

INSTALACIÓN Y CONFIGURACIÓN DE UN ESQUEMA SERVER-CLIENTE A TRAVÉS DE ZENTYAL SERVER COMO DISTRIBUCIÓN BASE PARA LA INTEGRACIÓN DE SERVICIOS WEB.

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI. Colombia.

Mayo de 2021

Diego Fernando Crespo Diaz
e-mail: diegofcrespo@gmail.com
Juan David Vásquez Godoy
e-mail: diegofcrespo@gmail.com
Sebastian Stivenn Pérez Sánchez
e-mail: ssperezsa@unadvirtual.edu.co
Andrés Ricardo Bolívar González
e-mail: arbolivarg@unadvirtual.edu.co
Diana Patricia Peñarete Mosquera
e-mail: dppenaretem@unadvirtual.edu.co

RESUMEN: *Implementar servicios de red por medio de sistema operativo Zentyal Server 6.2 usando sistemas virtualizados tanto para el equipo servidor como para los equipos clientes, se demostrara el uso de los servicios: DHCP, DNS, controlador de dominio, Proxy no transparente, cortafuegos, File server, Print server y VPN; con el fin de demostrar como estas soluciones pueden ser desplegadas haciendo uso de herramientas basadas solamente en software libre, lo cual para entornos empresariales es una ventaja en términos del costo de licenciamiento, de facilidad de implementación y gestión, sin detrimento de la calidad de los servicios.*

PALABRAS CLAVE: Servidor, Proxy, Cortafuegos, DHCP, DNS y VPN.

1 INTRODUCCIÓN

El presente documento tiene como objetivo demostrar la instalación, configuración, gestión de los diferentes servicios de red propuestos mediante diferentes temáticas; estos aspectos a desarrollar son fundamentales para cualquier organización empresarial y su implementación mediante software libre permite presentarla como una alternativa cuando se evalué el desarrollo de infraestructuras de T.I.

Se hará uso del sistema operativo de servidor Zentyal Server en su versión 6.2 y clientes implementando Ubuntu 18.4, funcionando en un ambiente virtualizado.

2 INSTALACIÓN DE ZENTYAL SERVER

Luego de realizada la descarga de la imagen del producto desde la página de la distribución, se procede a la creación de la máquina virtual, esta tiene como característica más relevante, que poseerá mínimo dos interfaces de red, para la red interna (clientes, LAN) y otra para la red externa (conexión a Internet, WAN).

2.1 INSTALACIÓN SERVIDOR

Luego se indicará la ubicación del instalador y se inicia la máquina virtual, se selecciona el idioma para iniciar el proceso de instalación del servidor.

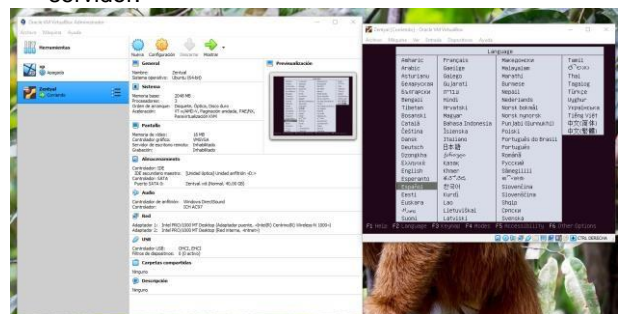


Figura 1. Selección de idioma

A continuación, se indica el idioma del teclado para luego indicar, la tarjeta de red principal (necesaria para descargar algunos componentes).

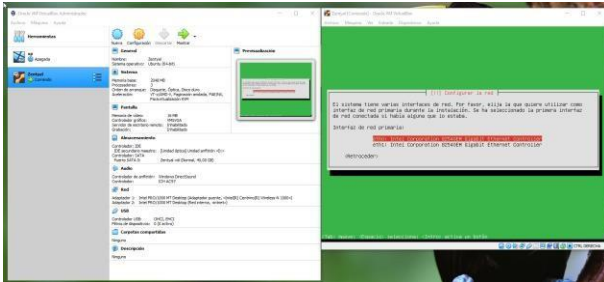


Figura 2. Selección tarjeta de red principal

Los siguientes pasos son: indicar el nombre de la máquina, nombre del usuario, zona horaria. Luego se realiza el particionamiento del disco.

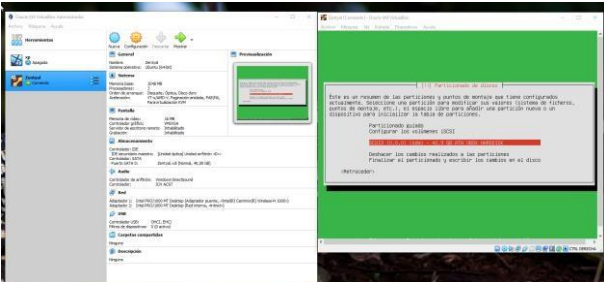


Figura 3. Particionamiento del disco

Seguido se realiza la instalación del sistema operativo en el disco y se indica si se desea incluir una interfaz gráfica, luego se solicitará reiniciar el equipo para terminar la instalación.

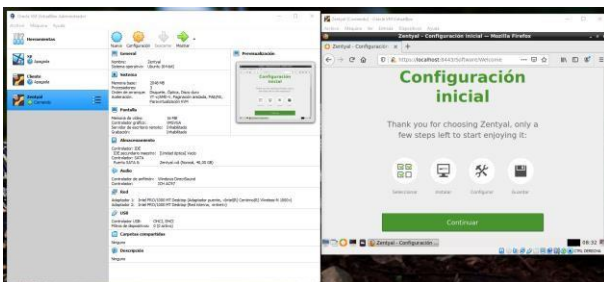


Figura 4. Sistema operativo instalado

2.2 CONFIGURACIÓN INICIAL

A continuación, se realiza la configuración inicial en la cual se seleccionan los roles (paquetes) a instalar, se configuran las interfaces de red y se indica el nombre de dominio para el servidor.



Figura 5. Configuración inicial

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

En caso de no haberse instalado previamente los servicios necesarios, se ingresa a: “Gestión de software” para instalar: DHCP, DNS y Dominio.

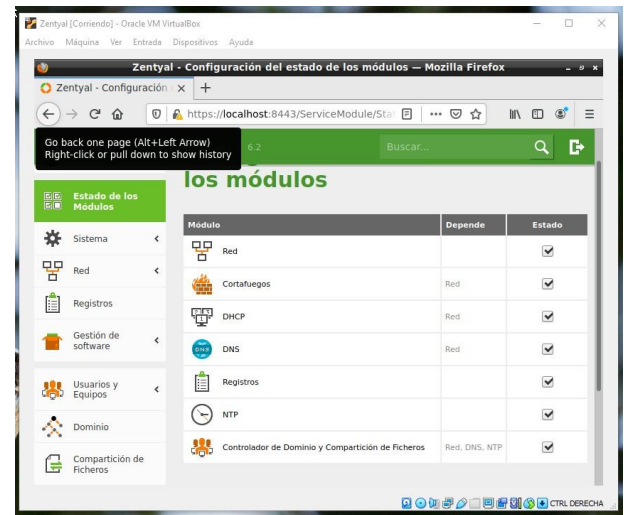


Figura 6. Servicios DHCP, DNS y Dominio

En “Estado de los módulos”, se debe verificar que estos se encuentren habilitados.

3.1 SERVIDOR DHCP

Se ingresa al módulo correspondiente y se selecciona la interfaz interna, encargada de proveer los servicios a los equipos clientes, para este caso asignar las direcciones IP y configurar las direcciones necesarias para suministrar los servicios de red (mascara de red, puerta de enlace y DNS).

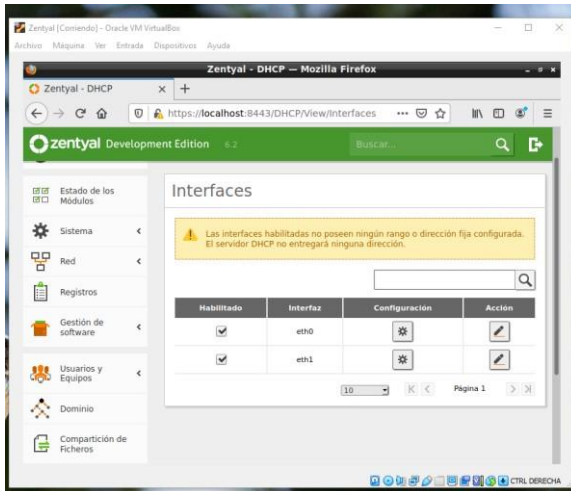


Figura 7. Selección de interfaz interna

A continuación, se ingresa la información de la puerta de enlace y de DNS que se configurara en los clientes.

Luego se ingresa un nombre para el rango de direcciones y se registra los valores de este rango.

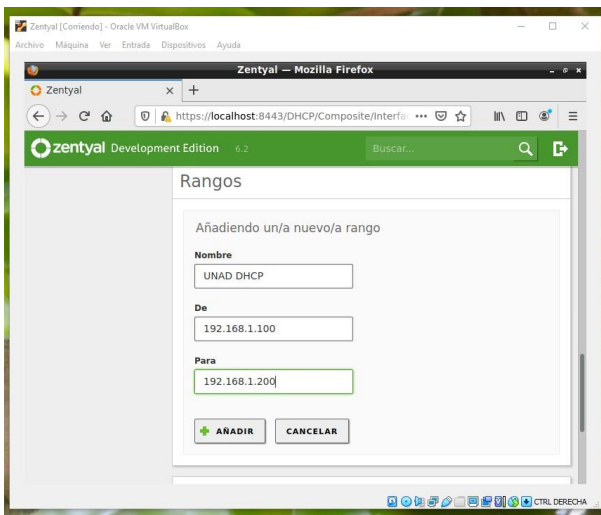


Figura 8. Configuración de rango de direcciones IP

Se verifica en el equipo cliente que las direcciones han sido configuradas de forma automática.

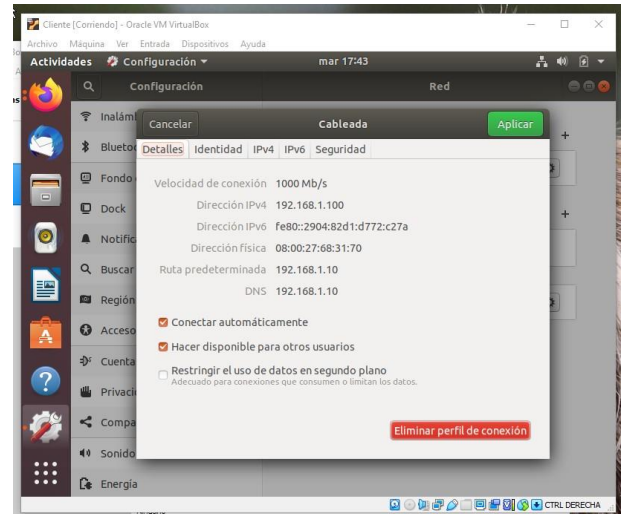


Figura 9. Asignación IP en equipo cliente

3.2 SERVIDOR DNS

En la configuración inicial previamente se configuro la información DNS, en el módulo correspondiente se puede verificar o editar dicha información.

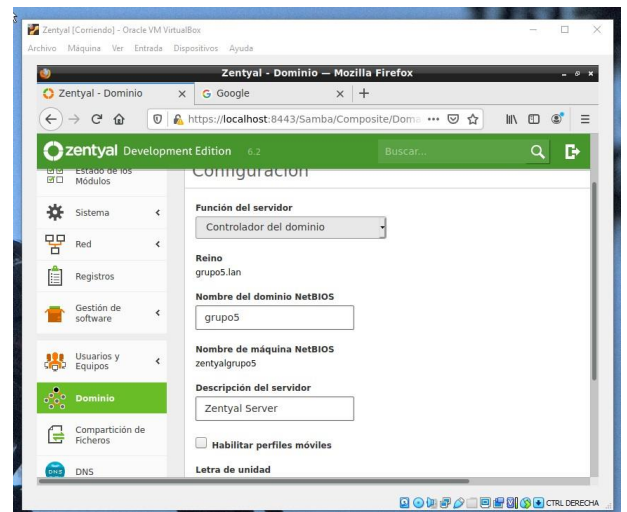


Figura 10. Módulo DNS

En el equipo cliente se puede verificar, haciendo un Ping a la dirección DNS.

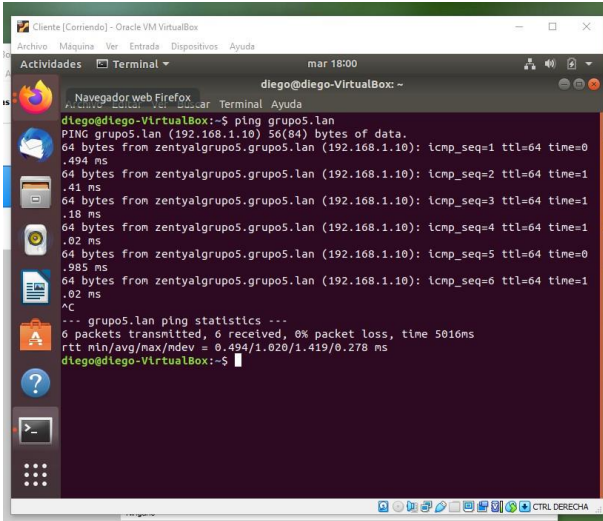


Figura 11. Prueba ping a dirección DNS

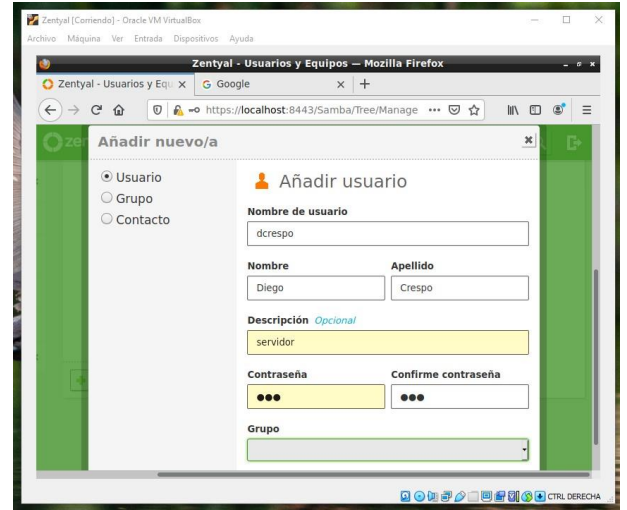


Figura 13. Registro usuario dominio

También se puede verificar la navegación en el cliente.

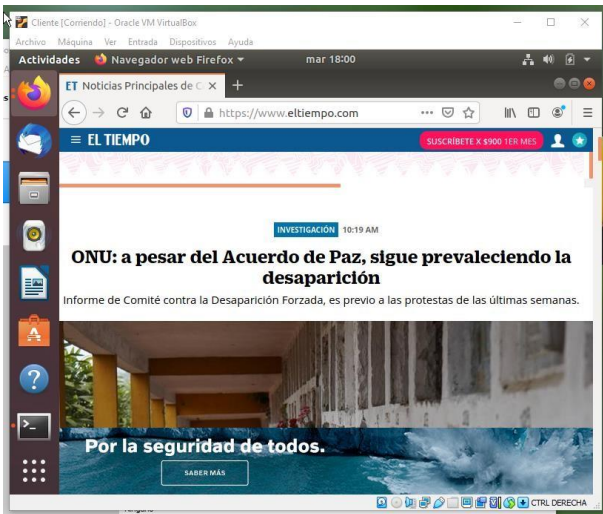


Figura 12. Prueba navegación en cliente

En el equipo cliente se debe instalar el paquete pbisopen previamente para poder realizar la unión al dominio mediante la instrucción.

```

/opt/pbis/bin/domainjoin-cli join --disable ssh [dominio]
[usuario]
  
```

Se verifica en el servidor para encontrar el equipo registrado correctamente.

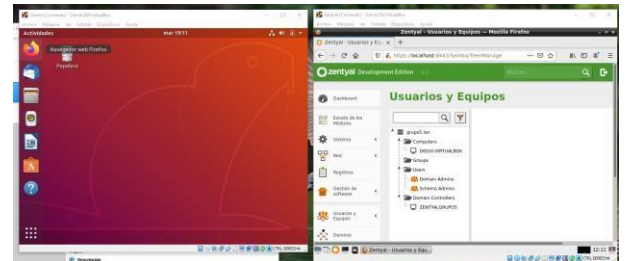


Figura 14. Registro equipo en árbol de dominio

3.3 CONTROLADOR DE DOMINIO

A continuación, se ingresa a "Usuarios y grupos", para configurar el usuario de dominio.

Al iniciar sesión en el cliente, por medio de la consola se puede observar el nombre de usuario y de dominio.

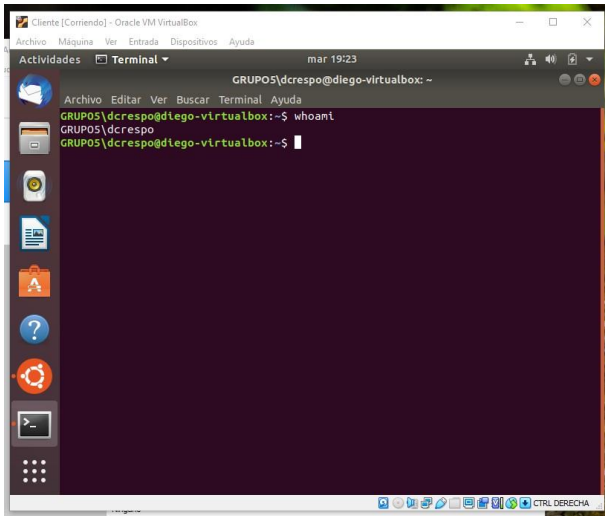


Figura 15. Prueba inicio sesión dominio

4 TEMÁTICA 2: PROXY NO TRANSPARENTE.

Se realiza la instalación y configuración de un servidor proxy no transparente en Zentyal que se validará a través de un Ubuntu desktop que actuará como cliente. Como primera acción cuando se instala nuestro Zentyal Server, verificamos que haya quedado instalado correctamente todos sus paquetes:

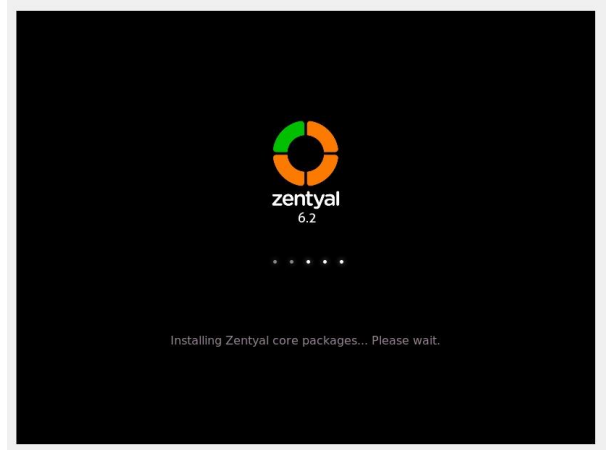


Figura 16. Instalación de paquetes

Ingresamos a la configuración de host local después de la instalación y ejecutamos la instalación del componente de Zentyal Proxy HTTP:

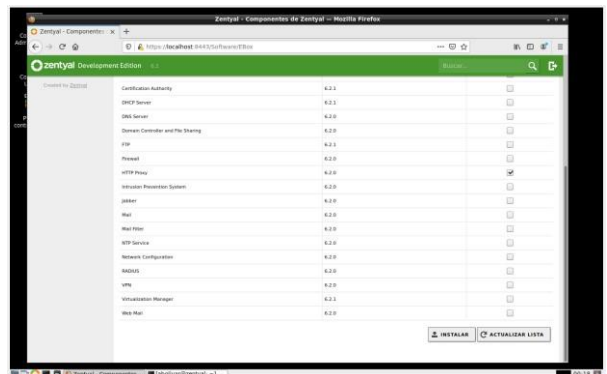


Figura 17. Instalación componente Proxy HTTP

Se inicia la instalación y deben quedar instalados los componentes seleccionados y se evidencia sin errores la totalidad de la instalación:

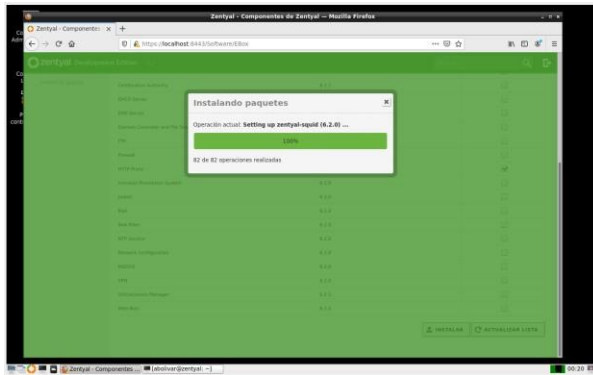


Figura 18. Instalación completa Proxy HTTP

En la Configuración General actualizamos los datos relacionados a si el proxy es transparente o no transparente, tamaño de los ficheros en caché, puerto, etc... Cambiamos el puerto al 1230 según se solicita en la guía de actividades:

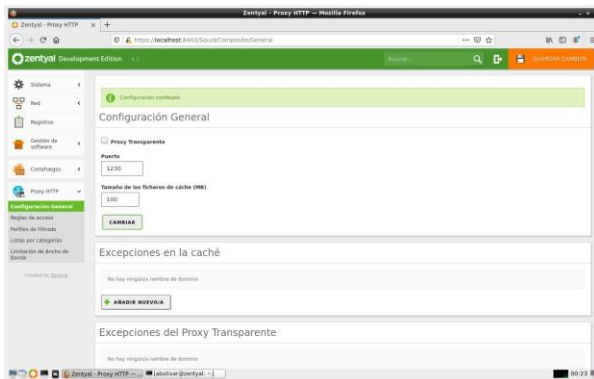


Figura 19. Configuración puerto Proxy

En seguida configuramos los perfiles de filtrado: esto es para permitir o denegar el acceso con base en su contenido:

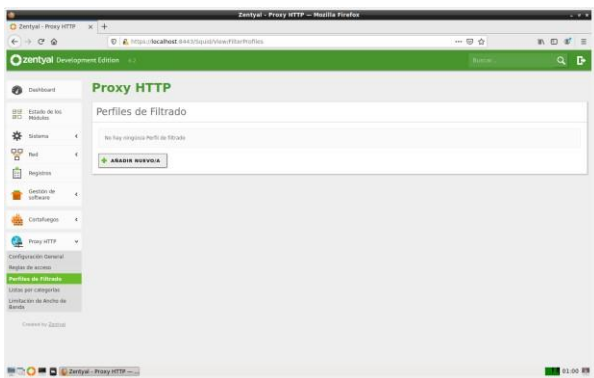


Figura 20. Configuración Perfiles de filtrado

Añadimos el perfil de filtrado y lo creamos: En este caso lo llamamos UNAD_Paso_8:

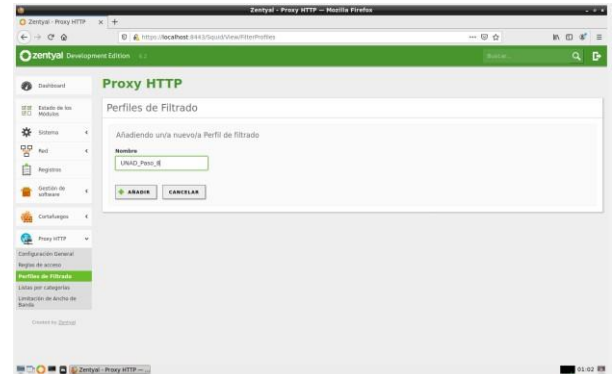


Figura 21. Nombre Perfiles de filtrado

Una vez creado el perfil de filtrado, procedemos a configurarlo tal como lo muestra la siguiente imagen: agregamos a las reglas de dominio y URLs las páginas que queremos bloquear una vez estemos apuntando al proxy, por esto es un proxy no transparente:



Figura 22. Reglas de dominio y URLs

Una vez configuradas las reglas de dominio y las URLs restringidas iremos a nuestro cliente y configuramos el navegador para que las peticiones a internet las haga a través de nuestro servidor proxy configurado:

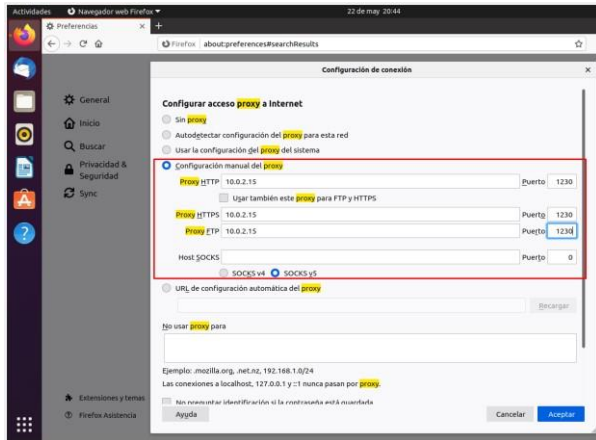


Figura 23. Configuración Proxy cliente

Y validamos la conexión a las páginas bloqueadas desde el proxy:

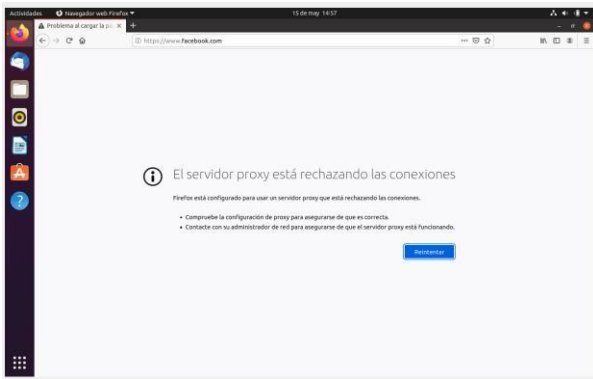


Figura 24. Validación página cliente.

Otra alternativa para realizar la configuración de control de acceso es denegando el tráfico de los servicios de conectividad, así, agregamos un objeto en las configuraciones de red, para este caso el objeto se llama UNAD:

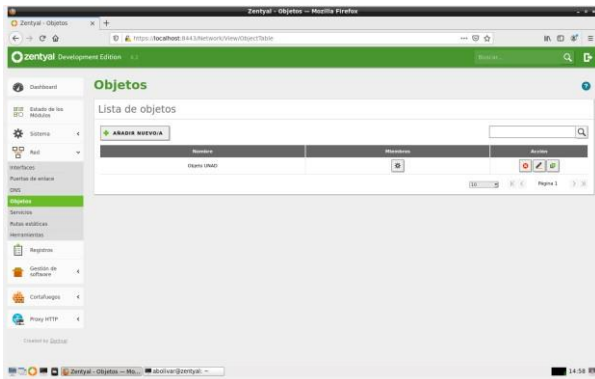


Figura 25. Objetos

Y configuramos los miembros, en este caso será un equipo con ip fija (pc1) y como puerta de enlace el direccionamiento a Zentyal:



Figura 26. Configuración de los objetos

Luego configuramos las reglas de acceso en el proxy y relacionamos el origen que sería el Objeto UNAD y la decisión Denegar Todo:

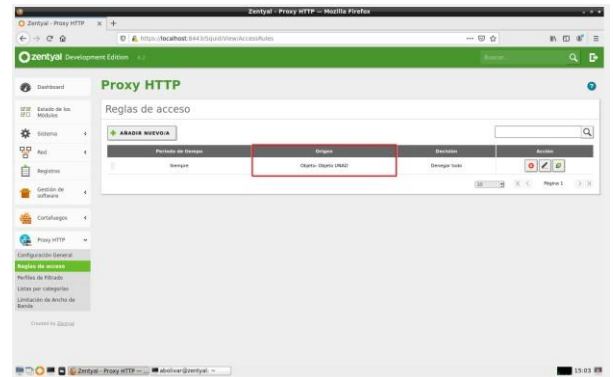


Figura 27. Configuración de las Reglas de acceso

Esto nos ofrece una conexión completamente nula para el cliente relacionado a nuestro proxy no transparente:

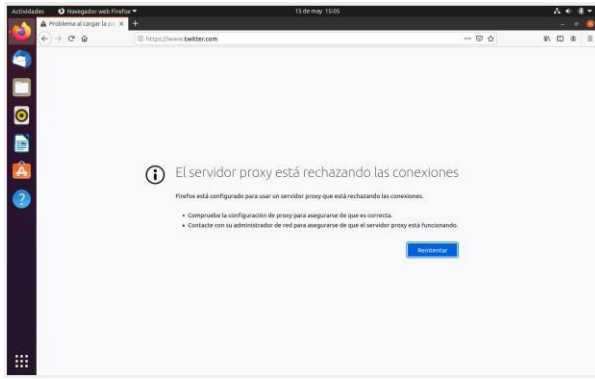


Figura 28. Configuración de las Reglas de acceso

5 TEMÁTICA 3: CORTAFUEGOS

Realizaremos la configuración del firewall a través del programa zentyal, por lo cual necesitaremos una máquina virtual con el zentyal y otra con un Ubuntu para realizar las respectivas validaciones.

Inicialmente lo que haremos es asignar la IP del servidor zentyal al servidor donde realizaremos las pruebas.

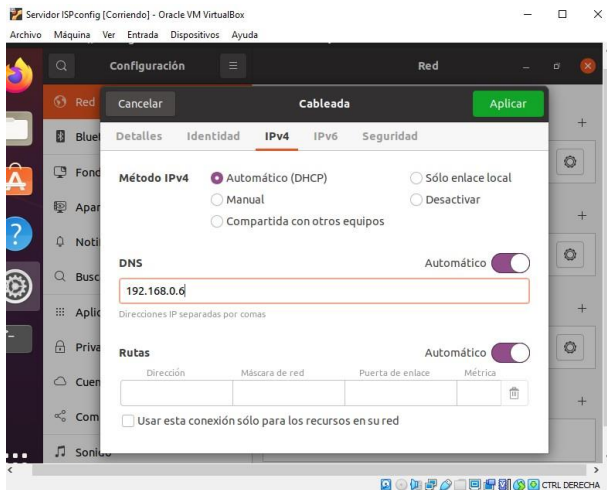


Figura 29. Asignación de DNS

Realizaremos una prueba para denegar todos los servicios de navegación de internet.

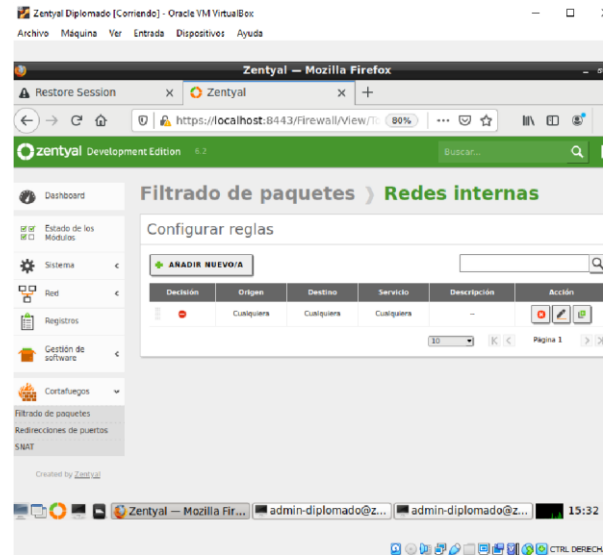


Figura 30. Prueba de denegación

Ahora validaremos como se ven las peticiones en la otra máquina.

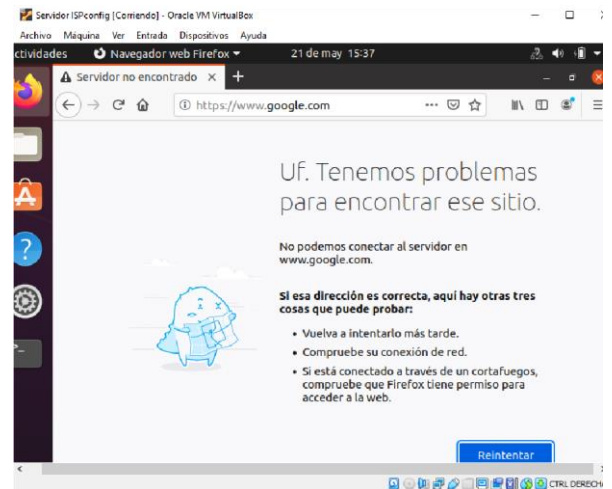


Figura 31. Denegación correcta.

Ahora activaremos todos los servicios para las redes internas para navegar con libertad en la red.

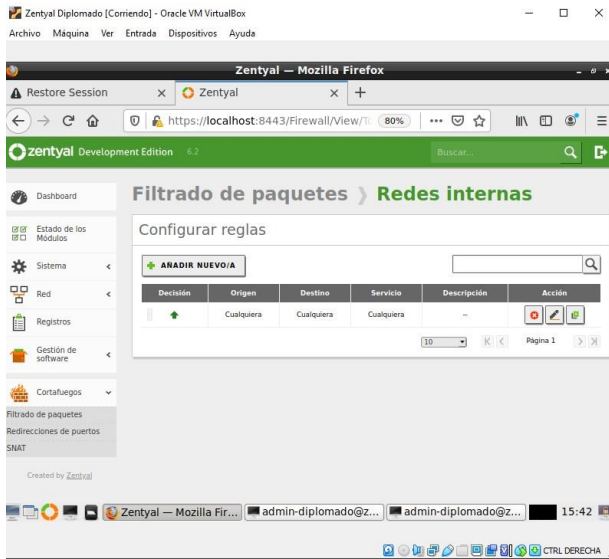


Figura 32. Activación de servicios.

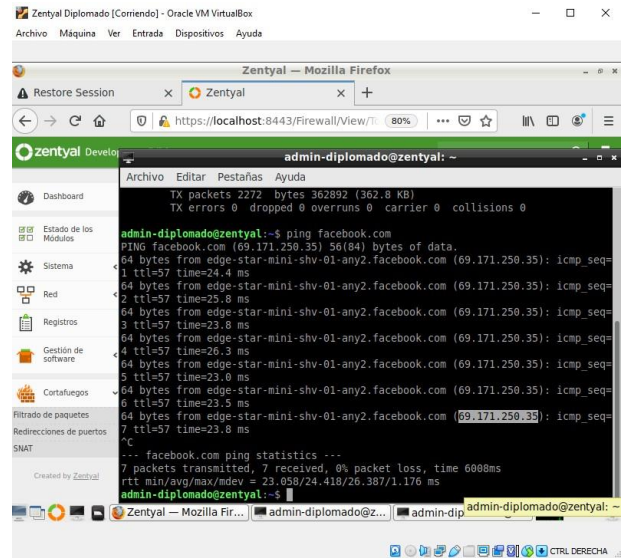


Figura 34. Obtener IP desde terminal

Validación de navegabilidad de la red sin problema.

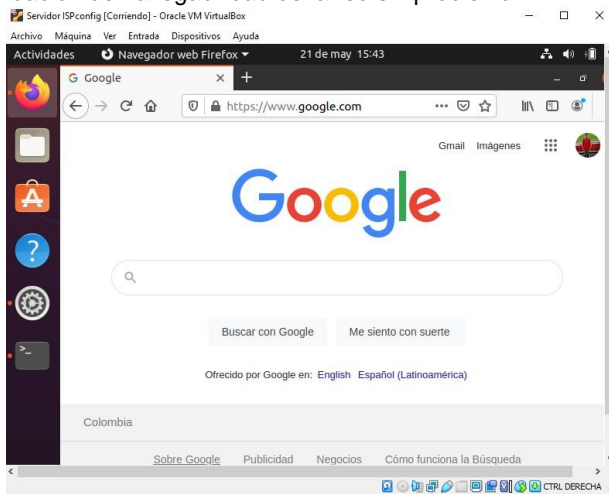


Figura 33. Navegación correcta

Obtenemos IP del sitio a bloquear.

Ahora crearemos un destino de objetos, es este destino de objetos incluiremos las IP a las cuales vamos a restringir, esto es una lista de direcciones IP totalmente administrables por el administrador del firewall, por lo cual esta creada la nueva regla de red

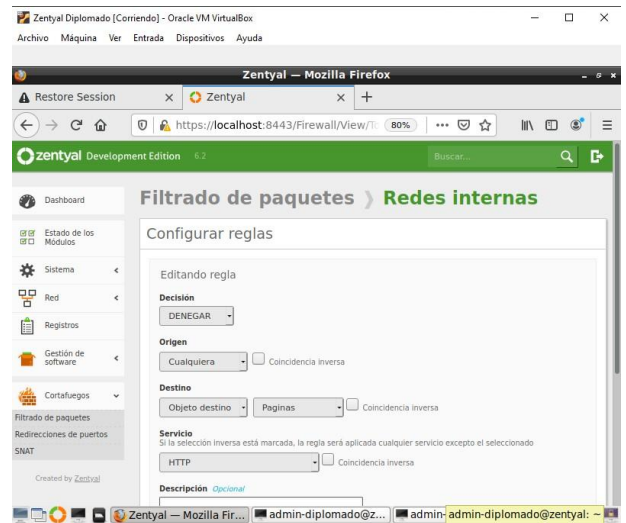


Figura 35. Creación de regla con su lista destino de objetos.

Ahora validaremos que la configuración funcione correctamente, en este caso realizamos la denegación de servicios a la IP de Facebook, por lo cual no le permite el acceso.

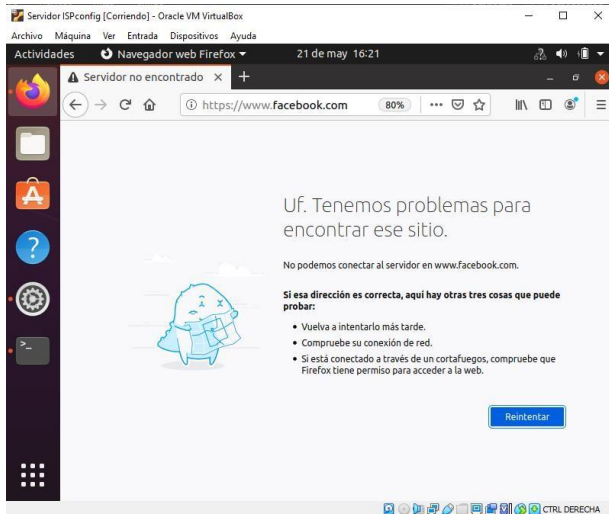


Figura 36. Validamos las restricciones de la red.

Validamos el acceso a una nueva página e ingresamos sin problema



Figura 37. Validamos el acceso a otra página.

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Para ello debemos contar con dos interfaces Zentyal una Interna y otra externa.



Figura 38. Configuración de acceso red

Luego se debe seleccionar el tipo de servidor y allí se solicita el nombre de dominio ya que será

indispensable cuando se realice la conexión a través de LDAP.



Figura 39. Nombre de ingreso al dominio

Se debe configurar la interfaz 1 como DHCP y la segunda interfaz con una IP fija



Figura 40. Verificación de redes

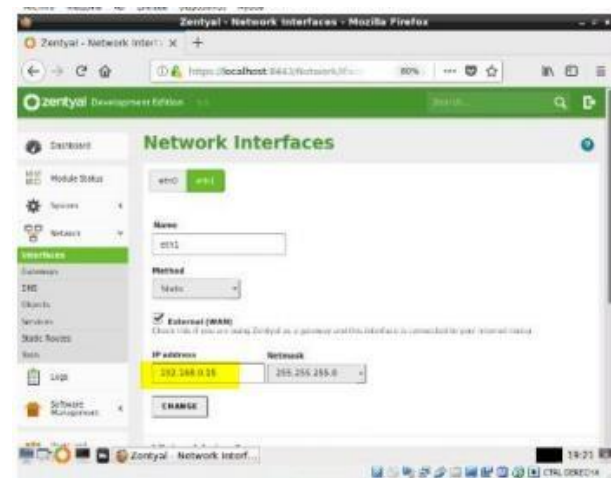


Figura 41. Ip fija interface 2

Cuando el cliente se encuentra conectado se puede visualizar en el dashboard, En esta ocasión se van a compartir archivos e impresoras las cuales se encuentren en el servidor Zentyal

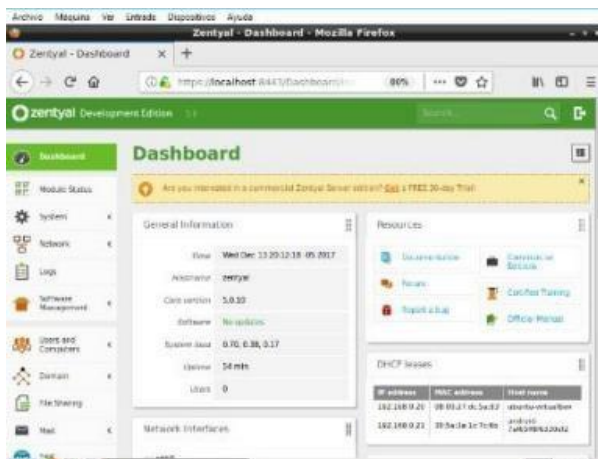


Figura 42. Verificación de comunicación

Luego se instala el cliente LDAP con el comando `sudo apt-get -y install libnss-ldap libpam-ldap-utils nscd`.

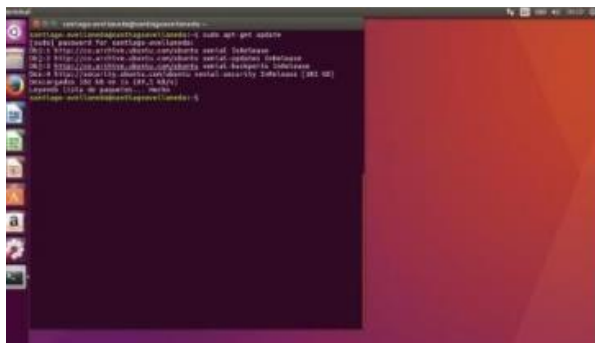


Figura 43. Instalación del cliente LDAP.

Luego para conectar el cliente al servidor de dominio se utiliza el Directorio activo esto a través de Open LDAP y para esto se debe escribir el dominio o la ip.

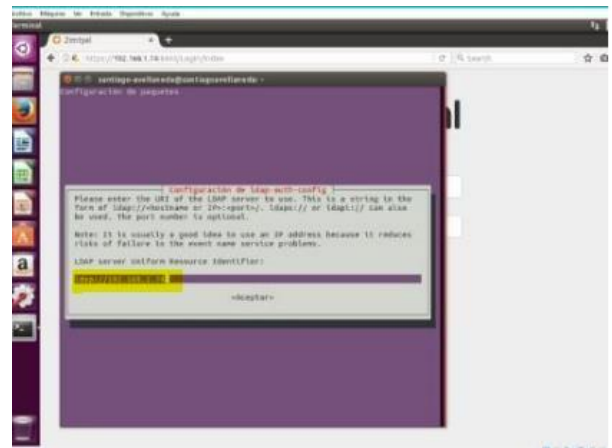


Figura 44. Comunicación Cliente- servidor.

Luego se deben ingresar los detalles de la cuenta de administrador.

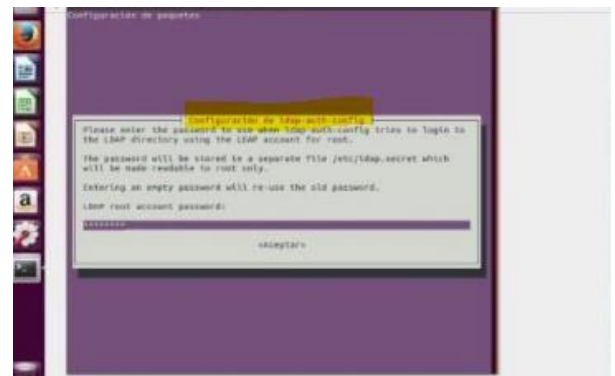


Figura 45. Datos de administrador

Luego se realiza creación de grupos y usuarios



Figura 46. Creación de grupos y usuarios

Se realiza creación de la carpeta compartida



Figura 47. Creación de carpeta compartida.

Por último, se realiza la configuración de la carpeta compartida.



Figura 48. Configuración carpeta compartida

Finalmente se agrega la impresora y de igual manera se comparte con los diferentes usuarios.



Figura 49. Configuración de impresora.

7 Temática 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

- Se procede a realizar la descarga del Zentyal desde la web.



Figura 50. Descarga Zentyal

- Luego se crea la máquina virtual

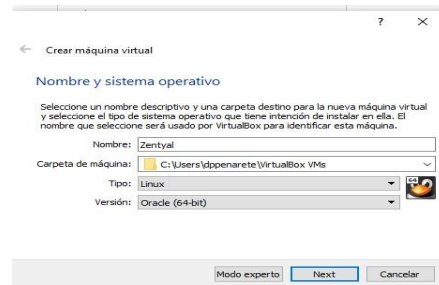


Figura 51. Creación Máquina Virtual.

Luego se procede a montar la ISO descargada.

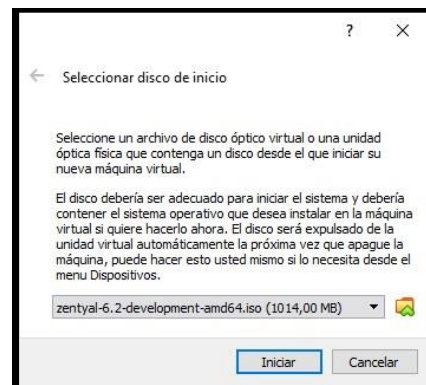


Figura 52. carga imagen iso

Una vez iniciamos la instalación, solicitará el idioma de instalación.

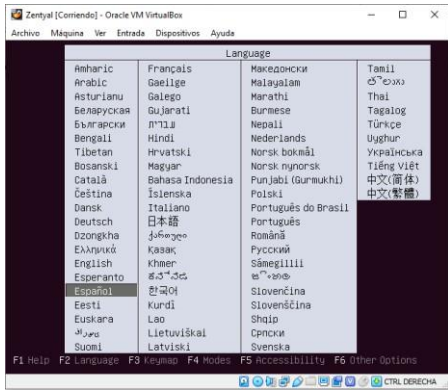


Figura 53. selección idioma instalación.

Aparecerá ahora el menú de instalación.

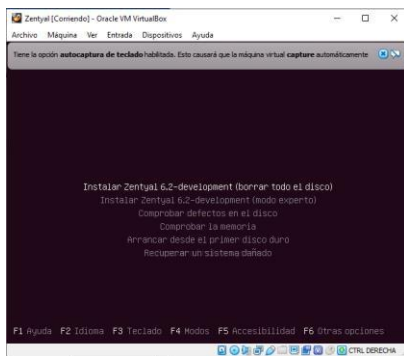


Figura 54. Menú Instalación.

Seleccionamos la primera opción y damos enter para continuar.

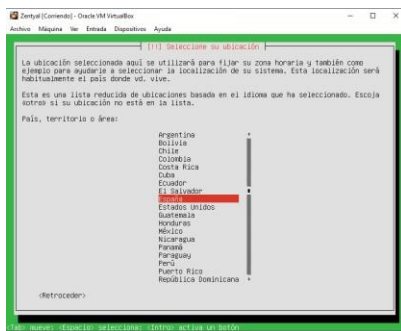


Figura 55. Ubicación instalación.

Preguntara la distribución del teclado.

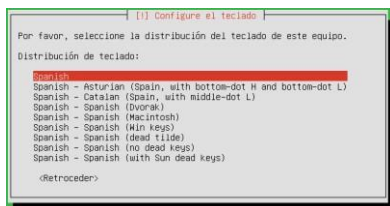


Figura 56. Distribución idioma Teclado.

Se asigna el nombre del servidor

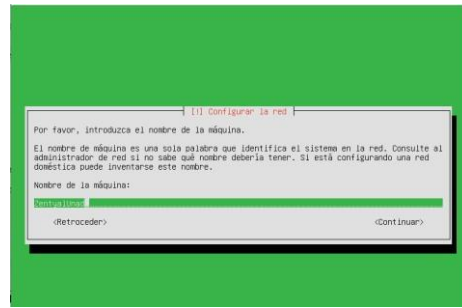


Figura 57. nombre servidor.

- Se asigna el nombre de usuario



Figura 58. Nombre de usuario.

Se asigna la contraseña.

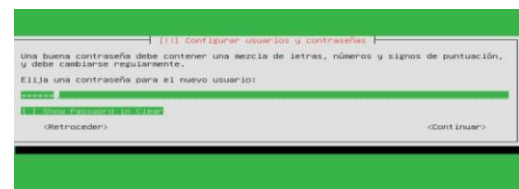


Figura 59. Contraseña - Toma la zona horaria automáticamente, aplica formato al disco duro e inicia la carga y copia de archivos de instalación.

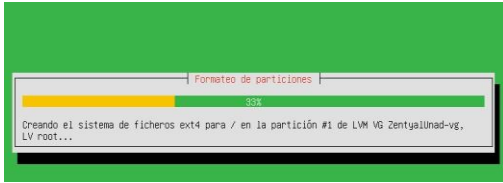


Figura 60. Proceso de carga de instalación.



Figura 61. Instalando Sistema.



Figura 62. Configuración apt.

Al finalizar la instalación el sistema notifica y solicita realizar el reinicio.



Figura 63, finalización instalación.

- Una vez dado enter, inicia la carga de zentyal



Figura 64. Cargando Inicio sistema.

- Una vez finalizada la carga del sistema zentyal, se muestra la interfaz del usuario final y se procede a abrir la consola de administración de esta plataforma.

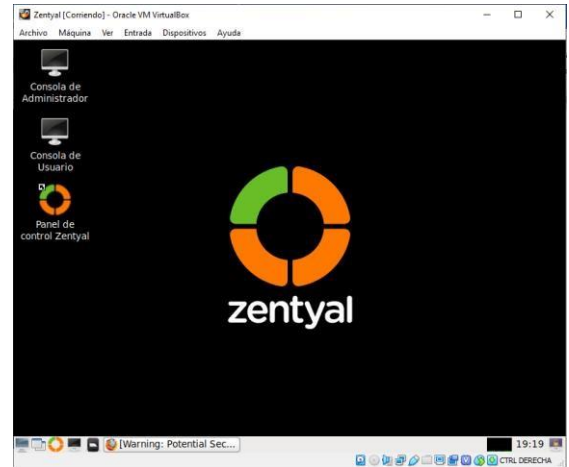


Figura 65. Escritorio Sistema.

- Se inicia el panel de control zentyal, en el cual ingresamos el usuario y contraseña.

Una vez realizado esto nos aparece el menú de configuración final.



Figura 66. Configuración. - Aparecen las opciones de instalación de los paquetes disponibles, en este caso selecciono la VPN que es la temática escogida.

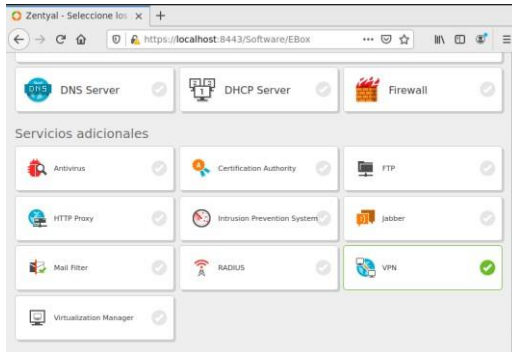


Figura 67. Aplicaciones Disponibles.

- Se da la opción instalar para que se inicie el proceso.



Figura 68. Seleccionar Vpn.

- Muestra el resumen de los paquetes que se van a instalar, a lo cual se le presiona continuar.

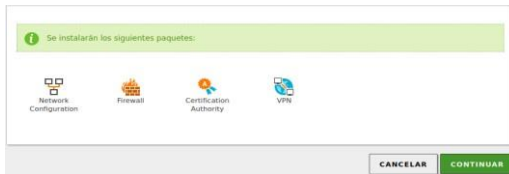


Figura 69. Instalación Módulos Vpn

Inicia la instalación de los módulos de la VPN seleccionados.

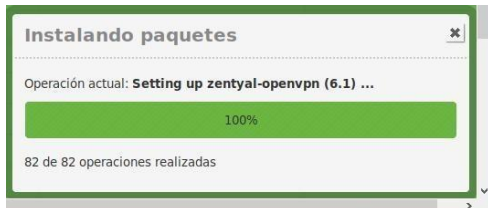


Figura 70. Avance instalación Paquetes

Al finalizar la instalación, el sistema arrojará una notificación de instalación finalizada.

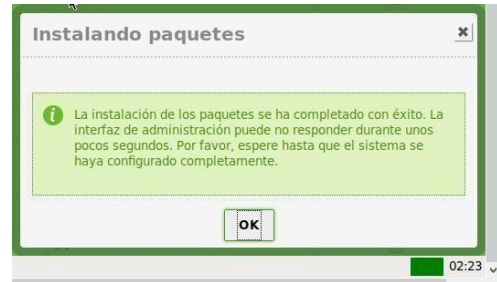


Figura 71. Notifica que se realizó la instalación.

En el panel aparece el módulo instalado

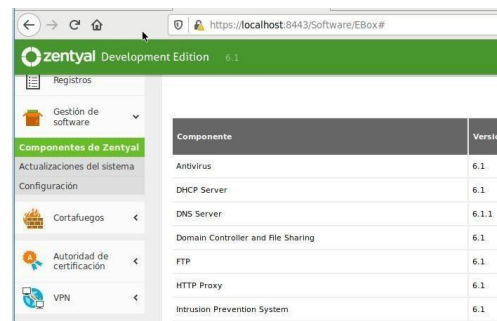


Figura 72. Módulos vpn.

Luego Activamos los módulos necesarios para la configuración aplicar.



Figura 73. Activación complemento.

Procedemos a guardar los cambios aplicados

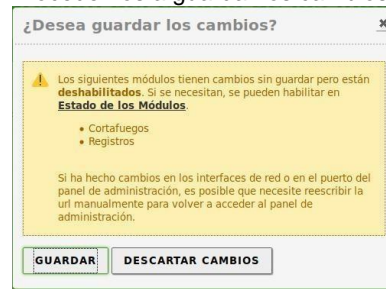


Figura 74. Guardar.

Se crea el servidor VPN.



Figura 75. Descargar Se descarga la configuración del servidor.



Figura 76. Guardar Archivo

Se procede a crear el certificado que permitirá a los clientes realizar la conexión al servidor VPN.

- Se ingresa al módulo de autoridad de certificación y se procede a realizar esta creación del certificado.



Figura 77. Crear Modulo.



Figura 78. crear certificado

- Ya creado, nos aparece en la lista de certificados.

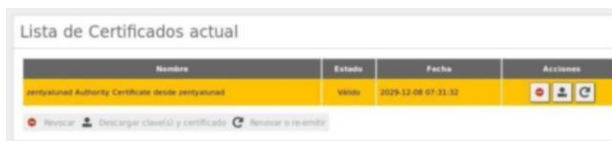


Figura 79. Lista Certificado.

Se descarga el certificado que se debe aplicar en el cliente VPN a conectar.

- Lo pasamos al equipo cliente donde lo aplicaremos después de instalar el OpenVPN como aplicación de conexión.



Figura 80. Descarga.

Desde la página oficial se procede a descargar el cliente VPN.

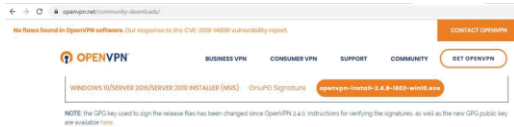


Figura 81. Sitio Oficial Vpn

Se procede a validar la aplicación descargada e instalarla.



Figura 82. Guardar archivo.

Se inicia el asistente de instalación, y se siguen los pasos.



Figura 83. Instalación cliente.

Al instalarse se procede a importar el archivo que descargamos, (el certificado) que nos permitirá establecer la conexión VPN.

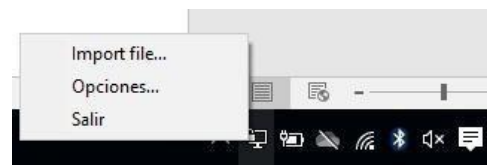


Figura 84. Configurar VPN.

Seleccionamos el archivo de configuración Notifica que el archivo se importa correctamente.

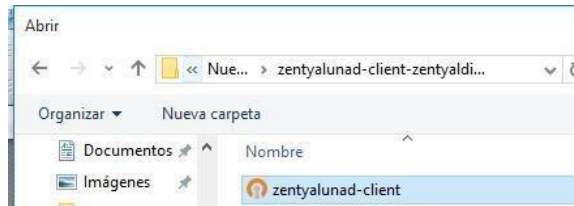


Figura 85. Ruta Archivo.



Figura 86. Carga Satisfactoria.

- Pegamos todos los archivos de configuración en la ruta de instalación de la aplicación OpenVPN en la carpeta config.

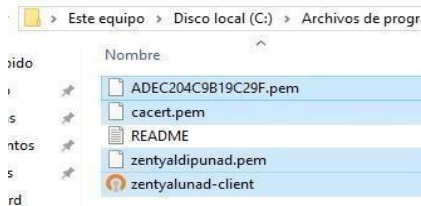


Figura 87. Ruta archivos configuración.

Se procede a realizar la conexión

Establecida la conexión se procede a realizar la prueba, en este caso validamos la dirección ip que tiene el servidor.

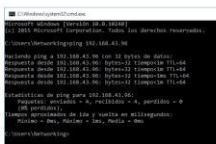
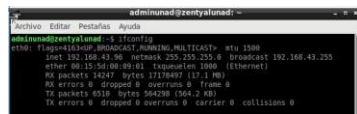


Figura 88. Ip servidor.

Se valida que dentro del zentyal aparezca la conexión activa de la VPN establecida.



Figura 89. Verificación en el servidor.

8 CONCLUSIONES.

Por medio del controlador de dominio que posee Zentyal es posible hacer uso de algunas de las características de un directorio activo de Windows, sin requerir la adquisición de alguna de las onerosas licencias que tienen este tipo de productos, es posible uso de GPO para configurar algunas características en los equipos o usuarios de los componentes unidos al dominio, así como también gestionar la autenticación de usuarios a los recursos y la red bajo el dominio.

A través del desarrollo de esta actividad, se evidencia la implementación de una herramienta que permite establecer conexiones remotas a través de túneles VPN, además se logra identificar como se realiza la conexión de un servidor con un cliente manejando las ip y realizando la configuración correcta para la administración de esta plataforma.

Con el autoaprendizaje se lograron alcanzar los objetivos propuestos en la guía, donde por medio de aportes y sugerencias u observaciones realizadas tanto por el grupo de trabajo, así como el tutor, se logra construir un trabajo a nivel individual y colaborativo.

9 REFERENCIAS

- Carvajal Palomares, F. (2017). Instalación y configuración del software de servidor Web: UF1271. Editorial CEP, S.L. <https://elibro.net/es/lc/unad/titulos/51181>
- How to install Moodle on ISPConfig. (s. f.). HowtoForge. Recuperado 17 de marzo de 2021, de <https://www.howtoforge.com/tutorial/how-to-install-moodleon-ispconfig/>
- ISPConfig 3.1: Automated installation on Ubuntu 18.04 LTS. (s. f.). HowtoForge. Recuperado 17 de marzo de 2021, de <https://www.howtoforge.com/tutorial/ubuntu-ispconfigautomated-install-script/>
- LaCroix, J. (2016). Mastering Ubuntu Server. Packt Publishing; eBook Collection (EBSCOhost). <https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1292906&lang=es&site=eds-live&scope=site>
- Step-by-step Installation Guide for Ubuntu—MoodleDocs. (s. f.). Recuperado 17 de marzo de 2021, de https://docs.moodle.org/310/en/Step-by-step_Installation_Guide_for_Ubuntu