

Administración y afinamiento del sistema operativo GNU/Linux Zentyal Server 5.0 para la disposición de servicios en la creación de una infraestructura TIC

Juan José Ceballos Navia, José Albeiro Ayala, Jonnathan Bucheli, Albaro José Ordoñez, Chrystian Miguel Quintero

Universidad Nacional Abierta y a Distancia UNAD

Bogotá, Colombia

juanfix@gmail.com

jualdacam@gmail.com

joobga@gmail.com

cmquinterome@unadvirtual.edu.co

ayala.181@hotmail.com

Abstract— El presente documento está orientado a la administración y afinamiento del sistema operativo GNU/Linux Zentyal Server 5.0, enfocado a la implementación de servicios para la creación de una infraestructura TIC con arquitecturas de red de Intranet y Extranet dirigido a instituciones de la vida real. En este orden de ideas, con el sistema operativo base Zentyal se pretende instalar y configurar los servicios necesarios para cumplir con el objetivo de la evaluación final del diplomado de Linux; estos servicios son DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.

Palabras clave - Linux, Zentyal, Servicios, Intranet, Extranet, DHCP, DNS, Controlador de dominio, Proxy, Infraestructura, Cortafuegos, File, Print, Server.

I. INTRODUCCIÓN

Zentyal es un servidor basado en la arquitectura GNU/Linux que funciona como una aplicación web, este sistema ofrece una variedad de servicios de red para potenciar una infraestructura informática. Con el desarrollo de las siguientes temáticas se pretende estudiar los resultados obtenidos en cuanto a configuración e implementación de servicios de infraestructura para intranet y Extranet; Y de esta manera afianzar los conocimientos necesarios para la administración y control de los protocolos y servicios de un servidor dedicado, garantizando el correcto funcionamiento y solución de las problemáticas planteadas.

II. INSTALACIÓN DE ZENTYAL

A. Proceso de instalación

Escoger la distribución Ubuntu de Linux

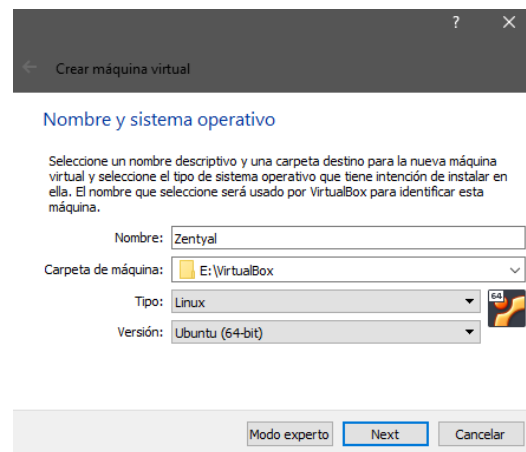


Fig. 1 Inicio de la instalación.

Configurar las dos tarjetas de red. El adaptador 1 se configura con la opción adaptador puente para tener acceso a internet.

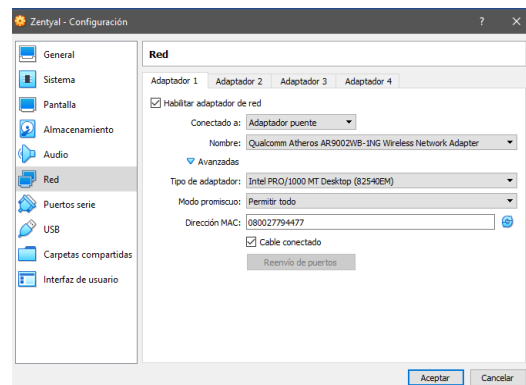


Fig. 2 Configuración adaptador 1.

El adaptador 2 se configura con un tipo de red interna para tener conexión posteriormente con la máquina de Ubuntu.

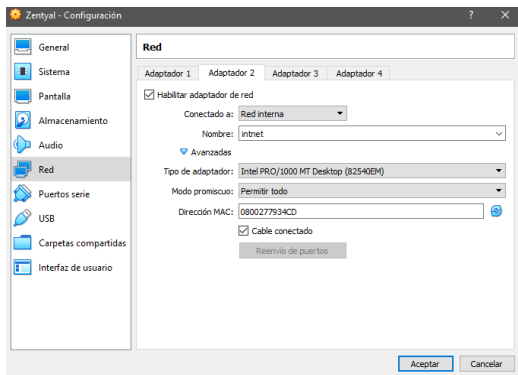


Fig. 3 Configuración adaptador 2.

Arrancar el sistema desde la ISO y escoger idioma del Sistema operativo deseado.

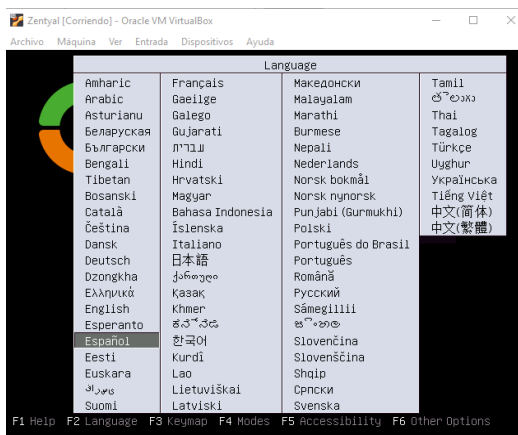


Fig. 4. Escoger idioma de Zentyal

Instalar con la opción de borrar el disco para realizar una instalación limpia desde cero.



Fig. 5 Instalación de Zentyal.

Escoger ubicación y luego la configuración y distribución del teclado en español Latinoamérica.

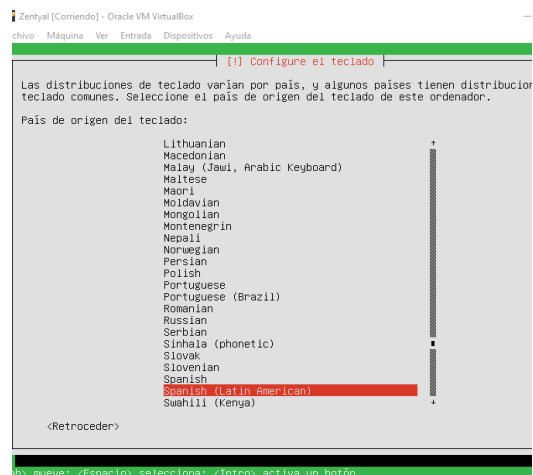


Fig. 6 Idioma del teclado.

Escoger la interfaz de red primaria para la instalación. Esto permitirá que se defina la red principal y se conecte a internet.

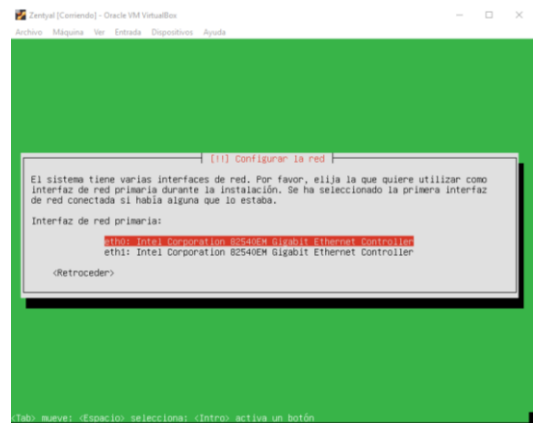


Fig. 7 Red principal.

Escoger el nombre que tendrá la máquina

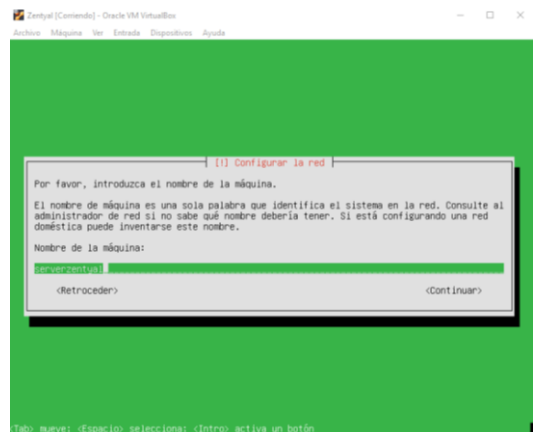


Fig. 8 Nombre de la máquina.

Configurar un nombre de usuario para Zentyal Server

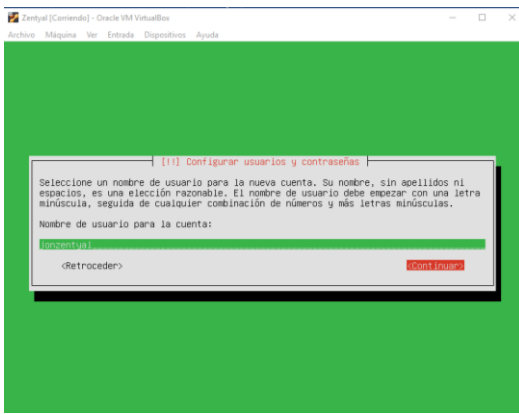


Fig. 9 Nombre de usuario.

Configurar una contraseña de usuario

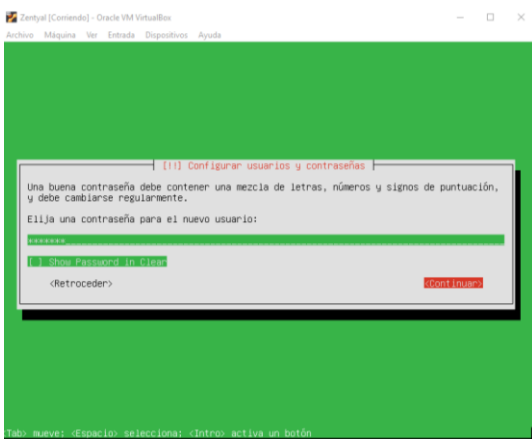


Fig. 10 Definir contraseña.

Completar la instalación y esperar al reinicio de la máquina.

B. Configuración

En cuanto termina la instalación, Zentyal nos lleva directamente al navegador para poder iniciar sesión en el servidor.

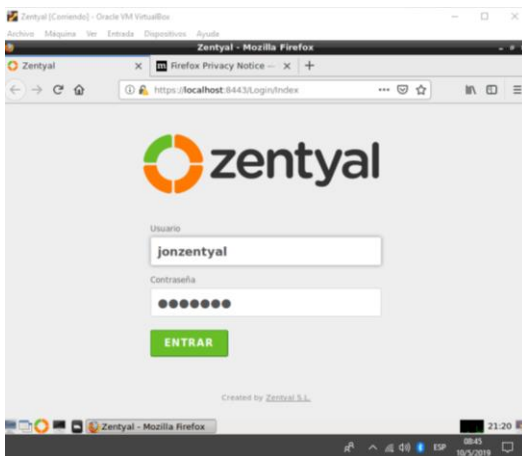


Fig. 11 Inicio de sesión.

En la configuración inicial se recomienda dar clic en continuar para empezar con las configuraciones básicas.

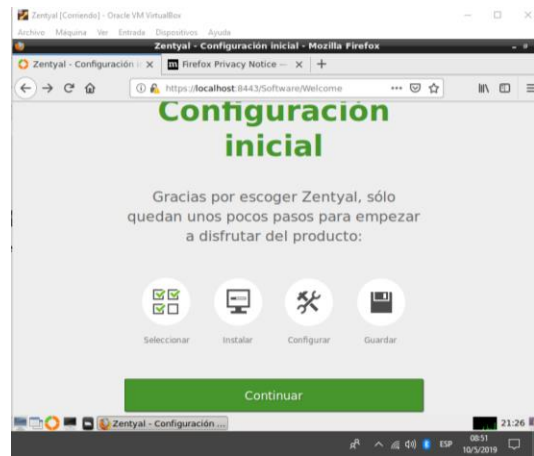


Fig. 12 Configuraciones básicas de Zentyal.

Seleccionar los servicios necesarios para realizar las temáticas planteadas.

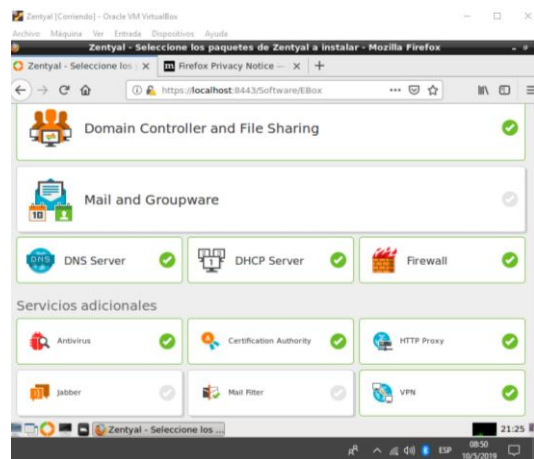


Fig. 13 Selección de módulos.

Confirmar la instalación de los paquetes a instalar y cuando la instalación haya terminado, aparecerá un mensaje de confirmación:

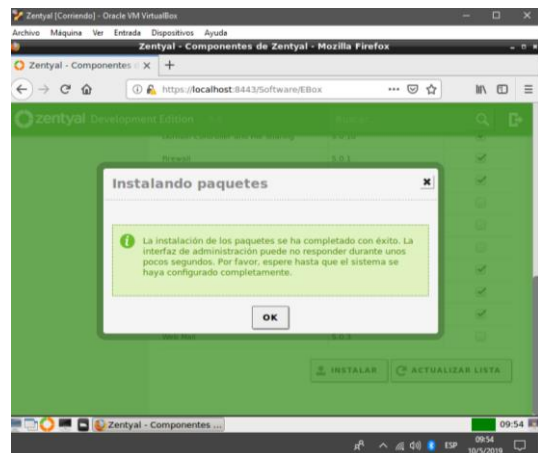


Fig. 14 Confirmación de instalación.

Configurar las dos interfaces, la primera como externa para la conexión a Internet.

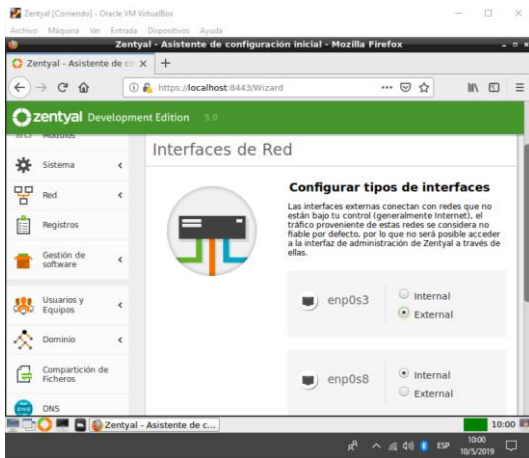


Fig. 15 Configuración de red externa.

Asignar una IP estática a la red interna para tener conexión con la máquina de Ubuntu.



Fig. 16 Configuración de red interna.

Asignar un nombre de dominio que identifique al servidor de Zentyal

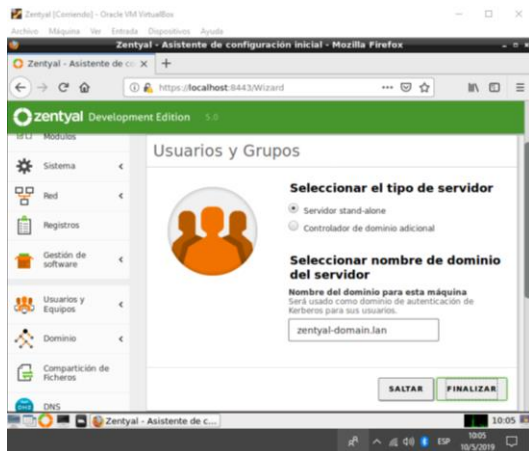


Fig. .17 Asignación del nombre de dominio.

Al finalizar es necesario guardar los cambios y a continuación se visualiza la Dashboard de Zentyal que brinda información del sistema.

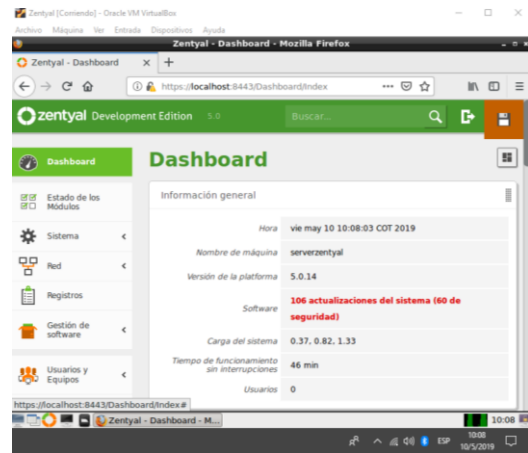


Fig. 18 Dashboard.

Con esto queda instalado y configurado el sistema operativo Zentyal Server 5.0.

III. TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Se debe activar el módulo DHCP en la pestaña “Estado de módulos” y luego guardar los cambios para trabajar con los servicios DHCP.

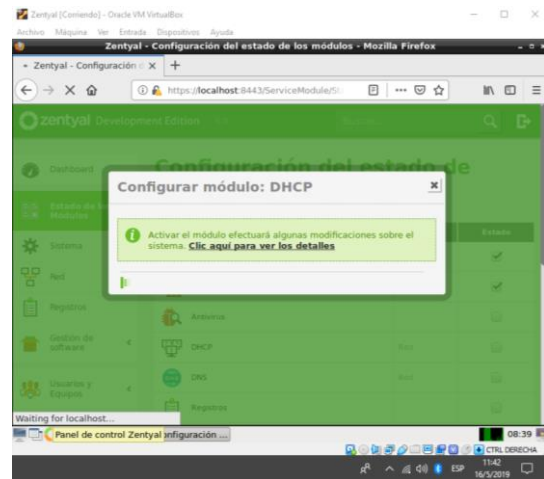


Fig. 19 Activar módulo DHCP.

En el menú izquierdo, ir a la pestaña DHCP y luego ir a la configuración de la red para crear la red en la que se conectará el servidor con el cliente; de esta manera se repartirán direcciones IP automáticamente dentro de un rango.

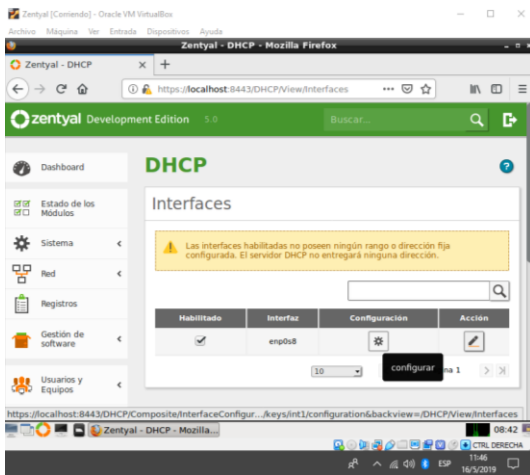


Fig. 20 Configuración DHCP.

Cambiar el servidor DNS y asignar los DNS de Google

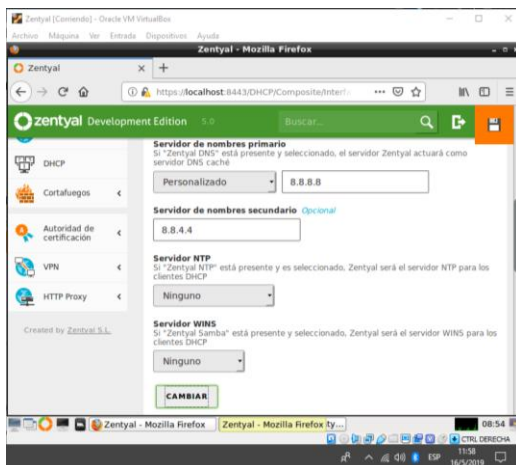


Fig. 21 DNS de Google.

En el apartado de rangos, asignar el rango de direcciones que van a tener los equipos dentro de la red.

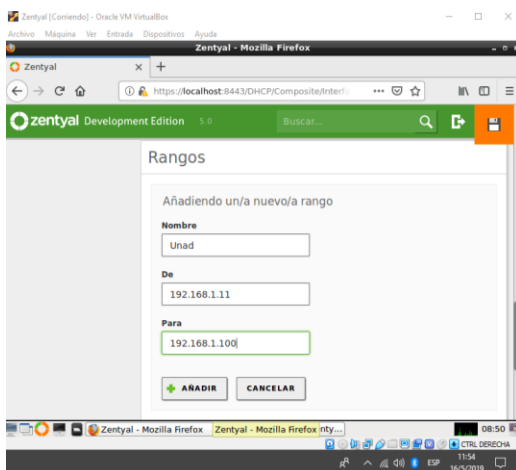


Fig. 22 Asignación de rango de red.

Comprobar la dirección IP en Ubuntu que se asigna automáticamente con el DHCP de Zentyal Server.

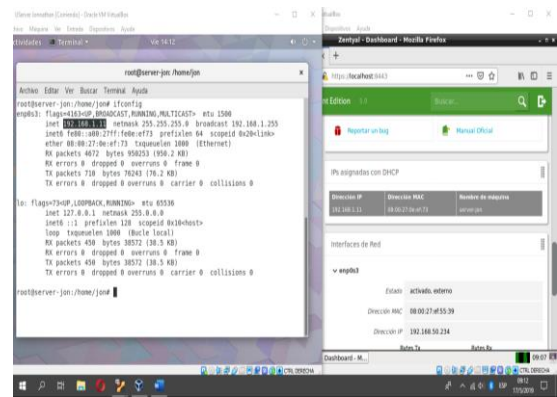


Fig. 23 Prueba de conexión entre el servidor y el cliente.

En la pestaña de DNS habilitar el caché de DNS transparente para identificar el tráfico de las peticiones de resolución de nombre de dominio de un cliente.

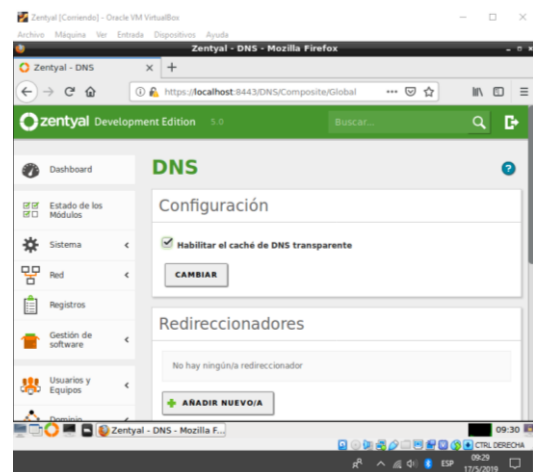


Fig. 24 DNS transparente.

Comprobar el nombre de dominio del servidor con el nombre que se asignó en las configuraciones básicas.

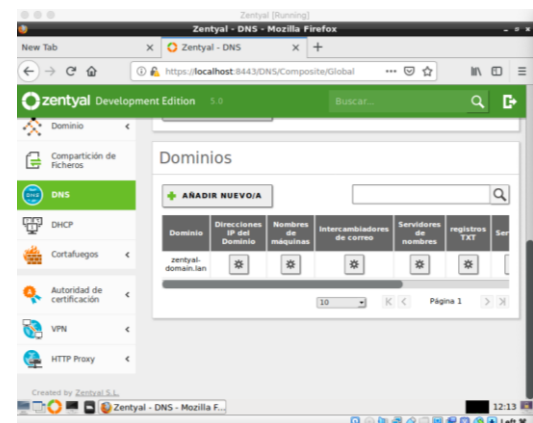


Fig. 25 Comprobación DNS.

En el menú ir a Usuarios y luego a Equipos/Gestión/Users/Añadir nuevo usuario. Agregar un nuevo grupo de seguridad que permita asignar permisos a recursos compartidos.

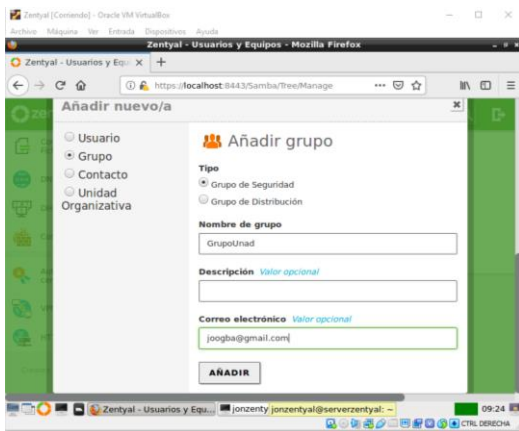


Fig. 26 Creación de grupo.

Crear un nuevo usuario que será usado como cliente

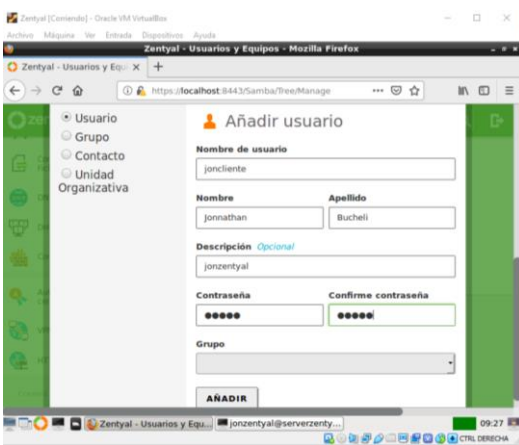


Fig. 27 Creación de usuario.

Agregar el grupo creado anteriormente y el grupo Domain Admins para que el usuario tenga permisos de administrador.

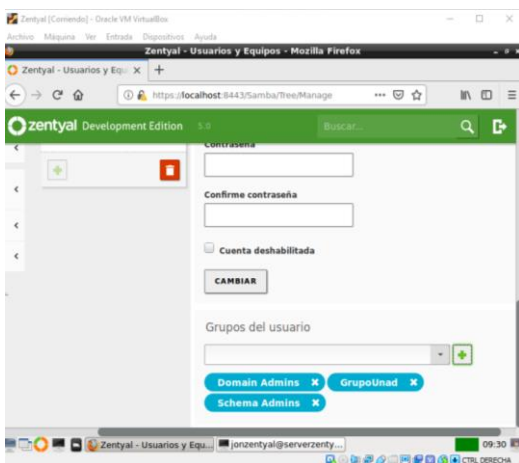


Fig. 28 Asignación de grupos al usuario.

Se le realiza ping al nombre de dominio zentyal-domain.lan (DNS de Zentyal server (Fig. 16.) para comprobar la creación correcta del servidor DNS.

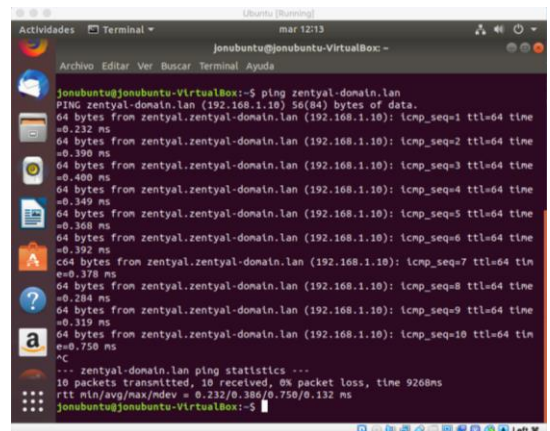


Fig. 29 Ping al servidor DNS de Zentyal.

IV. TEMÁTICA 2: PROXY NO TRANSPARENTE

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.

En la sección de los módulos se activa el módulo de red, luego se configuran las tarjetas de red, la enp0s3 se deja en modo DHCP para que se conecte a la red WAN y se activa la casilla de la WAN para que actúe como Gateway.

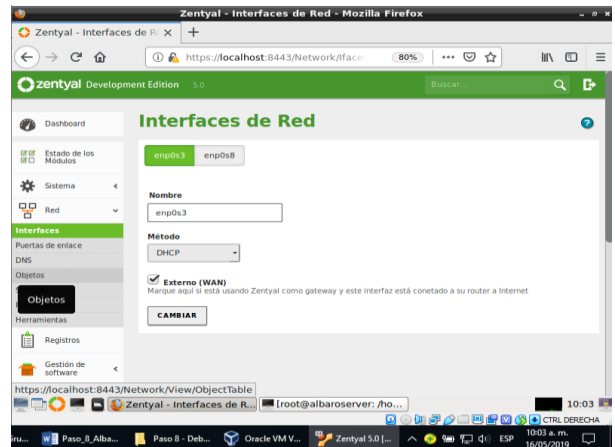


Fig. 30 Configuración de tarjetas de red.

La enp0s8 se configura en modo estático y se le asigna la IP 192.168.0.30 para conectar los clientes.

En la sección de Red/objetos añadimos un nuevo objeto y seleccionamos CIDR para un solo equipo, se le indica la dirección IP del cliente. Se hace con máscara 32 para que tome sólo esa IP.

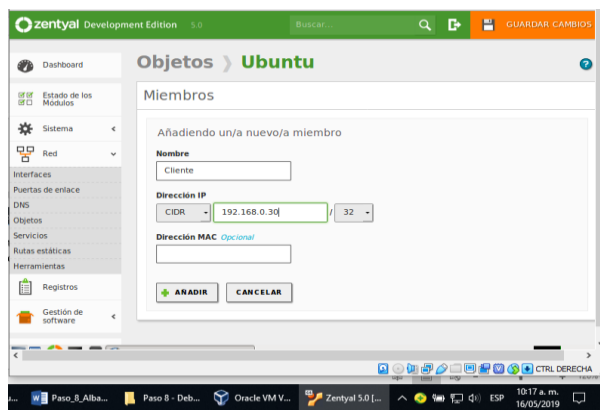


Fig. 31 Añadir nuevo objeto.

En la pestaña de HTTP Proxy, configuramos el servidor y se indica que este no va a ser transparente, desmarcamos la casilla correspondiente y configuramos el puerto 3128.

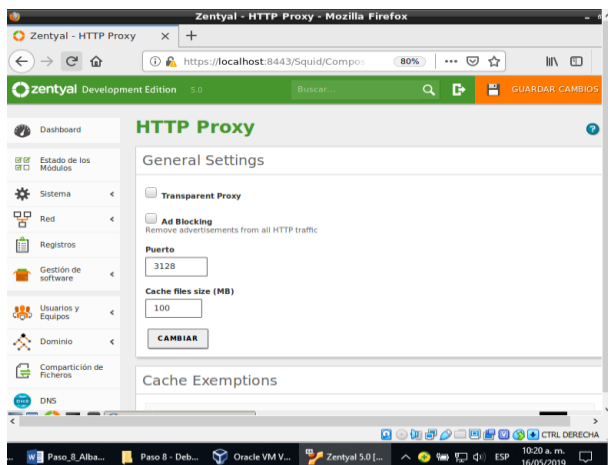


Fig. 32 Configuración de proxy.

En la sección de reglas de acceso del servidor proxy, creamos una nueva regla y en el origen seleccionamos el objeto creado anteriormente y en decisión seleccionamos denegar todo "Deny All".

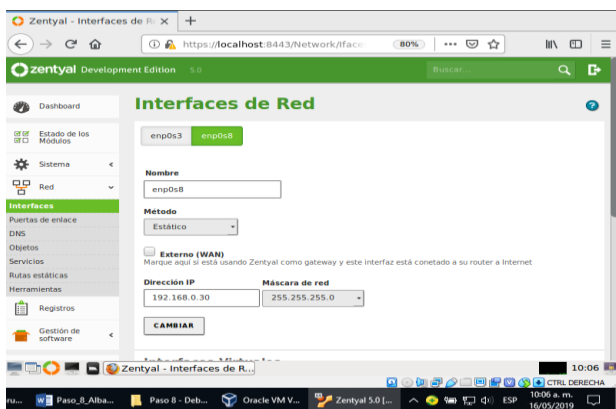


Fig. 33 Configuración de enp0s8.

Guardamos los cambios y procedemos a configurar en Ubuntu Desktop el proxy. Ingresamos al navegador Mozilla y se hace la configuración manual del proxy con la información de IP 192.168.0.30 y el puerto 3128.

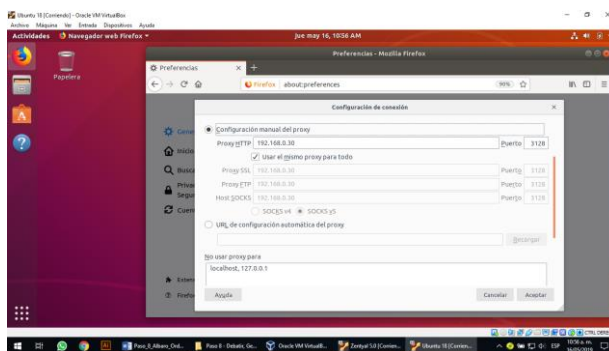


Fig. 34 Configuración manual del proxy.

Entramos a <https://www.youtube.com/> y observamos que el servidor proxy está rechazando las conexiones.

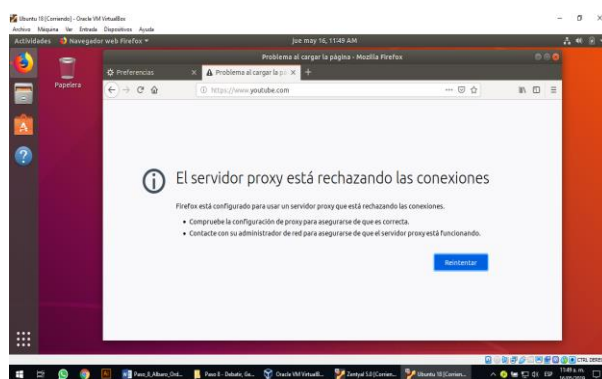


Fig. 34 Restricción de página

V. TEMÁTICA 3: CORTAFUEGOS

Para la presente temática se va a implementar la siguiente estructura.

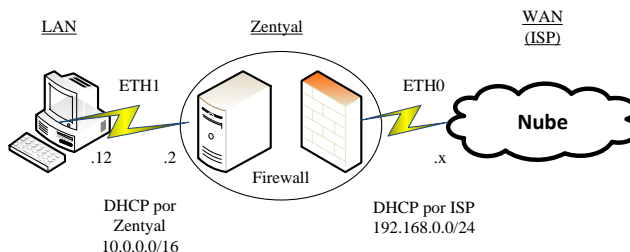


Fig. 35 Esquema de configuración del cortafuegos de Zentyal Server 5.0

Con esto se busca crear una puerta de enlace (Gateway) para gestionar las políticas de seguridad de acuerdo a las necesidades de la empresa objeto de estudio, con el direccionamiento IP indicado anteriormente.

Para lo anterior se proponen 3 pasos a cumplir que se resumirán en el presente apartado que son:

- Configurar de las tarjetas de red de la máquina virtual con Zentyal Server 5.0
- Realizar la restricción de los sitios web Facebook y Twitch.
- Verificar la restricción del cortafuegos desde el cliente Ubuntu Desktop 18.04 LTS.

El cortafuegos de Zentyal se basa en IPTables, la cual es la línea de comandos para la configuración de reglas de filtrado de paquetes de un sistema basado en GNU/Linux. Sin embargo, se posee una interfaz gráfica intuitiva que facilita la gestión de estas reglas y políticas según se requiera.

Se debe tener en cuenta las siguientes configuraciones para las tarjetas de red de la máquina virtual (Virtual Box).

A. Tarjeta de red 1 (WAN – ETH0)

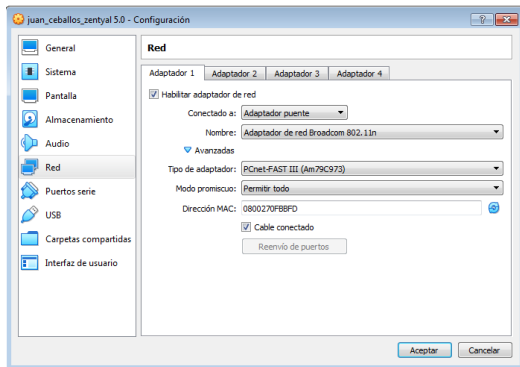


Fig. 36 Configuración de la tarjeta de red 1.

Esta tarjeta de red se va a encargar de la conexión entre Zentyal Server 5.0 y la WAN, la cual es suministrada por la ISP Claro

B. Tarjeta de red 2 (LAN – ETH1)

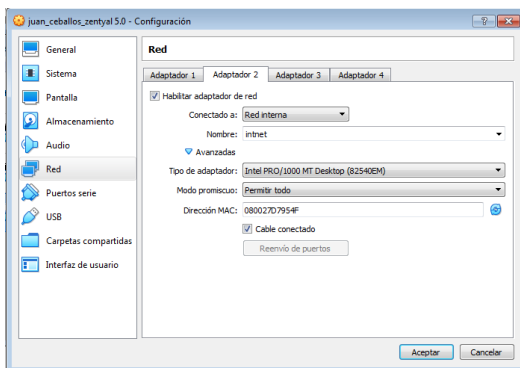


Fig. 37 Configuración de la tarjeta de red 2.

Esta tarjeta de red se va a encarga de la conexión entre los clientes LAN y Zentyal Server 5.0.

Una vez hecho esto, se debe iniciar la máquina virtual y hacer un ping a www.facebook.com y a www.twitch.tv para conocer la dirección IP de respuesta del servidor donde se alojan estas plataformas web. Se tienen las siguientes IP a la fecha:

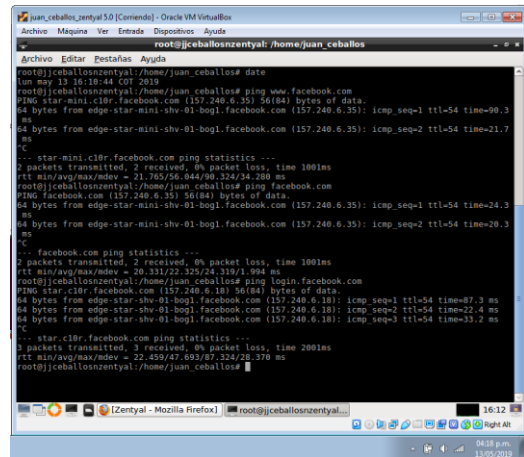


Fig. 38 Ejecución del comando ping a www.facebook.com.

Facebook: 157.240.6.35
Twitch: 151.101.6.167

Acto seguido, con la ayuda de la plataforma <http://whois.arin.net/ui/> se averigua el rango de IP para esas dos páginas web, en donde se arrojan los siguientes CIDR (Classless Inter-Domain Routing)

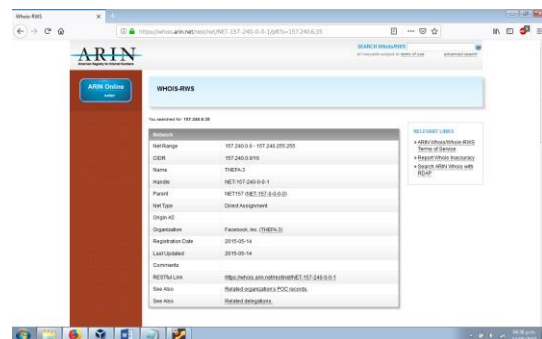


Fig. 39 Rango de IP para Facebook desde Whois.

CIDR Facebook: 157.240.0.0/16
CIDR Twitch: 151.101.0.0/16

Ahora se deben crear los objetos, a los que se asignarán los CIDR obtenidos anteriormente. Esto se hace en la ruta Red/Objetos/Añadir nuevo/a y posteriormente en agregar miembro.

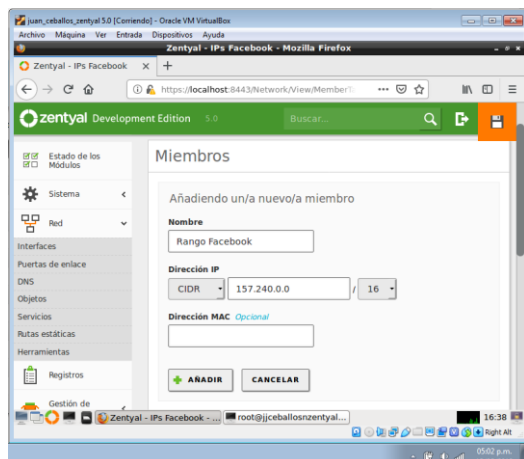


Fig. 40 Agregando miembro CIDR al objeto de Facebook.

Una vez hecho esto para las dos CIDR, se procede a crear las reglas para restringir los paquetes para estos rangos de IP y para habilitar el acceso a la WAN desde los clientes LAN. Se accede a la ruta Cortafuegos/Filtrado de paquetes/Reglas de filtrado para las redes internas/Añadir nuevo/a

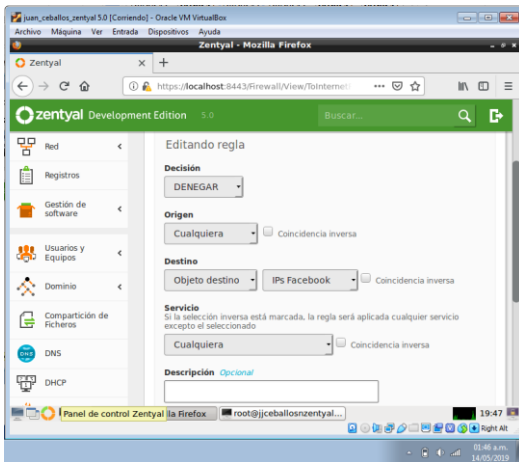


Fig. 41 Configuración de regla para restringir Facebook.

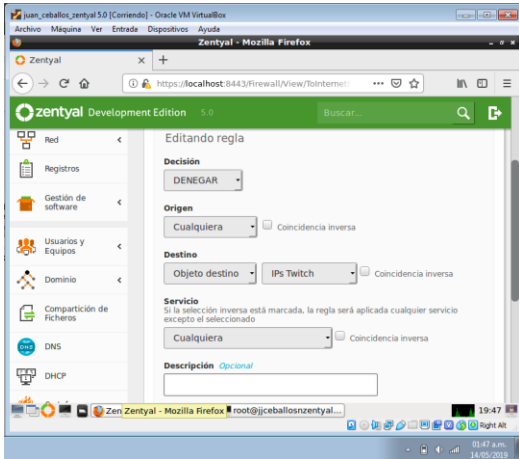


Fig. 42 Configuración de regla para restringir Twitch.

Se accede a la ruta Cortafuegos/Filtrado de paquetes/Desde redes externas hacia Zentyal/Añadir nuevo/a

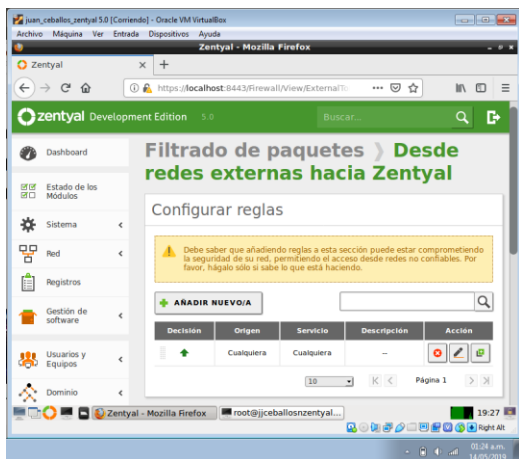


Fig. 43 Configuración de regla para habilitar la WAN en los clientes.

Finalmente, solo resta verificar la restricción de los sitios web

accediendo desde un cliente LAN Ubuntu Desktop 18.04 LTS con la siguiente configuración de la tarjeta de red en la máquina virtual:

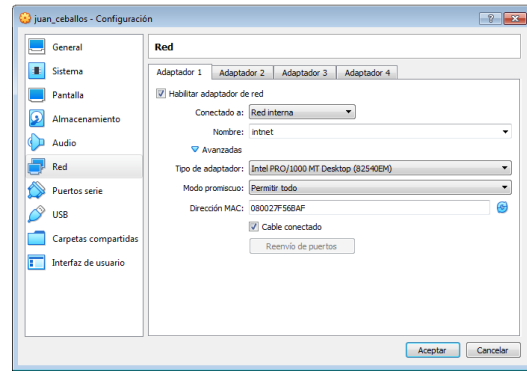


Fig. 44 Configuración de la tarjeta de red del cliente LAN.

Se inicia el sistema operativo y al intentar acceder a la página correspondiente, el firewall lo bloquea como se evidencia a continuación:

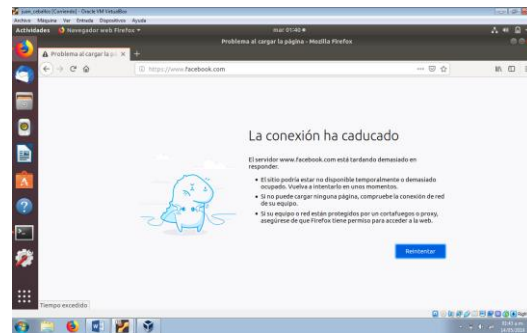


Fig. 45 Configuración de la tarjeta de red del cliente LAN.

Al intentar ingresar a la página web www.facebook.com se evidencia el cortafuego impide su acceso, de esta forma se evidencia el correcto funcionamiento del servidor.

VI. TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Después de haber instalado Zentyal en la máquina virtual se instalan los controladores y los paquetes requeridos para poder desarrollar la actividad y encontrando un perfecto funcionamiento de los paquetes instalados, ingresando al <https://localhost:8443> y seguidamente se ingresa con el usuario y contraseña.

Para la instalación de los paquetes se ingresa por gestión de servicio – componentes de Zentyal, se selecciona los paquetes que se desean instalar y por último se instalan.



Fig. 46 Instalación de componentes

Se habilitan los protocolos LDAP son las siglas de Lightweight Directory Access Protocol que hace referencia a un protocolo nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en u entorno de red.

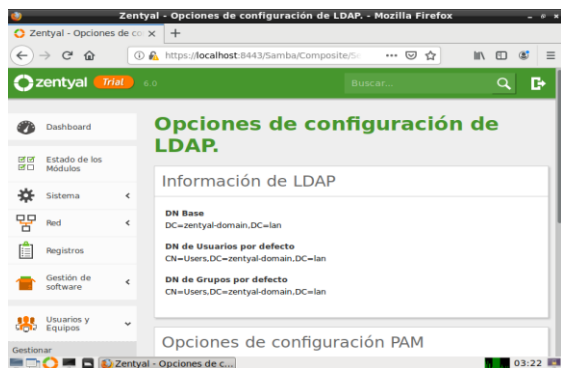


Fig. 47 Protocolo LDAP.

Se crea un directorio compartido desde la consola con el comando `sudo mkdir compartidas`.

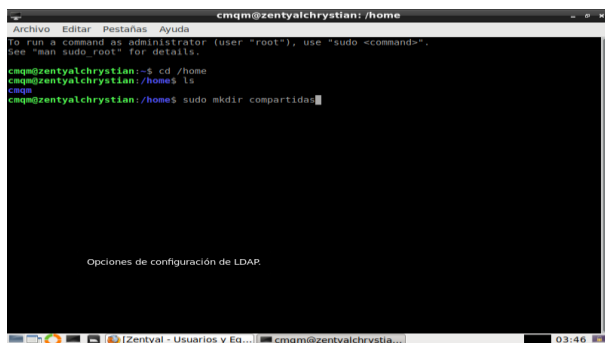


Fig. 48 Ejecución del comando `sudo mkdir compartidas`

Se agregan los usuarios por medio de usuario y equipos – gestionar – users – añadir nuevo/a en los campos disponibles para diligenciar el usuario y contraseña.

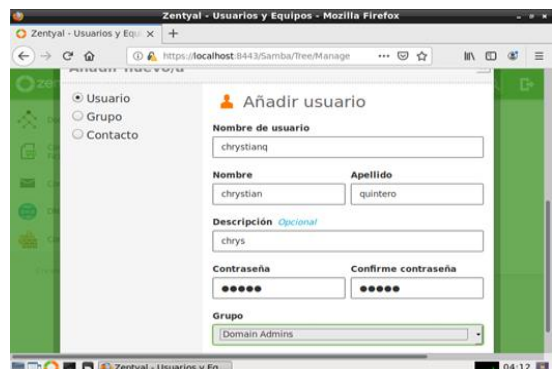


Fig. 49 Añadir Usuario.

Para la configuración de la impresora se realiza por la terminal usando el comando `sudo apt-get install cups`.

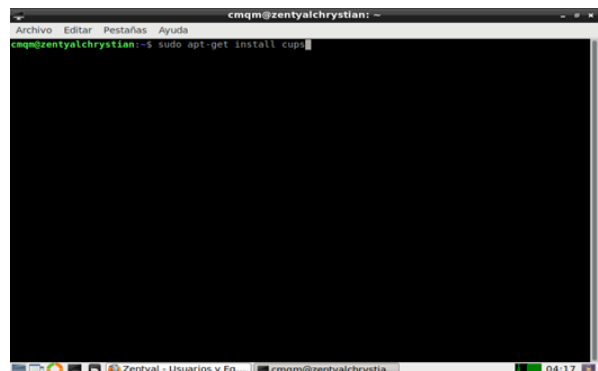


Fig. 50 Instalación impresora Cups.

Instalación de impresora cups-pdf con el comando `sudo apt-get install cups-pdf`

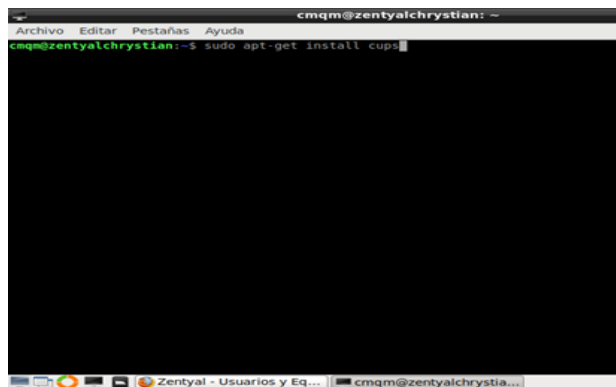


Fig. 51 Instalación impresora Cups-pdf.

Después de estar instalados desde la terminal ingresamos desde el navegador a la dirección `https://localhost:631` y desde administrador se configura la impresora que se desee compartir.



Fig. 52 Administración configuración de impresora.

Compartir archivos desde Zentyal al Sistema operativo Windows se configura desde compartición de ficheros donde se añaden los usuarios que desea compartir de igual manera se le dan los permisos que desean que tenga el archivo.



Fig. 53 Compartición de ficheros.

Configuración desde el sistema operativo Windows para compartir archivos.

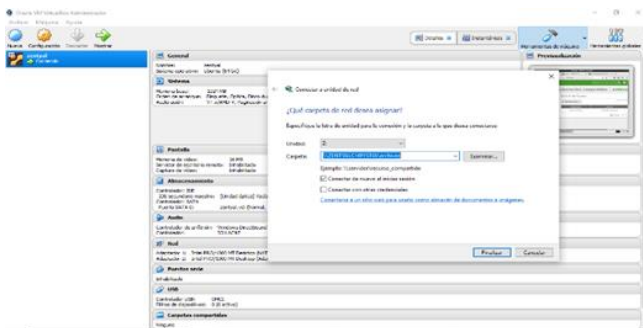


Fig. 54 Configuración compartir archivos

Configurado los archivos dentro del explorador de archivos desde Windows.

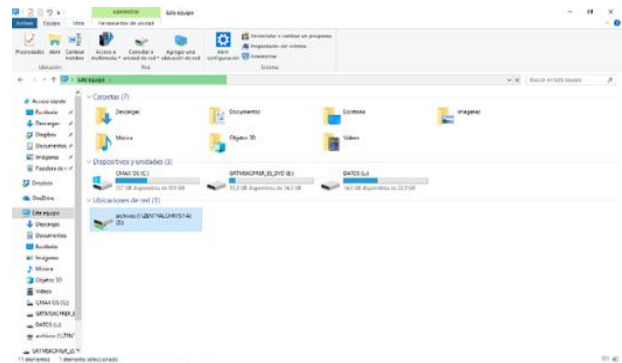


Fig. 55 Administrador de archivos.

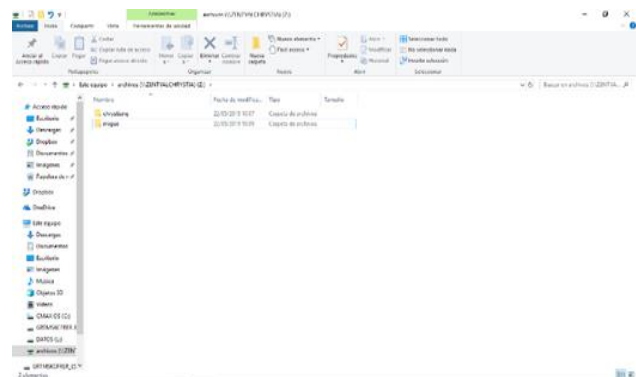


Fig. 56 Carpetas agregadas desde el archivo de Windows.

VII. TEMÁTICA 5: VPN

Las redes privadas virtuales tienen como finalidad permitir el acceso a las intranets a usuarios remotos a través de la Internet así como conectar de manera segura subredes distintas a través de redes no seguras. Es muy común que nuestros usuarios necesiten acceder a recursos de nuestra intranet, mientras se encuentran fuera de las instalaciones de la empresa, Es un caso habitual para comerciales o tele trabajadores, por poner un ejemplo. La solución pasa por permitir la conexión de estos usuarios a nuestras instalaciones a través de redes privadas virtuales que aseguran la confidencialidad de las comunicaciones

Usando una red privada virtual o VPN, (Virtual Private Network, de sus siglas en inglés), podemos crear un túnel seguro que sólo aceptará conexiones que provengan de usuarios autorizados. El tráfico viaja encapsulado y sólo es posible leerlo en el otro extremo del túnel. Para facilitar su uso y configuración, las conexiones aparecen como si estuviesen dentro de las redes internas, aprovechando así todos los recursos y configuraciones dispuestas por el administrador de sistemas para la red local.

He decidido conectarme por SSH desde mi maquina Windows al servidor ZENTYAL ya que me facilita más el trabajo de las fotografías, estoy en red local mi IP de Windows es 192.168.1.70 y la del servidor es 192.168.1.64

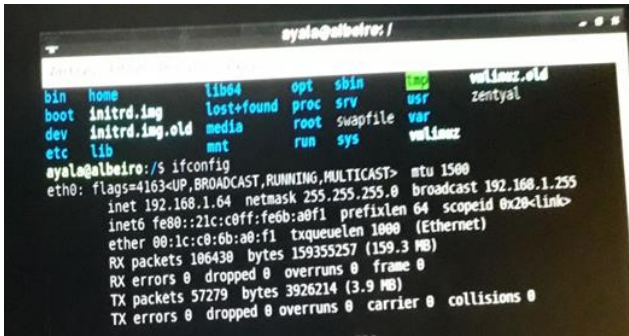


Fig. 57 Configuración de IP del servidor

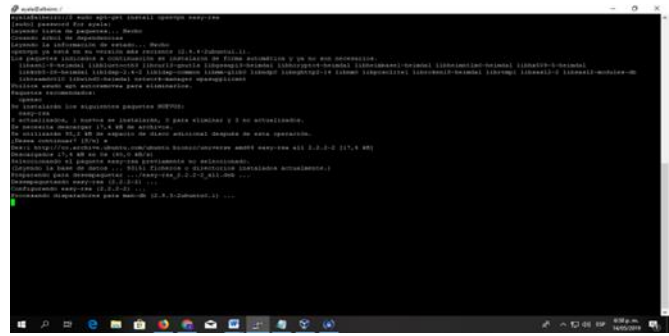


Fig. 59 Generación de llaves públicas y privadas.

A. Pasos para crear una conexión VPN con Zentyal

- Descargar e instalar Openvpn en Zentyal
- Crear los certificados de autoridad
- Crear las llaves públicas y privadas para el servidor
- Configurar el archivo server.config
- Crear certificados firmados para el clientes que se conectara, y de una vez lo obtendremos firmados. Para nuestro caso será user1
- Descargar los archivos de llaves públicas y privadas de user1 en USB y llevarlos a la maquina cliente
- Revisar si crea la interfaz de túnel en Zentical con ifconfig.
- Instalar en la maquina cliente Openvpn descargar de su página principal
- Copiar en la carpeta los archivos de la memoria USB para las llaves públicas y privadas junto con el certificados
- Configurar el archivo client.ovpn
- Conectar con Zentyal
- Si conecta, verificar con la IP asignada en el navegador

Generamos los parámetros Diffie Helman `./build-dh`

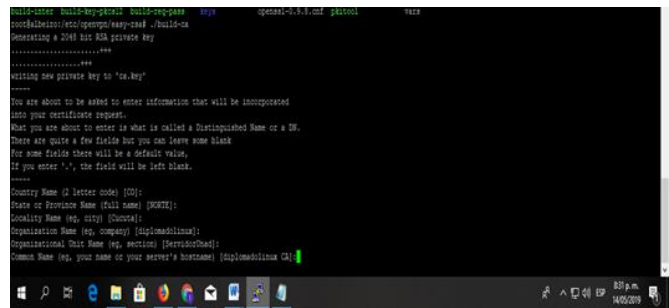


Fig. 60 Generación de los parámetros Diffie Heleman

Creación de claves para los clientes, lo hacemos acá por comodidad para este caso user1. `./build-key user1`

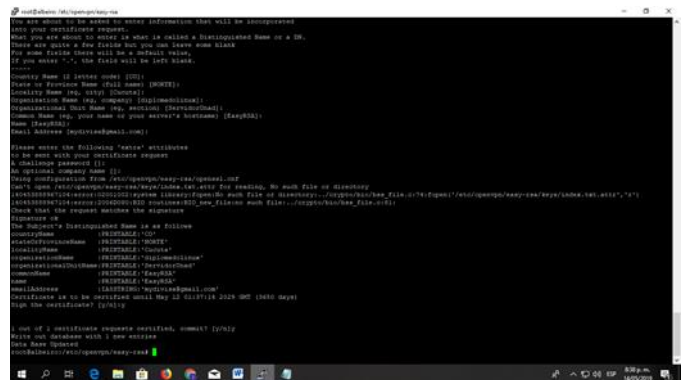


Fig. 61 Generación de claves usuarios

B. Instalación de Openvpn en el servidor Zentyal

`sudo apt-get install openvpn easy-rsa`

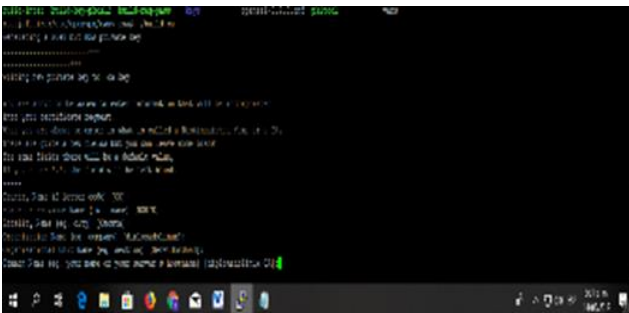


Fig. 58 Generación del certificado de autoridad para Zentyal.

Generamos las llaves públicas y privadas para el servidor. `./build-key-server server`.

Hecho esto crearemos en el directorio Openvpn el archivo `server.conf` Con `touch server.conf`

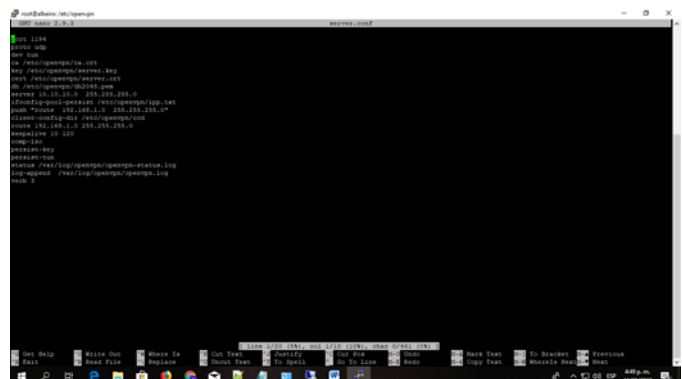


Fig. 62 Creación del archivo server.conf

Ya configurado corremos el daemon con: `/usr/sbin/openvpn --daemon --config /etc/openvpn/server.conf` y revisamos se creó la interfaces de tun0

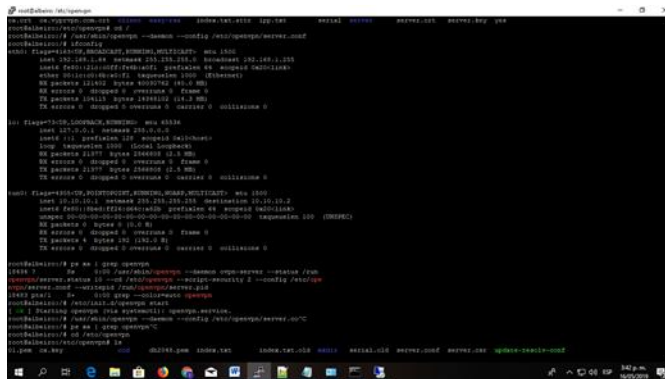


Fig. 63 Verificación de la creación del túnel

C. Configuración del cliente

Para este ejemplo lo haremos desde una maquina Windows descargamos desde <https://openvpn.net/community-downloads/>, después de la instalación del aplicativo. Iré a la configuración del archivo cliente VPN, para hacer el respectivo ajuste, utilizare las claves públicas y privadas que genera en Zentyal, para poder ingresar al servidor Zentyal desde el cliente

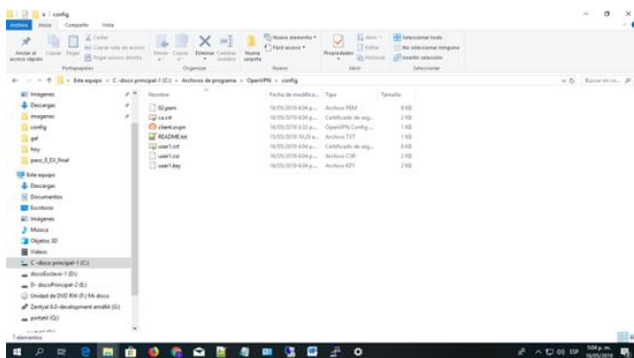


Fig. 64 Configuración del cliente en Windows

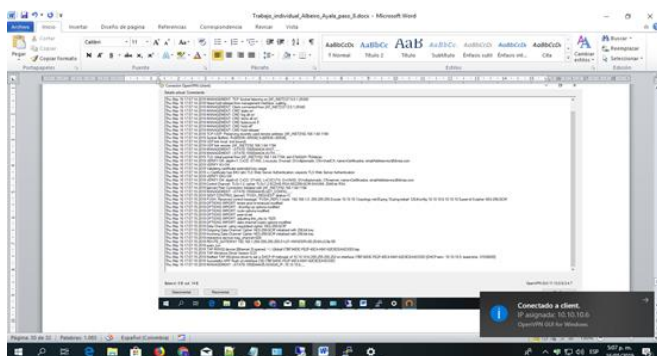


Fig. 65 Conexión establecida por medio de VPN

VIII.CONCLUSIONES

Al desarrollar esta práctica, se logró adquirir más conocimientos

acerca de los servidores y servicios que puede brindar un sistema como Zentyal; con este servidor es posible bloquear de manera eficaz el acceso a máquinas no autorizadas y mantener un control absoluto sobre la red.

Con un servidor DHCP es posible realizar una conexión de red privada entre varios computadores.

Con esta práctica se afianzaron conocimientos que pueden ser de mucha ayuda en la vida diaria puesto que la necesidad de control sobre la red es indispensable en cualquier empresa.

Zentyal Server es uno de los sistemas más completos y fáciles de manejar de los que se manejan en todo el proceso de práctica el diplomado, puesto que cuenta con todas las opciones de seguridad y control que se pueden necesitar en una red interna.

RECONOCIMIENTOS

No existen palabras suficientes para decirle a tantas personas que están a nuestro lado lo agradecidos que estamos por apoyarnos, compartir y sobre todo en confiar en que si podíamos culminar nuestros estudios. Gracias a nuestros tutores por su tiempo dedicado en evaluar cada trabajo presentado y por sus sugerencias las cuales nos permitieron mejorar cada vez más. Mil y mil gracias.

REFERENCIAS

- [1] Instalación y configuración de Zentyal, Zentyal wiki, comunidad zentyal, documentación, Recuperado de: <https://wiki.zentyal.org/wiki/Es/5.0/Instalacion#el-instalador-de-zentyal>.
- [2] JKnowITFree. How to join Ubuntu 16.04 LTS to Active Directory Created in zentyal 4.2 Server. [En línea]. Disponible en: <https://www.youtube.com/watch?v=oNCzh3dkdBM&t=102s>
- [3] ISO, https://es.osdn.net/frs/g_redir.php?m=kent&f=zentyal%2FOld+versions%2Fzentyal-5.0-development-amd64.iso
- [4] Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.0. (s.f.). Recuperado 22 mayo, 2019, de <https://doc.zentyal.org/es/directory.html>
- [5] Mora, A. (2017). Instalación Zentyal 5.0. [Online]. Available: <https://www.youtube.com/watch?v=5N9upYznnCo>
- [6] Velasquez, D. (2016). Firewall con Zentyal-UMG[Online]. Available: <https://www.youtube.com/watch?v=XPu5Nmh2rZg>
- [7] Zentyal Community (2017). En/5.0/Zentyal 5.0 Official Documentation [Online]. Available: https://wiki.zentyal.org/wiki/En/5.0/Zentyal_5.0_Official_Documentation
- [8] Zentyal Community (2017). Es/5.0/Cortafuegos Documentation [Online]. Available: <https://wiki.zentyal.org/wiki/Es/5.0/Cortafuegos#configuracion-de-un-cortafuegos-con-zentyal>