

IMPLEMENTACION Y GESTION DE SERVICIOS DENTRO DE INFRAESTRUCTURA IT CON ENFASIS EN NETHSERVER

Diana Patricia Tacuma Rivera
dptacumar@unadvirtual.edu.co

Jorge Enrique Calvo Ceballos
jecalvoc@unadvirtual.edu.co

RESUMEN: Este artículo demuestra las configuraciones necesarias para la interfaz de usuarios y escritorios con los servicios propios de la herramienta NethServer y VirtualBox donde se crean máquinas virtuales con requerimientos específicos en la red para su correcta conexión, se detalla el proceso de instalación del sistema operativo con las pautas básicas para ejecutar un nivel de seguridad apropiado para el cliente por medio del control de las distribuciones de Linux Ubuntu y los servicios de infraestructura IT.

Se identifican las redes administrables para acceder a NethServer y se implementan los servicios DHCP, DNS y Controlador de dominio en la estación de trabajo, controlando su acceso y conectividad a internet por medio del proxy, además se restringen algunos sitios web y se valida el funcionamiento del cortafuegos.

PALABRAS CLAVE: Cortafuegos, DHCP, DNS, Proxy, VPN, Seguridad.

1. INTRODUCCIÓN

En el ámbito donde se administran sistemas operativos, la debida configuración y la apropiada gestión de estaciones de trabajo implementadas bajo el sistema GNU/Linux se conciben de gran importancia dada su alta relevancia en términos de garantizar seguridad, eficiencia y conectividad en los entornos de tipo empresarial. Estos conjuntos de tareas de carácter administrativo no solo se ven enfocadas en términos de optimización de escritorios de usuario, sino que además, se busca abordar aspectos esenciales tales como, el control del acceso al sistema, la implementación de servicios de red, e igualmente la aplicación de políticas de seguridad.

Mediante la implementación de conjuntos de medidas de seguridad se busca abordar el campo de la restricción web mediante el uso de un cortafuegos. Limitando entonces el acceso a este tipo de sitios mediante la aplicación de un conjunto de reglas y políticas que se establecen dentro del sistema Firewall, logrando así condicionar el tráfico web del usuario.

Esta serie de procesos integrales busca que se desarrollen las habilidades necesarias para lograr no solo la eficiencia operativa, sino también la robustez y seguridad de los sistemas GNU/Linux en entornos empresariales, proporcionando a los

administradores las herramientas necesarias para enfrentar los desafíos contemporáneos en la administración de la infraestructura de TI.

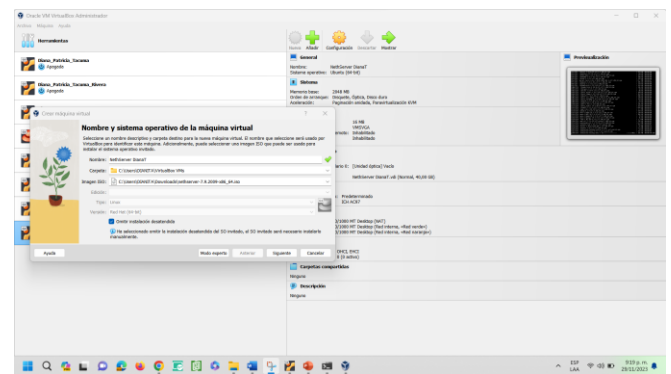
2. DESARROLLO DE LAS TEMÁTICAS

2.1 IMPLEMENTACION DE DHCP SERVER, DNS SERVER Y CONTROLADORES DE DOMINIO

Para el proceso de instalación del NethServer es necesario descargar la imagen ISO del sistema operativo con la versión más reciente, este software se configura creando una máquina virtual en la herramienta de VirtualBox y asignándole tres interfaces de red (zona verde, naranja y roja) las cuales se van a conectar a un equipo Desktop y un servidor web.

A su vez, se crea el equipo Desktop con el sistema operativo Ubuntu y se le asigna la interfaz de red verde.

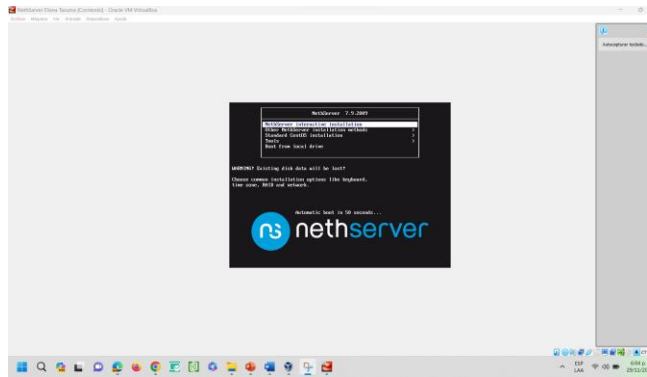
Figura 1. Configuración de la máquina virtual



Fuente: Autoría Propia

Inicio el proceso de instalación del NethServer, el cual por medio de la interfaz gráfica facilita que su configuración sea rápida y específica en los requerimientos base de la distribución.

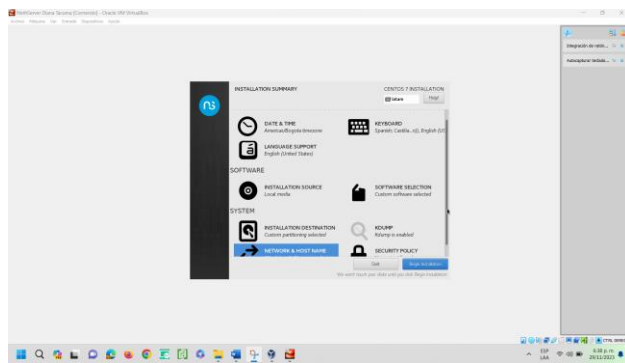
Figura 2. Interfaz de arranque NethServer



Fuente: Autoría Propia

El software permite modificar la fecha, hora, área o ubicación, teclado y las tarjetas de red que se crean al instalar la máquina virtual para el NethServer. Apenas se configura se da clic en el botón de iniciar instalación.

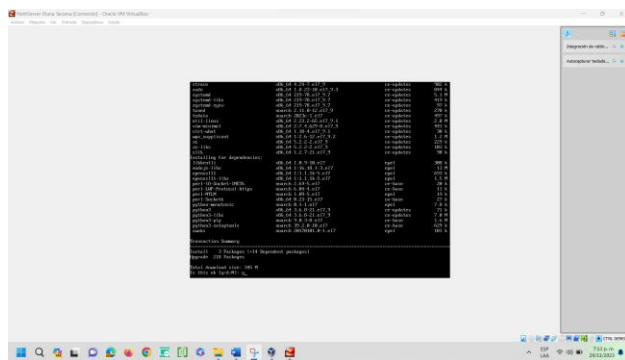
Figura 3. Configuración previa a la instalación



Fuente: Autoría Propia

Mientras se realiza la instalación de los paquetes y librerías, aparece la opción para asignar la clave del root. Al finalizar la instalación es importante reiniciar la máquina virtual y comprobar la conexión a internet, así mismo actualizar el servidor para verificar las actualizaciones que requiere el sistema y validar la IP con la que se tiene acceso al NethServer desde el navegador de internet.

Figura 4. Actualización de paquetes

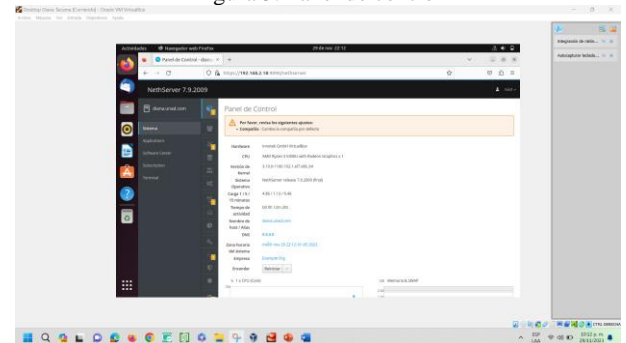


Fuente: Autoría Propia

Al iniciar de nuevo la máquina virtual se debe ingresar al navegador con la dirección IP consultada, aceptar los riesgos

que muestra el explorador e ingresar el usuario y contraseña del NethServer, la primera imagen que se evidencia al ingresar es el panel del control donde configuramos la información de la empresa y los servidores DNS.

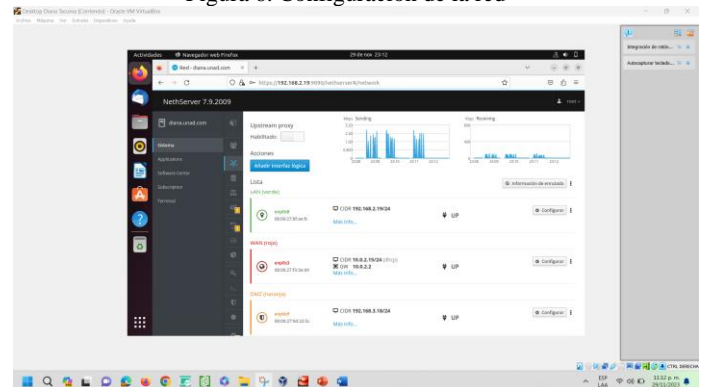
Figura 5. Panel de control



Fuente: Autoría Propia

En la opción Shell Seguro – SSH se cambia el puerto TCP a 2222 y al dar clic en Red se modifica el rol de la interfaz dejando para el DHCP el WAN rojo, la red LAN verde estática donde se añade la dirección IP del NethServer y el DMZ naranja con su respectiva dirección IP. Esta actualización también se puede consultar en la consola.

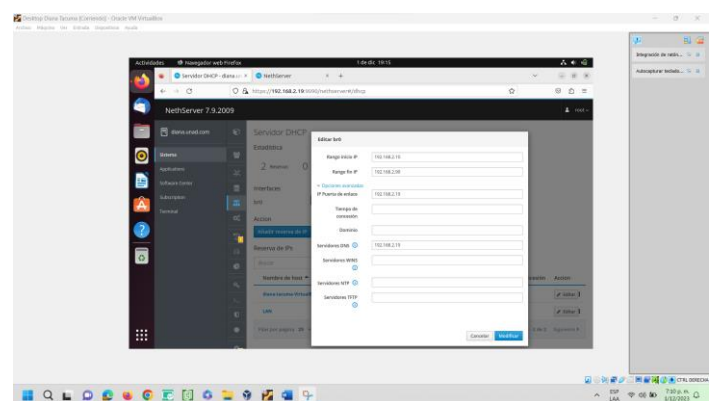
Figura 6. Configuración de la red



Fuente: Autoría Propia

La opción del servidor DHCP permite escanear la red LAN y modificar sus rangos, puerta de enlace y servidores DNS.

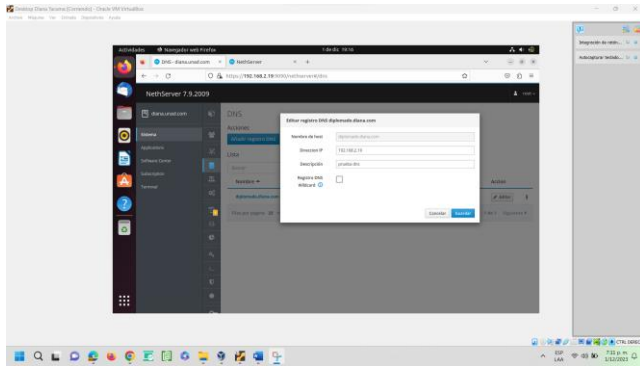
Figura 7. Configuración del DHCP



Fuente: Autoría Propia

Para configurar el DNS se añade un registro que permite asignar el nombre del host, la dirección IP que debe coincidir con la del NethServer o el sitio web a consultar y una breve descripción, apenas se guardan los cambios se comprueba en el explorador de internet escribiendo el nombre del host.

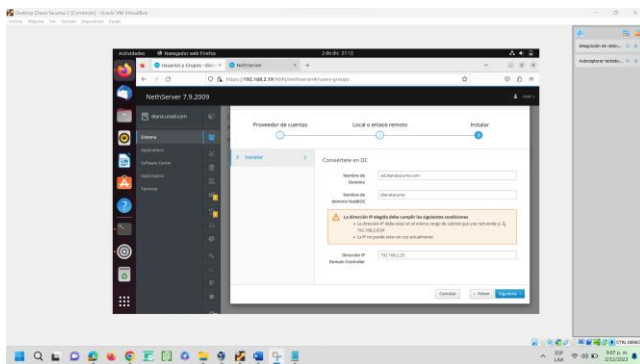
Figura 8. Configuración del DNS



Fuente: Autoría Propia

En la opción de usuarios y grupos se crea el dominio por medio del Active Directory asignando el nombre del dominio, nombre del NetBios y una dirección IP que se encuentre dentro de los rangos de la red LAN y sin utilización. En paralelo la red LAN se integra con el dominio creado y se percibe porque cambia el nombre a br0, indicando que ahora es un adaptador puente que contiene las dos direcciones IP, tanto la estática como la de dominio.

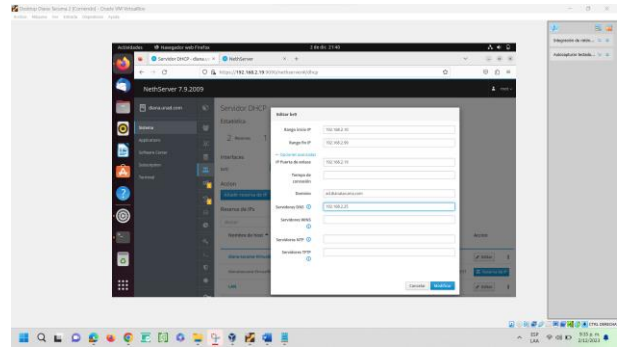
Figura 9. Active Directory Local



Fuente: Autoría Propia

Después de realizar los ajustes del Active Directory, es necesario ingresar a la opción del servidor DHCP para registrar el nombre del dominio creado y la dirección del servidor DNS

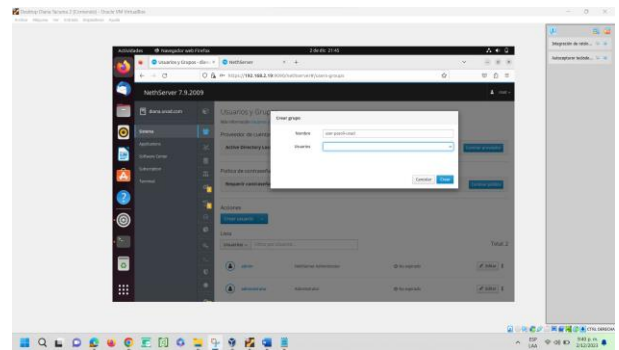
Figura 10. Actualización del DHCP



Fuente: Autoría Propia

En la opción de usuarios y grupos aparecen las cuentas de admin y administrador bloqueadas, por lo cual se les debe cambiar la contraseña para que se habiliten nuevamente. Después de hacer este proceso se despliegan las acciones y se elige crear un grupo.

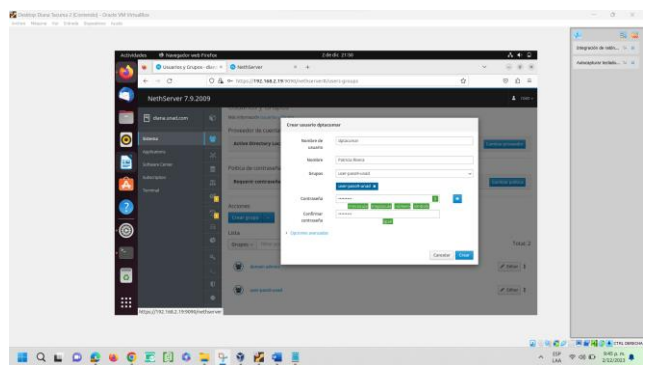
Figura 11. Crear un grupo



Fuente: Autoría Propia

Se despliega la acción para crear un usuario y se consigna el nombre de usuario, nombre, grupo y contraseña.

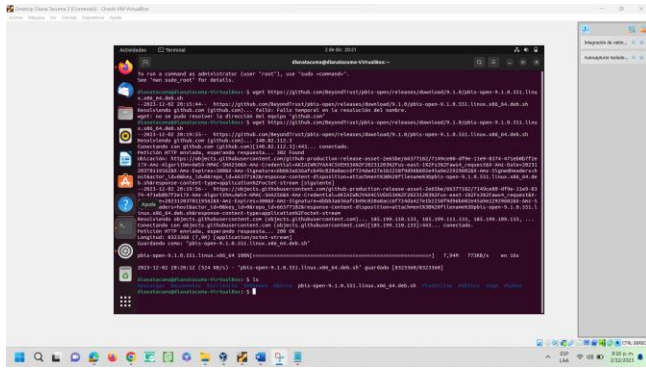
Figura 12. Crear un usuario



Fuente: Autoría Propia

Para continuar con el controlador del dominio se debe descargar el script pbis-open-9.1.0.551.linux.x86_64.deb.sh en el equipo desktop, para ello se utiliza el comando wget y se cambian los permisos de ejecución para el usuario propietario con chmod.

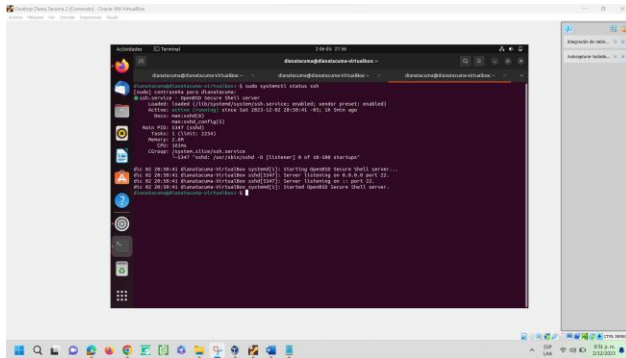
Figura 13. Descarga del Script



Fuente: Autoría Propia

Se instala openssh-server y se actualiza con el comando upgrade y update para que no genere error, por último se verifica que el servicio este activo.

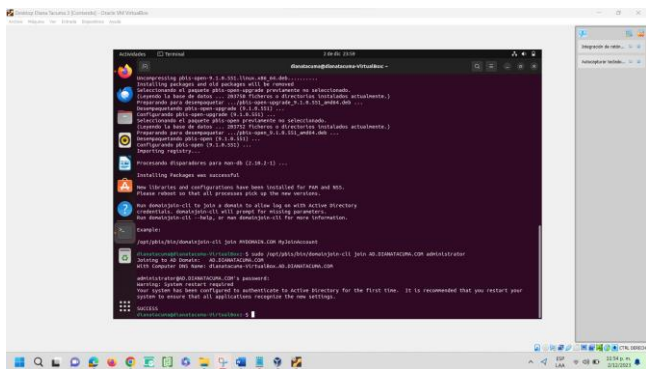
Figura 14. Status de SSH



Fuente: Autoría Propia

Se ejecuta en la consola el paquete del script descargado para preparar el vínculo del equipo desktop al dominio, para ello se ingresa como root y se modifica el dominio de la cuenta administrator. Se reinicia la máquina para actualizar los cambios.

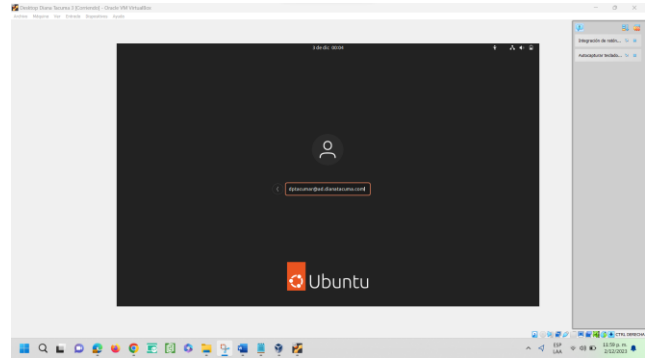
Figura 15. Vínculo del dominio



Fuente: Autoría Propia

Al arrancar la máquina se da clic en la opción ¿no está en la lista? Y se ingresa el usuario creado con la respectiva clave, de esta manera se logra acceder al escritorio Ubuntu con los permisos asignados para el cliente.

Figura 16. Vínculo del dominio

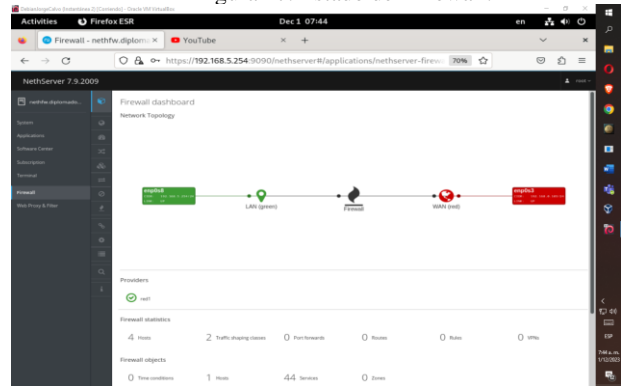


Fuente: Autoría Propia

2.2 IMPLEMENTACIÓN Y GESTIÓN DE CORTAFUEGOS

Teniendo configurada nuestra red base previamente, se configura el software pertinente para el bloqueo de acceso a servicios y dominios Web, el Firewall.

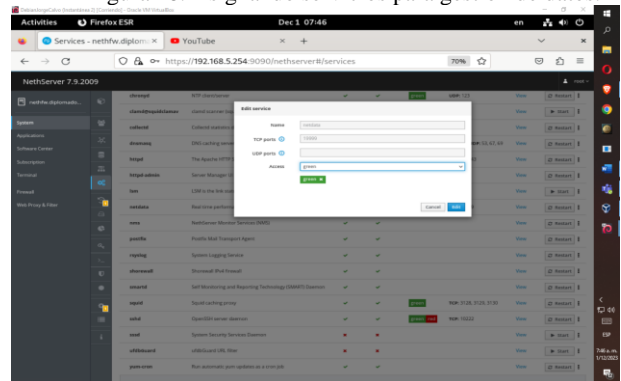
Figura 17. Estado del Firewall.



Fuente. Autoría propia. 2023.

Se verifica el estado actual del Firewall y su funcionamiento.

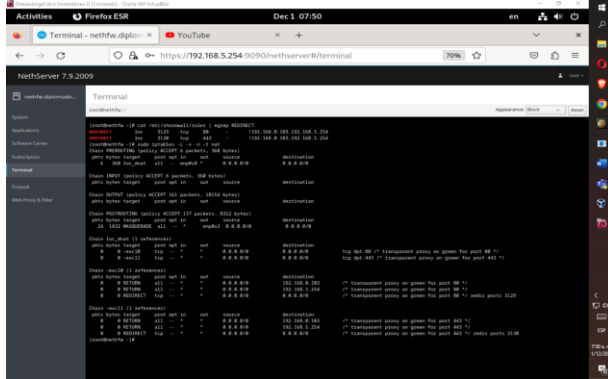
Figura 18. Asignando servicios para gestión de datos.



Fuente. Autoría propia. 2023

Se asigna el servicio netdata a green para obtener datos en tiempo real en el firewall

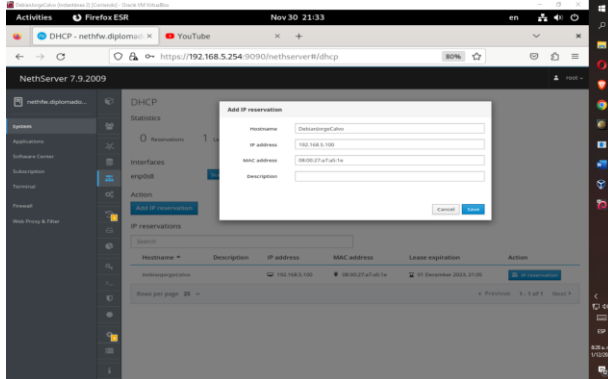
Figura 19. Verificamos servicio de redirección.



Fuente. Autoría Propia. 2023

Se verifica que shorewall está redireccionando adecuadamente los datos en el firewall, permitiendo así filtrar las páginas web a futuro.

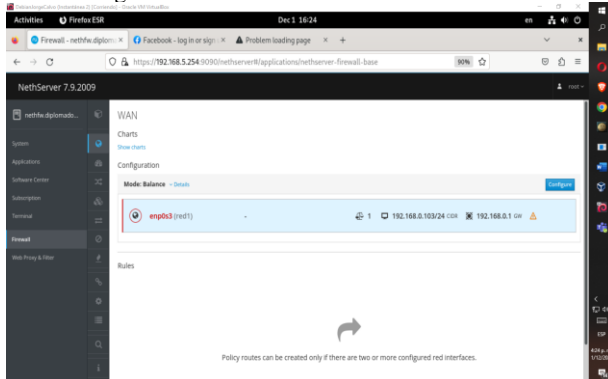
Figura 20. Asignación de Red MAC



Fuente. Autoría Propia. 2023.

Se revisa la asignación de dirección MAC que se ha dado al asignar servicios e implementar las reglas de redireccionamiento.

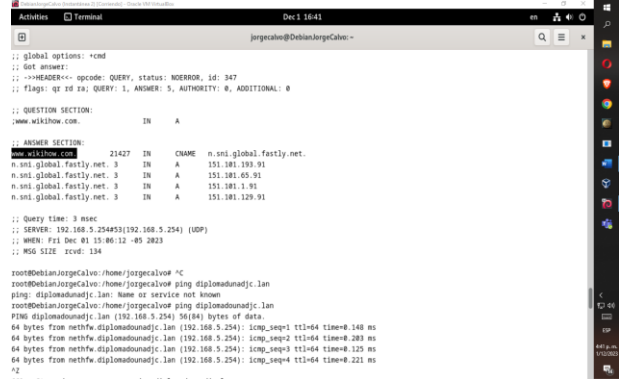
Figura 21. Estado de red WAN dentro de Firewall.



Fuente. Autoría propia. 2023

Se comprueba dentro del Firewall la configuración de red WAN y su implementación.

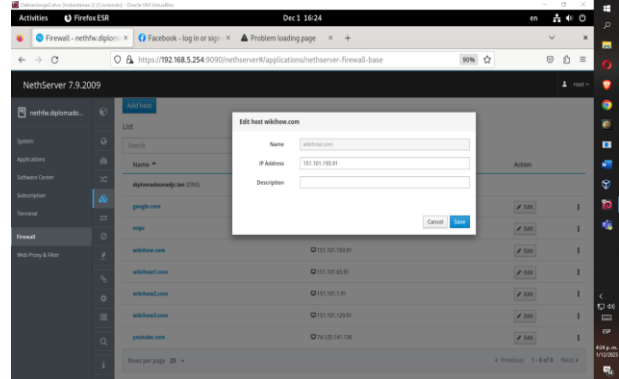
Figura 22. Obteniendo direcciones de dominios web.



Fuente. Autoría propia. 2023

Tendrá que emplearse el comando dig en la terminal, para solicitar las direcciones IP respectivas a los dominios web para aplicarlas en nuestros filtros.

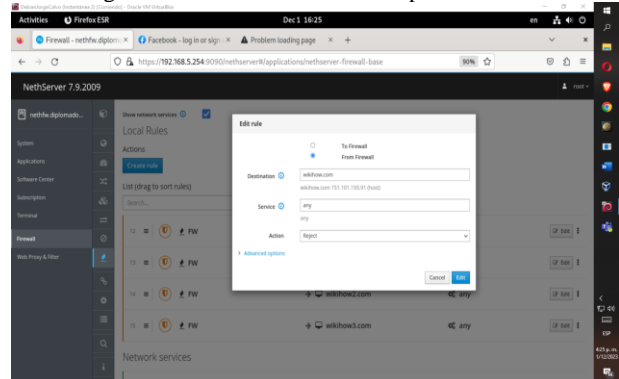
Figura 23. Creando registro Host de IP dominio.



Fuente. Autoría propia. 2023

Se debe agregar los grupos de direcciones IP como hosts dentro de las políticas del firewall.

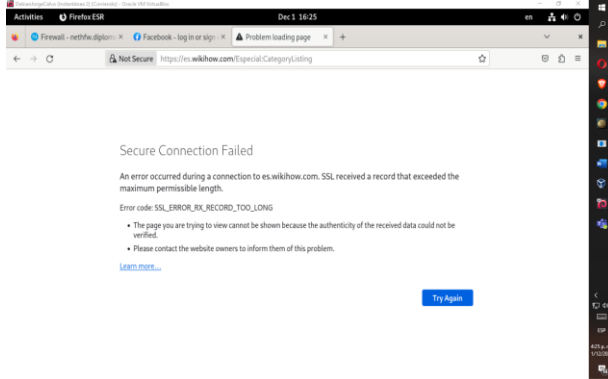
Figura 24. Definiendo a donde impedir el acceso web.



Fuente. Autoría propia. 2023

Se define la regla con la que el firewall detendrá accesos a la dirección Host que determinamos en pasos anteriores.

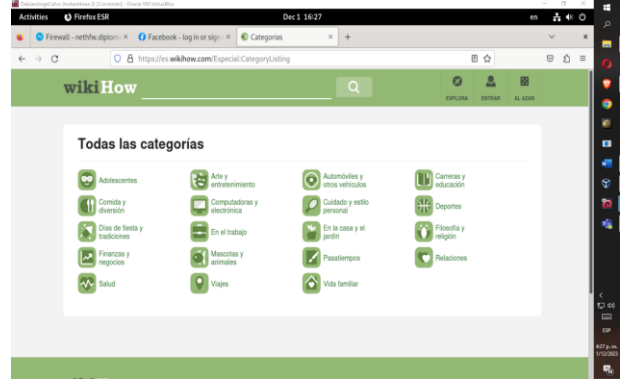
Figura 25. Prueba de restricción web.



Fuente. Autoría propia. 2023

Se comprueba el funcionamiento del Firewall al probar que la conexión a la página está restringida.

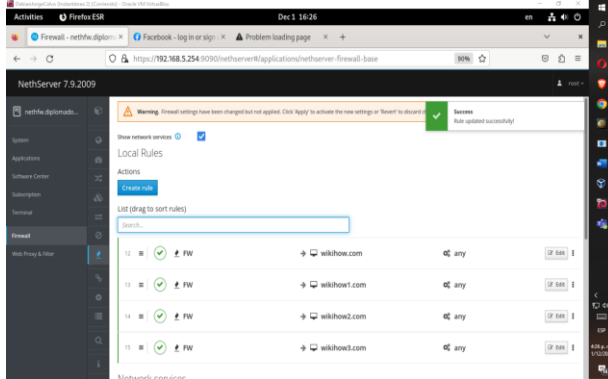
Figura 28. Comprobando acceso al dominio Web.



Fuente. Autoría propia. 2023

Mediante el ingreso a la página Web, podemos verificar que la regla ahora permite el acceso a la web.

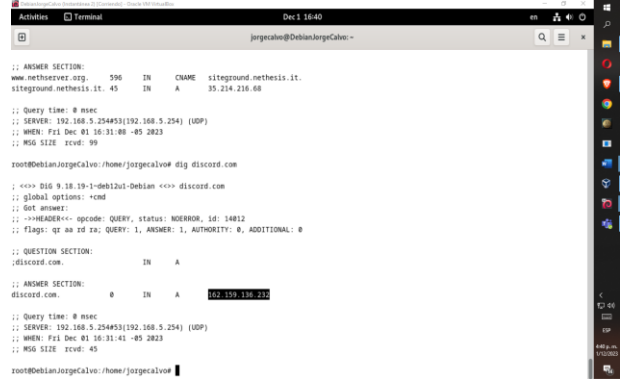
Figura 26. Invertimos el estado de la regla.



Fuente. Autoría propia. 2023

Se invierte el estado de la regla, para así verificar que no haya sido problema de red y comprobar el funcionamiento del Firewall.

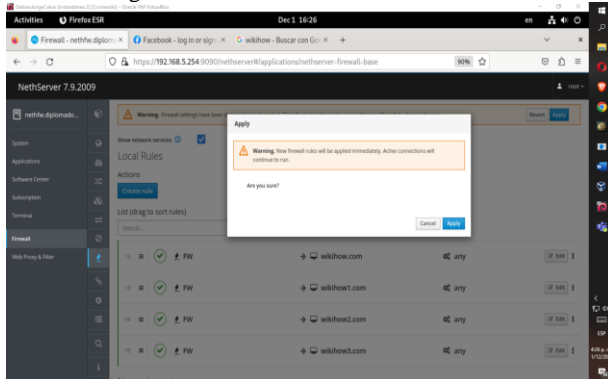
Figura 29. Obteniendo una nueva dirección Web.



Fuente. Autoría propia. 2023

En este caso, vamos a obtener la dirección del dominio web de una red social, comprobando así nuevamente el funcionamiento del Firewall.

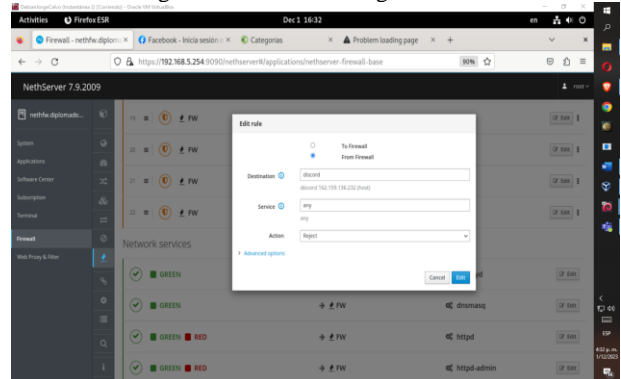
Figura 27. Se confirman cambios en el firewall.



Fuente. Autoría propia. 2023

Damos aplicar para confirmar que estos cambios se apliquen correctamente al Firewall y sus reglas.

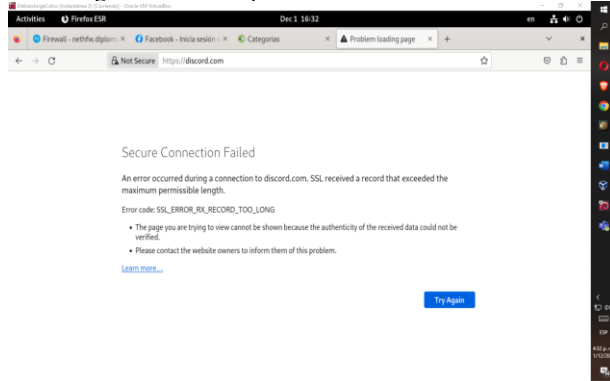
Figura 30. Creamos la regla en el Firewall.



Fuente. Autoría propia. 2023

Asignamos el conjunto de configuraciones necesarias para configurar la regla correspondiente que limite el acceso al dominio web de la Red Social.

Figura 31. Se comprueba la limitación del acceso Web.



Fuente. Autoría propia. 2023

Por último, mediante una nueva prueba, verificamos que funciona la regla asignada y bloquea el acceso a la web de esta red social, comprobando así que los filtros Firewall implementados están funcionando correctamente.

CONCLUSIONES

Se logró la implementación exitosa del servidor NethServer, representando así una base sólida sobre la que desarrollar las políticas y protocolos de seguridad para la red que se requería, permitiendo así desarrollar las actividades en una infraestructura de fiar y versátil para diversas funciones, tales como gestionar una impresora, administrar el tráfico de red, emplear los servicios de una VPN o utilizar un gestor de archivos.

Además, la implementación de políticas y reglas específicas de red para de esta forma lograr efectivamente la restricción al acceso de sitios web de entretenimiento y redes sociales, nos permite poner en práctica la funcionalidad del firewall de forma completa, permitiéndonos también identificar mecanismos para obtener las direcciones de red para diversas páginas web y sus debidos dominios o rangos de IP, de esta forma manteniendo un control preciso sobre el tráfico de red y alineado con los objetivos previamente establecidos.

REFERENCIAS

- LPI LPIC-1 Exam 102. (2022). Tema 109: Fundamentos de redes. <https://learning.lpi.org/es/learning-materials/102-500/109/>
- Canonical (2018). Guía del Ubuntu desktop 18.04 LTS. Help Ubuntu. <https://help.ubuntu.com/18.04/ubuntu-help/index.html>
- Debian (2020). El manual del administrador de Debian 10.04. Debian <https://www.debian.org/doc/manuals/debian-handbook/index.es.html>
- Nethesis, S. (2023b) Installation, Installation - NethServer 7 Final. Disponible en: <https://docs.nethserver.org/en/v7/installation.html> (Accedido: 01 Diciembre 2023).
- Nethesis, S. (2023) Firewall, Firewall - NethServer 7 Final. Disponible en: <https://docs.nethserver.org/en/v7/firewall.html> (Accedido: 01 Diciembre 2023).