IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS BASADAS EN TEMÁTICAS DEFINIDAS SEGÚN NECESIDADES ESPECÍFICAS CON GNU/LINUX

Gabriel Alexander Jaramillo Higuita
gajaramilloh@unadvirtual.edu.co
Carlos Alberto Moreno Calderín
Julián Andrés Quiceno Valencia
jaquicenov@unadvirtual.edu.co

RESUMEN: *En el presente artículo se pretende demostrar la correcta forma de realizar la instalación, configuración, administración y control de la distribución GNU/Linux NethServer basada en las populares distribuciones CentOS y Red Hat Enterprise Linux, por lo que la estabilidad y el soporte con actualizaciones son puntos que hacen de esta una excelente distribución, esta igualmente está enfocada a la implementación de servicios de infraestructura IT de mayor nivel.*
Permitiéndonos entonces disponer de los servicios necesarios para implementar casi en cualquier tipo de organización, ofreciéndonos soluciones para gestionar servicio tales como : DHCP Serve, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server y Print Server. Dándonos una interfaz web amigable, intuitiva y de fácil aprendizaje, desde donde podremos configurar los servicios ya mencionados, al igual que zona DMZ según sea las necesidades de la Red que se desea administrar.

PALABRAS CLAVE: Administración, Aplicaciones, Configuración, Instalación, Infraestructura Tecnológica, Servicios.

1 INTRODUCCIÓN

El presente documento tiene como finalidad dar a conocer la debida instalación y configuración de la distribución GNU/Linux Nethserver, demostrando igualmente la realización de la configuración para la zona DMZ, de acuerdo con la red administrable que se creará para dicha distribución. Complementado la construcción del documento se establecerán los desarrollo de las temáticas propuestas para demostrar de una forma practica la construcción y configuración de un servidor administrable para una infraestructura en red de una organización, demostrando así la compresión de las diferentes unidades y temáticas tratadas para el desarrollo del curso Diplomado de Profundización en Linux Opción de Grado.

2 INSTALACIÓN DE NETHSERVER 7.9.2009

2.1 REQUERIMIENTOS MÍNIMOS

Los requisitos mínimos son:

- 64 bit CPU (x86_64)
- 1 GB de RAM
- 10 GB de espacio en disco

Los desarrolladores de la distribución igualmente nos recomiendan la utilización de al menos 2 discos para configurar un RAID 1. Ya que el software RAID garantizará la integridad de los datos en caso de fallo del disco.

2.2 INSTALACIÓN DESDE ISO

Para realizar la creación de los medios para la instalación los desarrolladoras de la distribución, nos recomiendan descargar el último archivo ISO del sitio oficial www.nethserver.org. El archivo ISO descargado puede utilizarse para crear un medio de arranque como un DVD o una memoria USB.

2.3 ARRANQUE DE LA INSTALACIÓN

Comenzaremos encendiendo la máquina utilizando el soporte creado como medio de instalación. Si se presentara el caso de que la máquina no se iniciara desde el medio utilizado, se deberá consulte la documentación del BIOS según sea la placa base.

Al iniciar se nos presentara un menú donde se nos mostrara diferentes tipos de instalación.

Figura 1. Inicio booteador netserver.

Para este caso utilizaremos la primera opción, dando Enter en ella para que el sistema comienza con el cargue necesario de pagues y demás recursos.

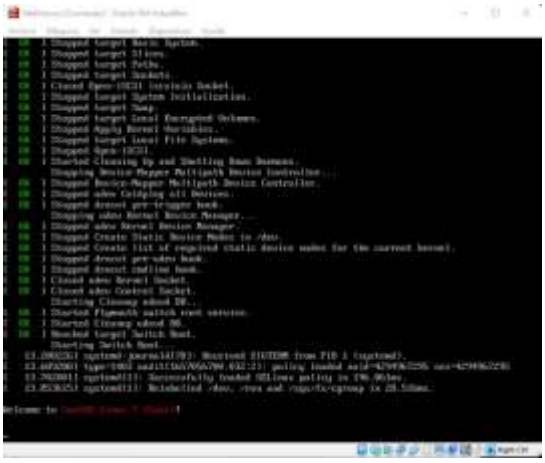

Figura 2. Inicialización de netserver.

Posteriormente a que termine la carga del sistema tendremos ya las opciones para comenzar con la instalación de nuestra distribución.

Figura 3. Inicio de asistente de instalación netserver.

Ahora como podemos observar en algunas de las opciones que vemos en pantalla, se nos alerta de unas opciones no seleccionadas, para configurar dichas opciones entraremos en cada una de ellas para seleccionar las que más se ajusten a nuestra necesidad.

Comenzaremos entonces realizando la debía configuración de la opción de “DATA & TIME”. Desde allí debemos elegir la zona en la que nos encontramos para el asistente active y configure la zona horaria que corresponde, y terminaremos dando clic en el botón “Done”.

Figura 4. Configuración de zona horaria.

Ahora procederemos a realizar la selección de la distribución de nuestro teclado para eso ingresaremos a la opción de “KEYBOARD”.

Para agregar un idioma para nuestro teclado deberemos dar clic en el “+” que observamos en pantana y buscaremos la distribución que deseamos seleccionar, para este caso ya que mi teclado tiene la distribución de Ingles solo seleccionare la opción que ya viene por defecto, finalizamos igualmente dando clic en “Done”.

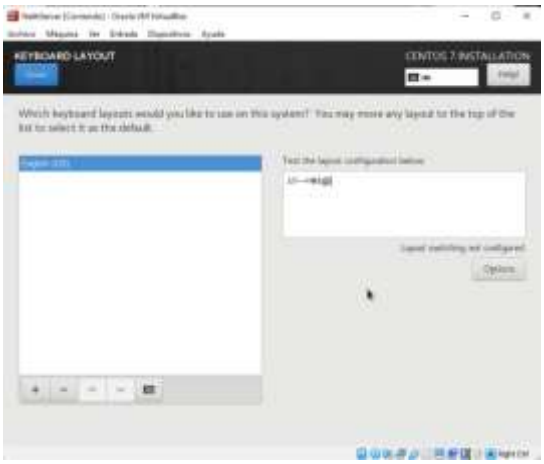

Figura 5. Configuración de distribución de teclado.

Ahora procederemos a realizar una configuración en el apartado de “NETWORK & HOST NAME”, desde donde configuraremos un nombre de dominio, el cual dejaremos las iniciales de mi nombre y el nombre del curso (gajh.diplomadoplinux.com) y validaremos que nuestras tarjetas de red hayan sido detectadas y estén activadas.

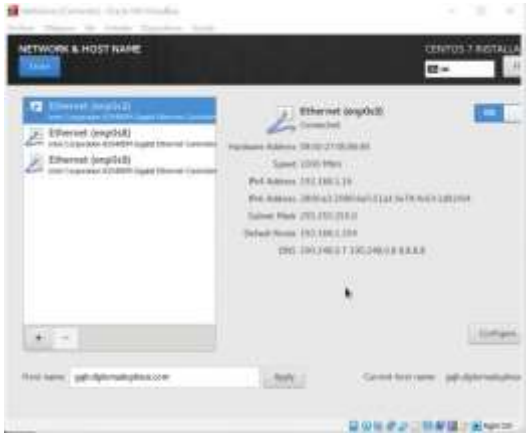

Figura 6. Configuración de interfaz de red.

Ahora para esta instalación no tocaremos el particionado y dejaremos que el mismo asisten realice la configuración, esto se opta de esta forma ya que es una instalación en una máquina virtual.

Por lo cual procedemos realizando clic en la opción de “Begin Installation”.

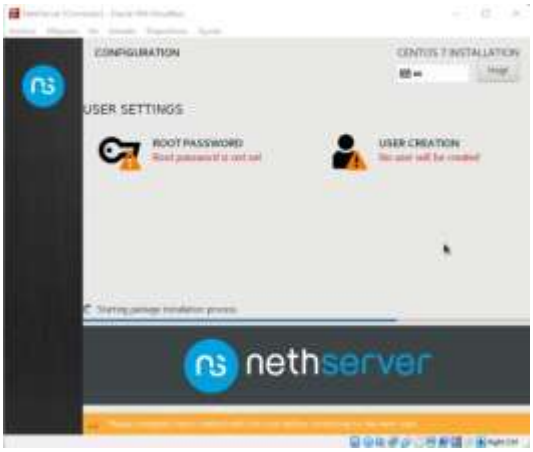

Figura 7. Creación de usuarios estándar y root.

Ahora podremos ver que la instalación de la distribución a comenzando, pero igualmente se nos da la opciones de crear una contraseña para el usuario root y crear otros usuarios si así lo deseamos, para este caso solo realizaremos la configuración de la contraseña del usuario root, ya que con este será con el que estaremos trabajando.

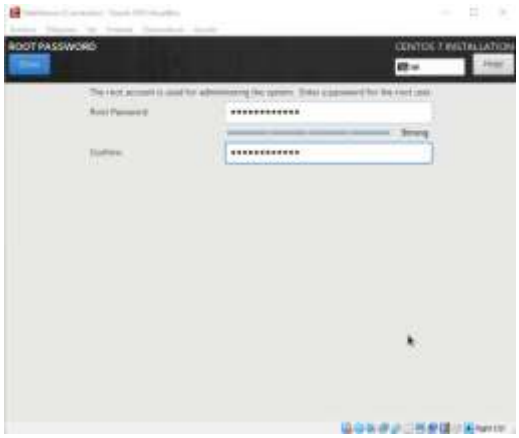

Figura 8. Establecimiento de contraseña root.

Ya solo deberemos esperar a que el asistente termine de realizar la instalación de la distribución. Este al finalizar se reiniciará y esperaremos hasta que este vuelva a cargar.

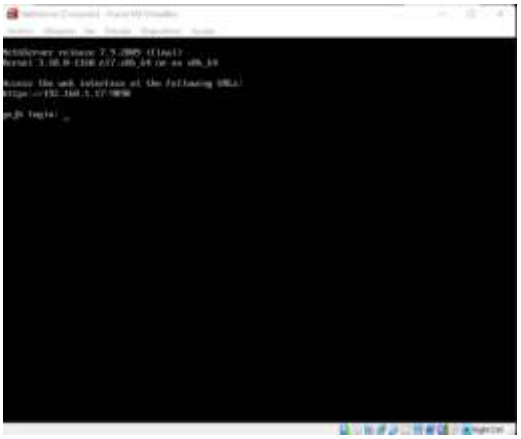

Figura 9. Inicio de sistema nethserver.

Una vez reiniciado, ingresaremos con los datos de nuestra cuenta y ejecutaremos el comando $ yum update, para que el sistema se actualiza si así lo requiere.

Ahora con la IP que tomo nuestra distribución ingresaremos a la administración del sistema desde un navegador utilizando el siguiente ejemplo de dirección: https://SuIP:9090, en nuestro caso sería de la siguiente forma: https://192.168.1.20:9090

Figura 10. Inicio de sesión en interfaz web.

3 DESARROLLO DE TEMÁTICAS SELECCIONADAS

3.1 TEMÁTICA 2: PROXY

El Proxy en una red informática, es un servidor, "programa o dispositivo", que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada por los usuarios, administradores o proveedores como legítima o delictiva y su uso es frecuentemente discutido.

Ahora bien conociendo lo anterior procedemos a realizar la configuración de nuestro servicio Proxy en nuestro servidor previamente configurado.

Para dicha configuración ingresaremos a la plataforma web que nos ofrece nuestro servidor ingresando a través de la dirección https://192.168.10.5:9090.

Una vez ingresados nos dirigiremos a la opción de "Software Center", desde allí filtraremos por la opción de "Firewall".

Una vez filtrado seleccionaremos las opciones "Monitor de Ancho de Banda", "Firewall Básico", "Sistema de Prevención de Intrusos", "Filtro Web" y "Proxy Web".

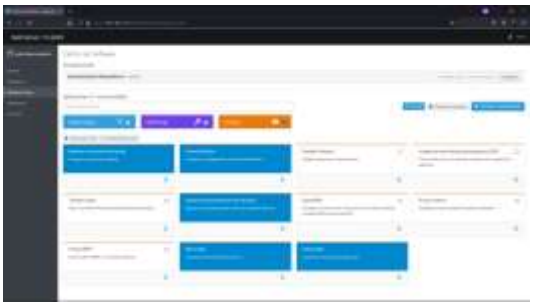

Figura 11. Panel de software center para instalación de aplicaciones.

Y daremos clic en la opción que se nos marcara como "Instalar # aplicaciones".

Confirmamos la instalación y esta iniciara a realizar la descarga e instalación de los paquetes necesarios.

Figura 12. Instalación de aplicaciones firewall.

Con esto ya tendremos instalado nuestros servicios seleccionados.

Ahora procederemos a realizar la configuración de estos, para lo cual nos dirigimos primeramente a la opción de "Aplicaciones", desde allí podremos ver los servicios o aplicaciones recientemente instaladas.

Figura 13. Panel de aplicaciones instaladas.

Desde allí daremos clic en la opción de “Ajustes” del aplicativo “Web Proxy & Filter”.

Figura 14. Panel principal de proxy y filtro web.

Como podemos observar nuestro proxy no se encuentra habilitado, por lo que en este apartado procedemos a realizar la configuración necesario y habilitarlo.

Para comenzar con dicha configuración dos dirigiremos a la opción de “Proxy” que podemos encontrar en las opciones de la izquierda.

Figura 15. Inicio de configuración proxy.

Para comenzar la con la configuración daremos clic en “Configurar proxy”.

Desde allí dejaremos la opción de “SSL Transparente” tanto para la zona Verde como Azul, esto con el finde de que todos los clientes sean obligados automáticamente a utilizar el proxy para las conexiones HTTP y HTTPS en la configuración avanzada especificaremos el puerto para el proxy, por defecto será el puerto el 3128, ya que en la guía se especifica que debe ser este puerto el que hará el filtrado del proxy se dejará tal cual esta.

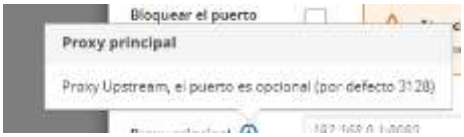

Figura 16. Validación de puerto por defecto.

Ahora solo damos clic en “Guardar” y este aplicara los cambios.

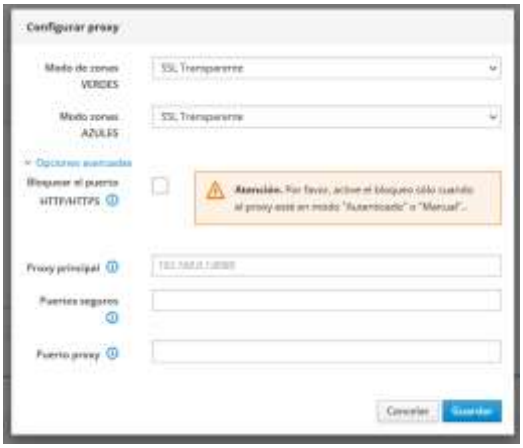

Figura 17. Configuración básica de proxy.

Figura 18. Estado final de configuración de proxy.

Ahora nos dirigimos a la opción de “Filtro”, desde allí deberemos realizar la descarga de dicha categoría, para eso simplemente daremos clic en la opción de “Descargar” y veremos que la descarga comenzara en breve, ya solo queda esperar a que esta finalice para tener las opciones que nos brinda esa opción de Filtro.

Figura 19. Opción de descarga para categoría.

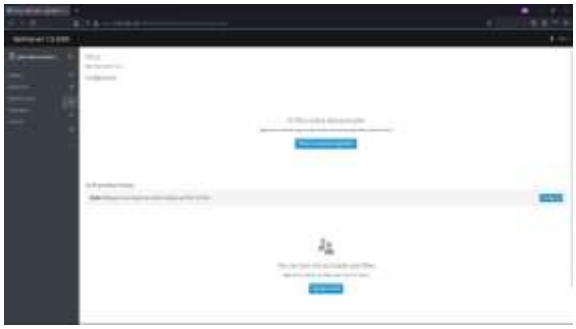

Figura 20. Inicio de configuración de filtro.

Una vez terminado el proceso, procederemos a realizar lo siguiente.

Primeramente editaremos las opciones globales, para eso daremos clic en la opción “Editar las opciones globales”, desde allí procedemos a especificar las extensiones de archivos que deseamos bloquear como lo pueden ser (.exe, .zip), igualmente podremos habilitar la conciencia de expresiones en las URL, para nuestro caso agregaremos un dominio el cual deseamos bloquear “yahoo”, igualmente habilitaremos la opción de coincidencia de expresiones para URL, esto con el fin de que los dominios en las listas sean más precisos, para finalizar daremos clic en “Guardar”.

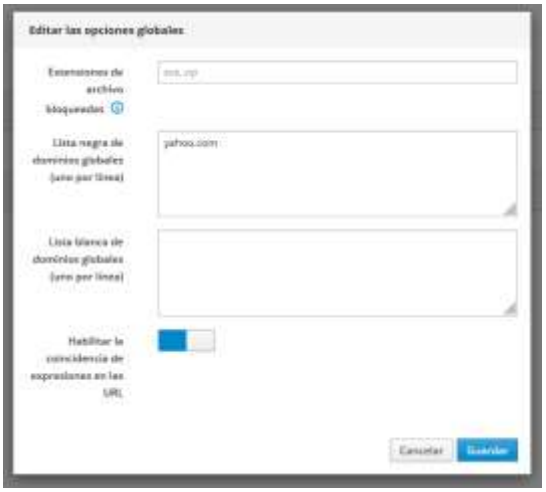

Figura 21. Edición de opciones globales.

Igualmente habilitaremos el antivirus como una opción adicional.

Figura 22. Finalización de configuración de filtro.

Ahora procederemos a realizar la configuración del perfil predeterminado, para habilitar las listas negras y blancas de los dominios bloqueados o permitidos, para eso daremos clic en la opción de configurar que veremos en “Perfil predeterminado”.

Desde allí igualmente podremos bloquear varios sitios según las categorías a las que pueden pertenecen.

Figura 23. Edición de perfil por defecto.

Ahora procederemos a ir a nuestro equipo cliente y desde las opciones de red y entraremos a la opción “Proxy de la red”, desde allí dejaremos marcada la opción de “Manual” y especificaremos la IP del servicio proxy como su puerto, el cual para este caso será 192.168.10.5:3128.

Figura 24. Agregando proxy a cliente.

Ahora procederemos a validar el funcionamiento de nuestro servidor, para lo cual nos dirigiremos a un navegador e ingresaremos a una página cualquiera para validar que estamos teniendo adecuadamente la salida a internet y posterior a esto ingresaremos al dominio que fue agregado a la lista negra, en este caso “yahoo.com’.

Figura 25. Validación de navegación.

Figura 26. Validación de funcionamiento de proxy.

Con esto se valida la funcionalidad del proxy configurado para la red.

3.2 TEMÁTICA 3: CORTAFUEGOS

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.

En la siguiente figura veremos la interfaz donde podremos iniciar con la instalación y configuración de nuestro cortafuegos en nethserver.

Figura 27. Inicio de netserver 7.6.

Figura 28. Configuración de host name.

Figura 29. Configuración de zona horaria.

Figura 30. Entrada puerto de enlace.

Figura 31. Configuración de red IP estática.

Agregamos cortafuegos básico y descargamos los paquetes del cortafuegos y puerta de enlace.

Figura 32. Instalación de paquetes para el cortafuegos.

Figura 33. Proceso de instalación.

Ahora debemos de actualizar la página para ver los paquetes instalados.

Figura 34. Actualización de página.

Ahora nos vamos a crear las reglas.

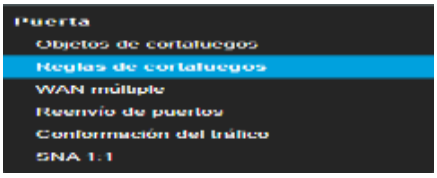

Figura 35. Creación de reglas para cortafuego.

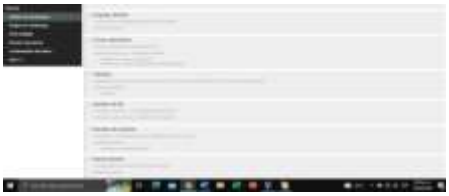

Figura 36. Definiendo reglas.

Primero hacemos ping en Google desde la máquina Ubuntu desktop 20.04.

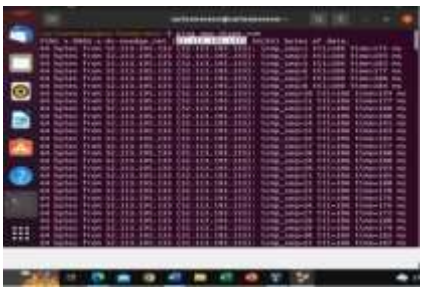

Figura 37. Prueba de conexión equipo cliente.

Ahora podemos ver la aplicación de las reglas.

Figura 38. Aplicación de las reglas.

Y como resultado verificamos el bloqueo de conexión a las redes en Ubuntu desktop después de guardar los cambios.

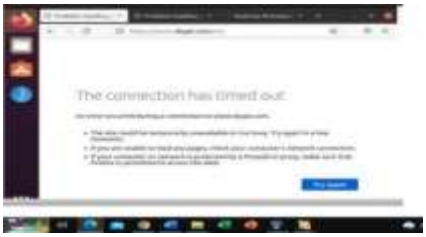

Figura 39. Comprobación de bloque de reglas.

Se hace verificación de la aplicación de la regla asignada y efectivamente funciona

3.3 TEMÁTICA 5: VPN

Para iniciar la configuración de nuestra VPN, debemos tener claros algunos aspectos tales como.

- Modo de autenticación en la sesión VPN
- Direccionamiento que se le asignara a los equipos remotos, cuando se establezca la conexión
- Direccionamiento público para que la VPN sea alcanzada desde cualquier lugar
- Asignación de usuarios en el LDAP
- Conexión física al equipo servidor, direccionamiento que se le asignara y servicios que prestara a los usuarios que se conecten, para nuestro caso, tendremos un servicio Apache y SSH
- Software que se usara en el lado cliente, para inicio de la sesión VPN
- Zonas, reglas y servicios que se deben habilitar en el firewall

Iniciamos la creación de nuestra VPN RoadWarrior

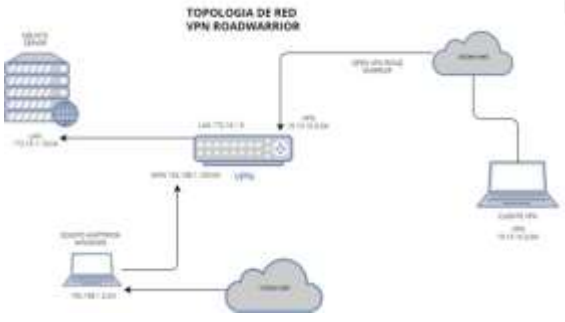

Figura 40. Esquema de la red.

Iniciaremos la configuración de nuestra RoadWarrior, para ello utilizaremos el modo de autenticación: Certificado, lo que quiere decir que debemos descargar un perfil y agregarlo al software que se usara al lado cliente, no aplica para todos los casos.

El direccionamiento que asignamos para los equipos remotos que entren en la sesión VPN será el 10.10.10.0 / 24 y la WAN Publica será 192.168.1.100

Figura 41. Configuración de RoadWarrior.

Continuamos con la instalación de LDAP para la creación de los usuarios que tendrán acceso a la VPN, se instalara el LDAP Local.

En la gestión de nuestro NethServer, debemos ingresar a Sistema, Usuarios y Grupos e instalamos el LDAP Local, luego de ello creamos los usuarios como se muestra continuación.

Figura 42. Creación de usuario.

Una vez creados los usuarios, debemos asociarlos en la cuenta de usuarios de nuestra RoadWarrior VPN.

Seleccionamos Añadir cuenta, luego usuario del sistema y por último seleccionamos el usuario que se vaya a asignar.

Figura 43. Agregación de cuenta.

Anteriormente mencionamos un equipo Ubuntu Desktop con la dirección IP 172.16.1.10. En este espacio lo asignaremos como el servidor Apache y SSH que permitirá a los usuarios de la VPN tener acceso a dichos servicios.

Servicio Apache

Figura 44. Validación de servidor Apache.

Servicio SSH

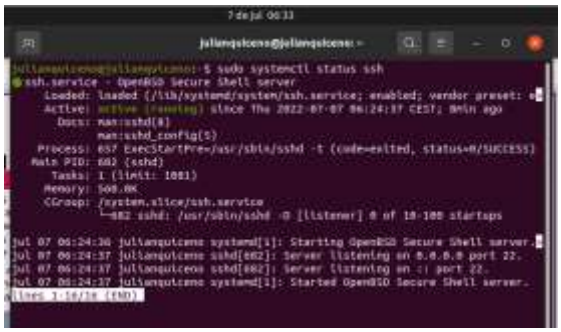

Figura 45. Servicio SSH.

Con todos los parámetros que configuramos anteriormente, estamos preparados para establecer la conexión VPN, haremos prueba de conexión con usuarios en Windows y usuarios en Linux Ubuntu, también estableceremos la VPN de diferentes maneras, en Windows usaremos el software OpenVPN Connect y en Linux utilizaremos la configuración propietaria desde el sistema operativo.

Conexión cliente VPN en Windows:

Una vez instalado el software OpenVPN Connect, este nos solicita un perfil para la conexión, el perfil lo descargaremos desde el Panel de administración de usuarios de nuestra zona Road Warriors en NethServer.

Figura 46. Aplicativo cliente VPN.

Ingresamos a la gestión de nuestro NethServer, nos dirigimos a nuestra zona RoadWarrior, seleccionamos el usuario que deseamos iniciar y descargamos el perfil.

Figura 47. Panel de OpenVPN.

Seleccionamos configuración OpenVPN y descargamos, para luego adjuntarlo en nuestro software OpenVPN Connect

Figura 48. Descarga configuración de cuenta.

Ejecutamos el software OpenVPN Connect y agregamos el perfil que acabamos de descargar,

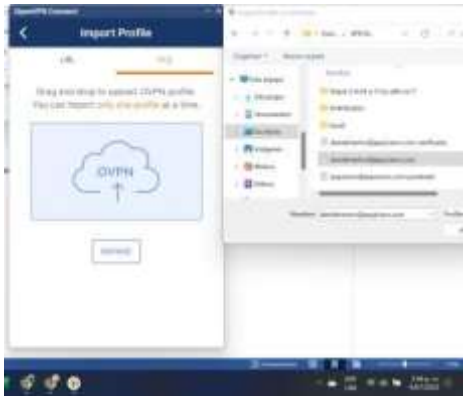

Figura 49. Ejecución de VPN cliente.

Cuando ingresamos el perfil descargado, agregamos la comprobación de usuario y contraseña, seleccionamos Connect y podemos verificar si se logra establecer la conexión.

Figura 50. Conexión establecida.

Una vez establecida la conexión con el software en mención, debemos verificar en el símbolo de sistema de Windows, el direccionamiento asignado y el alcance a las redes mencionadas en el apartado anterior sobre configuración de nuestra RoadWarrior. Logramos evidenciar que al Adaptador VPN, se le asigno una dirección IP en el rango configurado 10.10.10.2 / 24

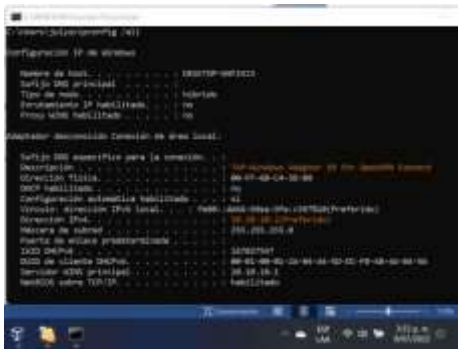

Figura 51. Validación de adaptador de red.

Haremos una prueba de conectividad hacia la IP del servidor 172.16.1.5, la cual se encuentra en otro segmento de la red. Este servidor nos proveerá los diferentes servicios internos por tener la conexión VPN establecida.

Prueba de conectividad exitosa hacia el servidor

Figura 52. Prueba conectividad.

Utilizaremos el software Putty para establecer una conexión SSH a nuestro servidor, servicio que solo se brinda a usuarios conectados a nuestra VPN RoadWarrior. Para establecer la conexión usaremos el puerto 2222 el cual fue cambios por motivos de seguridad

Figura 53. Prueba conectividad con PuTTY.

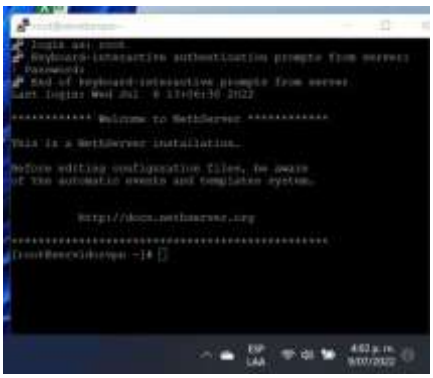

Figura 54. Validación exitosa de prueba.

Haremos una prueba de veracidad de la conexión VPN y su alcance en otras redes internas, gracias a la configuración y puesta en marcha nuestra zona RoadWarrior. Desconectamos el equipo de la VPN, en la gráfica muestra Adapter OpenVPN, medios desconectados. Realizamos

Figura 55. Prueba de veracidad de la conexión.

Realizamos una prueba de ping a la dirección IP del servidor 172.16.1.5 sin respuesta.

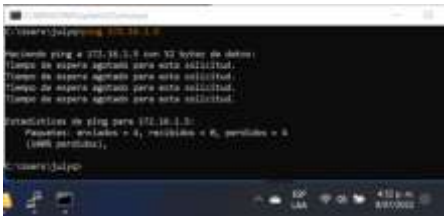

Figura 56. Prueba de Ping.

Iniciaremos juntos la configuración, para establecer la conexión VPN, con el usuario en Linux Ubuntu.

Ingresamos al módulo de configuración de Linux, en semejanza, vendría siendo el panel de control de Windows, allí seleccionamos Red, en sección VPN, hacemos clic en el signo más (+) para agregar y seleccionamos Importar desde un archivo.

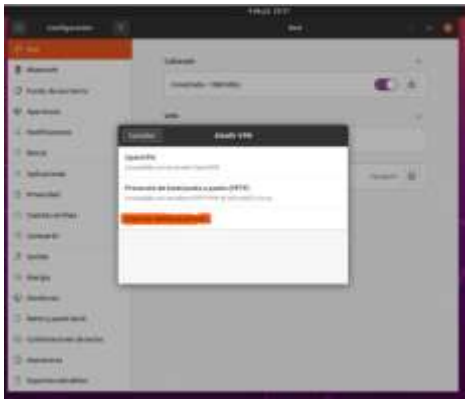

Figura 57. Configuración para nueva VPN.

Debemos agregar un archivo, el cual es el mismo perfil que anteriormente descargamos para establecer la conexión en Windows, una vez agregado se carga toda la configuración, solo resta poner el nombre de VPN que deseemos y agregar la clave del usuario creado en el LDAP y seleccionamos Añadir.

Figura 58. Configuración final VPN.

Lograremos la conexión solo activando el botón morado que aparece en módulo de VPN.

Figura 59. Validación de la conexión.

Validaremos que el equipo haya logrado establecer una conexión a la VPN y que en su interface OpenVPN, tenga el direccionamiento que se asignó desde nuestro servidor. Evidenciamos que el logo VPN se habilito de manera correcta en la barra de tareas

Figura 60. Prendemos la VPN.

Utilizaremos el comando Ifconfig en nuestra consola para validar el direccionamiento entregado, en este caso asigno la dirección IP 10.10.10.3/24 pool valido en la VPN.

Figura 61. Validación de IP.

Pondremos a prueba toda la conectividad de la red VPN, incluso entre los equipos cliente, los cuales están conectados a la VPN en diferentes extremos. Iniciaremos haciendo un ping a la dirección IP del servidor 172.16.1.5

Logramos tener respuesta, por lo tanto, concluimos que tenemos una conexión a la VPN de manera correcta.

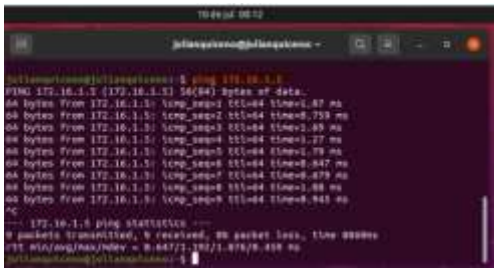

Figura 62. Prueba de Ping a la red de la VPN.

Como parte de un excelente parámetro de administración y control, todo el direccionamiento asignado a los equipos clientes lo podemos ver en nuestra gestión NethServer VPN RoadWarrior

Logramos evidenciar los usuarios conectados a la VPN y las ip asignadas.

Figura 63. Validación de clientes conectados a la VPN.

Haremos otra prueba hacia el equipo Windows, que también se encuentra conectado a la VPN, según la gestión de nuestra VPN, el direccionamiento asignado a danielmerino en la maquina Windows es 10.10.10.2.

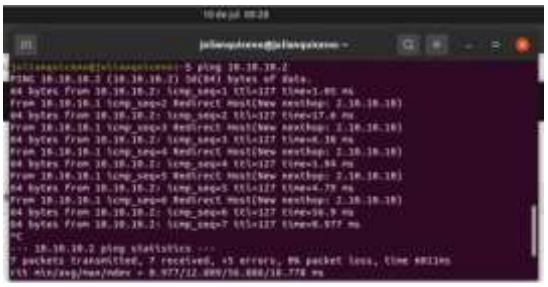

Figura 64. Validación de prueba con Ping.

Sabemos que queremos estar seguros, por lo cual haremos una prueba de ping, desde la maquina cliente en Windows hacia Ubuntu, según el parámetro anterior la Ip del usuario jaquiceno en Linux es 10.10.10.3

Probaremos ahora el servicio SSH desde el equipo cliente en Linux, hacia el servidor el cual tiene la ip de otro segmento 172.16.1.5

Utilizaremos el software Putty para mayor facilidad al cliente, utilizaremos el puerto 2222 para la conexión, ya que se cambió por temas de seguridad.

Figura 65. Prueba de conectividad final.

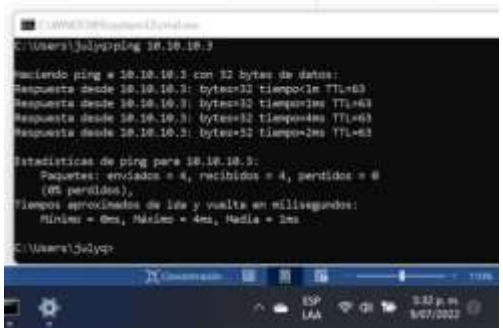

Figura 66. Validación de prueba.

Figura 67. Confirmación de prueba final.

4 CONCLUSIONES

Dentro de las opciones que hay hoy en día para las distribuciones GNU/Linux enfocadas en servidores, podemos decir que Nethserver es una de las más sencillas de instalar, configurar y administrar, ya que cuenta con un diseño y funcionalidad bastante intuitiva y fácil de llevar, igualmente incluye todos los servicios necesarios para abordar las diferentes gestiones y administraciones de los servicios esenciales para pequeñas y medianas empresas.

Siendo así entonces uno de los servidores más sencillos y potentes que existen hoy en día, pues este nos permite cubrir una gran variedad de posibles necesidades que pueda tener un cliente, esto incluiría los servicios como pueden ser: Gestión de red, Servidor de correo, Comunicaciones, Compartición de recursos y trabajo en grupo (Servidor de archivos, Servidor de impresión y groupware), Gestión centralizada de usuarios, Autoridad de certificación, etc.

5 REFERENCIAS

[1] Nethserver Tutorial | Instalación, actualización y primeros pasos 🐣. (2018, 16 octubre). YouTube. Recuperado 10 de julio de 2022, de https://www.youtube.com/watch?v=FNGmM-2fa_0

[2] Nethesis, & NethServer, P. (2022). Proxy web. nethserver.org. Recuperado 10 de julio de 2022, de https://docs.nethserver.org/es/v7/web_proxy.html

[3] Flores, R. (2016). Servidor Proxy con NethServer 6.8. openit.com. Recuperado 10 de julio de 2022, de http://mundo.openit.com.bo/?p=1104

[4] 1. Configuración Básica de Proxy en Nethserver. (2019, 8 mayo). YouTube. Recuperado 10 de julio de 2022, de https://www.youtube.com/watch?v=-G7lZ4-vT6s

[5] 2. Configuración Proxy Nethserver (reglas, usuarios). (2019, 8 mayo). YouTube. Recuperado 10 de julio de 2022, de https://www.youtube.com/watch?v=e1OpcGNhYYo

[6] Nethesis. (2022). Firewall — NethServer 7 Final. NethServer Firewall. https://docs.nethserver.org/es/v7/firewall.html

[7] Nethesis. (2022). VPN — NethServer 7 Final. NethServer VPN. https://docs.nethserver.org/es/v7/vpn.html