

DIPLOMADO DE PROFUNDIZACIÓN GNU/LINUX, PASO FINAL IMPLEMENTACIÓN ZENTYAL SERVER 6.2.

Edgar Leónidas Santa Garzón
e-mail: elsantag@unadvirtual.edu.co
Jaime David Burbano García
e-mail: jdburbanog@unadvirtual.edu.co
Johan Edisson Rubiano Gutiérrez
e-mail: jerubianogu@unadvirtual.com
Sergio Ernesto Ospitia Rojas
e-mail: seospitiar@unadvirtual.edu.co
Yuderly Burbano
e-mail: yburbano@unadvirtual.edu.co

RESUMEN: Durante el desarrollo de esta actividad implementamos las 5 Temáticas, iniciando con Instalación y configuración del sistema operativo GNU/Linux Zentyal Server 6.2 (Instalar y configurar como sistema operativo base para disponer de los servicios de Infraestructura IT). Cabe resaltar que para el desarrollo de esta actividad cada temática es seleccionada por un estudiante y posteriormente puesta en práctica de lo aprendido durante el DIPLOMADO, se debe definir la zona DMZ de acuerdo a la Red administrable que se debería crear para acceder desde el GNU/Linux al Zentyal Server 6.2, poniendo a prueba la potencia y versatilidad del servidor, Instalando y configurando Servicios como DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server, VPN.

PALABRAS CLAVE: Zentyal Server 6.2, servicios de Infraestructura IT, Controlador de Dominio, Proxy no Transparente, Cortafuegos, File Server, Vpn

1 INTRODUCCIÓN

Zentyal fue desarrollado con el objetivo de acercar Linux a las pymes y permitirles aprovechar todo su potencial como servidor de empresa pues las distribuciones Linux poseen muchas herramientas que le permiten adaptar la infraestructura IT según las necesidades de la empresa. Podemos indicar que es la alternativa en código abierto a los productos de Microsoft para infraestructura TIC en las pymes. Adicionalmente podemos indicar que está construido sobre Ubuntu y cuenta con una interfaz gráfica a la que podremos acceder desde cualquier navegador o aplicación web, logrando administrar los servicios de la red.

Zentyal permite a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red o las comunicaciones, de forma sencilla y a través de una única plataforma.

2 INSTALACIÓN ZENTYAL SERVER 6.2

2.1 DESCARGA ZENTYAL SERVER 6.2

Para realizarlo vamos a la página de Zentyal y descargamos la imagen ISO de Zentyal 6.2 <https://zentyal.com/es/news/zentyal-6-2-announcement-2/>



Figura 1. Descargando la ISO

2.2 CONFIGURACIÓN MAQUINA VIRTUAL

Detalles configuración de la máquina virtual usando Virtual Box[XX]. las características principales en la configuración son Nombre de la Máquina, Memoria RAM, Disco Duro, Tarjetas de Red.

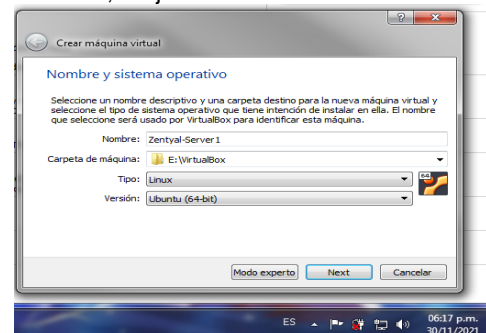


Figura 2. Creación de la Máquina Virtual

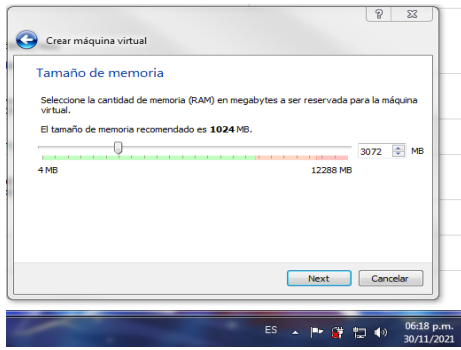


Figura 3. Configuración Memoria RAM

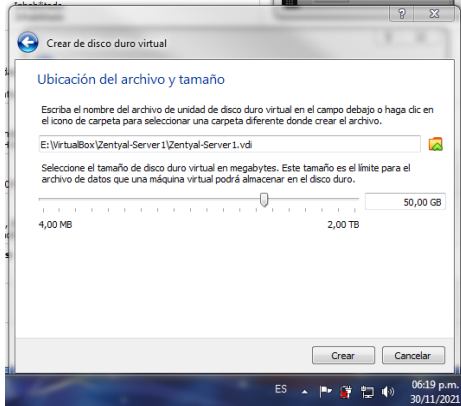


Figura 4. Asignación tamaño del Disco Duro

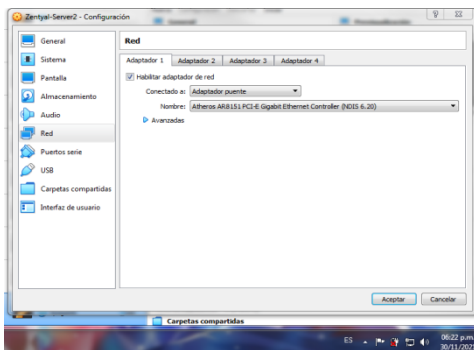


Figura 5. Configuración Tarjeta de Red WAN

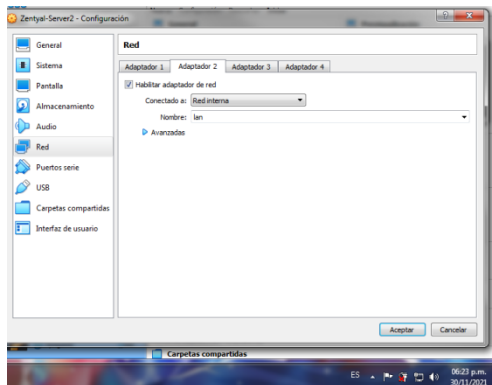


Figura 6. Configuración Tarjeta de Red LAN

En este paso 2.3, se inicia la instalación del Zentyal Server, Seleccionando idioma, tarjeta de red WAN, partición de disco Guiada, usuario de administración,[2]



Figura 7. Seleccionamos Idioma

Menú instalación Zentyal se selecciona la segunda opción para no instalar la interface grafica

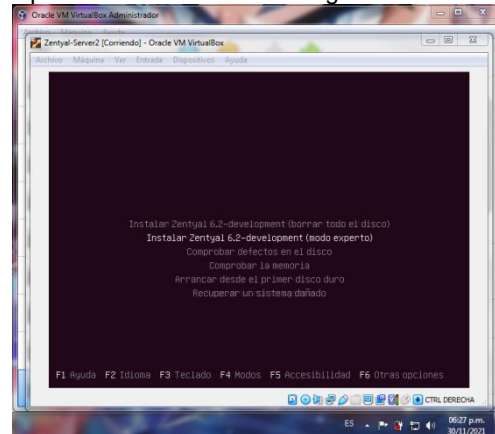


Figura 8. Seleccionamos Modo Experto, solo Consola

Selecciona el país Colombia para configuración teclado

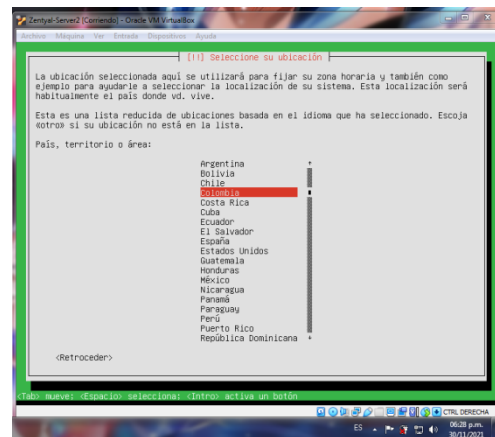


Figura 9. Seleccionamos País

2.3 INSTALACIÓN ZENTYAL SERVER

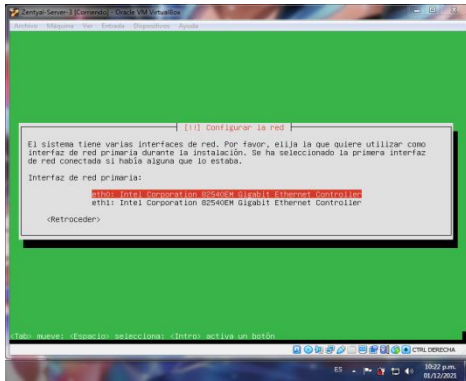


Figura 10. Configuramos Tarjeta de Red eth0 como WAN

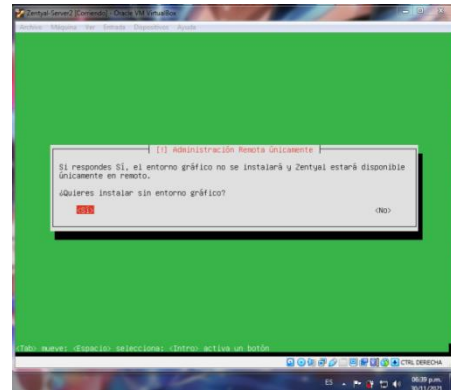


Figura 14. Seleccionamos Si para No Instalar Entorno Grafico

Asignamos nombre del usuario administrador edgarsanta.

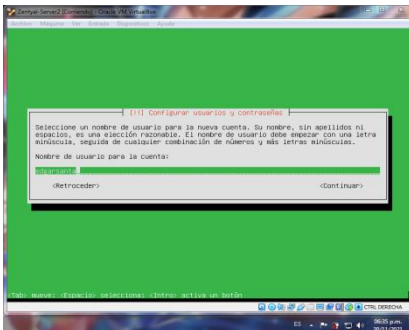


Figura 11. Digitamos Nombre de Usuario

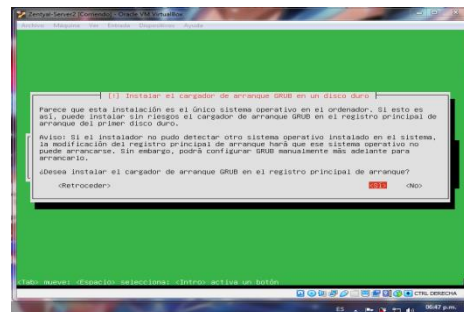


Figura 15. Instalamos Cargador de Arranque del Sistema Operativo

se establece contraseña para el usuario administrador, creado en la figura 11.

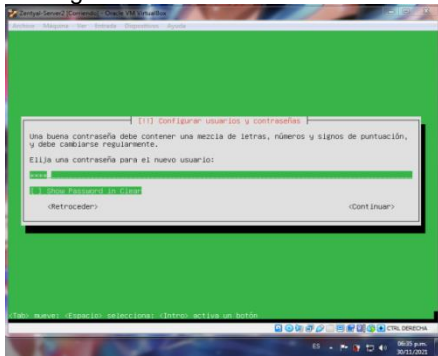


Figura 12. Digitamos Contraseña

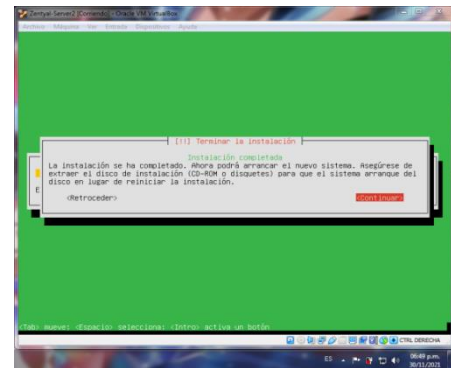


Figura 16. Instalación Completa Zentyal

se selecciona tipo de partición guiado



Figura 13. Partición de Disco, Guiado

Inicio de sesión Zentyal 6.2 Modo Consola.

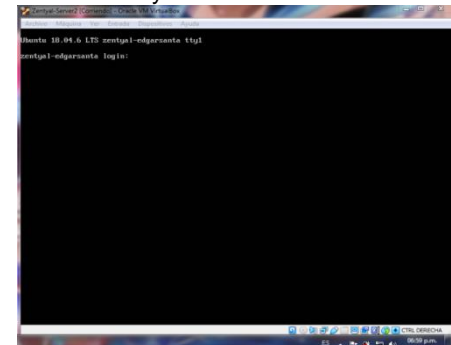


Figura 17. Iniciamos Zentyal por primera vez

para la siguiente figura 14, se va seleccionar no instalar entorno grafico

Ya queda instalada la máquina virtual de Zentyal



Figura 18. Escritorio de Zentyal

3 TEMÁTICA 1 : IMPLEMENTACIÓN Y CONFIGURACIÓN DE DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

3.1 INSTALACIÓN DE PAQUETES DHCP, DNS Y CONTROLADOR DE DOMINIO

En este paso 3.1 se instala los tres paquetes necesarios para el desarrollo de la Temática 1, ingresando desde la interface Web del Servidor Zentyal.

El servicio DHCP necesita una interfaz configurada estáticamente sobre la cual se despliega el servicio. Esta interfaz deberá además ser interna. Desde el menú DHCP podemos encontrar una lista de interfaces sobre las que podremos ofrecer el servicio.[4]

El módulo de servidor de DNS de Zentyal siempre funciona como servidor DNS caché para las redes marcadas como internas en Zentyal, así que, si solamente queremos que nuestro servidor realice caché de las consultas DNS, bastará con habilitar el módulo [5]

Zentyal integra Samba4 como servicio de directorio, implementando la funcionalidad de un controlador de dominio Linux/Windows, además de compartición de ficheros. [6]

Ingreso vía web desde el navegador de la maquina anfitriona, con la IP configurada en la interface WAN, configurada automáticamente, durante la instalación.

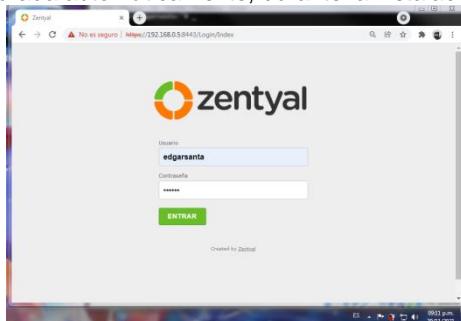


Figura 19. Inicio de Sesión Web Servidor Zentyal

Selección de paquetes controlador de dominio, DHCP y DNS Server a instalar.



Figura 20. Selección de Paquetes a Instalar

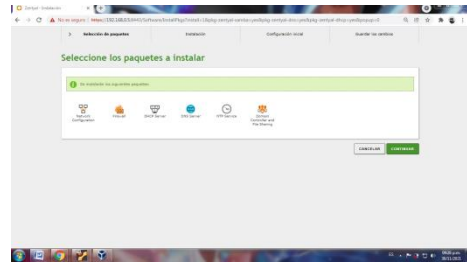


Figura 21. Paquetes a Instalar Seleccionado

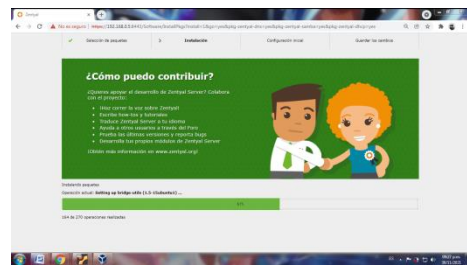


Figura 22. Instalando los Paquetes Seleccionados

Selección de interfaces externa para el eth0 WAN y interna para la interface LAN eth1.



Figura 23. Selección Interfaces de red, Externa y Interna

Configuración Interface de red, WAN modo estática IP:192.168.0.5, Interface LAN IP:192.10.66.1, figura 24.

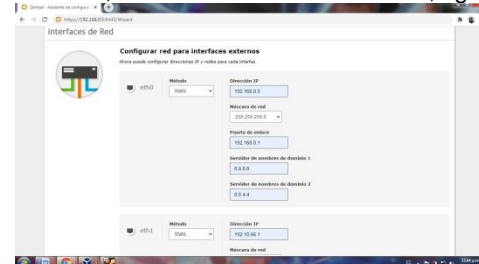


Figura 24. Configuración IP a las Tarjetas de Red

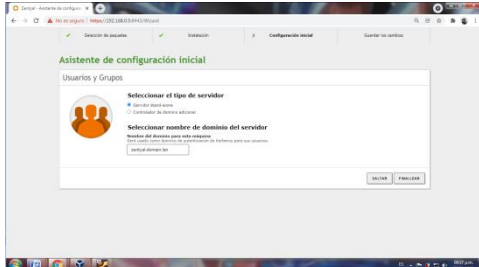


Figura 25. Configuración Nombre del Dominio del Servidor

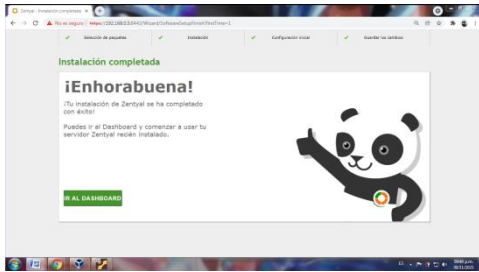


Figura 26. Instalación Satisfactoria

Activación de paquetes instalados, Controlador de Dominio, DHCP y DNS Server.



Figura 27. Activamos Módulos DHCP, DNS y Controlador de Dominio

3.2 CONFIGURACIÓN DHCP SERVER

Configuración básica eth1 LAN, figura 28 y añadimos nuevo rango DHCP figura 29.

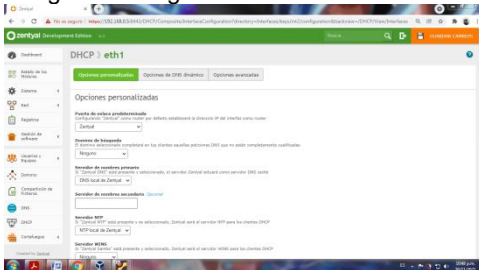


Figura 28. Configuramos Opciones DHCP Server

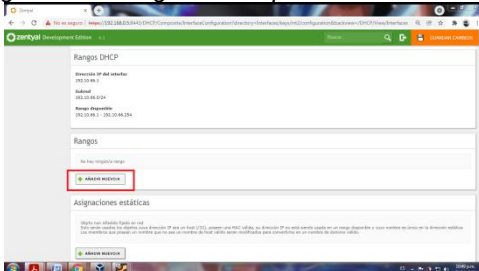


Figura 29. Añadimos Rango IP

Agregando rango de DHCP IP:192.10.66.5-192.10.66.30

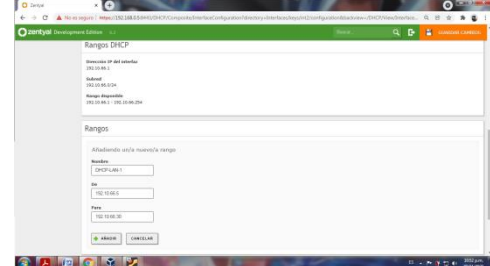


Figura 30. Digitamos Rango de IP, Inicio y Final

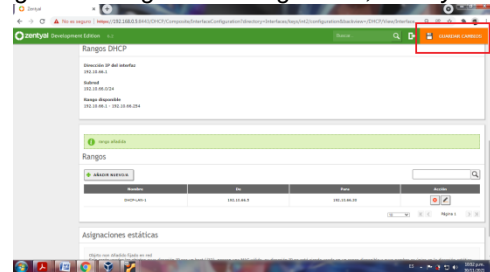


Figura 31. Guardar Nuevo Rango de IP DHCP Server

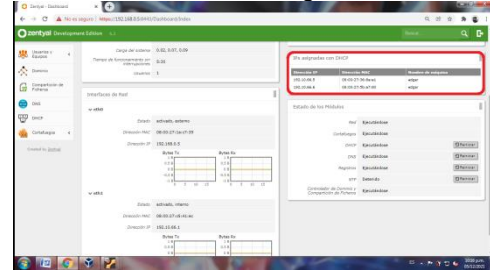


Figura 32. Registros de Equipos por DHCP

3.3 CONFIGURACIÓN DNS SERVER

El DNS de Zentyal funciona como servidor DNS caché para las redes internas en Zentyal, así que si queremos que nuestro servidor realice caché de las consultas DNS, solo con habilitar el módulo [6].

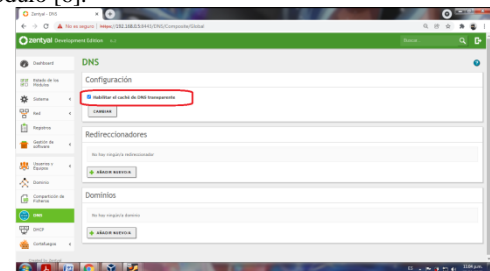


Figura 33. Activación DNS Server

3.4 CONFIGURACIÓN CONTROLADOR DE DOMINIO Y CREACIÓN DE GRUPOS Y USUARIOS CON SUS RESPECTIVOS DIRECTORIOS.

A continuación se crearan dos grupos Informática directorio figura 33 y tesorería datos figura 35. También se crearan dos Usuarios junto con sus directorios respectivos y se asignara cada uno a un grupo creado [6] anteriormente. figura 37,38

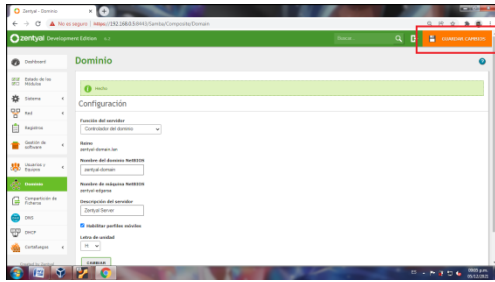


Figura 34. Configuración Inicial Controlador de Dominio

Creación de Grupo informática figura 35 y configuración de directorio compartido, figura 36

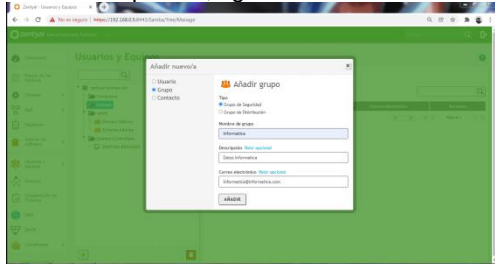


Figura 35. Agregamos el Primer Grupo

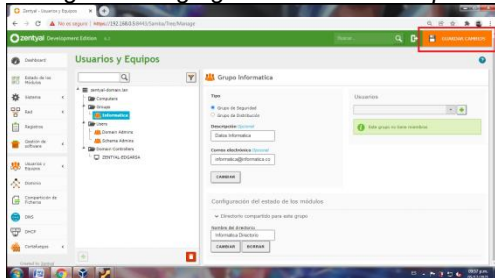


Figura 36. Activamos del Directorio Compartido al Grupo creado en la Figura anterior

Creación de Grupo tesorería figura 37 y configuración de directorio compartido, figura 38.

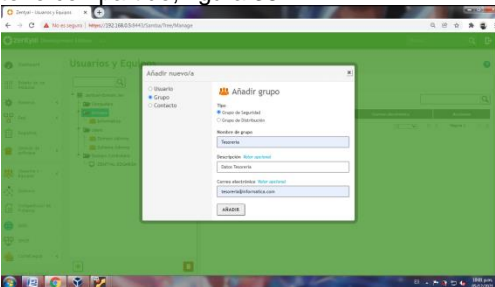


Figura 37. Agregamos el Segundo Grupo

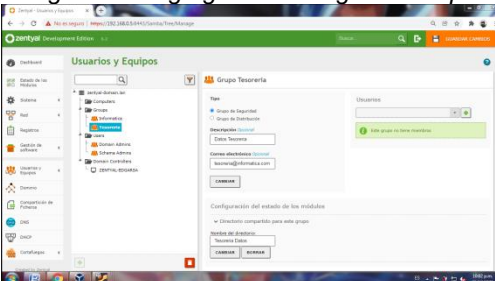


Figura 38. Activamos del Directorio Compartido al Grupo creado en la Figura 40

Creación de dos usuarios y asignación a directorios compartidos, figura 39 y 40.

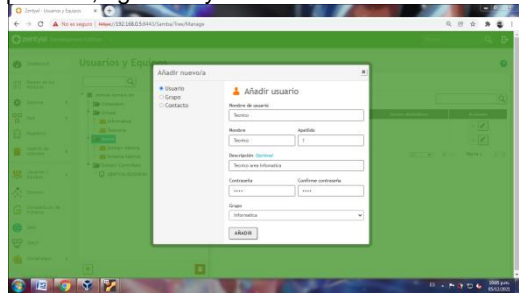


Figura 39. Creación Nuevo Usuario Técnico y Asignación de Grupo

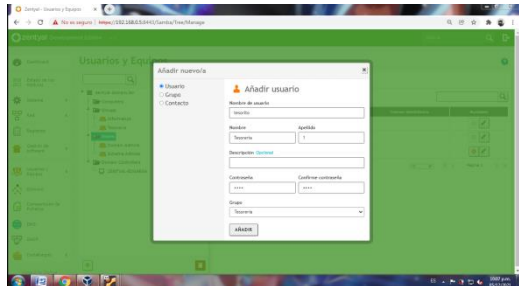


Figura 40. Creación Nuevo Usuario Tesorito y Asignación de Grupo

3.5 DIRECTORIOS COMPARTIDOS DESDE EQUIPOS UBUNTU DESKTOP, PRUEBAS

En este paso 3.5 se van a realizar pruebas de conexión al servidor de Dominio Zentyal con dos Ubuntu Desktop, probando los dos Usuarios creados en las Figuras 37,38 desde el explorador de archivos. de la siguiente forma.

smb:// 192.10.66.1 Usuario: técnico, figura 42
smb ://192.10.66.1 Usuario: tesorito, figura 42

Validación de asignación IP por DHCP a los Ubuntu Desktop, figura 41.

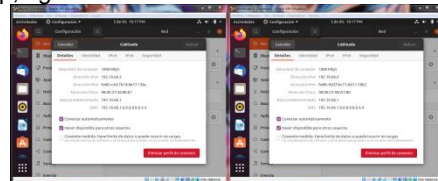


Figura 41. Validación IP Dinámicas en los dos Equipos Ubuntu

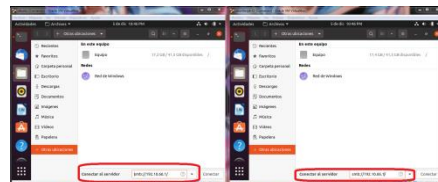


Figura 42. Conexión al Servidor Zentyal con la IP smb://192.10.66.1



Figura 43. Prueba de conexión al directorio Informática con un Usuario Errado.

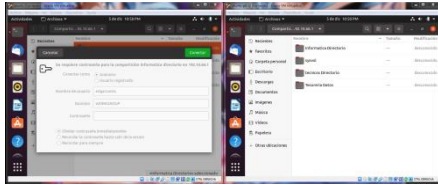


Figura 44. Conexión fallida de la prueba realizada en la Figura 41

prueba de conexión a los directorios informática y tesorería con los usuarios creados en figura 39 y 40

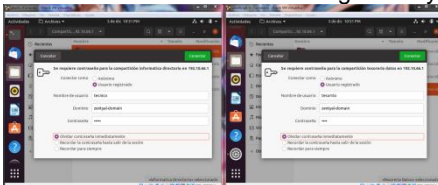


Figura 45. Conexión a los dos directorios Figura. 33,35

conexión a los directorio Informática y tesorería desde los Desktop Ubuntu, figura 46, en la figura 47 se puede observar los directorios cargados en las unidades de Red.

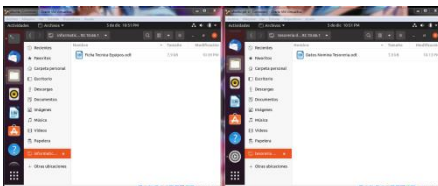


Figura 46. Conexiones Exitosas

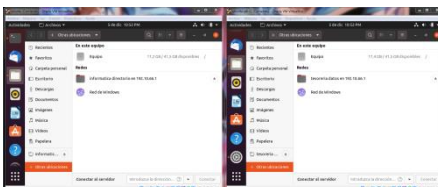


Figura 47. Directorios Cargados en la unidad de Red correspondiente

4 Temática 2: Proxy No Transparente

Al iniciar sesión correctamente, en nuestro dashboard nos aparecerá la siguiente pestaña, la cual le daremos click y posteriormente nos despliega unas opciones; De la cual seleccionaremos la opción que dice "componentes de Zentyal". Posteriormente damos click en la opción que dice "ver modo básico".



Figura 48. ver en modo básico opciones.

Entre las opciones que nos aparecen al realizar el paso anterior, nos aparecen algunas de las siguientes:



Figura 49. escoger la opción indicada http proxy.

Posteriormente escogemos la opción HTTP Proxy y le damos en instalar. Al dar click en instalar nos aparecerá lo siguiente:

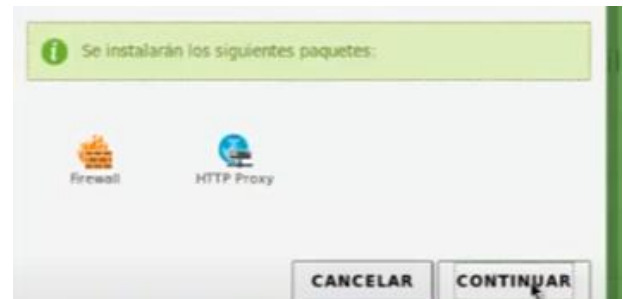


Figura 50. continuar la instalación.

Damos click en continuar para continuar con la configuración. Luego de realizar este paso nos aparecerá una barra de progreso, la cual muestra la instalación de los diferentes componentes que se requieren para nuestra proxy.

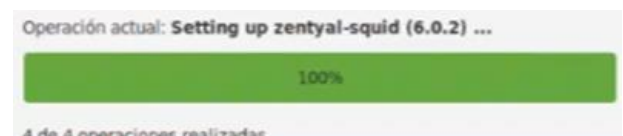


Figura 51. instalación completada.

Terminado el anterior proceso nos dirigimos a la opción que dice estado de los módulos o configuración de módulos.



Figura 52. estado de los módulos.

Hecho esto nos dirigimos a la opción de HTTP Proxy y la activamos dando click en la casilla.

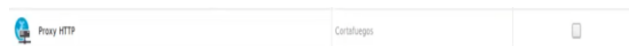


Figura 53. activar proxy.

Al activar nuestro módulo del Proxy, nos aparecerá el módulo ya activado en la parte lateral de nuestra pantalla. Posteriormente damos click en el módulo de proxy y nos aparecerán las siguientes opciones; a la cual le daremos click en configuración general.

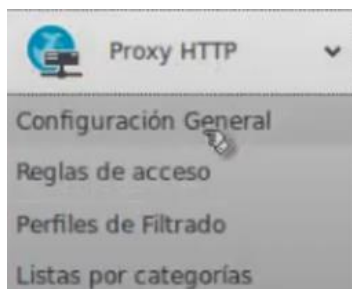


Figura 54. módulo proxy.

En la configuración general cambiamos el puerto y agregamos el puerto 1230, con el cual crearemos las reglas de acceso para controlar ciertas acciones en un determinado intervalo o asimismo restringir el acceso a ciertas páginas de internet al ser detectadas por nuestra proxy configurada.



Figura 55. Perfiles de filtrado.

Debemos crear también un nuevo perfil de filtrado en nuestra configuración de Proxy, la cual restringe y gestionará ciertas navegaciones en nuestro navegador.

Umbral de filtrado de contenido



Figura 56. Umbral de filtrado de contenido.

Configuramos nuestro filtrado de contenido con la opción de "filtrado", esto con el fin de gestionar dichas peticiones o conexiones que se requiera en nuestra red.



Figura 57. Configuración de filtrado de dominio.

En la configuración de filtrado de dominio podemos restringir el acceso, especificando ciertos parámetros como lo son: la URL e incluso la dirección IP de cierto sitio que queremos bloquear o denegar la conexión.

Luego de haber realizado lo siguiente nos dirigimos otra vez a las opciones de HTTP Proxy y seleccionamos la opción de "Reglas de Acceso", en la cual nos aparecen las siguientes opciones.



Figura 58. Reglas de acceso de Proxy.

Configurado los parámetros con las dichas opciones requeridas, podemos guardar los cambios y empezar a

testear nuestra configuración de proxy transparente. Para probar nuestra configuración realizamos la prueba con el navegador de Firefox, luego nos vamos a preferencias y editamos las opciones de nuestro proxy con la creada previamente.

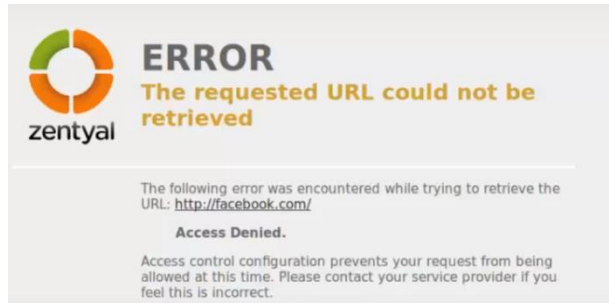


Figura 59. Verificación de rechazo de conexión http..

Si navegas por un sitio con protocolo http y si lo has establecido dentro de tus reglas de proxy, este no cargará y rechazará la conexión entre el servidor.

5 Temática 3: Cortafuegos

Temática 3: Contrafuegos

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.

En este punto vemos que nuestro servidor está funcionando correctamente

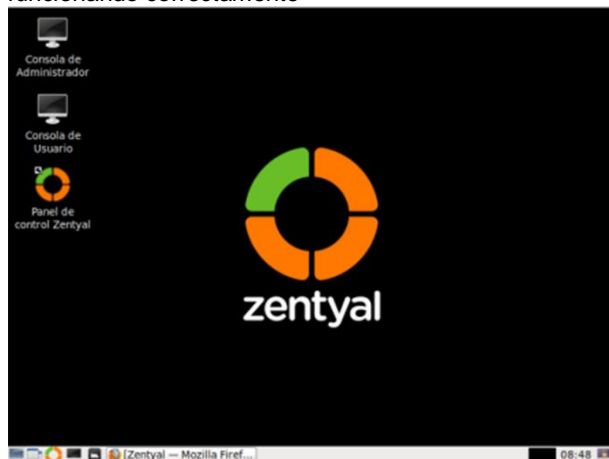


Figura 60. Interfaz principal

Accedemos a nuestro servidor por medio de la ip asignada

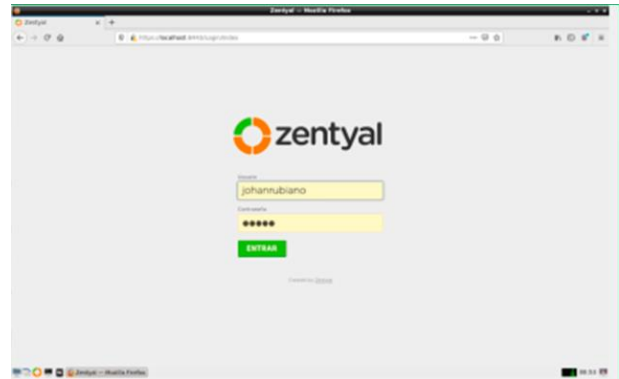


Figura 61. Acceso de usuario

Vemos los servicios que nos muestra nuestro servidor Zentyal y seleccionamos el que queremos instalar, para este caso vamos a instalar el servicio cortafuegos (firewall).

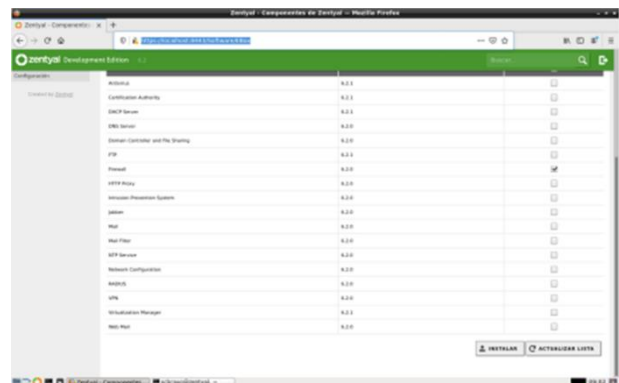


Figura 62. Interfaz del servidor

Verificamos que el proceso de instalación de halla iniciado correctamente.

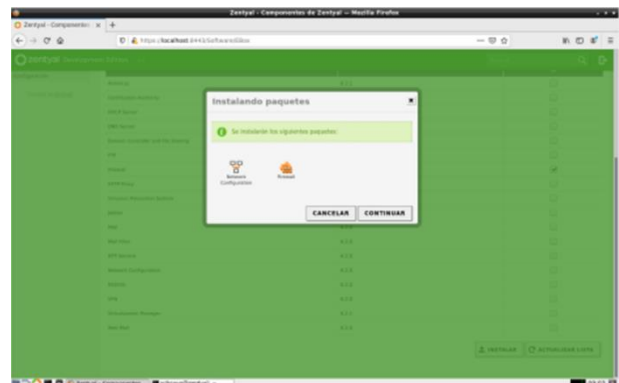


Figura 63. Verificación de instalación

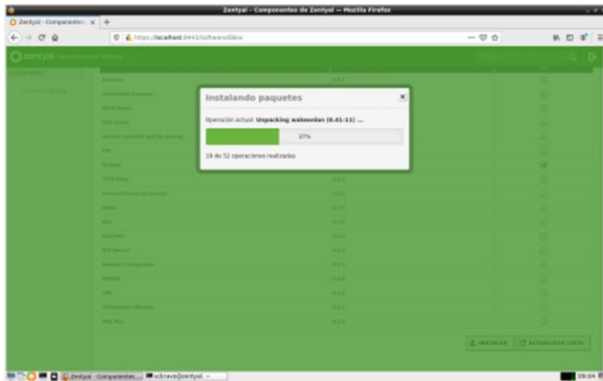


Figura 64. Progreso de instalación

Comprobamos que el proceso haya terminado de forma exitosa

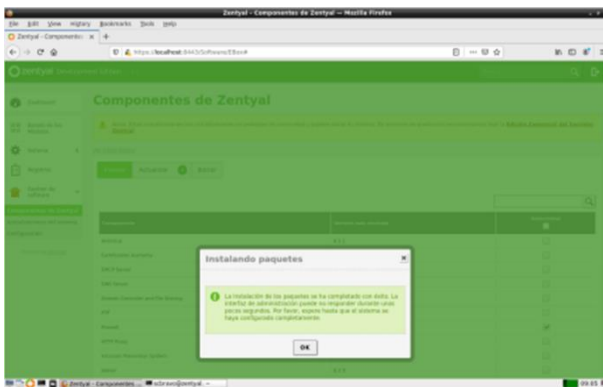


Figura 65. Instalación de paquetes

Estando en nuestra página principal vemos que el servicio firewall se halla instalado.

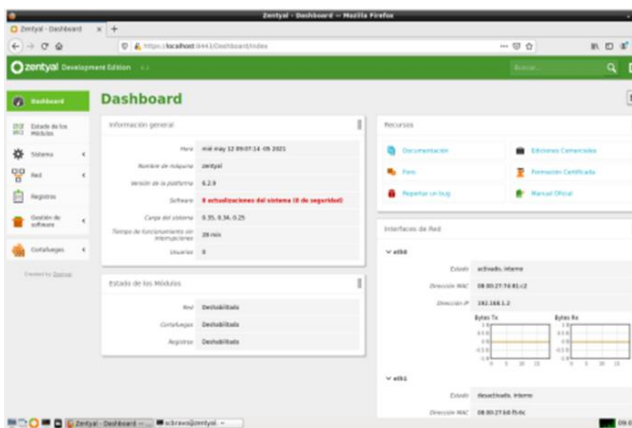


Figura 66. Página principal

En esta página de inicio vemos todos los servicios que nos ofrece nuestro cortafuego



Figura 67. Servicios de Contrafuegos

Para iniciar con la restricción de apertura de sitios o portales Web de entretenimiento y redes sociales, lo primero que hacemos es proteger el acceso a nuestro servidor, deshabilitando el acceso a este servidor desde otros dispositivos. Aquí vemos cómo puedo acceder desde mi computador principal al servidor Zentyal. Pero vamos a configurar la regla para quitar estos permisos de acceso.

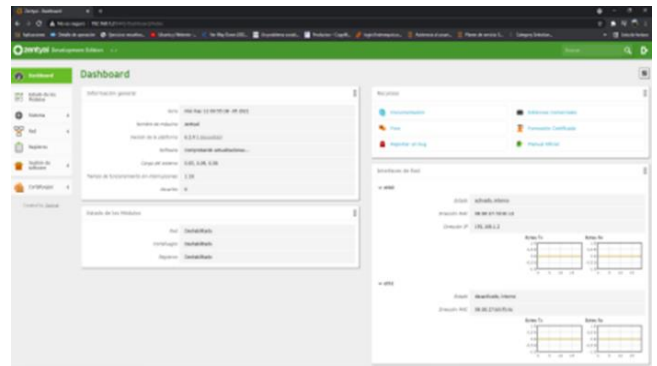


Figura 68. Servidor Zentyal

Ya en este punto vemos que el servicio de acceso a la Administración Web de Zentyal se encuentra deshabilitada.



Figura 69. Administrador web de Zentyal

Figura 73. Módulo de red

En este caso vamos a instalar las Reglas de filtrado para el tráfico saliente de Zentyal, que nos permiten controlar el acceso desde aquí a los servicios externos, a continuación, estamos restringiendo la salida Facebook. Lo primero que hacemos es saber cuál es la ip de las pagina a restringir. En mi caso la ip de Facebook es: 69.171.250.35

```
C:\Users\Usuario>ping www.facebook.com
Haciendo ping a star-mini.c10r.facebook.com [69.171.250.35] con 32 bytes de datos:
Respuesta desde 69.171.250.35: bytes=32 tiempo=27ms TTL=56
Respuesta desde 69.171.250.35: bytes=32 tiempo=27ms TTL=56
Respuesta desde 69.171.250.35: bytes=32 tiempo=27ms TTL=56
Respuesta desde 69.171.250.35: bytes=32 tiempo=27ms TTL=56

Estadísticas de ping para 69.171.250.35:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 27ms, Máximo = 27ms, Media = 27ms

C:\Users\Usuario>
```

Figura 70. Restringir Facebook IP

Posteriormente con la IP de Instagram: 69.171.250.174, como vemos está dentro del mismo segmento de ip's de Facebook, entonces lo que queremos es utilizar todo el nodo para no ingresar ip's individuales.

```
C:\Users\Usuario>ping www.instagram.com
Haciendo ping a z-p42-instagram.c10r.facebook.com [69.171.250.174] con 32 bytes de datos:
Respuesta desde 69.171.250.174: bytes=32 tiempo=29ms TTL=56
Respuesta desde 69.171.250.174: bytes=32 tiempo=30ms TTL=56
Respuesta desde 69.171.250.174: bytes=32 tiempo=28ms TTL=56
Respuesta desde 69.171.250.174: bytes=32 tiempo=28ms TTL=56

Estadísticas de ping para 69.171.250.174:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 28ms, Máximo = 30ms, Media = 28ms

C:\Users\Usuario>
```

Figura 71. Restringir instagram IP

Ahora nos dirigimos a la Ip de YouTube: 142.250.78.78

```
C:\Users\Usuario>ping www.youtube.com
Haciendo ping a youtube-ui.l.google.com [142.250.78.78] con 32 bytes de datos:
Respuesta desde 142.250.78.78: bytes=32 tiempo=73ms TTL=109
Respuesta desde 142.250.78.78: bytes=32 tiempo=70ms TTL=109
Respuesta desde 142.250.78.78: bytes=32 tiempo=72ms TTL=109
Respuesta desde 142.250.78.78: bytes=32 tiempo=71ms TTL=109

Estadísticas de ping para 142.250.78.78:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 70ms, Máximo = 73ms, Media = 71ms

C:\Users\Usuario>
```

Figura 72. Restringir Youtube IP

Una vez se tenga esta información lo que procedemos a hacer es lo siguiente: nos dirigimos al módulo de RED.



Luego damos click en objetos: y añadimos un nuevo objeto, este nos va a permitir crear una lista de direcciones, las cuales vamos a agregar en nuestro firewall para las respectivas restricciones.

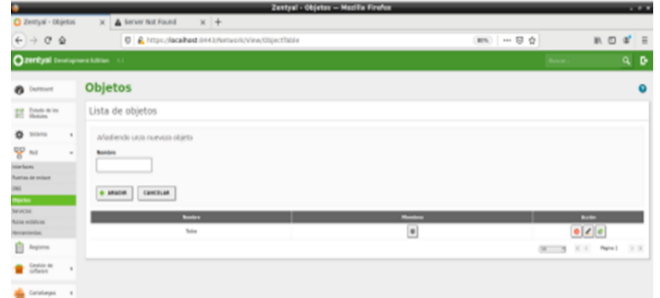


Figura 74. Creación del Firewall

Configuramos el rango de direcciones de Facebook, Youtube e Instagram que queremos restringir



Figura 75. Rango de direcciones de Facebook



Figura 76. Rango de direcciones de Youtube



Figura 77. Rango de direcciones de Instagram

Ahora agregamos las reglas de filtrado para las redes internas.



Figura 78. Reglas de filtrado

Agregamos las reglas de acceso para cada una de las redes sociales.

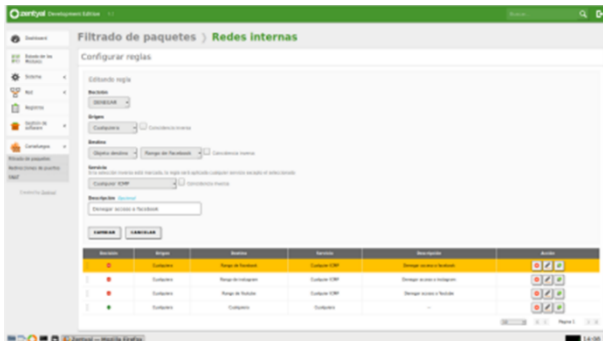


Figura 79. Denegando acceso a Facebook

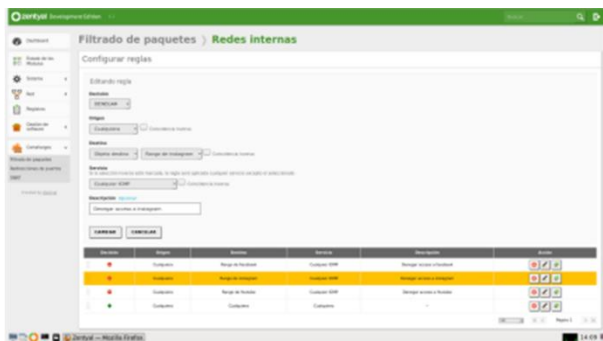


Figura 80. Denegando acceso a Instagram



Figura 81. Denegando acceso a Youtube

6 Temática 4: File Server y Print Server

Implementación y configuración detallada de la creación de un File Server y Print Server el cual permite la compartición de directorios e impresoras en red.

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

6.1 File Server

-Verifico que el controlador de dominio y compartición de ficheros esté instalado.

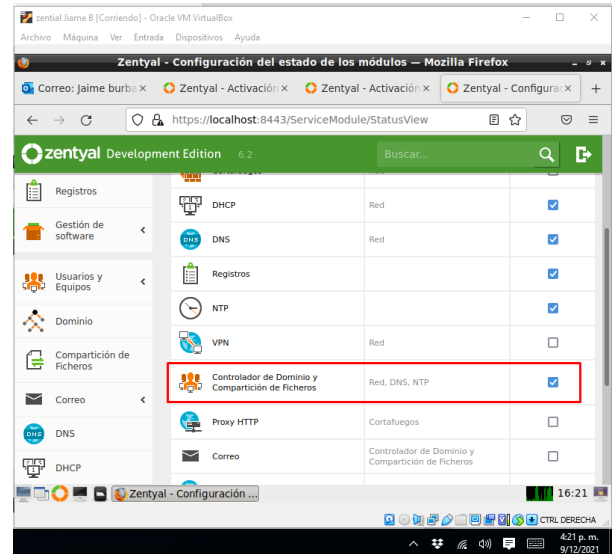


Figura 82. Verificación del módulo

-Ingreso al módulo Compartición de ficheros, para agregar un nuevo directorio compartido.

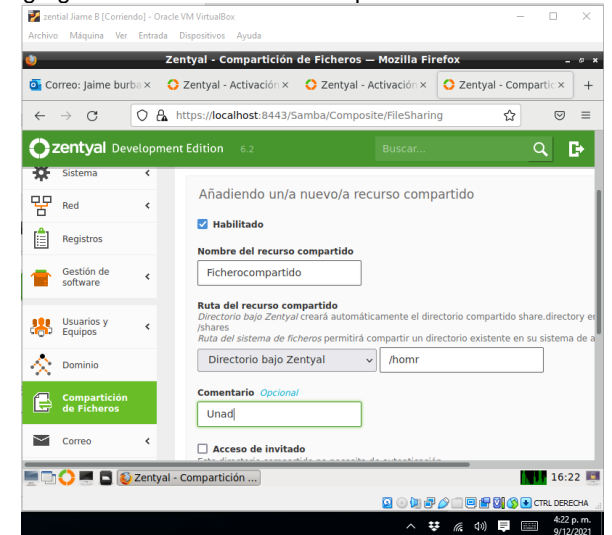


Figura 83. Agregar fichero compartido

-Creación de un usuario que tendrá acceso al dominio y permisos de lectura y escritura sobre el directorio creado.

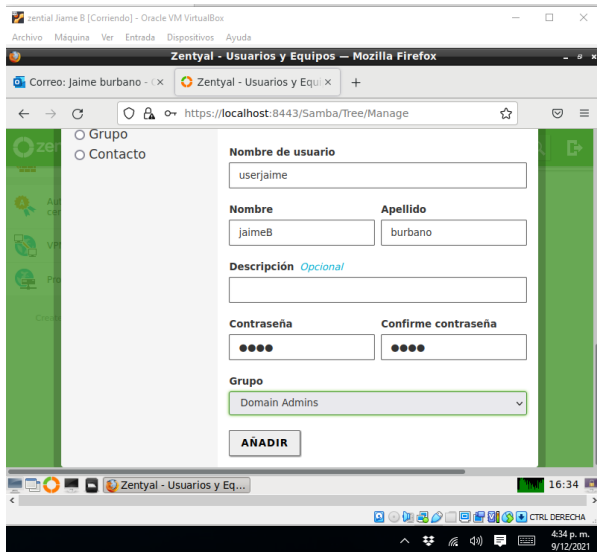


Figura 84. Creación de usuario

-Asignación de una ACL al fichero compartido, es decir, los permisos, para ello ingresamos a la configuración del directorio y damos clic en añadir.

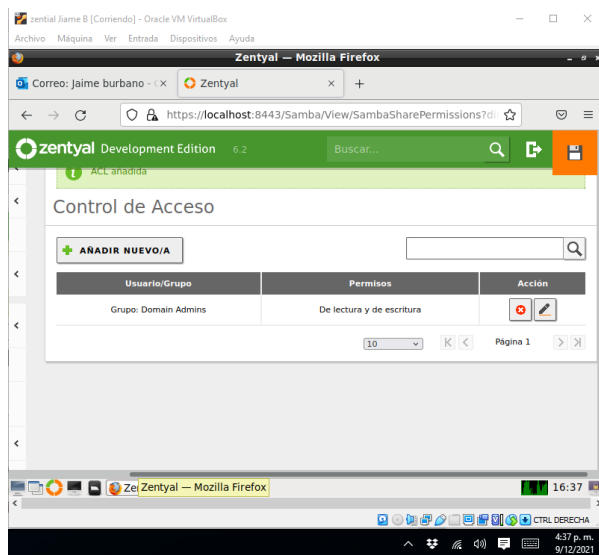


Figura 85. Control de acceso ACL

-Ahora nos dirigimos a la máquina virtual cliente, en este caso Ubuntu Desktop 20.04 para realizar la conexión, para ello instalamos samba cliente y se realiza la configuración necesaria del dominio, luego se abre el gestor de archivo, damos clic en otras ubicaciones y en la parte inferior digitamos en la casilla conexión smb://192.168.18.36 (ip del servidor) y damos clic en Conectar.

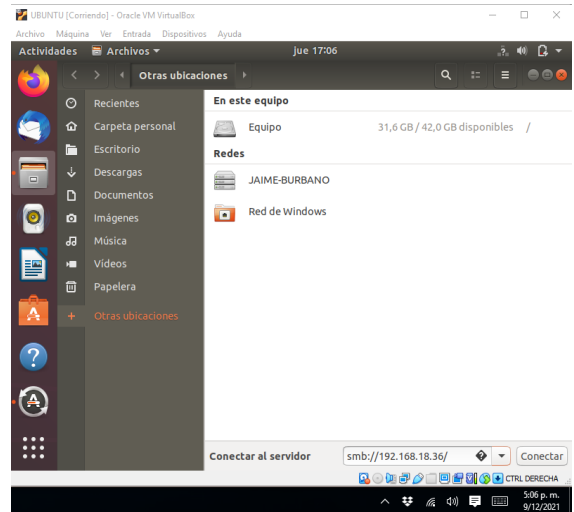


Figura 86. Conexión al servidor

-Podemos visualizar los directorios creados en el servidor.

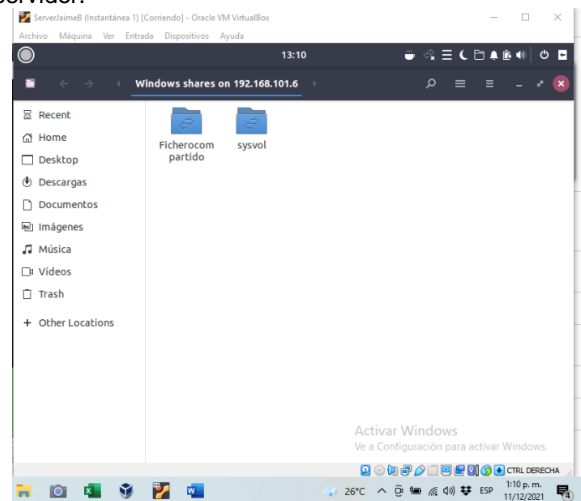


Figura 87. Vista del directorio compartido.

6.2 Print Server

-Se realiza la instalación del paquete cups-PDF en la consola de administrador en Zentyal

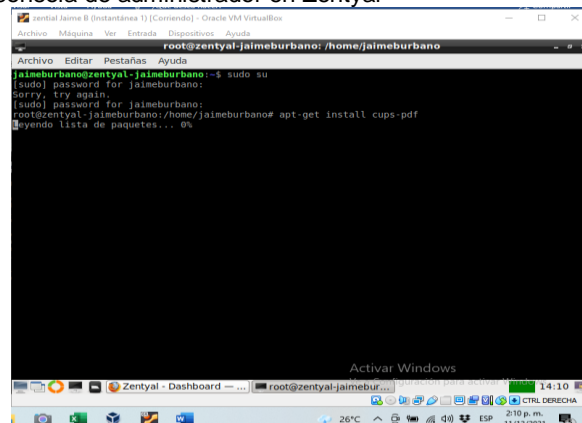


Figura 88. Instalación de Cups-PDF

-Se abre en el navegador el servidor con la dirección <https://localhost:631>, y se agrega una impresora dando clic en Administración y luego en Add Printer.

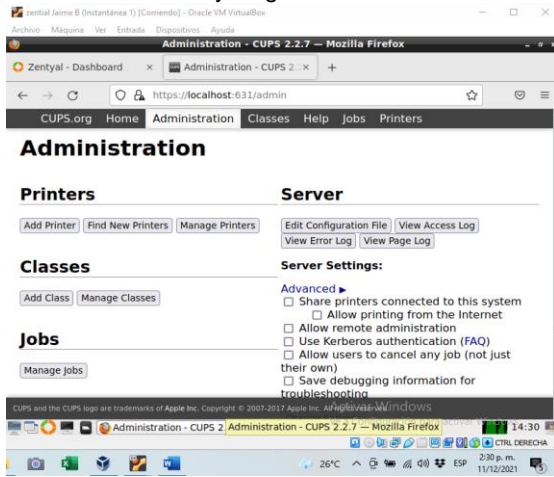


Figura 89. Ingreso a CUPS-PDF

-Seguimos las instrucciones del asistente, en este caso podemos elegir la red a la cual configuramos la impresora.

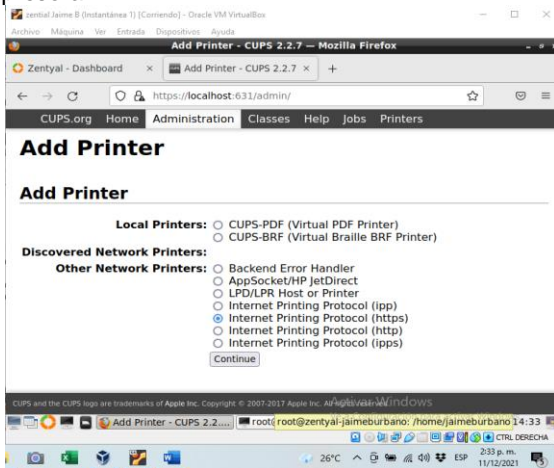


Figura 90. Agregar impresora

-Elegimos una dirección con la cual se va a realizar la conexión

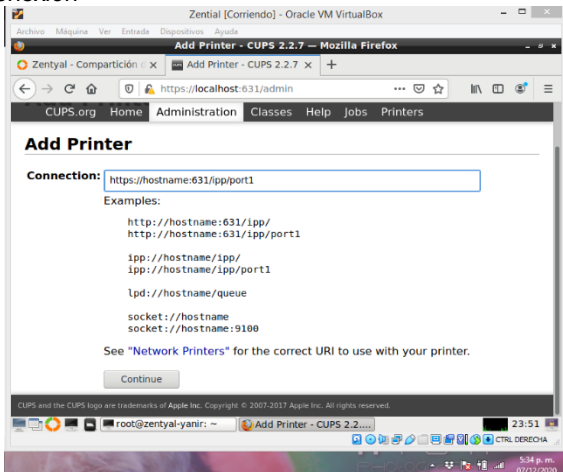


Figura 91. Conexión

-Se digita el nombre de la impresora, se selecciona Share This Printer, también elegimos modelo y marca, luego damos clic en continuar

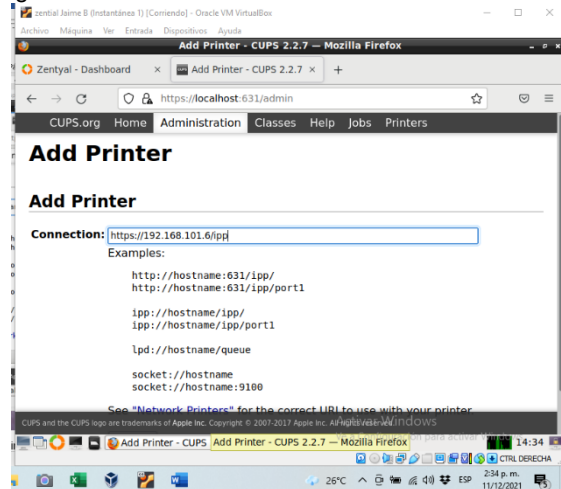


Figura 92. Nombre de la impresora
-También ingresamos al archivo `smb.conf` para editar los permisos de la impresora.

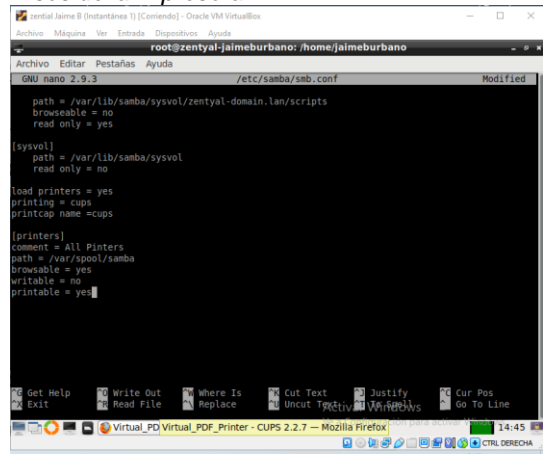


Figura 93. Configuración de impresora con samba

-Ahora ingresamos al cliente, después de la instalación de cups, realizamos la conexión de la impresora, colocando la dirección de conexión.

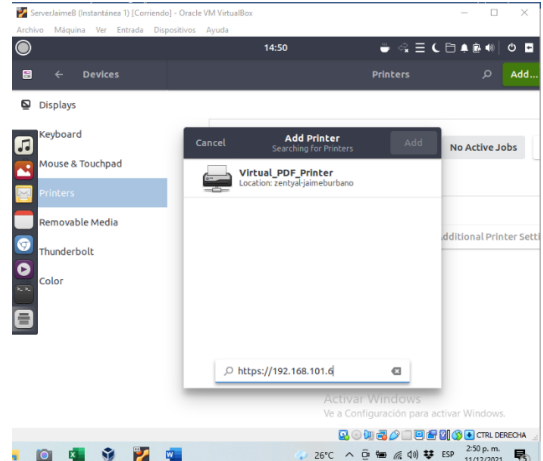


Figura 94. Conexión a la impresora del servidor.

-Enviamos una impresión de prueba.

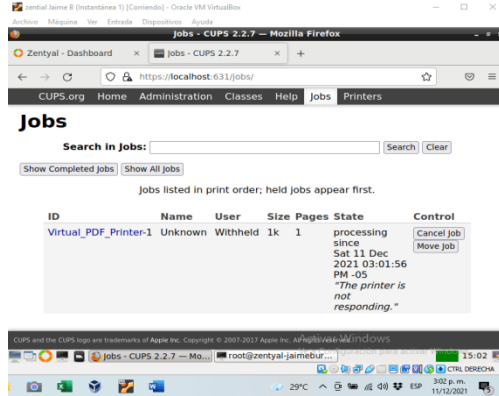


Figura 95. Impresión de prueba.

7 Temática 5: VPN

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux.

Uno de los primeros pasos para implementar una VPN en Zentyal es habilitar los módulos necesarios, tales como Firewall, autoridad de certificación y la VPN.

Posteriormente se realiza el proceso de instalación y se deja todo a punto para iniciar con el proceso.

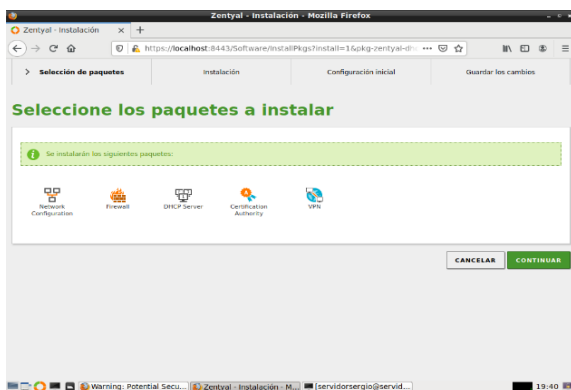


Figura 96. selección de módulos

Es necesario configurar las interfaces de red y para recibir el tráfico de internet que se denominaría como externa, y otra como interna o las que sean necesarias.



Figura 97. tipos de interfaces de red

Después de configurar estos temas generales que competen a todas las temáticas se procede a generar el certificado de autoridad para el Zentyal, en primera medida se emite uno para el funcionamiento del software como tal, y luego se puede emitir para las necesidades del proyecto.

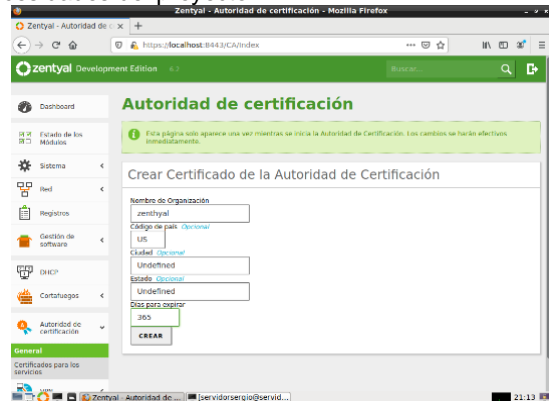


Figura 98. autoridad de certificación

Luego se genera los certificados para la VPN, aunque es de anotar que se crean también de manera automática, cuando se genera un nuevo servidor VPN.

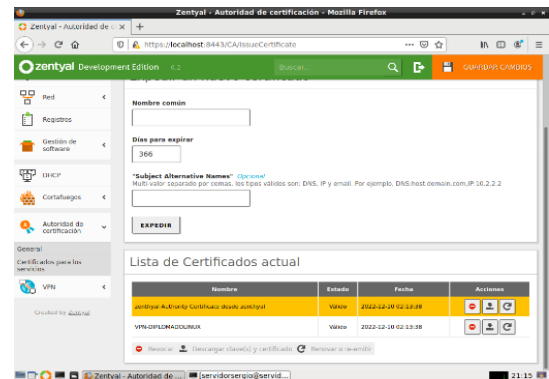


Figura 99. certificados emitidos por la autoridad

Para continuar con el proceso se debe ir al apartado VPN en su ítem servidores y elegir un nombre, de ahí ya se genera la VPN para configurar.

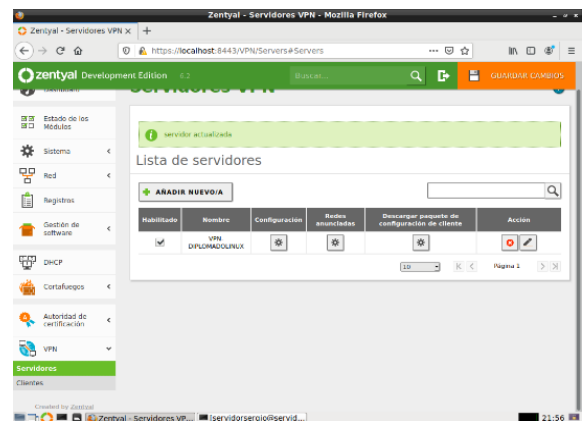


Figura 100. VPN generada para configurar

Se configura la VPN, poniendo el puerto que se va a escuchar, en este caso el 1194, el segmento de IP que va a asignar la VPN, se utiliza el certificado emitido, además el ítem que activa o desactiva la opción de túnel.

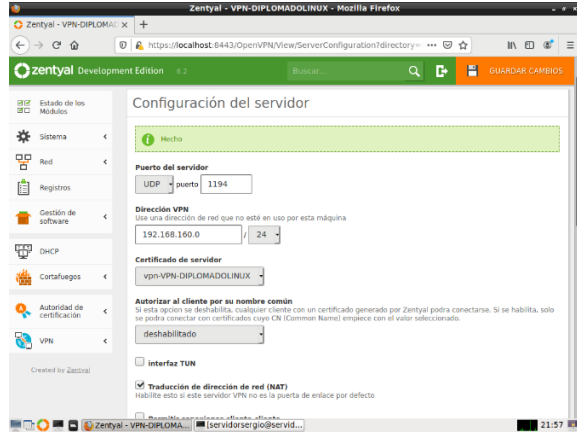


Figura 101. configuración de VPN

Después de configurar a conveniencia del lo que se necesite en el proyecto, se descarga el paquete de configuración de cliente. Muy necesario para conectarse.

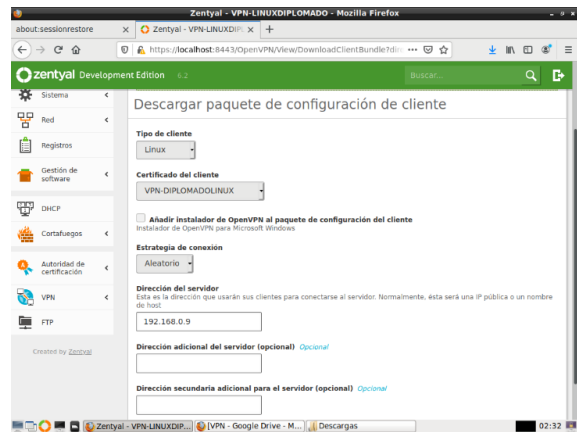


Figura 102. descarga de configuración para cliente

Se puede conectar open VPN en Ubuntu desktop a través de networkmanager, y aparece la conexión en el ítem de red del GNOME.

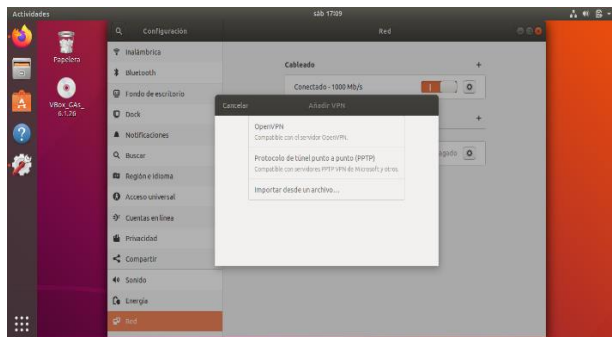


Figura 103. VPN en interfaz gráfica Ubuntu

Para conectar solo se ingresa al ítem de openvpn y se anexan todas las credenciales emitidas por el servidor. cabe anotar que se puede pasar esta información en varios medios desde físico o por SSH, en este caso se pasó a través de Google drive.

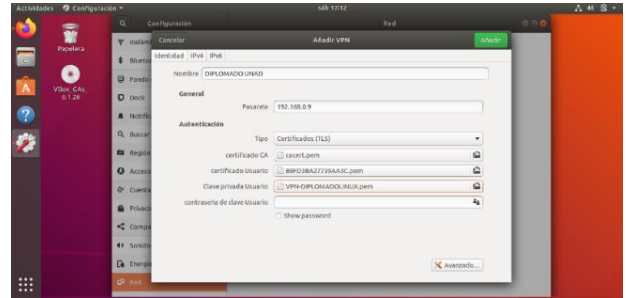


Figura 104. anexar certificados y llaves de la VPN

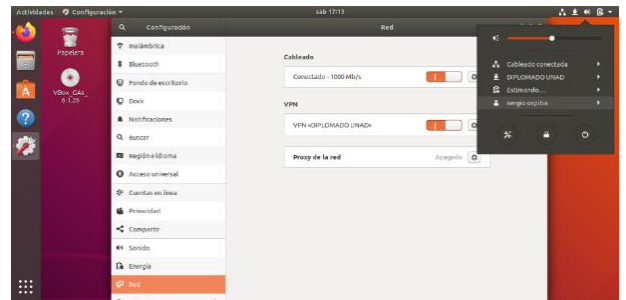
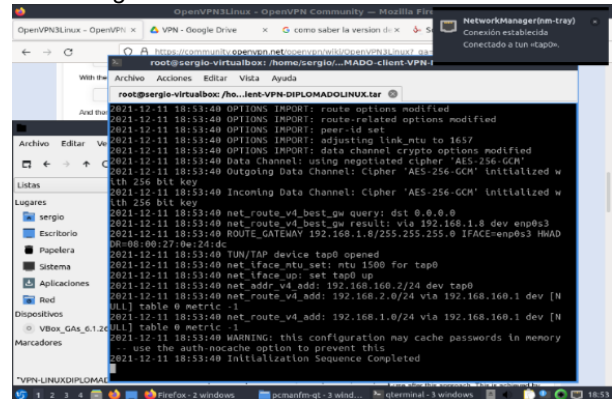


Figura 105. se evidencia conexión

Se procede a conectar otro usuario de la red VPN a través de terminal instalando openvpn y con su comando openvpn – config, y se enlaza el archivo de configuración emitido por la autoridad del Zentyal.

Figura 106 conexión a través de terminal



Por último, se realizan las pruebas de conexión de los usuarios, se comparte una carpeta y se conecta desde un usuario Lubuntu a un usuario desktop los dos en diferentes segmentos de red pero unidos a través de VPN.

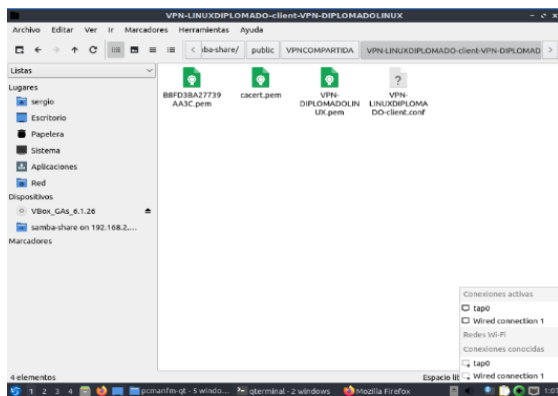


Figura 107 conexión a carpeta compartida con samba

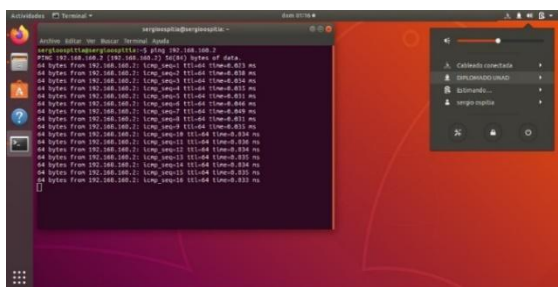


Figura 108 evidencia de conexión a VPN

Teniendo un canal seguro de comunicación, se puede realizar cosas muy interesantes, tales como un acceder desde diversos lugares a un recurso de red, sin necesariamente compartir la red. es importante recalcar que esta herramienta es una excelente medida de protección para una organización.

8 CONCLUSIONES

Durante el Desarrollo de esta Guía Final Paso 8, nos permitió poner en práctica los conocimientos adquiridos en los pasos anteriores 1,2,3,4,5,6,7. Implementando el Servidor Zentyal 6.2.

Instalamos los paquetes DHCP Server, DNS Server y Controlador de Dominio.

ya con el Sistema Operativos y los paquetes instalado, ingresamos a la interface Web del Zentyal, una herramienta muy cómoda para configurar los diferentes servicios instalados y configuración de Red LAN y WAN.

En el último paso de esta actividad realizamos pruebas con los Directorios Compartidos cuando realizamos la configuración del dominio, los dos maquinas Virtuales de Ubuntu se conectar a la red LAN del servidor, la asignación de IP y DNS será por DHCP, las pruebas de conexión a los Directorios fueron todo un éxito.

Durante el desarrollo de esta actividad final puedo mencionarles que esta me enseñó que Zentyal es un servidor muy sencillo de administrar, intuitivo y con una interfaz gráfica amigable con el usuario, ya que está basado en Ubuntu. Por otro lado, puedo indicarles que gracias a ello se facilita implementar la gestión y administración de los servicios esenciales para una

empresa, en donde podemos encontrar: 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, entre otros.

Podemos determinar que es de gran utilidad configurar un proxy transparente, ya que nos proporciona opciones para gestionar nuestras conexiones a dichos sitios, los cuales pueden ser a veces perjudiciales para nosotros. Un ejemplo es que si tal vez tenemos a nuestro hijo en la computadora y queremos que no acceda a ciertos sitios, pues gracias a nuestra configuración de proxy en Zentyal podemos hacerlo y pienso que eso es de gran utilidad; Otro caso sería su uso en una empresa, tal vez no quieres que tus empleados accedan a ciertos sitios mientras trabajan. Entonces la manera de proteger nuestra privacidad y sentirnos seguros mientras navegamos en la web es configurando un proxy y así protegernos para aumentar nuestra productividad laboralmente.

File server y Print server, abordan gran importancia con respecto a las redes, en la actualidad la compartición de archivos e impresoras en las grandes compañías, facilitan el trabajo y la organización, así mismo tendremos gran incidencia en la seguridad de la información, por ello es importante las restricciones y control de acceso de los usuarios.

Una red VPN implementada en Zentyal, es una herramienta que tiene mucho valor para la seguridad y el compartir recursos, tanto dentro como fuera de la red, esto implementado en ambientes de producción permite la intercomunicación entre estaciones que no necesariamente estén conectadas de manera física, esto es una ventaja para las organizaciones.

9 REFERENCIAS

- [1] Documentación de Zentyal 6.2. (2004-2018). Zentyal 6.2 Documentación Oficial. <https://doc.zentyal.org/6.2/es/>
- [2] Documentación de Zentyal 6.2. (2004-2018). Instalación. <https://doc.zentyal.org/6.2/es/installation.html#el-instalador-de-zentyal>
- [3] Documentación de Zentyal 6.2. (2004-2018). Configuración <https://doc.zentyal.org/6.2/es/installation.html#configuracion-inicial>
- [4] Documentación de Zentyal 6.2. (2004-2018). Servicio de configuración de red (DHCP). <https://doc.zentyal.org/6.2/es/dhcp.html>
- [5] Documentación de Zentyal 6.2. (2004-2018). Servicio de resolución de nombres de dominio (DNS). <https://doc.zentyal.org/6.2/es/dns.html>
- [6] Documentación de Zentyal 6.2. (2004-2018). Controlador de Dominio y Compartición de ficheros. <https://doc.zentyal.org/6.2/es/directory.html>
- [7] Virtual private network (VPN) service with OpenVPN — Zentyal 7.0 Documentation. (2021). [vpn. https://doc.zentyal.org/en/vpn.html](https://doc.zentyal.org/en/vpn.html)
- [8] Install OpenVPN GUI on Windows. (s. f.). OVPN.Com. <https://www.ovpn.com/en/guides/windows-openvpn-gui>
- [9] Zentyal Server 6.2 Development Now Available. (s. f.). Zentyal Linux Server. <https://zentyal.com/news/zentyal-6-2-announcement/>