RESULTADOS DEL DESARROLLO DE ACTIVIDADES INDIVIDUALES DEL TRABAJO COLABORATIVO "SOLUCIÓN DE NECESIDADES ESPECIFICAS CON GNU LINUX" TEMÁTICAS PROXY Y FIREWALL

Oscar Alirio Aponte Castilla
oaapontec@unadvirtual.edu.co
Carlos Augusto Gutiérrez Arias
cagutierreza@unadvirtual.edu.co

RESUMEN: *El presente artículo muestra el desarrollo de dos temáticas enfocadas en la solución de necesidades específicas de una empresa en su área informática, soluciones que se deben implementar mediante sistema operativo GNU Linux distribución Nethserver; las temáticas fueron elegidas por cada estudiante del grupo colaborativo 8 del diplomado de profundización en GNU Linux de la UNAD, cada temática se desarrolló logrando como resultado la solución a una necesidad de la empresa, los resultados registrados en este documento son la creación de una red LAN simulada en entornos virtuales, accesible para todos los usuarios de manera segura para la empresa y ágil para el usuario, administración de la red LAN con los controles de acceso correspondientes para garantizar disminución del riesgo de fuga o perdida de información, implementación de zonas de tráfico, DMZ, LAN y WAN, configuración de navegación fluida en la red LAN, reglas de restricción y de permiso de acceso de la red. Lo anterior cumpliendo los requerimientos de la empresa aplicando el conocimiento alcanzado, en un ejercicio práctico.*

PALABRAS CLAVE: Linux, Proxy, Firewall, Nethserver x.

1. INTRODUCCIÓN

Nethserver es una distribución Linux basada en CentOS y Red Hat orientada a servicios de administración de pequeñas y medianas redes, dentro de sus características más relevantes se encuentra el bajo costo de implementación y sus prestaciones en cuanto a control de tráfico de red, filtrado web, servicios DNS, DHCP y monitoreo de red, entre otros.

El presente informe expone algunos de estos servicios y su aplicación en un entorno simulado con fines prácticos aplicables a la realidad en el ejercicio profesional

2. INSTALACIÓN, CONFIGURACIÓN E INICIO DEL SERVIDOR NETHSERVER

Como primera medida cada estudiante efectúa la descarga de la herramienta de instalación del servidor Nethserver imagen iso de la página oficial, una vez descargada la imagen iso se guarda en la carpeta correspondiente a la ubicación desde la cual se añadirá y se instalará la herramienta en máquina virtual utilizando el gestor de máquinas virtuales Virtual Box de Oracle.

Los estudiantes previa instalación del servidor Nethserver configuran los recursos de hardware mínimos requeridos para el correcto funcionamiento de la distribución de acuerdo con los servicios requeridos por la empresa y los cuales se van a suministrar desde el servidor.

La configuración de la máquina virtual para la instalación de Nethserver es la siguiente:

-Almacenamiento en disco duro 50 GB
-Memoria RAM 2 GB
-Tarjetas de red, se activan 3 tarjetas
    -Tarjeta 1: modo red interna, nombre: LAN
    -Tarjeta 2: modo red interna, nombre: DMZ
    -Tarjeta 3: modo NAT
-Unidad óptica con la imagen ISO de Nethserver

Configurada la máquina virtual con los requerimientos mínimos para la instalación, configuración e implementación del servidor Nethserver, se inicia la instalación de la distribución bajo guía de página oficial https://www.nethserver.org/

Se elige instalación interactiva configurando cada uno de los elementos básicos de funcionamiento del servidor como teclado, nombre del servidor, ubicación, zona horaria, usuario administrador.

una vez realizada la instalación exitosa del servidor, se hace actualización del sistema para utilizar el último kernel estable desarrollado para la distribución; esto se realiza iniciando sesión como root o usuario administrador y con el comando ***yum update***.

Se reinicia el sistema, ingresando nuevamente como usuario administrador y se ejecutan pruebas de conexión como; comprobar la conexión del servidor con internet haciendo un ping a Google, revisar e identificar las ip de cada una de las tarjetas de red.

Para acceder al servidor en su interfaz web se debe iniciar un equipo cliente, este equipo debe tener una tarjeta de red activa en modo Red Interna, y conectada la red de nombre LAN o el nombre con el que se halla identificado la red segura en el servidor; así mismo se debe verificar que este equipo cliente tenga asignada una ip que se encuentre dentro del mismo sector que la ip del servidor; por ejemplo, si el servidor tiene asignada una ip 192.168.0.10, la dirección del equipo cliente debe ser 192.168.0.XX donde XX corresponde a un número entre 1 y 255 diferente a 10, ser recomienda realizar pruebas de tráfico entre el servidor y el cliente realizando ping entre los dos equipos para confirmar la correcta configuración de las tarjetas de red

Desde el equipo cliente se debe ingresar al navegador y realizar conexión a la ip del servidor indicando el puerto 9090, un ejemplo de este direccionamiento seria 192.168.0.10:9090

De esta manera se accede al campo Log del Server Manager o administrador web del servidor, se accede mediante la autenticación del usuario y la clave de acceso al servidor

.

Una vez ya en el panel de administración (Server Manager) se realiza la configuración inicial del servidor siguiendo las recomendaciones que muestra el panel antes de iniciar con la instalación de las herramientas necesarias para establecer los servicios que va a suministrar el servidor Nethserver según la temática de cada estudiante.

Dentro de las configuraciones iniciales la más importante es la configuración de red; en este apartado se definen las tres zonas cada una asignada a una tarjeta de red; la Tabla 1, ilustra la configuración recomendada

Tabla 1

ZONA	TARJETA - RED	ASIGNACIÓN IP
VERDE	LAN	MANUAL
NARANJA	DMZ	MANUAL
ROJA	WAN - NAT	DHCP

Configurada esta parte se procede a instalar las aplicaciones requeridas para el desarrollo de las temáticas desarrolladas; cada estudiante descarga e instala las aplicaciones desde el módulo de *Centro de software* de forma automática y realiza las configuraciones para cada servicio, así mismo realiza las pruebas que demuestran el funcionamiento de los servicios y el cumplimiento de lo solicitado en cada temática.

3. TEMÁTICAS DESARROLLADAS

- Temática 2: Proxy
- Temática 3: Firewall

3.1. 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.

Se puede observar la configuración de la máquina virtual e instalación del servidor Nethserver ya que durante la instalación y aun antes se debe configurar en la máquina virtual del servidor las tarjetas de red por las cuales recibirá conexión a internet y suministrará los servicios requeridos para la red de la empresa (figura 1).

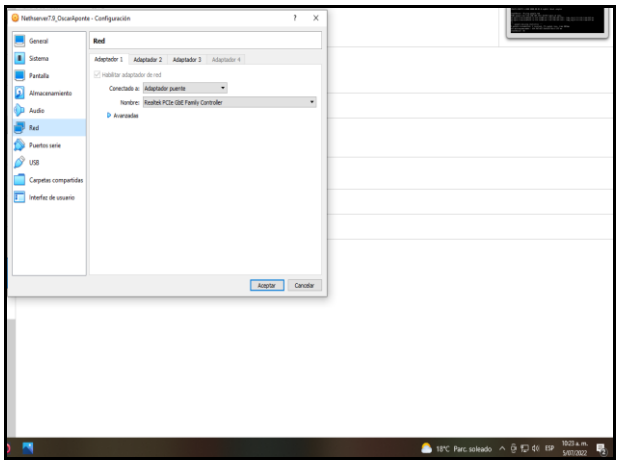

Figura 1 Configuración tarjetas de red.

Segundo paso se instala en máquina virtual el servidor Nethserver y se realiza conexión remota desde el equipo futuro cliente (Debian 11 desktop) a través dirección ip del servidor Nethserver, mediante “server manager” se ingresa a panel de control del servidor (figura 2).

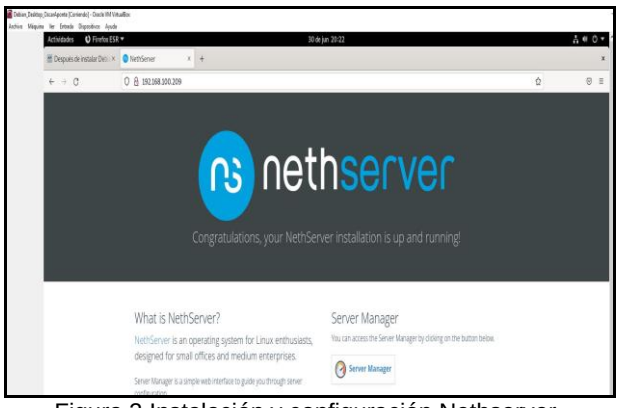

Figura 2 Instalación y configuración Nethserver.

Tercer paso, se logra ingreso al panel de control de Nethserver, se ingresa como usuario administrador root con la contraseña establecida en la instalación (Figura 3).

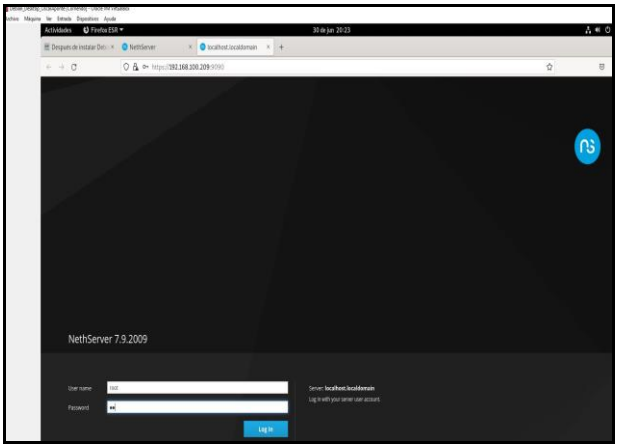

Figura 3 Ingreso a panel de control.

Cuarto paso, se inicia la administración y adecuación desde el panel de control para el correcto funcionamiento de nuestro servidor Nethserver, en la imagen se visualizan las alertas que el servidor muestra y las cuales se deben configurar de la manera básica que solicita para su funcionamiento, como o es establecer un dominio, cambiar el nombre que tiene por defecto de la compañía o empresa, actualizar hora y fecha, establecer si se va a realizar copias de seguridad con periodos y fechas de realización.

Se debe mirar cada una de las alertas del servidor y establecerlas según establezca la advertencia (Figura 4).

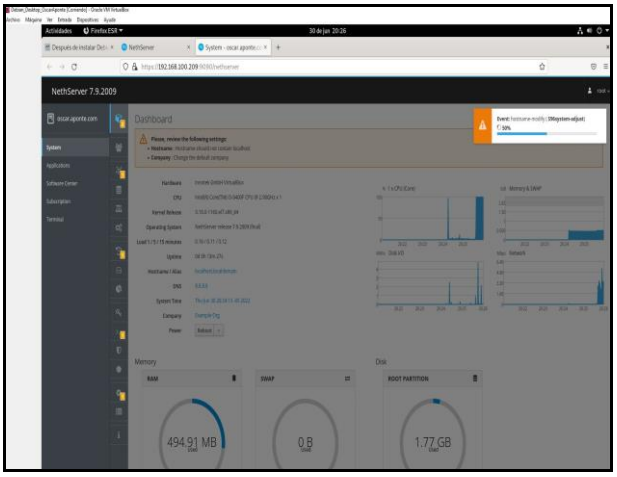

Figura 4 configurando servicios desde panel.

Quinto paso, se inicia la configuración de red para establecer los tipos de red de acuerdo con los servicios que el servidor brindará (Figura 5).

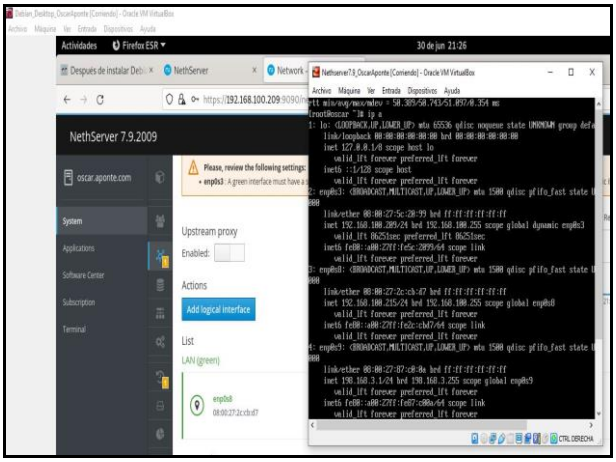

Figura 5 Configurando tarjetas de red.

En un principio se identifican y se configuran las cuatro tarjetas de red; la principal red Roja para conexión a internet, la segunda red Verde para la LAN red particular de la empresa, la tercera red Azul o clientes invitados y la cuarta red Naranja para zona DMZ zona desmilitarizada (Figura 6).

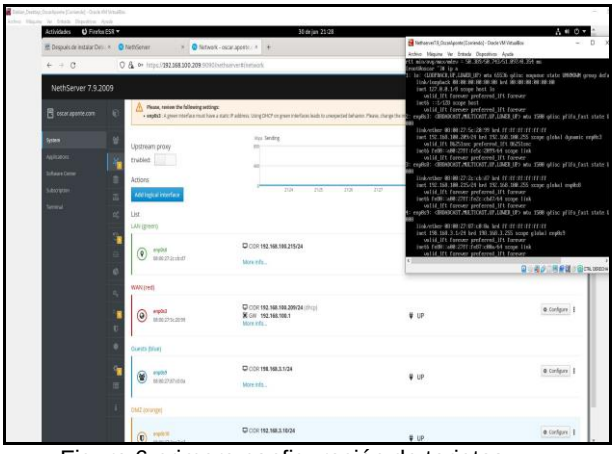

Figura 6 primera configuración de tarjetas.

Sexto paso, me enfoco entonces en acceso y control del acceso a internet de la red Verde o red LAN en la cual la empresa va a tener su mayor desempeño y por lo tanto necesita de una eficiente administración de la red y de cada uno de los accesos que pueda otorgárseles a los clientes de la LAN.

Se le suministra conexión a la red Verde activando el servidor DHCP del Nethserver y comprobando el suministro de rango de ips dinámicas y conexión establecida con equipo (Debian 11 desktop) o equipos cliente de la LAN.

Entonces, configurada la red de acceso de los clientes de la red LAN de la empresa con tarjeta de red interna GREEN o Verde, se configura en las maquinas clientes de la LAN, es decir cada maquina se conecta por una tarjeta de red en modo red interna GREEN para conectarse a la red GREEN del Nethserver (Figura 7).

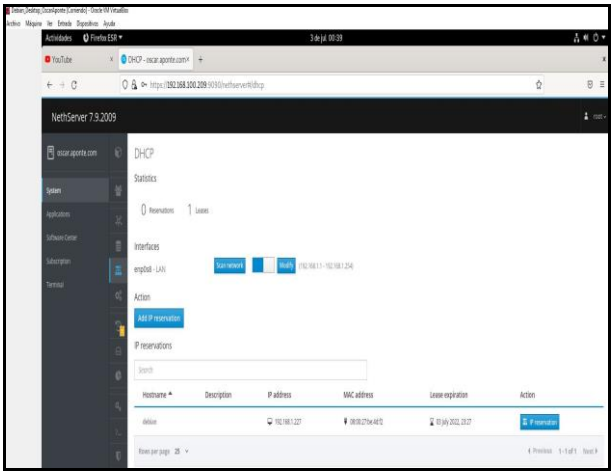

Figura 7 activación servidor DHCP.

Se comprueba conexión desde maquina cliente de red LAN a servicio de internet suministrado por el Nethserver (Figura 8 y 9).

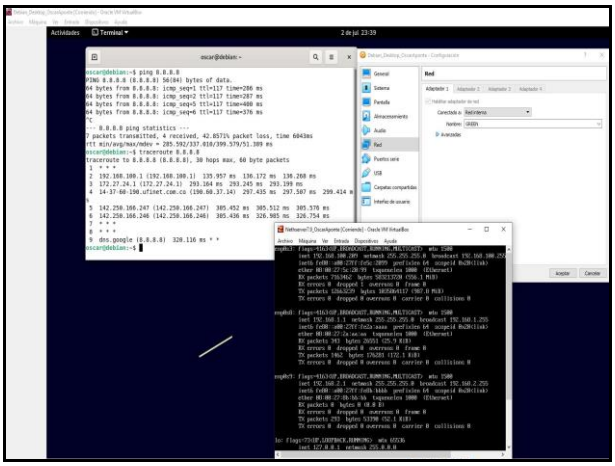

Figura 8 Conexión primer cliente.

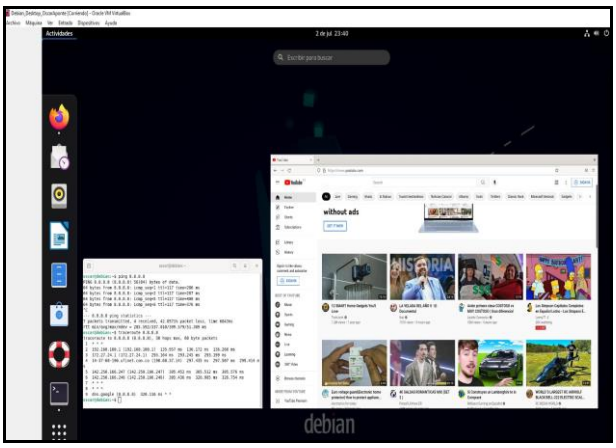

Figura 9 internet primer cliente.

Séptimo paso, se instala el web proxy y software complemento de este del “Software Center” de Nethserver, para su configuración y control del acceso por el puerto 3128 de los clientes de la red LAN (Figura 10).

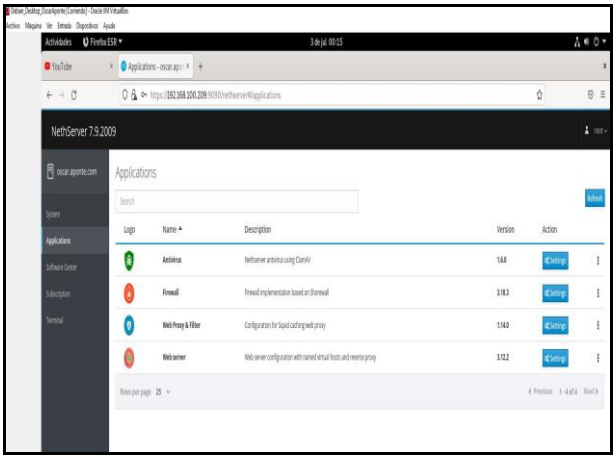

Figura 10 Instalación Proxy.

Se inicia configuración del proxy (Figura 11). Octavo paso se activa el Proxy, se establece en modo Transparente SSL mediante el cual se configura que todo el tráfico web de la LAN pase primero por el Proxy (Figura 12).

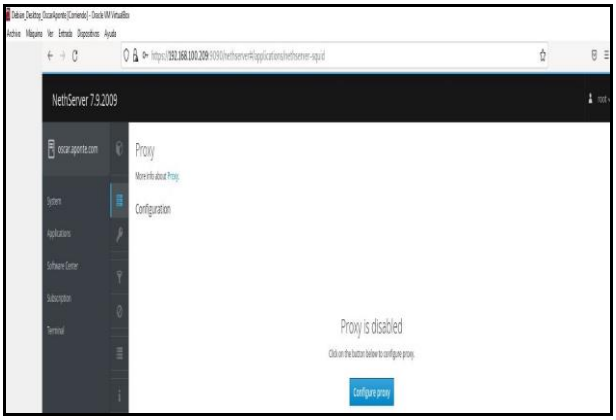

Figura 11 Activación Proxy.

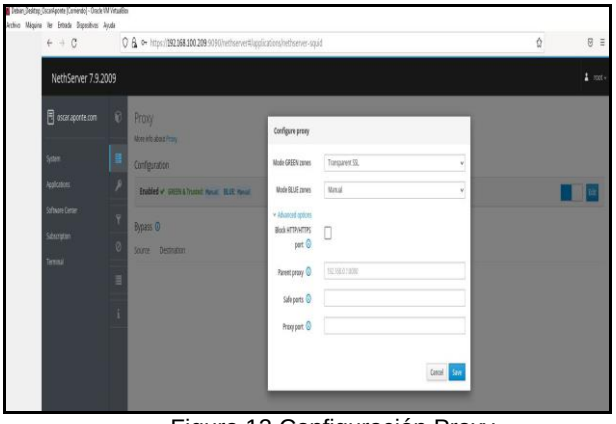

Figura 12 Configuración Proxy.

Noveno paso, se reconocen las secciones y formas de control de acceso que brinda el proxy y sus correspondientes configuraciones desde el panel del

control, se inicia la configuración del control de acceso de la red LAN a la web dentro de la sección Filter (Figura 13).

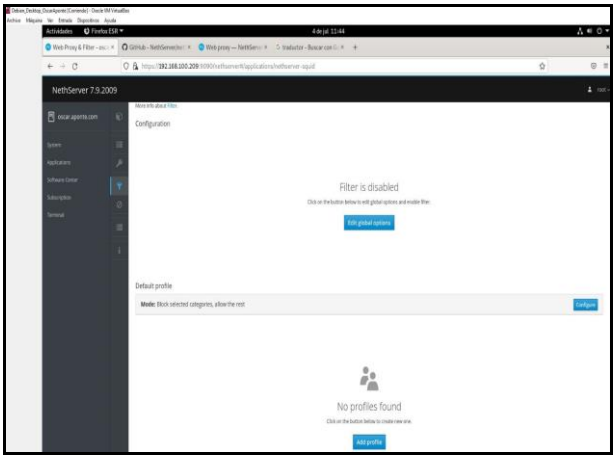

Figura 13 Módulo filter del Proxy.

Decimo paso, previamente se realiza descarga de categorías, es una lista preestablecida que permite seleccionar categorías de sitios a los que vamos a restringir o permitir el acceso según las políticas que la empresa nos dicte (Figura 14).

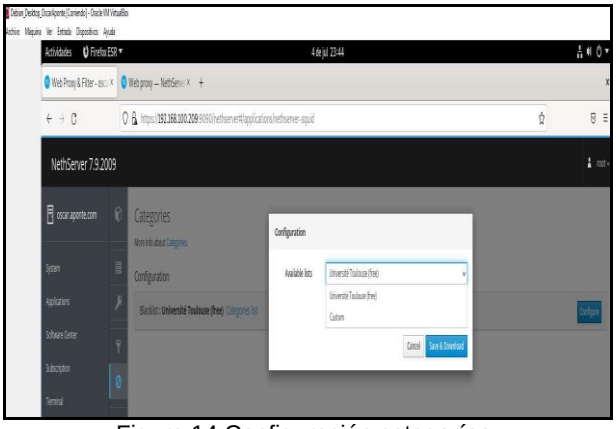

Figura 14 Configuración categorías.

Paso once, en la sección de filtro del proxy opciones globales de control de acceso se crea lista de sitios con acceso prohibido la cual esta etiquetada como lista negra o blacklist así mismo en esta opción se puede editar la lista de sitios web a los cuales vamos a establecer un acceso permitido (Figura 15).

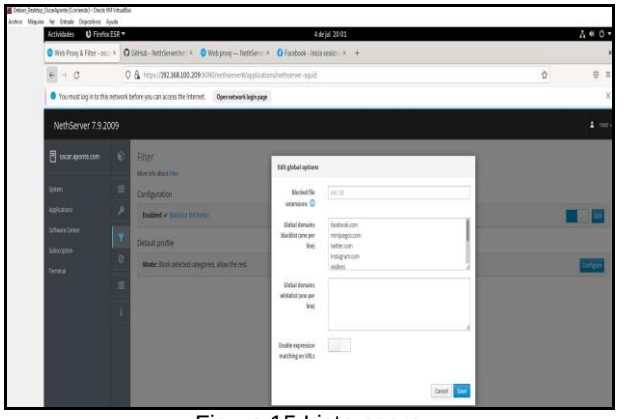

Figura 15 Lista negra

Paso doce, dentro de la sección filtro además se establece un perfil por defecto para las categorías de sitios el cual se elige siendo este “Bloquear seleccionadas permitir el resto” (figura 16).

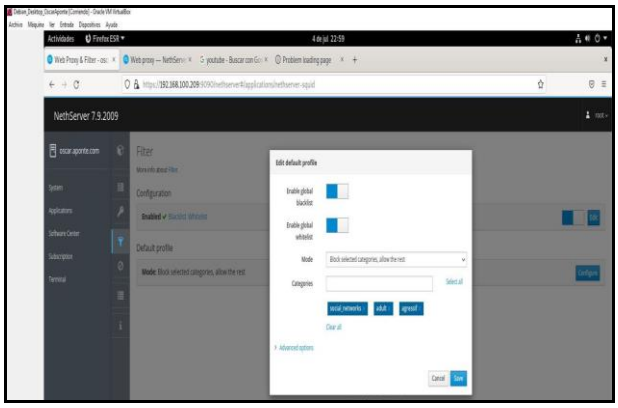

Figura 16 Perfil de filtro

Paso trece, se conecta perteneciente a la red LAN un segundo cliente, máquina virtual con sistema operativo ArchLinux la cual tiene acceso restringido a la LAN web configurado por categoría de sitios modo “permitir solo sitios seleccionados” (Figura 16).

Así mismo en el primer cliente de la LAN Debian-desktop.

Paso catorce, se establece control de acceso para red LAN por el puerto 3128 definiendo lista negra, lista blanca y categoría de sitios restringidos en modo “Bloquear seleccionadas permitir las demás” (Figura 20).

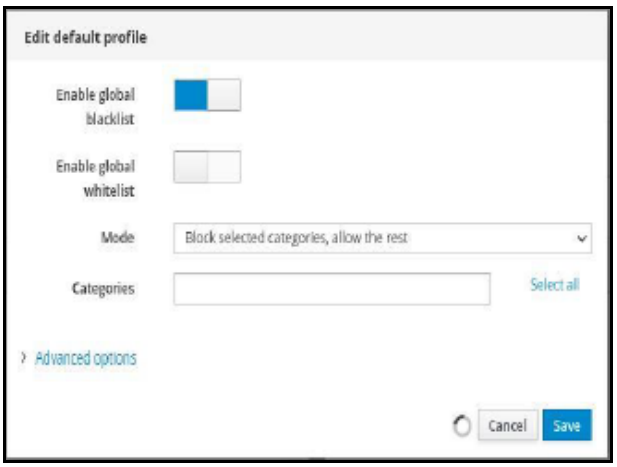

Figura 20 Modo Bloquear seleccionadas permitir las demás

Verificación en cliente ArchLinux (Figura 21). Verificación en cliente Debian-desktop ingreso a sitio web incluido en lista blanca (figura 22).

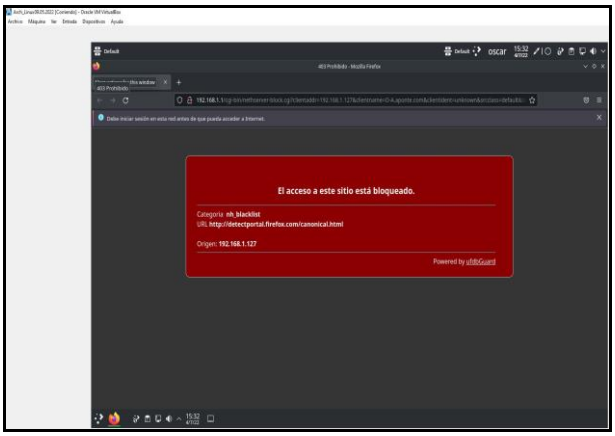

Figura 21 Acceso negado por el Proxy cliente Arch.

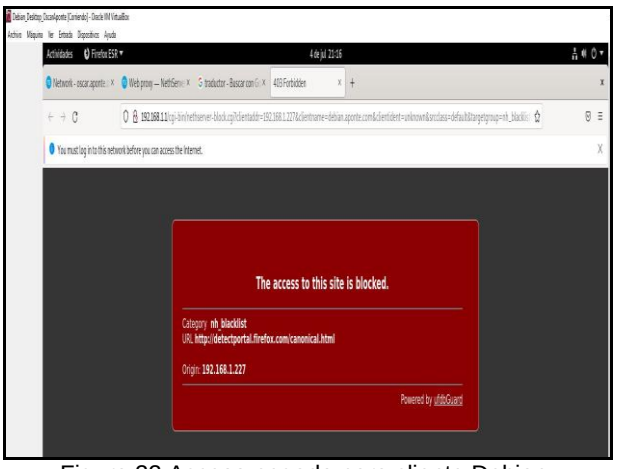

Figura 22 Acceso negado para cliente Debian.

3.2. TEMÁTICA 3: FIREWALL

Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

El filtrado de sitios web con reglas de firewall, se logra indistintamente del contenido del sitio, a diferencia de los filtrados por proxy en los que el bloqueo se da en función de la categorización de los contenidos, la restricción de tráfico por cortafuegos se fundamenta en el direccionamiento, el puerto de comunicación y el destino del tráfico por dirección ip

Con lo anterior de precedente se puede determinar que los parámetros a considerar en un filtrado por firewall son, la configuración de la red, las zonas y sentido del tráfico, el puerto y las ip destino; siendo este último parámetro uno de los más relevantes ya que se debe tener plenamente identificado el grupo de ip que apuntan al servidor que contiene el sitio web a bloquear.

Para establecer entonces la restricción a sitios web específicos por reglas de firewall, es necesario verificar la conectividad de las tarjetas de red de los equipos, respecto al servidor la configuración esperada es la definida en la Tabla 1; así mismo la ilustración en el panel de administración del servidor es la que se muestra en la Figura 23.

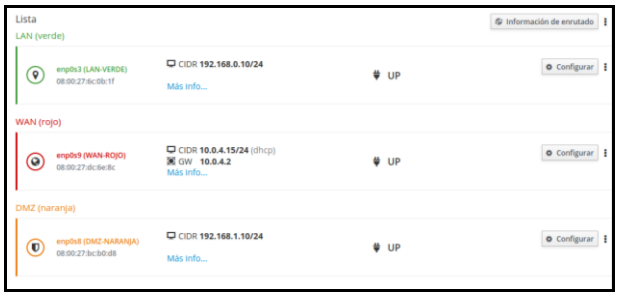

Figura 23 Configuración tarjetas de red

Respecto a los clientes, estos deben configurarse dentro de la red identificada como zona segura o VERDE de la red, usando como puerta de enlace la dirección ip del servidor que se encuentra en esta misma zona LAN, la Figura 24 ilustra un ejemplo de esta configuración

Figura 24 Configuracion red del cliente

El paso siguiente corresponde a instalar la aplicación firewall desde el gestor de aplicaciones del servidor, para esta instalación basta con identificar el paquete y dar click en el botón de instalar, el servidor procederá de forma automática a realizar la respectiva descarga e instalación del paquete; una vez terminado el proceso la aplicación estará disponible en el módulo de aplicaciones del panel de control, ver Figuras 25 y 26

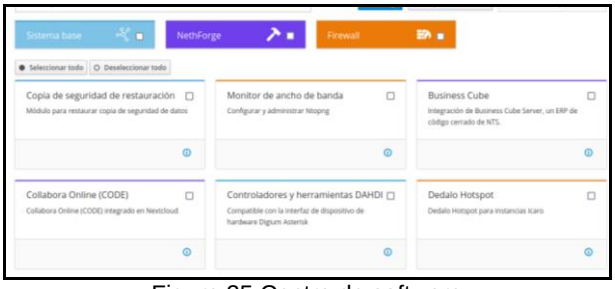

Figura 25 Centro de software

Figura 26 Aplicaciones instaladas

Ya con la aplicación firewall instalada se accede a su configuración con el botón a la derecha; Este módulo permite acceder al panel firewall, en el campo inicial el panel muestra una ilustración de la configuración de la red y su topología, este diagrama debe reflejar una configuración que evidencie el dispositivo firewall como un filtro entre las redes locales y la red Wan o de acceso a internet, Ver Figura 27

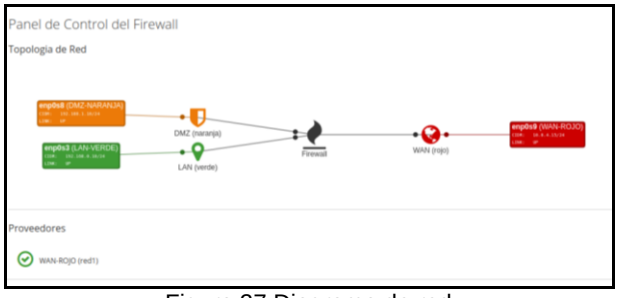

Figura 27 Diagrama de red

Verificado el diagrama de la topología de la red, se be verificar que este habilitado el tráfico hacia internet y el ping desde internet, esto se puede verificar y activar en el panel de ajustes, dentro del apartado firewall, con estas opciones activas ya se cuenta con el firewall activo y con un tráfico hacia internet desde los equipos clientes, este tráfico aun no está filtrado por lo que se podrá navegar libremente, Ver Figura 28

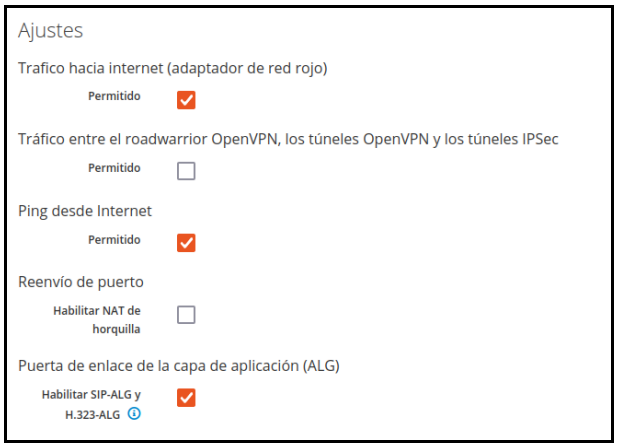

Figura 28 Ajustes firewall

A partir de este punto ya se cuenta con una base para iniciar con el proceso de control del tráfico en la red, este control se logra por medio de la implementación de reglas, estas se acceden en el módulo de *REGLAS* en el apartado de firewall

Las reglas son un conjunto de instrucciones que le indican al servidor que tipo de conexiones son permitidas y cuales son rechazadas, en esencia las reglas operan identificando el origen de la solicitud, el destino, el puerto y la acción a tomar, el siguiente ejemplo puede ilustrar el concepto

Tabla 2

ITEM	DATO
ORIGEN	192.168.0.10
DESTINO	ZONA ROJA
PUERTOS	21
ACCIÓN	RECHAZAR

El ejemplo anterior se traduce en una regla que bloquea las solicitudes hechas desde el cliente identificado con la ip 192.168.0.10 con destino a la zona roja, es decir la WAN o internet y que generan tráfico por

el puerto 21, en otras palabras, el host 192.168.0.10 no podrá conectarse vía ftp a ningún host que este fuera de su red local.

Bajo este mismo principio y como un segundo ejemplo una regla que nos permitiría bloquear la navegación desde un equipo cliente tendría la siguiente estructura

Tabla 3

ÍTEM	DATO
ORIGEN	192.168.0.10
DESTINO	ZONA ROJA
PUERTOS	80, 443, 980
ACCIÓN	RECHAZAR

La regla anterior rechaza toda solicitud hecha por el host 192.168.0.10 hacia la WAN por los puertos de navegación, http, https y TCP, con esto el host no podrá navegar en internet. Ver figura 29

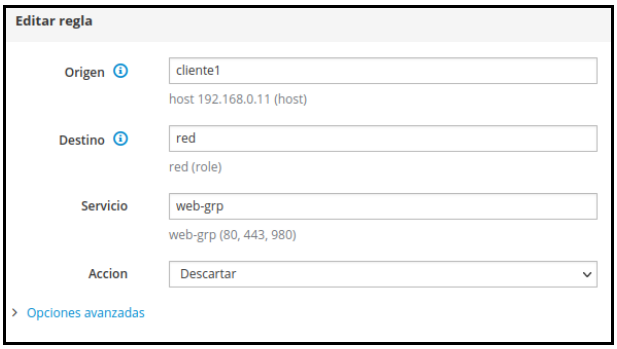

Figura 29 Regla que bloquea la navegación en un cliente

Otro aspecto a considerar en la creación de reglas es la posibilidad que ofrece el módulo de firewall de Nethserver de crear OBJETOS, estos objetos corresponden a la identificación de elementos o grupo de elementos sujetos a las reglas que se creen, una forma de entender el concepto es asumir el caso en el que se requiere crear una regla para bloquear el tráfico de 5 máquinas host, una alternativa es crear 5 reglas una para cada origen, no obstante si creamos un objeto que agrupe estas 5 ip, bastaría con crear una sola regla y determinar en el origen el grupo creado que contiene estas 5 direcciones ip o host; así las cosas gracias a la creación de objetos se pueden categorizar zonas (Verde, Naranja, Azul, Roja) crear un host, grupos de host, rangos de ip, entre otros. Estos objetos son aplicables tanto para los orígenes como para los destinos.

Con lo anterior en mente podemos llegar a la conclusión de que el método para bloquear el acceso a paginas especificas requiere de la creación de una regla que bloquee las solicitudes a las ip de las páginas a restringir desde el equipo cliente; por lo tanto, es necesario conocer la ip de las páginas objeto de filtrado, en este ejercicio se realizó el procedimiento aplicado a la red social INSTAGRAM.

Para conocer la ip de instragram se ejecutó desde la terminal el comando ping al dominio instagram.com, obteniendo como resultado la ip 157.240.6.18, ver Figura 30

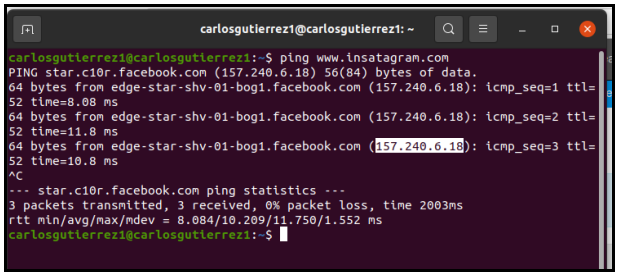

Figura 30 Resultados de ping a instagram.com

Lo siguiente es determinar el rango de ip asociadas a este servidor web, naturalmente se sabe que los rangos van de la ip 1 a la 255, no obstante, es favorable confirmarlo mediante la consulta al servicio whois, este servicio se encuentra de forma gratuita en la internet, en este caso se consultó en el portal who.is, y los resultados identifican el rango 157.240.0.0 a 157.240.255.255, ver Figura 31

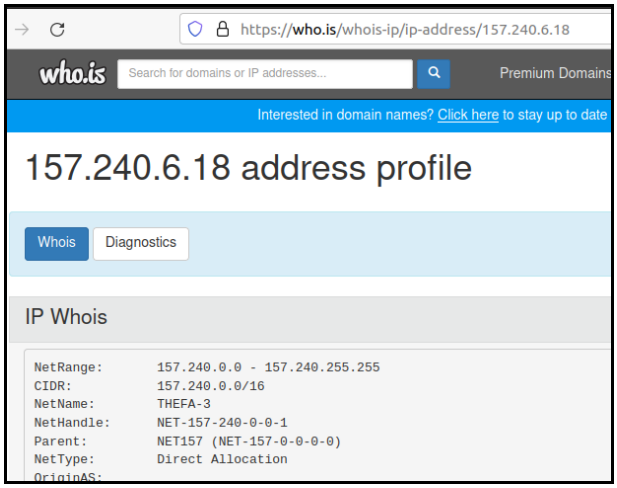

Figura 31 Resultado consulta who.is

Con esta información podemos crear un objeto administrable en el firewall que corresponda al rango de ip identificado en el paso anterior, Ver figuras 32 y 33

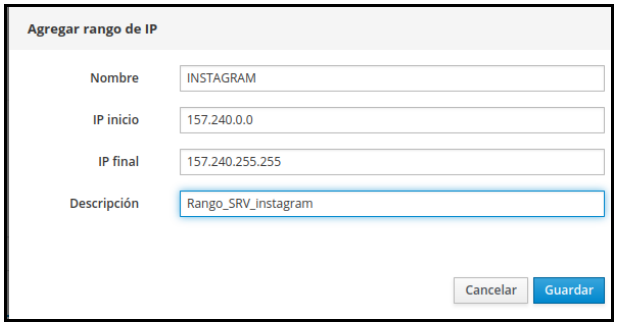

Figura 32 Creación de objeto INSTAGRAM por rango de ip

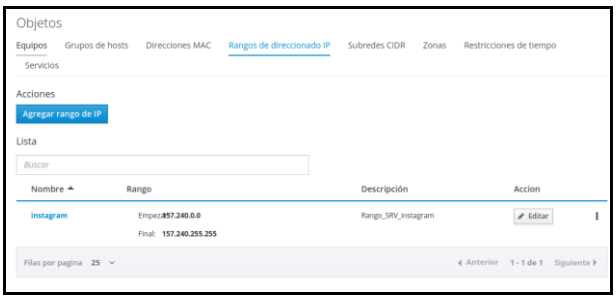

Figura 33 Objeto creado

Finalmente se creó la regla que bloquea las solicitudes por los puertos de navegación (80,443,980) desde el host cliente 1 (192.168.0.11) hacia el objeto ISTAGRAM (rango de ip), Ver Figuras 34 y 35

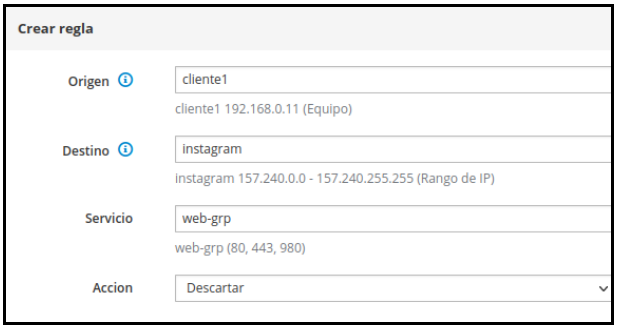

Figura 34 Regla para bloquear instragram

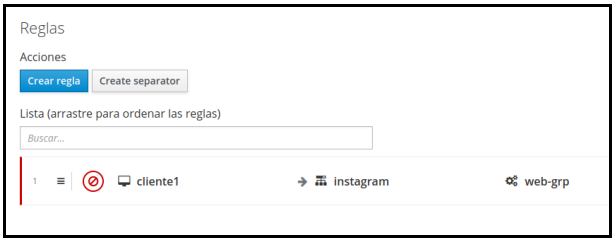

Figura 35 Regla creada y activa

Con la regla en ejecución, se pudo verificar el bloqueo al sitio INSTAGRAM, la prueba final correspondió a la navegación desde el equipo cliente evidenciando que se pudo acceder a Hotmail.com y otros portales, sin embargo, al tratar de ingresar a instragram.com el navegador no resolvió la solicitud y en consecuencia no se accedió al sitio web.

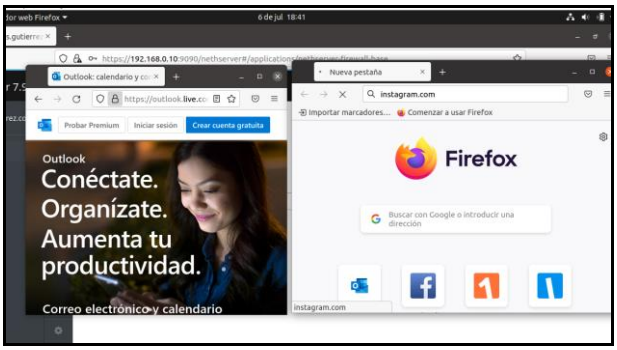

Figura 36 Prueba de la regla

Finalmente, para bloquear otros portales basta con replicar los pasos anteriormente descritos identificando previamente la dirección ip o rango de ip asociadas al portal que se desee restringir.

4. CONCLUSIONES.

Temática: Proxi, establecer una conexión estable y segura para la red privada LAN resulta ser de valiosa utilidad y necesidad para la empresa, sobre todo tener el control del tráfico web enfocándolo a los objetivos puntuales plasmados en la misión y visión de la empresa, es fundamental para su eficiencia y productividad

Temática: Firewall, El firewall de un servidor constituye la primera línea de defensa contra instrucciones en nuestra red local, así mismo constituye un elemento de gerencia de recursos que permite administrar las conexiones de nuestros usuarios autorizados; en este sentido la formulación asertiva de reglas de control de trafico no solo operan como componentes de seguridad si no también de eficiencia en los recursos de la red

5. REFERENCIAS

[1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, *"A globally convergent estimator for n frequencies"*, IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.

[2] H. Khalil, *"Nonlinear Systems"*, 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.

[3] Francis. B. A. and W. M. Wonham, *"The internal model principle of control theory"*, Automatica. Vol. 12. pp. 457-465. 1976.

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.

[7] Nethserver. (s. f.). Web proxy — NethServer 7 Final. Nethserver.Org. Recuperado 6 de julio de 2022, de https://docs.nethserver.org/en/v7/web_proxy.html

[8] Netserver. (s. f.). Firewall — NethServer 7 Final. Nethserver.Org. Recuperado 6 de julio de 2022, de https://docs.nethserver.org/en/v7/firewall.html