IMPLEMENTACIÓN DE SERVICIOS DE SEGURIDAD EN NETHSERVER

Francisco Javier Cortes Pérez
e-mail: fjcortesp@unadvirtual.edu.co
Freddy Alexander Vera Hernández
e-mail: faverah@unadvirtual.edu.co
Hernán León Coy
e-mail: hleonc@unadvirtual.edu.co
Jonny Hernández González
e-mail: jhernandezgonzale@unadvirtual.edu.co

RESUMEN: *El siguiente trabajo muestra el desarrollo practico de una solución tecnológica en donde se busca migrar a una solución de TI (Tecnologías de la Información) basada en código abierto. En particular, se detalla el proceso de implementación de un servidor con el aplicativo NethServer a través del cual, se implementan los siguientes servicios de red, como son DHCP, DNS, Controlador de dominio, Proxy, Corta Fuegos, Servidor de Archivos e Impresión y VPN.*

PALABRAS CLAVE: NethServer, DHCP, DNS, Controlador de dominio, Proxy, Cortafuegos, Servidor de Archivos e Impresión, VPN, Código Abierto.

1 INTRODUCCIÓN

En el mundo empresarial las soluciones tecnológicas juegan un papel relevante, ya que, no solo imprimen modernidad y eficiencia, sino que también implican reducción de costos y aumento de productividad.

Las soluciones propuestas en este trabajo buscan liberar a una empresa del pago de licenciamiento y/o suscripción por el uso soluciones tecnológicas que facilitan la comunicación interorganizacional en una empresa pequeña o mediana que está en busca de implementar soluciones robustas con software construido con código libre

El trabajo detalla cómo podrían implementarse soluciones de código abierto para ofrecer servicios de red como DHCP, DNS, Controlador de dominio, Proxy, Cortafuegos, Servidor de Archivos e Impresión y VPN, los pasos y detalles de implementación y los recursos e información requerida para dar solución a una empresa que desea no pagar, implementar o adquirir aplicativos privativos que ofrecen estos servicios y que puedan implicar costo de licenciamiento o suscripción para su adecuación.

Para el objetivo particular se ejecutará uso de una solución llamada NethServer, software de código abierto construida sobre CentOS para la gestión de servicios propios ofrecidos por un servidor que trabaja en red.

2 INSTALACION DE NETHSERVER

Para Instalar NethServer es requerido primero descargar el software de su página oficial https://www.nethserver.org/, el software utilizado para el desarrollo de esta la practica documentada fue la versión 7.9.2009 disponible desde 2020-11-26. Una vez descargado el software, normalmente un archivo .ISO se procede con la instalación. [2] [4]

2.1 REQUERIMIENTOS MÍNIMOS

Para poder instalar NethServer en un servidor (virtual o físico) se debe asegurar de que la máquina cuente con los siguientes recursos mínimos [3], los cuales son los siguientes:

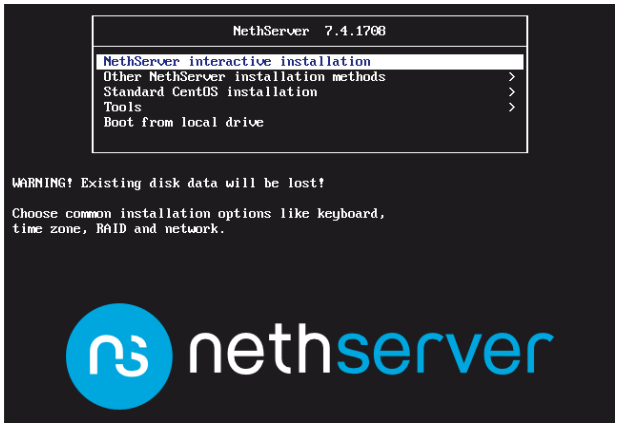
- CPU de 64 bits
- 1 GB de Memoria RAM
- 10 GB de espacio en disco duro

Cabe anotar, que lo indicado arriba puedan no ser suficientes los recursos para una implementación en gran escala. Se recomienda estudiar cuidadosamente los requerimientos particulares de red asociados con número de usuarios, latencia y posibilidades de escalamiento para, en los posible, mejorar los recursos que vayan a ser usados durante alguna otra implementación.

2.2 PROCESO DE INSTALACIÓN

Una vez se tenga el archivo de instalación .ISO preparado, de tal manera, que se pueda arrancar el servidor con él. Se inicia la máquina y se procede a la instalación como muestra la opción en la figura 1.

Figura 1. Pantalla de Inicio de Instalación

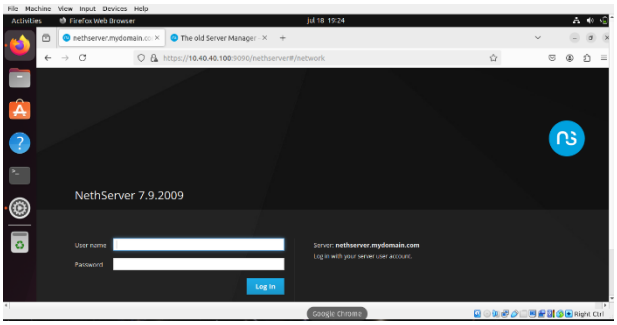


Fuente: NethServer.org

Una vez se da inicio al asistente de instalación este pedirá información sobre el usuario principal (root) y su clave y pedirá

la configuración de elementos como fecha y hora, tipo de teclado y direccionamiento de red, una vez estos elementos sean definidos la instalación sobre el disco duro procederá, una vez terminada instalación la maquina puede ser iniciada desde el disco duro y usando otro computador conectado en la misma red se podrá acceder a la página web de administración del servidor NethServer (ver Figura 2) usando el URL de la forma https://w.x.y.z:9090 en donde w.x.y.z es la dirección IP dada para el servidor durante el proceso de instalación.

Figura 2. Pantalla de Ingreso



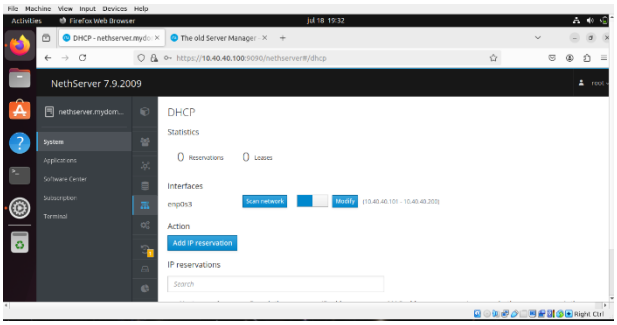
Fuente: Fuente Propia

3 CONFIGURACION DE SERVIDOR DHCP

Un servidor DHCP es aquel que ofrece información de direccionamiento a clientes que requieran tal información con el objeto de que estos puedan comunicarse y participar de los servicios de red. La información ofrecida por un servidor DHCP normalmente incluye dirección única IP para la red, subnet mask o mascara de red, dirección del enrutador o Gateway, servidores DNS para traducción de nombres de dominio en direcciones IP e información del nombre de dominio asociado con la red.

En NethServer, se habilita el servidor o servicio DHCP ingresando en la opción DHCP del menú principal. Desde allí se habilita este servicio en la interfaz de red como se muestra en la figura 3.

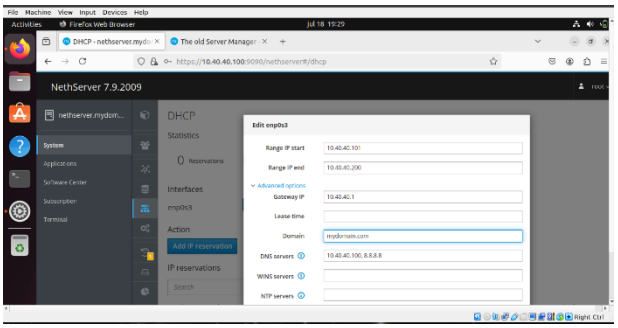
Figura 3. Habilitando el servicio DHCP en Interfaz



Fuente: Fuente Propia

Una vez habilitado el servicio en la interfaz, se define el rango de direcciones IP y otra información relevante que se ofertará a uno y cada uno de los clientes que busquen direccionamiento IP de algún servidor DHCP en la red, como se aprecia en la figura 4.

Figura 4. Definiendo rango de direcciones



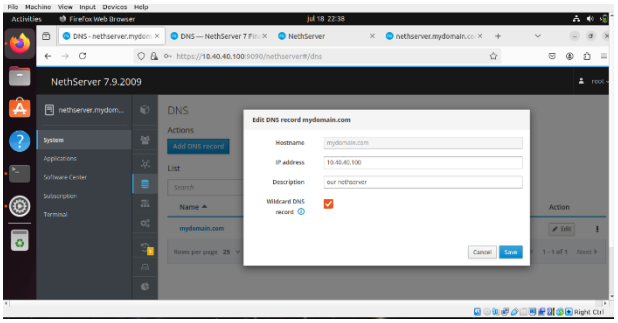
Fuente: Fuente Propia

4 CONFIGURACIÓN DE SERVIDOR DNS

Un servidor de DNS es un servicio adecuado en un servidor de red que responde a consultas de DNS en donde un cliente de red busca la dirección IP de un servidor que corresponda a un nombre calificado de dominio (FQDN).

En NethServer, esta adecuación se realiza en el área denominada DNS del menú principal en donde se pueden ingresar récords de DNS los cuales, como mínimo incluyen un nombre de dominio y la dirección IP correspondiente al servidor asociado con el dominio (Record A), tal y como se aprecia en la Figura 5.

Figura 5. Ingresando un Record A en DNS

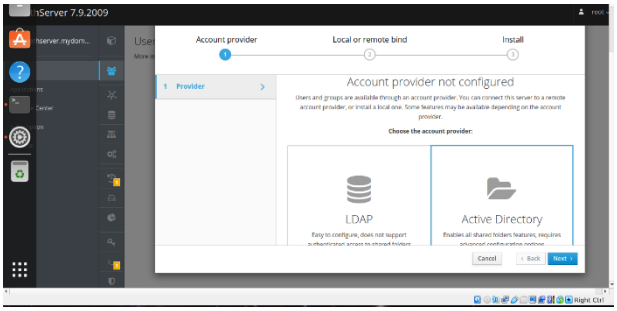


Fuente: Fuente Propia

5 CONFIGURACIÓN DE CONTROLADOR DE DOMINIO

Un servidor con el rol de controlador de dominio requiere la instalación del módulo de directorio activo, el cual, es una base de datos que, entre otras cosas, mantienen un repositorio central de información de acceso para usuarios, grupos y computadores que hacen parte de un dominio, normalmente local. En NethServer se instala este rol bajo la opción de Users and Groups (Figura 6) en donde se da la opción de hacer que el servidor sea parte de un dominio existente, o sea el primer servidor (servidor principal) de un nuevo dominio.

Figura 6. Instalando Active Directory



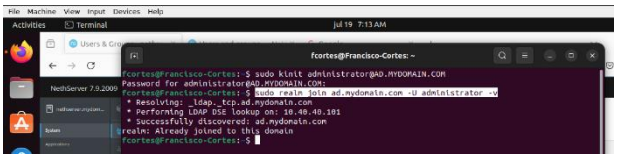
Fuente: Fuente Propia

Durante el proceso de creación de dominio, se indica el nuevo nombre de dominio, la dirección IP del controlador y el nombre completo y cualificado del controlador de dominio (ad.domain.tld), información que será requerida para que máquinas clientes y usuarios de dominio, puedan registrarse y autenticarse, respectivamente, con el controlador como parte del dominio administrado.

5.1 UNIENDO UNA MÁQUINA AL DOMINIO

Después de confirmar que una máquina en la red tiene conectividad (haciendo ping al AD) y puede comunicarse con el controlador de dominio (usando dig con la Instancia de NethServer con Active Directory), se procede a instalar los paquetes y servicios requeridos, para que un cliente con Ubuntu Linux pueda registrarse ante el controlador de dominio como una máquina que hace parte del dominio gestionado, posteriormente, se hace la configuración de estos servicios y paquetes, en particular de realmd (/etc/realmd.conf) y sssd (/etc/sssd/sssd/conf) y se procede con el registro de la máquina de Ubuntu con el controlador a través de la terminal. [1] [5]

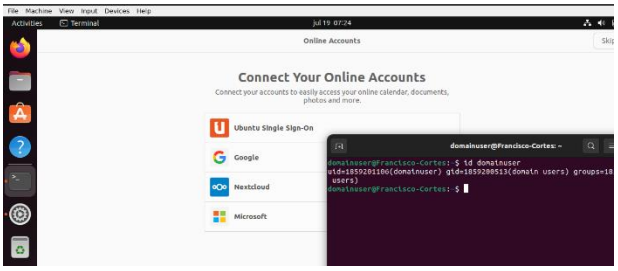
Figura 8. Registrando una maquina con el controlador



Fuente: Fuente Propia

Por último, se procede a verificar que a) un usuario de dominio, creado y configurado previamente dentro de Users and Grupos en el NethServer (controlador de dominio) con su usuario y clave respectivamente, pueda autenticarse desde la máquina cliente que se registró ante el dominio. (Figura 9), y b) se debe verificar también, que la máquina cliente que fue registrada ante el domino, en efecto aparezca allí, esta última tarea se realiza instalando una aplicación llamada phpldapadmin. [8] (Figura 10).

Figura 9. Autenticando un usuario de dominio desde una maquina registrada



Fuente: Fuente Propia

Figura 10. Maquinas registradas en el dominio

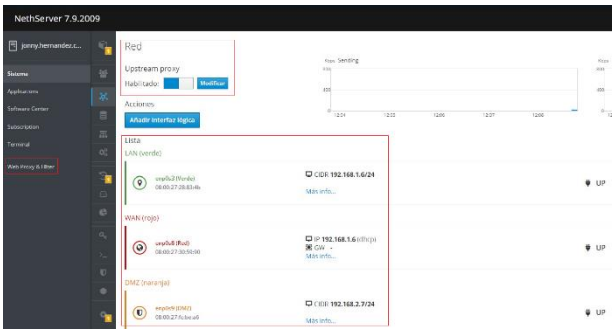
Fuente: Fuente Propia

Cabe anotar que la tarea de registro de maquina ante el controlador, al igual que otras tareas en preparación a este evento, puedan no ser fáciles de desarrollar si esto no se ha hecho previamente. En otras palabras, es posible que al ejecutar algunos comandos requeridos pueda que estos arrojen errores los cuales deben ser investigados con el soporte de NethServer y/o con consultas en línea en foros de soporte técnico comunitario, si esto es requerido.

6 PROXY

Un proxy es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que se visitan en línea [6]. El Proxy hace conexión directa a las zonas verdes, ya sea manual o con autenticación de transporte con simple o doble protocolo de seguridad. Para la conexión SSL se hace el cifrado entre el cliente y el servidor [7].

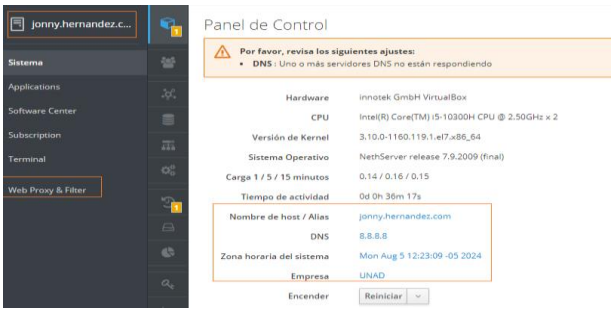
Figura 11. Configuración las zonas de red



Fuente: Imagen propia

En la (Figura 11) se muestra que la zona verde debe tener IP estática para filtrar por la puerta de enlace el tráfico de red de salida por el puerto 3128. En el panel principal, se debe realizar la configuración del nombre del host FQDN junto con los DNS como se muestra a continuación.

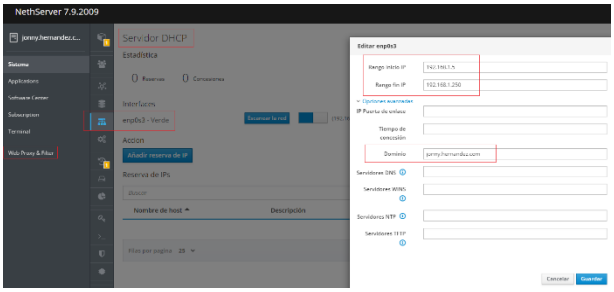
Figura 12. Configuración FQDN y DNS



Fuente: Imagen propia

Es fundamental realizar la configuración del DCHP, como se realiza en los pasos anteriores, ya que los rangos de IP's escogidas deben corresponder con el host, para que tenga conexión con el dominio. No se debe interactuar con la misma IP de puerta de enlace, de lo contrario se generaría error por redundancia y no permitiría habilitar el Proxy.

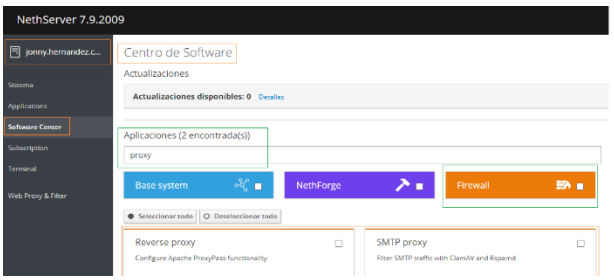
Figura 13. Configuración dominio y DHCP



Fuente: Imagen propia

Luego se valida con el botón de "Software Center", del centro de validación de Firewall, los paquetes tanto de web y filtros para el Proxy y poder así ejecutar el servicio a través de la red.

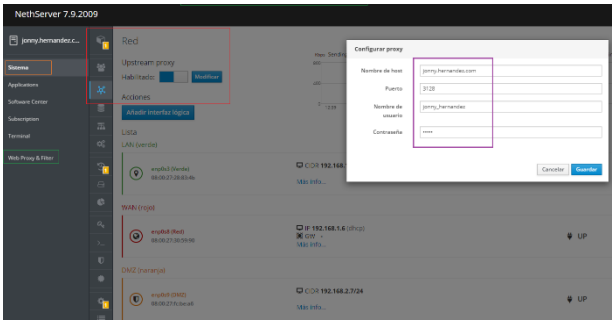
Figura 14. Validación y ejecución paquetes Proxy



Fuente: Imagen propia

Finalmente, se debe realizar la configuración del Proxy en la "Red" de transmisión de datos, con el nombre del host, al puerto 3128 y la debida autenticación de credenciales (usuario y contraseña), para proceder a confirmar la ejecución correcta del servicio con el filtrado de salida por medio del puerto indicado.

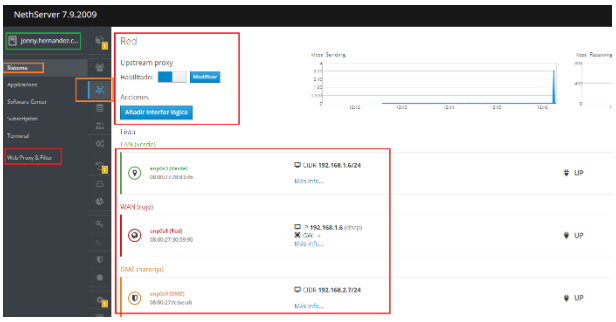
Figura 15. Validación y ejecución paquetes Proxy



Fuente: Imagen propia

Hay que tener presente, que, para activar el proxy, se debe confirmar en un entorno de red controlado, para dicha configuración, ya que los protocolos de seguridad bloquearán puertos y páginas de dudosa procedencia en el tráfico de salida a Internet. A continuación, se confirma la activación del Proxy.

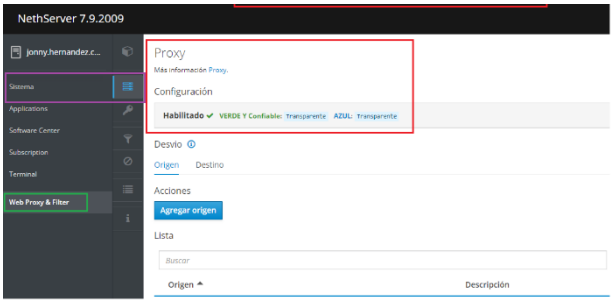
Figura 16. Validación de activación Proxy



Fuente: Imagen propia

Para el sitio web, se valida los servicios y el paquete de filtrado de las validaciones de prestación a los puertos configurados en NethServer para la zona verde y/o invitado.

Figura 17. Validación de activación Proxy web



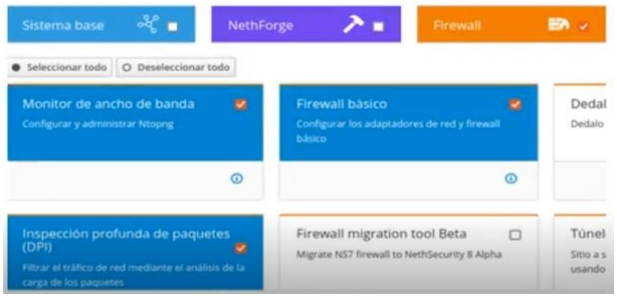
Fuente: Imagen propia

7 CORTAFUEGOS

Los cortafuegos son como un filtro que ayuda a proteger una red de los ataques informáticos. El filtro analiza el tráfico de red entrante y saliente, y bloquea todo el tráfico que no cumpla con las reglas de seguridad. Por ejemplo, una regla podría bloquear todas las conexiones desde una dirección IP específica podría ayudar a proteger una red de un ataque proveniente de esa dirección IP [9].

Para la configuración, se ingresa al apartado de "Software Center" y allí se selecciona la opción Firewall y Firewall básico.

Figura 18. Instalación de firewall



Fuente: Imagen propia

Una vez finalizada la instalación, se conecta al servidor y se observa la topología de la red. Esta topología se ha configurado de acuerdo con la zona DMZ.

Figura 19. Topología de la red.

Fuente: Imagen propia

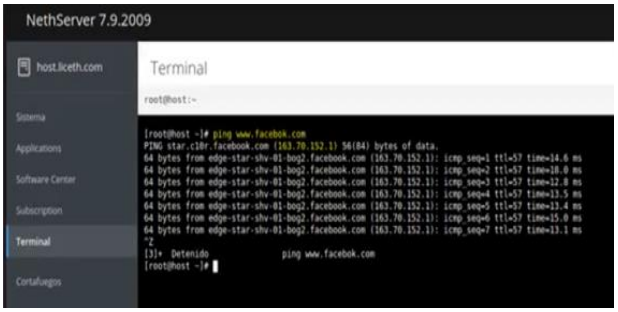
Para la restricción de la apertura de sitios o portales Web en redes sociales, se apunta el navegador, por ejemplo, a la página de Facebook, observando que responde de manera correcta.

Figura 20. Acceso a red social Facebook

Fuente: Imagen propia

Para bloquear el acceso a Facebook con el cortafuegos es necesario conocer la dirección IP de todos los servidores de Facebook. Una forma de obtener esta información es utilizando el comando ping en la terminal. Por ejemplo, para obtener la dirección IP del servidor principal de Facebook, se puede ejecutar el comando que se muestra en la Figura 21.

Figura 21. Ping a Facebook



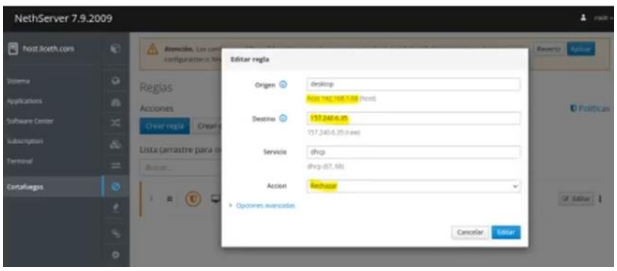
Fuente: Imagen propia

La dirección IP que se requiere es la que aparece después de la palabra "from". En este caso, la dirección IP es 163.70.152.1. Cuando se obtiene la dirección IP de los servidores de Facebook, se crean reglas de bloqueo en el cortafuegos para impedir el acceso de los usuarios a esta página. Para bloquear el acceso a Facebook con el cortafuegos, se crea una regla que rechace todas las conexiones desde el equipo de red a la dirección IP de Facebook [10].

Para ello, se realizan los siguientes pasos:

- Acceder a la configuración del cortafuegos.
- En la sección de reglas, crear una nueva regla y en el campo Origen ingresar a la dirección IP del equipo de red o red.
- En el campo destino se ingresa la dirección IP de Facebook.
- En el campo Servicio, se selecciona HTTPS.
- En el campo Acción, se selecciona Rechazar.
- Se guarda la regla.

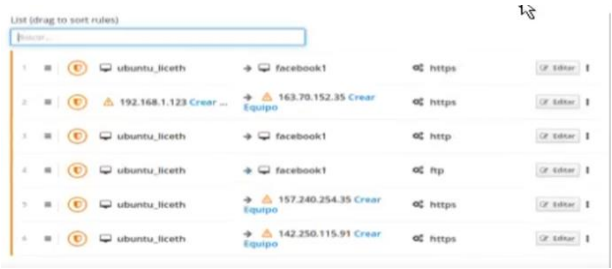
Figura 22. Creación de reglas.



Fuente: Imagen propia

Se verifica que se haya creado la regla correctamente. También es recomendable crear reglas para los protocolos HTTP y TCP, lo que ayudará a garantizar una mayor seguridad en los puertos. En este caso, se puede ver que se asignaron reglas para varias direcciones IP que permiten el acceso a Facebook.

Figura 23. Reglas para bloquear Facebook



Fuente: Imagen propia

Para probar, se dirige al navegador de nuevo a la página de Facebook, sin embargo, el sistema impide el acceso. Esto se debe a la regla configurada que bloquea el acceso a esta página.

Figura 24. Bloqueo de Facebook

Fuente: Imagen propia

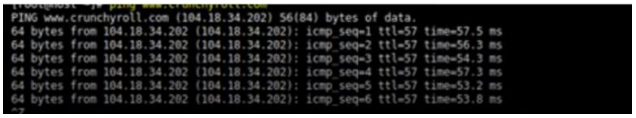
Para la restricción de la apertura de sitios o portales Web de venta en línea se realiza el mismo ejercicio abriendo este sitio en el navegador (Figura 25).

Figura 25. Página de compras

Fuente: Imagen propia

Se hace la verificación en la terminal con el comando ping https://www.mercadolibre.com.co/ mostrando la IP 104.18.34.202, con la que se va a crear la regla.

Figura 26. Ping a MercadoLibre

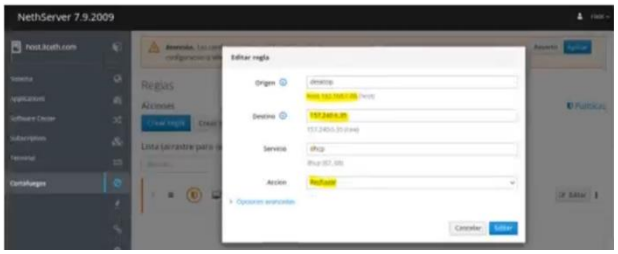


Fuente: Imagen propia

Para bloquear el acceso a Mercado Libre desde la red o equipo, se crea una nueva regla en el cortafuegos con los siguientes parámetros:

- Origen: Dirección IP de nuestro equipo.
- Destino: Dirección IP de Mercado Libre.
- Servicio: HTTPS.
- Acción: Rechazar.

Figura 27. Parámetros para bloqueo para MercadoLibre

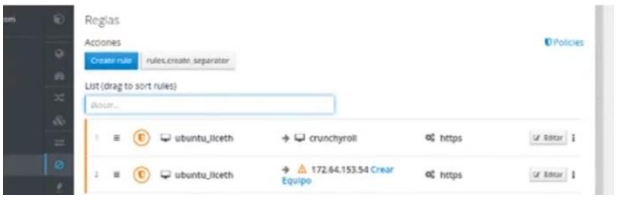


Fuente: Imagen propia

Para crear una nueva regla, se procede de la siguiente manera:

- Se accede a la interfaz de configuración del firewall
- En la sección "Reglas", se pulsa el botón "Añadir".
- En el campo "Origen", se introduce la dirección IP del equipo.
- En el campo "Destino", se introduce la dirección IP de Mercado Libre.
- En el campo "Servicio", se selecciona "HTTPS".
- En el campo "Acción", se selecciona "Rechazar".
- Por último, se pulsa el botón "Guardar".

Figura 28. Regla para MercadoLibre



Fuente: Imagen propia

Al ingresar de nuevo en el navegador a la página de mercado libre, ya se niega el ingreso, con esto se puede garantizar que el cortafuego está cumpliendo su función.

Figura 29. Bloqueo de MercadoLibre

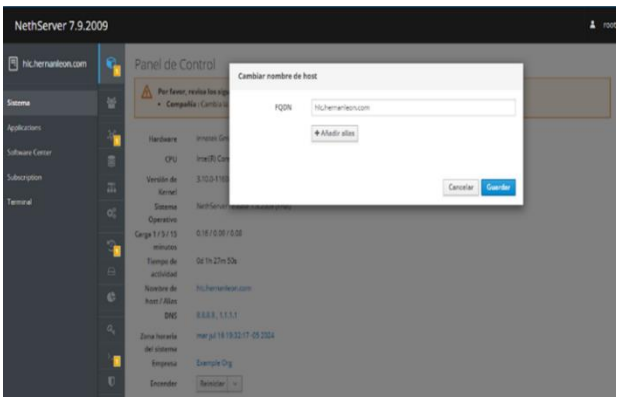
Fuente: Imagen propia

8 VNP

Una VPN permite establecer una conexión entre redes o nodos de red de forma segura enlazando dichos sistemas a través de una red pública [7].

Se procede a implementar y configurar una VNP que permita establecer un túnel de comunicación con una estación de trabajo donde se evidencia el ingreso a la aplicación desde la estación de trabajo.

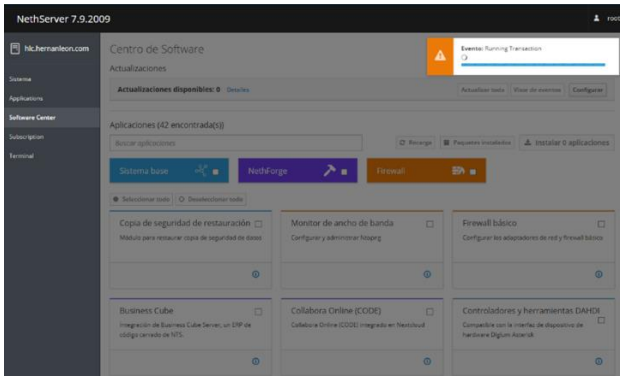
Figura 30. Cambiar Nombre de la empresa



Fuente: Fuente Propia

Luego de finalizar el proceso de actualizaciones y permisos requeridos, se debe desplazar al panel izquierdo donde se encontrará el enlace llamado “Software Center” allí se puede observar los programas necesarios para instalar.

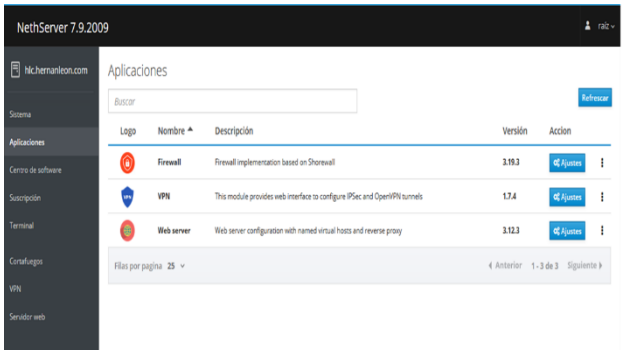
Figura 31. Programas necesarios para instalar



Fuente: Fuente Propia

Una vez se actualizan los servicios solicitados por NethServer, desde el menú lateral se encontrará un ítem llamado “Applications” desde donde se podrá acceder a la configuración.

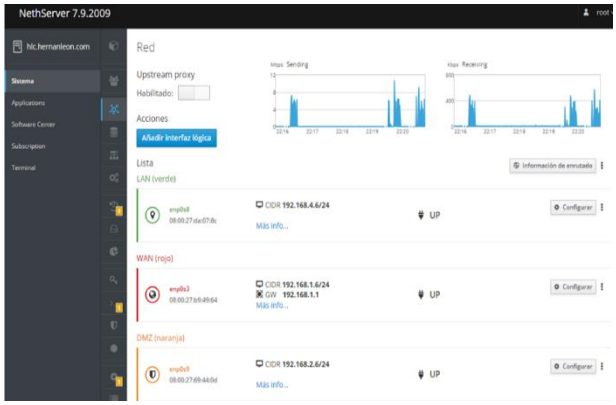
Figura32. Descargar e instalar Firewall y OpenVNP



Fuente: Fuente Propia

Luego se regresa al ítem del sistema para ir la red a configurar las tarjetas, ya que, estas se configuran según su color, verde “LAN”, rojo “WAN” y naranja” DMZ”.

Figura 33. Asignación de color y función a cada tarjeta

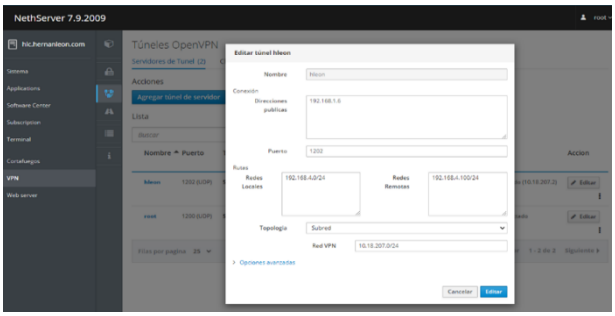


Fuente: Fuente Propia

Para el modo túnel se utilizarán dos enrutadores, donde cada uno de los enrutadores actúan como extremos de un túnel

virtual en la red pública, también se creará un túnel para el servidor, donde se tiene en cuenta las redes que se configuraron. “RED” como publica, “GREEN” red local, “DMZ” como remota.

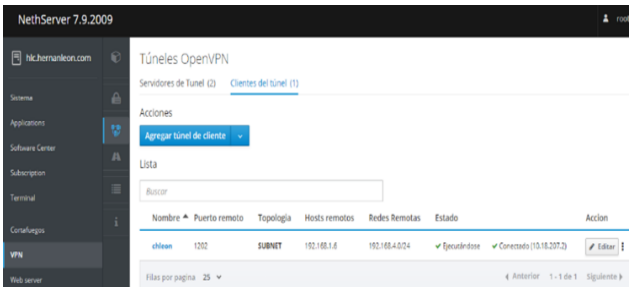
Figura 34. Creación de Túneles OpenVPN



Fuente: Fuente Propia

Se realiza la descarga de la configuración para crear los clientes del túnel para que así se pueda realizar la conexión.

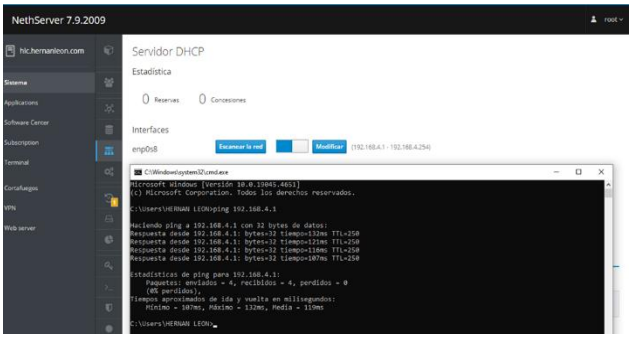
Figura 35. Implementación de la configuración para el cliente



Fuente: Fuente Propia

Creado el túnel se puede tener la conexión al desktop de forma remota, para esto se utiliza OpenVPN RoadWarrior, una configuración de OpenVPN que permite la conexión de un cliente remoto a una red privada.

Figura 36. Se configura el servidor RoadWarrior



Fuente: Fuente Propia

9 CONCLUSIONES

- Existen alternativas de open source frente a aplicaciones especializadas para administración de redes corporativas como lo es MS Server y su popular Active Directory, a pesar de esto, el proceso de registrar máquinas de Linux dentro de un dominio todavía resulta un proceso relativamente complicado cuando se usa una terminal.
- Habilitar el Proxy en NethServer es de gran ayuda para mantener una red segura y optimizada, ya que, filtra contenido malintencionado y garantiza un uso optimizado y enfocado del ancho de banda con el que se cuente en una red
- Los cortafuegos son cruciales para la seguridad de las redes. Actuando como una barrera entre redes internas seguras e Internet, controlan el tráfico de red y protegen contra amenazas externas y accesos no autorizados.
- Los cortafuegos de próxima generación (NGFW) ofrecen características avanzadas como la inspección profunda de paquetes y la prevención de intrusiones. Estos dispositivos y/o software mejoran la protección en zonas de red donde se implementan y proporcionan una defensa integral si se configuran adecuadamente y en la medida en que sean monitoreados de forma constante.
- NethServer permite la creación del servicio de redes privadas virtuales (VPN). Una vez configurado este servicio, se puede usar en redes con diversos sistemas operativos.
- Los servicios que se presentan en este artículo y que son ofrecidos dentro de la plataforma de NethServer en su versión 7.9, ofrecen bastantes ventajas para ambientes corporativos sin implicar costos de licenciamiento para su uso, adquisición y/o implementación.

10 REFERENCIAS

[1] Andreou, T. (2018). *"How To Join an Ubuntu Desktop into Active Directory Domain"*. https://www.unixmen.com/how-to-join-an-ubuntu-desktop-into-an-active-directory-domain/

[2] Linux Video Tutorials. (2018). “*NethServer 7.4 Installation + Configuration + Overview on Oracle VirtualBox*”. https://www.youtube.com/watch?v=kggkwioK-ls

[3] NethServer.org. (2023). *“NethServer Minimum Requirements". Recuperdado de* https://docs.nethserver.org/en/v7/.

[4] planet_jeroen. (2018, February 19). *“How to install NethServer as Samba AD domain controller v0.2. NethServer Community”*. https://community.nethserver.org/t/howto-install-nethserver-as-samba-ad-domain-controller-v0-2/9076

[5] Schieving, G. (2019). “How to Add an Ubuntu Client to Windows Server 2016 Domain”. https://www.youtube.com/watch?v=YgBh4SZVEZc&t=528s

[6] Nethserver. (2023). Proxy web. Obtenido de NethServer: https://docs.nethserver.org/es/v7/web_proxy.

[7] NethServer (2023). VPN Nethserver. Obtenido de https://docs.nethserver.org/es/v7/vpn.html

[8] Deon, George (leenooks), (2024). “phpLDAPAdmin”. Recuperado de https://github.com/leenooks/phpLDAPadmin

[9] Incibe. (19 de 9 de 2019). "¿Qué es un cortafuegos?" Obtenido de https://www.incibe.es/empresas/blog/dmz-yte-puede-ayudar-proteger-tu-empresa

[10] Site24x7. (s.f.). "Encuentre la dirección IP de su dominio, servidor o sitio web". Obtenido de https://www.site24x7.com/es/tools/buscardireccion-ip.html

11 NOTAS

1. El trabajo de instalación y adecuación de DHCP, DNS y Active Directory fue desarrollado en un ambiente virtual usando 2 máquinas virtuales, una maquina cliente con Ubuntu 22.04 y otra máquina virtual dentro de la misma red interna (Green) en donde se instaló NethServer.

2. Para la configuración del Proxy, es vital la configuración de un segmento de red en DCHP para el tipo de mascara de subred, a número 24 tipo "C", ya que, al no realizarse, se bloquea el acceso a Internet. En práctica de ejecución para la ISP, en el hogar, tanto cableada LAN como WIFI de WLAN, se debe tener cuidado también, debe ser la misma estáticamente para el tema de la puerta de enlace "Gateway", sin embargo, por pruebas y error de intentos fallidos, se logra, tanto en la red como en la web, el tráfico de salida a Internet en una máquina virtual Ubuntu 22.04 en VirtualBox.

3. Configurar un cortafuegos es crucial para la seguridad de la red. Primero, identifica las zonas que necesitan protección, como el perímetro de la red, subredes internas y dispositivos finales. Luego, define reglas de filtrado para controlar el tráfico entrante y saliente basado en políticas de seguridad. Asegúrate de monitorear y actualizar regularmente las configuraciones para adaptarte a nuevas amenazas. La correcta implementación de estas medidas garantiza una protección eficaz contra accesos no autorizados y ataques maliciosos.

4. Los servicios que se presentan en este artículo, en cuanto a la distribución de GNU/Linux con el manejo de NethServer en su versión 7.9, se puede obtener bastantes servicios en cuanto a sus aplicaciones, también brindan grandes ventajas, las cuales, se tienen como la creación de los túneles VPN, para mayor seguridad de la información, así mismo poder brindar estabilidad y confianza en el uso de estas herramientas de software libre, las cuales permiten a los usuarios obtener sin ningún costo y a la vez, son muy confiables y muy seguras al momento de su uso.