ABORDANDO REQUERIMIENTOS PARTICULARES MEDIANTE EL USO DE GNU/LINUX NETHSERVER.

Integrante 1 (David Felipe Diaz Galeano)
e-mail: dfdiaz@unadvirtual.edu.co
Integrante 2 (Alejandro Mejía Buitrago)
e-mail: amejiabu@unadvirtual.edu.co
Integrante 3 Breiner Mosquera Moreno
e-mail: bmosqueramor@unadvirtual.edu.co

RESUMEN: *El presente articulo enseña la instalación de Nethserver, la configuración y los servicios que presta al convertirse en la plataforma de internet, la cual pide la guía de actividades, para poner en marcha las funcionalidades de Nethserver se desarrollan cinco Temáticas en las cuales se configuran los servicios de DHCP Server, los servicios de DNS Server y controlador de dominio, configuración de servicio proxy, configuración de cortafuegos, File server, Print Server y los servicios de VPN.*

PALABRAS CLAVE: configuración de servicios, controlador de dominio, DHCP Server, nethserver, cortafuegos, proxy.

1 INTRODUCCIÓN

En el presente trabajo se pretende aplicar todos los conocimientos adquiridos en el desarrollo del diplomado, en especial todo lo relacionado con instalación y configuración de servicios web, para ello se deben resolver las problemáticas planteadas en la guía de actividades.

Con este trabajo se pretende implementar y configurar el acceso de una estación de trabajo GNU/Linux, a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras mediante el Nethserver.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar soluciones en GNU/Linux mediante la instalación, configuración y activación de una infraestructura tecnológica que satisfaga las necesidades particulares de la empresa.

2.2 OBJETIVOS ESPECIFICOS

- Establecer y configurar el acceso a una estación de trabajo GNU/Linux mediante un usuario y una contraseña, así como registrar esta estación en los servicios de infraestructura IT de Nethserver.
- Gestionar el acceso a la conectividad a Internet de estaciones GNU/Linux a través del puerto 3128 de un servidor proxy.

3 INSTALACION DEL NETHSERVER

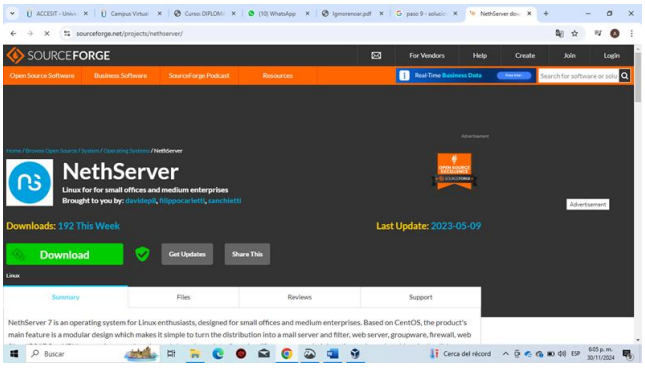
NethServer es una distribución de Linux, concretamente basada en CentOS y Red Hat, diseñada para funcionar como servidor en pequeñas y medianas empresas.

Este sistema operativo es altamente modular, lo que permite la fácil adición de nuevos plugins y software adicional para ampliar sus funcionalidades predeterminadas. Desde la versión 7.7, se introdujo una interfaz intuitiva con un diseño más moderno, que facilita la gestión de cuentas, DNS, DHCP, FQDN, configuración de aplicaciones, administración de almacenamiento y certificados SSL. También permite la configuración de VPN, el monitoreo del tráfico de cada túnel, el seguimiento del historial de conexión de los usuarios, la definición de rutas personalizadas y el cambio entre los protocolos UDP/TCP, entre otras características.

4 PROCESO DE INSTALACION DEL NETHSERVER

Primero ingresamos a la página oficial y realizamos la descarga de la imagen iso.

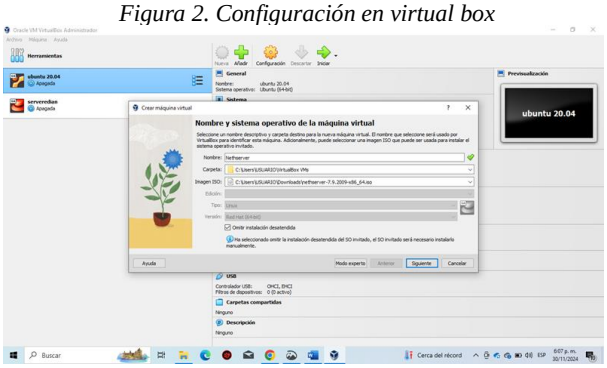
Figura 1. Instalación del Nethserver



fuente: Autoria propia

5 INICIAMOS CON LA INSTALACION EN VIRTUAL BOX

Figura 2. Configuración en virtual box



Fuente: Autoria propia

Figura 3. Instalación imagen iso.
Fuente: Autoría propia

Figura 4. Configuración del sistema

Fuente: Autoría propia

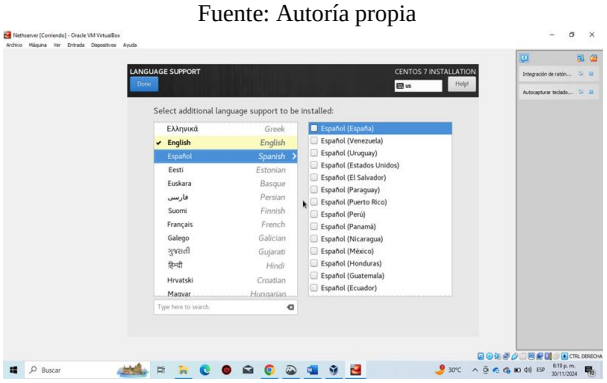


Figura 5. Configuración del teclado

Se configura el host name y se verifica las tres tarjetas red.

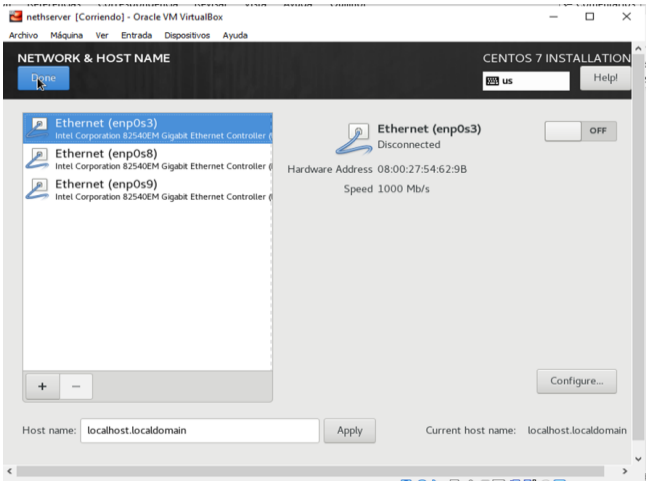


Figura 6. Configuración de redes

Se crea la contraseña para el usuario root y se inicia el proceso

Figura 7. Se inicia la instalación del Nethserver

Luego de la instalación, se procede a ingresar con las credenciales configuradas y se utiliza el comando yum update

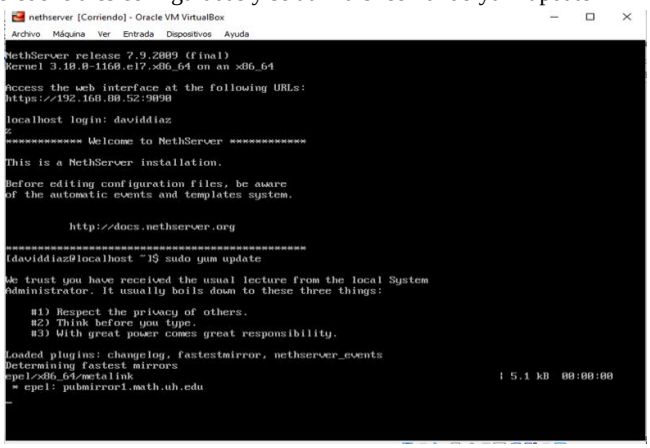


Figura 8. Instalación finalizada

Se cargará la página de ingreso, entrar con el usuario root y clave que ya se habían designado previamente

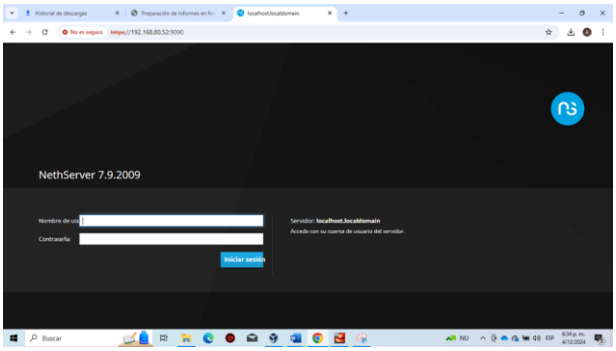


Figura 9. Pagina Nethserver

Ingresamos al panel de control y se realiza las configuraciones necesarias.

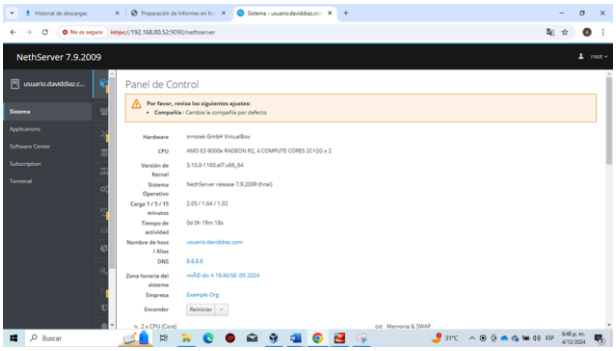


figura 10. Panel de control

6 DESARROLLO DE LAS TEMATICAS

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

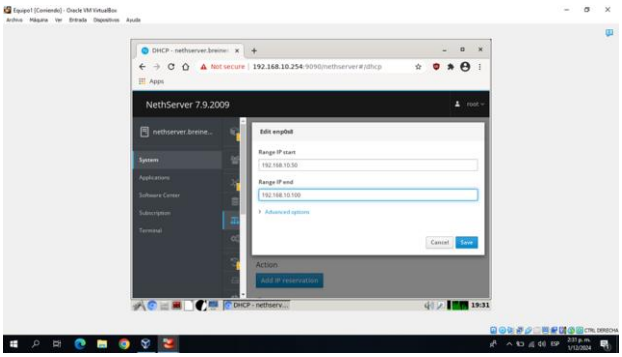


Figura 11. activamos DHCP servidor

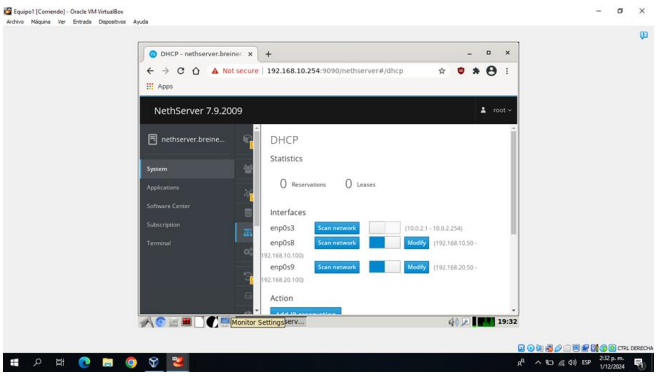


Figura 12. Configuramos DHCP

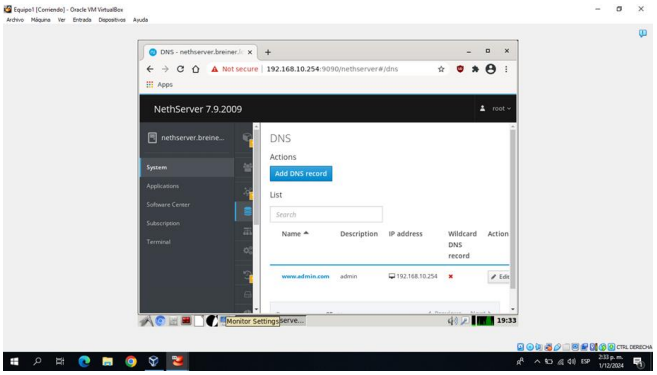


Figura 13. Activamos DNS con www.admin.com

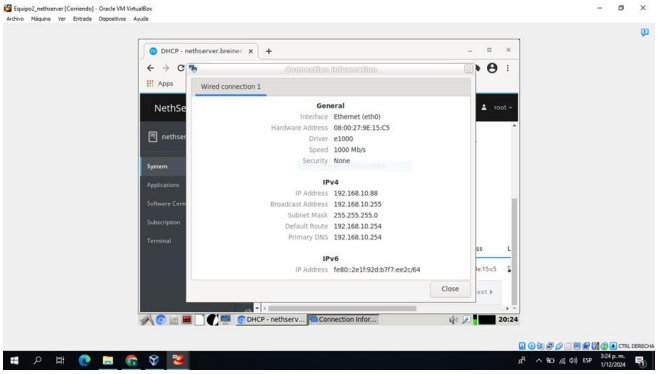


Figura 14. Verificamos la ip dada por el servidor

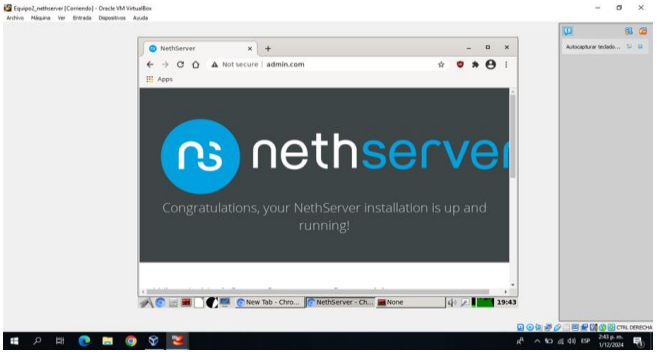


Figura 15. Verificamos el DNS del servidor

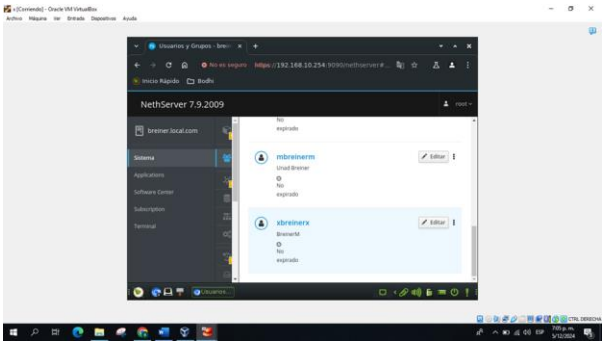


Figura 16. Creamos usuario

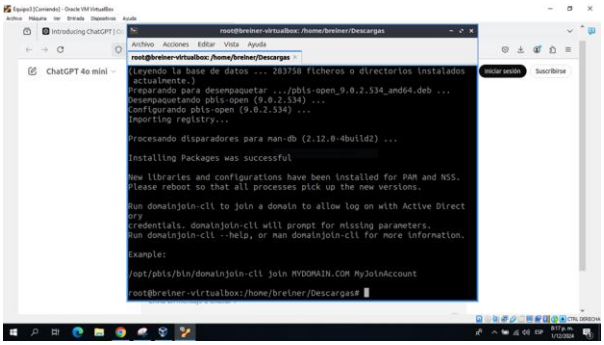


Figura 17. Descargamos PBIS OPEN

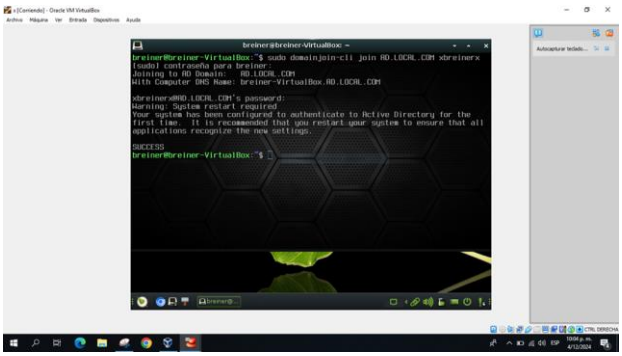


Figura 18. Hacemos la conexión al user

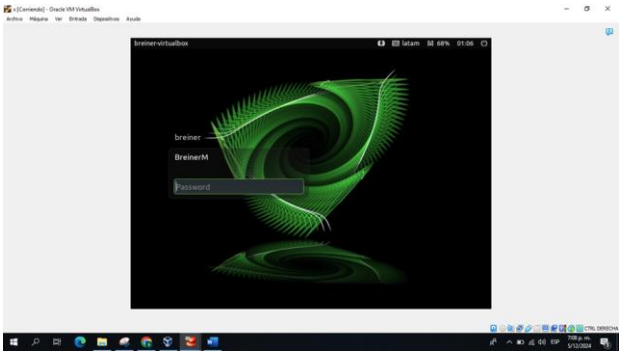


Figura 19. Hacemos el reboot

6.2 TEMÁTICA 2: PROXY

Un proxy es un servidor intermedio que actúa como un intermediario entre los clientes y los servidores a los que intentan acceder. Su función principal es redirigir las solicitudes de los clientes hacia el servidor de destino y devolver las respuestas a los usuarios. Este dispositivo es ampliamente utilizado en diversos entornos debido a sus capacidades para controlar el tráfico de la red, mejorar el rendimiento y garantizar la seguridad.

En entornos empresariales y organizacionales, los proxies son implementados para gestionar el acceso a Internet de los empleados, con el fin de aplicar políticas de uso, bloquear contenido no deseado, como redes sociales o sitios de entretenimiento, y controlar el tráfico de red de manera más eficiente. Además, los proxies pueden proporcionar mejoras en el rendimiento mediante el almacenamiento en caché de contenido estático, lo que reduce la carga en los servidores de origen y mejora la velocidad de acceso a sitios web frecuentemente visitados.

En términos de seguridad, los proxies actúan como una barrera entre la red interna y la web externa, permitiendo filtrar solicitudes maliciosas y proteger los dispositivos internos de posibles ataques. Adicionalmente, los proxies son utilizados para proporcionar anonimato a los usuarios, ocultando sus direcciones IP reales y dificultando el rastreo de sus actividades en línea.

En el ámbito de la educación, especialmente en escuelas y universidades, los proxys se utilizan para restringir el acceso a contenido inapropiado o no relacionado con el ámbito académico. Este tipo de implementación también facilita el monitoreo y la auditoría del uso de Internet para fines educativos.

Los usuarios individuales también recurren a los proxies para acceder a contenido geográficamente restringido, como en plataformas de streaming, y para mejorar su privacidad en línea, al ocultar su identidad y ubicación en la web.

6.2.1 CONFIGURACION DEL PROXY

La configuración del servidor proxy en Nethserver tuvo como objetivo principal establecer un control eficaz sobre el acceso a Internet desde las estaciones de trabajo conectadas a la red interna. Este servicio permite monitorear el tráfico de red, aplicar políticas de acceso y garantizar un uso eficiente de los recursos disponibles, especialmente en entornos de instituciones complejas donde es necesario restringir ciertos contenidos o priorizar aplicaciones críticas.

En este caso, el proxy se configuró para operar en el puerto estándar 3128, y se realizaron ajustes específicos para filtrar el acceso a sitios web de redes sociales y entretenimiento, como YouTube y Facebook. Esto incluyó la creación de reglas personalizadas que definen qué tipos de contenido están permitidos o bloqueados. Además, el proxy se integró con el sistema de autenticación de usuarios, asegurando que solo aquellos con credenciales válidas puedan acceder a los servicios de Internet.

Para validar la configuración, se utilizó una estación de trabajo virtual basada en Debian, configurada con la dirección IP estática 10.0.1.67. En esta máquina, se ajustaron las configuraciones del navegador Firefox para que todo el tráfico

pasara a través del proxy de Nethserver. Durante las pruebas, se verificó que las políticas establecidas funcionaran correctamente, bloqueando el acceso a sitios restringidos mientras se permitía la navegación en portales autorizados.

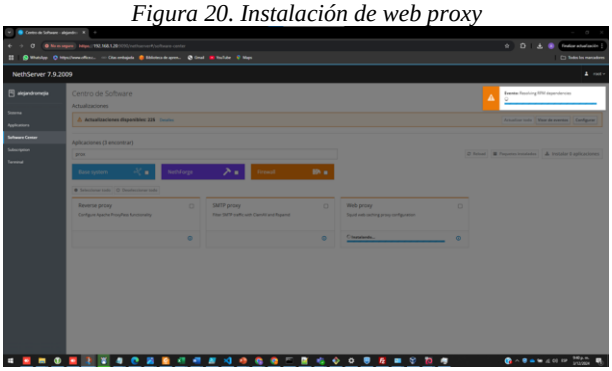
Esta implementación demuestra cómo el uso de un proxy no solo mejora la seguridad de la red interna, sino que también optimiza el ancho de banda disponible y facilita la auditoría del tráfico de red

6.2.2 HABILITACION DEL SERVICIO PROXY

INSTALACION DEL MODULO

El módulo "Web Proxy" se instaló desde el Software Center de Nethserver para habilitar las funciones de filtrado y control del tráfico web en la red interna. Esta herramienta permite gestionar de manera centralizada el acceso a Internet, estableciendo políticas de uso específicas para usuarios o dispositivos conectados. La instalación fue sencilla, ya que Nethserver proporciona un entorno intuitivo para agregar funcionalidades directamente desde su consola de administración web. Una vez instalado, se procedió con la configuración detallada para adaptar el proxy a las necesidades del entorno administrado

Figura 20. Instalación de web proxy



Fuente: Autoría Propia

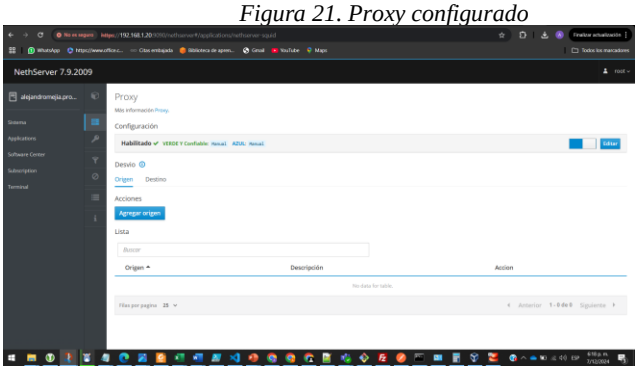
Configuración Básica

- Modo de operación: El modo de operación no transparente del Proxy implica que los clientes o navegadores deben configurarse manualmente para redirigir su tráfico a través del servidor Proxy. A diferencia del modo transparente, en el que el tráfico se redirige automáticamente sin intervención del cliente, el modo no transparente requiere que los usuarios especifiquen la dirección del Proxy en la configuración de su navegador. Esto permite un control más explícito sobre qué dispositivos y usuarios utilizan el Proxy para acceder a Internet, asegurando que todas las solicitudes sean filtradas y monitorizadas de acuerdo con las políticas definidas.

- El puerto predeterminado 3128: es comúnmente utilizado por el servidor Proxy para gestionar el tráfico web. Este puerto se configura para recibir y redirigir las solicitudes de los navegadores que están configurados para usar el Proxy. Es importante que el puerto esté abierto en el firewall de la red para asegurar la correcta comunicación entre los clientes y el servidor Proxy.Registro de actividad: Activado para auditar las solicitudes de acceso.

- Registro de actividad: al estar activado, permite auditar todas las solicitudes de acceso que pasan a través del Proxy. Esto es crucial para realizar un seguimiento detallado del tráfico web, identificar patrones de uso, y verificar el cumplimiento de las políticas de acceso a Internet. Los registros pueden incluir información como la URL solicitada, la dirección IP del cliente, el tipo de solicitud, y la hora de acceso, lo que facilita la administración y la resolución de problemas relacionados con la conectividad o el abuso del acceso a Internet.

Figura 21. Proxy configurado



Fuente: Autoría Propia

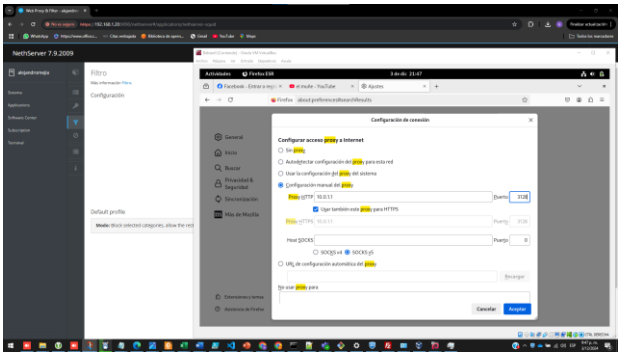
6.2.3 IMPLEMENTACION EN LA RED

Consistió en integrar los servicios configurados en el servidor Nethserver con la infraestructura de red interna. Para ello, se definieron adaptadores de red que conectaban el servidor tanto a la red local (Zona Verde) como al acceso externo (Zona Roja). La estación de trabajo, configurada como cliente en la red interna, fue ajustada para utilizar el servidor como punto central de control.

Este proceso incluyó asignar direcciones IP estáticas dentro del rango definido, configurar las reglas necesarias para el tráfico entre las zonas de red y validar el funcionamiento de los servicios, como el proxy y la VPN. Esta integración garantizó que los servicios ofrecidos por el servidor fueran accesibles y operativos dentro del entorno administrado, optimizando la conectividad y el control de recursos.

- Configuración de la Red Verde
  El adaptador de red interna en VirtualBox fue configurado como red interna.
  La máquina cliente Debian obtuvo la dirección IP 10.0.1.67 dentro del rango 10.0.1.0/24.
- Configuración del Cliente (Firefox)
  En la máquina virtual Debian, se configuró Firefox para usar el Proxy con la IP del servidor (10.0.1.1) y el puerto 3128.

Figura 22. Configuración de proxy en navegador



Fuente: Autoría Propia

6.2.4 PRUEBAS REALIZADAS

Detalla las pruebas ejecutadas para verificar el funcionamiento adecuado de los servicios implementados en el servidor Nethserver. Las pruebas fueron diseñadas para asegurar que los servicios de red y el Proxy, operaran según lo esperado en el entorno de la infraestructura configurada.

En el caso del Proxy, se configuraron estaciones de trabajo dentro de la red interna para verificar que el acceso a Internet fuera controlado a través del servidor, permitiendo el tráfico según las políticas establecidas.

Las pruebas también incluyeron la validación del rendimiento de cada servicio, la resolución de posibles incidencias y la revisión de logs para confirmar que los servicios estuvieran funcionando sin errores. Estas pruebas fueron fundamentales para garantizar la correcta implementación de los servicios de infraestructura IT.

6.2.5 ACCESOS A SITIOS PERMITIDOS

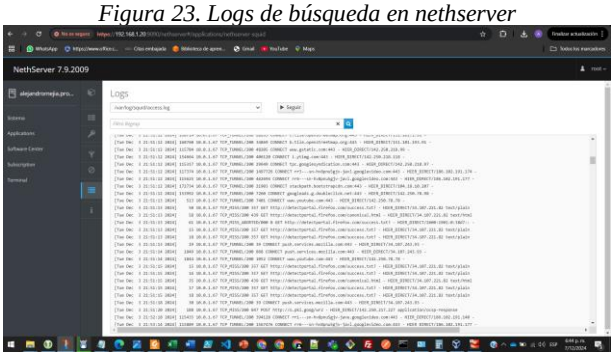
Para validar el funcionamiento del Proxy, se realizaron pruebas de navegación en sitios web populares como YouTube y Facebook desde una máquina virtual que operaba dentro de la red interna. Durante estas pruebas, se configuró el navegador de la estación de trabajo para que utilizara el Proxy, permitiendo que todo el tráfico de Internet pasara a través del servidor Nethserver. Con esto verificamos que el servidor estuviera cumpliendo con su función de control y filtrado de acceso a los sitios web.

Se observó que el Proxy no solo permitía el acceso a las páginas solicitadas, sino que también registraba todas las solicitudes HTTP realizadas. Esto fue confirmado al revisar los registros generados por el sistema. Los registros detallaban las solicitudes HTTP efectuadas por los usuarios, incluyendo la URL solicitada, la dirección IP de origen y otros detalles relevantes sobre cada petición. Estos registros permitieron verificar que el tráfico estaba siendo adecuadamente monitorizado y controlado, conforme a las políticas definidas para el acceso a Internet.

Las capturas de los registros mostraron que las solicitudes provenientes de la máquina virtual con la IP 10.0.1.67 estaban siendo correctamente gestionadas por el servidor Proxy. Las entradas en los registros indicaban las direcciones URL youtube.com y facebook.com, confirmando que el tráfico estaba pasando correctamente por el servidor Nethserver antes de llegar a su destino.

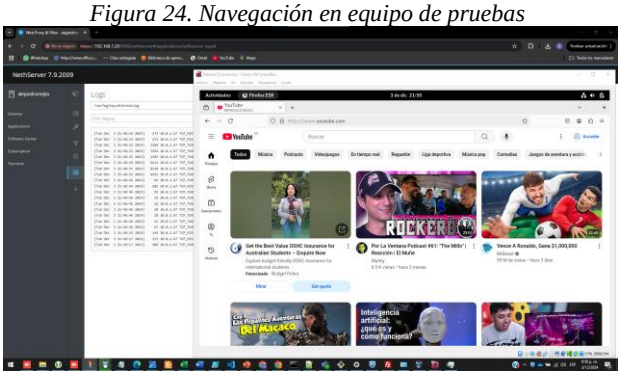
Este comportamiento demostró la operatividad del Proxy en términos de filtrado, monitoreo de tráfico y control de acceso a los servicios en línea, cumpliendo con los requisitos establecidos para la gestión de la conectividad en la red interna.

Figura 23. Logs de búsqueda en nethserver



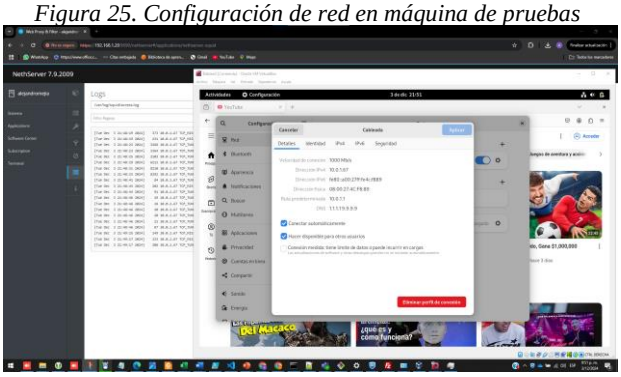
Fuente: Autoría Propia

Figura 24. Navegación en equipo de pruebas



Fuente: Autoría Propia

Figura 25. Configuración de red en máquina de pruebas



Fuente: Autoría Propia

6.3 TEMÁTICA 3: CORTAFUEGOS

Ingresamos a la plataforma e iniciamos con la configuración de cada uno de nuestros puertos, la cual el verde

se utilizará como red LAN, el naranja como red DMZ y finalmente el rojo como red WAN.

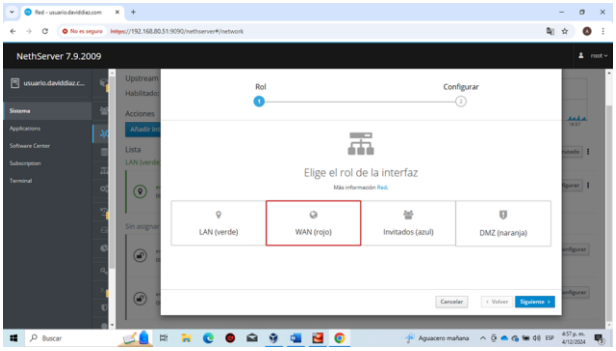


Figura 26. Configuración de la red roja-WAN

Para la red roja-WAN, indicaremos que su configuración de red sea por protocolo DHCP y tomaremos la IP que nos brinde la red, para utilizarla como puerta de enlace de nuestra red verde-LAN.

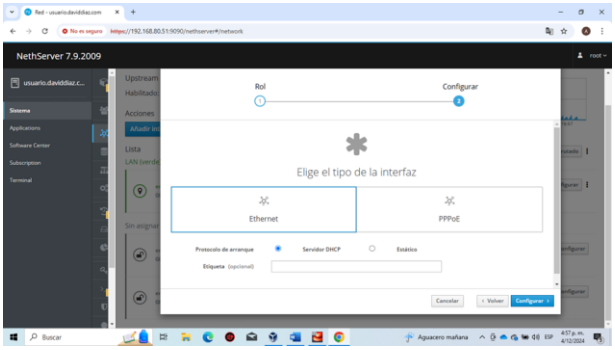


Figura 27. Se elige el protocolo DHCP

Para la configuración de la red verde-LAN elegiremos el puerto de nuestra máquina virtual que configuramos con red interna

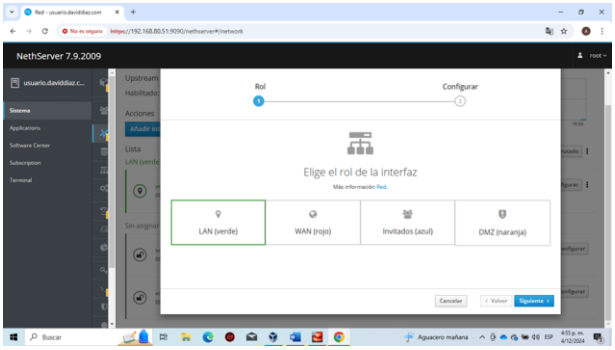


Figura 28. Se configura la red verde-LAN

Se procede con la configuración con protocolo de IP estática, la cual utilizamos la misma IP que se utilizó para ingresar a nethserver.

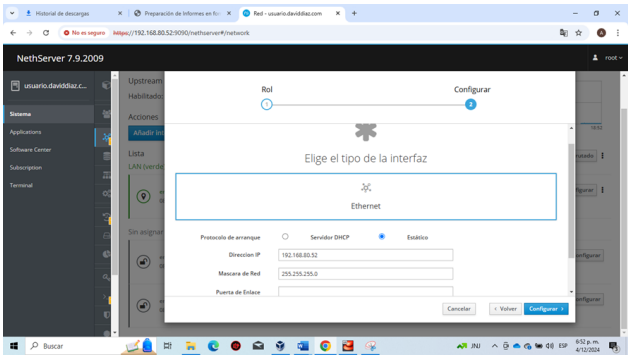


Figura 29. Se realiza la parametrización de nuestra red verde-LAN

Procedemos a la configuración de la red naranja-DMZ, la cual utilizaremos una IP diferente a la red LAN y a la red WAN.

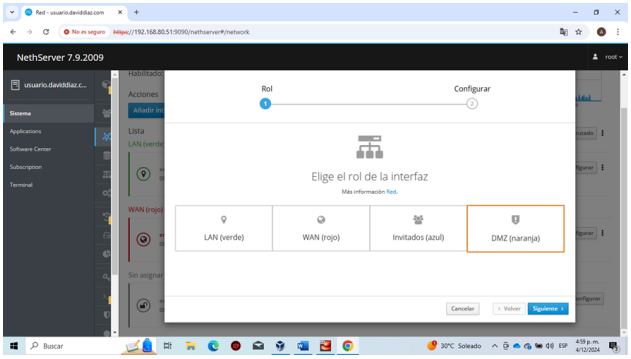


Figura 30. Elegimos la red DMZ naranja

Se procede a colocar la dirección IP con un segmento de red diferente al de la red LAN y red WAN.

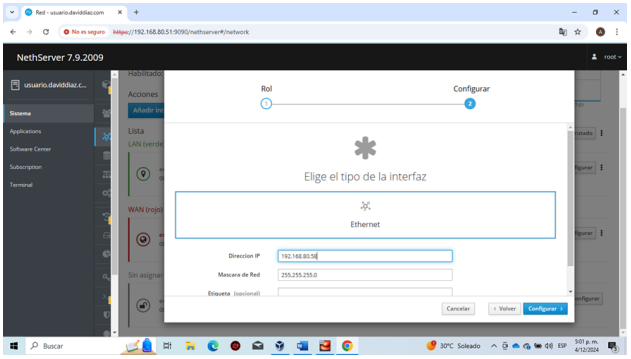


Figura 31. Se añade la dirección IP y la máscara de red.

Ingresamos a software center y descargamos las aplicaciones necesarias, la cual la más importante es la del paquete básico de firewall.

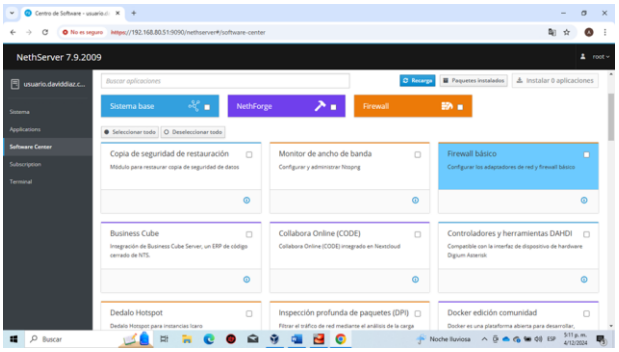


Figura 32. Instalación del firewall básico

Ingresamos al servidor del firewall y vemos como quedo nuestra topología

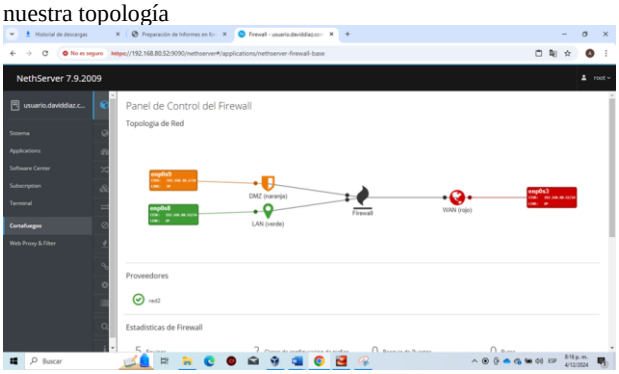


Figura 33. Topología de red

Procedemos a ingresar a web proxy y desde allí en categorías configuramos la lista negra.

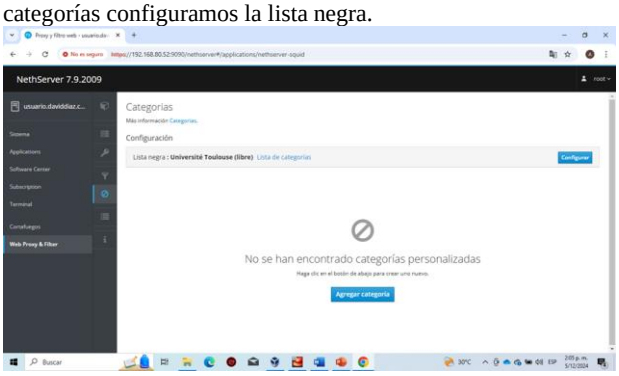


Figura 34. Web proxy

Luego, ingresamos a filtro y editamos el perfil por defecto, y allí seleccionamos social networks

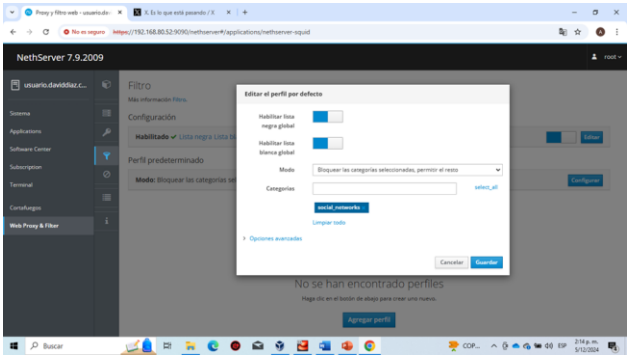


Figura 35. filtro

Ingresamos a la terminal del sistema e ingresamos el comando nslookup www.facebook.com para crear la regla

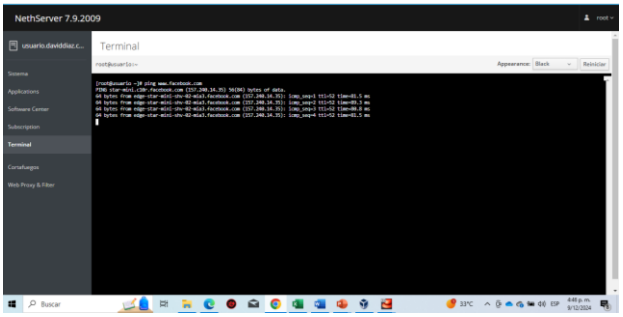


Figura 36. IP Facebook

Creamos la regla con la IP identificada en la terminal, la cual nos permitirá bloquear el acceso

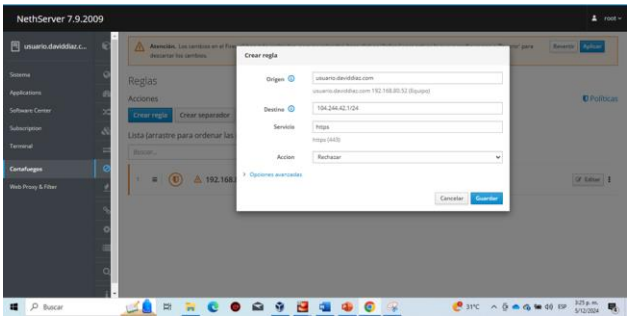


Figura 37. Configurar regla de bloqueo

Ingresamos a ubuntu, y verificamos inicialmente la conexión a la página y luego se puede observar que no hay conexión a la pagina

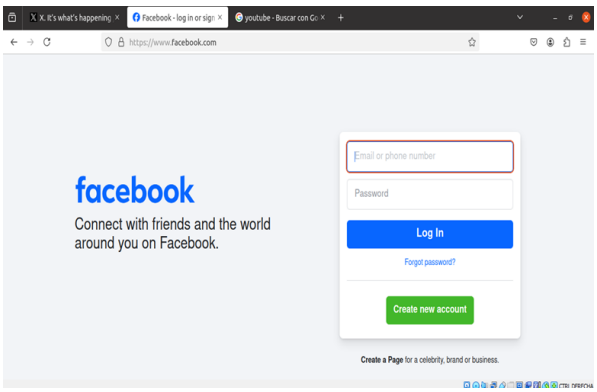


Figura 38. Pagina Facebook con conectividad

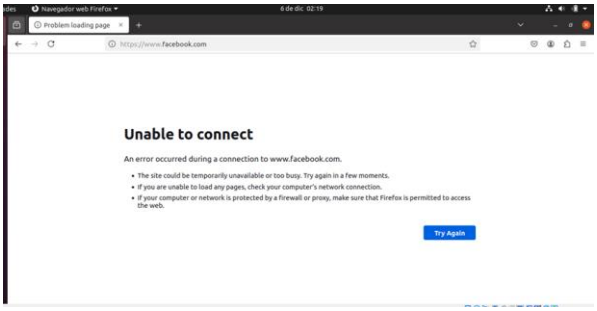


Figura 39. Pagina sin acceso

6.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

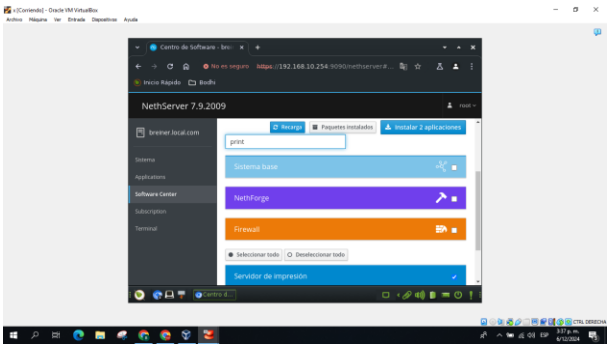


Figura 40. instalamos los paquetes de file server y print server

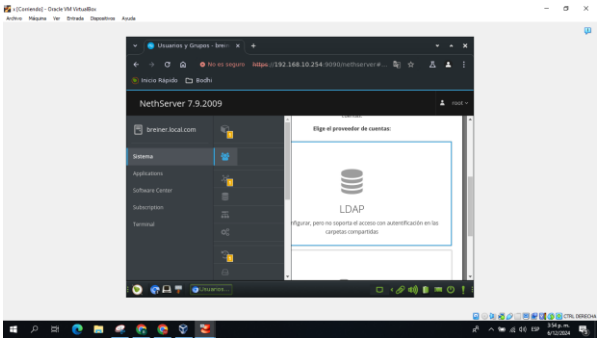


Figura 41.Setiamos el provedor de directorios con LDPA

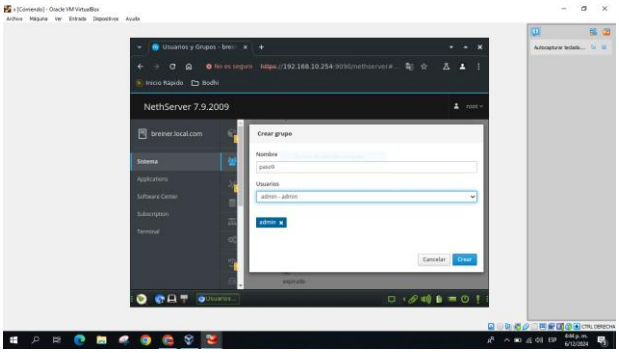


Figura 42.Creamos un grupo

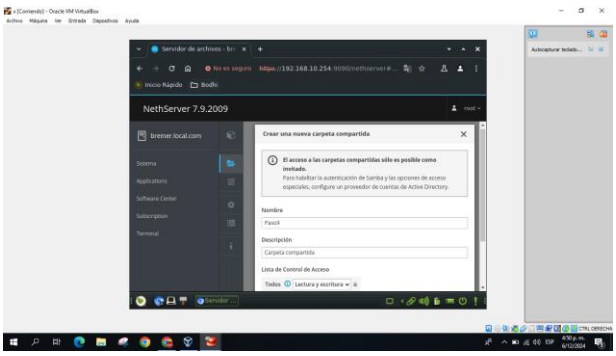


Figura 43.Creamos la carpeta compartidad y la llamamos paso9

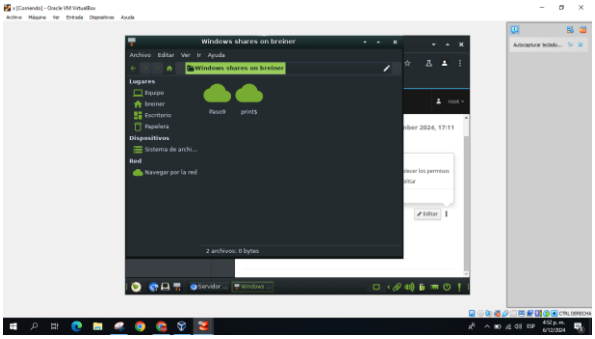


Figura 44.Verificamos la carpeta un equipo de la red

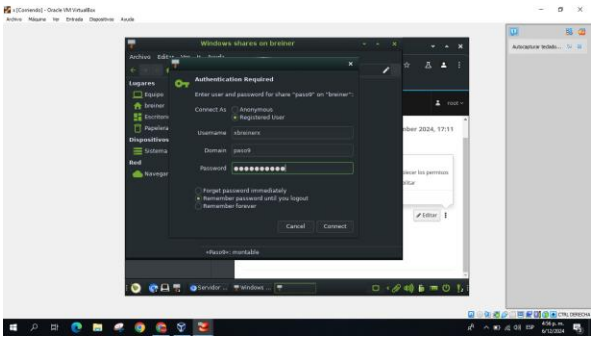


Figura 45. Verificando

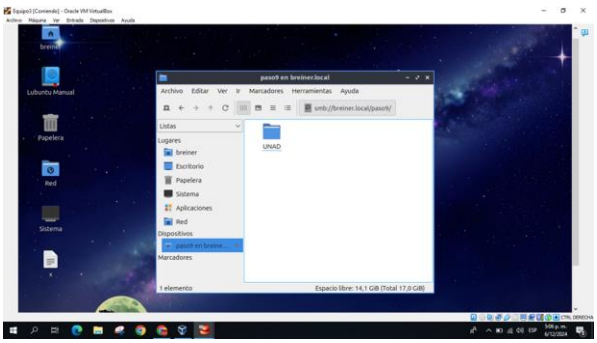


Figura 46. Verificamos en otro equipo de la red

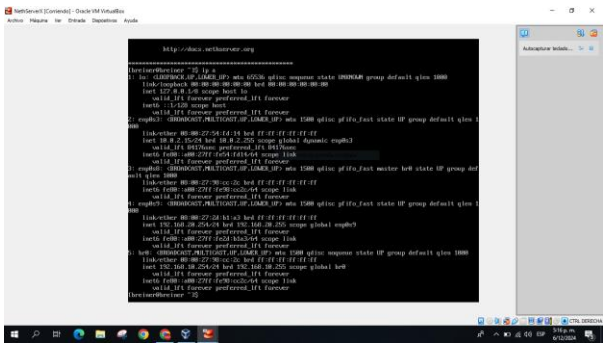


Figura 47.Chequeamos el ip asignano en la NAT

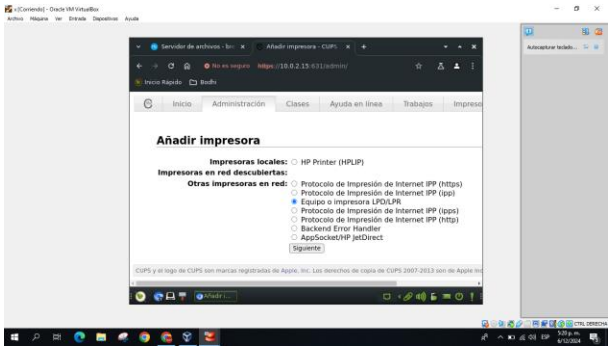


Figura 48.Entramos con la ip dada por NAT por el puerto 631

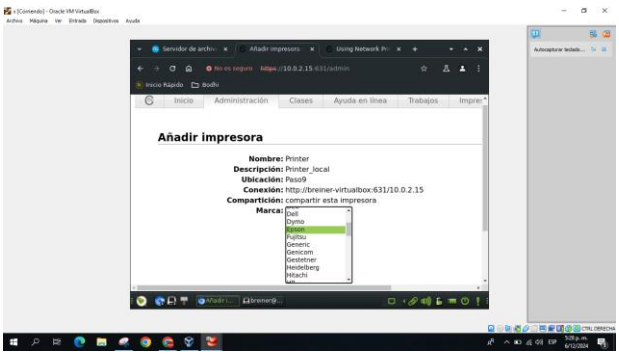


Figura 49. Setiamos la impresora

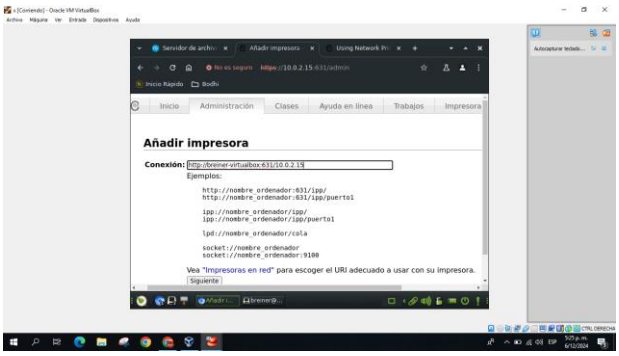


Figura 50.Configuramos la conexión de la impresora

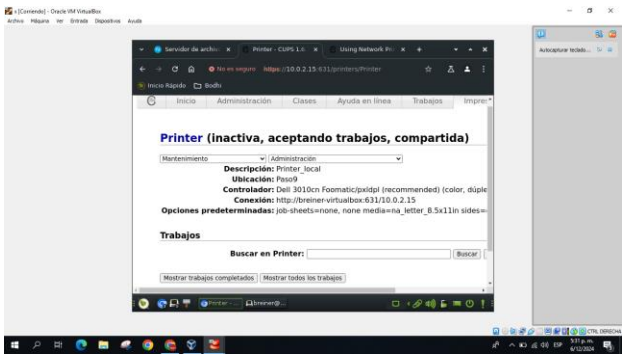


Figura 51.Verificamos la impresora

6.5 TEMATICA 5 CONFIGURACION DE VPN

Una Red Privada Virtual (VPN) es una tecnología que permite establecer una conexión segura y cifrada a través de una red pública, como Internet, permitiendo que los usuarios accedan de manera remota a una red privada, como la de una empresa, de manera segura. El uso principal de una VPN es garantizar la confidencialidad, integridad y autenticidad de los datos transmitidos entre los dispositivos conectados y la red privada a la que se accede.

Las VPNs son ampliamente utilizadas en entornos corporativos y empresariales para permitir a los empleados trabajar de manera remota desde cualquier ubicación, sin comprometer la seguridad de la información. A través de una VPN, los trabajadores pueden acceder a recursos internos, como servidores, bases de datos y aplicaciones, como si estuvieran físicamente en la oficina, pero con el beneficio de estar protegidos contra posibles amenazas en redes públicas.

Una de las funciones más destacadas de una VPN es la cifrado de datos, que protege la información sensible de ser interceptada por atacantes mientras viaja a través de redes inseguras. Esto es esencial, especialmente en sectores como la banca, salud y gobiernos, donde la protección de datos personales y confidenciales es crucial.

En cuanto a la privacidad en línea, las VPNs son utilizadas por usuarios individuales para ocultar su dirección IP real y cifrar su tráfico de Internet, evitando que terceros, como proveedores de servicios de Internet (ISP) o incluso sitios web, rastreen su actividad en línea. Las VPNs también son útiles para eludir restricciones geográficas de contenido, permitiendo el acceso a servicios y plataformas bloqueadas en determinadas ubicaciones geográficas.

Una VPN puede ayudar a optimizar la red mediante el uso de túneles de comunicación que priorizan el tráfico y mejoran la latencia, lo que puede resultar en una mejor experiencia para los usuarios, especialmente en aplicaciones críticas o en el acceso remoto a sistemas internos.

6.5.1 CONFIGURACION DE LA VPN

La implementación de la Red Privada Virtual (VPN) en el entorno de Nethserver permitió establecer un canal de comunicación seguro y cifrado entre la red interna gestionada por el servidor Nethserver y un cliente remoto. Esta solución fue diseñada para garantizar la seguridad de los datos transmitidos entre ambos puntos, especialmente cuando los dispositivos remotos acceden a recursos internos a través de redes públicas o no confiables como Internet.

El proceso comenzó con la configuración de OpenVPN en el servidor Nethserver, lo que permitió crear un túnel de comunicación seguro a través del cual los datos son cifrados, protegiendo así la confidencialidad e integridad de la información que circula entre el servidor y el cliente. Para los usuarios remotos, la VPN ofreció la posibilidad de conectarse a la red interna de la organización como si estuvieran físicamente en la oficina, proporcionando acceso a recursos como servidores de archivos, aplicaciones internas y bases de datos de manera segura.

La configuración de la VPN incluyó la asignación de una red interna específica para la conexión VPN, como es el caso del segmento de red 10.0.10.1/24, lo que permitió gestionar y direccionar adecuadamente el tráfico de la VPN dentro de la infraestructura de red administrada. En este contexto, el cliente remoto recibió una dirección IP dentro de este segmento, en este caso 10.0.10.2, asegurando que las solicitudes y respuestas fueran enrutadas de forma correcta y eficiente entre los dispositivos conectados.

6.5.2 INSTALACION DEL MODULO OPEN VPN

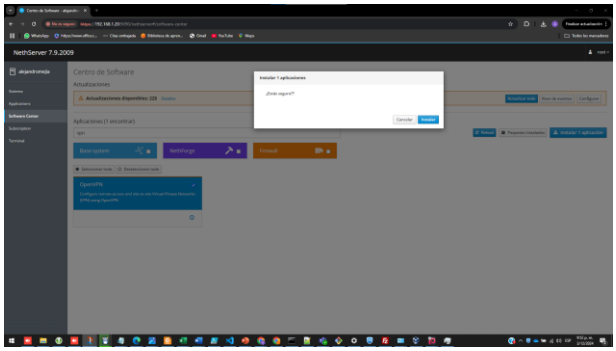
Para iniciar el proceso, se accedió al Software Center de Nethserver, una plataforma de administración que facilita la instalación y gestión de módulos adicionales necesarios para expandir las capacidades del servidor. A través de una interfaz intuitiva, se seleccionó OpenVPN, el cual es un servicio de código abierto que permite crear conexiones VPN seguras. Este módulo se instaló sin complicaciones, aprovechando las dependencias y configuraciones predeterminadas que Nethserver ofrece para asegurar una integración fluida con su infraestructura.

La instalación de OpenVPN a través del Software Center fue rápida y eficiente, ya que Nethserver gestiona automáticamente las configuraciones de software y los ajustes necesarios para que el servicio funcione correctamente en el sistema operativo.

Una vez instalado el módulo OpenVPN, se procedió a configurar las opciones de seguridad, como la autenticación de los clientes, la asignación de direcciones IP a los dispositivos remotos y la creación de las reglas de tráfico necesarias para que la VPN funcione correctamente.

También se realizó la configuración de certificados y claves criptográficas, que son esenciales para asegurar que la comunicación entre los dispositivos esté cifrada y protegida contra posibles ataques de interceptación.

Figura 52. Instalación del servicio Open VPN



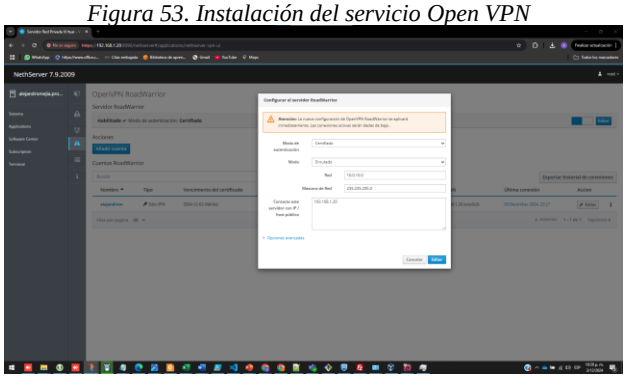
Fuente: Autoría Propia

6.5.3 CONFIGURACION DEL SERVIDOR VPN

La configuración de la VPN en Nethserver fue un paso esencial para garantizar la seguridad en la comunicación remota entre la red interna de la organización y los usuarios externos. Utilizando OpenVPN, una herramienta robusta y flexible, se configuró un túnel seguro para la transmisión de datos cifrados, protegiendo la integridad y confidencialidad de la información mientras transitaba a través de redes no confiables, como Internet.

Se definió un segmento de red privado específico para la VPN 10.0.10.1/24, permitiendo que los dispositivos conectados a través de la VPN recibieran direcciones IP dentro de este rango, como 10.0.10.2, asegurando que el tráfico fuera dirigido y enrutado de manera eficiente.

Figura 53. Instalación del servicio Open VPN



Fuente: Autoría Propia

6.5.4 CONFIGURACION DEL CLIENTE VPN

En el entorno del cliente, se utilizó un PC conectado a una red doméstica con acceso a Internet, el cual fue configurado para acceder de manera remota a la red interna mediante la implementación de OpenVPN. El software cliente de OpenVPN fue instalado en el dispositivo y configurado utilizando los archivos de configuración generados por Nethserver durante el proceso de implementación de la VPN. Estos archivos contenían los certificados y las claves necesarias para establecer una conexión segura, así como las direcciones de servidor y puerto, permitiendo al cliente autenticarse correctamente y acceder a la red interna.

Una vez configurado el cliente, se estableció una conexión VPN exitosa, y al cliente se le asignó una dirección IP dentro del rango de la red privada de la VPN, en este caso 10.0.10.2. Esta asignación de IP aseguraba que el tráfico del cliente fuera correctamente enrutado a través del túnel VPN hacia la red interna administrada por Nethserver.

Para verificar la funcionalidad del túnel y la correcta implementación de la VPN, se realizaron pruebas de conectividad desde el PC cliente hacia la red interna, confirmando que el túnel VPN funcionaba correctamente. Las pruebas demostraron que el tráfico enviado desde el cliente remoto era cifrado y transmitido de forma segura a través de Internet, y llegaba a su destino dentro de la red interna sin ningún tipo de interrupciones o vulnerabilidades, garantizando la privacidad e integridad de los datos transferidos. Esto validó la efectividad del proceso de implementación de la VPN, proporcionando acceso seguro a los recursos internos desde cualquier ubicación remota

Figura 54. VPN conectada al servidor Nethserver

Fuente: Autoría Propia

6.5.5 PRUEBAS DE CONEXIÓN

Como parte del proceso de validación de la implementación de la VPN, se realizaron diversas pruebas para verificar tanto la conectividad como la seguridad del túnel VPN establecido entre el cliente remoto y la red interna gestionada por Nethserver.

Se ejecutaron comandos ping desde el cliente remoto hacia los dispositivos internos en la red administrada por Nethserver. Las capturas de pantalla de estos comandos mostraron que las solicitudes ICMP fueron correctamente respondidas, lo que confirmó que el tráfico de la VPN estaba siendo correctamente enrutado a través del túnel. Además, se realizaron pruebas de interacción con servicios internos, como el acceso a servidores de archivos y aplicaciones, lo que corroboró que la conexión VPN permitía un acceso completo a los recursos internos de la red, proporcionando a los usuarios remotos la funcionalidad de red como si estuvieran en la sede de la organización.

Para asegurar que el tráfico transmitido a través de la VPN estuviera adecuadamente protegido, se monitoreó el tráfico desde la interfaz de administración de Nethserver. Este monitoreo permitió verificar que las comunicaciones estaban cifradas, lo que aseguraba la confidencialidad e integridad de los datos enviados a través del túnel. El proceso de cifrado utilizado por OpenVPN, basado en protocolos robustos como AES, garantizó que cualquier intento de interceptar los datos fuera inútil, dado que los paquetes eran ilegibles sin la clave de cifrado adecuada. Este monitoreo proporcionó una capa adicional de confianza en la seguridad de la conexión y demostró la eficacia del túnel VPN como un medio seguro para el acceso remoto.

Figura 55. Conexión VPN al servidor Nethserver

Fuente: Autoría Propia

Figura 56. Ping a equipo de pruebas permitido y denegado, VPN encendida y VPN apagada

Fuente: Autoría Propia

7 CONCLUSIONES.

Durante la realización de esta actividad, se observa un proceso sencillo para la instalación y configuración de un servidor utilizando NethServer. La variedad de servicios que ofrece nos brinda una herramienta poderosa y fácil de configurar, considerando las reglas de redireccionamiento establecidas en sus respectivas redes. Un servidor Proxy es esencial para las organizaciones que buscan asegurar la fiabilidad y eficiencia de sus operaciones, ya que permite gestionar de manera efectiva el tráfico de cada dispositivo en la red. Esto posibilita bloquear accesos a sitios maliciosos o innecesarios, según las necesidades específicas de la empresa.

NethServer se presenta como una de las distribuciones más adecuadas para implementar infraestructuras IT, ya que permite configurar todos los servicios necesarios para fortalecer la seguridad del tráfico en la red, incluyendo el cortafuegos, entre otros. Durante esta última fase, se abordaron de manera práctica diversas situaciones que surgen al instalar y configurar tecnologías como estas, especialmente en lo que respecta a la

implementación del cortafuegos. Esto incluyó desde la instalación del servidor hasta el acceso web a Cockpit para administrar el servidor, instalando componentes adicionales y definiendo reglas y categorías para restringir el acceso o el tráfico hacia sitios considerados de alto riesgo o inapropiados para el acceso desde las estaciones de trabajo.

En general, este proceso académico ha sido muy valioso, ya que ha permitido aplicar todos los conocimientos adquiridos a lo largo del semestre. Desde la administración de NethServer, es posible integrar fácilmente una VPN, lo que facilita la configuración y gestión de redes privadas virtuales. Esto permite conectar equipos de una red externa con dispositivos en una red interna a través del servidor OpenVPN en modo roadwarrior, conectando así a un cliente remoto con la red. Si necesitas más ajustes o información adicional, no dudes en decírmelo.

8 REFERENCIAS

[1] Nethserver (s.f). Manual del Administrador [En línea]. Disponible en: https://docs.nethserver.org/es/v7/index.html

[2] Nethesis (2020). Nethserver Documentation Version 6.10 Final [En línea]. Disponible en: https://docs.nethserver.org/_/downloads/es/v6/pdf

[3] NethServer, W. t. (s.f.). wiki.nethserver [En línea]. Disponible en: https://wiki.nethserver.org/doku.php?id=start

[4] Villada, R. J. L. (2015). Instalación y configuracióndel software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial [En línea]. Disponible en: https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92

[5] Nethserver.org (s.f). Web proxy [En línea]. Disponibleen: https://docs.nethserver.org/en/v7/web_proxy.html.