

USO DE SERVIDOR ZENTYAL COMO PROVEEDOR DE SERVICIOS DE SEGURIDAD PARA LA INFRAESTRUCTURA DE REDES

Heiber Arbey Pérez Rodríguez
e-mail. haperezr@unadvirtual.edu.co
Javier Andrés Calderón Herrera
e-mail. jacalderonhe@unadvirtual.edu.co
Wilton Calvo Barrios
e-mail. wcalvob@unadvirtual.edu.co
John Wilmar Álvarez Munera
e-mail. jwalvarezm@unadvirtual.edu.co
Bayrón Norbey Bolaños Portilla
e-mail. bnbolañosp@unadvirtual.edu.co

RESUMEN. Este informe comprende el desarrollo de implementación de servicios específicos solicitados como la creación de servidores DHCP, DNS, File y Print y el establecimiento de Controladores de Dominio, como también la definición de Proxy no transparente, reglas para el Firewall y Servicio de VPN definidos por requerimientos en función a una migración de servicios establecidos bajo el uso del sistema operativo Zentyal, basado en GNU/Linux, todo el desarrollo se basó en su versión 6.2

PALABRAS CLAVE. Controlador de dominio, Cortafuegos, Firewall, DHCP, DNS, Proxy, Print Server VPN, Zentyal, Ubuntu

1 INTRODUCCIÓN

A través de este documento se dará solución a la necesidad de migración de los servicios expuestos en la problemática inicial, para esto se requiere la puesta en marcha de servicios solicitados teniendo en cuenta los requerimientos específicos del cliente haciendo uso de Zentyal como proveedor de servicios como DHCP, DNS, Proxy, Cortafuegos, File Server, Print Server Y VPN que son los servicios precisos para los sistemas de seguridad de las redes internas de manera empresarial.

2 DESARROLLO POR TEMÁTICA

La instalación de Zentyal Server se basa con su versión 6.2 con requerimientos mínimos para los servicios que vamos a usar a continuación. CPU Pentium 4 o superior, RAM de 2GB, Disco 80Gb y 2 Tarjetas de Red o más. En este caso será representado por una máquina virtual con especificaciones similares a las mencionadas.

Después de crear la máquina virtual y asignar él .ISO de Zentyal, se configuran los adaptadores de red (Tabla 1).

Tabla 1. Adpatadores de red

| Adaptador | Nombre Interno | Conexión | Descripción |
|-----------|----------------|------------------|---|
| 1 | eth0 | Adaptador puente | Sera nuestro WAN para las redes internas |
| 2 | eth1 | Red Interna | Será la LAN donde estaran conectados los clientes |

Se inicia la máquina virtual y seleccionado el idioma de la instalación, se selecciona el proceso de instalación (Fig. 1).

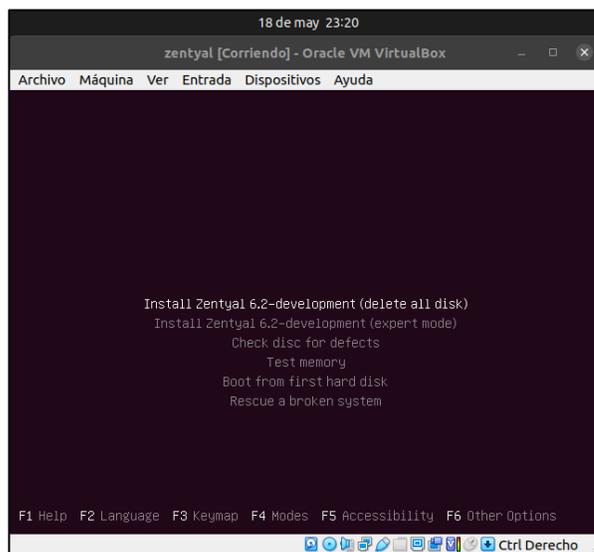


Fig. 1. Opciones de Instalación/Ejecución

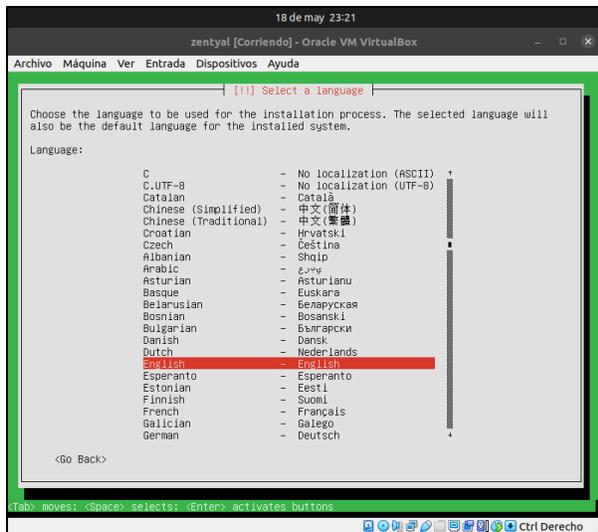


Fig. 2. Selección de idioma del sistema

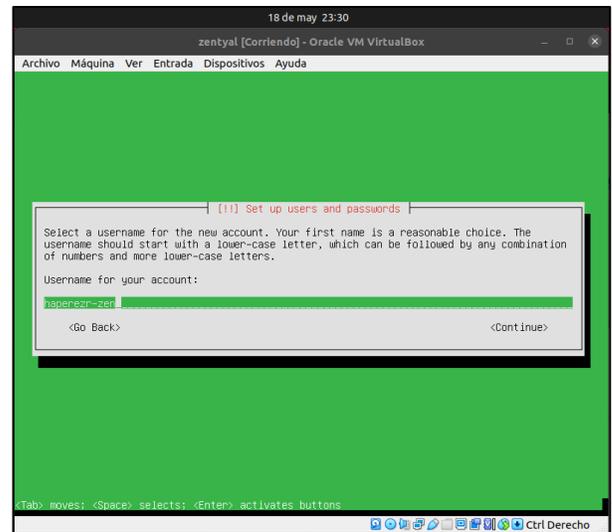


Fig. 5. Asignación nombre Usuario

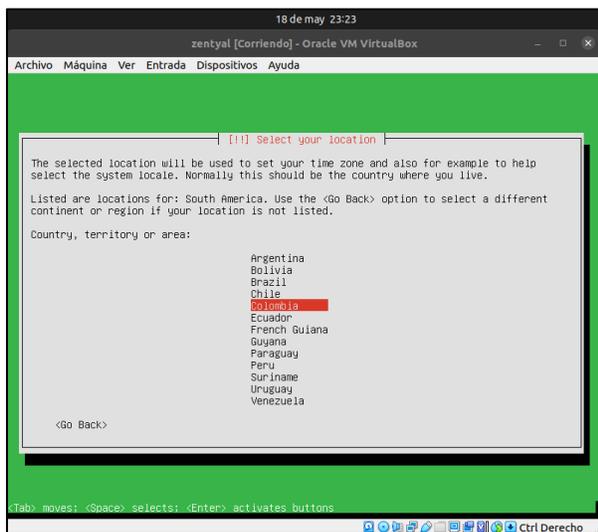


Fig. 3. Selección de ubicación

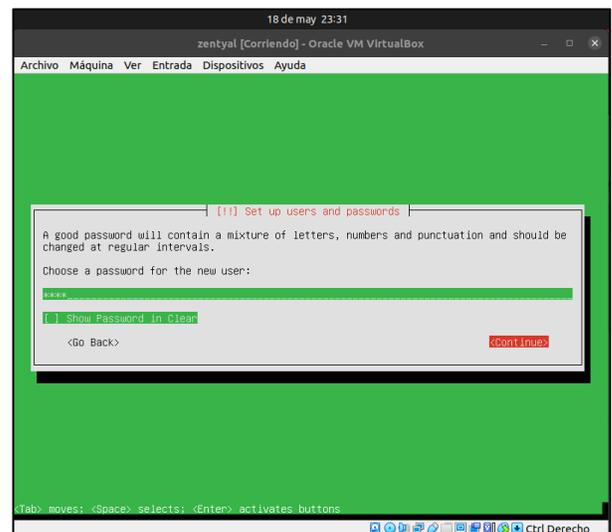


Fig. 6. Asignación contraseña de Usuario

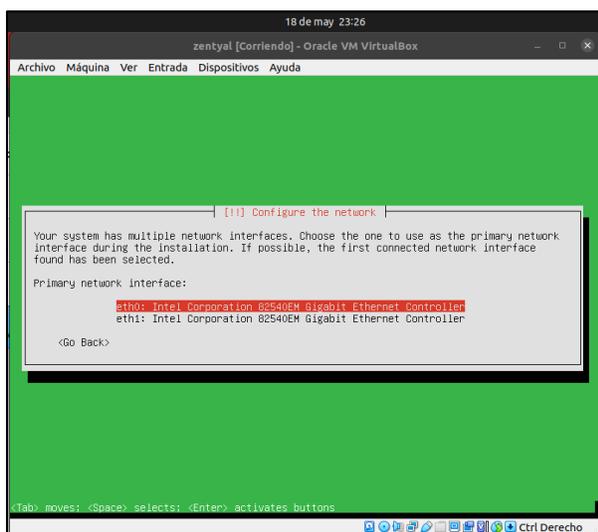


Fig. 4. Selección de Interfaz de red primaria



Fig. 7. Interfaz inicial de Zentyal

2.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Estos servicios son de los más indispensables para la administración de una red en una organización ya que podemos administrar los usuarios que se conectan a la red a través de un dominio, así mismo cada usuario que se conecta tendrá una asignación de IP automática lo cual se conoce como DHCP.

Para iniciar la configuración de estos servicios inicialmente ingresamos al módulo de red para configurar las interfaces de manera estática, para eth0 asignamos la IP 192.168.1.50 con máscara 24 y para la eth1 asignamos la IP 192.168.0.50 con máscara 24

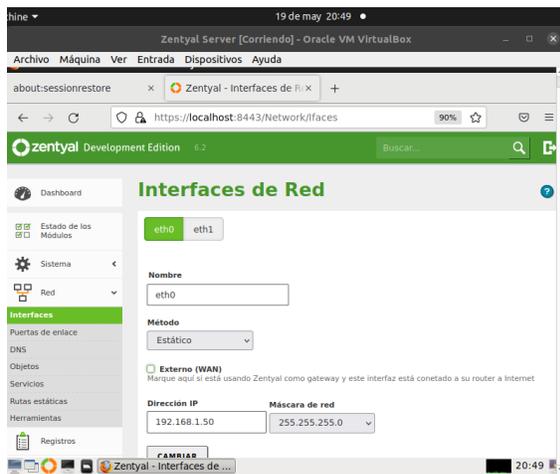


Fig. 8. Configuración de interfaces de red

Para nuestra interfaz eth0 le configuramos la puerta de enlace que es la que nos dará salida a internet.

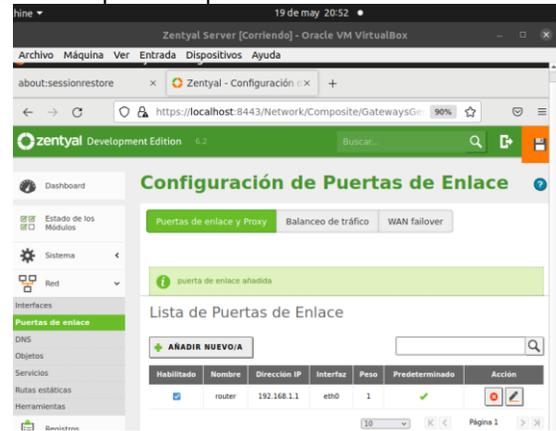


Fig. 9. Configuración de puerta de enlace

Ingresamos a DHCP y configuramos nuestra interfaz interna la cual corresponde a eth1

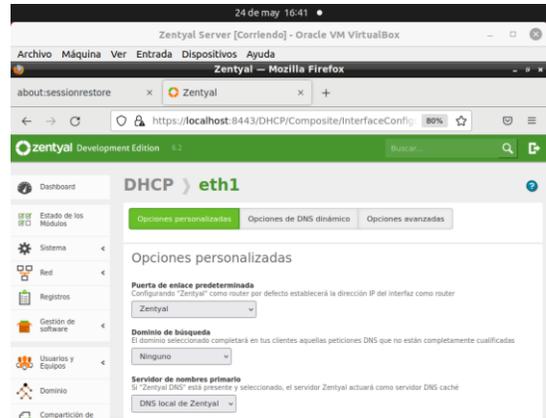


Fig. 10. Configuración de interfaz eth1

Asignamos un rango de asignación de IP, tomamos desde la 192.168.0.60 hasta la 192.168.0.100

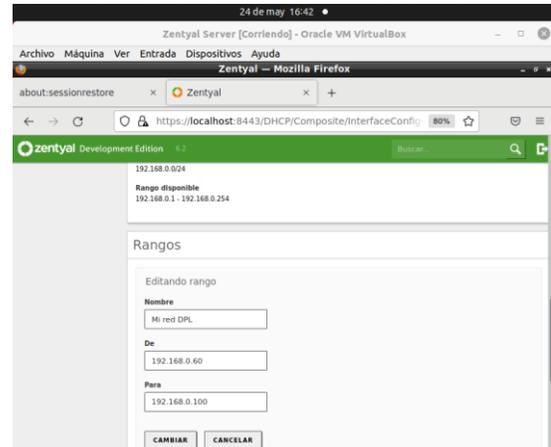


Fig. 11. Configuración de DHCP en eth1

Ingresamos a la configuración general del sistema y digitamos el dominio a gestionar en nuestro caso es "dpi2022.edu.co"

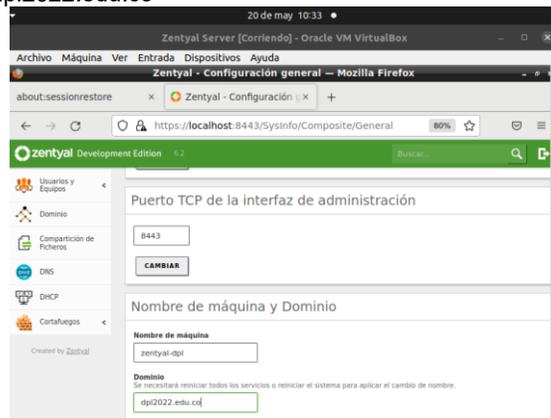


Fig. 12. Asignación de nombre de dominio

Ingresamos a usuarios y equipos donde podemos administrar los grupos y usuarios del dominio.

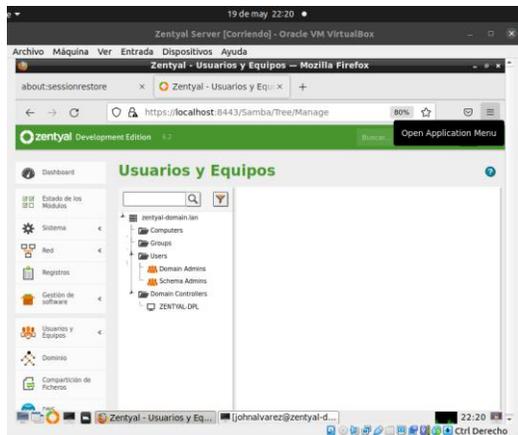


Fig. 13. Gestión de usuarios y equipos del dominio

Añadimos un usuario que tenga permisos de administrador, en este caso es mi usuario jwalvarez

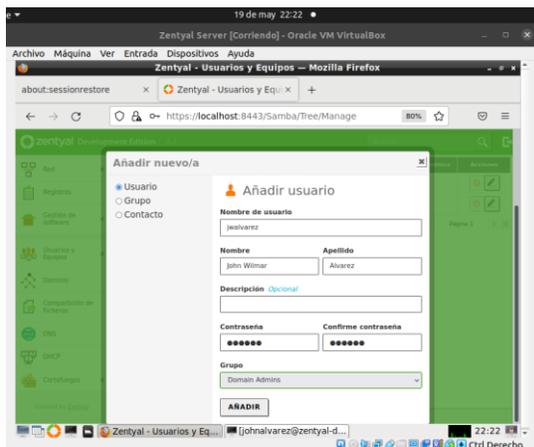


Fig. 14. Añadiendo usuarios al dominio

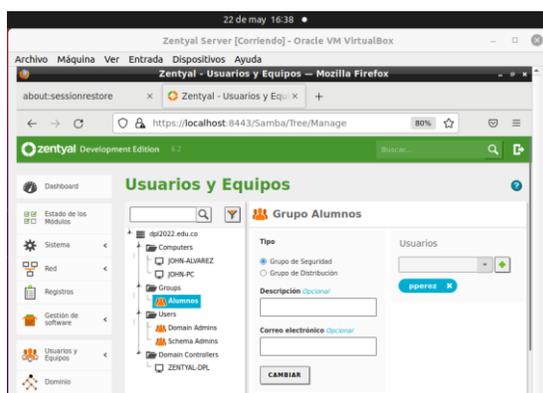


Fig. 15. Gestión de usuarios y equipos del dominio

Desde un cliente Windows agregamos nuestro dominio y confirmamos el ingreso con nuestro usuario administrador.

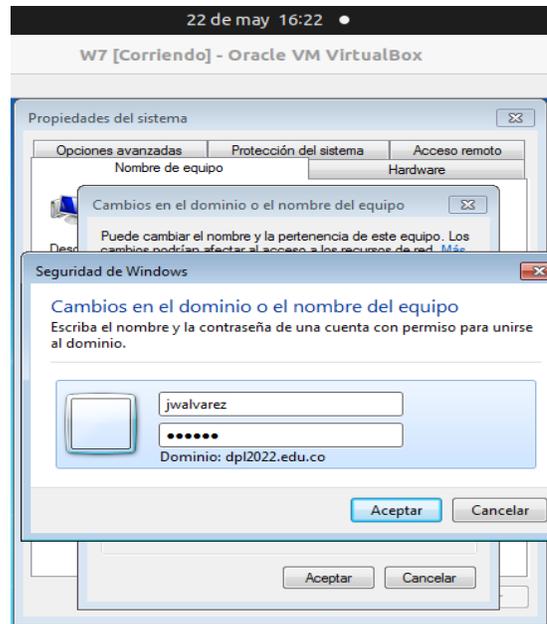


Fig. 16. Ingresando un cliente al dominio

El sistema nos confirma que ingresamos correctamente al dominio y nos pide reiniciar la máquina.

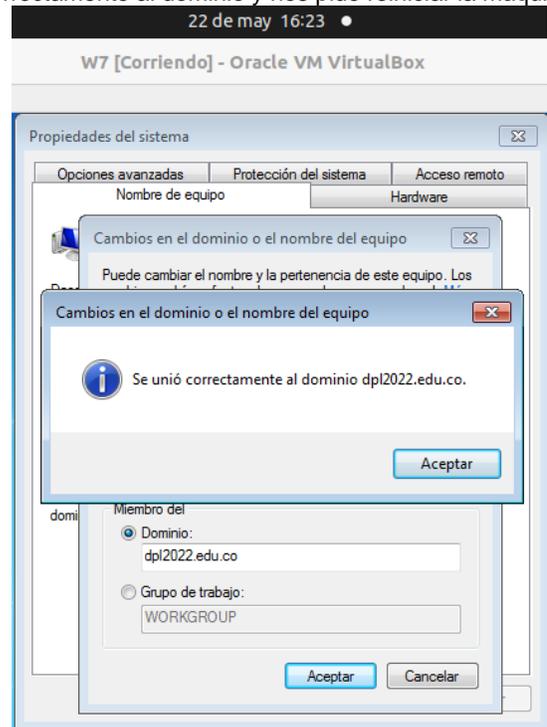


Fig. 17. Confirmación de ingreso de un cliente al dominio

Al reiniciar como ya estamos dentro del dominio iniciamos sesión con uno de los usuarios creados desde nuestro servidor zentyal.



Fig. 18. Iniciando sesión en un cliente conectado al dominio.

Aquí podemos evidenciar que se cargó el usuario correctamente.

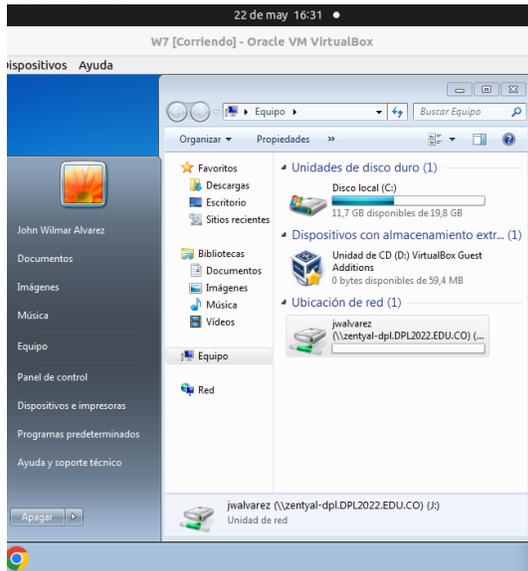


Fig. 19. Sesión iniciada en un cliente del dominio.

También comprobamos la asignación de IP de acuerdo con el rango definido en el DHCP.

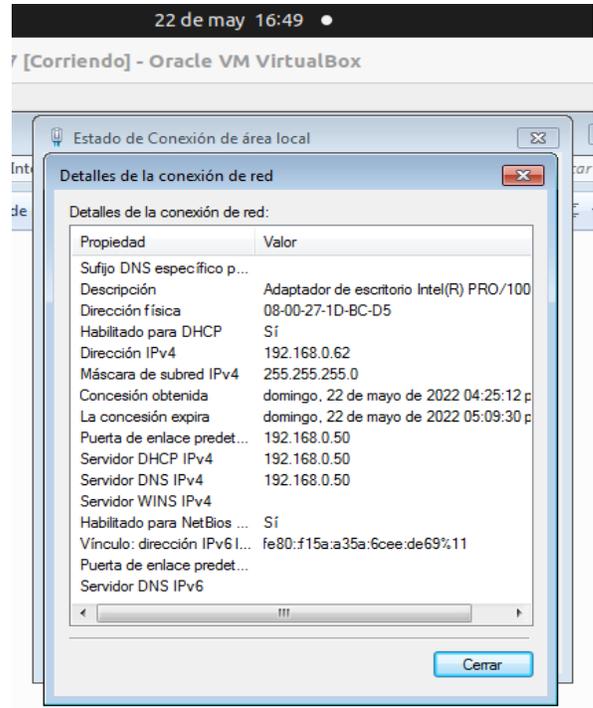


Fig. 20. Comprobando asignación de IP a través del servidor DHCP

Ingresamos a un cliente Ubuntu y verificamos la asignación de IP.



Fig. 21. Comprobación de DHCP y DNS en cliente Ubuntu

2.2 PROXY NO TRANSPARENTE

Paso 1. Después de iniciar sesión nos aparece una interfaz donde se encuentra la configuración inicial.

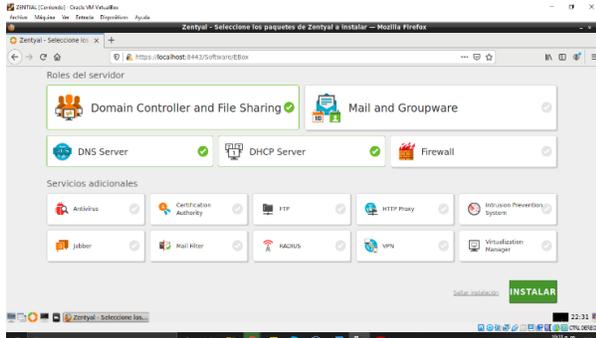


Fig. 22. Evidencia de interfaz de configuración

Paso 2. Realizamos las instalaciones de los paquetes que necesitamos para realizar la gestión y administración de usuarios.

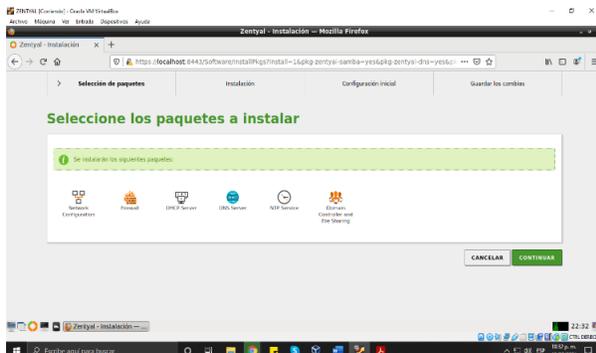


Fig. 23. Evidencia de instalación de paquetes

Paso 3. Comenzamos la instalación.



Fig. 24. Evidencia de inicio de instalación

Paso 4. Configuramos las tarjetas de red, la WAN por DHCP y la LAN estática.



Fig. 25. Evidencia de tarjetas de red

Paso 5. Para la práctica configuramos dos tarjetas de red una DHCP y RED INTERNA para poder comunicarnos los usuarios de las otras máquinas virtuales.



Fig. 26. Evidencia de tarjetas de red DHCP & red interna

Paso 6. Ingresamos el nombre del dominio Zentyal

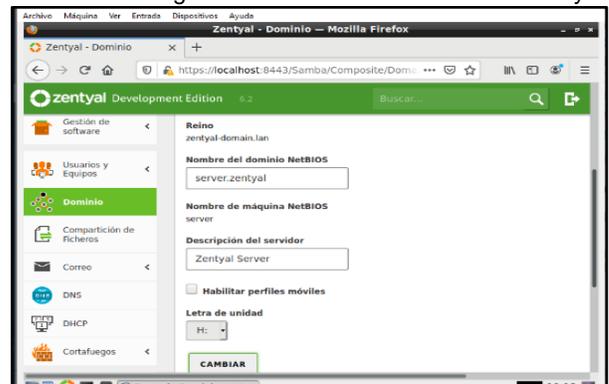


Fig. 27. Evidencia del dominio

Paso 7. Vamos a crear un usuario y grupos para poder ingresarlo al dominio. Para ello activamos el módulo de usuarios y equipos.

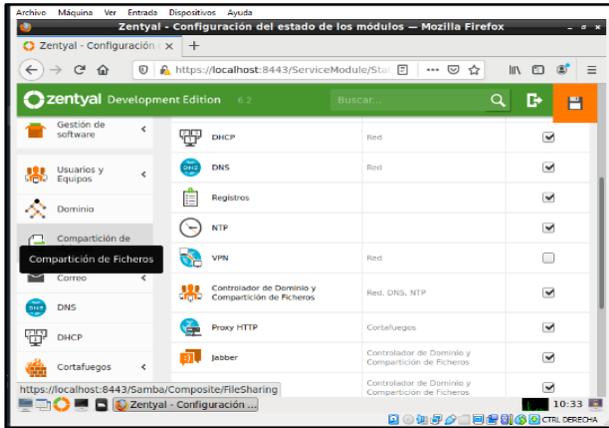


Fig. 28. Evidencia de usuario y grupos

Paso 8. Luego de ello vamos a crear un grupo.

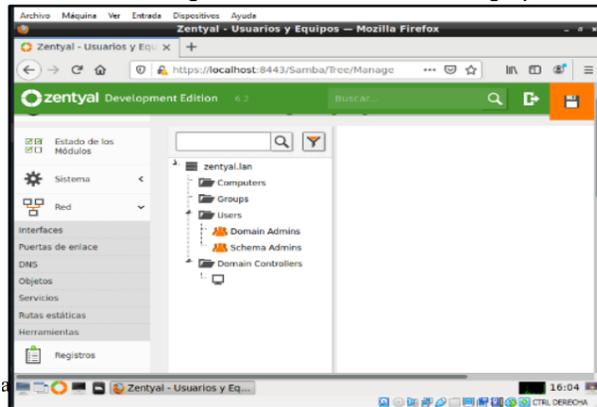


Fig. 29. Evidencia de crear grupo

Paso 9. Ingresamos los datos para identificar el grupo.

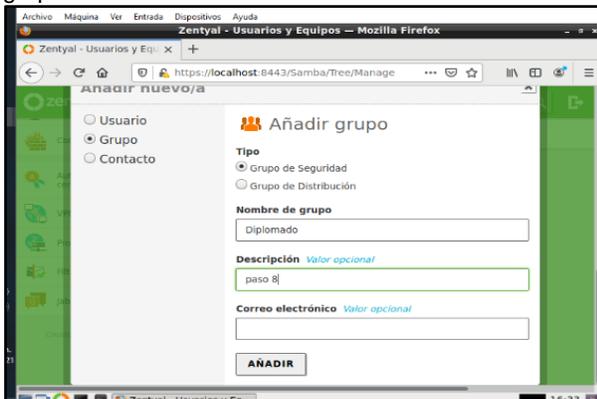


Fig. 30. Evidencia de datos del grupo

Paso 10. Creamos un usuario para el dominio creado anteriormente

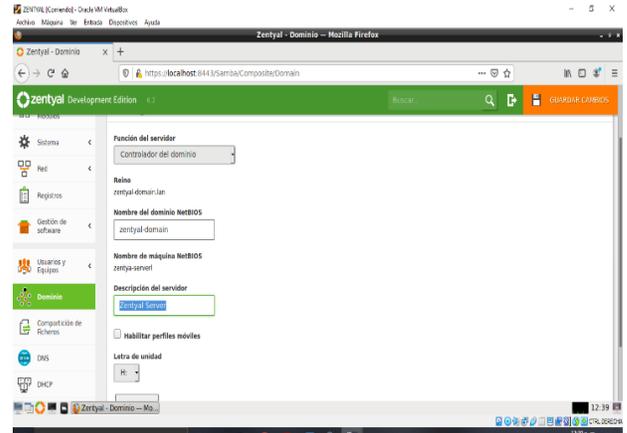


Fig. 31. Evidencia de usuario de dominio

Paso 11. Configuramos la red interna asignándole una ip fija para tener conexión con el Cliente.

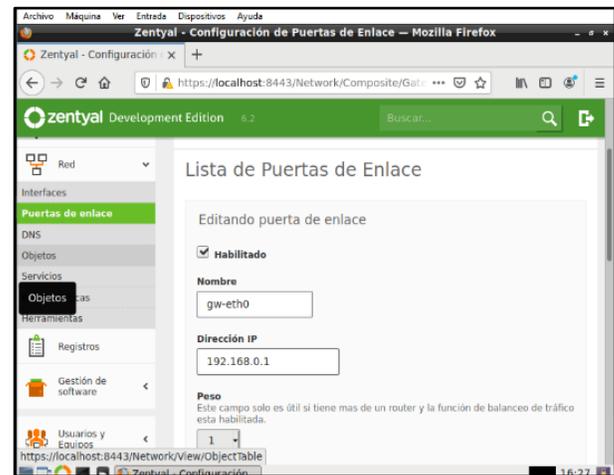


Fig. 32. Evidencia de configuración de red ip

Paso 12. Configuramos la Puerta de Enlace.

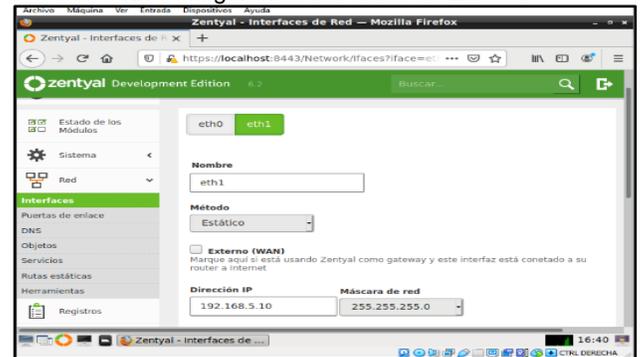


Fig. 33. Evidencia de configuración de puerta de enlace

Paso 13. Damos clic en la opción Objetos y agregamos el nombre de la máquina, en este caso baironbolanos-Diplomado.

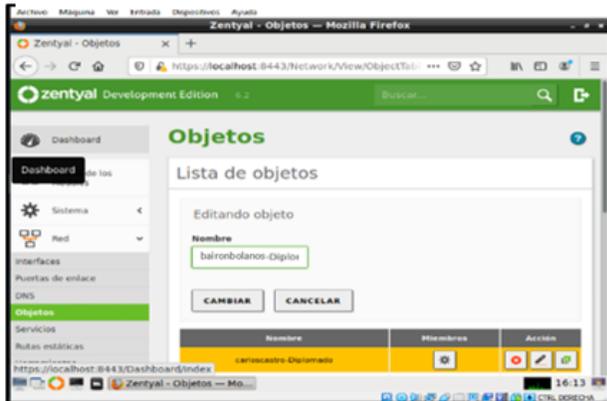


Fig. 34. Evidencia de máquina.

Paso 14. Nos vamos a la configuración del proxy y cambiamos el número del puerto en este caso 1320.

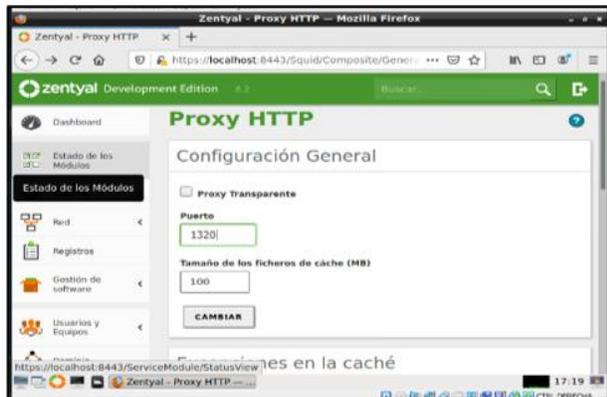


Fig. 35. Evidencia de configuración puerto.

Paso 15. Nos vamos a la opción de rutas de acceso y añadimos el nombre del equipo a conectar

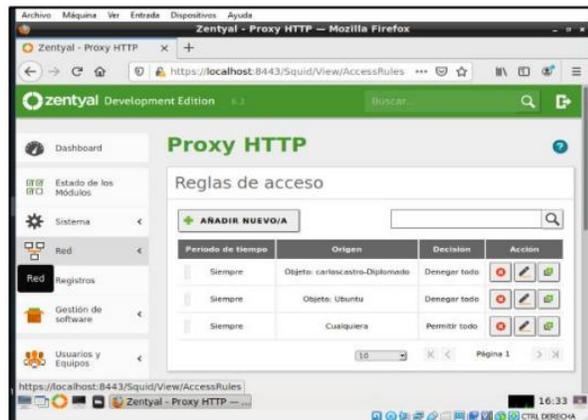


Fig. 36. Evidencia de equipo a conectar.

Paso 16. Se configura el proxy en el equipo de Ubuntu desktop

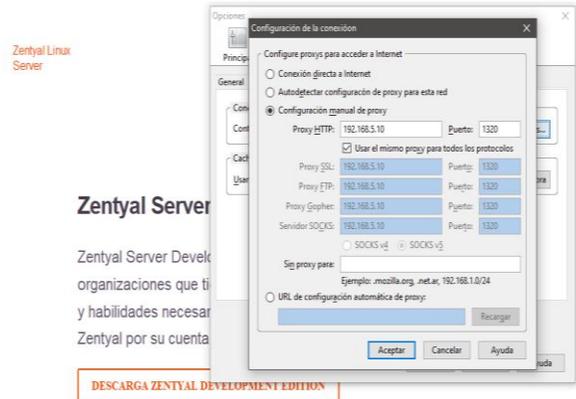


Fig. 37. Evidencia de configuración de proxy.

Paso 17. Se visualiza la prueba que el proxy está funcionando y restringiendo la navegación en el equipo.

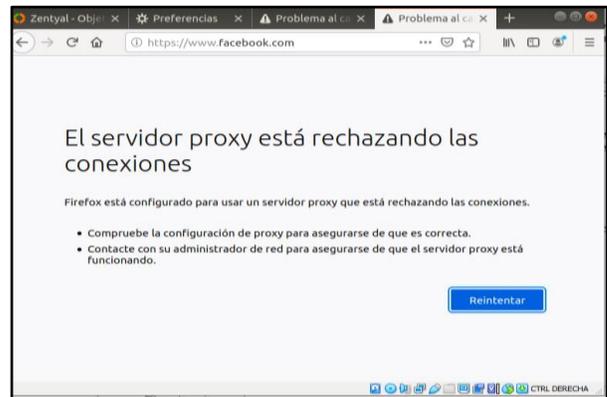


Fig. 38. Evidencia de funcionamiento de proxy.

2.3 CORTAFUEGOS

El cortafuegos o Firewall de Zentyal nos ayuda a proteger la red privada administrada por Zentyal controlando los accesos no autorizados y los no verificados hacia Zentyal, hacia el internet y desde internet.

Para este proceso verificamos los módulos de Zentyal que vamos a usar, por la temática usaremos Network y Firewall y para configurar nuestra red interna la proveemos con DHCP, DNS y Proxy (Fig. 39).

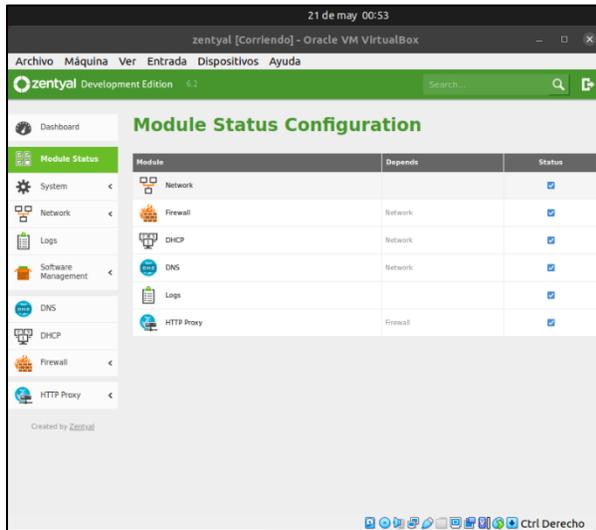


Fig. 39. Estado de módulos Zentyal

DHCP y la asignación del servidor Proxy se establecen para la red Interna para que garantice una conexión exitosa y con acceso a internet a los usuarios.

Se verifica el estado de conexión del cliente mediante sus opciones de red (Fig. 40) y corroboramos que efectivamente le asignó una IP dentro del rango dado en DHCP y con Proxy y DNS tenemos acceso a internet (Fig. 41).

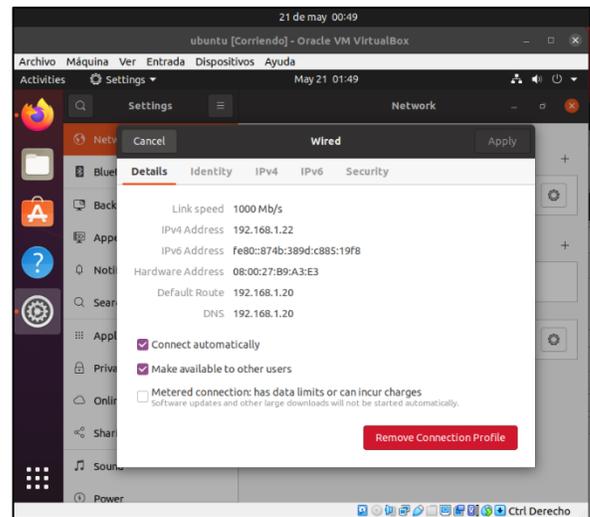


Fig. 40. Configuración de conexión del cliente

Aparte de Zentyal se tendrá el sistema cliente con Ubuntu Desktop conectado a la red interna (LAN) ofrecida por Zentyal.

Tabla 1 Sistemas y direcciones

| Distribución | Conexión red | Dirección IP | Puerta Enlace |
|----------------------|---------------------|--------------|---------------|
| Zentyal Server 6.2 | T.1 Conexión Puente | 192.168.0.27 | 192.168.0.1 |
| Zentyal Server 6.2 | T.2 Red Interna | 192.168.1.20 | 192.168.1.20 |
| Ubuntu Desktop 20.04 | T.1 Red Interna | 192.168.1.22 | 192.168.1.20 |

Para tener estas configuraciones se deben tener previamente configuradas las interfaces de red de Zentyal, La red Externa conectada al adaptador con conexión puente y la interna con una dirección estática asignada.

Se Asigna Gateway para Zentyal definiendo su puerta de enlace del adaptador principal, Mientras que la asignación de las direcciones de servidores de DNS La asignación de dirección IP de manera automática por

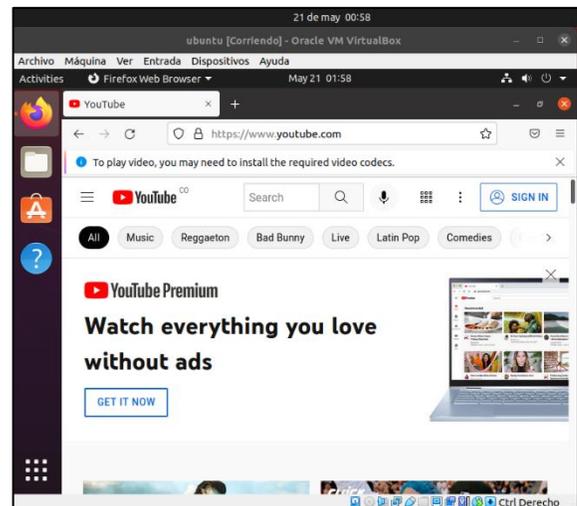


Fig. 41. Conexión exitosa del cliente

Para limitar acceso de las redes sociales y entretenimiento validamos páginas en particulares

- YouTube
- Instagram
- Facebook
- Twitch

Para cada una de ellas realizamos el siguiente proceso.

- Hacemos Ping al dominio por consola (Fig. 42).
- La IP que nos responda el ping la buscamos en whois.arin.net (Fig. 43).
- Agregamos el CIDR indicando las IP Disponible por subred a los miembros de la lista de objetos para usar más adelante (Fig. 44).

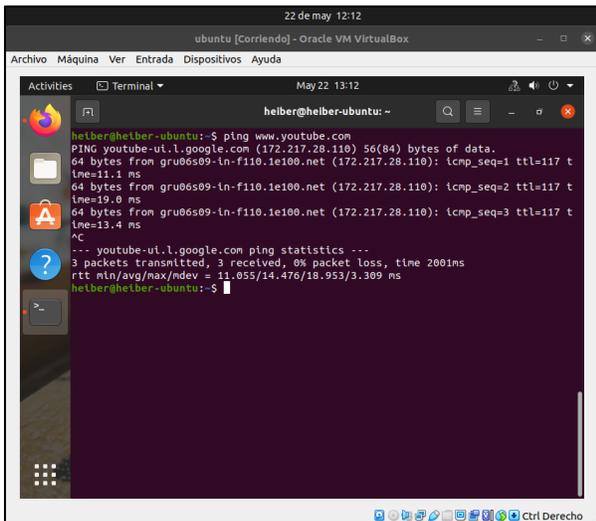


Fig. 42. Ping por dominio en terminal

You searched for: 172.217.28.110

| Network | |
|-------------------|---|
| Net Range | 172.217.0.0 - 172.217.255.255 |
| CIDR | 172.217.0.0/16 |
| Name | GOOGLE |
| Handle | NET-172-217-0-0-1 |
| Parent | NET172 (NET-172-0-0-0) |
| Net Type | Direct Allocation |
| Origin AS | AS15169 |
| Organization | Google LLC (GOGL) |
| Registration Date | 2012-04-16 |
| Last Updated | 2012-04-16 |
| Comments | |
| RESTful Link | https://whois.arin.net/rest/net/NET-172-217-0-0-1 |
| See Also | Related organization's POC records. |
| See Also | Related delegations. |

Fig. 43. Respuesta de whois.arin.net

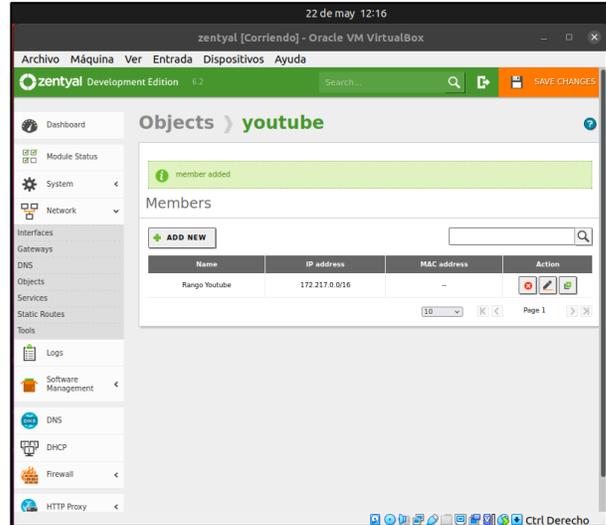


Fig. 44. Lista de miembros en el objeto

Realizamos de la misma manera con las demás redes quedando los rangos de los servidores de las páginas en un solo objeto (Fig. 45) llamado "social-entretenimiento".

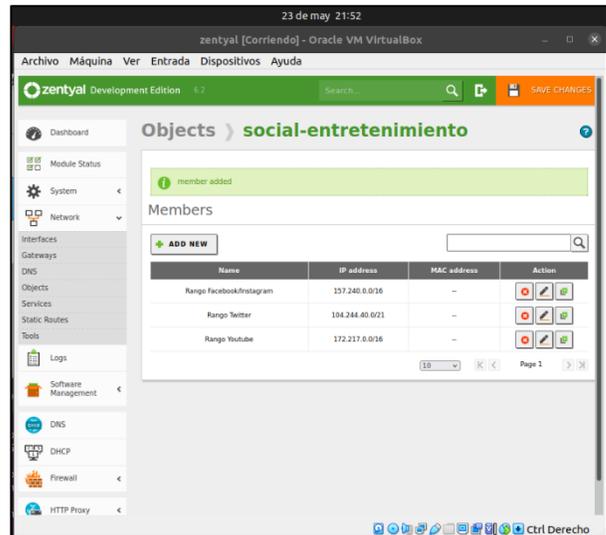


Fig. 45. Adición de las demás páginas en cuestión

Ahora creamos un objeto de clientes en este caso “clientes-Ubuntu” donde iremos registrando nuestros usuarios de la red interna administrada por Zentyal (Fig. 46).

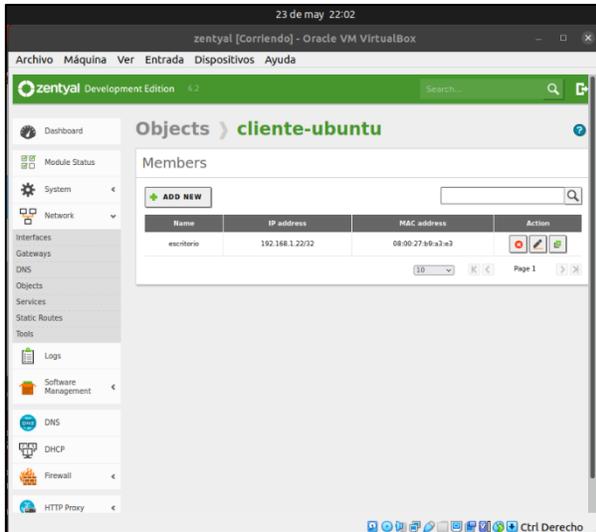


Fig. 46. Creación objeto direcciones clientes

Zentyal separa las direcciones de conexión entre las redes internas, internet y el mismo Zentyal, para este proceso vamos a crear una regla para las conexiones para las redes internas (Fig. 47) donde asignamos una conexión denegada de los usuarios “cliente-Ubuntu” hacia las páginas controladas de redes y entretenimiento “social-entretenimiento”.

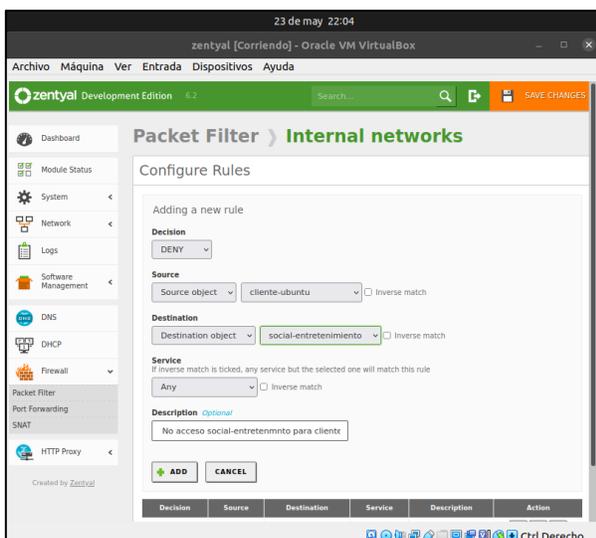


Fig. 47. Creación de regla para redes internas

De igual manera es recomendable crear una regla en las peticiones que vengan de internet a Zentyal (Fig. 48) por parte de las páginas controladas de redes y entretenimiento “social-entretenimiento” con eso se genera esta captura de peticiones que las páginas pueden generar a sus usuarios.

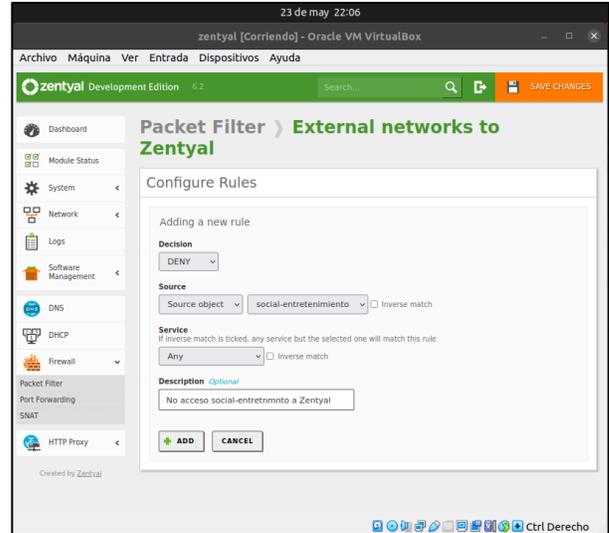


Fig. 48. Creación de regla de red externa a Zentyal

Con estas reglas asignadas podremos verificar (Fig. 49) que los usuarios pertenecientes al objeto de clientes no pueden acceder a ninguna de las direcciones consignadas en el objeto de redes.

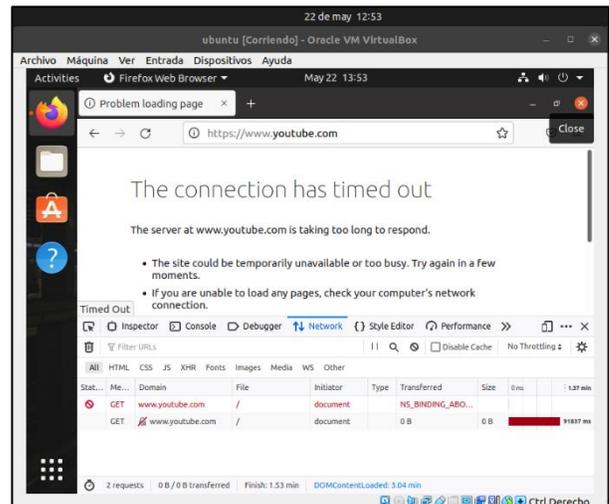


Fig. 49. Comprobación acceso a YouTube

2.4 FILE SERVER Y PRINT SERVER

Para la configuración de zentyal 7.0 se debe comenzar con la configuración de Configuramos los 2 adaptadores de red de forma DHCP que nos permitirá la conexión a internet y otra con ip fija que nos permite realizar configuración de instalaciones de aplicaciones.

Se hace la configuración de la primera red de forma con dhcp.

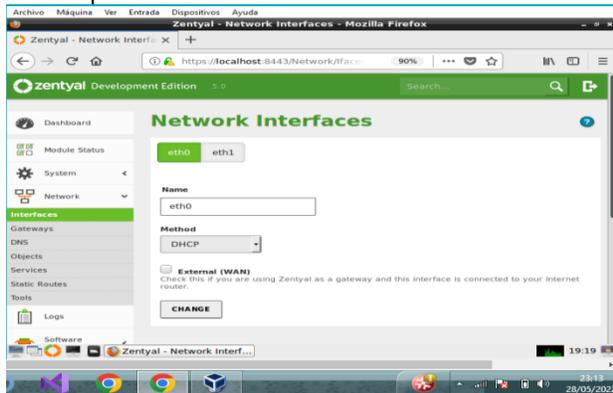


Fig. 50. configuración red dhcp

El segundo se configura con una dirección ip fija. 192.168.0.15

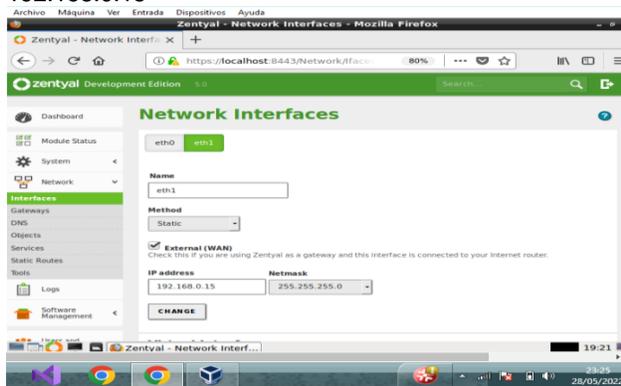


Fig. 51. configuración red fija

Para su óptimo funcionamiento definimos los dns que se van a utilizar en la conexión.

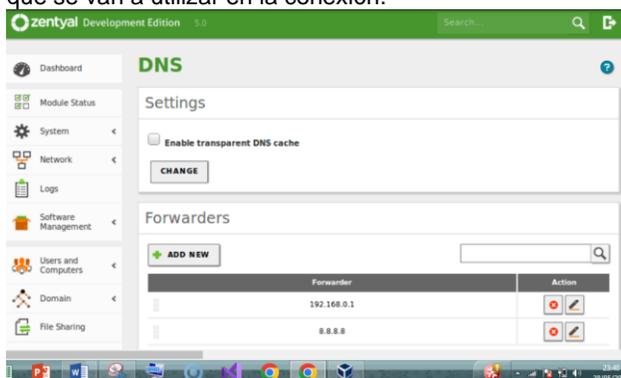


Fig. 52. Configuración de los dns

Debemos realizar la configuración de la que va a trabajar con DHCP y la ip fija.

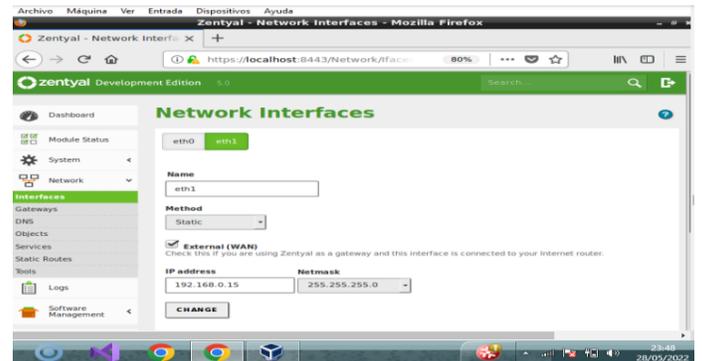


Fig. 53. Configuración ip

Una vez realizada las configuraciones guardan todos los cambios realizados.

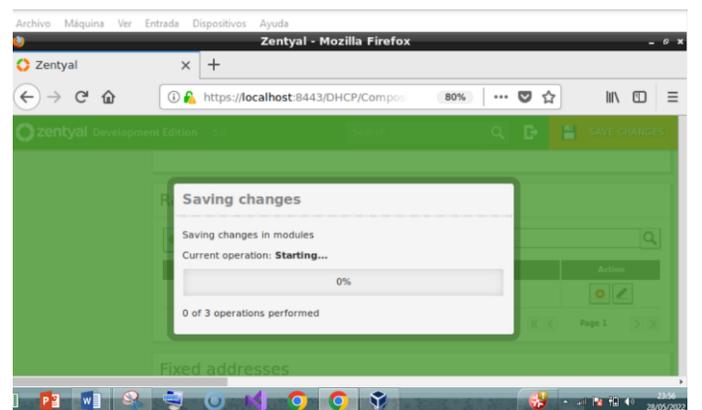


Fig. 54. salvar guardar la información.

Al finalizar esta configuración se guarda y es la encargada de poder asignar las direcciones ip.

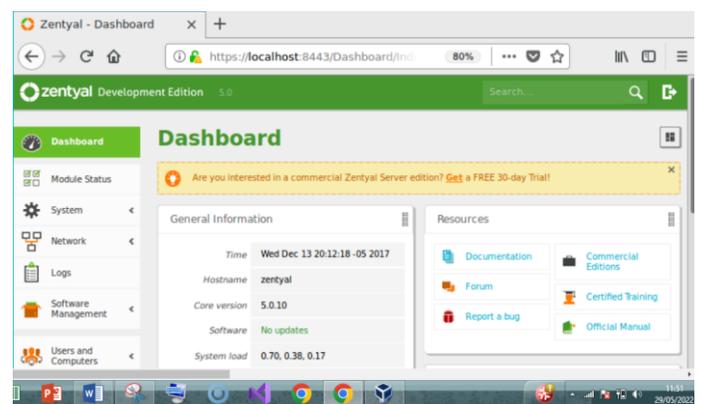


Fig. 55. Configuración ip

Instalamos el cliente por medio de LDAP

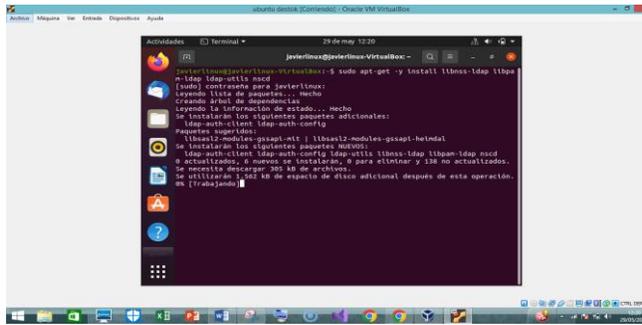


Fig. 56. instalación Idap

Se realiza la configuración de LDAP.

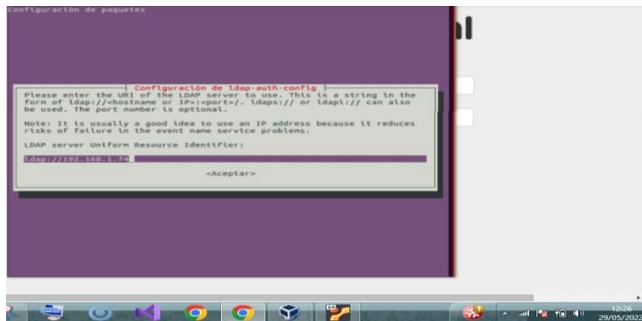


Fig. 57. Configuración Idap

Realizamos la Creación de los diferentes usuarios y grupos que vamos a utilizar.

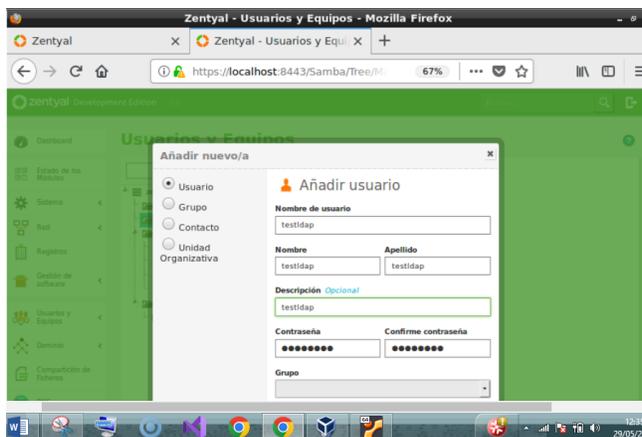


Fig. 58. Configuración usuarios

Realizamos la creación de una carpeta para compartirla posteriormente en la opción file sharing.

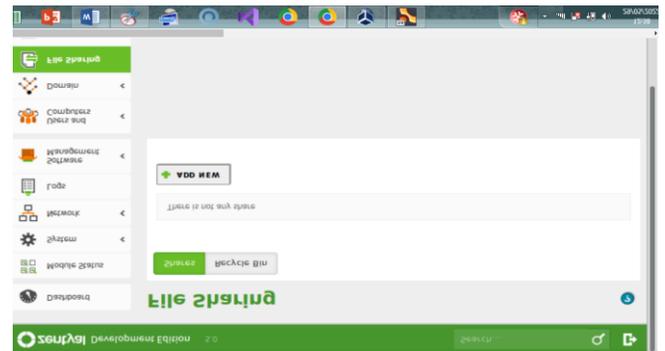


Fig. 59. Configuración carpeta compartida

Se asigna un nombre a la careta compartida.

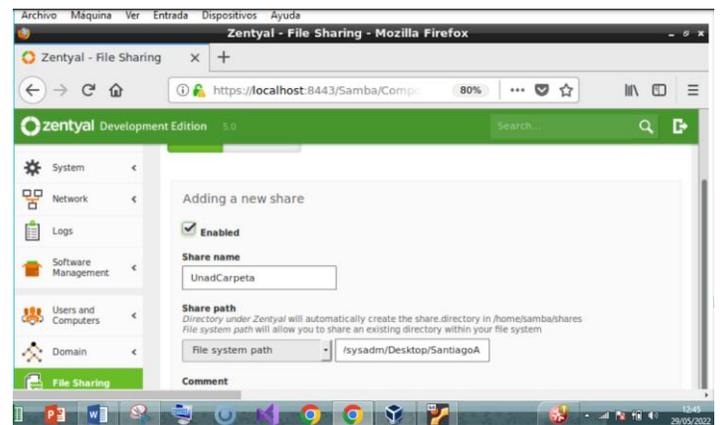


Fig. 60. asignación nombre carpeta compartida

Guardamos el cambio una vez realizado la configuración correcta.

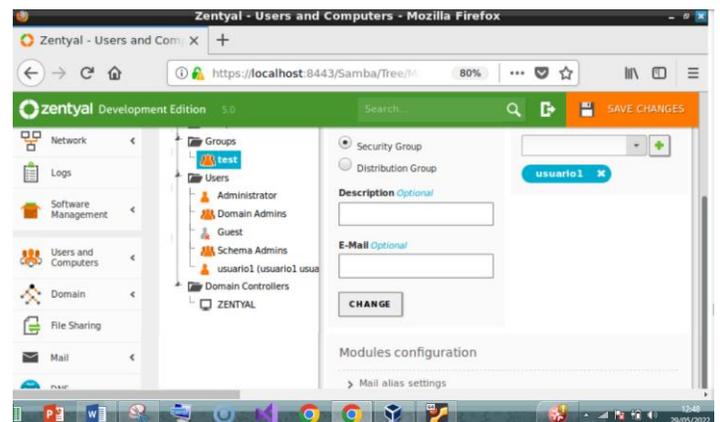


Fig. 61. se guarda la configuración

2.5 VPN

Para este caso se debe instalar el servicio de VPN, se selecciona VPN y se procede a instalar.

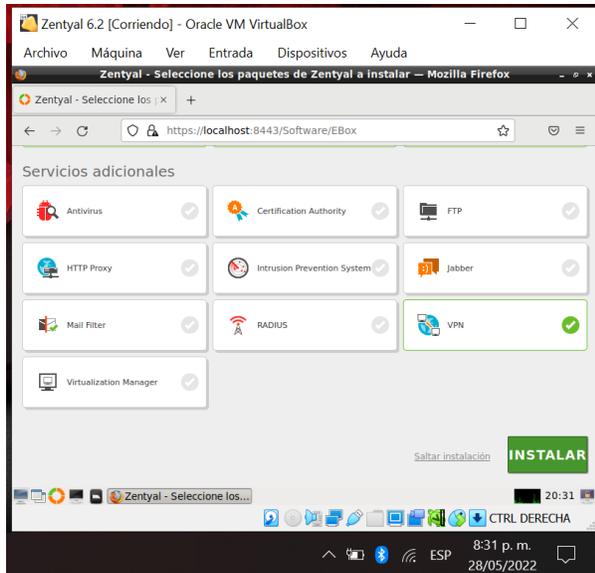


Fig. 62. Módulos a instalar en Zentyal

Posteriormente se configuran las interfaces de red, dejando una para red interna en modo estático y la otra configurada como DHCP para recibir la conexión externa de internet.

Esta parte es muy importante ya que de aquí se toma la dirección IP que será la conexión de los certificados que se descarguen para los clientes externos que hagan uso de la VPN a través del servicio OPEN VPN.

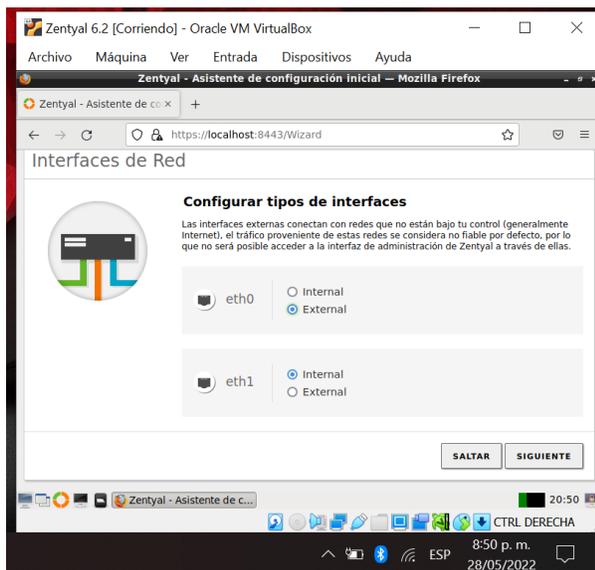


Fig. 63. Configurar tipos de interfaces

Luego de revisar los servicios a instalar y haber solicitado la instalación del servicio VPN, el servidor notifica la configuración exitosa.

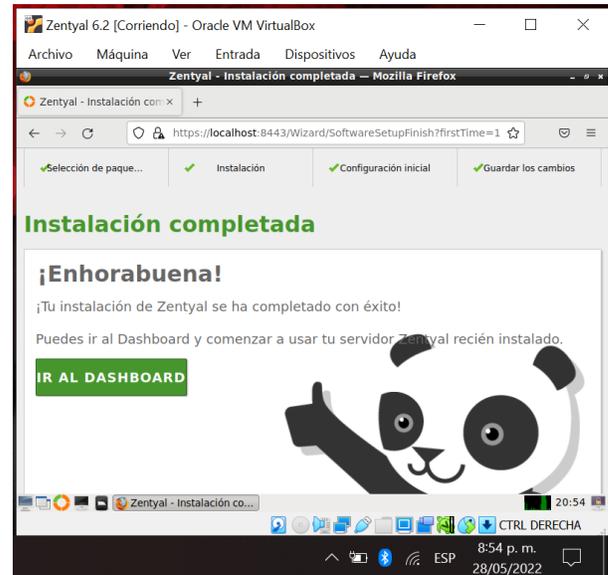


Fig. 64. Instalación completa módulos Zentyal

Se verifica que estén los servicios de prerequisite para usar el servicio VPN, en total los tres servicios que deben estar activos son. Cortafuegos, autoridad de certificación y VPN.

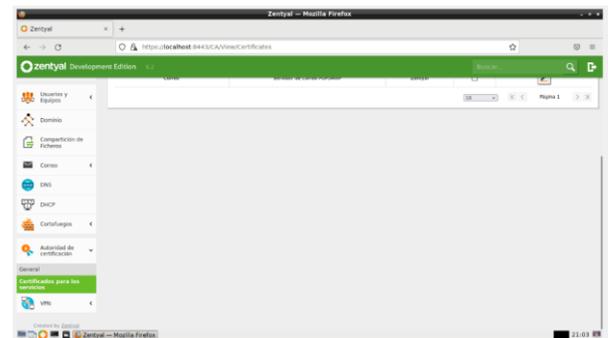


Fig. 65. Dashboard y módulos Zentyal

Lo primero que se debe realizar es la creación de los certificados que generarán los archivos de conexión entre el servidor, el cliente y los servicios VPN.

El primer certificado que va para la aplicación zentyal se denominó "diplomadowcb".



Fig. 66. Creación de certificados

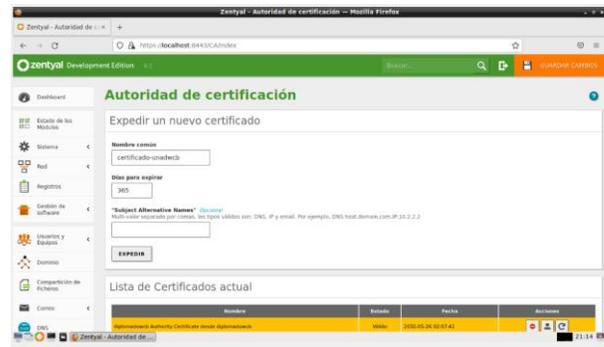


Fig. 70. Generar certificado VPN

Lista de Certificados actual

| Nombre | Estado | Fecha | Acciones |
|---|--------|---------------------|----------------------|
| Administración Authority Certificate desde administracion | Válido | 2023-05-28 22:07:43 | [Iconos de acciones] |

Fig. 67. Tabla de certificados existentes

Lista de Certificados actual

| Nombre | Estado | Fecha | Acciones |
|---|--------|---------------------|----------------------|
| Administración Authority Certificate desde administracion | Válido | 2023-05-28 22:07:43 | [Iconos de acciones] |
| vpn-serverunadwcb | Válido | 2023-05-28 22:07:43 | [Iconos de acciones] |
| certificado-unadwcb | Válido | 2023-05-28 21:15:22 | [Iconos de acciones] |

Fig. 71. Lista de certificados

Luego de crear el certificado inicial, se procede a la creación del servidor, se debe seleccionar la opción VPN y luego servidores.

Se realiza la verificación de los servidores VPN disponibles, en este caso se evidencia que el servidor denominado "serverunadwcb" está listo para su proceso de configuración.

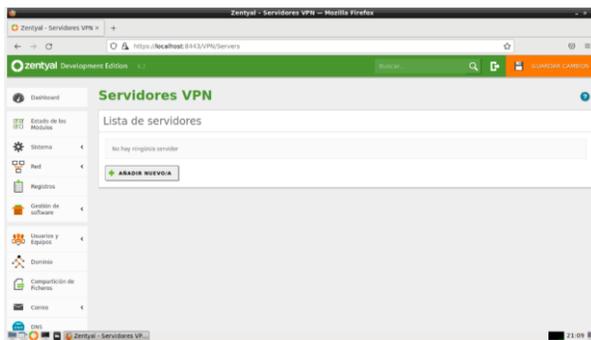


Fig. 68. Lista servidores VPN



Fig. 72. Lista de servidores VPN

Se procede a la creación del servidor VPN dentro del servicio Open VPN y se nombra "serverunadwcb".

Luego se ingresa a la opción de configuración del servidor y se evidencia el puerto UDP 1194 que es el puerto por el que se realiza conexión con el cliente, la dirección IP se deja por defecto la que nos arrojó el servidor.



Fig. 69. Creación de servidor VPN



Fig. 73. Configuración de servidor VPN

Se genera el certificado del servidor VPN, este certificado es el que se podrá configurar para posteriormente descargar los certificados de conexión.

Se realiza la activación de la interfaz TUN y las demás opciones se dejan por defecto.

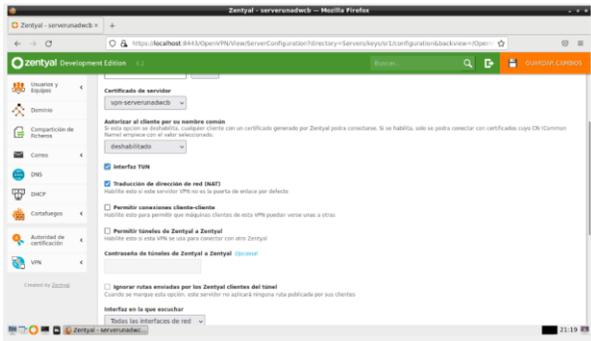


Fig. 74. Configuración de servidor VPN

Se debe crear el servicio para poder establecer la conexión a las VPNs.



Fig. 75. Lista y creación de servicios

Luego de Crear el servicio, se debe configurar, para este caso como se dejó por defecto, se usará el puerto 1194.



Fig. 76. Configuración de servicios

Se crea la regla de firewall permitiendo que acepte el tráfico originado desde cualquier equipo que tenga un certificado.



Fig. 77. Creación de reglas firewall

Se muestra la tabla donde se hace el resumen de los servicios que se están ejecutando.

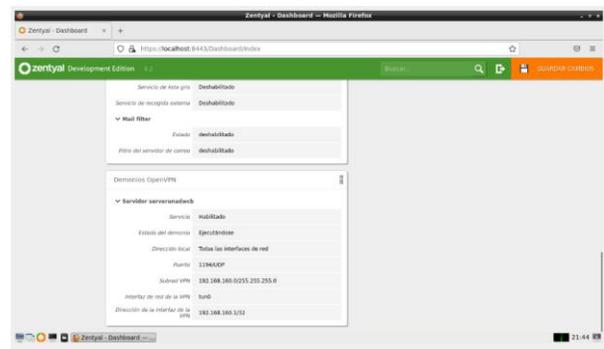


Fig. 78. Servicios en ejecución

Posterior a esto, se selecciona la opción VPN, luego se escoge el servidor que se va a usar y se debe escoger la opción descargar paquete de configuración del cliente, en esta opción se selecciona el tipo de cliente que usará el servicio, sea Windows o Linux, se descarga y usando la herramienta OPEN VPN (instalándola en Windows o usando por defecto la que viene instalada en UBUNTU) se genera la conexión y uso del servicio VPN.

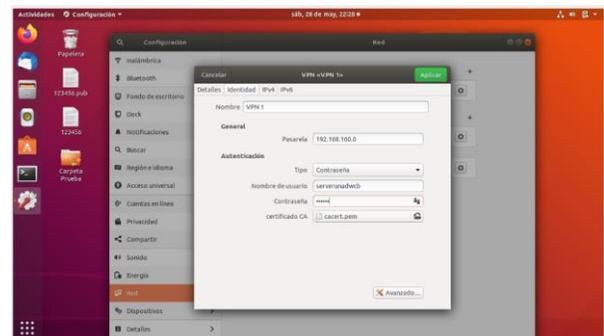


Fig. 79. Configuración VPN equipo cliente

3 CONCLUSIONES

Con el desarrollo de este trabajo se pudo brindar una solución óptima a problemáticas de infraestructura tecnológica poniendo en marcha servicios de gestión y controlador de dominio de una organización, por medio del cual se pudieron gestionar usuarios y grupos, adicionalmente se pudo configurar un servidor DNS el cual nos sirve para traducir o resolver una dirección IP a un nombre propio de dominio, también como apoyo al servidor de dominio, se pudo configurar un servidor DHCP el cuál se encargó de gestionar el asignamiento de IP de manera dinámica a las maquinas tipo clientes que conectamos al dominio creado.

Zentyal es un servidor muy sencillo de administrar basado en Ubuntu, que incluye todos los servicios necesarios para abordar la gestión y administración de los servicios esenciales para arrancar una empresa dentro de los cuales encontramos. Gestión de red, Servidor de correo, Comunicaciones, Compartición de recursos y trabajo en grupo. servidor de archivos, servidor de impresión y groupware Gestión centralizada de usuarios, Autoridad de certificación.

Con el servicio de Firewall o Cortafuegos ofrecido por Zentyal se puede administrar no solo las peticiones de acceso al mismo sistema, sino que podemos administrar el acceso de los usuarios y hacia los usuarios que vienen de las conexiones externas, esto garantiza una mejor seguridad a toda la red interna y garantiza un entorno seguro para el trabajo.

Desarrollamos destrezas en configuración de cada uno de los componentes los cuales nos permiten compartir archivos ingresando por medio de una dirección ip previamente configurada desde otro sistema operativo en este caso Ubuntu.

La conexión VPN permite crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet.

4 REFERENCIAS

- [1] A. (2020, 8 mayo). Zentyal Server 6.2 Development Ahora Disponible. Zentyal Linux Server. [https://zentyal.com/es/news/zentyal-6-2-announcement-2/Zentyal 6.2 Documentación Oficial](https://zentyal.com/es/news/zentyal-6-2-announcement-2/Zentyal%206.2%20Documentación%20Oficial).
- [2] Zentyal S.L. (2004). Cortafuegos — Documentación de Zentyal 6.2. Zentyal Community. <https://doc.zentyal.org/6.2/es/firewall.html>
- [3] Zentyal – Controlador de Dominio Linux y Políticas de Grupo. Diciembre de 2017. Archivo de Internet. Recuperado de <https://julioestrepo.wordpress.com/2015/02/09/zentyalcontrolador-dominio-linux-y-politicas-de-grupo/>
- [4] Sanz Mercado, P. (2014). Seguridad en linux. guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 61 - 105). elibro. <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=61>
- [5] ValorTop S.L. (2014-2018). ¿Qué es un proxy o servidor proxy. Recuperado de <http://www.valortop.com/blog/servidorproxy>