ZENTYAL SERVER, PUESTA EN MARCHA DE SERVICIOS DE INFRAESTRUCTURA TI

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI, Universidad Nacional Abierta y a Distancia UNAD
Cesar Augusto Millan Valencia
e-mail: cmvalencia.2014@outlook.com
John Stiven Vargas Escobar
e-mail: jhons_1101@hotmail.com
Guillermo Alberto Ramirez Pérez
e-mail: garamirezper@unadvirtual.edu.co
Lorgiam Arce Castaño
e-mail: larcec@unadvirtual.edu.co
Yadir Fabián Bejarano Varón
e-mail: yabej17@gmail.com

RESUMEN: *El presente artículo presenta la instalación y configuración y puesta en marcha de Zentyal Development Edition cómo opción de software para soluciones para infraestructura de servicios TI.*

PALABRAS CLAVE: Linux, Zentyal server, Ubuntu, servidor.

1 INTRODUCCIÓN

En el presente trabajo planteamos a Zentyal server en su versión 6.2, como servidor de servicios IT. Explicaremos su instalación, también la activación y configuración de algunos de sus módulos (servicios) como los son: DHCP server, DNS server, controladores de dominio, proxy no transparente, cortafuegos, Print Server y VPN.

2 INTALACIÓN DE ZENTYAL SERVER

La versión de Zentyal que instalaremos será la 6.2 en su distribución para desarrolladores, la cual es gratuita, ideal para una pequeña empresa y para mostrar algunos de sus servicios.

Una vez descargado el software de la pagina oficial de Zentyal, lo iniciamos para su instalación. En la ventana inicial elegimos el idioma.

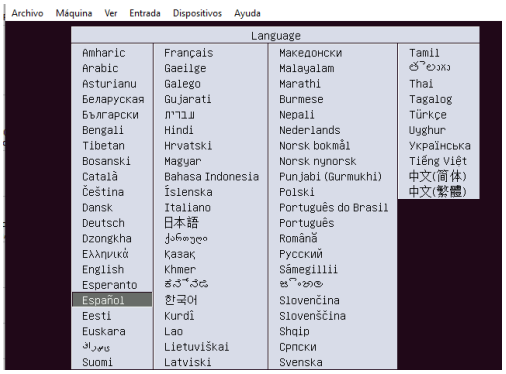

Figura 1. Selección del idioma

En la siguiente pantalla nos muestra las opciones de instalación con las que cuenta el software, en nuestro caso seleccionamos la primera opción.

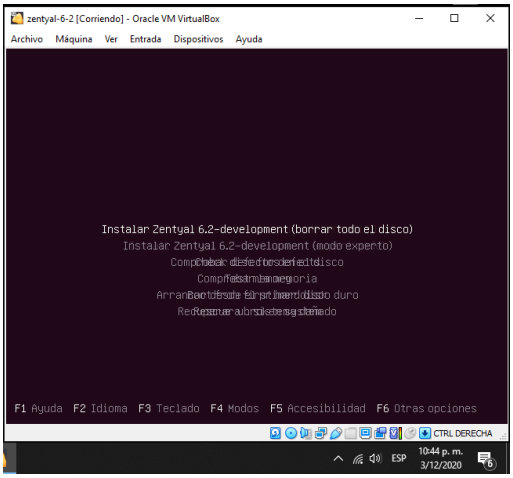

Figura 2. Tipo de instalación

Nuestra maquina tiene dos adaptadores de red, uno para la salida a internet (WAN) y otro para la red interna (LAN). En la siguiente pantalla seleccionaremos el adaptador que tiene la salida a internet.

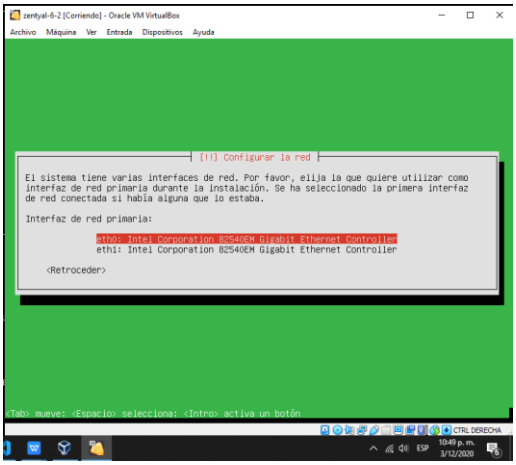

Figura 3. Configurar la red

En la siguiente pantalla debemos asignarle un nombre a la máquina.

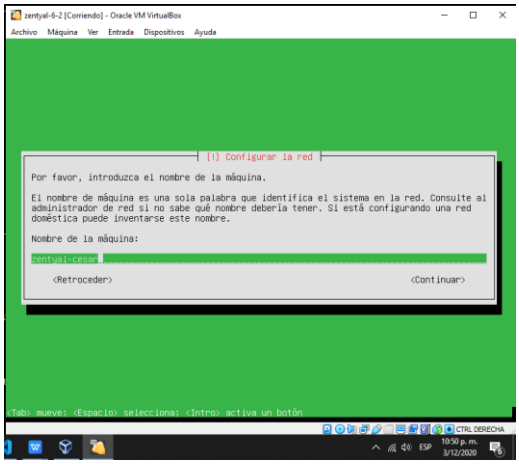

Figura 4. Asignación de nombre a la máquina

En esta etapa se configura una cuenta para el administrador del sistema. Iniciamos ingresando el usuario para el administrador.

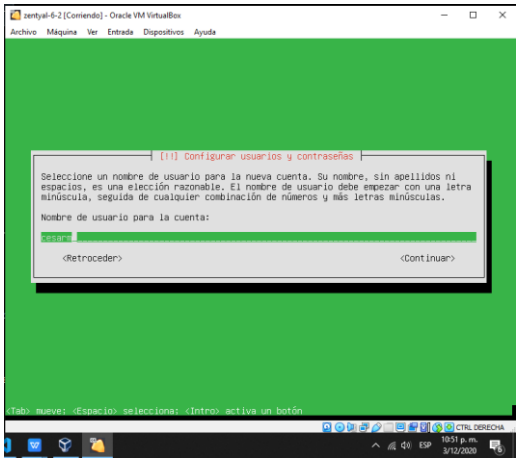

Figura 5. Configuración de usuario

Ahora procedemos a realizar la configuración de la contraseña para el usuario administrador.

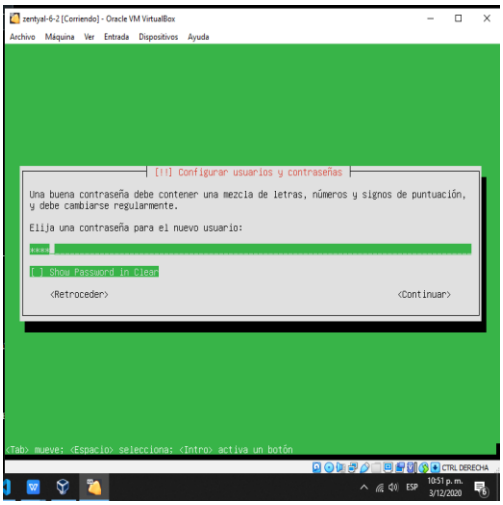

Figura 6. Configuración de la contraseña

En la siguiente pantalla nos despliega una ventana emergente donde nos indica la finalización de la instalación.

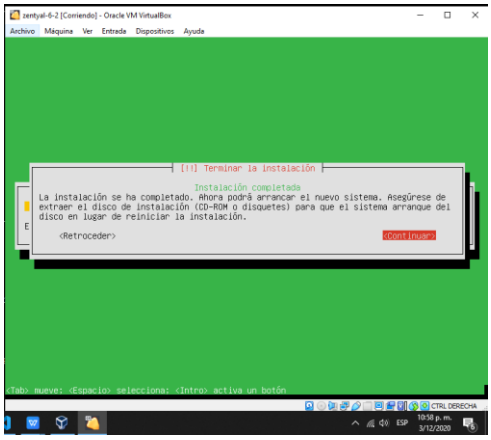

Figura 7. Finalización de la instalación

Terminada la instalación inicia el sistema.

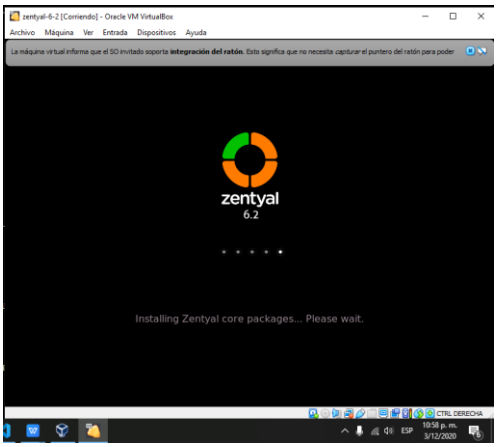

Figura 8. Inicio del sistema Zentyal

3 IMPLEMENTACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT

Una vez terminada la instalación de Zentyal, procedemos a la habilitación y configuración de algunos de sus módulos(servicios).

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Luego de la instalación de Zentyal se abre el navegador automáticamente seleccionamo los sistemas definidos que para este caso son: DHCP Server, DNS Server y Controlador de Dominio muestra una interfaz con las instalaciones que va a realizar.

Figura 9. Inicio del sistema Zentyal

Después de seleccionar el sistema se empiezan a instalar.

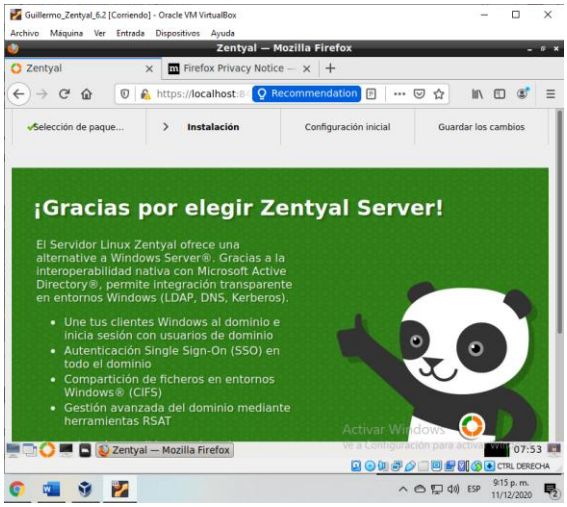

Figura 10. Instalación de paquetes

Después de aparecer la configuración de los tipos de redes de nuestro servidor, de manera que una gestione la salida a internet y otra los servicios internos en la red, una de ella con IP fija.

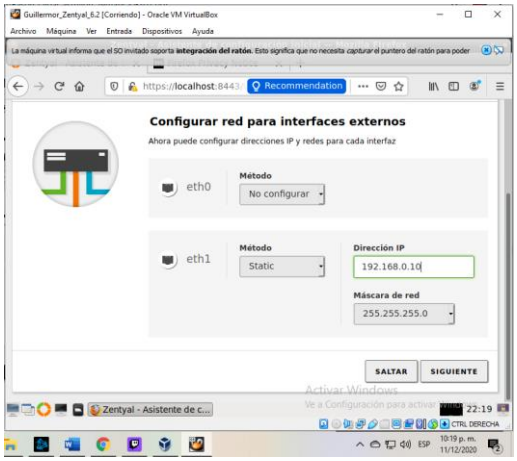

Figura 11. Configuración red

Aquí nos mostrara que domino que va a estar asociado a nuestro servidor y después procederá a su adecuación

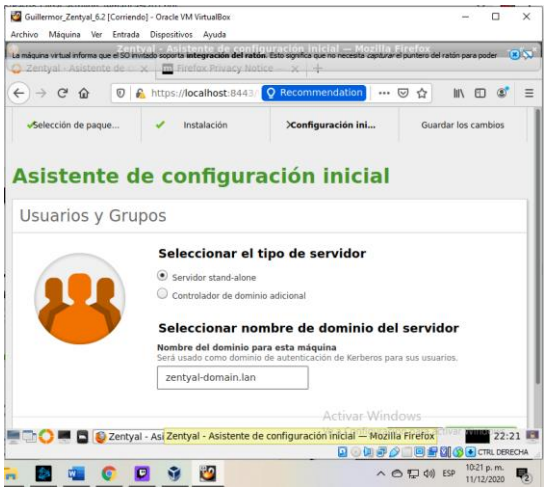

Figura 12. Configuración dominio

Finalmente culmina con las sus últimas adecuaciones y podemos acceder al Dashboard, con toda la configuración especificada

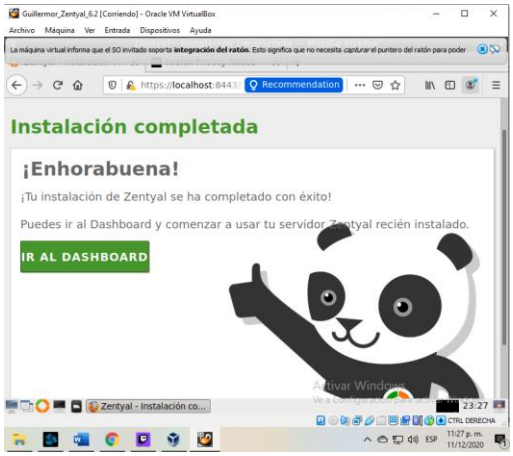

Figura 13. Configuración e instalación completa

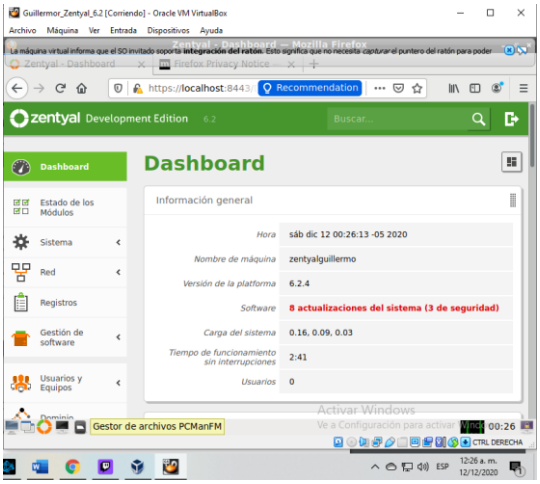

Figura 14. Interfaz Dashboard

Inicialmente se valida que los módulos hayan quedado instalados

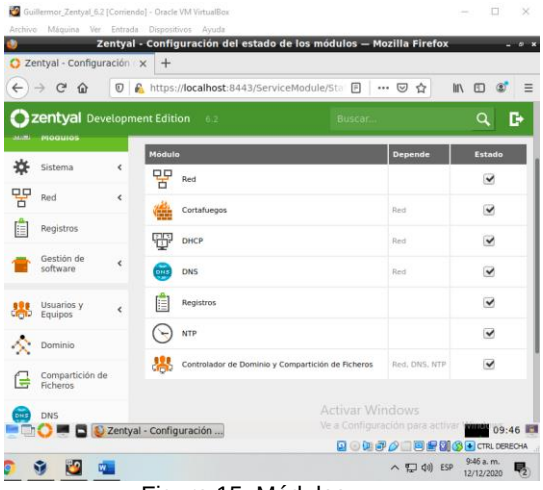

Figura 15. Módulos

Después pasamos a verificar nuestras interfaces de red

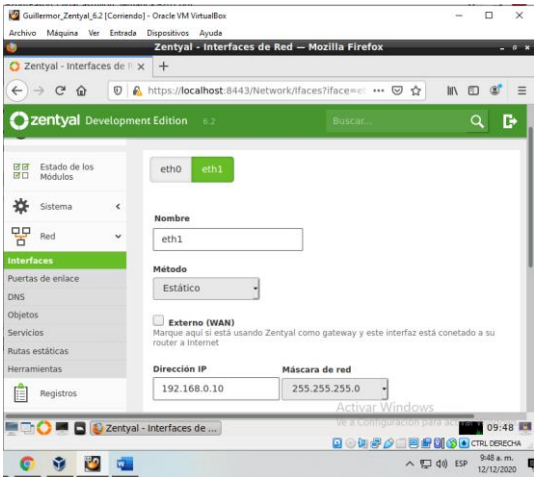

Figura 16. Interfaces de red

Luego vamos al menú que está a mano izquierda de nuestro panel y seleccionamos la opción DHCP.

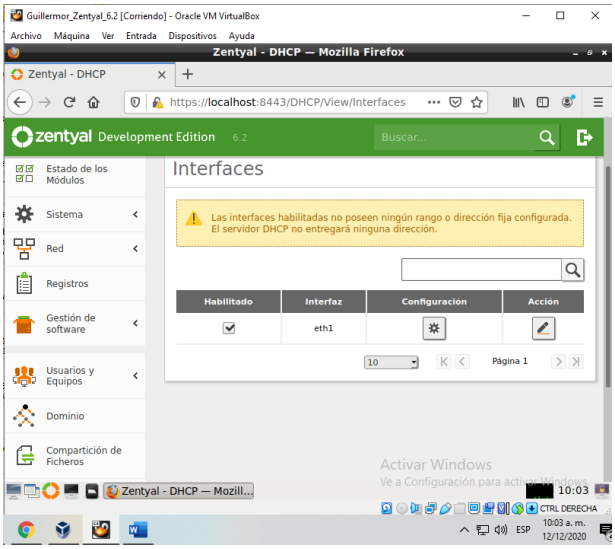

Figura 17. Configuración DHCP

En esta opción nos muestra la red que estamos trabajando, damos clic en Configuración, para comenzar a realizar las adecuaciones necesarias

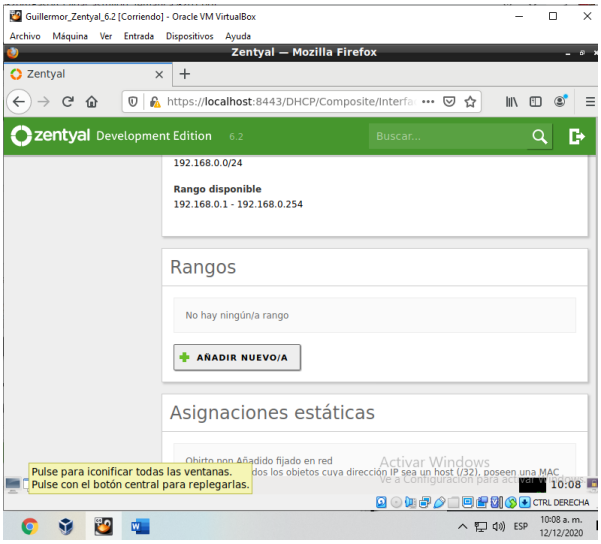

Figura 18. Configuración DHCP

Asignamos el rango de direcciones IP que pueden tomar nuestra red

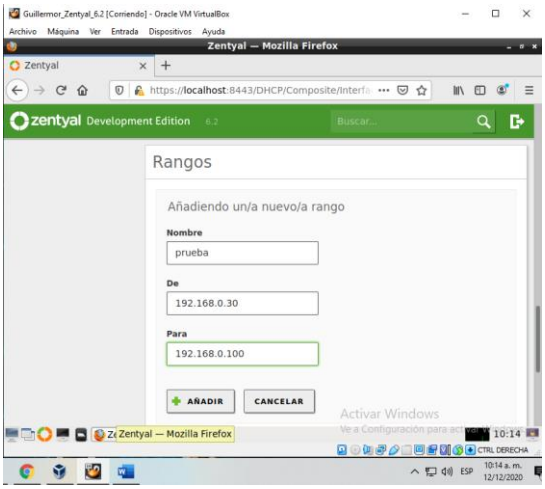

Figura 19. Rangos de IP

en la terminal de zentyal, procedemos a verificar si tiene conectividad.

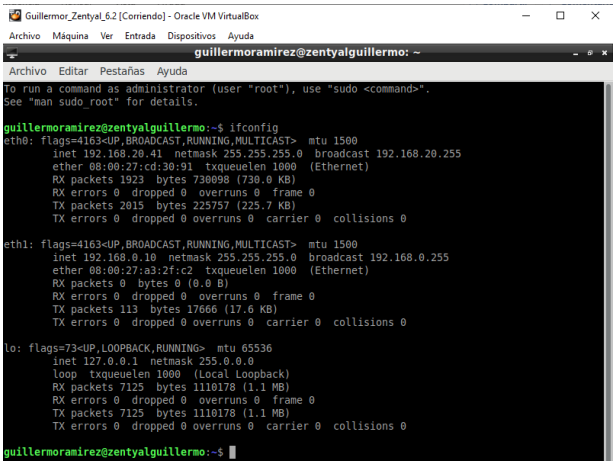

Figura 20. Verificación de red en Terminal

Nos desplazamos al escritorio de Ubuntu para verificar si el equipo está dentro de la red creada y si tiene conectividad con el servidor

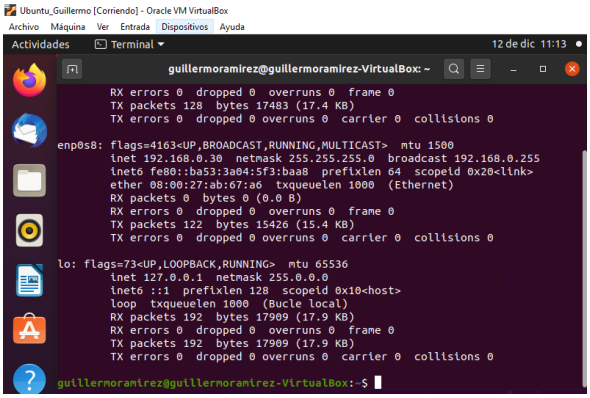

Figura 21. Verificación de red interna en Terminal de Ubuntu

Realizado la verificación nos damos de cuenta que dentro del panel de zentyal, nos nuestra la asignación de la dirección IP por medio del DHCP.

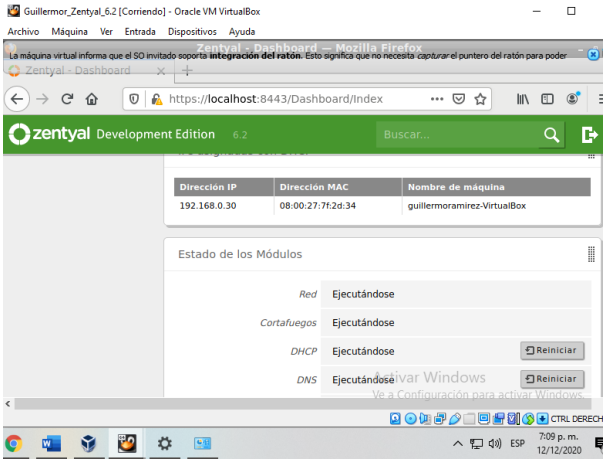

Figura 22. Verificación de la dirección entregada

Para la verificación del DNS, nos dirigimos nuevamente al menú a mano izquierda de nuestras pantallas, y seleccionamos la opción de DNS, aquí podemos verificar el nombre del dominio que se ha creado, el nombre de la máquina del servidor y su dirección IP.

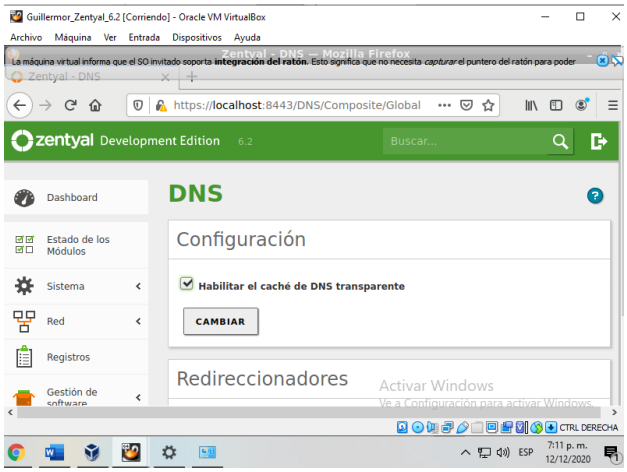

Figura 23. Configuración DNS

Para la verificación del Dominio, procedemos a dirigirnos a la opción de Domino que nos brinda el panel de zentyal, verificamos la asignación de los nombres entre otras configuraciones.

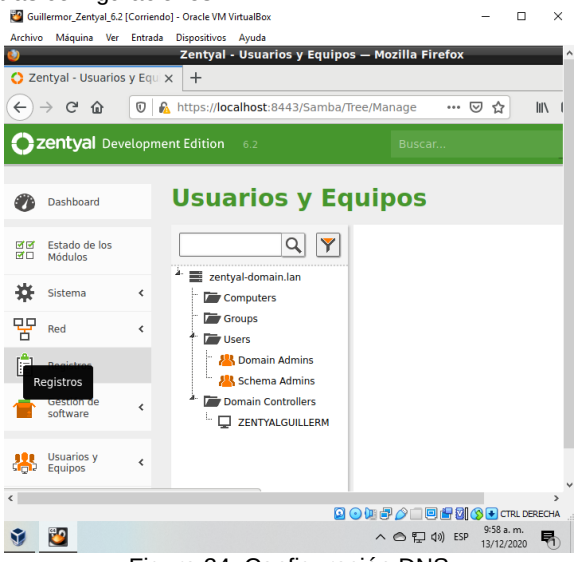

Figura 24. Configuración DNS

Procedemos a nuestro escritorio de Ubuntu y allí procedemos a instalar el paquete Pbis Open, la cual es una herramienta que permite unir Linux a un Active Directory

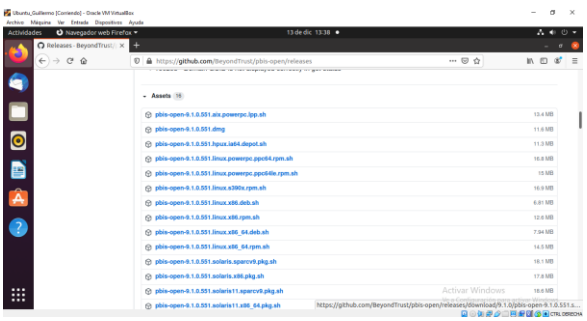

Figura 25. Descarga de Pbis Open.

Verificamos si tiene la configuración del dominio adecuada y que esté tomando los nombres adecuados

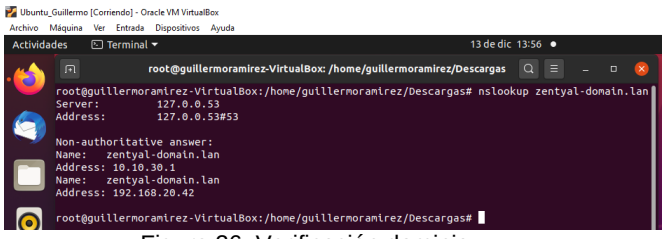

Figura 26. Verificación dominio.

Antes de unirlo al dominio en zentyal, en usuarios y equipos procedemos a asignarle un usuario y contraseña al administrador del dominio, para que nos genera error al momento de unir el equipo a nuestro dominio

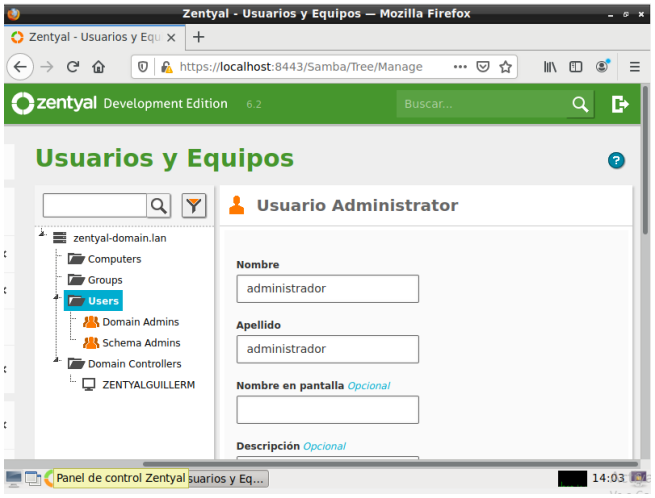

Figura 27. Configuración de usuarios

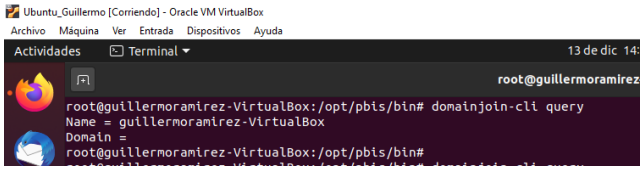

Figura 28. Dominio en la máquina de Ubuntu

Comprobamos en Zentyal si el equipo fue agregado al dominio.

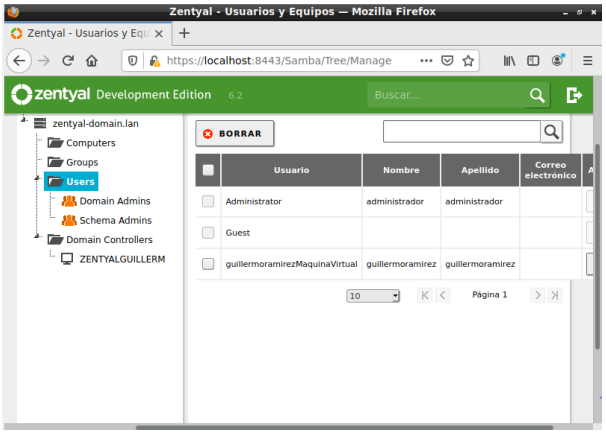

Figura 29. Dominio en la máquina de Ubuntu

3.2 PROXY NO TRANSPARENTE

Instalación del Servidor GNU/Linux Zentyal Server 6.2 (Instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT).

Procedemos la descarga del instalador Zentyal Server 6.2 desde la página: http://download.zentyal.com/

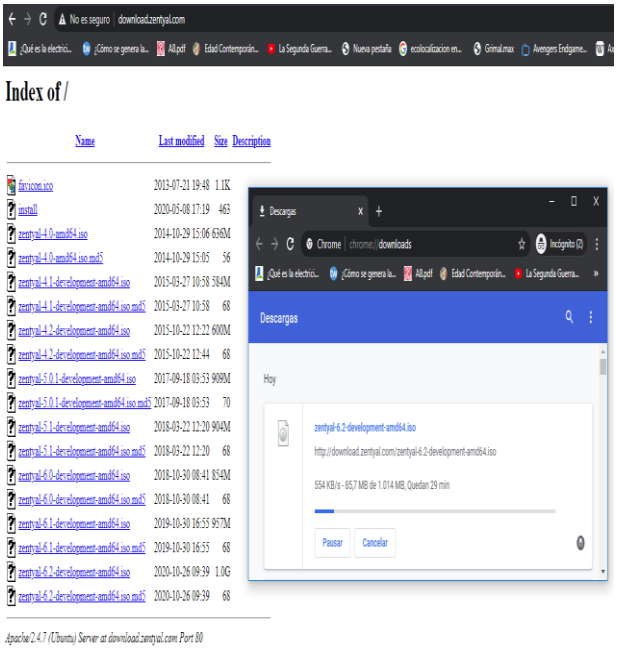

Figura 30. Instalación Zentyal Server

Se realiza el proceso de creación de una máquina virtual donde se configura con 2.048 de memoria y 20 GB de disco duro, también se configuran dos interfaces de red la primera con adaptador puente y la segunda con el modo de red interna.

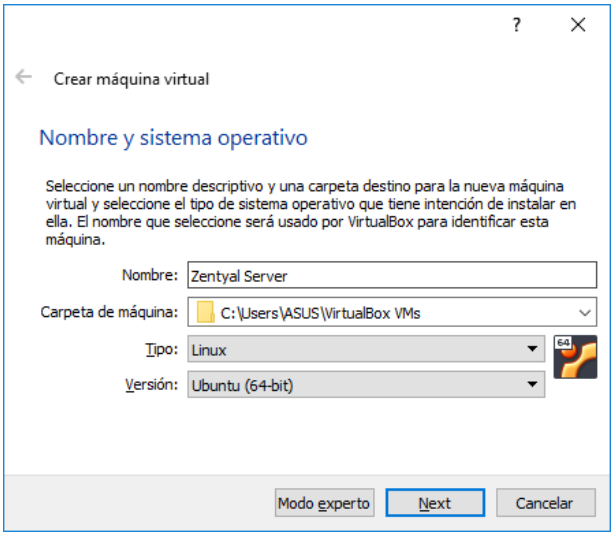

Figura 31. Instalación Zentyal Server

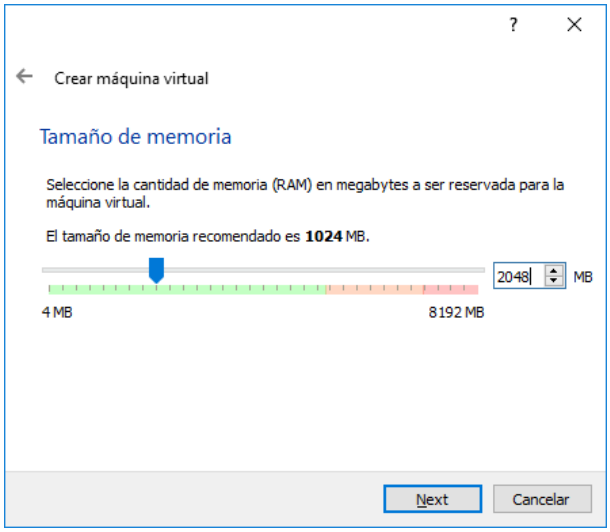

Figura 32. Instalación Zentyal Server

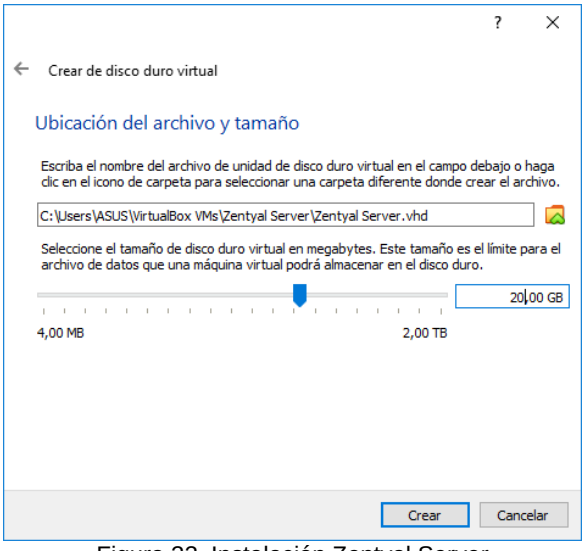

Figura 33. Instalación Zentyal Server

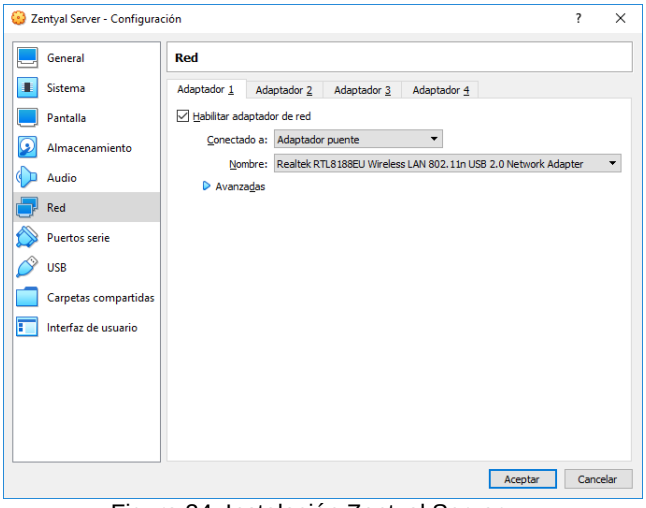

Figura 34. Instalación Zentyal Server

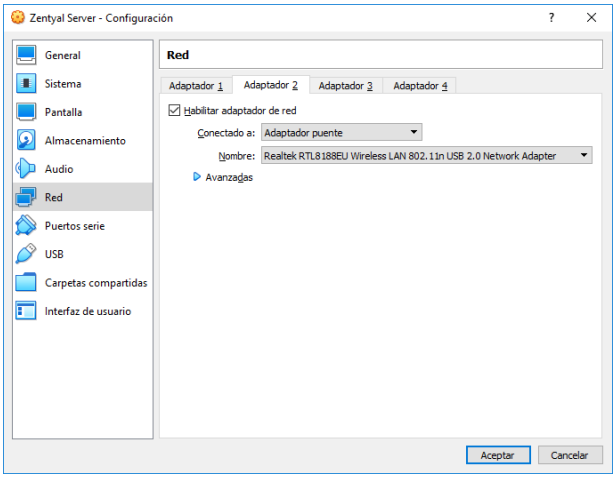

Figura 35. Instalación Zentyal Server

Una vez realizada la parametrización base de la máquina virtual procedemos a seleccionar el .ISO de Zentyal para iniciar la instalación. La instalación inicia con la selección del idioma. Selección del territorio y el idioma del teclado.

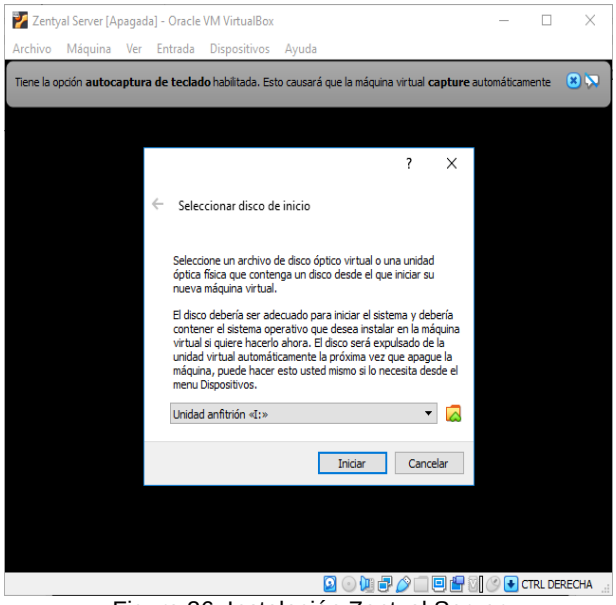

Figura 36. Instalación Zentyal Server

Figura 37. Instalación Zentyal Server

Figura 38. Instalación Zentyal Server

Figura 39. Instalación Zentyal Server

Figura 40. Instalación Zentyal Server

En esta sección del proceso de instalación se crea la cuenta y contraseña del usuario que servirá para la administración del servidor Zentyal, las cuales serán solicitadas terminando el proceso de instalación.

Figura 41. Instalación Zentyal Server

Configuración Usuario/Contraseña y realización proceso copiado e instalación del S.O.

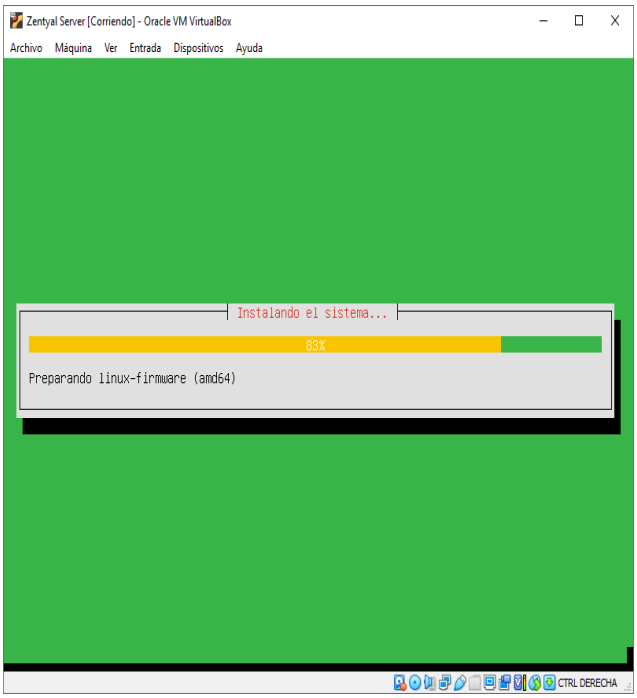

Figura 42. Instalación Zentyal Server

Figura 43. Instalación Zentyal Server

Configuración del Servidor:

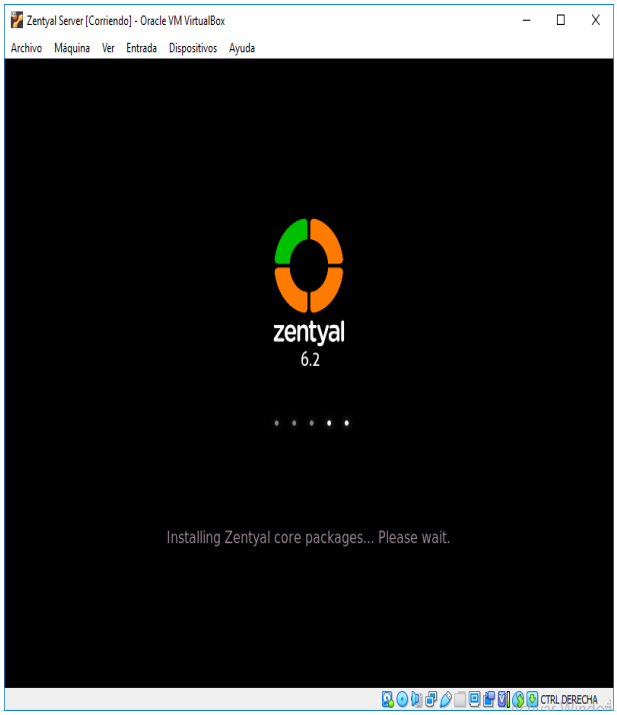

Figura 44. Configuración Zentyal Server

Figura 45. Configuración Zentyal Server

En esta sección iniciamos el proceso de configuración del Zentyal, donde se instalarán y configurarán los módulos Proxy. Para ingresar abrimos un navegador colocamos el usuario y la contraseña creadas anteriormente.

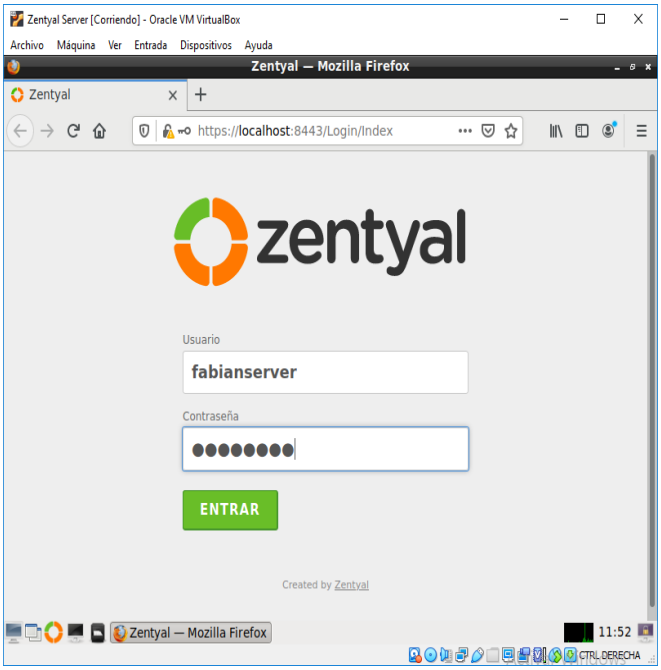

Figura 46. Configuración Zentyal Server

Figura 47. Configuración Zentyal Server

Seleccionamos el módulo a utilizar en el servidor del Zentyal: HTTP Proxy.

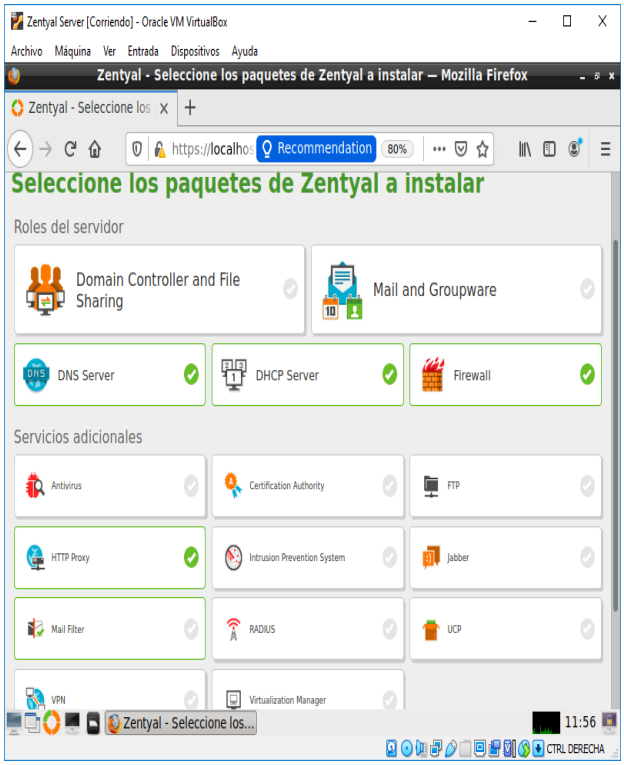

Figura 48. Configuración Zentyal Server

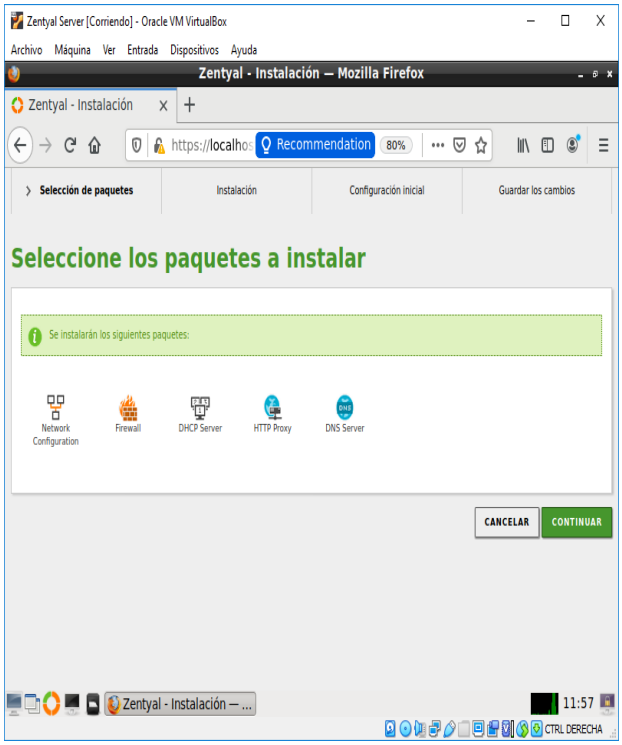

Figura 49. Configuración Zentyal Server

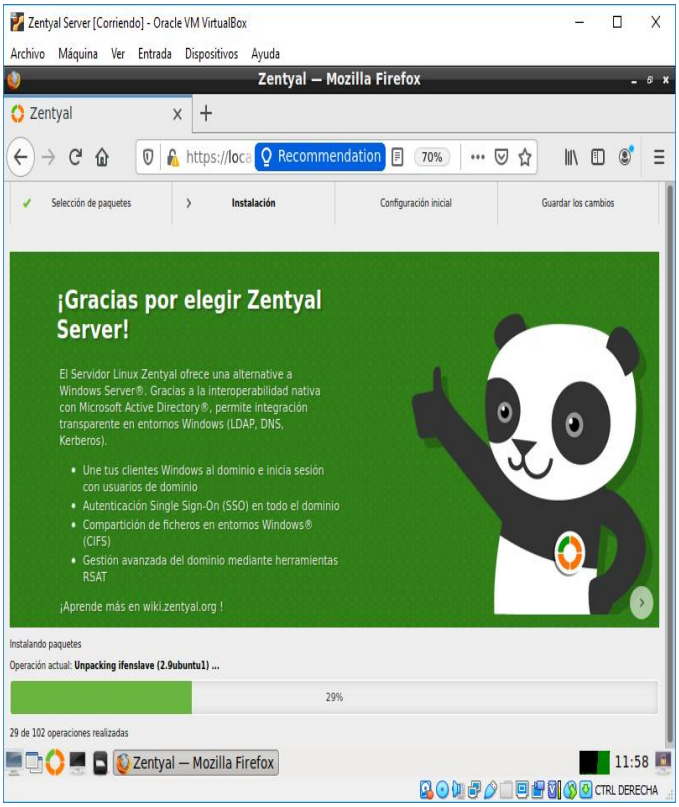

Figura 50. Configuración Zentyal Server

Ahora procedemos a realizar la configuración de las Interfaces de red, necesarias para activar el Proxy.

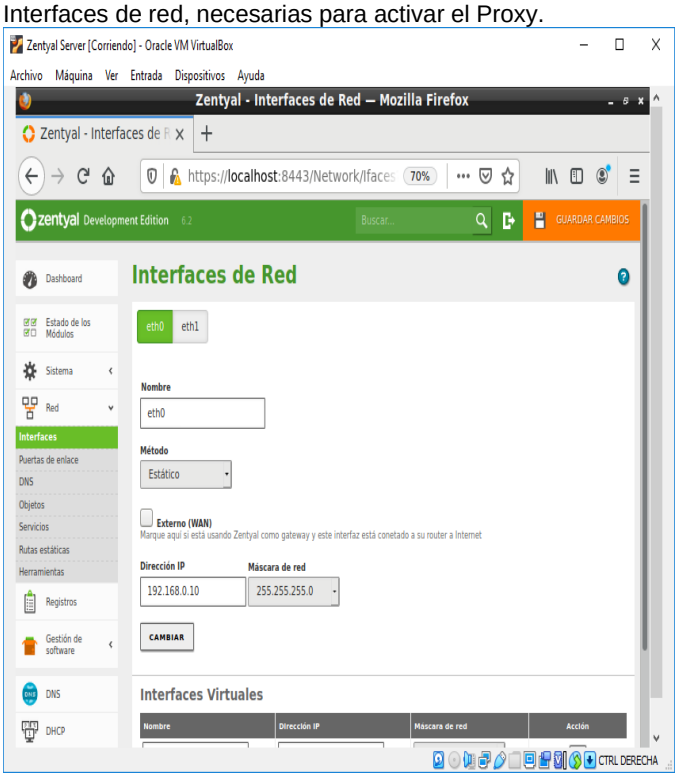

Figura 51. Configuración Zentyal Server

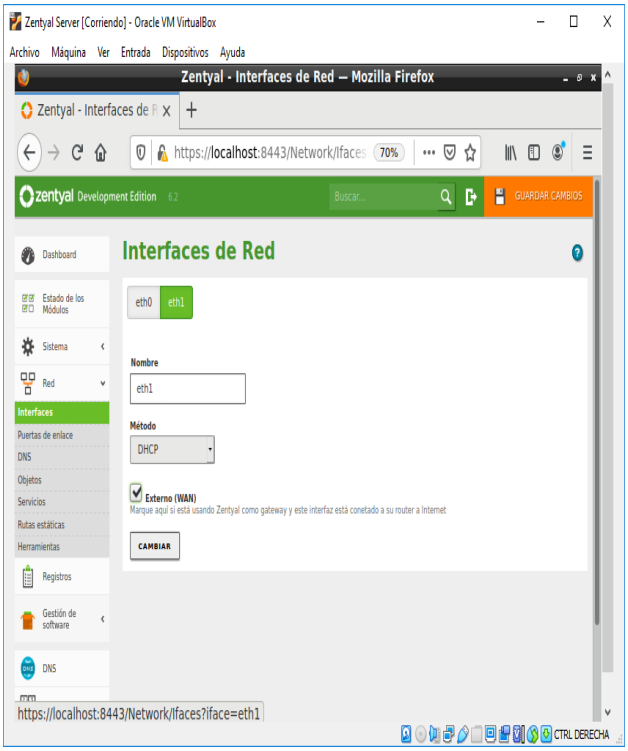

Figura 52. Configuración Zentyal Server

Validación de las IPs de las interfaces de red en el S.O. Zentyal

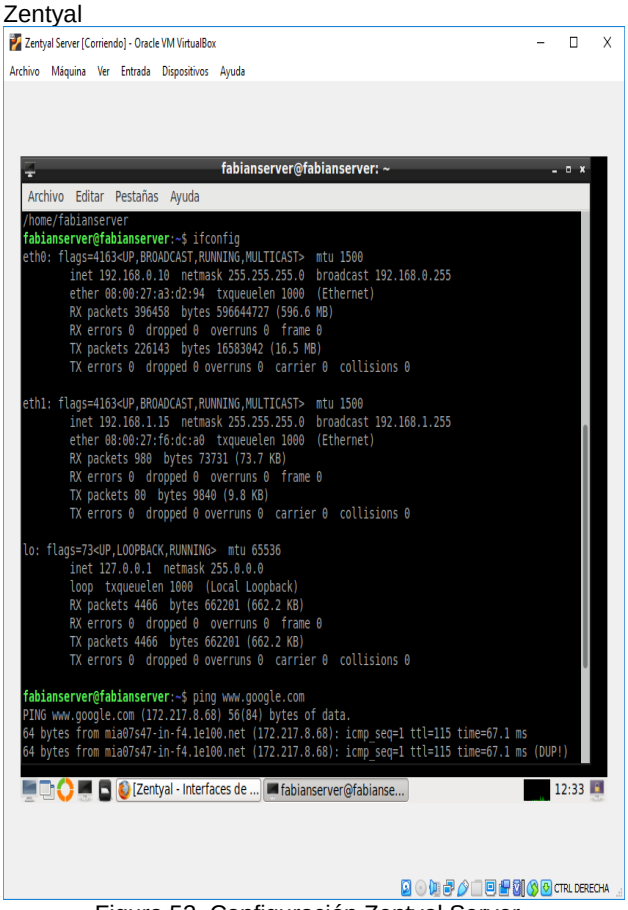

Figura 53. Configuración Zentyal Server

Continuamos con la Configuración del servicio Proxy No transparente. Es muy importante No seleccionar el check box “Proxy Transparente”

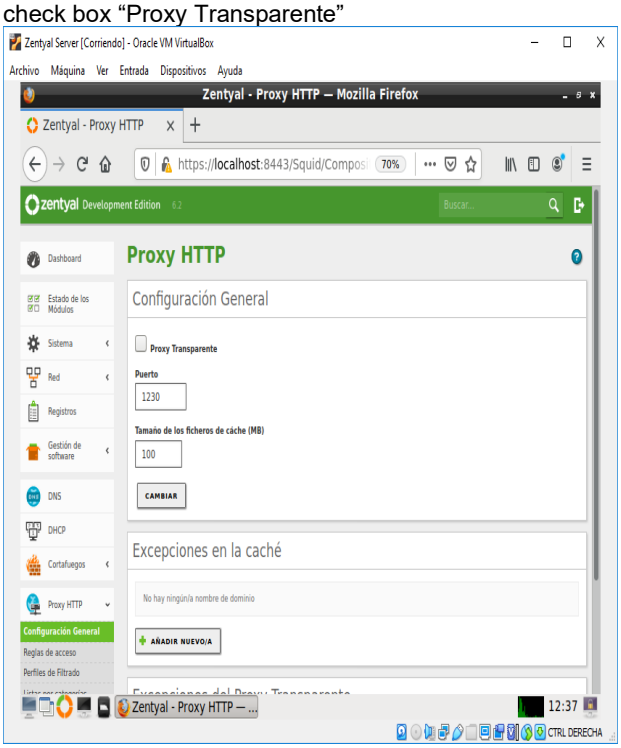

Figura 54. Configuración Proxy Zentyal Server

Configuración de Reglas de Acceso asociadas al Proxy No Transparente

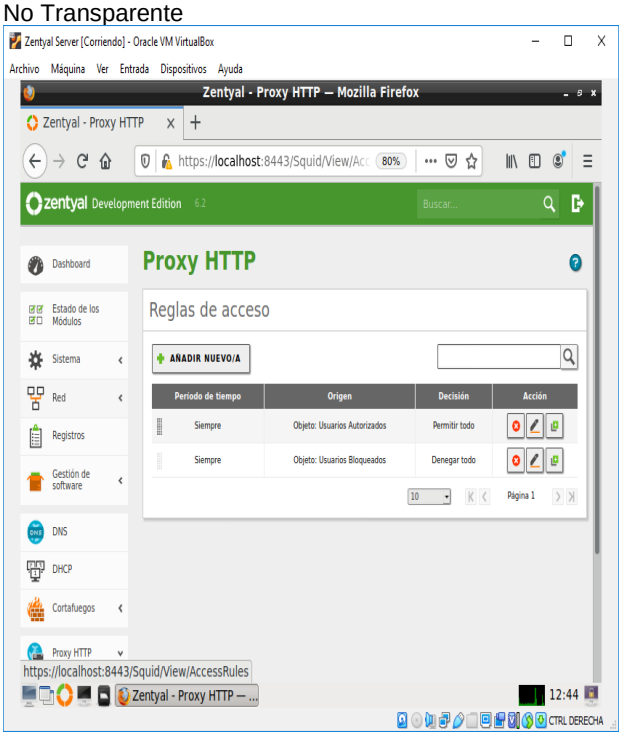

Figura 55. Configuración Proxy Zentyal Server

Creamos la Lista de objetos: Clientes Autorizados, la cual contendrá las IPs autorizadas para el acceso a la navegación en Internet a través del Proxy.

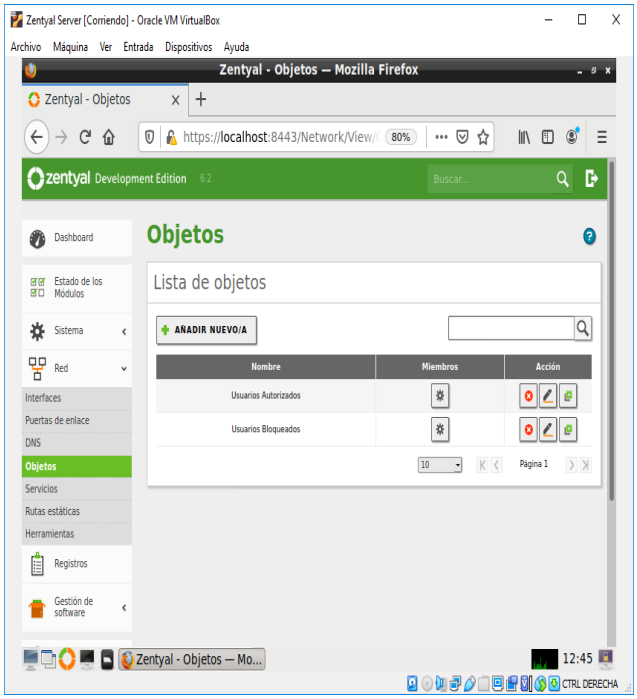

Figura 56. Configuración Proxy Zentyal Server

Creación de Objeto Clientes Autorizados con la IP del Cliente Ubuntu autorizado

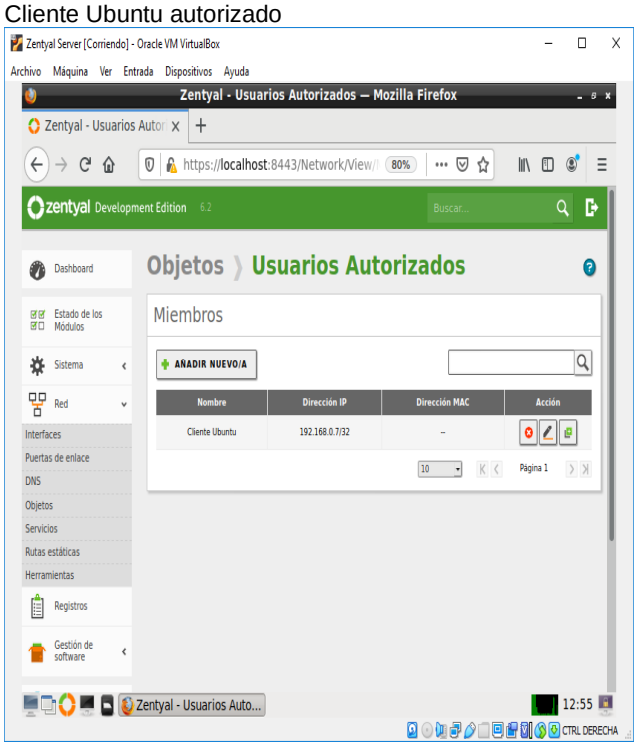

Figura 57. Configuración Proxy Zentyal Server

Finalmente realizamos la configuración en el Cliente Ubuntu Desktop para obtener acceso a Internet a través del Proxy preliminarmente configurado y habilitado.

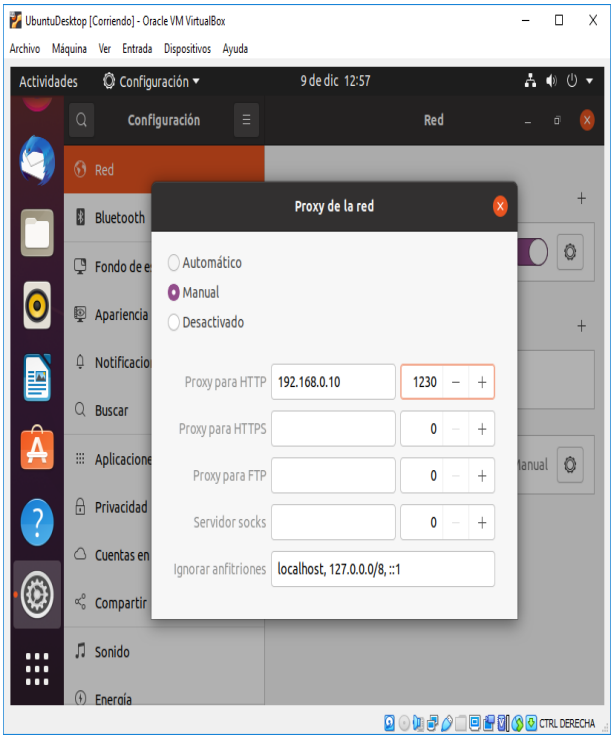

Figura 58. Configuración Proxy Zentyal Server

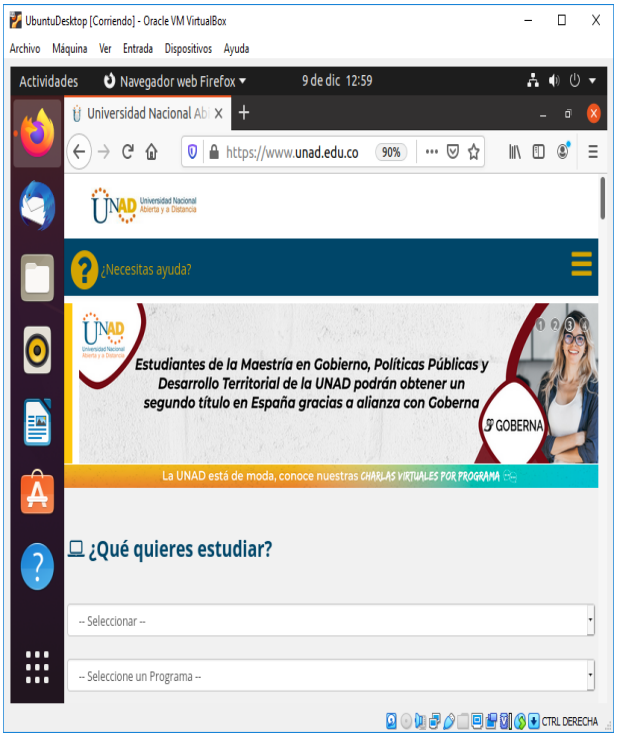

Figura 59. Configuración Proxy Zentyal Server

Ahora validamos la funcionalidad del control de acceso con el Proxy, realizando cambio en la configuración de la Lista de Clientes Bloqueados, agregando la IP del Cliente Ubuntu Desktop.

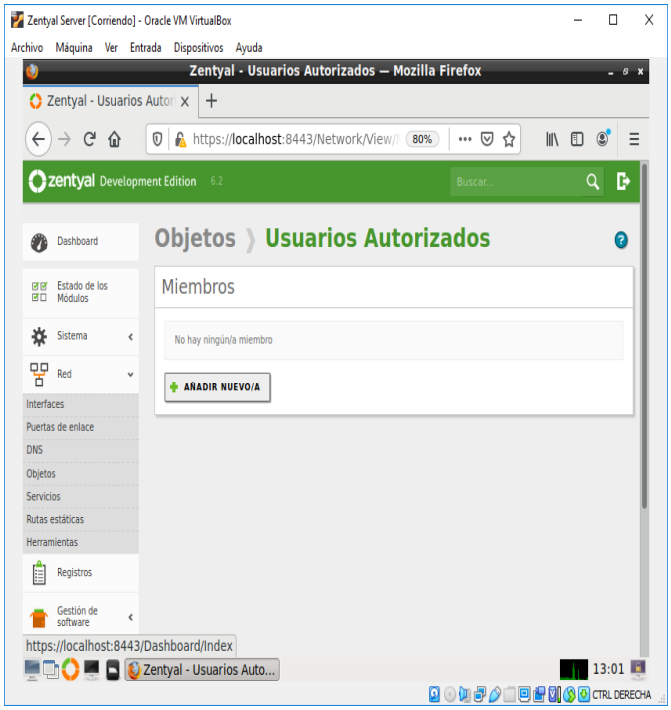

Figura 60. Configuración Proxy Zentyal Server

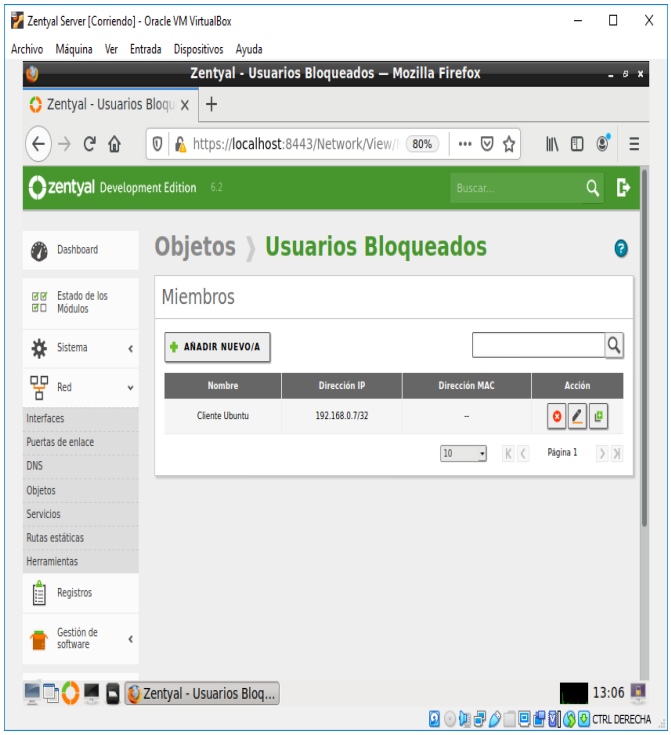

Figura 61. Configuración Proxy Zentyal Server

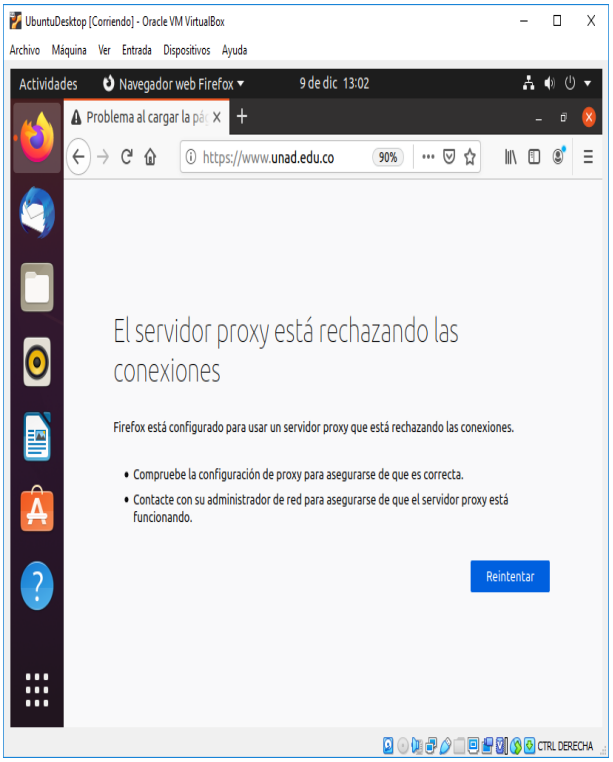

Figura 62. Configuración Proxy Zentyal Server

3.3 CORTAFUEGOS

Posteriormente a la instalación de Zentyal, se nos abre automáticamente el navegador con el sitio web en donde realizaremos la configuración de todos los elementos que necesitamos para la aplicación de la administración de la red dadas las necesidades de los servicios IT.

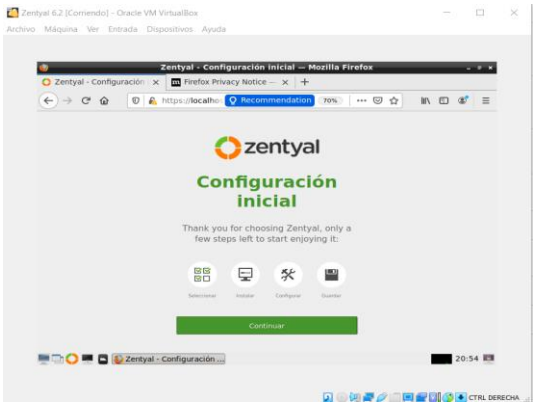

Figura 63. Configuración Inicial

Para el desarrollo de la temática seleccionaremos el paquete de Firewall, DHCP Server y DNS Server a instalar y la configuración de la red

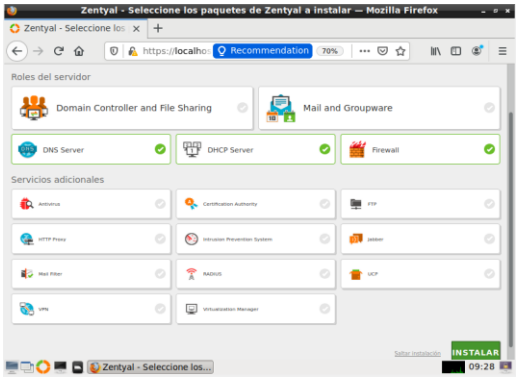

Figura 64. Gestor de Paquetes

Después de seleccionar los paquetes procedemos a la instalación.

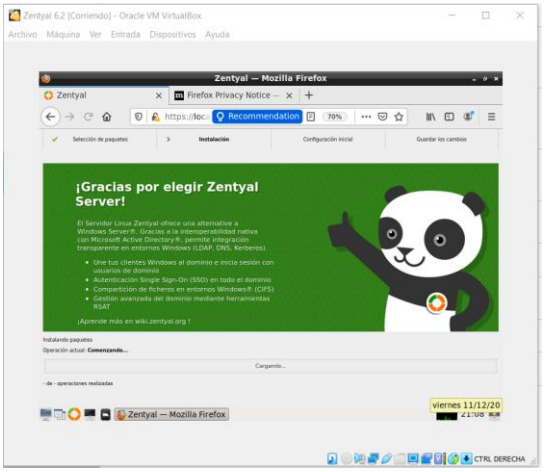

Figura 65. Instalación de Paquetes

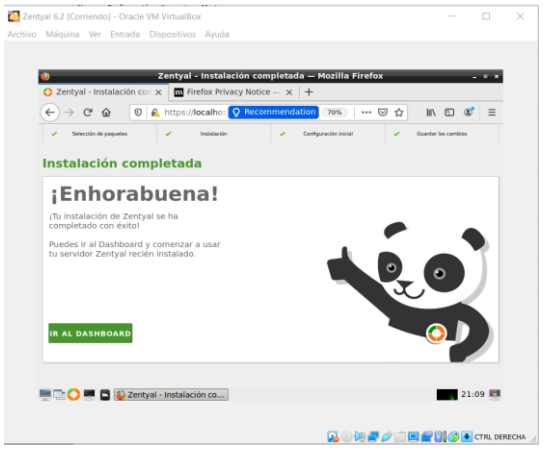

Figura 66. Finalización de Instalación

Nos envía a la página inicial (Dashboard)

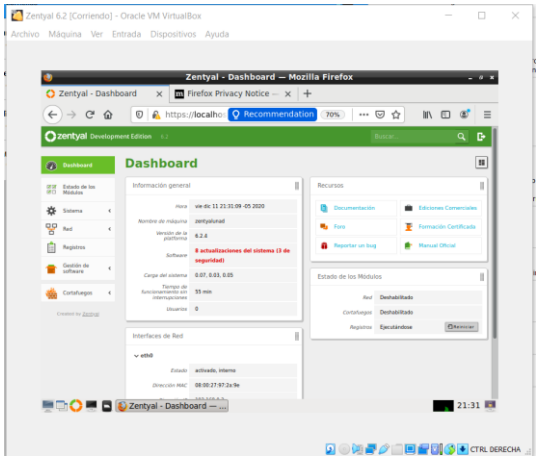

Figura 67. Dashboard Zentyal

Configuramos las interfaces de red, eth0 como externa (WAN) por DHCP y eth1 como interna (LAN) con IP estática 192.168.0.201

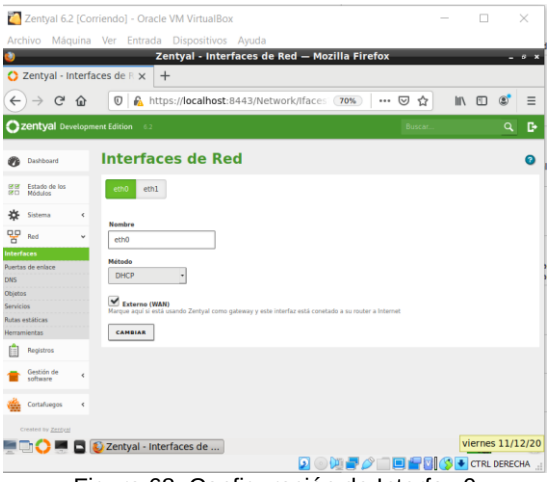

Figura 68. Configuración de Interfaz 0

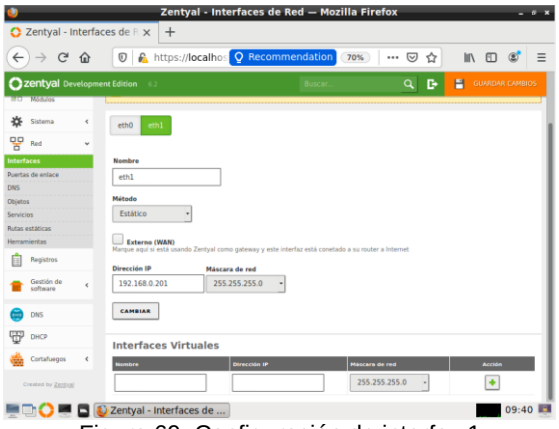

Figura 69. Configuración de interfaz 1

Para mejores efectos prácticos también configure el DNS Server y el DHCP Server, para el direccionamiento IP de la red interna.

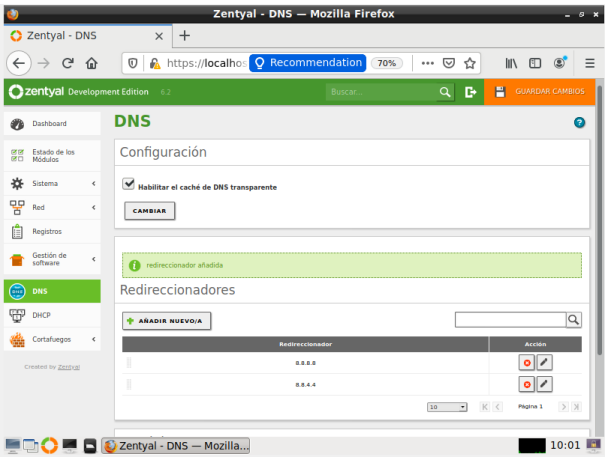

Figura 70. Configuración de DNS

Después de realizar la configuración del DNS, proseguimos con el DHCP Server

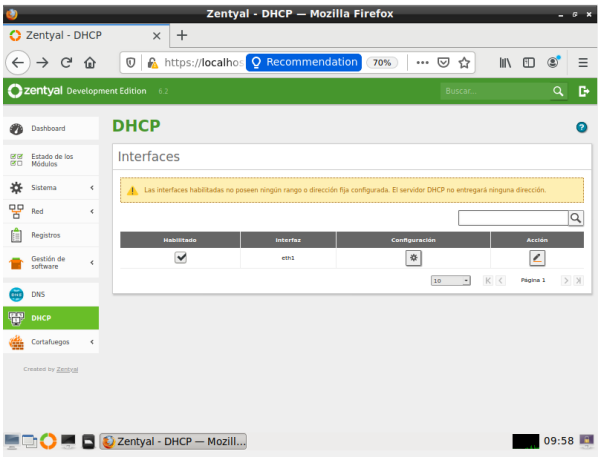

Figura 71. Configuración de DHCP

Configuramos Rango de Ips para el servidor DHCP

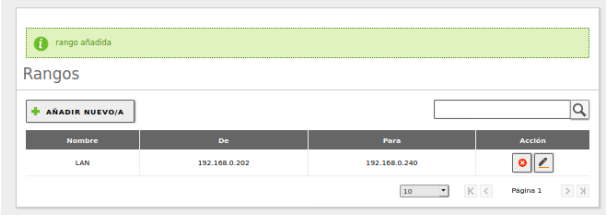

Figura 72. Configuración de Rango DHCP

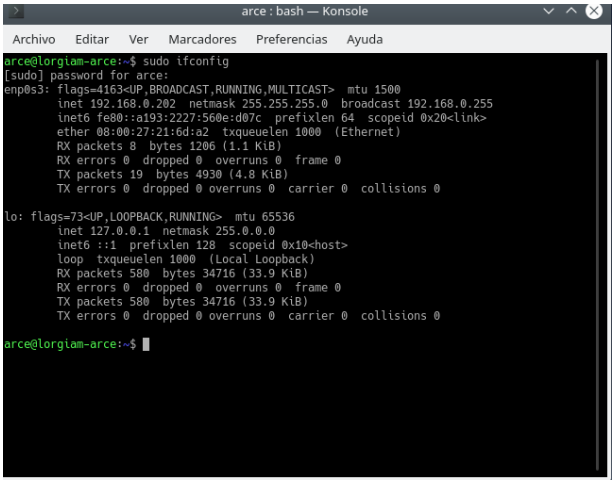

Figura 73. Validación de asignación de IP a Maquina Cliente

En el servidor Zentyal, en el apartado de red, creamos un objeto el cual nos va a agrupar los diferentes miembros a los cuales vamos a aplicarles las reglas del firewall, creamos el objeto UNAD

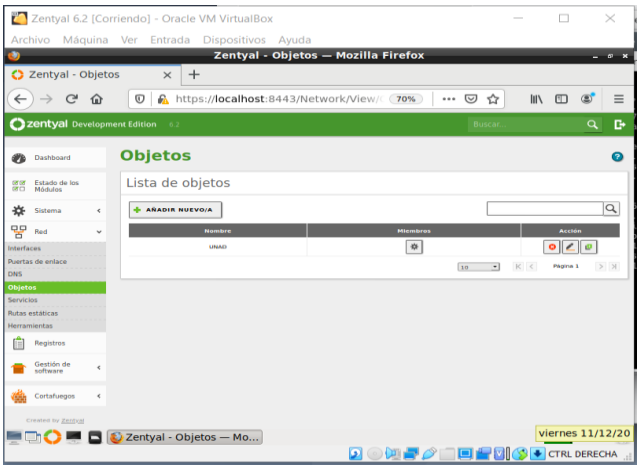

Figura 74. Creación de Objetos en la configuración de Red

Añadimos el rango de IP's a las cuales vamos a aplicar las reglas de firewall

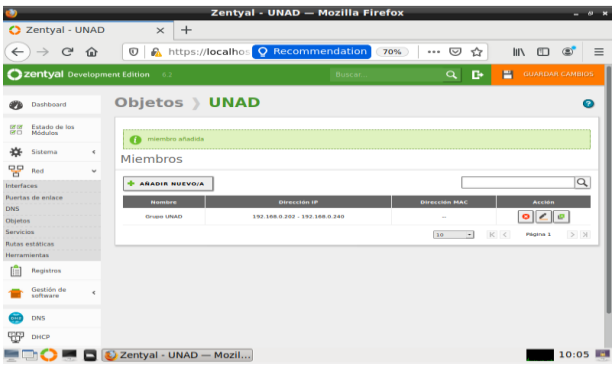

Figura 75. Asignación de Rango de IP's para el objeto creado

Ahora para conocer la ip a la que apunta nuestro host a internet para el sitio que vamos a bloquear corremos el siguiente comando ***host -t a <sitio-a-consultar>***

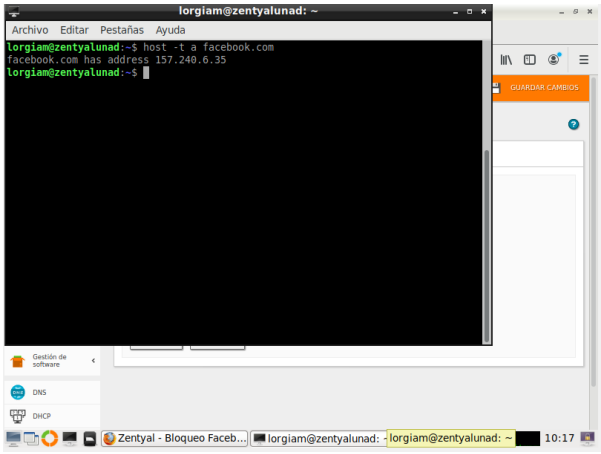

Figura 76. Validación de IP de sitio a bloquear

Para conocer el CIDR de la ip que obtuvimos anteriormente instalamos en zentyal el whois, con el siguiente comando ***sudo apt-get install whois***

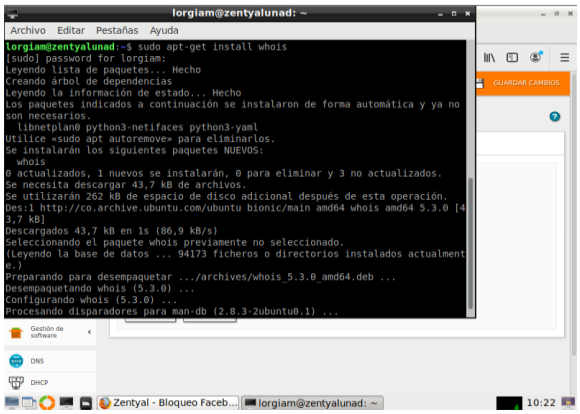

Figura 77. Instalación de Paquete Whois

Posteriormente corremos el comando ***whois <ip-obtenida> | grep CIDR***

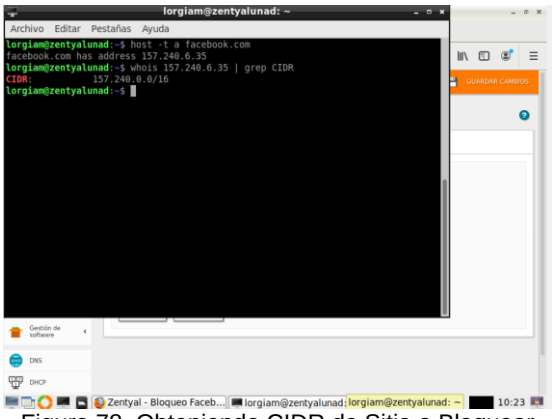

Figura 78. Obteniendo CIDR de Sitio a Bloquear

Ahora con el CIDR que obtuvimos, creamos un objeto en nuestra configuración de red para el bloqueo de los sitios específicos

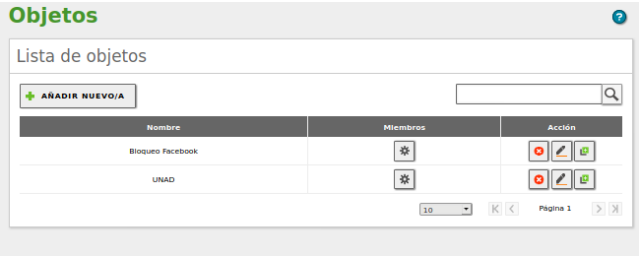

Figura 79. Creación de Objetos para los sitios a bloquear

Figura 80. Creación de los Miembros en los Objetos de los sitios a bloquear

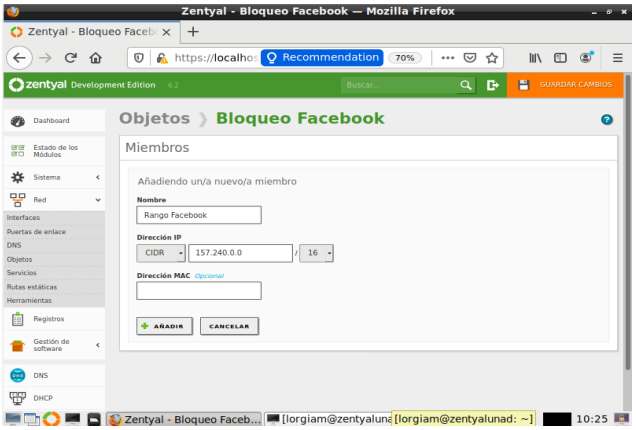

Figura 81. Asignación de CIDR a los Miembros de los sitios a bloquear.

Antes de crear las reglas validamos la conexión a estos sitios que deseamos restringir y podemos ver que se pueden acceder sin problemas

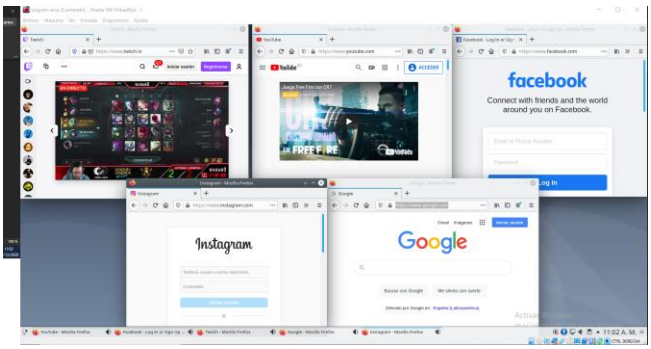

Figura 82. Validación de Acceso a los Sitios Web.

Ahora nos dirigimos al apartado de Firewall en el servidor Zentyal y seleccionamos la opción filtrado de paquetes, y allí ingresamos a la opción reglas de filtrado para las redes internas, damos en configurar reglas

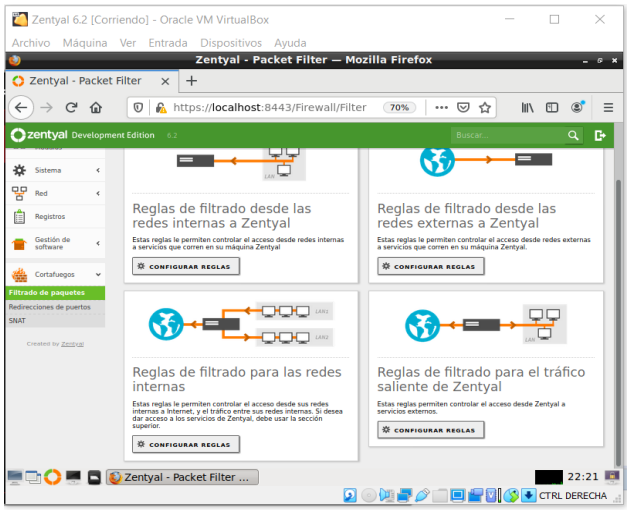

Figura 83. Panel Firewall

Creamos las reglas donde tomamos la decisión de aceptar o denegar ciertas conexiones, añadimos en el origen el objeto que creamos que contiene los diferentes miembros para que las reglas solo apliquen a estos, añadimos la IP destino que son las IPS de los sitios que deseamos restringe el acceso, para nuestro caso acceso a (redes sociales(Facebook e Instagram), y aplicaciones de entretenimiento como Youtube y Twitch)

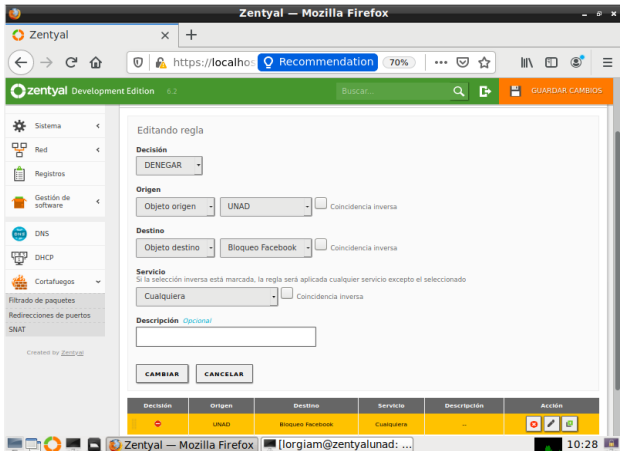

Figura 84. Creación de Regla de Denegación en el Firewall

Reglas creadas en el filtrado de paquetes de redes internas

Figura 85. Creación de reglas para los paquetes de redes internas.

Posteriormente creamos las reglas para el filtrado de paquetes de redes externas a Zentyal

Figura 86. Creación de reglas para los paquetes de redes externas.

Una vez creamos las reglas, probamos de nuevo la conexión y vemos que no nos permite acceder a las direcciones bloqueadas, solo nos da acceso a Google que fue la única que no bloqueamos

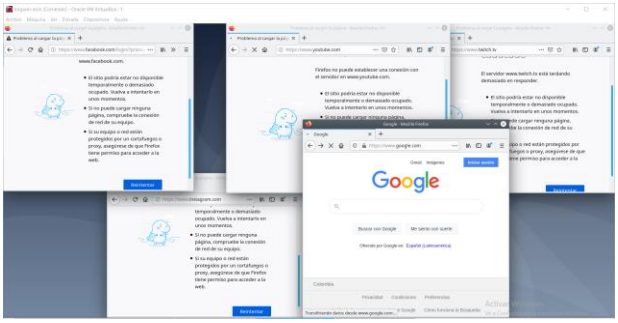

Figura 87. Validación de Acceso a los sitios bloqueados

De esta manera podemos crear las diferentes reglas para conservar la integridad del sistema y bloquear o restringir el acceso a páginas que no son destinadas para el uso en la organización

3.4 FILE SERVER Y PRINT SERVER

Una vez instalado los servicios necesarios, se procede a compartir impresoras.

Figura 88. Interfax Cups

Se selecciona la opción de “Add Printer”, añadir impresora y se selecciona la opción Internet Printing Protocol (ipps)

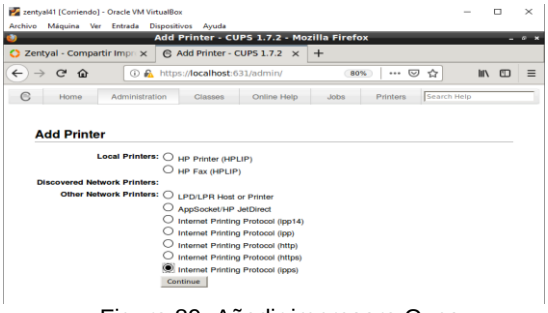

Figura 89. Añadir impresora Cups

Se define el nombre del recurso a compartir y se presiona continuar.

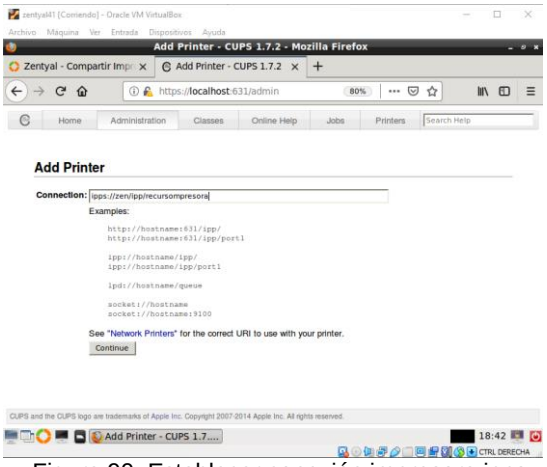

Figura 90. Establecer conexión impresora ipps

Se define el nombre del recurso compartido y se habilita la opción “Share this Printer” compartir esta impresora.

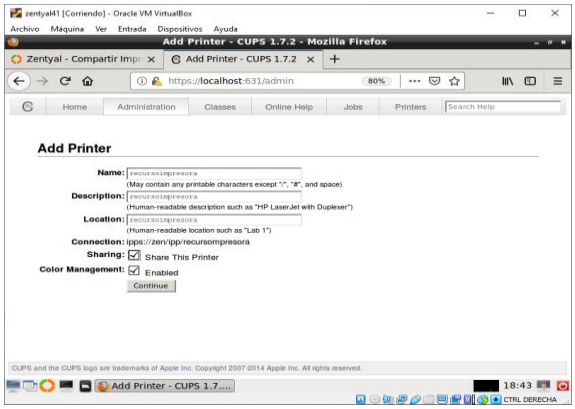

Figura 91. Definir nombre de la impresora compartida

Se selecciona el modelo y marca de la impresora a añadir y se presiona “Add Printer”.

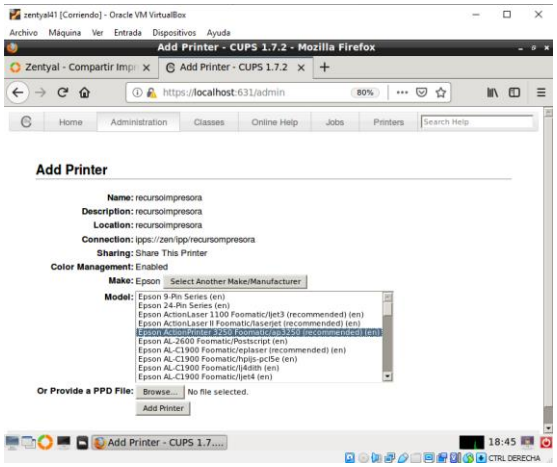

Figura 92. Selección de impresora a compartir

Se define el tamaño del papel y la resolución de impresión que tendrá por defecto la impresora compartida.

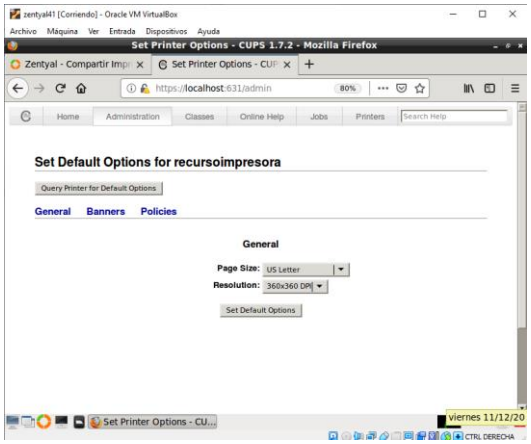

Figura 93. Selección hoja y resolución

Una vez se termine la configuración nos arroja esta hoja, la cual contiene la información para la confifuración en los equipos cliente para poder acceder a la impresora compartida.

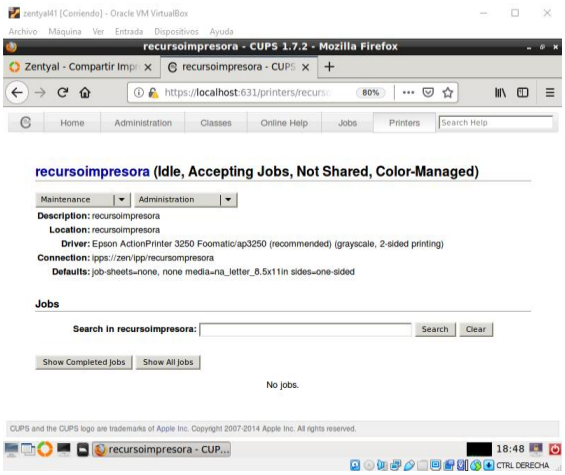

Figura 94. Datos de configuración impresora compartida.

En el equipo Cliente, Ubuntu 20 LTS, se configura la impresora con los datos provistos en la configuración.

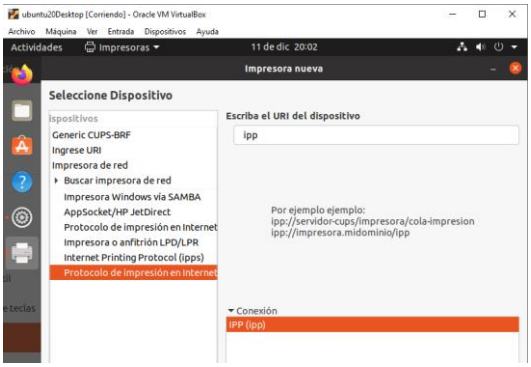

Figura 95. Configuración cliente impresora compartida

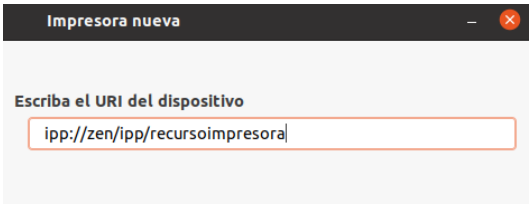

Figura 96. Establecer conexión cliente impresora compartida

Se selecciona la marca y modelo de la impresora.

Figura 97. Selección de marca y modelo impresora compartida cliente

Una vez terminada la configuración del recurso compartido se puede ver que la impresora quedó bien configurada y lista para usar en el equipo cliente (Ubuntu 20 LTS).

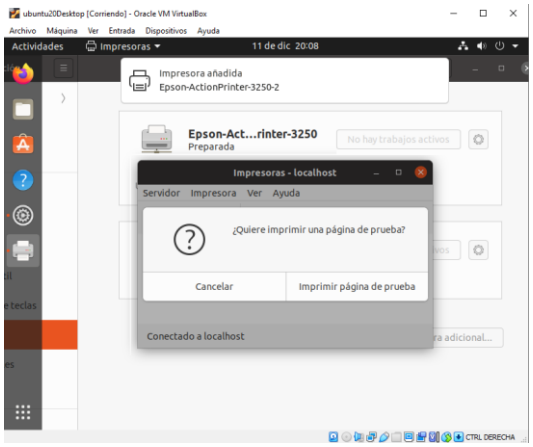

Figura 98. Comprobante de impresora compartida lista para usar

3.5 VPN

Una vez ingresamos con las credenciales del administrador, procedemos a seleccionar el paquete (Servicio) que seamos instalar; para nuestro caso seleccionamos el paquete “VPN”.

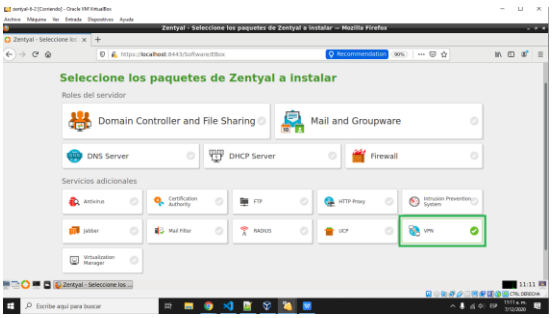

Figura 99. Seleccionamos el paquete a instalar

Al seleccionar el paquete que deseamos instalar y continuar con la instalación nos muestra otros paquetes que son prerrequisitos para el funcionamiento del paquete VPN. Damos continuar para que inicie el proceso de instalación de los paquetes listados.

Se recomienda tener el sistema actualizado antes de iniciar con el proceso de instalación de los paquetes.

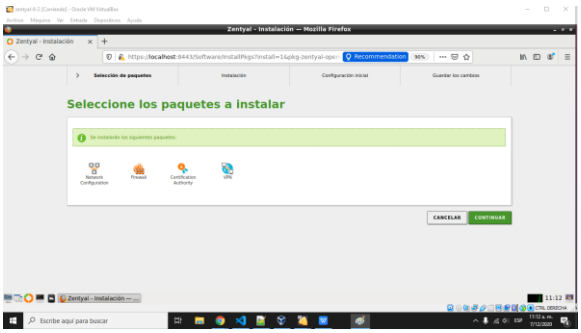

Figura 100. Paquetes prerrequisitos que se instalaran

Terminada la instalación de los paquetes pasa a la configuración inicial de las interfaces de red, para ello debemos indicar cual es la conexión externa (WAN) y cuál es la interna (LAN).

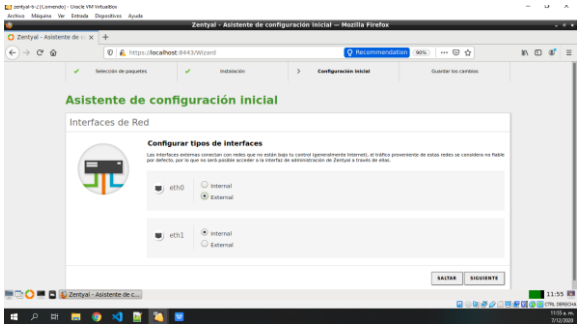

Figura 101. Configuración inicial

En la siguiente ventana debemos asignar una IP, la máscara de red y el método para la interface de red interna. Al terminar damos clic en el botón “FINALIZAR”.

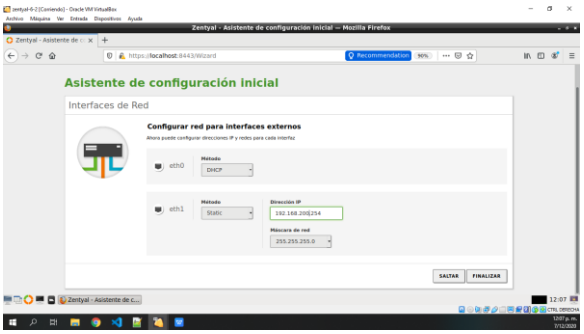

Figura 102. Configuraciones para las interfaces de red

Terminada la configuración inicial, nos dirige al dashboard en el cual podemos ver los paquetes instalados y la información de dichos paquetes activos.

Si damos ping a la IP que estaba expuesta vemos que no responde, esto es porque el firewall cerro la conexión para asegurar la red interna.

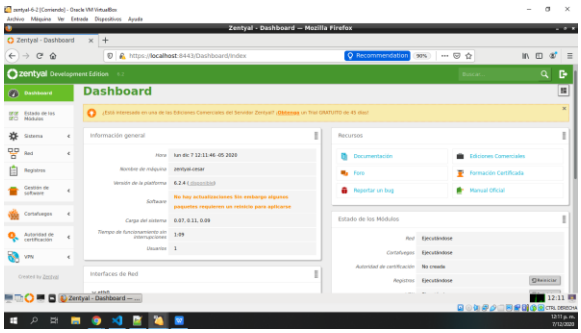

Figura 103. Dashboard

Debemos habilitar el cortafuegos, para ello nos dirigimos a “Registros” y en la pantalla desplegada nos ubicamos en la pestaña “Configurar los registros”. En la tabla desplegada buscamos el registro “Cortafuegos” y lo habilitamos.

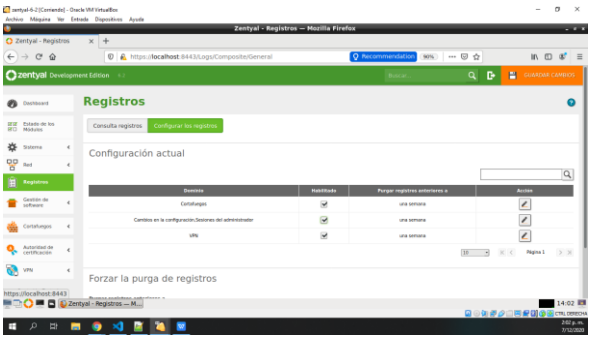

Figura 104. Habilitar cortafuegos

Ahora vamos a configurar la red interna para ello vamos a “Red” / “Interfaces”

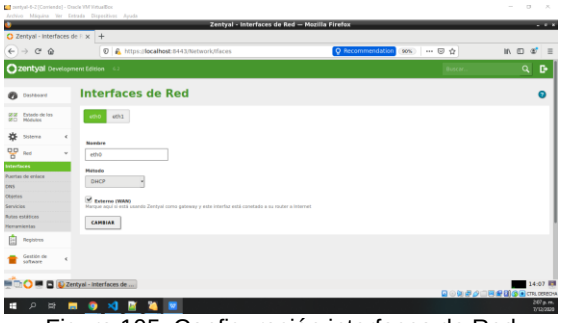

Figura 105. Configuración interfaces de Red

La interface de red “eth0” es la conexión externa, así que le cambiamos el nombre a WAN, el método lo cambiamos a estático, asignamos la IP y la máscara de red. Guardamos los cambios.

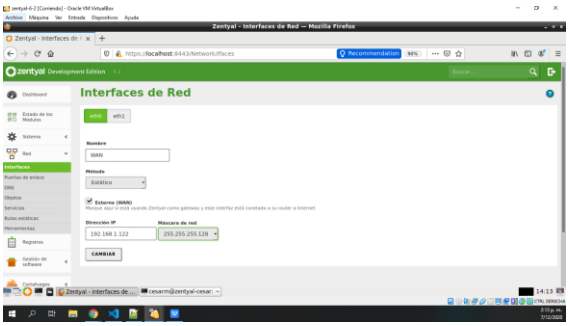

Figura 106. Configuración eth0 (red externa)

Ahora configuramos la interface de red “eth1” que será nuestra red interna. Le asignamos el nombre LAN, lo demás parámetros los dejamos igual. Guardamos los cambios.

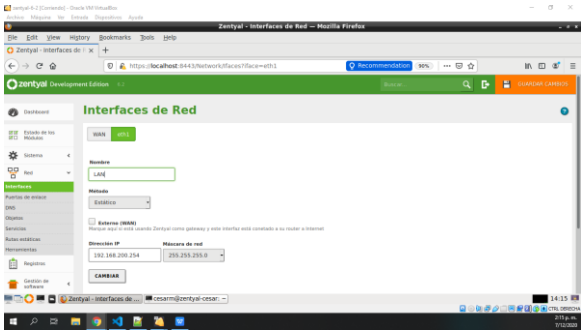

Figura 107. Configuración eth1 (red interna)

Ahora debemos configurar la puerta de enlace. Vamos a “Red” / “Puertas de enlace” y damos clic en el botón “AÑADIR NUEVO”. Le asignamos un nombre; en IP le asignamos la misma puerta de enlace que tenía antes, por último, damos clic en “AÑADIR”.

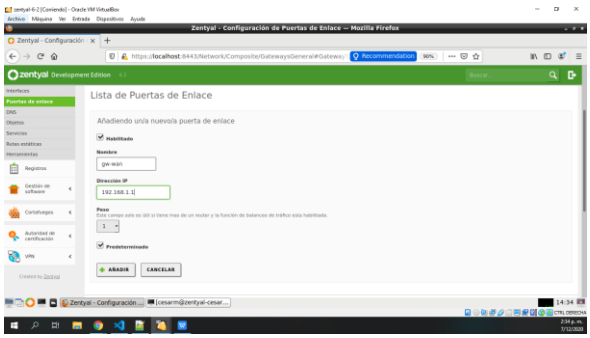

Figura 108. Configuración puerta de enlace

Ahora debemos crear una certificación, para ello vamos a “Autoridad de certificación”, Asignamos un nombre y la cantidad de días para expirar.

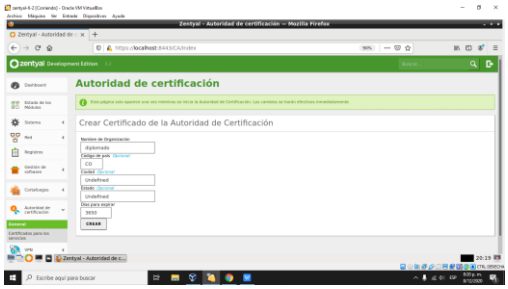

Figura 109. Crear autoridad de certificación

Configuramos la VPN, para ello vamos a “VPN” / “Servidores” y damos clic en el botón “AÑADIR NUEVO”, asignamos un nombre a nuestra VPN y lo habilitamos.

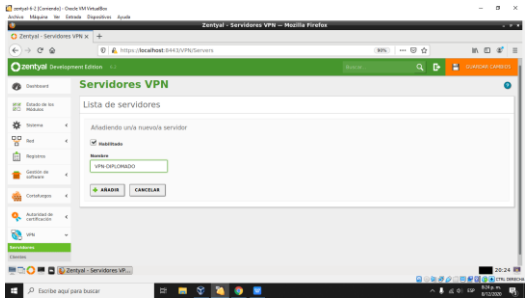

Figura 110. Crear servidor VPN

En la tabla donde se lista los servidores VPN creados debemos ubicar nuestro servidor y darle clic en configuración.

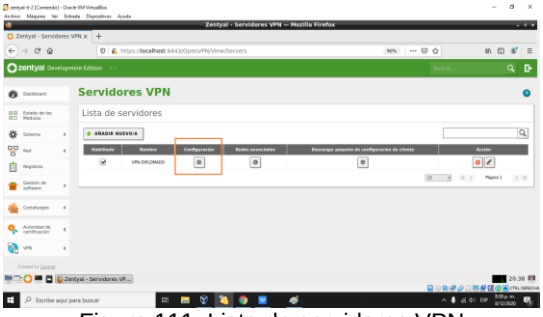

Figura 111. Lista de servidores VPN

Diligenciamos el formulario para la configuración del servidor.

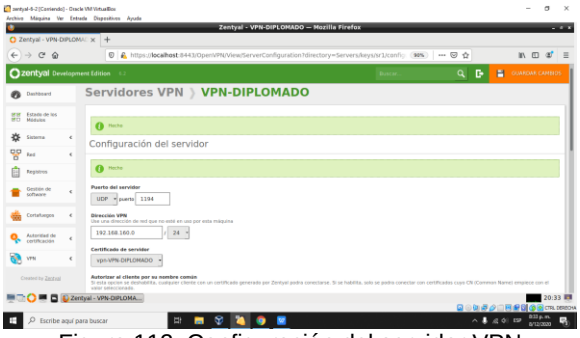

Figura 112. Configuración del servidor VPN

Descargamos el paquete de configuración para el cliente. Aquí encontraremos varios archivos que utilizaremos en la maquina desktop para establecer la conexión con openVPN.

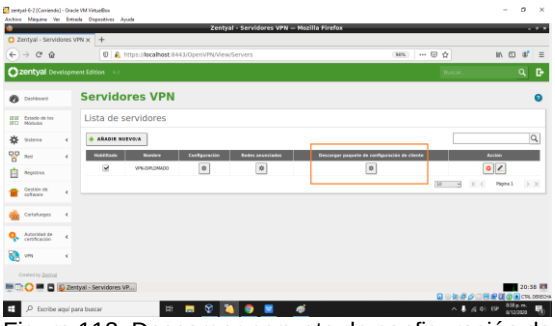

Figura 113. Descargar paquete de configuración de cliente

Realizamos la configuración para la conexión del cliente; debemos indicar el tipo de cliente, el certificado y la IP del servidor.

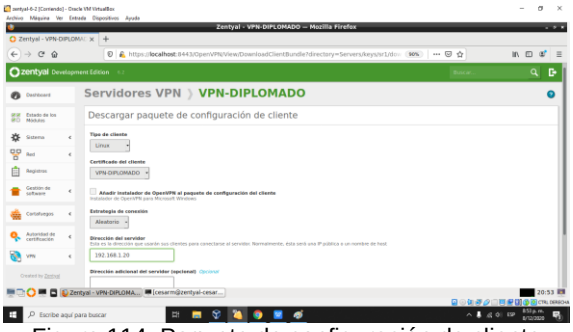

Figura 114. Paquete de configuración de cliente

Ahora nos vamos a nuestro desktop y realizamos la instalación de openVPN, programa por el cual estableceremos la conexión a nuestro servidor VPN.

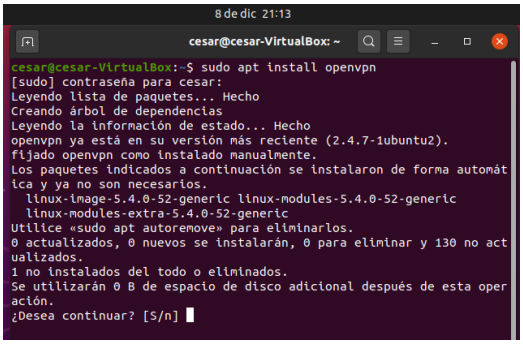

Figura 115. Instalación openVPN

El paquete de configuración lo copiamos en “/etc/openvpn”.

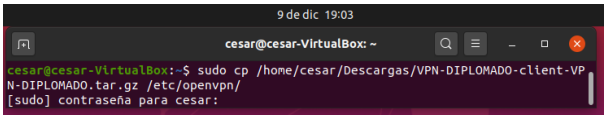

Figura 116. Copia de los archivos de configuración

Descomprimimos los archivos en el directorio “client” y el archivo de “.conf” lo dejamos en /etc/openvpn”.

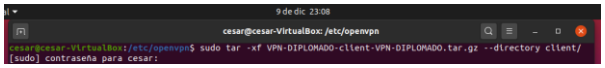

Figura 117. Descomprimos los archivos

Ahora nos ubicamos en la carpeta /etc/openvpn y ejecutamos el siguiente comando “sudo openvpn /etc/openvpn/documento-config-generado-client.conf” para conectarnos con la VPN.

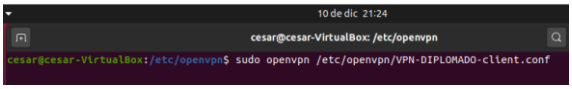

Figura 118. Estableciendo conexión con servidor VPN

Nos indica que la secuencia esta completada, es decir ya existe un tubo de conexión entre el servidor VPN y el cliente.

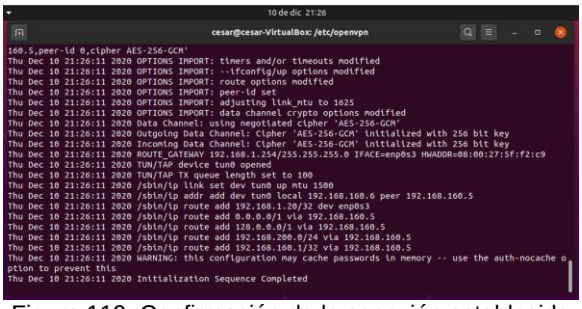

Figura 119. Confirmación de la conexión establecida

4 CONCLUSIONES.

Se logra comprender que Zentyal (Development Edition Edición Gratuita) es una herramienta completamente funcional para trabajar en entornos de producción profesional para pequeñas empresas, se presenta como una excelente solución a bajo costo, pues se puede virtualizar sin ningún problema o se puede instalar en una máquina que no sea muy costosa y tendrá un buen rendimiento.

Se le permite a equipos de red interna a tener su propio direccionamiento de IP, agregándose desde Zentyal cuándos equipos puede ser conectados en esta red interna y se pueden tener varias al tiempos si se desea.

Restringir el acceso a diferentes plataformas o sitios es de vital importancia, ya que permite conservar la seguridad e integridad del sistema, del mismo modo, con la implementación de las reglas del firewall, optimizamos la utilización de los recursos disponibles en la organización, debido a que plataformas como Youtube, Facebook, Spotify, entre otras, consumen ancho de banda y ralentizan la red.

5 REFERENCIAS

[1] Zentyal.org (2018). Es/vpn/Zentyal 6.2 Documentación official. Disponible en: https://doc.zentyal.org/es/vpn.html.

[2] Configuración del controlador del dominio en zentyal http://www.datebor.com/controlador-dominio-linux-zentyal/

[3] Instalación y configuración de zentyal - https://zentyal.com/es/news/tutorial-instalacion-y-configuracion-de-zentyal-server-para-la-implementacion-de-servicios-de-infraestructura-it/

[4] Configuración del servicio Squid - http://www.squid-cache.org/