Instalación y configuración DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, servicios File Server, Print Server y VPN

Leandro Diaz , Jonathan Ruiz Rodriguez, Johan Elvis Lasso, Fred José Rodríguez, Héctor Perdomo
Ingeniería de Sistemas
Universidad Nacional Abierta y a Distancia UNAD
Bogotá, Colombia
leandro-diaz@outlook.com, jonatanruizb@gmail.com, jlasso@live.com, ING.perdomoandrade@gmail.com

***Resumen*- En este documento se presenta el proceso de instalación y configuración de diferentes servicios para la administración de un entorno de red bajo el servidor Zentyal desde su interfaz Web, se iniciara desde la parte básica de implementación del entorno del servidor, se activaran los módulos necesarios que permitirán aplicar la configuración necesaria en las herramientas del software, finalmente a cada proceso se le aplicara pruebas para validar su correcto funcionamiento.**

I. INTRODUCCIÓN

Se instala Zentyal Server en una máquina virtual, en este caso se ha elegido la versión de desarrolladores, que es gratuita, de código abierto y está basado en Ubuntu; es ideal para las pequeñas y medianas empresas que quieren adoptar un servidor para sus redes que preste servicios como correo, DNS, DHCP implementando controlador de dominio desde una máquina virtual, Proxy desde un equipo servidor para un equipo cliente, aplicando diferentes procesos que permite la comunicación entre los dispositivos y su respectiva función para restringir el ingreso a los sitios web, Firewall teniendo a disposición varios servicios de Infraestructura para poder acceder a nuestra red, siendo compatible también con servicios que prestan los sistemas Windows. Para esta actividad se verá la configuración acerca de file server y print server.

Esto con el fin de tener el conocimiento al momento de trabajar en grupos donde se requieran estos procesos dependiendo el tipo de usuarios y lugar donde se aplique, para mantener cierto control en la red y establecer determinados procesos que garanticen un correcto funcionamiento en el servicio.

II. INSTALACIÓN DE ZENTYAL SERVER

2. 1 Requisitos de Instalación Hardware.

Zentyal funciona sobre hardware estándar arquitectura x86_64 (64-bit), se requiere para su instalación mínimo memoria de 1GB, disco duro 20 GB, procesador de doble núcleo y dos tarjetas de Red.

2. 2 Proceso de Instalación

Instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT.

Ingresar a virtualBox y crear la unidad de instalación del Sistema Operativo Zentyal Server, dar clic en esta unidad para iniciar la instalación del software.

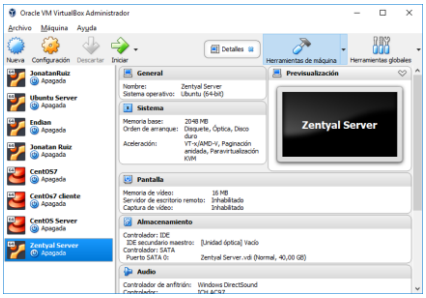


Imagen 1. Selección de unidad.

Se abre la ventana de búsqueda de software, ingresar la ruta donde de la aplicación para instalar, clic en el iniciar.

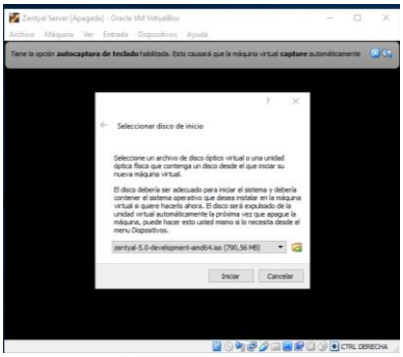


Imagen 2. Ruta de instalación.

Seleccionar el idioma de la instalación en este caso español, presionar la tecla enter para continuar con el proceso.

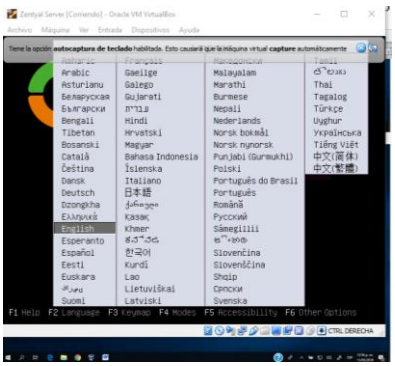


Imagen 3. Selección de idioma.

Se abre la ventana de instalación seleccionar la primera opción instalar Zentyal.

Imagen 4. Selección de software.

Solicita el idioma para el nuevo sistema operativo.

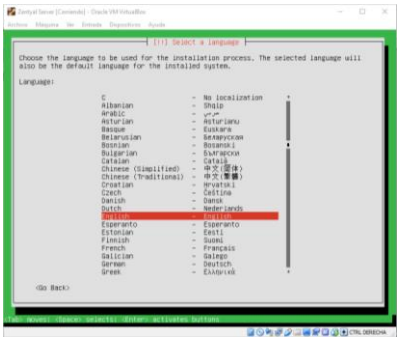


Imagen 5. Configuración de idioma software.

Seleccionamos en este caso español presionar la tecla enter para continuar con el proceso de instalación.

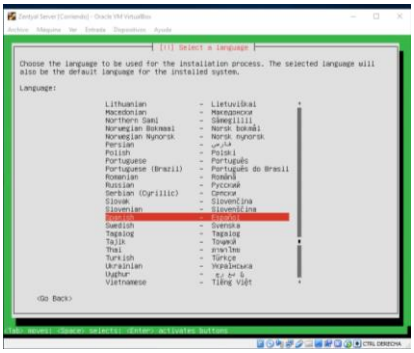


Imagen 6. Selección de idioma software.

Solicita el país, seleccionar Colombia y dar enter.

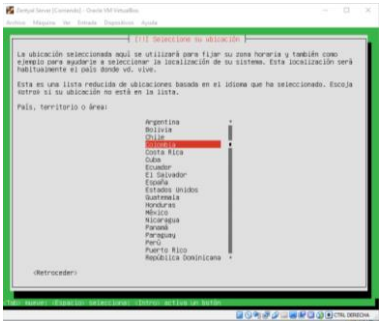


Imagen 7. Selección localización.

Solicita la configuración del teclado, seleccionamos la opción no para que detecte automáticamente el teclado.

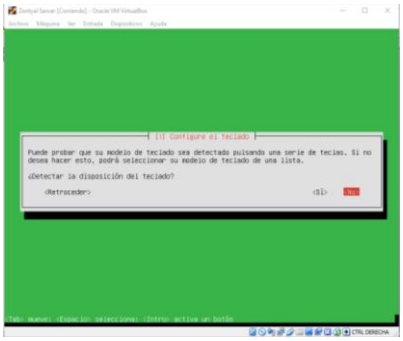


Imagen 8. Configuración de teclado.

Indica configuración detectada del teclado, presionar enter.

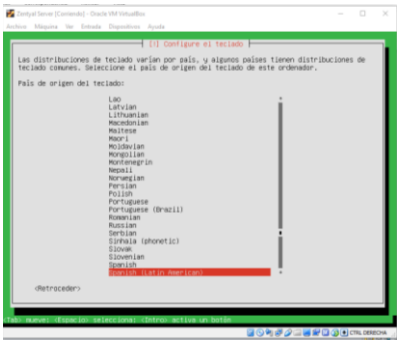


Imagen 9. Selección de teclado.

Detecta la configuración de teclado, dar Enter para continuar.

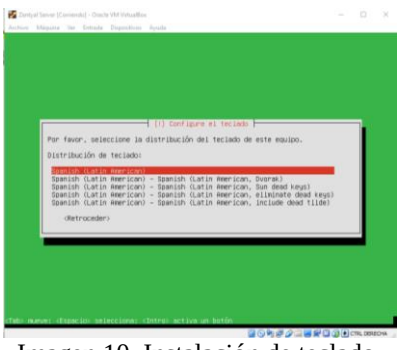


Imagen 10. Instalación de teclado.

Debemos esperar mientras realiza los procesos de instalación.

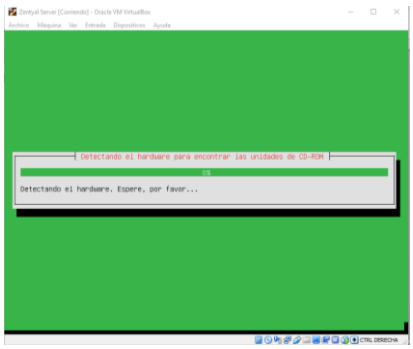


Imagen 11. Proceso de instalación.

Al realizar los procesos nos muestra el avance, hasta el punto de finalización.

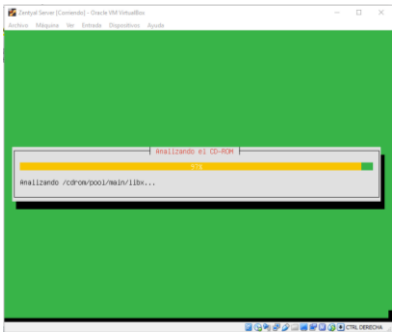


Imagen 12. Finaliza proceso.

Solicita configurar el equipo, asignar un nombre a la máquina y seleccionar el botón continuar.

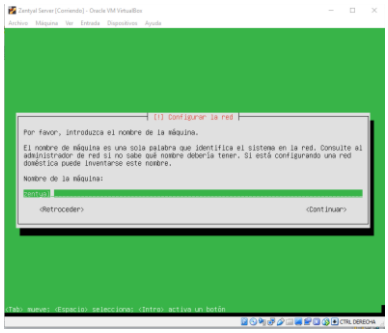


Imagen 13. Asignar nombre máquina.

Se solicita crear un usuario para el ingreso al equipo, este caso colocamos administrador para el ingreso.

Imagen 14. Configuración usuario.

Se solicita una clave para el usuario creado.

Imagen 15. Configuración contraseña.

Requiere validar contraseña, escribir nuevamente los datos.

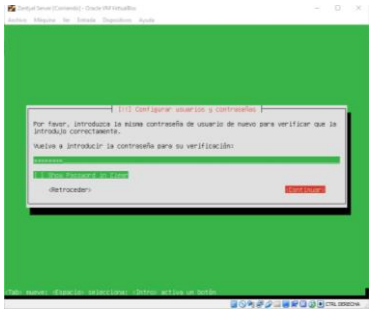


Imagen 16. Validación contraseña.

Se detecta la localización de la instalación, dar clic en el botón si para continuar.

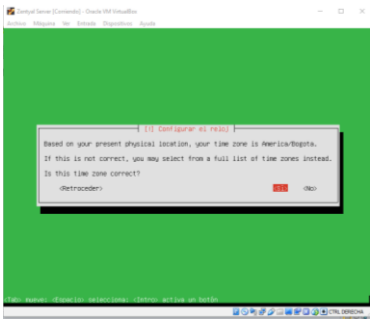


Imagen 17. Detectar localización.

Se muestra el proceso de configuración hasta finalizar la instalación.

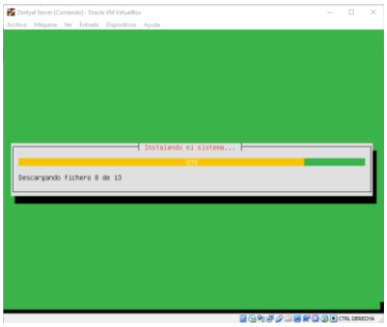


Imagen 18. Proceso configuración.

Al completar la instalación indica que se iniciara el sistema, dar clic en el botón continuar para terminar el proceso.

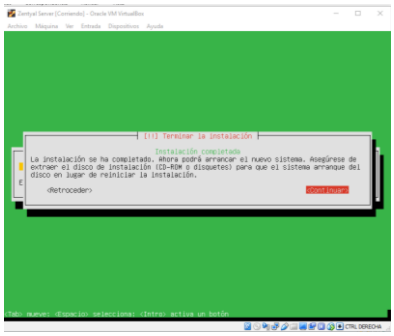


Imagen 19. Finaliza instalación.

Al finalizar el software se reinicia y luego ingresar al escritorio de Zentyal.

Imagen 20. Ingreso servidor.

2. 2 Ingreso a la interfaz de Zentyal

Abrir el navegador desde el escritorio, ingresar a la URL localhost:8443, esto para abrir la plataforma de zentyal, ingresar los datos del administrador.

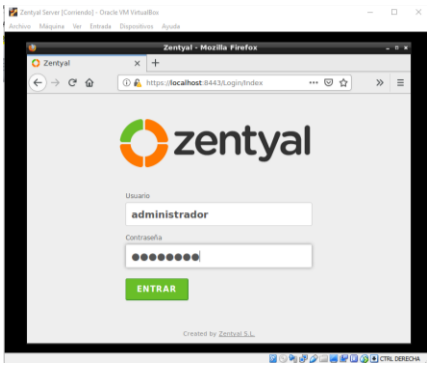


Imagen 21. Interfaz servidor.

Se abre la configuración inicial del software, desplazarse a la parte inferior de la página y dar clic en el botón continuar para validar los paquetes de instalación.

Imagen 22. Validar paquetes.

Muestra el listado de paquetes que se pueden instalar, seleccionamos los que se requieren y dar clic en el botón de la parte inferior derecha instalar.

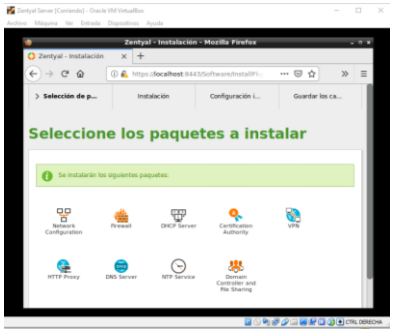


Imagen 23. Listado paquetes.

Se inicia el proceso de instalación y se muestra el avance debemos esperar hasta que finalice este proceso de instalación de paquetes.

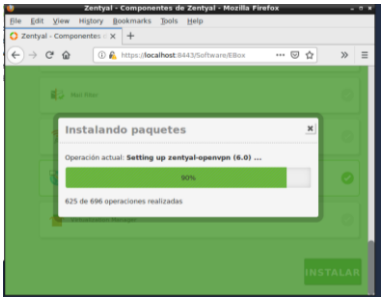


Imagen 24. Instalación de paquetes.

Se muestra el proceso de configuración de la interfaz.

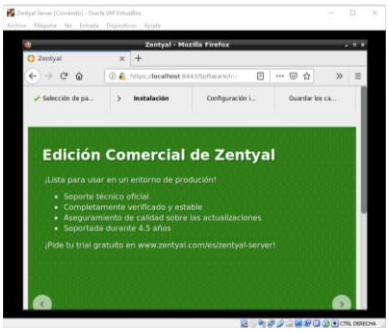


Imagen 25. Configuración interfaz.

Al finalizar indica que ha terminado el proceso y podemos ir al dashboard que es el panel de configuración de Zentyal.

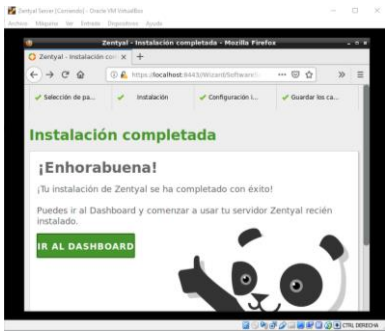


Imagen 26. Finaliza instalación paquetes.

III. **Temática 1 DHCP Server, DNS Server y Controlador de Dominio**

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Activamos los módulos de DHCP para generar la ip sobre otra máquina virtual por red interna.

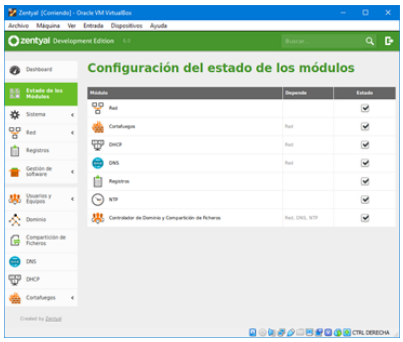


Imagen 27. Activación módulo DHCP.

Luego vamos a conectarnos a la ip definida por el servidor en este caso sería la 192.168.1.75

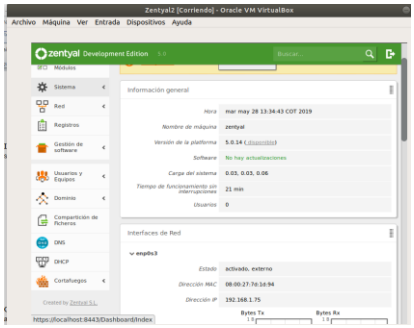


Imagen 28. Activación para comunicación servidor.

Como vemos en el dashboard no se muestra IP asignadas en el DHCP para luego activar el cliente Ubuntu y tomar por el rango asignado de 192.168.1.160 a la 192.168.1.170.

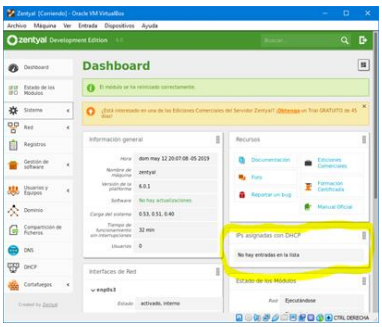
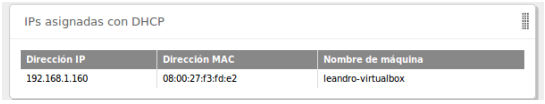


Imagen 29. Validación de ip DHCP.

Y por último verificamos que el cliente Ubuntu desktop tiene asignada la IP 192.168.1.160 junto con el apuntamiento a la IP del servidor.



Para la configuración de los DNS volvemos a los componentes de Zentyal pero como vemos anteriormente ya había realizado la instalación del módulo junto con el de directorio activo para ejecutarlo posteriormente.

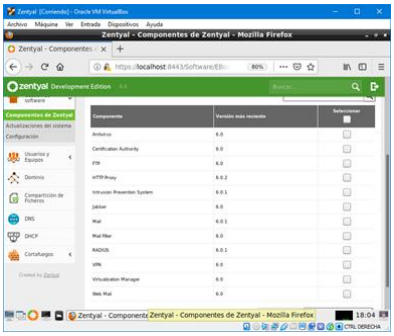


Imagen 30. Componentes servidor.

Vemos que en el módulo podemos configurar el DNS transparente y añadir un nuevo dominio configurando como nuevo.

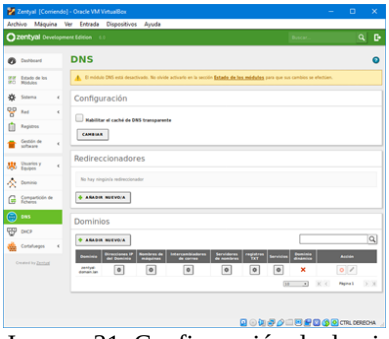


Imagen 31. Configuración de dominio.

Habilitamos el módulo para que comience el servicio del controlador de dominio y guardamos cambios.

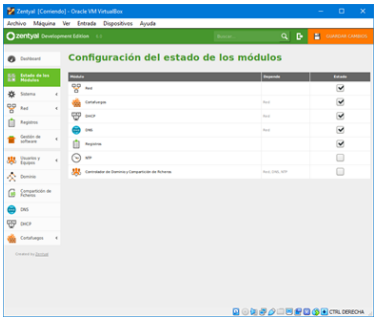


Imagen 32. Activación de modulo para dominio.

Y el dashboard nos muestra que se está ejecutando para comprobarlo posteriormente en nuestro equipo cliente.

Imagen 33. Comprobación de dominio.

Finalmente tenemos que configurar nuestro servicio de controlador de dominio LDPA el cual ya se había especificado la instalación del módulo junto con el DHCP y DNS anteriormente.

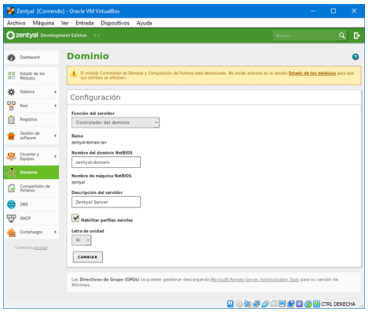


Imagen 34. Control de dominio LDPA.

Y activamos el módulo de controlador de dominio.

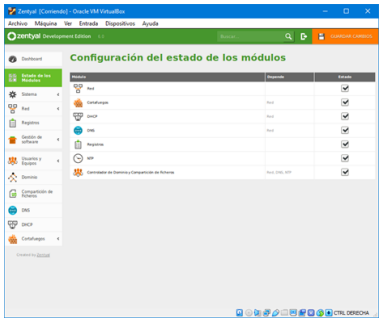


Imagen 35. Activar controlador de dominio LDPA.

Verificamos la configuración del módulo LDPA junto con la creación de los nombres de los equipos en el controlador de dominio en Zentyal.

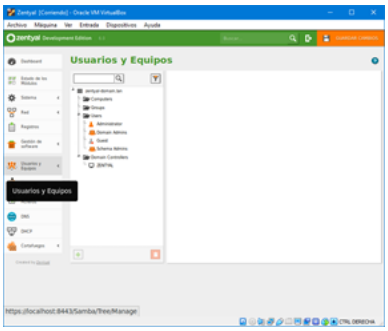


Imagen 36. Verificación control de dominio.

IV. **Temática 2 Proxy no transparente**

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

Abrimos el dashboard y se muestra la instalación realizada en la un panel al lado izquierdo de la pantalla.

Imagen 37. Ingreso módulo de red.

Inicialmente configuramos la interfaces de red desde virtualbox que permiten la comunicación de los equipos, ingresar a configuración del equipo zentyal, seleccionar la opción red, seleccionar la interfaz1 conectado NAT, interfaz2 conectado Red Interna.

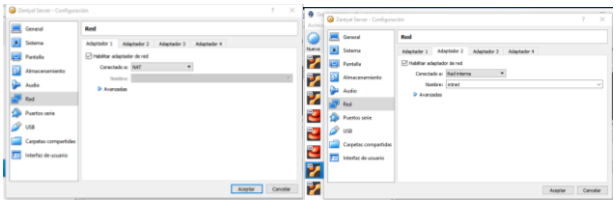


Imagen 38. Configuración interfaces servidor.

Ingresar a configuración del equipo Cliente, seleccionar la opción red, seleccionar la interfaz1 conectado Red Interna, interfaz2 conectado Adaptador Puente.

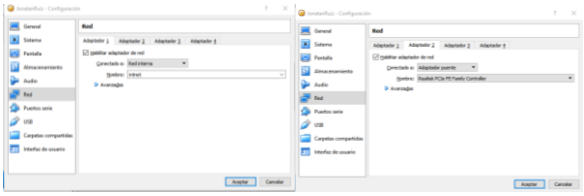


Imagen 39. Configuración interfaces cliente.

Ingresar al menú interfaces de red, configuramos la red inicial enp0s3 con método DHCP, marcamos la opción externo WAN y damos clic en el botón CAMBIAR.

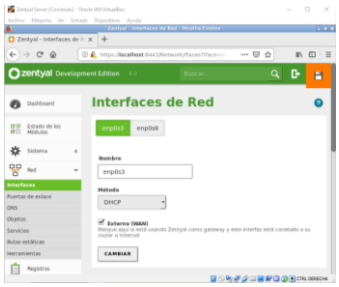


Imagen 40. Configuración red DHCP.

Configuramos la red enp0s8 con método Estático, no marcar la opción externo WAN, ingresar una ip que se convierte en el Gateway para los equipos cliente y damos clic en el botón CAMBIAR para guardar los cambios.

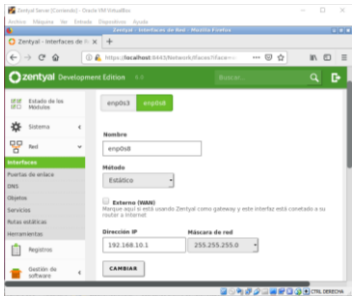


Imagen 41. Configuración red estática.

Crear un objeto para identificar los equipos en red seleccionamos objetos, dar clic en el botón Añadir Nuevo Colocamos el nombre Ubuntuc.

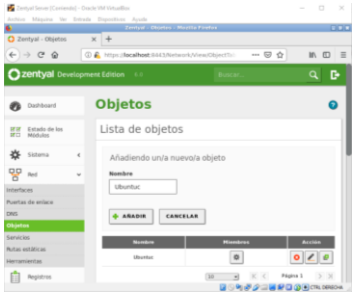


Imagen 42. Creación de objeto.

Luego de añadir validamos que el objeto ingrese a la lista inferior para poder realizar las configuraciones correspondientes.

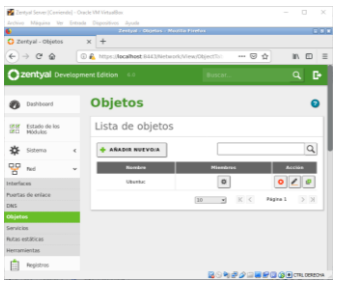


Imagen 43. Configuración de objeto.

Debemos agregar los usuarios cliente al listado de restricción, Ingresar al equipo cliente en Ubuntu configurar una ip fija para el equipo cliente y que el Gateway sea la ip del servidor.

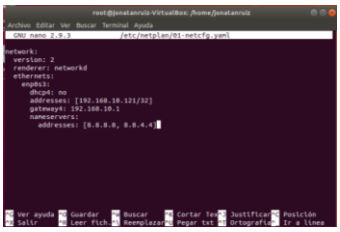


Imagen 44. Configuración red cliente.

Regresamos al servidor zentyal damos clic en el icono de miembros para agregar a los usuarios requeridos.

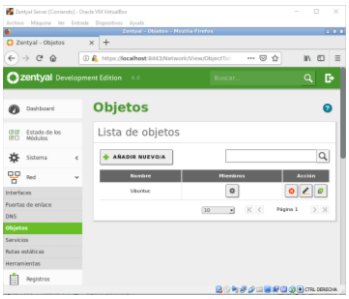


Imagen 45. Configuración usuarios.

Se abre la venta de miembros, dar clic en el botón Añadir Nuevo.

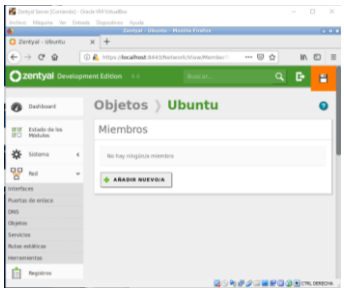


Imagen 46. Agregar usuarios.

Ingresar los datos del equipo cliente, nombre en la opción de dirección ip colocar CIDR, ingresar la ip del equipo cliente y dar clic en el botón Anadir para continuar con el proceso.

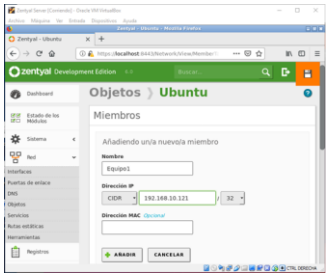


Imagen 47. Configuración datos usuario.

Luego de guardar la configuración se cierra la ventana y regresa a la pantalla inicial de objetos donde se evidencia la ip de cliente y la configuración aplicada.

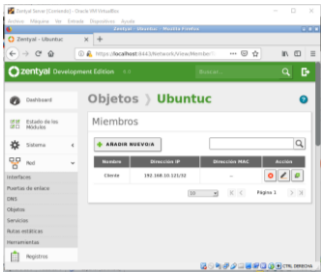


Imagen 48. Validación usuarios.

En el menú del lado izquierdo ingresar al módulo Proxy HTTP y seleccionar la opción Configuración General.

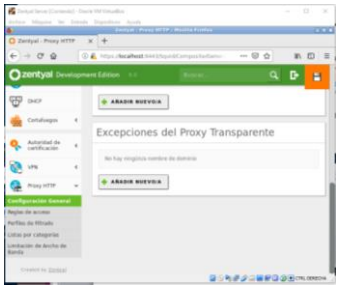


Imagen 49. Ingreso modulo proxy.

Validar que la opción proxy transparente no este marcada, en el cuadro puerto ingresar el puerto 3128y dar clic en el botón CAMBIAR para continuar con el proceso requerido.

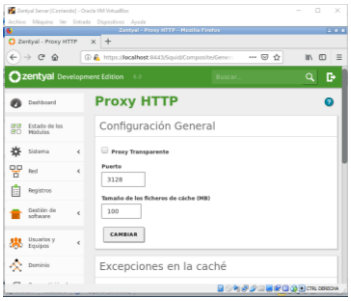


Imagen 50. Configuración proxy no transparente.

Debemos crear las reglas de trabajo para los usuarios, en el menú del lado izquierdo ingresar a Proxy HTTP, seleccionar la opción Reglas de acceso.

Dar clic en el botón Añadir Nuevo para agregar las reglas de los usuarios.

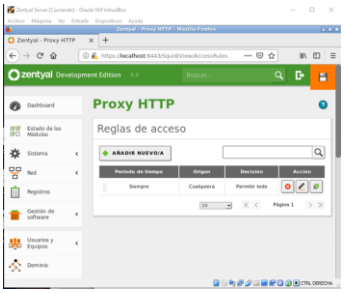


Imagen 51. Agregar reglas de acceso.

En el campo origen ingresar el objeto creado para este caso Ubuntu y en el campo decisión marcar la opción denegar todo, luego dar clic en el botón Añadir para continuar con el proceso, y estaría configurado el proxy para el trabajo con los usuarios.

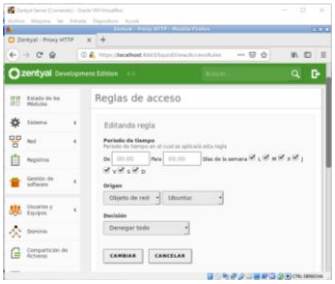


Imagen 52. Configuración reglas de acceso.

Muestra la pantalla inicial de proxy, donde se evidencia los cambios realizados, el origen y la configuración aplicada.

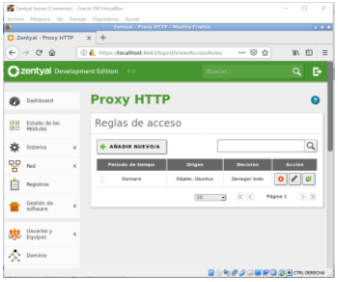


Imagen 53. Validación configuración proxy.

Reiniciar el equipo servidor y el equipo cliente
Regresar al equipo cliente y configurar el proxy en el navegador, desde la barra de menús ingresar a editar y seleccionar la opción preferencias.

En la parte inferior de preferencias en la opción configuración de red, dar clic en el botón configuración.

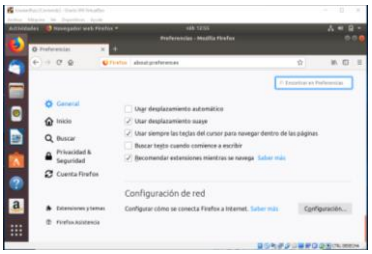


Imagen 54. Configuración preferencias cliente.

Debemos ingresar los datos del proxy del servidor, marcar la opción configuración manual proxy, ingresar los datos de la ip del servidor 192.168.10.1, con el puerto 3128 que están configurados en el servidor y marcar la opción usar para toda la configuración.

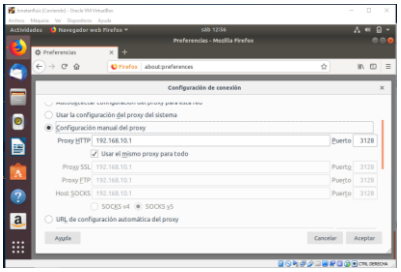


Imagen 55. Asignación de proxy cliente.

Validar en el navegador del equipo cliente el acceso a los sitios, colocar la dirección de un sitio web y validar que el servidor proxy no permita el ingreso ni conecte.

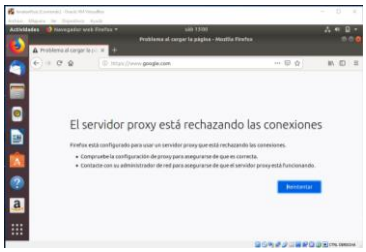


Imagen 56. Validación de proxy cliente.

V. **Temática 3 Cortafuegos**

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Al hablar de Cortafuegos podemos decir que este hace parte de un sistema o una red, el cual está diseñado para bloquear el acceso de páginas no autorizadas o dar autorización a páginas que si están autorizadas, para cualquier empresa ya sea grande o pequeña la seguridad es muy importante pues la información que manejan es muy valiosa para ellos y con el cortafuegos podemos ayudar a que esto sea así.

Luego de Finalizar la instalación de Zentyal Server 6.0, nos abrirá en el navegador y nos solicitara el usuario y la contraseña, estas fueron configuradas en la instalación.

Imagen 57. Ingreso usuario servidor.

Posteriormente Instalaremos los paquetes DNS Server, DHCP Server y el Firewall desde la consola de Zentyal.

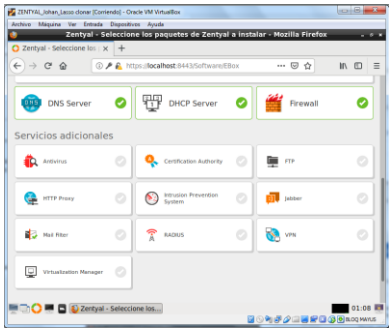
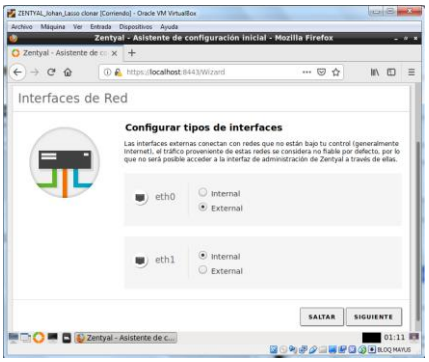


Imagen 58. Instalación paquetes firewall.

Configuramos las interfaces de red eth0 como externa (WAN) por DHCP y eth1 como interna (LAN) con IP estática 192.168.7.254.



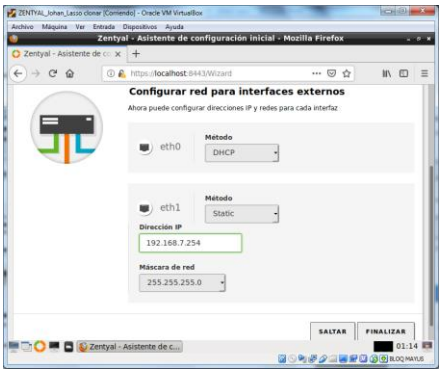


Imagen 59. Configuración interfaces red.

Luego configuramos en la máquina Ubuntu la puerta de enlace y servidor DNS para que se conecte a Internet a través de Zentyal.

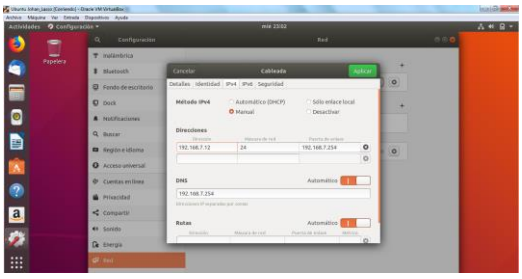


Imagen 60. Configuración datos red.

Antes de configurar las reglas, en nuestro equipo cliente Ubuntu iniciamos el navegador y abrimos una página de una red social, en nuestro caso Facebook, como podemos ver tenemos acceso.

Imagen 61. Validación ingreso red.

En el administrador de Zentyal, ingresamos por la opción de cortafuegos y luego a reglas de filtrado para las redes internas.

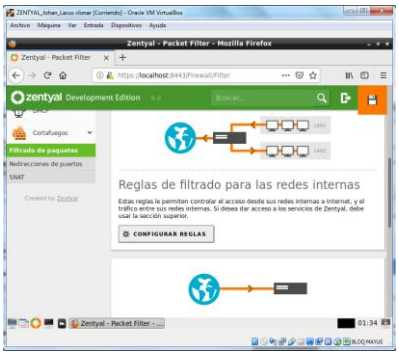


Imagen 62. Configuración reglas filtrado.

Antes de crear la regla comprobamos con el comando "nslookup" que ip relacionada corresponde a Facebook, en este caso es 157.240.6.35.

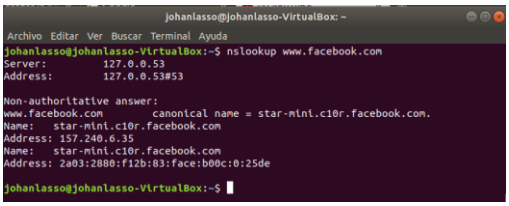


Imagen 63. Validación sitios web.

Se configuran las reglas las reglas de filtrado para algunos sitios de entretenimiento o redes sociales a partir de su IP.

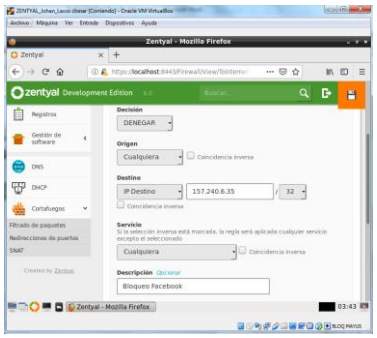


Imagen 64. Filtrado sitios web.

Posteriormente creamos varias reglas para otras paginas que vamos a bloquear como Youtube y Twitter.

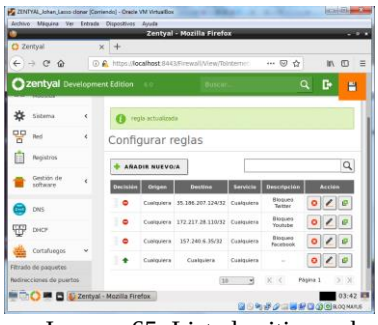


Imagen 65. Listado sitios web.

Resultados Obtenidos:

Después de guardar los cambios realizados, se ingresa desde el equipo Cliente Ubuntu a una de las páginas bloqueadas, en este caso Facebook.

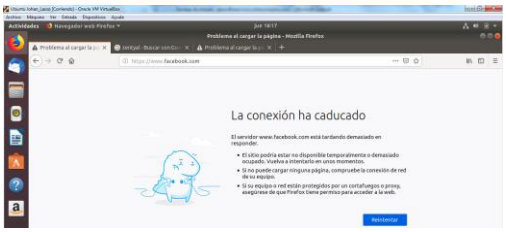


Imagen 66. Comprobación ingreso restringido.

Al ingresar la URL de una página diferente a las bloqueadas, seevidencia un normal funcionamiento, en este caso google.

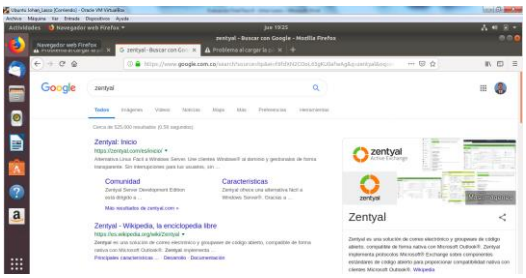


Imagen 67. Comprobación ingreso activo.

VI. **Temática 4 File Server y Print Server**

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

Al tener 2 interfaces Zentyal nos pregunta como deseamos manejarlas, para ello seleccionar la primera interfaz como Interna, la segunda como Externa.

Imagen 68. Configuración acceso red.

En el caso de la interfaz 1 esta puede dejarse con IP fija una vez revisado desde terminal con el comando ifconfig que configuración tiene asignada.

Imagen 69. Configuración datos red.

Solicita el nombre del dominio del servidor, este será necesario cuando se realice la conexión a través de LDAP.

Imagen 70. Ingreso nombre dominio.

Pregunta cómo se manejará el servidor, si como extensión de un servidor LDAP como por ejemplo desde Windows Server o configurarlo como servidor Stand Alone.

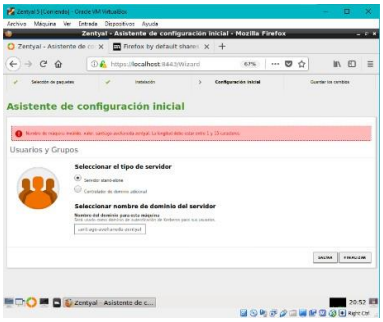


Imagen 71. Asignación de servidor.

En Interfaces en Redes revisar que la interfaz 1 esté en DHCP y exista conectividad Internet y la segunda interfaz con una dirección IP fija.

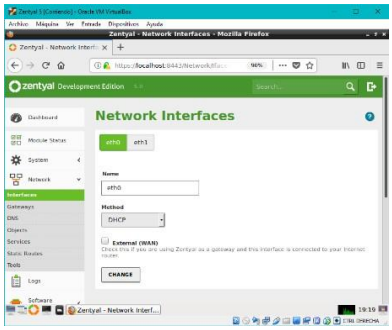


Imagen 72. Comprobación de redes.

En la segunda interfaz se define la dirección IP como fija.

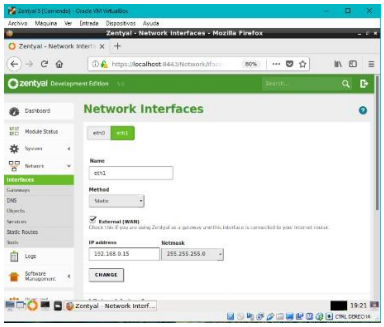


Imagen 73. Asignar interfaz ip estática.

Una vez conectado el cliente se ve desde el dashboard de Zentyal. En este caso se busca compartir archivos e impresoras entre computadoras que se encuentren en el dominio del servidor Zentyal.

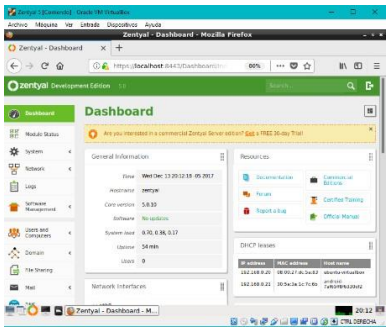


Imagen 74. Validación de comunicación.

Instalar el cliente LDAP a través del siguiente comando sudo apt-get -y install libnss-ldap libpam-ldap ldap-utils nscd.

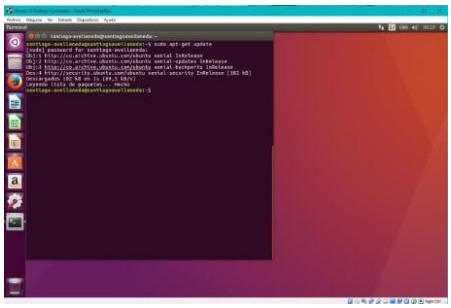


Imagen 75. Instalación cliente LDAP.

Se conecta el equipo cliente al dominio, para ello se usará Active Directory a través de Open LDAP, en esta parte primero pregunta la URL de LDAP, se debe escribir el dominio seleccionado o la IP.

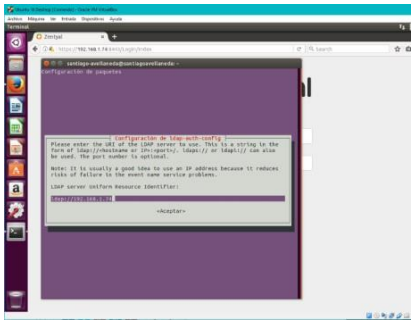


Imagen 76. Comunicación cliente servidor.

Seleccionar la versión de LDAP a usar.

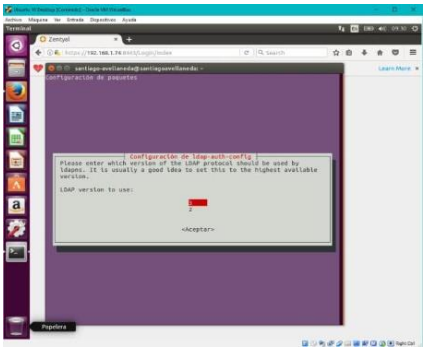


Imagen 77. Configuración versión LDPA.

Ahora se ingresan los detalles de la cuenta de administrador.

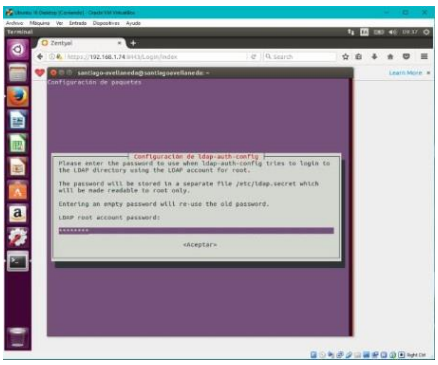


Imagen 78. Ingreso datos administrador.

Se modificará el archivo nsswitch.conf para trabajar con LDAP a través del comando sudo nano /etc/nsswitch.conf Archivo antes de cambios.

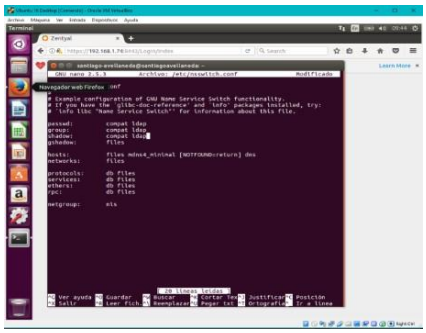


Imagen 79. Configuración cliente LDPA.

Se procede a crear los usuarios y grupos.

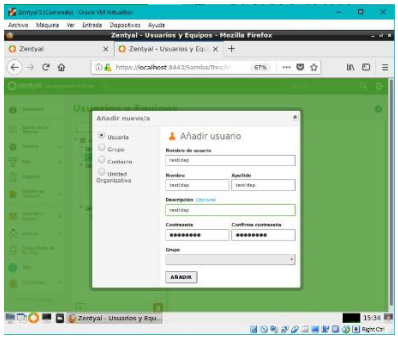


Imagen 80. Crear usuarios y grupos.

Se procede a crear una carpeta compartida en el módulo de carpetas compartidas, hacer clic en agregar nuevo.

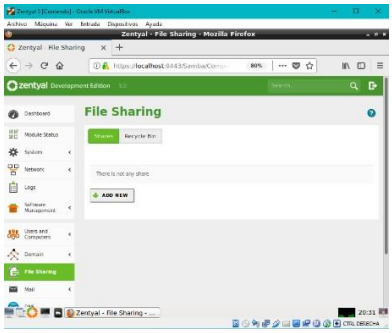


Imagen 81. Crear carpeta compartida.

Se le asigna un nombre a la carpeta compartida en Zentyal, luego se selecciona si se desea que sea una carpeta compartida dentro de los archivos de Zentyal o si se desea una ruta dentro del equipo.

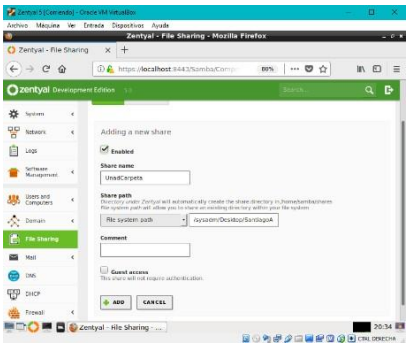


Imagen 82. Configuración carpeta compartida.

También es posible compartir una carpeta desde grupos en la parte inferior en Compartir directorio para grupo.

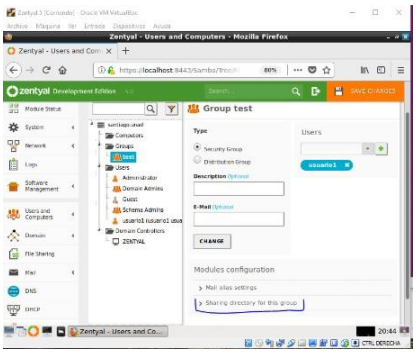


Imagen 83. Configuración servicio grupos.

VII. **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.

Configuración servidor VPN trabajaremos por el puerto 1194 default.

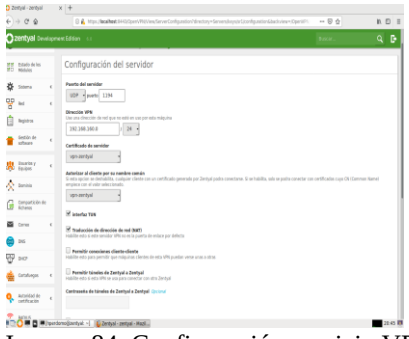


Imagen 84. Configuración servicio VPN.

Creación certificados.

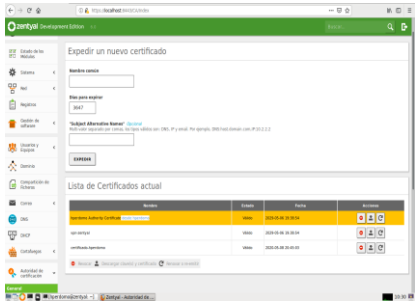


Imagen 85. Creación certificados.

Creamos el servidor VPN.

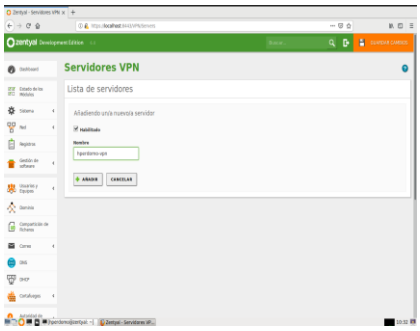


Imagen 86. Crear servidor VPN.

Realizamos la configuración del servidor con el certificado que se creó.

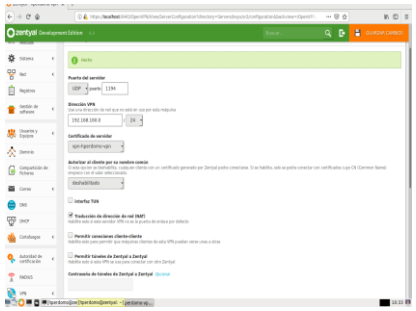


Imagen 87. Asignar certificado.

Creamos a través de Red el servicio para la VPN.

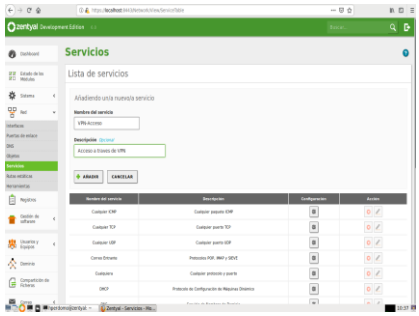


Imagen 88. Activar servicio de red.

Configuramos el servicio por puerto 1194 que fue el que dejamos por default.

Imagen 89. Configuración de puerto.

Configuramos el cortafuegos, configuramos las reglas.

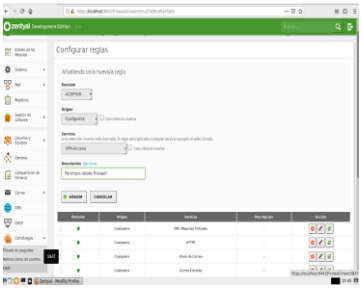


Imagen 90. Configuración de reglas.

Configuramos los paquetes de descarga del cliente en este caso se realizará desde un cliente Windows.

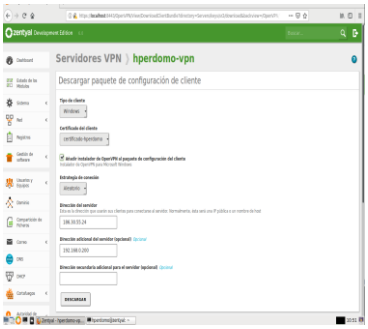


Imagen 91. Configuración de paquetes.

El servicio ya se encuentra arriba ejecutándose.

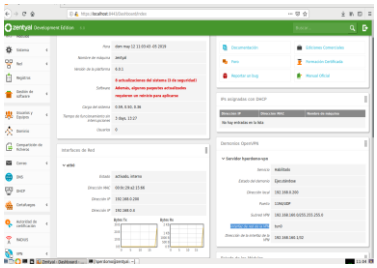


Imagen 92. Validación de comunicación.

Realizamos la descarga de los paquetes de conexión.

Imagen 93. Configuración de comunicación.

Instalación cliente en Ubuntu.

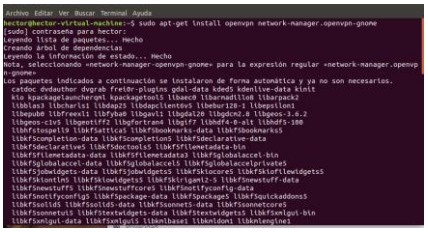


Imagen 94. Configuración ingreso usuario.

Creamos la conexión a través de la VPN en el cliente Linux.

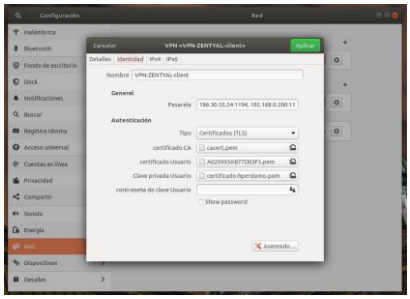


Imagen 95. Configuración cliente VPN.

Probamos la conexión desde un equipo Windows.

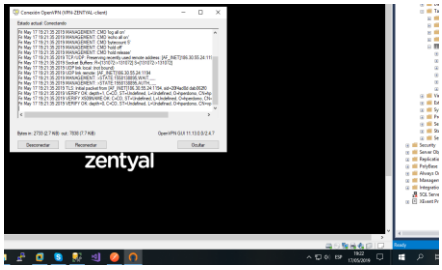


Imagen 96. Validación de servicio.

VIII. CONCLUSIONES

Aplicar los permisos y características básicos en el entorno de zentyal es muy importante ya que están limitados y sin su correcta configuración no funciona para el usuario cliente.

Las herramientas que ofrece el servidor zentyal son muy completas y ofrecen una gran ayuda, dando todos los servicios de configuración y control en el entorno de red para el control total de los usuarios.

Configurar y aplicar el servicio de proxy es muy útil ya que por medio de este podemos tener el control de los sitios web de los usuario, esto se puede hacer pro rangos o configuración de tiempo según los requerimientos del usuario.

Se realizó la instalación de zentyal como sistema servidor y se compara con un Windows server que sería más versátil empresarialmente.

Se adquirieron los conocimientos necesarios para la Instalación, configuración e implementación del servicio ofrecido por Zentyal Server 6.0, como en nuestro caso la configuración del servicio de Cortafuegos, opción que cumple una función importante en el control del tráfico en nuestra red, esto se logra con la creación de reglas de filtrado para la red interna. En donde se bloquearon páginas de multimedia y redes sociales como por ejemplo Facebook, YouTube y Twitter.

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

Zentyal VPN brinda la posibilidad de poder gestionarla de forma sencilla una gran cantidad de servicios sobre software libre con los mismos recursos de hardware.

Zentyal Server ofrece los servicios de compartir archivos, administrar un dominio, Proxy, Firewall, entre otros, prestando herramientas muy eficientes para empresas que requieran este tipo de soluciones.

REFERENCIAS

Apéndice A: Entorno de pruebas con VirtualBox. (2018). Obtenido de Zentyal Community: https://doc.zentyal.org/es/appendix-a.html

Configuración de un cortafuegos con Zentyal. (2018). Obtenido de Zentyal Community: https://doc.zentyal.org/es/firewall.html

Servicio de Proxy HTTP https://doc.zentyal.org/es/proxy.html

Esparza, F. (2017). Primeros pasos con ZentyaL [Archivo de video]. Disponible en: https://voutu.be/W18Cr7NBK'vw

rokitoh. (07 de 12 de 2016). Instalación y configuración de Zentyal Server 5. Obtenido de Red Orbita: http://red-orbita.com/?p=7634

zentyal. (2018). zentyal 6.0. Obtenido de zentyal.com: https://zentyal.com/