

# Instalación y Configuración de Zentyal Server, para servicios de DHCP Server, DNS, Cortafuegos, File Server, Print Server y VPN

Roger Mauricio Garzón Rubiano  
rmgarzonr@unadvirtual.edu.co  
Alejandro Martínez Tabares  
amartinezta@unadvirtual.edu.co  
Vladimir Enrique Henríquez Ilias  
vehenriquezi@unadvirtual.edu.co  
Oscar Leonardo Barrios  
olbarriosp@unadvirtual.edu.co

**RESUMEN:** A través de la implementación y configuración de un servidor Zentyal en su versión 6.2 Development, se desarrolla la gestión y solución de necesidades específicas para el correcto funcionamiento de herramientas tecnológicas en un entorno de red corporativa, aplicando las metodologías de cliente servidor y utilizando los diferentes servicios requeridos para una infraestructura tecnológica que dé respuesta a las necesidades del cliente.

**PALABRAS CLAVE:** Implementación, servidor, Infraestructura, Zentyal, VPN.

## 1 INTRODUCCIÓN

En el presente documento encontrará el desarrollo y solución de las necesidades específicas basadas en GNU/Linux, a partir de la instalación y creación de máquinas virtuales en VirtualBox, configurando de manera adecuada las características requeridas, asignación de espacio en disco virtual, memoria y procesador, así como la configuración de la red, dependiendo de la necesidad específica agregando, los adaptadores virtuales en modo puente para su adecuado funcionamiento. Se instaló la versión Development 6.2 de Zentyal, los servicios a configurar son DHCP, DNS, Directorio Activo, controlador de dominio LDAP, Firewall, VPN, Servidor de archivos y de impresiones, permitiendo la parametrización y uso de cada uno de estos servicios en función de solucionar los diferentes requerimientos planteados.

A partir de los conocimientos adquiridos a lo largo del Diplomado de Linux, se puede brindar solución a las cinco temáticas planteadas abordando diferentes niveles de configuración, administración y ejecución en cuanto a permisos, ficheros, usuarios y gestión de paquetes, enfrentando desafíos de la vida real en la profesión, de manera práctica que permiten resolver de forma adecuada los inconvenientes que se presenten.

## 2 INSTALACIÓN DE ZENTYAL SERVER

Se descarga la versión de Zentyal 6.2 Development desde la página oficial, ubicando el archivo .iso.

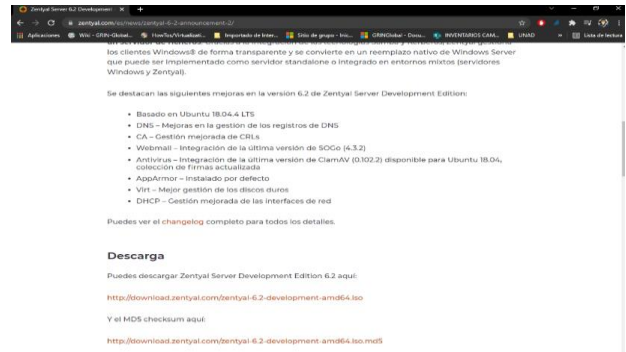


Figura 1. Descarga de Zentyal 6.2 Development.

En VirtualBox proceder a crear una nueva máquina virtual con el nombre Zentyal Server, clic en siguiente.

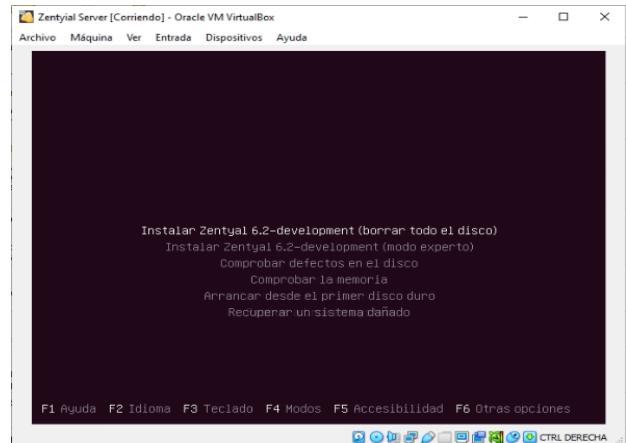


Figura 2. Selección de distribución para instalar.

A continuación, se selecciona la ubicación del país para determinar condiciones horarias, regionales y de idioma.

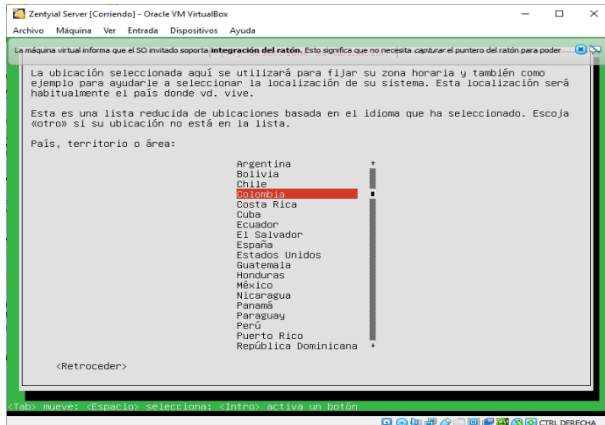


Figura 3. Selección de ubicación regional.

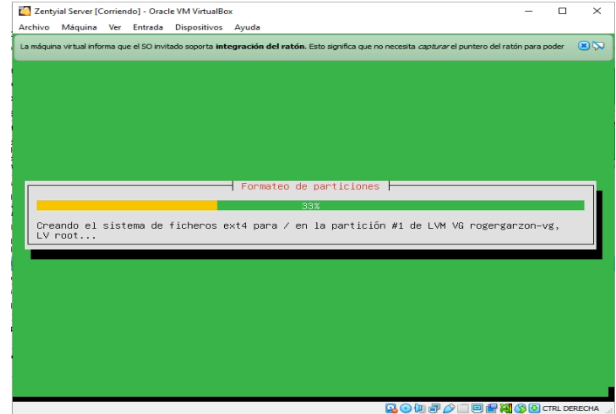


Figura 6. Instalación del sistema operativo.

Se inicia el proceso de descarga de los módulos requeridos y componentes adicionales.

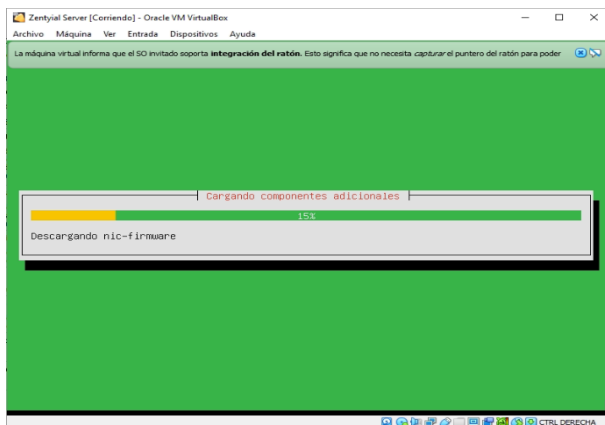


Figura 4. Descarga de módulos y componentes.

Una vez finaliza el proceso de instalación, se reinicia la máquina virtual y arranca con el nuevo sistema operativo, e inicia directamente en el panel de control de Zentyal.

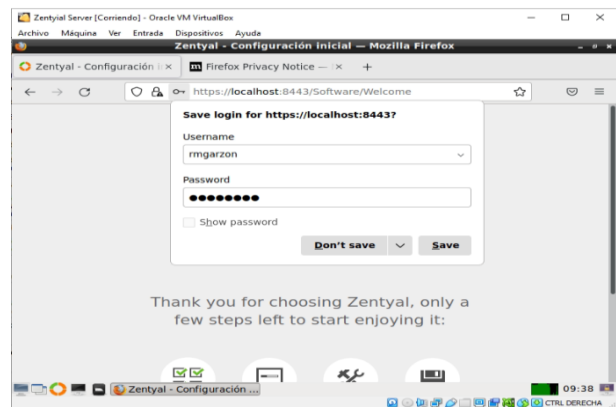


Figura 7. Ingreso al panel de control Zentyal.

Al finalizar la descarga, se inicia el proceso de asignación del hostname al servidor y el usuario administrador.

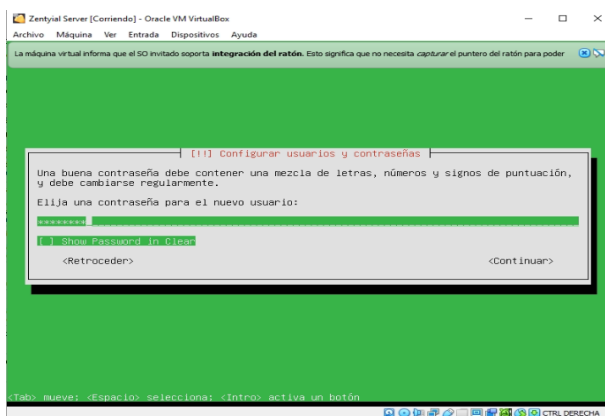


Figura 5. Asignación de hostname, usuario y contraseña.

Se procede a realizar la configuración de los paquetes a instalar para configurar los servicios requeridos.

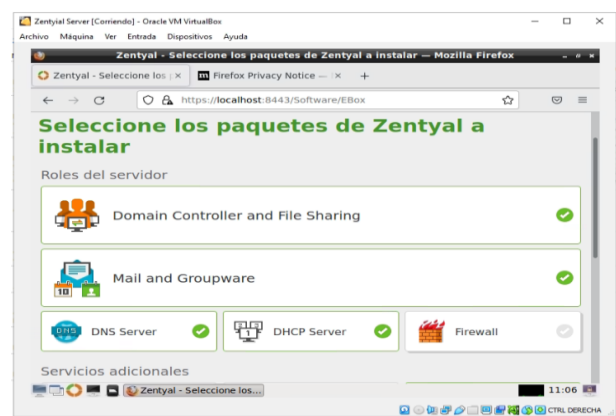


Figura 8. Instalación de paquetes en Zentyal.

Se inicia el formateo e instalación completa del nuevo sistema operativo.

### 3 TEMATICA 1.

## DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

### DHCP SERVER

Instalar y configurar DHCP server, Para repartir direcciones IP dinámicamente en nuestra red.

Primero debemos abrir el apartado de gestión de software=> Componentes de Zentyal y seleccionamos la opción de DHCP Server, vamos al final de la página y damos clic en Instalar.

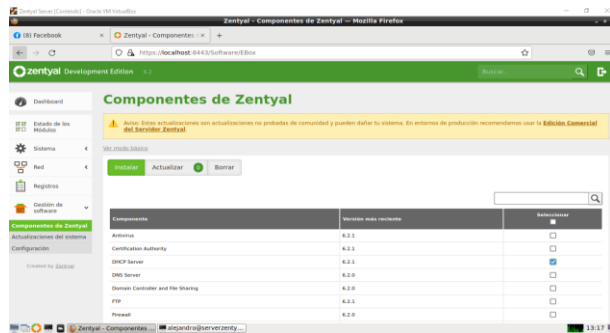


Figura 9. Componentes de Zentyal.

Nos indicara que paquetes necesita Zentyal , para continuar con la instalación, iniciando con la descarga de los paquetes requeridos.

Al finalizar la instalación de paquetes, nos avisara que el proceso se ha cumplido exitosamente.

En los componentes de Zentyal se crea las áreas de trabajo, según los paquetes que acabamos de instalar.



Figura 10. Componente DHCP agregado.

Al ingresar al área de trabajo de DHCP, nos mostrara dos advertencias, una sobre la habilitación del módulo de DHCP y otro para los rangos de las interfaces. Damos clic en configurar y vemos la siguiente ventana.

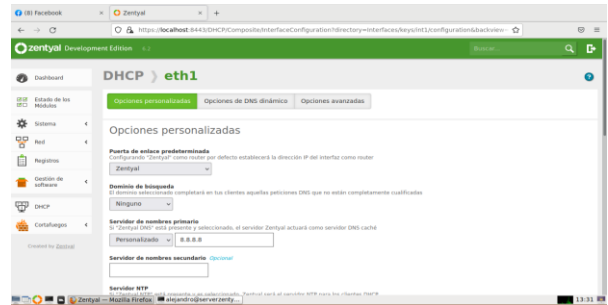


Figura 11. Opciones personalizadas.

Dejamos la configuración según la siguiente imagen y damos clic en cambiar.

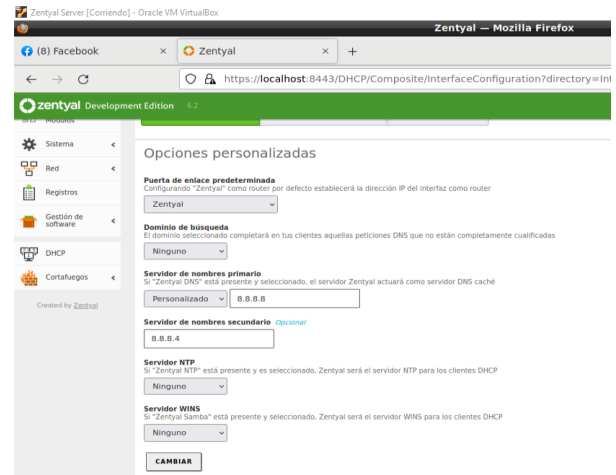


Figura 12. Personalización de interfaz.

Ahora damos clic en añadir un nuevo rango. Damos clic en añadir nuevo rango y lo dejamos según la siguiente imagen, y por último clic en añadir.



Figura 13. Rangos DHCP.

Así se mostrará el rango una vez definido.

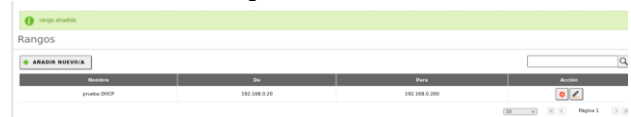


Figura 14. Rangos.

Y por último habilitamos el módulo, en la sección Estado de módulos.

Para ello habilitamos el módulo DHCP y el firewall, en el Dashboard identificamos como está funcionando el módulo DHCP. Para este caso como aún no ha conectado ninguna maquina no muestra información relevante.

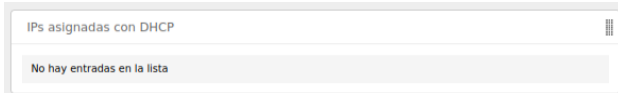


Figura 15. Verificación Ips Asignadas DHCP.

Lanzamos un pc de la red, en este caso con Windows 7, y lo conectamos al Servidor DHCP. Comprobamos la conexión, como se observa se asignó la ip 192.168.0.20 a través de la puerta de enlace 192.168.0.10

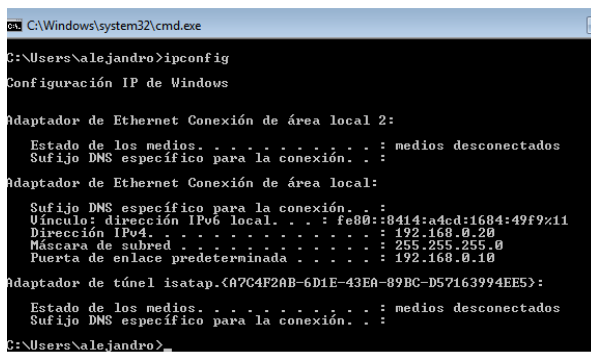


Figura 16. Asignación IP cliente.

Por último, validamos el Dashboard e identificamos que efectivamente la maquina este dentro del cuadro de IP's asignadas.

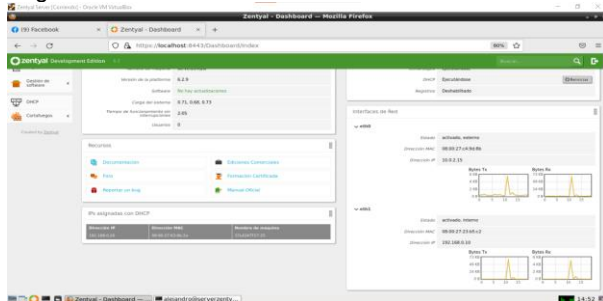


Figura 17. Nueva verificación IPs Asignadas.

## DNS SERVER

Vamos a configurar el servidor de DNS local, para ello vamos a Gestión de software => componentes Zentyal y seleccionamos la opción DNS server.

Damos clic en instalar, esperamos a que nos confirme la instalación. En el estado de módulos debemos habilitar el módulo DNS.

Ahora vamos al área de DHCP y cambiamos la configuración, para editar las direcciones DNS.

Como se muestra en la imagen, así está configurado nuestro servidor DNS, Inicialmente.

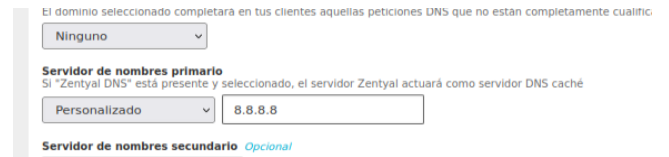


Figura 18. Configuración DNS.

Así debe quedar configurado.

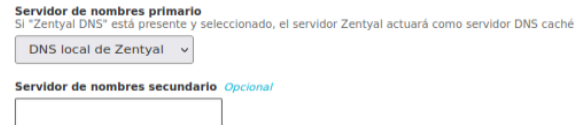


Figura 19. Servidor de nombres primario.

Ahora abrimos la maquina cliente, en este caso Windows 7. Y validamos que el servidor DNS sea la dirección del servidor 192.168.0.10

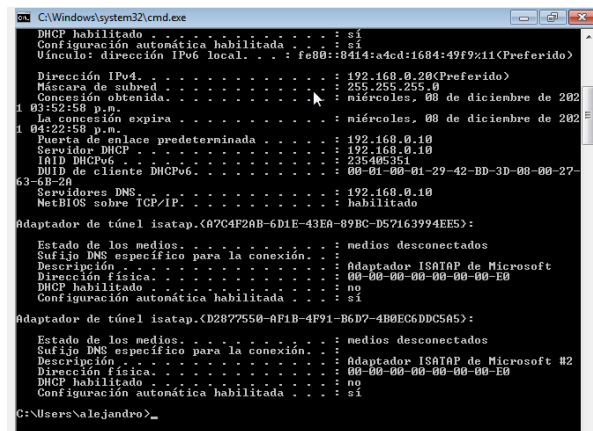


Figura 20. DNS cliente.

## CONTROLADOR DE DOMINIO

Ingresamos al panel de control, e instalamos los paquetes señalados en la siguiente imagen.



Figura 21. Paquetes a instalar.

Esperamos que se Instalen los paquetes.



Figura 22. Instalación de paquetes.

Ingresamos al apartado de dominio y realizamos la configuración como se muestra en la imagen y damos clic en cambiar y guardar cambios.



Figura 23. Configuración de dominio.

Nos preguntará si deseamos guardar estos cambios y confirmamos.

Ahora vamos a estado de módulos y allí activaremos.

- Antivirus
- DNS
- Compartición de ficheros y servicios de dominio
- NTP
- Usuarios y equipos.

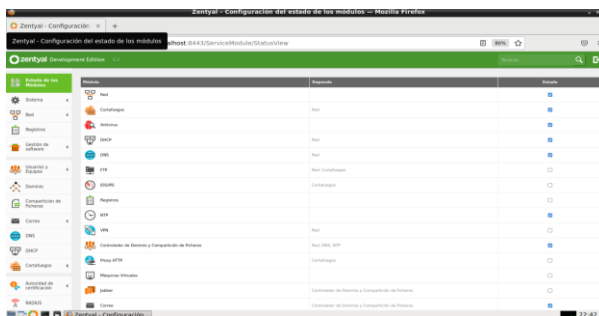


Figura 24. Selección de paquetes.

Vamos a usuarios y equipos=>gestionar. Y allí veremos nuestros usuarios y equipos y la raíz de dominio.

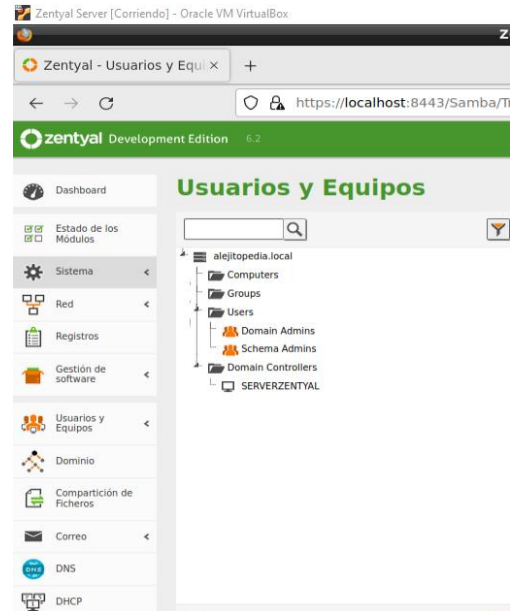


Figura 25. Usuarios y equipos.

Podemos configurar, equipos, grupos y usuarios. Damos clic en el más y se nos abrirá la siguiente interfaz gráfica, como lo muestra la imagen.



Figura 26. Añadir usuario.

En esta parte creamos un usuario con nombre de usuario, y contraseña y la asignamos a una persona real que tenga nombre y apellido. Configuramos el primer usuario, que es el director de sistemas y lo agregamos al dominio de Administradores de dominio "Domain Admins".



Figura 27. Adición de usuario.

Revisamos que se haya agregado el usuario en la carpeta de users; también en este apartado podemos editar el usuario



Figura 28. Usuarios.

Desde acá podemos configurar correo electrónico, resignar grupos de usuario y reiniciar contraseña. También podemos inhabilitar la cuenta cuando lo necesitemos.

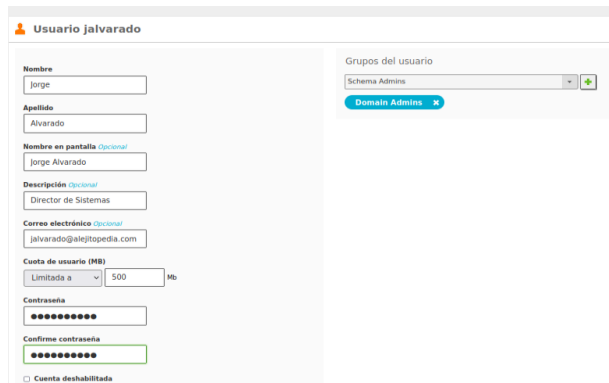


Figura 29. Edición usuario.

## 4 TEMATICA 3.

### CORTAFUEGOS

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del funcionamiento del cortafuego aplicando

las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

La administración de un cortafuegos nos permite bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, brindando seguridad y control de las comunicaciones de nuestra red computacional. Esto hace que los usuarios de internet no autorizados tengan acceso a nuestra red privada o intranet. Controlando los mensajes que entren o salgan de la intranet para que pasen a través del cortafuegos, el cual examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad que fueron especificados.

Después de realizada la instalación de Zentyal Server 6.2, se inicia el panel de control de zentyal a través del navegador, se introducen las credenciales que se configuraron en la instalación.

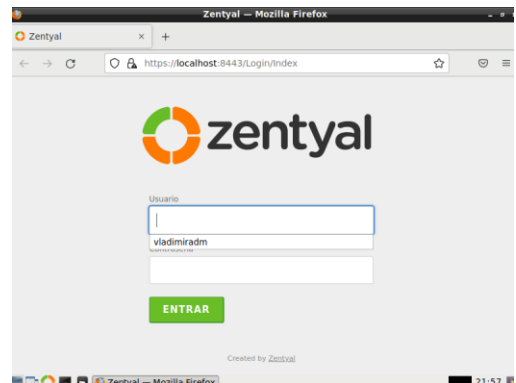


Figura 30. Loguin usuario.

Ahora se procede a realizar la instalación de los módulos necesarios, en este caso se instalará el módulo de Firewall.

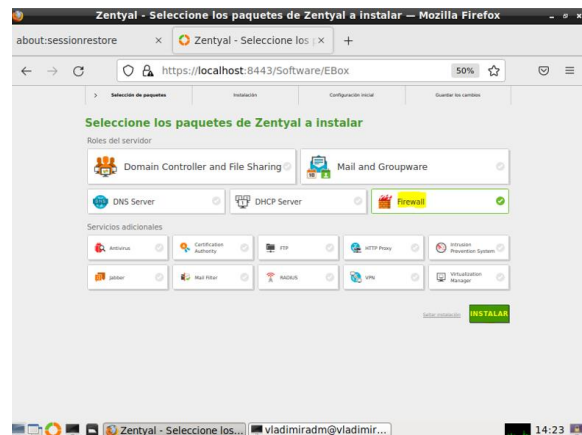


Figura 31. Instalación módulo firewall

Se configura los tipos de interfaces, que obedece a las tarjetas de red eth0, esta obedece a la interfaz externa (WAN), y la tarjeta eth1, esta obedece a la interfaz interna (LAN).



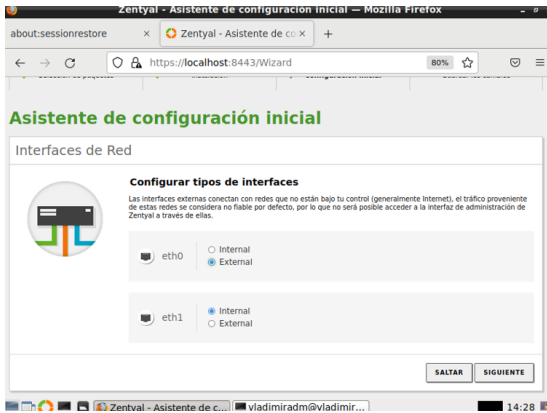


Figura 32. Configuración interfaces de red primera parte

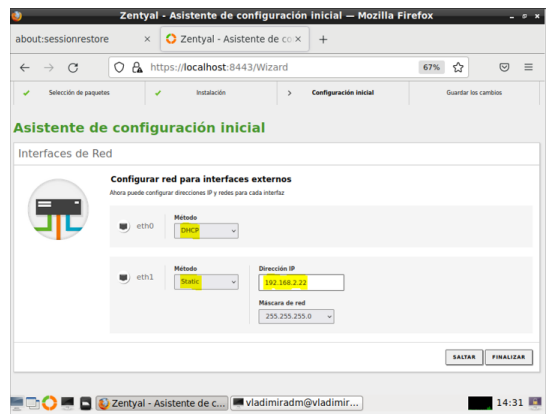


Figura 33. Config. interfaces de red segunda parte

Continuamos con la configuración y procedemos a realizar la habilitación de los registros que nos permitirán llevar un seguimiento de los cambios y posibles fallos.

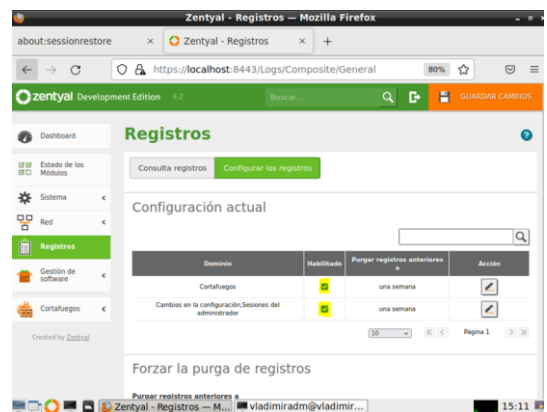


Figura 34. Habilidad de registros.

Ahora se procede a crear los objetos para la mejor administración de las reglas de firewall, se crea un objeto nombrado Redes interna para la gestión de reglas asociadas a este perfil, se añade un nuevo miembro en este caso se crea con el nombre LAN1, se asigna el segmento de red ip con el método CIDR, y la máscara asociada.

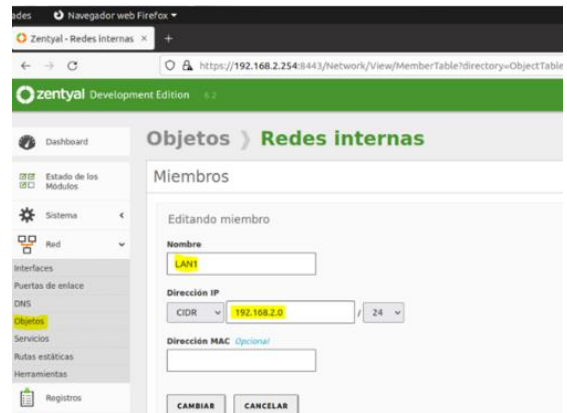


Figura 35. Creación objeto Redes internas y miembro.

Se procede a crear los servicios, en este caso para una gestión de reglas en conjunto se crea el servicio de http y https. Se selecciona el protocolo, que para efectos de eficacia se selecciona TCP/UDP, el puerto de origen dejamos por defecto cualquiera, en puerto de destino seleccionamos puerto único y escribimos el puerto, que para el primer caso http sería el 80, y el segundo caso https sería el 443.

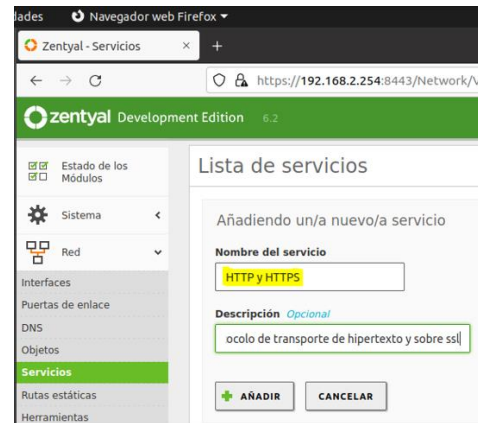


Figura 36. Creación servicio http y https.

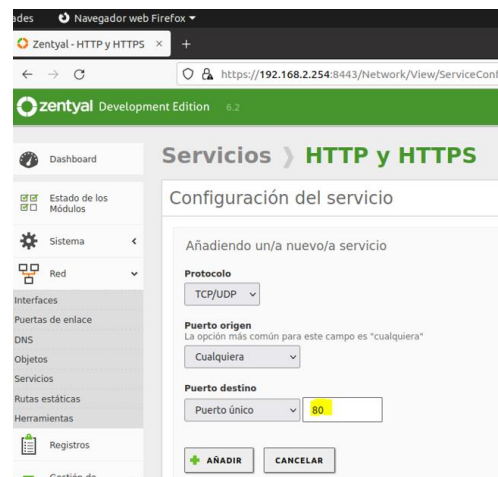


Figura 37. Config. servicio http y https para el puerto 80.

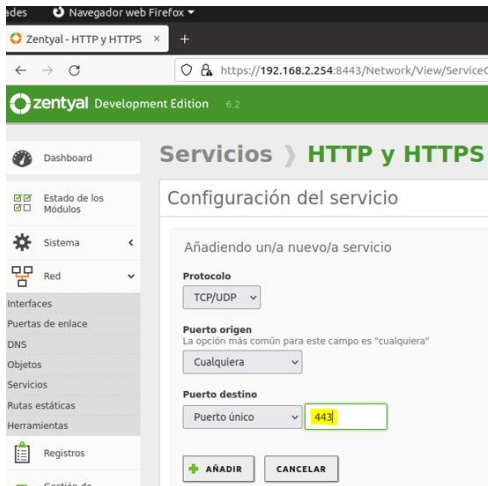


Figura 38. Config. servicio http y https para puerto 443.

Luego configuramos en la máquina cliente la puerta de enlace y servidor DNS para que se conecte a Internet a través de Zentyal.

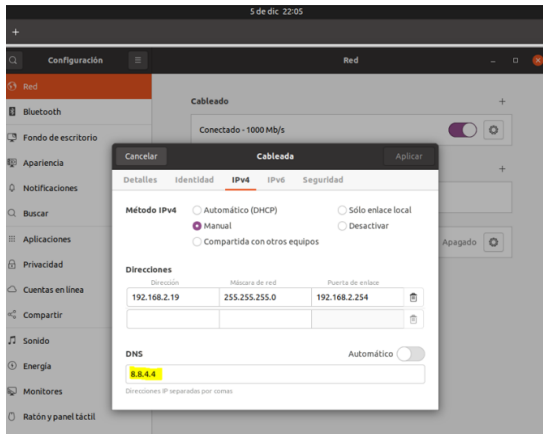


Figura 39. Configuración datos red.

Previo a la configuración de las reglas de firewall, verificamos en el equipo cliente el acceso a una página de redes sociales, en este caso Facebook, se observa que hay acceso.



Figura 40. Acceso a facebook.

En el panel de control de Zentyal, nos dirigimos al módulo cortafuegos y luego a reglas de filtrado para las redes internas.

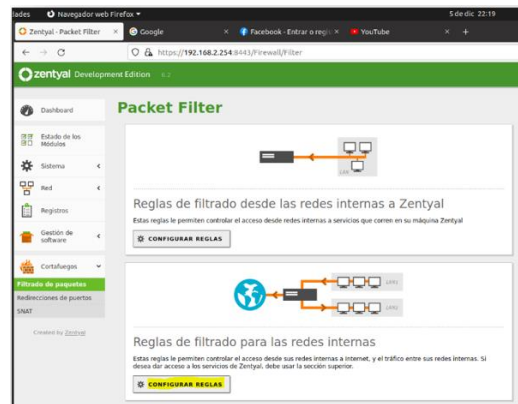


Figura 41. Reglas de filtrado para redes internas.

Ahora se comprueba con el comando “nslookup” que ip corresponde a Facebook, en este caso es 157.240.6.35.

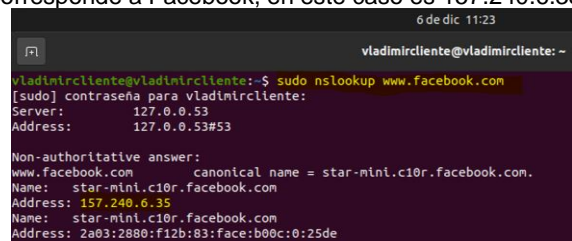


Figura 42. Obtención ip del dominio de Facebook.

Se configuran las reglas las reglas de filtrado para denegar el acceso a sitios redes sociales a partir de su IP, en este caso Facebook.

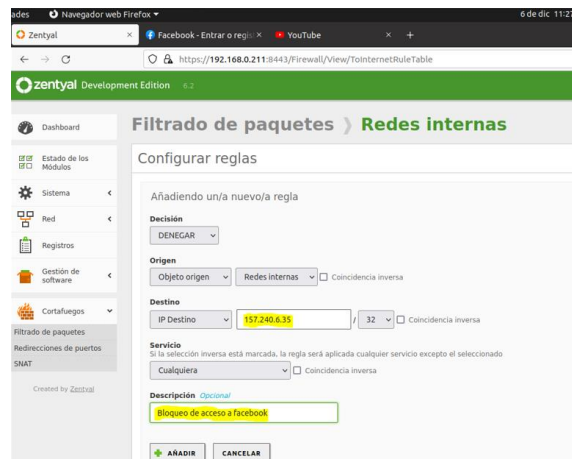


Figura 43. Regla para bloqueo de ip de Facebook.

### Resultados Obtenidos:

Después de la configuración de bloqueo, se ingresa desde el equipo Cliente a las páginas bloqueadas, en este caso Facebook y que por ejemplo el acceso a otras páginas es permitido.



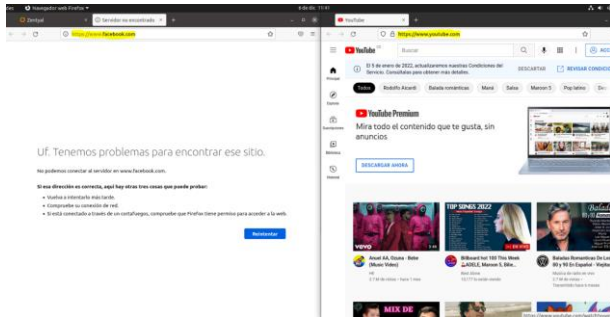


Figura 44. Evidencia bloqueo acceso a Facebook y acceso permitido a youtube.

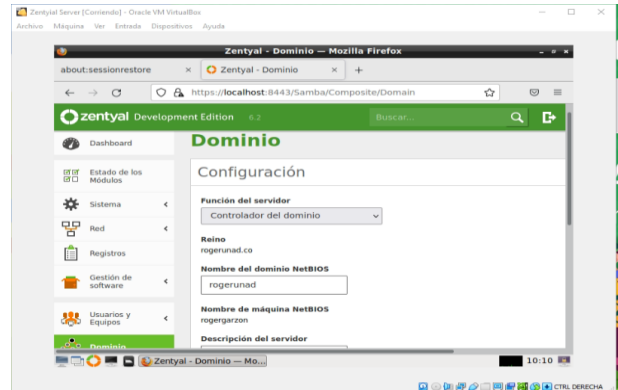


Figura 46. Configuración del dominio.

## 5 TEMATICA 4.

### FILE SERVER Y PRINT SERVER.

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Según la afirmación “El dominio en este contexto consiste en una serie de servicios distribuidos a lo largo de todos los controladores, siendo los más importantes el directorio LDAP, el servidor DNS y la autenticación distribuida mediante Kerberos” (*Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.2, 2018*)

Lo primero que se va a realizar es configurar la tarjeta de red, dejando la IP manera estática.

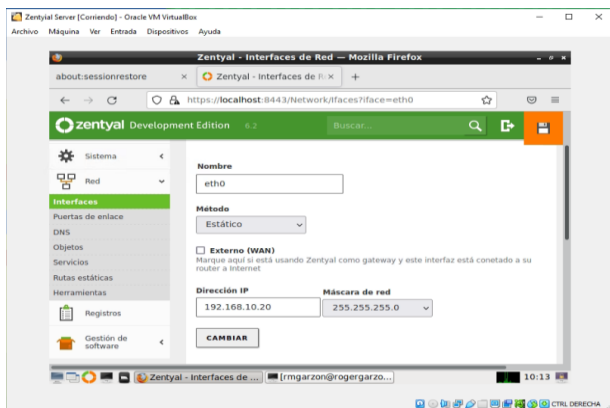


Figura 45. Configuración IP estática.

Lo próximo que se va a realizar es asignar un dominio, a través de la opción Dominio para crear el directorio activo, rogerunad.co.

Dentro del módulo de Usuarios y Equipos se pueden validar los diferentes perfiles de usuario y computadores dentro de los grupos de trabajo existentes, allí se creará un nuevo usuario.

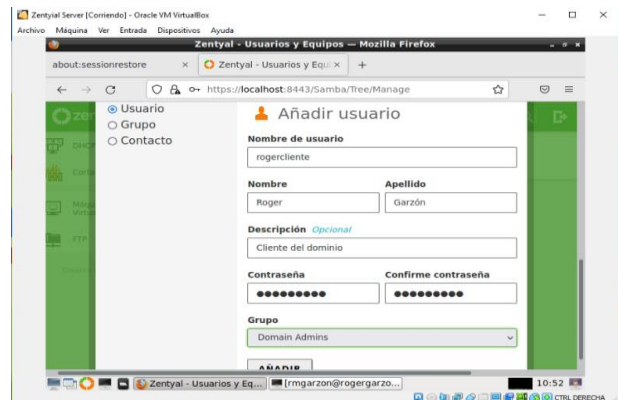


Figura 47. Creación de usuario en el dominio.

Ahora se puede verificar que la creación del usuario cumpla con las condiciones requeridas.

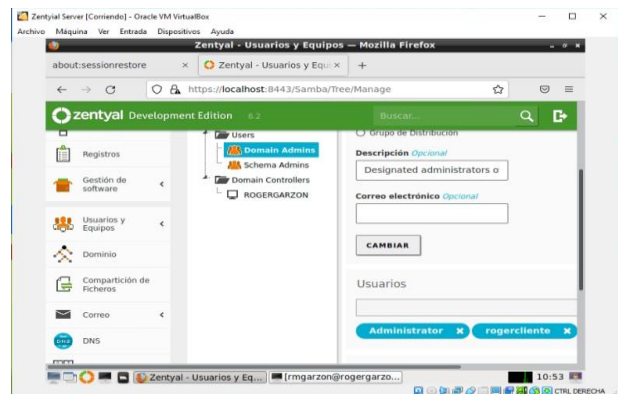


Figura 48. Verificación usuario en dominio.

Una vez creado el usuario dentro del Directorio Activo se procede a unir el equipo cliente con sistema operativo Linux distribución Ubuntu 18.04, para esto es necesario

descargar un cliente de configuración y administración del Directorio Activo llamado pbis-open.

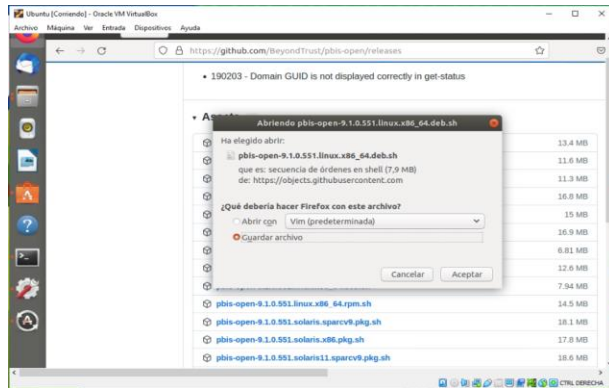


Figura 49. Descarga de pbis-open.

Una vez descargado se procede a dirigirse a la carpeta de descargas y asignarle permisos de ejecución y luego se realiza la instalación con el comando con la orden “.”

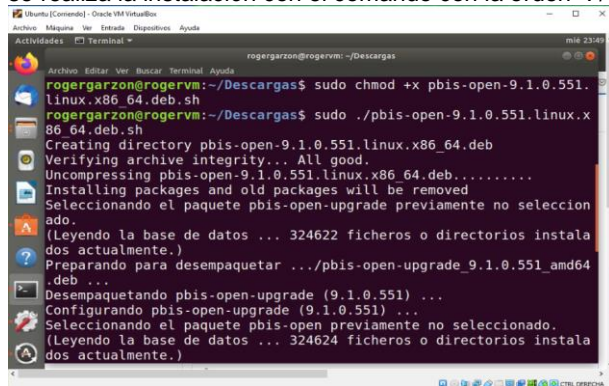


Figura 50. Instalación de pbis-open.

Al finalizar la instalación se procede a unir al equipo cliente al dominio a través del comando sudo domainjoin-cli join rogerunad.co rogercliente agregando tanto del directorio activo del servidor como el usuario creado previamente.

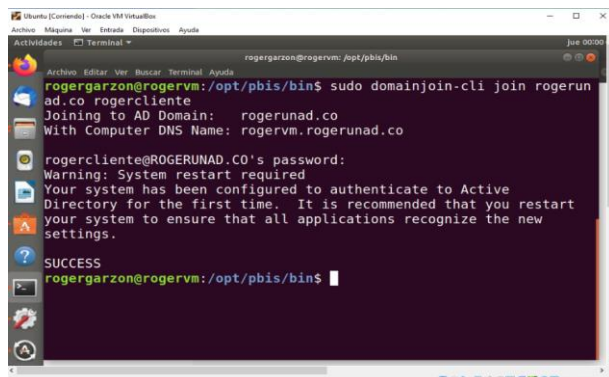


Figura 51. Unir equipo cliente al dominio

Al quedar asociado el computador cliente al dominio, se reinicia y se puede iniciar sesión con las credenciales definidas en Zentyal.

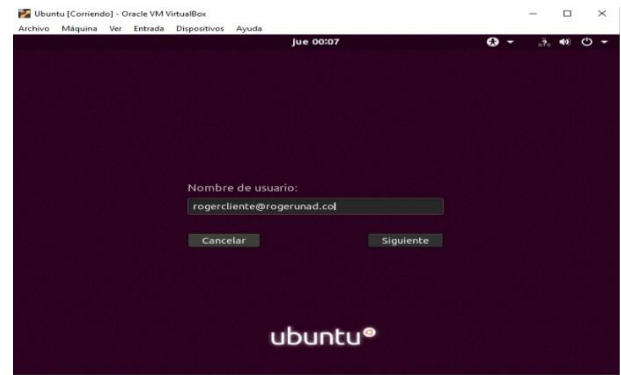


Figura 52. Inicio de sesión con credenciales de dominio.

Al ingresar con las credenciales, se puede observar en el módulo de usuarios y equipos que el computador cliente ya se encuentra dentro del directorio activo y su nombre es ROGERVM

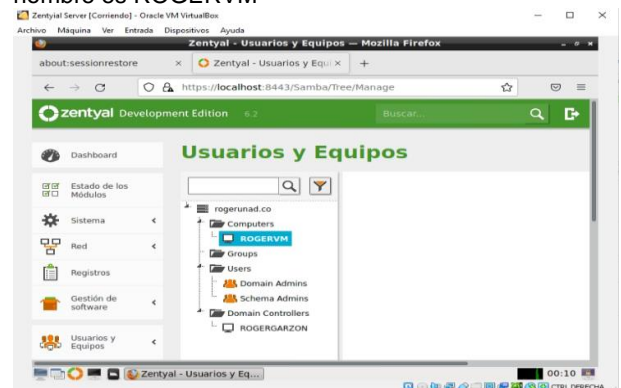


Figura 53. Validación de equipo asociado al AD.

Una vez se ingresa al escritorio con el Login del directorio activo y estando conectado al dominio creado en Zentyal se puede proceder con el File Server y Print Server

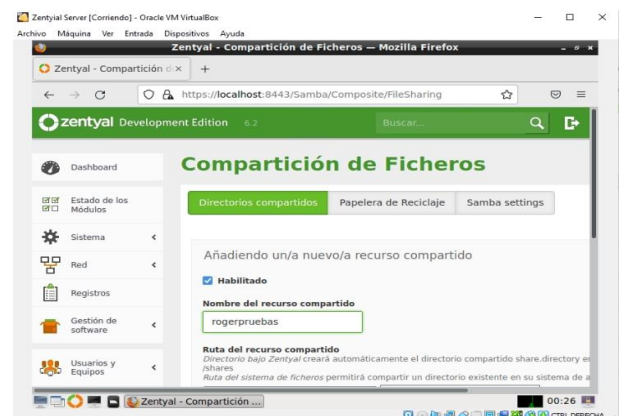


Figura 54. Creación de recurso compartido.

Dentro del menú **Compartición de Ficheros** se crea el nombre del nuevo recurso compartido y se asigna el directorio donde estará permitido su uso. El nombre es **rogerpruebas** y se asocia al usuario **rogercliente** con permisos de lectura y escritura.

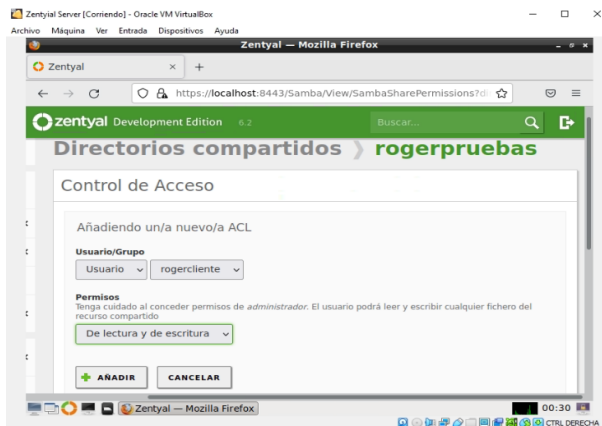


Figura 55. Asignación de usuario a recurso compartido. Se ingresa desde el equipo cliente y solicita las credenciales del usuario creado en el directorio activo.

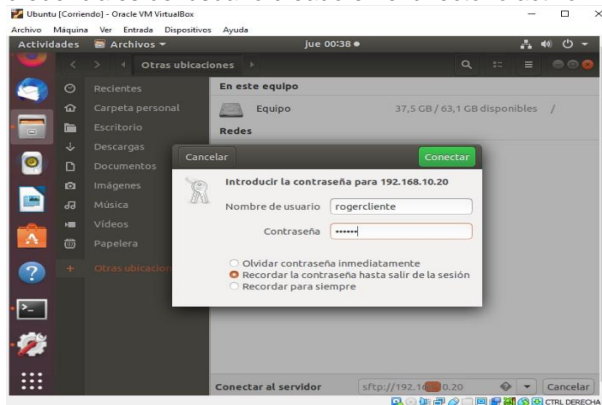


Figura 56. Conexión al recurso del servidor.

Al finalizar conexión con el directorio activo, se puede acceder al recurso compartido y trabajar con los permisos otorgados desde el servidor.

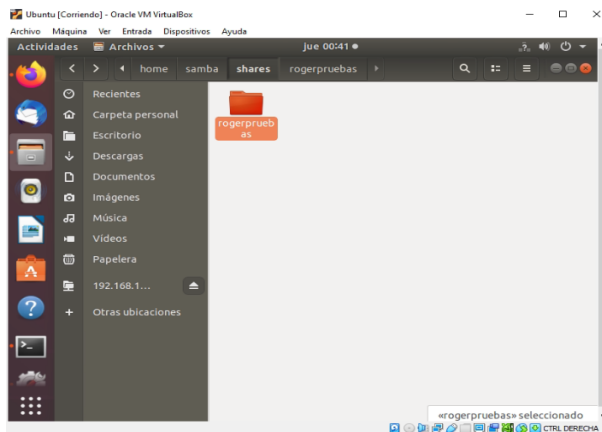


Figura 57. Ingreso al recurso con permisos asociados.

Dentro del servidor Zentyal es necesario instalar el servicio de impresión cups, mediante el comando `sudo apt-get install cups cups-client cups-pdf`

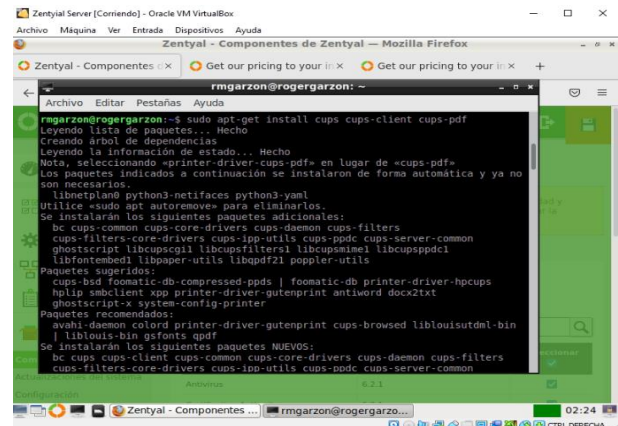


Figura 58. Instalación del servicio CUPS.

Una vez finalizada la instalación se ingresa por el puerto 631 y se crea la nueva impresora

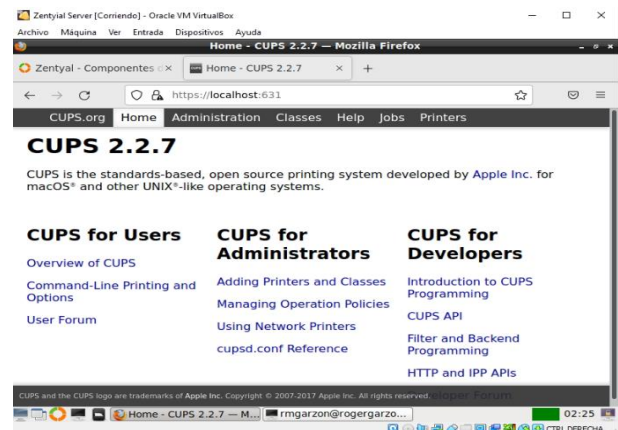


Figura 59. Creación de impresora en el servidor.

Se crean los datos de la impresora, nombres y ubicación. Seleccionar la opción de compartir la impresora para que pueda ser vista por el cliente.

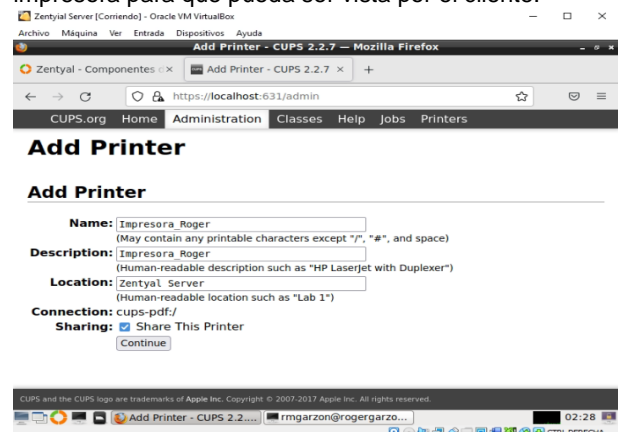


Figura 60. Parametrización de la impresora compartida.

Ahora del lado del cliente, se busca la nueva impresora, con la dirección IP del servidor Zentyal

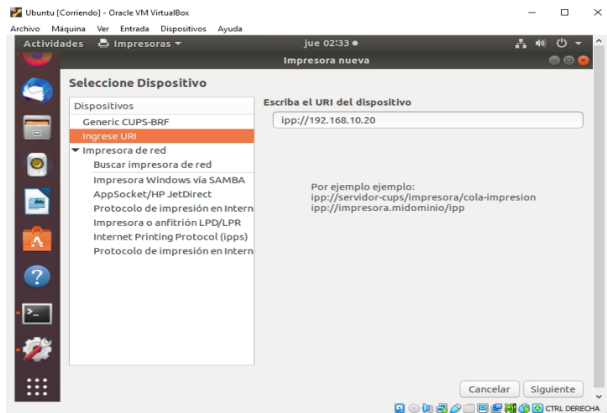


Figura 61. Conexión con impresora desde cliente.

La impresora ha sido creada exitosamente y es compartida desde el servidor Zentyal hacia el cliente mediante el directorio activo conectado.

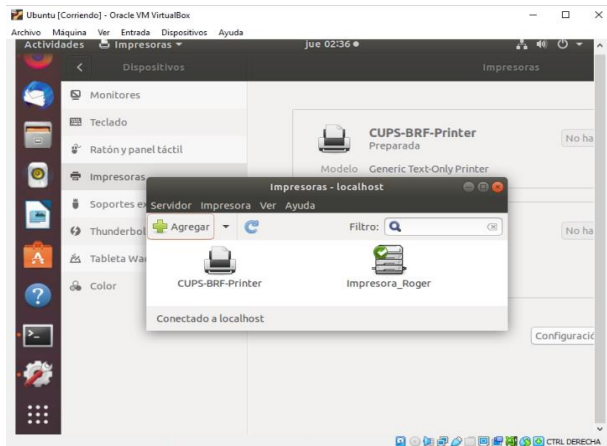


Figura 62. Finalización de instalación de impresora.

## 6 TEMATICA 5.

### VPN.

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Para la implementación y configuración de la VPN lo primero que se hace es ingresar a localhost, esto se debe hacer una vez se finalice la instalación del sistema

operativo Zentyal, tal y como se aprecia en las siguientes 2 imágenes:

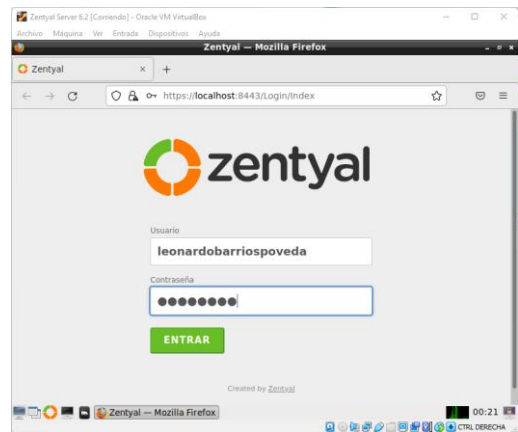


Figura 63. Se ingresa a la configuración desde localhost.



Figura 64. Se inicia con la configuración de Zentyal.

Después de esto, e procede a realizar la instalación del paquete de VPN

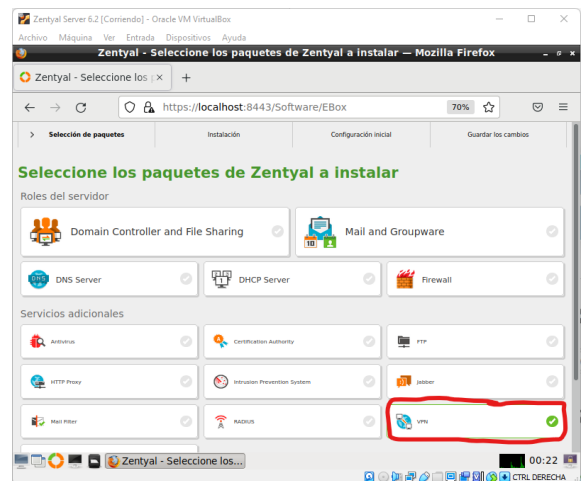


Figura 65. Se selecciona VPN

Se configuran los tipos de interfaces. Para este caso se utilizará una interna y una externa.



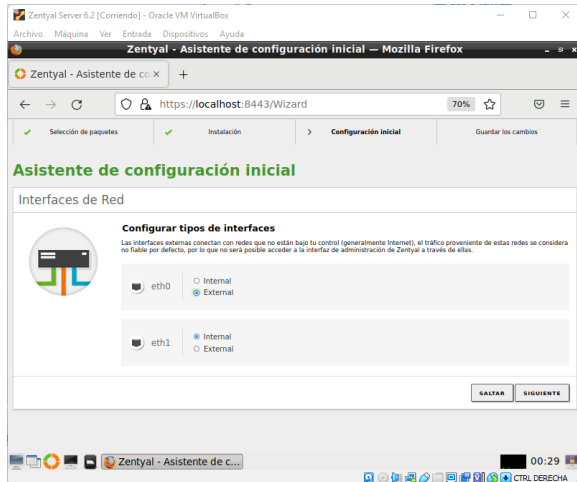


Figura 66. Se configuran los tipos de interfaces.

Se crea el certificado de la autoridad de certificación

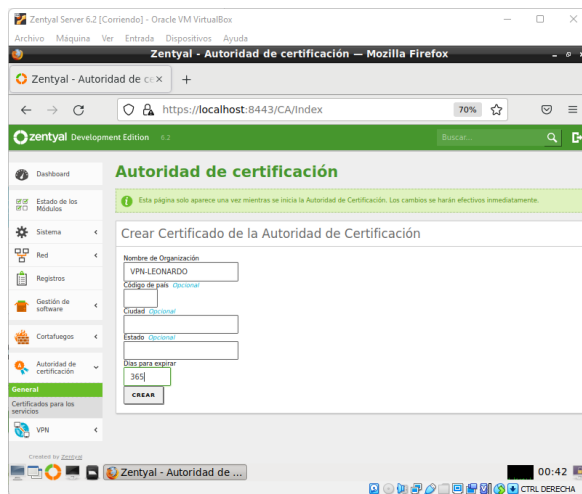


Figura 67. Creación certificado autoridad de certificación.

Se añade un nuevo servidor para poder continuar con la configuración de manera correcta

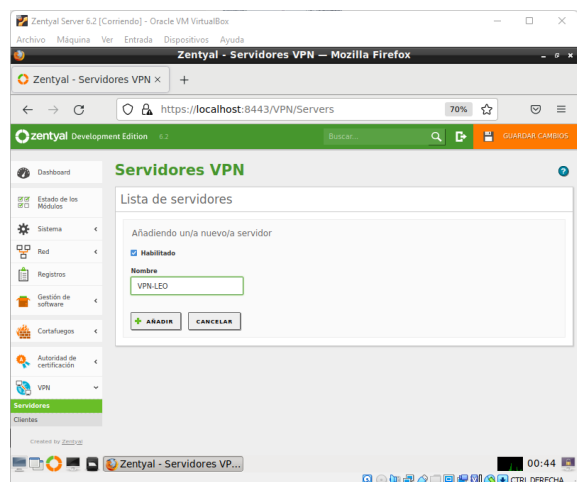


Figura 68. Se añade un nuevo servidor VPN.

Se configura el servidor con la IP que se desea utilizar

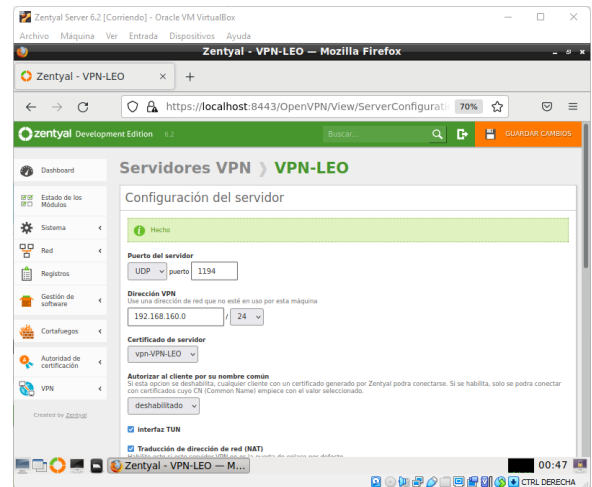


Figura 69. Configuración puerto, dirección VPN y activación interfaz TUN.

Se expide el nuevo certificado que es el que se va a utilizar para la conexión desde el cliente.

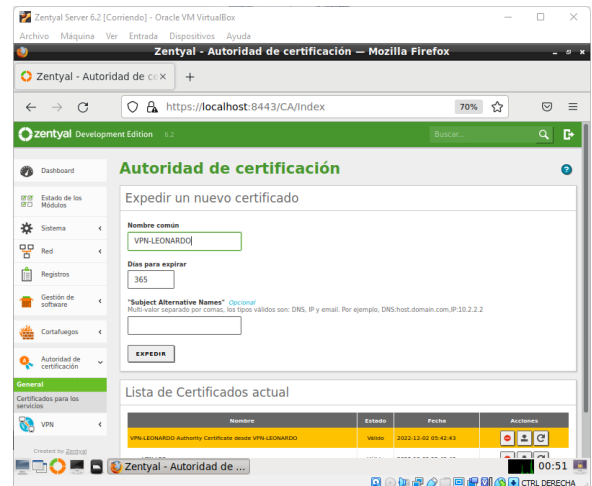


Figura 70. Se crea un nuevo certificado válido.

Se descarga el certificado para su posterior instalación en la maquina cliente.



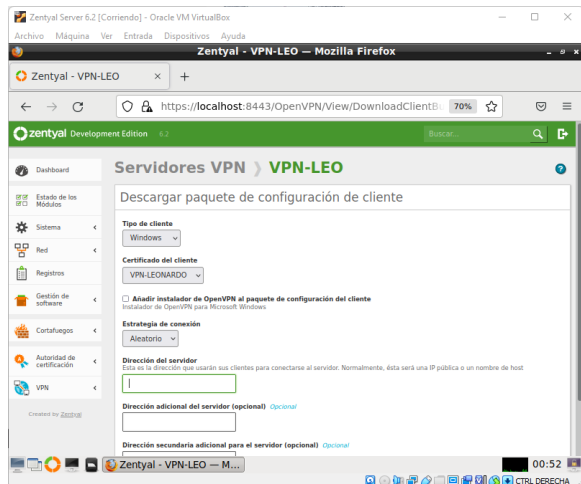


Figura 71. Se descarga el certificado.

Se carga el certificado en la maquina cliente por medio de OpenVPN

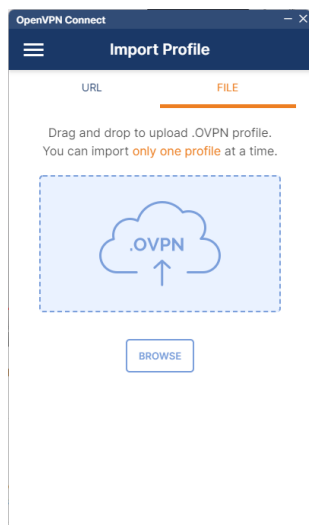


Figura 72. Se carga el certificado.

Se realiza la conexión después de que el certificado esté correctamente cargado.

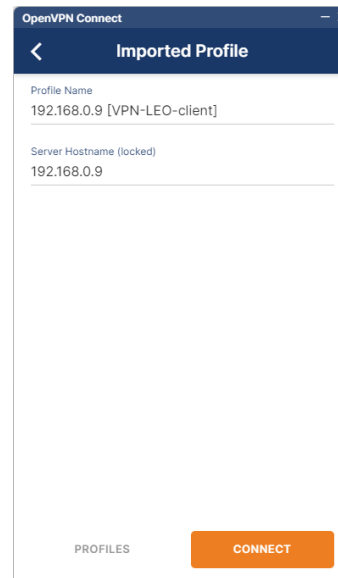


Figura 73. Se confirman los datos y se realiza la conexión.

Se confirma que la conexión se realiza de manera exitosa

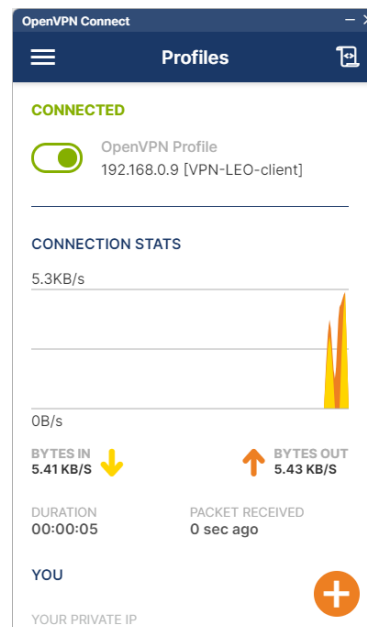


Figura 74. Conexión realizada de manera exitosa.

## 7 CONCLUSIONES

Demostramos gráficamente como se realiza la instalación de Zentyal 6.2 y realizamos las configuraciones de los Servicios DHCP Server, DNS Server y Controlador de dominio, Demostrando las habilidades adquiridas durante el desarrollo del presente Diplomado, hicimos pruebas de conexión con el pc cliente validando y demostrando que los servicios se ejecutaban correctamente.

Se observa la importancia que tiene la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas que permite la administración y control de una distribución GNU/Linux basada en Ubuntu, a través de la administración de un cortafuegos nos permite bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, brindando seguridad y control de las comunicaciones de nuestra red computacional.

Se logra conectar de manera efectiva el servidor y asociar el servicio LDAP para crear un directorio activo que permita configurar usuarios, contraseñas y permisos para un manejo efectivo en una red corporativa. Las carpetas compartidas y el servidor de impresoras representan una gran utilidad en las labores cotidianas de una organización, tener predeterminados los permisos y niveles de alcance de cada usuario otorgan un mayor control y seguridad en los permisos definidos.

Se logra instalar y configurar la VPN de manera correcta, se confirma su correcto funcionamiento y conexión con el servidor desde la máquina cliente. Se evidencia la importancia de realizar una correcta configuración de la VPN.

## 8 REFERENCIAS

Offensive Security. (2020). Kali dentro de VirtualBox (VM invitada). Recuperado de <https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/>.

LaCroix, J. (2016). Mastering Ubuntu Server. Packt Publishing. Paginas (325 – 348). Recuperado de [https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1292906&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp\\_348](https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1292906&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_348)

Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. (Páginas. 291 - 296). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=291>

Jorba, J. (2012). Administración de seguridad. Paginas (27 – 33). Recuperado de [http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU\\_Linux\\_M%C3%B3dulo\\_4\\_Administraci%C3%B3n%20de%20seguridad.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo_4_Administraci%C3%B3n%20de%20seguridad.pdf)

Jorba, J. (2012). Administración de seguridad. Paginas (27 – 33). Recuperado de [http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU\\_Linux\\_M%C3%B3dulo\\_4\\_Administraci%C3%B3n%20de%20seguridad.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo_4_Administraci%C3%B3n%20de%20seguridad.pdf)

Zentyal S.L. — Documentación de Zentyal 6.2. (2018). Cortafuegos [En línea]. <https://doc.zentyal.org/6.2/es/firewall.html>

Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.2. (2018). Controlador de Dominio y Compartición de Ficheros [En línea]. <https://doc.zentyal.org/6.2/es/directory.html>

Sanz Mercado, P. (2014). Seguridad en linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 61 - 105). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=61>