CONFIGURANDO SERVICIOS DE UN SERVIDOR ZENTYAL EN UNA RED INTERNA DE MAQUINAS CLIENTE CON DISTRIBUCIONES LINUX

Yamid Hernando Navea
e-mail: yhnaveal@unadvirtual.edu.co
Hamilton Arévalo Álvarez
e-mail: harevaloal@unadvirtual.edu.co
Néstor Geoging Martínez Rodríguez
e-mail: ngmartinezr@unadvirtual.edu.co
Gina Oliva Puerto
e-mail: gopuertoe@unadvirtual.edu.co
Jorge Giovanny Becerra Alba
e-mail: jgbecerraa@unadvirtual.edu.co

RESUMEN: *El presente documento contiene una guía detallada para la implementación paso a paso de una infraestructura de red virtual conformada por máquinas virtuales, la primera mediante clientes con distribución GNU Linux Ubuntu y debian y la segunda mediante una distribución Zentyal Server que funcionará como maquina Servidor para proveer y administrar servicios en nuestra red, todo esto soportado en un entorno Virtual a través de VirtualBox. De la misma manera se explica cómo configurar y parametrizar nuestro servidor para proveer cada uno de los servicios de infraestructura de red requeridos por las maquinas clientes para conectarse y tener acceso a internet, así mismo se explica cómo deben implementarse accesos y restricciones alos diferentes recursos por medio de parámetros y reglas en los diferentes servicios del servidor zentyal como una medida de control para el uso eficiente de los recursos tecnológicos de una empresa con el fin mejorar los procesos productivos de los usuarios de Red.*

PALABRAS CLAVE: Servidor, Acceso, Restricción, cortafuegos.

1 INTRODUCCIÓN

El siguiente trabajo tiene la finalidad de aplicar conceptos de administración de Servidores Linux para realizar la instalación, configuración y puesta en servicio de un Servidor a través de una distribución de Linux Zentyal para proveer y administrar los servicios en una red interna con máquinas clientes Linux, y de la misma manera implementar en el servidor cada una de las temáticas correspondientes a la configuraciones de Red, Acceso a internet, cortafuegos, Accesos por VPN, recursos compartidos entre otros servicios dentro de una red de datos que sirva como herramienta de trabajo de un grupo de usuarios, para ello es necesario que los administradores de TI implementen ciertos accesos y restricciones para que estos no hagan uso indebido de los servicios y recursos tecnológicos de la empresa, de esta manera se otorga un nivel de seguridad a nuestro entorno y a su vez se aprovechan de manera eficiente en pro de un mejor desarrollo de sus actividades laborales. Para ello es importante que se haga una debida parametrización de las reglas de Cortafuegos y proxys dentro de cualquier tipo de servidor de tal manera que no se afecten los procesos productivos los usuarios pero que por el contrario se restrinjan aquellas actividades que puedan afectar su desempeño.

2 TEMATICAS DESARROLLADAS

Tabla 1

2.1	CREACIÓN Y CONFIGURACION MAQUINA VIRTUAL
2.2	INSTALACIÓN DE ZENTYAL SERVER
2.3	CONFIGURACIÓN ZENTYAL COMO ROUTER
2.4	RESTRINGIENDO SITIOS WEB MEDIANTE CORTAFUEGOS
2.5	IMPLEMENTACION DNS SERVER Y CONTROLADOR DE DOMINIO.
2.6	IMPLEMENTACION Y GESTION DE PROXY NO TRANSPARENTE
2.7	IMPLEMENTACION Y GESTION DE FILE SERVER Y PRINT SERVER
2.8	IMPLEMENTACION Y GESTION DE VPN

2.1 CREACION Y CONFIGURACIÓN MAQUINA VIRTUAL

2.1.1 Creando maquina Virtual

Haciendo uso de la aplicación virtualbox creamos nuestra máquina virtual para una distribucion GNU Linux de 64 bits a la cual denominamos zentyal-server

Figura1. Navea Y (2021). Creación Maquina Virtual. . Autoria propia.

2.1.2 Confguracion Memoria Ram

Establecemos una memoria de 2Mb para nuestra máquina virtual Zentyal-server

Figura2. Navea Y (2021).Configuracion Memoria para VM. Autoría Propia

2.1.3 CONFIGURACIÓN TAMAÑO DISCO DURO VIRTUAL

Establecemos un tamaño de 50 Gigas para el disco duro virtual de nuestra VM, suficiente para la instalación de nuestro sistema operativo y sus servicios

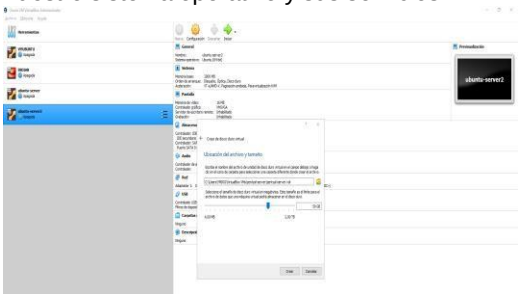

Figura3. Navea Y (2021). Tamaño de disco virtual. Autoría Propia.

2.1.3 CONFIGURACIÓN INTERFACES DE RED

Configuramos nuestras 2 tarjetas de red de la siguiente manera: Adaptador1 para la conexión a internet (Red externa WAN o Zona Roja) y Adaptador2 (Red Interna LAN o Zona Verde) por medio de la cual suministrara los servicios a las maquinas clientes conectadas allí

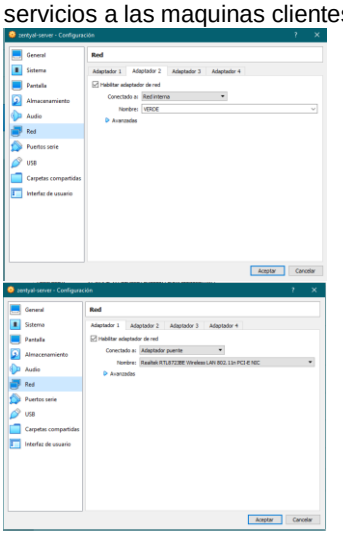

Figura4. Navea Y (2021). Configuración Interfaces de Red. Autoría Propia

2.1.4. RESUMEN CONFIGURACIÓN GENERAL

En esta Figura observamos toda la configuración de hardware de nuestra máquina virtual Zentyal la cual es suficiente para correr su sistema operativo y servir respectivamente a las maquinas clientes que se encuentren conectadas a su red interna

Figura5. Navea Y (2021). Resumen configuración. Autoría propia.

2.2 INSTALACIÓN ZENTYAL SERVER

2.2.1 Cargue de la iso de Instalación de Zentyal

En la unidad virtual óptica de nuestra VM cargamos la iso zentyal-6.2-developmen-amd64.iso para poder arrancar la maquina e iniciar el proceso de instalación

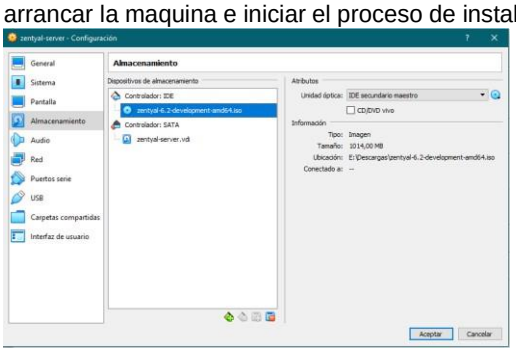

Figura6. Navea Y (2021). Cargue de la .iso de Instalación. Autoría propia.

2.2.3 SELECCIÓN DEL IDIOMA DE INSTALACIÓN

Ya iniciada nuestra VM y el programa de instalación seleccionamos el idioma con el cual vamos a seguir paso a paso el proceso de instalación del zentyal. Autoría propia.

Figura7. Navea Y (2021). Selección de Idioma de Instalación.

2.2.4 SELECCIÓN DE LA UBICACIÓN

Seleccionamos la ubicación de Colombia para fijar la zona horaria con el cual quedará instalado nuestro servidor Zentyal..

Figura8. Navea Y (2021). Ubicación. Autoría propia

2.2.5 SELECCIÓN DE LA UBICACIÓN

Seleccionamos el idioma del teclado acorde a la configuracion de teclas de nuestro teclado fisico para no tener inconvenientes con la escritura de signos, simbolos y caracteres especiales

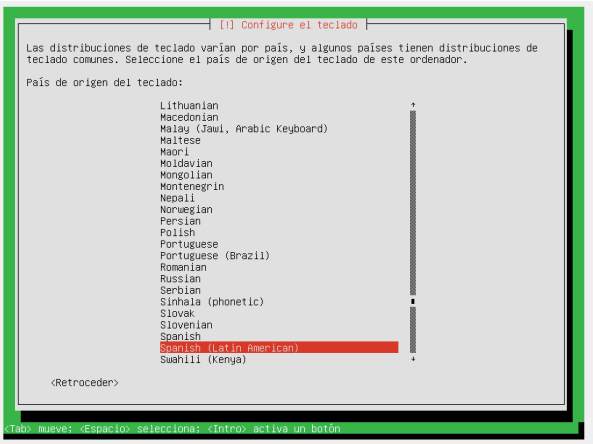

Figura9. Navea Y (2021). Selección del Idioma del Teclado. Autoría propia.

2.2.6 NOMBRE DE LA MÁQUINA

Digitamos el nombre de nuestra VM con la cual se identificará dentro de nuestra red interna

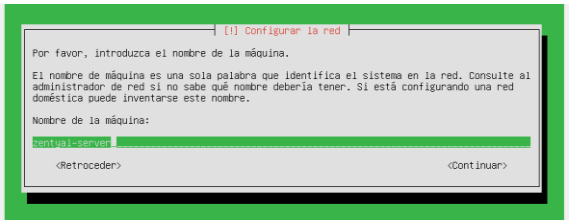

Figura10. Navea Y (2021). Nombre de la VM. Autoría Propia.

2.2.7 NOMBRE DE USUARIO Y CONTRASEÑA

Escribimos el nombre de usuario y contraseña del usuario por defecto con el cual ingresaremos al Zentyal y a su panel de configuracion

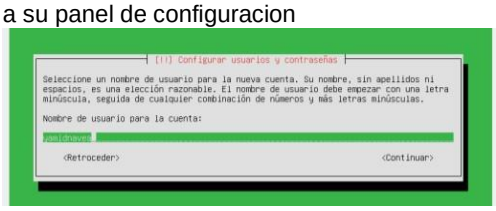

Figura11. Navea Y (2021). Usuario y contraseña. Autoría propia.

2.2.8 CONFIRMACIÓN RELOJ DEL SISTEMA

Confirmamos que el reloj del sistema es acorde a la ubicación geografica y el pais que seleccionamos en punto 2.2.4

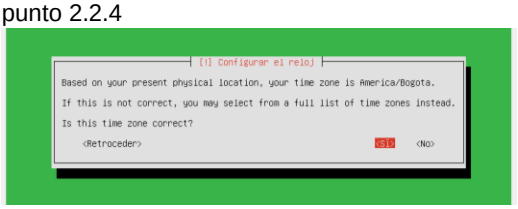

Figura12. Navea Y (2021). Confirmación Reloj del Sistema. Autoria propia.

2.2.9 Iniciando Instalación

Despues de haber ingresado todos los datos de la parametrización de nuestro Servidor Zentyal, se inicia la instalacion del sistema copiando todos los archivos y repositorios al disco duro virtual de nuestro servidor zentyal.

Figura13. Navea Y (2021). Iniciando Instalación. Autoría propia.

2.2.10 FINALIZANDO INSTALACIÓN Y PRIMER INICIO.

Finalizado el proceso de instalación la VM se reniciará y arrancará por primera vez el sistema operativo mostrando como primera pantalla el panel de control en el navegador en la dirección localhost de nuestro servidor zentyal.

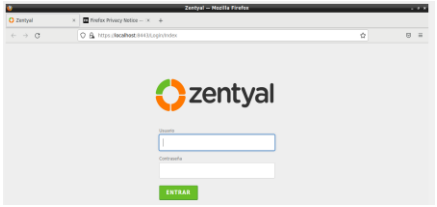

Figura14. Navea Y (2021). Primer Inicio de Zentyal. Autoría Propia

2.2.11 CREAR CLAVE DE SUDO Y ACTUALIZACIÓN

Como primera actividad como administrador de nuestro servidor zentyal, asignamos una clave al super usuario root mediante el comando “sudo passwd”, porteriormente reralizamos una actualización los repositorios mediante el comando “sudo apt update” y “sudo dist-upgrade”

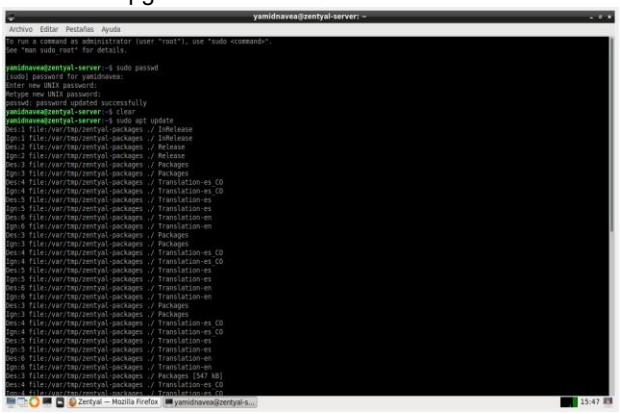

Figura15. Navea Y (2021). Clave root y actualización de paquetes
. Autoría propia.

2.2.12 INGRESO AL PANEL DE CONTROL DE ZENTYAL

Ya teniendo nuestro sistema actualizado procedemos a ingresar al panel de control de nuestro servidor zentyal para comenzar a configurar todos los servicios que vamos a suministrar a nuestras maquinas clientes de la red interna, para ingresar usamos las credenciales de acceso creadas en el punto 3.2.7.

Figura16. Navea Y (2021). Ingreso al panel de control. Autoría propia

2.3 CONFIGURANDO ZENTYAL COMO ROUTER

Para poder restringir sitios web en los clientes de nuestra red interna es necesario que nuestro zentyal funcione como router de internet para poder realizar un filtrado de paquetes a traves de su cortafuegos. Aunque por defecto Zentyal viene preconfigurado para funcionar como router es necesario instalar y parametrizar algunos servicios para que este cumpla dicha funcion de manera eficiente.

2.3.1 INSTALACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

Para el desarrollo de la tematica procedemos a instalar y habilitar el Cortafuegos de nuestro sistema teniendo en cuenta que el bloqueo de sitios debe hacerce a traves de reglas establecidas en el Cortafuegos, para ello en la pantalla inicial de nuestro panel de control damos clic en la opcion Cortafuegos y posteriormente damos clic en instalar, posteriormente el sistema nos indicara en una segunda pantalla los paquetes necesarios para el servicio, por ultimo damos clic en continuar para su instalacion final.

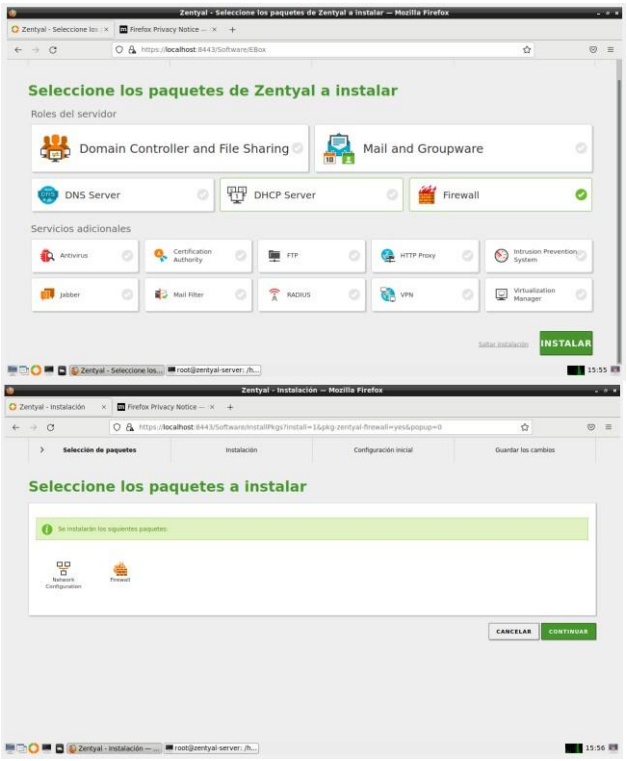

Figura17. Navea Y (2021). Instalación y Configuración de Cortafuegos. Autoría propia.

2.3.2 INSTALACIÓN DE FIREWALL Y COMPONENTESADICIONALES

En la pantalla de la figura observamos el proceso de instalacion de los servicios seleccionados.

Figura18. Navea Y (2021). Instalación cortafuegos. Autoría propia.

2.3.3 HABILITANDO EL CORTAFUEGOS

Para habilitar nuestro cortafuegos nos dirigimos al menu lateral izquierdo y damos clic en la seccion “Estado de los Modulos”, observamos que nuestros servicios no estan habilitados aún, para ello marcamos las casillas de Cortafuegos, Red y guardamos Cambios con el boton “GUARDAR CAMBIOS” que se encuentra en la parte superior derecha, con esto ya tenemos nuestro Cortafuegos habilitado.

Figura19. Navea Y (2021). Habilitar Cortafuegos. Autoría propia.

2.3.4 VERIFICANDO LA EJECUCIÓN DEL CORTAFUEGOS

Para verificar que el Cortafuegos ya se encuentra habilitado y funcionando nos dirigimos al menu lateral izquierdo y damos clic en la seccion “Dashboard”, observamos dentro del dashboard una seccion denominada “Estado de los modulos” y verificamos que los servicios de “Red” y “Cortafuegos” se estan ejecutando correctamente. Autoria propia.

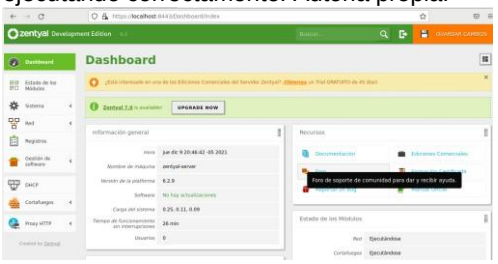

Figura20. Navea Y (2021). Verificando servicio del cortafuegos. Autoría Propia

2.3.5 ESTABLECIENDO INTERFACES DE RED EN ELCORTAFUEGOS

Para comenzar con la parametrización del Cortafuegos o cortafuegos damos clic en el menu lateral izquierdo del panel de control en la seccion cortafuegos, nos aparece una pantalla de configuracion inicial donde configuraremos nuestras interfaces de red, para nuestro caso la interfaz eth0 corresponde a nuestra red externa WAN (internet) y la eth1 corresponde a nuestra red interna LAN, aqui le asignamos una ip fija para nuestra red interna con la dirección 192.168.1.1, mascara de subred 255.255.255.0. Para finalizar el proceso de configuracion damos clic en el boton “GUARDAR CAMBIOS”

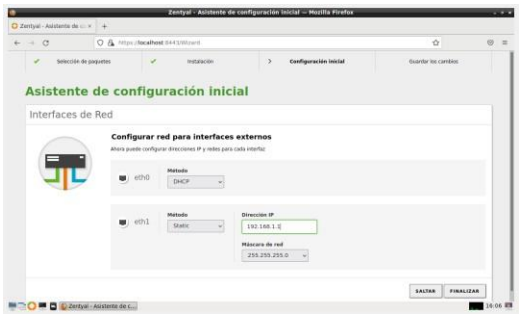

Figura21. Navea Y (2021). Configuración de interfaces de red en el cortafuegos. Autoría propia.

2.3.6 COMPROBANDO INTERFACES DE RED

Para verificar las interfaces nos dirigimos al “Dashboard” y en la seccion “Interfaces de Red”, verificamos que estas esten activas y correctamente configuradas.

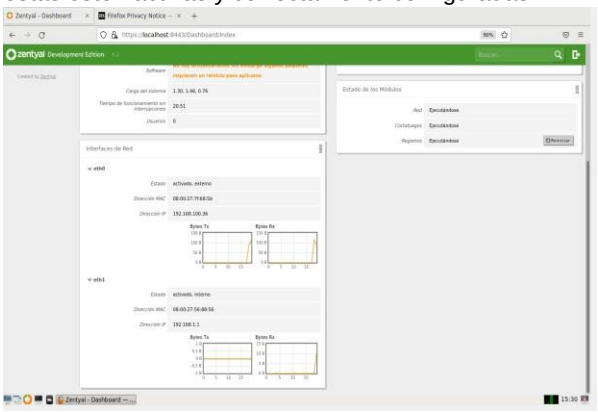

Figura22. Navea Y (2021). Verificando Interfaces. Autoría propia.

2.3.7 CONFIGURANDO IP ESTATICA PARA LA RED Wan

Para poder realizar un filtrado de paquetes mediante el cortafuegos que nos permita bloquear sitios en internet en nuestras maquinas clientes de nuestra red interna debemos configurar nuestro zentyal como router, de hecho este viene por defecto configurado para tal fin mediante una configuraciòn DHCP en la interfaz eth0 lo que hace que su direccionamiento ip sea dinamico, por

lo tanto para para tener un mejor control de nuestro direccionamiento ip para proveer servicios, asignamos una ip fija a la interfaz eth0 cuya direccion debe estar dentro del rango de nuestro proveedor de internet, para ello nos dirigimos a la seccion Red/Interfaces/Eth0 y colocamos la direccion ip y mascara de subred de nuestro proveedor.

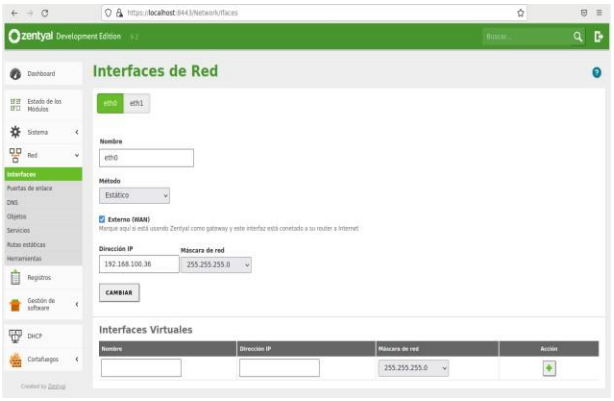

Figura20. Navea Y (2021). Estableciendo Direccionamiento estatico en eth0. Autoría propia.

2.3.8 CONFIGURANDO GATEWAY

Como nuestro zentyal funcionara como router es necesario establecer un gateway que sera entregado a las máquinas clientes mediante DHCP. Para ello en la seccion Red/Puerta de Enlace, añadimos la direccion ip de nuestro router externo de conexión a internet a la interfaz eth0, este gateway sera servido mediante dhcp como puerta de enlace a internet en cada una de las maquinas clientes.

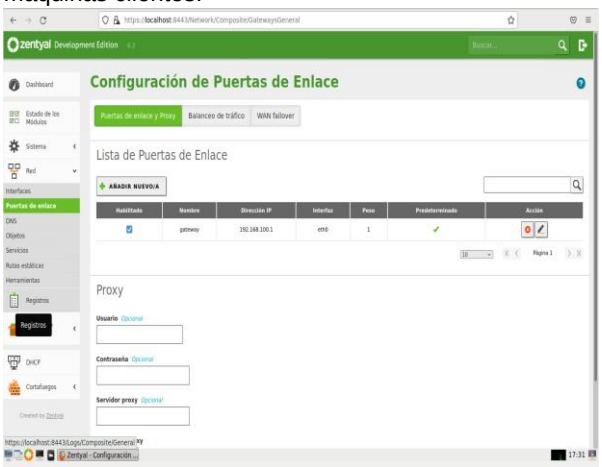

Figura21. Navea Y (2021). Configurando Gateway. Autoría propia.

2.3.9 CONFIGURANDO DNS

Para permitir que nuestro router zentyal entregue DNS mediante dhcp a las maquinas cliente, debemos incluir las direcciones para DNS para ello añadimos y registramos los DNS de google para que cada cliente obtenga este parametro mediante DHCP y haga su respectiva resolucion de nombres de dominio en internet.

Figura22. Navea Y (2021). Configurando DNS. Autoría propia.

2.3.10 INSTALANDO Y HABILITANDO EL SERVICIO DHCP

Para que nuestro zentyal entregue todos los parametros de red a nuestras maquinas clientes debemos instalar y configurar el servicio DHCP. Para ello en la sección “Gestión de Software/Componentes de Zentyal”, seleccionamos e instalamos el servicio DHCP, luego lo habilitamos en la Sección “Estado de los Módulos”. Para terminar “Guardamos cambios”.

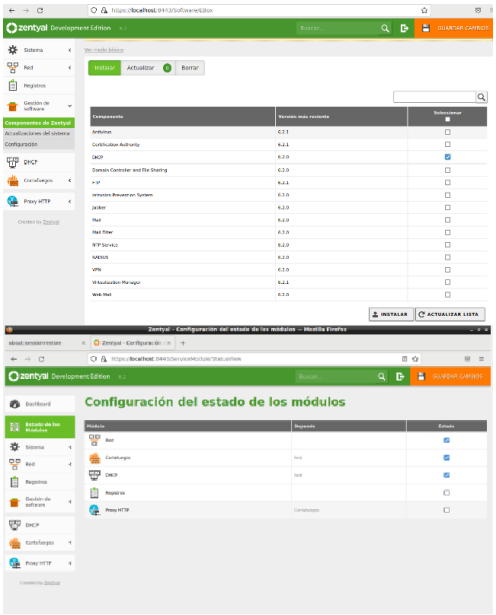

Figura23. Navea Y (2021). Instalando y habilitando el servicio DHCP. Autoría Propia

2.3.11 CONFIGURANDO EL SERVICIO DHCP

Para configurar DHCP, ingramos en el menu lateral izquierdo en la seccion DHCP, y seleccionamos la interfaz por medio de la cual suministraremos el servicio en la red interna, en nuestro caso la eth1, damos clic en el botón configuración de la interfaz eth1.

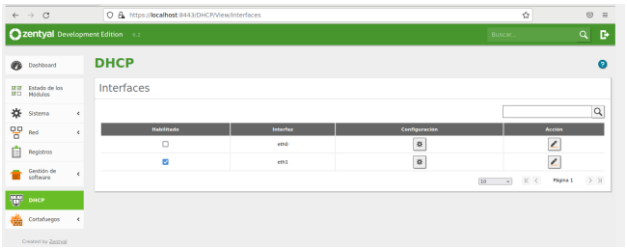

Figura24. Navea Y (2021). Configurando interfaz para el servicio DHCP. Autoria propia.

2.3.12 PARAMETRIZANDO SERVICIO DHCP

En esta sección parametrizamos toda la configuración de red que sera entregada mediante el servicio DHCP a las máquinas clientes, como son la ip dinamica, la ip de la puerta de enlace que en este caso se deja por defecto el Zentyal y la dirección del DNS primario 8.8.8.8. En la sección Rangos DHCP, agregamos un pool o rango de direcciones que entregaremos a nuestras máquinas clientes. Finalizada toda la parametrización guardamos cambios para que se empiece a suministrar el servicio DHCP en la red interna.

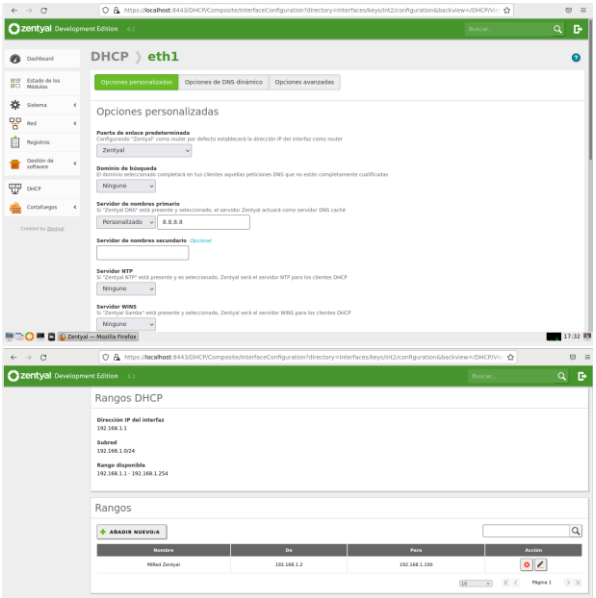

Figura25. Navea Y (2021). Parametrizando DHCP. Autoría propia.

2.3.13 Verificando servicio DHCP en máquina cliente

En una máquina virtual cliente Ubuntu con una interfaz de red conectada a nuestra red interna (Zona Verde) verificamos desde la terminal mediante el comando “ifconfig” los parámetros de red, con ello verificamos el consumo del servicio DHCP suministrado por nuestro servidor Zentyal, y mediante el navegador verificamos que tenemos acceso a internet comprobando de esta manera que nuestro zentyal funciona como router de internet en la red interna. Autoría Propia.

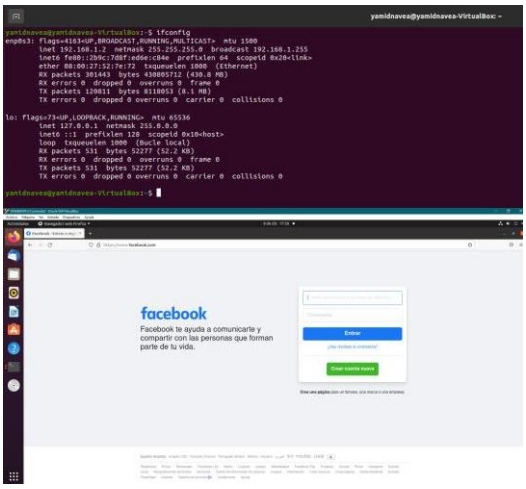

Figura26. Navea Y (2021). Verificando servicio DHCP. Autoría propia.

2.4 RESTRINGIENDO SITIOS WEB MEDIANTE CORTAFUEGOS

Para implementar un bloqueo de sitios web en las máquinas cliente a través del cortafuegos del zentyal es necesario conocer la direcciones ip de los sitios que queremos bloquear ya que dicho bloqueo aplica solo mediante direciones o rangos de ip. La validación del Funcionamiento del cortafuego aplicando y las restricciones solicitadas se hará desde una estación de trabajo GNU/Linux cliente.

2.4.1 VERIFICANDO DIRECCIONES IP DE LOS SITIOS WEB

Desde la terminal del zentyal hacemos ping a los sitios web de facebook y youtube para conocer sus direcciones ip en internet, de esta manera podemos implementar reglas de bloqueo mediante filtrado de paquetes a través de los protolos de red tcp y de navegacion http y https en cada una de las máquinas clientes que se encuentren conectadas a nuestra red interna y que tengan acceso a internet mediante nuestro servidor Zentyal. Para el caso de algunos sitios como youtube que cambia constantemente sus direcciones ip, el bloqueo debe hacerse con la dirección de la subred con su respectivo prefijo para que tome todas las direcciones posibles de su rango.

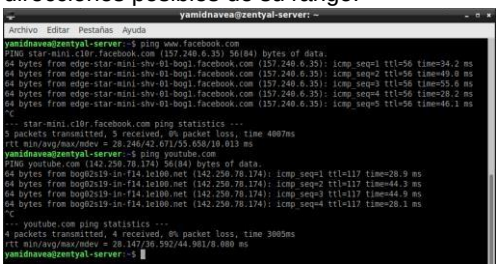

Figura25. Navea Y (2021). Conociendo las ip de facebook y youtube mediante ping desde terminal. Autoría propia.

2.4.2 CREANDO UN SERVICIO PARA LAS REGLAS DE BLOQUEO

Creamos un servicio en la Seccion de Red/Servicios para asi poder crear una sola regla de bloqueo en el Cortafuegos para los protocoles http y https, registrando para ambos casos los protocolos TCPy UDP con sus respectivos puertos 80 y 443.

Figura27. Navea Y (2021). Creando Servicio para crear reglas en el cortafuegos. Autoría propia

2.4.3 CREANDO REGLAS DE FILTRADO EN EL CORTAFUEGOS DEZENTYAL

Teniendo en cuenta que las reglas a aplicar son para filtrar el tráfico de nuestra red interna hacia el internet damos clic en la Sección “Cortafuegos” y seleccionamos el boton “CONFIGURAR REGLAS” de la sección “Reglas de filtrado para las redes internas”.

Figura28. Navea Y (2021). Seleccionando el Tipo de filtrado en el cortafuegos. Autoría propia.

2.4.4 CREANDO PRIRMERA REGLA DE FILTRADO EN ELCORTAFUEGOS PARA EL PROTOCOLO TCP

Nos diriginos a la seccion Cortafuegos/Filtrado de paquetes y añadimos nuestra primera regla la cual es un bloqueo o negación de acceso a la dirección ip de facebook o subred de youtube a través del protocolo TCP desde cualquier terminal de nuestra red interna.

Figura29. Navea Y (2021). Creando Primera Regla de Bloqueo en el cortafuegos para el protocolo tcp. Autoría Propia

2.4.4 CREANDO REGLAS DE FILTRADO PARA LOS PROTOCOLOSHTTP Y HTTPS

Añadimos las siguientes reglas la cuales consisten es un bloqueo o negación de acceso a las direcciones ip de facebook y youtube para los protocolos http y https que tendran efecto en los navegadores de cualquier máquina terminal de nuestra red interna.

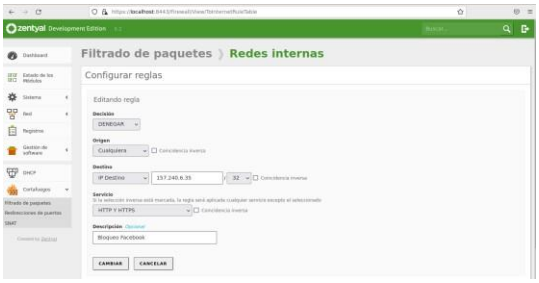

Figura30. Navea Y (2021). Creando Reglas de Bloqueo para los protocolos http y https en el cortafuegos. Autoría propia

Figura31. Navea Y (2021). Creando Reglas de Bloqueo para los protocolos http y https con subred. Autoría propia.

2.4.4 VERIFICANDO LISTA DE REGLAS DE FILTRADO

Después de añadidas cada una de las reglas de filtrado estas aparecerán relacionadas en la sección de Filtrado de Paquetes para redes internas, allí se pueden observar los parámetros de filtrado para cada una de ellas. Para aplicar las reglas, damos clic en el botón “GUARDAR CAMBIOS”.

Figura31. Navea Y (2021). Verificando Lista de Reglas de filtrado. Autoría propia.

2.4.5. VERIFICANDO REGLAS DEL CORTAFUEGO.

Desde el navegador de nuestra máquina cliente ubuntu intentamos acceder a cualquier sitio en internet y observamos que navega normalmente, más sin embargo a tratar de ingresar a los sitios de Facebook y youtube, comprobamos que el acceso es bloqueado por el cortafuegos.

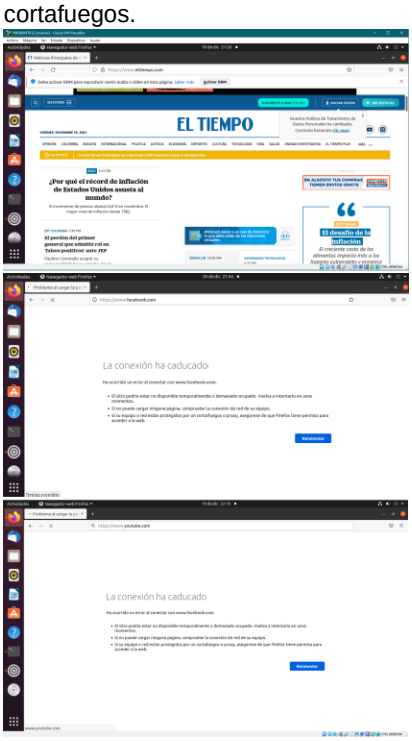

Figura32. Navea Y (2021). Verificando el bloqueo de los sitios de facebook y youtube. Autoría propia

2.4.5. Restableciendo reglas de acceso a sitios.

Al eliminar las reglas de bloqueo para Facebook y youtube creadas anteriormente y guardar los cambios nuevamente volvemos comprobar en el navegador de nuestra máquina Ubuntu cliente que este ya tiene acceso nuevamente a los sitios que estaban bloqueados por el cortafuegos comprobando así su funcionalidad.

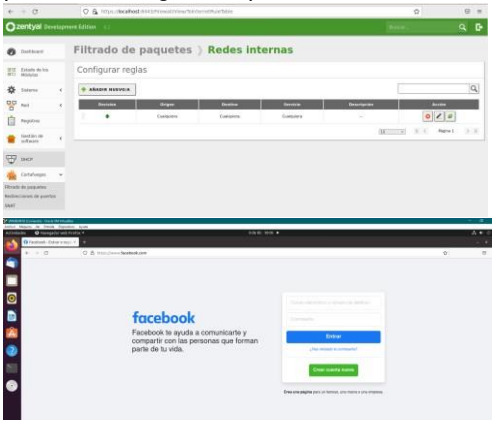

Figura33. Navea Y (2021). Verificando el acceso a los sitios web. Autoría propia

2.5 IMPLEMENTACIÓN Y CONFIGURACIÓN DE DNS SERVER Y CONTROLADOR DE DOMINIO.

Nos Dirigimos al Dashboard e instalamos el Paquete de DNS Server.

Figura 34. Arevalo H (2021). Instalación de DNS Server. Autoría Propia

Despues de instalado y habilitado el Servidor DNS se nos dirigimos al Dashboard menulateral Izquierdo y seleccionamos DNS Server, donde me aparec en las siguientes opciones. Para mi caso habilitó la opción caché de DNS transparente.

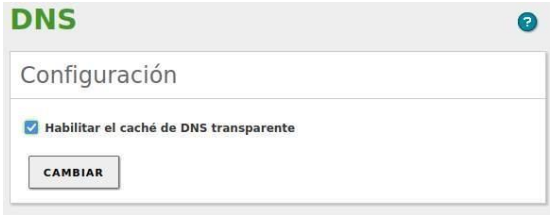

Figura 35. Arevalo H (2021). Habilitar cache de DNS transparentes. Autoría Propia

Lo siguiente es ir a la opción de dominio y se realiza la siguiente configuración, seleccionamos el servidor, asignamos nombre y descripción de nuestro dominio.

Figura 36. Arevalo H (2021). Asignación de nombre de dominio. Autoría Propia

Confirmamos la configuración anterior

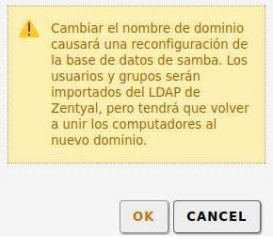

Figura 37. Arevalo H (2021). Confirmación de asignación de nombre de dominio. Autoría Propia

En la configuración general se realiza el siguiente cambio del dominio. z-haminton.unad.

Figura 38. Arevalo H (2021). Nombre de dominio. Autoría Propia

Por último al ir a la opción de DNS se puede reflejar el cambio del dominó.

Figura 39. Arevalo H (2021). Verificación de dominio. Autoría Propia

Para la implementación de usuarios y grupos en el dashboard nos dirigimos a la opción usuarios y grupos. Y seleccionamos la opción añadir. En la interfaz que se muestra lo primero que se realiza es la creación de un grupo con la siguiente configuración.

Figura 40. Arevalo H (2021). Creación de grupo. Autoría Propia

Una vez creado el grupo se procede a hacer un nuevo usuario con la siguiente configuración asignando al nuevo grupo llamado unad.

Figura 41. Arevalo H (2021). Creación de usuario. Autoría Propia

2.6 IMPLEMENTACIÓN Y GESTIÓN DE PROXY NO TRANSPARENTE

Nos dirigimos al Dashboard seleccionamos e instalamos el paquete HTTP Proxy con sus respectivos servicios adicionales.

Figura 42. Arevalo H (2021). Selección e Instalación de Paquetes para el Servicio de HTTP Proxy. Autoría Propia

El proxy no transparente nos permite configurar la ip en todos los equipos a diferencia del transparente este no requiere configurar los datos del servicio proxy. El proxy no transparente restringe los permisos a los usuarios y deja solo el permiso del proxy es por esto que se tiene

un control directo de la ip o sitio que se quiere restringir el acceso a usuario o cliente.

Creamos un objeto de red para nuestro grupo de clientes proxy, para ello nos ubicamos en la pestaña red, entramos en la pestaña objetos, damos clic en añadir, creamos el nuevo grupo de clientes, luego dentro del grupo ya creado creamos nuestro cliente1 para un equipo Debian como ejemplo y le colocamos la ip para el equipo cliente.

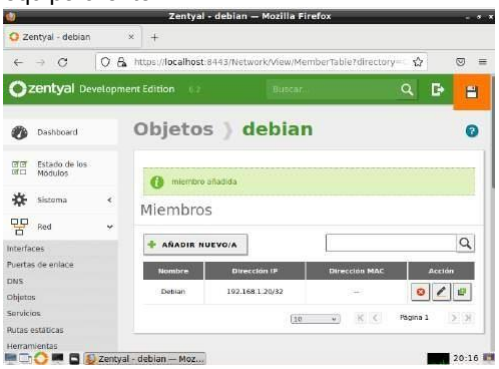

Figura 43. Arevalo H (2021). Creación de Grupos y clientes para el proxy. Autoría Propia

Ingresamos a modulo proxy HTTP, para configurar el puerto solicitado “1230”, dejamos desmarcada la opción proxy transparente.

Figura 44. Arevalo H (2021). Configuración proxy HTTP. Autoría Propia

Creamos reglas de acceso para permitir o restringir el acceso a internet por días y horas según el control que queramos establecer en nuestra red interna.

Figure 45. Arevalo H (2021). Parametrización de Reglas de Acceso y Restricción. Autoría Propia

En nuestras maquinas cliente en preferencias del navegador parametrizamos la conexión a internet mediante proxy para ellos de indicamos la ip y el puerto de nuestro servidor Zentyal como proxy

Figure 46. Arevalo H (2021). Configuración de proxy en cliente. Autoría Propia

Por último, ingresamos a cualquier pagina en internet de nuestra maquina cliente ya parametrizada para navegar mediante proxy y verificamos el acceso a internet.

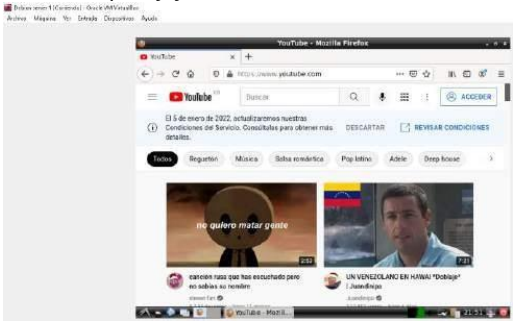

Figure 47. Arevalo H (2021). Navegación por medio de proxy zentyal. Autoría Propia

2.7 IMPLEMENTACIÓN Y GESTIÓN DE FILE SERVER Y PRINT SERVER

En la opción de usuarios y equipos del menú lateral izquierdo del Dashboard ingresamos y creamos un nuevo usuario el cual vamos a conectar desde nuestro cliente ubuntu.

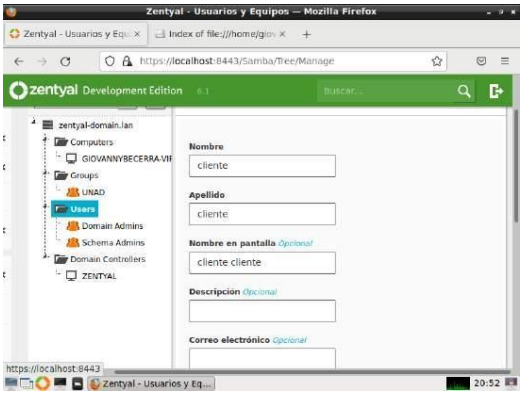

Figura 48. Becerra G (2021). Creación de usuario. Autoría Propia

Para unir nuestro Ubuntu a nuestro dominio se requiere tener el instalado en cada una de las maquinas cliente el software PowerBroker Identity ServicesOpen, el cual procedemos a descargar instalar mediante consola de nuestro cliente ubuntu.

Figura 49. Becerra G (2021). Instalación de PowerBroker Identify Services Open. Autoría Propia

Comprobamos que tengamos comunicación entre el cliente y el servidor mediante el comando ping.

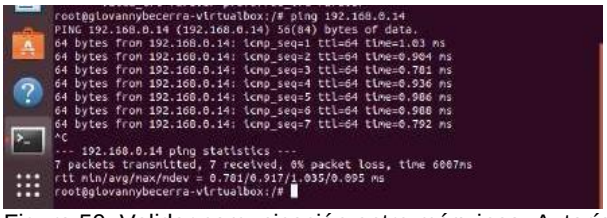

Figura 50. Validar comunicación entre máquinas, Autoría propia.

En configuración de red DNS de la maquina cliente mediante digitamos la ip de nuestro servidor.

Figura 51. Becerra G (2021). Configuración ip DNS del servidor en el cliente. Autoría propia.

Una vez realizada la configuración anterior se puede ingresar el equipo de Ubuntu al servidor mediante el comando: domainjoin-cli join --disable ssh zentyal-domain.lan.

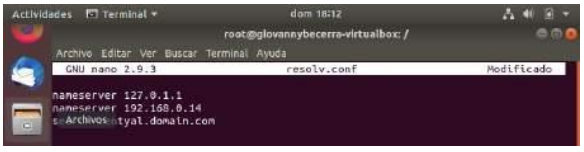

Figura 52. Becerra G (2021). Configuración permisos para conectar el servidor. Autoría propia.

En la opción de compartición de ficheros del menú del Dashboard añadimos una carpeta en este caso la llamamos impresoras.

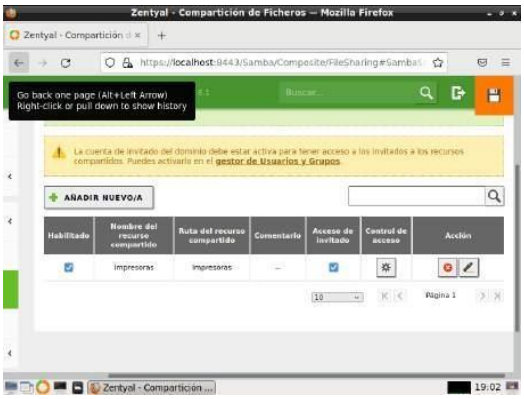

Figura 53. Becerra G (2021). Creamos una carpeta para compartir desde el servidor. Autoría propia.

Nos conectamos al servidor desde nuestro cliente por medio de su nombre de dominio.

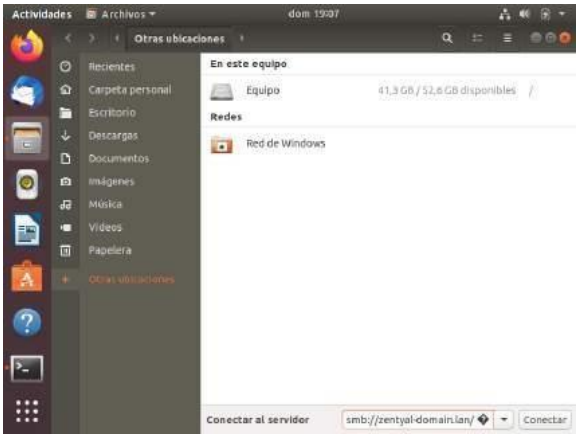

Figura 54. Becerra G (2021). Conexión al servidor desde nuestro cliente Autoría propia.

Verificamos que el recurso compartido impresoras aparezca después de realizar la conexión.

Figura 55. Becerra G (2021). Verificando carpeta compartida en el servidor desde el cliente. Autoría propia.

Ahora desde nuestro cliente creamos la carpeta Diplomado Linux la cual debe aparecer dentro de la estructura de carpetas compartidas de nuestro servidor.

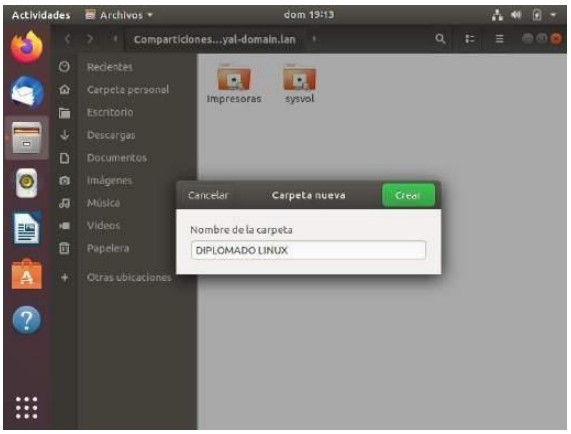

Figura 56. Becerra G (2021). Creando una carpeta desde el cliente, Autoría propia.

Dentro de la carpeta Diplomado Linux, creamos otra carpeta que se llama Zential

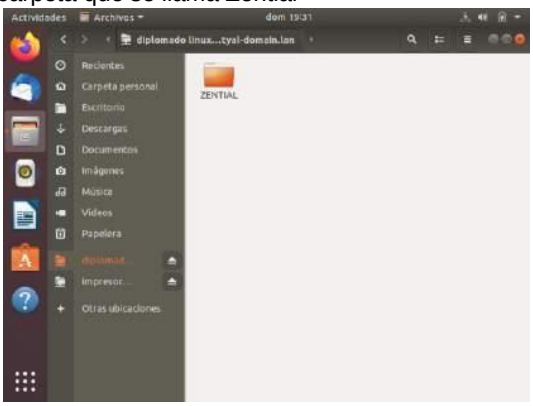

Figura 57. Becerra G (2021). Carpeta Zentyal creada en nuestra carpeta Diplomado Linux desde nuestra máquina cliente. Autoría propia.

Ahora observamos desde nuestro servidor que ya aparece la carpeta que creamos desde nuestro cliente.

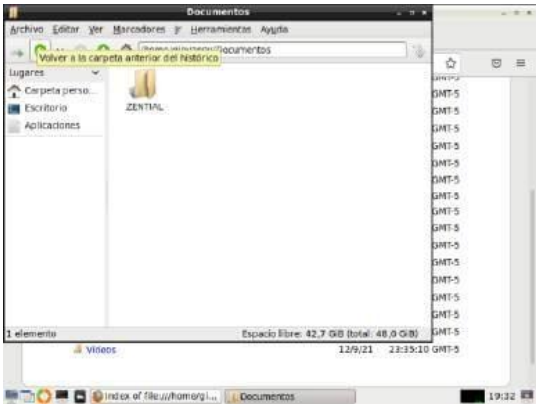

Figura 58. Becerra G (2021). Verificando Carpeta creada desde el cliente en nuestro servidor zentyal. Autoría propia.

2.8 IMPLEMENTACIÓN Y GESTIÓN DE VPN

Dentro del Dashboard Seleccionamos el paquete a instalar: Para este caso seleccionar VPN y dar clic en instalar.

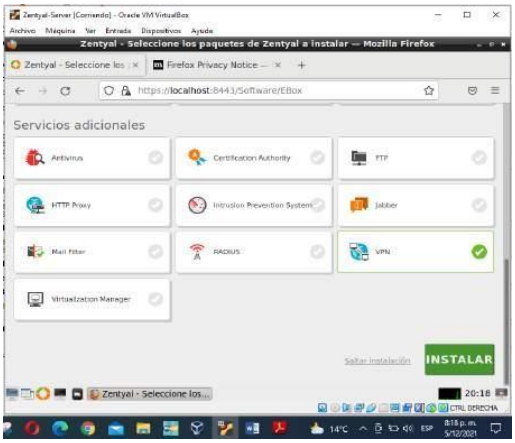

Figura 59. Martínez G (2021). Selección paquete a Instalar. Autoría propia.

Muestra los paquetes requeridos a instalar en este caso:

- Configuración de la red
- Cortafuegos
- Autoridad de certificación
- VPN

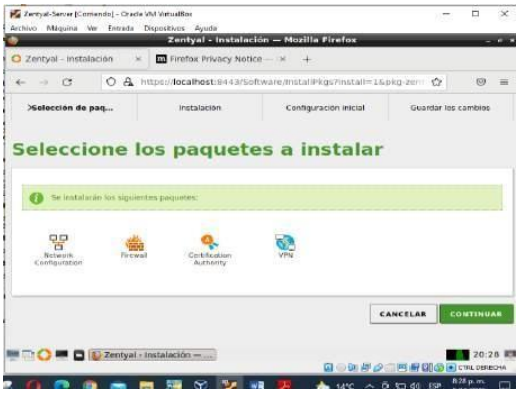

Figura 60. Martínez G (2021). Servicios requeridos, Autoría propia.

Instalación VPN Completada: A partir de este momento se puede hacer uso del tablero para continuar con la configuración requerida en la temática. Luego de finalizada la instalación, podremos acceder al tablero donde se llevará a cabo la creación y gestión de la VPN.

Configuración inicial en tablero: Dar clic en VPN, y luego en servidores.

Figura 61. Martínez G (2021). Servidores VPN. Autoría propia.

Configurando interfaz eth1: Configurar ip estática.

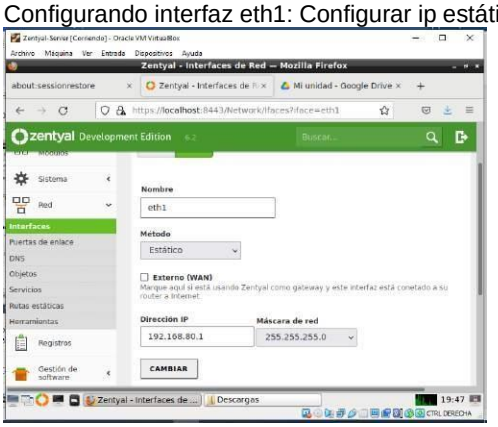

Figura 62. Martínez G (2021). Interfaz eth1. Autoría propia.

Creando Modulo de autoridad de certificación: Como primera medida se debe crear el módulo. Se deben asignar valores y oprimir en crear.

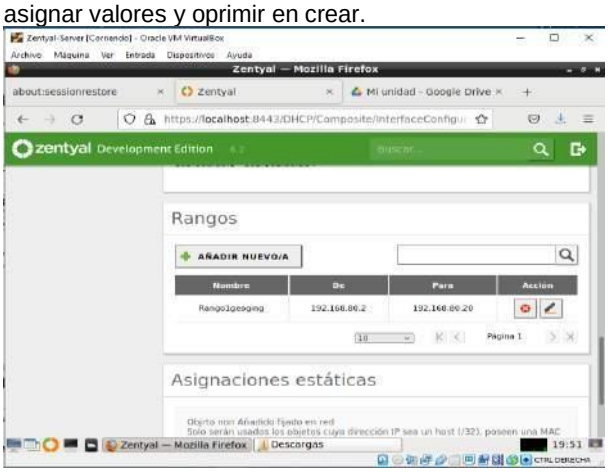

Figura 63. Martínez G (2021). Asignando rangos. Autoría propia.

Creando Modulo de autoridad de certificación: Como primera medida se debe crear el módulo. Se deben asignar valores y oprimir en crear.

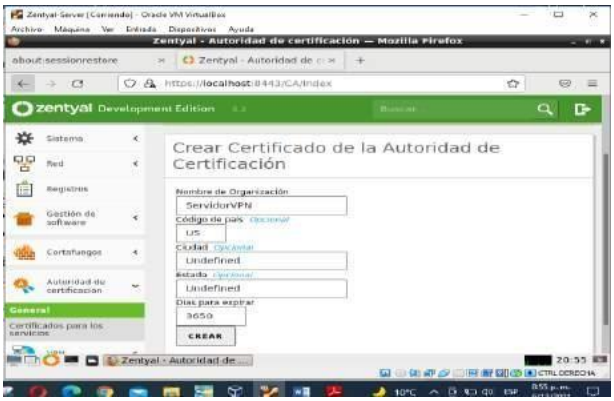

Figura 64. Martínez G (2021). Certificado de autoridad. Autoría propia.

Dando Nombre: clic en expedir.

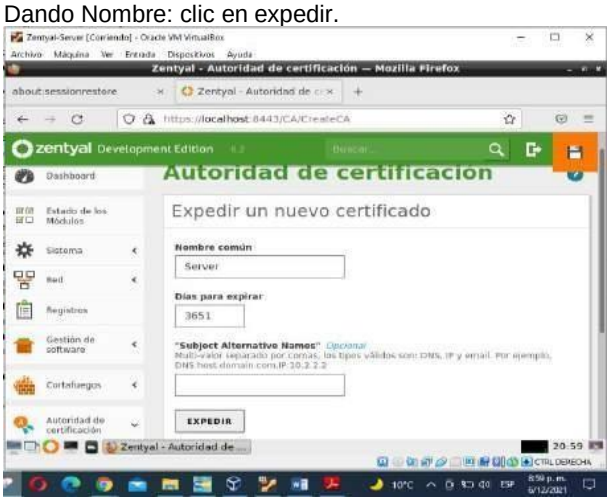

Figura 65. Martínez G (2021). Expedir certificado. Autoría propia.

Observando certificado creado: Brinda Nombre, estado fecha y acciones para el certificado, dar clic en guardar.

Figura 66. Martínez G (2021) Lista certificados. Autoría propia

Guardando cambios: clic en Guardar.

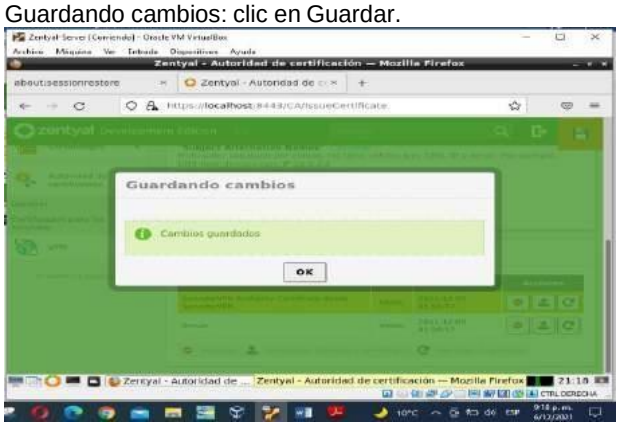

Figura 67. Martínez G (2021). Guardando cambios. Autoría propia

Añadiendo servidor: Nuevamente módulo VPN - Servidores – añadir Nuevo.

Figura 68. Martínez G (2021). Añadiendo servidor. Autoría propia

Configurando servidor VPN creado: Seleccionar certificado de servidor creado (server), habilitar interfaz TUN, conexiones cliente - cliente y Nat. Las demás configuraciones se dejan por defecto.

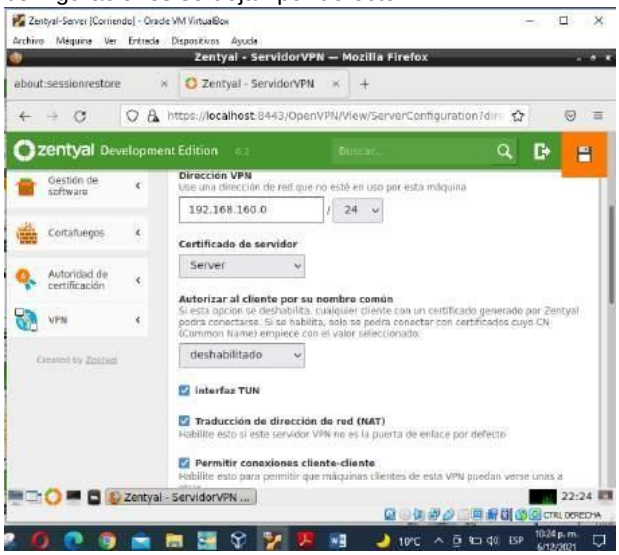

Figura 69. Martínez G (2021). Configuración servidor VPN. Autoría Propia

Generando certificado cliente: Dirigirse a VPN autoridad de certificación – General. Con el fin de generar un certificado para el CLIENTE.

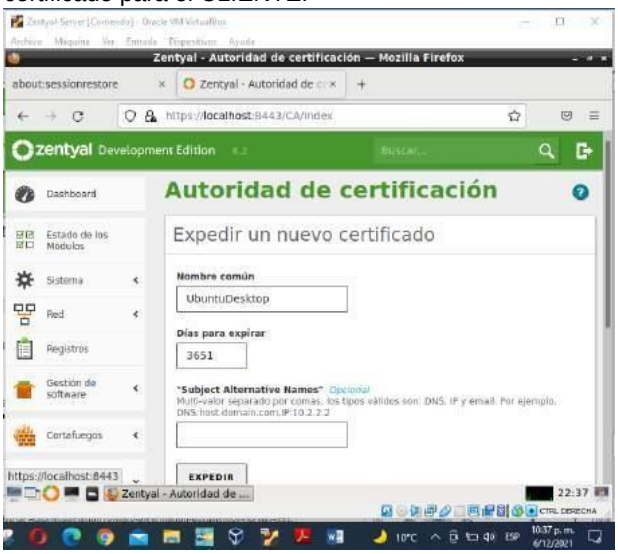

Figura 70. Martínez G (2021). Certificado cliente. Autoría Propia

Lista certificados:

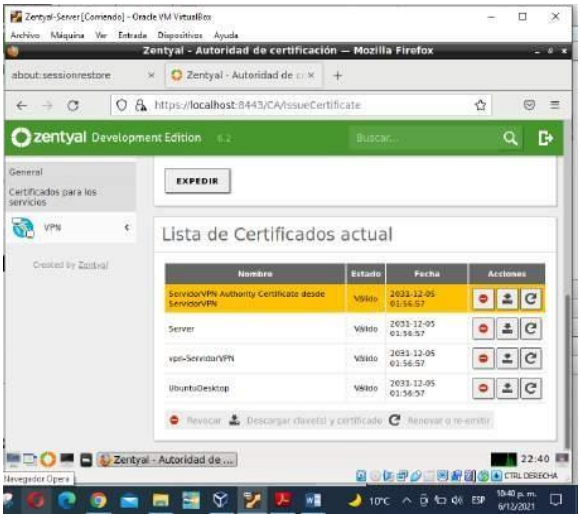

Figura 71. Martínez G (2021) Lista certificados. Autoría Propia

Para continuar con la configuración se debe:

- Dar clic en VPN
- Dar clic en servidores
- Dar clic en la configuración de descarga de paquetes de configuración para cliente.

Una vez dentro de la configuración de la descarga de paquetes para cliente:

- Escoger tipo de cliente (Linux)
- Escoger certificado creado para cliente (Ubuntu)
- Definir IP estática

Descargando paquete de configuración de cliente: Clic en descargar.

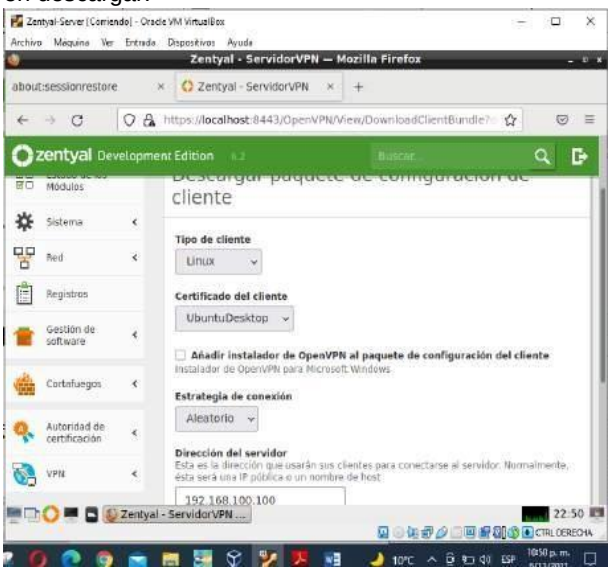

Figura 72. Paquete configuración cliente. Autoría Propia

Guardando certificado descargado para el cliente:

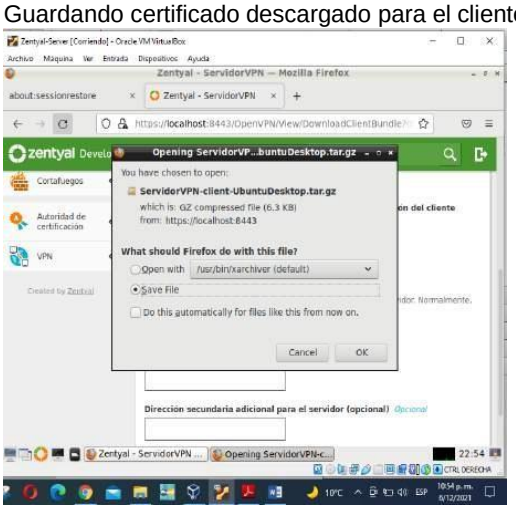

Figura 73. Martínez G (2021). Guardando paquete cliente. Autoría Propia

Ahora se procede a la configuración de la VPN desde el servidor hacia el Cliente. Para este fin, nos dirigimos a windows (cliente) para configurar las conexiones VPN en este.

Preparando paquete descargado desde el servidor (zentyal) en cliente: Previamente se prepara el archivo de configuración que se descargó del servidor zentyal, copiando los archivos en el cliente.

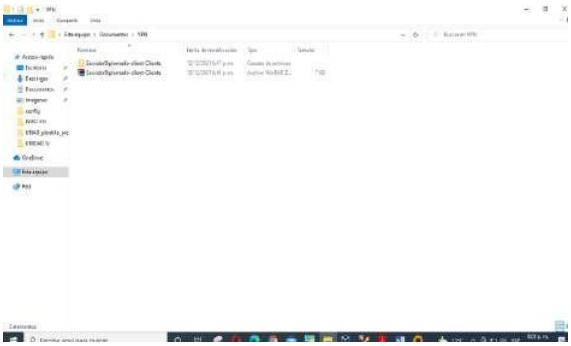

Figura 74. Martínez G (2021). paquete cliente. Autoría Propia

Configurando VPN en cliente: Se usa OpenVPN Connect para importar el archivo con la configuración del servidor.

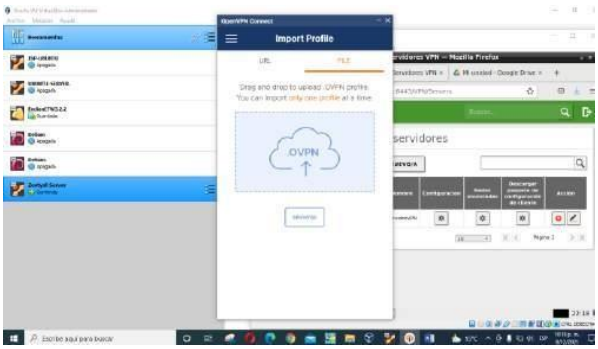

Figura 75. Martínez G (2021). VPN Connet. Autoría Propia

Verificando datos importados:

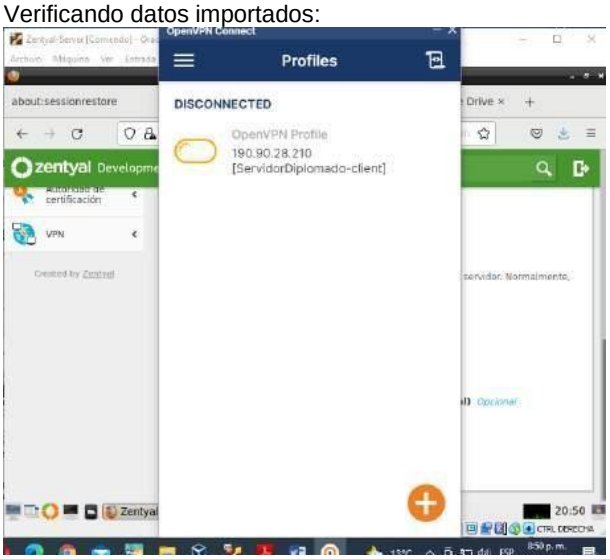

Figura 76. Martínez G (2021). Conectando VPN. Autoría Propia

3. CONCLUSIONES

Es importante tener en cuenta que existen alternativas de software libre para dar solución a cualquier necesidad que requiera de tecnología informática, las distribuciones de Linux son una potente alternativa ya que cuenta con todas las herramientas necesarias para satisfacer las necesidades ya sea en el ámbito empresarial o individual.

Toda infraestructura de red es un conjunto de máquinas, conexiones y servicios que dependen de un servidor encargado de proveer dichos servicios los cuales deben ser debidamente administrados otorgar accesos o restricciones a los recursos según sea el caso.

Zentyal es una distribución de Linux muy potente para proveer y administrar servicios dentro de cualquier entorno Tecnológico por complejo que sea; ya que cuenta con una interfaz muy amigable con una serie de herramientas y opciones de parametrización que nos permiten realizar de manera eficaz y eficiente todo tipo de control y monitoreo a nuestra Red.

4. REFERENCIAS BIBLIOGRAFICAS

[1] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial. Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92

[2] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 6 – 84). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56046?page=6

[3] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing. Recuperado de https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page-_-20

[4] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40

[5] Ramírez Restrepo, J. (1,06,2021). OVI - Unidad 6 - ISPConfig. [Archivo de video]. Recuperado de https://repository.unad.edu.co/handle/10596/41421

[6] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 205 - 236). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43262?page=205