

Zentyal como infraestructura Linux que brinda soluciones basadas en Ubuntu a las pequeñas y medianas empresas en Colombia.

Jorge Eliecer Arredondo Monsalve
jearredondom@unadvirtual.edu.co
Aura María Acosta Serrano
amacostase@unadvirtual.edu.co
Antonio José Navarrete Calderón
ajnavarretec@unadvirtual.edu.co
Blanca Delmira Montaña Martínez
bdmontanam@unadvirtual.edu.co
Nelly Bulla Cely
nbullac@unadvirtual.edu.co

RESUMEN: Las pequeñas y medianas empresas en Colombia (PYMES), enfrentan situaciones complejas para surgir y mantenerse vigentes debido a los costos enormes que implican su sostenibilidad en el mediano y largo plazo. Lo anterior no solo por los asfixiantes impuestos legales, que sumados les demandan más del 70% de su producción. En términos generales, de 100 pesos producidos una PYME debe facturar 70 pesos en obligaciones fiscales. Sumado a lo anterior, los costos de infraestructura TI, tan necesarios para su implementación son abrumadoramente costosos, sobre tecnologías ya conocidas como Windows. En estos tiempos tan difíciles para la pequeña y mediana empresa, agravados por la condición pandémica por la que atraviesa la economía del país, es indispensable ofrecer soluciones de infraestructura de TI de Linux, fáciles de usar y con un soporte en los servicios que no implique sobrecostos. En este punto es de enorme beneficio que por primera vez Canonical proporciona soporte integrado de Ubuntu para una solución de otro proveedor de código abierto como lo es Zentyal.

PALABRAS CLAVE: Servidor, proxy, DHCP, DNS, firewall, VPN.

1 INTRODUCCIÓN

Este informe presenta la forma de instalar y brindar una configuración inicial básica de Zentyal, que le permita ejercer los roles de servidor y firewall dentro de una infraestructura de TI, al tiempo que gestiona los servicios de DNS, DHCP, Proxy, File Server, Print Server y VPN, solicitados por las estaciones de trabajo dentro de una LAN.

2 ENTORNO DE TRABAJO

Debido a que estaremos desarrollando las actividades sobre un sistema anfitrión basado en Windows, procedemos entonces con la creación de dos (2) MV (Máquina Virtual) haciendo uso del programa VirtualBox, con las cuales estaremos configurando una red básica que nos permitirá evidenciar el funcionamiento de Zentyal. Una de estas MV soportará

el servidor y la otra MV cumplirá la función de estación cliente que estará solicitando los servicios provistos y gestionados por Zentyal.

2.1 CONFIGURACIÓN DE RED

Presentamos un esquema sencillo de red, en el cual Zentyal funge como Firewall recibiendo la zona roja, que para este propósito es la puerta de entrada (Gateway) o Modem del proveedor de servicios de internet con IP 192.168.20.1. La zona desmilitarizada (DMZ) es representada por el rol de servidor, ejercido por el mismo Zentyal. La DMZ maneja entonces la IP 192.168.20.100.

Creamos la LAN dentro del rango 192.168.100.0/24, donde la puerta de enlace la maneja la tarjeta de red en el servidor Zentyal con IP 192.168.100.2.

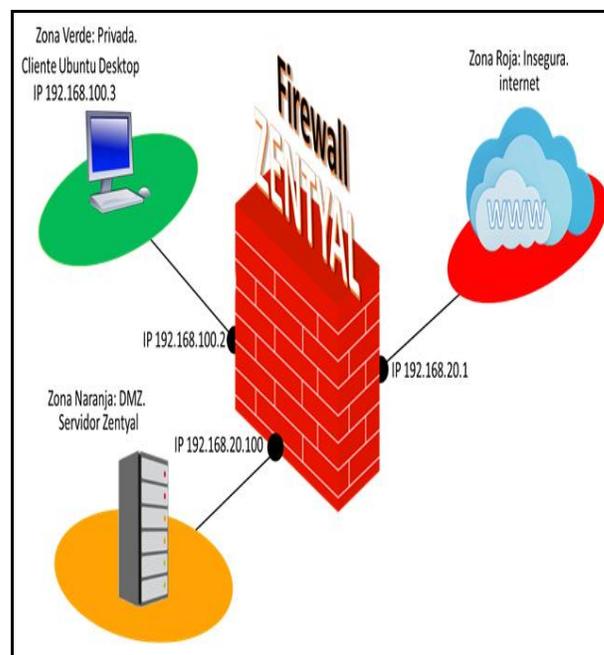


Figura 1. Red básica. Por Jorge Arredondo

3 INSTALACIÓN DE ZENTYAL

3.1 FUENTE DEL SOFTWARE

Obtenemos la imagen ISO con versión 6.2., que estaremos cargando en la MV del servidor, del sitio oficial de Zentyal, en el siguiente enlace: <http://download.zentyal.com/>.

3.2 CONFIGURACIÓN BÁSICA DE LA MV

Los siguientes son los aspectos de configuración que hemos asignado a la MV sobre la cual se instalará el servidor Zentyal:

- Tipo: Linux.
- Versión: Ubuntu (64-bit).
- RAM: 2048 MB.
- Disco Virtual: 50 GB.
- 2 Adaptadores de red:
 - o (1) Adaptador puente.
 - o (2) Red interna.

Sobre la MV cargamos la imagen ISO y procedemos a iniciar la instalación.

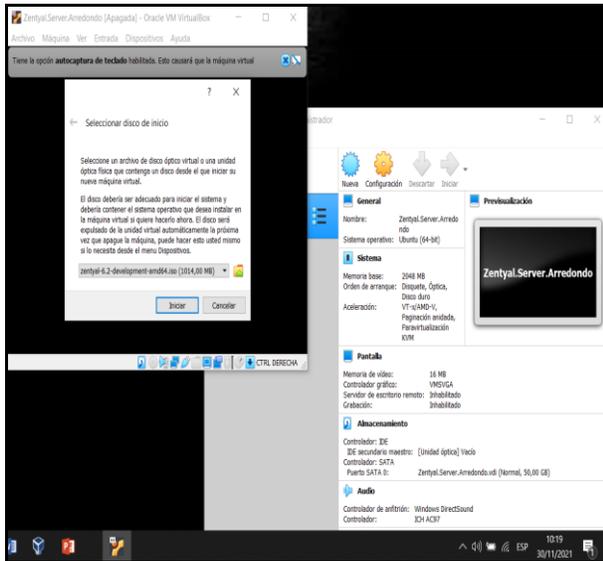


Figura 2. Carga de ISO en MV. Por Jorge Arredondo

3.3 INSTALACIÓN

3.3.1 LENGUAJE DE INSTALACIÓN

Al inicio de la instalación se nos presenta un menú con opciones de lenguajes sobre el cual podemos desplazarnos con las flechas de nuestro teclado y seleccionar el que se acomoda a nuestro interés. En este caso hemos seleccionado el idioma español. Cabe anotar que aparece en la parte inferior un menú que nos presenta las opciones de F1 Ayuda, F2 Lenguajes de instalación, F3 Referencia de atajos con el teclado, F4 Modos opcionales, F5 Accesibilidad y opciones complementarias con la tecla F6.

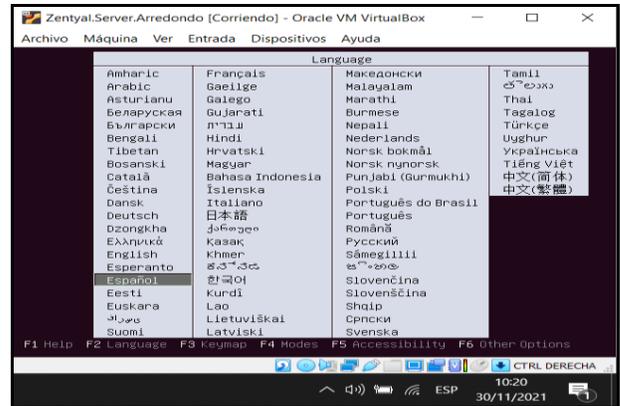


Figura 3. Lenguaje de instalación. Por Jorge Arredondo

3.3.2 MENÚ INICIAL DE INSTALACIÓN

El menú inicial de instalación nos brinda las opciones de proceder en modo experto, diagnosticar el disco duro y la memoria RAM, cambiar el punto de arranque o proceder con el método de recuperación. Para esta práctica estaremos seleccionando la primera opción que elimina todo el contenido del disco y procede con la instalación estándar.



Figura 4. Menú inicial de instalación. Por Jorge Arredondo

3.3.3 GEOLOCALIZACIÓN

El instalador nos solicita que le indiquemos el país donde está ubicado nuestro sistema para fijar nuestra zona horaria.

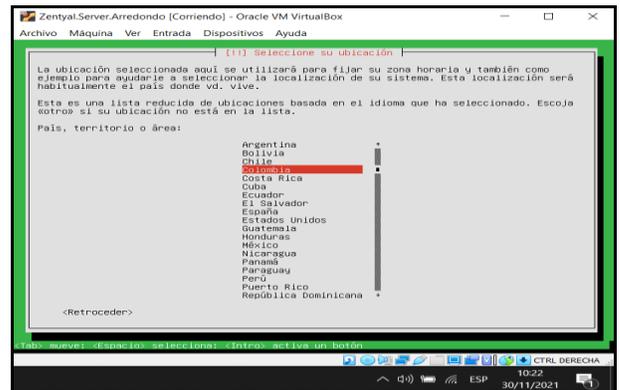


Figura 5. Menú inicial de instalación. Por Jorge Arredondo

3.3.4 DISTRIBUCIÓN DEL TECLADO

Especificamos la distribución de nuestro teclado conforme a nuestra región e idioma, esto es español (Latino América).

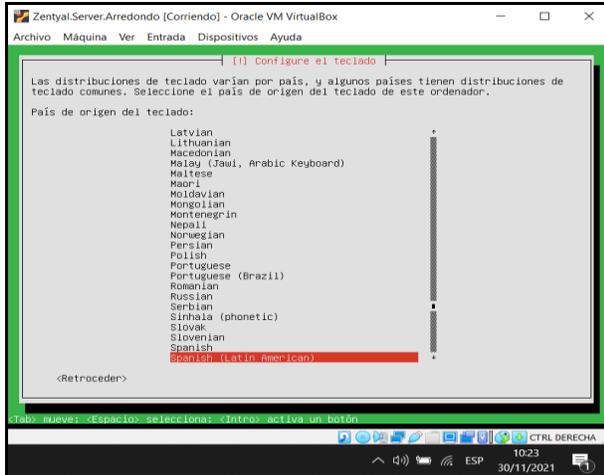


Figura 6. Distribución del teclado. Por Jorge Arredondo

3.3.5 CONFIGURACIÓN DE RED

El sistema detecta las dos interfaces de red que configuramos en la MV. Seleccionamos la eth0 como tarjeta de red primaria por donde se comunica con la zona roja.

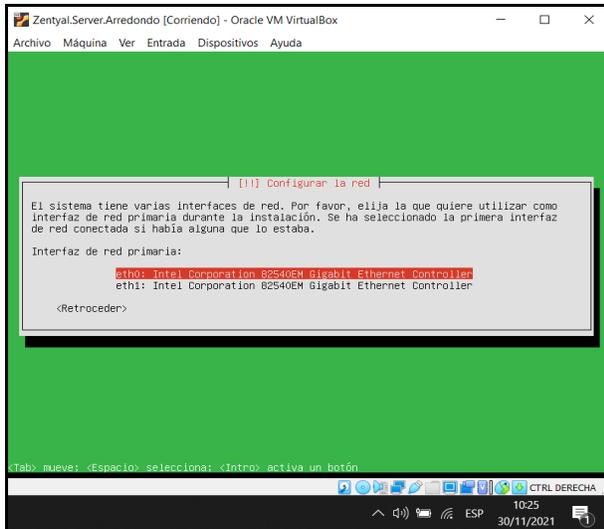


Figura 7. Interfaces de red. Por Jorge Arredondo

3.3.6 NOMBRES DEL SERVIDOR Y EL USUARIO

De forma consecutiva nos solicita el nombre que le daremos al servidor y el nombre del usuario administrador del sistema. Manteniendo las buenas prácticas, se usa una sola palabra y en minúscula. En lo que respecta al inicio de esta práctica el servidor se llamará "zentyal" y el usuario será "arredondo". Como más adelante intervienen los aportes de otros estudiantes, estos nombres pueden cambiar.

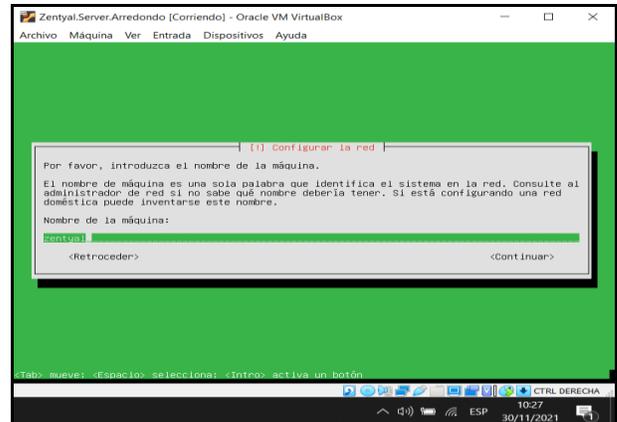


Figura 8. Nombres de servidor y usuario. Por Jorge Arredondo

3.3.7 CLAVE

La instalación nos pide que ingresemos una clave y posteriormente la confirmamos.

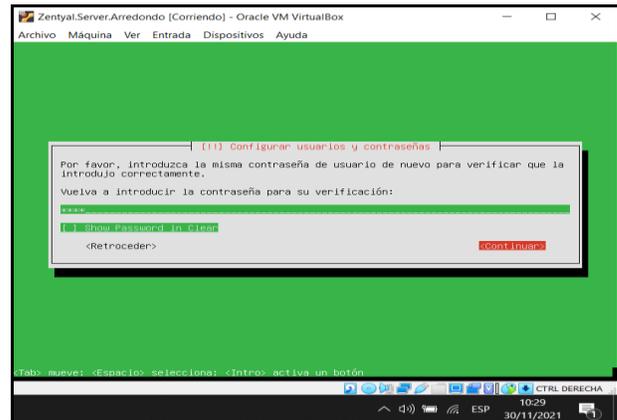


Figura 9. Clave y confirmación. Por Jorge Arredondo

3.3.8 REINICIO DEL SISTEMA

Lo que sigue a continuación es la confirmación de la zona horaria, precedida por la copia e instalación de todos los archivos necesarios para este propósito. Al final nos presenta un mensaje indicando la culminación de la instalación, pidiéndonos que removamos el dispositivo fuente de la instalación y procedemos a reiniciar el sistema.

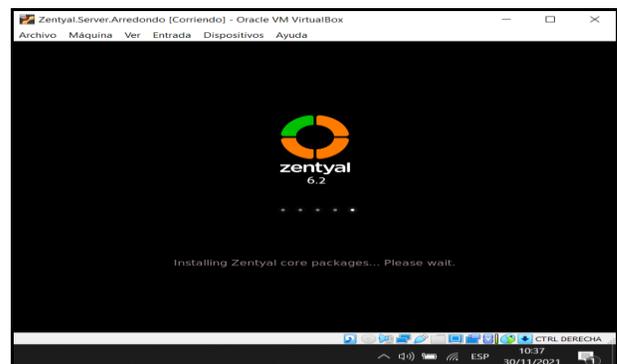


Figura 10. Reinicio del sistema. Por Jorge Arredondo

3.4 CONFIGURACIÓN INICIAL

Una vez reiniciado el sistema se nos abre la interfaz de Zentyal, la cual opera sobre protocolo HTTP y es por esto que se abre en un navegador web. Lo primero que debemos hacer es aceptar el certificado SSL y proceder a validar nuestro ingreso con el nombre de usuario y clave, creados durante la instalación.

Una vez que hemos validado nuestras credenciales y nos encontramos dentro de Zentyal, nos recibe un mensaje que nos indica que procederemos con la configuración inicial del servidor. Presionamos continuar.

3.4.1 PAQUETES REQUERIDOS

Seleccionamos todos los paquetes que necesitamos instalar a través de Zentyal y que se nos hacen indispensables para la implementación y gestión de los servicios que llevaremos a cabo en el presente informe.

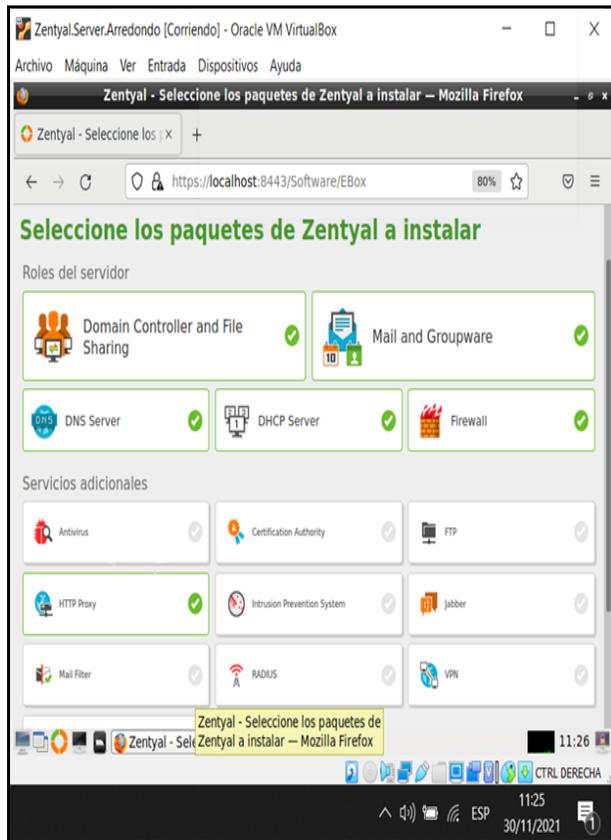


Figura 11. Instalación de paquetes. Por Jorge Arredondo

3.4.2 INTERFACES DE RED

Luego de la instalación exitosa de los paquetes de zentyal, se nos presenta un asistente de configuración de red, el cual nos ha detectado las interfaces de red configuradas en nuestro sistema. Procedemos a asignar como interfaz de red externa la eth0 (Zona roja, internet) y como interfaz de red interna la eth1 (Zona privada, LAN).

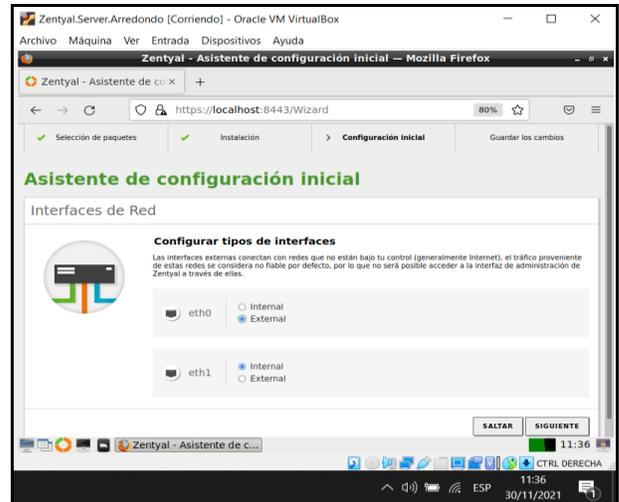


Figura 12. Configurar interfaces de red. Por Jorge Arredondo

3.4.3 DIRECCIONAMIENTO IP

Una vez definidas las interfaces de red, según su zona de influencia, procedemos a asignar el direccionamiento IP dentro del rango que cada una maneja. El rango de la zona roja se encuentra en 192.168.20.0/24. El Gateway tiene asignada la IP 192.168.20.1. De esta manera hemos asignado a la interfaz eth0 que recibe esta puerta de enlace, con la IP estática 192.168.20.100, que hace las veces de Zona naranja o desmilitarizada DMZ, en donde se configurará el Firewall del servidor.

Con respecto a la zona privada o verde, esto es la LAN, hemos ubicado la interfaz de red en el rango 192.168.100.0/24, teniendo como puerta de enlace la IP 192.168.100.2 que es el mismo servidor.

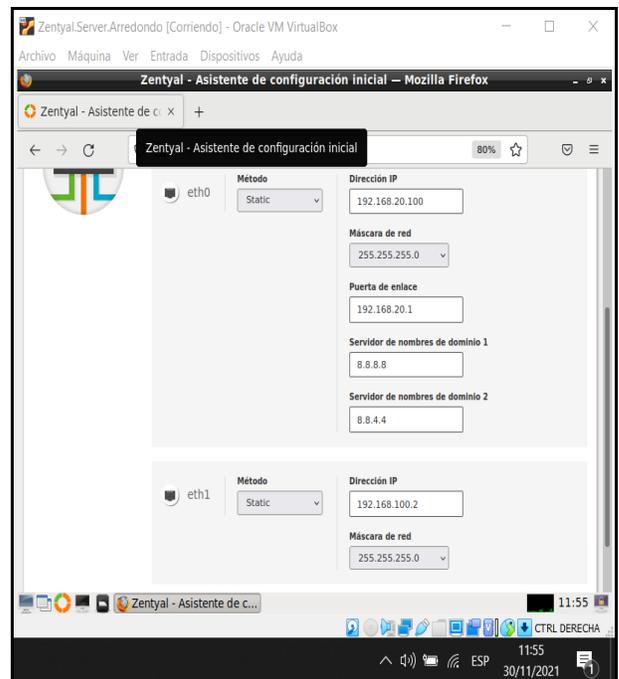


Figura 13. Direccionamiento IP. Por Jorge Arredondo

Para finalizar con la configuración inicial, el sistema nos pide el tipo de servidor, nombre de dominio y cuenta de correo. Se guardan los cambios de la configuración y nos presenta un mensaje de culminación exitosa de todo el proceso de instalación y nos accede al Dashboard de trabajo en Zentyal.

4 SERVICIOS PARA LA GESTIÓN DE INFRAESTRUCTURA IT

4.1 DHCP Server

Procedemos a habilitar y configurar los servicios de DHCP para asignar IP de forma dinámica en la LAN y proveer de servicios específicos a las terminales conectadas.

Nos dirigimos a “Estado de los módulos”, ubicado en el panel izquierdo del Dashboard. Ubicamos DHCP y marcamos la casilla de estado para que se habiliten los servicios. Se nos presenta un mensaje que nos advierte de la reconfiguración que se efectuará en el sistema a raíz de esta activación de servicios DHCP, a lo cual damos aceptar.

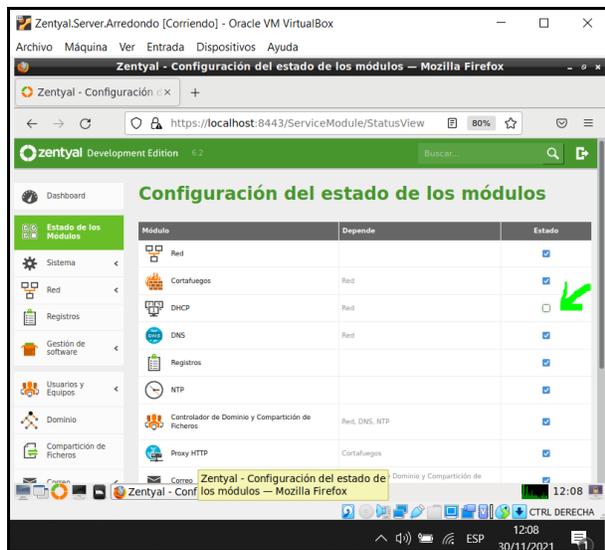


Figura 14. Activar servicios DHCP. Por Jorge Arredondo

Una vez activados los servicios DHCP, se habilita el módulo de este servidor en el panel izquierdo del Dashboard donde lo ubicamos y haciendo clic en él se despliega un menú que nos presenta la opción “Interfaces”.

Haciendo clic en esta opción se nos despliegan las interfaces de red habilitadas desde la configuración inicial de Zentyal.

Como nos proponemos configurar los servicios de DHCP para la LAN, presionamos el botón de configuración en la tarjeta de red eth1. Cabe anotar que seguido a este botón de configuración, también se encuentra uno que permite editar la configuración de las interfaces de red, siempre que lo necesitemos.

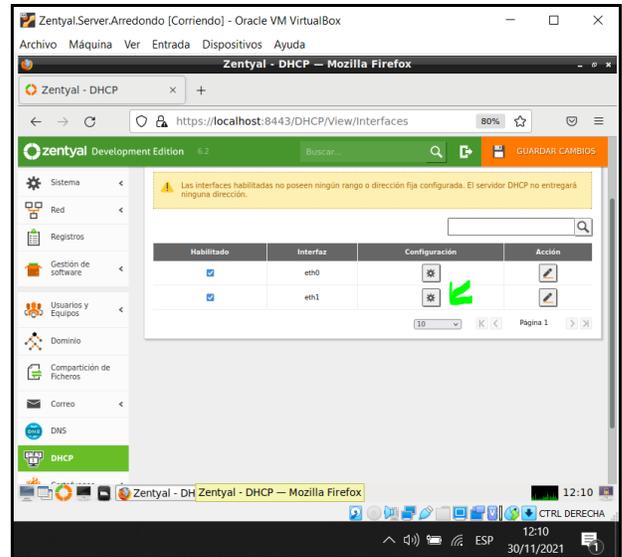


Figura 15. Configurar interfaz eth1. Por Jorge Arredondo

Al ingresar a la configuración de la interfaz eth1, nos desplazamos hacia abajo hasta encontrar la sección “Rangos”, que está antecedida por “Rangos DHCP” en la cual podemos ver la dirección IP de la interfaz (192.168.100.2). La subred (192.168.100.0/24). Y el rango maestro disponible para asignar dinámicamente, que va desde la IP 192.168.100.1 hasta la IP 192.168.100.254. Por supuesto la IP 192.168.100.2, ya no está disponible pues está asignada de forma estática a la puerta de enlace.

Presionamos ahora, en la sección “Rangos”, el botón que dice “Añadir nuevo”. Le damos un nombre distintivo a nuestro nuevo rango de direcciones IP que se asignaran dinámicamente y discriminamos el rango ingresando en la primera casilla, la primera IP 192.168.100.3, y en la casilla siguiente, la IP con la que se cierra el rango definido en 192.168.100.10. Un total de 8 IP, para asignar de forma dinámica.

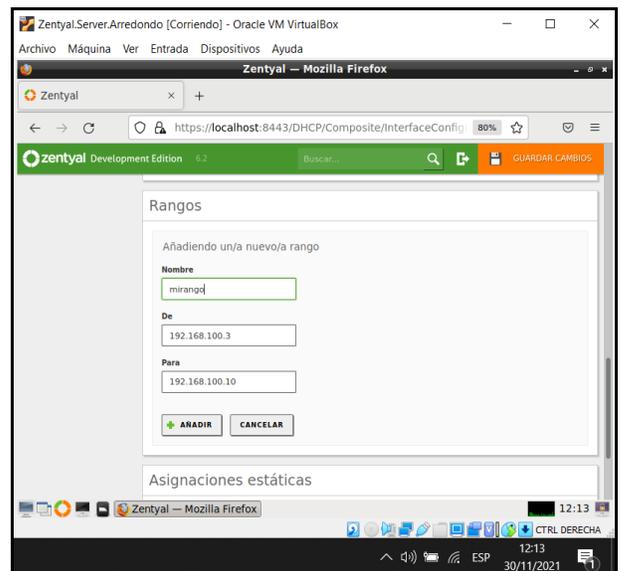


Figura 16. Rango IP. Por Jorge Arredondo

Debemos recordar guardar los cambios realizados en el sistema. Podemos observar que el nuevo rango ha sido creado y procedemos ahora a guardar todos los cambios presionando el botón de color naranja en la parte superior, que dice guardar cambios.

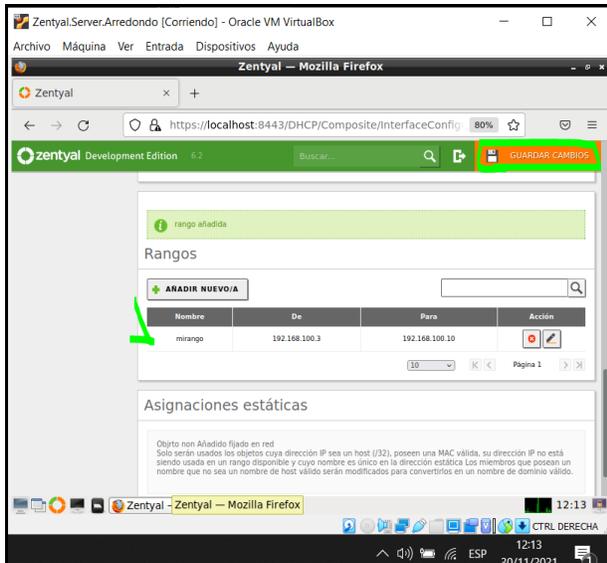


Figura 17. Guardar cambios de DHCP. Por Jorge Arredondo

Si abrimos una terminal cliente conectada a la LAN, podemos evidenciar como los servicios DHCP del servidor, le han asignado de forma dinámica la primera IP 192.168.100.3, del rango definido con anterioridad.

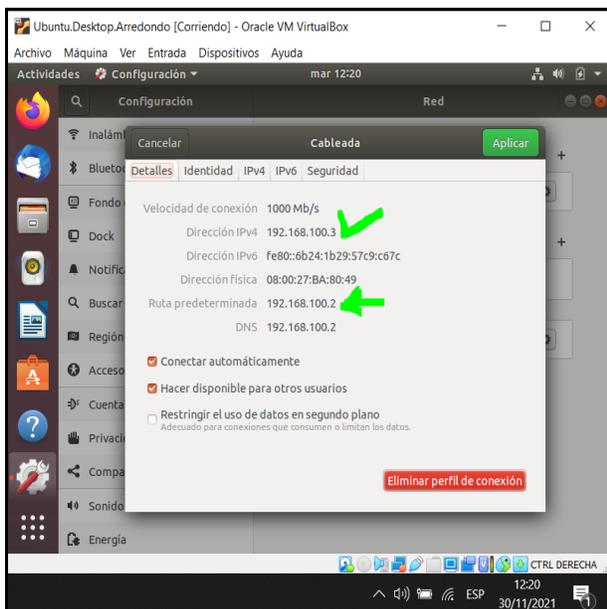


Figura 18. IP asignada de forma dinámica. Por Jorge Arredondo

4.2 DNS Server

Ahora para configurar el servidor DNS, nuevamente nos dirigimos a "Estados de los módulos" y verificamos si está activo el servicio DNS, de no ser así lo marcamos en la casilla correspondiente.

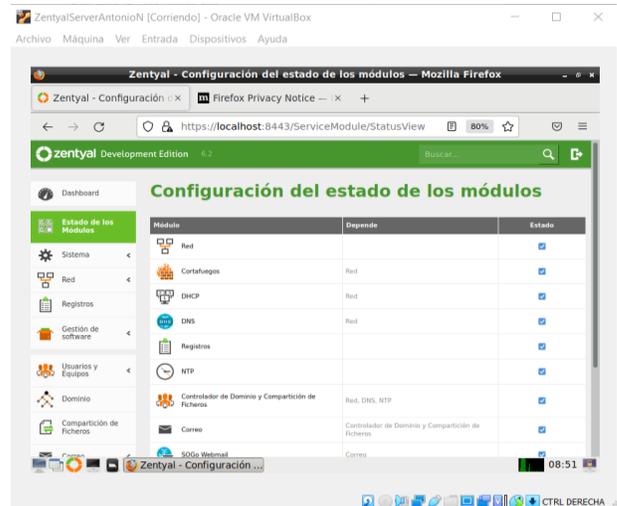


Figura 19. Configuración de módulos. Por Antonio Navarrete

Procedemos a verificar que en el módulo DHCP esté habilitado en la opción de servidor de nombres propios DNS local de Zentyal.

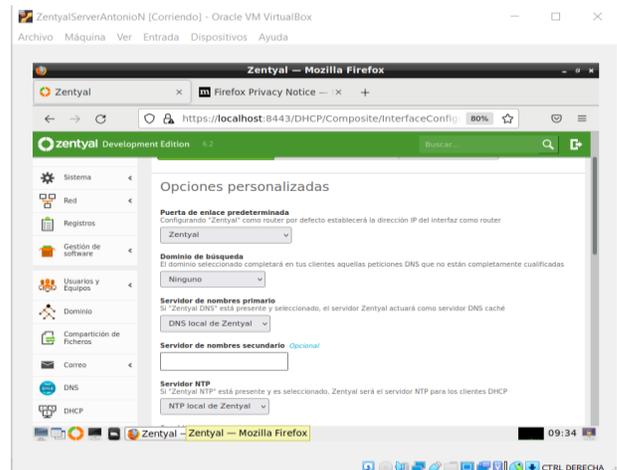


Figura 20. Verificación DHCP. Por Antonio Navarrete

Ahora nos dirigimos al módulo de DNS para configurar el dominio nuevo.

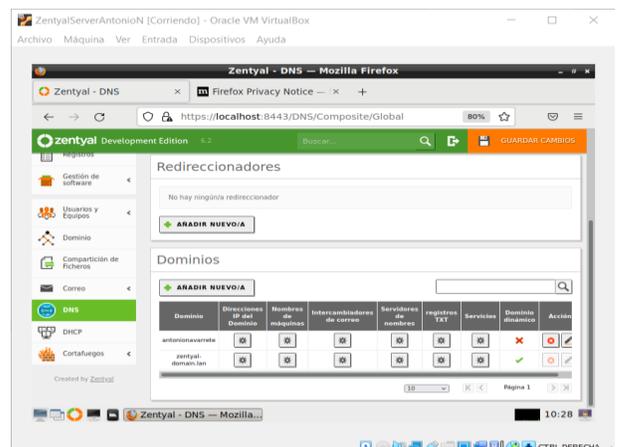


Figura 21. Verificación módulo DNS. Por Antonio Navarrete

Procedemos a configurar este dominio dirigiéndonos a ip del dominio con el fin de añadir un nuevo.

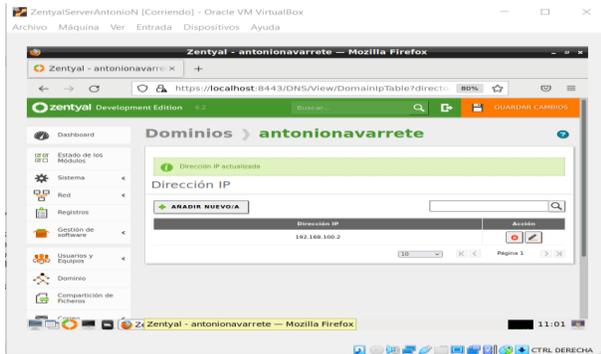


Figura 22. Añadiendo IP al Dominio. Por Antonio Navarrete

Posterior a esto procedemos a iniciar la máquina del cliente donde evidenciamos que la DNS quedó configurada.

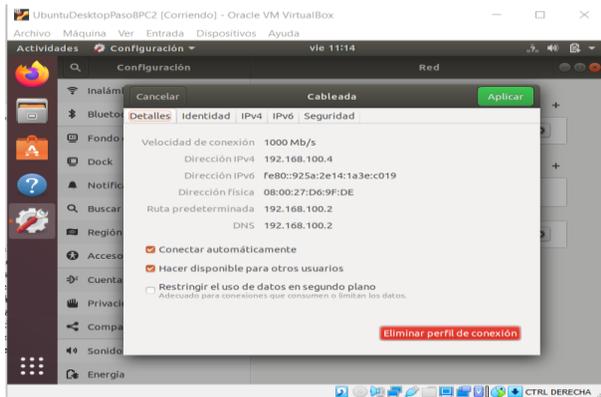


Figura 23. Verificación DNS. Por Antonio Navarrete

4.3 Controlador de dominio

Procedemos a verificar en el módulo DHCP, la tarjeta de red eth0 en la opción configuraciones la opción de dominio de búsqueda este como dominio de Zentyal.

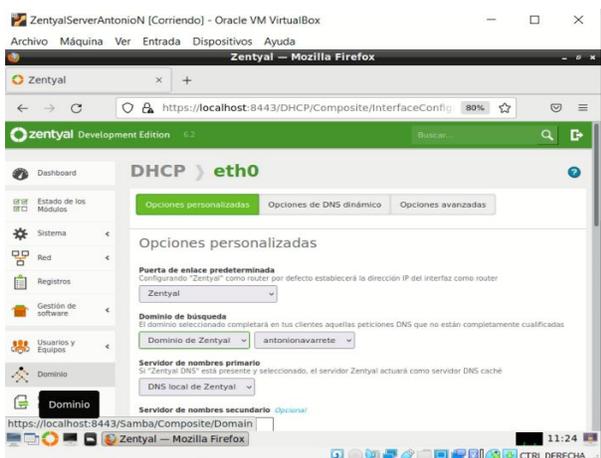


Figura 24. Dominio de Búsqueda. Por Antonio Navarrete

Procedemos a ir al módulo de usuarios y equipos, allí crearemos un usuario nuevo que vamos a agregar al grupo de administradores.

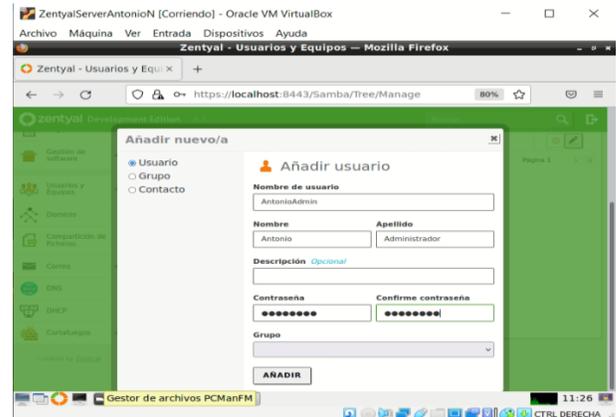


Figura 25. Creación de Usuario. Por Antonio Navarrete

Ahora nos dirigimos al módulo de dominio donde veremos que este activo la opción de función del servidor y el reino donde estará nuestro dominio.

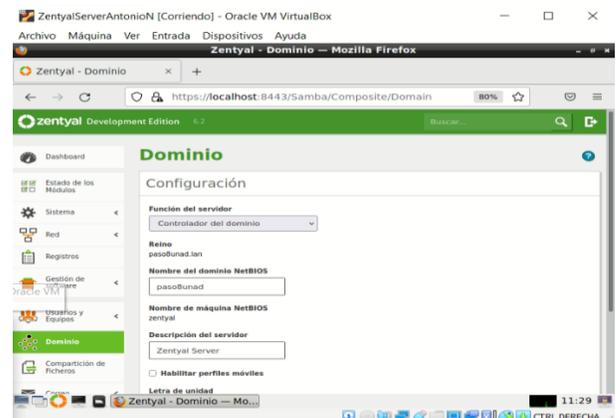


Figura 26. Creación de Usuario. Por Antonio Navarrete

Después de esto iniciamos la máquina virtual con el equipo cliente e iniciamos la terminal, posterior a esto debemos modificar el archivo "resolv.conf", en este archivo direccionamos el equipo al servidor.

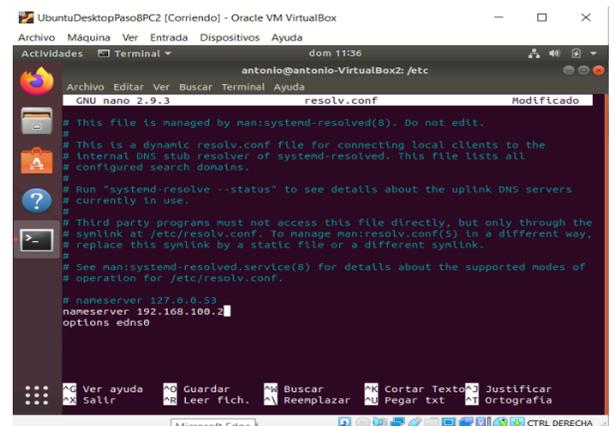


Figura 27. Direccionamiento Servidor. Por Antonio Navarrete

4.4 Proxy no transparente

Nos dirigimos a “Estados de módulos” en el panel izquierdo del Dashboard, para verificar que los servicios de Proxy HTTP, se encuentren activados. De no ser así, marcamos la casilla de estado y aceptamos la reconfiguración del sistema.

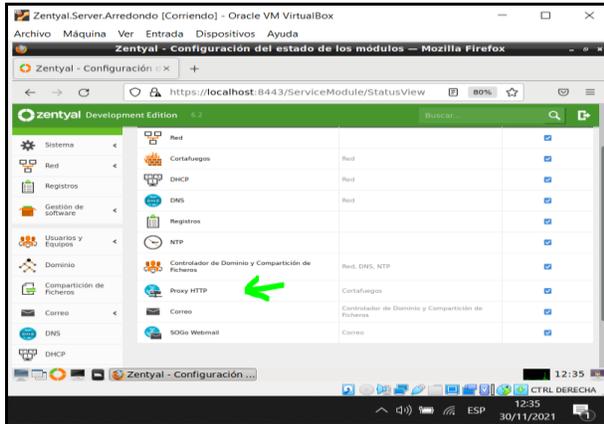


Figura 28. Servicios de Proxy HTTP. Por Jorge Arredondo

En la sección de Proxy HTTP, que aparece en el panel izquierdo del Dashboard, desplegamos las opciones y escogemos la primera que dice “Configuración general”.

Se nos despliega un menú de configuración y en la casilla que dice puerto, estaremos escribiendo el puerto 1230, por el cual deseamos filtrar las salidas de peticiones a Internet.

Si quisiéramos, podríamos marcar la casilla de Proxy Transparente para que también filtre los sitios seguros https, esto dentro de otras opciones de configuración general, como el aumento de la caché para el almacenaje en los ficheros.

En nuestro caso, solo estaremos asignado el puerto de escucha para este tipo de peticiones.

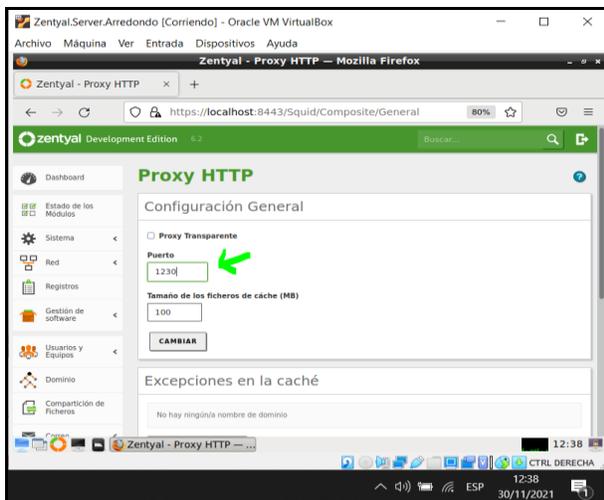


Figura 29. Puerto 1230. Por Jorge Arredondo

En el módulo de Proxy HTTP, escogemos ahora la opción “Perfiles de filtrado”, hacemos clic en “Añadir nuevo”, y asignamos un nombre característico a nuestro nuevo perfil de filtrado de dominios y URLs, el cual llamaremos “Paginas_Noticias”, y damos de nuevo clic en “Añadir”.

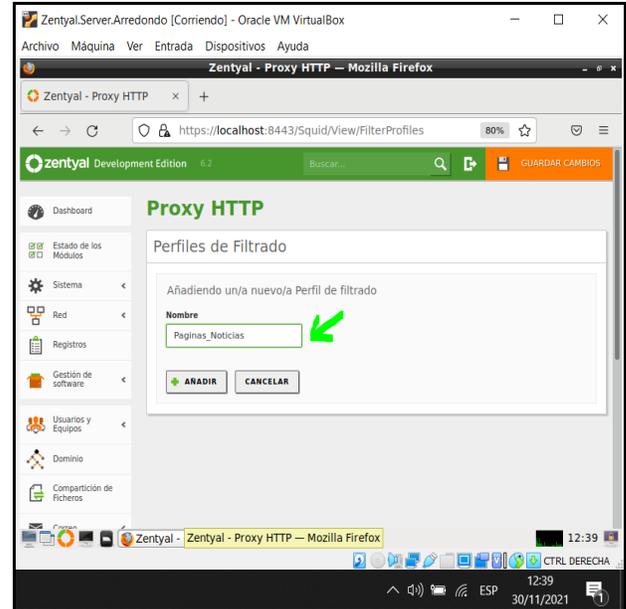


Figura 30. Perfil de filtrado. Por Jorge Arredondo

Una vez que aparezca listado nuestro nuevo perfil de filtrado, hacemos clic en el botón de configuración, para que nos permita definir el nivel de restricción.

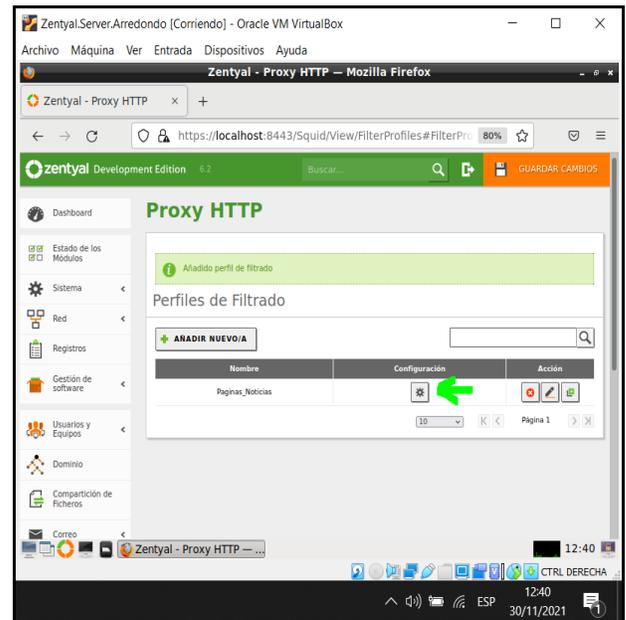


Figura 31. Configuración del perfil. Por Jorge Arredondo

En la primera opción de configuración, podemos asignar un umbral de restricción a este perfil que, en nuestro caso, lo estaremos definiendo en “Estricto”, y presionamos el botón “Cambiar”.

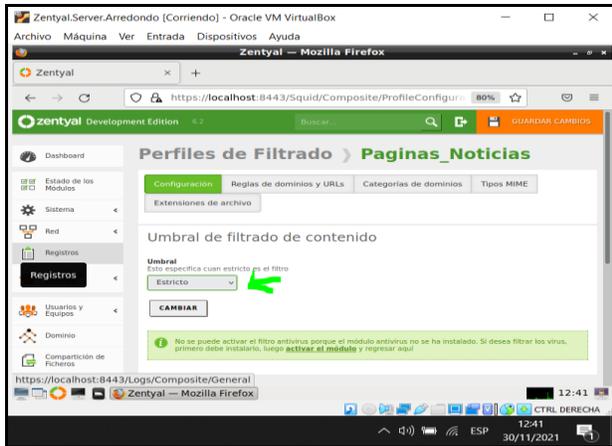


Figura 32. Umbral de restricción. Por Jorge Arredondo

Estando aún en la opción de configuración del perfil de filtrado, hacemos clic en la pestaña con la opción "Reglas de dominios y URLs" y damos clic en "Añadir nuevo".

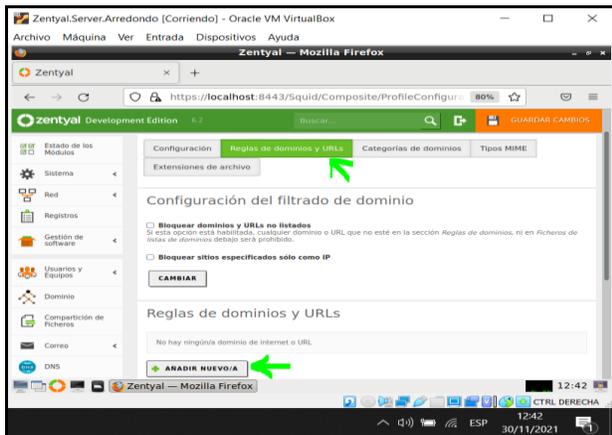


Figura 33. Reglas de dominios. Por Jorge Arredondo

Procedemos entonces a ingresar todos los dominios que queremos filtrar, asignando la opción "Denegar", para que se restrinja el acceso a los mismos. Para nuestro ejemplo y según el perfil de filtrado, restringimos el acceso a tres portales de noticias.

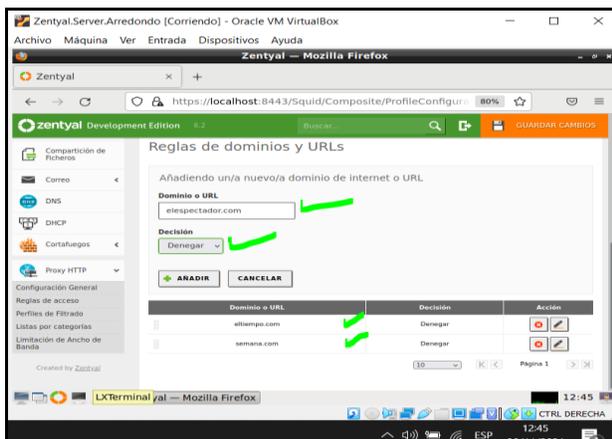


Figura 34. Dominios restringidos. Por Jorge Arredondo

Nos dirigimos de nuevo a las opciones principales en el módulo Proxy HTTP, y esta vez seleccionamos la opción "Reglas de acceso". Eliminamos cualquier regla que esté allí creada, para que tome como eje principal del filtrado, nuestro perfil creado. Damos clic en "Añadir nuevo". En el formulario que se nos presenta escogemos como origen, cualquier terminal o dispositivo que esté conectado a la red, que esté realizando la petición del servicio. Le indicamos como decisión "Aplicar perfil de filtrado" y en la casilla de enseguida, seleccionamos el perfil de filtrado que hemos configurado anteriormente.

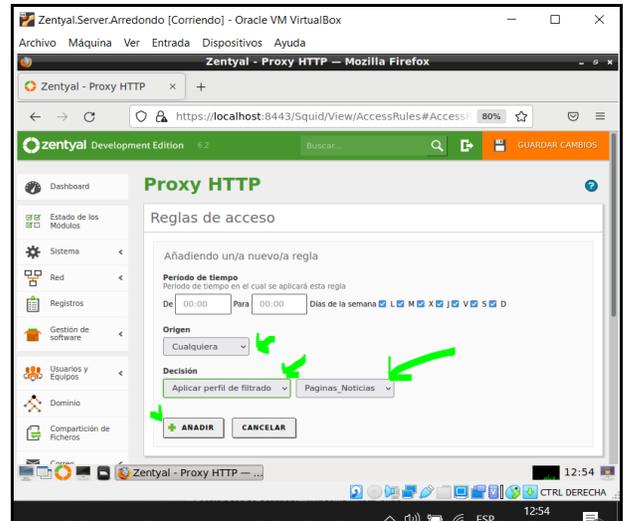


Figura 35. Regla de acceso. Por Jorge Arredondo

Después de haber creado, configurado e implementado nuestro Proxy no transparente, procedemos a guardar todos los cambios del mismo en el sistema. Damos clic en el botón naranja "Guardar cambios".

Ahora procedemos a abrir nuevamente nuestra MV cliente, para configurar el Proxy de red. Para esto una vez cargada nuestra máquina con Ubuntu desktop, nos dirigimos a configuración de red y hacemos clic en el botón de configuración de Proxy de la red

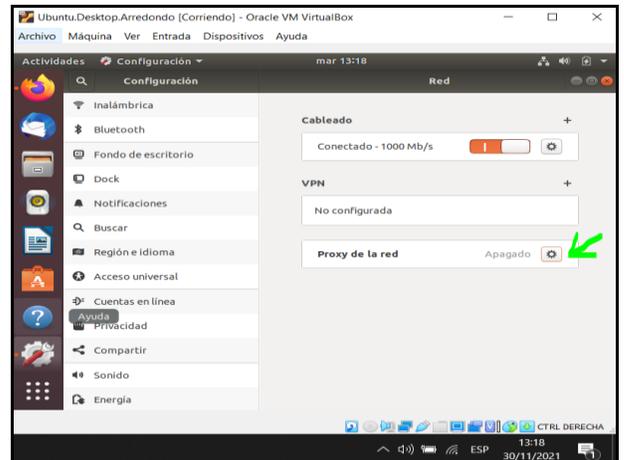


Figura 36. Cliente, configuración proxy. Por Jorge Arredondo

Configuramos de forma manual, ingresando en la casilla de "Proxy para HTTP", la IP donde se origina nuestro proxy, la cual es 192.168.100.2, y en la casilla contigua ingresamos el puerto de escucha por el cual se filtrarán las peticiones: 1230.

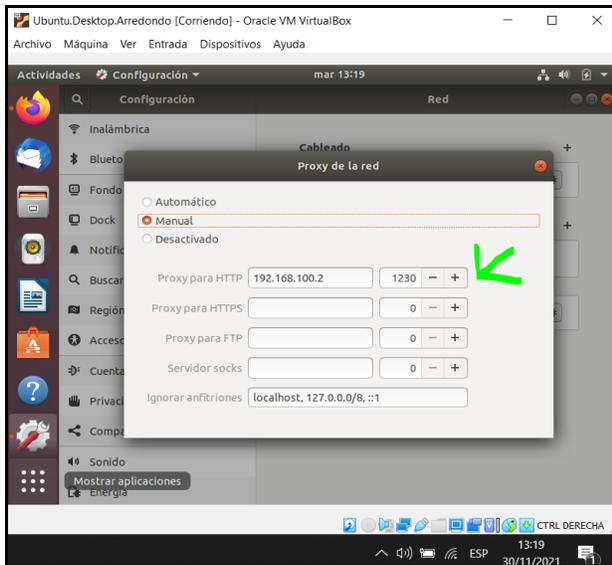


Figura 37. Proxy para HTTP. Por Jorge Arredondo

Ahora procedemos a realizar las pruebas que como producto esperado se infiere la negación del acceso a los dominios de los portales de noticias que hemos configurado en las reglas de dominios y URLs.

Como prueba intentamos ingresar a los portales: <http://semana.com>, <http://eltiempo.com> y al portal <http://elespectador.com>.

Como resultado nos encontramos con la negación de acceso a estos dominios, y se nos presenta una página generada por Zentyal, donde indica que la configuración de control de acceso evita que estas solicitudes sean resueltas para el cliente que hace la petición.

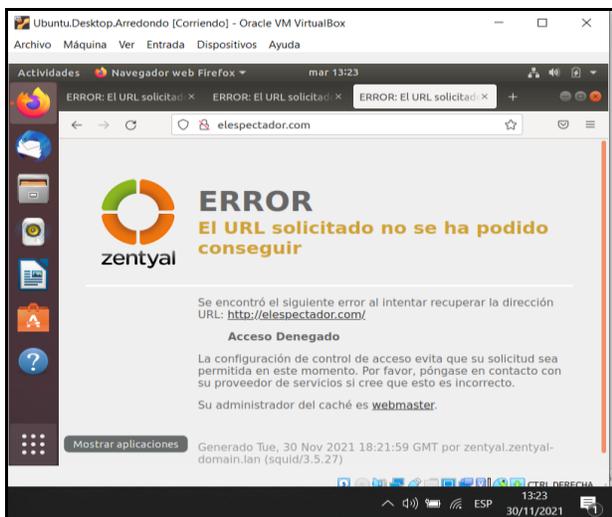


Figura 38. Proxy restringe acceso. Por Jorge Arredondo

Para verificar que el Proxy no transparente, efectivamente está restringiendo el acceso en virtud del perfil de filtrado, las reglas de dominios y la regla de acceso, intentamos ingresar al dominio <http://www.elnuevoherald.com> y el resultado es exitoso, incluso redirigiendo a un enlace seguro.



Figura 39. Proxy permite acceso. Por Jorge Arredondo

4.5 Firewall

A continuación, se realiza la implementación y configuración de firewall, el cual restringe el ingreso a redes sociales, su configuración se realizará mediante el servidor zentyal. Su validación se hará mediante cliente desde la estación de trabajo GNU/Linux Ubuntu Desktop.

Para empezar con la configuración del cortafuego, nos dirigimos a crear las reglas, en cortafuegos, filtrado de paquetes.

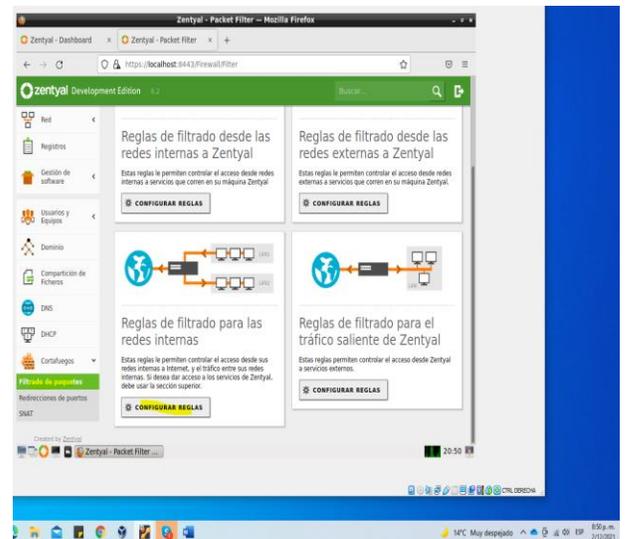


Figura 40. Filtrado de paquetes. Por Blanca Montaña

Se verifica desde Ubuntu la ip de Facebook la cual se le va a restringir. Antes de guardar los cambios con un ping muestro que si tenga ingreso a la página.

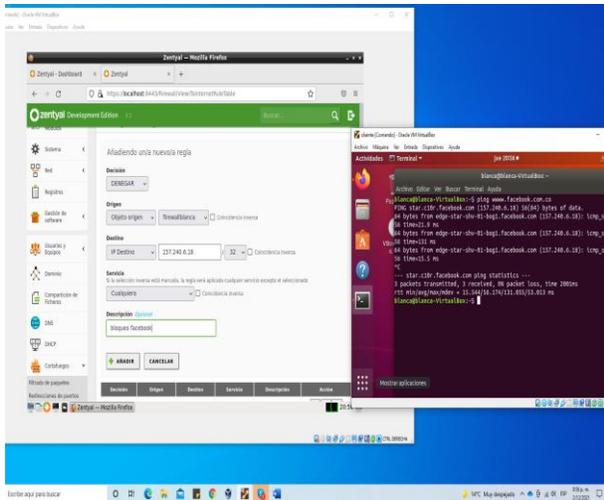


Figura 41. Configuración reglas. Por Blanca Montaña

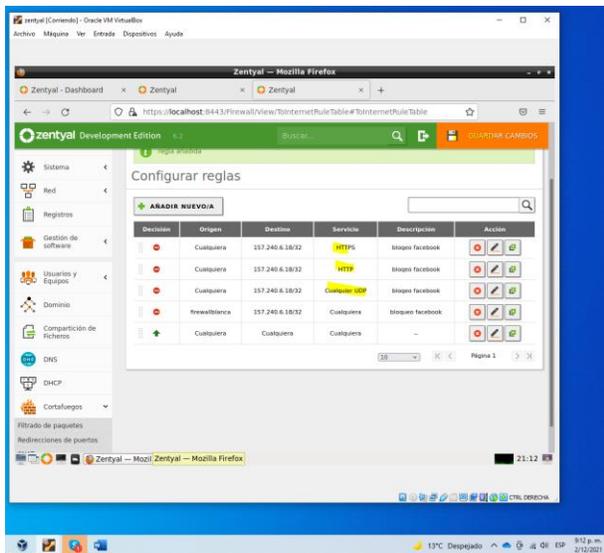


Figura 42. Configuración reglas. Por Blanca Montaña

Ahora podemos confirmar que ya no tenemos ingreso a la página de Facebook, realizar el mismo proceso para cada sitio a restringir.

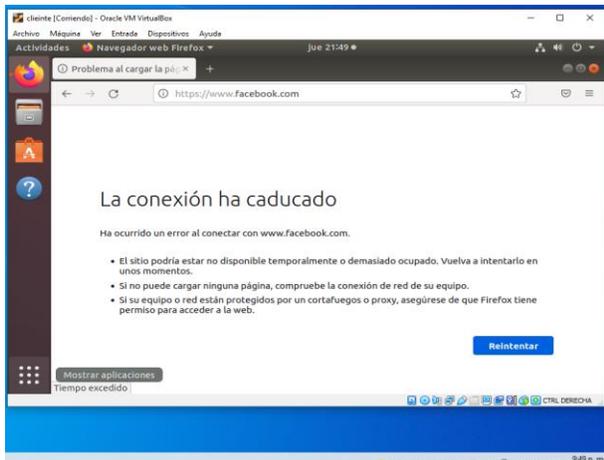


Figura 43. Verificación Ubuntu Desktop. Por Blanca Montaña

4.6 File Server

Para realizar el proceso de compartir archivos dentro de nuestro servidor Zentyal, debemos instalar los módulos de controlador de dominio, compartición de archivos y DNS. Este proceso lo podemos buscar desde el gestor de software.

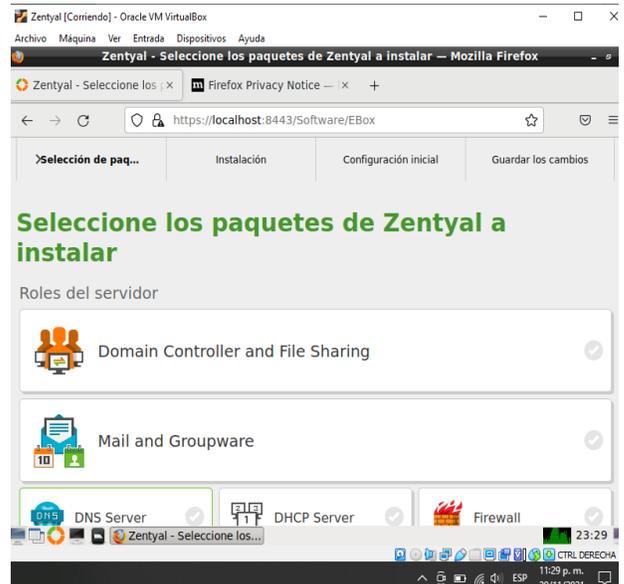


Figura 44. Instalación de software. Por Nelly Bulla

Nos dirigimos a la pestaña de DNS, procedemos a agregar los DNS y se nos habilita la opción de habilitar cache del DNS transparente, la cual procedemos a activar.

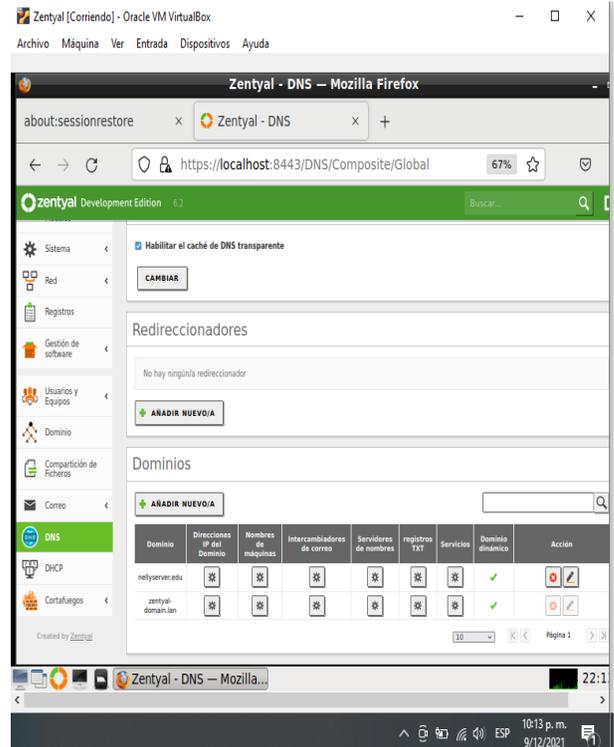


Figura 45. Configuración de la pestaña DNS. Por: Nelly Bulla

Procedemos a validar la configuración del dominio en la pestaña que encontramos en el menú de dominio.

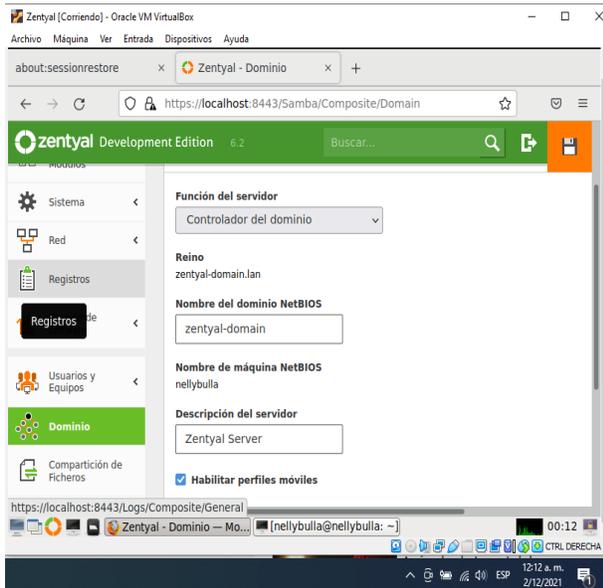


Figura 46. Configuración de pestaña dominio. Por: Nelly Bulla

Para realizar la configuración de las carpetas que vamos a compartir ingresamos a la pestaña que dice usuarios y equipos, donde vamos a agregar los usuarios que van a tener permisos para ingresar a las carpetas compartidas posterior a eso creamos nuestras carpetas a compartir.

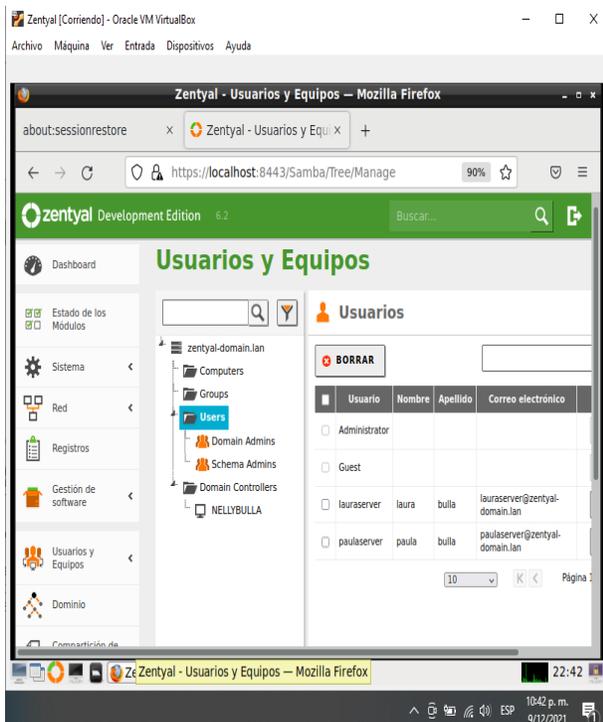


Figura 47. Creación de usuario. Por: Nelly Bulla

Vamos a la pestaña compartición de ficheros y creamos la carpeta

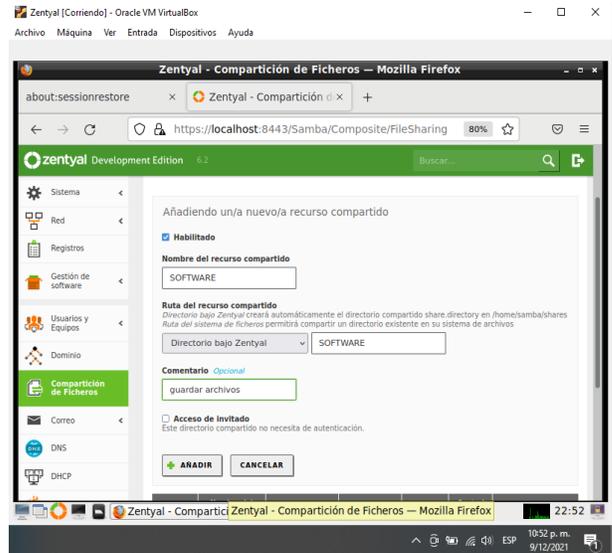


Figura 48. Creación de la carpeta. Por: Nelly Bulla

Procedemos a darle los permisos a la carpeta solo seleccionamos el usuario y los permisos que queremos dejarle ya sea administrador, lectura escritura o solo lectura, guardamos cambios.

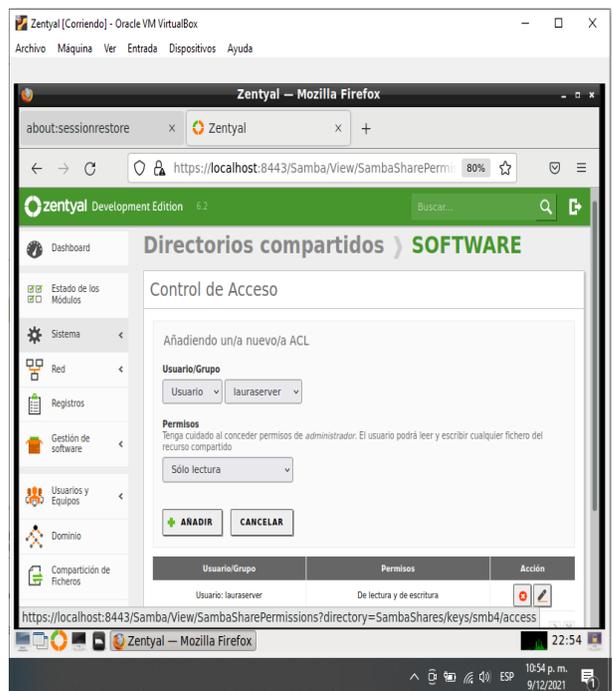


Figura 49. Permisos. Por: Nelly Bulla

Para finalizar procedemos a ingresar a nuestro equipo el cual se encuentra en la misma red, abrimos una carpeta y le damos la opción que dice otras ubicaciones y colocamos en la parte inferior en el cuadro donde dice conectar el servidor, ingresamos los datos de nuestro servidor smb://192.168.1.60/, una vez realizamos ese proceso nos muestra nuestra carpetas que tenemos compartidas, procedemos a abrirla y nos pide los datos de autenticación para nuestro caso son los datos de los usuarios creados.

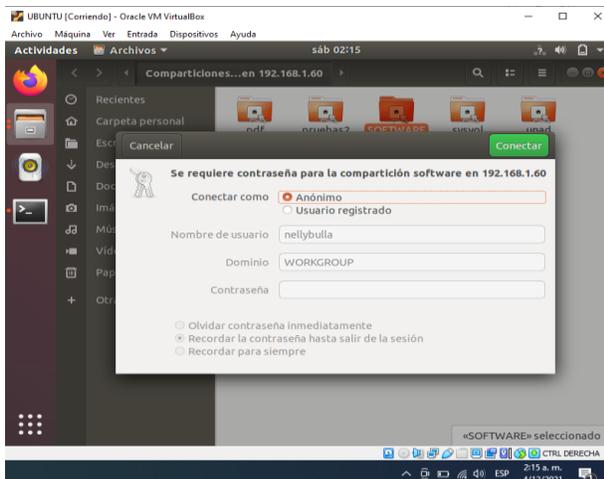


Figura 50. Configuración carpetas cliente. Por: Nelly Bulla

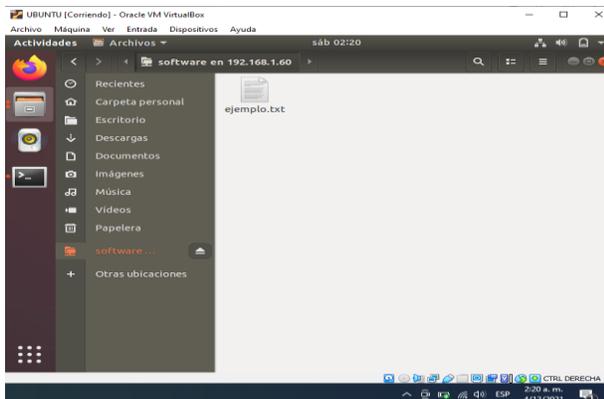


Figura 51. Copia de la carpeta compartida. Por: Nelly Bulla

4.7 Print Server

Para la configuración del Print Server no se puede realizar directamente en Zentyal, ya que esta opción dejó de funcionar desde la versión 5.1, pero se puede integrar con CUPS, por lo cual se instala y crea la impresora.

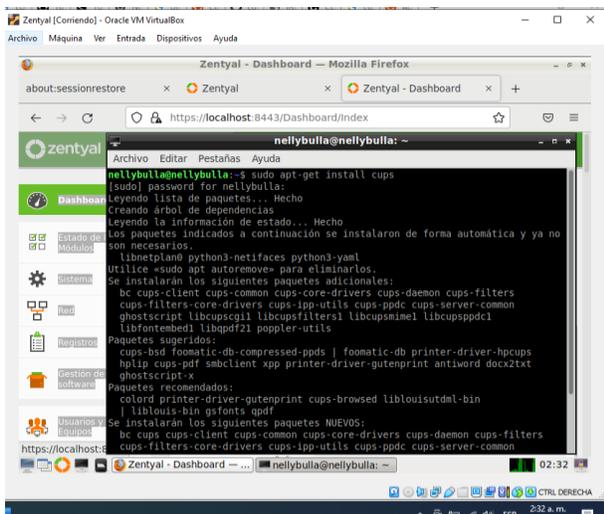


Figura 52. Instalación cups en servidor Zentyal. Por Nelly Bulla

Se entra a la consola de configuración <https://localhost:631/admin>, esto debido a que es una instalación local en el zentyal y se realiza la creación de la impresora.

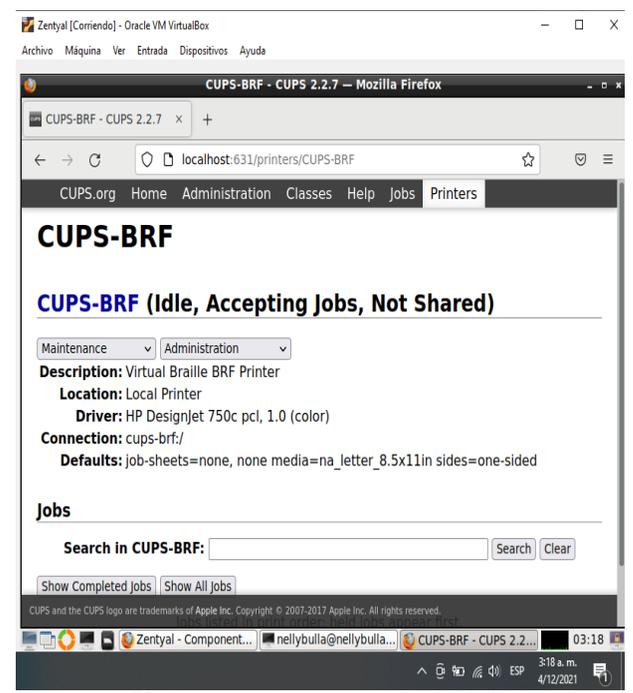


Figura 53. Creación de impresora. Por Nelly Bulla

Ahora procedemos a configurar la impresora en nuestra máquina local

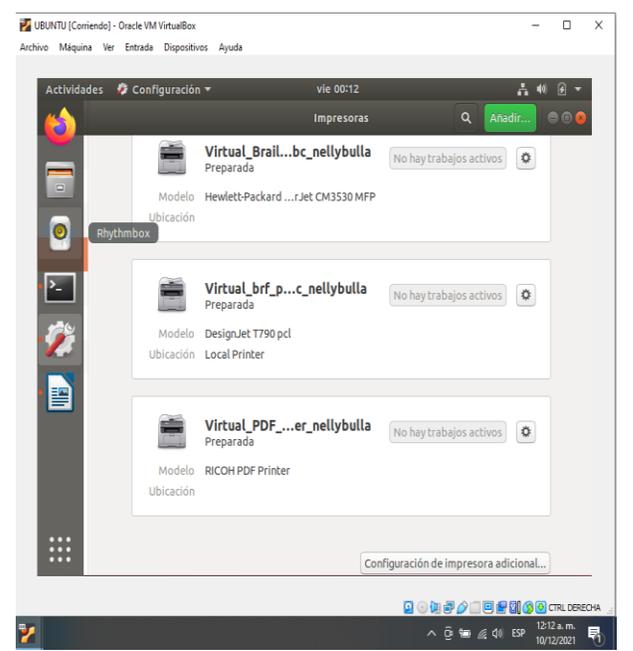


Figura 54. Visualización de impresoras. Por Nelly Bulla

4.8 VPN

Lo primero es el Certificado de la Autoridad de Certificación para el Servidor y para el Cliente.

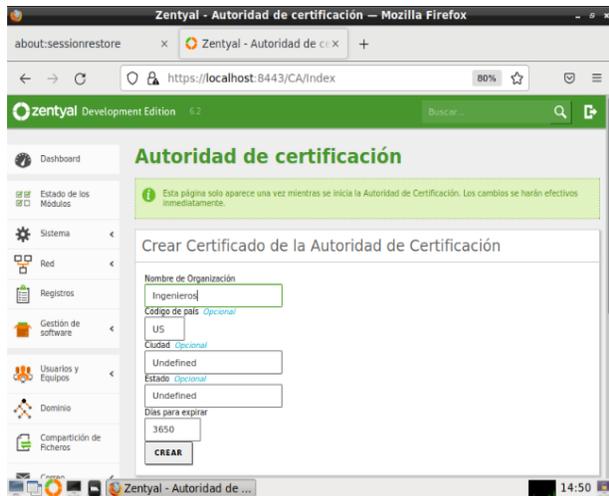


Figura 55. Certificación Servidor. Por: Aura Acosta

A continuación, creamos el Certificado del Cliente.

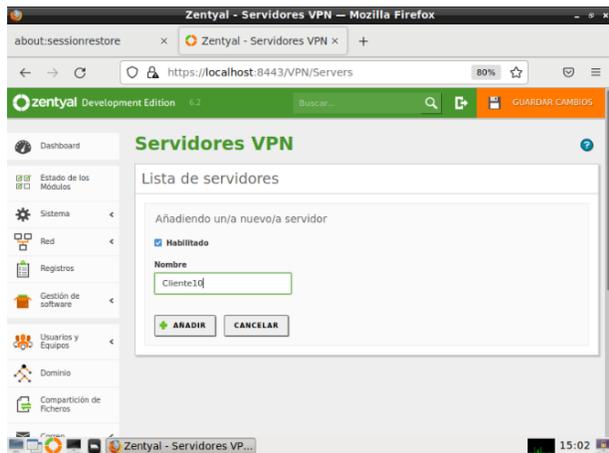


Figura 56. Certificación Cliente. Por: Aura Acosta

Ahora vamos a crear el Servidor VPN.

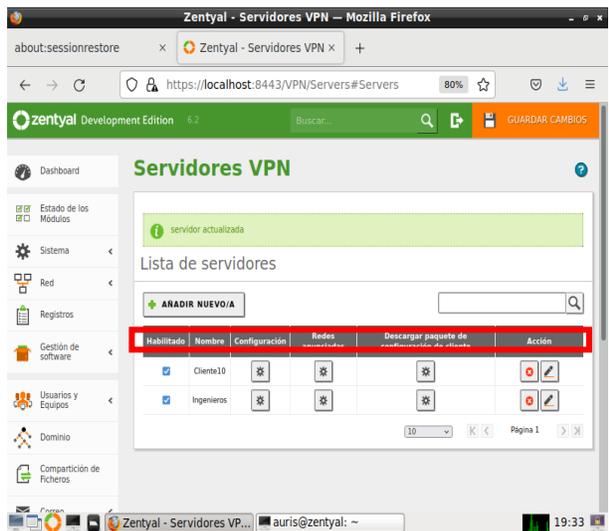


Figura 57. Servidores. Por: Aura Acosta

Configuramos el Servidor llamado Ingenieros.

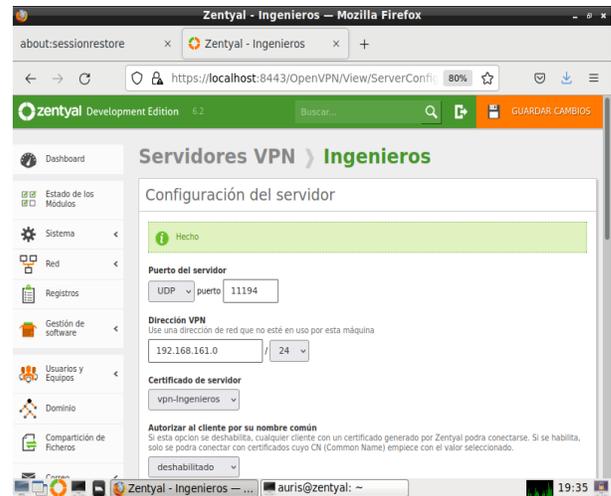


Figura 58. Configuración Servidor VPN. Por: Aura Acosta

Vamos al Módulo Red, después Servicios y añadimos un servicio.

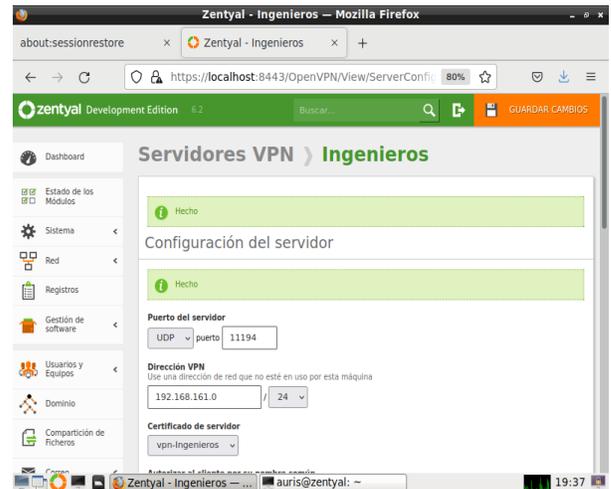


Figura 59. Añadir Servicios. Por: Aura Acosta

Vamos al Módulo Cortafuegos y vamos a darle permisos desde el cortafuego para permitir el acceso

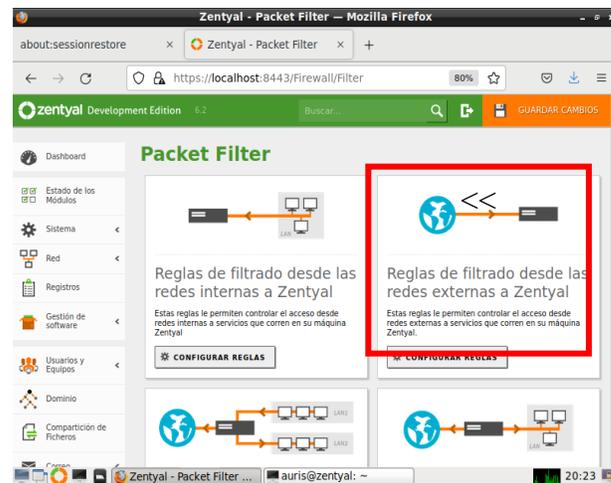


Figura 60. Configuración permisos. Por: Aura Acosta

Ahora vamos a los servidores VPN para descargar el certificado y tener acceso desde cualquier máquina.

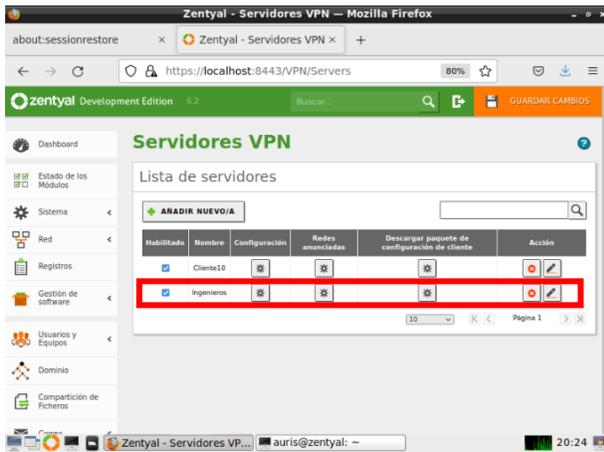


Figura 61. Descargar Certificado. Por: Aura Acosta

Verificación del estado del servicio y si está activo.

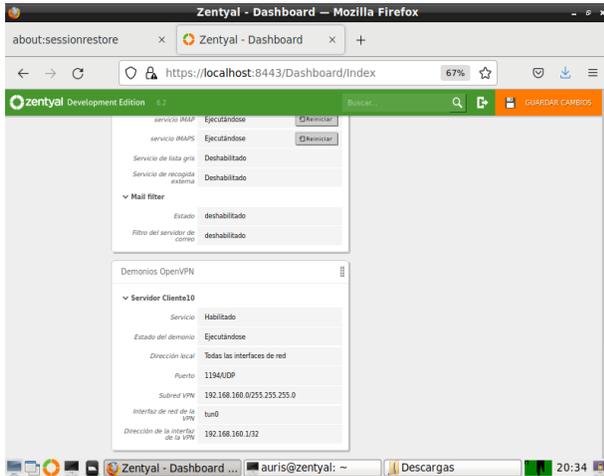


Figura 62. Confirmando estado. Por: Aura Acosta
Vamos a la MV-Cliente y vamos a instalar open VPN.

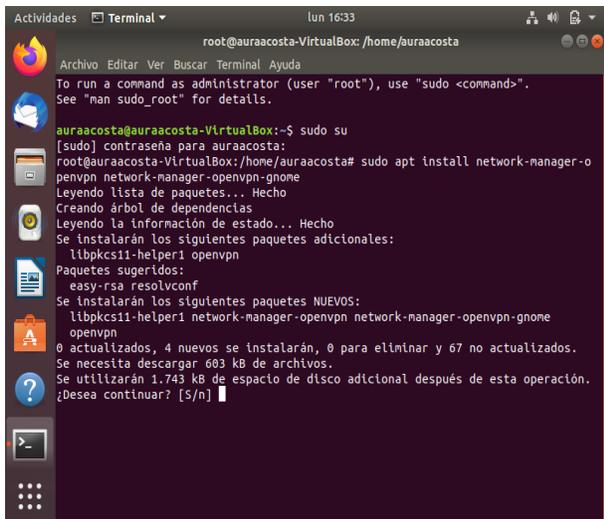


Figura 63. Instalar open VPN en Cliente. Por: Aura Acosta

Habilitar y ver el estado del servicio de Open VPN.

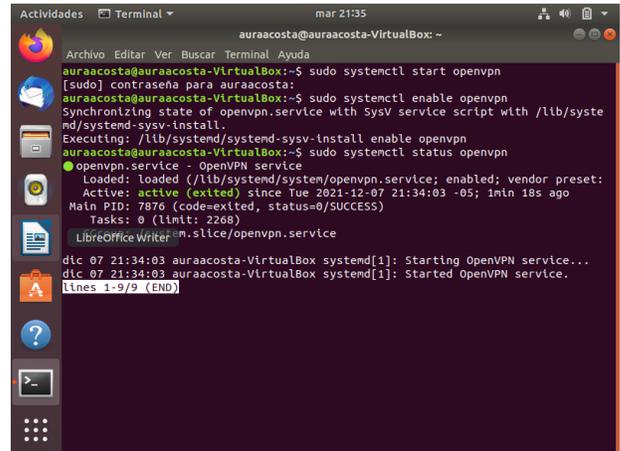


Figura 64. Habilitar estado del servicio. Por Aura Acosta

Descargamos el paquete de Zentyal y lo llevamos a /etc/openvpn/.

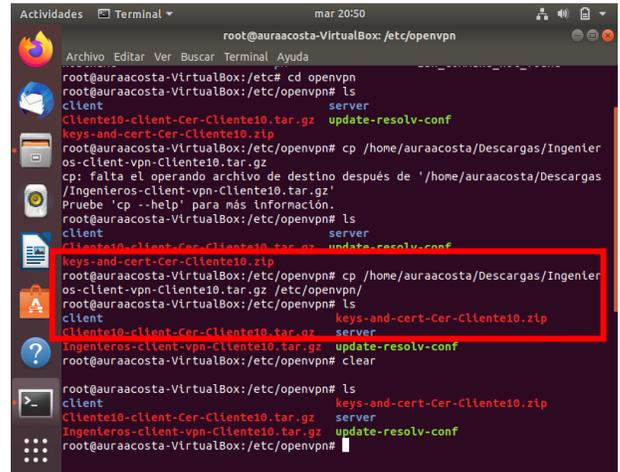


Figura 65. Instalar openvpn en Cliente. Por: Aura Acosta
Verificamos que haya conexión entre Zentyal Server y el cliente.

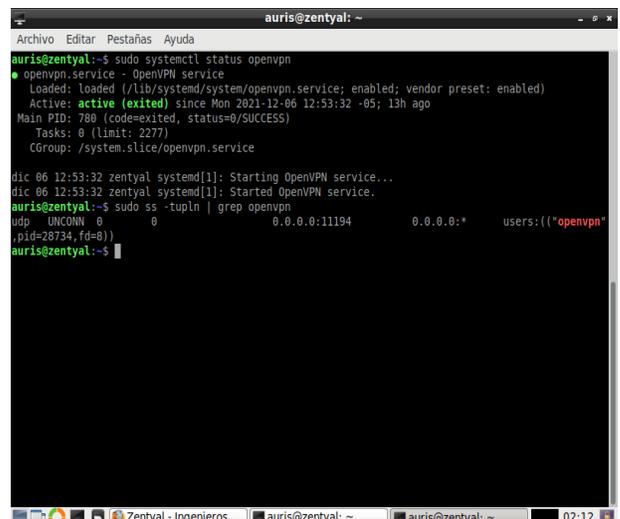


Figura 66. Verificación de estado. Por: Aura Acosta

```

auris@zentyal: ~
Archivo Editar Pestañas Ayuda
auris@zentyal:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid lft forever preferred lft forever
    inet 127.0.1.1/8 scope host secondary lo
        valid lft forever preferred lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2d:ff:22 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.100/24 brd 192.168.10.255 scope global eth0
        valid lft forever preferred lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e0:ac:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.2/24 brd 192.168.100.255 scope global eth1
        valid lft forever preferred lft forever
8: tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100
    link/none
    inet 192.168.161.1 peer 192.168.161.2/32 scope global tun1
        valid lft forever preferred lft forever
auris@zentyal:~$

```

Figura 67. Ejecución openvpn. Por: Aura Acosta

5 CONCLUSIONES

Este informe deja en evidencia lo sencillo e intuitivo que resulta instalar y configurar de forma básica el gestor de servidores Zentyal.

Desde la instalación se facilita la configuración de las interfaces de red, asignando en ellas nuestra tabla prediseñada de direccionamiento IP, discriminando en ellas las zonas de acción (roja, naranja y verde). Configuración que se complementa luego con los servicios DHCP, que permiten mediante formularios claros y sencillos, listar las diferentes interfaces y crear rangos de redistribución dinámica IP.

Si deseamos que nuestro servidor Zentyal sea un DNS para nuestra subred, debemos apuntar una de las NIC del servidor a la dirección IP del mismo y configurarlo para que sea al tiempo un servidor DHCP para la LAN interna. De esta manera, nuestro servidor Zentyal y nuestro PDC (Primary Domain Controller – Controlador de dominio primario) actual no competirán por quién está a cargo con los servicios DNS DHCP para nuestra subred.

Es importante que recordemos que las NIC de Zentyal deben configurarse con una IP estática que no entre en conflicto con otros hosts de nuestra subred y de esta manera nuestra NIC interna actuará como puerta de enlace predeterminada para todos nuestros clientes en la LAN.

<- (módem) <--> (enrutador) <- (servidor PDC / AD) <--> NIC externa (servidor Zentyal-DNS / DHCP) NIC interna <--> (clientes).

La implementación de Proxys transparentes y no transparentes es muy práctica, pues maneja un menú de opciones muy ágil, que permite en pocos pasos, realizar una configuración básica del mismo, crear reglas de acceso, generar perfiles de filtrado, listar categorías y definir el ancho de banda.

Esto simplifica el trabajo que a lo largo del curso se aprendió a realizar de forma nativa desde consola en el servidor de distribución Linux, actuando directamente en las Iptables y configurando en este cortafuego vinculado al kernel de Linux, creando las reglas de filtrado y aun configurando las NAT.

También tuvimos la oportunidad de a través de pfSense que actúa como firewall, instalar el módulo de Squid que trabajaba como proxy de red, y aunque su uso es más práctico que el desarrollado directamente en las iptables, su configuración nunca fue tan intuitiva, práctica y sencilla como nos lo presenta Zentyal.

Hemos dado soluciones a las problemáticas presentadas de migración de sus sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, ahora, orientados a la puesta en marcha de servicios de infraestructura IT para Intranet y Extranet, presento la solución con esta red privada virtual (VPN) para darle una mayor seguridad en las comunicaciones.

Esta implementación del VPN nos permite conectarnos de forma remota desde cualquier lugar del mundo con una alta confiabilidad en los datos y en los lugares donde estemos conectados.

Los pasos para la configuración de esta red virtual (VPN), son complicados pero necesarios, si queremos seguridad en las conexiones e información confiable.

Realizar la configuración de reglas firewall ayuda a la restricción de páginas no laborales y evita el tráfico malicioso antes de que llegue al computador. Por supuesto, Zentyal nos permite realizar una configuración del cortafuego, de una manera cómoda y confiable, configurando protocolos, reglas y permisos de forma intuitiva.

La configuración del File Server en Zentyal, nos evidenció con claridad la forma en que el servidor está dedicado a almacenar archivos en una ubicación centralizada mientras permite el acceso a las computadoras en la subred. Al tener un File Server, los usuarios pueden ahorrar trabajo y tener acceso a los archivos sin tener que llevar un disco, y este servicio es fácilmente configurable gracias a la practicidad que presenta Zentyal.

El Print Server administra las impresoras en la red. Todos los datos que se van a imprimir se pasan al servidor de impresión que asigna trabajos a las impresoras de la red. Esta configuración al igual que el File Server, es fácilmente implementada en Zentyal.

6 REFERENCIAS

[1] Guzmán D. A. (2021, Nov 30), "Evaluación final por POA. Web conferencia No. 8. Presentación en Power Point". [En línea] Disponible en: <https://campus109.unad.edu.co/ecbt96/pluginfile.php/303/lo>

- cal_mail/message/54515/Octava%20WebConferencia%20Curso%20201494.pptx?forcedownload=1
- [2] Guzmán D. A. (2021, Nov 30), "Paso 8 - Solucionando necesidades específicas con GNU/Linux. Formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos". [En línea] Disponible en: <https://bit.ly/3Ed73xe>.
- [3] UNAD (2021, nov. 30), "Paper IEEE", [En línea] Disponible en: https://campus109.unad.edu.co/ecbti96/pluginfile.php/303/local_mail/message/54515/Paper%20IEEE.doc?forcedownload=1.
- [4] Zentyal (2021), "Zentyal 6.2 Documentación Oficial", [En línea] Disponible en: <https://doc.zentyal.org/6.2/es/>.
- [5] Zentyal (2021), "Virtual private network (VPN) service with OpenVPN - Configuration of an OpenVPN server with Zentyal", [En línea] Disponible en: <https://doc.zentyal.org/en/vpn.html>.
- [6] Solvetic Sistemas (2020), "Cómo instalar VPN en Ubuntu 20.04", [En línea] Disponible en: <https://www.solvetic.com/tutoriales/article/8441-como-instalar-vpn-en-ubuntu-20-04/>.
- [7] Agudelo S. (2021), "Zentyal como cortafuegos", [En línea] Disponible en: <https://www.youtube.com/watch?v=zdTobQh7GW0>
- [8] Cezar M. (2015), "Setup File Sharing and Permissions for All Users in Zentyal 3.4 PDC – Part 4", [En línea] Disponible en: [https://www.tecmint.com/setup-file-sharing-in-zentyal-3-4-pdc/#:~:text=Go%20to%20File%20Sharing%20Module,from%20command%20line%20\)%20and%20lastly](https://www.tecmint.com/setup-file-sharing-in-zentyal-3-4-pdc/#:~:text=Go%20to%20File%20Sharing%20Module,from%20command%20line%20)%20and%20lastly)
- [9] Zentyal. (2021), "Printer server configuration with Zentyal", [En línea] Disponible en: https://wiki.zentyal.org/wiki/En/4.0/Printers_sharing_service
- [10] Zentyal. (2021), "En/4.0/Configuring a file server with Zentyal", [En línea] Disponible en: https://wiki.zentyal.org/wiki/En/4.0/Configuring_a_file_server_with_Zentyal