CONFIGURACIÓN DE SERVICIOS ESENCIALES IT CON NETHSERVER EN ENTORNOS BASADOS EN GNU/LINUX

Jonathan Neira Torres
e-mail: jneirat@unadvirtual.edu.co
Edgardo Leonel Leal Ariza
e-mail: elleala@unadvirtual.edu.co
Leonardo Uribe Guerrero
e-mail: luribeg@unadvirtual.edu.co
William David Perilla Vanegas
e-mail: wdperillav@unadvirtual.edu.co
Oscar David De Salvador Peña
e-mail: oddesalvadorp@unadvirtual.edu.co

RESUMEN: *En este trabajo se detalla el proceso de configuración e implementación de servicios de infraestructura IT mediante GNU/Linux NethServer. Se realizaron procesos como la instalación del sistema operativo Nethserver, la creación de una zona DMZ y la configuración de servicios esenciales, entre ellos DHCP, DNS, Proxy, Cortafuegos, Servidor de Archivos, Impresoras y VPN. Los resultados obtenidos validaron el funcionamiento de los servicios configurados, demostrando su aplicabilidad para satisfacer las necesidades de administración y seguridad en redes corporativas.*

PALABRAS CLAVE: Controlador de Dominio, File Server, Firewall, Proxy, VPN

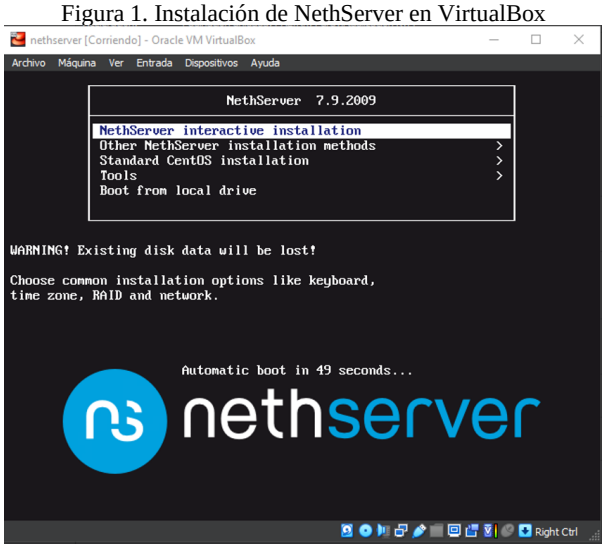
1 INTRODUCCIÓN

En este trabajo se llevará a cabo la implementación y configuración de varios servicios esenciales en un entorno basado en GNU/Linux NethServer. Se instalarán y configurarán servicios como DHCP, DNS, Proxy, Cortafuegos, File Server, Print Server y VPN, afianzando la seguridad y eficiencia del sistema. Todo el proceso se realizará a través de la implementación de NethServer, lo que permitirá optimizar la administración y garantizar un control completo. De igual manera, se prestará especial atención a la creación de zonas DMZ y a la implementación de políticas de seguridad.

2 INSTALACION NETHSERVER

La ISO de NethServer es montada utilizando una máquina virtual con una versión de Red Hat (64 bits) (Fig. 1). Una vez que el sistema inicia, se realizan las configuraciones correspondientes, tales como la fecha, el idioma, los adaptadores de red y el hostname (Figs. 2 y 3).

Figura 1. Instalación de NethServer en VirtualBox

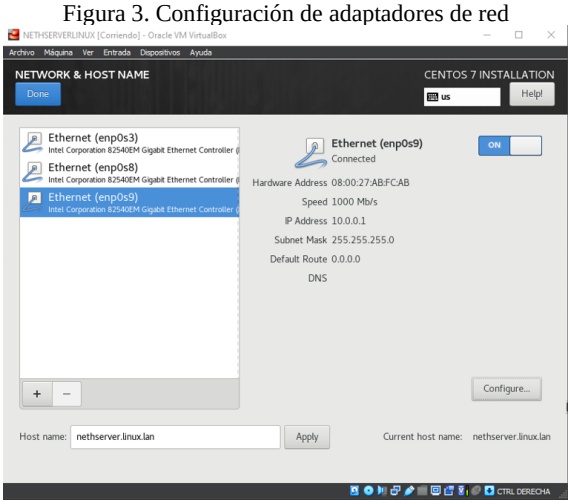


. Fuente: Autoría Propia

Figura 2. Configuración de NethServer

. Fuente: Autoría Propia

Figura 3. Configuración de adaptadores de red



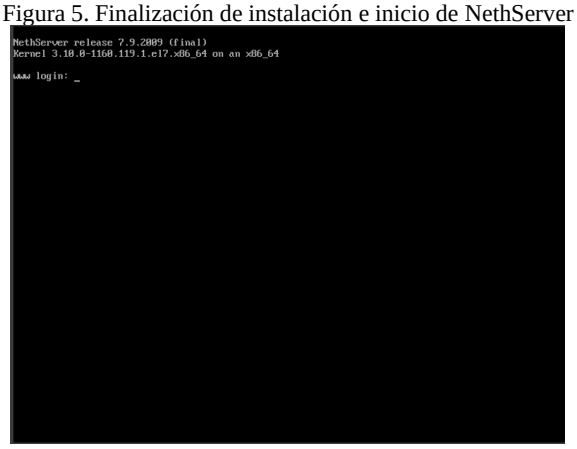
. Fuente: Autoría Propia

Se procede a configurar la contraseña del usuario root (Fig. 4), y se espera la finalización de la instalación (Fig. 5).

Figura 4. Configuración de contraseña usuario root

. Fuente: Autoría Propia

Figura 5. Finalización de instalación e inicio de NethServer



. Fuente: Autoría Propia

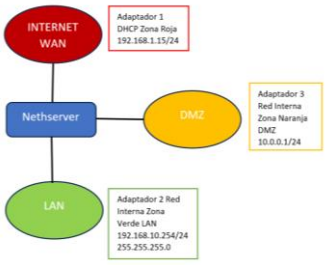
La validación del ingreso a NethServer se realiza a través del puerto 9090, utilizando el usuario root y la contraseña asignada durante la instalación (Fig. 6).

Figura 6. Ingreso a NethServer

. Fuente: Autoría Propia

Ahora, teniendo presente el siguiente diagrama de zonas WAN, LAN y DMZ, se procede a configurar dentro de NethServer (Fig. 7 y 8).

Figura 7. Diagrama de zonas WAN, LAN y DMZ



. Fuente: Autoría Propia

Figura 8. Configuración de zonas en NethServer

. Fuente: Autoría Propia

De esta forma, se finaliza la instalación de NethServer y la configuración de las zonas WAN, LAN y DMZ dentro del mismo.

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

3.1 DHCP SERVER

En el módulo de servidor DHCP, se realiza la siguiente configuración (Fig. 9):

Rango de Direcciones IP:

- Inicio: 192.168.10.1
- Fin: 192.168.10.254
- Este rango cubre casi toda la subred 192.168.10.0/24 (excepto la dirección de red 192.168.10.0 y la dirección de broadcast 192.168.10.255).

Puerta de Enlace (Gateway):

- IP Puerta de Enlace: 192.168.10.3 Esta dirección corresponde al dispositivo que actúa como router o punto de salida de la red hacia otras redes (como Internet).

Dominio: www.nethlab.co

- Esta configuración especifica el dominio predeterminado que se asignará a los dispositivos de la red, útil para redes internas o servicios que utilicen nombres de dominio locales (DNS internos).

Servidores DNS:

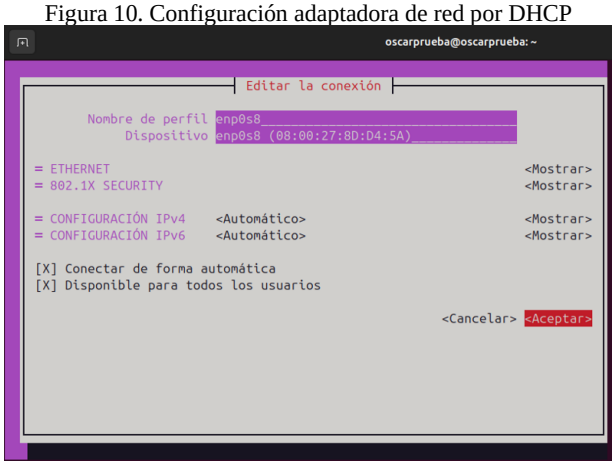
- DNS Primario: 192.168.10.254.

Figura 9. Configuración de servidor DHCP

. Fuente: Autoría Propia

Una vez configurado el servidor DHCP, se procede a configurar el adaptador de red en el Ubuntu Desktop para permitir el acceso a Internet. Esta configuración se realiza utilizando el comando sudo nmtui (Fig. 10).

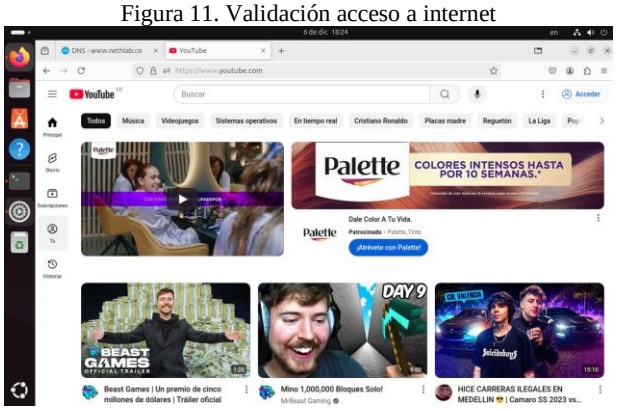
Figura 10. Configuración adaptadora de red por DHCP



. Fuente: Autoría Propia

Se valida tanto la navegación como el escaneo de la interfaz de red para identificar los dispositivos conectados a la Red Interna Verde (LAN) (Fig. 11 Y 12).

Figura 11. Validación acceso a internet



. Fuente: Autoría Propia

Figura 12. Escaneo de IP dentro del rango configurado

. Fuente: Autoría Propia

Se verifica la IP asignada al Ubuntu Desktop utilizando el comando ip a para confirmar la dirección IP (Fig. 13). Posteriormente, esta dirección IP se reserva en el Servidor DHCP para garantizar que siempre se asigne la misma IP al dispositivo (Fig. 14).

Figura 13. Escaneo de IP dentro del rango configurado

. Fuente: Autoría Propia

Figura 14. Escaneo de IP dentro del rango configurado

. Fuente: Autoría Propia

Finalmente, una vez realizadas todas las configuraciones necesarias, el servidor DHCP dentro de NethServer se encuentra configurado y listo para gestionar automáticamente las asignaciones de direcciones IP a los dispositivos de la red.

3.2 DNS SERVER

La configuración del servidor DNS se realiza de la siguiente manera:

Nombre de Host:

- El nombre de host www.nethlab.co se configura como un subdominio dentro del dominio nethlab.co.

Dirección IP:

- La dirección IP configurada para www.nethlab.co es 192.168.10.254, la cual corresponde a un recurso interno dentro de la red local gestionada por el servidor NethServer. Esta IP es utilizada para los dispositivos en la red interna que consultan el servidor DNS.

Registro DNS Wildcard:

- Se configura un registro DNS Wildcard para cubrir cualquier subdominio bajo nethlab.co (*. nethlab.co), redirigiendo todas las consultas a la misma dirección IP interna 192.168.10.254.

Con esta configuración, los dispositivos de la red interna pueden resolver correctamente los nombres de dominio y subdominio definidos en el servidor NethServer (Fig. 15).

Figura 15. Configuración DNS

. Fuente: Autoría Propia

Se verifica que el host haya sido añadido en el apartado de DNS de NethServer y, mediante el uso del navegador, se valida que el dominio www.nethlab.co cargue contenido (Fig. 16 Y 17).

Figura 16. Registro de DNS

. Fuente: Autoría Propia

Figura 17. Validación dominio de DNS

. Fuente: Autoría Propia

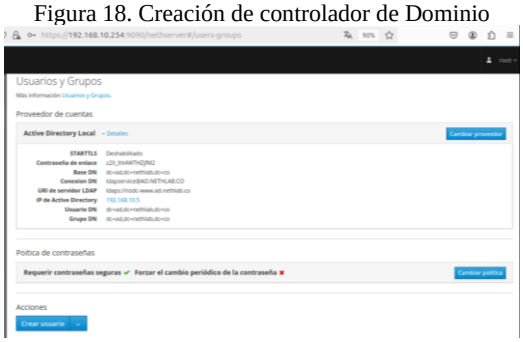
Con esto, se confirma que el DNS ha sido registrado correctamente y está funcionando de manera adecuada desde NethServer.

3.3 CONTROLADOR DE DOMINIO

La configuración del módulo de Usuarios y Grupos en NethServer se realiza utilizando un proveedor de cuentas basado en Active Directory (AD) (Fig. 18).

Active Directory Local: Indica que el servidor está ejecutando un AD interno, lo que permite la gestión centralizada de usuarios, grupos y políticas en la red.

Figura 18. Creación de controlador de Dominio



. Fuente: Autoría Propia

Configuración del AD:

- Contraseña de enlace: Proporciona la autenticación del servidor LDAP al interactuar con el AD.
- URI del servidor LDAP: El servidor LDAP está configurado con un esquema seguro ("ldaps://nsdc-www.ad.nethlab.co").
- IP de Active Directory: 192.168.10.5 es la dirección IP del servidor AD local.

Se procede a crear un usuario en Active Directory para validar su funcionamiento (Fig. 19).

Figura 19. Creación de usuario

. Fuente: Autoría Propia

En NethServer, al activar el controlador de dominio (Active Directory), el sistema configura automáticamente una red virtual para manejar la comunicación interna del controlador de dominio. Como resultado, el dispositivo de red asociado cambia su configuración a un puente de red (br0) (Fig. 20).

Figura 20. Cambio de configuración de adaptador de red

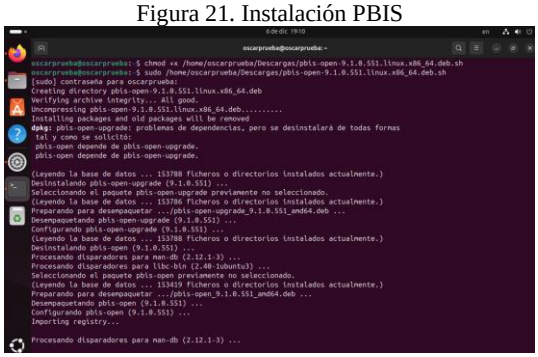
. Fuente: Autoría Propia

Para integrar Ubuntu Desktop al dominio, se utiliza PBIS, que permite la autenticación de usuarios de Active Directory y la aplicación de políticas centralizadas (Fig. 21).

Para la instalación de PBIS, se utilizan los siguientes comandos:

- chmod +x /home/oscarprueba/Descargas/pbis-open-9.0.2.534.linux.x86_64.deb.sh
- sudo /home/oscar_desalvador/Descargas/pbis-open-9.0.2.534.linux.x86_64.deb.sh

Figura 21. Instalación PBIS



. Fuente: Autoría Propia

Para unirse al dominio, se debe ejecutar la siguiente línea de comando en Ubuntu Desktop (Fig. 22):

- sudo /opt/pbis/bin/domainjoin-cli join ad.nethlab.co oscar_unad

Figura 22. Unirse al dominio

. Fuente: Autoría Propia

Una vez que el equipo esté en el dominio, se reinicia y se verifica el ingreso del usuario el cual fue creado previamente en Active Directory (Fig. 23).

Figura 23. Validación de usuario de dominio

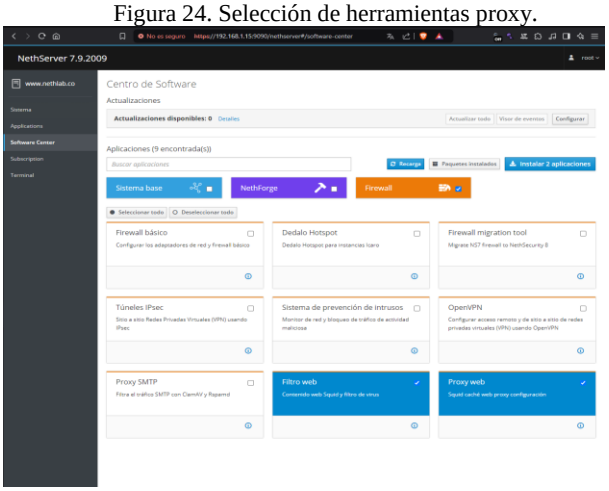
. Fuente: Autoría Propia

4 TEMÁTICA 2 PROXY

4.1 CONFIGURACIÓN INICIAL

Se realizó la selección de dos servicios clave: el Filtro web y el Proxy web. El filtro web se encargó de gestionar el contenido que se podía acceder a través del proxy, mientras que el proxy web gestionó la configuración de Squid para el caché y el manejo del tráfico (Fig. 24).

Figura 24. Selección de herramientas proxy.

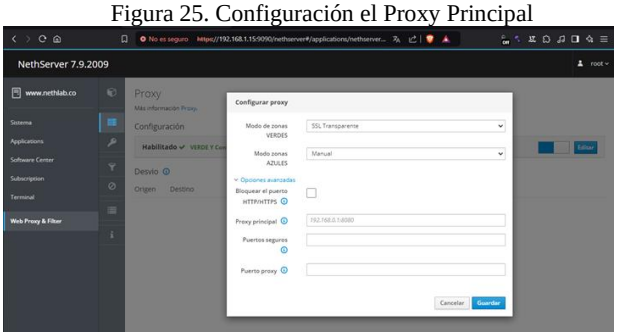


. Fuente: Autoría Propia

4.2 CONFIGURACIÓN DEL PROXY

Se configuró el proxy en NethServer para definir el comportamiento de las zonas de red y asegurar que el filtrado y el manejo de tráfico fueran los adecuados (Fig. 25).

Figura 25. Configuración el Proxy Principal



. Fuente: Autoría Propia

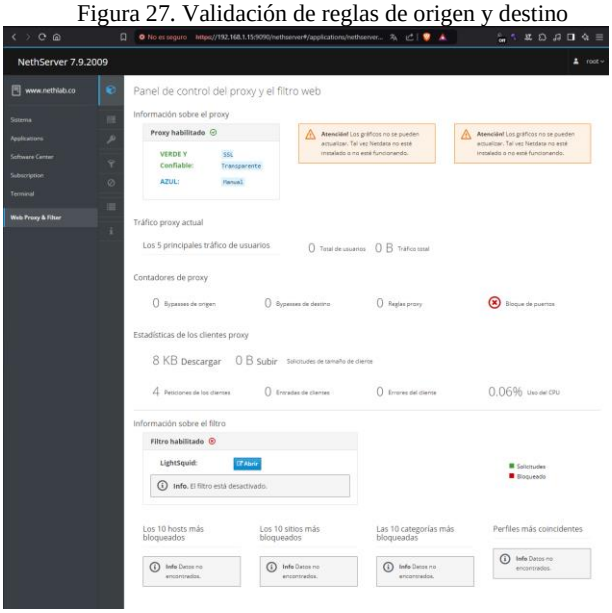
En el Modo de Zonas, se configuró la zona VERDE en modo SSL Transparente, permitiendo la inspección y el filtrado eficiente del tráfico HTTPS sin afectar la experiencia del usuario. Por su parte, la zona AZUL permaneció en modo manual para ajustes futuros. En las Opciones Avanzadas, se habilitaron configuraciones adicionales, como el bloqueo de tráfico HTTP/HTTPS no deseado, reforzando la seguridad. Para la Definición del Proxy Principal, se estableció la IP y el puerto del proxy (192.168.0.1:8080), asegurando la redirección de solicitudes (Fig. 26).

Figura 26. Configuración reglas de origen y destino

. Fuente: Autoría Propia

Se confirmó que el proxy estaba habilitado y que las zonas habían sido configuradas correctamente (Fig. 27).

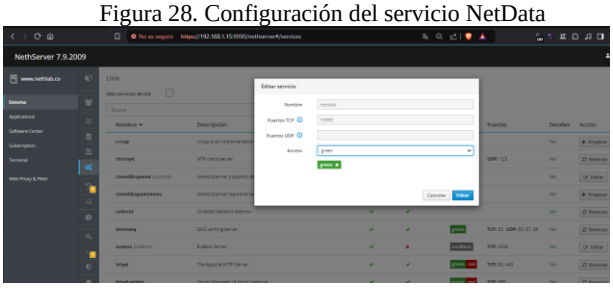
Figura 27. Validación de reglas de origen y destino



. Fuente: Autoría Propia

En el cuadro de diálogo de edición del servicio NetData, se configuró el puerto TCP en 19999 y se restringió el acceso a la red confiable (Green) para habilitar el monitoreo en tiempo real del proxy y otros servicios. Se verificó que el servicio estuviera activo y, tras revisar los parámetros, se aplicaron los cambios para garantizar un diagnóstico eficiente y una resolución ágil de problemas (Fig. 28).

Figura 28. Configuración del servicio NetData



. Fuente: Autoría Propia

Se verificaron las reglas de redirección en Shorewall y las cadenas de iptables para validar la implementación del proxy transparente en el puerto 3128. Se utilizó el comando cat /etc/shorewall/rules | egrep REDIRECT para confirmar que el tráfico HTTP y HTTPS era redirigido correctamente al proxy Squid desde la red confiable (green). Además, se revisaron las cadenas PREROUTING en iptables, donde las reglas etiquetadas como "transparent proxy on green" aseguraron que todo el tráfico pasara por Squid, permitiendo aplicar políticas de filtrado y monitoreo (Fig. 29).

Figura 29. Configuración del servicio NetData

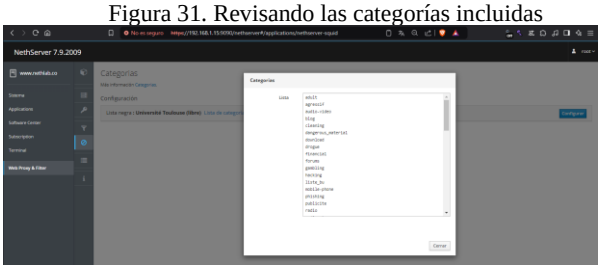
. Fuente: Autoría Propia

Se configuraron categorías en el módulo Web Proxy & Filter de NethServer, activando la lista negra "Université Toulouse" en estado "libre" y permitiendo la creación de reglas adicionales para gestionar el acceso según las necesidades. También se mostró el listado de categorías incluidas (Fig. 30 y 31).

Figura 30. Ajustando las opciones para la lista negra

. Fuente: Autoría Propia

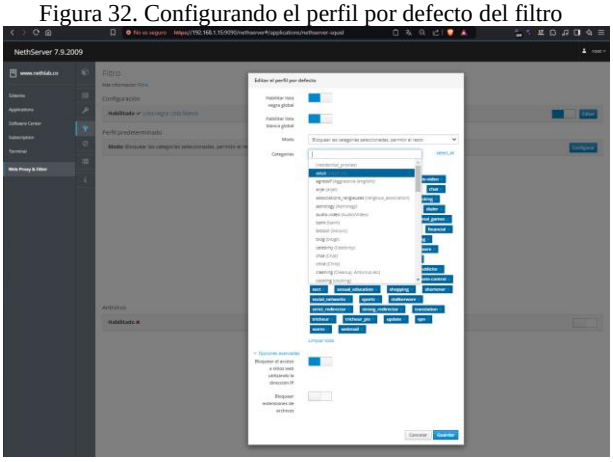
Figura 31. Revisando las categorías incluidas



. Fuente: Autoría Propia

Se revisaron las categorías de la lista negra "Université Toulouse" en el módulo Web Proxy & Filter de NethServer, las cuales incluían categorías como adult, audio-video, hacking, gambling, phishing y publicite, diseñadas para bloquear contenido específico. Esta configuración permitió aplicar políticas de bloqueo detalladas, mejorando la seguridad y adaptándose a las necesidades de la red (Fig. 32).

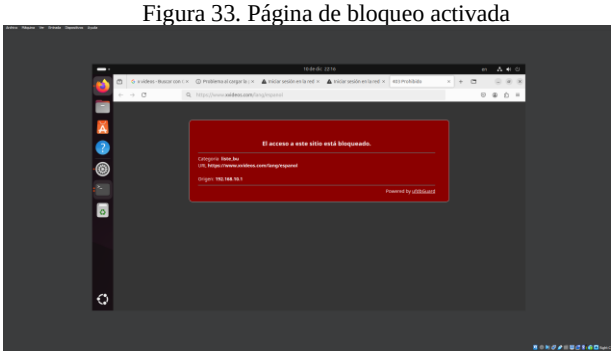
Figura 32. Configurando el perfil por defecto del filtro



. Fuente: Autoría Propia

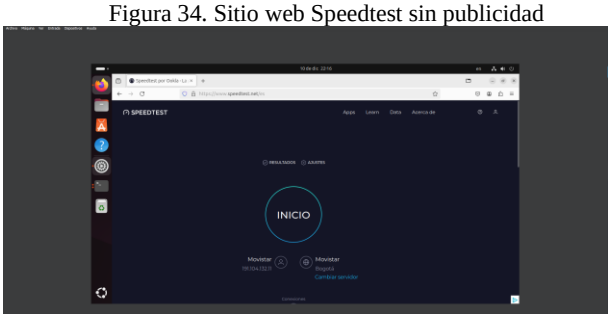
En el primer caso, se presentó una página de bloqueo generada por el filtro web de NethServer, donde se denegó el acceso a la URL [https://www[.]xvideos[.]com/Lang/español] por pertenecer a la categoría liste_bu. Esto evidenció la efectividad de las políticas configuradas con SquidGuard y ufdbGuard para restringir contenido no deseado (Fig. 33). Por otro lado, el segundo caso mostró un acceso exitoso al sitio Speedtest.net, demostrando que herramientas de diagnóstico como esta no están restringidas, permitiendo realizar pruebas de conectividad y monitoreo de la red sin inconvenientes (Fig. 34).

Figura 33. Página de bloqueo activada



. Fuente: Autoría Propia

Figura 34. Sitio web Speedtest sin publicidad



. Fuente: Autoría Propia

5 TEMÁTICA 3: CORTAFUEGOS

5.1 CONFIGURACIÓN INICIAL

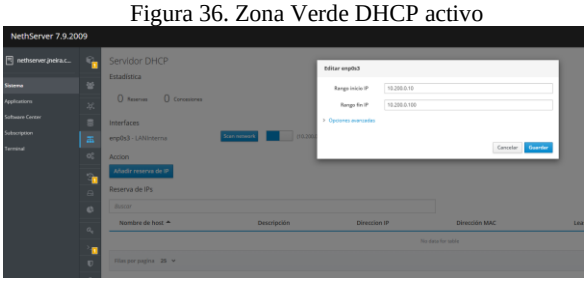
Se verifica el estado de las interfaces antes de la instalación del módulo de cortafuegos. La parametrización inicial del NethServer se completa antes de configurar las reglas del firewall. Se confirma que las interfaces se encuentran en modo activo (UP) (Fig. 35).

Figura 35. Revisión de Interfaces de red.

Fuente: Autoría Propia

Se configura el servicio DHCP en la red LAN (Zona Verde). Se habilita un rango de direcciones IP (pool) desde 10.200.0.10 hasta 10.200.0.100 para su uso posterior en el cortafuegos (Fig. 36).

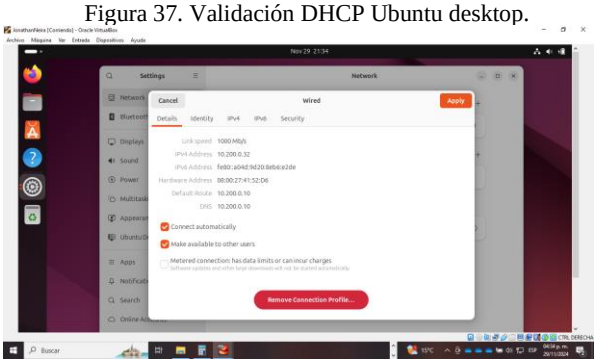
Figura 36. Zona Verde DHCP activo



. Fuente: Autoría Propia

Se comprueba la asignación DHCP en la máquina Ubuntu Desktop (Fig. 37).

Figura 37. Validación DHCP Ubuntu desktop.



. Fuente: Autoría Propia

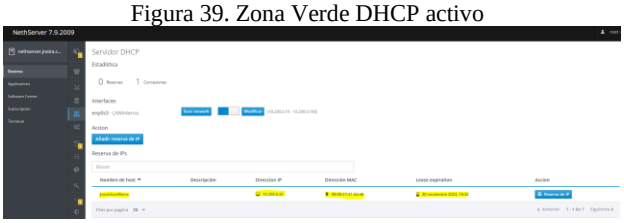
Se comprueba el acceso desde la red LAN Interna (GREEN LAN) al firewall a través del default Gateway 10.200.0.10 (Fig. 38).

Figura 38. Acceso NethServer

Fuente: Autoría Propia

Comprobación de asignación DHCP desde NethServer. Se valida que desde el servidor este tomando correctamente DHCP para asignar posteriores políticas de cortafuegos a la subnet asignada (Fig. 39).

Figura 39. Zona Verde DHCP activo

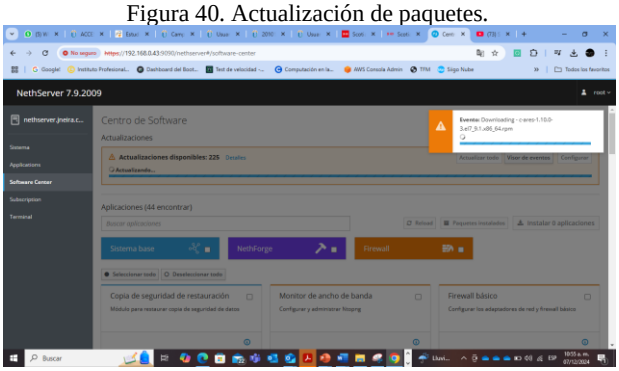


Fuente: Autoría Propia

5.2 INSTALACIÓN CORTAFUEGOS

Antes de proceder con la instalación de la aplicación de cortafuegos, es necesario llevar a cabo la instalación de las actualizaciones de paquetes pendientes. Esto permite prevenir posibles errores durante la configuración (Fig. 40).

Figura 40. Actualización de paquetes.



. Fuente: Autoría Propia

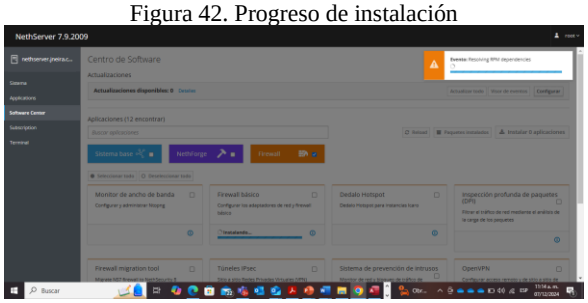
A través del Software Center, se lleva a cabo la instalación de la aplicación de firewall básico, la cual incluye características esenciales de cortafuegos. Esta aplicación permite la creación de reglas para autorizar o denegar tráfico entre las diferentes interfaces del firewall (Fig. 41).

Figura 41. Instalación Firewall Básico.

. Fuente: Autoría Propia

Ejecución del paquete de instalación en progreso (Fig. 42).

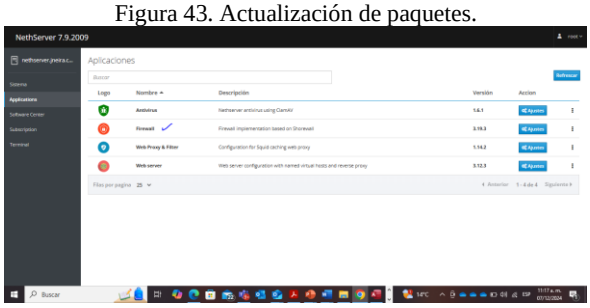
Figura 42. Progreso de instalación



. Fuente: Autoría Propia

Se verifica la correcta instalación del paquete de cortafuegos o firewall básico en el servidor NethServer (Fig. 43).

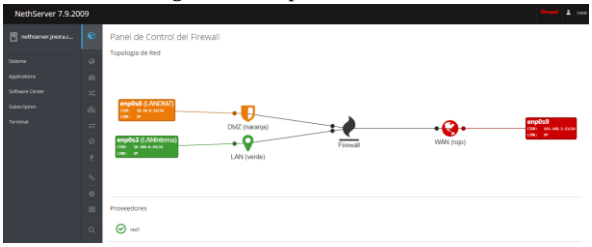
Figura 43. Actualización de paquetes.



. Fuente: Autoría Propia

Una vez realizada la instalación correctamente se verifica el entorno principal del cortafuegos donde se validan las interfaces configuradas (Fig. 44).

Figura 44. Mapa de Interfaces

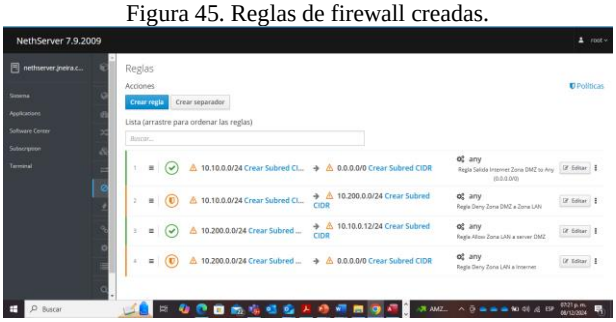


. Fuente: Autoría Propia

Reglas de Firewall creadas (Fig. 45).

- Regla 1: Se otorgan permisos para cualquier destino hacia la Zona DMZ.
- Regla 2: Se deniega el tráfico proveniente de la Zona DMZ hacia la Zona LAN interna.
- Regla 3: Se permite el tráfico desde la Zona LAN (Verde) hacia la Zona DMZ (Naranja) para habilitar el acceso al servidor.
- Regla 4: Se deniega la salida a Internet (destino 0.0.0.0/0) desde la red interna.

Figura 45. Reglas de firewall creadas.



. Fuente: Autoría Propia

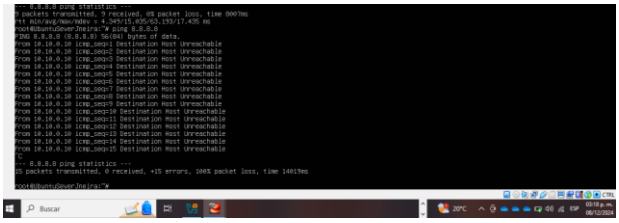
5.3 PRUEBAS DE OPERACIÓN

Evidencias de Reglas de Cortafuegos (Fig. 46).

Prueba No 1:

- Tráfico desde la Zona DMZ hacia Internet.
- Resultado: Sin una regla aplicada, la conexión no funciona.

Figura 46. Prueba No 1

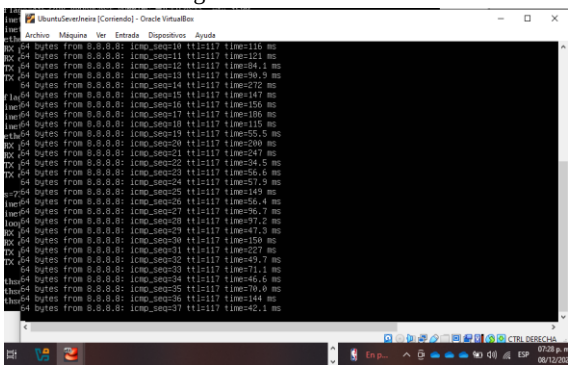


. Fuente: Autoría Propia

Prueba exitosa:

Al aplicar la regla de salida hacia cualquier destino (Regla 1), el tráfico desde la Zona DMZ hacia Internet funciona correctamente (Fig. 47).

Figura 47. Prueba No 1

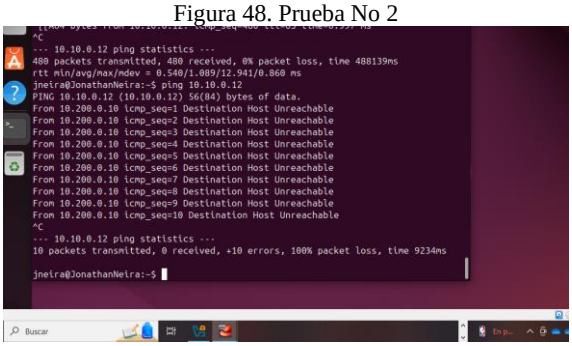


. Fuente: Autoría Propia

Prueba No 2:

- Prueba sin generar regla desde la Zona LAN hacia la Zona DMZ.
- Resultado: Sin la regla correspondiente, no se establece comunicación entre las zonas (Fig. 48).

Figura 48. Prueba No 2

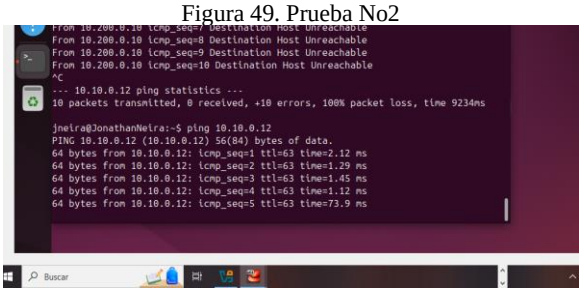


. Fuente: Autoría Propia

Prueba exitosa:

Al asignar la regla desde la Zona LAN hacia la Zona DMZ, se permite el tráfico desde el equipo de escritorio Ubuntu hacia el servidor ubicado en la Zona DMZ (Fig. 49).

Figura 49. Prueba No2

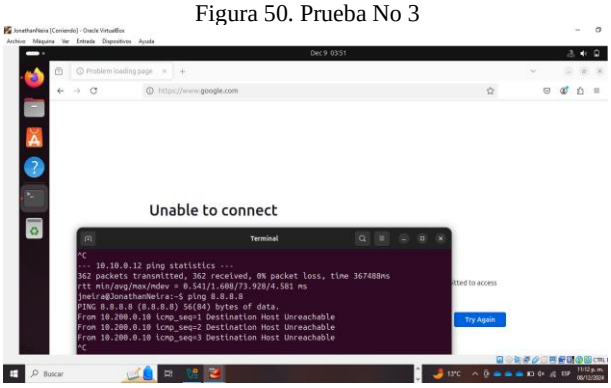


. Fuente: Autoría Propia

Prueba exitosa:

Se logró la denegación del tráfico desde la Zona LAN (Green) hacia Internet, conforme a la regla configurada (Fig. 50).

Figura 50. Prueba No 3



. Fuente: Autoría Propia

6 TEMATICA 4 FILE SERVER Y PRINT SERVER

Se procede a instalar el Print Server utilizando el Centro de Software de NethServer para habilitar la funcionalidad de gestión de impresoras en el sistema. (Fig. 51).

Figura 51. Instalación Print Serve

. Fuente: Autoría Propia

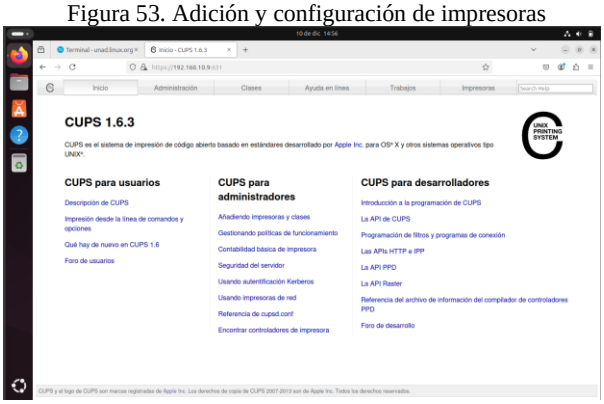
Se realiza la configuración a través de la consola para agregar una impresora virtual y habilitar el firewall, asegurando el correcto funcionamiento del sistema de impresión y la protección de la red (Fig. 51).

Figura 52. Configuración por consola

. Fuente: Autoría Propia

Se realiza el proceso de adición y configuración de impresoras en el sistema, lo que permite que los usuarios puedan acceder y utilizar los recursos de impresión de manera adecuada (Fig. 53).

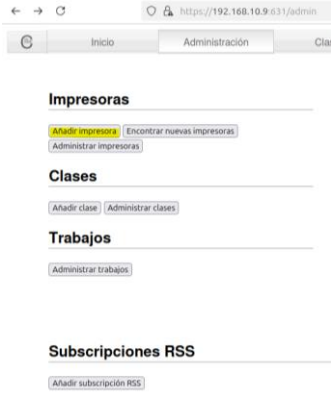
Figura 53. Adición y configuración de impresoras



. Fuente: Autoría Propia

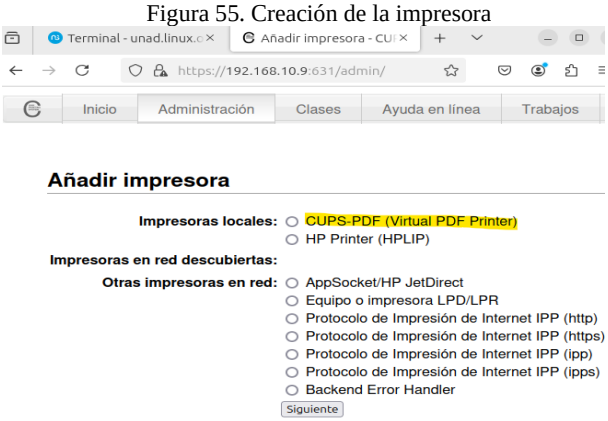
Se lleva a cabo el proceso de creación de la impresora en el sistema, permitiendo su integración y configuración para su uso adecuado (Fig. 54 y 55).

Figura 54. Creación de la impresora



. Fuente: Autoría Propia

Figura 55. Creación de la impresora



. Fuente: Autoría Propia

Se realiza la validación de las impresiones para asegurar que el proceso de impresión funcione correctamente y que los documentos se impriman según las configuraciones establecidas (Fig. 56 y 57).

Figura 56. Validar impresiones

. Fuente: Autoría Propia

Figura 57. Validar impresiones

. Fuente: Autoría Propia

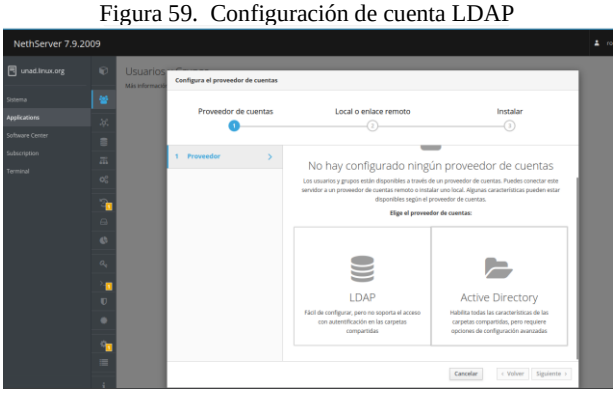
Se lleva a cabo la instalación del servidor de archivos (File Server) para permitir el almacenamiento y acceso compartido de datos en la red (Fig. 58).

Figura 58. Instalación de File Server

. Fuente: Autoría Propia

Se realiza la configuración de la cuenta LDAP para gestionar de manera centralizada las autenticaciones y permisos de acceso en el sistema (Fig. 59).

Figura 59. Configuración de cuenta LDAP



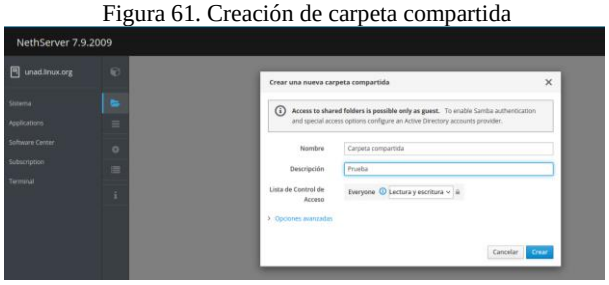
. Fuente: Autoría Propia

Se lleva a cabo la creación de una carpeta compartida en el sistema, lo que permite que los usuarios autorizados accedan a los archivos dentro de la red (Fig. 60 y 61).

Figura 60. Creación de carpeta compartida

. Fuente: Autoría Propia

Figura 61. Creación de carpeta compartida



. Fuente: Autoría Propia

Se puede verificar que la carpeta compartida se visualice, facilitando el acceso y la gestión de los recursos compartidos en la red. (Fig. 62).

Figura 62. Validación carpeta compartida

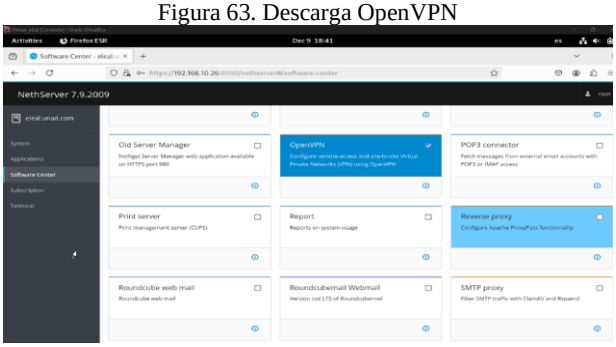
. Fuente: Autoría Propia

7 TEMATICA 5 VPN

7.1 INSTALACIÓN OPENVPN

Es necesario que se instale OpenVPN en el NethServer desde el Software Center para que se pueda iniciar la configuración de la VPN según los parámetros y cuentas deseadas (Fig. 63 y 64).

Figura 63. Descarga OpenVPN



. Fuente: Autoría Propia

Figura 64. Instalación OpenVPN

. Fuente: Autoría Propia

7.2 CREACIÓN DE CUENTA LDAP

Se crean las cuentas del proveedor local LDAP para que se pueda proceder con la descarga de certificados por usuario y la configuración de cuentas locales, lo que permitirá el acceso a la conexión por VPN (Fig. 65 y 66).

Figura 65. Instalación proveedor LDAP

. Fuente: Autoría Propia

Figura 66. Configuración de usuario LDAP

. Fuente: Autoría Propia

Finalmente, se descarga el certificado, el cual debe ser utilizado en el cliente VPN que se instalará posteriormente en el equipo que se desea conectar (Fig. 67).

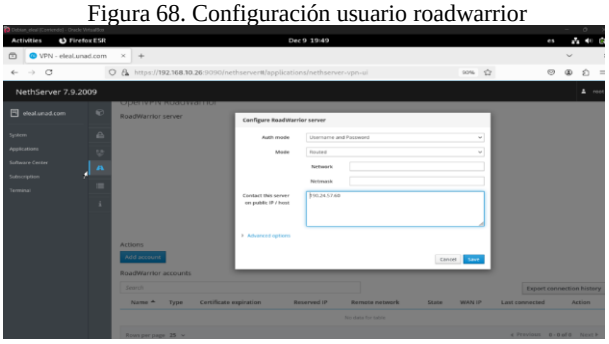
Figura 67. Descarga del certificado privado

. Fuente: Autoría Propia

7.3 CONFIGURACIÓN DEL ROADMIRROR EN VPN

Se debe realizar la configuración en el NethServer, denominado roadmirror, el cual establece los parámetros de conexión VPN para los usuarios clientes (Fig. 68).

Figura 68. Configuración usuario roadwarrior

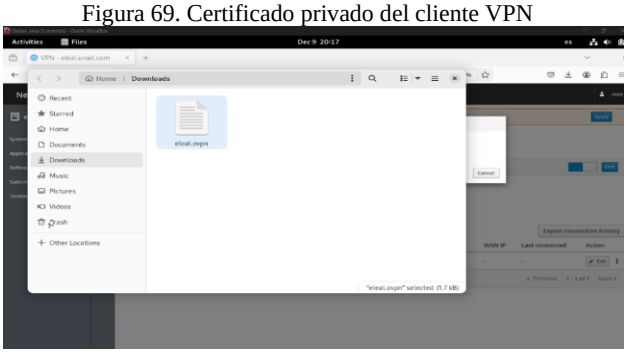


. Fuente: Autoría Propia

7.4 INSTALACIÓN DE CERTIFICADO Y CLIENTE VPN

Para la conexión VPN en un equipo cliente, es necesario descargar una aplicación llamada OpenVPN, en la cual se aplicará el certificado privado de la conexión y se configurará el acceso bajo usuario y contraseña (Fig. 69).

Figura 69. Certificado privado del cliente VPN



. Fuente: Autoría Propia

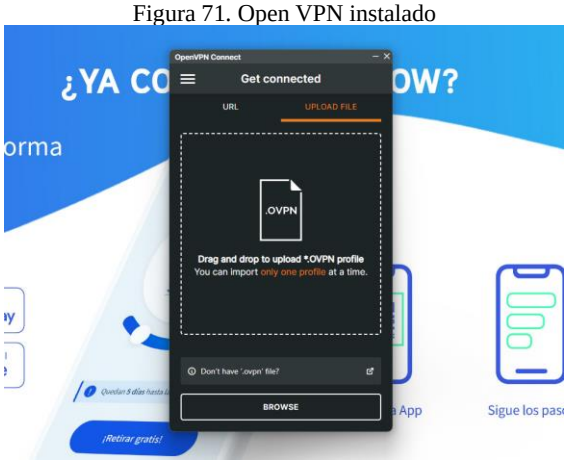
En el equipo cliente se instala la aplicación OpenVPN. En este ejercicio práctico, la instalación se realizó en un equipo con Windows de forma estándar para poder probar la conexión (Fig. 70).

Figura 70. Descarga OpenVPN en cliente Windows

. Fuente: Autoría Propia

Se instala como una aplicación estándar de Windows y, al abrirla, se debe cargar el certificado, el usuario y la contraseña previamente creados en NethServer, con el fin de garantizar una conexión segura (Fig. 71 y 72).

Figura 71. Open VPN instalado



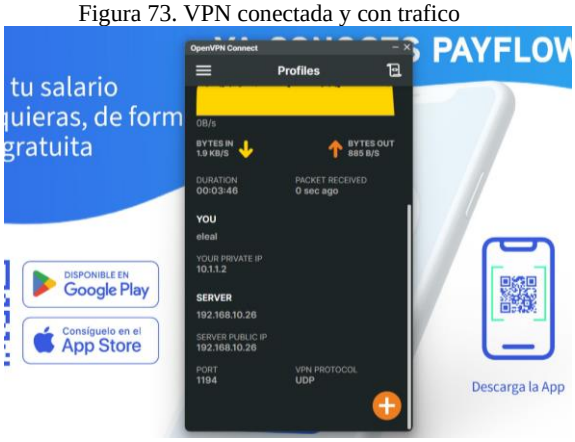
. Fuente: Autoría Propia

Figura 72. Configuración de usuario en OpenVPN

. Fuente: Autoría Propia

Ahora es posible visualizar la VPN conectada en el equipo cliente, con tráfico de subida y bajada hacia el direccionamiento de red configurado, utilizando el usuario creado en el NethServer (Fig. 73).

Figura 73. VPN conectada y con trafico



. Fuente: Autoría Propia

Una vez activa y configurada la VPN, se puede visualizar desde la consola de NethServer el equipo cliente correctamente conectado, con consumo y tráfico, lo cual permite hacer uso de aplicaciones o servicios locales propios de la red a la que se desea conectar a través del túnel VPN (Fig. 74).

Figura 74. Consumo de la red por VPN entre cliente - Server

. Fuente: Autoría Propia

8 CONCLUSIONES

La implementación de Nethserver con zonas segmentadas mejora la seguridad y eficiencia en la gestión de tráfico. La configuración de DHCP y DNS automatiza la asignación de direcciones IP y la administración de dominios internos. Finalmente, la integración de Ubuntu Desktop con Active Directory mediante PBIS centraliza la gestión de usuarios, mejorando la seguridad y administración en la red.

La actividad evidencia la capacidad del filtro web para gestionar accesos según políticas definidas, reforzando la seguridad y eficiencia en la red. Este balance entre bloquear contenido no autorizado y permitir herramientas útiles es esencial para garantizar un entorno de trabajo seguro y funcional.

Mediante el uso de NetServer es viable realizar reglas de tráfico tanto entrante como saliente aprovechando la característica de cortafuegos que puede ser instalada. Definiendo correctamente la topología y permisos de tráfico que deben operar sobre los servicios internos, se puede asegurar mediante este servicio los equipos o dispositivos que no requieran ser expuestos hacia internet.

En NethServer, los File Server y Print Server son servicios esenciales para gestionar recursos compartidos en una red. El File Server permite almacenar, organizar y compartir archivos entre los usuarios, facilitando el acceso y la colaboración en entornos de trabajo. NethServer soporta protocolos como SMB (Samba), lo que permite la integración con sistemas Windows, asegurando una gestión eficiente de los archivos. Por otro lado, el Print Server en NethServer permite compartir impresoras en la red, lo que permite a los usuarios enviar trabajos de impresión de manera centralizada, mejorando la eficiencia y reduciendo costos al gestionar una única impresora para múltiples usuarios. Este servicio se configura fácilmente, y NethServer asegura un manejó sencillo de la impresión en entornos mixtos (Linux y Windows).

Gracias a nethserver podemos también crear VPNs que permiten conexiones seguras hacia otras redes o ambientes delimitados y configurados, garantizando seguridad y estabilidad en la conectividad de clientes y grupos de trabajo, lo anterior nos permite crear redes más administrables y con parámetros propios de entornos colaborativos a menor costos sin poner en riesgo las políticas de ciberseguridad de una compañía.

9 REFERENCIAS

[1] Guía Debian GNU/Linux de instalación. (s/f). Debian.org. Recuperado el 11 de diciembre de 2024, de https://www.debian.org/releases/stable/amd64/index.es.html

[2] Juárez, A. [@antoniojuarez9858]. (s/f). 2. NethServer | Configuración e instalación de aplicaciones. Youtube. Recuperado el 11 de diciembre de 2024, de https://www.youtube.com/watch?v=aNAbGaayx2Y

[3] Murillo, R. [@RobertoMurillo]. (s/f). Instalar #NethServer + configurar web proxy & filtrar contenidos web. Youtube. Recuperado el 7 de diciembre de 2024, de https://www.youtube.com/watch?v=R7qNw06qOPs&t=1345s

[4] Tema 109: Fundamentos de redes. (s/f). Lpi.org. Recuperado el 11 de diciembre de 2024, de https://learning.lpi.org/es/learning-materials/102-500/109/

[5] Virt, T. [@TechVirt1]. (s/f). NethServer OpenVPN Site2Site. Youtube. Recuperado el 11 de diciembre de 2024, de https://www.youtube.com/watch?v=pX5IqeoSyng&t=1173s