

# SERVICIOS ÚTILES EN ZENTYAL SERVER EN GNU/LINUX

Diego Armando Vásquez Padilla  
e-mail: [davasquezp@unadvirtual.edu.co](mailto:davasquezp@unadvirtual.edu.co)  
Brayan Jesus Romero Reyes  
e-mail: [bjromeror@unadvirtual.edu.co](mailto:bjromeror@unadvirtual.edu.co)  
Jhon Eduar Cespedes Dicelis  
e-mail: [jcespedesd@unadvirtual.edu.co](mailto:jcespedesd@unadvirtual.edu.co)  
Brayan Giovany Villalobos Delgado  
e-mail: [bgvillalobosd@unadvirtual.edu.co](mailto:bgvillalobosd@unadvirtual.edu.co)  
Juan David Duarte Beltran  
e-mail: [jdduarteb@unadvirtual.edu.co](mailto:jdduarteb@unadvirtual.edu.co)

**RESUMEN:** *En la actualidad, se busca satisfacer las necesidades específicas del cliente en materia de GNU/Linux, a través del servidor Zentyal Server enfocado a la implementación de servicios de infraestructura intervisible de alto nivel para Intranet y Extranet en instituciones complejas, partiendo de su instalación, configuración y puesta en marcha de los diferentes módulos que ofrece esta completa distribución como alternativa para resolver diferentes problemas a los que se enfrentan las empresas a diario con respecto a la administración y seguridad de redes de datos.*

**Abstract—** *Currently, we seek to meet the specific needs of the customer in terms of GNU/Linux, through Zentyal Server focused on the implementation of high-level intervisible infrastructure services for Intranet and Extranet in complex institutions, starting with the installation, configuration and implementation of the different modules offered by this complete distribution as an alternative to solve different problems faced by companies on a daily basis with respect to the administration and security of data networks.*

**PALABRAS CLAVE:** Zentyal, Proxy, DHCP, DNS, Proxy, Firewall, VPN, Servidor de impresión.

## 1 INTRODUCCIÓN

El objetivo de este artículo es proponer soluciones utilizando GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente, todo ello, a través del sistema operativo Zentyal Server 6.2 bajo el cual se implementarán servicios y plataformas como Servidor DHCP, Servidor DNS y Controlador de Dominio, Proxy, Firewall, Servidor de archivos y servidor de impresión, VPN.

Abstract - The objective of this article is to propose using GNU/Linux through the installation, configuration and start-up of technological infrastructure that allows responding to the specific requirements of the client, all

through the Zentyal Server 6.2 operating system under which Services and platforms such as DHCP Server, DNS Server and Domain Controller, Proxy, Firewall, File Server and Print Server, VPN will be implemented.

## 2 MARCO TEÓRICO

### 2.1 ZENTYAL SERVER

Distribución GNU/Linux con base en Ubuntu en sus versiones más recientes, cuenta actualmente con los principales servicios informáticos usados a nivel global, de gran utilidad en la mayoría de infraestructuras TI, logrando brindar, conectividad, seguridad, trazabilidad, transparencia entre otros beneficios requeridos en una compañía.

## 3 INSTALACIÓN Y CONFIGURACIÓN ZENTYAL

Zentyal se encuentra fácilmente en la web principalmente en su sitio web oficial donde entre sus versiones podemos descargar su versión Development Edition a través del siguiente enlace: <https://zentyal.com/es/comunidad/>

Utilizando el software VirtualBox procedemos a crear la máquina correspondiente

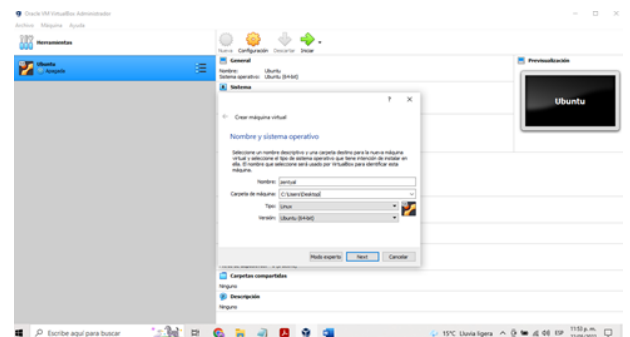


Figura 1. Creación de la VirtualBox

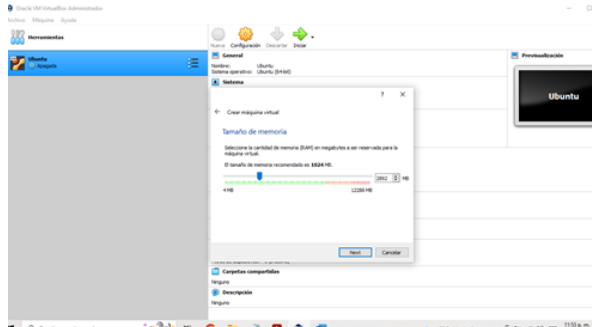


Figura 2. Selección de memoria RAM para la máquina

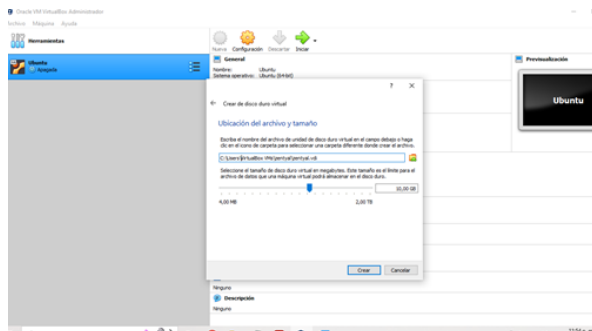


Figura 3. Selección del tamaño del disco duro.

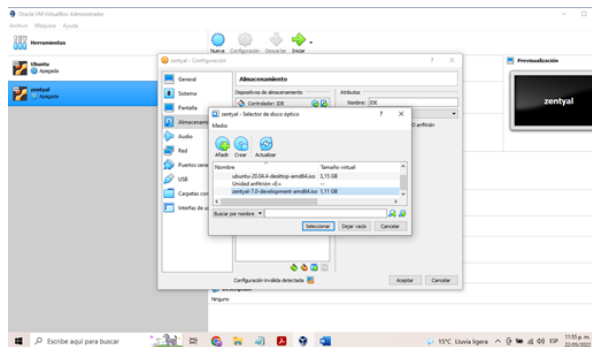


Figura 4. Navegación de imágenes ISO y configuración de red puenteada.

Escogemos la ISO donde se encuentra Zentyal Developments Edition y lanzamos la máquina Virtual.

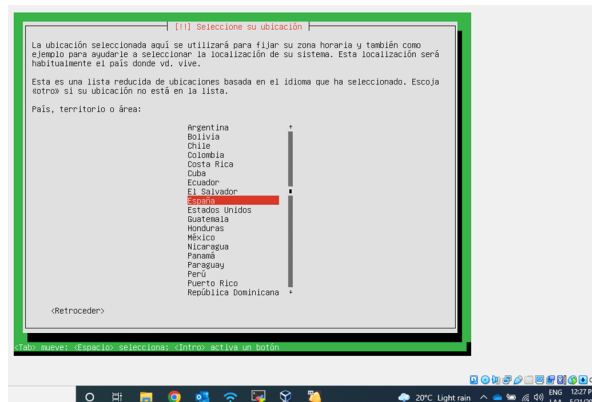


Figura 5. Instalación Zentyal – Selección Idioma

Posteriormente seleccionamos la distribución del teclado, asignamos un nombre a la máquina así como también un nombre de usuario y contraseña, La zona horaria es obtenida automáticamente si la máquina tiene conexión a internet, luego se debe proceder con la configuración de la(s) interface(s) de acuerdo al (los) servicio(s) que sean requeridos.

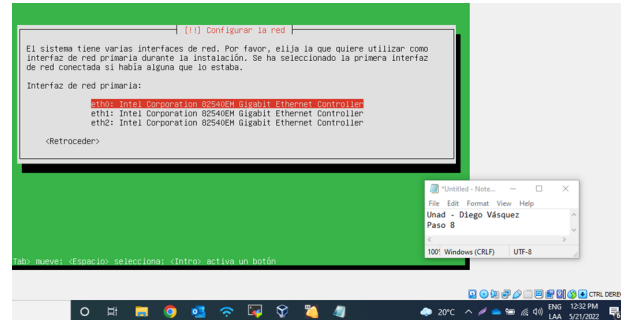


Figura 6. Selección de interfaz desde donde se podrá acceder vía web.

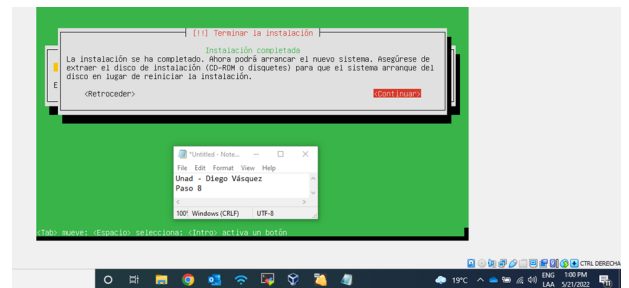


Figura 7. Instalación Finalizada.

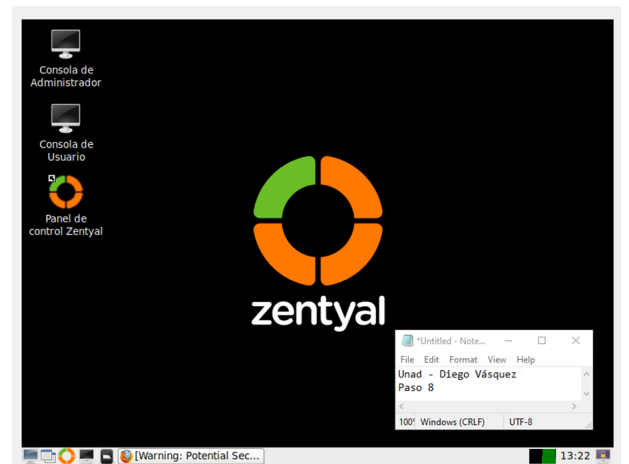


Figura 8. Panel principal Sistema Zentyal.

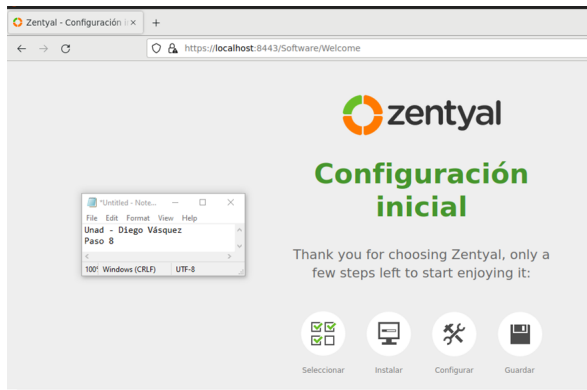


Figura 9. Configuración inicial – De acuerdo a la temática seleccionada se procede a configurar..

## 4 TEMÁTICA 1 - DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Se procede a realizar la configuración inicial correspondiente a la temática seleccionada o servicios a utilizar a través de la configuración inicial una vez finalizada la instalación de Zentyal.

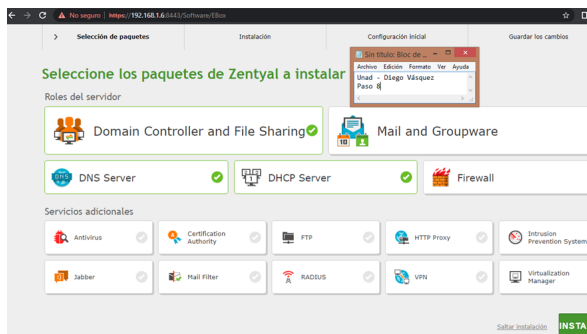


Figura 10. Selección servicios a instalar

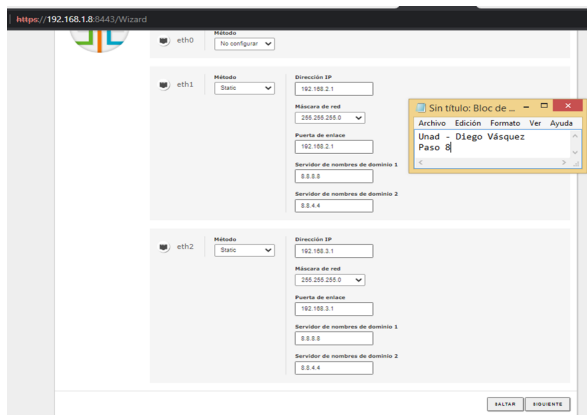


Figura 11. Configuración redes de interfaces según sea el caso o servicio.

## 4.1 DHCP SERVER

En este caso, se usaron 3 interfaces de red con lo cual se debe configurar las mismas para la asignación de direcciones IP, una (1) interfaz para el paso de internet o WAN, las otras dos redes o interfaces son para las redes internas.

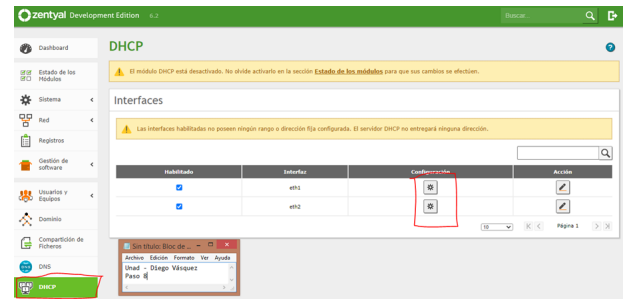


Figura 12. Configuración del servicio DHCP en interfaces eth1 y eth2.

Se debe establecer los rangos de direcciones IPs a asignar de acuerdo a la interfaz que estemos configurando



Figura 13. Configuración rango de asignaciones en eth1

Se realiza el proceso en las interfaces deseadas, se deben guardar los cambios y reiniciar el servicio DHCP para que los cambios sean aplicados.

Se procede a conectar o encender los equipos en las correspondientes interfaces con el fin de probar la asignación de direcciones IP.

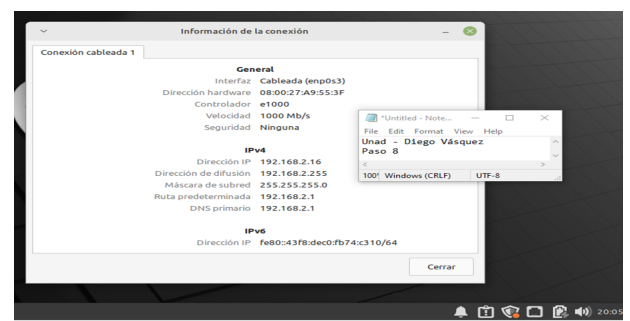


Figura 14. Asignación correspondiente a interfaz eth1 - Linux MINT

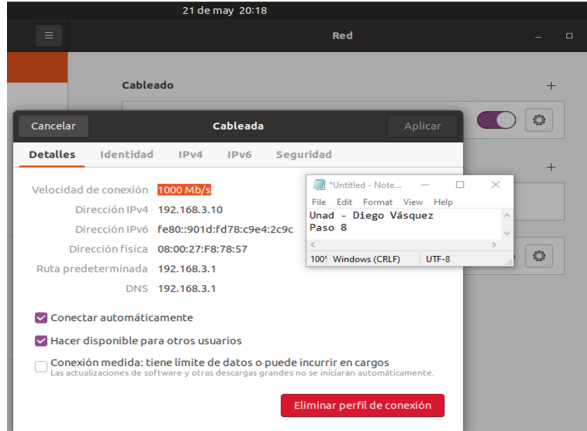


Figura 15. Asignación correspondiente a interfaz eth2 - Linux Ubuntu.

Se procede a comprobar estas asignaciones desde Zentyal



Figura 16. Validación de IPs asignadas desde interfaces eth1 y eth2 - Servicio DHCP.

## 4.2 DNS SERVER

Con la configuración actual se tiene que los equipos conectados a las interfaces eth1 y eth2 tienen conexión entre ellos pero no resuelven direcciones de internet, es por esto que se procede a realizar la configuración de los DNS, para cuando el servidor DNS zentyal no conozca un dominio sepa en qué lugar consultarlo.

Se debe validar que el tráfico entre zonas y también el tráfico entre las zonas internas y el internet esté permitido.

Se debe agregar el redireccionador 8.8.8 de Google y los DNS del operador en este caso movistar, como servidores DNS externos en caso que nuestro servidor Zentyal DNS no encuentre respuesta a una petición.

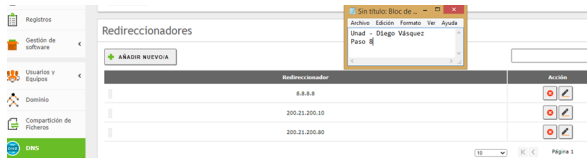


Figura 17. Configuración redirección - Servidor DNS.

Ahora estos equipos ubicados en diferentes zonas deberían encontrar ubicaciones de internet, una vez se realice el siguiente procedimiento.

Se debe configurar las puertas de enlace dejando como predeterminada la interfaz que tiene comunicación con internet o la puerta de enlace (modem de internet operador).

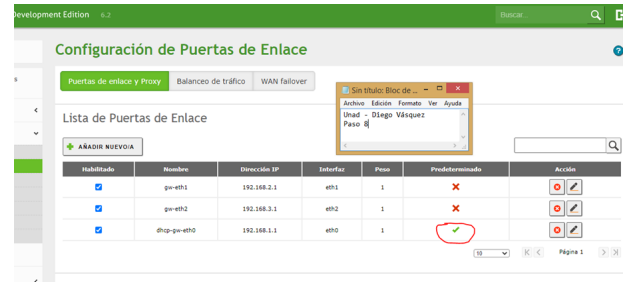


Figura 18. Establecer puerta de enlace predeterminada - Servidor DNS.

Se debe marcar la casilla "externo" en la interfaz que tiene conexión a internet



Figura 19. Se marca casilla Externo (WAN) en la configuración de interfaces - Servidor DNS.

Se agregan unos registros DNS con el fin de probar su funcionalidad en los diferentes equipos.

Se agrega un nombre de máquina en el dominio zentyal.domain.lan la máquina diego-ubuntu



Figura 20. Asignación dirección IP a equipo Ubuntu - Servidor DNS.

También agregamos un alias "ubuntuserver" para que este equipo sea ubicado desde cualquier lugar del dominio.



Figura 21. Asignación de alias para el equipo Ubuntu - Servidor DNS.

Se reinicia el servicio DNS y se procede a comprobar su funcionamiento en una máquina diferente a la creada en los registros DNS.

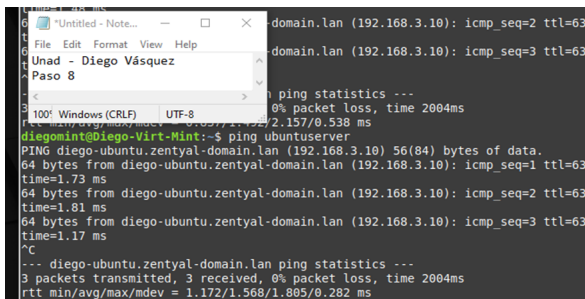


Figura 22. Al hacer ping al Alias ubuntuserver el DNS resuelve la dirección IP correcta - Servidor DNS

### 4.3 CONTROLADOR DE DOMINIO

Se debe crear un usuario con perfil administrativo

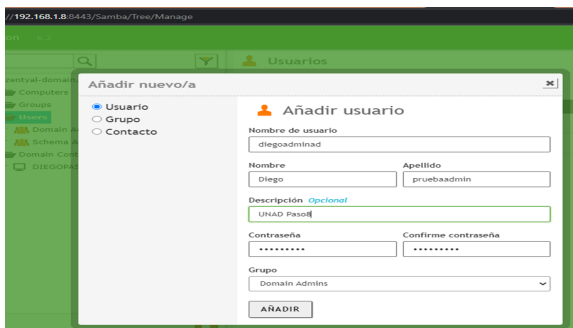


Figura 23. Creación de usuario administrador de dominio - Controlador de dominio.

Se crea otro usuario estándar llamado usuario1



Figura 24. Lista de usuarios del dominio.

Unimos un cliente con sistema Ubuntu 20 Desktop al dominio.

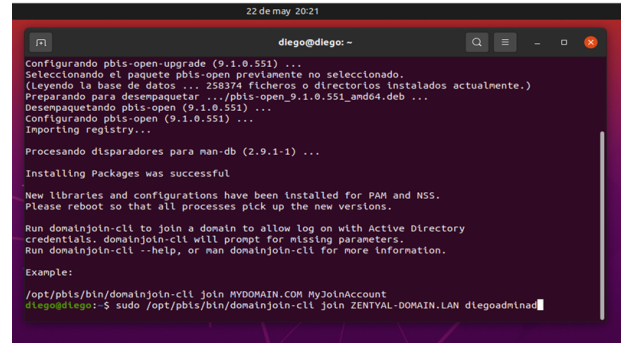


Figura 25. Comando domainjoin-cli para unir nuestro equipo al dominio

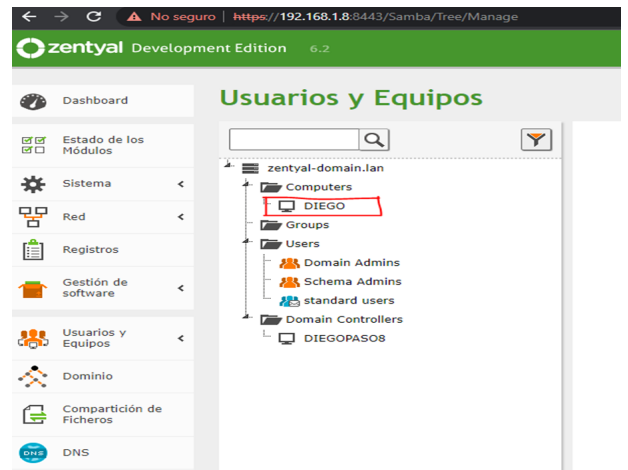


Figura 26. Validación de equipo en dominio desde Zentyal web

### 5 TEMÁTICA 2 - PROXY NO TRANSPARENTE

Se debe configurar el control del 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 el puerto 1320.

Se inicia el proceso de configuración inicial de Zentyal 6.2 ingresando el usuario administrador y su contraseña:

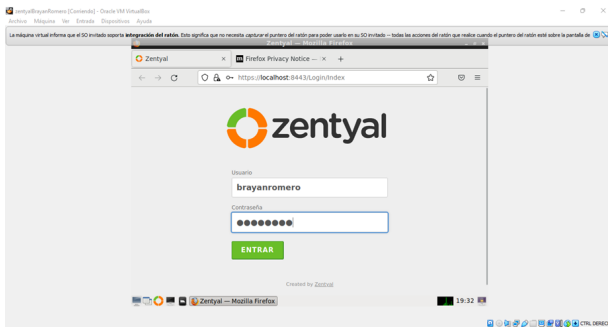


Figura 27. Se visualiza el login para continuar con la configuración de Zentyal

En la configuración inicial, se escogen los paquetes necesarios que se desean instalar, en este caso, se instala el paquete HTTP Proxy:

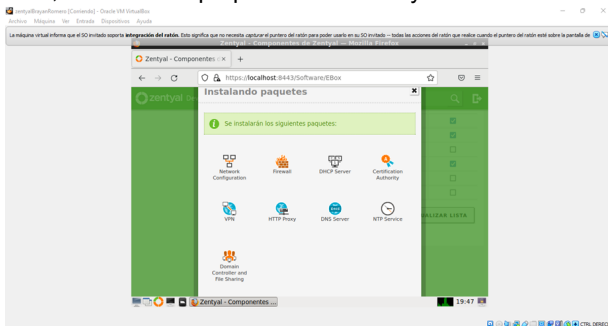


Figura 28. Se visualiza los paquetes que se van a instalar

Terminada la instalación de los paquetes, se configuran las interfaces. La interfaz eth0, que es el adaptador 1 (según lo ajustado en VirtualBox), es la conexión externa (WAN), por lo que se marca la opción "External" y la interfaz eth1, que es la red interna, se selecciona la opción "Internal":

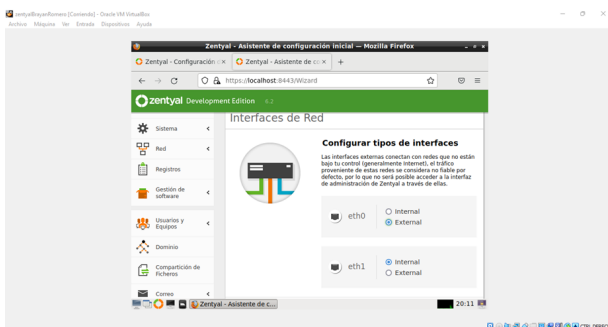


Figura 29. Configurar tipos de interfaces de red.

Para el método de configuración de eth0, se escoge como DHCP, se selecciona el modo Static y como dirección IP para esta interfaz: 10.0.2.15 con máscara de red de 24: 255.255.255.0

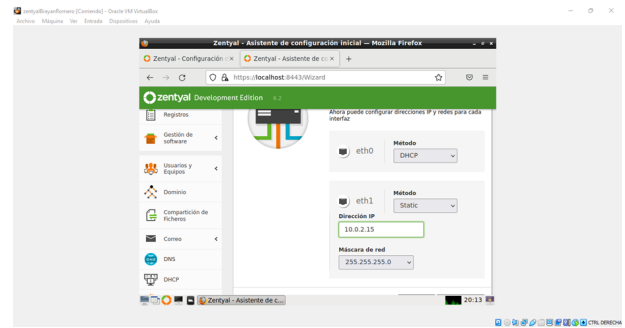


Figura 30. Se configuran los métodos de las interfaces.

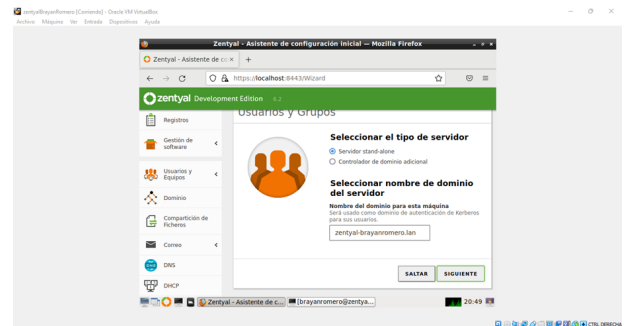


Figura 31. Se configura el dominio del servidor.

Se verifica para la interfaz eth1, que es la red interna, que el método sea "Estático", la casilla debe encontrarse desactivada y la dirección IP debe ser

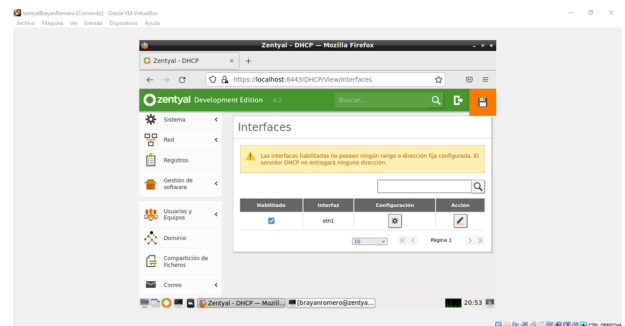


Figura 32. zona de DHCP, en las interfaces se da click al botón de configuración.

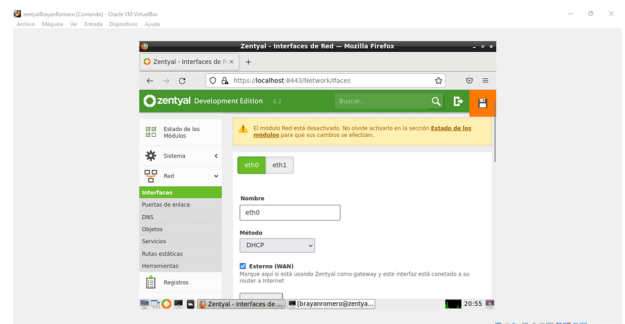


Figura 33. Interfaz de red eth0.

Se verifica para la interfaz eth1, que es la red interna, que el método sea “Estático”, la casilla debe encontrarse desactivada y la dirección IP debe ser 10.0.2.15

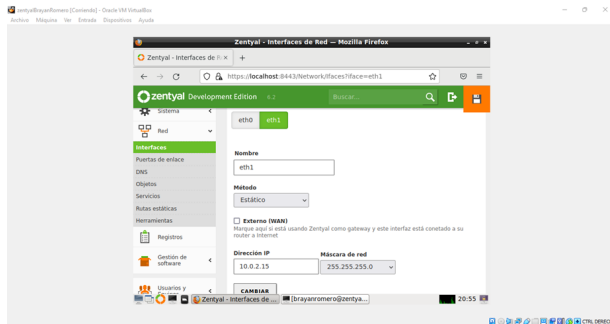


Figura 34. Interfaz de red eth1

Para comenzar con la configuración de HTTP Proxy, se debe ingresar al panel de “Red” – “Objetos y “Añadir nuevo”. Este permitirá identificar el grupo al que se le aplicarán las reglas. Se le asigna un nombre al objeto: Ubuntu

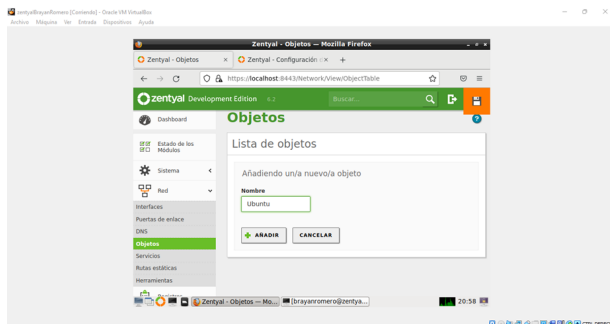


Figura 35. Añadir objeto.

En la misma página de “Objetos” donde se identifica al nuevo objeto creado, se muestra la columna Miembros con un botón de engranaje para poder agregarlos. Al ingresar a la página de Miembros, clic en “Añadir nuevo”. Se especifica un nombre al nuevo miembro (PC1) y su dirección IP: 10.0.2.16

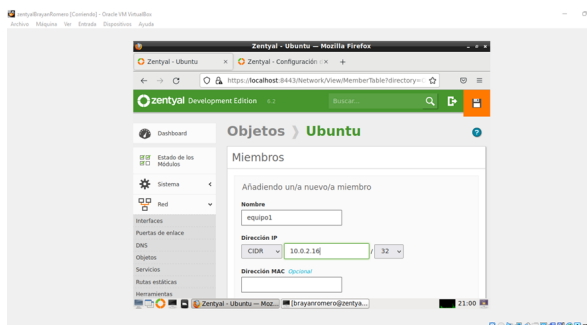


Figura 36. Configurar nuevo miembro

En el panel izquierdo, se ingresa al servicio HTTP Proxy y se selecciona la opción “Configuración general”. Se verifica que la casilla Proxy transparente NO esté activada. Esto significa que se configurará como Proxy no transparente, por lo cual se deberá especificar en cada navegador de un equipo, la dirección IP del proxy y el puerto para su uso. Se asigna el número de puerto requerido: 1320.

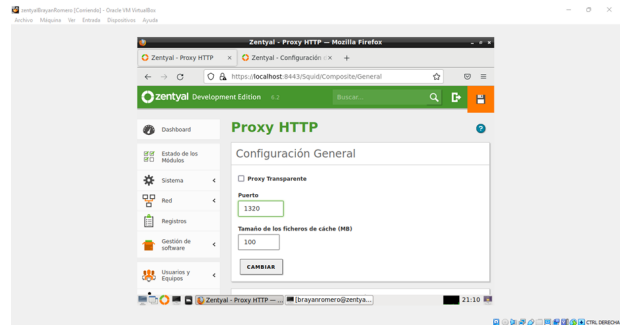


Figura 37. Configurar HTTP Proxy no transparente

En el mismo panel izquierdo de Proxy HTTP, se selecciona “Reglas de acceso”, donde se asignará quienes podrán acceder al Web Proxy.

Para configurar una regla de acceso, se puede escoger un periodo de tiempo para que se aplique según los días de la semana y horas. En “Origen”, se selecciona “Objeto de red”, y enseguida, se especifica el objeto que fue creado anteriormente: Ubuntu. Finalmente, en “Decisión”, se escoge la opción “Denegar todo”:

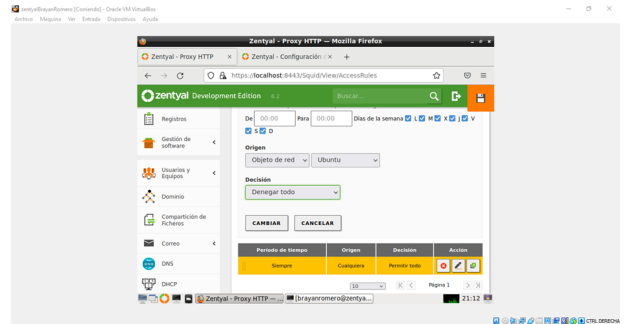


Figura 38. Configurar la regla de acceso para denegar.

Se muestra la regla de acceso creada como “Denegar todo”:

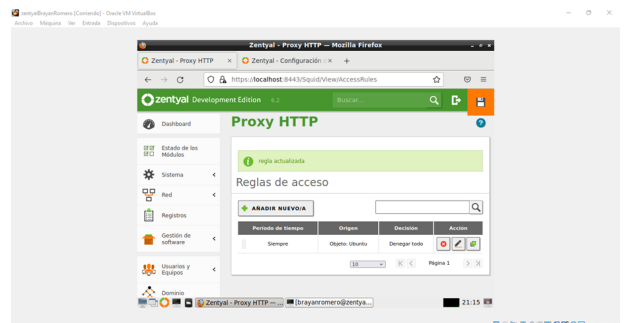


Figura 39. Regla de acceso creada para denegar todo.

En el equipo cliente Ubuntu Desktop, se configura en VirtualBox, el adaptador 1 como Red interna y el segundo como Adaptador puente. Al iniciar sesión se le asigna una dirección IP estática, teniendo en cuenta que se encuentre dentro del mismo segmento de la red interna del server y que sea la misma dirección de la configuración anterior de nuevo miembro.

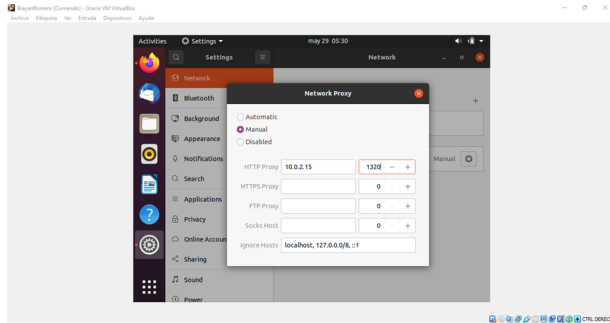


Figura 40. Configurar dirección IP estática en cliente.

En el navegador web del cliente, se ingresa a una página web y se verifica que se está rechazando la conexión debido al proxy:

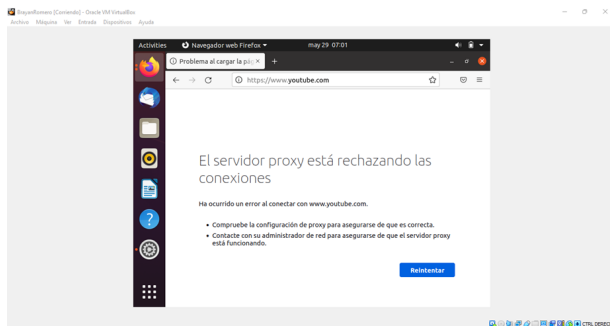


Figura 41. Servidor proxy rechaza la conexión.

Para realizar otra prueba y comprobar que está funcionando el Proxy HTTP, se cambia la regla de acceso en el Zentyal a "Permitir todo":

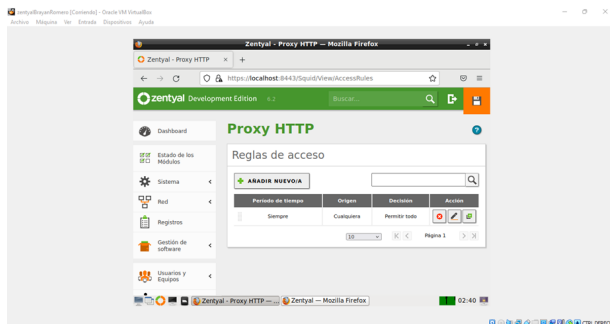


Figura 42. Configurar regla a permitir todo.

Al actualizar la página web del navegador, nuevamente se tiene conexión a Internet debido a este cambio de regla en el proxy:

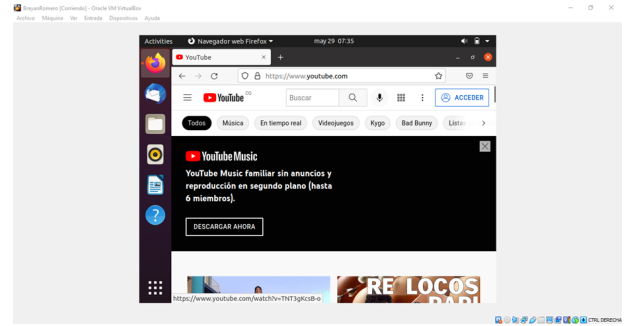


Figura 43. Navegación en Internet por Proxy HTTP.

## 6 TEMÁTICA 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 Ubuntu Desktop. Instalación de herramientas en zentyal importantes para la implementación y configuración posterior de reglas las cuales están alojadas en el proceso de instalación del servidor de igual forma estas pueden ser instaladas

mediante el panel de administración en cualquier momento Figura 44:

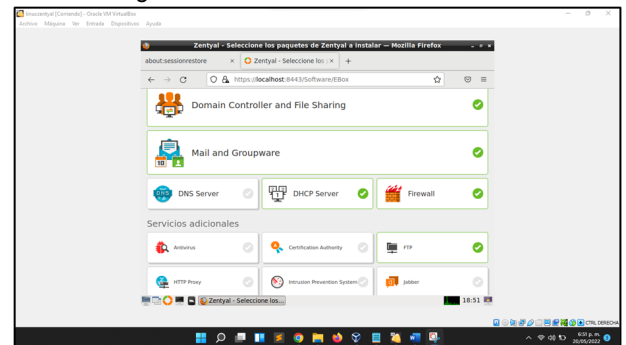


Figura 44. Instalación de herramientas.

Configuración de interfaces para comunicación posterior entre servidor zentyal y desktop remote kali linux siendo eth1 la red con salida wan de nuestro isp y la eth0 para la parte de red figura 45:



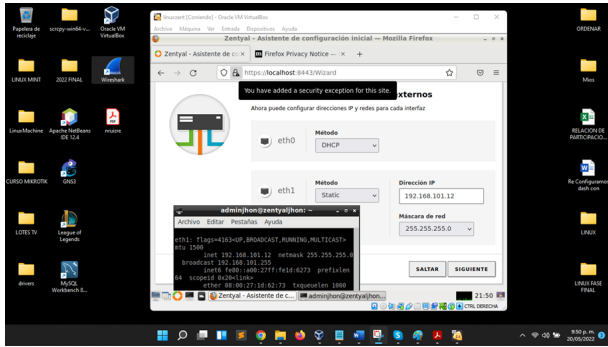


Figura 45. configuración de interfaces.

Configuramos las reglas de bloqueo como lo indica entre redes internas basados en PF (Packet Filter) es el filtro de paquetes o cortafuegos basado en configuración dinámica (stateful rules) figura 46:



Figura 46. bloqueo Packet Filter.

Creamos reglas con bloqueos https,http y tcp con origen de ip de servidores para bloqueo como lo es youtube la ip es alcanzada bajo ping figura 47:

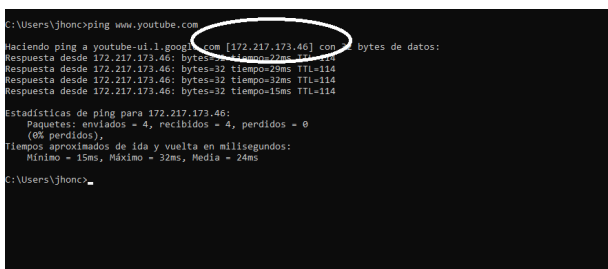


Figura 47. ip servidor destino página.

Creación de reglas con ip destino de bloqueo youtube bajo servicios de red negando de esta manera desde todo destino de la red esta ip con bloqueo por el cortafuegos figura 48:

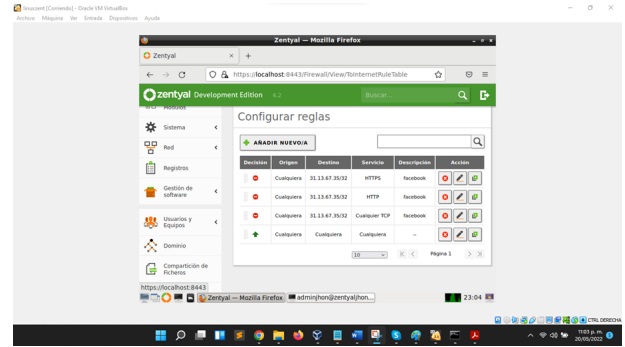


Figura 48. configurar reglas.

Configuramos ip estática para la red LAN del zentyal desde el cliente Kali Linux basado en el rango de direccionamiento seleccionado las razones que nos pueden llevar a asignar nosotros mismos la IP que deseamos a cada dispositivo en este caso nuestro cliente kali con, una IP estática, puede ser el uso de aplicaciones que requieren asociar la IP a los puertos por los que se tienen que comunicar Pero también si asignamos nosotros la IP de forma estática en los dispositivos ganamos en seguridad y nos será más fácil identificar posibles problemas que tengamos en la red de acuerdo a nuestro modelo de red propuesto figura 49:

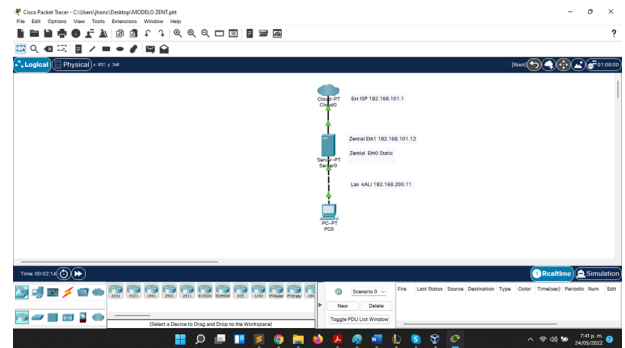


Figura 49. Modelo de red.

Configuración ip estática cliente kali linux figura 50:

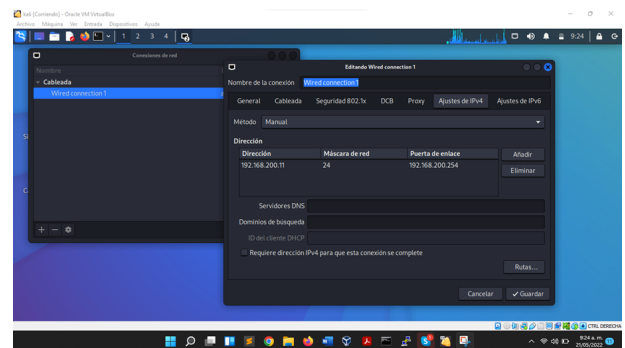


Figura 50. configuración ip estática cliente.

Validación ping entre máquinas e interfaces con conexión establecida correcta para aplicar reglas de bloqueo creadas a la red interna en este caso nuestro cliente kali figura 51;

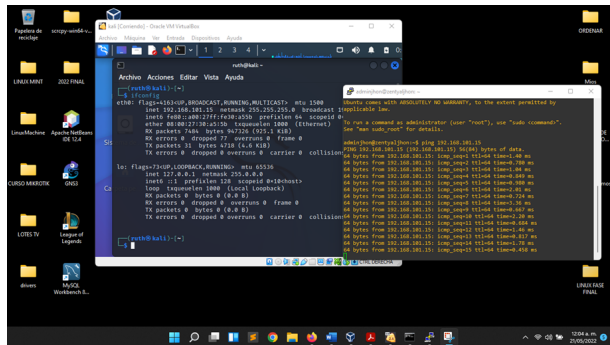


Figura 51. validación ping máquinas.

Validación de conexión desde Kali via ssh de zentyal con putty con acceso correcto al servidor desde cliente Su principal ventaja es el uso de cifrado, que garantiza que la comunicación entre servidores remotos se realice de forma segura. Este protocolo proporciona un mecanismo que autentica al usuario remoto y transfiere la entrada del cliente al host, retransmitiendo la salida al cliente figura 52:

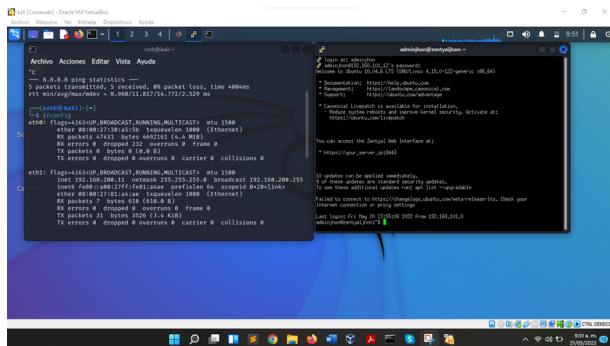


Figura 52. validación conexión ssh client-server.

LAN de zentyal con tráfico de conexión Kali Linux de esta manera validamos que nuestra configuración de red cumple con todos los parámetros de conexión establecidos en el modelo de red propuesto figura 53:



Figura 53. tráfico de red.

Validación bloqueo de sitio YouTube por medio de cortafuegos configurado a la ip servidor del sitio figura 54:

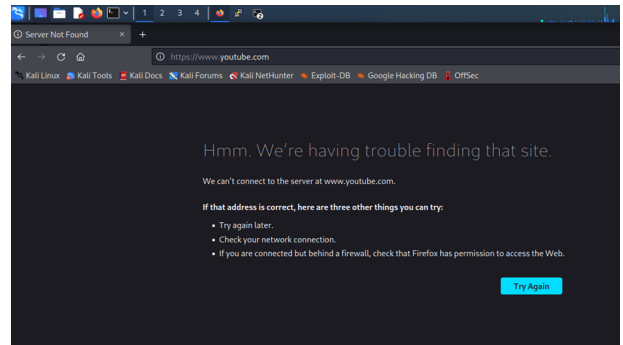


Figura 54. bloqueo conexión.

Reglas de bloqueo creadas aplicadas a cada servicio Las reglas de cortafuegos definen qué tipo de tráfico de Internet se permite o bloquea. Cada perfil de cortafuegos tiene un conjunto predefinido de reglas de cortafuegos, el cual no puede cambiar. Sólo puede agregar reglas nuevas a algunos de los perfiles en este caso usamos las siguientes figura 55:



Figura 55. configuración de reglas de bloqueo.

Bloqueo por proxy denegando todas las conexiones Un servidor proxy funciona como un intermediario en la red Este tipo de servicios puede actuar para bloquear el acceso a una determinada página web o conexiones en este caso lo usaremos para bloquear todas las conexiones que nosotros le asignemos figura 56:



Figura 56. denegando reglas.

Creamos un filtrado de dominio este filtrado de DNS es una técnica para bloquear el acceso a ciertos sitios web o direcciones IP. Esto significa que a la hora de que el servidor DNS devuelve la dirección directamente, este proceso estará sujeto a ciertos controles que establecemos de la siguiente manera figura 57:

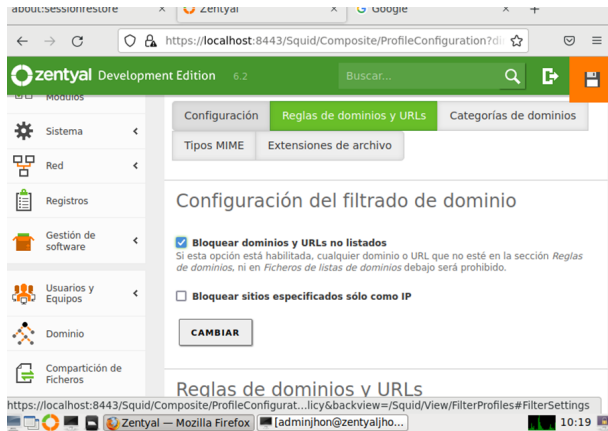


Figura 57. configurando bloqueo de dominio.

Añadimos lista bloqueo de páginas que deseamos bloquear en este caso aplicaremos regla a youtube figura 58:

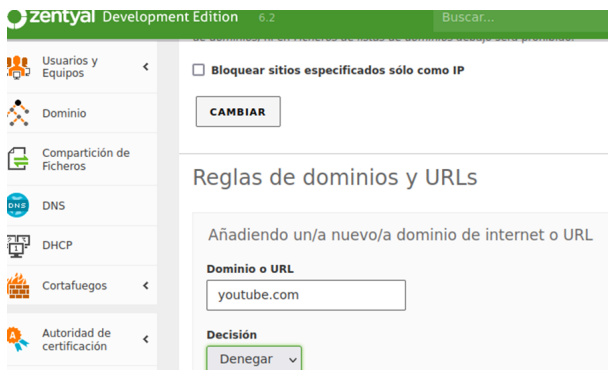


Figura 58. lista de bloqueo.

Validación cliente Kali linux con bloqueo página figura 59:

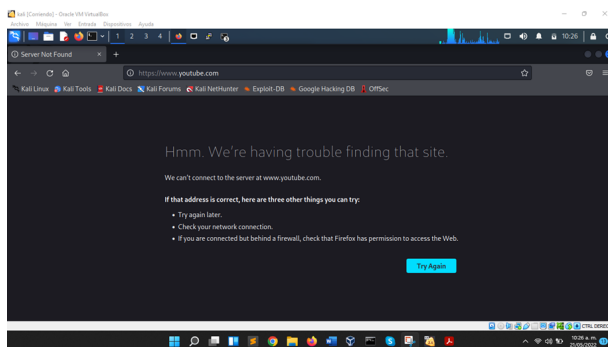


Figura 59. Validación denegación de conexión.

## 7 TEMÁTICA 4 - FILE SERVER Y PRINT SERVER

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

Se inició instalando Zentyal, después de eso se confirmaron los paquetes de instalación de controlador de archivos y compartición de archivos

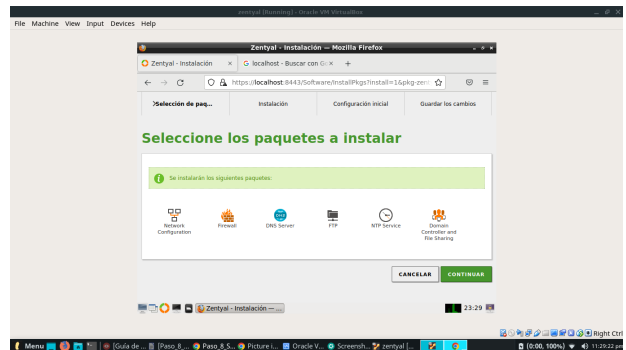


Figura 60. seleccion de instalacion de paquetes.



Figura 61. esperando instalación.

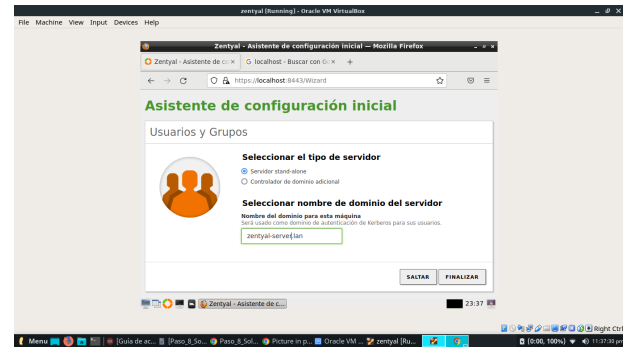


Figura 62. Configuración del dominio del servicio.

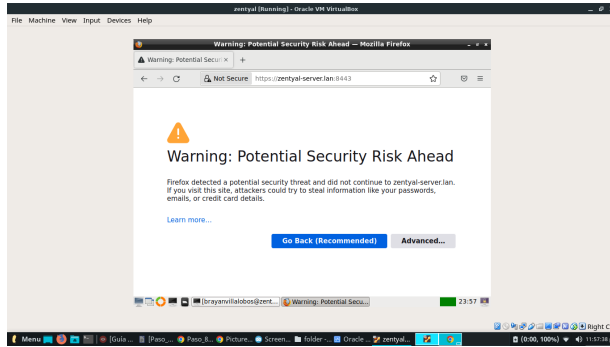


Figura 63. como hicimos cambio en la dirección del servicio el se nos reinicia el navegador para volver acceder.

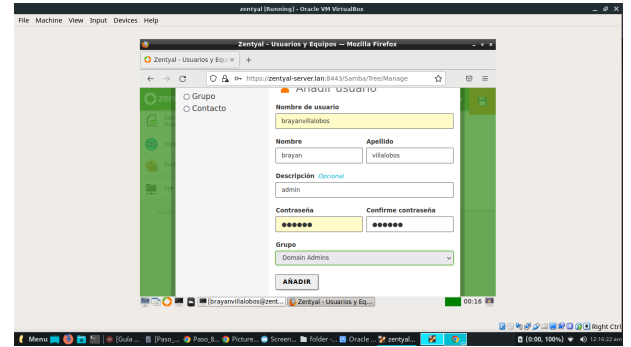


Figura 66. llenamos los espacios correspondientes.

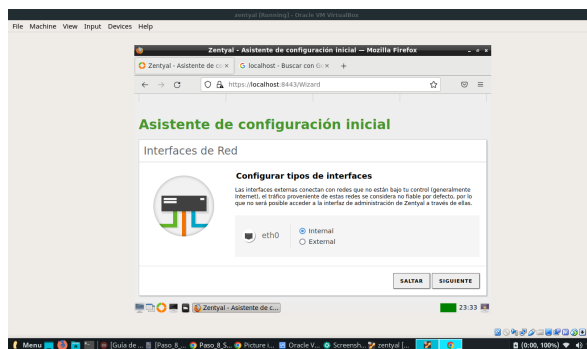


Figura 64. selección de interfaz de red.

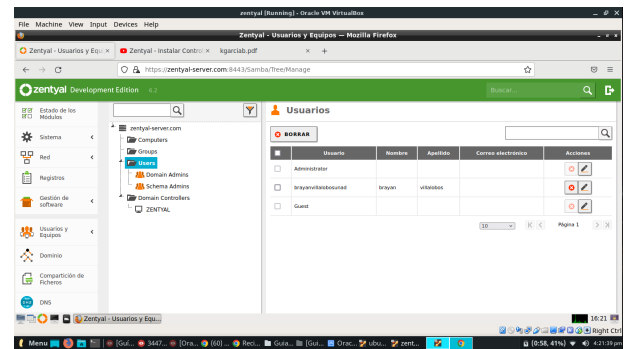


Figura 67. la creación de nuestro usuario es exitosa, no lo muestra en la tabla.

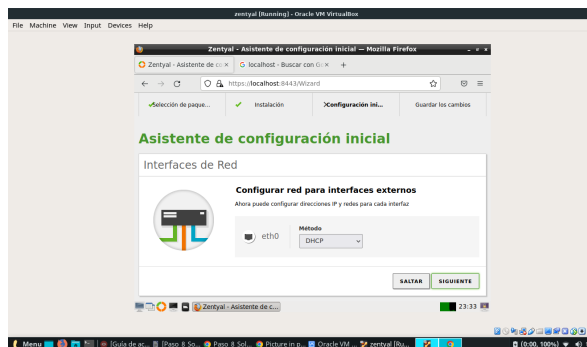


Figura 65. selección de red externa.

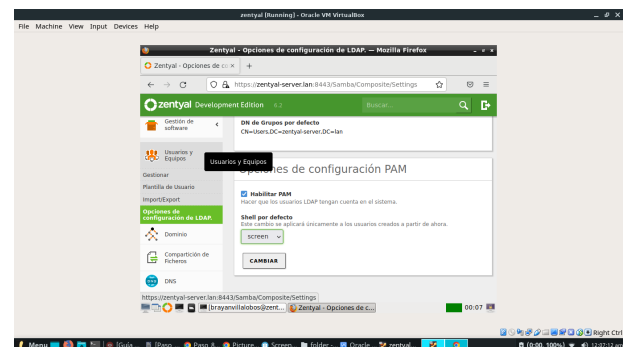


Figura 68. Habilitación del LDAP.

Procedemos a crear el usuario a compartir, seleccionamos en usuarios y equipos

Agregue un directorio compartido, se crea con el comando:

```
mkdir /home/compartida
```

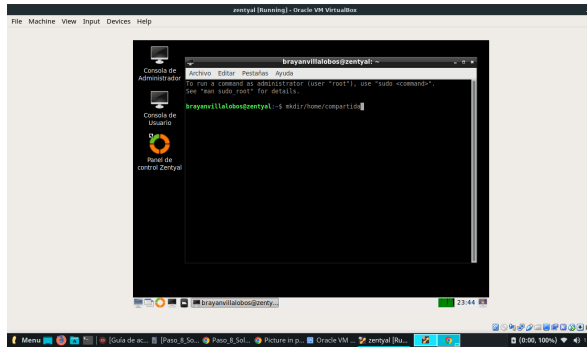


Figura 69. En zentyal nos dirigiremos a compartición de ficheros

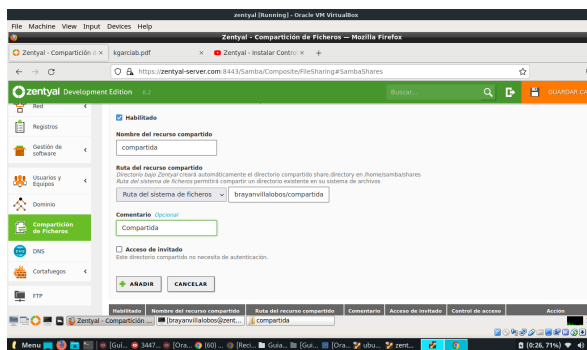
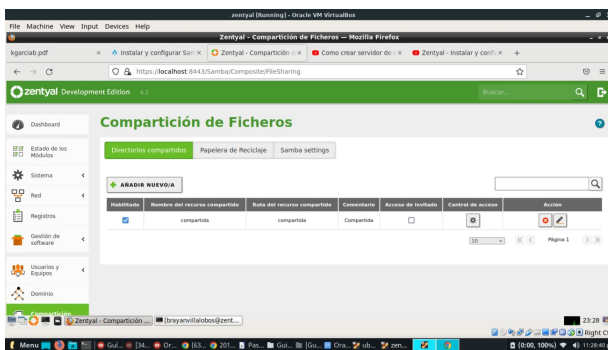


Figura 70. llenamos los campos con el nombre del recurso en este caso la carpeta es compartida, la ruta de localización de la carpeta y en comentario ponemos el nombre de la misma carpeta, y guardamos



Vemos reflejada la creación en la tabla

Ahora en control de acceso añadimos el usuario a compartir en usuarios y equipos



Figura 71. llenemos los campos con el nombre del usuario que comparte

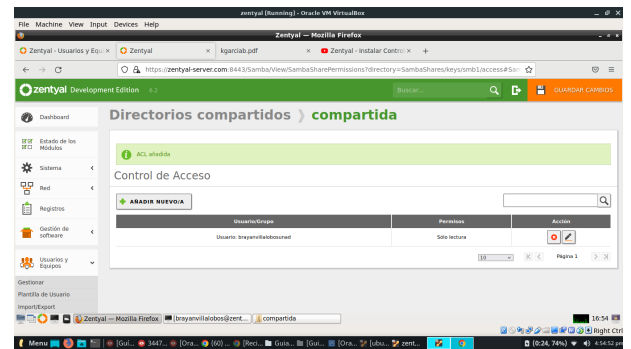


Figura 72. Ahora se nos refleja en un atbala la creación del usuario compartido

Como zentyal no tiene la parte de creación de impresoras lo hacemos desde otra dirección url la cual nos comparte ese servicio de creación

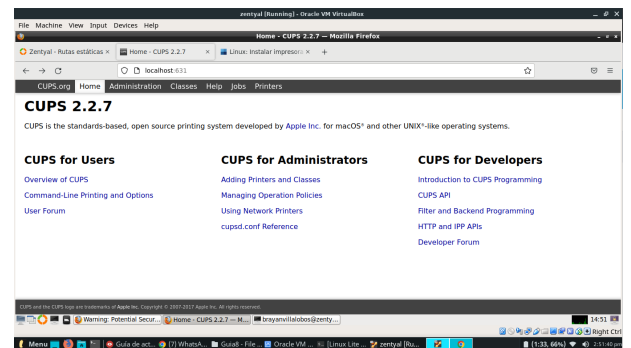


Figura 73. selección de creación de impresora.

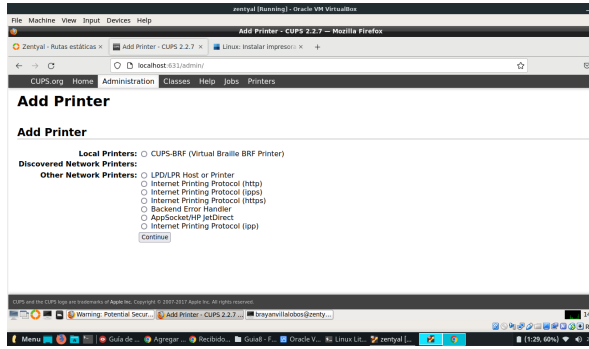


Figura 74. Seleccione la creación de la impresora.

Ingresamos nos aparece la Carpeta Compartida con la creación de la carpeta de la impresora

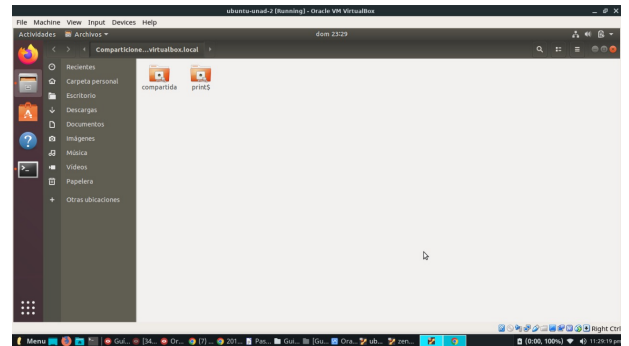


Figura 77. visualización de carpetas compartidas

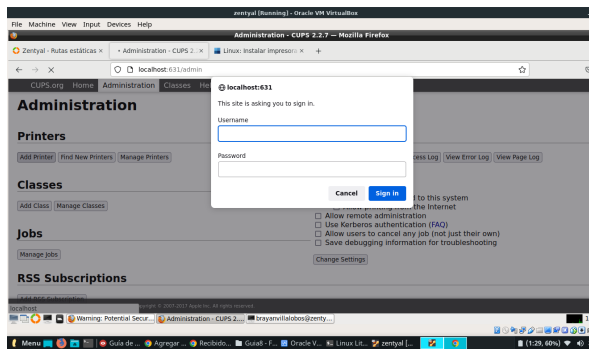


Figura 75. Le damos la autorización de creación.

## 8 TEMÁTICA 5 - VPN

Una vez introducido el Dashboard de Zentyal, se producen las respectivas configuraciones, en este caso se añadirá el paquete VPN, Firewall y Autoridad de Certificación para poder configurar un puente VPN.

Ahora para ver reflejado la compartición de carpeta e impresora, vamos a nuestro Desktop y vamos a ir a otras ubicaciones.

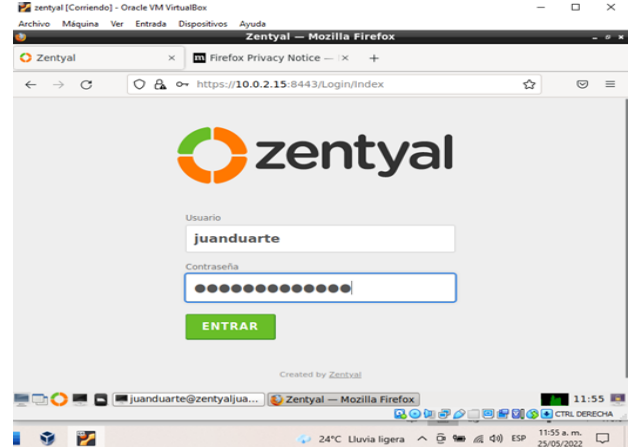


Figura 78. Login to zentyal dashboard (autoría propia)

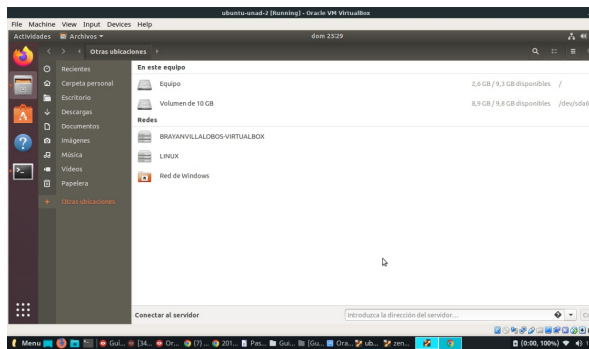


Figura 76. vemos el nombre de red compartida es brayanvillalobos-virtualbox

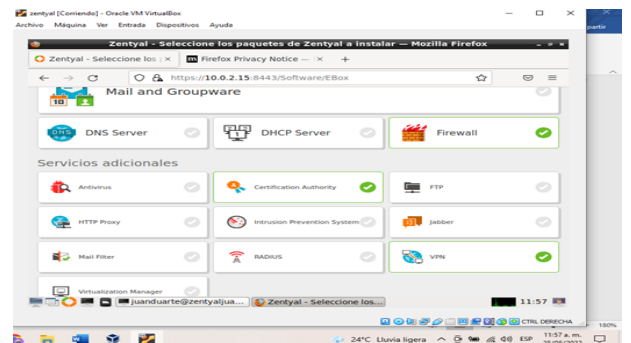


Figura 79. Selección de paquetes a instalar (autoría propia)

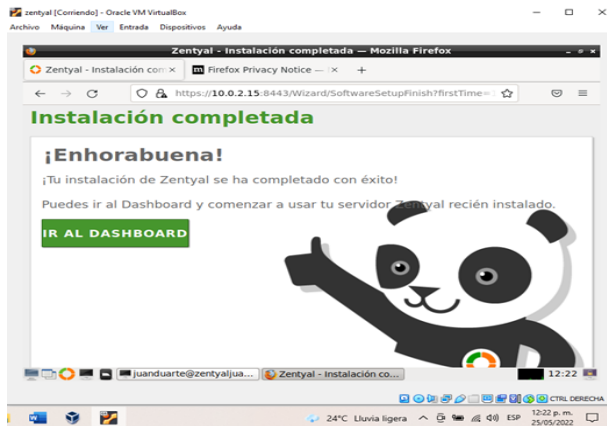


Figura 80. instalación completada de paquetes seleccionados (autoría propia)

Una vez instalados los módulos, se configurará la VPN. Para ello, primero debemos crear un certificado de Entidad emisora de certificados en la pestaña General. A continuación, seleccione crear, validar y, a continuación, guardar los cambios.

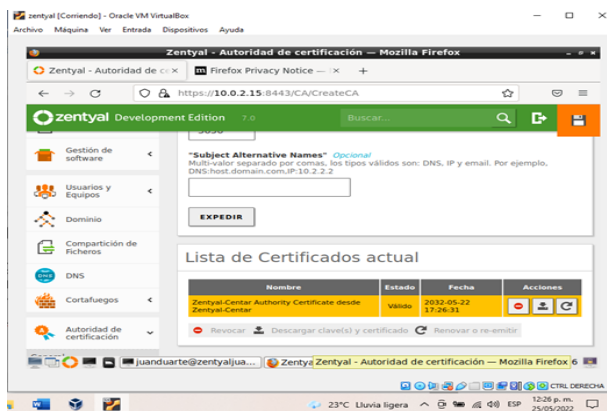


Figura 81. Create Certificado de Autoridad (autoría propia)

Ahora, vaya a Servidores VPN, donde se eliminará el estado habilitado, se asignará un nombre, haga clic en agregar y luego se guardarán los cambios.

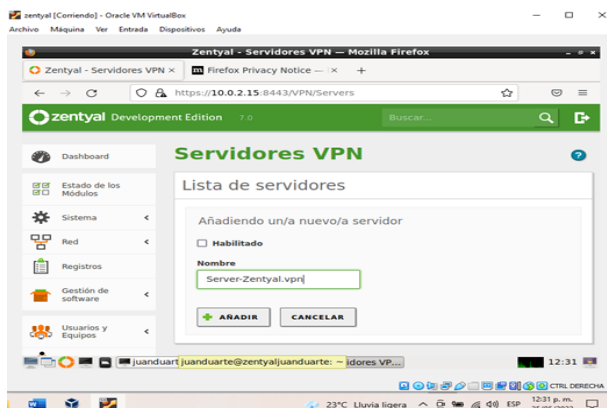


Figura 82. Creación de Certificado (autoría propia)

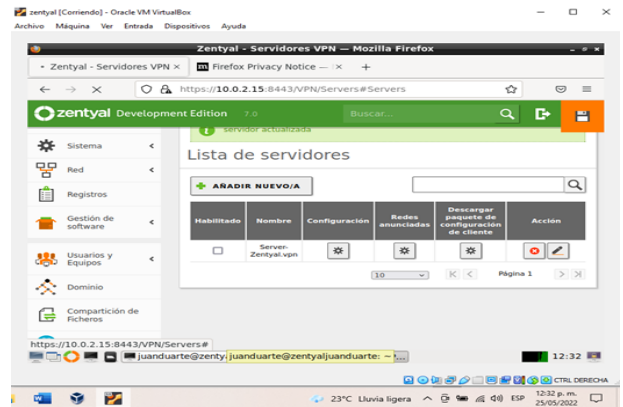


Figura 83. Creación de Certificado (autoría propia)

Dado que el certificado creado es para Zentyal, se creará un nuevo certificado para el servidor, se asignará un nombre y se hará clic en el botón de emisión.

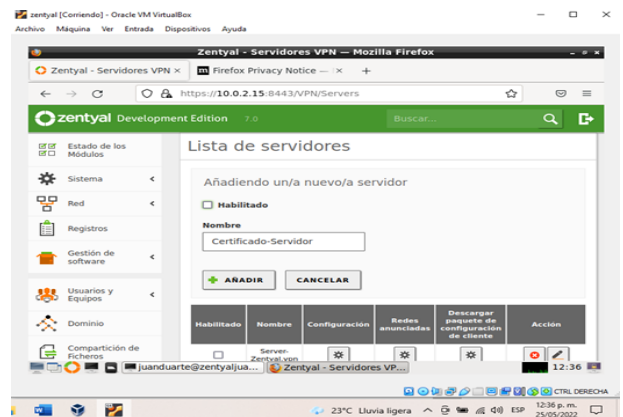


Figura 84. Creación de Certificado (autoría propia)

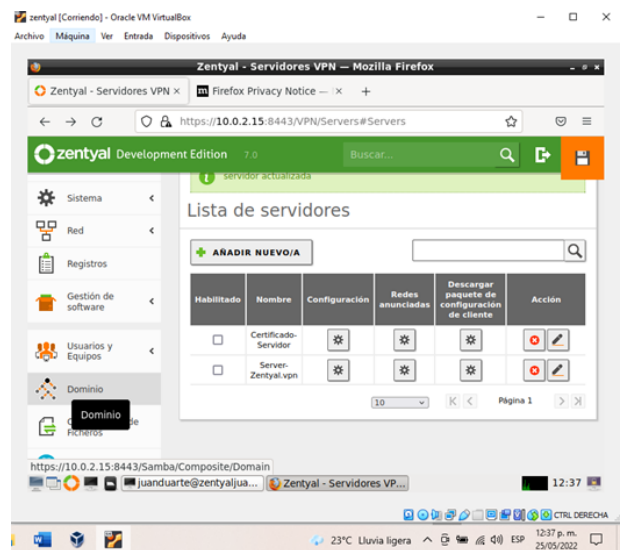


Figura 85. Creación de Certificado (autoría propia)

Una vez creado el certificado, éste irá a Servidores VPN y configura el Servidor creado previamente, en él debemos asegurarnos de que está en UDP con su

respectivo puerto en este caso 11194, se seleccionará la dirección VPN que se asignará y se seleccionará el certificado de servidor creado previamente, luego se activará la interfaz TUN, donde, haga clic en cambiar y luego en guardar cambios.

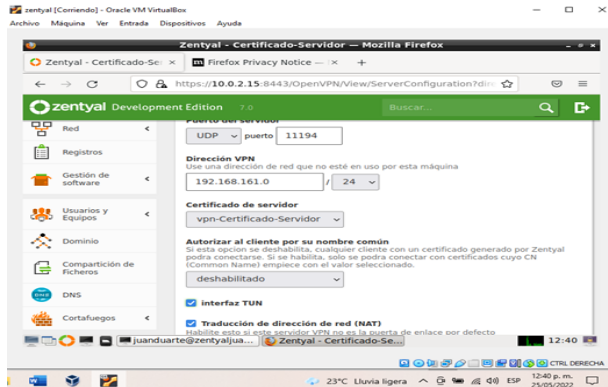


Figura 86. Servidor VPN (autoría propia)

Una vez guardados los cambios, irás a la opción Red, servicios y se creará un nuevo servicio para la conexión VPN, se le asignará un nombre y una descripción.

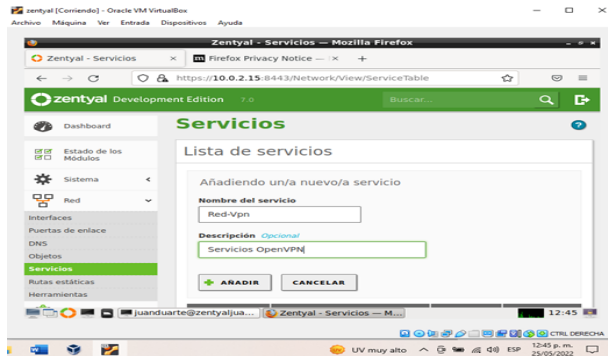


Figura 87. Servicios de red VPN (autoría propia)

Después de crear el servicio, se configura con el puerto VPN que utilizará, seleccionamos el protocolo en este caso el UDP, en el puerto de origen se selecciona cualquiera y en el puerto de destino seleccionamos un solo puerto y el número del previamente definido que es 11194, finalmente agregamos y guardamos los cambios.

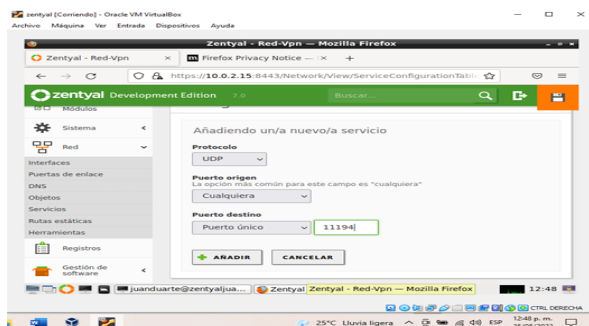


Figura 88. Configuración de servicios VPN (autoría propia)

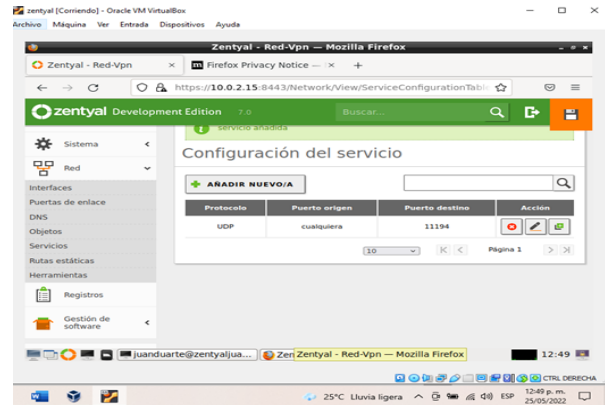


Figura 89. Configuración de servicios VPN (autoría propia)

Luego debes ir a configurar el Firewall, haciendo clic en Filtrado de paquetes, configurar reglas en la sección Reglas de Filtrado de redes internas de Zentyal, luego hacer clic en Agregar nuevo, en la ventana que aparece en Decisión debes tener Aceptar, en Origen Cualquiera, en Servicio el servicio que se creó anteriormente en este caso Red-VPN y si lo deseas, coloque una descripción y, a continuación, haga clic en Agregar y guarde los cambios.

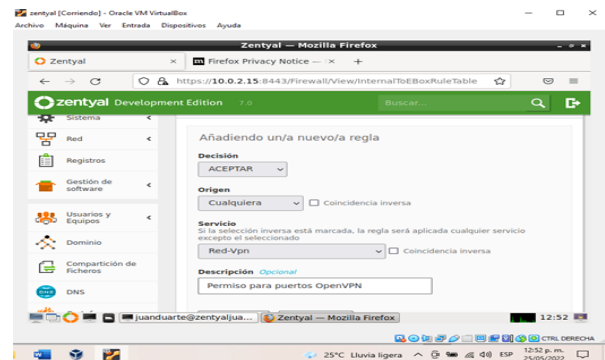


Figura 90. Configuración del cortafuegos (autoría propia)

Luego debes ir a la pestaña VPN, Servidores, Redes Anunciadas y se muestra la predeterminada creada por Zentyal, se añade la red con la que trabajarás.



Figura 91. Una red descentralizada (autoría propia)



Ahora, los paquetes que el cliente debe descargar deben estar configurados, dependiendo de si se trata de un cliente Windows, Linux o Mac OS X, en este caso seleccionaremos Linux, el certificado creado previamente, por lo que se debe conocer la dirección pública del servidor; se introducirá la dirección IP fija asignada al servidor; Finalmente, haga clic en descargar, regrese a la pestaña de servidores y el servicio estará habilitado.

Finalmente, se verifica que el servicio está activo en la página principal del panel de control. Posteriormente, el archivo que se generó en .rar debe enviarse por correo o guardarse en una memoria para luego abrirlo en la estación cliente.

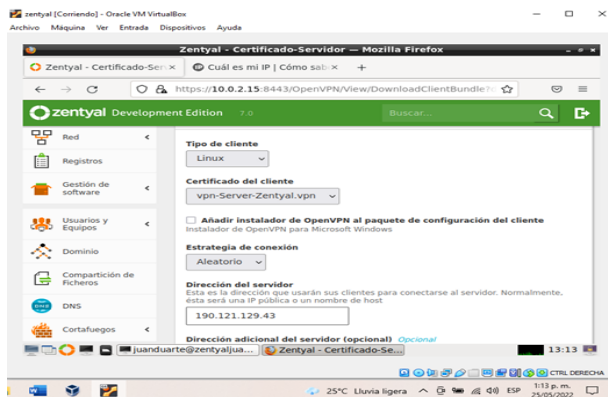


Figura 92. Customer packages (autoría propia)



Figura 93. Habilitación del servicio (autoría propia)

Una vez configurado Zentyal con la VPN, dirígete a la máquina cliente, instala Openvpn con un entorno gráfico desde el terminal con el comando: `apt-get update && apt-get install openvpn`.

Luego, se escribirá el siguiente comando en la consola: `sudo apt-get install network-manager-openvpn-gnome`. Una vez instalado, el archivo de configuración se descarga, se copia en la carpeta `/etc/openvpn/client` y luego se extrae del rar.

Debes ir a la configuración de red de Ubuntu en la sección VPN, seleccionar importar desde un archivo y buscar el archivo de configuración que creó el Servidor

Zentyal y que ya había sido descargado, añadirlo, habilitar el servicio VPN y ver si hay conexión.

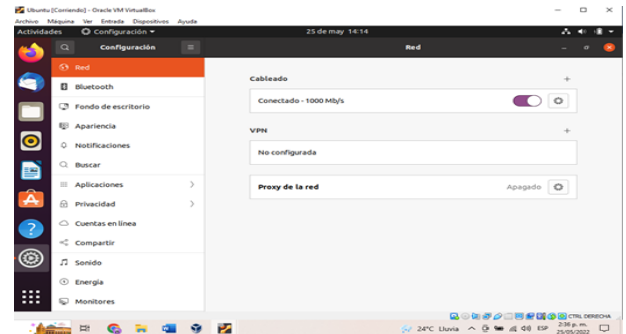


Figura 94. VPN planteada (autoría propia)

Ahora, el cliente de escritorio remoto de Ubuntu se instalará remmina, para ello, se realizará una descarga de los repositorios para tener la última versión, abrimos el terminal y escribimos: `sudo apt-add-repository ppa:remmina-ppa-team/remmina-next`

Luego escribimos: `sudo apt-get update && sudo apt-get install remmina remmina-plugin-rdp libfreerdp-plugins-standard`

Una vez instalado, se abre el programa, y se introduce la dirección del servidor para entrar, nos pedirá la contraseña que hemos introducido y listo, una vez dentro del servidor se realiza una prueba creando un archivo en el escritorio y efectivamente, nos damos cuenta de que fue creado desde la estación de trabajo al servidor.

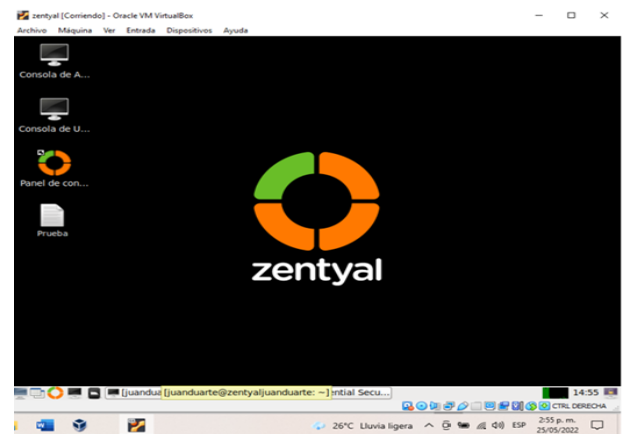


Figura 95. Verificación del archivo creado (autoría propia)

## 9 CONCLUSIONES

Con la implementación de las temáticas propuestas se logró formular soluciones propias bajo el uso de GNU/Linux cliente y servidor a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica. que permitió dar solución a los requerimientos específicos brindados. De esta manera, se puede observar las grandes virtudes que posee linux como software libre para soluciones de infraestructura. a través de este podemos realizar configuraciones de servicios de Correos Electrónicos, Gestión de red, Servidor de correo, Comunicaciones, y Compartición de recursos que son base fundamental en la administración de una red y de esta manera poder junto a nuestro servidor Zentyal unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet. Ya que Zentyal integra servicios como DNS/DHCP, CA, VPN, backup, gateway, cortafuegos y proxy HTTP, por mencionar algunos ya que este cuenta con grandes características de administración.

Se conoce ahora que en una red corporativa o cualquier red local, es de gran importancia contar un controlador de Dominio un servidor DNS y un servidor DHCP en orden de poder implementar otros servicios posteriores, los cuales se pueden encontrar en la Herramienta Zentyal Server.

Se evidencio una comunicación de un intermediario a través del proxy que filtra la salida por medio del puerto 1320 se genera una conexión indirecta entre remitente Zentyal al destinatario Ubuntu cliente puede denegar accesos o permitir.

Con la implementación del cortafuegos a la red se logra dar robustez al sistema de seguridad en el cual se puede bloquear accesos no autorizados en base a una serie de reglas preestablecidas con información que trata de salir o entrar a la red.

Podemos concluir que Zentyal Server es una alternativa como solución para la infraestructura IT de una organización ya que es bastante estable en cuanto a sus servicios y en sus procesos dentro de una máquina además de que su aplicación web es muy sencilla de manejar e intuitivo por lo que un administrador de sistemas puede realizar las configuraciones pertinentes de manera eficiente y eficaz.

Por otro lado, la implementación de LDAP, de compartición de archivos o impresoras en un entorno laboral, es de mucha ayuda y se da de una manera sencillas donde se crean de acuerdo a las políticas que opte una organización, además, lo que lo hace ser muy completo la administración del tráfico en la red.

Fue posible generar la configuración para el Servidor Zentyal con el paquete VPN y conectarse a él desde una estación de trabajo Ubuntu a través de un túnel de comunicación privado y crear archivos con una conexión remota.

## 10 CITAS Y/O REFERENCIAS

- [1] Zambrano. R. febrero 2015. 01. Curso Práctico de Zentyal - Instalación de Zentyal listo y preparado para Instalar servicios. Recuperado de <https://www.youtube.com/watch?v=hW-oLbCNj5I>
- [2] Cómo instalar Zentyal Server pasó a paso. Recuperado de <https://drivemeca.blogspot.com/2018/04/como-instalar-zentyal-server-paso-paso.html>
- [3] Cabrera Caballero. M. abril 2018. Zentyal Server. Instalación y primeros pasos DETALLADOS para ti. Recuperado de [https://www.youtube.com/watch?v=tG\\_NHAUYUbu&feature=youtu.be](https://www.youtube.com/watch?v=tG_NHAUYUbu&feature=youtu.be)
- [4] Llorente Gimeno. D. Diciembre 2015. Instalación y configuración de servidor DHCP en Zentyal. Recuperado de <https://www.youtube.com/watch?v=AEFwwJ8b56Y>
- [5] JGAITPro. Abril 2014. Zentyal - Instalar y configurar DHCP Server. Recuperado de <https://www.youtube.com/watch?v=H5lhAKOH5LM>
- [6] Arias, J. G. (20 de 05 de 2014). YouTube. Obtenido de YouTube: <https://www.youtube.com/watch?v=PG7pcYmBkw4>
- [7] Fernández, R. P. (16 de 04 de 2016). raulprietofernandez. Obtenido de raulprietofernandez: <https://www.raulprietofernandez.net/blog/gnu-linux/como-configurar-proxy-squid-en-modo-no-transparente>
- [8] Lema, A. d. (03 de 01 de 2016). YouTube. Obtenido de YouTube: [https://www.youtube.com/watch?v=oiQjqe9\\_618](https://www.youtube.com/watch?v=oiQjqe9_618)
- [9] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid. ES: IC Editorial. elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92>
- [10] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 6 – 84). elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56046?page=6>
- [11] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing. elibro. <https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page--20>
- [12] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. elibro. [http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp\\_40](http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40)