Instalación y configuración de Zentyal Server para implementar los servicios de infraestructura IT

Paul H. Vargas, Jhonatan Campuzano, Sandra L. Araujo, Milton Vanegas, Germán A. Ramírez
Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI, Universidad Nacional Abierta y a Distancia UNAD
Bogotá D.C., Colombia
phvargasp@unadvirtual.edu.co
jcampuzanou@unadvirtual.edu.co
slaraujoc@unadvirtual.edu.co
mvanegaspl@unadvirtual.edu.co
gramirezpi@unadvirtual.edu.co

Resumen— El presente documento expone los procedimientos efectuados para instalar y configurar un servidor sobre el sistema operativo de código abierto Zentyal, para posteriormente realizar la implementación de los siguientes servicios de infraestructura tecnológica IT: servidor DHCP, servidor DNS, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server, y red privada virtual VPN.

***Abstract*— This document describes the procedures performed to install and configure a server on the open source operating system Zentyal, to afterward implement the following technology infrastructure services: DHCP server, DNS server, Domain Controller, Non-transparent Proxy, Firewall, File Server and Print Server, and VPN virtual private network.**

Palabras Clave— Zentyal, VirtualBox, servicios, DHCP, DNS, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server, VPN.

I. INTRODUCCIÓN

Durante el curso de Profundización de Linux, hemos aprendido a instalar y a configurar diferentes versiones de Linux Server, conocer las diferencias entre versiones, grados de complejidad y los diferentes aplicativos para su administración. Las prácticas realizadas se han realizado en máquinas virtuales a través de Virtual Box. En este ejercicio, realizaremos una instalación de la distribución Zentyal Server 5.0, que trae diferentes aplicativos y una ambientación gráfica bastante amigable que la hace fácil, las pruebas se practicaran bajo Ubuntu Desktop 18.04 LTS donde nos enfocaremos a la seguridad y las propiedades de una red.

II. INSTALACION DE ZENTYAL SERVER

A. *Requisitos de Hardware*

Los requisitos mínimos de Hardware para instalar Zentyal Server son: disco duro de 80 GB, memoria RAM de 2 GB, procesador Pentium IV hacia adelante, 2 tarjetas de red.

B. *Link de descarga*

Para obtener la ISO de Zentyal Server podemos descargarla desde el siguiente enlace web: http://download.zentyal.com/

C. *Instalación*

Se crea una máquina virtual con las siguientes características: Memoria RAM 2048 MB, Procesadores 2, almacenamiento de disco duro 20 GB, y dos adaptadores de red, uno conecto en modo Puente para acceso a Internet y el segundo para la Red Interna. Antes de iniciar la máquina virtual se configura el disco óptico virtual cargando la imagen ISO de Zentyal.

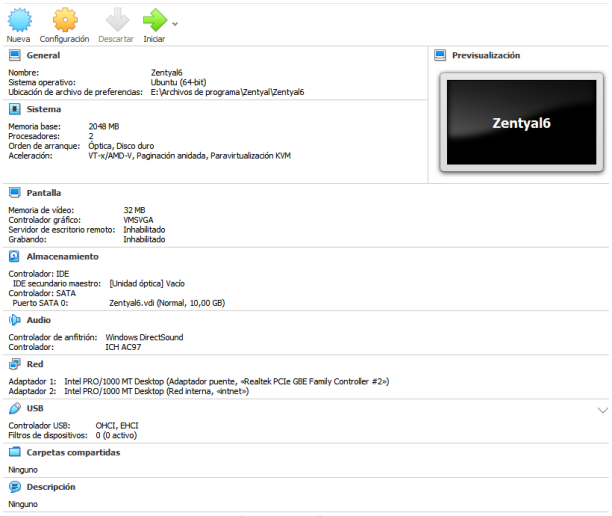

Fig. 1 Características máquina virtual Zentyal

Al arrancar el sistema nos carga un menú, donde seleccionamos la primera opción “Instalar Zentyal…”.

Fig. 2 Menú boot de Zentyal

Posteriormente seleccionamos el idioma español, país, y la distribución del teclado. Más adelante el asisten nos solicita asignarle un nombre al equipo, y crear un nombre de usuario y su contraseña.

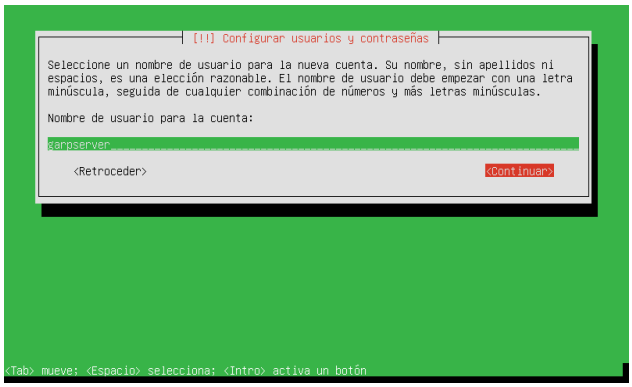

Fig. 3 Creación nombre de usuario

Cuando el proceso de instalación se ha completado el sistema solicita retirar la ISO. El sistema se reinicia y solicitará por primera vez el usuario y contraseña creado anteriormente.

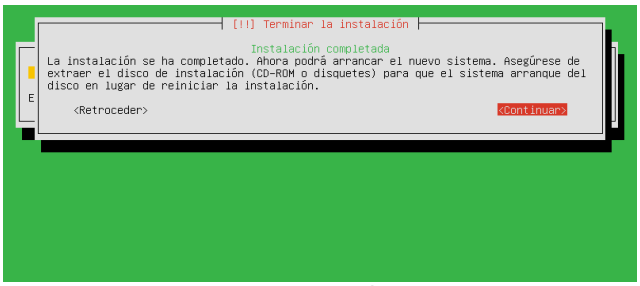

Fig. 4 Retirando medio extraíble para reiniciar

Una vez se ingresa a Zentyal el sistema automáticamente carga el browser Mozilla y nos direcciona al localhost con puerto 8443. Se digita el usuario y la contraseña y el browser nos carga un asistente de configuración inicial.

Fig. 5 Pantalla de inicio de Zentyal

Fig. 6 Configuración inicial

Hasta el paso anterior va la instalación básica del servidor Zentyal, ya que su configuración varía dependiendo de la temática desarrollada.

III. DHCP Server, DNS Server y Controlador de Dominio

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Solución planteada: para la instalación y configuración del DHCP Server, se da clic en el icono engranaje para iniciar la configuración.

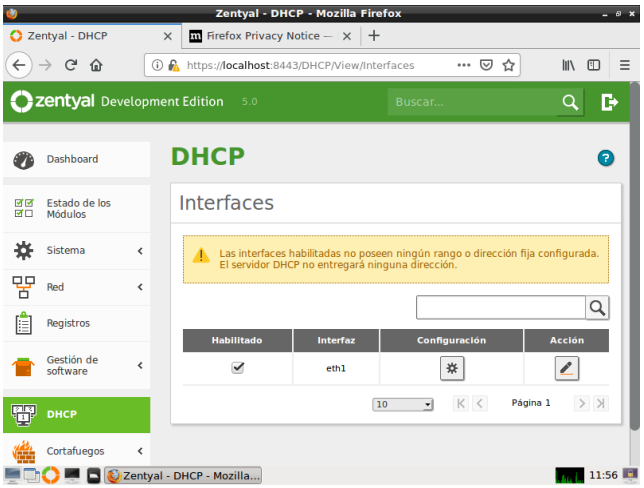

Fig. 7 Configuración inicial DHCP Server

Procedemos a configurar el rango de direcciones IP a repartir.

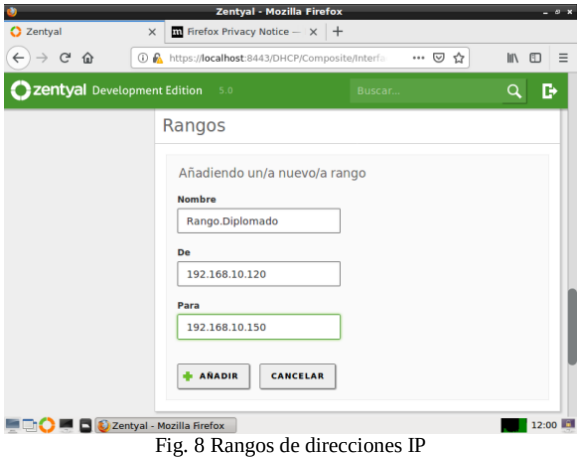

Fig. 8 Rangos de direcciones IP

Ingresar al cliente Ubuntu y confirmar la dirección IP dentro del rango programado.

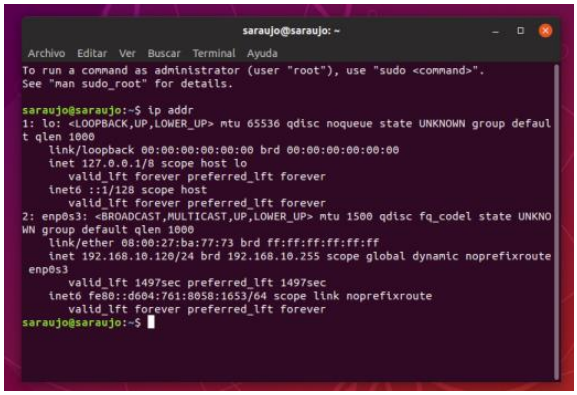

Fig. 9 Rangos direcciones IP

Para la instalación y configuración del DNS Server vamos al icono DNS en el Dashboard.

Fig. 10 Configuración DNS Server

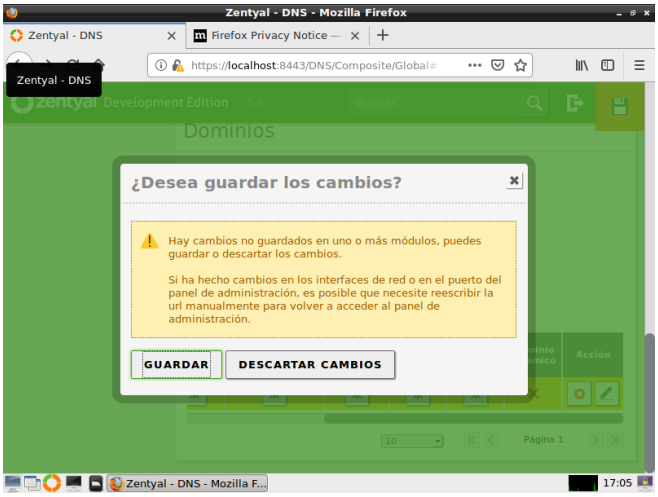

Fig. 11 Guardar cambios

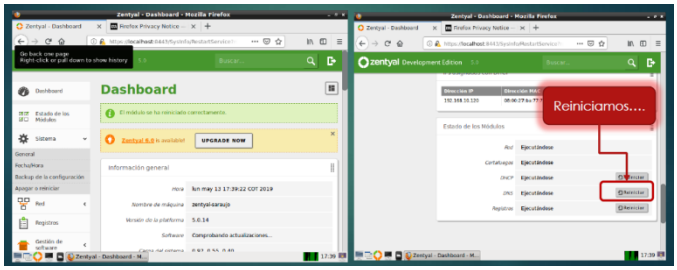

Fig. 12 Reinicio de servicio DNS

Fig. 13 Prueba DNS en el cliente

Para la instalación y configuración del Controlador de Dominio, primero se instala el módulo respectivo.

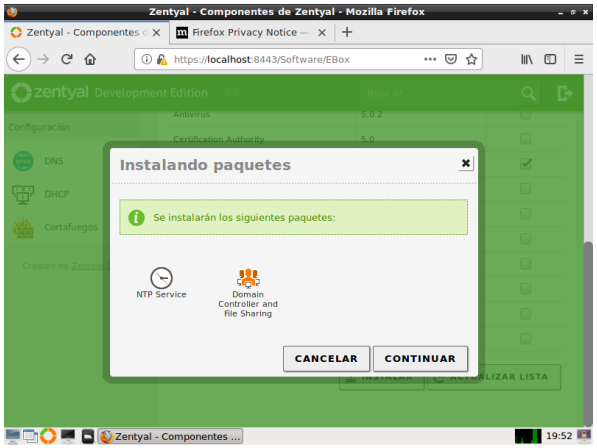

Fig. 14 Instalación modulo controlador de dominio

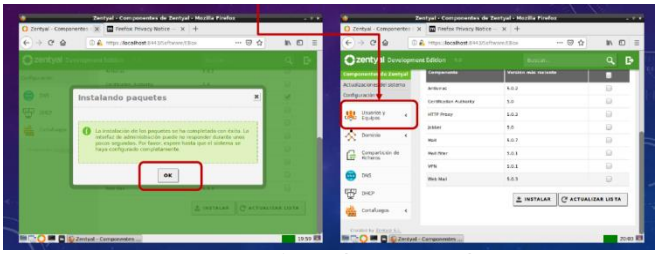

Fig. 15 Confirmación de instalación

Se procede a verificar la configuración del Dominio.

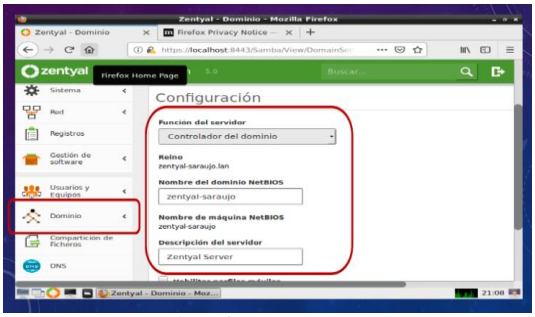

Fig. 16 Verificación asignaciones del dominio

Ahora se crean el grupo, usuarios, y el administrador.

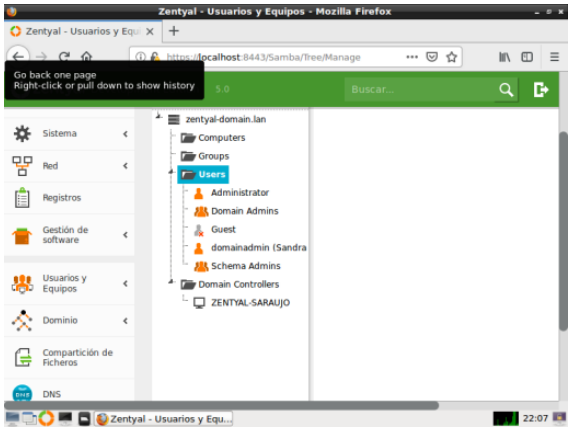

Fig. 17 Creación usuarios, grupos y administrador

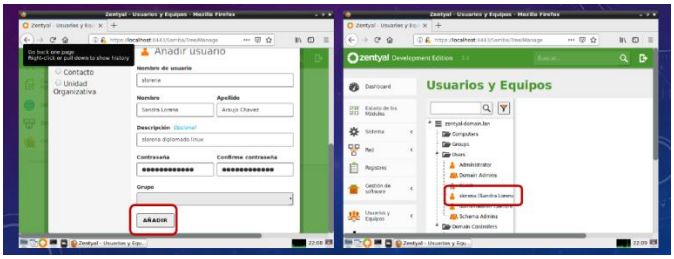

Fig. 18 Confirmación de usuario creado

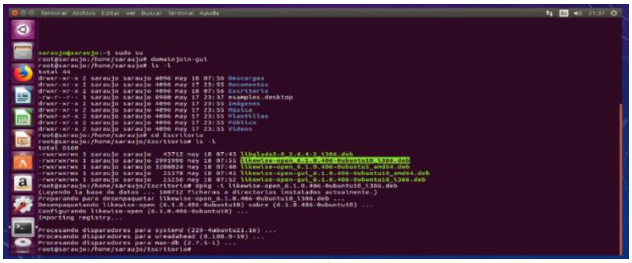

Fig. 19 Instalación de paquetes

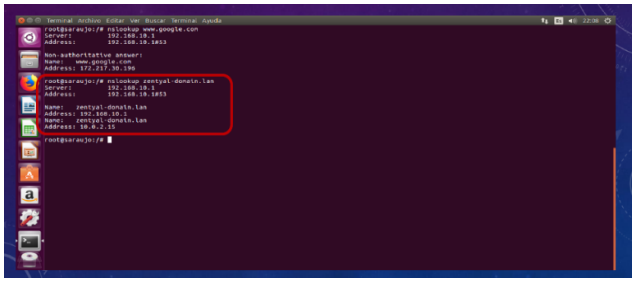

Fig. 20 Dominio activado y conectado

Se realiza la prueba de conexión al Dominio desde el cliente Ubuntu.

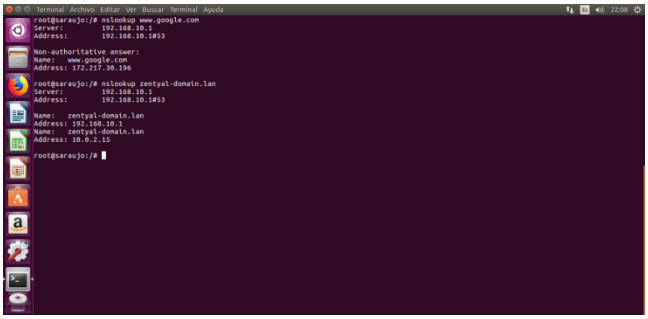

Fig. 21 Conexión del cliente Ubuntu

Como se observa en el resultado, se logró la conexión al servidor Zentyal desde el cliente Ubuntu, a través del usuario creado como controlador del Dominio.

IV. PROXY NO TRANSPARENTE

Producto esperado: 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.

Solución planteada: en interfaces de red, se configuran las tarjetas, estableciendo eth0 en DHCP para que establezca comunicación con la red WAN, por lo cual se activa (WAN), y así

opere como puerta de enlace.

La interfaz eth0 se configura externa y DHCP y la interfaz eth1 se configura interna con IP estática asignándose la 192.168.10.1

Fig. 22 Tipos de interfaces de red

Fig. 23 Configuración de las interfaces de red

Este es el resumen de la Dashboard con visualización de IP y de servicios activos.

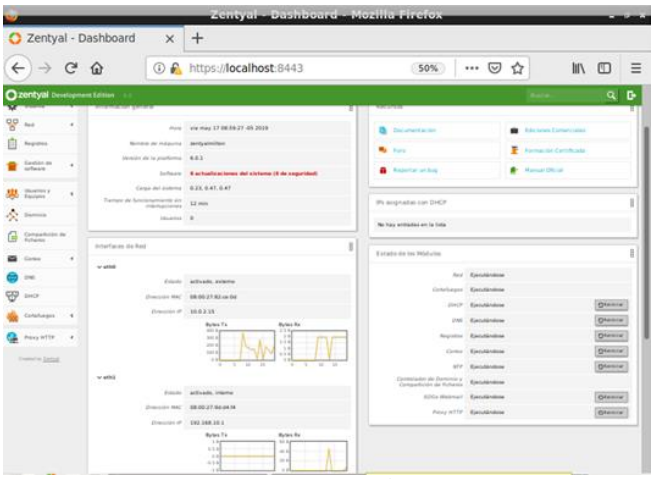

Fig. 24 Resumen de interfaces de red

La puerta de enlace debe apuntar al Servidor Zentyal, los clientes deben tener direcciones IP estáticas para poder hacer la configuración del módulo HTTP Proxy, ahora se crea y añade un nuevo objeto de nombre “interna”, en la pestaña de Red, Objetos.

Fig. 25 Añadir nuevo objeto y miembro

Se da nombre al miembro como “Cliente” y se selecciona CIDR para un nodo, indicando la dirección IP del equipo cliente, se hace con máscara 32 para que tome solo esas IP y se añade.

En la pestaña de HTTP Proxy, se configura el servidor y se indica que este va a ser No Transparente, desmarcando la casilla correspondiente y configurando el puerto 3128.

Fig. 26 Configuración proxy no transparente

Ahora vamos a crear un perfil de filtrado con el nombre general para luego poder aplicarlo a la regla de acceso.

Fig. 27 Creación perfil general

En la pestaña de reglas de dominio agregamos un dominio “eltiempo.com” y en decisión Denegar.

Fig. 28 Regla para URL eltiempo.com

Ahora en reglas de acceso se configura como Origen Objeto de Red Interna que es el nombre que dimos al Cliente, en decisión escogemos aplicar perfil de filtrado y general.

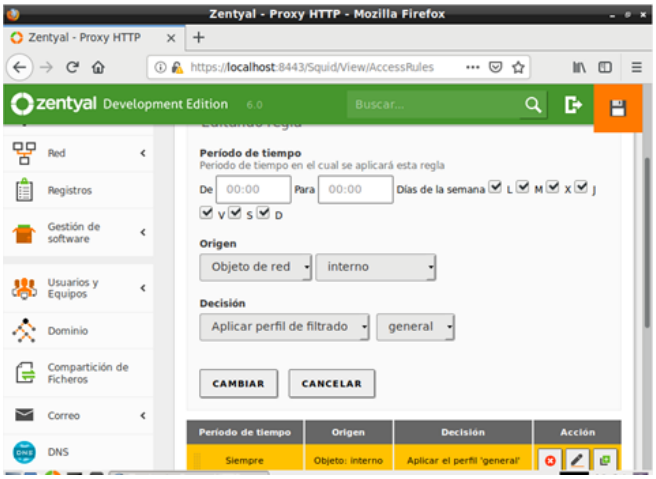

Fig. 29 Configuración reglas de acceso

Ahora configuramos Mozilla en Ubuntu con la dirección IP de nuestro proxy y el puerto3128.

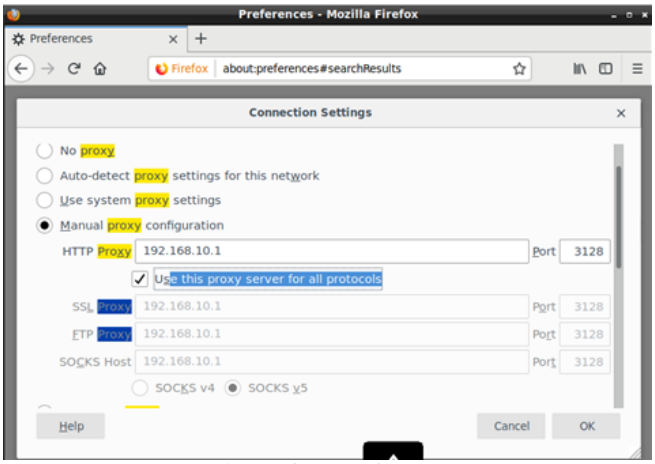

Fig. 30 Configuración conexión proxy en cliente

Ahora iniciamos Ubuntu e intentamos ingresar a la página www.eltiempo.com para evidenciar el correcto funcionamiento del proxy transparente en Zentyal. Es importante establecer la dirección IP fija en Ubuntu en el rango de direcciones para que se conecte a nuestra LAN o interna como la configure.

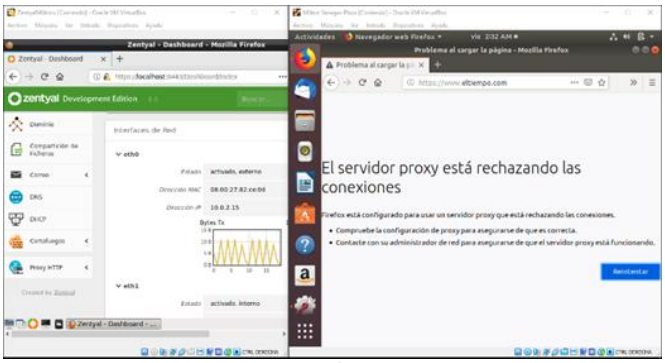

Fig. 31 Restricción de proxy no transparente

Como se puede observar, se logra filtrar desde el servidor Proxy no transparente el acceso a la dirección web www.eltiempo.com, creando el respectivo perfil de filtrado hacia cualquier URL que se desee.

V. 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 del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Solución planteada:

A. *Configurando Firewall*

Al intentar bloquear redes sociales por IP nos vamos a encontrar con dificultades, ya que son sitios complejos que constan de varios servidores y varias direcciones IP para prestar los servicios, no obstante, podríamos utilizar reglar para cada IP y bloquear estos dominios.

En ese caso iríamos al módulo Firewall y creeríamos las reglas para cada IP. Donde la IP de origen es la estación a la cual queremos restringir el servicio y la IP destino el dominio al cual se quiere alcanzar.

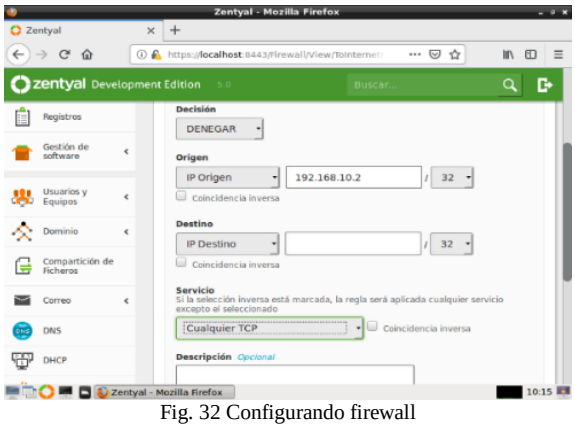

Fig. 32 Configurando firewall

Como segunda opción, quizá la más recomendable, usamos un proxy no transparente para restringir el acceso a ciertos dominios. Para ello nos vamos al módulo red y creamos un objeto. En mi caso

el objeto “lan”

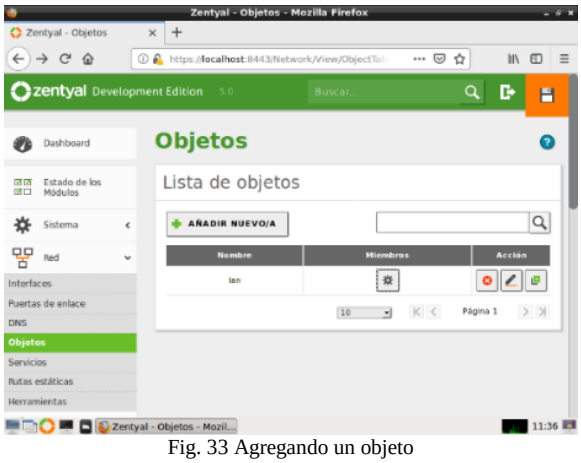

Fig. 33 Agregando un objeto

Dentro del objeto agregamos los miembros (las IP de las estaciones a las que deseamos restringir el acceso).

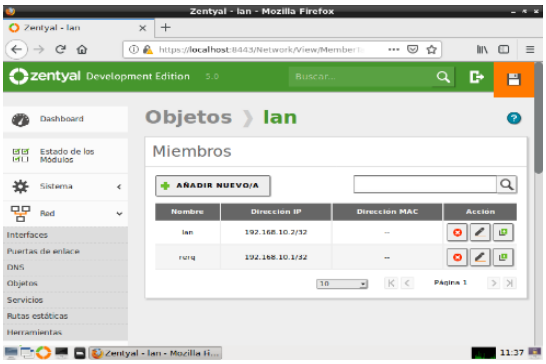

Fig. 34 Agregando miembros al objeto

Nos vamos modulo Proxy y agregamos un filtro, en mi caso es “FiltroLAN”.

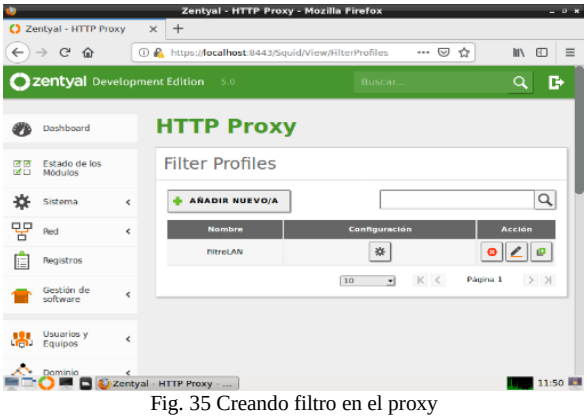

Fig. 35 Creando filtro en el proxy

Entramos en las opciones del filtro y nos dirigimos a Domains and URLs.

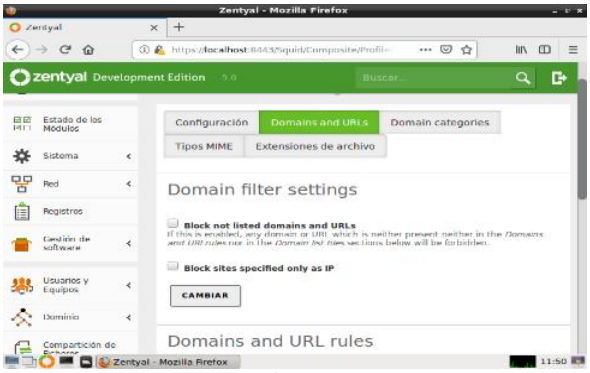

Fig. 36 Configuración de Domains and URLs

Y agregamos todas las URLs que queremos bloquear denegando el acceso.

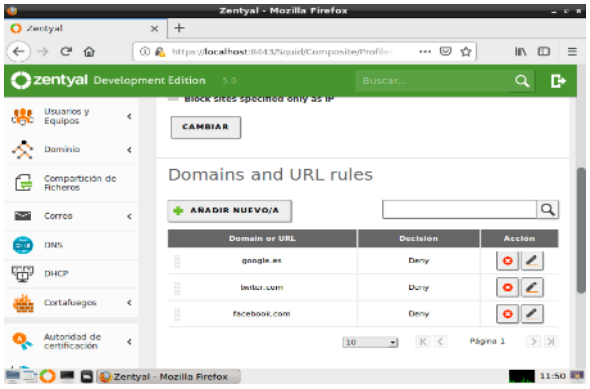

Fig. 37 Agregando URLs a bloquear

Por último, nos vamos a las políticas de acceso en el mismo modulo y ponemos como origen el objeto que hemos creado y le aplicamos el filtro que hemos creado.

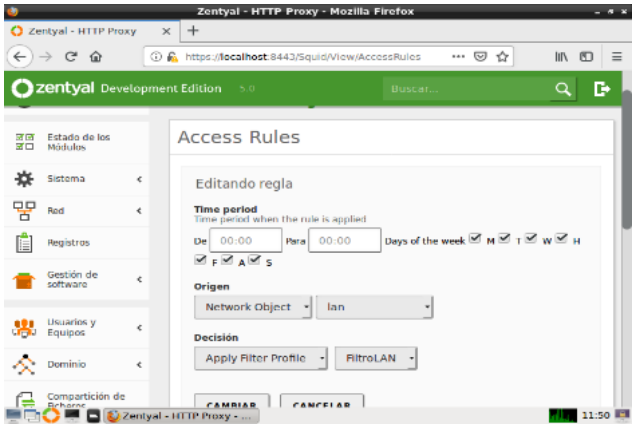

Fig. 38 Estableciendo políticas de acceso

Ahora comprobamos que esté funcionando lo que hemos realizado, tratamos de ingresar Facebook.

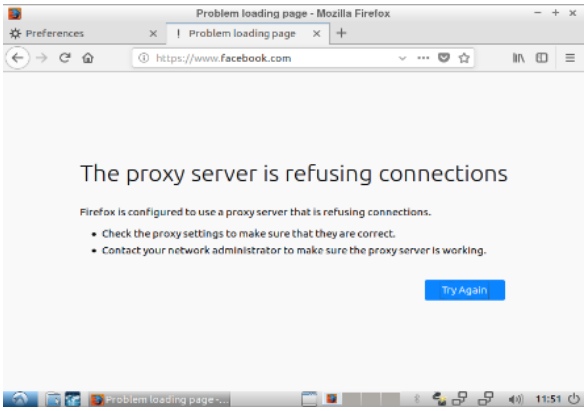

Fig. 39 Probando conexión a Facebook

Ahora intentamos con el sitio Dropbox que no está en la lista y vemos que si hay acceso.

Fig. 40 Accediendo a Dropbox

El resultado que evidenciamos se logra gracias a la configuración del proxy y del navegador, en este caso a través del puerto 3128 que viene configurado por defecto y las reglas de acceso y los filtros que hemos creado, los cuales permiten el tráfico de todas las páginas web a excepción de las que hemos puesto en la lista.

VI. FILE SERVER Y PRINT SERVER

Producto esperado: 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.

Solución planteada:

A. Activación de Módulo Controlador de Dominio y Compartición de Ficheros

Desde Estado de Módulos verificamos si el Módulo de Controlador de Dominio y Compartición de Ficheros se encuentra activo, si aparece seleccionado el cuadro quiere decir que se encuentra activo.

Fig. 41 Verificación de módulos

B. Configuración de Dominio

En el módulo de Dominio agregamos el nombre de Dominio "garspserver" y damos clic en Añadir, luego damos guardar para ajustar los cambios.

Fig. 42 Configurando el dominio

C. Configuración de Grupo y Usuario

Nos dirigimos a Usuarios y Equipos, damos clic sobre Grupo ubicado en el árbol para selecciona y en la parte inferior damos clic en + para agregar un Grupo.

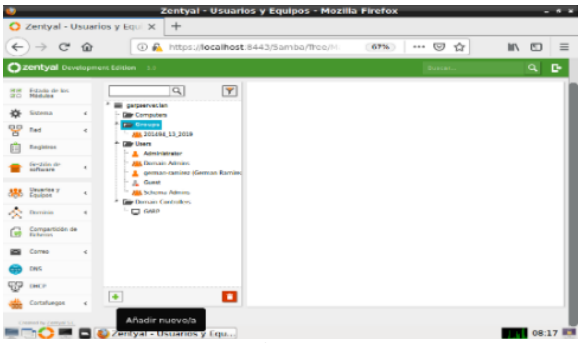

Fig. 43 Configurando un grupo

Digitamos en nombre de grupo 201494_93_2019 y damos clic en Añadir.

Fig. 44 Creando un grupo

Realizamos el mismo proceso para crear un Usuario, esta vez en el árbol seleccionamos "Users" y damos clic en + ubicado en

la parte inferior de pantalla. Diligenciamos los campos como Nombre de Usuario, Nombre, Apellido, contraseña y seleccionamos en Grupo “201494_13_2019”.

Fig. 45 Creando un usuario

D. Creando Fichero y configurando Acceso

Nos dirigimos a Compartición de Ficheros y damos clic en Añadir.

Fig. 46 Creando el fichero

Se diligencia los campos los campos Nombre del Recurso Compartido, Ruta del Recurso y Comentario. Seguido clic en añadir.

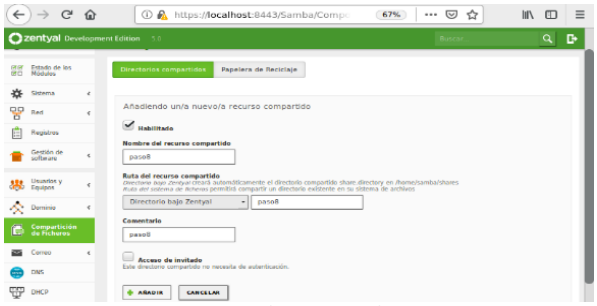

Fig. 47 Configurando el fichero

Vamos a control de Acceso, seleccionamos el Usuario y damos los permisos respectivos, finalizado el proceso damos clic en Añadir.

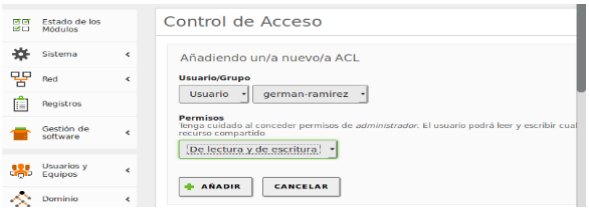

Fig. 48 Configurando control de acceso

Se guardan los cambios, y ahora vamos a Ubuntu Desktop para realizar la prueba de conexión, abrimos el visualizador de ficheros y en la parte inferior digitamos en la casilla conexión *smb://192.168.100.1* y damos clic en Conectar.

Fig. 49 Conectando al servidor en Ubuntu desktop

Nos pide autenticarnos, aquí digitamos el usuario y contraseña creados desde Zentyal, una vez ingresados observamos la carpeta creado con el nombre *Paso8*. La conexión fue exitosa.

Fig. 50 Conectando al servidor

Fig. 51 Vista de conexión al fichero compartido

E. Conexión Print Server

Nos dirigimos al localhost con puerto 631, el cual pertenece a CUPS para configurar la impresora. Vamos a “Add Printer”.

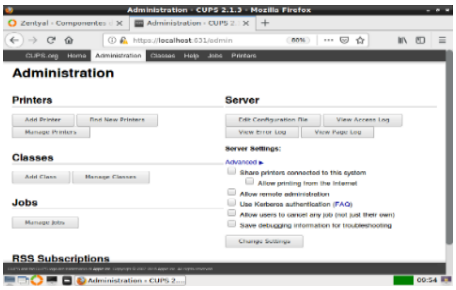

Fig. 52 Ingresado a Cups

Cuando ingresamos nos pide Usuario y Contraseña los cuales se digitan para su ingreso.

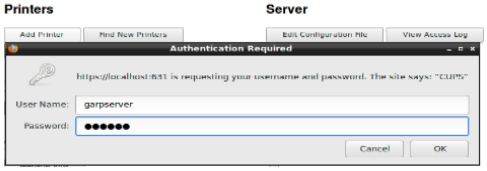

Fig. 53 Solicitud de credenciales

Seleccionamos el Protocolo a usar AppSocket HP y

continuar.

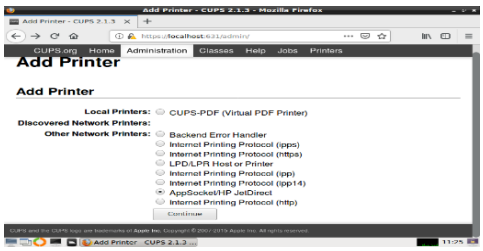

Fig. 54 Seleccionando protocolo

Digitamos el nombre "HP" y el campo Location es opcional, se selecciona "Share This Printer" (compartir) y clic en continuar.

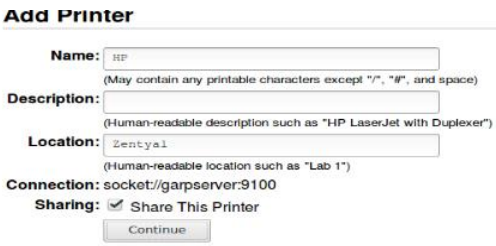

Fig. 55 Digitando nombre de impresora

Seleccionamos la marca y luego el modelo de impresora.

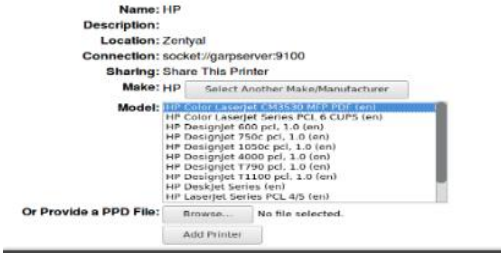

Fig. 56 Selección modelo de impresora

Se deja opciones por defecto en tamaño de hoja y otras características, una vez finalizada la configuración el sistema nos dice que se ha completado.

Fig. 57 Finalizada la instalación

Vamos a Ubuntu Desktop y agregamos la impresora, y debe darnos estado Inactiva.

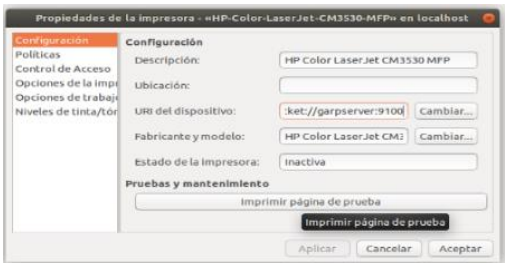

Fig. 58 Agregando impresora en Ubuntu desktop

Se envía una impresión de página de prueba y observamos el estado desde el servidor, prueba exitosa.

Fig. 59 Prueba de impresión

Con la opción CUPS al instalar una impresora local o una impresora en Red en otro ordenador podemos generar una configuración en el Server para compartir impresoras con nuestros usuarios de red mediante diferentes protocolos que son conectados por Red y administrador por el Server.

VII. 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 Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Solución planteada: Una vez terminada la instalación del servidor Zentyal, se instalan los paquetes necesarios para poner en marcha el servicio de red VPN.

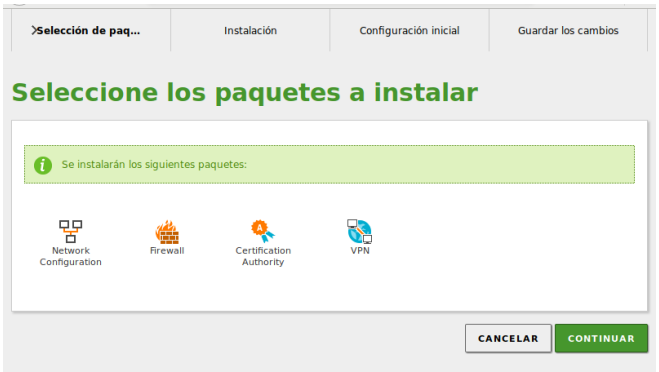

Fig. 60 Paquetes a instalar

Terminada la instalación de los paquetes, se configuran las interfaces de red, que en este caso son dos. La interfaz eth0 se deja como externa (WAN) y la interfaz eth1 como interna (LAN).

Desde la Dashboard ubicamos la opción “Autoridad de certificación” y damos clic allí para proceder a crear dos certificados: una para el servidor VPN y otro para el cliente.

Fig. 61 Listado de certificados

Ya creados los certificados, vamos a la opción de VPN y se procede a crear el servidor.

Fig. 62 Lista de servidores

Se configuran luego algunos parámetros del servidor VPN como la dirección de red, el puerto, el certificado y los servidores de nombre de Dominio.

Ahora se procede a crear el servicio respectivo para el servidor VPN, desde la opción Red y el menú Servicios.

Fig. 63 Lista de servicios

Luego se configura el servicio, seleccionando el protocolo UDP, el puerto de origen en cualquiera y el puerto destino 1194, que es el que usará el servidor VPN.

Configuramos el Cortafuegos accediendo al menú “Filtrado de paquetes”. En la sección de las redes internas a Zentyal se añade una regla que permita el acceso por el puerto 1194 a través del servicio creado “servicio-vpn”.

Fig. 64 Reglas de filtrado del Cortafuegos

La anterior regla se crea igualmente para la sección de redes externas a Zentyal.

Una vez realizadas todas las configuraciones anteriores, es recomendable guardar los cambios en el servidor.

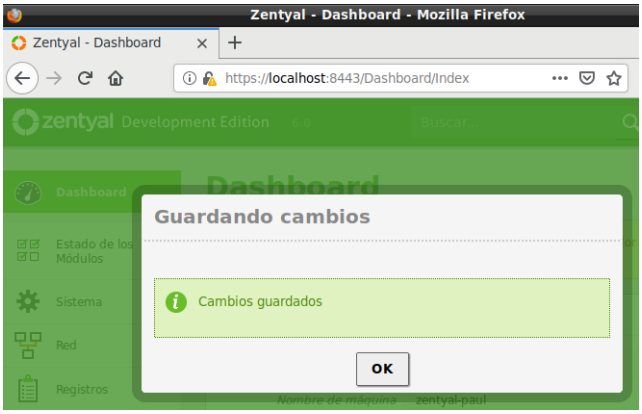

Fig. 65 Guardando cambios del servidor

Podemos verificar también que el demonio del servidor VPN está habilitado y corriendo.

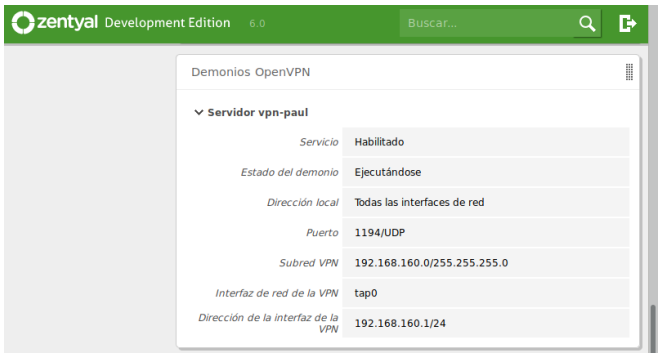

Fig. 66 Widget de OpenVPN

Se procede a descargar el paquete de configuración para el cliente Ubuntu, donde primero hay que escoger algunas opciones como: tipo de cliente, certificado del cliente, estrategia de conexión y dirección del servidor. Al dar clic en el botón descargar vemos que se ha generado un archivo con extensión tar.gz.

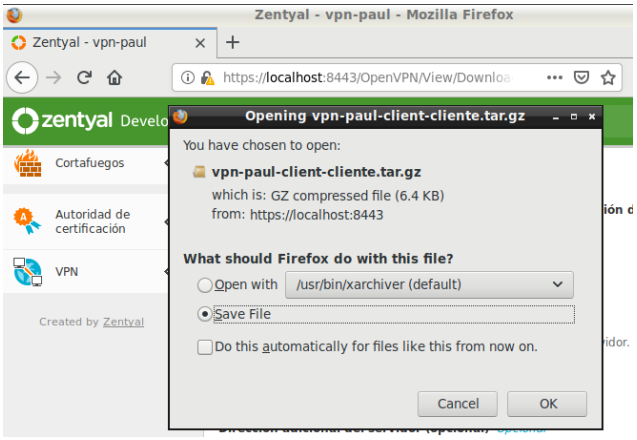

Fig. 67 Descarga de configuración del cliente

El anterior archivo de configuración del cliente se copia al equipo del cliente Ubuntu, luego se extrae en la misma ubicación. Hecho lo anterior, se realiza la instalación del paquete OpenVPN. Si en este punto se intenta acceder a Internet veremos que no hay acceso.

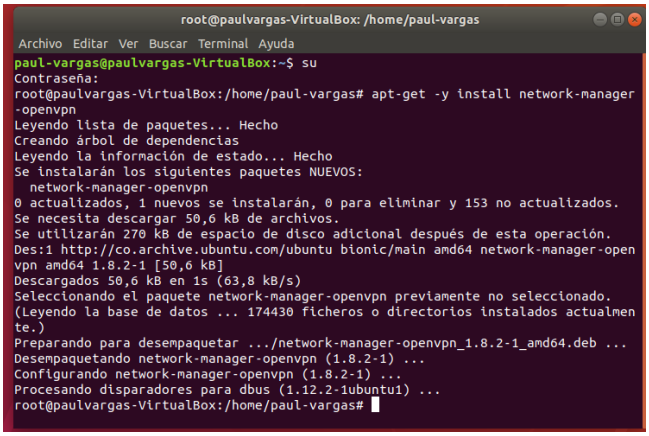

Fig. 68 Instalación de OpenVPN

Luego, se reinicia el servicio de Network Manager para que actualice la GUI. Entramos al editor de configuración de la Red y vemos una nueva sección llamada "VPN". Damos clic en el símbolo + para añadir la red VPN, escogemos la opción "Importar desde un archivo…". Seleccionamos y abrimos el archivo de extensión "conf" que se haya en el directorio extraído anteriormente. De ese modo quedan guardados los parámetros de conexión a la VPN. Al activar la conexión VPN podemos ver que nos aparece un nuevo ícono de red.

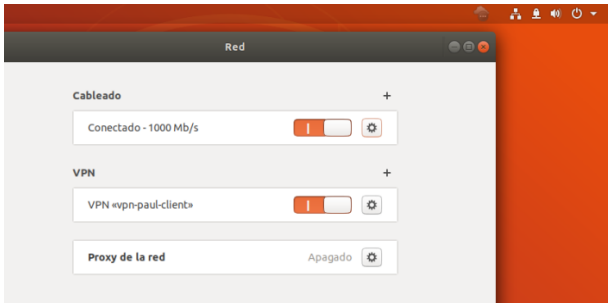

Fig. 69 Propiedades de red del cliente

Desde el servidor Zentyal, podemos visualizar que el cliente Ubuntu está realmente activo y conectado a la VPN.

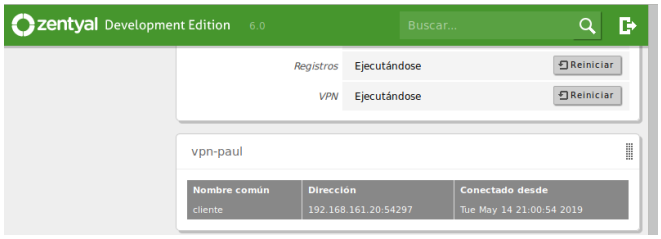

Fig. 70 Widget de clientes conectados a la VPN

Al realizarse otra prueba de acceso a Internet desde el cliente Ubuntu encontramos que satisfactoriamente nos carga la página web.

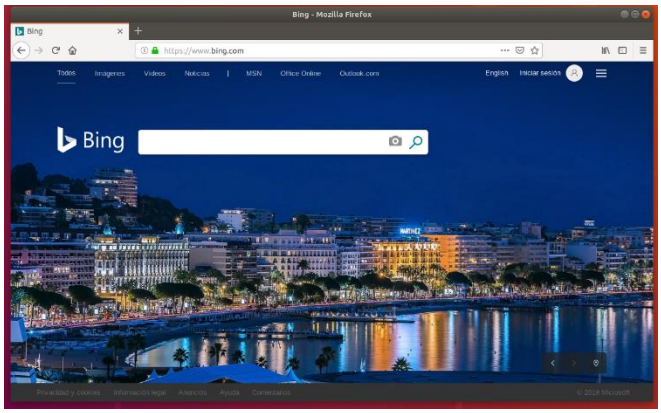

Fig. 71 Confirmación de acceso a Internet

Mientras el equipo cliente no haya validado el acceso al servidor VPN, no se tiene ningún tipo de acceso a ninguna red, ya que hace parte de una red interna; una vez logueado el cliente Ubuntu a la VPN a través del certificado que se expidió desde el servidor, tenemos acceso abierto a la red VPN e Internet.

VIII. CONCLUSIONES

El sistema operativo Zentyal es una distribución Linux para servidores, basada en Ubuntu, que ha sido diseñada y desarrollada como una seria alternativa a las versiones Windows Server de Microsoft. La última versión de Zentyal (6.0), está basada en la distribución Ubuntu Server 18.04.1 LTS. Zentyal nos ofrece la

opción de integrar toda nuestra infraestructura de red, ofreciendo diversos módulos y servicios, entre los cuales se destacan: servidor DHCP, DNS, Proxy HTTP, cortafuegos, controlador de Dominio, servicio de sincronización de hora (NTP), servicio de transferencia de ficheros (FTP), servicio de redes privadas virtuales (VPN), gestión de máquinas virtuales y copias de seguridad.

Se aprendió a configurar los servicios para la administración de una red basada en Linux con un directorio activo, se instaló y se configuró Zentyal server como sistema operativo base para la implementación y configuración de DHCP Server, DNS Server y Controlador de Dominio.

Se aprendió la implementación y configuración detallada del control del acceso desde una estación GNU/Linux Ubuntu Desktop hacia los servicios de conectividad de Internet del servidor Zentyal a través de un Proxy no transparente que filtra la salida por medio del puerto 3128.

Los cortafuegos son indispensables para tomar control y protección de los sistemas a los cuales estamos administrando y a los cuales queremos ofrecer servicios, Zentyal ofrece un módulo de cortafuegos muy completo que nos permite controlar el tráfico de una red WAN y redes internas. Con el trabajo realizado pudimos evidenciar que en el caso de restringir páginas web es muy remendable hacer uso de un proxy para crear filtros que nos permitan cumplir con este objetivo.

La configuración de File Server permitió conocer las bondades del compartir ficheros administrados por el Zentyal Server creando grupos y usuarios y asignando permisos de forma fácil. El Print Server nos demostró una forma sencilla de compartir impresoras en Red a su vez poder compartir el fichero de instalación y configuración, conceptos aprendidos en la Temática 4.

Una red VPN nos permite crear una red local sin la necesidad de que los usuarios estén físicamente conectados entre sí, y también puede ofrecernos algunas ventajas, como evitar bloqueos de sitios web por un país o zona geográfica. Cabe resaltar también, que una Red Privada Virtual se puede trabajar como una extensión de una red local (LAN), ofreciendo mayor seguridad por medio del cifrado de paquetes de datos; además de la opción de autenticación de clientes/usuarios, a través de certificados (firmas digitales). Lo anterior nos garantiza, que los datos o información transmitida por la red VPN no podrá ser fácilmente leída por terceros o capturada por alguna persona inescrupulosa.

IX. BIBLIOGRAFIA

[1] Configurar un servidor de Ficheros. [En línea]
Disponible en:
https://doc.zentyal.org/es/directory.html#configurar-un-servidor-de-ficheros-con-zentyal

[2] Gestionar Usuarios, Grupos y Equipos. [En línea]
Disponible en:
https://doc.zentyal.org/es/directory.html#gestionar-usuarios-grupos-y-equipos

[3] CUPS – Servidor de impresión. [En línea]
Disponible en:
https://help.ubuntu.com/lts/serverguide/cups.html.es

[4] Servicio de compartición de impresoras. [En línea]
Disponible en:
https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_comparticion_de_impresoras

[5] Instalación - Documentación de Zentyal 6.0. [En línea]
Disponible en:
https://doc.zentyal.org/es/installation.html

[6] Instalar servidor de VPN en Zentyal Server 5. [En línea]
Disponible en:
http://red-orbita.com/?p=7680