INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER COMO SOLUCIÓN DE INFRAESTRUCTURA TECNOLÓGICA.

Esteban Danilo Cerón Arcos
edcerona@unadvirtual.edu.co
Marcela Gómez Álvarez
rmgomeza@unadvirtual.edu.co
Pablo Gómez Silva
pgomezs@unadvirtual.edu.co
Alejandro Molina Gómez
amolinago@unadvirtual.edu.co

RESUMEN: *El siguiente articulo muestra la instalación, configuración y puesta en marcha del servidor GNU/Linux Zentyal para dar soluciones de infraestructura tecnológica a requerimientos específicos de un cliente, donde se formula soluciones implementando los servicios DHCP, DNS, controlador de dominio, proxy no transparente, cortafuegos, VPN, carpetas compartidas e impresoras, utilizando una interfaz amigable que permite dar soluciones efectivas, seguras e intuitivas de configurar, facilitando la centralización y la gestión integral de los servicios.*

PALABRAS CLAVE: Cortafuegos, DHCP/DNS, GNU/Linux Zentyal, VPN.

1 INTRODUCCIÓN

Este articulo incluye las instrucciones de instalación del servidor Zentyal y la configuración de servicios de infraestructura tecnológica como el acceso a una estación de trabajo a través de un usuario y contraseña del controlador de dominio, control y acceso a internet bajo un proxy no transparente, apertura de sitios web mediante reglas y políticas en el cortafuegos, acceso a carpetas e impresoras compartidas y establecer un túnel privado de comunicación con una estación de trabajo bajo una VPN.

2 SERVIDOR ZENTYAL

Para la instalación del servidor Zentyal [1] se debe descargar la ISO que se obtiene de la página oficial https://zentyal.com, en la siguiente instalación se utiliza la versión 6.2 [2]

En la configuración inicial se utiliza VirtualBox [3] para emular dos estaciones de trabajo, la cual una de ellas corresponde al servidor Zentyal y la otra como estación cliente, en la máquina virtual del servidor se configuran dos adaptadores de red, uno de ellos corresponde al adaptador puente para acceder a internet y el otro corresponde a una red interna “LAN”. En cuanto al cliente, solo tiene un adaptador con una red interna “LAN”. Ver figura 1 y 2.

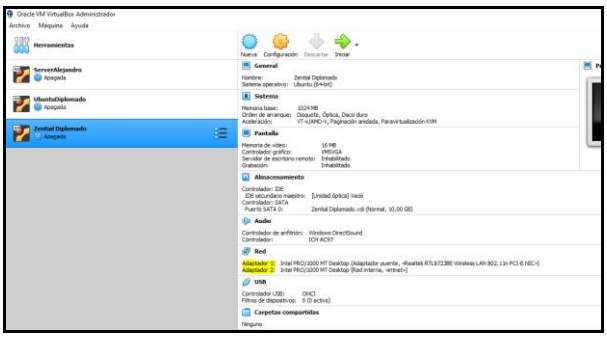

Figura 1. Configuración tarjeta de red servidor Zentyal.

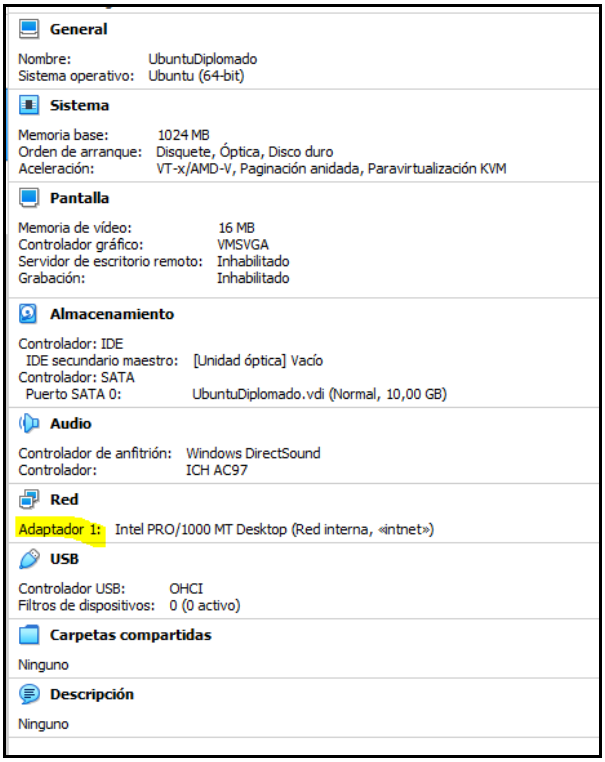

Figura 2. Configuración tarjeta de red estación cliente.

Una vez realizadas las configuraciones anteriores se inicia la instalación del servidor Zentyal [4], donde inicialmente el instalador solicita el idioma, donde se elige “español”. Ver figura 3.

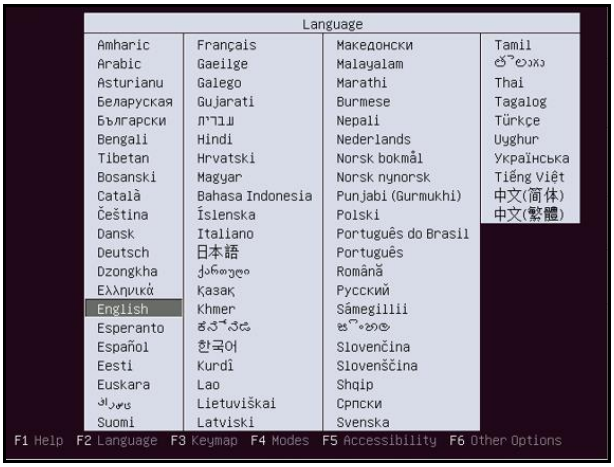

Figura 3. Selección del idioma de instalación.

En el instalador se despliegan opciones que permite el instalador, en este caso escogemos “Instalar Zentyal 6.2-development”, luego seleccionamos el idioma por defecto del sistema operativo una vez se instala Zentyal, donde escogemos la opción “español” y continuamos con la selección de la zona horaria escogiendo el país, en este caso “Colombia”. Ver figura 4.

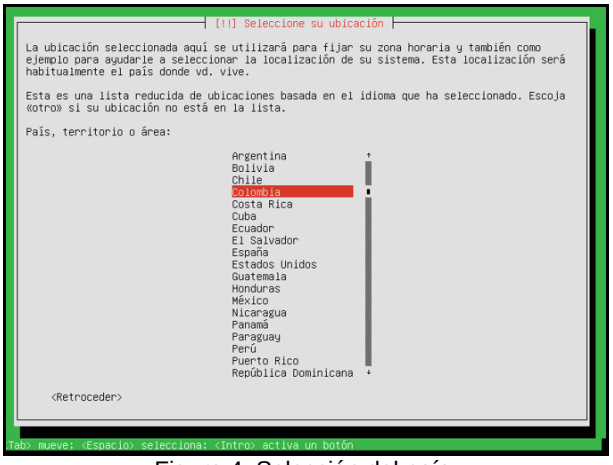

Figura 4. Selección del país.

A continuación, se configura el teclado y su distribución, seleccionando la opción “Spanish (Latin American)”, la configuración de la red, seleccionando la interfaz principal que se utilizará durante la instalación y el nombre de la máquina. Ver figura 5 y 6.

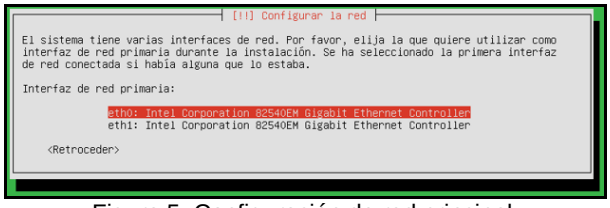

Figura 5. Configuración de red principal.

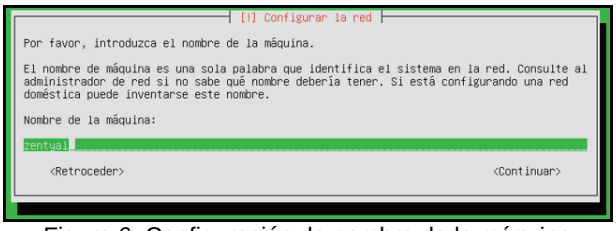

Figura 6. Configuración de nombre de la máquina

Como paso siguiente se realiza la configuración del usuario y contraseña para la administración del servidor, la zona horaria basado en el país seleccionado que el sistema inicialmente ha configurado.

Una vez realizado los pasos anteriores, inicia la instalación, se muestra barra de progreso y cuando termina la instalación se muestra mensaje de confirmación, en este punto se presiona continuar, en donde el sistema se reiniciará e iniciará el sistema operativo mostrando el navegador Firefox con la página administrativa. Ver figura 7.

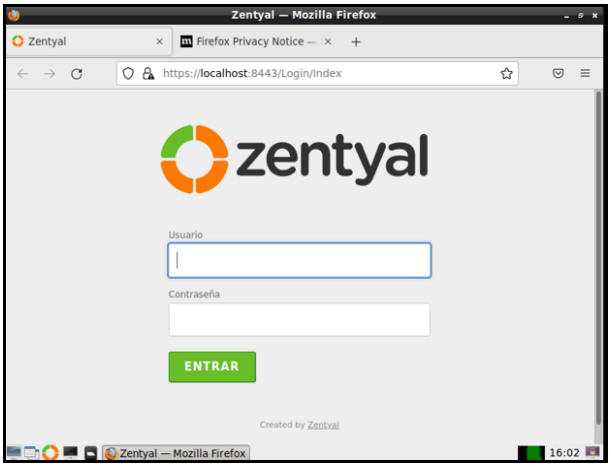

Figura 7. Inicio del servidor Zentyal.

Se inicializa la configuración del servidor, instalando el paquete de red y configurando las interfaces de red, dejando el primer adaptador para la red de interna, y el segundo para la red local. Ver figura 8 y 9.

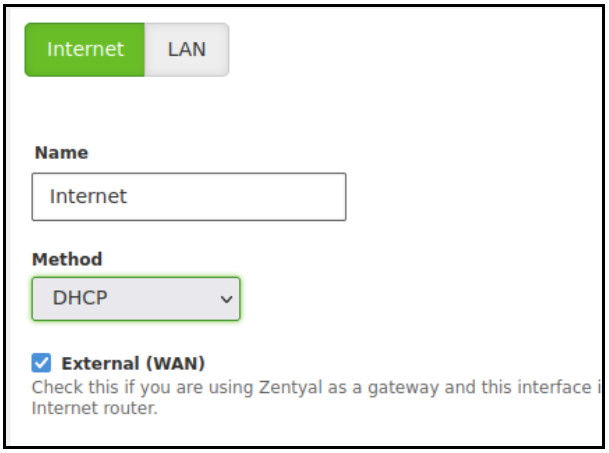

Figura 8. Configuración de interfaz de internet

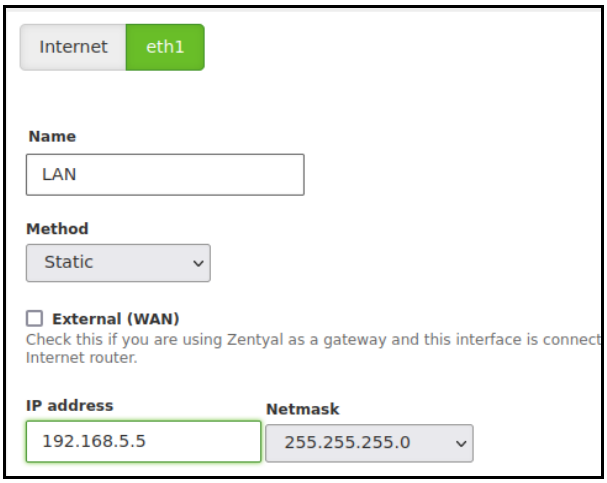

Figura 9. Configuración de interfaz LAN

3 CONFIGURACIÓN DEL SERVICIO DHCP, DNS Y CONTROLADOR DE DOMINIO.

3.1 INSTALACIÓN DE PAQUETES PARA EL MANEJO DEL DOMINIO.

Se instalan los paquetes para la configuración de nuestro servidor y poder configurarlo como dominio. Ver figura 10.

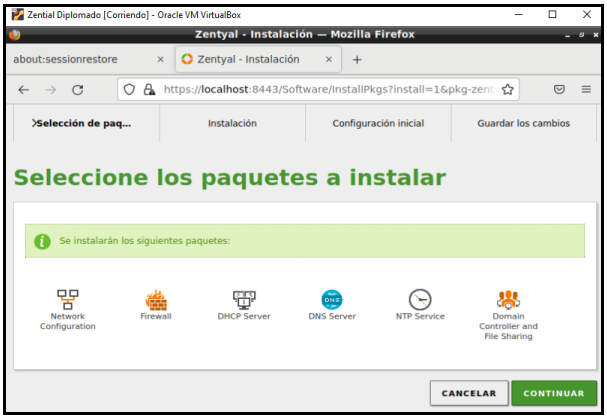

Figura 10. Instalación aplicaciones.

3.2 CONFIGURACION INICIAL DEL DOMINIO.

Se configura el nombre de dominio como grupo32.unad.com. Ver figura 11[5].

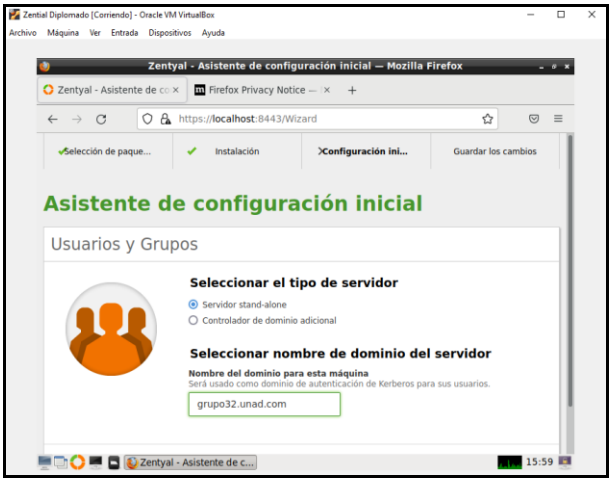

Figura 11. Configuración nombre dominio.

Configuramos la sección DNS y validamos que esté activo el dominio que creamos y que tenga una IP válida dentro del rango de la red. Ver figura 12.

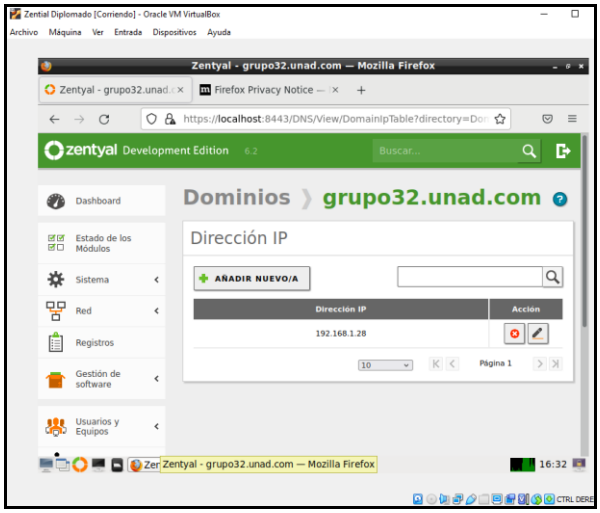

Figura 12. Asignación IP de dominio

Para la configuración del DHCP [6], procedemos a ponerle dirección a la red interna, como estática y le damos la IP 192.169.2.100. Ver figura 13.

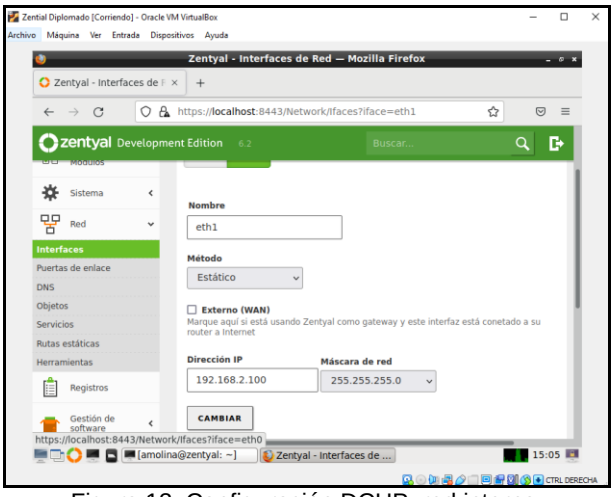

Figura 13. Configuración DCHP, red interna.

Configuramos nuestro nuevo rango, el cual va a hacer el único que se asignara a los clientes, desde la IP 192.168.2.10 a 192.168.2.50.

Validamos qué la dirección IP que le asigna a nuestro cliente este dentro del rango seleccionado. Ver figura 14.

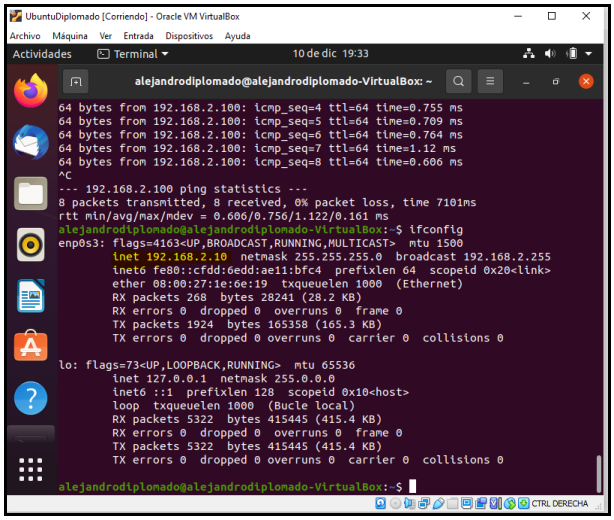

Figura 14. Validación IP cliente.

Para la configuración de los usuarios vamos a la parte izquierda usuarios y grupos y creamos nuestro nuevo usuario dentro del grupo creado. Ver figura 15.

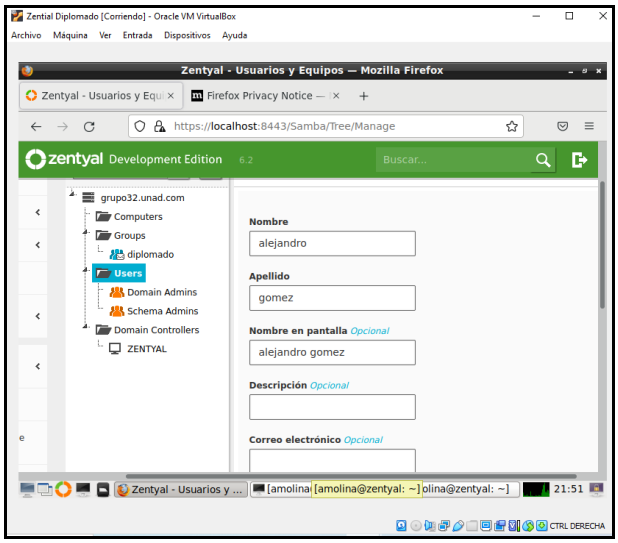

Figura 15. Creación usuarios y grupos.

Procedemos con la configuración de nuestro cliente, lo primero que hacemos es descargar un programa para la gestión de directorio activo en este caso 64 bits desde la página oficial, luego le asignamos permisos 777 y lo instalamos. Ver figura 16.

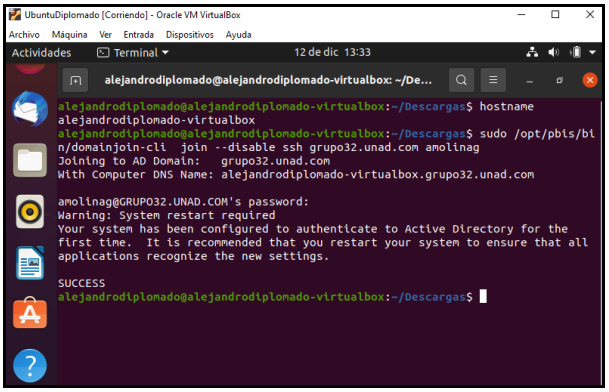

Figura 16. Instalación paquetes dominio cliente.

Cuando termine reiniciamos el sistema y luego configuramos el usuario amolinag en el dominio grupo6.unad.com. Ver figura 17.

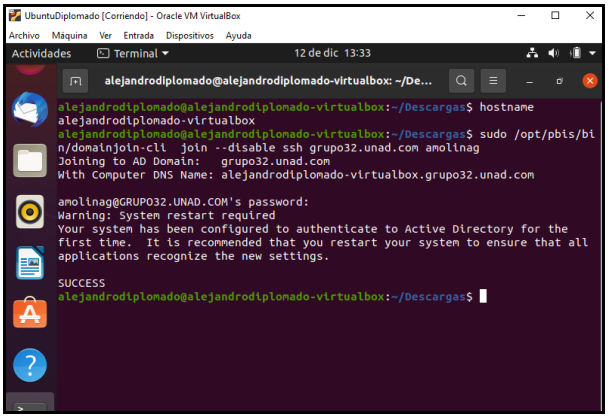

Figura 17. Configuración usuario al dominio cliente.

Validamos en nuestro servidor Zentyal, que aparezca nuestro cliente ya en lista de computadores. Ver figura 18.

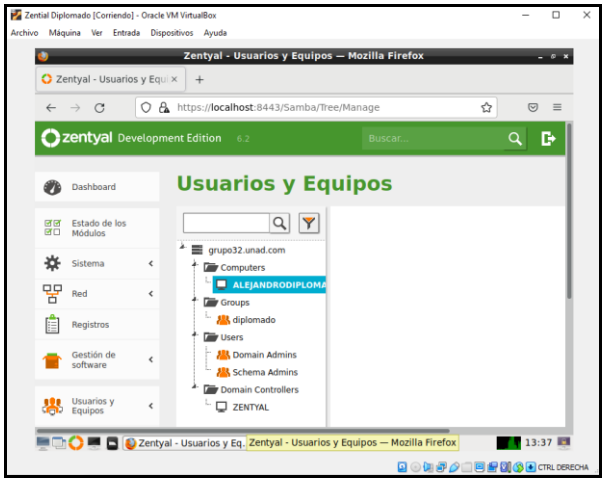

Figura 18. Validación cliente asignado en servidor.

Después en nuestro cliente editamos el archivo 50-ubuntu.conf para colocar un login manual y finalmente agregamos un Shell al usuario cuando inicie sesión. Ver figura 19.

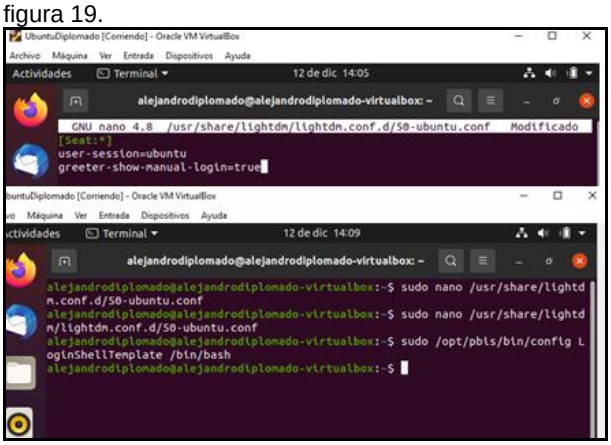

Figura 19. Instalación utilidades cliente.

Reiniciamos nuestro cliente e iniciamos con nuestro dominio con grupo32.undad.com\amolinag, después debe aparecer ya por defecto los dos usuarios el del cliente y el del dominio que Alejandro Gómez. Ver figura 20.

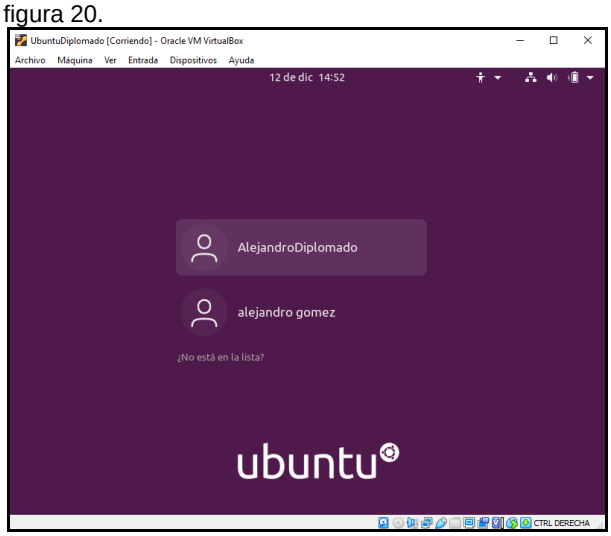

Figura 20. Validación de los dos usuarios cliente.

Nuestro usuario y contraseña se encuentra registrados en el controlador de dominio Zentyal, se iniciará la sesión donde al abrir la terminal observamos que aparecerá de la siguiente forma especificando que se estará conectado desde el servidor "GRUPO32\amolinag@alejandrodiplomado-virtualbox". Ver figura 21.

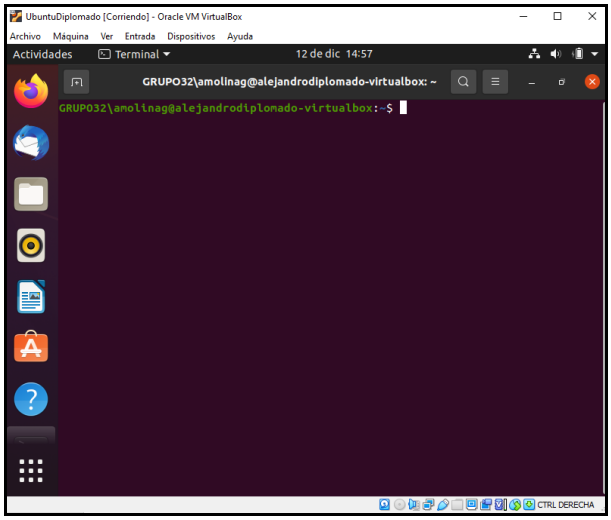

Figura 21. Terminal cliente con usuario dominio.

4 CONFIGURACIÓN DEL SERVICIO HTTP PROXY.

Para la instalación y configuración del servicio HTTP Proxy [7] se accede al menú de Gestión de software para realizar la instalación de los componentes requeridos, en la instalación se mostrará mensaje con los paquetes requeridos y una vez finaliza se muestra mensaje de confirmación de la instalación. Ver figura 22.

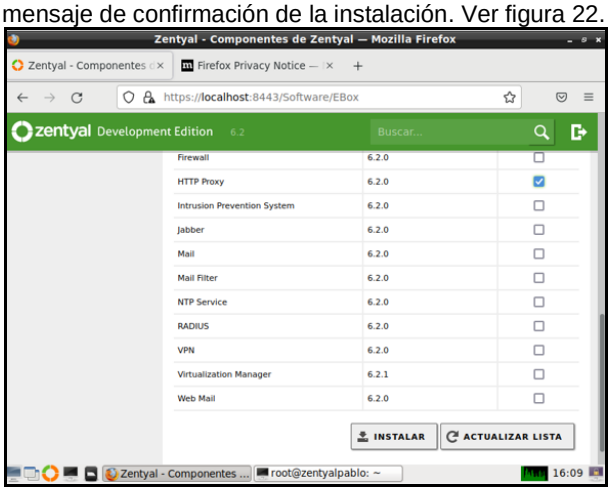

Figura 22. Instalación de componente HTTP Proxy.

Se navega al menú de estado de módulos para activar los paquetes previamente instalados y guardar la configuración. Ver figura 23.

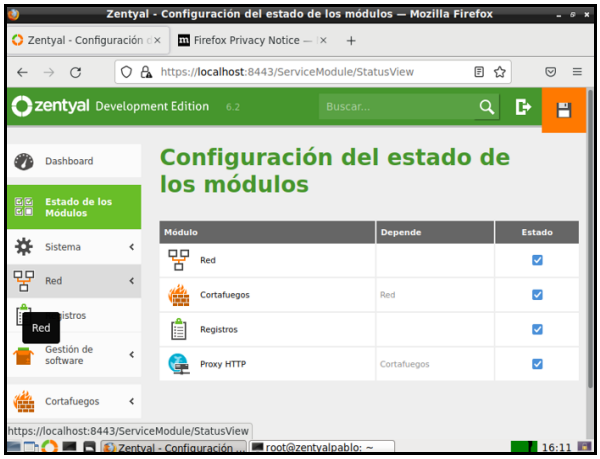

Figura 23. Configuración del estado de módulos.

Al finalizar la activación de los paquetes es importante que en el dashboard aparezcan ejecutándose los servicios. Ver figura 24.

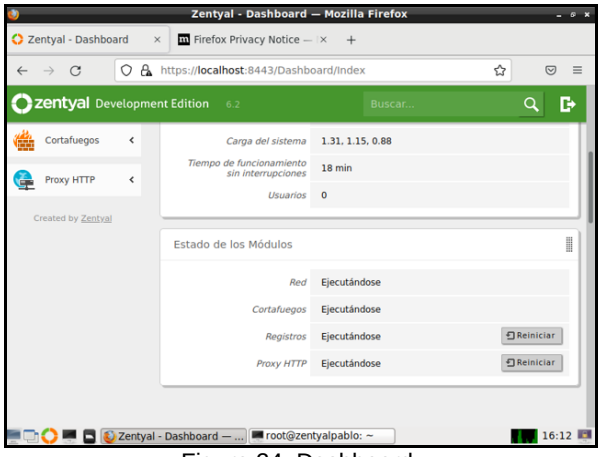

Figura 24. Dashboard.

A continuación, se procede a realizar el cambio del puerto por defecto del proxy por el 1230, accediendo al menú del Proxy HTTP opción Configuración general. Ver figura 25.

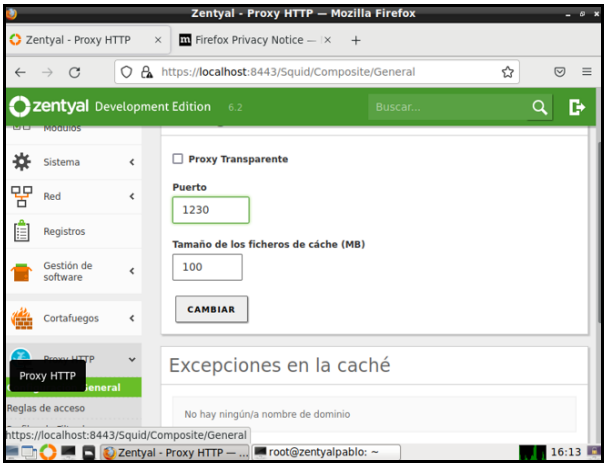

Figura 25. Configuración de puerto del proxy.

Se realiza configuración de perfil de filtrado y adición de dominios y URL para restringir el acceso a páginas de redes sociales. Ver figura 26 y 27.

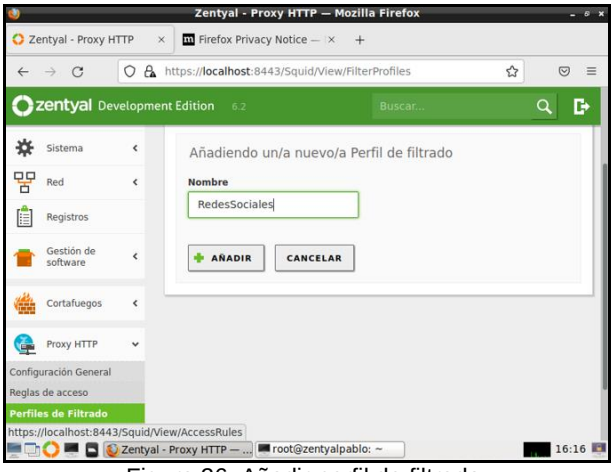

Figura 26. Añadir perfil de filtrado.

Figura 27. Añadir dominio y URL.

Se procede a ingresar al menú de reglas de acceso para configurar la regla actual y se cambia la decisión por defecto para aplicar el perfil de filtrado y seleccionamos el registro previamente creado. Ver figura 28.

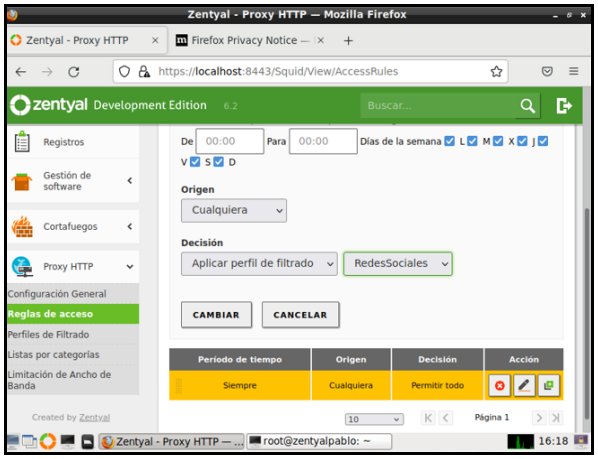

Figura 28. Configuración de regla de acceso.

Se realiza la prueba de la configuración previamente realizada, se realiza ajuste del proxy en la estación cliente con el host y puerto del servidor. Ver figura 29.


Figura 29. Configuración de proxy.

Teniendo en cuenta la configuración de las reglas de filtrado se observa que no se puede acceder a una de la paginas de redes sociales, en este caso Facebook. Ver figura 30.

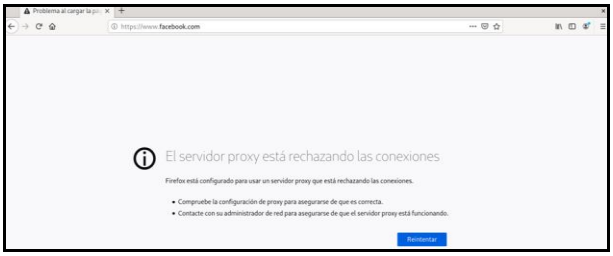

Figura 30. Acceso denegado por el proxy.

5 CONFIGURACIÓN DEL SERVICIO CORTAFUEGOS.

A continuación, se indicará como cerrar los puertos a portales web de entretenimiento y redes sociales, donde nos dirigimos a firewall para bloquear las redes sociales (Facebook e Instagram).

Configuramos la red interna y externa del servidor. Configuramos dos adaptadores de red para el servidor, una como adaptador puente y otra como red interna para aislar la red. Ver figura 31.

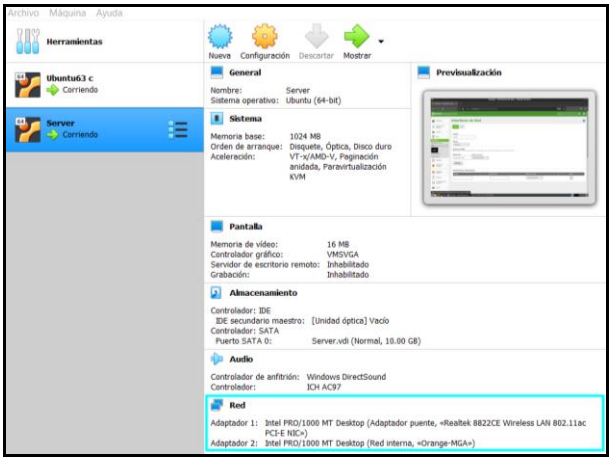

Figura 31. Configuración de red interna y externa.

Ahora configuramos las interfaces de red de cada adaptador, el primero con un método estático y configuramos una red estática, seleccionamos una ip que se encuentre disponible, en nuestro caso la 192.168.0.10 debido a que funcionara como la red externa. Ver figura 32.

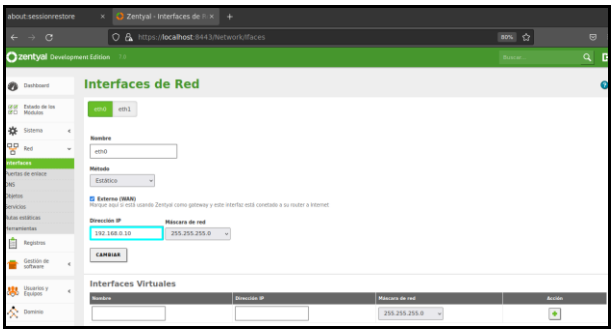

Figura 32. Configuración de interfaces de red.

Configuramos el adaptador 2, con un método estático y definimos la ip que deseamos para nuestra red interna, que es donde funcionara el cortafuegos. Ver figura 33.

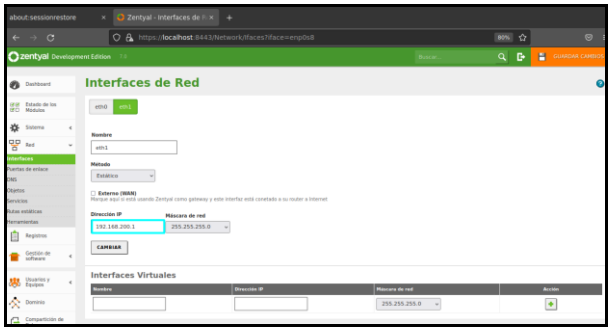

Figura 33. Configuración de segunda interfaz de red.

Configuramos la puerta de enlace, usamos la ip que nos provee nuestro router y la guardamos como puerta.

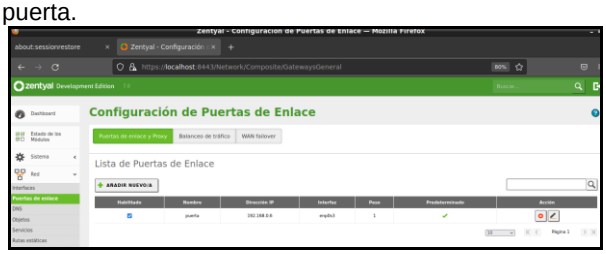

Figura 34. Configuración de puerta de enlace.

En DNS pasamos a configurar el traductor de servidores de nombre de dominio, colocando la ip correspondiente a Google. Ver figura 35.

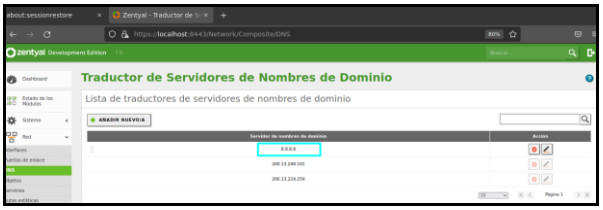

Figura 35. Configuración de traductor de servidores de nombre de dominio.

Luego nos dirigimos a objetos, en donde añadiremos dos objetos nuevos nombrados como “Facebook” e “Instagram”. Ver figura 37.

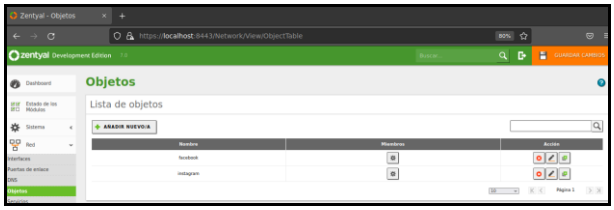

Figura 36. Configuración de objetos.

Luego ejecutamos el comando “nslookup <nombre de la pagina>” para obtener las ip correspondientes al sitio. Ver figura 37.

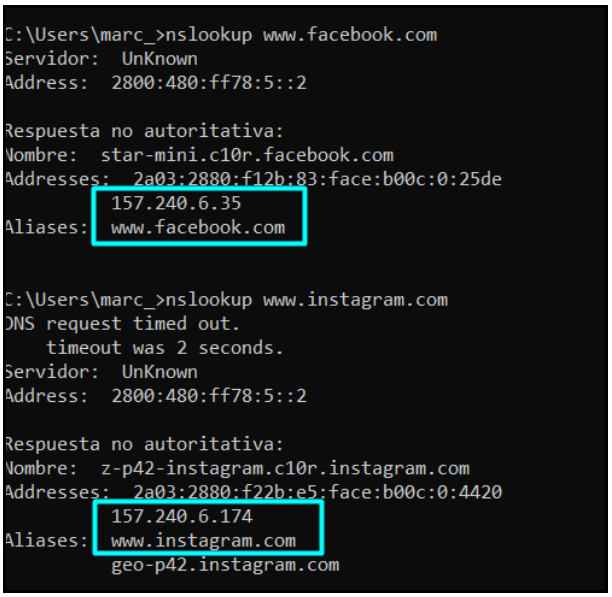

Figura 37. Verificación de ip.

Ahora configuramos cada una de esas ip en los objetos que creamos en el paso 6. Para lo que haremos clic en miembros, lo cual nos dirigirá a otra pantalla en donde podremos configurar tantas ip como hayamos obtenido en el paso anterior. Ver figura 38 y 39.

Figura 38. Configuración objeto Facebook.

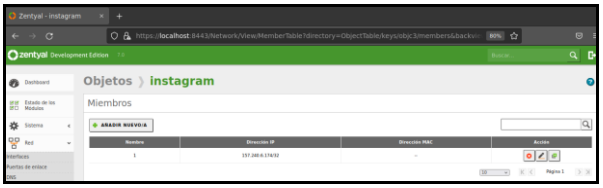

Figura 39. Configuración objeto Instagram.

Nos dirigimos a Cortafuegos, reglas de filtrado para las redes internas saliente de Zentyal y hacemos clic en “Configurar reglas”. Ver figura 40.

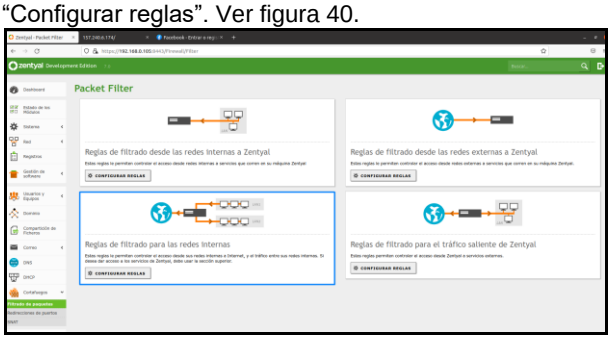

Figura 40. Configuración de reglas.

Damos clic en “añadir nuevo” para definir la regla. Ver figura 41.

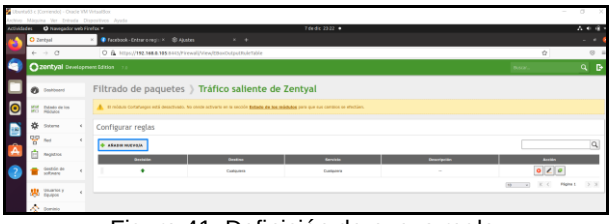

Figura 41. Definición de nueva regla.

Configuramos el tipo de decisión, que en nuestro caso sería de denegación, origen seleccionamos cualquiera, en destino seleccionamos objetos destino (Facebook) y en servicio cualquiera y añadimos la regla. Ver figura 42.

Figura 42. Parametrización de regla Facebook.

Configuramos el tipo de decisión, que en nuestro caso sería de denegación, origen seleccionamos cualquiera, en destino seleccionamos objetos destino (Instagram) y en servicio cualquiera y añadimos la regla.

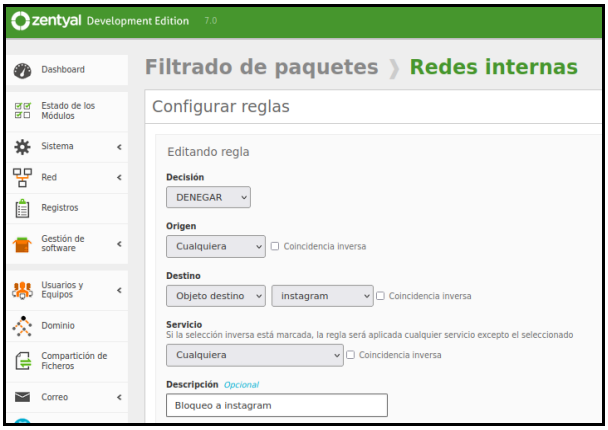

Figura 43. Parametrización de regla Instagram.

Una vez configuradas las reglas, pasamos a hacer guardado de las mismas haciendo clic en botón naranja “Guardar cambios” ubicado en el lado superior derecho. Ver figura 45 y 46.

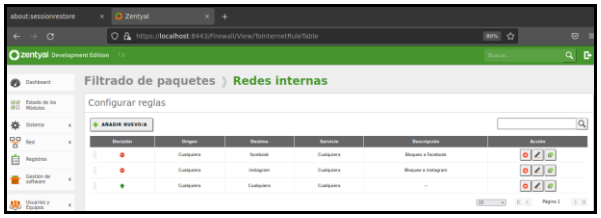

Figura 44. Listado de reglas parametrizadas.

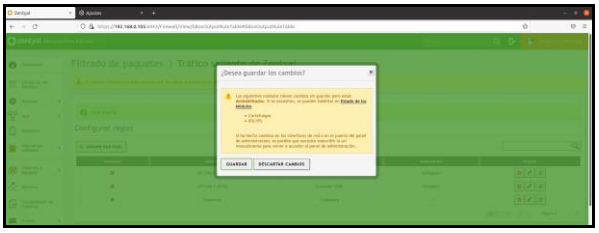

Figura 45. Guardado de reglas configuradas.

Debido a que el cortafuegos se encuentra desactivado, nos dirigimos al estado de módulos, activamos el cortafuegos y guardamos los cambios para que los cambios efectuados se vean reflejados en la red.

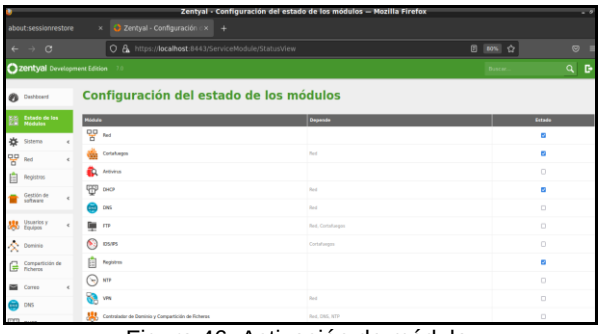

Figura 46. Activación de módulo.

Ahora nos dirigimos a DHCP para la asignación de las ip a las máquinas de la red interna, adicionando un rango para ello. Ver figura 47 y 48.

Figura 47. Configuración DHCP.

Figura 48. Configuración de rango de Ip

Ahora verificamos desde el navegador accediendo con las ip bloqueadas. Ver figura 49 y 50.

Facebook:

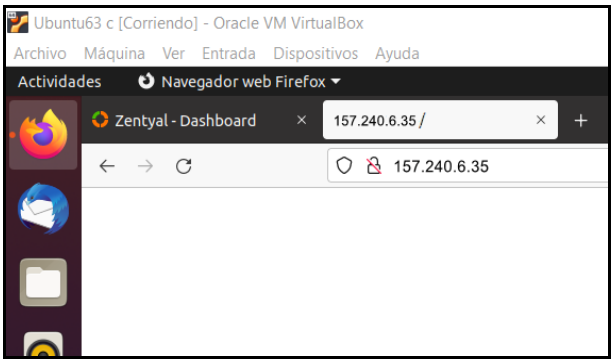

Figura 49. Facebook bloqueado.

Instagram:

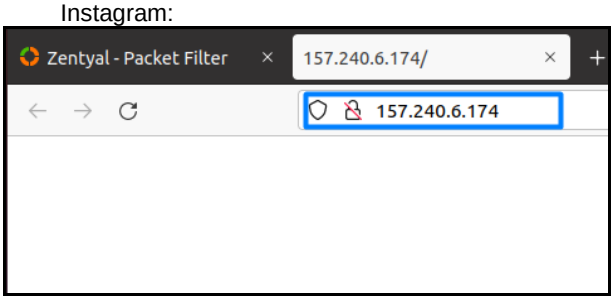

Figura 50. Instagram bloqueado.

6 CONFIGURACIÓN DEL SERVICIO VPN.

Antes de configurar el servidor VPN es necesario crear una “Autoridad de certificación” y un certificado de autoridad para el cliente y otro para el servidor [8]

A continuación, se crea una “Autoridad de certificación” con tiempo de expiración en 1000 días. Ver figura 51.

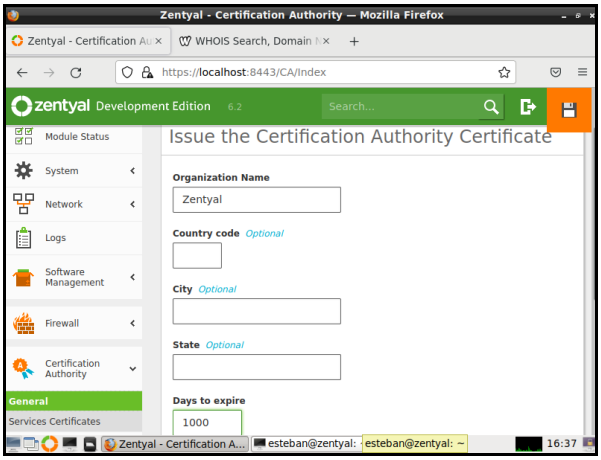

Figura 51. Creación de autoridad de certificación

El certificado de autoridad del servidor se crea automáticamente al crear la VPN, así que se procede a crear el certificado del cliente. Ver figura 52.

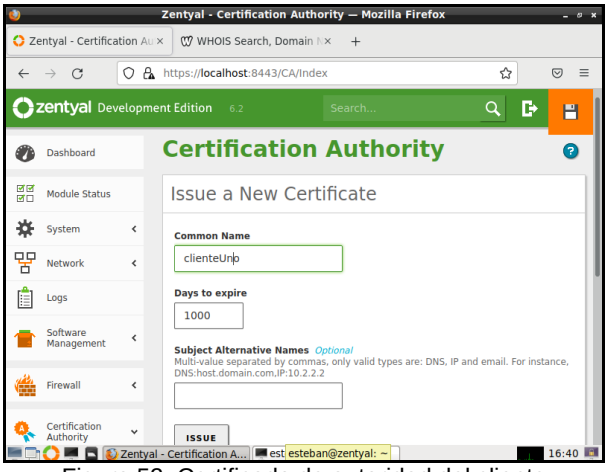

Figura 52. Certificado de autoridad del cliente

Se crea el servidor de VPN con el nombre "servidorvpn", se realiza la configuración de puerto y dirección las cuales se dejan por defecto. Zentyal automáticamente creó y le asignó el certificado de autoridad llamado "vpn-servidorvpn", adicional en las opciones de configuración, se habilita la interfaz TUN, por último, se habilita el servidor y se guardan los cambios. Ver figura 53.

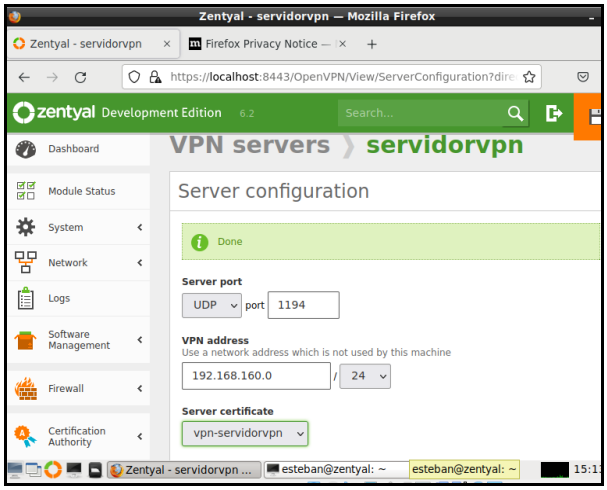

Figura 53. Configuración servidor VPN.

Una vez configurado, se procede a generar el perfil que usará el cliente para conectarse. Se le asigna el certificado creado, y se configura la IP pública del servidor. Ver figura 54.

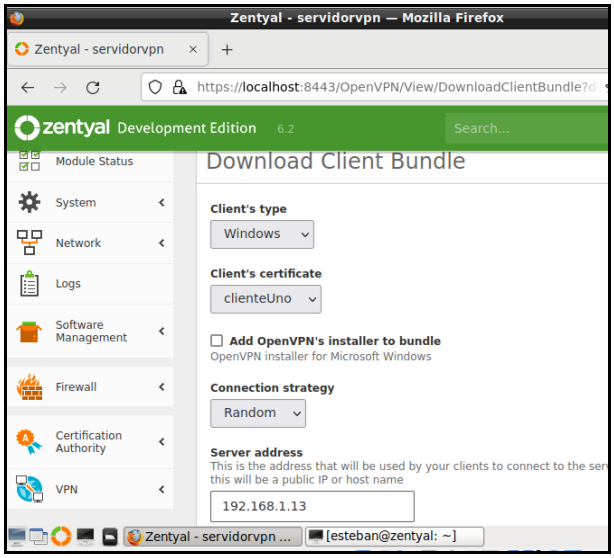

Figura 54. Generación y descarga del perfil del cliente

Desde una máquina Windows, se importan los archivos del perfil generado para establecer la conexión, mediante la herramienta OpenVPN Connect [9]. Ver figura 55.

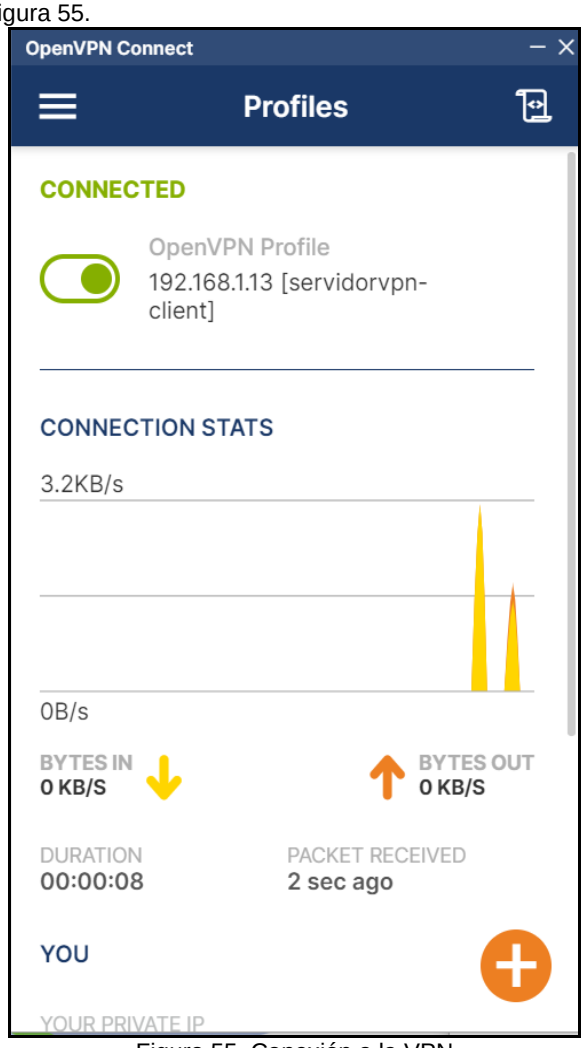

Figura 55. Conexión a la VPN

Al realizar ping a la dirección de la red interna del servidor desde el cliente Windows, se comprueba que está accesible. Ver figura 56.

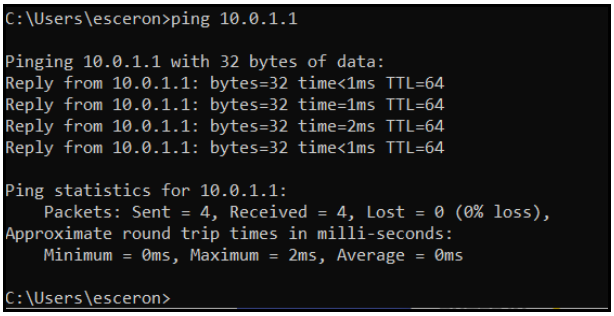

Figura 56. Prueba de acceso al contenido del servidor mediante a VPN

La anterior IP 10.0.1.1 corresponde a la red interna configurada en el servidor. Ver figura 57.

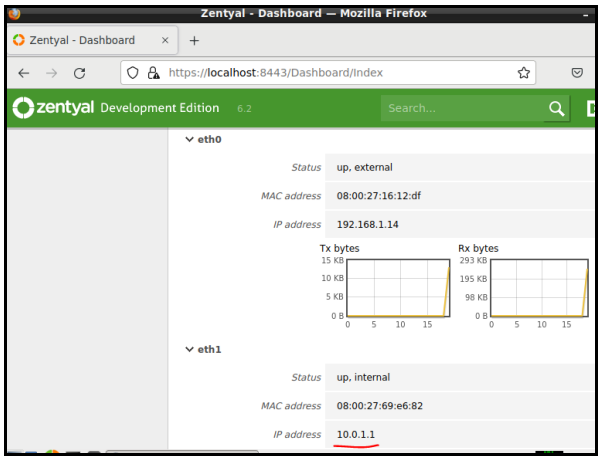

Figura 57. Verificación de IP de red interna

7 CONCLUSIONES

Con el servidor Zentyal, pudimos configurar nuestro dominio, configurar rangos de direcciones IP, y poder tener toda la seguridad de un cliente dentro del servidor, así mismo facilita muchas configuraciones de la Infraestructura TI.

La utilización de un proxy no transparente es una opción muy importante para la administración y seguridad de los accesos a internet de las estaciones de trabajo de una compañía, Zentyal proporciona una herramienta intuitiva y fácil de administrar, esta permite regular el acceso, filtrar el acceso a paginas ya sea porque no son necesarias para el uso de los colaboradores o por seguridad y limitación del ancho de banda, un proceso vital para controlar y asegurar la disponibilidad del ancho de banda de la compañía.

El desarrollo de la temática firewall permitió el apropiamiento de conocimiento respecto a las parametrización de necesarias para restringir la navegación en determinados sitios, que habitualmente se realizan para mitigar el riesgo de desconcentración de sus colaboradores y la optimización de los recursos de red, incrementando el enfoque y buen uso de los recursos de red dispuestos.

Zentyal permitió fácilmente exponer el contenido de la red interna del servidor solo a aquellos que establecieran una conexión por VPN. Mediante la configuración de certificados de autoridad y el servidor VPN, se logró la conectar un cliente a la red local del servidor con la posibilidad de acceder a los servicios o contenido que estén disponibles

8 REFERENCIAS

[1] Zentyal (s.f.). *Alternativa Linux Fácil a Windows Server*. Recuperado de: https://zentyal.com/es/inicio.
[2] Zentyal (2020). *Zentyal Server 6.2 Development Ahora Disponible*. Recuperado de: https://zentyal.com/es/news/zentyal-6-2-announcement-2
[3] VirtualBox (s.f.). About VirtualBox. Recuperado de: https://www.virtualbox.org/wiki/VirtualBox.
[4] Zentyal (s.f.). Installation. Recuperado de: https://doc.zentyal.org/6.2/en/installation.html
[5] https://zentyal.com/es/news/tutorial-servidor-zentyal-como-servidor-dns-dhcp-dominio-y-directorio-proxy-y-cortafuegos/
[6] https://eltallerdelbit.com/servidor-dhcp-zentyal/
[7] Zentyal (s.f.). HTTP Proxy Service. Recuperado de: https://doc.zentyal.org/6.2/en/proxy.html
[8] ProngeR TV. (2019, 13 diciembre). Cómo instalar y configurar un servidor VPN en Zentyal - Tutorial 2020. YouTube. https://www.youtube.com/watch?v=8zaxU1C7qBc&ab_channel=ProngeRTV
[9] OpenVPN (s.f.). OFFICIAL OPENVPN CONNECT CLIENT PROGRAM. Recuperado de: https://openvpn.net/client-connect-vpn-for-windows