CONFIGURACIÓN Y PUESTA EN MARCHA DE SERVICIOS EN NETHSERVER

Carlos Eduardo Calvache Espiñeira
cecalvachee@unadvirtual.edu.co
Giovanni Alexis Ruiz Herrera
galex3122@unadvirtual.edu.co
José Mauricio Santos Orellanos
jmsantoso@unadvirtual.edu.co
Cesar Augusto León Zabala
caleonz@unadvirtual.edu.co

RESUMEN: En el presente artículo se podrá observar el paso a paso de la instalación del sistema operativo NethServer, su configuración para una conexión de red LAN, DMZ y WAN, la puesta en marcha del servidor GNU/Linux en base a la distribución servidor Neth 7.9.2009 en los que se dispondrán los servicios de infraestructura TI.

Se describirá la implementación de servicios DHCP server, DNS server, controlador de dominio, Proxy, cortafuegos y VPN.

PALABRAS CLAVE: DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, VPN, Linux, OpenVPN, LDAP, DHCP.

1 INTRODUCCIÓN

En el presente artículo se podrán observar los requerimientos, requisitos y pasos necesarios para orientar a la administración y control de una distribución GNU/Linux a través del servidor NethServer, esto para la implementación de servicios de infraestructura TI, esto con el fin de poder obtener información importante de los usuarios, administración y bloqueos de accesos a la web, implementación de seguridad y acciones que serán controladas desde la interfaz gráfica del servidor NethServer.

2 NETHSERVER

NethServer es un sistema operativo Linux basado en CentOS/RHEL, está diseñado para pequeñas y medianas empresas.

Cuenta con variedad de funciones relacionadas con la seguridad y conectividad entre la web, VPN y usuarios, tiene servidor de correo electrónico, servidor web, software colaborativo, cortafuegos, filtro web, configuración DHCP y DNS, entre otros.

Su administración puede realizarse desde una interfaz gráfica web muy intuitiva y rápida.

2.1 REQUERIMIENTOS MÍNIMOS PARA LA INSTALACIÓN

- CPU de 64 bits (x86_64)
- 1 GB de RAM
- 10 GB de espacio en disco
- Tarjeta de red habilitada

2.2 INSTALACIÓN

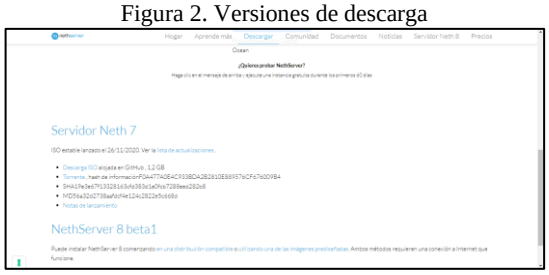
Ingresar al enlace oficial de NethServer en la página principal como se muestra en la Fig. 1 la dirección es https://www.NethServer.org/.

Figura 1. Página principal de NethServer

Fuente: Autoría propia

En el apartado de descargar seleccionar la versión que se desea instalar, en este caso se descargó la versión 7.9, ver Fig. 2.

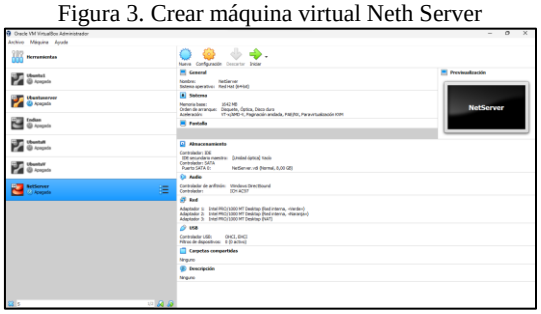
Figura 2. Versiones de descarga



Fuente: Autoría propia

Una vez se descargue la ISO, en VirtualBox creamos la virtualización de la máquina, ver Fig. 3, esta está basada en RedHat de 64bits.

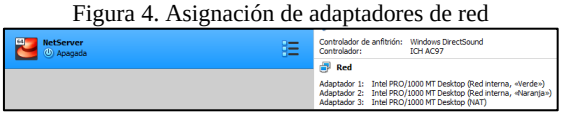
Figura 3. Crear máquina virtual Neth Server



Fuente: Autoría propia

Al crear la máquina virtual es necesario realizar unas primeras configuraciones con respecto a los adaptadores de red como se muestra en la Fig. 4, desktop – verde (LAN), server – naranja (DMZ), estas dos estarán como red interna y por último la red WAN – rojo, esta será configurada como NAT o Adaptador Puente.

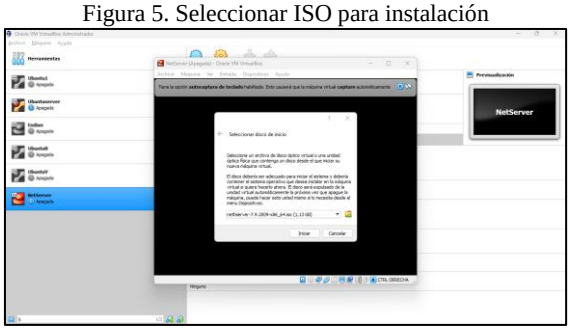
Figura 4. Asignación de adaptadores de red



Fuente: Autoría propia

Ya configurados los adaptadores de red, procedemos a iniciar la máquina virtual para continuar con la instalación y seleccionamos la ISO descargada, ver Fig. 5.

Figura 5. Seleccionar ISO para instalación



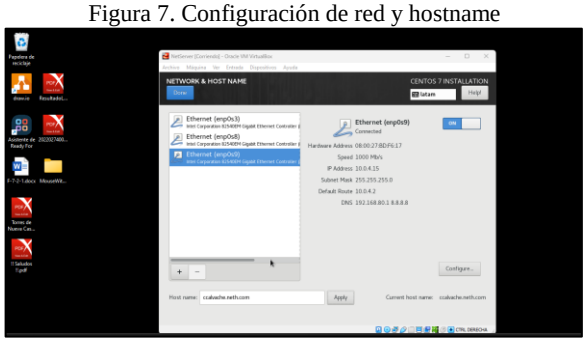
Fuente: Autoría propia

Iniciamos y nos muestra una ventana de configuraciones, se realizan las configuraciones de zona, teclado y redes en Fig. 6 y el Hostname en Fig. 7.

Figura 6. Ventana de configuración inicial

Fuente: Autoría propia

Figura 7. Configuración de red y hostname



Fuente: Autoría propia

Se crea la contraseña de ingreso para el usuario root desde el navegador o desde la consola. Ver Fig. 8.

Figura 8. Crear contraseña de usuario root

Fuente: Autoría propia

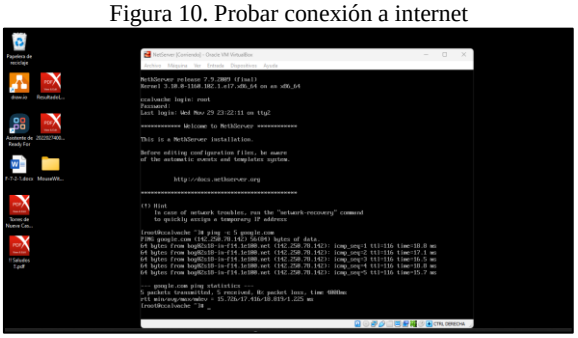
Una vez se finalice la instalación solicitará la autenticación en la consola del NethServer, ver Fig. 9.

Figura 9. Instalación finalizada

Fuente: Autoría propia

Realizamos la actualización de paquetes del servidor con el comando sudo yum update, cuando estén instalados damos reboot para que se configuren los nuevos paquetes y probamos que tengamos conexión a internet con un ping así como se puede observar en la Fig. 10.

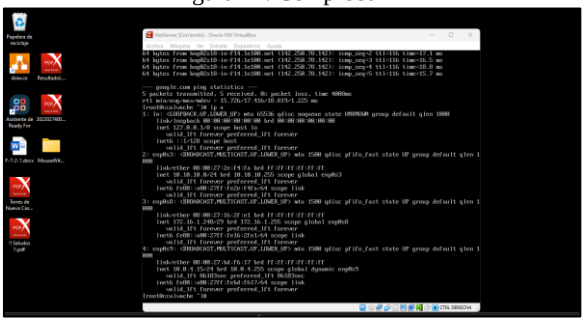
Figura 10. Probar conexión a internet



Fuente: Autoría propia

Es opcional realizar la validación de la configuración de las IP de adaptadores para las zonas verde (red interna), naranja (red interna) y roja (DHCP), identificación de direccionamiento IP en la Fig. 11.

Figura 11. Comprobar IP

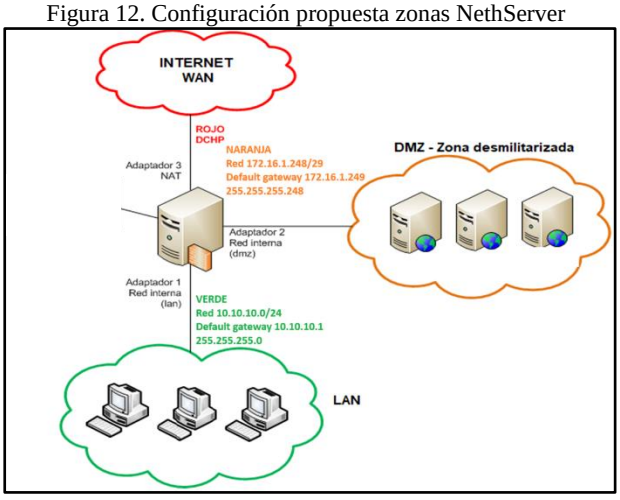


Fuente: Autoría propia

2.3 CONFIGURACIÓN

La configuración de las zonas de NethServer se realiza de acuerdo con la configuración ilustrada en la Fig. 12 estableciendo direcciones IP para la Zona Verde (LAN) y Naranja (DMZ) además de un acceso por DHCP a Internet.

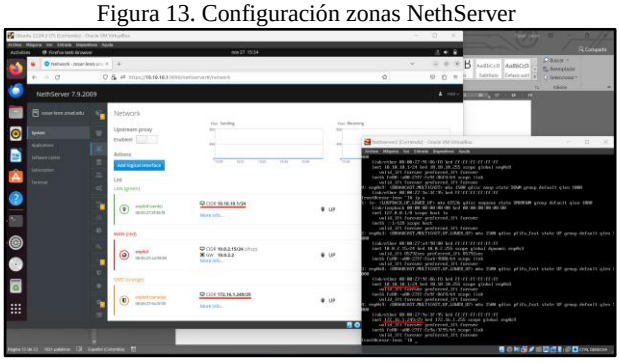
Figura 12. Configuración propuesta zonas NethServer



Fuente: Autoría Propia

Toda la configuración se realiza desde System -> Network de la GUI de NethServer como se aprecia en la Fig. 13. Esta misma configuración se puede validar directamente en la Terminal de NethServer utilizando el comando IP a, el cual detalla las direcciones IP de todas las interfaces de red habilitadas Fig. 13.

Figura 13. Configuración zonas NethServer



Fuente: Autoría Propia

3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

En esta temática se realiza la configuración de un servidor por DHCP, es decir la generación dinámica de la IP para el dispositivo, la configuración DNS para la máquina virtual Ubuntu desktop que representa la zona verde y será el sistema operativo desde donde se realizará la conexión a la interfaz gráfica de NethServer y este último será posible gracias al controlador de dominios.

Para poder realizar la configuración del acceso a una estación de trabajo GNU/Linux con un usuario y contraseña, lo primero que se debe realizar es la instalación del NethServer y tener instalada una máquina virtual desktop que para el ejercicio será la zona verde o red LAN, en la Fig. 14 se describe la configuración.

Figura 14. Configuración de adaptadores de red

Fuente: Autoría Propia

Una vez finalizada la instalación y la configuración inicial de adaptadores de red tanto del NethServer como en la máquina virtual Ubuntu desktop, desde el navegador de Windows o el sistema operativo con el que cuente la máquina física ingresamos a la dirección IP arrojada por el NethServer en la instalación del servidor, teniendo en cuenta que se debe hacer referencia al puerto 9090 para el acceso al servidor web, ver Fig. 15, esta dirección nos llevará a la interfaz gráfica web de NethServer.

https://192.168.80.33:9090/

Cuando ingresamos a la IP nos arroja la siguiente ventana:

Figura 15. Ventana inicial de NethServer

Fuente: Autoría Propia

En este punto se debe ingresar con el usuario root y la contraseña asignada al usuario en la instalación del servidor NethServer.

Ya teniendo acceso a la administración del servidor NethServer, debemos realizar la configuración del DNS como se muestra en la Fig. 16, para ello debemos ingresar en el menú a la opción DNS y realizar la asignación de IP que corresponde.

Figura 16. Panel de configuración DNS

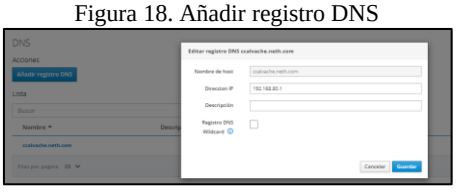
Fuente: Autoría propia

Añadimos un registro DNS ver Fig. 18, la dirección IP puede ser corroborada desde cmd de Windows como se ve en la Fig. 17.

Figura 17. Validación de IP para DNS

Fuente: Autoría propia

Figura 18. Añadir registro DNS



Fuente: Autoría Propia

La modificación de la IP del DNS también es posible realizarla desde la ventana de panel de control.

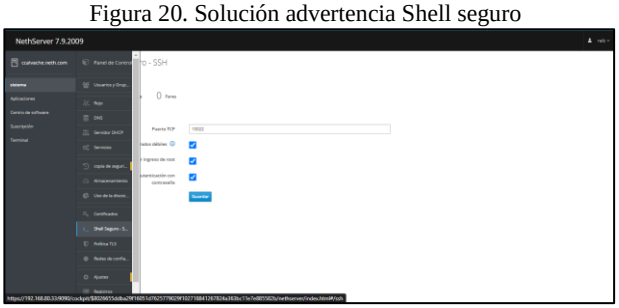
Realizamos la configuración del servidor DHCP en la sección del menú Servidor DHCP ver Fig. 19 en donde se debe habilitar la interfaz del adaptador y se da clic en escanear red, para que nos muestre la red disponible para conexión.

Figura 19. Configuración servidor DHCP

Fuente: Autoría Propia

Se deben eliminar algunas de las advertencias que genera el sistema ya que puede crear conflictos en la conexión de la red, por ejemplo, en el apartado de Shell seguro descrito en la Fig. 20.

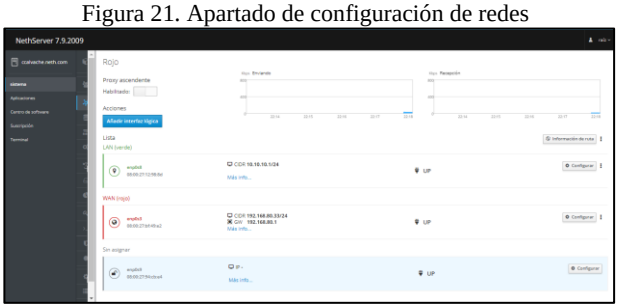
Figura 20. Solución advertencia Shell seguro



Fuente: Autoría propia

En el apartado de red realizamos la configuración de las zonas ver Fig. 21, incluyendo su dirección IP, si es dinámica o estática, indicar su máscara y su Gateway.

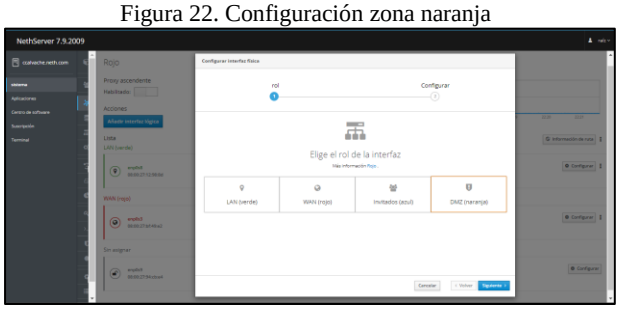
Figura 21. Apartado de configuración de redes



Fuente: Autoría propia

Por defecto aparece una zona verde, sin embargo, se debe crear otra que será la que se va a configurar para la red, la zona verde inicial será cambiada por la zona roja. En cada zona se da clic en el botón configuración y se ingresa la información que le corresponde, de igual forma con la zona naranja como se muestra en la Fig. 22.

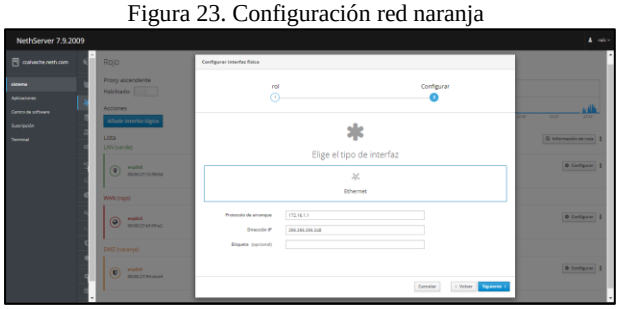
Figura 22. Configuración zona naranja



Fuente: Autoría propia

Se elige DMZ (naranja) y se le da siguiente, se muestra la ventana de configuración ver Fig. 23.

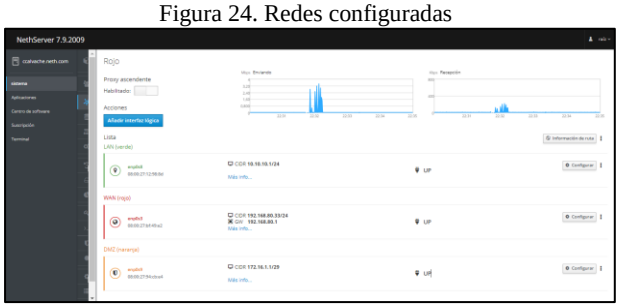
Figura 23. Configuración red naranja



Fuente: Autoría propia

Se muestran las tres redes configuradas y servicios activos en la Fig. 24 en este punto la red ya es funcional y se encuentra configurada de manera correcta.

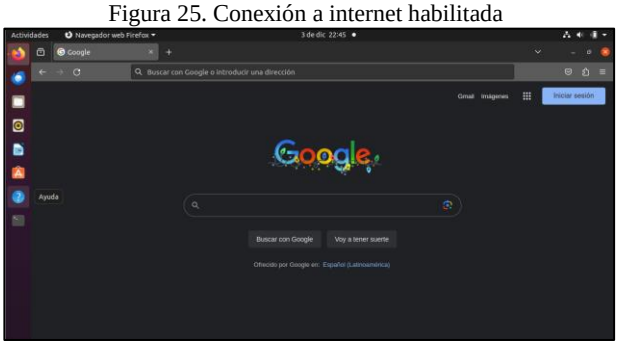
Figura 24. Redes configuradas



Fuente: Autoría propia

Ahora se debe iniciar la máquina virtual Ubuntu desktop que está configurada como zona verde, podemos validar la conexión a internet realizando un intento de navegación ver Fig. 25 y comprobamos la conexión con el servidor NethServer por medio de un ping a su IP ver Fig.26.

Figura 25. Conexión a internet habilitada



Fuente: Autoría propia

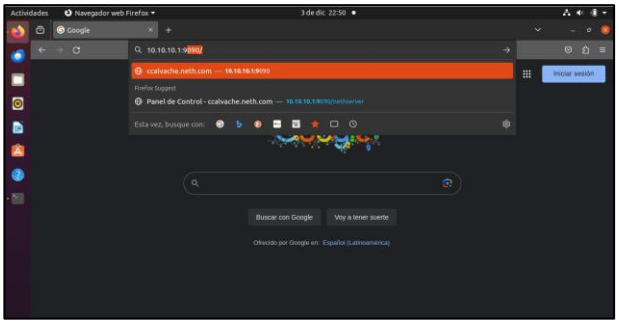
Figura 26. Conexión a Google y servidor NethServer

Fuente: Autoría propia

Desde el navegador de la máquina virtual ingresamos la dirección del servidor NethServer para ingresar a su interfaz gráfica, se reconoce el dominio del host configurado se muestra en la Fig.27, es decir, podremos ingresar también con este dominio.

Se muestra en la Fig. 28 el ingreso sin indicar el puerto 9090 y en la Fig. 29 se muestra el ingreso indicando el puerto 9090.

Figura 27. Reconoce el host configurado con la IP del NethServer



Fuente: Autoría propia

Figura 28. Ingreso con el dominio sin el puerto 9090

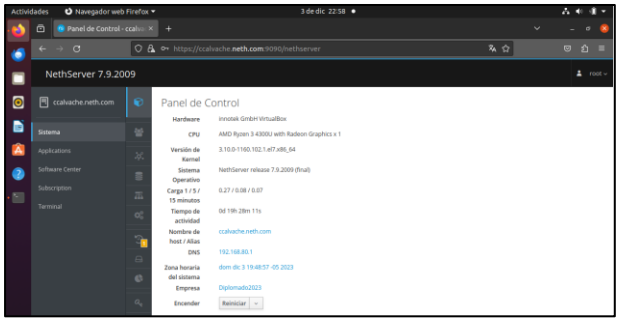
Fuente: Autoría propia

Figura 29. Ingreso con el dominio y con el puerto 9090

Fuente: Autoría propia

Se ingresa con el usuario y contraseñas creado root para llegar al panel de control, ver Fig.30.

Figura 30. Ingreso a interfaz gráfica por medio de máquina virtual

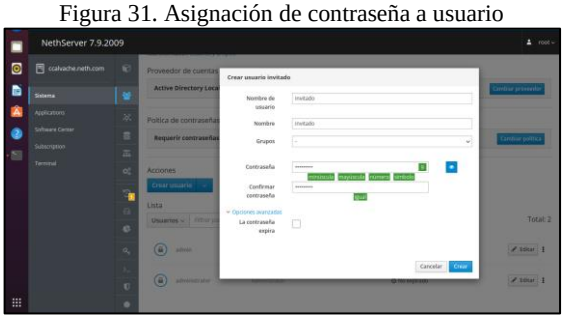


Fuente: Autoría propia

Se puede realizar la creación de usuarios para el ingreso, para ello se debe ingresar a grupos y usuarios y acceder al directorio activo ver Fig.31.

Se le asigna un IP de ingreso y un dominio, se crea el usuario y se asigna una contraseña.

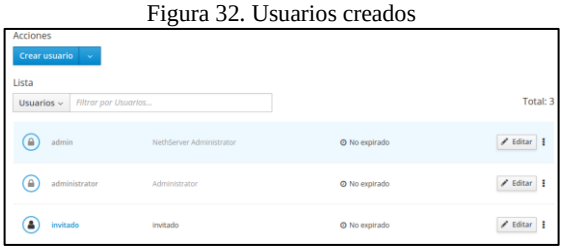
Figura 31. Asignación de contraseña a usuario



Fuente: Autoría propia

Lista de usuarios creados ver Fig.32.

Figura 32. Usuarios creados



Fuente: Autoría propia

4 PROXY

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.

Se procede a realizar la configuración del servicio proxy a través de ciertas configuraciones que se describirán a continuación.

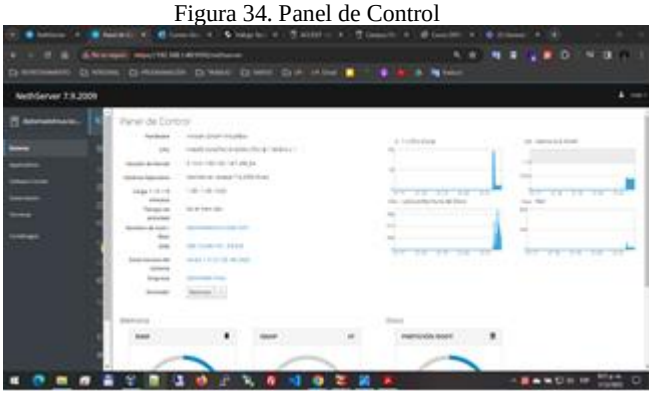
Vamos a ingresar a nuestro servidor NethServer por medio de su entorno gráfico como vemos en la Fig. 33 donde debemos colocar el usuario y contraseña.

Figura 33. Entorno gráfico

Fuente: Autoría propia

En el panel de control Fig. 34 se cambia las configuraciones en el apartado nombre del host se ingresa diplomadolinux.local.com y en el nombre de compañía se coloca diplomado Linux.

Figura 34. Panel de Control

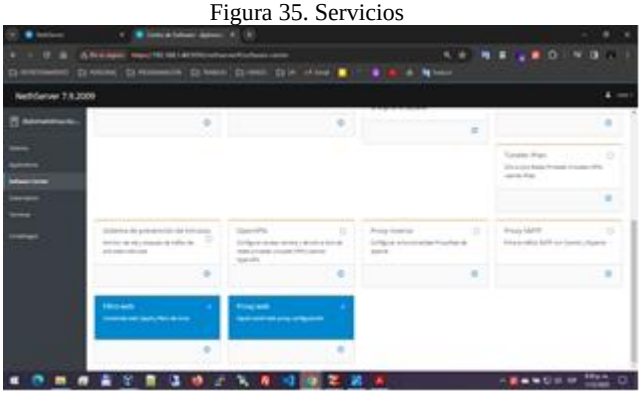


Fuente Autoría propia

Ahora nos dentro del apartado software center como se muestra en la Fig. 35 Entorno grafico y seleccionamos los servicios de:

Firewall
Proxy web
Filtro web

Figura 35. Servicios

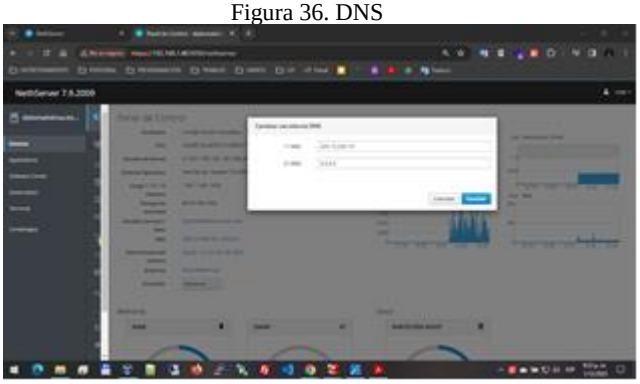


Fuente Autoría propia

Se realiza la configuración de la red.

Se realiza el cambio como se muestra en la Fig. 36 DNS los DNS en el panel de control colocando el respectivo DNS del proveedor de servicio de internet.

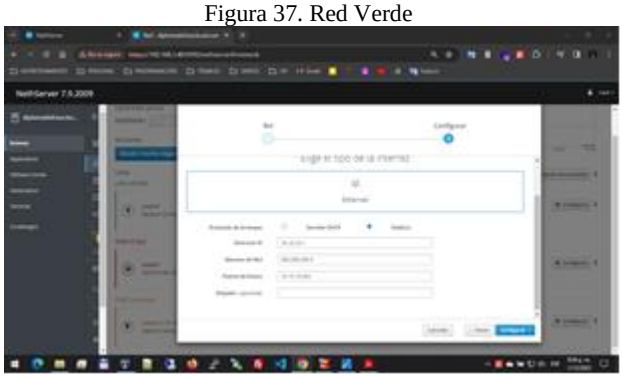
Figura 36. DNS



Fuente Autoría propia

La configuración de la zona verde con la tarjeta de red enp0s8 con la IP fija 10.10.10.1/24 y puerta de enlace 192.168.1.254 como se muestra en la Fig. 37 Red Verde.

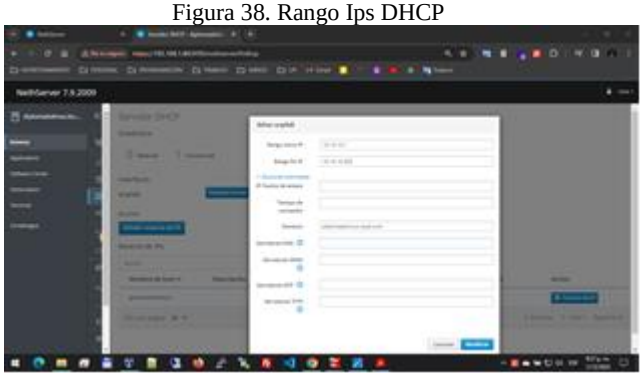
Figura 37. Red Verde



Fuente: Autoría Propia

Luego en la configuración de los servicios por DHCP para la red LAN, se establece un rango como se muestra en la Fig. 38 entre las siguientes direcciones inicio 10.10.10.2 hasta la IP 10.10.10.253, esto con el fin que cada usuario que se conecte se le asigne una IP dentro de este rango.

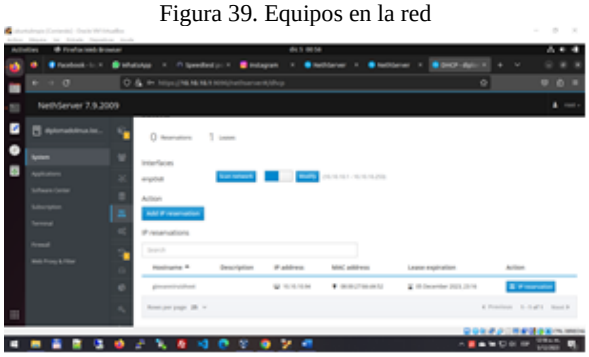
Figura 38. Rango Ips DHCP



Fuente: Autoría Propia

Cuando se configura la tarjeta de red en uno de los dispositivos que se tiene en la red LAN se puede ver en la Fig. 39 en el apartado DHCP donde se muestra un equipo de la red LAN.

Figura 39. Equipos en la red



Fuente: Autoría Propia

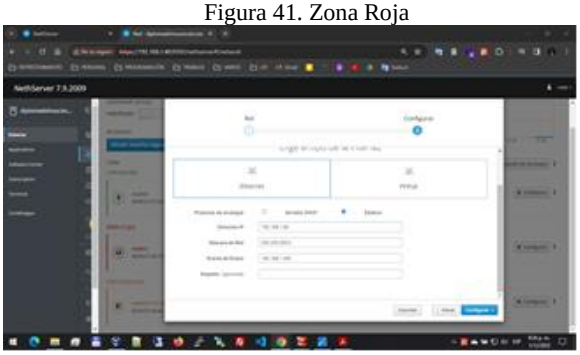
Se realiza pruebas de acceso a internet desde un equipo conectado desde la red LAN Fig. 40 y se observa el acceso a internet.

Figura 40. Acceso Internet.

Fuente: Autoría Propia

Se realiza la configuración de la zona DMZ naranja en la tarjeta de red enp0s9 con la dirección IP 172.16.1.249 / 29 y por último Fig. 41 se realiza la configuración de la zona roja con la siguiente dirección IP 192.168.1.40 con mascara 24 y puerta de enlace 192.168.1.254.

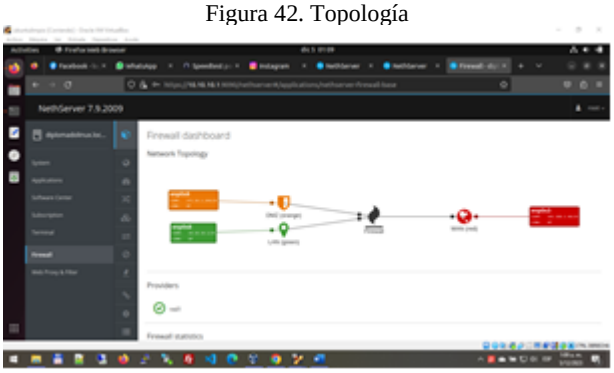
Figura 41. Zona Roja



Fuente: Autoría Propia

Confirmamos Fig. 42 el tipo de topología aplicada.

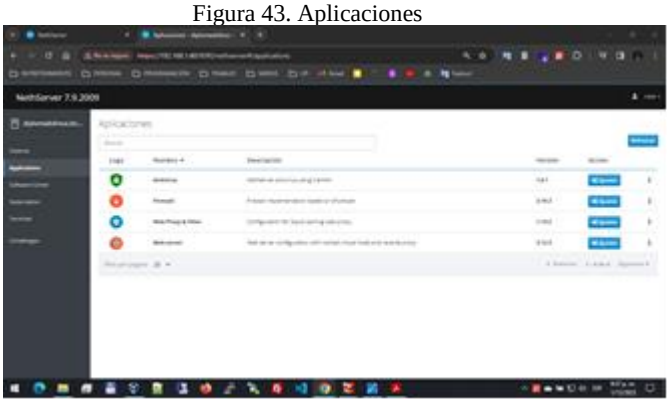
Figura 42. Topología



Fuente: Autoría Propia

Inicia la configuración del proxy para la zona verde desde la opción aplicaciones como se observa en la Fig. 43 Aplicaciones.

Figura 43. Aplicaciones



Fuente: Autoría Propia

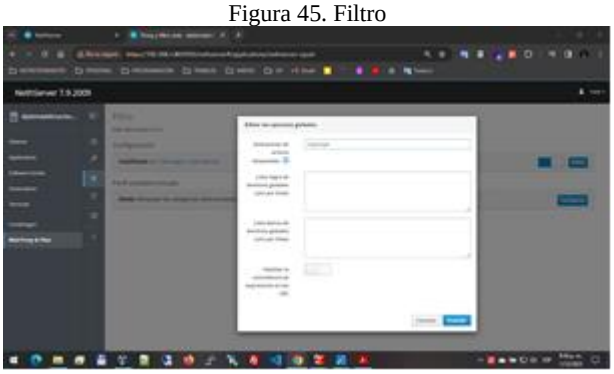
El proxi siempre está escuchando por el puerto 3128 en la Fig. 44 por lo que se realiza es la configuración de la zona verde colocando SSL transparente.

Figura 44. Configuración Proxy

Fuente: Autoría Propia

Luego se realiza la configuración de un filtro para luego si elegir como se muestra en la Fig. 45 la configuración de este filtro.

Figura 45. Filtro



Fuente: Autoría Propia

Se hace la configuración de agregar el tipo de restricciones que se aplicaran en el ejemplo como se muestra en la Fig. 46 se observa que se bloquea las páginas de redes sociales, chat y publicidad.

Figura 46. Filtro aplicado

Fuente: Autoría Propia

Al realizar la prueba se observa que a las páginas que anterior mente se tenía acceso, en el momento de activar el proxy se muestra un mensaje de bloqueo y que no está permitido el acceso como se muestra en la Fig.47.

Figura 47. Bloqueo

Fuente: Autoría Propia

Y en la Fig. 48 es una página que contiene mucha publicidad y que en el momento no muestra dichos anuncios.

Figura 48. Acceso Limitado

Fuente: Autoría Propia

5 CORTAFUEGOS

Implementación y configuración detallada para 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.

En esta temática se realiza la configuración de firewall para el servidor NethServer, es necesario instalar varios servicios que proveerán las distintas instancias de seguridad requeridas para su implementación, esta fase se realiza desde una máquina LAN dentro de la zona verde y será el sistema operativo desde donde se realizará la conexión a la interfaz de administración del servidor.

Para reducir el número de ataques de fuerza bruta es necesario realizar la configuración del puerto SSH [1], en este caso cambiamos del 22 al 10222 evitando accesos no deseados al puerto estándar por defecto como se muestra en la Fig.49.

Figura 49. Configuración puerto SSH

Fuente: Autoría Propia

En la opción de configuración de DNS debe agregar el host LAN como se muestra en la Fig.50.

Figura 50. Configuración del puerto DNS

Fuente: Autoría Propia

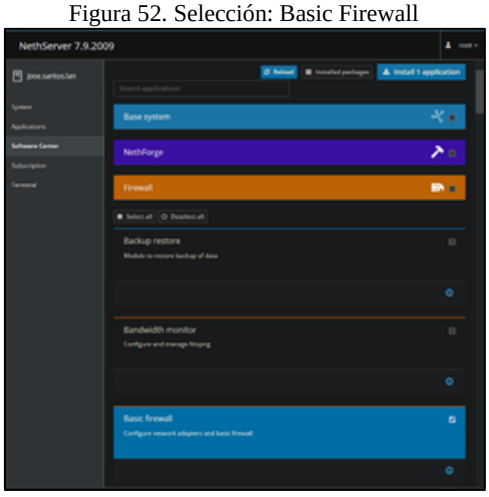
En la opción de servidor DHCP debe asignar el rango de IP del segmento de red y el dominio correspondiente a la zona Verde LAN como se muestra en la Fig.51

Figura 51. Configuración del servidor DHCP

Fuente: Autoría Propia

En la sección Software center del administrador del servidor se debe aplicar la descarga de los servicios necesarios, para ello ubique lo siguiente: Basic firewall, como se muestra en la Fig. 52.

Figura 52. Selección: Basic Firewall



Fuente: Autoría Propia

Ubique adicionalmente SMTP proxy, web filter y web proxy y proceda con la instalación de esos servicios como se muestra en la Fig. 53.

Figura 53. Selección: SMTP proxy, web filter y web proxy

Fuente: Autoría Propia

Espere a que finalice la instalación de los servicios seleccionados y luego reinicie el servidor como se muestra en la Fig.54.

Figura 54. Avance del proceso de instalación de servicios

Fuente: Autoría Propia

Active el Proxy y configúrelo como: Manual

En la sección "Políticas", clic en "Crear nueva política" para comenzar a configurar la política de filtro.

Asigne un nombre descriptivo a la política, como "Bloqueo Redes Sociales".

Seleccione las categorías de sitios web que debe bloquear [2]. En este caso, puede seleccionar categorías relacionadas con redes sociales como se muestra en la Fig.55.

Figura 55. Política de bloqueo y categoría

Fuente: Autoría Propia

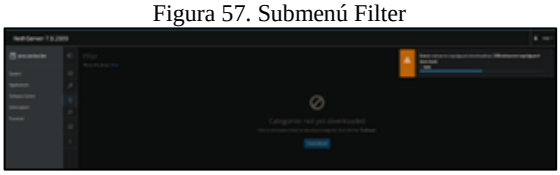
Configure el Web Proxy & filter mediante el botón azul Settings como se muestra en la Fig.56.

Figura 56. Selección Web Proxy & filter

Fuente: Autoría Propia

Una vez haya ingresado a las opciones de Web Proxy & filter ubique el submenú Filter y proceda a descargar las categorías como se muestra en la Fig. 57

Figura 57. Submenú Filter



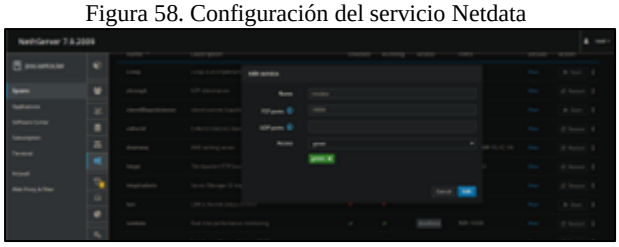
Fuente: Autoría Propia

En la sección Filtro Web del menú encienda y parametrice el filtro, luego seleccione Filtrado de usuarios donde creará un nuevo filtro de usuario y asigne la política creada anteriormente.

Aplique esta política a los usuarios o grupos específicos que debe restringir.

En el servicio Netdata edite el acceso para que solo quede green (Zona Verde) este realiza una recolección estadística para evitar penalizar el hardware lento y así permitir un mejor rendimiento de las IP y sitios ya visitados (Caché) como se muestra en la Fig.58.

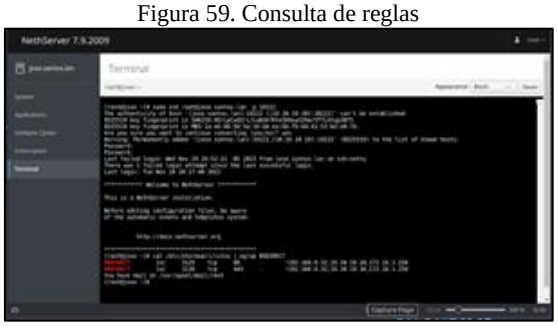
Figura 58. Configuración del servicio Netdata



Fuente: Autoría Propia

Se evidencia al menos 2 reglas activas que ya se están aplicando como se muestra en la Fig.59

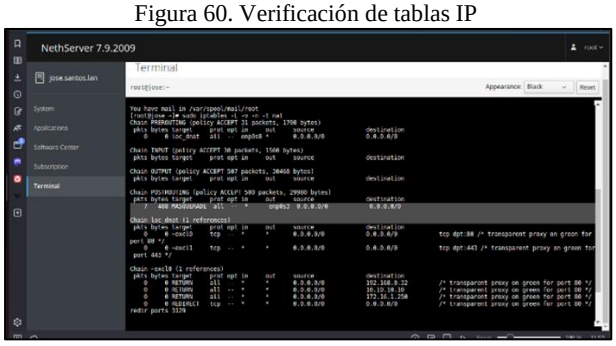
Figura 59. Consulta de reglas



Fuente: Autoría Propia

Consulta las tablas IP mediante el comando iptables del nat para verificar el proxy transparente y el destino como se muestra en la Fig.60.

Figura 60. Verificación de tablas IP



Fuente: Autoría Propia

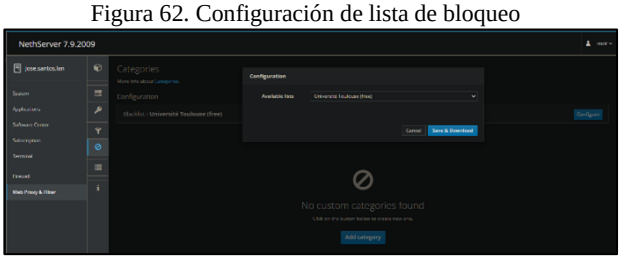
Se puede evidenciar tras la configuración anterior el bloqueo de anuncios publicitarios gracias a las reglas aplicadas, como se muestra en la Fig.61.

Figura 61. Bloqueo de publicidad en página web.

Fuente: Autoría Propia

Configure la lista de bloqueo, por defecto se puede seleccionar la lista de la Universidad de Tolouse [3], aunque también es posible crear una lista propia como se muestra en la Fig.62.

Figura 62. Configuración de lista de bloqueo



Fuente: Autoría Propia

Luego edita el filtro en Web Proxy & Filter adicionando los formatos de video y audio mp3 y mp4 como se muestra en la Fig.63.

Figura 63. Edición del Filtro Web Proxy & Filter

Fuente: Autoría Propia

Seguidamente en el menú principal del sistema edita el filtro en el botón Edit global options como se muestra en la Fig.64.

Figura 64. Botón: Edit global options

Fuente: Autoría Propia

Active las opciones Enable global blacklist y Enable global whitelist, seleccione el modo Block selected categories, allow the rest y en Categorías adicione las que requiera dentro de las predeterminadas, en este caso: Social_networks como se muestra en la Fig.65.

Figura 65. Opciones de lista negra y lista blanca, modo y categorías.

Fuente: Autoría Propia

Finalmente comprobamos el bloqueo a redes sociales, aunque están en caché pronto evidenciamos el bloqueo de estas, como se muestra en la Fig. 66 y Fig.67.

Figura 66. Bloqueo de acceso a la red social Facebook

Fuente: Autoría Propia

Figura 67. Bloqueo de acceso a la red social Mastodon

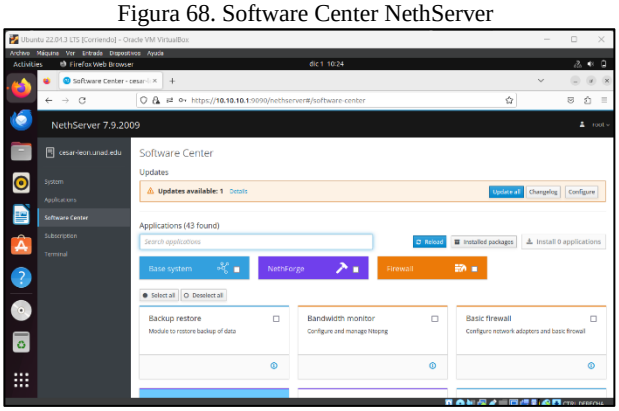
Fuente: Autoría Propia

6 VPN

Se realiza la instalación de OpenVPN desde el Software Center de NethSever y se configura la VPN para lograr un acceso externo a la red LAN directamente a uno de los hosts con Ubuntu Desktop como sistema operativo.

La configuración de la VPN desde NethServer se realiza de acuerdo con el procedimiento referenciado en [4]. La instalación de OpenVPN se realiza desde el Software Center de NethServer como se aprecia en la Fig.68.

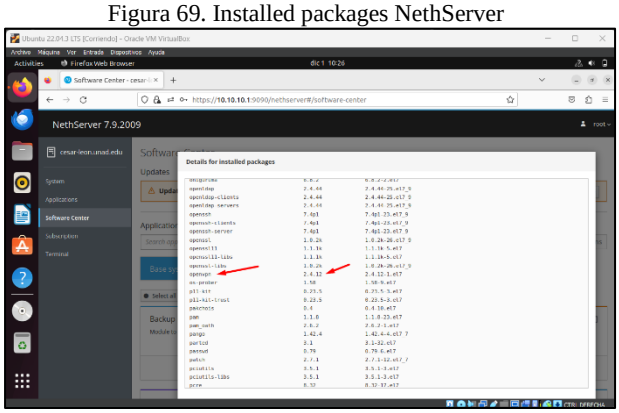
Figura 68. Software Center NethServer



Fuente: Autoría Propia

Se valida que OpenVPN haya quedado instalado con la función “Installed packages” de NethServer como se aprecia en la Fig.69. La versión de OpenVPN instalada es la 2.4.12.

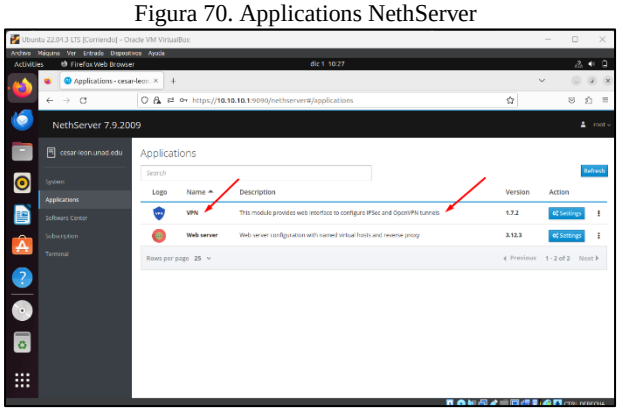
Figura 69. Installed packages NethServer



Fuente: Autoría Propia

Otra forma de validar la instalación es yendo a Applications donde se encuentra disponible la aplicación VPN como se aprecia en la Fig.70. Aquí mismo se puede iniciar con el proceso de configuración referenciado en [4].

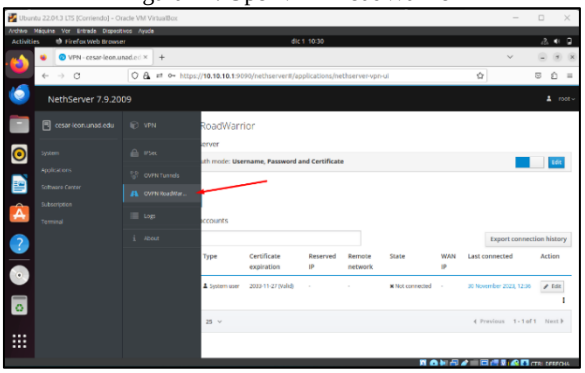
Figura 70. Applications NethServer



Fuente: Autoría Propia

Se inicia con la configuración de OpenVPN RoadWarrior como se ve en la Fig. 71 que, de acuerdo con lo referenciado en [5], se utiliza cuando se requiere conectar múltiples clientes a una red interna como el caso planteado en el presente artículo.

Figura 71. OpenVPN RoadWarrior



Fuente: Autoría Propia

Lo que se pretende con la VPN es simular una conexión externa a las máquinas virtuales (desde un host físico con Windows). Por lo tanto, se configura la interfaz para la Zona Roja de NethServer como Bridged en lugar de NAT como se aprecia en la salida de NethServer de la Fig.72.

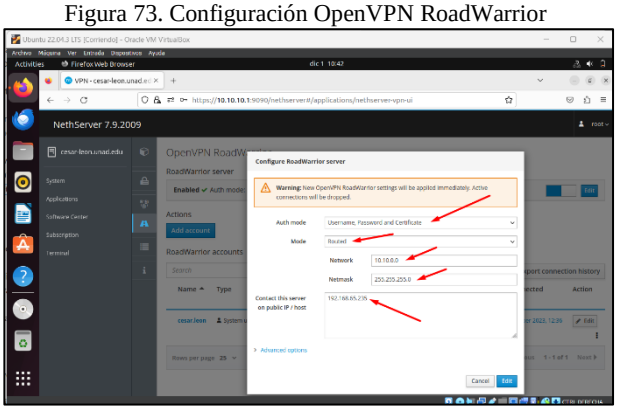
Figura 72. Configuración interfaces de red en NethServer

Fuente: Autoría Propia

Para el ejemplo planteado en el presente artículo, la primera interfaz de red de NethServer toma la dirección IP 192.168.65.235/24 como se aprecia en la Fig. 72 que se utiliza en la configuración de OpenVPN RoadWarrior.

Dentro de OpenVPN RoadWarrior y como se aprecia en la Fig. 73 se configura la VPN con la opción Auth mode en Username, Password and Certificate, Mode en Routed, se establece como Network la red 10.10.0.0 (Debe ser una red diferente a las configuradas para la LAN y DMZ de NethServer), una Netmask 255.255.255.0 que se encuentra en el segmento /24 o en cualquier otro, y en la opción Contact this server on public IP / host se define la IP 192.168.65.235 (que tomó NethServer en la configuración Bridged mencionada).

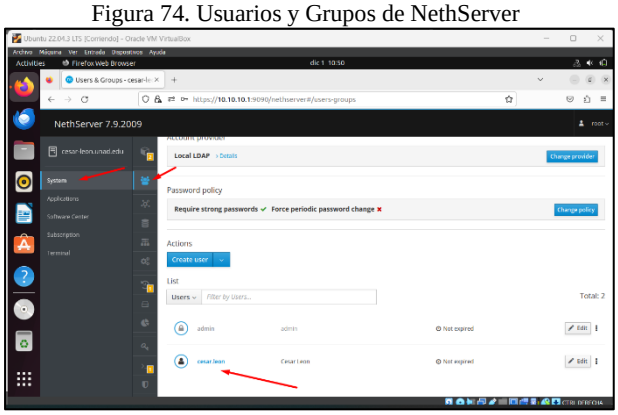
Figura 73. Configuración OpenVPN RoadWarrior



Fuente: Autoría Propia

Para utilizar OpenVPN se requiere mínimo de un usuario de sistema (system user), este se debe crear primero en System -> Users & Groups de NethServer como se aprecia en la Fig.74.

Figura 74. Usuarios y Grupos de NethServer

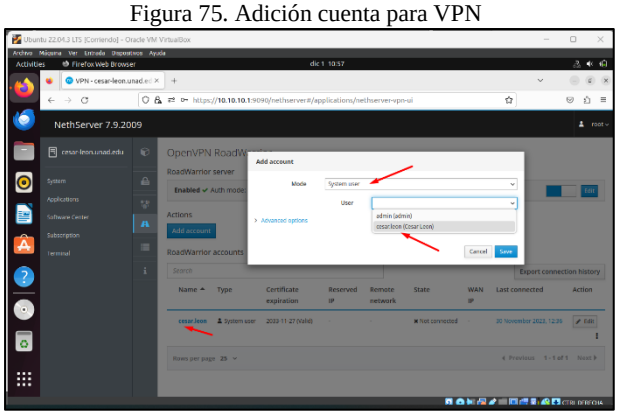


Fuente: Autoría Propia

Para crear el usuario de sistema se debe instalar la funcionalidad de LDAP (Lightweight directory access protocol) de manera que OpenVPN pueda determinar las credenciales del usuario que utilizará la VPN. En el ejemplo de la Fig.74, el usuario creado en el LDAP fue cesar.leon.

De vuelta en Applications -> OpenVPN RoadWarrior, como se aprecia en la Fig.75, se agrega la cuenta con el usuario de sistema cesar.leon para simular el acceso a la VPN. De esta manera, se finaliza con la configuración.

Figura 75. Adición cuenta para VPN

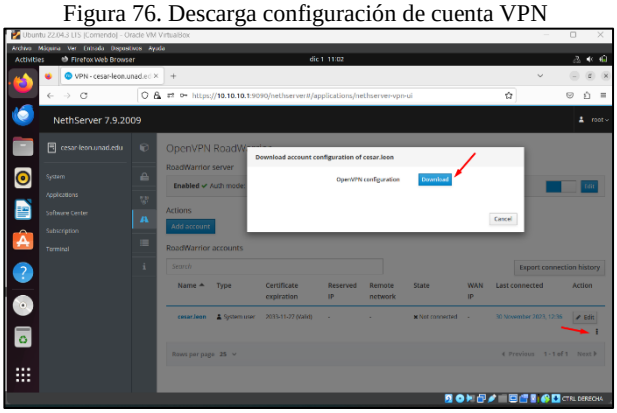


Fuente: Autoría Propia

Con el fin de probar la configuración, se genera una conexión a la VPN desde una red externa (host físico con Windows 11) siguiendo el procedimiento referenciado en [6].

En primer lugar, desde el usuario de sistema de OpenVPN creado en el ejemplo planteado en este artículo, se realiza la descarga de la configuración de la VPN para este usuario como se aprecia en la Fig.76, que después se utilizará para establecer la conexión desde el PC físico con sistema operativo Windows a la red de máquinas virtuales con sistema operativo Linux y administrada por NethServer (Ubuntu Desktop, Ubuntu Server, NethServer).

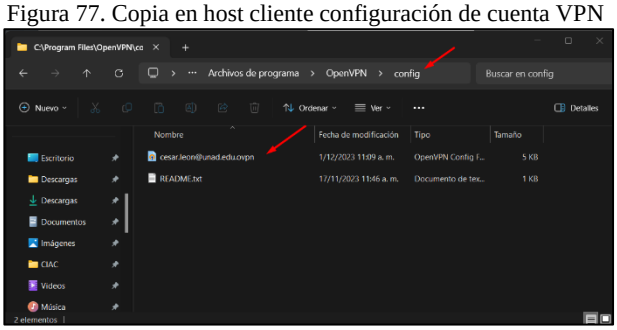
Figura 76. Descarga configuración de cuenta VPN



Fuente: Autoría Propia

Como se probará la conexión desde un host físico con Windows 11, se debe descargar OpenVPN desde el website oficial referenciado en [7]. Después de instalado, se copia el archivo de configuración descargado desde OpenVPN de NethServer en la ruta de Windows C:\Program Files\OpenVPN\Config o en la ruta donde se haya instalado como se detalla en la Fig.77.

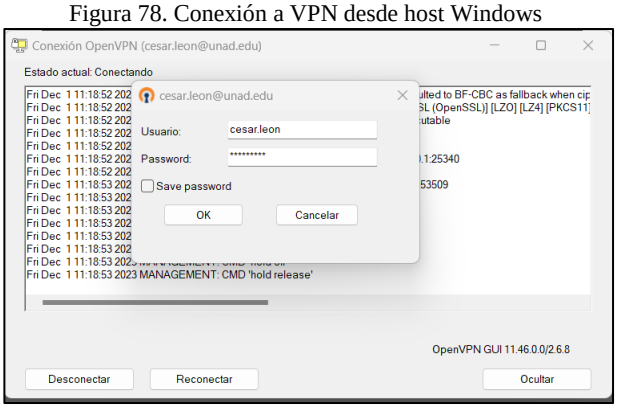
Figura 77. Copia en host cliente configuración de cuenta VPN



Fuente: Autoría Propia

Copiado el archivo de configuración, se abre OpenVPN en Windows y se ingresa la contraseña creada para el usuario de sistema de OpenVPN en NethServer como se aprecia en la Fig.78.

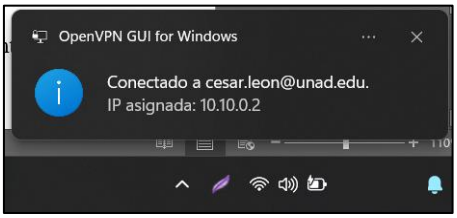
Figura 78. Conexión a VPN desde host Windows



Fuente: Autoría Propia

De esta manera se establece una conexión exitosa como se aprecia en la Fig. 79 desde Windows 11 a los recursos administrados por NethServer.

Figura 79. Conexión exitosa a VPN desde host Windows



Fuente: Autoría Propia

Con el fin de probar el acceso desde la VPN a los recursos de NethServer (LAN, DMZ), se instala la aplicación xrdp de acceso remoto en la máquina virtual con Ubuntu Desktop para poder acceder desde el escritorio remoto de Windows siguiendo el procedimiento referenciado en [8] y se valida que el servicio xrdp esté corriendo como se aprecia en la Fig.80.

Figura 80. Validación servicio xrdp en Ubuntu Desktop

Fuente: Autoría Propia

Además, se verifica que el puerto de acceso remoto a Ubuntu Desktop es el 3389.

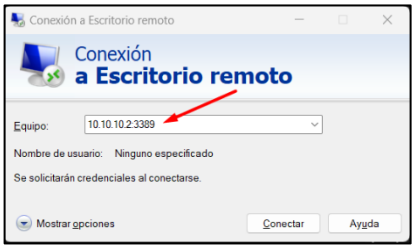
Como la conexión con la VPN ya está establecida, y Ubuntu Desktop ya tiene configurada una IP válida en la zona verde de NethServer (LAN) como se aprecia en la Fig.81, es posible establecer la conexión por escritorio remoto de Windows a Ubuntu Desktop.

Figura 81. Dirección IP Ubuntu Desktop en LAN

Fuente: Autoría Propia

Para la conexión por escritorio remoto de Windows, se utiliza la IP de Ubuntu Desktop y el puerto 3389 empleado por el servicio xrdp como se aprecia en la Fig.82. Muy importante tener en cuenta que, para acceder a Ubuntu por escritorio remoto, la cuenta de usuario a emplear debe estar cerrada.

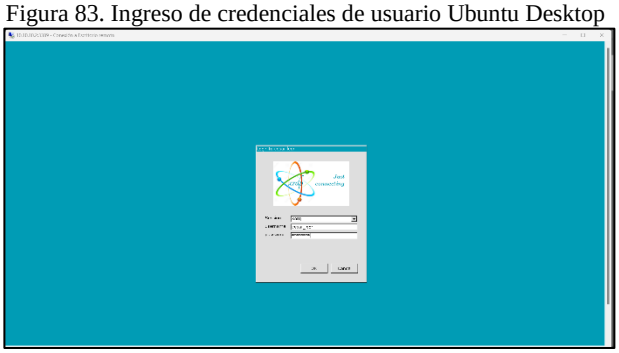
Figura 82. Credenciales escritorio remoto Windows



Fuente: Autoría Propia

Establecida la conexión por escritorio remoto gracias a la VPN, se ingresan las credenciales del usuario de Ubuntu Desktop como se aprecia en la Fig. 83 para habilitar el acceso.

Figura 83. Ingreso de credenciales de usuario Ubuntu Desktop



Fuente: Autoría Propia

De esta manera se establece una conexión exitosa a los recursos administrados por NethServer como se aprecia en la Fig. 84 usando el escritorio remoto de Windows y la VPN.

Figura 84. Acceso a Ubuntu Desktop por escritorio remoto

Fuente: Autoría Propia

7 CONCLUSIONES

Tener el servidor NethServer es muy útil, ya que se podrá controlar y administrar los usuarios con permisos de acceso, los cambios que se puedan presentar en la red y su configuración, además de permitir el acceso desde una máquina remota, virtual o móvil, esto gracias a la asignación de IP por DHCP y DNS según corresponda en la red.

Se logra comprender como se realiza la configuración de proxy para una red LAN y WAN estableciendo ciertos Filtros para

controlar el tráfico de nuestra red.

Se ha presentado la implementación del firewall en NethServer, un sistema operativo de servidor de código abierto. El firewall de NethServer es un firewall de estado completo que proporciona una amplia gama de funciones para proteger las redes en entornos empresariales. Se evidencia que el firewall de NethServer es una herramienta potente y flexible como barrera robusta contra amenazas externas y controlar el tráfico interno de manera efectiva. Su implementación es sencilla y se puede hacer en pocos pasos, ofreciendo funciones para proteger las redes, incluyendo el filtrado de tráfico, la inspección de paquetes y la prevención de intrusiones. La implementación del firewall de NethServer es una tarea importante para cualquier administrador de red. El firewall puede ayudar a proteger la red. Se recomienda actualizar el firewall regularmente con las últimas reglas de seguridad, utilizar un sistema de detección de intrusiones (IDS) para detectar posibles amenazas e implementar una política de seguridad de la información para guiar el uso del firewall.

OpenVPN es una herramienta que ofrece conectividad a usuarios localizados remotamente que soporta una amplia configuración. OpenVPN en conjunto con NethServer facilitan la parametrización de una red privada virtual incluso para gente inexperta en este tipo de tecnología.

8 REFERENCIAS

[1] Manuel Cabrera Caballero. (2018). Nethserver Tutorial | Instalación, actualización y primeros pasos [En línea]. Disponible en https://youtu.be/FNGmM-2fa_0?t=1110

[2] Madrid, O. (2020). Nethserver OZSEC SL por Oriol Madrid [En línea]. Disponible en https://youtu.be/__az-6xPC6k?t=845

[3] NethServer Community. (2017, Julio 28). Nethserver Firewall and Squid Guard [En línea]. Disponible en https://community.nethserver.org/t/nethserver-firewall-and-squid-guard/7463/5

[4] NethServer (2017, Octubre). How to configure Open VPN [En línea]. Disponible en https://community.NethServer.org/t/how-to-configure-open-vpn/8027

[5] NethServer (2023). VPN [En línea]. Disponible en https://docs.NethServer.org/en/v7/vpn.html

[6] NethServer (2015, Septiembre). How can I configure vpn server? [En línea]. Disponible en https://community.NethServer.org/t/how-can-i-configure-vpn-server/1508

[7] OpenVPN (2023, Noviembre). Community Downloads [En línea]. Disponible en https://openvpn.net/community-downloads/

[8] PhoenixNAP (2023, Octubre 12). How to Access Ubuntu via Remote Desktop from Windows [En línea]. Disponible en https://phoenixnap.com/kb/ubuntu-remote-desktop-from-windows

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

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

Canonical (2018). Guía del Ubuntu desktop 18.04 LTS. Help Ubuntu. [En línea]. Disponible en https://help.ubuntu.com/18.04/ubuntu-help/index.html

Debian (2020). El manual del administrador de Debian 10.04. [En línea]. Disponible en https://www.debian.org/doc/manuals/debian-handbook/index.es.htmlhttps://www.debian.org/doc/manuals/debian-handbook/index.es.html

Fandiño, B. (2023). Zonas de red en Netshserver. [En línea]. Disponible en https://www.youtube.com/watch?v=KoluHFwFiOY&t=31s

Lab Virtuales Servidores (2023). Instalar #NethServer + Configurar Web Proxy & Filtrar Contenidos Web. [En línea]. Disponible en https://www.youtube.com/watch?v=cIHJbtTehKg&t=1901s