CONFIGURACIÓN Y GESTIÓN DE SERVICIOS DE RED EN LINUX CON NETHSERVER: DHCP, DNS, PROXY, VPN, LDAP.

Julián Andrés Castillo Rodríguez
e-mail: jacastillorod@unadvirtual.edu.co
Johann Andrés Jurado Muñoz
e-mail: jajuradom@unadvirtual.edu.co
Johnny Andrés Ibarra Diago
e-mail: jaibarrad@unadvirtual.edu.co
Héctor Fabián Pinto Ospina
e-mail: hfpintoo@unadvirtual.edu.co

RESUMEN: *Este paso se enfocó en trabajar en NETHSERVER, una distribución que ofrece distintos servicios para administrar la red corporativa, y para esta actividad final se pretende dar soluciones específicas en servidores DHCP, controladores de dominio para clientes, configuración DNS, configuración de proxy, cortafuegos, file server y print server a través del controlador de dominio LDAP, VPN. De esta forma se inicia con la instalación y configuración de NETHSERVER en el VirtualBox configurando tres adaptadores de red, red WAN, red verde (conexiones para clientes), red naranja (red desmilitarizada), por lo general las conexiones a la red verde desde el cliente Ubuntu es para conectividad de internet y realización de pruebas funcionales en el panel de control del NETHSERVER*

PALABRAS CLAVE: Proxy, servidor DHCP, servidor DNS, VPN.

1 INTRODUCCIÓN

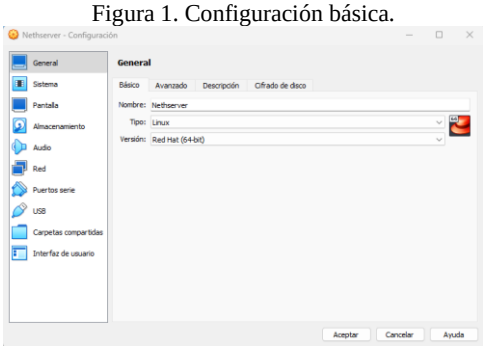
En el artículo que se presenta a continuación, abordaremos la instalación y configuración de NethServer como eje principal, para dar solución a las diferentes necesidades de servicios, que se pueden presentar en entornos Linux. Esto es de vital importancia debido a que se trata de servicios, que en la gran mayoría de los casos son esenciales en las áreas de TI, para el funcionamiento de las mismas y como servicios que se brindan a los usuarios finales. En una primera instancia nos centraremos en la instalación y configuración de NethServer, para luego abordar la configuración de servicios como el DHCP, el Proxy, el Firewall, etc. Todo esto, apoyado siempre con material gráfico, que facilitara el entendimiento de cada uno de los procesos y configuraciones realizadas.

2 SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

2.1 INSTALACIÓN DE NETHSERVER

Una vez se descargamos la imagen ISO, lo montamos en VirtualBox, damos el nombre de la maquina “Nethserver”, seleccionamos la imagen ISO a montar, en Tipo, seleccionamos “Linux” y Versión Red Hat (64-bit).

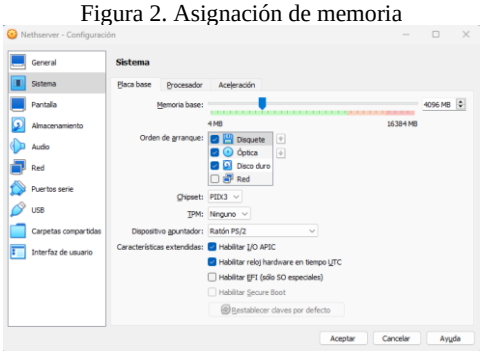
Figura 1. Configuración básica.



Fuente: Autoría propia

Asignamos lo recursos de hardware, Memoria base (RAM) 8192 MB, en procesadores seleccionamos 2.

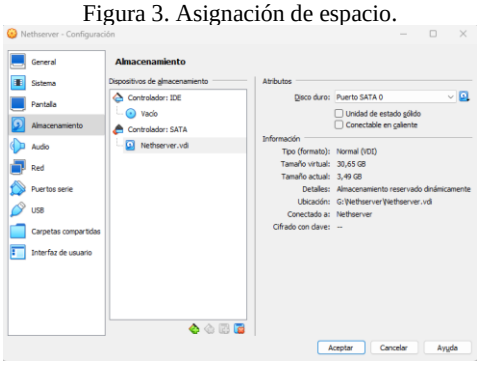
Figura 2. Asignación de memoria



Fuente: Autoría propia

Asignamos 31.53GB de espacio de disco.

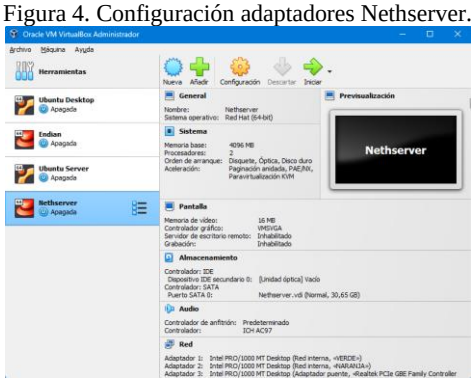
Figura 3. Asignación de espacio.



Fuente: Autoría propia

Configuramos la zona DMZ, estando en VirtualBox antes de ejecutar las distribuciones establecemos los adaptadores de red de Nethserver: adaptador 1, red interna "VERDE", en adaptador 2, Red interna "NARANJA" y en adaptador 3 NAT.

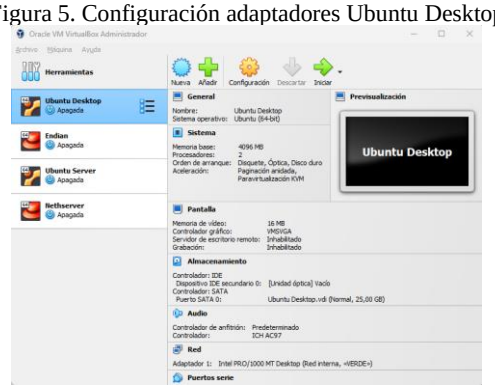
Figura 4. Configuración adaptadores Nethserver.



Fuente: Autoría propia

En Ubuntu Desktop, configuramos el adaptador 1 en red interna "VERDE".

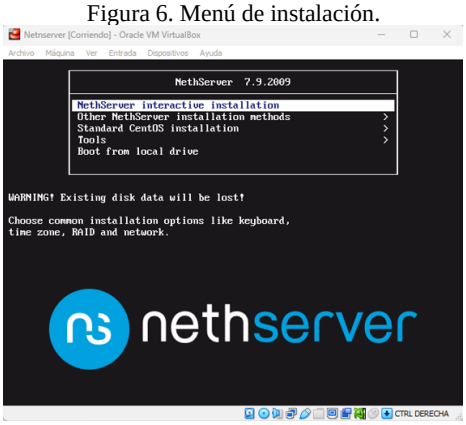
Figura 5. Configuración adaptadores Ubuntu Desktop



Fuente: Autoría propia

Ejecutamos la maquina Nethserver dando clic en Iniciar. Después seleccionamos la opción "Nethserver interactive installation".

Figura 6. Menú de instalación.



Fuente: Autoría propia

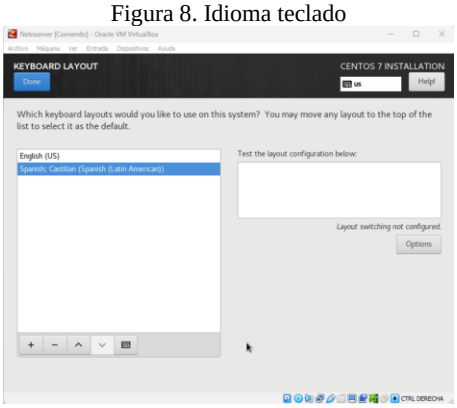
Configuramos la zona horaria.

Figura 7. Ubicación y tiempo.

Fuente: Autoría propia

Configuramos idioma del teclado

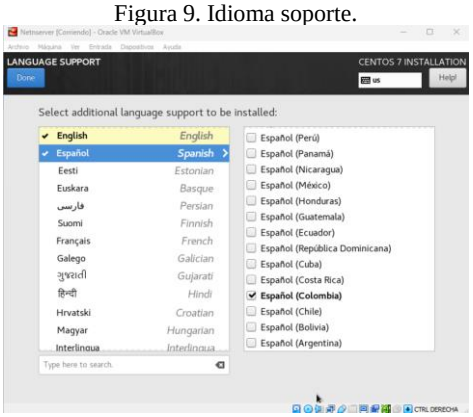
Figura 8. Idioma teclado



Fuente: Autoría propia

Configuramos el idioma de soporte de la distribución a instalar.

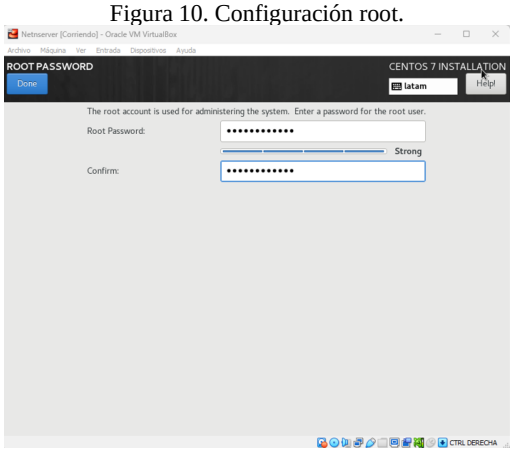
Figura 9. Idioma soporte.



Fuente: Autoría propia

Modificamos la contraseña para el usuario root.

Figura 10. Configuración root.



Fuente: Autoría propia

Creamos la cuenta para el usuario invitado asignando un nombre y una contraseña.

Figura 11. Configuración Usuario.

Fuente: Autoría propia

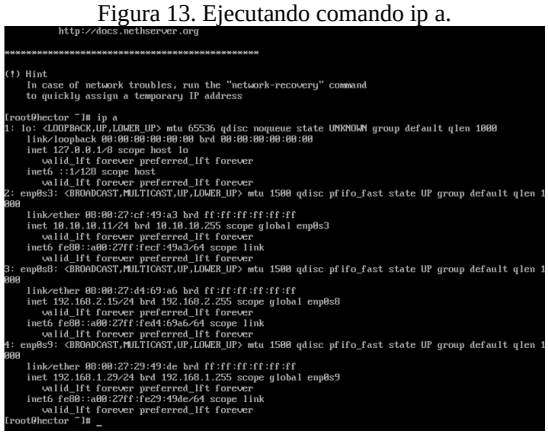
Iniciamos la instalación

Figura 12. Instalación Nethserver.

Fuente: Autoría propia

Ingresamos con el usuario root y contraseña para empezar a usar el servidor Nethserver. Digitamos el comando ip a para ver la dirección IP que nos permitirá conectarnos en el equipo anfitrión por https://192.168.1.29:9090/.

Figura 13. Ejecutando comando ip a.



Fuente: Autoría propia

2.1.1 CONFIGURACION NETHSERVER

Una vez hemos digitado el enlace de acceso, nos va a pedir el usuario root y la contraseña.

Figura 14. Acceso a Nethserver.

Fuente: Autoría propia

Una vez hemos ingresado, registramos un nombre de dominio y empresa u organización.

Figura 15. Cambiando nombre host y organización.

Fuente: Autoría propia

A la red interna verde establecemos una dirección estática 10.10.10.11 con mascara de red 255.255.255.0.

Figura 16. Configurando red verde.

Fuente: Autoría propia

En el adaptador 3 NAT (ROJO), establecemos una red IP 192.168.1.29 y esta debe ser estática, con mascara de red 255.255.255.0 y puerta de enlace 192.198.1.1.

Figura 17. Configurando red NAT.

Fuente: Autoría propia

En la red interna NARANJA se establece una dirección IP dinámica 192.168.2.15 con mascar de subred 255.255.255.0.

Figura 18. Configurando DMZ.

Fuente: Autoría propia

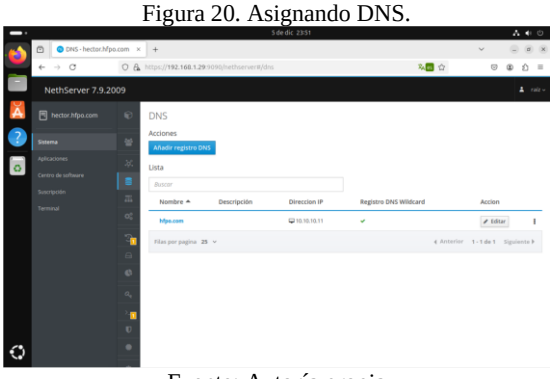
En la opción de servidor DHCP, lo activamos para establecer conexión con el equipo anfitrión.

Figura 19. Activando DHCP.

Fuente: Autoría propia

Agregamos los DNS 8.8.8.8 y 1.1.1.1 estos proporcionados por Google y Cloudflare.

Figura 20. Asignando DNS.



Fuente: Autoría propia

2.2 CONFIGURACION SERVIDOR DHCP

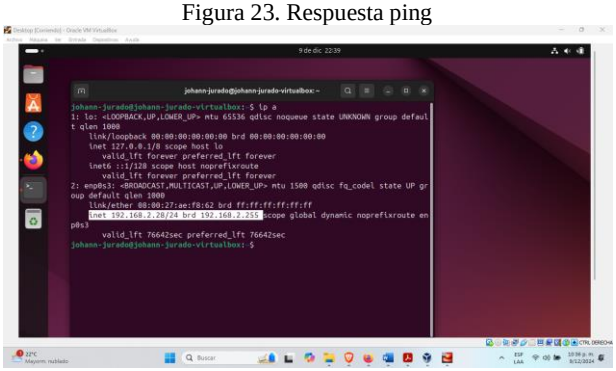
Para configurar el servidor DHCP inicialmente parte del rango inicial y final que se asignó en la red LAN, en este caso se asigna IP de la Puerta de enlace de la zona verde.

Figura 22. Configuración rango DHCP

Fuente: Autoría propia.

Después de aplicar cambios se inicia el servicio y en el escritorio cliente validamos que asigne IP dentro del rango permitido.

Figura 23. Respuesta ping

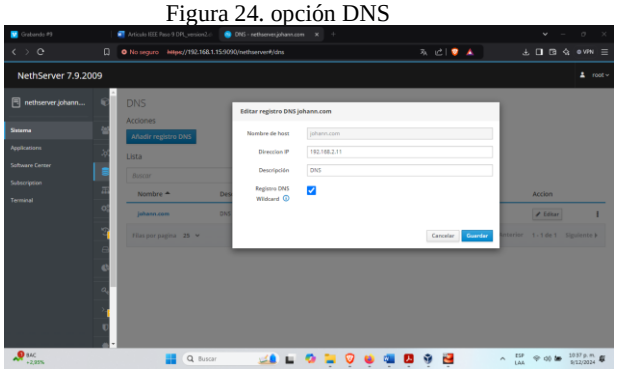


Fuente: Autoria propia.

2.2.1 CONFIGURACION DNS

la configuración DNS se hace dentro de la red LAN, zona verde con la IP 192.168.2.11, nombre de dominio johann.com

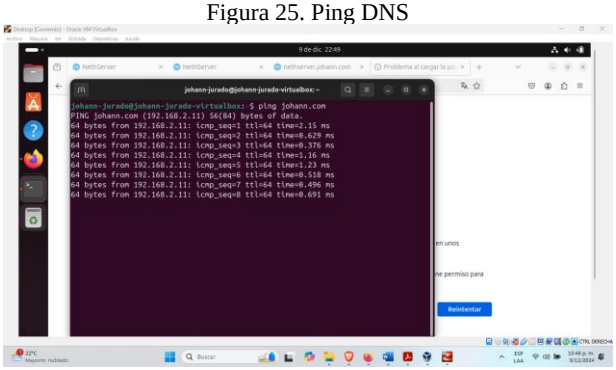
Figura 24. opción DNS



Fuente: Autoria propia.

Se valida DNS en el escritorio Ubuntu haciendo ping johann.com.

Figura 25. Ping DNS

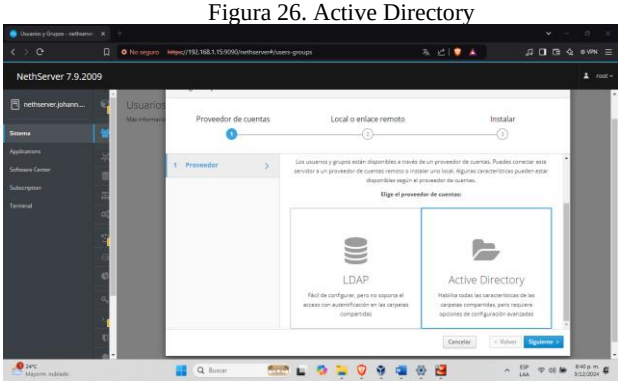


Fuente: Autoría propia

2.2.2 CONFIGURACION CONTROL DE DOMINIO

Se configura Active Directory en la sección de usuario y grupos, asignando IP dentro de la red LAN, paso siguiente créate domain.

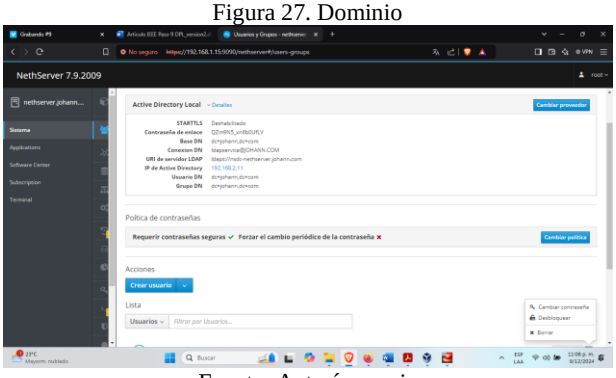
Figura 26. Active Directory



Fuente: Autoría propia

Al final de la configuración se crea usuario cliente dominio, johann.jurado.

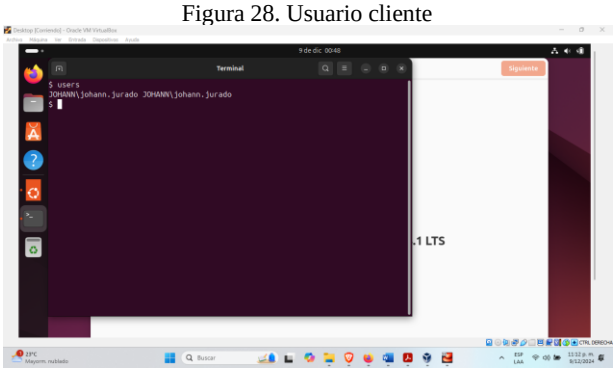
Figura 27. Dominio



Fuente: Autoría propia

Se valida el dominio creado ingresando al usuario en la terminal cliente Ubuntu.

Figura 28. Usuario cliente



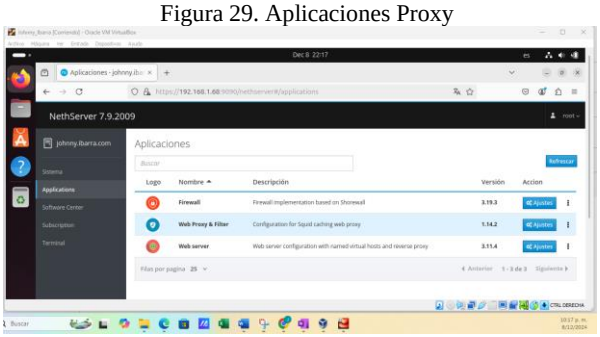
Fuente: Autoría propia

2.3 CONFIGURACIÓN DEL PROXY

Para realizar el correcto funcionamiento del Proxy debemos descargar una serie de aplicaciones las cuales nos ayudaran con los permisos ya que actúa como intermediario en la red, gestionando las conexiones de los clientes y aplicando políticas como el bloqueo de publicidad. El puerto 3128 es el canal específico que el proxy utiliza para recibir y manejar las solicitudes para esto se requiere de las siguientes aplicaciones:

Firewall, Web Proxy & Filter, Web Server.

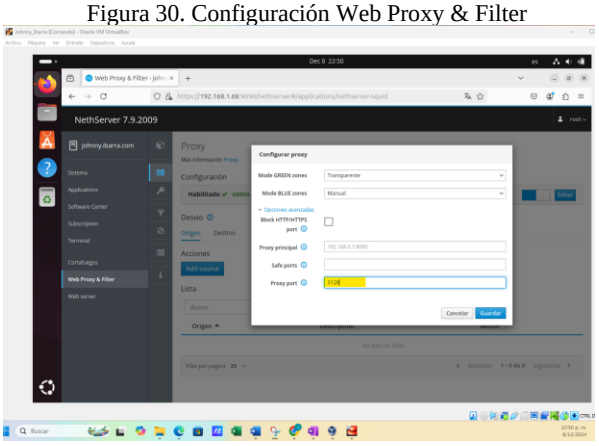
Figura 29. Aplicaciones Proxy



Fuente: Autoría propia

Habilitamos y Configuramos las zonas verdes como Transparente y zonas azules como Manuales y nuestro Proxy con puerto 3128.

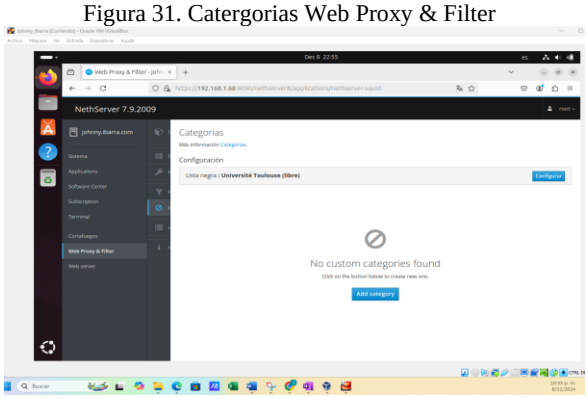
Figura 30. Configuración Web Proxy & Filter



Fuente: Autoría propia

Configuramos la lista Negra en la opción de Categoría. De ser necesario se descargan los paquetes correspondientes para que se parametrice la Lista Negra de la Universidad de Tolouse para bloquear las publicidades en el sitio web.

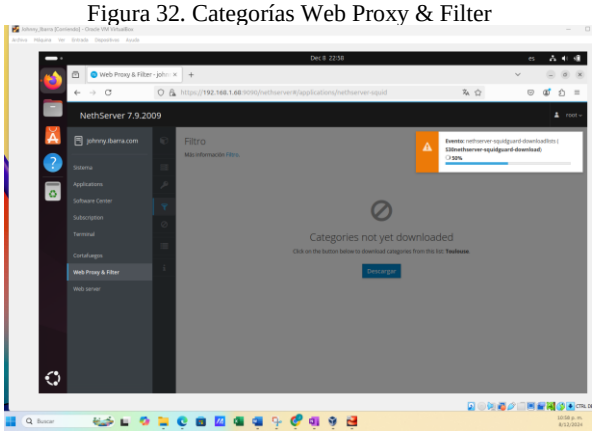
Figura 31. Catergorias Web Proxy & Filter



Fuente: Autoría propia

Es necesario descargar los filtros correspondientes a la lista Negra de la Universidad de Tolouse.

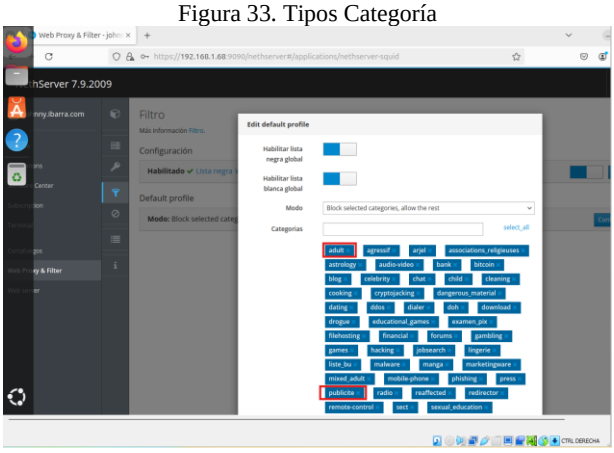
Figura 32. Categorías Web Proxy & Filter



Fuente: Autoría propia

Procedemos con el bloqueo de cualquier anuncio en formato mp3 o mp4 y procedemos con el bloqueo de los tipos de contenido ya sean de adultos, publicidad entre otros.

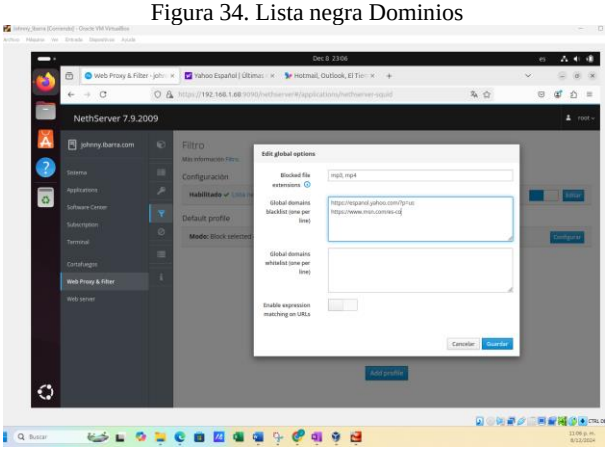
Figura 33. Tipos Categoría



Fuente: Autoría propia

El paso siguiente es listar los dominios a los cuales les aplicará la configuración del Proxy con puerto 3128.

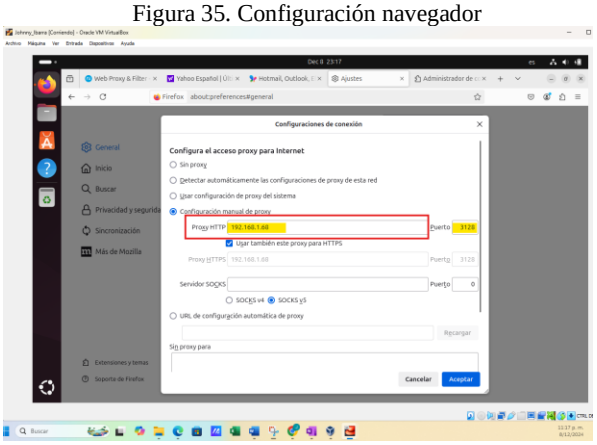
Figura 34. Lista negra Dominios



Fuente: Autoría propia

La validación en nuestro navegador se encuentra alojada en la opción configuraciones de Conexión donde agregaremos el puerto 3128 y la IP que origina la solicitud desde el Proxy NethServer.

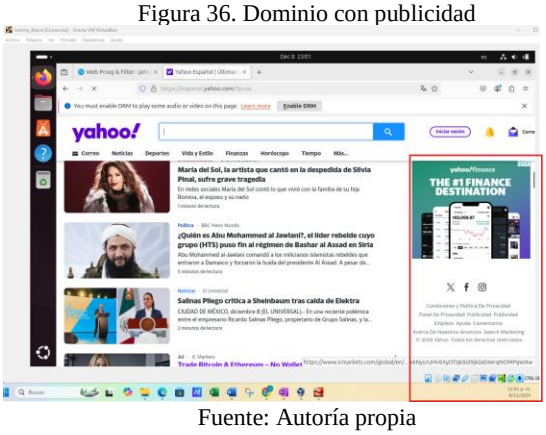
Figura 35. Configuración navegador



Fuente: Autoría propia

Vamos a colocar en lista negra 1 página de correo electrónico que muestra varios anuncios para eliminarlos.

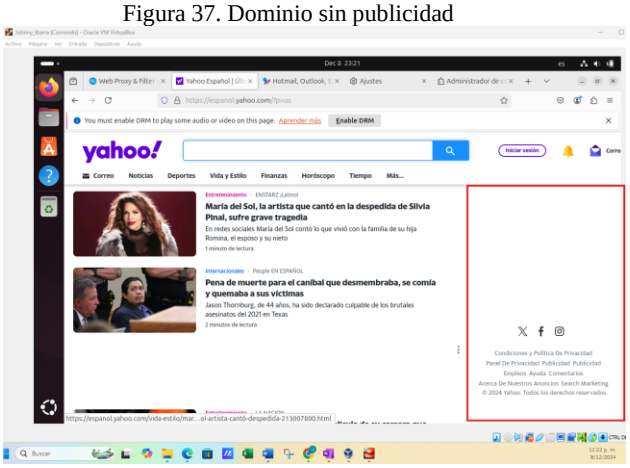
Figura 36. Dominio con publicidad



Fuente: Autoría propia

Actualizamos nuestro navegador para garantizar que se halla implementado los ajustes de puerto 3128, en la cual no se deben mostrar ni contenido no deseado como las publicidades.

Figura 37. Dominio sin publicidad

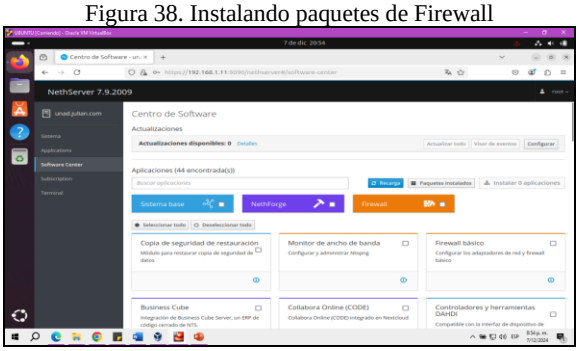


Fuente: Autoría propia

2.4 CONFIGURATION DEL FIREWALL

Para la implementación del Firewall, lo primero que deberemos hacer, es realizar la instalación del aplicativo y para ello nos dirigimos a al centro de software desde donde podremos realizar la instalación de los paquetes.

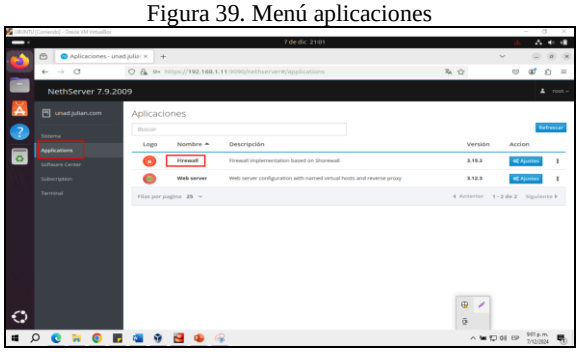
Figura 38. Instalando paquetes de Firewall



Fuente: Autoría propia

Cuando finalice la instalación del Firewall, podemos ir al menú aplicaciones y evidenciaremos que ya se encuentra disponible.

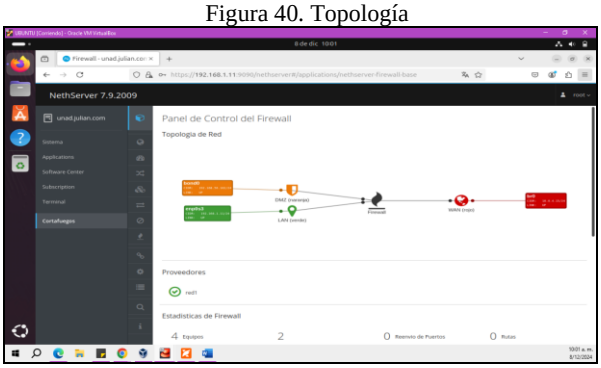
Figura 39. Menú aplicaciones



Fuente: Autoría propia

Al entrar en la entrar en la configuración del Proxy, se nos mostrara de manera gráfica, la forma en que ha quedado estructurado.

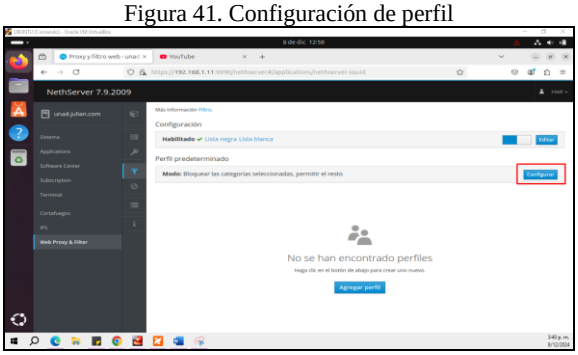
Figura 40. Topología



Fuente: Autoría propia

Antes de crear las reglas en el Firewall, es importante que en la configuración del proxy establezcamos un perfil para el bloqueo de las categorías solicitadas. Para ello y teniendo en cuenta que el punto anterior ya realizamos la configuración del Proxy, nos vamos a dirigir directamente al menú de "Filtro" en el Proxy.

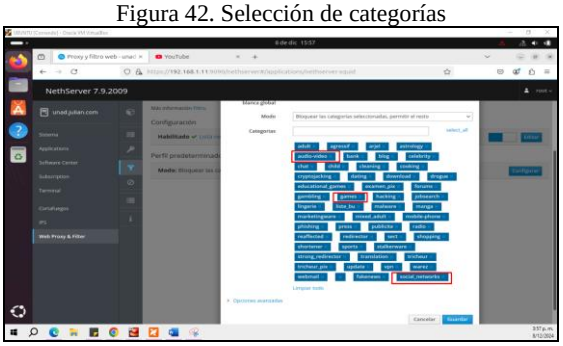
Figura 41. Configuración de perfil



Fuente: Autoría propia

En el menú de "Listas Negras" procedemos a seleccionar las categorías solicitas y las que se encuentren relacionadas.

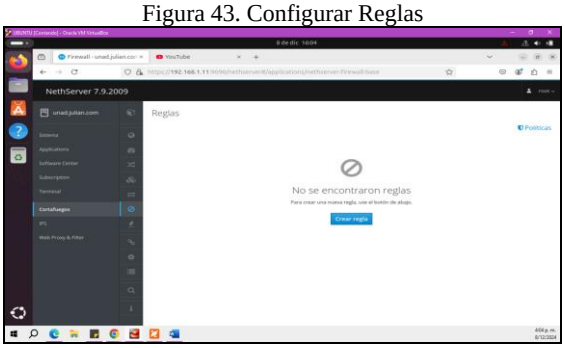
Figura 42. Selección de categorías



Fuente: Autoría propia

Ahora que hemos configurado el perfil en el proxy, nos podremos dirigir de nuevo al menú de Firewall donde nos dirigiremos a la opción reglas, para realizar la parametrización del bloqueo.

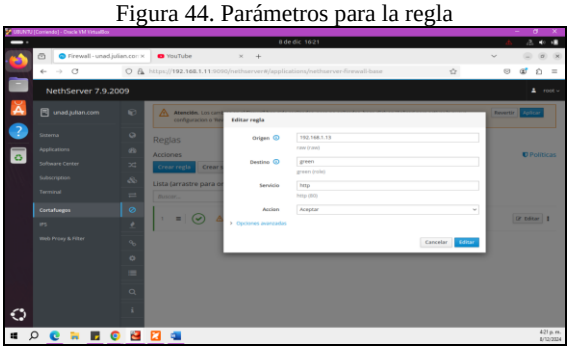
Figura 43. Configurar Reglas



Fuente: Autoría propia

Entramos en el menú Reglas, donde se nos presentara la siguiente ventana. Seguidamente deberemos diligenciar todos los campos, de acuerdo con las siguientes indicaciones. En el campo origen, podremos establecer un bloque de toda la red, hasta un segmento o como en nuestro caso que escribiremos la IP del equipo que vamos a filtrar. En el Destino debemos seleccionar nuestra red interna, ya que el tráfico deberá ir hacia el Proxy que hemos configurado. Por último, el servicio deberá ser http y https y la acción deberá ser Permitir, pues estamos configurando la regla para que el tráfico pase a través del proxy.

Figura 44. Parámetros para la regla



Fuente: Autoría propia

Al guardar los cambios en el punto anterior, se nos presentara un resumen de la regla que acabamos de configurar y solo bastara con presionar el botón "Aplicar" para que se empiece a ejecutar la regla. Es importe tener en cuenta que en los equipos que se va a realizar el filtrado, se debe realizar la configuración del proxy, estableciendo la dirección IP que establecimos para NethServer.

Figura 45. Aplicar la regla

Fuente: Autoría propia

2.5 CONFIGURATION FILE SERVER Y PRINT SERVER

Instalación de paquetes File Server y Print Server, ingresamos a “Centro de software” y en el buscador hacemos llamado de los paquetes a instalar.

Figura 46. Instalando paquetes.

Fuente: Autoría propia

Configuración e instalación de controlador de domino LDPA a los servicios de carpetas compartidas. Damos Clic en LDAP y Clic en siguiente.

Figura 47. Instalando servicio LDAP.

Fuente: Autoría propia

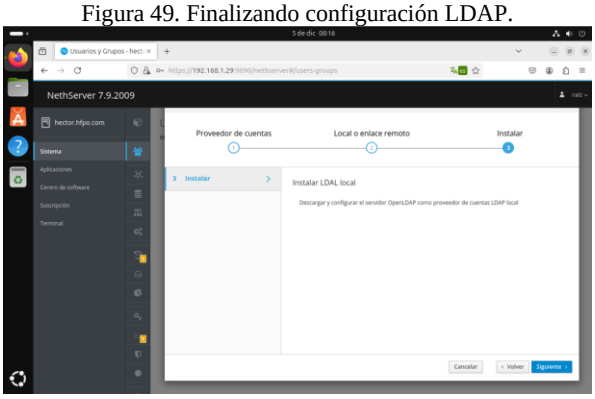
Damos clic en “Instalar LDAL local” y clic en “Siguiente”.

Figura 48. Configurando acceso remoto.

Fuente: Autoría propia

Damos clic en “Siguiente” para descargar y configurar el servidor OpenLDAP como proveedor de cuentas LDAP local.

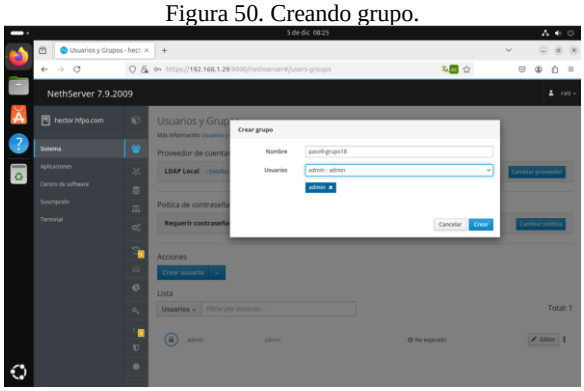
Figura 49. Finalizando configuración LDAP.



Fuente: Autoría propia

En Acciones desplegamos la flecha y damos clic en la opción de “Crear grupo” y le damos un nombre al grupo para los Usuarios que trae por defecto (admin-admin). Clic en “Crear”.

Figura 50. Creando grupo.



Fuente: Autoría propia

Pasamos a crear un usuario asignándolo al grupo creado. Clic en crear.

Figura 51. Creando usuario.

Fuente: Autoría propia

Vamos a la opción de “Aplicaciones” y en File server vamos a dar clic en “Ajustes”.

Figura 52. Acceso a configuración File server.

Fuente: Autoría propia

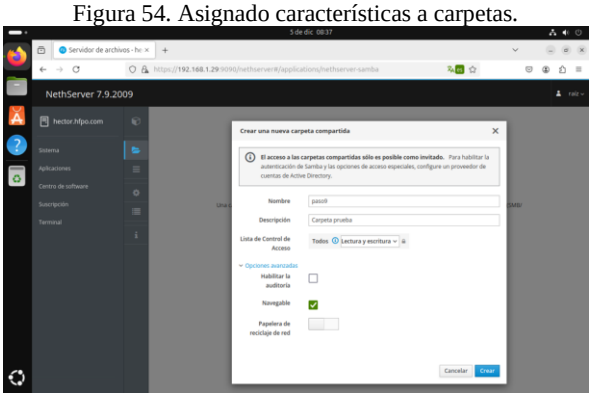
Damos clic en “Crear una carpeta compartida”.

Figura 53. Creando carpetas compartidas.

Fuente: Autoría propia

Damos un nombre a la carpeta compartida, una breve descripción de lo que es, en lista y control de acceso le damos permisos de lectura y escritura. Clic en Crear.

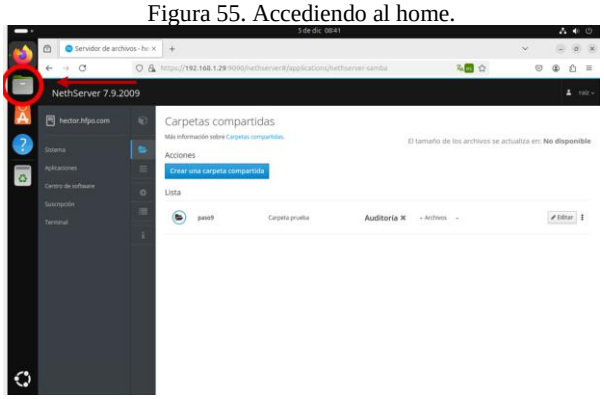
Figura 54. Asignado características a carpetas.



Fuente: Autoría propia

Una vez hemos creado la carpeta compartida, damos clic en archivos desde el equipo local Ubuntu Desktop.

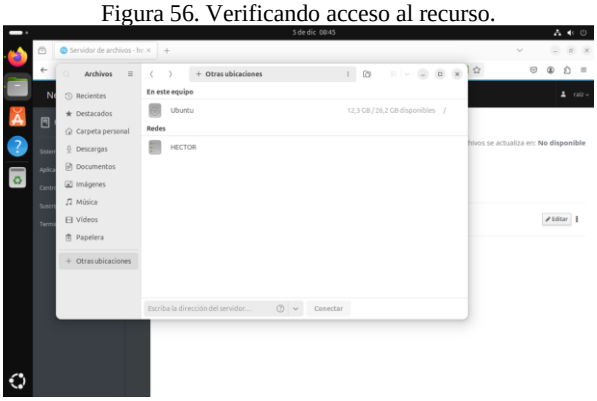
Figura 55. Accediendo al home.



Fuente: Autoría propia

Damos clic en “+ Otras ubicaciones” y en Redes podemos visualizar una carpeta con mi nombre de usuario, damos clic para abrir.

Figura 56. Verificando acceso al recurso.



Fuente: Autoría propia

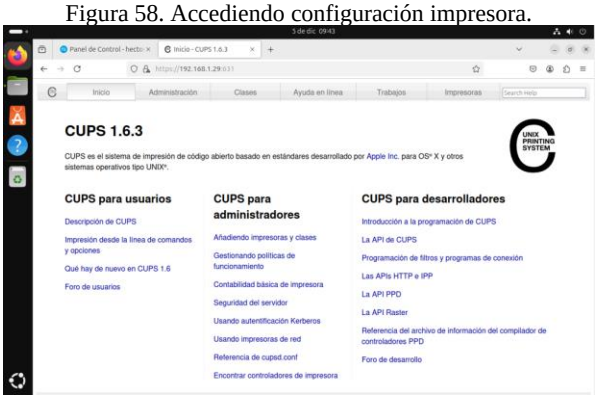
Aquí podemos visualizar que las carpetas compartidas han sido creadas satisfactoriamente.

Figura 57. Carpetas compartidas creadas.

Fuente: Autoría propia

Accedemos a configurar la impresora en nethserver desde la dirección IP asignada pero esta vez utilizando el puerto 631 así: https://192.168.1.29:631/.

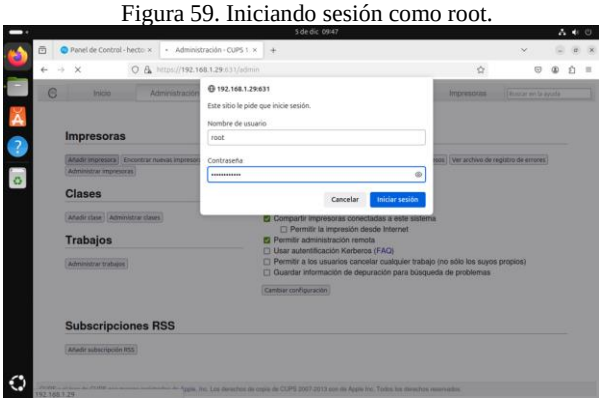
Figura 58. Accediendo configuración impresora.



Fuente: Autoría propia

Damos clic en la pestaña de administración y luego en Añadir impresora, nos va a solicitar que iniciemos sesión con nuestra cuenta. Clic en iniciar sesión.

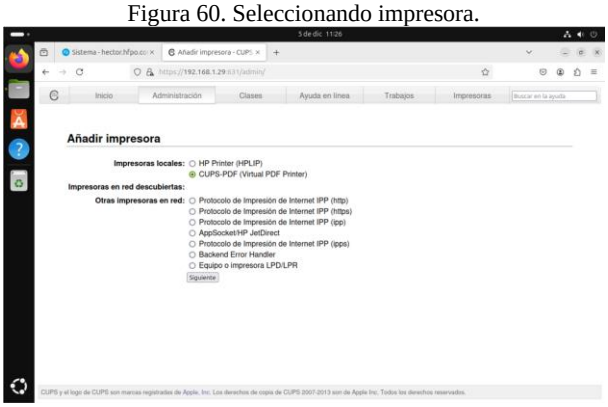
Figura 59. Iniciando sesión como root.



Fuente: Autoría propia

Seleccionamos una impresora de red virtual en este caso seleccioné CUPS-PDF (Virtual PDF Printer). Clic en siguiente.

Figura 60. Seleccionando impresora.



Fuente: Autoría propia

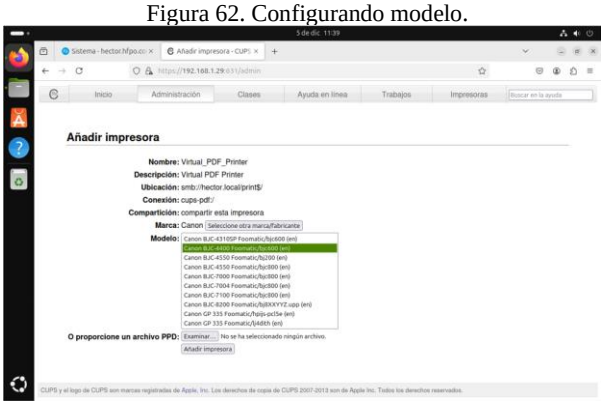
Damos un nombre a la impresora, descripción y la ubicación donde se redirigen las pruebas de impresión. Clic en siguiente.

Figura 61. Añadiendo características.

Fuente: Autoría propia

Buscamos una marca y modelo para nuestra impresora. Clic en añadir impresora

Figura 62. Configurando modelo.



Fuente: Autoría propia

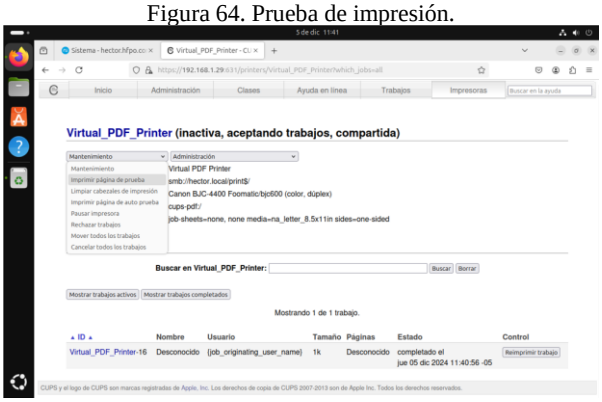
Realizamos ajustes de diseño y salida de la impresión si es necesario.

Figura 63. Estableciendo opciones de impresión.

Fuente: Autoría propia

Nos dirigimos a administrar impresoras y vamos a imprimir una página de prueba, para verificar la conexión, vemos que el trabajo fue completado con éxito.

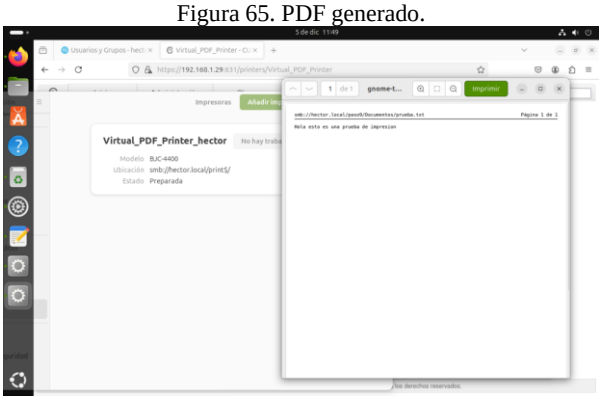
Figura 64. Prueba de impresión.



Fuente: Autoría propia

Ahora realizamos una prueba de impresión a la impresora configurada desde Ubuntu Desktop.

Figura 65. PDF generado.



Fuente: Autoría propia

2.6 INSTALACIÓN Y CONFIGURACIÓN VPN

En centro de software, vamos a buscar OpenVPN. Clic en instalar 1 aplicación.

Figura 66. Instalando paquete.

Fuente: Autoría propia

Creamos una cuenta de usuario LDAP para permitir a este usuario tener acceso a la VPN por medio de una autenticación.

Figura 67. Creando cuenta de usuario.

Fuente: Autoría propia

Nos dirigimos a “Aplicaciones” y vemos que ya tenemos instalado VPN. Clic en Ajustes.

Figura 68. Accediendo a ajustes VPN.

Fuente: Autoría propia

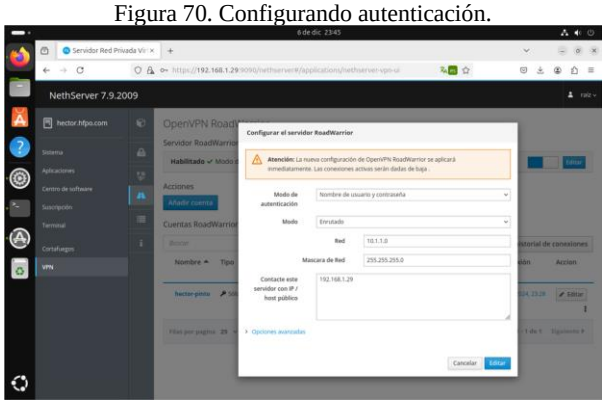
Vamos a la opción de “OpenVPN RoadWarrior” y damos clic en “Habilitar el servidor OpenVPN RoadWarrior”.

Figura 69. Habilitando servicio VPN.

Fuente: Autoría propia

En modo de autenticación vamos a elegir “Certificado”, modo “Enrutado”, para la red definí la 10.1.1.0, mascara de red 255.255.255.0, cambiamos también la IP publica por 192.168.1.19 correspondiente a mi red WAN (ROJA). Clic en guardar.

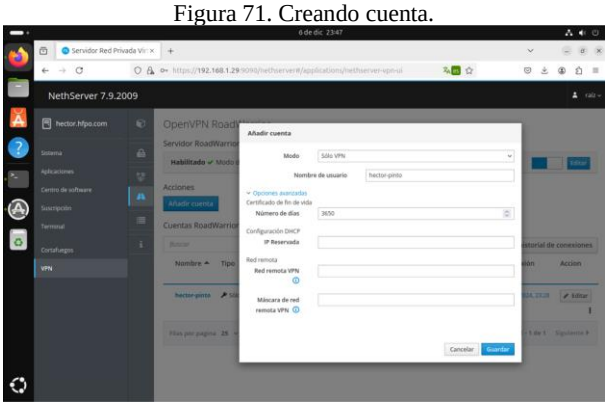
Figura 70. Configurando autenticación.



Fuente: Autoría propia

Una vez se configure OpenVPN RoadWarrior vamos a dar clic en “Añadir cuenta”, en el modo vamos a dejar “Sólo VPN”, damos el nombre de usuario. Clic en “Guardar”.

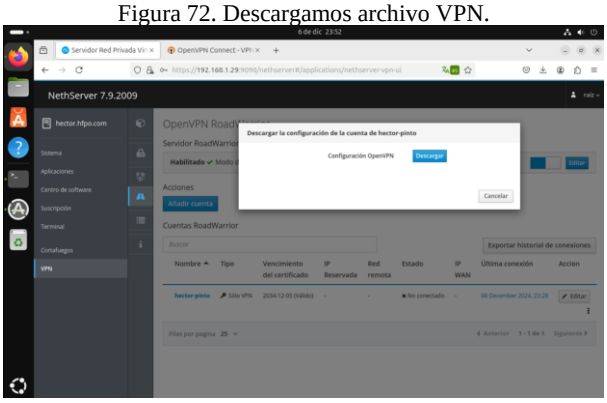
Figura 71. Creando cuenta.



Fuente: Autoría propia

Descargamos la configuración para cuenta OpenVPN.

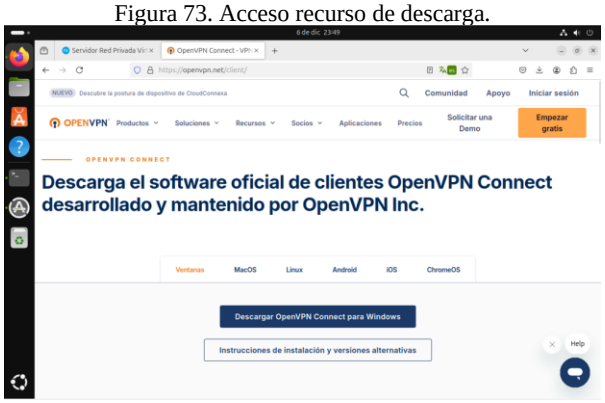
Figura 72. Descargamos archivo VPN.



Fuente: Autoría propia

Ingresamos a la página https://openvpn.net/client/, desde vamos a descargar OpenVPN.

Figura 73. Acceso recurso de descarga.



Fuente: Autoría propia

Descargamos e instalamos OpenVPN Connect en la maquina local de Windows. Vamos a realizar la prueba de conexión en la maquina anfitriona Windows.

Figura 74. Instalación OpenVPN.

Fuente: Autoría propia

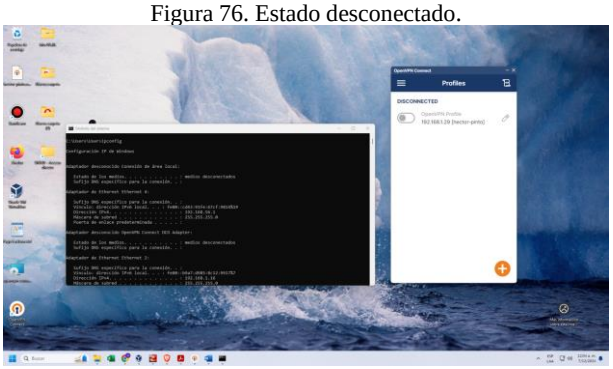
Cargamos el archivo a la herramienta OpenVPN Connect y damos clic en “CONNECT”.

Figura 75. Cargando archivo VPN.

Fuente: Autoría propia

Visualizamos que en el símbolo de sistema en el Adaptador desconocido conexión de área local no tienen activa ninguna conexión.

Figura 76. Estado desconectado.



Fuente: Autoría propia

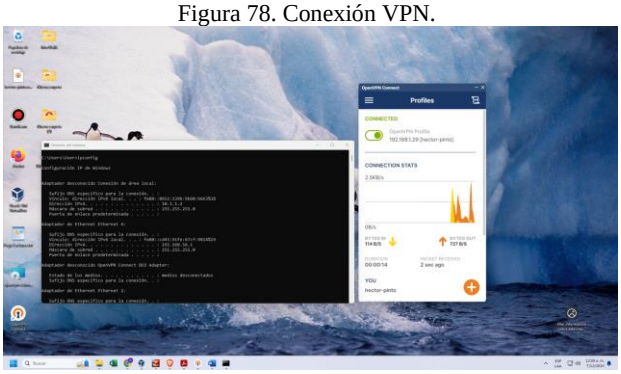
Damos clic en “CONNECT”.

Figura 77. Aceptando conexión.

Fuente: Autoría propia

Una vez nos conectamos podemos ver que ya tenemos la conexión activa 10.1.1.2.

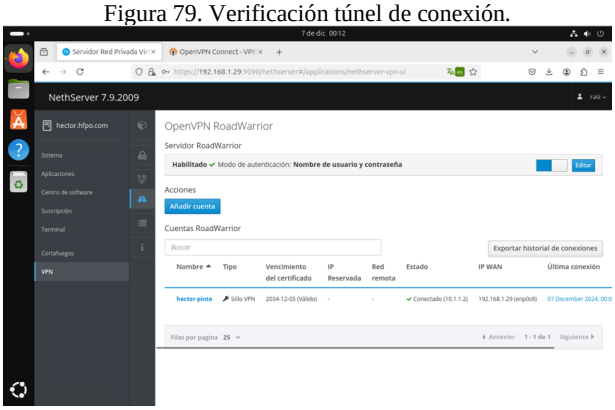
Figura 78. Conexión VPN.



Fuente: Autoría propia

Podemos ver que la conexión corresponde al usuario creado.

Figura 79. Verificación túnel de conexión.



Fuente: Autoría propia

3 CONCLUSIONES

La configuración de una zona DMZ resalta la importancia de establecer controles de seguridad entre las redes internas y externas. Este enfoque asegura que los servicios sean accesibles solo bajo condiciones controladas, protegiendo los recursos y datos valiosos frente a amenazas externas, lo cual es clave para cualquier infraestructura IT corporativa.

Por consiguiente, la configuración del proxy en el puerto 3128 ha sido fundamental para controlar el acceso a internet y mejorar la seguridad de la red, aplicar políticas de red bien definidas promoviendo tranquilidad en la navegación a los usuarios finales evitando publicidad engañosa y el acceso a sitios no deseados y obteniendo buenas prácticas en la gestión de sistemas operativos y servicios de red.

Como conclusión adicional, es importante mencionar que la correcta implementación y configuración del Firewall de _NethServer, nos permite garantizar aspectos tan importantes como la prevención de ataques, la protección de datos y la optimización de nuestra red y reconocemos que las instrucciones brindadas en este trabajo facilitaran un poco más, dicho proceso de configuración

La implementación de servidores de archivos e impresión junto con el controlador de dominio LDAP demuestra cómo se puede gestionar de forma centralizada el acceso a recursos compartidos. Esto mejora la administración de permisos y seguridad, lo que incrementa la eficiencia y productividad en un entorno corporativo.

La configuración de una VPN es una solución eficaz para garantizar la seguridad y privacidad en las comunicaciones, permitiendo el acceso seguro a recursos en redes remotas. Al crear un túnel cifrado entre un dispositivo cliente y una estación de trabajo GNU/Linux, se protege la información y se minimizan riesgos de seguridad. Este proyecto demuestra cómo una VPN puede ser utilizada para acceder de forma segura a aplicaciones y contenidos específicos, asegurando la confidencialidad e integridad de los datos.

4 REFERENCIAS

LPI LPIC-1 Exam 102. (2022). Tema 109: Fundamentos de redes. https://learning.lpi.org/es/learning-materials/102-500/109/

LPI LPIC-1 Exam 102. (2022). Tema 110: Seguridad. https://learning.lpi.org/es/learning-materials/102-500/110/
Oracle (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/
AVG Technologies. (s.f.). ¿Qué es un servidor proxy? Recuperado el 9 de diciembre de 2024, de https://www.avg.com/es/signal/proxy-server-definition.
NethServer, W. t. (2019). wiki. NethServer & NethSecurrity. https://wiki.NethServer .org/doku.php?id=start
Jeroen, P. (2018, febrero 19). How to install NethServer as Samba AD domain controller v0.2. NethServer Community. https://community.nethserver.org/t/howto-install-nethserver-assamba-ad-domain-controller-v0-2/9076
[YouTube]. (2019). Nethserver Tutorial | Instalación, actualización y primeros pasos. Recuperado de https://www.youtube.com/watch?v=FNGmM-2fa_0
LPIC-1. (Versión 5.1). Tema 105: Shell y Scripts. (página 1-84). https://learning.lpi.org/es/learning-materials/102-500/105/
LPIC-1. (Versión 5.1). Tema 106: Interfaces de usuarios y escritorios. https://learning.lpi.org/es/learning-materials/102-500/106/