INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER, PARA LA IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT

Juan Camilo Alonso Bohórquez
e-mail: jcalonsob@unadvirtual.edu.co
Juan Sebastián García Álvarez
e-mail: jgarciaalva@unadvirtual.edu.co
Mayerli Tatiana Correa Ardila
e-mail: mtcorreaa@unadvirtual.edu.co
Cristhiam David Guerrero Cruz
e-mail: cdguerrerocr@unadvirtual.edu.co
Wilson Leonardo Guantivar Avendaño
e-mail: wguantivara@unadvirtual.edu.co

RESUMEN: *Con el siguiente documento se presenta la solución a la actividad donde se requiere validar servicios de infraestructura internos y externos con arquitectura Linux, durante el documento se solucionan cinco problemáticas, y se da manejo y gestión a la herramienta de distribución basado en Linux "Zentyal Server 6.2". Dentro de la solución se presentarán soluciones en servicios como DHCP, DNS, Firewall, Proxy y VPN.*

ABSTRACT: *With this document is intend to present the solution to the activity where it's required to validate infrastructure services either internal or external with Linux architecture, it will also provide the management of the tool distributed based on Linux "Zentyal Server 6.2". Into the solution will be presented solutions in services such as DHCP, DNS, Firewall, Proxy and VPN.*

PALABRAS CLAVE: Linux, Ubuntu, Zentyal Server, DHCP, Firewall, File Server, DNS, Servidor, Print Server.

1 INTRODUCCIÓN

Con el siguiente documento se realizó la instalación y configuración de Zentyal Server cuyo aplicativo permitirá instalar y trabajar diferentes servicios de servidor, adicional mantiene un entorno amigable con el usuario que permitirá de manera intuitiva hacer las diferentes modificaciones de estos servicios en el momento que se requiera. Durante la lectura del documento el lector podrá encontrar de manera cómoda y amigable los parámetros y requerimientos necesarios para la instalación, configuración y manipulación de los servicios requeridos en la guía de actividades del Diplomado de Ingeniería de Sistemas con énfasis en Linux, tales como: Firewall, DHCP, VPN, Print Server.

2 ZENTYAL SERVER

2.1. INSTALACIÓN ZENTYAL SERVER 6.2

Zentyal trabaja bajo arquitectura X86(64 bits), con requerimientos mínimos de 2GB de memoria RAM, procesador de doble núcleo y 10GB de Disco duro.

URL: http://download.zentyal.com/zentyal-6.2-development-amd64.iso

Paso 1: Selección de la imagen des disco de ISO que fue descargada para el server de Zentyal.

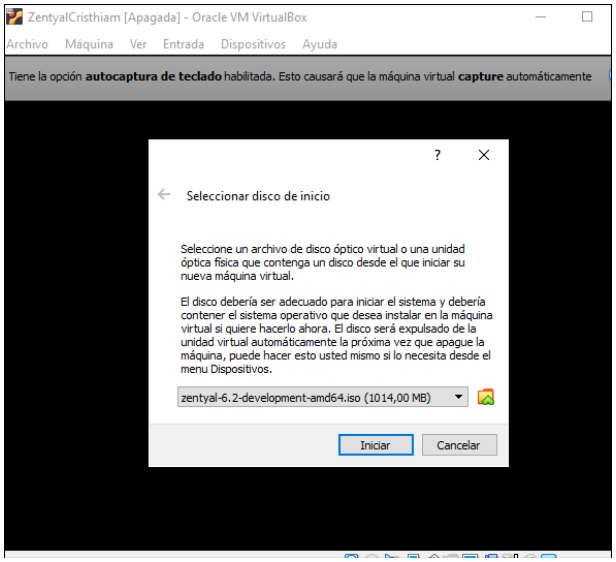

Figura 1. Selección imagen ISO

Paso 2: En este paso se muestra las opciones de instalación del Zentyal en donde se selecciona la primea opción la cual indica el borrado de los discos para su instalación

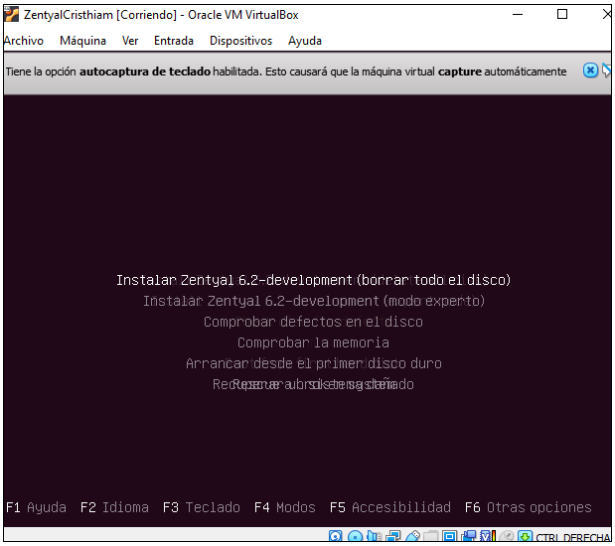

Figura 1.1. Selección Zentyal

Paso 3: Se selecciona el país donde se realiza la instalación. Esto permite que Zentyal configure la zona horaria correspondiente ya que este tiene configuraciones por hora y días de la semana

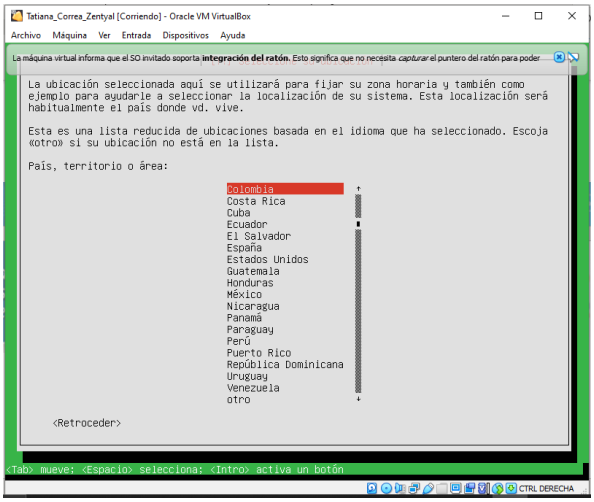

Figura 1.2. Selección Ubicación

Paso 4: Al tener seleccionada la ubicación, se procede a seleccionar el idioma del teclado en este caso será español (Latinoamérica) con el fin de que reconozca los caracteres especiales como la eñe(ñ)

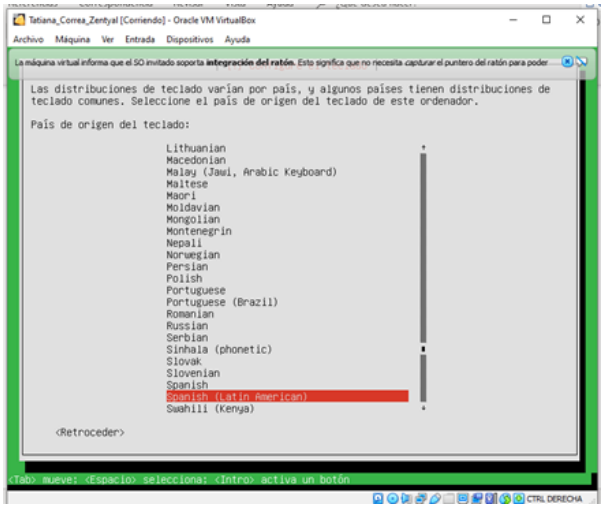

Figura 1.3. Idioma teclado

Paso 5: En este punto se selecciona las variaciones que puede tener el teclado latinoamericano y se escoge el que corresponda

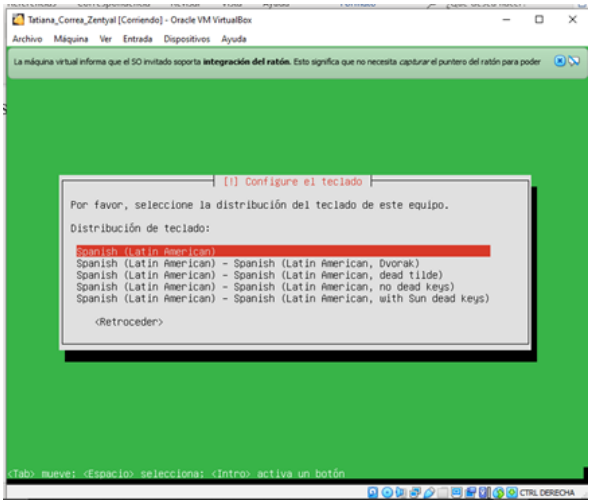

Figura 1.4. Distribución teclado

Paso 6: Para este paso aparecerán las redes configuradas en la máquina virtual donde se selecciona la red principal que será la encargada de proporcionar el internet. En este caso es eth0

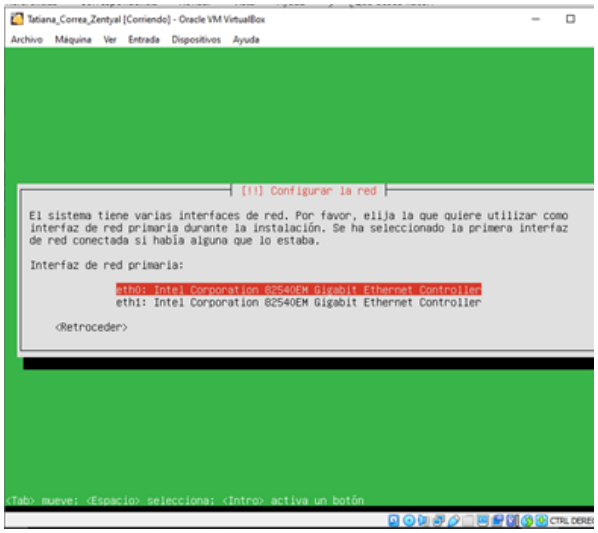

Figura 1.5. Interfaz de red primaria

Paso 7: Se asigna el nombre del servidor Zentyal en el cual se selecciona el que se muestra en pantalla

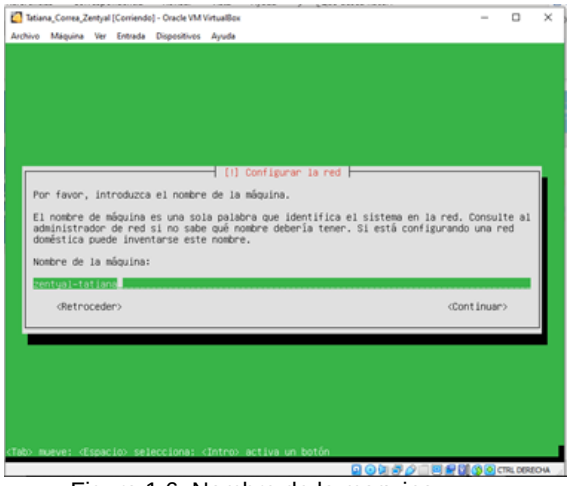

Figura 1.6. Nombre de la maquina

Paso 8: Se asigna un nombre de usuario con el que se ingresara al servidor de Zentyal y con el cual se realizaran todas las configuraciones

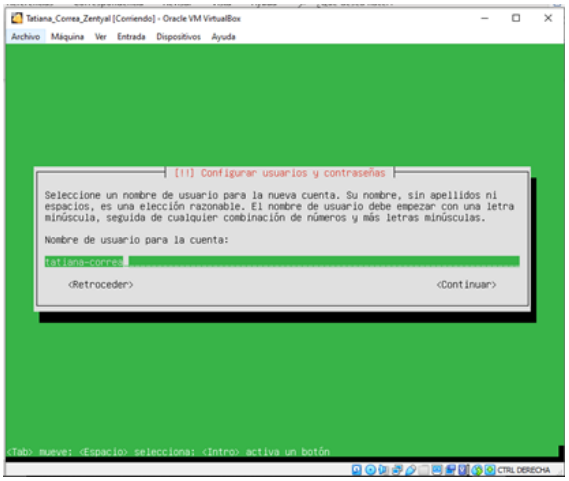

Figura 1.7. Nombre usuario

Paso 9: En este punto se asigna la contraseña para el usuario creado en el paso anterior el cual permitirá realizar el inicio de sesión en el servidor

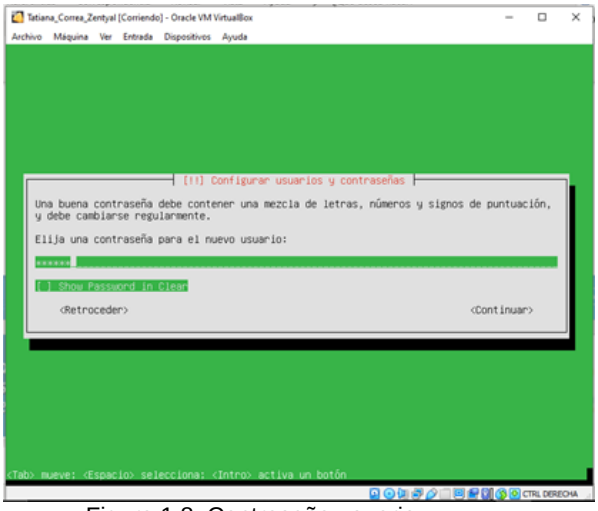

Figura 1.8. Contraseña usuario

Paso 10: Se realiza la confirmación de la contraseña creada

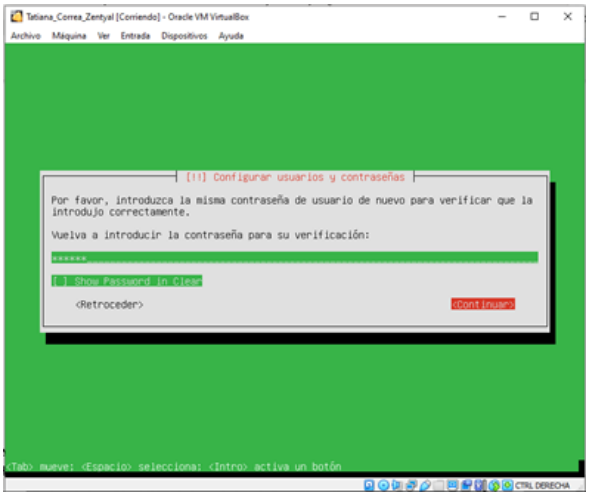

Figura 1.9. Confirmación contraseña

Paso 11: En este escenario se selecciona la localización del sistema para realizar la configuración del reloj. Para este caso se selecciona la opción que se muestra en pantalla

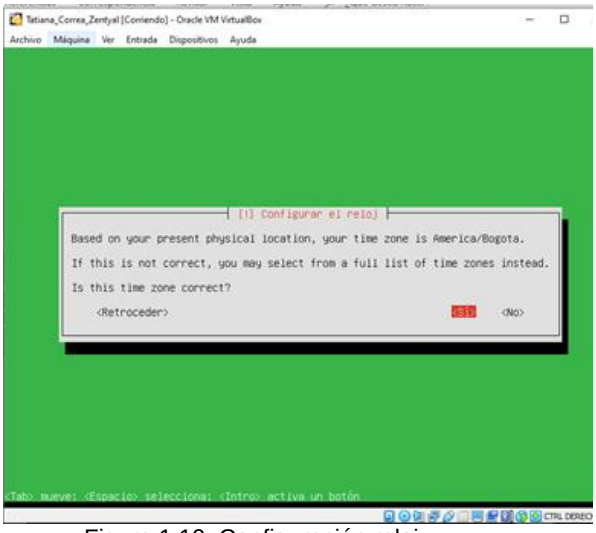

Figura 1.10. Configuración reloj

Paso 12: En este paso se muestra que la instalación y configuración de Zentyal ha terminado en donde muestra la opción de continuar para el reinicio de la maquina automáticamente

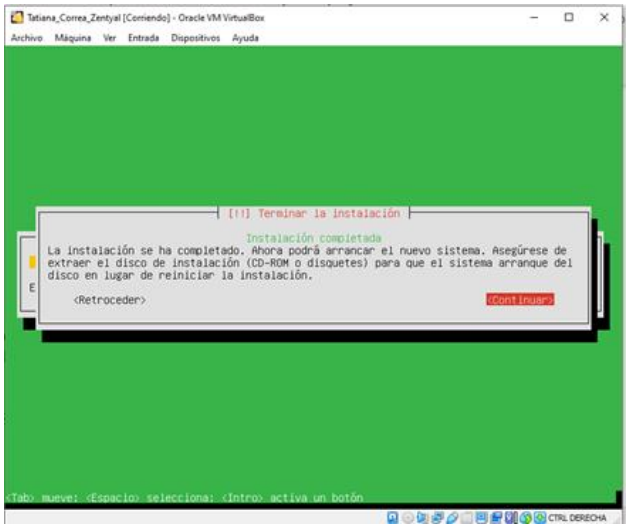

Figura 1.11. Finalización de instalación

Paso 13: Después del reinicio de la maquina el sistema muestra el inicio del programa.

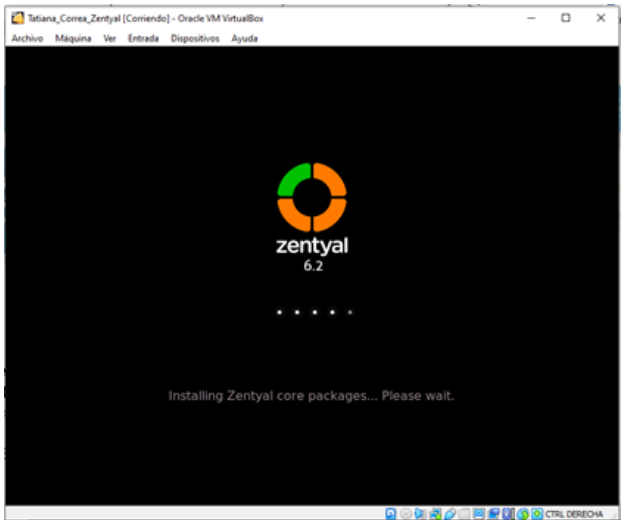

Figura 1.12. Inicio de Zentyal

3 IMPLEMENTACIÓN SERVICIOS DE GESTIÓN INGRESTRUCTURA IT

3.1. TEMATICA 1: DHCP SERVER, DNS SERVER Y CONTROLADORES DE DOMINIO

Producto esperado: 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.

Lo primero que se debe realizar es la instalación de los tres módulos a trabajar, para este caso DHCP, DNS y el controlador de dominio.

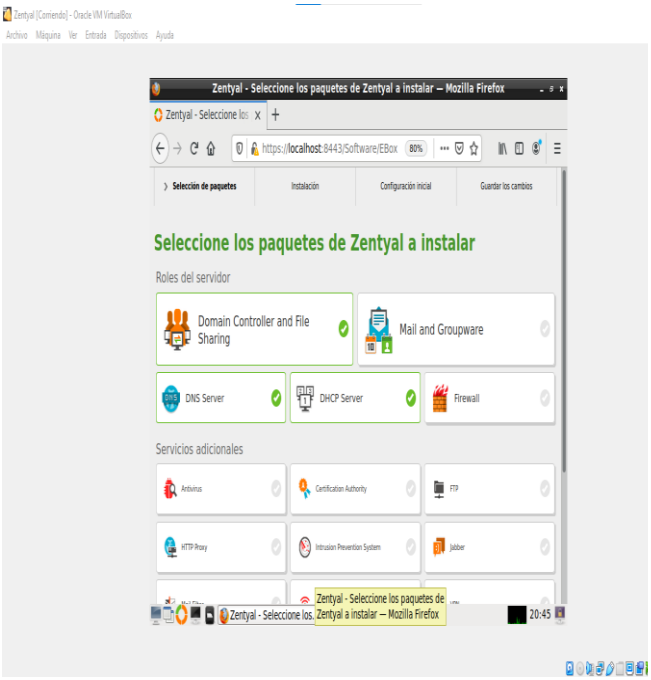

Figura 2.1. Selección de los módulos

Con los módulos instalados, se procede a activarlos para que sean útiles y funcionales.

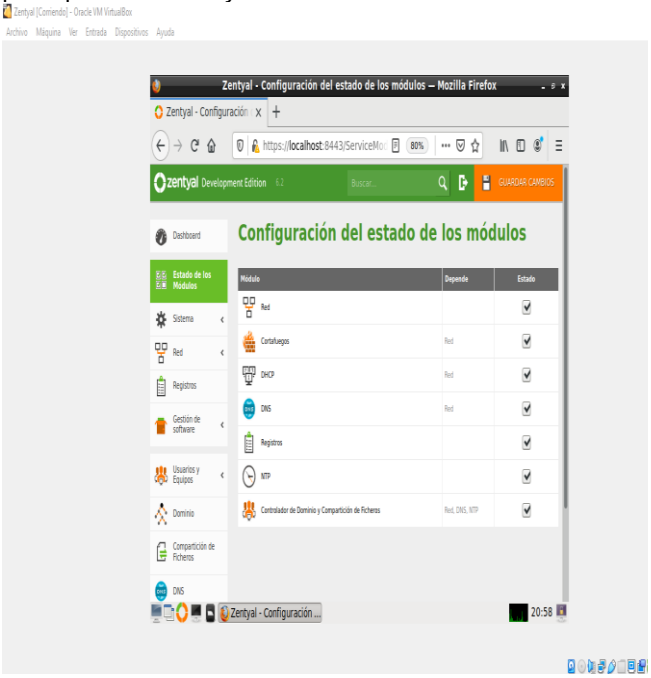

Figura 2.2. Selección de los módulos

El orden correcto es instalar el servidor DNS, para identificar a donde se conectará el equipo que se prepara y se configura como estación de trabajo. En el servidor zentyal, se cuenta con dos adaptadores de red, uno para red interna y otro para red externa. De esta manera, se debe configurar el primero para que desde el equipo Ubuntu configurado, se pueda acceder y sea asignada la ip de acuerdo al servidor DHCP. Para la red eth0, se configura la asignación automática de IP (DHCP), adicionalmente se configura como externo para que el servidor cuente con acceso a internet.

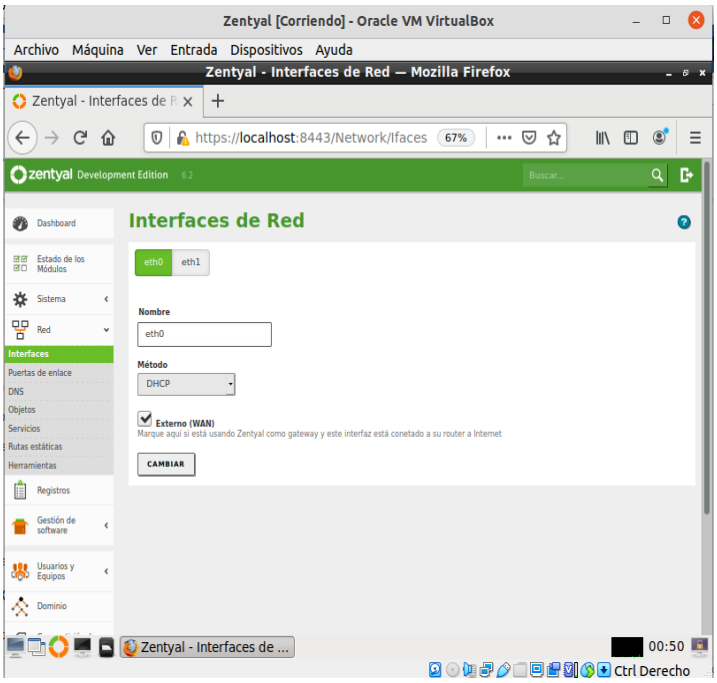

Figura 2.3. Configuración eth0

Por otra parte, se configuro la dirección que tendrá el servidor y sobre el que accederán los equipos que se conecten al mismo. Para ellos se selecciona como método ***estático*** que permite configurar una dirección IP y la seleccionada es 10.22.0.4, con mascara de red 255.255.255.0.

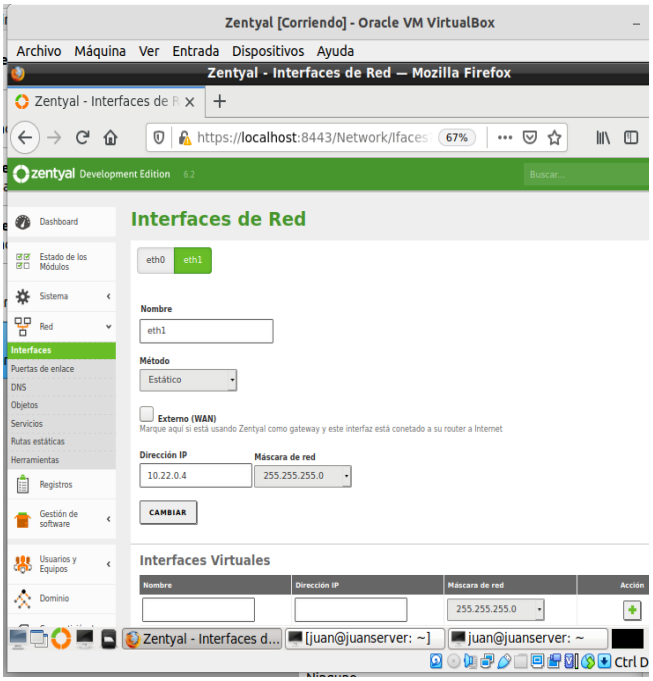

Figura 2.4. Configuración eth0

Ahora en el módulo de controlador de dominio, se procede a realizar la creación del usuario que permitirá realizar las pruebas correspondientes para el módulo, el usuario creado será ***juanpc.***

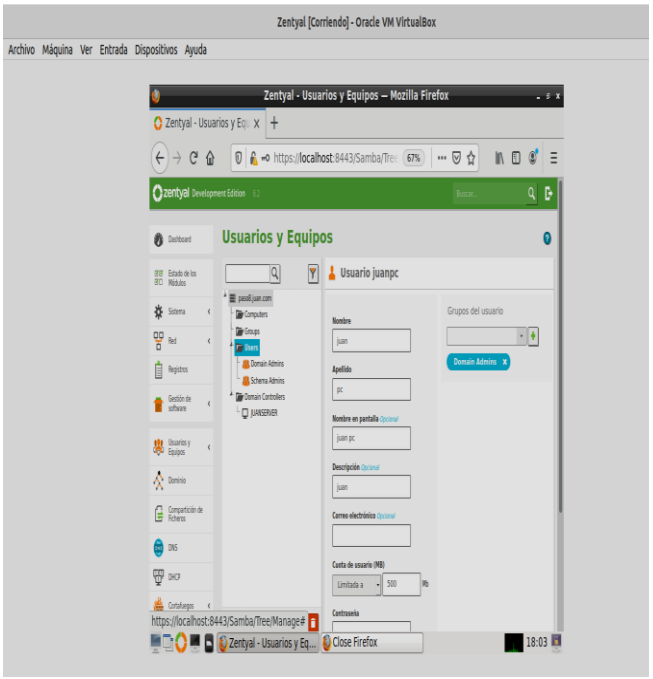

Figura 2.5. Creación Usuario

Con estos pasos, se culmina con la configuración del servidor y se inicia a la máquina virtual con el equipo de escritorio, en donde se deben realizar pasos clave que permitan agregar el usuario al dominio. Para ello, se debe incluir en el dominio, no sin antes configurar el archivo resolv.conf, que permita apuntar al servidor zentyal.

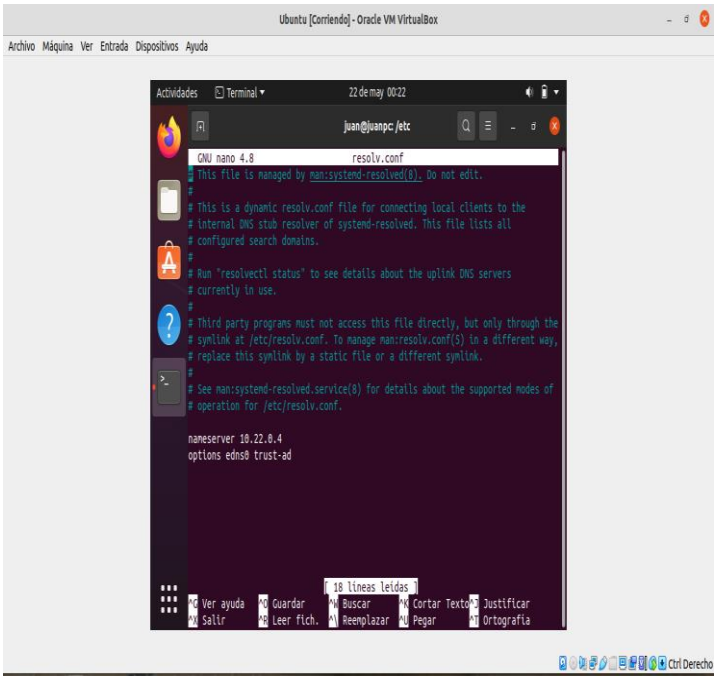

Figura 2.6. Configuración resolv.conf

Luego de esto y con la instalación del programa AD Bridge Open 9.1.0.551 en versión 64 bits, que permitirá con los siguientes comandos en consola agregar el usuario al dominio juanpc al dominio paso8.juan.com.

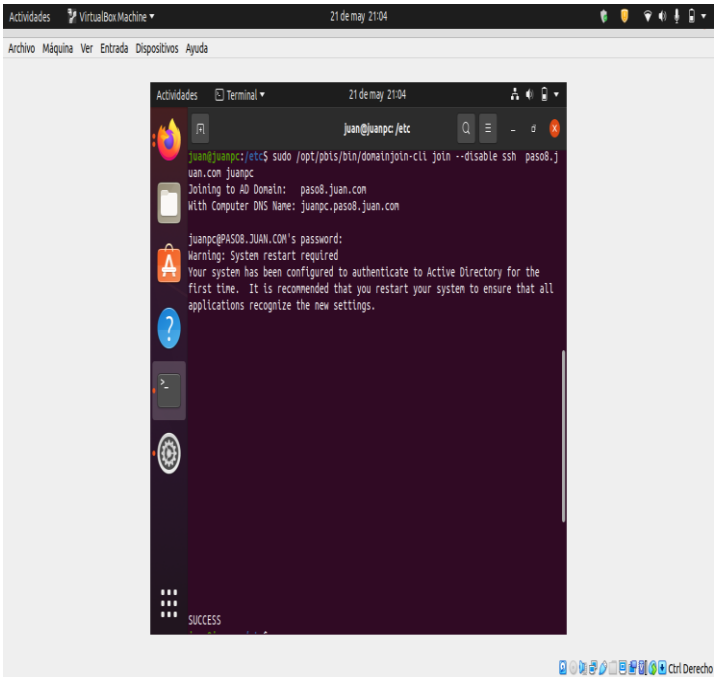

Figura 2.7. Agregar Usuario a dominio

De esta manera, se confirma la creación del usuario juanpc y este a su vez puede ingresar al equipo con el dominio correspondiente

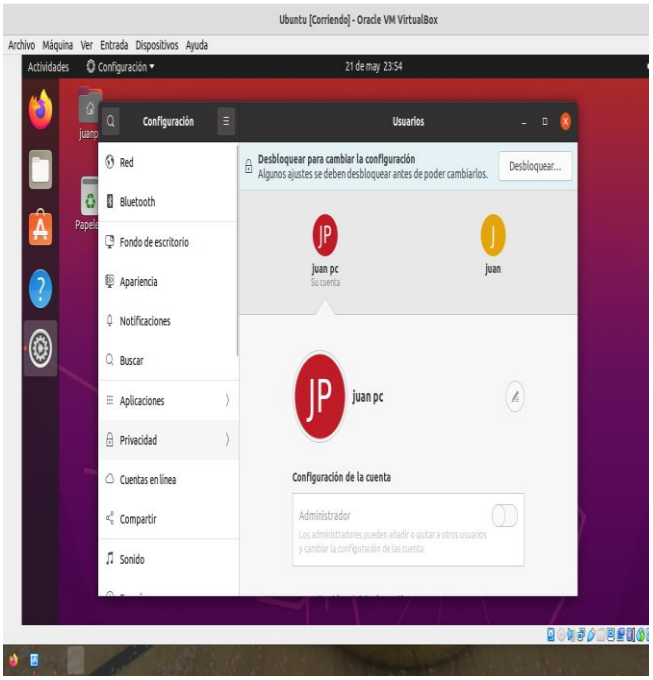

Figura 2.8. Usuario configurado

Ahora, la configuración del dhcp, aunque en la maquina ya está configurado. Para ellos y ya teniendo el módulo instalado, se procede a realizar la configuración de los rangos

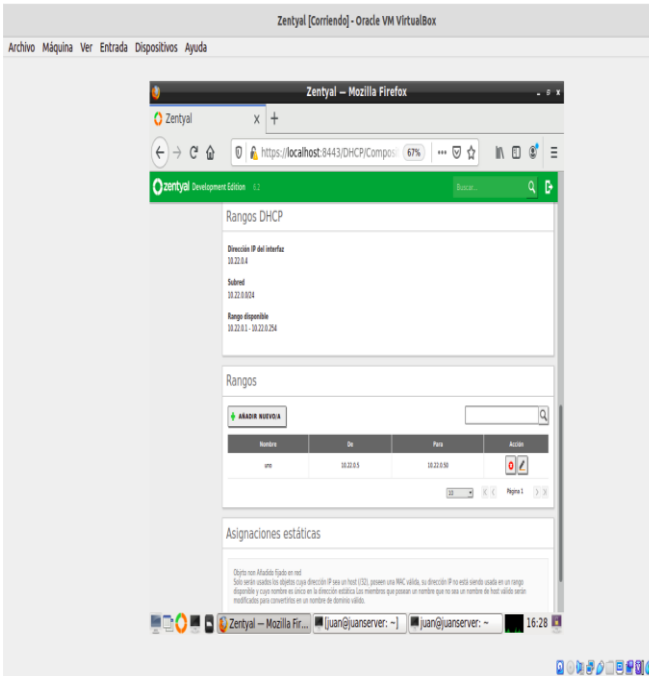

Figura 2.9. Rangos DHCP

En la maquina será asignada la ip con el rango seleccionado iniciando desde la ip 10.22.0.5.

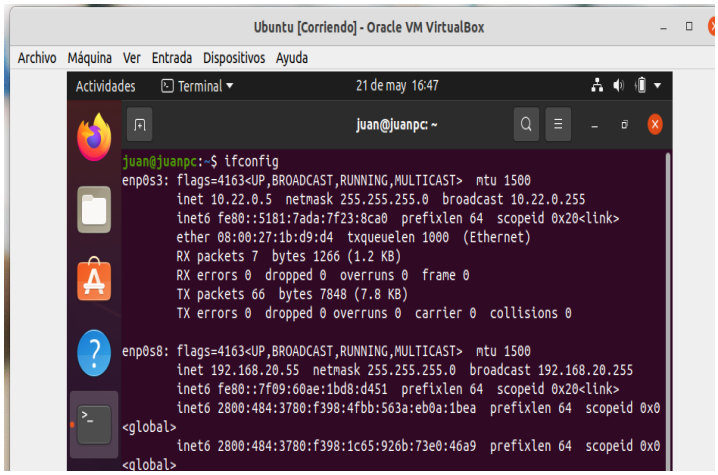

Figura 2.10. Validación con ifconfig

Y de igual manera la configuración del DNS que ya estaba implementada para interpretación de direcciones.

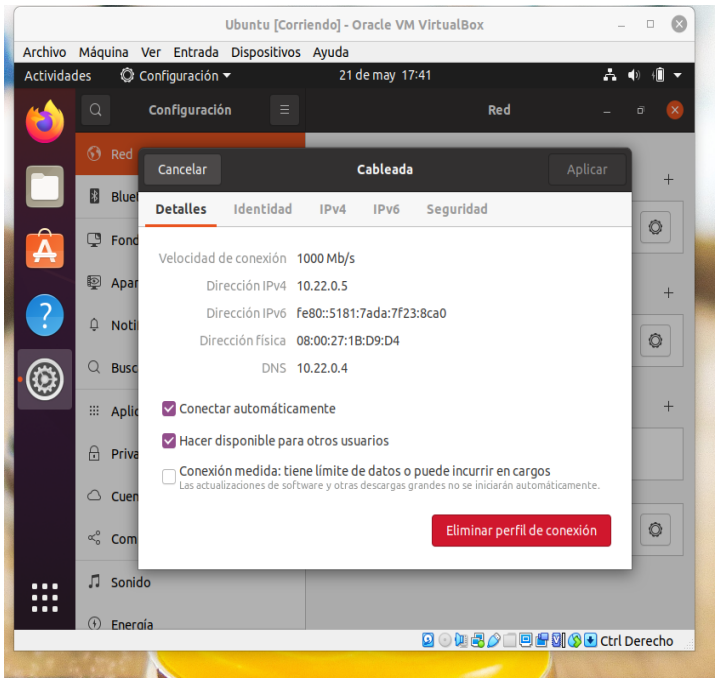

Figura 2.11. Información de red

3.2. TEMATICA 2: PROXY NO TRANSPARENTE

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

Para realizar la configuración adecuada del proxy no transparente se debe configurar los módulos a utilizar dentro del Zentyal, para ello, se realiza la instalación de

firewall, DHCP, DNS y Proxy HTTP. Para ello, también es fundamental asegurar que se encuentren activos.

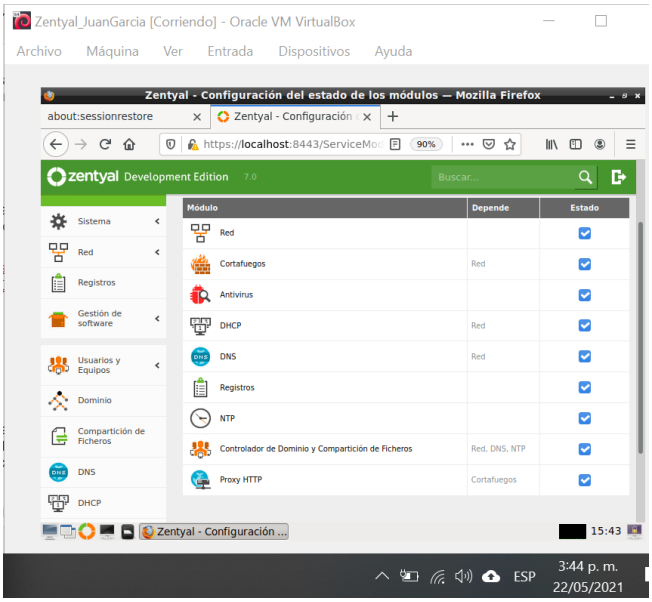

Figura 3.1. Estado de los módulos instalados

A continuación, se debe realizar la modificación de las interfaces de red, en este caso, se tienen dos, la primera eth0 con IP estática y de manera interna y la segunda eth1 con método DHCP y de manera externa

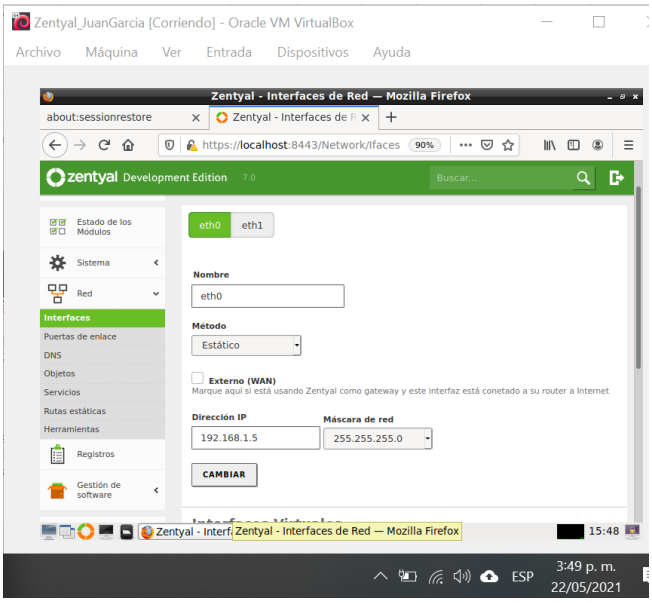

Figura 3.2. Configuración de la interfaz eth0 con dirección ip estática

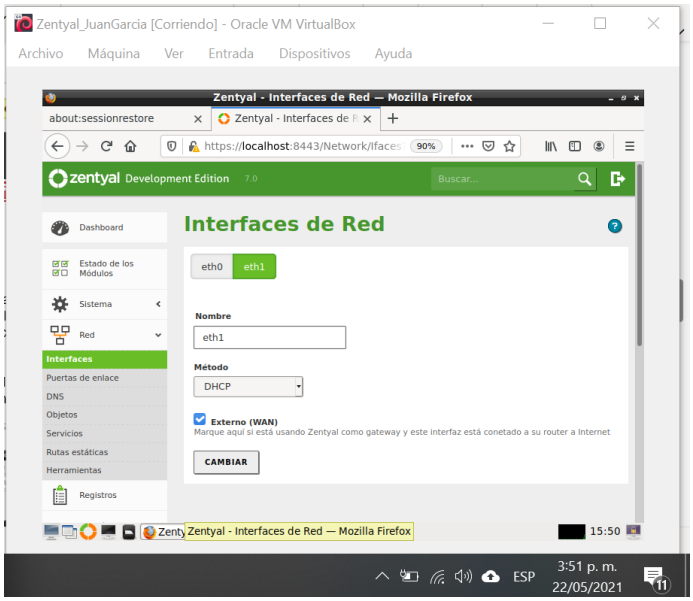

Figura 3.3. Configuración de la interfaz eth1 asignación DHCP

Una vez configuradas las interfaces, se debe garantizar que los módulos sigan corriendo o en dado caso realizar el proceso de reinicio desde el dashboard. A continuación, se procede con la modificación del HTTP Proxy, para asignar un proxy no transparente y modificar el puerto.

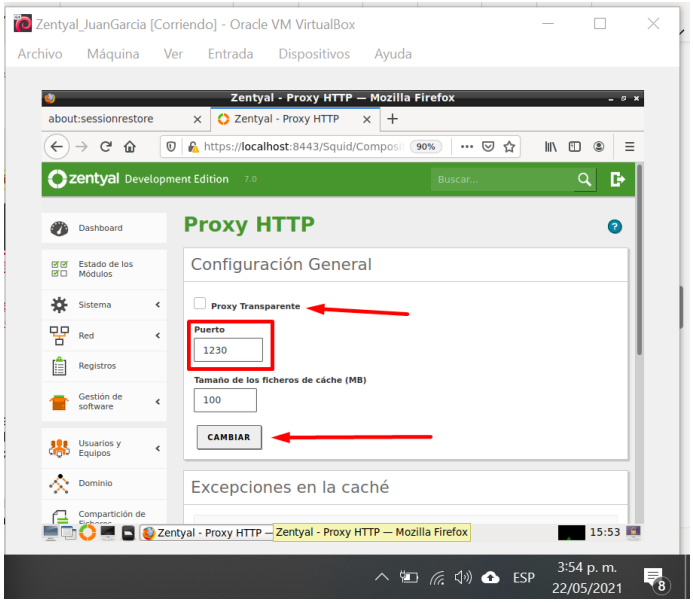

Figura 3.4. Configuración del proxy no transparente y el puerto

El siguiente proceso es llevar a cabo la creación de un perfil de filtrado, cuyo fin es filtrar la información de internet a través del puerto anteriormente especificado (1230), para este ejemplo práctico, el perfil se llamará redes_sociales.

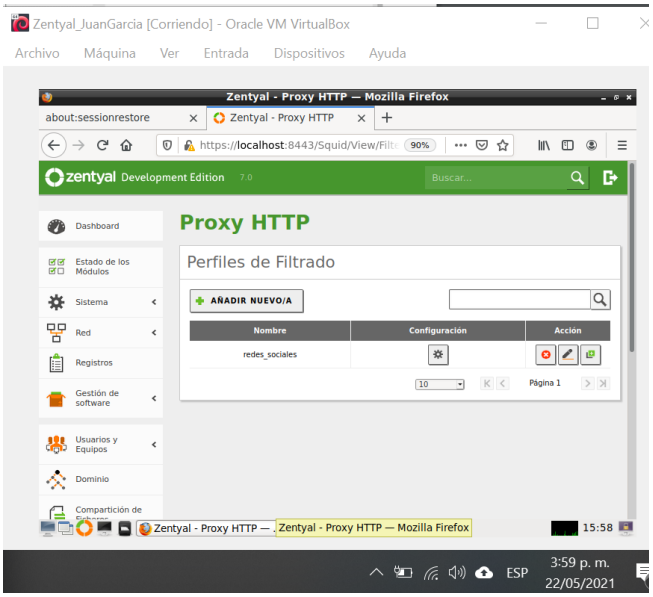

Figura 3.5. Perfiles de filtrado creados

En la creación de este perfil de filtrado se deben llevar a cabo unas modificaciones en el umbral de filtrado de contenido, esto, con el fin de determinar cuan estricto debe ser el filtro en este caso se establecerá como muy estricto.

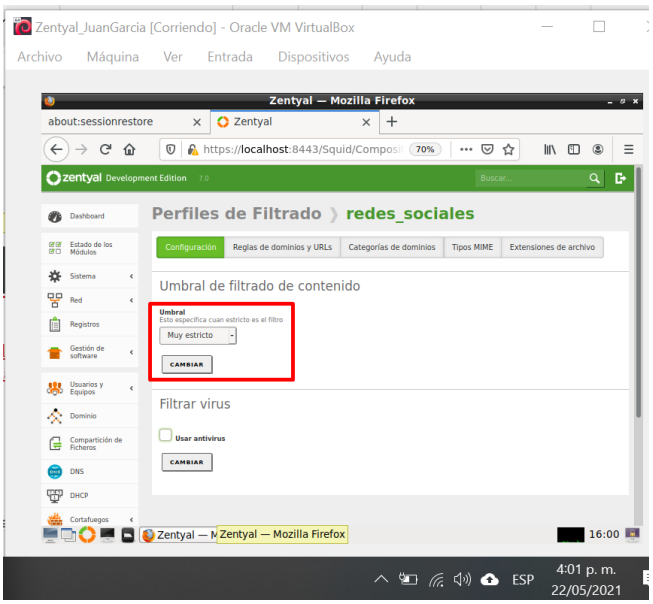

Figura 3.6. Umbral de filtrado de contenido

Una vez establecido la configuración del umbral, se procede a la siguiente pestaña denominada reglas de dominio de URLs, esto, con el fin de poder listar los dominios que van a tener las restricciones de acceso a través del puerto configurado. Se puede realizar a través de dos opciones, la primera, establecer los dominios con acceso y bloquear los dominios no listados o viceversa, en este caso, se permite acceso a URLs no listados y los listados son denegados.

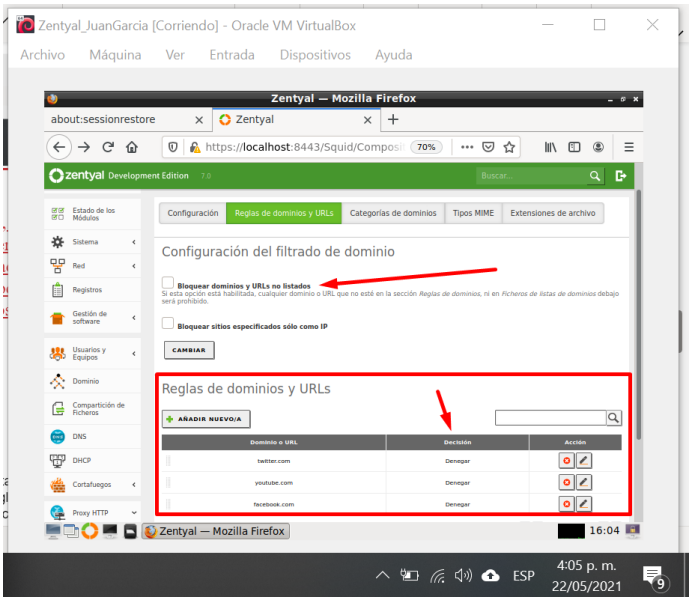

Figura 3.7. Reglas de dominios y URLs

El siguiente paso es realizar la creación de las reglas de acceso con el fin de asociar el perfil anteriormente creado y llamado redes_sociales.

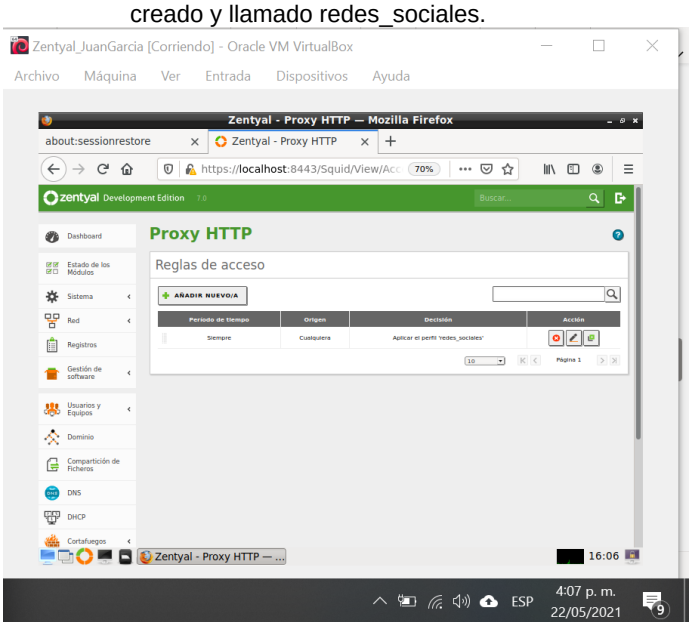

Figura 3.8. Reglas de acceso

Dentro de las reglas de acceso permite realizar una configuración especifica que aplique para ciertas franjas horarias y para ciertos días, también permite aplicar las reglas a un origen seleccionado y finalmente una decisión que permite todo, denegar todo o aplicar un perfil de filtrado, en este caso se selecciona dicha opción y se selecciona redes_sociales, anteriormente creado.

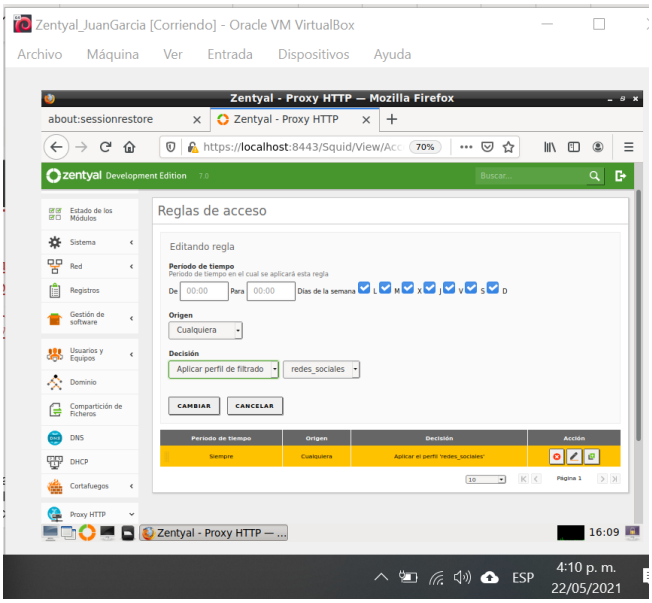

Figura 3.9. Editando la regla de acceso

Una vez realizadas estas configuraciones, se procede a almacenar las configuraciones y reiniciar los módulos anteriormente especificados con el fin de tomar los cambios anteriormente aplicados. Ahora bien, se procede a configurar el proxy en el navegador de Ubuntu Desktop e intentar ingresar a las páginas listadas en el perfil de filtrado.

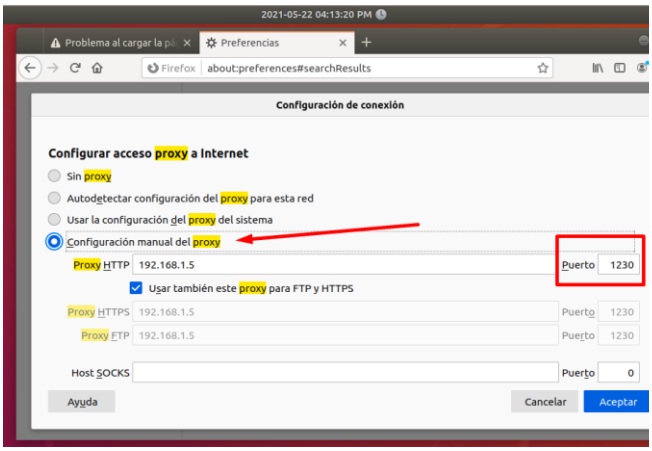

Figura 3.10. Configuración de proxy y asignación de puerto de filtrado

Una vez realizado dicho proceso, se procede a ingresar a las páginas web listadas en el perfil de filtrado.

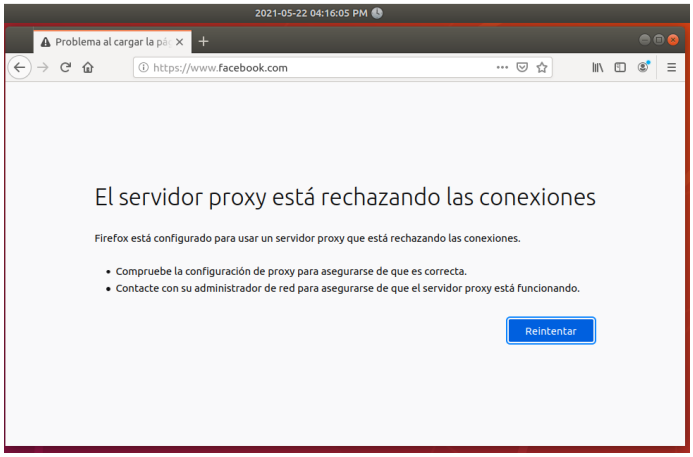

Figura 3.11. Ingreso al dominio de Facebook

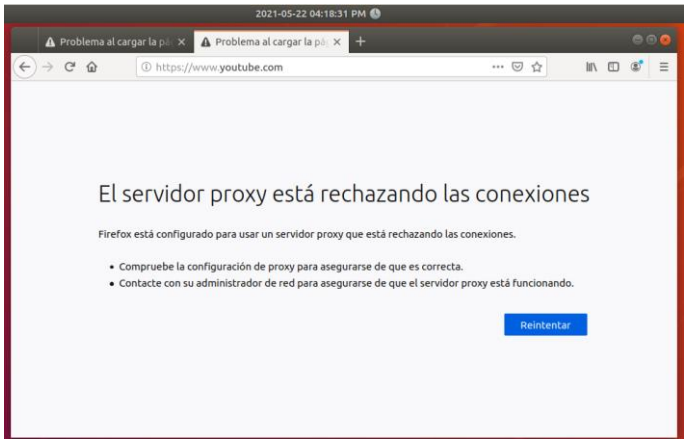

Figura 3.12. Ingreso al dominio de YouTube

3.3. TEMATICA 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 3 del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Se inicia la configuración del servidor Zentyal para el método de cortafuegos en donde el primer paso que se realizó fue la creación de una máquina virtual, la instalación y configuración del servidor zentyal

Figura 4. Inicio de Zentyal

Se accede al Zentyal para realizar la configuración e instalación del servicio de firewall, proxy y los paquetes que este contenga. De igual manera se genera la configuración para los tipos de interfaces y la configuración de red para interfaces externas en los puertos eth0 y eth1

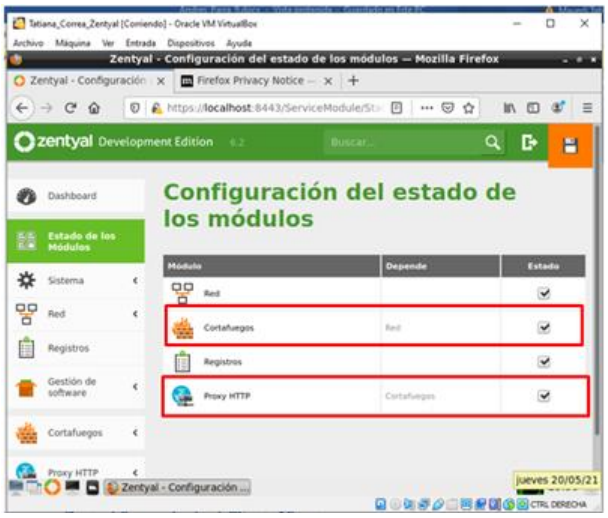

Figura 4.1. Configuración de los módulos

Para este punto se genera la construcción de una máquina virtual tipo escritorio la cual se usa para realizar las pruebas de funcionamiento del servidor. Después de su instalación en la opción Network y se crea un nuevo perfil de red con la dirección IP asignada al servidor.

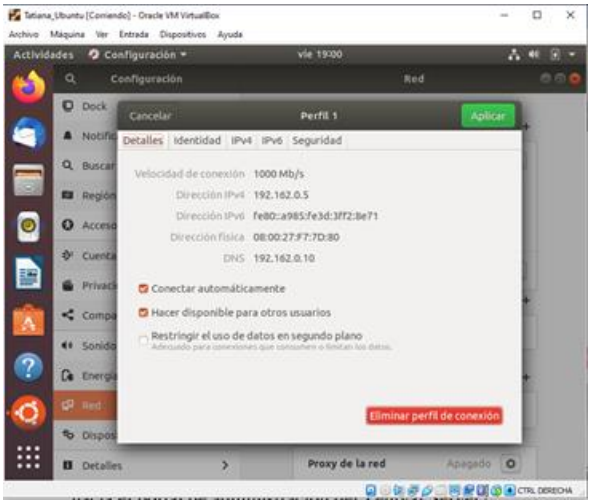

Figura 4.2. Configuración maquina cliente

Se ingresa al servidor Zentyal desde la maquina cliente y se comprueba su acceso, luego se procede a descargar los dominios de diferentes direcciones IP para facilitar las configuraciones del proxy y el bloqueo por firewall, estos son cargados en la opción de proxy HTTP – Listas por categorías

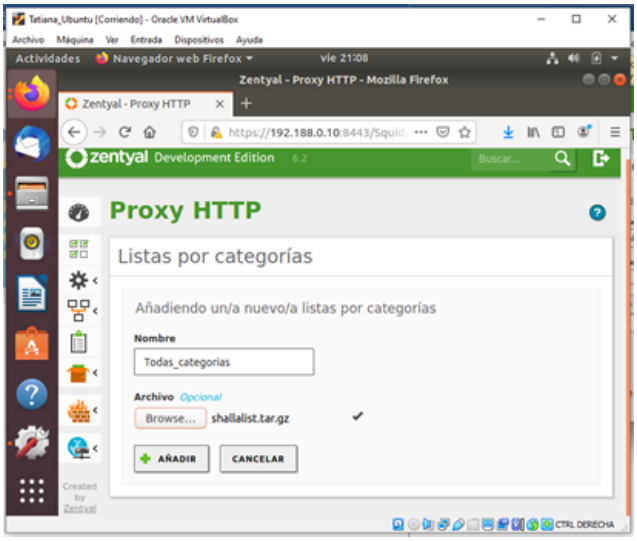

Figura 4.3. Configuración proxy

Para realizar este paso en el menú perfiles de filtrado y se seleccionó la opción de categorías de dominio en donde se buscó las categorías que tenga relación con redes sociales y entretenimiento de los cuales se desea denegar el acceso.

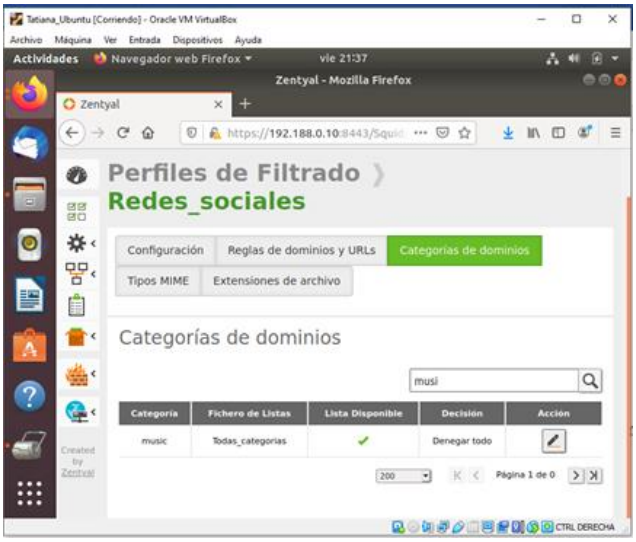

Figura 4.4. Denegación de acceso

A continuación en la configuración de reglas de acceso en las cuales se asignaron el periodo de tiempo que se desea que se ejecute el proxy y el cortafuegos, también se ajusta el origen que sería Cualquiera y aplicar perfil de filtrado a redes sociales

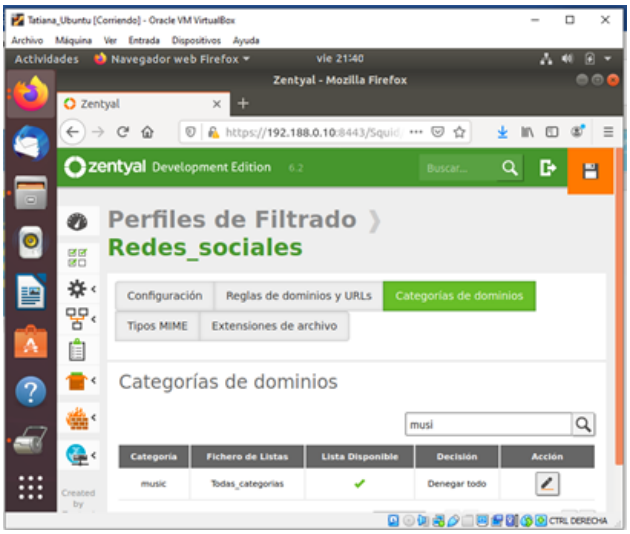

Figura 4.5. Configuración de reglas de acceso

En la máquina virtual se procede a abrir el navegador de Firefox donde en la opción **preferences**, se selecciona **general** y luego de esto **Network settings,** se establece la configuración manual de proxy y se asignó la dirección IP configurada junto con el puerto para http proxy y hptts proxy y se selecciona la opción para no proxy for

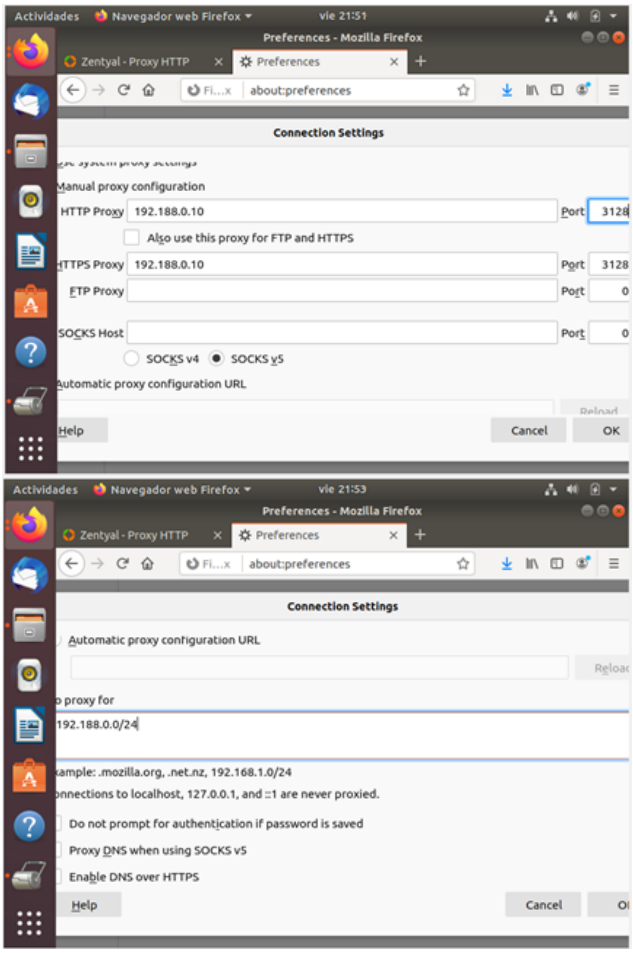

Figura 4.6. Configuración de Connection Settings

Se procede a validar la configuración realizada para las redes sociales en donde se ingresará a Facebook donde su acceso debe ser denegado y su mensaje de error debe ser de Proxy server

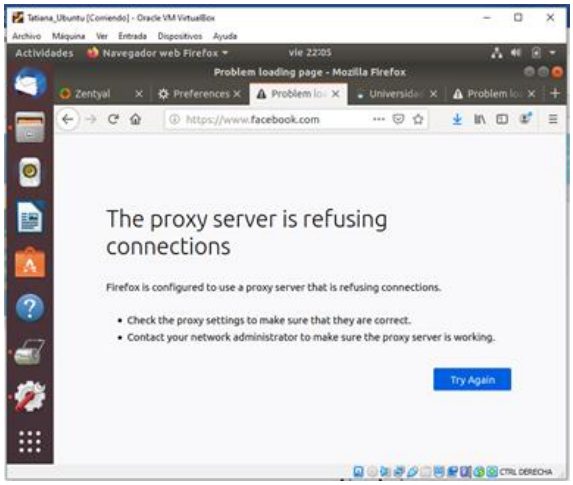

Figura 4.7. Acceso denegado a Facebook

Ahora se prueba el ingreso a la plataforma de la UNAD donde su acceso no debe ser denegado ya que no está

dentro de las plataformas configuradas en el proxy y cortafuegos

Figura 4.8. Acceso a la plataforma UNAD

3.4. TEMATICA 4: FILE SERVER Y PRINT SERVER

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

Configuración del SO Zentyal Server

Mediante el servicio de impresión se solucionan diferentes problemáticas, por ejemplo, el de imprimir de manera remota diferentes archivos que se desee, este servicio permitirá a los equipos que estén conectados a la red poder acceder a la misma impresora.

En la opción compartición de ficheros se añade uno nuevo para ser compartido.

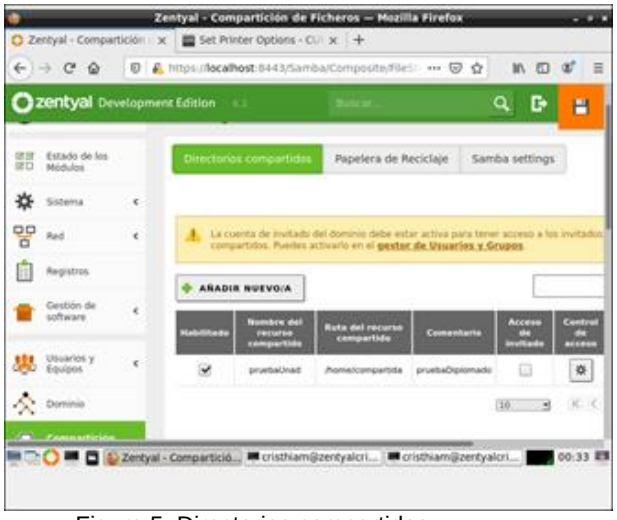

Figura 5. Directorios compartidos

Se adiciona la impresora virtual por medio de CUPS

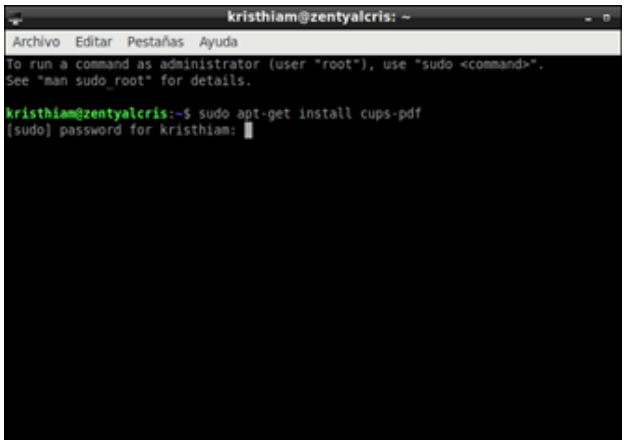

Figura 5.1. Instalación impresora virtual (Cups)

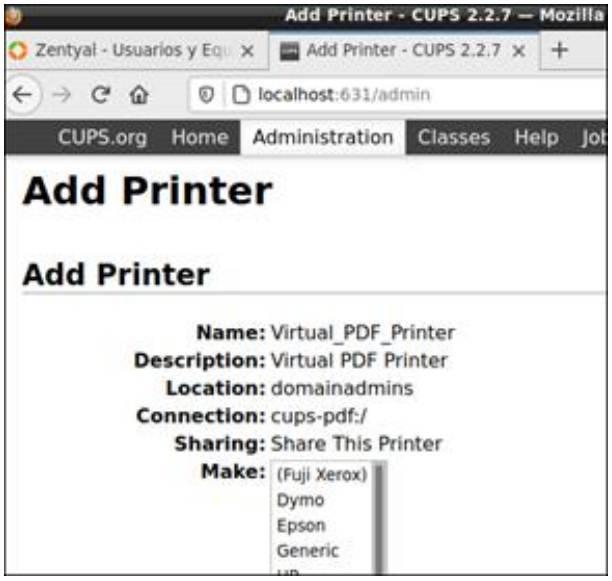

Figura 5.2. Configuración impresora virtual por dirección: localhost:631/admin

En el cliente que para este caso se trabajará en Ubuntu, se debe instalar y configurar el usuario de Samba, allí se configurará el archivo smb.conf que se encuentra alojado en la ruta: /etc/samba//smb.conf

Para la instalación de Samba se debe ejecutar las siguientes líneas de código en la terminal:

a. Sudo apt get install samba.

Para verificar el estado de su ejecución se ejecuta:

b. Sudo systemctl status nbmd

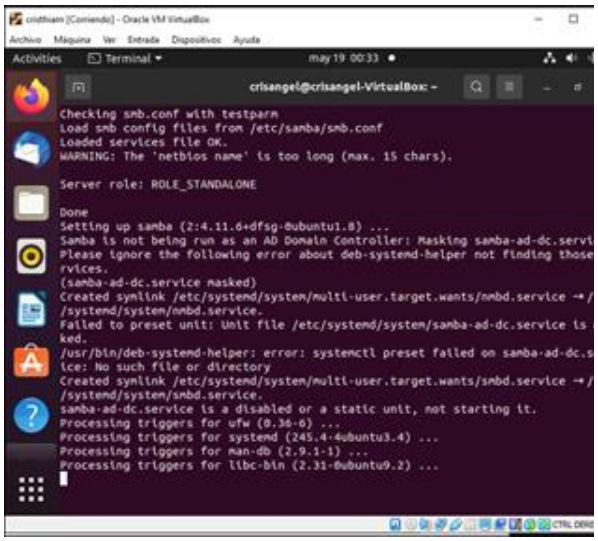

Figura 5.3. Instalación samba

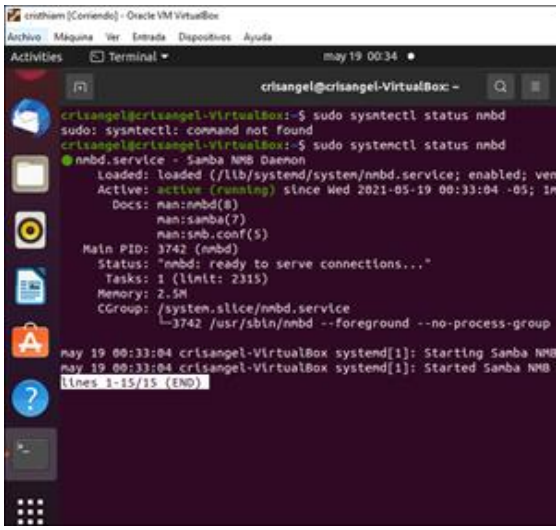

Figura 5.4.Estado de Samba

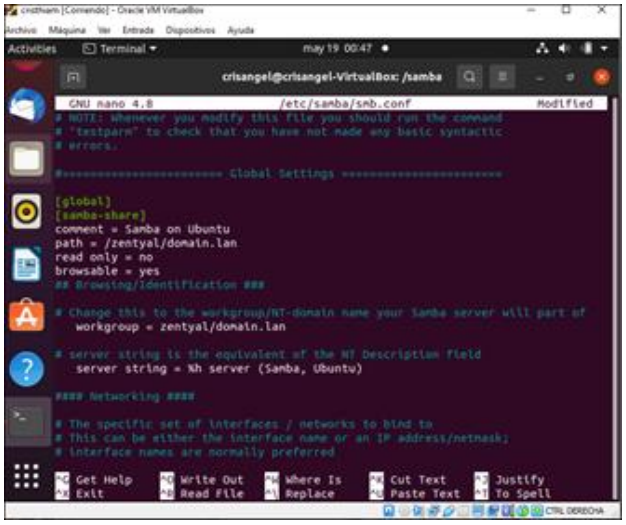

Figura 5.5. Edición archivo de configuración sudo nano /etc/samba/smb.conf

En el archivo Samba

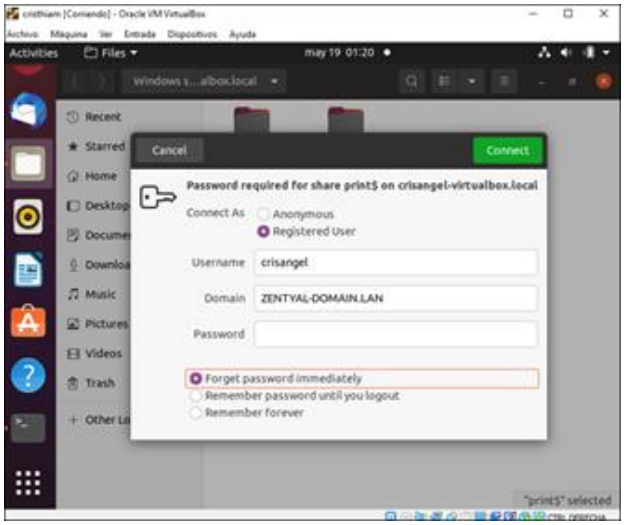

Figura 5.6. Acceso al servidor Zentyal

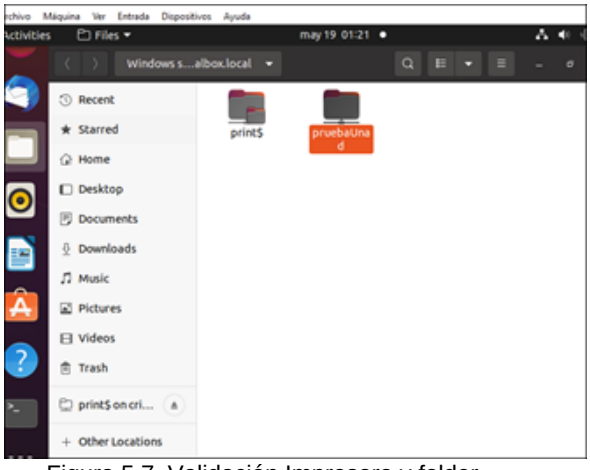

Figura 5.7. Validación Impresora y folder

3.5. TEMATICA 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Se precede a instalar ZENTYAL SERVER 6.2

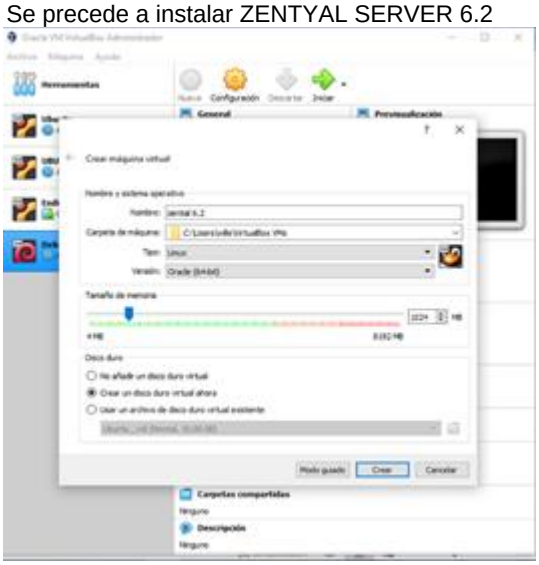

Figura 6.1 Instalación de ZENTYAL 6.2

Se siguen las instrucciones en pantalla tal como se ha realizado las instalaciones de los programas anteriores de Ubuntu y Debian

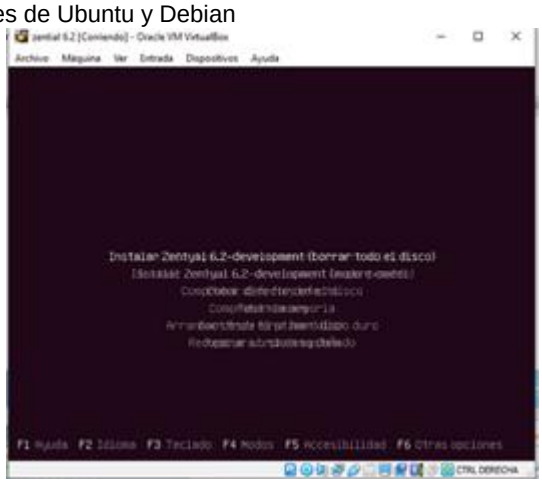

Figura 6.2 Instalación de ZENTYAL 6.2

Se configuran los diferentes complementos de la instalación entre ellos la red

Figura 6.3 Configuracion de complementos de ZENTYAL 6.2

Una vez terminada la instalación se procederá a ingresar el usuario y contraseña que se habían diligenciado en la configuración de la instalación.

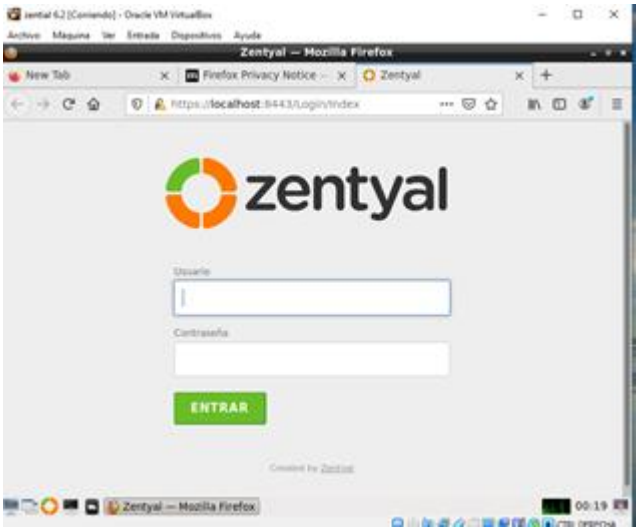

Figura 6.4 ingresar el usuario y contraseña

Al iniciar por primera vez Zentyal este solicitara los servicios a instalar, en este caso se selecciona VPN CERTIFICADO DE AUTORIZACION Y FIREWALL

Figura 6.5 instalación de la VPN

Se realiza la configuración de la red interna por DHCP

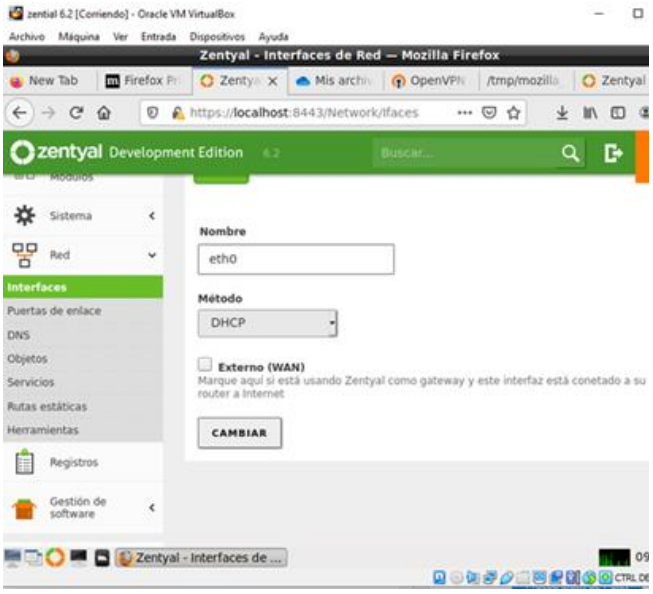

Figura 6.6. Instalación de ZENTYAL 6.2

Se realiza la creación de los certificados para el servidor y para los clientes

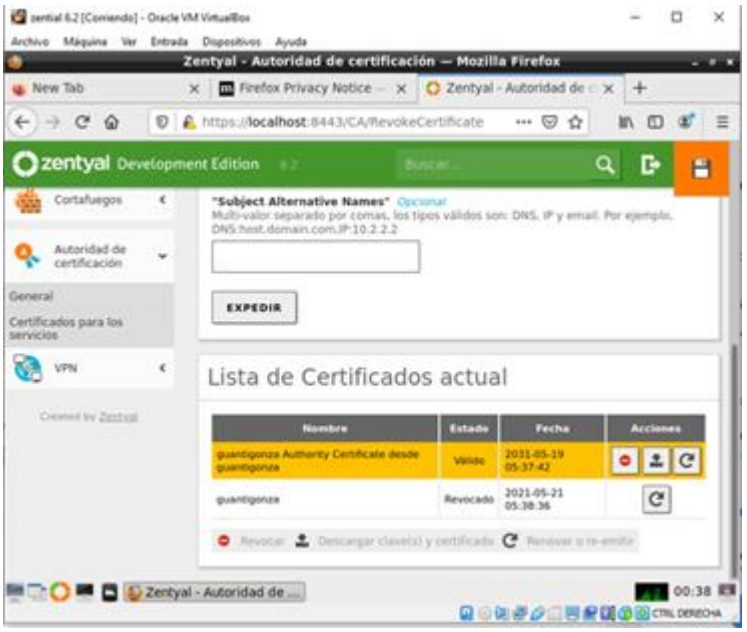

Figura 6.7 creación certificados

Se procede a crear el servidor VPN

Figura 6.8 servidor VPN

Se procede a crear el certificado para clientes y se genera el comprimido de este para ejecutarlo en esta maquina

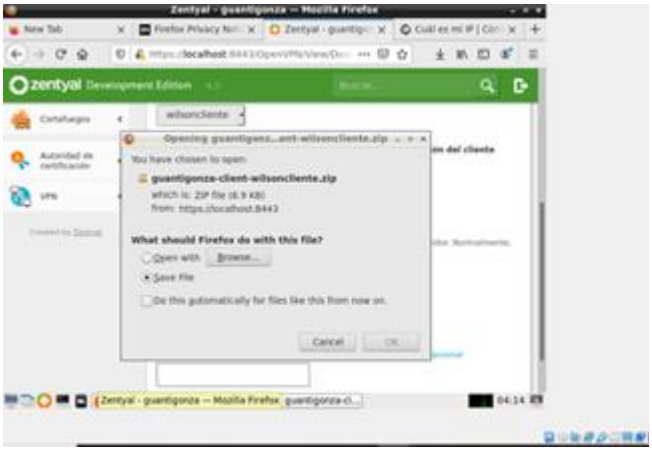

Figura 6.9 Certificados cliente

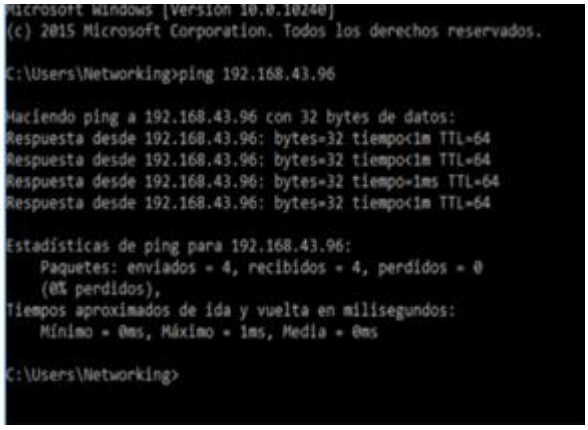

Figura 6.11 ping de prueba

Se realiza la instalación en Windows del cliente VPN y se descarga el certificado para realizar la interfase de esta.

Figura 6.10 Instalación de cliente VPN en Windows

Se valida que dentro del zentyal aparezca la conexión activa de la vpn establecida

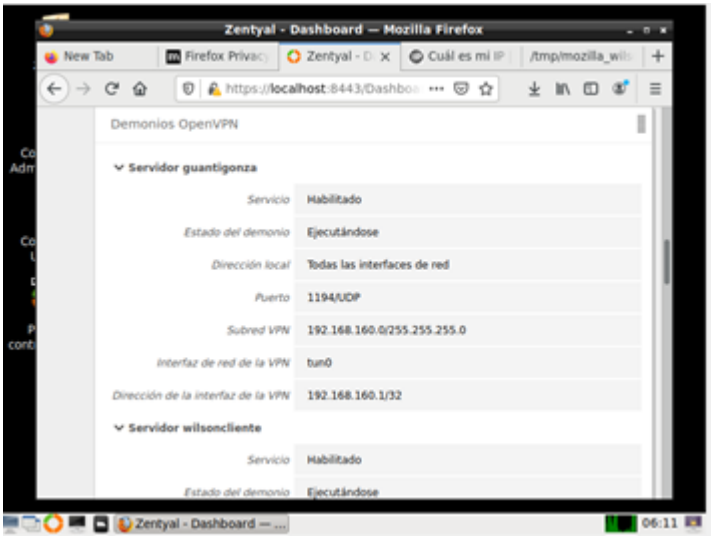

Figura 6.12.1 visor VPN servidor

Establecida la conexión se procede a realizar la prueba, en este caso se validó la dirección ip que tiene el servidor.

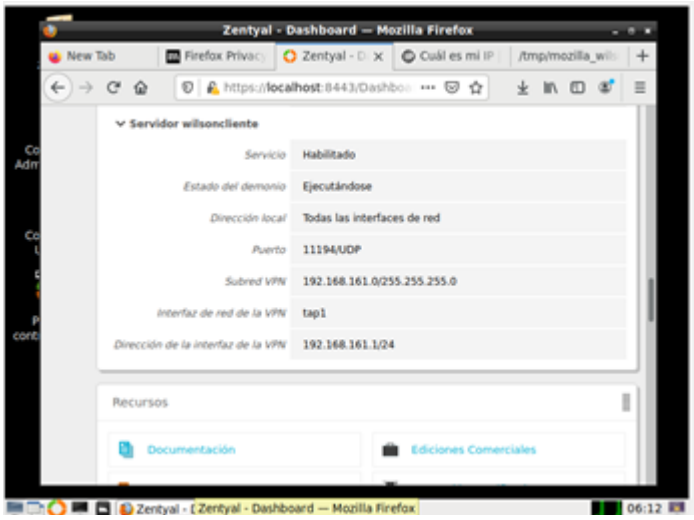

Figura 6.12.2 Ivisor VPN cliente

4 CONCLUSIONES

El uso de software como Zentyal, permite administrar y unificar de manera idónea los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro con la integración de servicios como DNS/DHCP, CA, VPN, etc. Gracias a esto se puede realizar también un monitoreo constante y un filtro de información a subir y a bajar con el fin de disminuir riesgos ante posibles ataques y demás, esto, con el fin de poder determinar un grado superior de seguridad dentro de las redes de las organizaciones bajo requerimientos específicos.

A su vez, se profundizó en el método de cortafuegos que puede ser utilizado por medio de servidores, los cuales, ayudan a restringir de forma masiva accesos a diferentes plataformas como son las redes sociales y permitiendo la navegación a paginas a las que se desea permitir el acceso.

Se logra analizar la importancia de los servicios de file server y print server, generando ejemplos prácticos que validan y simulan un ejercicio para compañías pequeñas y medianas, resaltando los beneficios que esta configuración trae.

Zentyal permite configurar de forma sencilla, diferentes funcionalidades con el uso de pocos clics, esto hace que sea una herramienta completa, en cuanto a la configuración de controlador de dominio, es una de las grandes ventajas de esta distribución, al tener integrado samba, permite manejar directorios activos de Windows server. Por otro lado, el manejo de Zentyal, requiere un conocimiento previo en los ficheros de configuración, ya que, cada cambio que se realiza en el GUI, muestra que archivos se van a modificar, con lo que se debe comprender los cambios realizados en el sistema. Finalmente, videncia la implementación de una herramienta que permite establecer conexiones remotas a través de VPN, se logra verificar como se realiza la conexión de un servidor con un cliente manejando por medio de interfase

5 REFERENCIAS BIBLIOGRAFICAS

D. del Barrio. (2012, Julio 16). Firewall Zentyal. El Taller del Bit. [En línea]. Disponible en: http://eltallerdelbit.com/firewall-zentyal

Zentyal Community. (2014). Es/3.5/Cortafuegos. Zentyal Wiki. [En línea]. Disponible en: https://wiki.zentyal.org/wiki/Es/3.5/Cortafuegos

Zentyal (2021). Instalación. Recuperado de: https://doc.zentyal.org/7.0/es/installation.html

Zentyal (2021). Primeros pasos con Zentyal. Recuperado de: https://doc.zentyal.org/7.0/es/firststeps.html

Zentyal (2021). Actualización de software. Recuperado de: https://doc.zentyal.org/7.0/es/software.html

Zentyal (2021). Servicio de Proxy HTTP. Recuperado de: https://doc.zentyal.org/7.0/es/proxy.html