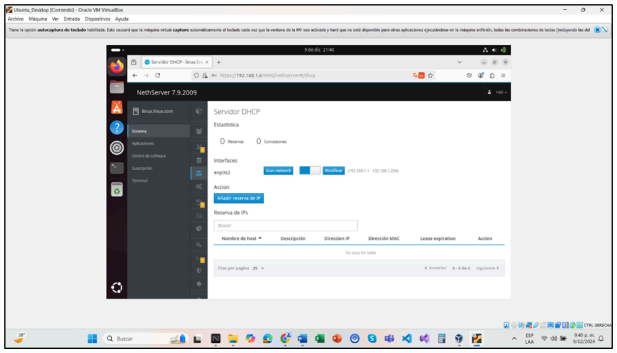


Imagen 8: creación propia – VirtualBox

En esta imagen realizamos la configuración del servidor DNS.

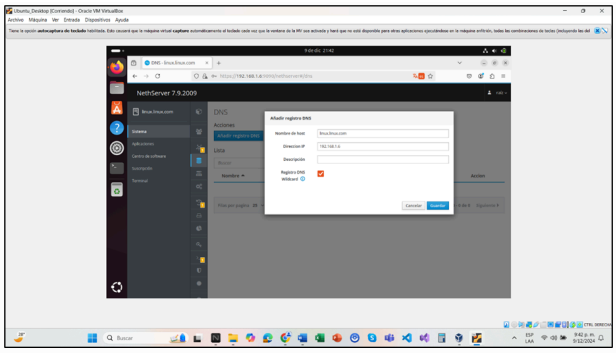


Imagen 9: creación propia – VirtualBox

En la imagen podemos apreciar que la configuración de la ip para el servidor DNS quedó creada correctamente como nos muestra el sistema.

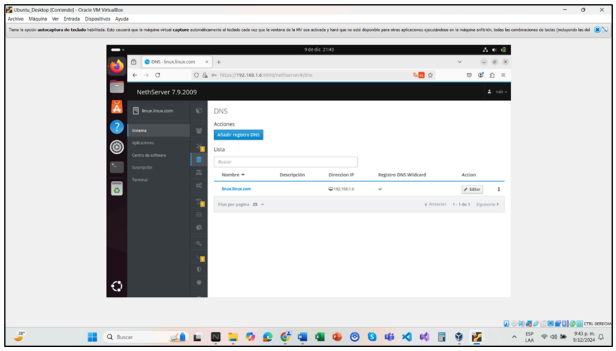


Imagen 10: creación propia – VirtualBox

3.6 CONTROLADOR DE DOMINIO.

Los usuarios y grupos se acumulan en una base de datos LDAP, atendida por un canon de distribuidor de cuentas, diversos módulos logran trabajar adyacentes para tener en cuenta la propia base de datos LDAP como réplicas. Una base de datos LDAP personifica un dominio de cuentas .
El clúster NS8 obtiene albergar varios dominios de cuentas locales de desiguales implementaciones, igualmente es viable configurar y conectar servicios LDAP externos los bosquejos LDAP compatibles son:

- Directorio activo - Samba
- Atributos de Unix RFC2307 - OpenLDAP

Conjuntamente de elegir enlazar un proveedor externo o instalar uno interno, el administrador debe resolver qué tipo de backend se acomoda a sus necesidades, la aplicación de servidor de archivos Samba puede certificar clientes SMB/CIFS solo cuando se maneja un dominio de Active Directory, por otro lado, el distribuidor OpenLDAP interno es más fácil de colocar y configurar, al final, si no se solicita la concurrencia con la formalidad de intercambio de archivos SMB, un proveedor LDAP es la mejor opción. Tenga en cuenta siempre que alcanza a alojar varias instancias de OpenLDAP en el mismo nodo, mientras que solo puede situar una instancia de Samba por nodo.

En la imagen podemos ver la activación del directorio en la configuración del proveedor de cuentas en el sistema.

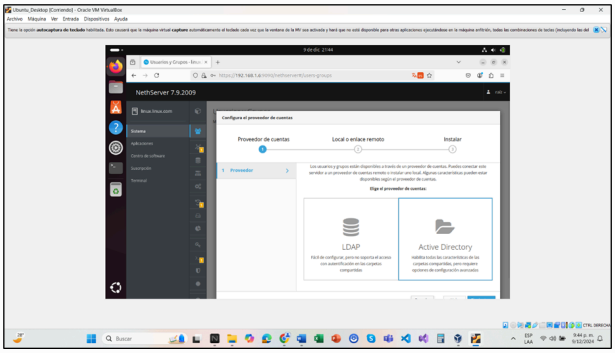


Imagen 11: creación propia – VirtualBox

En esta imagen realizamos la activación local o enlace remoto del create domain and become DC.

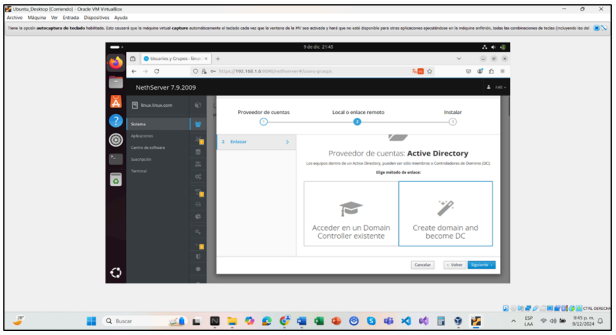


Imagen 12: creación propia – VirtualBox

En esta imagen se realiza la configuración de la ip para el become DC, y dominio controller de las cuentas y grupos.

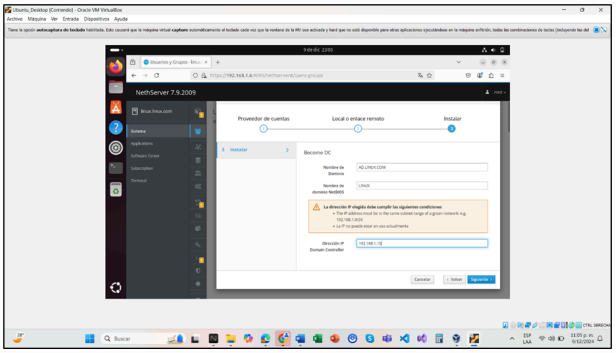


Imagen 13: creación propia – VirtualBox

4 CONTROL DE ACCESO A INTERNET A TRAVÉS DEL PUERTO 3128

Un proxy es un servicio intermedio que actúa como puente entre los usuarios de una red y los servicios a los que intentan acceder, como Internet. Su implementación tiene como objetivo principal gestionar, monitorear y restringir el tráfico de datos para garantizar tanto la seguridad como la eficiencia en el uso de los recursos de red.

En el contexto de NethServer, el proxy se configura como una solución integral para el control de acceso y filtrado de contenido en redes locales e institucionales. A través del uso del puerto estándar 3128, el proxy permite supervisar las conexiones, establecer políticas de acceso específicas y proteger los sistemas contra amenazas externas, mientras optimiza el uso del ancho de banda.

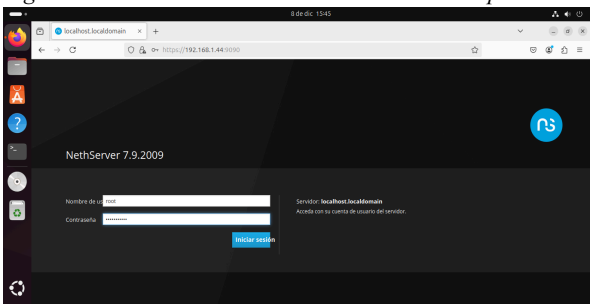
Este enfoque es especialmente útil en entornos organizacionales donde es crucial garantizar un acceso seguro, eficiente y administrado a los recursos de Internet, alineándose con los requerimientos de control y gestión de redes modernas. La configuración del proxy en NethServer incluye herramientas para definir reglas avanzadas de filtrado, como listas de permitidos y bloqueados, horarios de uso y limitaciones por tipo de contenido, adaptándose a las necesidades de cualquier institución o empresa.

Ya habiendo instalado y configurado anteriormente nethserver, procedemos a ingresar desde la máquina desktop. Abrimos el navegador y digitamos la dirección ip proporcionada en nethserver:

Imagen 14: Dirección ip nethserver.

Fuente: Autoría propia

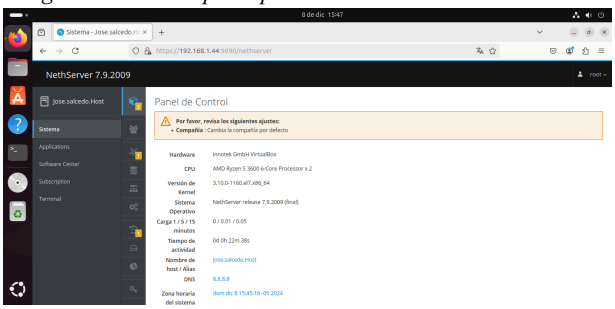
Imagen 15: Inicio de sesión nethserver desde desktop.



Fuente: Autoría propia.

Una vez iniciada la sesión se nos mostrará la ventana principal del nethserver:

Imagen 16: Ventana principal del sistema de nethserver.



Fuente: Autoría propia.

Ahora procedemos a descargar diferentes aplicaciones que se van a requerir para llevar a cabo las indicaciones establecidas con respecto al proxy.

Primero que todo descargamos e instalamos las siguientes aplicaciones:

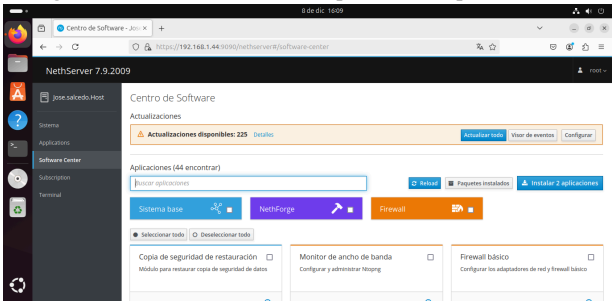
- Web Proxy & Filter
- Firewall

Usaremos principalmente Web Proxy & Filter. Como concepto general, es una funcionalidad clave que se encuentra en distribuciones de GNU/Linux diseñadas para administrar redes, como NethServer. Este módulo permite implementar un servicio de proxy que no solo redirige el tráfico entre clientes y servidores externos, sino que también aplica filtros avanzados para controlar y supervisar el acceso a Internet desde una red interna.

En NethServer, el módulo Web Proxy & Filter es accesible desde su interfaz de administración. Es una herramienta poderosa para instituciones que necesitan un control granular del acceso a Internet, como escuelas, oficinas gubernamentales o empresas con políticas estrictas de ciberseguridad y productividad.

Por lo tanto, nos dirigimos a la sección de Software center y procedemos con su instalación:

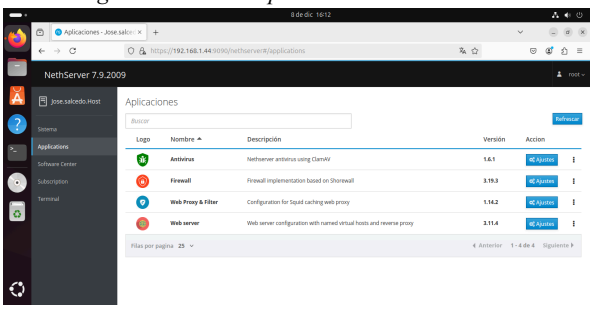
Imagen 17: Buscar e instalar la aplicación requerida.



Fuente: Autoría propia.

Verificamos que la aplicación se haya descargado e instalado correctamente en la opción Applications:

Imagen 18: Sección aplicaciones instaladas.

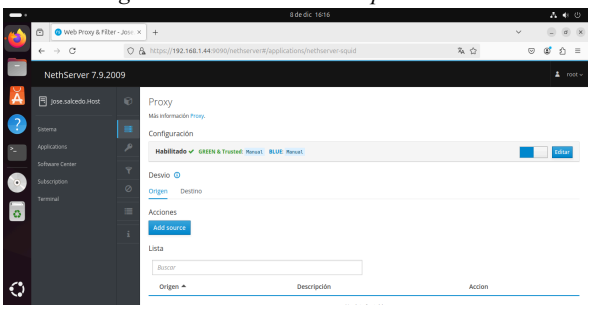


Fuente: Autoría propia.

Ahora procedemos a realizar la configuración de la aplicación proxy según lo requerido en la temática:

Primero que todo activamos Web Proxy & Filter para poder iniciar:

Imagen 19: Activación de la aplicación.



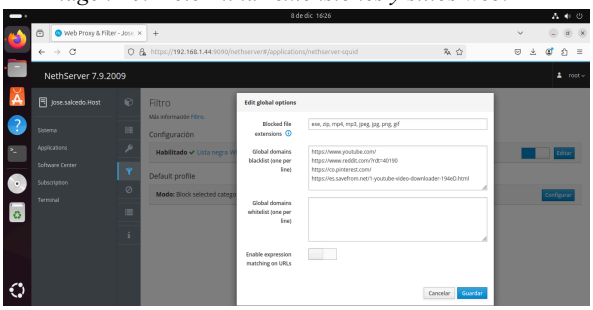
Fuente: Autoría propia.

Después le damos en el botón editar para realizar las respectivos cambios:

Se determina controlar los formatos o extensiones de archivos de imágenes y videos como jpeg, png, gif, mp4 entre otros.

También se determina controlar sitios web como youtube, reddit y speedtest (agregado después) para controlar el flujo de anuncios y demás acciones sospechosas.

Imagen 20: Determinar extensiones y sitios web.

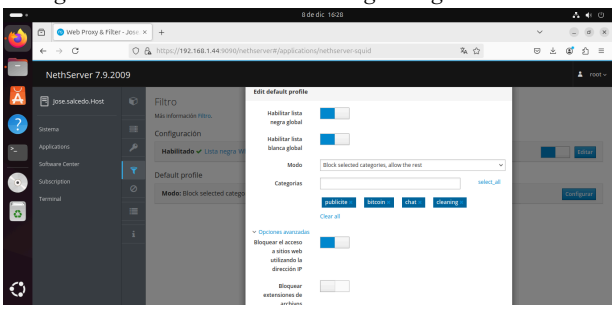


Fuente: Autoría propia.

Ahora realizamos una segunda configuración correspondiente a las etiquetas generales que se maneja en este aspecto:

Fueron anexadas etiquetas relacionadas con la publicidad, ventanas de chat, avisos de limpieza y otro tipo de ventanas o acciones que pueden aparecer mientras se navega.

Imagen 21: Se anexa al control categorías generales.

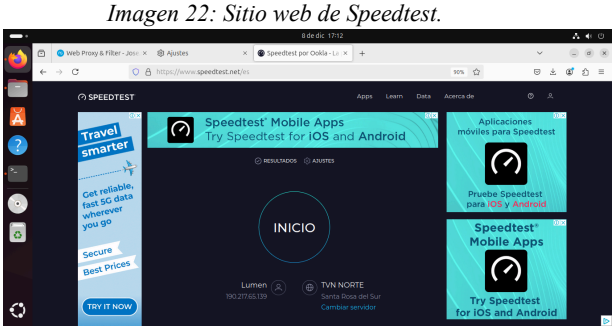


Fuente: Autoría propia.

Ya teniendo las configuraciones necesarias en la aplicación Web Proxy & Filter, procedemos a comprobar el funcionamiento del servicio proxy.

Como primer paso, vamos a uno de los sitios determinados en la parte de control anterior y navegamos en el, en este caso entramos al sitio web de Speedtest. Podemos observar que contienen varios anuncios:

Imagen 22: Sitio web de Speedtest.

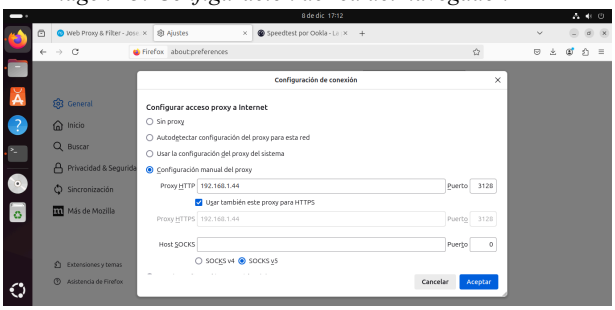


Fuente: Autoría propia.

Ahora como segundo paso, vamos a la configuración de red del navegador que estemos usando, en este caso el Firefox.

Hacemos los cambios que se requieran, en este caso configuramos manualmente el proxy colocando la dirección ip necesaria y el puerto requerido (3128).

Imagen 23: Configuración de red del navegador.

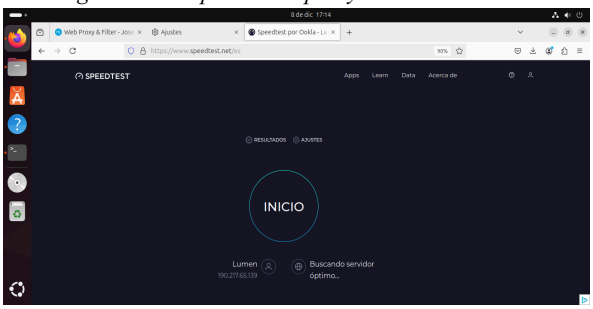


Fuente: Autoría propia.

Ya teniendo las configuraciones establecidas del proxy y del navegador, procedemos con el último paso y es comprobar volviendo a cargar el sitio web de Speedtest.

Al hacer esto podemos ver que los anuncios ya no aparecen, lo que quiere decir que el servicio de proxy y sus cambios realizados funcionan correctamente:

Imagen 24: Comprobación proxy en el sitio web.



Fuente: Autoría propia.

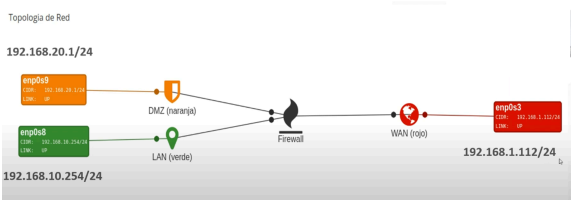
5 CONFIGURACIÓN DE CORTAFUEGO: RESTRICCIÓN DE ACCESO A SITIOS WEB DE ENTRETENIMIENTO Y REDES SOCIALES

La configuración adecuada de un cortafuegos (firewall) es esencial para gestionar y restringir el acceso a sitios web de entretenimiento y redes sociales dentro de una red corporativa o educativa. Para ello, se pueden implementar políticas de filtrado de contenido que bloqueen o restrinjan el acceso a plataformas de entretenimiento, como servicios de streaming, videojuegos en línea y redes sociales populares. Esto se logra mediante la identificación y bloqueo de direcciones URL, palabras clave o categorías de contenido específicas, asegurando que el tráfico no autorizado sea rechazado. Además, se pueden establecer niveles de acceso diferenciados, permitiendo que ciertos usuarios, como los administradores, mantengan un acceso más amplio mientras que otros, como los empleados o estudiantes, tengan restricciones. La implementación de estas políticas no solo mejora la productividad, sino que también protege la red de posibles riesgos de seguridad asociados con el uso no controlado de plataformas no relacionadas con el trabajo o estudio.

5.1 IMPLEMENTACIÓN DE LA TOPOLOGÍA DE RED DESMILITARIZADA

La DMZ (zona desmilitarizada) es una red accesible desde Internet, pero que está separada de la red interna (verde). Los servidores que deben ser accesibles desde el exterior (como servidores web, servidores de correo electrónico, y servidores DNS) se colocan en esta zona, ya que están expuestos a riesgos de seguridad debido a su accesibilidad pública. Así, la DMZ sirve como un área de contención entre la red interna y el exterior. Aunque los servicios en la DMZ están disponibles para los usuarios de Internet, no tienen acceso directo a los recursos internos de la organización. Este aislamiento ayuda a proteger la red interna de posibles ataques desde Internet. Si un atacante compromete un servidor en la DMZ, no podrá moverse fácilmente a la red verde interna.

Imagen 25: Topología generada por Nethserver



Fuente: generado por nethserver

5.2 IMPLEMENTACIÓN DEL FIREWALL EN NETHSERVER

Se configura una interfaz de red en NethServer para la DMZ, con una dirección IP pública o privada distinta, por ejemplo `192.168.20.1/24`.

De modo que el tráfico entre la DMZ y la red naranja debe ser cuidadosamente controlado. Se puede permitir el acceso de solo algunos puertos específicos desde la DMZ hacia la red interna (por ejemplo, para acceder a una base de datos interna desde un servidor web en la DMZ). También se pueden configurar reglas que limiten el tráfico entre la DMZ y la red verde, permitiendo solo lo necesario.

Así los servicios que deben ser accesibles desde Internet (como HTTP, HTTPS, o FTP) se colocan en servidores dentro de la DMZ. NethServer permite exponer estos servicios de forma segura, protegiéndolos con cortafuegos y asegurándose de que no puedan acceder a la red interna sin pasar por un proceso de autenticación o revisión de seguridad.

6 CONFIGURACIÓN DE SERVICIOS DE ARCHIVO E IMPRESIÓN: ACCESO A CARPETAS COMPARTIDAS E IMPRESORAS A TRAVÉS DE LDAP

En el ámbito de la tecnología de la información, la gestión eficiente de recursos compartidos, como archivos e impresoras, es fundamental para optimizar las operaciones organizacionales. Un File Server permite almacenar, compartir y proteger datos de manera centralizada, mientras que un Print Server administra de forma eficiente las solicitudes de impresión en una red. Para maximizar su funcionalidad y seguridad, estos servicios deben integrarse con un controlador de dominio, como LDAP, que ofrece autenticación y automatización centralizadas.

6.1 INFRAESTRUCTURA DE RED

La arquitectura de red para esta implementación está dividida en dos zonas principales:

- LAN (Local Area Network):
  - Conecta estaciones de trabajo y servidores internos.
  - Ofrece acceso a servicios compartidos, como carpetas e impresoras.

- Garantiza privacidad mediante reglas de firewall estrictas.

- DMZ (Desmilitarized Zone):
  - Aisla servicios accesibles externamente, como el portal de administración.
  - Mejora la seguridad mediante la separación lógica de la LAN.
  - Facilita la gestión remota utilizando protocolos seguros como SSH y TLS.

Esta separación asegura que los recursos internos estén protegidos frente a accesos no autorizados desde redes externas.

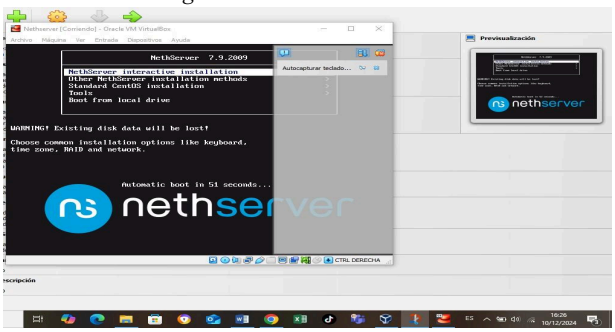
6.2 PROCESO DE CONFIGURACIÓN

6.2.1 INSTALACION DE NETHSERVER

Esta distribución nos proporciona herramientas fáciles de usar para configurar servidores de correo, web, archivos, impresión, y más, con un enfoque en la seguridad y la escalabilidad.

1. Requisitos previos:
   - Máquina virtual con al menos 2 GB de RAM y 20 GB de almacenamiento.
   - Descarga de la imagen ISO de NethServer desde su sitio oficial.
2. Configuración inicial:
   - Instalación del sistema operativo con interfaces de red asignadas para LAN y DMZ.
   - Asignación de direcciones IP estáticas.
   - Configuración del dominio y hostname.

Imagen 26: Instalación de NethServer.

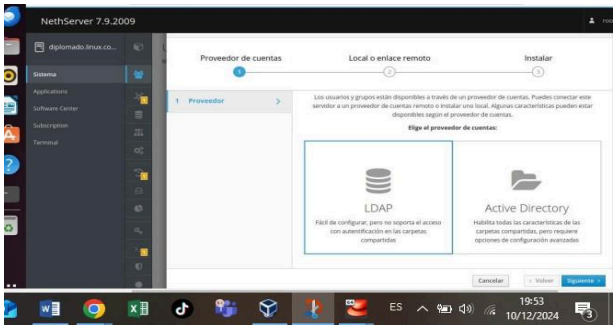


Fuente: Autoría propia.

6.2.2 CONFIGURACIÓN DEL CONTROLADOR DE DOMINIO LDAP

1. Instalar el módulo Accounts Provider en NethServer.
2. Configurar el controlador de dominio para soportar LDAP.
3. Creación de usuarios y grupos.

Imagen 27: Instalación de LDAP.

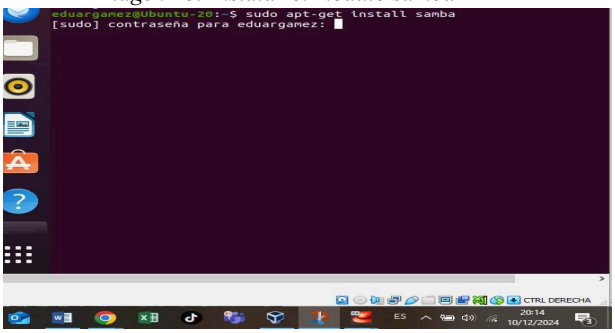


Fuente: Autoría propia

6.2.3 CONFIGURACIÓN DEL FILE SERVER

1. Instalar el módulo Samba File Server.

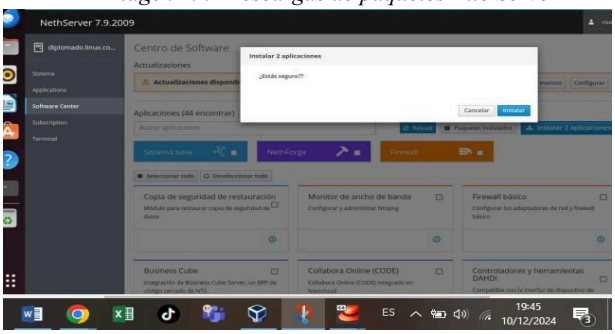
Imagen 28: Instalar el módulo samba



Fuente: Autoría propia.

2. Crear carpetas compartidas con permisos definidos según usuarios y grupos LDAP.
   - Carpeta pública: Acceso para todos los usuarios autenticados.
   - Carpeta privada: Restricción basada en grupos.
3. Configuración del acceso desde estaciones de trabajo GNU/Linux:
   - Usar herramientas como smbclient para probar conectividad.
   - Montar carpetas compartidas en los exploradores de archivos de los usuarios.

Imagen 29: Descargas de paquetes File Server



Fuente: Autoría propia.

6.2.4 CONFIGURACIÓN DEL PRINT SERVER

1. Instalar el módulo CUPS (Common UNIX Printing System).
2. Configurar impresoras conectadas localmente o descubiertas en la red.
3. Establecer permisos de impresión según grupos LDAP.
4. Verificar el servicio enviando trabajos de impresión desde clientes GNU/Linux.

Imagen 30: Configuración del Print Server

Fuente: Autoría propia.

6.2.5 SEGURIDAD Y MANTENIMIENTO

1. Configurar reglas de firewall en NethServer para restringir accesos no autorizados.
2. Habilitar TLS para proteger las comunicaciones LDAP.
3. realizar auditorías regulares y actualizaciones del sistema para mantener la seguridad.

6.3 BENEFICIOS

1. Centralización de recursos:
   - Simplifica la gestión de carpetas compartidas e impresoras desde un único punto.
   - Proporciona control granular mediante permisos basados en LDAP.
2. Seguridad:
   - Protege los datos mediante autenticación centralizada.
   - La segregación de LAN y DMZ reduce el riesgo de ataques externos.
3. Escalabilidad
   - Fácil integración de nuevos usuarios y estaciones de trabajo.
   - Adaptabilidad a futuras necesidades de infraestructura.
4. Eficiencia operativa:
   - Acceso rápido y confiable a recursos compartidos.
   - Impresión en red sin interrupciones.

6.4 IMPORTANCIA

En redes empresariales actuales, donde la conectividad y la seguridad son prioridades, los servicios de archivo e impresión centralizados son esenciales. NethServer, combinado con LDAP, ofrecen:

- Mayor control administrativo.
- Soluciones seguras y adaptables.
- Cumplimiento con estándares abiertos, evitando el uso de software propietario.

La separación de zonas LAN y DMZ, junto con configuraciones adecuadas de firewall, aseguran la protección de recursos críticos, incluso en redes con accesos externos.

6.5 RESULTADOS

Al finalizar la implementación, se obtuvo un entorno de red donde los usuarios pueden acceder de forma segura y eficiente a los archivos y las impresoras compartidas desde sus estaciones de trabajo Linux.
La implementación de un servidor de archivos y un servidor de impresión utilizando NethServer y LDAP proporciona una solución robusta y flexible para compartir recursos en una red local.

7 IMPLEMENTACIÓN DE VPN: CREACIÓN DE UN TÚNEL PRIVADO PARA CONEXIÓN REMOTA

En la actualidad, las redes privadas virtuales (VPN, por sus siglas en inglés) son fundamentales para garantizar la seguridad de la información al establecer conexiones remotas. Una VPN permite que los usuarios accedan a recursos internos de una red de manera segura a través de internet, utilizando un túnel cifrado que protege los datos de posibles interceptaciones o accesos no autorizados.

En este proyecto, se utilizó la plataforma NethServer para implementar un túnel privado. NethServer ofrece una interfaz intuitiva que simplifica el proceso de configuración de una VPN mediante protocolos como OpenVPN, ampliamente reconocido por su seguridad y flexibilidad.

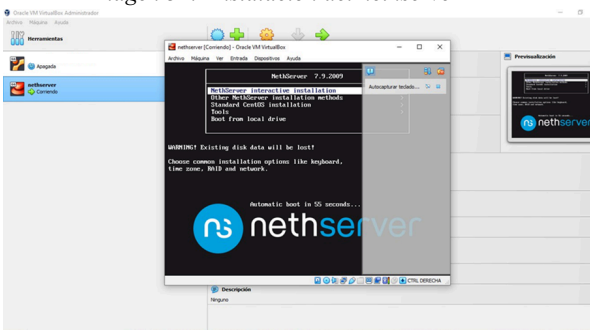
La configuración se inició con la instalación del módulo de VPN a través del *Software Center* de NethServer. Posteriormente, se definieron parámetros clave, como el rango de direcciones IP asignado a los clientes, el puerto de comunicación y el protocolo de transporte. Adicionalmente, se habilitó la autenticación mediante certificados y usuarios locales para garantizar un acceso controlado.

Para conectar clientes remotos, se generaron archivos de configuración compatibles con OpenVPN. Estos archivos incluyen las credenciales necesarias para establecer el túnel cifrado. En pruebas posteriores, los usuarios pudieron conectarse de manera exitosa desde dispositivos remotos, validando el acceso seguro a los recursos internos.

En este proyecto se llevó a cabo la implementación y configuración de una Red Privada Virtual (VPN) utilizando

NethServer, un servidor basado en Linux que facilita la gestión de redes y la seguridad en infraestructuras informáticas. El objetivo principal fue establecer una conexión segura y privada entre una estación de trabajo GNU/Linux y un servidor, mediante la creación de un túnel cifrado a través de la red pública.

Imagen 31: Instalación del nethserver



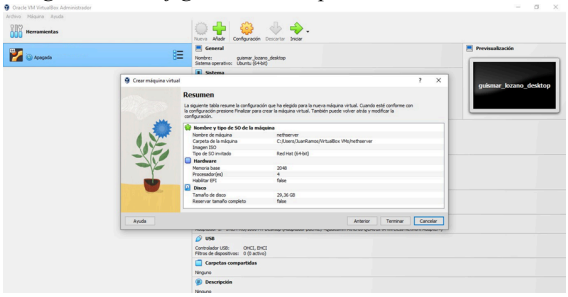
Fuente: Autoría propia.

Para comenzar, se instaló NethServer en una máquina virtual y se configuraron las interfaces de red, estableciendo una red interna segura (zona verde) y una red externa (zona roja) para el acceso a Internet. Se realizaron configuraciones tanto en el servidor como en los adaptadores de red de la máquina virtual para garantizar que la red interna estuviera aislada y protegida.

A continuación, se habilitó el servicio OpenVPN en NethServer, configurando el servidor para aceptar conexiones de clientes remotos de manera segura. El servidor OpenVPN se configuró en modo "RoadWarrior", utilizando autenticación basada en certificados y enrutamiento de red para asegurar la transmisión de datos. Además, se crearon varias cuentas de usuario con direcciones IP reservadas para los clientes, y se descargaron los archivos de configuración necesarios para conectarse a la VPN desde una estación de trabajo remota.

Finalmente, se verificó la conectividad estableciendo conexiones VPN desde máquinas con sistemas operativos Windows y GNU/Linux, comprobando que la conexión era exitosa y que los datos se transmitían de forma segura a través del túnel VPN. Todo el proceso fue documentado con capturas de pantalla, y se realizó una evaluación final del funcionamiento de la VPN para garantizar que cumpliera con los requisitos de seguridad y acceso remoto de la organización.

Imagen 30: Configuración de OpenVPN en NethServer



Fuente: Autoría propia.

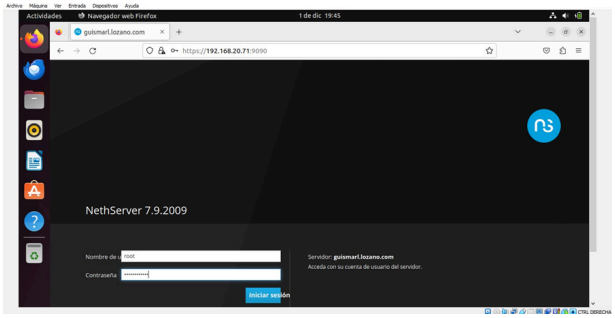
7.1 CONFIGURACIÓN INICIAL DE NETHSERVER

El proceso comenzó con la instalación de NethServer en una máquina virtual. Se configuraron dos adaptadores de red:

- **Adaptador 1:** Conectado a la red interna, denominada "red verde", para crear una conexión privada con la máquina Ubuntu Desktop.
- **Adaptador 2:** Configurado en modo puente (bridge), lo que permitió a la máquina virtual acceder a la red externa.

Durante la instalación, se configuraron parámetros básicos, como la zona horaria, el idioma, el teclado y el nombre del host. NethServer obtuvo una dirección IP temporal mediante DHCP, lo que permitió acceder al servidor a través de su interfaz web. Con la IP asignada, se pudo continuar con la configuración de las zonas de red.

Imagen 32: Inicio de sección en nethserver



Fuente: Autoría propia.

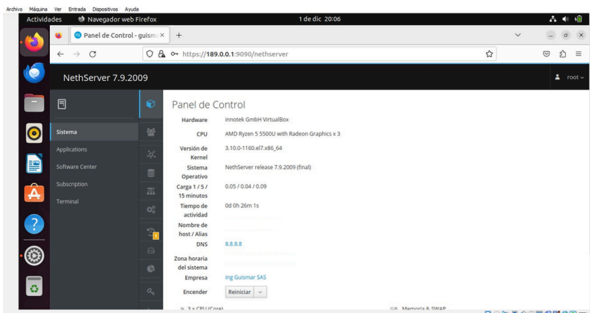
7.2 CONFIGURACIÓN DE ZONAS DE RED

Para garantizar una correcta segregación de las redes y el acceso remoto seguro, se configuraron dos zonas de red:

- **Zona Roja:** Esta zona está conectada a la red externa y utiliza una IP estática (192.168.20.245). Es la que permite el acceso a Internet.
- **Zona Verde:** Se configuró con una dirección IP de 189.0.0.1, que actúa como puerta de enlace para la red interna. Esta red permite la conexión entre el servidor y los clientes dentro de la infraestructura local.

La máquina cliente (Ubuntu Desktop) se configuró con una IP manual dentro del rango de la zona verde (189.0.0.5), con máscara de subred 255.255.255.0 y la puerta de enlace establecida en 189.0.0.1. Con esta configuración, se habilitó la comunicación entre la red interna y el servidor NethServer.

Imagen 33: Ingresamos al nethserver por la red interna con la ip 189.0.0.1, puerto 9090



Fuente: Autoría propia.

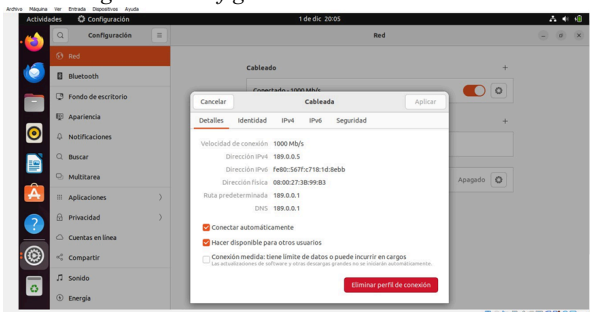
7.3 INSTALACIÓN Y CONFIGURACIÓN DE OPENVPN

Una vez configurada la infraestructura básica de red, se procedió con la instalación de OpenVPN, específicamente la opción "OpenVPN RoadWarrior" a través del Software Center de NethServer. La configuración del servidor OpenVPN incluyó los siguientes pasos:

- Se seleccionó la autenticación mediante certificados.
- Se configuró el modo "enrutado" para la transmisión de datos.
- La red privada VPN se definió como 10.1.1.0/24, con una máscara de subred 255.255.255.0.
- Se configuró la IP pública del servidor VPN (192.168.20.245) para permitir a los clientes remotos conectarse de manera segura.

Posteriormente, se crearon varias cuentas de usuario dentro del servidor OpenVPN, asignándoles direcciones IP reservadas dentro del rango de la VPN. Para cada usuario, se descargó el archivo de configuración necesario para conectar los clientes de forma remota.

Imagen 34: Configuración de Zonas de Red



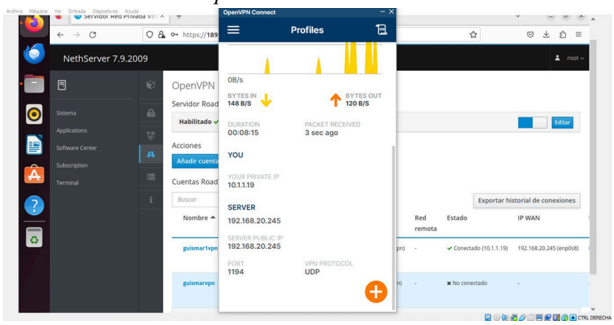
Fuente: Autoría propia.

7.4 CONEXIÓN DE CLIENTES

Para realizar la conexión remota, se utilizó OpenVPN Connect en una máquina anfitriona con Windows. El proceso incluyó la instalación del software OpenVPN y la importación de los perfiles de configuración previamente descargados desde el servidor NethServer. La conexión se estableció con éxito utilizando los perfiles configurados para cada cuenta de usuario.

La conexión remota se validó exitosamente mediante la verificación de estadísticas en el servidor y en los registros de conexión. Se observó que los clientes conectados a través de VPN estaban autenticados correctamente y con sus direcciones IP reservadas activas.

Imagen 35: Configuración de Perfiles de Usuario en OpenVPN



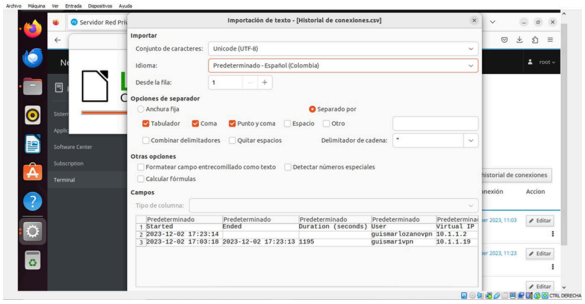
Fuente: Autoría propia.

7.5 RESULTADOS

La implementación de la VPN permitió establecer conexiones seguras entre el servidor y los clientes remotos. Los resultados de la prueba de conexión confirmaron que el túnel VPN estaba funcionando correctamente, permitiendo el acceso seguro a los recursos internos de la red. Entre los resultados más relevantes se encuentran:

- **Conexiones Exitosas:** Las cuentas configuradas pudieron acceder a la red interna a través de la VPN sin problemas.
- **Seguridad Validada:** Los registros del servidor mostraron que la autenticación por certificado fue exitosa y que las conexiones fueron seguras.
- **Control de Conexiones:** Los registros en el servidor NethServer indicaron la actividad de los usuarios conectados, incluyendo la fecha, hora e IP, lo que facilita el monitoreo de la red.

Imagen 36: Historial de conexiones



Fuente: Autoría propia.

En el mundo digital actual, donde las organizaciones dependen de la conectividad constante para sus operaciones diarias, la seguridad de la información y la protección de los datos son aspectos fundamentales en la gestión de redes. Las amenazas cibernéticas, como el acceso no autorizado y la interceptación de comunicaciones, han incrementado la necesidad de soluciones que garanticen la privacidad de los datos, especialmente cuando se accede a recursos sensibles de forma remota. En este contexto, la implementación de una Red Privada Virtual (VPN) se ha convertido en una de las herramientas más efectivas para proporcionar comunicaciones seguras a través de redes públicas, como Internet.

Una VPN crea un túnel cifrado entre el usuario y la red, ocultando la dirección IP y asegurando la transmisión de datos al garantizar que solo los usuarios autenticados puedan acceder a los recursos internos. Este tipo de red privada permite, además, el acceso remoto a recursos de la organización de manera controlada y confiable, lo cual es esencial en escenarios de trabajo a distancia o para empresas con múltiples sedes. La implementación de una VPN no solo mejora la seguridad, sino que también optimiza la conectividad y eficiencia operativa, al permitir que los usuarios accedan a sus sistemas de manera remota, sin comprometer la integridad de los datos o la privacidad de las comunicaciones.

Este artículo se centra en la implementación de una VPN utilizando NethServer, una solución de servidor basada en Linux que ofrece herramientas para la administración de redes, seguridad y servicios de infraestructura. NethServer permite crear y gestionar una VPN de manera eficiente, brindando control sobre las configuraciones de seguridad y facilitando la integración de la infraestructura de red en la organización. A través de una serie de pasos detallados, se explica cómo instalar y configurar OpenVPN dentro de NethServer, así como las configuraciones de red necesarias para establecer una conexión segura entre un servidor y clientes remotos.

El proceso comienza con la instalación del sistema NethServer en una máquina virtual, seguida de la configuración de las interfaces de red para la creación de una red interna segura. Posteriormente, se habilita el servicio OpenVPN, una de las soluciones más populares para la implementación de VPN, que permite a los usuarios remotos conectarse al servidor a través de un túnel cifrado. Además, se detalla la configuración de los clientes VPN, asegurando que puedan acceder a la red de manera efectiva.

Las pruebas de conectividad y la verificación del funcionamiento de la VPN también son parte integral de este proceso, asegurando que la solución no solo esté implementada correctamente, sino que también cumpla con los requisitos de seguridad y operatividad establecidos por la organización. Este artículo, por tanto, tiene como objetivo proporcionar una guía paso a paso para la configuración e implementación de una VPN, mostrando cómo esta tecnología puede ser una solución práctica y segura para las organizaciones que buscan mejorar la seguridad en sus redes y permitir el acceso remoto de forma controlada.

Además de su valor en la protección de datos, la VPN también se configura como una herramienta importante para optimizar la conectividad en redes distribuidas y facilitar la comunicación entre empleados en diferentes ubicaciones geográficas. Este artículo demuestra cómo la implementación de una infraestructura de VPN no solo resuelve problemas de seguridad, sino que también puede contribuir a la eficiencia y escalabilidad de las redes corporativas.

8 CONCLUSIONES

En síntesis, este trabajo ha demostrado la relevancia y eficacia de los sistemas operativos como GNU/Linux en la solución de necesidades tecnológicas complejas. A través de las prácticas realizadas, hemos evidenciado cómo la flexibilidad y la amplia comunidad de desarrolladores de Linux permiten adaptarse a diversos escenarios y resolver inconvenientes de manera eficiente. Su naturaleza de código abierto y su capacidad de personalización hacen que sea una opción atractiva tanto para usuarios individuales como para organizaciones, siempre que se elija en función de las necesidades específicas de cada entorno.

En el ámbito de la gestión de redes, la implementación de un proxy en NethServer ha probado ser una solución robusta para el control del tráfico y la seguridad en entornos organizacionales. Gracias a sus herramientas avanzadas, como el módulo Web Proxy & Filter, es posible gestionar el acceso a Internet, filtrar contenido no deseado y mejorar la eficiencia de la red mediante la autenticación de usuarios y la generación de reportes detallados, lo que es esencial para instituciones que requieren un control y supervisión precisos de sus recursos.

La adopción de topologías de red avanzadas, como la configuración verde, naranja y DMZ, ha mostrado ser una estrategia eficaz para proteger las infraestructuras mediante la segmentación del tráfico y el control del acceso. Utilizando NethServer como cortafuegos, esta configuración asegura que los servicios públicos estén disponibles de manera segura, mientras que las redes internas permanecen protegidas, brindando un control total sobre el flujo de información y reduciendo los riesgos de intrusión.

Por otro lado, la implementación de servicios de archivo e impresión en NethServer, junto con un controlador de dominio LDAP, ha mejorado significativamente la gestión de recursos compartidos en entornos corporativos. Esta integración no sólo centraliza la administración, sino que también optimiza la seguridad y facilita el acceso a carpetas e impresoras compartidas, mejorando la conectividad y

productividad de los usuarios dentro de la organización, mientras refuerza la capacidad de la empresa para enfrentar los desafíos tecnológicos actuales.

Por último, la implementación de una VPN utilizando NethServer y OpenVPN ha proporcionado una solución segura para el acceso remoto a redes internas. Esta configuración garantiza la protección de los datos mediante cifrado y oculta las direcciones IP de los usuarios, mejorando así la confidencialidad y la seguridad. La combinación de NethServer y OpenVPN se ha consolidado como una herramienta confiable y robusta para organizaciones que requieren un acceso remoto seguro y un control eficiente sobre su infraestructura de red, asegurando la protección de la información en todo momento.

9 REFERENCIAS

[1] I. Gómez-Marí and A. Pedrosa-Sáez, "La educación en la era del metaverso. ¿Está la comunidad educativa preparada?: Análisis de las actitudes y el conocimiento del alumnado, docentes y familias hacia la inclusión del metaverso en la educación," *EducaT: Educación Virtual, Innovación Y Tecnologías*, vol. 4, no. 1, pp. 3-44, 2023.

[2] D. Guzmán Arévalo, "OVI Unidad I_Nivelación," *Repositorio Institucional UNAD*, 2017.

[3] P. F. Hernández, "Software Libre y Open Source," Objeto Virtual de Aprendizaje (OVA), Repositorio Institucional UNAD, 2022.

[4] P. F. Hernández and J. Sánchez, "Monitoreo y administración de sistemas Linux," *Objeto Virtual de Información (OVI)*, *Repositorio Institucional UNAD*, 2022.

[5] C. H. Vargas, "OVI Implementando el entorno de trabajo GNU Linux," *Repositorio Institucional UNAD*, 2020.

[6] NethServer: https://www.nethserver.org/

[7] NethServer: https://docs.nethserver.org/projects/ns8/en/latest/user_domains.html

[8] Equipo de Documentación de NethServer. (2020). Filtro de contenido web — NethServer 6.10 Final. Nethesis Srl. Recuperado de https://docs.nethserver.org/

[9] NethServer Community. (2018). Configuración de Proxy y Filtro de Contenido en NethServer. Recuperado de https://community.nethserver.org/

[10] López, R. (2019). Implementación de servicios de proxy y filtrado de contenido en redes empresariales. Editorial TecnoRed.

[11] Fundación Squid. (2023). Squid: Optimizando la entrega web. Proyecto Squid. Recuperado de http://www.squid-cache.org/

Notas:

1. La implementación de Nethserver permite automatizar tareas clave como la asignación de direcciones IP (DHCP) y la resolución de nombres (DNS), lo que mejora la eficiencia en la administración de redes, reduciendo la intervención manual y los errores.

2. La configuración de un proxy y un cortafuegos en Nethserver es crucial para garantizar el control del acceso a Internet y la seguridad de la red, limitando el acceso a contenido no deseado y protegiendo la infraestructura contra amenazas externas.

3. Nethserver facilita la integración con estaciones de trabajo GNU/Linux a través de servicios como LDAP para la autenticación centralizada, mejorando la gestión de usuarios y el acceso a recursos compartidos.