IMPLEMENTAR CON NETHSERVER SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA TI

Wilinton Ortega Castilla
e-mail: wortegac@unadvirtual.edu.co
Wilder Danilo Bayona Verjel
e-mail: wdbayonav@unadvirtual.edu.co
Jennifer Paola Arciniegas Arciniegas
e-mail: jparciniegasa@unadvirtual.edu.co
Nelson Arley Esteban Hernandez
e-mail: naestebanh@unadvirtual.edu.co
Julio Andrey Torres Acosta
e-mail: jatorresac@unadvirtual.edu.co

RESUMEN: *En el presente artículo se presentará la creación e implementación de diferentes servicios de gestión de infraestructura a través de la distribución basada en GNU/Linux, con NethServer se logró la creación de los siguientes servicios de gestión de infraestructura TI: Servidor DHCP, Servidor DNS y un Controlador de Dominio, La creación de un Proxy para filtrar la conectividad a internet a través del puerto 3128, permitiendo a través de la creación de un Cortafuegos o Firewall la implementación de restricciones a diferentes contenidos, Se logró a través del controlador de dominio crear y tener acceso a servicios de carpetas e impresoras compartidas, finalmente se pudo establecer un servicio de VPN logrando la comunicación privada.*

PALABRAS CLAVE: Distribución GNU/Linux, Infraestructura TI, NethServer, Servicios de Gestión de redes.

1 INTRODUCCIÓN

Teniendo como base una infraestructura de red que cuente con diferentes entornos como una Red LAN, WAN y DMZ, A continuación, se agregaran diferentes servicios de gestión de red que permitan la comunicación, creación de reglas, filtrado de contenido y una red privada, con NethServer se logra la creación y administración de estos servicios de gestión de infraestructura TI.

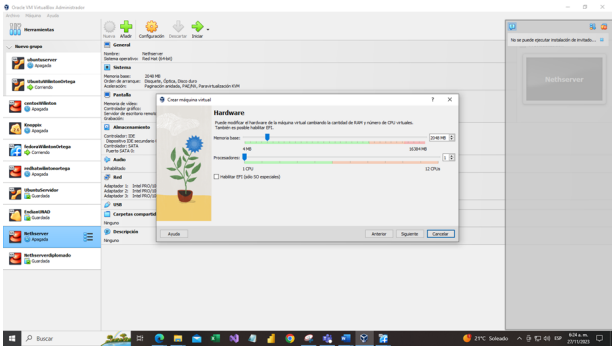
2 INSTALACIÓN Y CONFIGURACIÓN DE NETHSERVER

2.1 INSTALACIÓN DE NETHSERVER

En el proceso de instalación se asignaron los siguientes recursos necesarios para el correcto funcionamiento del NethServer a través del VirtualBox:
Memoria RAM: 2 GB.
Procesador: 1 Núcleo.
Almacenamiento: 20 GB
Imagen ISO: 1 GB

Enlace de descarga imagen ISO de NethServer: https://www.nethserver.org/getting-started-with-nethserver/, El suministro y ampliación de esta informacion fue a traves de los pasos de instalación y configuración del NethServer como lo indica el manual del administrador, ver [1].

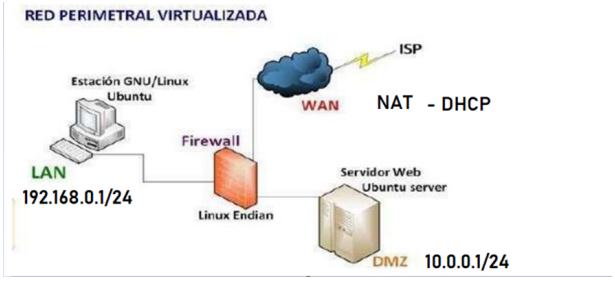
Figura 1. Creación de máquina virtual NethServer a través de VirtualBox.



Fuente: Autoría Propia

Teniendo como base la configuración de zonas de la infraestructura TI establecida en pasos anteriores

Figura 2. Configuración de infraestructura TI

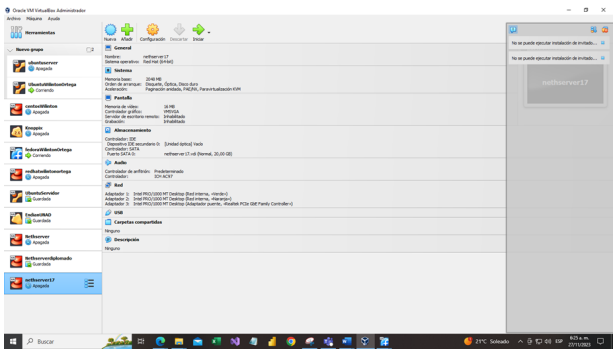


Fuente: Autoría propia.

Una vez instalado el NethServer en VirtualBox, se habilitan tres (3) adaptadores de red, para la red LAN se describe como “verde” y se habilita como una red interna, para la red WAN se habilita como un adaptador puente, para la red

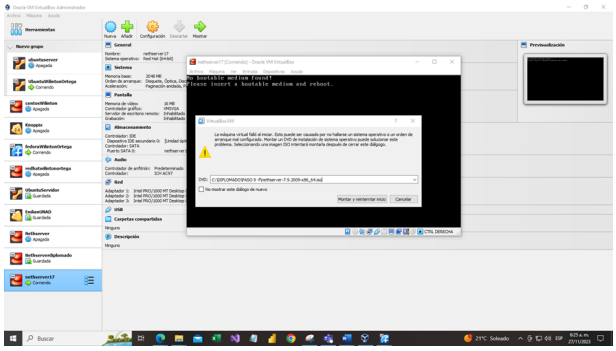
DMZ se describe como “naranja” y se habilita como otra red interna, dando como resultado los siguientes adaptadores habilitados LAN(verde - interna), DMZ (naranja - interna), y WAN (puente).

Figura 3. Adaptadores habilitados en Maquina Virtual NethServer



Fuente: Autoría propia.

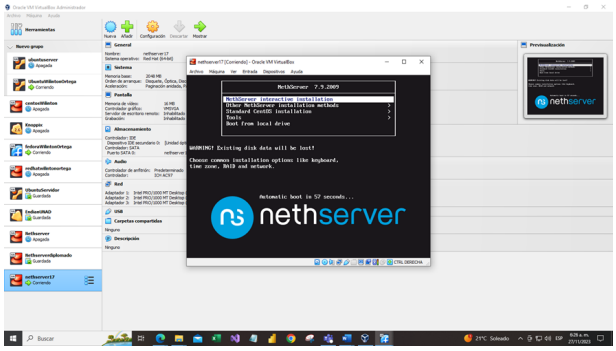
Figura 4. Proceso de instalación y configuración de ISO NethServer.



Fuente: Autoría propia.

Se escoge la opción “NethServer interactive installation” para comenzar el proceso de instalación del servidor NethServer de manera interactiva.

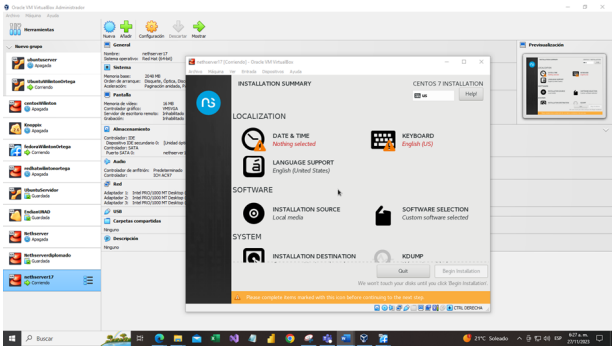
Figura 5. Opciones de instalación de NethServer.



Fuente: Autoría propia.

Se valida resumen de instalación donde requiere insertar zona horaria y configuración de teclado para el servidor e iniciar proceso de instalación.

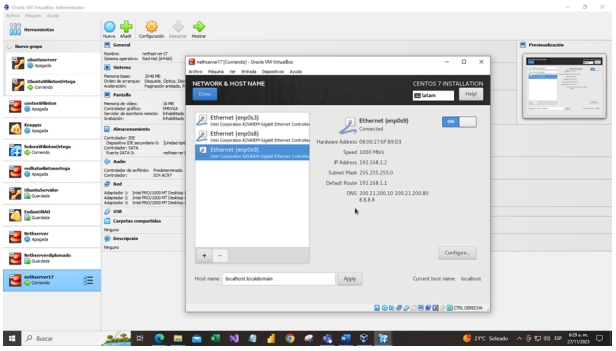
Figura 6. Resumen de Instalación de NethServer



Fuente: Autoría propia.

Se validan en Network & Hostname los adaptadores instalados en especial el de la red WAN, Se ingresa a configure para establecer parámetros manuales.

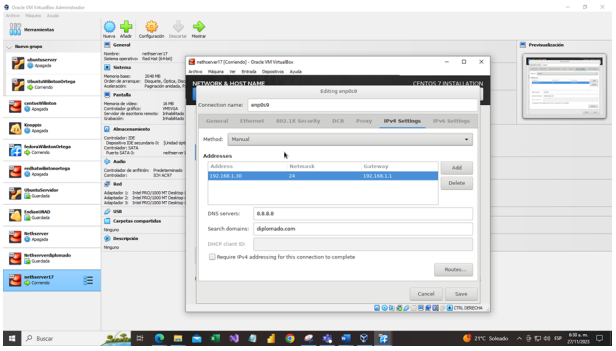
Figura 7. Configuración de Network & Hostname



Fuente: Autoría propia.

Se habilita en la opción de general el cuadro automatically connect to this network when it is available y En la configuración de las opciones de IPV4, se establece el method manual, ademas se establece la IP 192.168.1.30/24 con puerta de enlace 192.168.1.1, finalmente se agrega el dominio diplomado.com

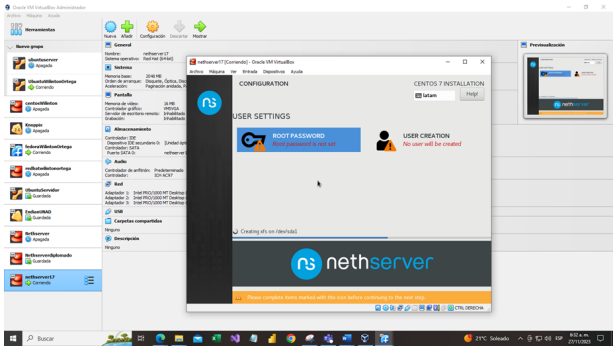
Figura 8. configuración de adaptador enp0s9



Fuente: Autoría propia.

Se asigna una contraseña para el usuario root en la opción de ROOT PASSWORD y se tiene la opción de crear un usuario con privilegios en USER CREATION.

Figura 9. Configuración de Usuario NethServer.

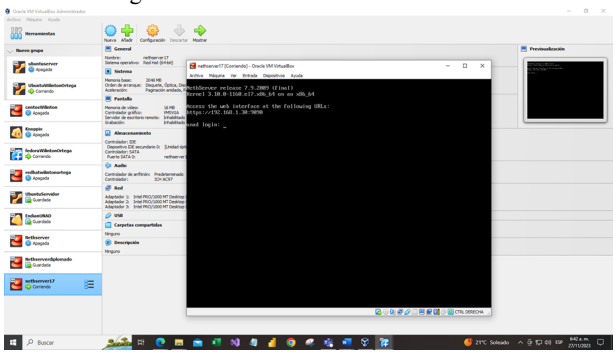


Fuente: Autoría propia.

2.2 CONFIGURACIÓN

Una vez finaliza la instalación del servidor de NethServer en la ventana de inicio o de cargue se indica la IP y puerto (192.168.1.30:9090) para ingresar a la interfaz web de NethServer, se ingresa al servidor con el usuario root y su respectiva contraseña y como se sugiere [2] se realizan pruebas con el adaptador puente para validar el acceso a internet en este caso el adaptador enp0s9 con el comando ping a www.google.com y se valida el nombre del servidor con el comando hostname.

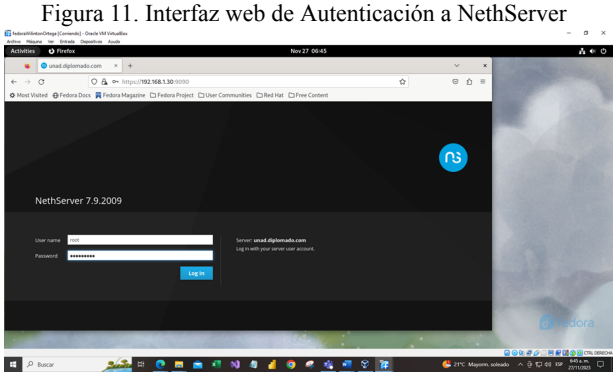
Figura 10. Interfaz de inicio NethServer.



Fuente: Autoría propia.

Se usa una máquina con un adaptador puente que tenga la misma red de NethServer (adaptador puente) y desde el navegador de la máquina de pruebas se ingresa la IP y puerto del NethServer.

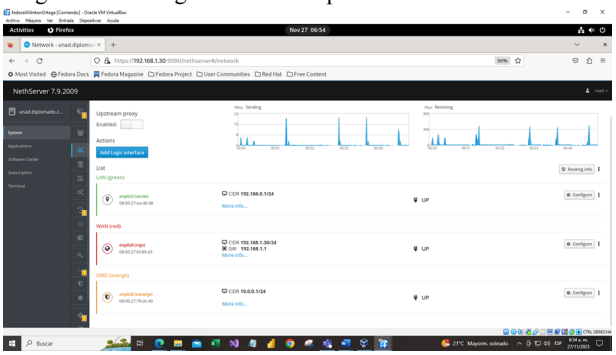
Figura 11. Interfaz web de Autenticación a NethServer



Fuente: Autoría propia.

Se valida en la opción Network los adaptadores y se asigna la IP según el modelo de infraestructura TI, dando como resultado en este caso para la red LAN (verde) 192.168.0.1, la red DMZ (naranja) 10.0.0.1 y la red WAN 192.168.1.30.

Figura 12. Configuración de adaptadores de red habilitados.



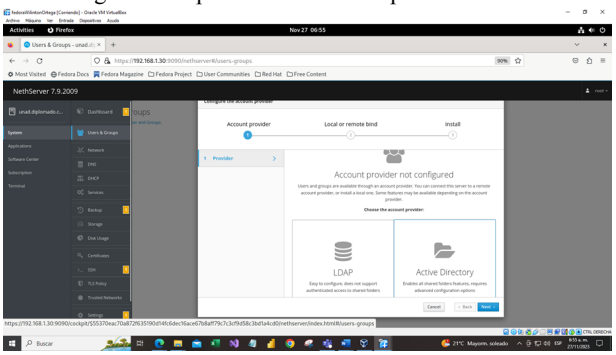
Fuente: Autoría propia.

3 TEMÁTICA 1: SERVIDOR DHCP, DNS Y CONTROLADOR DE DOMINIO.

3.1 CONTROLADOR DE DOMINIO

Se ingresa a la opción de Users & Groups en el dashboard del NethServer, para instalar y configurar el controlador de dominio, se cargará una ventana en la cual se escoge la opción Active Directory.

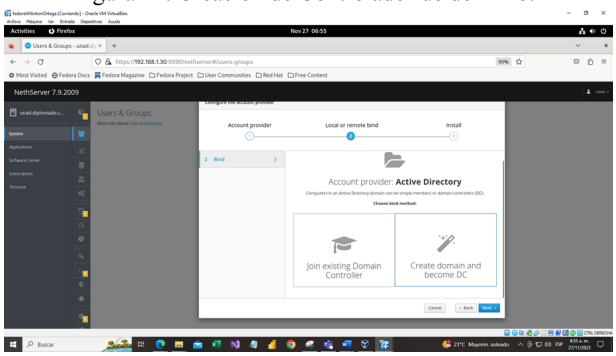
Figura 13. Opción Users & Groups NethServer.



Fuente: Autoría propia.

Luego de seleccionar el botón de Next para continuar el proceso de creación del controlador de dominio, se debe seleccionar la opción créate domain and become DC, y nuevamente seleccionar el botón Next que cargara un cuadro donde se deberá ingresar los parámetros para identificar el controlador de dominio, como lo es nombre del dominio y una IP dentro del rango de la red LAN (verde).

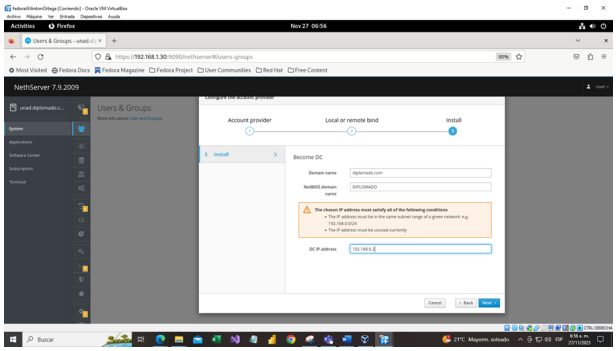
Figura 14. Creación de Controlador de dominio.



Fuente: Autoría propia.

Se establece nombre de dominio diplomado.com, y dirección IP dentro del rango de la red LAN(verde) 192.168.0.2

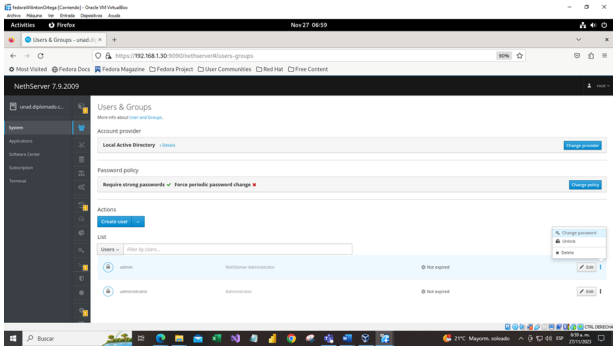
Figura 15. Asignación de parámetros en Controlador de Dominio.



Fuente: Autoría propia.

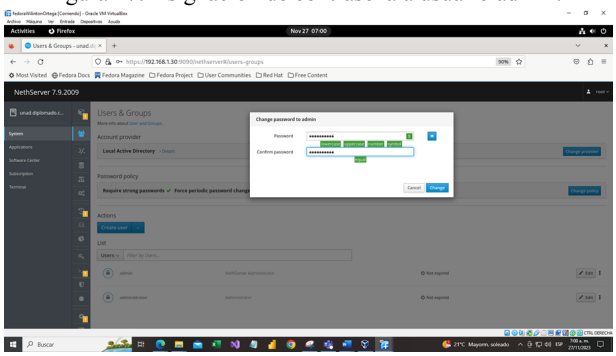
Se valida la creación del controlador de dominio y usuarios creados por defecto, se selecciona la opción Change Password del usuario admin, para establecer una contraseña en el usuario admin, según los parámetros requeridos, los cuales indican que la contraseña debe llevar mayusculas, minusculas, numeros y simbolos.

Figura 16. Usuarios por defecto de Controlador de Dominio.



Fuente: Autoría propia.

Figura 17. Asignación de contraseña a usuario admin.



Fuente: Autoría propia.

3.2 SERVIDOR DNS

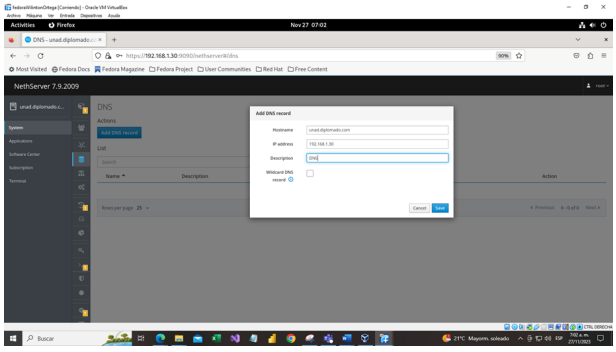
Se ingresa a la opción DNS del NethServer y se selecciona el botón Add DNS record, para crear los parámetros del servidor DNS .

Figura 18. Opción DNS de NethServer.

Fuente: Autoría propia.

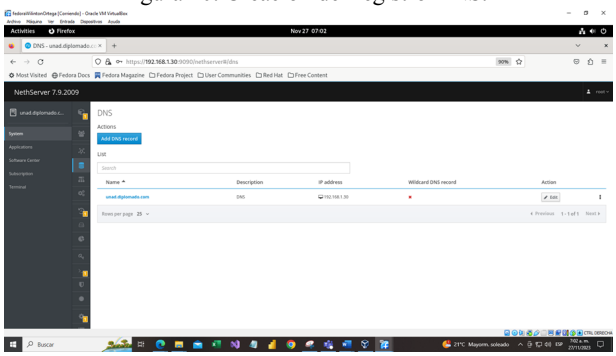
Se establece un hostname (unad.diplomado.com), una dirección IP (NethServer 192.168.1.30) y una descripción (DNS) para el servidor DNS.

Figura 19. Cuadro de Asignación de Registro DNS.



Fuente: Autoría propia.

Figura 20. Creación de Registro DNS.

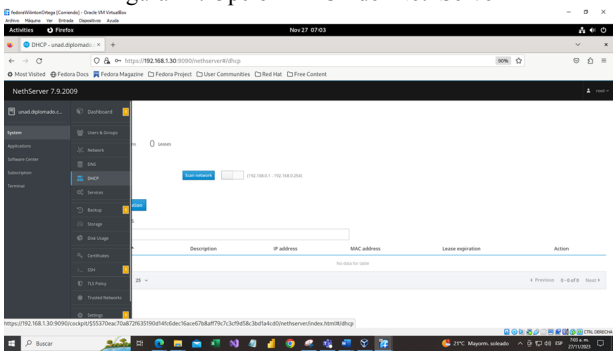


Fuente: Autoría propia.

3.3 SERVIDOR DHCP

Se ingresa a la opción DHCP del NethServer para crear servidor DHCP.

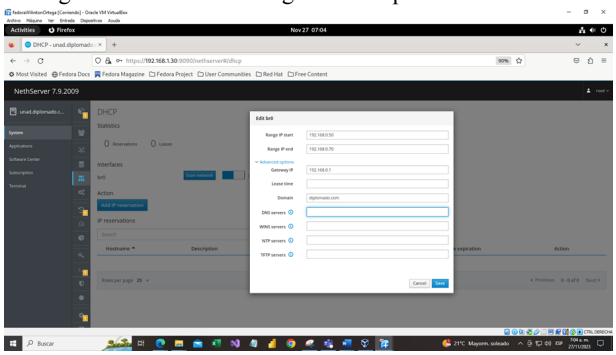
Figura 21. Opción DHCP del NethServer



Fuente: Autoría propia.

Se establece un rango de IP de red LAN (192.1680.50 - 192.168.0.70), puerta de enlace (192.168.0.1) y dominio (diplomado.com) en el servidor DHCP

Figura 22. Cuadro de Asignación de parámetros DHCP

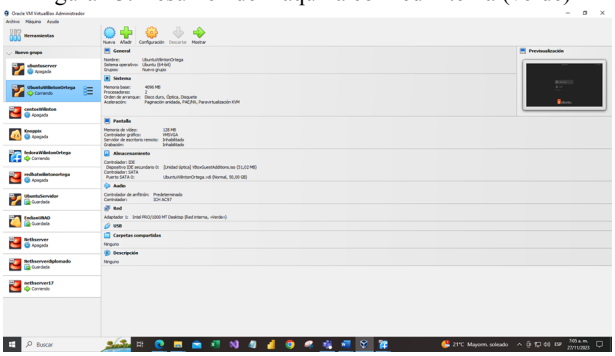


Fuente: Autoría propia.

3.4 PRUEBAS

Se ingresa a una máquina desktop con red LAN (verde)

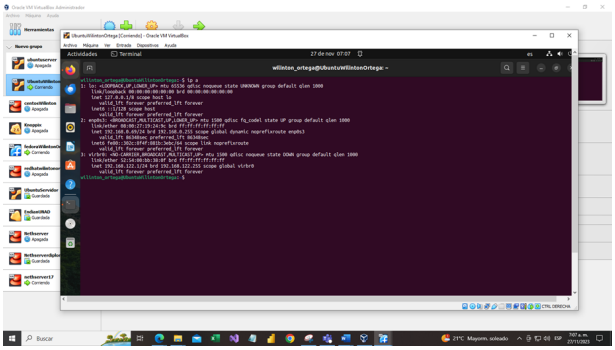
Figura 23. Resumen de máquina con red interna (verde)



Fuente: Autoría propia.

Se valida que maquina con adaptador de red LAN, toma direccionamiento dentro de rango DHCP (192.168.0.69/24).

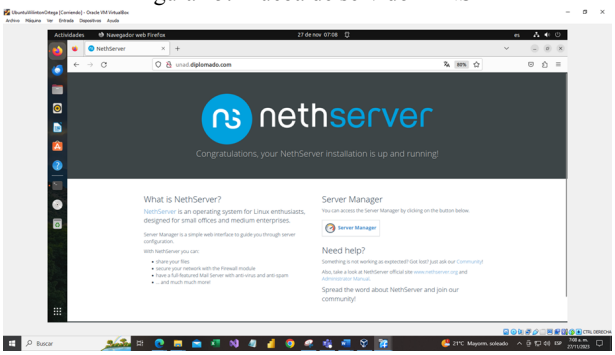
Figura 24. Prueba de Servidor DHCP.



Fuente: Autoría propia.

Se valida servidor DNS en máquina de red LAN, ingresando al navegador el nombre de dominio, en este caso se carga dirección establecida en el registro DNS (NethServer)

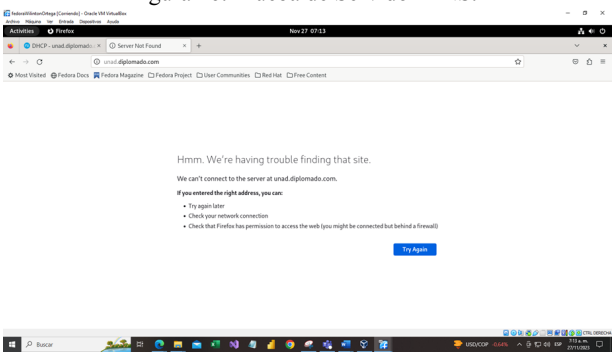
Figura 25. Prueba de servidor DNS



Fuente: Autoría propia.

Se realiza la misma prueba de validar el DNS desde el navegador de una máquina por fuera de la red LAN, y no se obtiene respuesta.

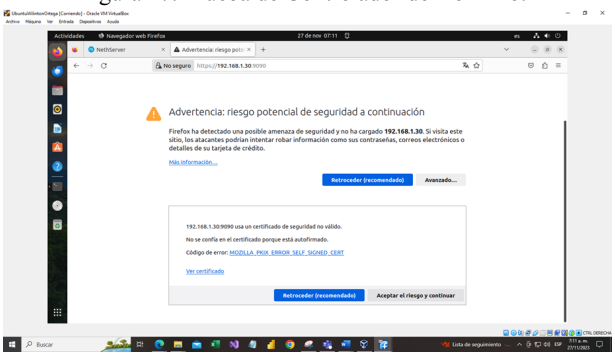
Figura 26. Prueba de Servidor DNS.



Fuente: Autoría propia.

Se accede desde una máquina con red LAN y se desde el navegador la IP y Puerto del servidor de NethServer en este caso (192.168.1.30:9090), se genera un cuadro donde se debe aceptar el riesgo debido a los certificados del portal y continuar,

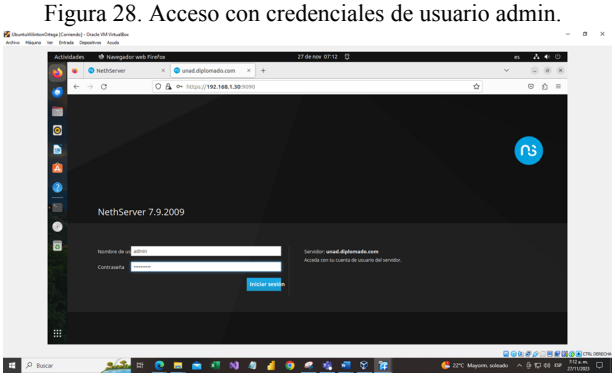
Figura 27. Prueba de Controlador de Dominio.



Fuente: Autoría propia.

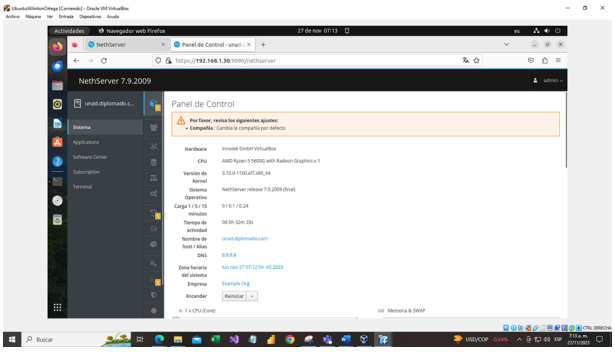
Se accede con credenciales de autenticación asignadas para el usuario admin en la instalación del controlador de dominio, y poder validar el ingreso al dashboard del NethServer.

Figura 28. Acceso con credenciales de usuario admin.



Fuente: Autoría propia.

Figura 29. Dashboard de NethServer autenticado con cuenta admin.

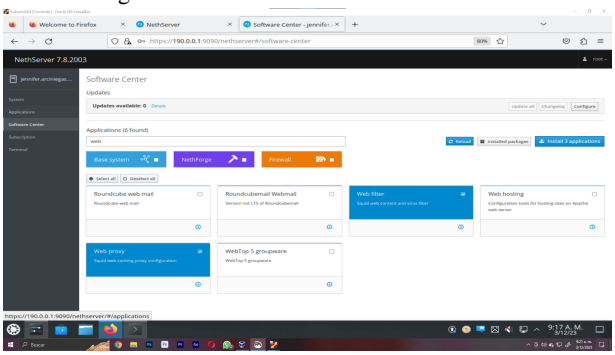


Fuente: Autoría propia.

4 TEMÁTICA 2: PROXY

Una vez realizada la instalación de NethServer y la configuración de las tarjetas de red, se realiza la instalación de las aplicaciones web proxy y web filter, que se encuentran en el entorno de software center.

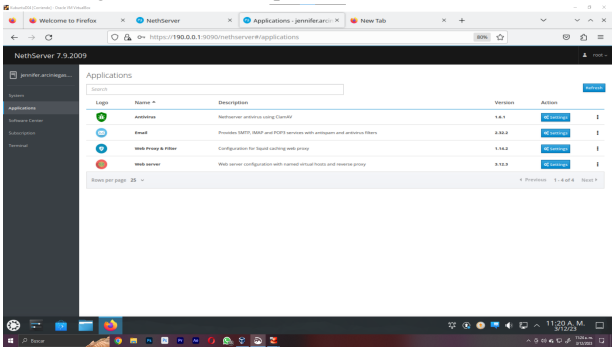
Figura 30. Software Center de NethServer.



Fuente: Autoría propia.

Se ingresa al entorno aplicaciones en NethServer para ver las aplicaciones instaladas.

Figura 31. Entorno aplicaciones de NethServer.



Fuente: Autoría propia.

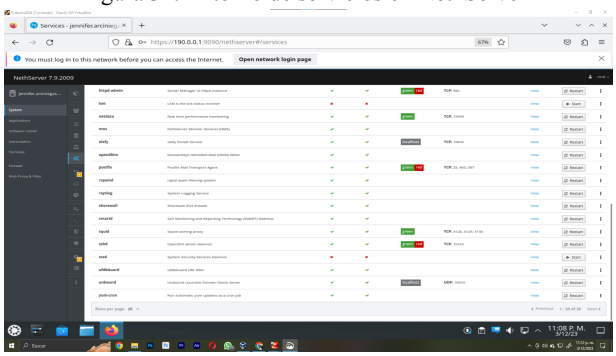
Instaladas las aplicaciones en el entorno de servicios, se podrán observar servicios como el squid proxy, el cual funciona funciona con tres puertos, 3128 usado para el proxy no transparente, filtrando peticiones HTTP, el puerto 3129 se

utiliza para el proxy transparente filtrando peticiones HTTPS y el puerto 3130 para el proxy transparente en conjunto con un certificado SSL [3].

Otro servicio que es importante tener activo es el ufdbGuard, se utiliza para filtrar usando la URL mediante base de datos.

Se ingresa al entorno de servicios en NethServer para ver el estado de los nuevos servicios

Figura 32. Entorno de servicios en NethServer

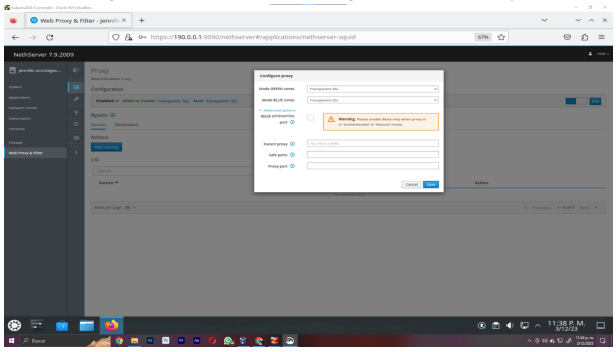


Fuente: Autoría propia.

En un principio los servicios no están activados por lo que es necesario realizar su respectiva configuración, a través de la aplicación Web Proxy & Filter se activan los servicios requeridos, Se asigna a la zona verde el modo transparente con opciones SSL.

pues se optó por utilizar el proxy en modo SSL transparente, en [4] se explica que todos los clientes se ven obligados a utilizar el proxy en conexiones HTTP y HTTPS.

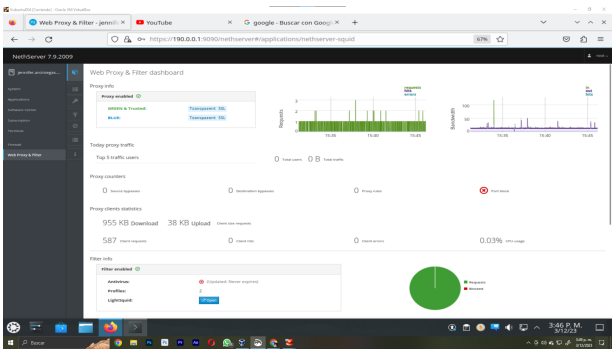
Figura 33. Cuadro de configuración de Proxy



Fuente: Autoría propia.

En el entorno proxy de Web Proxy & Filter se observa información y representaciones gráficas del proxy principalmente información sobre el estado sobre el filtro.

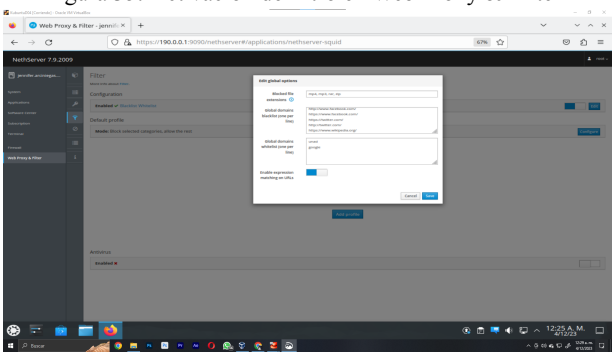
Figura 34. Entorno principal de Web Proxy & Filter



Fuente: Autoría propia.

Ahora en el entorno de categorías para los filtros de contenido web se agrega la categoría université Toulouse (free), para ver las categorías deben habilitarse los filtros, en la que se pueden asignar las URL de las páginas que se quieren en lista negra.

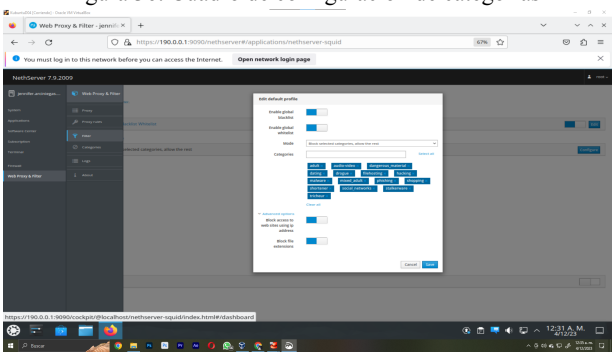
Figura 35. Activación de filtro en Web Proxy & Filter



Fuente: Autoría propia.

Se ingresa a definir las categorías con la configuración, de bloquear las categorías seleccionadas y permitir el resto, dónde está habilitada la lista negra y blanca global.

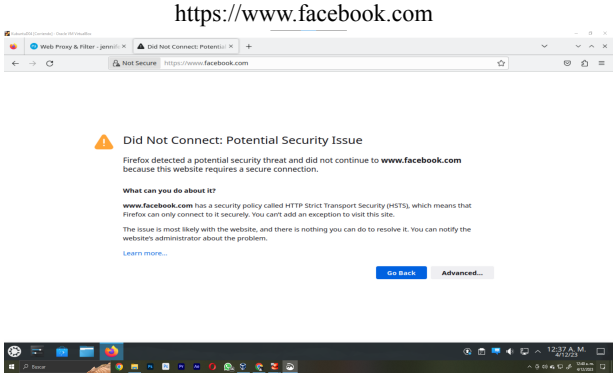
Figura 36. Cuadro de configuración de categorías



Fuente: Autoría propia.

Al final se realiza la prueba con una de las páginas asignadas a lista negra, está bloqueada como se puede observar en la Figura 37, sin embargo, se puede navegar y acceder a las páginas que no estén en lista negra o que no estén dentro de las categorías seleccionadas.

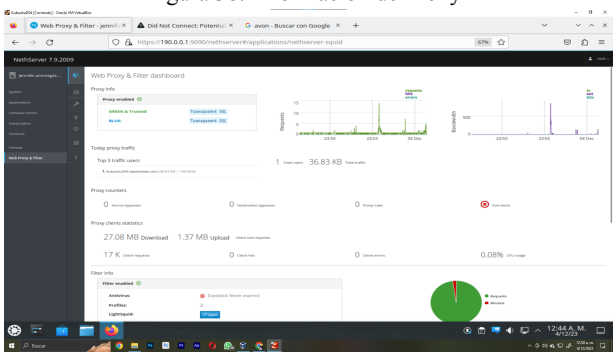
Figura 37. Prueba de acceso a portal web https://www.facebook.com



Fuente: Autoría propia.

En el entorno proxy de Web Proxy & Filter se observa en los 5 principales tráficos de usuario, un cliente que es el computador que se está usando, se puede observar en la interfaz las estadísticas del ancho de banda y la CPU

Figura 38. Información de Proxy



Fuente: Autoría propia.

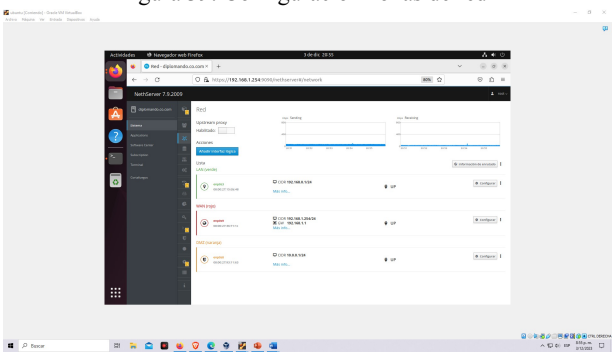
5 TEMÁTICA 3: CORTAFUEGOS

Es crucial comprender que la configuración adecuada de la red proporciona el marco necesario para el correcto funcionamiento y desempeño del firewall. En este contexto, la red se estructura cuidadosamente, para asegurar la separación eficiente de funciones y garantizar una gestión efectiva del tráfico de datos.

Dentro de la sección de red, se lleva a cabo la configuración de las redes asignando roles específicos a cada una. Esta práctica se basa en principios teóricos de diseño de redes, donde la segmentación de las redes, como LAN (Local Area Network), DMZ (Zona Desmilitarizada) y WAN (Wide Area Network), contribuye a fortalecer la seguridad y la administración del sistema.

Finalmente se muestran cómo se configuraron las tres redes:

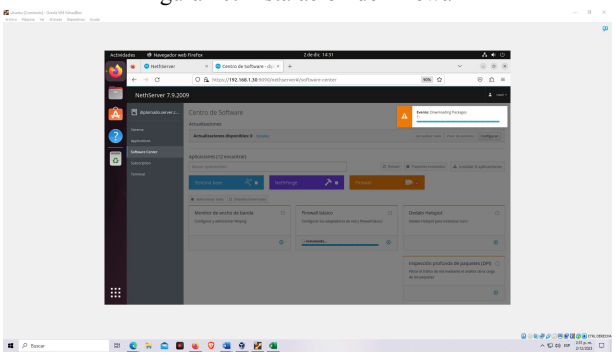
Figura 39. Configuración zonas de red



Fuente: Autoría propia

Ahora se inicia la descarga e instalación del firewall en NethServer. En esta etapa, se accede al apartado de "Software Center" para llevar a cabo la instalación del firewall básico.

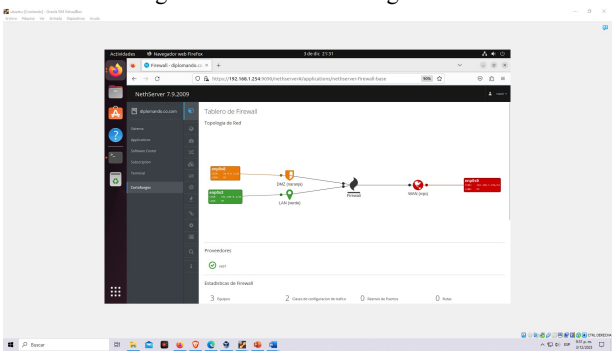
Figura 40. Instalación del firewall



Fuente: Autoría propia

Luego de instalado el firewall, se accede a este apartado y se observa la tipología de red que se creó en los pasos anteriores.

Figura 41. Firewall Configuración

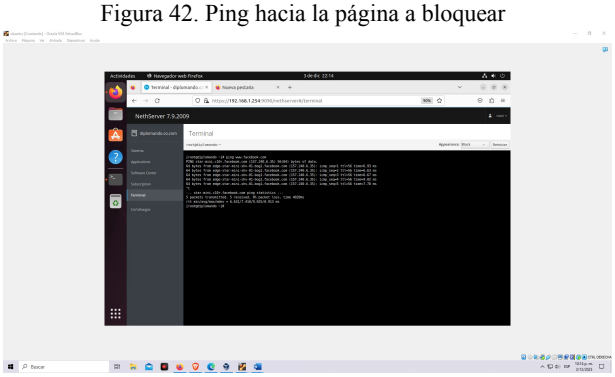


Fuente: Autoría propia

Ahora se inicia el proceso de establecimiento de reglas en el firewall para restringir el acceso a determinadas páginas de entretenimiento y redes sociales. En este sentido, se dirige a la sección de "Reglas" y se comienza a definir cada una de ellas de manera específica. Un paso crucial en este proceso implica conocer la dirección IP de las páginas que se desean bloquear. Para lograr esto, se utiliza el comando ping en la terminal hacia la página deseada. Al realizar este

procedimiento, se obtiene la dirección IP de la página correspondiente, la cual se usará para la creación de las reglas en el firewall.

Figura 42. Ping hacia la página a bloquear



Fuente: Autoría propia

Una vez obtenida la dirección de la página, se inicia la creación de la regla para bloquear el acceso a la misma. Durante la configuración de la regla, se solicitan diversos parámetros, entre ellos:

Origen: Representa la dirección del PC al cual se desea bloquear el acceso.

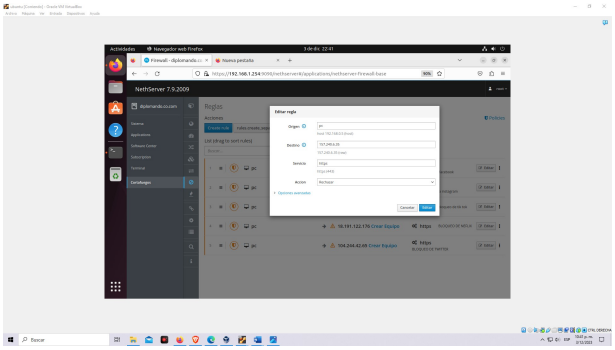
Destino: Corresponde a la dirección IP de la página que se busca bloquear.

Servicio: En este caso, se especifica el protocolo, siendo HTTPS.

Acción: La acción configurada es "rechazar", con el propósito de bloquear el acceso a la página.

Este proceso permite una definición precisa de los parámetros necesarios para establecer restricciones de acceso específicas a través del firewall. Al configurar cada elemento de la regla de manera detallada, se asegura un bloqueo efectivo del acceso a la página deseada desde el origen especificado. Para finalizar la creación de la regla se guarda la regla y se aceptan los cambios.

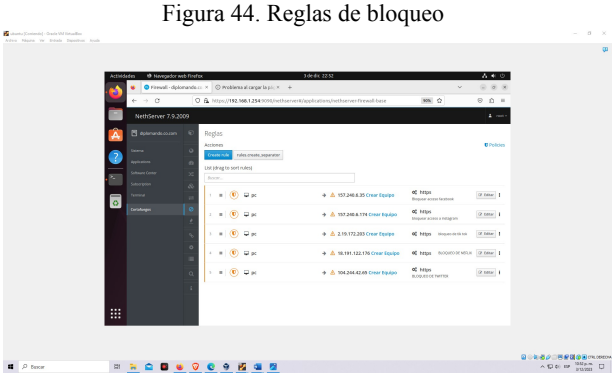
Figura 43. Configuración de la regla en el firewall.



Fuente: Autoría propia

La creación de diversas reglas sigue un proceso similar al descrito anteriormente, permitiendo bloquear el acceso a diversas páginas de entretenimiento y redes sociales. A continuación, se presentan las reglas específicas para el bloqueo de estas páginas. Este enfoque proporciona una metodología coherente y consistente para establecer restricciones de acceso en el firewall, asegurando un control efectivo sobre el acceso a sitios web específicos.

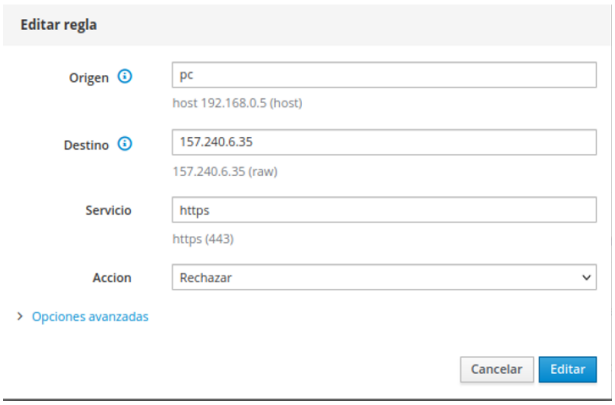
Figura 44. Reglas de bloqueo



Fuente: Autoría propia

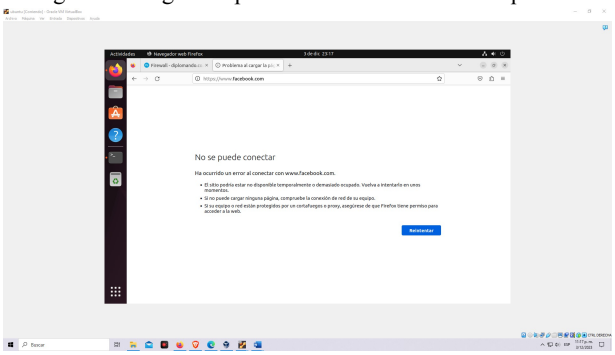
Ahora se prueban las reglas, para ver el funcionamiento de estas: Con la regla de rechazo configurada para Facebook, se evidencia que cualquier intento de acceder a la dirección https://www.facebook.com, resultará infructuoso.

Figura 45. Regla para el bloqueo de Facebook



Fuente: Autoría propia

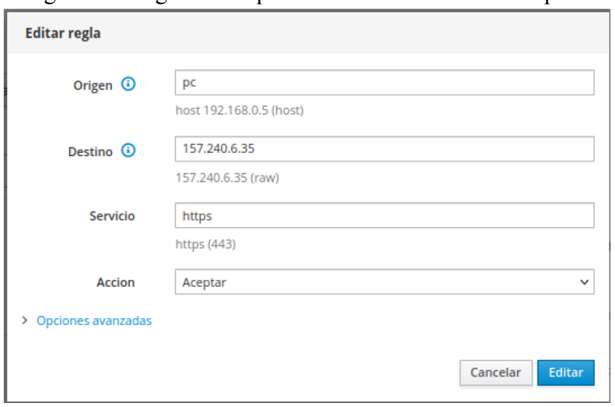
Figura 46. Pagina https://www.facebook.com bloqueada



Fuente: Autoría propia

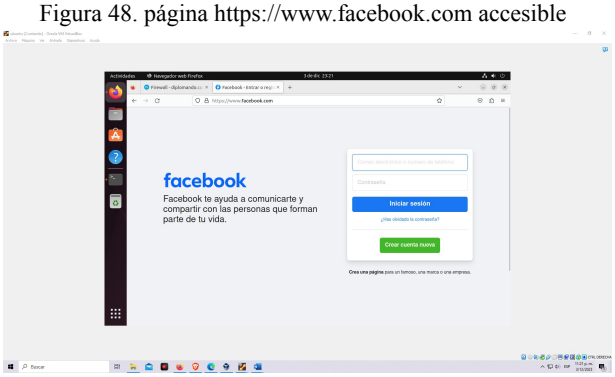
Con la regla en aceptar configurada para Facebook, se observa que al intentar acceder a la dirección https://www.facebook.com, se logrará el acceso sin inconvenientes.

Figura 47. Regla de bloqueo de Facebook Acción: aceptar



Fuente: Autoría propia

Figura 48. página https://www.facebook.com accesible



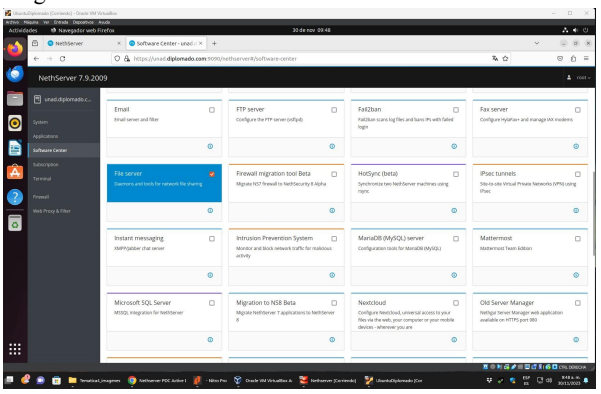
Fuente: Autoría propia

Como se evidenció previamente, la regla del firewall opera de manera adecuada, cumpliendo su función al permitir o denegar el acceso a una red social. De manera similar, este patrón se replica con las demás páginas y reglas que gestionan la autorización o restricción de acceso a dichos sitios web. Este comportamiento coherente valida la efectividad del conjunto de reglas en la administración del tráfico de la red.

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

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

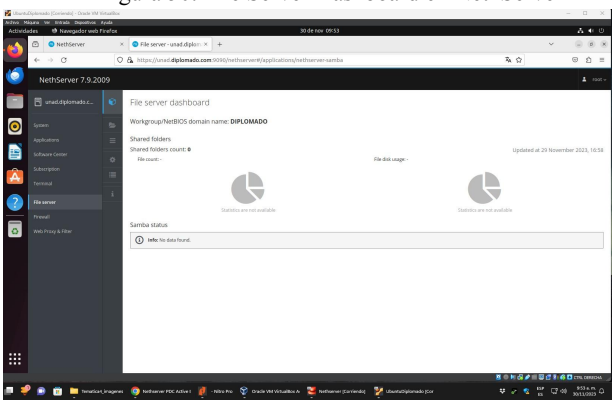
Figura 49. Software Center se instala el módulo File Server



Fuente: Autoría propia

El módulo File Server es el encargado de gestionar los archivos compartidos en el NethServer.

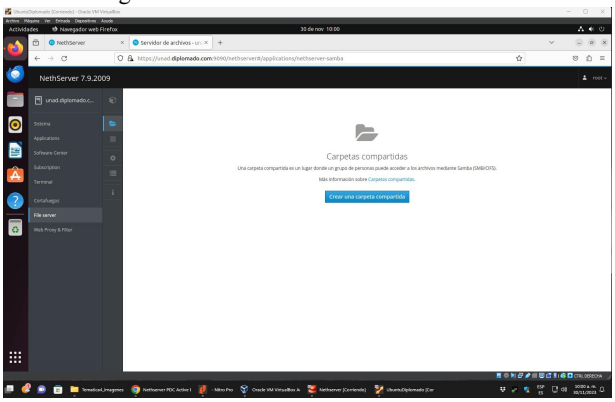
Figura 50. File Server Dashboard en NethServer



Fuente: Autoría propia

En el Dashboard de File Server, se evidencia el grupo de trabajo, en este ejemplo de nombre “DIPLOMADO”.

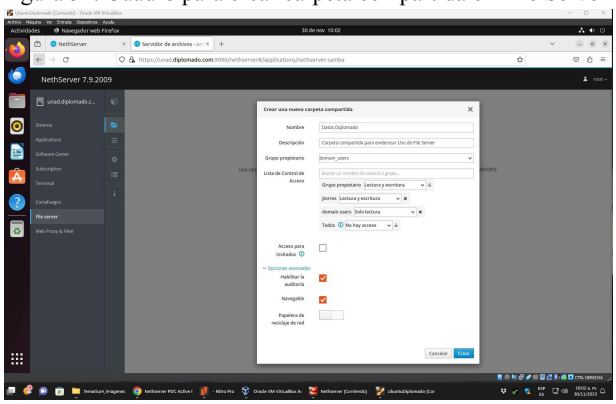
Figura 51. File Server Dashboard en NethServer



Fuente: Autoría propia

Las carpetas compartidas usan los servicios de Samba (SMB/CIFS).

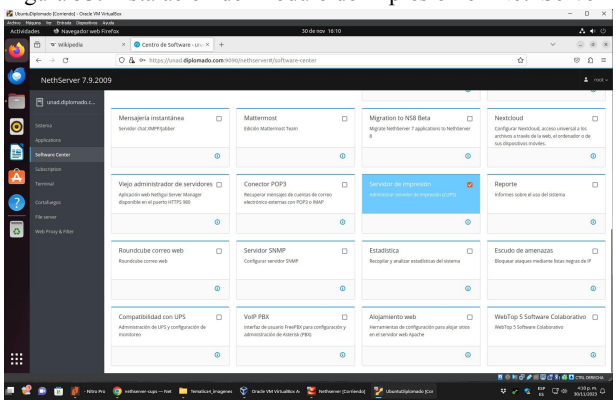
Figura 52. Cuadro para crear carpeta compartida en File Server



Fuente: Autoría propia

Para este ejemplo práctico, se crea una carpeta compartida de nombre “Datos Diplomado” y el dominio domain_users, se habilita la Auditoría.

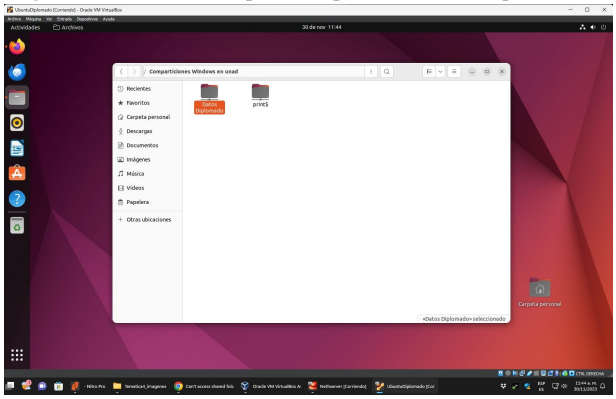
Figura 53. Instalación del módulo de impresión en NethServer



Fuente: Autoría propia

El servidor de impresión, es el módulo encargado de administrar el servicio de impresión de documentos en NethServer.

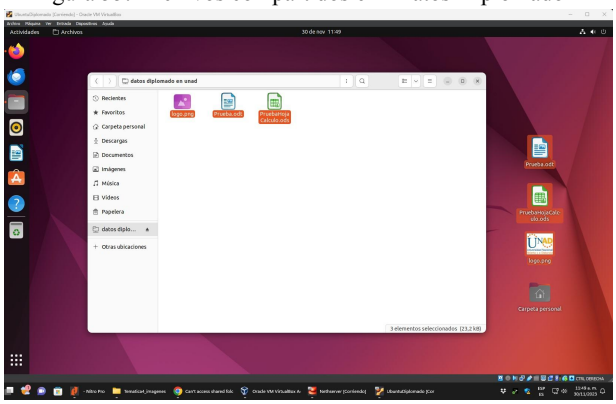
Figura 54. Evidencia carpeta compartida “Datos Diplomado”



Fuente: Autoría propia

La carpeta de “Datos Diplomado” se representa por medio de la red puesto que se accede a ella por medio del LDAP.

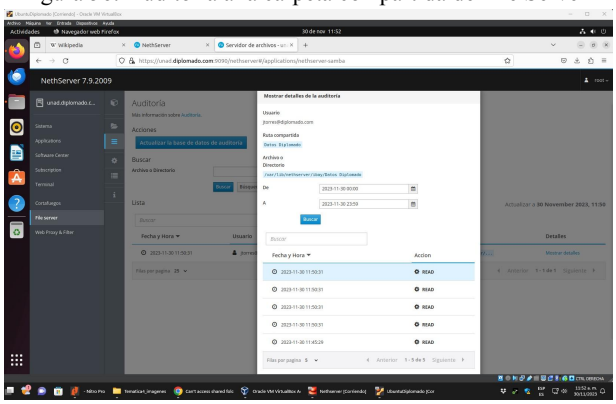
Figura 55. Archivos compartidos en “Datos Diplomado”



Fuente: Autoría propia

En esta prueba se puede evidenciar que la carpeta permite incluir archivos de varios formatos, en este ejemplo se usó imágenes, documento de texto y hoja de cálculo.

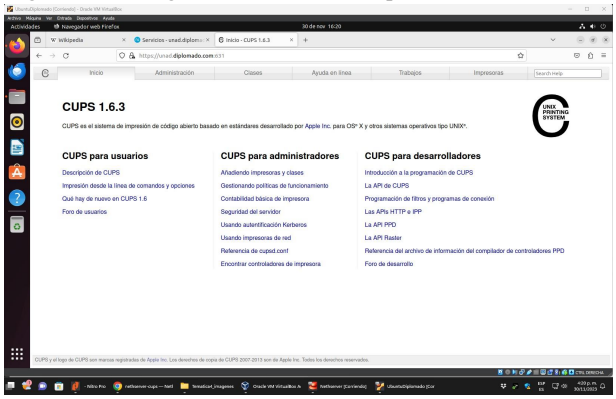
Figura 56. Auditoría a la carpeta compartida de File Server



Fuente: Autoría propia

En el registro se evidencia la fecha y hora del acceso y la ruta en la red usada por el usuario, también la acción realizada, puede ser READ o WRITE.

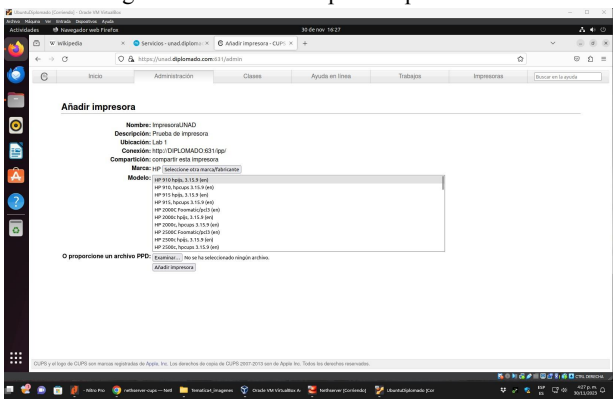
Figura 57. Configurando servicio de impresión en NethServer



Fuente: Autoría propia

En el módulo de configuración CUPS, están todas las opciones para configurar las impresoras para su uso en red.

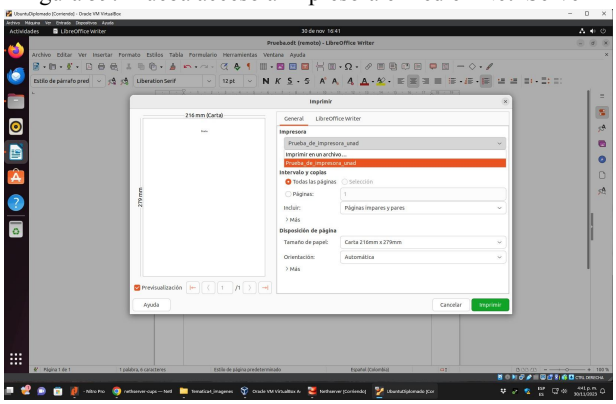
Figura 58. Añadir la impresora para NethServer



Fuente: Autoría propia

El menú de configuración de Print Server, incluye modelos y marcas de las impresoras en el mercado.

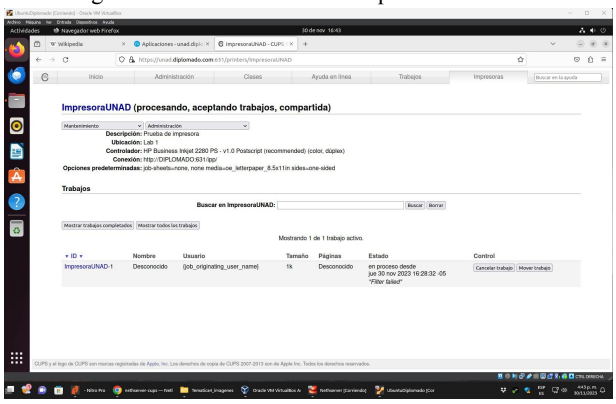
Figura 59. Prueba acceso a impresora en red en NethServer



Fuente: Autoría propia

En este ejemplo práctico, se marca la opción de imprimir un documento y se evidencia la impresora en red desde el usuario Desktop (Red Verde).

Figura 60. Evidencia cola de impresión en NethServer



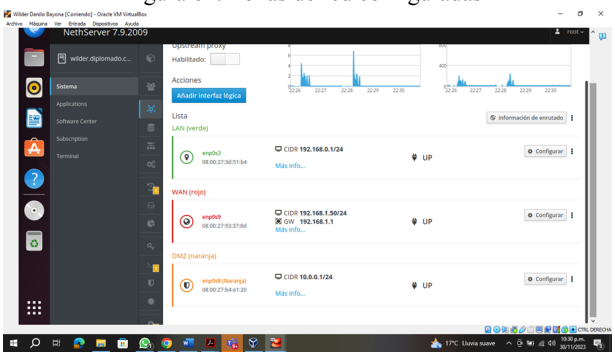
Fuente: Autoría propia

Al ingresar a la configuración de impresoras en NethServer se evidencia la impresión que se envía desde el usuario Desktop usando el servicio de Print Server.

7 TEMÁTICA 5: VPN

Se lleva a cabo la configuración que permitirá las conexiones VPN. Sin embargo, como paso previo a la instalación del servicio VPN, se procede a configurar las zonas de la red, con el objetivo de establecer una clara separación entre la red interna y otros segmentos de la red. Este paso es esencial para garantizar una estructura de red organizada y segura antes de implementar y habilitar el servicio de VPN.

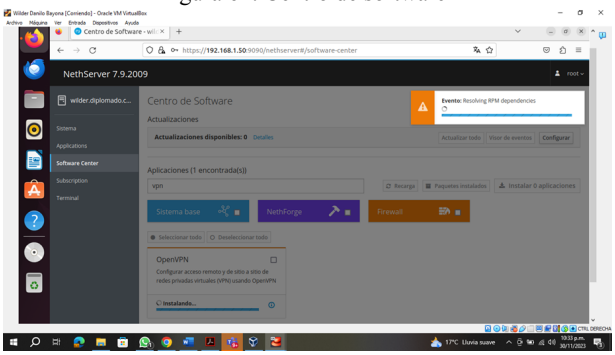
Figura 61. Zonas de red configuradas



Fuente: Autoría propia

Se ingresa al Centro de Software y se realiza una búsqueda para localizar la aplicación OpenVPN. Posteriormente, se lleva a cabo la instalación de OpenVPN a través de la interfaz del Centro de Software. Este proceso garantizará que la aplicación sea descargada e integrada en el sistema, permitiendo avanzar con la configuración y puesta en marcha del servicio VPN de manera eficiente.

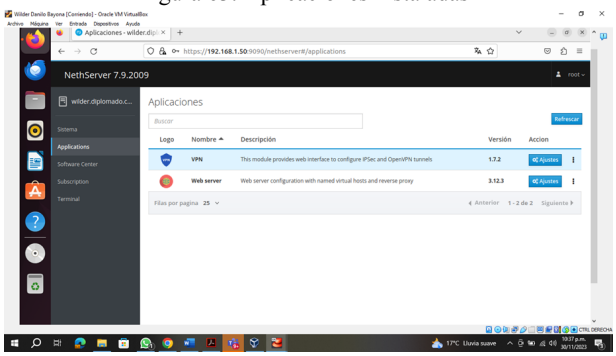
Figura 62. Centro de software



Fuente: Autoría propia

Se accede al menú de aplicaciones con el propósito de configurar la VPN. En esta sección, se explora y se ajusta las configuraciones específicas relacionadas con la Red Privada Virtual (VPN). Este paso permite personalizar y adecuar la VPN según las necesidades requeridas, estableciendo así un entorno seguro y funcional para las conexiones a través de la red.

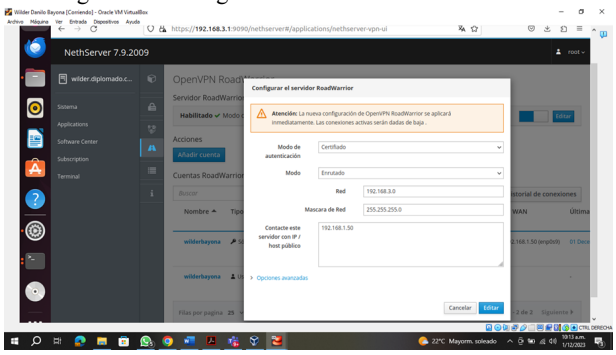
Figura 63. Aplicaciones instaladas



Fuente: Autoría propia

En la fase de configuración del servidor VPN, se hace necesario asignar una dirección IP que delinee el rango destinado a los dispositivos conectados a través de la VPN. Además, se establece el método de conexión mediante certificados, los cuales serán generados directamente por el servidor. En este contexto, se requiere proporcionar la dirección IP pública del servidor VPN como parte integral de este proceso. Este enfoque garantizará una asignación ordenada de direcciones IP a los dispositivos conectados, al mismo tiempo que establecerá un nivel de seguridad a través del uso de certificados generados internamente.

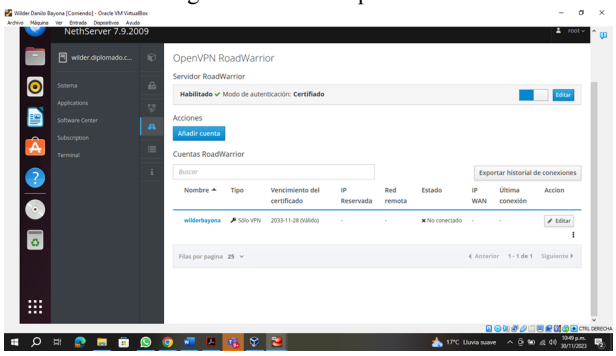
Figura 64. Configuración del servidor RoadWarrior



Fuente: Autoría propia

Se procede a la creación de una nueva cuenta de usuario para facilitar el acceso al sistema. Es importante destacar que se debe generar una cuenta individualizada para cada equipo cliente que se conectará al servidor VPN. En esta instancia, se ha creado una cuenta específica para el usuario denominado "wilderbayona". Este enfoque asegura un control preciso de la autenticación, permitiendo a cada usuario acceder de manera segura al servidor VPN con sus credenciales únicas.

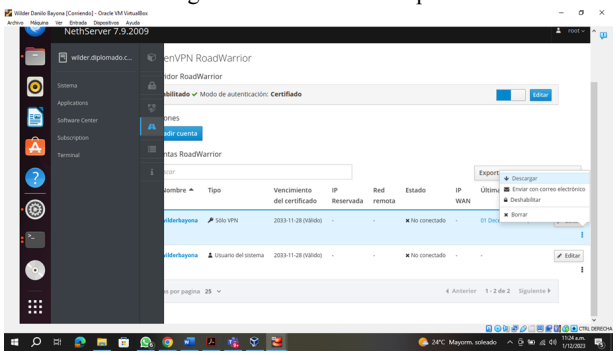
Figura 65. Cuenta openVPN



Fuente: Autoría propia

Después de completar la configuración del servidor y la creación de la cuenta para el usuario, el certificado se genera de manera automática. La única acción requerida en este punto es la descarga del certificado, que tiene la extensión .ovpn. Este archivo, esencial para establecer conexiones seguras a través de la VPN, puede ser obtenido mediante la descarga directa.

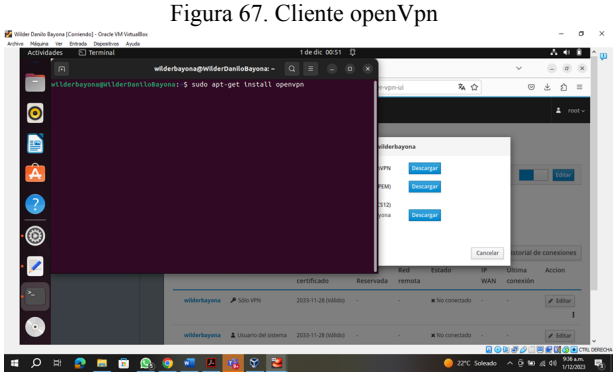
Figura 66. Certificado .ovpn



Fuente: Autoría propia

Para habilitar la conexión desde el cliente Ubuntu, se necesita instalar el cliente OpenVPN. En este caso, se descarga el cliente OpenVPN y se lleva a cabo su instalación mediante la terminal de comandos. Este procedimiento se ejecuta con el objetivo de facilitar la configuración y la posterior conexión segura a través de OpenVPN desde el sistema operativo Ubuntu.

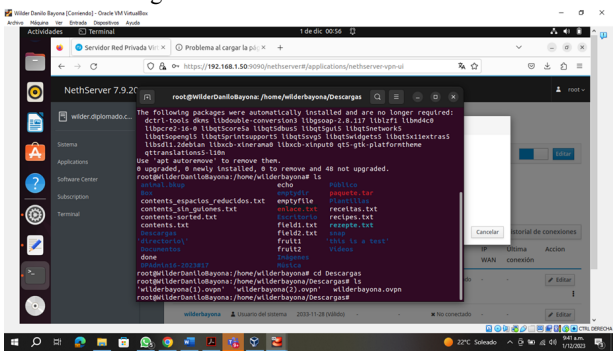
Figura 67. Cliente openVpn



Fuente: Autoría propia

Una vez que se ha completado la instalación del cliente OpenVPN, se procede a copiar el archivo de conexión generado en el servidor VPN. Posteriormente, se ejecuta este archivo utilizando el cliente que se ha instalado previamente. Este proceso asegura que el cliente esté correctamente configurado para establecer una conexión segura con el servidor VPN, utilizando la información específica proporcionada en el archivo de conexión.

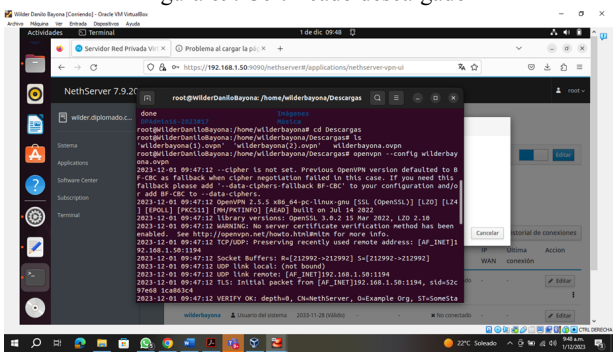
Figura 68. Ubicación del certificado



Fuente: Autoría propia

Para iniciar la conexión VPN mediante el cliente, se ejecuta el certificado con el siguiente comando en la terminal: sudo openvpn --config wilderbayona.ovpn. En este contexto, "wilderbayona" hace referencia al certificado que ha descargado anteriormente desde el servidor. Al utilizar este comando, se activa la configuración específica del certificado, estableciendo de esta manera la conexión VPN a través del cliente.

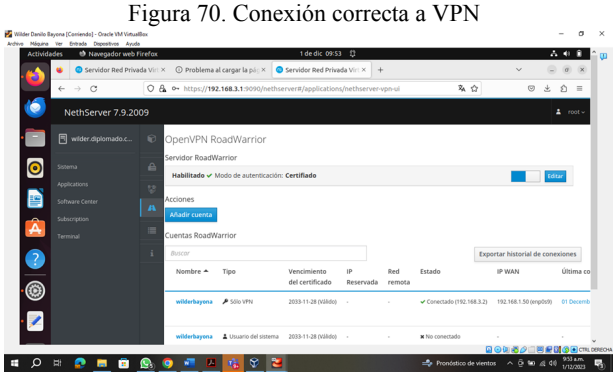
Figura 69. Certificado descargado



Fuente: Autoría propia

Si todas las configuraciones se realizaron de manera correcta, desde el servidor se puede verificar la lista de equipos que están actualmente conectados a través de la VPN. Esto implica que, en caso de una configuración exitosa, el servidor tiene la capacidad de mostrar una visión detallada de los dispositivos que han establecido una conexión segura mediante el servicio VPN.

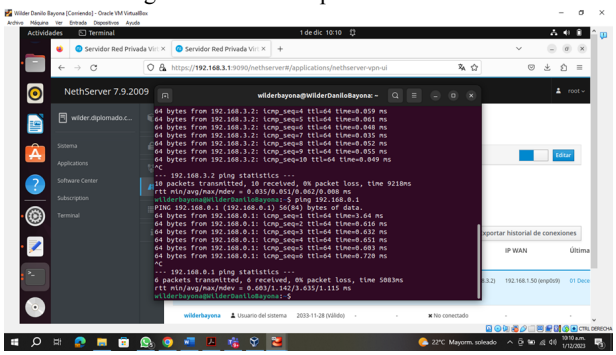
Figura 70. Conexión correcta a VPN



Fuente: Autoría propia

Para verificar la conexión de manera rápida, se lleva a cabo una prueba ejecutando el comando ping desde el dispositivo cliente, el cual está conectado a la VPN, hacia la dirección IP asignada en la zona verde del servidor. Esta dirección forma parte de la red interna. Este procedimiento permite evaluar de manera inmediata si la conexión VPN está establecida correctamente y si se logra la comunicación efectiva entre el cliente y el servidor en la red interna.

Figura 71. Prueba rápida de conexión



Fuente: Autoría propia

7.1.1 CONCLUSIONES.

NethServer es una distribución basada en linux OpenSource la cual funciona como servidor el cual permite mediante la interfaz gráfica web de usuario descargar plugins y administrar los servicios.

A través del NethServer se logró configurar el servidor DHCP, DNS y Controlador de dominio de una forma fácil, con un dashboard y una interfaz gráfica agradable para el administrador de la infraestructura TI.

NethServer mediante las aplicaciones Web Proxy y Web Filter permite una configuración y administración del Proxy pues uno de sus servicios es el Squid proxy que usa los puertos 3128, 3129 y 3130 que permiten aceptar o denegar paginas segun la configuracion que se haya dado en lista negra y lista blanca mediante las URL o las categorías no permitidas, de tal manera que se podrá navegar en la web, pero se permitirá el acceso a las páginas bajo la categoría denegada o específicas

en la lista negra.

La implementación exitosa de un cortafuegos para restringir el acceso a sitios de entretenimiento y redes sociales en estaciones GNU/Linux destaca la importancia de esta medida en la protección de redes informáticas. La configuración detallada de redes, la creación precisa de reglas y la validación efectiva del funcionamiento evidencian la versatilidad y eficacia de los cortafuegos en la gestión del tráfico. En un entorno laboral, esta solución no solo contribuye a mantener la productividad, sino que también desempeña un papel esencial en la mitigación de riesgos cibernéticos. La conclusión reafirma la necesidad continua de medidas proactivas de ciberseguridad para preservar la integridad de las redes y garantizar la privacidad de los usuarios.

Las pruebas llevadas a cabo en torno a la temática de File Server y Print Server han arrojado resultados positivos y han validado de manera efectiva la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux mediante el controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras. La ejecución de estas pruebas ha permitido verificar la eficiencia y la coherencia de la infraestructura diseñada, demostrando que el sistema responde adecuadamente a las necesidades específicas relacionadas con la gestión de archivos y la impresión en un entorno de red. Este proceso ha fortalecido la confianza en la robustez de la solución propuesta, subrayando la importancia de la correcta implementación de un File Server y Print Server para optimizar la conectividad y la accesibilidad en entornos de trabajo basados en GNU/Linux.

La implementación y configuración detallada de la VPN, con el establecimiento exitoso de un túnel privado de comunicación hacia una estación de trabajo GNU/Linux, han resultado en un logro significativo para fortalecer la seguridad y la accesibilidad en el entorno digital. La meticulosa configuración de las zonas DMZ, la generación de certificados, la creación de cuentas de usuario y la instalación del cliente OpenVPN han sentado las bases para una conexión segura y eficiente.

La prueba de conexión exitosa, respaldada por la capacidad de visualizar los equipos conectados desde el servidor, valida la funcionalidad de la VPN. Este logro se evidenció aún más a través de la rápida prueba de conexión mediante ping, donde la estación de trabajo cliente, conectada a través de la VPN, pudo comunicarse de manera efectiva con la red interna del servidor.

8 REFERENCIAS

[1] “Manual del Administrador — NethServer 7 Final,” NethServer.org, 2020. https://docs.nethserver.org/es/v7/ (accessed Dec. 05, 2023).

[2] Manuel Cabrera Caballero, “NethServer Tutorial | Instalación, Actualización y primeros pasos,” YouTube. Oct. 16, 2018. Accessed: Dec. 05, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=FNGmM-2fa_0

[3] Lab Virtuales Servidores, “Instalar #NethServer + Configurar Web Proxy & Filtrar Contenidos Web,” YouTube. Oct. 12, 2023. Accessed: Dec. 05, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=cIHJbtTehKg

[4] “Web proxy — NethServer 7 Final,” NethServer.org, 2023. https://docs.nethserver.org/en/v7/web_proxy.html (accessed Dec. 05, 2023).