SOLUCIONANDO NECESIDADES ESPECÍFICAS CON ZENTYAL SERVER EN GNU LINUX.

Harol Santiago Molina Romero
e-mail: hsmolinar@unadvirtual.edu.co
Jhon Fredy Católico Ávila
e-mail: jfcatolicoa@unadvirtual.edu.co
Juan Carlos Tapiero Miranda
e-mail: jctapierom@unadvirtual.edu.co
Fernando González Ortiz
e-mail: fagonzalezo@unadvirtual.edu.co
Raúl Andrés Alfonso
e-mail: raalfonsor@unadvirtual.edu.co

RESUMEN: *El articulo muestra la manera en cómo se puede instalar y configurar Zentyal Server para utilizarse como plataforma de TI, de igual forma se aborda la forma de cómo se puede instalar la plataforma y configurar servicios DHCP Server, DNS Server, Controlador de Dominio, proxy no transparente, cortafuegos, File Server, Print Server y VPN.*

PALABRAS CLAVE: Conexión, interfaz, servidor, zentyal.

1 INTRODUCCIÓN

La administración de servidores por medio de Linux, es uno de los métodos más seguros que se están usando en este instante y más con Herramientas como Zentyal, el cual es una gran herramienta para pequeñas y medianas empresas teniendo en cuenta su interfaz gráfica, la cual es bastante amigable, al permitir agilizar mucho los procesos que realizaremos en el presente trabajo.

2 INSTALACIÓN DE ZENTYAL SERVER EN MAQUINA VIRTUAL

2.1 CONFIGURACIÓN DE LA MAQUINA VIRTUAL

Para la instalación de Zentyal, se creó una máquina virtual basada en Linux Ubuntu con una memoria RAM de 2 GB, un disco duro de 20 Gb, dos adaptadores de red uno para la conexión WAN como adaptador puente, y otro para la conexión LAN como adaptador de red interna. Se descargó la imagen .iso de http://download.zentyal.com/zentyal-6.2-development-amd64.iso, la cual fue la solicitada en la guía de desarrollo.

2.2 PROCESO DE INSTALACIÓN DE ZENTYAL

Luego de montar la imagen .iso en la máquina virtual, esta se pulsó en arrancar, para escoger el proceso de instalación, seleccionando el idioma y la instalación a realizar.

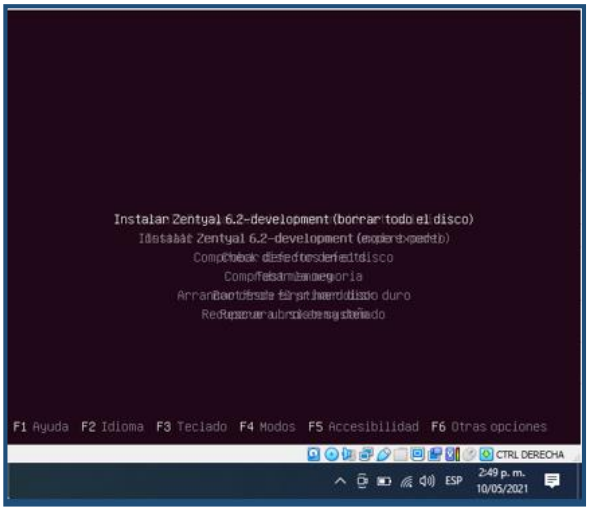

Figura 1. Modo de instalación para zentyal.

De igual forma se escogió el país de residencia, el cual fue tomado como referente para la zona horaria de la máquina, y luego se seleccionó la distribución de teclado la cual será usada para el sistema operativo.

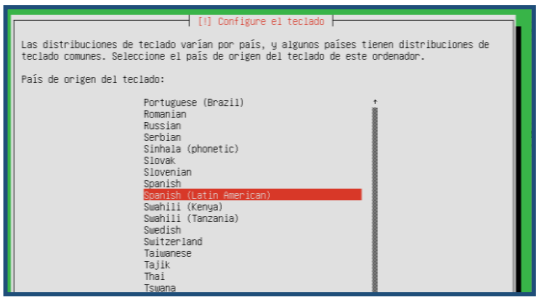

Figura 2. Distribución de teclado.

Se asignó un nombre a la maquina con el fin de ser identificada dentro de la red

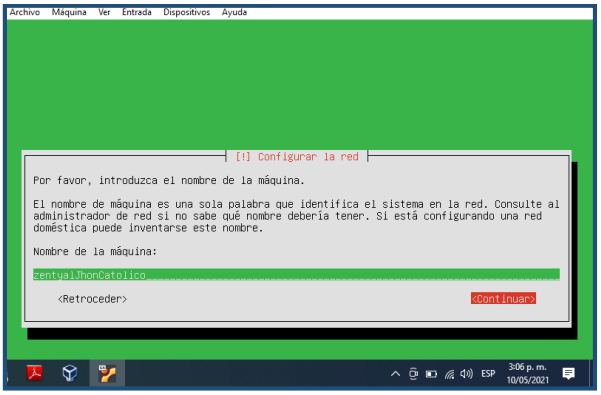

Figura 3. Asignación del nombre de la máquina.

Se creó un nombre de usuario para el ingreso al servidor

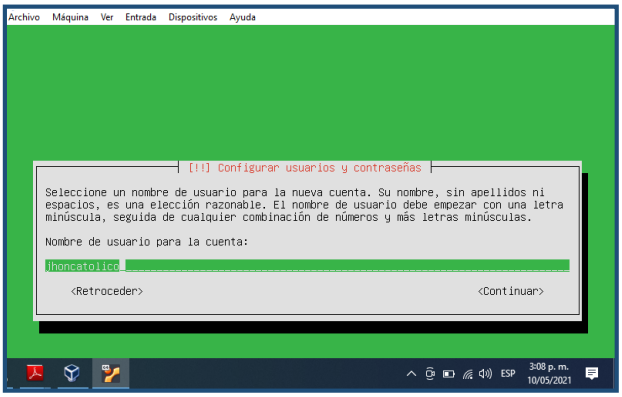

Figura 4. Asignación del nombre de usuario.

A la cuenta de usuario creada se le asignó una contraseña de seguridad en el acceso al servidor

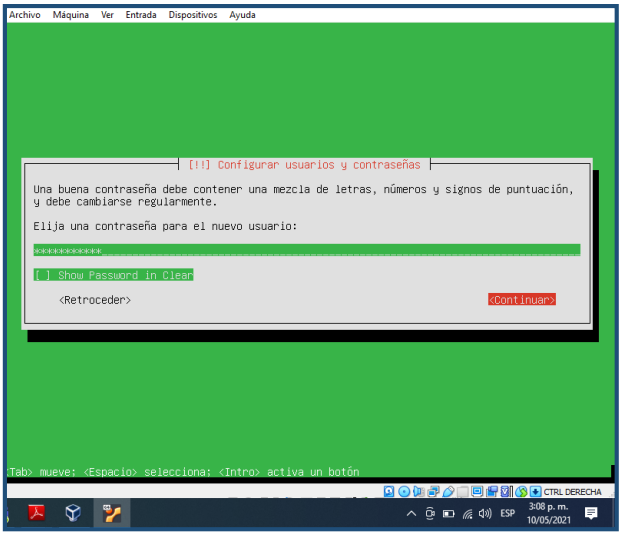

Figura 5. Asignación de contraseña.

Luego de realizar las configuraciones anteriores se culminó exitosamente con el proceso de instalación

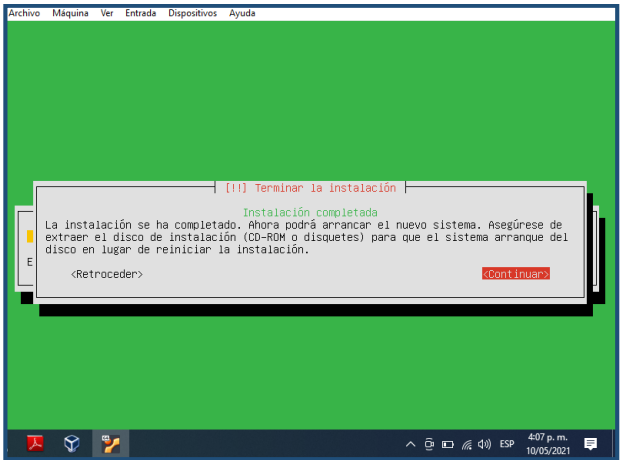

Figura 6. Finalización de la instalación.

Después de haber instalado y arrancado el sistema, se cargó de manera automática la dirección de dominio de zentyal web, con el fin de realizar la autenticación de ingreso al servidor.

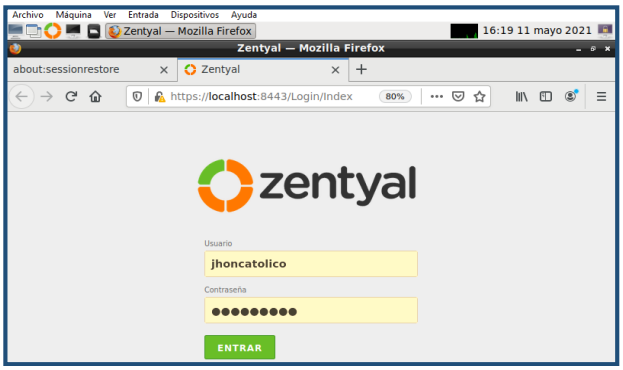

Figura 7. Autenticación de ingreso a zentyal web.

Luego de haber realzado la autenticación, se realizó la configuración inicial de zentyal.

Figura 8. Autenticación de ingreso a zentyal web.

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

Para el inicio de las configuraciones se debe ingresar y verificar que los servicios que se necesitan ya estén subidos.

Se ingresa con la contraseña y el usuario que se creó durante la instalación.

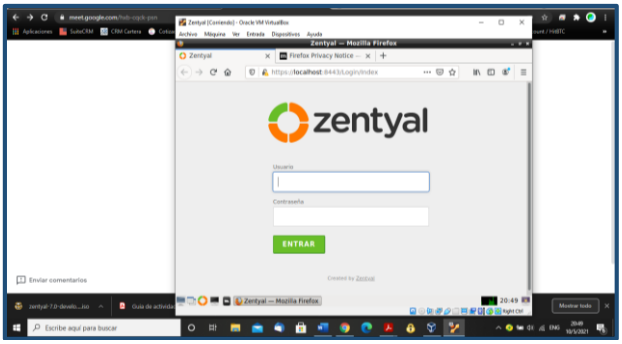

Figura 9. Inicio de zenyal.

Por medio de la configuración inicial se realizará la subida de los servicios que se necesitan.

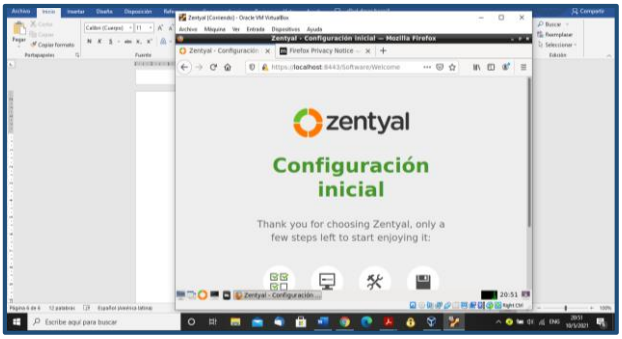

Figura 10. Arranque de instalación de servicios zentyal

Se inicia la instalación asistida por el servidor.

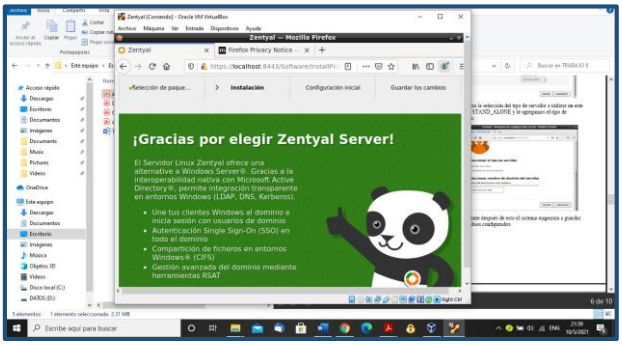

Figura 7. Se revisan los términos del instalador

Para subir los servicios creamos un tipo de servidor STAN ALONE y se deja el nombre de dominio que trae por defecto.

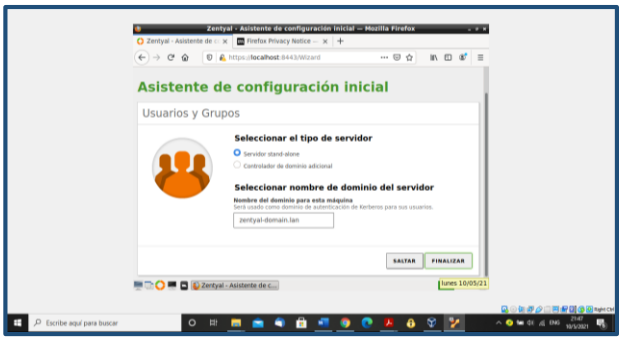

Figura 11. *Selección tipo de servidor*

Se configuran las conexiones de red donde ETH0 es la red externa y la ETH1 es la interna.

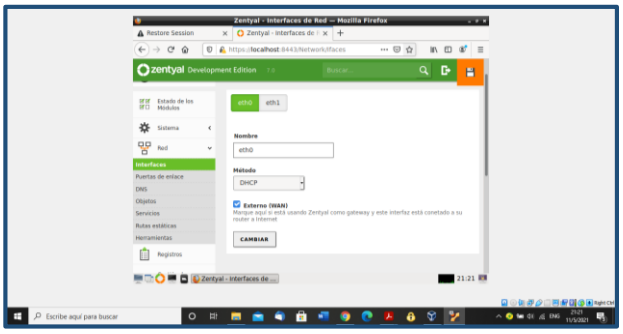

Figura 12. Configuración conexión 1 (WAN)

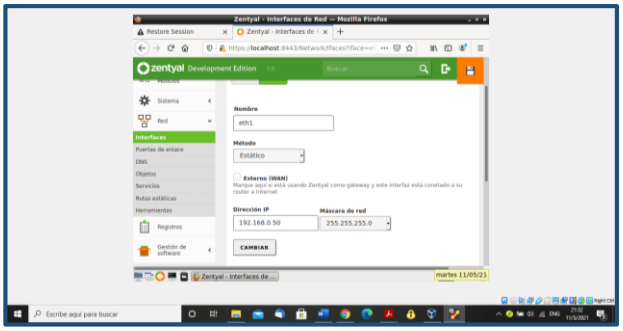

Figura 13. Configuración conexión 2 (LAN)

Se activa el DHCP con el punto de enlace por defecto.

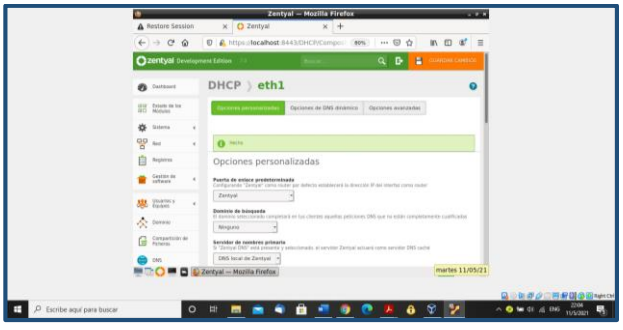

Figura 14. Configuración DHCP

Se añade un rango de ip para el dominio.

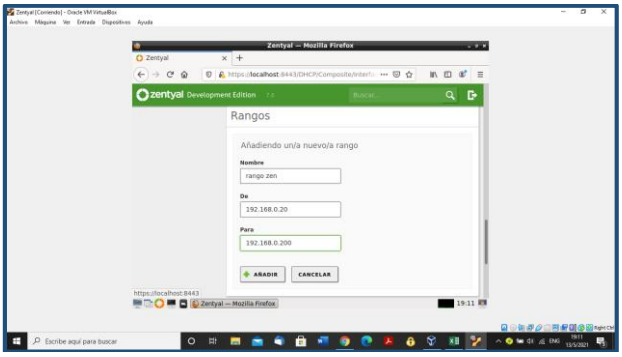

Figura 15. Asignación de rangos

Se verifica que los rangos estén asignados.

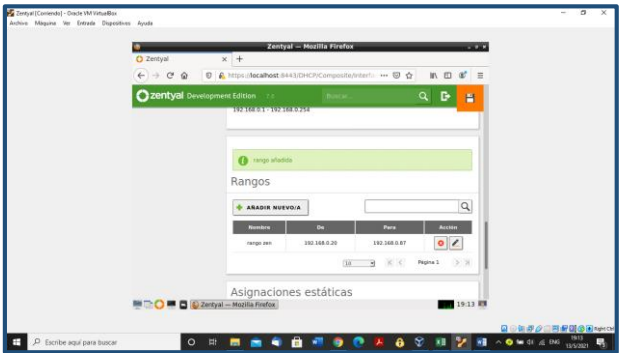

Figura 16. Verificación de rangos creados

Se ingresa a una maquina cliente y se verifica que al conectarse se une al rango que configuramos en zentyal.

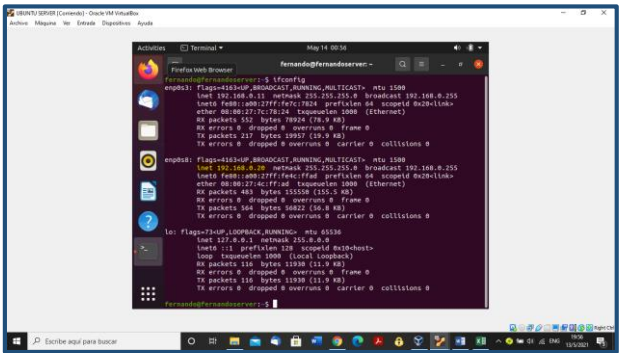

Figura 17. Verificación de rango en maquina cliente

Se verifica en el servidor Zentyal y se demuestra que queda registrada la entrada de la maquina cliente al servidor.

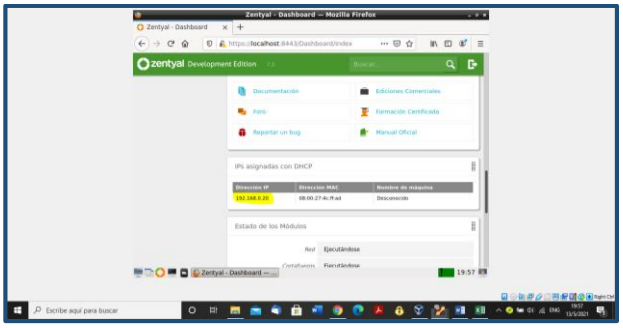

Figura 18. Vista de maquina conectada al servidor

Se crea una nueva máquina.

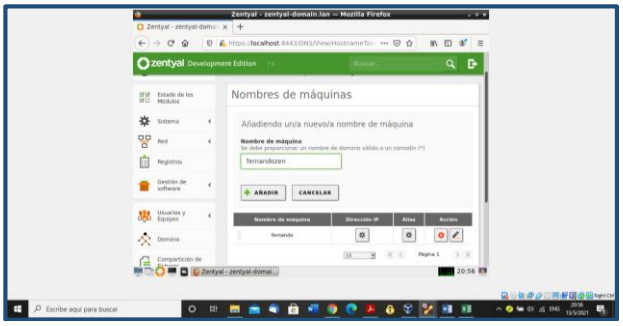

Figura 19. Visualización de maquina creada

Se configura la IP de la misma.

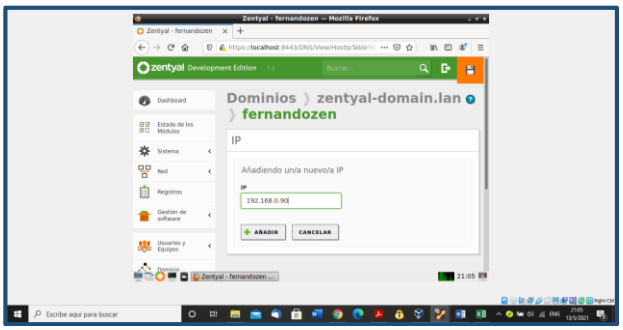

Figura 20. Asignación de IP de la maquina

Se verifica desde la maquina cliente la configuración que se acaba de hacer en el servidor.

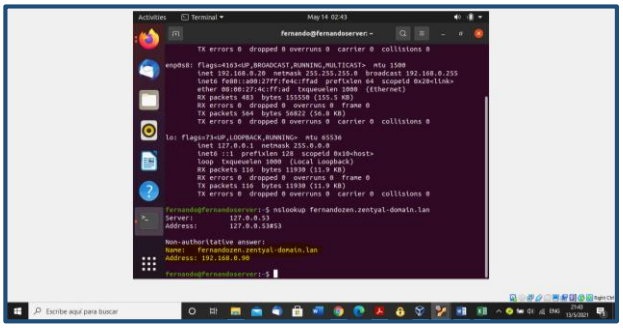

Figura 21. Visualización de la asignación IP y servidor

Se crea un usuario con el cual se conectará cuando se termine de configurar el dominio.

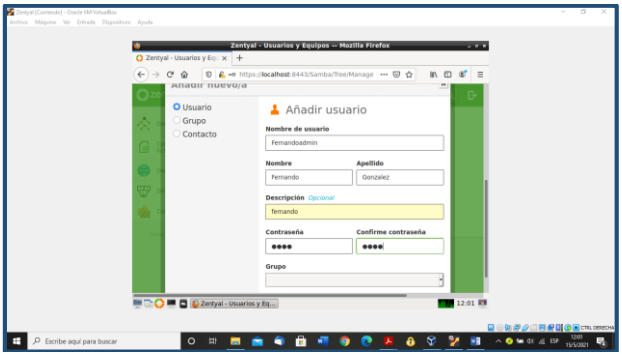

Figura 22. Datos para creación de usuario de dominio

El nuevo usuario se incluye dentro de los usuarios de administración.

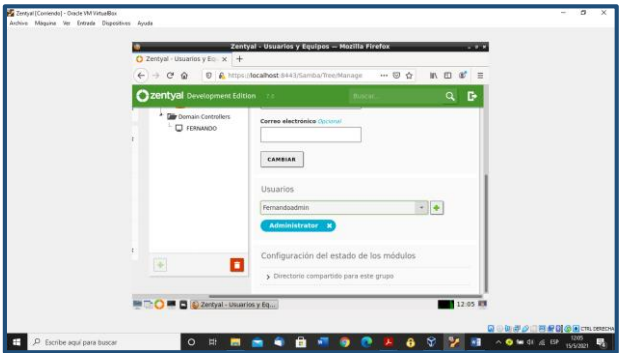

Figura 23. Asignación de usuario como administrador

Para verificar que el dominio está configurado, se ingresa a una maquina Windows y se configura un dominio para conectarse al servidor.

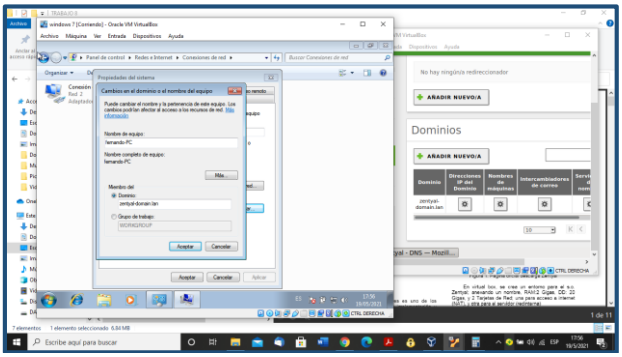

Figura 24. Creación de conexión al dominio en maquina Windows

Se ingresa el nombre del servidor y se autentica por medio del usuario que se creó anteriormente.

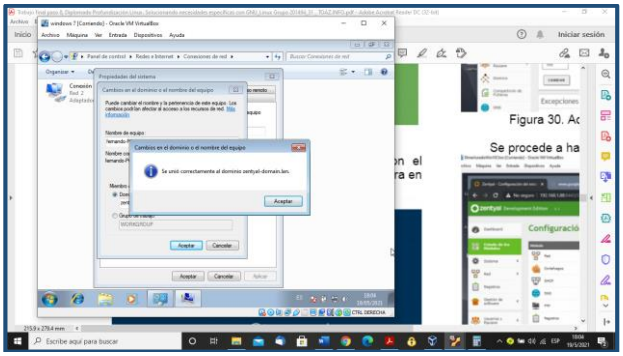

Figura 25. Conexión exitosa con el servidor

Al poder conectar, se pide reinicio de la maquina cliente para confirmar la configuración.

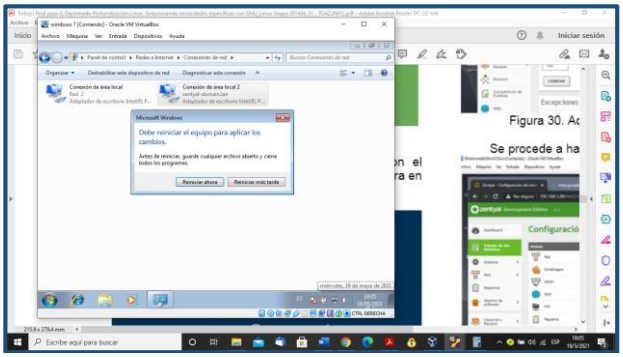

Figura 26. Reinicio solicitado por maquina Windows para configuración

Después del reinicio, se pide entrada con un usuario, se ingresa por la opción OTRO USUARIO y allí se indica que se puede acceder al dominio del servidor con el usuario.

Figura 27. Pantalla de inicio de sesión por medio del dominio

Se ingresa a las redes con el ánimo de verificar que se encuentra en el dominio.

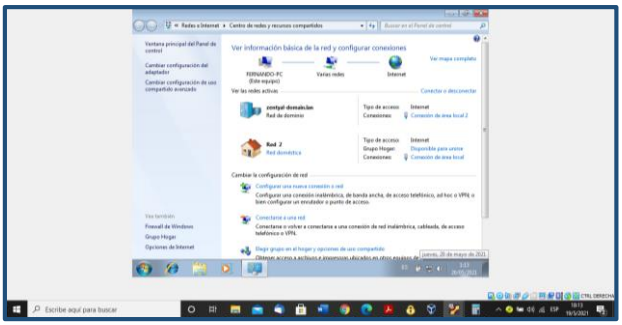

Figura 28. Verificación de conexión al dominio

4 TEMÁTICA 2: PROXY NO TRANSPARENTE

Dentro del desarrollo de la presente temática, se realizó la 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.

Como primer paso se instalaron en Zentyal los paquetes de DHCP server y HTTP Proxy requeridos para configuración del proxy no transparente.

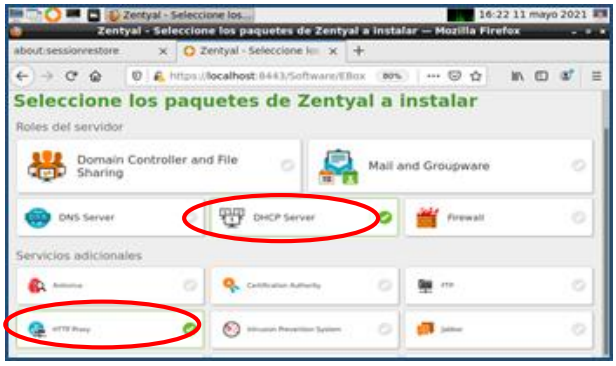

Figura 29. Instalación de paquetes requeridos

Luego de tener instalados los paquetes, se realizó las configuraciones de red en donde eth0 se dejó mediante DHCP y a eth1 mediante el método estático se le asigno la dirección IP 192.168.2.1 con mascara de red tipo c 255.255.255.0

Figura 30. Configuración interfaces de red

Se le asignaron los rangos a la interfaz de eth1 para realizar la respectiva asignación de dirección IP a cada uno de los clientes.

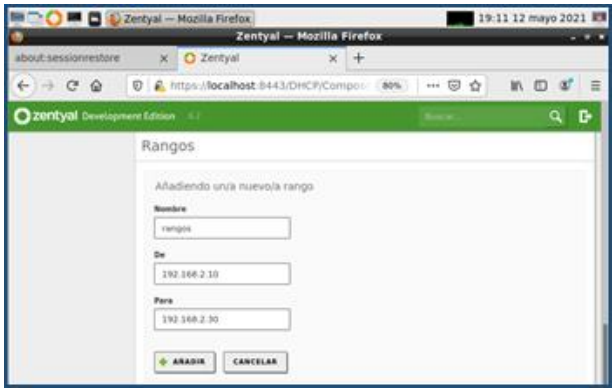

Figura 31. Rango interfaz de red eth1

En el equipo cliente se configuró el adaptador de la red LAN para que la asignación de las direcciones IP se realicen mediante DHCP de acuerdo como van ingresando al servicio y dentro del rango establecido.

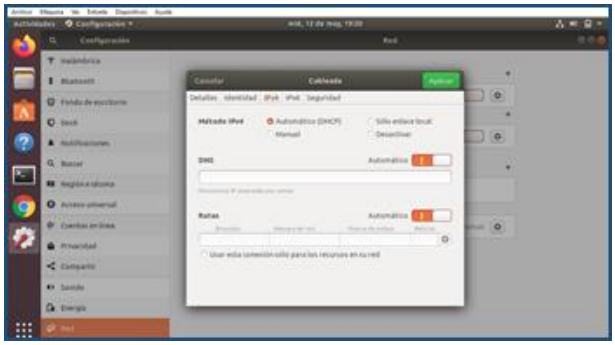

Figura 32. Configuración del adaptador LAN del cliente

Se realizó una prueba con dos máquinas cliente con el fin de verificar que las direcciones IP dentro de la LAN sean asignadas de forma correcta.

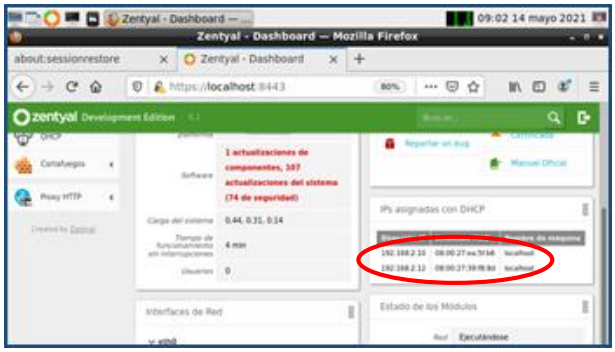

Figura 33. Asignaciones de direcciones IP

Se creó un objeto denominado Ubuntudesktop quien es el cliente1 identificado dentro de la red LAN con la dirección IP 192.168.2.10.

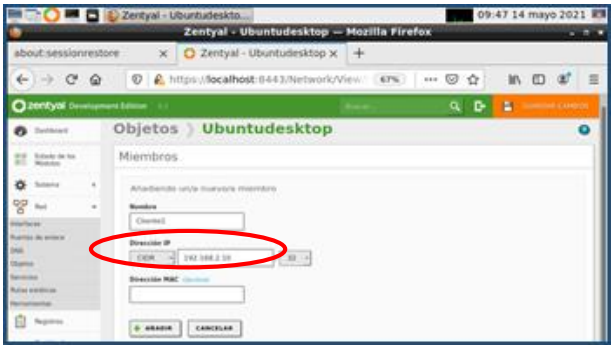

Figura 34. Creación de nuevo objeto

Después de tener creado el objeto, se realizó la configuración general del proxy estableciendo el puerto a través del cual es filtrada la salida que según la guía de aprendizajes es el puerto 1230.

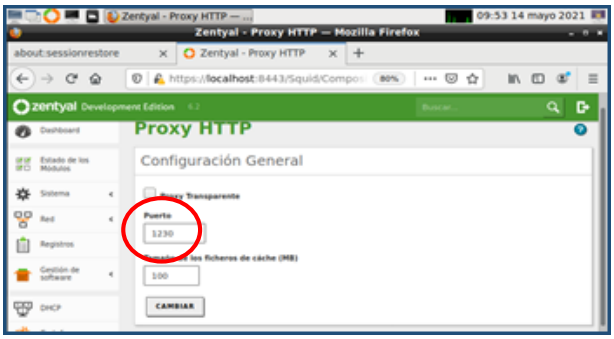

Figura 35. Asignación de puerto de filtrado

De igual forma se agregó una nueva regla de acceso estableciendo el origen que para este caso es el objeto creado como Ubuntudesktop y la decisión que es denegar todo.

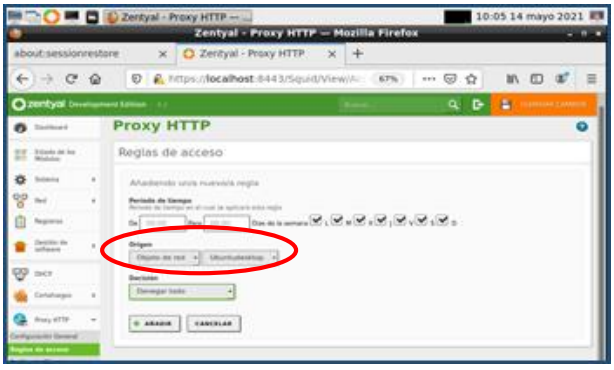

Figura 36. Creación de regla de acceso

Se verificó que la regla haya sido creada de manera correcta relacionando el origen y la decisión.

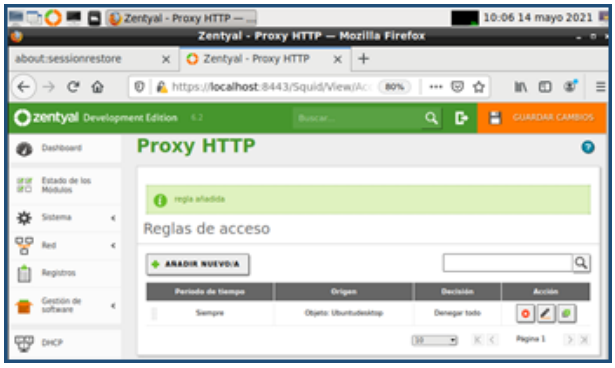

Figura 37. Verificación regla de acceso

Antes de realizar la implementación del proxy no transparente en el cliente, se verificó que la navegación web funcione de manera correcta.

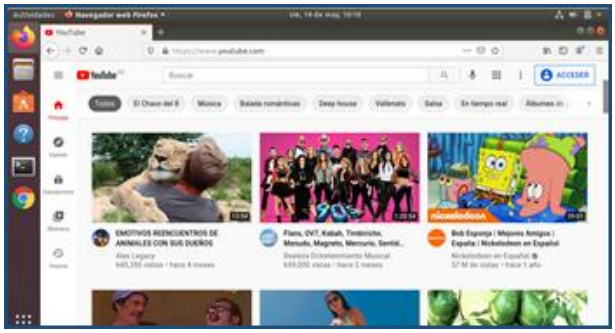

Figura 38. Verificación de la navegación web

Para aplicar el proxy configurado anteriormente se ingresó a la opción de preferencias del navegador con el fin de indicar la dirección IP del servidor proxy y el puerto de filtrado al igual que la configuración del proxy se realiza de forma manual.

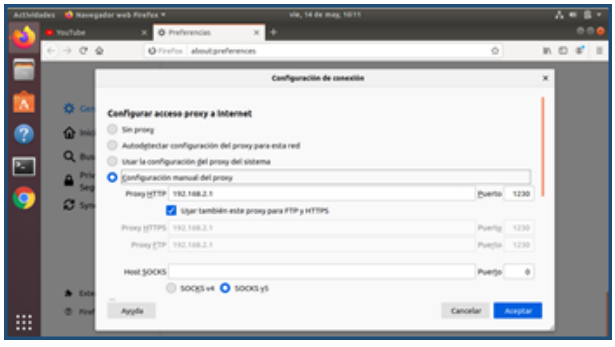

Figura 39. Configuración del proxy en el cliente

Una vez realizadas las configuraciones del proxy en el navegador del cliente, se trató de ingresar a la página de YouTube donde el acceso fue denegado lo que quiere decir que el proxy se encuentra en funcionamiento como se evidencia en la imagen.

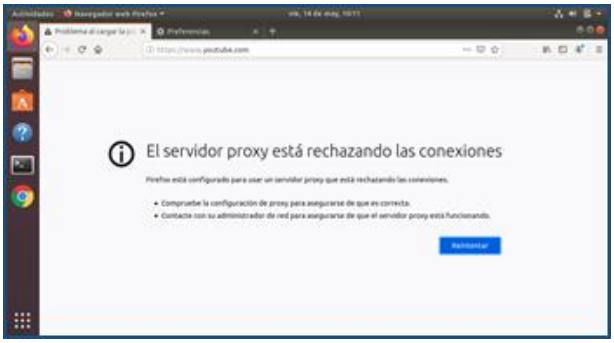

Figura 40. Implementación del proxy no transparente en https

De igual forma se comprobó que al intenta ingresar a un sitio web que este bajo el protocolo http también funciona de forma correcta el proxy restringiendo el acceso.

Figura 41. Implementación del proxy no transparente en http

5 TEMÁTICA 3: CORTAFUEGOS

Procedemos inicialmente a configurar la conexión de red de la máquina virtual y los adaptadores de conexión.

Ingresamos a la configuración de red de la conexión en la máquina virtual.

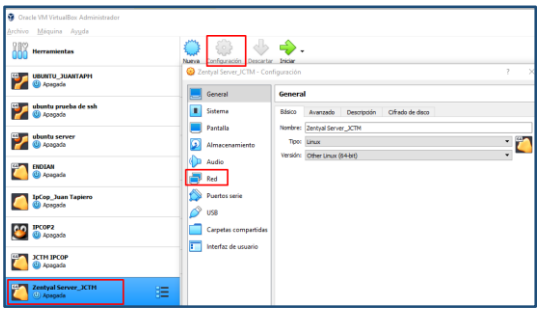

Figura 42. Configuración de red

Configurar red mediante adaptador de red con el pc físico.

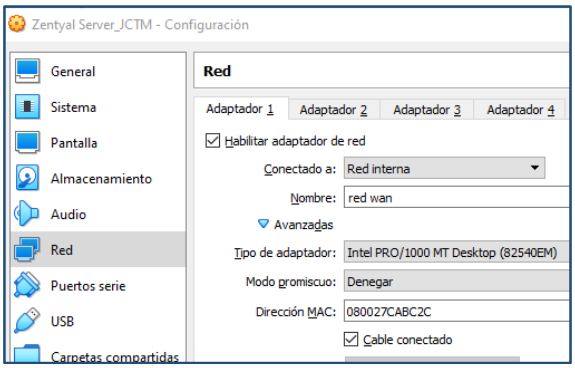

Figura 43. Adaptador 1

Configuración de red nat interna.

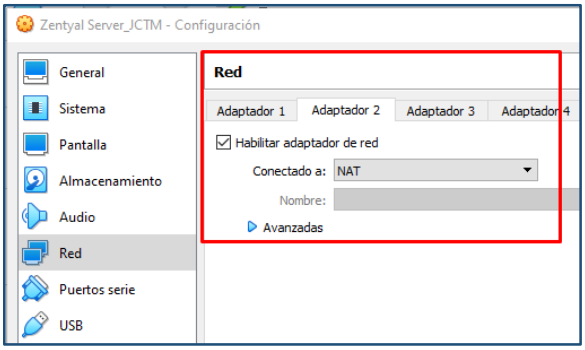

Figura 44. Adaptador 2

Procedemos con realizar la búsqueda de los rangos de direccionamiento IP definidos para restricción mediante acceso web; se procede con añadir un objeto donde se definen los rangos.

Procedemos con la instalación del paquete de firewall y cortafuegos para ejecución del procedimiento correspondiente así:

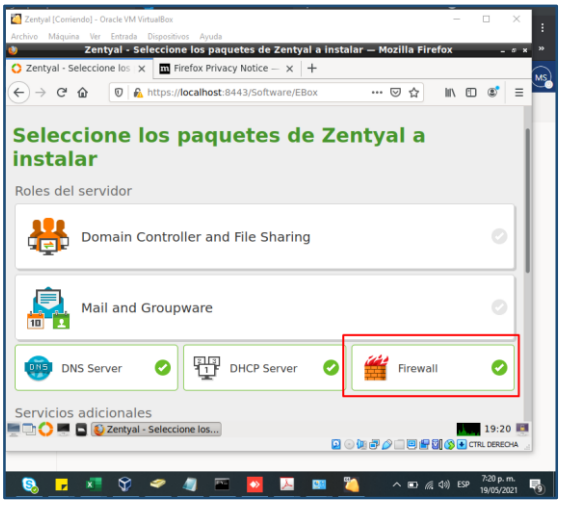

Figura 45. Paquetes a instalar

Procedemos con la selección de los paquetes a instalar así:

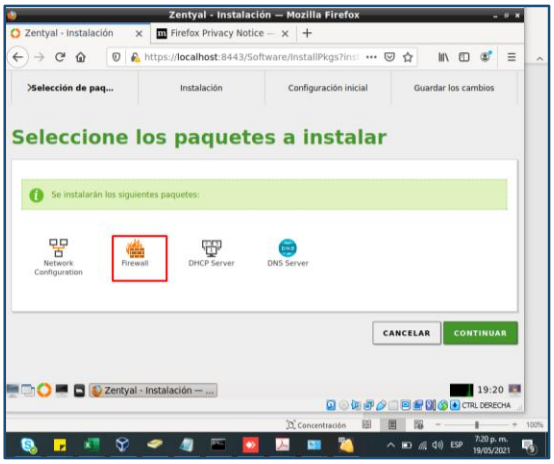

Figura 46. Selección de paquetes

Se observan los avances de instalación correspondiente así:

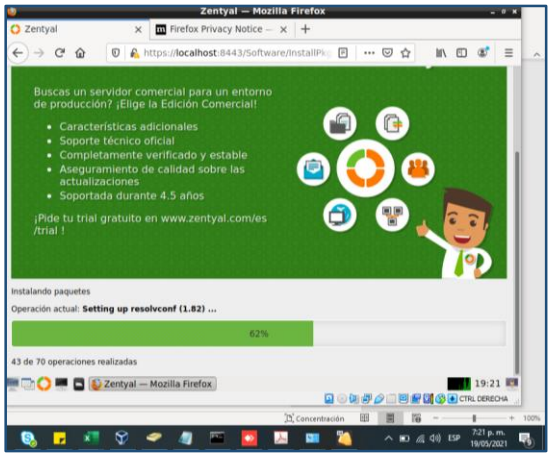

Figura 47. Avances de instalación.

Se procede con dar inicio al asistente de configuración así:

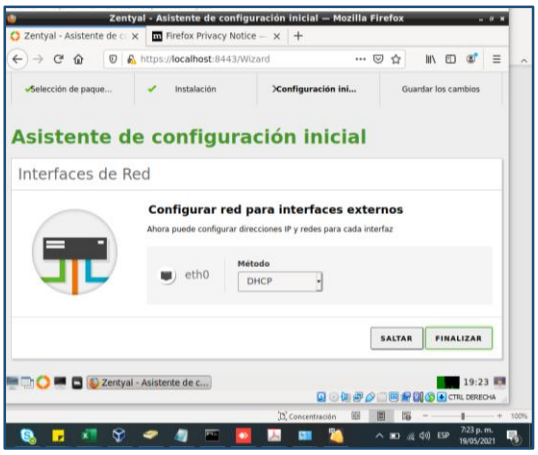

Figura 48. Configuración de red

Nuevamente se observa el avance de la ejecución así:

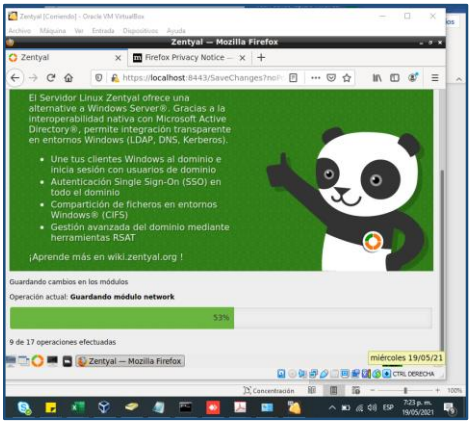

Figura 49. Guardado de configuración.

Se visualiza y se observa la finalización e instalación de los paquetes ejecutados así:

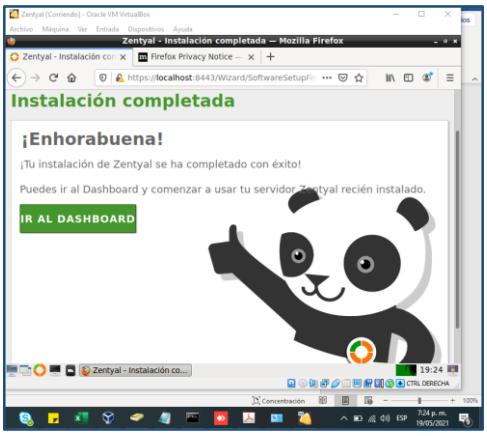

Figura 50. Instalación terminada

Nos dirigimos a la opción de red y seleccionamos la categoría de objetos con el objetivo de crear los objetos de configuración así:

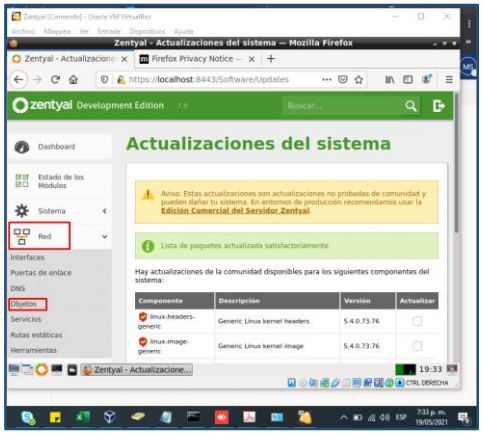

Figura 51. Opción de red

Procedemos con añadir un objeto el cual especifican los rangos de IP.

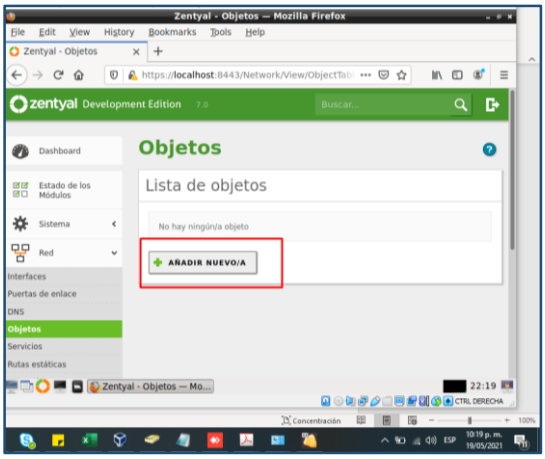

Figura 52. Añadiendo objetos

Se evidencia la opción donde se añade el nombre del objeto.

Figura 53. Objeto creado

Una vez creado el grupo de objetos nos dirigimos a la opción de cortafuegos.

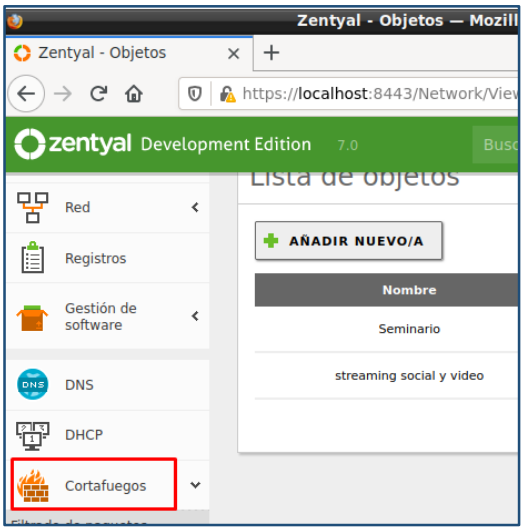

Figura 54. Firewall

Seleccionamos la opción de filtrado de paquetes para efectuar la configuración y administración de las reglas correspondientes de restricción en la navegación de sitios de entretenimiento y redes sociales.

Figura 55. Opción de filtrado

Se observa navegación y acceso a cualquier servicio disponible en la web, desde este módulo procederemos con las reglas de restricción así:

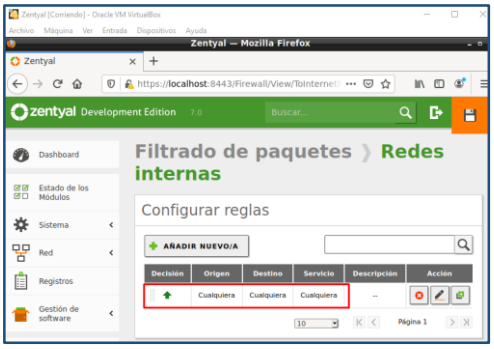

Figura 56. Accediendo a las reglas

Seleccionamos la opción de añadir regla el cual nos permite generar acciones de restricción.

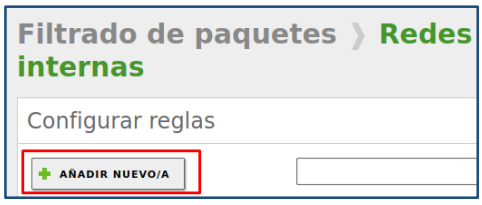

Figura 57. Añadiendo nueva regla

Se ejecuta la configuración así: Opción decisión, el cual permite denegar, permitir o advertir del acceso al sitio web restringido.

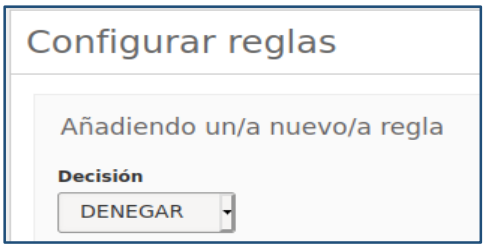

Figura 58. Decisión de regla

En la opción de origen procedeos con la restricción definida así:

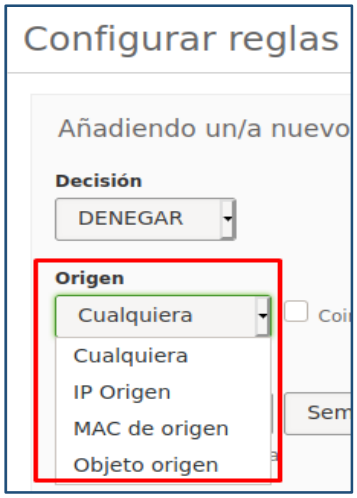

Figura 59. Origen de regla

En la opción de destino seleccionamos si queremos aplicar la restricción a cualquier equipo de la misma red, una ip en específico, una mac de origen o seleccionar un grupo de objeto previamente creado; en este caso específico seleccionaremos una ip de origen así:

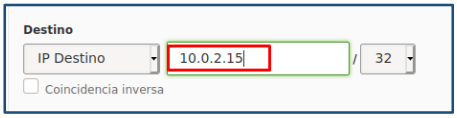

Figura 60. Destino de regla

Seleccionamos el servicio, en este caso específico seleccionamos la opción cualquier tcp así:

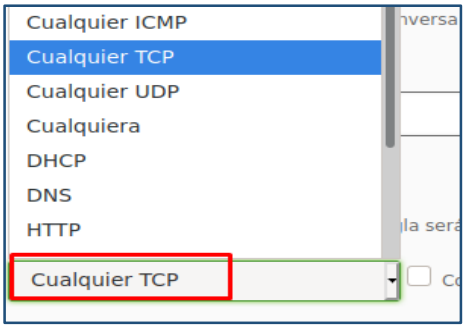

Figura 61. Servicio de la regla

Realizamos la descripción opcional de la regla creada así:

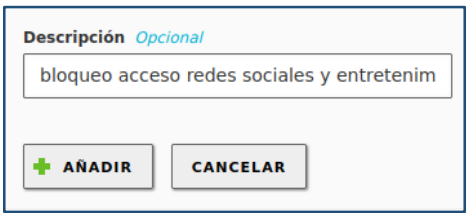

Figura 62. Descripción.

Añadimos regla exitosamente así:

Figura 63. Regla añadida

Se evidencia restricción en el acceso de redes sociales al no cargar la página.

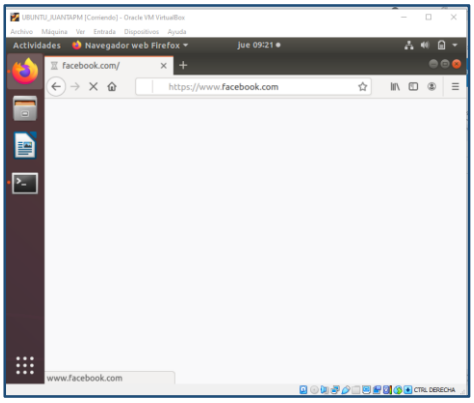

Figura 64. Evidencia de restricción

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

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.

Recordemos que Zentyal permite unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet. Zentyal integra servicios como DNS/DHCP, CA, VPN, backup, gateway, cortafuegos y proxy HTTP, por mencionar algunos.

Después de terminada la instalación inicia el servicio de Zentyal, debemos ingresar Ingresamos con usuario y contraseña creados en los pasos anteriores.

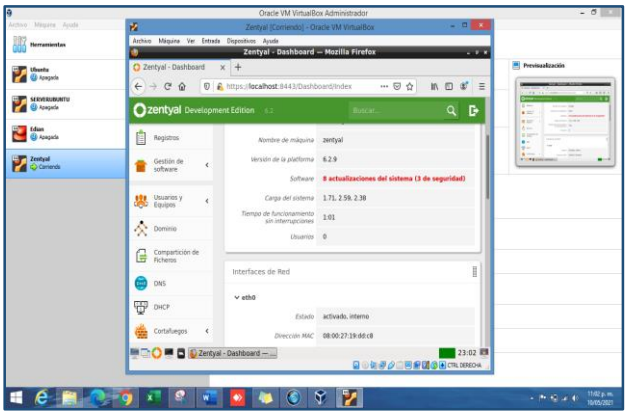

Figura 65. Ingreso con usuario y contraseña asignados. Ingreso correcto.

En esta pantalla nos solicita crear una compartición de ficheros, damos clic en añadir.

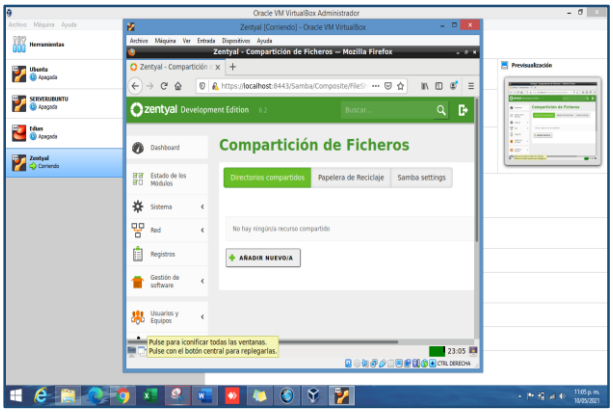

Figura 66. Creación configuración de ficheros

Damos los atributos respectivos al fichero como por ejemplo un comentario. Se crea el directorio compartido santiago_unad el cual quedará /home/samba/shares

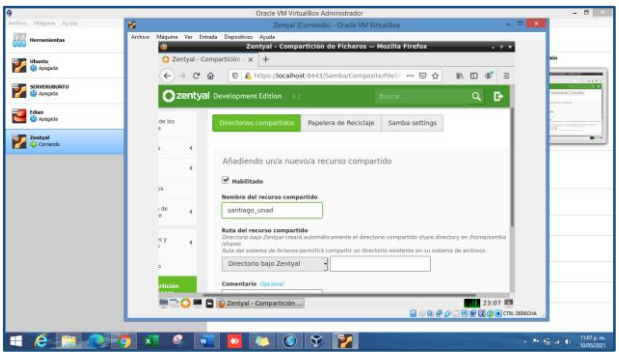

Figura 67. Fichero creado correctamente

Podemos visualizar entonces cómo se crea el servicio compartido con sus respectivos atributos de configuración.

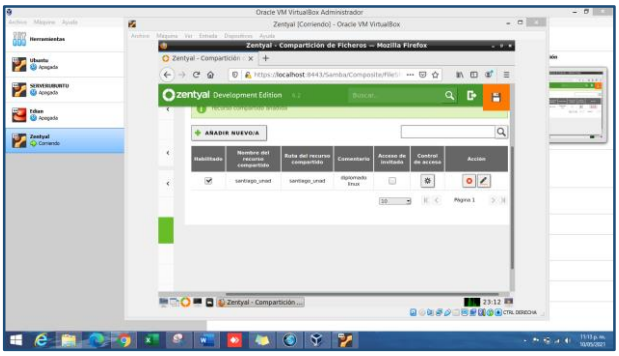

Figura 68. Finalización Fichero compartido

Se ingresa a la máquina cliente y se realizan las actualizaciones respectivas para mantener la máquina actualizada. Después de ingresar la dirección 10.0.2.15 se evidencia la visualización del fichero compartido.

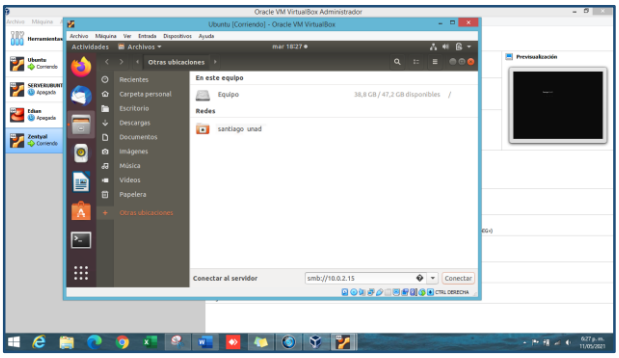

Figura 69. Acceso fichero desde Cliente

Para poder compartir impresoras es necesario utilizar el componente CUPS ya que para esta versión de Zentyal se necesita este complemento.

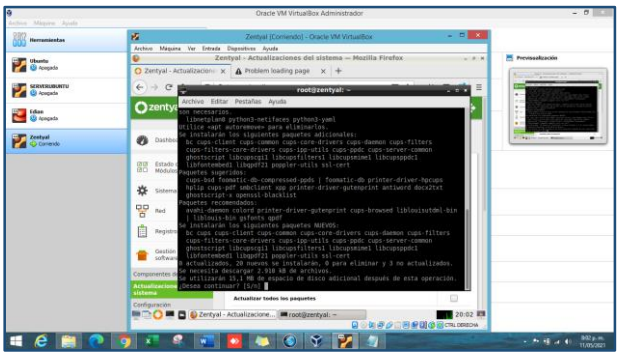

Figura 70. Configuración componente CUBS

Utilizando el comando sudo apt-get install cups se instalará el componente y complemento de gestión de impresoras. Posteriormente Ingresamos a la dirección https://localhost:613/admin donde se evidencia el panel de control para la gestión de impresoras.

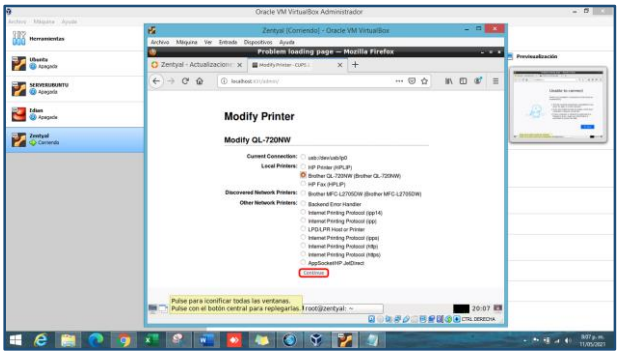

Figura 71. Panel Gestión de Impresoras

7 TEMÁTICA 5: VPN

Una vez instalado Zentyal, se puede realizar su configuración inicial, instalando el módulo VPN. Donde adicionalmente se instalarán los paquetes de Certification Autority, Firewall, Network Configuration y VPN.

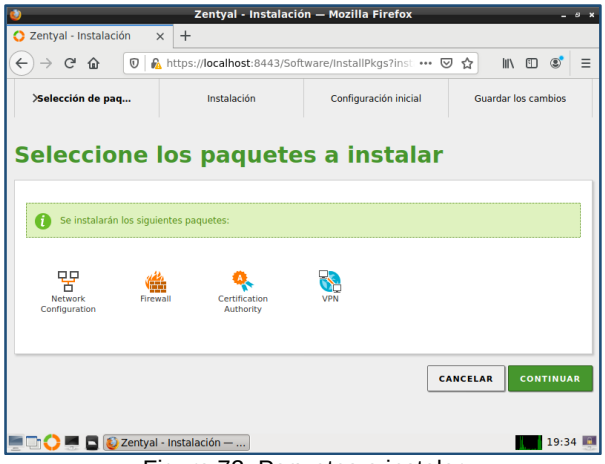

Figura 72. Paquetes a instalar

7.1 CERTIFICACIÓN Y CONFIGURACIÓN DE SERVIDOR VPN

Una vez se realiza la configuración inicial, el sistema empieza a guardar dicha configuración. Una vez hecho esto, se cargará la Dashboard, en la cual se puede apreciar en la parte izquierda, las distintas opciones que tiene disponible, allí, se deberá ir inicialmente a Autoridad de Certificación/General, esto, para expedir un certificado que permita la implementación del servidor VPN.

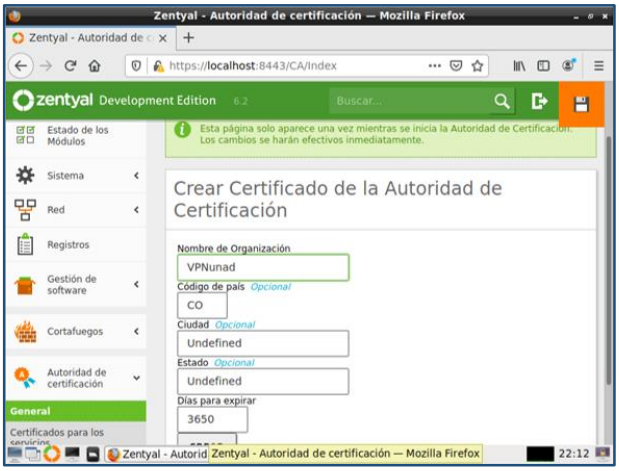

Figura 73. Certificado para servidor vpn

Una vez creado el certificado para el servidor VPN se puede continuar a añadir un nuevo servidor VPN, esto, desde VPN/Servidores, que estará ya habilitado.

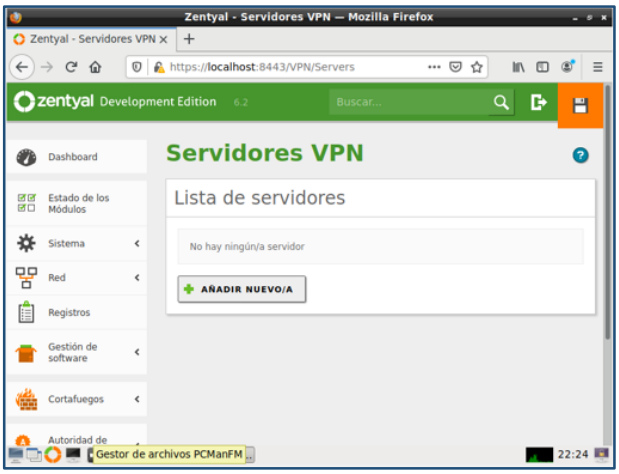

Figura 74. Función de servidor vpn habilitada

Después de añadir un nuevo servidor, se le asignará un nombre y se añadirá, una vez hecho esto, mostrará lo siguiente:

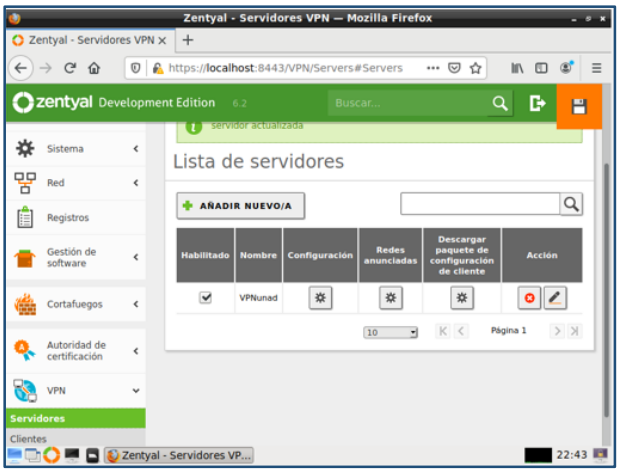

Figura 75. Servidor vpn añadido

Siguiente al añadimiento del nuevo servidor VPN, se procede a configurarle los parámetros en los que funcionará. En esta configuración se le asignará un puerto, una dirección VPN, el certificado anteriormente creado para el servidor VPN y los parámetros necesitados.

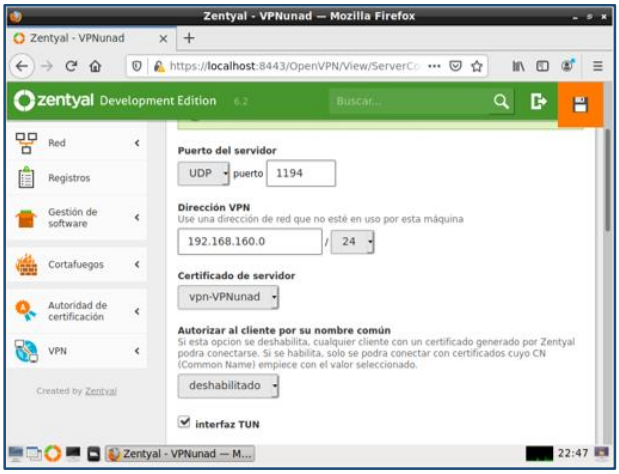

Figura 76. Parámetros de configuración en servidor vpn

7.2 CERTIFICACIÓN Y CONFIGURACIÓN DE USUARIO

Para que un usuario pueda hacer uso del servidor VPN se deberá crear un certificado que le permita al usuario hacer uso de este servidor. Para ello, nuevamente en Autoridad de Certificación/General se expide un certificado para el usuario.

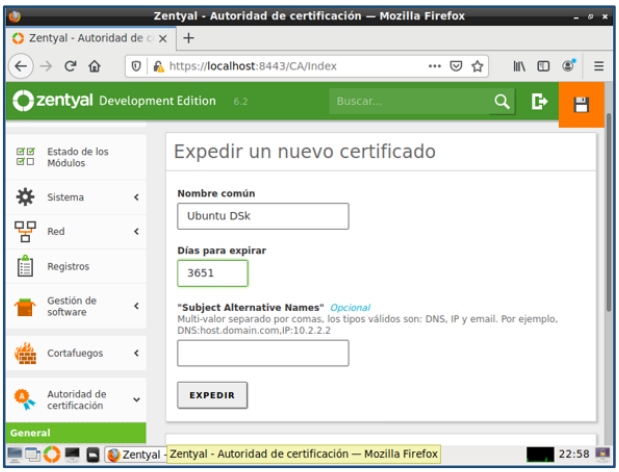

Figura 77. Certificado para usuario

Una vez expedido el certificado para el usuario, nuevamente en Servidores VPN se escoge la opción de “Descargar paquete de configuración de cliente”, después cargará la ventana donde se deberán configurar los parámetros del usuario donde se seleccionará el tipo de usuario, el certificado del usuario, tipo de conexión y dirección del servidor, la cual deberá ser una IP estática.

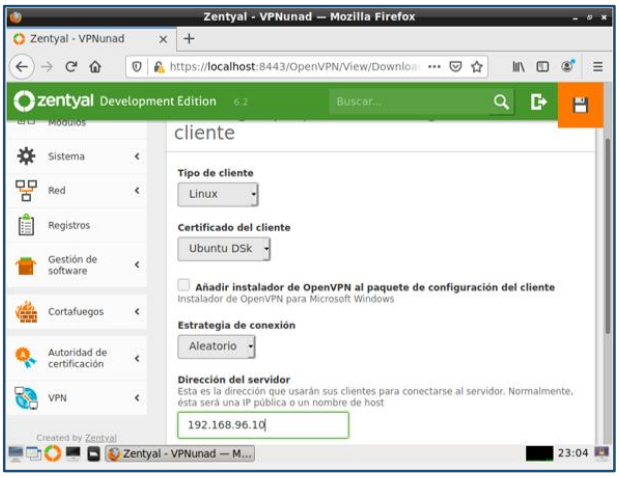

Figura 78. Parámetros de configuración del cliente

Este generará un paquete de configuración para el cliente y que así se pueda configurar los parámetros de configuración en el equipo del cliente de manera más sencilla.

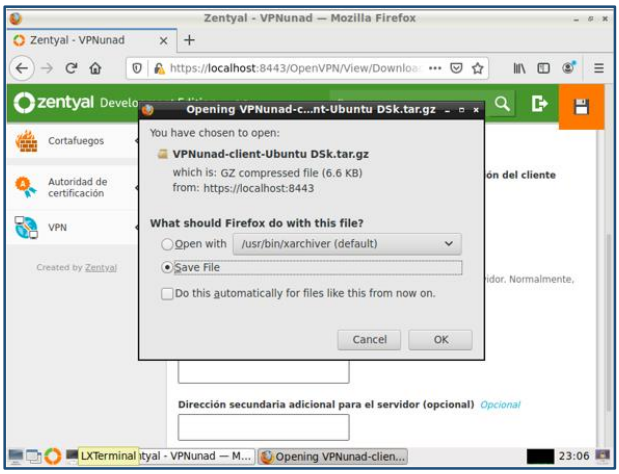

Figura 79. Paquete de configuración para cliente

Ahora desde el cliente se añade una nueva VPN, esto, desde configuración de red del equipo, donde si no es posible mover el paquete de configuración previamente descargado en el servidor, se escogerá un el “Protocolo de túnel punto a punto (PPTP)”.

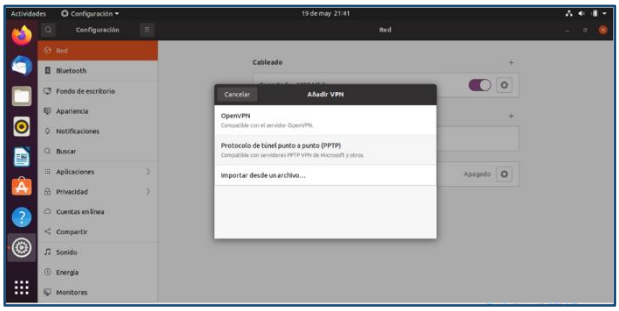

Figura 80. Añadiendo vpn en cliente

Una vez seleccionado el protocolo, se define un nombre con el que se identificará en el equipo (este nombre no afecta la configuración y funcionamiento), y se le agrega la pasarela, que es la IP configurada en los parámetros del cliente en el servidor. Después de esto se seleccionará la configuración avanzada.

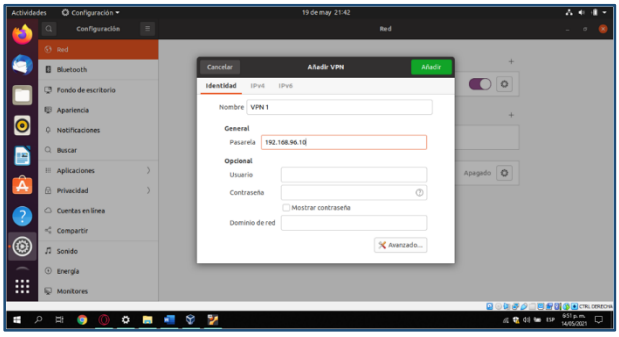

Figura 81. Configuración inicial en cliente

En configuración avanzada, se selecciona la casilla “Usar cifrado punto a punto (MPPE)”, luego se acepta la configuración y se añade la conexión VPN.

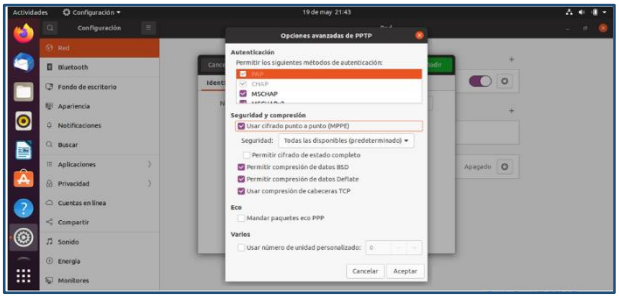

Figura 82. Configuración del cifrado en cliente

Después de configurar lo anterior se podrá habilitar la conexión VPN.

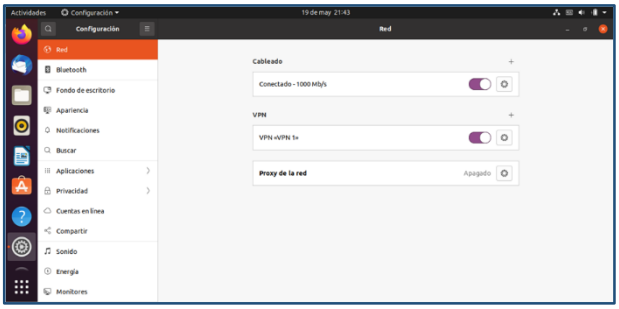

Figura 83. Conexión vpn habilitada en cliente

Otra forma de demostrar que el servidor VPN se está ejecutando, es en la Dashboard del servidor Zentyal donde muestra la información de los “Demonios OpenVPN”.

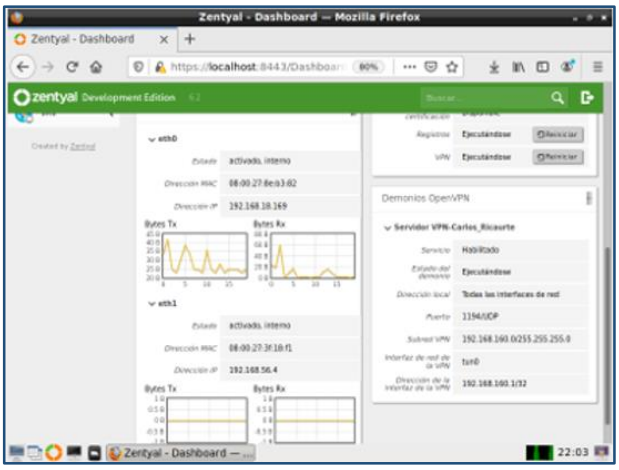

Figura 84. Pruebas de ejecución en la dashboard

8 CONCLUSIONES

El presente trabajo nos permitió la manipulación de un sistema de servidor el cual es muy simple y amigable para realizar las configuraciones de seguridad y acceso solicitados en la guía, reconociendo los parámetros necesarios para su uso correcto.

La implementación de un proxy no transparente puede ser muy útil tanto en el ámbito laboral como en el profesional, ya que si se quiere tener el control del acceso a internet de los diferentes equipos que pertenecen a una LAN basta con realizar la implementación de este servicio y así permitir o restringir el acceso por medio del filtrado de salida a través de un puerto determinado.

Una de las grandes diferencias entre el proxy transparente y el no transparente es que, en primero, el navegador no es notificado que se encuentra bajo un servidor proxy a diferencia del segundo el cual para su aplicación se debe configurar en cada uno de los clientes indicando la IP del servidor proxy y el puerto para su uso

Durante el desarrollo del Paso 8 - Solucionando necesidades específicas con GNU/Linux, pudimos aprender a administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet. Zentyal integra servicios como DNS/DHCP, CA, VPN, backup, gateway, cortafuegos y proxy HTTP, por mencionar algunos. Se realizó la formulación de soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente.

Se aprendió a como instalar y configurar el servidor VPN y en su proceso la configuración inicial de Zentyal. Con la instalación VPN se nos permite crear conexiones a una red local de manera privada.

En esta actividad se logra entender que la administración, control y auditoria de la infraestructura tecnológica son de vital importancia dado a que brindan servicios de acceso y permanencia al buen uso adecuado de los recursos tecnológicos a disposición.

La identificación de las necesidades e incidencias permiten la mejora continua para así garantizar el acceso y permanencia continua de cada uno de los sistemas a disposición y es de esta manera que se generan planes de acción que mitigan los riesgos operativos.

9 REFERENCIAS

[1] Zentyal 7.0 Documentación Oficial — Documentación de Zentyal 7.0. (2004, 1 enero). zentyal. Disponible en: https://doc.zentyal.org/es/

[2] Zentyal. (2020, 6 febrero). Tutorial: Instalación y configuración de Zentyal Server para la implementación de servicios de Infraestructura IT. Zentyal Linux Server. Disponible en: https://zentyal.com/es/news/tutorial-instalacion-y-configuracion-de-zentyal-server-para-la-implementacion-de-servicios-de-infraestructura-it/

[3] Doc.zentyal.org (2015). Apéndice A: Entorno de pruebas con VirtualBox. Disponible en: https://doc.zentyal.org/es/appendix-a.html

[4] Zentyal (2004-2020). Servicio de configuración de red (DHCP). Disponible en: https://doc.zentyal.org/es/dhcp.html

[5] Zentyal Community. (2015). Servicio de redes privadas virtuales (VPN) con OpenVPN [En línea]. Disponible en: https://doc.zentyal.org/6.2/es/vpn.html#configuracion-de-un-servidor-openvpn-con-zentyal