

SOLUCIÓN DE NECESIDADES ESPECÍFICAS CON GNU/LINUX NETHSERVER

Yordy Riascos González
yriascosg@unadvirtual.edu.co
Marlon José Montaguth Sepúlveda
mjm Montaguths@unadvirtual.edu.co
Rodolfo Castaño Cárdenas
rcastanoc@unadvirtual.edu.co
Sergio Alexander Jaime Porras
sajaimep@unadvirtual.edu.co

RESUMEN: *Linux ofrece numerosas ventajas que lo convierten en una opción atractiva para pequeñas y medianas empresas. La distribución NethServer, basada en Linux, es una solución eficiente gracias a su interfaz amigable, su capacidad para manejar procesos de manera efectiva y su simplicidad operativa.*

PALABRAS CLAVE: DHCP, DNS, GNU/Linux, Nethserver, Server, VPN.

1. INTRODUCCIÓN

La atención centrada en la seguridad de NethServer enriquece la experiencia de los usuarios al ofrecer un entorno de operación robusto y confiable, permitiendo que los servicios esenciales operen de manera eficaz y segura en entornos empresariales. En el desarrollo de la actividad se da solución mediante variadas temáticas al contexto presentado estructurando de manera consecuente el estudio, implementación y puesta en marcha de los servicios requeridos mediante la gestión DHCP Server, DNS Server, Controlador de Dominio, proxy, cortafuegos, File Server, Print Server y VPN.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Proporcionar soluciones utilizando GNU/Linux mediante la instalación, configuración y puesta en marcha de una infraestructura tecnológica que satisfaga los requerimientos específicos de la empresa.

2.2 OBJETIVOS ESPECIFICOS

- Configurar Estaciones de Trabajo:

Implementar y configurar el acceso de una estación de trabajo GNU/Linux utilizando un usuario y contraseña, registrándola en los servicios de infraestructura IT de NethServer.

- Control de Acceso a Internet: Gestionar el acceso a internet de las estaciones GNU/Linux a través del puerto 3128 utilizando un servidor proxy.

2. INSTALACIÓN DE NETHSERVER

NethServer es una distribución basada en Linux, específicamente en CentOS y Red Hat, diseñada para actuar como servidor en pequeñas y medianas empresas. Es un sistema altamente modular que permite la fácil integración de nuevos plugins y software adicional, mejorando sus opciones predeterminadas. A partir de la versión 7.7, NethServer ofrece una interfaz moderna e intuitiva que facilita la administración de cuentas, DNS, DHCP, FQDN, configuración de aplicaciones, gestión de almacenamiento y certificados SSL. Además, permite configurar VPNs, evaluar el tráfico de cada túnel, rastrear el historial de conexión de usuarios, definir rutas personalizadas y cambiar protocolos UDP/TCP, entre otras funcionalidades.

3. REQUISITOS

Los requisitos para instalar NethServer son los siguientes:

- CPU de 64 bits (x86_64)
- 1 GB de RAM
- 10 GB de espacio en disco
- Al menos una interfaz de red
- Unidad óptica de arranque (DVD, USB) para instalaciones en servidores físicos.

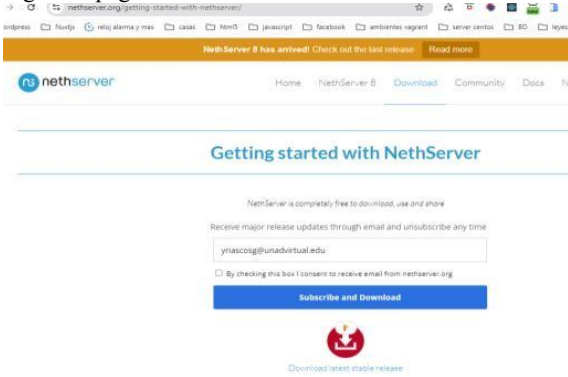
3.1 ENLACE DE DESCARGA

<https://www.nethserver.org/getting-started-withnethserver/>

4. PRÁCTICA

Se ingresa a la página oficial de nethserver en la opción download para proceder con la descarga.

Figura 1. página oficial de nethserver.

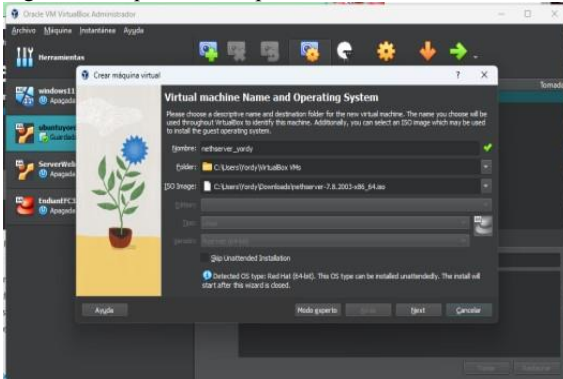


Fuente: Autoría Propia

Una vez descargado se abre el VirtualBox e iniciar la creación de una nueva máquina virtual

Proceder a crear la máquina virtual que se va a necesitar.

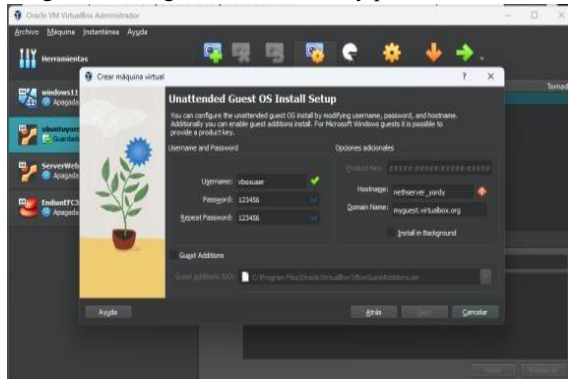
Figura 2. Máquina virtual para instalar Nethserver .



Fuente: Autoría Propia

Asignar nuestro username.

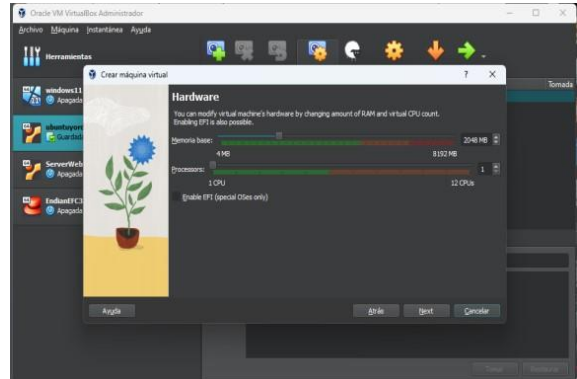
Figura 3. Configurar ahora usuario y password.



Fuente: Autoría Propia

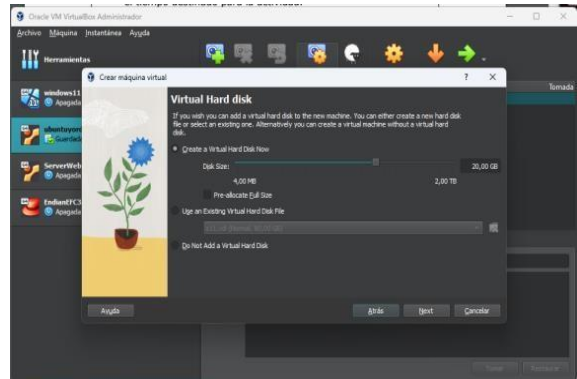
Asignar cantidades de memoria base y procesador.

Figura 4. Configuración de memoria, espacio en disco y finalización.



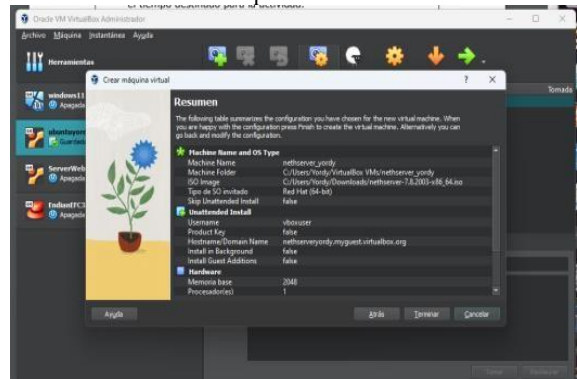
Fuente: Autoría Propia.

Figura 5. asignación de espacio en el disco.



Fuente: Autoría Propia

Figura 6. Configuración del sistemas y sus requisitos.



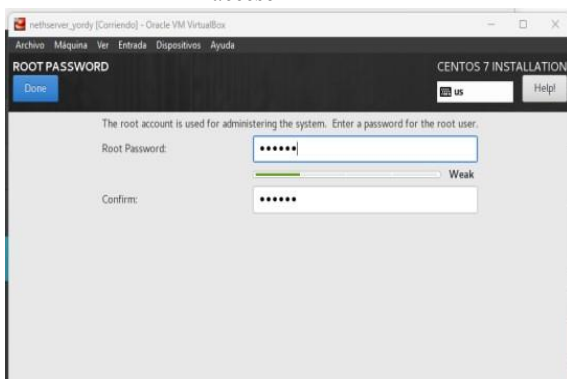
Fuente: Autoría Propia.

Figura 7. Configuración de fecha/hora y distribución del teclado .



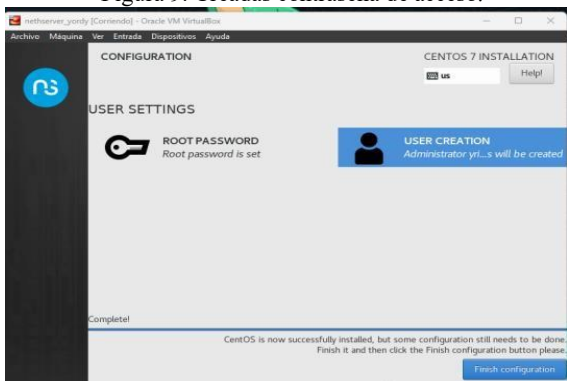
Fuente: Autoría Propia.

Figura 8. Estableciendo contraseña de acceso .



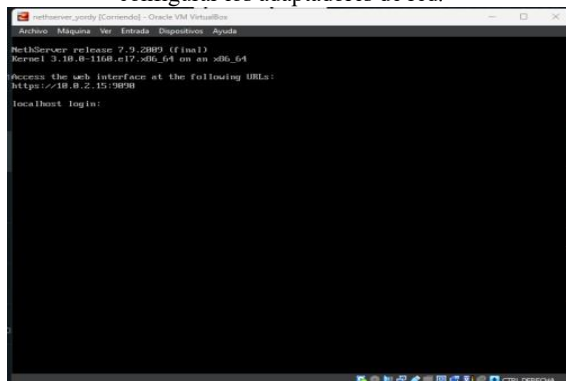
Fuente: Autoría Propia.

Figura 9. Creadas contraseña de acceso.



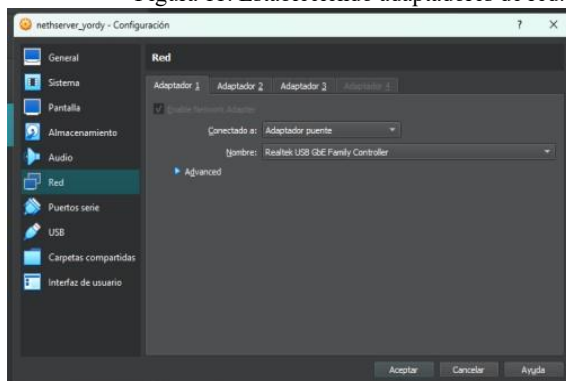
Fuente: Autoría Propia.

Figura 10. Proceder apagar la máquina y configurar los adaptadores de red.



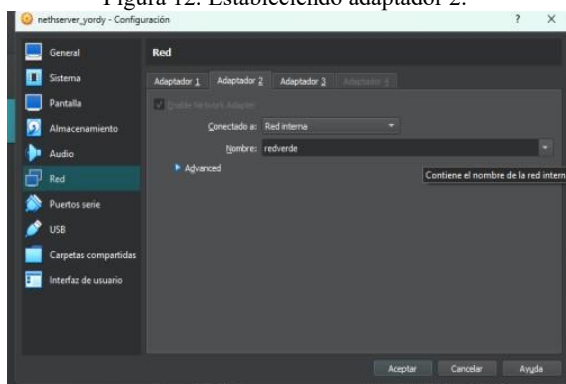
Fuente: Autoría Propia.

Figura 11. Estableciendo adaptadores de red.



Fuente: Autoría Propia.

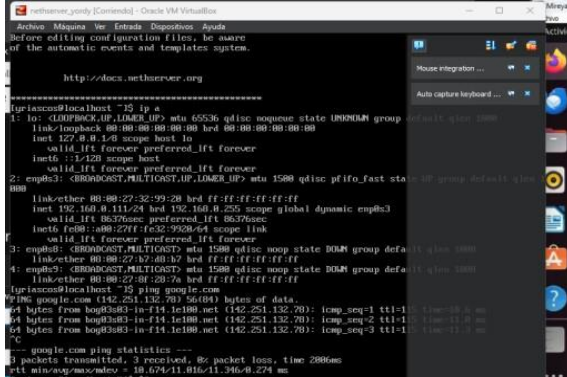
Adaptador de red
Figura 12. Estableciendo adaptador 2.



Fuente: Autoría Propia.

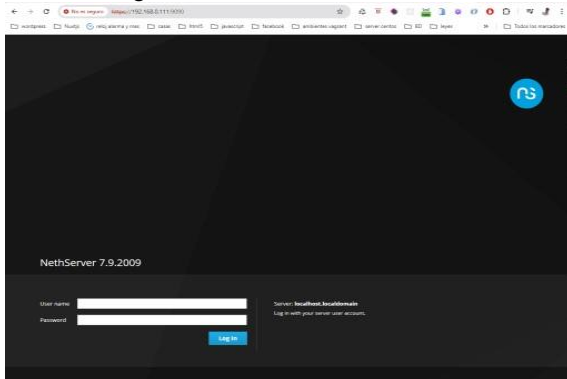
Ver los adaptadores configurados y la salida a internet

Figura 13. Ver el acceso desde el equipo local y desde una de las más maquinas virtual con Ubuntu que ya tienen acceso al servidor nethserver Equipo local.



Fuente: Autoría Propia.

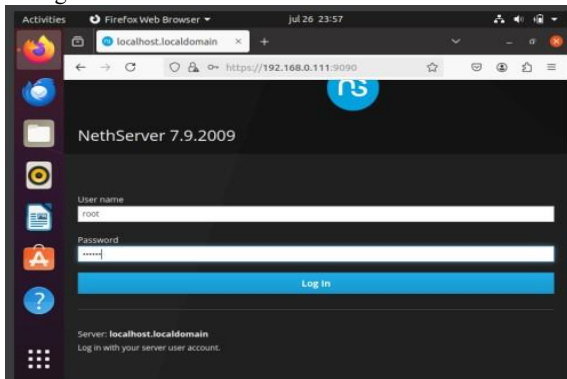
Figura 14. Accediendo al servidor.



Fuente: Autoría Propia.

Equipo máquina virtual Ubuntu server

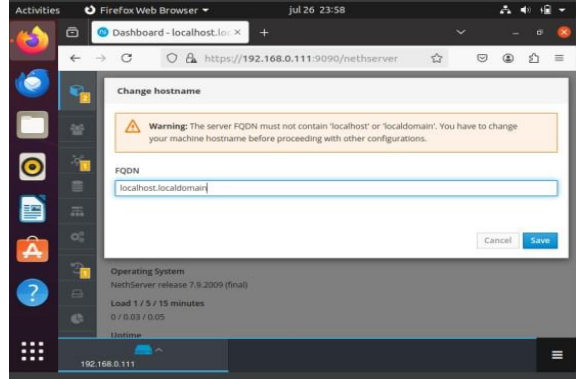
Figura 15. Ingresar con las credenciales configuradas al final de la instalación.



Fuente: Autoría Propia.

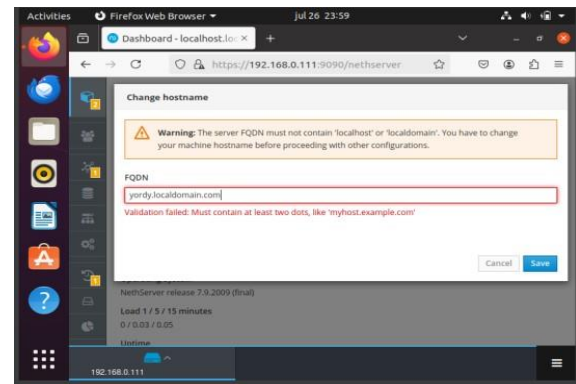
Se logra el ingreso y ahora dentro de la plataforma la primera pantalla que nos muestra contiene un modal que nos solicita configurar un dominio.

Figura 16. Configurando FQDN .



Fuente: Autoría Propia.

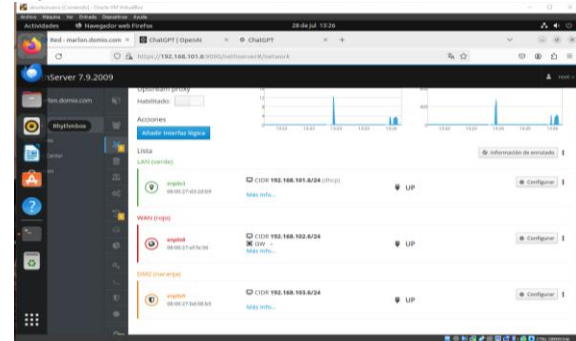
Figura 17. Se debe ir al apartado de red, donde se ubica las 3 tarjetas de red .



Fuente: Autoría Propia.

Proceder a configurar la tarjeta enp0s3 , como enlace rojo y salida a internet, para ello la seleccionar y le dar clic en configurar.

Figura 18. Lista redes NethServer.



Fuente: Autoría Propia.

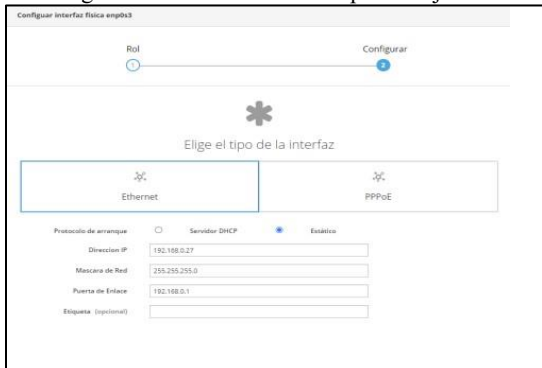
Seleccionar WAN rojo, presionar siguiente .
 Figura19. Wan Rojo NetServer



Fuente: Autoría Propia.

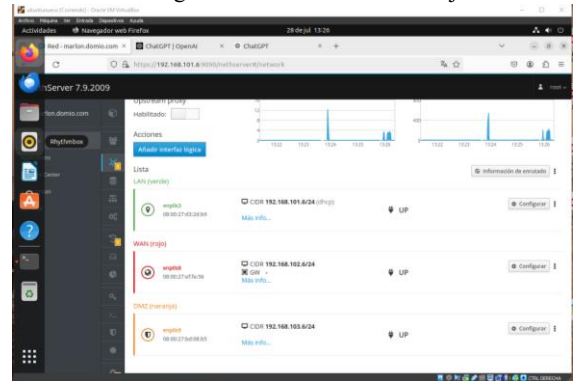
Continuar digitando los datos de la red y luego seleccionar configurar .

Figura 20. Direccionamiento ip wan rojo.



Fuente: Autoría Propia.

Figura21. Activación WAN Rojo



Fuente: Autoría Propia.

Luego continuar con la tarjeta enp0s8, la cual será la red de color verde y se encargara de manejar nuestra LAN y la conexión a los dispositivos de red de usuarios internos. Para eso repetir el mismo proceso, pero seleccionar verde al momento de seleccionar el rol de la interfaz.

Figura22. Activación LAN verde.



Fuente: Autoría Propia.

Y luego le dar los parámetros de nuestra red.

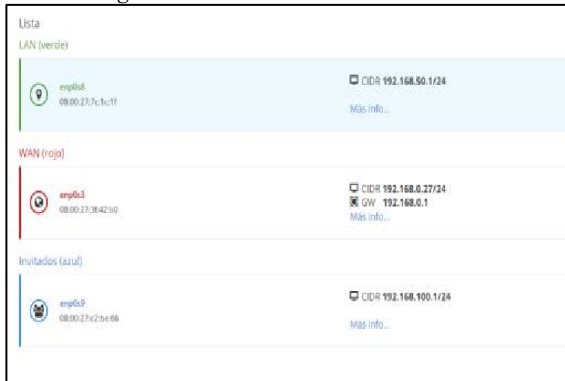
Figura 23. Direccionamiento LAN verde



Fuente: Autoría Propia

El mismo proceso se hace para la red azul , la cual está pensada para que los visitantes de la empresa se conecten a internet y no tengan acceso a los datos internos. En resumen quedan así.

Figura 24. Resumen enlaces de red



Fuente: Autoría Propia

3 DESARROLLO TEMÁTICA

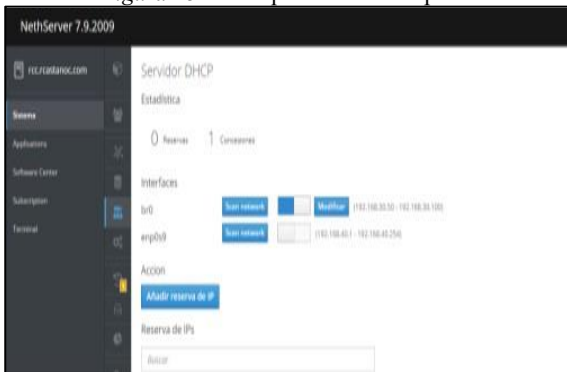
3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

TEMÁTICA 3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Para el cumplimiento de esta actividad, inicialmente se diseña un diagrama de como funcionara la red.

Ahora nuestro paso a seguir es configurar el servidor dhcp de la red verde , se debe ingresar al apartado servidor DHCP y allí poder ver el interfaz verde y azul , para efectos del ejercicio se va a trabajar con la interfaz verde.

Figura 25. Arranque servidor dhcp



Fuente: Autoría Propia

Activar el interfaz para que funcione el dhcp y seleccionar el rango de asignación de nuestro segmento. Para nuestro ejercicio seleccionar desde la ip 192.168.30.50 hasta la ip 192.168.30.100 es decir solo se podrán conectar 50

equipos.

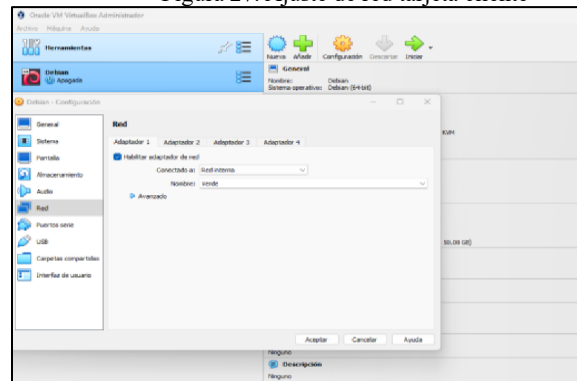
Figura 26. Rango asignación ip



Fuente: Autoría Propia

Con esta configuración, se debe poder iniciar en otra máquina virtual con una ip asignada por nuestro servidor dhcp dentro del segmento dado, pero es importante recalcar que se debe ajustar los parámetros de red de la máquina virtual tal y como se muestra en la imagen.

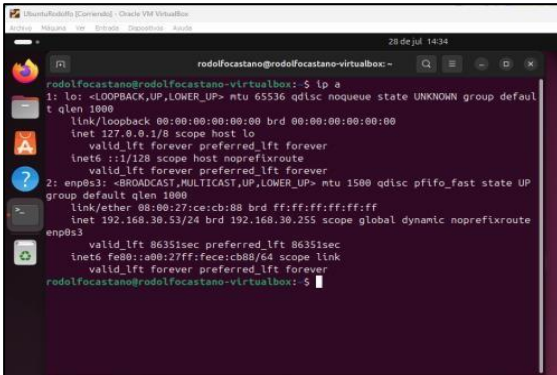
Figura 27. Ajuste de red tarjeta cliente



Fuente: Autoría Propia

Se valida el funcionamiento del servidor dhcp poniendo en marcha la máquina virtual y validando que la dirección este acorde a los ajustes realizados en el servidor.

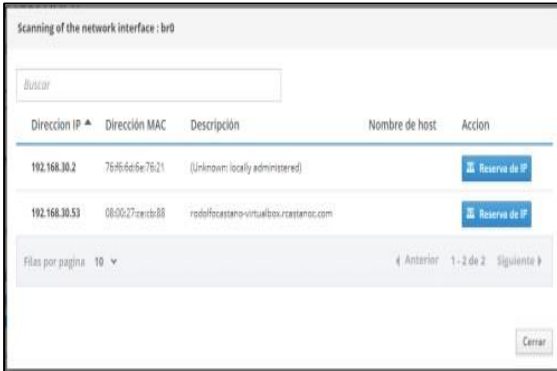
Figura 28. Validación parámetros de red equipo cliente.



Fuente: Autoría Propia

También se puede validar los equipos conectados desde el dashboard de NethServer, escaneando las conexiones.

Figura 29. Validación parámetros de red equipo cliente



Fuente: Autoría Propia

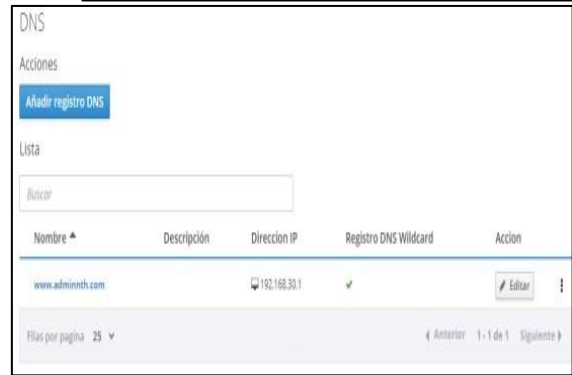
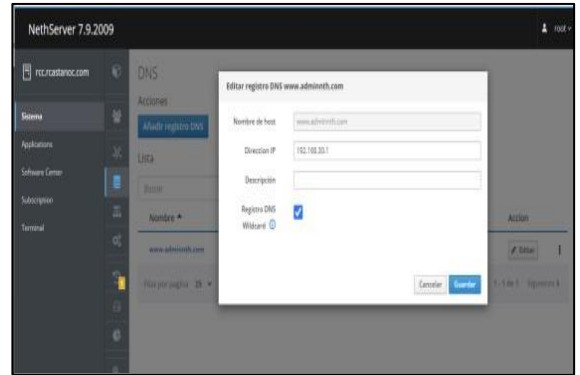
El paso siguiente es crear nuestro servidor DNS el cual le dira a los host clientes a que ip redirigir las peticiones ue hacen, en nuestro caso redirigir el dominio www.adminnth.com a la ip 192.168.30.1, la cual corresponde al mismo servidor. Al dirigirse al apartado DNS, seleccionar añadir registro DNS y digitar los siguientes datos:

Figura 30. Creación registro DNS

Fuente: Autoría Propia

Evidenciar el registro DNS en la lista de la parte inferior.

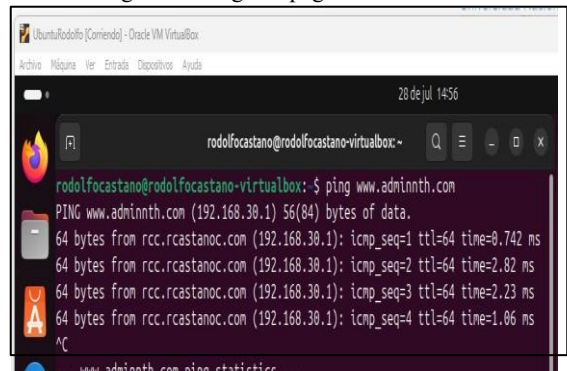
Figura 31. Listado registros DNS



Fuente: Autoría Propia

Se debe ingresar al host cliente para validar si resuelve el nombre www.adminnth.com Le hacer ping a la página y efectivamente ya responde.

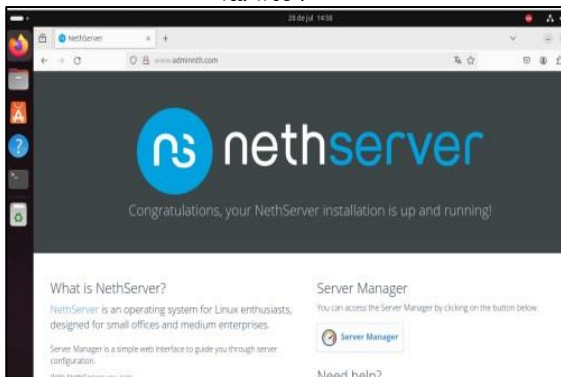
Figura 32 Ping a la página.



Fuente: Autoría Propia

Ahora ir al navegador web y consultar la página www.adminnth.com los resolverá como la página de administración del nethserver, es decir la resolución DNS funciona perfectamente.

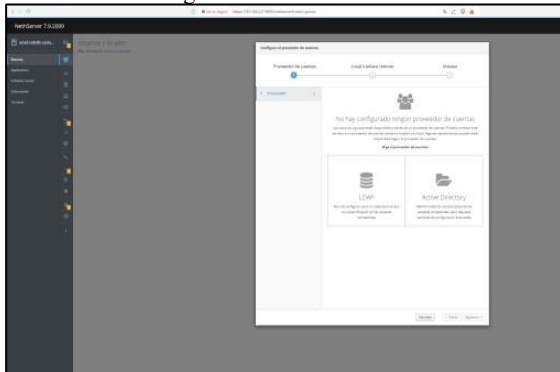
Figura 33 Validación DNS desde cliente vía web .



Fuente: Autoría Propia

Ahora el paso a seguir es crear nuestro active directory, se debe ingresar al apartado usuarios y grupos y seleccionar tipo Active Directory

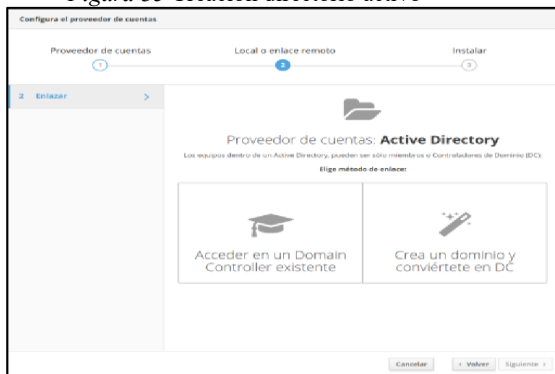
Figura 34 Creación directorio activo



Fuente: Autoría Propia

Luego presionar clic en la opción “Crea un dominio y conviértete en DC”

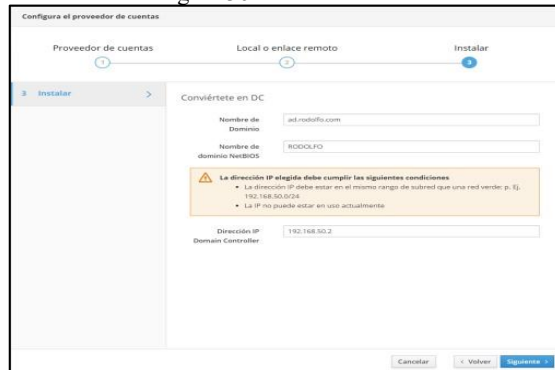
Figura 35 Creación directorio activo



Fuente: Autoría Propia

El siguiente paso es ponerle un nombre al dominio y una dirección ip del segmento verde:

Figura 36 Nombre directorio activo



Fuente: Autoría Propia

Luego dar clic en siguiente y esperar que instale.

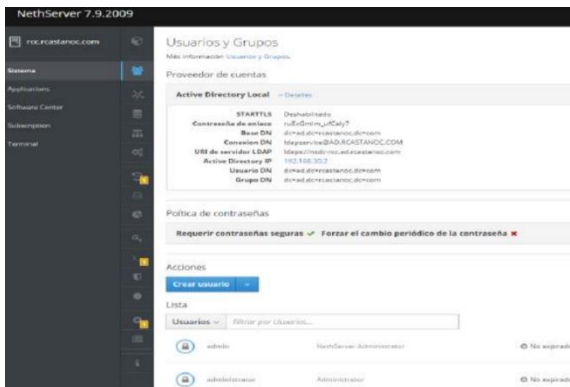
Figura 37 Finalizando instalación controlador de dominio



Fuente: Autoría Propia

Luego de instalado, nos saldrá el siguiente menú con la descripción de nuestro controlador de dominio , en dicho menú tendrá las opciones para la creación de usuarios , grupos y establecer políticas de contraseñas.

Figura 38 Datos controlador de dominio.



Fuente: Autoría Propia

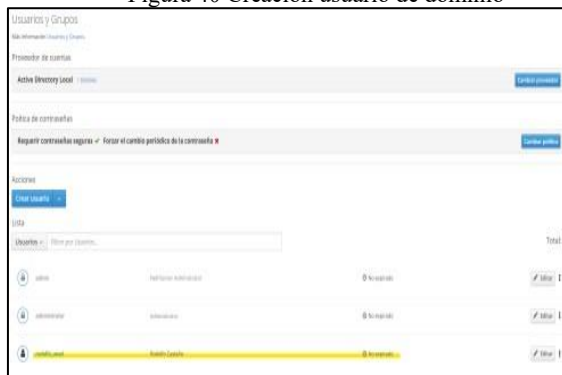
Figura 39 Creación usuario de dominio.



Fuente: Autoría Propia

Al crearlo se puede ver y administrar nuestro usuario desde el panel de grupos y usuarios de Nethserver.

Figura 40 Creación usuario de dominio

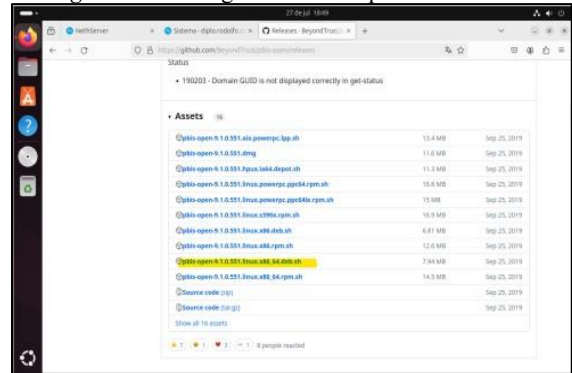


Fuente: Autoría Propia

Ahora lo que tener que hacer es afiliar el equipo cliente al dominio, para ello ir a nuestro host que está bajo Ubuntu y ejecutar el siguiente proceso.

Primero descargar el siguiente archivo pbis-open-9.1.0.551.linux.x86_64.deb.sh en el enlace <https://github.com/BeyondTrust/pbis-open/releases>

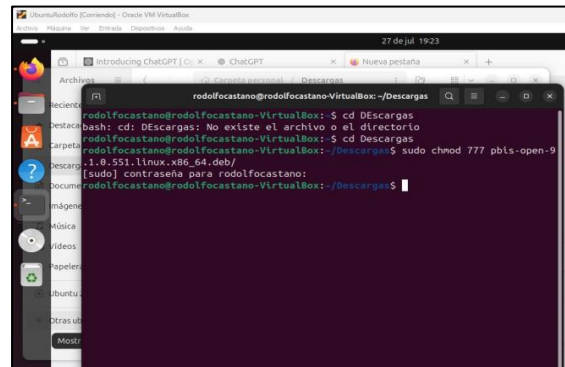
Figura 41 Descarga herramienta para unión de dominio



Fuente: Autoría Propia

Luego le modificar los permisos al programa utilizando chmod 777 .

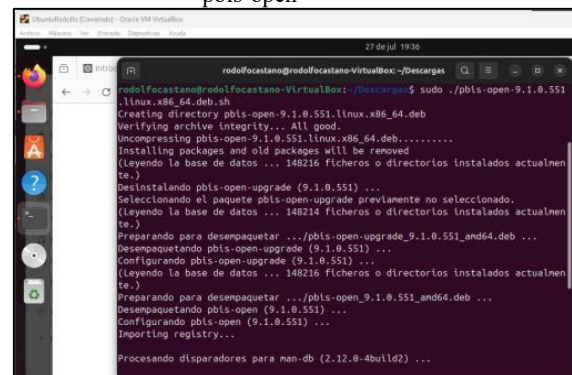
Figura 42 Asignación permisos



Fuente: Autoría Propia

Luego se debe ejecutar el instalador con el comando `sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh` con esto el proceso inicia la instalación.

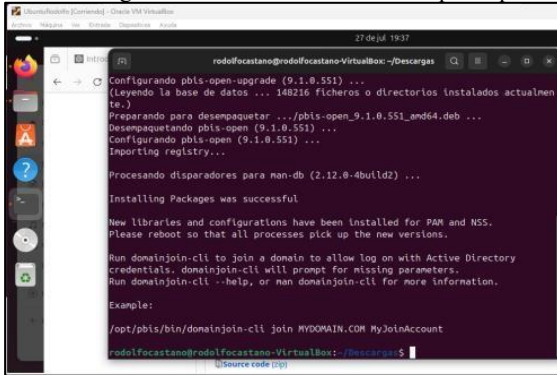
Figura 43 Instalación herramienta pbis-open



Fuente: Autoría Propia

Cuando el programa finaliza, poder ver el ejemplo de cómo se hace la afiliación al dominio

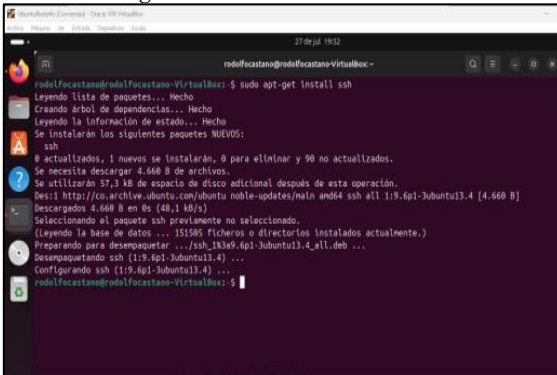
Figura 44 Finalización instalación pbis-open



Fuente: Autoría Propia

Antes de unirnos al dominio es necesario instalar el ssh server con el comando apt-get install ssh .

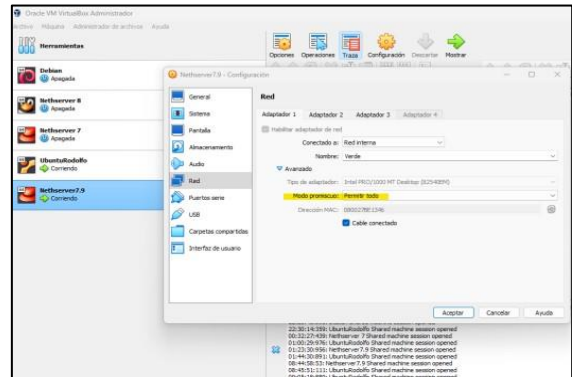
Figura 45 Instalación herramienta ssh



Fuente: Autoría Propia

Algo que se debe tener muy en cuenta es que en la configuración del virtualbox de nuestro Nethserver en el apartado red, se debe tener habilitado en nuestra red verde el modo promiscuo “permitir todo” para que los clientes puedan ver al controlador de dominio.

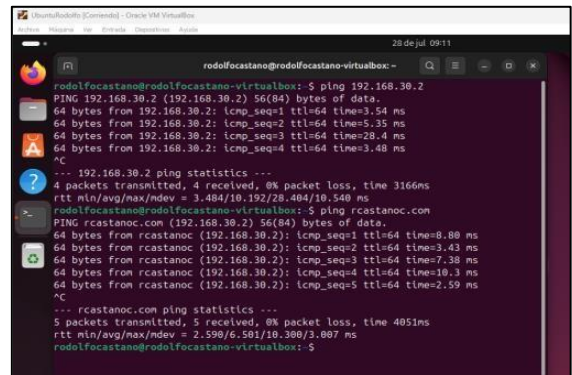
Figura 46 Configuración modo promiscuo NethServer



Fuente: Autoría Propia

Luego de hacer este ajuste ir a realizar pruebas de conectividad y resolución de nombres desde nuestro host cliente hacia nuestro controlador de dominio:

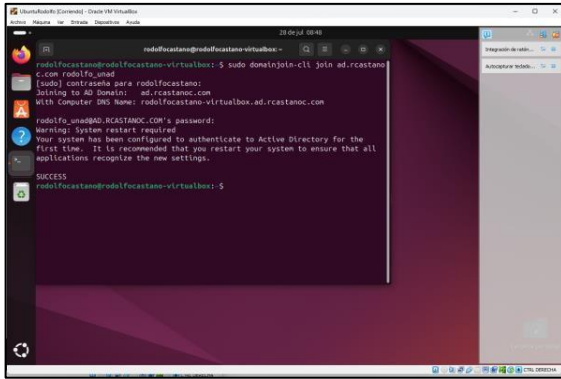
Figura 47 Validación conexión hostcontrolador de dominio.



Fuente: Autoría Propia

Luego de instalada la herramienta nos unir al dominio con el siguiente comando **sudo domainjoincli join ad.rcastanoc.com rodolfo_unad** , en este caso nos pedirá la contraseña que se creo para este usuario en el portal de usuarios de nuestro nethserver. Luego de que se valida el registro en el dominio es necesario reiniciar nuestro cliente para que tome los cambios.

Figura 48 Unión a dominio equipo cliente

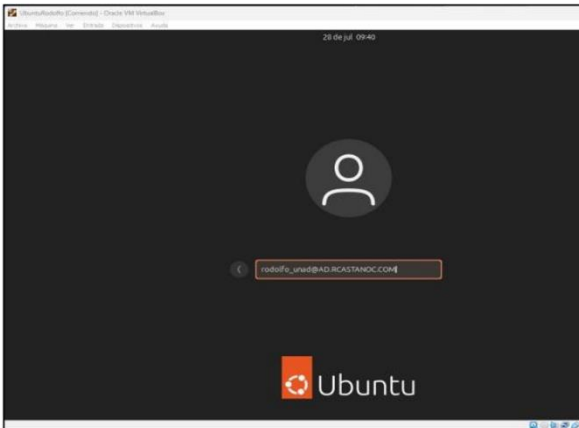


Fuente: Autoría Propia

Cuando reinicie el equipo, donde se hace el login es necesario seleccionar ¿No esta en la lista?, luego de esto digitar el usuario y la contraseña de nuestro usuario de dominio, en nuestro caso es

rodolfo_unad@AD.RCASTANOC.COM

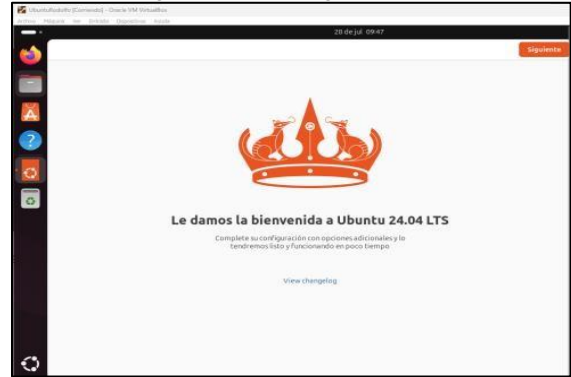
Figura 49 Inicio de sesión usuario del dominio



Fuente: Autoría Propia

Al iniciar el sistema lo identificara como un usuario nuevo y le dara la bienvenida al sistema.

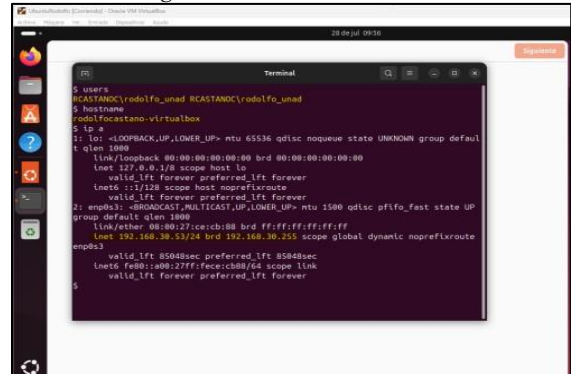
Figura 50 Primer login usuario de dominio



Fuente: Autoría Propia

Poder validar que estar conectados a nuestro dominio validando desde la terminal el usuario, nombre e ip de la maquina con los comandos **users**, **hostname**, **ip a**

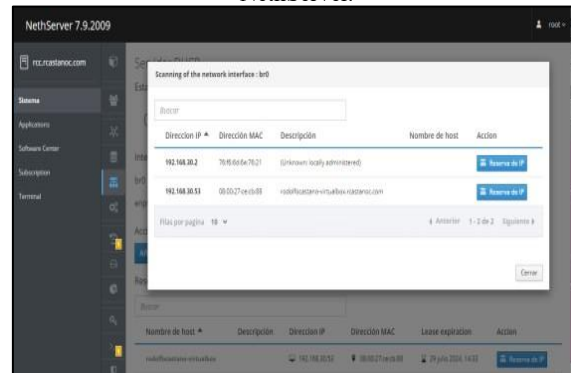
Figura 51 validación datos del dominio



Fuente: Autoría Propia

Validar desde el NethServer que sean iguales, datos que muestra el host.

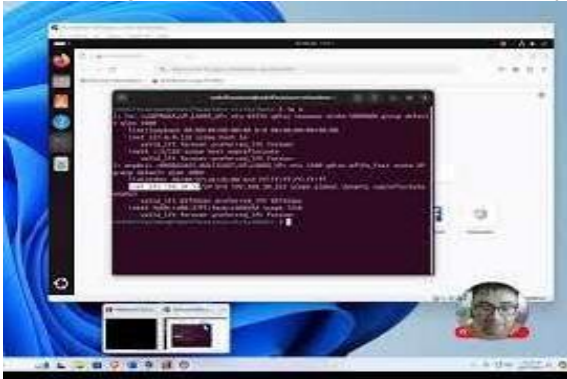
Figura 52 validación datos del dominio NethServer.



Fuente: Autoría Propia

El estudiante deberá realizar el proceso de sustentación del trabajo final, en donde expondrá la solución que fue implementada en cada uno de los escenarios propuestos, mediante un video, el cual no deberá ser superior a 15 minutos.

Figura 53. Sustentación del trabajo



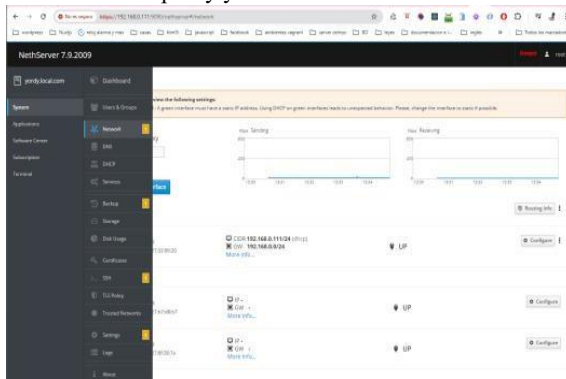
Fuente: Autoría Propia

Temática 2:

Proxy Producto esperado:
Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Nethserver a través de un proxy que filtra la salida por medio del puerto 3128.

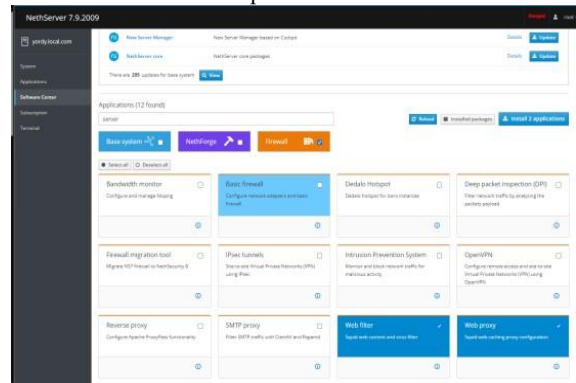
1. Una vez ya configurado dentro del dashboard de nethserver proceder a la configuración de proxy por medio del puerto 3128 ingresar a la opción red.

Figura 54. Ingresar al software center y proceder a buscar e instalar 2 aplicaciones web proxy y web filter



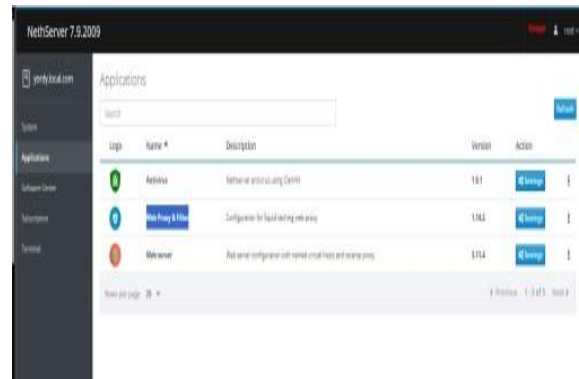
Fuente: Autoría Propia

Figura 55. Una vez instaladas nos aparecerán en aplicaciones.



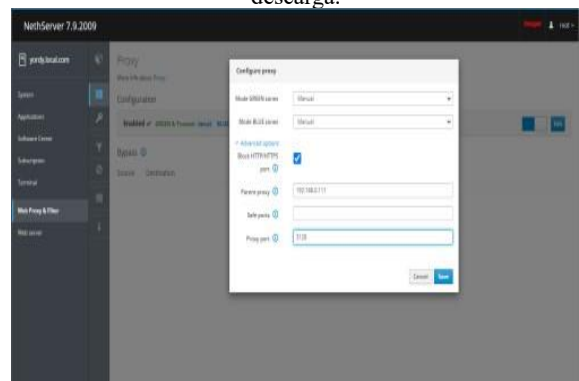
Fuente: Autoría Propia

Figura 56. Ingresar a las opciones web proxy & filter del menú y seleccionar configurar proxy. Establecer los valores de configuración y el puerto 3128 y luego dar click en guardar.



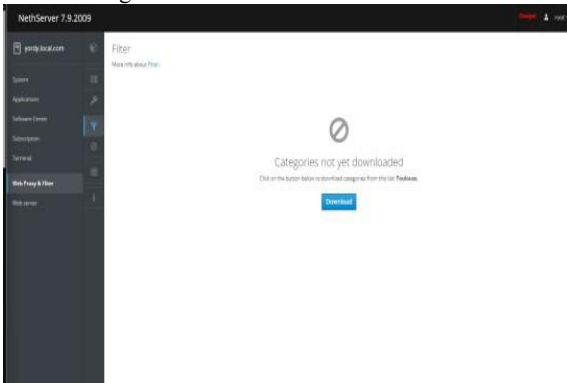
Fuente: Autoría Propia

Figura 57. Ahora ir a la opción categorías como instancia inicial no aparecerán, pero nos sugerirá que si querer descargar. Dar click e iniciara el proceso de descarga.



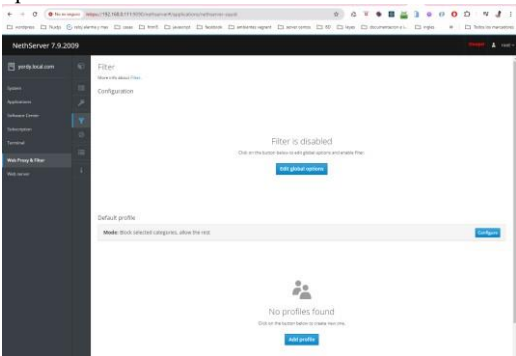
Fuente: Autoría Propia

Figura 58. se ve de esta manera



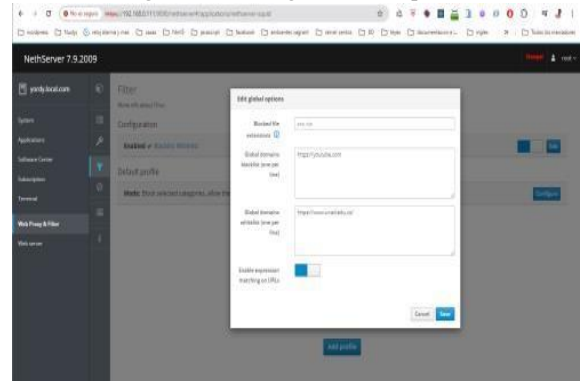
Fuente: Autoría Propia

Figura 59. Ahora dar clic en editar opciones del filtro.



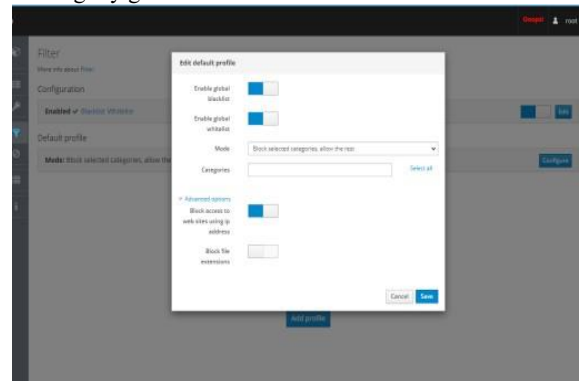
Fuente: Autoría Propia

Figura 60. Configuración del perfil



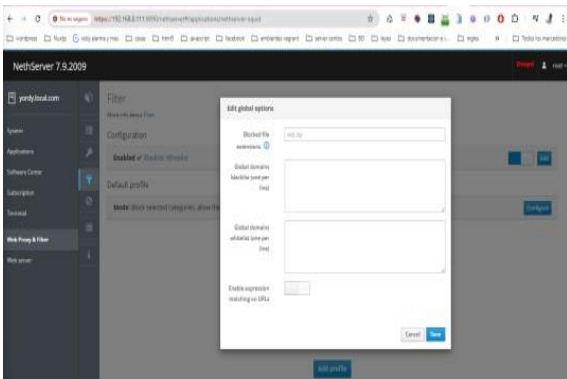
Fuente: Autoría Propia

Figura 61. Ahora se lista las categorías las descargar y guardar.



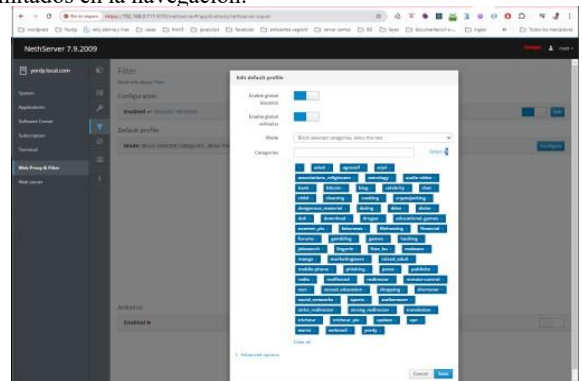
Fuente: Autoría Propia

Figura 60. Agregar algunas listas negras y blancas al filtro.



Fuente: Autoría Propia

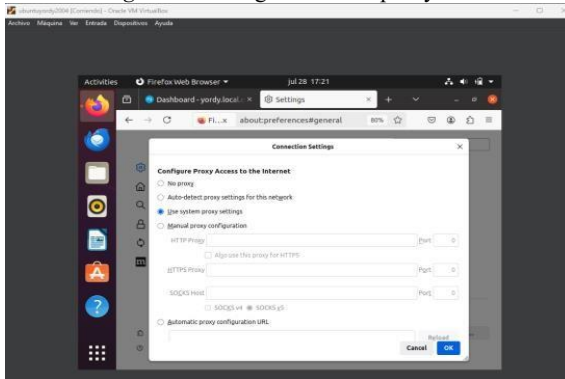
Figura 62. configuración de contenidos para ser limitados en la navegación.



Fuente: Autoría Propia

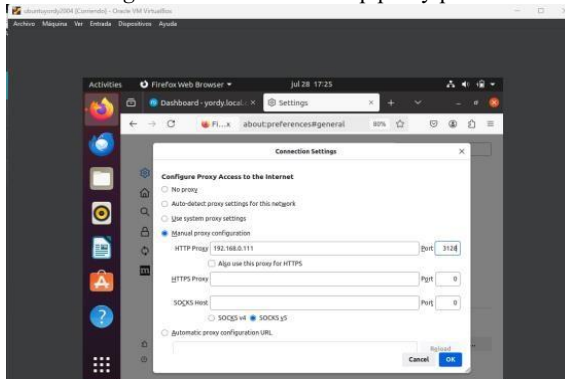
Configurar el proxy en el navegador de nuestro equipo Linux.

Figura 63. configuración del proxy.



Fuente: Autoría Propia

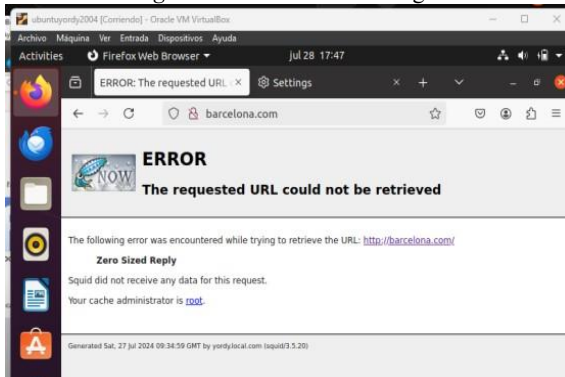
Figura 64. Con dirección ip proxy puerto 3128



Fuente: Autoría Propia

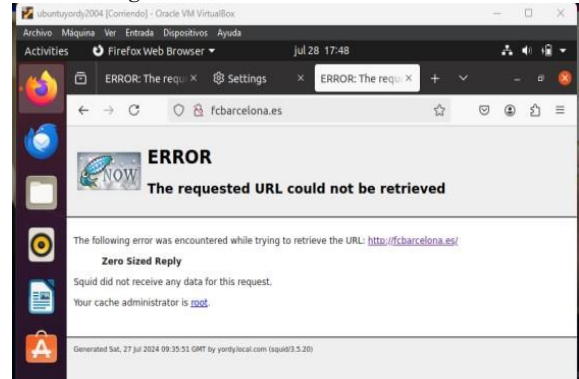
2. La página antes de configurar el proxy que si permite el ingreso y luego la página cuando se configura el proxy.

Figura 65. limitacion de navegación.



Fuente: Autoría Propia

Figura 66. Direccionamiento con error url



Fuente: Autoría Propia

Temática 3:

Cortafuegos ¿Que se busca?

Para esta temática se busca implementar y configurar de forma detallada la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Procedimiento

Ahora se ingresa la dirección IP de net server, en la máquina o escritorio, se obtiene la interfaz de inicio y se procede a configurar el servidor.

Figura 67. Pagina inicial al navegar a la dirección



Fuente: Autoría Propia

Se ingresan las credenciales creadas anteriormente

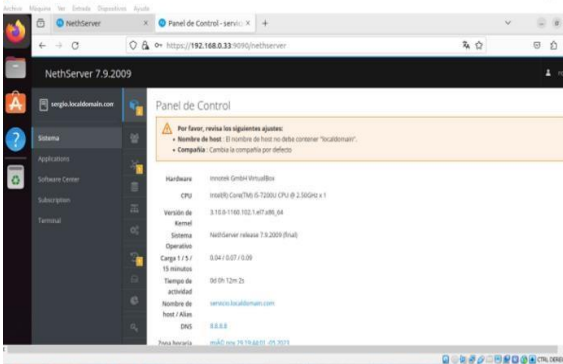
Figura 68 Ingreso de credenciales creadas



Fuente: Autoría Propia

Como pantalla de inicio se observan las características del equipo.

Figura 69. Interfaz de inicio de Nethserver

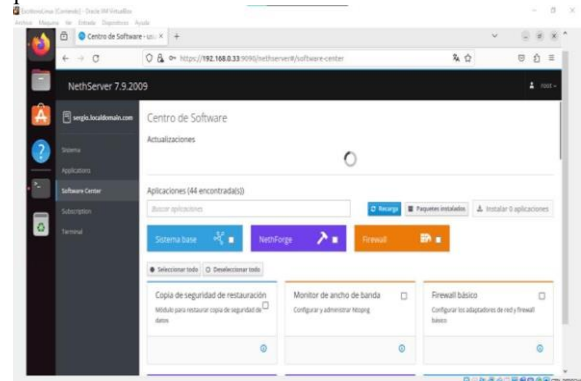


Fuente: Autoría Propia

Descarga de aplicaciones para Firewall y Proxy Filter.

Ahora se accede al centro de software y se actualizan las aplicaciones actuales

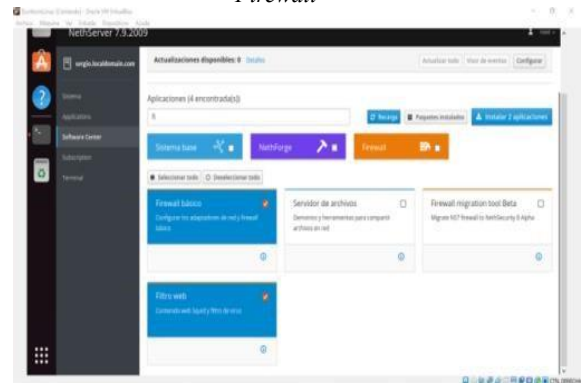
Figura 70. Actualización de paquetes predeterminados



Fuente: Autoría Propia

Luego se hace la búsqueda de las aplicaciones para Firewall que se va a usar

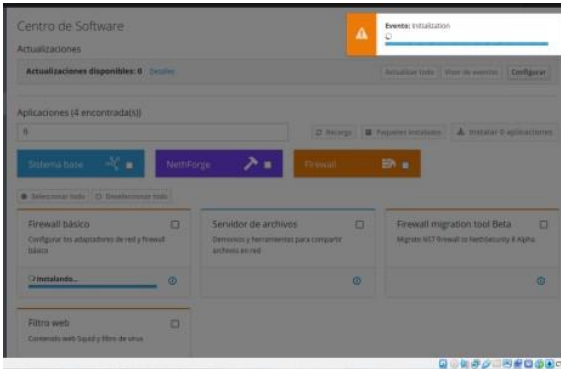
Figura 71. Selección de los paquetes para Firewall



Fuente: Autoría Propia

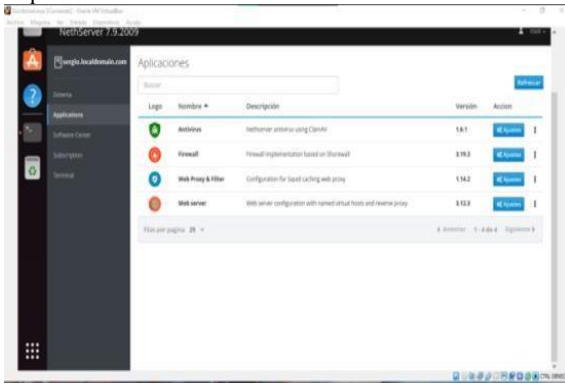
Luego se espera un momento mientras se descargan y después se pueden observar en el apartado de aplicaciones

Figura 72. Listado de aplicaciones necesarias instaladas



Fuente: Autoría Propia

Figura 73. Proceso de instalación de los paquetes requeridos



Fuente: Autoría Propia

En el panel de control del firewall se puede observar la topología de red creada con la Zona Roja la zona verde y la zona naranja

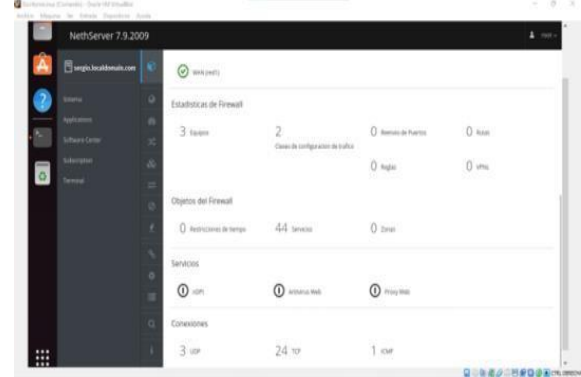
Figura 74. Topología de las zonas creadas



Fuente: Autoría Propia

Así mismo se pueden observar las estadísticas del Firewall actual, así como los servicios que está usando

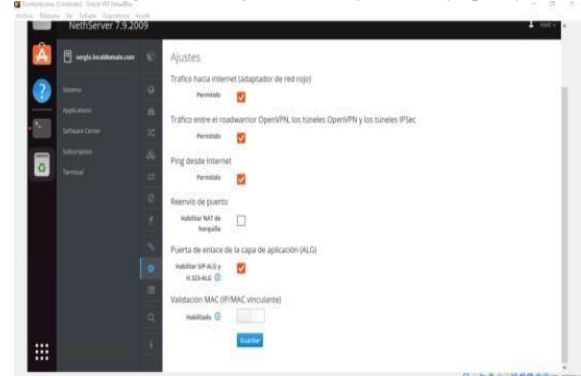
Figura 75. Detalles del proxy web actual



Fuente: Autoría Propia

Para iniciar con la configuración se ingresa a los ajustes y se modifican las siguientes opciones

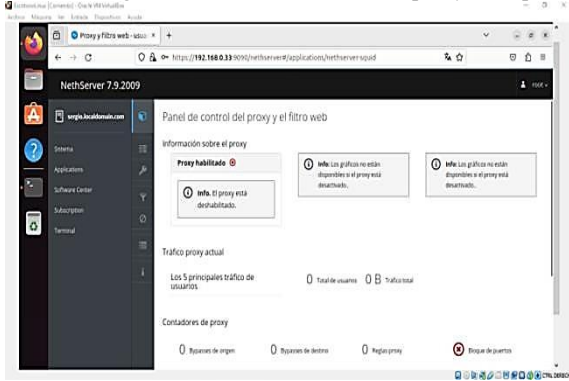
Figura 76. Ajustes del firewall y proxy web



Fuente: Autoría Propia

Para llevar a cabo el bloqueo de páginas es necesario utilizar el Proxy y el filtro web, pero se observa que este está deshabilitado entonces se procede a habilitarlo.

Figura 77. Estado actual del proxy completo

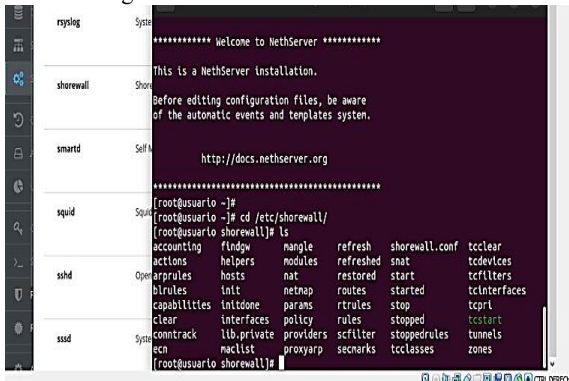


Fuente: Autoría Propia

Políticas y reglas actuales del Firewall

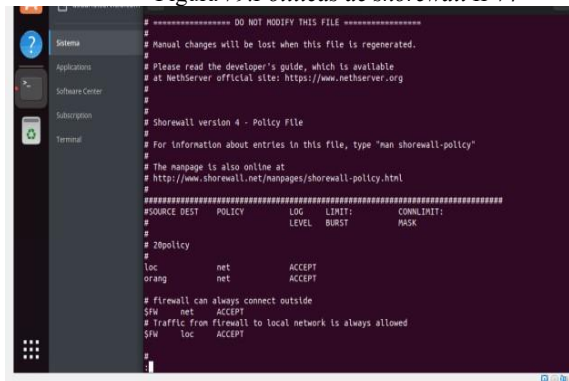
Primero se verifica que los archivos y las políticas de shorewall estén bien configuradas, esto debido a que este es el servicio principal que permitirá configurar el firewall y las reglas correspondientes.

Figura 78. Archivos de shorewall IPv4



Fuente: Autoría Propia

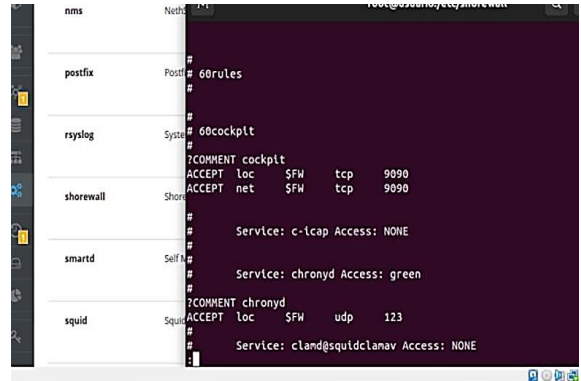
Figura 79. Políticas de shorewall IPv4



Fuente: Autoría Propia

Se observa en la imagen anterior que la política ya está configurada, ahora se visualizan las reglas de cortafuegos.

Figura 80. Reglas actuales configuradas en shorewall.

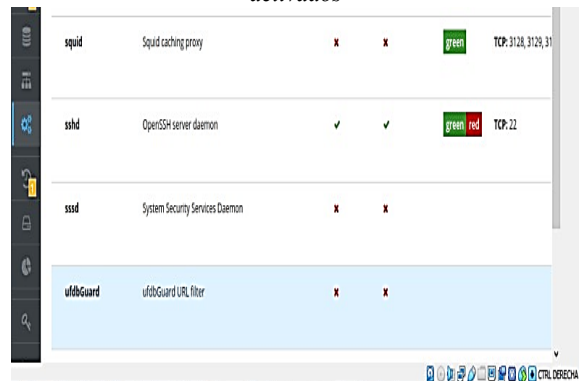


Fuente: Autoría Propia

Se observa en la imagen anterior que la regla de tipo tcp en el puerto 9090 está correctamente configurada para la LAN. Las configuraciones del firewall no son recomendables realizarlas en el modo consola según la web de nethserver, es por ello que se sigue configurando en la interfaz gráfica.

Luego de la instalación de las aplicaciones se observa que el servicio squid esté bien configurado, este Usa los puertos 3128 3291 y 3130 para el filtrado web, ya bien sea para http o https

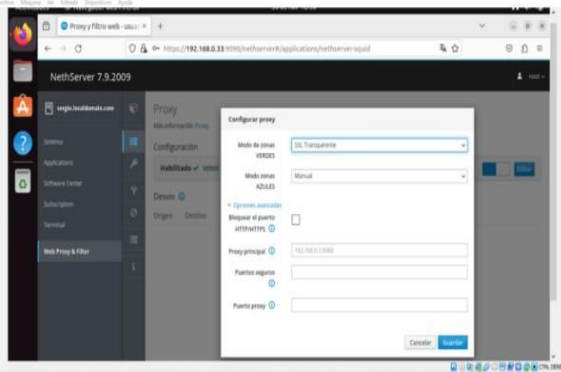
Figura 81. Verificación de los servicios firewall activados



Fuente: Autoría Propia

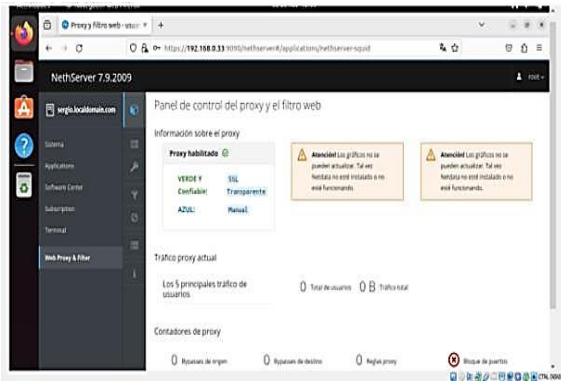
Ahora si se puede proceder a configurar el proxy para luego realizar el filtrado web, se asigna para la zona verde que sea de tipo SSL transparente

Figura 82 .Especificación de proxy para la zona LAN/verde



Fuente: Autoría Propia

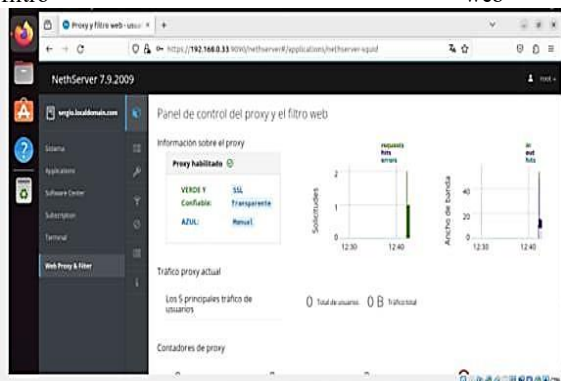
Figura 83. Se activa el servicio netdata



Fuente: Autoría Propia

Se activa el servicio netdata para que haga monitorización en tiempo real y se puede observar que ya existen solicitudes y ancho de banda empleado.

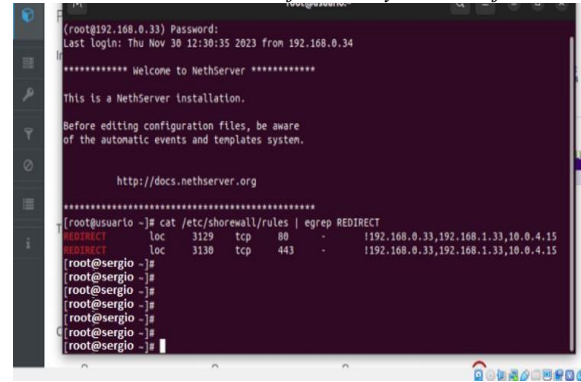
Figura 83. Panel de control de proxy y filtro web



Fuente: Autoría Propia

El uso ya de tráfico es debido a lo siguiente:

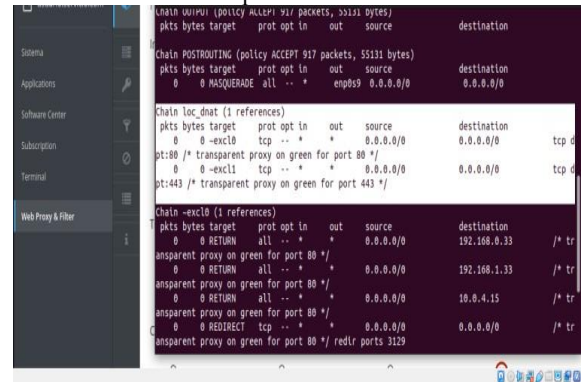
Figura 84. Reglas predeterminadas para la zona naranja y roja



Fuente: Autoría Propia

Se puede observar que ya hay dos reglas activas que son de tipo tcp y hacen uso de los puertos 80by 443 es decir http y https, estos redireccionan a la WAN y la zona naranja (se puede observar la dirección ip de cada una)

Figura 85. Verificación del proxy transparente por consola

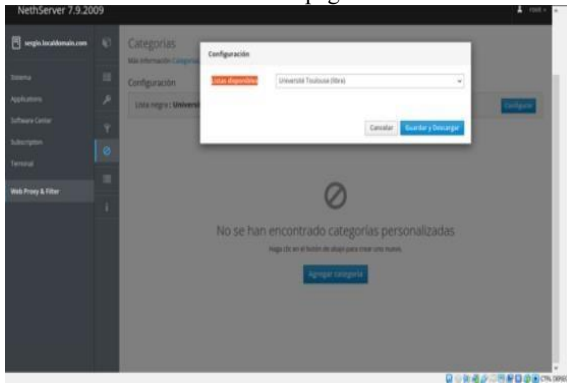


Fuente: Autoría Propia

Configuración de los filtros web

Con todo esto, ahora se van a configurar los filtros web, se ingresa a la pestaña de Categorías y se selecciona la lista Toulouse.

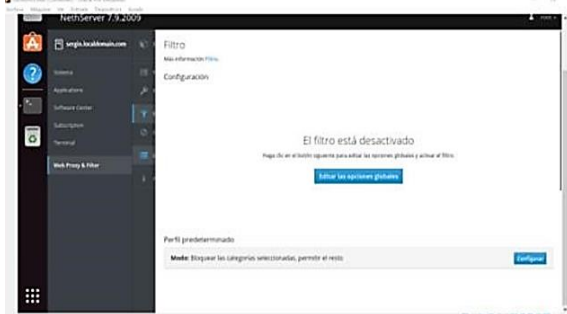
Figura 86. Descarga de la lista Toulouse para filtrado de páginas



Fuente: Autoría Propia

Cuando esta lista finaliza su instalación, ahora se ingresa a la pestaña de filtros y se especifican las extensiones que se quieren filtrar.

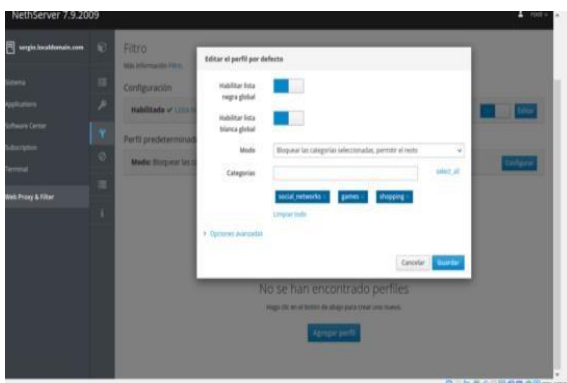
Figura 87. Registro de filtros desactivados



Fuente: Autoría Propia

Ahora se configura el perfil asignando que se bloqueen las categorías especificadas y permita el resto, en este caso se bloquearon los temas relacionados de redes sociales, contenido para adultos y juegos.

Figura 88. Categorías bloqueadas/filtradas de navegación

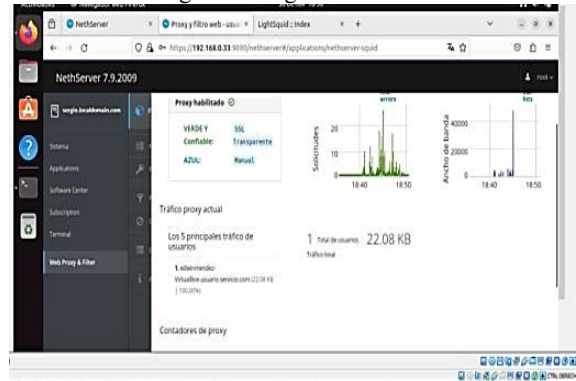


Fuente: Autoría Propia

Al aplicar los cambios se finaliza con la configuración y se observa ahora en la pestaña

principal del firewall que hay un usuario activo en la red creada y estará haciendo uso de estos filtrados.

Figura 89.Registro visual de usuarios.



Fuente: Autoría Propia

Verificación de las páginas web filtradas y permitidas.

También con LightSquid se puede observar los eventos que ocurren por día, el número de usuarios activos entre otros datos.

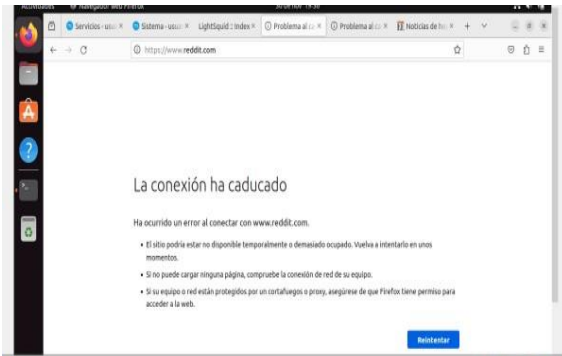
Figura 90 Registro de eventos de lightsquid



Fuente: Autoría Propia

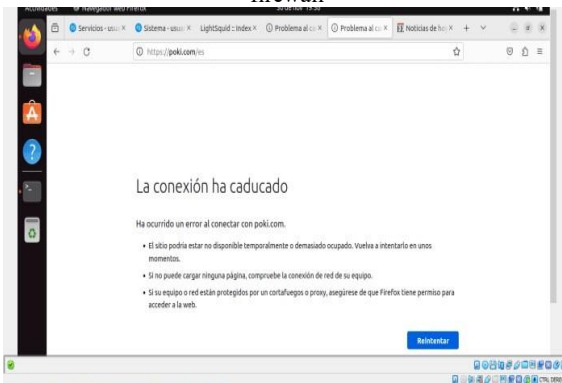
Con todas estas configuraciones ahora se navega a sitios de red social y se observa que son bloqueados, también se navega a páginas de ámbito general y de redes y estas entran sin problema

Figura 91. Pagina Reddit bloqueada por el firewall



Fuente: Autoría Propia

Figura 92. Página de juegos bloqueada por el firewall



Fuente: Autoría Propia

Figura 93. Página de noticias permitida por el firewall



Fuente: Autoría Propia

Figura 94. Pagina de recursos y estudios permitida por el firewall



Fuente: Autoría Propia

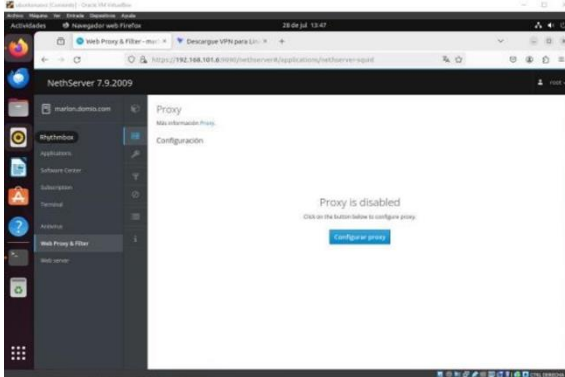
Temática 5: Vpn

Después de la instalación del Nethserver, y la configuración de los adaptadores se realizó la conexión interna y se ingresa por medio del Ubuntu Desktop, a través del navegador Firefox con la IP

192.168.101.6 que arroja la instalación final del Nethserver, se ingresa con el usuario root y contraseña asignada previamente.

Al dar clic sobre la opción Web Proxy & Filer, nos despliega una ventana con las diferentes acciones para configurar el servicio.

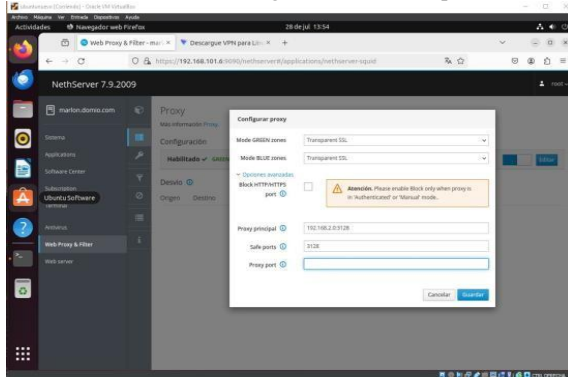
Figura 95. Configuración del proxy



Fuente : Autoría Propia.

Dar clic en el botón azul y se despliega la opciones, seleccionar SSL . Transparente y en el puerto seleccionar 3128.

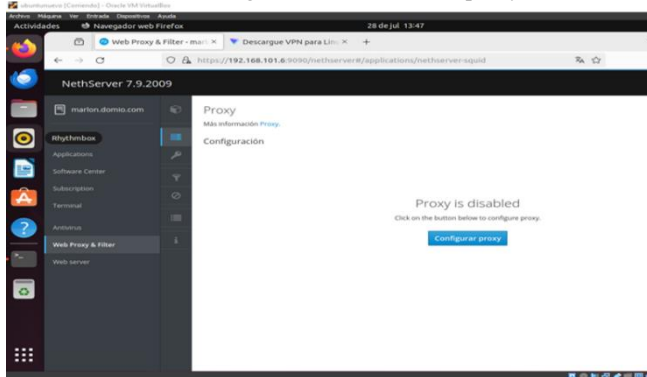
Figura 96. SSL con puerto 3128



Fuente : Autoría Propia.

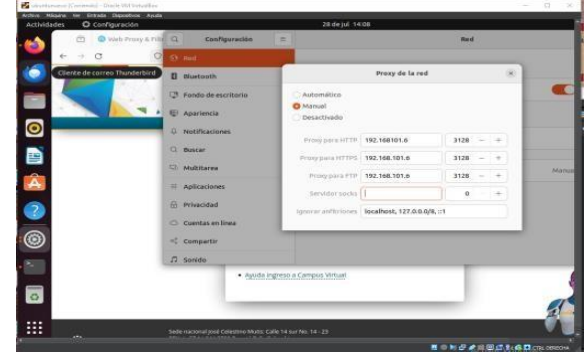
Seleccionar la opción filtro y establecer que restricciones debe controlar el proxy.

Figura 97. Habilitando el proxy.



Fuente : Autoría Propia.

Figura 98. Configurando el proxy con las ip HTTP



Fuente : Autoría Propia.
figura 99. Acceso a internet



Fuente : Autoría Propia.

5. CONCLUSIONES

La implementación y gestión eficiente de servicios específicos con NethServer garantiza un nivel óptimo de seguridad, en la migración de sistemas y la implementación de nueva infraestructura.

En un mundo digital en constante evolución, donde la ciberseguridad es esencial, esta actividad destaca la necesidad de implementar estrategias proactivas para proteger la información y los recursos del sistema. La capacidad de gestionar con precisión el acceso a determinados sitios web contribuye no solo a la seguridad, sino también a la optimización de recursos y al cumplimiento de objetivos laborales.

Cabe destacar que, la segmentación, configuración de reglas de firewall y otras políticas de seguridad en cada zona permite controlar qué tipo de tráfico se permite o se bloquea entre las zonas, contribuyendo a una mayor protección contra amenazas externas e internas, con todo esto contribuyendo a la mejora de la seguridad al limitar el alcance de posibles ataques.

6.REFERENCIAS

[1] LPI LPIC-1 Exam 102. (2022). Tema 110: Seguridad. <https://learning.lpi.org/es/learning-materials/102-500/110/>

[2] Canonical (2018). Guía del Ubuntu desktop 18.04 LTS. Help Ubuntu. <https://help.ubuntu.com/18.04/ubuntu-help/index.html>

[3] Debian (2020). El manual del administrador de Debian 10.04. Debian <https://www.debian.org/doc/manuals/debian-handbook/index.es.html>

[4] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. <https://www.virtualbox.org/manual/>

[5]LPI LPIC-1 Exam 101. (2022). Tema 101: Arquitectura del Sistema. <https://learning.lpi.org/es/learning-materials/101-500/101/>

[6]LPI LPIC-1 Exam 101. (2022). Tema 102: Instalación de Linux y gestión de paquetes. <https://learning.lpi.org/es/learning-materials/101-500/102/>

[7]Canonical (2018). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>

[8]Debian (2020). El manual del administrador de Debian 12.5.0. Debian <https://www.debian.org/releases/stable/amd64/index.es.html>

[9]Oracle (2020). Manual de usuario VirtualBox. VirtualBox. <https://www.virtualbox.org/manual/>

[10]LPI LPIC-1 Exam 102. (2022). Tema 106: Interfaces de usuario y escritorios. <https://learning.lpi.org/es/learning-materials/102-500/106/>