CONFIGURACIÓN DE INFRAESTRUCTURA IT CON ZENTYAL SERVER 6.2

Diana Vanessa Miranda Cuesta
e-mail: dvmirandac@unadvirtual.edu.co
Marlon Esteban Girón
e-mail: megironb@unadvirtual.edu.co
Diego Fernando Varela Heredia
e-mail: dvarelah@unadvirtual.edu.co
Carlos Eduardo Agudelo Velasco
e-mail: ceagudelov@unadvirtual.edu.co
Gustavo Adolfo Ramírez Olave
e-mail: garamirezo@unadvirtual.edu.co

RESUMEN: *En este artículo se documenta el proceso de configuración de una estructura IT donde se incluyen servicios para la intranet y extranet. Para ésto, se utilizó el software de virtualización virtualbox, en ésta, se creó una máquina virtual con los requerimientos de hardware (CPU, RAM, RED y DISCO DURO) y se instaló una imagen ISO de zentyal server 6.2. zentyal se utilizó como sistema operativo para la administración de los servicios: servidor DHCP, DNS, controlador de dominio, proxy, reglas firewall, file server, print server y VPN. Para las máquinas clientes se emplearon los sistemas operativos Ubuntu Desktop y Windows 10.*

PALABRAS CLAVE: Controlador de Dominio, Cortafuegos, DHCP Server, DNS Server, File Server, Print Server, Sistema Operativo, GNU/Linux, VPN, Zentyal Server.

1 INTRODUCCIÓN

Los sistemas operativos bajo licencia libre cuentan con diversas distribuciones que son especializadas para la administración de los servicios que cada empresa requiere, estos tienen muchos beneficios debido a que no tienen un costo de licenciamiento, están respaldados por una gran comunidad para soportarlos y cuentan con un alto nivel de seguridad.

Por lo anterior se utilizó Zentyal Server como sistema operativo base para realizar las configuraciones pertinentes y cumplir con los requerimientos planteados por el usuario, de esta manera se puede evidenciar que se puede obtener una estructura IT completa con software libre.

Los principales servicios que se instalaron y configuraron son: el servidor DHCP para asignar las IP a las máquinas cliente, el servidor DNS para la administración de la nomenclatura de la red, el proxy no transparente para delimitar la conexión a internet, definición de las reglas en el cortafuegos para dar acceso o restringir los recursos, la compartición de directorios e impresoras en las estaciones de trabajo y la creación de una VPN que permita establecer conexiones privadas.

2 INSTALACIÓN Y CONFIGURACIÓN INICIAL ZENTYAL

2.1 INSTALACIÓN ZENTYAL

La primera pantalla del proceso de instalación corresponde a la selección del idioma del programa, en este caso se selecciona español.

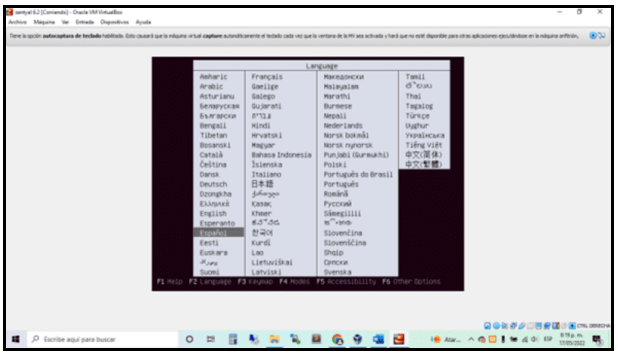

Figura 1. Selección del idioma para Zentyal 6.2.

Posteriormente se muestran las opciones de instalación, se selecciona instalar zentyal 6.2-development (borrar todo el disco), esta opción crea automáticamente las particiones.

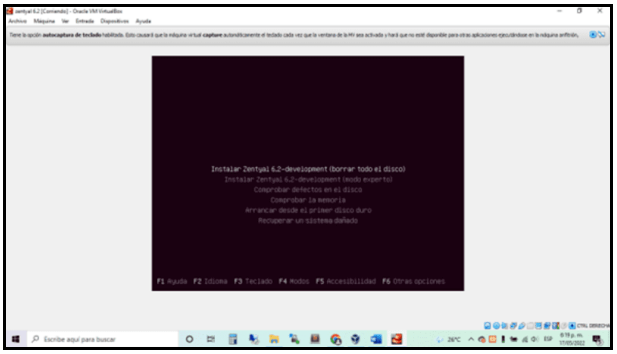

Figura 2. Selección del tipo de instalación para Zentyal 6.2.

Después se selecciona la ubicación, que se utiliza para definir la zona horaria, para la práctica se escoge Colombia.

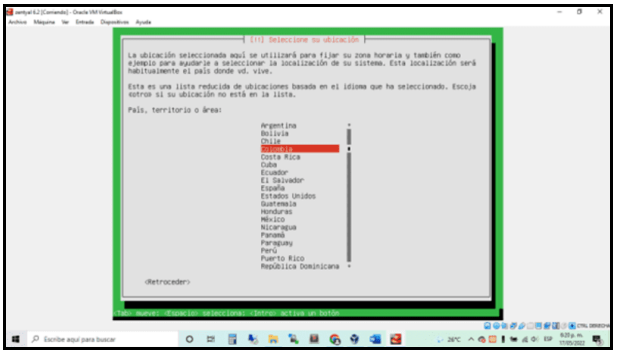

Figura 3. Selección de la ubicación física de Zentyal 6.2.

Se configura el idioma del teclado, para ello se selecciona español (latinoamericano).

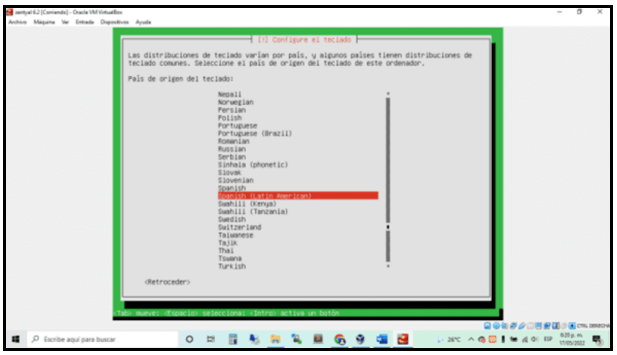

Figura 4. Selección del idioma del teclado de Zentyal 6.2.

Posteriormente se inicia con la configuración de la red, para ello se agrega el nombre como se identificará la máquina.

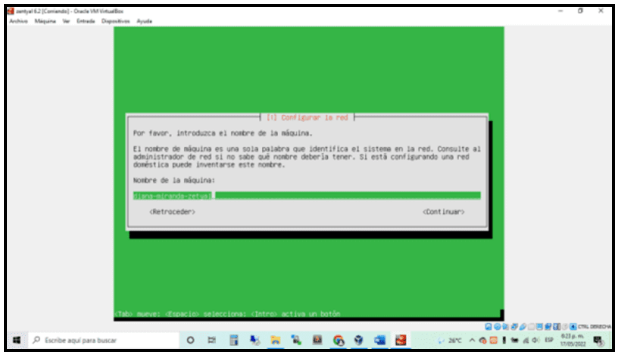

Figura 5. Definición del nombre de la máquina de Zentyal 6.2.

Se configura el nombre de usuario que se creará para acceder al sistema.

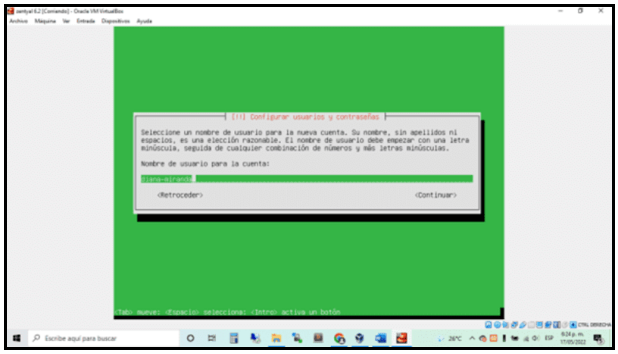

Figura 6. Nombre de usuario para acceder a Zentyal 6.2.

Se configura la contraseña del usuario que se creará para acceder al sistema y posteriormente su respectiva verificación.

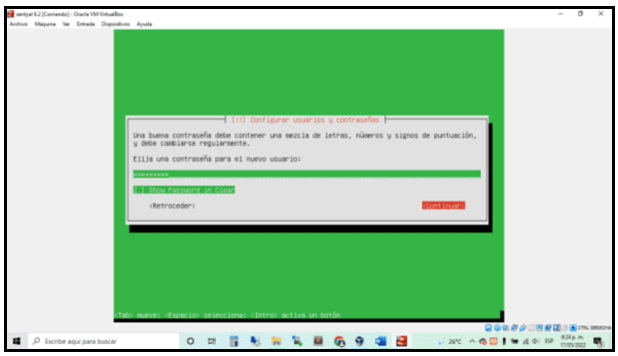

Figura 7. Contraseña de usuario para acceder a Zentyal 6.2.

Valida la zona horaria y solicita la confirmación para la configuración del reloj. Después se reinicia la máquina para que tome la configuración de la instalación.

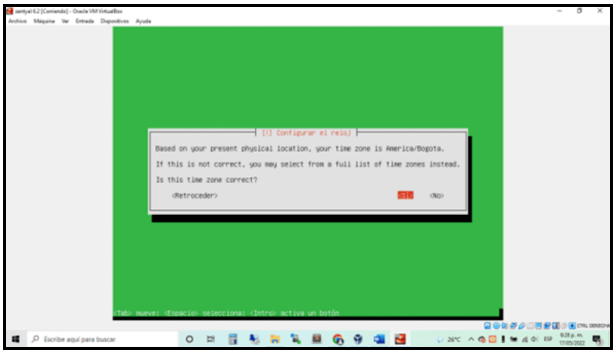

Figura 8. Confirmación de la zona horaria para Zentyal 6.2.

2.2 CONFIGURACIÓN INICIAL ZENTYAL

Página inicial del Zentyal desde su interfaz web, en la cual solicita el usuario y la contraseña que se definieron anteriormente.

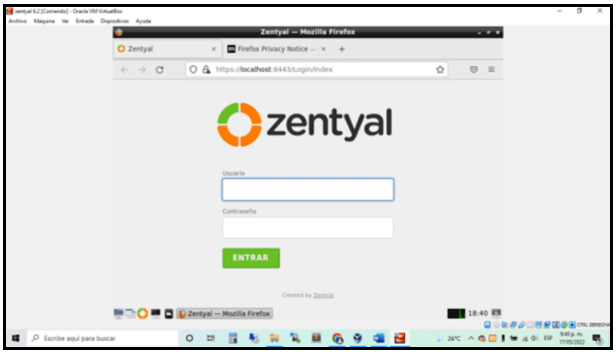

Figura 9. Inicio de sesión en la interfaz web de Zentyal 6.2.

En esta página se seleccionan los servicios que se van a instalar, en este caso se seleccionaron los siguientes:

- Controlador de dominio y uso compartido de archivos.
- Correo y grupos.
- Servidor DNS.
- Servidor DHCP.
- Firewall.
- FTP.

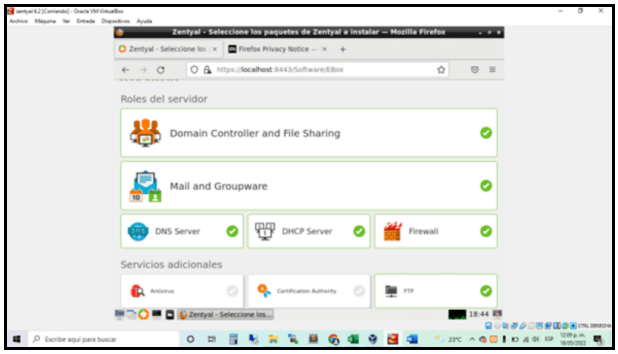

Figura 10. Selección de servicios para instalar desde Zentyal 6.2.

Como se configuró la máquina con un solo adaptador de red, se solicita la configuración de este, la cual se establece como External.

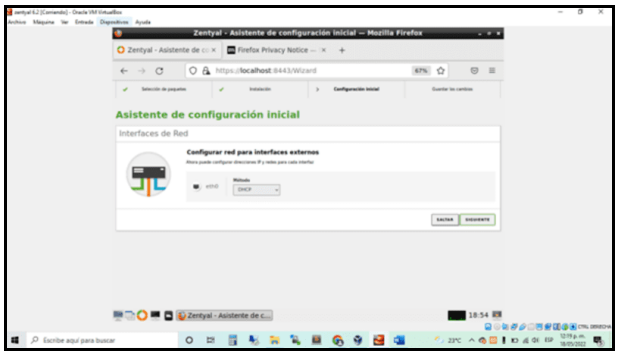

Figura 11. Configuración del adaptador de red en Zentyal 6.2.

Se establece que el método que empleará el adaptador de red es DHCP para tomar una IP de forma dinámica.

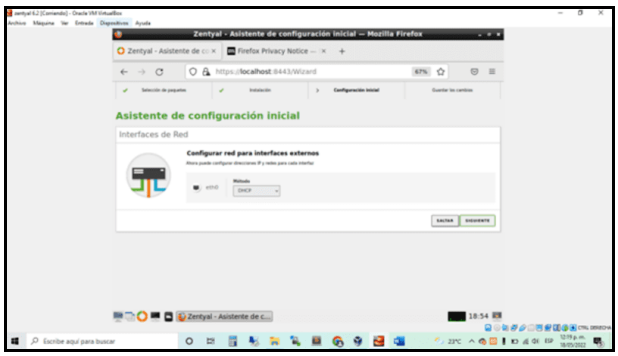

Figura 12. Configuración del método adaptador de red en Zentyal 6.2.

Posteriormente se establece que el tipo de servidor es stand-alone y el nombre de dominio para la máquina es diana-miranda-zentyal.

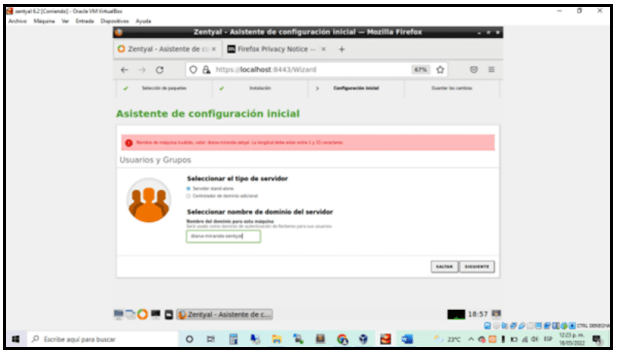

Figura 13. Configuración de usuarios y grupos en Zentyal 6.2.

Se deja por defecto el nombre del dominio virtual de correos.

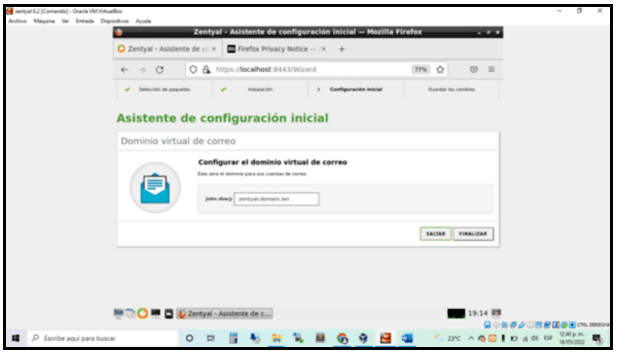

Figura 14. Configuración del nombre de dominio de correos en Zentyal 6.2.

Página donde se confirma la terminación de la instalación.

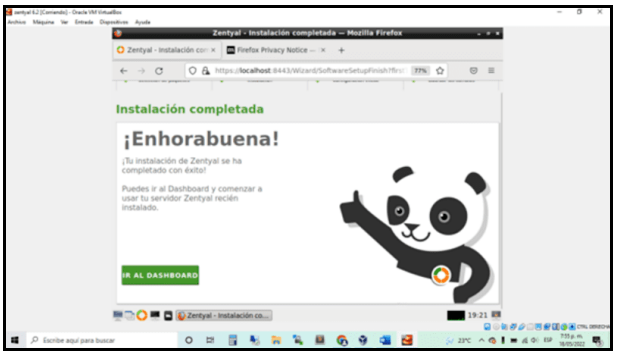

Figura 15. Página de terminación de configuración inicial de Zentyal 6.2.

3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

DHCP Server, DNS Server y Controlador de Dominio. Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Configurar la interfaz 1 de red, asignando una dirección IP.

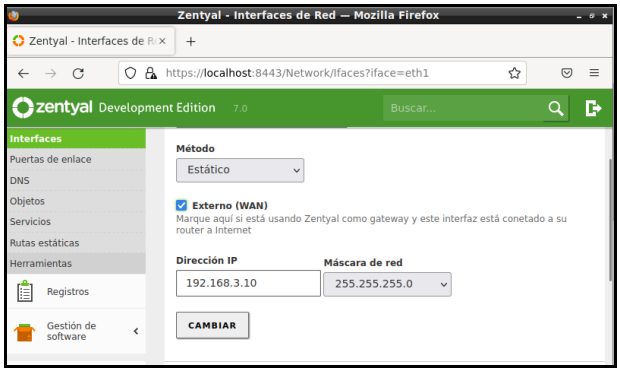

Figura 16. Configuración Tarjeta de red 1.

Ingresar al módulo de DHCP, para asignar los DNS.

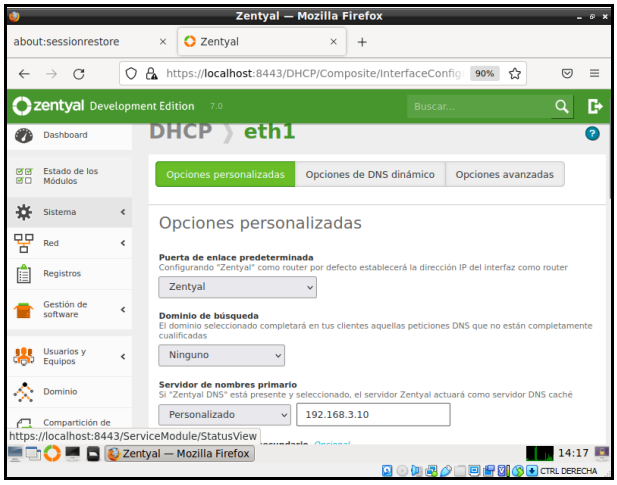

Figura 17. Asignación DNS.

Se configura el rango DHCP para la entrega de las IP desde la 192.168.3.20 hasta la IP 192.168.3.40.

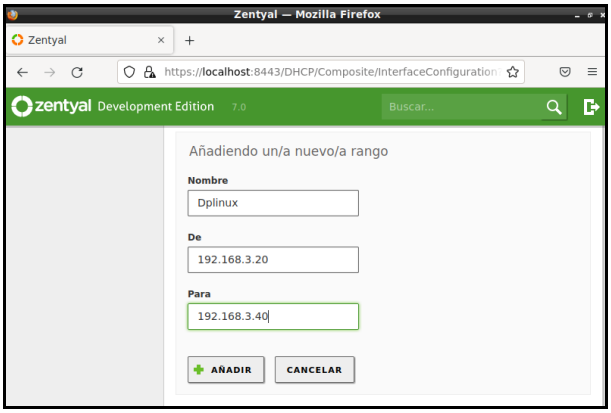

Figura 18. Configuración Pool de IPs a utilizar.

Ahora se carga una máquina virtual de Ubuntu Desktop, y se verifica que asigne una IP dentro del rango 192.168.3.xxx con una terminación de IP que puede ir desde la 20 hasta la 40.

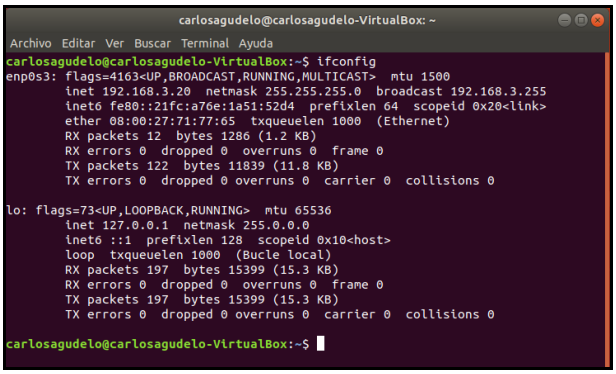

Figura 19. Validación de asignación de IP desde la terminal en una máquina virtual.

Validacion de la IP asignada desde la interfaz del Ubuntu Desktop.

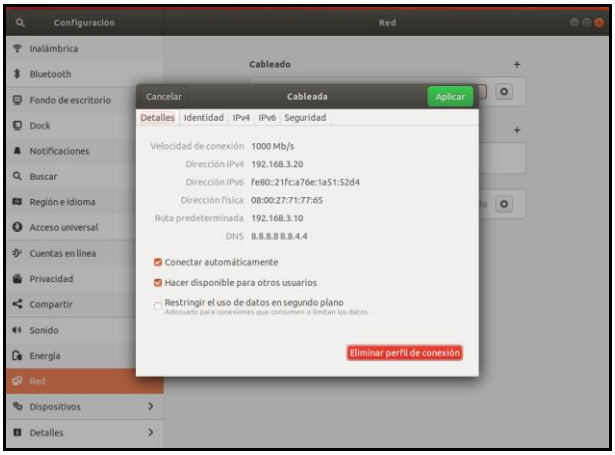

Figura 20. Validación de asignación de IP desde la interfaz gráfica en una máquina virtual.

Se valida en el panel de administración en las IP asignadas por DHCP y se encuentra que la IP 192.168.3.20 esta asignada a la máquina virtual.

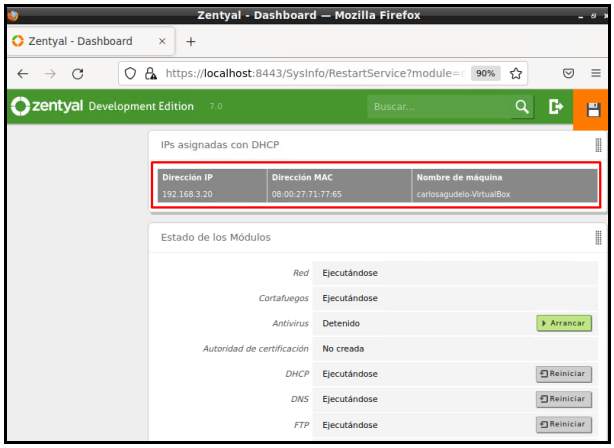

Figura 21. Validación de IP utilizadas en Zentyal.

En el módulo del DNS se valida que su configuración sea la correcta.

Figura 22. Configuración DNS.

Se crea un DNS con el nombre de la máquina.

Figura 23. DNS creado.

Se configura el controlador de dominio, para ello se ingresa al módulo de Dominio, para la realizar la configuración de este.

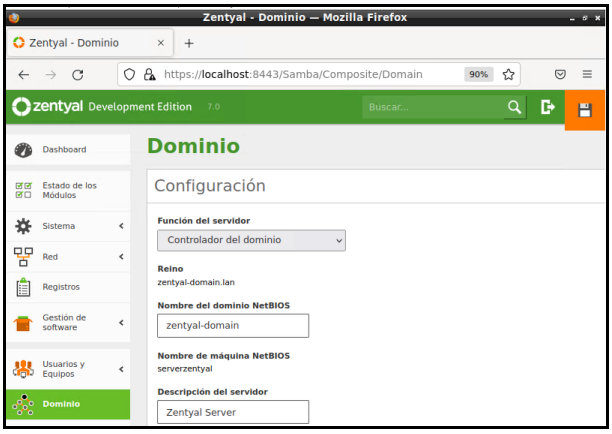

Figura 24. Configuración controladora de dominio.

Ahora se crea un usuario y un equipo en el dominio en el directorio activo.

Figura 25. Creamos usuario.

Se visualiza la lista de los usuarios registrados.

Figura 26. Lista de usuarios.

Se registra un nuevo equipo en el dominio.

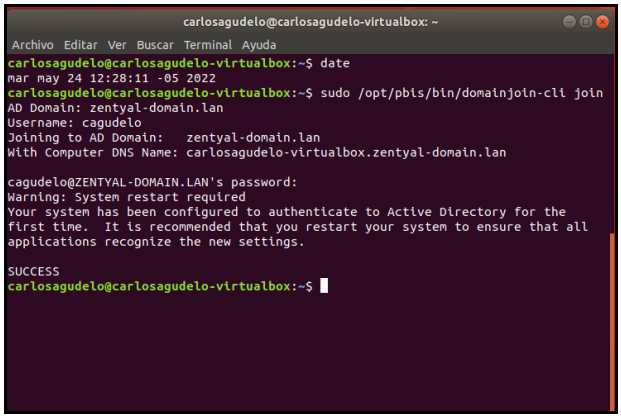

Figura 27. Registro de equipo en el dominio.

Se valida que el directorio activo en el equipo se allá registrado de forma correcta, con lo cual se evidencia que el equipo y el directorio activo o dominio creado tienen comunicación y permite el registro de equipo mediante la validación de un usuario creado.

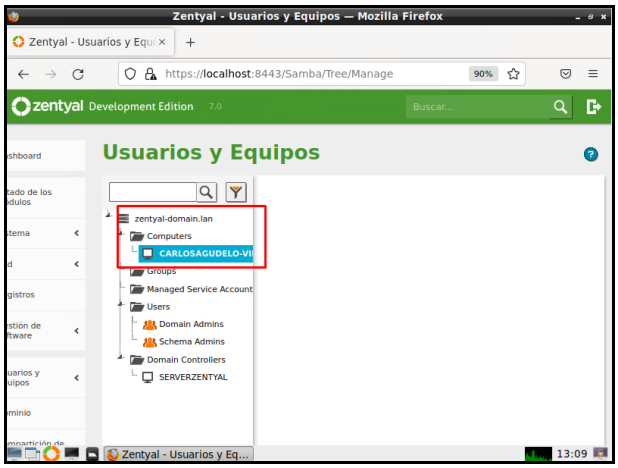

Figura 28. El equipo se registró en el dominio.

4 PROXY NO TRANSPARENTE

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1320.

Se instala el componente HTTP-Proxy. Se ingresa al dashboard y se muestra la instalación realizada en el panel al lado izquierdo de la pantalla.

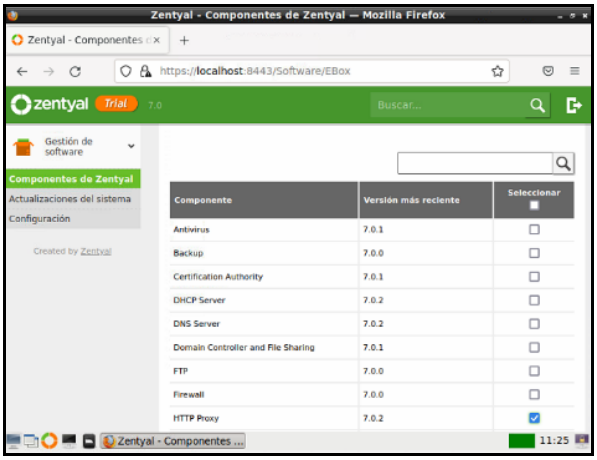

Figura 29. Instalación componente HTTP-PROXY.

Se configura la tarjeta de red externa en método DHCP y se selecciona la opción Externo (WAN).

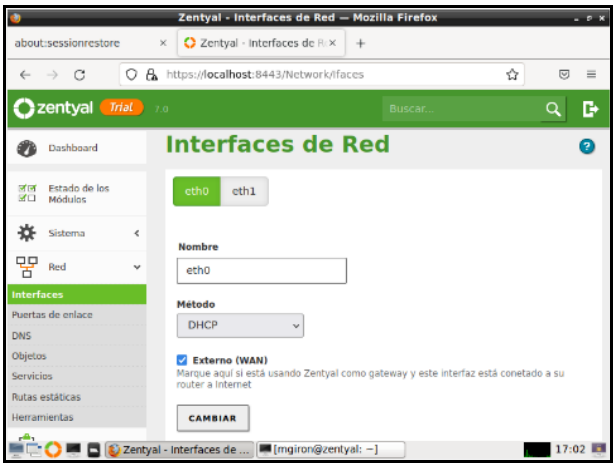

Figura 30. Configuración tarjeta de red externa.

Se configura la tarjeta de red interna, donde se establece por método estático y se le asigna la IP 192.168.10.1 y máscara de red 255.255.255.0.

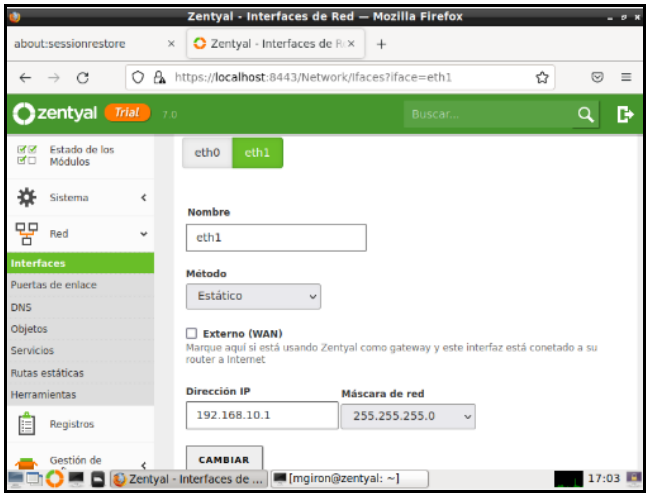

Figura 31. Configuración tarjeta de red interna.

Se crea un objeto para identificar los equipos en red.

Figura 32. Creación de objeto en el módulo de red.

Se debe de agregar el equipo cliente al listado de restricción, dar clic en el icono de miembros para agregar al equipo requerido.

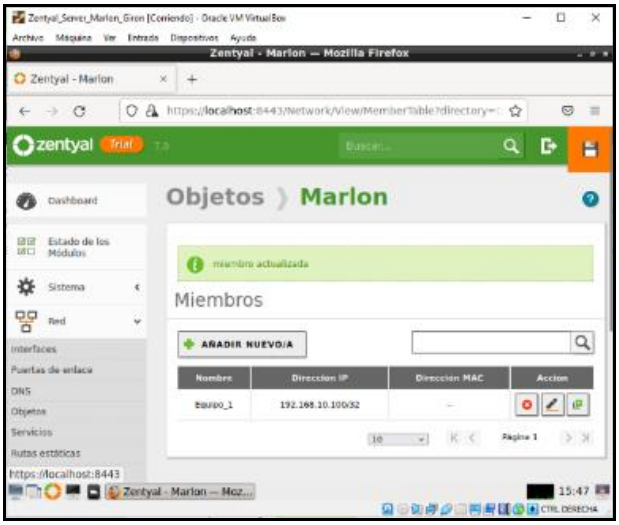

Figura 33. Agregar equipo cliente como miembro del objeto.

En el menú del lado izquierdo ingresar al módulo Proxy HTTP y seleccionar la opción Configuración General. Se valida que la opción proxy transparente no está marcada, en el cuadro puerto ingresar el puerto 1320 y dar clic en el botón CAMBIAR.

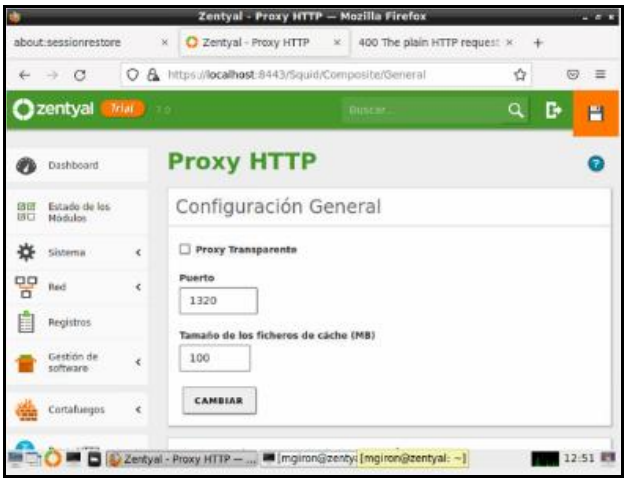

Figura 34. Filtro de salida por medio del puerto 1320.

Se deben de crear las reglas de trabajo, en el menú del lado izquierdo ingresar a Proxy HTTP, seleccionar la opción Reglas de acceso. En el campo origen ingresar el objeto creado para este caso Marlon y en el campo decisión marcar la opción denegar todo, luego dar clic en el botón Añadir.

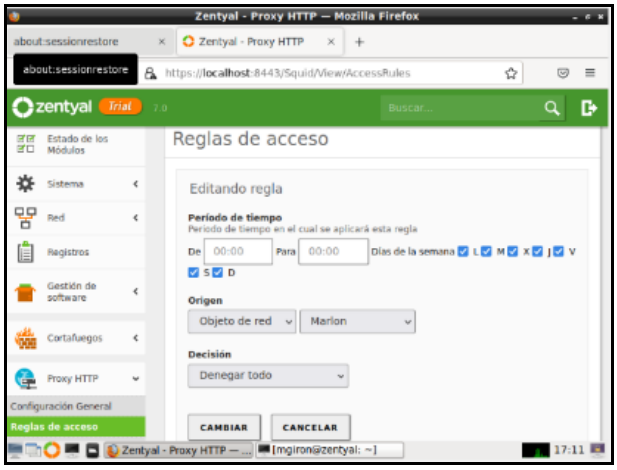

Figura 35. Crear las reglas de acceso.

Equipo cliente con la IP 192.168.10.100.

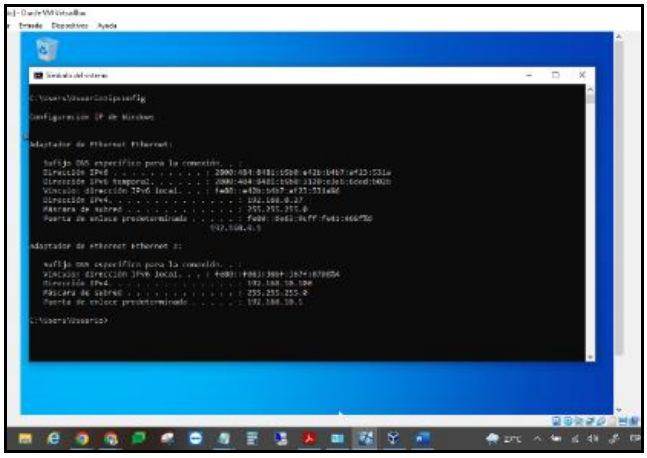

Figura 36. Validación de la IP del equipo cliente.

Dirigirse al equipo cliente y configurar el proxy en las propiedades de internet.

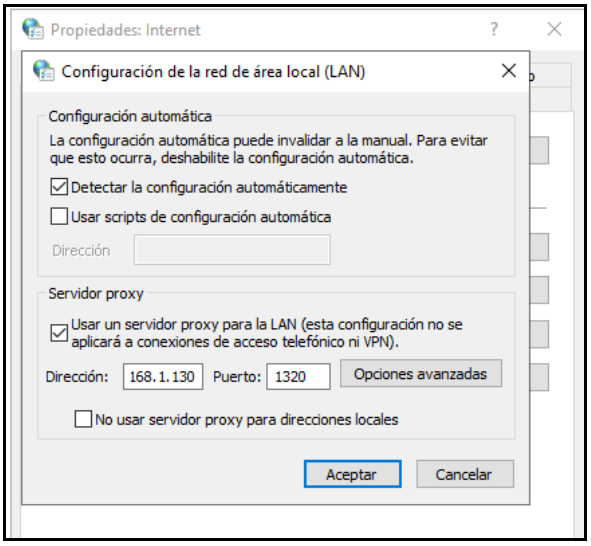

Figura 37. Configuración proxy equipo cliente.

Validar en el navegador web del equipo cliente, al intentar acceder a una página web como www.google.com se puede observar que el servidor Proxy no permite el ingreso ni la conexión al sitio.

Figura 38. Validación de proxy cliente.

Se hace una segunda prueba tratando de ingresar a la página del País (https://www.elpais.com.co/).

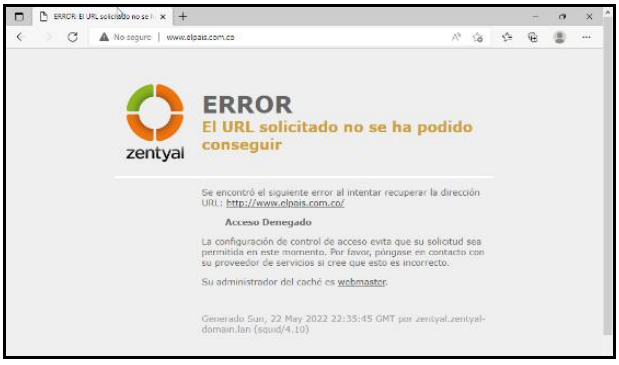

Figura 39. Validación de proxy cliente.

Cambiar la política de acceso en el Zentyal definiendo que permita todo el tráfico sobre el objeto u origen Marlon.

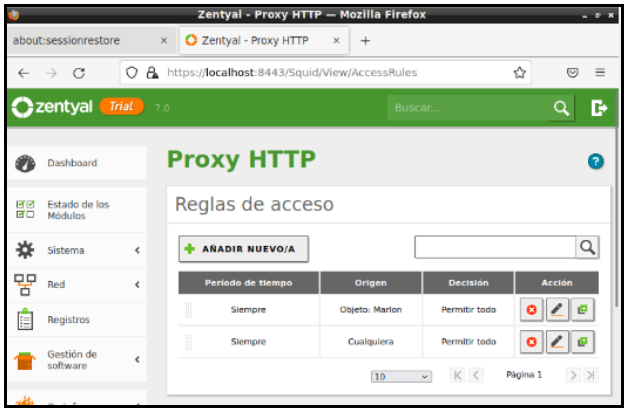

Figura 40. Permitimos todo en reglas de acceso.

Al realizar nuevamente la prueba en el equipo cliente se puede observar que ya permite el acceso a la página web.

Figura 41. Validación de proxy cliente.

5 CORTAFUEGOS

El primer paso es realizar la instalación del cortafuegos.

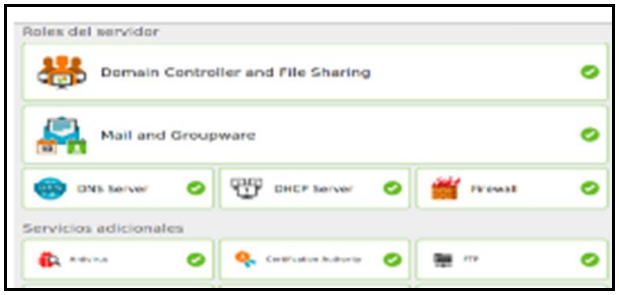

Figura 42. Instalación de DNS Server.

Ahora en el menú lateral se valida que aparezca la opción de cortafuegos.

Figura 43. validación de la instalación de cortafuegos.

Posteriormente se procede a realizar la configuración de la primera tarjeta de red.

Figura 44. Configuración primera tarjera de red.

Después se configura la red eth1 como interna (LAN) con método Estático con IP 192.168.7.254

Figura 45. Configuración segunda tarjera de red.

Se configura en Ubuntu Desktop, la red LAN de manera manual, para que el equipo cliente en Ubuntu, este se pueda conectar a través de la puerta de enlace con el Zentyal Server. En este caso, la puerta de enlace y el servidor DNS apunta a la dirección IP 192.168.7.254.

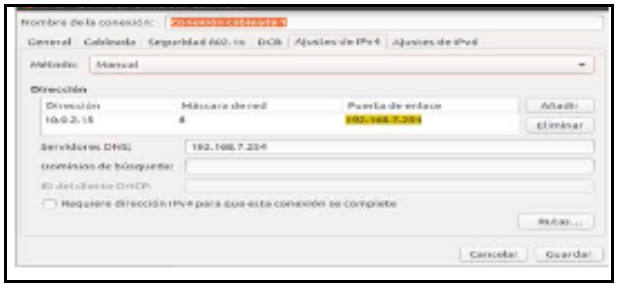

Figura 46. Configuración Ubuntu Desktop.

Es necesario tener presente que antes de crear las reglas, se debe obtener las IPs de los sitios web por intermedio del comando ping. Esto se puede realizar por la opción de Red/Herramientas y allí se digita la página que se necesita obtener la dirección de internet.

Figura 47. Uso de las herramientas de diagnóstico de la red de Zentyal Server.

Resultado de la herramienta de diagnostico de la red.

Figura 48. Resultado de las herramientas de diagnóstico de la red de Zentyal Server.

Para la realización de la practica se va a restringir el acceso a la página de youtube, para ello se realiza ping desde la herramienta de diagnostico de la red para validar el acceso.

Figura 49. Resultado de las herramientas de diagnóstico de la red a youtube.

Ahora se debe de dirigir al menú lateral, seleccionar el cortafuegos y posteriormente filtrado de paquetes.

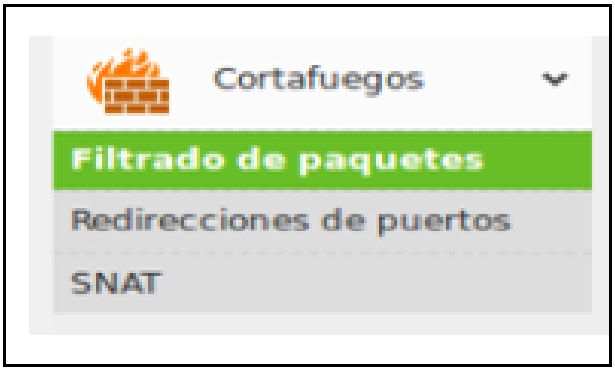

Figura 50. Ingreso a la opción de cortafuegos.

Se crean las reglas de filtrado para las redes internas, solicitadas en la guía como son algunos sitios de entretenimiento o redes sociales como Skype, Facebook y YouTube.

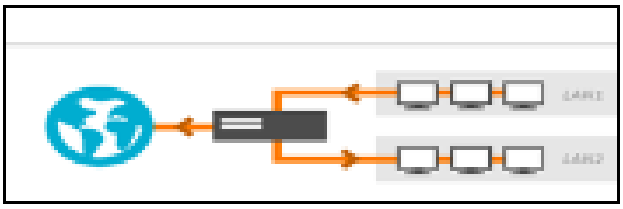

Figura 51. Selección de redes internas.

Posteriormente se muestra una lista de las reglas creadas, para crear las del ejercicio se selecciona el botón de añadir nuevo.

Figura 52. Lista de reglas de las redes internas.

Se procede a ingresar la información necesaria para la creación de la regla, en este caso se define que la decisión es aceptar, el origen es desde cualquier dispositivo y el destino se ingresa la dirección IP.

Figura 53. Formulario para la creación de la regla de las redes internas.

Visualización de las reglas creadas.

Figura 54. Lista de reglas de las redes internas.

Después de que se guarden los cambios realizados, desde Ubuntu Desktop se verifica el acceso a las páginas de entretenimiento y redes sociales.

Figura 55. Lista de reglas de las redes internas.

6 FILE SERVER Y PRINT SERVER

6.1 COMPARTICIÓN DE FICHEROS

Para compartir ficheros se debe de dirigir a la opción de compartición de ficheros que se encuentra en el menú lateral de la interfaz web de Zentyal.

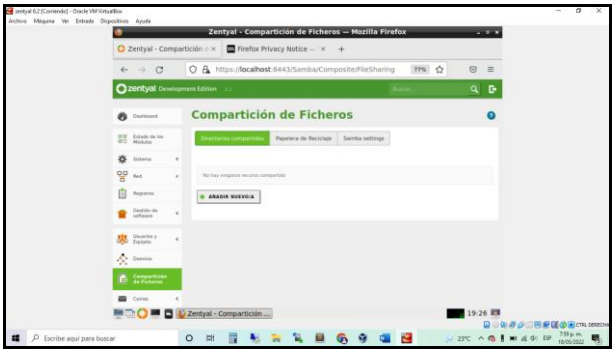

Figura 56. Página de inicio para la compartición de ficheros en Zentyal 6.2.

Se selecciona el botón de añadir nuevo, que direcciona a un formulario donde solicita la siguiente información: validación de habilitación, nombre del recurso a compartir, ruta del recurso, comentario (opcional) y validación de acceso para requerir contraseña.

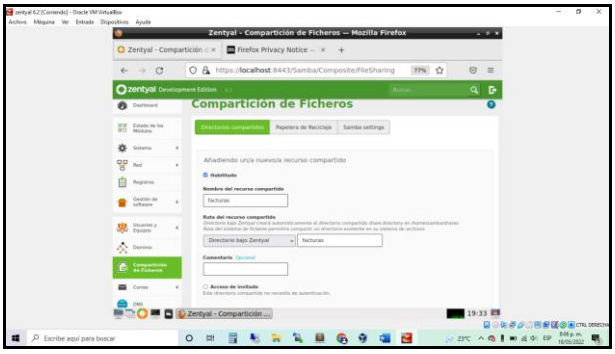

Figura 57. Formulario para registrar directorio compartido en Zentyal 6.2.

Para configurar el control de acceso al directorio compartido, en la lista de los que se han registrado se debe se seleccionar el botón con icono de configuración, este direcciona a una página donde se encuentra la lista de los controles de acceso y el botón de registrar.

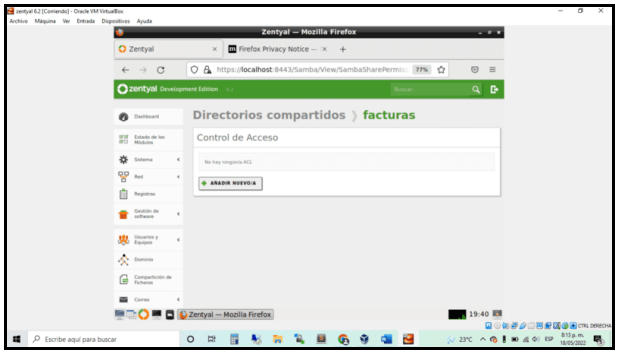

Figura 58. Lista de control de acceso del directorio compartido en Zentyal 6.2.

Se selecciona el botón añadir nuevo, posteriormente se muestra un formulario para registrar el control de acceso al directorio compartido que solicita la siguiente información: grupo y usuarios que tendrán acceso y la definición de los permisos que tendrán.

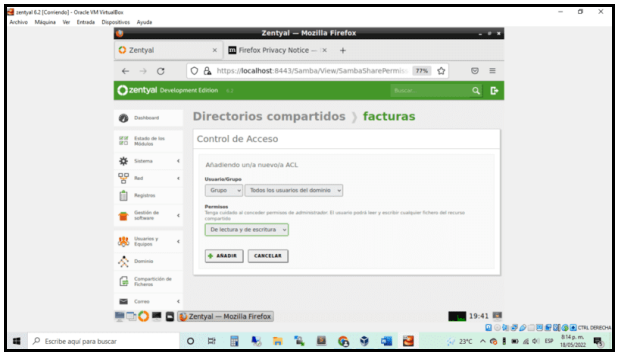

Figura 59. Formulario para registrar el control de acceso al directorio compartido en Zentyal 6.2.

Para tener acceso a los recursos del servidor Zentyal se debe de habilitar desde el fiewall, seleccionar la opción de filtrado de paquetes, después la opción desde redes externas hacia Zentyal, aquí se registra una regla de acceso al servicio de samba.

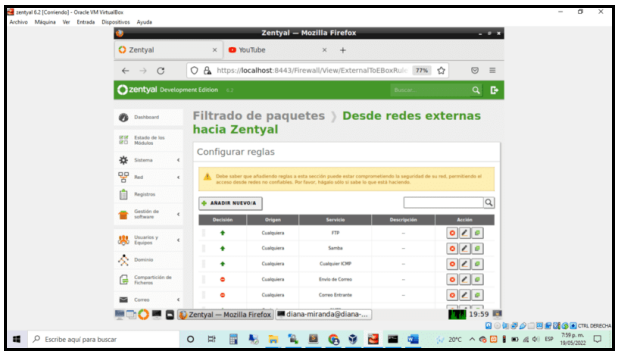

Figura 60. Registro de regla de acceso a recurso en el firewall en Zentyal 6.2.

6.2 COMPARTICIÓN DE IMPRESORAS

Instalación de CUPS desde la terminal de Zentyal, que es un sistema de impresión que utiliza el protocolo de impresión de internet.

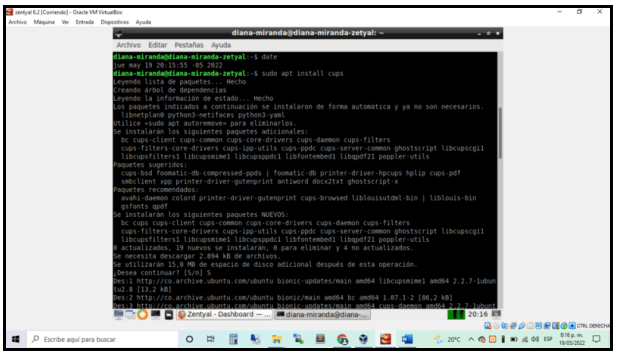

Figura 61. Instalación de CUPS en Zentyal 6.2.

Para acceder a la interfaz web de CUPS se debe de dirigir al navegador, escribir en este caso localhost o en su defecto la IP del servidor Zentyal, acompañado del puerto 631, después solicita las credenciales para validar el acceso.

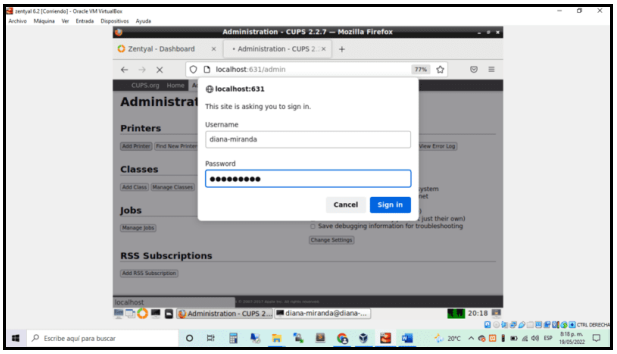

Figura 62. Acceso a la interfaz web de CUPS en Zentyal 6.2.

En el menú principal seleccionar la opción de agregar impresora, el cual da paso a la configuración, para esta práctica se selecciona que la impresora es de red por medio del protocolo de impresión de internet (http).

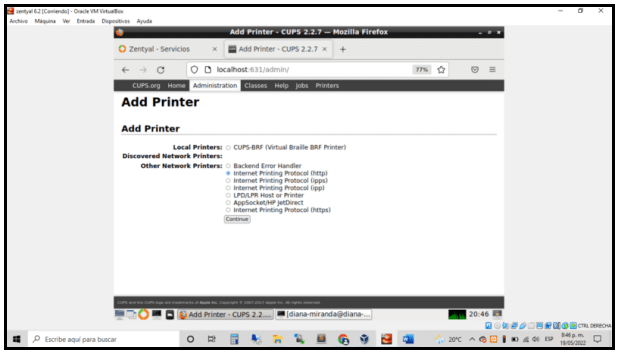

Figura 63. Configuración del protocolo de la nueva impresora en Zentyal 6.2.

Posteriormente se describe la conexión, en este caso se establece la IP del servidor Zentyal y se relaciona un nombre para identificar la impresora.

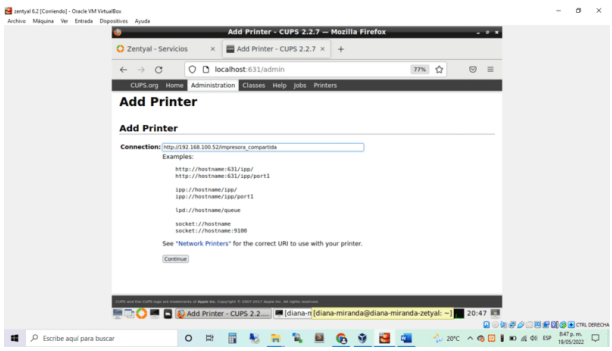

Figura 64. Configuración de la conexión de la nueva impresora en Zentyal 6.2.

Después se agrega la información de la impresora, se establece su nombre, descripción y ubicación, también se habilita la opción para compartir la impresora.

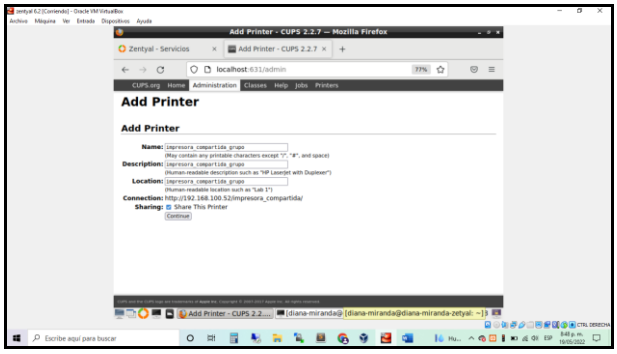

Figura 65. Configuración de la información de la nueva impresora en Zentyal 6.2.

Se selecciona la marca de la impresora.

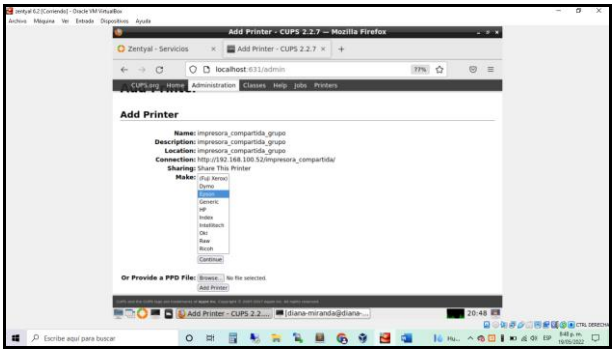

Figura 66. Configuración de la marca de la nueva impresora en Zentyal 6.2.

Se selecciona el modelo de la impresora.

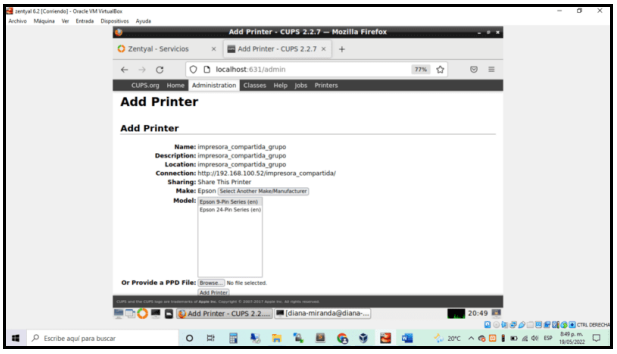

Figura 67. Configuración del modelo de la nueva impresora Zentyal 6.2.

Se establecen las configuraciones de impresión de la impresora, posteriormente se muestra la confirmación de la creación de la impresora.

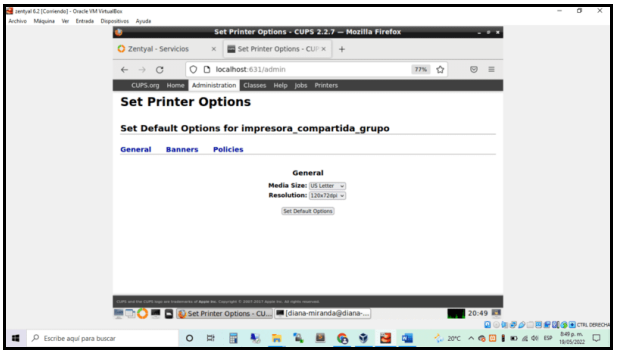

Figura 68. Configuración de impresión de la nueva impresora en Zentyal 6.2.

Para que la impresora pueda aparecer en los recursos compartidos de Zentyal, se debe de modificar el archivo /etc/samba/smb.conf, primero se agrega la línea que se resalta en la siguiente figura.

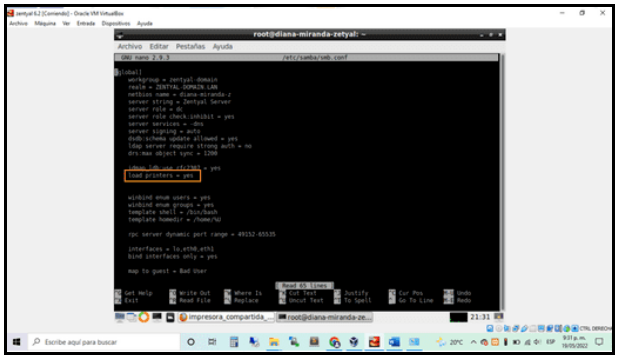

Figura 69. Modificación del archivo de configuración de samba parte 1 en Zentyal 6.2.

Al finalizar el contenido del archivo se agrega el segmento de líneas que se encuentra resultado en la siguiente figura.

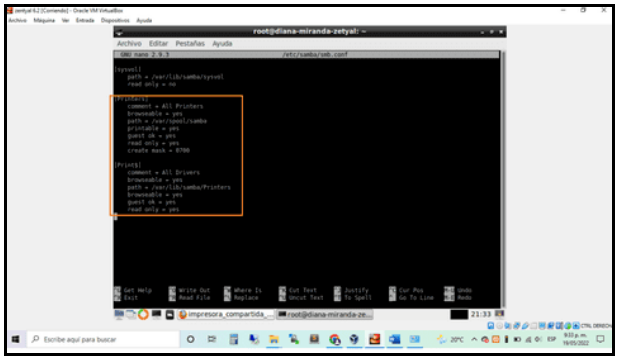

Figura 70. Modificación del archivo de configuración de samba parte 2 en Zentyal 6.2.

Se reinician los servicios de CUPS y samba, posteriormente se valida su estado desde la terminal de comandos.

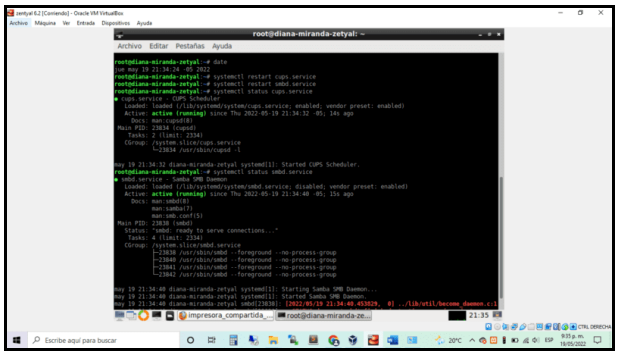

Figura 71. Reinicio de los servicios de CUPS y samba desde en Zentyal 6.2.

Desde la máquina anfitrión se accede a los recursos del servidor Zentyal con las credenciales de usuario, aquí se visualiza los recursos compartidos y la impresora.

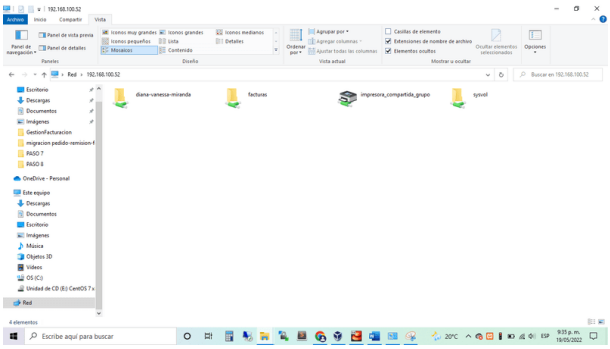

Figura 72. Comprobación de la compartición de los recursos e impresoras de Zentyla desde la máquina anfitrión.

7 VPN

Ejecución del comando apt update && apt upgrade -y desde la terminal en Ubuntu 18.04.

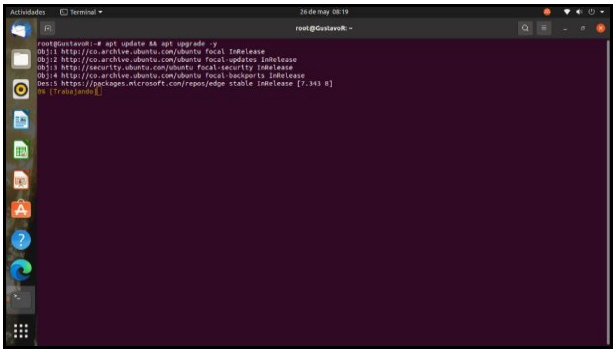

Figura 73. Actualización de los repositorios y paquetes en Ubuntu 18.04.

Para realizar la instalación wireguard se ejecuta el siguiente comando apt install wireguard desde la terminal en Ubuntu 18.04.

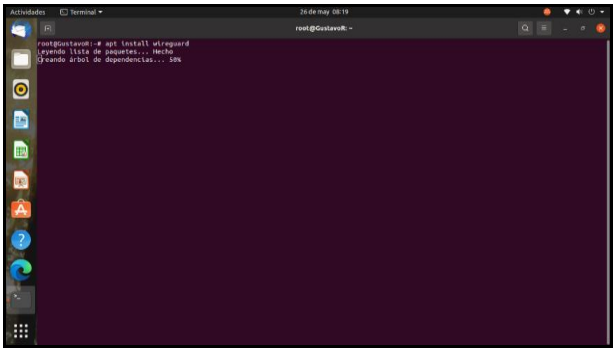

Figura 74. Instalación de wireguard en Ubuntu 18.04.

Para abrir el directorio wireguardse ejecuta el siguiente comando cd /etc/wireguard/ desde la terminal en Ubuntu 18.04.

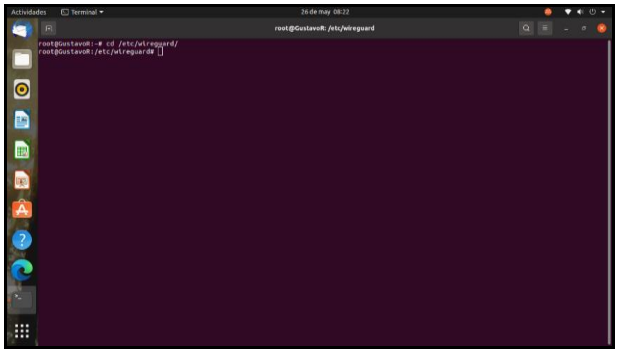

Figura 75. Abrir directorio de wireguard en Ubuntu 18.04.

Para cambiar los permisos se ejecuta el comando umask con el valor 077, para que las claves solo puedan ser leídos por el usuario Root.

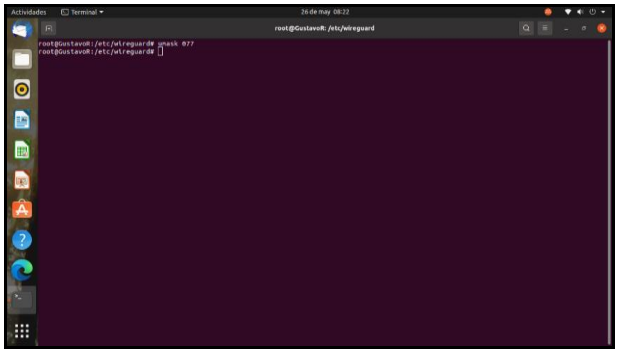

Figura 76. Cambio de los permisos de la carpeta en Ubuntu 18.04.

Se realiza la creación de claves para el servidor, clave pública y privada mediante los comandos wg genkey |tee 00_server_clave_privada | wg pubkey > 00_server_publica desde la terminal en Ubuntu 18.04.

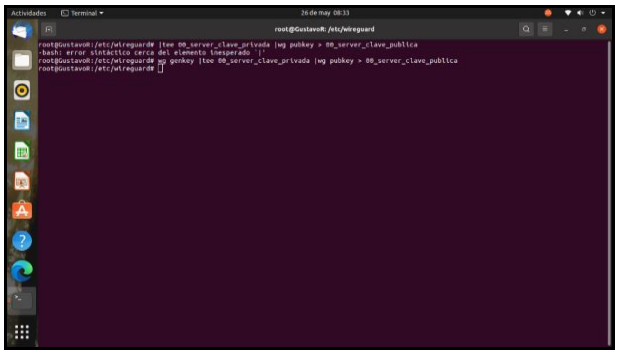

Figura 77. Creación de clave pública y privada para el servidor en Ubuntu 18.04.

Creación de clave pública y privada para el cliente, por medio del comando wg genkey |tee 01_client_clave_privada | wg pubkey > 01_client_publica desde la terminal en Ubuntu 18.04.

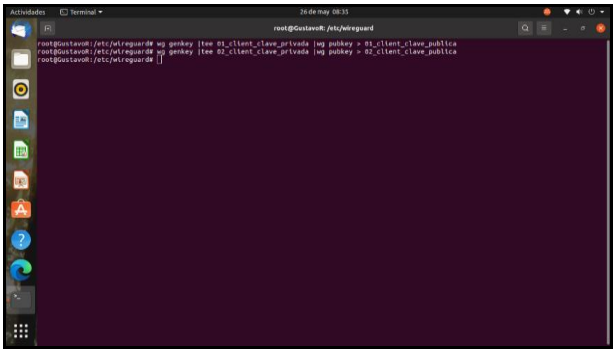

Figura 78. Creación de clave pública y privada para el cliente en Ubuntu 18.04.

Se listan las claves del cliente y servidor para validar la creación de las antesriores, con el comando ls -ln desde la terminal en Ubuntu 18.04.

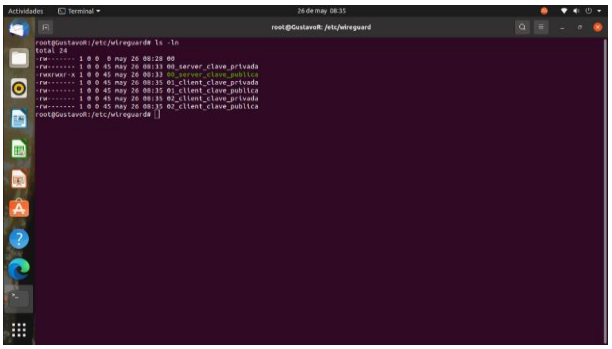

Figura 79. Lista de clave pública y privada para el cliente y el servidor en Ubuntu 18.04.

Se copian y se pegan las claves en un documento de texto.

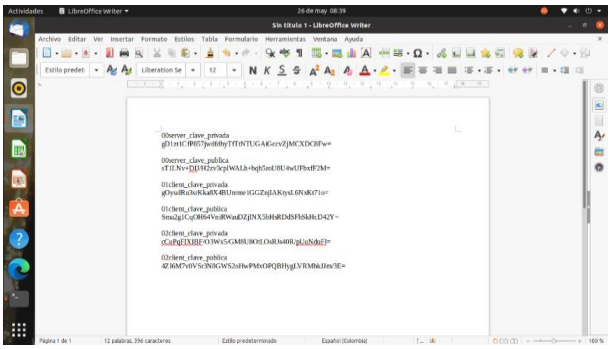

Figura 80. Copiar y pegar las claves del cliente y del servidor en un archivo de texto en Ubuntu 18.04.

Se crea un archivo de configuración del servidor con el comando nano wg0.conf desde la terminal en Ubuntu 18.04.

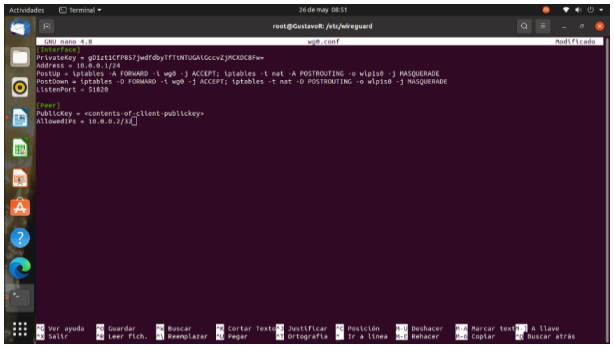

Figura 81. Creación de archivo de configuración Ubuntu 18.04.

Se debe de modificar el archivo del servidor, cambiando la PrivateKey y la PublicKey por las que asignó el sistema y previamente se había guardado en un archivo de texto. La Address es la dirección IP del servidor y la AllowedIPs es la IP para los clientes desde la terminal en Ubuntu 18.04.

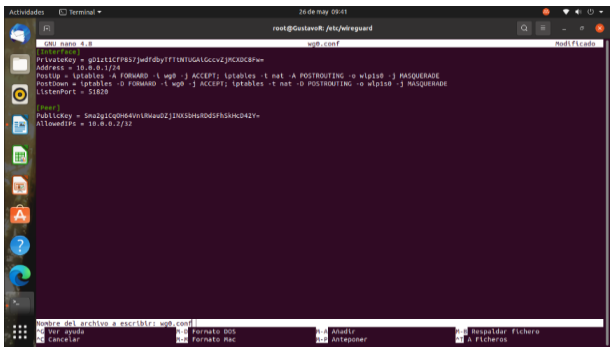

Figura 82. Modificación de archivo de configuración del servidor Ubuntu 18.04.

Activación del reviso de paquetes con el comando sysctl -w net.ipv4.ip_forward=1 desde la terminal en Ubuntu 18.04.

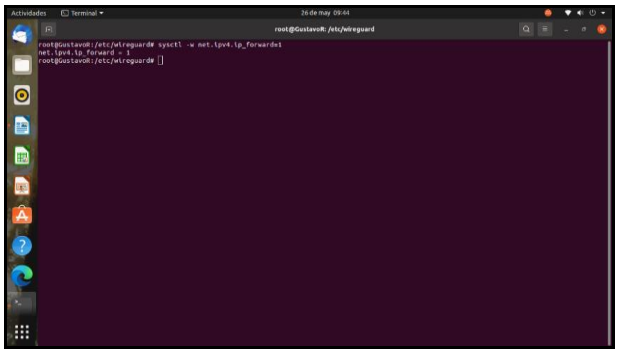

Figura 83. Activación del recibido de paquetes Ubuntu 18.04.

En la máquina cliente que tiene sistema operativo Windows 10, se instala WireGuard.

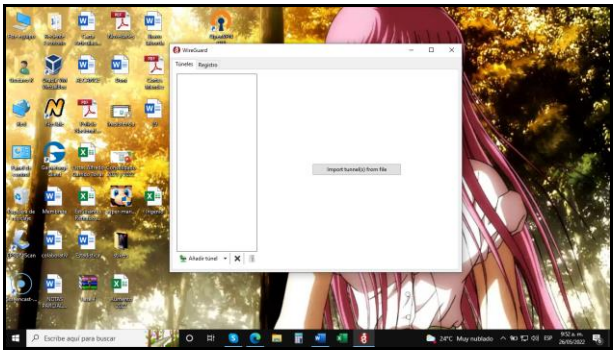

Figura 84. Instalación de WireGuard en Windows 10.

Se selecciona la opción de añadir un nuevo túnel, posteriormente se realiza la configuración de la interfaz de conexión WireGuard en Windows con la clave privada y la clave pública del servidor, finalmente esta se debe de activar.

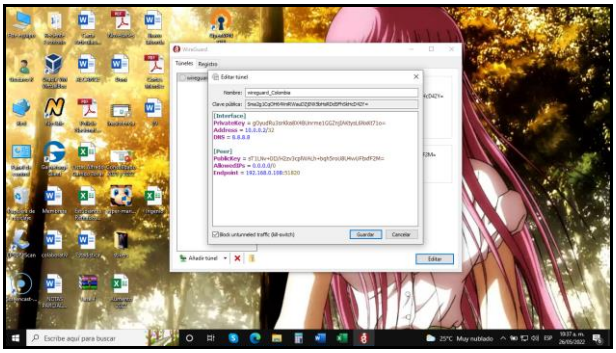

Figura 85. Configuración de la interfaz de conexión en Windows 10.

Se verifica la conexión establecida con el servidor VPN desde el programa WireGuard en Windows10.

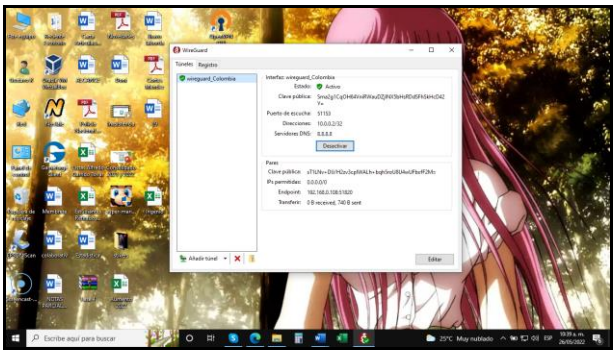

Figura 86. Conexión entre el cliente y el servidor por medio de VPN.

Verificación del envío de paquetes desde WireGuard en Windows hacia servidor.

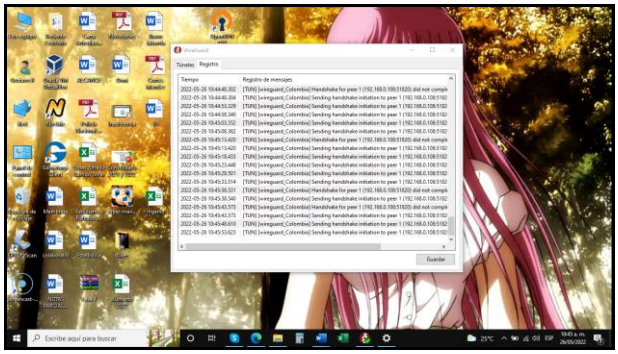

Figura 87. Verificación del envío de paquetes desde el cliente al servidor por medio de VPN.

8 CONCLUSIONES

Toda la configuración de los servicios realizada en Zentyal Server 6.2 se pudo realizar mediante su interfaz web, lo que permite que sea un proceso más fácil e intuitivo al ser esta amigable y fácil de usar.

Se logra identificar y apropiar los conceptos para realizar la configuración de un servidor para la asignación de direcciones IP por DHCP, de igual manera se configura el servicio de dominio.

Mediante el desarrollo de la práctica se evidencia que el servidor Proxy ayuda a tener control sobre las conexiones que se adelantan en una red, para identificar las posibles amenazas de navegación que se pueden presentar.

Los cortafuegos son una necesidad que permite dar confiabilidad en algunos sistemas tanto a nivel empresarial como personal para limitar el acceso a los recursos.

Por medio de la compartición de ficheros e impresoras entre los usuarios de la red, se identificó que esta funcionalidad es importante debido a que permite tener mayor control, aumentar el nivel de disponibilidad y centralizar los recursos tecnológicos.

La implementación de conexiones privadas VPN son muy útiles para restringir el acceso desde el exterior a los recursos de la privados del cliente.

9 REFERENCIAS

[1] Z. Community, «Zentyal 6.2 Official Documentation,» [En línea]. Available: https://doc.zentyal.org/6.2/en/. [Último acceso: 2022 05 20].

[2] J. Gómez López, Administración de sistema operativos. Madrid. Spain: RA-MA Editorial., 2015.

[3] Z. Community, Servicio de configuración de red (DHCP).

[4] R. Velasco, «Protege Linux aprendiendo a usar un Firewall,» 18 09 2021. [En línea]. Available: https://www.softzone.es/linux/tutoriales/firewall-ufw/.

[5] C. Community, «Apple CUPS.,» [En línea]. Available: https://www.cups.org/. [Último acceso: 20 05 2022].

[6] R. J. L. Villada, Instalación y configuración del software de servidor web (UF1271), Madrid. ES: IC Editorial, 2015.