INSTALACION Y CONFIGURACION DEL SISTEMA OPERATIVO ZENTYAL SERVER 6.2 PARA ADMINISTRAR LOS SERVICIOS DE INFRAESTRUCTURA TI

Darwin Andrey Céspedes Jiménez
e-mail: dacespedesj@unadvirtual.edu.co
Lucas Hernando Bonilla Conde
e-mail: lhbonillaco@unadvirtual.edu.co
Duvan Andres Barrera Figueroa
e-mail: dabarrerafi@unadvirtual.edu.co
Veronica Yurany Muñoz Bolaños
e-mail: vymunozb@unadvirtual.edu.co
Natalia Palacio Leonel
e-mail: npalaciol@unadvirtual.edu.co

RESUMEN: *El actual documento describe la solución a los requerimientos específicos del cliente, basados en un sistema operativo GNU/Linux instalamos, configuramos y colocamos en marcha Zentyal Server 6.2. el cual contiene los servicios de infraestructura TI que permiten satisfacer las necesidades tecnológicas solicitadas, dentro de las cuales gestionamos DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.*

Ya que bajo la implementación de dichos servicios podemos articular diferentes protocolos de control, verificación y transmisión de datos, logrando así poder conectar diferentes tipos de dispositivos sobre una misma red, convirtiendo a esta en el puente que logre la comunicación entre el servidor y estos dispositivos, colocando como base fundamental la protección de los datos de los usuarios que acceden a dicha red bajo la creación de protocolos tanto para la conexión como para el intercambio de datos a través de los diferentes servicios configurados en nuestro servidor.

PALABRAS CLAVE: Interfaces, Proxy, VPN, Servicios, Dominio, Red, Internet, DHCP, Datos, Zentyal.

INTRODUCCIÓN

El desarrollo de la presente actividad busca demostrar los resultados obtenidos con la configuración e implementación de los servicios de infraestructura a nivel de redes internas y externas, lo anterior por medio de Zentyal Server, el cual esta concebido para ser instalado en una maquina (real o virtual) funciona sobre la distribución de GNU/Linux Ubuntu en su versión para servidores, usando siempre las ediciones Long Team Support [1], la pruebas de implementación se realizaran sobre el sistema operativo Ubuntu el cual funcionara como cliente.

Para realizar dicha implementación se colocará en práctica los conocimientos adquiridos previamente en el desarrollo del diplomado, donde utilizaremos temáticas como DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN, para cada una de las temáticas se evidencia la instalación, configuración y funcionamiento, dando por solucionado las necesidades de seguridad en la infraestructura de la red.

1 TEMATICAS DESARROLLADAS

El artículo se elabora con la participación de forma activa y asertiva de los integrantes del grupo colaborativo, donde cada uno selecciono una de las temáticas dispuestas en la guía de actividades y elaboro el desarrollo de la actividad con las evidencias correspondientes. La tabla 1 refleja el listado de las temáticas expuestas en el presente trabajo.

Tabla 1

N°	TEMÁTICA
1	DHCP Server, DNS Server y Controlador de Dominio
2	Proxy no transparente
3	Cortafuegos
4	File Server y Print Server
5	VPN

2 INSTALACION ZENTYAL SERVER

2.1 INSTALACION DE ZENTYAL SERVER 6.2

PASO 1: Seleccionamos la ubicación del país donde se va realizar la instalación de zentyal.

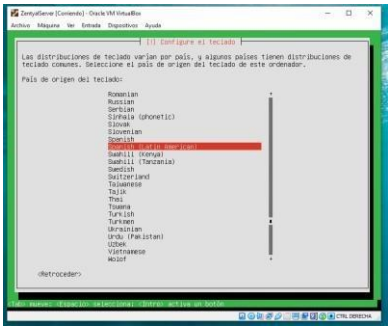

Figura 1: Selección del país

PASO 2: Se configura el idioma con el cual el teclado va trabajar dentro del sistema operativo.

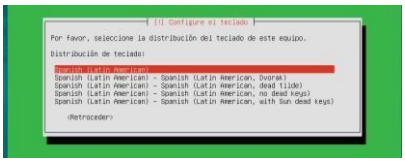

Figura 2: Selección de distribución de teclado

PASO 3: Se espera hasta que el instalador descargue los módulos necesarios para el funcionamiento del sistema operativo de zentyal.

Figura 3: Configuracion de modulos de zentyal

PASO 4:Se configura la interfaz de red con la cual se va realizar la configuración de la red local que controlara zentyal desde su interce de administración.

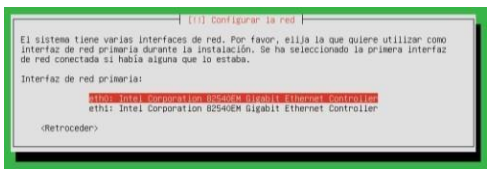

Figura 4: Configuracion de la interface de red

PASO 5: Se espera que se configure la modulos de DHCP para así aplicar sus configuraciones a la interce de la red local seleccionada anteriormente.

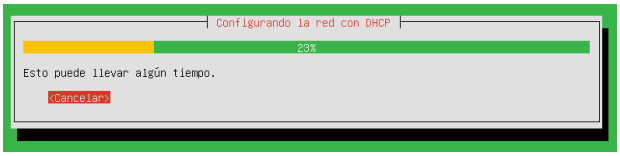

Figura 5: Configuración de red DCHP

PASO 6: Ahora se configura la dirección ip con la cual será reconocido y trabaja el servidor donde estará contenido el sistema operativo de zentyal.

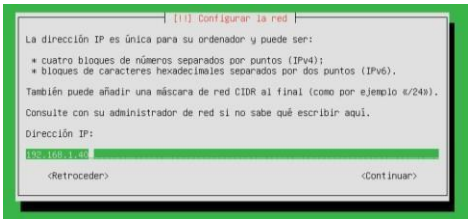

Figura 6: Configuracion de direccion ip

PASO 7: Configuramos la máscara de red con la cual trabaja nuestra red para así poder reconocer posteriormente la puerta de enlace de la misma.

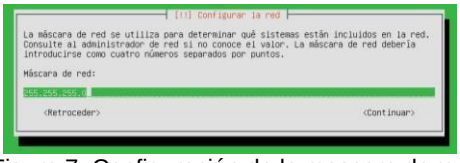

Figura 7: Configuración de la mascara de red

PASO 8: Confirmamos y verificamos la puerta de enlace de la red sienda esta la base para la asignación y configuración del rango de direcciones ip de la red.

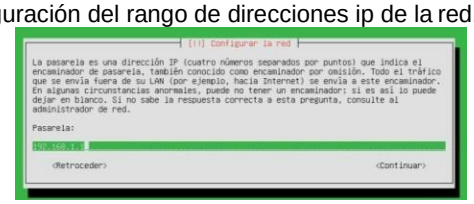

Figura 8: Configuracion de la puerta de enlace

PASO 9: Asignamos el nombre a nuestra máquina zentyal esto se hace que físicamente se reconozca en la agrupación de la red.

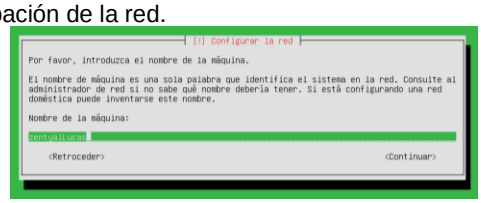

Figura 9: Configuracion del nombre del equipo

PASO 10: Configuramos el dominio local del Zentyal para así poder acceder a su panel administrativo desde el mismo servidor.

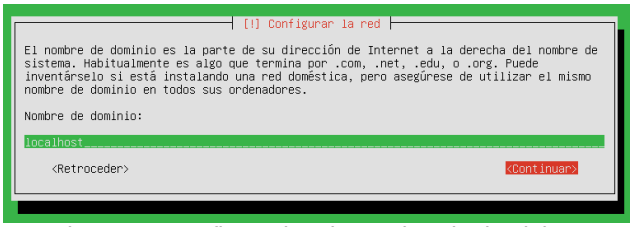

Figura 10: Configuracion de nombre de dominio

PASO 11: Configuramos el nombre del usuario que actuará como el administrador del servidor de zentyal.

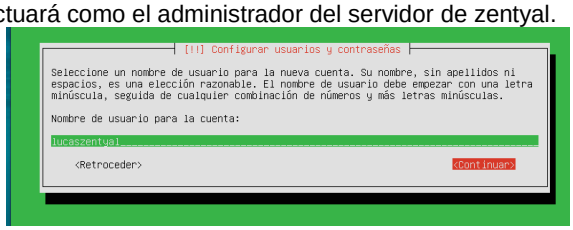

Figura 11: Configuracion de usuario de zentyal

PASO 12: Configuramos la contraseña para poder acceder al panel administrativo del zentyal.

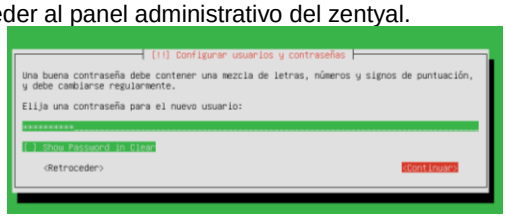

Figura 12: Configuracion de asignacion de contraseña

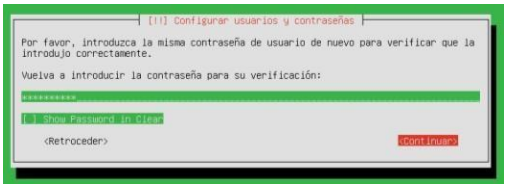

Figura 13: Confirmacion de la contraseña

PASO 13: Esperamos a que el kernel el cual contiene el núcleo del sistema y los programas del mismo se cargue, este procesos puede variar según la conexión de internet que tengamos.

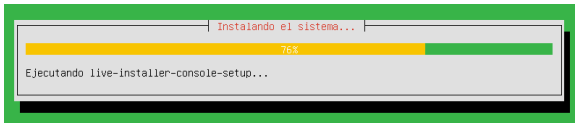

Figura 14: Instalación del núcleo del sistema

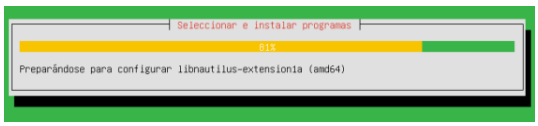

Figura 15: Instalacion de programas de Zentyal

PASO 14: Se verifica que los módulos del sistema operativo zentyal se hayan cargado correctamente, esto lo confirma el propio instalador a partir de una notificación.

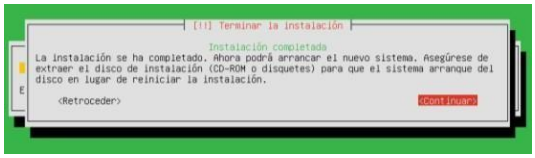

Figura 16: Confirmacion de instalación

PASO 15: Reiniciamos el sistema operativo zentyal para que este pueda arrancar desde 0 y así confirmar que este se encuentra funcionando correctamente.

Figura 17: Reinicio del sistema zentyal

PASO 16: Desde de máquina Desktop ingresamos al panel administrativo del zentyal buscando así comprobar que la configuración de red aplicada anteriormente este correctamente configurada y así mismo colocamos las credenciales anteriormente creadas en el proceso de instalación.

Figura 18: Inicio del panel de administrativo de zentyal

2.2 TEMATICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

PASO 1: Activamos el módulo DHCP tras haber asignado el rango de direcciones ip que en este caso 192.168.1.1 hasta 192.168.1.254 teniendo en cuenta el limite bando de ancha.

Figura 19: Activación del servicio DCHP

PASO 2: Confirmamos que queremos activar el módulo y continuamos hacia su configuración.

Figura 20: Confirmación de activacion DHCP

PASO 3: Ahora para configurar el dominio local que nos proporciona zentyal debemos configurar sus especificaciones de respuesta a partir de la DNS local del mismo la cual va terminar apuntando así la misma dirección ip estática que se le fue configurada previamente a servidor de zentyal.

Figura 21: Configuracion del dominio

PASO 4: Verificamos el rango de direcciones ip de nuestro servidor DHCP para saber que nuestra máquina le fue asignada de forma correcta una dirección ip de dicho rango.

Figura 22: Verificación de los rangos de ip DHCP

PASO 5: Verificamos si la asignación de dirección ip para la maquina desktop se realizo correctamente haciéndole ifconfig a la misma.

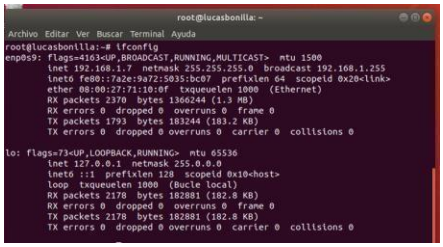

Figura 23: Verificacion de asignacion de ip

PASO 6: Ya con esta configuraciones listas debemos verificar que nuestro equipo ya se encuentre dentro de nuestra red para ello confirmamos ello haciendo ping tanto al servidor como al cliente (Desktop).

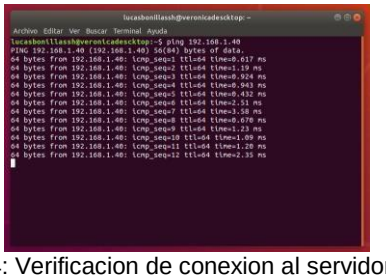

Figura 24: Verificacion de conexion al servidor zentyal

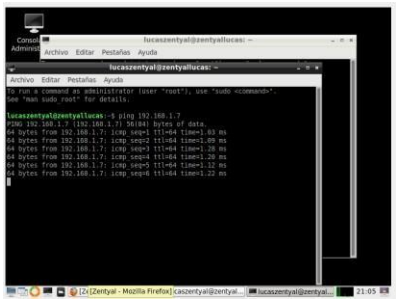

Figura 25: Verificación de conexión al cliente

PASO 7: Activamos los protocolos DHCP para el adaptador de red interna esto se hace para que este pueda proporcionar direcciones dinámicamente a los dispositivos que se conecte en un futuro a nuestra red.

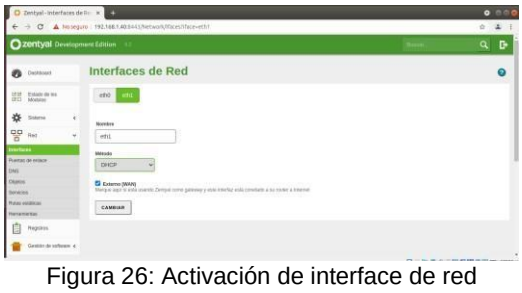

Figura 26: Activación de interface de red

PASO 8: Confirmamos los cambios de los módulos de DHCP que tenemos sobre el adaptador con esto las ip del rango se asignan automáticamente.

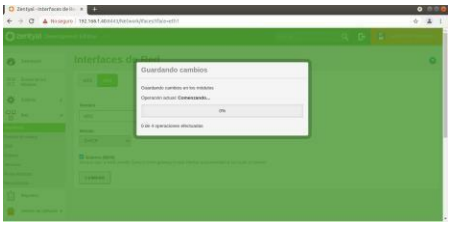

Figura 27: Confirmacion de activacion de interface

PASO 9: Verificamos los dominios que tenemos registrados para asi comprobar las configuraciones que tiene cada uno.

Figura 28: Verificación de creacion del dominio

PASO 10: Verificamos la configuración de los usuarios que se encuentra ingresado para el dominio que creamos anteriormente, para poder crear asi un nuevo usuario que sera asignado a su puesto de trabajo.

Figura 29: Verificación de usuarios del dominio

PASO 11: Configuramos el usuario con el cual procederemos a autenticarnos desde el puesto de trabajo desde el que nos conectaremos.

Figura 30: Creación de usuario nuevo del dominio

PASO 12: Ya creado nuestro usuario debemos asignarlo o un grupo de usuarios para poderle asignar permisos en este caso se le asignan el grupo de administradores para que en teoría pueda realizar ciertas configuraciones de servicios dentro de su puesto de trabajo.

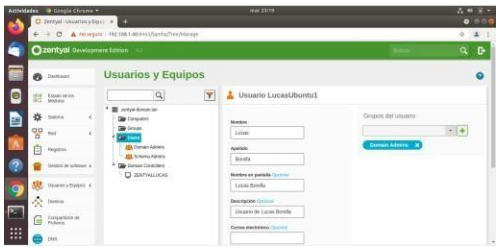

Figura 31: Asignación del usuario al dominio

PASO 13: Dentro de la maquina que se convertirá en el puesto de trabajo instalaremos el paquete likewise-open el cual permitirá que la máquina se conecte al dominio y así poder lograr que el zentyal lo ingrese y lo reconozca como puesto de trabajo.

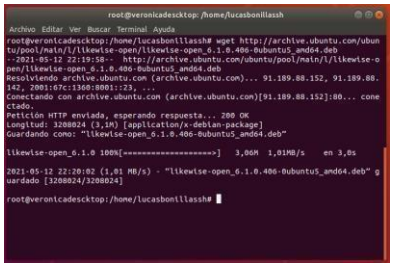

Figura 32: Descarga del conector del dominio

PASO 14: Descomprimimos e instalamos el paquete likewise-open para empezar la union del puesto de trabajo con el dominio.

Figura 33: Descompresión del conector del domino

PASO 15: Ahora por medio del comando domain-cli join [Dominio] [Usuario del dominio] procederemos a conectarnos al dominio y así lograr que el zentyal reconozca nuestro equipo como un puesto de trabajo.

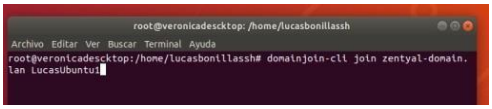

Figura 34: Conexión y registro del puesto de trabajo

PASO 16: Observamos como el dominio nos exige las credenciales (contraseña) y si todo esta correcto este nos dirá que se ha conectado de forma correcta y nos dirá que reiniciemos el equipo para asociar al inicio de session el dominio y usuario acreditado anteriormente.

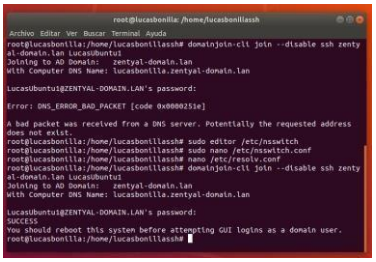

Figura 35:Confirmacion de conexion al dominio

PASO 17: Verificamos que el zentyal realizó el registro del usuario y del puesto de trabajo por lo cual sabemos que dicha máquina ya esta conectada a nuestro dominio y que ya es plenamente reconocida como un puesto de trabajo del mismo.

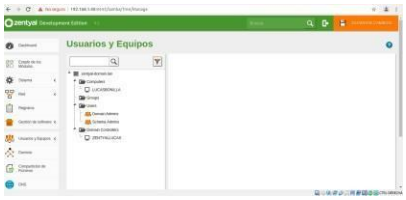

Figura 36: Verificacion de creacion del equipo

PASO 18: Configuramos el inicio de sesión del ubuntu para que permita el inicio de sesión con usuarios no creados por el mismo sistema esto se hace para que reconozca los usuarios creados por el dominio.

Figura 37: Configuración del inicio de ubuntu

PASO 19: Aceptamos el inicio de sesión por dominio agregando el parámetro de muestra manual de usuario.

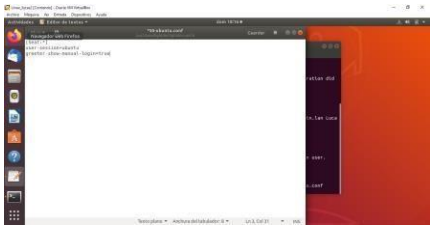
Figura 38: Activación de la sesión por dominio

PASO 20: Para iniciar sesion en ubuntu lo hacemos de la siguiente forma usuario@dominio

Figura 39: Ingreso del usuario con el dominio

PASO 21: Si acepta la existencia del usuario este pedirá la contraseña para iniciar sesión dentro de ubuntu.

Figura 40: Ingreso y validacion de contraseña

PASO 22: Después de iniciada la sesión comprobamos que nuestro usuario ha podido ingresar sin problemas, es de recordar que dicho usuario está vinculado a nuestro dominio.


Figura 41: Verificación del inicio de sesión

2.3 TEMATICA 2: PROXY NO TRANSPARENTE

A continuación, se realiza la 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.

PASO 1: una vez realizada la instalación del servidor zentyal, ingresamos las credenciales configuradas en el proceso de instalación.

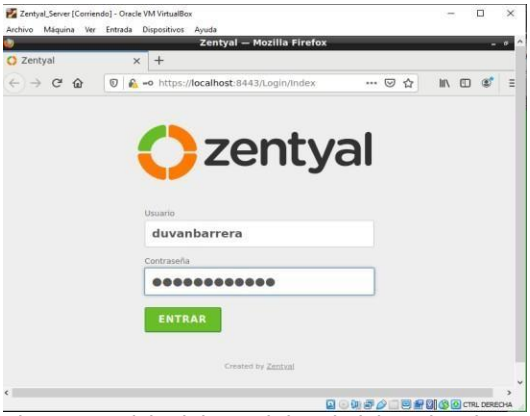

Figura 42 Inicio del panel de administrativo de Zentyal

PASO 2: Posteriormente podremos establecer diversos parámetros de configuración: IP asignada por DHCP o estática, IP asociada, etc. Estos parámetros pueden ser reconfigurados desde la interfaz de Zentyal en cualquier otro momento.

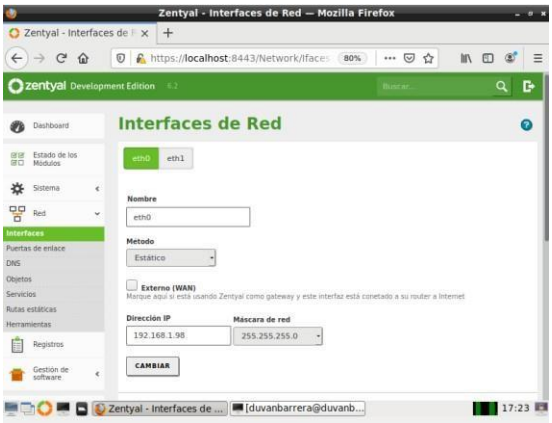

Figura 43 Configuración de interfaces de red

PASO 3: Se realiza la comprobación en la máquina cliente de Ubuntu configuramos la Red. Le asignamos la IP 192.168.1.101 al desktop y la IP 192.168.1.98 al zentyal, seguidamente hacemos pruebas de conexión entre el servidor Zentyal y la máquina cliente Ubuntu

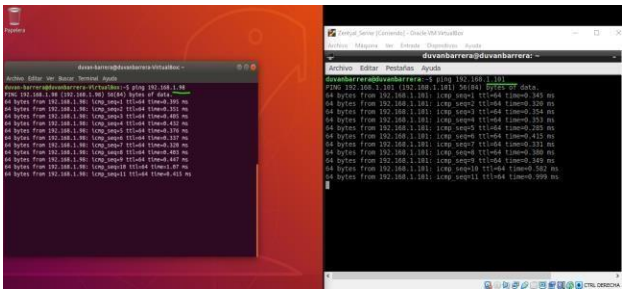
Figura 44 Verificación de conexión con la red de zentyal desde Ubuntu

PASO 4: Iniciamos con la configuración para el proxy no transparente, a través de un proxy que filtra la salida por medio del puerto 1230.

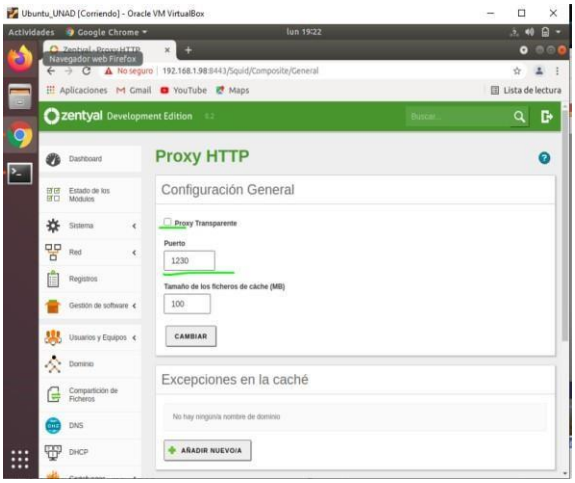

Figura 45 Configuración proxy 1230

PASO 5: Agregamos Perfiles de filtrado, añadimos u agregamos que deseamos bloquear a través de los diferentes perfiles.

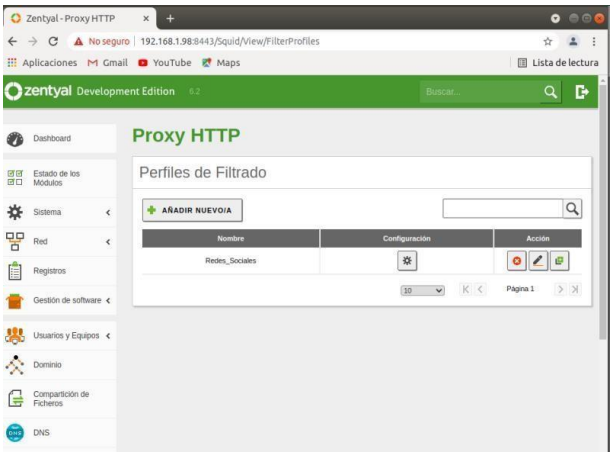

Figura 46 Se agrega los Perfiles de Filtrado

PASO 6: Se continua con la configuración del perfil filtrado redes sociales

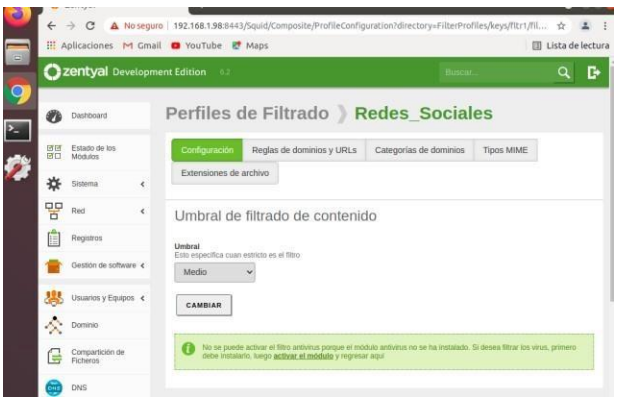

Figura 47: Umbral de filtrado de contenido

PASO 7: Añadimos las reglas del Dominio y URLS que deseamos denegar el acceso.

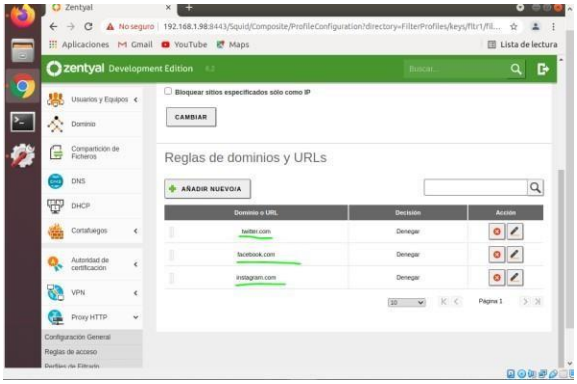

Figura 48 Reglas de Dominio y ARLs

PASO 8: Procedemos a definir las Reglas de acceso del Proxy HTTP.

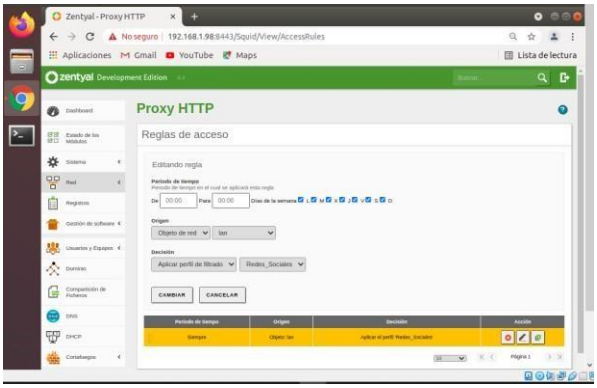

Figura 49 Proxy HTTP

PASO 9: Se configura las reglas de acceso por medio del proxy HTTP

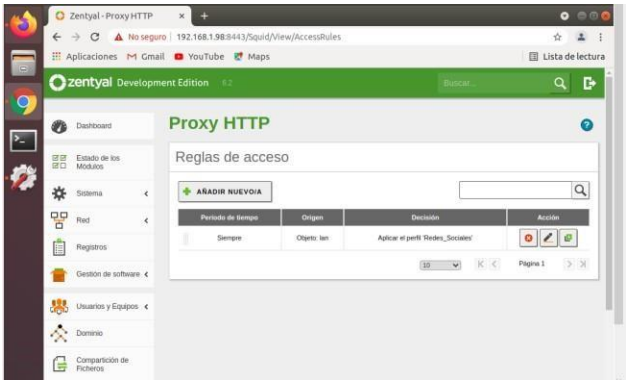

Figura 50 Reglas de acceso

PASO 10: Se realiza la configuración del navegador a través de un proxy que filtra la salida por medio del puerto 1230.

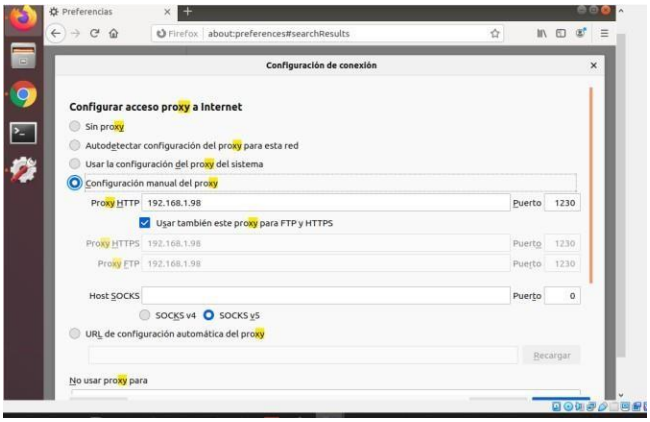

Figura 51 Configuración de acceso

PASO 11: Producto esperado y comprobado

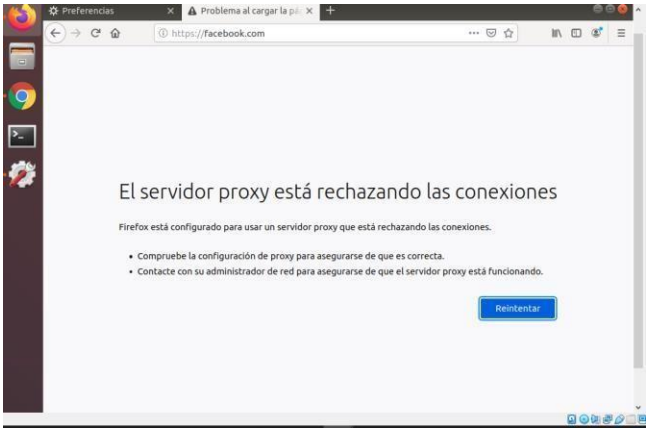

Figura :52 URL Facebook.com acceso denegado.

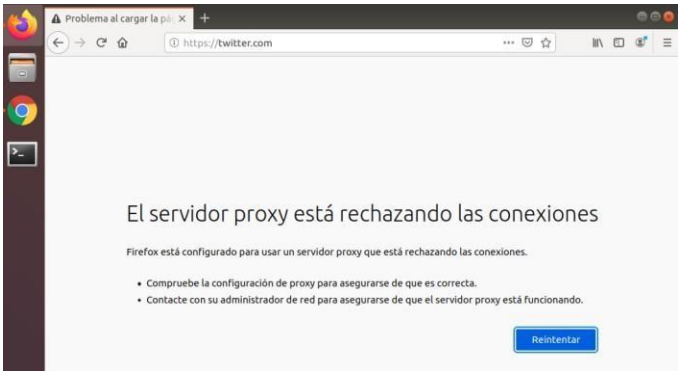

Figura: 53 URL twitter.com acceso denegado

PASO 12: Finalmente, se realiza pruebas y se comprueba a url que NO asignamos perfil de filtrado si tienen si tienen acceso.

Figura 54: url que NO asignamos perfil de filtrado.

2.4 TEMATICA 3: CORTAFUEGOS

La función principal de un firewall o corta fuego es bloquear cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet comúnmente llamado WAN.

PASO1: En la configuración inicial seleccionamos los componentes que queremos instalar, en este caso elegimos DCHP Server y Firewall.

Figura 55: Instalación de servicios.

PASO 2: Procedemos a configurar las interfaces de red, dejando una de forma externa que es la encargada de proporcionar internet a los dispositivos de la red interna y la otra se configura como interna la cual se conectara a los equipos cliente.

Figura 56: Configuración tipos de interfaces.

PASO 3: La primera interfaz la configuramos como estática y le asignamos una dirección ip disponible.

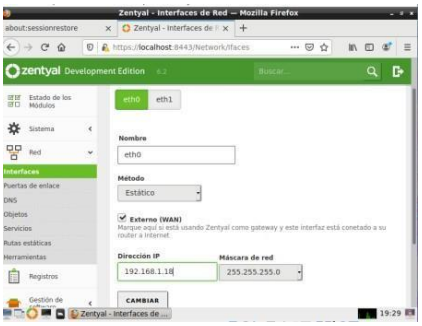

Figura 57: Configuración primera interfaz.

PASO 4: La interfaz interna la configuramos como estática y le asignamos una dirección ip.

Figura 58: Configuración segunda interfaz

PASO 5: Creamos y configuramos la puerta de enlace con dirección ip del router.

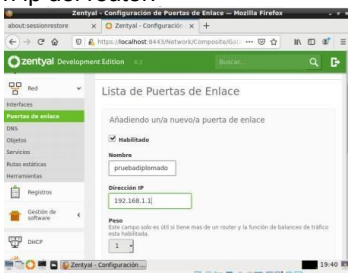

Figura 59: Asignación puerta de enlace.

PASO 6: Ahora procedemos a crear los objetos donde vamos a añadir las ip's de las redes que queremos bloquear, en este caso YouTube y Facebook.

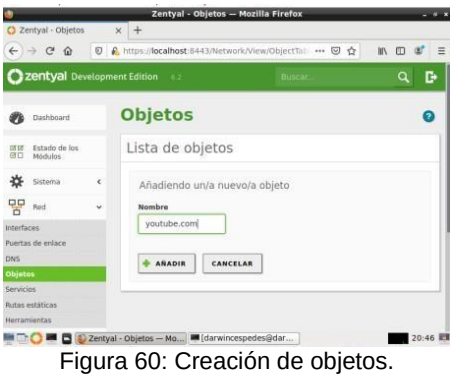

Figura 60: Creación de objetos.

PASO 7: Creamos el objeto YouTube y añadimos las ip's

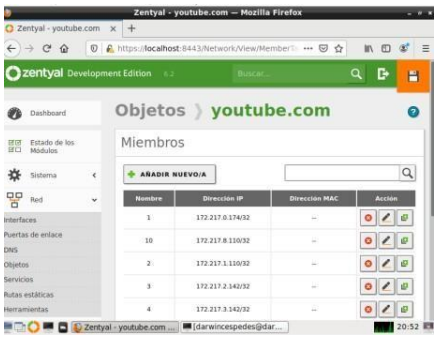

Figura 61: Objeto YouTube

PASO 8: Creamos el objeto Facebook y añadimos la ip.

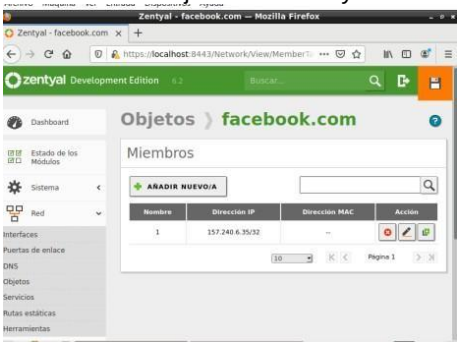

Figura 62: Objeto Facebook

PASO 9: Se evidencian los 2 objetos creados

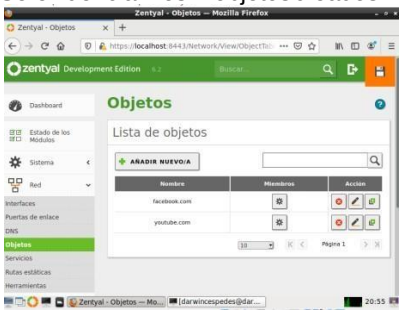

Figura 63: Objetos creados.

PASO 10: Ahora desde el servicio cortafuegos creamos la regla para el filtrado de paquetes de la red interna. Creamos la regla para denegar el tráfico al objeto de Facebook.

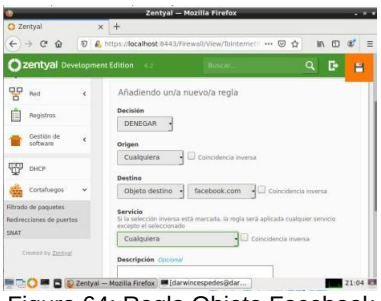

Figura 64: Regla Objeto Facebook.

PASO 11: Creamos la regla para denegar el tráfico al objeto de YouTube.

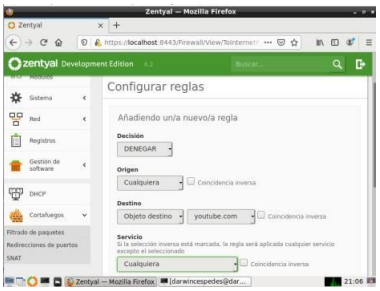

Figura 65: Regla Objeto YouTube

PASO 12: En el DCHP configuramos el rango de direcciones para la interfaz interna.

Figura 66: Asignación de Rango

PASO 13: En el Dashboard validamos las ip's asignadas por DHCP al S.O. Ubuntu Desktop.

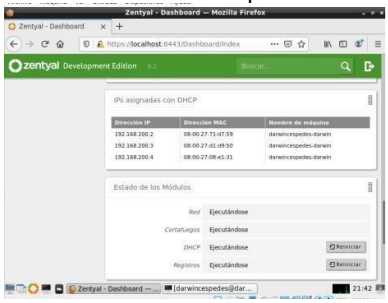

Figura 67: Asignación de ip's

PASO 14: En el Ubuntu Desktop validamos el acceso a internet, probamos con la página Outlook.com.

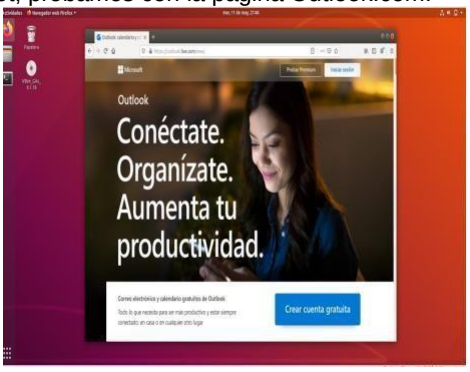

Figura 68: Conexión a Internet

PASO 15: Ahora probamos el acceso a las redes restringidas, donde no se realiza la conexión.

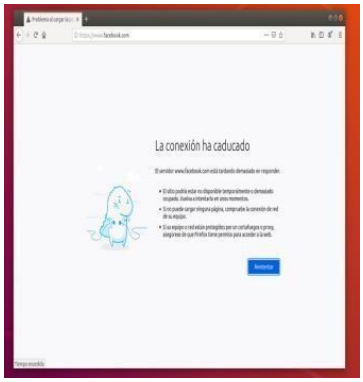

Figura 69: Comprobación Regla Facebook

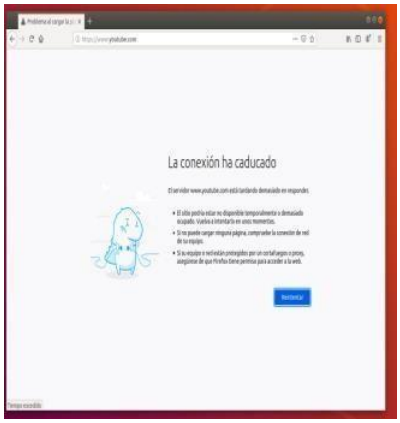

Figura 70: Comprobación Regla YouTube

2.5 TEMATICA 4: FILE SEVER Y PRINT SERVER

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.

PASO:1 Lo primero que se debe hacer es verificar en Zentyal que el módulo: Controlador de Dominio y Ficheros este activo.

Figura 71: Controlador de Dominio y Ficheros

PASO:2 Configuramos el Dominio para lo cual se debe agregar el nombre del dominio, se completan los demás campos y se guardan los cambios realizados.

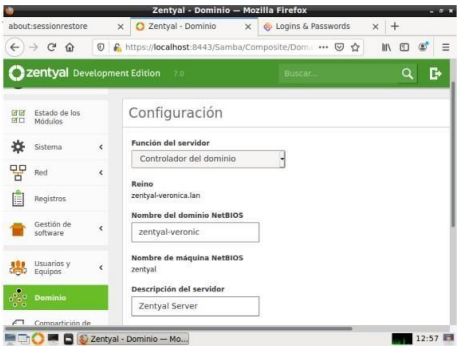

Figura 72: Configuracion de Dominio.

PASO:3
Configuramos grupo y usuario, en la opción de usuarios y equipos se da clic en gestionar donde se despliega la opción Groups, en la parte inferior se da clic en el símbolo + y se da añadir nuevo grupo.

Figura 73: Cofiguracion de Grupo y Usuario.

PASO 4: El siguiente paso es asignar nombre del grupo en este caso: UNAD,como se muestra en la
Figura anterior.

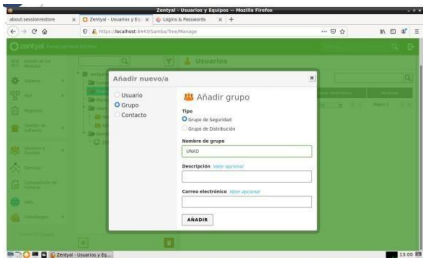

Figura 74: Asignación de Nombre al Grupo.

PASO:5 En el siguiente paso se hace lo mismo que el anterior, donde se crea un nuevo usuario, para
lo cual vamos a la opción Users añadir nuevo, se deben completar los campos, teniendo en cuenta seleccionar el grupo que se creó anteriormente.

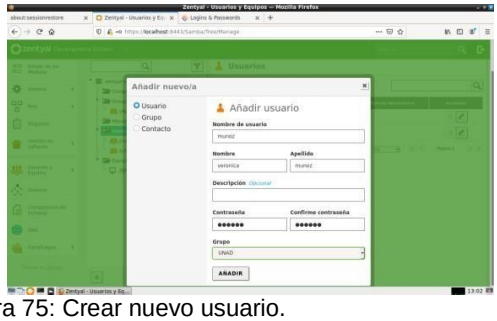

Figura 75: Crear nuevo usuario.

PASO 6:Se crea un fichero , se comparte y se configura su acceso, para lo cual es necesario, dirigirse a la opción de: Compartición de ficheros ubicado en la parte lateral izquierda, se da clic en añadir nuevo, se diligencian los cambios, donde se debe dar nombre del recurso compartido.

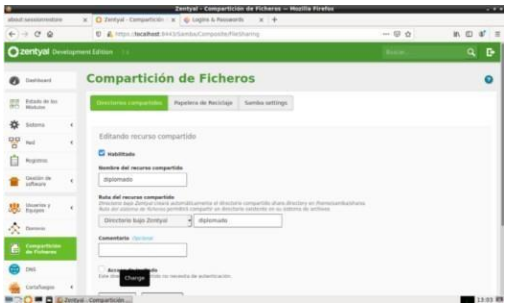

Figura 76:Comparticion de Ficheros

PASO7: El siguiente paso es dirigirse a Directorios compartidos (Diplomado) que fue creado anteriormente. Dando clic en Añadir Nuevo(a). Para lo cual se debe seleccionar el usuario y asignar los permisos necesarios, finalmente se da clic en añadir.

Figura 77: Directorios Compartidos.

PASO 8: Seguidamente lo que se hace es ingresar al Ubuntu desktop y en la parte de archivos, se conecta al servidor digitando smb://192.168.10.1 y clic en conectar:

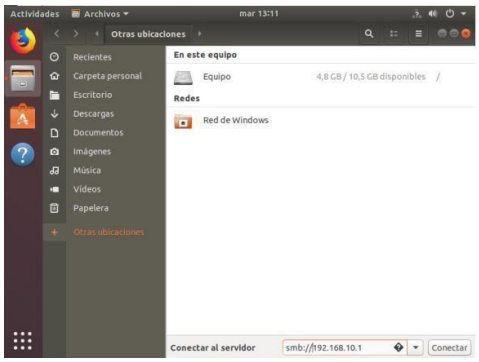

Figura 78: Conexión desde Desktop con IP.

PASO 9: El siguiente paso es ingresar a directorio creado por medio de compartición: diplomado con la respectiva ip : 192.168.10.1, donde se deben digitar las credenciales solicitadas, se da clic en conectar.

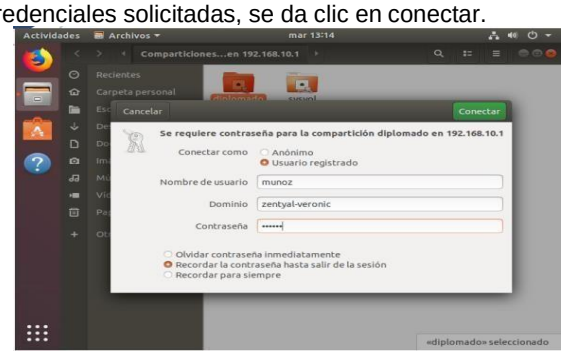

Figura 79: Ingresando al directrio Diplomado por medio de la IP asignada.

PASO 10: Se observa que se logra ingresar con éxito al recurso compartido, como se muestra en la Figura anterior.

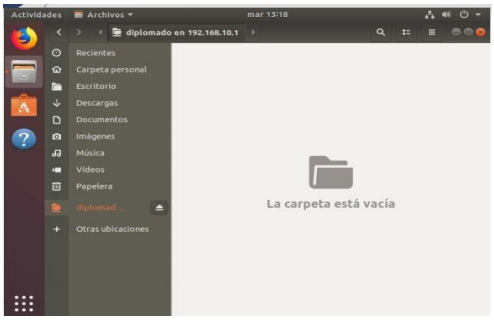

Figura 80: Ingresando al recurso compartido.

PASO 11: Lo que se procede a hacer para configurar y compartir la impresora es necesario hacer uso de CUPS, para lo cual se procede a instalar mediante el comando: sudo apt install cups (en mi caso ya se realice la respectiva instalación).

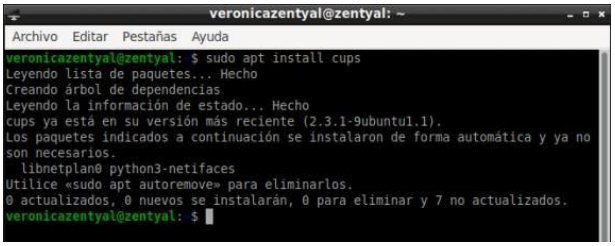

Figura 81: Configurando la impresora mediante CUPS.

PASO:12 El siguiente paso es crear una máquina virtual, para lo cual se debe instalar CUPS-PDF,para lo cual se utiliza el comando: sudo apt install cups-pdf.

Figura 82: Instalando CUPS-PDF.

PASO 13: El siguiente paso es acceder a cups mediante localhost:631, en administración se selecciona
Add Printer para agregar la impresora.

Figura 83: Acceder a cups mediante localhost:631.

PASO 14: El siguiente paso es agregar nombre, “diplomado_pdf” a la impresora para activar la compartición.

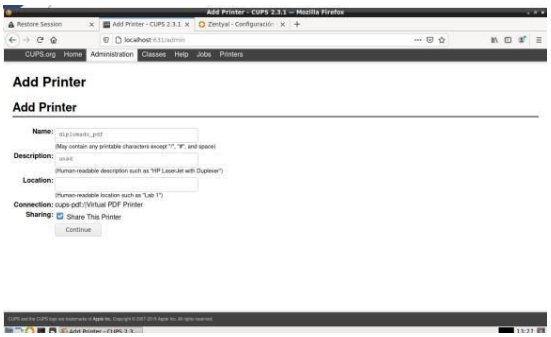

Figura 84: Activar la compartición.

PASO 15: El siguiente paso es seleccionar la opción driver genérico.

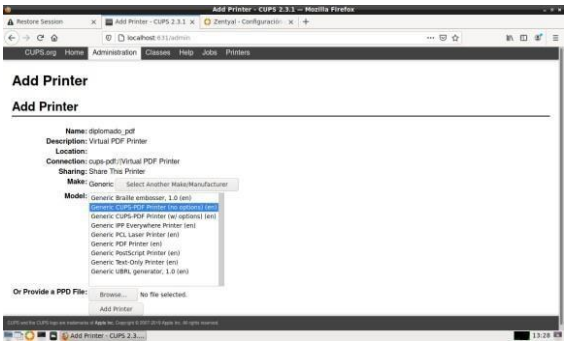

Figura 85: Seleccionar Driver.

PASO 16: Se puede observar que la impresora ha sido instalada exitosamente.

Figura 86: Impresora Instalada.

PASO 17: El siguiente paso es dirigirse a la maquina ubuntu desktop en la opción impresoras, en la pestaña servidor se digita la IP, de Zentyal y se puede ver la impresora compartida, se da clic en ella para agregarla.

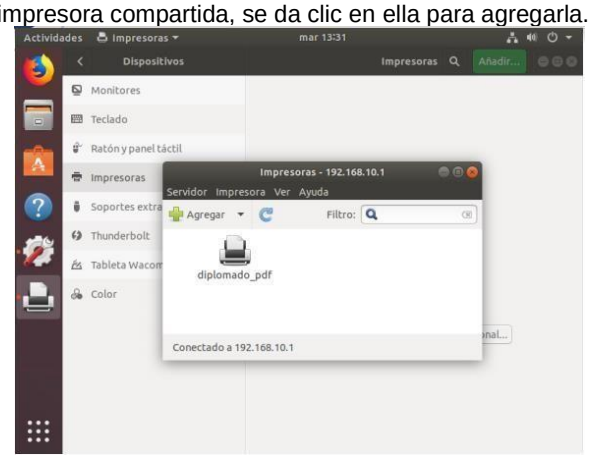

Figura 87: Impresora Compartida.

PASO:18 Ahora para comprobar la configuración de la impresora lo que se hace es dirigirse a configuración, imprimir página de prueba, para verificar funcionamiento como lo muestra la Figura anterior.

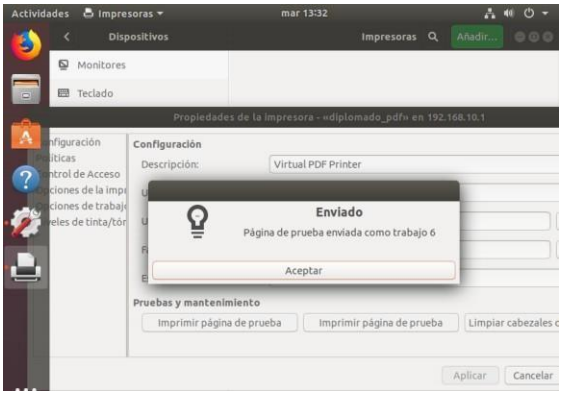

Figura 88: Comprobando Configuracion.

PASO 19: Ahora se puede verificar en el servidor que la configuración se realizó correctamente como lo muestra la Figura anterior.

Figura 89: Verificando la configuración en el servidor.

2.6 TEMATICA 5: VPN

La implementación de VPN tipo cliente – servidor, permite establecer un túnel privado de comunicación entre equipos sin importar donde estén ubicados geográficamente, de forma segura y confiable. Dentro de los servicios que ofrece Zentyal se encuentra la instalación del servidor VPN, mediante la implementación de OpenVPN, permitiendo en este caso establecer comunicación entre un equipo cliente y un servidor.

Importante que durante el primer arranque de Zentyal se configure las interfaces de red:

Una vez completada la descarga el sistema nos dirige a la configuración de tipo de interfaces.

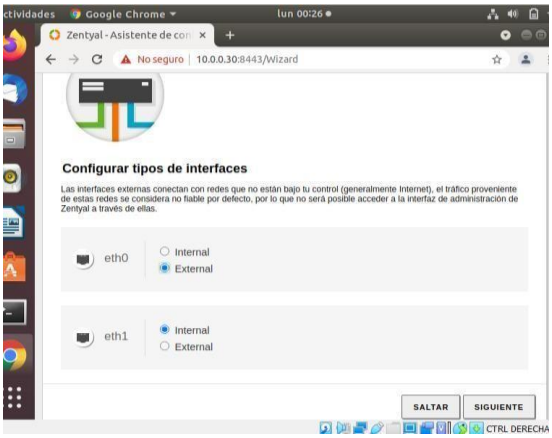

Figura 90: Configuración tipos de interfaces.

Para el caso de la práctica la configuración de red para interfaces externos queda de la siguiente manera: External (eth0): DHCP e Internal (eth1): Estática: 10.0.0.30 con mascara de red 255.0.0.0

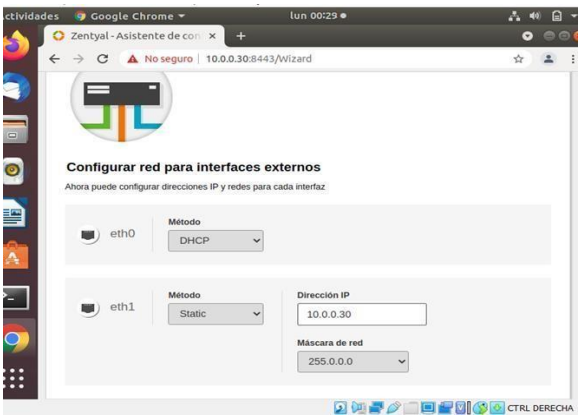

Figura 91: Configuración red para interfaces externos.

2.6.1 Configuración DHCP

Antes de ejecutar nuestro servicio DHCP es necesario ir a su configuración para establecer un rango.

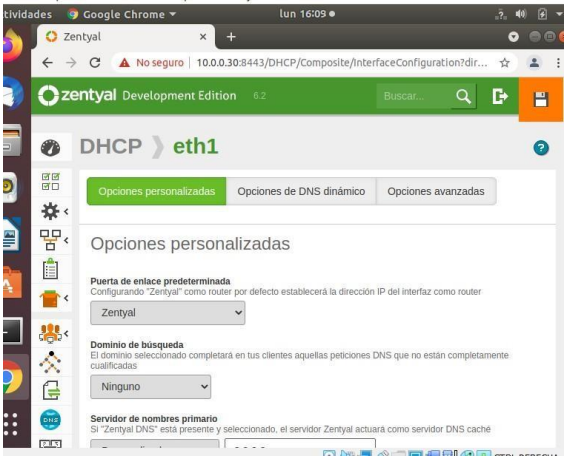

Figura 92: Configuración DHCP.

2.6.2 Rango Establecido

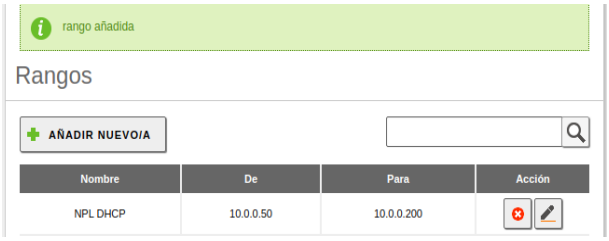

Figura 93: Rango IPs añadido.

Para la configuración del servidor VPN, se requiere ir a la pestaña Autoridad de certificación y crear una certificación para la entidad certificadora, que en este caso es el mismo servidor Zentyal.

Figura 94: Certificación para entidad certificadora.

Se procede a ingresar a la pestaña VPN y crear el servidor OpenVPN:

Figura 95: Creación de servidor openVPN.

Cuando creamos el servidor instantemente se generará su respectivo certificado, por lo que, solo nos faltaría crear un último certificado para cliente para que en su totalidad sean 3 certificados como evidenciamos:

Figura 96: Certificados para el Servidor Zentyal y para el Cliente.

Activar la casilla de interfaz túnel (TUN) para escuchar por el puerto 1194 UDP y se guardan cambios:

Figura 97: Configuración del servidor vpn.

Configurar el servicio de la VPN, en el menú servicios, Añadir nuevo servicio, en este caso se va a llamar “red-vpn” y añadir.

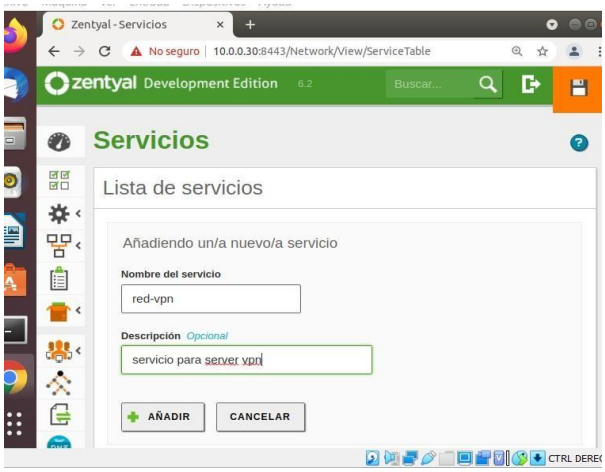

Figura 98: Creación de servicio VPN.

Se procede con la configuración del servicio OpenVPN, en la opción servicios, seleccionar el protocolo y el puerto de destino que es el 1194 UDP, añadir y guardar cambios.
Quedando así la configuración del puerto:

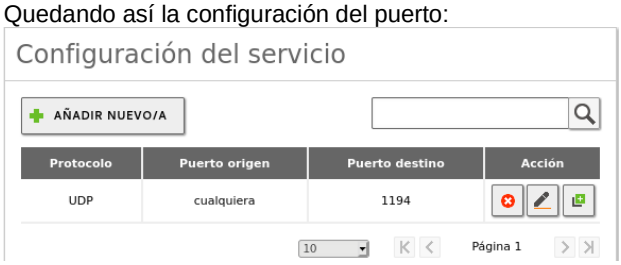

Figura 99: Configuración de puerto UDP

En el menú Cortafuegos habilitar las conexiones entrantes para que estas sean permitidas en el puerto 1194, mediante esto Zentyal escucha y permite las conexiones por OpenVPN, añadir la configuración y guardar los cambios. Esta es la configuración que debe quedar para que Zentyal permita conexiones entrantes

por el puerto 1194 de OpenVPN:

Figura 100: Configuración del firewall para OpenVPN.

En el menú servidores VPN, seleccionar el sistema operativo cliente, el certificado previamente creado como “linuxdiplomado” y proceder con la descarga de los archivos de configuración:

Figura 101: Descarga de paquete de configuración de cliente.

Verificar en el dashboard que el servicio OpenVPN se encuentre habilitado y ejecutándose:

Figura 102: Verificación habilitación y ejecución servicio OpenVPN

2.6.3 Instalación de OpenVPN

En la consola de nuestro desktop vamos a instalarlo de la siguiente manera:

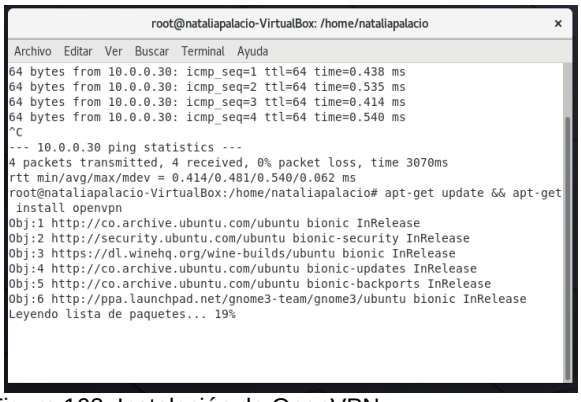

Figura 103: Instalación de OpenVPN

Después verificamos que el programa se encuentre activo:

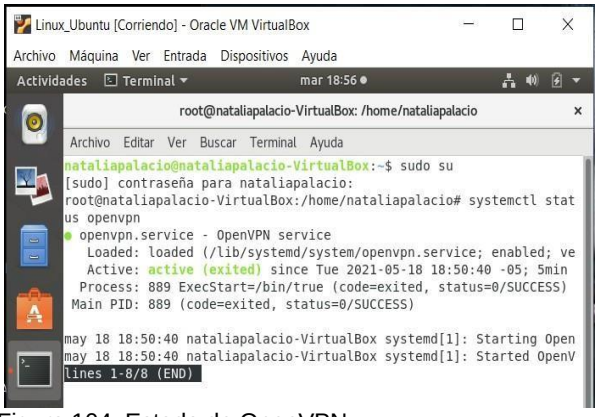

Figura 104: Estado de OpenVPN

2.6.4 Instalación y configuración del cliente OpenVPN

Figura 105: Paquete configuración de Cliente comprimido y descomprimido.

Una vez descargado el paquete de configuración de cliente lo descomprimimos y copiamos los archivos que se encuentran dentro de la carpeta a la siguiente dirección **/etc/ssl/certs/**

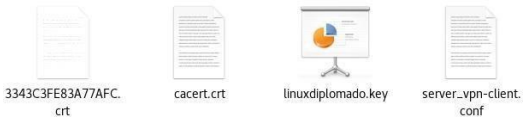

Figura 106: archivos del paquete comprimido de la configuración de cliente.

Ahora mediante la consola vamos a abrir el documento **server_vpn_client.conf** de la siguiente manera:
sudo nano /etc/ssl/certs/server_vpn_client.conf

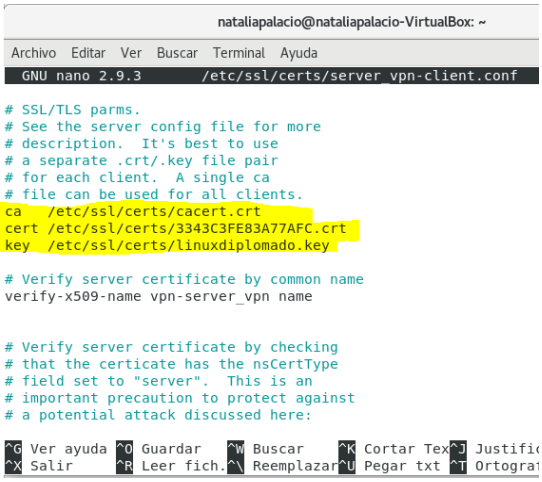

Figura 107: Documento server_vpn_client.conf

Ya estando configurado el archivo ahora procedemos a ejecutarlo de esta manera:
sudo openvpn /etc/ssl/certs/server_vpn_client.conf

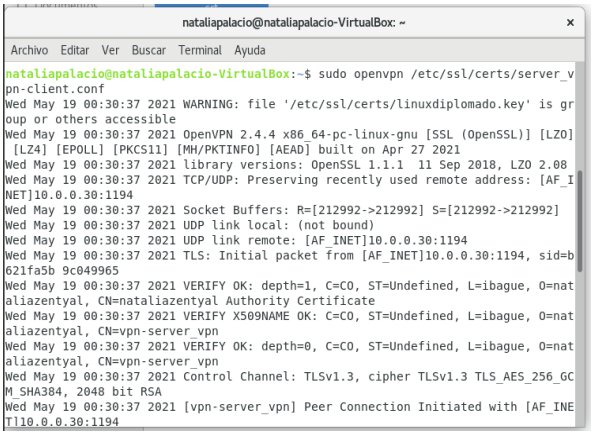

Figura 108: Ejecución de archivo .conf

Para verificar que nuestro túnel privado haya sido establecido debidamente le realizamos a nuestra maquina un ifconfig donde lo identificamos como **tun0.**

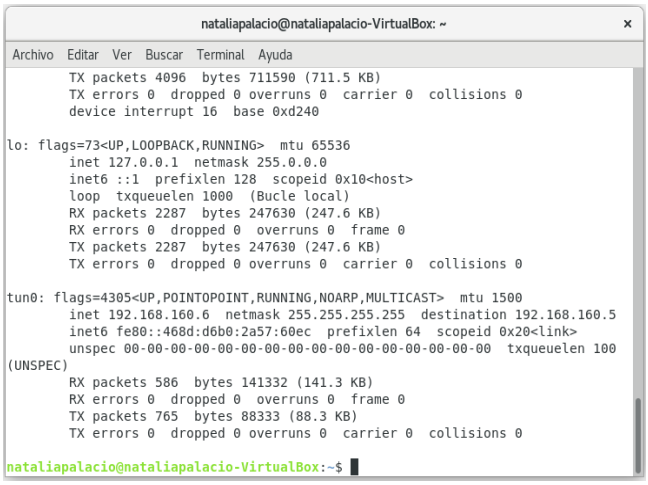

Figura 109: Ejecución de ifconfig en consola.

Por medio de la función traceroute verificamos que trace la ruta que hace el paquete desde su host hasta nuestro puesto de trabajo.


Figura 110: Ejecución de función traceroute.

3. CONCLUSIONES.

El servidor Zentyal es una gran alternativa, a servidores como Windows, tiempo un amplio uso en configuración de redes y compartición e instalación de archivos, dispositivos como impresoras, es de resaltar que es utilizado por grandes y pequeñas empresas como es el caso de la empresa internacional proveedores de servicios de internet ISP.

Para llevar a cabo las diferentes actividades que se realizan dentro de la misma. Cuenta con una interfaz fácil y amigable. El uso de Zentyal es de vital importancia especialmente el ámbito laboral empresarial.

4 REFERENCIAS

[1] Zentyal (2018). Zentyal Community. Recuperado de Documentación de Zentyal 6.2: https://doc.zentyal.org/es/installation.html#el-instalador-de- zentyal

[2] IT DATA SAS (2018) Firewall. IT DATA. Itdata.com.co. Recuperado de http://www.itdata.com.co/servicios/firewall/

[3] Zentyal Community. (2018). Instalación. Disponible en: https://doc.Zentyal.org/es/installation.html

[4] Zentyal Community. (2018). Servicio de redes privadas virtuales (VPN) con OpenVPN. Disponible en: https://doc.Zentyal.org/es/vpn.html

[5] Zentyal Community. (2018). Servicio de redes privadas virtuales (VPN) con OpenVPN. Obtenido de https://doc.Zentyal.org/es/vpn.html