SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX "APLICANDO FUNCIONALIDADES DE NETHSERVER"

Alex Daniel Gazcón Rojas
e-mail: adgazconr@unadvirtual.edu.co
Byron Esneyder Fandiño Morales
e-mail: befandinom@unadvirtual.edu.co
Diego Alonso Ojeda Medina
e-mail: daojedam@unadvirtual.edu.co
Edwin Ferney Velasco Baez
e-mail: efvelascoba@unadvirtual.edu.co
Maida Nataly Montenegro Cabezas
e-mail: mnmontenegroc@unadvirtual.edu.co

RESUMEN: *El presente articulo tiene como fin demostrar la implementación del servidor Nethserver el cual permite configurar hasta 4 zonas de red, sin embargo, para el desarrollo de las temáticas se tendrán en cuenta hasta 3 zonas identificadas como roja, verde y naranja; teniendo en cuenta la configuración del segmento de red de cada una de ellas, se procederá a demostrar el funcionamiento de algunos de los servicios que se pueden administrar en Nethserver.*

PALABRAS CLAVE: Controlador de dominio, Firewall, File Server, Nethserver, Print Server, Proxy, VPN.

1 INTRODUCCIÓN

Solucionada gran parte de las problemáticas de migración de sus sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, se entra en la fase final de la migración y puesta en marcha de los servicios solicitados. Sistema operativo bajo el cual se implementa los servicios y plataformas: GNU/Linux Nethserver (Instalar y configurar como sistema operativo base para disponer de los servicios de Infraestructura IT).

Es importante que para el desarrollo de cada temática cada estudiante debe aplicar cada uno de lo aprendido en los pasos anteriores, ejemplo se debe definir la zona DMZ de acuerdo con la Red administrable que se debería crear para acceder desde el GNU/Linux al Nethserver.

2 OBJETIVOS

Configurar Interfaces de usuario y escritorio a través de tareas administrativas con los servicios esenciales dándole un óptimo nivel de seguridad al sistema operativo GNU Linux.

2.1 OBJETIVOS ESPECIFICOS

Los márgenes externos deben de respetar los siguientes criterios:

- Instalar en una máquina virtualizada el sistema operativo NethServer, con el fin de configurar las zonas de red para adquirir los conocimientos básicos en seguridad de redes mediante la solución de cada una de las temáticas
- Configurar un servidor DHCP, DNS y un Controlador de Dominio, permitiendo la vinculación de un equipo Desktop al Active Directory, y validando el funcionamiento mediante el acceso del usuario de dominio creado con su respectiva contraseña.
- Implementar el 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.
- Configurar la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas, mediante restricciones de un cortafuego.
- Implementar de un controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.
- Configurar una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo.

3 MARCO TEORICO

Nethserver es una distribución de Linux basada en CentOS/RHEL diseñada para servidores. Ofrece una amplia gama de funciones y servicios, entre los cuales encontramos:[1].

- Servidor DHCP, DNS y Active Directory
- Proxy web
- Firewall
- Servidor de correo electrónico
- Servidor de impresión
- Servidor de archivos compartidos
- VPN

Nethserver es una buena opción para pequeñas y medianas empresas que buscan una solución de servidor completa y asequible. Es fácil de instalar y configurar, y ofrece una gran flexibilidad para satisfacer las necesidades específicas de su negocio.

4 CONFIGURACIÓN E INSTALACION DEL GNU/LINUX NETHSERVER

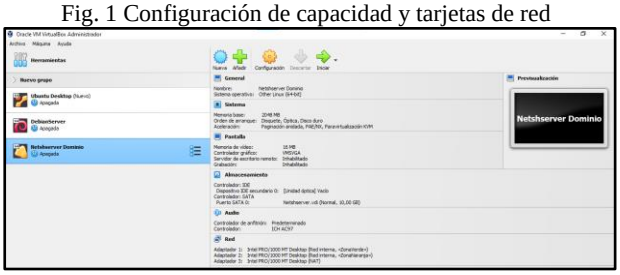
4.1 DESCARGA DE LA IMAGEN ISO

La versión estable encontrada en la página para el desarrollo de las actividades es la versión 7.9.2009, la cual se descarga del siguiente enlace: https://github.com/NethServer/dev/releases/download/iso-7.9.2009/nethserver-7.9.2009-x86_64.iso

4.2 PARÁMETROS DE CONFIGURACIÓN

Para la instalación del sistema operativo NethServer, se utiliza el software de virtualización Virtualbox v.7.0. configurando los parámetros de capacidad de disco duro de 50GB, memoria RAM 2GB y un núcleo del procesador. Adicionalmente se configuran 3 adaptadores de red, donde las 2 primeras se asignan como red interna de las zonas verde y naranja respectivamente; y el último adaptador se encuentra configurado como NAT para representar la zona roja.

Fig. 1 Configuración de capacidad y tarjetas de red

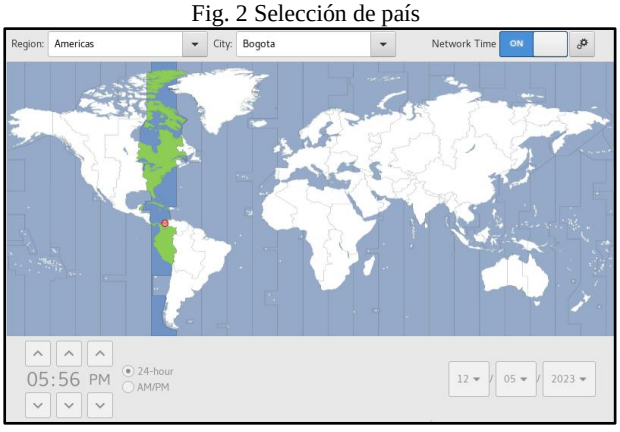


Fuente: Autoría Propia

4.3 INSTALACIÓN DEL NETHSERVER

Al iniciar la instalación de la máquina virtual demuestra gran rendimiento en su proceso de instalación pese a la poca asignación de recursos para su funcionamiento. Además, tiene interfaz gráfica bastante sencilla de configurar, para lo cual solo se requiere inicialmente configuración de red si así se requiere, contraseña del root, y la configuración de la zona horaria.

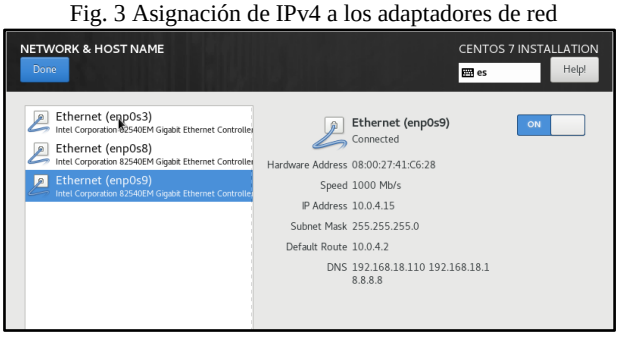
Fig. 2 Selección de país



Fuente: Autoría Propia

Partiendo que antes de comenzar la instalación de NethServer se realizó una configuración de zonas a cada uno de los adaptadores, Se asigna a los dos primeros adaptadores de red una dirección IP estática, en segmentos de red diferentes para tener una distinción más precisa según el rango utilizado, sin embargo el ultimo adaptador de red el cual se establece como zona WAN se configura como DHCP, para que el router asigne una IP de forma manual y no afecte el acceso a internet a través del servidor NethServer.

Fig. 3 Asignación de IPv4 a los adaptadores de red



Fuente: Autoría Propia

Otra de las opciones de las que dispone NethServer para configurar las direcciones IP con sus respectivas zonas, es mediante la configuración del adaptador puente que brinda el acceso a internet, conectando de la misma manera el equipo desktop para pertenecer al mismo segmento de red, e ingresando desde el navegador del equipo desktop mediante la dirección IP de la zona roja. No obstante, es recomendable realizar la configuración de las tres zonas de red, para luego vincular el equipo desktop a la red interna de la zona verde[3].

Aunque una de las ventajas de NetshServer es contar con una comunicación remota por ssh para realizar la configuración de cualquier servicio, no es posible dejar de lado el uso de su interfaz gráfica que, con pocos clics, ejecuta gran cantidad de comandos de forma interna que son invisibles al usuario, volviéndolo un sistema muy práctico de utilizar no solo por personas que no tienen mucho conocimiento de línea de comandos lo cual es la esencia de las distribuciones de Linux sino que además demuestra tener gran estabilidad y escalabilidad de su funcionamiento en la gran variedad de herramientas que emplea y como ejemplo de ello está la configuración de cada de las zonas de red, tal y como se muestra en la Fig. 4.

Fig. 4 Configuración de zonas de red

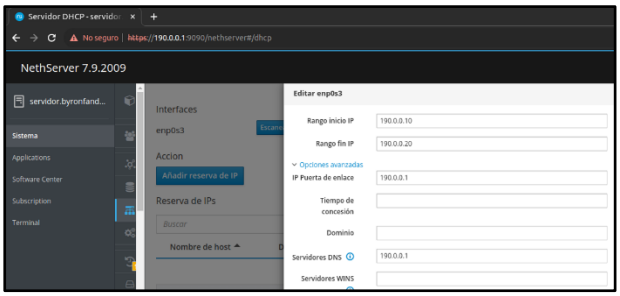
Fuente: Autoría Propia

5 SERVIDOR DHCP, DNS Y CONTROLADOR DE DOMINIO

5.1 SERVIDOR DHCP

En el menú Sistema se encuentra el submenú Servidor DHCP, el cual cuenta solamente con un switch para activar su configuración, apareciendo un formulario emergente en el cual se especifica los datos básicos de Rango de Inicio IP en donde la dirección ingresada debe estar alejada de la IP de la zona verde para tener un rango de IP iniciales estáticas que se consideren importantes vincular posteriormente de acuerdo a las necesidades que se puedan presentar, por otro lado está el campo de Rango fin IP, para lo cual se sugiere que no sea demasiado amplia para evitar los intentos de conexión innecesarios que para este ejemplo solo se tendrá un intervalo de 10 equipos. De igual manera se tiene a disposición el campo de puerta de enlace para establecer la comunicación con las otras zonas de red si así se desea y servidores DNS para utilizar el NethServer como puente de conexión a internet.

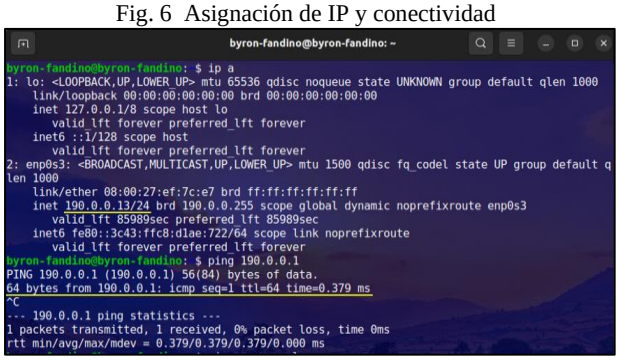
Fig. 5 Configuración de DHCP Nethserver



Fuente: Autoría Propia

Debido a que fue necesario colocar una dirección IP estática al servidor para que hiciera parte del segmento de red e ingresar al panel principal del servidor mediante la red interna; para este punto se procede a configurar el equipo desktop como DHCP, aplicando los cambios, no obstante, es necesario realizar un reinicio del servicio de red cada vez que se realiza una configuración diferente o en su defecto reiniciar el sistema operativo. Una vez hecho el reinicio se procede a verificar la nueva dirección IP asignada por el servidor DHCP, y su comunicación con la red.

Fig. 6 Asignación de IP y conectividad



Fuente: Autoría Propia

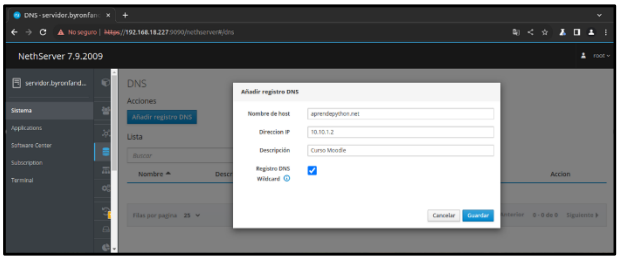
5.2 CONFIGURACIÓN DE DNS

Para el desarrollo de esta temática se realizaron dos configuraciones de DNS, la primera en un servidor web conectado a la zona naranja, el cual contiene una página web denominada aprendepython.net, mediante la instalación de herramientas como ISPConfig y Moodle [4]; y la segunda es la configuración en el NethServer para realizar el redireccionamiento de las peticiones del equipo de la zona verde mediante el navegador web al solicitar la página mencionada; es de aclarar que el servidor web tiene asignada una dirección IPv4 estática 10.10.1.2/24.

Teniendo en cuenta la información anterior, se procede a verificar inicialmente si el equipo desktop de la zona verde realiza ping de respuesta satisfactoria al servidor web que se encuentra en la zona naranja, para lo cual es necesario que este servidor tenga configurada en la puerta de enlace la dirección IP del adaptador de la zona en mención.

Se procede a ingresar al Menú principal Sistema y luego se da clic en el submenú DNS, el cual cuenta únicamente con un botón denominado como Añadir Registro DNS, que al dar clic se abre un formulario emergente para colocar 3 datos básicos, el nombre del host, dirección IP del host y una descripción general, así como se muestra en la Fig. 7.

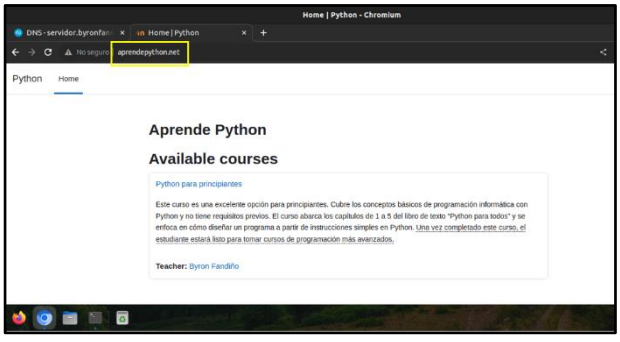
Fig. 7 Configuración DNS del NethSetver



Fuente: Autoría Propia

Haciendo énfasis en la configuración realizada en el servidor DHCP, no es necesario realizar ninguna configuración adicional al local al equipo desktop, por lo tanto, en este equipo se procede a abrir el navegador web, digitando la url aprendepython.net, y obteniendo como resultado el contenido de la página almacenada en el servidor web.

Fig. 8 Configuración DNS del NethSetver



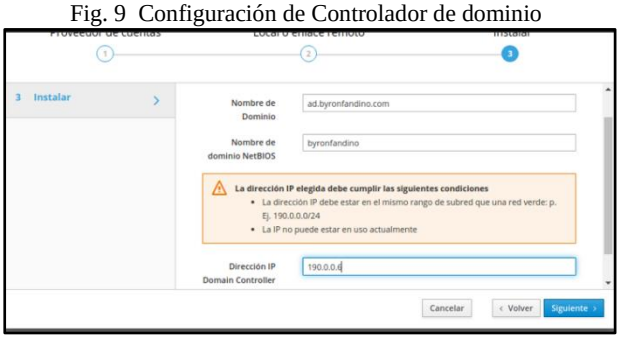
Fuente: Autoría Propia

5.3 CONTROLADOR DE DOMINIO

Antes de iniciar con la instalación del Controlador de Dominio, es necesario desplazarse hasta el menú Software Center, no para instalar algún paquete adicional sino actualizar los paquetes que ya se encuentran instalados, para lo cual es recomendable instalar cualquier actualización sugerida por el sistema y posteriormente continuar con el proceso de configuración del Active Directory.

Finalizada la actualización se procede a ingresar al submenú Usuarios y Grupos del Menú Sistema, se ejecuta de forma automática un asistente de configuración del Active Directory, el cual guía en el paso a paso según las necesidades del administrador del sistema, para culminar de forma satisfactoria la implementación de la nueva configuración.

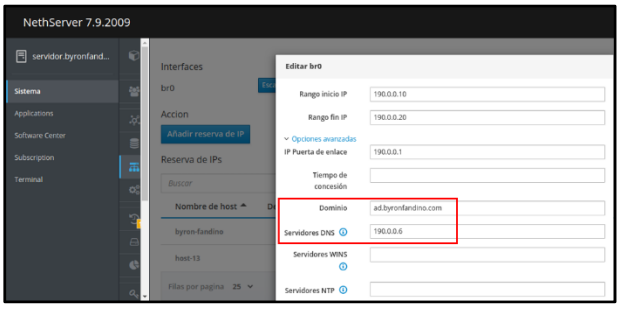
Fig. 9 Configuración de Controlador de dominio



Fuente: Autoría Propia

En la configuración del Active Directory se creó una nueva dirección IP, la cual es asignada al adaptador de red de la zona verde, estableciéndose como puente de dos direcciones IP, es decir, si se desea vincular un equipo al dominio es necesario especificar en su DNS la IP del dominio; por lo tanto, se realiza un ajuste en la configuración del servidor DHCP, para que los equipos de la misma zona tengan adopten estos parámetros antes de la vinculación al dominio.

Fig. 10 Actualización de Dominio y DNS en DHCP



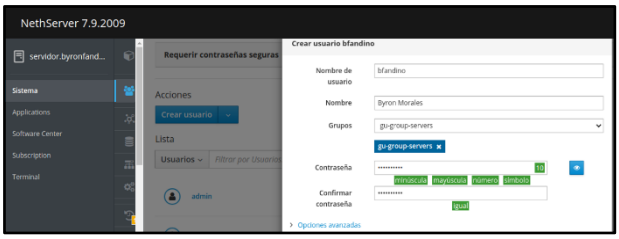
Fuente: Autoría Propia

Así como se reinicia el servicio de DHCP en el NethServer cuando adopta una nueva configuración, de la misma manera se debe reiniciar el servicio de red del equipo Desktop que se encuentre conectado haciendo uso de los servicios del servidor, porque de lo contrario no será posible la vinculación al dominio.

En el momento que la configuración del Active Directory termina, se crean dos cuentas administradoras por defecto, las cuales se encuentran bloqueadas, sin embargo, es necesario realizar su desbloqueo mediante la asignación de contraseñas, porque son indispensables en el proceso de vinculación del equipo de la zona verde al dominio.

Enseguida, se crea un nuevo grupo y usuario, en el orden mencionado, estableciendo una contraseña que debe cumplir con los parámetros de seguridad mínimos requeridos por el sistema de lo contrario no permite completar el proceso.

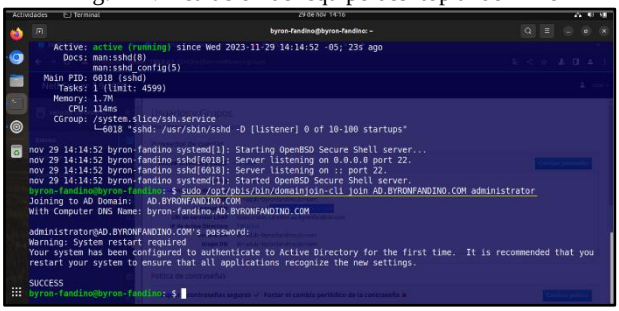
Fig. 11 Creación de usuario de dominio



Fuente: Autoría Propia

En el equipo Ubuntu Desktop de la zona verde se procede a instalar el paquete openssh-server, porque si este servicio no se encuentra activo al momento de digitar los comandos para la vinculación al dominio, este proceso no se llevará a cabo.

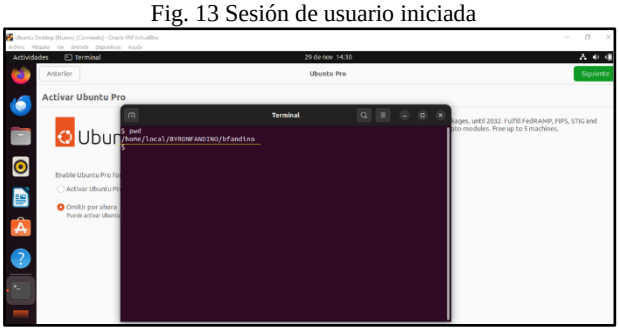
Fig. 12 Vinculación del equipo desktop al dominio



Fuente: Autoría Propia

Se reinicia el equipo desktop y se procede a digitar el nombre del usuario creado seguido del caracter arroba (@) y el nombre del dominio, con su respectiva contraseña.

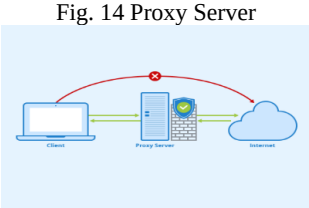
Fig. 13 Sesión de usuario iniciada



Fuente: Autoría Propia

6. PROXY

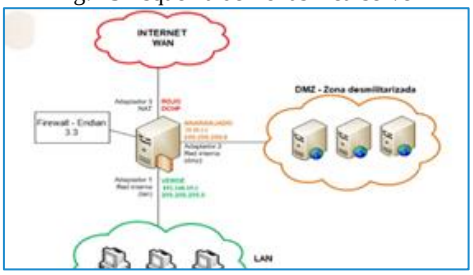
Fig. 14 Proxy Server



Fuente: Seobility - License: CC BY-SA 4.0

Los servidores proxy son intermediarios que se encargan de gestionar el tráfico web entre los clientes y los servidores de origen. Su uso en las empresas puede aportar beneficios en términos de seguridad, rendimiento y control, pero también implica ciertos desafíos técnicos y administrativos. NethServer es una herramienta que facilita la instalación, configuración y mantenimiento de un servidor proxy en el entorno empresarial. El servidor proxy que implementa NethServer, se basa en el software Squid, y este se puede complementar con otros módulos como SquidGuard, ClamAV, Lightsquid o Samba, para añadir funcionalidades de filtrado, antivirus, reportes o autenticación, respectivamente. Una de las principales ventajas de NethServer es que tiene una interfaz web intuitiva, desde la cual se puede acceder a las opciones del servidor proxy, como el modo de operación (transparente o manual), el puerto, el caché, las reglas de acceso, las listas negras o blancas, los perfiles de usuarios o grupos, los horarios, los informes, etc. Por medio de esta herramienta las empresas pueden optimizar el uso de Internet, proteger su red interna, y controlar y monitorizar el tráfico web de sus empleados, clientes o socios.

Fig. 15 Esquema de Zonas Nethserver

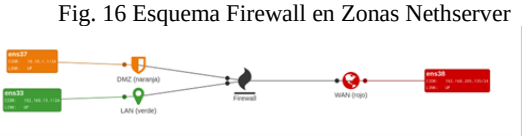


Fuente: Autoría Propia

A continuación, mostraremos el proceso requerido para realizar la instalación y configuración del servidor proxy en NethServer. Para ello, tendremos en cuenta los pasos realizados con anterioridad, teniendo como base la instalación ya demostrada y asumiendo que ya están configuradas las zonas verdes y rojas requeridas para demostrar el funcionamiento del proxy de la manera expuesta en la figura 20. Es de resaltar que el servicio de proxy es demandante en recursos de hardware, lo que requiere que se cuente con al menos 2 GB de RAM para el funcionamiento de este. Pero si se instalan más servicios en NethServer o el número de clientes aumenta, se debe ampliar la memoria, ya que puede generar bloqueos o demora en las respuestas o solicitudes.

Aunque no es necesario instalar un firewall previamente para instalar Squid proxy, ya que Squid proxy puede funcionar sin un firewall, se recomienda configurar uno para mejorar la seguridad y el control del tráfico web. Un firewall puede ayudar a filtrar los paquetes entrantes y salientes, a bloquear los puertos no utilizados o no deseados, y a prevenir posibles ataques o intrusiones. Esto se explicará más adelante en este artículo y para nuestra demostración previamente se ha configurado el firewall de la siguiente manera:

Fig. 16 Esquema Firewall en Zonas Nethserver



Fuente: Autoría Propia

También es recomendable que el administrador ya tenga configurado el Servidor DHCP para su Zona verde desde NethServer. Esto para que los equipos conectados a la red verde obtengan esta configuración automáticamente y se pueda asegurar que están conectados al servidor NethServer [1].

6.1 CONFIGURACION EN NETHSERVER

- Para instalar su servidor proxy, el administrador accede al apartado de Software Center y busca por la palabra web. Selecciona los paquetes de Web Filter y Web Proxy y hace clic en Install. Espera a que se complete la instalación y hace clic en Apply changes.

- Se verifica que los servicios estén funcionando, accediendo a la opción de Services en System. Puede que los servicios de Squid y ufdbGuard están detenidos. Estos servicios son los que se encargan del proxy y del filtrado web, respectivamente. Para iniciarlos, hace clic en el botón de Start que aparece al lado de cada uno. También puede activar la opción de Start at boot para que se inicien automáticamente al arrancar el sistema.

- El administrador accede al apartado de **Applications** y puede ver las dos nuevas opciones de **Web Proxy and Antivirus y Web Filter**. Estas opciones le permiten configurar el servidor proxy y el filtro web, respectivamente. Se agrega **Web Proxy and Antivirus** a su menú principal y se hace clic en esta opción.

- Se puede observar que el proxy no está funcionando debido a que no se ha configurado. Para ello, se debe de configurar las zonas por las que funcionará, así como el modo que tendrá: manual o transparente. El modo manual requiere que configure manualmente el proxy en cada cliente, mientras que el modo transparente intercepta automáticamente el tráfico web sin necesidad de configuración adicional. Para este caso, inicialmente se configurará en modo manual por requerimientos del ejercicio. También se bloquea el puerto HTTP-HTTPS para que desde la zona verde no se pueda acceder a NethServer. Para

hacer esto, se va a la sección de Settings y se selecciona las siguientes opciones: a. Status: enabled b. Mode: manual c. Networks: green d. Block HTTP and HTTPS ports: enabled e.

- Ahora, si se verifica el estado del servicio, se puede observar que ya está funcionando correctamente el servicio de Squid en los puertos **3128, 3129 y 3130**. Estos puertos corresponden al protocolo **HTTP, HTTPS y FTP**, respectivamente. Puede ver el estado del servicio en la sección de Dashboard, donde también puede ver el uso de la memoria caché y el número de conexiones activas.

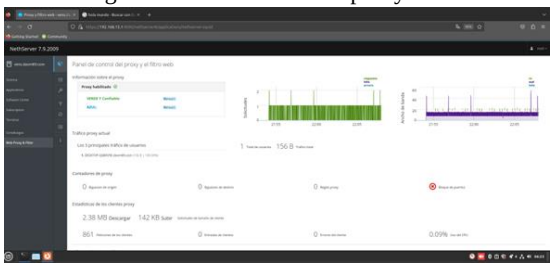
- Ahora, se retorna al apartado de **Web Proxy and Antivirus** y se puede observar que tiene dos advertencias relacionadas con **Netdata** que no está configurado correctamente. Netdata es un servicio que permite monitorizar el rendimiento del sistema y de los servicios en tiempo real. Las advertencias indican que Netdata no está escuchando en la zona verde, lo que impide que pueda acceder a sus gráficos desde el panel de control. Para arreglar esto, se debe de volver a **Services** en el menú de **System** y configurar el servicio de Netdata para que escuche en la zona verde. Para hacer esto, se hace clic en el botón de **Edit** que aparece al lado del servicio de Netdata y seleccionar la opción de **green** en la sección de **Access**. Se hace clic en Update para guardar los cambios.

- Para configurar las reglas de filtrado, el administrador accede a la opción de **Categories** en el menú de **Web Proxy and Antivirus**. Aquí puede ver la opción de **Université Toulouse 1 Capitole (free)**, que son las reglas por defecto del proyecto NethServer, que para este caso servirán para filtrar el contenido. Lo primero que se hace es dar clic en el botón de **Configure** y luego en el botón de **Download** para descargar las listas correspondientes. Estas listas contienen más de 100 categorías de sitios web clasificados según su contenido, como educación, entretenimiento, juegos, noticias, redes sociales, etc. Una vez descargadas las categorías, se procede a configurar los filtros. Para ello, accede al menú de **Filter** dentro de **Web Proxy and Antivirus**. Aquí se puede crear diferentes perfiles de filtrado para aplicarlos a distintos usuarios o grupos. Se crea un perfil de opción global para poder agregar las listas que se descargaron. Para hacer esto, se hace clic en el botón de **Create new profile** y se le da un nombre, por ejemplo, **Global**. Luego, selecciona la opción de **Global** en el campo de Profile type y hace clic en **Save**.

- Ahora que tiene un perfil predeterminado, se procede a agregarle las categorías de las listas que se quiere bloquear. Para edste caso, selecciona las opciones de **adult, mixed_adult y publicite**, que corresponden a sitios web de contenido adulto, mixto o publicitario, respectivamente. Para hacer esto, se hace clic en el botón de **Edit** que aparece al lado del perfil **Global** y luego en el botón de **Add categories**. Se selecciona las categorías deseadas y se hace clic en **Save**. También puede configurar otras opciones, como el nivel de bloqueo, el mensaje de advertencia, el horario, etc.

- El administrador verifica en el panel principal de **Web Proxy and Antivirus** que todo esté funcionando correctamente. También puede verificar que Squid le permite acceder a los reportes, haciendo clic en el botón de **Report** que aparece al lado del servicio de **Squid**. Aquí puede ver estadísticas sobre el tráfico web, como el número de solicitudes, el tamaño de la caché, el uso del ancho de banda, las categorías más visitadas, etc. Estos reportes le pueden ayudar a analizar el comportamiento de los usuarios, a identificar los sitios web más demandados o bloqueados, y a optimizar el uso de los recursos. También puede exportar los reportes en formato CSV o PDF, haciendo clic en los botones correspondientes que aparecen en la parte superior derecha de la pantalla.

Fig. 17 Estado del servidor proxy



Fuente: Autoría Propia

6.2 CONFIGURACIÓN EN CLIENTES:

- Ahora que ya se tiene configurado el servidor proxy, el administrador procede a configurarlo en los clientes. Para ello, va a hacer una prueba ingresando a la página de Speedtest, la cual como se puede identificar carga bastante publicidad. La intención es bloquear esto por medio del proxy, ya que este tiene ya determinada la categoría de publicite que bloqueará este contenido. Para hacer esto, el administrador debe de seguir los siguientes pasos:

- El administrador se dirige a la configuración de red de su cliente y la establece en manual. Coloca la IP de su servidor proxy y el puerto 3128, que es el que corresponde al protocolo HTTP. También puede configurar el puerto 3129 para el protocolo HTTPS y el puerto 3130 para el protocolo FTP. Estos puertos son los que ha configurado en el servidor proxy en los anteriores pasos.

Fig. 18 Configuración Proxy en Cliente

Fuente: Autoría Propia

- Ahora vuelve a ingresar a la página de Speedtest y cómo puede observar toda la publicidad fue filtrada por el proxy, entregando una página más limpia. Esto se debe a que el proxy ha bloqueado las solicitudes que pertenecen a la categoría de publicite, en nethserver.

- Además, Además, si intenta acceder a alguna página para adultos, tiene el siguiente mensaje de error:

  "*Access to the following web site is denied: https://www.example.com/ This web site belongs to one or more categories that are blocked by the web filter: adult, mixed_adult. If you think this web site should not be blocked, please contact your network administrator*."

  Este mensaje se muestra porque el proxy ha bloqueado las solicitudes que pertenecen a las categorías de adult y mixed_adult.

Fig. 19 Bloqueo de pagina por proxy

Fuente: Autoría Propia

- Si ve el registro de acceso desde NethServer, puede ver que el contenido ha sido filtrado. Para hacer esto, va al menú de Web Proxy and Antivirus y hace clic en el botón de Access que aparece al lado del servicio de Squid. Aquí puede ver el detalle de cada solicitud, como la fecha, la hora, la IP del cliente, el método, la URL, el código de respuesta, el tamaño, el tiempo, etc. También puede ver el color de cada solicitud, que indica si fue permitida (verde), bloqueada (rojo) o redirigida (amarillo).

- También es posible configurar el proxy en modo transparente. Para ello, el administrador debe de modificar la configuración del proxy de manual a transparente en Nethserver Servidor Proxy y dejar la configuración de red de los clientes en modo automático. De esta manera, el proxy interceptará automáticamente el tráfico web sin necesidad de configurar el proxy en cada cliente. Para hacer esto, se va a la sección de Settings en el menú de Web Proxy and Antivirus y selecciona la opción de transparent en el campo de Mode. Hace clic en Save para guardar los cambios. Luego, en los clientes, va a la configuración de red y la establece en automático. Así, el proxy funcionará de forma transparente para los clientes.

Todo este procedimiento de la configuración del proxy, así como la demostración del funcionamiento de este se muestra de manera visual por medio del siguiente enlace web: Diego. Ojeda. Sustentación Paso 9 - Diplomado Linux - Proxy Nethserver. (Dec 11, 2023). Accessed: Dec 12, 2023. [https://youtu.be/e7tks8rlT8Y]. Donde está de manera más específica las configuraciones realizadas en netserver.

7. CORTAFUEGOS

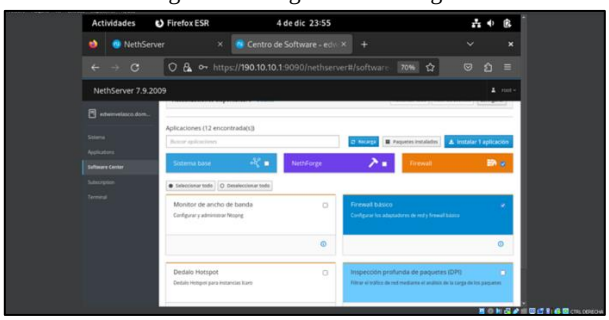
Un cortafuegos de aplicaciones, también conocido como firewall de aplicaciones, es un tipo de cortafuegos que controla el tráfico entrante y saliente en la capa de aplicaciones de una red, controlando la ejecución de archivos o código por parte de aplicaciones concretas. Aunque un intruso acceda a una red o un servidor, no puede ejecutar código malicioso.

En el contexto de un servidor web como NethServer, un cortafuegos de aplicaciones protege las páginas web de diferentes índoles al inspeccionar y filtrar el tráfico a nivel de aplicación. Esto ayuda a prevenir ataques y otras vulnerabilidades comunes en la seguridad de las aplicaciones web [14].

7.1 CONFIGURACIÓN DE CORTAFUEGOS DESDE NETHSERVER

Como primera instancia se debe instalar el Firewall para ejecutar la labor de restricción a diferentes sitios web de entretenimiento y, asimismo, redes sociales. Por lo cual, desde el panel de NethServer, se escoge la opción de Software center para instalar el cortafuegos, dando clic sobre Firewall, Firewall Básico y luego en se pulsa en instalar.

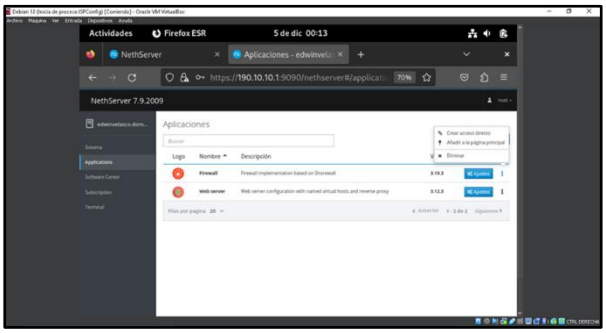
Fig. 20 Descarga de Cortafuegos



Fuente: Autoría propia

Después de la instalación del Firewall se crea un acceso directo, para visualizar la herramienta desde el panel principal de NethServer. Para esto, se ubica el Cortafuegos instalado en la pestaña de aplicaciones, y luego se da clic en la parte final del mismo, en donde se visualizará el apartado de crear acceso directo, con lo cual, quedará anclado al panel principal para su uso.

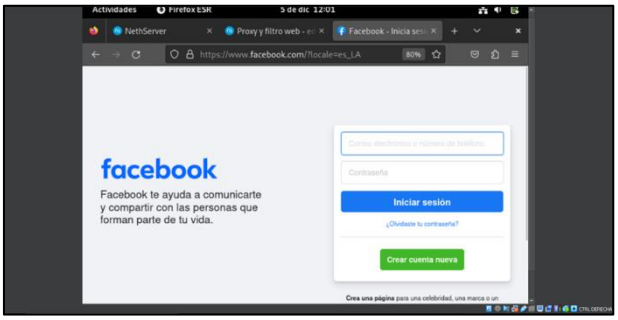
Fig. 21 Acceso directo de Cortafuegos



Fuente: Autoría propia

Después de tener el cortafuegos listo para empezar a implementar las diferentes reglas de restricción en redes sociales y sitios de entretenimiento, se verifica que una de las páginas web esté funcionando correctamente.

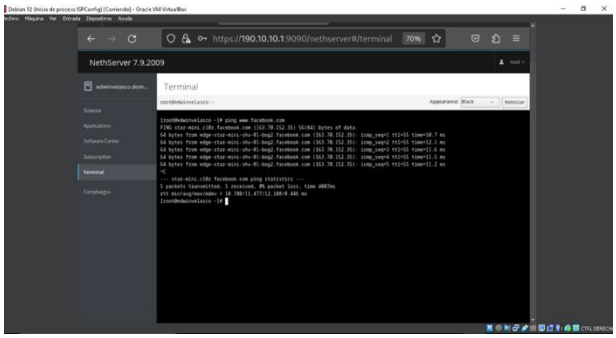
Fig. 22 Descarga de Cortafuegos



Fuente: Autoría propia

En este caso, se iniciará con una red social como lo es Facebook. En primera instancia, se deben hallar la o las IPS que esta plataforma utiliza para su Andamiaje. De acuerdo a esto, se procede a ubicar dichas direcciones, realizando un ping desde la terminal de NethServer, y luego se ejecuta el comando nslookup www.facebook.com, ya que esta plataforma, dispone de varias IPS para su acceso.

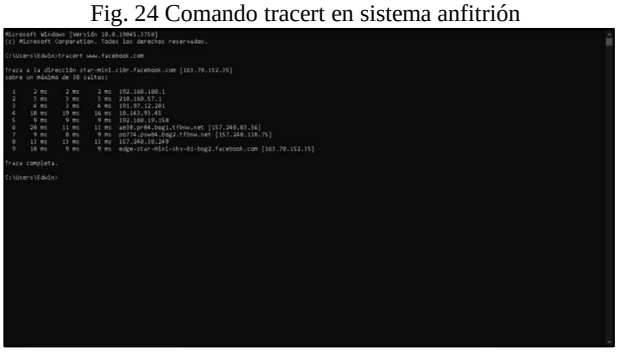
Fig. 23 Identificación de IP de Facebook



Fuente: Autoría Propia

También, se ejecuta el comando tracert www.facebook.com en el sistema anfitrión para evidenciar el tráfico de Facebook por las diferentes IPS y se eligen aquellas de carácter público. Este proceso también se podría ejecutar en NethServer, cambiando el adaptador 3 a puente nuevamente.

Fig. 24 Comando tracert en sistema anfitrión

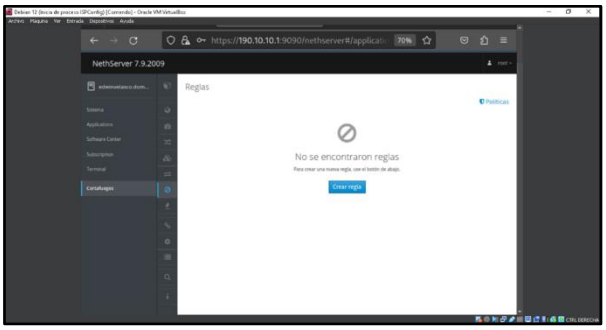


Fuente: Autoría Propia

7.2 CREACIÓN DE REGLAS EN FIREWALL

Luego de obtenidas la IPS de Facebook, se da clic en el menú Cortafuegos del panel principal y se escoge la opción Reglas, en el cual aparece un único botón para crear la primera regla del firewall; al pulsar el botón aparece un formulario emergente.

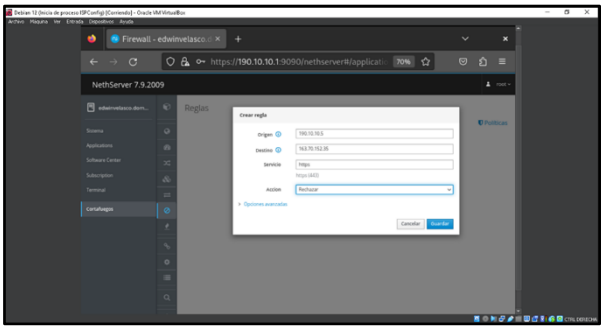
Fig. 25 Creación de reglas en Firewall



Fuente: Autoría Propia

Se crea la primera regla poniendo como origen la IP de la máquina virtual con su respectivo host. Luego, se ingresa la primera IP a bloquear, en servicio se escoge la opción https y en la acción se rechaza. Se da clic en guardar y ya está configurada la primera regla de restricción para el ingreso de Facebook.

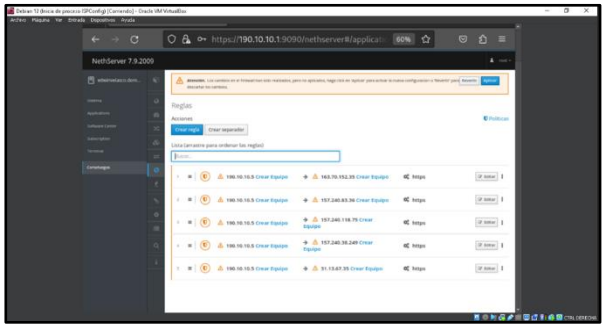
Fig. 26 Creación y configuración de reglas en Firewall



Fuente: Autoría propia

Como en Facebook son varias IPS disponibles, entonces se procede a crear las siguientes reglas de bloqueo, siguiendo los mismos pasos y cambiando únicamente la IP en destino. Después de configurar las reglas correspondientes, se procede a activar los cambios y reiniciar NethServer

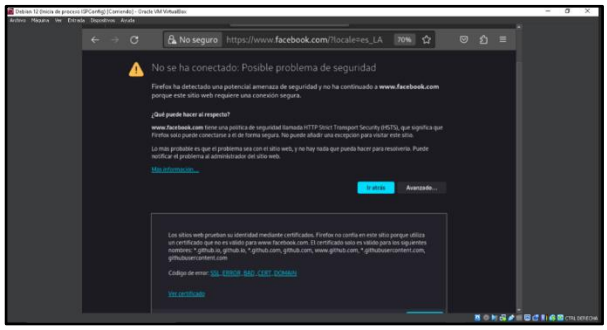
Fig. 27 Creación de reglas en Firewall



Fuente: Autoría propia

Después de aplicar los cambios y reiniciar NethServer con el comando reboot ejecutado desde la terminal, se procede a evidenciar que efectivamente, no se puede ingresar a la red social de Facebook, debido a las restricciones configuradas, mediante las 5 reglas anteriormente descritas.

Fig. 28 Bloqueo web con Firewall



Fuente: Autoría Propia

8 FILE SERVER Y PRINT SERVER

Cuando se habla de FileServer se hace referencia básicamente a un servidor de archivos o en otras palabras una serie de carpetas compartidas en donde según la configuración un grupo de personas o usuarios pueden acceder y dependiendo los permisos a leer o escribir dentro de las carpetas, y para PrintServer podemos aplicar lo anterior, pero en vez de carpetas habría impresoras compartidas los cuales los usuarios de la red pueden usar para imprimir documentos [15].

A partir del punto 4 en el proceso de instalación y configuración Nethserver, se configuraron la tipología de red en donde hay 3 adaptadores, uno para zona verde, naranja y roja para internet.

8.1 CONFIGURAR LDAP

Se ingresa a la opción de Usuario y grupos dentro de sistema y seleccionamos Configurar el proveedor de cuentas y seleccionamos LDAP

Fig. 29 Selección proveedor de cuentas

Fuente: Autoría Propia

Se selecciona instalar LDAL local y se presiona en siguiente

Fig. 30 Instalación proveedor de cuentas

Fuente: Autoría Propia

Se procede a instalar el paquete y verificar que el proveedor se haya instalado correctamente.

Fig. 31 Instalación paquetes

Fuente: Autoría Propia

Se procede a crear un usuario nuevo para asociarlo al servicio y terminar con la configuración del proveedor de cuentas.

Fig. 32 Creación usuario

Fuente: Autoría Propia

8.2 INSTALACIÓN FILESERVER Y PRINTSERVER

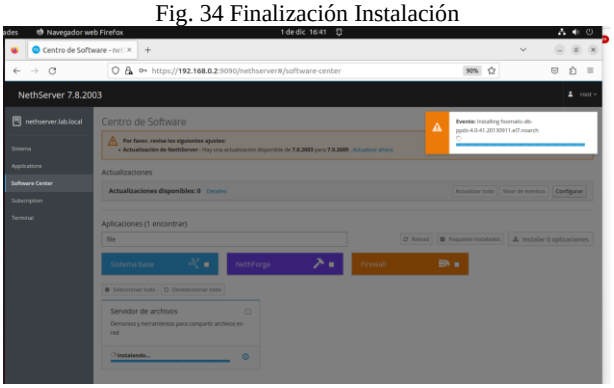
Se procede a verificar que tengamos los servicios instalados, nos dirigimos a la opción de Software Center y procedemos a buscar Print y file y darle instalar

Fig. 33 Instalación aplicativos

Fuente: Autoría Propia

Se procede con la instalación

Fig. 34 Finalización Instalación



Fuente: Autoría Propia

Se procede a verificar que los aplicativos se encuentren instalados

Fig. 35 Verificación aplicativos

Fuente: Autoría Propia

8.3 CONFIGURAR FILESERVER Y PRINTSERVER

Se verifica el grupo de trabajo o nombre de dominio WORKGROUP para poder configurar los terminales de la zona verde

Fig. 36 Verificación grupo de trabajo

Fuente: Autoría Propia

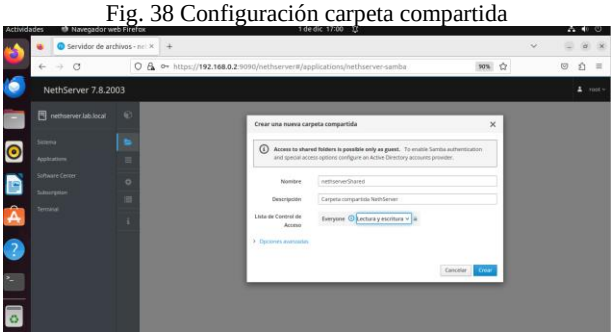
Se ingresa a la opción de carpetas y se procede a crear un nuevo folder

Fig. 37 Creación carpeta compartida

Fuente: Autoría Propia

Dentro de la configuración de la carpeta se indica el nombre de la carpeta, la descripción y los permisos deseados (lectura o lectura y escritura)

Fig. 38 Configuración carpeta compartida



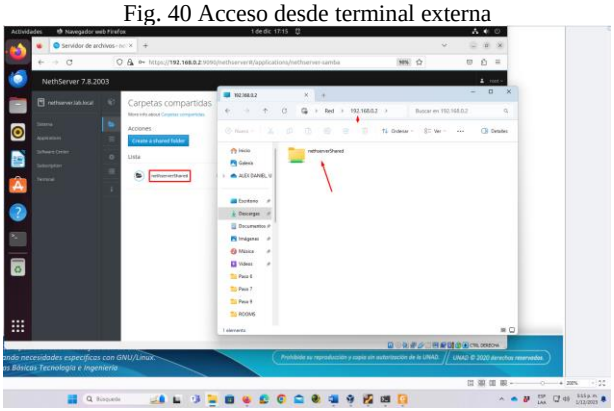
Fuente: Autoría Propia

Fig. 39 Carpeta compartida

Fuente: Autoría Propia

Se verifica desde otra terminal que se encuentra en la zona verde que se tenga acceso a la carpeta compartida

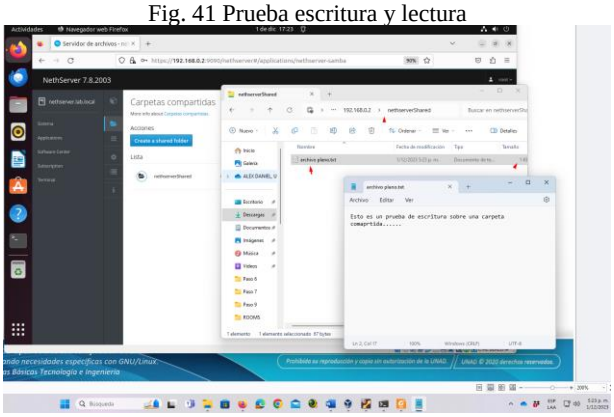
Fig. 40 Acceso desde terminal externa



Fuente: Autoría Propia

Se realiza prueba de escritura y lectura sobre la carpeta compartida, donde se evidencia que se puede crear archivos.

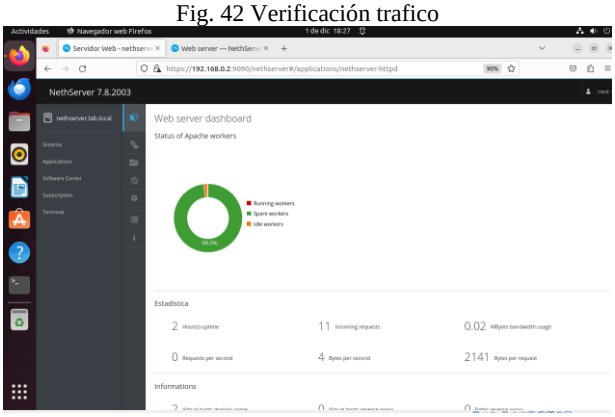
Fig. 41 Prueba escritura y lectura



Fuente: Autoría Propia

Se verifica el tráfico que se tiene hacia la carpeta compartida

Fig. 42 Verificación trafico



Fuente: Autoría Propia

Se verifica que, desde otra terminal, en este caso un Windows XP que está dentro de la zona verde tenga

acceso a las carperas y también a las impresoras compartidas, se verifica la IP de la terminal.

Fig. 43 Comprobación IP zona verde

Fuente: Autoría Propia

Ahora se verifica que tengamos acceso a la IP 191.0.0.1 donde se encuentran las carpetas e impresoras compartidas.

Fig. 44 Acceso a IP

Fuente: Autoría Propia

Se verifica que si se esté listando las impresoras compartidas.

Fig. 45 Verificación recursos compartidos

Fuente: Autoría Propia

9 VPN

VPN o Red Privada Virtual es una tecnología que brinda una conexión segura entre un host usuario y servidor brindado así privacidad y seguridad de la información, de acuerdo con [13]

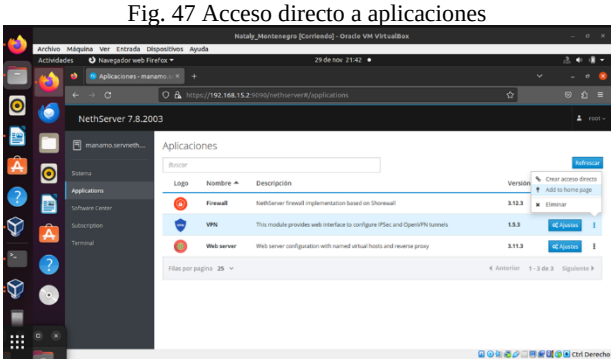
Tras culminar con la instalación de NethServer y realizar las configuraciones de las zonas de red verde, naranja y roja. Desde el centro de software se buscan e instalan las aplicaciones requeridas en este caso Firewall básico y OpenVPN.

Fig. 46 Instalación de Aplicaciones

Fuente: Autoría Propia

Culminada la instalación de las aplicaciones requeridas son ubicadas en el menú de Aplicaciones; para facilitar la navegación se adiciona un acceso directo de cada aplicación al menú desde la opción crear acceso directo.

Fig. 47 Acceso directo a aplicaciones



Fuente: Autoría Propia

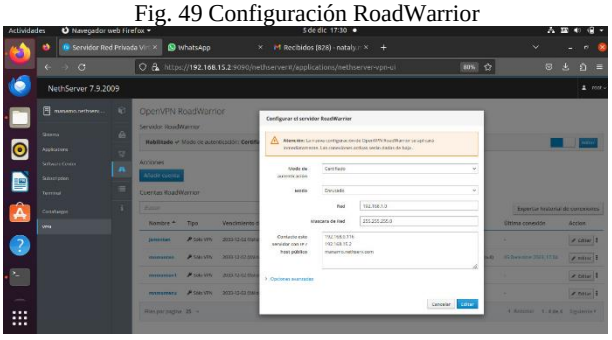
Desde la aplicación de administración del firewall, sección de configuración se habilita la opción de trafico de roadwarrior OpenVPN.

Fig. 48 Aplicaciones instaladas

Fuente: Autoría Propia

Posteriormente, a través del menú VPN opción OpenVPN RoadWarrior se crea y habilita la configuración de servidor RoadWarrior, indicando modo de autenticación, red por la cual se implementará el túnel seguro de las conexiones recibidas por medio de túnel VPN, además de los servidores a los cuales se dará acceso.

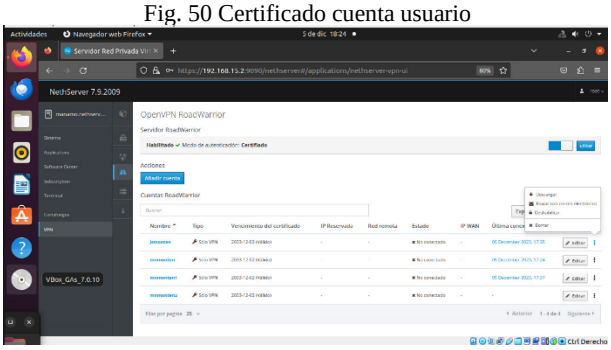
Fig. 49 Configuración RoadWarrior



Fuente: Autoría Propia

Una vez configurado y habilitado el servidor RoadWarrior, se procede a crear las cuentas de usuario a las cuales se dará conexión a través de VPN y se descargará el certificado proporcionado.

Fig. 50 Certificado cuenta usuario



Fuente: Autoría Propia

Obtenido el certificado de acceso de VPN se importa desde los hosts usuarios, una de las formas de hacer la importación en Ubuntu es desde el entorno gráfico por medio del gestor de configuraciones, sección red, opción Añadir VPN, importar desde un archivo.

Fig. 51 Importar certificado

Fuente: Autoría Propia

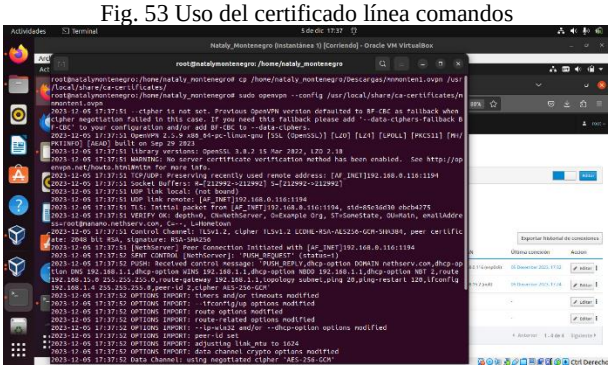
Finalizada la importación del certificado se corrobora la identidad y se activa la conexión VPN, y en la barra de tareas se evidencia la correcta conexión.

Fig. 52 Identidad certificado

Fuente: Autoría Propia

Otra de las formas de usar el certificado en Ubuntu es realizando la importación desde línea de comando, para ello debemos contar con la previa instalación de OpenVPN, copiamos el certificado a la carpeta de certificados de la aplicación y procedemos a hacer uso de este con el comando sudo --OpenVPN y a ruta del certificado.

Fig. 53 Uso del certificado línea comandos



Fuente: Autoría Propia

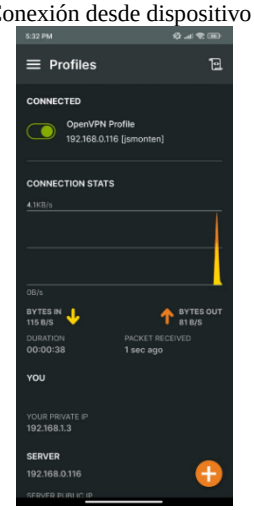
Si la conexión del túnel VPN es correcto se evidencia el mensaje de inicialización de secuencia completada.

Fig. 54 Conexión VPN terminal

Fuente: Autoría Propia

De igual forma el túnel de conexión de VPN permite realizar conexión desde cualquier otro dispositivo, para el siguiente ejemplo celular SO Android, en donde teniendo previamente instalada la aplicación OpenVPN se importa certificado proporcionado y se evidencia conexión exitosa con la activación de la conexión y graficas de trasmisión de información.

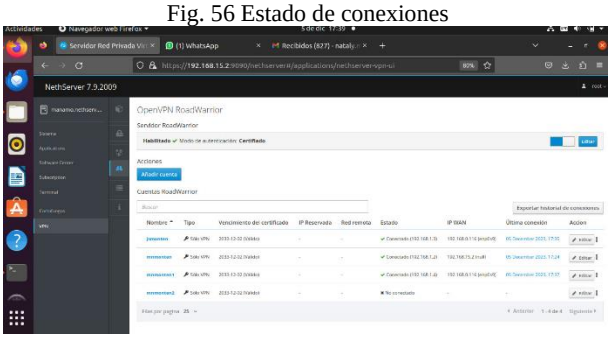
Fig. 55 Conexión desde dispositivo Android



Fuente: Autoría Propia

Desde el entorno grafico de NethServer, menú VPN, submenú OpenVPN RoadWarrior se administra las conexiones de VPN y se brinda la posibilidad de evidenciar el estado de cada uno de los usuarios habilitados, su estado de conexión, además de fecha y hora de ultima conexión.

Fig. 56 Estado de conexiones



Fuente: Autoría Propia

CONCLUSIONES

La configuración del servidor DHCP, permitió realizar una vinculación rápida para cualquier equipo Ubuntu que se asigne a la zona verde, sin embargo, se tuvo el inconveniente en algunos equipos que presentaban fallas durante el proceso de registro en el Active Directory, debido a que se habían alterado varios registros propios del sistema que impedían su adecuada vinculación al dominio; para lo cual fue necesario conectar a la zona verde solo máquinas virtuales recién instaladas, solucionando no solo la vinculación exitosa al dominio sino el inicio de sesión con el usuario creado.

El servidor proxy se ha implementado en la zona verde de la red, que corresponde a la red interna de la empresa, y se ha encargado de gestionar el tráfico web entre los clientes y la zona roja, que corresponde a la red externa o Internet. El servidor proxy se ha complementado con otros módulos, como Web Filter, Web Proxy and Antivirus que han permitido realizar funciones de filtrado, antivirus y reportes, respectivamente. Con estas funciones se ha logrado bloquear el tráfico inapropiado, como el contenido adulto o publicitario, y se ha generado informes del tráfico generado entre las zonas, lo que ha permitido controlar y monitorizar el uso de Internet por parte de los empleados, clientes o socios. Estas acciones han contribuido a mejorar la seguridad, el rendimiento y el control de la red empresarial, así como a optimizar el uso de los recursos y a prevenir posibles ataques o intrusiones. Se recomienda que el administrador del servidor proxy revise periódicamente los reportes y las reglas de filtrado, y que actualice los módulos y el software cuando sea necesario. También se sugiere que se realicen pruebas de rendimiento y seguridad para verificar el correcto funcionamiento del servidor proxy y sus complementos. Finalmente, se propone que se explore otras funcionalidades que ofrece NethServer, como la autenticación, la caché o el modo transparente, que pueden ser de utilidad para mejorar la experiencia del usuario y la administración del servidor proxy.

Los servidores de archivos ofrecen una serie de ventajas, entre las que se incluyen Centralización de los archivos, Mejora

de la seguridad, Optimización del rendimiento ya que estos proporcionan un lugar centralizado para almacenar archivos, lo que facilita su acceso y gestión a los usuarios de la red.

Haciendo uso de la aplicación OpenVPN, la cual es soportada por el SO NethServer se puede habilitar túneles seguros de comunicación entre las diferentes zonas del prototipo de red a usar en pequeñas y medianas empresas, e incluir hosts externos brindado así conexiones seguras y de fácil administración.

REFERENCIAS

[1] RedesZone (2016). NethServer: conoce esta distro basada en CentOS/RHEL. https://www.redeszone.net/2016/09/26/nethserver-conoce-esta-distro-basada-centosrhel-crear-propio-servidor-casa-u-oficina/

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

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

[4] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid. ES: IC Editorial. elibro. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92

[5] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

[6] Red Hat. (2023). Red Hat Enterprise Linux. https://www.redhat.com/es

[7] Knoppix. (2021). What is KNOPPIX®?. https://www.knopper.net/knoppix/index-en.html

[8] Mandriva. (2023). Open Mandriva Association. https://sourceforge.net/projects/openmandriva/files/release/ROME/

*ingeniería.*UNAD.Ibagué.https://repository.unad.edu.co/handle/10596/42009

[9] CentOS. (2023). The CentOS Project. https://www.centos.org/

[10] Fedora Project. (2023). Fedora Linux. https://www.fedoraproject.org/en/workstation/download/

[11] Nethserver (2023). Nethserver Community. https://www.nethserver.org/getting-started-with-nethserver/

[12] Servidores, L. V. [@LabVirtualesServidores]. (2023, octubre 12). Instalar #NethServer + Configurar Web Proxy & Filtrar Contenidos Web. Youtube. https://www.youtube.com/watch?v=cIHJbtTehKg

[13] CISET. Centro de Innovación (2023). VPN - Red Privada Virtual [En línea]. Disponible en: https://www.ciset.es/glosario/494-vpn

[14] Vazquez Pantaleon, J., Fombona, G. N., & Rojas Cid, J. D. (2022). Implementación de cortafuego de aplicación en plataformas web y API´s para la contención y mitigación de ciberataques. Ciencia Latina Revista Científica Multidisciplinar, 6(6), 4045-4064. https://doi.org/10.37811/cl_rcm.v6i6.3757

[15] Nethserver(). Carpetas compartidas [En linea]. https://docs.nethserver.org/en/v7/shared_folder.html