

IMPLEMENTACIÓN Y CONFIGURACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT MEDIANTE NETHSERVER

Faruk Perez Montalvo
fperezmon@unadvirtual.edu.co
Juan David Restrepo Portilla
jdrestrepop@unadvirtual.edu.co
Viviana Yiseth Pardo Vargas
vypardov@unadvirtual.edu.co
Brandon Torres Rojas
bdtorresr@unadvirtual.edu.com

RESUMEN: Se implementaron servicios de gestión de infraestructura IT mediante la plataforma Nethserver. La primera fase abarcó la configuración de servicios esenciales como DHCP Server, DNS Server y Controlador de Dominio para permitir el acceso seguro de estaciones de trabajo GNU/Linux. La segunda etapa se centró en desplegar y configurar un Proxy que filtra el acceso a Internet para estaciones GNU/Linux, utilizando el puerto 3128 como punto de control. La tercera fase se dedicó a la implementación de un Cortafuegos que restringe el acceso a sitios de entretenimiento y redes sociales, con pruebas desde una estación GNU/Linux para validar las restricciones. La última fase se concentró en la creación y configuración de una VPN donde se estableció un túnel privado de comunicación con una estación GNU/Linux, demostrando el acceso a un contenido específico.

PALABRAS CLAVE: DNS, nethserver, proxy, VPN.

1 INTRODUCCIÓN

NethServer, en la actualidad, se destaca como una plataforma de gestión de infraestructura IT esencial, especialmente en un entorno empresarial donde la eficiencia y la seguridad son prioritarias. Su enfoque modular y su naturaleza de código abierto proporcionan a las organizaciones una flexibilidad única para adaptar y personalizar sus servicios de red [1]. Es por ello, que se describe el paso a paso de los procedimientos realizados y los resultados obtenidos en cada una de las temáticas o servicios implementados. Este enfoque detallado y estructurado aportará una guía para una implementación efectiva y documentada de los servicios de gestión (DHCP Server, DNS Server, Controlador de Dominio, Proxy y VPN) en la plataforma Nethserver.

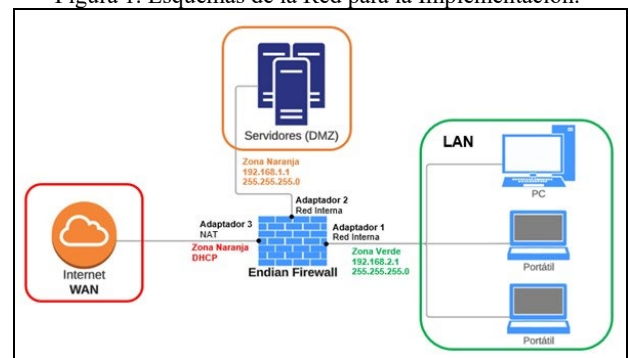
2 INSTALACIÓN Y CONFIGURACIÓN DE NETHSERVER

2.1 ESQUEMA DE RED

Para empezar, se definió un esquema de red para la comunicación entre las zonas y NethServer como servidor,

zona roja o WAN, zona verde o LAN (192.168.2.1) y zona naranja o DMZ (192.168.1.1). Ver Figura 1.

Figura 1. Esquemas de la Red para la Implementación.

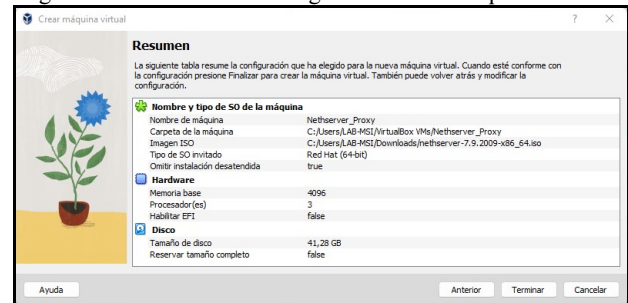


Fuente: Autoría Propia

2.2 MAQUINA NETHSERVER

Como parte del procedimiento, se configura la máquina virtual de la siguiente manera. Ver Figura 2.

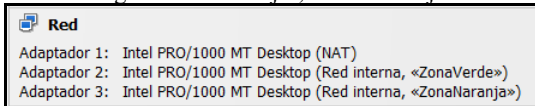
Figura 2. Resumen de la configuración de la Máquina Virtual.



Fuente: Autoría Propia

Una vez creada la máquina virtual, se procede a configurar en las tarjetas de red las tres zonas definidas. Ver Figura 3.

Figura 3. Zonas rojas, verde Naranja.



Fuente: Autoría Propia.

Se inicia la máquina virtual desde la ISO de “NethServer”, y lo primero que muestra es la selección de la instalación interactiva donde solo se necesita configurar el teclado y la zona horaria [2]. Ver Figura 4.

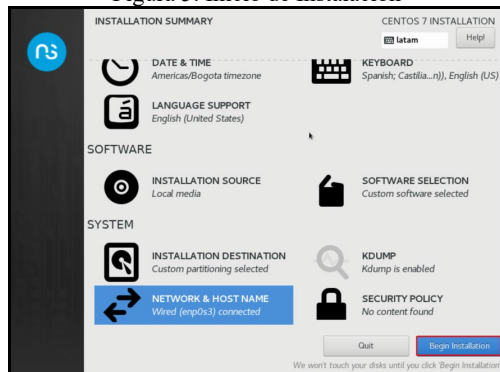
Figura 4. Inicio de instalación.



Fuente: Autoría Propia.

En cuanto inicia la instalación, la primera pantalla que se observa es el asistente de instalación en el que se deben configurar zona horaria, distribución de teclado y redes. Ver Figura 5.

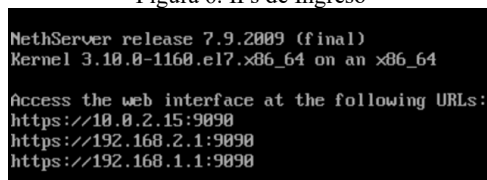
Figura 5. Inicio de Instalación



Fuente: Autoría Propia

La instalación de este punto en adelante es totalmente desatendida y al finalizar, el servidor se reinicia. Al subir nuevamente el sistema operativo se visualiza una pantalla en donde se muestran las IPs y puerto por donde es posible acceder al portal de administración. Ver Figura 6.

Figura 6. IPs de Ingreso



Fuente: Autoría Propia

Luego de recibir esta pantalla y antes de entrar a configurar los servicios, es necesario asegurarse de que todos los servicios queden con las últimas versiones disponibles, para eso se ejecuta el comando “yum update” [3].

2.3 ACCESO DESDE UBUNTU DESKTOP

Teniendo en cuenta que aún no se han configurado los servicios, se debe configurar una máquina cliente para estar sobre el mismo segmento de la zona verde, por lo tanto, manualmente se asigna a Ubuntu Desktop, la dirección 192.168.2.10, con máscara de red 255.255.255.0 y puerta de enlace 192.168.2.1. Ver Figura 7.

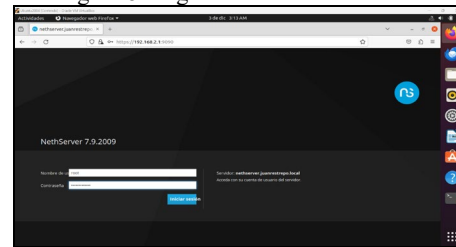
Figura 7. Configuración de red Ubuntu Desktop



Fuente: Autoría Propia

Sobre Ubuntu Desktop, desde el explorador Firefox se ingresa <https://192.168.2.1:9090>. Visualizándose una ventana de inicio de sesión de NethServer 7.9.2009 [4]. Ver Figura 8.

Figura 8. Login del Portal NethServer

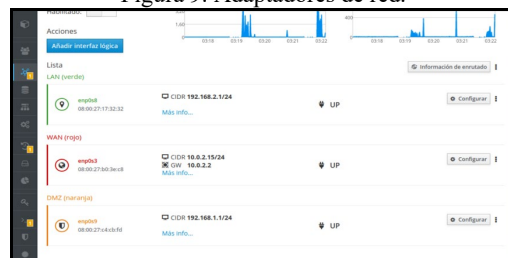


Fuente: Autoría Propia

Ya teniendo el control del servidor a través de la interfaz gráfica se procede a configurar los valores por defecto tales como datos de la empresa y DNS de la máquina. Teniendo ya personalizados los anteriores datos, lo primero que por hacer es la configuración de las tarjetas de red.

Al dirigirse a este apartado, se evidencia que todos los adaptadores automáticamente fueron asignados a la zona verde, en este caso, se tienen los adaptadores enp03s, enp08s y enp09s y que van a ser configurados en las zonas roja, verde y naranja en el mismo orden. Ver Figura 9.

Figura 9. Adaptadores de red.



Fuente: Autoría Propia

Ya con la configuración de red terminada y previo a la publicación de los servicios requeridos, es sugerido cambiar el valor por defecto que tiene el puerto por el cual se hacen las conexiones SSH, inicialmente se encuentra en el puerto 22, se debe realizar el cambio por uno que sea menos común, para aumentar la seguridad y dificultar mucho los intentos de accesos no autorizados [5]. Como se observa en la Figura 10, se selecciona el puerto 2222 y se guardan los cambios.

Figura 10. Cambio puerto SSH.



Fuente: Autoría propia

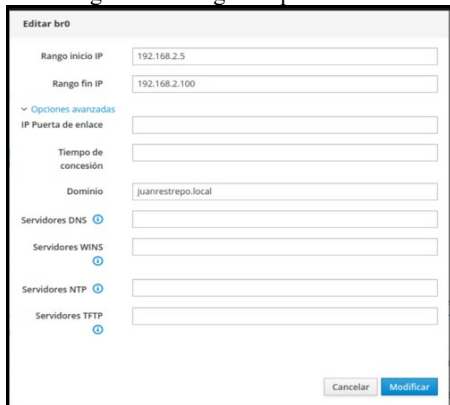
3 TEMÁTICA #1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

3.1 CONFIGURACIÓN DHCP

Acceder al apartado de DHCP [6], donde se ve la zona verde a la cual se procede a activar este servicio de entrega de IPs a la red.

Se procede a configurar el rango con IP de inicio 192.168.2.5 y como IP final 192.168.2.1. Adicional es requerido ingresar el dominio que se va a usar para el resto del ejercicio. Ver Figura 11.

Figura 11. Rango IPs para DHCP



Fuente: Autoría Propia

Ahora, para probar el correcto funcionamiento en la entrega automática de IPs, a través de la configuración de red de la máquina Ubuntu y se debe cambiar a la opción en método IPv4 a automático (DHCP). Una vez guardados los cambios se puede evidenciar en la pestaña de detalles que

efectivamente la máquina ya está tomando una dirección asignada por el servidor. Ver Figura 12.

Figura 12. Funcionamiento DHCP

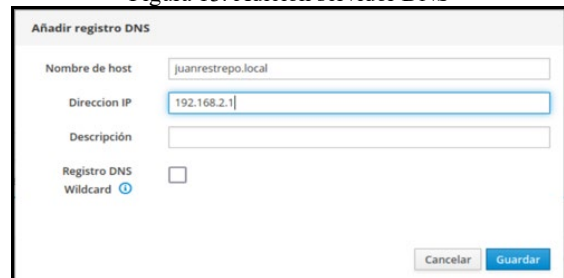


Fuente: Autoría propia

3.2 CONFIGURACIÓN DNS

Dentro del apartado de DNS [7] y se añade un nuevo registro, acá se ingresa el nombre del host y añadimos como dirección IP, la puerta de enlace de la zona verde (192.168.2.1). Ver Figura 13.

Figura 13. Adición servidor DNS

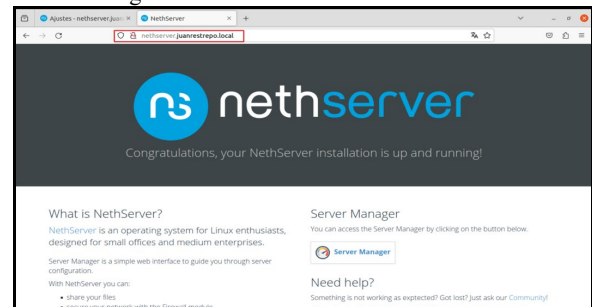


Fuente: Autoría propia

Una vez realizado el cambio, es posible regresar a las opciones de red de Ubuntu y ver que en la pestaña detalles, la máquina ya está tomando el servidor como DNS.

Como prueba de funcionamiento del servidor DNS, dentro de la máquina Ubuntu, se ingresa el nombre del servidor de NethServer (nethserver.juanrestrepo.local), el cual muestra una pantalla de confirmación. Ver Figura 14.

Figura 14. Prueba de Funcionamiento DNS



Fuente: Autoría Propia

Adicional a la anterior prueba, se ejecuta el comando traceroute se puede validar el enrutamiento hacia un servidor o sitio en específico, en este caso probamos con Google, donde se evidencia que al salir la solicitud en la máquina Ubuntu, el primer paso es a través de nuestro servidor DNS [8]. Ver Figura 15.

Figura 15. Prueba de Enrutamiento DNS

```

Juan_restrepo@Ubuntu2004: ~
Juan_restrepo@Ubuntu2004:~$
Juan_restrepo@Ubuntu2004:~$ traceroute google.com
traceroute to google.com (142.250.78.142), 30 hops max, 60 byte packets
 1 nethserver.juanrestrepo.local (192.168.2.1)  0.784 ms  0.686 ms  0.612 ms
 2 10.0.2.2 (10.0.2.2)  1.222 ms  1.702 ms  1.629 ms
 3 10.0.2.2 (10.0.2.2)  9.327 ms  12.757 ms  12.686 ms
Juan_restrepo@Ubuntu2004:~$

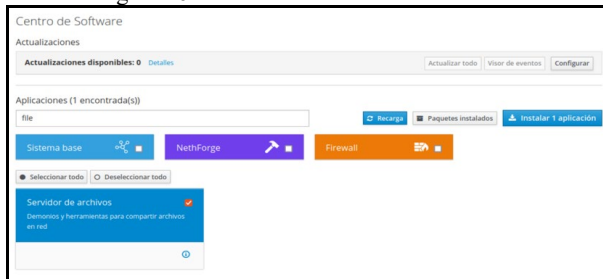
```

Fuente: Autoría Propia

3.3 CONFIGURACIÓN CONTROLADOR DE DOMINIO

Antes de lanzar la configuración del Controlador de Dominio, como prerrequisito es necesario instalar samba o servidor de archivos, esta tarea es realizada desde Software Center [9]. Ver Figura 16.

Figura 16. Instalación Servidor de Archivos.

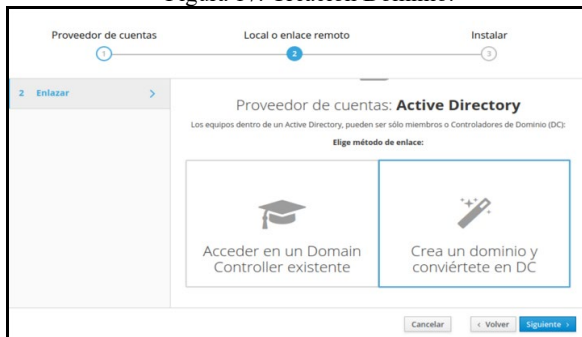


Fuente: Autoría Propia

Teniendo ya instalado este servicio, es posible, a través de Samba, compartir carpetas y archivos entre las distintas estaciones de trabajo, en el cual a través de los diferentes grupos de acceso y permisos que provee el directorio activo.

Para configurar el servidor NethServer como controlador de dominio, se procede a abrir el apartado de usuarios y grupos y seleccionamos "Active Directory", esta opción ayuda a configurar de forma automática tanto los servicios de controlador de dominio, como de directorio activo para nuestra red. Ver Figura 17.

Figura 17. Creación Dominio.

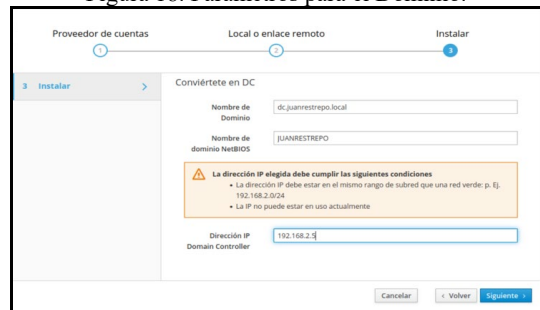


Fuente: Autoría Propia

Se ingresa el nombre del host para el dominio (dc.juanrestrepo.local) y asignamos una IP que debe pertenecer al segmento 192.168.2.0/24, pero as su vez debe estar dentro del rango asignado a las estaciones para DHCP, en este caso 192.168.2.5. Ver Figura 18.

El proceso comienza de manera automática instalando los distintos servicios y realizando configuraciones, este paso puede tardar dependiendo de los recursos asignados a el servidor NethServer.

Figura 18. Parámetros para el Dominio.



Fuente: Autoría Propia

Una vez finalizada la configuración, el portal muestra un resumen de los datos necesarios para unir las estaciones de trabajo. Ver Figura 19.

Figura 19. Detalles del dominio.

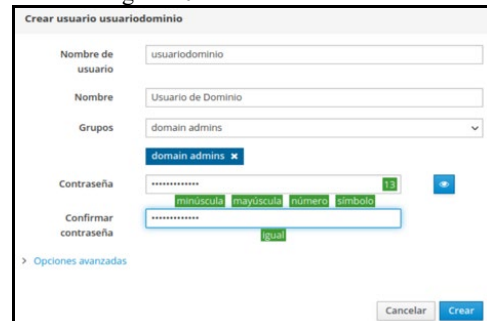


Fuente: Autoría Propia

Lo primero que se debe hacer es habilitar las cuentas de administrador, cambiando su contraseña. En este punto ya se puede empezar con la gestión y creación de los distintos usuarios y grupos del directorio activo donde es posible editar campos tales como la expiración de la contraseña.

Para la demostración del funcionamiento, se empieza creando una cuenta con la cual se va a acceder a una estación de trabajo con sistema operativo Windows 7. Ver Figura 20

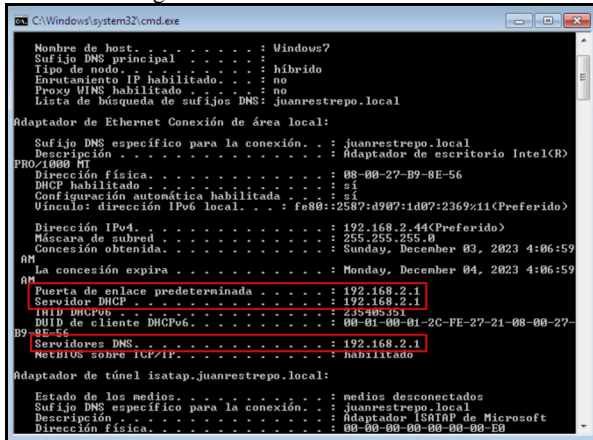
Figura 20. Creación de usuario.



Fuente: Autoría Propia

Ahora, dentro de la máquina corriendo Windows, la cual debe estar en la zona verde, se debe validar que tenga conectividad con el servidor Nethserver, para esto, se realiza una prueba de ping al servidor principal (192.168.2.1) y adicional al controlador de dominio (192.168.2.5). Ver Figura 21.

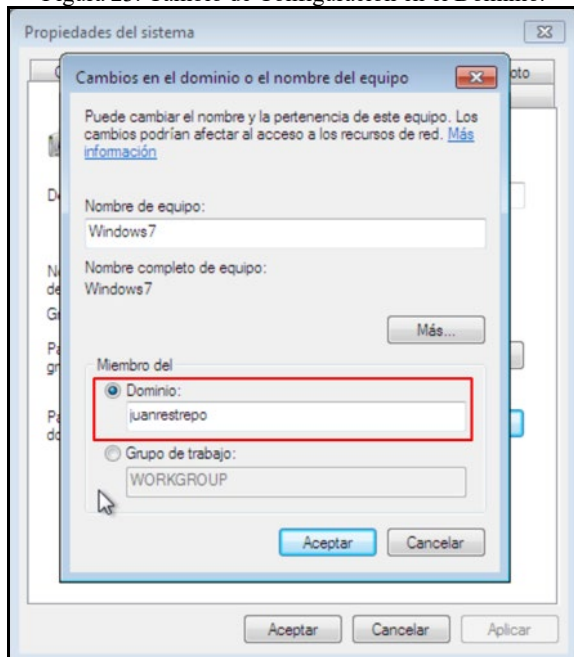
Figura 21. Prueba de Conectividad.



Fuente: Autoría Propia

Estando en la misma máquina, se debe ingresar a las propiedades de equipo y luego sobre el apartado de sistema, se debe seleccionar la opción de cambiar configuración. Estando en esta pantalla, el paso siguiente es ingresar el dominio en el campo requerido. Ver Figura 22.

Figura 22. Cambio de Configuración en el Dominio.



Fuente: Autoría Propia

Luego de que sean validadas las credenciales, la máquina ya estará matriculada dentro del dominio, el paso a seguir es aplicar un reinicio para que se tomen todos los cambios.

Una vez el sistema inicia, se puede comprobar que en la pantalla de login de usuario, ya el usuario se está conectando al dominio inscrito. Ver Figura 23.

Figura 23. Prueba de conectividad.



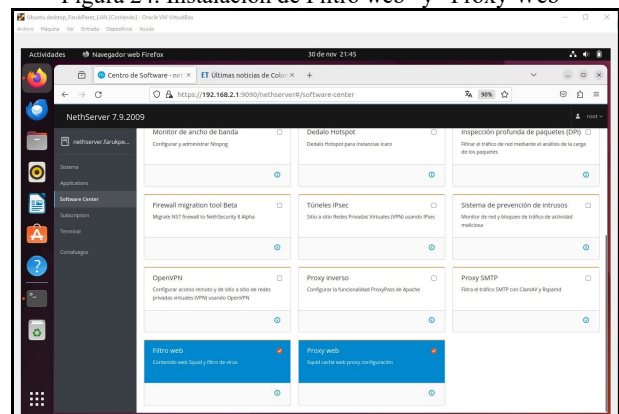
Fuente: Autoría Propia

4 TEMÁTICA # 2: PROXY

4.1 INSTALACIÓN DEL PROXY

Esta fase se inicia con la instalación de dos aplicaciones necesarias para la implementación del servicio proxy. Las aplicaciones son “Filtro web” [10] y “Proxy Web” [11]. Ver Figura 24.

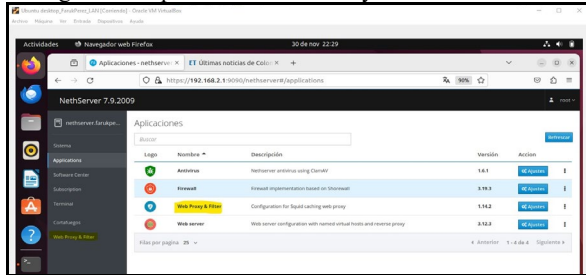
Figura 24. Instalación de Filtro web” y “Proxy Web”



Fuente: Autoría Propia

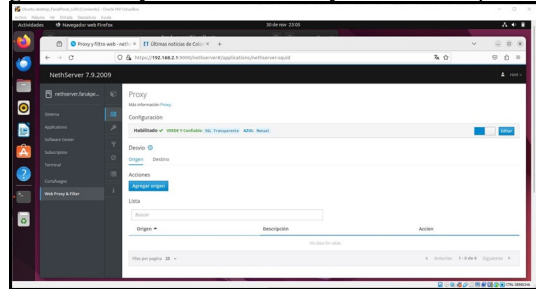
Al verificar en “Applications”, se observa que la aplicación “Web Proxy & Filter” está instalado. Ver Figura 25.

Figura 25. Aplicación “Web Proxy & Filter” instalada



Fuente: Autoría Propia

Figura 28. Proxy en la Zona Verde y en SSL Transparente”

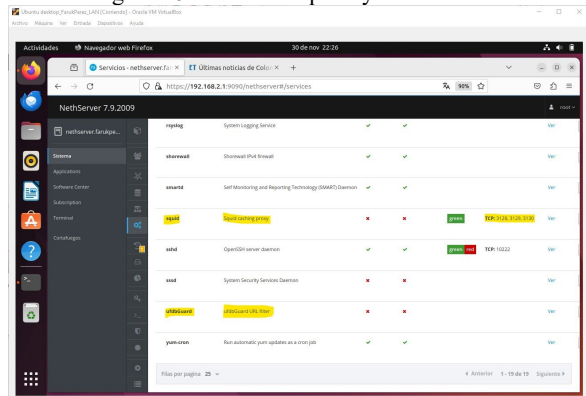


Fuente: Autoría Propia

4.2 CONFIGURACIONES NECESARIAS

Posteriormente, se ingresa a “Sistemas” – “Servicios”, observando que los servicio “squid” y “ufdbGuard”, y ya se encuentra disponible, pero deshabilitado. Estos se deben habilitar. Ver Figura 26.

Figura 26. Servicio “squid” y “ufdbGuard”

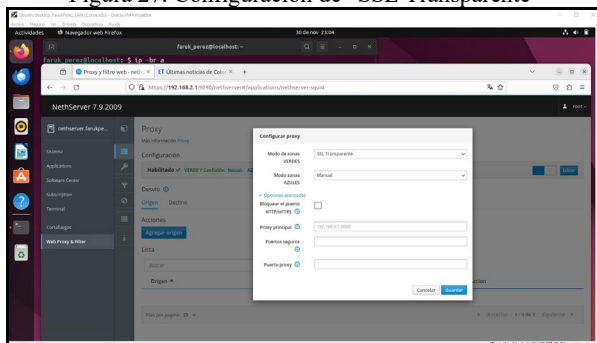


Fuente: Autoría Propia

Squid en NethServer permite filtrar el contenido web y brinda herramientas de control de acceso para gestionar de manera eficiente el uso de Internet en la red. [12]. En este caso squid filtra la salida por medio de los puertos TCP 3128, 3129 y 3130. El servicio “ufdbGuard”, es un filtro de URL para el servidor proxy web Squid. ufdbGuard se utiliza para bloquear el acceso a determinados sitios web o tipos de contenido [13].

Se ingresa a la configuración del Proxy. En el Modo de zonas verdes se selecciona “SSL Transparente” y se da clic en “Guardar”. Ver Figura 27 y 28.

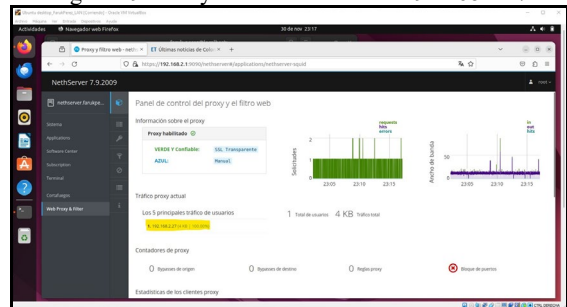
Figura 27. Configuración de “SSL Transparente”



Fuente: Autoría Propia

Ubicados nuevamente en el “Panel de Control del Proxy y el Filtro Web”, se observa que el proxy está habilitado en la zona verde y en modo SSL Transparente. En el tráfico del proxy actual se evidencia que la IP 198.168.2.27 está siendo filtrada y monitoreada. Ver Figura 29.

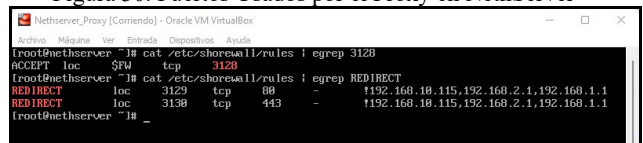
Figura 29. Proxy en filtrado de la IP 192.168.2.27



Fuente: Autoría Propia

Ahora se verifica desde el terminal del Servidor Nethserver, que los puertos 3128, 3129 y 3130 están siendo usados para redireccionar el tráfico y hacer los filtros del proxy. Ver Figura 30.

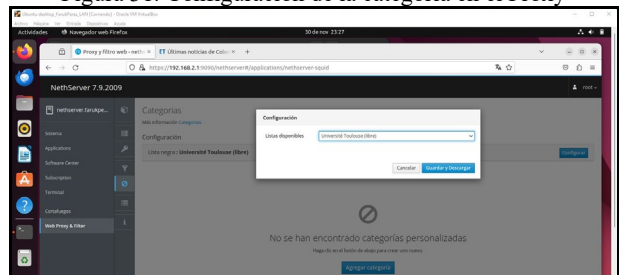
Figura 30. Puertos Usados por el Proxy en NethServer



Fuente: Autoría Propia

Para seguir configurando el Proxy, se ingresa a “Web Proxy & Filter” - “Categorías”, aquí se configura la lista negra: Université Toulouse (Libre), dando clic en “Configurar” Ver Figura 31.

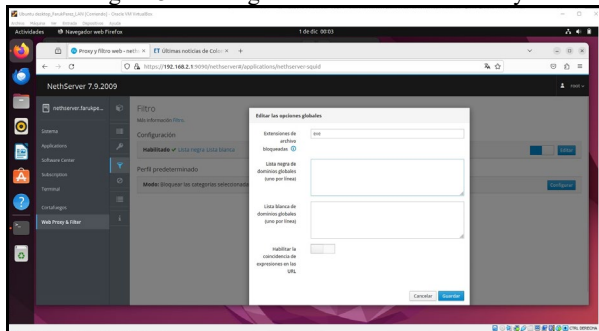
Figura 31. Configuración de la categoría en el Proxy



Fuente: Autoría Propia

Seguido, se configura el “Filtro” en “Web Proxy & Filter”, presionando el botón “Editar las opciones globales”. En extensiones de archivo se seleccionó “exe”. Clic en “Guardar”. Ver Figura 32.

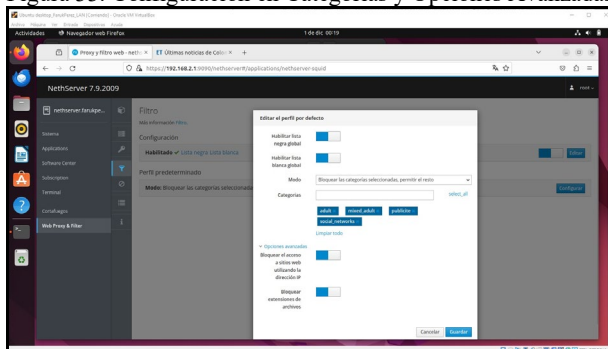
Figura 32. Configuración del Filtro del Proxy



Fuente: Autoría Propia

Se continua el proceso, haciendo clic en “Configurar” el perfil predeterminado. Luego, en el Modo, se selecciona la opción “Bloquear las categorías seleccionadas, permitir el resto”. Para este caso educativo, en categorías se selecciona adult, mixed_adult, publicite, social_networks. Además, en opciones avanzadas se habilita “Bloquear el acceso a sitios web utilizando la dirección IP” y “Bloquear extensiones de archivos”. Las categorías funcionan como parámetros para realizar el filtrado. Ver Figura 33.

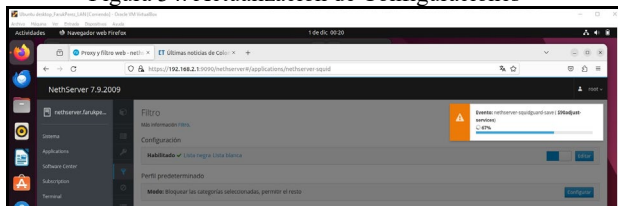
Figura 33. Configuración en Categorías y Opciones Avanzadas



Fuente: Autoría Propia

Por último, se actualizan las configuraciones realizadas. Ver figura 34.

Figura 34. Actualización de Configuraciones”



Fuente: Autoría Propia

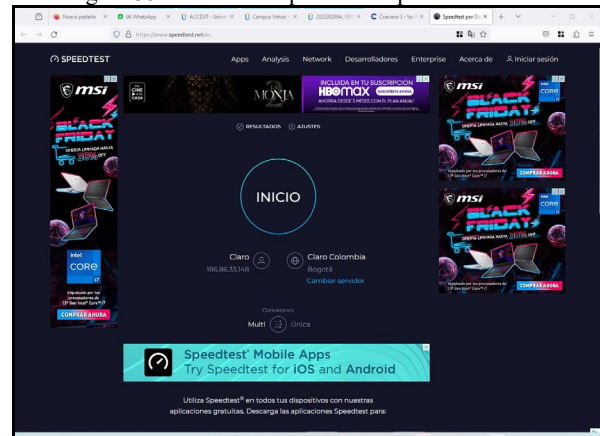
Estas configuraciones permitirán al proxy hacer filtrado y bloqueo de acceso a internet a través de los puertos TCP 3128, 3129 y 3130 cuando se detecten peticiones de acceder a sitios web catalogados para adultos o pornografía, bloqueará

publicidades detectadas en los sitios web que se naveguen y no permitirá acceder a sitios web de redes sociales.

4.3 PRUEBAS DE FUNCIONAMIENTO DEL PROXY EN NETHSERVER

En primera instancia, se accede desde la máquina física o máquina real a un sitio web (<https://www.speedtest.net/es>) que muestra mucha publicidad. Ver Figura 35.

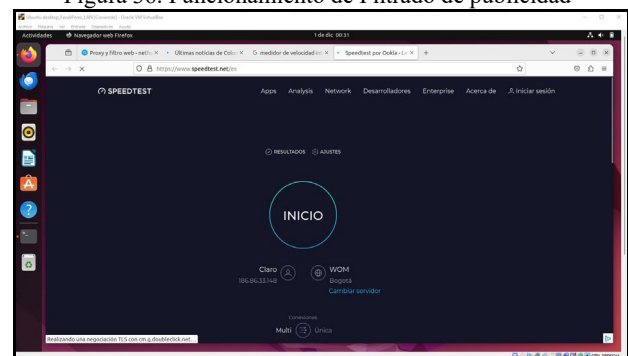
Figura 35. Acceso a <https://www.speedtest.net/es>”



Fuente: Autoría Propia

Ahora, desde el equipo Ubuntu Desktop accedemos al mismo sitio web <https://www.speedtest.net/es>, se puede evidenciar que no carga publicidad por el trabajo de filtrado del Proxy. Ver Figura 36.

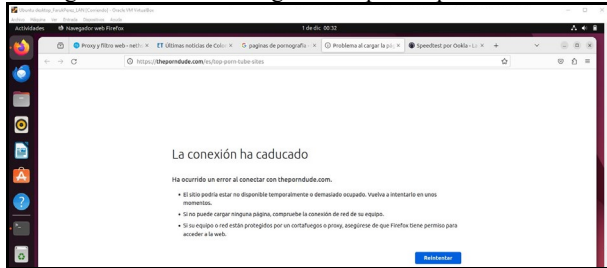
Figura 36. Funcionamiento de Filtrado de publicidad



Fuente: Autoría Propia

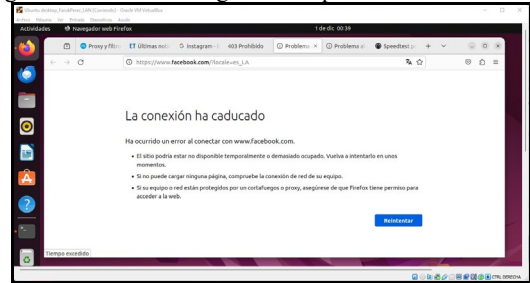
La siguiente verificación será acceder a sitios con contenido pornográfico desde el equipo Ubuntu Desktop, se puede observar que el proxy bloquea el acceso a estos sitios web. Ver Figuras 37, 38 y 39.

Figura 37. Acceso denegado a https://thepornude.com



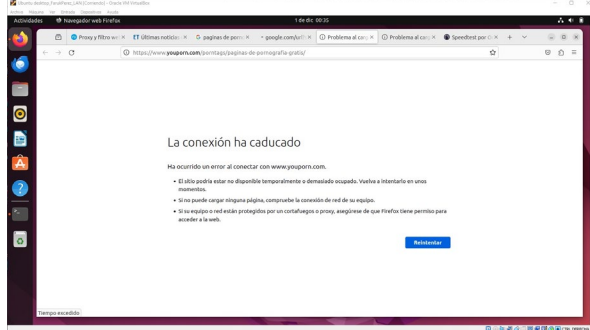
Fuente: Autoría Propia

Figura 41. Acceso Denegado a “http://www.facebook.com”



Fuente: Autoría Propia

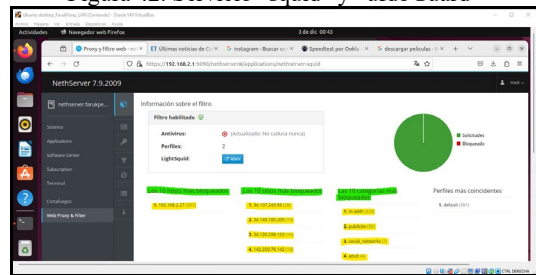
Figura 38. Acceso denegado a https://www.youporn.com



Fuente: Autoría Propia

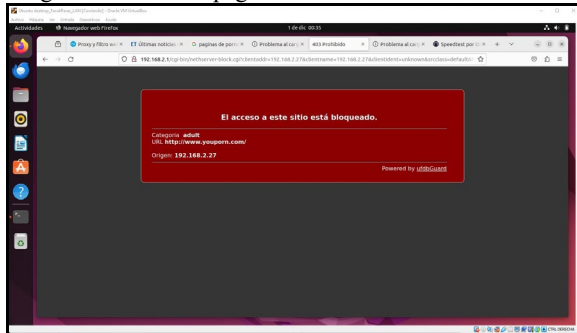
Para finalizar, se ingresa nuevamente al dashboard de NethServer, en el “Panel de Control del Proxy y el Filtro”, Este panel muestra información de los Hosts bloqueados, sitios bloqueados y las categorías empleadas en filtro. Ver Figura 42

Figura 42. Servicio “squid” y “ufdbGuard”



Fuente: Autoría Propia

Figura 39. Filtro de páginas con HTTP con Restricciones



Fuente: Autoría Propia

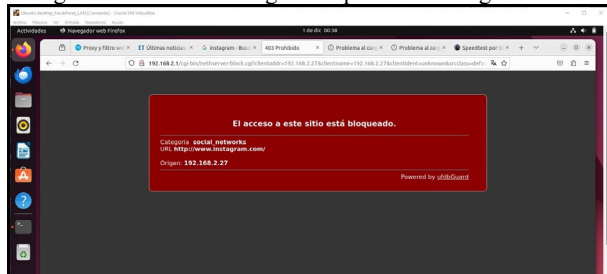
5 TEMÁTICA # 3: CORTAFUEGO

5.1 CONFIGURACIÓN DE NAVEGACIÓN

Otra verificación del funcionamiento del Proxy está encaminada al boqueo del acceso a redes sociales por parte del Equipo Ubuntu Desktop. Ver Figuras 40 y 41.

Una vez se tiene realizada la instalación de Nethserver, se verifican las dos interfaces configuradas, la de la zona roja y la de la zona verde. Con la zona verde se puede ingresar por la interfaz gráfica desde una Desktop diferente.

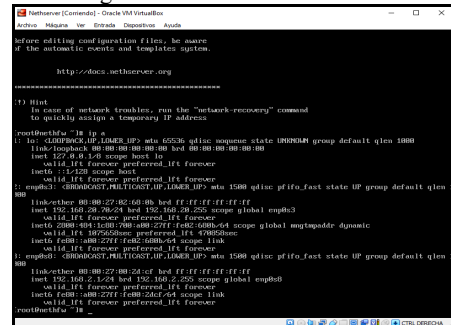
Figura 40. Acceso Denegado http://www.instagram.com”



Fuente: Autoría Propia

Para esto, en el Ubuntu Desktop se configura la IP con la zona verde, para que permita ingresar a la interfaz gráfica del nethserver. Por medio del comando “nmtui” se configura la IP del Ubuntu Desktop, en este caso la IP que se configura es 192.168.2.1 con Gateway 192.168.2.254. Una vez configurada la interfaz de red, por medio de la ip 192.168.2.1:9090 se ingresa a la interfaz gráfica de nethserver, con el usuario root y la contraseña que se estableció previamente.

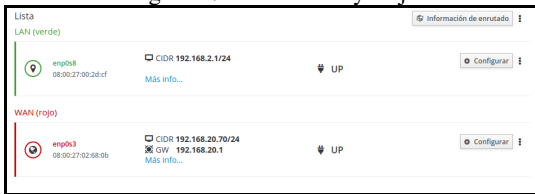
Figura 46. Interfaces Nethserver



Fuente: Autoría Propia

Lo primero que se debe hacer al ingresar a Nethserver es configurar la zona roja que es la que permitirá la salida a internet y la zona verde, que será la zona LAN, la cual tendrá la restricción de navegación. Ver Figura 47.

Figura 47. Zona Verde y Roja



Fuente: Autoría Propia

Luego, se configura los DNS, para eso se coloca el DNS primario 192.168.20.1 y se deja el secundario como el 8.8.8.8 y se crea un registro DNS con la IP de la zona verde 192.168.2.1 y un dominio llamado milabvirtual.lan. Ver Figura 48.

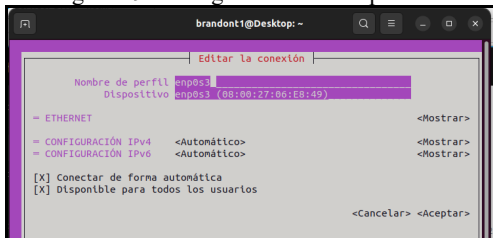
Figura 48. Registro DNS

Nombre	Descripción	Dirección IP	Registro DNS Wildcard	Acción
milabvirtual.lan		192.168.2.1		Editar

Fuente: Autoría Propia

Para finalizar, se realiza la creación del servicio DHCP, para así liberar la ip de la zona verde y configurar el desktop con IP automática. Ver Figura 49.

Figura 49. Configuración Desktop DHCP

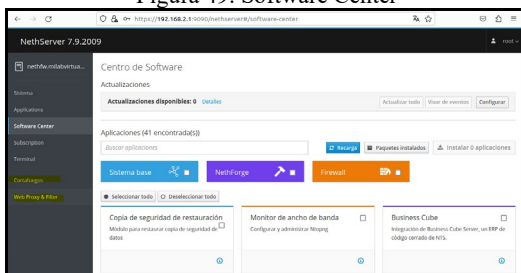


Fuente: Autoría Propia

5.2 CONFIGURACIÓN DEL PROXY WEB

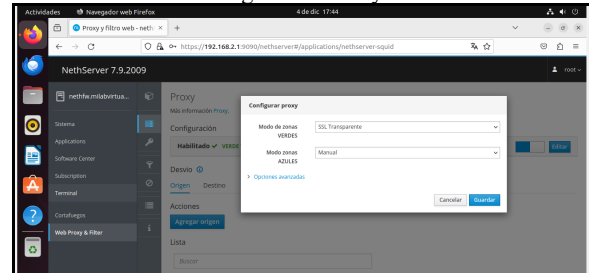
Una vez configurado el entorno verde, se configura el cortafuegos, proxy y filtrado de web. Para esto se ingresa al centro de software y se busca el firewall, el proxy y el filtrado de web, los cuales se deben instalar en el servidor. Instalado el firewall, se verifica el esquema de la red, luego, se ingresa al web proxy y allí se crea el proxy con SSL Transparente. Ver Figura 49 y 50.

Figura 49. Software Center



Fuente: Autoría Propia

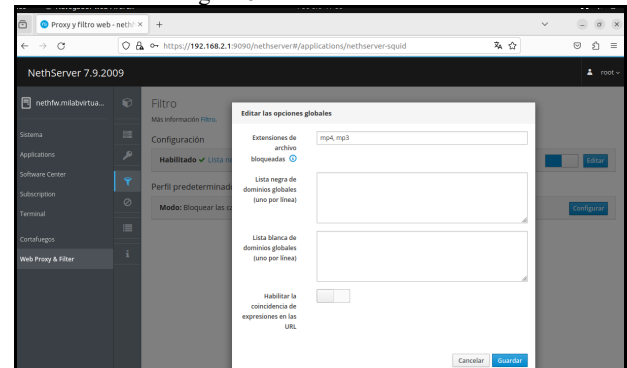
Figura 50. Proxy



Fuente: Autoría Propia

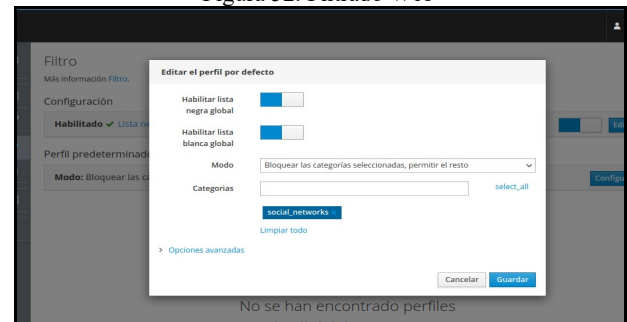
Ahora, se debe pasar al filtro, lo primero es crear el filtro de extensiones, lo cual es obligatorio para poder acceder a la configuración del perfil predeterminado. En el perfil, se busca la opción de redes sociales, la cual permitirá bloquear todas las URL que estén en la lista de esta categoría. Ver Figura 21 y 52.

Figura 51. Filtro Extensiones



Fuente: Autoría Propia

Figura 52. Filtrado Web



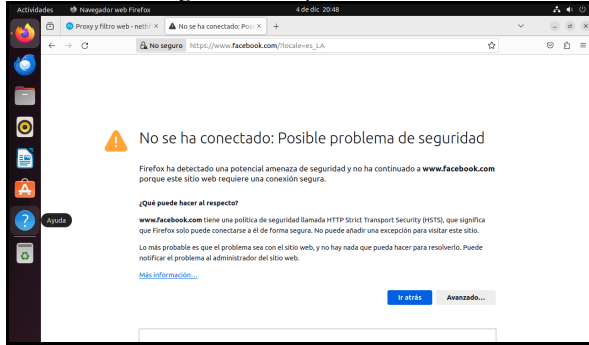
Fuente: Autoría Propia

5.3 VALIDACIÓN DE LA CONFIGURACIÓN

Una vez aplicada la configuración anterior, ya se cuenta con la restricción de páginas solicitadas.

Para poder validar que las páginas se encuentran bloqueadas, desde el desktop se podría tratar de ingresar a alguna página relacionada con redes sociales y evidenciar que se encuentra bloqueada. Ver Figura 53.

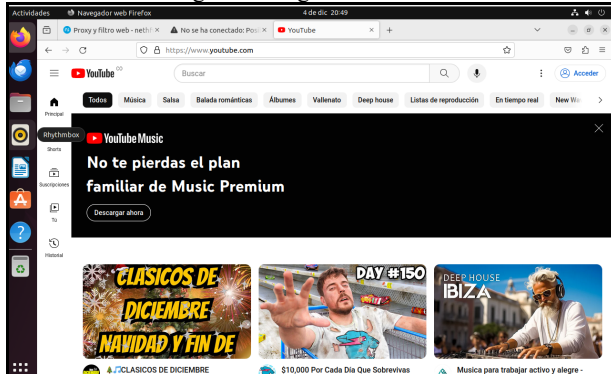
Figura 53. Bloqueo Facebook



Fuente: Autoría Propia

Si se intenta ingresar a una página con un fin diferente, es posible evidenciar que ingresa con normalidad. Ver Figura 54

Figura 54. Ingreso YouTube

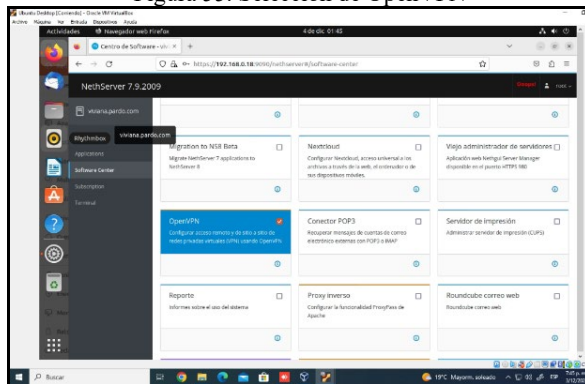


Fuente: Autoría Propia

6 TEMÁTICA # 5: VPN

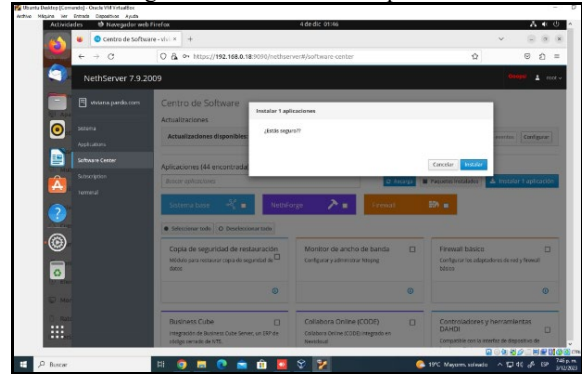
Dentro de NetchServer en la columna Software Center, se encuentra la opción OpenVPN, que permite crear fácilmente conexiones VPN [14], es necesario seleccionarla y en la parte superior dar clic en "Instalar 1 aplicación". Ver Figura 55 y 56.

Figura 55. Selección de OpenVPN



Fuente: Autoría Propia

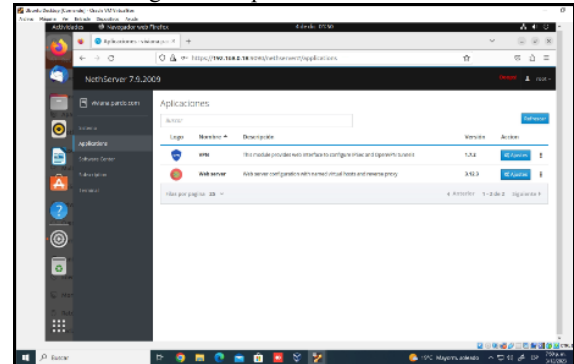
Figura 56. Instalación de OpenVPN



Fuente: Autoría Propia

Una vez instalado OpenVPN, a través de la opción aplicaciones aparecen todas las aplicaciones que tiene instalado NetchServer. Posteriores se da clic en ajustes. Ver Figura 57.

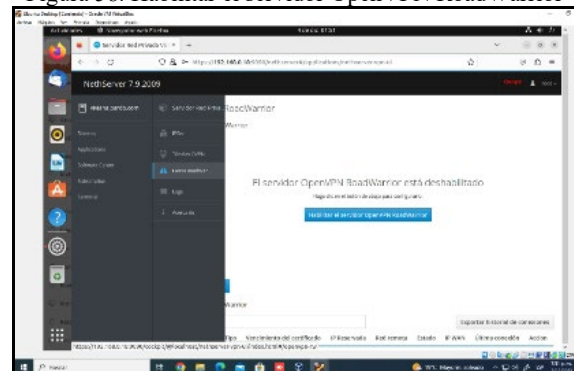
Figura 57. Aplicaciones instaladas



Fuente: Autoría Propia

Se configura OPENVPN RoadWarrior, se procede a dar clic en habilitar el servidor OpenVPN RoadWarrior. Ver Figura 58.

Figura 58. Habilitar el servidor OpenVPN RoadWarrior



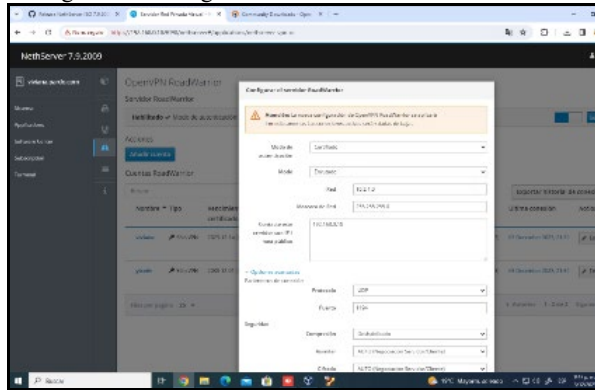
Fuente: Autoría Propia

Aparecerá la ventana para configurar el servidor RoadWarrior, para este caso se utilizará la configuración que aparece en las Figura 59 y 60.

Los métodos de autenticación admitidos son:

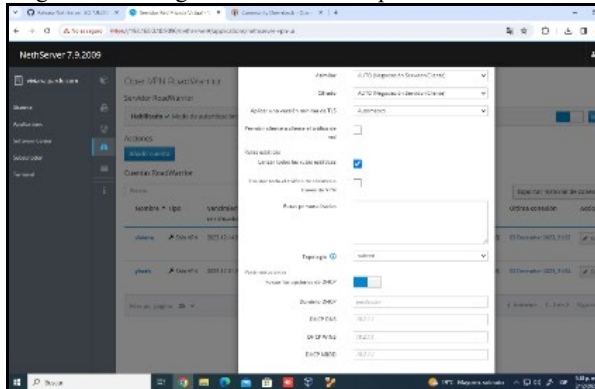
- Usuario y contraseña del sistema.
- Certificado.
- Nombre de usuario, contraseña y certificado.
- Nombre de usuario, contraseña (OTP) y certificado.

Figura 59. Configuración inicial servidor RoadWarrior



Fuente: Autoría Propia

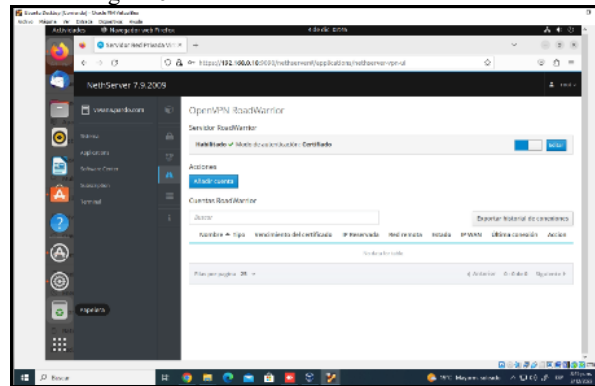
Figura 60. Configuración avanzada OpenVPN RoadWarrior



Fuente: Autoría Propia

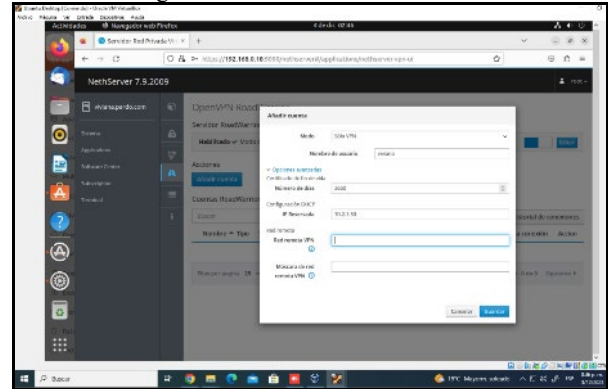
Una vez configurado el servidor RoadWarrior, se procede a crear las cuentas RoadWarrior. Damos clic en la opción añadir cuenta. Ver Figura 61 y 62

Figura 61. Servidor Road Warrior Habilitado



Fuente: Autoría Propia

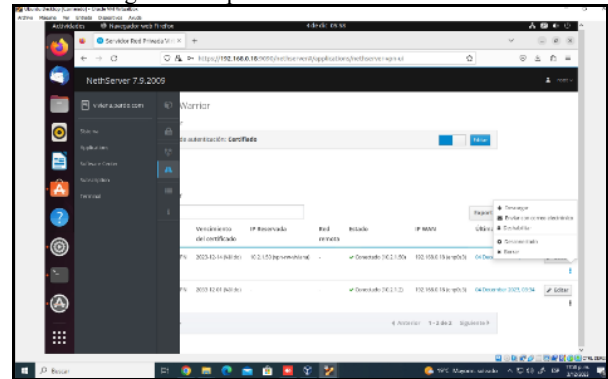
Figura 62. Creación de Cuenta VPN



Fuente: Autoría Propia

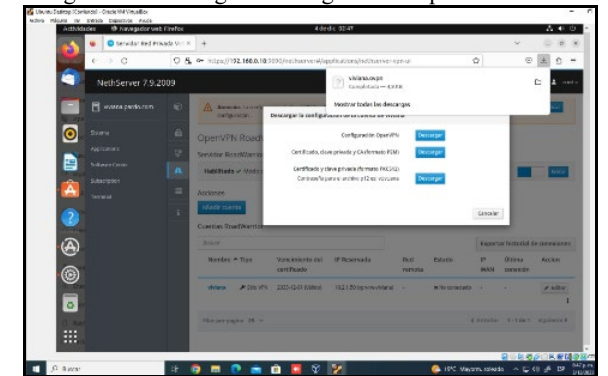
Una vez creado el usuario es posible descargar el archivo.ovpn el cual contiene la configuración del OpenVPN client/NetchServer. En este punto se puede observar que además de la configuración contiene el certificado, clave Privada y CA. Ver Figura 63 y 64.

Figura 63. Opciones de cuenta Client/VPN



Fuente: Autoría Propia

Figura 64. Descarga de configuración OpenVPN/Client



Fuente: Autoría Propia

En la máquina virtual de Ubuntu Desktop, se debe permitir las conexiones por el puerto 1194 TCP/UDP y 443 TCP/UDP. Ver Figura 65.

- [5] De Luz, S. (2023, junio 28). Configurar servidor OpenSSH en Linux con la máxima seguridad. RedesZone. <https://www.redeszone.net/tutoriales/servidores/servidor-openssh-linux-configuracion-maxima-seguridad/>.
- [6] Protocolo de configuración dinámica de host. (2023). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host&oldid=155731553.
- [7] DNS — NethServer 6.10 Final. (s. f.). Recuperado 6 de diciembre de 2023, de <https://docs.nethserver.org/es/v6/dns.html?highlight=DNS>.
- [8] Uso del comando Traceroute explicado con ejemplos - Aprender Linux. (2021, septiembre 4). <https://aprenderlinux.org/uso-del-comando-traceroute-explicado-con-ejemplos/>.
- [9] Jeroen, V. (2018, marzo 4). Howto install NethServer as Samba AD domain controller v0.2. NethServer Community. <https://community.nethserver.org/t/howto-install-nethserver-as-samba-ad-domain-controller-v0-2/9076>.
- [10] Filtro de contenido web—NethServer 6.10 Final. (s. f.). Recuperado 6 de diciembre de 2023, de https://docs.nethserver.org/es/v6/content_filter.html.
- [11] Proxy web—NethServer 6.10 Final. (s. f.). Recuperado 6 de diciembre de 2023, de https://docs.nethserver.org/es/v6/web_proxy.html.
- [12] squid: Optimising Web Delivery. (s. f.). Recuperado 4 de diciembre de 2023, de <http://www.squid-cache.org/>.
- [13] B.V, Url. (2023, febrero 1). ufdbGuard, a URL filter for Squid | URLfilterDB. <https://www.urlfilterdb.com/products/ufdbguard.html>.
- [14] VPN - NethServer 6.10 Final. (s. f.). Recuperado 6 de diciembre de 2023, de <https://docs.nethserver.org/es/v6/vpn.html?highlight=open%20vpn#>.