

# SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX NETHSERVER

Gilberto Varela Sánchez  
e-mail: gilvarsan@gmail.com  
Francia Edith Duran Santa  
email: frdurans@unadvirtual.edu.co  
Janer Eduardo Cubillos Rentería  
email: jcubillosr2604@gmail.com  
Ruben Alberto Gomez Mosquera  
e-mail: ragomezmos@unadvirtual.edu.co

**RESUMEN:** *La administración de servidores es una de las principales ventajas de Linux. De esta forma la distribución Nethserver se convierte en una alternativa eficiente para medianas y pequeñas empresas, gracias a su entorno amigable, manejo de tiempos y simplicidad en sus procesos.*

*En el desarrollo de esta actividad, trabajaremos una de las cinco temáticas propuestas ofreciendo soluciones a partir de la aplicación e implementación de los conocimientos adquiridos usando como herramienta principal GNU/Linux, enfocándonos en la instalación y configuración de varios servicios que aseguren y brinden el respaldo de una infraestructura tecnológica robusta para una empresa.*

**PALABRAS CLAVE:** Linux, DHCP, NethServer, Infraestructura, DNS, Server, Controlador de dominio.

## 1 OBJETIVOS

### 1.1 OBJETIVO GENERAL

Formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de una infraestructura tecnológica que permita dar respuesta a los requerimientos específicos de la compañía.

### 1.2 OBJETIVOS ESPECIFICOS

- Implementar y configurar el acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Nethserver.
- Controlar acceso a conectividad internet de estaciones GNU/Linux a través del puerto 3128 de un servidor proxy.

## 2 INSTALACION DE NETHSERVER

NethServer es una distribución basada en Linux, más específicamente en CentOS y Red Hat, la cual está orientada específicamente a actuar como servidor en pequeñas y medianas empresas.

Es un sistema operativo muy modular al cual se le pueden incorporar fácilmente nuevos plugins y software adicional para aumentar sus opciones predeterminadas. A partir de la versión 7.7 se ofreció una interfaz muy intuitiva que ofrece un diseño más moderno. La interfaz proporciona herramientas para administrar cuentas, DNS, DHCP, FQDN, configurar aplicaciones, administrar el almacenamiento y los certificados

SSL, también permite configurar VPN, evaluar el tráfico de cada túnel, rastrear el historial de conexión de cada usuario, definir rutas propias, cambiar el protocolo UDP/TCP, entre otras características.

## 2.1 REQUISITOS

Los requerimientos para instalar NethServer son:

- 64 bit CPU (x86\_64)
- 1 GB de RAM
- 10 GB de espacio en disco
- Interfaz de red (al menos una)
- Unidad óptica de arranque (DVD, USB) para instalaciones en servidores físicos.

Se recomienda utilizar al menos 2 discos para configurar un RAID 1. El software RAID garantizará la integridad de los datos en caso de fallo del disco.

## 2.2 ENLACE DE DESCARGA

[https://github.com/NethServer/dev/releases/download/iso-7.9.2009/nethserver-7.9.2009-x86\\_64.iso](https://github.com/NethServer/dev/releases/download/iso-7.9.2009/nethserver-7.9.2009-x86_64.iso)

## 2.3 PRÁCTICA 1

Para realizar la instalación de NethServer crearemos una máquina virtual en VirtualBox con la configuración recomendada



Figura 1 Máquina virtual para instalar Nethserver

Luego de crear la máquina virtual procedemos a realizar la instalación de NethServer

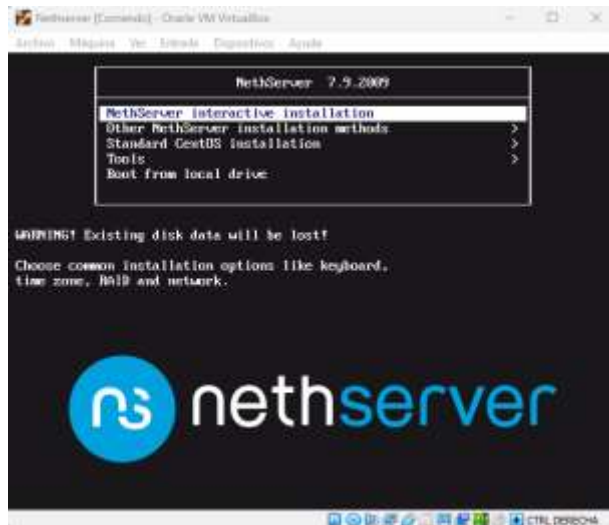


Figura 1. Pantalla de instalación

Configuramos la fecha y hora del sistema y la distribución del teclado



Figura 2. Configuración de fecha/hora y distribución del teclado

Revisamos la configuración de red y establecemos el nombre que llevará el servidor

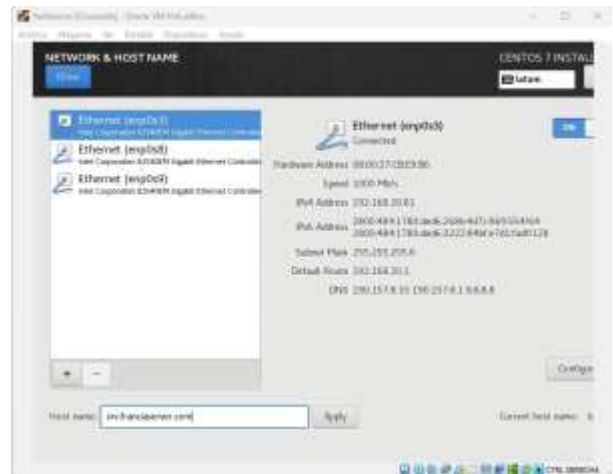


Figura 3. Configuración de red y nombre del servidor

Procedemos a instalar y se nos pedirá una contraseña, si lo deseamos podemos crear una cuenta de usuario nueva, pero para el desarrollo de este ejercicio solo asignaremos la contraseña al usuario root y continuamos con la instalación.

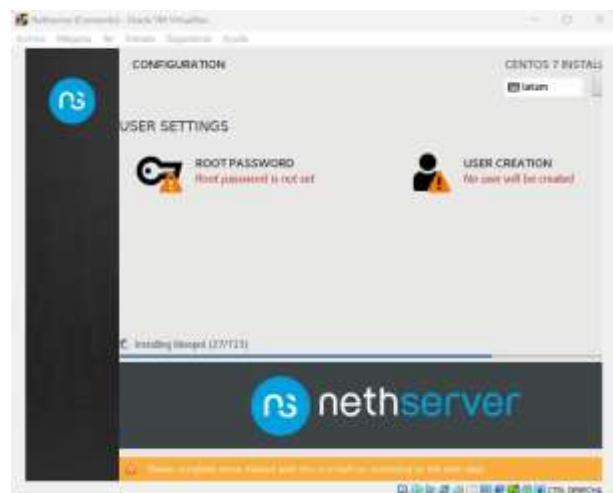


Figura 4. Estableciendo contraseña de acceso

Una vez finalizada la instalación, podemos iniciar sesión con el usuario root y la contraseña establecida.



Figura 5. Acceso con el usuario root y contraseña establecida

Procedemos a realizar una actualización de sistema usando el comando yum update.

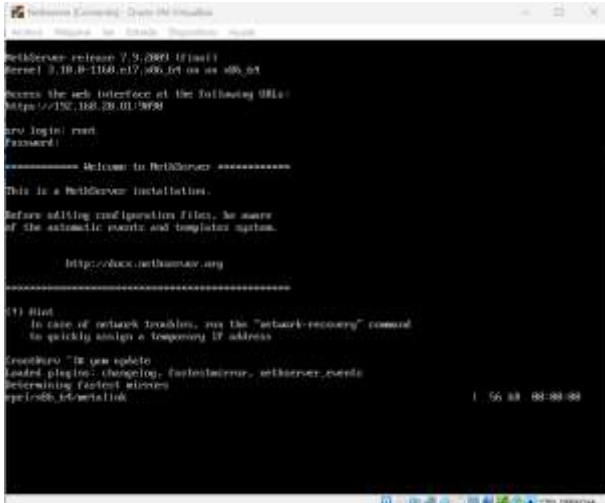


Figura 6. Realizando proceso de actualización

Una vez finalizada la actualización de los paquetes, procedemos a comprobar el acceso desde otra máquina.

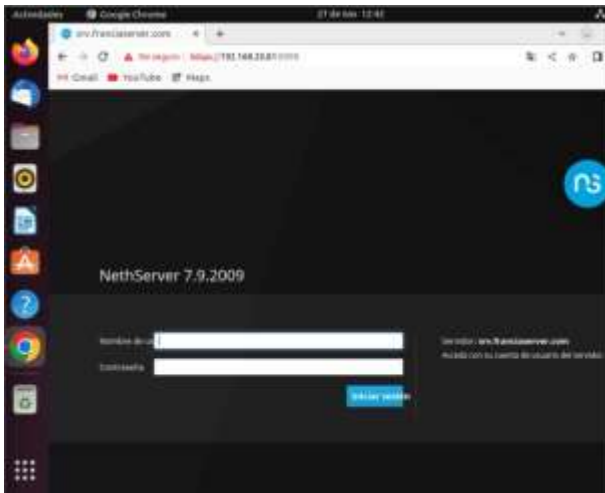


Figura 7. Comprobando acceso desde navegador web

### 3 DESARROLLO TEMÁTICA

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

Para validar el funcionamiento de los servicios usaremos dos máquinas, una con Ubuntu Server desde la que accederemos a las configuraciones del NethServer y otra con Ubuntu desktop que estará conectada a la red LAN.



Figura 8. Máquinas de comprobación

Desde la máquina con Ubuntu Server, accedemos al servidor por medio del navegador y validamos que se encuentre instalado y actualizado.

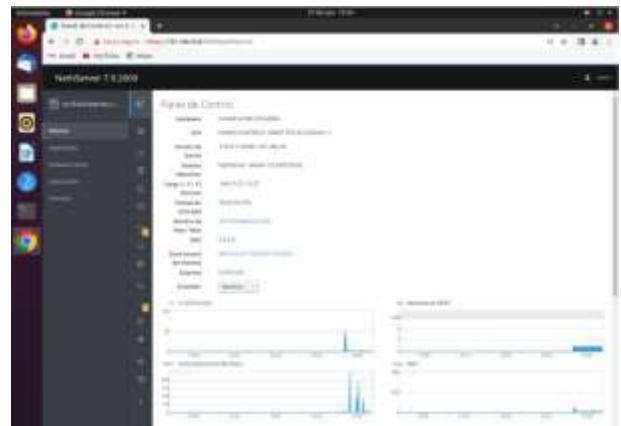


Figura 9. Verificación del servidor

Procedemos a configurar las redes para las conexiones de los dispositivos. Primero configuramos la red WAN (Roja) para dejarla con acceso a internet.

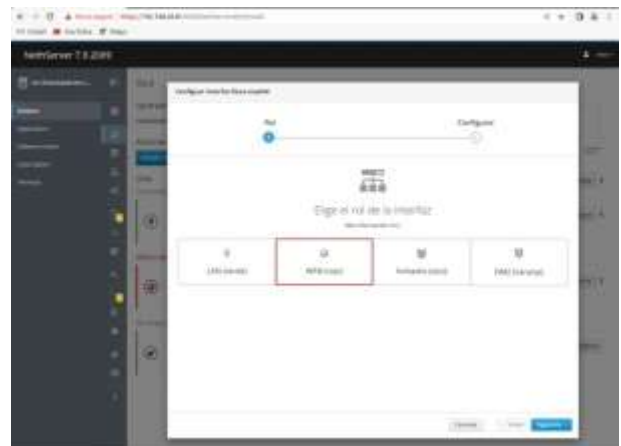


Figura 10. Configuración de red WAN.

Asignamos una IP estática, para que el servidor DHCP no la cambie automáticamente al momento de reiniciar la máquina.

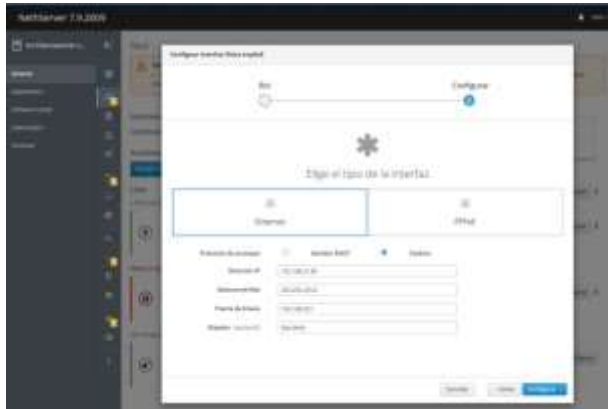


Figura 11. Asignación de IP estática

Configuramos la red LAN (verde). Para evitar conflictos de red, asignamos una dirección IP diferente a la asignada para la red WAN.

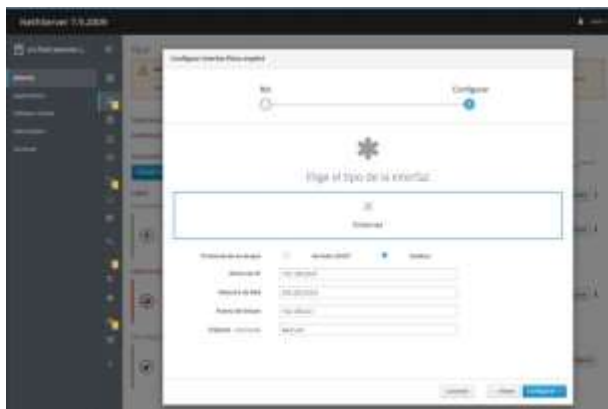


Figura 12. Configuración red LAN

Validamos la configuración realizada en las redes.

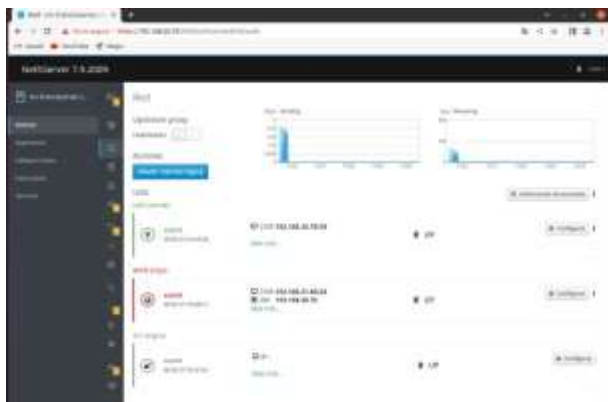


Figura 13. Validación de redes creadas

Procedemos a configurar el servidor DHCP.

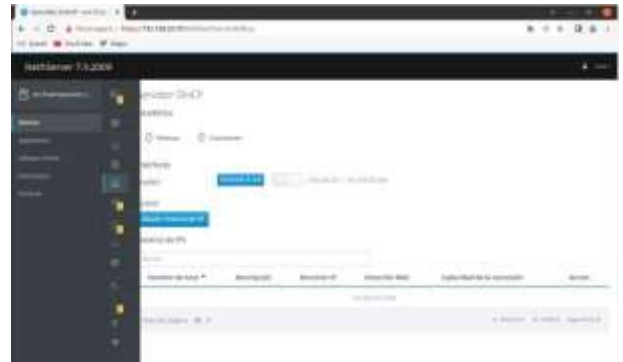


Figura 14. Configuración servidor DHCP

Asignamos las direcciones IP para habilitar un rango de 90 dispositivos.



Figura 15. Creación rango IP

Validamos que el rango establecido se encuentre habilitado y haya queda registrado.

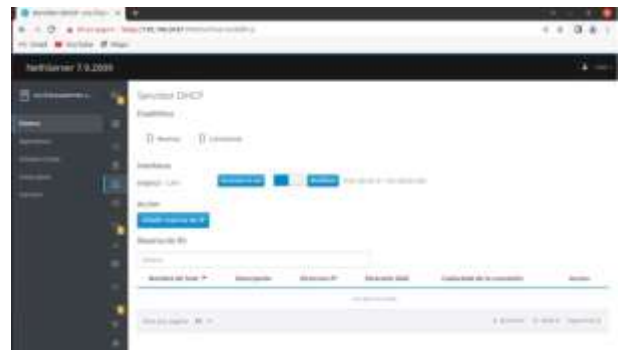


Figura 16. Validación de rango creado

Comprobamos el funcionamiento, para esto iniciamos sesión en la máquina con Ubuntu desktop la cual debe estar configurada para cargar en la red LAN. A esta se le asignará una IP y lo mostrará en el panel de control como uno de los equipos conectados.

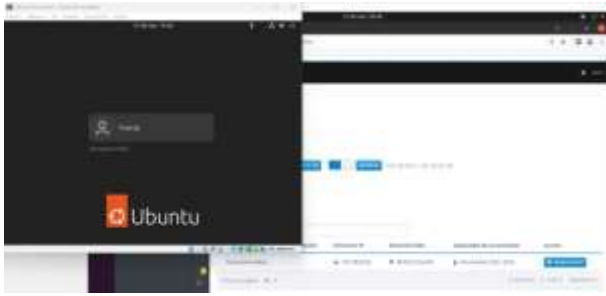


Figura 17. Comprobación de funcionamiento servidor DHCP

Procedemos a configurar el servicio DNS, para habilitarlo ingresamos a la opción de DNS en el navegador.



Figura 18. Configuración servicio DNS

Definimos un nombre de dominio, para este ejemplo usaremos la misma IP del NethServer.



Figura 19. Definiendo nombre de dominio

Se debe tener en cuenta que las solicitudes solo se verán en clientes locales y solo los equipos en la red LAN podrán visualizarlas.

Tratamos de ingresar desde la máquina Ubuntu Server y nos debe mostrar que tiene problemas para conectarse ya que este equipo se encuentra fuera de la red LAN.



Figura 20. Comprobación de acceso bajo nombre de dominio en máquina Ubuntu Server

Realizamos el mismo procedimiento desde la máquina Ubuntu desktop y debemos acceder sin ningún problema.



Figura 21. Comprobación de acceso bajo nombre de dominio en máquina Ubuntu Desktop

### 3.2 TEMÁTICA 2: PROXY

Para el desarrollo de la temática, inicialmente se realizó la instalación y configuración de un sistema Nethserver, donde fue necesario realizar configuraciones básicas, como: configuración de interfaces, configuración de servidor DHCP, configuración de DNS, entre otras.

Luego de instalar Nethserver se accedió a la administración de este, a través de la dirección 192.168.1.30 configurada para la interfaz WAN, desde el equipo Ubuntu desktop.



Figura 23. Acceso a administrador Nethserver

Al realizarse las configuraciones básicas iniciales mencionadas anteriormente, es necesario descargar los paquetes web proxy y web filter en el apartado de Software center.



Figura 24. Paquetes disponibles en Software center

Instalados los paquetes necesarios, se ingresa al apartado de aplicaciones a verificar los servicios instalados.



Figura 25. Servicios instalados

Se procede a activar el servicio proxy entrando a los ajustes de este. En donde la zona verde se configura en modo Transparent SSL, con lo cual se evita realizar configuraciones adicionales en los clientes. Cabe mencionar que, al no tener una interfaz de zona azul contemplada, esta se deja en su valor por defecto (Manual).



Figura 26. Activación servidor proxy

Paso seguido a la activación del servicio, es necesario realizar una descarga de listados con categorías que ayudan a realizar los filtrados de sitios en la red. Para esto se ingresa al apartado de categorías, donde se selecciona una opción disponible. Igualmente es posible adicionar categorías personalizadas, para esta practica solamente se usó la opción de "Universit  Toulouse (free)".



Figura 27. Activaci n categor as

Descargadas las listas de categor as o configuradas listas personalizadas se hace uso de estas desde el apartado filtro. En este es posible configurar perfiles personalizadas, mas sin embargo se configurar  el perfil predeterminado que se aplica a todos los clientes que no cuenten con un perfil especifico. Adem s, se activa la funci n de antivirus en este apartado.



Figura28. Categor as seleccionadas a bloquear

Terminadas las configuraciones m nimas para el buen funcionamiento del servicio proxy, se procedi  a realizar algunas pruebas de funcionamiento.

Inicialmente se valida el acceso a Facebook, que se encuentra en la categor a de redes sociales, la cual se eligi  para bloquear. Luego se validar  el acceso a MediaFire catalogo como file hosting, categor a igualmente bloqueada.



Figura 29. Validaci n acceso a Facebook



Figura 30. Validando acceso a MediaFire

Por ultimo se valida una categor a que no haya sido bloqueada, por lo tanto, se realiza la prueba con la categor a audio y video, espec ficamente en YouTube.



Figura 31. Validando acceso a YouTube

Con esto, se logra validar el correcto funcionamiento del servidor proxy, cabe acotar que todo el tráfico pasa por el puerto 3128, el cual queda configurado por defecto al activar el sistema.

Existe la posibilidad de revisar estadísticas como: sitios mas bloqueados, equipos con mas bloqueos, categorías más bloqueadas, entre otras.



Figura 32. Estadísticas de bloqueo proxy

### 3.3 TEMÁTICA 3: CORTAFUEGOS

Realizado el proceso de instalación de Nethserver es posible la administración de este desde una terminal con acceso a la red donde esté conectado el servidor. Es importante que se realice una actualización de los paquetes usando el comando “yum update”.

Desde el cockpit se realiza la instalación del paquete básico Firewall ingresando en la zona de Software Center. Se debe ser cuidadoso con la configuración de la red pues una mala configuración impedirá la conexión a los sitios de descarga de los paquetes, presentándose el error `code: system-packages/update`. Si todo está correcto, tendremos disponible la administración del Firewall instalado en el espacio de Applications.

El cortafuegos es un sistema de seguridad que permitirá bloquear accesos no autorizados a un ordenador mientras se da la comunicación con otros servicios autorizados.

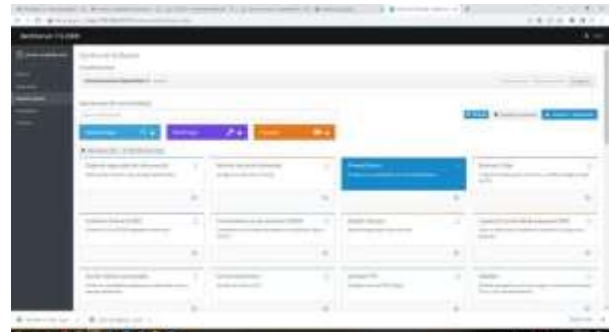


Figura 33. Software center de Nethserver para instalar firewall básico

Se deben realizar ajustes de parámetros de seguridad como el ssh y cambios de ip dinámicas a estáticas para las tarjetas de red, así como la configuración de las zonas verdes, rojas y naranjas de la red. De esta manera se podrán establecer las listas blancas y negras. Estas corresponden a un listado de sitios que tienen acceso y los que no tienen acceso desde las terminales que estén configurados con el cortafuegos.



Figura 34. Configuración de puerto ssh



Figura 35. Topología de red

Se realiza la definición de las reglas del Firewall, estableciendo los filtros en el cual se establecen las restricciones a los sitios de entretenimiento y redes sociales como Instagram o los que determine el equipo de administración de los servicios TICs de la empresa.

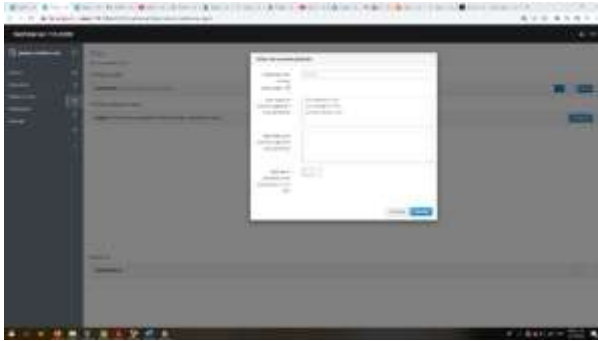


Figura 36. Reglas globales cortafuegos

Se establecen categorías personalizadas con la cual se filtrará el tráfico en la red.



Figura 37. Creación de categorías

En la administración del cortafuegos se define el perfil por defecto agregando las categorías personalizadas que se han creado y las categorías que vienen en la lista Université Toulouse (libre) de nuestro interés por ejemplo la social\_networks y adult.



Figura 38. Edición de perfil por defecto

En la terminal se procede a la configuración del navegador parametrizando la dirección del servidor proxy que realizara el filtrado.

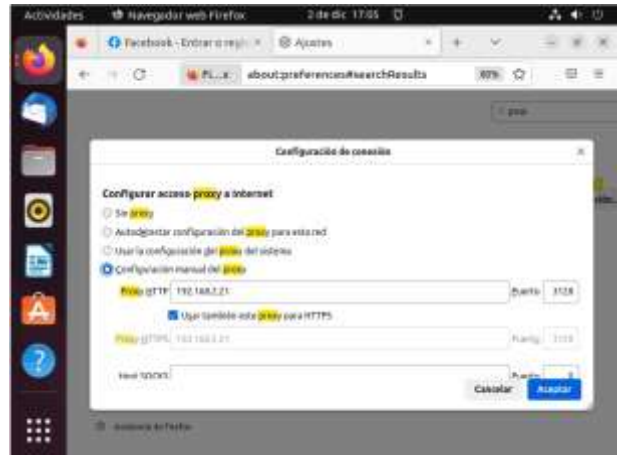


Figura 39. Configuración del terminal

A continuación, se valida el funcionamiento de los filtros en la estación de trabajo para redes sociales y adultos.

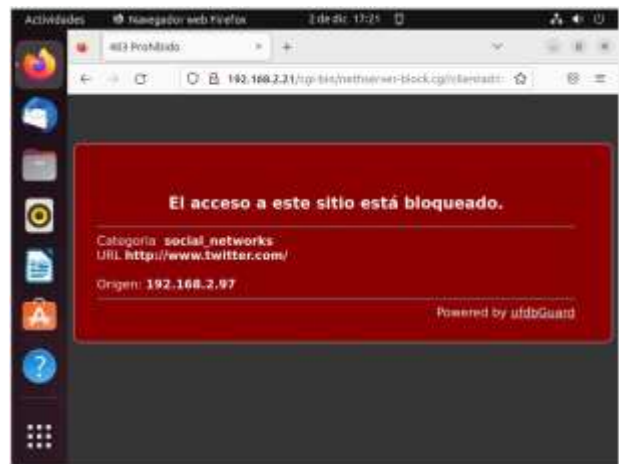


Figura 40. Acceso bloqueado a sitio de red social

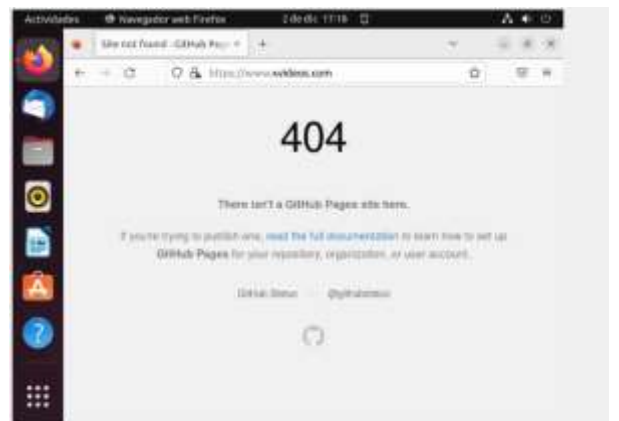


Figura 41. Acceso bloqueado a entretenimiento

### 3.4 TEMÁTICA 5: VPN

Para el desarrollo de la temática 5, se realizó la instalación y configuración del sistema NethServer, donde se realizó configuraciones básicas, como las interfaces de red.

Una vez instalado NethServer se puede acceder a la administración desde el navegador en la ruta <https://192.168.1.10:9090> configurada para la interfaz WAN, desde el equipo Ubuntu que está en la LAN.



Figura 42. Configuración de interfaces de red

Desde software Center se realiza la búsqueda y posterior instalación del paquete del servicio de la VPN.

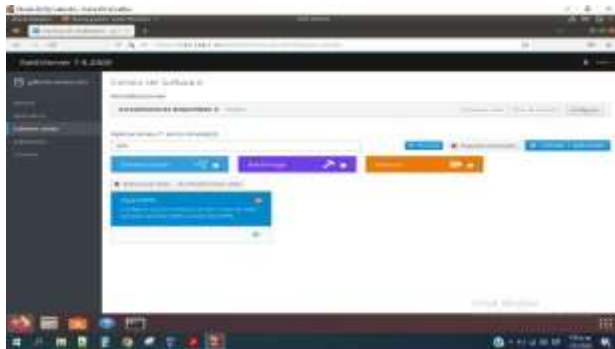


Figura 43. Búsqueda servicio VPN

Una vez instalado el paquete de la VPN podemos ver los servicios ya instalados desde la opción de Applications. Se activa el servicio VPN accediendo a los ajustes de este.

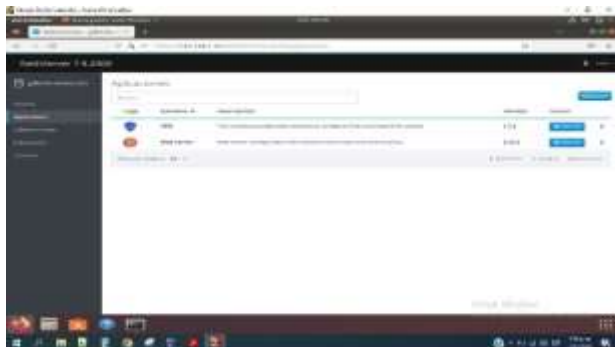


Figura 44. Servicios instalados

Luego de ingresar se procede a configurar el servidor OpenVPN en modo roadwarrior - o modo guerrero – que conecta un cliente remoto a la red.

Los métodos de autenticación admitidos son:

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

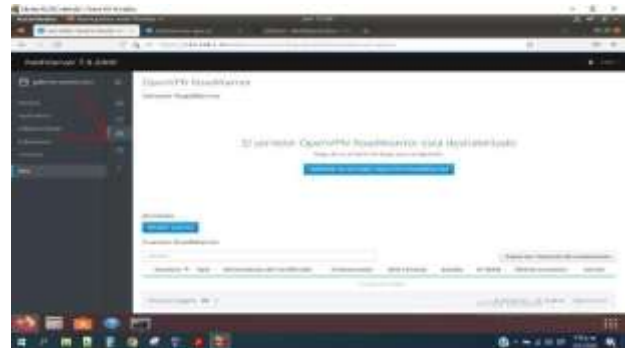


Figura 45. Servidor OpenVPN RoadWarrior

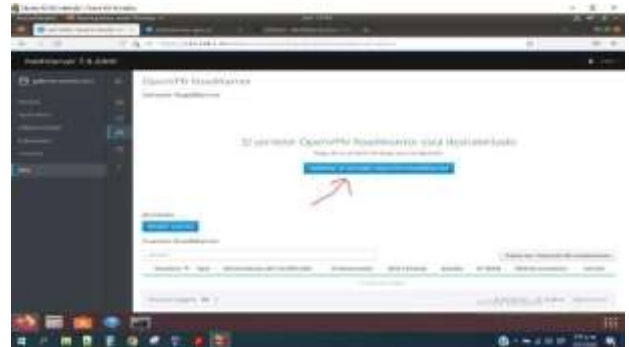


Figura 46. Habilitar Servidor OpenVPN RoadWarrior

Se habilita una modal en la cual se realiza la configuración como tal de la VPN donde se indica que:

- Método de autenticación: Certificado, el cual el usuario va a acceder por medio de un certificado a la VPN.
- Modo: Enrutado, para indicar por medio de cual segmento de red va a acceder el usuario.
- Red: IP del segmento con el cual van a acceder los usuarios.
- Mascara de Red: la máscara correspondiente a la IP dada en la red.
- Host Publico: corresponde la IP que tiene la WAN.

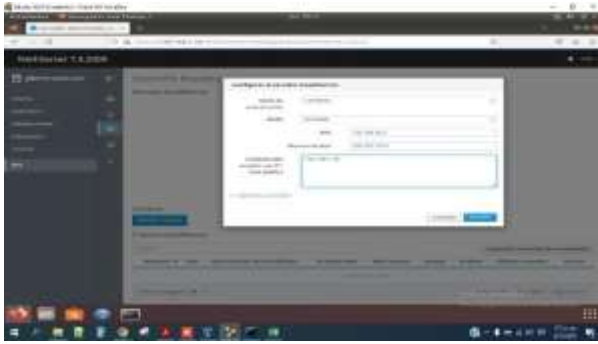


Figura 47. Configuración Servidor OpenVPN RoadWarrior

Se procede a añadir una cuenta para generar el certificado con el cual se va a conectar el usuario.

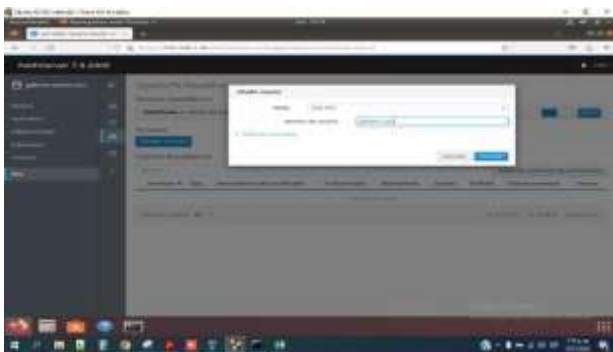


Figura 48. Adicionando cuenta RoadWarrior

Una vez generado la cuenta se puede visualizar cuando vence el certificado y el estado actual que es desconectado.

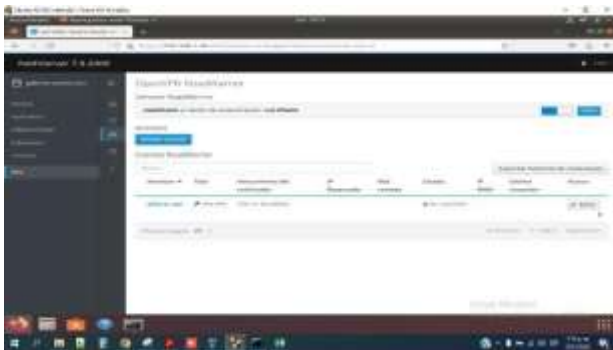


Figura 49. Visualización de la cuenta RoadWarrior

Ya con la cuenta generada se puede descargar el certificado que es el que se le va a entregar al usuario que requiere acceder a la VPN.

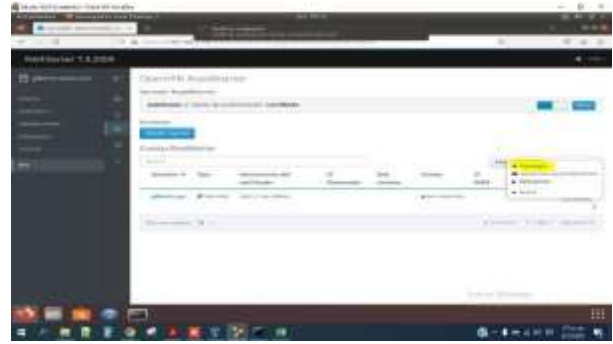


Figura 50. Opción de descarga del certificado paso 1.



Figura 51. Opción de descarga del certificado paso 2.

Ya con el certificado descargado se procede a realizar validación del funcionamiento de la VPN.

Antes de nada, se verifica que no tengamos conexión desde el Ubuntu Desktop con el equipo Ubuntu que está en la red LAN dando ping a la IP 192.168.20.2 y desde el navegador a una página HTML.

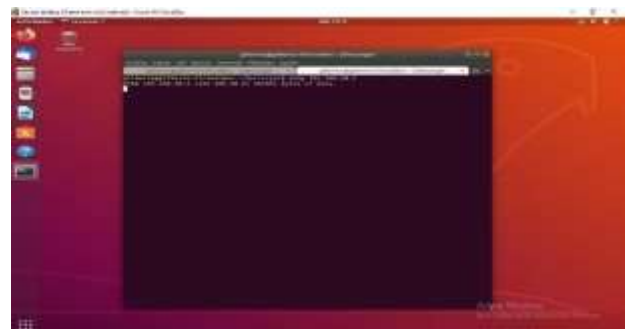


Figura 52. Validación con ping a la IP.



Figura 53. Validación desde el navegador.

Una vez instalado el paquete Cliente Open VPN en el Ubuntu Desktop se ejecuta el comando para activar el servicio con el certificado descargado anteriormente.

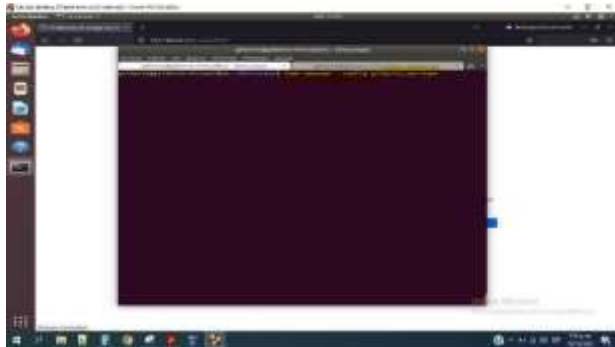


Figura 53. Activación VPN con el certificado.

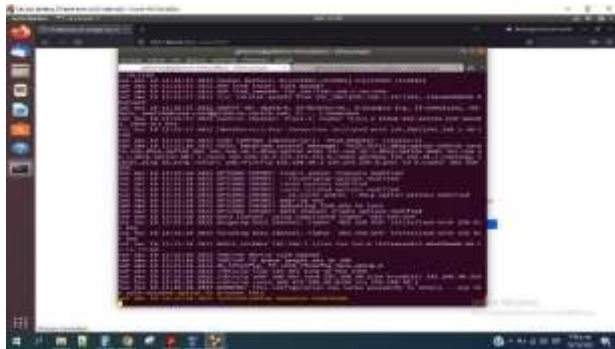


Figura 54. VPN activada correctamente.

Una vez activa la VPN se verifica conexión con el equipo que está en la red LAN por medio del ping antes generado y accediendo a la página HTML.

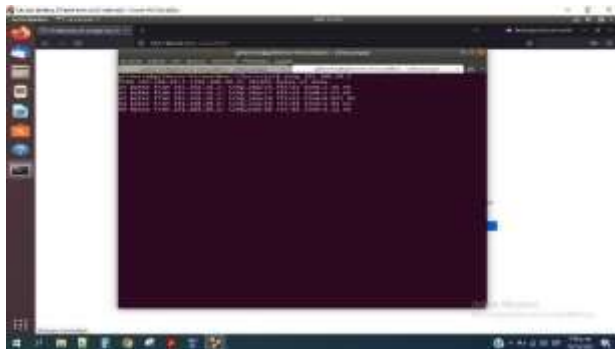


Figura 55. Ping generado correctamente.



Figura 56. Se visualiza la página correctamente.

Desde la administración del NethServer podemos visualizar la fecha y hora de conexión del usuario a la VPN y también del estado en el que se encuentra que es conectado con su respectiva IP 192.168.30.2, de igual manera desde los logs de conexión.

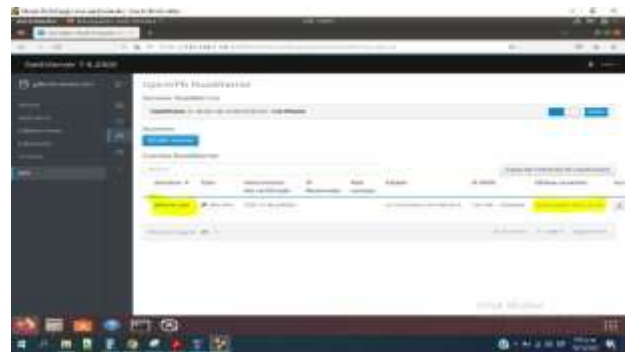


Figura 57. Conexión desde la cuenta del usuario.



Figura 58. Log de conexiones.

## 4 CONCLUSIONES

Durante el desarrollo de esta actividad, se evidencia un sencillo proceso de instalación y configuración de un servidor ayudados con NethServer. El conjunto de servicios ofrecidos nos proporciona una herramienta potente y de fácil configuración teniendo en cuenta las respectivas reglas de redireccionamiento, configuradas en sus respectivas redes.

Un servidor Proxy es una herramienta fundamental para aquellas organizaciones que pretenden garantizar la fiabilidad y eficiencia de sus operaciones pues permite realizar una gestión confiable del tráfico de cada uno de los equipos de la red. Con este es posible realizar los bloqueos pertinentes a sitios

malintencionados o que no sean necesarios acceder de acuerdo con las funciones de la empresa.

Una de las distribuciones óptimas para la implementación de infraestructura IT es el Nethserver, permitiendo la configuración de todos los servicios necesarios para el fortalecimiento de la seguridad en el tráfico de la red como lo es el cortafuegos entre otros. Durante el desarrollo de esta última fase se pudo de una manera practica resolver las diferentes situaciones que se presentan al instalar y configurar tecnologías como estas, particularmente la implementación del cortafuegos, desde la instalación del servidor, así como el acceso desde la web al Cockpit para administrar el servidor, instalando los componentes adicionales, definiendo reglas y categorías para restringir el acceso o tráfico de red a sitios que políticamente se han clasificado en la empresa como de alto riesgo o no aptos para el acceso desde las estaciones de trabajo. En general este proceso académico ha sido significativo pues se ha puesto en práctica todos los conocimientos adquiridos durante el semestre.

Desde la administración del NethServer se puede integrar fácilmente con una VPN el cual permite configurar y gestionar redes privadas virtuales, de tal forma que facilita la conexión de equipos de una red externa con equipos de una red interna por medio del servidor OpenVPN en modo roadwarrior - o modo guerrero – que conecta un cliente remoto a la red.

## 5 REFERENCIAS

- [1] Nethserver (s.f). Manual del Administrador [En línea]. Disponible en: <https://docs.nethserver.org/es/v7/index.html>
- [2] Nethesis (2020). Nethserver Documentation Version 6.10 Final [En línea]. Disponible en: <https://docs.nethserver.org/downloads/es/v6/pdf>
- [3] NethServer, W. t. (s.f.). wiki.nethserver [En línea]. Disponible en: <https://wiki.nethserver.org/doku.php?id=start>
- [4] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial [En línea]. Disponible en: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92>
- [5] Nethserver.org (s.f). Web proxy [En línea]. Disponible en: [https://docs.nethserver.org/en/v7/web\\_proxy.html](https://docs.nethserver.org/en/v7/web_proxy.html).
- [6] Nethserver.org (s.f). VPN [En línea]. Disponible en: <https://docs.nethserver.org/es/v7/vpn.html>.