IMPLEMENTACIÓN DE SERVICIOS ESPECÍFICOS CON ZENTYAL

Fredy Valerio Prada Suarez
e-mail: fvpradas@unad.edu.co
Juan Rafael Polo Avendaño
e-mail: jrpoloa@unadvirtual.edu.co
Sneyder Saavedra Cárdenas
e-mail: esaavedraca@unadvirtual.edu.co
Sergio Armando Romero Abril
e-mail: saromeroab@unadvirtual.edu.co
Andrés Felipe Serrano
e-mail: afserranob@unadvirtual.edu.co

RESUMEN: *Este artículo expone el desarrollo de la actividad final del Diplomado de Profundización en Linux, la cual se realizó utilizando el sistema operativo Linux Zentyal Server, que es la base para disponer de los servicios de Infraestructura TI donde se realizaron configuraciones de DHCP, DNS, Proxy, Firewall, File Server, Print Server y VPN. Las configuraciones se probaron a través de Ubuntu Desktop, y se demuestra la funcionalidad de las configuraciones realizadas en cada paso.*

ABSTRACT: *This article show us the development of the final activity deepening diploma in Linux which was carried out using the operating system, Linux Zentyal Server, which is the basis for having the IT infrastructure services where configurations were made, DHCP, DNS, PROXY, Firewall, File Server, Print Server and VPN, the configurations were tested through Ubuntu Desktop and the functionality of the configurations made in each step is demonstrated.*

PALABRAS CLAVE: Cortafuegos, DHCP, DNS, Dominio.

1 INTRODUCCIÓN

La administración de servidores es uno de los grandes méritos de Linux, más su implementación y configuración son procesos relativamente complejos desde una terminal. De esta manera la distribución Zentyal se convierte en una alternativa eficiente para medianas y pequeñas organizaciones por su entorno amigable, manejo de tiempos y simplicidad en sus procesos. Al poseer una interfaz gráfica bajo navegador, se vuelve intuitivo, con una configuración rápida y segura por su configuración atendida. Posee una larga lista de servicios compatibles. Para este trabajo se utiliza la versión “Development Edition” similar a las versiones comerciales, pero sin soporte técnico oficial, y aunque incluye las últimas novedades del producto, el sistema puede ser levemente inestable.

2 INSTALACIÓN DE ZENTYAL SERVER COMO SISTEMA OPERATIVO

2.1 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Para la instalación de Zentyal como sistema operativo se creó una máquina basada en Linux Ubuntu con una memoria RAM de 2 GB, un disco duro de 20 Gb, dos adaptadores de red uno para la conexión LAN y otro para la conexión WAN. Se descargó la imagen .iso de http://download.zentyal.com/zentyal-6.2-development-amd64.iso.

2.2 PROCESO DE INSTALACIÓN

Luego de montar la imagen .iso en la máquina virtual se arranca e inicia el proceso de instalación, seleccionando el idioma, posteriormente seleccionando la instalación a realizar.

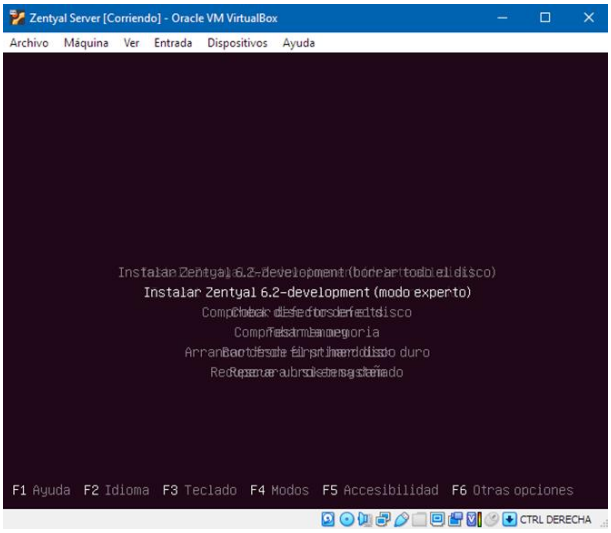

Figura 1. Selección modo de instalación Zentyal

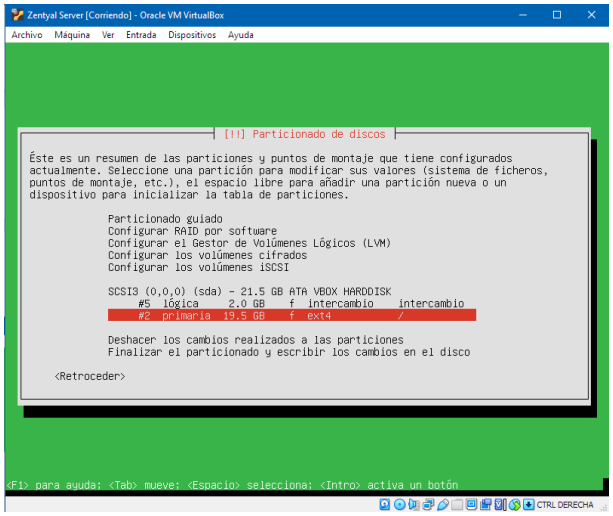

Figura 2. Configuración de disco duro

Para esta ocasión se seleccionó el modo experto, posteriormente se selecciona la ubicación, la distribución de teclado, posteriormente la pantalla nos muestra los adaptadores de red que tiene la máquina, se selecciona el usuario y contraseña para la máquina en que se instalará Zentyal, y se procede a configurar las particiones del disco duro.

Continuando con la selección de la instalación del entorno gráfico, para mejorar la respuesta de la máquina virtual se decidió no instalar este entorno gráfico, luego se configura el proxy, en caso de ser necesario y la instalación del cargador de arranque.

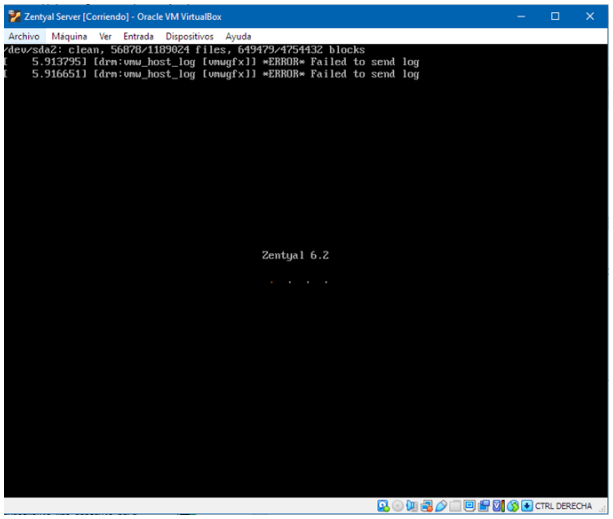

Figura 3. Arranque de Zentyal

Posterior a la instalación se procede a iniciar sesión con el usuario y contraseña configurados durante la instalación, luego ingresar se hace la actualización y para acceder de manera gráfica se hace desde una máquina externa a través del navegador web.

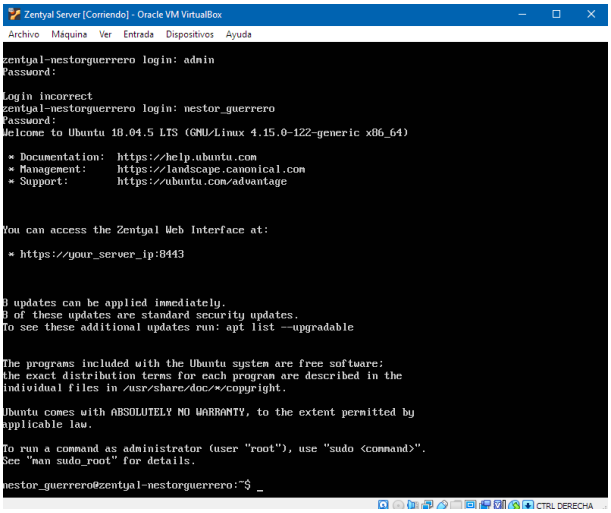

Figura 4. Iniciando sesión en Zentyal

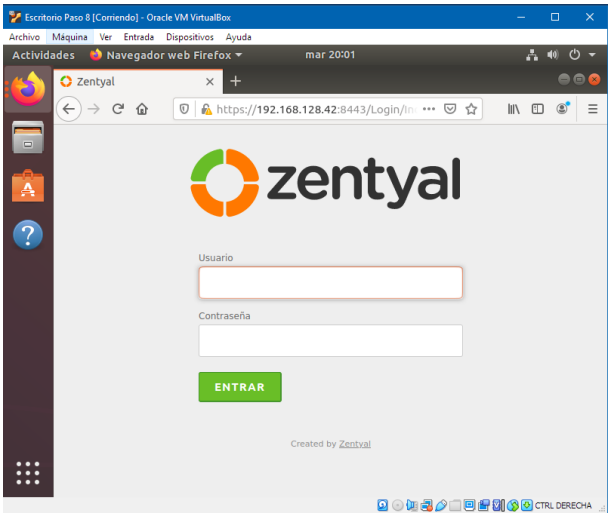

Figura 5. Arranque de Zentyal

A partir de esta conexión se continua con la configuración de los diferentes módulos de Zentyal.

3 TEMÁTICAS

- **Temática 1**: DHCP Server, DNS Server y Controlador de Dominio.
- **Temática 2:** Proxy no transparente
- **Temática 3:** Cortafuegos
- **Temática 4:** File Server y Print Server
- **Temática 5:** VPN

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

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.

3.1.1 DHCP SERVER

Inicialmente se procede a buscar el módulo de DHCP, y se crea el rango del direccionamiento a utilizar, una vez realizado lo anterior se guardan cambios y se verifica la asignación desde el panel de administración del Zentyal y desde la estación de trabajo.

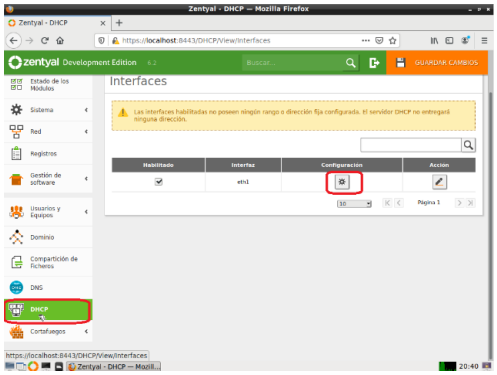

Figura 6. Creación rango direccionamiento

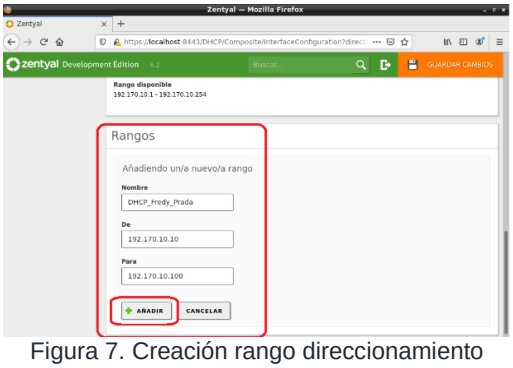

Figura 7. Creación rango direccionamiento

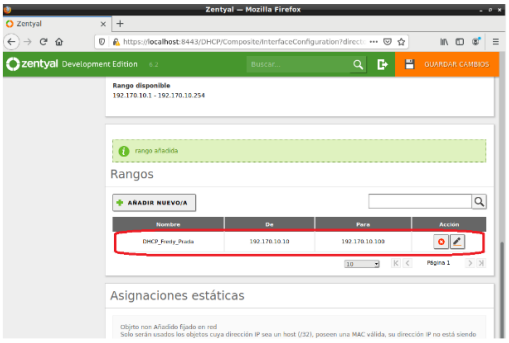

Figura 8. Creación rango direccionamiento

Seguidamente se procede a realizar la verificación desde la estación del cliente y verificar conectividad entre los equipos.

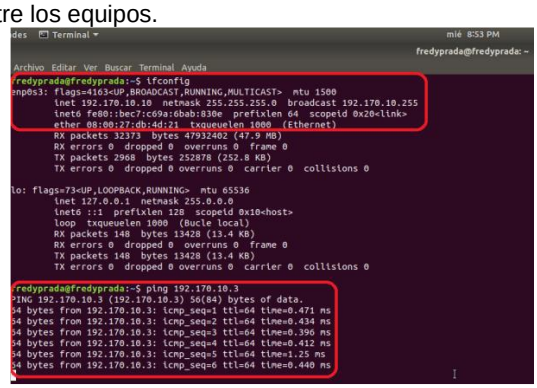

Figura 9. Verificación asignación IP DHCP

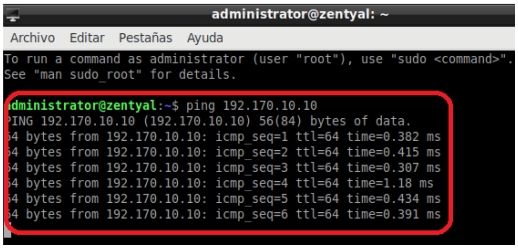

Figura 10. Verificación conectividad

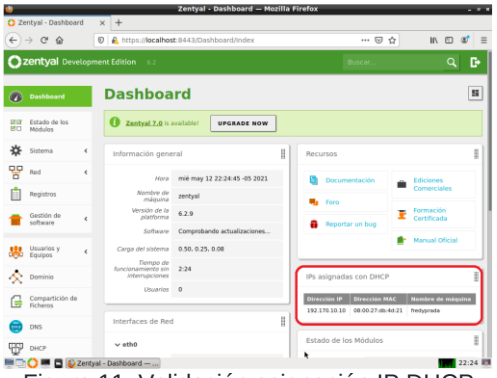

Figura 11. Validación asignación IP DHCP

3.1.2 DNS SERVER

Inicialmente se identifica el módulo de DNS para agregar el dominio fredyprada.loc y verificar la conectividad con la estación de trabajo. En caso de no

contar aún con el dominio creado, se procede a crearlo para su posterior inclusión al servidor DNS, desde el menú principal, en el módulo de Dominio.

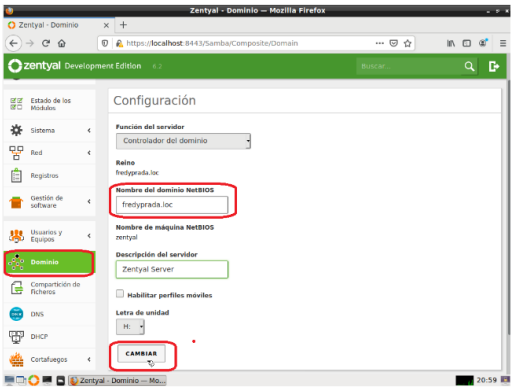

Figura 12. Creación dominio

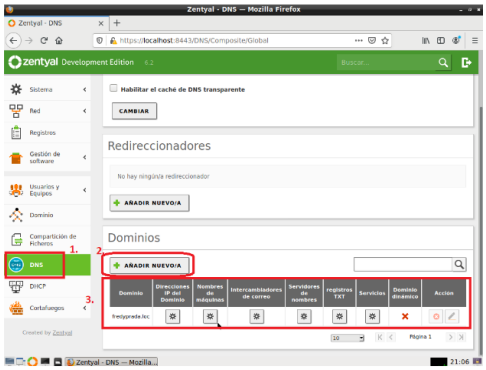

Figura 13. Configuración DNS - Dominio

Mediante el comando nmcli dev show | grep DNS se verifica que corresponda a la maquina Zentyal.

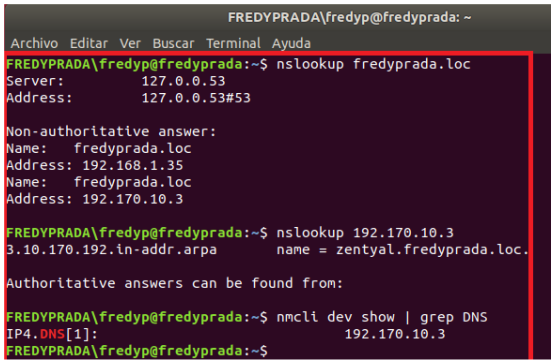

Figura 14. Validación funcionamiento DNS

3.1.3 CONTROLADOR DE DOMINIO

Inicialmente se procede a verificar nuevamente la creación del dominio, seguidamente se crea el usuario de red, el cual pertenecerá al directorio y tendrá el rol de administrador.

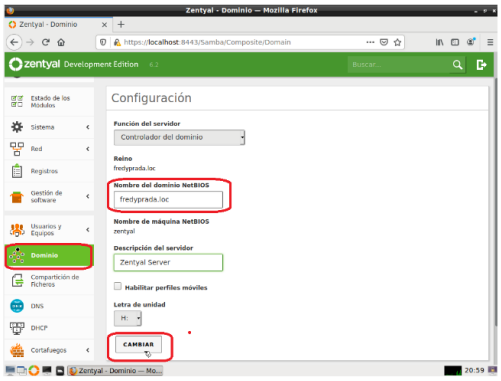

Figura 15. Creación dominio

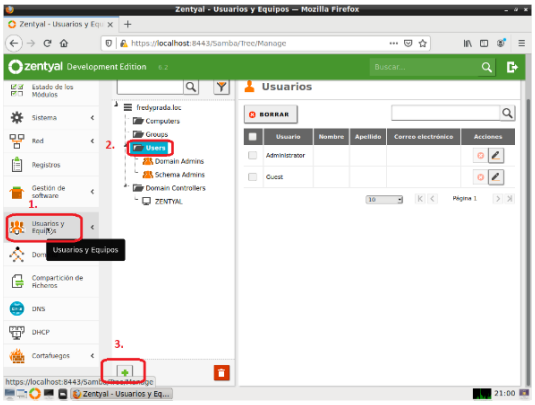

Figura 16. Creación usuario red

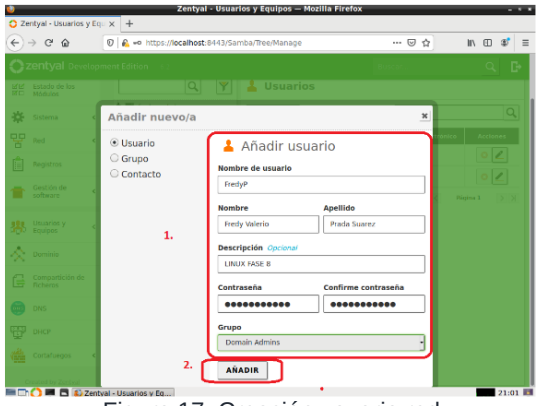

Figura 17. Creación usuario red

El próximo paso para seguir será la unión al dominio desde la estación de trabajo de Ubuntu, para esto se utilizará la herramienta pbis-open, la cual se descargará desde el repositorio oficial de github. Una vez realizada la descarga, se asignan permisos de lectura, ejecución y se inicia la instalación del aplicativo.

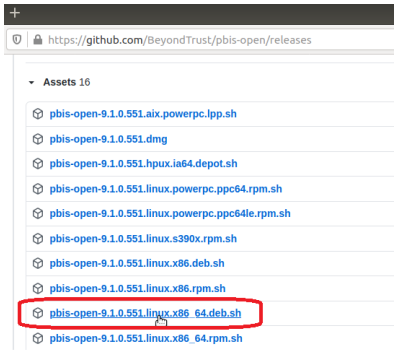

Figura 18. Descarga Pbis-Open

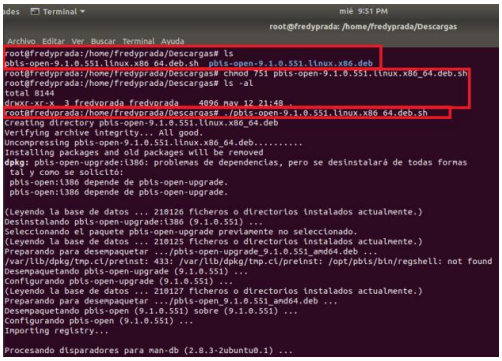

Figura 19. Instalación Pbis-Open

Una vez finalizada la instalación, se procede agregar el equipo al dominio desde la terminal utilizando la herramienta instalada anteriormente.

Figura 20. Unión dominio estación trabajo

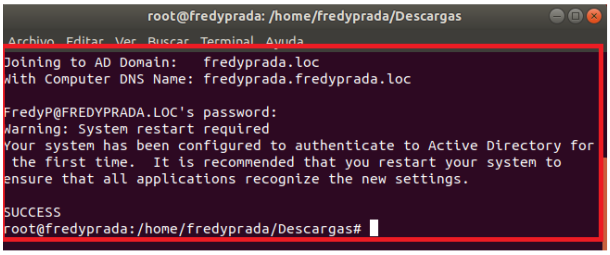

Figura 21. Verificación credenciales red

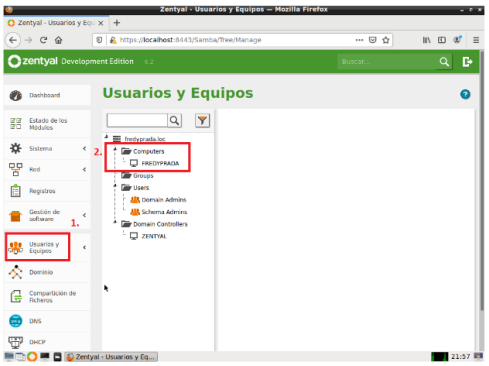

Figura 22. Validación unión equipo - dominio

Finalmente se procede activar la capacidad del cliente de escribir el dominio para iniciar sesión, se edita el fichero agregando el login manual.

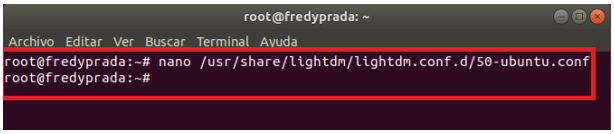

Figura 23. Edición fichero login manual

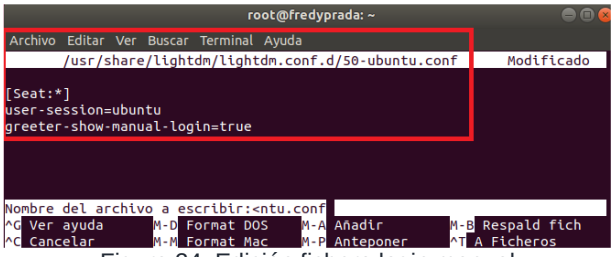

Figura 24. Edición fichero login manual

Una vez realizada la modificación al fichero, se asigna un Shell al usuario para que ingrese a través de la configuración del pbis-open y se reinicia el equipo para aplicar cambios.

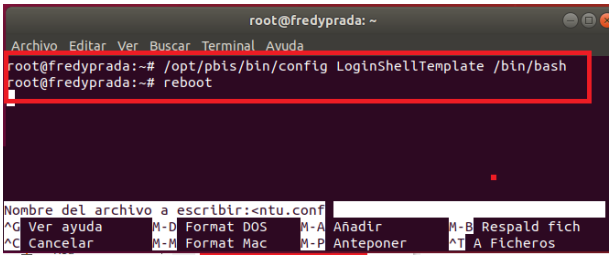

Figura 25. Asignación shell usuario

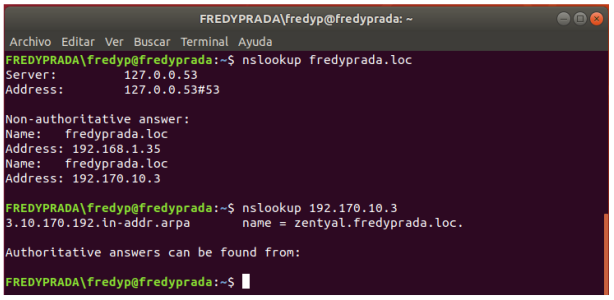

Figura 26. Verificación funcionamiento controlador dominio

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un Proxy que filtra la salida por medio del puerto 1230.

Se ha tomado la decisión de desarrollar la temática bajo un sencillo modelo de red con seguridad perimetral

(VirtualBox), ya que este permite poner a prueba las diferentes competencias adquiridas:

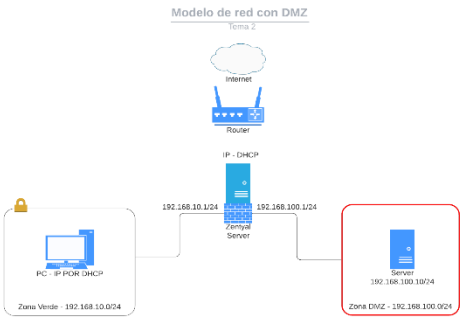

Figura 27. Modelo de red con DMZ

Para simular la Zona Verde se hará uso de una estación de trabajo corriendo bajo una máquina virtual con sistema Ubuntu Desktop 18.04 y para la Zona DMZ se utilizará dentro de ella una máquina virtual con Ubuntu Server 18.04. El Servidor Gateway será implementado en una máquina virtual con Zentyal Server y tres adaptadores de red, el primero en modo *Bridge* y los otros dos en modo *Red interna*, mientras que las otras máquinas funcionarán con un sólo adaptador en modo *Red interna*.

Una vez instalados los módulos HTTP Proxy, DHCP Server, DNS Server y Firewall en el Zentyal Server desde su configuración inicial, como se indicó en la Temática 1, se procede a configurar el servidor DHCP para dar soporte a la asignación automática de IPs, para la LAN o Zona Verde del modelo de red.

El direccionamiento para los adaptadores del Zentyal se configura así:

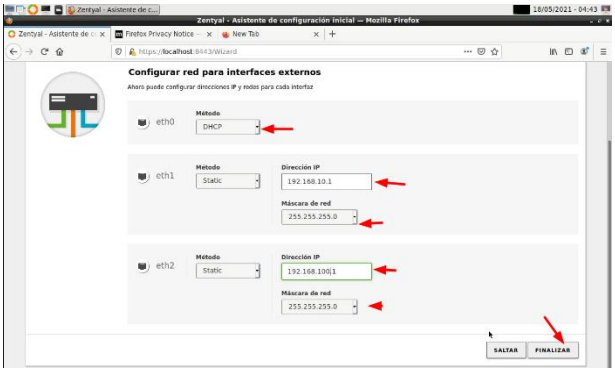

Figura 28. Direccionamiento IP del Zentyal

El adaptador eth0 será el enlace con Internet o Zona Roja y su dirección será tomada desde el DHCP del router.

El adaptador eth1 (192.168.10.1/24) y eth2 (192.168.100.1/24) serán para la intranet, como se indicó en la figura. Ambos serán las puertas de enlace predeterminadas para la Zona Verde y DMZ respectivamente.

3.2.1 CONFIGURACIÓN DHCP

Se procede a configurar eth1 para que sirva direcciones IPs automáticas hacia la LAN o Zona Verde, en el servidor DHCP [1]:

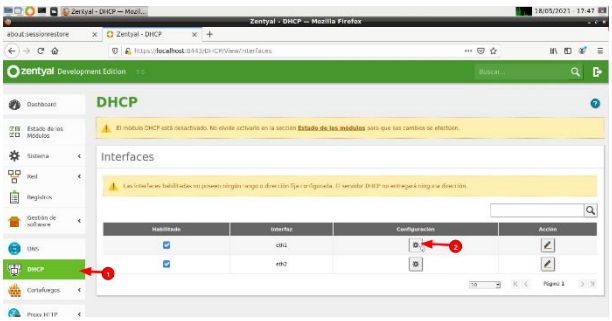

Figura 29. Configurar DHCP para eth1.

La configuración DHCP queda de la siguiente forma:

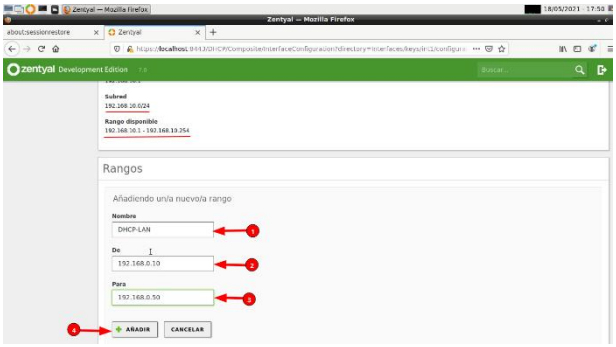

Figura 30. Configurar DHCP para eth1.

Las estaciones de la LAN, que para el ejemplo es uno solo, se configuran para que obtengan sus IPs en forma automática:

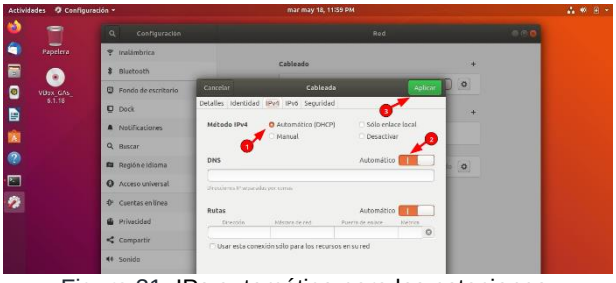

Figura 31. IPs automático para las estaciones.

Con ello queda configurado el servicio DHCP para la Zona Verde.

3.2.2 CONFIGURACIÓN DEL PROXY

Primeramente, se ingresa a la configuración general del módulo Proxy HTTP y configura el puerto de escucha como 1230, como indican los requerimientos y se guarda la configuración:

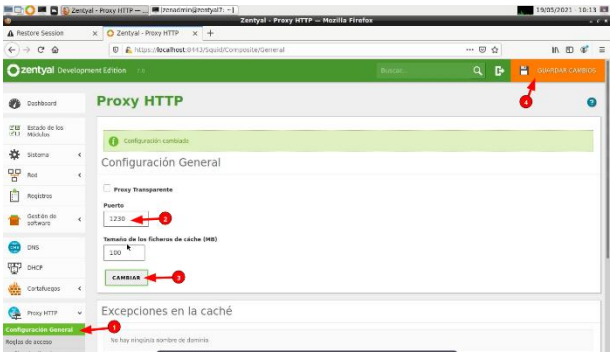

Figura 32. Proxy a través del puerto 1230.

Se ingresa a la opción de perfiles de filtrado dentro de la pestaña de Proxy HTTP y se añade un nuevo perfil que tendrá el nombre de Solo_YouTube, porque el ejercicio consiste en denegar el acceso a cualquier otro sitio http diferente a https://www.youtube.com. Una vez asignado el nombre del perfil se procede a configurarlo, así:

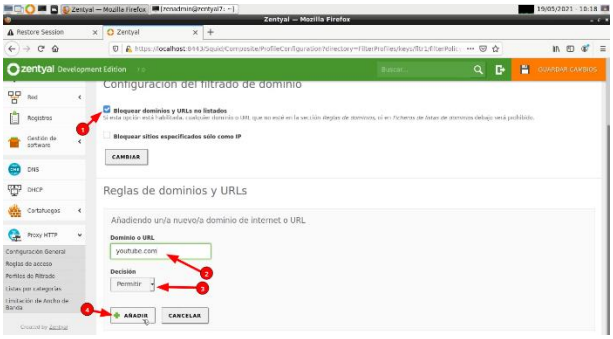

Figura 33. Bloquear dominios diferentes a youtube.com.

Este perfil (Solo_YouTube) se asocia a la regla de acceso del proxy para que se haga efectivo el filtrado. Se accede a la configuración a través de la opción *Reglas de acceso* de la pestaña del Proxy:

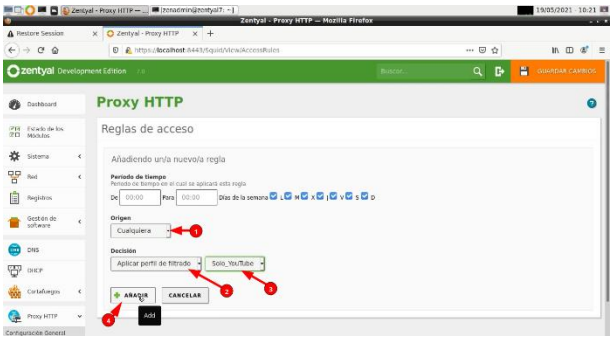

Figura 34. Regla de acceso con filtro Solo_YouTube.

Configuración Proxy para la estación de trabajo:

Figura 35. Configuración Proxy en Ubuntu Desktop.

Se prueba la navegación. Se observa que una pestaña tiene el icono de YouTube, evidenciando que se pudo navegar allí, mientras que el otro sitio es denegado por ser diferente a ese dominio:

Figura 36. Se deniegan los sitios diferentes a YouTube.

Cabe mencionar que el Proxy HTTP no hace filtrados HTTPS, por cuanto su contenido viene cifrado. Zentyal implementa una integración con el Firewall para poder lograr esto, pero esa característica sólo está disponible en la edición comercial de Zentyal [2].

Con esto queda validado el correcto funcionamiento del servicio Proxy a través de Zentyal Server, como lo indica el requerimiento de esta temática.

3.2.3 CONFIGURACIÓN DEL DMZ

Se expondrá un Webservice en la máquina que se aloja en la DMZ y esta contará con un direccionamiento IP estático, configurado así:

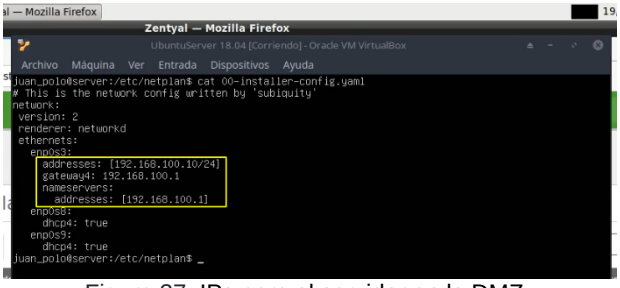

Figura 37. IPs para el servidor en la DMZ.

En el modelo con seguridad perimetral, se debe permitir el tráfico desde la Zona Verde hacia la Zona DMZ, pero denegarlo en el sentido contrario, porque de no ser así se pueden estar dejando agujeros de seguridad aprovechables por algún atacante externo,

para ingresar a la LAN a través de la DMZ. Para ello se ingresa al módulo de Firewall > Riltrado de paquetes > Reglas de filtrado para las redes internas [3]. Se elimina la regla que viene predeterminada en el Firewall. Se configura una para permitir ejecutar el comando ping desde la LAN hacia la DMZ:

Figura 38. Se permite ping desde la LAN hacia la DMZ.

Se agrega la regla para denegar cualquier comunicación (servicio) en el sentido opuesto, a saber, desde la Zona DMZ hacia la Zona Verde:

Figura 39. Se deniegan las peticiones DMZ hacia LAN.

Ahora se añade una nueva regla para permitir el paso de tráfico con protocolo HTTP desde la Zona Verde hacia la Zona Naranja, la cual expone un Webservice:

Figura 40. Aceptar peticiones HTTP de LAN hacia DMZ.

De esa misma forma se crea una regla para aceptar peticiones HTTPS desde la LAN hacia DMZ y otra para denegar cualquier otro tipo de petición diferente a las ya creadas, desde la LAN hacia DMZ. El listado de reglas quedaría así:

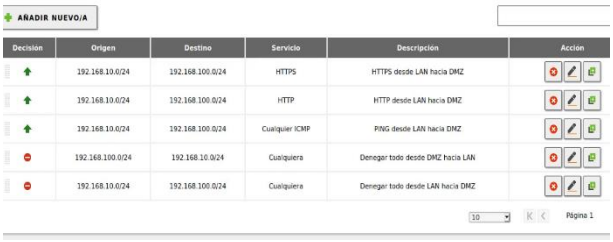

Figura 41. Listado de reglas del Firewall.

Ahora se puede apreciar en las siguientes ilustraciones, cómo desde el equipo Ubuntu Desktop de la LAN o Zona Verde, se puede hacer una petición http al servidor de la Zona DMZ, mostrándose una pátina web php, alojada con antelación en el Ubuntu Server. También cómo se acepta el ping desde la LAN hacia la DMZ y se deniega desde la DMZ hacia la LAN:

Figura 42. Petición http desde la LAN hacia DMZ.

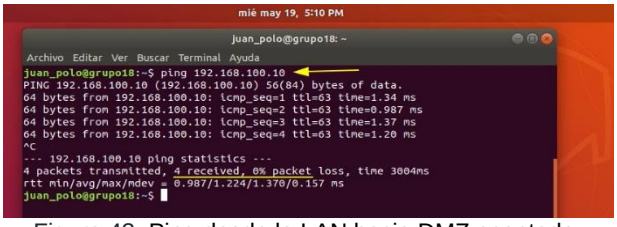

Figura 43. Ping desde la LAN hacia DMZ aceptado.

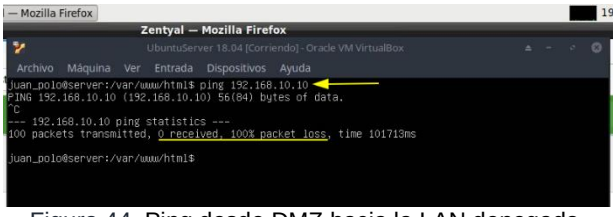

Figura 44. Ping desde DMZ hacia la LAN denegado.

Las ilustraciones son evidencia de la implementación exitosa de la Zona DMZ dentro de la topología de red, con una configuración básica en Zentyal Server.

3.3 TEMÁTICA 3: CORTAFUEGOS.

La siguiente, es la pantalla dashboard donde se tiene el control total para realizar los cambios.

Figura 45. Dashboard

En el PC cliente se realiza los cambios de red para que este quede conectado a través de la puerta de enlace con el Zentyal. Para esto se realiza el siguiente cambio en la conexión LAN. Donde es importante seleccionar la opción Manual y en la puerta de enlace colocar la IP 192.168.1.20.

Figura 46. Configuración conexión LAN

En el dashboard de Zentyal, se ingresa en el panel izquierdo, en la opción cortafuegos y se selecciona la opción “filtrado de paquetes”, ahí se selecciona la opción (Reglas de filtrado para las redes internas).

Figura 47. Cortafuegos

Lo anterior lleva a la siguiente pantalla, donde se añaden las reglas que se quieren realizar en el sistema, en este caso, bloquear redes sociales.

Figura 48. Configuración reglas

En este ejemplo, se realiza el bloqueo del sitio Facebook, para esto se hace un ping en la terminal para saber la IP del sitio.

```
andres-serrano@temporint:~$ ping facebook.com
PING facebook.com (69.171.250.35) 56(84) bytes of data.
```

Figura 49. Ping a sitio web

Se verifica que la IP arrojada lleve al sitio de la red social, colocando en el navegador la IP que arrojó el ping y comprobando si efectivamente cargó el sitio deseado.

Figura 50. Acceso a sitio web

Se regresa al dashboard de zentyal y se prosigue a configurar la regla, el cual es necesario seleccionar la opción, en **decisión:** denegar y en la opción **destino:** IP destino, colocar la IP que arrojó el ping realizado anteriormente y en **servicio,** la opción: cualquier TCP.

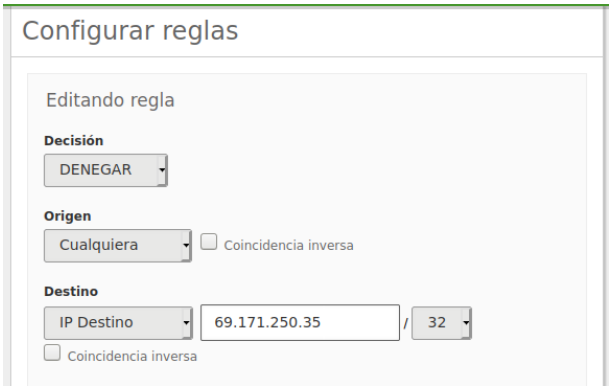

Figura 51. Creación de reglas

Se guardan los cambios y el sistema arroja la siguiente pantalla, la cual muestra las reglas creadas en el sistema.

Figura 52. Reglas creadas

Para saber si la configuración fue tomada de manera correcta, se dirige al pc cliente y se intenta ingresar al sitio bloqueado, ahí se debe visualizar que no se tiene acceso.

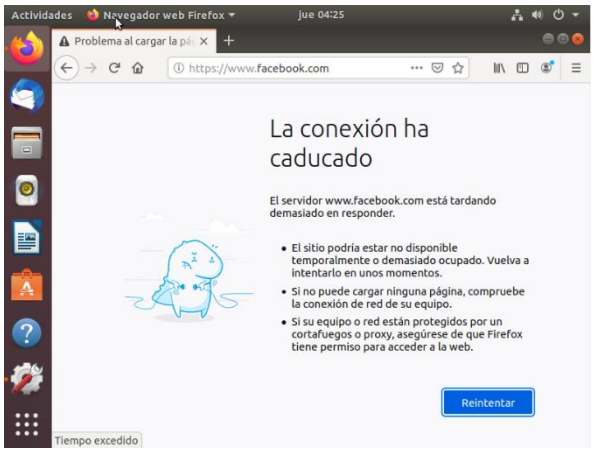

Figura 53. Verificando acceso sitio restringido.

Se verifica que tenga acceso a otros sitios web, que no estén bloqueados en Zentyal.

Figura 54. Verificando navegación a otros sitios web

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER.

3.4.1 FILE SERVER

Para la configuración del recurso: compartir ficheros e impresoras. Se validará el estado de los módulos, si el Controlador de dominio, archivos compartidos y DNS, ya se encuentran instalados en el servidor, a través de la interfaz de administración.

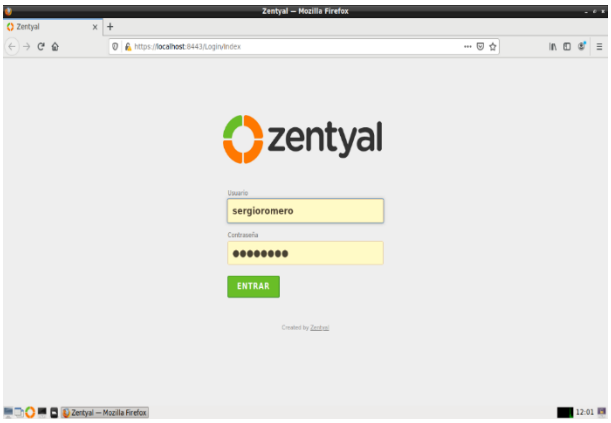

Figura 55. Ingreso al programa Zentyal.

Si no están instalados, se seleccionan y se continúa.

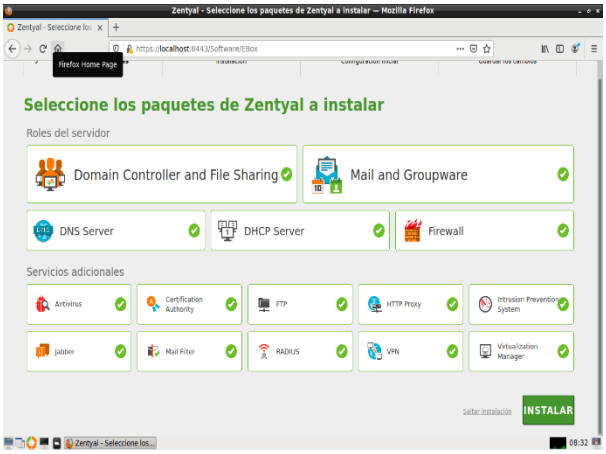

Figura 56. Selección paquetes de Zentyal.

Es posible también actualizarlos sí ya se encuentran instalados.

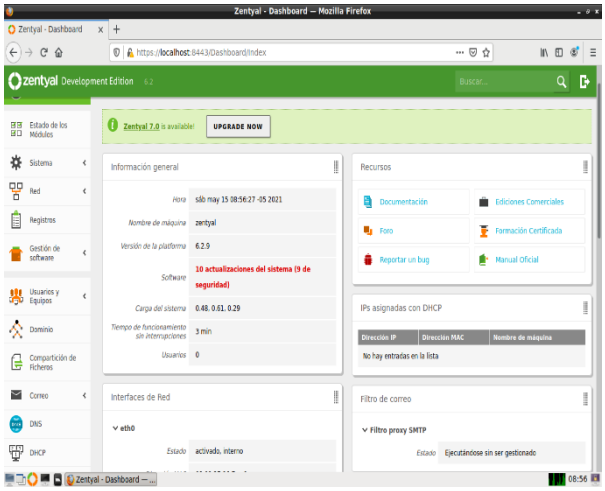

Figura 57. Dashboard de Zentyal.

Los servicios como el controlador de dominio permiten identificar todos los usuarios, equipos y recursos autorizados a través de los roles de seguridad. El servicio DNS resuelve nombres de equipos en la red asociados a una IP y el módulo de compartir ficheros, para administrar y habilitar carpetas y/o recursos a compartir en la red.

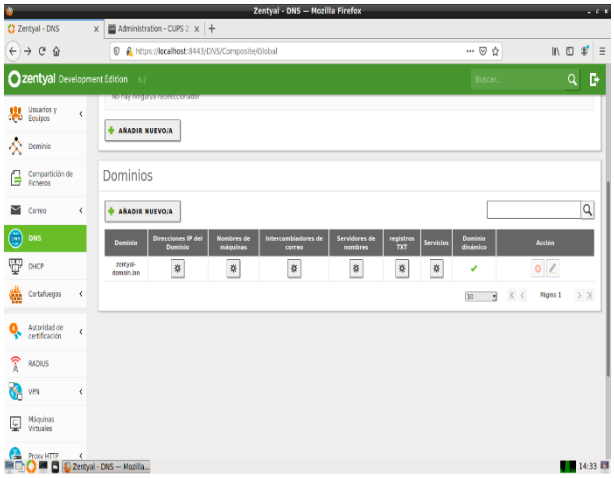

Figura 58. Servicios DNS Zentyal.

Se valida los usuarios, grupos creados en Zentyal.

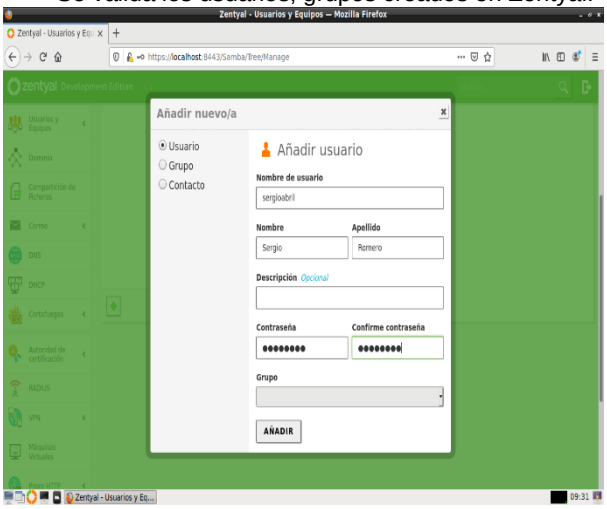

Figura 59. Crear usuario en Zentyal.

Se Ingresa al módulo compartición de ficheros para habilitar un directorio nuevo y/o bajo la raíz y se guardan cambios.

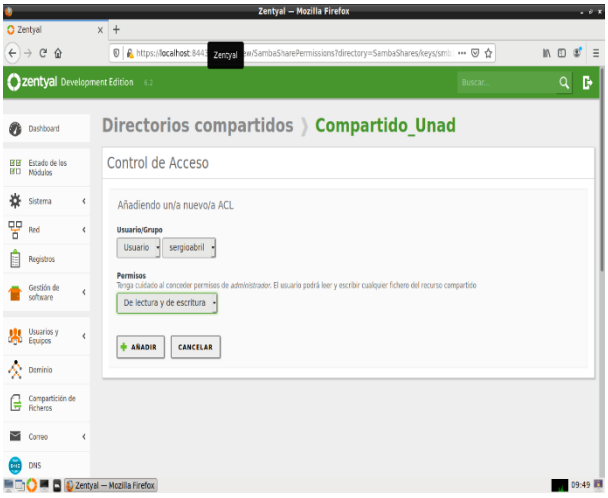

Figura 60. Permisos usuario en Zentyal.

En este módulo se pueden compartir los directorios que considere y a los usuarios que se asignen. También se puede ingresar como invitado al contenido de la carpeta si habilita la opción. En este caso se crea el fichero Compartido_Unad.

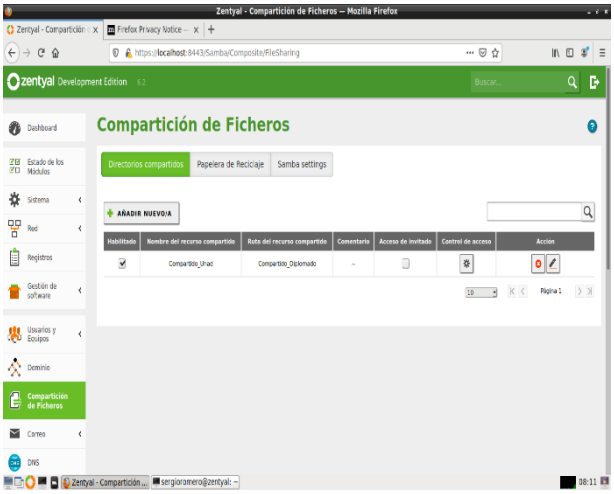

Figura 61. Permisos a ficheros.

El usuario asignado a esta carpeta se llama empleado, usuario con permisos de lectura y escritura sobre el directorio compartido creado. Control de acceso a carpeta compartida.

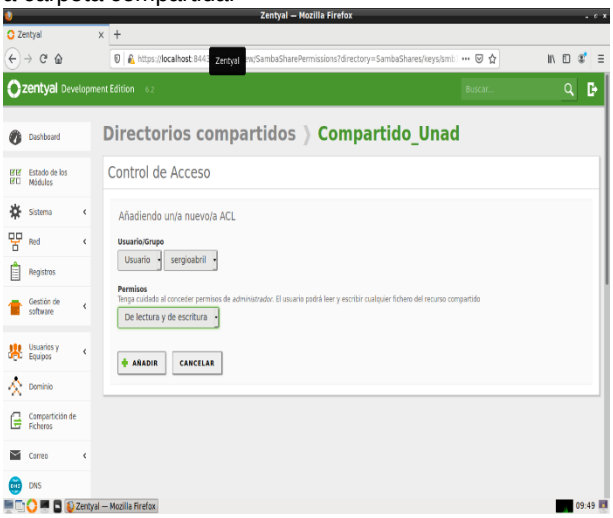

Figura 62. Permisos usuario al recurso compartido.

Ahora, desde un equipo con Ubuntu en el mismo segmento de red, valida los sitios de red para encontrar el equipo servidor. También a través del comando ejecutar con la IP se puede acceder al recurso compartido.

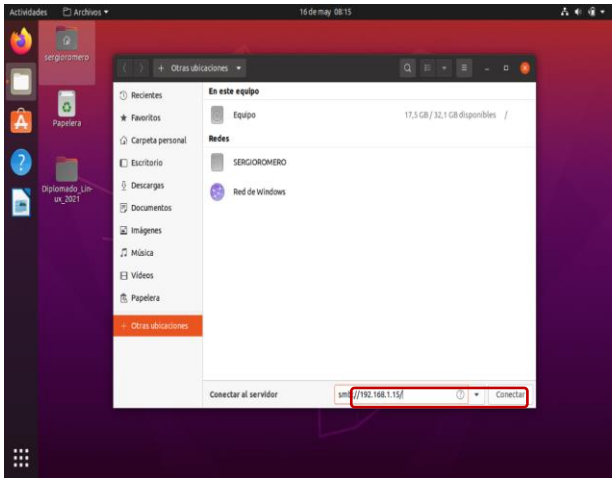

Figura 63. Conexión a servidor

Se da clic en conectar y mostrará el recurso compartido creado anteriormente (Compartido_Unad).

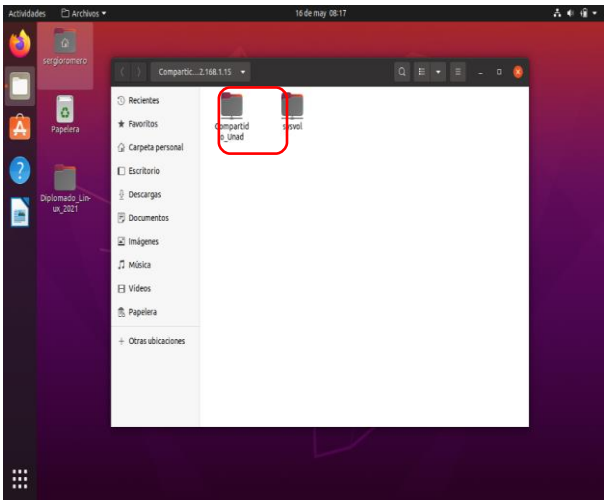

Figura 64. Conexión a recurso compartido

Al ingresar, pedirá las credenciales para el ingreso, se digita las creadas en Zentyal para que permita el acceso.

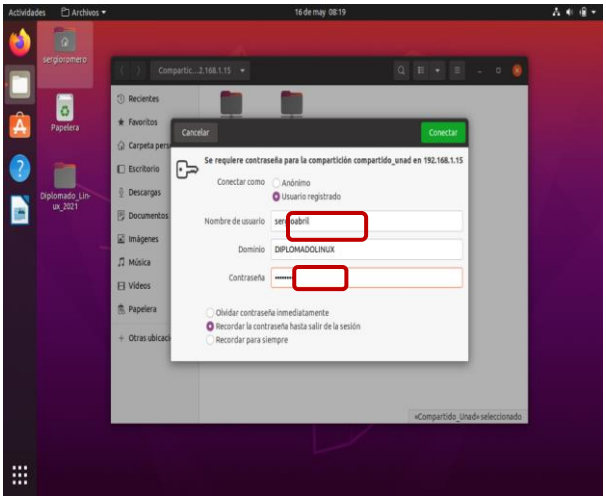

Figura 65. Credenciales de conexión.

Se crea una carpeta para comprobar los permisos del usuario que ingreso al recurso compartido.

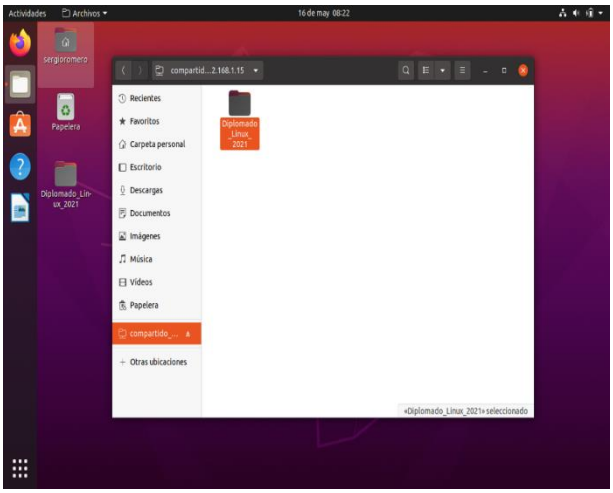

Figura 66. Validación de permisos.

3.4.2 PRINT SERVER

Se instala el comando para la configuración de la impresora. (**$sudo apt-get install cups**).

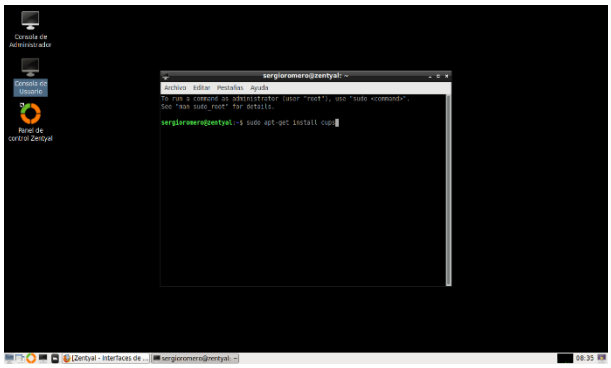

Figura 67. Comando **apt-get install cups**

Se instala CUPS para la configuración de la impresora.

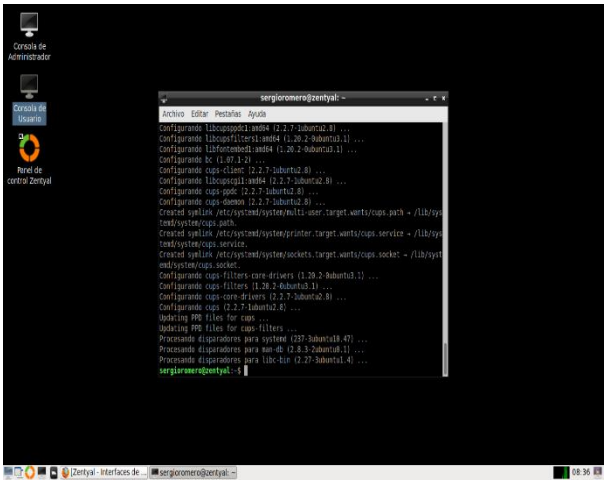

Figura 68. Instalar CUPS.

Instala el controlador requerido para la impresión.

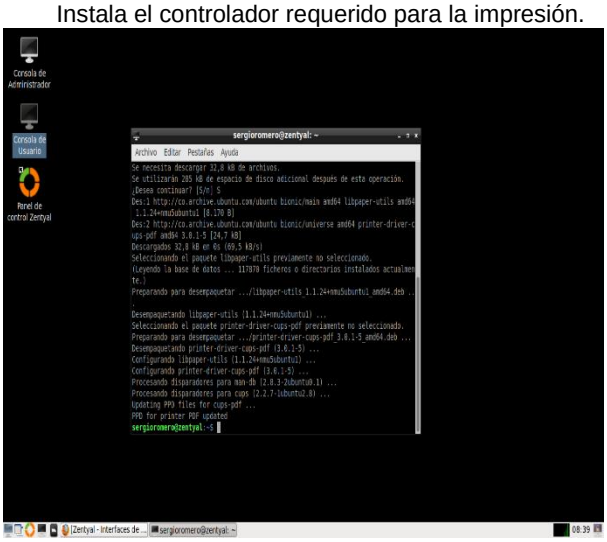

Figura 69. Instala ***install cups-pdf***.

Una vez finalizada la instalación de los paquetes, se abre el navegador y se ingresa a la interfaz web del servidor CUPS mediante la url http://localhost:631/admin. Para la autenticación se usará el mismo usuario y contraseña con el que se accede al servidor.

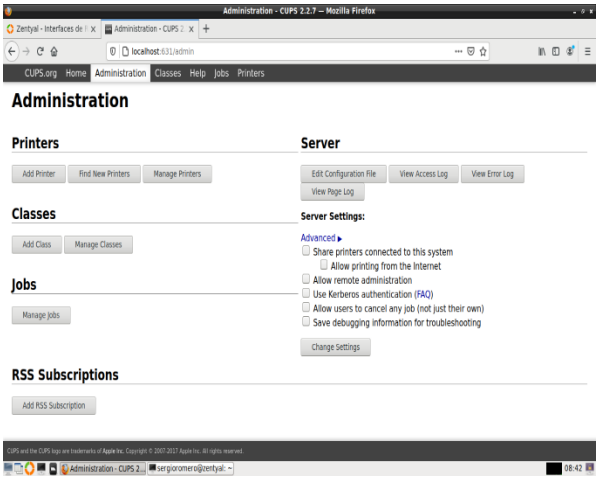

Figura 70. Inicio ***CUPS***

Ingresar a Add Printer para agregar la impresora. Se selecciona el protocolo ***ipp.***

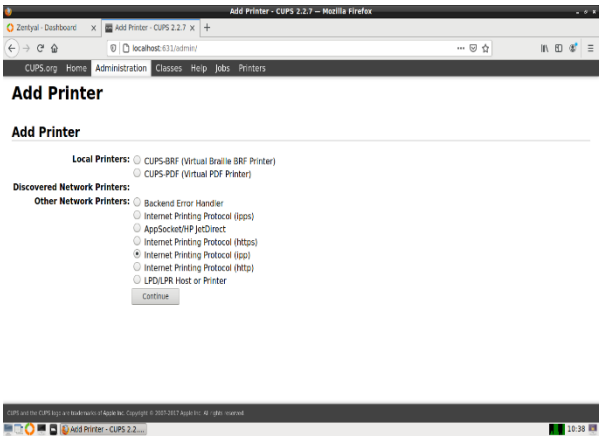

Figura 71. Agregar Impresora*.*

Al seleccionar el protocolo ***ipp (Internet Printing Protocol)*** se ingresa la conexión para la impresora.Con la ip del servidor.(192.168.1.15).

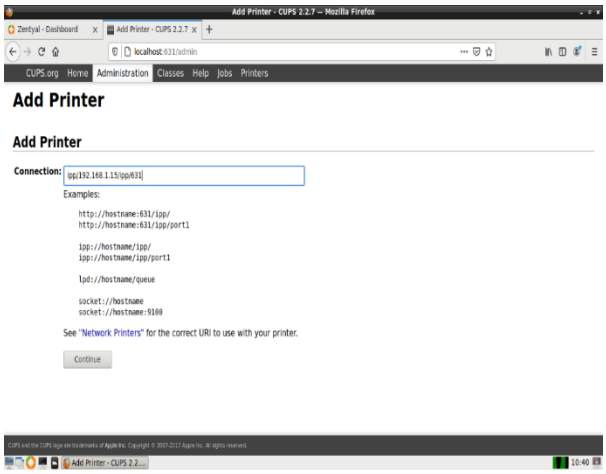

Figura 72. Selección protocolo*.*

En la siguiente pantalla, se agrega el nombre de la impresora, una descripción (No es obligatorio), la ubicación y compartir la impresora, para que se pueda visualizar (Share this Printer).

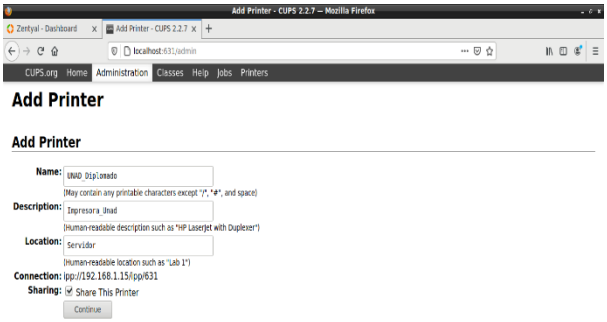

Figura 73. Selección nombre impresora.

En la opción de Impresoras (Printers), está agregada la impresora UNAD_Diplomado.

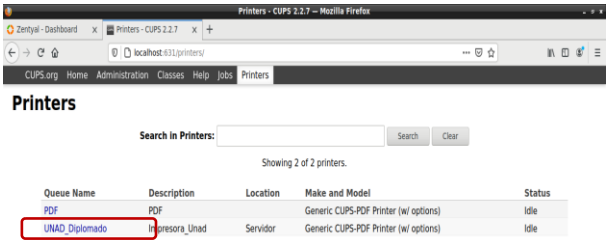

Figura 74. Agregar impresora*.*

3.5 TEMÁTICA 5: VPN

Una vez instalado Zentyal, se realiza la configuración inicial, instalando el módulo VPN. Donde adicionalmente se instalarán los paquetes de Autoridad Certificadora, Firewall, Configuración de Red y VPN.

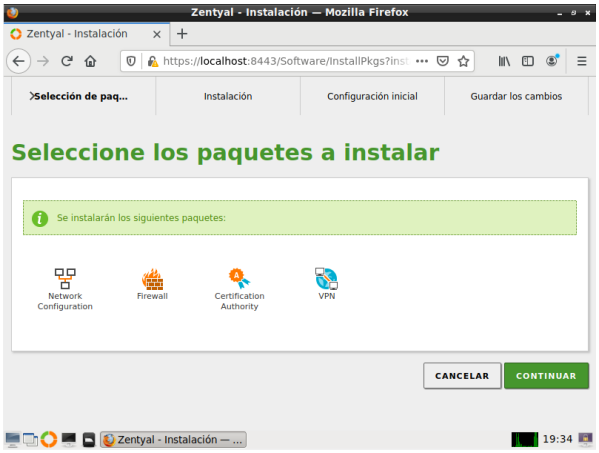

Figura 75. Paquetes para instalar

3.5.1 CERTIFICACIÓN Y CONFIGURACIÓN DEL SERVIDOR VPN EN ZENTYAL

Una vez se realiza la configuración inicial, el sistema empieza a guardar dicha configuración. Una vez hecho esto, se cargará la Dashboard, en la cual se puede apreciar en la parte izquierda, las distintas opciones que tiene disponible, allí, se deberá ir inicialmente a Autoridad de Certificación/General, esto, para expedir un certificado que permita la implementación del servidor VPN.

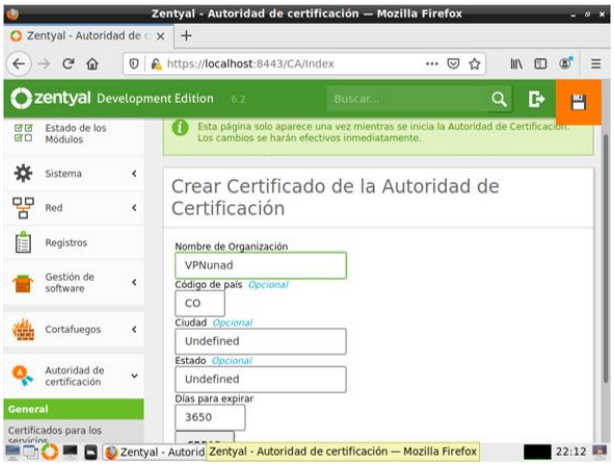

Figura 76. Certificado para servidor VPN

Una vez creado el certificado para el servidor VPN se puede continuar a añadir un nuevo servidor VPN, esto, desde VPN/Servidores, que estará ya habilitado.

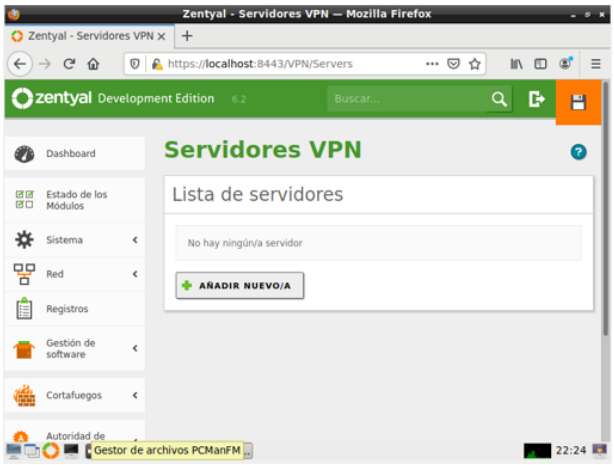

Figura 77. Función de añadir en el servidor VPN habilitada

Después de añadir un nuevo servidor, se le asignará un nombre y se añadirá, una vez hecho esto, mostrará lo siguiente:

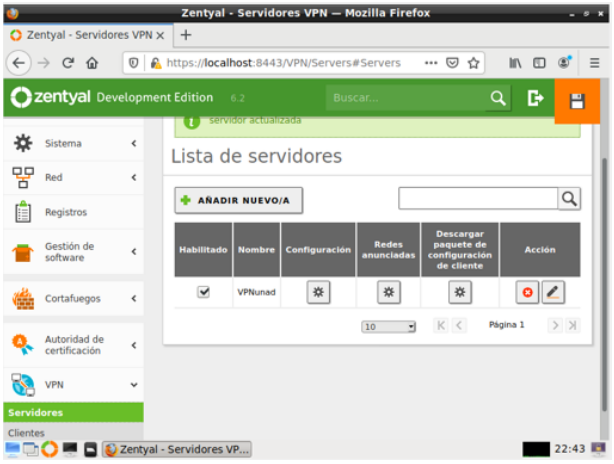

Figura 78. Servidor VPN añadido

Siguiente al añadimiento del nuevo servidor VPN, se procede a configurarle los parámetros en los que funcionará. En esta configuración se le asignará un puerto, una dirección VPN, el certificado anteriormente creado para el servidor VPN y los parámetros necesitados.

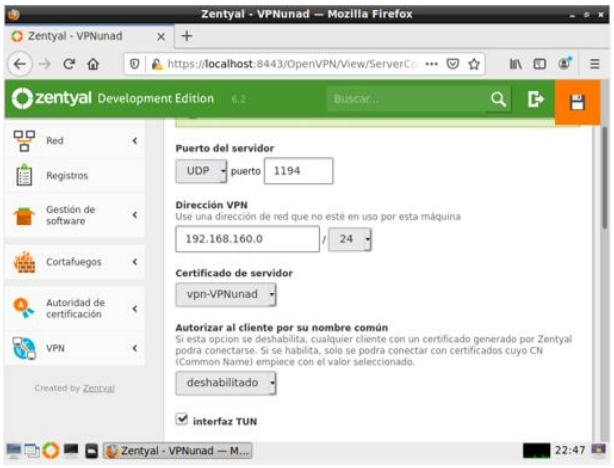

Figura 79. Configuración del servidor VPN

3.5.2 CERTIFICACIÓN Y CONFIGURACIÓN DEL USUARIO

Para que un usuario pueda hacer uso del servidor VPN se deberá crear un certificado que le permita al usuario hacer uso de este servidor. Para ello, nuevamente en Autoridad de Certificación/General se expide un certificado para el usuario.

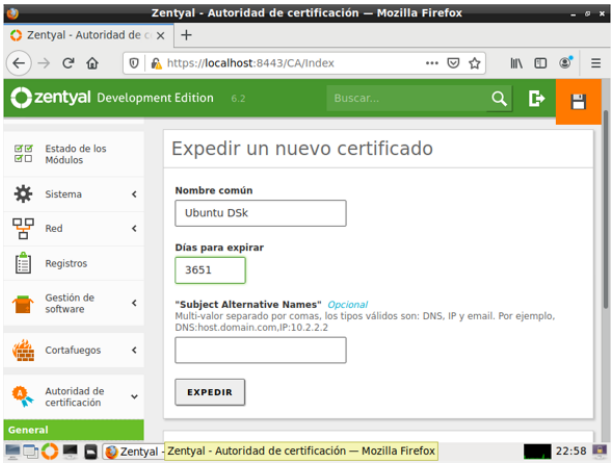

Figura 80. Certificado para el usuario/cliente

Una vez expedido el certificado para el usuario, nuevamente en Servidores VPN se escoge la opción de “Descargar paquete de configuración de cliente”, después cargará la ventana donde se deberán configurar los parámetros del usuario donde se seleccionará el tipo de usuario, el certificado del usuario, tipo de conexión y dirección del servidor, la cual deberá ser una IP estática.

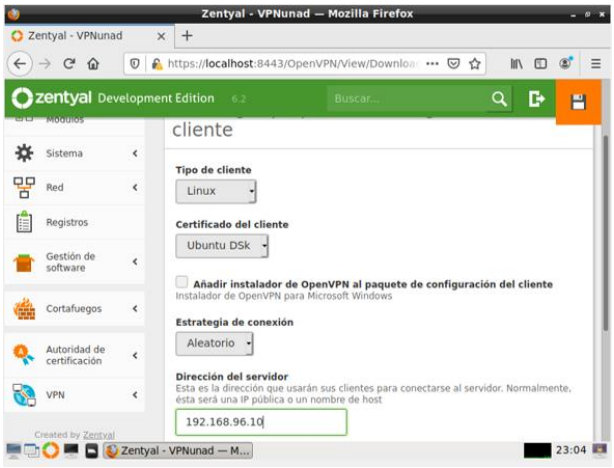

Figura 81. Configuración del cliente

Este generará un paquete de configuración para el cliente y que así se pueda configurar los parámetros de configuración en el equipo del cliente de manera más sencilla.

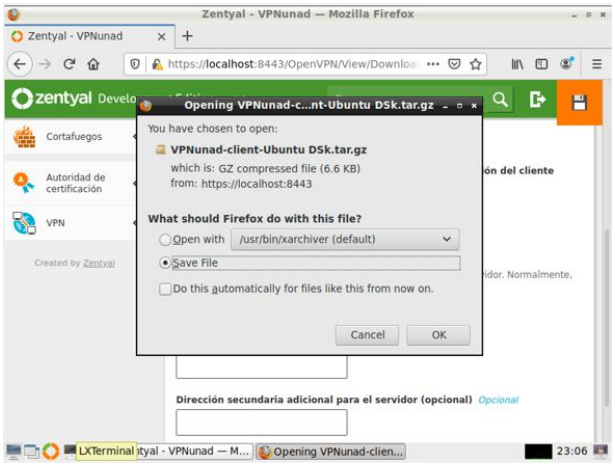

Figura 82. Paquete de configuración para cliente

Ahora desde el cliente se añade una nueva VPN, esto, desde configuración de red del equipo, donde si no es posible mover el paquete de configuración previamente descargado en el servidor, se escogerá un el “Protocolo de túnel punto a punto (PPTP)”.

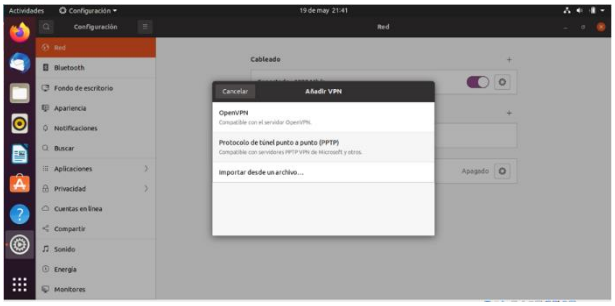

Figura 83. Añadiendo VPN en cliente

Una vez seleccionado el protocolo, se define un nombre con el que se identificará en el equipo (este

nombre no afecta la configuración y funcionamiento), y se le agrega la pasarela, que es la IP configurada en los parámetros del cliente en el servidor. Después de esto se seleccionará la configuración avanzada.

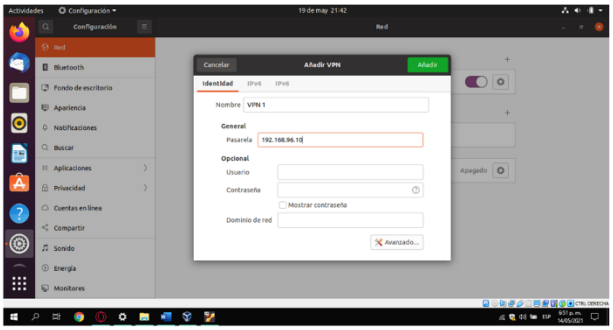

Figura 84. Configuración inicial en cliente

En configuración avanzada, se selecciona la casilla “Usar cifrado punto a punto (MPPE)”, luego se acepta la configuración y se añade la conexión VPN.

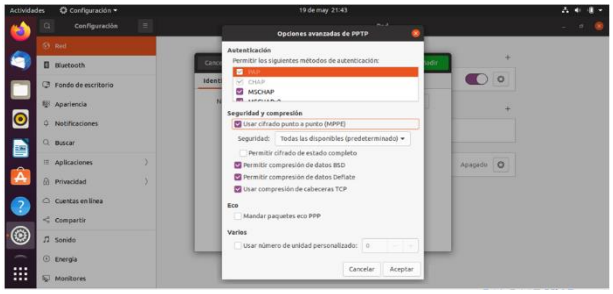

Figura 85. Configuración del cifrado en cliente

Después de configurar lo anterior se podrá habilitar la conexión VPN.

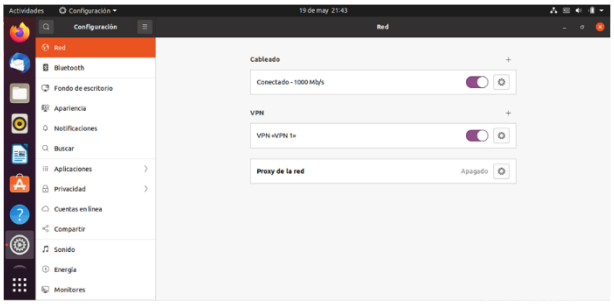

Figura 86. Conexión vpn habilitada en cliente

Otra forma de demostrar que el servidor VPN se está ejecutando, es en la Dashboard del servidor Zentyal donde muestra la información de los “Demonios OpenVPN”.

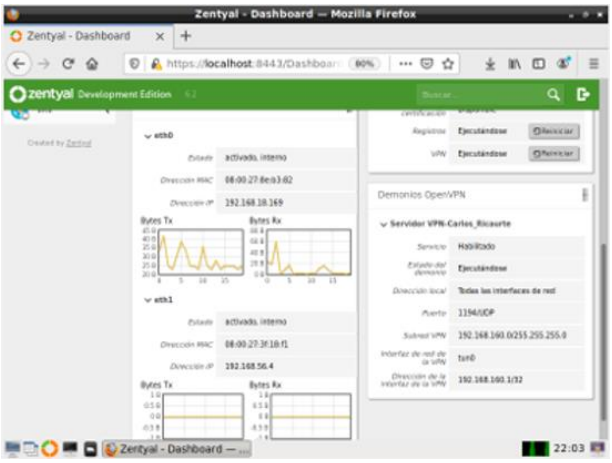

Figura 87. Pruebas de ejecución en la DashBoard

4 CONCLUSIONES.

El desarrollo de esta fase permitió conocer una herramienta muy completa como lo es Zentyal, destinada para aquellos tipos de empresas que están empezando o que llevan años en el mercado y están en la búsqueda de alternativas para la reducción de costos sin afectar sus diferentes servicios.

Un punto fuerte a destacar en Zentyal Server es la incorporación nativa de protocolos Microsoft, que le da completa compatibilidad con algunos de sus productos, como Outlook y Active Directory. Empero, hay otro punto que puede ser interpretado como una debilidad para la versión Community y es que el servicio Proxy no hace filtrado HTTPS, siendo una característica exclusiva de la versión comercial. No obstante, se agradece sus prestaciones para limitar el ancho de banda de los usuarios, la caché para agilizar el acceso, el filtrado por categorías, entre otras.

Durante el desarrollo e implementación del servicio cortafuego bajo el sistema operativo Zentyal en su versión 6.2, comprendimos la importancia en llevar una muy organizada administración teniendo en cuenta la importancia e impacto que genera en una organización y los riesgos que se pueden mitigar al evitar su respectivo acceso.

Zentyal ofrece una alternativa DNS para la resolución de nombres para no tener que depender de las DNS de Google. Para compartir una impresora de nuestra red, permitiendo o denegando el acceso a usuarios y grupos para su uso, se debe tener accesibilidad a dicha impresora desde la máquina que contenga Zentyal, ya sea por conexión directa, puerto paralelo, USB, o a través de la red local.

Durante el desarrollo del Paso 8 - Solucionando necesidades específicas con GNU/Linux, pudimos aprender a 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, Backus, Gateway, cortafuegos y proxy HTTP, por mencionar algunos. Se realizo la formulación de soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente.

5 REFERENCIAS

[1] Zentyal 6.2 Documentación Oficial — Documentación de Zentyal 6.2. (s. f.). Zentyal. https://doc.zentyal.org/6.2/es/

[2] "Servicio de configuración de red (DHCP)", Zentyal Community. [Online]. https://doc.zentyal.org/es/dhcp.html.

[3] "Servicio de Proxy HTTP", Zentyal Community. [Online]. https://doc.zentyal.org/es/proxy.html.

[4] "Cortafuegos", Zentyal Community. [Online]. https://doc.zentyal.org/es/firewall.html.

[5] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40

[6] Zentyal Community. Zentyal 6.2 Documentación Oficial (2015). Servicio de redes privadas virtuales (VPN) con OpenVPN. https://doc.zentyal.org/6.2/es/vpn.html#configuracion-de-un-servidor-openvpn-con-zentyal