INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL-SERVER 5.0 PARA LA IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT

Integrantes:

Frank de Jesús Barrios Yépez
e-mail: fdbarrios3@gmail.com
Nelson Yessy López Hidalgo
e-mail: nelson.hidalgo1@gmail.com
Luis Alberto Robles Logreira
e-mail: lrobles5046@hotmail.com
Jorge Andrés Medina Martínez
e-mail: jamedina1207@gmail.com
Bilmer Antonio Pérez Ordoñez
e-mail: Bilmer25@hotmail.com

RESUMEN: *La finalidad de la creación de Zentyal Server 5.0, es ofrecer a empresas, un servidor Linux con Mail, Dominio & Directorio, Servidor de Archivos e Impresión, Firewall e Infraestructura de Red básica, que se instala en menos de 30 minutos, que es fácil de usar y accesible y que tiene compatibilidad nativa con Microsoft® Outlook sin necesidad de plugin ni conectores.*

PALABRAS CLAVE: Zentyal, protocolo, DHCP, DNS, Dominio, Samba, CUPS, Cortafuegos, Proxy, VPN.

I. INTRODUCCIÓN

El presente trabajo tiene como propósito estudiar temas encaminados a la instalación y configuración de Zentyal Server 5.0, que nos permita crear un espacio de trabajo para la instalación y configuración de servicios DNS, DHCP, Controladores de Dominios, Servidor de Archivos e Impresión, y Proxy no transparente que garanticen la seguridad y el acceso en una red local.

II. OBJETIVOS

- Investigar, comprender y poner en práctica los diferentes comandos para la instalación y configuración de Zentyal.
- Implementar y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña.
- Implementación y configuración detallada del control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.
- Implementar y configurar de manera detallada la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas.

- Validar el funcionamiento del cortafuego aplicando las restricciones solicitadas, desde una estación de trabajo GNU/Linux Ubuntu Desktop.

- Implementar y configurar de manera detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

- Implementar y configurar de manera detallada la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop.

III. INSTALACIÓN DE ZENTYAL

A continuación, se describe el proceso de instalación de Zentyal 5.0:
Fig. 1: inicio de instalación
Luego se elige idioma de la distribución:

Fig. 2: Selección idioma de la distribución

Luego se debe seleccionar el idioma del proceso de instalación:

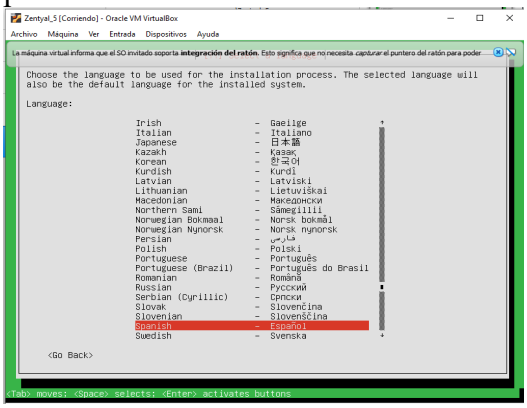


Fig. 3: Selección del idioma del proceso de instalación

Luego se debe seleccionar una ubicación geográfica:

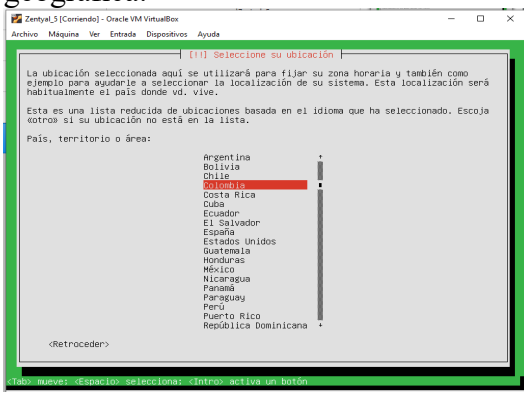


Fig. 4: Especificación de la ubicación geográfica

Seleccionar una configuración de teclado:

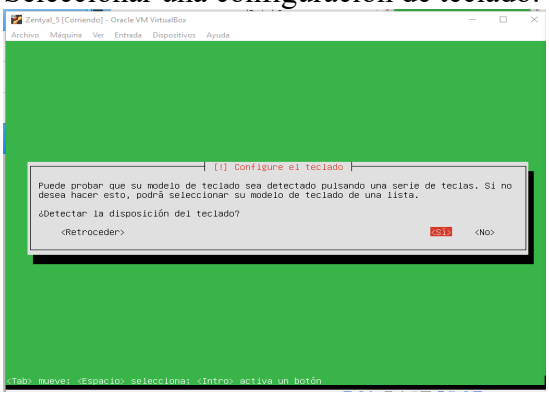


Fig. 5: Configuración del teclado

Se elige la distribución del teclado a usar

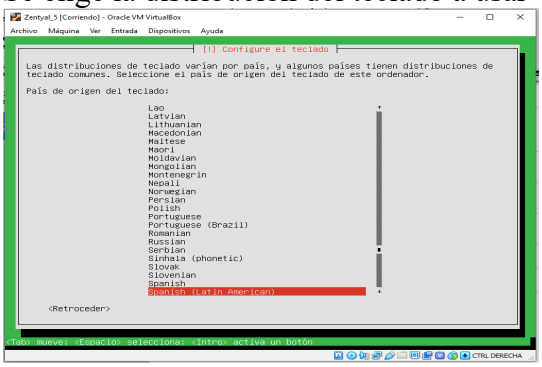


Fig. 6: distribución del teclado

Se empieza la carga de componentes y para el proceso de instalación y detección de Hardware:

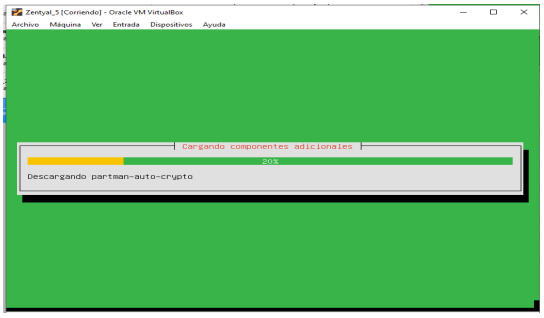


Fig. 7: cargando componentes

Comienza el proceso de instalación y nos pide un nombre para el S.O.

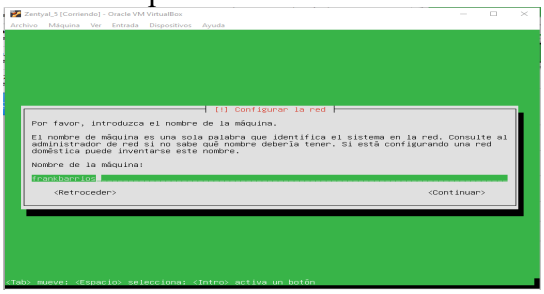


Fig. 8: nombre del sistema operativo

Elegimos un nombre para la cuenta de usuario

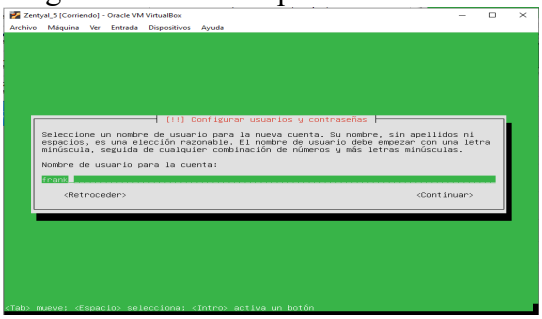


Fig. 9: nombre de usuario.

Se ingresa una contraseña para la cuenta de usuario y se confirma:

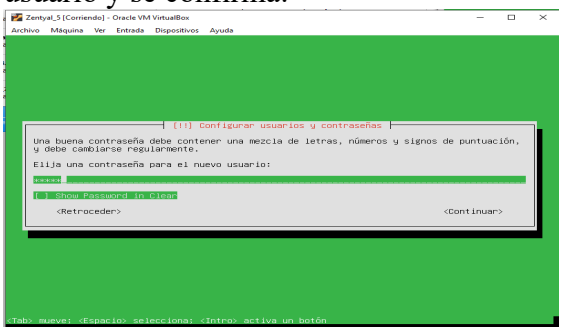


Fig. 10: contraseña cuenta de usuario

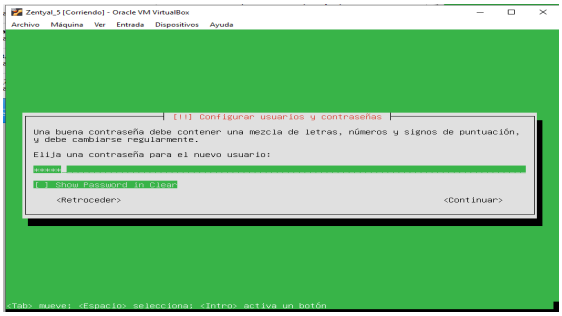


Fig. 11: confirmación de contraseña

Especificar la zona horaria:

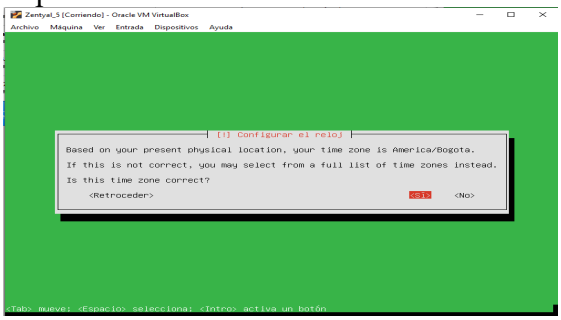


Fig. 12: zona horaria

Esperar un momento a que el proceso de instalación termine de descargar los paquetes necesarios del proceso:

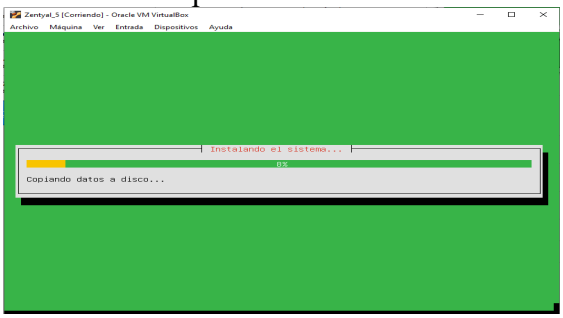


Fig. 13: instalación de paquetes

Al terminar la instalación pide reiniciar el sistema.

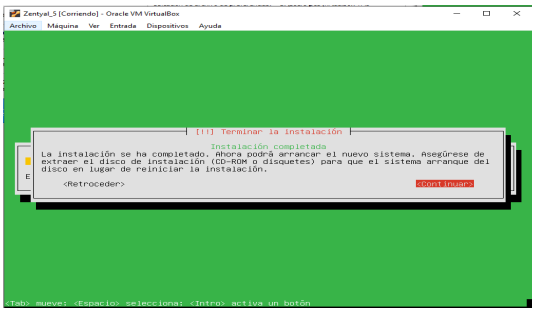


Fig. 14: fin de la instalación

Al reiniciar el sistema empieza a cargar los paquetes instalacos:

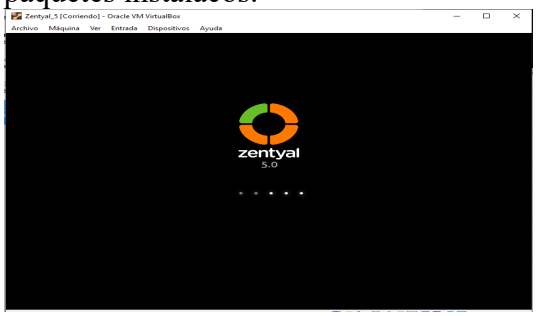


Fig.15: cargando componentes instalados

Al finalizar la carga de componentes instalados se inicia el sistema operativo

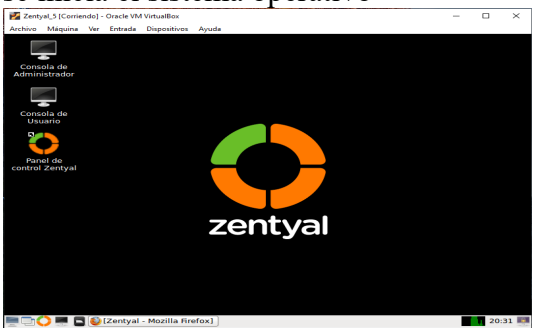


Fig. 16: inicio del sistema.

IV. INSTALACIÓN Y CONFIGURACIÓN DE DHCP

Descargamos el paquete de DHCP: apt-get install isc-dhcp-server.

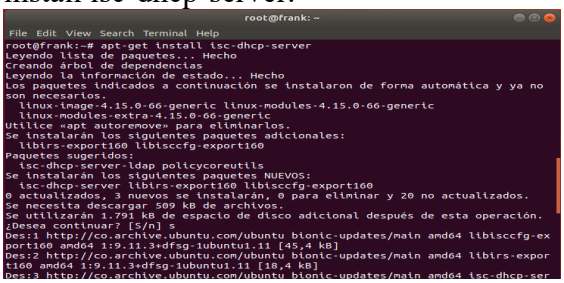


Fig. 17: instalación DHCP

Abrimos el archivo vim /etc/defaults/isc-dhcp-server y donde dice INTERFACES, colocamos el nombre de la tarjeta de red que se va a encargar de asignar direcciones IP.

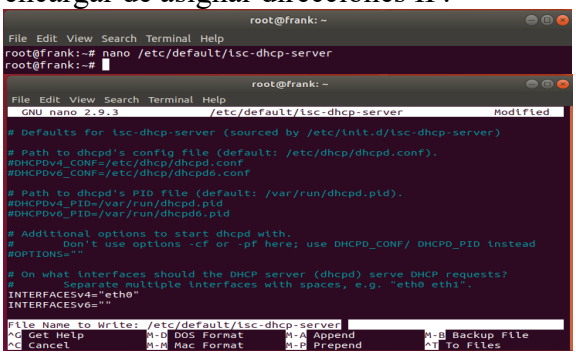


Fig. 18: configuración de interfaces de red

Editamos el archivo vim /etc/dhcp/dhcpd.conf
Y agregamos lo siguiente:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.0.20 192.168.0.200;
option domain-name-servers 8.8.8.8, 4.4.4.4;
option domain-name "miservidordhcp";
option routers 192.168.1.1;
option broadcast-address 192.168.1.255;
default-lease-time 600;
max-lease-time 7200;}
```

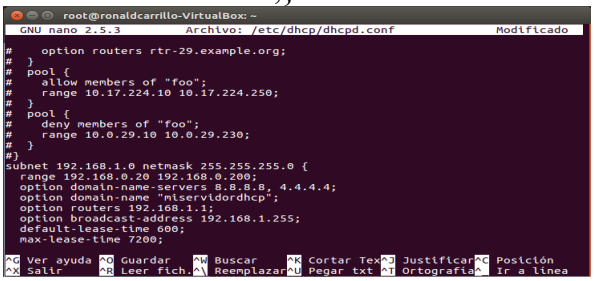


Fig. 19: asignación de IP a interfaces de red

En el anterior texto, indicamos la red, mascara de subred, rango de direcciones IP, servidores

DNS, nombre de nuestro dominio, puerta de enlace. Reiniciamos el servicio con:
service isc-dhcp-server restart

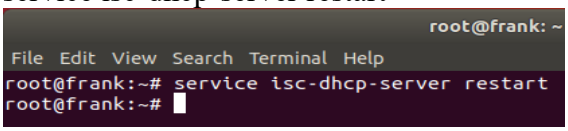


Fig. 20: reinicio de dhcp server

V. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR DNS

Instalamos el servidor DNS: sudo aptitude install bind9.

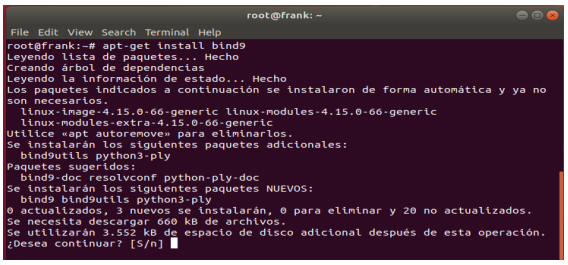
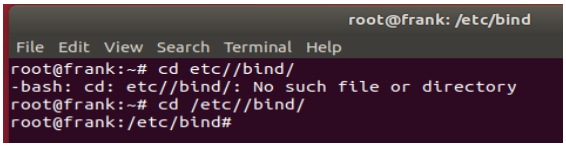


Fig. 21: Instalación del DNS

Vamos al directorio del programa para editar los archivos de configuración:
cd /etc/bind/



Editamos el archivo named.conf.local
gedit named.conf.local.

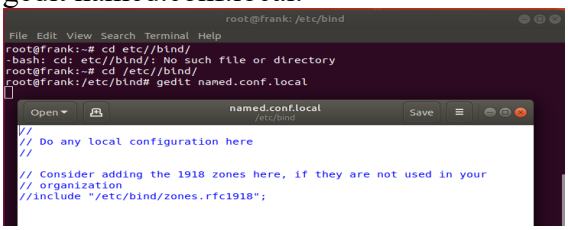


Fig. 22: Edición del archivo named.conf.local

Creamos el fichero de configuración a partir de uno ya creado (db.local)

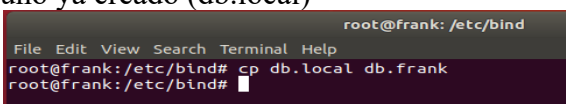


Fig. 23: Fichero de configuración db.local

Modificación del archivo “localhost” por el nombre del dominio que hemos elegido: “ronald.carrillo.net”

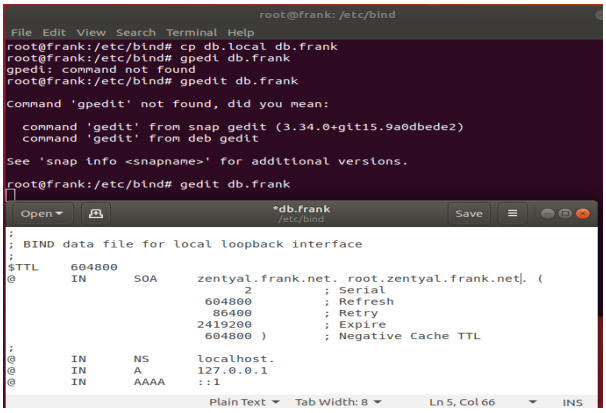


Fig. 24:

Reiniciamos el proceso bind con el siguiente comando: sudo /etc/init.d/bind9 restart.

Fig. 25:

Editamos el fichero de configuración resolv.conf para que el ordenador utilice este servidor DNS que hemos configurado:
sudo gedit /etc/resolv.conf.

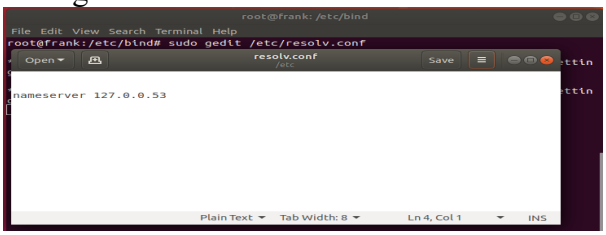


Fig. 26

Editamos el fichero de configuración resolv.conf para que el ordenador utilice este servidor DNS que hemos configurado:
sudo gedit /etc/resolv.conf.

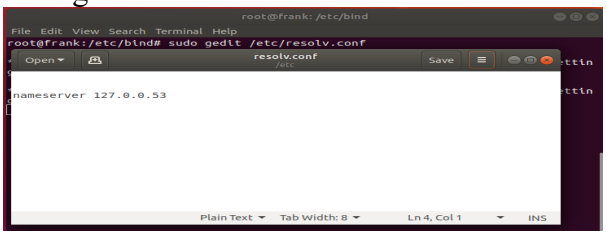


Fig. 27.

VI. INSTALACIÓN Y CONFIGURACIÓN DE CONTROLADORES DE DOMINIO

Actualizamos el repositorio: apt-get update.

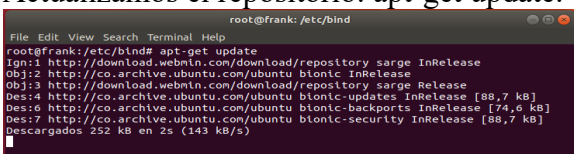
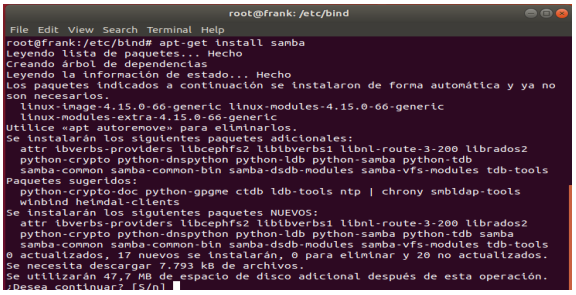


Fig. 28

Instalamos el paquete samba: apt-get install samba.



Comprobamos la versión de samba.

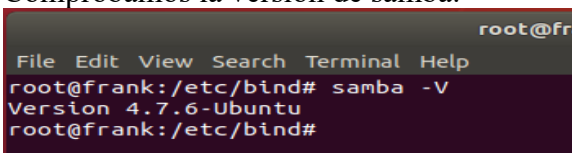


Fig. 29

moveremos el archivo /etc/samba/smb.conf para conservarlo, porque el proceso de creación del dominio creará un archivo nuevo: mv /etc/samba/smb.conf /etc/samba/smb.old

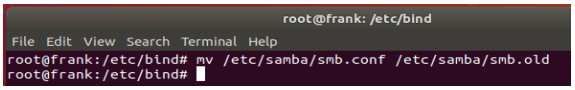


Fig. 30:

A continuación, realizaremos la provisón del dominio, añadiendo la opción –use-rfc-2307 que sirve para habilitar a Samba para guardar atributos POSIX y crear la información de NIS para administrar usuarios Unix:

samba-tool domain provision --use-rfc2307 –interactive.

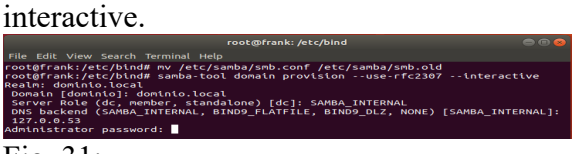


Fig. 31:

De esta manera ya tenemos nuestro controlador de dominio configurado.

VII. PROXY NO TRANSPATENTE

A continuación, se describe el proceso para la instalación y configuración de un proxy no transparente usando Zentyal.

Lo primero que se debe hacer es instalar el servidor proxy squid, tal como se indica a continuación:

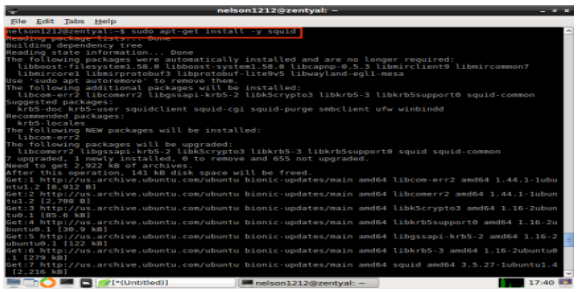


Fig. 32: Instalación de Squid.

Para configurar el servidor se debe abrir el archivo se configurar squid.conf tal como se indica a continuación: **sudo gedit etc/squid/squid.conf**

Fig. 33: Archivo se configurar squid.conf.

Por defecto es no transparente, a menos que al lado del puerto se especifique lo siguiente **http_port puerto transparent**, en la guía se indica que debe funcionar por el puerto **3128**, a continuación, se deja evidencia del cambio:

Fig. 34: Verificación del puerto.

Luego se procede a especificar reglas ACL para bloquear dominios, en este caso, pongo tres dominios de prueba:

www.elespectador.com, www.youtube.com y www.facebook.com

tal como se evidencia a continuación:

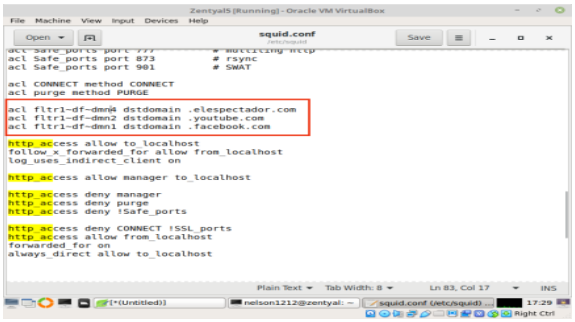


Fig. 35: Configuración de las reglas ACL.

Luego de lo anterior se debe reiniciar el servicio squid:

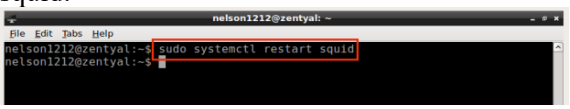


Fig. 36: Reiniciación del servidor.

Luego de agregar las reglas se debe consultar la IP del servidor Zentyal para configurar el proxy en cada equipo cliente:

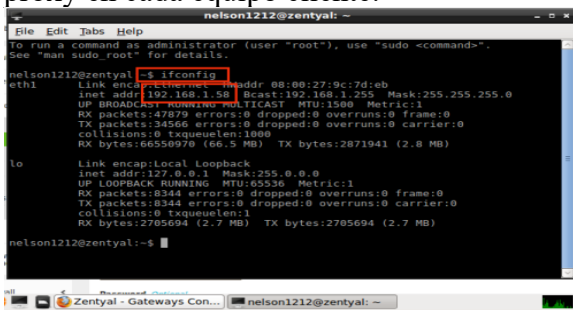


Fig. 37: Consulta de la IP del servidor zentyal.

Luego en un navegador web de un equipo cliente se configura el servidor proxy tal como se indica a continuación:

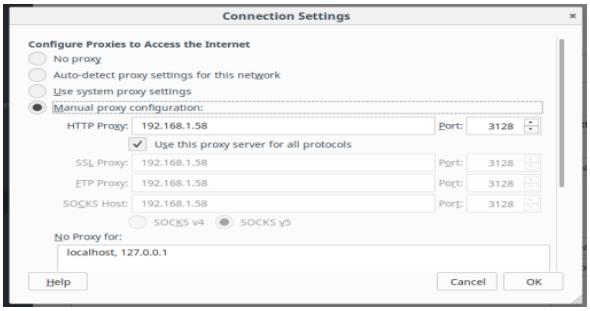


Fig. 38: Configuración de la IP del servidor en el equipo cliente.

Luego desde el equipo cliente, se debe proceder a probar los dominios bloqueados: www.facebook.com

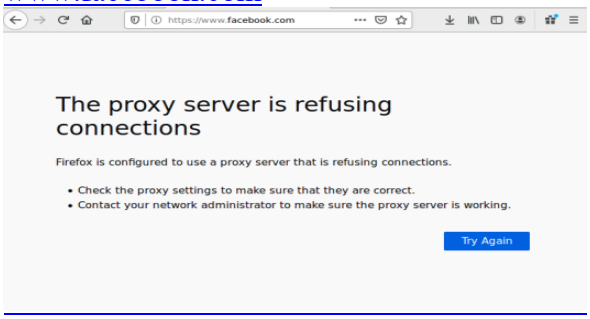


Fig. 39: Verificación del bloqueo de Facebook.

www.youtube.com

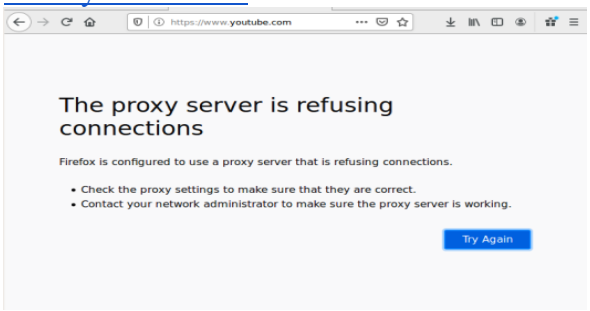


Fig. 40: Verificación del bloqueo de Youtube.

Para cualquier otro sitio se permite el acceso sin restricciones:

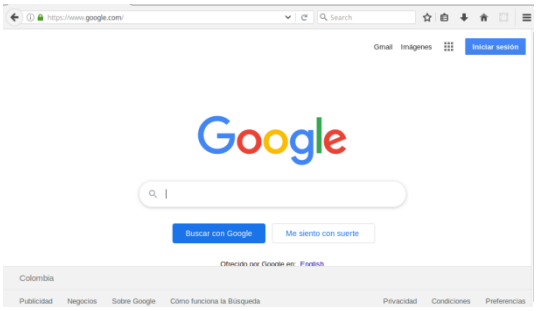


Fig. 41. Verificación del bloqueo de Google.

VIII. FILE SERVER Y PRINT SERVER

A continuación, se describe el proceso para la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

FILE SERVER

Configuramos el directorio compartido de la siguiente manera:

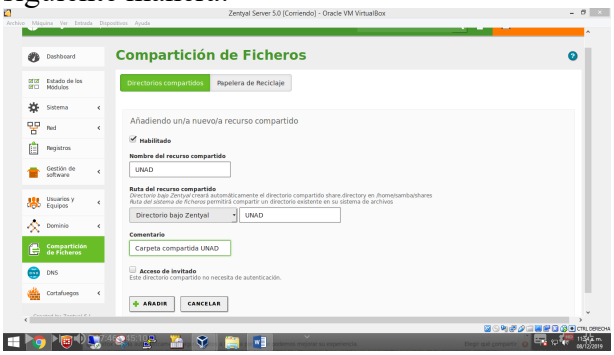


Fig. 42:

Añadimos un usuario como administrador de dominio

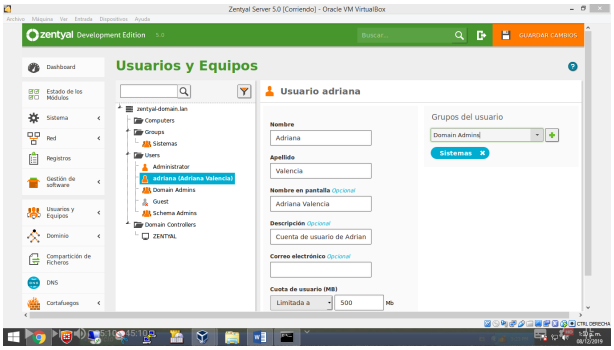


Fig. 43

Añadimos el directorio compartido UNAD al usuario creado, haciendo click en Compartición de ficheros.

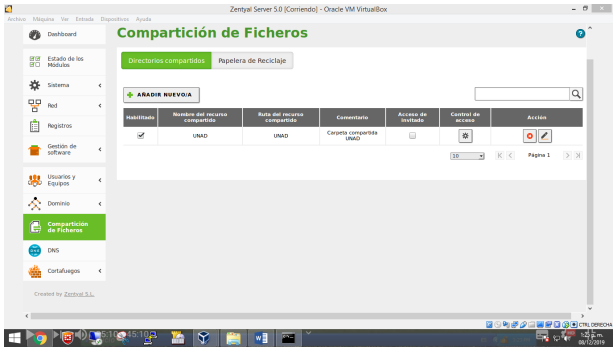


Fig. 44

Seleccionamos el usuario previamente creado y le damos permisos de Lectura y Escritura.

Fig. 45

Ingresamos a la máquina cliente Ubuntu con nuestro usuario de dominio

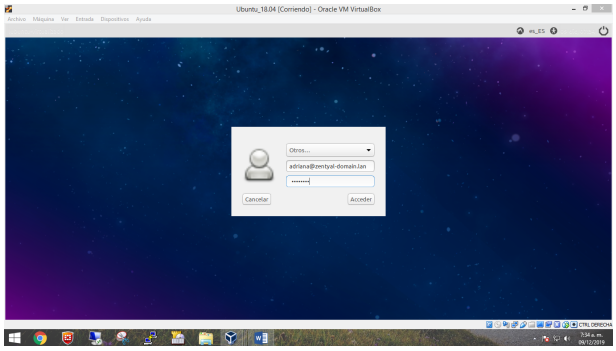


Fig. 46

Comprobaremos la compartición de archivos desde el servidor Zentyal y la carpeta UNAD

en el equipo cliente Ubuntu.

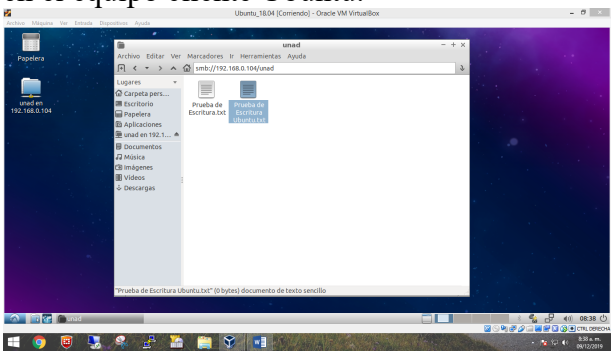


Fig. 47

PRINT SERVER

Instalamos el servicio CUPS (Common Unix Printing System)

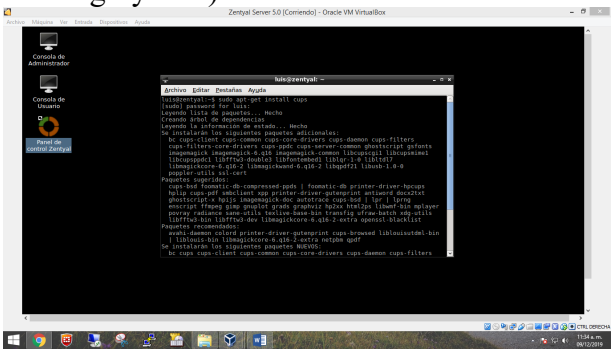


Fig. 48

Instalamos el driver de la impresora

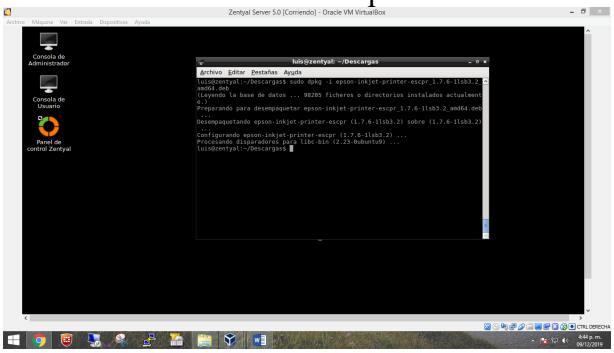


Fig. 49

Y podemos observar que la Impresora se ha agregado a la consola de administración de impresoras CUPS de Zentyal.

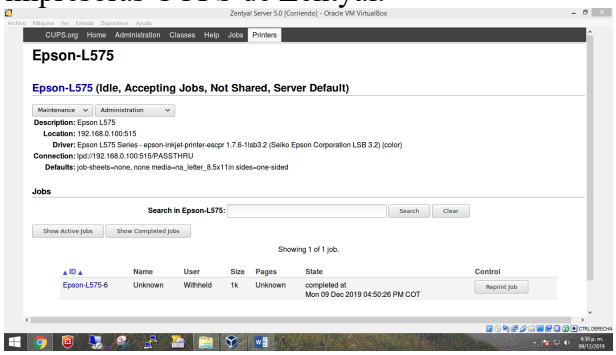


Fig. 50

Verificamos que la impresora compartida se encuentre visible como un recurso de red para otros equipos del dominio.

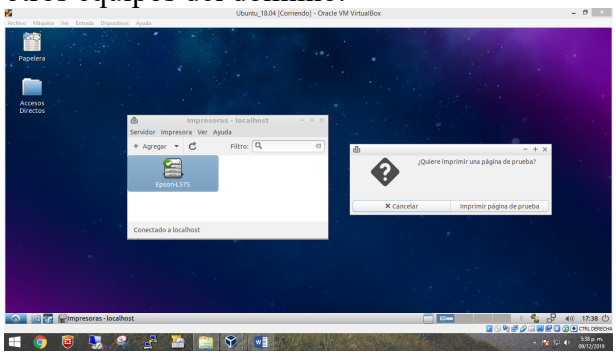


Fig. 51

Imprimimos una página de prueba desde el cliente Ubuntu

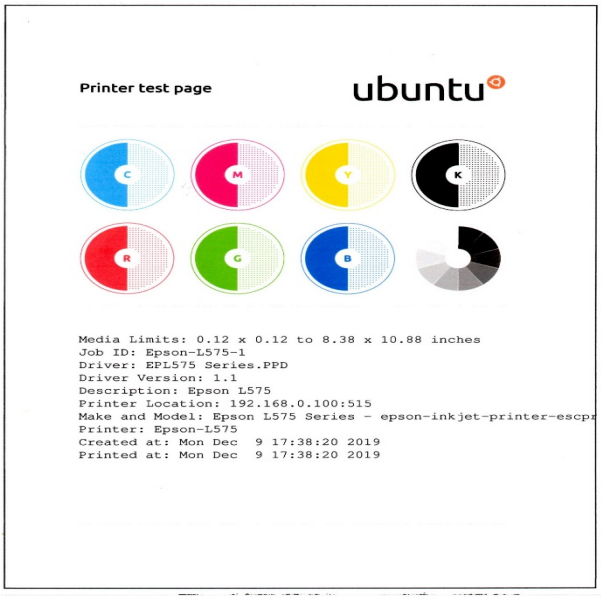


Fig. 52

IX. TEMÁTICA VPN

La actividad correspondiente a este paso consiste en crear una VPN la cual permita la creación de un túnel privado de comunicación. A continuación, utilizaremos la distribución de Linux Zentyal como base para los servicios de infraestructura TI.

Al culminar la instalación, ingresamos por la siguiente dirección a nuestro Zentyal Server para descargar su configuración inicial.

https://localhost:8443/Loguin/Index.

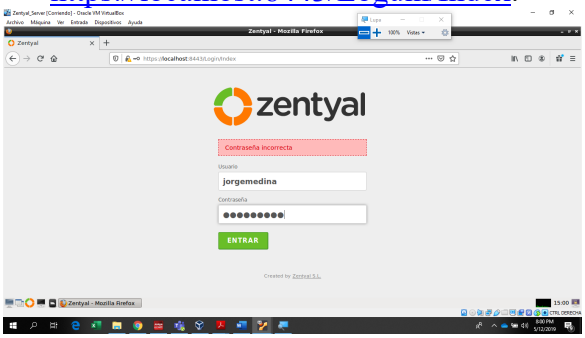


Fig. 53

Continuando en nuestra máquina de Zentyal realizamos la descarga y configuración de la VPN desde https://localhost:8443/Software/EBox.

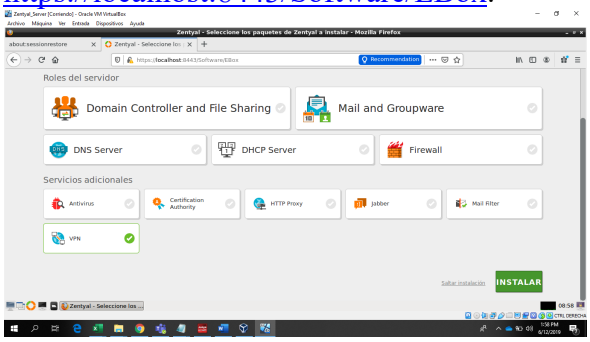


Fig. 54

Se instalan los siguientes paquetes.

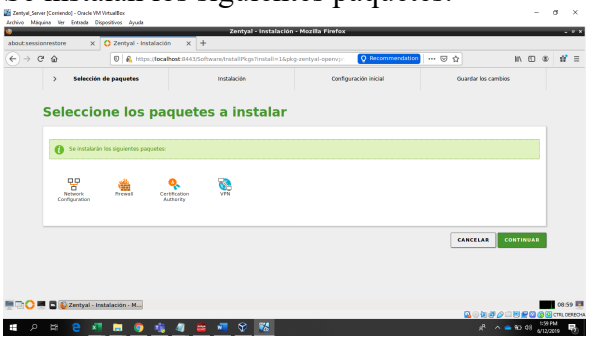


Fig. 55

Realizamos la configuración de las interfaces eth0 interna y eth1 como externa.

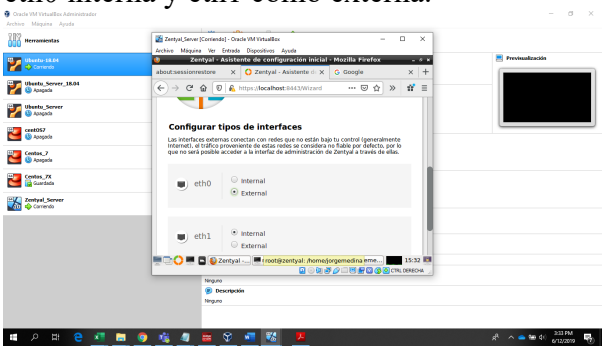


Fig. 56

Configuramos las IPs para cada una de las interfaces y guardamos la configuración realizada.

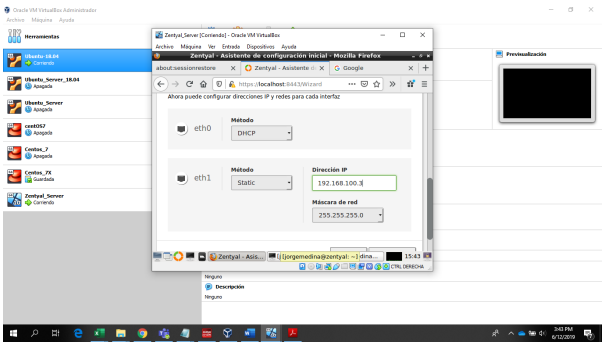


Fig. 57

En la estación de Ubuntu asignamos el direccionamiento de red 192.168.100.2

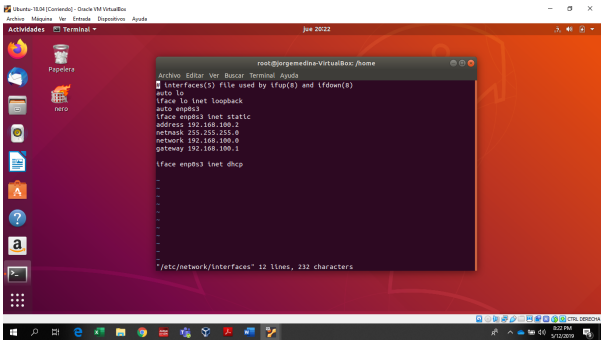


Fig. 58

Validamos en la interfaz de red por medio de ifconfig.

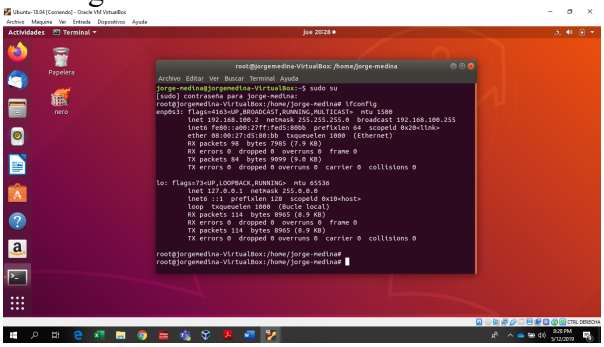


Fig. 59

También la configuración de red en Zentyal Server 192.168.100.3

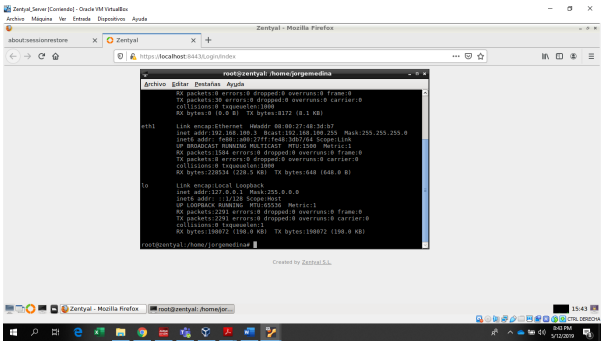


Fig. 60

Prueba de conectividad a nivel LAN desde Zentyal.

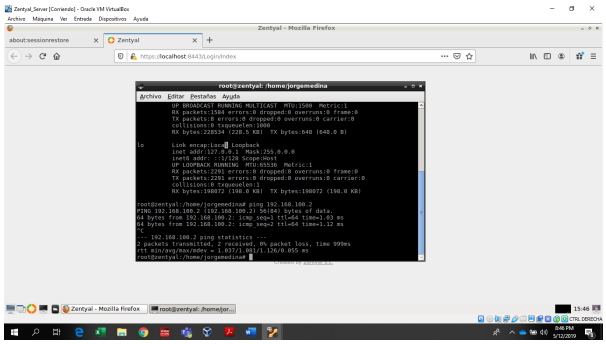


Fig. 61

Prueba de conectividad desde la estación Ubuntu.

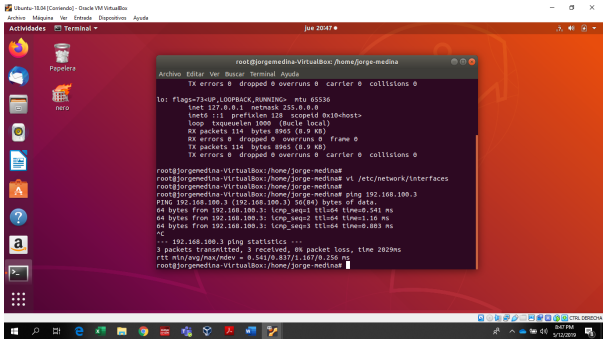


Fig. 62

Con lo anterior se garantiza que se tiene tanto red LAN como WAN en el ambiente de simulación.

En la estación de Ubuntu procedemos a realiza la instalación del OpenVpn.

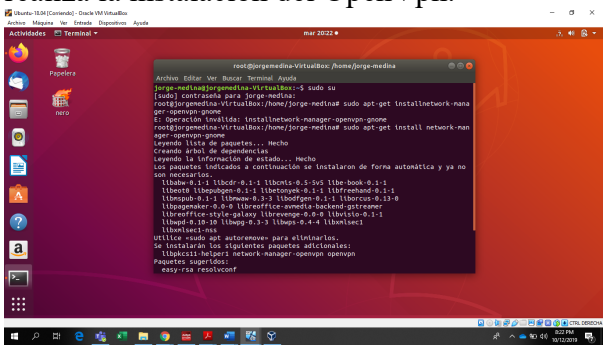


Fig. 63

Culminamos la instalación.

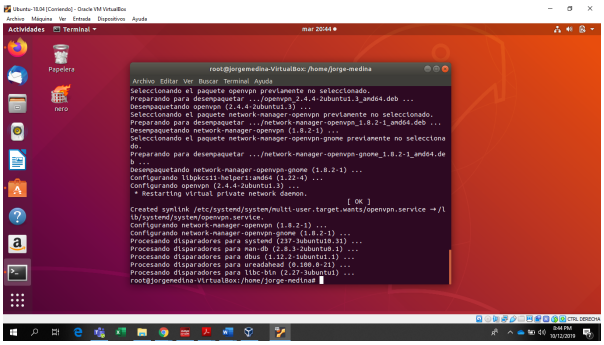


Fig. 64

Realizamos la configuración en la ruta OpenVpn.

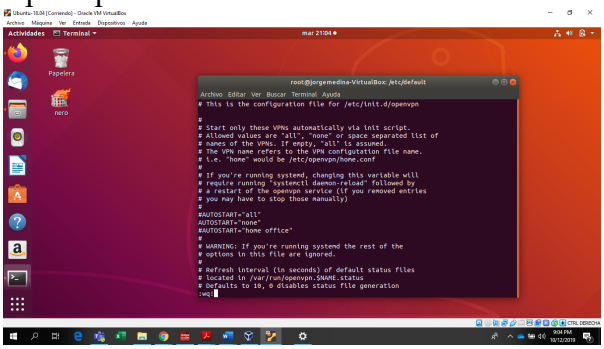


Fig. 65

Realizamos la descarga y configuración de los certificados.

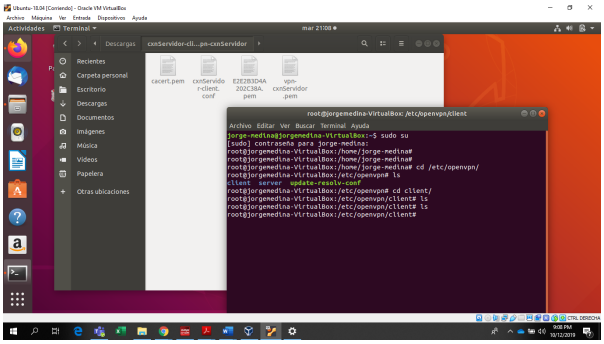


Fig. 66

Hacemos copia de los archivos de configuración en la carpeta de configuración OpenVpn.

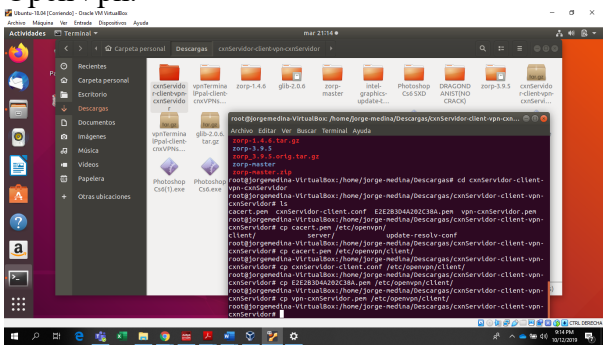


Fig. 67

Se muestran los archivos de configuración.

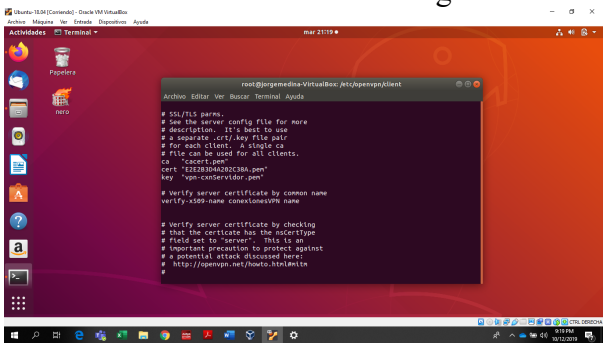


Fig. 68

Copia de los archivos de configuración en la carpeta SSL.

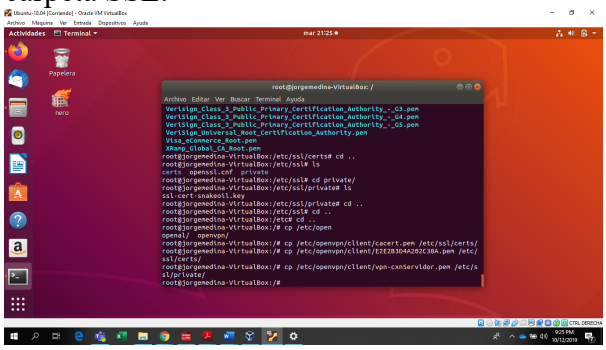


Fig. 69

Ejecución de OpenVpn client.

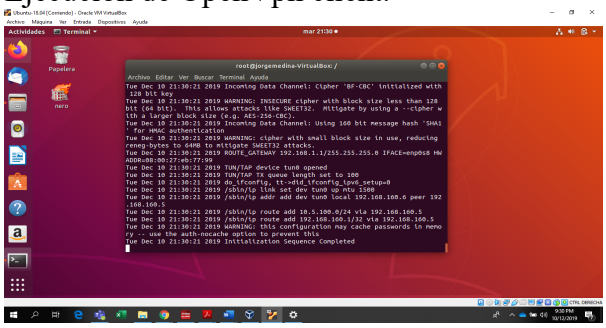


Fig. 70

Direccionamiento de red dado por la conexión vpn.

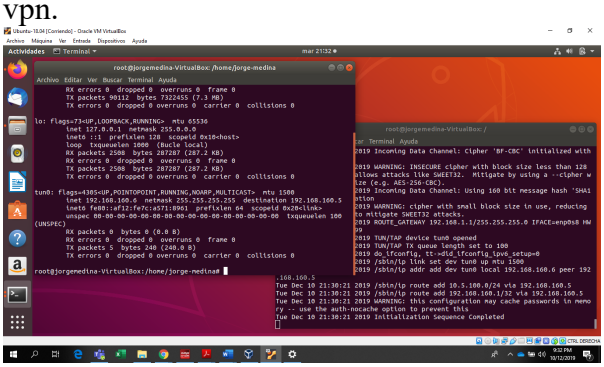


Fig. 71

Damos ping a la dirección del Gateway 192.168.160.1

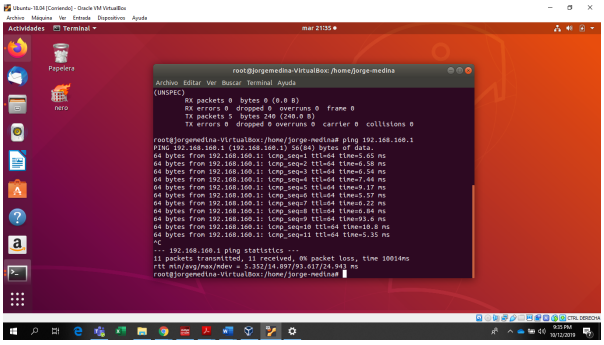


Fig. 72

Prueba de conectividad a nivel LAN de los equipos Zentyal y servidor web en una máquina física y dos virtualizada.

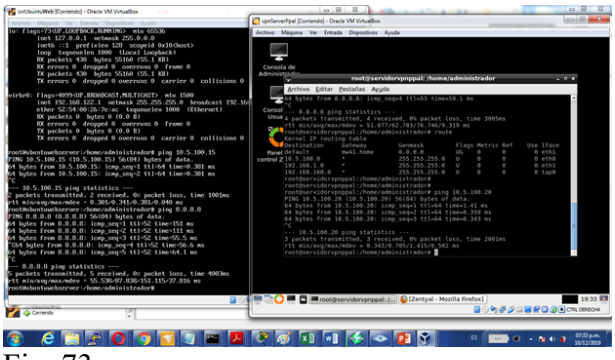


Fig. 73.

Dirección IP de túnel de Centyal.

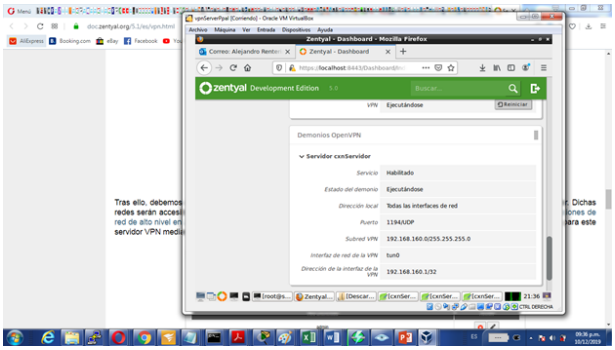


Fig. 74.

Prueba de conexión hacia el servidor de la red remota.

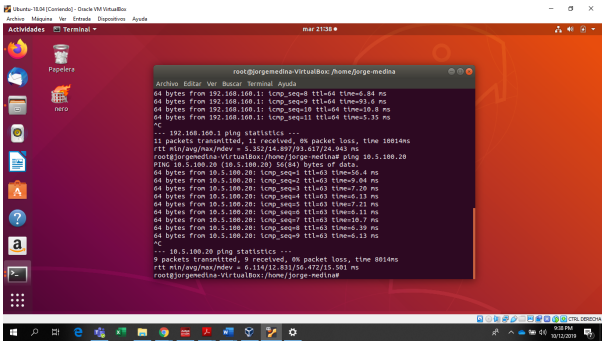
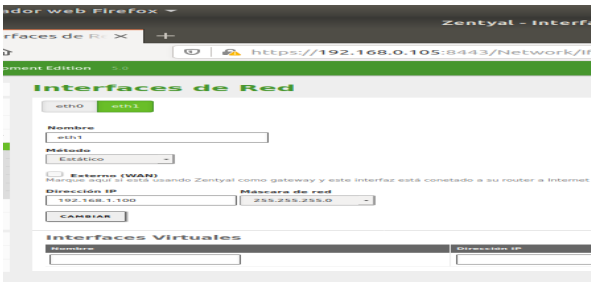


Fig. 75

Acceso web desde el equipo cliente hacia el servidor de la red remota.



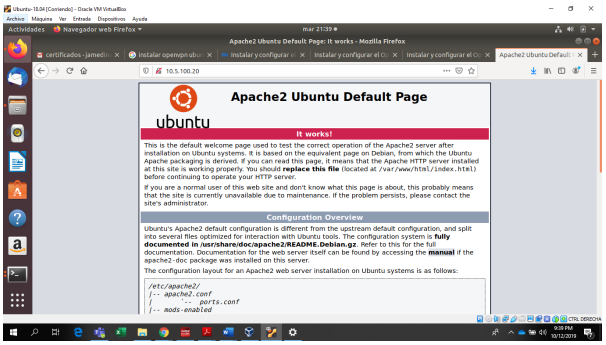


Fig. 76.

Finalmente visto desde el equipo cliente.

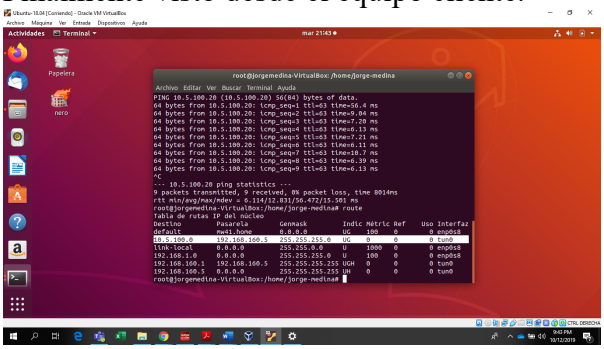


Fig. 77.

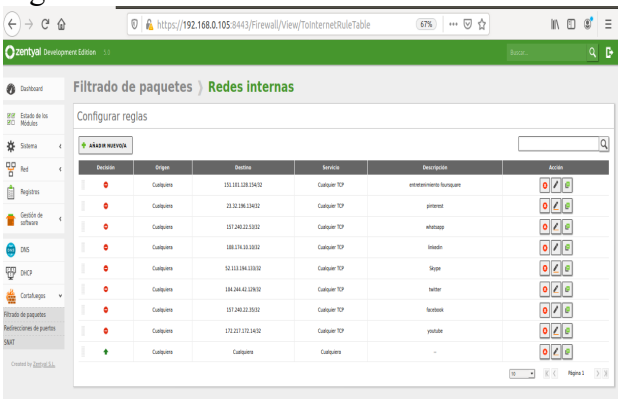
X. CORTAFUEGOS

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

Terminada la instalación nos lleva a la configuración de interfaz de red

necesitamos una interna estática (eth1) y otra externa DHCP (eth0) que se enlace con el router para acceder a internet

Fig. 78. Interfaz de red estática eth1.



Ahora para dar solución a la temática del cortafuego necesitamos conocer las direcciones web, dominio e IP de las páginas de entretenimiento y redes sociales.

Para obtener las IP de las páginas de entretenimiento o red social simplemente realizamos un ping desde la terminal a la

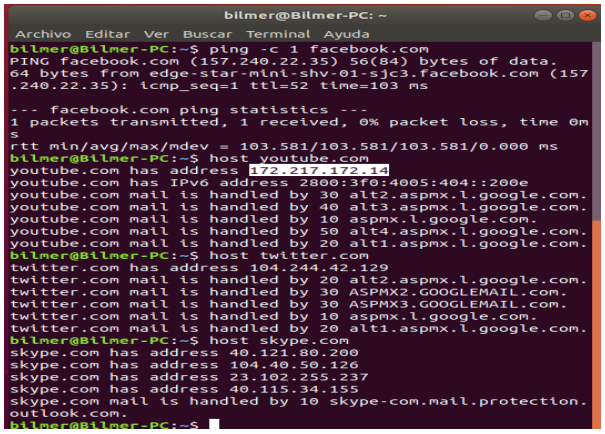


Fig. 79. Buscando IP de sitios web

Ya tenemos una lista de páginas comunes de entretenimiento y/o redes sociales con las cuales podemos empezar a realizar las reglas de filtrado desde el cortafuegos de Zentyal nos dirigimos a la sección correspondiente al cortafuegos de zentyal y damos click en filtrado de paquetes y elegimos reglas de filtrado para redes internas.

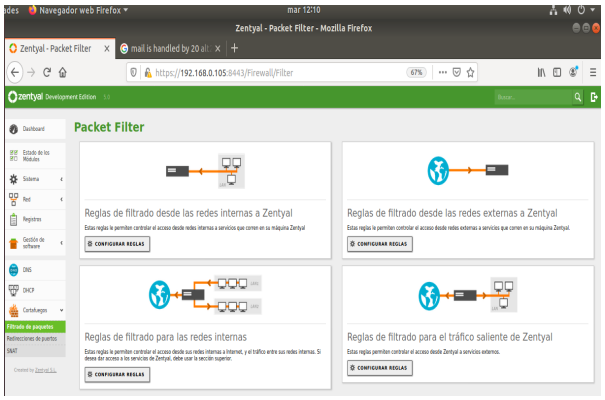


Fig. 80. Reglas de filtrado Zentyal

Empezamos a crear las reglas de filtrado añadimos y no olvidarse por cada regla ir guardando los cambios

Tenemos nuestro filtrado con las reglas establecidas

Fig. 80. Reglas de filtrado redes internas

Ahora para realizar la prueba, iniciamos el ubuntu-desktop de la red interna y revisamos que tenga una ip asignada por nuestro servidor.

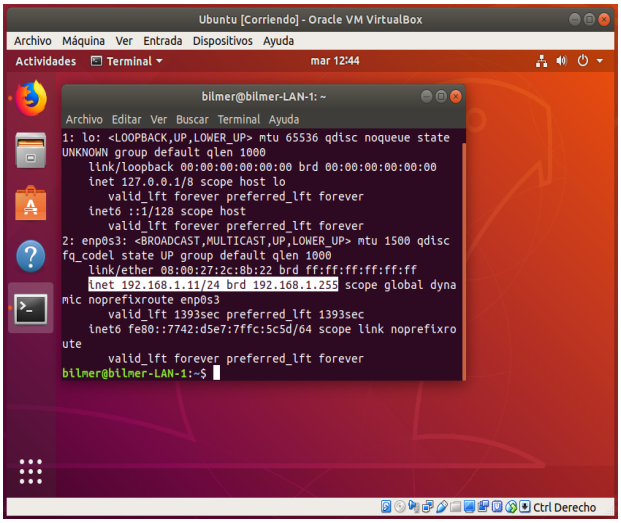


Fig. 80. Red Ubuntu desktop

Comprobamos que es la misma que nos asigna el servidor Zentyal.

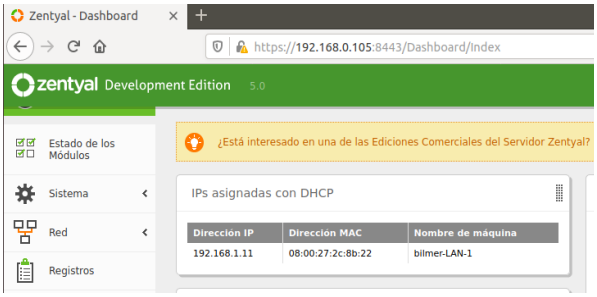


Fig. 81. IP asignada por Zentyal DHCP

Comprobamos que tenemos conexión a internet en nuestro navegador Firefox

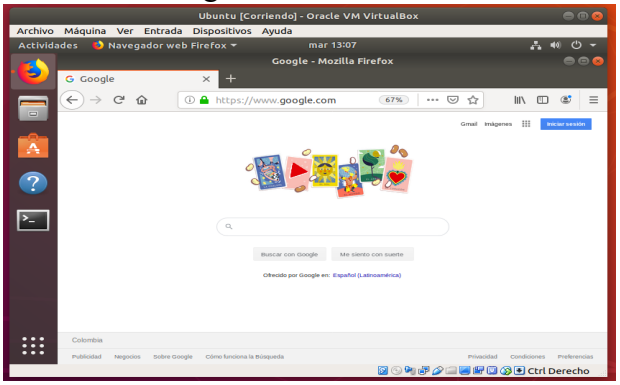


Fig. 82. Conexión a internet

Abrimos una nueva pestaña e intentamos conectar con una red social, y se evidencia que no procede a cargar la página y eso es porque se filtró cualquier tcp/443 que salga hacia la IP correspondiente al sitio web.

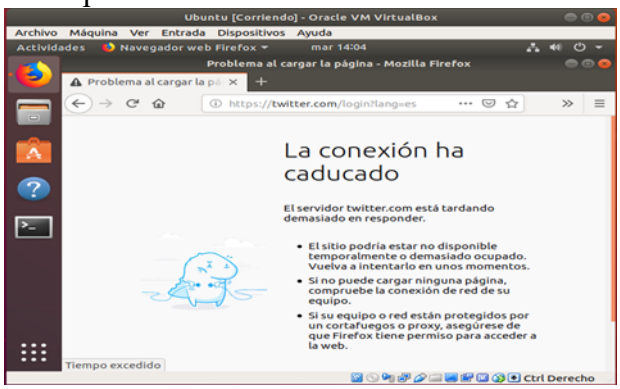


Fig. 83. Conexión a twitter.com

Realizamos otra prueba con la red social whatsapp

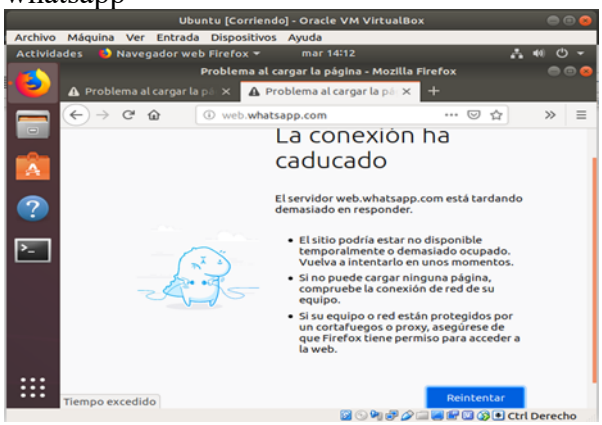


Fig. 84. Intento de conexión a whatsapp

En el caso cuando un sitio web utiliza diferentes ips alojadas en servidores que se redireccionan es necesario utilizar un Proxy donde se creará un perfil de usuarios o host en la red a los cuales les aplicaremos unas reglas por dominios.

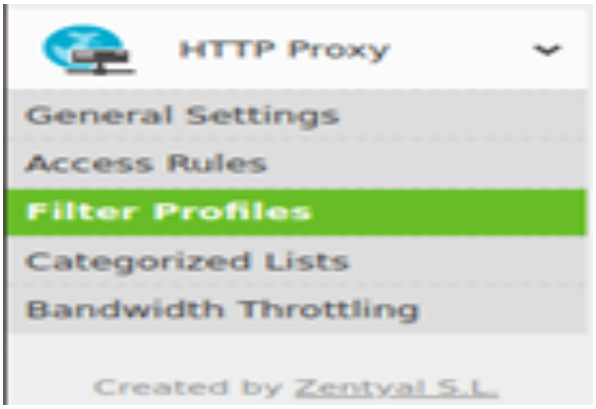


Fig. 85. Perfiles de filtrado proxy

Se crea un perfil de filtrado por dominio para youtube.com en la red interna LAN-1

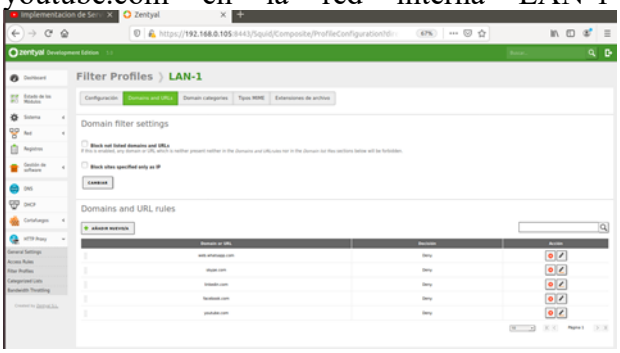


Fig. 86. Perfil de filtrado LAN-1

Se crea la regla en el proxy http

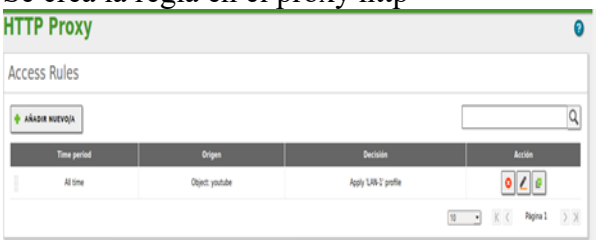


Fig. 87. Regla de filtrado http

Nos dirigimos a nuestro host en la red y abrimos el navegador verificamos conexión a Internet y probamos el funcionamiento del proxy con el sitio web indicado en la regla.

Se inicia el navegador e ingresamos a Hotmail.com para verificar acceso a internet, luego intentamos ingresar a youtube.com para probar el funcionamiento del proxy.

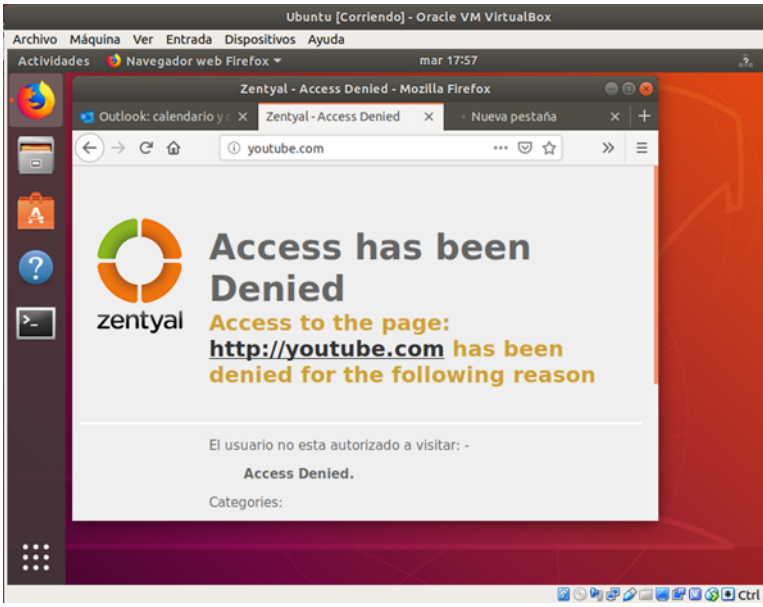


Fig. 88. Intento de acceso a youtube.com

Como se evidencia el proxy está realizando el proceso correctamente, por lo tanto el uso del cortafuego es muy importante para manejar las posibles conexiones en nuestra red, pero junto al proxy se puede dar un mejor control.

XI. CONCLUSIONES

DHCP puede llegar a ser realmente útil, pero sobre todo en infraestructuras como pueden ser universidades, bares y zonas donde haya Wi-Fi público, pero hay que tener en cuenta que en este tipo de sitios siempre interesa tener un lease-time bajo, de aproximadamente 2-3 horas como mucho, ya que al usuario que se conecte a nuestra red Wi-Fi, no le va a hacer falta esa misma dirección IP la próxima vez que venga. Sin embargo, si estamos conectando servidores a un servidor DHCP (cosa que no recomiendo), recomiendo poner un lease-time alto, como el que está puesto en la configuración, para que así, en caso de caída reserve la dirección IP al servidor durante bastante tiempo.

La razón principal para utilizar un proxy no transparente es para que el navegador web y otras aplicaciones “cliente” sepan que se está utilizando un proxy, para poder acceder a

internet. La configuración inicial de un proxy no transparente puede ser más complicada, pero en última instancia proporciona un servicio de proxy mucho más potente y flexible. Es posible que el software espía y los gusanos que utilizan la web para la transmisión no puedan funcionar porque la configuración de proxy es desconocida. Esto puede reducir la propagación de software malicioso y evitar que el ancho de banda se desperdicie por los sistemas infectados.

Un servidor Zentyal también puede usarse como File Server y Print Server de una manera sencilla que nos permita implementar estos servicios de infraestructura IT a un bajo costo en empresas Pymes. Lo interesante es que, para el usuario final, los servicios son tan transparentes que no notará el cambio. Podrá seguir accediendo a sus unidades de red e imprimir documentos en las impresoras compartidas de su oficina tal como si estos servicios estuvieran ofrecidos por servidores Windows.

La instalación de la distribución Zentyal Server permitió conocer y aplicar las herramientas base y suplir las necesidades de los entornos de infraestructura TI en intranet y extranet en organizaciones complejas.
Luego de la instalación del Zentyal Server se logra realizar la configuración e instalación de la vpn desde el localhost, la configuración IP del cliente servidor, la creación de los certificados de autenticación y la creación del túnel de comunicación para la conexión vpn.

XII. REFERENCIAS

Cómo instalar y configurar un servidor DHCP en Ubuntu Linux, Kevin, 21 junio, 2016, [En línea], Disponible en: http://www.linuxforthefuture.com/configurar-servidor-dhcp-ubuntu/

Configurar un servidor DNS (Bind) en Linux Ubuntu, Sergio De Luz, 7 febrero 2013, [En línea], Disponible en: https://www.redeszone.net/gnu-linux/configurar-un-servidor-dns-bind-en-linux-ubuntu/

Controlador dominio Samba 4 en Ubuntu 14.04, Carlos Alonso Martínez, junio 8, [En línea], Disponible en: 2014, https://waytoit.wordpress.com/2014/06/08/controlador-dominio-samba-4-en-ubuntu-14-04/

Configurar dchp desde consola en Linux, Disponible en: https://camber1redes.wordpress.com/configurar-dchp-desde-consola-en-linux/

Controlador de Dominio y Compartición de ficheros, Disponible en: https://doc.zentyal.org/es/directory.html