

# FORMULACIÓN DE SOLUCIONES BAJO GNU/LINUX

Aydee Xiomara García Victoria  
axgarcia@unadvirtual.edu.co  
Lina Marcela Ramírez Carvajal  
lramirezcar@unadvirtual.edu.co  
Carlos Jesús Orozco Gelves  
cporozcog@unadvirtual.edu.co  
Jahn Carlos Suárez Serrano  
jcserranos@unadvirtual.edu.co  
Javier Forero Ayala  
jforero@unadvirtual.edu.co

**RESUMEN:** El presente informe es elaborado con el fin de dar solución a una serie de problemáticas planteadas dentro del desarrollo de la actividad del Diplomado de Profundización Linux, dentro de las cuales encontramos: instalación y configuración de Zentyal Server como sistema operativo base para configuración de infraestructura informativa; implementación y configuración de Proxy no transparente; Implementación de cortafuegos para la aplicación de restricciones; configuración de file server y print server; implementación y configuración de VPN.

**PALABRAS CLAVE:** Zentyal Server, proxy no transparente, DHCP Server, DNS server, controlador de dominio, VPN, cortafuegos, file server, print server.

## 1 INTRODUCCIÓN

Para la fase final se desarrollará la administración y control de la distribución Zentyal Server basada en Ubuntu, junto con la versión 18.04 de Ubuntu como cliente, dirigida a la implementación de servicios de infraestructura IT de mayor nivel para intranet y extranet. Se llevará a cabo la configuración detallada del acceso a una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Realización de la administración y el control de la distribución de GNU/Linux basada en Ubuntu, mediante la implementación de servicios de infraestructura desde Zentyal Server como sistema operativo base.

## 2 INSTALACION DE ZENTYAL SERVER

Se procede a instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT, desde una máquina virtual creada en VirtualBox.

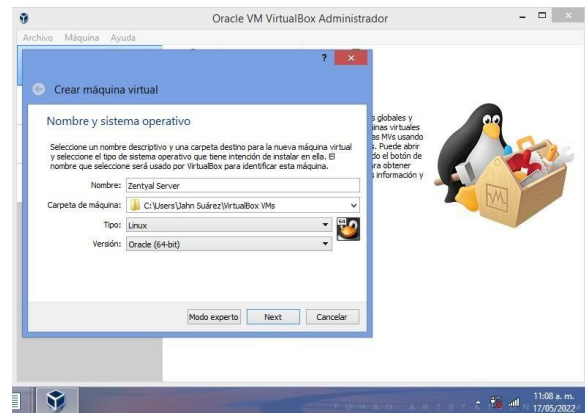


Fig. 1. Creación de máquina virtual

Al iniciar la instalación seleccionamos el idioma sobre el cual se va a trabajar el sistema operativo.

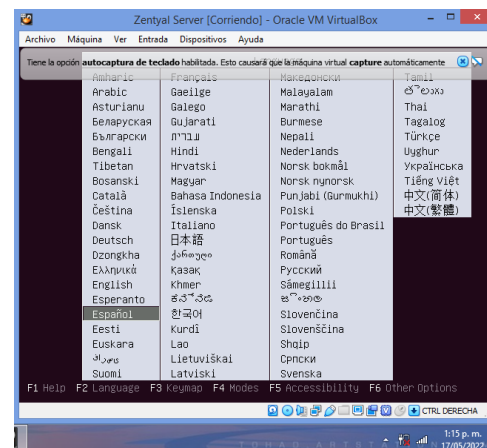


Fig. 2. Selección de idioma

Se establece nombre de usuario para ingreso a la máquina.

### 3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Implementación y configuración detallada del acceso de una estación de trabajo en 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.

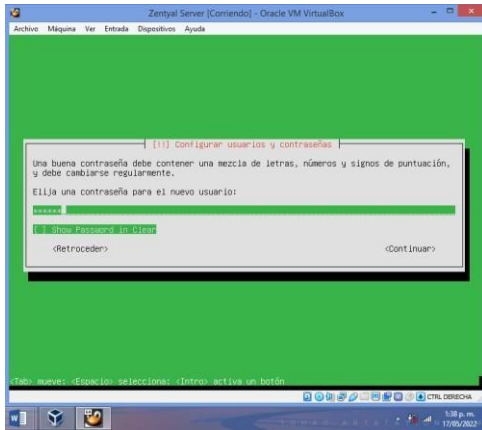


Fig. 3. Nombre de usuario

Se da en continuar para completar la instalación.

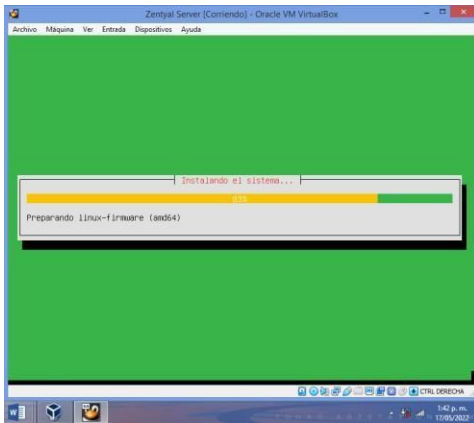


Fig. 4. Terminando instalación

Una vez culminada la instalación se muestra la interfaz gráfica de escritorio Zentyal Server.



Fig. 5. Interfaz escritorio Zentyal

### 3 TEMÁTICAS

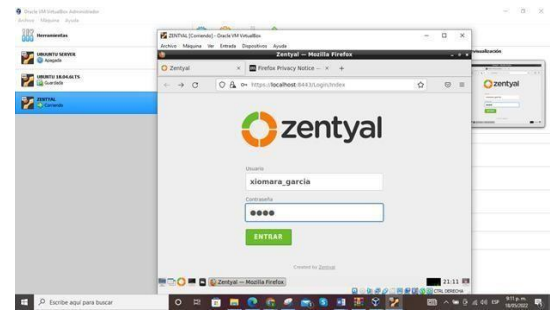


Fig. 6. inicio de zentyal

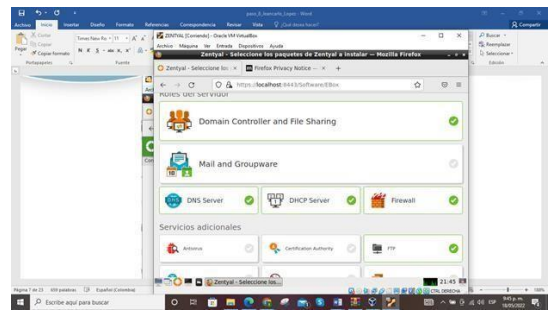


Fig. 7. seleccionamos los paquetes que vamos a instalar

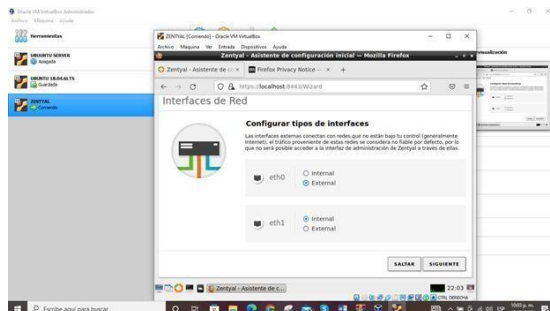


Fig. 8. Procedemos a seleccionar la configuración de tipo de red de interfaces externas, escogemos DHCP y STATIC agregamos la ip 192.168.1.19 y la máscara

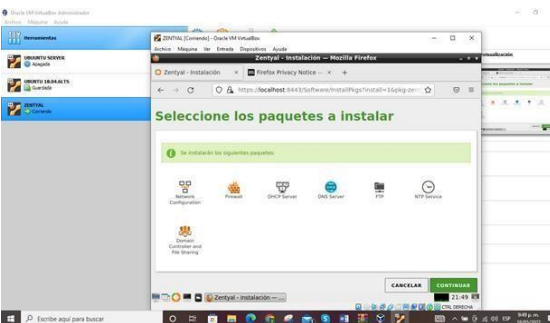


Fig. 9. instalación en proceso

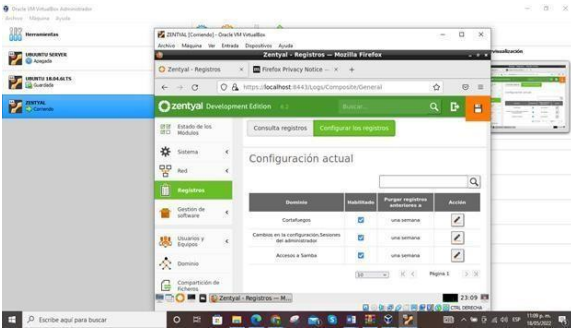


Fig. 10. ingresamos a registro y verificamos la instalación actual y habilitamos los registros de dominio

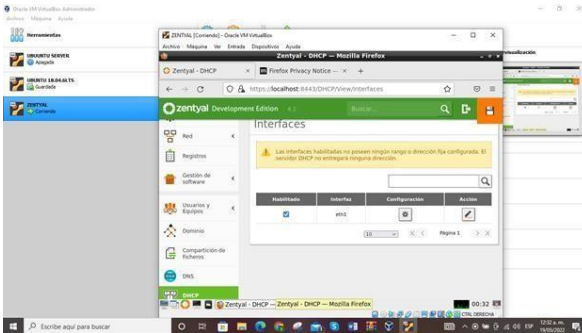


Fig. 11. en el módulo de DHCP entramos a interfaces para su configuración

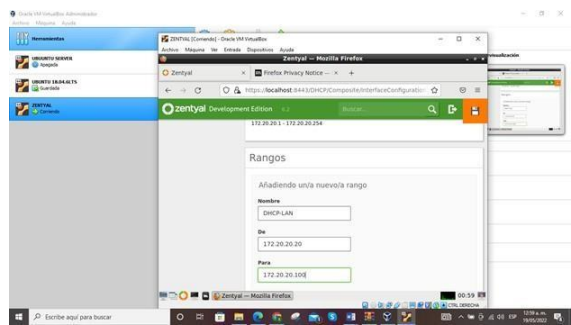


Fig. 12. se asignan rangos ip del DHCP

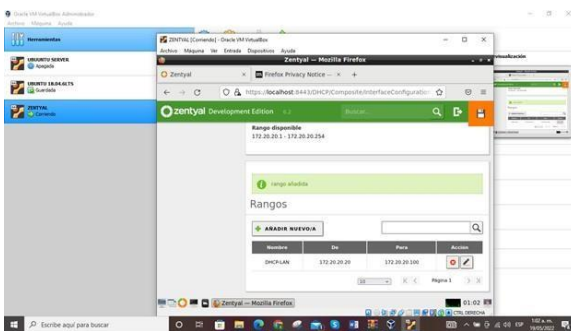


Fig. 13. configuración completa del DHCP

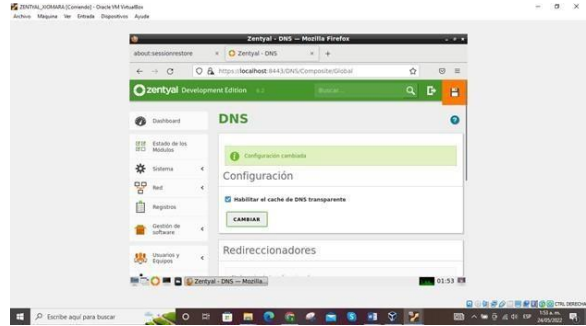


Fig. 14. habilitamos el cache del DNS transparente

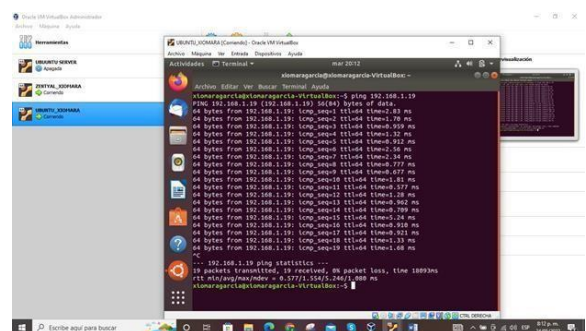


Fig. 15. comprobación de la ip configurada y verificamos la conexión con el cliente Ubuntu

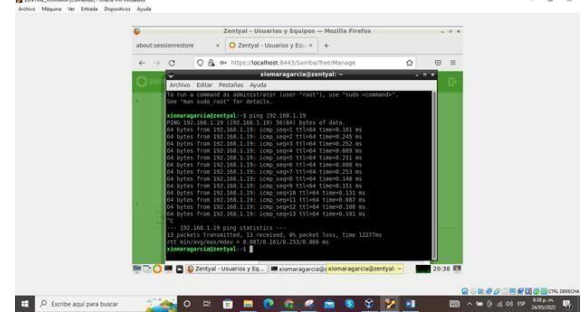


Fig. 16. verificamos la conexión en zentyal

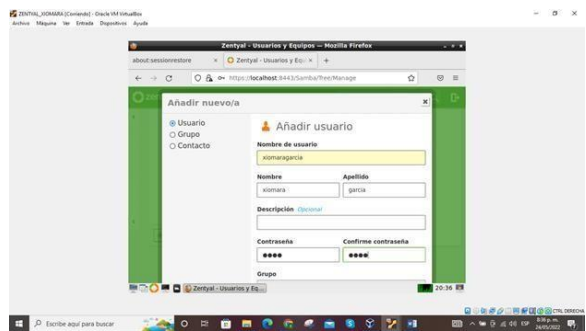


Fig. 17. creamos el usuario que genera el control de dominio

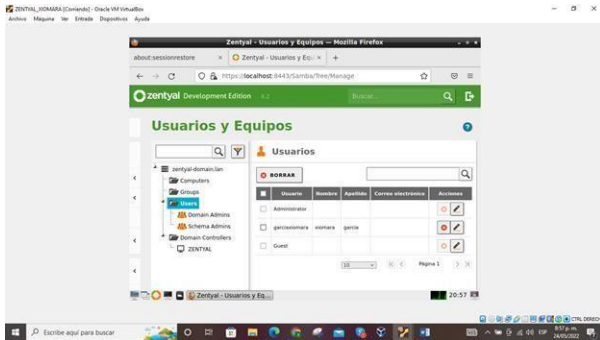


Fig. 18. usuario creado

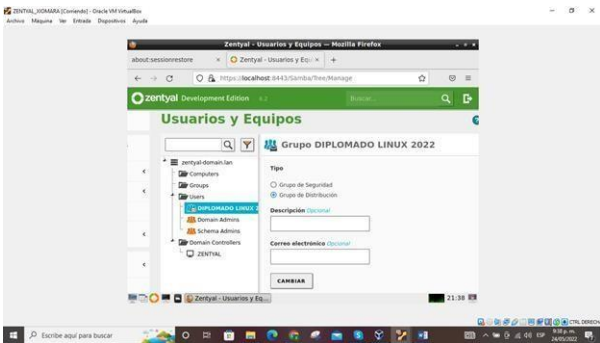


Fig. 19. creamos un grupo

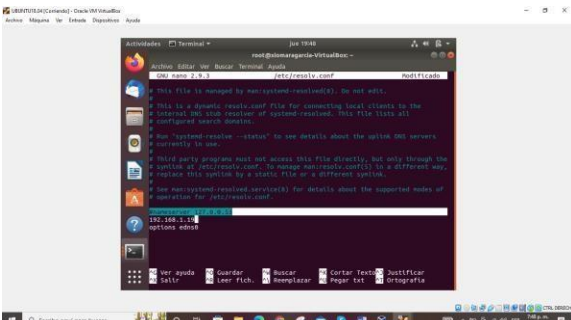


Fig. 20. Se ingresa por la terminal con el comando sudo y editamos el nameserver del equipo

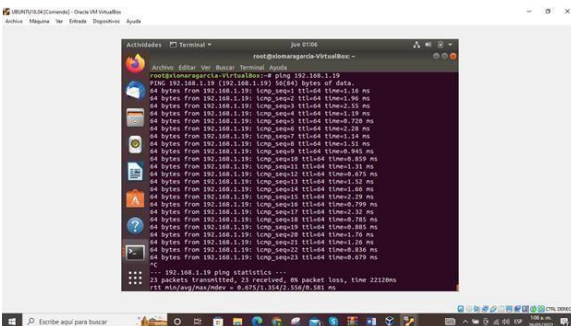


Figura 21. Verificamos su funcionalidad

### 3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

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.

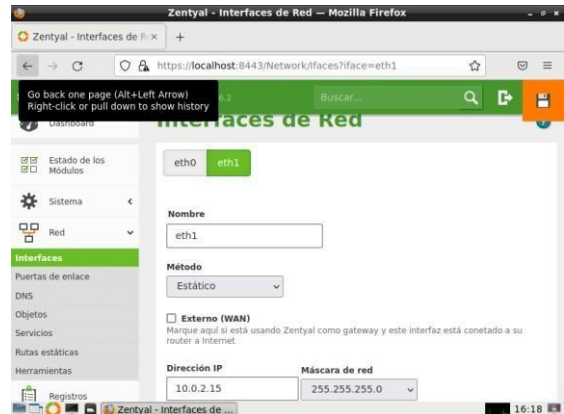


Fig. 22. Configuración de interfaz de red.

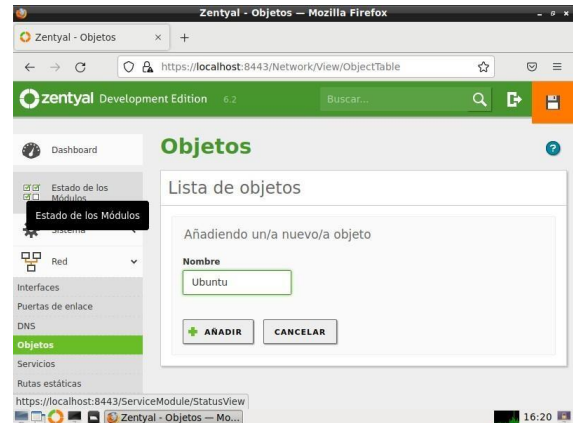


Fig. 23. Creación de objeto

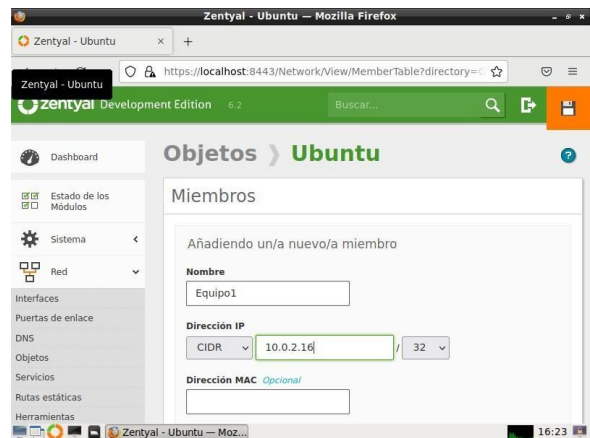


Fig. 24. Modificación miembro

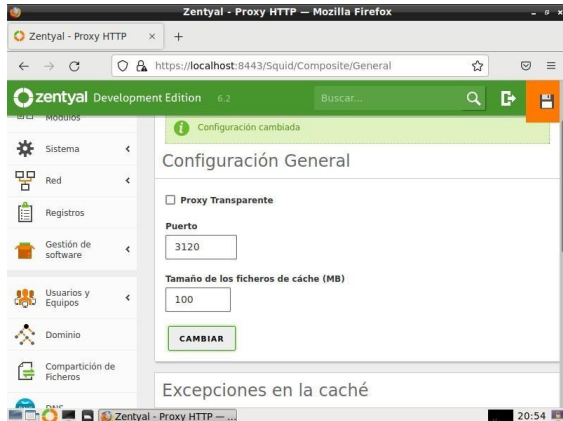


Fig. 25. Configuración regla de acceso, Proxy HTTP

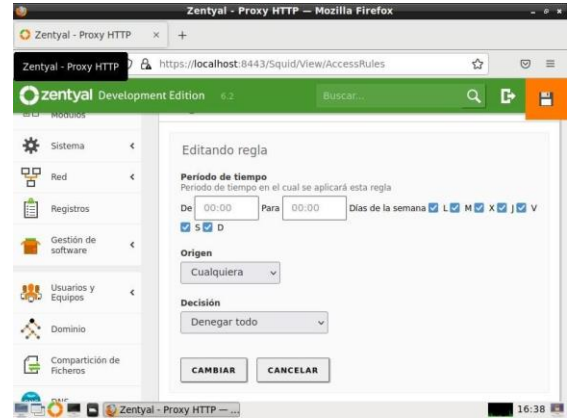


Fig. 28. Edición regla de acceso

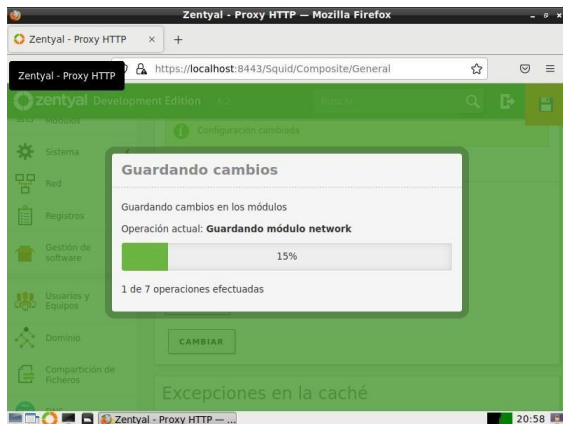


Fig. 26. Cambiamos y guardamos cambios

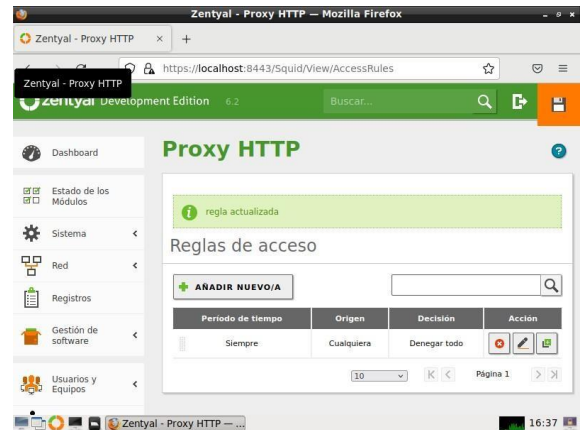


Fig. 29. Denegar todo en decisión

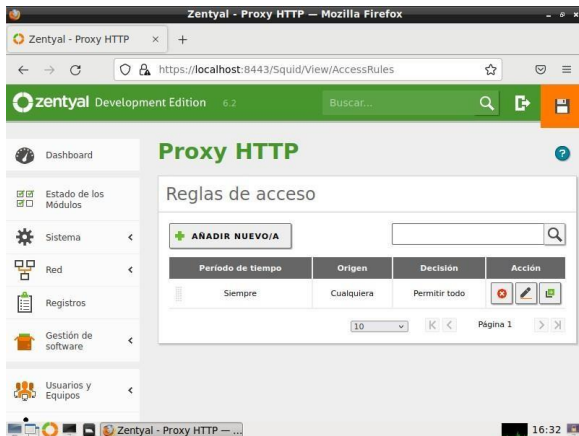


Fig. 27. Regla de acceso

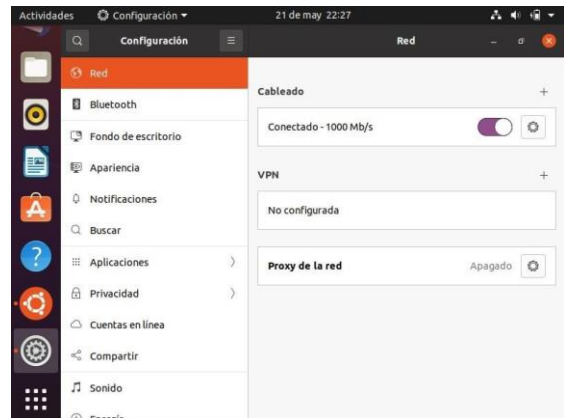


Fig. 30. Configuración Proxy de la red Ubuntu.

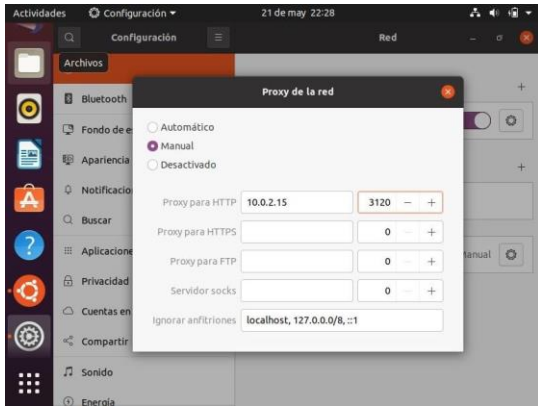


Fig. 31. Ingresamos Proxy y número de puerto a filtrar.

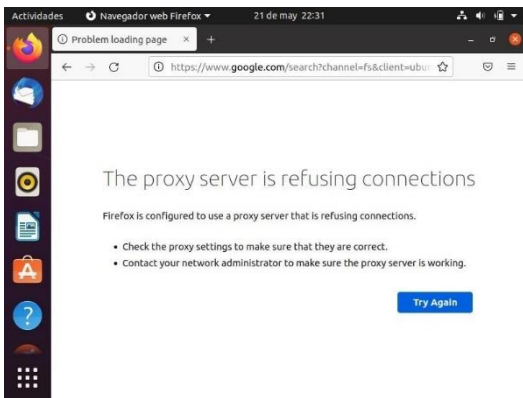


Fig. 32. Verificación de aplicación de la regla.

### 3.3 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 3 del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Primero ingresamos las credenciales que se crearon al momento de instalar Zentyal server.

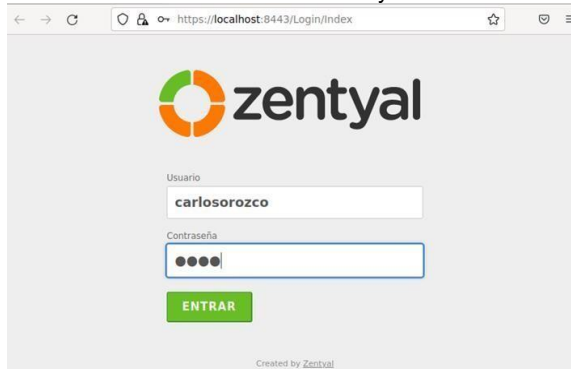


Fig 33. Credenciales de acceso.

Luego de ingresar nuestras credenciales e ingresar al Zentyal nos saldrá la configuración inicial, daremos clic en continuar para luego instalar los componentes necesarios para mi temática, los cuales son el DNS y Firewall.

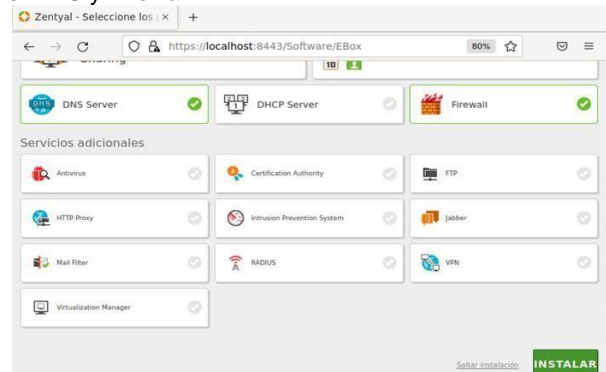


Fig. 34. Instalación de componentes

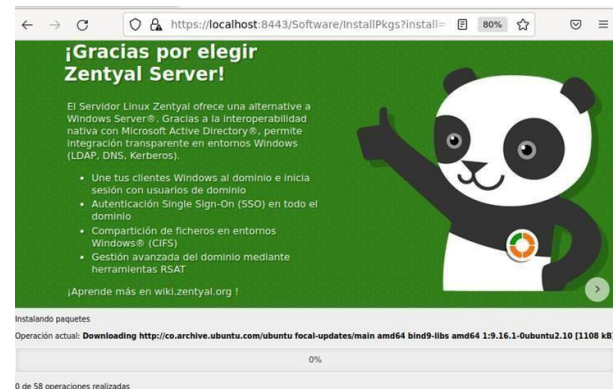


Fig. 35. Proceso de Instalación.

Al terminar el proceso de instalación nos saldrá la configuración para los tipos de interfaces, en este caso la dejo como interna.

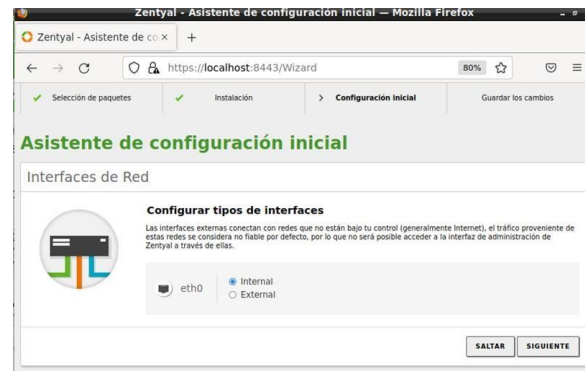


Fig. 36 Configuración de interfaces

En seguida de configurar nuestras interfaces damos clic en siguiente y se empezaran a guardar los cambios.

Luego de terminada la instalación, damos clic en ir al escritorio, luego de ello nos dirigimos al componente cortafuegos e ingresamos al filtrado de paquetes, posteriormente nos dirigimos a la configuración de reglas, mediante las reglas de filtrado desde las redes internas a zentyal.

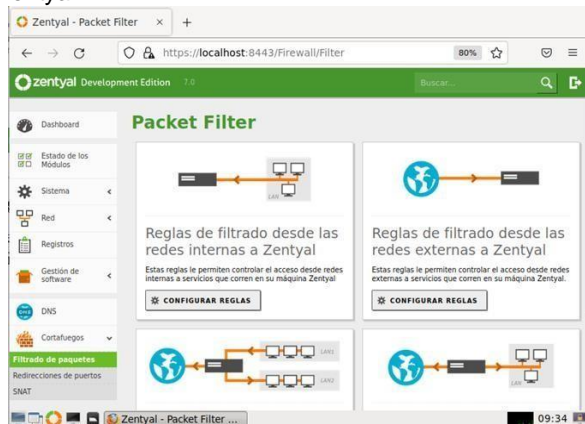


Fig. 37. Filtrado de paquetes

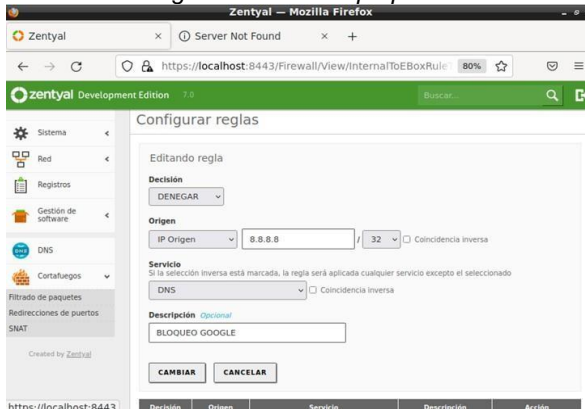


Fig. 38. Configuración de nueva regla

Al guardar los cambios se evidenciará la regla que se agregó.

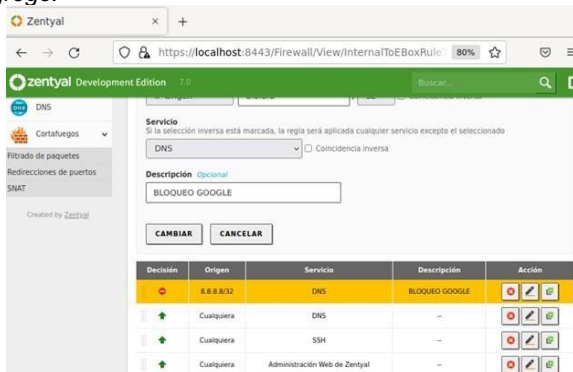


Fig. 39. Regla agregada

Posteriormente de agregar la regla en el componente Firewall nos dirigimos al componente DNS en donde escribiremos el redireccionamiento 8.8.8.8

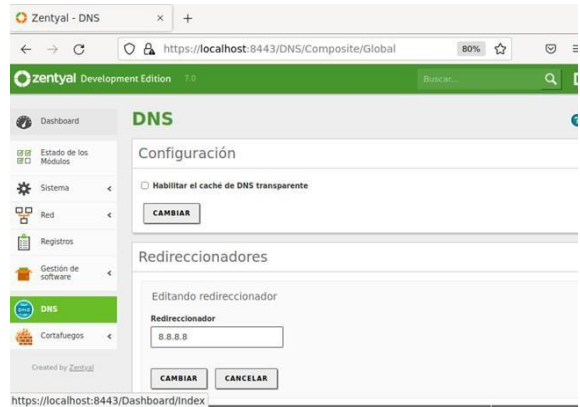


Fig. 40. Redireccionamiento

En seguida realizamos la configuración del dominio la cual sería en este caso google.com



Fig. 41. Dominio Google.com

Luego de realizar los cambios comprobamos abriendo una nueva pestaña en nuestro navegador y escribimos www.google.com

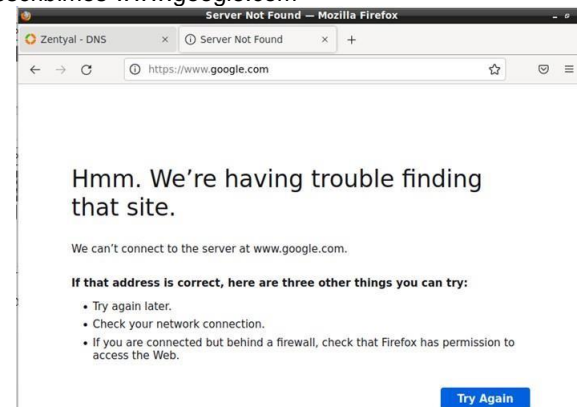


Fig. 42. Comprobación

### 3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Damos acceso desde el navegador con el usuario y contraseña que se creó anteriormente al servidor de Zentyal.

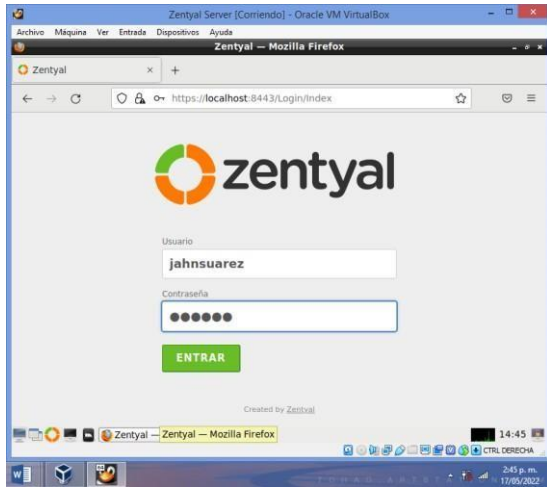


Fig 43. Login Zentyal

En el asistente de configuración inicial se procede a seleccionar el tipo de servidor, en este caso servidor Stand-alo

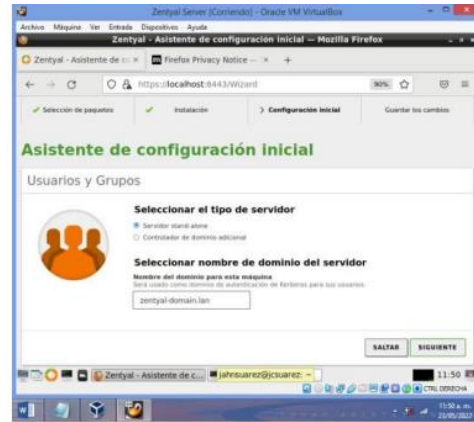


Fig. 46. Asistente de configuración inicial



Fig. 44. Paquetes Zentyal

Una vez seleccionados se inicia la instalación de los paquetes, los cuales van a permitir disponer de los diferentes servicios.



Fig. 45. Progreso de instalación

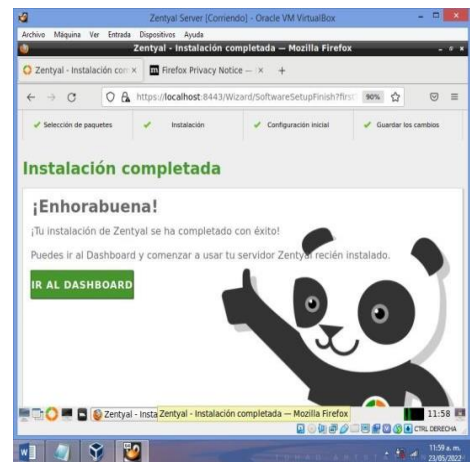


Fig. 47. Instalación completada

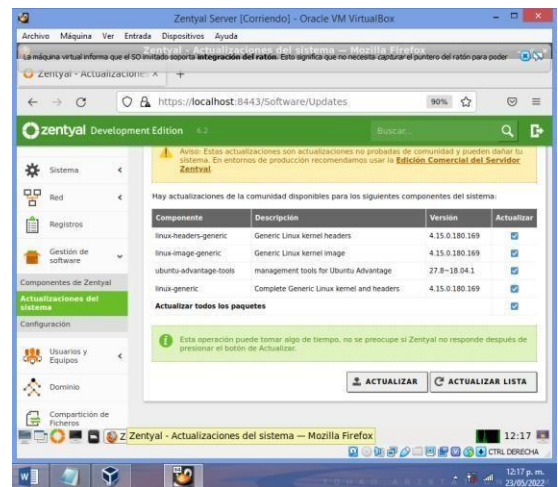


Fig. 48. Actualización de complementos



Se observa que efectivamente se están cargando las actualizaciones.

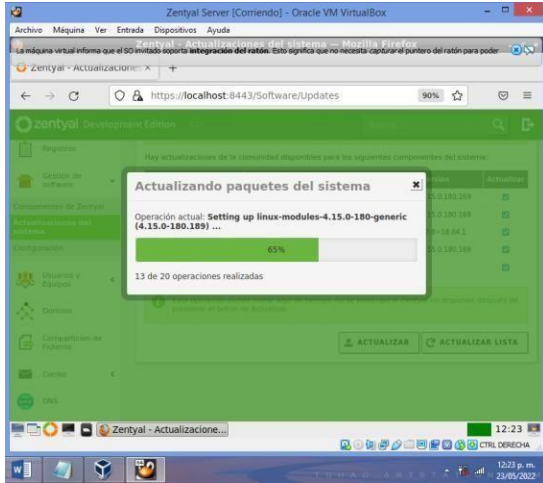


Fig. 49. Progreso de instalación

Desde Ubuntu cliente se hace la configuración de la red IPv4 para poder generar la conexión.

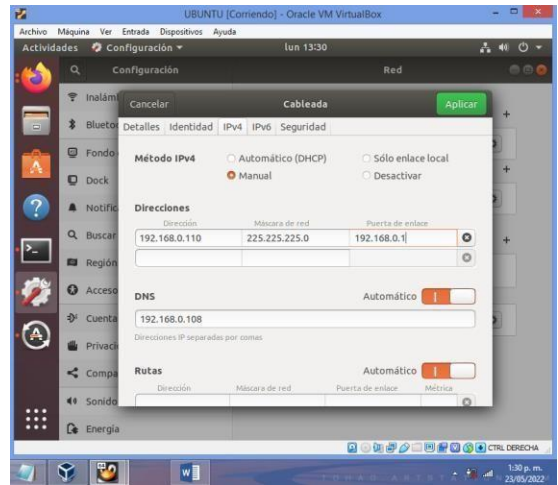


Fig. 52. Configuración de red Ubuntu cliente

La configuración del dominio se deja por defecto tal cual como está en el módulo de dominio.

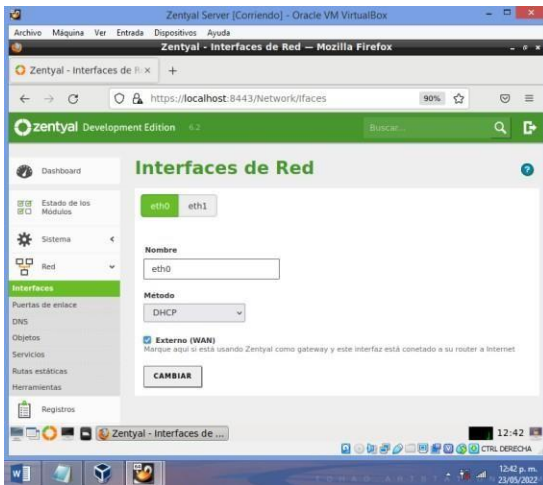


Fig. 50. Interfaz de red eth0

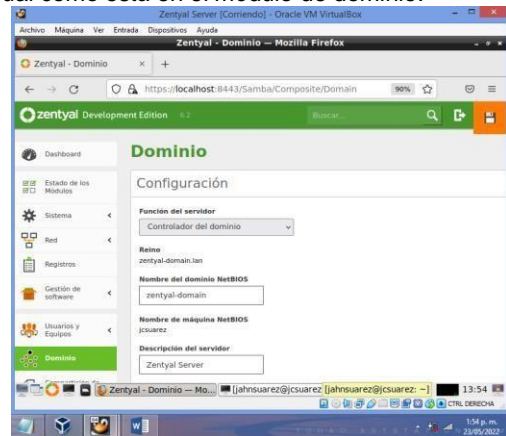


Fig. 53. Configuración de dominio

En el módulo de usuarios y equipos, en opciones de configuración de LDAP se selecciona la casilla habilitar PAM.

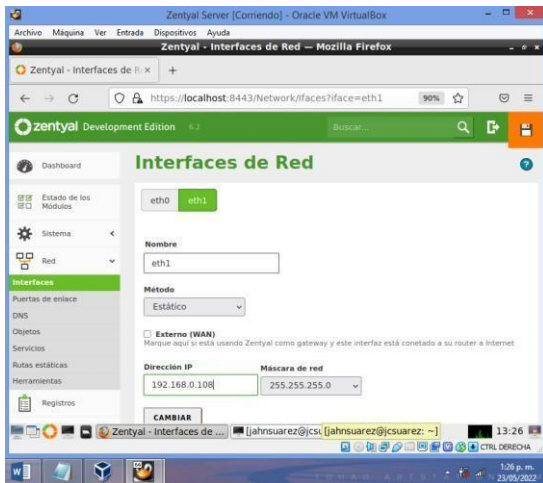


Fig 51. Interfaz de red eth1

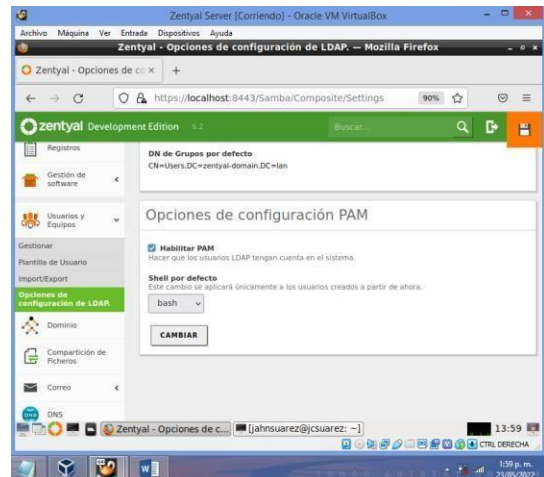


Fig. 54. Opciones de configuración LDAP

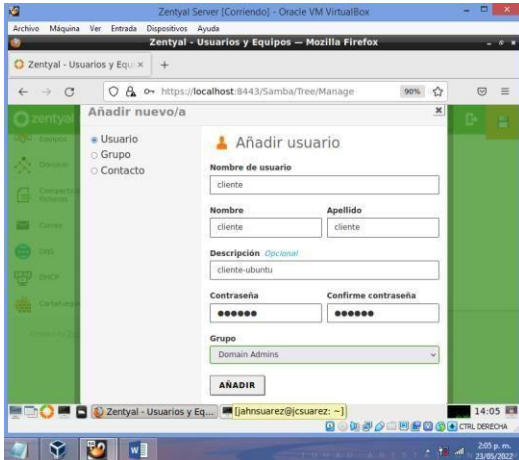


Fig. 55. Gestión de usuario

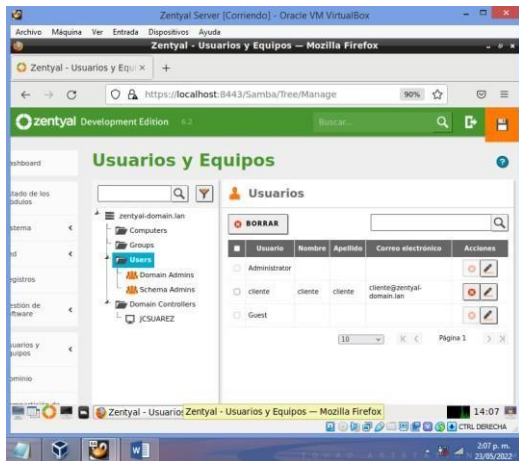


Fig. 56. usuario "cliente"

Desde el cliente se descarga el paquete pbis-open que permite habilitar el login con la autenticación al dominio de Zentyal.

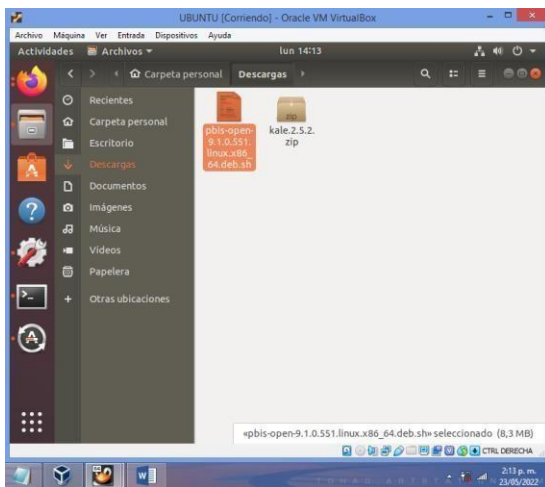


Fig. 57. Descarga paquete pbis-open

Desde la terminal de Ubuntu cliente se coloca el comando `chmod +x` (permiso de ejecución) seguido de la descripción del archivo que se ha descargado.

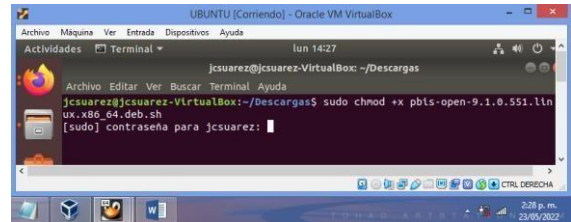


Fig. 58. Comando de ejecución

Seguidamente se utiliza el comando `sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh` para desempaquetar e instalar los complementos.

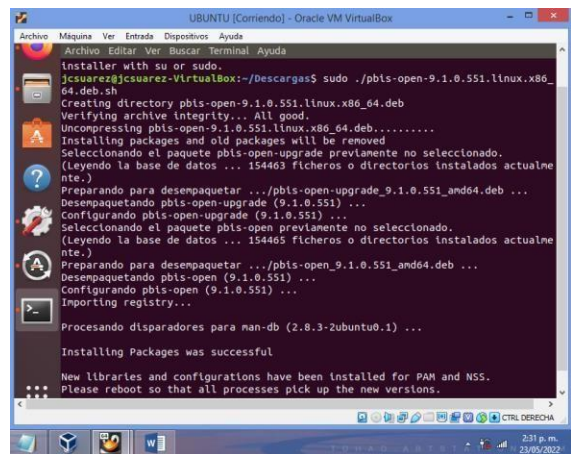


Fig. 59. Desempaquetado de archivos

Se modifica el archivo `resolv.conf` con un editor de texto, agregando la dirección ip del servidor al cual se desea conectar.

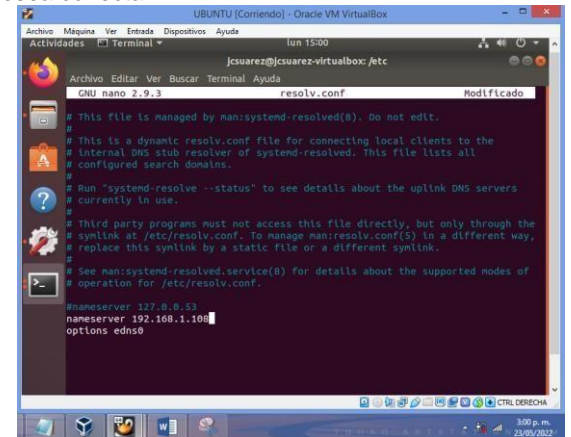


Fig. 60. Edición de archivo resolv.conf

Se comprueba mediante un ping a la ip del servidor que existe conexión.

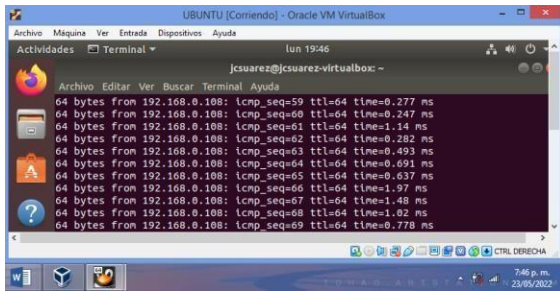


Fig. 61. Ping a IP servidor

Se genera el acceso desde consola a través del comando `sudo /opt/pbis/bin/domainjoin-cli join --disable ssh zentyal-domain.lan` cliente.

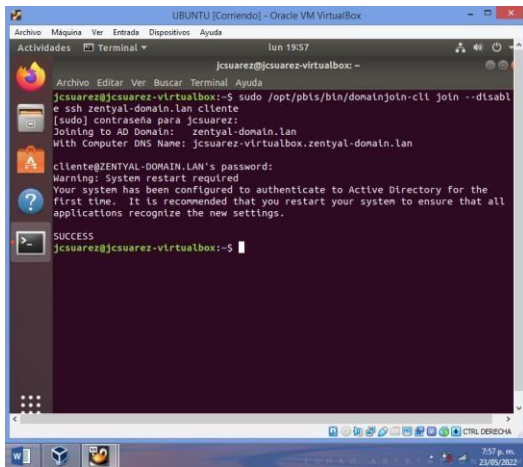


Fig. 62. Acceso al servidor

Se reinicia el sistema del cliente para poder iniciar sesión a través de la dirección `cliente@zentyal-domain.lan`.

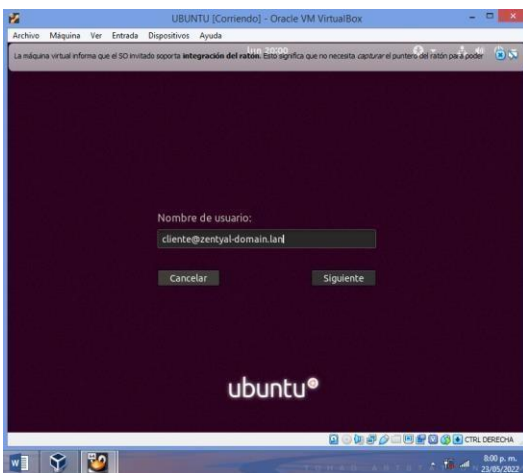


Fig. 63. Inicio de sesión con cliente

Ahora se procede a crear el directorio compartido desde Zentyal, el cual puede ser utilizado por el cliente Ubuntu.

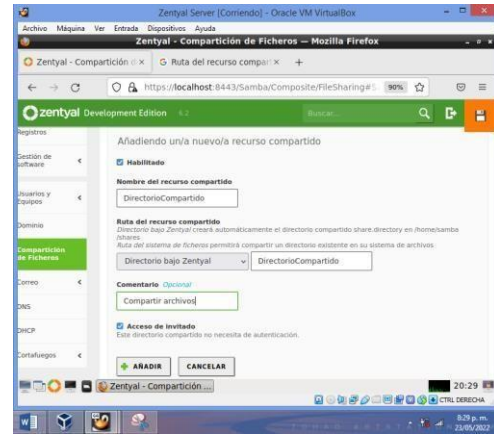


Fig. 64. Gestión directoria compartido

En control de acceso se le otorgan permisos de lectura y escritura al directorio compartido.

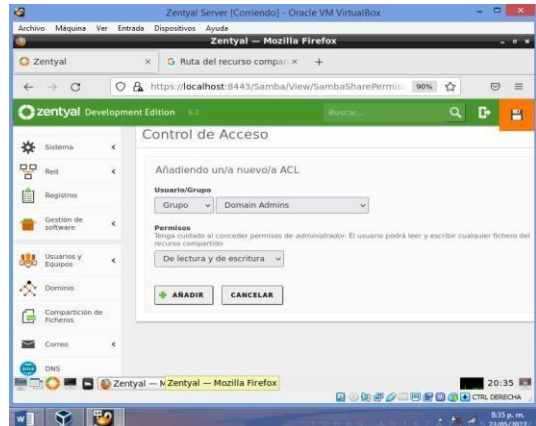


Fig. 65. Control de acceso a directorio compartido

Accedemos al servidor y buscamos la carpeta compartida en zentyal en la ruta `home/samba/shares/DirectorioCompartido`, donde encontramos un documento de texto el cual puede ser editado y eliminado por el cliente.

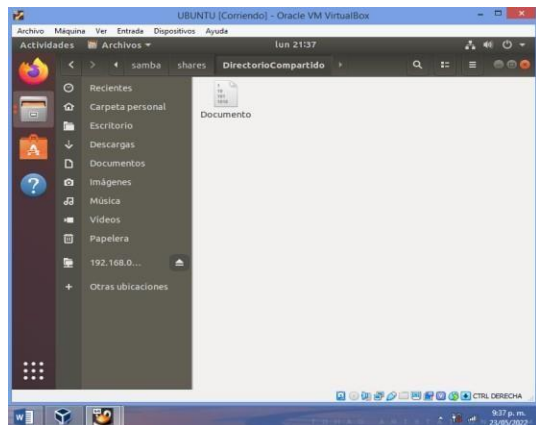


Fig 66. Acceso a DirectorioCompartido desde el cliente

Para la configuración de la impresora se instala desde la consola de Zentyal un sistema modular de código abierto llamado CUPS, el cual permite crear la impresora desde servidor. Sudo apt-get install cups

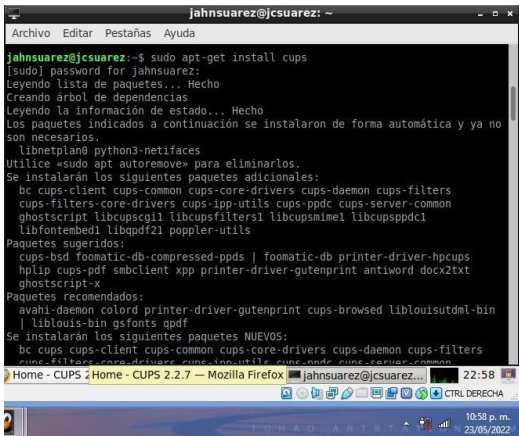


Fig 67. Instalación CUPS

Se selecciona el protocolo ipp (Internet Printing Protocol) para la configuración de la impresora.

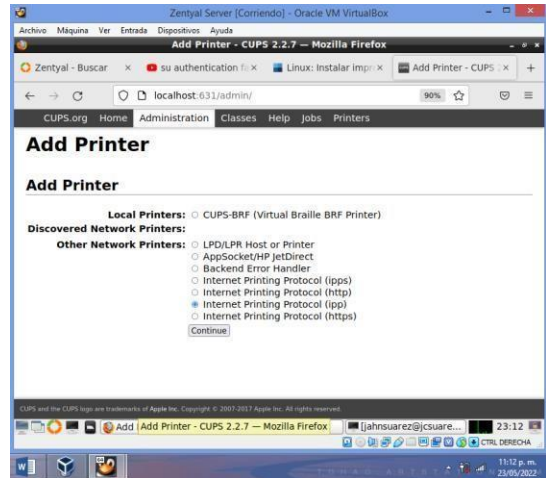


Fig 70. Asignación De protocolo

En el navegador de Zentyal se accede a la gestión de impresoras a través de la dirección https://localhost:631.

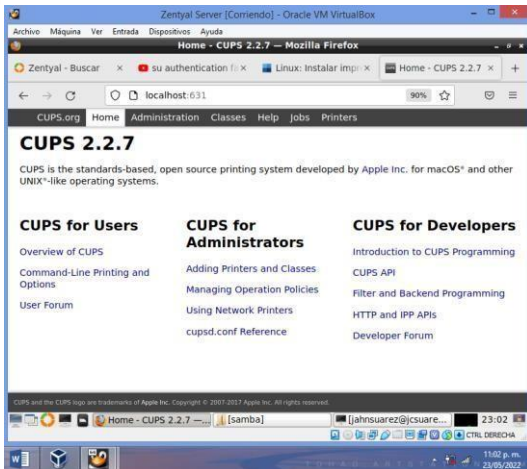


Fig. 68. Interfaz CUPS

Se agrega la dirección que identifica la impresora en la red interna.

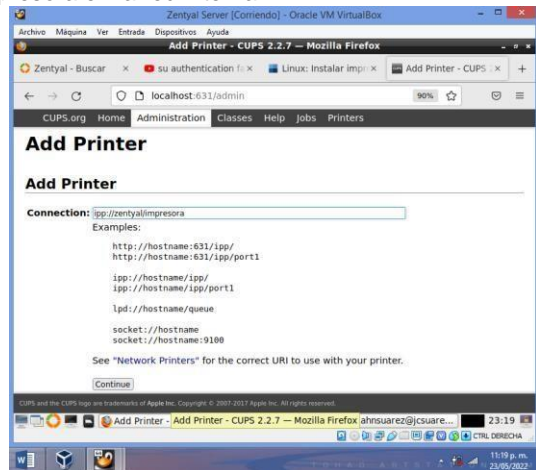


Fig. 71. Asignación De protocolo

Se ingresa al módulo de administración para agregar la impresora.

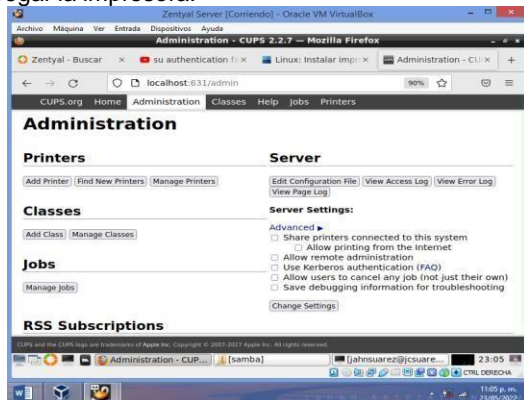


Fig. 69. Módulo administración CUPS

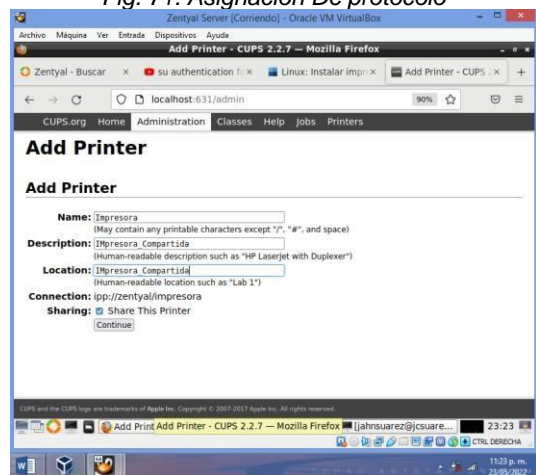


Fig. 72. Descripción de impresora

Finalmente se verifica en el módulo Printers la asignación de la impresora creada.

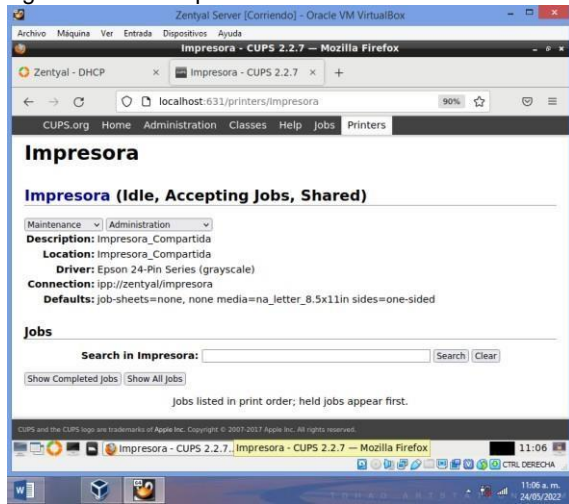


Fig. 73. Configuración completada

### 3.5 TEMÁTICA 5: VPN

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux.

En Muchas empresas crear una red virtual privada es de mucha importancia, con estas redes podemos controlar el tráfico de las conexiones y los accesos de los usuarios a determinadas conexiones Y datos de interés para dicha empresa. La necesidad de crear un túnel privado con una estación de trabajo es de vital importancia porque demuestra la funcionalidad de los servicios de estas redes VPN

Para iniciar este proceso vamos a crear una red VPN en Zentyal donde Se seleccionan los Paquetes necesarios para la instalación y configuración de la VPN

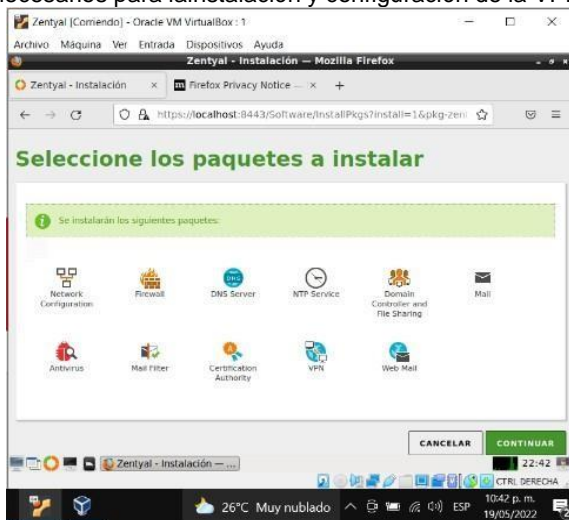


Fig. 74. Comprobación de descarga de paquetes

Finalizada la instalación de los componentes, se inicia el asistente para la configuración de redes.



Fig. 75. Inicio de configuración de red

Asignamos La red eth001 queda en modo DHCP.

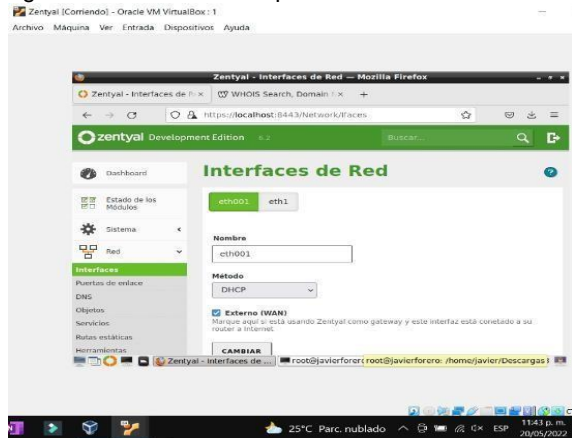


Fig. 76. Red DHCP

Asignamos a La red eth1 queda en modo estática y va ser la tarjeta interna.192.168.1.30

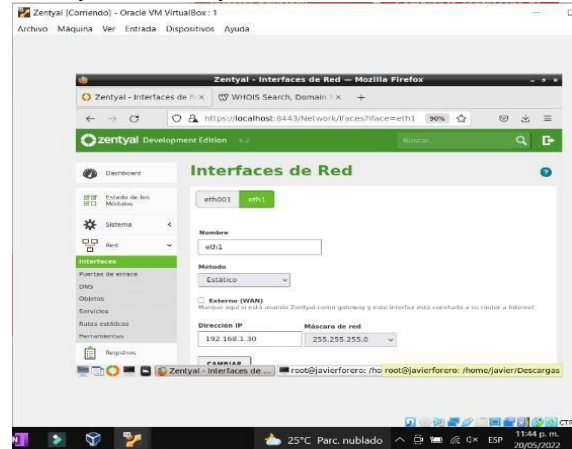


Fig.77. Red eth1

El dominio lo dejamos por defecto.

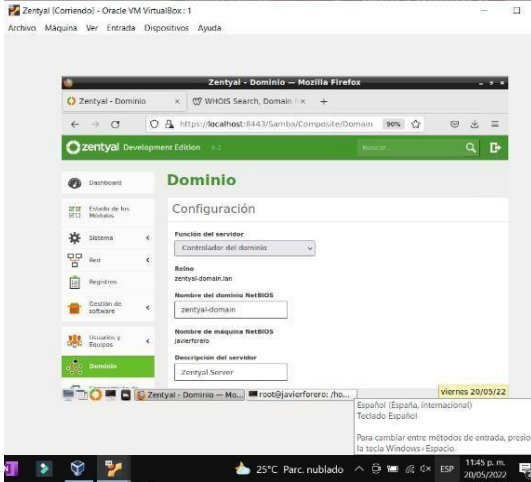


Fig. 78. Selección de Dominio

Guardamos los cambios y verificamos que esté válido y expedido

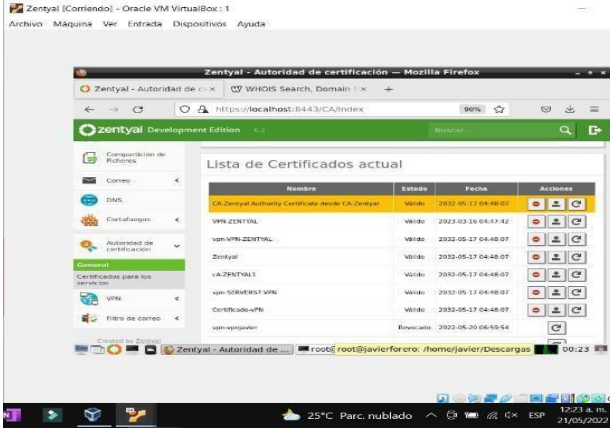


Fig. 79. Validación de certificado en Zentyal

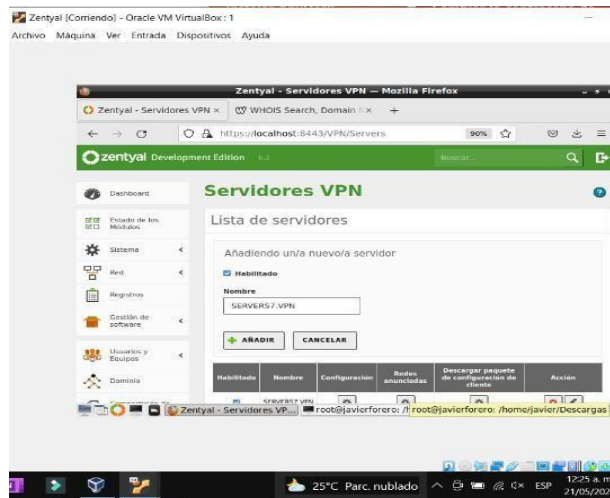


Fig. 80. Creación del VPN

Nuevamente creamos un certificado que será de uso para el servidor. Llamado en este caso Certificado-vPN.

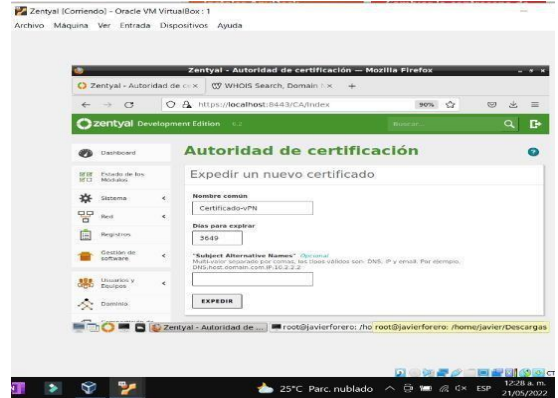


Fig. 81. Certificado para VPN

Guardamos los cambios y verificamos que se haya creado válido.

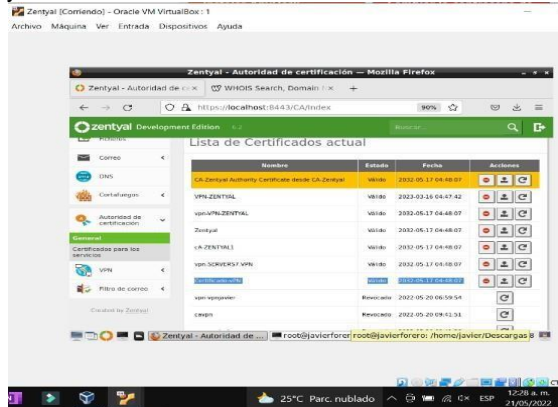


Fig. 82. Actualización del VPN

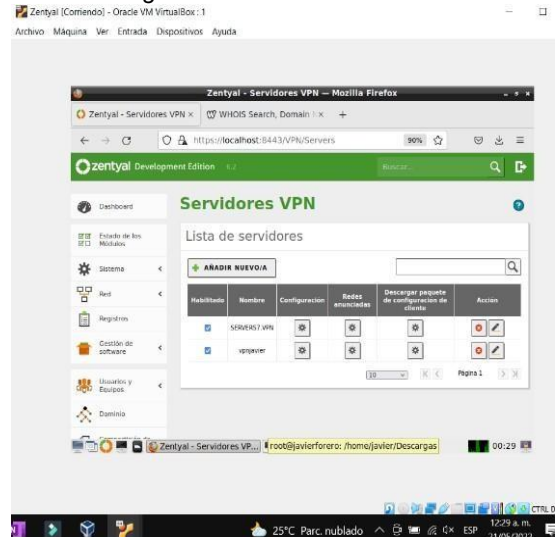


Fig. 83. Configuración del VPN

En puerto del servidor lo dejamos en modo UDP con el puerto 11194, en dirección VPN lo dejamos por defecto con máscara 24. En el certificado del servidor escogemos el certificado "certificado-vpn" y guardamos los cambios para que se apliquen.

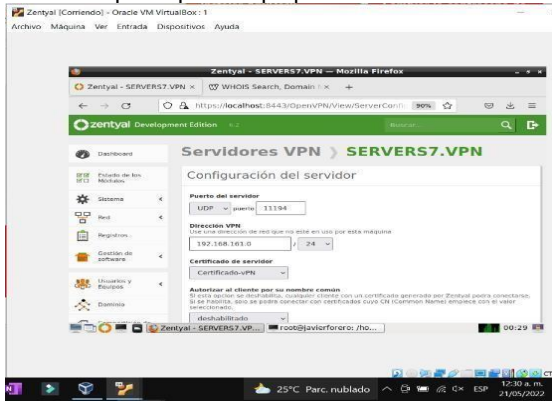


Fig. 84. Creamos el Certificado- Vpn

Asignamos un nombre del servicio (red-serviciosvpn) y una descripción (opcional) y añadir.

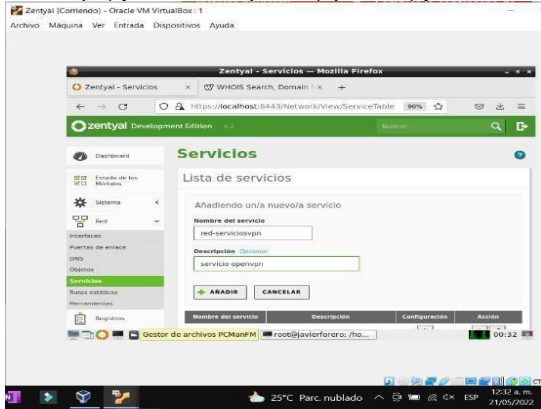


Fig. 85. Creación Red-servicios VPN

Una vez creado, clic en configuración del servicio, el protocolo será UDP con puerto de destino en 1194

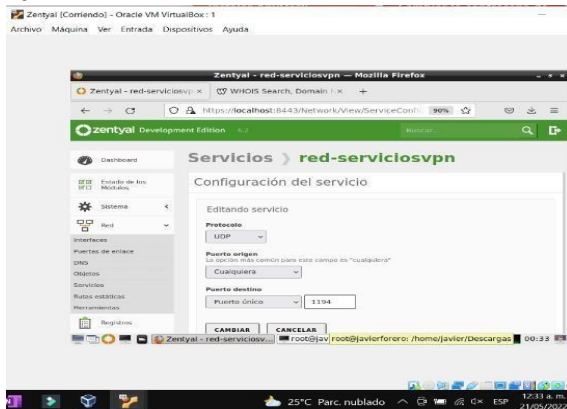


Fig. 86. Verificación del puerto 1194

Guardamos los cambios y verificamos que se haya creado correctamente.

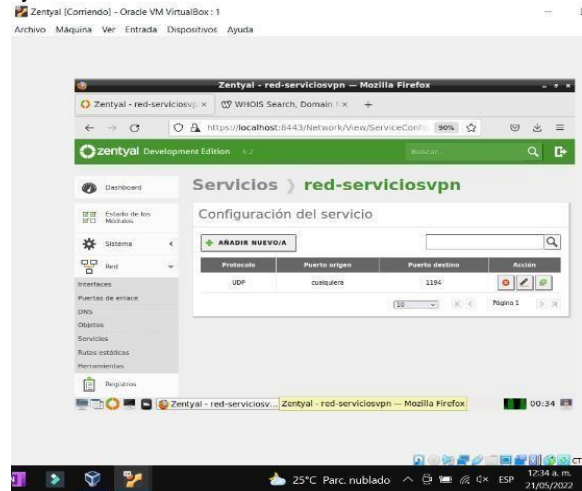


Fig. 87. Configuración del puerto VPN

Después vamos a añadir una nueva regla en el cortafuegos, clic en configurar reglas.

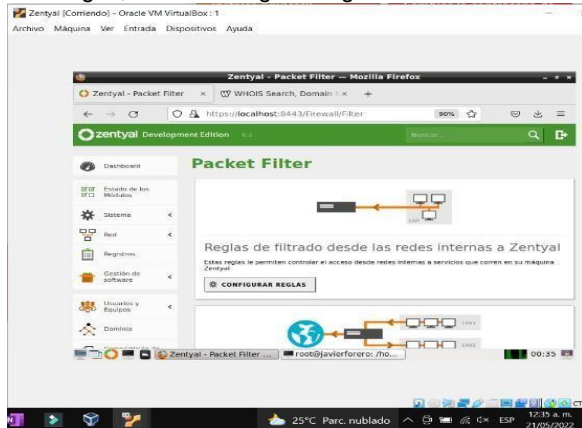


Fig. 88. creación de regla VPN

Verificamos que la regla se haya creado correctamente.

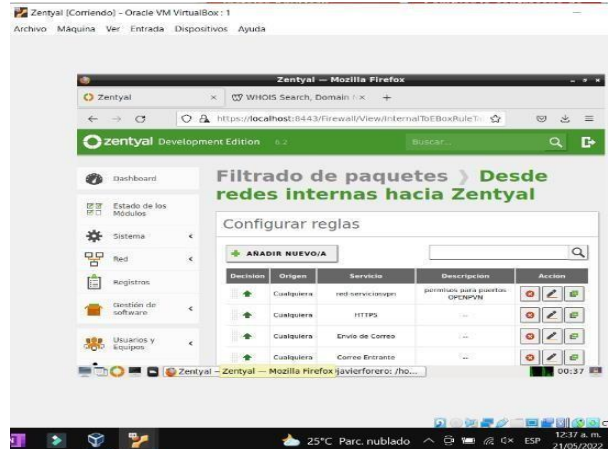


Fig. 89. Verificación de la configuración de la Regla

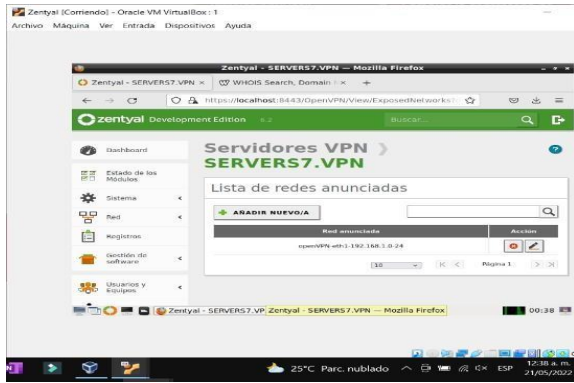


Fig. 90. Red por defecto VPN

Este paso es importante ya que tenemos que configurar el paquete del cliente para poder acceder a la VPN.

Tipo cliente: Linux

Certificado: el que habíamos creado anteriormente al principio.

Dirección del servidor: Esa es la IP del router o modem, en este caso para asegurarme que el saque de la página [www.who.is](http://www.who.is) y nos dio la: 181.33.137.22

Dirección adicional de la sacamos de la consola a través del ifconfig: 192.168.0.100

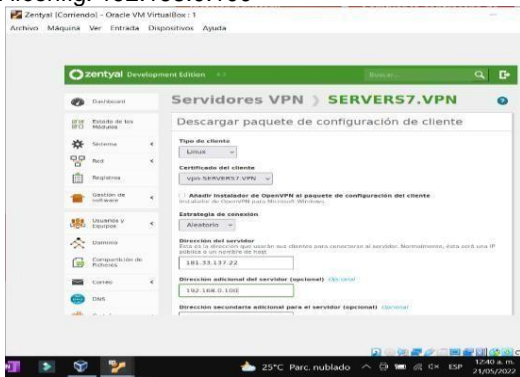


Fig. 91. Verificación de ip para conexión al VPN

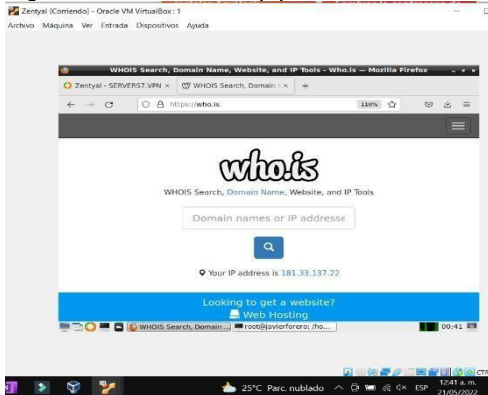


Fig. 92. Verificación de la Ip publica para VPN  
Como resultado generamos todos los certificados configurados en un archivo comprimido.

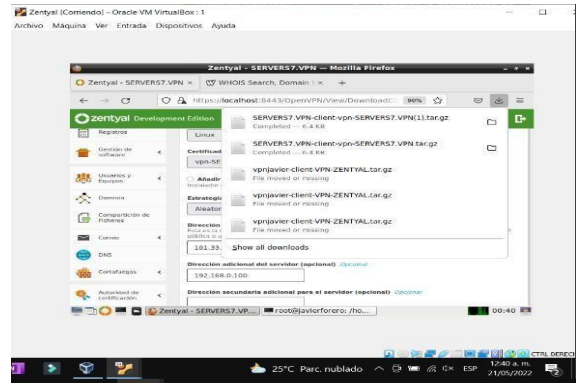


Fig. 93. Certificados de conexión del VPN

Por último, verificamos en el Zentyal el resume de la configuración del servidor VPN.

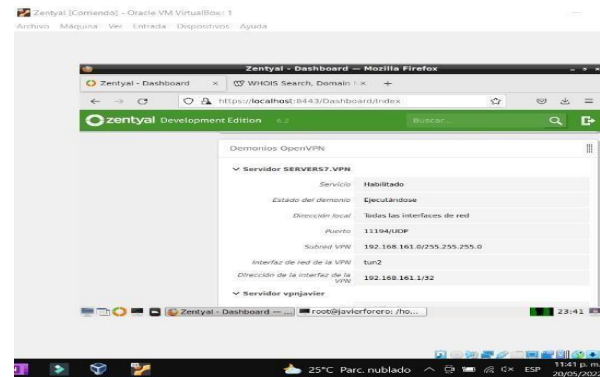


Fig. 94. Verificación de la creación del VPN

Pasamos los certificados del Zentyal a la máquina del cliente.

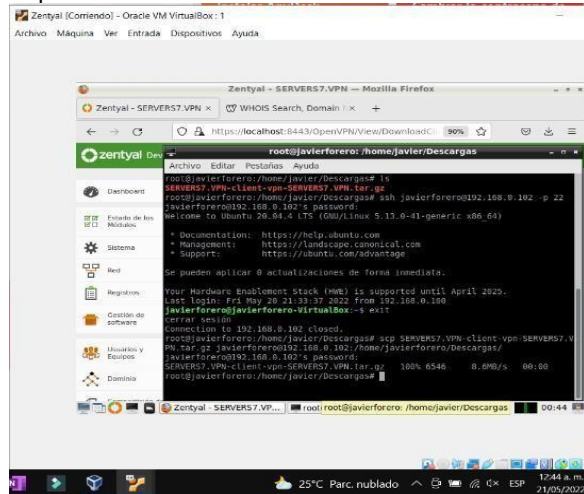


Fig. 95. Certificados en el cliente



Aquí ya estamos dentro del cliente, y lo que hacemos es descomprimir los certificados.

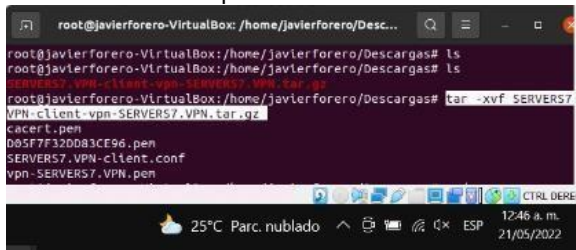


Fig. 96. Evidencia de certificados en el cliente

En esta sesión vamos a descargar e instalar el openvpn para permitir la conexión al zentyal.

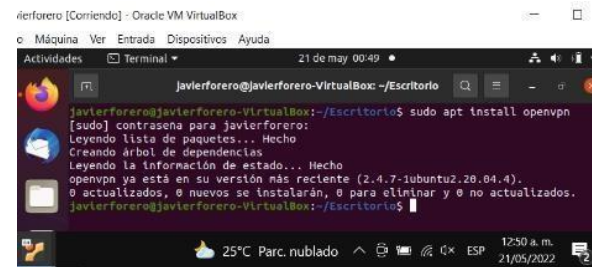


Fig. 97. Comando openvpn

A través del comando "openvpn --config" buscamos los certificados con extensión .conf

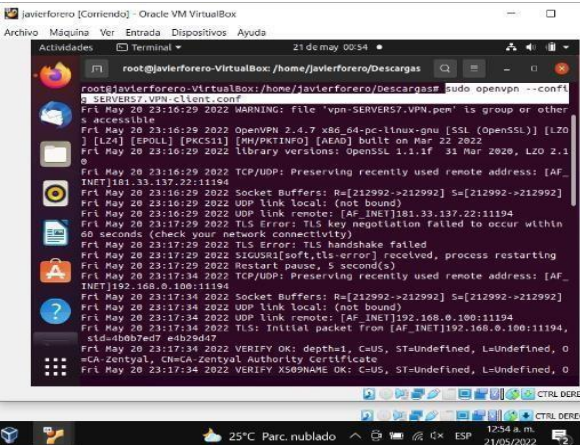


Fig. 98. Verificación de certificados en config

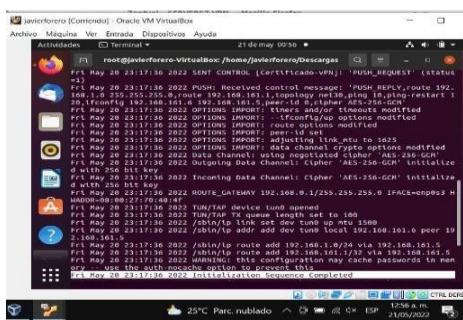


Fig. 99. Conectando cliente a Vpn

Esperamos a que permita la conexión cuando la secuencia se haya completado

Ya tenemos control total del Zentyal en el módulo principal.

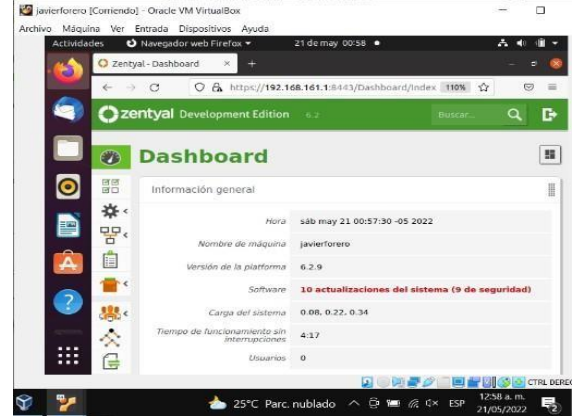


Fig. 100. Verificación de la creación del VPN

Podemos evidenciar también que mientras navegamos en el zentyal, en la consola siguen corriendo los procesos de la VPN.

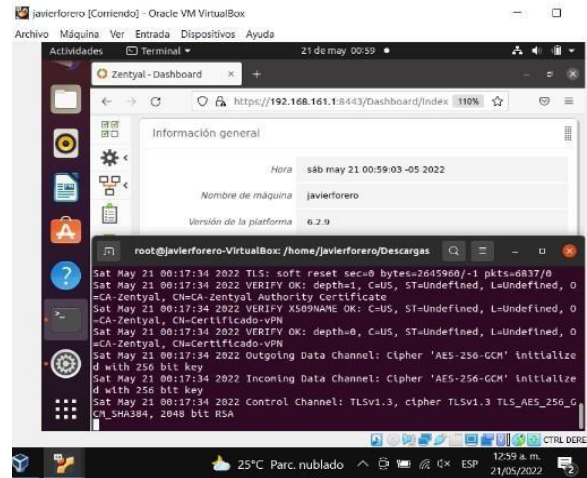


Fig. 101. Comprobación de conexión de VPN

## 4 CONCLUSIONES.

Según lo comprobado se concluye que el sistema operativo Zentyal es una herramienta óptima para iniciar con un proceso de migración de infraestructura TI.

Después de realizar las actividades correspondientes, con esta actividad se logró formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente.

Se logra configurar el acceso a una estación de trabajo Linux a través del controlador de dominio LDAP, a los servicios de carpetas compartidas e impresoras.

Se comprendió la importancia de herramientas como el Zentyal para lograr una escalabilidad en un sin número de servicios de redes para infraestructuras GNU Linux de manera más amigable al usuario Final.

Se aprendió y Reconoció el aprendizaje de la instalación del sistema zentyal server en una máquina virtual. Comprendiendo su escalabilidad y funcionalidad con herramientas de uso común en empresas y servicios TI

## 5 REFERENCIAS

- [1] Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.2. (s. f.). zentyal.org. <https://doc.zentyal.org/6.2/es/directory.html>
- [2] E. H. Miller, "A note on reflector arrays", IEEE Trans. Antennas Propagat., Aceptado para su publicación.
- [3] Es/3.5/Servicio de compartición de impresoras - Zentyal Linux Small Business Server. (s. f.). Zentyal.Org. [https://wiki.zentyal.org/wiki/Es/3.5/Servicio\\_de\\_comparticion\\_de\\_impresoras](https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_comparticion_de_impresoras)
- [4] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: <http://www.atm.com>.
- [5] Sanz Mercado, P. (2014). Seguridad en linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 13 - 26). elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=13>
- [6] Sanz Mercado, P. (2014). Seguridad en linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 45 - 60). elibro <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=45>
- [7] Sanz Mercado, P. (2014). Seguridad en linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 61 - 105). elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=61>
- [8] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 - 137). Madrid. ES: IC Editorial. elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92>
- [9] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 205 - 236). elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43262?page=205>