

IMPLEMENTACIÓN DE NETHSERVER PARA DAR SOLUCIÓN A LAS NECESIDADES ESPECÍFICAS DE LA COMPAÑÍA TECNOLÓGICA

Sneider Alexander Tova Campos
e-mail: satovarc@unadvirtual.edu.co

Heidy Katherine Rojas Acosta
e-mail: hkrojasa@unad.edu.co

Gonzalo Gómez Baquero
e-mail: ggomezba@unad.edu.co

Sebastián Poloche
e-mail: spoloche@unadvirtual.edu.co

RESUMEN: En este artículo se presentará la propuesta para implementar un servidor GNU/Linux, usando la distribución Nethserver 7.9.200. Para tal propósito se presentará el paso a paso de la instalación y configuración del servidor en una máquina virtual, seguido de esto se configurará y demostrará el funcionamiento de los servicios de: DHCP server, DNS server, controlador de dominio, servidor proxy, firewall, FTP server, Impresoras compartidas y VPN.

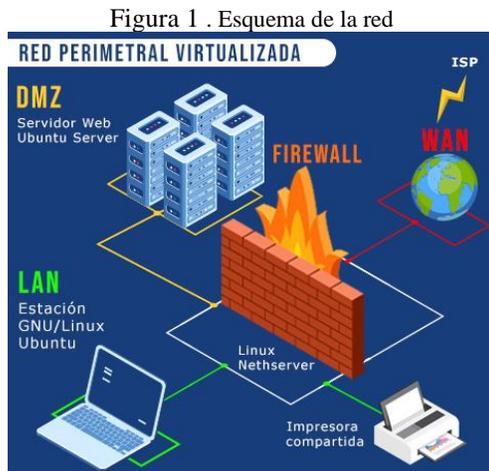
PALABRAS CLAVE: Nethserver, Firewall, Red, Servidores, GNU/Linux.

1. INTRODUCCIÓN

En el presente documento se busca dar solución a la problemática de migración de la infraestructura tecnológica, para lo cual se implementará GNU/Linux, principalmente la distribución de Nethserver y se realizará la configuración de sus diversos servicios para compartir información y recursos dentro de la red de manera segura y eficiente, logrando así ofrecer una infraestructura de alta calidad a la compañía.

2. DISEÑO DE LA RED

2.1 ESQUEMA DE LA RED



Fuente: Autoría Propia

2.2 TABLA DE DIRECCIONES IP

Tabla 1. Direcciones IP

Zona	Adaptador	Dirección IP	Sub red	Puerta de enlace
Verde (LAN)	eth0	192.168.2.20	192.168.2.0/24	192.168.2.15
Naranja (DMZ)	eth1	192.168.1.20	192.168.1.0/24	192.168.1.15
Roja (NAT)	eth2	10.0.4.15	10.0.4.0/24	

Fuente: Autoría Propia

3. INSTALACIÓN DE NETHSERVER

Nethserver es una distribución de GNU/Linux que está enfocada específicamente para funcionar como servidor en pequeñas y medianas empresas.

3.1 REQUISITOS

Los requisitos recomendados para instalar Nethserver son:

- Procesador arquitectura 64 bits
- 1 GB RAM
- 10 GB de espacio en disco
- Interfaz de red
- Unidad óptica o USB.

3.2 ENLACE DE DESCARGA

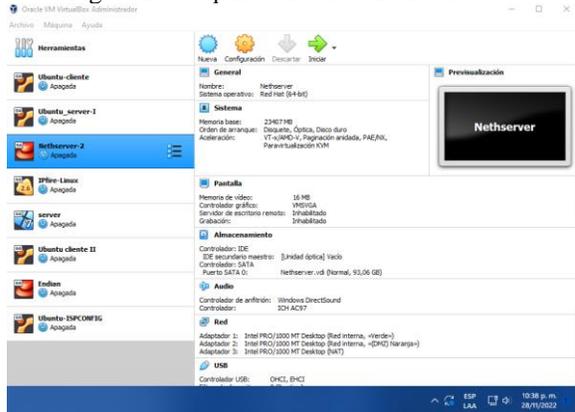
Enlace de descarga de Nethserver:
<https://sourceforge.net/projects/nethserver/>

3.3 PROCESO DE INSTALACIÓN DE NETHSERVER

En VirtualBox configuramos tres máquinas virtuales, la primera se llamará Ubuntu-cliente y estará conectada a la red interna (verde), la segunda se llamará ubuntu_server-I y estará conectado a la red (DMZ -naranja), y la tercera máquina será el firewall de Nethserver y estará conectado a la red WAN (roja), red LAN (verde) y DMZ (naranja).

Cabe aclarar que la maquina ubuntu_server-I es la misma que se utilizó en las actividades anteriores, por lo que podremos acceder a todos sus servicios una vez configuremos la red.

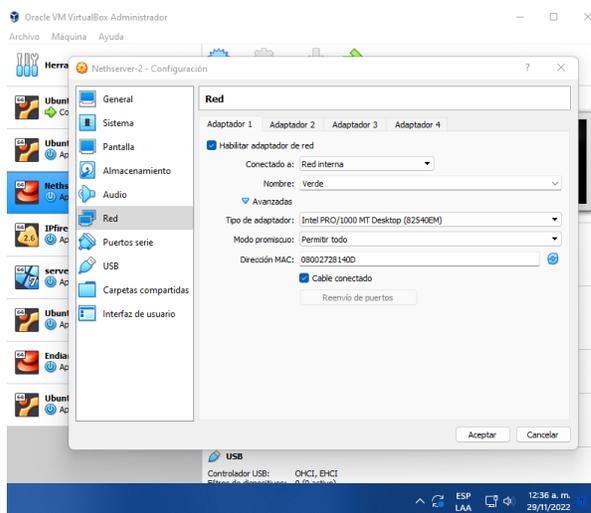
Figura 2 . Máquinas virtuales en virtual box



Fuente: Autoría Propia

En la maquina Nethserver el primer adaptador lo configuramos como red interna y el nombre será verde, la cual será la red LAN. En el segundo adaptador lo configuramos como red interna y el nombre será (DMZ) Naranja, la cual será la red de la zona desmilitarizada (DMZ). Y el tercer adaptador lo configuramos como NAT, debido a que este será la red WAN (roja) la cual proporciona la salida a Internet.

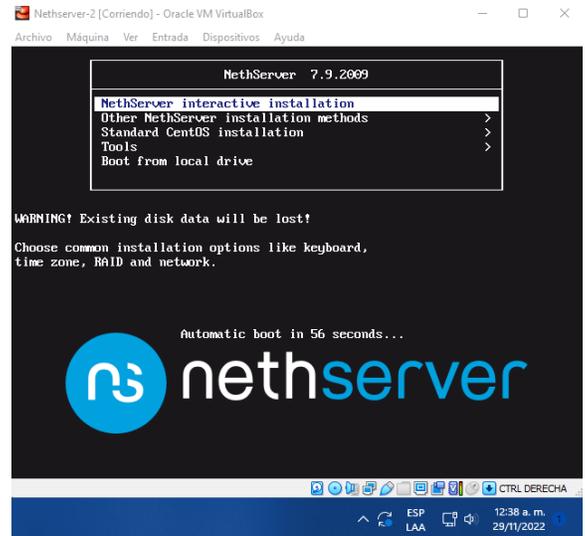
Figura 3 . Configuración de los adaptadores



Fuente: Autoría Propia

Iniciamos con el proceso de instalación de Nethserver dando Enter en “Nethserver interactive instalacion”.

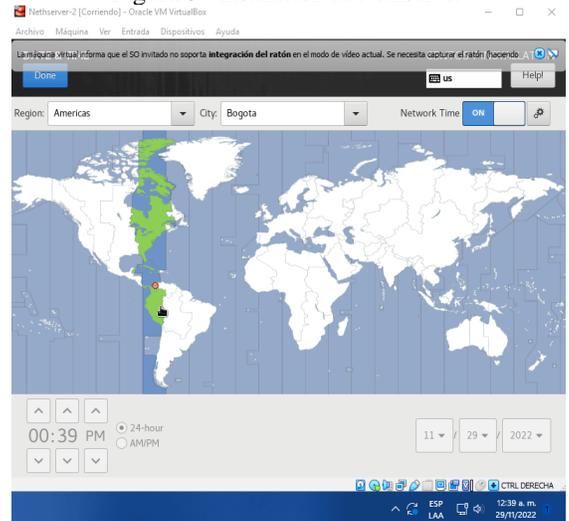
Figura 4 . Instalación de Nethserver



Fuente: Autoría Propia

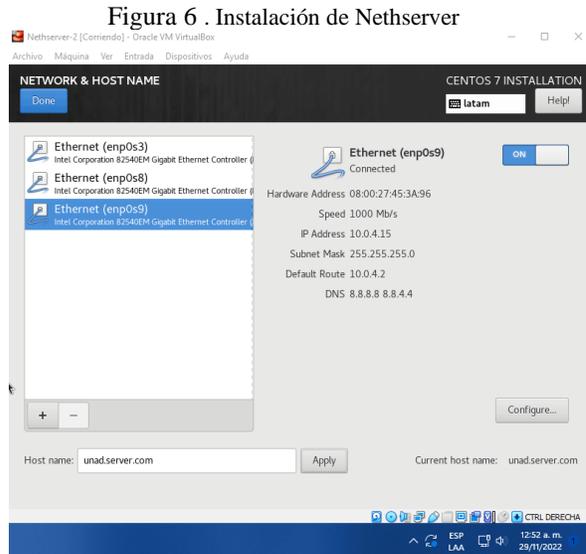
Configuramos el país y la zona horaria, damos clic en “Done” para guardar los cambios.

Figura 5 . Instalación de Nethserver



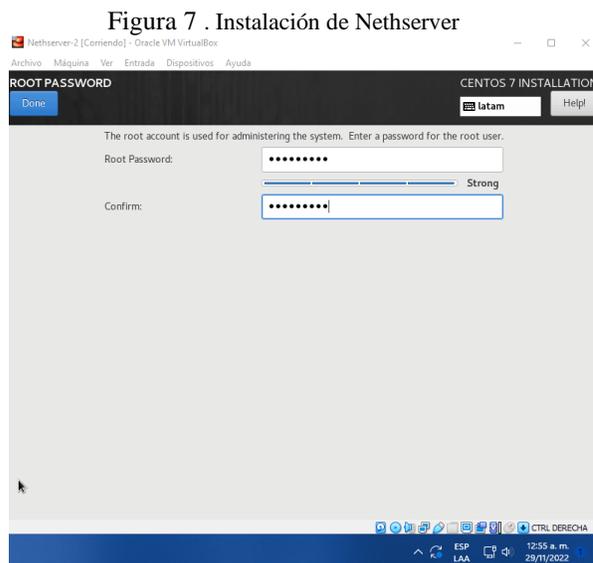
Fuente: Autoría Propia

Después dejamos la asignación de la red WAN (roja) por DHCP, por lo que el proveedor de internet nos asigna la dirección 10.0.4.15 con la máscara de red 255.255.255.0. También establecemos el nombre del host como "unad.server.com" y damos clic en aplicar para guardar los datos.



Fuente: Autoría Propia

Establecemos una contraseña para el usuario root y damos clic en el botón "Done" para continuar con la instalación.



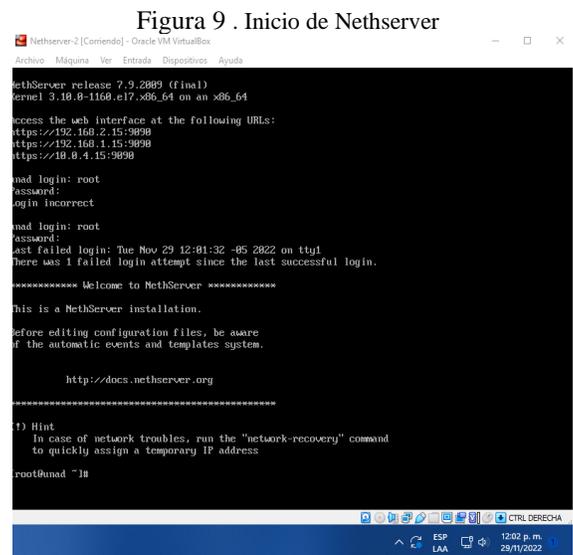
Fuente: Autoría Propia

Esperamos hasta que la instalación de Nethserver se complete y reinicie el equipo.



Fuente: Autoría Propia

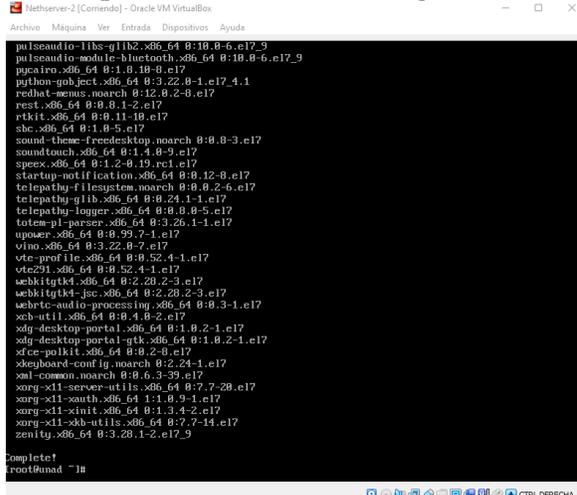
Una vez se inicia el Nethserver, nos registramos con la cuenta del usuario root y su respectiva contraseña.



Fuente: Autoría Propia

Para poder configurar las redes de manera adecuada es necesario hacerlo desde la interfaz web, por lo que instalamos un entorno gráfico en el servidor para poder acceder al navegador. En este caso instalaremos la interfaz gráfica de KDE Plasma por lo cual ejecutamos el comando "yum groups install "KDE Plasma Workspaces"" y reiniciamos la máquina para iniciar desde el entorno gráfico.

Figura 10 . Instalación de entorno grafico

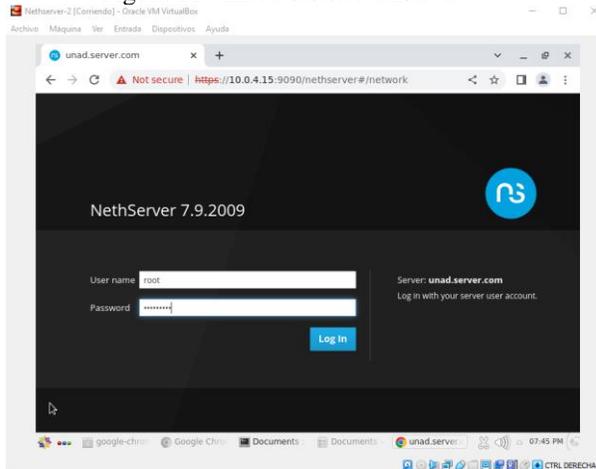


Fuente: Autoría Propia

3.4 CONFIGURACIÓN DE LAS REDES

Desde el servidor accedemos al navegador usando la interfaz gráfica que hemos instalado en el paso anterior, ingresamos la URL 10.0.15:9090 e ingresamos el nombre de usuario root y su contraseña.

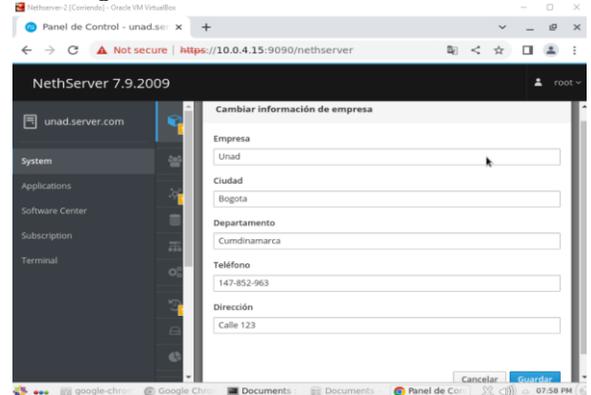
Figura 11 . Iniciar sesión Nethserver



Fuente: Autoría Propia

En las configuraciones del sistema ingresamos el nombre de la empresa (Unad), ciudad (Bogotá), departamento (Cundinamarca), teléfono y dirección.

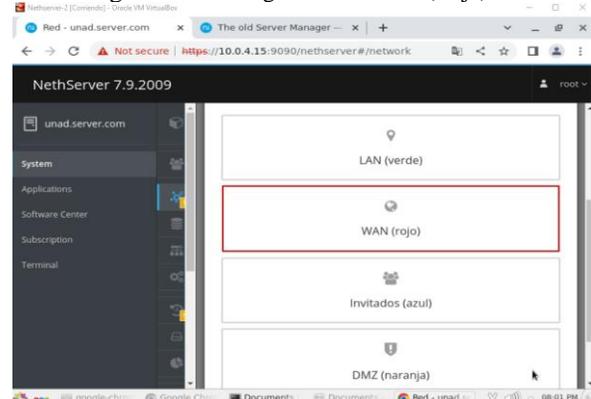
Figura 12 . Información básica del servidor



Fuente: Autoría Propia

Después nos dirigimos a la pestaña Network y seleccionamos el dispositivo enp0s9, establecemos que la red de este dispositivo será WAN (rojo) y damos clic en "Siguiente".

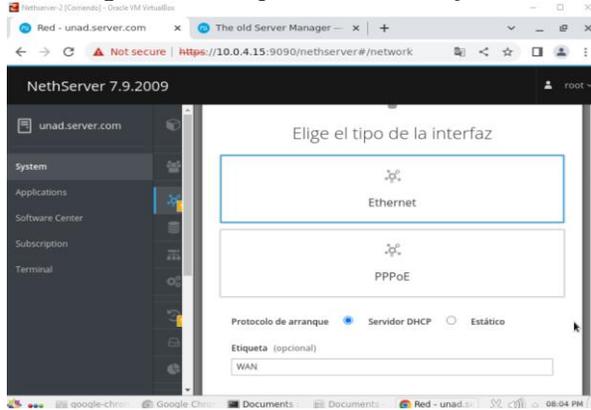
Figura 13 . Configurar Red WAN (Roja)



Fuente: Autoría Propia

Elegimos que la red WAN (roja) será un interfaz de Ethernet y su asignación será por DHCP, por lo que el proveedor de internet nos asigna la dirección 10.0.4.15 con la máscara de red 255.255.255.0. Guardamos los cambios y salimos.

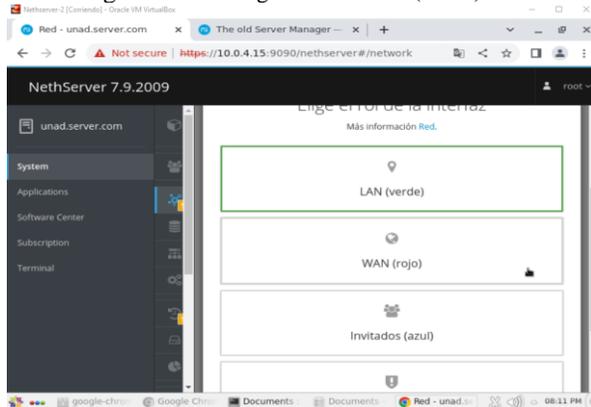
Figura 14 . Configurar Red WAN (Roja)



Fuente: Autoría Propia

Después nos dirigimos a la pestaña Network y seleccionamos el dispositivo enp0s3, establecemos que la red de este dispositivo será LAN (verde) y damos clic en “Siguiente”.

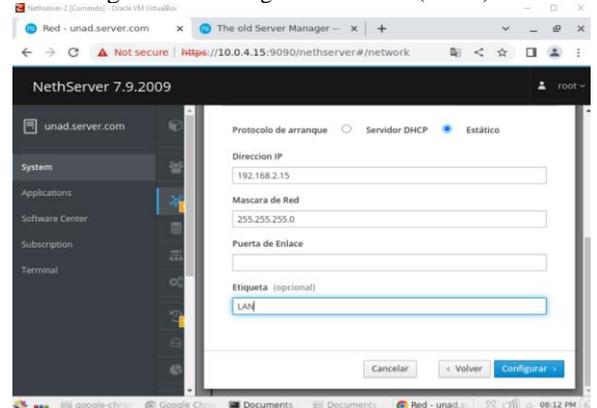
Figura 15 . Configurar Red LAN (verde)



Fuente: Autoría Propia

Establecemos la configuración de la red LAN (verde) como estática, con la dirección IP 192.168.2.15 la máscara de red 255.255.255.0, y damos en “Configurar” para guardar los cambios.

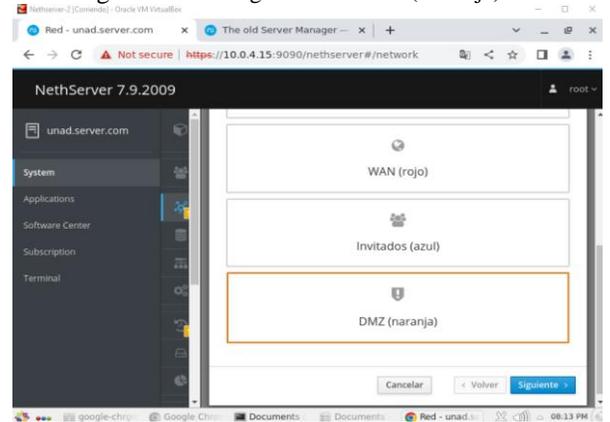
Figura 16 . Configurar Red LAN (Verde)



Fuente: Autoría Propia

Después nos dirigimos a la pestaña Network y seleccionamos el dispositivo enp0s8, establecemos que la red de este dispositivo será DMZ (naranja) y damos clic en “Siguiente”.

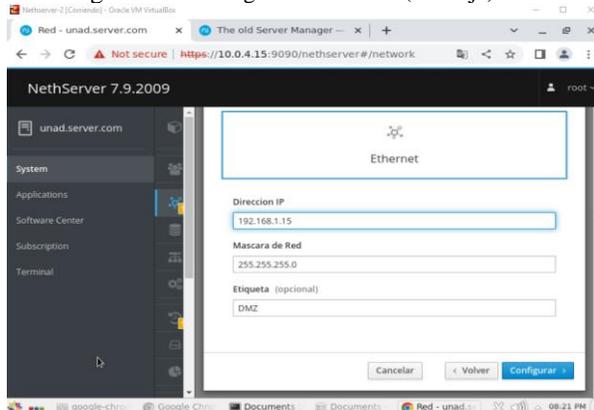
Figura 17 . Configurar Red DMZ (Naranja)



Fuente: Autoría Propia

Establecemos la configuración de la red DMZ (naranja) como estática, con la dirección IP 192.168.1.15 la máscara de red 255.255.255.0, y damos en “Configurar” para guardar los cambios.

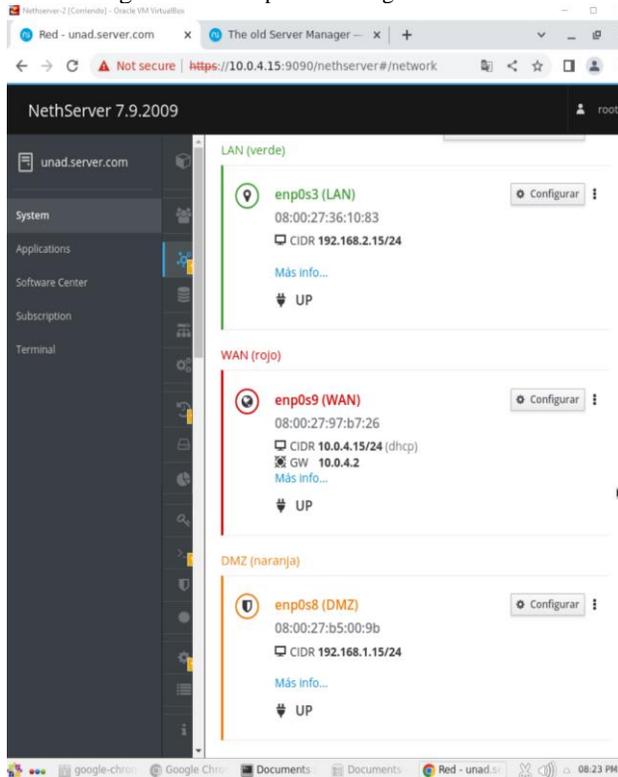
Figura 18 . Configurar Red DMZ (Naranja)



Fuente: Autoría Propia

Desde la interfaz web revisamos que las tres redes se han configurado correctamente donde enp0s3 (LAN - verde) con IP 192.168.2.15/24, enp0s9 (WAN - rojo) con IP 10.0.4.15/24 y enp0s8 (DMZ - naranja) con IP 192.168.1.15/24.

Figura 19 . Comprobar configuración



Fuente: Autoría Propia

4. TEMÁTICAS

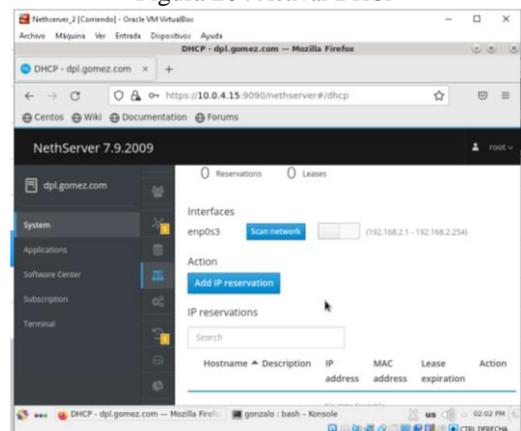
4.1 TEMÁTICA 1: DHCP Y DNS

DHCP Server, DNS Server y Controlador de Dominio. Producto esperado: Implementación y configuración detallada del 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

4.1.1 DHCP SERVER

Para configurar el DHCP vamos a la pestaña de servidor DHCP, activamos el servidor para la interfaz enp0s3 -LAN

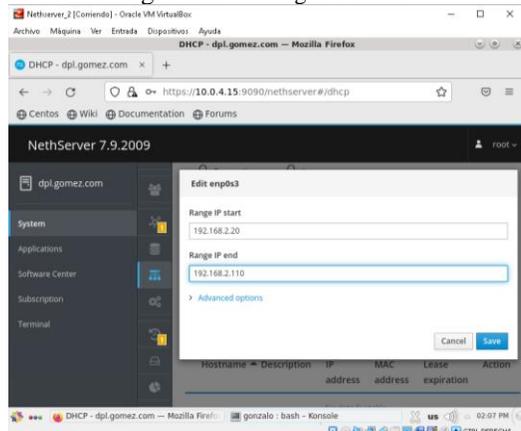
Figura 20 . Activar DHCP



Fuente: Autoría Propia

Configuramos el servidor DHCP tomando como rango de inicio la IP 192.168.2.20 y la final 192.168.2.110. También configuramos la puerta de enlace IP como 192.168.2.15, el dominio del server como “dpl.gomez.com” y los servidores DNS como “1.1.1.1, 8.8.8.8”

Figura 21 . Configurar DHCP



Fuente: Autoría Propia

Resultado obtenido del DHCP

Desde el cliente ejecutamos el comando “ifconfig” y es posible ver que el servidor DHCP nos ha asignado automáticamente la dirección IP 192.168.2.20, por lo que el servidor DHCP funciona correctamente. Ahora ejecutamos el comando “ping 192.168.2.15” para hacer ping con el firewall de Nethserver, como podemos ver se han enviado 4 paquetes sin error, por lo que la conexión entre el cliente y el firewall de Nethserver es correcta.

Figura 22 . Probar DHCP

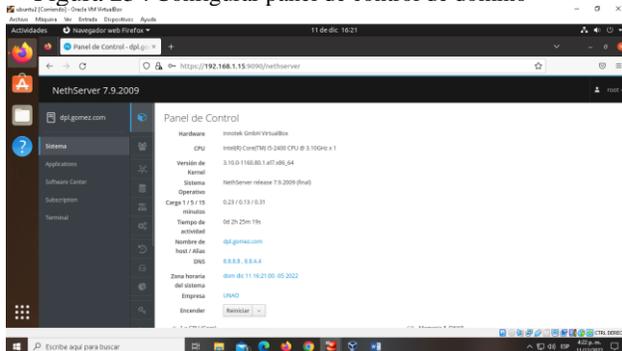
```
gonzalopez@gonzalopez-VirtualBox ~  
gonzalopez@gonzalopez-VirtualBox:~$ ifconfig  
enp0s3: flags=163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.2.21 netmask 255.255.255.0 broadcast 192.168.2.255  
inet6 fe80::79d3:f402:99f2:71db prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:86:ed:a9 txqueuelen 1000 (Ethernet)  
RX packets 5243 bytes 5582797 (5.5 MB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1779 bytes 186680 (180.6 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
Loop txqueuelen 1000 (local loopback)  
RX packets 332 bytes 31940 (31.9 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 332 bytes 31940 (31.9 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
gonzalopez@gonzalopez-VirtualBox:~$ ping 192.168.1.15  
PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data:  
64 bytes from 192.168.1.15: icmp_seq=1 ttl=64 time=0.416 ms  
64 bytes from 192.168.1.15: icmp_seq=2 ttl=64 time=0.505 ms  
64 bytes from 192.168.1.15: icmp_seq=3 ttl=64 time=0.402 ms  
^C  
--- 192.168.1.15 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2051ms  
rtt min/avg/max/mdev = 0.402/0.441/0.505/0.045 ms  
gonzalopez@gonzalopez-VirtualBox:~$
```

Fuente: Autoría Propia

4.1.1 CONTROLADOR DE DOMINIO

Activamos el controlador de dominio y establecemos que el dominio para el Nethserver sera “dpl.gomez.com”.

Figura 23 . Configurar panel de control de dominio



Fuente: Autoría Propia

Resulta obtenido Control DNS

Desde el navegador podremos acceder correctamente al dominio dpl.gomez.com

Figura 24 . Probar dominio DNS

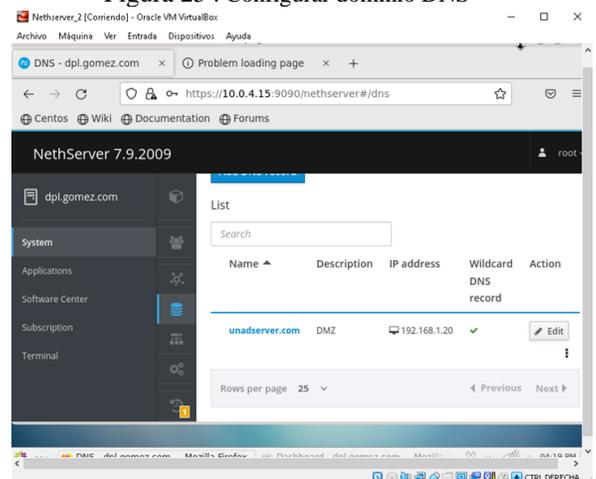


Fuente: Autoría Propia

4.1.2 DNS SERVER

Configuramos el dominio DNS como unadserver.com, el cual se conectará a al servidor DMZ con la IP 192.168.1.20, dándonos acceso a la página web que contiene este.

Figura 25 . Configurar dominio DNS

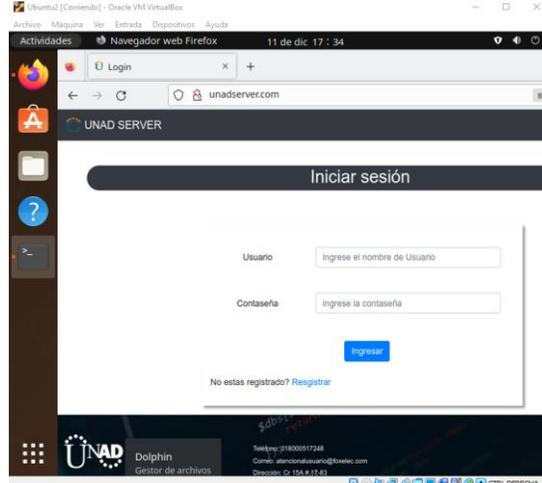


Fuente: Autoría Propia

Resultado obtenido del DNS Server

Desde el cliente, ingresamos la dirección IP unadserver.com en la barra de URL y podemos ver que el cliente puede acceder correctamente a la página php que está en el servidor de Ubuntu, lo que significa que el cliente puede acceder a todos los servicios que ofrece este y que fueron configurados en actividades anteriores.

Figura 26 . Probar domino DNS



Fuente: Autoría Propia

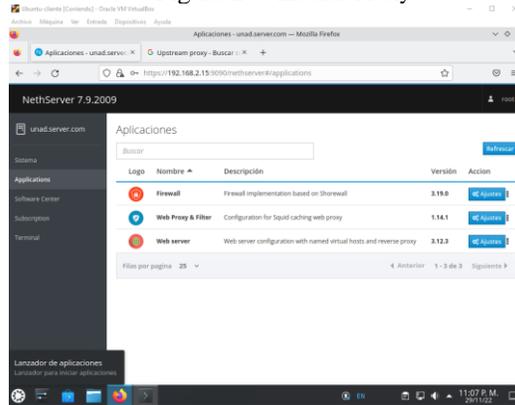
4.2 TEMÁTICA 2: PROXY

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.

4.2.1 CONFIGURACIÓN DEL SERVIDOR PROXY

Desde la opción de “Software center” instalamos la aplicación de “Web Proxy & Filter” y “Firewall”. Después vamos a la pestaña de “Applications” y damos clic en Ajustes para la aplicación de Web Proxy & Filter.

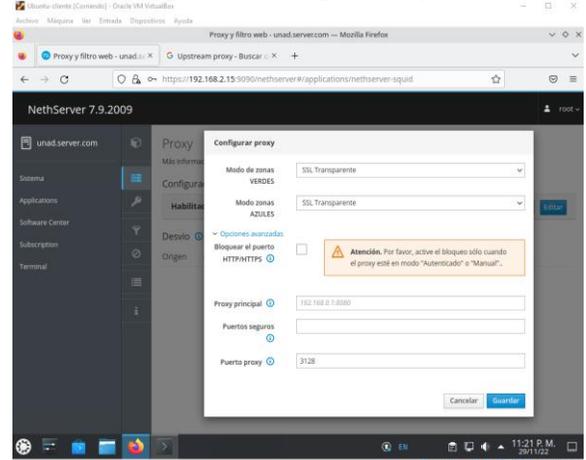
Figura 27 . Instalar Proxy



Fuente: Autoría Propia

Después damos clic en la pestaña de “Proxy” y después en “Editar” configuración del proxy. Establecemos que la red LAN (Verde) tendrán un modo proxy SSL Transparente y el puerto proxy será el 3128.

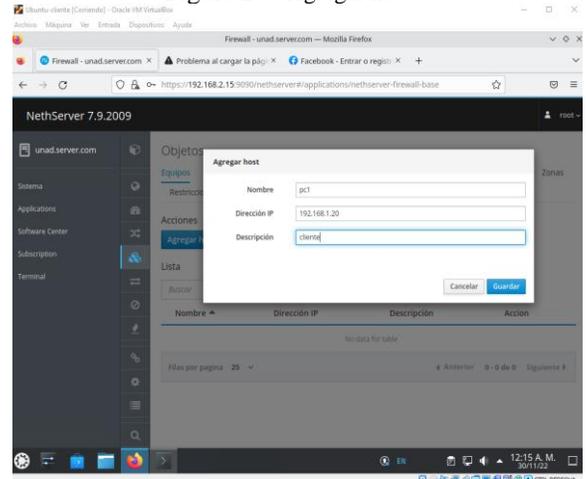
Figura 28 . Configurar Proxy



Fuente: Autoría Propia

Desde la aplicación de firewall ingresamos a la pestaña Objetos y damos clic en “Agregar host”. Creamos un nuevo objeto de tipo host llamado pc1, que será nuestro equipo cliente con la dirección IP 192.168.1.20. Damos clic en “Guardar” para guardar los cambios.

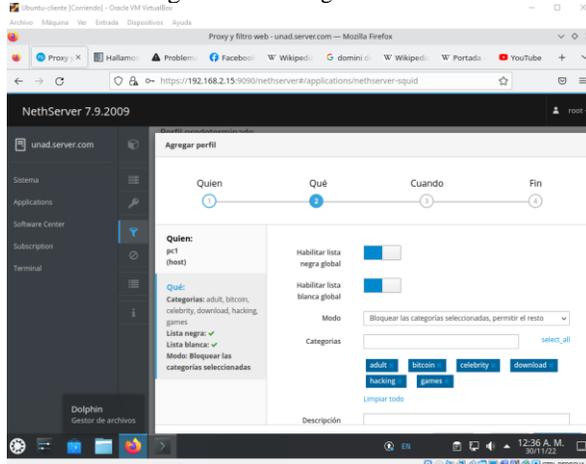
Figura 29 . Agregar host



Fuente: Autoría Propia

Después vamos a la aplicación de “Web Proxy & Filter” e ingresamos a la opción de filtro, damos clic en “crear perfil”, creamos un nuevo filtro para el objeto pc1 (cliente). activamos listas negras, lista negra modo bloquear categorías, permitir el resto y seleccionamos las categorías que queremos bloquear.

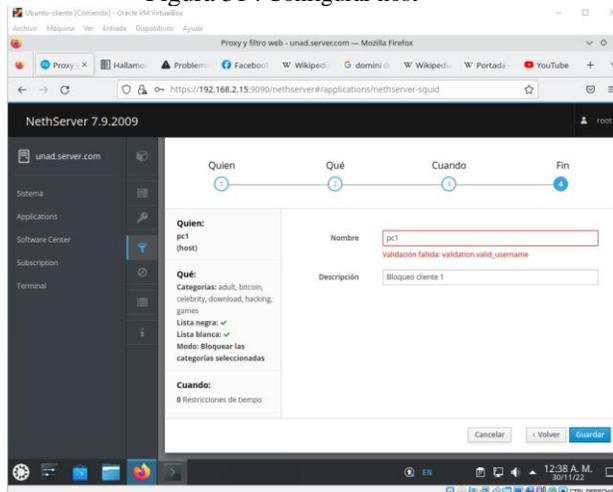
Figura 30 . Configurar host



Fuente: Autoría Propia

Después establecemos el nombre de la regla y su respectiva descripción, finalmente damos clic en “Guardar” para guardar los cambios y salir.

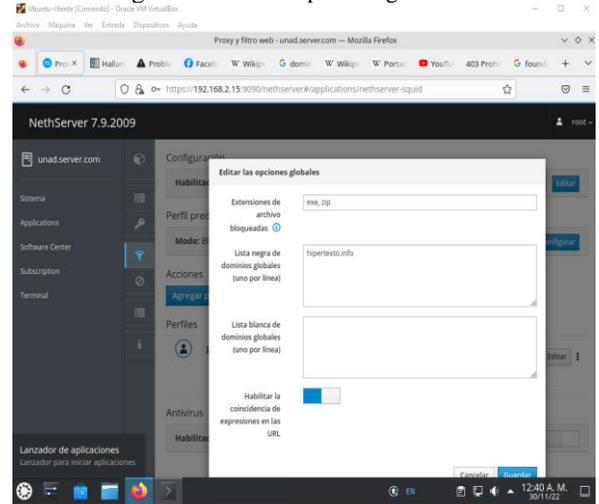
Figura 31 . Configurar host



Fuente: Autoría Propia

Después damos clic en “Editar” lista blanca y negra, agregamos el tipo de extensiones que deseamos bloquear (exe, zip). Al igual que la lista negra bloquearemos la página “hipertexto.info” y habilitamos la coincidencia de expresiones en las URL. Finalmente damos clic en “Guardar” para guardar los cambios y salir.

Figura 32 . Editar opciones globales

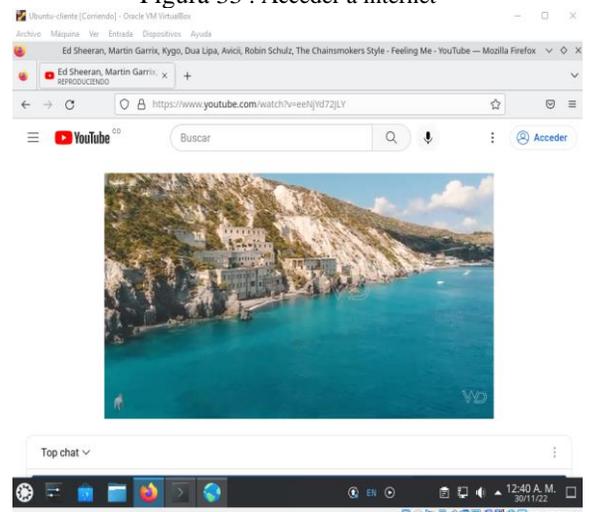


Fuente: Autoría Propia

Resultado obtenido del servidor Proxy

Desde el cliente accedemos a internet y podemos comprobar que el firewall de Nethserver permite una correcta conexión a internet.

Figura 33 . Acceder a internet



Fuente: Autoría Propia

Desde el cliente intentamos acceder a la página que hemos agregado a la lista negra en el servidor Nethserver (hipertexto.info), al acceder a la página podemos ver que el acceso a dicho sitio está bloqueado por el proxy. Lo que significa que la configuración del servidor proxy correcta y está filtrando el flujo de la red de acuerdo a las indicaciones dadas.

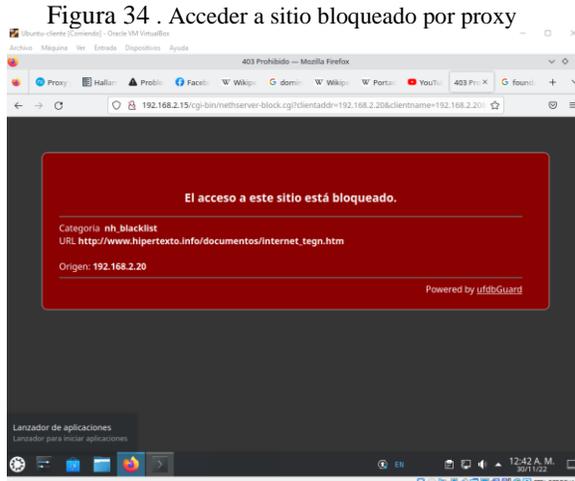


Figura 34. Acceder a sitio bloqueado por proxy

Fuente: Autoría Propia

4.3 TEMÁTICA 3: CORTAFUEGOS PRODUCTO ESPERADO

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.

4.3.1 CONFIGURACIÓN DEL FIREWALL

Vamos a la pestaña de “Applications” y damos clic en Ajustes para la aplicación de Firewall.

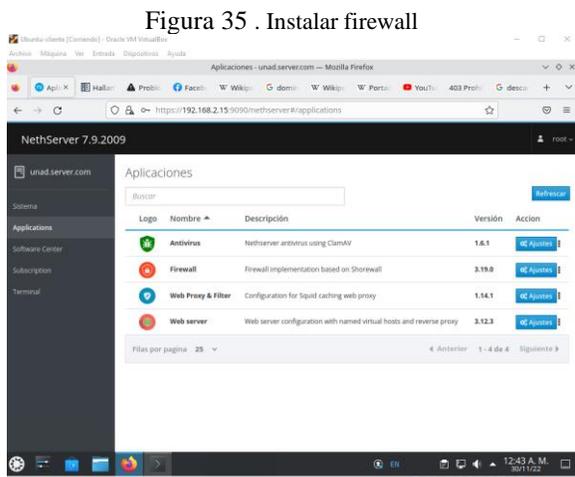


Figura 35. Instalar firewall

Fuente: Autoría Propia

4.3.2 CREACIÓN DE RANGOS IP EN FIREWALL

Para bloquear correctamente una red social es necesario bloquear el rango de direcciones IP que utilizan sus servidores, de esta manera es posible evitar que las direcciones IP dinámicas y los múltiples servidores permitan el acceso a los sitios web.

Para llevar a cabo este proceso vamos a la pestaña de “Objetos” y seleccionamos la opción de “Rangos de direccionado IP”, para luego dar clic en “Agregar rango de IP”, ingresamos el nombre del sitio que deseamos bloquear, la IP inicial, la IP final y una breve descripción, este proceso lo realizamos para las tres plataformas de redes sociales que deseamos bloquear, que en este caso son Facebook, Twitter y YouTube.

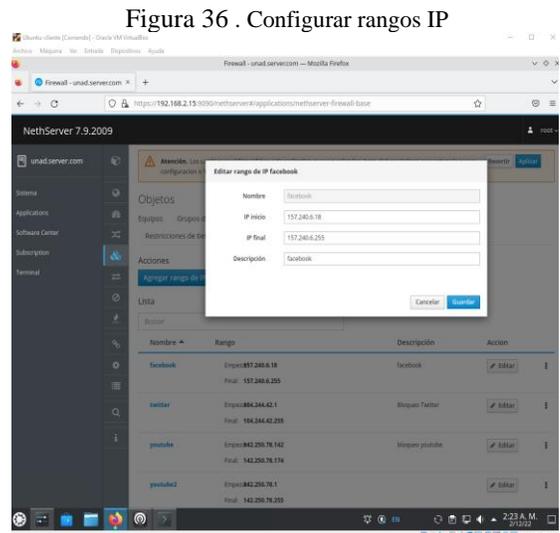


Figura 36. Configurar rangos IP

Fuente: Autoría Propia

En la pestaña de “Rangos de direccionado IP” deben quedar establecidos los tres rangos de bloqueo para Facebook, Twitter y YouTube.

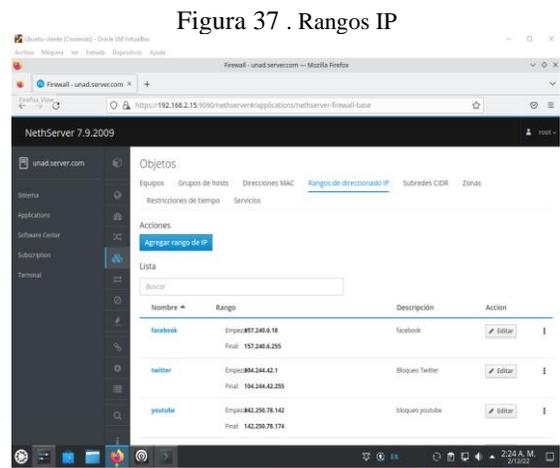


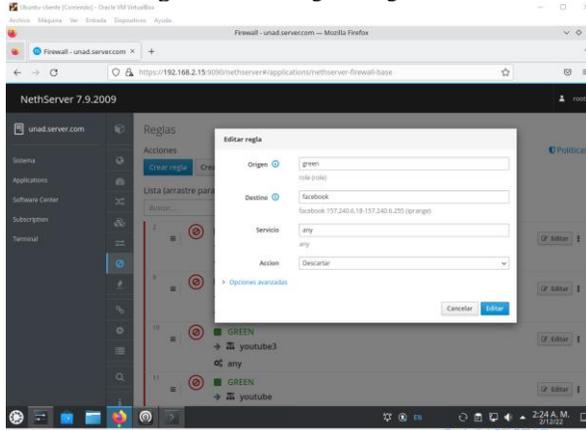
Figura 37. Rangos IP

Fuente: Autoría Propia

4.3.3 CREACIÓN DE REGLAS FIREWALL

Después vamos a la pestaña de “Reglas” y damos clic en “Crear regla”, establecemos que el origen será la red verde, el destino el rango de Facebook, que no se permitirá ningún servicio y la acción será de descarte. La anterior configuración se repetirá para los tres sitios de redes sociales: Facebook, YouTube y Twitter.

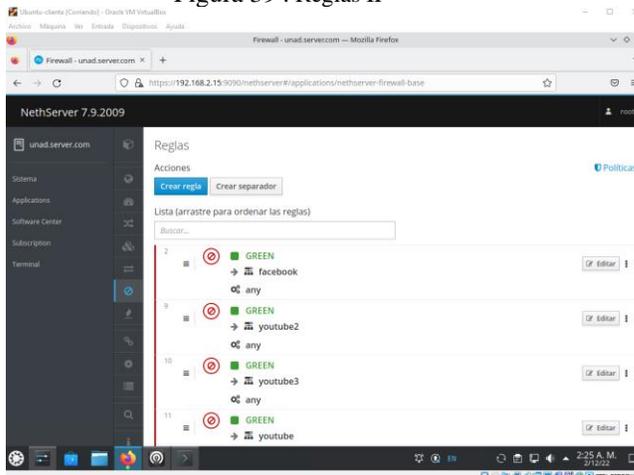
Figura 38 . Configurar reglas



Fuente: Autoría Propia

En la pestaña de “Reglas” deben quedar establecidos las tres reglas de bloqueo del acceso de la red Verde a Facebook, YouTube y Twitter.

Figura 39 . Reglas IP

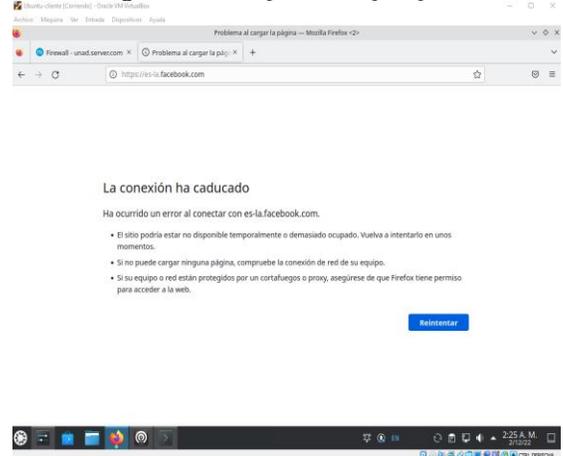


Fuente: Autoría Propia

Resultado obtenido del firewall

Desde el cliente ingresamos a las páginas de Facebook, YouTube y Twitter. Como podemos ver que las páginas se encuentran bloqueadas, por lo que la regla del firewall funciona correctamente.

Figura 40 . Comprobar bloqueo por IP



Fuente: Autoría Propia

Para comprobar que el bloqueo es solo a las páginas especificadas y no a todo el tráfico de la red, accedemos a otra página y cómo podemos ver el cliente accede con normalidad a la página de Wikipedia, por lo que el firewall solo filtra el contenido especificado en las reglas.

Figura 41 . Comprobar acceso a internet



Fuente: Autoría Propia

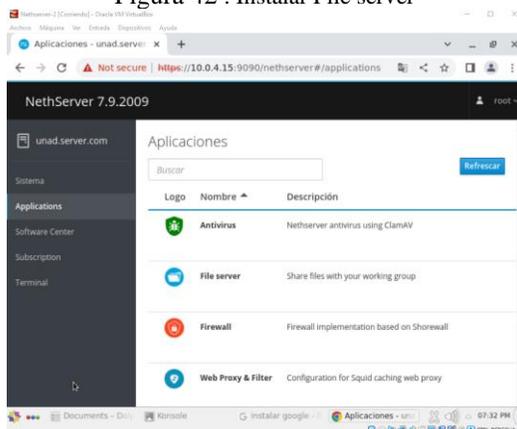
4.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

4.4.1 FILE SERVER

Desde el servidor de Nethserver instalamos la aplicación de File server.

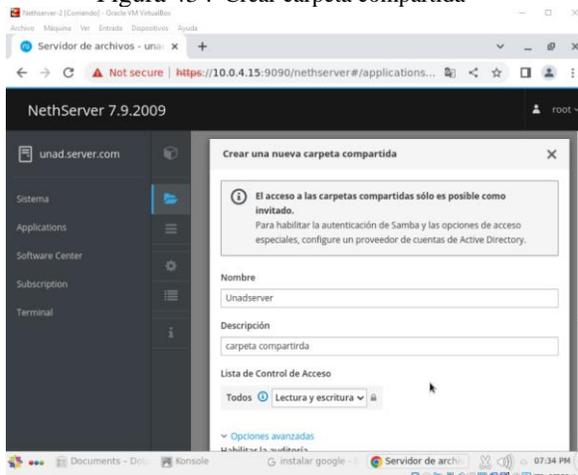
Figura 42 . Instalar File server



Fuente: Autoría Propia

Abrimos la aplicación File server que acabamos de instalar y creamos una carpeta compartida que se llamará “Unadserver” y le damos permisos de escritura y lectura para todos los usuarios.

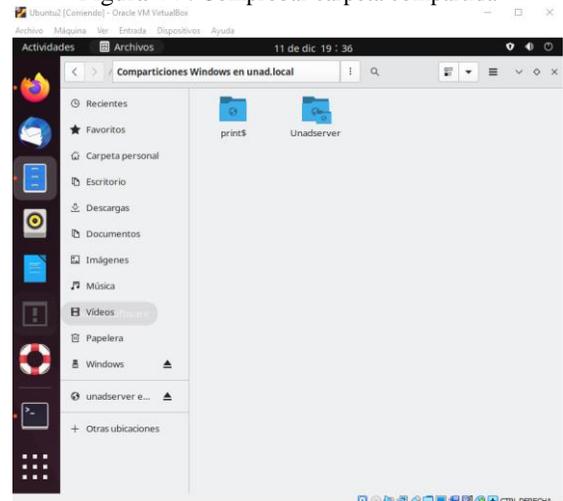
Figura 43 . Crear carpeta compartida



Fuente: Autoría Propia

Desde el cliente accedemos al administrador de archivos, nos dirigimos a “+ Otras ubicaciones” y encontraremos la carpeta Unadserver en la red local.

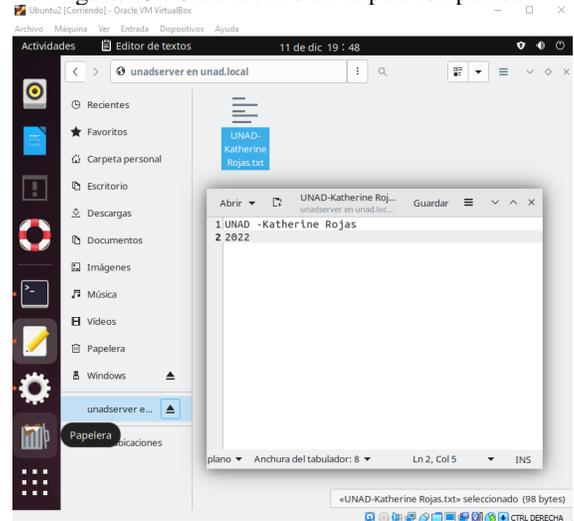
Figura 44 . Comprobar carpeta compartida



Fuente: Autoría Propia

Desde el cliente creamos un archivo llamado “UNAD - Katherine Rojas” en la carpeta compartida.

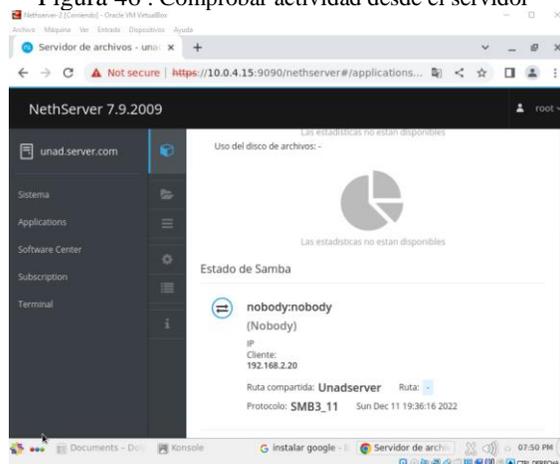
Figura 45 . Crear archivo en carpeta compartida



Fuente: Autoría Propia

Desde el servidor Nethserver verificamos que el cliente ha accedido a la carpeta compartida.

Figura 46 . Comprobar actividad desde el servidor

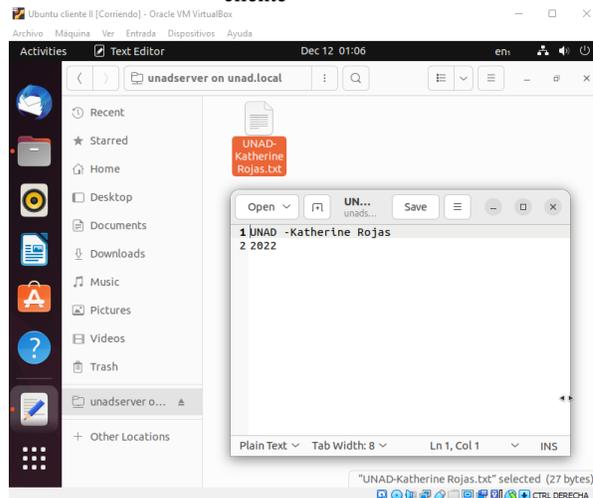


Fuente: Autoría Propia

Resultado obtenido del File server

Desde otro equipo cliente conectado a la red verde, accedemos a la carpeta compartida y podemos ver que el documento se ha almacenado correctamente en el servidor de archivos y está disponible para todos los usuarios de la red LAN.

Figura 47 . Comprobar archivo compartido desde otro cliente

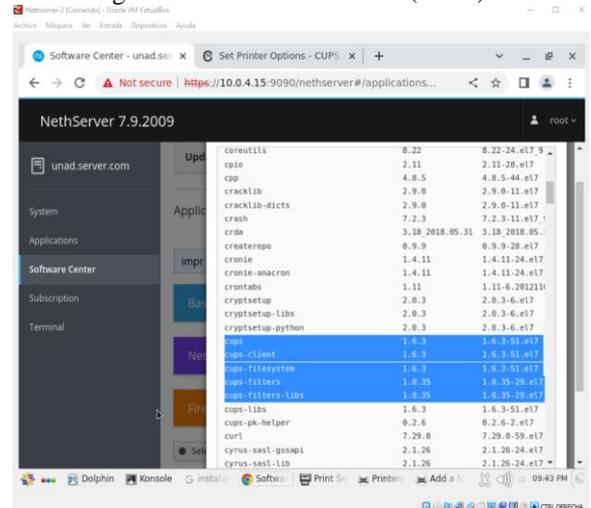


Fuente: Autoría Propia

4.4.2 PRINT SERVER

Desde el Nethserver instalamos los complementos para el servidor de impresoras (CUPS).

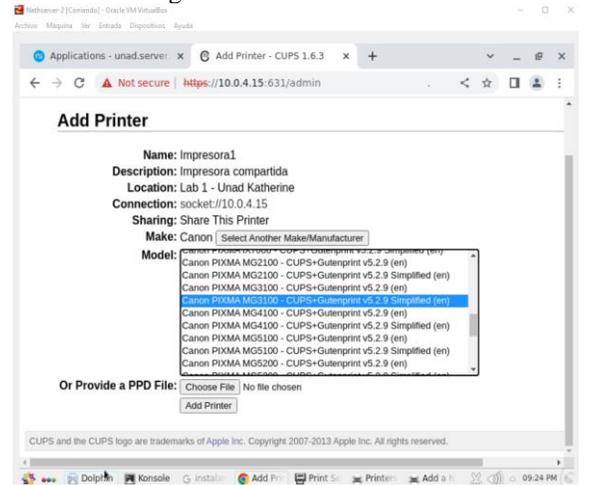
Figura 48 . Instalar Print Server (CUPS)



Fuente: Autoría Propia

Desde el servidor de Nethserver ingresamos al localhost usando el puerto: 631 y configuramos la impresora la cual es una Canon Pixman MG 3100 y esta usara la dirección del servidor 10.0.4.15.

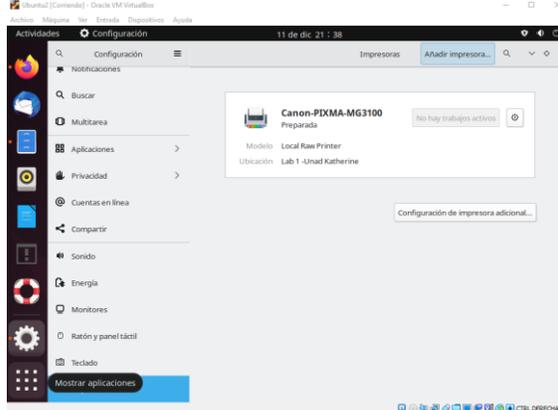
Figura 49 . Acceder a CUPS



Fuente: Autoría Propia

Desde el cliente accedemos a la configuración de impresoras y configuramos la impresora, la cual podemos ver que se carga automáticamente su nombre y ubicación “Lab 1 - Unad Kaherine”.

Figura 50 . Acceder a la impresora desde el cliente

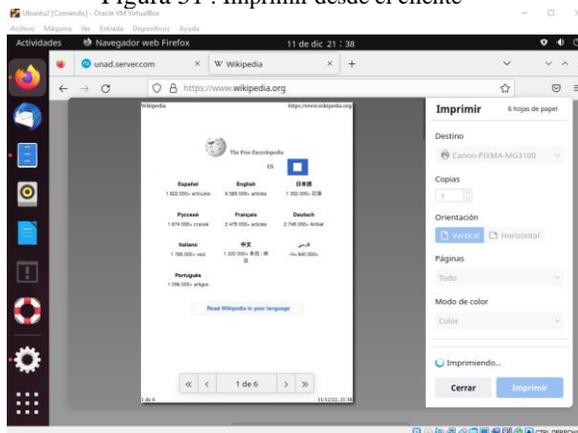


Fuente: Autoría Propia

Resultado obtenido del Print Server

Desde el cliente realizamos una impresión una impresión utilizando la impresora compartida y como se puede evidenciar esta se procesa correctamente.

Figura 51 . Imprimir desde el cliente



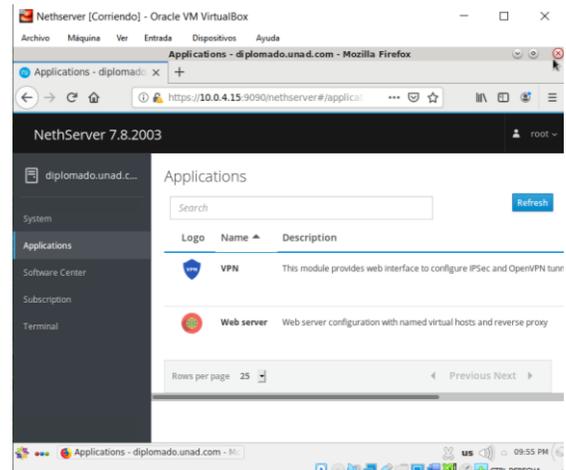
Fuente: Autoría Propia

4.5 TEMÁTICA 5: VPN

Implementación y configuración detallada de la creación de una VPN.

Para configurar la vpn ingresamos a software center e instalamos el paquete de OpenVpn. Procedemos a verificar que se allá instalado en el apartado de aplicaciones.

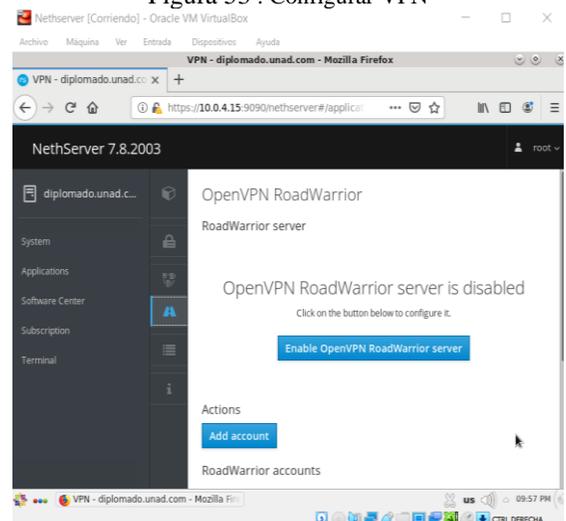
Figura 52 . Instalar el VPN



Fuente: Autoría Propia

Ahora realizamos unas configuraciones para nuestra vpn en roadWarrior.

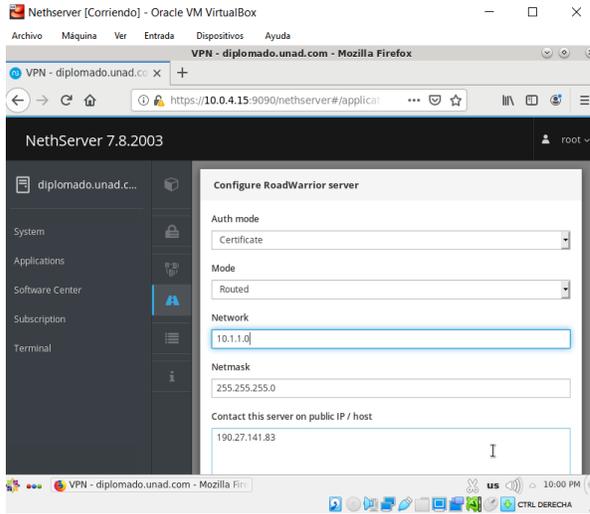
Figura 53 . Configurar VPN



Fuente: Autoría Propia

Procedemos a configurar la vpn con el fin de poder más adelante trabajar con ella.

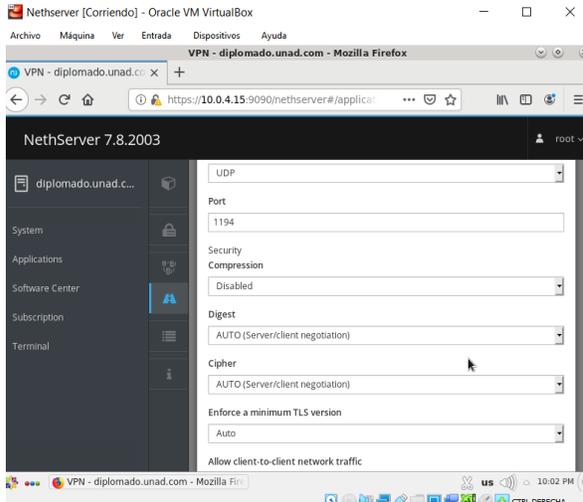
Figura 54 . Configurar VPN



Fuente: Autoría Propia

Seleccionamos opciones avanzadas y terminamos de configurar. Y Se guardan los cambios de la configuración realizada.

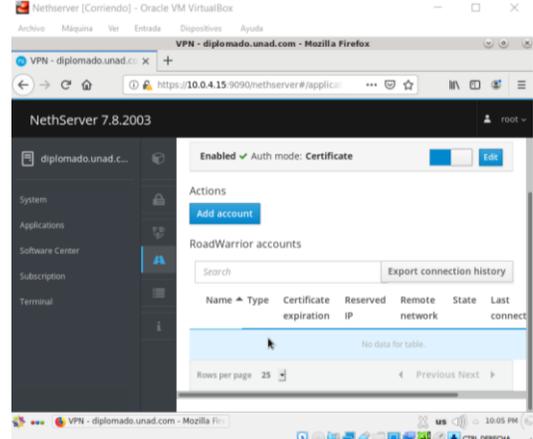
Figura 55 . Configurar opciones avanzadas



Fuente: Autoría Propia

En la opción add account o agregar cuenta presionamos.

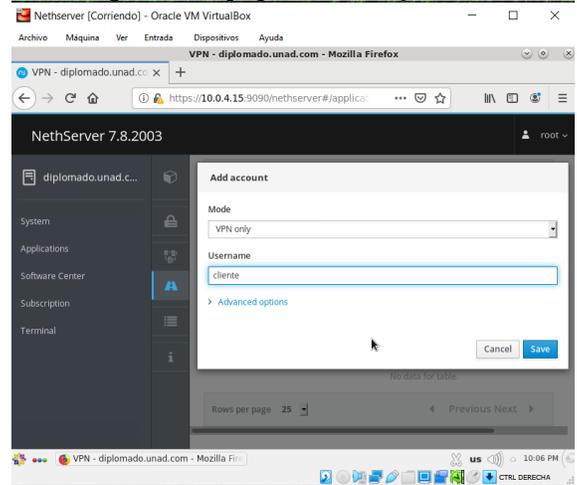
Figura 56 . Agregar cuenta con permisos



Fuente: Autoría Propia

Ahora creamos las cuentas o usuarios de que van a conectarse a nuestra vpn.

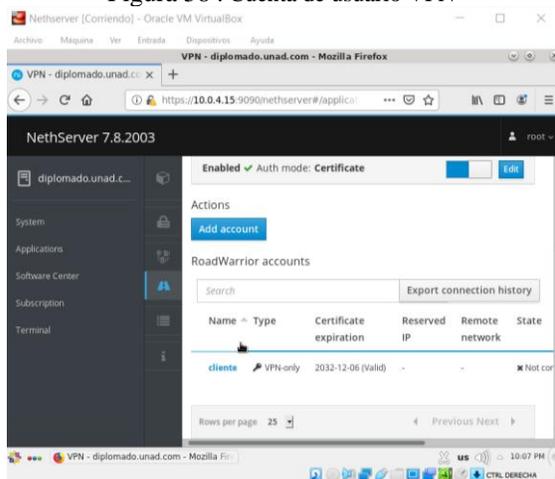
Figura 57 . Agregar cuenta con permisos



Fuente: Autoría Propia

Ahora podemos observar que nuestra cuenta o usuario ya se encuentra creada y registrada en la VPN.

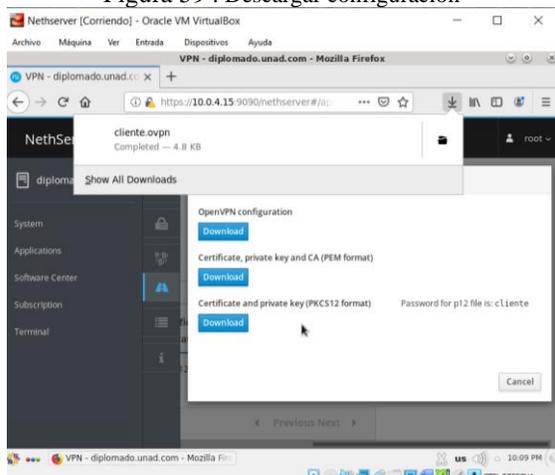
Figura 58 . Cuenta de usuario VPN



Fuente: Autoría Propia

Presionamos en los tres puntos sobre la cuenta que acabamos de crear y descargamos la configuración de la vpn para nuestro cliente.

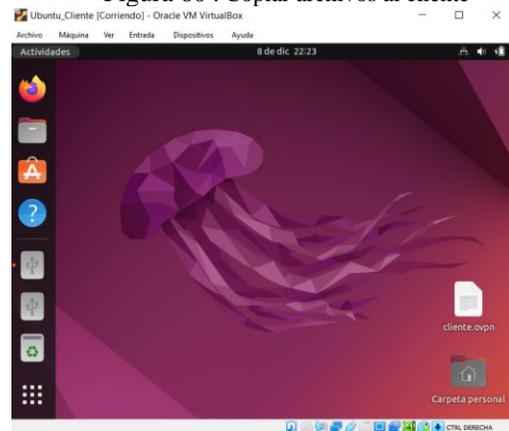
Figura 59 . Descargar configuración



Fuente: Autoría Propia

Ingresamos al cliente y copiamos el archivo creado en nethserver de la vpn.

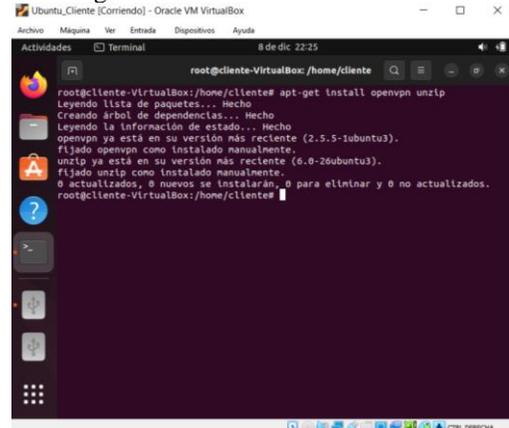
Figura 60 . Copiar archivos al cliente



Fuente: Autoría Propia

Ahora realizamos la instalación del cliente de open vpn mediante terminal.

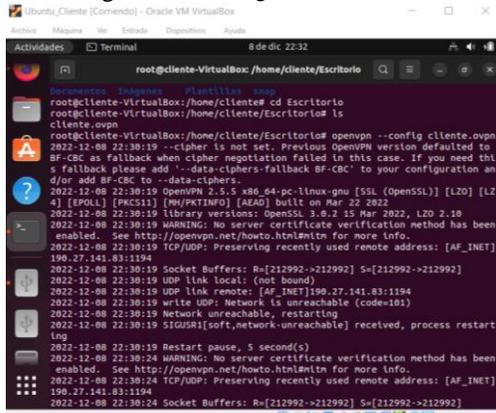
Figura 61 . Instalación de VPN en el cliente



Fuente: Autoría Propia

Configuramos el cliente de OpenVPN con el archivo mencionado anteriormente.

Figura 62 . Configurar VPN en el cliente

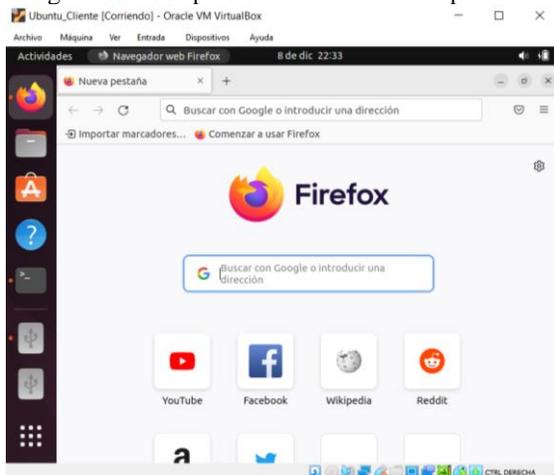


Fuente: Autoría Propia

Resultado obtenido del VPN

Ahora validamos que se conectó correctamente a internet mediante nuestra vpn.

Figura 63 . Comprobar conexión a internet por VPN



Fuente: Autoría Propia

5. CONCLUSIONES

- El desarrollo de la actividad permitió identificar los tipos de servidores que existen dentro del sistema Linux, los protocolos que permiten la transferencia de archivos e información entre los equipos de la red (cliente/servidor), los gestores para el control de cortafuegos y las distribuciones GNU/Linux que funcionan como plataformas operativas tipo cortafuegos. También permitió comprender las características y funcionamiento de las herramientas de administración que permiten

montar y configurar toda la infraestructura de la red, como es el caso de Nethserver.

- Configurar una red de tipo DMZ es muy importante porque permite delimitar el acceso a los servidores, por lo que un atacante externo no podría robar fácilmente la información. Esto debido a que la red se encuentra segmentada en tres zonas: la zona verde (red LAN), roja (red WAN) y naranja (Servidor DMZ).
- Las distribuciones tipo firewall de GNU/Linux cuentan con una estructura de seguridad sólida, debido a que cuentan con estrictas reglas de seguridad, en las cuales se establecen políticas de contenido, direccionamiento de paquetes, bloqueo de IP y listas negras.
- El servidor DHCP es una herramienta muy útil, debido a que permite asignar de manera automática la dirección IP a cada uno de los dispositivos de la red, lo cual es de gran utilidad cuando se trabaja con una red de muchos ordenadores y resulta tedioso asignar manualmente la dirección IP a cada uno.
- El servidor proxy es de gran utilidad debido a que permite filtrar el contenido de la red WAN al que acceden los equipos de la red interna de esta manera evita que se realicen búsquedas inadecuadas o se descarguen archivos maliciosos.
- El firewall aporta una gran capa de seguridad a la red debido a que permite establecer políticas y reglas para el bloqueo de páginas web o bloqueo de direcciones IP.
- Los servidores de FTP e impresoras permiten compartir de manera eficiente y segura archivos, recursos e impresoras entre los diferentes equipos de la red.
- El servicio de VPN es muy importante debido a que le permite al equipo navegar de manera segura por la red, sin que su dirección IP se vea comprometida o sea visible para un atacante externo.

6. REFERENCIAS

- Cabrera, M. (2021). *Nethserver Tutorial | Formas de actualizar el servidor*. [Video]. YouTube. <https://www.youtube.com/watch?v=AbTLCisTE3Q>
- Cabrera, M. (2018). *Nethserver Tutorial | Instalación, actualización y primeros pasos*. [Video]. YouTube. https://www.youtube.com/watch?v=FNGmM-2fa_0
- Cabrera, M. (2018). *Nethserver Tutorial | Manejando backups de tu server linux*. [Video]. YouTube. <https://www.youtube.com/watch?v=g4QnKqRZhXE>
- Nethserver. (2022). *Nethserver-cups*. <https://docs.nethserver.org/projects/nethserver-devel/en/latest/nethserver-cups.html>
- Nethserver. (2022). *Servidor DHCP y PXE*. <https://docs.nethserver.org/es/v7/dhcp.html>
- Nethserver. (2022). *DNS*. <https://docs.nethserver.org/es/v7/dns.html>
- Nethserver. (2022). *Proxy*. https://docs.nethserver.org/es/v7/web_proxy.html
- Nethserver. (2022). *VPN*. <https://docs.nethserver.org/es/v7/vpn.html>