

INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO ZENTYAL SERVER EN LA GESTIÓN DE INFRAESTRUCTURA TI

Uriel Andres Henao Gil
e-mail: uhenao@gmail.com
Esleida Marley Cárdenas Medina
e-mail: emcardenasme@unadvirtual.edu.co
Joseph Stiven Mosquera Rodriguez
e-mail: jsmosquero@unadvirtual.edu.co
Liceth Mallerly Gomez Moscoso
e-mail: lmgomezmos@unadvirtual.edu.co
Liza María Castrillón Pimienta
e-mail: lmcastrillonp@unadvirtual.edu.co

RESUMEN: El desarrollo de la actividad final del Diplomado de Profundización en Linux se realiza mediante el sistema operativo Zentyal Server, el cual se usa como base para disponer de los servicios de Infraestructura IT. Se realiza la instalación, configuración y puesta en marcha de los servicios de DHCP, DNS, Proxy, Cortafuegos, File Server y Print Server y VPN para finalmente poder acceder a estos servicios desde los equipos conectados dentro de la red, en este caso se comprueba mediante el sistema operativo Ubuntu Desktop el correcto funcionamiento de cada uno de los servicios configurados.

PALABRAS CLAVE: Cortafuegos, DHCP, File Server y Print Server, Zentyal Server

1 INTRODUCCIÓN

Este artículo contiene el desarrollo de la actividad propuesta en el Paso 8, la cual consiste en realizar la instalación y configuración de los servicios y plataformas de infraestructura IT a través del sistema operativo Zentyal Server de acuerdo a cada una de las temáticas.

2 INSTALACIÓN ZENTYAL SERVER

Zentyal es un sistema operativo basado en GNU/Linux que facilita la gestión de los servicios de infraestructura TIC como Servidor de Dominio y Directorio, Servidor de Correo, Gateway y Servidor de Infraestructura, Mantenimiento, Actualizaciones y Soporte, este último para la versión comercial.

Creamos la máquina virtual Zentyal por medio de Virtual Box, la cual configuramos con el archivo recomendado por el tutor (6.2) y la red Adaptador Puente.

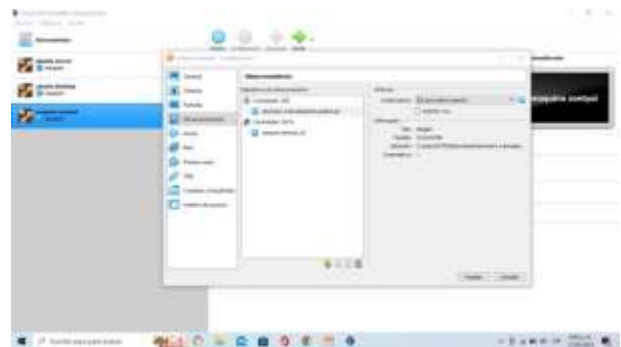


Figura 1. Configuración de almacenamiento.

Seleccionamos el idioma Español.



Figura 2. Configuración de idioma.

Seleccionamos la primera opción para instalar Zentyal.

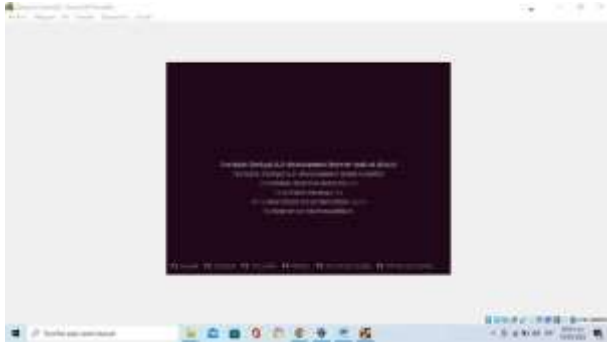


Figura 3. Instalación Zentyal.

Seleccionamos la distribución del teclado Spanish.



Figura 4. Distribución del teclado.

En la configuración de red seleccionamos la interfaz de red primaria eth0.



Figura 5. Configuración de red.

Configuramos el nombre de la máquina virtual.



Figura 6. Configuración del nombre de la máquina.

Configuramos el nombre de usuario para la cuenta.



Figura 7. Configuración nombre de usuario.

Ingresamos la contraseña para el usuario.



Figura 8. Configuración contraseña usuario.

Observamos que ha terminado la instalación de manera correcta y damos clic en continuar.



Figura 9. Instalación terminada.

Empieza a cargar el inicio de zentyal.



Figura 10. Inicio Zentyal.

3 TEMÁTICAS

3. 1 TEMÁTICA 1: DHCP SERVER, DNSSERVER Y CONTROLADOR DE DOMINIO

Lo primero que hacemos es activar el módulo de servidor DHCP desde el Modulo correspondiente, así como se puede ver en la imagen.



Figura 11. Activar módulo de servidor DHCP.

Configuramos y personalizamos nuestro servidor DHCP, colocando los datos que nos solicitan en esta sección.

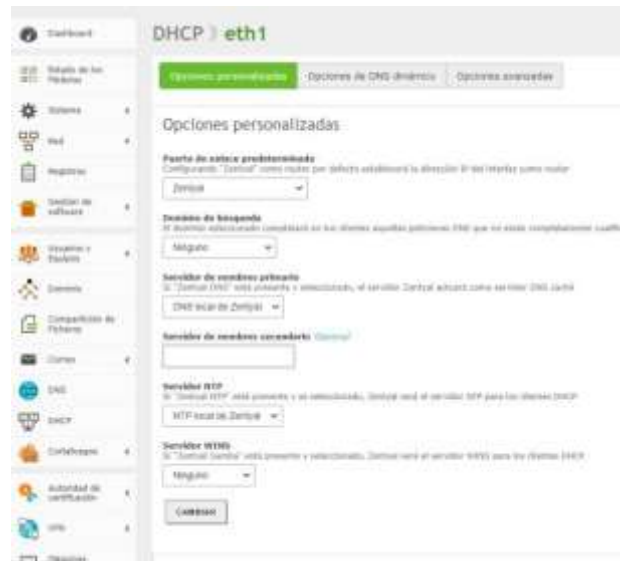


Figura 12. Configurar servidor DHCP.

Asignamos los rangos en los cuales nuestro servidor DHCP puede entregar Direcciones a los Clientes como se muestra en la imagen.



Figura 13. Configurar servidor DHCP.

Esperamos a que los cambios surtan efecto.

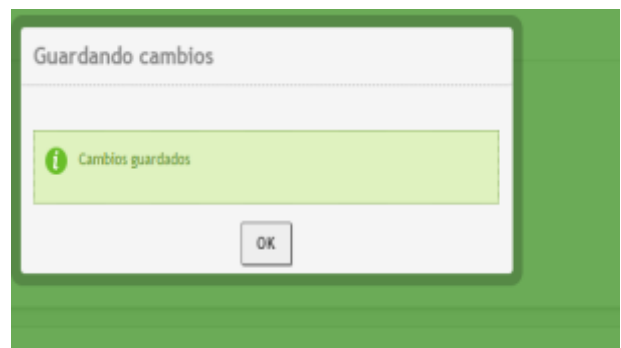


Figura 14. Guardar cambios.

Una vez guardados los cambios iniciamos una nueva máquina y verificamos si nuestros cambios tuvieron éxito, para esto nos damos cuenta que los datos de la red han cambiado a los datos asignados en nuestro

DHCP, además podemos verificar en el dashboard de Zentyal y vemos como nos muestra las conexiones y los equipos conectados a este servidor.

```

Adaptador de Ethernet Ethernet 1:
Su fijo DNS específico para la conexión. . . : uriel.com
Vínculo dirección IPv6 local. . . : fe80::11de:2579:F918:c9a45%
Dirección IPv4. . . : 192.168.2.4
Máscara de subred. . . : 255.255.255.0
Puerta de enlace predeterminada. . . : 192.168.2.1
C:\Users\uriel-95
  
```

Figura 15. Validar servidor DHCP.

| IPs asignadas con DHCP | | |
|------------------------|-------------------|-------------------|
| Dirección IP | Dirección MAC | Nombre de máquina |
| 192.168.2.3 | 08:00:27:75:21:70 | DESKTOP-SESONRQ |
| 192.168.2.4 | 08:00:27:14:82:49 | DESKTOP-SESONRQ |

Figura 16. Validar servidor DHCP.

3. 2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Procederemos entonces a hacer la configuración inicial y la instalación de Zentyal.



Figura 17. Selección de paquetes de Zentyal.

Seleccionaremos los servicios que vayamos a utilizar, en este caso la temática nos dice que tenemos que crear un Proxy no transparente, por lo tanto, añadiremos el servicio HTTP Proxy.



Figura 18. Confirmación de paquetes a instalar.



Figura 19. Proceso de instalación de los paquetes.



Figura 20. Proceso de instalación de los paquetes.



Figura 21. Instalación de los paquetes completada.

Procedemos a activar el módulo HTTP Proxy, para ello en el Dashboard de Zentyal nos dirigimos a la sección Estado de los módulos y activamos la casilla de HTTP Proxy.

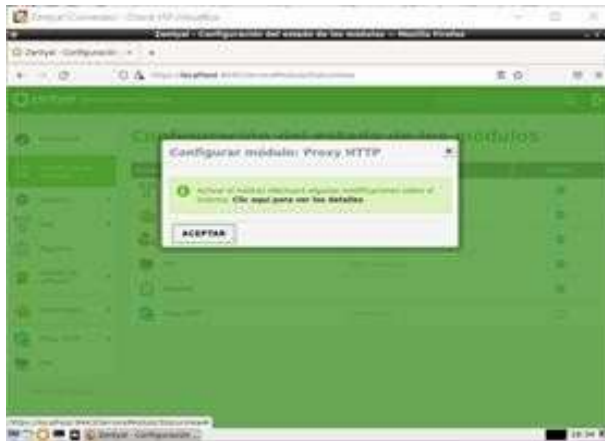


Figura 22. Activación del módulo HTTP Proxy.



Figura 23. Módulo Proxy HTTP activado.

Procedemos a dirigimos a la sección de Proxy HTTP, Configuración general y allí procederemos a configurar nuestro Proxy no transparente.



Figura 24. Configuración general de HTTP Proxy.

Deshabilitamos la opción de Proxy transparente y establecemos el puerto en el que queremos filtrar que en este caso es el puerto 1320.



Figura 25. Estableciendo la configuración general de HTTP Proxy.

Procedemos ahora a testear nuestro Proxy no transparente, bloqueando el acceso a algunas páginas en este caso serán algunas páginas de juegos. Para ello nos dirigiremos a la sección de Perfiles de filtrado y crearemos el perfil para bloquear algunas páginas de juegos.



Figura 26. Configuración del Perfil de filtrado.



Figura 27. Perfil de filtrado añadido.

Una vez creado el perfil, procedemos a configurarlo, para ello presionamos el icono de engranaje y cuando estemos dentro de la página nos dirigimos a la parte de Reglas de dominios y URLs y procedemos añadir las respectivas URLs de los sitios que queremos bloquear acceso.



Figura 28. Configuración de Reglas de dominios y URLs.



Figura 29. Reglas de dominios y URLs añadidas.

Procedemos en nuestro navegador en el sistema de escritorio, configurarlo para conectarlos a la dirección IP de nuestro proxy y el puerto que establecimos. Para ello en la configuración de nuestro navegador en el escritorio, establecemos la configuración del proxy que en este caso es la dirección IP del servidor Zentyal y el puerto 1320 que establecimos anteriormente.

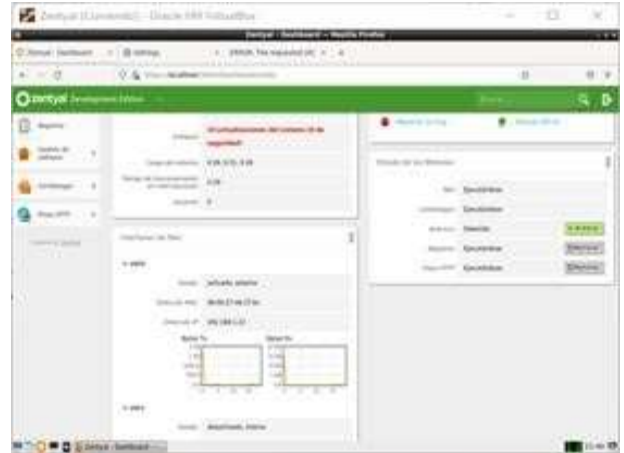


Figura 30. Vista del Dashboard de Zentyal.



Figura 31. Búsqueda de Proxy en configuración de Mozilla Firefox.



Figura 32. Configuración de Proxy.

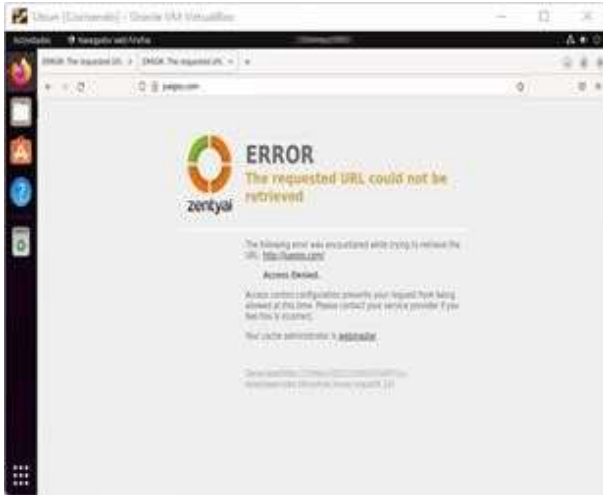


Figura 33. Muestra 1 acceso denegado a juegos.com.

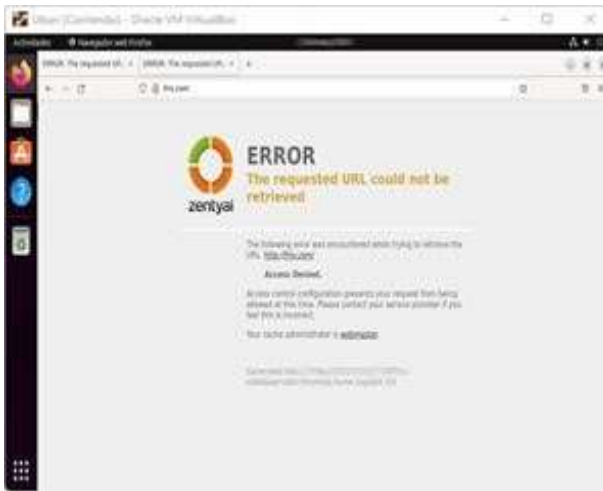


Figura 34. Muestra 2 acceso denegado a friv.com.

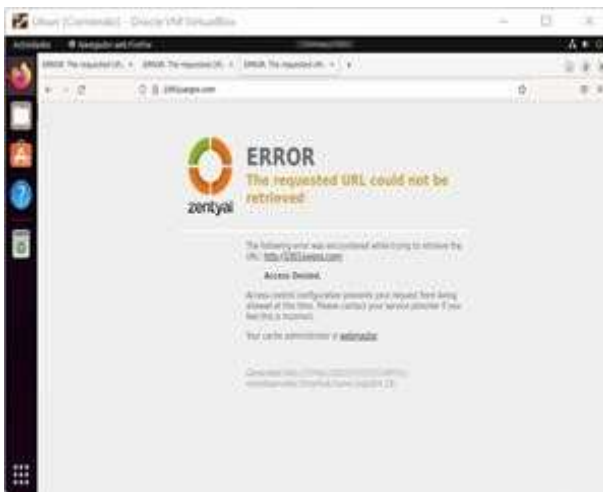


Figura 35. Muestra 3 acceso denegado a 1001juegos.com.

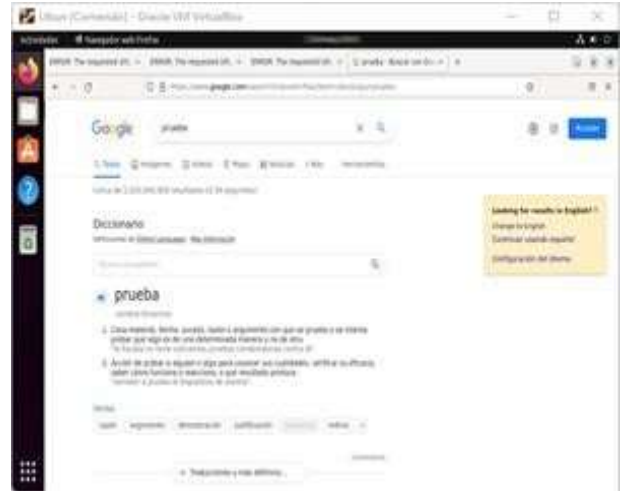


Figura 36. Prueba de la denegación de acceso solo en las páginas establecidas.

De esta manera tendríamos configurado nuestro Proxy no transparente, si queremos seguir con la configuración del proxy como lo es la limitación por ancho de banda o la listas por categoría podríamos acceder desde la misma sección de HTTP Proxy

3. 3 TEMÁTICA 3: CORTAFUEGOS

Lo primordial para el desarrollo de esta temática es hablar un poco sobre la configuración de red de nuestras máquinas virtuales.

Para nuestra máquina virtual que será nuestro servidor Zentyal dispondrá de las siguientes configuraciones de red:

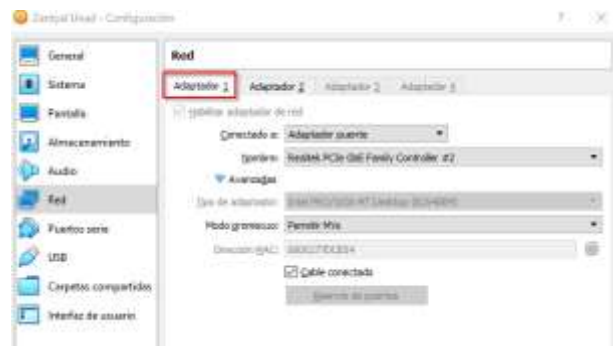


Figura 37. Configuración de red - Máquina virtual del Servidor Zentyal.

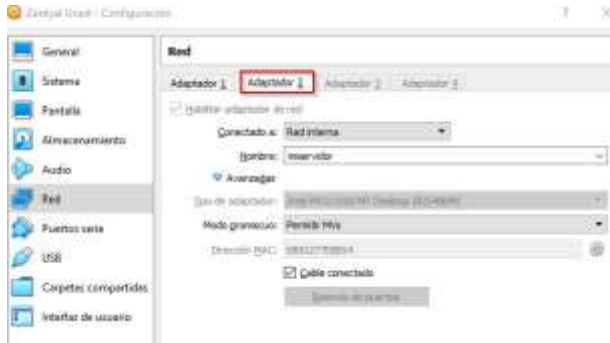


Figura 38. Configuración de red - Máquina virtual del Servidor Zentyal.

Por último, nuestra máquina virtual que será nuestro cliente o estación de trabajo dispondrá de la siguiente configuración de red:



Figura 39. Configuración de red - Máquina virtual del Cliente.

Teniendo muy en cuenta las configuraciones pertinentes para nuestras máquinas virtuales, se procede dar uso al paquete o módulo Firewall en nuestro Zentyal Server previamente ya instalado.

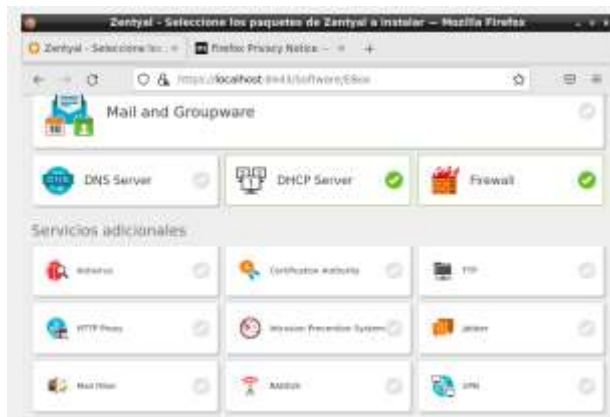


Figura 40. Servicio Firewall implementado.



Figura 41. Servicio Firewall implementado.

Accedemos a la sección de red, para visualizar las interfaces de red.



Figura 42. Interfaces – Red.

Se procede en configurar el eth0. Este tendrá una IP estática externa que esté disponible en nuestra red física. Además, esta IP representará a nuestro servidor Zentyal.

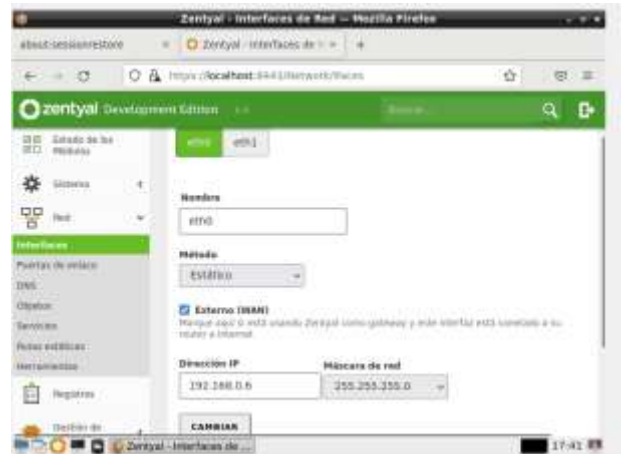


Figura 43. Configuración Interfaces de red.

Para nuestro eth1 manejará una misma configuración, una IP estática, solo que será de manera interna. (Este se usará de puerta de enlace para nuestro cliente).

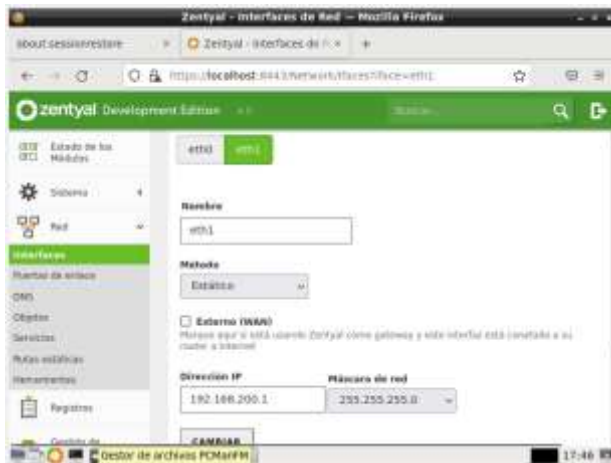


Figura 44. Configuración Interfaces de red.

Ya concluida la configuración de nuestras interfaces de red, nuestro siguiente paso es configurar las puertas de enlace y el DNS de la red.



Figura 45. Configuración puerta de enlace y DNS.

Configuración de la puerta de enlace para nuestro eth0 de la red Zentyal server:

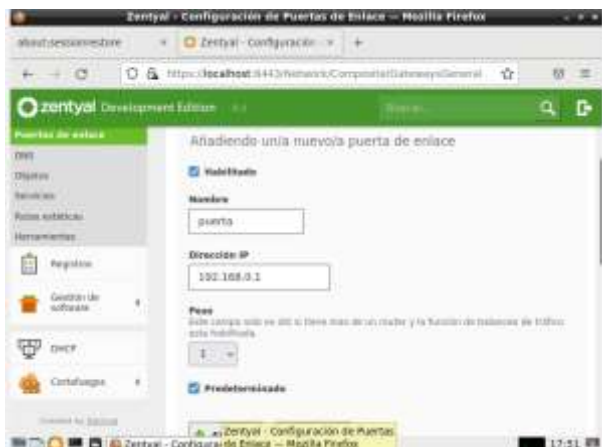


Figura 46. Configuración puerta de enlace.

Configuración de nuestro DNS de la red Zentyal server, aquí se ha tomado el DNS de 8.8.8.8 (el cual es de Google).



Figura 47. Configuración DNS.

Ya configurada toda la sección de la red. Se pasará a configurar el DHCP el cual se encargará de entregar de manera automática la IP correspondiente para nuestro cliente o estación de trabajo que se encuentre conectada a nuestra red interna de Zentyal Server.

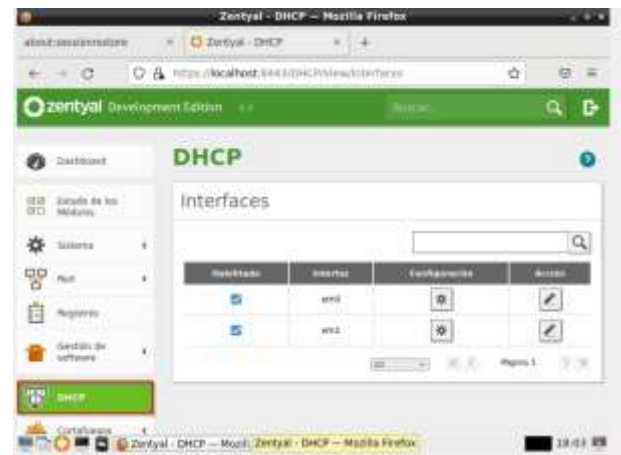


Figura 48. Configuración DHCP.

Accedemos al eth1 para añadir un nuevo rango de nuestros IP's a asignar.



Figura 49. Añadir Rango IP del eth1.

Como previamente en nuestra configuración de la IP estática del eth1 inicia como 192.168.200.1, nuestro rango ha de iniciar de 192.168.200.1 para 192.168.200.254.



Figura 50. Añadir Rango IP del eth1.

Añadido ya el rango, el resultado será el siguiente:



Figura 51. Resultado Rango IP.

Ya hecha estas configuraciones primordiales, nuestra estación de trabajo o el cliente que se encuentre conectada a la red interna, se reflejará la asignación IP de

manera automática, entregada por nuestro servidor Zentyl. Además, contará con conexión a Internet.



Figura 52. Conexión Cliente.



Figura 53. Conexión Cliente.

Ahora bien, nuestra necesidad o requerimiento a cumplir es bloquear aquellas determinadas páginas web para nuestro cliente.

Para este caso tomaremos las siguientes páginas web que son: Facebook de España y Google México.



Figura 54. Facebook de España antes de ser bloqueada.



Figura 55. Google México antes de ser bloqueada.

Ya identificadas nuestras páginas a bloquear, procedemos a usar el siguiente comando para identificar el IP de dichas páginas mediante sus respectivos dominios.

```

joseph@zentyal(1193525003)-$ nslookup es-es.facebook.com
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
es-es.facebook.com canonical name = star.facebook.com.
star.facebook.com canonical name = star.c10r.facebook.com.
Name:   star.c10r.facebook.com
Address: 157.240.6.18
Name:   star.c10r.facebook.com
Address: 2a03:2880:f02b:11:face:b00c:0:2
  
```

Figura 56. Nslookup Facebook España.

```

joseph@zentyal(1193525003)-$ nslookup www.google.com.mx
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com.mx
Address: 142.250.78.131
Name:   www.google.com.mx
Address: 2800:3f0:4005:40b::2003
  
```

Figura 57. Nslookup Google México.

Podemos observar que nos ha arrojado el respectivo IP de la página web, cosa tal que usaremos en nuestro servidor Zentyal.

Procedemos en acceder a nuestro Cortafuegos o Firewall. En la sección de filtrado de paquetes y la configuración de reglas de filtrado para las redes internas.



Figura 58. Reglas de filtrado para las redes internas.

Nos redirige a las reglas existentes de nuestra red interna. De allí se añadirá las siguientes reglas de filtrado:

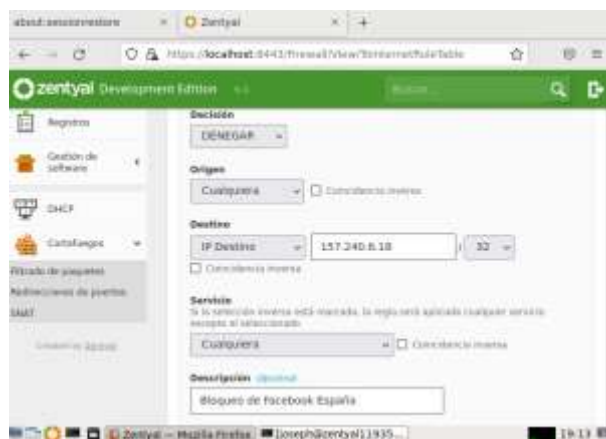


Figura 59. Bloqueo Facebook España.

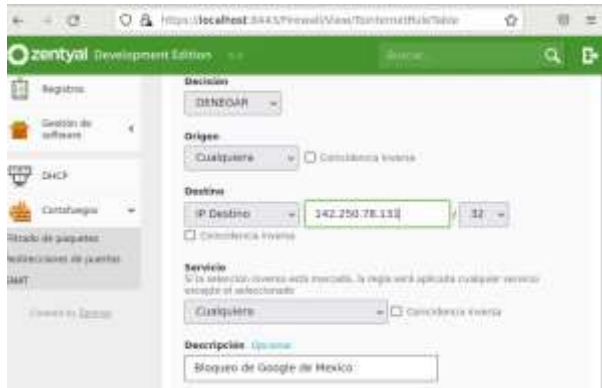


Figura 60. Bloqueo Google México.

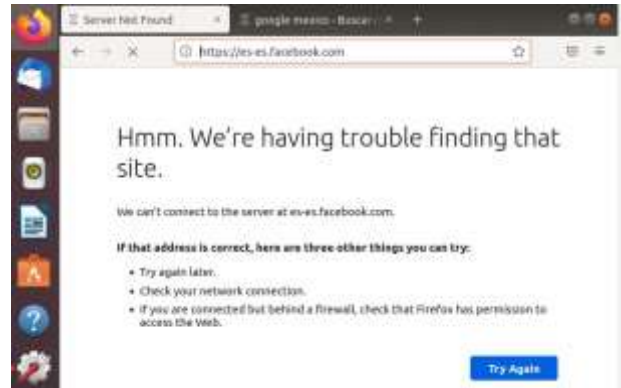


Figura 63. Conexión no permitida – Google México



Figura 61. Reglas de filtrado – Red Interna.

Ahora validamos de nuestra estación de trabajo o cliente Linux el bloqueo de dichas páginas por nuestro Firewall establecido por el Servidor Zentyal.

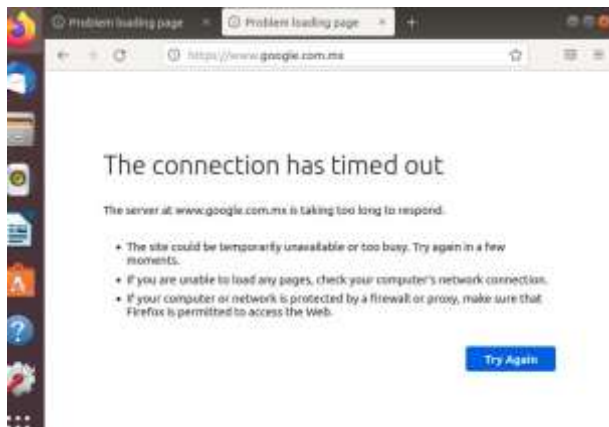


Figura 62. Conexión no permitida – Facebook España.

3. 4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Instalamos el servicio “Domain Controller and File Sharing”.



Figura 64. Instalación de servicios.

Configuramos la Interface de red de tipo Internal por el método Static.



Figura 65. Configuración de red.

Activamos el módulo de controlador de dominio y compartición de archivos.

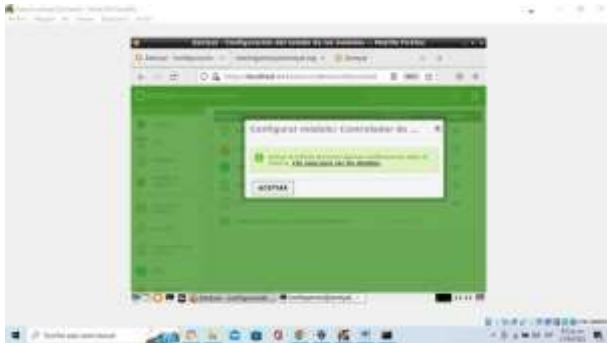


Figura 66. Activar módulos.



Figura 69. Configuración control de acceso.

Creamos los grupos y usuarios que consideramos necesarios.

Instalamos el servidor Samba (permite a las distribuciones de Linux/Ubuntu compartir archivos e impresoras con cualquier otro dispositivo conectado a la red).



Figura 67. Configuración de usuarios y equipos.

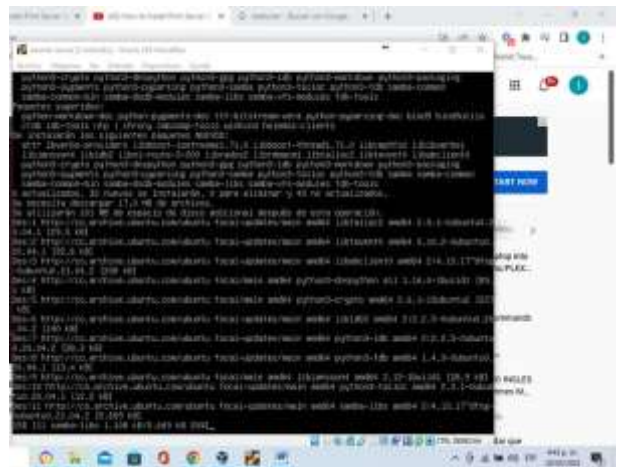


Figura 70. Instalación servidor Samba.

Añadimos una nueva compartición de ficheros.

Accedemos al archivo de configuración smb.conf, agregamos el parámetro security=user y en la etiqueta pinterms le ponemos yes los parámetro browseable y quest ok.



Figura 68. Configuración compartición de ficheros.

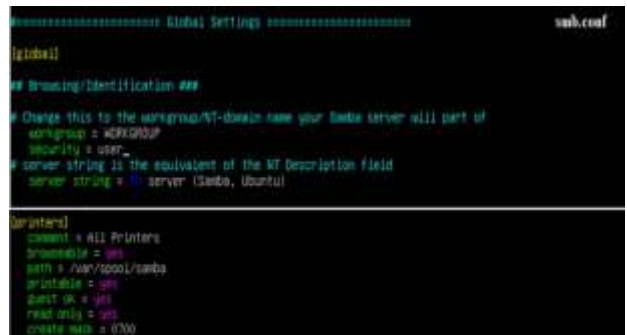


Figura 71. Configuración Samba.

Configuramos el control de acceso (Usuario/Grupo - Permiso).

Reiniciamos el servidor de samba para aplicar todos los cambios.

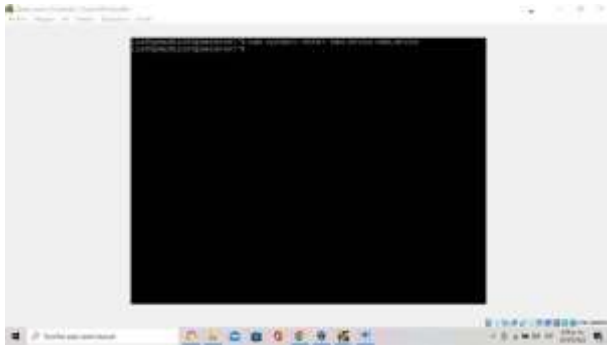


Figura 72. Reiniciar Samba.

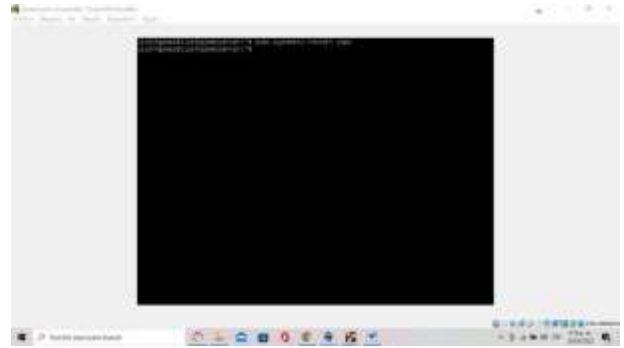


Figura 75. Reiniciar CUPS.

Instalamos el servidor CUPS (Sistema de impresión que permite configurar un equipo como servidor de impresión en Linux, puede administrar impresoras desde ordenadores cliente).

Ingresamos a ubuntu desktop y configuramos la conexión al servidor mb://192.168.101.13/.

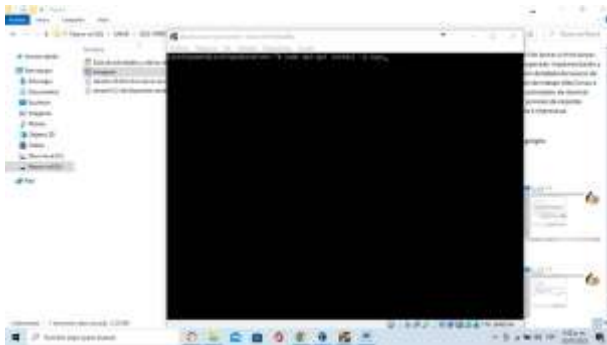


Figura 73. Instalación servidor CUPS.

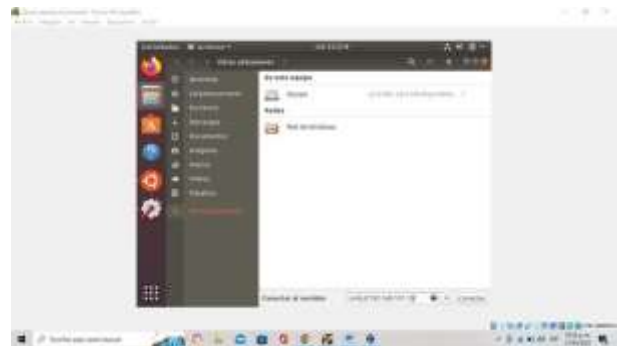


Figura 76. Conexión al servidor.

Accedemos al archivo de configuración cups.conf, reemplazamos Listen localhost:631 por Port 631 y agregamos el parámetro Allow all.

Una vez conectados podemos observar la carpeta compartida "biblioteca".

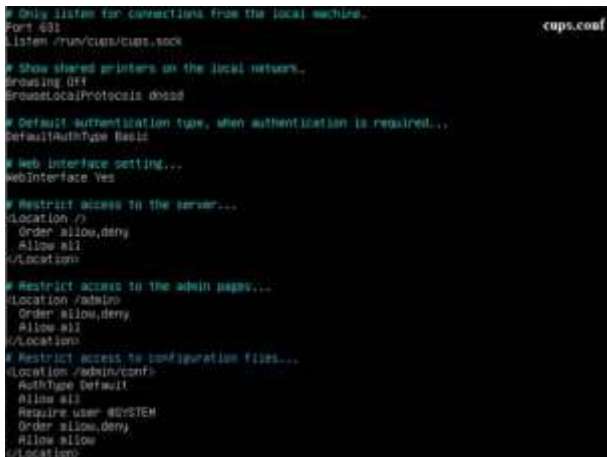


Figura 74. Configuración CUPS.

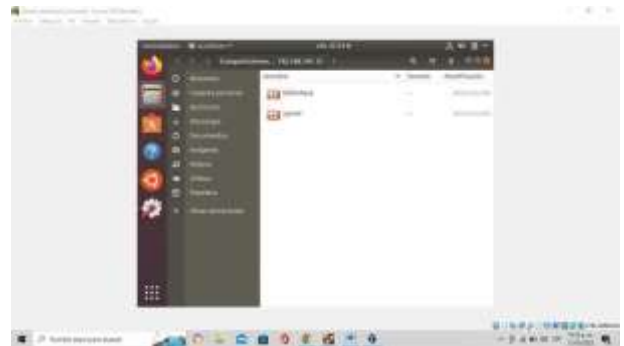


Figura 77. Carpeta compartida.

Reiniciamos el servicio de impresión CUPS para que tome los cambios realizados.

Para acceder a la carpeta ingresamos usuario y contraseña.

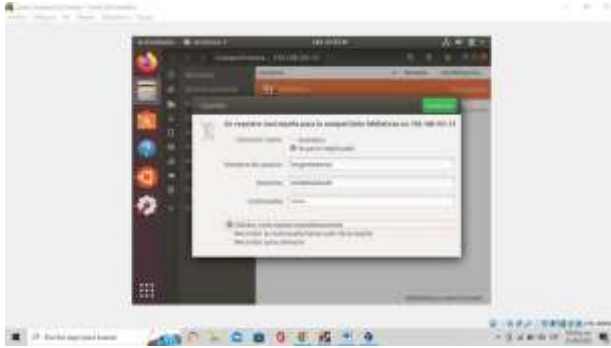


Figura 78. Usuario y contraseña para acceder a la carpeta.

Podremos realizar acciones de acuerdo a los permisos que tenga asignado el usuario.



Figura 79. Permiso del usuario.

Abrimos el navegador e ingresamos la ip del ubuntu server con el puerto 631 donde podemos administrar el print server.



Figura 80. Administración de impresoras.

En la configuración de dispositivos añadimos la nueva impresora CUPS.



Figura 81. Añadir impresora CUPS.

Una vez añadida la impresora podemos verla disponible.



Figura 82. Impresora CUPS.

3. 5 TEMÁTICA 5: VPN

Para la creación del VPN, se realiza la instalación del paquete de VPN desde el menú gestión del software e instala el paquete de VPN en Zentyal y se activa. Para este proceso se procede a crear los certificados de autorización para comenzar con la configuración de la VPN.

Seleccionamos los servicios a instalar. Hacemos clic en instalar.



Figura 83. Seleccionar módulos a instalar en Zentyal Server.

Procedemos a configurar las interfaces externas que conectan con la red.



Figura 84. Configuración interfaz de red en Zentyal Server.



Figura 85. Configuración interfaz de red en Zentyal Server.

Termina la instalación. Hacemos clic en ir al Dashboard. Se abre la página principal del administrador del servidor.

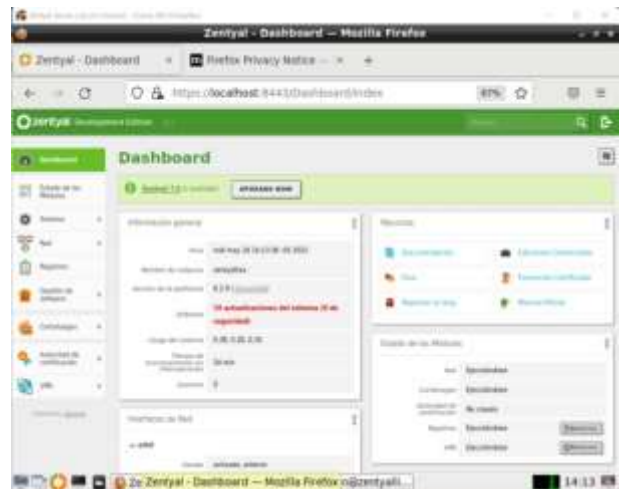


Figura 86. Página principal del administrador de Zentyal Server.

Hacemos clic en la pestaña VPN, en ella nos solicita crear un certificado para poder usar el servidor, hacemos clic en módulo de autoridad de certificación y creamos el certificado.



Figura 87. Pestaña VPN en Zentyal Server.

Creamos el certificado ingresando los datos solicitados.



Figura 88. Crear autoridad de certificación.

Validamos que se encuentre creado y en estado valido el certificado anteriormente creado.



Figura 89. Validar la certificación anteriormente creada.

Procedemos a guardar los cambios realizados en el servidor.



Figura 90. Guardar cambios.

Procedemos Crear el Servidor VPN, para ello volvemos a dar clic en la pestaña VPN, seleccionamos servidores. Se abre la interfaz que aparece a continuación y hacemos clic en AÑADIR NUEVO/A.



Figura 91. Crear un servidor VPN.

Seleccionamos Habilitado, para habilitar el servidor e ingresamos el nombre que deseamos poner, para este caso ingresamos VPNLiza. Hacemos clic en añadir.



Figura 92. Crear un servidor VPN.

Validamos que el servidor se encuentre creado y habilitado.



Figura 93. Validar la creación del servidor.

Procedemos a configurar el servidor VPN, para ello hacemos clic en configuración y observamos se abre la siguiente interfaz, ingresamos los datos que nos solicita, para este caso solo ingresamos los datos de certificado de servidor y en interfaz a escuchar seleccionamos todas las interfaces de red, las demás configuraciones las dejamos por default.



Figura 94. Configuración del servidor VPN.



Figura 95. Configuración del servidor VPN.

Validamos que la configuración del servidor se haya guardado.



Figura 96. Configuración del servidor VPN.

Regresamos a la interfaz del servidor VPN y hacemos clic en descargar paquete de configuración de cliente, esto con el fin de posteriormente configurar los equipos clientes del servidor.



Figura 97. Validar la creación del servidor VPN.

En la interfaz que se abre nos informa que no hay certificados disponibles para este cliente. Por favor crear uno. Debemos hacer clic en crear uno.



Figura 98. Configuración del servidor VPN.

A continuación, ingresamos los datos que nos solicita, ingresamos el nombre, los días para expirar y hacemos clic en expedir.



Figura 99. Configuración del servidor VPN.

Posterior a ello se abre la interfaz en la cual nos permite descargar el paquete de configuración del cliente, como vamos a conectar nuestro equipo anfitrión que para este caso es Windows, seleccionamos en tipo de cliente a Windows, seleccionamos el certificado de cliente, en estrategia de conexión dejamos en Aleatorio, ingresamos la Ip del servidor Zentyal Server y hacemos clic en descargar.



Figura 100. Configuración del servidor VPN.

4 CONCLUSIONES

La implementación de servicios tales como DHCP, DNS y control de dominio permite tener flexibilidad dentro de una red estableciendo los parámetros necesarios para la administración y utilización de servicios permitiendo tener una conexión segura, estableciendo rangos específicos en el servicio. El control de dominio permite tener un control sobre los equipos registrados sobre el servidor.

La implementación de servicios de infraestructura IT que nos ofrece Zentyal Server nos permite dar solución a muchas problemáticas en especial a aquellas que están más dirigidas a un entorno local, en este caso con la implementación de un Proxy no transparente podemos

restringir el consumo de diversas páginas que decidamos establecer.

Zentyal Server nos ofrece muchas opciones de control de zona DMZ, aunque esta es una versión gratuita y de open source, también se puede contar con un software privativo que cuenta con muchas más facilidades.

El Proxy no transparente lo usamos principalmente para proteger la identidad de las verdaderas conexiones IP que acceden a Internet.

Durante el desarrollo de la actividad, se demuestra la habilidad para la puesta en marcha del Sistema Operativo Zentyal Server tanto su instalación y configuración. Además, se demuestra la habilidad para con la implementación del servicio Cortafuego al sistema operativo Zentyal Server.

Zentyal Server se especializa en ofrecer servidores con módulos, es decir, Zentyal Server puede ser instalado con fines de firewall o servidor de infraestructura, esto va dependiendo de los paquetes instalados.

A través del desarrollo de la presente actividad fue posible conocer y aprender sobre el sistema operativo GNU/Linux Zentyal Server, al igual que su instalación y configuración para disponer de los servicios de Infraestructura IT, conocer las principales características que nos ofrece esta herramienta para cada uno de los servicios, especialmente para los servicios de File Server y Print Server, los cuales trabajen en la temática elegida

La realización de la presente actividad nos proporcionó las herramientas montar un servidor VPN con conexión a una red local por medio del sistema operativo Zentyal server 6.2. en el desarrollo de esta actividad se pudo poner en practica todos los conocimientos adquiridos a lo largo del curso y poder comprender el funcionamiento de los SO GNU/Linux tanto en Desktop como en Servidores.

5 REFERENCIAS

- [1] Borges, S. (2019, August 27). Servidor Proxy: ¿Qué es? Características, Tipos y Ventajas de usar uno. Infranetworking. Retrieved May 25, 2022, from <https://blog.infranetworking.com/servidor-proxy/>
- [2] EL CANAL DE DANNY. (2018, July 12). Descargar e Instalar Zentyal 5.1 / VirtualBox. YouTube. Retrieved May 25, 2022, from <https://youtu.be/PjvqkIXW4pc>
- [3] Instalación y configuración del Servidor Zentyal en zona DMZ del cortafuegos Endian - 10596/38552. (n.d.). Repositorio Institucional UNAD. Retrieved May 25, 2022, from <https://repository.unad.edu.co/handle/10596/38552?show=full>
- [4] JGAITPro. (2014, May 7). Zentyal - Instalar y configurar Proxy Web HTTP Transparente. YouTube. Retrieved May 25, 2022, from <https://youtu.be/X54YKfeFQhQ>
- [5] Zentyal. (n.d.). Gestión de máquinas virtuales — Documentación de Zentyal 7.0. Zentyal 7.0 Documentation. Retrieved May 25, 2022, from <https://doc.zentyal.org/es/virt.html>
- [6] Offensive Security. (2020). Kali dentro de VirtualBox (VM invitada). Kali. <https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/>
- [7] Jorba, J. (2012). Administración de seguridad. Páginas (27 – 33). OpenAccess. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo4_Administraci%C3%B3n%20de%20seguridad.pdf
- [8] Muhammad Arifin, F., Andriana Mutiara, G., & Ismail, I. (2017). Implementation of Management and Network Security Using Endian UTM Firewall. (Páginas. 1 - 9). ebscohost. <http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C2217DD&lang=es&site=eds-live&scope=site>
- [9] Canonical (2020). cuentas de usuario Ubuntu 18.04 LTS. Help Ubuntu. [En línea]. Disponible en: <https://help.ubuntu.com/stable/ubuntu-help/user-accounts.html.es>
- [10] Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. [En línea]. Disponible en: <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=219>
- [11] Apache/2.4.7 (Ubuntu) Server at download.zentyal.com Port 80. (2022). Retrieved from <http://download.zentyal.com/>
- [12] Arevalo, M. S. (2022, Mayo 16). Web conferencia académica Paso 8 curso DPL 16-1-Grabación de la reunión.mp4. Retrieved from Drive: <https://drive.google.com/file/d/1UGXGmYcKMCWzI67cj6O0NQxvQ0FqRg/view>
- [13] OpenVPN, Inc. (2022). Cliente OpenVPN 3 para Linux. Retrieved from OPENVPN: <https://openvpn.net/cloud-docs/openvpn-3-client-for-linux/>
- [14] Zentyal S.L. (2022). Zentyal 6.2 Documentación Oficial. Retrieved from zentyal community: <https://doc.zentyal.org/6.2/es/>