IMPLEMENTACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER PARA LA ASIGNACIÓN DE SERVICIOS

Anyerina Paola Cabarcas Diaz
e-mail: apcabarcasd@unadvirtual.edu.co
Edwin Rafael Marquez Melendez
e-mail: ermarquezm@unadvirtual.edu.co
Galo Jose Munoz
e-mail: gjmunozma@unadvirtual.edu.co
Jhon Jairo Montoya Moreno
e-mail: jjmontoyamo@unadvirtual.edu.co
Yurani Andrea Rativa
e-mail: yarativab@unadvirtual.edu.co

RESUMEN: *El documento contempla cinco temáticas con la cuales se busca establecer servicios de infraestructura IT direccionados a medios Internos y Externos (Intranet, Extranet) todo bajo la plataforma de Zentyal en su versión 6.2 quien nos provee diversas herramientas que permiten gestionar diversos componentes de seguridad y control aplicados en el campo de la informática bajo el ambiente de sistema operativo GNU/Linux.*

PALABRAS CLAVE: Servidor, interfaz, DHCP, Proxy, DNS.

1 INTRODUCCIÓN

Zentyal Server es una plataforma basada en GNU/ Linux la cual se puede ejecutar desde la Web, posee características de servidor desde de donde podemos se puede suministrar diversos servicios y red que permite fortalecer las plataformas informáticas.

2 INSTALACION DE ZENTYAL SERVER

2.1 REQUISITOS

Zentyal Server se puede ejecutar bajo las siguientes especificaciones mínimas de Hardware.
2 GB en RAM, 8 GB de Disco Duro espaciamiento procesador doble núcleo, tarjetas de red para la configuración de la red interna y la red externa.

2.2 PASO A PASO DE LA INSTALACIÓN DE ZENTYAL SERVER 6.2 DESDE UNA MÁQUINA VIRTUAL (VIRTUAL BOX)

La iso de zentyal server puede ser descargada desde el siguiente enlace:
https://download02.public.zentyal.com/zentyal-6.2-development-amd64.iso.

Se inicia configurando las especificaciones como memoria RAM a utilizar, espacio en disco duro, configuración de interfaces. se inicao desde la iso previamente descargada la cual contiene los instaladores de Zentyal Server, ver en la Figura 1.

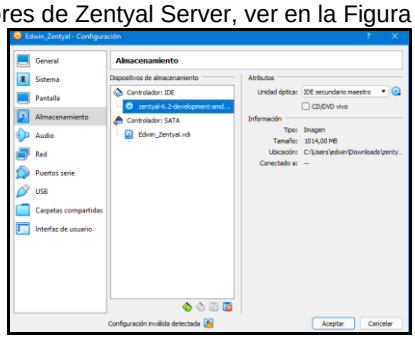

Figura 1. Elección de la iso de Zentyal server

En la Figura 2 podemos evidenciar la opción a seleccionar durante el proceso de instalación de zentyal server en virtual box cuando se nos pregunta el tipo de instalación que vamos a realizar

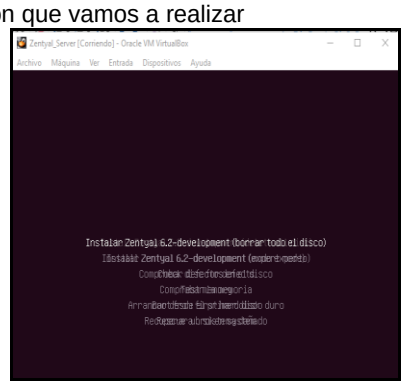

Figura 2. Instalación de zentyal server

Al seleccionar el modo de instalación del Zentyal y configurar la zona horaria, se comenzará con la instalación de los componentes adicionales, como podemos observar en la Figura 3.

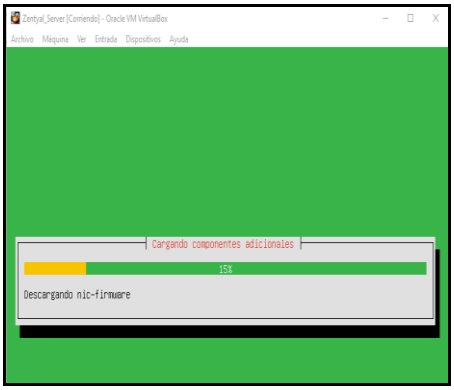

Figura 3. Instalación componentes adicionales

Automaticamente se iniciara la configuración de red, ver en la Figura 4.

Figura 4. *configuracion del DHCP para la Red*

Asignamos un nombre a la máquina para ser identificada por la red, ver en la Figura 5.

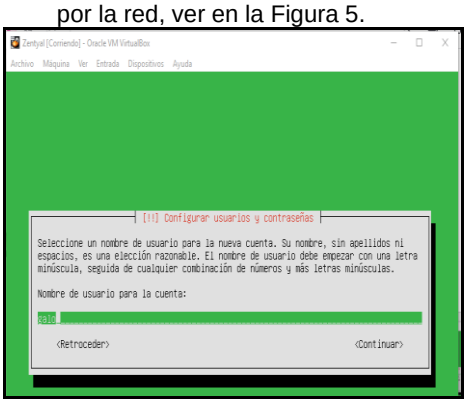

Figura 5. Asignación de usuario

Una vez terminada la instalación se procede automáticamente a instalar los paquetes necesarios para iniciar el sistema, ver en la Figura 6.

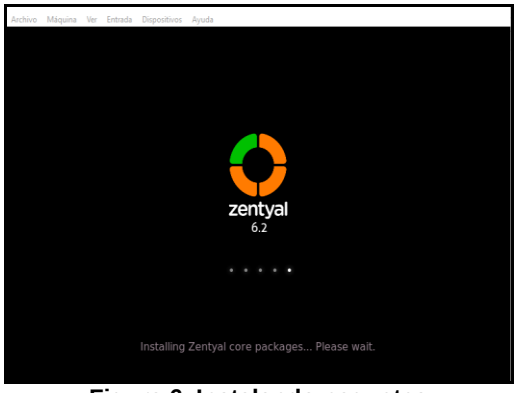

Figura 6. Instalando paquetes

Una vez terminada la instalacion de los paquetes necesarios como observamos en la Figura 7, se inicializa el sistema de Zentyal server.

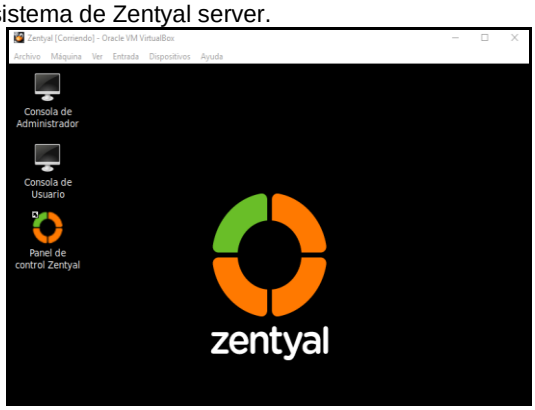

Figura 7. *escritorio de Zentyal Server*

3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Comenzamos seleccionando la opción **DHCP** dentro de la dashboard de Zential server, como se observa en la Figura 8.

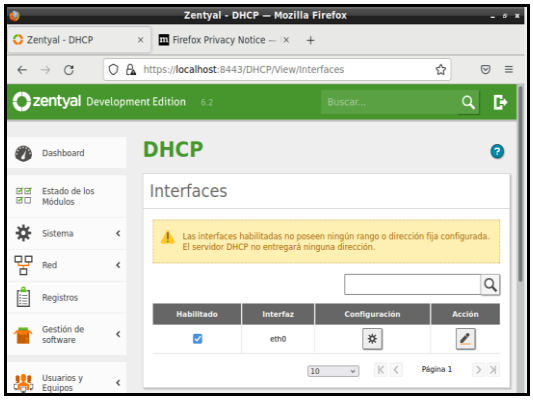

Figura 8. Inicio de instalación de los servicios DHCP

En la figura 9 podemos observar la configuración de la dirección IP como puerta de enlace predeterminada.

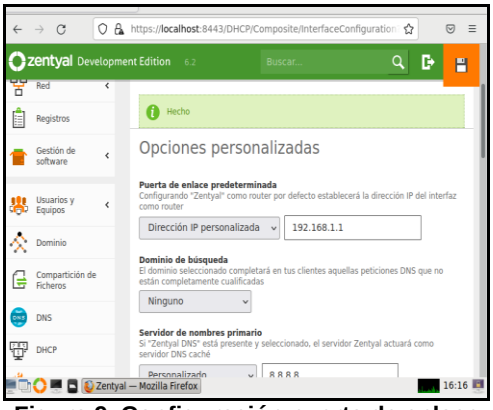

Figura 9. Configuración puerta de enlace predeterminada

Posterior a la configuración de la dirección IP, procedemos a configurar el rango de direcciones Ip, como podemos ver en la Figura 10.

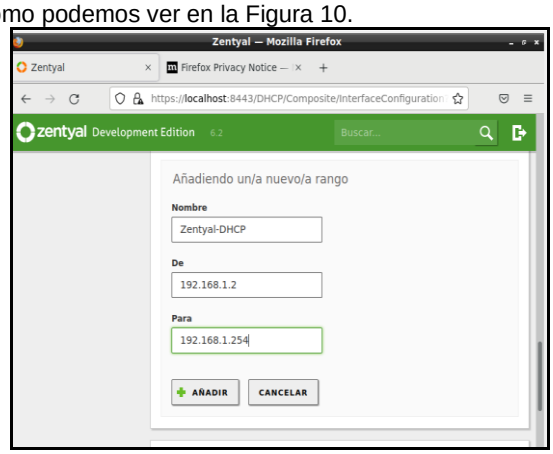

Figura 10. Rangos de IP disponibles

Comprobamos las asignaciones de direcciones IP por medio de DHCP en un cliente desktop, ver en la Figura 11.

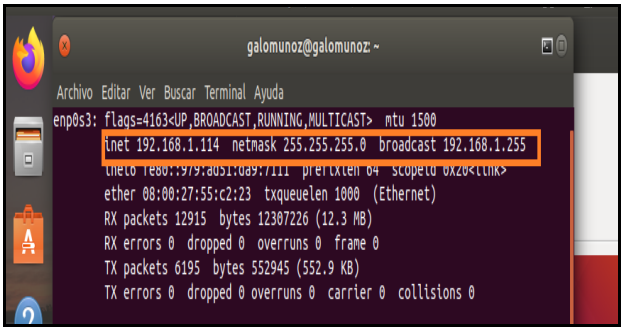

Figura 11. *Comprobamos ip establecida en cliente por medio de consola*

También podemos utilizar el entorno grafico del cliente Desktop para comprobar las direcciones IP asignadas, ver en la Figura 12.

Figura 12. *Comprobando ip en usuario Desktop en el entorno grafico*

3.1 INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS DNS EN ZENTYAL SERVER.

Configurando DNS Server con Zentyal en esta opción no permite ver que servidor está resolviendo nuestro DNS por lo tanto seleccionamos **Zentyal-domain.lan**, como observamos en la Figura 13.

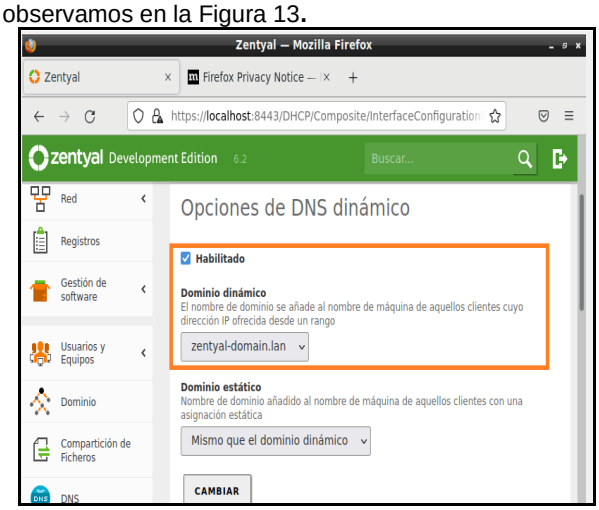

Figura 13. *Habilitando el dominio dinamico*

Comprobamos el servidor DNS que está operando en nuestra RED utilizando el comado **NSLOOKUP**, sobre la direccion web de Google (www.google.com) traduciendo la pagina IP, ver en la Figura 14.

Figura 14. *comprobando dominio con nslookup*

3.2 CONTROLADOR DE DOMINIO

Esto traduce que Zentyal administrará, en el menú sistemas seleccionamos general donde colocamos el nombre del dominio para nuestro caso **Zentyal-domain.lan**, ver en la Figura 15.

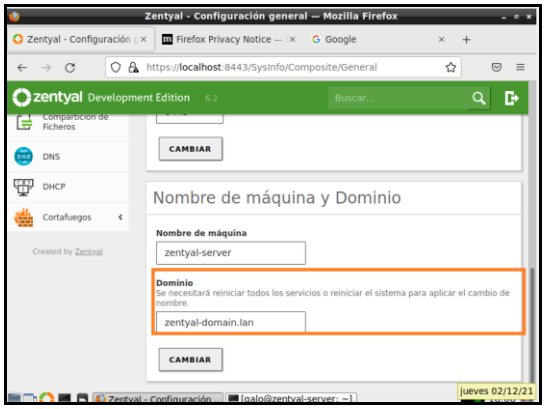

Figura 15. Configurando el nombre de maquina y dominio

Procedemos a verificar que zentyal es nuestro controlador de dominios, ver en la Figura 16.

Figura 16 Comprobación del dominio

Una vez comprobado el dominio, como observamos en la Figura 17, vamos a verificar que los usuarios y equipos se encuentran unidos a nuestro dominio.

Figura 17. *usuarios y equipos del dominio*

Finalmente creamos un usuario administrador, dentro de la opción de usuarios y equipos de Zentyal, ver en la Figura 18.

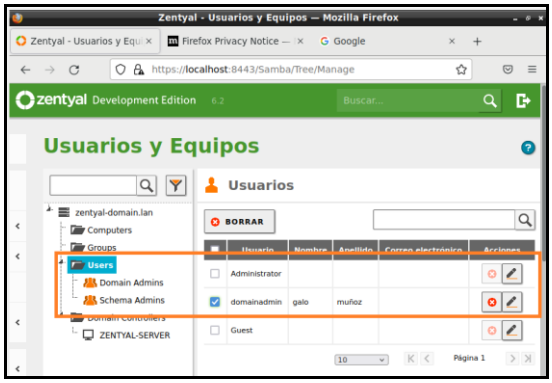

Figura 18. Usuario administrador

4 PROXY NO TRANSPARENTE

Una vez instalamos el sistema operativo de Zentyal, procedemos con la descarga de paquetes necesarios para la implementación:
Domain controller and file sharing, DHCP server y HTTP proxy, ver Figura 19**.**

Figura 19. Instalación de paquetes Domain controller and file sharing, DHCP server y HTTP proxy

Posterior se nos solicita confirmar la descarga de los paquetes seleccionados, ver Figura 20.

Figura 20. Confirmación de paquetes a instalar

Una vez finalizamos de instalar todos los paquetes, como podemos observar en la Figura 21, procedemos a configurar cada una de las interfaces de red: **eth0** definida como red interna y la **eth1** la cual definimos como externa.

Figura 21. Configuración inicial

Posterior configuramos la IP y la máscara de red, ver en la Figura 22.

Figura 22. Configuración de ip y mascara de red

Al finalizar la configuración de red tendremos un servidor del tipo Stand-alone y le asignamos un nombre al dominio. **diplomadolinux.net**, ver Figura 23.

Figura 23. Configuración stand-alone

Al seleccionar la opción de 'Finalizar', se descargarán de forma automática los cambios necesarios para la configuración, ver Figura 24

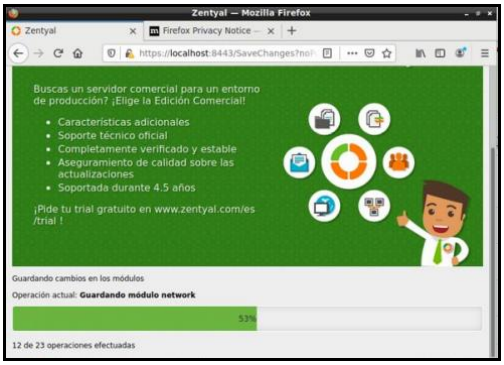

Figura 24. Instalación de la configuración del servidor

Al finalizar la instalación nos dirigimos al módulo de red en la opción eth0 y seleccionamos el check en (Externo WAN), ver Figura 25.

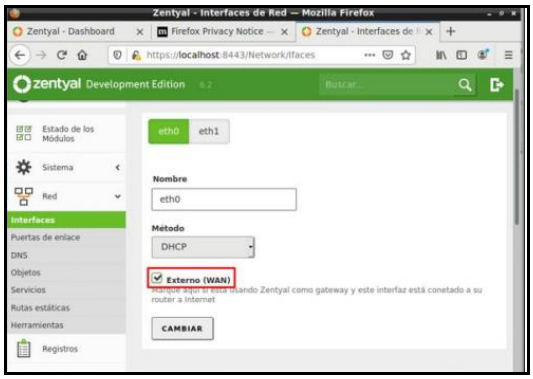

Figura 25. Selección del módulo de red

En la sección de red eth1 ingresamos la IP y la máscara de red, ver Figura 26.

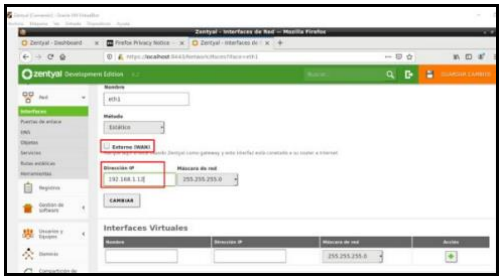

Figura 26. Ingreso de Ip y mascara de red

Creamos un nuevo miembro con el nombre de **ClientZentyal** con la IP apuntando al puerto 32 con el cual vamos a identificar todos los equipos que pertenecen a la red LAN, ver Figura 27.

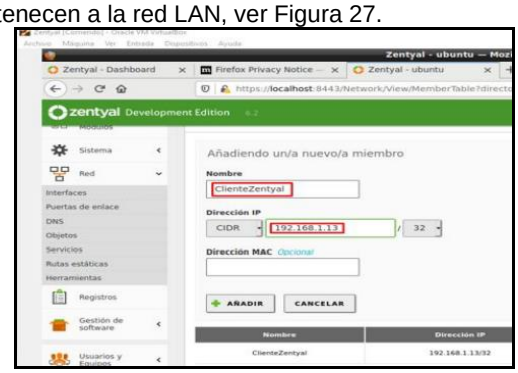

Figura 27. Creación de un nuevo miembro de cliente

En la opción de configuración general, ingresamos el puerto 1230, ver Figura 28.

Figura 28. Configuración general del proxy

Dentro de las reglas de acceso, seleccionamos la red creada anteriormente y seleccionamos la opción de denegar todo, ver Figura 29.

Figura 29. Reglas de acceso

Inicializamos el cliente desktop y configuramos manualmente el proxy y el puerto en el navegado, ver Figura 30.

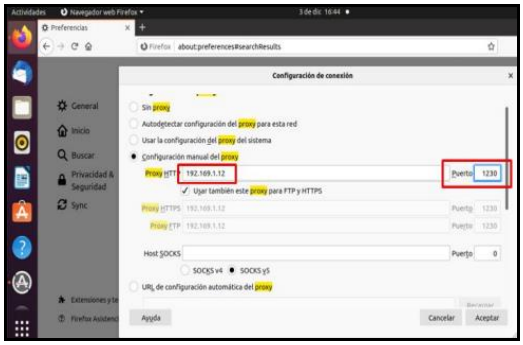

Figura 30. Configuración de proxy y puerto en el navegador

Procedemos a verificar que funciona la configuración realizada intentando acceder a la página de www.youtube.com, desde una estación cliente y se evidencia que por la configuración realizada al servidor Zentyal no se permite el acceso, ver Figura 31.

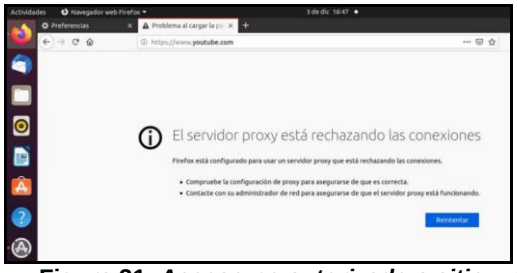

Figura 31. *Acceso no autorizado a sitio web*

Se muestra de manera explícita un mensaje de rechazo al cliente, ver Figura 32.

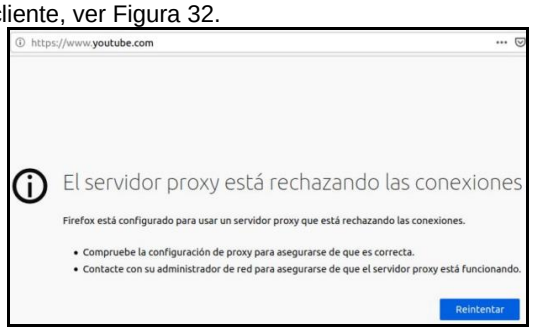

Figura 32. 39 mensaje causa negación del acceso a la página.

5 CORTAFUEGOS

Con el fin de realizar la implementación del cortafuegos a través del servidor zentyal, se realiza la instalación del módulo "*firewall"*, con el cual se busca realizar la creación de políticas o reglas para la restricción de acceso a sitios o portales web de entretenimiento y redes sociales, ver Figura 33.

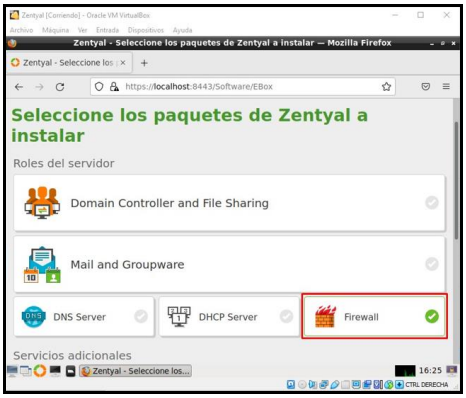

Figura 33. Instalación de módulo Firewall.

Es importante recalcar que al realizar la instalación de cualquier módulo de zentyal, este debe habilitarse para que sean aplicadas las configuraciones realizadas en el servidor, ver Figura 34.

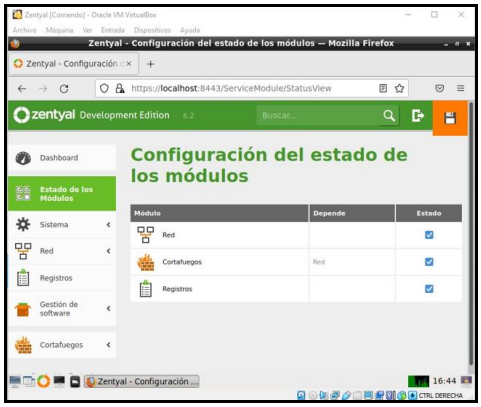

Figura 34. Habilitación de módulos instalados.

Uno de los puntos más importantes al momento de realizar una implementación de un servicio como lo es el firewall, es la creación de redes tanto internas (lan) como externas (wan) que serán administradas, definiendo un direccionamiento a través de una segmentación de Ips específicas para cada una de ellas, así como tambien la puerta de enlace y servidor DNS, las cuales nos permitirán establecer una conexión, ver Figura 35.

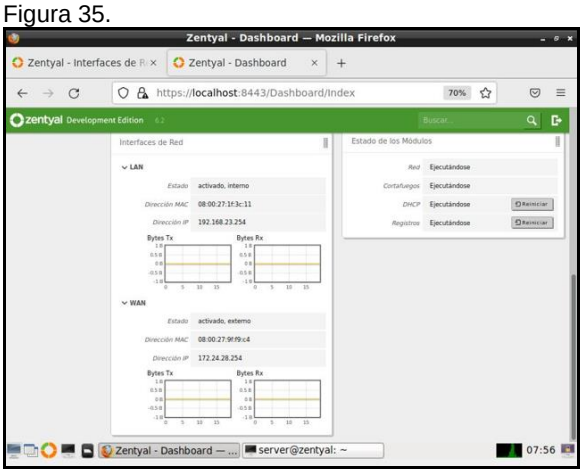

Figura 35. Creación y definición de un direccionamiento de red Lan y Wan.

Con el fin de generar una administración adecuada en las redes que fueron creadas, zentyal permite realizar la creación de "*objetos de red*", los cuales permitirán definir a través de grupos usuarios específicos de red específicos, así como también un rango de direcciones, ver Figura 36.

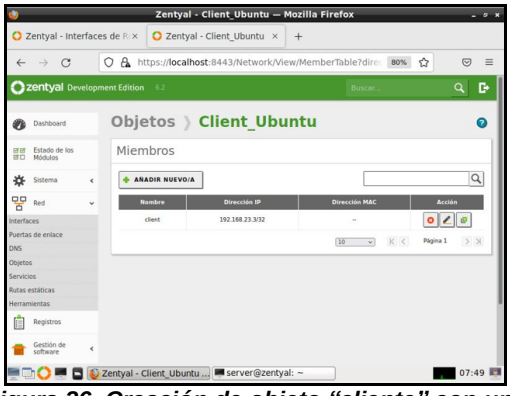

***Figura 36. Creación de objeto "cliente" con una dirección ip especifica*.**

Realizada las configuraciones iniciales en el servidor zentyal, procedemos a ingresar a nuestro equipo "*cliente*" con una dirección ip ya definida y como puerta de enlace la direccion ip que fue establecida para nuestra red lan en el servidor zentyal con el fin de lograr una conexión de red lan, ver Figura 37.

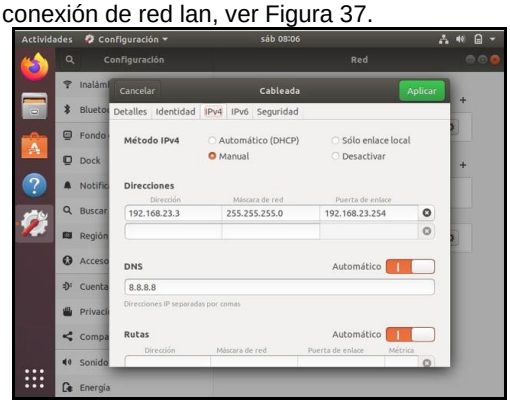

Figura 37. Se establece un direccionamiento ip fijo en la maquina cliente.

Con el fin de verificar la conexión de red de nuestro equipo cliente, realizamos una busqueda en navegador hacia la página www.facebook.com, así como tambien se realiza un ping en donde se evidencia la conexión establecida, ver Figura 38.

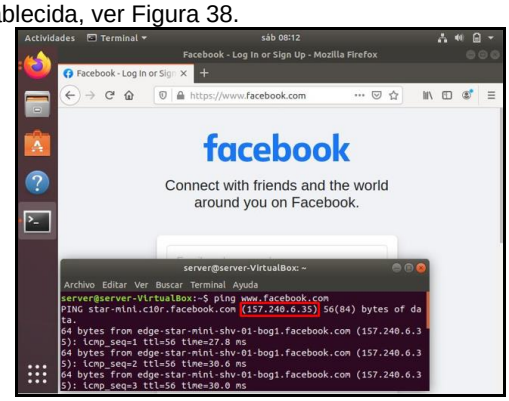

Figura 38. Verificación de conexión exitosa hacia la dirección web de Facebook.

Con el fin de conocer el segmento de red de la dirección ip de Facebook a través del ping realizado, se realizar

por medio de la página https://whois.arin.net/ui/ una búsqueda para conocer este segmento que será primordial para la creación de reglas en el firewall, ver Figura 39.

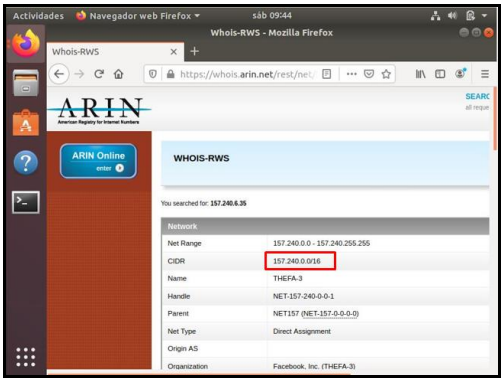

Figura 39. Verificación del segmento de red origen.

Así mismo realizamos una verificación de conectividad hacia la página www.youtube.com, al cual de igual forma se evidencia una acceso y respuesta de pin exitosa, ver Figura 40 y Figura 41.

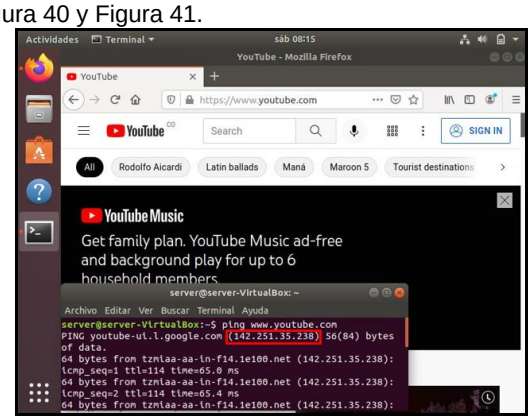

Figura 40. Verificación de conexión exitosa hacia la dirección web de facebook.

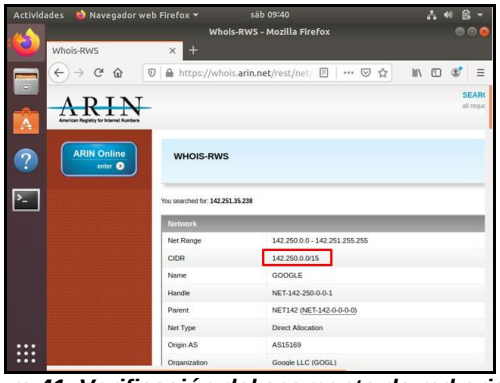

Figura 41. Verificación del segmento de red origen.

Al haber identificado de forma exitosa los segmentos origen de cada dirección ip que fue resulta a través una solicitud ICMP *(ping)* a las direcciones web ejemplo, se procede a realizar la creación de políticas o reglas con el fin de restringir el acceso y respuesta de estos sitios web, para ellos se realizara a través de Reglas de filtrado para las redes internas en el módulo de cortafuegos de zentyal, ver Figura 42.

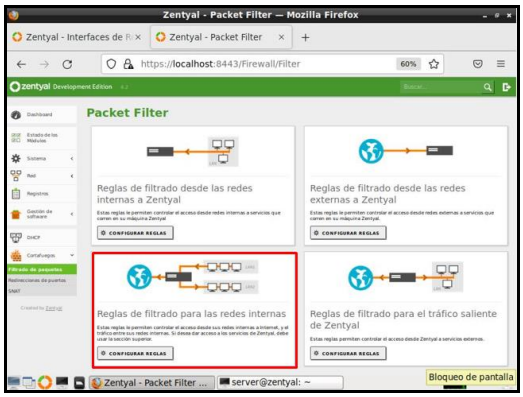

Figura 42. Modulos de creación de reglas en firewall de zentyal.

Se procede a realizar creación de regla de denegación de acceso desde el origen "*cliente_ubuntu*" creado previamente para establecer la dirección ip del equipo cliente, hacia la ip de destino del segmento de red origen de sitio web de Facebook, con el cual se realizará el bloqueo de todos los servicios de acceso y conexión, ver Figura 43.

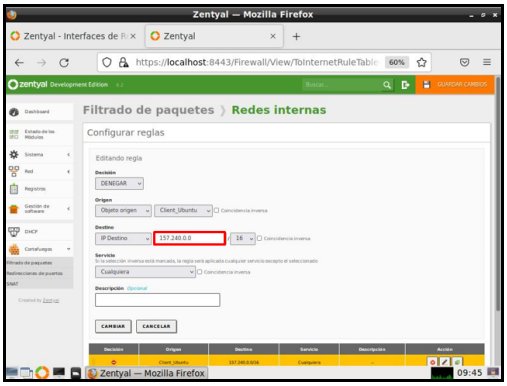

Figura 43. Creación de regla denegación de acceso o conexión.

De igual forma se realiza la creación de regla de denegación de acceso desde el origen "cliente_ubuntu", hacia la dirección ip de destino del segmento de red origen de sitio web de Youtube, ver Figura 44.

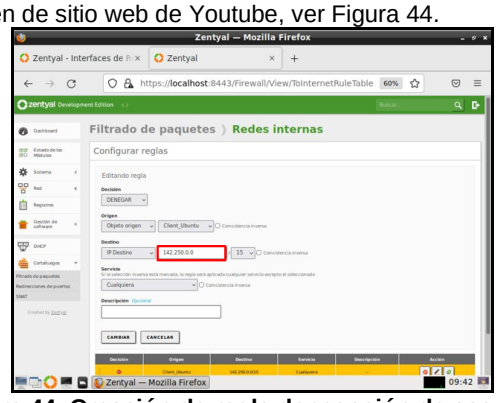

Figura 44. Creación de regla denegación de acceso o conexión.

Realizada la creación de reglas de denegación de acceso en el firewall, se realiza la verificación de conexión en nuestro equipo cliente, el cual se evidencia que no tiene conexión a la dirección del sitio web de YouTube y Facebook, así como también no tiene respuesta de ping, pero continúa permitiendo la conexión de red a otros sitios web, ver Figura 45.

Figura 45. Bloqueo de conexión a sitio web de Youtube y respuesta de ping

6 FILE SERVER Y PRINT SERVER

Para el desarrollo de la temática se realizó inicialmente la configuración y aprovisionamiento de un servidor zentyal el cual otorgará a la empresa de un sistema de archivos, sistema de directorio activo, sistema de DHCP, sistema DNS y un sistema de compartición de impresora lo cual será configurado para clientes tanto Linux como Windows en este proyecto se configuro una maquina cliente Linux para las pruebas, ver Figura 46 y Figura 47

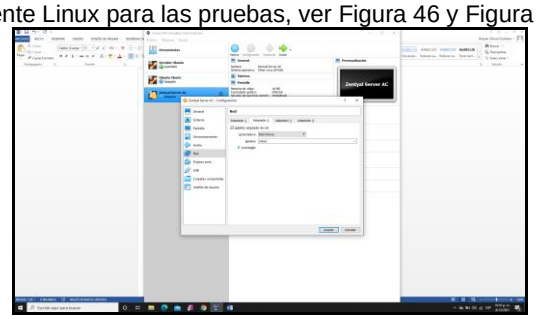

Figura 46. Configuración un servidor Zentyal

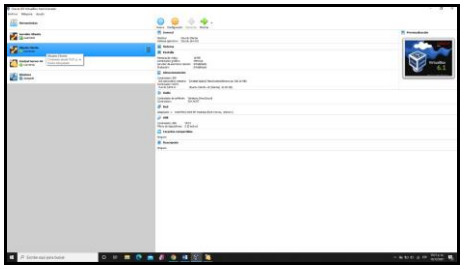

Figura 47. Configuración un cliente con Ubuntu 20.04

Al finalizar el aprovisionamiento nos dirige al dashboard damos click en estado de los módulos y seleccionamos los módulos que deseamos activar en nuestro caso son RED, DHCP, DNS NTP, Y DOMAIN CONTOLER.

6.1 FILE SERVER

Al finalizar la configuración anterior nos dirigimos al módulo de DHCP y verificamos las interfaces creadas y que rangos de IP están habilitados, damos click en la configuración de la interfaz eth1 como lo muestra la figura 27, Al dar clic nos redirige a esta ventana donde podemos configurar un Nuevo rango de ip para el dhcp de nuestra red interna damos añadir Nuevo en el apartado de Rangos como lo muestra en la figura xx, Digitamos un nombre y un rango de direcciones ip y damos añadir en nuestro caso nuestro segmento es 192.168.2.0/24 como lo muestra la figura 48, Figura 49, Figura 50 y Figura 51.

Figura 48. Modulo DHCP Interfaz eth1.

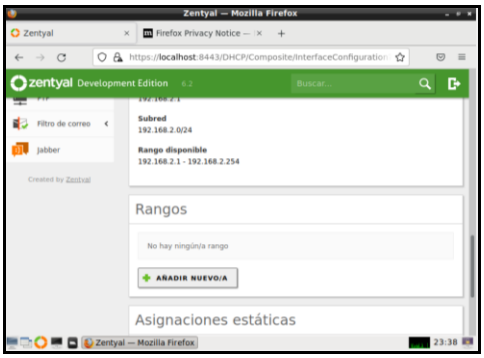

Figura 49. Localizar apartado de Rangos y boton añadir Nuevo

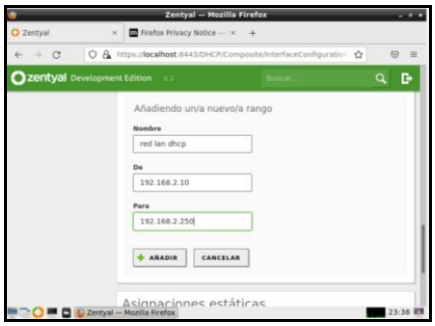

Figura 50 configuración del Rango IP

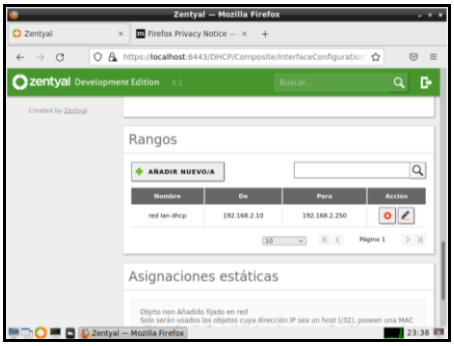

Figura 51 Resultado

Iniciamos sesión en nuestro sistema Ubuntu 20.04 Cliente y mediante el comando ifconfig verificamos que se le esté asignando una IP dentro del rango establecido, ver Figura 52

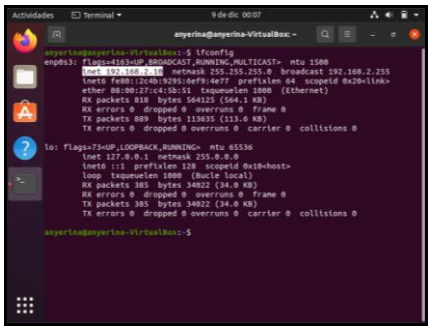

Figura 52. Direccionamiento IP

Verificamos comunicación con nuestro servidor zentyal por medio del comando ping, ver Figura 53.

Figura 53. Prueba de Conexión Servidor

Creamos un Grupo en la ruta Usuarios y Equipos > Gestionar seleccionamos la carpeta de Usuarios y Creamos un nuevo llamado lucas con los parámetros que nos exige el formulario damos añadir, ver Figura 54

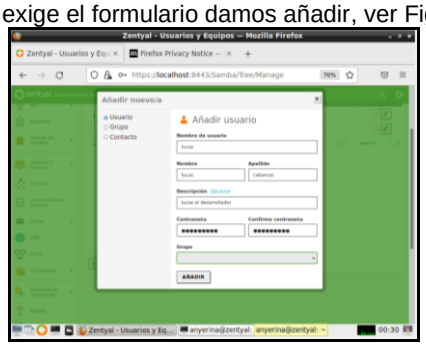

Figura 54. Creación de Usuario Domain Controller

Añadimos a lucas a nuestro grupo de Domain Admin dando click sobre estos Users y en el apartado de usuarios seleccionar a lucas y darle en el símbolo de más a un lado para añadirlo, ver Figura 55

Figura 55. Añadir a Usuario a grupo admin

Nos dirigimos a la opción de compartir ficheros > directorios compartidos y damos click en añadir uno nuevo, ver Figura 56

Figura 56. Ubicación Compartir Ficheros

Colocamos un nombre de recurso y como podra ser mapeado en el servidor en nuestro caso colocamos desarrolladores y un comentario damos añadir, ver Figura 57

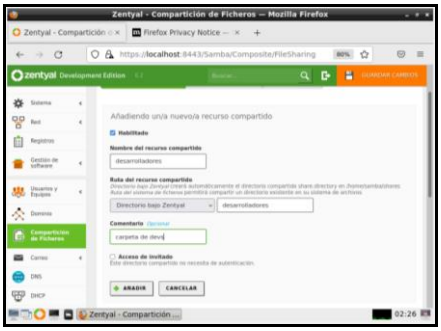

Figura 57. configuración de Carpeta Compartida

Verificamos la creación del recurso y damos click en control de acceso para añadir el acceso a este recurso compartido, ver Figura 58 y Figura 59.

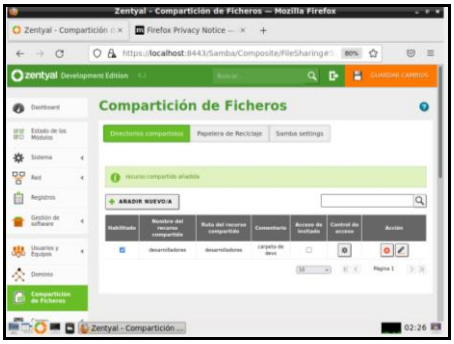

Figura 58. verificación de creación y Control de acceso

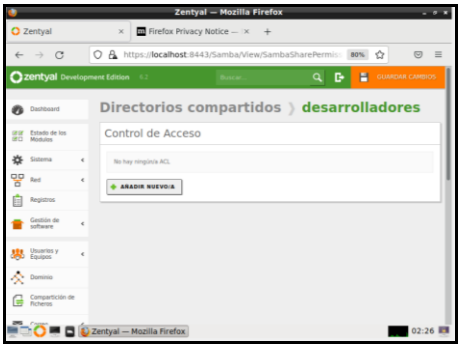

Figura 59 Añadir ACL

Buscamos por usuario a lucas y le damos permisos de escritura y lectura damos añadir y guardar en el botón de la esquina superior derecha Figura 39
Se debe ingresar con el usuario "cliente1" para comprobar el acceso al recurso y los permisos concedidos al grupo de usuarios, ver en la Figura 60.

Figura 60. Acceso a nuestro usuario a escritura y Lectura

Enlace de descarga de Script para la instalación del cliente por CLI que nos permitirá configurar nuestro dominio en la maquina cliente Ubuntu
Enlace: https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh

Asignamos permisos de ejecución al archive antes descargado con el comando chmod +x, ver Figura 61.

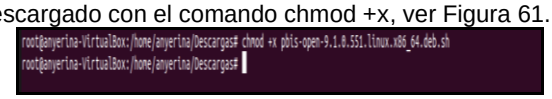

Figura 61. Permisos de ejecución archive descargado

Ejecutamos el archivo descargado con el comando ./pbis-open-9.1.0.551.linux.x86_64.deb.sh, ver Figura 62

Figura 62. Ejecución del archivo descargado

Añadimos nuestra maquina cliente con el siguiente comando al dominio de zentyal /opt/pbis/bin/domainjoin-cli join –disable ssh zentyal-domain.lan luca, la primera linea del comando es un ejecutable, desactiva el ssh y siguiente va nuestro dominio, que configuramos como controlador de dominio y nuestro usuario, luego de la ejecución del comando nos pide la contraseña de este usuario la colocamos y nos debería mostrar un mensaje de success, ver Figura 63.

Figura 63 Contraseña del usuario de Dominio y success

Aparece ya nuestro cliente ANYERINA-VIRTUALBOX en nuestra consola de administración, conectamos nuestra unidad de Red Compartida creada anteriormente, ver Figura 64

Figura 64 Conexión de unidad de red compartida

.

Se nos pide el usuario, nuestro dominio de zentyal y la contraseña creada como lo muestra la Figura 65.

Figura 65 Credenciales de acceso

Creación y Edición de un archive en el recurso compartido, ver Figura 66 y Figura 67.

Figura 66 Creación de Archivo

Figura 67. Edición de archivo

6.2 PRINT SERVER

Instalación de los paquetes necesarios para el funcionamiento de nuestro servidor para esto instalamos cups y sus dependencias, ver Figura 68.

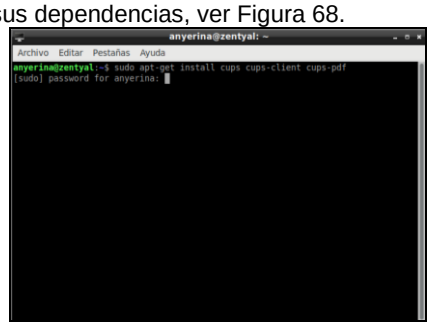

Figura 68 Instalación de cups y dependencias

Ingreso al sitio de administración de cups localhost:631, ver Figura 69

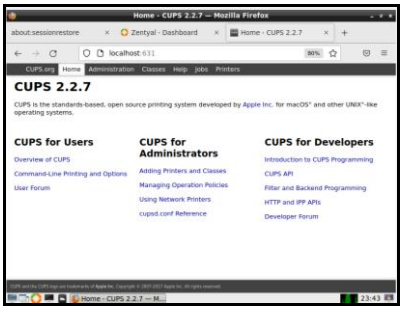

Figura 69. Administración de Cups

Añadir una nueva impresora en la ruta Administration>printers>add printer, ver Figura 70.

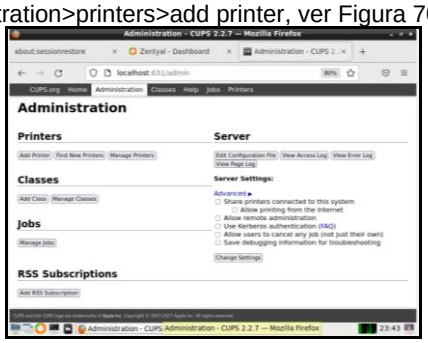

Figura 70 Opciones para añadir una nueva impresora

Tipo de impresora a instalar y asignación de nombre y una descripción dejamos por defectos los valores, ver Figura 71.

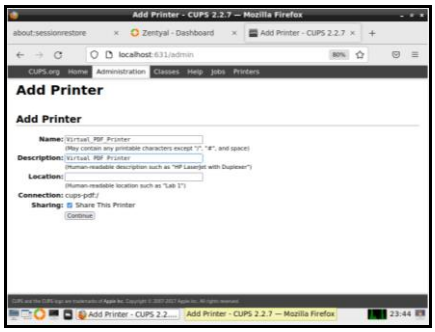

Figura 71 Asignación de nombres para impresora

Tipo de Controlador para la impresora seleccionamos genérico, asignamos del modelo tipo Genérico con opciones y colocamos la impresora antes creada como predeterminada en nuestro servidor con el commando lpoptions –d nombre de la impresora, ver Figura 72

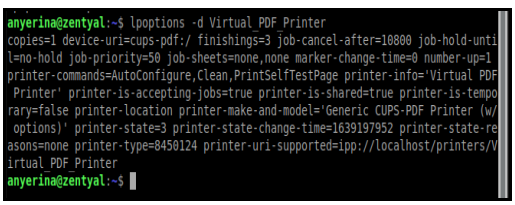

Figura 72. añadir impresora por defecto

Buscamos la impresora en nuestro cliente Ubuntu dando clic en configuración>impresoras>buscar impresoras

Figura XX, se da clic en el botón añadir y se configura en nuestro cliente, ver Figura 73 y Figura 74.

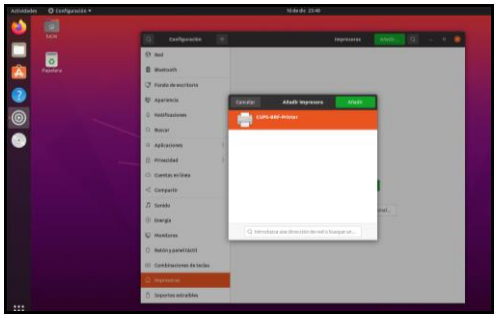

Figura 73 Buscar impresora configurada en nuestro server

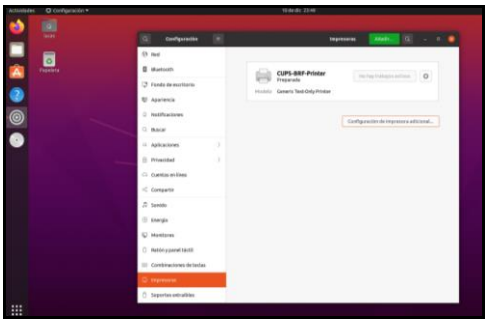

Figura 74 añadir impresora a nuestro cliente

7 VPN

Se puede configurar Zentyal con el fin de Implementar una VPN que nos permita una conexión segura a un entorno local incluso si estamos fuera de nuestra red o en una red pública.

Para configurar una VPN en Zentyal lo primero que necesitamos es crear una Autoridad de Certificación y certificados individuales para los clientes remotos que vamos a conectar a la VPN

Con el fin de crear un crear Autoridad de Certificación El sistema nos va a solicitar la información de este como muestra la siguiente ilustración, donde el Nombre de la organización y los días de expiración son obligatorios y los demás campos son opcionales, ver Figura 75.

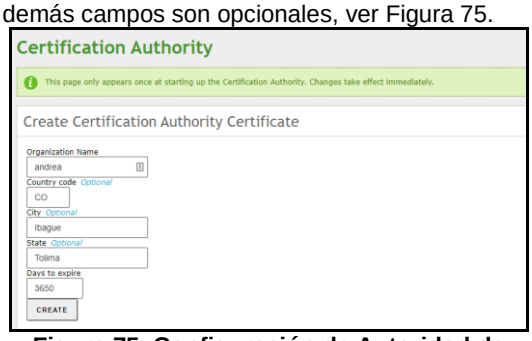

Figura 75. Configuración de Autoridad de Certificación

Una vez tenemos la Autoridad de Certificación y los certificados, debemos poner a punto el servidor VPN en Zentyal usando el botón Crear un nuevo servidor

Para configurar nuestro Nuevo servidor Agregamos un nombre y una vez creado nuestro servidor procedemos a configurar el servicio para ello Vamos a la pestaña servicios y creamos uno nuevo, ver Figura 76.

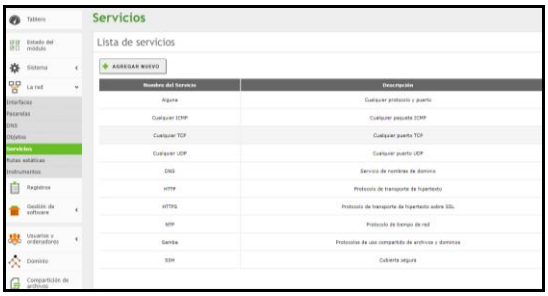

Figura 76. Vista de Servicios instalados

En el panel de Agregar servicio, digitamos el nombre del servicio y damos clic en “Agregar”, ver Figura 77.

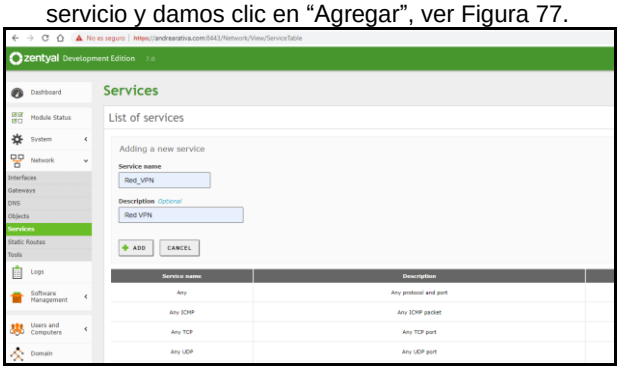

Figura 77. Vista del panel de Agregar Servicio

Posterior a su creación vamos a configurar nuestro nuevo servicio dando clic en el icono de configurar, ver Figura 78.

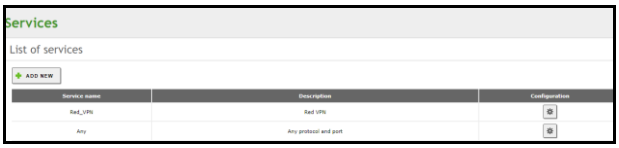

Figura 78 Vista parcial listado de servicio con énfasis en el botón configurar

Esta opción nos abre una vista donde podemos configurar nuestro servicio creado y poder configurar nuestro Servicio como UDP y en el puerto 1194, ver Figura 79,

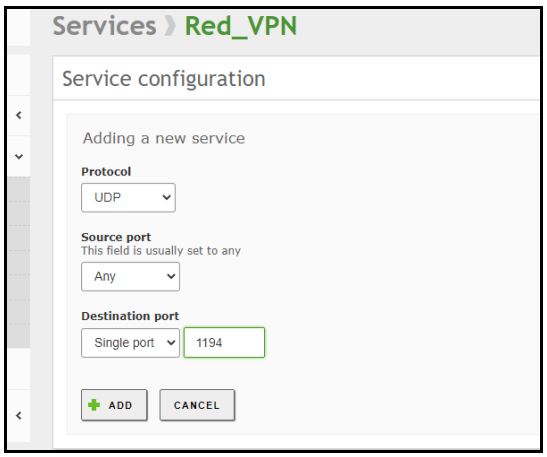

Figura 79 Vista de Configuración servicio UDP

Para guardar nuestros procesos realizados damos clic en el botón Gradar cambios de la parte superior derecha de nuestra página.

Configurado nuestro servicio procedemos a configurar el cortafuegos de nuestro Servidor.
Para ello nos vamos al Cortafuegos y damos clic en filtrado de paquetes.

Damos clic en configurar reglas y damos clic en agregar nueva, ver Figura 80.

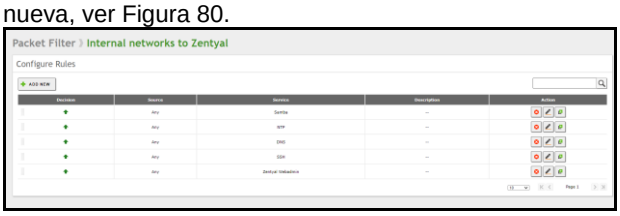

Figura 80 Vista de paquetes de filtros

Con el fin de que nuestro servicio tenga acceso por medio de nuestro corta fuego configuramos la regla como aceptar cualquiera en el servicio de Red_VPN, ver Figura 81.

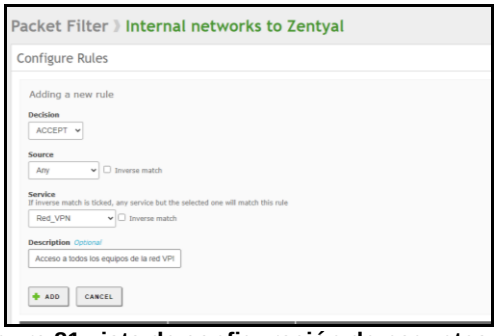

Figura 81 vista de configuración de paquetes de filtros

Después de configurar nuestro servicio y cortafuego vamos a configurar el Servidor VPN que creamos para esto damos clic en el botón de configurar, ver Figura 82.

Figura 82 Vista de listado de servidores VPN Creados

En el panel de configuración vamos a verificar el puerto y el servicio que creamos con anterioridad y habilitamos la interfaz TUN lo demás lo dejamos predeterminado como muestra la Figura 83.

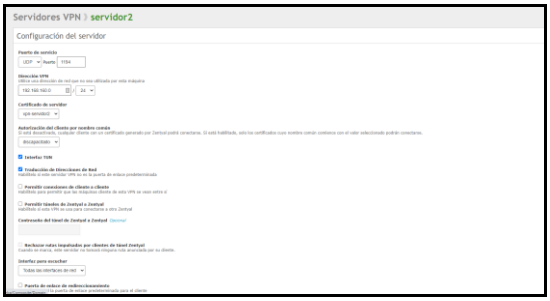

Figura 83 Vista de configuración del servidor VPN

Guardada nuestra configuración verificamos que nuestro servidor este activo si no seleccionamos la casilla de activación

Terminada la configuración del servidor procedemos a configurar los clientes que se van a conectar a nuestro servidor para esto vamos a dar clic en el botón de descargar paquete de cliente.

Como no hemos creado certificados para nuestros clientes, el sistema nos enviara a crear los certificados para el acceso seguro a nuestra VPN, ver Figura 84.

Figura 84. Vista de solicitud de creación de certificado para cliente

Al igual que con el certificado principal del Servidor; El sistema nos envía a crear los certificados para los clientes, para eso agregamos el nombre del certificado y los días de vigencia, ver Figura 85.

Figura 85. Vista de creación de certificado de autorización

Creado nuestros certificados procedemos a ir de nuevo a nuestro listado de servidores y damos clic en botón descargar paquete de cliente, esto nos enviara a una vista la cual nos permitirá configurar el tipo de cliente que se conectara a nuestra VPN.

En esta Vista el sistema nos solicita el tipo de cliente que vamos a utilizar y el certificado que vamos a asignar, en nuestro caso usaremos uno para Windows, asignamos el certificado del cliente 1 y agregamos la IP de nuestro servidor y damos clic en descargar, ver Figura 86.

Figura 86. Vista de Configuración de paquete de descarga para cliente VPN

Con esto el sistema nos descargar un archivo zip que contiene el certificado con una llave publica y una privada adicional a un archivo ce conexión que, al descomprimir, ver Figura 87.

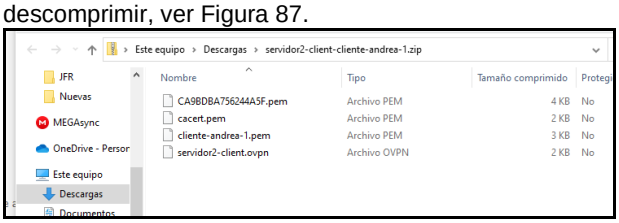

Figura 87. Vista de archivos generados por el sistema después de descomprimirlos

Con este paso terminamos con la configuración del servidor VPN y procedemos a conectarnos a este desde nuestros equipos cliente.

Para conectarnos a nuestro servidor podemos descargar un cliente de conexión VPN como “OpenVPN” desde su página oficial, en nuestro caso elegimos la versión para Windows, ver Figura 88.

Figura 88. Pagina de descarga de la herramienta OpenVPN Connect

Terminada la descarga ejecutamos el instalador de la aplicación, ver Figura 89.

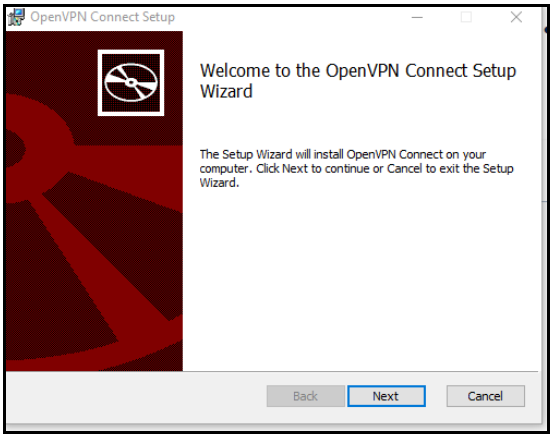

Figura 89. Vista inicial de Wizar de instalación de OpenVPN Connet

Aceptamos Términos y condiciones e instalamos la aplicación.

Finalizada la instalación automáticamente se no va a abrir el panel de inicio de la herramienta, ver Figura 90.

Figura 90. Vista inicial de OpenVPN Connect

Damos clic en la pestaña Archivo y este nos permite cargar el archivo de configuración que descargamos de nuestro servidor, ver Figura 91.

Figura 91. vista de la pestaña de conexión por archivo de configuración

Vamos a nuestra carpeta que tiene los archivos que descomprimimos y seleccionamos en archivo .ovpn, ver Figura 92.

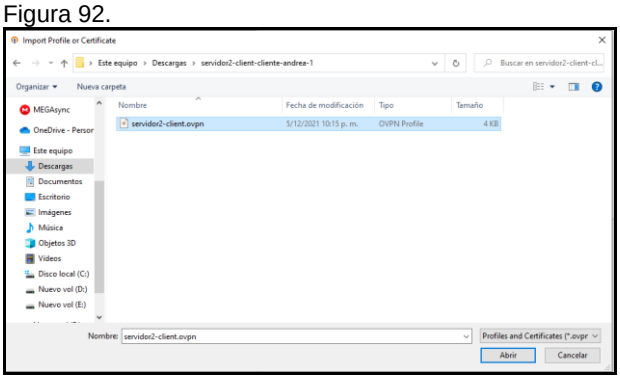

Imagen 92. Vista de la carpeta de configuración y el archivo .ovpn

Cargado el archivo, la herramienta nos va a mostrar la IP de nuestro servidor y el perfil de conexión y damos clic en conectar, ver Figura 93.

Imagen 93. Vista de OpenVPN después de cargado el archivo de configuración

Si todo esta correcto en la herramienta podemos ver una conexión exitosa a nuestra VPN, ver Figura 94.

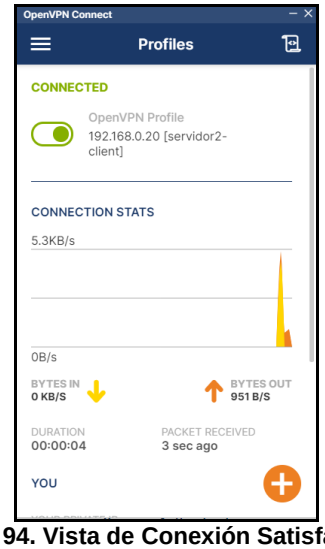

Imagen 94. Vista de Conexión Satisfactoria y estadísticas de OpenVPN Connect

Con esto el servidor VPN nos asigna una IP privada dentro del rango que nosotros seleccionamos, ver Figura 95.

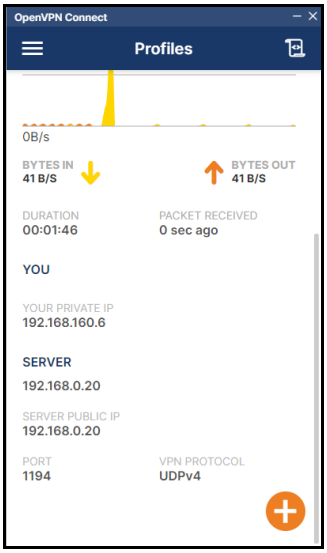

Figura 95. Vista de Conexión Satisfactoria y estadísticas de OpenVPN Connect

Si desde muestra consola ejecutamos un IPconfig nos va a mostrar nuestra ip y la conexión a la VPN, ver Figura 96.

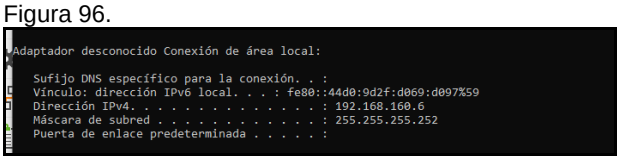

Figura 96. Vista del adaptado que genera la conexión a la VPN

8 CONCLUSIONES

Por medio de la configuración e implementación de los servicios DHCP, DNS, y Controlador de Dominio a través de Zentyal Server se puede administrar una red de manera adecuada y remotamente gracias a las diferentes opciones o servicios que nos brinda esta plataforma que se ejecuta en el entorno WEB.

Zentyal Server nos ofrece una manera de administrar los servicios de la red, por medio nos permite tener accesos y navegación segura a internet, ya que nos ayuda a tener el control de las páginas web que se tienen acceso y nos ofrece un bloqueo a las páginas o sitios que no sean permitidos navegar dentro de la red, dando así una calidad de la información confiable ya que todo este proceso se hace mediante el uso del filtrado proxy donde se definen los criterios necesarios.

Por medio de la práctica realizada se apropian conceptos y conocimientos técnicos para la instalación, administración y operación de un sistema de cortafuegos en Zentyal, con el fin de poder implementar reglas de denegación de acceso, brindando soporte a los requerimientos de seguridad que se requiera para salvaguardar la infraestructura tecnológica en pro de la prevención de infección de malware por acceso y descargas desde sitios web.

A través del desarrollo de las actividades propuestas se Logró Implementar bajo Zentyal Server, los servicios de gestión de infraestructura IT File Server y Print Server así como también la aplicación de los demás conocimientos recibidos en los pasos anteriores.

Podemos concluir que a nivel empresarial y para servicios de estaciones de trabajo y otros servicios (VPN, FTP, entre otros) es una buena alternativa de trabajo basada en Linux a nivel empresarial.

9 REFERENCIAS

[1] Página oficial Zentyal. Recuperado de: http://www.zentyal.org/server/.

[2] Instalación y configuración de servidor DHCP en Zentyal. [en Línea]. Recuperado de: https://www.youtube.com/watch?v=AEwvwJ8b56Y.

[3] Seguí Cristín, J. (2015). Servicios Internet para pymes con Zentyal. Recuperado de http://search.ebscohost.com.bibliotecavirtual.unad.edu.c o/login.spx? direct=true&db=edsbas&AN=edsbas.3B864C81&lang=es& ite=eds-live&scope=site

[4] KnowITFree. (2016, Octubre 6). 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

[5] Flores, R. (2 de Septiembre de 2016). Realizar VPNs con Zentyal y OpenVPN. Obtenido de openit.com.bo: http://mundo.openit.com.bo/?p=925

[6] rokitoh. (8 de Diciembre de 2016). Instalar servidor de VPN en Zentyal Server 5. Obtenido de red orbita: https://red-orbita.com/?p=7680

[7] zentyal. (01 de 01 de 2021). Zentyal para Adminstradores de redes. Obtenido de zentyal: https://zentyal.com/wp-content/themes/storefront-zentyal-child/assets/files/sample_chapter_zentyal_vpn_openvpn_es.pdf