# IMPLEMENTACIÓN DE SOLUCIONES ESPECÍFICAS EN ZENTYAL SERVER SOBRE INFRAESTRUCTURAS DE SERVICIO TI

Universidad Nacional Abierta y a Distancia UNAD, Escuela de ciencias básicas Tecnología e Ingeniería ECBTI. Colombia
Mayo de 2021

Luis Alejandro Ferro Bejarano
laferrob@unadvirtual.edu.co
Alejandro Arias Gallo
aariasga@unadvirtual.edu.co
Oscar Mauricio Morales Agudelo
ommoralesa@unadvirtual.edu.co
Hermes Yezid Melo Montenegro
hymelomo@unadvirtual.edu.co
Cristian Valencia Peña
Cristian.valencia2727@hotmail.com

**RESUMEN:** *El presente documento informa acerca de la instalación y configuración del sistema operativo Zentyal Server 6.2, implementando servicios como el DHCP server, DNS server, controlador de dominio, proxy no transparente, cortafuegos, file server, print server y VPN con el fin de demostrar las bondades y virtudes de este servidor en la administración de servicios.*

**PALABRAS CLAVE**: Sistema operativo, Zentyal, servidor, cliente, ip, usuarios, DHCP, dominio, proxy, Linux, Ubuntu, Servidor.

## INTRODUCCIÓN

El presente documento evidencia la instalación y configuración del servidor zentyal 6.2, implementando la administración de servicios que permitirán una mayor seguridad y protección de los datos, como lo son el DHCP server, DNS server, controlador de dominio, que permite el acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña.

Implementación y configuración del proxy no transparente, controlando el acceso de una estación GNU/Linux a los servicios de conectividad a internet desde zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

Implementación y configuración de un cortafuego, restringiendo la apertura de sitios o portales web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas.

File server y print server, permitiendo acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Creación de una VPN que permita un túnel privado de comunicación con una estación de trabajo GNU/Linux.

## INSTALACIÓN DE ZENTYAL SERVER

Nombre máquina virtual

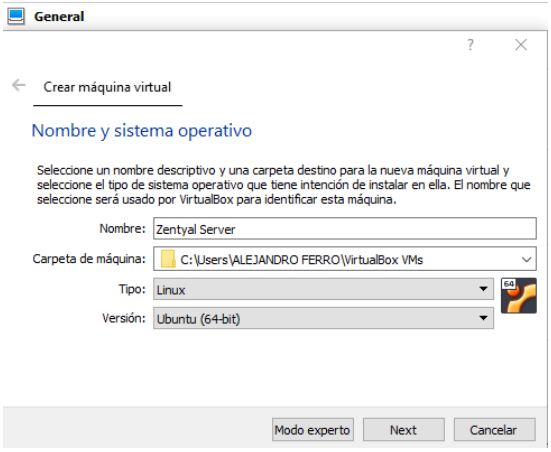


Figura 1. Nombre sistema operativo

Asignación de memoria RAM para la máquina virtual

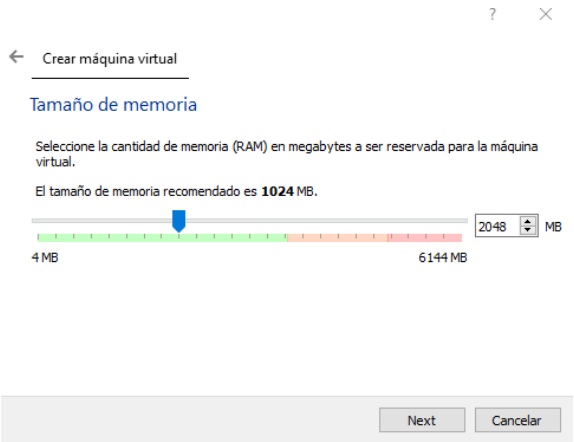


Figura 2. Tamaño de memoria RAM

Configuración de la máquina virtual

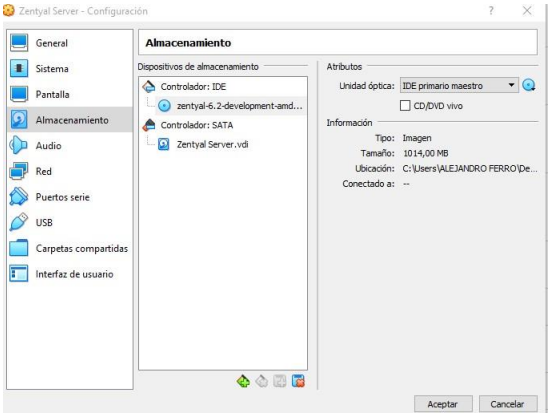


Figura 3. Configuración de la máquina virtual

Elegir el idioma del sistema operativo

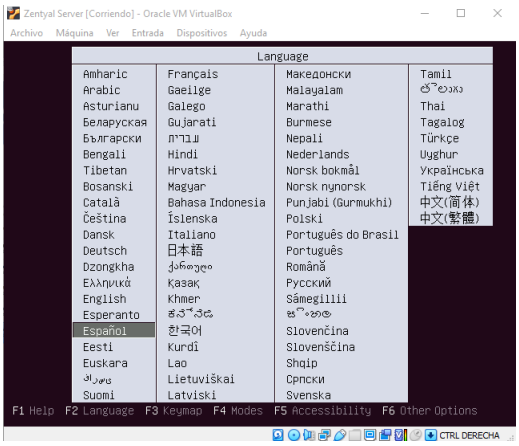


Figura 4. Idioma del sistema operativo

Elegir en instalar zentyal 6.2, dar la tecla enter

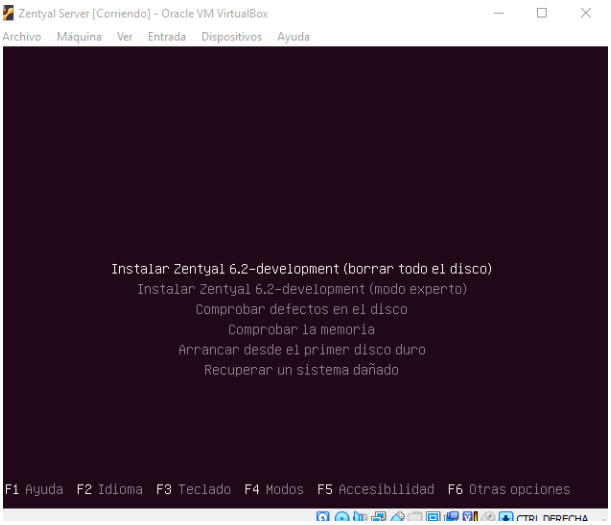


Figura 5. Menú instalación zentyal 6.2

Elegir la ubicación (País)

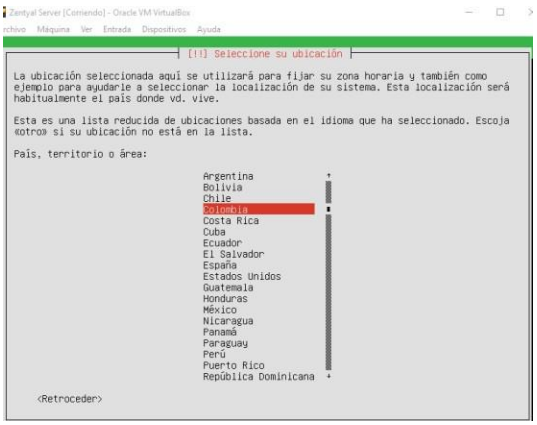


Figura 6. Elegir el país

Configurar el teclado

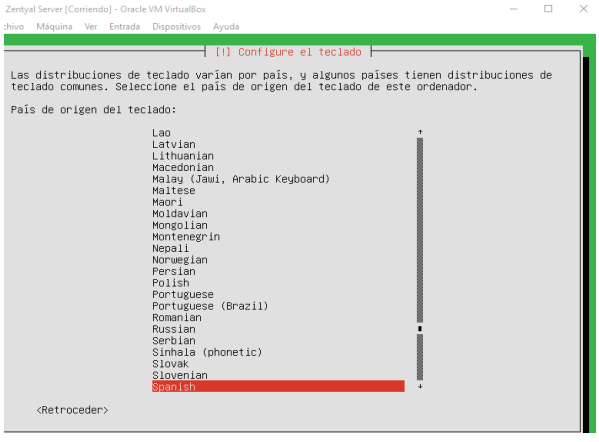


Figura 7. Configuración del teclado

Cargando componentes adicionales

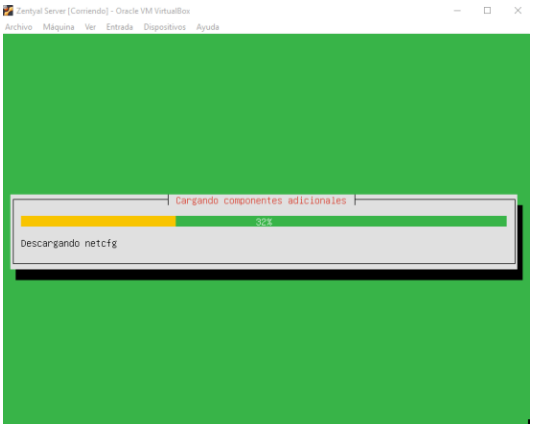


Figura 8. Cargando componentes

Configuración de red

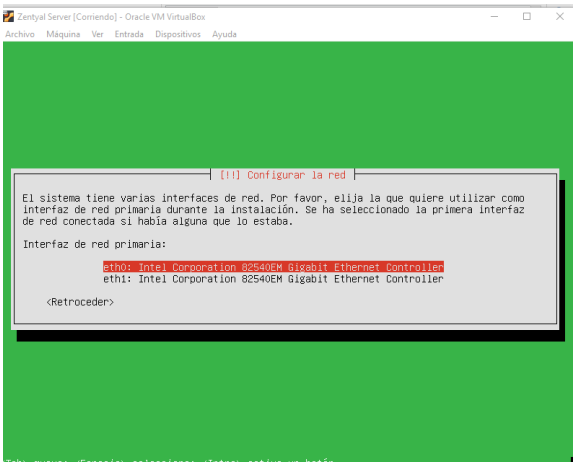


Figura 9. Configuración de red

Configurar el nombre de la maquina

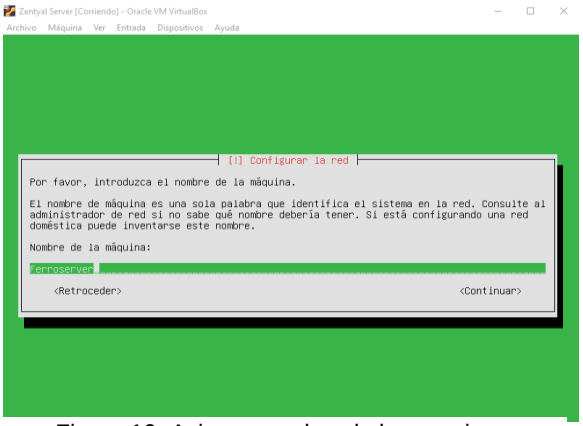


Figura 10. Asignar nombre de la maquina

Nombre de usuario

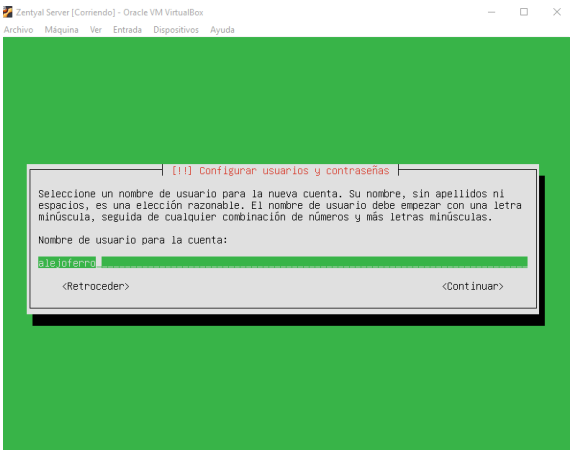


Figura 11. Asignar nombre de usuario

Elegir contraseña

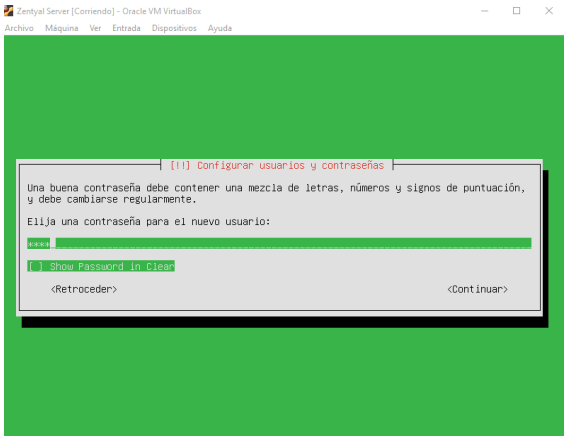


Figura 12. Asignar contraseña de usuario

Configuración de reloj

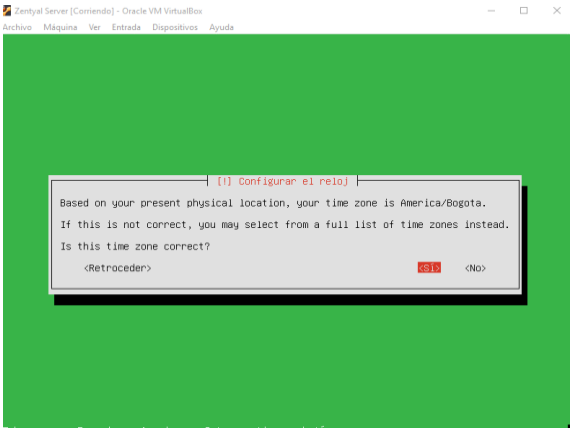


Figura 11. Configuración del reloj

Instalando el sistema operativo

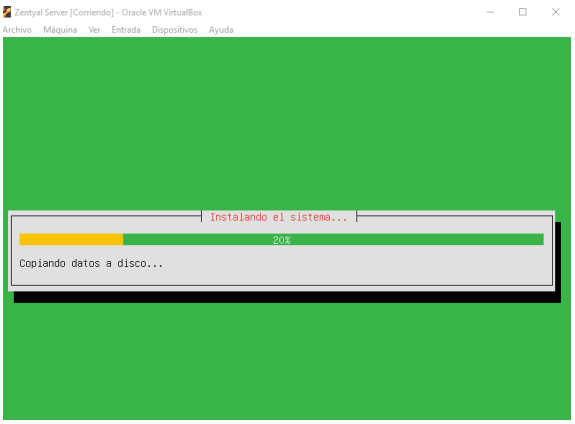


Figura 12. Instalando el sistema operativo

Instalando programas

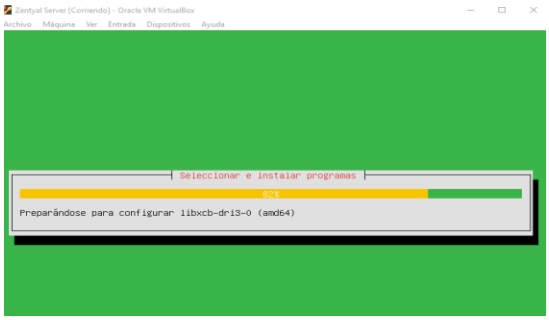


Figura 13. Instalación de programas

Inicio de sección para entrar a la configuración del servidor


Figura 14. Inicio de sesión

Configuración inicial del servidor Zentyal, le damos en continuar


Figura 15. Configuración inicial del servidor Zentyal 6.2

**TEMATICA 1 DHCP Server, DNS Server y Controlador de dominio.**

Instalación y configuración sistema Zentyal. Se configura usuario y contraseña:


Figura18. Interfaz gráfica de administración.

Se muestra a continuación las funcionalidades del sistema, se señalan los componentes que se instalarán en nuestro sistema, para nuestro ejercicio DNS y DNS Server y Controlador de dominio:

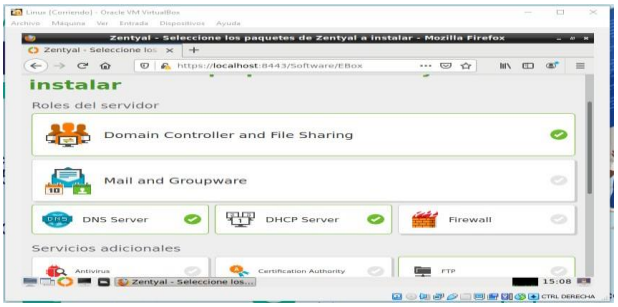


Figura 19. Interfaz gráfica de administración

Luego se realiza la implementación de los servicios DHCP y DNS server y el controlador de dominio bajo Zentyal Server 6.2.

**DHCP Server:**

Seguidamente se realiza la configuración de la red, donde se debe definir la interfaz de red como la interna o externa, para nuestro caso definimos la Externa


Figura 20. Configurar tipos de interfaces.

Luego a través del asistente de configuración inicial, se configura la red para interfaces externos, por el método DHCP.


Figura 21. Configurar de red método DHCP.

Ya definidas las interfaces de red, se configura nuestro dominio y se selecciona tipo de servidor:

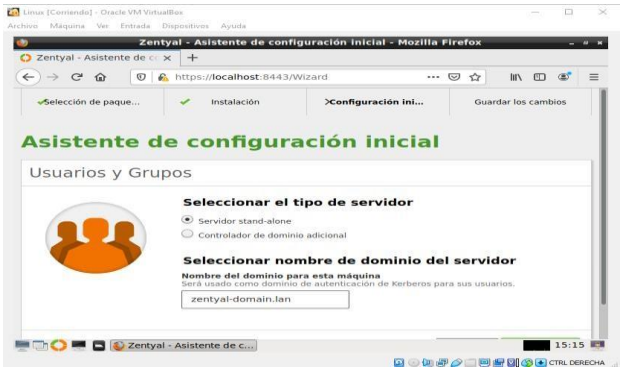


Figura 22. Configurar dominio local del servidor

El sistema nos muestra que la instalación fue completada

Ya luego nos muestra el sistema el Módulo de Interfaces, se procede a la configuración de una interfaz estática.

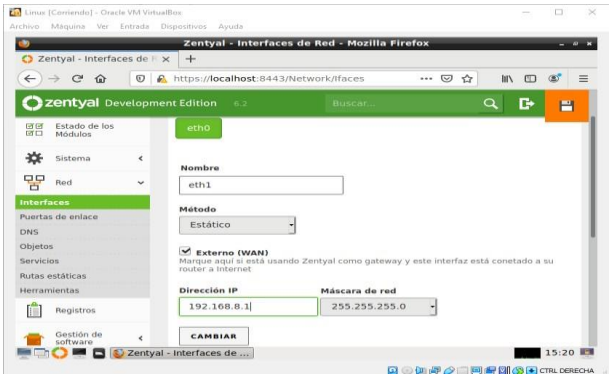


Figura 23. Interfaz nombre eth1.

Posterior se realiza la configuración de los rangos DHCP, y se asignan las IP's

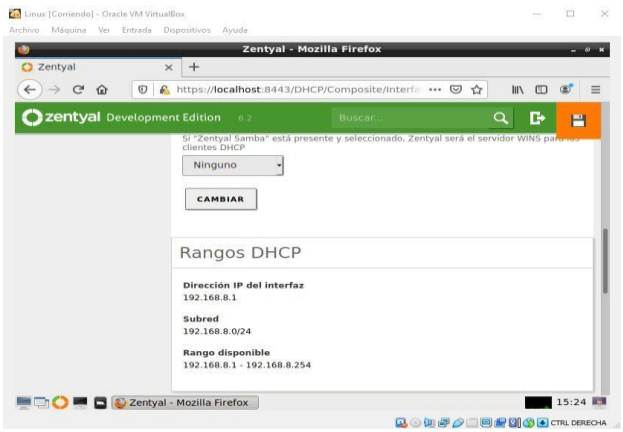


Figura 24. Segmento de red Rangos DHCP

Como se puede, se muestra el nombre del servidor 'Yezid DHCP' y los rangos de red asignados.

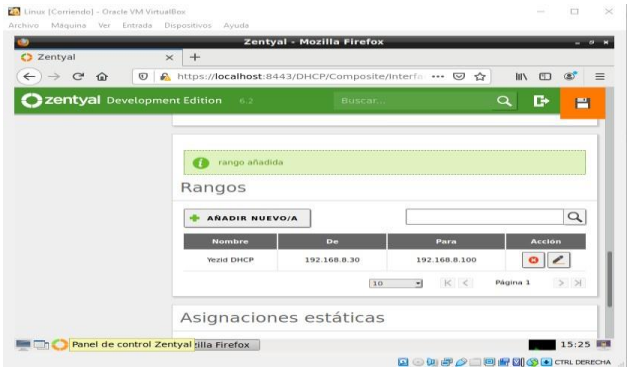


Figura 25. Direccionamiento IP Rangos definidos

Ya, por último, se muestra el estado de los módulos  configuración del estado de los módulos ‘DHCP’

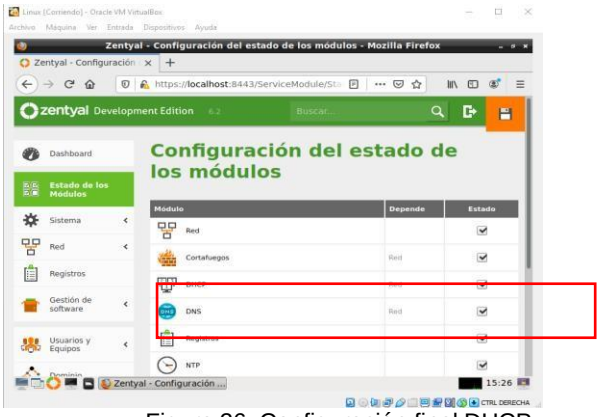


Figura 26. Configuración final DHCP

**DNS Server**

Luego de haber instalado los paquetes correspondientes al DNS y habilitado el mismo, se añade un nuevo dominio, por defecto el sistema presenta el ‘zentyal-domain.lan’.

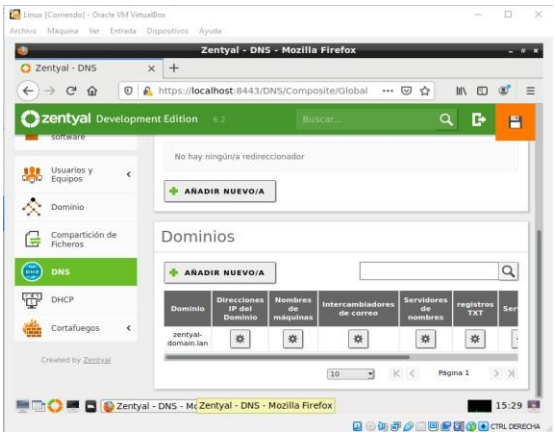


Figura 27. Configuración final DHCP

Seguidamente y en la configuración realizada al DHCP, se procede a habilitar los DNS en los clientes.

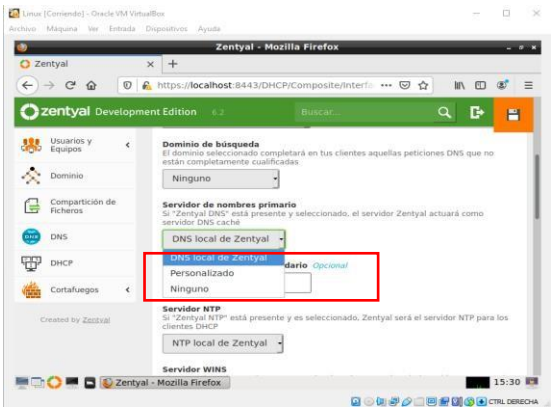


Figura 28. DNS local en servicio DHCP

**Controlador de Dominio:**

De manera siguiente y luego de haber instalado los paquetes correspondientes módulo del controlador de dominio, la imagen nos muestra la información general referente al dominio:

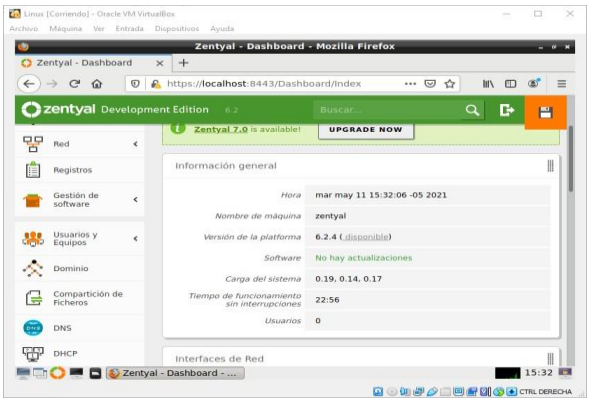


Figura 29. Información general del Dominio

Ahora se muestra el ‘Dominio’ y nos presenta la información en relación a la Configuración y descripción del servidor en uso.

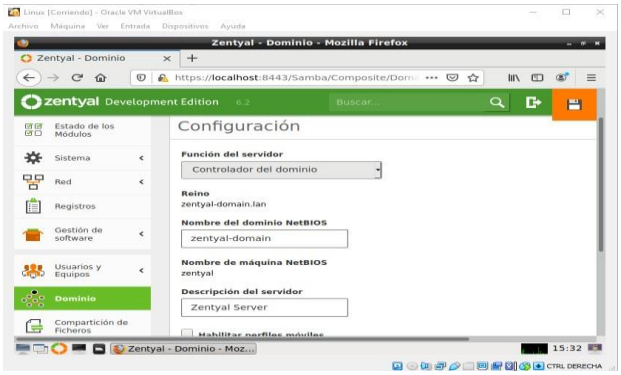


Figura 30. Información configuración del Dominio

Posterior se procede a ‘Añadir usuario’, se ingresan los datos a registrar:

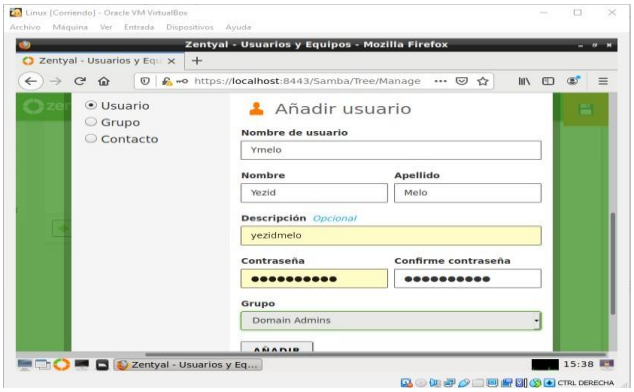


Figura 31. Añadir usuario en el dominio

Luego de ello, se muestran los Usuarios y Equipos que presenta el Dominio.

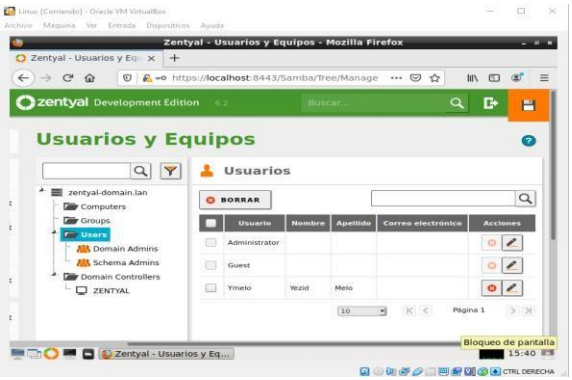


Figura 32. Usuarios y equipos del dominio

## TEMÁTICA 2 PROXY NO TRANSPARENTE

Para la temática proxy no transparente, los módulos a utilizar en el servidor del Zentyal, son los módulos de DHCP server, HTTP Proxy. Una vez seleccionado los módulos
el sistema nos muestra los módulos seleccionados y pregunta si deseamos instalarlos, se le da en instalar.

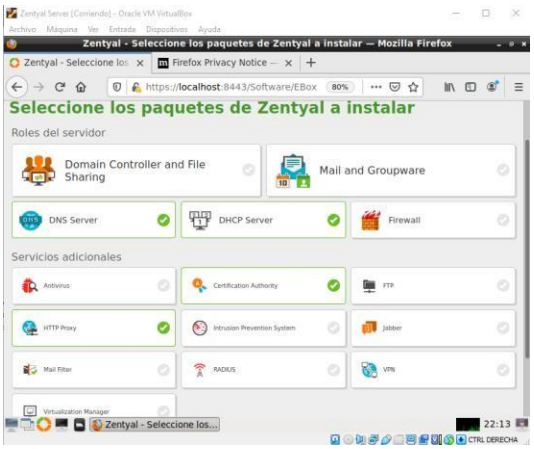


Figura 33. Módulos a utilizar para el proxy no transparente

Muestra los paquetes seleccionados a instalar, y dar en continuar

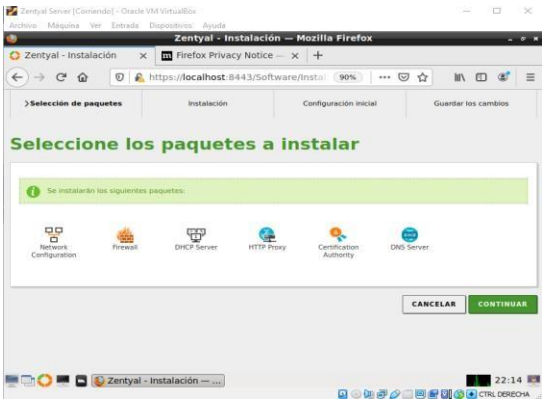


Figura 34. Instalar paquetes

Una vez instalados los módulos inicia el proceso de configuración de las tarjetas de red creadas donde el eth0 y eth1 será externo y DHCP y la eth1 será la red interna con una ip estática.

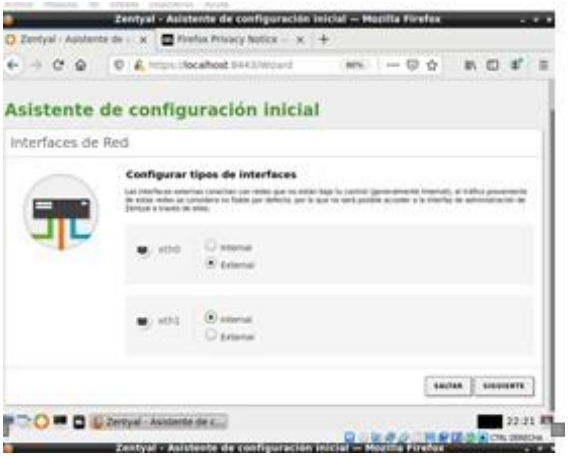


Figura 35. Configuración de la red

Verificamos que la configuración de la red eth0 y eth1 estén correcta

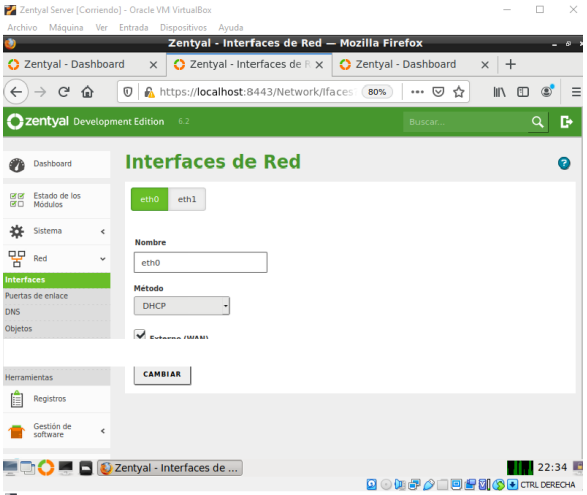


Figura 36. Instalación completa

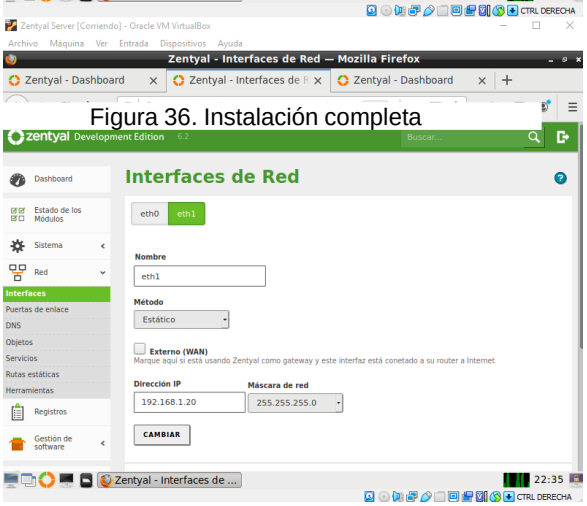


Figura 37. Paquetes instalados

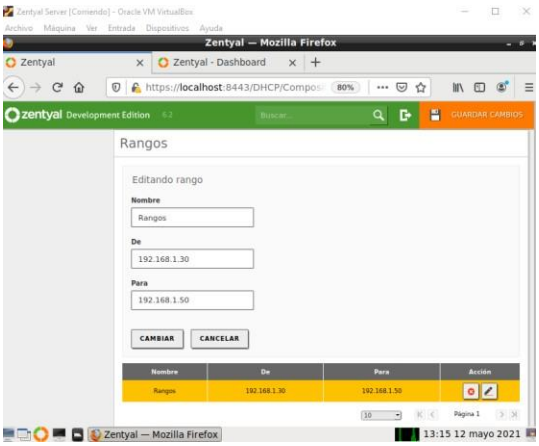


Figura 38. Paquetes instalados

Agregar los rangos de ip para que nuestra maquina Ubuntu tome alguno de estos rangos y se evidencie la conexión entre el Zentyal y el Ubuntu. El rango asignado es de 192.168.1.30 a 192.168.1.50

Al agregar los rangos el zentyal reconoce al Ubuntu dentro de la red interna con ip dentro del rango que se asignó, nos muestra la ip del Ubuntu, dirección MAC y el

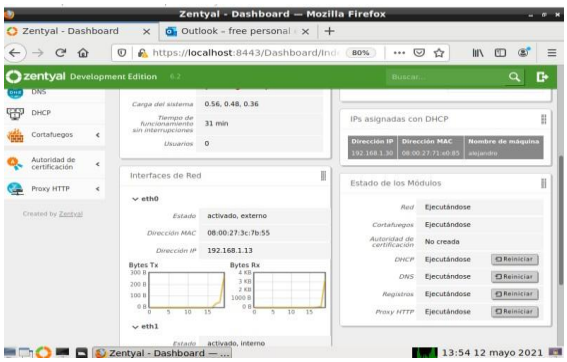


Figura 39. Configurar el DHCP para asignar rangos de Ip a los clientes

Configuración del zentyal para bloquear los servicios desde el puerto 1230, inicia creando un objeto con la ip de la máquina de Ubuntu

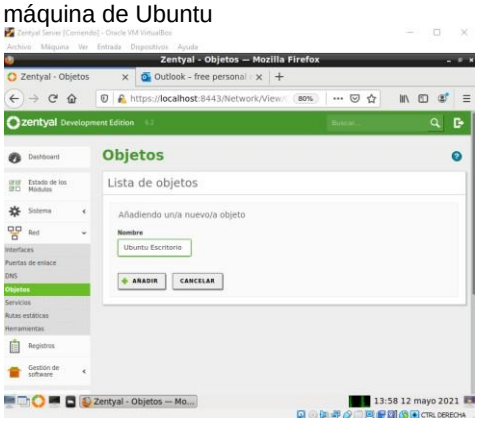


Figura 40. Crear el objeto a bloquear los servicios

Configurar el módulo de proxy HTTP donde se coloca el puerto 1230, con base en lo que dice la guía, para el proxy no transparente

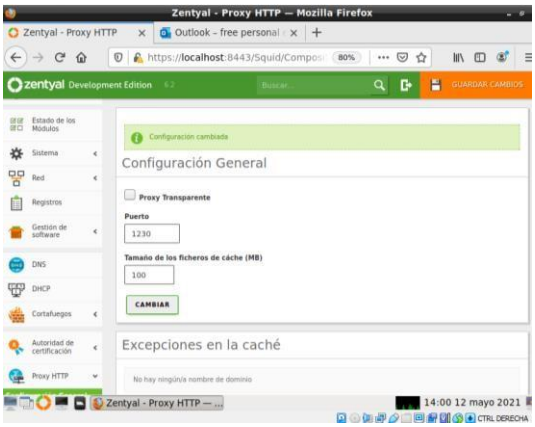


Figura 41. Configuración del proxy HTTP

Configurar las reglas de acceso en el módulo HTTP proxy, por el puerto 1230 denegando los servicios al objeto creado el cual tiene la dirección ip del Ubuntu desktop.

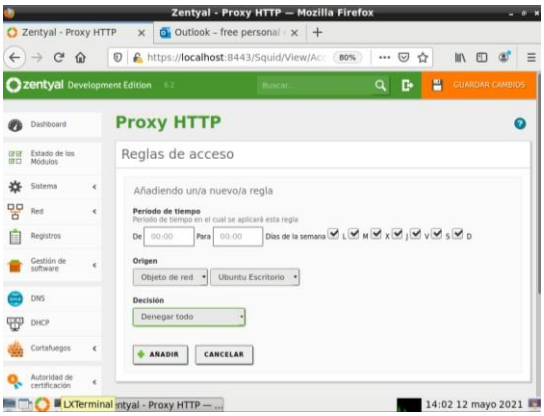


Figura 42. Configuración de las reglas de acceso por el puerto 1230

Realizar el proceso de activación del proxy en el navegador de Ubuntu colocando la ip estática de la red eth1 192.168.1.20 y colocando el puerto 1230. Recargar la página del navegador.

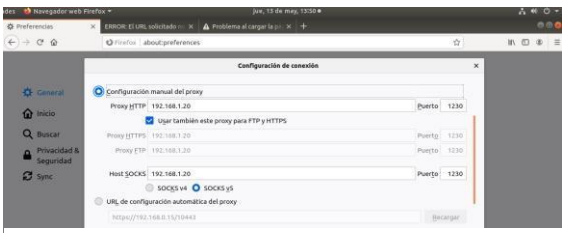


Figura 43. Configuración del proxy en el navegador del cliente


Figura 44. Bloqueo por parte del servidor zentyal
Después de recargar la página muestra el mensaje de restricción por el servidor Zentyal.

## TEMÁTICA 3 CORTAFUEGOS

Para la instalación de cortafuegos en primera instancia se deben señalar los paquetes a instalar tal como se ve en la imagen

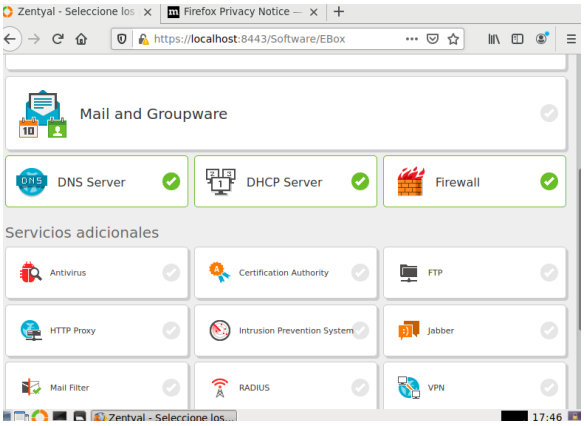


Figura 45. instalaciones de paquete Firewall

Seguidamente Zentyal debe confirmar la instalación exitosa de los paquetes


Figura 46. Confirmación de la instalación

Seguidamente el primer paso es ir a las opciones de cortafuegos


Figura 47. Panel de administración Firewall

Seguidamente se debe seleccionar la opción de Filtro de paquetes para redes internas y presionar la opción añadir nuevo/a


Figura 48. Filtrado de paquetes redes internas

Seguidamente procedo a configurar el filtrado de paquetes en donde la decisión debe ser denegación, origen cualquiera y se debe conocer la Ip de destino. Para saber la Ip de destino de una página en específico solo basta con hacer ping al dominio o Url

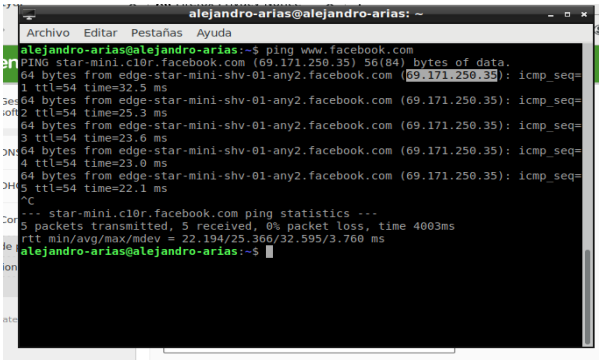


Figura 49. Ping dominio Facebook.com

Ya sabiendo la Ip de destino solo basta especificar en el campo específico de la configuración. Además de esto es importante seleccionar el servicio que será filtrado. En este caso inicio con el TCP

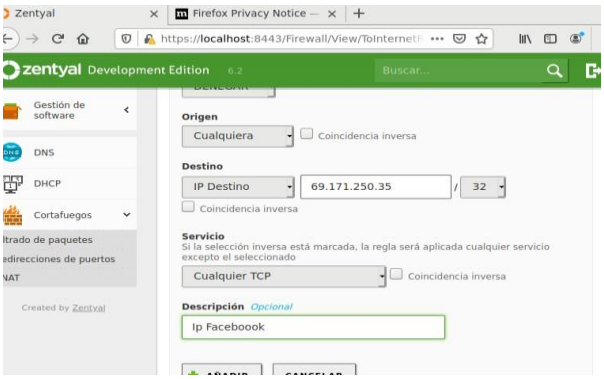


Figura 50. Parámetros denegación de paquetes e la nueva regla de filtrado sea listada.


Figura 51. Listado de reglas

Facebook trabaja con protocolos seguros por tal motivo se hace necesario bloquear también los protocolos http y https


Figura 52. Denegación de servicio Http y Https

Se verifica nuevamente que las reglas hayan sido añadidas correctamente

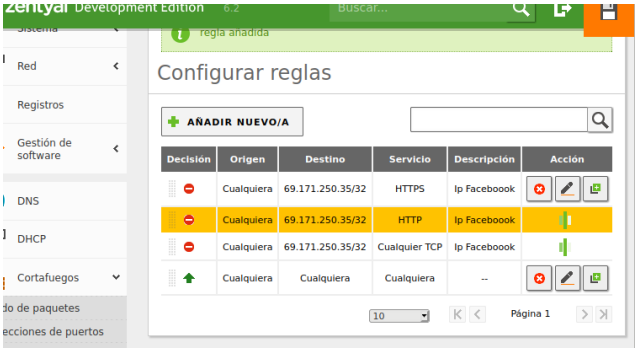


Figura 53. Verificación de reglas para servicios servicio Http y Https

Seguidamente se procede a verificar que el cliente Ubuntu si tenga conexión a internet y acceso inicial a Facebook.com


Figura 54. Verificación acceso a internet y a dominio

Se procede a configurar el entorno de red de acuerdo a la Ip asignada en el Zentyal.

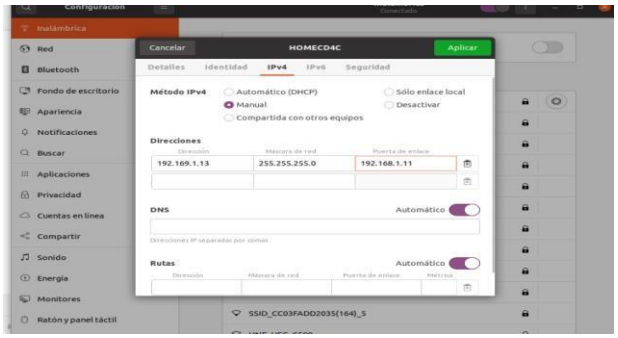


Figura 55. Configuración de red cliente Ubuntu

Una vez realizada la configuración accedo nuevamente a Facebook.com y se puede comprobar la denegación de acceso impidiendo el cague de la página


Figura 56. Validación denegación de acceso

Se puede observar entonces que en esta ocasión la página se queda cargado y nunca aparece, verificando entonces que si se están aplicando las debidas restricciones por parte del cortafuego.

De igual forma se verifica que el equipo continuo que acceso a internet accediendo a domino diferente


Figura 57. Verificación acceso a internet

Seguidamente realizo los mismos procesos para el sitio de entretenimiento https://www.cosmopolitan.com

Verifico cual es la Ip pública del sitio haciendo ping a su dominio

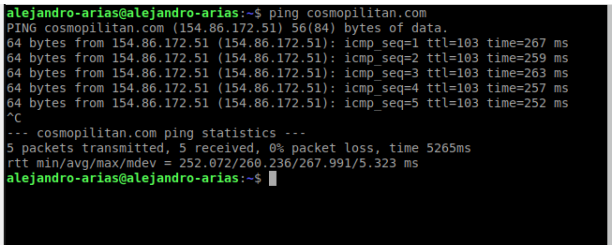


Figura 58. Ip dominio www.cosmopolitan.com

Seguidamente procedo a crear las mismas reglas para esta dirección Ip


Figura 59. Configuración de reglas para la Ip 154.86.172.51

Se verifica que los cambios sean guardados y que las reglas sean listadas en la tabla.


Figura 60. Listado de reglas para nuevo dominio

Se procede a verificar conectividad en el cliente Ubuntu


Figura 61. Verificación de conexión cliente Ubuntu

Se procedo a ingresar la dirección 151.101.128.155 o a su dominio Cosmopolitan.com


Figura 62. Verificación de impedir el acceso.

## TEMÁTICA 4 FILE SERVER Y PRINT SERVER

File server para su funcionamiento se debe ejecutar el módulo LDAP.


Figura 63. Modulo activo de controlador de Dominio y Compartición de Ficheros.

En la Opción de Dominio se crea un nuevo dominio donde se implementó los servicios que configuro el administrador.

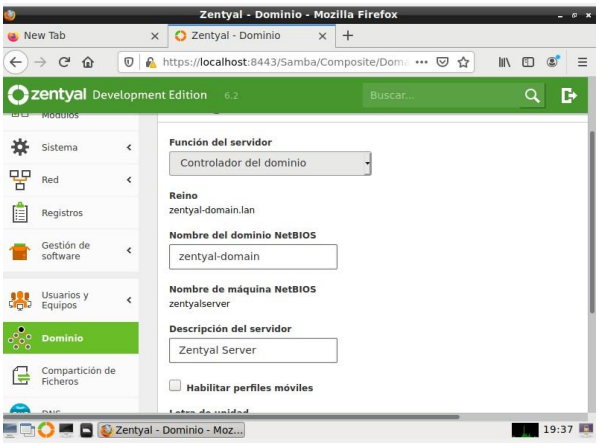


Figura 64. Modulo activo de controlador de Dominio y Compartición de Ficheros


Figura 65. Información del controlador de dominio.

Se crean los usuarios, grupos que se vincularan al Dominio creado por el administrador.

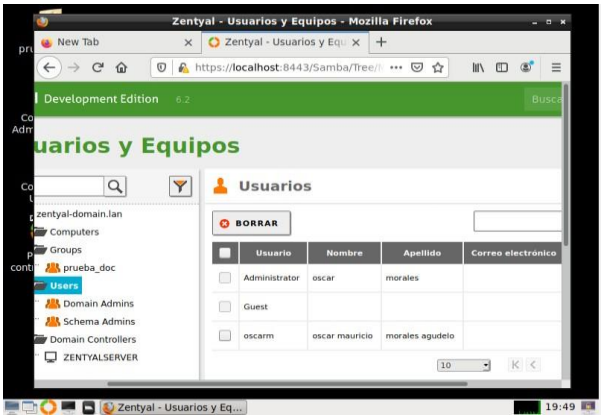


Figura 66. Gestor de usuarios y equipos.

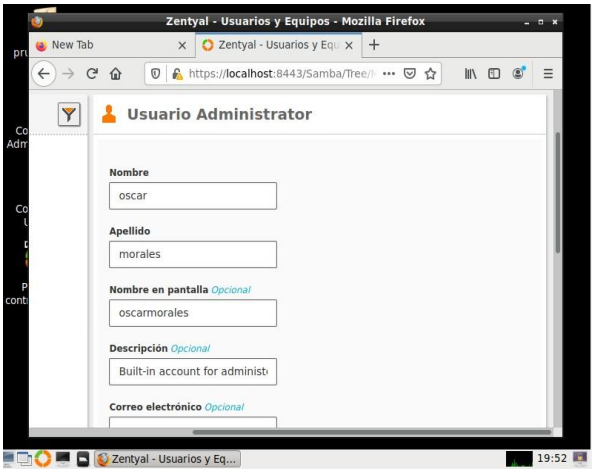


Figura 67. Creación usuario Oscar

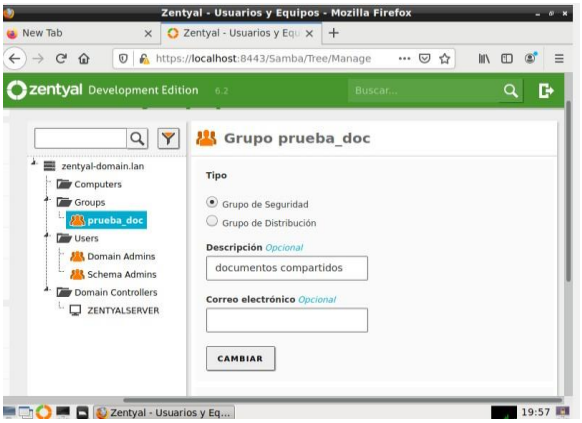


Figura 68. Creación grupo prueba_doc.

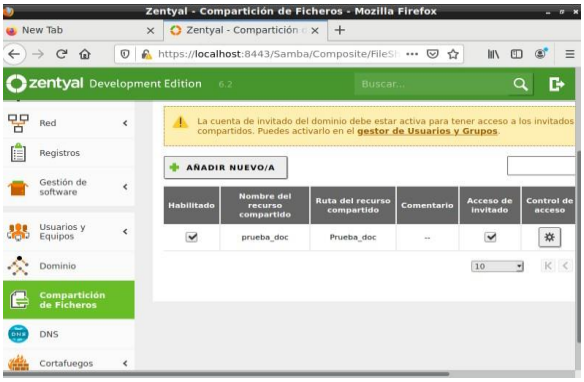


Figura 69. Creación del fichero prueba compartido.

Se muestra la creación de ficheros y la conexión de los clientes al dominio ya que hace parte de la temática anterior.

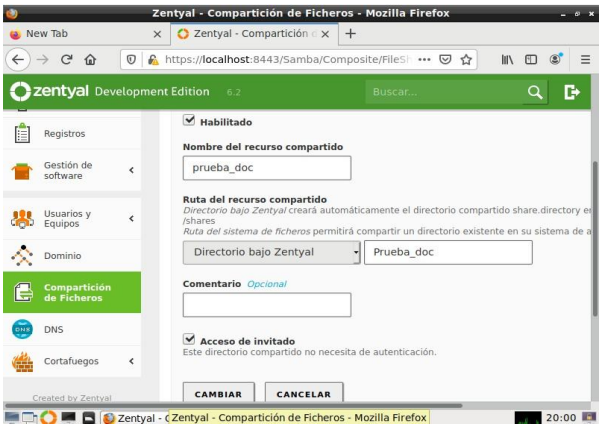


Figura 70. Habilitación del recurso compartido prueba_doc

Por modo consola en el servidor Zentyal se verifica que el directorio tenga el fichero y los documentos que se comparten

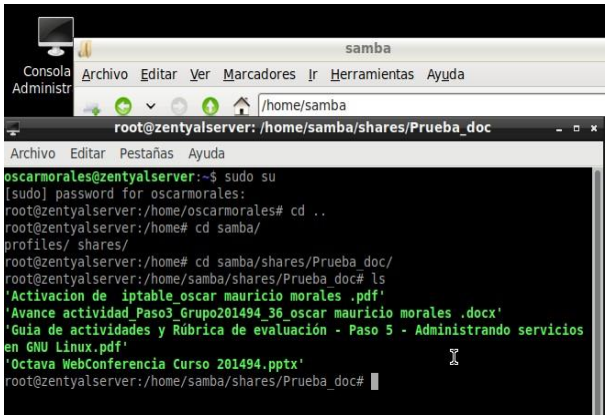


Figura 71. Documentos en la carpeta compartida prueba_doc

Por medio de la dirección Ip del servidor se accede al fichero, dándole las credenciales de acceso por oscarmorales.

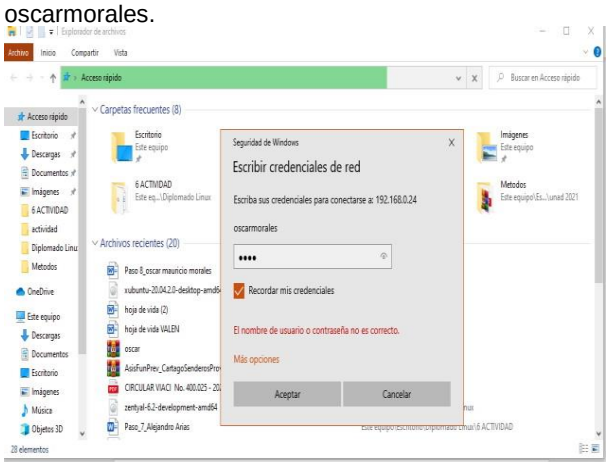


Figura 72. Acceso desde Windows al fichero.

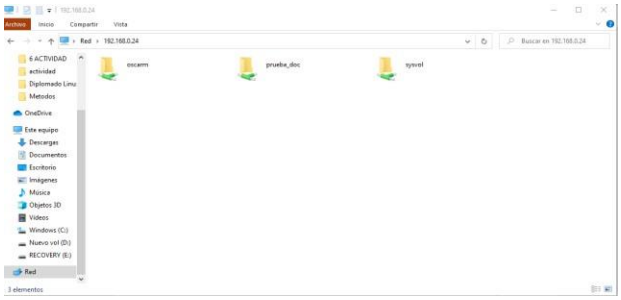

Figura 73. Carpetas compartidas.

Al igual se visualiza los ficheros por el cliente Ubuntu.


Figura 74. Ingreso Cliente Ubuntu.

Se genera la visualización de los documentos accediendo por las credenciales de Ubuntu se observan los documentos compartidos.

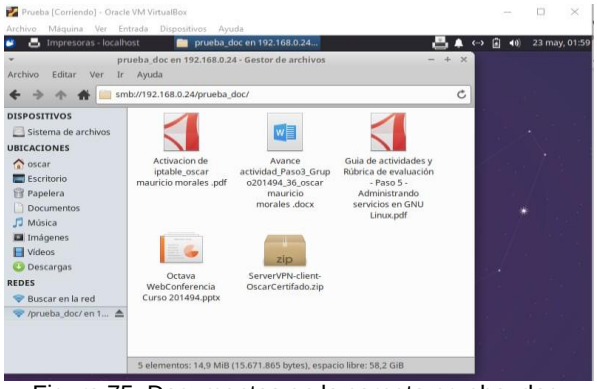

Figura 75. Documentos en la carpeta prueba_doc.

## Print Server

La última versión de Zentyal que permitía la administración de impresoras fue la 4.2 donde tenía un módulo de administración para este servicio. Este motivo hace que la mejor manera de configurar este servicio fue con CUPS (Common UNIX printing System).

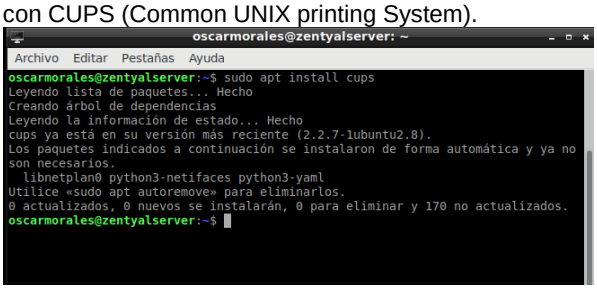


Figura 76. Instalación de Cups.

La consola de administración se encuentra por medio del puerto 631y la ruta es https:localhost:631/admin.


Figura 77. Consola de administración CUPS.

Solicita credenciales de verificación para el inicio de la configuración.

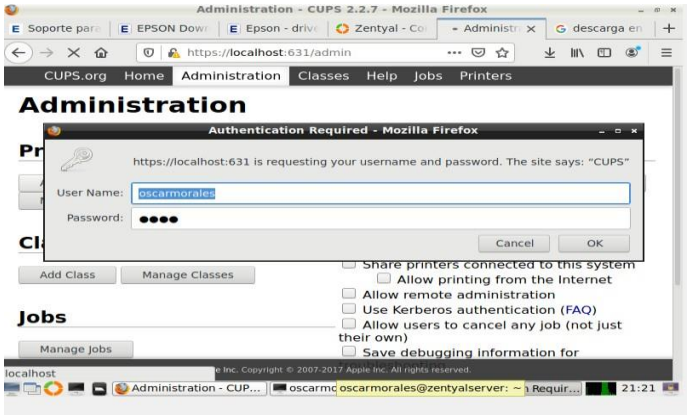


Figura 78. Autentificación ingreso.

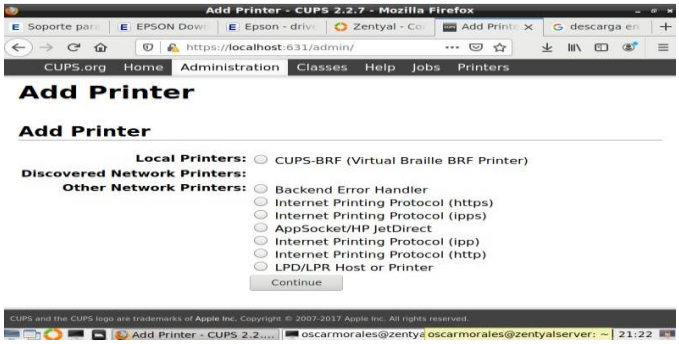


Figura 79. Selección impresora a instalar

La información necesaria para la conexión del cliente en ubuntu es a través del socket://192.168.0.24

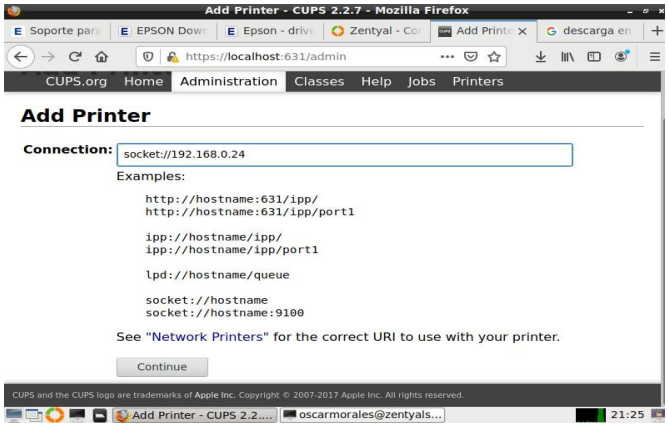


Figura 80. Datos de conexión impresora

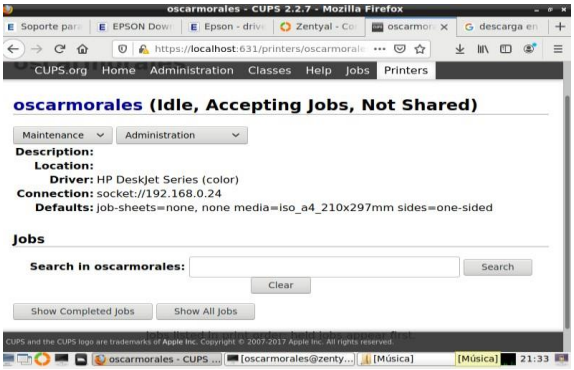


Figura 81. Datos e instalación impresora.

Configuración en el equipo cliente Ubuntu.

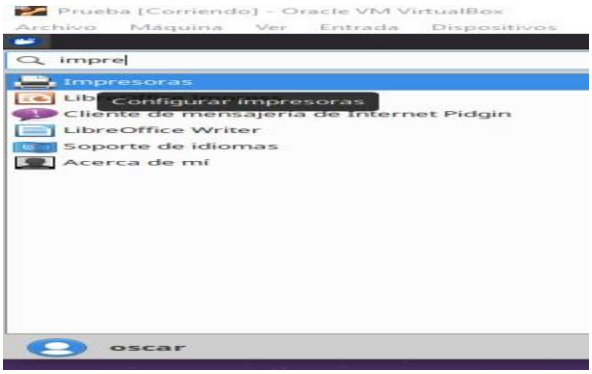


Figura 82. Configuración equipo cliente.

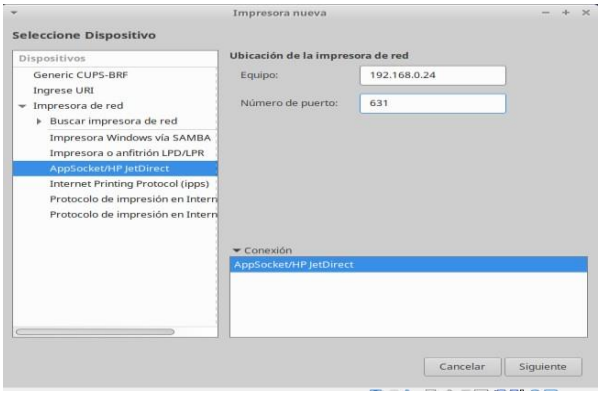


Figura 83. Selección ubicación impresora.

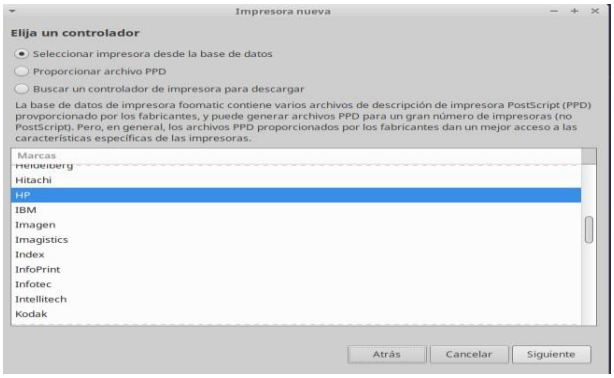


Figura 84. Configuración equipo cliente.

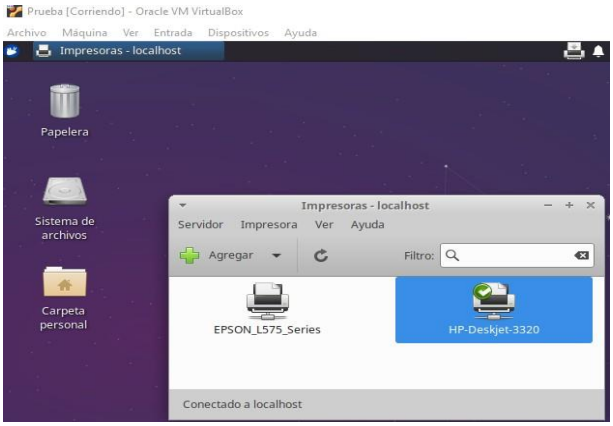


Figura 85. Impresora instalada.

## 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.
Se procede con la instalación de los paquetes para dicha tarea.

La VPN: para crear el túnel privado.
Autoridad de certificación: para crear los certificados del servidor, de la vpn y de los equipos que se van a conectar.
Firewall: Para habilitar los puertos que se necesitan


Figura 86 Zentyal paquetes instalado

Ya instalados los diferentes paquetes se procede a ingresar a la configuración y se elige nuestra interfaz de red. En este caso escogí la Internal y damos en la siguiente.


Figura 87 configuración de red

Se procede a elegir en la interface externa el método para asignación de IP por DHCP.


Figura 88 configuración de red

Se procede a ingresar en la opción de red donde están las interfaces, la primera la configuramos con protocolo DHCP para la asignación de las IP de equipos que se conecten a nuestro servidor a través de VPN y la segunda IP estática con fines de parametrización del servidor.


Figura 89 configuración de interface de red

Se procede a ingresar al “módulo de autoridad de certificación”. En la ventana que nos aparece definimos el nombre de la organización y los días para expirar,

luego damos clic en el botón crear

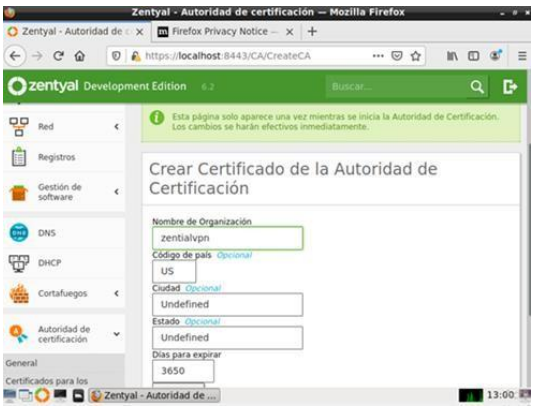


Figura 90 creación de certificados

Se crearán tres certificados
- Certificado para el servidor Zentyal
- Certificado para el servidor VPN
- Certificado para clientes

Certificado del servidor Zentyal


Figura 91 creación servidores

Se procede a ingresar en la opción de servidores y creamos uno nuevo. Le asignamos un nombre, en este caso server 2021


Figura 92 creación servidores

Una vez asignado el servidor se procede a ingresar en la opción de configuración, y se configura de acuerdo a nuestros requerimientos.


Figura 93 configuración de servidores

En la misma opción del servidor se procede a la configuración y descarga de los clientes para la conexión, se asigna el tipo de cliente, el certificado del cliente y lo más importante la IP del servidor y se procede con la descarga

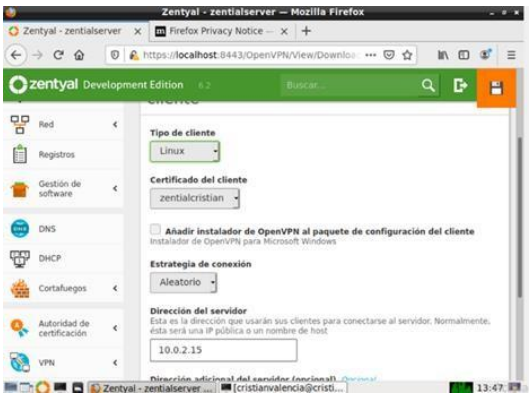


Figura 94 configuración de servidores

Se visualiza la descarga del certificado del cliente para su conexión

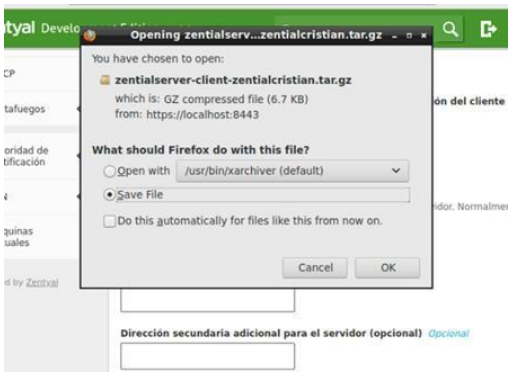


Figura 95 descarga de certificado

Ingresamos al Desktop Ubuntu donde están alojados los archivos, pueden ser transferidos por SSH, Drive o carpetas compartidas, desde la consola nos ubicamos en el directorio en el que se encuentran y con el comando sudo openvpn y el archivo de configuración que en este caso es Zentyal2021.client.conf realizamos la conexión.

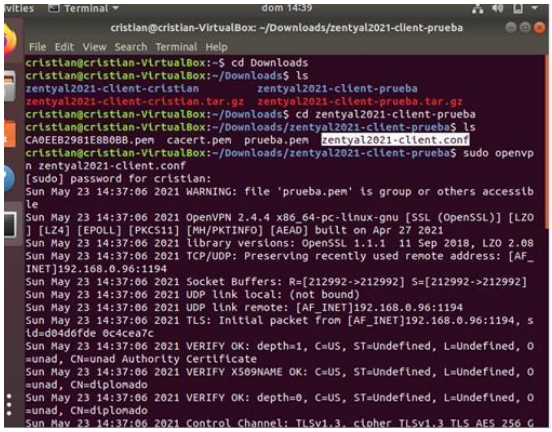


Figura 96 instalación openvpn

Por último, podemos observar la conexión VPN corriendo con estado “ejecutándose” en el panel de control webadmin de zentyal.


Figura 97 zentyal

## i. Conclusiones.

En el desarrollo de la actividad presentada, se implementó y configuró de manera clara y detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal, propuestos en la guía de actividades.

Al concluir este trabajo vemos la importancia de una VPN en cuanto a la conexión privada que le brinda al cliente para estar protegido y conectado de una forma segura entre diferentes equipos de una misma red lo cual brinda estabilidad por medio de los certificados que dan plena autenticación para su ingreso.

Al momento de configurar el servidor ZENTYAL se debe tener claro la tarjeta o adaptador de red, si esto no se configura correctamente no funciona y genera inconvenientes.

El servidor ZENTYAL para configurar los paquetes LDAP es muy fácil, solo se debe tener en cuenta las

configuraciones de usuario, claridad en el direccionamiento Ip de servidor y clientes.

ZENTYAL 6.2 no tiene soporte para el servidor de impresión este solo llego hasta la versión 4.2, en este caso se utilizó CUPS 2.2 para emular y lograr compartir impresoras para los Clientes

Se realizó el fortalecimiento de los conocimientos adquiridos con la temática 3 cortafuegos el entorno de trabajo de Linux donde se dieron soluciones o reglas de bloqueos de contenidos web, que nos ayudan a proteger y delimitar el servicio.

Mediante el desarrollo de este trabajo, permitió el correcto análisis, identificación, aplicación y solución a un problema como lo es la seguridad de la información, por medio de la implementación de proxy no trasparente donde la salida a internet debe ser válida por el puerto 1230, permitiendo mayor seguridad en los sistemas informáticos o de la información. Aprender la administración y control de la seguridad en los sistemas informáticos o de la información, esto permitirá un mejor control, administración, protección de la infraestructura, información valiosa, por medio de la restricción o acceso de cada usuario. Brindar soluciones de manera acertada tipo cliente servidor

## REFERENCIAS


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

Sanz Mercado, P. (2014). Seguridad en Linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 45 - 60). https://elibro net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=45.

Zentyal.org, (2014). Es/3.5/Servicio de redes privadas virtuales (VPN) con OpenVPN. https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_(VP N) _con_OpenVPN.

Hydemyass.com. (2016). Using Linux Virtual Machine instead of a router for VPN. https://support.hidemyass.com/hc/en-us/articles/202721486-Using-Linux Virtual-Machine-instead-of-a-router-for-VPN.

Sanz Mercado, P. (2014). Seguridad en Linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 13 - 26). Recuperado de https://elibro net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=13.