Instalación y configuración de Zentyal Server para implementar los servicios de infraestructura IT.

Integrante 1 (Edward Haidygguert González Rodríguez)
e-mail: ehgonzalezro@unadvirtual.edu.co
Integrante 2 (Rafael E Cepeda Tapias)
e-mail: recepedat@unadvirtual.edu.co
Integrante 3 (Heiver Arley Adame)
e-mail: haadamec@unadvirtual.edu.co
Integrante 4 (Daniela Giraldo Quintero)
e-mail: dgiraldoq@unadvirtual.edu.co
Integrante 5 (Jennifer Alexandra Román Rogelis)
e-mail: jaromanr@unadvirtual.edu.co

RESUMEN: *El presente artículo detalla la administración y control de la distribución GNU/Linux Zentyal Server 6.2, para la solución de servicios de infraestructura TI; detallando la implementación de servicios específicos como es: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN.*

PALABRAS CLAVE: proxy no transparente, cortafuegos, DNS, VPN.

1 INTRODUCCIÓN

En el presente artículo se encuentra la solución a problemáticas específicas de infraestructura tecnológica utilizando e implementando tecnologías GNU/Linux como es el caso de Zentyal, es así que en el artículo se detalla la instalación y configuración básica de este sistema operativo ya que Zentyal incluye los elementos necesarios para control, administración y gestión de servicios esenciales de la estructura de red ofreciendo acceso fiable y seguro a Internet. También, se detalla implementación y configuración los servicios de DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN, de acuerdo a los requerimientos especificados.

2 INSTALACIÓN DE ZENTYAL 6.2

2.1 CARACTERÍSTICAS DE INSTALACIÓN EN VIRTUALBOX.

La máquina virtual para la instalación de Zentyal 6.2, tiene las siguientes características memoria RAM 2048 MB, Procesadores 1, almacenamiento de disco HDD 100 GB y dos adaptadores de red, uno como adaptador puente con acceso a Internet, el segundo como red interna para conexión con Ubuntu desktop.

2.2 INSTALANDO ZENTYAL SERVER EN MAQUINA VIRTUAL VIRTUALBOX

Ver figuras 1,2 ,3

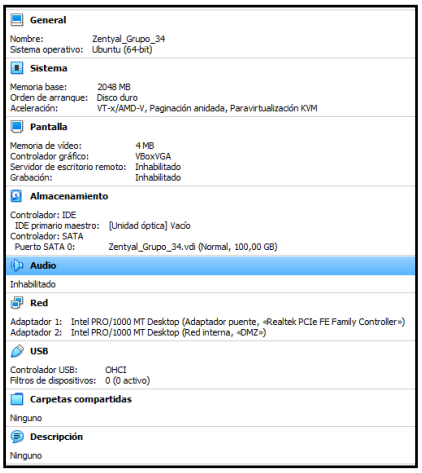

Figura 1. Configuración de máquina virtual en virtualBox para instalación de Zentyal 6.2

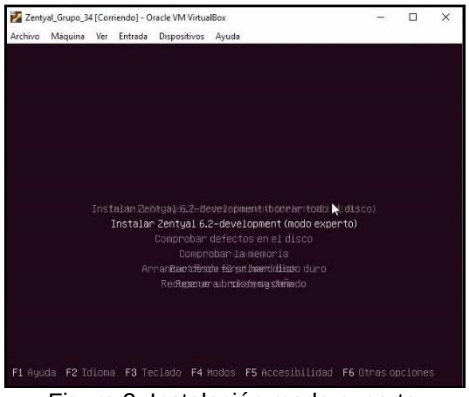

Figura 2. Instalación modo experto

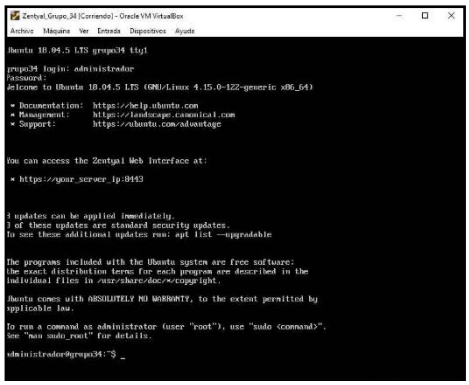

Figura 3. Instalación Zentyal 6.2 sin entorno gráfico.

2.3 CONFIGURACIÓN INICIAL DE ZENTYAL

Una vez terminada la instalación, se accede remotamente al servidor mediante un navegador indicando la dirección del servidor Zentyal (https://ip_servidor:8443), introducir usuario y contraseña para iniciar la configuración inicia, allí puede elegirse alguno de los paquetes a utilizar, los demás paquetes se pueden instalar posteriormente ingresando al módulo gestión de software (Figura 4).

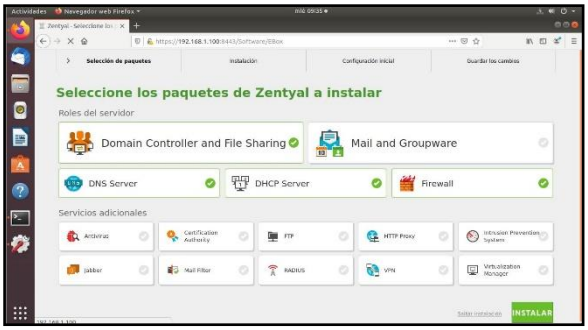

Figura 4. Selección inicial de paquetes a instalar.

Es importante aclarar que Zentyal realiza la instalación de los paquetes básicos y necesarios como es el módulo de red, luego de la instalación se debe configurar los dispositivos de red de los cuales uno de ellos debe estar conectado a red externa y el otro a red interna, indicando una dirección ip fija en la red interna, el dispositivo externo puede ir configurado como DHCP (figuras 5 y 6).

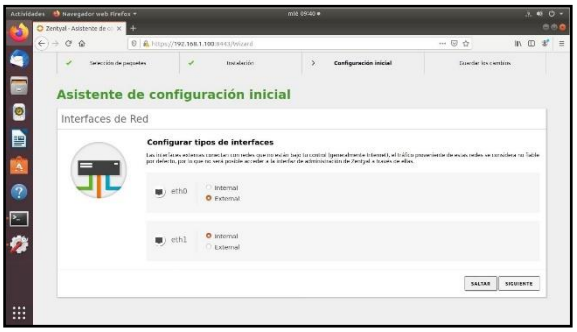

Figura 5. Configuración de tipo de interfaces.

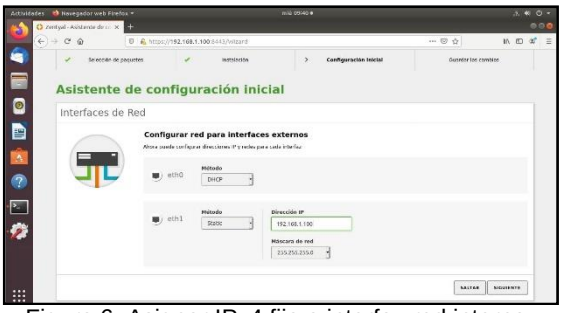

Figura 6. Asignar IPv4 fija a interfaz red interna.

Por último, en la configuración inicial se asigna el nombre de dominio para el servidor, finalizando así la configuración inicial (Figura 7).

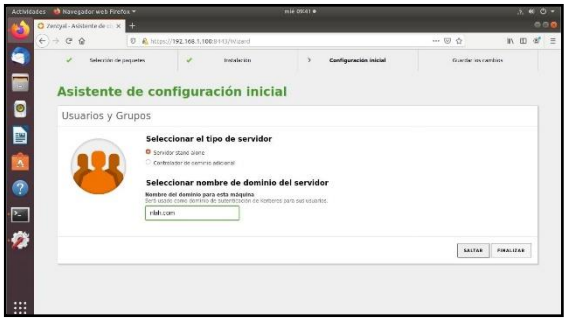

Figura 7. Asignar nombre de dominio el servidor.

3 INTEGRACIÓN TECNOLÓGICA

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

3.1.1 DHCP SERVER

En la configuración del servidor DHCP, primero que se verifica las interfaces de red, para asignar el servicio DHCP a la a la interface de red interna, en este caso interface Eth1, luego seleccionar el módulo DHCP, donde se observan las interfaces para asignación del servicios, en la interface seleccionada se da clic en el botón de configuración (figura 8), esto abre una nueva ventana, se observa las secciones opciones personalizadas, donde sólo se modifica el dominio de búsqueda, asignando el dominio creado el instalación inicial (figura 9), en la sesión rangos se asignan el rango de direcciones IPv4 para este ejemplo va desde 192.168.1.101 a 192.198.1.200 (figura 10), en esta misma ventana en la parte superior se encuentran botón Opciones de DNS Dinámico, se da clic en este botón; en la ventana que despliega, activar en el cuadro de verificación opciones de DNS dinámico, en dominio dinámico establecer el nombre de dominio el cual se asignó en la configuración inicial para este caso y en dominio estático, el mismo que el dominio dinámico (figura 11).

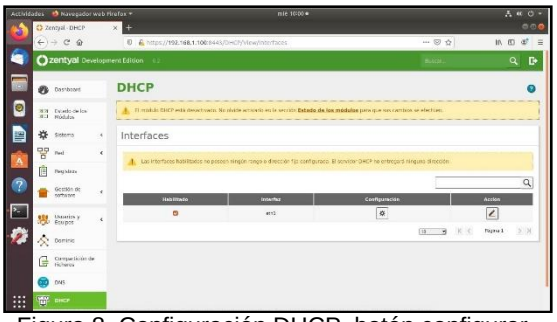

Figura 8. Configuración DHCP, botón configurar.

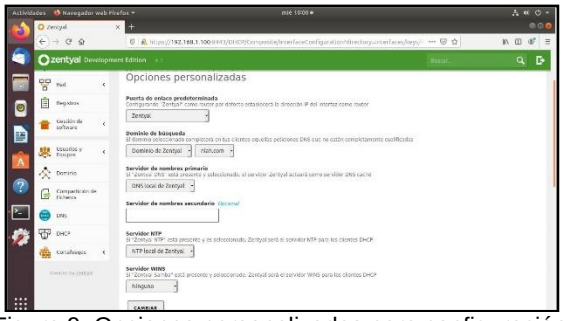

Figura 9. Opciones personalizadas para configuración del servidor DHCP.

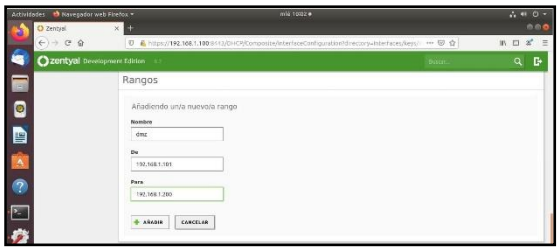

Figura 10. Rango de direcciones IPv4 a asignar.

Figura 11. Opciones de DNS dinámico.

Terminada la configuración del servidor DHCP, se guardan los cambios, se pasa a la configuración cableada del equipo de escritorio, estableciendo el método como automático asignación por DHCP (Figura 12).

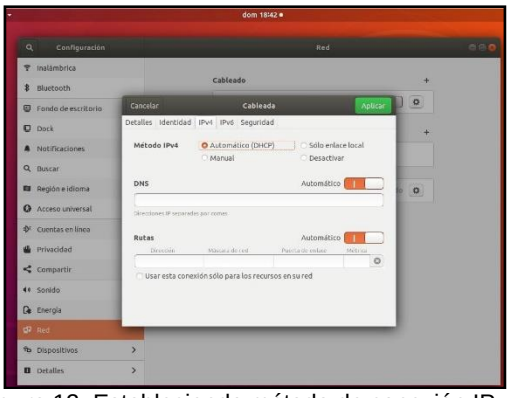

Figura 12. Estableciendo método de conexión IPv4.

3.1.2 DNS SERVER

Para la configuración del servidor DNS, en este caso ya se había creado el nombre de dominio del servidor en la configuración inicial, las toma el servidor DNS, por lo cual sólo se harán unas pequeñas adiciones a la configuración del servidor DNS para garantizar la conexión a Internet. Es así que se activa Habilitar el caché de DNS transparente (ver figura 13) el consiste en que Zentyal identifica el tráfico de las peticiones de resolución de nombre de dominio de un cliente y realiza el cambio en el destino de la petición y en lugar de que el cliente pida la información a un equipo foráneo este se la solicite al servidor DNS

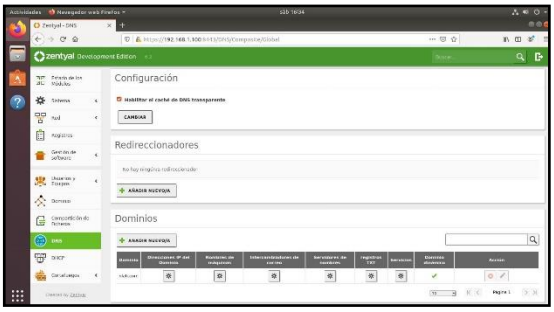

Figura 13. Configuración del servidor DNS.

3.1.3 CONTROLADOR DE DOMINIO

En la configuración de control de dominio, en el menú de la izquierda del Dashboard se encuentra dominio, en la ventana que se despliega en la parte donde dice función del servidor, se asigna controlador del dominio (figura 14), se da clic en cambiar y guardar cambios. A continuación, se procede a modificar el usuario administrador en la gestión de usuarios y equipo; asignando una clave la llenar el formulario (figura 15).

Después de configurar el servidor, se procede a integrar el equipo Ubuntu deskto al controlador de dominio en Zentyal, para esto se descargan los siguientes paquetes: libglade2-0_2.6.4-2_amd64.deb, dpkg -i likewise-open_6.1.0.406-0ubuntu5_amd64.deb y likewise-open-gui_6.1.0.406-0ubuntu10_amd64.deb, estos se descargan de de las respectivas URL mediante el comando wget, con las siguientes instrucciones (figura 16):

wget http://ftp.ntou.edu.tw/ubuntu/ubuntu/pool/universe/libg/libglade2/libglade2-0_2.6.4-2_amd64.deb

wget http://archive.ubuntu.com/ubuntu/pool/main/l/likewise-open/likewise-open_6.1.0.406-0ubuntu5_amd64.deb

wget http://old-releases.ubuntu.com/ubuntu/pool/universe/l/likewise-open/likewise-open-gui_6.1.0.406-0ubuntu10_amd64.deb

Luego de descargar los paquetes debían continúa con la instalación de estos mediante los siguientes comandos (figura 17):

sudo dpkg -i libglade2-0_2.6.4-2_amd64.deb

sudo dpkg -i likewise-open_6.1.0.406-0ubuntu5_amd64.deb

sudo dpkg -i likewise-open-gui_6.1.0.406-0ubuntu10_amd64.deb

Por último, se ejecuta el siguiente comando sudo domainjoin-gui (figura 18), para ejecutar likewise, el cual no permite acceder al dominio, suministrando el nombre del dominio, el usuario y el password (ver figuras 19), una vez suministrados los datos de ingreso, un mensaje informa que se ha unido a dominio (figura 20).

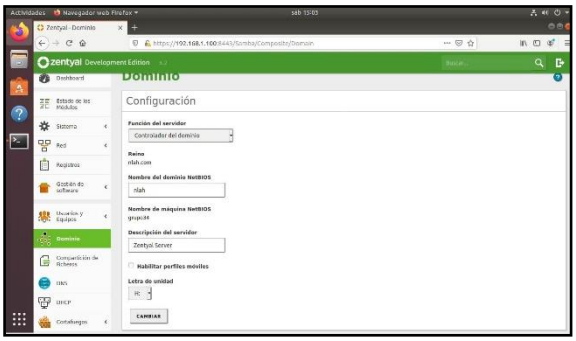

Figura 14. Configuración de dominio.

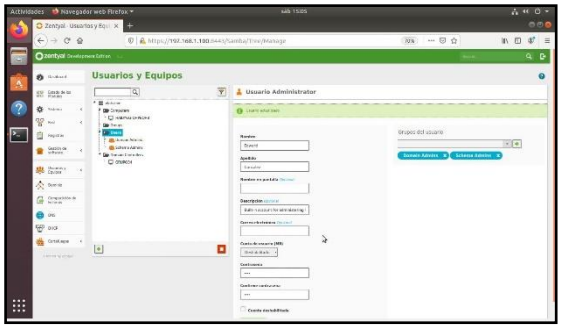

Figura 15. Formulario del administrador del dominio.

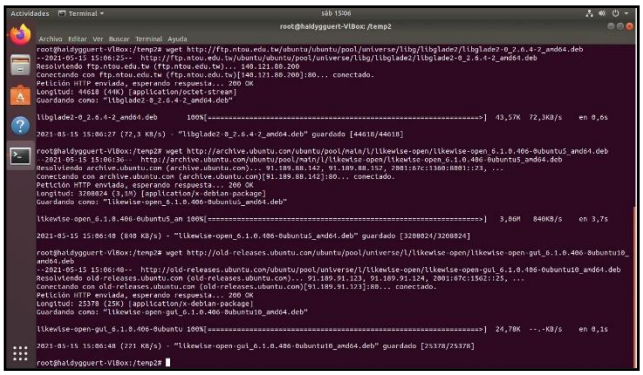

Figura 16. Descarga de paquetes deb debian para instalación de likewise.

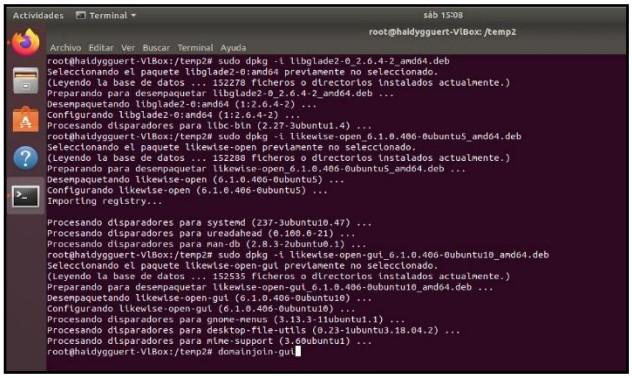

Figura 17. Instalación de paquetes debían para likewise.

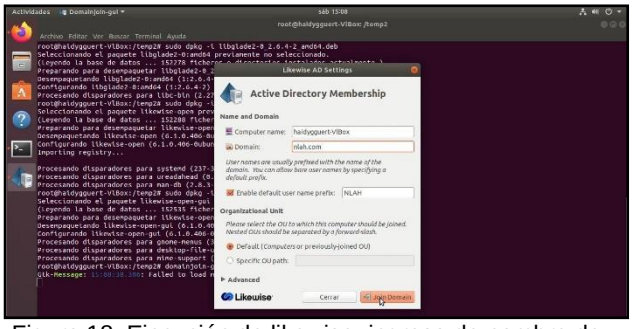

Figura 18. Ejecución de likewise, ingreso de nombre de dominio.

Figura 19. Autenticación de usuario y password.

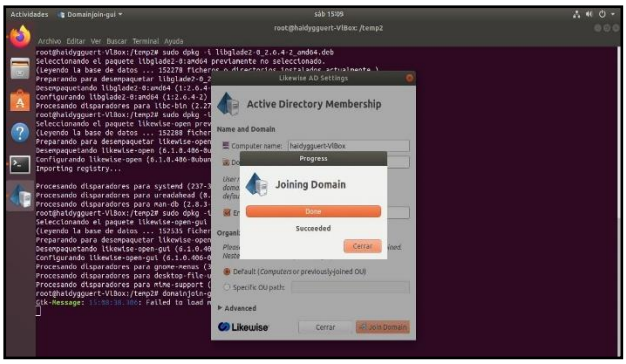

Figura 20. Mensaje indicando el ingreso al dominio.

Por último, se realiza una verificación para constatar que el equipo se encuentra en el dominio (Figura 21).

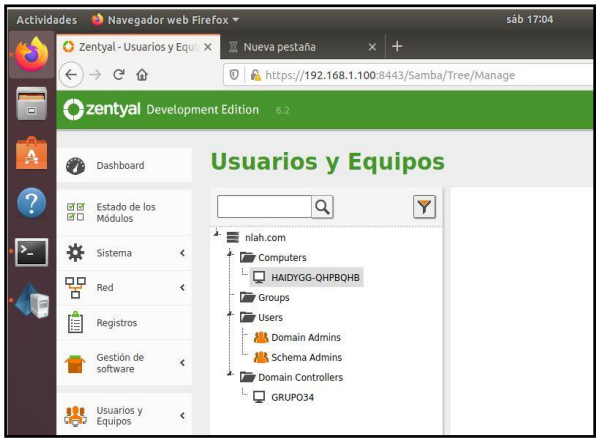

Figura 21. Verificación que el equipo de escritorio Ubuntu 18.04 se encuentra en el dominio.

3.2 PROXY NO TRANSPARENTE

Ya configurados el servidor DHCP y el servidor DNS, se procede a la instalación del Proxy para esto buscar al lado izquierdo del Dashboard la opción “gestión de software” y seleccionar el componente Proxy (Figuras 22 y 23).

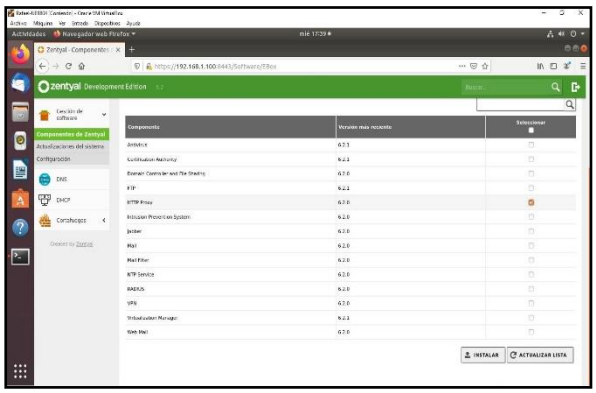

Figura 22. Selección de componente Proxy.

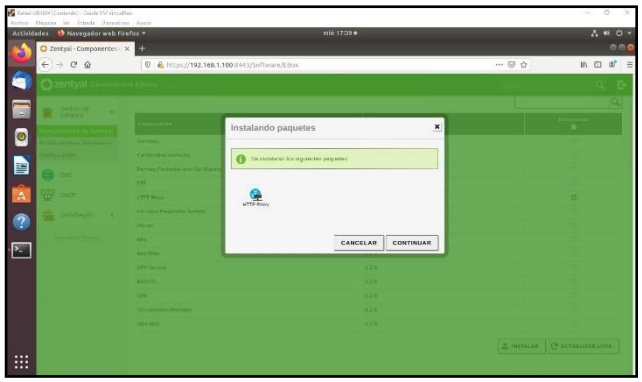

Figura 23. Instalando servidor Proxy

Al terminar el proceso de instalación Zentyal, informa que el componente Zentyal-squid no se instala correctamente, además está la solución indicando la distribución que se debe de ejecutar desde la consola en el servidor (Figuras 24 y 25).

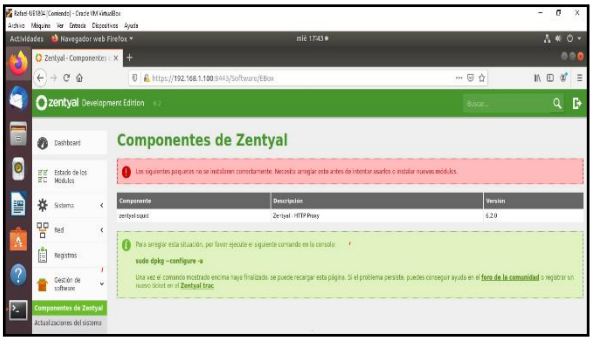

Figura 24. Solución a instalación incorrecta.

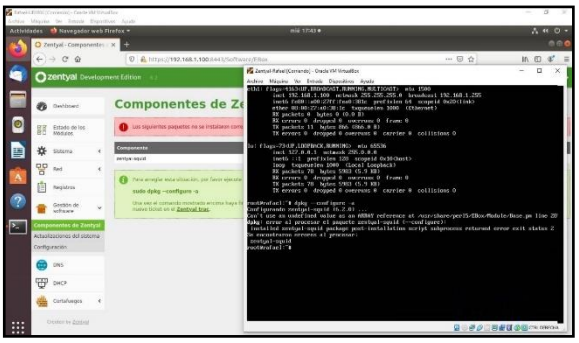

Figura 25. Ejecución de instrucción sudodpkg –configure -a, para solucionar problemas de instalación del servidor Proxy.

Una vez solucionado el problema de instalación, se procede a establecer las reglas de acceso a Internet por parte del equipo con los equipos conectados a Zentyal. Para establecer estas reglas de acceso primero se debe crear un objeto en la moción red del Dashboard. Para Zentyal Un objeto está compuesto por cualquier cantidad de miembros, cada uno de los cuales está a su vez compuesto por un rango de red o un host específico.

Entonces se crea el objeto **Ubuntu** y se configura sus miembros dando el nombre a estos como

Desktop, estableciendo estos miembros como los equipos en el rango de direcciones IP desde 192.168.1.101 y 192.168.1.200, (Ver figura 26 y 27).

Una vez creado el objeto y sus miembros, es posible configurar las reglas para que los miembros del objeto puedan acceder Internet, restringir el acceso a Internet, negar el acceso a sitios específicos como por ejemplo YouTube (Figura 28).

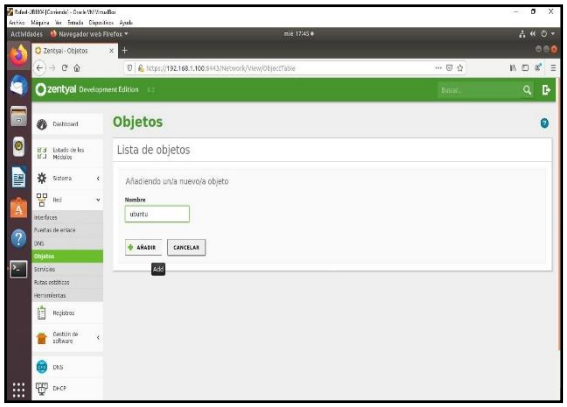

Figura 26. Añadiendo objeto a la red.

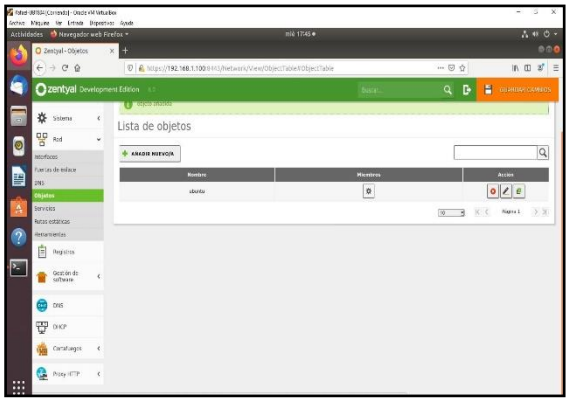

Figura 27. Configurar miembros al objeto Ubuntu.

Figura 28. Estableciendo el rango de los miembros del objeto Ubuntu, miembros con el nombre desktop.

Después, crear el objeto; hay que dirigirse a la configuración general del Proxy, donde se establece el puerto 1230 para el filtro de salida (Figura 29).

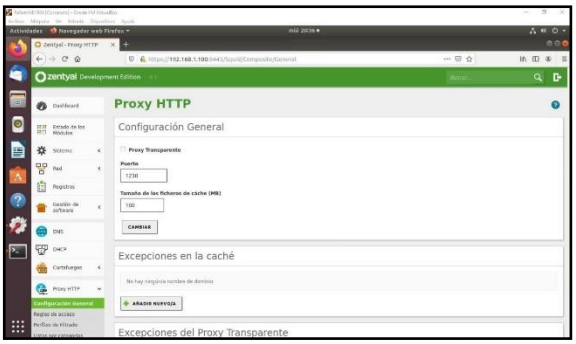

Figura 29. Configuración del Proxy no transparente.

Luego de realizar la configuración general del Proxy no transparente, se procede a realizar dos operaciones una la creación de perfiles de filtrado y la otra la creación de reglas de acceso.

Para este caso se realiza el siguiente ejemplo: se añade el perfil de filtrado llamado **Desktop,** luego se procede a configurar el perfil añadido, donde se especifica el nivel de filtrado para este caso se especifica como **Muy Estricto,** se guarda los cambios realizados y se procede a la pestaña **Reglas de dominio y URL**, aquí en la sección reglas de dominio y URL se procede añadir una nueva regla; donde se establece el dominio y la decisión; para este ejemplo el **dominio** es youTube.com y la **Decisión** es denegar (Figura 30, 31, 32 y 33).

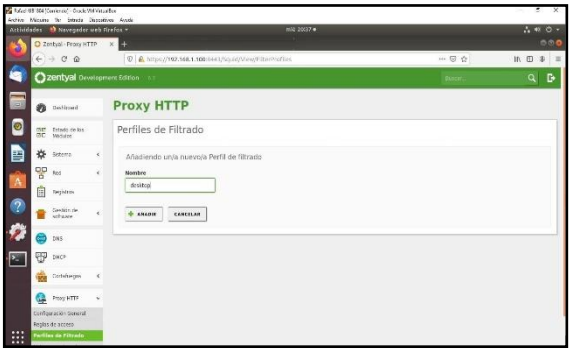

Figura 30. Añadiendo perfil de filtrado.

Figura 31. Estableciendo el umbral de filtrado.

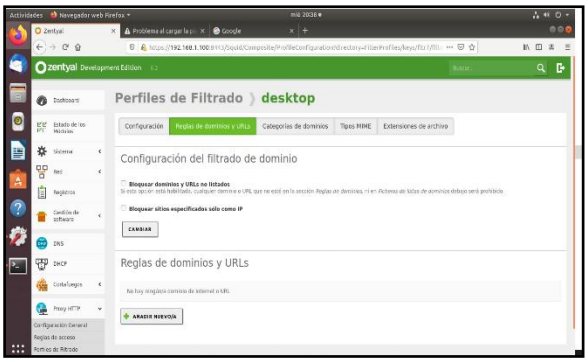

Figura 32. Añadir nueva regla de dominio y URL.

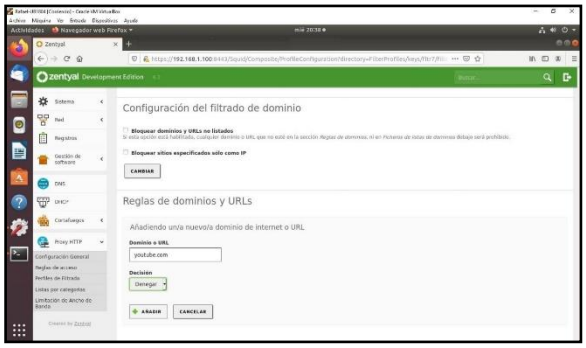

Figura 33. Acción de negación a dominio YouTube.com.

Una vez configuradas y añadidas la regla de filtrado de dominio, se procede añadir la regla de acceso (Figura 34).

Figura 34. Añadir nueva regla de acceso.

En la configuración de la regla, se establece el origen que es el objeto de la red creado anteriormente en la sesión de red del Dashboard y en la decisión se le aplica el filtro al perfil de filtrado creado (Figuras 35 y 36).

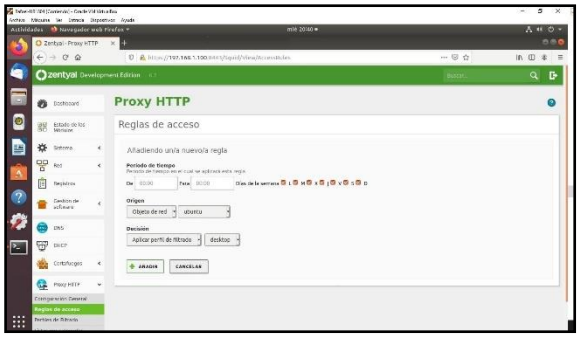

Figura 35. Figuración de regla de acceso.

Figura 36. Regla añadida.

Una vez realizadas todas las configuraciones del servidor Proxy, en los computadores de escritorio se configura el Proxy de la red, el cual puede realizarse en la configuración de red del equipo o en el navegador, para este caso realizo la configuración de Proxy de la red en las configuraciones de red de Ubuntu desktop y en las configuraciones de conexión del navegador, indico que utilice el Proxy del sistema (Figuras 37, 38 y 39).

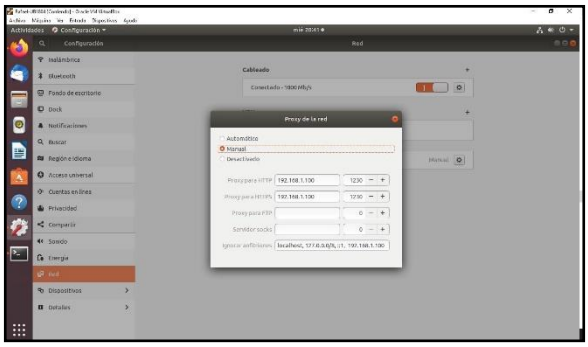

Figura 37. Configuración del Proxy de la red.

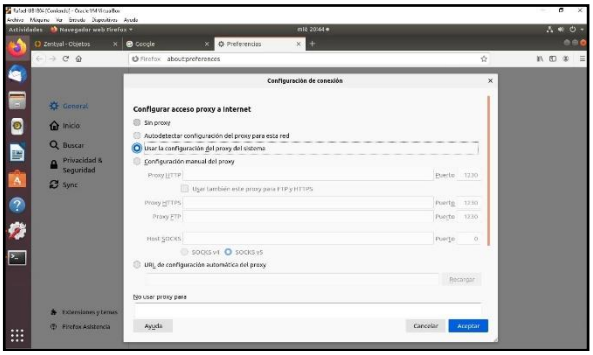

Figura 38. Configuración de conexiones en el navegador Firefox.

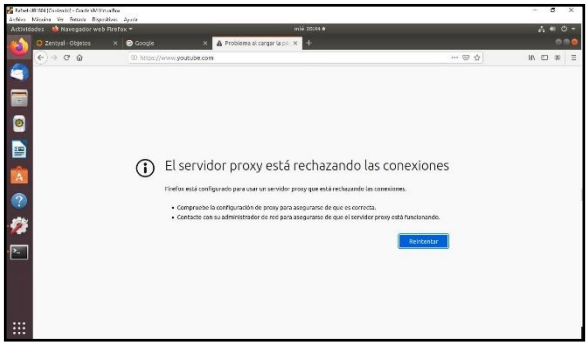

Figura 39. Evidencia de rechazo del servidor a la conexión a YouTube.

3.3 CORTAFUEGOS

Cuando zentyal interviene como cortafuegos, generalmente se realiza la instalación entre una red interna y el Reuter conectado a una red externa o internet.

Mediante la implementación del cortafuegos se implementas o establecen políticas de filtrado estrictas para las conexiones. Zentyal utiliza para su módulo de cortafuegos el subsistema del kernel de Linux llamado Netfilte, el cual proporciona funcionalidades de filtrado, marcado de tráfico y redireccionamiento.

Se implementa una red mediante máquinas virtuales montada en la aplicación VirtualBox para la configuración de cortafuegos, se utiliza dos máquinas con la siguiente característica.

Una máquina virtual en la cual está corriendo Ubuntu Desktop, la cual está configurada con una red intenta asociada a la una IP automática que se encuentra dentro las IP del servidor.

En la otra máquina virtual se encuentra montado Zentyal al cual se le asignaron dos redes, una red con adaptador de puente el cual dará acceso a internet y una red interna.

A continuación, se describe los pasos realizados para el proceso de configuración del cortafuegos.

Para realizar la validación de la funcionalidad del cortafuegos, en la siguiente imagen se muestra en ingreso a Facebook. Antes de definir la regla de filtrado (Figura 40).

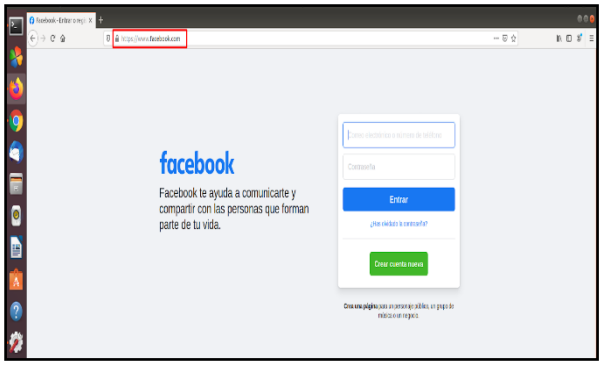

Figura 40. Verificación ingreso a Facebook antes de activar cortafuego.

Se da inicio al proceso de la configuración del cortafuego, en pantalla principal se ingresa por la opción cortafuegos como se resalta en la siguiente figura (Figura 41).

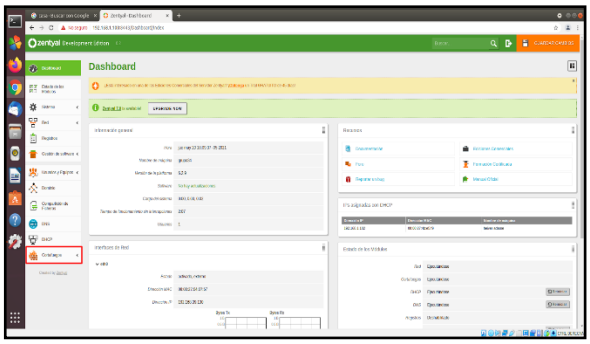

Figura 41. Inicio configuración cortafuego.

Tras ingresar a la opción cortafuegos, se muestra el pack de filtrados, para nuestra configuración se selecciona la regla de filtrado para rede interna como se resalta en la siguiente imagen, se da clic en configurar regla (Figura 42).

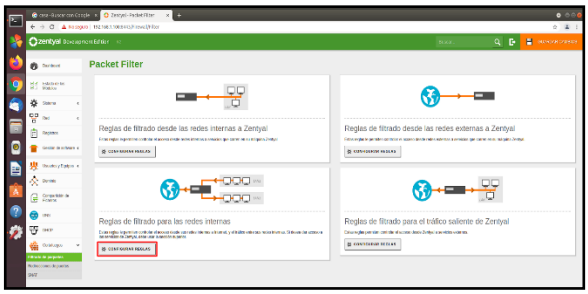

Figura 42. Selección del packet filter.

Luego se seleccionar el packet, se muestra la siguiente ventana en la cual se debe dar clic en el botón de añadir nueva regla (Figura 43).

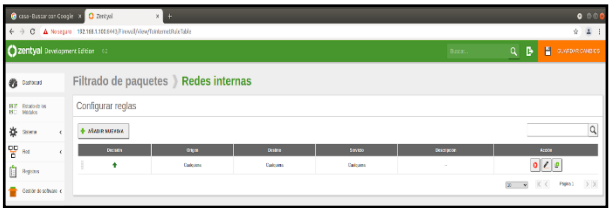

Figura 43. Crear nueva regla.

Para la creación de la regla se requiere la IP, En la siguiente imagen se muestra la IP para Facebook, mediante la utilización de comando nslookup y luego el dominio de la página (Figura 44).

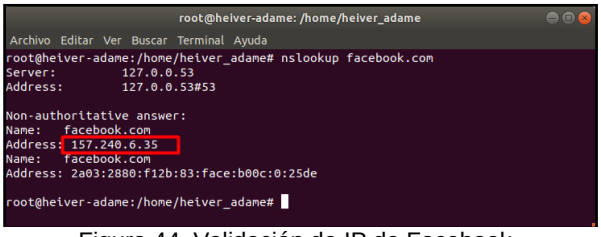

Figura 44. Validación de IP de Facebook.

A continuación, se ingresan los parámetros para configurar el cortafuegos en la página de Facebook, se indica denegar, si ingresa en la opción IP destino, la ip de la página Facebook la cual se consultó anteriormente, luego se indica que para cualquier servicio se da clic en añadir como se muestra en la siguiente imagen (Figura 45).

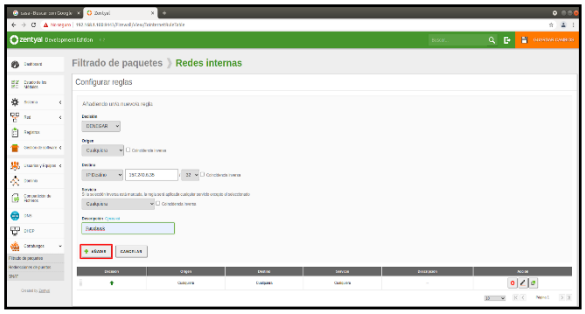

Figura 45. Regla de Cortafuego de Facebook.

Se muestra en la siguiente imagen que se creó la regla, para finalizar se da clic en guarda cambios en el botón naranja del parte superior derecho (Figura 46).

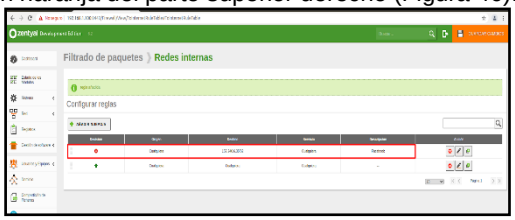

Figura 46. Validación de creación de cortafuego.

En la siguiente imagen se muestra el cuadro de dialogo donde de confirma el cambio de los datos (Figura 47).

Figura 47. Confirmación de los cambios.

Luego se intenta nuevamente ingresar a Facebook, y se puede evidencia que la configuración del cortafuego esta correcta, pues restringe el acceso a la página (Figura 48).

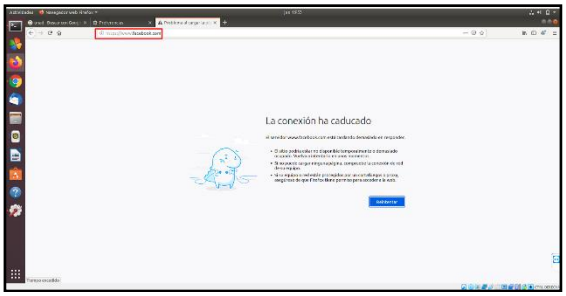

Figura 48. Cortafuegos para Facebook.

En la siguiente imagen se muestran la lista de reglas que se configuraron en el cortafuegos, para da una de la configuración se realiza el proceso de igual manera.

Se identifica la IP de dominio que será restringido (Figura 49).

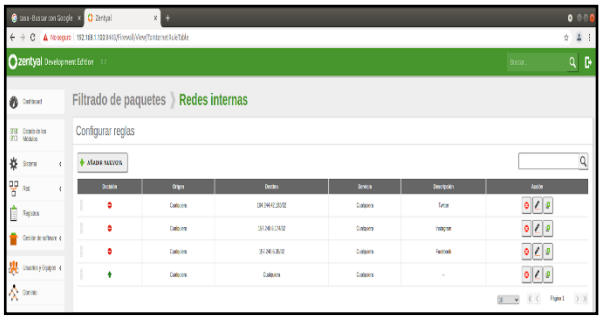

Figura 49. Reglas vigentes.

Tras realizar las configuraciones del cortafuegos, en la siguiente imagen se realiza la verificación que para otras páginas web se tiene acceso a internet sin ningún tipo de problema, para el caso ejemplo se ingresó a la página de la UNAD y a la página del periódico El tiempo, si ingresa sin ningún tipo de restricción permitiendo navegar en internet (Figura 50).

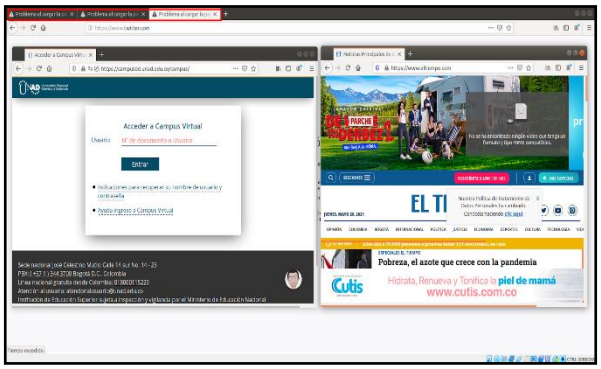

Figura 50. Validación de acceso a otros sitios Web.

3.4 FILE SERVER Y PRINT SERVER

3.4.1 File Server

Lo primero es verificar que en el apartado “Estado de los módulos” se encuentre habilitado el módulo “Controlador de Dominio y Compartición de Ficheros” (Figura 51).

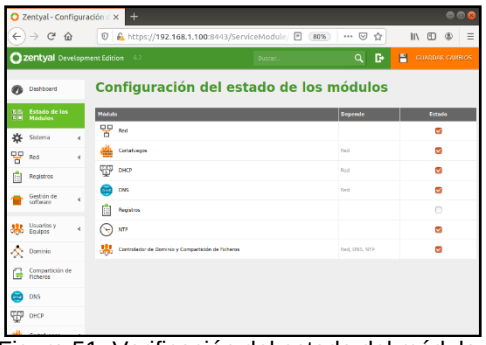

Figura 51. Verificación del estado del módulo.

Después de esto se ingresa a la opción Usuarios y Equipos > Opciones de configuración de LDAP, allí se habilita el PAM que permite que los usuarios que pertenecen al LDAP tengan cuenta en el sistema (Figura 52).

Figura 52. Habilitación PAM.

Ahora, en Usuarios y Equipos se crea el usuario con el que se harán las pruebas y se verifica que si se haya creado la carpeta en el home después de creado el usuario (Figuras 53 y 54) .

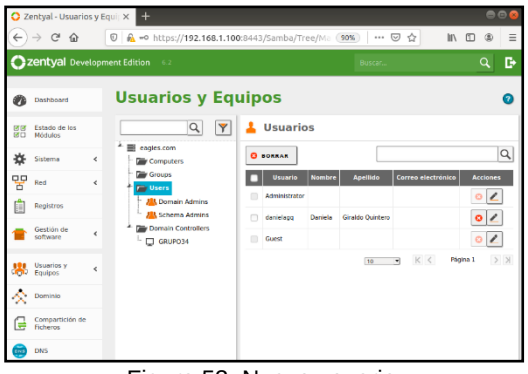

Figura 53. Nuevo usuario.

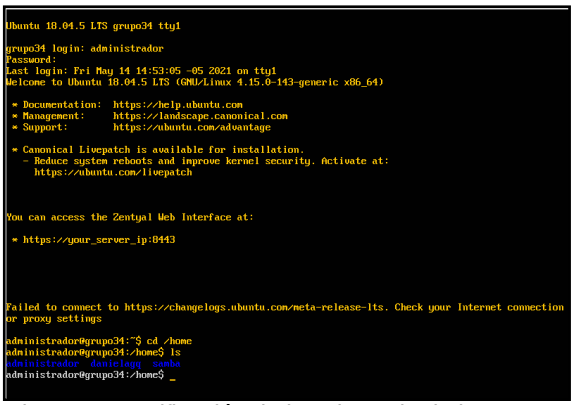

Figura 54. Verificación de la existencia de la carpeta /home/danielagq.

Al corroborar que el usuario quedó bien creado, se procede a compartir las carpetas, se inicia creando una carpeta en el home, la cuál será la raíz de las carpetas compartidas, además se le brindan todos los permisos con idea de que el usuario pueda realizar cambios allí (Figura 55).

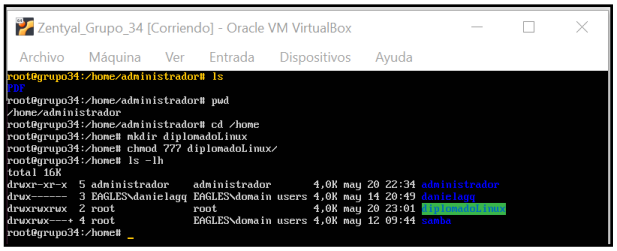

Figura 55. Creación de la carpeta compartida.

Desde el Ubuntu Desktop en el dashboard del Zentyal, se crea la carpeta compartida con los datos que se creó desde el servidor (Figura 56).

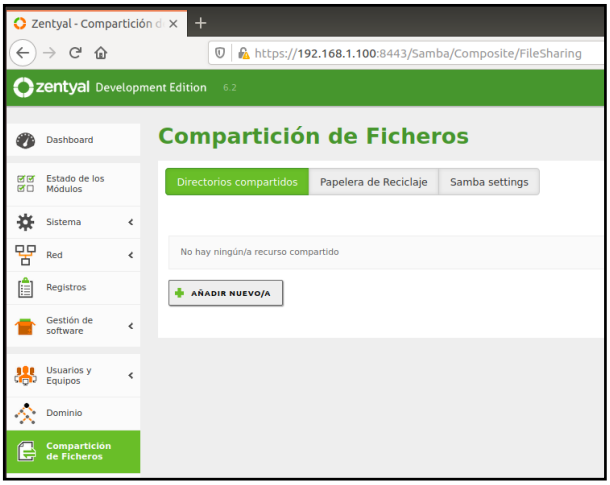

Figura 56. Compartición de ficheros Zentyal.

Se crea un nuevo directorio con el nombre que se desee, siempre y cuando la ruta sea de la carpeta creada en el servidor Zentyal y se guardan los cambios (Figuras 57 y 58).

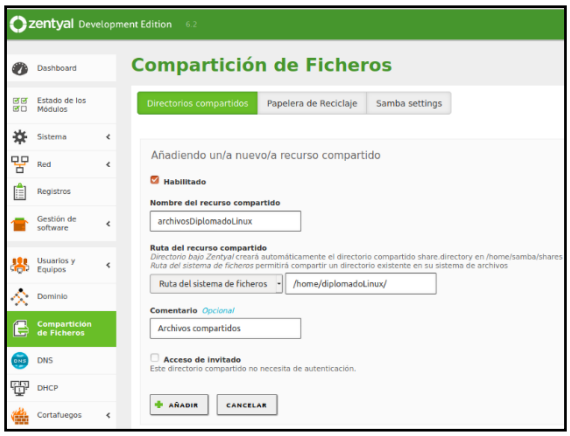

Figura 57. Nueva carpeta compartida.

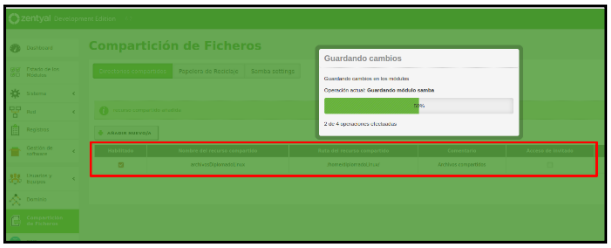

Figura 58. Guardando cambios.

Seguido de lo anterior se ingresa a la opción “Control de acceso”, se agrega el usuario que se creó inicialmente y de nuevo se guardan los cambios (Figuras 59 y 60).

Figura 59. Modificando el control de acceso.

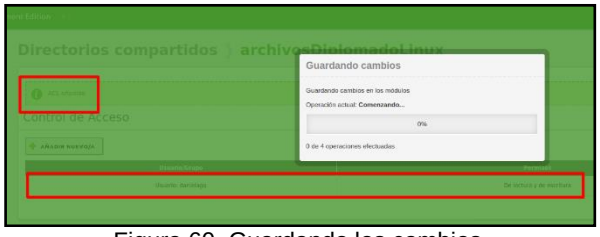

Figura 60. Guardando los cambios.

Ingresando desde el explorador de archivos se conecta al servidor (Figura 61).

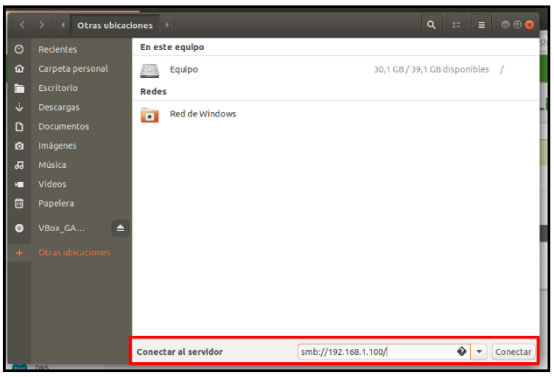

Figura 61. Ingresando al servidor.

Finalmente, allí se encuentra la carpeta creada (Figura 62).

Figura 62. Carpeta compartida.

Al ingresar se solicitan las credenciales y el dominio, luego de estar allí se puede demostrar que se puede leer y escribir en la carpeta compartida (Figuras 63 y 64).

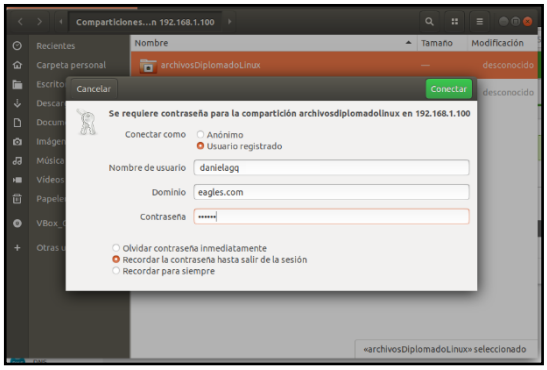

Figura 63. Crendenciales.

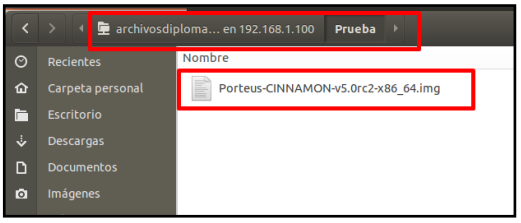

Figura 64. Creación de archivos dentro de la carpeta compartida.

Por último, se verifica en el servidor (Figura 65).

```
root@grupo34:/home# cd diplomadoLinux/
root@grupo34:/home/diplomadoLinux# ls
Prueba
root@grupo34:/home/diplomadoLinux# ls Prueba/
Porteus-CINNAMON-v5.0rc2-x86_64.img
root@grupo34:/home/diplomadoLinux#
```

Figua 65. Verificación de las carpertas creadas por el usuario.

3.4.2 Print Server

Lo primero será crear una impresora virtual. Para esto se instala cups-pdf, el comando a ejecutar es **apt-get install cups-pdf** (Figura 66).

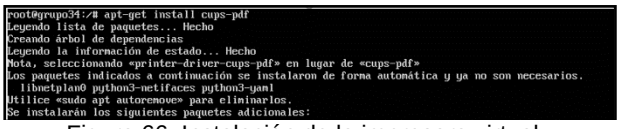

Figura 66. Instalación de la impresora virtual.

Ahora se realizan las verificaciones para corroborar que haya quedado instalada correctamente. Los comandos son los siguientes, con los cuales se revisa el estado de la impresora (Figura 67):

lpstat -a: Aceptación. Muestra si los destinos de impresión están aceptando solicitudes.

lpstat -p: Impresora/Descripción/Lista larga. Muestra el estado de las impresoras.

lpstat -v: Muestra los dispositivos.

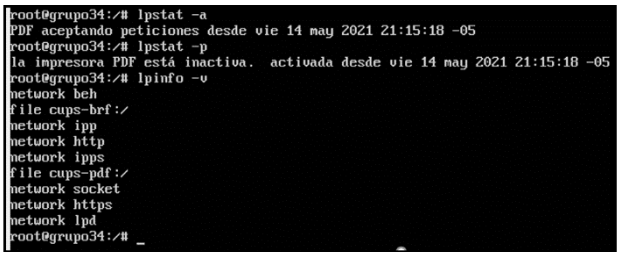

Figura 67. Estado de la impresora instalada.

Luego es necesario cambiar algunas configuraciones del archivo **/etc/cups/cupsd.conf** para que no escuche por localhost sino por la IP del servidor. Para realizar la modificación se ejecuta **nano /etc/cups/cupsd.conf**.

La línea a modificar es donde dice “Listen” se debe quitar la palabra “localhost” y poner la IP del servidor Zentyal (Figura 68).

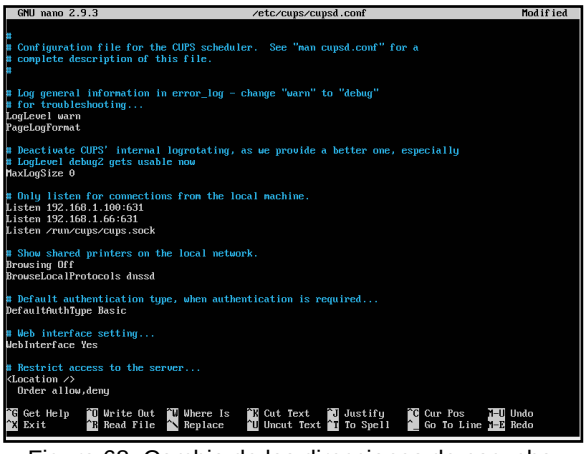

Figura 68. Cambio de las direcciones de escucha.

En ese mismo archivo es necesario configurar que se permita ingresar a la localización, ya que el cortafuegos que está habilitado así lo solicita (Figura 69).

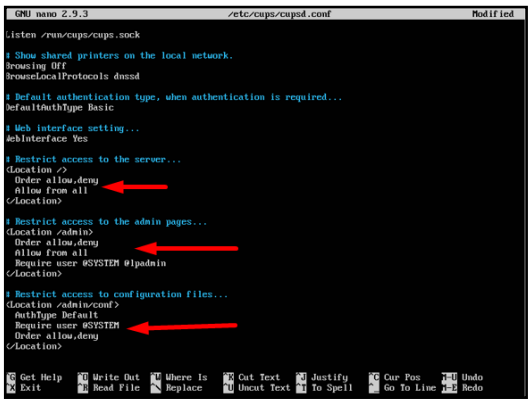

Figura 69. Brindando acceso.

Después de guardar, es necesario reiniciar el servicio cups.

En el Zentyal en la opción Cortafuegos > Filtrado de paquetes > Reglas de filtrado desde las redes internas a Zentyal, se da clic en “Configurar Reglas” (Figura 70).

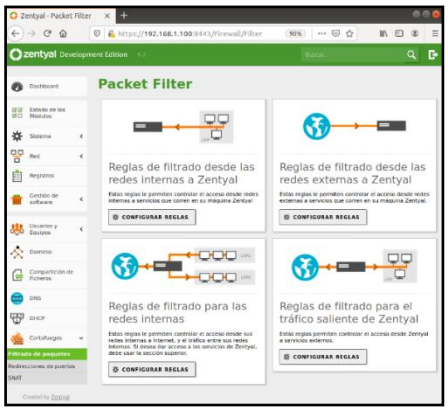

Figura 70. Reglas del cortafuegos.

Estando en la configuración de las reglas, se crea una nueva para el CUPS de la siguiente manera (Figuras 71, 72, 73 y 74).

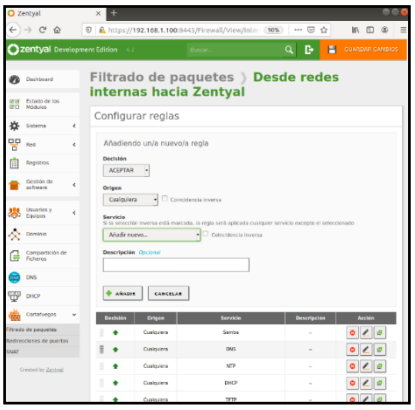

Figura 71. Crear nuevas reglas.

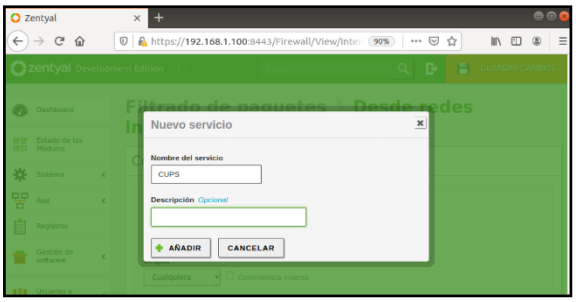

Figura 72. Datos básicos del nuevo servicio.

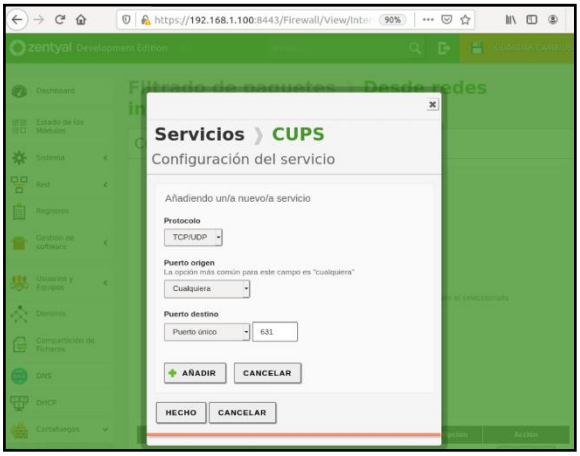

Figura 73. Datos específicos del nuevo sevicio.

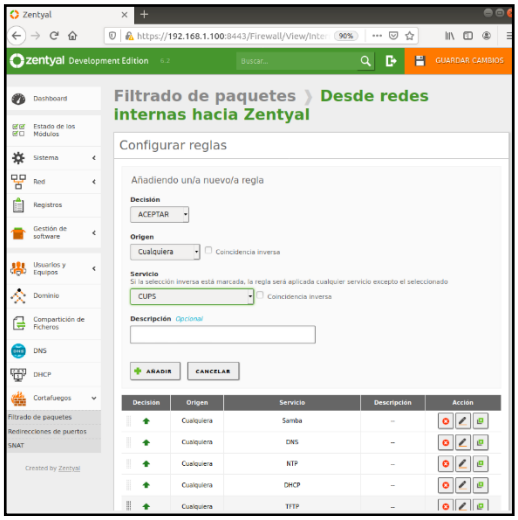

Figura 74. Listado de las reglas.

Ahora, desde el Ubuntu Desktop se ingresa al navegador a la IP que se configuró por el puerto 631. Allí se inicia la conifguración de la impresora así (Figuras 75, 76 y 77 y 78):

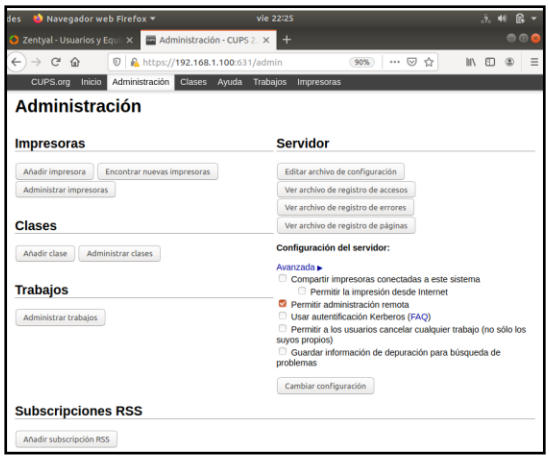

Figura 75. Agregar impresora.

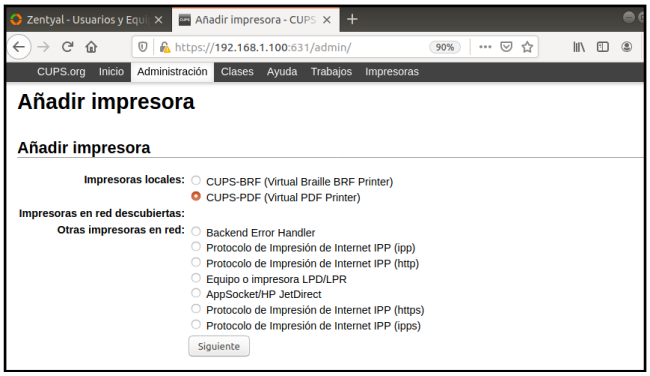

Figura 76. Configuración de la impresora.

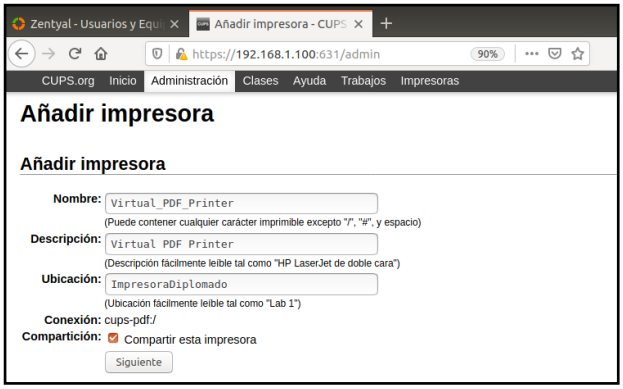

Figura 77. Configuración de la impresora.

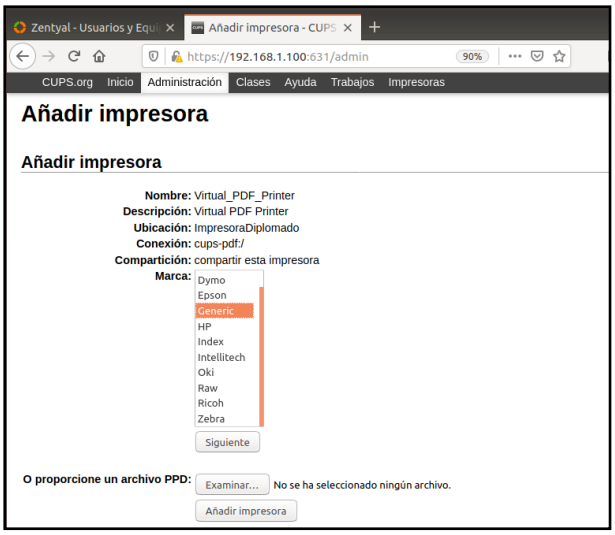

Figura 78. Configuración de la impresora.

Ahora es necesario verificar que aparezca en alguno de los clientes, puede ser en el Ubuntu Desktop (Figura 79).

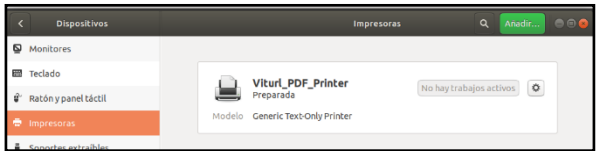

Figura 79. Impresora compartida.

3.5 VPN

La implementación y configuración de una VPN para establecer un túnel privado de comunicación requiere desde el servidor Zentyal tomar los paquetes adecuados para este, dentro de los cuales se destaca el Firewall, el certificado de autenticación y el paquete VPN.

Ingresando por el menú de VPN – Servidores, se crean los certificados de autoridad, empezando por el certificado del servidor, asignando un nombre y los días de expiración del mismo (figura 80).

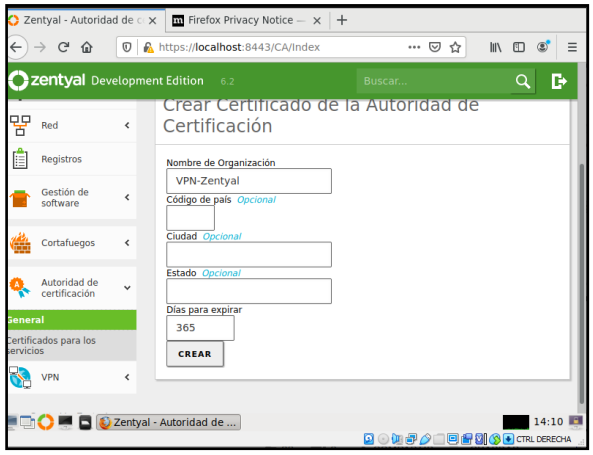

Figura 80. Certificado de autoridad.

En el equipo cliente, se realiza la conexión por medio de la dirección https//192.168.1.100:8443, allí se continúa con las demás configuraciones, por lo cual se realiza la configuración del rango de direcciones IP sobre las cuales está el equipo cliente (figura 81), cabe aclarar que deben ser superiores a las del equipo servidor.

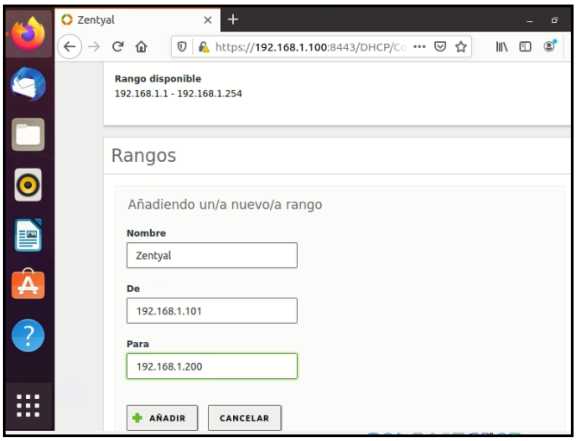

Figura 81. Rango de direcciones.

Con el rango de direcciones configurado, se crea el servidor asignando el nombre respetivo (figura 82).

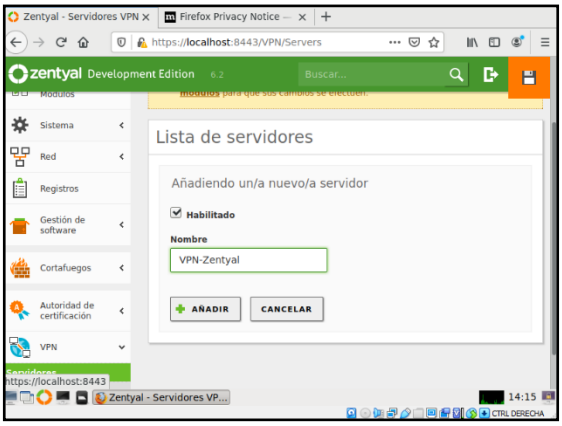

Figura 82. Asignación nombre de servidor.

Contiguo a ello se realiza la configuración del servicio (figura 83), en el cual se selecciona el protocolo UDP y el puerto de destino es el 1194.

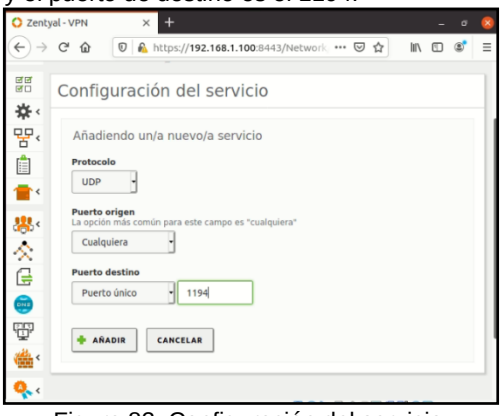

Figura 83. Configuración del servicio.

Con el servicio configurado, se procede a ingresar a través del menú de cortafuegos, donde se organizan las reglas de filtrado desde las redes internas a Zentyal y de las redes externas a Zentyal (figura 84), en ambas se realiza la misma configuración para aceptar todo tipo de navegación.

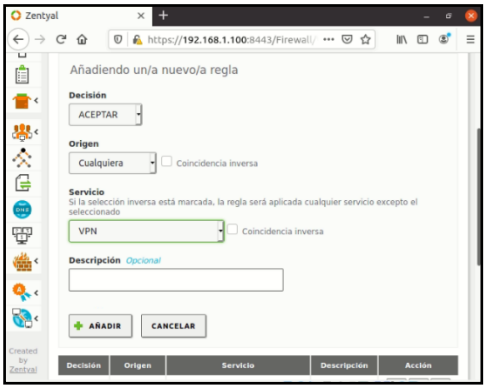

Figura 84. Configuración reglas de filtrado.

Luego, se guardan las configuraciones y en el servidor quedan guardados estos datos. Ahora se deben expedir los certificados para los clientes, puesto que cada uno debe contar con el certificado adecuado para no tener inconvenientes de la conexión (figura 85).

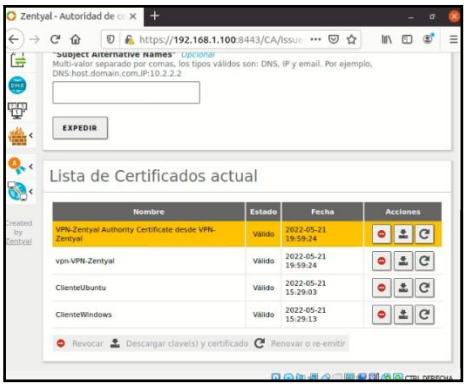

Figura 85. Certificados para cliente Ubuntu y Windows.

Con los certificados listos, se realiza la configuración del servidor (figura 86), en el cual se valida que el puerto es el adecuado y se habilitan la interfaz TUN y la conexión cliente-cliente, luego se guarda esta configuración.

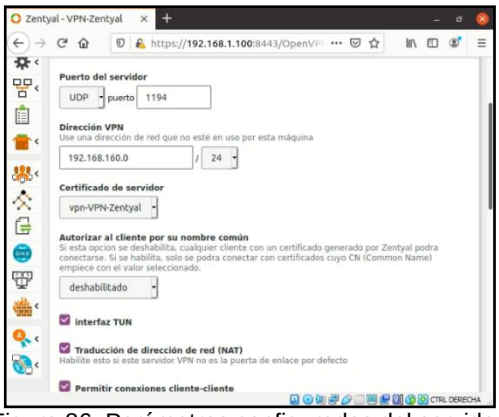

Figura 86. Parámetros configurados del servidor.

Con esta configuración realizada, se procede a realizar la descarga de los paquetes para el equipo cliente, en este caso del Cliente Ubuntu que se encuentra conectado a la red interna, conectado a una IP fija que se configura desde un inicio (figura 87). Cabe recalcar que debe apuntar a la dirección del servidor, además de asignarle el certificado adecuado.

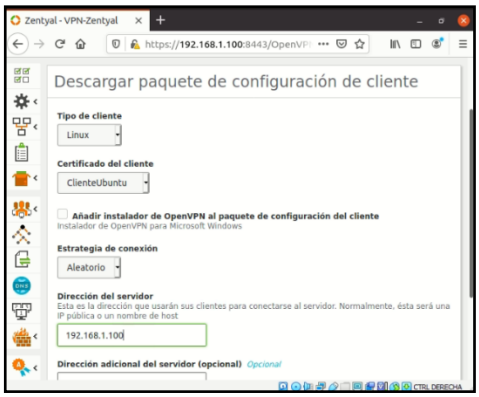

Figura 87. Configuración para descarga de paquete.

El paquete queda almacenado en la carpeta de descargas y se debe descomprimir. Ahora en la terminal del cliente, se valida con el comando apt-get -y install network-manager-openvpn que se encuentre instalado, además del ssh activo (ver figuras 88 y 89).

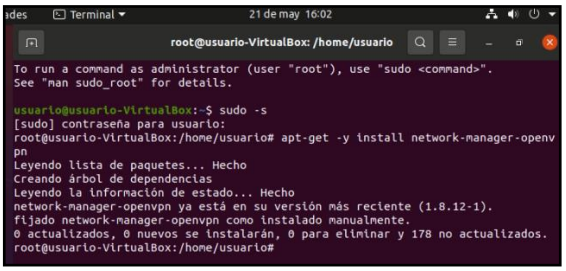

Figura 88. Instalación OpenVPN y SSH 1.

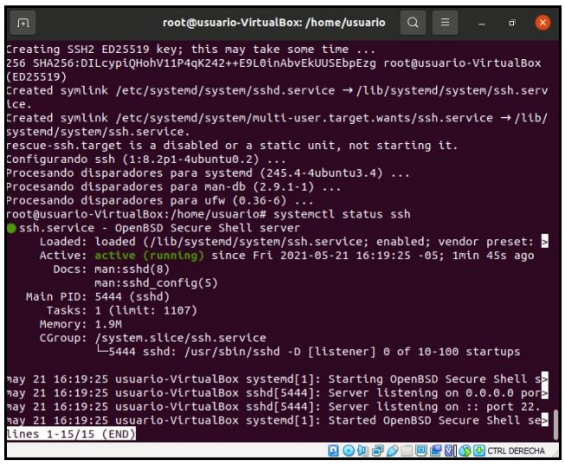

Figura 89. Instalación OpenVPN y SSH 2.

Luego por las configuraciones de red, se observa que la casilla de VPN no tiene nada configurado, por lo cual allí se agrega el archivo que se ha generado, teniendo en cuenta que debe agregarse el archivo con el formato .conf (figura 90).

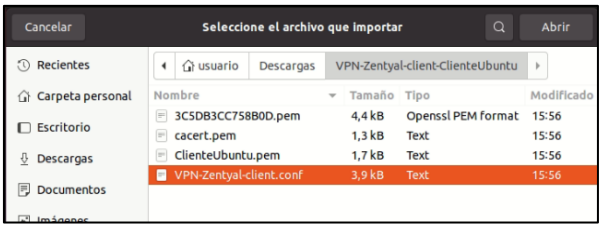

Figura 90. Archivo para configuración de red.

Luego se valida en las configuraciones que se haya cargado correctamente el archivo y luego al activar la VPN, sobre la parte superior derecha se observa la activación de la VPN a la cual se encuentra conectado (figura 91).

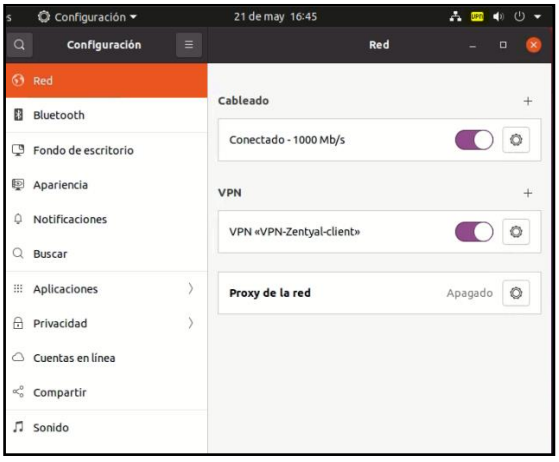

Figura 91. Activación de la VPN.

Se valida que adecuadamente se encuentra conectada a la VPN del archivo que se cargó (figura 92), donde se observa la IP configurada en el puerto 1194.

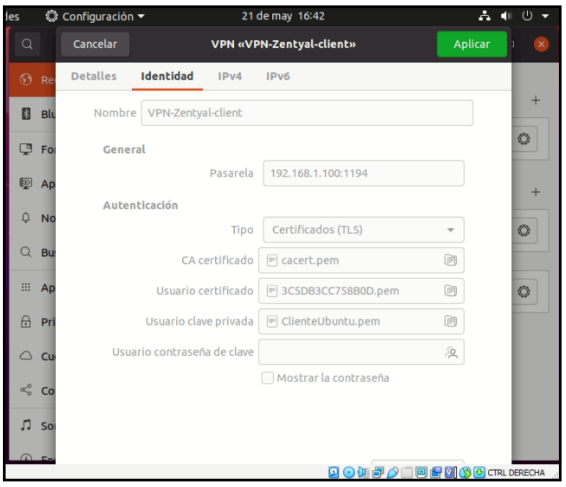

Figura 92. Comprobación de configuración.

Finalmente se realiza la prueba de conexión al sitio web de Google para mostrar que se encuentra funcionando de manera adecuada la VPN (figura 93).

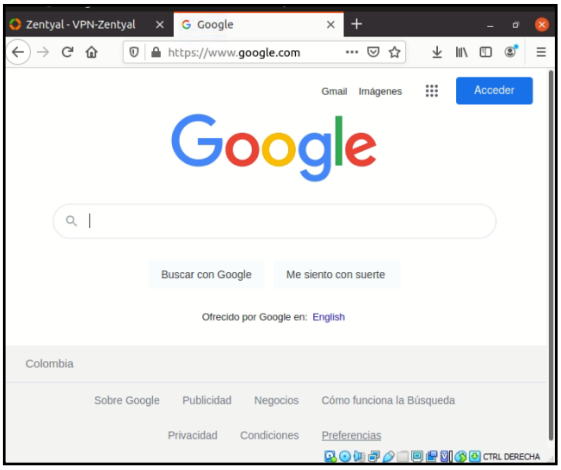

Figura 93. Comprobación de conexión.

4 CONCLUSIONES

1. El Dashboard de la herramienta tecnológica Zentyal, es sencilla intuitiva; sin embargo, para la configuración de alguna de sus utilidades se debe de tener conocimiento previo de la estructura lógica que estaba herramienta maneja para lograr los objetivos de control y seguridad.

2. Por otro lado, un aspecto importante a considerar es que en la configuración de Proxy de la red en el cuadro de texto ignorar anfitriones, se debe añadir la dirección IP del servidor.

3. Mediante la utilización de las configuraciones de cortafuegos se permite el administrar los recursos dentro de las diferentes organizaciones apoyando la toma de decisiones en la administración de redes internas.

4. La configuración del servidor de archivo proporciona a los usuarios un lugar de almacenamiento centralizado para los archivos en sus propios soportes de datos y brinda acceso únicamente a los recursos a los que el usuario puede gestionar.

5. El servidor de impresión logra que el usuario tenga acceso a las impresoras compartidas, sin perder la conexión al apagar el equipo.

6. Las redes VPN permiten crear redes locales sin la necesidad que los usuarios se encuentren conectados por un medio físico, además de brindar restricciones para la navegación de los usuarios y de que sea empleada como una extensión de red local (LAN), ofreciendo mayor seguridad por el cifrado de los paquetes de datos y garantizando que el flujo de datos de la red VPN no sea fácilmente leída por terceros.

5 REFERENCIAS

Documentación de Zentyal 6.2. Instalación. https://doc.zentyal.org/6.2/es/

Documentación de Zentyal 6.2. Servicio de Proxy HTTP. https://doc.zentyal.org/6.2/es/proxy.html

Documentación Zentyal 7.0. Configuración de cortafuego con Zentyal. https://doc.zentyal.org/es/firewall.html

Controlador de Dominio — Documentación de Zentyal 7.0. (s. f.). Zentyal.org. Recuperado 8 de mayo de 2021, de https://doc.zentyal.org/es/directory.html#

JRamos (2016). Controlador de dominio Active Directory sobre Linux Ubuntu. https://blog.ragasys.es/controlador-de-dominio-active-directory-sobre-linux-ubuntu

Servicio de configuración de red (DHCP) — Documentación de Zentyal 6.2. (s. f.). Zentyal.org. Recuperado 5 de mayo de 2021, de https://doc.zentyal.org/6.2/es/dhcp.html

Servicio de resolución de nombres de dominio (DNS) — Documentación de Zentyal 6.2. (s. f.). Zentyal.org. Recuperado 8 de mayo de 2021, de https://doc.zentyal.org/6.2/es/dns.html

Zentyal. Configurar Proxy Web HTTP No Transparente (2014). https://www.youtube.com/watch?v=PG7pcYmBkw4

Zentyal Community. Controlador de dominio. https://doc.zentyal.org/es/directory.html

Zentyal Community. Servicio de compartición de impresoras. https://wiki.zentyal.org/wiki/En/3.5/Printers_sharing_service

Zentyal Community. Virtual private network (VPN) service with OpenVPN. https://doc.zentyal.org/6.2/en/vpn.html