Implementación de servicios de infraestructura IT a través de ZENTYAL Server 6.2

Hugo León Aguilar
hlaguilarr@unadvirtual.edu.co
John Anderson Hernández
jahernandezre@unadvirtual.edu.co
Pablo Andrés Villegas
pavillegasmo@unadvirtual.edu.co
Eddy Aristizábal
ejaristizabala@unadvirtual.edu.co
Jonathan Vergara Arango
jvergaraar@unadvirtual.edu.co

RESUMEN: *Se realiza la implementación de un servidor de control de dominio el cual se selecciona como producto a implementar el Zentyal 6.2 cumpliendo con el requerimiento de solucionar necesidades específicas, como la administración, control de los equipos definidos en la infraestructura, dirigida a implementación de servicios como DHCP, VPN, DNS, Firewall, Proxy no trasparente, permitiendo tener una infraestructura más completa, administrada y con un mayor control brindando una mayor seguridad.*

PALABRAS CLAVE: DHCP, DNS, dominio, file-server, grupos, LDAP, print-server, proxy, usuarios.

1 INTRODUCCIÓN

Se realiza el desarrollo para la implementación de los servicios requeridos y se deja la documentación como evidencia del paso a paso de la actividad realizada, la actividad está definida por la integración de un servidor Zentyal como controlador de dominio a la infraestructura, al igual que la integración de los servidores que se encuentran en este ambiente a este controlador de domino, con la documentación se deja cada uno de los pasos realizados para lograr los objetivos definido.

De esta forma se logra cumplir con cada uno de los puntos esperados en la implementación de cada una de las temáticas definidas para el logro del plan definido.

2 SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

2.1 INSTALACIÓN DE ZENTYAL SERVER 6.2

Se inicia el proceso de instalación con la descarga del producto Zentyal 6.2 desde el sitio oficial de Zentyal, https://zentyal.com/es/news/zentyal-6-2-announcement-2/ o es posible usar el enlace directo el cual es: http://download.zentyal.com/zentyal-6.2-development-amd64.iso. Una vez descargado el ISO se procede a realizar la instalación en el servidor aprovisionado, se realiza la carga del ISO como unidad booteable.

Se inicia la carga del instalador y se selecciona el idioma del instalador.

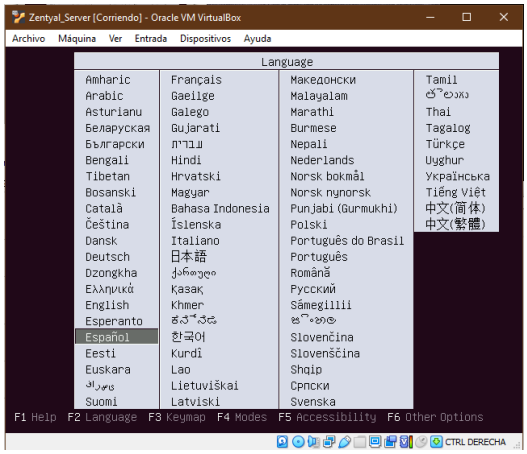

Figura 1. Selección de idioma.

Se selecciona el modo de instalación, el cual se realiza en modo experto.

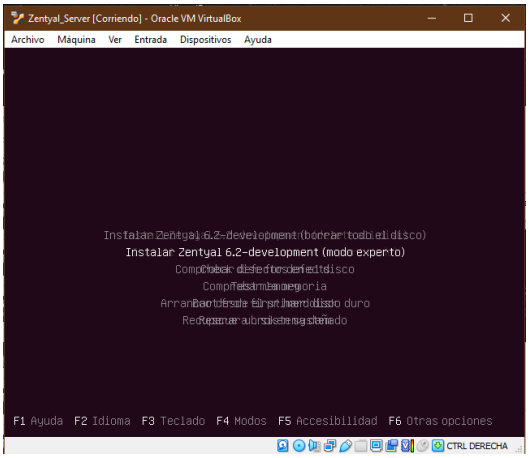

Figura 2. Selección modo de instalación.

Luego se realiza la selección de la ubicación para tener definido la configuración del reloj en el sistema.

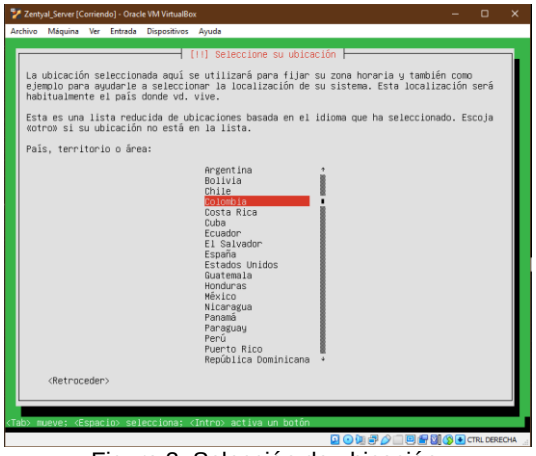

Figura 3. Selección de ubicación.

Se procede a seleccionar el tipo de adaptador de red primario, para realizar la configuración requerida.

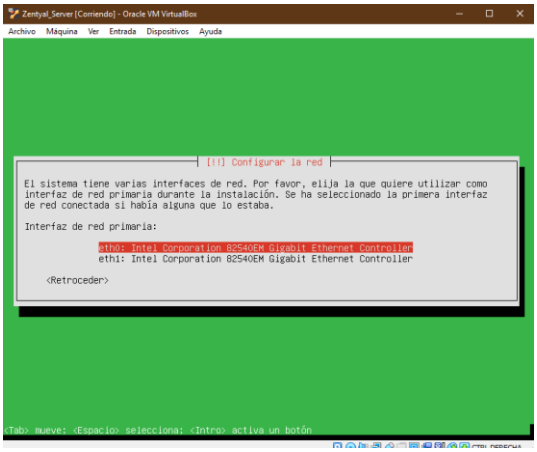

Figura 4. Selección de adaptador de red

Se ingresa el nombre al servidor para su identificación en la red.

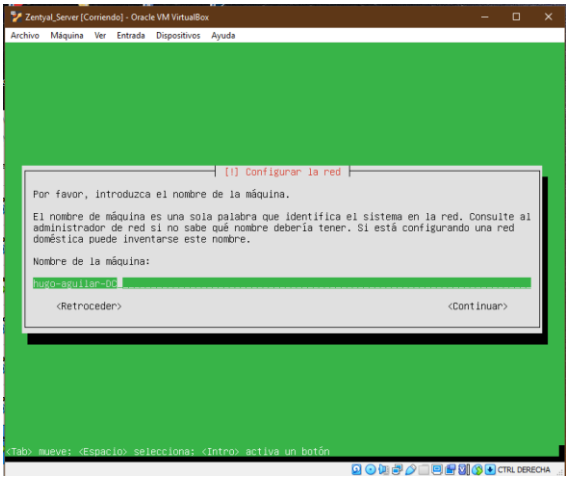

Figura 5. Nombre de la maquina

Se selecciona el nombre de usuario a utilizar en el servidor.

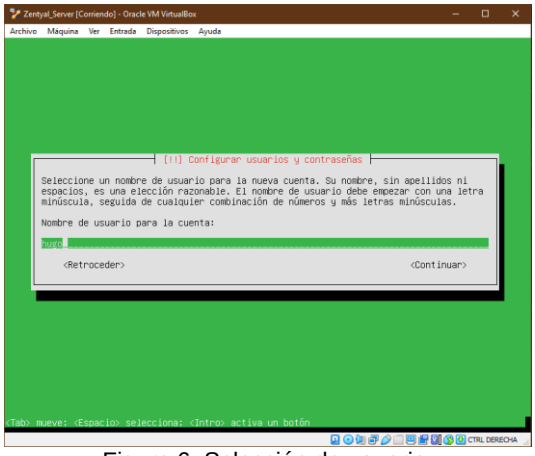

Figura 6. Selección de usuario.

Se realiza la creación de la contraseña para el usuario creado previamente, el cual debe agregar la seguridad necesaria en el servidor.

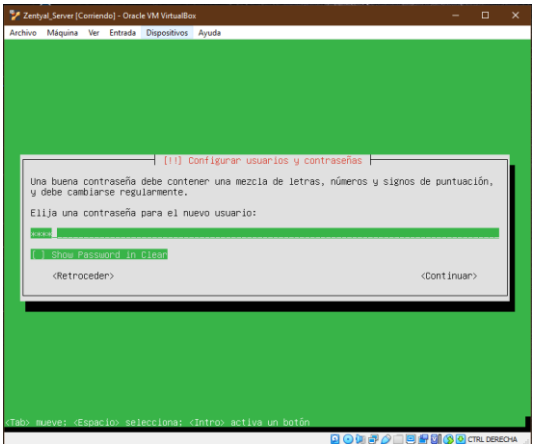

Figura 7. Creación de contraseña.

El sistema procede a realizar la configuración de reloj según la ubicación seleccionada previamente.

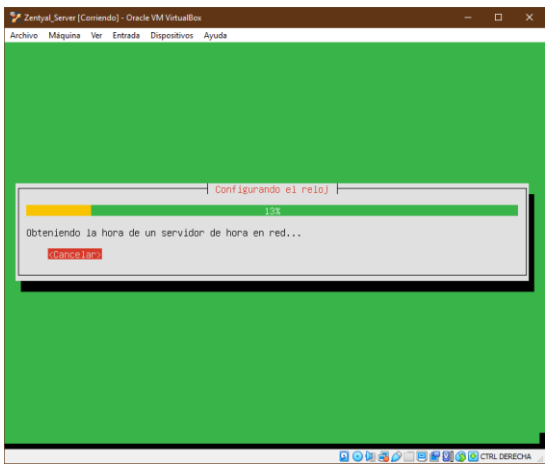

Figura 8. Configuración de reloj.

Se selecciona el disco a particionar, en este caso se realizan dos particiones requeridas.

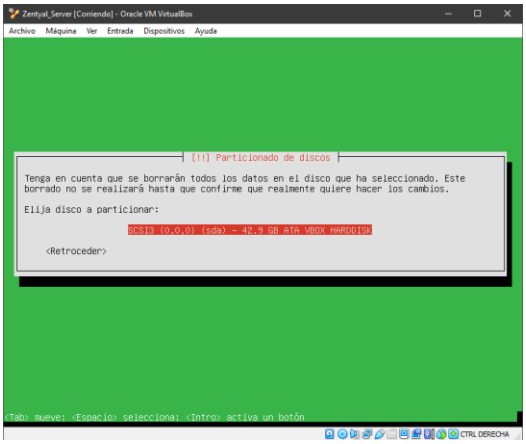

Figura 9. Selección de discos.

Como primera partición se crea la SWAP de tipo área de intercambio.

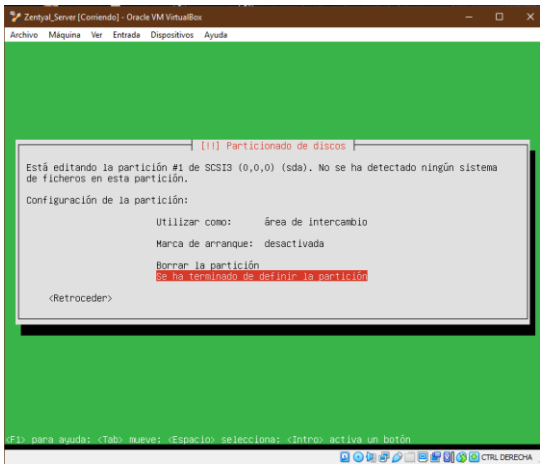

Figura 10. Partición SWAP.

Una vez creada se procede a realizar la creación de la partición principal tipo ext4.

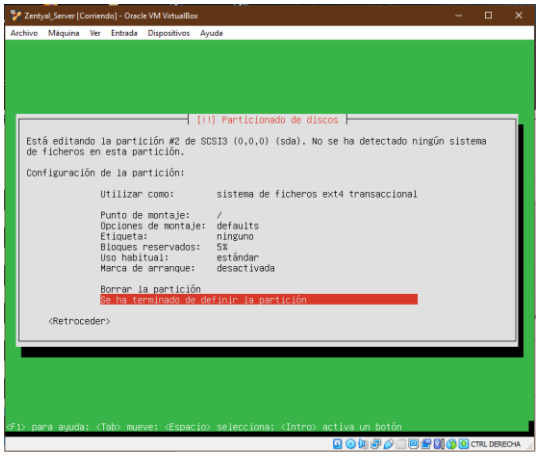

Figura 11. Partición primaria.

Se finaliza la creación de las particiones escribiendo los cambios en disco y se realiza la selección de instalación en entorno gráfico.

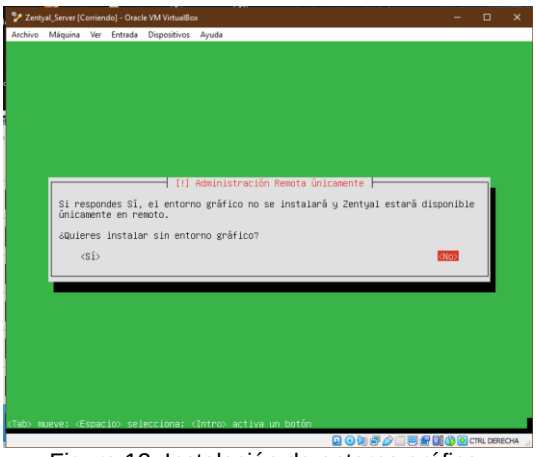

Figura 12. Instalación de entorno gráfico.

El sistema inicia la descarga de ficheros requeridos por la instalación.

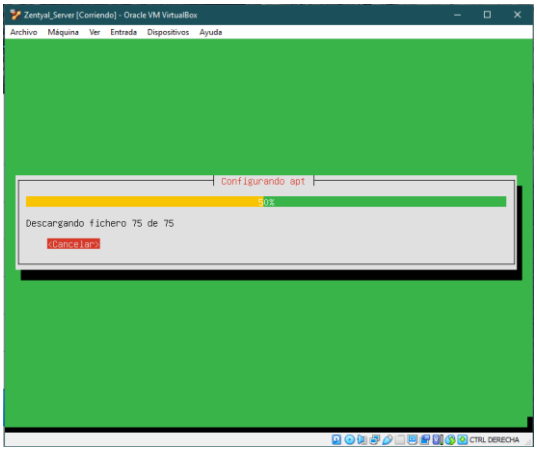

Figura 13. Descarga de ficheros.

Una vez finalizado el proceso de instalación se ejecuta el reinicio del sistema operativo y se inicia la instalación de unos paquetes del core.

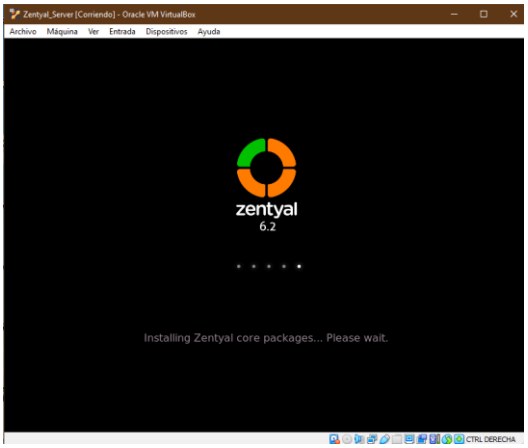

Figura 14. Instalación de paquetes del Core

2.2 CONFIGURACIÓN BÁSICA DE ZENTYAL SERVER 6.2

Una vez iniciado el sistema operativo de forma automática, se inicia el navegador con la consola administrativa del Zentyal, la cual detecta un riesgo de seguridad al reconocimiento de certificado, este debe ser aceptado para avanzar.

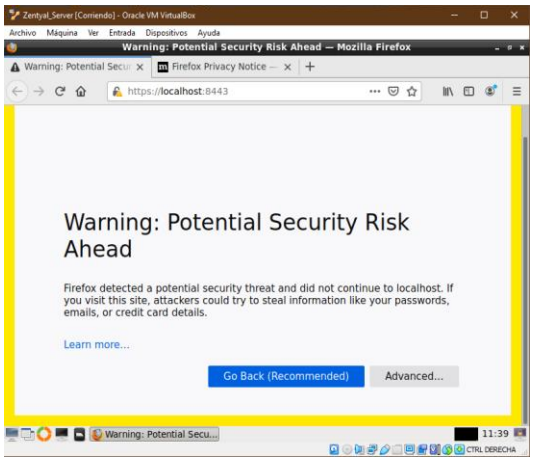

Figura 15. Zentyal desktop.

Una vez carga la página de Login de la consola se ingresa con el usuario definido en la instalación.

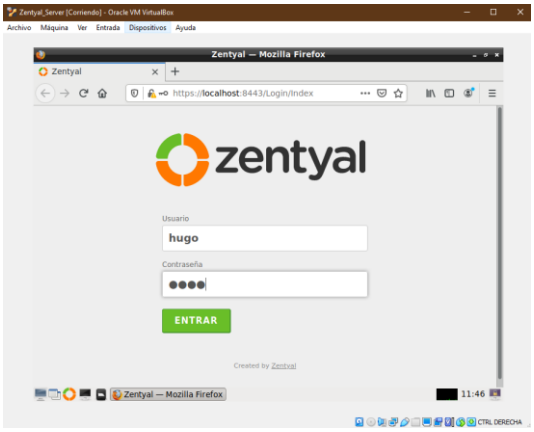

Figura 16. Login a la consola Zentyal.

Una vez con la sesión iniciada se realiza por primera vez la configuración inicial.

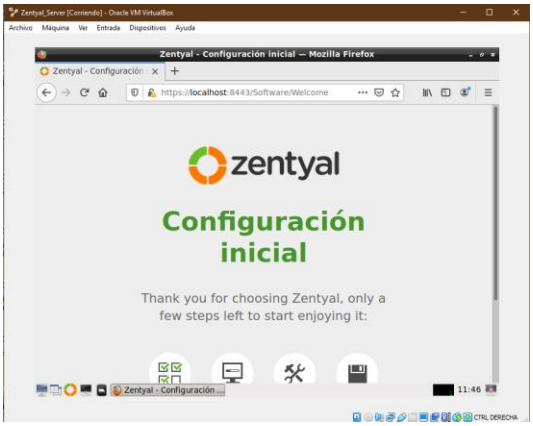

Figura 17. Configuración inicial.

Esta configuración comprende la selección de paquetes y la instalación de estos, los cuales se detallarán de acuerdo con la temática a aplicar.

3 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

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

Primero se seleccionan los paquetes de los servicios a instalar, en este caso se selecciona el Control de dominio, el DHCP Server y el DNS Server.

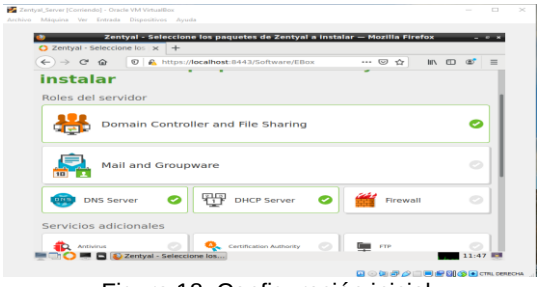

Figura 18. Configuración inicial.

Se realiza la validación de los paquetes a instalar y se continua.

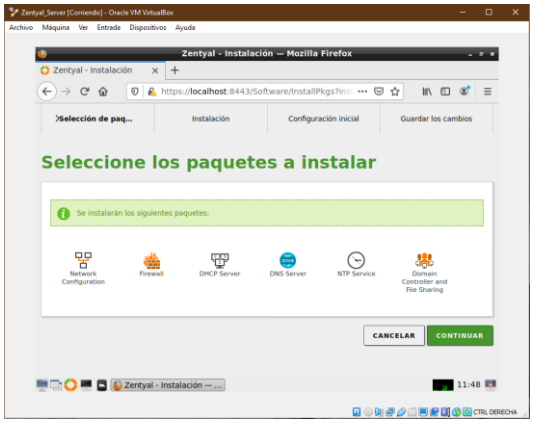

Figura 19. Validación de paquetes a instalar.

Se inicia el proceso de descarga de los paquetes a instalar y el sistema de forma automática procede con la instalación de estos.

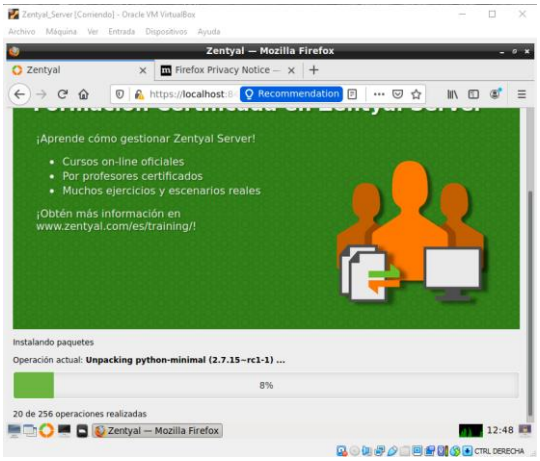

Figura 20. Descarga de paquetes a instalar.

Una vez instalado los paquetes se inicia el proceso de configuración de las interfaces de red para su correcto funcionamiento, el eth0 se configura como DHCP y al eth1 red interna se define con IP estática.

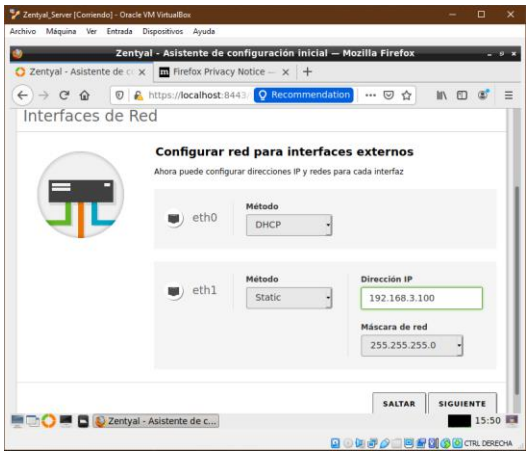

Figura 21. Definición de tipos de red.

Se realiza la selección de forma stand-alone para el servidor de dominio y se define el nombre del dominio a utilizar.

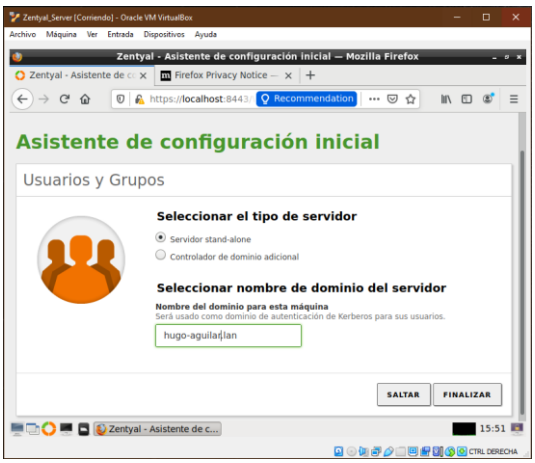

Figura 22. Tipo de servidor y nombre de dominio.

Luego se procede a ingresar al Dashboard para la revisión de la información de los servicios.

Se realiza la creación del Dominio

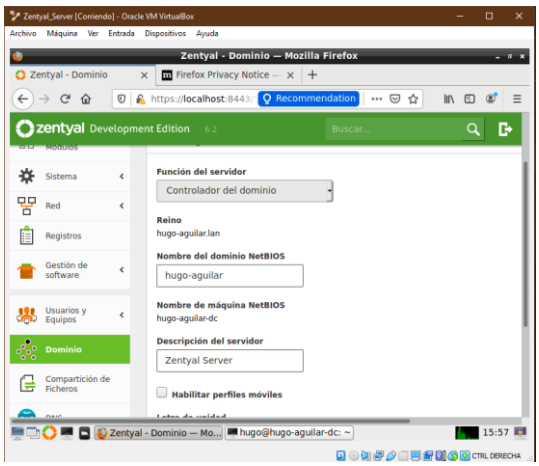

Figura 23. Dominio.

Configuración DNS según el dominio creado en la figura 23.

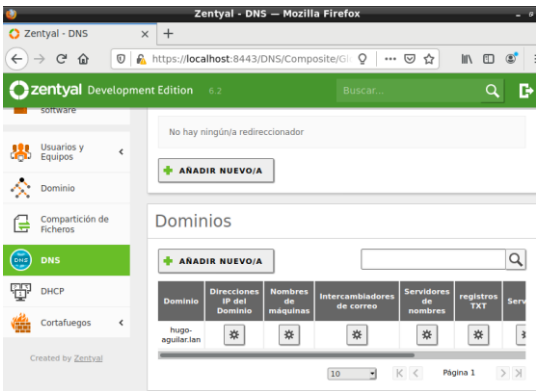

Figura 24. DNS.

Se crea un usuario en el control de dominio para el inicio de sesión desde el servidor.

Figura 25. Creación de usuario control de domino.

Para el ingreso de desktop al domino se procede a editar el archivo resolv.conf, se agrega una línea nameserver donde se define el control de dominio como DNS interno en el desktop.

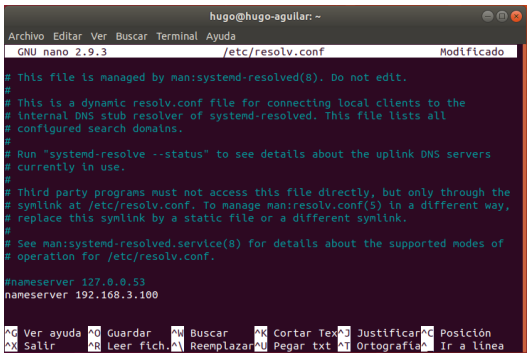

Figura 26. Editar resolv.conf.

Estado de los equipos de cómputo en el control de dominio con el servidor desktop ya detectado por este.

Figura 27. Equipos y usuarios.

Se procede a realizar la configuración del lado del desktop para ingresar este al dominio, para esto se necesita de una aplicación pbis-open.

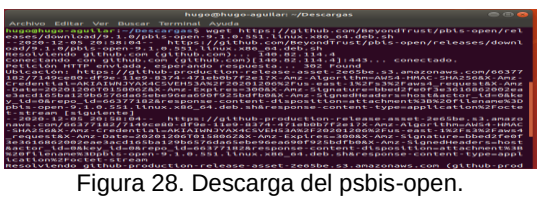

Figura 28. Descarga del psbis-open.

Se realiza la ejecución e instalación de pbis-open. Una vez hecho esto, se realiza una prueba de conexión con el comando “domainjoin-cli” con el usuario creado en el dominio, en este caso con el usuario “administrator” el cual se conecta de forma exitosa.

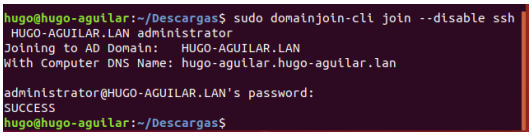

Figura 29. Prueba de conexión al dominio.

Luego de la prueba de conexión se edita el archivo 50-ubuntu.conf ubicado en /usr/share/lightdm/lightdm.config.d/ y se agrega la línea “greeter-show-manual-login=true”

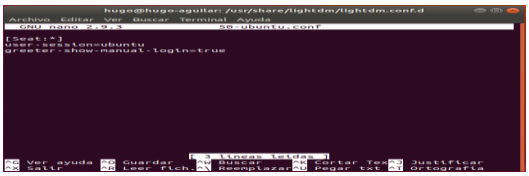

Figura 30. Edición 50-ubuntu.conf.

Se agrega una Shell para el inicio de sesión en el dominio.

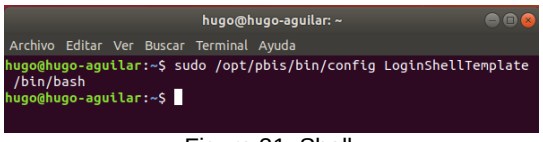

Figura 31. Shell.

Se reinicia el desktop y se ingresa el usuario en minúscula y el dominio en mayúscula quedando finalmente como “HUGO-AGUILAR.LAN/administrator” se debe discriminar mayúsculas de las minúsculas según el usuario creado.

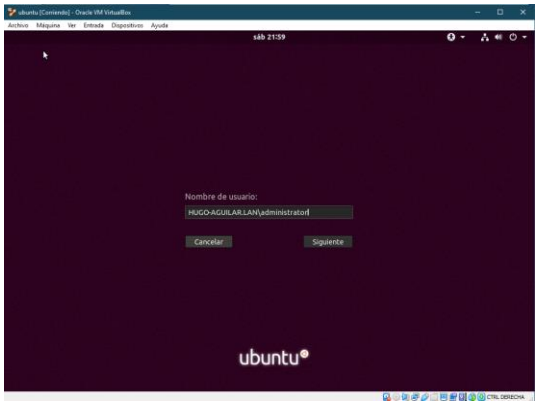

Figura 32. Inicio de sesión en el dominio por primera vez.

Se ingresa la contraseña definida en el control de domino para ese usuario, así se iniciará sesión con el usuario del control de dominio por primera vez de forma exitosa.

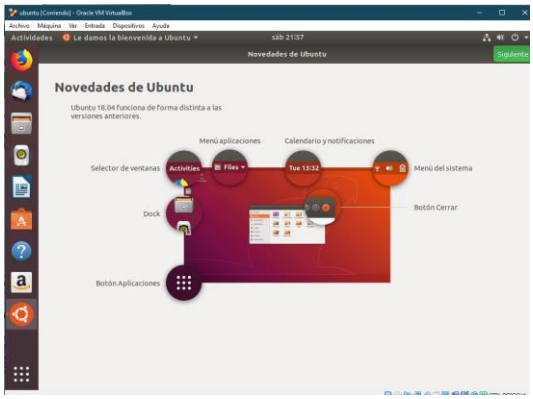

Figura 33. Inicio de sesión.

4 PROXY NO TRANSPARENTE.

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

Posterior a la instalación de Zentyal, se debe instalar el paquete HTTP Proxy

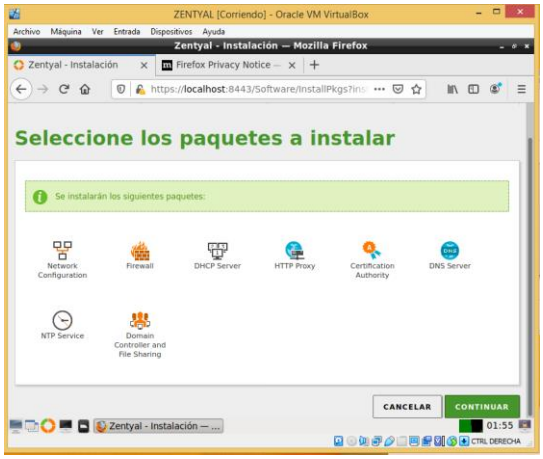

Figura 34. Instalación HTTP Proxy

Luego de la instalación, se ingresa al menú HTTP Proxy, configuración general, allí se ingresa el puerto 1230 como lo solicita el ejercicio y se deja sin seleccionar el Checkbox Proxy Transparente, esto hará que quede configurado como Proxy No Transparente.

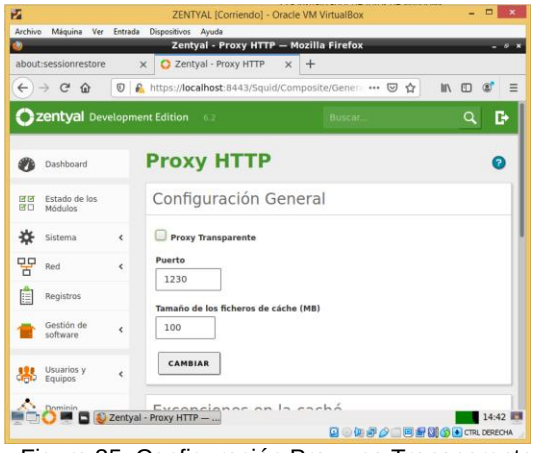

Figura 35. Configuración Proxy no Transparente

Posteriormente, se debe realizar la configuración de las Interfaces de Red, dirigiéndose al Menú “red” y luego a Interfaces de red, allí se pondrá la red eth0 como red externa(WAN) con método DHCP y la red eth1 como interna con método estático indicando la dirección IP por la cual se podrá acceder al servidor.

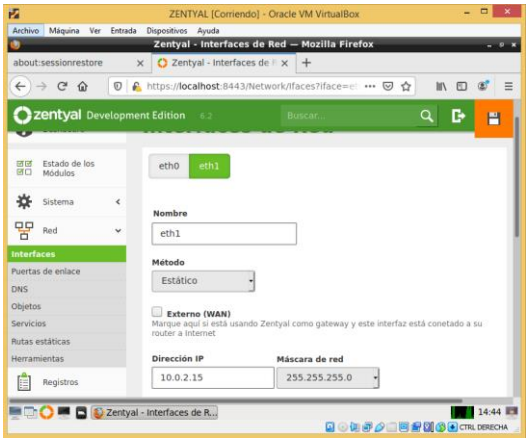

Figura 36. Configuración red Interna

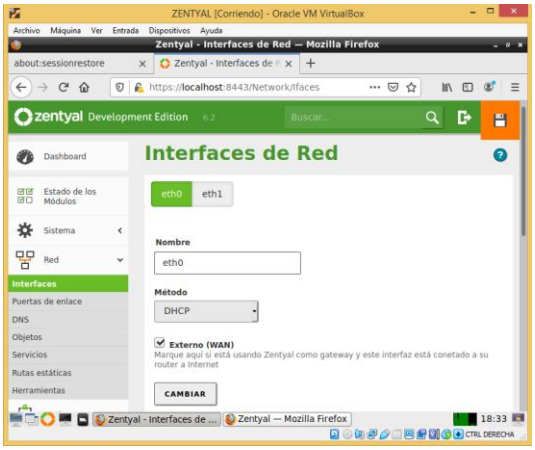

Figura 37.Configuración red Externa

Se ingresa al Menú HTTP Proxy y luego a reglas de acceso, allí se configuran las reglas de acceso a internet

para el objeto creado, el cual contiene la información del equipo desktop que accederá al servidor.

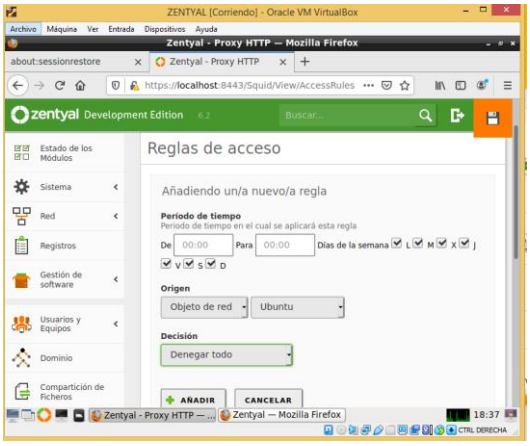

Figura 38. Creación reglas de acceso

Al finalizar se deben guardar los cambios realizados en el servidor.

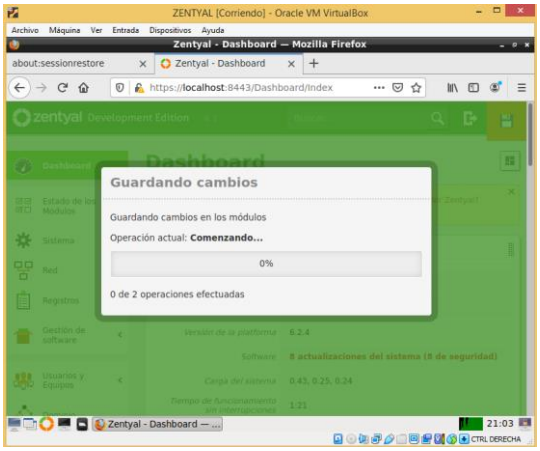

Figura 39. Guardando cambios en el servidor

Como último paso, se configura en el equipo desktop el proxy y luego se valida que el servidor si restrinja el acceso a Internet.

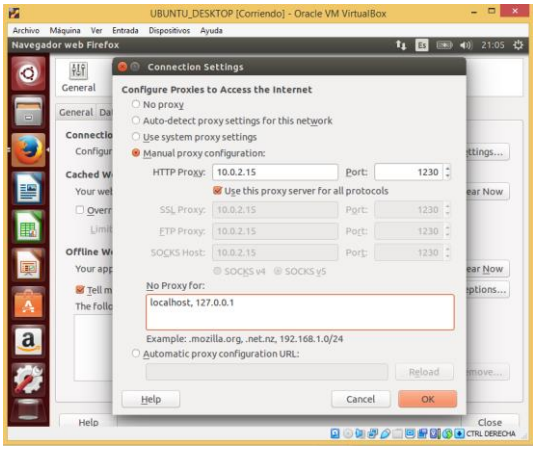

Figura 40. Configurar Proxy en equipo desktop

Se valida el ingreso a www.facebook.com para comprobar si permite la conexión y el servidor Proxy rechaza las conexiones.

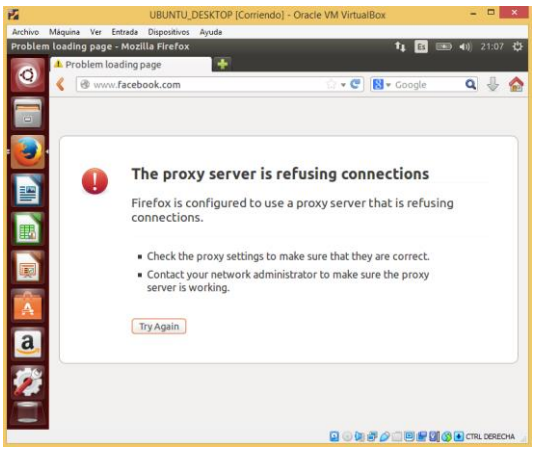

Figura 41. Validación de acceso a internet

5 CORTAFUEGOS

Se seleccionan los paquetes de Zentyal a instalar los cuales son DNS Server, DHCP Server y Firewall.

Figura 42 Paquetes de Zentyal a instalar

Se configuran las interfaces de red de la siguiente manera: eth0 como red externa (WAN) y eht1 como red interna (LAN).

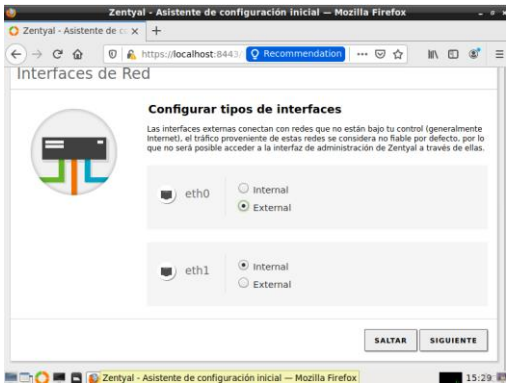

Figura 43 Configuración de interfaces de red

Se configuran las redes para las interfaces externas de la siguiente manera: eth0 por DHCP y eth1 como estática asignando la IP: 192.168.0.254

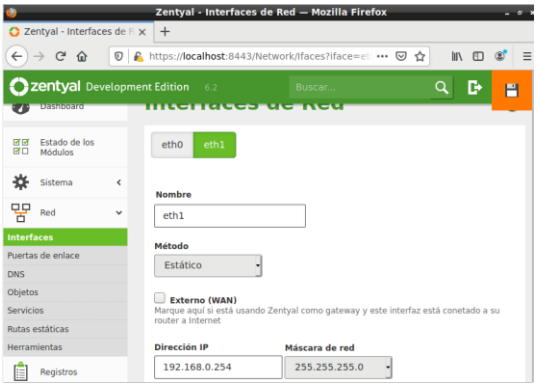

Figura 44 Configuración de redes para las interfaces

Se configuran los servicios DHCP por medio de Zentyal asignando un rango dentro del segmento de red para que la máquina cliente tome una IP del rango asignado.

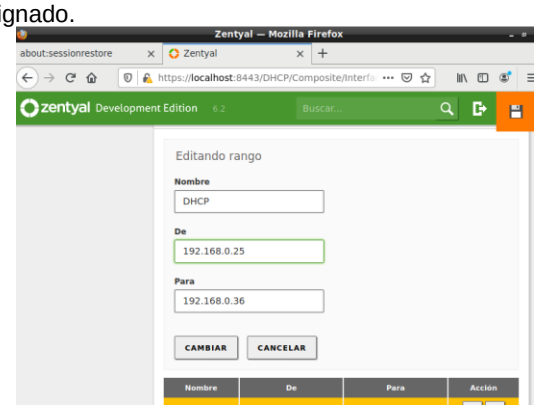

Figura 45 Configuración de servicios DHCP

En la máquina cliente, se configura el adaptador 1 como red interna y se selecciona la red creada por medio de Zentyal como Zentyal_LAN. Se observa que la máquina cliente toma una dirección IP del rango asignado.

Figura 46 Configuración de red en máquina cliente

Se verifica el acceso desde la máquina cliente a los sitios de entretenimiento y redes sociales identificando que se tiene acceso correctamente.

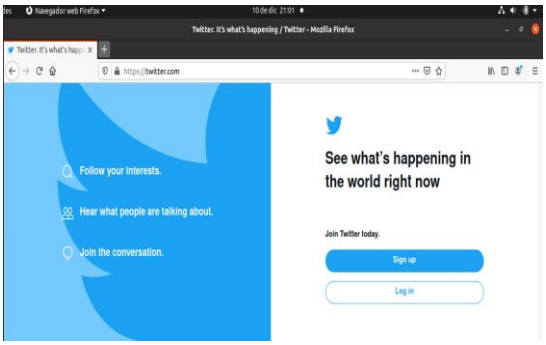

Figura 47 Verificación de acceso a sitios

Se utiliza el comando nslookup para obtener la dirección IP de cada uno de los sitios en los cuales se va a restringir el acceso.

Figura 48 Verificación de direcciones IP

Se debe acceder a la opción reglas de filtrado de redes internas para configurar las reglas.

Figura 49 Acceso a opción reglas de filtrado

Se crean las reglas de bloqueo para los sitios de entretenimiento y redes sociales, denegando los permisos desde cualquier origen hasta la dirección IP del sitio.

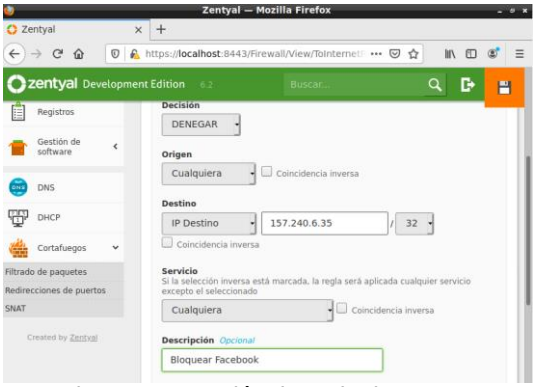

Figura 50 Creación de regla de acceso

Una vez se asignan todas las reglas se evidencian en el panel de filtrado de paquetes. Para que se tomen los cambios y estos puedan ser replicados en la red se deben guardar.

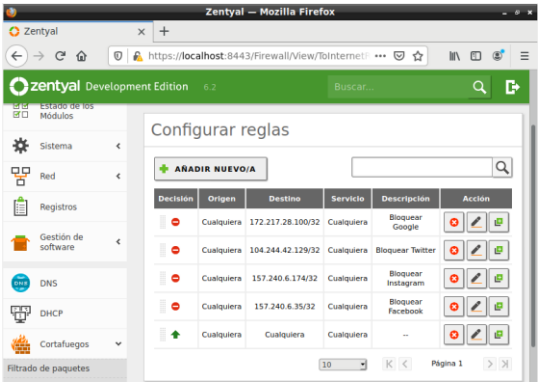

Figura 51 Panel de filtrado de paquetes

Se verifica el acceso a internet desde la máquina cliente y se evidencia que se puede acceder de manera correcta.

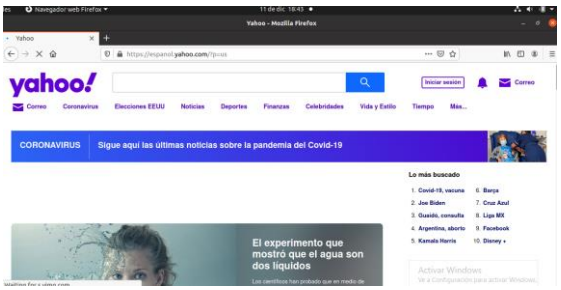

Figura 52 Verificación de acceso a internet

Se verifica el acceso a cada uno de los sitios bloqueados por medio de la regla y se corrobora que fue aplicada y no se permite el acceso al sitio.

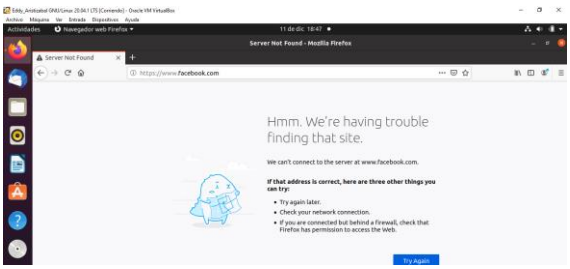

Figura 53 Verificación de aplicación de la regla

6 FILE SERVER Y PRINT SERVER.

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

Para utilizar carpetas compartidas e impresoras se valida lo siguiente: controlador de dominio LDAP, DHCP y DNS, los cuales deben estar operando correctamente.

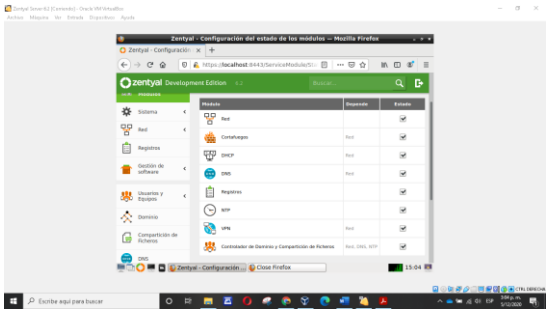

Figura 54 Validar los módulos activados

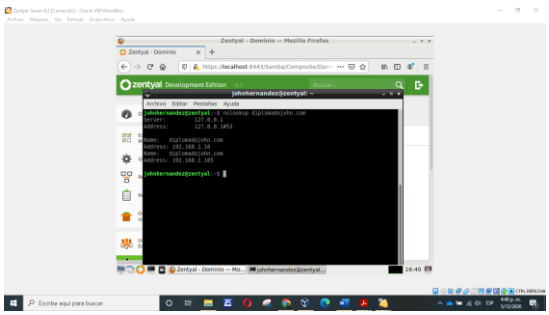

Figura 55 Validar el funcionamiento del controlador de dominio

Figura 56 Unirse al dominio

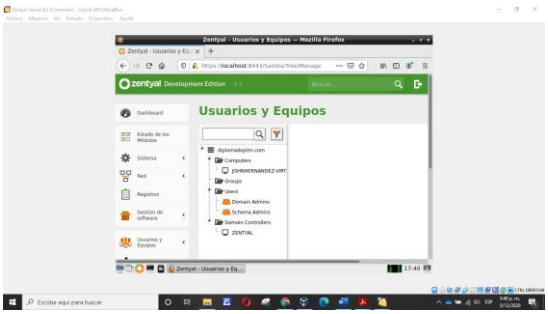

Figura 57 Validar en el servidor la unión al dominio del equipo

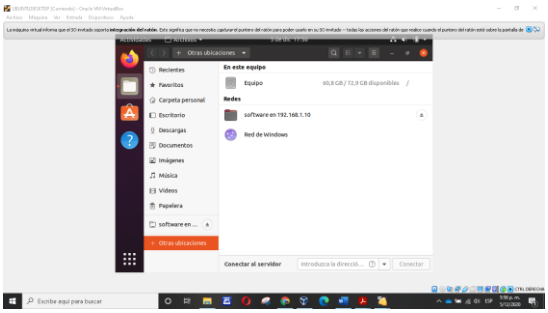

Figura 61 Se accede desde el cliente que inicio sesión en el dominio al recurso compartido

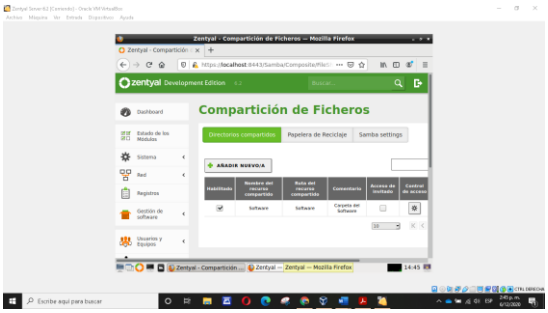

Figura 58 Compartición de Ficheros

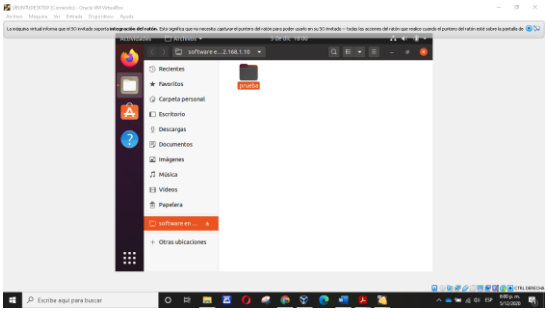

Figura 62 Se crea una carpeta dentro del recurso compartido para validar permisos

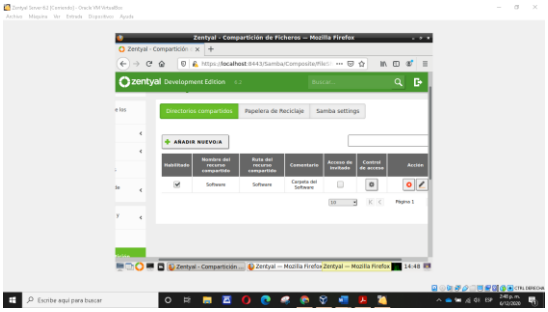

Figura 59 Se añade carpeta compartida Software

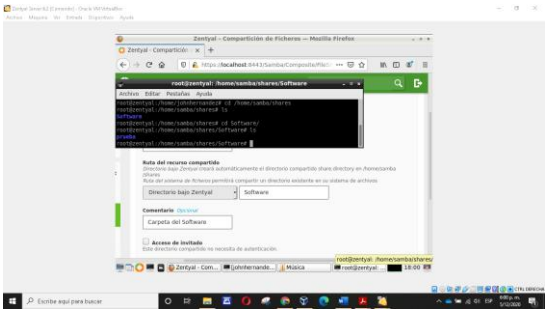

Figura 63 Se valida desde el servidor la carpeta creada en el recurso compartido

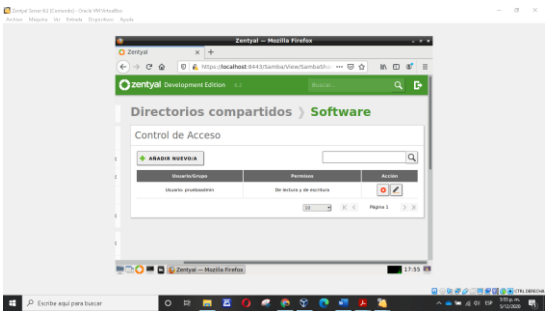

Figura 60 Se añade el usuario que puede acceder y se asignan permisos.

En Zentyal 6.2 no se observa un módulo para implementar el Print Server, por lo tanto, se utiliza CUPS (Common UNIX Printing System) para implementar este servicio desde el servidor.

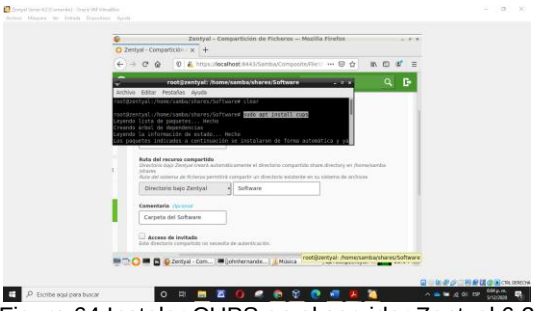

Figura 64 Instalar CUPS en el servidor Zentyal 6.2

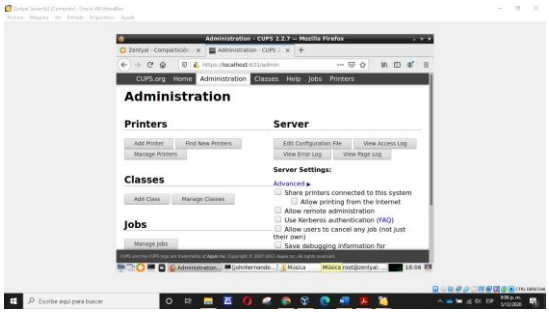

Figura 65 Se inicia sesión y se ingresa a “Administration”

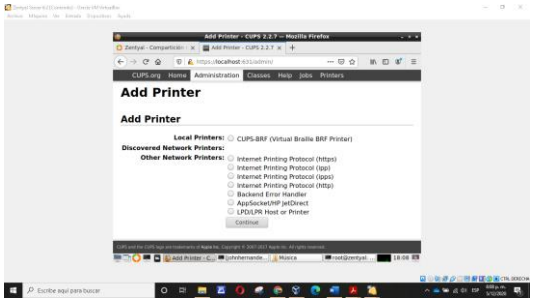

Figura 66 Se inicia sesión y se ingresa a “Administration”

Figura 67 Adicionar la impresora

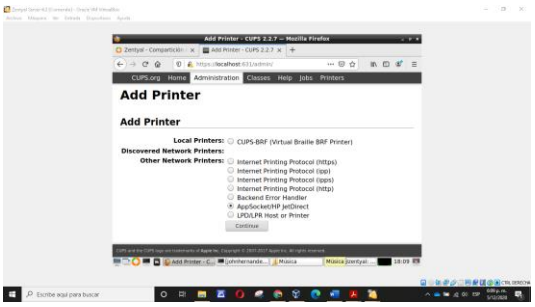

Figura 68 Seleccionar AppSocket

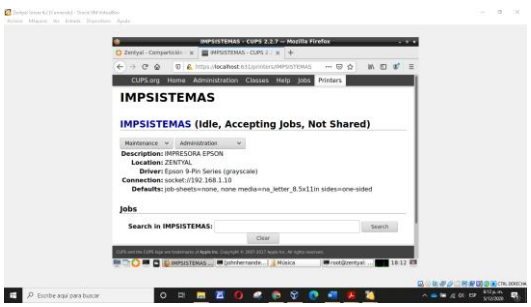

Figura 69 Asignar nombre a la impresora y el tipo

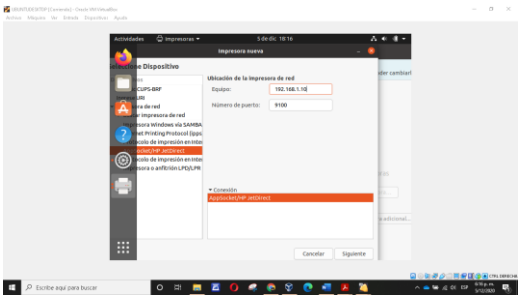

Figura 70 Agregar la impresora desde el equipo cliente adicionando la IP del servidor

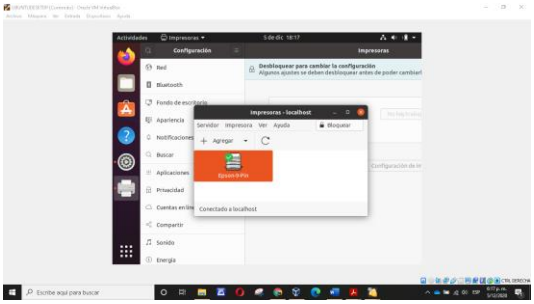

Figura 71 Finaliza la instalación de la impresora de red en el cliente

7 VPN

Para esta temática se espera como producto de entrega, la 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Con el entorno de Zentyal instalado y la sesión iniciada, se da paso a la disposición de los paquetes de configuración de red, cortafuegos, autoridad de certificación y VPN.

Figura 72 Instalación de paquetes.

Una vez instalados los paquetes, es necesario hacer un recorrido por el Dashboard para identificar la actualización, además de esto se debe activar en los 4

módulos la casilla de verificación que habilita el servicio de cada uno.

La configuración de red se inicia por medio de la asignación de IP, mascara de red y método, la primera de ellas es designada a la interfaz externa WAN.

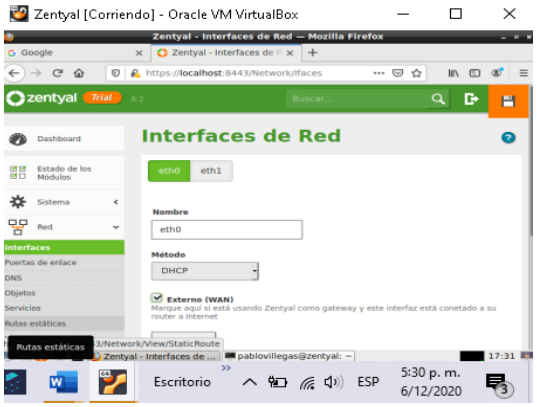

Figura 73 Configuración interfaz externa.

De igual forma se realiza las configuraciones respectivas para la interfaz interna.

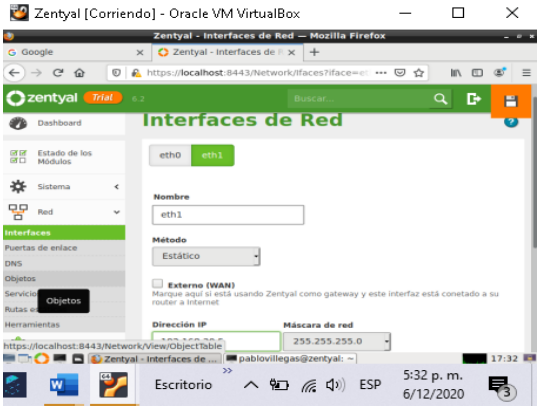

Figura 74 Configuración interfaz interna.

El siguiente paso consiste en crear la autoridad de certificación que permitirá dar acceso al túnel VPN.

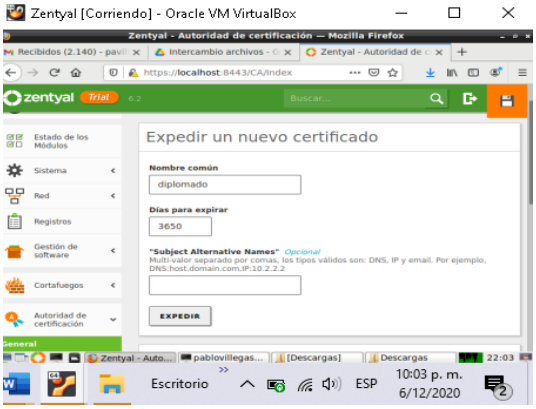

Figura 75 Generación de certificado.

En el apartado de VPN se agrega un servidor con un nombre identificador, puerto y dirección IP.

Figura 76 Creación de servidor VPN.

También se requiere habilitar y configurar el certificado para los servicios a partir de un nombre identificador.

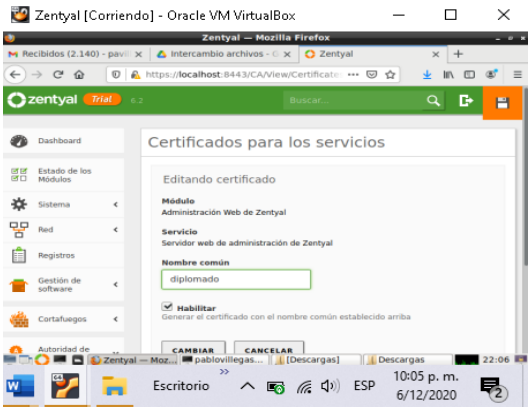

Figura 77 Generación de certificado de servicios.

En este punto de la administración de Zentyal ya es posible generar y descargar un archivo de configuración para la VPN del cliente en el menú de servidores.

Figura 78 Descarga de configuración VPN cliente.

Los archivos de configuración deben ser enviados a la máquina cliente, posteriormente a este proceso se descomprimen generando de esta forma 4 archivos con las características de conexión del túnel VPN.

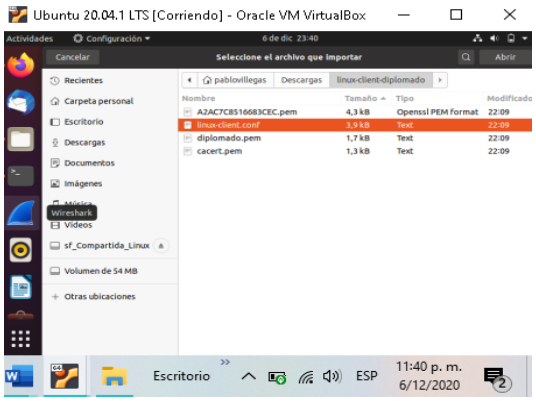

Figura 79 Envío de configuración VPN al cliente.

En la máquina cliente se dispone la instalación de OpenVPN a través del comando sudo apt-get install openvpn.

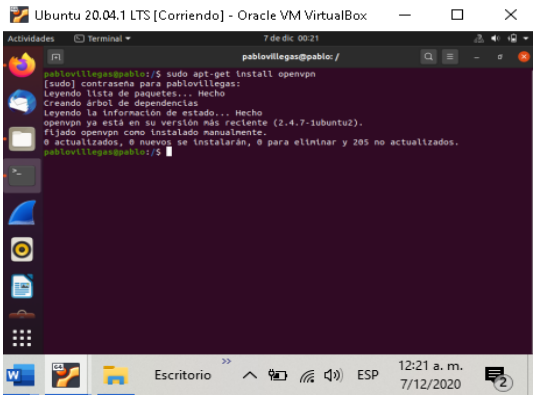

Figura 80 Instalación de OpenVPN.

Luego de haber instalado OpenVPN se ubican los archivos anteriormente descomprimidos en la ruta /etc/openvpn.

A continuación, se procede a editar uno de los archivos de configuración, en este caso el archivo Linux-Client.conf, en este se debe retirar las comillas que registren en las líneas marcadas como ca, cert y key.

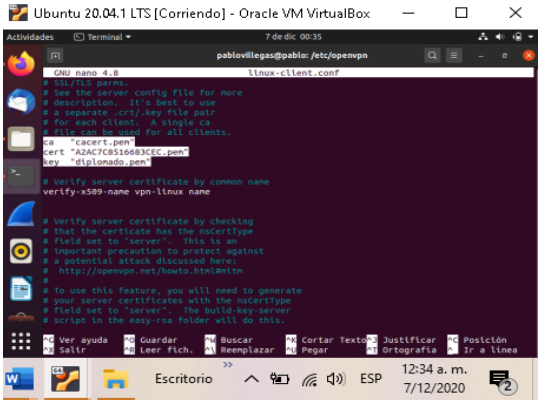

Figura 81 Modificación en configuración.

Luego de guardar los cambios del archivo de configuración se reinicia el programa OpenVPN con el comando /etc/init.d/openvpn restart

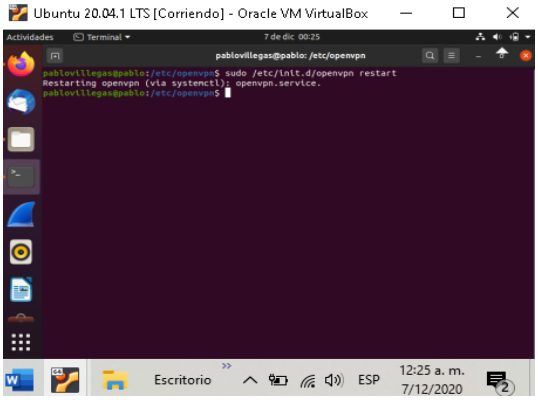

Figura 82 Reinicio de OpenVPN.

Ejecutando el comando ifconfig se podrá identificar la interfaz tap0 del cliente con la IP de VNP creada.

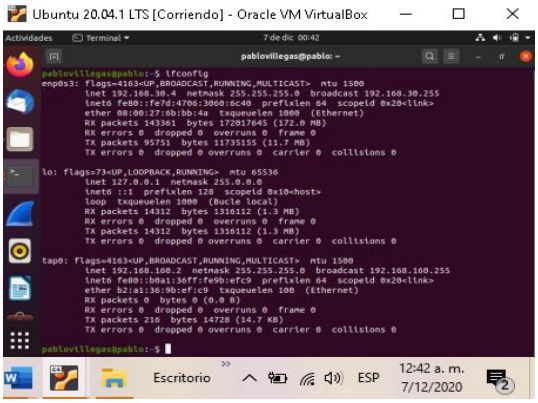

Figura 83 Asignación de IP VPN.

A través de los comandos IPTables se deberán abrir además los puertos UDP 1194 en la máquina cliente

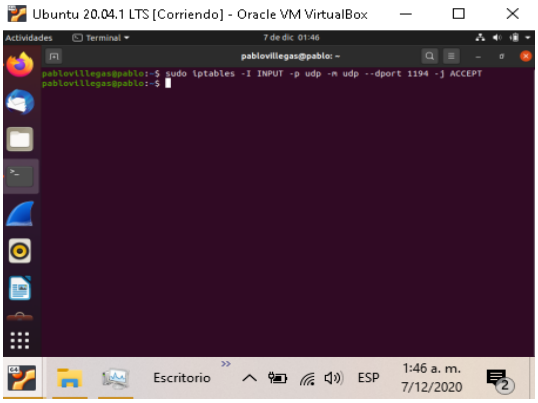

Figura 84 Apertura de puerto 1194 en cliente.

De igual manera se aplica la apertura de puertos para la máquina servidor.

Figura 85 Apertura de puerto 1194 en Zentyal.

A continuación, se arranca el servicio con el comando openvpn Linux-Client.conf. En este se evidenciará el proceso realizado por OpenVPN y la inicialización completada.

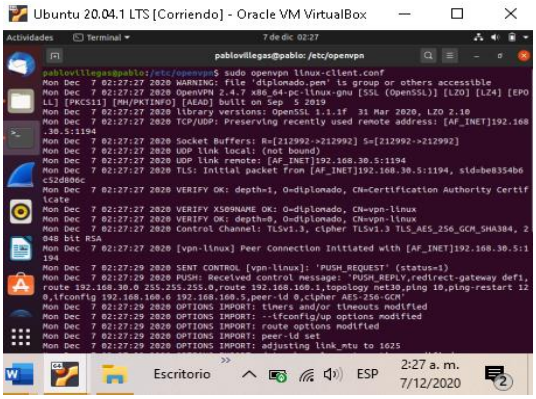

Figura 86 Inicialización completa de OpenVPN.

Finalmente, se realiza una prueba de acceso del cliente al servidor para ingresar al servidor web apache instalado en Zentyal.

Figura 87 Prueba de acceso desde el cliente.

Se valida el servidor web desde Zentyal.

Figura 88 Información mostrada por el servidor web.

8 CONCLUSIONES

Se logra realizar la configuración requerida en el servidor Zentyal de forma correcta el cual permite realizar el ingreso de equipo y usuarios a este, así como un monitoreo de la red configurada y servicios instalados de DHCP, DNS y controlador de dominio.

Se pudo realizar la conexión de forma correcta del servidor desktop al dominio con el usuario “administrador” definidos en el controlador de dominio no siendo un usuario local de este equipo.

Se realiza una correcta configuración del servidor Proxy no Transparente, logrando impedir el acceso a internet por el puerto 1230 ingresando desde un equipo desktop.

Con la instalación y el uso de Zentyal se conoció el uso del cortafuegos el cual brinda mayor protección en el momento de ingresar a ciertas páginas que pueden ser peligrosas para el usuario final, además de su funcionamiento, se aprendió a realizar la configuración.

Se dispuso dentro de la Infraestructura IT, la implementación de los servicios File Server y Print Server usando cups.

Se implementaron los procesos necesarios para integrar el servicio de VPN en el software Zentyal y validar su funcionamiento.

9 REFERENCIAS

[1] zentyal.com (2020), Zentyal Server 6.2 Development Ahora Disponible. Disponible en: https://zentyal.com/es/news/zentyal-6-2-announcement-2/

[2] doc.zentyal.org (s/f), Zentyal 6.2 Documentación Oficial. Disponible en: https://doc.zentyal.org/es/index.html

[3] Ramos J. (2019), Agregar Ubuntu 18.04 LTS a dominio Active Directory. Disponible en: https://blog.ragasys.es/agregar-ubuntu-18-04-lts-a-dominio-active-directory-windows

[4] Zentyal Community (2018). Servicio de redes privadas virtuales (VPN) con OpenVPN. Recuperado de https://doc.zentyal.org/es/vpn.html