INSTALACIÓN Y CONFIGURACIÓN DE LINUX ZENTYAL SERVER PARA LA ADMINISTRACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT

Sebastian Ortega Ruiz
sortegar@unadvirtual.edu.co
Giancarlo Bedon Vinasco
gbedonv@unadvirtual.edu.co
Carlos Andrés Ruales Acosta
carualesa@unadvirtual.edu.co
Alan Fabián Patiño Jiménez
afpatinoj@unadvirtual.edu.co
Hector Fabio Ramos López
hframosl@unadvirtual.edu.co

RESUMEN: *El presente artículo desarrolla la instalación, configuración y puesta en marcha de un servidor Zentyal en su versión 7.0, emulando una red empresarial, donde se consideran las zonas roja, naranja y verde que son conocidas como la zona de internet, zona desmilitarizada y zona local respectivamente. Se instalarán y se pondrán en marcha módulos que provee Zentyal para el uso de cortafuegos, DHCP, Proxys, entre otros. El artículo se divide en las temáticas, en donde cada una abordará la configuración y puesta en marcha de cada servicio.*

PALABRAS CLAVE: Controlador de Dominio, Cortafuegos, Proxy, VPN, Zentyal Server.

1 INTRODUCCIÓN

En el presente artículo se trabajará en la instalación del sistema operativo Linux Zentyal Server el cual es una distribución GNU/Linux basada en Ubuntu, mediante el cual se realizará la implementación de los siguientes servicios: DHCP, DNS, Controlador de dominio, Proxy no transparente, Cortafuegos, File server, Print server y VPN, permitiendo así el desarrollo de las temáticas planteadas en la actividad, evidenciando su correcto funcionamiento y permitiendo ver la importancia para la administración de servicios de infraestructura IT.

2 INSTALACIÓN Y CONFIGURACIÓN DE LINUX ZENTYAL SERVER

Para realizar la instalación es necesario realizar la descarga de la imagen de Zetyal Server del siguiente link https://zentyal.com/community/, del que se obtiene el archivo zentyal-7.0-development-amd64.iso.

Es necesario crear una nueva máquina virtual en virtual box que deberá tener las siguientes configuraciones, ver Figura 1.

Figura 1. Configuración máquina virtual.

Se inicia la máquina virtual, se selecciona el idioma de instalación. En la Figura 2 se debe seleccionar el tipo de instalación a realizar “Install Zentyal 7.0-Development (delete all disk)”

Figura 2. Selección tipo de instalación Zentyal Server.

Se inicia la instalación, se solicita seleccionar la zona horaria, distribución del teclado, distribución de las teclas y selección de la interfaz de red primaria que debe corresponder a la interfaz de red configurada en virtual box como adaptador puente, ver Figura 3.

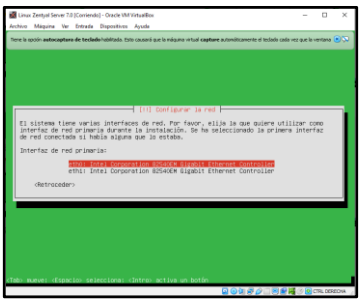

Figura 3. Selección interfaz de red primaria.

Se debe ingresar el nombre de la máquina, el nombre del usuario administrador, luego como se observa en la Figura 4 se ingresa la contraseña de ingreso al sistema operativo.

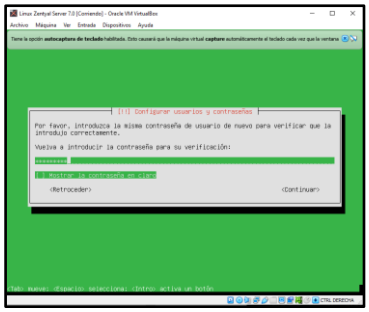

Figura 4. Ingreso de contraseña usuario administrador.

Se finaliza la instalación de manera exitosa, a continuación, se reinicia la máquina virtual dando inicio al sistema operativo Linux Zentyal Server instalado, ver Figura 5.

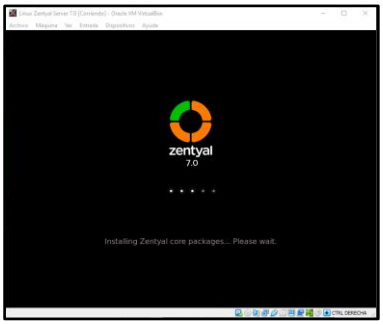

Figura 5. Arranque de Linux Zentyal Server.

Se finaliza el arranque del sistema operativo y se debe ingresar el usuario y contraseña ingresados en la instalación, ver Figura 6.

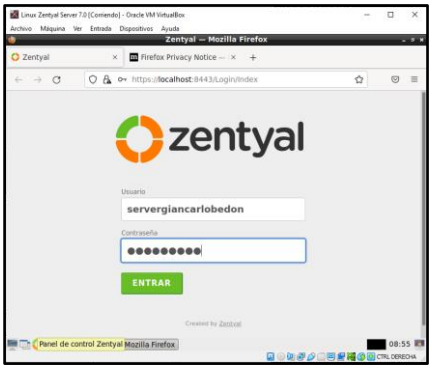

Figura 6. Login de Linux Zentyal Server.

Al ingresar se inicia la configuración inicial de Zentyal, En la Figura 7 se solicita los paquetes a ser instalados, se van a seleccionar: Domain controller and file sharing, DNS server, DHCP Server, Firewall, VPN y Http Proxy. Dando luego clic en instalar para iniciar con el proceso de instalación de los paquetes seleccionados.

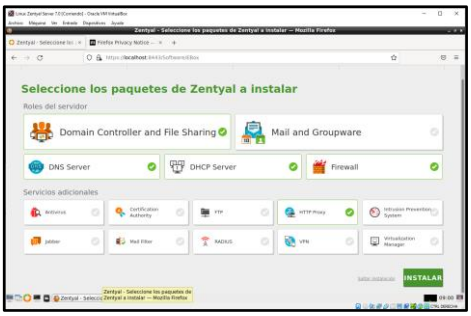

Figura 7. Selección paquetes a instalar en Zentyal Server.

Se finaliza el proceso de instalación de paquetes y se debe proceder a configurar los métodos para las interfaces de red detectadas por la instalación, ver Figura 8.

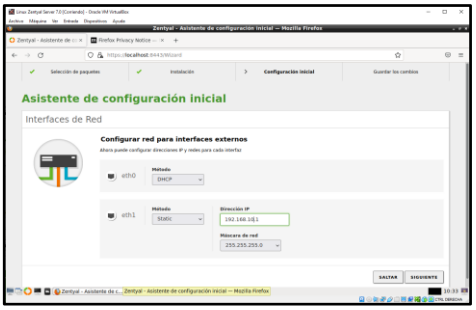

Figura 8. Selección método interfaz eth1.

Luego se ingresa el nombre del dominio para el servidor, se da clic en finalizar y se debe aceptar los cambios realizados para finalizar la configuración inicial de Linux Zentyal Server, ver Figura 9.

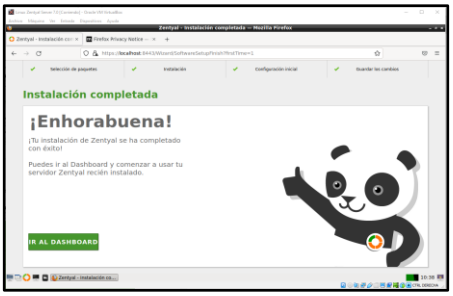

Figura 9. Instalación completa Linux Zentyal Server

En la figura 10 se muestra el dashboard inicial del sistema operativo Linux Zentyal Server.

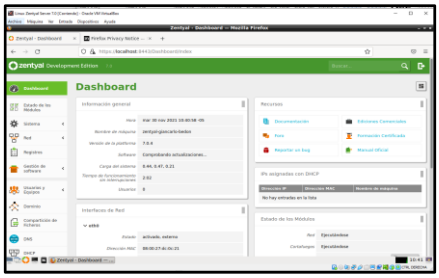

Figura 10. Dashboard inicial de Linux Zentyal Server

3 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

3.1 DHCP SERVER

Para configurar el servicio DHCP se busca el módulo en el menú lateral izquierdo y se da clic en el botón de configuración de la interfaz de red que se usará para proveer direcciones IP. En la figura 11 se observa la ruta al módulo y a la interfaz de red disponible para el servicio.

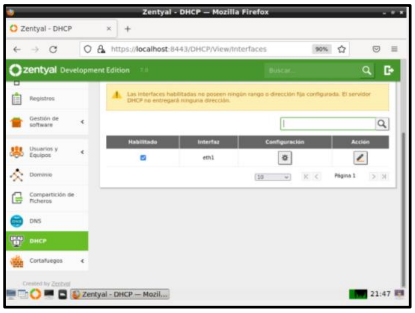

Figura 11. Módulo de DHCP

En la figura 12 se muestra como al ingresar a configuración en la pestaña de opciones personalizadas se debe elegir a Zentyal como la puerta de enlace, dominio de búsqueda y servidor DNS primario.

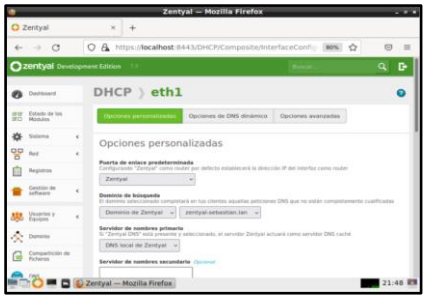

Figura 12. Opciones personalizadas DHCP

Luego se desplaza hacia abajo en la pestaña de opciones personalizadas y se selecciona Zentyal como servidor NTP, la figura 13 muestra cómo se ingresan los rangos de direcciones IP para asignación a los clientes.

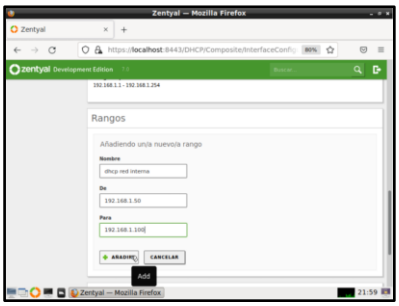

Figura 13. Ingreso de rangos de direcciones IP para la asignación por DHCP en los clientes

La figura 14 muestra los botones a los que se debe dar clic para añadir y guardar los cambios y aplicar la configuración realizada.

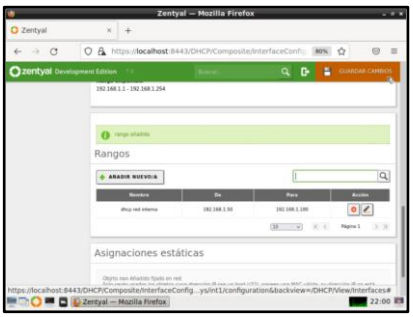

Figura 14. Guardar cambios de configuración DHCP

En un equipo cliente con Linux Ubuntu se ingresa a la configuración de la red cableada, en la pestaña IPV4 se selecciona que la configuración es automática por DHCP, DNS automático y se da clic en aplicar. La figura 15 muestra la configuración realizada en la tarjeta de red.

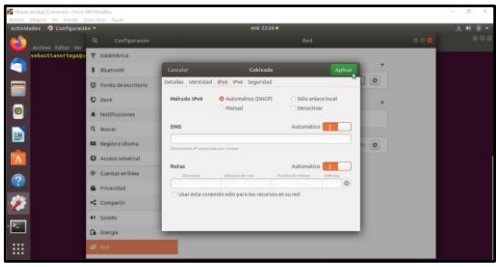

Figura 15. Configuración de red en equipo cliente con Linux Ubuntu

A continuación, se debe ingresar en una terminal y se ejecuta el comando ifconfig -a, en la figura 16 se comprueba que la dirección IP asignada se encuentra dentro del rango configurado en el servicio DHCP del servidor.

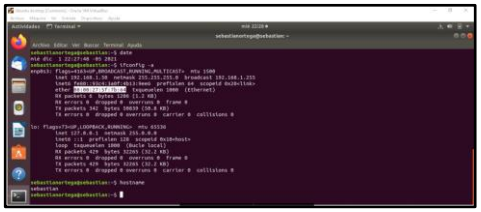

Figura 16. Comprobación de asignación dirección IP en equipo cliente con Linux Ubuntu

3.2 DNS SERVER

Para configurar el DNS Server, se debe tener en cuenta que este servicio lo provee automáticamente Zentyal Server cuando configuramos el servicio DHCP, sin embargo, para obligar a los clientes a usar Zentyal como su servidor de nombre de dominios se deberá activar la opción cache de DNS transparente, en la figura 17 se observa cómo se ingresa al módulo de DNS, se activa la casilla correspondiente y se configura el servidor DNS de Google 8.8.8.8 como posible redireccionador

para responder peticiones que Zentyal no pueda responder..

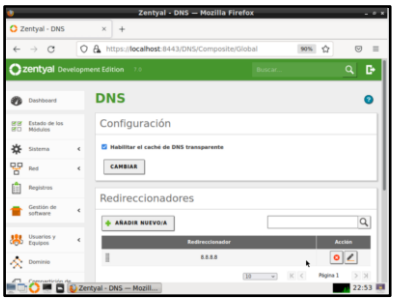

Figura 17. Configuración de DNS

Una vez se termine la configuración se da clic en cambiar y luego en guardar cambios en el servidor para que se aplique la configuración.

Una vez configurados los servicios se debe proveer internet a los clientes, en la figura 18 se muestra la ubicación del módulo de red y las interfaces, en la tarjeta de red que recibe internet se selecciona el método de puente de red y se da clic en cambiar para que aparezca la nueva pestaña con el adaptador virtual.

Figura 18. Configuración interfaz de red primaria

La figura 19 muestra cómo se despliega la nueva pestaña de adaptador puente que se debe configurar por DHCP y se da clic en cambiar.

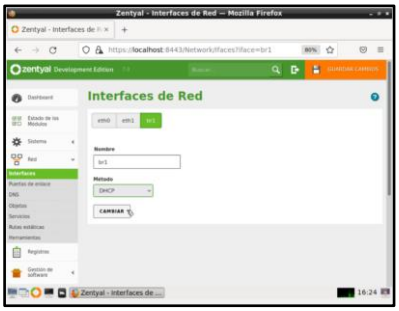

Figura 19. Configuración interfaz de red DHCP

Por último, se da clic en guardar los cambios para que se aplique las configuraciones realizadas, en la figura 20 se observan los cambios aplicándose a las interfaces de red.

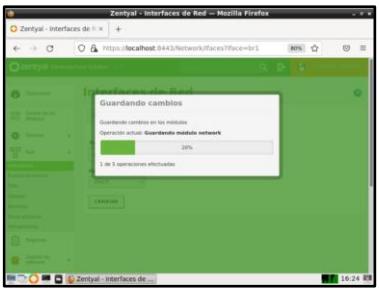

Figura 20. Guardar configuración

Ahora se debe ingresar al equipo cliente al cual se le realizo la configuración de dirección IP por DHCP y en una terminal se valida que se tenga salida a internet haciendo un ping a google.com. La figura 21 muestra la dirección IP asignada por DHCP y el dominio Google.com respondiendo la conexión.

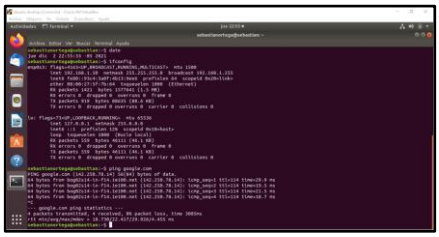
Figura 21. Validación de conexión a internet en equipo cliente con Linux Ubuntu

3.3 CONTROLADOR DE DOMINIO

Para configurar el controlador de dominio stand-alone en Zentyal Server, se debe dar clic en el menú lateral izquierdo en el módulo de dominio, configurar el nombre de dominio y guardar los cambios. La figura 22 muestra cómo se elige la función del servidor como único controlador de dominio

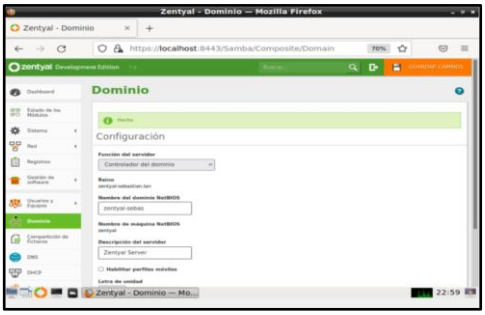

Figura 22. Configuración nombre de dominio

El siguiente paso es crear un usuario que será el administrador del dominio, la figura 23 muestra la ruta y contenido del módulo de usuario y equipos.

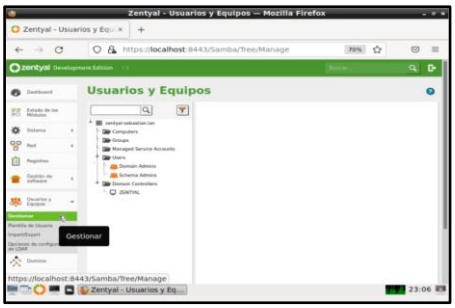

Figura 23. Configuración de usuarios y equipos

Se selecciona la carpeta Users y se da clic en el icono (+) para agregar un nuevo usuario, se despliega un formulario, se debe ingresar los datos para el usuario administrador, en la opción de grupo se elige Domain Admins y se da clic al botón Añadir. En la figura 24 se observa la creación de las credenciales del usuario administrador de dominio.

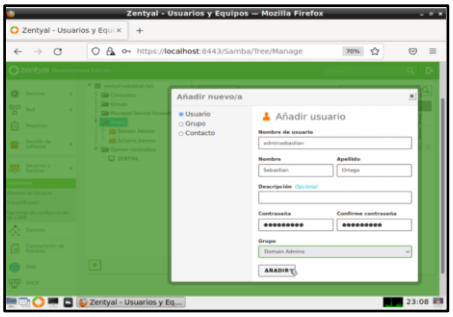

Figura 24. Añadir usuario administrador de controlador de dominio

La figura 25 muestra el mismo proceso para crear un usuario cliente que accederá al dominio a través de una cuenta con autenticación desde el equipo cliente con Linux Ubuntu, este usuario no se añade a ningún grupo.

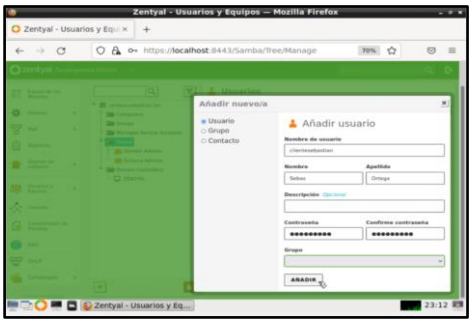

Figura 25. Añadir usuario cliente para acceso a dominio

Al finalizar la configuración se debe ingresar al equipo cliente con Linux Ubuntu y descargar la aplicación Pbis-open (PowerBroker Identity Services) que permite unir una máquina GNU/Linux a un dominio con los usuarios del directorio activo del controlador de dominio para compartición en red de recursos y servicios. Se descarga con wget https://github.com/BeyondTrust/pbis-open/releases/download/8.7.1/pbis-open-8.7.1.494.linux.x86_64.deb.sh se dan permisos de ejecución al archivo. La figura 26 muestra el proceso de instalación.

Figura 26. Instalación de la aplicación Pbis-open en equipo cliente con Linux Ubuntu

Al finalizar la instalación se indica un ejemplo de cómo unirse a un dominio. La figura 27 muestra cómo usando el ejemplo se ingresan las credenciales del dominio y el usuario con permisos admin que se ha creado para acceder al dominio. Primero se ubica en la ruta que se específica y se une al dominio con el comando: domainjoin-cli join zentyal-sebastian.lan adminsebastian.

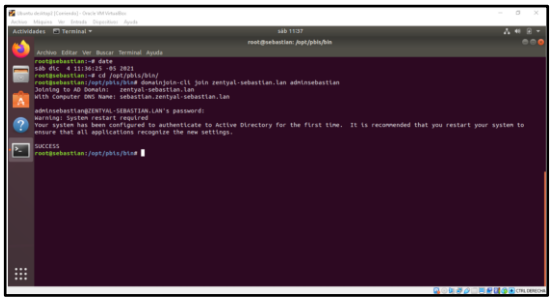

Figura 27. Configuración de conexión al dominio en equipo cliente con Linux Ubuntu.

A continuación, se solicita que se reinicie la máquina cliente, al iniciar la máquina se debe editar el archivo 50-ubuntu.conf para indicarle a Ubuntu que permita el Login de los usuarios creados en el directorio activo. La figura 28 muestra las líneas de código que debe contener el archivo.

Figura 28. Activación de login a usuarios creados en el directorio del control de dominio en Zentyal.

Por último, se debe especificar el Shell de los usuarios del dominio para que permita el login y reiniciar. La figura 29 contiene el código que debe usarse para finalizar la configuración del cliente.

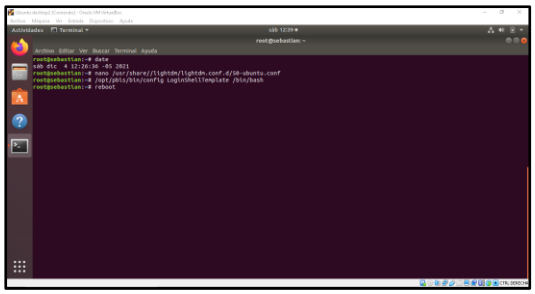

Figura 29. Especificación del Shell

Al iniciar la máquina cliente nuevamente se puede realizar el login con las credenciales de los usuarios creados para el dominio. En la figura 30 se observa al usuario administrador logueado desde el Linux Ubuntu.

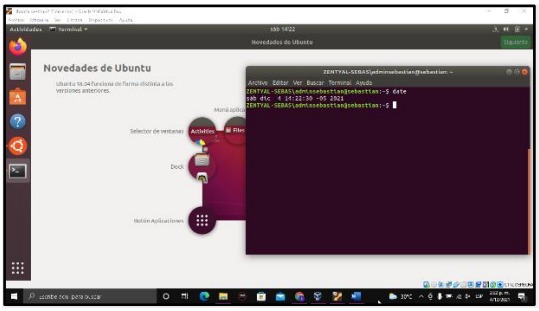

Figura 30. Login en equipo cliente con usuario administrador de dominio.

El servidor Zentyal ofrece una alternativa Linux a los servidores Windows, su principal ventaja es la facilidad con la que permite gestionar los servicios de dominio y directorio típicos a un dominio Windows gracias a la implementación nativa de los protocolos de directorio activo de Microsoft. [1]

Con dos tarjetas de red como mínimo en el servidor se consigue tener un controlador de dominio sobre un sistema GNU/Linux en el que se pueden administrar cuentas tanto de otros sistemas Linux como de sistemas Windows que podrán acceder al dominio desde cualquier computador de la red con sus respectivas credenciales creadas en el directorio activo y podrán compartir recursos de red de manera más eficiente y controlada.

4 TEMÁTICA 2: PROXY NO TRANSPARTENTE

4.1 CONFIGURACIÓN PROXY HTTP

Para configurar el servicio de HTTP Proxy se debe crear primero un objeto como parte de la red para referenciar nuestra máquina cliente con Ubuntu. Para esto se va a dar cliente en el menú lateral izquierdo en red, luego en objetos y se debe añadir uno nuevo.

La configuración y la instalación fue realizada mediante la documentación que se encuentra en la siguiente cita [2].

En la Figura 31 se observa que se ingresa el nombre del objeto de red a ser añadido.

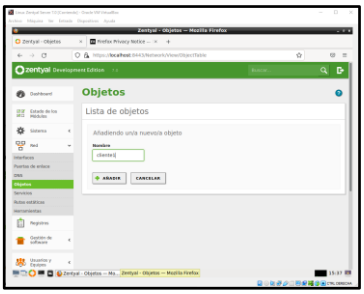

Figura 31. Añadir objeto de red.

Luego se da clic en añadir y guardar los cambios para que se aplique la configuración realizada. A continuación, en la Figura 32 se debe crear un miembro para el objeto para lo cual se da clic en configurar y se añade un nuevo miembro.

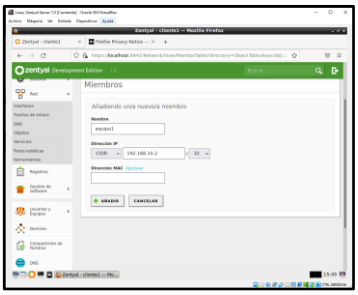

Figura 32. Añadir miembro al objeto de red.

Al añadir el miembro se debe dar clic en guardar los cambios para que la configuración quede aplicada, ver Figura 33.

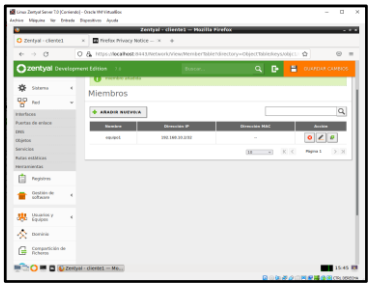

Figura 33. Guardar cambios en miembro agregado.

El siguiente paso es dar clic en el menú lateral izquierdo en el módulo Proxy HTTP, luego en configuración general, En la Figura 34 se observa el dónde se cambia la asignación del puerto al 1230 y se da clic en cambiar.

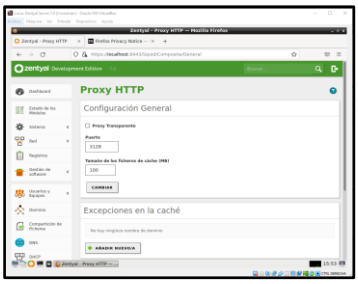

Figura 34. Configuración general Proxy HTTP.

A continuación, se inicia la maquina cliente con Ubuntu y se le configura la red estática con ip 192.168.10.2 para esto se debe tener la interfaz de red como red interna, ver Figura 35.

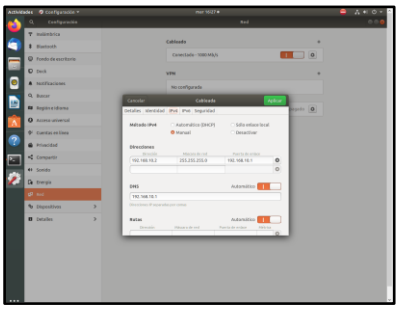

Figura 35. Configuración de red en equipo cliente con Linux Ubuntu.

Ahora se debe ingresar a un navegador web como el Firefox y se debe ingresar a configurar como servidor proxy para peticiones http y https la ip 192.168.10.1 por el puerto 1230 que corresponde al servicio Proxy HTTP configurado en el Linux Zentyal Server, ver Figura 36.

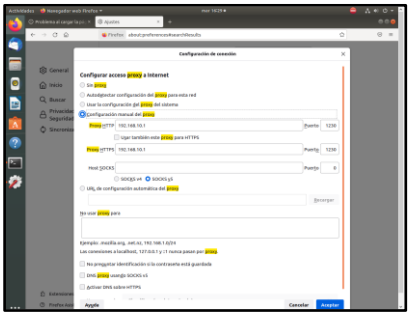

Figura 36. Configuración de Proxy HTTP en Firefox en el equipo cliente con Linux Ubuntu.

En la Figura 37 se observa la prueba realizada de navegación al dominio www.google.com.co, y se podrá evidencia como carga correctamente la página web indicada, lo cual indica que las políticas del Proxy HTPP se encuentran permitiendo toda la navegación desde el equipo cliente.

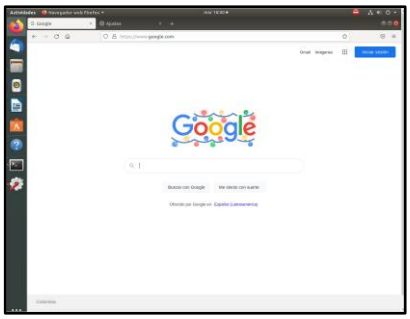

Figura 37. Validación de navegación a través de proxy en el equipo cliente con Linux Ubuntu.

A continuación, en el servidor con Zentyal Server se valida la regla de acceso en el servicio Proxy Http y se observa que para el cliente1 creado esta como permitir todo, por lo cual podemos navegar sin ninguna restricción, para cambiar la regla se da clic en edición y se da clic en denegar todo para el cliente1, ver Figura 38.

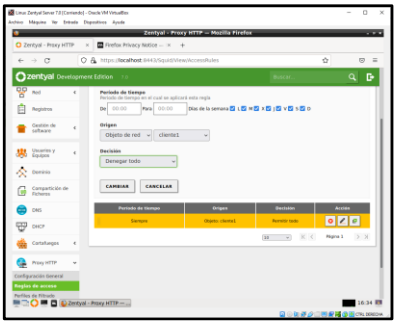

Figura 38. Edición de regla de acceso para el cliente1.

A continuación, se da clic en cambiar y guardar los cambios para aplicar la configuración realizada, ver Figura 39.

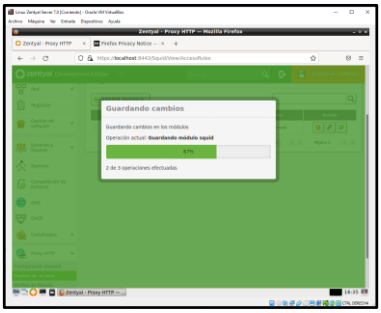

Figura 39. Aplicar cambios en edición regla de acceso.

Al finalizar de aplicar los cambios, se ingresa nuevamente al equipo cliente con Linux Ubuntu, en la Figura 40 se realiza la misma prueba de intentar ingresar a www.google.com.co, y se podrá evidenciar cómo se restringe ya el acceso por el servidor proxy instalado en Zentyal Server.

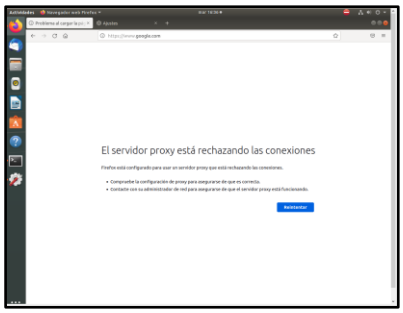

Figura 40. Validación de navegación en equipo cliente con denegación de acceso.

A continuación, se vuelve a configurar nuevamente en el servidor en las reglas de acceso que permita nuevamente todo para el cliente 1.

Luego se va a crear una lista de páginas con acceso bloqueado, se debe seleccionar la opción dentro del módulo Proxy HTTP perfiles de filtrado, se da clic en añadir nuevo y se ingresa un nombre para el perfil, ver Figura 41.

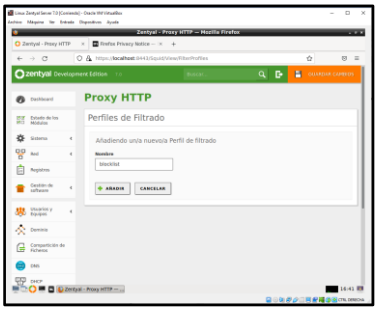

Figura 41. Añadir perfil de filtrado.

Se podrá visualizar como el perfil es añadido correctamente, luego se va a dar clic en configuración, posterior a esto se da clic en reglas de dominios y URLs, y se va a dar clic en añadir uno nuevo donde se debe indicar el nombre del dominio y seleccionar la opción de denegar acceso.

Se debe tener en cuenta que este módulo se podrá adicionar las URLs a las cuales se quiere que los equipos clientes no tengan acceso.

En la Figura 42 se observa que se adiciona la URL faceebook.com a las reglas de dominios y URLs.

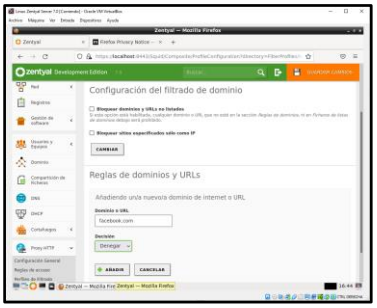

Figura 42. Añadir URL facebook.com al perfil.

Se da clic en añadir y se guardan los cambios para que sea aplicado el nuevo filtro adicionado en el servicio Proxy HTTP.

Ahora se debe ir a la regla de acceso que tiene nuestro cliente1 se le debe indicar que aplique el filtrado creado blocklist, ver Figura 43.

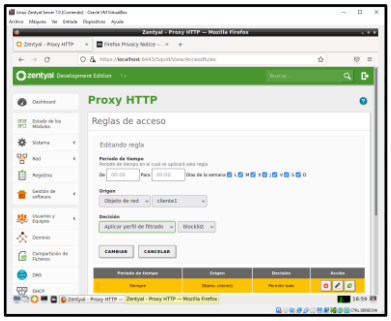

Figura 43. Configurar regla de acceso para que aplique filtrado.

Se da clic en cambiar y guardar los cambios para que sea aplicada la configuración realizada, al finalizar la configuración se ingresa al equipo cliente con Linux Ubuntu, en la Figura 44 se ingresa a un navegador y se intenta ingresar al dominio de facebook.com y se podrá observar que este se encuentra bloqueado por el proxy, pero si se ingresa al dominio de outlook.com si permite navegar sin ninguna restricción.

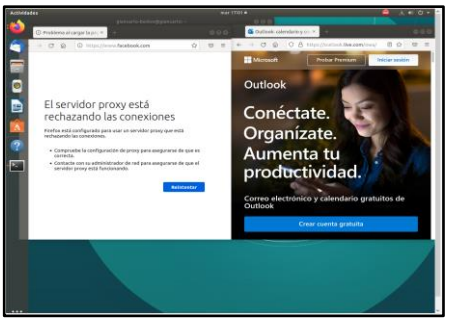

Figura 44. Añadir URL facebook.com al perfil.

Al finalizar la validación se logra observar que al cliente se le es restringido el acceso a la página facebook.com, pero a otros dominios como el de outlook.com si se le permite navegar sin ninguna restricción.

4.2 CASOS DE USO

En la actualidad los servicios de Proxy HTTP son comúnmente utilizados en las diferentes organizaciones, porque este les permite realizar el control de acceso y filtrado de contenido que todos los clientes de la red realizan hacía internet, de esta manera las organizaciones bloquean el acceso a páginas web o aplicaciones como Facebook, Instagram, Twitter, Youtube y otras muchas más, evitando así que los colabores durante su horario laboral ingresen a estos sitios que pueden ocasionar distracción en las labores a realizar.

4.3 VENTAJAS

Permite controlar y filtrar todo el tráfico de la red hacía internet por el administrador del servicio.

El administrador del servicio puede denegar el acceso a los clientes a dominios que la organización considere que no son necesarios para las labores que se realizan día a día.

El administrador del servicio puede denegar a los clientes de la red ingresen a sitios web que pueden ser peligrosos, como puede ser que contengan malware, enlaces de suplantación de identidad, evitando así que haya fuga de información. [3]

Un servidor proxy puede almacenar datos en caché lo cual se reduce a que las páginas se muestren con mayor velocidad al tener información de ella guardada en cache. [4]

5 TEMÁTICA 3: CORTAFUEGOS

Zentyal provee un módulo de cortafuegos que funciona bajo Netfilter, este proporciona labores de filtrado, redirección, denegación y aceptación de paquetes, entre otros.

La configuración y las máquinas que intervienen se utilizan de la siguiente manera:

- Servidor Zentyal 7.0, basado en Ubuntu server con configuración de dos tarjetas de red, una para la zona roja con DHCP y otra para la zona verde con IP estática 192.168.0.10
- Máquina cliente, con Ubuntu desktop, con zona verde configurada con la IP 192.168.0.20 con puerta de enlace 192.168.0.10

Se debe instalar el módulo de cortafuegos, para trabajar con la configuración que este provee, ver Figura 45.

Figura 45. Módulo de cortafuegos

En la Figura 46 y Figura 47 se debe revisar y configurar las interfaces de red que intervienen en el proceso de filtrado. En este caso la interfaz eth0 corresponde a la zona roja y la interfaz eth1 corresponde a la zona verde.

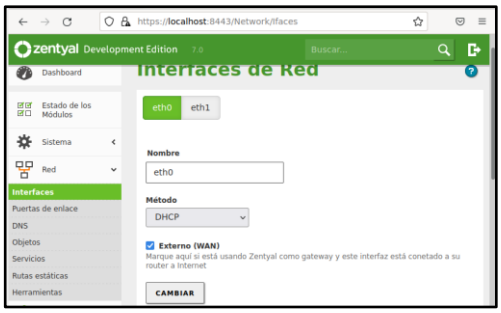

Figura 46. Configuración interfaces de red eth0

Figura 47. Configuración interfaces de red eth1

Lo siguiente es verificar la máquina de Ubuntu desktop para revisar la configuración de las tarjetas de red a través del comando ifconfig, ver Figura 48.

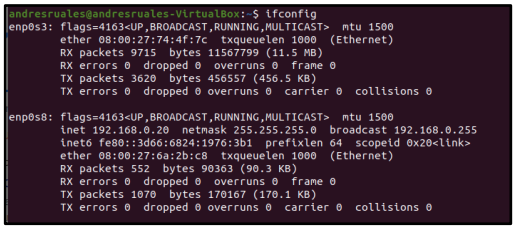

Figura 48. Configuración interfaces de red Ubuntu desktop

Se verifica que se tiene acceso a internet por medio de un ping a un sitio web público, en este caso google.com, ver Figura 49.

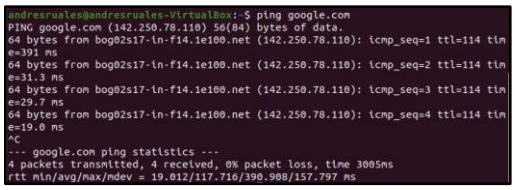

Figura 49. Verificación acceso a internet

Una vez verificado el acceso a internet se procede a ingresar en la configuración del cortafuego, en este caso se desea bloquear la salida a internet a sitios de entretenimiento, por ello las reglas que se deben configurar están en la opción de reglas de filtrado para las redes internas, ver Figura 50.

Figura 50. Configuración de reglas para redes internas

Para bloquear o denegar el servicio a un grupo de sitios específicos se deben configurar unos objetos, estos objetos son básicamente agrupamientos bajo ciertos criterios. En la Figura 51 se observa como añadir nuevos objetos.

Figura 51. Listado de objetos

Los objetos poseen miembros y estos miembros pueden ser identificados por direcciones MAC o direcciones IP. Para este caso se incluye la IP de Facebook.com, ver Figura 52.

Figura 52. Lista de miembros del objeto entretenimiento

Una vez creado el objeto se procede a realizar la configuración para la red interna, en la Figura 53 y Figura 54 se observa que para este caso se denegarán los servicios a los miembros del objeto previamente creados y configurados.

Figura 53. Creación de regla

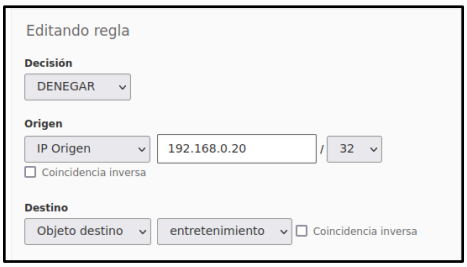

Figura 54. Configuración red interna para objetos de tipo entretenimiento

Ahora se debe verificar que la configuración anterior esté funcionando correctamente, para ello, en la máquina de Ubuntu desktop, se realizan las pruebas de nuevo con el comando ping, la primera a un sitio que no haya sido bloqueado y el segundo al sitio bloqueado, ver Figura 55 y Figura 56.

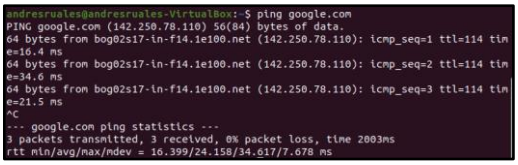

Figura 55. Ping a google.com

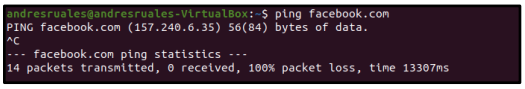

Figura 56. Ping a facebook.com

Por último, En la Figura 57 se observa que se puede realizar una comprobación de tipo usuario final para verificar nuevamente que todo esté funcionando correctamente

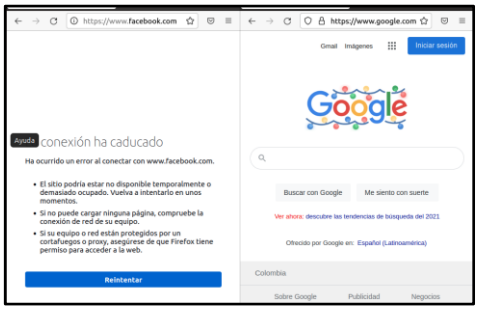

Figura 57. Comprobación visual

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Para realizar la compartición de ficheros, después de instalado el módulo se debe ir al menú lateral y seleccionar la opción de compartición de ficheros, esto abre la interfaz donde se puede agregar un nuevo fichero compartido, En la Figura 58 se observa que este pedirá un nombre de recurso compartido, la ruta del recurso compartido, un comentario para más detalle.

La configuración y la instalación fue realizada mediante la documentación que se encuentra en la siguiente cita [5].

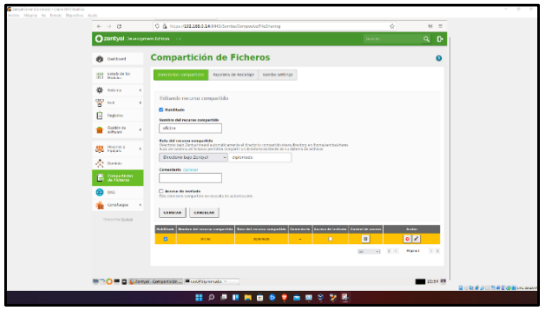

Figura 58. Creación de carpeta de recurso compartido

ahora se selecciona la opción de control de acceso y se da clic para que muestre con qué grupos se va a compartir esta carpeta, ver Figura 59.

Figura 59. Configuración para el control de acceso

En la Figura 60 se comparte la carpeta con el grupo “todos los usuarios administradores” y se dan permisos administrativos:
/home/samba/sharers

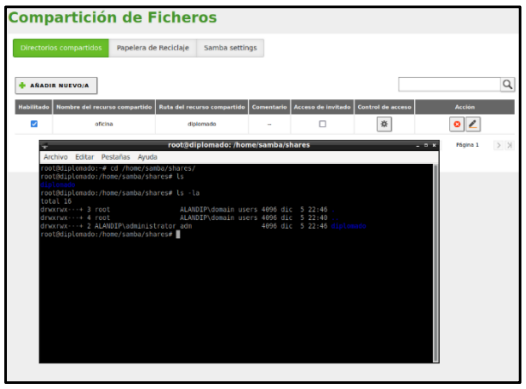

Figura 60. evidencia de creación de carpeta compartida

Ahora, para comprobar la conexión con la carpeta compartida, se dirige a la máquina virtual de escritorio, en este caso **linux mint**, se ingresa a la parte de red y en la cabecera de búsqueda se inserta smb://alandip esto abre una interfaz donde pedirá un nombre de usuario creado en el servidor **zentyal**, el nombre del dominio y la contraseña, ver Figura 61.

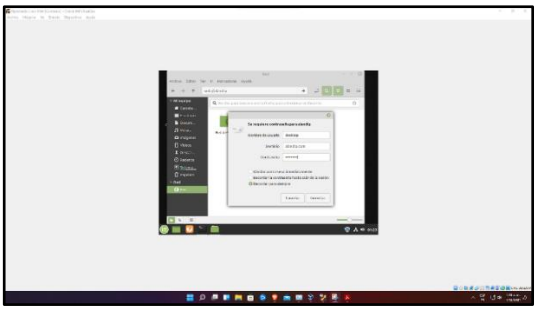

Figura 61. establecer conexión a la carpeta compartida

Se puede observar en la Figura 62 que al ingresar los datos y esperar un tiempo de carga se muestra la carpeta compartida.

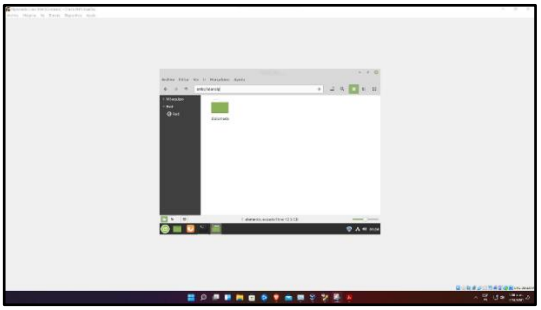

Figura 62. Evidencia de acceso a la carpeta compartida

6.1 CONFIGURACIÓN PRINT SERVER

Para la gestión de impresoras y de los permisos de acceso, se necesita realizar la instalación de los CUPS, Common Unix Printing System. Para eso se ejecuta el comando apt-get install cups, ver Figura 63.

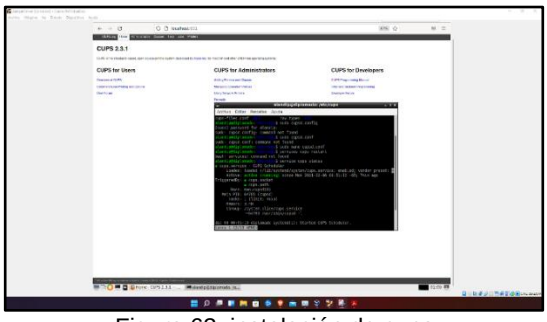

Figura 63. instalación de cups

Para realizar la configuración se debe tener una impresora instalada, se da en el botón de agregar impresora, esto pedirá los datos de acceso, luego de esto se tiene la lista de las impresoras, ver Figura 64.

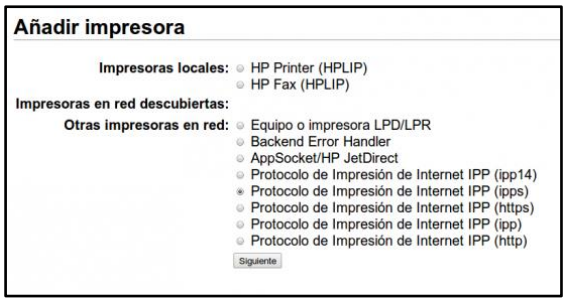

Figura 64. listado de impresoras

En la Figura 65 se elige la impresora que se desea agregar y le se da a continuar, esto pedirá la dirección de conexión, en este caso será la dirección IP del servidor.

Figura 65. conexión impresora

Ahora se muestra el nombre, descripción y el lugar en el que debe estar, ver Figura 66.

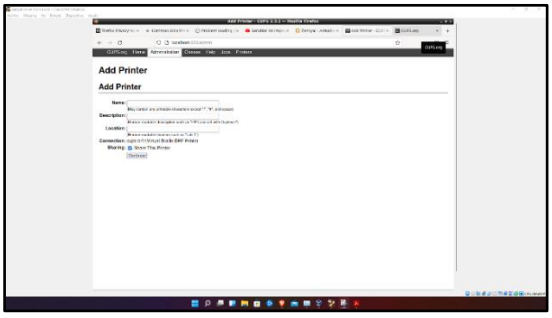

Figura 66. Datos básicos de la impresora

En la Figura 67 se muestra los datos generales de la configuración realizada.

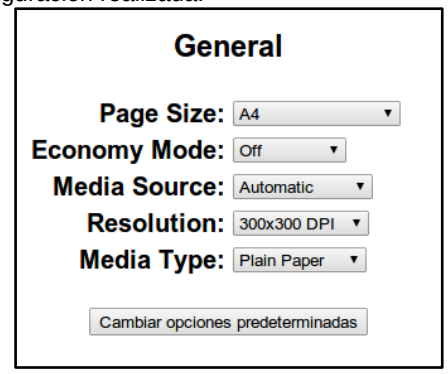

Figura 67. Datos generales de impresora

Cuando se haya añadido la impresora a través de CUPS, Zentyal es capaz de exportar usando Samba para ello. Una vez añadida la impresora, en la Figura 68 podrá ser vista en la lista presente en Compartir Impresoras.

Figura 68. Visualización en interfaz

6.2 CASOS DE USO

Actualmente en muchas empresas es necesario tener unas carpetas compartidas para diferentes departamentos donde les permita compartir documentos importantes y que una persona o algunos miembros de un grupo puedan tener acceso.

El servidor de impresoras es sumamente útil al momento de brindar conexión a una o varias impresoras ya sea en un piso de un edificio o departamentos enteros que tengan varias impresoras, también facilita su uso porque no requiere de ninguna instalación necesaria, solo hacer parte de la red.

6.3 VENTAJAS

Si hace parte de la red los colaboradores tendrán acceso a elementos compartidos de una forma rápida y sencilla.

Uso de una o más impresora sin instalaciones de drivers o software en cada uno de los equipos que hacen parte de la red.

Se brinda un mejor control sobre el manejo de los archivos y a qué personas se les debe dar acceso de lectura y escritura.

7 TEMÁTICA 5: VPN

Para configurar el servicio de VPN en Zentyal server, después de haber instalado el servidor lo siguiente es instalar los paquetes necesarios, como se puede observar en la Figura 69 se debe instalar el paquete de VPN.

La configuración y la instalación fue realizada mediante la documentación que se encuentra en la siguiente cita [6].

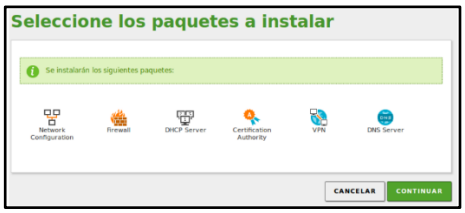

Figura 69. instalando paquetes

En la Figura 70 se crean los certificados de autoría, ya es posible expedir certificados.

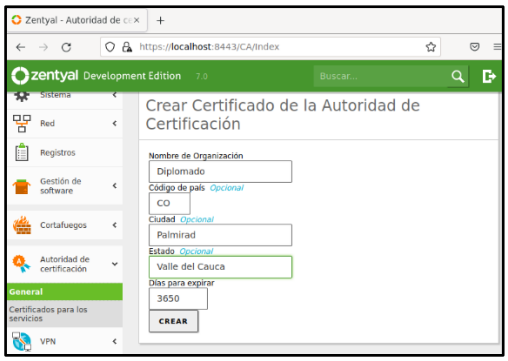

Figura 70. certificados de autoría

En la Figura 71 se observa el paso siguiente que es crear el servidor, que se debe identificar con un nombre y encontrase habilitado.

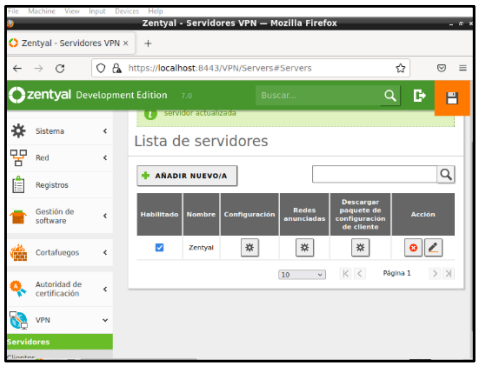

Figura 71. Creando el servidor

Después de creado el servidor y crear los certificados lo siguiente es configurar y descargar el paquete de configuración del cliente, ver Figura 72.

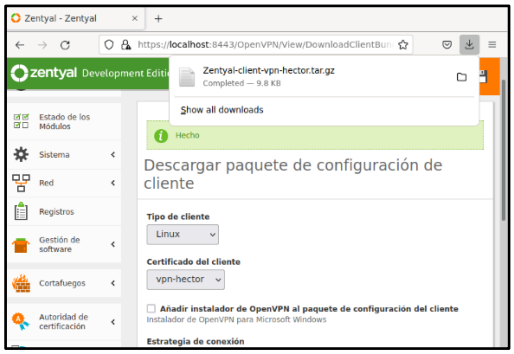

Figura 72. paquete de cliente

En esta parte se indica el protocolo necesario y el puerto de destino, que sería el 1194, en la Figura 73 se puede observar la configuración que se realiza.

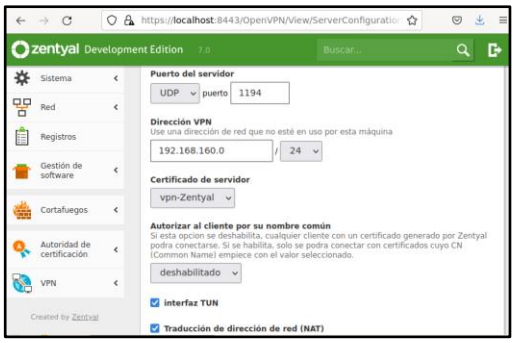

Figura 73. puerto del servidor

Se guarda el progreso y se evidencia que el demonio está ejecutándose, ver Figura 74.

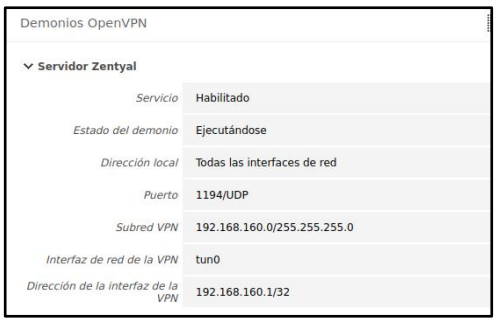

Figura 74. Demonio OpenVpn

Una vez realizado esto, se dirige a Linux para descargar network manager openvpn y así poder configurar la VPN, en la Figura 75 se observa la instalación de openvpn en el equipo cliente.

Figura 75. VPN

El siguiente paso sería ir a la configuración de redes de Ubuntu, en esta parte saldrá la opción de VPN, se añade una nueva, ver Figura 76.

Figura 76. Nueva VPN

Se importa desde un archivo, este archivo será el que se descargó de Zentyal Server, en este caso se usó google drive para poder utilizar el archivo. En la Figura 77 se observa cómo se importa el archivo de configuración de VPN.

Figura 77. Importar archivo

En la Figura 78 se observa que al encontrase el equipo cliente ya conectado mediante la VPN, se pude confirmar la conexión al servidor realizando un ping.

Figura 78. Ping al servidor

8 CONCLUSIONES

Uno de los principales usos de Zentyal es el de controlador de dominio puesto que zentyal Server es una alternativa a Windows Server que ofrece funcionalidades propias de Microsoft Active Directory desde Linux para la administración de clientes Windows por lo que lo hace un servidor muy utilizado en todo tipo de empresas de cualquier tamaño.

Linux Zentyal Server ofrece un servicio Http Proxy de fácil administración, mediante el cual un administrador de los servicios de tecnología en una compañía podría realizar filtrados de acceso a los diferentes recursos de internet, permitiendo crear agrupación de equipos, así como también una lista de dominios a los cuales se les debe restringir el acceso a los equipos de la compañía.

Tener un servidor de impresoras nos permite poder controlar el acceso de las personas que desean realizar trabajos en esta, es un recurso muy administrable el cual nos permite repartir mejor las impresoras en un entorno laboral.

9 REFERENCIAS

[1] Zentyal. (14 de septiembre de 2018). *Zentyal como único Controlador de Dominio (Tutorial 1)*. [Archivo de Video]. Disponible en. https://www.youtube.com/watch?v=ogr9L67JcMg&ab_channel=Zentyal.
[2] Zentyal. (2004-2021). *Servicio de Proxy HTTP*. [En línea]. Disponible en: https://doc.zentyal.org/es/proxy.html
[3] Mocan, T. (2019). *¿Cuáles Son los Beneficios de Usar un Servidor Proxy?.* [En línea]. Disponible en: https://www.cactusvpn.com/es/vpn/cuales-son-los-beneficios-de-usar-un-servidor-proxy/#proxy4
[4] Barbosa, D. (2020). *Qué es un proxy y para qué sirve.* [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/
[5] MSC.GuadalupeGT. (20 de marzo de 2020). Servidor de Impresión con CUPS y SAMBA a través de Linux y Windows [Archivo de video]. Disponible en. https://www.youtube.com/watch?v=S_XrLYoIiqg
[6] Servicio de redes privadas virtuales (VPN) con OpenVPN Disponible en *https://doc.zentyal.org/es/vpn.html*