

NETHSERVER SIMPLIFICA LA ADMINISTRACIÓN DE SERVIDORES. GUÍA RÁPIDA PARA PRINCIPIANTES IMPLEMENTADA EN VIRTUALBOX.

Carlos Andrés Hormizda Mosquera
e-mail: cahormizdam@unadvirtual.edu.co
Ifreth de Jesús Ortiz Ortiz
e-mail: idortizo@unadvirtual.edu.co
Andrés Gómez Eslava
e-mail: agomez@unadvirtual.edu.co
José Ernesto Ruiz Neita
e-mail: jeruizn@unadvirtual.edu.co
Fabio Alonso Contreras Montes
e-mail: facontrerasm@unadvirtual.edu.co

RESUMEN:

Este artículo presenta una guía sencilla e ilustrada para instalar y configurar NethServer 7.9 e implementar algunos de los servicios que ofrece, todo ello desarrollado en VirtualBox. NethServer 7.9 permite la implementación de reglas específicas para diferentes interfaces de red (zonas o segmentos de red) facilitando su gestión al especificar políticas de acceso y restricciones para cada interfaz, esta guía se centrará en tres de las cuatro zonas posibles. Posterior a la instalación y configuración de NethServer, se abordará de manera eficiente la implementación de diversos servicios esenciales, un Servidor DHCP, un Servidor DNS, un Controlador de Dominio, un Proxy, un Cortafuegos (firewall), un Servidor de Archivos, un Servidor de Impresoras y un VPN. Finalmente, este documento se convierte en una solución práctica e integral para usuarios principiantes que buscan establecer un entorno de servidor versátil, facilitando la puesta en marcha de servicios clave en un sistema operativo GNU/Linux.

PALABRAS CLAVE: NethServer, Tutorial NethServer, Guía NethServer, NethServer VirtualBox.

1 INTRODUCCIÓN

En la era digital, la configuración eficiente de servidores es esencial para garantizar la estabilidad y seguridad de una red. En un mundo empresarial que demanda flexibilidad y seguridad, NethServer 7.9 emerge como una solución integral. Este recurso está diseñado para ser accesible y efectivo, proporcionando a los usuarios las herramientas necesarias para construir un entorno de servidor funcional. Descubra cómo aprovechar al máximo las capacidades de NethServer 7.9 en un entorno virtualizado.

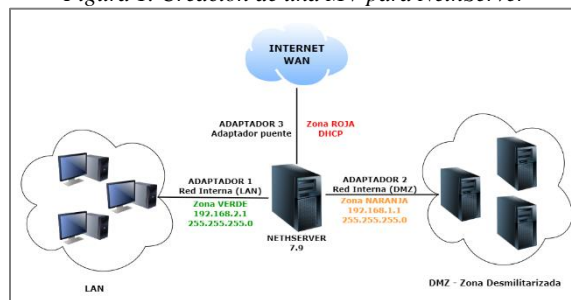
2 INSTALACIÓN NETHSERVER 7.9

Configurar e implementar GNU/Linux NethServer 7.9, implica el uso de al menos tres tarjetas de red en esta **Máquina Virtual (MV)**, una que se conectará con el grupo de servidores DMZ, otra a la red LAN y una última a la WAN (Internet). Los siguientes son los pasos que permitirán el desarrollo de esta configuración e implementación:

2.1 DEFINIR ZONAS

La zona es un segmento de red que permite organizar una red más extensa en partes más manejables y especializadas, de manera, que en cada zona se defina una estrategia para el intercambio de tráfico, sólo en ciertas direcciones, mejorando así la eficiencia, la seguridad y la administración de toda la red. Este ejercicio se desarrollará en las zonas ROJA, VERDE y AMARILLA, es decir, en tres de las cuatro zonas posibles (roja, verde, naranja y azul) que ofrece NethServer 7.9. La cuarta zona denominada AZUL corresponde a la zona de los invitados que usualmente se asigna a una red inalámbrica. Las siguientes son las zonas definidas para este ejercicio Fig. 1:

Figura 1. Creación de una MV para NethServer



Fuente: Elaboración propia (2023).

- Zona ROJA: Constituye todas las redes fuera del dispositivo NethServer, es decir, Internet (WAN).
- Zona VERDE: Corresponde a la red interna, es decir, la LAN. Está dedicada a las estaciones de trabajo y usualmente es la más protegida.
- Zona NARANJA: Corresponde a la red DMZ. Aquí se encuentran los servidores que requieren acceder a Internet para brindar servicios como, por ejemplo, HTTP, SVN y SMTP/POP.

2.2 IDENTIFICAR REQUISITOS MÍNIMOS

Los requisitos mínimos que debe tener la MV o el equipo de cómputo para instalar NethServer 7.9 son los siguientes [1]:

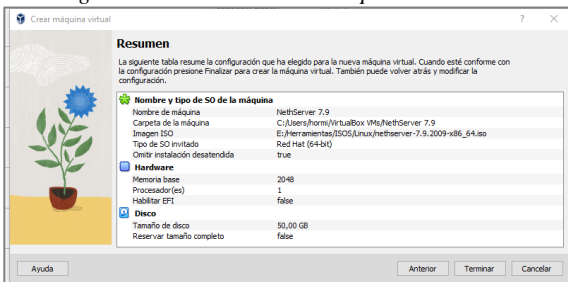
- Procesador (CPU) de 64 bits (x86_64).

- Memoria de 1 GB de RAM.
- Almacenamiento de 10 GB de espacio en disco.

2.3 CONFIGURAR UNA MV PARA NETHSERVER

Inicialmente descargamos la imagen ISO del sistema operativo NethServer en la página oficial [2] luego abrimos VirtualBox, le damos clic al botón “Nueva” y creamos una nueva MV, en la ventana emergente que aparece establecemos el nombre como “NethServer 7.9”, luego seleccionamos la imagen ISO descargada, en el “Tipo” escogemos “Linux”, en la “Versión” optamos por “Red Hat (64-bit)”, marcamos entonces la casilla de verificación “Omitir instalación desatendida” para realizarla de forma manual y oprimimos el botón “Siguiente”. En la ventana que aparece establecemos: Memoria base: 2048 MB (2 GB) y Procesador: 1. Posteriormente, determinaremos la creación del disco duro virtual con una capacidad dinámica de 50 GB. Finalmente, aparecerá una ventana con el resumen de las características establecidas anteriormente. Fig. 2, luego le damos clic al botón “Terminar”.

Figura 2. Creación de una MV para NethServer



Fuente: Elaboración propia (2023).

2.4 CONFIGURAR LAS INTERFACES DE RED DE LA MV NETHSERVER

En la MV NethServer debemos establecer y configurar las tres interfaces de red (tres adaptadores), una para cada zona:

- Zona VERDE: Vamos al botón “Configuración” y seleccionamos la opción “Red”. Posteriormente y estando en la primera pestaña denominada “Adaptador 1”, habilitamos el adaptador de red en la casilla de selección, y en la opción “Conectado a” escogemos la alternativa “Red Interna”, después en la sección “Nombre” escribimos el nombre de esta zona “Zona VERDE”, luego le damos clic al ícono de la flecha “Avanzado” y en “Modo promiscuo” seleccionamos “Permitir todo”, finalmente le damos clic al botón “Aceptar”.
- Zona NARANJA: Vamos al botón “Configuración” y seleccionamos la opción “Red”, posteriormente le damos clic a la segunda pestaña denominada “Adaptador 2”, habilitamos el adaptador de red en la casilla de selección, y en la opción “Conectado a” escogemos la alternativa “Red Interna”, después en la sección “Nombre” escribimos el nombre de esta zona “Zona NARANJA”, luego le damos clic al ícono de la flecha “Avanzado” y en “Modo promiscuo”

seleccionamos “Permitir todo”, finalmente le damos clic al botón “Aceptar”.

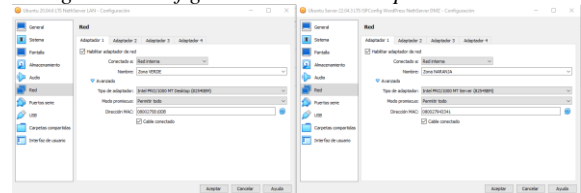
- Zona ROJA: Vamos al botón “Configuración” y seleccionamos la opción “Red”, posteriormente le damos clic a la tercera pestaña denominada “Adaptador 3”, habilitamos el adaptador de red en la casilla de selección, y en la opción “Conectado a” escogemos la alternativa “Adaptador puente”, luego le damos clic al ícono de la flecha “Avanzado” y en “Modo promiscuo” seleccionamos “Permitir todo”, finalmente le damos clic al botón “Aceptar”.

2.5 CONFIGURAR INTERFACES DE RED DE LAS MV DE LA RED LAN Y DE LA RED DMZ

Asignamos las interfaces de red establecidas con anterioridad a las MV de LAN y DMZ. Fig. 3:

- MV de la red LAN (Zona VERDE): Usaremos una MV denominada “Ubuntu 20.04.6 LTS NethServer LAN”. Ahora para establecer la zona de red que le corresponde nos dirigimos al botón “Configuración” y seleccionamos la opción “Red”, posteriormente le damos clic a la primera pestaña denominada “Adaptador 1”, habilitamos el adaptador de red en la casilla de selección, y en la opción “Conectado a” escogemos la alternativa “Red interna”, después en la sección “Nombre” seleccionamos el nombre de esta zona “Zona VERDE”, luego le damos clic al ícono de la flecha “Avanzado” y en “Modo promiscuo” seleccionamos “Permitir todo”, finalmente le damos clic al botón “Aceptar”.
- MV de la red DMZ (Zona NARANJA): Usaremos una MV denominada “Ubuntu Server 22.04.3 LTS ISPConfig WordPress NethServer DMZ”. Ahora para establecer la zona de red que le corresponde nos dirigimos al botón “Configuración” y seleccionamos la opción “Red”, posteriormente le damos clic a la primera pestaña denominada “Adaptador 1”, habilitamos el adaptador de red en la casilla de selección, y en la opción “Conectado a” escogemos la alternativa “Red interna”, después en la sección “Nombre” seleccionamos el nombre de esta zona “Zona NARANJA”, luego le damos clic al ícono de la flecha “Avanzado” y en “Modo promiscuo” seleccionamos “Permitir todo”, finalmente le damos clic al botón “Aceptar”.

Figura 3. Configuración de una MV para NethServer



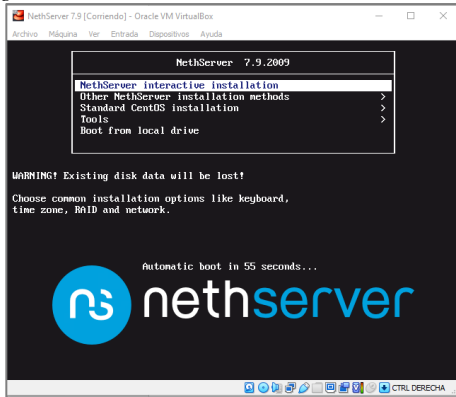
Fuente: Elaboración propia (2023).

2.6 INSTALAR NETHSERVER 7.9

Una vez descargado el archivo ISO, iniciamos la MV NethServer 7.9 para comenzar con la instalación. Pasados unos

segundos nos aparece una ventana emergente en la que debemos elegir alguna de las distintas opciones que se proponen. Aquí escogemos “NethServer interactive installation”. Fig. 4.

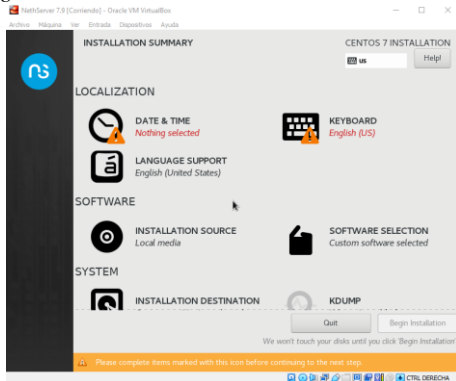
Figura 4. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Aparece una ventana emergente que nos presenta un par de alertas, así que debemos atenderlas para avanzar en la configuración. Fig. 5.

Figura 5. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Iniciamos con el módulo de la fecha y hora “Date & Time”, definimos la región y la ciudad Fig. 6, incluso tenemos la oportunidad de cambiar el formato de hora., es decir, pasar de 24 hora a 12 horas, luego le damos clic al botón “Done”.

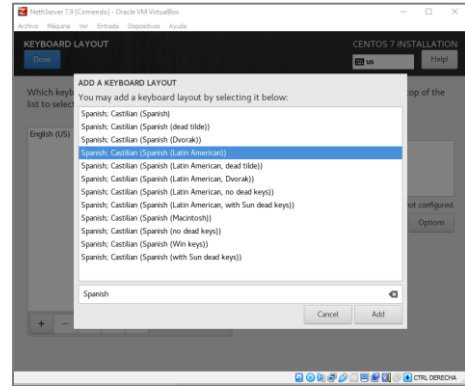
Figura 6. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Ajustamos el módulo que nos falta por configurar, teclado o “Keyboard”, le damos clic a esa opción Fig. 7 y finalmente le damos clic al botón “Add”.

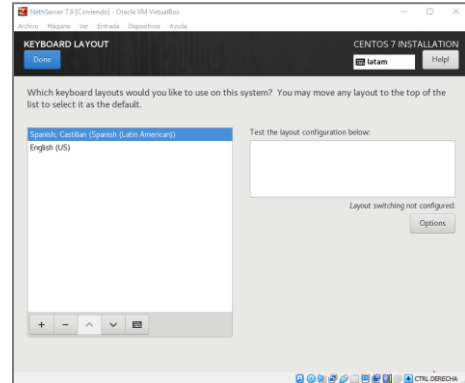
Figura 7. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Nos aparece una ventana en la que debemos definir la distribución del teclado. Fig. 8.

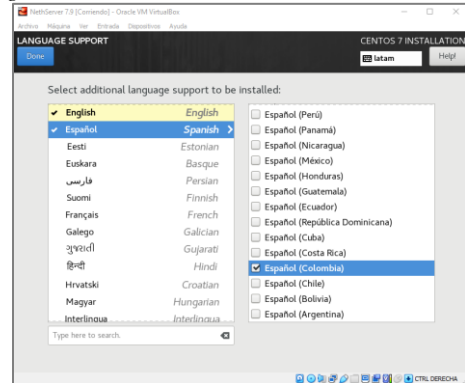
Figura 8. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Luego, determinamos el idioma de soporte y le damos clic al botón “Done”. Fig. 9.

Figura 9. Instalación de GNU/Linux NethServer 7.9.

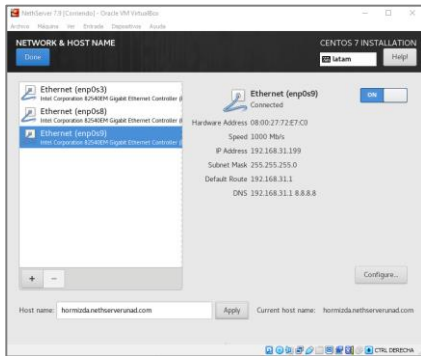


Fuente: Elaboración propia (2023).

Por último, escogemos la opción “Network & Hostname”. En esta ventana, encontramos un campo

denominado “Host name”, en este espacio podemos cambiar el nombre de la máquina (host) y del dominio, se establecerá así: hormizda.nethserverunad.com, luego le damos clic al botón “Apply” y después le damos clic al botón “Done” Fig. 10.

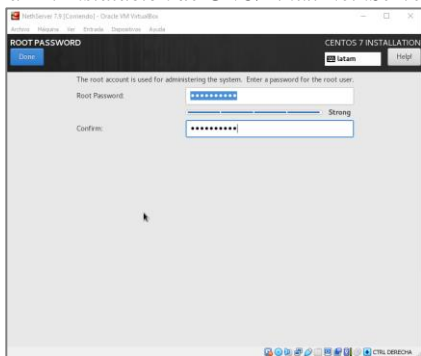
Figura 10. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Ahora, podemos comenzar con la instalación dándole clic al botón “Begin Installation”. Una vez hecho esto, aparecerá una ventana que nos solicita la contraseña del root, la escribimos y le damos clic al botón “Done”. Fig. 11.

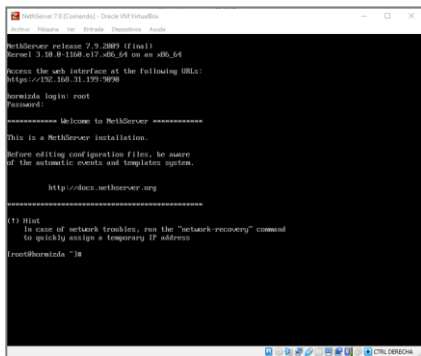
Figura 11. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Se completa la instalación y aparecerá la ventana de la terminal del NethServer, en la que se nos muestra la URL para el acceso a través de la interfaz web, en nuestro caso <https://192.168.31.100:9090>. Escribimos las credenciales de ingreso, en el “login” escribiremos root y en el “password” escribiremos la contraseña definida anteriormente Fig. 12.

Figura 12. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Realizamos la actualización con ayuda del comando: `yum update`. Reiniciamos la MV NethServer 7.9. En seguida, nos dirigimos a un navegador (Google Chrome) de la máquina anfitriona (Windows 10) y escribimos la URL <https://192.168.31.100:9090> para que finalmente nos dirija al panel de control de NethServer 7.9. Fig. 13.

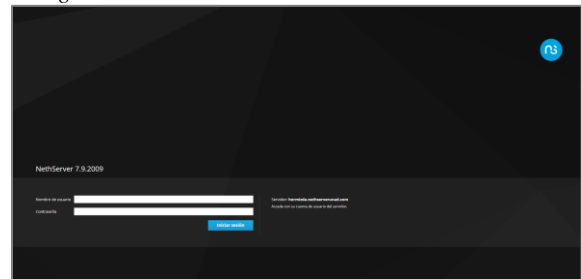
Figura 13. Instalación de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Aquí el navegador Google Chrome, por seguridad, nos indica que el certificado no es confiable, por ello, debemos ingresar dándole clic al botón “Configuración avanzada” y luego al enlace “Acceder a 192.168.31.100 (sitio no seguro)”. Aparecerá la pantalla inicial de NethServer 7.9. Fig. 14.

Figura 14. Instalación de GNU/Linux NethServer 7.9.

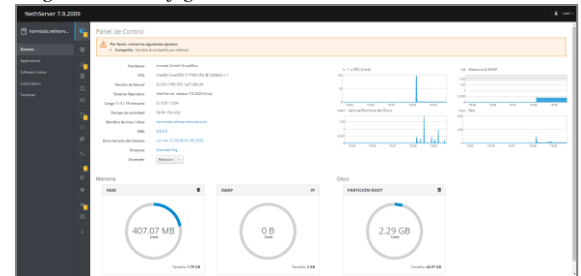


Fuente: Elaboración propia (2023).

3 CONFIGURACIÓN NETHSERVER 7.9

Escribimos las credenciales y le damos clic al botón “Iniciar sesión”. Aparecerá el panel de control indicándonos algunas alertas en pequeños recuadros con el número 1 que requieren atención. Fig. 15.

Figura 15. Configuración de GNU/Linux NethServer 7.9.

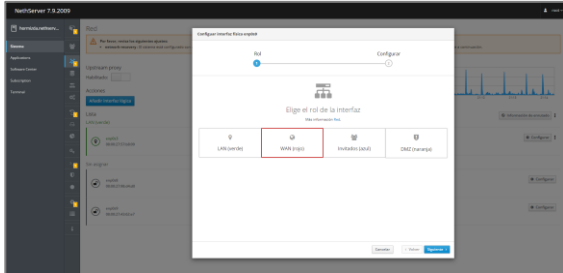


Fuente: Elaboración propia (2023).

Comenzamos con el primer módulo, el nombre de la empresa, para ello, en la ventana emergente se diligencian todos los datos solicitados. Ahora nos dirigimos a la sección “Red” del menú lateral izquierdo, Aparece configurada la IP de esta

MV en la zona VERDE, pero realmente debe corresponder a la zona ROJA por cuanto la MAC 0800274362E7 corresponde al NethServer, entonces debemos cambiar el rol de esta interfaz de LAN a WAN, para ello, le damos clic al botón “Configurar” en la franja de la interfaz enp0s9. Fig. 16, luego le damos clic al botón “Siguiente”.

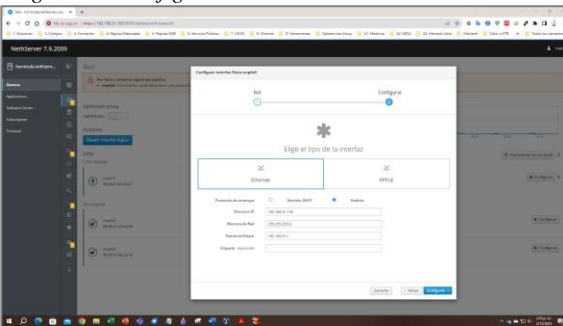
Figura 16. Configuración de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Establecemos la interfaz como “Ethernet”. En la misma ventana, escogemos el protocolo de arranque, “Estático” y le asignamos la dirección IP **192.168.31.100**, en la puerta de enlace escribiremos la IP **192.168.31.1**, luego le damos clic al botón “Configurar”. Fig. 17.

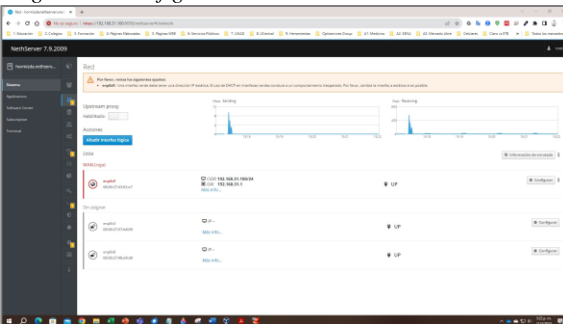
Figura 17. Configuración de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Aparecerá en la ventana un mensaje en la parte superior indicando que la interfaz verde debe tener una dirección IP estática, como se muestra en la Fig. 18. Aquí simplemente refrescaremos la página para que tome los cambios.

Figura 18. Configuración de GNU/Linux NethServer 7.9.

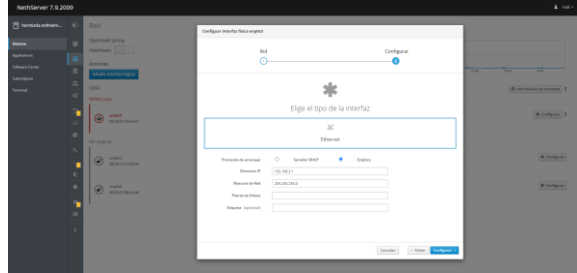


Fuente: Elaboración propia (2023).

Ubicaremos la franja de la interfaz de red identificada como enp0s3 con la MAC 08002757B809 que corresponde a la zona VERDE y le damos clic al botón “Configurar”, escogemos

el rol de la interfaz como “LAN” y le damos clic al botón “Siguiente”. Luego en el protocolo de arranque, le damos clic a la casilla “Estática” y escribiremos la siguiente información: Dirección IP: **192.168.2.1** y Mascara de red: **255.255.255.0**. El campo frente al título “Puerta de enlace” lo dejamos vacío. Fig. 19. Luego le damos clic al botón “Configurar”.

Figura 19. Configuración de GNU/Linux NethServer 7.9.

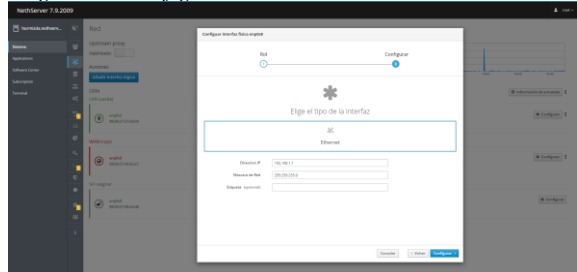


Fuente: Elaboración propia (2023).

Posteriormente, debemos asignar a la zona NARANJA la interfaz faltante que corresponde a enp0s8 con la MAC 08002798D4D0. Para ello le damos clic al botón “Configurar”, aparecerá una ventana en la que tenemos la posibilidad de escoger el rol de la interfaz, seleccionaremos “DMZ” y le damos clic al botón “Siguiente”.

Aparece una ventana en la que debemos escribir la dirección IP y la máscara de red que utilizará la zona DMZ (zona NARANJA), esta es la información: Dirección IP: 192.168.1.1 y Mascara de red: 255.255.255.0. Fig. 20.

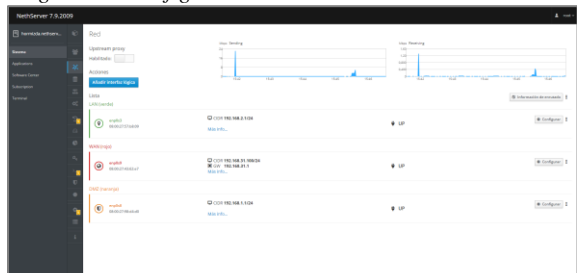
Figura 20. Configuración de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

Finalmente, le damos clic al botón “Configurar”. El servidor realizará los ajustes correspondientes y posiblemente se desconectará. Para volver al panel de control le damos clic al botón “Reconectarse” y aparecerá la información establecida. Fig. 21.

Figura 21. Configuración de GNU/Linux NethServer 7.9.



Fuente: Elaboración propia (2023).

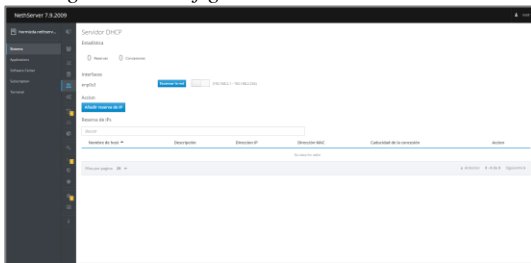
4 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Una vez instalado y configurado GNU/Linux NethServer 7.9 vamos a realizar la configuración del servidor DHCP, del servidor DNS y el Controlador de Dominio [3].

4.1 CONFIGURACIÓN DEL SERVIDOR DHCP.

La configuración de un servidor DHCP en NethServer 7.9 se realiza a través de la interfaz web de administración o panel de control. Estando allí, vamos a la sección “Servidor DHCP” del menú lateral izquierdo y le damos clic. Allí encontraremos la interfaz enp0s3 configurada anteriormente y que corresponde a la zona VERDE. Fig. 22.

Figura 22. Configuración del servidor DHCP.



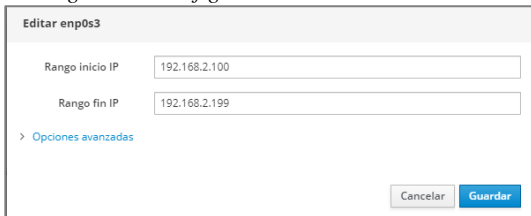
Fuente: Elaboración propia (2023).

Le damos clic al botón de encendido ubicado justo al lado del botón “Escanear la red”. Aparecerá una ventana emergente en la que estableceremos el siguiente rango:

Rango inicio IP: 192.168.2.100.
Rango fin IP: 192.168.2.199.

Esta asignación implica que el servidor DHCP entregará 100 direcciones IP dentro de este rango. Fig. 23.

Figura 23. Configuración del servidor DHCP.



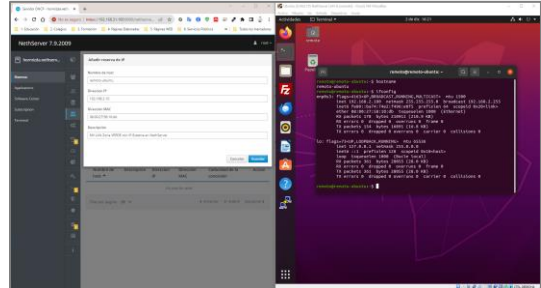
Fuente: Elaboración propia (2023).

Asignaremos adicionalmente, una dirección IP estática a la MV que corresponde a la red LAN (zona verde). Para ello, en el panel de control de NethServer 7.9, en el módulo “Servidor DHCP” nos dirigimos al botón denominado “Añadir reserva de IP” y le damos clic, diligenciamos varios campos. Fig. 24. Así que escribiremos la siguiente información:

- Nombre de host: remoto-ubuntu
- Dirección IP: 192.168.2.10
- Dirección MAC: 08:00:27:58:10:db
- Descripción: MV LAN Zona VERDE con IP Estática en NethServer

Finalmente, le damos clic al botón “Guardar”. Los datos de nombre del host y dirección MAC los podemos obtener al iniciar la MV, abrir una terminal (consola) y escribir los siguientes comandos `hostname` e `ifconfig` respectivamente. Fig. 24.

Figura 24. Configuración del servidor DHCP.



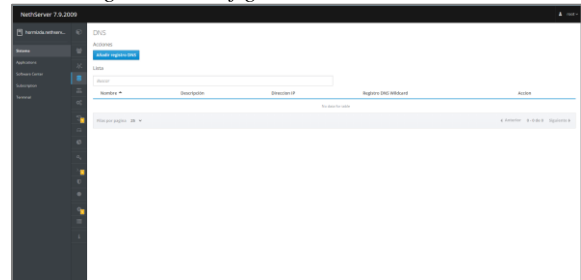
Fuente: Elaboración propia (2023).

Ahora se requiere reiniciar la interfaz de red en la MV Cliente de la red LAN o reiniciar el sistema para que el cambio surta efecto. Aquí usaremos el comando `sudo systemctl restart NetworkManager` para reiniciar la interfaz e inmediatamente, escribiremos el comando `ifconfig` para verificar el cambio

4.2 CONFIGURACIÓN DEL SERVIDOR DNS.

Configurar un servidor DNS en NethServer 7.9 se realiza a través de la interfaz web de administración o panel de control (dashboard), estando allí nos dirigimos a la sección denominada DNS en el menú lateral izquierdo y le damos clic. Fig. 25.

Figura 25. Configuración del servidor DNS.



Fuente: Elaboración propia (2023).

Una vez aquí agregaremos los registros DNS para la resolución de nombres de dominio y direcciones IP, entonces daremos clic al botón denominado “Añadir registro DNS”, aparecerá una ventana emergente en la que debemos diligenciar los datos que relacionan una dirección IP con un nombre de dominio y adicionalmente una descripción. De modo que, usaremos la dirección IP de la MV ubicada en la zona ROJA, es decir, la MV NethServer 7.9 precisamente donde está instalado NethServer, para que sea asociada al nombre de dominio www.nethserverhormizda.net, por ende, escribiremos la siguiente información en la ventana emergente. Fig. 26:

- Nombre de host: www.nethserverhormizda.net

- Dirección IP: 192.168.31.100
- Descripción: Máquina Virtual (MV) NethServer 7.9 ubicada en la zona ROJA

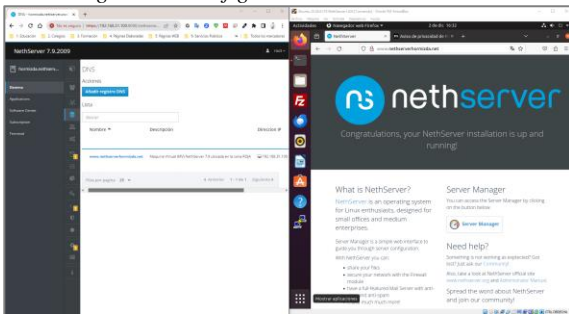
Finalmente le damos clic al botón “Guardar”.

Figura 26. Configuración del servidor DNS.

Fuente: Elaboración propia (2023).

Para verificar la reciente configuración iniciamos la MV Cliente de la red LAN ubicada en la zona VERDE, abrimos el navegador, instalado de forma predeterminada, “Mozilla Firefox” y escribimos en la barra de direcciones el nombre de dominio www.nethserverhormizda.net, inmediatamente nos dirigirá a la página web de inicio del GNU/Linux NethServer 7.9. Fig. 27.

Figura 27. Configuración del servidor DNS.



Fuente: Elaboración propia (2023).

4.3 IMPLEMENTACIÓN DEL CONTROLADOR DE DOMINIO

La implementación de un controlador de dominio en NethServer 7.9 se realiza a través del módulo “Usuarios y Grupo” del panel de control o administrador web. A continuación, se presentan las actividades para su desarrollo:

4.3.1 ELEGIR EL PROVEEDOR DE CUENTA

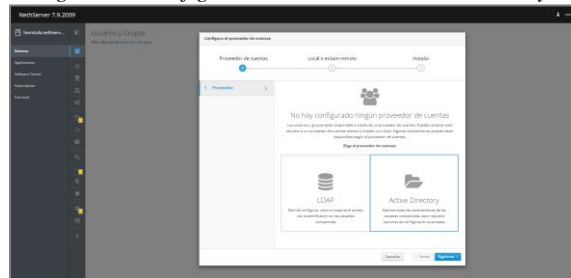
En virtud de las bondades que ofrece Samba Active Directory (Samba AD) será esta la elección del proveedor de cuenta para el controlador de dominio.

4.3.2 INSTALAR EL PROVEEDOR LOCAL ACTIVE DIRECTORY DE SAMBA

Para instalar y configurar el proveedor de cuentas locales Samba Active Directory, es necesario ir al módulo “Usuarios y

Grupos” y darle clic, aparecerá una ventana emergente en la que se debe escoger el proveedor de cuentas. Fig. 28.

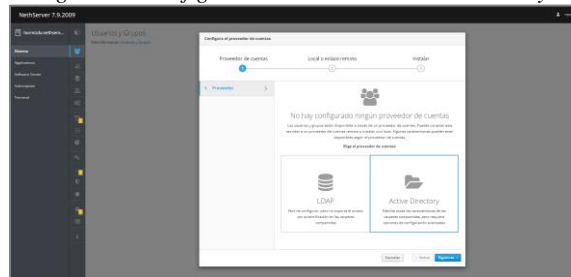
Figura 28. Configuración de Samba Active Directory.



Fuente: Elaboración propia (2023).

Aquí seleccionamos la opción Active Directory y le damos clic al botón “Siguiente”, aparecerá nueva información en la ventana emergente. En esta ventana se nos solicita seleccionar el método de enlace, debemos optar entre “Acceder en un controlador de dominio existente” o “Crear un dominio y convertirlo en Controlador de Dominio”, escogeremos la alternativa “Crear un dominio y convertirlo en Controlador de Dominio”. Fig. 29.

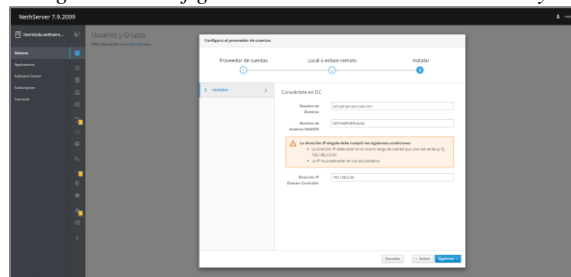
Figura 29. Configuración de Samba Active Directory.



Fuente: Elaboración propia (2023).

Aparecerá un formulario para diligenciar algunos campos relevantes: nombre de dominio, nombre de dominio NetBIOS y Dirección IP Domain Controller. Los dos primeros campos aparecerán definidos de forma predeterminada, aun cuando se pueden modificar, los dejaremos como aparece: Nombre de dominio: ad.nethserverunad.com, Nombre de dominio NetBIOS: NETHSERVERUNAD. En el tercer campo, “Dirección IP Domain Controller” debemos escribir una dirección IP estática que se encuentre en el mismo rango de la zona VERDE y por obvias razones la IP no puede estar en uso actualmente, así que diligenciaremos este campo con la dirección IP 192.168.2.20. Fig. 30.

Figura 30. Configuración de Samba Active Directory.

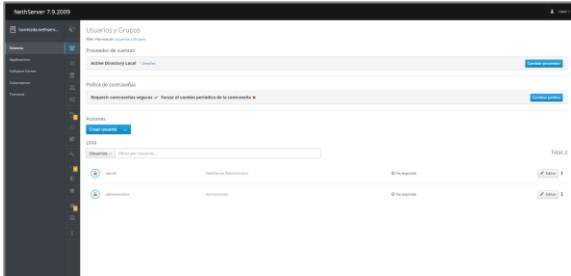


Fuente: Elaboración propia (2023).

Luego, le damos clic al botón “Siguiete”. Comenzará la instalación de Samba Active Directory que tomará algunos minutos.

Finalizada la instalación aparecerá una ventana en el panel de control titulada “Usuarios y Grupos”. Fig. 31.

Figura 31. Configuración de Samba Active Directory.



Fuente: Elaboración propia (2023).

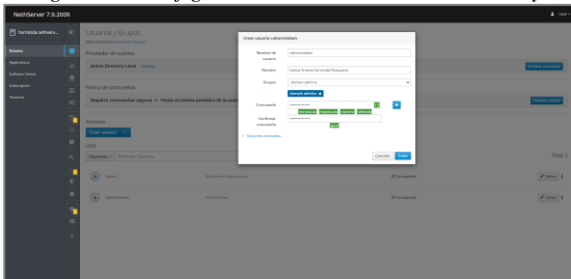
4.3.3 CREAR USUARIOS EN EL PROVEEDOR LOCAL ACTIVE DIRECTORY DE SAMBA

Estando en este módulo “Usuarios y grupos” le damos clic al botón “Crear usuario”, aparecerá una ventana emergente en la que debemos diligenciar algunos campos, la siguiente es la información que escribiremos Fig. 32:

- Nombre de usuario: cahormizdam
- Nombre: Carlos Andrés Hormizda Mosquera
- Grupos: domain admin
- Contraseña: NethServer2023!
- Confirmar contraseña: NethServer2023!
- Opciones avanzadas: No la marcamos.

Finalmente le damos clic al botón “Crear”.

Figura 32. Configuración de Samba Active Directory.



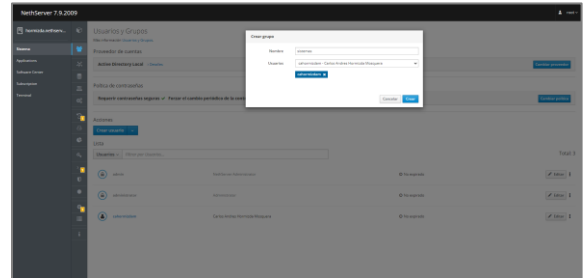
Fuente: Elaboración propia (2023).

Ahora crearemos un grupo denominado “sistemas”, para ello, le damos clic al botón con la flecha (justo al lado del botón “Crear usuario”) que despliega dos opciones: “Crear usuario” y “Crear grupo”, le damos clic a la opción “Crear grupo”, aparecerá una ventana emergente en la que debemos diligenciar únicamente dos campos. Así que crearemos un nuevo grupo con la siguiente información Fig. 33:

- Nombre: sistemas
- Usuarios: cahormizdam

Finalmente le damos clic al botón “Crear” y ya tenemos el primer grupo creado.

Figura 33. Configuración de Samba Active Directory.



Fuente: Elaboración propia (2023).

4.3.4 UNIR UN CLIENTE GNU/LINUX A ACTIVE DIRECTORY DE SAMBA

Iniciamos la MV Cliente de la red LAN, previamente configurada para acceder a la zona VERDE, luego abrimos la terminal (consola) y realizaremos algunas acciones con ayuda de varios comandos de línea en el siguiente orden:

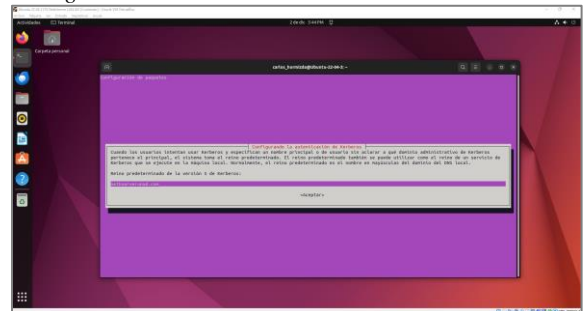
Verificamos la conexión con el recién creado servidor de dominio, tanto con la IP como con el nombre de dominio, así que escribimos primero el comando `ping -c5 192.168.2.20` para corroborar la conexión IP, ahora usamos el comando `ping -c5 ad.nethserverunad.com`, para comprobar que también hay resolución de nombres DNS.

Después escribimos el comando `sudo apt update` para actualizar la lista de paquetes disponibles en los repositorios configurados en el sistema. Usamos el comando `sudo apt upgrade` para actualizar los paquetes instalados en el sistema a sus versiones más recientes descargando las que están disponibles en los repositorios configurados.

Escribiremos el comando `sudo apt install realmd sssd sssd-tools ancle krb5-user packagekit` que realiza la instalación de varios paquetes relacionados con la integración de Linux en un entorno Active Directory (AD) y los servicios de red [4].

Se inicia la instalación y después de unos segundos aparecerá la autenticación. Esta se visualiza en una ventana que nos solicita el nombre de dominio con la frase “Reino predeterminado de la versión 5 de Kerberos”, allí escribiremos `nethserverunad.com` Fig. 34.

Figura 34. Unir un cliente GNU/Linux a Samba AD.



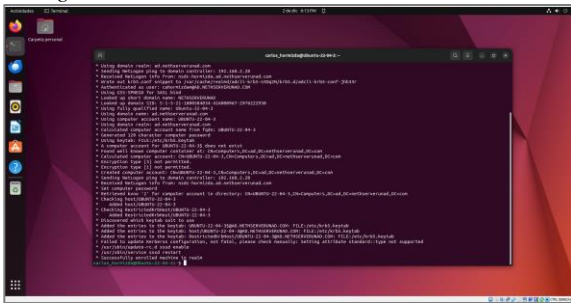
Fuente: Elaboración propia (2023).

Aparece otra ventana en la que debemos introducir los nombres de los servidores en el reino nethserverunad.com de Kerberos, separados por espacios. Aquí escribiremos el dominio completo **ad.nethserverunad.com** y oprimimos “Aceptar” usando el teclado.

Ahora se nos presenta otra ventana que nos solicita “Introducir el nombre del servidor administrativo (cambio de contraseña) para el reino nethserverunad.net de Kerberos”, aquí escribiremos el nombre de dominio nuevamente **ad.nethserverunad.com** y con ayuda del teclado oprimimos “Aceptar”. Se completará la instalación de los paquetes necesarios para unir la MV Cliente de la red LAN a Samba AD.

Posteriormente, se debe usar el comando: **sudo realm join ad.nethserverunad.com -U 'cahormizdam' -v** para unir la MV Cliente de la red LAN. Esta línea de comando se utiliza para unir un equipo GNU/Linux a un dominio Active Directory (AD) especificado. Una vez escribimos el comando nos aparece en la consola un mensaje que nos solicita la contraseña de este usuario, la escribimos: NethServer2023!. Se realizará la conexión con el Samba Active Directory Fig. 35.

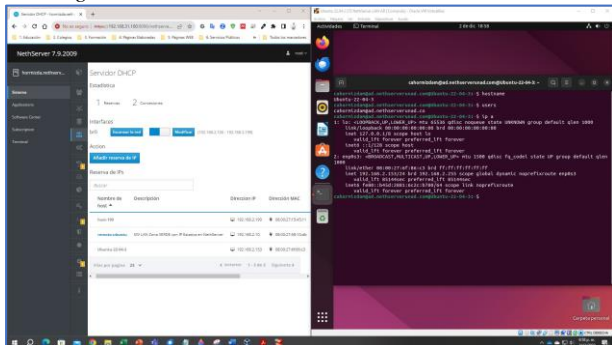
Figura 35. Unir un cliente GNU/Linux a Samba AD.



Fuente: Elaboración propia (2023).

Luego, configuramos PAM (Pluggable Authentication Modules) para que se cree la carpeta personal del usuario con ayuda del comando **sudo pam-auth-update --enable mkhomedir** Fig. 36. Esta línea de comando se utiliza para habilitar la creación automática del directorio de inicio del usuario si este no existe al iniciar sesión. Este directorio se crea con base en la configuración predeterminada del sistema.

Figura 36. Unir un cliente GNU/Linux a Samba AD.

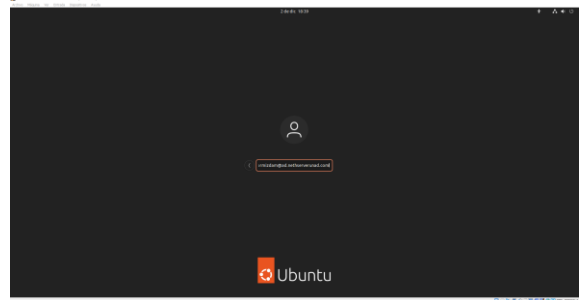


Fuente: Elaboración propia (2023).

Se debe reiniciar la MV Cliente de la red LAN para autenticarse como un usuario del directorio activo, aquí puede usar el comando **reboot** en la terminal. Una vez se inicie la MV cuando aparecen los campos de ingreso, le daremos clic a la opción “¿No está en la lista?”, aparecerán los espacios en donde se diligenciarán las credenciales de ingreso para acceder al Directorio Activo Samba Fig. 37. Estas son:

- Usuario: cahormizdam@ad.nethserverunad.com
- Contraseña: NethServer2023!

Figura 37. Unir un cliente GNU/Linux a Samba AD.

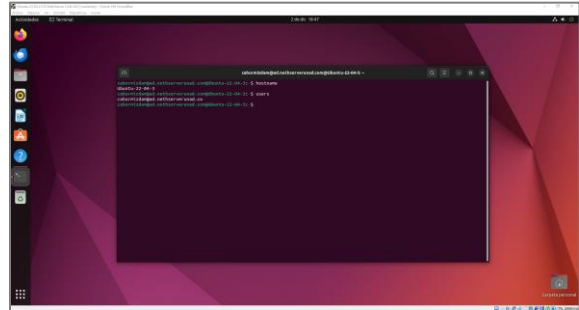


Fuente: Elaboración propia (2023).

Una vez ingresamos observaremos que se iniciará la “Configuración inicial” de la MV Cliente.

Verificaremos que nos encontramos en el Directorio Activo Samba al abrir la terminal y escribir el comando **hostname** y luego el comando **users** Fig. 38.

Figura 38. Unir un cliente GNU/Linux a Samba AD.



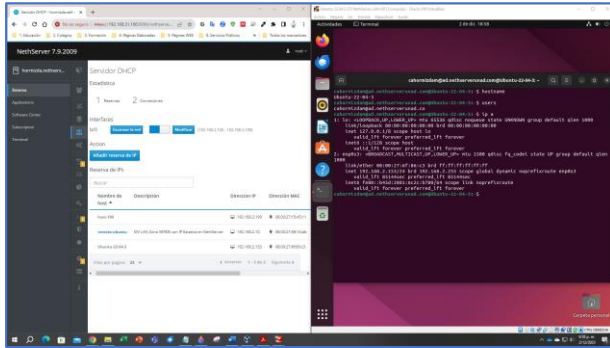
Fuente: Elaboración propia (2023).

4.3.5 EVIDENCIAR EL REGISTRO DE LA MV EN NETHSERVER 7.9

Para corroborar que la MV Cliente tiene un registro en GNU/Linux NethServer 7.9 nos dirigimos nuevamente al panel de control o administrador web de NethServer, estando allí le damos clic al módulo “Servidor DHCP” inmediatamente podemos observar el registro de la MV Cliente de la red LAN en uno de los registros, allí se encontrarán los siguientes datos propios de esta MV Fig. 39:

- Nombre de host: Ubuntu 22-04-3
- Dirección IP: 192.168.2.153
- Dirección MAC: 08:00:27:6f:86:c3
- Caducidad de la concesión: 03 diciembre 2023, 18:37
- Finalmente, la posibilidad de “Reserva de IP”.

Figura 39. Unir un cliente GNU/Linux a Samba AD.



Fuente: Elaboración propia (2023).

5 PROXY

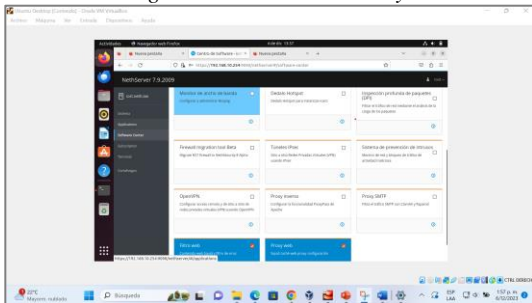
Un proxy, es un intermediario que actúa como un servidor intermedio entre un usuario y el destino al que se está accediendo. Funciona como una pasarela que facilita la comunicación entre sistemas, permitiendo que los clientes accedan a recursos en la web de manera indirecta, a través de este servidor. Concretamente en NethServer 7.9, el Proxy Web es un servidor que se encuentra entre las PCs de LAN y los sitios de Internet. Los clientes hacen peticiones al proxy que se comunica con sitios externos y luego envían la respuesta al cliente [5].

Este servidor tiene la capacidad de filtrar contenido y reducir el uso del ancho de banda mediante el almacenamiento en caché de las páginas que visita. Es importante tener en cuenta que en el proxy de NethServer 7.9 sólo se puede activar en zonas verdes y azules y que siempre está escuchando en el puerto **3128** [6].

5.1 INSTALACIÓN PROXY

El adecuado funcionamiento del Proxy requiere de la instalación de dos servicios, así que nos dirigimos al centro de aplicaciones y realizamos la descarga de uno denominado **servicio Proxy Web** (Configuración del proxy web de caché de Squid) y de otro denominado **Filtro Web** (Contenido web Squid y filtro de virus) Fig. 40.

Figura 40. Instalación Proxy.

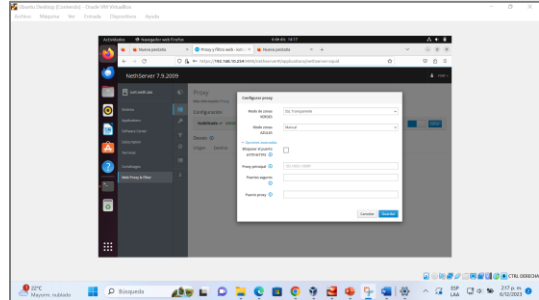


Fuente: Elaboración propia

5.2 CONFIGURACIÓN DEL PROXY WEB JUNTO Y DEL FILTRO WEB.

Una vez instalados debemos activar el servicio Proxy, así que nos vamos al módulo aplicaciones, y le damos clic al botón “Ajuste” de la aplicación “Web Proxy & Filter”, se abrirá la aplicación en el panel de control del proxy indicándonos que no está activo. Nos dirigimos entonces al módulo “Proxy” y le damos clic al botón “Configurar proxy”, aparecerá una ventana emergente en la que configuraremos únicamente el modo de zonas verdes en SSL Transparente para que todos los clientes estén obligados automáticamente a utilizar el proxy para las conexiones HTTP y HTTPS [6] Fig.41.

Figura 41. Configuración Proxy web.

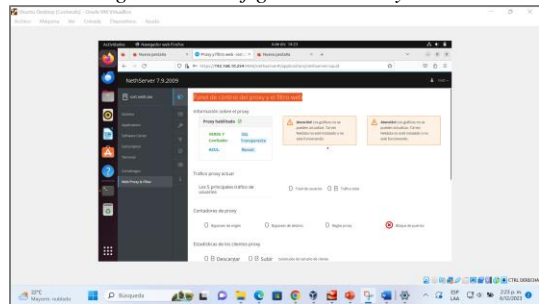


Fuente: Elaboración propia

5.3 AJUSTES EN EL PANEL DE CONTROL “PROXY Y FILTRO WEB”.

En el panel de control “Proxy y Filtro Web”, aparecen dos mensajes de alerta que indican la necesidad de realizar ajustes para mostrar los gráficos Fig. 42.

Figura 42. Configuración Proxy Web



Fuente: Elaboración propia

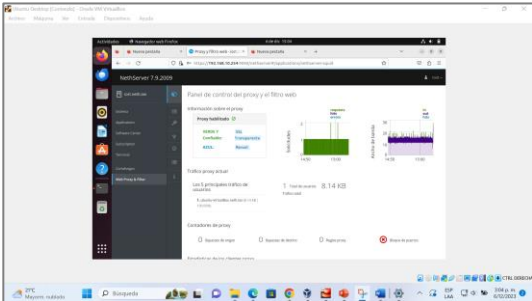
Así que nos vamos al módulo “Sistema”, luego al módulo “Servicios” y ubicamos “Netdata”, allí observamos que el sistema de monitoreo en tiempo real se está escuchando en localhost, entonces se requiere ajustar para que escuche en la red local (red LAN o zona VERDE), así que le damos clic a la opción de los “tres puntos”, luego escogemos “Editar”, aparecerá una ventana emergente en la que ajustamos el “Acceso” y seleccionamos “Green”

5.4 VERIFICACIÓN DE LAS REGLAS

Solucionadas las advertencias encontradas en el módulo “Panel de control del Proxy y el Filtro Web” se puede apreciar que las gráficas ya están funcionando, la primera gráfica

presenta las solicitudes HTTP y HTTPS y la segunda el ancho de banda Fig. 43.

Figura 43. Gráficas de las solicitudes y ancho de banda



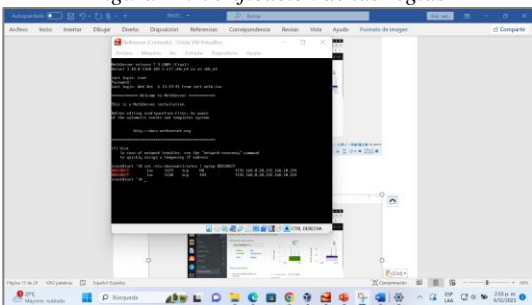
Fuente: Elaboración propia

Esto significa que al menos se encuentran dos reglas que están redireccionando las solicitudes HTTP y HTTPS hacia el Proxy. Para verificarlas nos vamos a la MV de NethServer, ingresamos las credenciales y escribimos el comando:

`cat /etc/shorewall/rules | egrep REDIRECT`

Este comando mostrará que las solicitudes hacia cualquier destino en internet de la red local denominada “loc”, usando los puertos 80 (HTTP) y 443 (HTTPS), se redireccionan mediante el protocolo TCP hacia los puertos 3129 y 3130, respectivamente, de la IP del NethServer Fig. 44.

Figura 44. Verificación de las reglas



Fuente: Elaboración propia

5.5 CONFIGURACIÓN DE LAS CATEGORÍAS PARA HABILITAR EL FILTRO WEB

Ahora se configurarán las categorías para establecer las restricciones, lo que implica el uso de un servicio denominado **ufdbGuard** que se puede encontrar en el módulo “Servicios”.

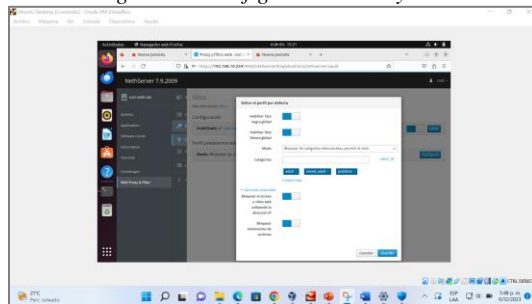
Para esta configuración nos dirigimos al módulo “Categorías” del “Panel de control del Proxy y el Filtro Web” y configuramos la lista de categorías libre de la Universidad de Toulouse que aparece de forma predeterminada, usando el botón “Configurar”, aparecerá una ventana emergente en la que se presentan las listas disponibles, entre ellas, alguna personalizada en la que se requerirá la URL de esa lista, sin embargo, se usará la lista de categorías predeterminada, oprimimos el botón “Guardar y descargar” y se iniciará la descarga e instalación de esta lista.

Luego nos vamos al módulo “Filtros” y lo activamos usando el botón “Editar las opciones globales”, se abrirá una ventana emergente en donde se podrá bloquear el acceso a sitios web usando extensiones, una lista negra o una lista blanca, para activar este filtro debemos diligenciar al menos un campo, así que escribiremos mp3 en el campo “Extensiones de archivo bloqueadas”.

Después, nos vamos a la opción “Perfil predeterminado” y le damos clic al botón “Configurar”, aparecerá una ventana emergente en la que tendremos la opción de habilitar o no las listas globales (negra y blanca), podremos gestionar el modo de bloqueo, para este ejercicio escogeremos “Bloquear las categorías seleccionadas, permitir el resto”.

Posteriormente seleccionamos las categorías por temas que se quieren bloquear, aquí seleccionamos algunas (adultos, mezcla adultos y publicidad), en “Opciones avanzadas” tendremos la posibilidad de “Bloquear el acceso a sitios web utilizando la dirección IP” y “Bloquear extensiones de archivos” Fig. 45.

Figura 45. Configuración Proxy web



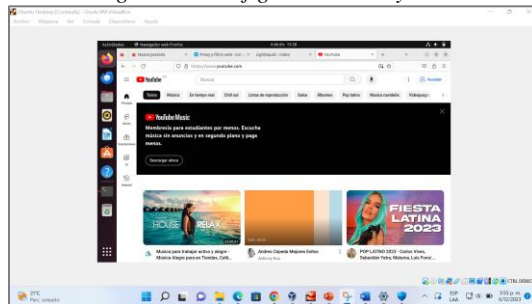
Fuente: Elaboración propia

En este punto es relevante indicar que el servidor Proxy tiene un uso considerable de recursos, particularmente de memoria RAM, por ello, se sugiere configurar la MV con suficiente memoria

5.6 VERIFICACIÓN DEL FILTRO WEB

Corroboramos las restricciones de publicidad ingresando a la página www.youtube.com, aquí podemos observar la no presencia de avisos publicitarios Fig. 46.

Figura 46. Configuración Proxy web

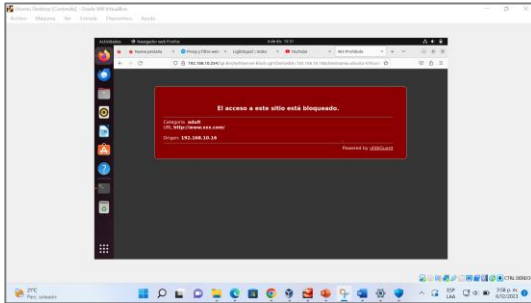


Fuente: Elaboración propia

Luego, intentaremos ingresar a los siguientes sitios para adultos: www.xxx.com y www.xvideos.com, inmediatamente

aparecerá un recuadro de letras blancas y fondo rojo mencionando la imposibilidad de acceder Fig. 47.

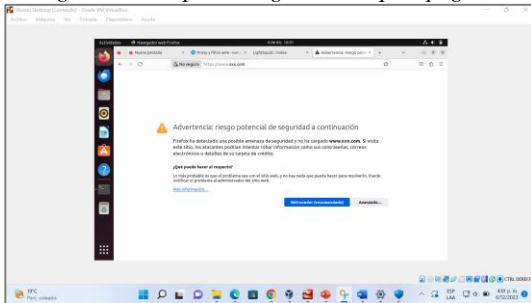
Figura 47. Configuración Proxy web



Fuente: Elaboración propia

Por último, intentaremos saltar el bloqueo del proxy utilizando el acceso HTTPS, así que escribiremos en la barra de dirección del navegador la URL <https://www.xxx.com> y observaremos que, a pesar de ello, no se podrá acceder a la página web solicitada por acción del SSL Transparente Fig. 48.

Figura 48. Bloqueo categorías, bloqueo páginas



Fuente: Elaboración propia

6 CORTAFUEGOS (FIREWALL)

En informática, un cortafuegos (del término original en inglés firewall) es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos [7].

NethServer puede actuar como cortafuegos (Firewall) y puerta de enlace (Gateway) dentro de la red donde está instalado. Todo el tráfico entre las computadoras de la red local e Internet pasa por el servidor que decide cómo enrutar los paquetes y qué reglas aplicar. Los modos firewall y gateway están habilitados solo si el paquete **nethserver-firewall-base** está instalado y el sistema tiene al menos una interfaz de red configurada con función roja [8].

Inicialmente se presentará otra manera para acceder al panel de control o administrador web. Esto se logra una vez se inicia la **MV de NethServer** y además se inicia la **MV Cliente** en la red LAN, en esta última, abrimos el navegador web Mozilla (instalado de forma predeterminada en Ubuntu) e ingresamos la URL con la IP de la MV NethServer, sin escribir el puerto. En esta sección la IP corresponde a <https://192.168.10.15> Fig. 49.

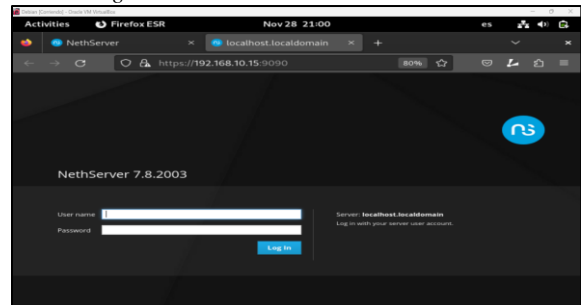
Figura 49. Acceso a NethServer a través del sitio web



Fuente: Elaboración propia

Luego le damos clic al botón denominado “Server Manager”, inmediatamente nos llevará a la página web de ingreso al panel de control en donde se nos solicita las credenciales Fig. 50.

Figura 50. Panel de control de NethServer

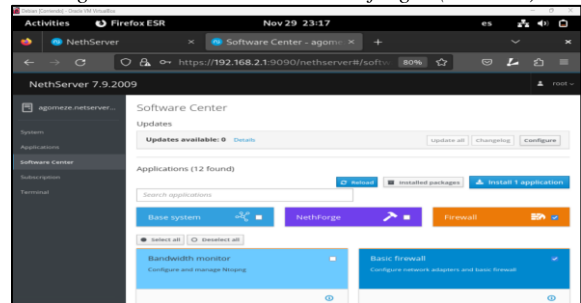


Fuente: Elaboración propia

6.1 INSTALACIÓN Y CONFIGURACIÓN DEL CORTAFUEGOS

Para desarrollar la configuración del cortafuegos se ingresa al módulo denominado “Centro de Software” y se activa la casilla correspondiente al recuadro “Firewall”, aparecerán las distintas aplicaciones relacionadas con el cortafuegos, luego se selecciona el recuadro denominado “Firewall básico – Configurar los adaptadores de red y firewall básico”, se selecciona marcando en la casilla de verificación y posteriormente se le da clic al botón “Instalar 1 aplicación” Fig. 51.

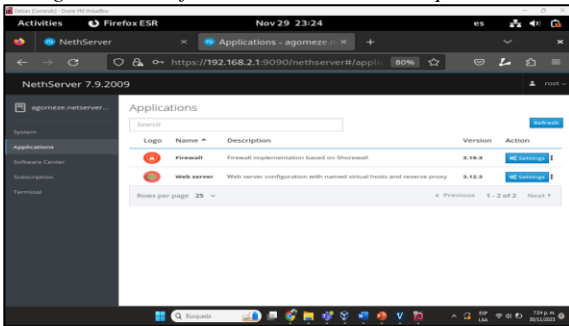
Figura 51. Instalación del Cortafuegos (Firewall)



Fuente: Elaboración propia

Luego, vamos al módulo “Aplicaciones” para confirmar la instalación de esta aplicación Fig. 52.

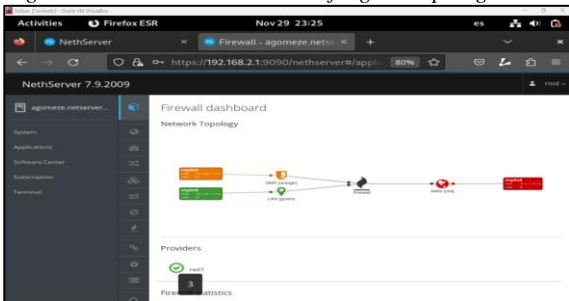
Figura 52. Verificación en el módulo de aplicaciones



Fuente: Elaboración propia

Estando en este módulo y ubicándonos en la franja de la aplicación “Firewall”, le damos clic al botón “Ajustes”, inmediatamente se presentará el “Panel de control del Firewall” en donde encontramos la tipología de la red acorde con la configuración previamente realizada durante la instalación de NetServer 7.9. En este espacio podremos acceder a diferentes opciones para ajustar la configuración del cortafuegos Fig. 53.

Figura 53. Panel de control cortafuegos - Tipología de red



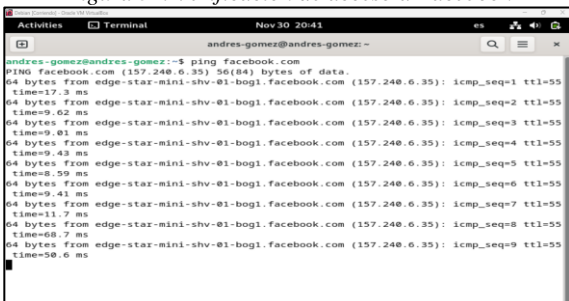
Fuente: Elaboración propia

6.2 CONFIGURACIÓN DE LAS REGLAS

Ahora vamos a la opción denominada “Reglas” y le damos clic. En este espacio podemos crear las reglas que determinarán el acceso al tráfico entre las MVs (equipos) de la red LAN y de la red DMZ y la WAN (Internet).

A manera de ejemplo, restringiremos el acceso a la página web de Facebook, así que primero validaremos ingreso a este sitio web, para ello iremos a la terminal de la MV Cliente, allí escribiremos el comando [ping facebook.com](https://www.facebook.com), observaremos que el acceso funciona de forma adecuada Fig. 54.

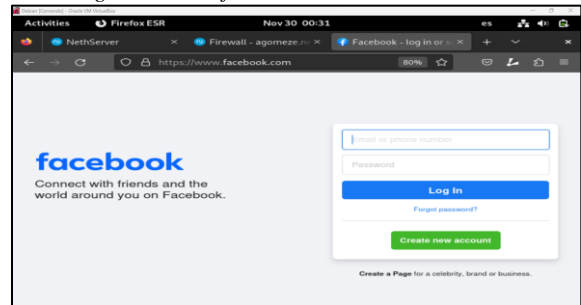
Figura 54. Verificación de acceso a Facebook



Fuente: Elaboración propia

Haremos lo propio ingresando al navegador web de la MV Cliente de la red LAN y escribiendo la URL de este sitio web <https://www.facebook.com> Fig. 55.

Figura 55. Verificación de acceso a Facebook



Fuente: Elaboración propia

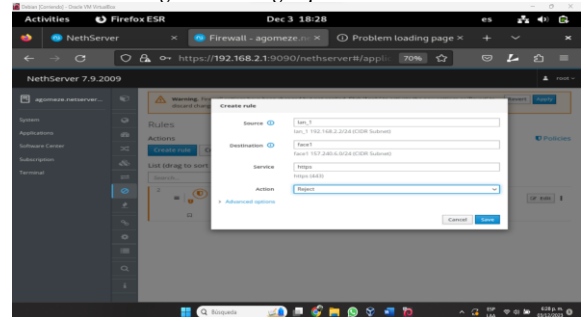
Cabe mencionar que, las reglas se aplican a todo el tráfico que pasa a través del cortafuegos. Cuando un paquete de red se desplaza de una zona a otra, el sistema busca entre las reglas configuradas. Si el paquete coincide con una regla, se aplica la regla. Además, el orden de la regla es muy importante porque el sistema siempre aplicará la primera regla que coincide [8].

Ahora crearemos la **primera regla**, para ello, volvemos al panel de control de NetServer 7.9, nos dirigimos al módulo “Firewall” y luego a la opción “Reglas”, allí le damos clic al botón “Crear regla”.

Se abrirá una ventana emergente en la que debemos diligenciar varios campos en un formulario, en el “Origen” se ubica la dirección IP de la MV que requiere un acceso restringido en los protocolos sea esta de la red LAN o de la red DMZ, en “Destino” se ingresa la dirección IP de la página que se desea restringir, en este caso, la **dirección IP de Facebook 157.240.6.0/24**, los campos de origen y destino aceptan roles integrados, objetos del cortafuegos y direcciones IPv4 sin formato o CIDR [8], en “Servicio” se escribe https para restringir el protocolo seguro de transferencia de hipertexto de este sitio, en “Acción” seleccionamos “Aceptar”, teniendo en cuenta que existen otras dos opciones (Rechazar y Descartar), en “Opciones avanzadas” se podrá realizar una descripción, habilitar un registro, establecer una restricción de tiempo, habilitar la aplicación a las conexiones existentes y establecer la posición de la regla Fig. 56.

Finalmente le damos clic al botón “Guardar”.

Figura 56. Regla para Facebook

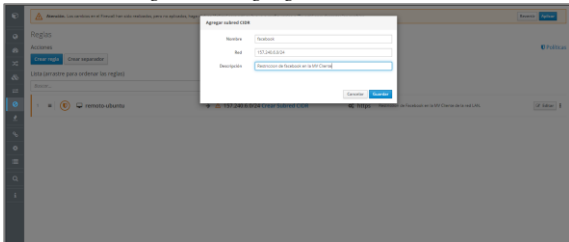


Fuente: Elaboración propia

Aparecerá entonces una alerta en el destino que se solucionará dándole clic, se abrirá una ventana emergente en la que debemos establecer un CIDR o enrutamiento entre dominios sin clases que es un método de asignación de direcciones IP cuyo objetivo es mejorar la eficiencia del enrutamiento de datos en Internet, allí diligenciaremos los campos así Fig. 57:

- Nombre: Facebook
- Red: 157.240.6.0/24
- Descripción: Restricción de Facebook en la MV Cliente

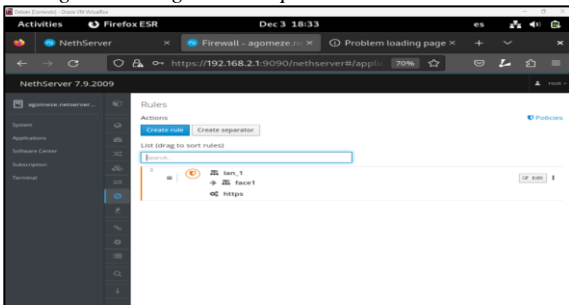
Figura 57. Agregar subred CIDR



Fuente: Elaboración propia

Ahora se deben aplicar las reglas establecidas, así que le damos clic al botón “Aplicar”, así quedará habilitada la regla para restringir el acceso a Facebook Fig. 58.

Figura 58. Regla creada para el acceso a Facebook



Fuente: Elaboración propia

En este segundo ejemplo restringiremos el acceso a la página web de Instagram, así que primero validaremos el correcto ingreso a este sitio web, para ello iremos a la terminal de la MV Cliente en la red LAN y escribiremos el comando `ping instagram.com`, observaremos que el acceso funciona de forma adecuada Fig. 59.

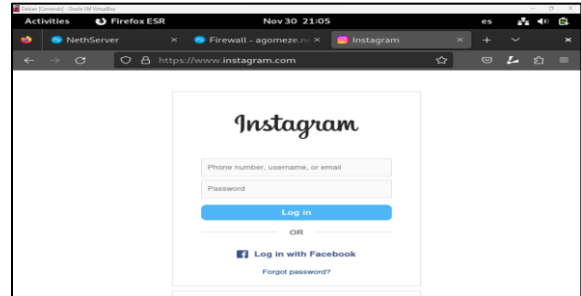
Figura 59. Acceso correcto a la IP de Instagram



Fuente: Elaboración propia

Haremos lo propio ingresando al navegador web de la MV Cliente de la red LAN y escribiendo la URL de este sitio web `https://www.instagram.com` Fig. 60.

Figura 60. Acceso correcto al dominio de Instagram



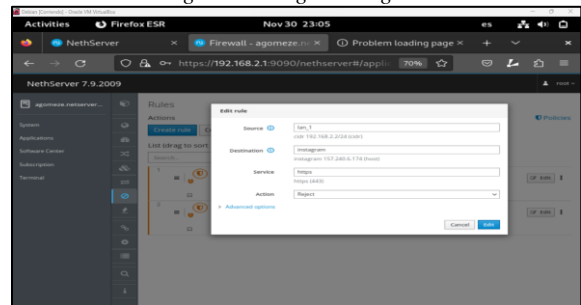
Fuente: Elaboración propia

Entonces, creemos una **segunda regla** para restringir el acceso a Instagram, así que allí le damos clic nuevamente al botón “Crear regla”.

Se abrirá la ventana emergente en la que debemos diligenciar varios campos, en el “Origen” se ubica la dirección IP de la MV que requiere un acceso restringido en los protocolos sea esta de la red LAN o de la red DMZ, en “Destino” se ingresa la dirección IP de la página que se desea restringir, en este caso, la **dirección IP de Instagram 157.240.6.174/24**, en “Servicio” se escribe https para restringir el protocolo seguro de transferencia de hipertexto de este sitio, en “Acción” escogemos “Aceptar”, en “Opciones avanzadas” se podrá realizar una descripción, habilitar un registro, establecer una restricción de tiempo, habilitar la aplicación a las conexiones existentes y establecer la posición de la regla Fig. 61.

Finalmente le damos clic al botón “Guardar”.

Figura 61. Regla Instagram

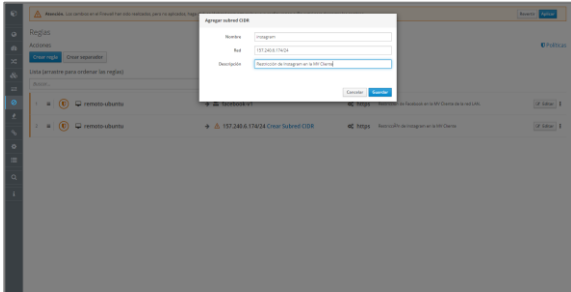


Fuente: Elaboración propia

Aparecerá entonces una alerta que se solucionará dándole clic, se abrirá una ventana emergente en la que debemos establecer un CIDR o enrutamiento entre dominios sin clases que es un método de asignación de direcciones IP cuyo objetivo es mejorar la eficiencia del enrutamiento de datos en Internet, allí diligenciaremos los campos así Fig. 62:

- Nombre: Instagram
- Red: 157.240.6.174/24
- Descripción: Restricción de Instagram en la MV Cliente

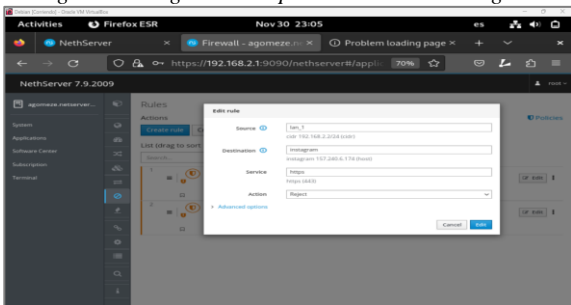
Figura 62. Agregar subred CIDR



Fuente: Elaboración propia

Ahora se deben aplicar las reglas establecidas, así que le damos clic al botón “Aplicar”, así quedará habilitada la regla para restringir el acceso a Instagram Fig. 63.

Figura 63. Regla creada para el acceso a Instagram

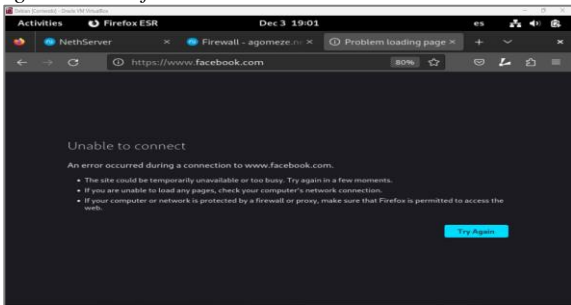


Fuente: Elaboración propia

6.3 VERIFICACIÓN DE LAS REGLAS

Para verificar la restricción de acceso a la página web de Facebook, nos dirigimos a la MV Cliente en la red LAN, abrimos el navegador Mozilla (instalado de forma predeterminada en MVS ubuntu) y escribimos la URL <https://www.facebook.com>, inmediatamente observaremos un mensaje que nos indica la imposibilidad de conectarse con este sitio Fig. 64.

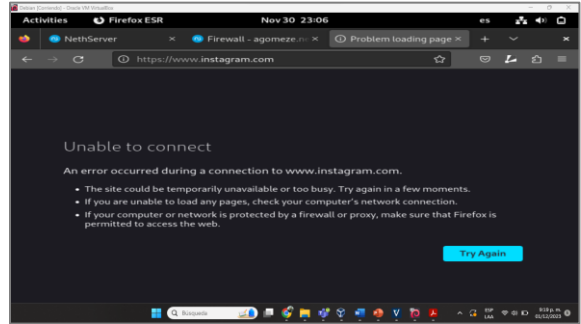
Figura 64. Verificación de la restricción de acceso Facebook



Fuente: Elaboración propia

Ahora, para verificar la restricción de acceso a la página web de Instagram, estando en la MV Cliente de la red LAN, nos dirigimos nuevamente al navegador Mozilla (instalado de forma predeterminada en MVS ubuntu) y escribimos la URL <https://www.instagram.com>, observaremos un mensaje similar al anterior, que nos indica la imposibilidad de conectarse con este sitio Fig. 65.

Figura 65. Verificación de la restricción de acceso Facebook



Fuente: Elaboración propia

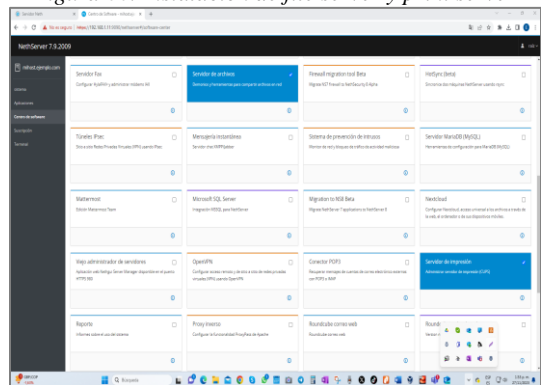
7 FILE SERVER Y PRINT SERVER.

En este apartado se instalará e implementará el servidor de archivos (File Server) que permitirá acceder a los archivos desde cualquier MV cliente dentro de una red local y el servidor de impresión (Print Server) que facilitará la impresión de documentos desde cualquier MV cliente en la red local.

7.1 INSTALACIÓN DE LOS SERVIDORES DE ARCHIVOS Y DE IMPRESIÓN

Estando en el administrador web de NethServer 7.9 nos vamos al módulo “Centro de Software (Software Center)”, luego le damos clic a la casilla de verificación del recuadro denominado “Sistema base”, aparecerán las aplicaciones relacionadas con este ítem, buscaremos y seleccionaremos dos de ellas: el “Servidor de impresión – Administrar el servidor de impresión (CUPS)” y el “Servidor de archivos – Demonios y herramientas para compartir archivos en red” Fig. 66.

Figura 66. Instalación de file server y print server

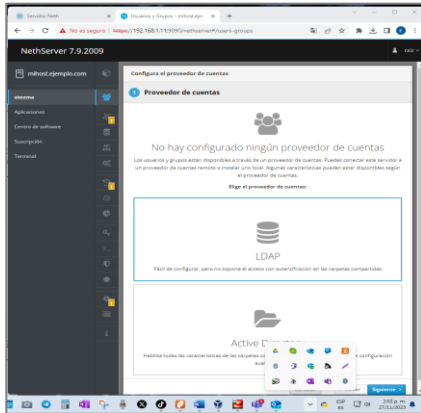


Fuente: Elaboración propia

Una vez instalados, nos dirigimos al módulo “Sistema” y después a la opción “Usuarios y grupos”. Para los propósitos establecidos en esta guía debemos cambiar el proveedor de cuentas instalado, el Servidor Samba AD por el Servidor LDAP, para ello, le damos clic al botón “Cambiar proveedor”, aparecerá una ventana emergente que nos preguntará si estamos seguros de eliminar el proveedor de cuentas actual, así que le damos clic al botón “Eliminar”. Una vez desinstalado Samba AD, nos aparece una ventana emergente en la que tendremos la posibilidad de instalar y configurar LDAP Fig. 67, aquí seleccionamos LDAP y le damos clic al botón “Siguiente”,

luego escogeremos como método de enlace la opción “Instalar LDAL local” y le damos clic al botón “Siguiente”, aparecerá una ventana en la se brinda información de la instalación, así que le daremos clic al botón “Siguiente”.

Figura 67. Instalación y configuración del Servidor LDAP



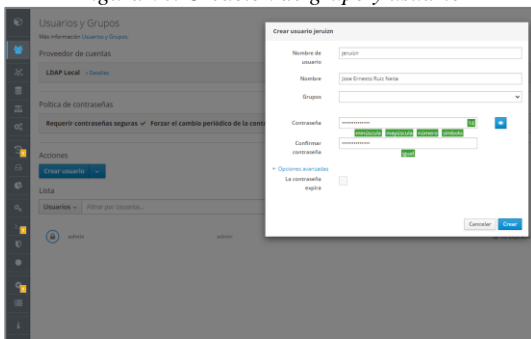
Fuente: Elaboración propia

7.2 CREACIÓN DE USUARIO Y GRUPO

Una vez instalado el Servidor LDAP se debe crear al menos un usuario y un grupo, para la creación del usuario nos vamos a la sección “Acciones” y le damos clic al botón “Crear usuario”, aparecerá una ventana emergente en la que diligenciamos los siguientes datos:

- Nombre de usuario: jeruizn
- Nombre: José Ernesto Ruiz Neita
- Grupos:
- Contraseña: Diplomado2023*
- Confirmar contraseña: Diplomado2023*
- Finalmente, le damos clic al botón “Crear”.

Figura 68. Creación de grupo y usuario



Fuente: Elaboración propia

Ahora crearemos un grupo, para ello, le damos clic al botón de la lista desplegable justo al lado del botón “Crear usuario” y seleccionamos “Crear grupo”, aparecerá una ventana emergente en la que escribiremos los siguientes datos:

- Nombre: diplomado
- Usuarios: José Ernesto Ruiz

Le damos clic al botón “Crear” y reiniciaremos la MV NethServer desde el panel de control.

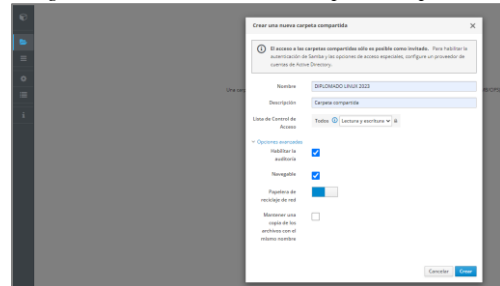
7.3 CREACIÓN DE CARPETAS COMPARTIDAS

Una carpeta compartida es un lugar donde un grupo de personas que utilizan Samba (SMB/CIFS) pueden acceder a los archivos [9]. Crearemos una carpeta que se compartirá Fig. 69, para ello, iremos al módulo “Aplicaciones” y le damos clic al botón “Ajustes” que se encuentra en la misma fila de la aplicación “File server”, se abrirá el “Panel de control del servidor de archivos”, luego le daremos clic a la opción “Carpetas compartidas”, allí le damos clic al botón “Crear una carpeta compartida”, se abrirá una ventana emergente en la que diligenciamos los siguientes datos:

- Nombre: DIPLOMADO LINUX 2023
- Descripción: Carpeta compartida
- Lista de control de acceso: Lectura y escritura
- En el punto “Opciones avanzadas”, habilitaremos la “Auditoría”, permitiremos que sea “Navegable” y activaremos la “Papelera de reciclaje de red”.

Finalmente, le damos clic al botón “Crear”.

Figura 69. Creación de una carpeta compartida

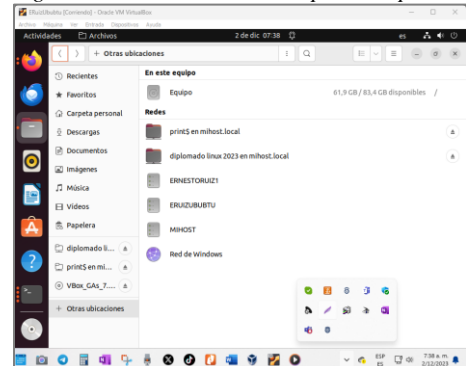


Fuente: Elaboración propia

7.4 VERIFICACIÓN DE LA CARPETA COMPARTIDA

Ingresamos a la MV cliente, abrimos el directorio de archivos (ícono de la carpeta), buscamos la carpeta compartida en la opción “Otras ubicaciones”, allí aparecerá el nombre de la carpeta compartida y el nombre del host en la que se encuentra ubicada “diplomado Linux 2023 en mihost.local” Fig. 70.

Figura 70. Ubicación de la carpeta compartida



Fuente: Elaboración propia

Le daremos clic a esta carpeta y se abrirá una ventana emergente que nos solicitará las credenciales para acceder al recurso compartido, allí escribiremos el usuario y la contraseña creados anteriormente en el módulo “Usuarios y grupos” de NethServer 7.9, le daremos clic a la opción “Recordar la contraseña hasta salir de la sesión” y finalmente le damos clic al botón “Conectar” Fig. 71.

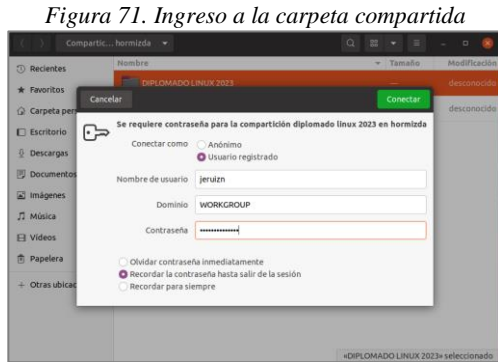


Figura 71. Ingreso a la carpeta compartida

Fuente: Elaboración propia

Aparecerá la carpeta vacía y allí podremos crear y/o guardar carpetas y/o archivos para que sean compartidos.

7.5 SERVIDOR DE IMPRESIÓN

Para el acceso al servicio de impresión, iniciamos una MV cliente de la red, abriremos el navegador web e ingresaremos la URL correspondiente a la MV NethServer, pero con el puerto 631, propio del sistema de impresión modular de código abierto CUPS [10] <https://192.168.31.100:631>, se abrirá una página en la que podemos gestionar el uso de las impresoras conectadas a la red Fig. 72.



Figura 72. Servidor de impresión CUPS

Fuente: Elaboración propia

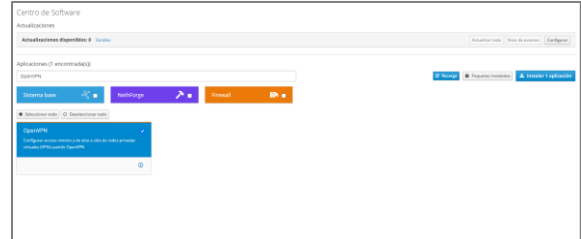
8 VPN

Una VPN (Virtual Private Network, Red Privada Virtual) le permite establecer una conexión segura y encriptada entre dos o más sistemas usando una red pública, como la Internet [11]. En NethServer, hay varias opciones para implementar una VPN, en esta guía se optará por utilizar OpenVPN, adicionalmente, es relevante tener en cuenta que NethServer admite dos tipos de VPN, el “Modo guerrero o roadwarrior”, que conecta un cliente remoto a la red interna y el “Túnel o net2net”, que conecta dos redes remotas [11].

8.1 INSTALACIÓN DE OPENVPN

Seguimos trabajando desde el navegador Google Chrome de la máquina anfitriona (Windows 10), estando en el Panel de Control de NethServer, nos dirigimos al “Centro de Software” y ubicamos la aplicación OpenVPN utilizando la barra de búsqueda. Una vez localizado, le damos clic a la casilla de verificación para seleccionarla, después le damos clic al botón “Instalar 1 aplicación” Fig. 74. El proceso de instalación nos solicitará una confirmación, así que lo haremos y entonces se iniciará.

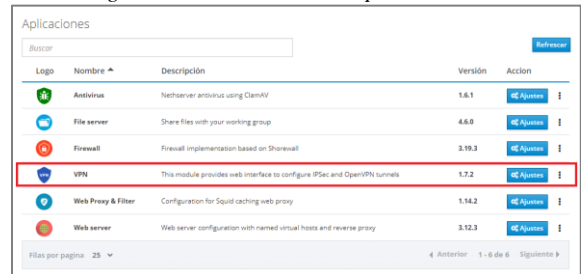
Figura 74. Instalación de OpenVPN



Fuente: Elaboración propia

Ahora nos vamos al módulo “Aplicaciones” y ubicaremos la opción “VPN” Fig. 75, allí le daremos clic al botón “Ajustes”.

Figura 75. Ubicación de la aplicación VPN

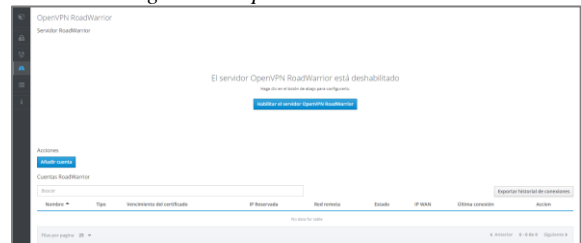


Fuente: Elaboración propia

8.2 CONFIGURACIÓN DEL SERVIDOR DESTINO

Se abrirá el “Panel de control VPN”, aquí se procederá a configurar el servidor de destino al cual nos conectaremos, en seguida, nos iremos a la opción OVPN RoadWarrior Server” para habilitarlo Fig. 76.

Figura 76. OpenVPN RoadWarrior



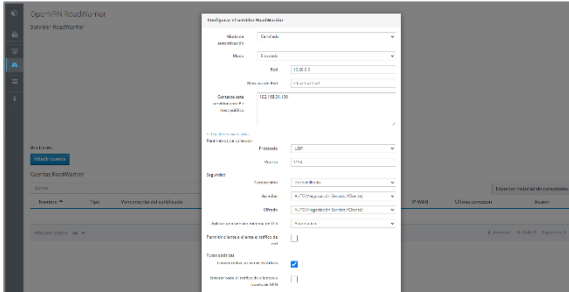
Fuente: Elaboración propia

Luego, le daremos clic al botón “Habilitar el servidor OpenVPN RoadWarrior”, se abrirá una ventana emergente en la que debemos diligenciar varios campos Fig. 77, así:

- Modo de autenticación: Certificado.
- Modo: Enrutado.
- Red: 10.20.0.0 (IP al azar, debe terminar en 0)
- Máscara de red: 255.255.255.0
- Contacte este servidor con IP: 192.168.31.100 (IP de la MV NethServer o el host más el dominio FQNS hormizda.nethserverunad.com)

Los demás datos se dejan de forma predeterminada y finalmente le damos clic al botón “Guardar”.

Figura 77. Activación de OpenVPN RoadWarrior

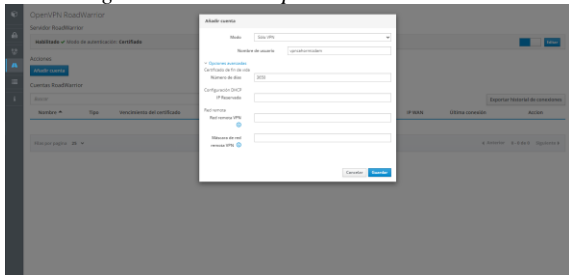


Fuente: Elaboración propia

8.3 CREACIÓN DE UNA CUENTA OPENVPN

Inmediatamente aparecerá información de OpenVPN RoadWarrior, ahora le damos clic al botón “Añadir cuenta”, surge una ventana emergente en la que debemos establecer el “Modo” aquí dejaremos Solo VPN y el “Nombre de usuario”, aquí crearemos uno **vpncahormizdam**, las opciones avanzadas las dejaremos de forma predeterminada [12], después le daremos clic al botón “Guardar” Fig. 78. Ahora se requiere actualizar la configuración recién cambiada, por esto, le damos clic al botón “Aplicar”, preguntará de nuevo si estamos seguros y le daremos nuevamente clic al botón “Aplicar”.

Figura 78. Cuenta OpenVPN RoadWarrior

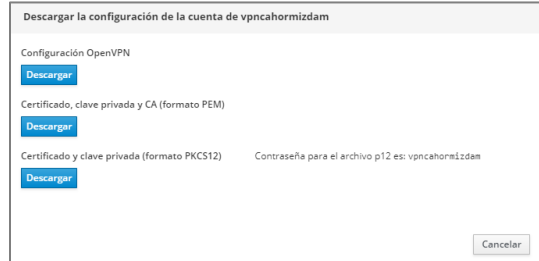


Fuente: Elaboración propia

Para descargar el certificado de autenticación VPN de extensión **ovpn** necesario para realizar la conexión, debemos iniciar la MV Cliente de la red LAN, aquí abriremos el navegador Mozilla (predeterminado en Ubuntu) y escribiremos la URL del administrador web (panel de control) de NethServer 7.9 que corresponde a <https://192.168.31.100:9090>, una vez allí escribiremos las credenciales de ingreso, luego nos dirigiremos al módulo “Aplicaciones”, en seguida le daremos clic al botón “Ajustes” correspondiente a la aplicación “VPN”, se abrirá el “Panel de Control VPN”, ahora nos vamos a la alternativa “OVPN RoadWarrior”, aquí le damos clic a los tres puntos justo

al final del registro de la nueva cuenta de nombre **vpncahormizdam**, surgirá una pequeña ventana emergente en la que seleccionamos la opción “Descarga”, aparecerá otra ventana emergente en la que le daremos clic al botón frente a la opción “Configuración OpenVPN”, esto con el propósito de descargar el certificado de autenticación VPN. Se descargará el archivo **vpncahormizdam.ovpn** Fig. 79.

Figura 79. Descarga del Certificado de autenticación VPN

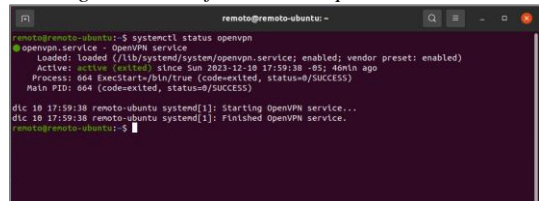


Fuente: Elaboración propia

8.4 CONEXIÓN DE LA MV CLIENTE A TRAVÉS DE LA VPN

Estando en la MV Cliente debemos corroborar que el servicio **openvpn** esté instalado y activo, para ello, abrimos la terminal y escribimos el siguiente comando **systemctl status openvpn** Fig. 80.

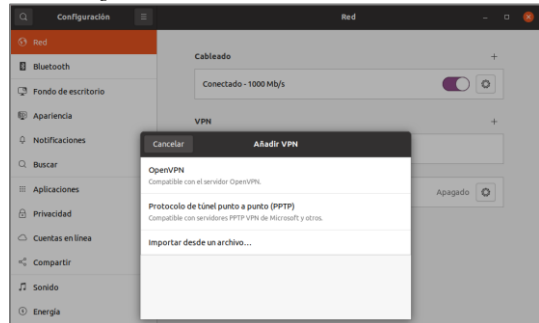
Figura 80. Verificación de OpenVPN Cliente



Fuente: Elaboración propia

En la MV Cliente abriremos la “Configuración”, luego le daremos clic a la opción “Red”, después, en la sección VPN, le daremos clic al signo más (+) para crear la conexión Fig. 81.

Figura 81. Creación de la conexión VPN

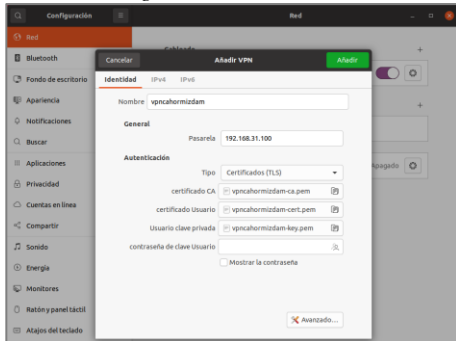


Fuente: Elaboración propia

Posteriormente, le damos clic a la opción “Importar desde un archivo...”, aquí se abrirá la ventana del explorador de archivos, ubicaremos el archivo descargado, lo seleccionaremos y le daremos clic al botón “Abrir”, entonces aparecerá una ventana titulada “Añadir VPN” que estará

diligenciada completamente con la información del archivo descargado Fig. 82, en seguida le daremos clic al botón “Añadir”.

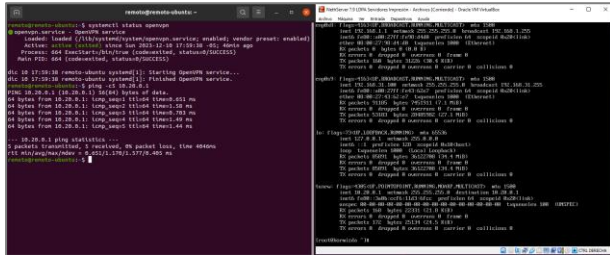
Figura 82. Añadir VPN



Fuente: Elaboración propia

Finalmente, se añadirá esta conexión VPN, ahora para activarla simplemente le daremos clic al interruptor ubicado al frente del nombre de la nueva conexión vpngahormizdam, aparecerá un icono en la esquina superior derecha de la MV Cliente indicándonos que se realizó la conexión. Sin embargo, podemos corroborarlo desde la MV Cliente con el comando `ping -c5 10.20.0.1` y desde la MV NethServer 7.9 con el comando `ifconfig` Fig. 83.

Figura 83. Verificación tráfico VPN



Fuente: Elaboración propia

9 CONCLUSIONES

La configuración adecuada de los servicios DHCP, DNS y un Controlador de Dominio con Samba AD, es esencial para garantizar la asignación eficiente de direcciones IP, la resolución de nombres de dominio y la implementación de políticas de seguridad, creando así un entorno de red robusto y confiable.

La guía destaca la capacidad del servicio Proxy en NethServer 7.9 para controlar y filtrar el tráfico web. Al seguir los pasos detallados, los administradores pueden establecer políticas de acceso que protegen la red de posibles amenazas y garantizan un uso adecuado de los recursos en línea.

La importancia de la seguridad informática se ve reflejada en la implementación del servicio cortafuegos en NethServer 7.9. La guía proporciona una visión clara de los pasos necesarios para establecer una barrera efectiva contra posibles amenazas y ataques.

Este documento no solo facilita la creación de un sistema de almacenamiento centralizado (File Server), sino que también simplifica la gestión de impresoras (Print Server), mejorando significativamente la eficiencia operativa de la red.

La seguridad y la gestión eficiente de la conectividad remota son pilares clave en la implementación de una VPN en NethServer 7.9. Además de establecer conexiones seguras, la documentación resalta la importancia de la monitorización y la actualización periódica para garantizar la resistencia del sistema frente a amenazas emergentes.

10 REFERENCIAS

- [1] Documentación NethServer. (s. f.), *Requerimientos mínimos*. <https://docs.nethserver.org/es/v7/installation.html>
- [2] NethServer. (s. f.), *Getting started with NethServer*. <https://www.nethserver.org/getting-started-with-nethserver/>
- [3] Documentación NethServer. (s. f.), *Servidor DHCP y PXE*. <https://docs.nethserver.org/es/v7/dhcp.html>
- [4] Portillo, S. (7 de julio de 2022), *Como unir un cliente Ubuntu a un dominio de Active Directory*. Tutoriales IT <https://tutorialesit.com/como-unir-un-cliente-ubuntu-a-un-dominio-de-active-directory/>
- [5] Servidor proxy. (20 de octubre de 2023), *En Wikipedia*. https://es.wikipedia.org/w/index.php?title=Servidor_proxy&oldid=154755046
- [6] NethServer. (s. f.), *Web Proxy*. https://docs.nethserver.org/es/v7/web_proxy.html
- [7] Cortafuegos. (5 de octubre de 2023), *En Wikipedia*. [https://es.wikipedia.org/w/index.php?title=Cortafuegos_\(inform%C3%A1tica\)&oldid=154310173](https://es.wikipedia.org/w/index.php?title=Cortafuegos_(inform%C3%A1tica)&oldid=154310173)
- [8] NethServer. (s. f.), *Cortafuego y puerta de enlace*. <https://docs.nethserver.org/es/v6/firewall.html>
- [9] NethServer. (s. f.), *Carpetas compartidas*. https://docs.nethserver.org/es/v7/shared_folder.html
- [10] NethServer. (s. f.), *CUPS - NethServer*. <https://docs.nethserver.org/projects/nethserver-devel/en/latest/nethserver-cups.html>
- [11] NethServer. (s. f.), *VPN*. <https://docs.nethserver.org/es/v7/vpn.html>
- [12] Universidad de Córdoba. (s. f.), *OpenVPN en Linux - GNOME*. <https://www.uco.es/servicios/informatica/es/openvpn-en-linux-gnome>

Notas:

1. Esta guía está construida sobre la base de una implementación en VirtualBox, sin embargo, su uso se puede extender fácilmente a equipos de cómputo reales.
2. Además, de los servicios que se presentan en este artículo, la distribución GNU/Linux NethServer 7.9, ofrece otros tantos servicios, módulos y aplicaciones, entre ellos, correo electrónico, nextcloud, antivirus, webmail, copia de seguridad, PBX y escudo de amenazas.