INSTALAR Y CONFIGURAR ZENTYAL SERVER IMPLEMENTANDO LOS SERVICIOS DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO, PROXY NO TRANSPARENTE, CORTAFUEGOS, FILE SERVER, PRINT SERVER Y VPN.

Cristhian Fernando Ariza Camacho
cfarizac@unadvirtual.edu.co
Esther Cecilia Correa Quiroz
eccorreaq@unadvirtual.edu.co
Cristian Camilo Villada
ccvilladaz@unadvirtual.edu.co
Mónica Méndez
mpmendezi@unadvirtual.edu.co
Cesar Beltran Musiry
cabeltranmus@unadvirtual.edu.co

RESUMEN: *En este artículo se presentará la implementación y configuración de los servicios DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN, que serán administrados por Zentyal, cuyo servidor muestra una interfaz web, y se evidenciara el funcionamiento de los servicios con sus resultados obtenidos.*

PALABRAS CLAVE: Cortafuegos, DHCP, Proxy, Zentyal.

ABSTRACT: *This article will present the implementation and configuration of the DHCP Server, DNS Server and Domain Controller, Non-transparent Proxy, Firewall, File Server, Print Server and VPN services, which will be managed by Zentyal, whose server shows a web interface, and the operation of the services will be evidenced with the results obtained.*

KEY WORDS: Firewall, DHCP, Proxy, Zentyal.

1 INTRODUCCIÓN

En el presente informe se instalará y configurará la distribución Zentyal Server de GNU/Linux, como sistema operativo base para disponer de los servicios de la infraestructura de la tecnología de la información IT.

Se implementará bajo Zentyal Server los servicios DHCP Server, DNS Server y Controlador de Dominio, realizando la 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.

Como también se realizará la 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. Siguiendo con la implementación en Zentyal se realizará la configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

También se realizará la 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, siguiendo con la configuración se creará una VPN la cual permitirá establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se deberá evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo. Y para la demostración del todo el proceso se debe describir paso a paso el procedimiento realizado y las evidencias de los resultados obtenidos.

2 SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Zentyal está concebido para ser instalado en una máquina (real o virtual), Zentyal funciona sobre la distribución de GNU/Linux Ubuntu en su versión para servidores, usando siempre las ediciones LTS (Long Term Support) [1].

La instalación y configuración de Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT [2].

Como se muestra en la figura 1, se describe la configuración de la máquina virtual en VirtualBox, colocando en la configuración de la red en el adaptador 1 la tarjeta NAT para la descarga de paquetes, y en el adaptador 2 la tarjeta Adaptador puente.

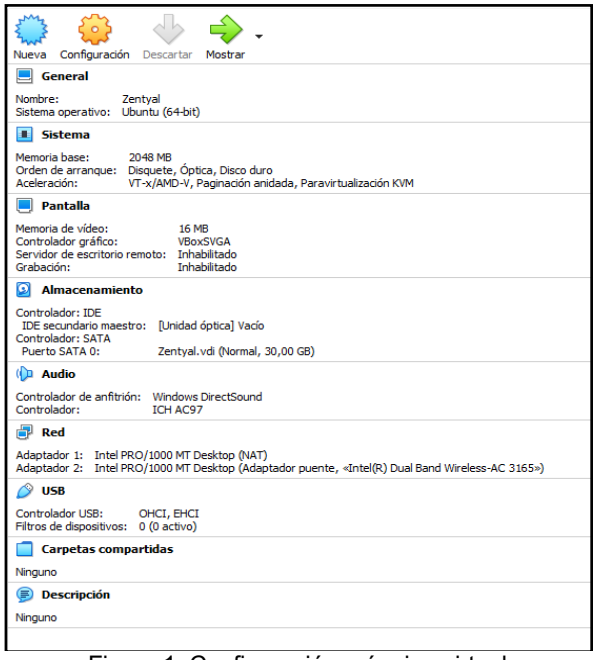

Figura 1. Configuración máquina virtual

Como se muestra en la figura 2, se utiliza la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal 6.2

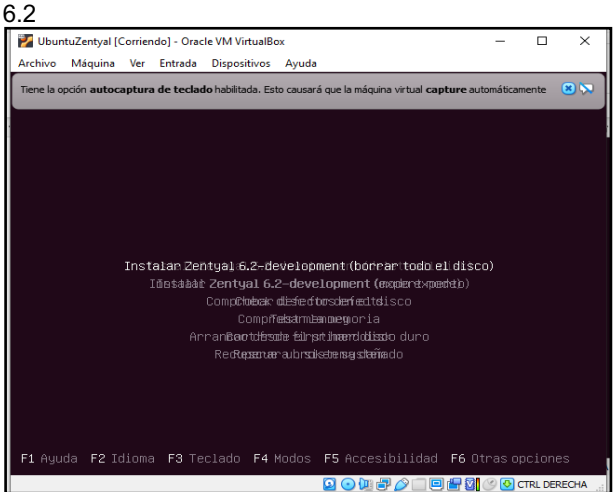

Figura 2. Inicio de instalador

Como se muestra en la figura 3, se selecciona la interfaz de red primaria eth0 que se usara en la instalación para la descarga de paqueterías y actualización.

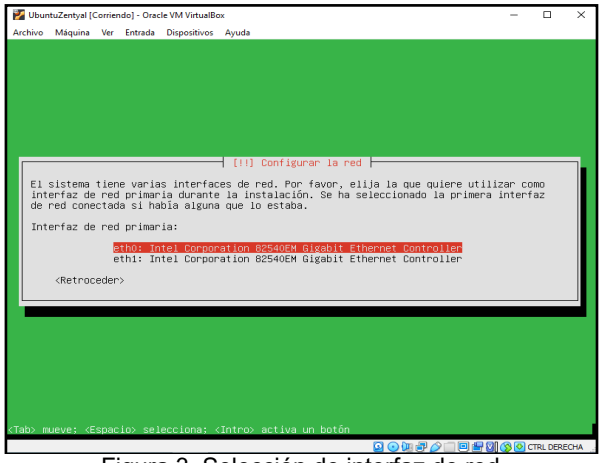

Figura 3. Selección de interfaz de red

Como se muestra en la figura 4, se realiza la instalación de Zentyal, se realiza ping al host de Google (8.8.8.8) para comprobar si hay conexión a internet.

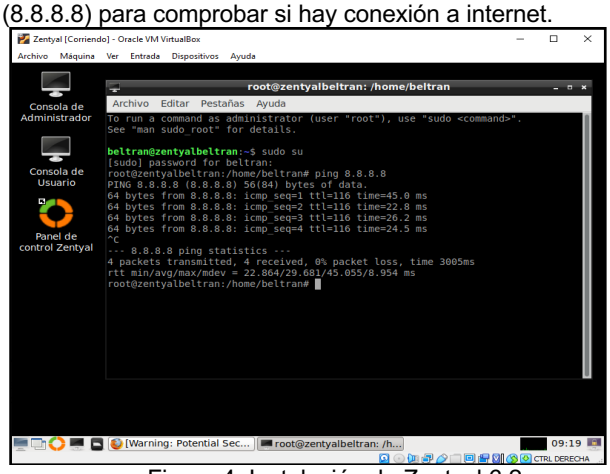

Figura 4. Instalación de Zentyal 6.2

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

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.

3.1 CONFIGURACIÓN INTERFAZ DE RED

En la figura 5 inicio con la configuración e instalación de la red, ingresando a la siguiente ruta gestión de software / Componentes de Zentyal/ seleccionando Networking Configuration y posteriormente comienzo con la debida instalación.

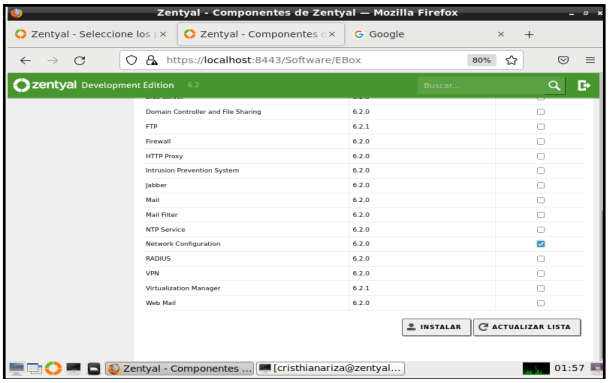

Figura 5. Instalación servicio de red

Ya instalado el paquete me desplazo al menú Dashboard a estado de los módulos y activo el mismo, posteriormente sigo la siguiente ruta Red/Interfaces para configurar las dos interfaces de red eth0 y eth1.

En la figura 6 configuró la interfaz eth0 con método estático asignándole la dirección IP.

Figura 6. Configuración interfaz eth0

En la figura 7 se configura la interfaz eth1 también con método estático asignándole una dirección IP.

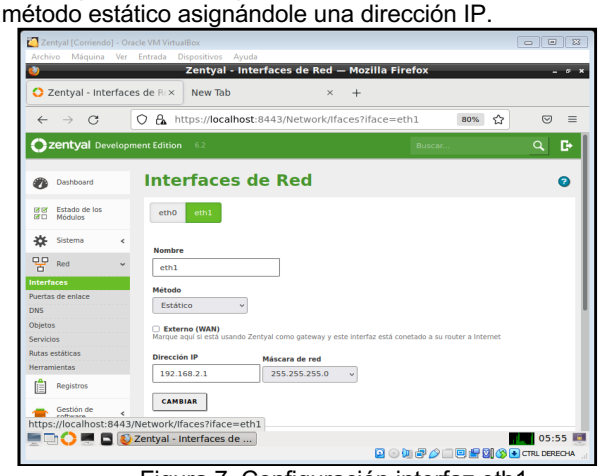

Figura 7. Configuración interfaz eth1

3.2 CONFIGURACIÓN DHCP SERVER

Configurada la red iniciamos con la instalación del DHCP, donde se continua con la ruta gestión de software / Componentes de Zentyal/ seleccionando la opción DHCP Server, iniciando con la instalación.

En la figura 8 en la parte izquierda del menú se puede constatar la correcta instalación del servicio DHCP, al darle clic al servicio nos muestra una nueva página donde observamos las dos interfaces de red configuradas anteriormente, selecciono la interfaz “eth1” que corresponde a la red “LAN”, ingresando a la opción “configuraciones”.

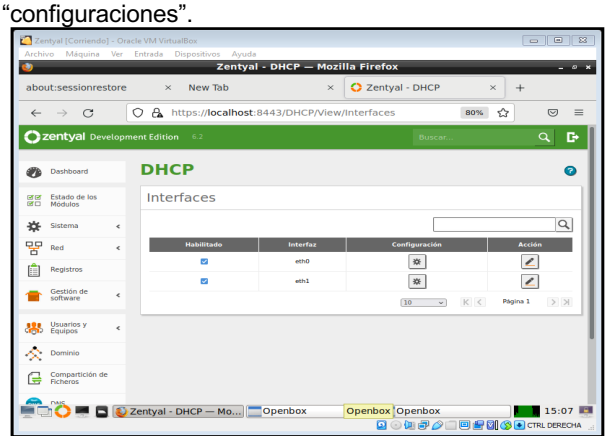

Figura 8. Configuración DHCP

Ya selecciona la interfaz eth1 se modifica los siguientes parámetros como el dominio de búsqueda: Dominio de Zentyal, cristhian-ariza-local, servidor de nombre primario: DNS local Zentyal, en el servidor de nombre secundario, agrego el DNS de Google 8.8.8.8.

En la figura 9 agregó y configuró los rangos de direcciones IP, donde seleccionó la opción de añadir nuevo y digitamos el nombre y el parámetro a establecer.

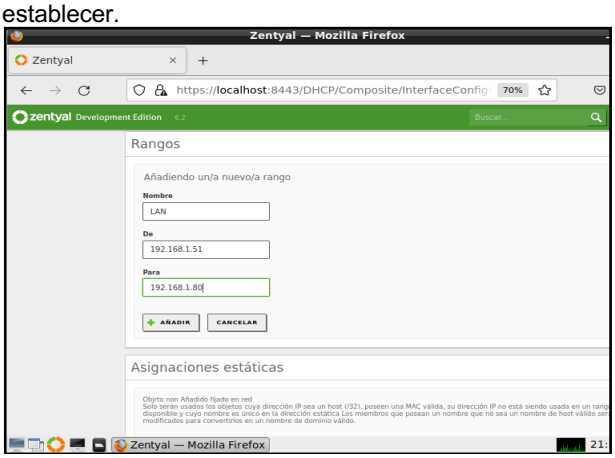

Figura 9. Configuración Rangos

Una vez configurado el DHCP en el Zentyal procedo a ingresar a la terminal del Ubuntu de escritorio, donde me muestra la dirección IP 192.168.10.31, la cual está fuera del rango establecido, de inmediato verifico la configuración de red a través del fichero del directorio /etc/netplan. Configuro la dirección IP ejecutando el comando ***nano /etc/netplan/00-installer-config.yaml*** donde el servidor recibe su dirección IPv4 a través de DHCP.

En la figura 10 se encuentra la configuración para que el Ubuntu de escritorio me reconozca el DHCP.

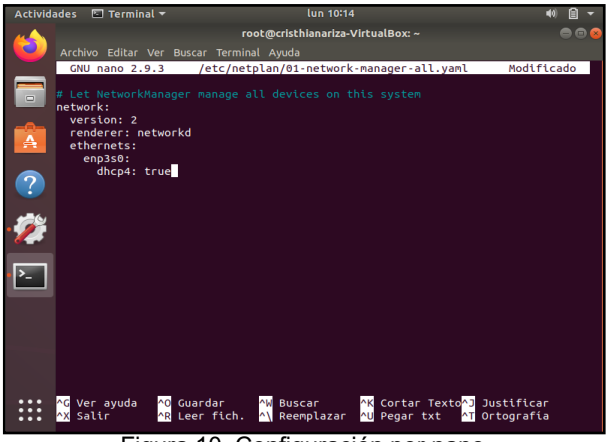

Figura 10. Configuración por nano

En la imagen 11 mediante la ejecución del comando ip address *se* confirma que la dirección IP está dentro del rango programado 192.168.2.50.

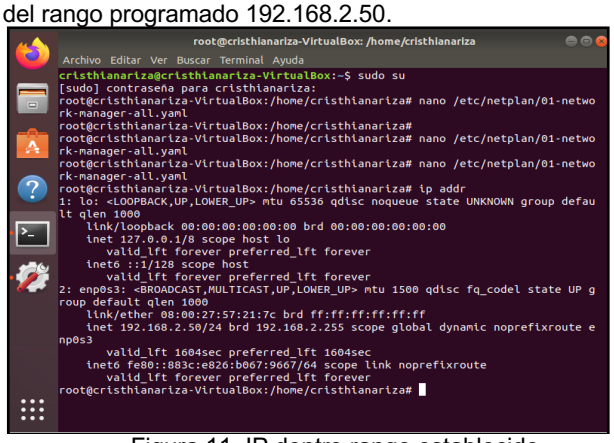

Figura 11. IP dentro rango establecido

En la figura 12 mediante la ejecución del comando ip address *se* confirma que la dirección IP está dentro del rango programado 192.168.2.50.

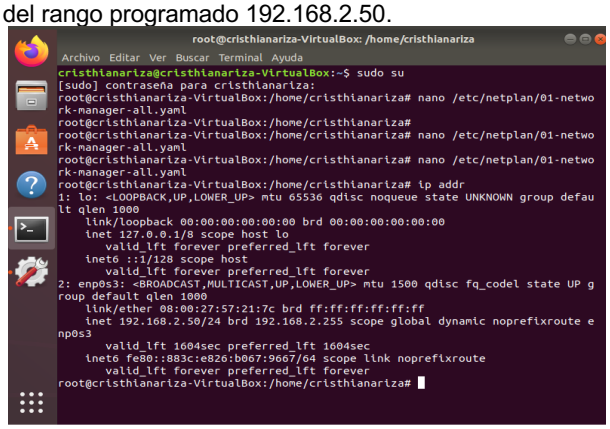

Figura 12. IP dentro rango establecido

3.3 INSTALACION CONFIGURACIÓN DNS SERVER

En la figura 12 se demuestra la instalación y configuración del DNS Server, donde me dirijo al icono DNS en el Dashboard, iniciando con la configuración del sistema de nombres de dominio (DNS), añadiendo un nuevo dominio dejando el nombre que registra por defecto.

También se comprueba que este configurado el servidor DNS con dominio de nombre cristhian-ariza.local; configuración que se realizó durante la instalación y configuración inicial del servidor.

Figura 13. Configuración DNS

En la figura 13 se realiza la respectiva prueba del DNS desde el Ubuntu de escritorio.

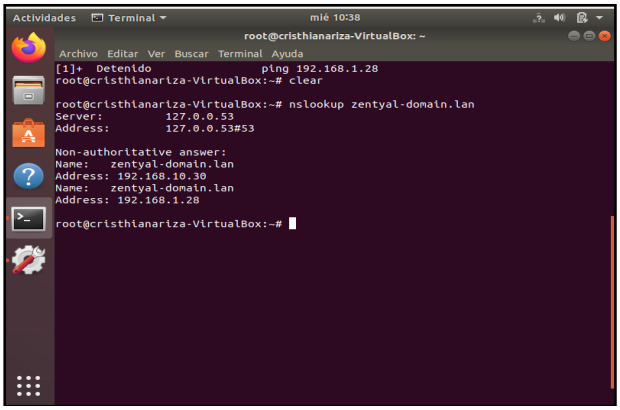

Figura 14. Prueba del DNS

4 TEMÁTICA 2: PROXY NO TRANSPARENTE

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.

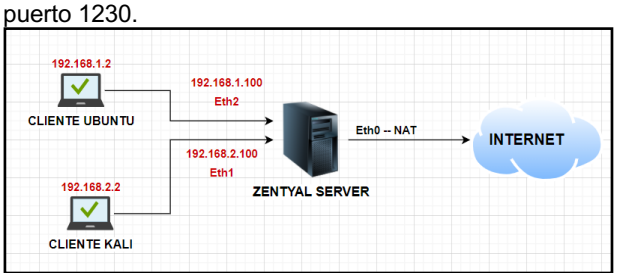

Figura 15. Arquitectura desarrollada en la temática

En el apartado de gestión de software se realiza la instalación del módulo Proxy Http, sin embargo, para una operación correcta se requieren los módulos de FW y Red.

Figura 16. Instalación módulo Proxy http zentyal.

El siguiente paso es realizar las configuraciones básicas del servidor Zentyal, configurando la interface eth0 como la externa ya que es la que está en modo NAT y la eth1 y eth2 en redes internas respectivamente llamamos las redes como verde y naranja para diferenciarlas.

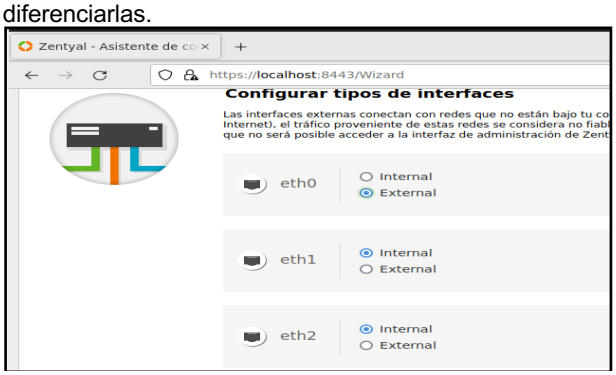

Figura 17. Asignación de interfaces externas e internas.

A continuación, se asigna las direcciones ips fijas para las redes internas correspondientes a las interfaces eth1 y eth2 respectivamente.

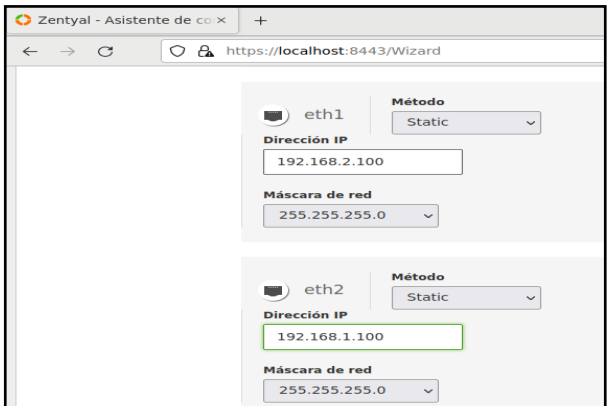

Figura 18. Asignación de ip fija a interfaces del servidore zentyal

Una vez instalado el servicio de proxy en el servidor se configura el puerto requerido: 1230 y se habilita el módulo en el servidor.

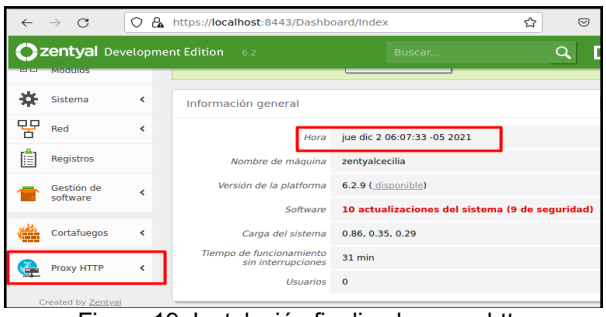

Figura 19. Instalación finalizada proxy http

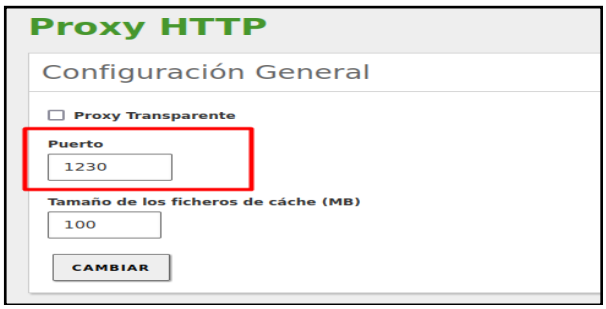

Figura 20. Configuración puerto servicio proxy.

Es importante recordar que al ser No transparente se requiere su configuración en las opciones de cada navegador, además como tenemos conectados dos clientes y dos interfaces a redes internas respectivamente necesitamos que el servidor Zentyal asigne direcciones ips a dichas redes de forma automática, para ello instalamos y activamos el módulo DHCP y configuramos dos rangos de direcciones ips para las interfaces eth1 y eth2 respectivamente.

Figura 21. Configuración interface eth1

Figura 22. Configuración rango de direccionamiento para interface eth1

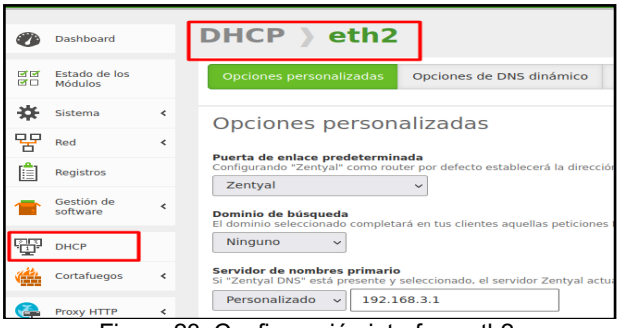

Figura 23. Configuración interface eth2

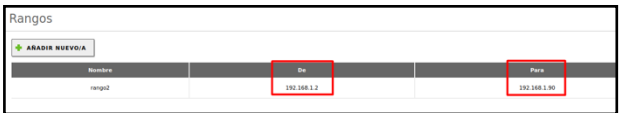

Figura 24. Configuración rango de direccionamiento para interface eth2

Una vez configuradas las dos interfaces con los rangos de direccionamiento que entregarán de manera dinámica, verificamos el direccionamiento en los clientes. si observamos la máquina cliente podemos confirmar la ip asignada por el Zentyal la cual es la 192.168.1.2 que corresponde al rango asignado a través de la interface eth2 del servicio DHCP.

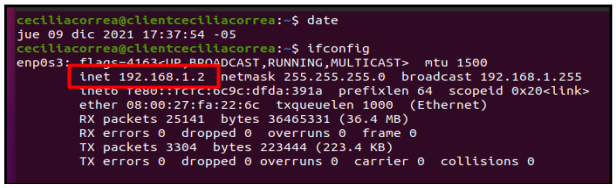

Figura 25. Direccionamiento cliente ubuntu de manera dinamica

El siguiente paso es configurar el proxy de manera manual en el navegador del cliente Ubuntu.

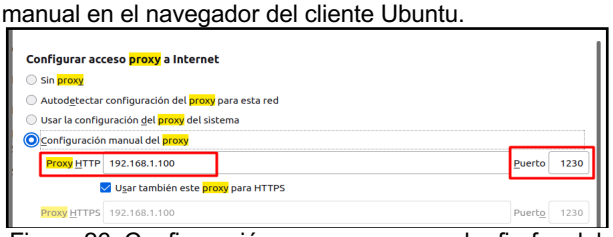

Figura 26. Configuración proxy en navegador firefox del cliente ubuntu.

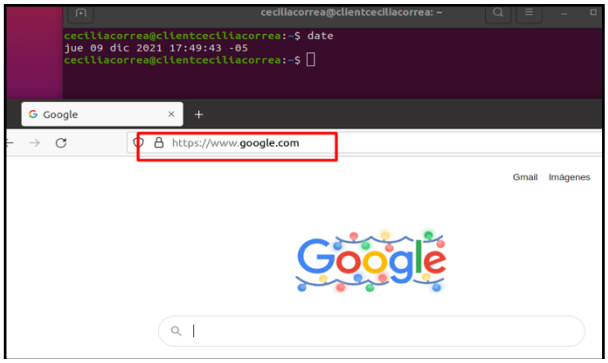

Figura 27. Prueba de navegación de internet a través del proxy.

Como se observa en la arquitectura vamos a configurar otro cliente, en este caso vamos a usar KALI Linux que es una distribución de Linux muy popular para todo lo relacionado con pentesting de seguridad. Confirmemos la ip que entrega el Zentyal en este caso para la otra interface Eth1, como se puede observar el servicio DHCP del servidor entregó al equipo Kali la ip 192.168.2.2

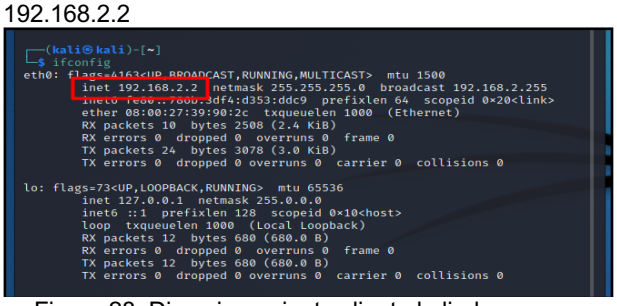

Figura 28. Direccionamiento cliente kali de manera dinamica.

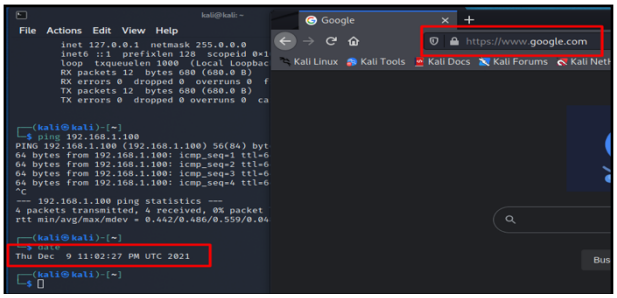

Figura 29. Prueba de navegación del cliente Kali a traves del proxy.

Para confirmar aun mas el funcionamiento del proxy se crean dos reglas en el servidor Zentyal una de denegación para el cliente Ubuntu.

Figura 30. Regla de denegación de servicio de proxy a la ip del cliente ubuntu.

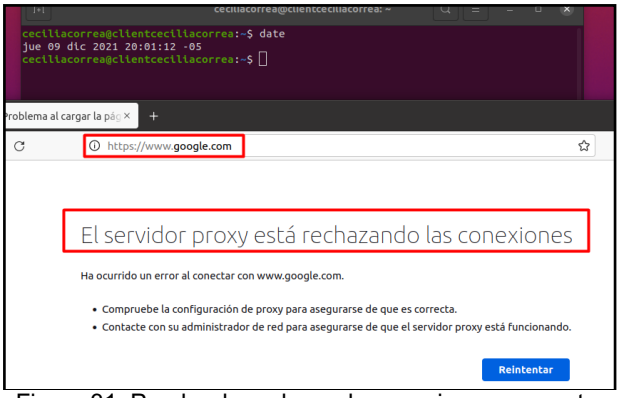

Figura 31. Prueba de rechazo de conexiones por parte del servidor Zentyal.

Como se pudo observar el Zentyal es muy versátil y fácil de configurar para entornos de redes de pequeñas y medias empresas o pymes, para empresas también orientadas en su arquitectura empresarial 100% on premise puede ser una excelente opción, no solo visto desde el punto de un centralizador de servicios de ti sino también para la implementación de controles de defensa como son un proxy http. Teniendo en cuenta la situación actual de muchas compañías por el trabajo hibrido, estas requieren rediseñar su estrategia de control de navegación como es un proxy ya que sus empleados se conectan desde casa y bajo una arquitectura como la planteada requieren una conexión VPN para garantizar el funcionamiento del control, sin embargo, se puede plantear una arquitectura híbrida que garantice la aplicación del control incluso conectándose desde redes de hogares o no corporativas. A continuación, se plantea una posible arquitectura de referencia que puede ayudar a los administradores a resolver este inconveniente y sus consideraciones.

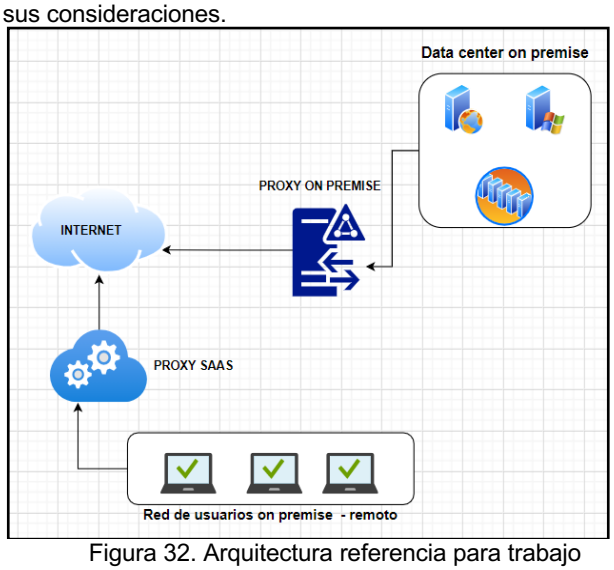

Figura 32. Arquitectura referencia para trabajo remoto y garantiza el control proxy en cualquier red de internet.

Principales consideraciones:

- El uso de un servicio SAAS garantiza el consumo de un servicio proxy en todo momento bajo politicas de maquina.
- El uso de un servidor proxy on premise que garantice el control a nivel de datacenter o nube privada de la compañía.
- Se deben establecer controles de directorio activo o controles de dominio que garanticen la integridad de la configuración en navegadores y el sistema del servidor proxy.

5 TEMÁTICA 3: CORTAFUEGOS

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

A dar comiendo se da un inició a la máquina virtual conectada a la red de nuestro servidor Zentyal comprobamos que las conexiones a redes sociales están funcionando.

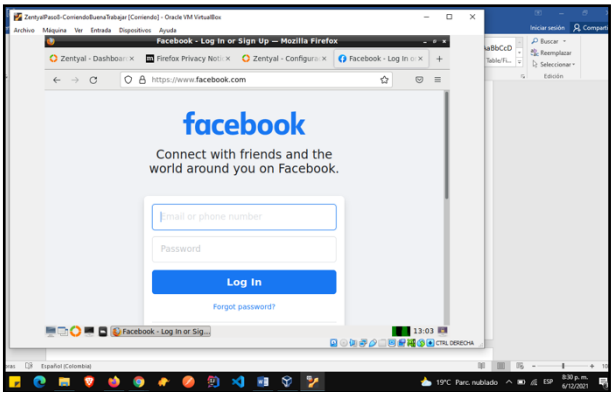

Figura 33. Ingreso a redes sociales

Luego de estos volvemos a nuestro servidor Zentyal y nos dirigimos a la sección de cortafuego y en el menú que se despliega elegimos la opción de filtrado de paquete.

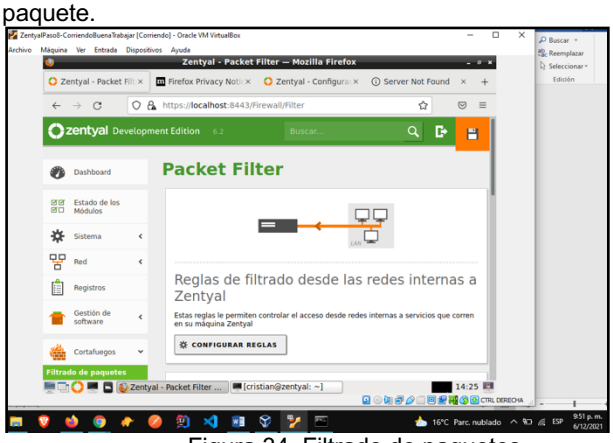

Figura 34. Filtrado de paquetes

En filtrado de paquetes como vamos a filtrar son paquetes que permitan de la red interna (red LAN) Reglas de filtrado para redes internas: Estas reglas le permiten controlar el acceso desde sus redes internas a

internet, y el tráfico entre sus redes internas. Si desea dar acceso a los servicios de Zentyal, debe usar la sección superior.

Figura 35. Elección de paquete de filtrado

Creamos la regla para denegar Facebook, para ello lo primero que se debe realizar es comunicar con la página oficial de Facebook a través de un ping a su página principal desde Zentyal para ver que ip está contestando y denegar esta IP.

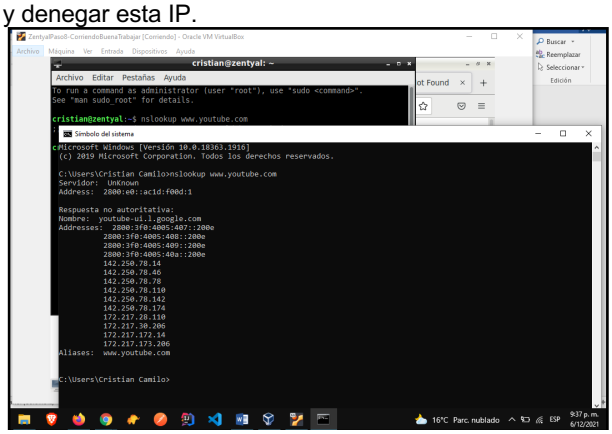

Figura 36. Dirección nslookup

A través de la ip (142.250.78.14) obtenida a través del comando ping creamos la regle de denegación luego damos en guardar.

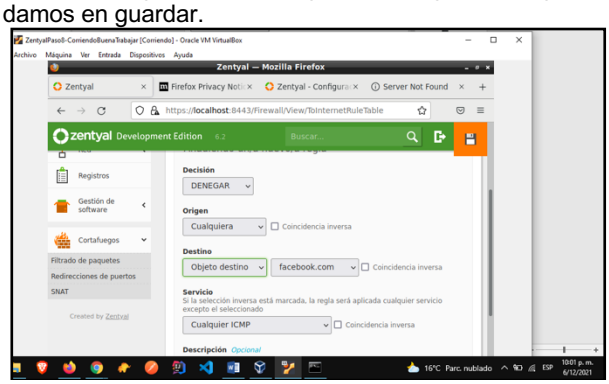

Figura 37. Creación regla filtrado

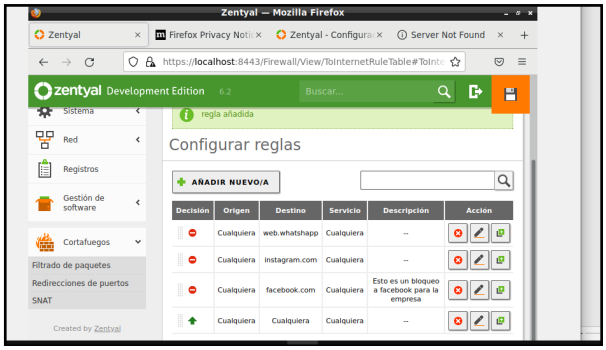

Figura 38. Regla agregada

Después se debe probar la configuración en máquina virtual Ubuntu y se debe correr y revisar que la regla de filtrado restrinja la entrada a la página de la red social Facebook.

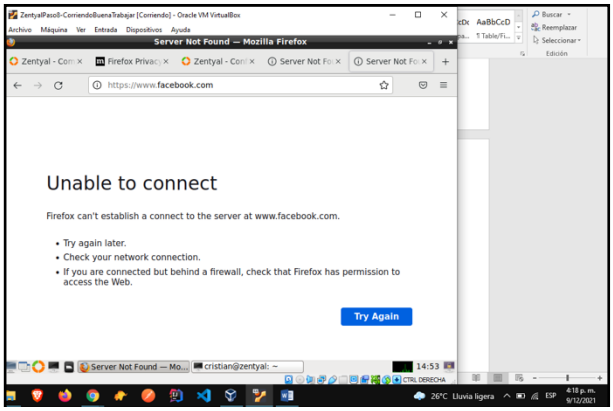

Figura 39. Comprobación de regla

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.

Iniciamos con el usuario y contraseña que asignamos en la instalación

Figura 40. Configuración zentyal

Seleccionamos los paquetes a instalar

Figura 41. Configuración Zentyal

Ahora se debe crear un servidor de dominio y agregar el Cliente Ubuntu 20.04 a dicho dominio
Se configuran las interfaces de red de Zentyal Server

Figura 42. Configuración Zentyal

Ahora se crea un usuario del dominio

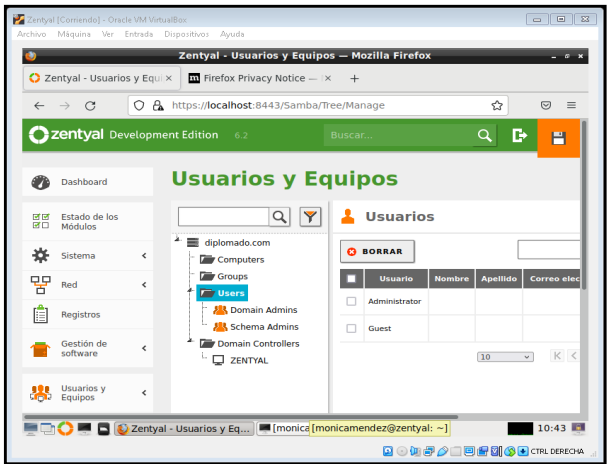

Figura 43. Configuración Zentyal

Añadimos el usuario

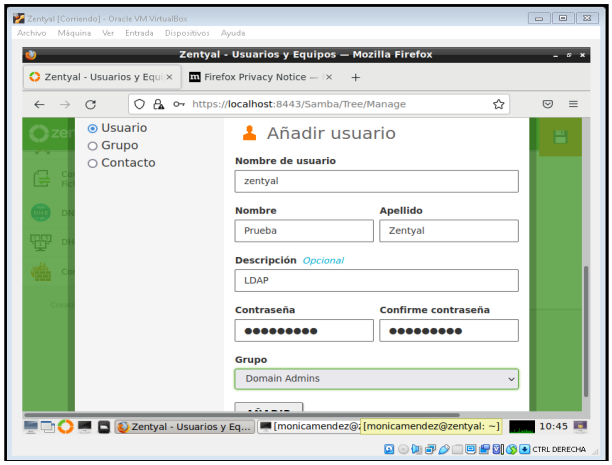

Figura 44. Configuración Zentyal

Ahora conectamos la máquina virtual con Ubuntu 20.04lts al dominio de Zentyal.

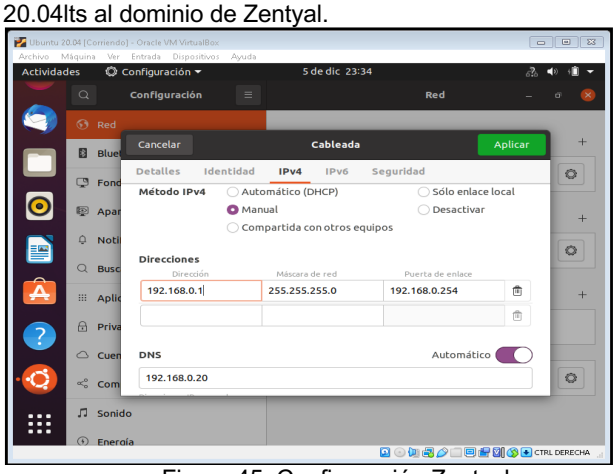

Figura 45. Configuración Zentyal

7 TEMÁTICA 5: VPN

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.

Imagen donde continuamos la configuración en la interfaz web de Zentyal donde nos muestra los diferentes pasos del asistente.

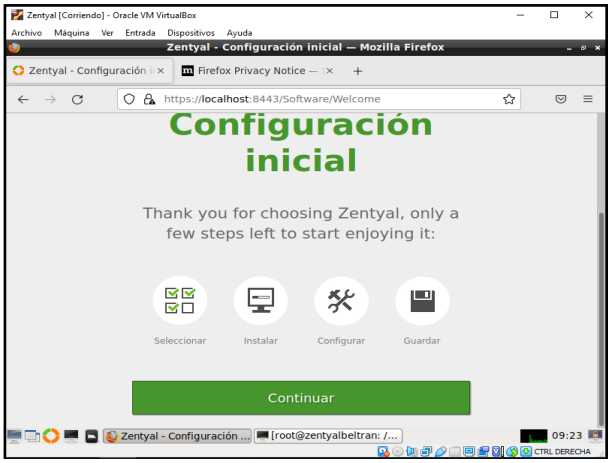

Figura 46. Configuración inicial

Imagen donde seleccionamos los servicios de Zentyal adicionales a instalar, que para este caso gestionaremos redes privadas virtuales (VPN), se seleccionan los paquetes de Firewall, Certificación, VPN.

Figura 47. Paquetes de inatalacion

Imagen donde se configurarán las interfaces de la red, eth0 externa que toma el internet, eth1 interna que será con la que interactúen los clientes.

Figura 48. Configurar interfaz de red

Imagen donde se configuran las interfaces de las tarjetas de red, eth0 DHCP para que tome direcciones aleatorias generadas por la red de internet, eth1 Statica por la cual se conectara al servidor Zentyal.

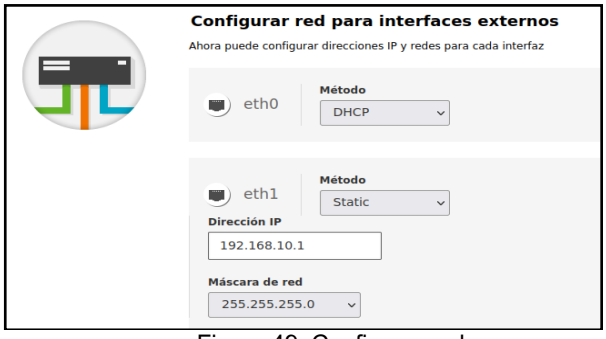

Figura 49. Configurar red

Imagen donde se muestra la información general de la configuración de los componentes en Zentyal.

Figura 50. Dashboard

Imagen donde se crea el certificado de la autoridad de certificación, el cual se utilizará al crear el servidor VPN.

Figura 51. Crear certificado

Imagen donde se crea un nuevo servidor, en (VPN, servidores, añadir nuevo servidor).

Figura 52. Crear nuevo servidor VPN

Imagen donde se configura el servidor, que entre al servidor por el puerto 1194 UDP, se habilita la interfaz TUN, escuchara todas las interfaces interna y externa, redirigimos la puerta de enlace Zentyal para el cliente con el fin de habilitar o deshabilitar el acceso a internet.

Figura 53. Configuración del servidor

Imagen donde se expide un nuevo certificado para nuestro cliente.

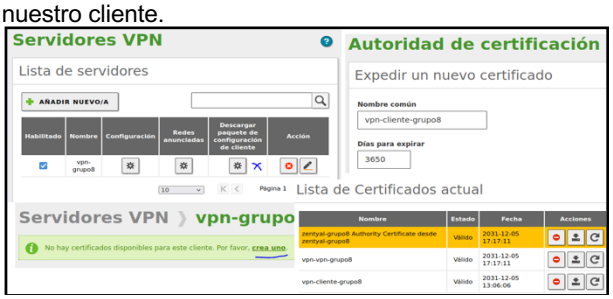

Figura 54. Creación certificado para cliente

Imagen donde nos dirigimos nuevamente a la casilla VPN, servidores, descargar paquete de configuración de cliente, y se descarga el paquete de configuración de cliente, el cual el cliente instalara en su máquina para la conexión.

Figura 55. Descarga paquete cliente

Imagen donde se muestra el servicio habilitado del servidor VPN creado.

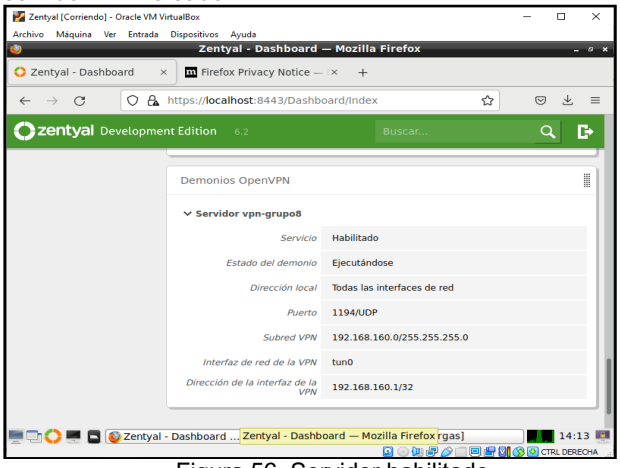

Figura 56. Servidor habilitado.

Imagen donde se instala openvpn en el equipo del cliente para que consuma el paquete que se le enviará para la conexión VPN.

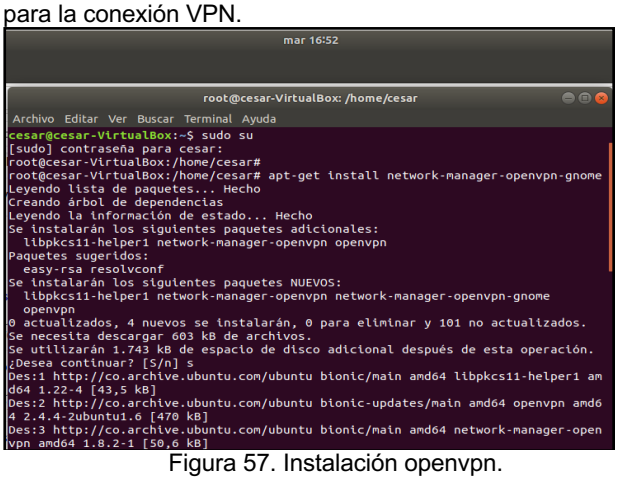

Figura 57. Instalación openvpn.

Imagen de la configuración de los permisos de conexión VPN en la maquina cliente.

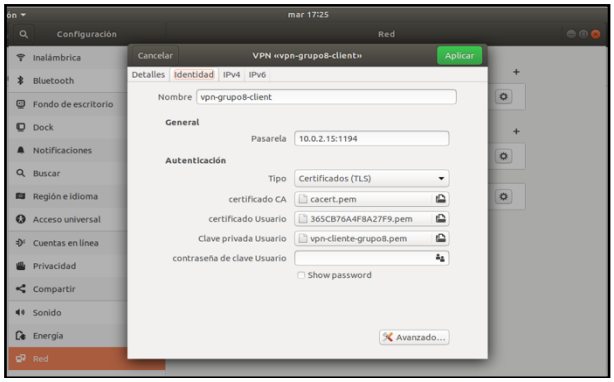

Figura 58. Conexión VPN

Imagen donde se ingresa a la interfaz de openvpn y nos logueamos para la interacción con otros clientes.

Figura 59. Login.

8 CONCLUSIONES

Se instaló y configuró la distribución Zentyal Server de GNU/Linux, como sistema operativo base para disponer de los servicios de la infraestructura de la tecnología de la información IT.

Se implementó bajo Zentyal Server los servicios DHCP Server, DNS Server y Controlador de Dominio, y se realizó la 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.

Se implementó bajo Zentyal Server los servicios Proxy no transparente, y se realizó la 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.

Se implementó bajo Zentyal Server los servicios Cortafuegos, y se realizó la configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Se implementó bajo Zentyal Server los servicios File Server y Print Server, y se realizó la 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.

Se implementó bajo Zentyal Server los servicios VPN, y se creó una VPN la cual permitió establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se evidencio el ingreso a algún contenido o aplicación de la estación de trabajo.

Se demostró en un paso a paso el procedimiento realizado y las evidencias de los resultados obtenidos.

9 REFERENCIAS

[1] Zentyal (s.f.). Zentyal Server Development Edition.Disponible en: https://zentyal.com/es/comunidad/

[2] Zentyal. (s.f.). Zentyal Community. Disponible en: https://doc.zentyal.org/6.2/es/installation.html