# Despliegue de solución global de seguridad y servicios TI a la medida basados en Zentyal Server

**Juan Pablo Zapata, Fabián Andrés Martínez, Luis Andrés Murcia, Ángela Adriana Pulido, Edgar Mauricio Cárdenas**

*ECBTI, Universidad Nacional Abierta y A Distancia UNAD*

*Bogotá, Colombia*

juan.pablo.zapata.gonzalez@gmail.com

fama2091@gmail.com

lamurcia0@unadvirtual.edu.co

angelap8118@gmail.com

emcardenasc@unadvirtual.edu.co

**ABSTRACT: Final step of the migration and start of the requested requirements in relation to the administration and control of a Linux distribution for this case Zentyal Server. It is oriented to the implementation of higher-level IT infrastructure services for Intranet and Extranet such as: DHCP Server, DNS Server, Domain Controller, Non-transparent Proxy, Firewall, File Server, Print Server and VPN.**

**RESUMEN:** ***Paso final de la migración y arranque de los requerimientos solicitados en relación con la administración y control de una distribución Linux para este caso Zentyal Server. Está orientada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet como son: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Sprint Server y VPN.***

**PALABRAS CLAVE: Zentyal, Dominio, Proxy, DHCP, DNS, Cortafuegos, VPN, Usuario, Interfaces, IP.**

## I. INTRODUCCIÓN

Linux facilita la administración de servidores, para ingenieros no relacionados con manejo de consola de comandos su implementación y configuración pueden ser procesos relativamente complejos. La distribución Zentyal se convierte en una alternativa eficiente tanto para ingenieros como para medianas y pequeñas empresas; posee un entorno amigable y simplicidad en sus procesos. Al permitir interfaz gráfica tipo web, su administración es intuitiva para una configuración rápida y segura.

## II. SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

### *A. INSTALACIÓN Y CONFIGURACIÓN ZENTYAL*

Se crea la máquina virtual

***Fig. 1 Configuración VM***

Se realiza descarga de la ISO de la página : http://www.zentyal.org/server/


***Fig. 2 URL descarga***

Se ingresa a configuración y se crean dos adaptadores o tarjetas de red

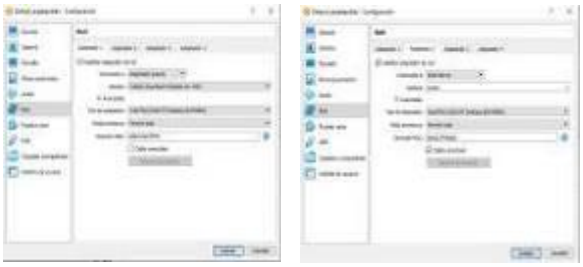

*Fig. 3 Configuración tarjetas de red VirtualBox*

Buscamos la ISO descargada.

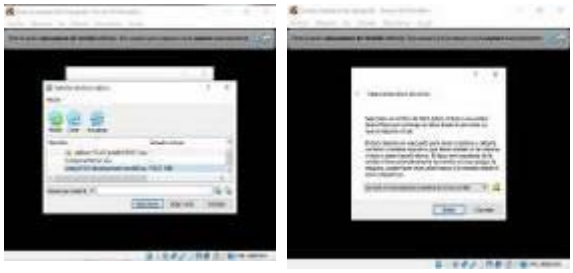

*Fig. 4 Selección ISO*

Configuramos Zentyal

*Fig. 5 Inicio instalación Zentyal*


*Fig. 6 Proceso instalación Zentyal*

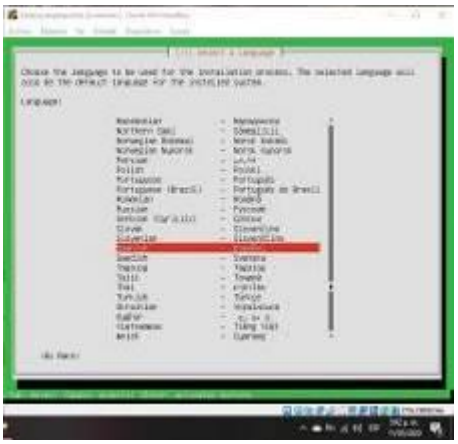

*Fig. 7 Selección de idioma*

*Fig. 8 Ubicación geográfica*

*Fig. 9 Configuración del teclado*

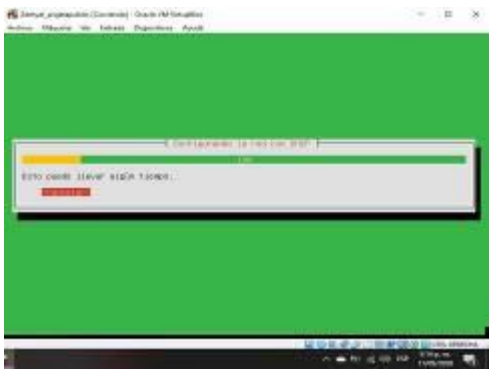

*Fig. 10 Tarjetas de red Zentyal*

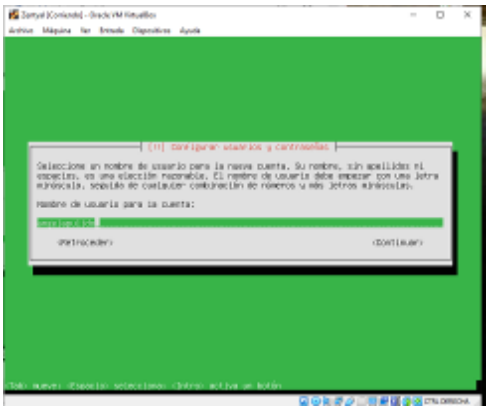

*Fig.11 Configuración de usuarios*

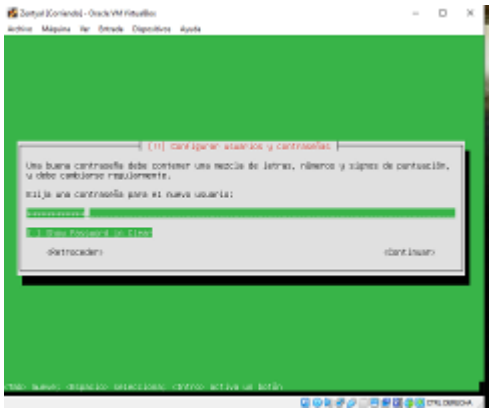

*Fig.12 creación de contraseña*

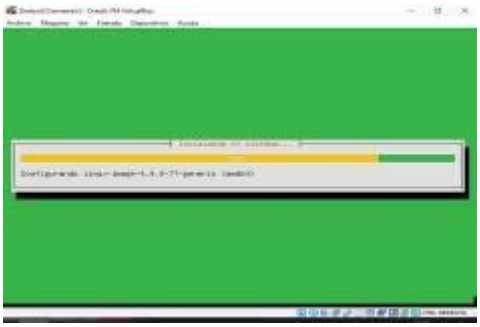

*Fig. 13 Instalación binarios*

*Fig. 14 Configurando APT*

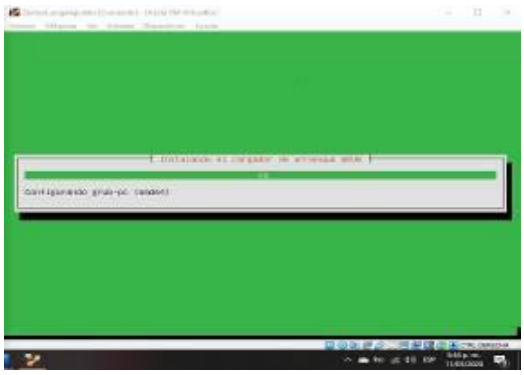

*Fig. 15 Instalación GRUB*

*Fig. 16 Fin instalación*

Se reinicia el sistema como paso final.

### *B. TEMÁTICA 1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO: JUAN ZAPATA*

Una vez instalado se procede con configuración de Controlador de Dominio standalone.
Iniciada la VM automáticamente se abre URL de administración de SO, usar usuario/contraseña creada durante instalación.


*Fig. 17 Ingreso Zentyal*

Se seleccionan las opciones “Domain controller and file sharing”, “DNS Server”, “DHCP Server” y luego “Instalar”

Se confirman paquetes a Instalar y se inicia el proceso.

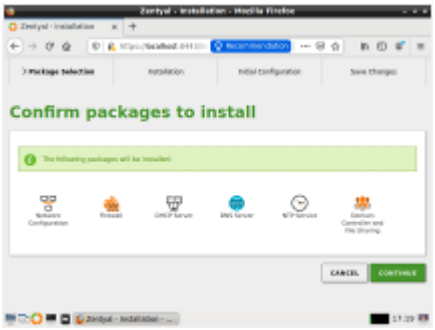


*Fig. 18 Selección paquetes*

*Fig. 19 Fin instalación paquetes*

Se procede a configurar interfaces de red

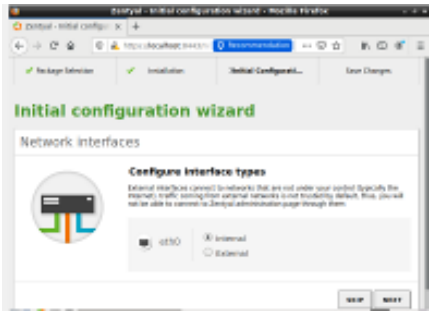


*Fig. 20 Red*

El server funcionará como controlador de dominio, la recomendación es usar IP fija.


*Fig. 21 Config IP*

Configuración de grupos y usuarios, así como host domain name.


*Fig. 22 Users*

Finalizada la primera configuración, se procede a cambiar el nombre de dominio. Se realiza en System – General – Hostname and Domain.

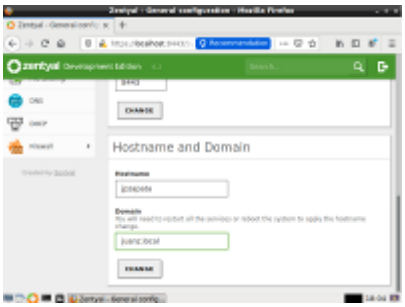


*Fig. 23 Create user*

En sección “Module status” se activan los módulos necesarios en caso de no estar configurados.

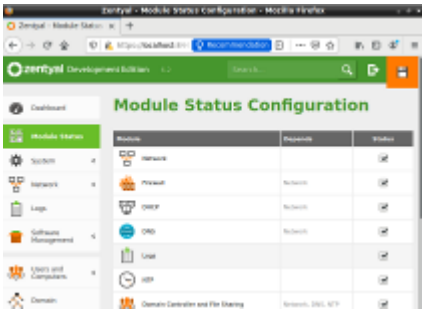


*Fig. 24 Módulos*

Procedemos a configurar DHCP


*Fig. 25 DHCP 1*

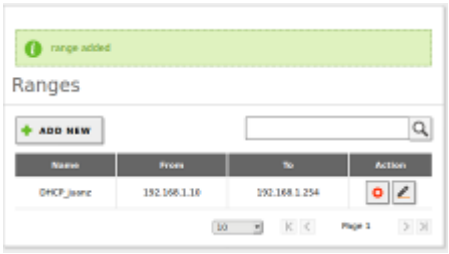


*Fig. 26 DHCP 2*

Procedemos a configurar DNS

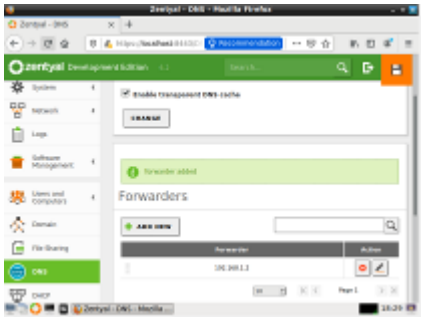


*Fig. 27 DNS*

En opción "Users and groups" adicionamos usuarios.

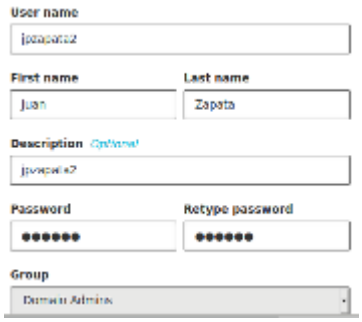


*Fig. 28 Datos usuario*

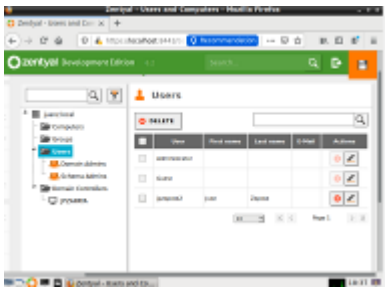


*Fig. 29 Usuarios AD*

Desde una estación cliente (Debian 10) se procede a unir el equipo al dominio e ingresar con el usuario creado y validar que tome parámetros configurados en DHCP y DNS.
DHCP y DNS funcionando correctamente. Es de resaltar que en VirtualBox se hace necesario configurar las dos VMs en red interna para que pueda funcionar de manera correcta.

*Fig. 30 Cliente Debian*

Desde el equipo cliente se abre terminal y se descubre el dominio. Sudo realm discover juanz.local

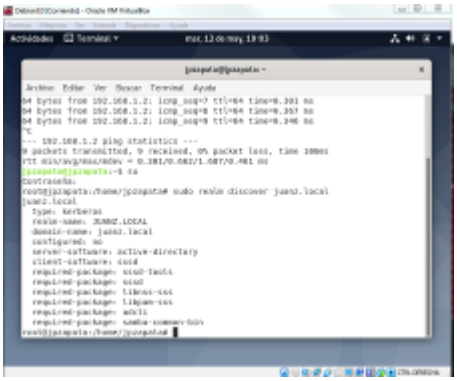

*Fig. 31 Descubrimiento dominio*

Unimos el equipo con el comando
Sudo realm join –U jpzapata juanz.local

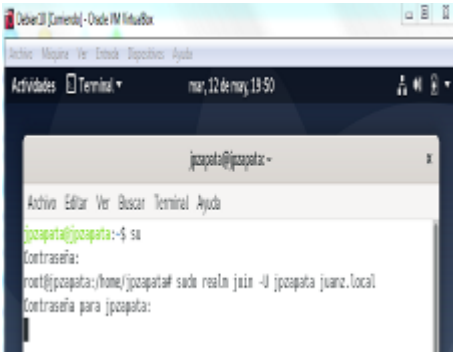


*Fig. 32 Unión a dominio*

### *C. TEMÁTICA 2 PROXY NO TRANSPARENTE: FABIÁN ANDRÉS MARTINEZ*

A continuación, configuraremos un proxy no transparente que una herramienta imprescindible de seguridad que tiene por finalidad administrar los accesos de dispositivos y redes.
Se establece IP estática

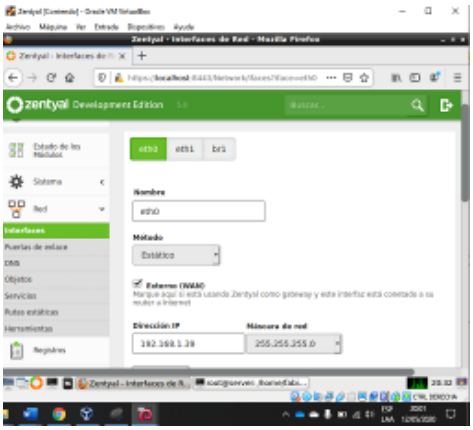

*Fig. 33 IP estática*

Se activan módulos

*Fig. 34 Activación de módulos*

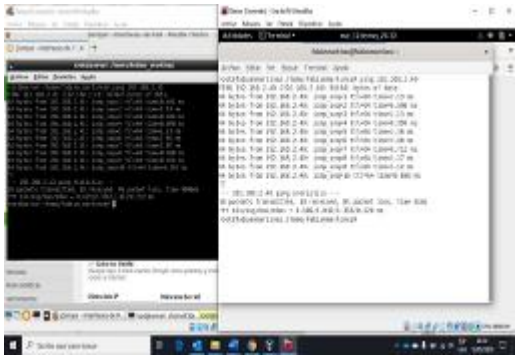

*Fig. 35 Conectividad serv_cliente*

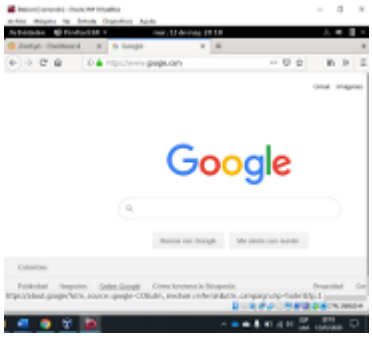

*Fig. 36 Acceso Internet*

Activamos y configuramos proxy

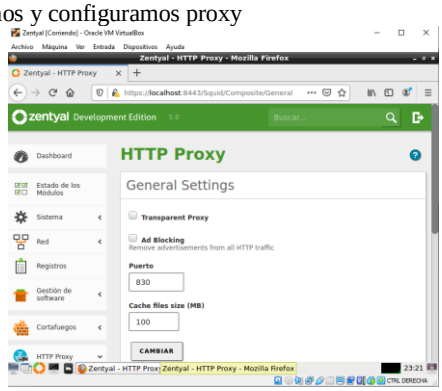

*Fig. 37 Configuración Proxy*

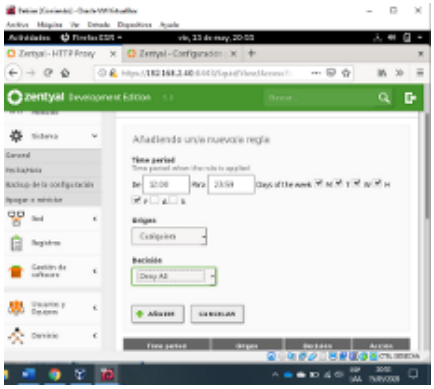

*Fig. 38 creación regla Proxy*

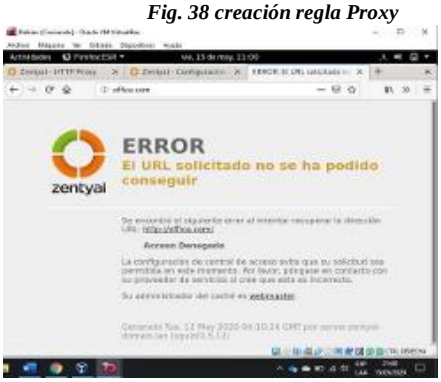

*Fig. 39 Prueba*

Accedemos a perfiles de filtrado y creamos un nuevo perfil

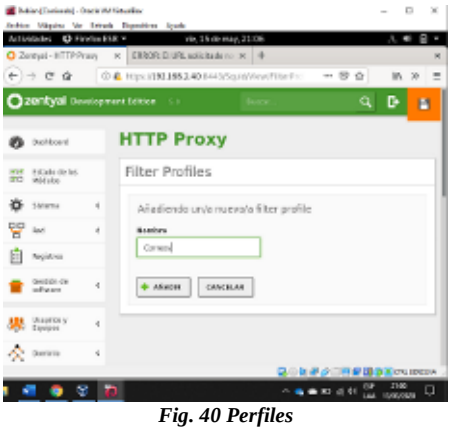

*Fig. 40 Perfiles*

Realizamos configuración del perfil

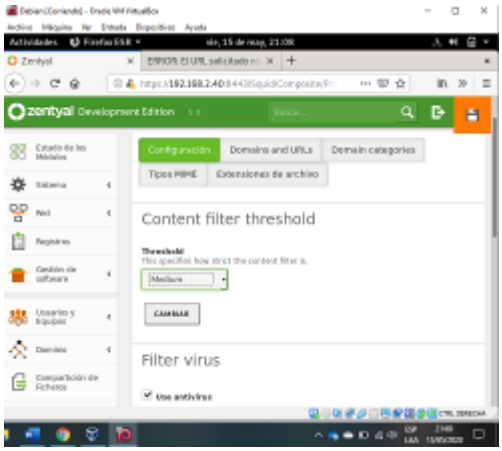


*Fig. 41 configuración perfil*

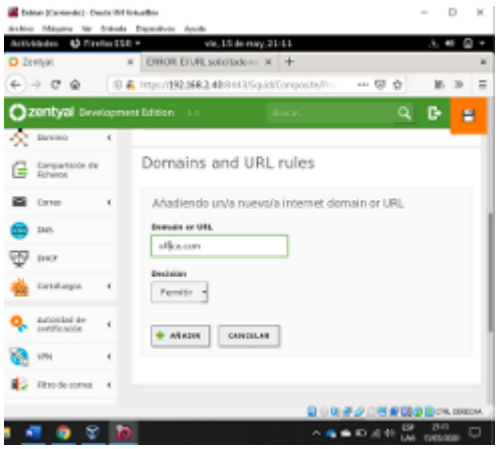


*Fig. 41.1 configuración dominios perfil*

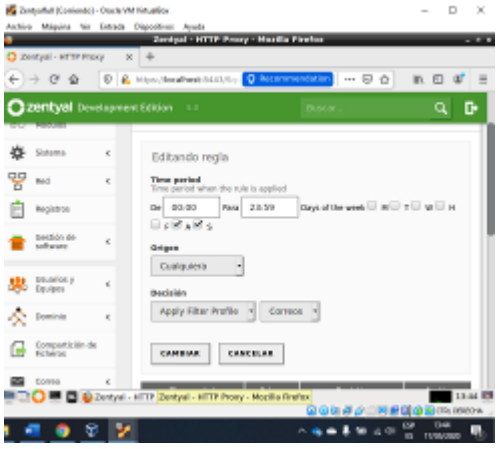


*Fig. 41.2 configuración regla de acceso con perfil*

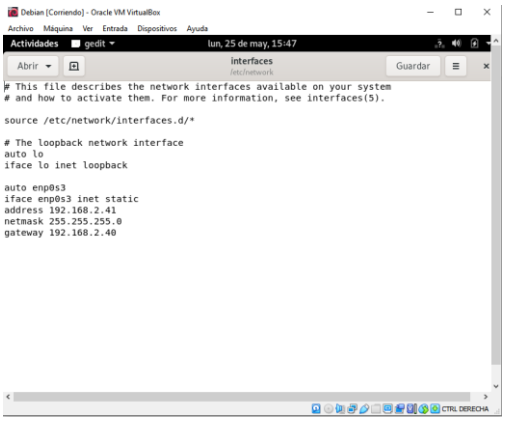


*Fig. 42 configuración de ip en el cliente*

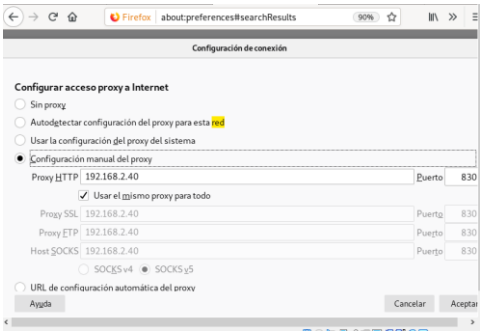


*Fig. 42.1 configuración de proxy en el cliente*

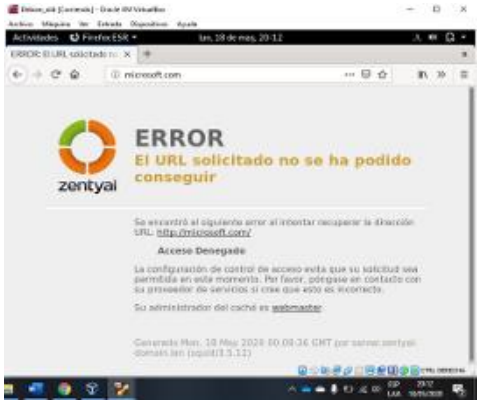


*Fig. 42.2 Prueba de regla*

La configuración de http proxy a través de zentyal depende como la mayor parte de los módulos de este de la configuración de red según los adaptadores habilitados, esta configuración de red se puede realizar de varias maneras para este caso se usaron con configuración de ip estática, pero por obligación se debe tener una configuración de red externa la cual es la que proveerá de internet la segunda red a la cual se conectaran los diferentes clientes. Teniendo esta configuración y habilitando el módulo http proxy se puede realizar la configuración de reglas de acceso, esta tiene varias modalidades según la necesidad, se puede bloquear todo el acceso, realizar bloqueos por días u horas, crear perfiles sobre los cuales se puede negar o permitir accesos a diferentes urls, extensiones, categorías o mimes, para la realización de este proceso lo ideal es establecer una política de seguridad y acceso a internet con el fin de poder aplicarla en este medio.

### *D. TEMÁTICA 3 CORTAFUEGOS: LUIS ANDRÉS MURCIA*

Accedemos al panel de control donde empezaremos a crear las reglas de tráfico del firewall que nos permitan filtrar el tráfico salientes y bloquear el entrante

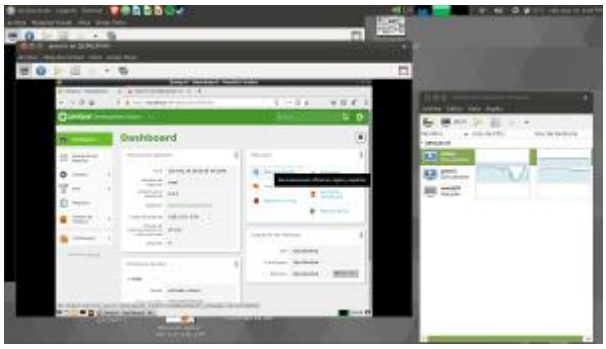


***Fig. 43 Acceso al panel de control***

Una vez en la sección de configuración del Firewall configuraremos la sección de reglas de filtrado para las redes internas


***Fig. 44 Reglas de Filtrado***

Definimos las interfaces de red externas e internas

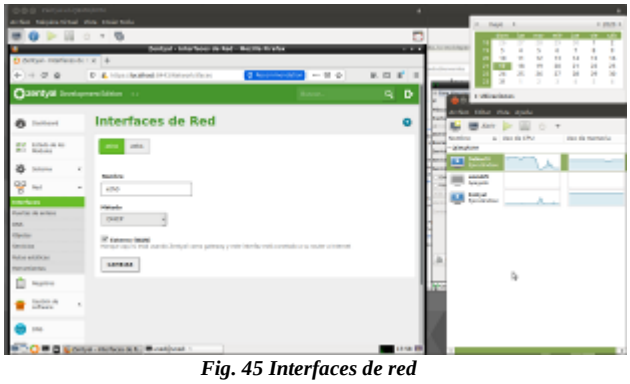


***Fig. 45 Interfaces de red***

Interfaces de red No. 2 donde asignamos una IP estática

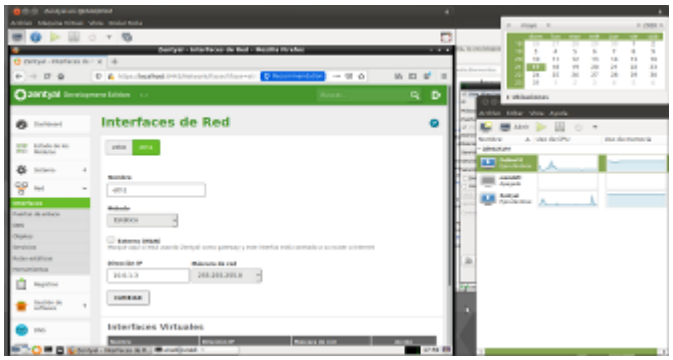


***Fig. 46 Asignación de IP***

En la maquina Debian 10 asignamos una IP estática y como puerta de enlace asignamos la IP de la interface de red No. 2.

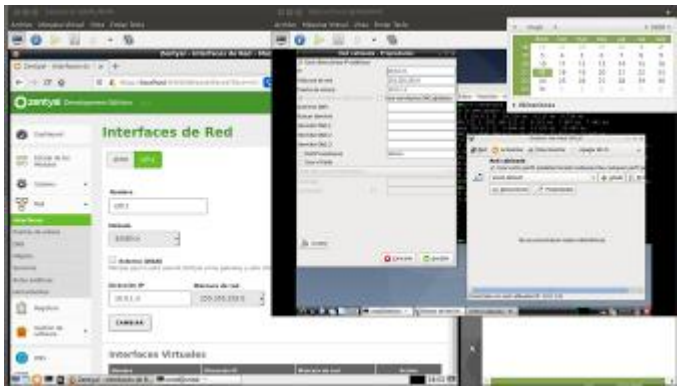


***Fig. 47 Interfaces de Red***

Una vez configurada la puerta de enlace procedemos a crear las reglas del Firewall. En este caso restringimos el acceso a www.facebook.com

***Fig. 48 Restricción de acceso***

Verificamos que el portal www.facebook.com no puede ser accedido desde nuestra red interna

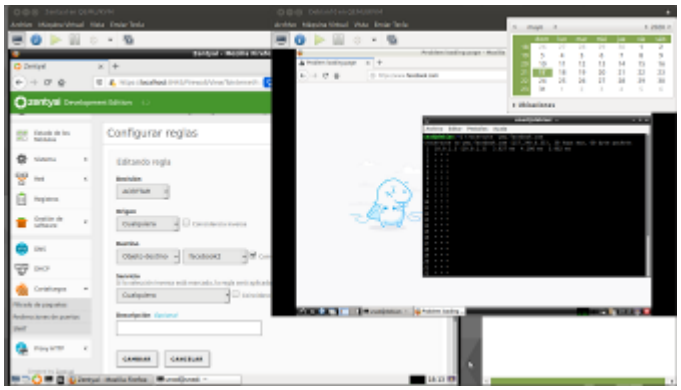


*Fig. 49 Verificación de control de acceso*

Procedemos a impedir el acceso al portal www.youtube.com

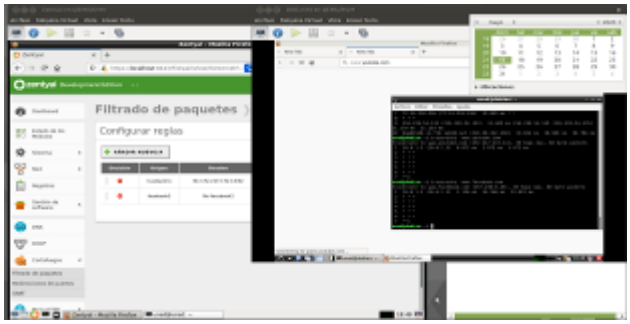


*Fig. 50 Restricción de Acceso*

Permitimos el acceso a Wikipedia.org


*Fig. 51 Permiso de Acceso*

## *E. TEMÁTICA 4 FILE SERVER Y PRINT SERVER: ANGELA PULIDO*

Desde el menú Usuarios y Equipos ‣ Configurar modo podemos comprobar cuál es el modo de funcionamiento de nuestro servidor LDAP antes de activar el módulo. Si hemos activado el módulo de Usuarios, Equipos y Ficheros, nuestro servidor funcionará como Servidor stand-alone por defecto.
Una vez activado el módulo podemos acceder a Usuarios y Equipos --> Opciones de configuración de LDAP, en el bloque superior podemos ver la Información de LDAP


*Fig. 52 Configuración LDAP*

En la parte inferior se podrán establecer Opciones de configuración PAM, pero no se hace ninguna modificación

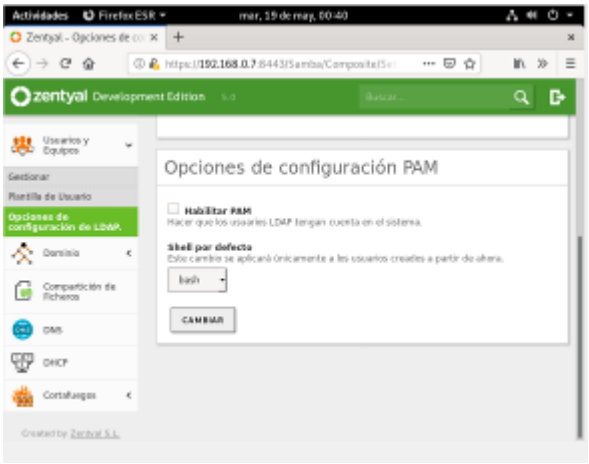


*Fig. 53 Opciones de PAM*

Gestionar Usuarios, Grupos y Equipos Desde el menú Usuarios y Equipos‣ Gestionar podremos ver el árbol de LDAP. Usando esta interfaz podemos crear y borrar nodos del árbol, gestionar los atributos de los nodos y modificar los permisos de los usuarios para otros servicios que utilizan este directorio Para agregar un usurario simplemente pulsamos en la cruz verde

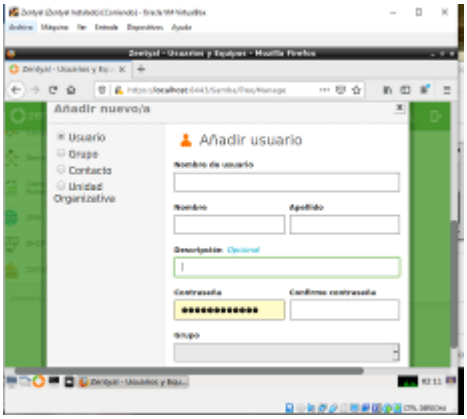


*Fig. 54 Añadir Usuario*

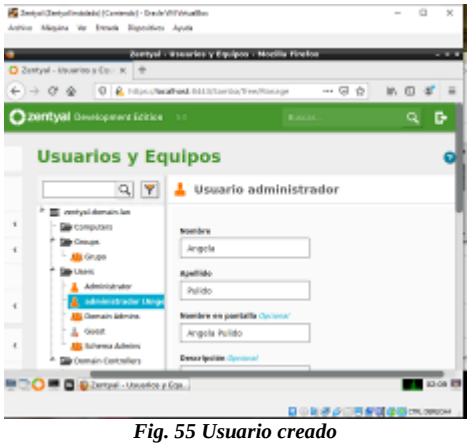


*Fig. 55 Usuario creado*

Configurar Zentyal como un servidor de Dominio Standalone
Antes de activar Usuarios, Equipos y Ficheros por primera vez nos aseguraremos de que:

- Hemos configurado el modo de operación, por defecto Controlador del Dominio, pero también podemos configurar el servidor para ser un controlador adicional unido a otros nodos. En este último caso, configuraremos el modo de operaciones y las credenciales antes de activar el módulo, y seguiremos las instrucciones para este supuesto en las siguientes secciones. Si el servidor va a funcionar como primer Controlador del Dominio, no es necesario modificar los datos por defecto

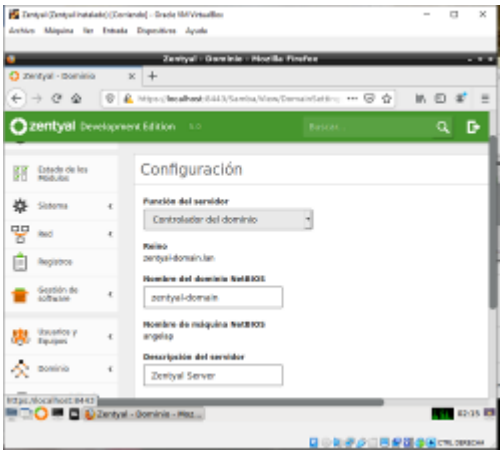


*Fig. 56 Controlador de dominio*

Creando un directorio compartido: en el control de acceso se gestiona los directorios compartidos, dependiendo del usuario. Accederemos a Compartición de Ficheros, tab de Directorios compartidos y seleccionaremos Añadir nuevo.

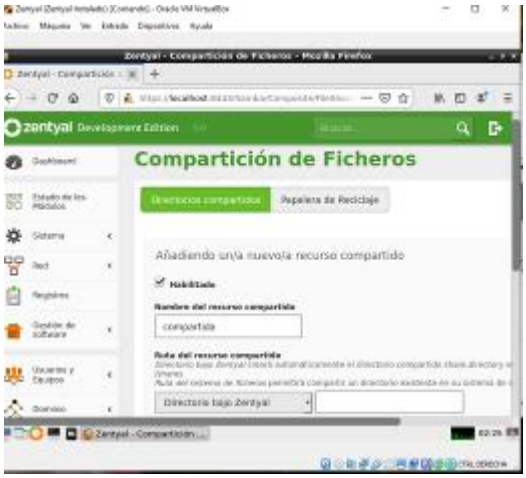


*Fig. 57 Creación de carpeta compartida*

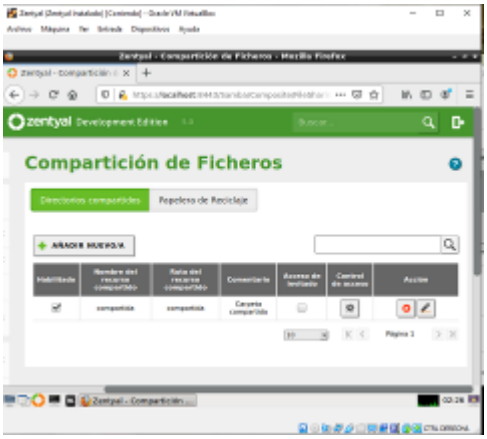


*Fig. 58 Resumen de creación de carpeta*

Los directorios compartidos pueden ser gestionados accediendo a Control de Acceso. Usando el botón Añadir nuevo, podemos asignar permisos de lectura, lectura escritura o administrador a usuarios y grupos. Si un usuario es el administrador de un directorio compartido, puede leer, escribir y borrar cualquier fichero dentro de ese directorio

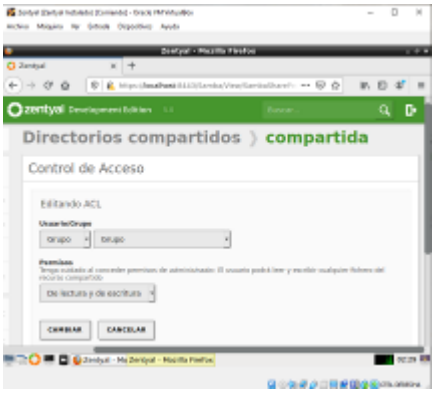


*Fig. 59 Ruta de directorio creado*

Ingresando al menú archivo configuro la carpeta creada en Zentyal con el nombre compartida

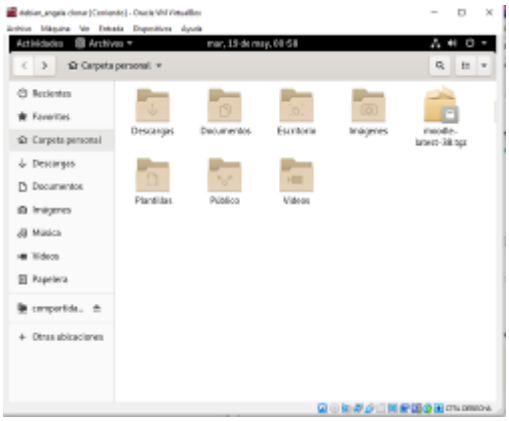

*Fig. 60 Archivos cliente*

Se coneta el debian en la misma red del eth1

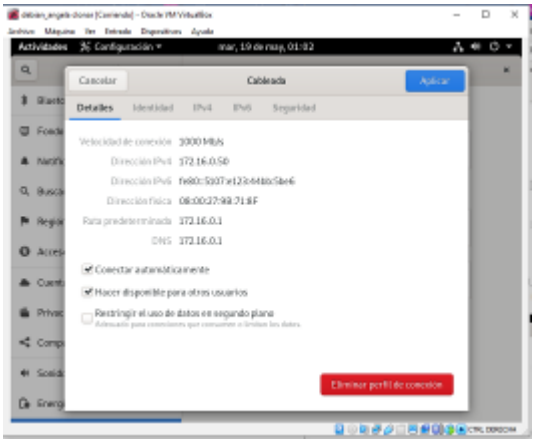

*Fig. 61 Configuración Red cliente*

Se conecta ahora a la compartida con esta ruta:

smb://172.16.0.1

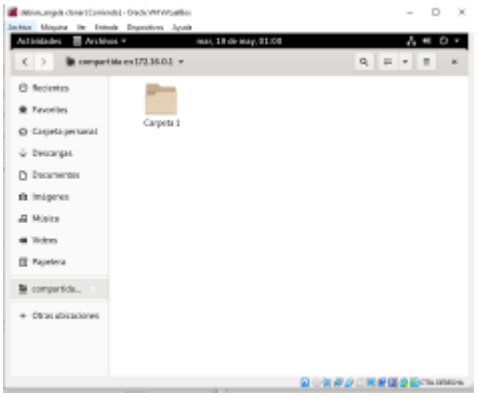

*Fig. 62 carpeta compartida cliente*

## *F. TEMÁTICA 5 VPN: EDGAR MAURICIO CARDENAS*

Es necesario crear un certificado de operación para el servidor damos click en VPN, Servidores y luego en la opción autoridad de certificación, hay realizamos la configuración de la vida útil del certificado que vamos a expedir diligenciamos los datos que nos solicita Zentyal y le damos crear y luego expedir.

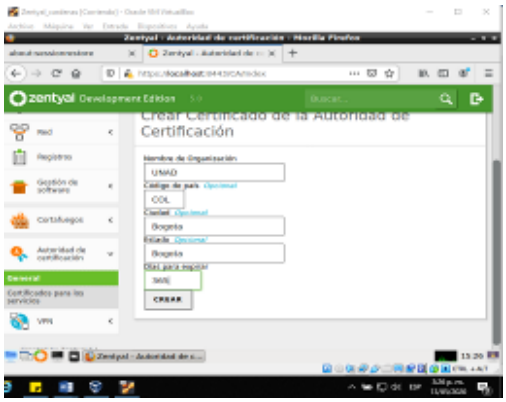

*Fig. 63 creación de Certificado de Autoridad*

Ahora procedemos a crear el servidor VPN, vamos a la opción VPN, servidores y realizamos la creación de nuestro servidor, el cual atenderá todas las solicitudes externas que se realizan por VPN.

*Fig. 64 Creación de Servidores VPN*

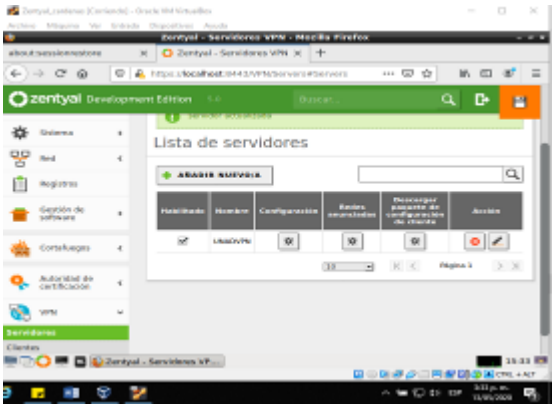

*Fig. 65 Lista de Servidores VPN creados*

Damos click en el icono de configuración y procedemos asignar la IP para nuestra conexión VPN y asignamos el certificado que creamos

*Fig. 66 Asignación de IP*

Procedemos a descargar el paquete de configuración del cliente y colocamos la IP que tiene nuestro servidor Zentyal luego damos click en descargar y guardamos el archivo.

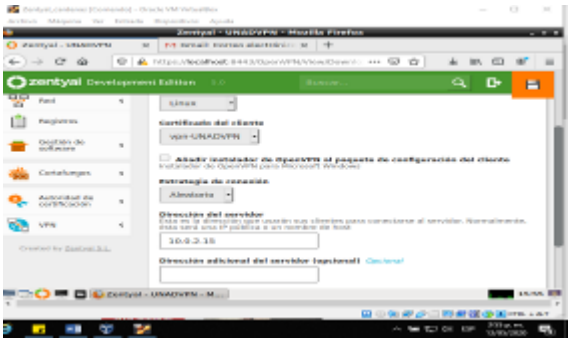

*Fig. 67 Certificación del cliente*

Ahora procedemos a instalar OPENVPN en nuestro cliente debían

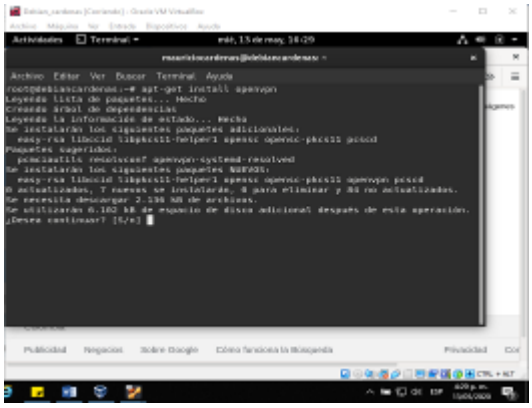

*Fig. 68 Instalación de OPENCPN en cliente*

En Nuestro cliente Debian colocamos la carpeta que creamos desde el Zentyal para nuestra conexión VPN desde el cliente la colocamos en descargas y la descomprimimos

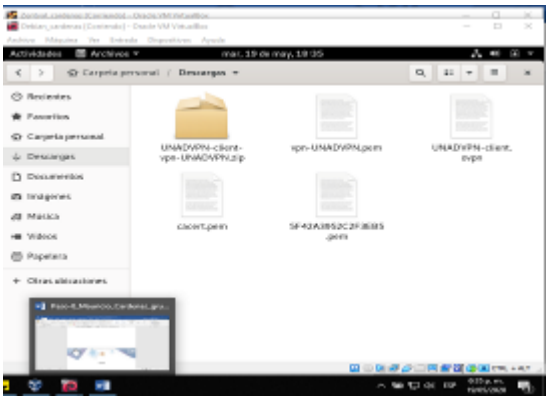

*Fig. 69 Descomprimir carpeta en cliente*

Desde nuestra consola vamos a la ruta de descargas y corremos el comando que se ve en la pantalla para nuestra conexión a la VPN

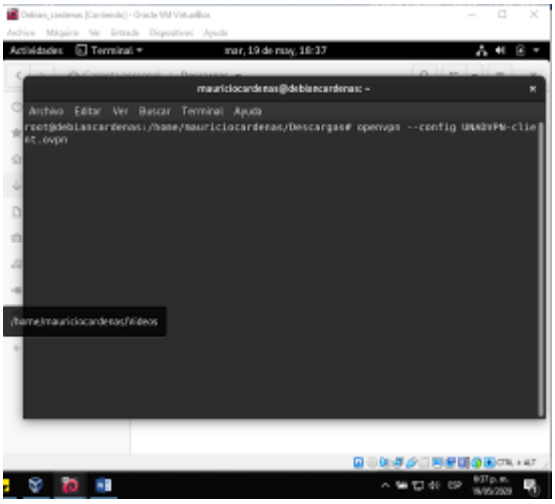

*Fig. 70 Creación de conexión VPN*

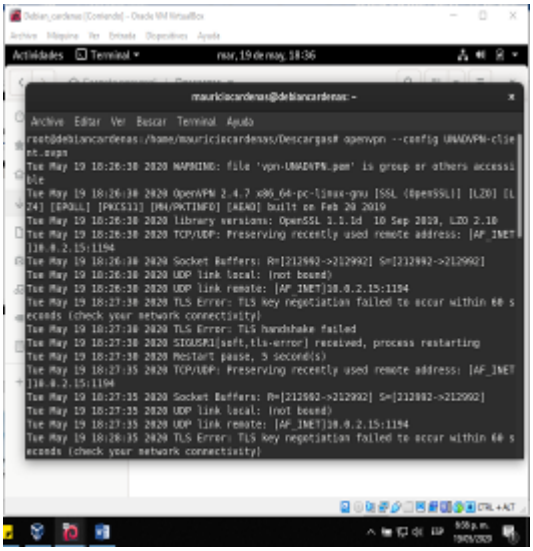

*Fig. 71 Proceso de Conexión*

## III. CONCLUSIONES

En escenarios de migración de sistemas operativos y arranque de servicios de sistemas de seguridad y de infraestructura, se puede obtener como beneficio para la empresa el uso de servidor Zentyal, ofrece la opción de administración de manera intuitiva ofreciendo numerosos servicios en un entorno de configuración web.

Zentyal facilita el proceso de formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente.

## RECONOCIMIENTO

Agradecimiento especial a los tutores que han acompañado de alguna manera la enseñanza de las temáticas aquí relacionadas, por medio de artículos, libros de investigación, y toda la referencia bibliográfica proporcionada durante el curso, con lo que el Estudiante logra la apropiación de conocimiento y deja como evidencia la puesta en marcha de la práctica visualizada en este artículo y con la cual se culmina de manera satisfactoria el diplomado de Profundización en Linux

## REFERENCIAS

[1] Sanz, M. P. (2008). Seguridad en Linux: Guía práctica. (Páginas. 60 - 76). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3218549&ppg=68

[2] Sanz, M. P. (2008). Seguridad en Linux: Guía práctica. (Páginas. 85 - 95). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3218549&ppg=93

[3] Muhammad Arifin, F., Andriana Mutiara, G., & Ismail, I. (2017). Implementation of Management and Network Security Using Endian UTM Firewall. (Páginas. 1 - 9). Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C2217DDD&lang=es&site=eds-live&scope=site

[4] Torres, E. F., & Pizarro, G. A. M. (2017). Linux para usuarios. (Páginas. 259 - 261). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4946218&ppg=259

[5] Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. (Páginas. 291 - 296). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228996&ppg=287

[6] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 121 – 148). Madrid, ES: IC Editorial. Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4310544&ppg=126

[7] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 146 - 229). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3217129&ppg=147