

IMPLEMENTACIÓN DE ZENTYAL SERVER COMO HERRAMIENTA PARA LA SOLUCIÓN DE NECESIDADES ESPECÍFICAS CON GNU/LINUX

Universidad Nacional Abierta y a Distancia "UNAD"

Efreicer Sánchez Mena

fsanchezm@unadvirtual.edu.co

Eddie Enrique Leudo Asprilla

eeleudoa@unadvirtual.edu.co

José Alexander Bermúdez

jabermudez@unadvirtual.edu.co

Yoly Milena Mosquera González

ymmosquerag@unadvirtual.edu.co

Ana Catalina Guzmán González

acguzmang@unadvirtual.edu.co

RESUMEN: *El documento en mención contempla primeramente los conocimientos adquiridos en las unidades 1,2,3,4,5 y 6 establecidos como metas para cumplir a cabalidad con las metas del diplomado de profundización en Linux, siendo así, se establece una actividad final que se desarrolla como producto final, llevando a la practica la implementación del server Zentyal Linux, donde se desarrollan grandes procesos de administración de servidores, en este orden, se desarrolló de forma individual y según la temática de cada alumno escogida, la instalación del servidor Zentyal Linux en primera instancia, y se derivan proceso individuales como implementación servidor DHCP, servidor DNS, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server, y red privada virtual VPN. Esto se realizó según las pautas establecidas en la guía de actividades para cada temática, como resultado se obtuvo la implementación total de todos los servicios, lo que representa satisfacción.*

ABSTRACT: *The document in question first contemplates the knowledge acquired in units 1,2,3,4,5 and 6 established as goals to fully comply with the goals of the diploma course of deepening in Linux, thus establishing a final activity that ips developed as a final product, putting into practice the implementation of the Zentyal Linux server, where major server administration processes are developed, in this order, the installation of the Zentyal Linux server was developed individually and according to each student's chosen topic, and individual processes such as DHCP server implementation, DNS server, Domain Controller, Non-transparent Proxy, Firewall, File Server and Print Server, and VPN virtual private network are derived. This was done according to the guidelines established in the activity guide for each topic, as a result, the total implementation of all services was obtained, which represents satisfaction.*

PALABRAS CLAVE: Implementación, Servicios, Servidor, Zentyal.

1 INTRODUCCIÓN

La seguridad en las empresas siempre ha sido una necesidad que cada día cobra más vida dada la cantidad amenazas que día a día crecen en la sociedad, lo cual ha llevado a que se desarrollen diversos medios o entornos que ayuden a mitigar este flagelo, donde se hacen procesos de ayuda en la solución a la seguridad TIC'S desde el entorno Hardware hasta aplicaciones Software, como lo es Zentyal, es así como la finalidad de este diplomado se enfocó en mostrar desde cero un conglomerado de aplicaciones de código abierto y uso libre que fortalecen las capacidades en los alumnos sobre la seguridad informática, y la implementación de soluciones de bajo costo y de fácil utilidad para ser puestas en marcha dar un esquema seguro a las empresas, blindando las mismas con medios fácil de obtener y que claro, requieren personal capacitado y con destrezas en diferentes áreas, así como experiencia para que estas herramientas pueden desbordar su potencial y ser la herramienta cabecera en la gestión de sus servicio.

2 INSTALACION DE ZENTIAL SERVER

2.1 REQUISITOS DE HARDWARE PARA INSTALACION

Las especificaciones de sistemas para la instalación del Zentyal son: Disco duro de 80 GB, memoria RAM de 2 GB, procesador Pentium IV hacia adelante, 2 tarjetas de red. [3]

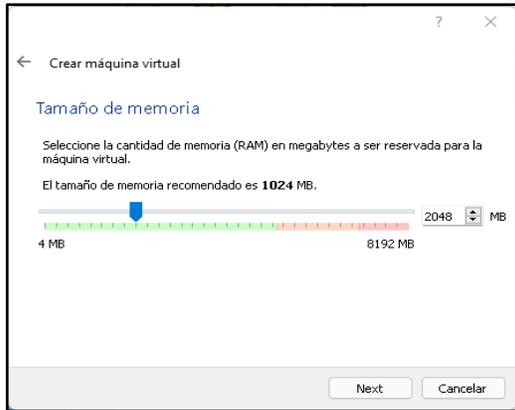


Figura 1. Instalación de Zentyal Server

Se configura un adaptador en modo Bridge y otro como red interna como muestra la figura 2.

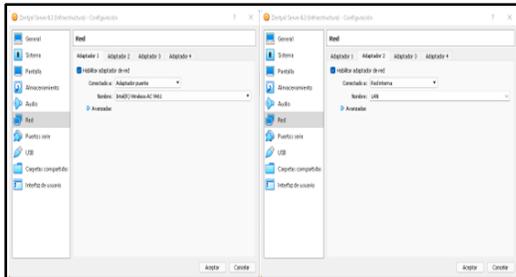


Figura 2. Instalación de Zentyal Server

Se escoge a continuación la primera opción como muestra la figura 3. [1]

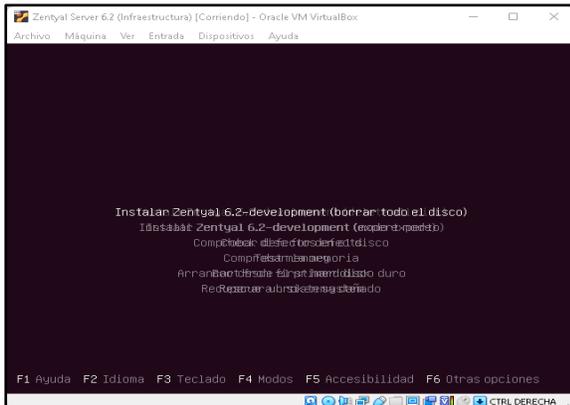


Figura 3. Instalación de Zentyal Server

Empieza la instalación de Zentyal server en el disco duro evidenciado en la figura 4.

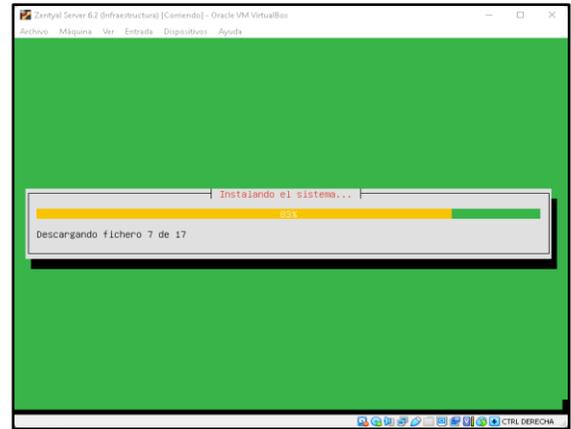


Figura 4. Instalación de Zentyal Server

Ahora es cuestión de esperar a que se terminen de instalar paquetes restantes ilustrado en la figura 5.

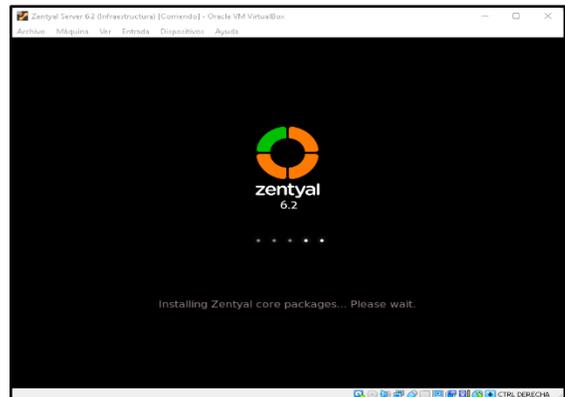


Figura 5. Instalación de Zentyal Server

En este momento ya se puede visualizar el escritorio de Zentyal en la figura 6.

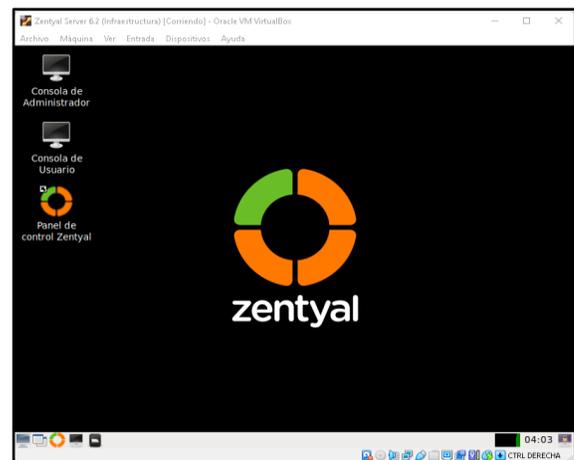


Figura 6. Instalación de Zentyal Server

Se ingresa a Zentyal con usuario y contraseña asignados durante la instalación como muestra la figura 7.



Figura 7. Instalación de Zentyal Server

Se da clic en continuar como muestra la figura 8.

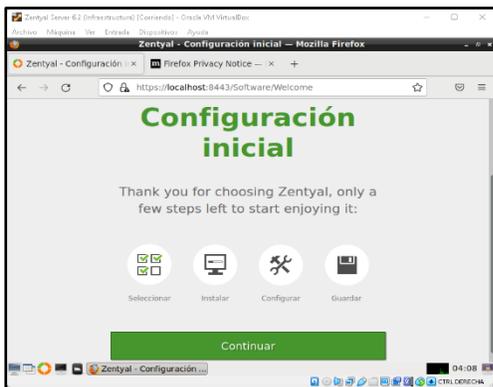


Figura 8. Instalación de Zentyal Server

Por el momento solo se seleccionarán algunos módulos útiles para realizar el producto esperado como muestra la figura 9.



Figura 9. Instalación de Zentyal Server

Se da clic en continuar como muestra la figura 10.

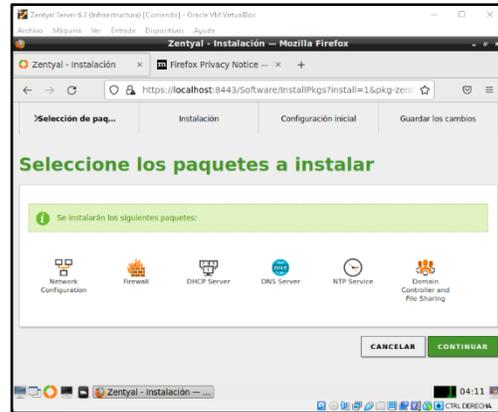


Figura 10. Instalación de Zentyal Server

Ahora empieza el proceso de instalación de los módulos tal como lo muestra la figura 11.

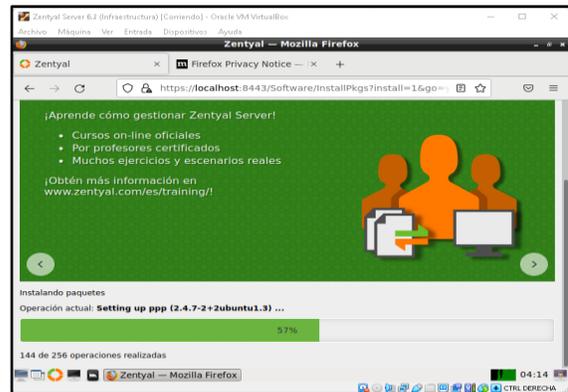


Figura 11. Instalación de Zentyal Server

Es momento de ir a finalizar las configuraciones al panel de control de Zentyal tal como muestra la figura 12.



Figura 12. Instalación de Zentyal Server

**3 PLANTEAMIENTO
CONTEXTUALIZACIÓN
PROBLEMA A RESOLVER:** **Y
DEL**

3.1 TEMATICA 1: 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.

Para configurar el DHCP, ingresamos por el módulo DHCP y le damos clic sobre configuración, ya estando allí realizamos los cambios pertinentes como muestra la figura 13.

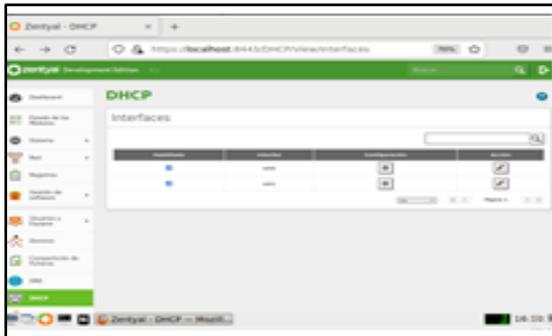


Figura 13. Módulo DHCP.

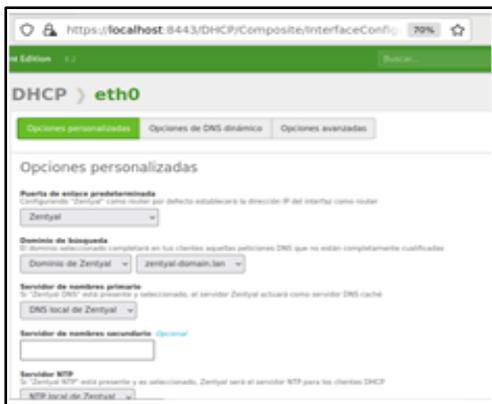


Figura 14. Configuración DHCP.

Agregamos el Rango de las direcciones IP, van desde la 192.168.1.50 hasta la 192.168.1.150. Le damos en añadir y luego en guardar como muestra la figura 15.

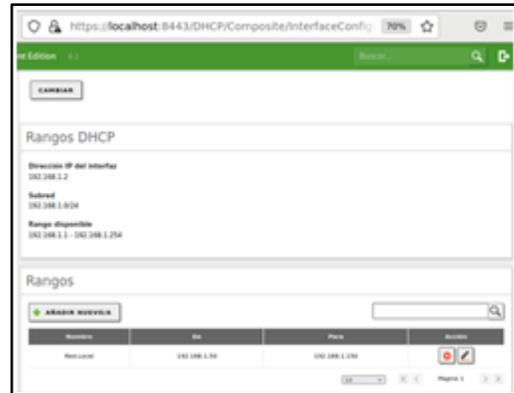


Figura 15. Rangos DHCP.

Iniciamos la máquina y se verifica que el DHCP está funcionando, le otorgo la ip dentro del rango como muestra la figura 16.

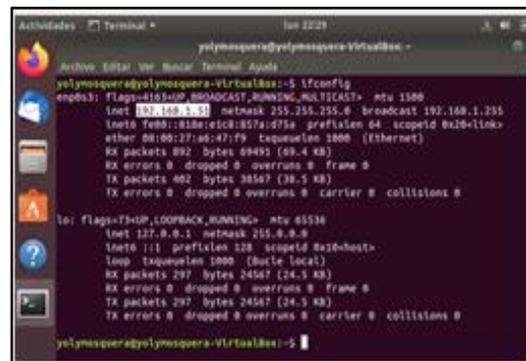


Figura 16. IP asignada maquina usuario.

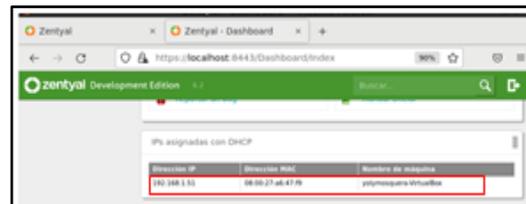


Figura 17. IPs Asignadas con DHCP.

Para configurar el DNS, ingresamos por el módulo DNS en este caso como ya habíamos designado un dominio al inicio de la configuración nos toma ese, habilitamos el DNS transparente y guardamos los cambios como muestra la figura 18.

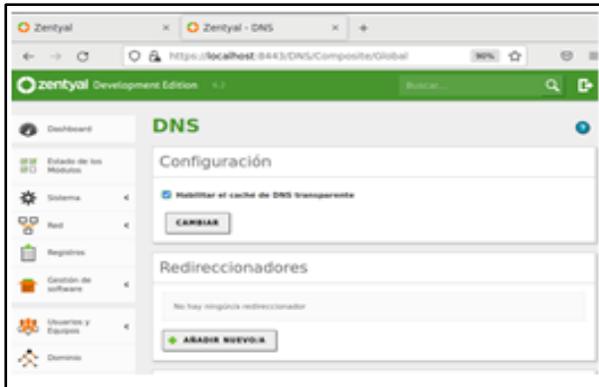


Figura 18. Configuración DNS



Figura 19. Dominio asignado.

Se realizan las pruebas para saber si el cliente se está conectando a la ip de nuestro servidor como muestra la figura 20.

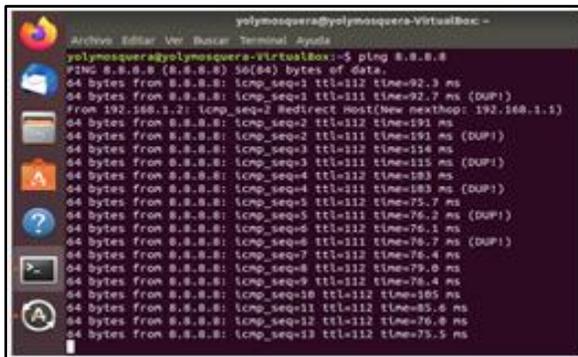


Figura 20. Ping 8.8.8.8

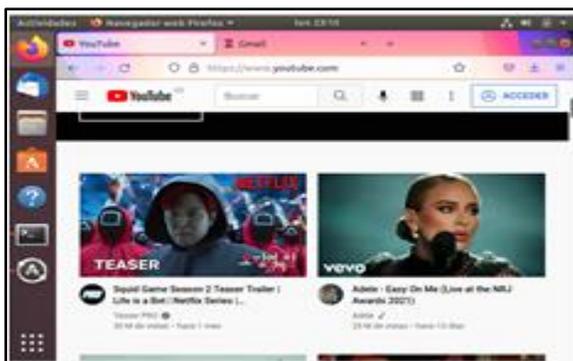


Figura 21. Prueba página YouTube.

Para configurar el Controlador de Dominio, primero ingresamos por Dominio y en "función del servidor" seleccionamos Controlador de dominio, luego habilitamos perfiles móviles y guardamos los cambios como muestra la figura 22.

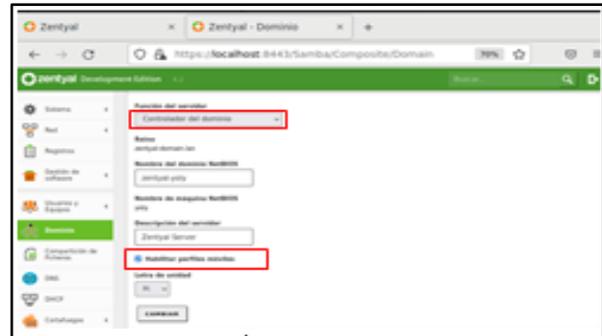


Figura 22. Selección del controlador de Dominio.

Luego ingresamos por "Usuarios y Equipos" le damos en "Gestionar" desde aquí vamos a agregar un nuevo usuario "DPL" dándole clic en "Users" como muestra la figura 23.



Figura 23. Se crea el usuario DPL

En opciones de configuración "LDAP" habilitamos "PAM" para gestionar el inicio de sesión del usuario dentro de la red como muestra la figura 24.



Figura 24. Se habilita PAM

Descargamos pbis-open en la maquina cliente para configurarlo dentro de nuestro dominio. Este servicio nos va a permitir gestionar el alcance del Directorio Activo. Ver figura 25.

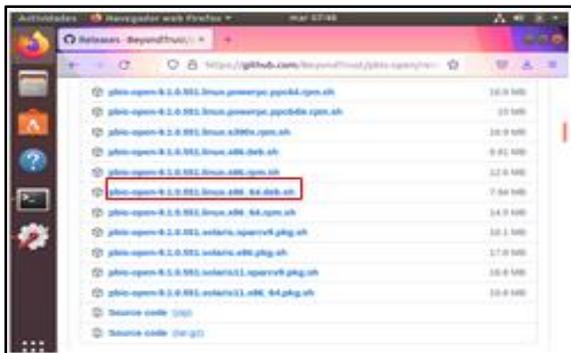


Figura 25. Descarga de pbis-open.

En este paso ubicamos el archivo descargado y le otorgamos los permisos para su ejecución desde el terminal, ver figura 26.

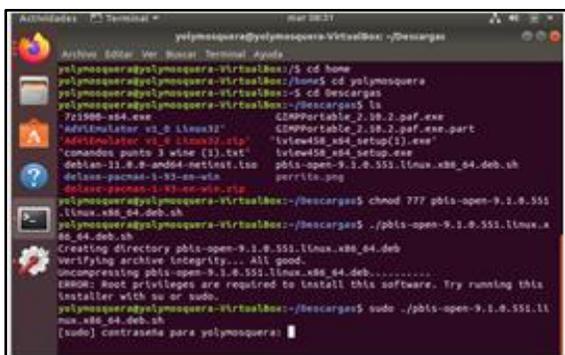


Figura 26. Se otorgan los permisos.

Proceso de instalación de pbis-open. Ver figura 27.



Figura 27. Instalación pbis-open.

Añadimos el usuario "DPL" al dominio "zentyal-domain.lan" como muestra la figura 28.



Figura 28. Se añade el Usuario al Dominio

Se agregó la maquina cliente al dominio, ver figura 29.

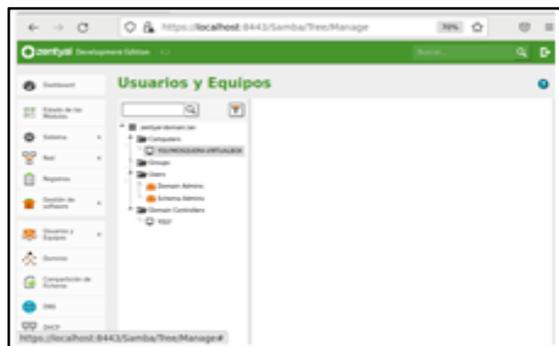


Figura 29. Maquina cliente al dominio.

Se reinicia la máquina y se inicia sesión con el usuario creado en con el dominio, ver figura 30.



Figura 30. Se inicia sesión con Dominio.

3.2 TEMATICA 2: 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 1230.

Se abre la máquina virtual Ubuntu y se configura el adaptador de red NatNetwork, ver figura 31.

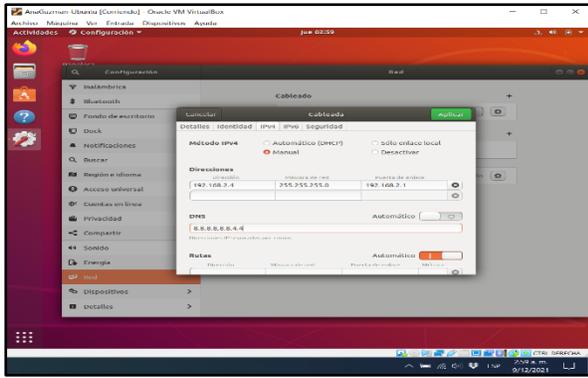


Figura 31. Ip estática en LAN.

Se configura el direccionamiento estático en el equipo Ubuntu, ver figura 32.

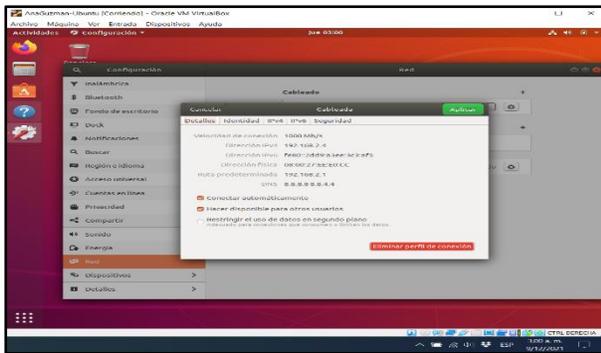


Figura 32. Configuración de direccionamiento. Se crea un nuevo objeto con el nombre Equipo Ubuntu ana.

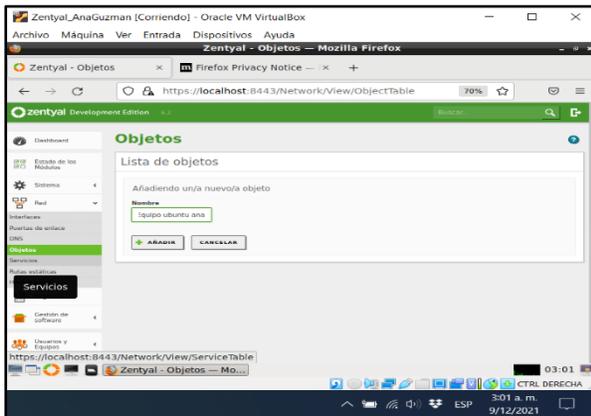


Figura 33. Creación de objeto.

Se edita el objeto creado, ver figura 34.

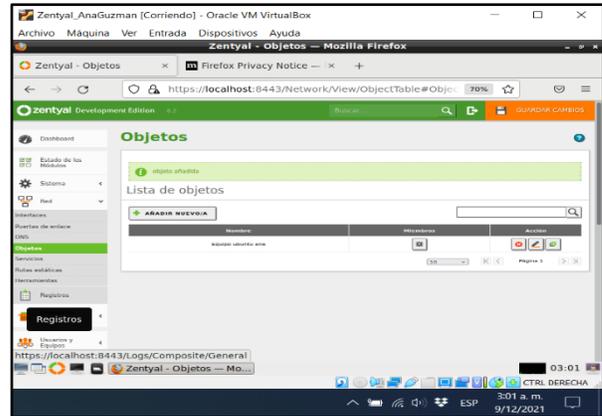


Figura 34. Edición de objeto.

Se añade un nuevo miembro al objeto creado, ver figura 35.

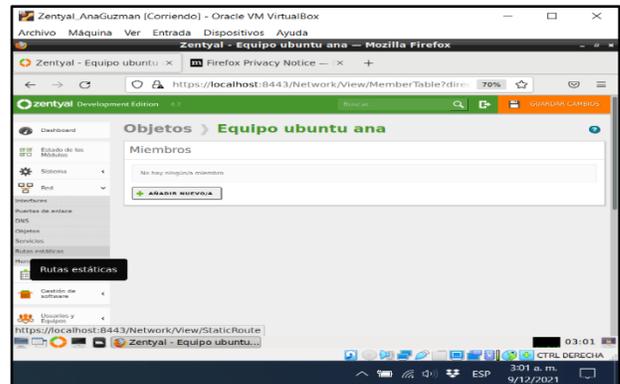


Figura 35. Edición de objeto.

Se configura el direccionamiento y el nombre al nuevo miembro, ver figura 36.

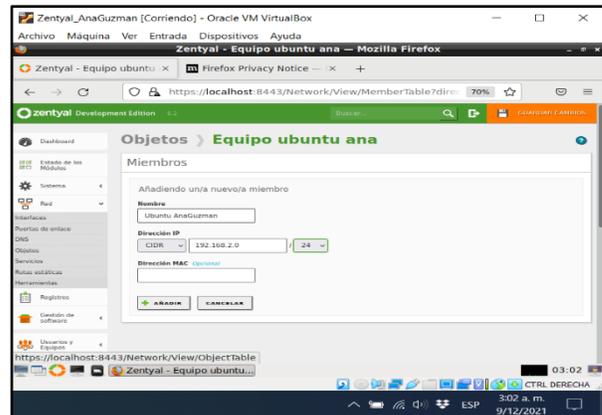


Figura 36. Se crea nuevo miembro.

Se añade el nuevo miembro y se procede a guardar los cambios realizados, ver figura 37.

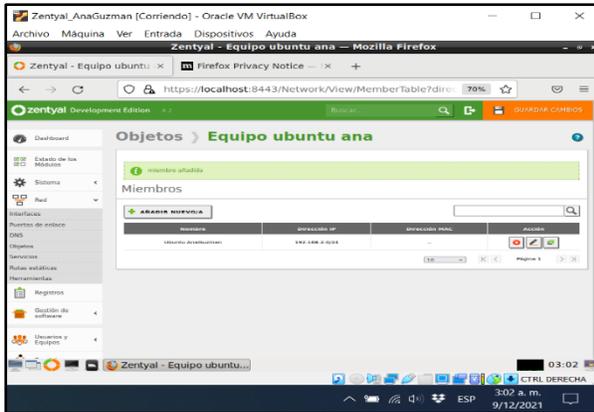


Figura 37. Se añaden cambios.

A continuación, se procede a configurar el servidor proxy no transparente con puerto 1230 y se guardan cambios, ver figura 38.

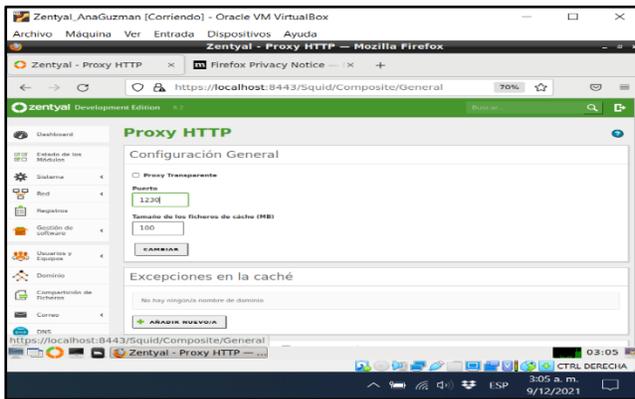


Figura 38. Se añaden cambios.

Se accede a las reglas de acceso del servidor proxy, ver figura 39.

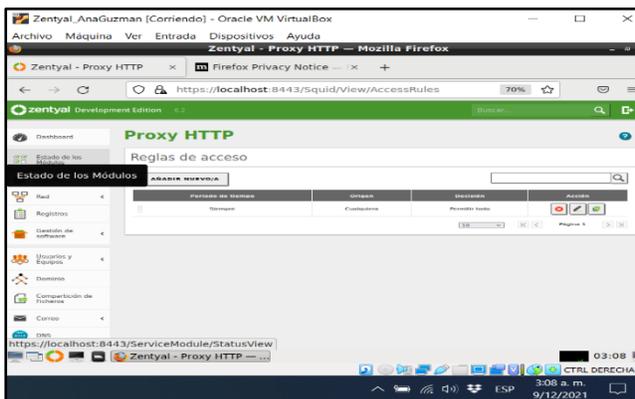


Figura 39. Reglas de acceso a servidor proxy.

Se crea una nueva regla donde se especifica como origen el objeto de red creado y se deniega, ver figura 40.

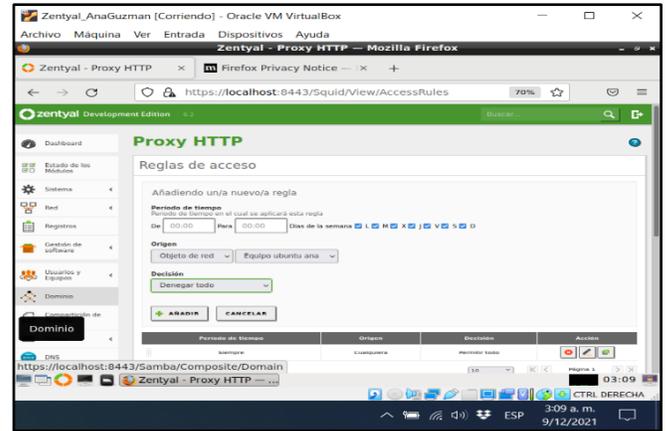


Figura 40. Especificación de objeto a denegar.

Se borra la regla creada predeterminedada y se guardan cambios, ver figura 41.

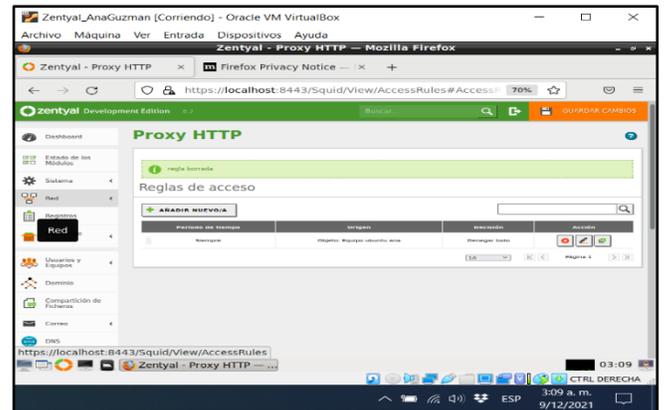


Figura 41. Se borra regla por defecto.

Se comprueba que el equipo Ubuntu cuenta con acceso a internet, ver figura 42.

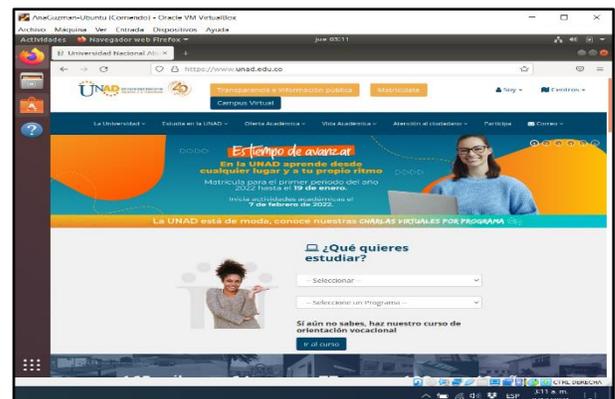


Figura 42. Comprobación de internet en LAN.

Se configura en el navegador la configuración de conexión con el servidor proxy y el puerto 1230, ver figura 43.

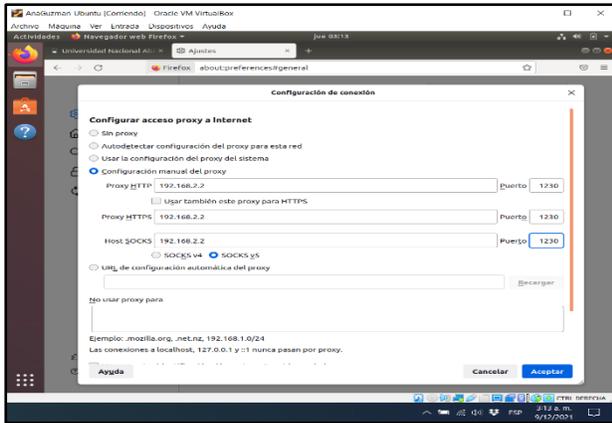


Figura 43. Configuración de proxy en LAN.

Se refresca la página web y se verifica que el servidor proxy rechaza las conexiones, de esta forma se comprueba que el servidor Zentyal está configurado como proxy no transparente, ver figura 44.

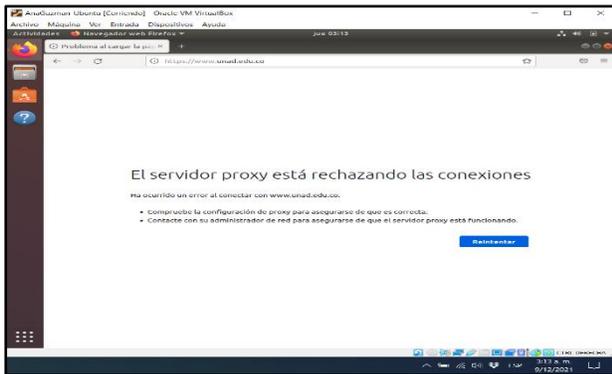


Figura 44. Validación de aplicación de proxy.

3.3 TEMATICA 3: CORTAFUEGOS

Producto esperado: 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.

Se configura un full de 9 ips que se pueden visualizar en la imagen. Se guardan los cambios, ver figura 45.

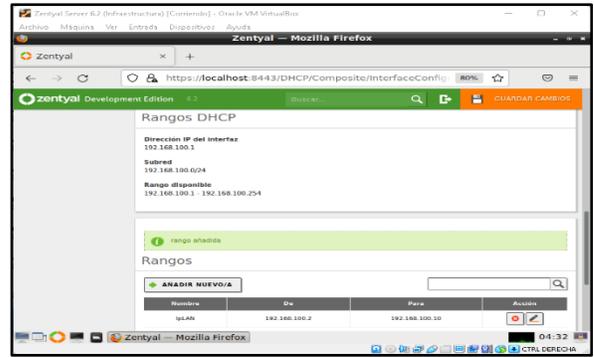


Figura 45. Rango IP por DHCP.

A través de un ping exitoso se comprueba que el cliente está alcanzando tanto el Gateway de la red LAN como también el Gateway de la WAN, ver figura 46.

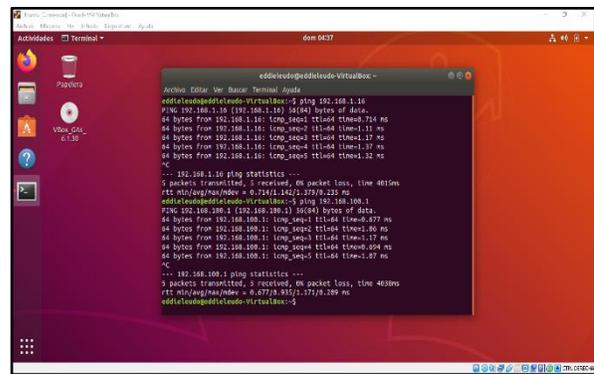


Figura 46. Verificación Ping con cliente.

Se verifica que en la red LAN ya hay gestión, ver figura 47.



Figura 47. Verificación de internet en LAN.

Se añade un objeto con el CIDR (direccionamiento interdominio sin clase) de la página de Facebook y Twitter para luego bloquearlos desde el cortafuego. Una herramienta para identificar fácilmente el CIDR de distintos sitios en la web es www.arin.net. En la siguiente imagen con la ip de Facebook y la de Twitter se realiza la identificación de su CIDR, ver figura 48.

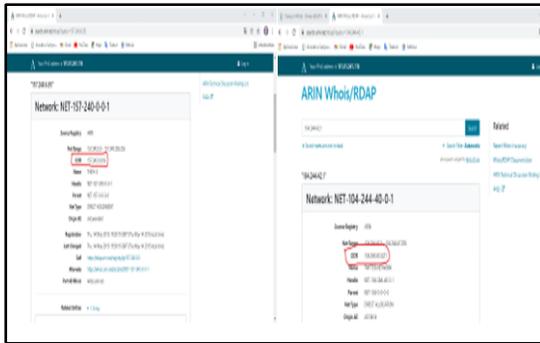


Figura 48. CIDR de páginas web.

Y se procede a crear el objeto que se le llaman Redes sociales y se crean los miembros con los CIDR de Facebook y Twitter y se guardan los cambios, ver figura 49.

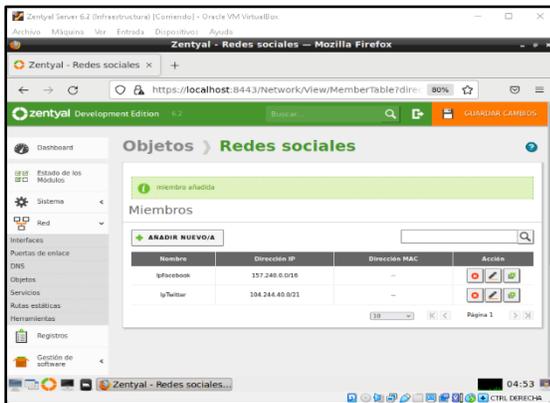


Figura 49. Creación de objeto.

Ahora desde la opción del cortafuego, filtrado de paquetes>Redes internas, se realiza la denegación del objeto que se llama Redes sociales y se guardan cambios, ver figura 50. [2]

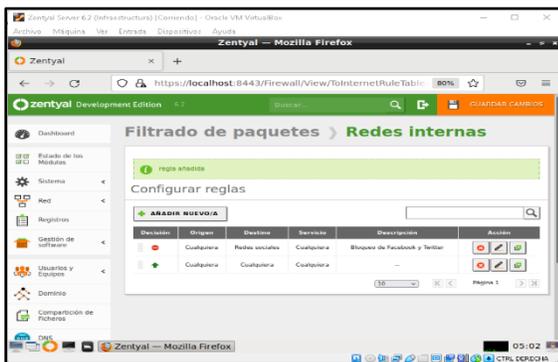


Figura 50. Aplicación de regla de cortafuego.

Aquí se evidencia entonces que el cliente ubicado en la LAN no puede acceder a la red social Facebook ni Twitter, ver figura 51.

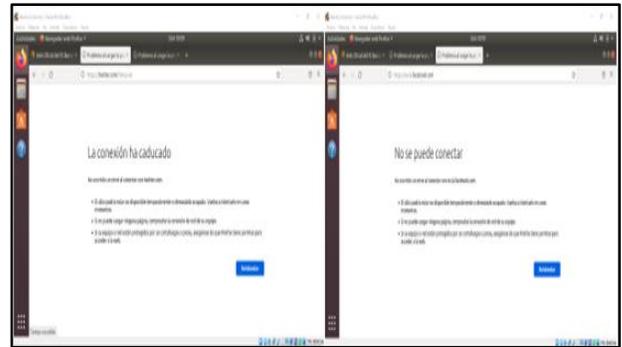


Figura 51. Comprobación de denegación.

Pero si podrá acceder a cualquier otro sitio, por el ejemplo a www.fcbarcelona.com como muestra la figura 52.

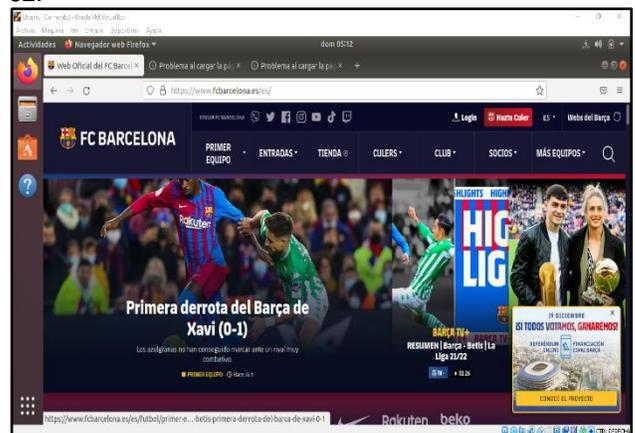


Figura 52. Acceso a otros sitios.

3.4 TEMATICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Dentro de la instalación configuración de Zentyal se establecieron algunos parámetros que permitirán terminar la implementación y configuración a los servicios de carpetas compartidas e impresoras desde Ubuntu.

Se establecieron dos controladores de red, el primero permitirá la conexión a internet tanto desde el servidor Zentyal como desde los equipos que se conecten a través del servidor, el segundo permitirá la conexión interna de los equipos clientes configurados a través del DHCP lo que nos brinda los servicios de boquear páginas, compartir archivos e impresoras etc. Ver figura 53.

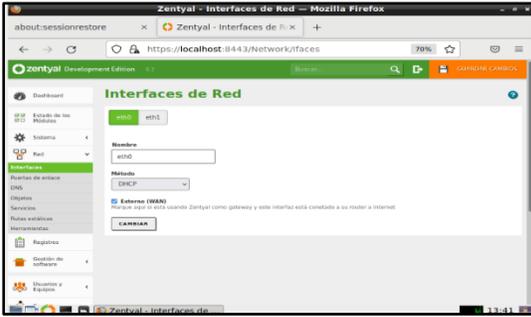


Figura 53. Verificación de red interface 0 – externa

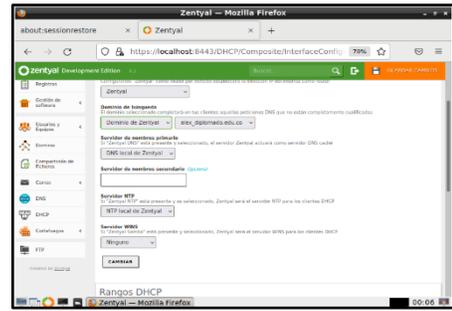


Figura 57. Configuración de DHCP



Figura 54. Verificación de red interface 1- interna

Se realiza la verificación de las interfaces de red donde la interface 0 corresponde a la red externa que permitirá acceso a Internet y la interface 1 será la red interna que permitirá conectar los diferentes clientes internos a Zentyal a través de una ip fija, la cual compartirá los recursos que se requieran, ver figura 55.

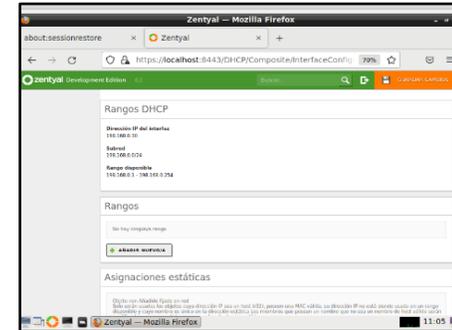


Figura 58. Asignación de rangos de IP fijas

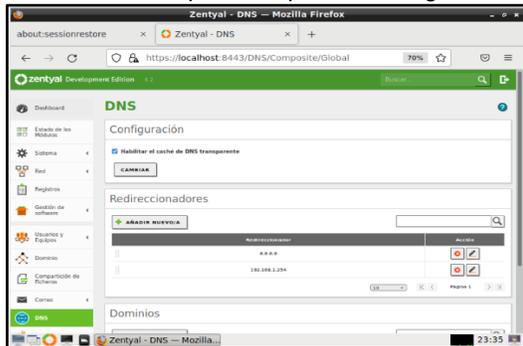


Figura 55. Definición de DNS

Se establece los DNS del proveedor de servicio o los DNS de Google, ver figura 56.

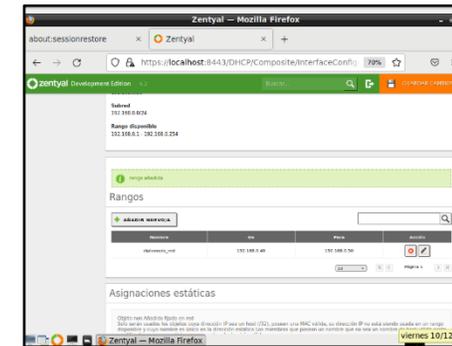


Figura 59. Asignación rangos de ip

Con la asignación de rangos de IP, el servidor Zentyal generará IP para los clientes de se conecten a la red de acuerdo al rango de IP asignadas.



Figura 56. Verificación DHCP

Se verifica en el dashboard donde ya la asignación de IP se está realizando a través del DHCP, lo cual indica que ya se puede empezar a configurar el cliente Ubuntu para compartir archivos e impresoras entre equipos que estén en el mismo rango de red, ver figura 60.



Figura 60. Reconocimiento equipo en asignación DHCP

Se procede a verificar si el módulo se encuentra activo y configurado para compartir ficheros, ver figura 61.

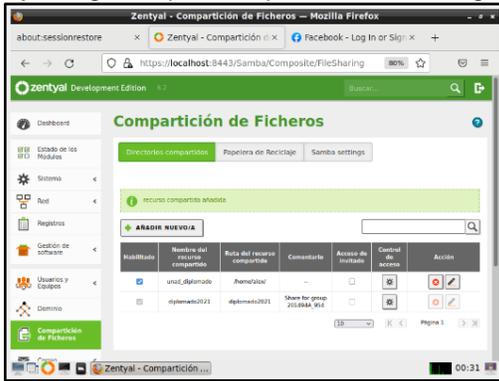


Figura 61. Verificación módulo de compartición ficheros

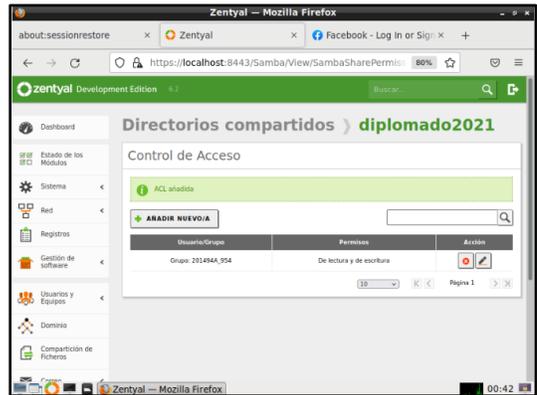


Figura 64. Control de permisos en el directorio

Realizadas las pruebas de conexión se pasa a verificar en Ubuntu Desktop la conexión y la IP asignada por el servidor Zentyal a través del DHCP, ver figura 65.

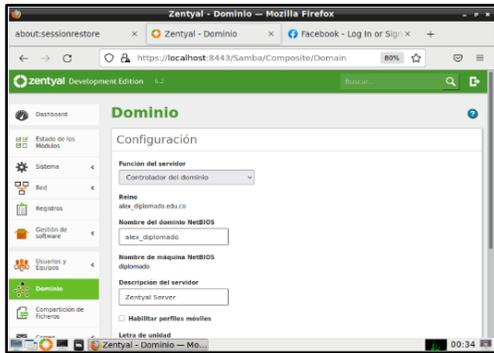


Figura 62. verificación del dominio

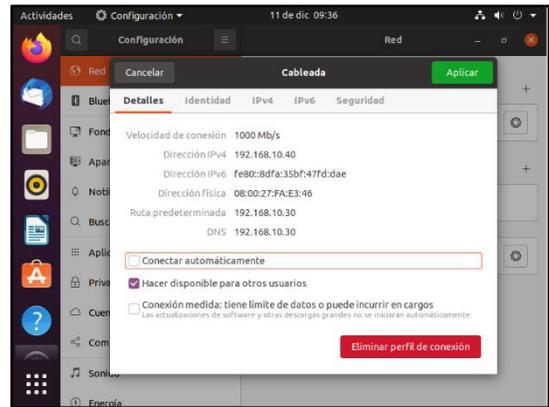


Figura 65. IP Asignada a través del DHCP del servidor Zentyal

En Ubuntu Desktop se procede a realizar la conexión con el servidor Zentyal que permitirá compartir ficheros y acceder a las carpetas del grupo y usuarios creados, figura 66.

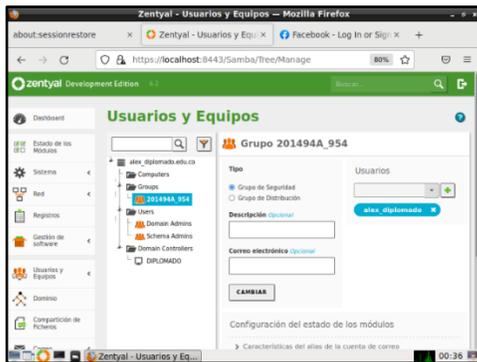


Figura 63. Configuración grupo y usuarios



Figura 66. Conexión con el servidor Zentyal

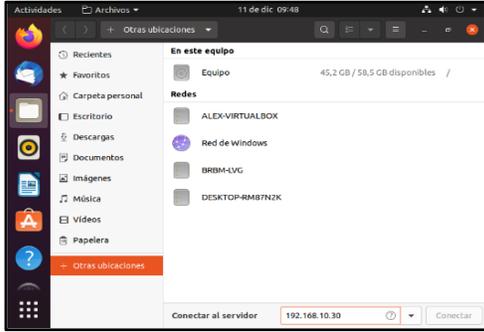


Figura 67. Conexión con el servidor Zentyal

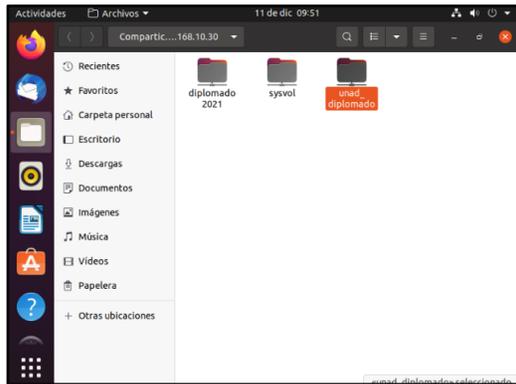


Figura 68. Acceso carpetas creadas en servidor

Compartir impresoras no se realiza con Zentyal, éste no se encuentra implementado desde la versión 5.1, este proceso se puede realizar a través de CUPS, instalado y creando la impresora que se desea compartir.

3.5 TEMATICA 5: VPN

Producto esperado: 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Seleccionamos los Paquetes de instalación necesarios para nuestro proceso, ver figura 69.

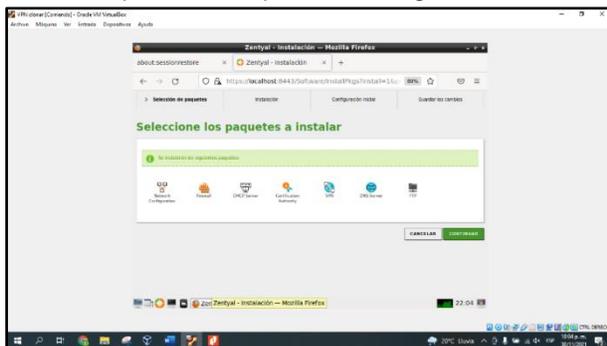


Figura 69. Instalación de paquetes

Selección de interfaces, ver figura 70.

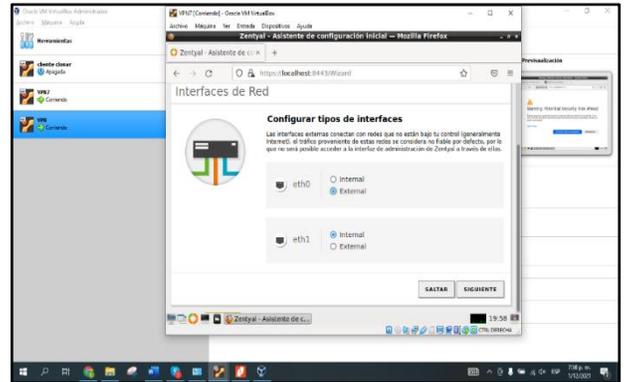


Figura 70. Interfaz

Configuración, ver figura 71

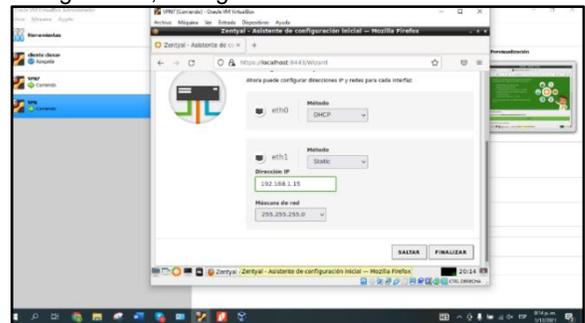


Figura 71. Direccionamiento IP

Estando en la DASHBOARD, no dirigimos al ítem de autoridad de certificación, esto con el fin de crear los certificados relacionados para el servidor VPN y el del cliente que se conectara a nuestra red, damos clic en expedir, y al final guardamos los cambios, ver figura 72.

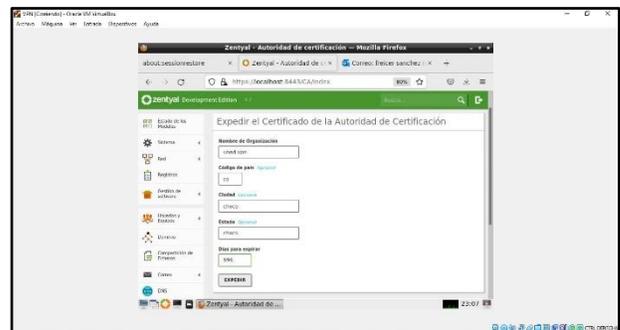


Figura 72. Certificados

Evidencia de certificados creados, ver figura 73.



Figura 73. Certificados

Ahora en el apartado VPN nos dirigimos a servidores haciendo clic, a fin de crear nuestro servidor, ver figura 74.



Figura 74. Server creado.

Creamos nuestros servicios en el apartado Red, opción servicios, añadimos los que consideremos necesitamos y guardamos los cambios al terminar, ver figura 75.

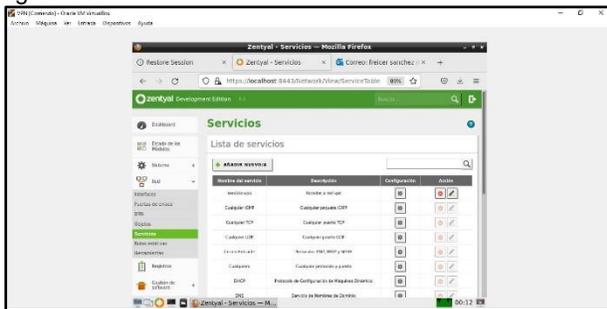


Figura 75. Servicios establecidos

Nos dirigimos al cortafuego opción filtrado de paquetes, seleccionamos reglas de redes interna a Zentyal, y lo mismo en reglas de filtrado desde redes externas a Zentyal, creamos las reglas y guardamos los cambios establecidos, ver figura 76.

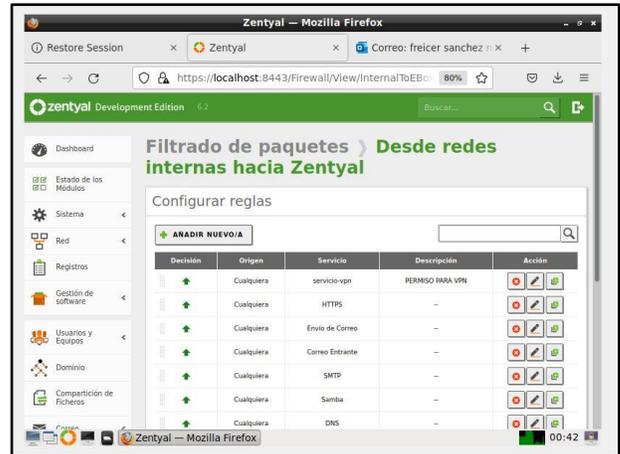


Figura 76. Reglas internas

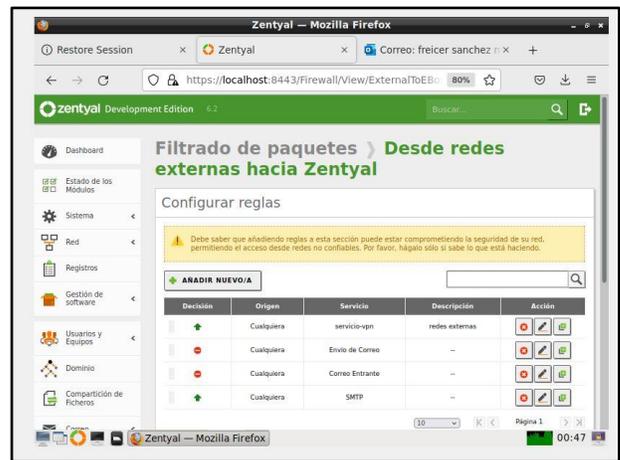


Figura 77. Reglas externas

Descargamos paquete de configuración del servidor en el apartado VPN, servidor y descargar configuración, esto serán importados al equipo cliente, ver figura 78.

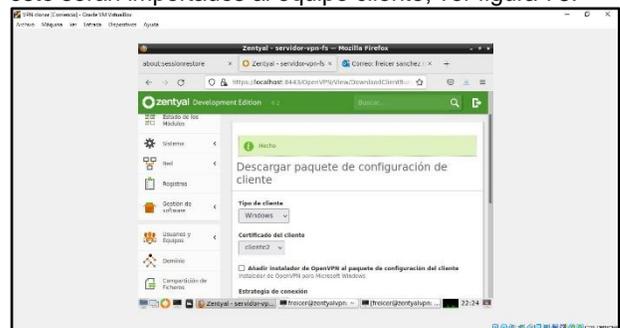


Figura 78. Descarga de archivos para cliente.



Figura 79. Zentyal

Volvemos dashboard y confirmamos que el servicio está arriba y corriendo normalmente como muestra de la configuración exitosa, ver figura 80.

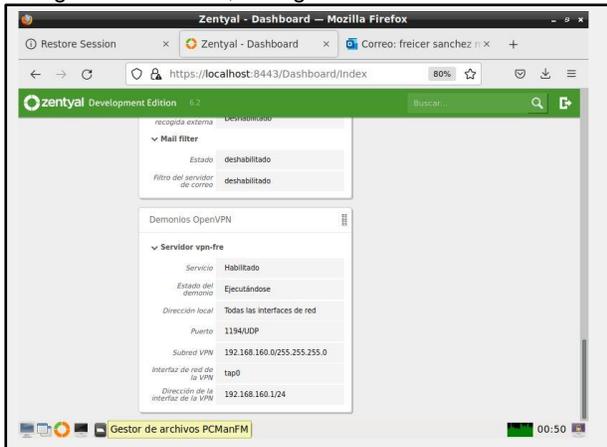


Figura 80. Estado de servicios VPN creados y demonios activos.

Hecha la configuración nos dirigimos a la página de openVPN OpenVPN Connect Client | Our Official VPN Client | OpenVPN, ver figura 81.

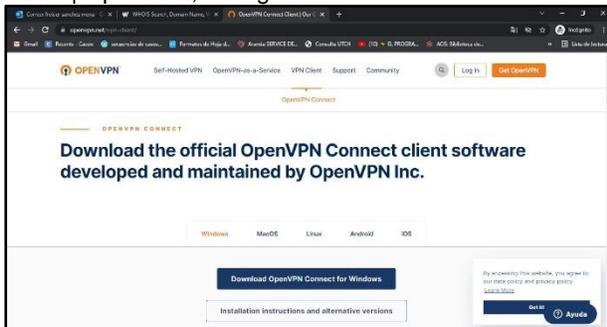


Figura 81. Descarga OPEN VPN

Terminada la descarga procedemos a instalar el software emulador, ver figura 82.



Figura 82. Instalación.

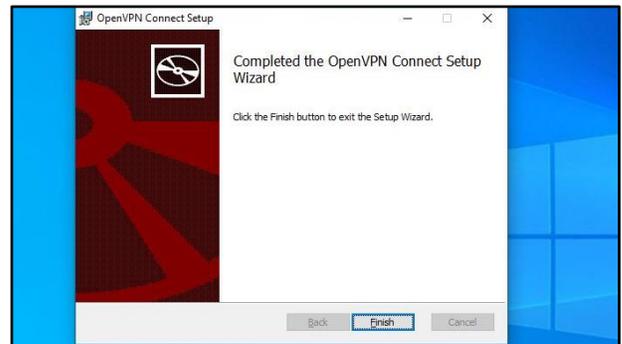


Figura 83. Finalización de la instalación

Descargamos los archivos en nuestro cliente, y extraemos en una carpeta para hacer desde allí la conexión, ver figura 84.

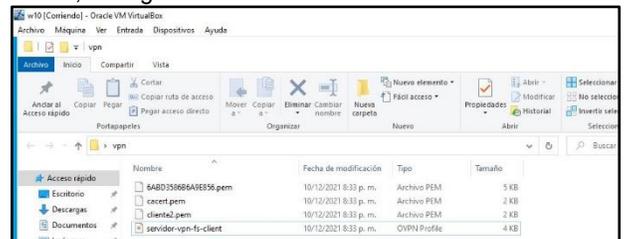


Figura 84. Archivos de configuración y conexión a zentyal

Nos dirigimos al acceso directo de Open vpn Connect, lo abrimos e importamos los archivos, ver figura 85.

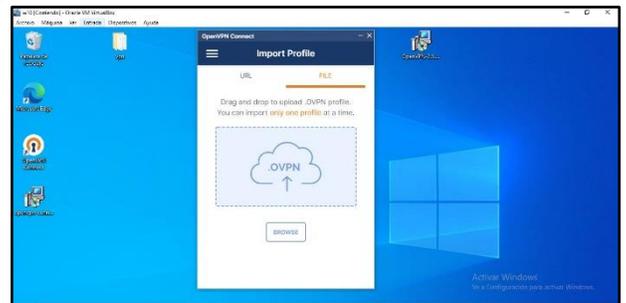


Figura 85. Importar archivo

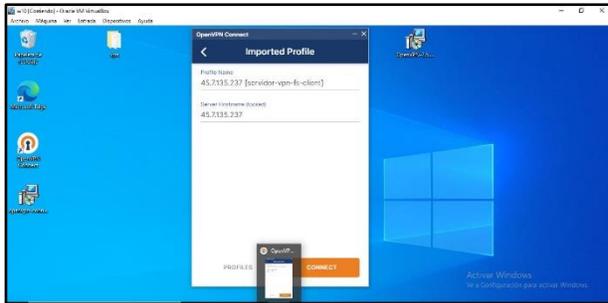


Figura 86. Conexión de archivo.

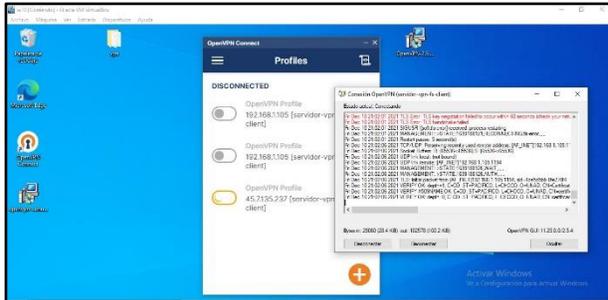


Figura 87. Conexión VPN establecida

4 CONCLUSIONES.

La experiencia que tuve con Zentyal fue satisfactoria, la instalación y configuración no es compleja, pero se requiere de conocimientos básicos para realizarla. Zentyal ofrece interoperabilidad entre servidores Windows y es un servidor completo que presenta una interfaz gráfica que es fácil de gestionar y amigable con el cliente. Los servicios que se implementaron y configuraron para esta actividad fueron DHCP, DNS y Controlador de dominio, estos le permitieron a mi máquina cliente obtener ip dinámicamente, traducir los nombres de dominio en direcciones IP y la autenticación de los usuarios creados desde Zentyal.

Con el desarrollo de esta actividad se permite comprender previamente la configuración de Zentyal en una máquina virtual. Así como permite unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet. Zentyal integra servicios como DNS/DHCP, CA, VPN, Backup, gateway, cortafuegos y proxy HTTP, por mencionar algunos.

En este documento, se utiliza Zentyal para configurar un proxy no transparente y realizar la validación en una máquina virtual Ubuntu que hace parte de la red nat configurada sin activar el servicio dhcp y en ella se hace la prueba donde se filtra la salida por medio del puerto 1230.

Los servicios que ofrece Zentyal son soluciones eficaces para las empresas de hoy día que requieren no solo una infraestructura tecnológica robusta sino también, el control centralizado de su red informática. De esta manera se evidencia que, a la hora de buscar soluciones

tecnológicas para las organizaciones, Zentyal aparece como una de las herramientas Open Source, más acorde a las necesidades de las empresas en cuanto a servicios y también en cuanto a ciberseguridad gracias a la amplia gama de módulos disponibles en su panel de control.

Compartir e imprimir ficheros y documentos en una red controlada por el servidor Zentyal brinda seguridad en la red y da tranquilidad a los usuarios ya que a través del éste servidor se puede parametrizar configuraciones para que determinados equipos o usuarios pueda acceder a ciertos ficheros sin necesidad de exponer toda la información completa en toda la red, sino que se comparte y se da acceso de acuerdo al nivel de privacidad e importancia que cada usuario pueda tener dentro de una organización.

Una VPN es una Red Privada Virtual, es decir, un servicio que cifra los datos de nuestra navegación en Internet. Es un "túnel seguro" que crea una red privada y segura entre la conexión a Internet que estamos utilizando y los servidores de Internet.

El servidor VPN es un servidor externo que interviene en los intercambios de información que se producen, de esta forma se aseguran los datos privados y se mantiene la confidencialidad e integridad de nuestra información.

De una manera más sencilla, se podría decir que Internet es una vía de comunicación e intercambio (como una autopista) por la que circulan datos que viajan en paquetes de información de un destino a otro.

Cada vez que accedemos a un enlace en Internet, nuestro equipo debe identificarse y enviar la solicitud de la información que queremos a los proveedores de servicios para que le respondan con la respuesta que estamos buscando. Es decir, hay un canal de comunicación continuo y bidireccional.

5 REFERENCIAS

- [1] Apéndice A: Entorno de pruebas con VirtualBox. (2021). Obtenido de Zentyal Community: <https://doc.zentyal.org/es/appendix-a.html>
- [2] Configuración de un cortafuegos con Zentyal. (2021). Obtenido de Zentyal Community: <https://doc.zentyal.org/es/firewall.html>
- [3] Guzman, D, A. (30 de noviembre 2021). octava Webconferencia del curso: Solucionando necesidades específicas con GNU/Linux. Recuperado de: <https://bit.ly/3Ed73xe>