

TEMATICAS DE IMPLEMENTACION EN INFRAESTRUCTURAS TI BAJO LOS SERVICIOS DE GESTION DE NETHSERVER

Ronal Gómez Rosero C.C 1116242550
rgomezros@unadvirtual.edu.co
Jorge Leonardo Cárdenas Arias C.C 1115072071
jlcardenasa@unadvirtual.edu.co
María Angélica Cuervo Carrillo C.C 38144970
macuervoc@unadvirtual.edu.co
Juan Gabriel Muñoz Martínez C.C 6406079
jgmunozma@unadvirtual.edu.co
Julián Fernando Ramírez Manzano C.C 14703073
jframirezma@unadvirtual.edu.co

RESUMEN: Nethserver es una solución integral para la gestión de infraestructura IT que permite implementar de manera centralizada servicios clave como DHCP Server para la asignación automática de direcciones IP, DNS Server para la resolución de nombres de dominio, y Controlador de Dominio para la administración centralizada de usuarios y equipos. Además, incluye un servidor proxy y cortafuegos que protegen la red y regulan el acceso a internet, un File Server para compartir archivos de forma segura y un Print Server para la gestión centralizada de impresoras. Finalmente, su funcionalidad VPN proporciona acceso remoto seguro, convirtiéndolo en una herramienta versátil y eficiente para optimizar y proteger entornos empresariales modernos.

PALABRAS CLAVE: DHCP server, nethserver, dominio, Dirección IP, VPN

1 INTRODUCCIÓN

Nethserver es una plataforma completa para la gestión de infraestructura IT, que permite la implementación de servicios clave como DHCP, DNS, Controlador de Dominio, servidor proxy, cortafuegos, File Server, Print Server y VPN, ofreciendo soluciones integrales para optimizar, proteger y administrar redes empresariales de manera eficiente y escalable por la IEEE.

2 INSTALACION Y CONFIGURACION

2.1 CREACION DE MAQUINA VIRTUAL

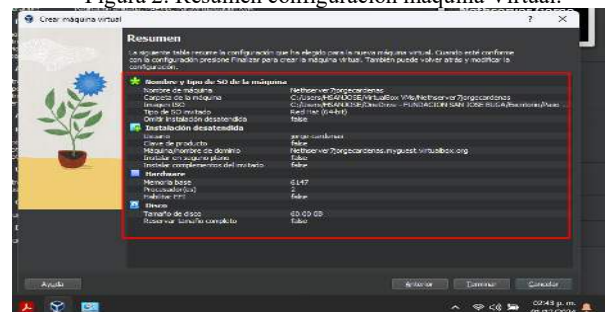
Se lleva a cabo la configuración de la máquina virtual en VirtualBox, considerando los requisitos mínimos del sistema especificados en la documentación de nethserver. Posteriormente, se configuran las tarjetas de red del servidor para establecer los parámetros necesarios en la implementación de las tres redes: WAN (roja), DMZ (naranja) y LAN (verde).

Figura 1. Requisitos de instalación Nethserver



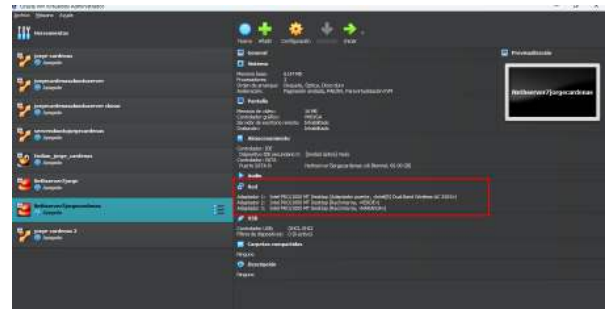
Fuente: Autoría Propia

Figura 2. Resumen configuración máquina Virtual.



Fuente: Autoría Propia

Figura 3. Configuración tarjetas de red para la máquina virtual

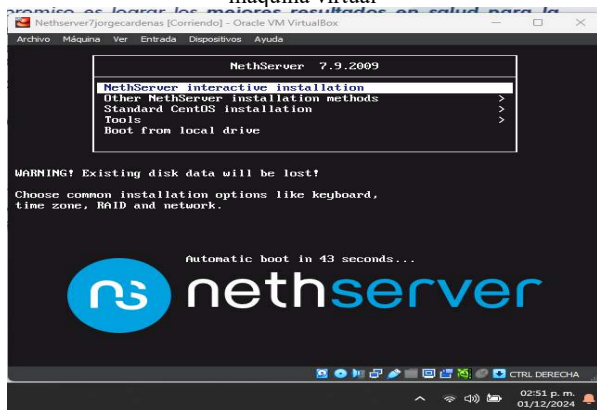


Fuente: Autoría Propia

2.2 PROCESO DE INSTALACIÓN DE NETHSERVER

Se procede con la instalación de nethserver en la máquina virtual previamente configurada en VirtualBox. Al iniciar el proceso, nethserver solicita seleccionar el método de instalación. En este caso, se elige la instalación interactiva para personalizar la configuración del sistema de acuerdo con los requisitos específicos.

Figura 4. Instalación interactiva de nethserver en la máquina virtual



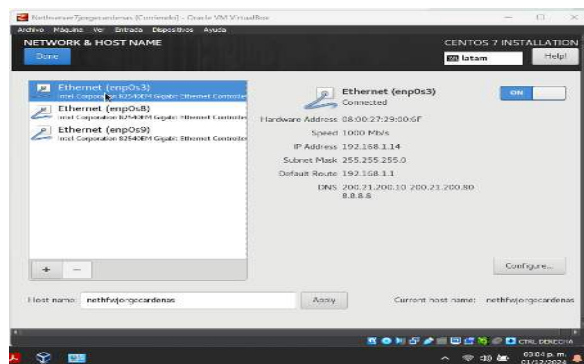
Fuente: Autoría Propia

Figura 5. Resumen de la instalación de nethserver: configuración de la zona horaria y la distribución del teclado.



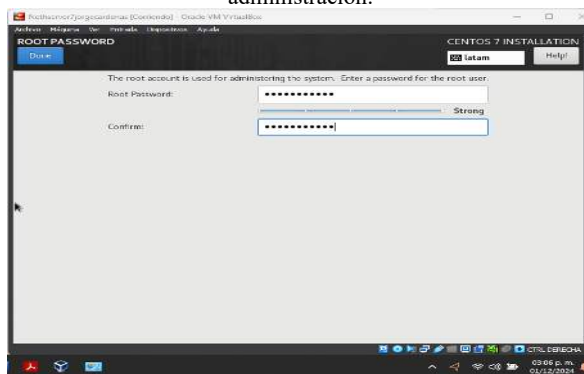
Fuente: Autoría Propia

Figura 6. Configuración tarjetas de red de la máquina virtual una para cada zona Roja WAN, Verde LAN y Naranja DMZ



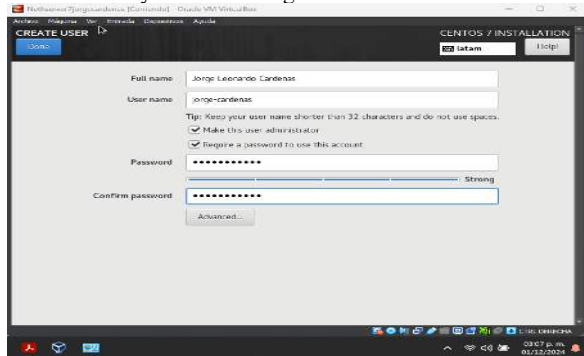
Fuente: Autoría Propia

Figura 7. Estableciendo la contraseña de root para acceso seguro al sistema, garantizando credenciales de administración.



Fuente: Autoría Propia

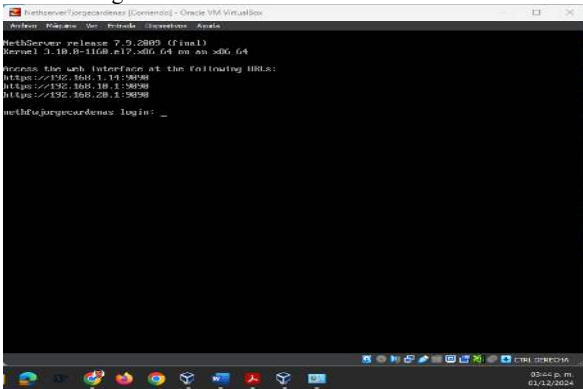
Figura 8. Creación de usuario con permisos de administrador y contraseña segura.



Fuente: Autoría Propia

Tras reiniciar la máquina virtual, se accede con las credenciales de root o jorge-cardenas. Se utiliza la IP de la zona VERDE (192.168.10.1) para ingresar a la consola web y configurar las demás zonas de red.

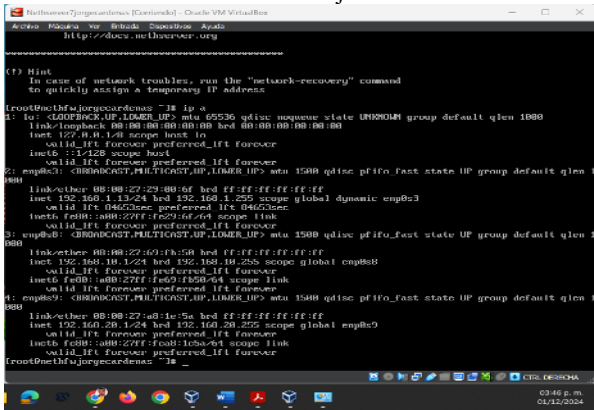
Figura 9. Inicio de nethserver



Fuente: Autoría Propia

Al iniciar sesión como root, se usa el comando ip para verificar las direcciones IP asignadas. Las interfaces se identifican fácilmente por su dirección MAC, confirmando la configuración correcta.

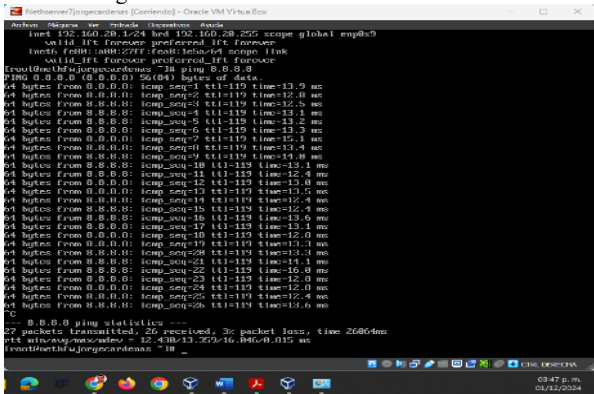
Figura 10. Verificación de direcciones IP e identificación de tarjetas de red.



Fuente: Autoría Propia

Se ejecuta un ping a 8.8.8.8 para confirmar la conexión a Internet a través de la zona ROJA, garantizando la capacidad del servidor para actualizar o instalar software.

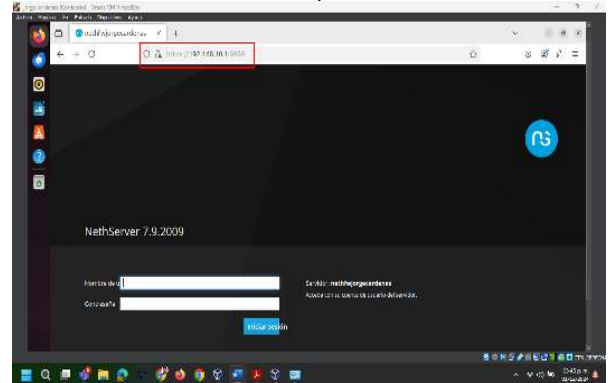
Figura 11. Verificación de conexión a Internet



Fuente: Autoría Propia

Se accede a nethserver desde el navegador en 192.168.10.1:9090 con las credenciales de root. Desde un equipo Ubuntu Desktop en la red LAN VERDE, configurado con la IP fija 192.168.10.2 debido a la ausencia de DHCP.

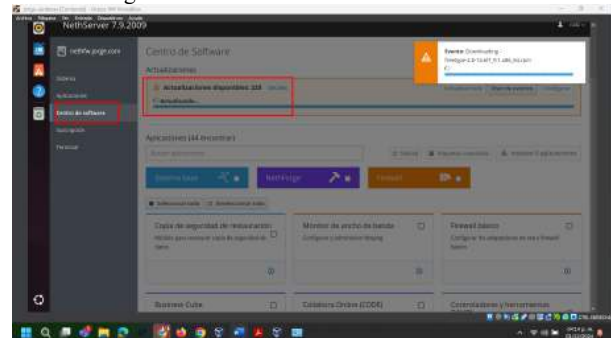
Figura 12. Acceso a la interfaz de administración de nethserver desde Ubuntu Desktop



Fuente: Autoría Propia

Se accede al Centro de Software y se realizan las 225 actualizaciones pendientes.

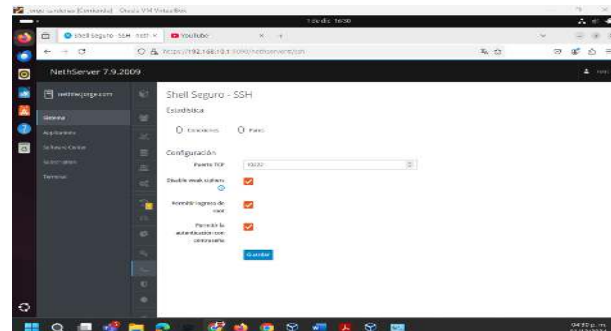
Figura 13. Actualización en centro de software



Fuente: Autoría Propia

Se configura el shell seguro (SSH), cambiando el puerto por defecto 22 a 10222. Aunque no es recomendable, se permite el acceso como usuario root por el momento.

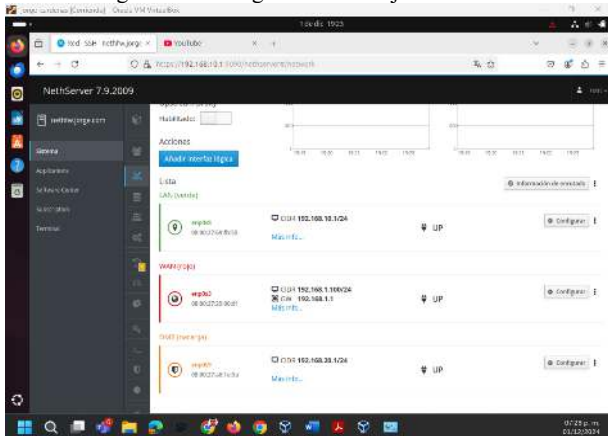
Figura 14. Configuración puerto y acceso root en SSH



Fuente: Autoría Propia

Se configuran las tarjetas de red en NethServer.
 enp0s8: Red LAN VERDE con IP 192.168.10.1/24.
 enp0s3: Red ROJA WAN con IP estática 192.168.1.100/24 y
 puerta de enlace 192.168.1.1.
 enp0s9: Zona Naranja DMZ con IP 192.168.20.1/24.
 Nota: Si no se asigna una IP estática a la zona ROJA, el
 sistema alerta sobre una configuración incorrecta.

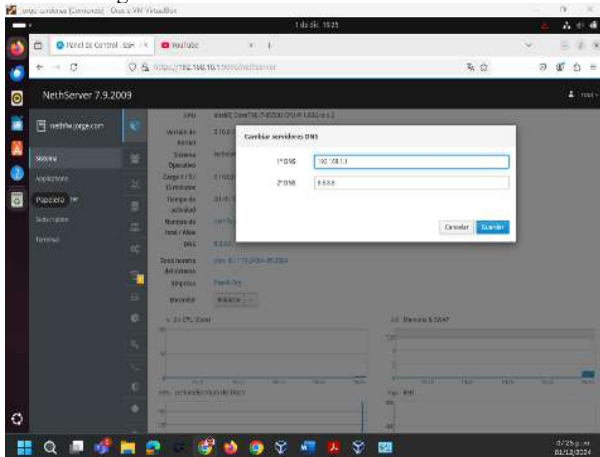
Figura 15. Configuración de tarjetas de red



Fuente: Autoría Propia

Se cambian los servidores DNS, configurando como principal la IP 192.168.1.1, correspondiente a la puerta de enlace del router en la red ROJA WAN.

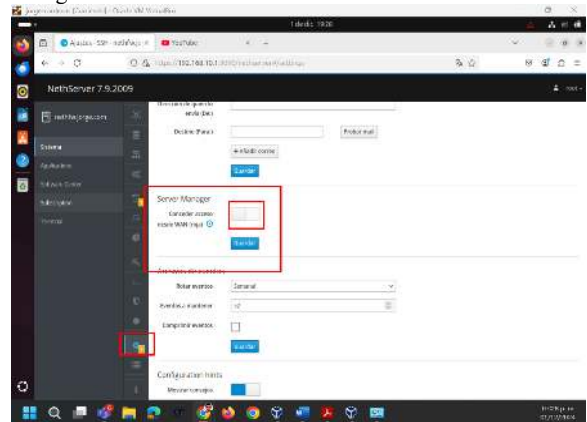
Figura 16. Cambio de servidores DNS



Fuente: Autoría Propia

Se accede al menú de Sistema, se selecciona la opción de ajustes y se deshabilita el acceso al Server Manager desde la red WAN ROJA, por razones de seguridad, para reducir el riesgo de ataques

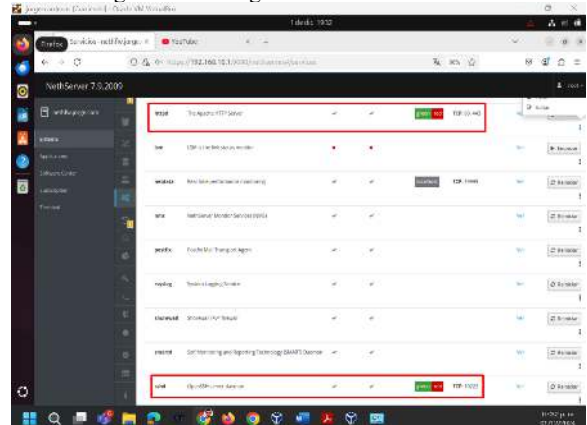
Figura 17. Desactivación del acceso al Server Manager desde la WAN ROJA



Fuente: Autoría Propia

Se verifican los servicios en ejecución. En la columna de acceso, se identifica que algunos servicios, como sshd y httpd, tienen acceso permitido desde la interfaz ROJA. Por lo que se retiran los permisos

Figura 18. Configuración de acceso en servicios



Fuente: Autoría Propia

3 DESARROLLO TEMATICA

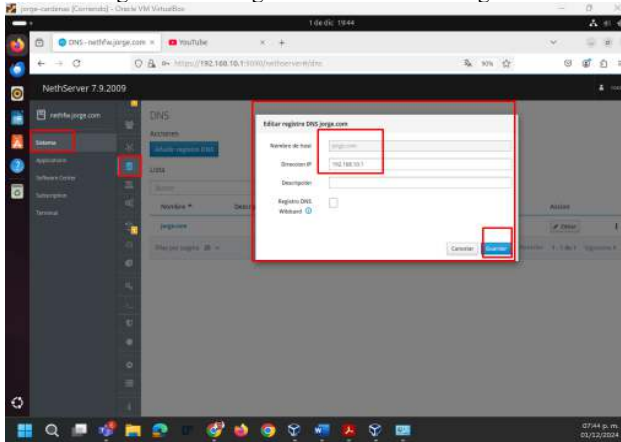
3.1 Temática 1: DHCP Server, DNS Server y Controlador de Dominio.

El producto esperado consiste en la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como el registro de dicha estación en los servicios de Infraestructura IT de nethserver.

3.1.1 Configuración DNS server

Se accede al menú Sistema, se selecciona la opción DNS y se agrega un nuevo registro DNS con el nombre de host jorge.com y la IP 192.168.10.1, correspondiente a la interfaz LAN VERDE. Finalmente, se guarda el registro, permitiendo que los dispositivos de la red interna resuelvan jorge.com a la IP configurada, facilitando la conexión interna al servidor.

Figura 19. Configuración de un nuevo registro DNS

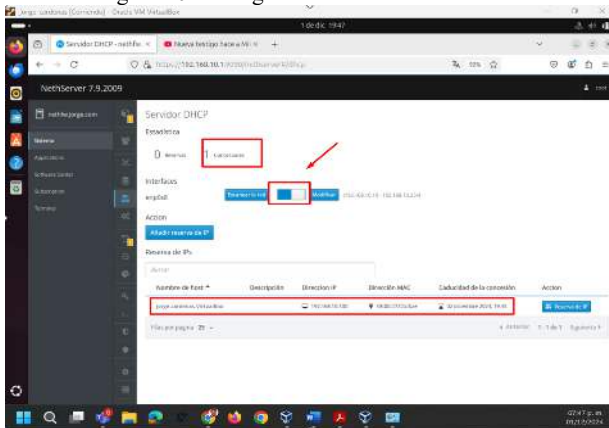


Fuente: Autoría Propia

3.1.2 Configuración Servidor DHCP

Se accede al menú Sistema, se selecciona la opción Servidor DHCP y se activa la casilla Escanear red. Luego, se configura el rango de IPs de 192.168.10.10 a 192.168.10.254, se especifica el dominio como jorge.com y se guardan los cambios. Después de aplicar la configuración, se verifica que el equipo Ubuntu Desktop recibe la IP 192.168.10.100 asignada por el servidor DHCP.

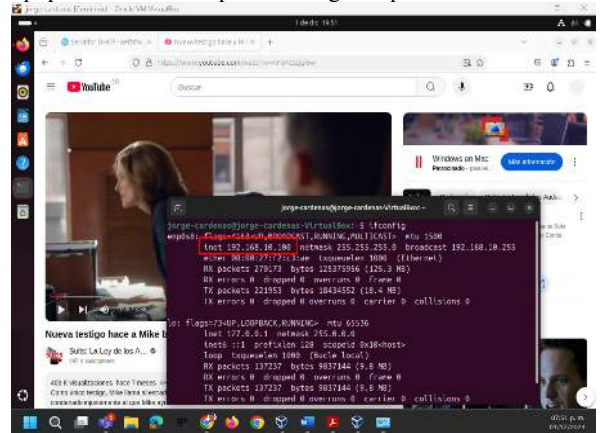
Figura 20. Configuración del Servidor DHCP



Fuente: Autoría Propia

Se verifica que el equipo Ubuntu Desktop, con la IP 192.168.10.100 asignada por DHCP, tenga acceso a la navegación web. Al confirmar que la conexión a Internet funciona correctamente, se asegura que la configuración de red y el servidor DHCP están operando adecuadamente.

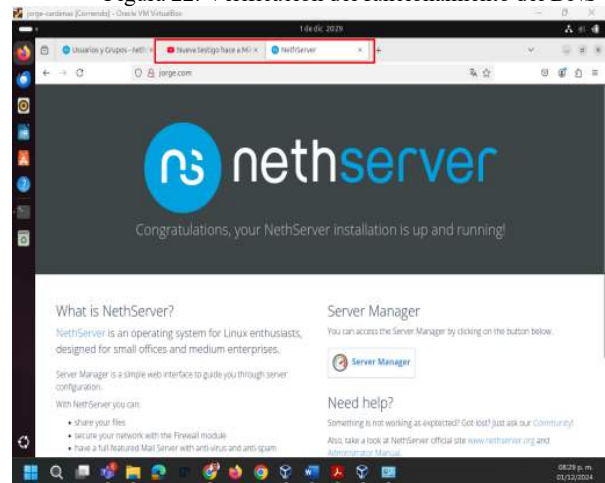
Figura 21. Verificación de acceso a Internet en el equipo Ubuntu Desktop con IP asignada por DHCP.



Fuente: Autoría Propia

Finalmente, se verifica que el DNS jorge.com funcione correctamente accediendo a esta dirección a través del navegador. Al cargar la página de NethServer, se confirma que la configuración del DNS fue exitosa.

Figura 22. Verificación del funcionamiento del DNS

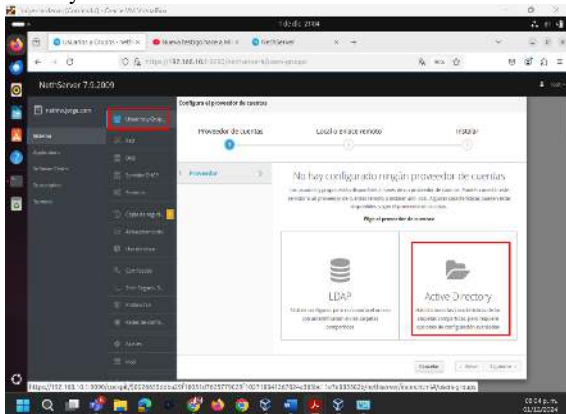


Fuente: Autoría Propia

3.1.3 Controlador de Dominio.

Se accede al menú Sistema, se selecciona la opción Usuarios y Grupos, y luego se elige Active Directory para iniciar la configuración del controlador de dominio.

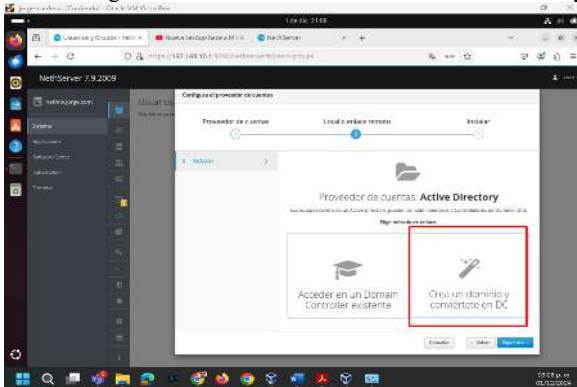
Figura 23. Acceso a la configuración de Active Directory



Fuente: Autoría Propia

Al acceder a la opción Active Directory, se selecciona Crear un dominio y conviértete en (DC). Esta configuración permite gestionar de manera centralizada usuarios, grupos y políticas de seguridad dentro de la red.

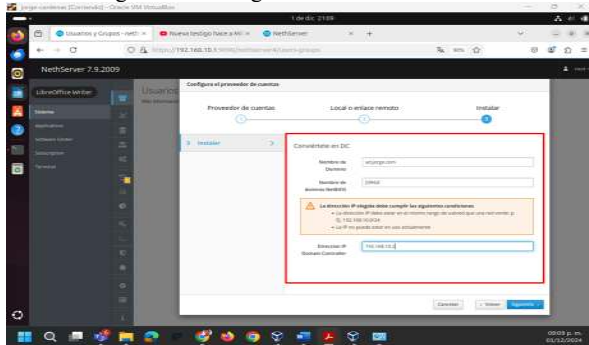
Figura 24. Creación del dominio en Active Directory



Fuente: Autoría Propia

Se configura el nombre del dominio como ad.jorge.com y el nombre NetBIOS como JORGE. También se asigna la dirección IP del Controlador de Dominio como 192.168.10.2, dentro del mismo rango de la subred VERDE.

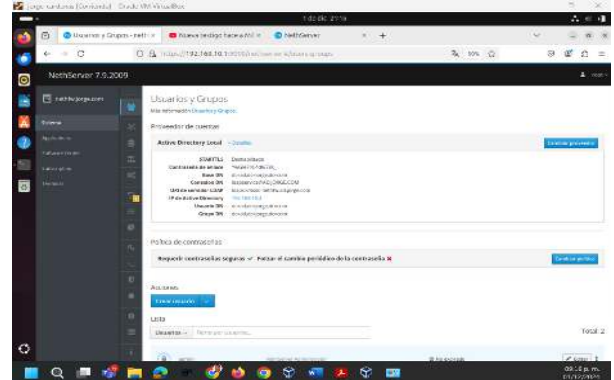
Figura 25. Configuración del dominio AD



Fuente: Autoría Propia

Una vez instalado, aparece el menú de descripción del Controlador de Dominio, que incluye opciones para la creación de usuarios, grupos y la configuración de políticas de contraseñas.

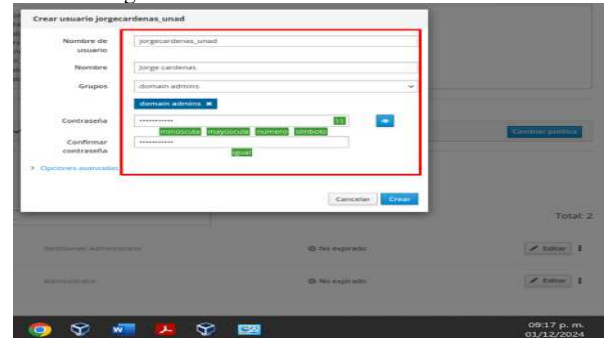
Figura 26. Menú del Controlador de Dominio



Fuente: Autoría Propia

Se procede a crear un usuario de dominio, completando los campos de nombre de usuario, nombre, grupos y contraseña. Se recomienda que la contraseña incluya minúsculas, mayúsculas, números y símbolos para garantizar su seguridad.

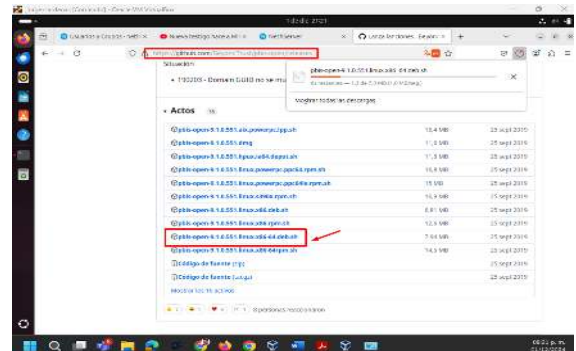
Figura 27. Creación de un usuario de dominio



Fuente: Autoría Propia

Se procede a afiliarse al equipo cliente al dominio. En el equipo Ubuntu, se inicia el proceso descargando el archivo pbis-open-9.1.0.551.linux.x86_64.deb.sh.

Figura 28. Descarga del archivo de afiliación al dominio



Fuente: Autoría Propia

Una vez descargado el archivo, se cambian los permisos del programa utilizando el comando sudo chmod 777.

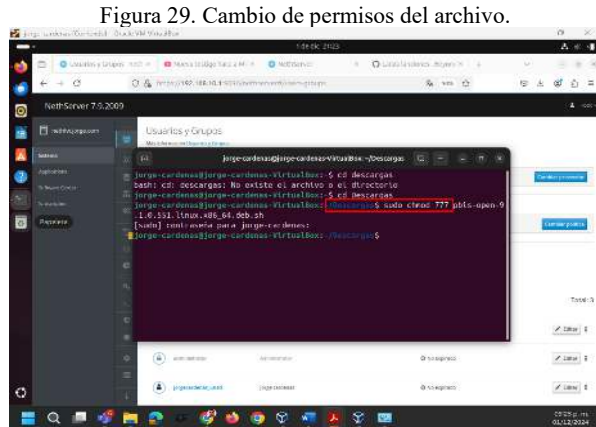


Figura 29. Cambio de permisos del archivo.

Fuente: Autoría Propia

Se ejecuta el instalador con el comando sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh, iniciando el proceso de instalación.

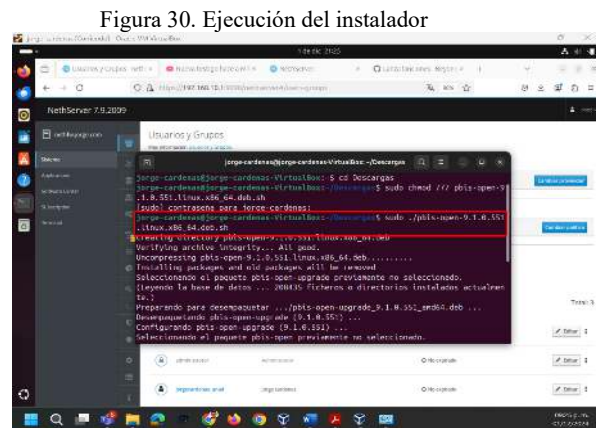


Figura 30. Ejecución del instalador

Fuente: Autoría Propia

Cuando el programa pbis-open finaliza, muestra un ejemplo de cómo realizar la afiliación al dominio.

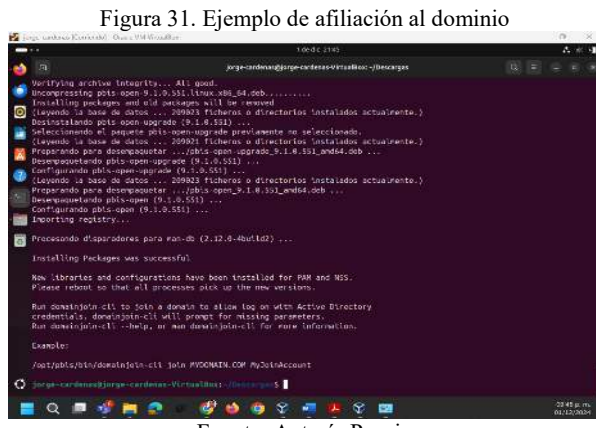


Figura 31. Ejemplo de afiliación al dominio

Fuente: Autoría Propia

Antes de unir el equipo Ubuntu al dominio, es importante instalar el servidor SSH utilizando el comando sudo apt-get install ssh.



Figura 32. Instalación del servidor SSH

Fuente: Autoría Propia

Otro ajuste necesario es configurar la red en VirtualBox para nethserver. En el apartado de red, se debe habilitar el modo promiscuo "Permitir todo" en la red verde para que los clientes puedan ver el controlador de dominio.



Figura 33. Configuración de red en VirtualBox

Fuente: Autoría Propia

Se procede a unir el equipo al dominio utilizando el comando sudo domainjoin-cli join ad.jorge.com jorgecardenas_unad. Se solicitará la contraseña creada para este usuario en el portal de usuarios de nethserver. Después de validar el registro en el dominio, es necesario reiniciar el cliente para aplicar los cambios.

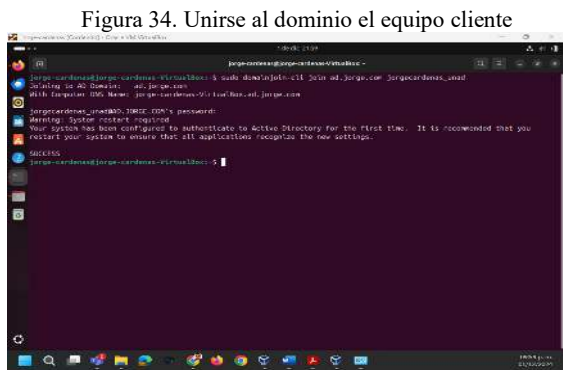
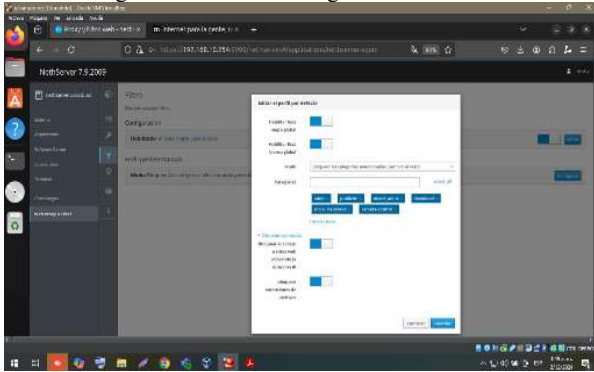


Figura 34. Unirse al dominio el equipo cliente

Fuente: Autoría Propia

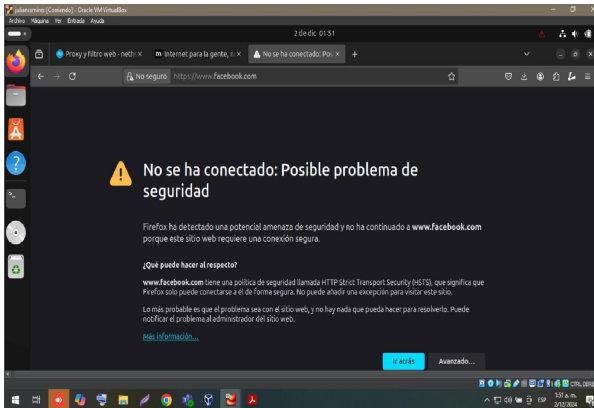
Figura 40. Filtro de categorías



Fuente: Autoría Propia

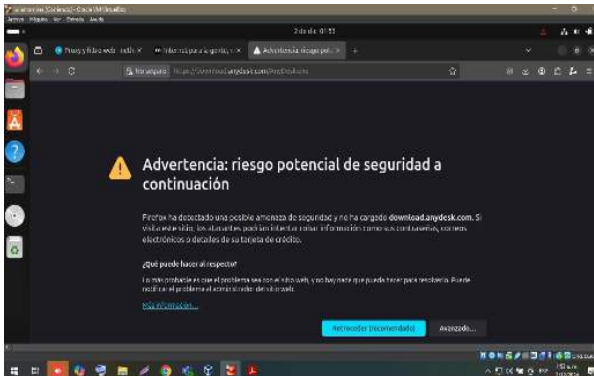
Se realizan pruebas de filtrado y bloqueo de páginas web, así como de descargas de extensiones no permitidas.

Figura 41. No permite la navegación hacia páginas de redes sociales como facebook



Fuente: Autoría Propia

Figura 42. No permite la descarga de archivos con extensión .exe



Fuente: Autoría Propia

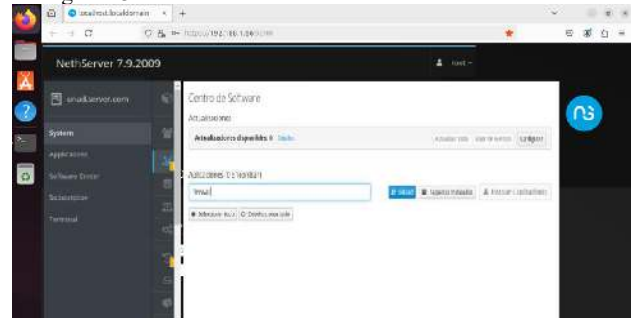
Con esto se finaliza la configuración y puesta en marcha del proxy web y filtro de contenido en netserver.

3.3 TEMATICA 3: CORTAFUEGOS

Consiste en la implementación y configuración de restricciones para bloquear sitios web de entretenimiento y redes sociales, con reglas y políticas aplicadas en el cortafuego, validando su funcionamiento desde una estación de trabajo GNU/Linux.

3.3.1 INSTALAR SERVICIOS DE FIREWALL

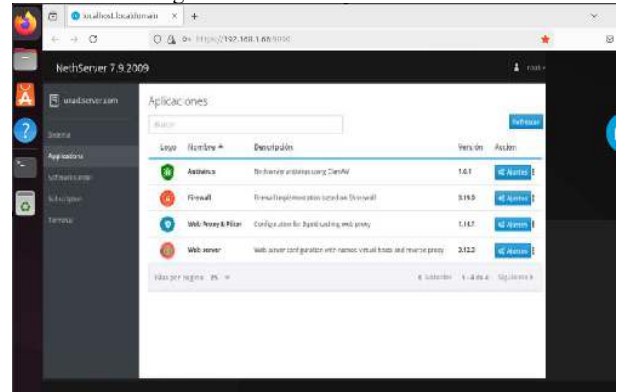
Figura 43. Se instalan los servicios de firewall



Fuente: Autoría Propia

Nos desplazamos hasta la pestaña de applications, y damos clic en ajustes para instalar y configurar nuestro firewall.

Figura 44. Instalación de firewall

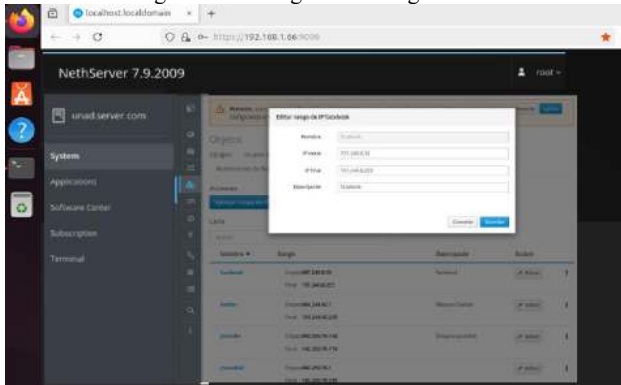


Fuente: Autoría Propia

3.3.2 CREACIÓN DE RANGOS IP EN FIREWALL

Para bloquear correctamente las páginas deseadas, es necesario introducir los rangos de las direcciones IP. De esta forma cuando se intente acceder a ellas, serán omitidas o rechazadas por el buscador.

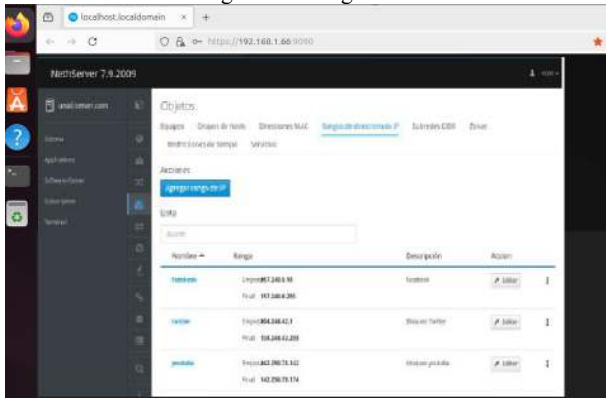
Figura 45. Configuración rangos IP



Fuente: Autoria Propia

Para realizar este proceso, debemos realizar la respectiva configuración. Para esto nos dirigimos a la pestaña objetos, y seleccionamos Rangos de direccionado IP. En este punto seleccionamos agregar rango de IP. Ingresamos el nombre de la página que se desea bloquear, la dirección IP inicial y la final, así como una descripción de esta. Este proceso lo realice para las 3 redes sociales, a continuación, mencionadas: YouTube, Facebook y Twitter.

Figura 46. Rangos IP

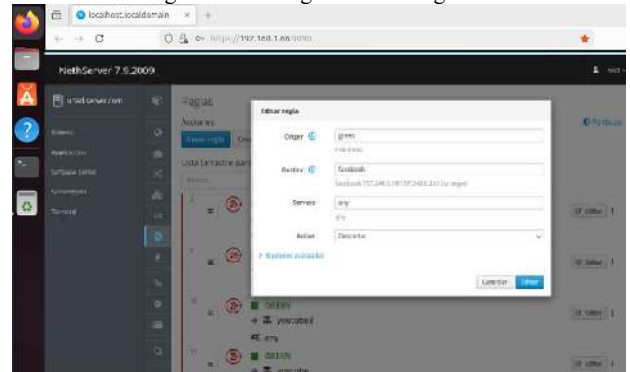


Fuente: Autoria Propia

3.3.3 CREACIÓN DE REGLAS FIREWALL

A continuación, nos dirigimos a la pestaña Reglas, y damos clic agregar regla. Aquí establecemos que el origen será de la red verde que al inicio de la instalación de Nethserver configuramos. Al realizar este paso, en el momento de buscarla o intentar llegar a alguna de las páginas bloqueadas, será de rechazo u omisión.

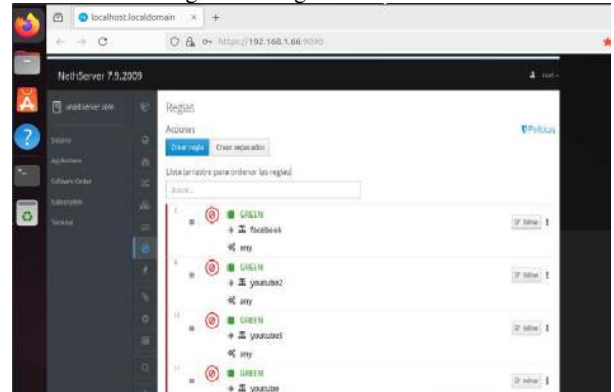
Figura 47. Configuración de reglas



Fuente: Autoria Propia

En la pestaña de Reglas, quedan establecidas las tres reglas de bloqueo del acceso de la red Verde a Facebook, YouTube y Twitter.

Figura 48. Reglas establecidas

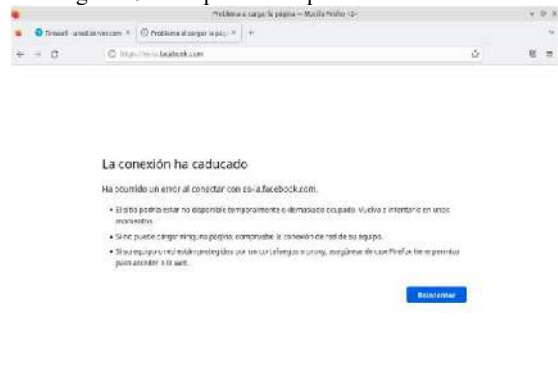


Fuente: Autoria Propia

3.3.4 DEMOSTRACION FINAL DE CONFIGURACION DEL FIREWALL

Ahora desde el servidor de Ubuntu Desktop, ingresamos la dirección de las páginas a consultar. El resultado en este caso es que tienen acceso denegado.

Figura 49. Comprobar bloqueo de direcciones IP



Fuente: Autoria Propia

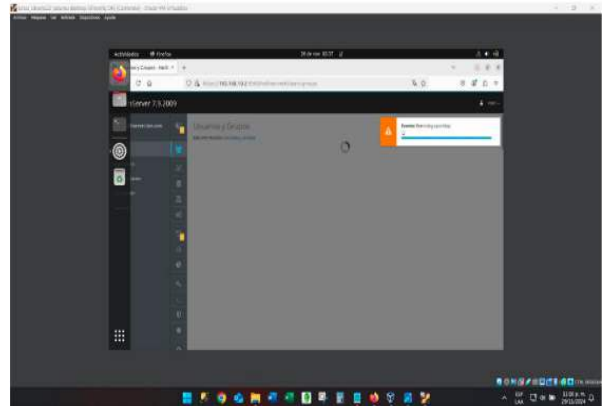
Para comprobar que la restricción es únicamente en las direcciones configuradas para ellos, ingresamos a otra página y cómo se observa, esta ingresa con normalidad a la página de Wikipedia, por lo que el firewall solo filtra el contenido especificado en las reglas.

Figura 50. Comprobando acceso a internet



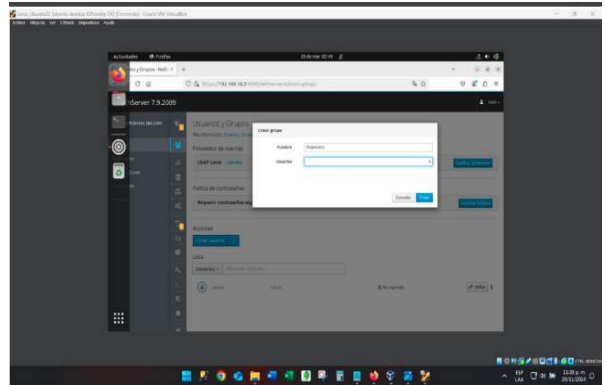
Fuente: Autoría Propia

Figura 52. Procedemos a instalar los servicios necesarios



Fuente: Autoría Propia

Figura 53. Creamos un grupo primero llamado financiero dentro del servicio LDAP

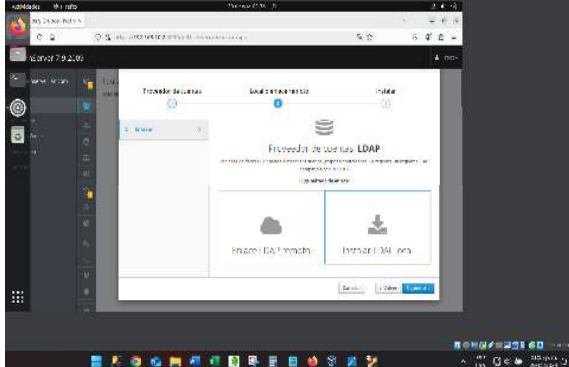


Fuente: Autoría Propia

3.4 TEMATICA 4: FILE SERVER Y PRINT SERVER

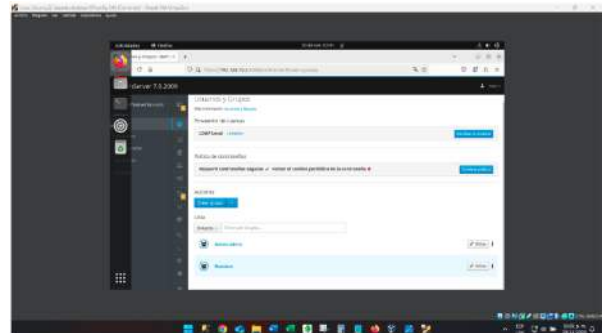
Consiste en la implementación y configuración del acceso de una estación de trabajo GNU/Linux a los servicios de carpetas compartidas e impresoras, utilizando un controlador de dominio LDAP.

Figura 51. Instalación opción remota local del servicio LDAP



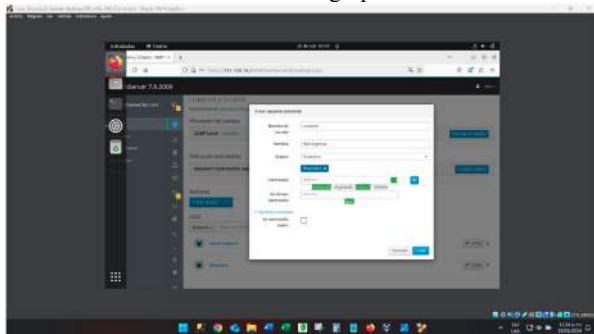
Fuente: Autoría Propia

Figura 54. Observamos que el grupo queda creado exitosamente



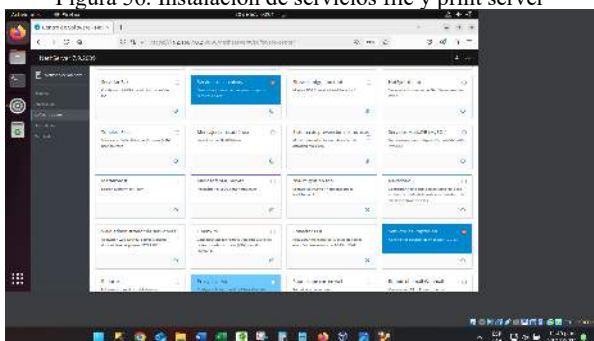
Fuente: Autoría Propia

Figura 55. Creamos luego un Usuario llamado asistente y lo vinculamos dentro del grupo financiero



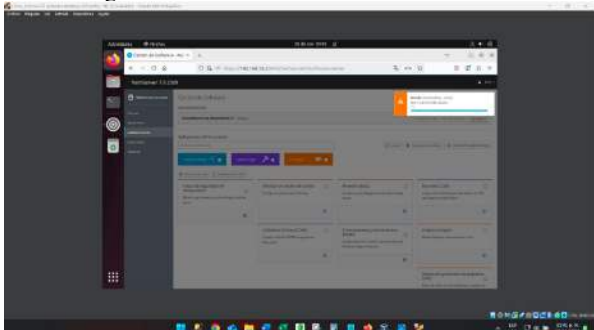
Fuente: Autoría Propia

Figura 56. Instalación de servicios file y print server



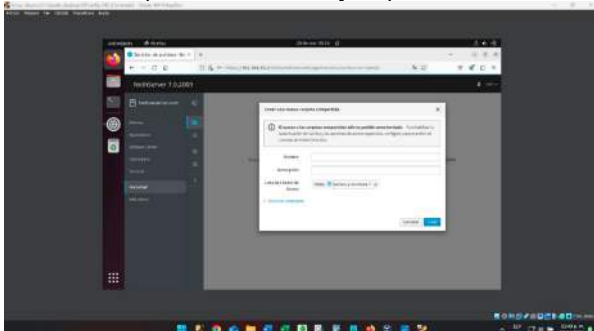
Fuente: Autoría Propia

Figura 57. Procedemos a instalar los servicios



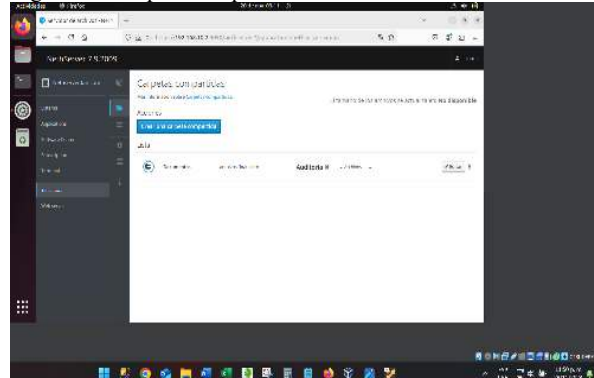
Fuente: Autoría Propia

Figura 58. En la opción File Server procedemos a crear una nueva carpeta compartida llamada Documentos, le damos los permisos necesarios y aceptamos



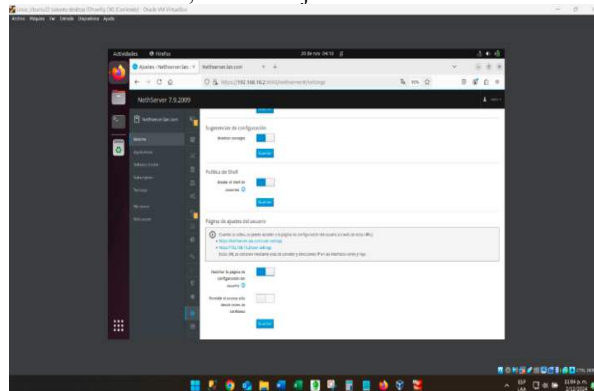
Fuente: Autoría Propia

Figura 59. Carpeta compartida "Documentos" creada con éxito



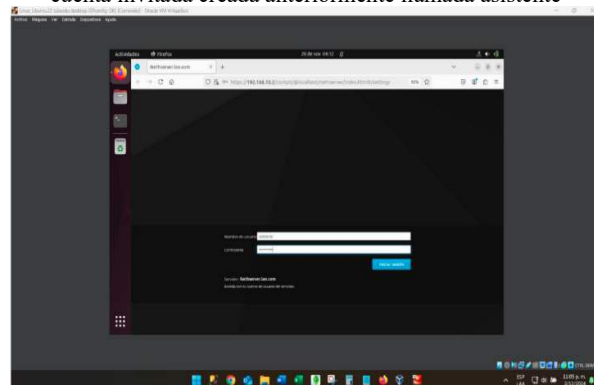
Fuente: Autoría Propia

Figura 60. Para el ingreso mediante URL a los usuarios invitados debemos habilitar la opción configuración del Usuario, desde los ajustes en Dashboard.



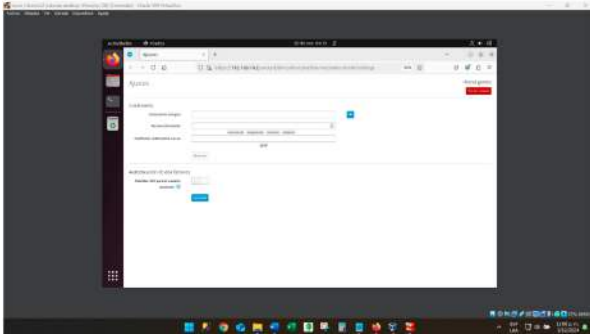
Fuente: Autoría Propia

Figura 61. Copiamos la URL y probamos el ingreso con la cuenta invitada creada anteriormente llamada asistente



Fuente: Autoría Propia

Figura 62. Nos pide cambio de contraseña en nuestro perfil para observar la carpeta compartida y la impresora



Fuente: Autoría Propia

3.5 TEMATICA 5: VPN

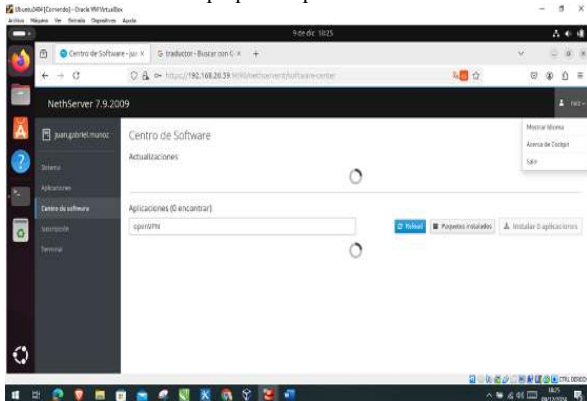
Consiste en la implementación y configuración de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux, evidenciando el acceso a contenido o aplicaciones de dicha estación.

3.5.1. Instalar el módulo de VPN

- Vamos a la sección Software Center desde el panel de administración.
- Buscamos e instalamos el módulo OpenVPN (RoadWarrior).

El módulo de VPN (OpenVPN) debe ser instalado a través del Software Center de NethServer. Este módulo habilita la funcionalidad de servidor VPN que permite a los dispositivos remotos conectarse de manera segura a la red interna.

Figura 63. Se accede al Centro de Software y se busca el paquete OpenVPN.



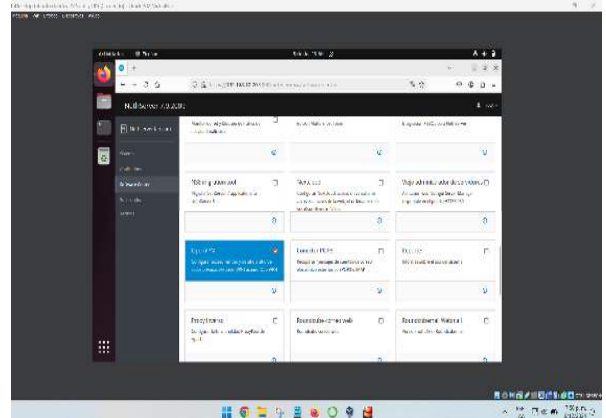
Fuente: Autoría Propia

El Software Center es la sección que permite visualizar todos los módulos adicionales disponibles para instalación en NethServer.

Se debe localizar el paquete denominado OpenVPN (RoadWarrior), un módulo diseñado específicamente para configurar un servidor VPN compatible con múltiples clientes.

Al finalizar la instalación, se debe acceder a la sección Red > VPN desde el menú lateral.

Figura 64. En la opción Software Center, se procede a instalar el servicio OpenVPN.

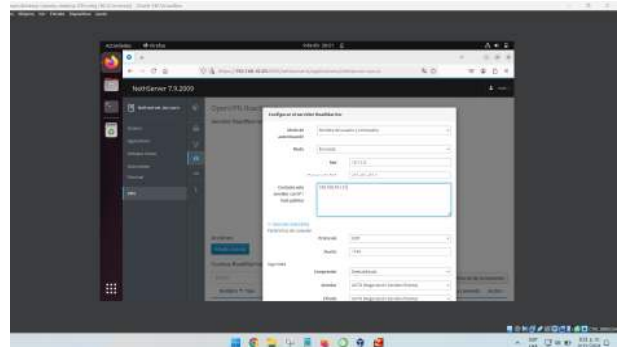


Fuente: Autoría Propia

Si la instalación se realiza correctamente, se habilitará una nueva pestaña denominada RoadWarrior o OpenVPN.

3.5.2. Configurar la VPN en NethServer

Figura 65. Configuramos el servidor RoadWarrior VPN con IP 10.1.1.0



Fuente: Autoría Propia

3.5.2. Crear una nueva configuración de OpenVPN

Para configurar una nueva instancia de OpenVPN, es necesario ajustar los siguientes parámetros básicos:

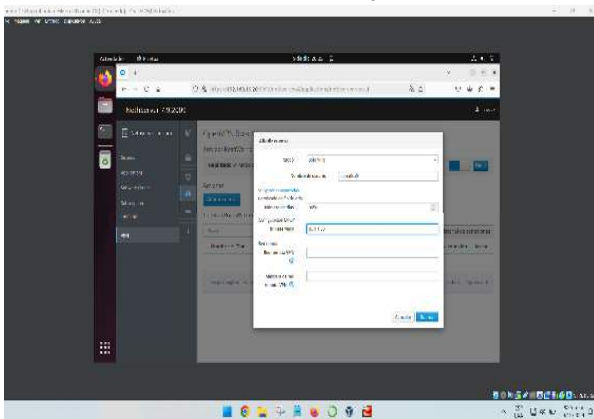
- Habilitar servidor VPN: Activado.

- Rango de direcciones VPN: Especifique una red virtual para -los clientes VPN, por ejemplo, 10.1.1.0.
- Protocolo: Seleccione UDP (recomendado por su eficiencia para VPN).
- Puerto: 1194 (puerto estándar de OpenVPN).
- Guardamos la configuración

3.5.3 Crear un usuario VPN

- Vamos a Cuentas > Usuarios y crea un usuario que se conectará al servidor VPN.
- Nos aseguramos de habilitar el acceso a VPN para este usuario.

Figura 66. Se añade una nueva cuenta de usuario VPN con el nombre tematica5.

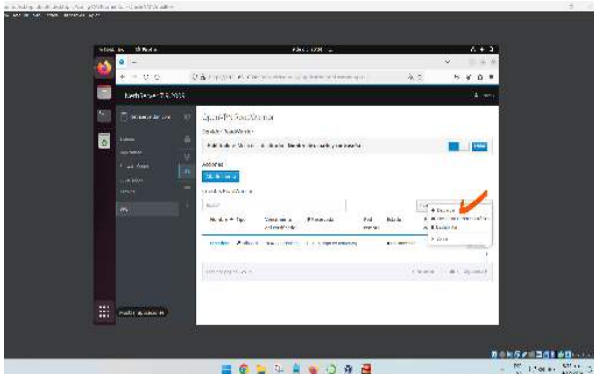


Fuente: Autoría Propia

Descargar el perfil de configuración del cliente.

- Seleccionamos el usuario creado y hacemos clic en Descargar perfil. Esto generará un archivo .ovpn que contiene la configuración necesaria para el cliente OpenVPN.

Figura 67. Se descarga la configuración o el certificado VPN creado.



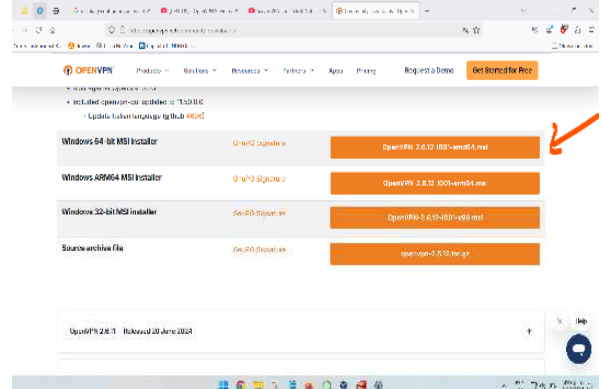
Fuente: Autoría Propia

3.5.4. Configurar la estación de trabajo GNU/Linux

Instalar OpenVPN en la estación de trabajo

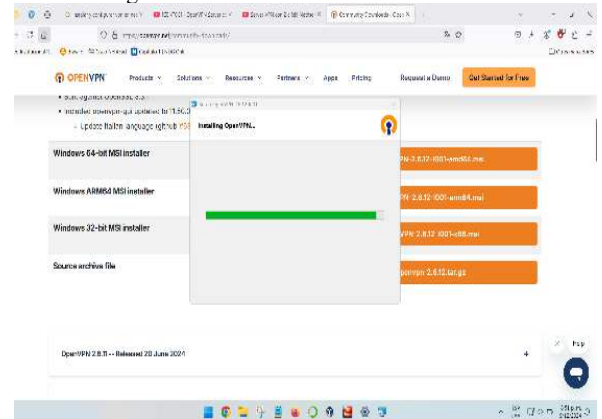
Para configurar la estación de trabajo GNU/Linux, es necesario instalar el cliente OpenVPN.

Figura 68. Se descarga el aplicativo VPN para la conexión desde cualquier equipo.



Fuente: Autoría Propia

Figura 69. Proceso de instalación en curso



Fuente: Autoría Propia

Figura 70 Desde la app OpenVPN abrimos el archivo descargado llamado tematica5.ovpn para la conexión.



Fuente: Autoría Propia

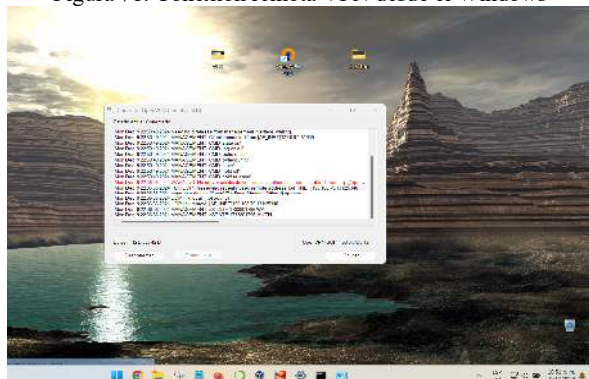
- Se debe iniciar el cliente OpenVPN utilizando el perfil de configuración previamente copiado (.ovpn).

- Es necesario verificar que la conexión se haya establecido correctamente revisando los registros (logs) del cliente para identificar posibles errores.

En la estación de trabajo:

- Se debe comprobar la creación de la nueva interfaz de red generada por OpenVPN, generalmente denominada tun0.
- También se debe confirmar el acceso a la red interna de NethServer desde la estación de trabajo.

Figura 71. Conexión remota VPN desde el Windows



Fuente: Autoría Propia

Una vez establecida la conexión VPN, se debe probar acceder a algún contenido alojado en la red interna de NethServer para verificar que la conexión es exitosa y se tiene acceso adecuado a los recursos compartidos.

Figura 72. Se realiza un ping a la IP de la VPN y se verifica una conexión exitosa.



Fuente: Autoría Propia

4 CONCLUSIONES

Temática 1: Durante la implementación de los servicios de DHCP, DNS y Controlador de Dominio en nethserver, pude observar cómo la centralización de la administración facilita la gestión de los recursos de red. La automatización en la asignación de direcciones IP mediante DHCP redujo considerablemente las tareas manuales, permitiendo que las estaciones de trabajo GNU/Linux se conecten de manera rápida y eficiente. Esto no solo mejoró la organización de la

red, sino que también optimizó el uso de los recursos disponibles. La configuración del Controlador de Dominio me permitió implementar un sistema de autenticación robusto, donde cada usuario debía identificarse mediante credenciales seguras. Esto fortaleció significativamente la seguridad de la red, asegurando que solo los usuarios autorizados tuvieran acceso.

Temática 2: El servidor proxy configurado permitió filtrar y controlar el acceso a Internet desde una estación GNU/Linux, cumpliendo los requisitos planteados para el control del tráfico de red.

Temática 3: Los cortafuegos en Linux sirven para proteger los dispositivos de red de usuarios externos, aplicaciones y archivos maliciosos. Su función principal es actuar como barrera de seguridad para evitar ciberataques y ataques de malware. Por otro lado, permite regular el tráfico de entrada y salida de la máquina, permitir o denegar conexiones de manera selectiva, determina los servicios a los que pueden acceder los usuarios remotos, evita que software malintencionado se extienda al equipo y por último evita que usuarios no autorizados accedan al equipo.

Temática 4: La implementación de Nethserver con servicios de File Server y Print Server demuestra ser una solución eficaz para la administración de recursos compartidos y periféricos en entornos de red. Su facilidad de configuración y flexibilidad garantizan una gestión centralizada, segura y accesible para los usuarios.

Temática 5: La implementación de NethServer como servidor VPN ofrece una solución robusta y flexible para garantizar comunicaciones seguras en entornos de red corporativos o domésticos. Su interfaz gráfica intuitiva y la compatibilidad con estándares como OpenVPN facilitan tanto la configuración inicial como la administración continua del servicio.

5 REFERENCIAS

- [1] NethServer. (2020, Noviembre 17). NethServer 7.9.2009 ISO release [Repositorio GitHub]. <https://github.com/NethServer/dev/releases/tag/iso-7.9.2009>
- [2] NethServer documentation (Version 7). NethServer Documentation. <https://docs.nethserver.org/en/v7/>
- [3] Oracle. (2020). Manual de usuario VirtualBox. VirtualBox. <https://www.virtualbox.org/manual/>
- [4] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>
- [5] Cabrera, M. (2021). "Nethserver Tutorial | Instalación, actualización y primeros pasos" Disponible en: https://www.youtube.com/watch?v=FNgmM-2fa_0
- [6] Free Software Foundation. (2016). Software libre y educación. El sistema operativo GNU. <http://www.gnu.org/education/education.html>