ZENTYAL SERVER 6.2 SERVIDOR DE ADMINISTRACIÓN DE SERVICIOS DE RED EN GNU/LINUX

Diego Alexander Rodriguez Arango – código: 1.098.626.229
e-mail: dralex18@hotmail.coml.com

Jean Carlos Vega - código: 1091595644

e-mail: jecaveni@gmail.com

Jorge Armando Rodriguez– código: 91.523.232

e-mail: Jorge.r@msn.com

Julian Ernesto Rojas Garavito – código: 1.100.951.546

e-mail: j.rojas.garavito@gmail.com

Mairon Tobias Sandoval Becerra – código: 1.091.671.006

e-mail: mtsandovalb@unadvirtual.edu.co

RESUMEN: *El objetivo de este trabajo fue formular soluciones bajo GNU/Linux que permita dar respuesta a los requerimientos específicos del cliente. Usando como sistema operativo Zentyal Server 6.2 con el que se implementaran los servicios y plataformas tales como, Controlador de Dominio, DHCP Server, DNS Server, Proxy, Cortafuegos, File Server y Print Server, VPN.*

ABSTRACT: *The objective of this work was to formulate solutions under GNU / Linux that allow to respond to the specific requirements of the client. Using Zentyal Server 6.2 as the operating system with which services and platforms such as Domain Controller, DHCP Server, DNS Server, Proxy, Firewall, File Server and Print Server, VPN will be implemented.*

PALABRAS CLAVE: Zentyal, DNS, DCHP, VPN, cortafuegos, proxy, Servidor, cliente, controlador de dominio.

1 INTRODUCCIÓN

Este documento tiene como finalidad describir los diferentes procesos que permiten dar soluciones a las problemáticas presentadas, donde se implementará y usará Tecnologías GNU/Linux, para dar solución a los requerimientos del cliente, estas soluciones se realizaran mediante el sistema operativo Zentyal Server, este sistema operativo incluye todo lo necesario en cuanto a gestión y administración de los servicios esenciales requeridos.

.

2 DESARROLLO DEL PASO 8 - SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX.

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

Desarrollada por: Jorge Armando Rodriguez.

Se inicia la instalación de Zentyal y se elige el país Colombia.

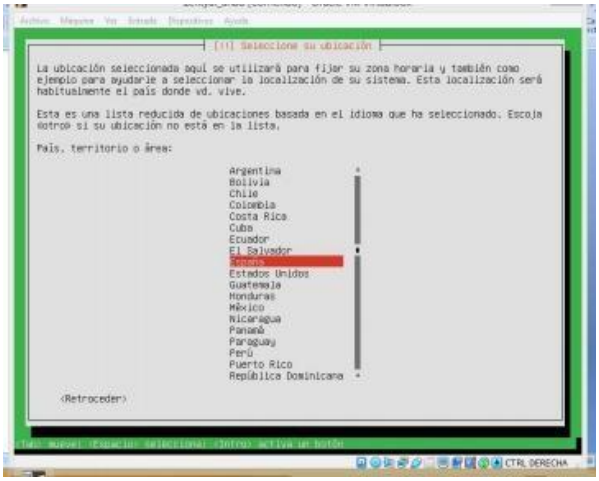

Imagen 1. Instalación Zentyal 6.2. Ilustración propia.

Se selecciona el nombre de la máquina que se va a instalar, se elige contraseña, zona horaria, entre otros datos básicos de instalación.

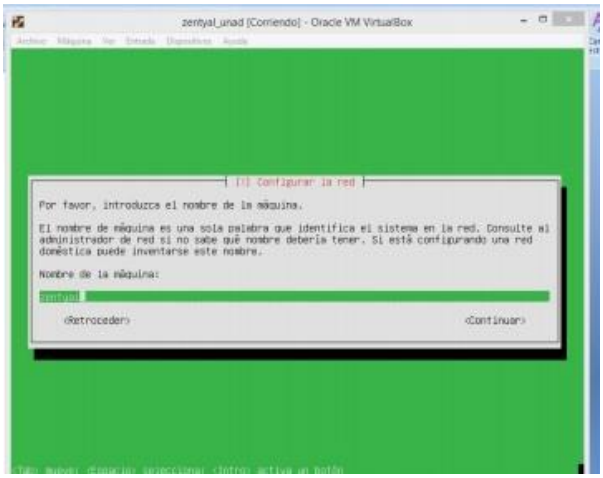

Imagen 2. Selección nombre de máquina. Ilustración propia.

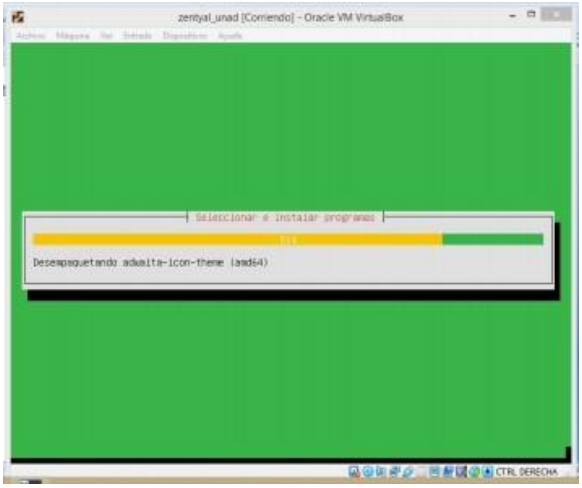

Imagen 3. Progreso Instalación. Ilustración propia

Imagen 4. Finalización Instalación. Ilustración propia

Imagen 5. Ventana escritorio Zentyal 6.2. Ilustración propia.

Se ingresa al sistema de administración de Zentyal con el usuario y contraseña seleccionados.

Imagen 6. Acceso Zentyal 6.2. Ilustración propia

En el tablero de control se selecciona gestión de software paquetes instalados.

Imagen 7. Gestión de Software. Ilustración propia

Se selecciona los paquetes a instalar, DHCP Server, DNS Server y Controlador de Dominio.

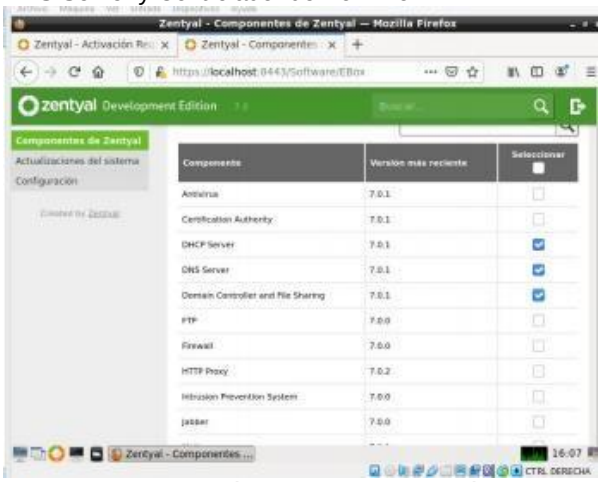

Imagen 8. Selección de paquetes. Ilustración propia

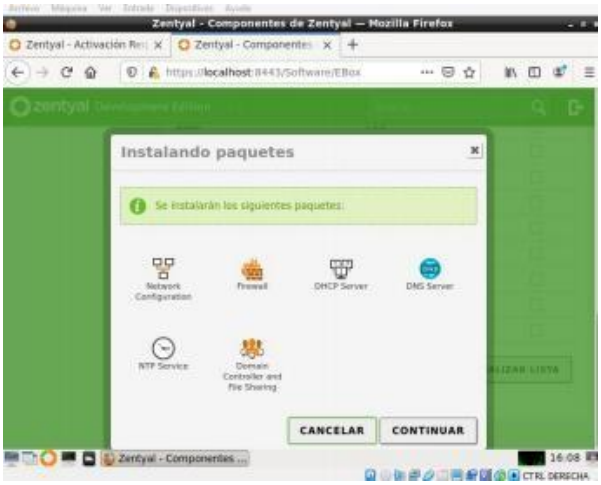

Imagen 9. Paquetes instalados. Ilustración propia

Se activa y configura cada módulo DNS.

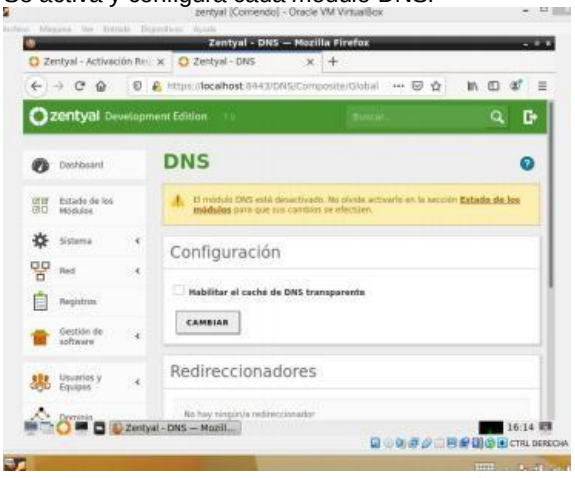

Imagen 10. Panel de control DNS. Ilustración propia

Se configura el modulo DNS.

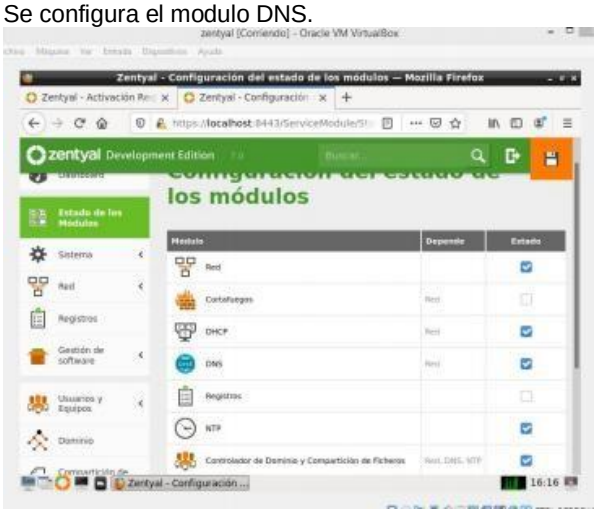

Imagen 11. Configuración DNS. Ilustración propia

Se configura el módulo DHCP.

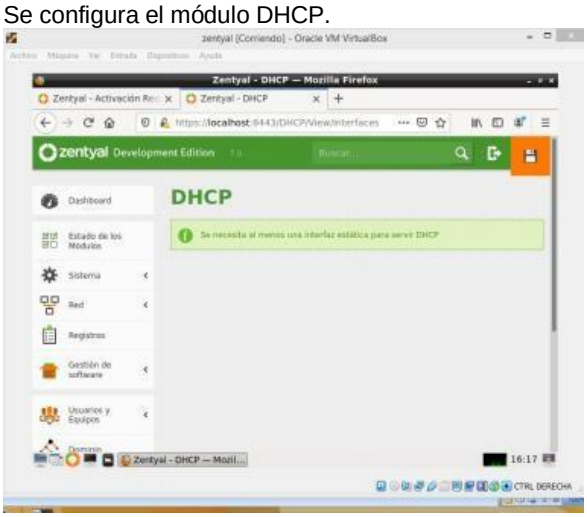

Imagen 12. Panel de control DHCP. Ilustración propia

Se configura el módulo controlador de dominio.

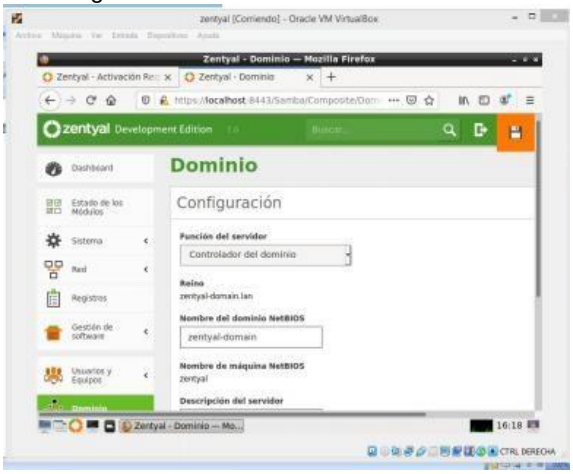

Imagen 13. Configuración módulo. Ilustración propia

2.2 TEMÁTICA 2: PROXY NO TRANSPARENTE.

Desarrollada por: Julian Ernesto Rojas Garavito.

Se realiza la instalación de los componentes requeridos para la configuración del proxy no transparente.

Imagen 14. Componentes, ilustración propia.

Para la configuración es necesario instalar los paquetes de firewall y proxy http.

Imagen 15. Instalación paquetes, ilustración propia.

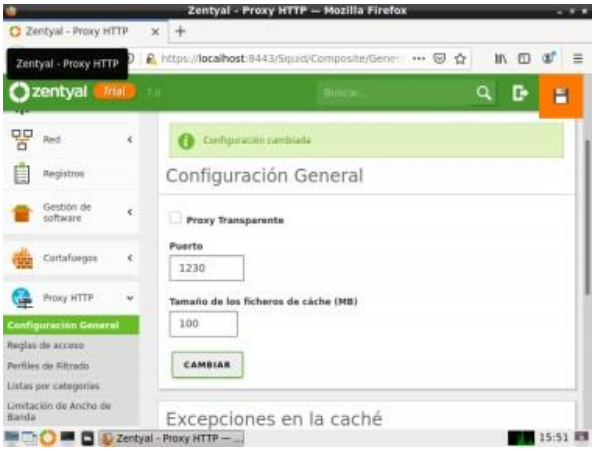

Imagen 16. Configuración general proxy, ilustración propia.

Se ingresa al menú interfaces de red, se configura la red inicial enp0s3 con método DHCP, se marca la opción externo WAN y se da clic en el botón CAMBIAR.

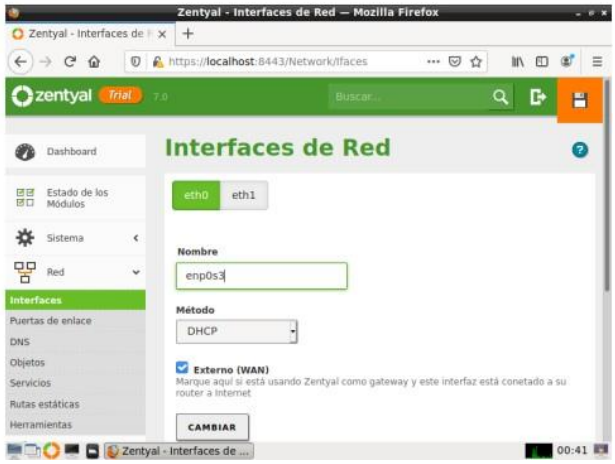

Imagen 17. Interfaces de red, ilustración propia

Se Configura la red enp0s8 con método Estático, no marcar la opción externo WAN, ingresar una ip que se convierte en el Gateway para los equipos cliente y se das clic en el botón CAMBIAR para guardar los cambios.

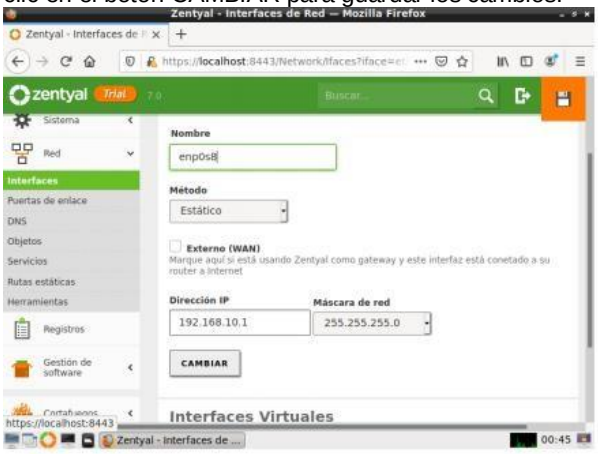

Imagen 18. Configuración de red, ilustración propia

Crear un objeto para identificar los equipos en red se selecciona objetos, dar clic en el botón Añadir Nuevo Colocamos el nombre Ubuntu.

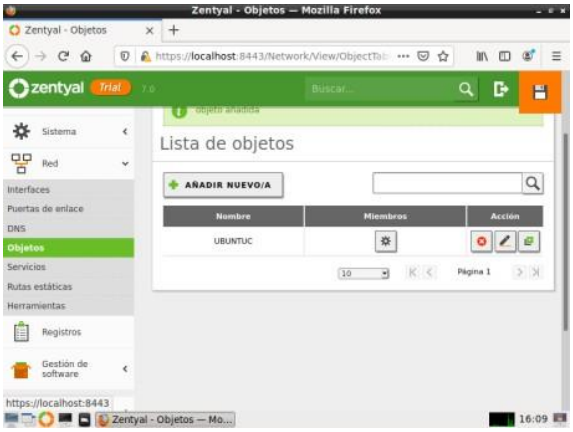

Imagen 19. Crear objeto, ilustración propia

Se Debe agregar los usuarios cliente al listado de restricción, Ingresar al equipo cliente en Ubuntu configurar una IP fija para el equipo cliente y que el Gateway sea la IP del servidor

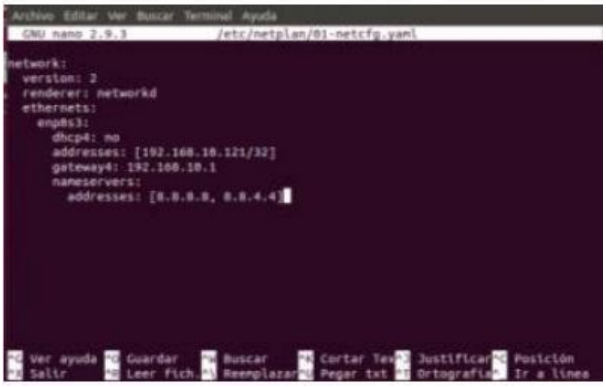

Imagen 20. Agregar usuarios, ilustración propia

Se Regresa al servidor Zentyal dar clic en el icono de miembros para agregar a los usuarios requeridos

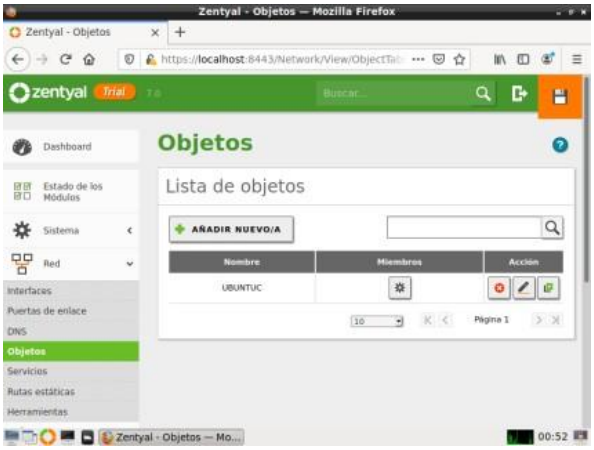

Imagen 21. Miembros - Agregar usuarios, ilustración propia

Se abre la venta de miembros, dar clic en el botón Añadir Nuevo.

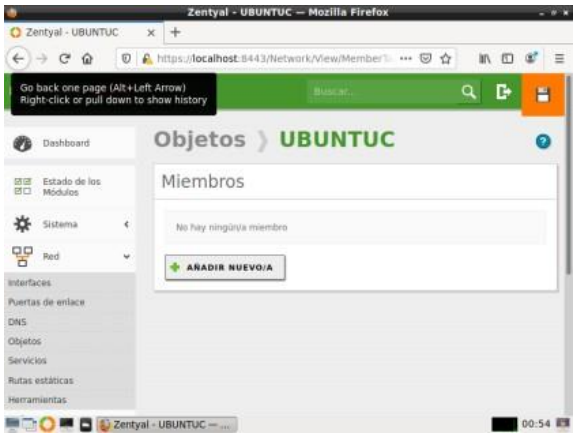

Imagen 22. Añadir nuevo, ilustración propia

Ingresar los datos del equipo cliente, nombre en la opción de dirección IP colocar CIDR, ingresar la IP del equipo cliente y dar clic en el botón Anadir para continuar con el proceso.

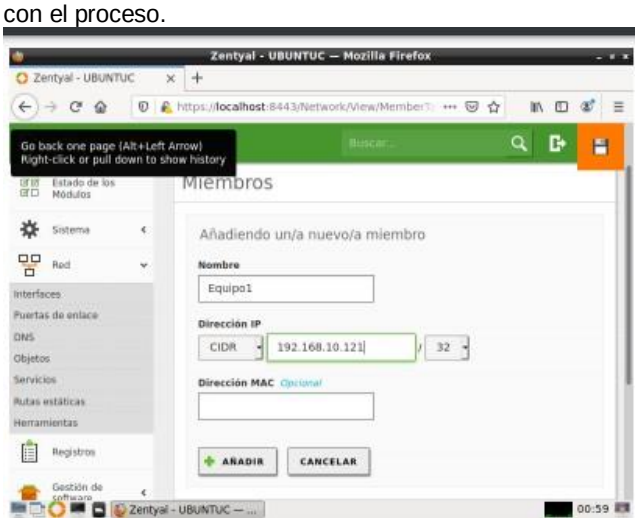

Imagen 23. Ingreso datos, ilustración propia

Luego de guardar la configuración se cierra la ventana y regresa a la pantalla inicial de objetos donde se evidencia la IP de cliente y la configuración aplicada.

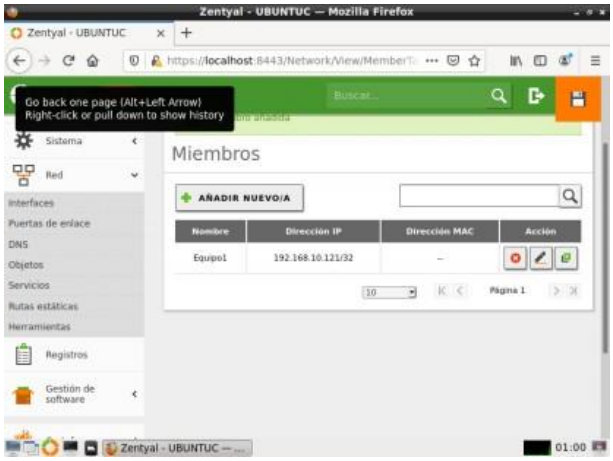

Imagen 24. Pantalla principal objetos, ilustración propia

En el menú del lado izquierdo ingresar al módulo Proxy HTTP y seleccionar la opción Configuración General. Validar que la opción proxy transparente no está marcada, en el cuadro puerto ingresar el puerto 1230 y dar clic en el botón CAMBIAR para continuar con el proceso requerido.

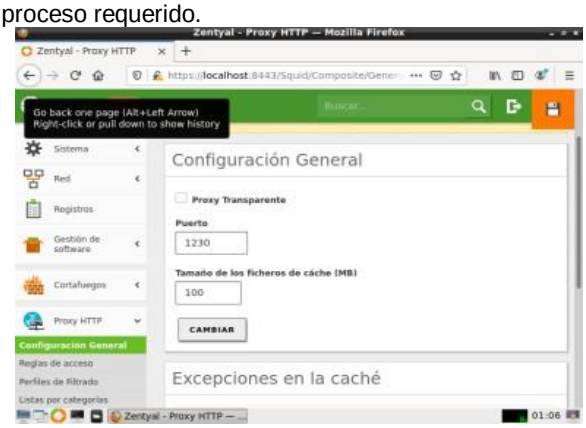

Imagen 25. Configuración general, ilustración propia

Se deben crear las reglas de trabajo para los usuarios, en el menú del lado izquierdo ingresar a Proxy HTTP, seleccionar la opción Reglas de acceso. Dar clic en el botón Añadir Nuevo para agregar las reglas de los usuarios.

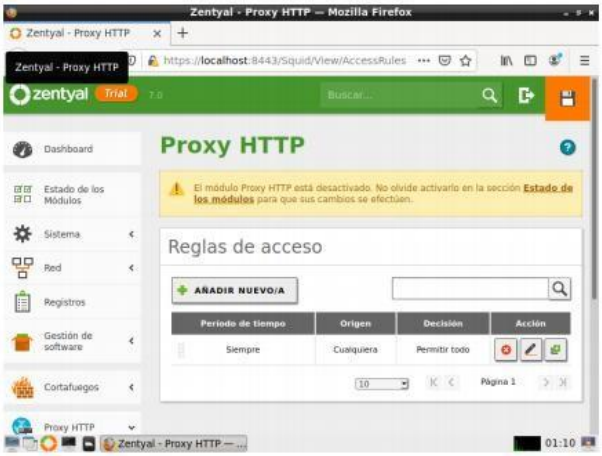

Imagen 26. Reglas de acceso, ilustración propia

En el campo origen ingresar el objeto creado para este caso Ubuntu y en el campo decisión marcar la opción denegar todo, luego dar clic en el botón Añadir para continuar con el proceso, y estaría configurado el proxy para el trabajo con los usuarios.

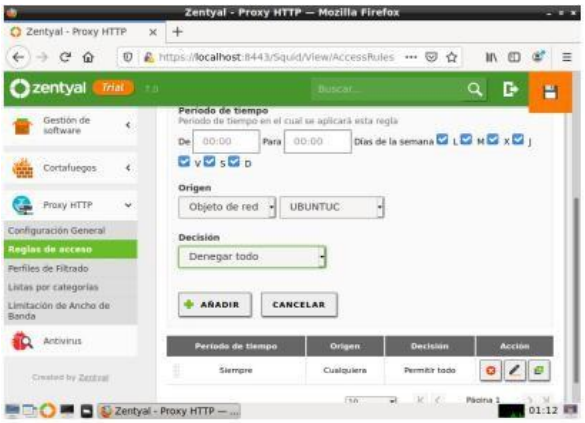

Imagen 27. Ingreso objeto creado, ilustración propia

Muestra la pantalla inicial de proxy, donde se evidencia los cambios realizados, el origen y la configuración aplicada.

Imagen 28. Evidencia de cambios, ilustración propia

Reiniciar el equipo servidor y el equipo cliente Regresar al equipo cliente y configurar el proxy en el navegador, desde la barra de menús ingresar a editar y seleccionar la opción preferencias.

En la parte inferior de preferencias en la opción configuración de red, dar clic en el botón configuración.

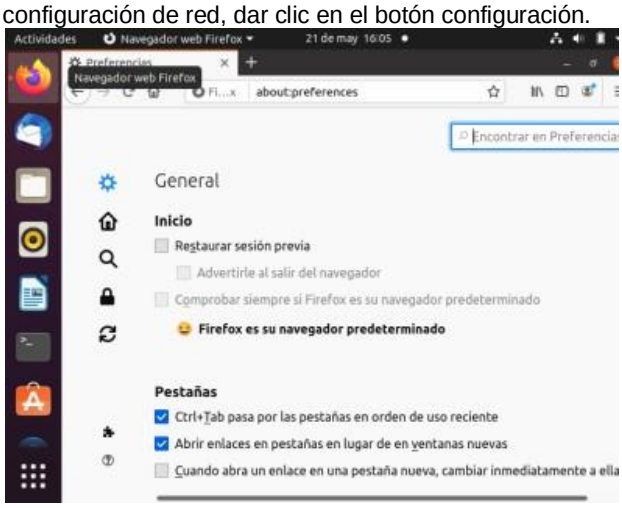

Imagen 29.Configuración proxy navegador, ilustración propia

Se deben ingresar los datos del proxy del servidor, marcar la opción configuración manual proxy, ingresar los

datos de la ip del servidor 192.168.10.1, con el puerto 3128 que están configurados en el servidor y marcar la opción usar para toda la configuración.

Imagen 30. Rechazo conexiones, ilustración propia

2.3 TEMÁTICA 3: CORTAFUEGOS

Desarrollada por: Diego Alexander Rodriguez Arango.

Ya instalado Zentyal, seleccionar los módulos que se requieren para dar solución y desarrollo de la temática. La temática en esta ocasión es *corta fuegos, para la cual se debe* instalar el Firewall, esto brinda una mejor comunicación del host cliente - servidor, y garantizará que el tráfico pase por el firewall.

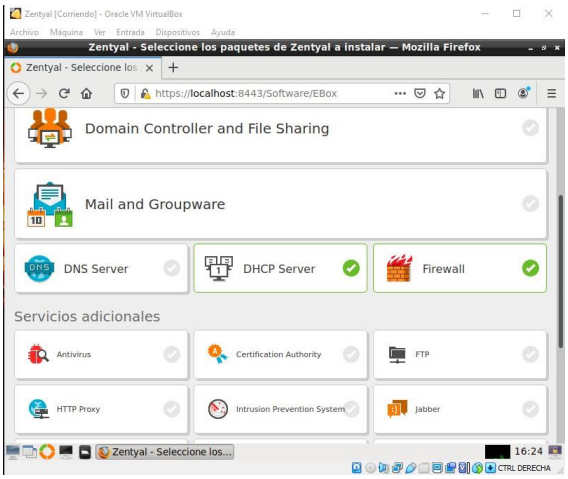

Imagen 31. Selección de módulos, ilustración propia.

Terminada la instalación de los paquetes DHCP server y Firewall, solicita configurar las dos interfaces de red, las cuales se debió haber ajustado en la máquina virtual; la primera que dará la salida a internet, en el caso de un Firewall esta sería la zona Roja y la otra será la red interna o zona verde, donde van a estar los equipos clientes en la red LAN , la interfaz eth1 va a ser la zona roja o una tarjeta de red externa, y la interfaz eth0 va a ser la zona verde o la red interna. Ahora solicitará el método de direccionamiento y la red interna que se utilizará es 10.0.2.1

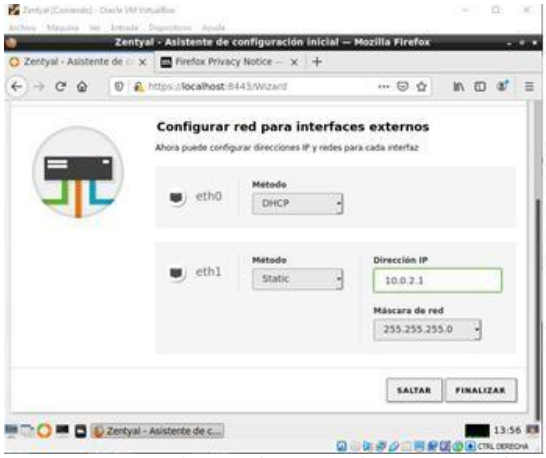

Imagen 32. Configuración de interfaces, ilustración propia.

Finaliza la configuración, se accede al dashboard de Zentyal:

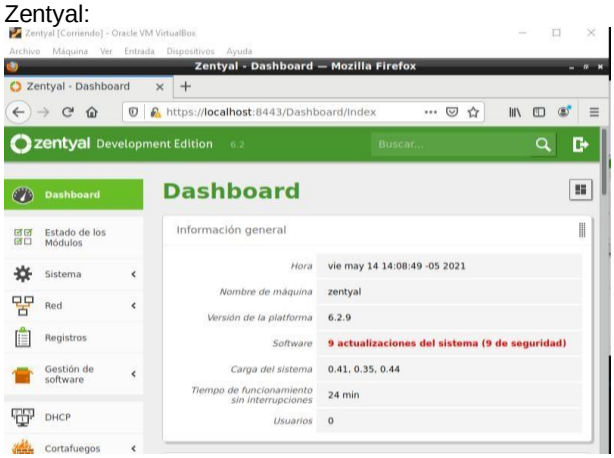

Imagen 33. Dashboard, ilustración propia.

Ahora se revisa el servicio DHCP, y se configura el o los rangos de direcciones IP

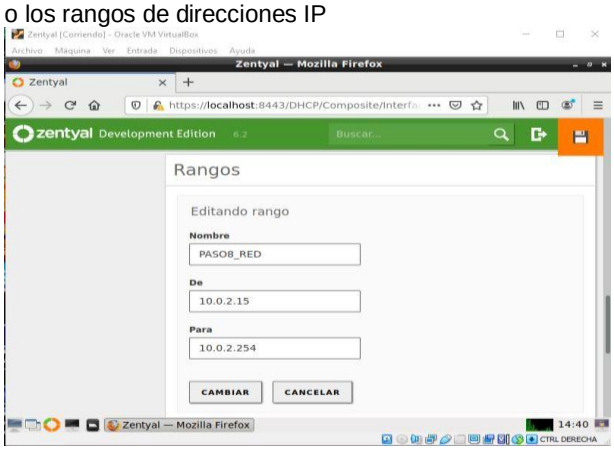

Imagen 342. Configuración de direccionamiento DHCP. Ilustración propia.

Lista la configuración, se enciende el equipo cliente, (Ubuntu Desktop) debe aparecer conexión en el dashboard.

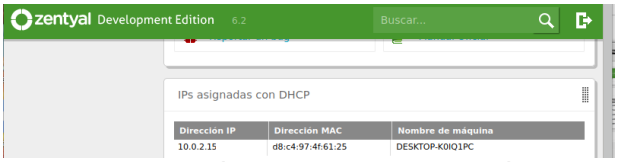

Imagen 35. Asignación de IP por DHCP. Ilustración propia.

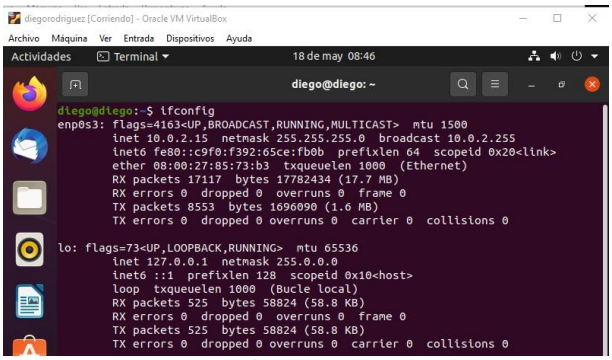

Imagen 36. Ejecución de comando ifconfig Ubuntu.

Ahora se entra a configurar el Firewall o cortafuegos con la finalidad de establecer las políticas requeridas.
Se debe hacer desde Ubuntu desktop, ingresando la dirección IP que se configuró 10.0.2.1 con el puerto 8443 que es el designado para la administración.

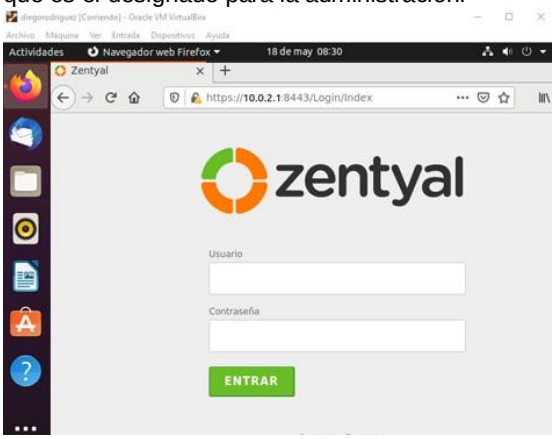

Imagen 37. Acceso a panel de administración Zentyal desde Ubuntu. Ilustración propia.

Para poder crear las reglas del bloqueo de las páginas, primero se va a ver cuál es su dirección IP:

Imagen 38. IP. Ilustración propia.

Como se observa en la imagen la dirección IP de los servidores de Facebook es: 69.171.250.35, esta es la IP a utilizar para realizar el bloqueo de ingreso a este sitio. Se tienen listas las direcciones a bloquear empieza a configurar las reglas de bloqueo con el cortafuego de Zentyal Ingresar a cortafuegos, filtrado de paquetes, Reglas de filtrado para redes internas y dar en configurar reglas:

Imagen 39. Panel de filtrados. Ilustración propia.

Se procede adicionar el primer sitio a bloquear, se inicia con Facebook.
Se selecciona en añadir nuevo(a) y selecciona denegar, esto va a bloquear el tráfico, aplicando a cualquiera de los equipos de la red de la zona verde, como destino ponemos la IP del sitio a bloquear y en servicio se selecciona cualquiera, porque va a bloquear completamente cualquier tráfico o servicio a esta IP

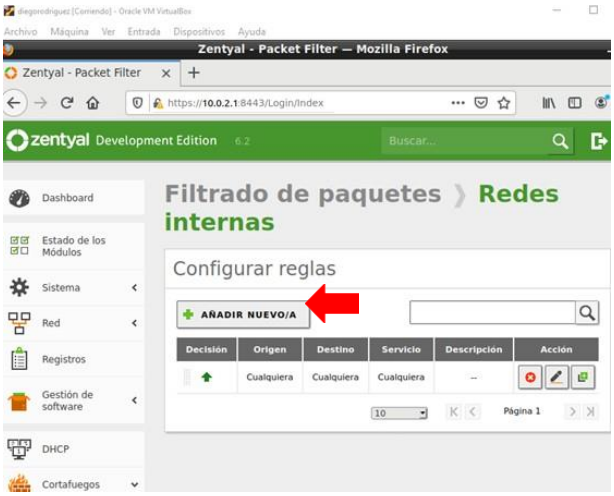

Imagen 40. Panel de administración de reglas de filtrados cortafuegos. Ilustración propia.

Añadimos la regla:

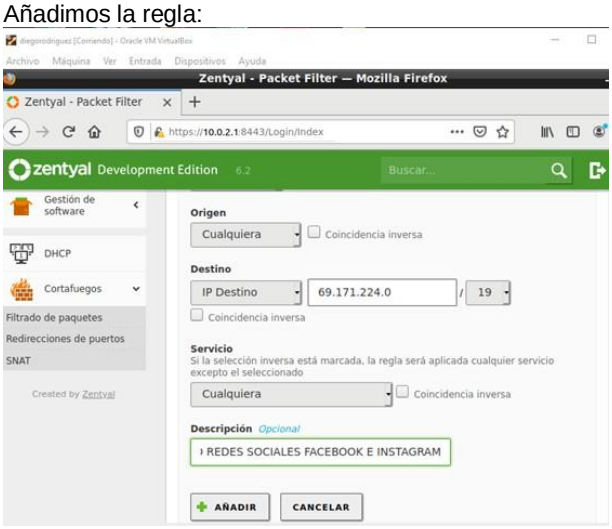

Imagen 41. Creación de regla de bloqueo Facebook e Instagram. Ilustración propia.

Se realiza el mismo procedimiento para las direcciones IP que se deseen bloquear:

Imagen 42. Reglas de filtrado creadas, panel cortafuegos. Ilustración propia.

Listas la configuración de bloqueo o reglas de bloqueo se debe validar su funcionamiento, se solicita ping a la dirección IP, al dominio facebook.com

Imagen 43. Navegación a Facebook bloqueada, Ilustración Propia.

Imagen 44. Navegación Instagram, bloqueada. Ilustración propia.

Se puede evidenciar que al solicitar dirección ping a los sitios a los cuales se le asignaron reglas, se encuentran bloqueadas.

2.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Desarrollada por: Jean Carlos Vega

En el apartado de usuarios y equipos se va a crear un nuevo usuario con el cual se pueda realizar las pruebas de funcionamiento de la configuración.

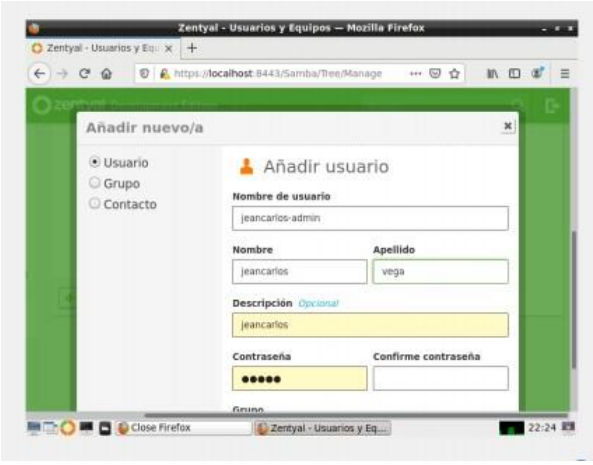

Imagen 45. Creación de usuario, Ilustración Propia

Con el usuario creado se va a la configuración de LDAP y se establece los siguientes parámetros. LDAP permitirá conectar con los usuarios que se cran en nuestro servidor desde el cliente. Esto es útil para poder controlar el File Server de configuración

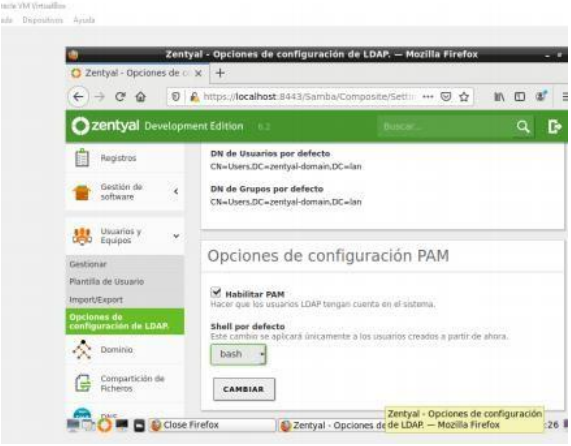

Imagen 46. Configuración LDAP Ilustración propia.

Se procede a configurar el dominio como se observa a continuación

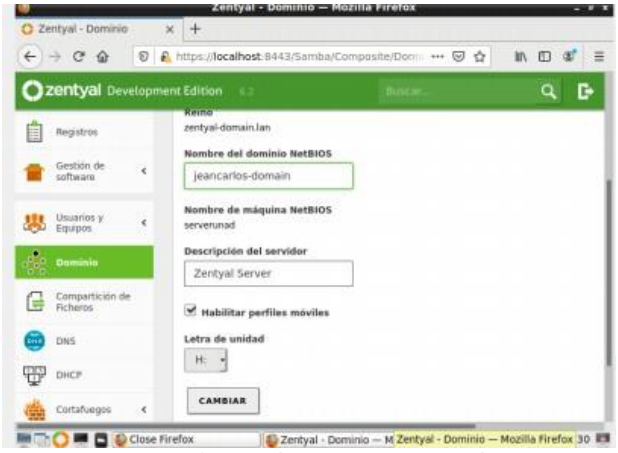

Imagen 47. Configuración Dominio Ilustración propia.

Con el servicio LDAP configurado, ahora se va a configurar el DHCP. Para esto habilitamos el modulo correspondiente dentro Zentyal, ya con el módulo activo se agrega un rango de IP, estas serán las que podrán tomar los equipos dentro de la red.

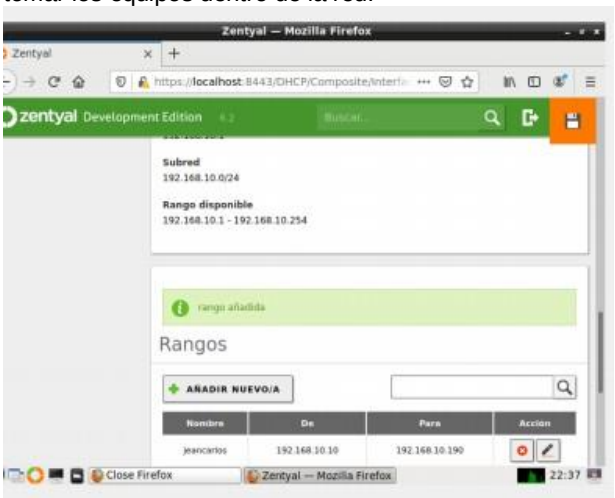

Imagen 48. Configuración Rangos Ilustración propia.

Se termina la configuración del servidor. Ahora se pasa a la configuración de los clientes. Lo primero es establecer que todos los equipos dentro de la red deben ser configurados en modo puente. De esta forma tendrán comunicación con el servidor.

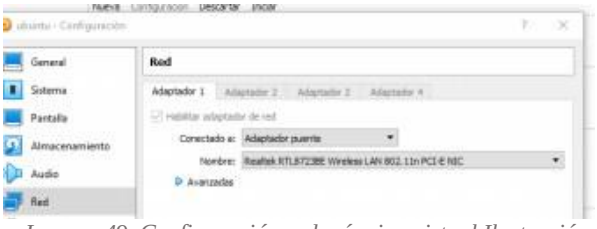

Imagen 49. Configuración red máquina virtual Ilustración propia.

2.4.1 SERVIDOR ZENTYAL Y CONFIGURAREMOS EL FILE SERVER

Lo primero que se debe hacer es con el comando Mkdir crear una carpeta la cual se usará para comprobar el funcionamiento del servicio.

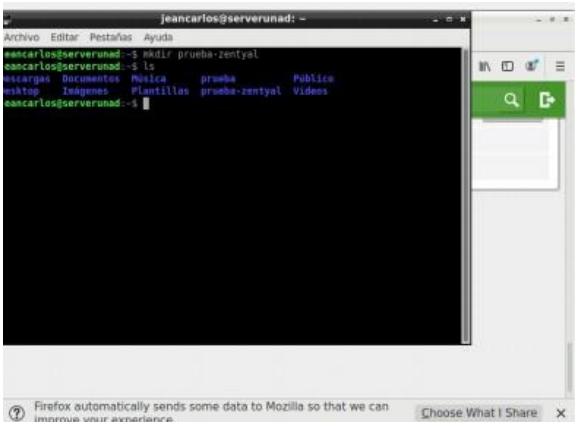

Imagen 50. Creación de carpeta Ilustración propia.

Dentro del módulo de ficheros compartidos, se va a crear un nuevo recurso. Para esto se agrega un nombre que será el que ven otros usuarios, además se ingresa a la ruta en la cual se encuentra esta carpeta y que se crearon en el paso anterior.

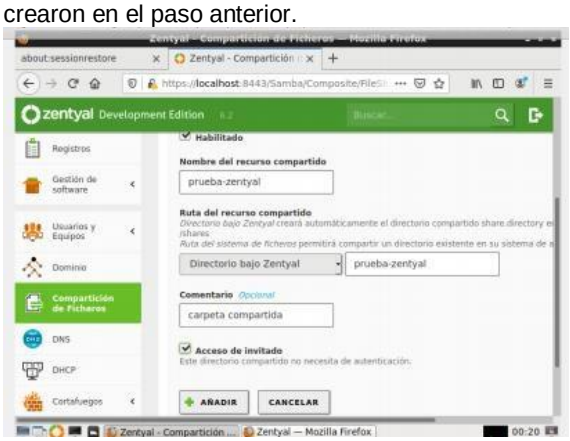

Imagen 51. Modulo ficheros Ilustración propia.

Se agregan a los usuarios que podrán acceder a este recurso. Aquí se dará permisos al usuario creado cuando se configuró LDAP.

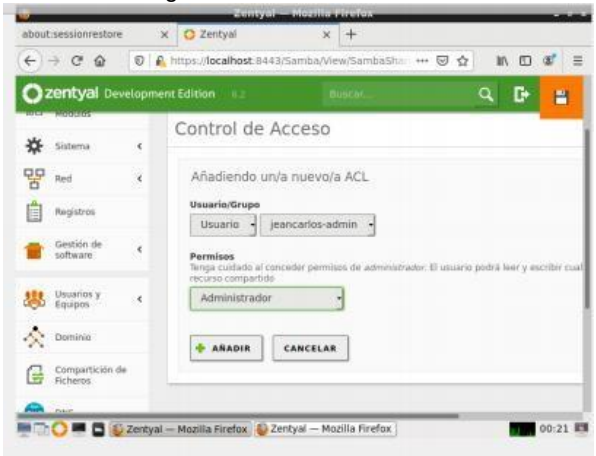

Imagen 52. Control de acceso Ilustración propia.

Por último se verifica el acceso al recurso compartido en los equipos conectados por DHCP

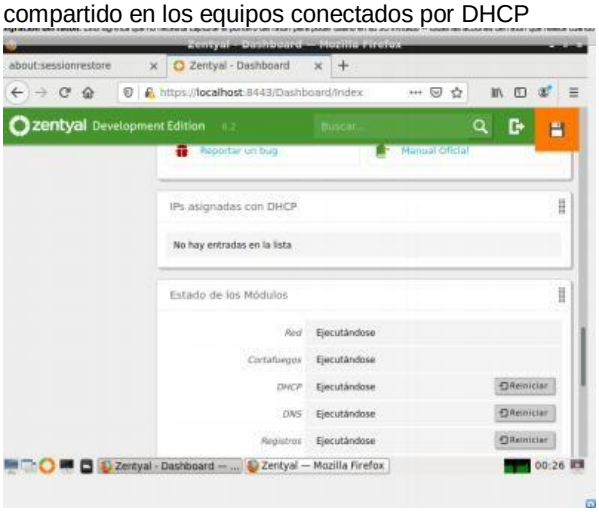

Imagen 53. Verificación de acceso Ilustración propia.

2.5 TEMÁTICA 5: VPN

Desarrollada por: Mairon Tobias Sandoval Becerra

Para empezar, se creará un certificado para el servidor Zentyal el cual actúa como una Autoridad de Certificación.

Imagen 54. Creación certificado Ilustración propia

El siguiente paso es crear un nuevo servidor VPN.

Para este ejemplo se creará Servidor-VPN.

Imagen 55. Creación VPN Ilustración propia

Después de crear el servidor VPN se debe crear un nuevo certificado para la nueva conexión.

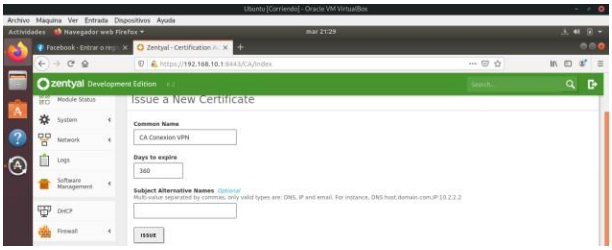

Imagen 56. Creación nuevo certificado Ilustración propia

Se verifica la creación de los certificados y que tengan un estado valido.

Imagen 57. Verificación estado. Ilustración propia

Posteriormente se configura el servidor VPN anteriormente creado de la siguiente manera: El puerto será 1194, puerto por defecto, se asigna una dirección VPN para la conexión, en el certificado del servidor se asigna el certificado creado anteriormente (CA Conexión VPN) y por último se habilita el TUN interface. Las demás opciones de configuración se dejarán por defecto ya que para este ejemplo no son necesaria

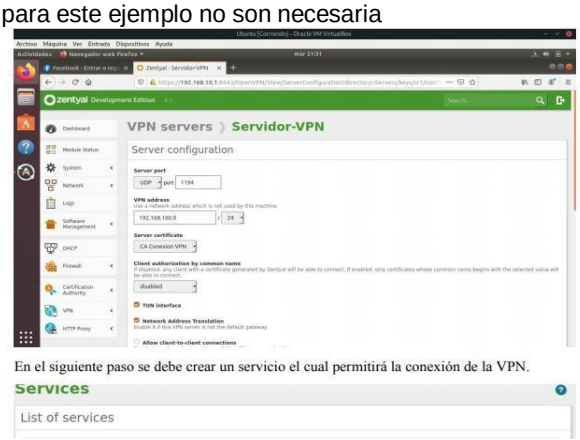

Imagen 58. Configuración VPN. Ilustración propia.

En el siguiente paso se debe crear un servicio el cual permitirá la conexión

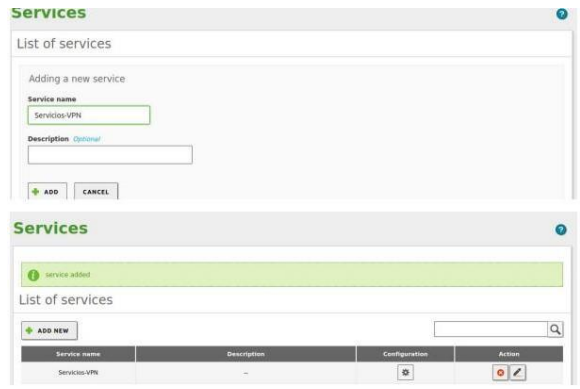

Imagen 59. Creación servicio Ilustración propia

El protocolo será UDP, el puerto origen será cualquiera y el destino el mismo del servidor VPN, 1194.

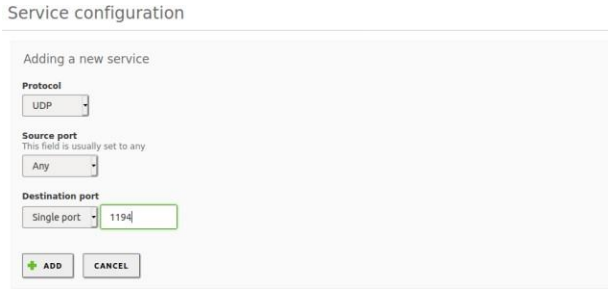

Imagen 60. Configuración servidor VPN .Ilustración propia

Después de hacer todos los pasos anteriormente mencionados el servidor VPN está lista para realizar una conexión desde un cliente. En la opción de VPN Servers se selecciona el servidor creado para poder descargar el cliente de la conexión.

Imagen 61. conexión cliente Ilustración propia

Se selecciona el tipo de cliente de la VPN, para este caso será un equipo Ubuntu desktop desde el cual se realizará la prueba de conexión, se selecciona el certificado para el cliente y por último se tiene que configurar la dirección de servidor. La prueba de conexión que se realizará será poder acceder al servidor Zentyal e iniciar sesión desde internet. Se debe consultar la IP pública del proveedor de internet al cual estamos conectados y esa será la dirección del servidor.

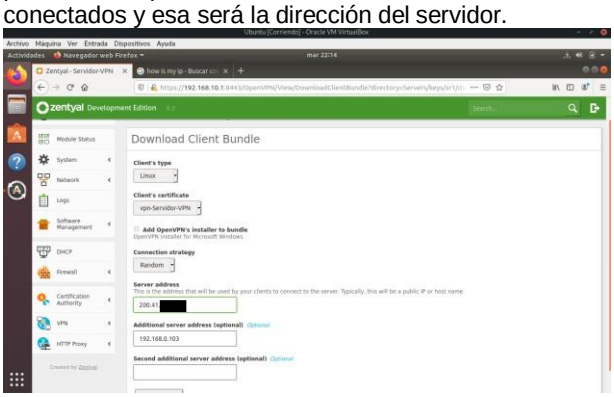

Imagen 62. Configuración conexión. Ilustración propia

2.5.1 CONFIGURACIÓN DEL CLIENTE

Al descargar el cliente se obtienen los siguientes archivos. El Servidor-VPN-cliente.conf es el archivo con toda la configuración de la conexión, el archivo cacert.pem es el certificado del Zentyal, el archivo 7E5EE1CBF8E23FB1.pem es el certificado del cliente y el archivo vpn-Servidor-VPN.pem es la key para el cliente.

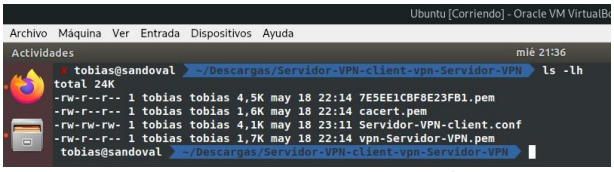

Imagen 63. Descarga cliente Ilustración propia

Se utiliza el comando sudo openvpn Servidor-VPN-client.conf para realizar la conexión con el servidor VPN.

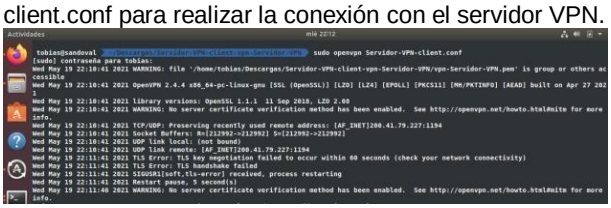

Imagen 64. Conexión cliente con servidor VPN Ilustración propia

Al finalizar la conexión aparece el siguiente mensaje indicando que la conexión está establecida.

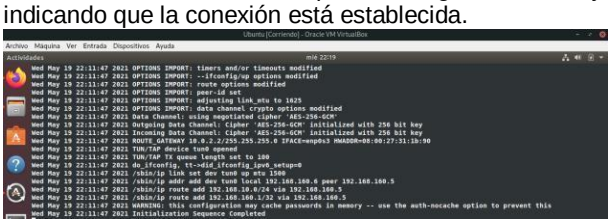

Imagen 65. Conexión establecida con servidor VPN. Ilustración propia

2.5.2 EVIDENCIA DE NO CONEXIÓN AL SERVIDOR ZENTYAL

Antes de conectar la VPN se comprueba que no se tiene conexión con el servidor, se asignó una interfaz de red a la máquina virtual de Ubuntu desktop que se comporta como red NAT la cual no conoce la IP del servidor, posteriormente se verifica la IP asignada por la red NAT que no esté en el mismo segmento de red del servidor y se verifica el ping al servidor Zentyal.

Imagen 66. No conexión Ilustración propia

Se intenta acceder por navegador al servidor.

Imagen 67. Acceso por navegador Ilustración propia

2.5.3 EVIDENCIA DE LA CONEXIÓN AL SERVIDOR ZENTYAL POR VPN

Al conectar la VPN esta nos entrega una IP deferente al segmento de la red NAT la cual crea una conexión directa y segura al servidor Zentyal a través de internet, esto permite administrar el servidor remotamente.

Para hacer la prueba de conexión se realizarán los mismos pasos que se hicieron anteriormente:

- Se verifica la IP asignada de la conexión VPN sea diferente al segmento de la red NAT.
- Se realiza ping a la IP del servidor Zentyal.
- Se inicia sesión al servidor Zentyal remotamente

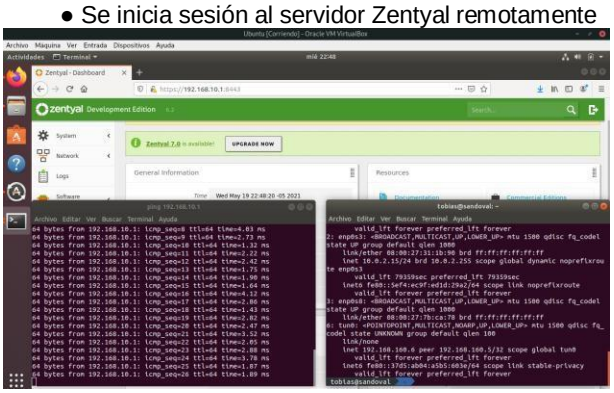

Imagen 68. Prueba conexión Ilustración. propia

Después de iniciar sesión ya se puede administrar el servidor remotamente.

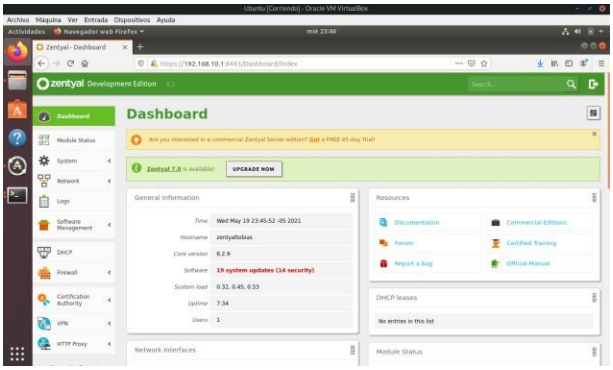

Imagen 69. Conexión establecida. Ilustración propia

3 CONCLUSIONES

Se documentó paso a paso a cabo la instalación del sistema operativo Zentyal 6.2, logrando identificar correctamente las diferentes interfaces de red las cuales permiten una adecuada conexión a la red externa o red interna dependiendo del caso.

Se implementan y asignan reglas de filtrado web, arrojando el resultado esperado, que consistía en bloqueo de ingreso a cualquier sitio web.

Las herramientas que ofrece el servidor Zentyal son muy completas y ofrecen una gran ayuda, dando todos los servicios de configuración y control en el entorno de red para el control total de los usuarios, adicionalmente aplicar los permisos y características básicos en el entorno de Zentyal es muy importante ya que están limitados y sin su correcta configuración no funciona para el usuario cliente.

La infraestructura generada por Zentyal basada en Ubuntu 20 genera muchas ventajas a las empresas de IT, además de la seguridad que ofrece con su compatibilidad con diferentes módulos. Contando con ventajas de las opciones opensource son ilimitadas debido a los bajos costos y facilidades de acceso a documentación.

4 REFERENCIAS

[1] Zentyal 6.2 Documentación Oficial — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. https://doc.zentyal.org/es/

[2] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing. Recuperado de https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page-_-20

[3] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40

[4] Instalar y configurar el cliente OpenVPN en GNU/Linux. (2021). Retrieved 21 May 2021, from https://sobrebits.com/instalar-y-configurar-cliente-openvpn-en-gnulinux/