MUNDO ZENTYAL

Miguel Angel Caro
E-Mail: macaroq@unadvirtual.edu.co
Anderson Julian Cadavid
E-Mail: ajcadavidm@unad.edu.co
Camilo Andres Rudas
E-Mail: carudasg@unadvirtual.edu.co
Yilber Alexander Rodriguez
E-Mail: yarodriguezgil@unadvirtual.edu.co
Luis Alberto Contreras Perdomo
E-Mail: lacontreraspe@unadvirtual.edu.co

RESUMEN: *Este documento presenta la instalación, configuración y puesta en marcha de GNU/Linux Zentyal Server; a lo largo de 5 temáticas desarrolladas veremos DHCP Server, DNS Server y Controlador de Dominio. Proxy no transparente. Cortafuegos. File Server y Print Server. VPN; realizado a través de máquinas virtuales (VirtualBox) con la versión 6.2 de Zentyal.*

PALABRAS CLAVE: Zentyal, DHCP Server, DNS Server, Firewall, Proxy, VPN

ABSTRACT: *This document presents the installation, configuration and start-up of GNU/Linux Zentyal Server; Throughout 5 developed themes we will see DHCP Server, DNS Server and Domain Controller. Non-transparent proxy. Firewalls. File Server and Print Server. VPN; performed through virtual machines (VirtualBox) with version 6.2 of Zentyal.*

KEYWORDS: Zentyal, DHCP server, DNS server, Firewall, Proxy, VPN

Responsable	**Temática**
Luis Alberto Contreras	Temática 1: DHCP Server, DNS Server y Controlador de Dominio.
Camilo Andres Rudas	Temática 2: Proxy no transparente
Yilber Alexander Rodriguez Gil	Temática 3: Cortafuegos
Anderson Dadavid	Temática 4: File Server y Print Server
Miguel Angel Caro	Temática 5: VPN

1. INTRODUCCIÓN

Esta guía incluye las descripciones completas de los tipos de letra, del espaciamiento, y la información relacionada para elaborar sus reportes, basada en los formatos utilizados por la IEEE.

2. ZENTYAL SERVER

2.1 REQUERIMIENTOS

"Esto depende de los servicios que se despliegan y la cantidad de usuarios concurrentes. Los requisitos mínimos que solemos dar son: Intel Core i5, 8GB de RAM y el disco según los datos. Recomendamos usar hardware certificado por Ubuntu." tomado de: https://zentyal.com/es/faq-2/.

2.2 URL DE DESCARGA

https://zentyal.com/es/trial-gratuito-de-45-dias-del-servidor-zentyal/

3. INSTALANDO ZENTYAL

Una vez descargado y montado sobre una máquina virtual con los requisitos mínimos indicados se inicia el proceso de instalación.
Seleccionar idioma.

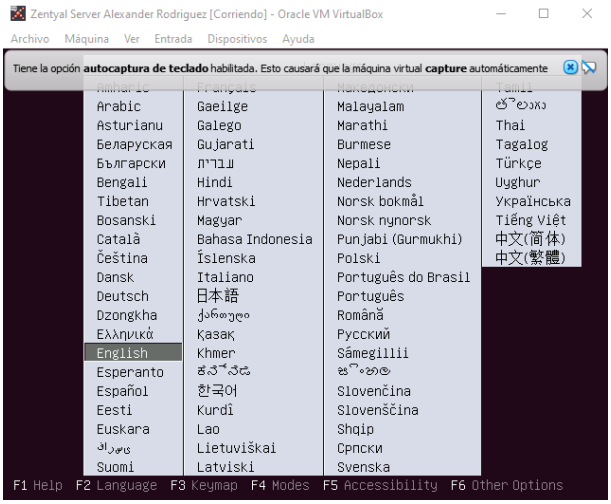

Imagen 1. Selección de idioma.

Seleccionar la primera opción “Instalar Zentyal 6.2-development (borrar todo el disco)”.

Imagen 2. Selección de instalación.

Seleccionar ubicación para fijar zona horaria y localización del sistema.

Imagen 3. Selección de ubicación.

Seleccionar distribución del teclado

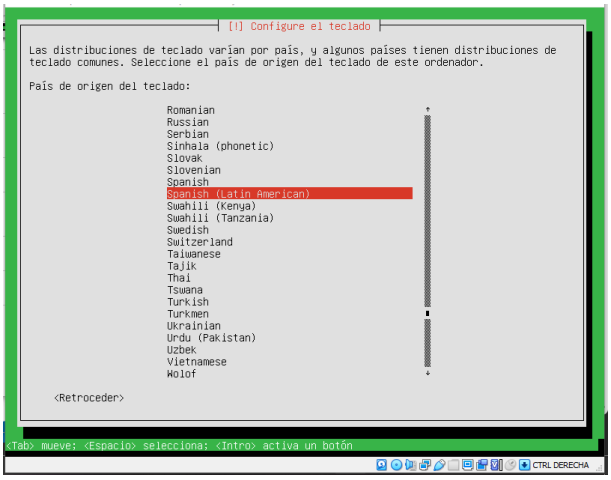

Imagen 4. Selección de ubicación.

Introducir nombre para la máquina.

Imagen 5. Selección nombre de máquina.

Configurar usuario y contraseña.

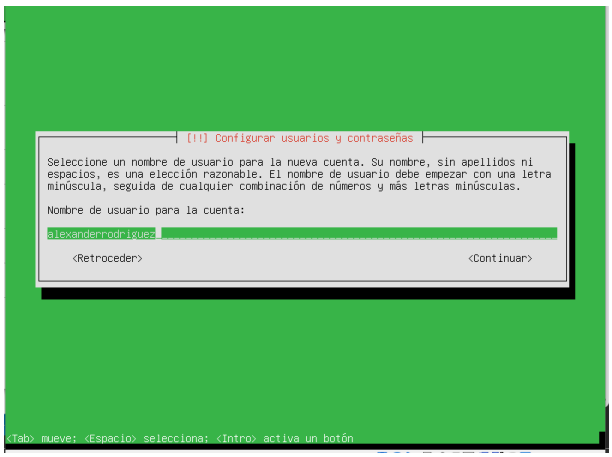

Imagen 6. Seleccionar usuario.

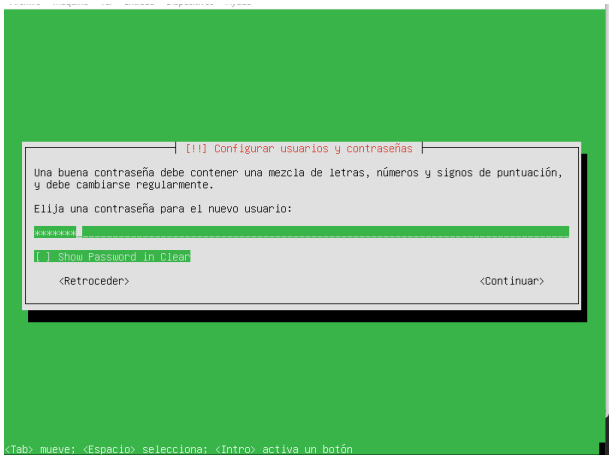

Imagen 7. Seleccionar contraseña.

Confirmar reloj.

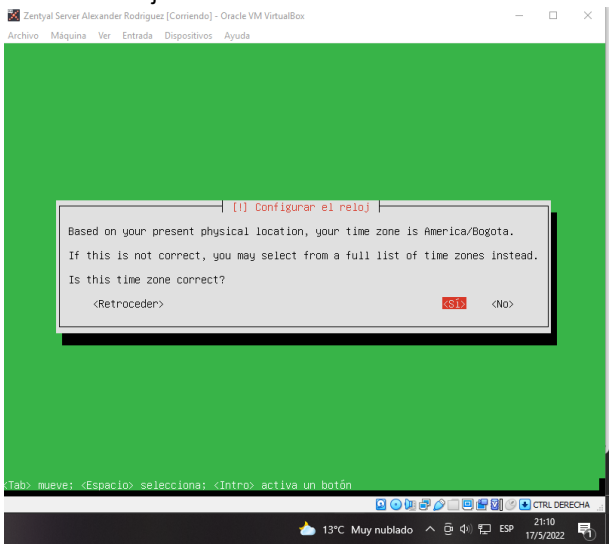

Imagen 8. Confirmar reloj.

Una vez configurado inicia el proceso de instalación y se debe esperar hasta que finalice el mismo.

Imagen 9. Instalación finalizada.

Al finalizar la instalación se inicia el sistema operativo y abre el navegador apuntando al servicio donde se abre una ventana de login para acceder con las credenciales indicadas en la imagen 6 y 7.

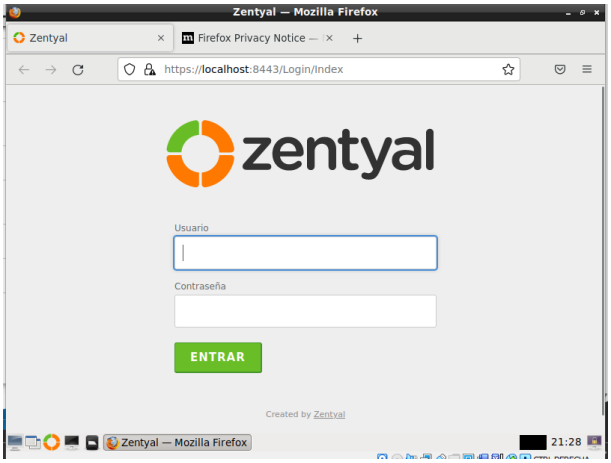

Imagen 10. Instalación finalizada.

Una vez iniciada la sesión nos da la opción de continuar con el proceso de instalación y seleccionar los servicios que se van a utilizar

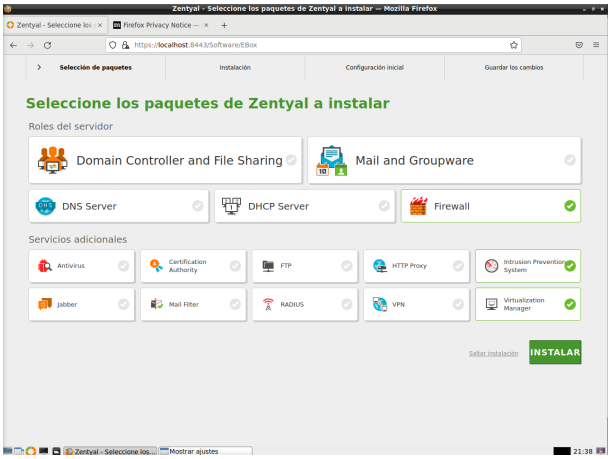

Imagen 11. Selección de paquetes 1.

Una vez seleccionado muestra los paquetes necesarios para que funcionen los seleccionados.

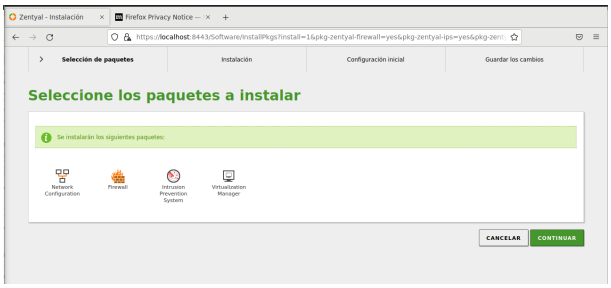

Imagen 12. Selección de paquetes 2.

Luego se debe realizar la configuración de red, en este caso con DHCP

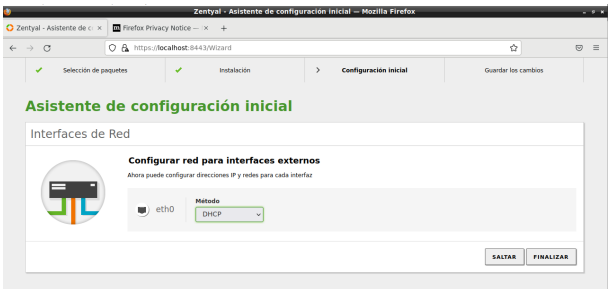

Imagen 13. Configuración de red.

Al finalizar se mostrará la siguiente pantalla.

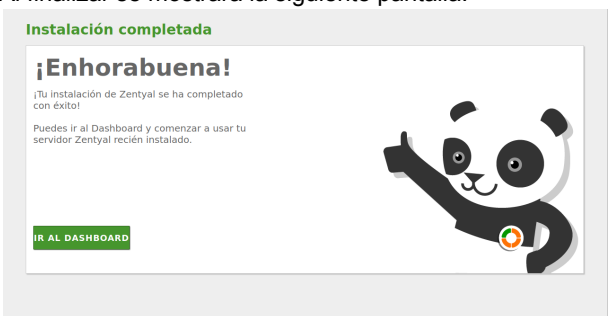

Imagen 14. Configuración finalizada

Para finalizar se va a mostrar el dashboard

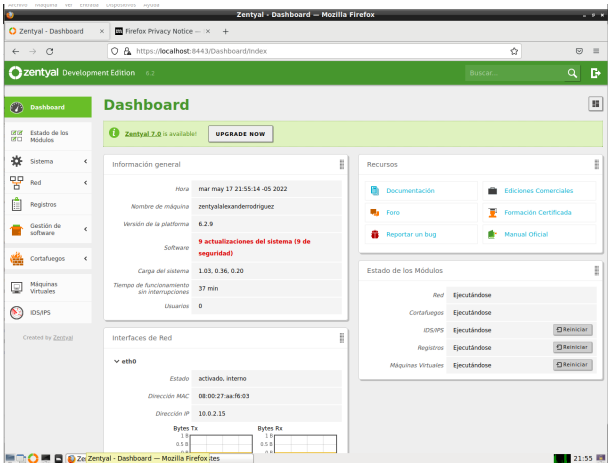

Imagen 15. Dashboard Zentyal

4. TEMÁTICAS.

Este documento se divide en 5 temáticas, de la siguiente manera:

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

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

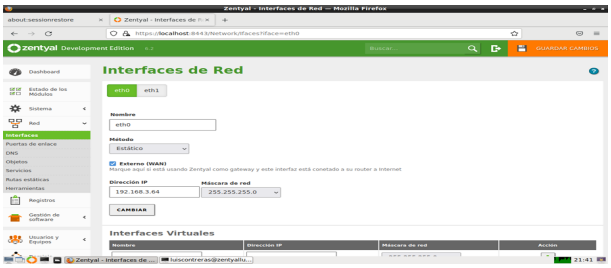

Imagen 15. IP estática

Imagen 16. Puerta enlace

Imagen 17. LDAP

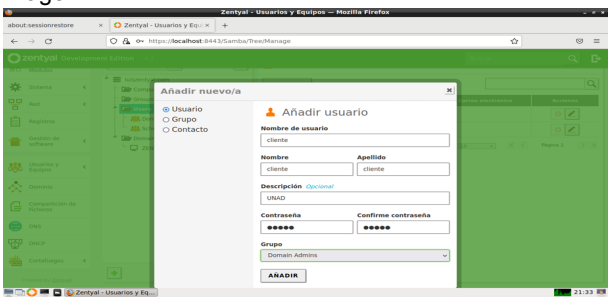

Imagen 18. usuario

En las imágenes 15 a la 18 se hace la configuración necesaria en Zentyal para poder realizar la conexion,

configuracion que implica cambiar de DHCP a estático, habilitar y poner una puerta de enlace, algo muy importante es la habilitación del PAM en el LDAP y la creación del usuario con el cual vamos a realizar la conexión, para este caso el usuario es “cliente” luego de realizado esto podemos olvidarnos del servidor y nos pasamos a la maquina que sera cliente, en las siguiente imágenes se dejará gráficamente el proceso que se debe realizar.

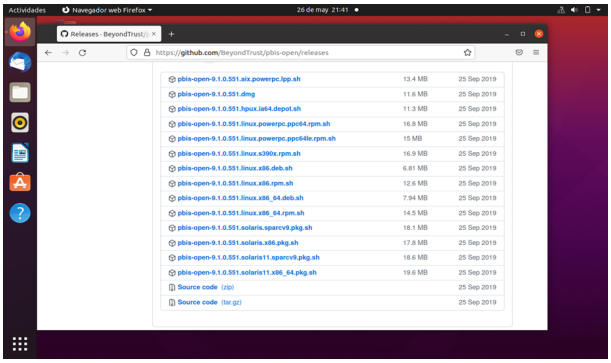

Imagen 19. Descarga PbisImagen 20. Chmod

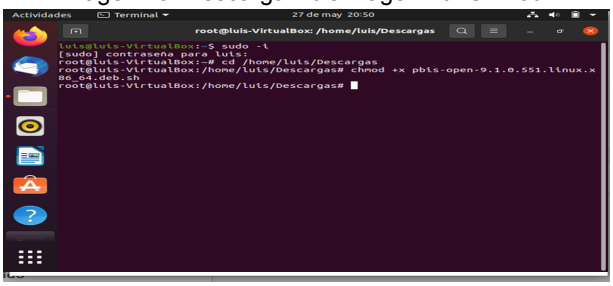

Imagen 21. DNS

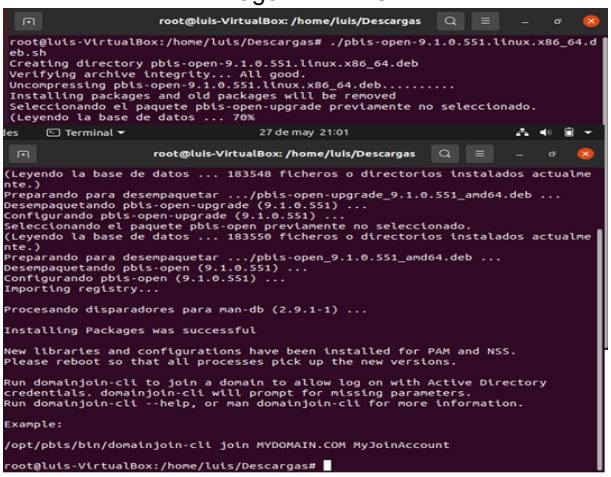

Imagen 22. Ejecutando Pbis

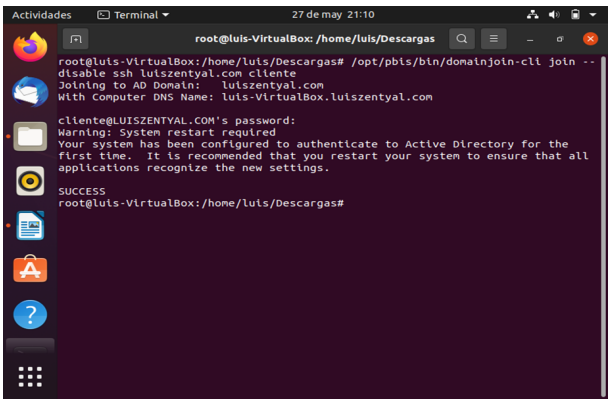

Imagen 23. Conectando

En este punto ya tenemos completa la conexión debemos descargar el Pbis, para hacerlo es tan sencillo como escribir por google “pbis download” vamos al enlace de Github y descargamos el archivo, luego de esto es tan sencillo como ejecutar los comandos ilustrados, algo muy importante y que nadie debe olvidar es lo que se muestra en la imagen 21, ya que si no se realiza la configuración de este DNS no va a ser posible generar la conexión.

Se debe reiniciar la máquina cliente y una vez inicie nuevamente se debe iniciar sesión con el usuario creado en zentyal, para el caso de este documento es “cliente@luiszentyal.com” y la contraseña que creamos para el mismo.

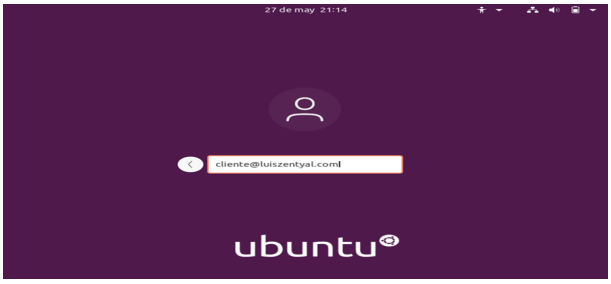

Imagen 24. conexión de usuario

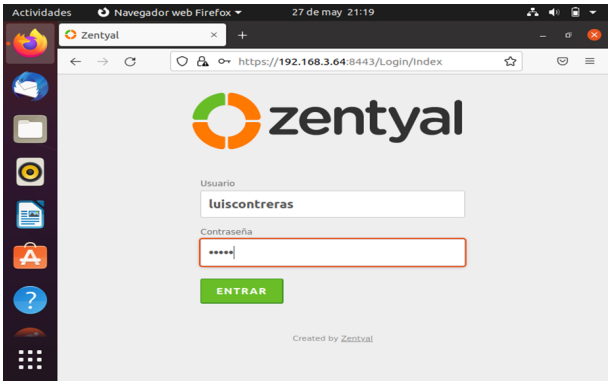

Imagen 25. inicio de sesión

Abriremos el navegador e iniciamos sesión en Zentyal con la ip configurada.

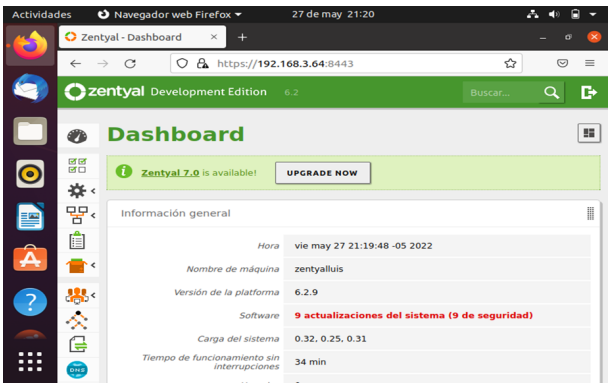

Imagen 26. Zentyal cliente

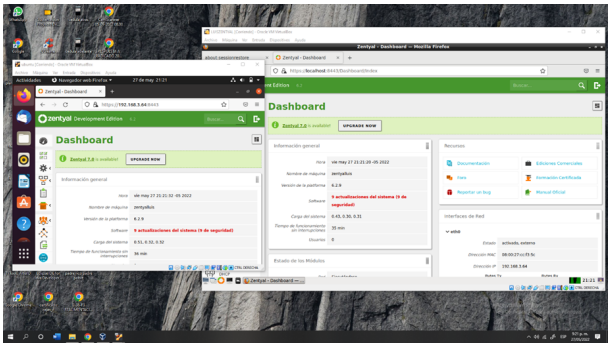
Imagen 27. Conexión definitiva

4.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Primero vamos a definir que es un proxy es cual podemos decir que es un dispositivo, programa o servidor el cual se utiliza como intermediario. Esta intermediación permite que nuestro recurso destino no sepa quien es su recurso origen, por tal motivo es que dentro de las muchas funcionalidades que tenemos de este tipo de servicio esta control de acceso, log de todo el tráfico, restricción a cierto tráfico, mejora el rendimiento y el que ya habíamos hablado está el de anonimato. Ahora si miramos podemos decir que un proxy mejora el rendimiento ya que este puede mantener conexiones en caché lo cual hace que la navegación sea mucho más rápida pero es una desventaja si la página es actualizada y el cache del proxy no.

Por otro lado podemos clasificar de muchas formas un proxy entre los cuales está exterior, local, transparente, no transparente, Proxy HTTP, proxy Inverso, Proxy Nat, entre otros. Pero el que nos vamos a enfocar en este momento es el tipo de proxy transparente el cual tiene como fin forzar la política establecida, esto quiere decir que todo el tráfico que sale de la red local debe pasar por nuestro proxy para esto se necesita configurar otros componentes en nuestro segmento de red. En algunos libros podemos encontrar que la forma más sencilla es con un firewall ya que como sabemos el proxy necesita un puerto específico que veremos más adelante. Por ende, podemos bloquear los otros puertos o desviar toda la comunicación para que vaya a nuestro proxy y la otra es configurar una regla para que el único medio o dispositivo que pueda salir a internet sea nuestro proxy, y con esto se garantiza que siempre este funcione como intermediario. Todas esas configuraciones que se realizan a nivel de red para tener un proxy transparente pueden ser desapercibidas por los usuarios y por ende no se necesita ninguna configuración manual para garantizar este servicio.

Si ya hemos entendido que es un proxy transparente, vamos a poder configurar fácilmente un proxy no transparente el cual requiere una configuración manual en cada uno de nuestros usuarios, los cuales sí tienen privilegios de administrador sobre el sistema operativo puedan evitarlo cambiando dicha configuración la cual es muy sencilla. Pero antes de ver la configuración de nuestros usuarios vamos a ver cómo se configura un proxy HTTP en Zentyal, para esto lo primero que debemos definir es el puerto de nuestro servidor y lo otro que se define es el tamaño de los diferentes caches que se van a tener almacenados como lo indica la siguiente imagen.

Imagen 28. Configuración servidor Proxy HTTP

Ya realizada la configuración básica del proxy ahora vamos a poder definir el tráfico que deseamos tanto permitir y restringir, los horarios en que vamos a tener el servicio arriba, las extensiones de archivos que vamos a permitir entrar y restringir a nuestra red y hasta la limitación de ancho de banda y las penalizaciones que puedo hacerle a mis usuarios si estos completan el tamaño máximo permitido. Ya sabiendo todas las configuraciones que podemos hacer vamos a dar un ejemplo con la más sencilla que es la de bloqueo por URL, para esto vamos a configurar los diferentes dominios que deseamos bloquear o permitir como se puede apreciar en la siguiente imagen. Donde vamos a poder visualizar que estamos bloqueando el acceso a youtube y estamos permitiendo el acceso a google. Para esto se crea una regla por cada dominio que queremos incluir las cuales van a estar en una misma categoría o perfil para nuestro sistema Zentyal.

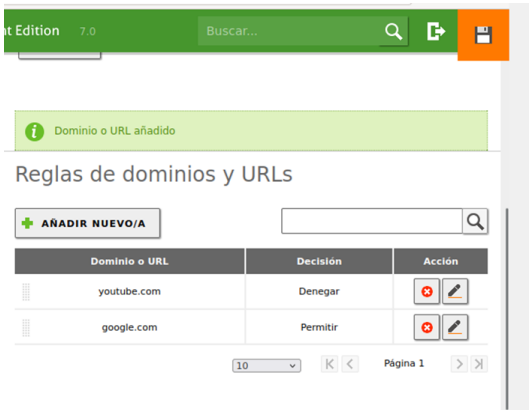

Imagen 29. Configuración Bloqueos de dominios y URLs

Luego de esto vamos a establecer los horarios en que va a estar disponible nuestro proxy y cuales son las decisiones que van a ser aplicadas en este tiempo como lo podemos observar en la siguiente imagen.

Imagen 30. Configuración Horarios y decisiones del proxy

Luego de realizar todo este proceso ya tenemos configurado nuestro Proxy HTTP y solo nos hace falta configurarlo en el SO de nuestros usuarios. La cual es muy sencilla y es en la parte donde se configura la red del equipo de nuestro usuario vamos a tener la opción para configurar nuestro proxy de forma manual, para esto debemos es conocer dirección IP o Hostname si utilizamos un DNS y el puerto de nuestro proxy. Como se puede ver en la siguiente imagen.

Imagen 31. Configuración Proxy en el usuario.

Con esto hemos terminado ya la configuración en cada uno de los respectivos sistemas que intervienen en la configuración de un proxy HTTP no transparente y que si deseamos validar si este está corriendo correctamente podemos hacer una prueba navegando a Internet desde el equipo de nuestro usuario o mirando el dashboard de monitoreo que nos proporciona Zentyal donde vamos a ver tanto el comportamiento de nuestra red interna y el punto de salida de la red que va a internet. En nuestro caso lo que hicimos fue la prueba en el ordenador de nuestro usuario como se puede ver a continuación.

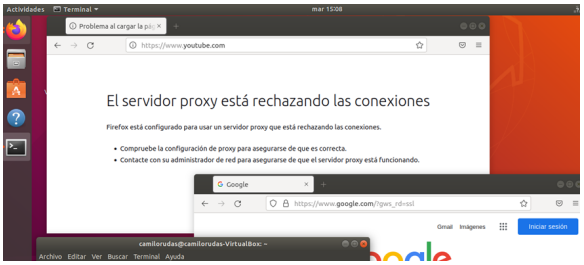

Imagen 32. Prueba desde el navegador del usuario

4.3 TEMÁTICA 3: CORTAFUEGOS

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

El cortafuegos es una funcionalidad que se usa desde el servidor intermediario entre el computador e internet donde se pueden aceptar o rechazar paquetes tanto entrantes como salientes sobre páginas específicas, controlando así a qué tienen acceso y restringiendo también páginas que puedan vulnerar el equipo, también permitiendo por ejemplo el acceso

únicamente a una lista de paginas especificas para reducir las posibilidades de un ataque externo.

Lo primero que se debe hacer es configurar las dos máquinas dentro de una misma red interna cómo se muestra a continuación.

Configuración del servidor:

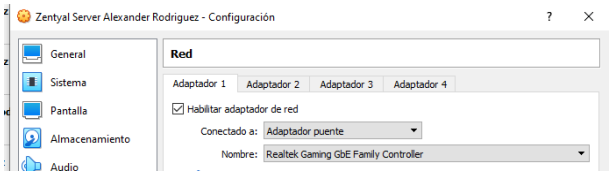

Imagen 33. Configuración servidor red adaptador 1

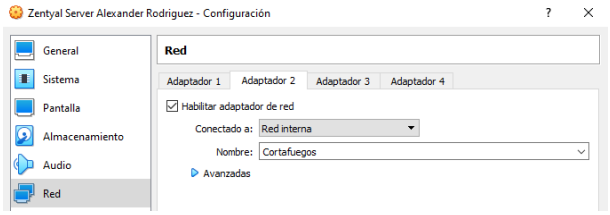

Imagen 34. Configuración servidor red adaptador 2

Configuración equipo de escritorio:

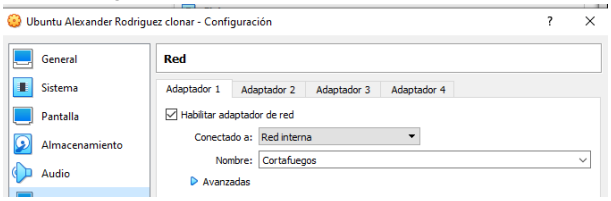

Imagen 35. Configuración desktop red adaptador 1

Lo primero que se debe hacer es habilitar los módulos de red y cortafuegos desde el dashboard.

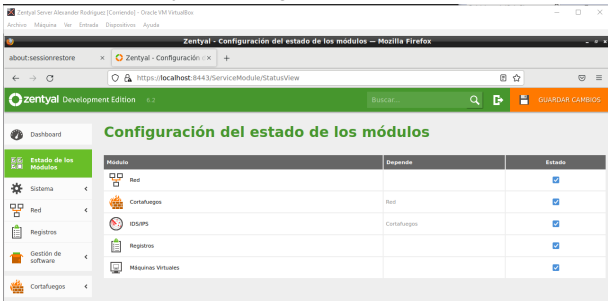

Imagen 36. Habilitar módulos.

Una vez configurada, desde la sección de red se ajusta una IP dentro del rango que se va a asignar a esta red interna, en este caso 192.168.100.5/24

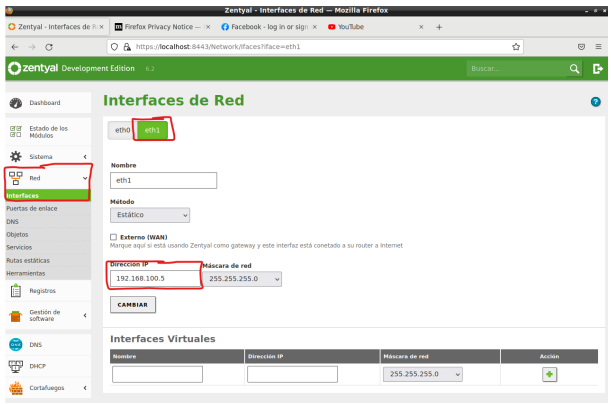

Imagen 37. Configurar red eth1.

También se asigna la red eth0 como la designada a conexión WAN

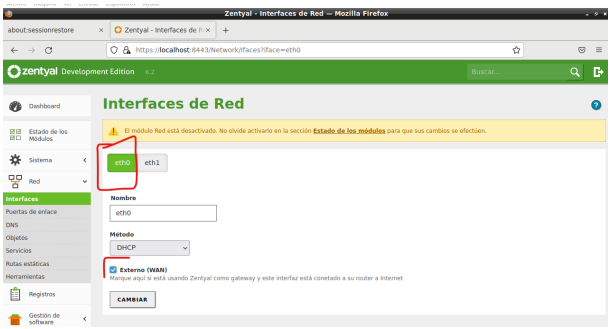

Imagen 38. Configurar red eth0.

Luego click sobre el botón “Cambiar” y finalmente sobre guardar.

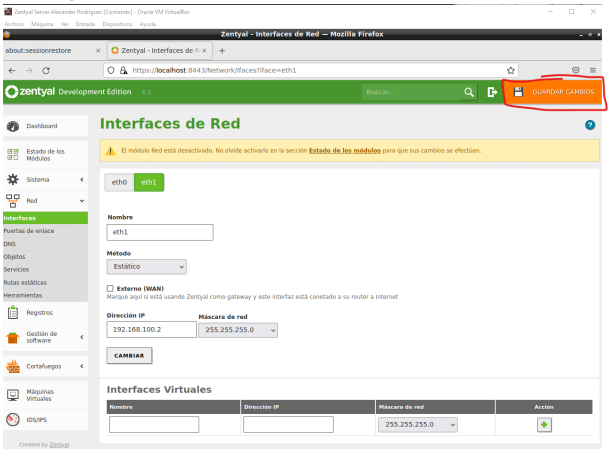

Imagen 39. Guardar cambios.

Se puede validar la configuración desde consola.

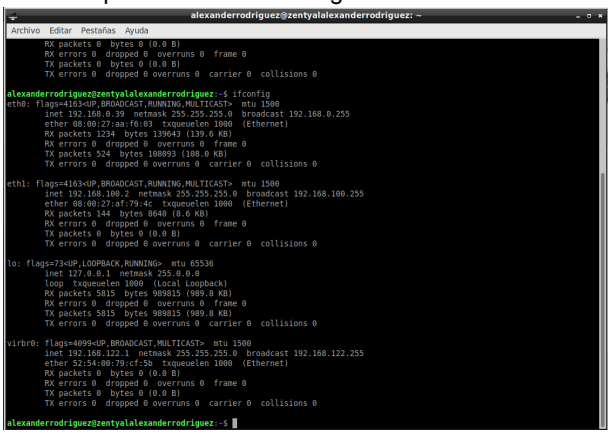

Imagen 40. Configuración de red servidor.

Luego se debe configurar un equipo desktop dejando como puerta de salida y DNS equivalente a la IP asignada

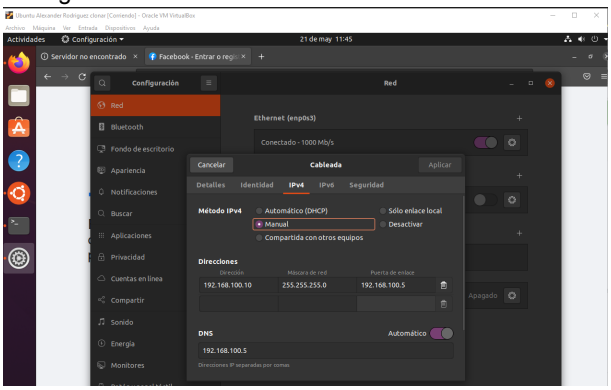

Imagen 41. Configuración de red servidor.

Comprobar acceso a facebook desde equipo desktop

Imagen 42. Comprobar acceso a Facebook 1.

Con el comando nslookup www.facebook.com se consulta la ip del servidor

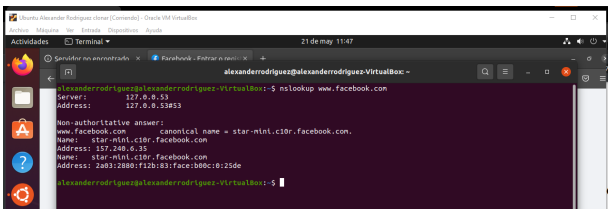

Imagen 43. Consulta IPs Facebook.

Luego desde el servidor Zentyal accederemos a la sección de cortafuegos ->Filtrado de paquetes ->Reglas de filtro para las redes internas.

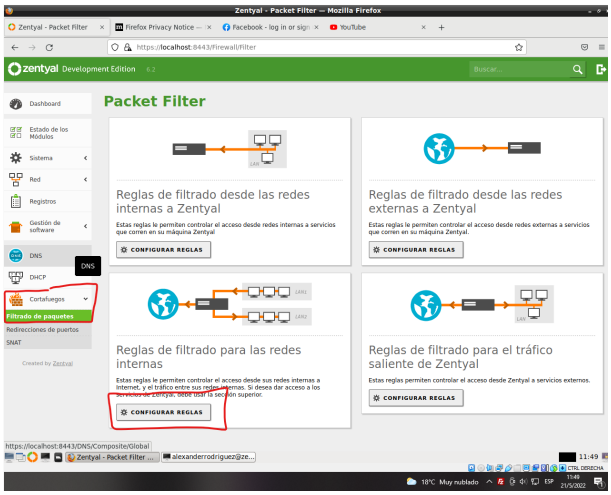

Imagen 44. Filtrado de paquetes.

En este punto nos encontramos con que existe solo una regla con acceso total desde todas las IPs, para crear una nueva se dará clic sobre “Añadir nuevo/a” y se realizará la configuración.

Imagen 45. Añadir nueva regla.

Para añadir una nueva regla se tienen las opciones de “Decisión” en este caso son Aceptar, Denegar o Registrar, También un origen y un destino, además del servicio que se quiere aplicar.

En este caso para restringir facebook se restringen todos los servicios cuando el destino sea 157.240.6.35, qué es la ip del servidor como vimos en el punto anterior, quedando entonces de la siguiente forma.

Imagen 46. Añadir nueva regla 2.

.Tener en cuenta que al crear una nueva regla esta queda en la parte superior y el cortafuegos utiliza ese mismo orden para filtrar el contenido.

Imagen 47. Vista reglas 1.

Validamos desde el equipo desktop que ya no se puede ingresar a facebook

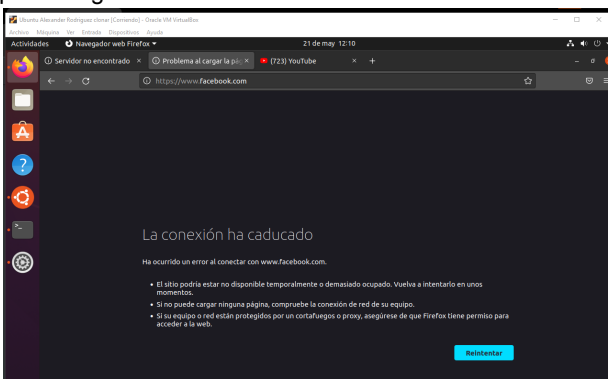

Imagen 48. Comprobar acceso a Facebook 2.

Pero si se puede acceder a otras páginas, cómo youtube

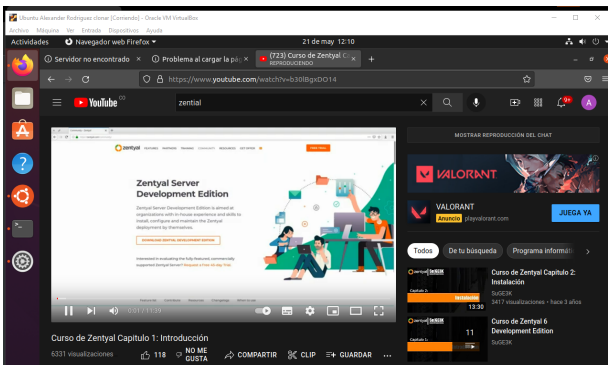

Imagen 49. Comprobar acceso a Youtube 1.

De acuerdo a la guía de actividades también se deben restringir las demás redes sociales o sitios de entretenimiento, por lo que se realiza el mismo proceso para de más páginas terminando de la siguiente forma las reglas de firewall

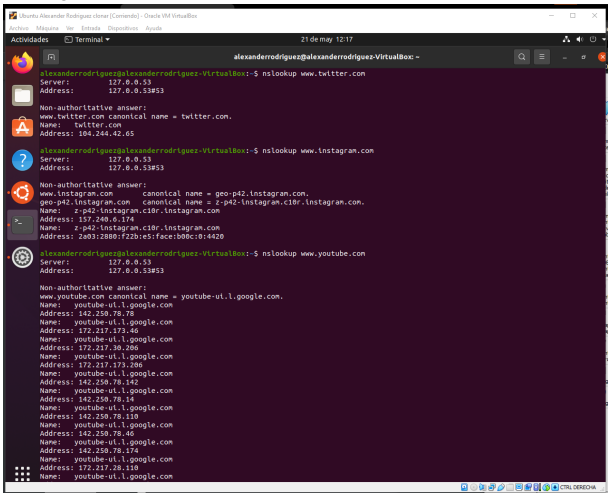

Imagen 50. Consulta IPs redes sociales.

Imagen 51. Vista reglas 2.

Cómo se puede mostrar en la primera imagen, youtube tiene no solo una IP asignada sino varias, por lo que en este caso se recomienda mejor crear un objeto de IPs para las reglas como se muestra a continuación.

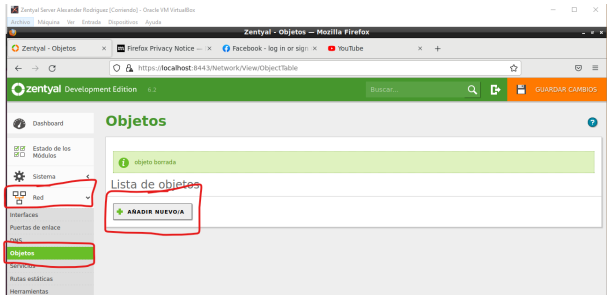

Imagen 52. Vista Objetos 1.

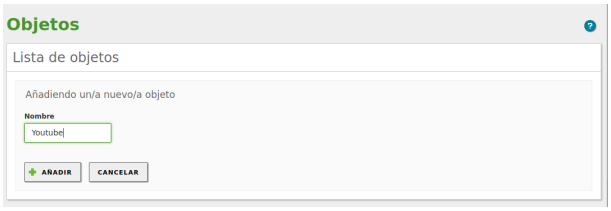

Imagen 53. Vista Objetos 2.

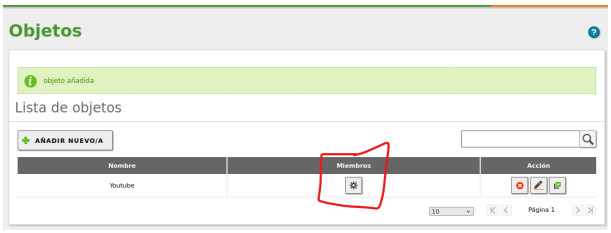

Imagen 54. Vista Objetos 3.

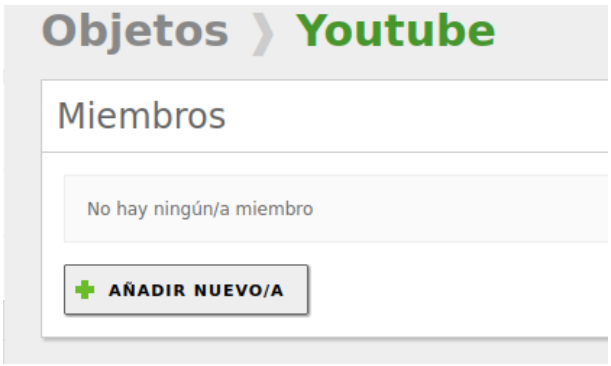

Imagen 55. Vista miembros del objeto 1.

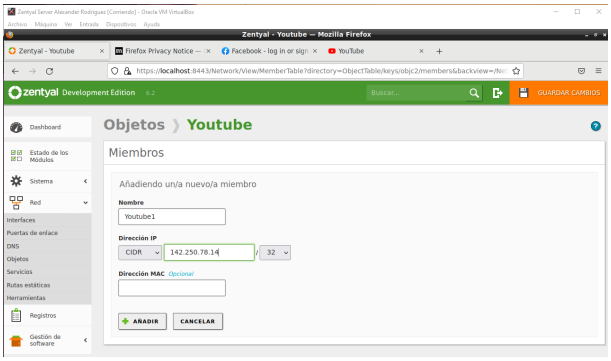

Imagen 56. Crear miembro objeto.

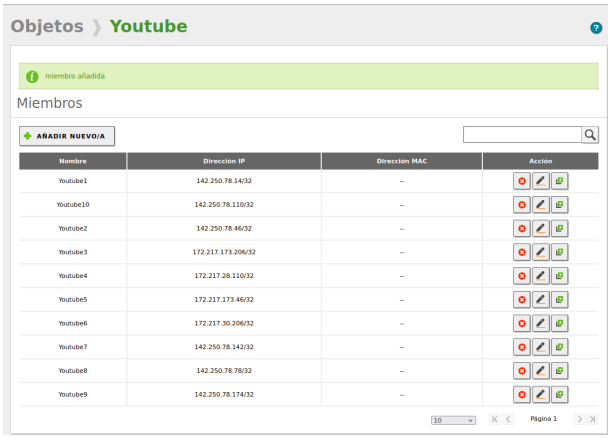

Imagen 57. Vista Objetos 4

Volviendo a la configuración de firewall sería similar cambiando únicamente el destino de una ip fija a un objeto.

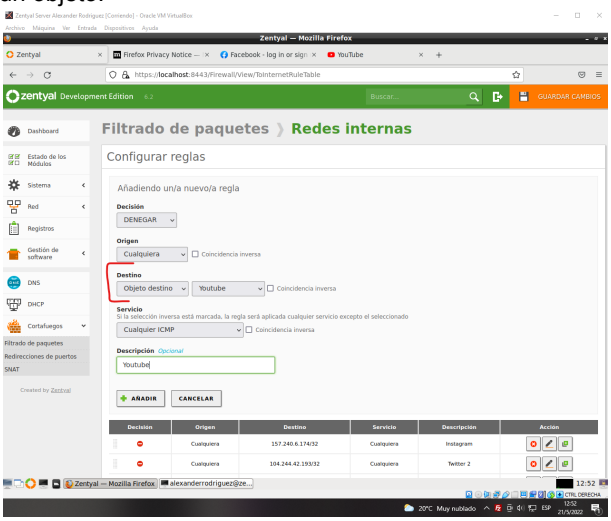

Imagen 58. Añadir nueva regla 2.

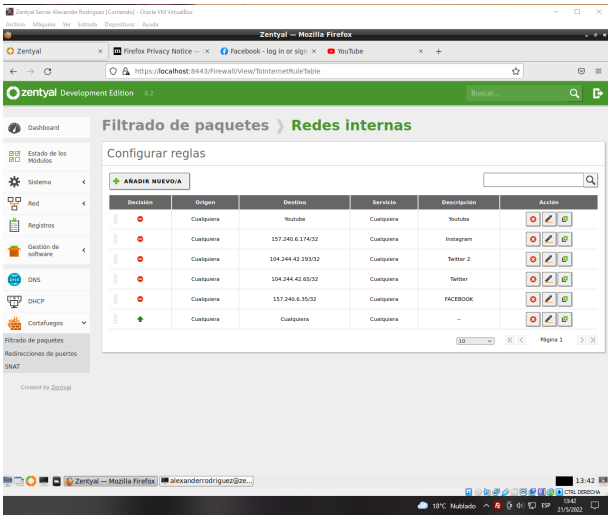

Imagen 59. Vista reglas 3.

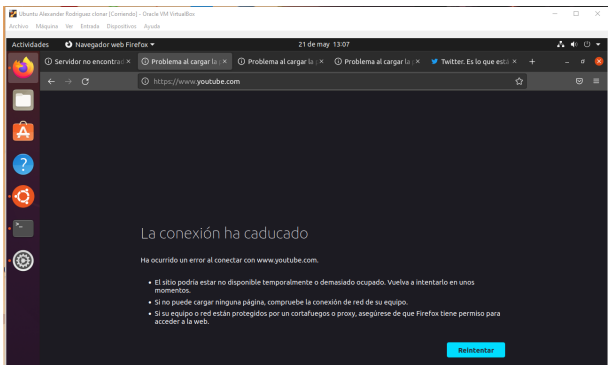

Imagen 60. Comprobar acceso a Youtube 2.

4.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER.

Para la configuración del File Server y Print Server, fue necesario la configuración de dos interfaces de red, la principal se le asignó configuración para servicios puntuales de Zentyal como lo son actualizaciones, instalación de paquetes y administración. La segunda interfaz se configura como DHCP para que los usuario tengan conexión para los servicios configurados.

Para este paso se inicia la configuración de los archivos compartidos.

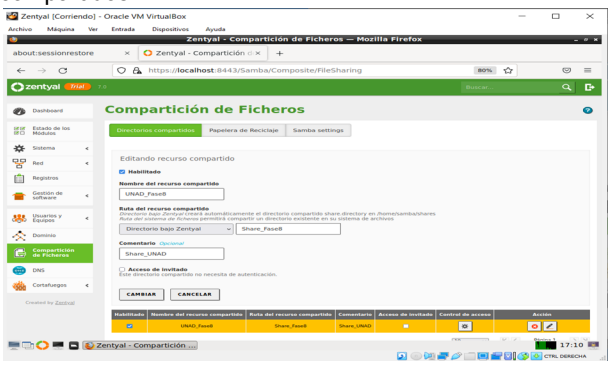

Imagen 61 File Server y Print Server

Posterior a la creación del recurso compartido, procedemos a agregar los usuarios que tendrán acceso al recurso compartido mediante la opción de control de acceso y agregando el usuario mediante ACL.

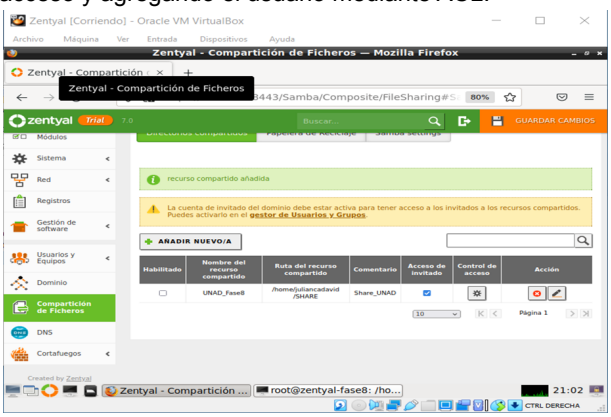

Imagen 62 File Server y Print Server

Por medio de esta interfaz confirmamos que el usuario (usertest) cuenta con los accesos al recurso compartido.

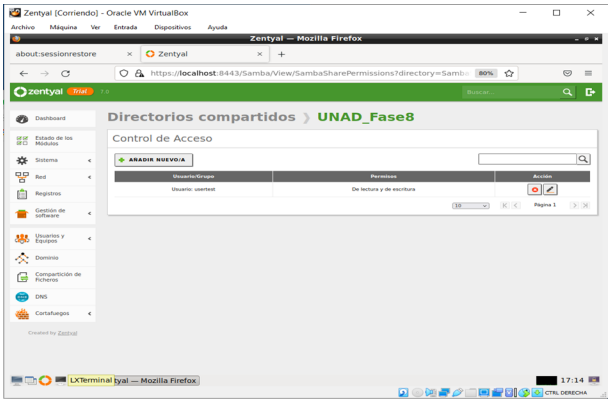

Imagen 63 File Server y Print Server

En este paso se lista el usuario que se encuentra creado.

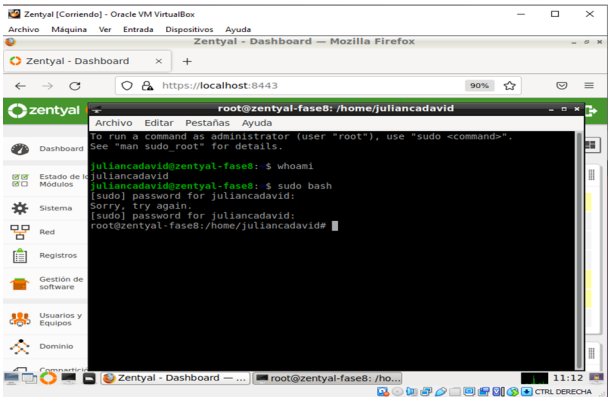

Imagen 64 File Server y Print Server

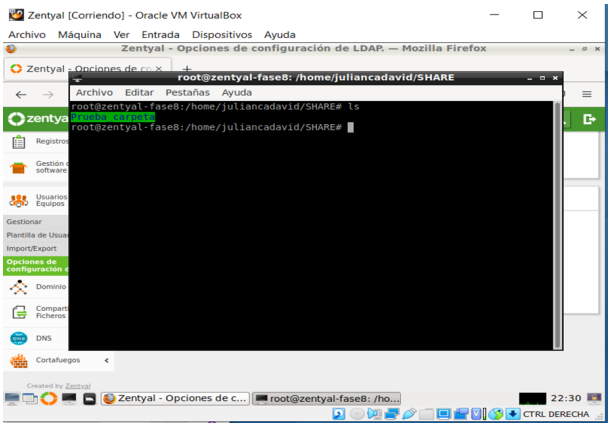

Imagen 65 File Server y Print Server

En este paso se realiza prueba de conexión al recurso compartido desde un S.O Windows 10.

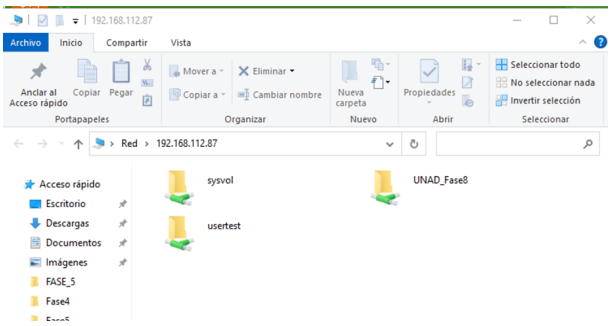

Imagen 66 File Server y Print Server

Para el funcionamiento del servicio de impresora, procedemos a realizar la instalación del servicio CUPS.

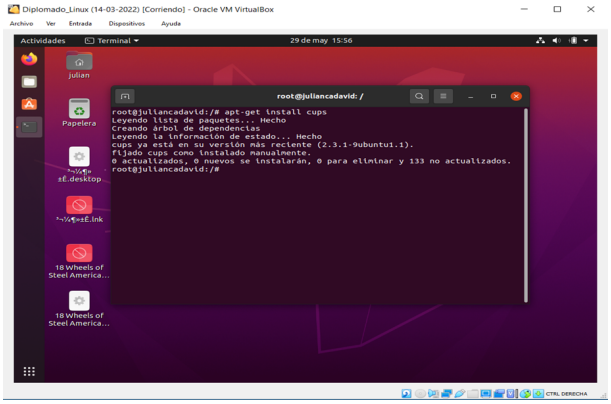

Imagen 67 File Server y Print Server

Ingresamos a la administración del servicio CUPS mediante la URL (localhost:631)

Imagen 68 File Server y Print Server

En este paso se realiza el proceso de añadir impresora seleccionada bien sea la que tengamos conectada vía USB de manera local o en red LAN.

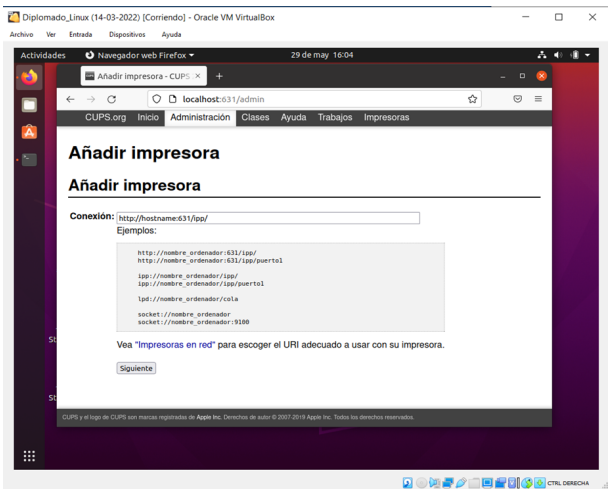

Imagen 69 File Server y Print Server

Luego de seleccionar la impresora requerida, podemos ver la configuración de manera exitosa, es decir que a nivel de red podemos realizar la respectiva conexión y obtener los respectivos (logs) de servicio de impresión.

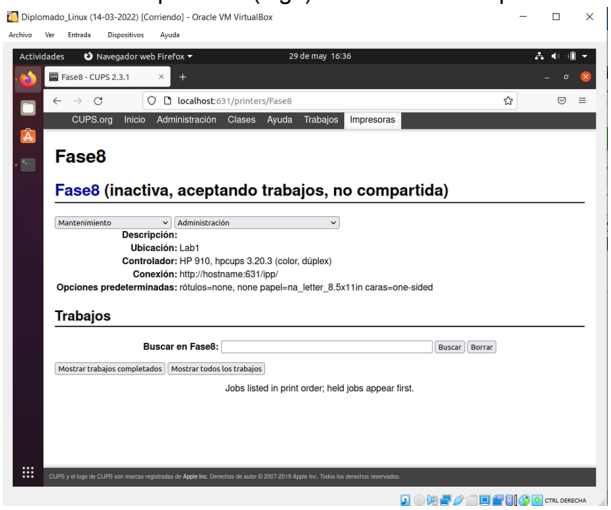

Imagen 70 File Server y Print Server

4.5 TEMÁTICA 5: VPN

Para contar con el servicio de servidor privado virtual desde Zentyal lo primero que se debe hacer es la instalación de los paquetes VPN y Certification Authority desde el menú Gestión de software, opción componentes de Zentyal

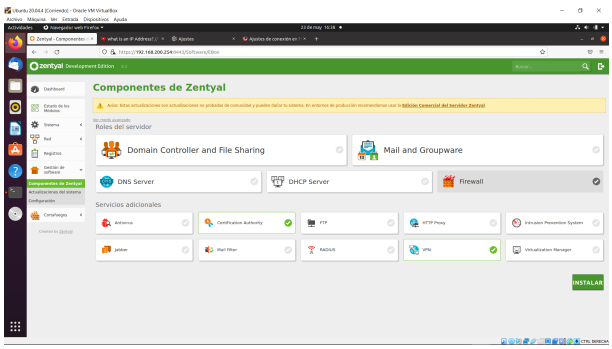

Imagen 71. Selección de los paquetes de instalación VPN

Luego de la instalación se deben habilitar los módulos y guardar cambios.

Desde la opción general, del menú autoridad de certificación se crea un nuevo certificado

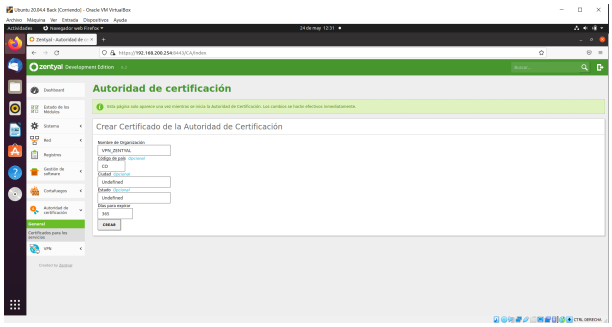

Imagen 72 . Creación de certificado de autoridad.

Se añade servidor VPN con el nombre VPNZENTYAL, se realiza la respectiva configuración para transmisión de datos con el protocolo UDP, puerto 1194, asignación de IP que creará el servidor y se guardan cambios

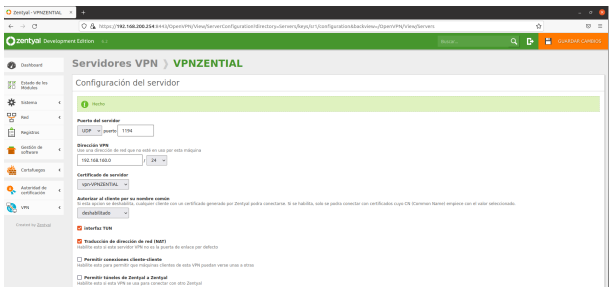

Imagen 73 . Configuración del servidor VPN

Se debe descargar el paquete de configuración del cliente que permitirá la conexión, se debe expedir primero un nuevo certificado para cada cliente que se vaya a conectar

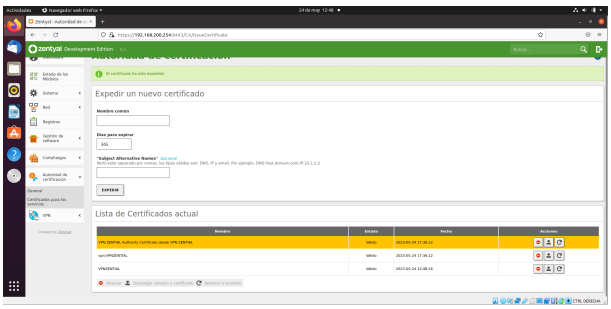

Imagen 74 . Expedición de certificado para cliente

Para realizar la descarga del paquete de configuración VPN que será utilizado en el cliente Ubuntu Desktop, se debe tener en cuenta que la dirección del servidor debe ser la IP del servidor Zentyal correspondiente a la red externa.

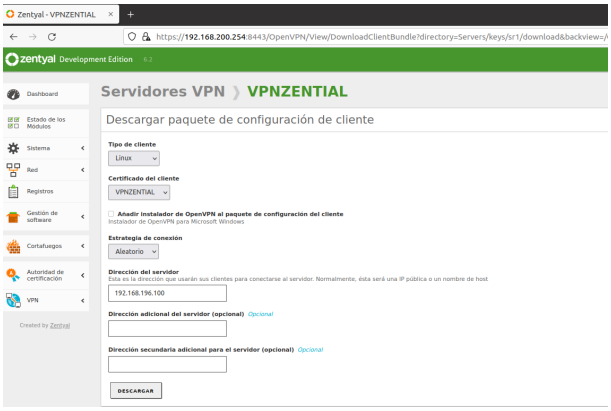

Imagen 75 . Configuración del paquete para el cliente

En el servidor Zentyal se adiciona un servicio, que en este caso fue llamado VPN, para permitir el tráfico VPN (abrir puerto 1194) antes de realizar la conexión. Se configura el servicio y se guardan cambios.

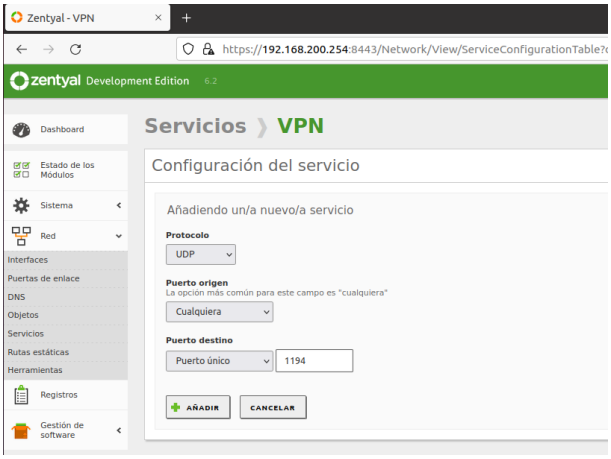

Imagen 76 . Creación y configuración del servicio VPN.

En el cortafuegos se deben configurar una regla de filtrado desde las redes internas a Zentyal, también una

regla de filtrado de redes externas a Zentyal y se guardan cambios.

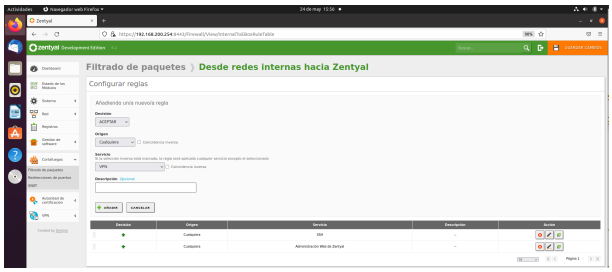

Imagen 77 . Regla de tráfico de redes internas a Zentyal

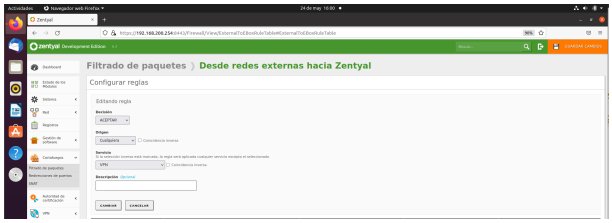

Imagen 78 . Regla de tráfico de redes externas a Zentyal

Estando en el cliente Ubuntu Desktop se descarga y descomprime el paquete de instalación creado en Zentyal

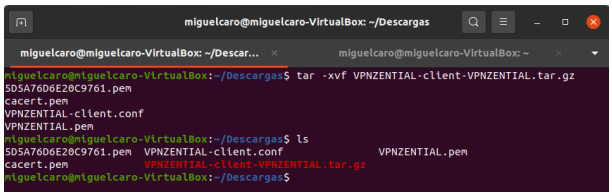

Imagen 79 . Descarga y descompresión del paquete VPN

En el cliente debe estar instalada la aplicación OpenVPN para poder aplicar el paquete de configuración generado en el servidor Zentyal. En este momento se verifica la IP y la interfaz que tiene el equipo cliente para ver los cambios que se producen al conectarse a la VPN.

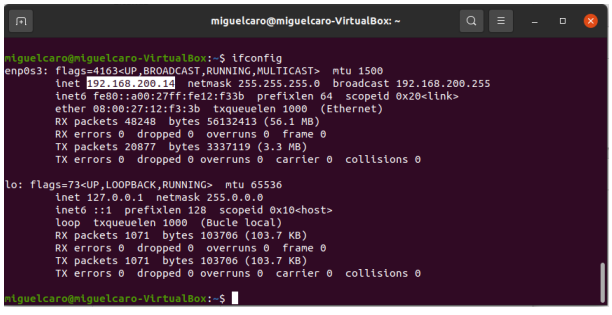

Imagen 80 . Configuración de red del sistema sin VPN

Desde la configuración de red se agrega una nueva conexión VPN compatible con el servidor OpenVPN

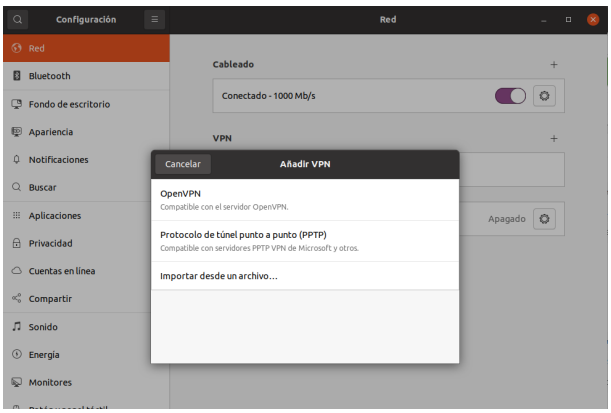

Imagen 81 . Creación de conexión VPN en el cliente

Se cargan los certificados que se descomprimieron y se activa la conexión VPN

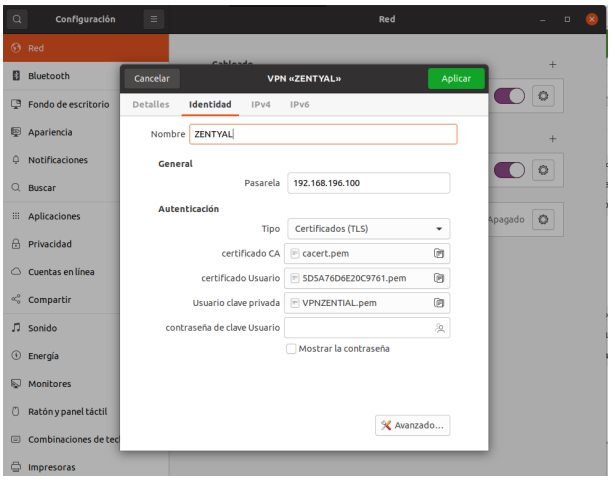

Imagen 82. Configuración de la conexión VPN

Al realizar esta conexión se puede observar por consola que se ha agregado una nueva ip (dentro del rango de las IP del servidor VPN) en el equipo cliente Ubuntu así como una nueva interfaz llamada tun0, tal como se habilitó en la configuración del servidor.

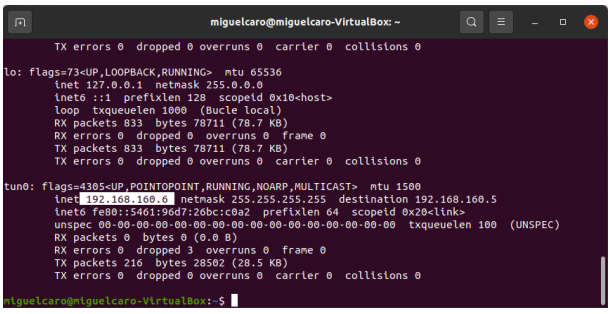

Imagen 83 . Configuración de red del sistema con VPN

También se puede observar en el cliente el icono de conexión a VPN

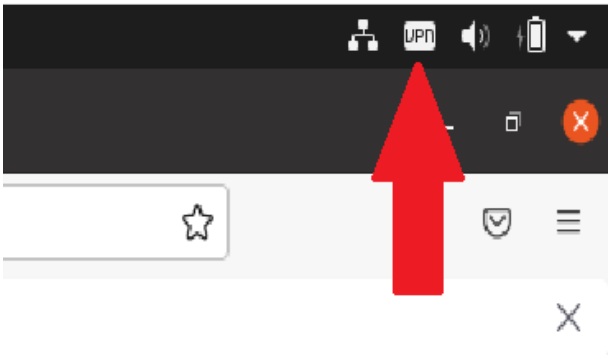

Imagen 84 . Prueba de conexión VPN en el equipo cliente.

En el panel de administración de Zentyal se puede observar un listado de las conexiones del cliente Ubuntu con la dirección IP 192.168.200.14 al servidor VPNZENTYAL generando un informe de registros del módulo VPN.

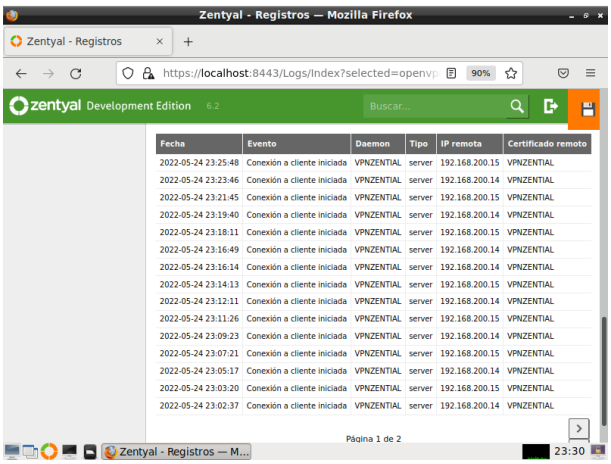

Imagen 85 . Informe de registros de conexión VPN

Finalmente se observa el acceso a Internet manteniendo la conexión VPN

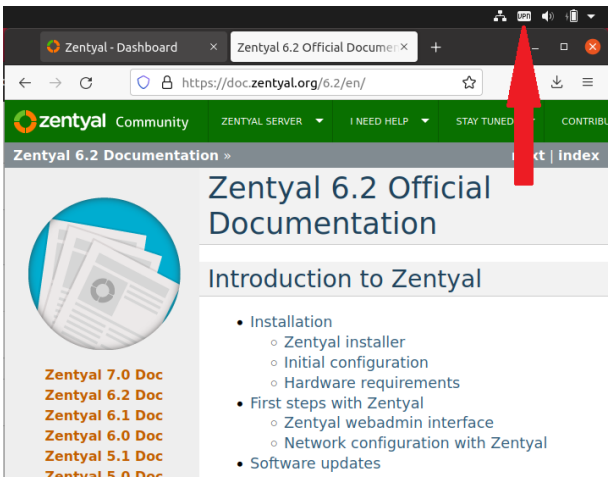

Imagen 85 . Acceso a Internet con VPN

5. CONCLUSIONES

El cortafuegos o firewall es un sistema indispensable para la seguridad de la información, permitiendo o limitando peticiones para que solo las direcciones en las que se confía puedan ser procesadas, evitando así que direcciones no seguras puedan acceder a la información del sistema y la pueda secuestrar o vulnerar de cualquier forma.

A través de la conexión al servidor desde un cliente con usuario y contraseña, tenemos la posibilidad de realizar trabajo remoto bajo los parámetros y configuraciones (proxy y firewall) del servidor, así como también si somos administradores realizar configuraciones en el servidor.

Zentyal ofrece una alternativa de conexión VPN integrada con OpenVPN, que se puede configurar desde un panel de control para gestionar redes privativas virtuales de forma sencilla, generar certificados de autoridad, permitiendo la conexión de equipos en una red interna con un equipo conectado a una red externa que provee Internet, todo a través de un túnel privado de comunicación que suministra al equipo cliente una dirección IP generada, sin tener que usar alguna en el rango de IP´s de la red real.

6. REFERENCIAS

[1]. *Zentyal 6.2 Documentación Oficial Documentación de Zentyal 6.2*. (2018). Zentyal. https://doc.zentyal.org/6.2/es/

[2]. *Cómo instalar y configurar LDAP Server Zentyal y Cliente Ubuntu 20.04*. (2021, 9 diciembre). Disponible en: https://www.youtube.com/watch?v=T6HMrDAi0gU

[3]. *Servicio de redes privadas virtuales (VPN) con OpenVPN. (2018). Documentación de Zentyal 6.2. Recuperado de https://doc.zentyal.org/es/vpn.html*

[4]. *Configuración general del Proxy HTTP con Zentyal. (2018). Recuperado de https://doc.zentyal.org/es/proxy.html*

[5]. *Servicio de resolución de nombres de dominio (DNS). (2018). Recuperado de https://doc.zentyal.org/es/dns.html#configuracion-de-un-servidor-dns-autoritario-con-zentyal*