ACTIVANDO SERVICIOS DE SOPORTE IT PARA INTRANET Y EXTRANET EN ORGANIZACIONES EMPRESARIALES, UTILIZANDO SISTEMAS BASADOS EN GNU/LINUX.

Dilan Fabian Bocanegra Cardenas
e-mail: dfbocanegrac@unadvirtual.edu.co
Walter José Patiño Caro
e-mail: wjpatinoc@unadvirtual.edu.co
Eberto Alber Acuna
e-mail: eaacuna@unadvirtual.edu.co

RESUMEN: *Implementación de servicios de infraestructura IT para intranet y extranet en la institución, realizado después de solucionar las problemáticas de migración de sistemas operativos, servicios y puesta en marcha de los servicios solicitados. Los ingenieros a cargo del despliegue del proyecto desarrollaron el trabajo fragmentado en los puntos críticos a atender en la solicitud del cliente, los cuales fueron DHCP server, DNS server y controlador de dominio, proxy no transparente, cortafuegos, file server y prima server y VPN, con lo anterior ejecutando, el sistema del cliente puede ser inicializado y empezar la operación.*

PALABRAS CLAVE: Controlador de dominio, proxy, red privada virtual (VPN), Zentyal.

1 INTRODUCCIÓN

Hoy en día el sistema GNU/Linux es "líder indiscutible" en software en el mundo, fue el 14 de marzo de 1994 cuando finalmente se lanzó al público por primera vez su versión 1.0.0, que constaba de 176.250 líneas de código [1], impulsado por el ingeniero Linus Torvalds. La institución requiere soporte con la migración de su sistema, a software basado en GNU/Linux.

El objetivo del proyecto para la empresa internacional proveedores de servicios de internet ISP, es la implementación de un centro avanzada de comunicaciones backbone donde serán soportado los servidores con el sistema operativo Linux.

2 DESARROLLO DE LA ACTIVIDAD

2.1 Temática 1: DHCP Server, DNS Server y Controlador de Dominio.

Iniciando la instalación de Zentyal; es necesario descargar el sistema operativo desde el sitio web oficial, después proceder con la puesta en marcha del sistema, a continuación de evidencian los procesos:

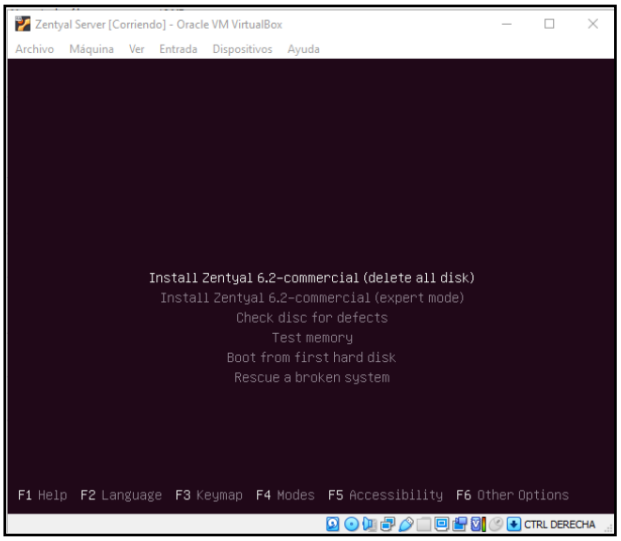

Figura 1. Instalando Zentyal

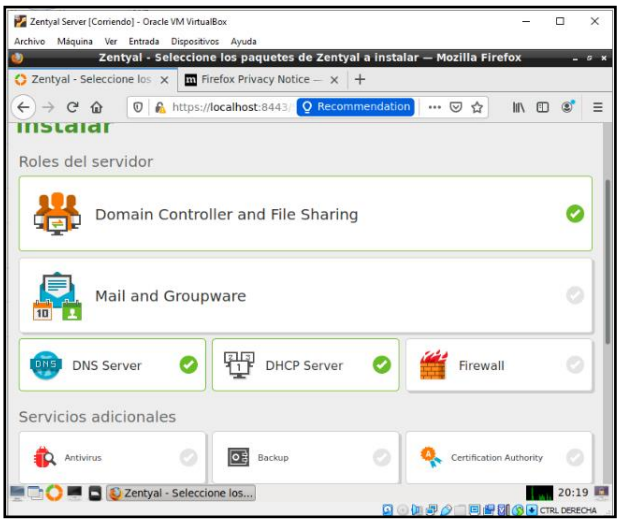

Figura 2. Selección de módulos DNS, DHCP & Domain controller

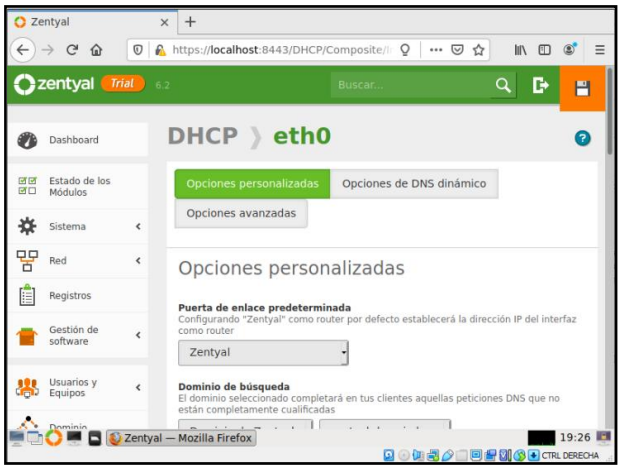

Figura 3. Configurando servidor DHCP

Se continua con el proceso de configuración del servidor DHCP, en este punto se configura el dominio de búsqueda, el servidor de nombres primarios y secundarios.

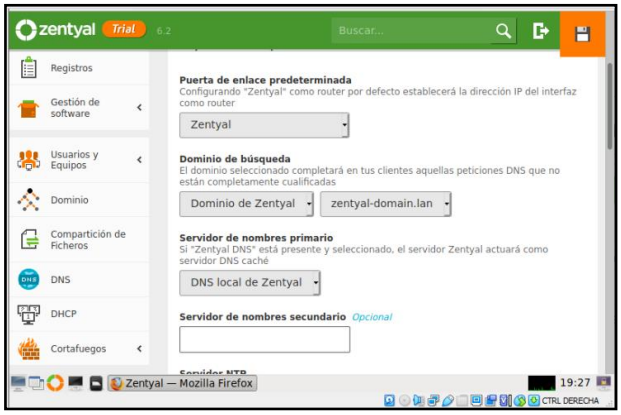

Figura 4. Paso dos de configuración DHCP

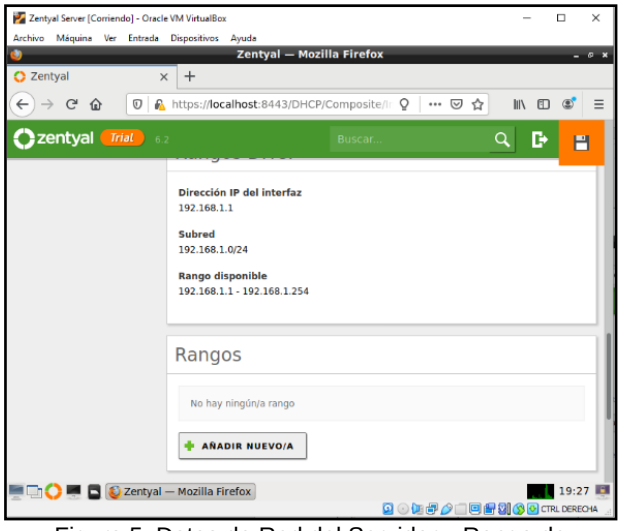

Figura 5. Datos de Red del Servidor y Rango de Direcciones que asigna

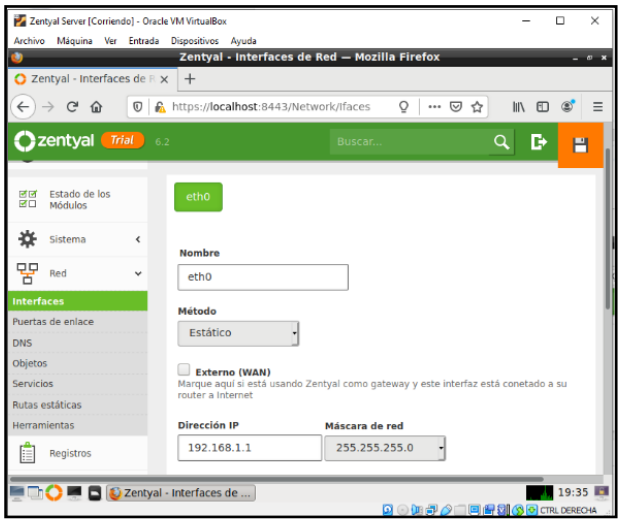

Figura 6. Configurando interfaces de red

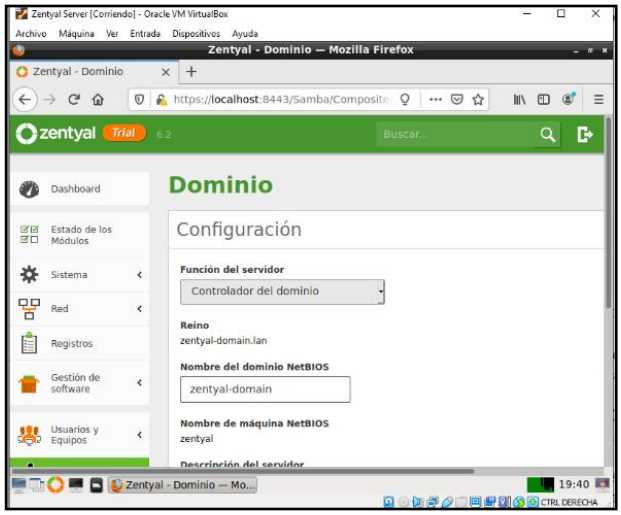

Figura 7. Configurando controlador de dominio

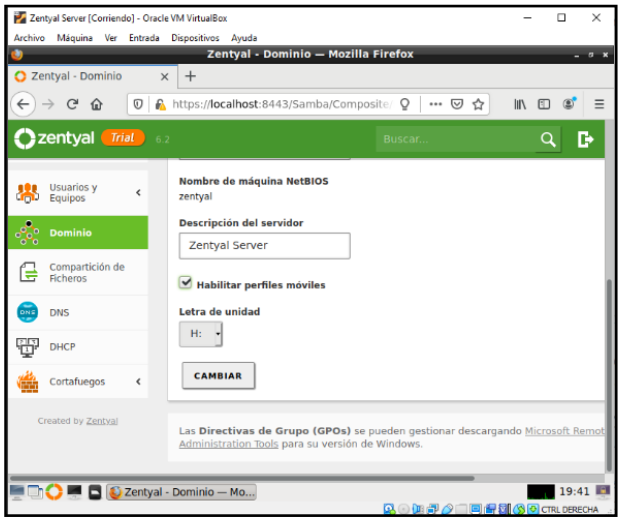

Figura 8. Configurando controlador de dominio paso 2

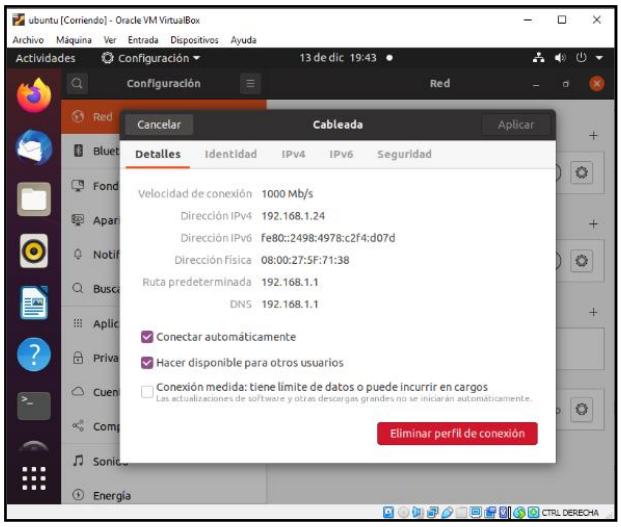

Figura 9. Verificando configuración desde cliente GNU/Linux

2.2 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 1230.

Es necesario configurar las interfaces de red de la maquina zentyal, interfaz 1 como NAT e interfaz dos como red interna.

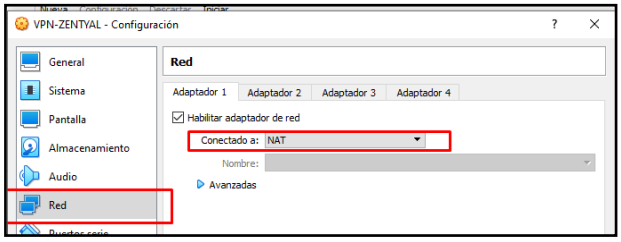

Figura 10. Configuración interfaz de red uno

Figura 11. Configuración interfaz de red dos

En el equipo de cliente también se requiere de la configuración de red, interfaz uno como red interna e interfaz dos como adaptador de puente.

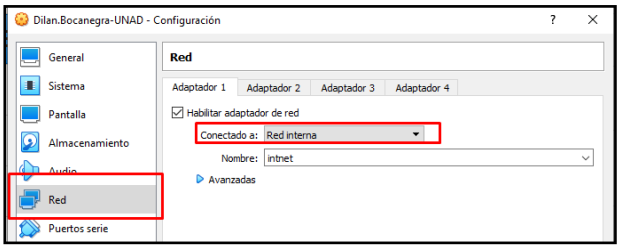

Figura 11. Configuración interfaz de red uno

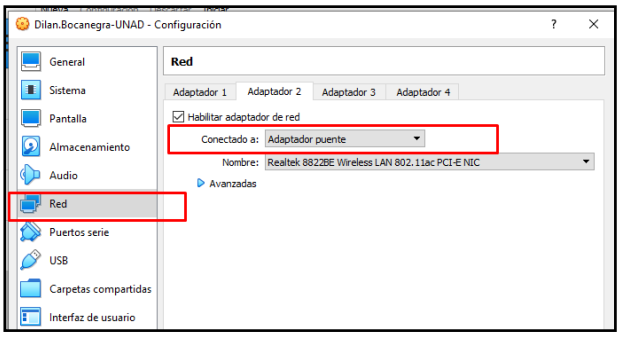

Figura 12. Configuración interfaz de red dos

Ingreso a menú interfaces de red, configuramos la red inicial con método DHCP, marcamos la opción externo WAN y damos clic en el botón CAMBIAR.

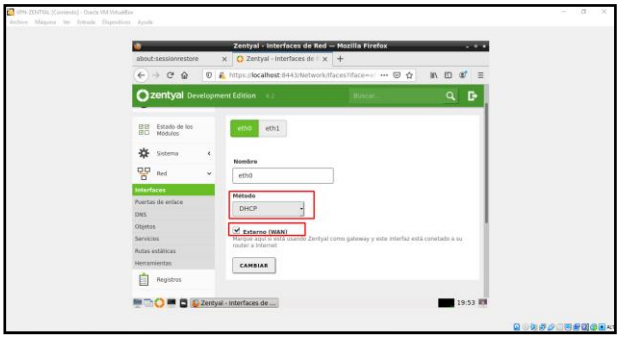

Figura 13. Configuración red inicial

Configuramos la red secundaria con método Estático, no se marca la opción externo WAN, Se ingresa una ip que se comporta como Gateway para los equipos cliente y clic en el botón CAMBIAR para guardar los cambios.

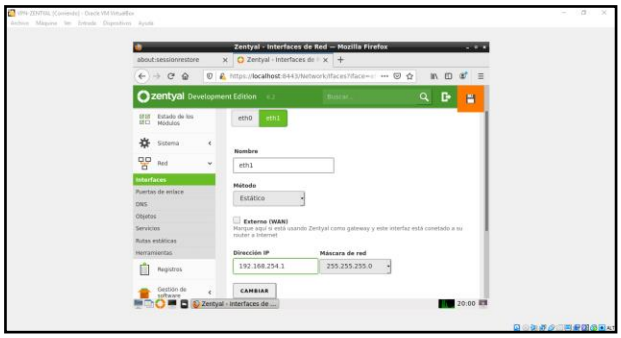

Figura 14. Configuración red inicial

Ahora crearemos un objeto para identificar los equipos en red, seleccionamos objetos, dar clic en el botón Añadir Nuevo Colocamos el nombre.

Figura 15. Creación de objeto identificador

Luego de añadir el objeto verificamos su creación en la lista inferior para poder realizar las configuraciones correspondientes.

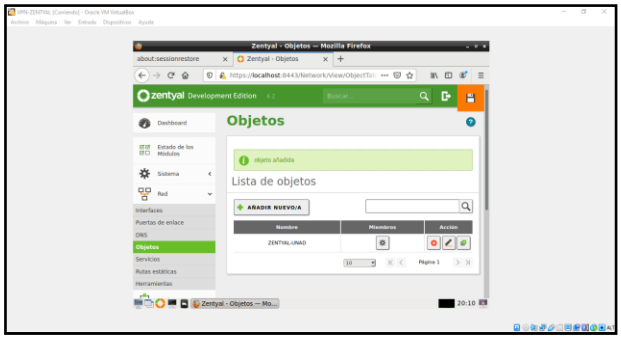

Figura 16. Verificando creación de objeto.

En este estado del proceso se hace necesario ingresar a la maquina cliente, para configurar una dirección ip fija y configurar el Gateway apuntando al servidor

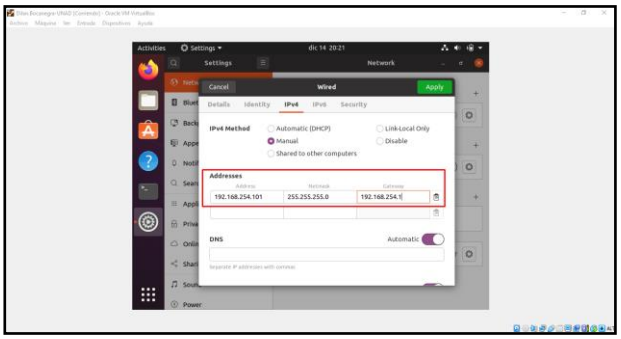

Figura 17. Configuración de red en cliente

De regreso en el servidor zentyal, clic en el icono de miembros para agregar usuarios necesarios, se encuentra como una opción del objeto que creamos anteriormente. Se ingresan los datos de la maquina cliente, en la opción de dirección ip colocar CIDR, ingresamos la ip de la maquina cliente y damos clic en botón añadir para seguir con el proceso.

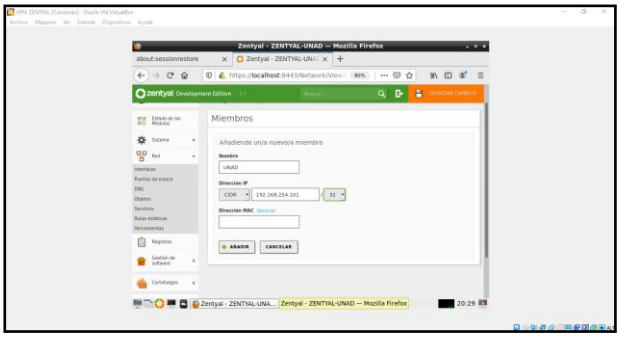

Figura 18. Creando usuario para servicio

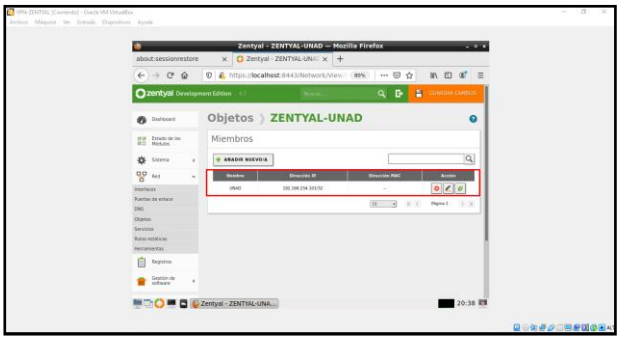

Figura 19. Validando información de nuevo usuario

En el menú del lado izquierdo ingresar al módulo Proxy HTTP y seleccionar la opción Configuración General.

Validamos que la opción proxy transparente no esté seleccionada, en la opción puerto ingresamos el puerto 1230 y clic en el botón CAMBIAR para seguir con el proceso.

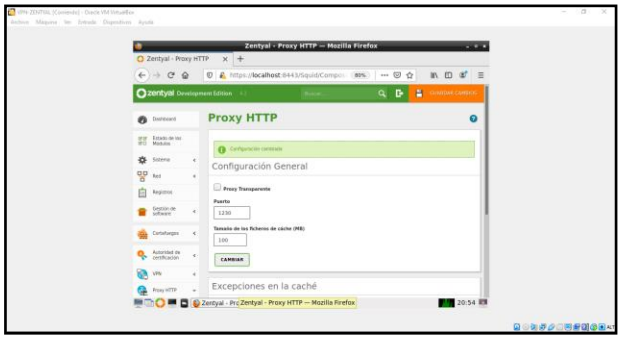

Figura 20. Creación de proxy

Es necesario crear reglas de trabajo para los usuarios, en el menú a la izquierda, ingresamos a Proxy HTTP, seleccionamos la opción Reglas de acceso y Damos clic en el botón Añadir Nuevo para agregar reglas a usuarios.

En la opción origen ingresamos el objeto creado anteriormente y en la opción decisión seleccionamos denegar todo, después clic en el botón Añadir para seguir, y ahora estaría configurado el proxy para trabajar los usuarios.

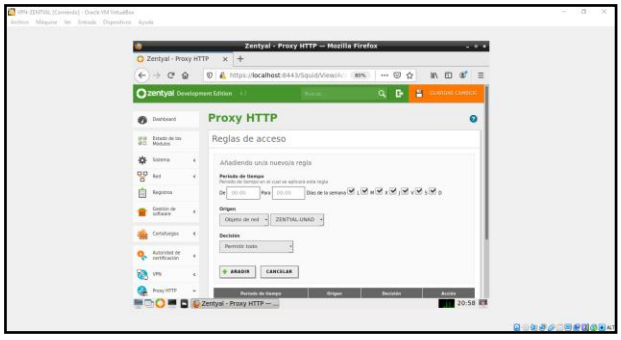

Figura 21. Configurando reglas de acceso

Reiniciamos las maquinas, el servidor y el cliente, luego regresamos al equipo cliente y configuramos el proxy en el navegador, en la barra de menú ingresamos a editar y seleccionamos la opción preferencias. En la sección inferior de preferencias, en la opción configuración de red, dar clic en el botón de configuración.

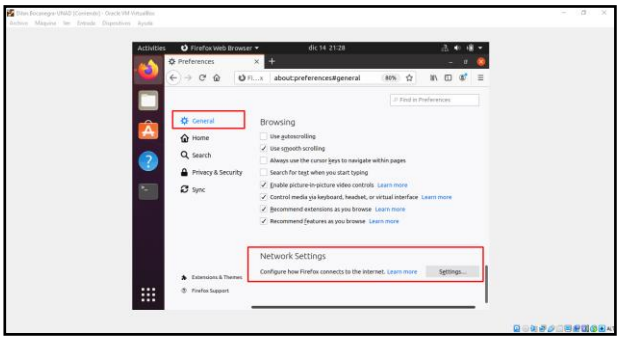

Figura 22. Configurando ajustes de red en cliente

Se requiere ingresar los datos del proxy, marcamos la opción configuración manual proxy, ingresamos los datos de la ip del servidor 192.168.254.1, con el puerto 1230 que está configurado en el servidor y seleccionamos la opción usar para toda la configuración.

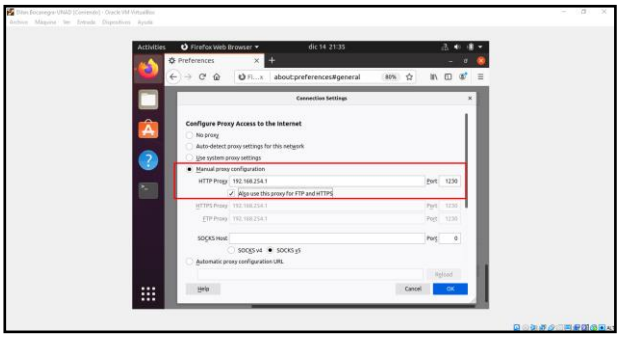

Figura 23. Configurando proxy en navegador de cliente

Validamos en navegador de la maquina cliente el acceso a sitio, escribimos la dirección de un sitio web y verificamos que el servidor proxy no permita la navegación.

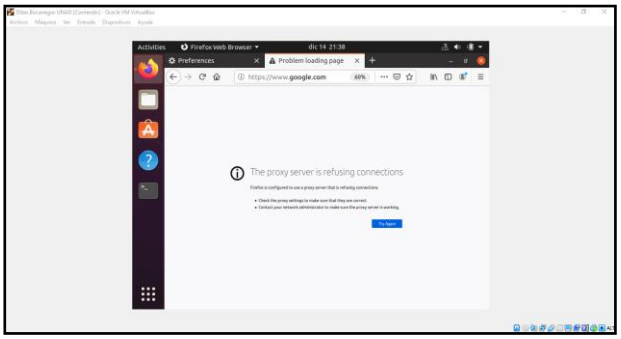

Figura 24. Validando funcionamiento de proxy

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

Antes de la puesta en marcha del sistema zentyal, es necesario configurar las interfaces de red del dispositivo.

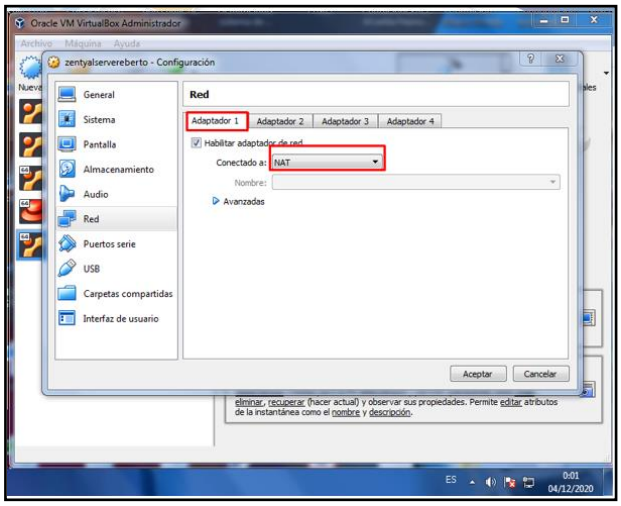

Figura 25. Configurando interfaz de red uno para zentyal

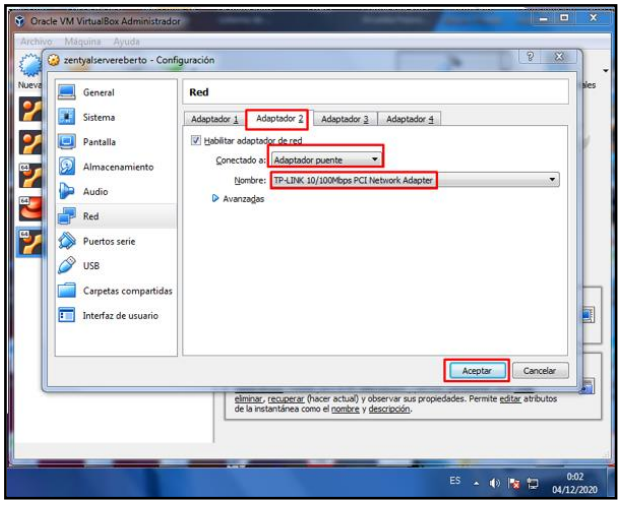

Figura 26. Configurando interfaz de red dos para zentyal

Para poder realizar la configuración de nuestro cortafuegos primero debemos configurar la red de nuestro servidor zentyal y lo realizamos con la configuración del DHCP, Protocolo de configuración dinámica de Host. Utilizando lo configurado en la ip y la máscara de red con lo cual tenemos un rango de 8 bits para la red y tenemos disponibles desde 1 a 254 ip y podremos configurar nuestro DHCP.

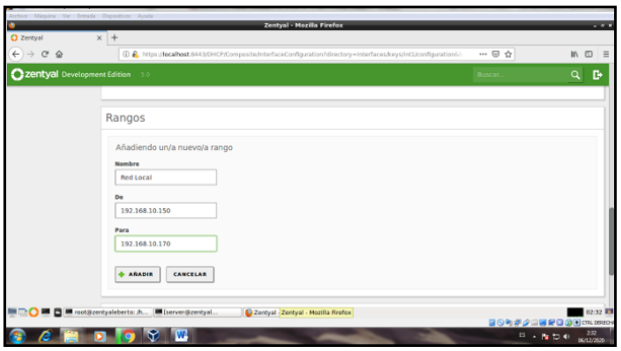

Figura 27. Configurando segmento IP

Después de realizar la configuración del servicio DHCP, procedemos a iniciar la maquina Ubuntu cliente para verificar que se encuentre funcionando nuestro servicio y que se puede conectar a nuestro servidor zentyal.

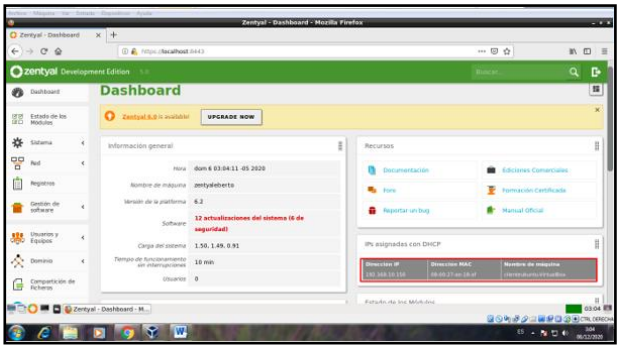

Figura 28. Ingreso desde servidor externo

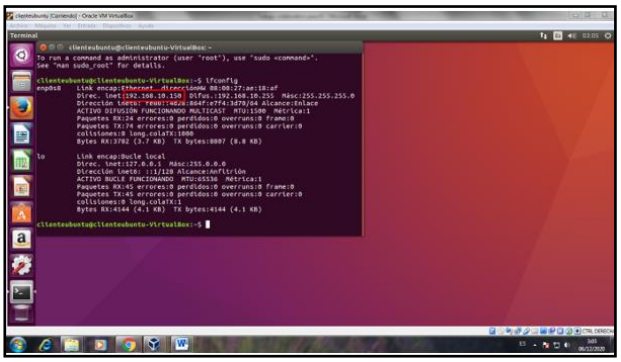

Figura 29. Confirmando en línea de comandos conexión con servidor.

Para el proceso de configuración del cortafuego o firewall en nuestro servidor zentyal y su respectiva comprobación en el cliente Ubuntu, verificamos la navegación en web.

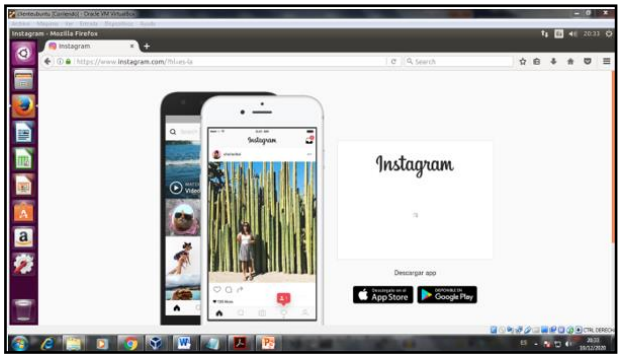

Figura 30. Validando navegación web desde cliente.

Para realizar la configuración del firewall en la red LAN. Es necesario bloquear la red social Facebook para lo cual se configura el cortafuegos de tal manera que bloquee el protocolo https y es necesario tener todas las ip que tiene asignadas el dominio Facebook.com. estas direcciones ip o rangos se pueden encontrar en la siguiente dirección web: https://bit.ly/3a97cFW

Teniendo claro las direcciones ip a aplicar con las reglas y políticas del cortafuegos de zentyal, se empieza por crear un objeto de red en donde se puede agregar todas las CIDR (Ruteo interno de dominios sin clases) es un estándar de red para la interpretación de direcciones IP.

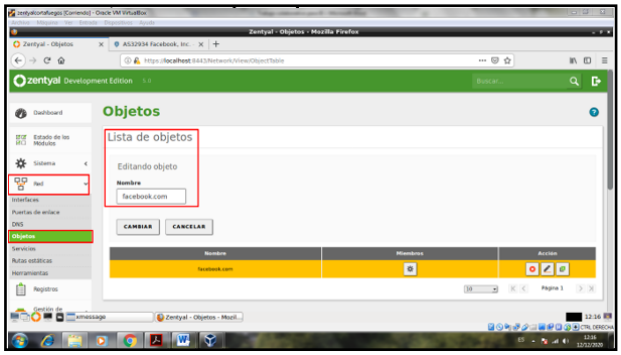

Figura 31. Creación de objeto.

Agregamos cada uno de los miembros que compone nuestro objeto y guardamos cambios después de agregar todas los CIDR.

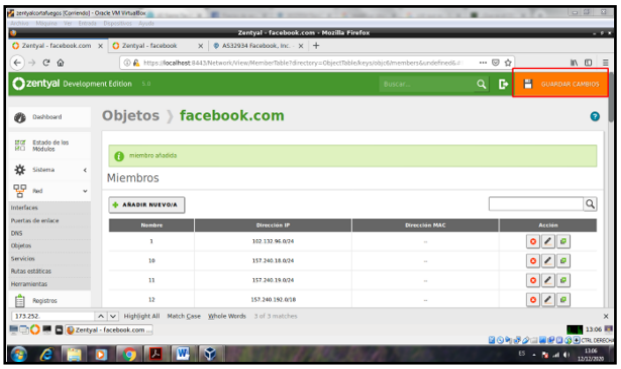

Figura 32. Validando objetos creados.

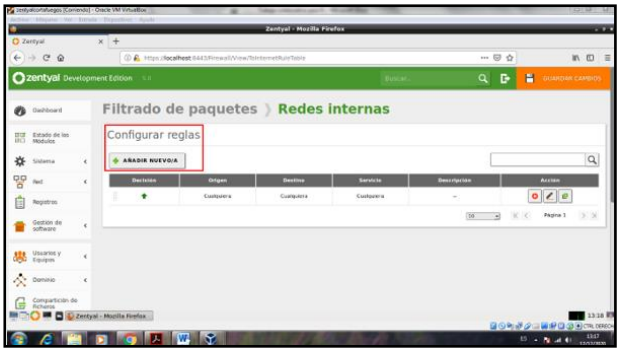

Figura 33. Creando filtrado de paquetes

Procedemos a realizar la configuración de las reglas y políticas del cortafuego. Reglas de filtrado para redes internas.

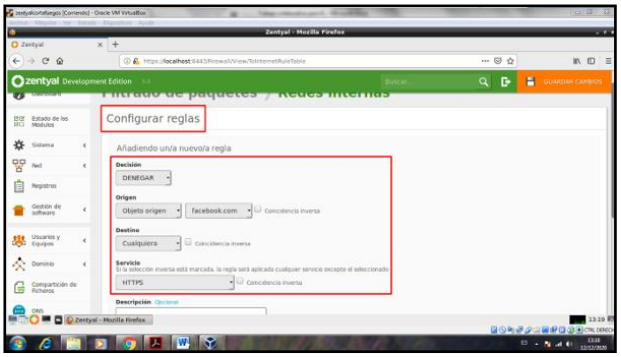

Figura 34. Configurando reglas.

Guardados los cambios de las configuraciones realizadas, ingresamos al cliente y validamos navegación web.

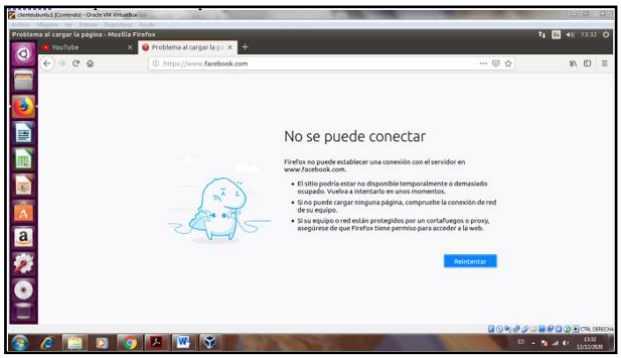

Figura 35. Validando navegación en red social

Validamos acceso a otras paginas

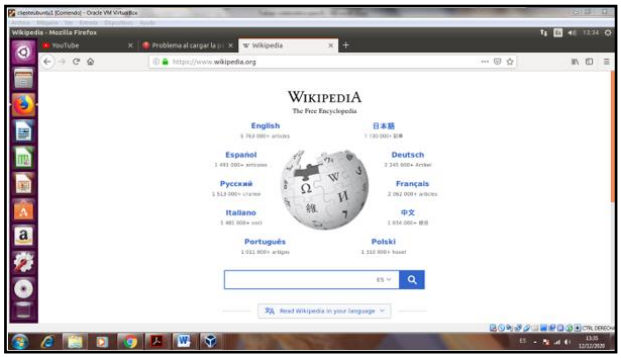

Figura 36. Navegando otras fuentes de información

2.4 Temática 4: File Server y Print Server

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

La ruta inicial, es dirigirnos al módulo dominio

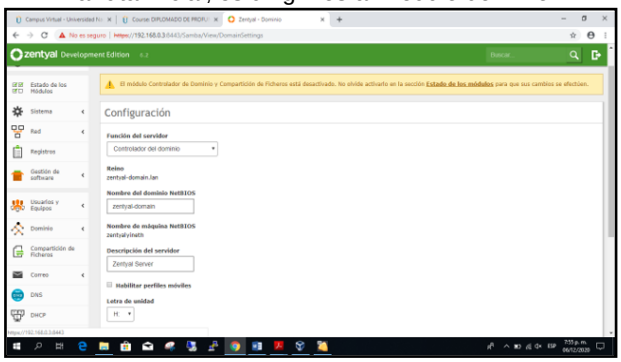

Figura 37. Ingreso módulo de dominio

En el primer ingreso al módulo, se puede ver en la parte superior aparece un mensaje de alerta que indica que el controlador de dominio y ficheros se encuentra desactivado. Para ello nos dirigimos a “estados de los módulos” esto con el fin de activarlo.

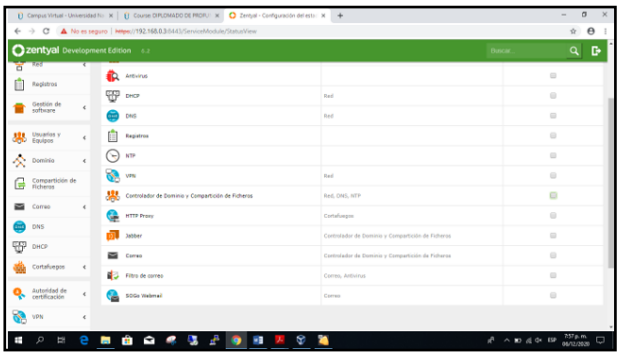

Figura 38. Habilitando controlador

Se habilita la casilla de “controlador de dominio y compartición de ficheros”, también se aceptan condiciones.

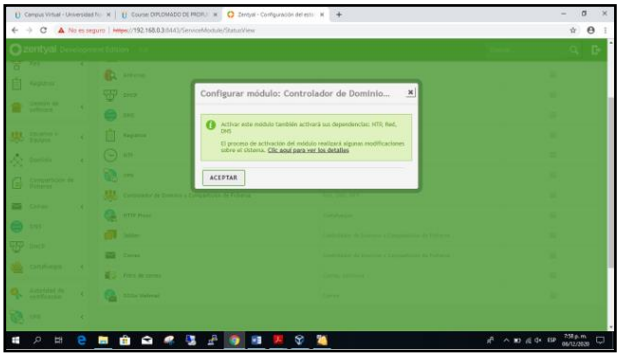

Figura 39. Aceptando cambios en habilitación

Se guardan los cambios en el botón naranja de la parte superior derecha que dice guardar cambios.

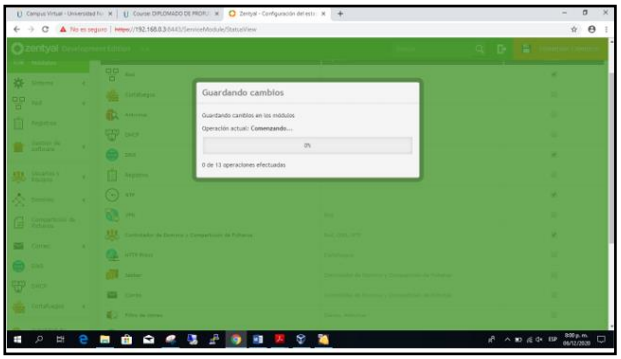

Figura 40. Guardando configuración.

La siguiente sección a la que nos dirigimos es a la opción Usuarios y Equipos, entonces se crea un grupo.

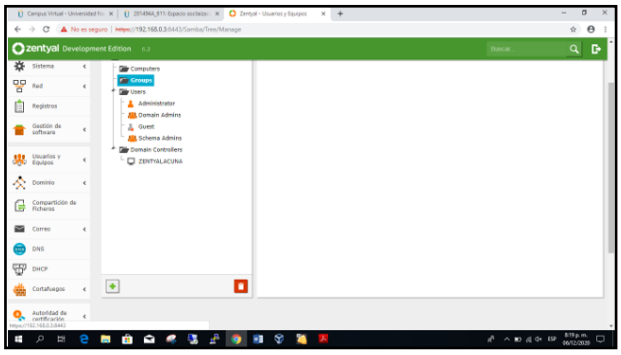

Figura 41. Sección usuarios y equipos.

ingresamos los datos del grupo.

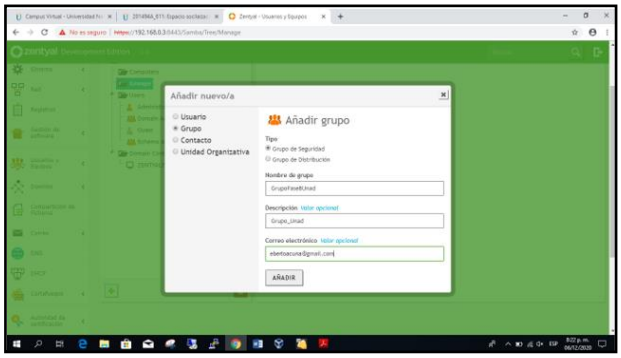

Figura 42. Ingresando datos de grupo.

Creamos el grupo y confirmamos aparición de este, en listado de grupos.

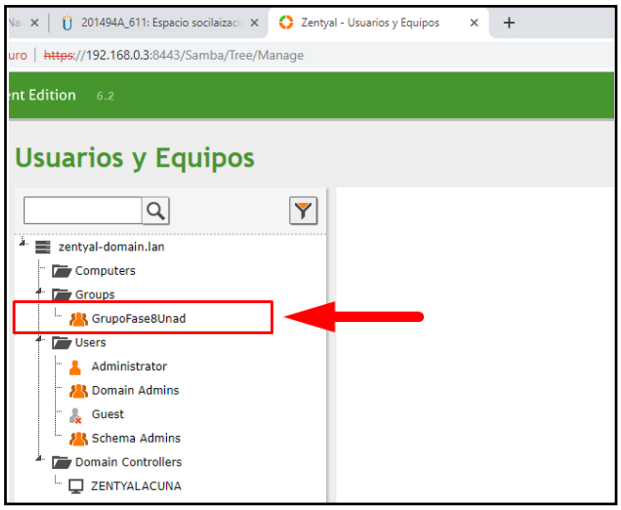

Figura 43. Verificando creación de grupo.

También es necesario crear un usuario.

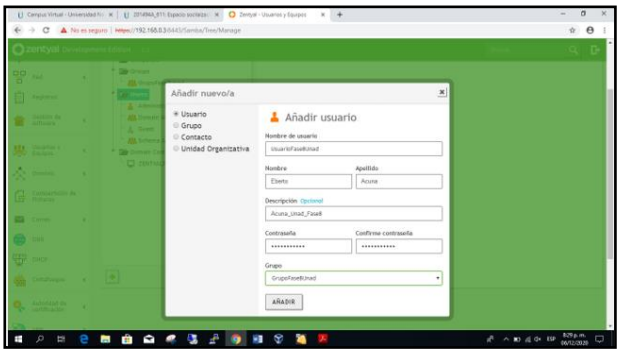

Figura 44. Creando usuario para servicio.

Verificamos usuario creado

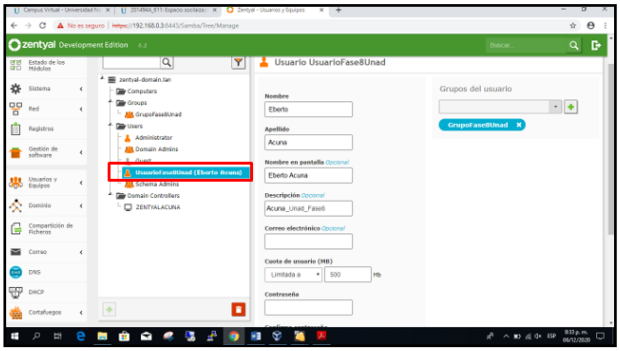

Figura 45. Verificando creación de usuario.

Es necesario vincular el usuario creado a los grupos correspondientes.

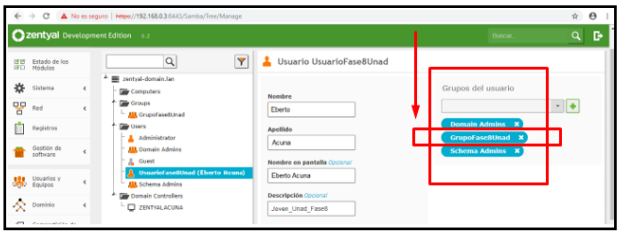

Figura 46. Vinculación de usuario a grupos.

Una vez configurados estos puntos, es necesario validar conexión con el sistema operativo cliente. Es una maquina Ubuntu y se ejecuta ping hacia la maquina con zentyal, para validar la comunicación de los dos sistemas.

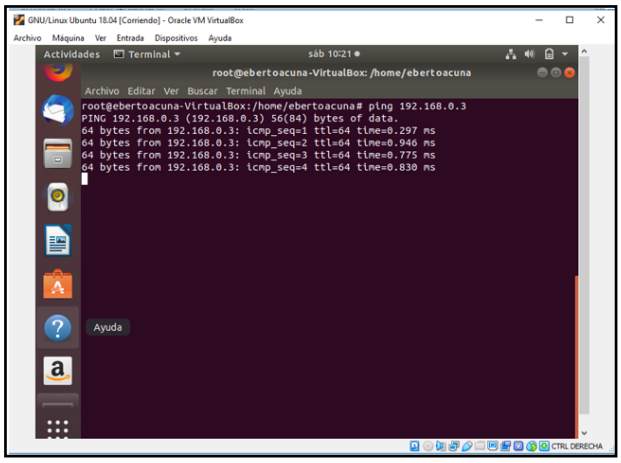

Figura 47. Ping desde cliente a servidor.

Para comunicar la máquina Ubuntu al dominio creado es necesario descargar he instalar los siguientes paquetes: libglade2, likewise- open y likewise-open-gui. Esto se realiza en la máquina Ubuntu desde consola como ROOT.

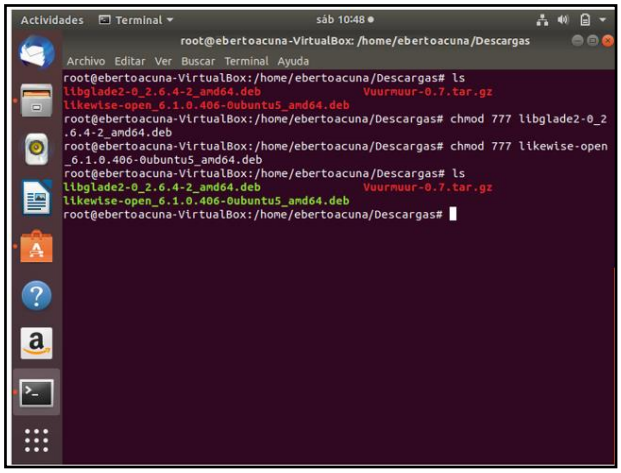

Figura 48. Instalando paquetes para comunicación.

También necesitamos instalar likewise-open-gui.

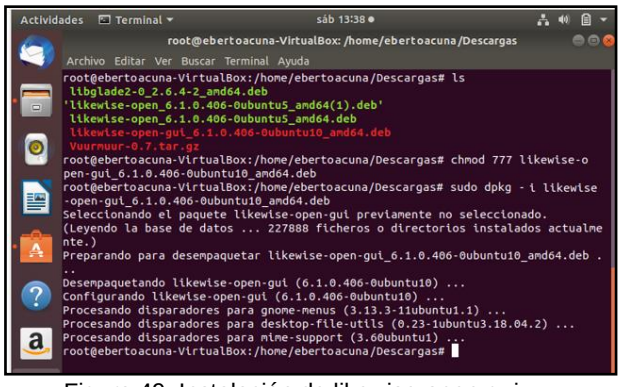

Figura 49. Instalación de likewise-open-gui.

Se procede a reiniciar el sistema de Ubuntu Desktop y desde el servidor Zentyal se procede a crear y configurar el recurso compartido de la siguiente manera:

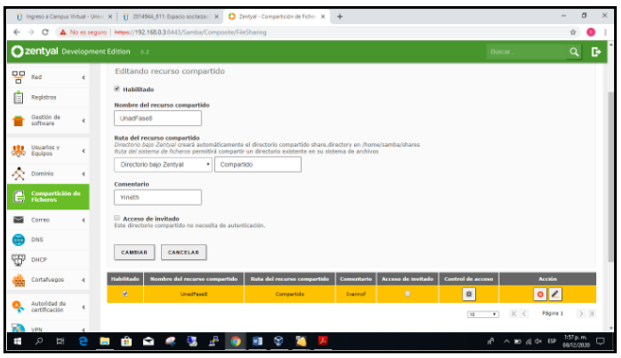

Figura 50. Opción de compartición de ficheros.

En la opción “Control de Acceso” se asocia el recurso compartido con el usuario y grupo creado previamente, adicional se asigna permisos de lectura y escritura.

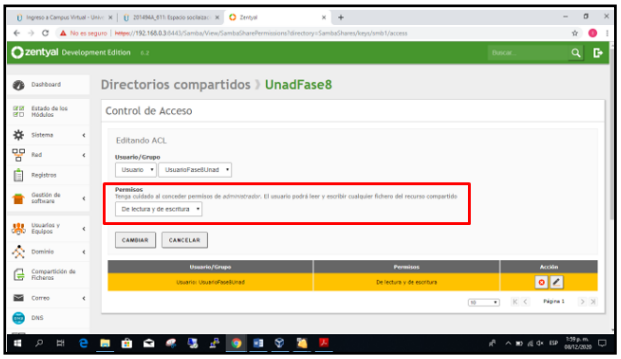

Figura 51. Asignando permisos de lectura y escritura

Una vez que esta creado el recurso compartido “UnadFase8” desde el servidor Zentyal, se procede a validar conexión desde Ubuntu Desktop:

Desde el gestor de archivos de Ubuntu en la parte inferior que dice “Otras Ubicaciones” se introduce lo siguiente en el campo conectar al servidor: smb://192.168.0.3. Que es la dirección del servidor Zentyal. Y clic en “Conectar”.

Figura 52. Conexión desde cliente a servidor.

Se observa en la siguiente imagen, desde Ubuntu el recurso compartido creado en Zentyal.

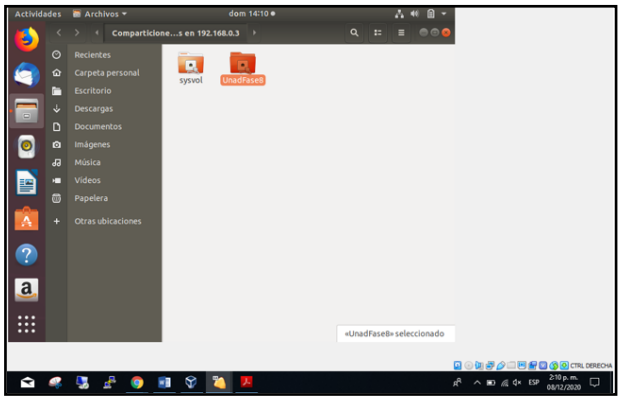

Figura 53. Verificación de recurso compartido.

Dando doble clic en el recurso compartido este nos solicita las credenciales de acceso previamente creadas desde Zentyal.

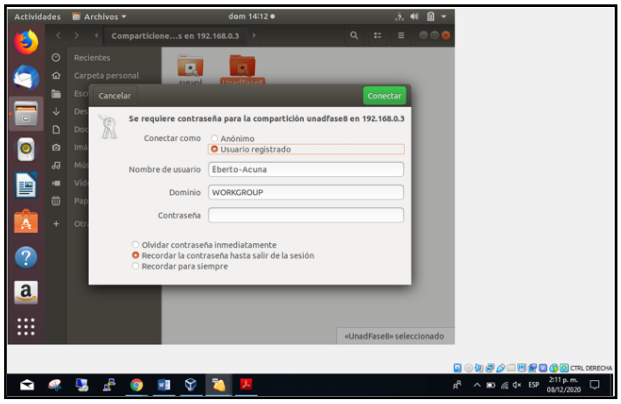

Figura 54. Solicitud de credenciales del recurso.

2.5 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 la configuración inicial de zentyal, es necesario instalar el modulo para VPN.

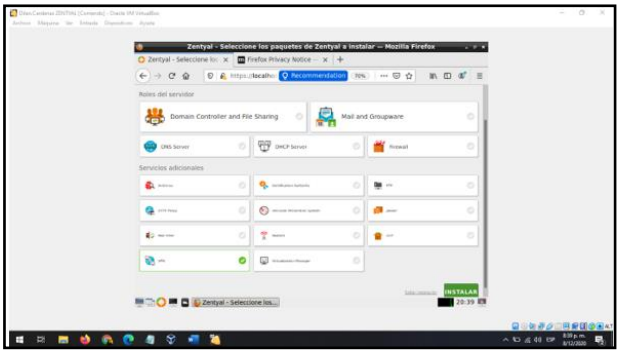

Figura 55. Instalación de modulo VPN.

Confirmamos instalación de paquetes.

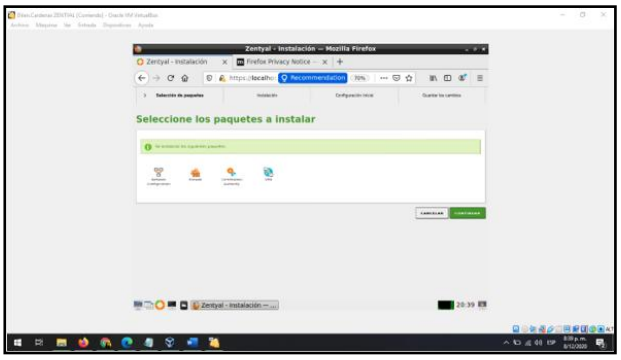

Figura 56. Instalación de paquetes necesarios.

Después de la instalación del modulo VPN y de los paquetes necesarios, una nueva ventana aparece.

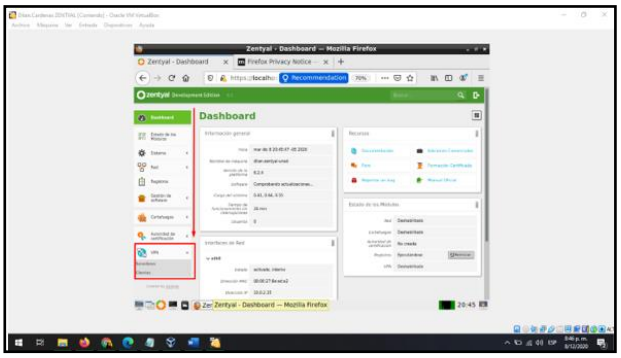

Figura 57. Nueva ventana de opciones VPN.

Desde la opción de estado de módulos, se ubica las opciones con las que trabajaremos y guardamos los cambios.

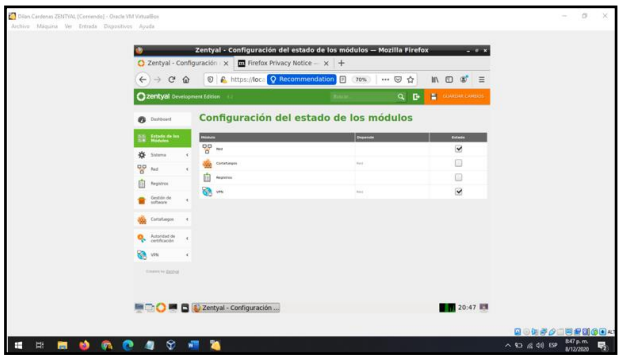

Figura 58. Configurando estado de módulos.

Es necesario guardar los cambios en el estado de los módulos.

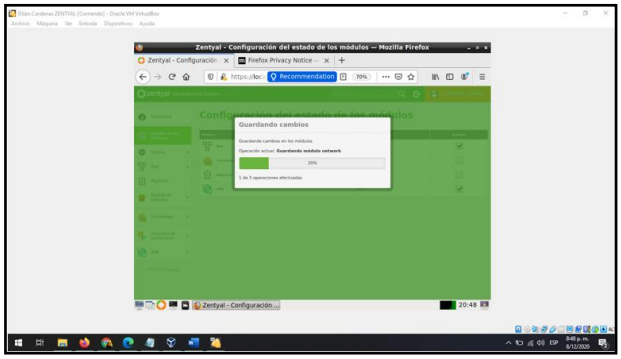

Figura 59. Guardando cambios en módulos.

El siguiente paso es crear un certificado de autoridad, para poder crear un servidor VPN.

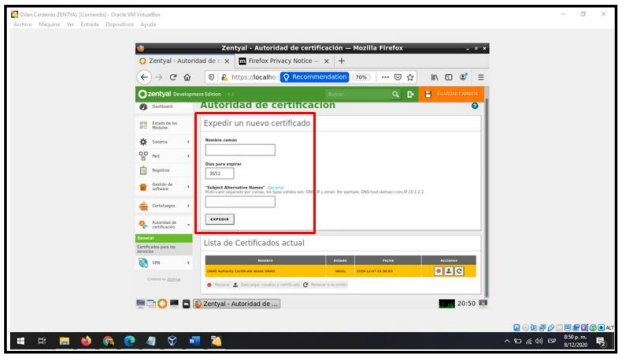

Figura 60. Creación de certificado de autoridad.

El paso por seguir es crear el servidor VPN

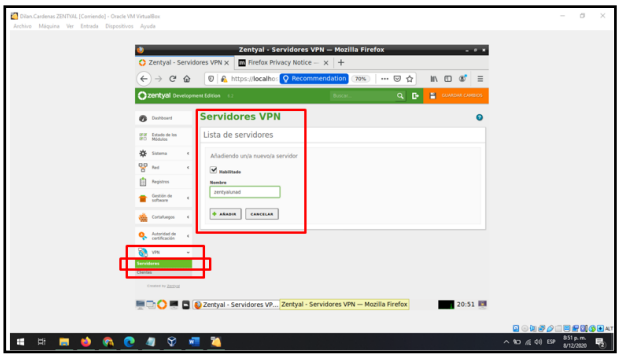

Figura 61. Creación de certificado de autoridad.

Descargaremos el certificado del servidor para que pueda ser usado en el cliente.

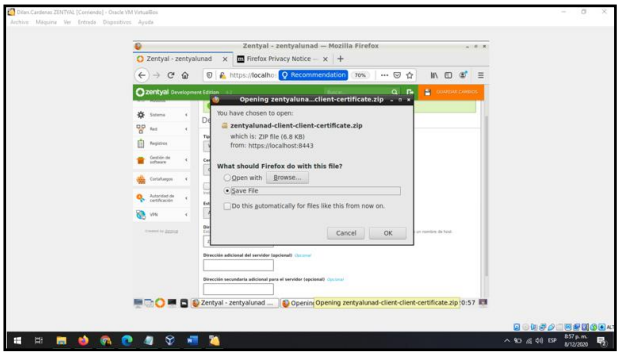

Figura 62. Descargando certificado para cliente.

Después de los procesos realizados, desde la maquina cliente, se utiliza el archivo de certificado de cliente para poder tener comunicación.

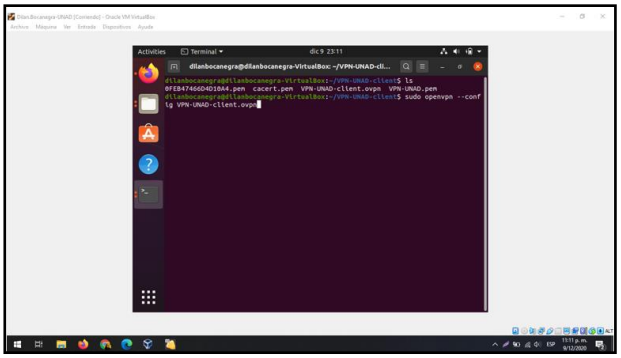

Figura 63. Utilizando certificado en cliente.

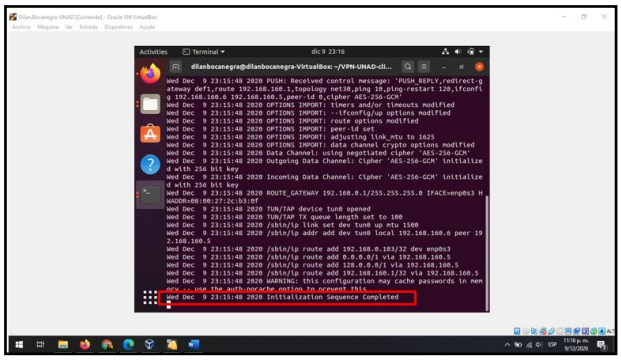

Figura 64. Ejecución de certificado desde cliente.

Antes de la ejecución del archivo se revisa con el comando ifconfig la información de red del sistema

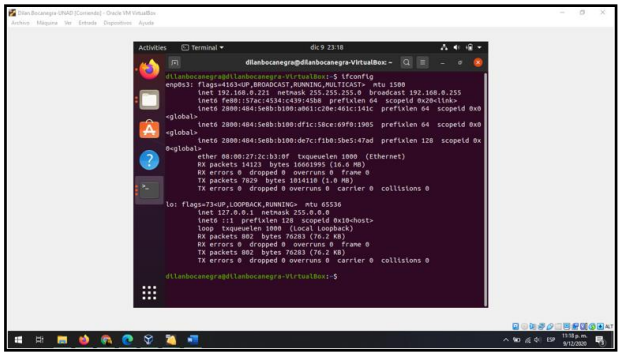

Figura 65. Ifconfig antes de conexión a vpn server.

Después de la ejecución del certificado de cliente se comprueba nuevamente información de red y se valida conexión con servidor vpn.

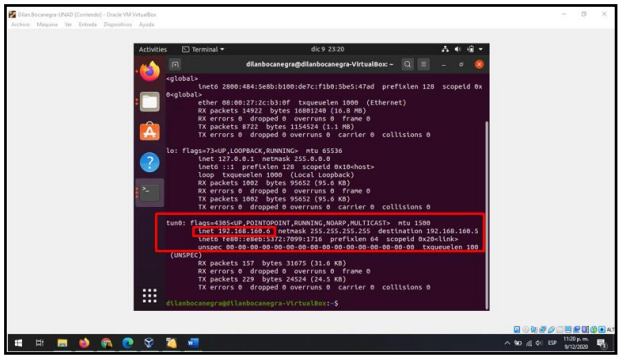

Figura 66. Ifconfig después de conexión a vpn server.

Confirmamos en zentyal el direccionamiento ip del servidor VPN

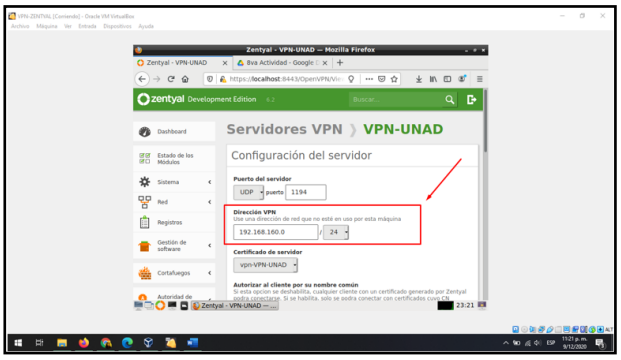

Figura 67. Direccionamiento ip de servidor vpn.

3. Conclusiones

Una vez puesto en marcha los servicios en zentyal, la institución cuenta con un servidor DHCP, servidor DNS y controlador dominio, con esta implementación y configuración se permite el acceso de una estación de trabajo con software basado en Linux mediante un usuario y contraseña, también se realiza el registro de esa estación en los servicios de infraestructura IT de zentyal. Además, posee un proxy no transparente que permite control de acceso para las estaciones de trabajo cliente a los servicios de conexión a internet, todo esto configurado desde zentyal mediante el proxy que filtra la salida por medio del puerto 1230; El sistema de la institución también posee un cortafuegos para la restricción de la apertura de sitios o portales web de entretenimiento y redes sociales. También cuentan con un servidor de archivo y servidor de impresión, con el cual pueden acceder desde una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a servicios de carpetas compartidas e impresoras, por último, la institución también contará con conexión mediante una red privada virtual (vpn), lo que permite establecer un túnel privado de comunicación con las estaciones de trabajo.

4. Referencias

[1] Riesco, A. Q. (2019, 14 marzo). Linux, el referente del sistema operativo más usado del mundo cumple 25 años. La Vanguardia. [En línea] Disponible en: https://www.lavanguardia.com/tecnologia/20190314/461023633171/linux-el-referente-del-sistema-operativo-mas-usado-del-mundo-cumple-25-anos.html

Zentyal 6.2 Official Documentation. (s. f.). Zentyal. [En Línea], Disponible en: https://doc.zentyal.org/en/

Ubuntu Server Guide. (s. f.). Ubuntu. [En Línea], Disponible en: https://assets.ubuntu.com/v1/e5021317-ubuntu-server-guide.pdf