UNIFICAR Y ADMINISTRAR ALGUNOS SERVICIOS BÁSICOS EN UNA INFRAESTRUCTURA DE RED DE FORMA SEGURA Y CONFIABLE, MEDIANTE EL PREÁMBULO A LA IMPLEMENTACIÓN DE SERVICIOS EN ZENTYAL SERVER.

Juan Pablo Bayona Soto
e-mail: jpbayonas@unadvirtual.edu.co
Franklin José Alarza Moreno
e-mail: falarzam@unadvirtual.edu.co
Carlos Martínez Balasnoa
e-mail: cmartinezbal@unadvirtual.edu.co
Maira Alejandra Castro Ochoa
e-mail: macastrooc@unadvirtual.edu.co
Jose Alfredo Mejía Moreno
e-mail: jamejiam@unadvirtual.edu.co

RESUMEN: *En este artículo busca dar solución a gran parte de las problemáticas de migración de sus sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, en busca de la migración y puesta en marcha de los servicios solicitados, enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas, mediante los sistema operativo bajo el cual se implementaran los servicios y plataformas: GNU/Linux Zentyal Server 6.2 (Instalación y configuración Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT).*

ABSTRACT: *In this article, it seeks to solve a large part of the migration problems of its operating systems, services and start-up of the security systems of the network infrastructure, in search of the migration and start-up of the requested services , focused on the implementation of higher level IT infrastructure services for Intranet and Extranet in complex institutions, through the operating systems under which the services and platforms will be implemented: GNU / Linux Zentyal Server 6.2 (Installation and configuration of Zentyal Server as operating system base to have IT Infrastructure services).*

PALABRAS CLAVE: Proxy, File Server, Firewall, Print Server, VPN.

1 INTRODUCCIÓN

Mucho se ha dicho respecto al alcance de la infraestructura tecnológica y las diferentes ofertas en el mercado, en el presenta artículo se muestra una opción ágil, versátil, segura y confiable, orientando al lector sobre la instalación, configuración y puesta en marcha de algunos servicios del servidor Zentyal en su versión 6.2.

2. INSTALACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ZENTYAL SERVER 6.2

Figura 1. Página oficial de descarga.

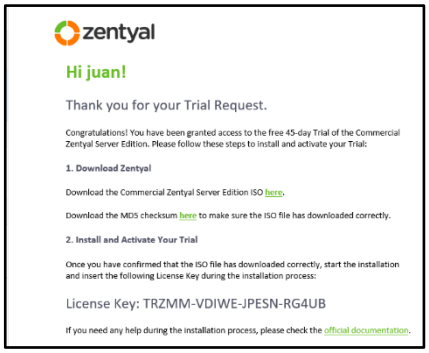

Figura 2. Clave de Activación.

En primer lugar, seleccionaremos el lenguaje de la instalación

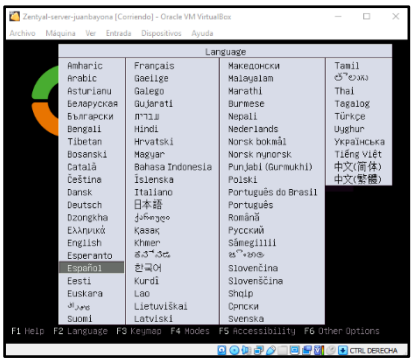

Figura 3. Selección del idioma.

Figura 4. Inicio instalador.

De manera intuitiva el instalador nos mostrará una serie de opciones como: Localización geográfica, Selección del teclado (español-Latinoamérica), esto es intuitivo la selección del país donde se está instalando, luego se presiona enter en continuar a cada proceso seleccionado en el instalador procederá a configurar la red.

Figura 5. Selección de interfaz de red: eth0.

A continuación, se mostrarán las siguientes pantallas de configuración: nombre de la máquina, Usuario administrador (Debemos ser especialmente cuidadosos y elegir una contraseña segura (más de 12 carácteres incluyendo letras, cifras y símbolos de puntuación), Contraseña y repetirla, Zona horaria (si, para configure nuestra selección de país en nuestro caso Colombia).

Figura 6. Enter en reiniciar.

El sistema arrancará una aplicación web de administración a la que podremos acceder, local o remotamente, mediante nuestro navegador (Firefox-Mozilla por defecto).

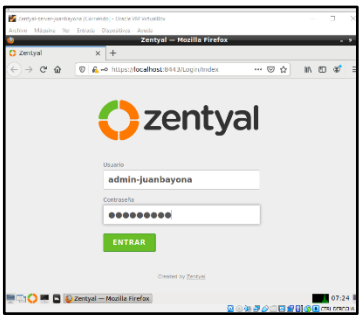

Figura 7. Entorno gráfico con el interfaz de administración.

Por último, ingresamos la clave de activación requerida para continuar operando y configurando el servicio:

Figura 8. Ingreso clave de activación.

2.1 CONFIGURACIÓN

Seleccionar qué funcionalidades queremos incluir en nuestro sistema. Como algunos componentes dependen de otros, Zentyal debe administrar esas dependencias instalando automáticamente los módulos necesarios para el funcionamiento del que hemos escogido.

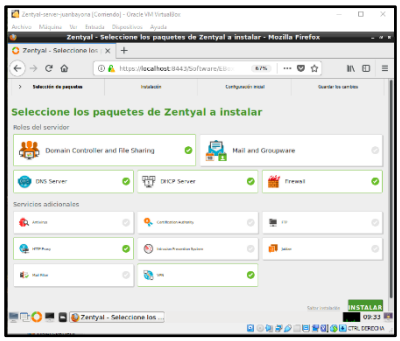

Figura 9. Selección e instalación: Domain Controller and File Sharing, DNS Server, DHCP Server, Firewall, HTTP Proxy y VPN + continuar.

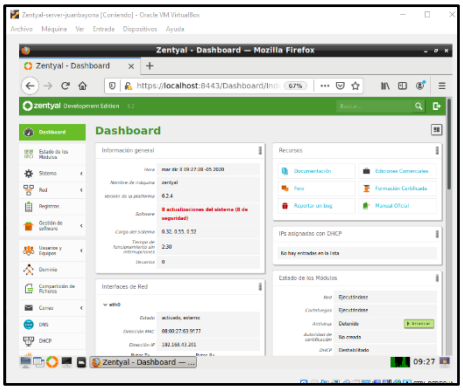

Figura 10. Inicio de Dashboard.

3. DESARROLLO DE CONTENIDOS

Tabla 1. TEMÁTICAS

ID	Temática	Integrante a cargo
1	DHCP Server, DNS Server y Controlador de Dominio	Franklin Alarza
2	Proxy no transparente	Juan Bayona
3	Cortafuegos	Carlos Martínez
4	File Server y Print Server	José Mejía
5	VPN	Maíra Castro

3. 1 IMPLEMENTACION BAJO ZENTYAL SERVER DE SERVICIOS GESTIÓN DE INFRAESTRUCTURA IT:

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

Los servicios seleccionados en el proceso inicial de configuración abarcan los necesarios para poner en marcha los que se abarcan en esta temática, durante el proceso de instalación de los mismos tendremos que configurar la red desde la que estarán funcionando, con ello podremos establecer una IP estática que facilite la prestación de los servicios, que esté dentro de la Red DMZ que se está administrando por medio de Endian que nos sirve de Firewall para asegurar que se desplieguen desde un entorno seguro.

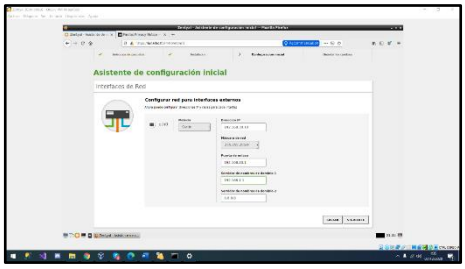

Figura 11. Configuración de IP y acceso a la red.

Seguidamente tendremos que tener en cuenta como se controlarán los accesos a archivos y dispositivos que se compartirán en la red, es por ello que nuestro controlador de dominio será del tipo “stand-alone” con lo que será el centro de todo aquello que se interconectará, se gestionarán entonces los accesos solo por medio de nuestro Zentyal Server.

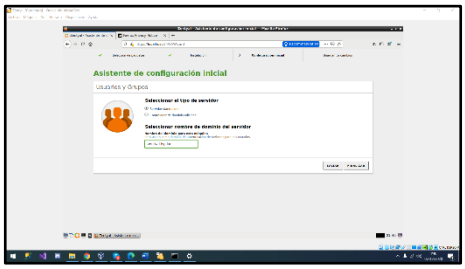

Figura 12. Configuración del control de dominio.

Revisando ya dentro del dashboard en el sidebar izquierdo por medio de la opción “Estado de los Módulos” comprobaremos que están levantados, para solo encargarnos de su configuración según las necesidades presentadas que serán un Servidor DNS brindado por el server, que con solo designar en las máquinas cliente podrán disponer de un traductor de dominios y poder navegar con normalidad resolviendo las IP que sean necesarias.

Con el despliegue del servicio DHCP permitirá a la empresa controlar la cantidad de dispositivos que podrán conectarse al resto de servicios que preste nuestro servidor, optimizando así los recursos y gestionando de manera eficaz la puesta en marcha de lo necesario y con ello también en la prestación de servicios a los clientes que adquieran nuestros servicios minimizando errores.

Por medio del servicio podremos definir el rango de IP que necesitemos distribuir, en este caso lo configuraremos desde 192.168.30.15 hasta 192.168.30.20 dejando entonces 6 IP’s disponibles. Asignamos un nombre descriptivo y damos clic en [Añadir]. Y posteriormente para que se apliquen los

cambios damos clic en [Guardar Cambios] que aparecerá en la parte superior derecha de nuestro panel de administración Zentyal.

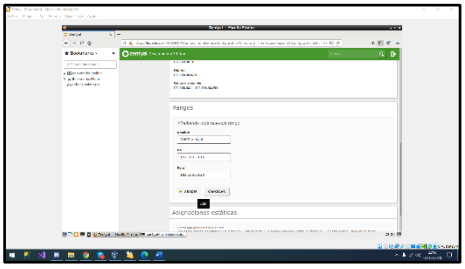

Figura 13. Asignación del rango personalizado disponible en nuestra interface.

Para comprobar que nuestro servicio levantado gracias a nuestro Zentyal, podemos acceder desde una maquina conectada en la red DMZ y con la configuración de la interface con DHCP habilitado, con el hecho de iniciarla se debería asignar la IP dentro del rango definido, lo comprobamos por medio del comando: ifconfig. En la cual se evidencia que asigna automáticamente la IP 192.168.30.15.

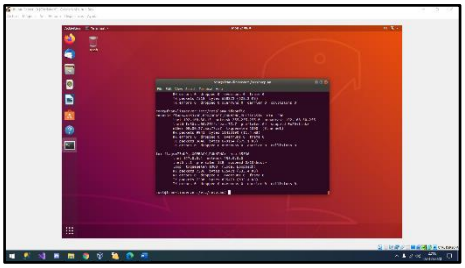

Figura 14. Comprobación del servicio DHCP en maquina con Ubuntu Server 18.

Con ello en funcionamiento, podemos continuar con la comprobación de que servicio de DNS está funcionando correctamente, tenemos en cuenta que, al ser instalado al inicio, lo tenemos ya activo por defecto, en el podemos añadir manualmente las resoluciones de direcciones o que lo haga de manera automática, dando clic en el banner derecho [DNS] podemos configurarlo.

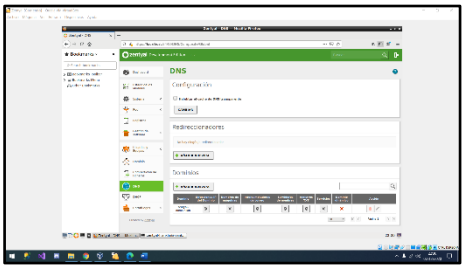

Figura 15. Interfaz de configuración del servidor DNS activo.

Para luego poder comprobar que está en funcionamiento, por medio de la misma maquina conectada en su servicio DHCP, si podemos hacer ping a dominios, esto querrá decir que está haciendo bien las traducciones.

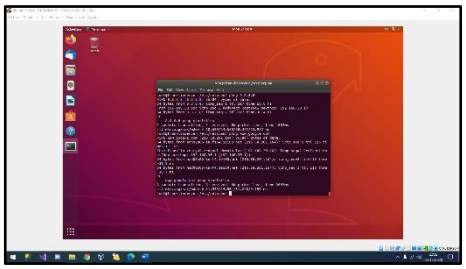

Figura 16. Ping correcto hacia el dominio www.google.com.

Procedemos con el control de dominios que gracias a tenerlo en funcionamiento, daremos de alta a todos aquellos usuarios que van a necesitar el compartir información entre ellos y con el servidor, es por esto que será vital la planeación de la estructura jerárquica que se manejará, controlable con la creación de grupos y asignación de roles para facilitar su administración, se recomienda entonces evaluar la estructura de la misma periódicamente para poder brindar la posibilidad de adaptarse según los cambios y crecimiento que vaya teniendo el equipo de trabajo.

Para configurar nuestro servicio de Control de dominio, podemos ir a nuestro módulo por el banner izquierdo dando clic en [Usuarios y equipos] seguido de [Gestionar]. Pudiendo ver al lado derecho el control de dominios en formato de árbol. Para añadir un nuevo usuario, seleccionamos [Users] del mismo y luego damos clic en el botón verde [+] ubicado justo en la parte inferior izquierda del árbol de control.

Con ello se nos levantará un modal, en el cual debemos registrar los datos que tendrá este nuevo usuario, en nuestro caso crearemos uno que funcione de administrador, con lo cual ingresamos datos de acceso como el nombre de usuario y contraseña, y adicionales como el nombre, apellido y descripción. Como queremos que haga parte del grupo existente administrador, seleccionamos en el desplegable [Domain Admins] y con ello damos clic en [Añadir] para culminar el proceso de agregado.

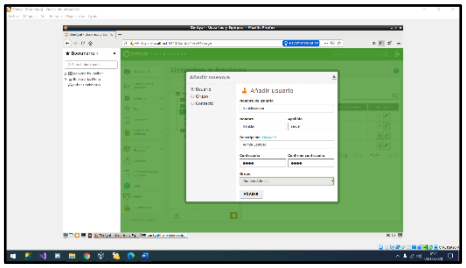

Figura 17. Ingreso de los datos del nuevo usuario.

Solo nos queda comprobar que podemos acceder a este grupo de dominio, identificando nuestro nombre de dominio que es: zentyal-domain.lan, para ello debemos agregar un equipo nuevo, vamos a nuestra maquina y necesitamos una herramienta que nos

permita hacer parte del grupo de dominio ya creado, para ello ejecutamos el comando:

wget -O - https://repo.pbis.beyondtrust.com/apt/RPM-GPG-KEY-pbis|apt-key add
wget -O /etc/apt/sources.list.d/pbiso.list https://repo.pbis.beyondtrust.com/apt/pbiso.list
y posteriormente procedemos entonces a la instalación de la herramienta por medio del comando: apt-get install pbis-open.

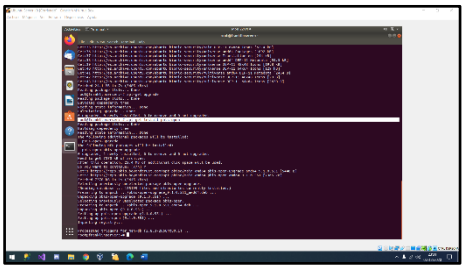

Figura 18. Instalación del software PBIS Open por línea de comando.

Con ello solo nos queda realizar un apt-get update y también un apt-get upgrade para evitar paquetes faltantes para el correcto funcionamiento de la herramienta. Para asegurarnos de que los DNS se resolverán de la mejor manera, instalamos el siguiente paquete por medio del comando: apt-get install resolvconf Y ya con ello podremos ejecutar el comando para unirnos al dominio de Zentyal, por medio del comando: domainjoin-cli join zentyal-domain.lan franklinserver@zentyal-domain.lan

La relación que poseen estos tres servicios van desde los usuarios que los consumirán, como también de la necesidad del uno del otro, ya que la estructura que se ejerza según la planeación va determinar el éxito de la implementación de los mismos, brindará entonces alto control de los grupos necesarios para poder ejercer una distribución de servicios según las necesidades de cada uno, permitiendo un amplio aprovechamiento de recursos, disminución en el mantenimiento de los servicios, fácil adaptación a cambios que surjan por el crecimiento o no deseable disminución de la infraestructura de la empresa y por ende la reducción o aumento de los grupos a quienes se les suministran los servicios.

Temática 2: Proxy no transparente

La implementación de proxy no transparentes es lo más recomendable en la práctica ya que los usuarios conectan los equipos a la red, no van a tener acceso al servicio de internet hasta que se configure el navegador web con la IP del servidor proxy y el proxy, se recomienda que el puerto sea diferente que los que se utilizan por defecto.

Se implementa y configura el 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, de la siguiente manera:

Configuración del servidor como Proxy no Transparente:

Selección e instalación de los siguientes servicios como lo es Firewall y Http Proxy.

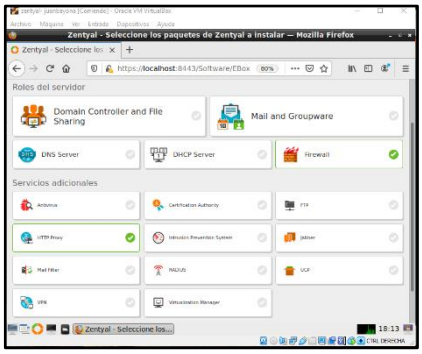

Figura 19. Instalación de paquetes requeridos.

Configuración de las dos tarjetas de red una como red Externa para el acceso a Internet servidor y la otra para la red LAN (red externa y red interna), cambiando los segmentos de red que nos da el proveedor de internet.

Figura 20. Interfaces del servidor.

Procedemos a configurar las interfaces de red, en el panel izquierdo la opción Red/Interfaces, seleccionamos la interface (eth0) marcando WAN, ya que será el encargado de administrar la red y guardamos los cambios.

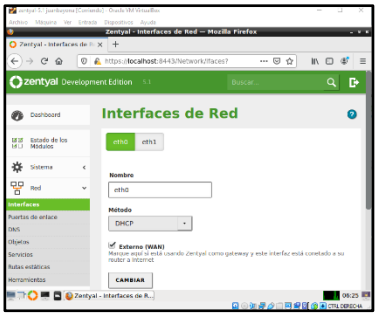

Figura 21. Configuración de Red eth0, administra internet servidor.

Iniciamos con la configuración de la segunda interfaz (eth1) colocándola en método (estático) y se le asigna la IP 192.168.2.1.

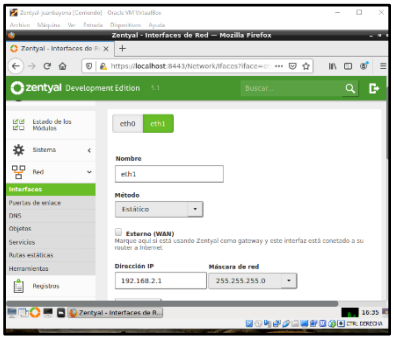

Figura 22. Configuración Interfaces de Red como estática.

Vamos a nuestro panel (Dashboard) para revisar si el servicio de Proxy está ejecutándose:

Configuración opción Proxy HTTP

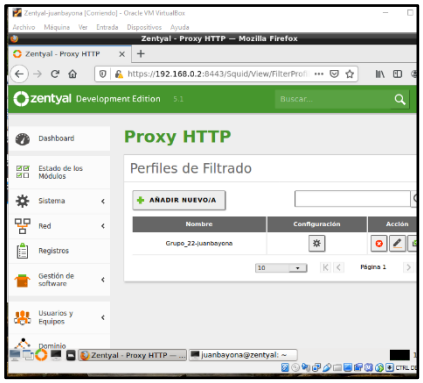

Figura 23. Perfiles de filtrado.

Configuración del Umbral y se guardan los cambios.

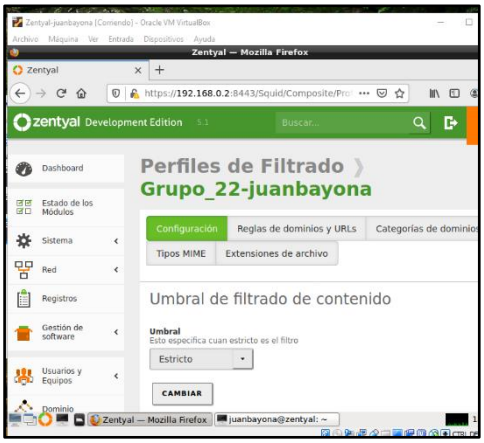

Figura 24. Añadido nuevo perfil de filtrado.

Ingresamos a la máquina y le configuramos la IP y la puerta de enlace configurada en el Zentyal para la interface (eth1).

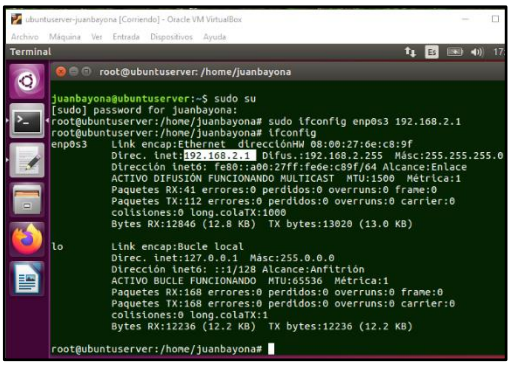

Figura 25. Configuración IP estática de la maquina cliente.

En Zentyal se configura Proxy HTTP por el puerto 1230.

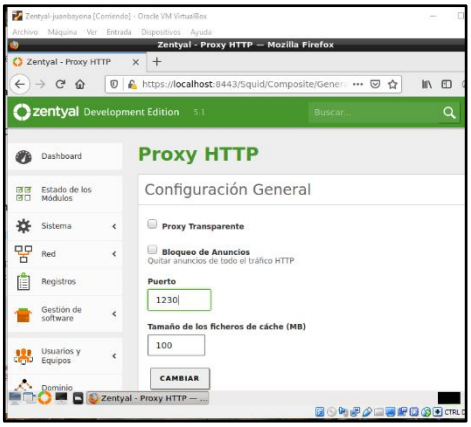

Figura 26. Configuración puerta de enlace.

Desde la maquina Ubuntu-server se realiza la configuración del Proxy no transparente para los puertos HTTP Y HTTPS.

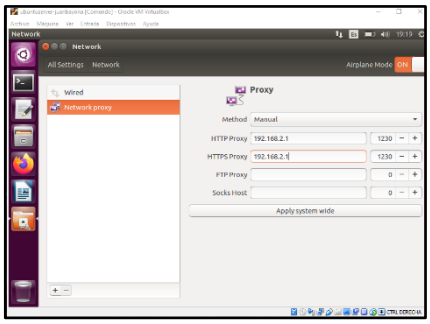

Figura 27. Configuración del Proxy.

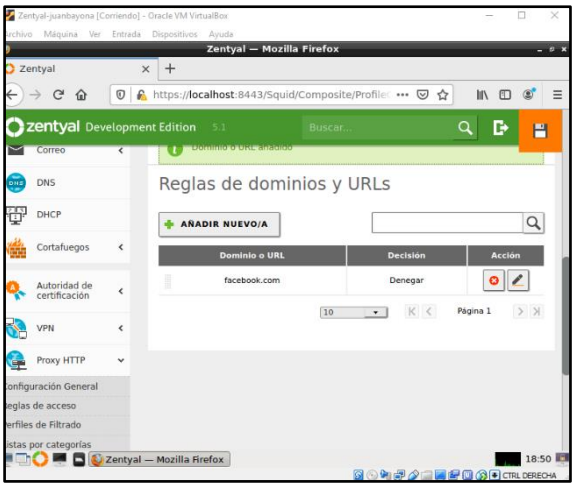

Figura 28. Configuración del Proxy denegar página Facebook.com.

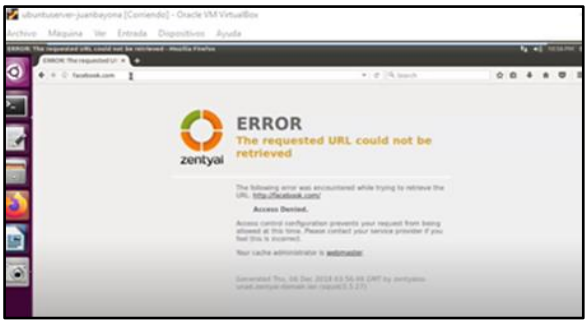

Figura 29. Verificación bloqueo desde ubuntuserver con servicio zentyal.

Temática 3: Cortafuegos

En el campo de la informática se denomina a cortafuegos como esa parte de un sistema o red enfocada en denegar o permitir accesos de acuerdo con el tipo de autorización.

El cortafuegos principalmente es utilizado en redes locales, enfocándose en mejorar la seguridad este es dado como una de las primeras medidas utilizadas en los inicios de lo que conocemos como internet. En el ámbito empresarial este es utilizado en la zona desmilitarizada (DMZ) estableciendo reglas que permiten establecer el filtrado de paquetes relacionados con los servidores los cuales están enfocados en este tipo de red.

Principalmente podemos encontrar dos tipos de firewall (en inglés), los enfocadas en hardware, que se fundamentan en estar conectados entre el acceso a internet y el switch que divide el tráfico a los demás equipos conectados. Los que se basan en software fundamentado en un aplicativo que se instala en el equipo, ambos encargados del análisis de paquetes aplicando el filtrado dadas las reglas establecidas.

En el caso de estudio se aplican reglas de filtrado de redes internas, dado el proceso de instalación de zentyal server, ingresamos al entorno con los datos de acceso requeridos por el sistema.

Figura 30. Ventana de acceso al panel de control de zentyal.

Verificada la instalación de los paquetes básicos, se inicia el proceso de configuración del cortafuegos para la red estando ubicados en el dashboard se accede a la sección del cortafuegos para iniciar la configuración de las reglas de filtrado.

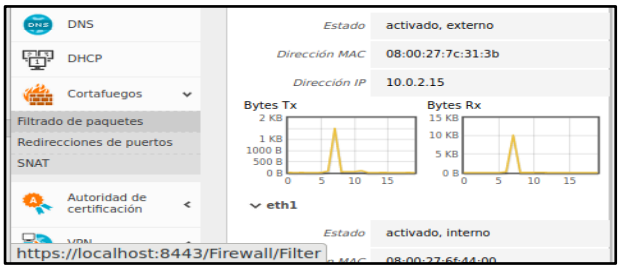

Figura 31. Acceso a la configuración del cortafuegos.

Se destaca el proceso que desarrolla zentyal, a medida que se realiza el proceso de instalación de paquetes, se establecen reglas básicas en el firewall en la búsqueda de un óptimo funcionamiento de estos. Ubicada la sección de cortafuegos se accede a la opción de filtrado de paquetes.

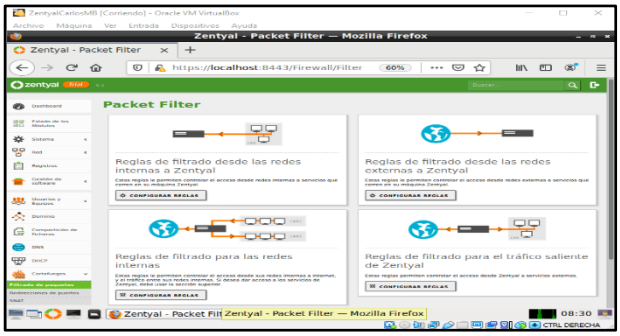

Figura 32. Sección - filtrado de paquetes - cortafuegos.

Son varias las posibilidades de filtrado de paquetes disponibles, en el caso de estudio el enfoque estará dado en el uso de las reglas de filtrado para las redes internas.

Figura 33. Reglas de filtrado para las redes internas.

Al iniciar el proceso de configuración de las reglas tras hacer clic en el botón configurar en el primer acceso se identifica una de las reglas por defecto.

Figura 34. Reglas de filtrado por defecto.

Continuando el proceso se agrega una nueva regla de filtrado en el caso de estudio se aplican reglas para denegar el acceso a páginas de redes sociales, inicialmente la página de Facebook, por lo tanto, se realiza el proceso de verificación de la dirección ip en este caso a través del comando nslookup, información requerida para agregar correctamente la regla.

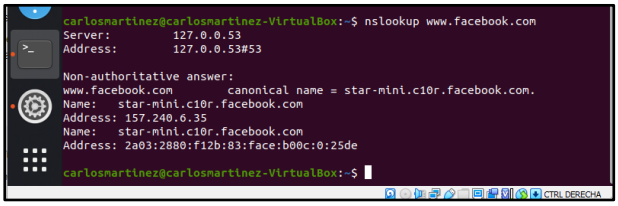

Figura 35. Identificación dirección IP red social Facebook.

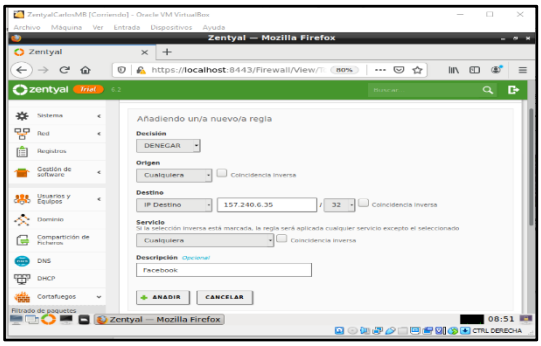

Figura 36. Añadiendo nueva regla.

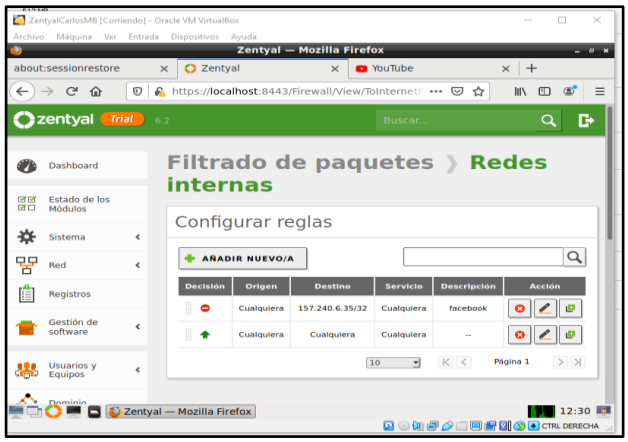

Figura 37. Regla añadida.

Antes de añadir la regla y aplicar los cambios registrados, se verifica el acceso de uno de los dispositivos en la red DMZ en el caso de estudio, confirmando su acceso al sitio.

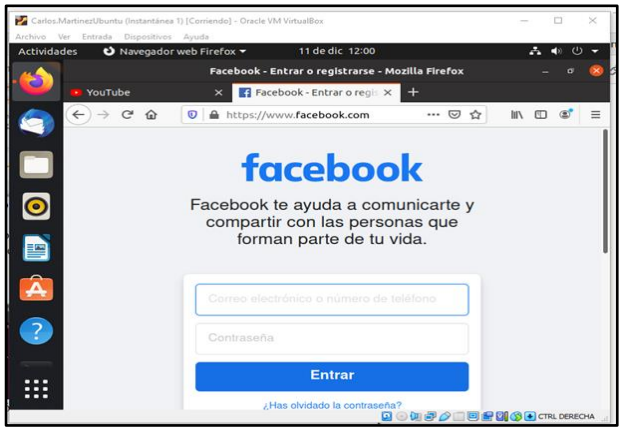

Figura 38. Verificación de acceso correcto al sitio.

Verificado el acceso se añade la regla y se aplican los cambios realizados, se recarga el sitio y el usuario tendrá denegado el acceso a este.

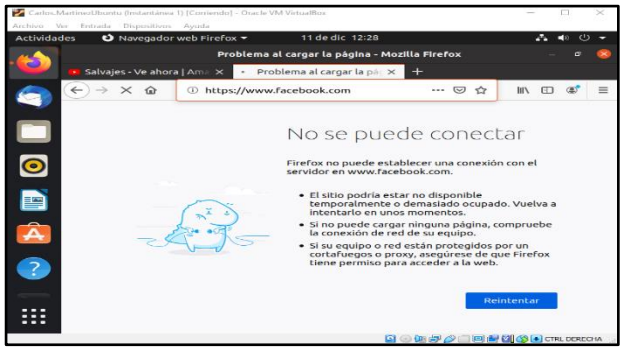

Figura 39. Verificación de acceso denegado al sitio.

Validado el funcionamiento de la regla, se aplica a otros sitios aplicando el mismo procedimiento.

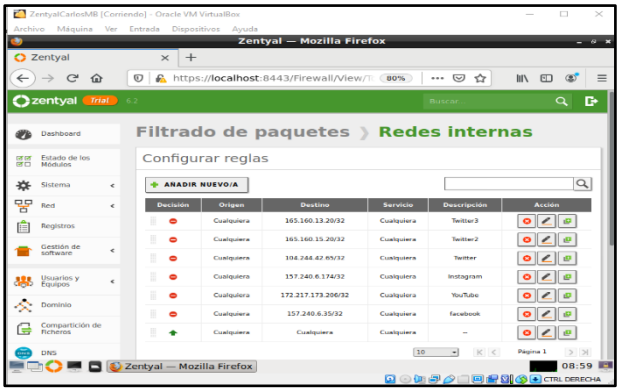

Figura 40. Reglas aplicadas a otras redes sociales.

Temática 4: File Server y Print Server

La compartición de ficheros es el proceso por el cual una serie de archivos se ponen a disposición de los usuarios de una Red, dándole acceso para trabajar sobre ellos, en esta actividad vamos a realizar el proceso de compartir archivos e impresora, para ello iniciamos abriendo la interfaz de Zentyal, la cual ya se encuentra instalada.

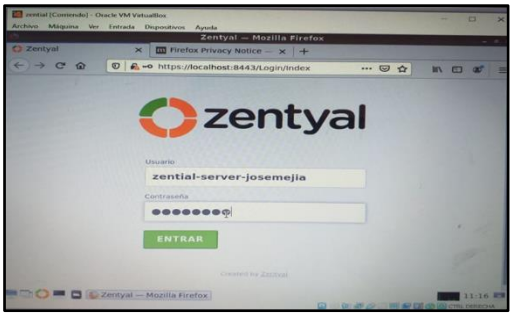

Figura 41. Logín de inicio de sección.

Después de haber ingresado a la plataforma, procedemos a seleccionar los módulos necesarios para realizar la actividad.

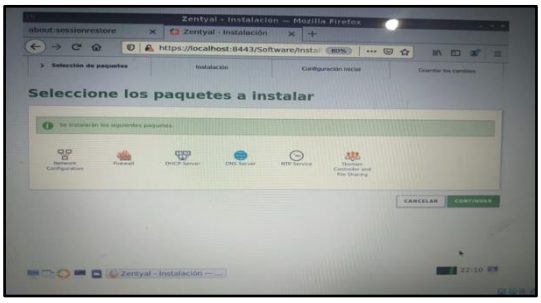

Figura 42. Módulos de servicios.

Habiendo instalados los módulos necesarios, procedemos a realizar configuración de la tarjeta de Red como interna.

Figura 43. Configuración de Red.

Seguidamente vamos a la interfaz de la red creada y configuramos una IP estática que se encuentre dentro del rango de la zona DMZ.

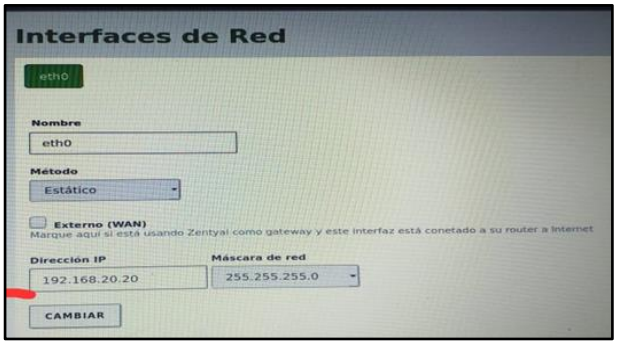

Figura 44. Configuración interfaz de red.

Posteriormente creamos un objeto dentro de la Red con la IP que va a tener nuestra estación de trabajo 192.168.20.21 ya que nos sirve para simplificar y consecuentemente facilitar la gestión de la configuración de la red, pudiendo dotar de un nombre fácilmente reconocible al elemento o al conjunto y aplicar la misma configuración a todos ellos, en pocas palabras nos sirve para no tener que escribir los datos de la Red creada cada vez que lo soliciten, en vez de ello se utiliza el objeto.

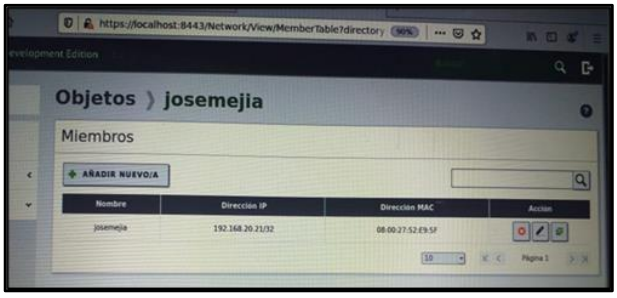

Figura 45. Creación de objeto.

Seguidamente procedemos a configurar la dirección estática de nuestra estación de trabajo desde el módulo DHCP, por medio del objeto creado anteriormente.

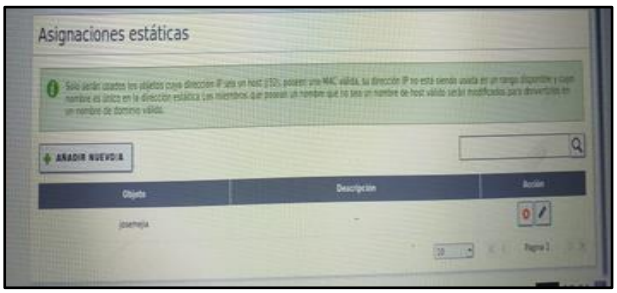

Figura 46. Configuración DHCP estática.

Luego vamos a crear un usuario, el cual será el encargado de administrar el archivo a compartir, para ello vamos al módulo usuarios y grupos y damos clic en gestionar, para esta actividad usuario (josemejia1).

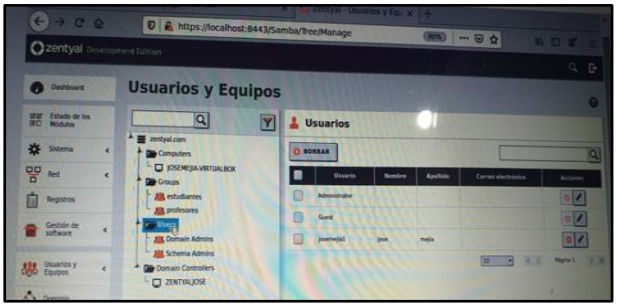

Figura 47. Creación de usuario.

Creado el usuario nos dirigimos al módulo compartición de ficheros y creamos el fichero a compartir llamado fase8 para esta actividad.

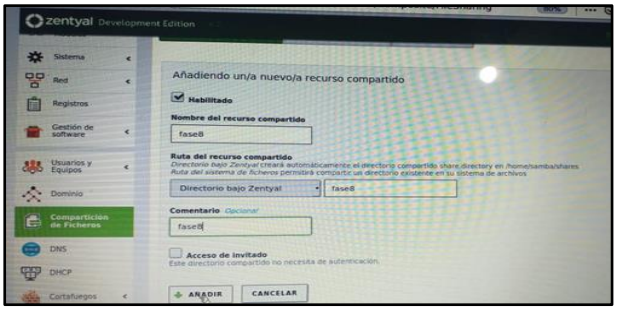

Figura 48. Creación de fichero.

Luego nos muestra la carpeta creada para compartir llamada fase8 en la cual debemos dirigirnos al botón control de acceso y configurar el usuario que va a tener los permisos de dicha carpeta.

Figura 49. Control de acceso.

El control de acceso se crea para asignarle permisos específicos al usuario sobre el fichero.

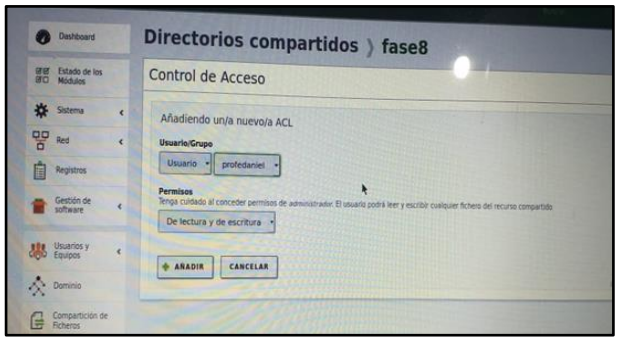

Figura 50. Asignación de permisos.

Después de haber asignados los permisos necesarios al usuario nos dirigimos a la estación de trabajo (Ubuntu 18.04) para realizar las configuraciones necesarias para el proceso de compartición, para ello entramos a la terminal y miramos si se creó la IP estática asignada desde DHCP 190.168.20.21

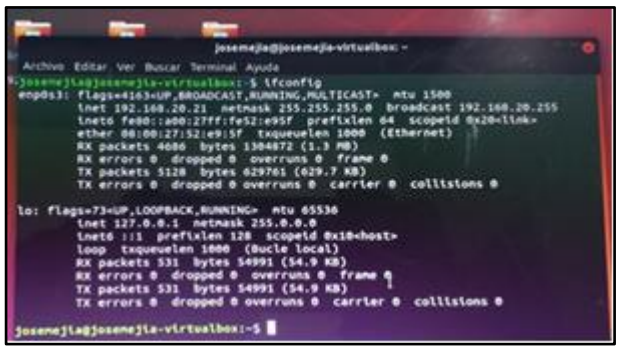

Figura 51. IP creada en Ubuntu.

Posteriormente procedemos a instalar los repositorios de una herramienta que nos permite hacer parte de los dominios creados, utilizando los comandos que se muestran en las siguientes imágenes.

Comandos de repositorios a instalar.

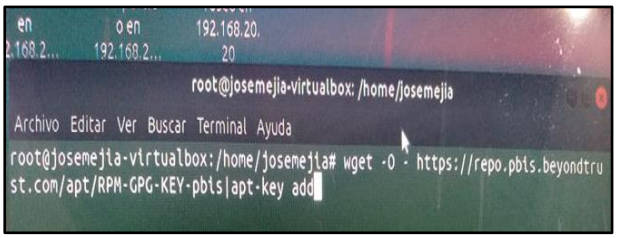

Figura 52. Comando repositorio.

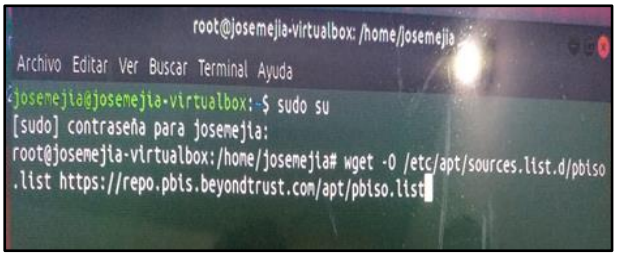

Figura 53. Comando repositorio.

Luego actualizamos e instalamos la herramienta con el comando sudo apt-get install pbis-open.

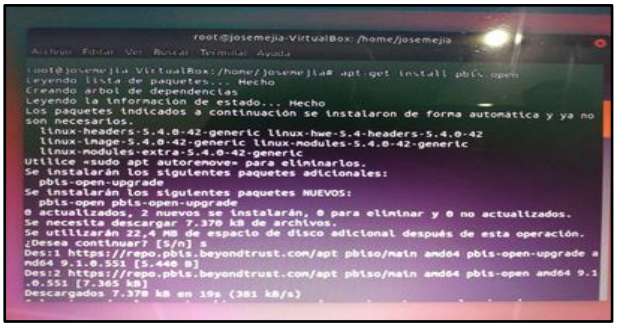

Figura 54. Instalación herramienta.

Luego nos dirigimos a los directorios, damos clic en otras ubicaciones y posteriormente debemos poner el enlace con la dirección smb://192.168.20.20 para hacer la conexión con el servidor Zentyal.

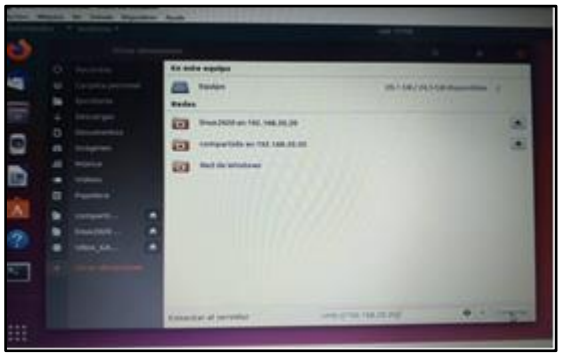

Figura 55. Conexión con servidor Zentyal.

Finalmente nos muestra el fichero creado llamado fase8, terminando así el proceso de compartir ficheros por medio de Zentyal.

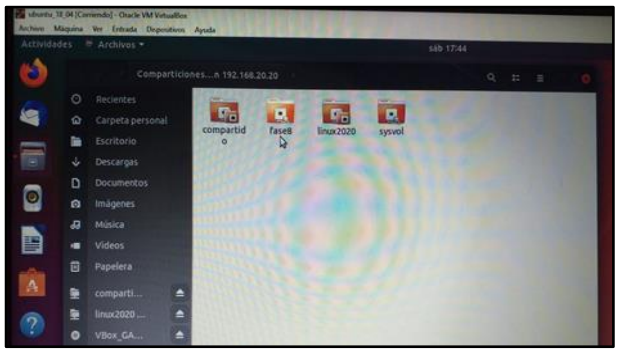

Figura 56. Fichero recibido en Ubuntu.

Luego procedemos a realizar el proceso de **compartir impresora**, proceso que se hará con algunas de las anteriores configuraciones. Para ello nos dirigimos al módulo **Impresoras.**

Figura 57. Compartición de impresora.

Luego nos muestra un mensaje donde nos dice que para añadir impresora se debe usar la interfaz web de CUPS, hacemos clic sobre el enlace y nos direcciona a dicha interfaz.

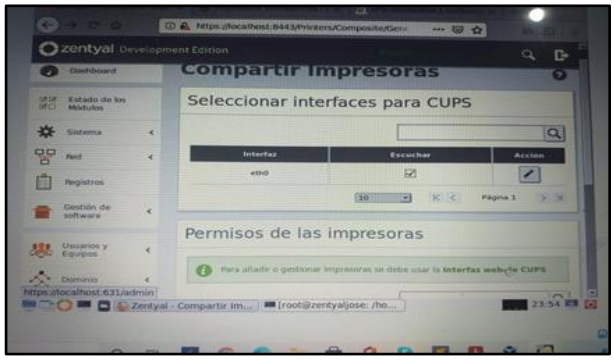

Figura 58. Interfaz CUP.

Posteriormente procedemos a agregar la impresora y realizar la configuración correspondiente, como es ponerle un enlace, el nombre de la misma etc.

Iniciamos agregando una impresora.

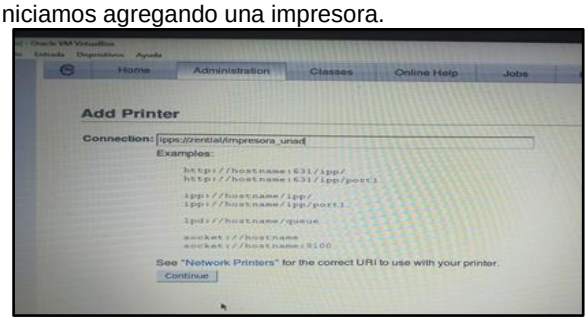

Figura 59. Adicción de impresora.

Luego configuramos el nombre y serie de la impresora.

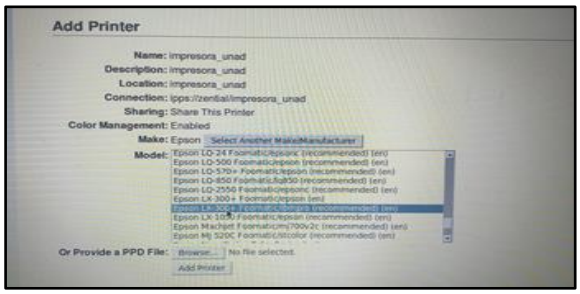

Figura 60. Configuración serie.

Posteriormente nos muestra un mensaje diciéndonos que la impresora se agregó correctamente

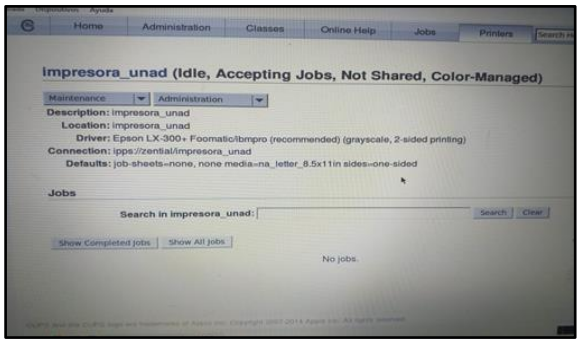

Figura 61. Confirmación de adición.

Luego nos muestra la impresora agregada en Zentyal

Figura 62. Impresora agregada en Zentyal.

Nos dirigimos a Ubuntu y entramos a conectar a server en directorio, con la dirección smb://192.168.20.20.

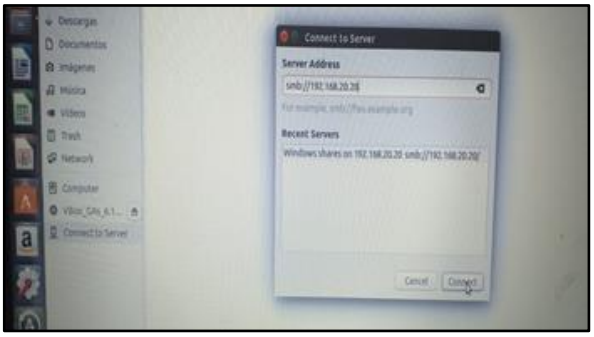

Figura 63. Conexión servidor Zentyal.

Posteriormente nos muestra la carpeta Print$, la abrimos y nos muestra los componentes de la impresora.

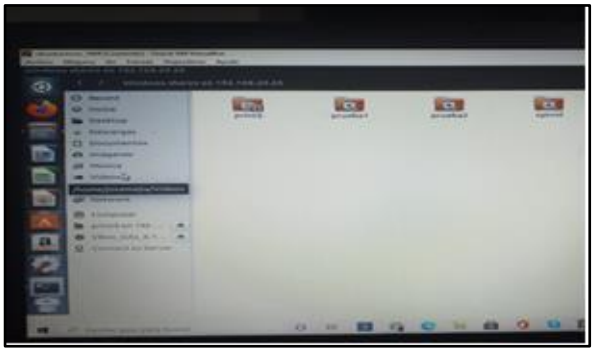

Figura 64. Fichero de impresora.

Figura 65. Componentes de impresora.

Temática 5: VPN

Una VPN (red privada virtual) es una tecnología que utiliza Internet para conectarse a una ubicación específica y de esta manera poder acceder a ciertos servicios. Esta conexión a la red puede ocurrir de varias maneras, pero generalmente utiliza el cifrado como mecanismo para proteger la comunicación entre el usuario y el servidor.

En la presente actividad crearemos una red VNP 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.

Una vez instalado y configurado Zentyal server, procedemos a la creación de una nueva VPN, ingresando al módulo VPN y damos clic en servidores y automáticamente nos va a pedir que creemos la VPN.

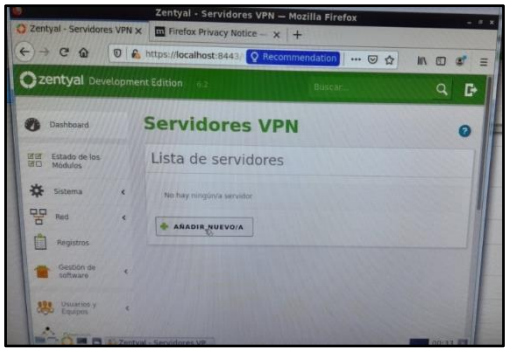

Figura 66. Creación VPN.

Le damos el nombre a la VPN, los datos y los días de expedición.

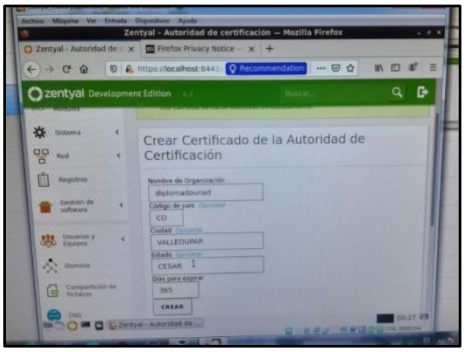

Figura 67. Creación de certificado.

Luego de crear el certificado procedemos a configurarlo.

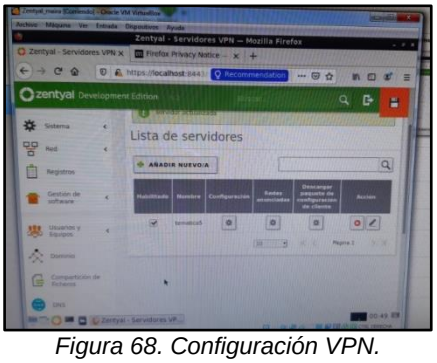

Figura 68. Configuración VPN.

Configuramos el puerto del servidor UDP el cual configuramos para que entre por el puerto 1194 y dejamos la ip que nos da el sistema por defecto.

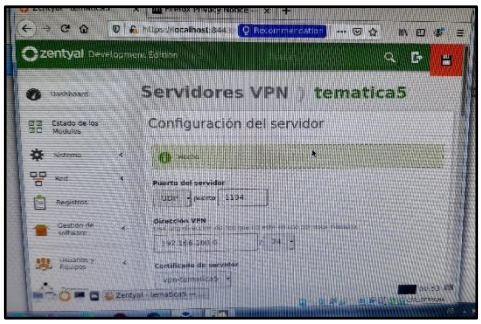

Figura 69. Configuración VPN.

Se debe adicionar el servicio que permita la conexión con el puerto predeterminado para las conexiones VPN, el puerto UDP 1194.

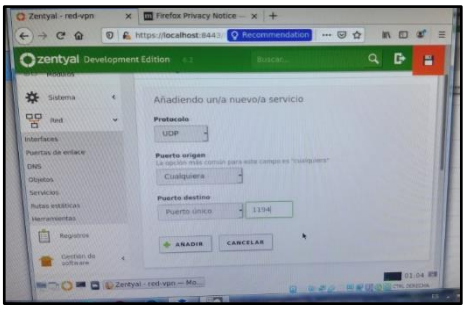

Figura 70. Configuración del servicio.

Se debe configurar la regla de filtrado desde las redes internas.

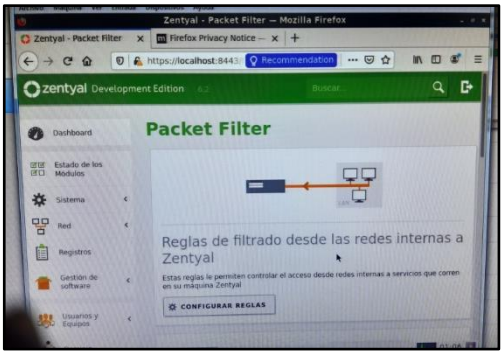

Figura 70. Configuración regla de filtrado.

Aceptamos el permiso con el servicio antes creado, en el que tenga como origen a cualquiera, para que permita que todas nuestras redes que pasen por la red virtual, tengan acceso.

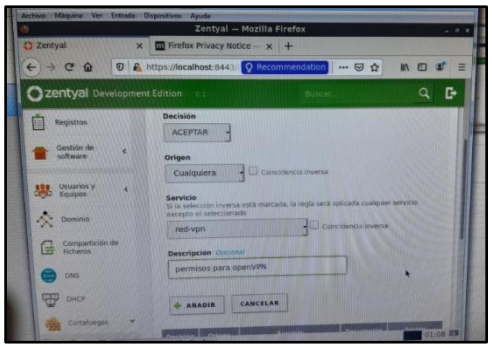

Figura 71. Configuración regla de filtrado.

Nos muestra el certificado del permiso para el OpenVPN con las descripciones establecidas en el formulario.

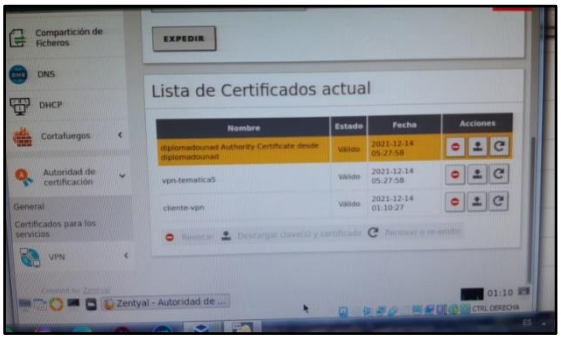

Figura 72. Lista de certificados.

Creado la VPN se genera el certificado del cliente, esta vez generamos uno para Linux y le damos descargar.

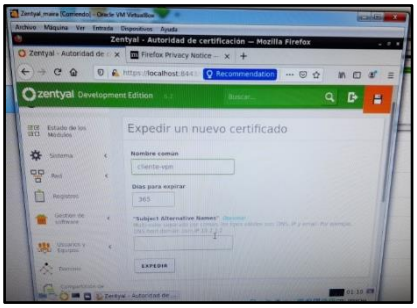

Figura 74. Creación del certificado.

Posteriormente procedemos a descargar el certificado antes generado, para poder por medio del mismo permitir a nuestros clientes el acceso a la red VPN que gestionaremos.

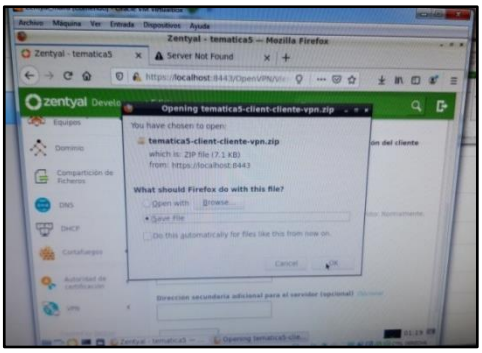

Figura 73. Descarga del certificado.

Para finalizar verificamos que el dominio del servicio este corriendo, gracias a que Zentyal permite hacerlo por medio de un Widget en la pantalla principal de la interfaz web.

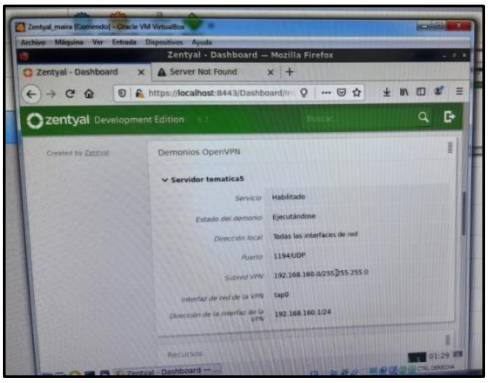

Figura 76. Verificación del dominio.

4. RECONOCIMIENTOS

Primero que todo darle gracias a Dios por permitirnos cumplir la meta, posteriormente gracias al tutor del diplomado, a nuestro Director, a nuestros compañeros de estudio y a todas las personas que de una u otra manera ayudaron al desarrollo de la actividad.

5. CONCLUSIONES.

Después de realizada la anterior actividad, podemos concluir que ha sido de gran enseñanza, ya que nos ha llevado a conocer las diferentes implementaciones y configuraciones de servidores, movernos dentro de sus servicios y realizar tareas específicas, solucionando necesidades de los clientes.

Hay muchas razones para que las empresas busquen cada vez más usar VPN, entre ellas podemos destacar el perfeccionamiento de la seguridad, privacidad e integridad de los datos traficados. Además, las VPN permiten a los usuarios acceder a datos sensibles de la empresa en redes públicas, de manera segura, con mayor disponibilidad y movilidad para negocios y personas.

6. REFERENCIAS

[1] Zentyal (2004-2018). Primeros pasos con Zentyal. Disponible en: https://doc.zentyal.org

[2] Sandoval Cardozo, D., Zambrano Zuñiga, J., Orozco Espinoza, C. A., Montano Ospina, C. E., & Soto Del Campo, R. Instalación y configuración Zentyal Server.

[3] Beltrán Ruiz, Y. A., Sepúlveda Rondón, L. L., Ríos Bohórquez, C. A., Rodríguez Rivera, R. A., & Celeita Gallegos, L. F. Implementación servicios de infraestructura IT: DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, VPN, File Server y Print Server en Zentyal server.

[4] Guerrero Hurtado, J. S., Jimenez Camargo, J. A., Chaves, E. I., Camayo Camayo, J. P., & Ortiz, M. Zentyal Server– Instalación y configuración para implementación de servicios.

[5] Ibarguen Moreno, J. O., Mora Orejuela, A. M., & Mosquera Ruiz, E. Instalación y configuración de Zentyal Server, para la implementación de servicios.

[6] Espinosa Velandia, S., Cubillos Reyes, C. E., Céspedes Pisso, A. F., Bolaños Suárez, D. J., & Díaz Aricapa, A. Instalación, Configuración Zentyal Server 5.1 y servicios DHCP Server, DNS Server, Controlador de Dominio, Proxy no Transparente, Cortafuegos, File Server, Print Server y VPN.

[7] Jaramillo Cruz, C. J., Hernández Peinado, J. F., & Covaleda, C. C. Instalación, Configuración SO GNU/Linux Zentyal Server 5.1 y servicios DHCP Server, DNS Server, Controlador de Dominio, Proxy no Transparente, Cortafuegos, File Server, Print Server y VPN.

[8] Cortafuegos (informática). (2020). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Cortafuegos_(inform%C3%A1tica)&oldid=130889707

[9] Fernández, Y. (2019, octubre 17). Firewall: Qué es un cortafuegos, para qué sirve y cómo funciona. Xataka. https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

[10] Andrés, R. (2015, abril 28). Cortafuegos informáticos: Qué son y para qué sirven. ComputerHoy. https://computerhoy.com/noticias/internet/cortafuegos-informaticos-que-son-que-sirven-26747