

ADMINISTRACIÓN DE SERVICIOS Y PROTOCOLOS CON EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE BASADAS EN GNU/LINUX.

Diego Raúl Forero Nivia Cod: 13992426
drforeron@unadvirtual.edu.co
Jhon Alejandro Camargo Jiménez Cod: 93238319
jacamargoj@unadvirtual.edu.co
Alejandra Morales Ropero Cod: 1110535917
amoralesrop@unadvirtual.edu.co
Luis Eduardo Obando Bonilla Cod: 1105614452
leobandob@unadvirtual.edu.co
Emilsen Palacio Carvajal Cod: 28540106
epalacioc@unadvirtual.edu.co

RESUMEN: *El principal objetivo es brindar soluciones a gran parte de las problemáticas en la migración e implementación de sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red de las pequeñas y medianas empresas. Por este motivo se desarrolla este documento donde se explicará la instalación y configuración del sistema operativo Zentyal Server 6.2, donde implementáramos los servicios como el DHCP server, DNS server, controlador de dominio, proxy no transparente, cortafuegos, file server, print server y VPN*

PALABRAS CLAVE: Sistema operativo, Zentyal, servidor, cliente, IP, usuarios, DHCP, dominio, proxy, protocolos, interfaz.

1 INTRODUCCIÓN

Para el desarrollo de esta actividad aprenderemos, aplicar y dar soluciones bajo el modelo cliente-servidor, donde cada uno de los servicios configurados responderán a solicitudes hechas por equipos clientes unidos a la red LAN corporativa. Por este motivo se realiza la instalación del servidor zentyal 6,2, y se configurara e implementación servicios tales como proxy no trasparenten donde la salida a internet debe ser válida por el puerto 1230, permitiendo mayor seguridad en los sistemas informáticos o de la información.

Implementación y configuración de un cortafuego, restringiendo la apertura de sitios o portales web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas.

File server y print server, permitiendo acceso de una estación de trabajo GNU/Linux a través del controlador del protocolo LDAP a los servicios de carpetas compartidas e impresoras.

Creación de una VPN que permita un túnel privado de comunicación con una estación de trabajo GNU/Linux.

Y Configuración e implementación del servicio de direccionamiento IPs automático DHCP, DNS server y controlador de dominio permitiendo administrar salvaguardas, permisos y otros protocolos de acceso de forma remota en cada dispositivo.

2 TEMATICAS

2.1 SERVIDOR ZENTYAL

La implementación realizada para dar solución a la problemática planteada, se ejecutará bajo GNU/Linux Zentyal server versión 6,2. Dicha plataforma nos permitirá gestionar infraestructura TI por medio de módulos configurables que permitirá unificar y administrar fácilmente todos los servicios básicos de infraestructura de red, accesibilidad, seguridad y control sobre los recursos informáticos, y que en este documento se explicará el paso a paso para instalar esta distribución de Linux como sistema operativo base para disponer de los servicios de infraestructura TI.

2.2 SERVICIOS DE GESTION DE INFRAESTRUCTURA TI

Para el desarrollo de este trabajo, se plantea explicar el proceso de instalación y configuración de servicios para la gestión de infraestructura TI, el cual estará dividida en cinco temáticas que indican a continuación.

Temática 1: DHCP Server, DNS Server y Controlador de Dominio.

Temática 2: Proxy no transparente.

Temática 3: Cortafuegos.

Temática 4: File Server y Print Server.

Temática 5: VPN.

De esta manera se pretende que los procesos documentados durante la instalación y configuración sea de fácil comprensión y cumpla la funcionalidad esperada para cada temática planteada.

3 INSTALACION SERVIDOR ZENTYAL

Para el proceso de instalación del servidor Zentyal se usa un software de virtualización, que nos permitirá crear una máquina virtual que tendrá ciertas características de hardware que nos permitirá instalar la distribución de Linux Zentyal server versión 6,2.

Características de la máquina virtual:

- Procesador: 1 núcleo
- Memoria RAM: 2 Gb
- Disco duro de almacenamiento: 19 Gb
- Interfaces de red: 2 tarjetas de red
- 1 interfaz puente para conexión con internet
- 2 interfaz red interna para conectar los hosts locales

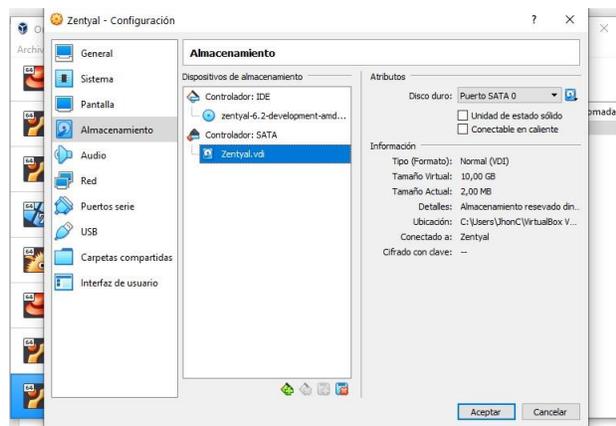


Figura 1. Configuración De Unidad Almacenamiento.
Fuente: Elaboración propia.

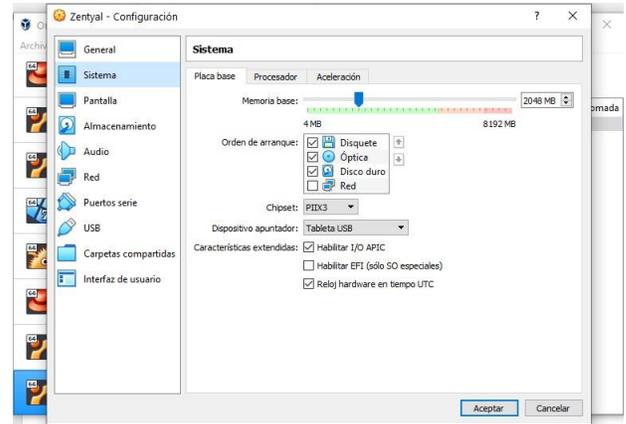


Figura 2. Configuración memoria RAM virtual.
Fuente: Elaboración propia

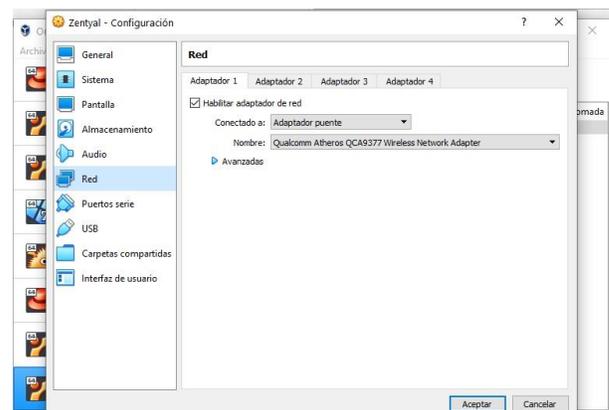


Figura 3 Configuración De Interfaz WAN
Fuente: Elaboración propia.

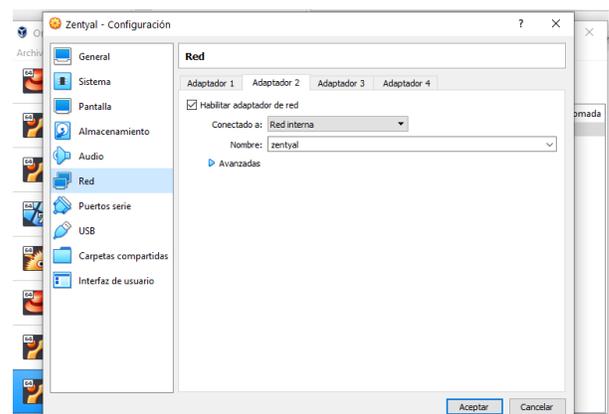


Figura 4 Configuración de interfaz LAN
Fuente: Elaboración propia.

Después de tener configurada la máquina virtual con los requerimientos mínimos de hardware, procedemos a instalar la distribución de Zentyal a través del archivo ISO obtenida de la URL <http://download.zentyal.com/> y cuya arquitectura es de 64 bits.

Al iniciar el proceso de instalación del Zentyal la primera pantalla nos muestra el listado de idiomas el cual debemos seleccionar español como lenguaje del asistente de instalación.

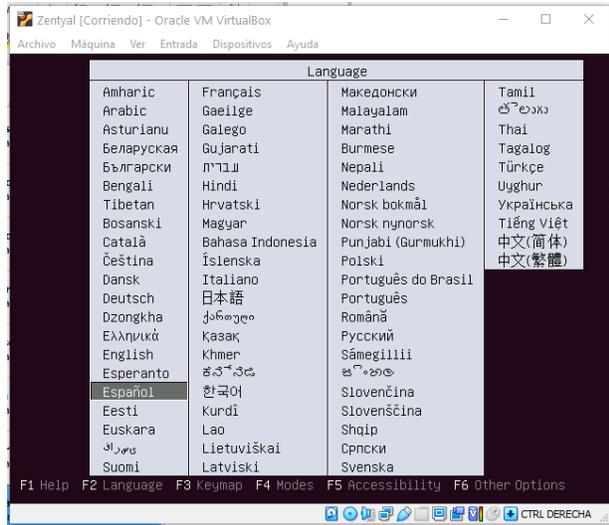


Figura 5 Seleccionar Lenguaje De Instalación.
Fuente: Elaboración propia

Después de seleccionar el lenguaje de instalación procedemos a instalar la distribución utilizando la opción por omisión que elimina todo el contenido del disco duro virtual configurado y crea las particiones necesarias para la ejecución del Zentyal 6.2.

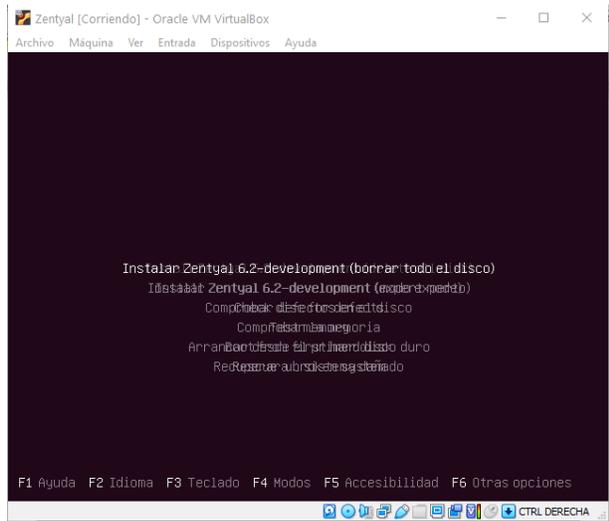


Figura 6 Selección De La Opción De Instalación Por Omisión. Fuente: Elaboración propia

Seleccionamos el nombre del país Colombia como configuración local de nuestro sistema para fijar la zona horaria.

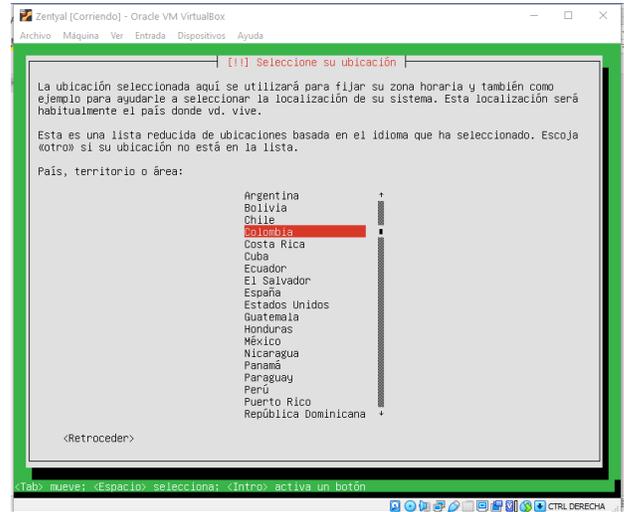


Figura 7 Seleccionar La Ubicación.
Fuente: Elaboración propia.

Posteriormente se selecciona la distribución de teclado dejando por defecto el idioma español.

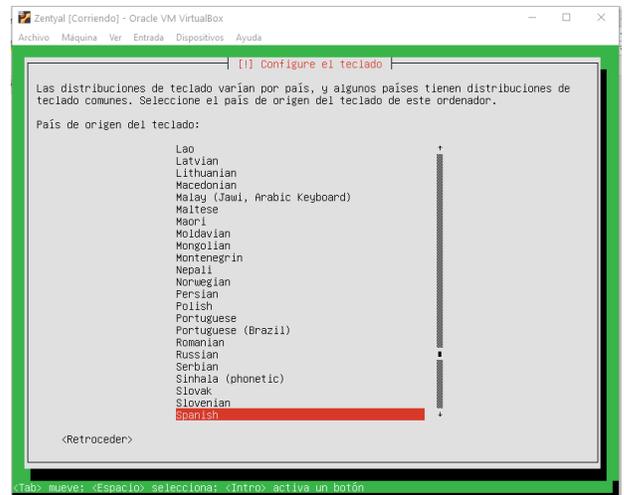


Figura 8 Configuración De Teclado.
Fuente: Elaboración propia

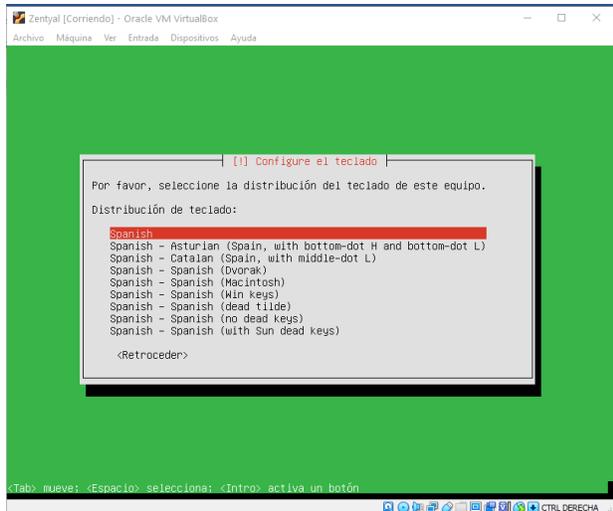


Figura 9 Selección Del Idioma Del Teclado.
Fuente: Elaboración Propia.

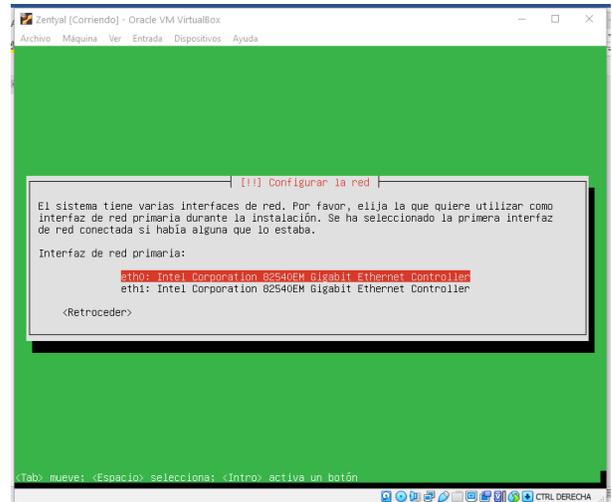


Figura 11 Configuración De Interfaz Red
Fuente: Elaboración propia.

En esta parte de la instalación se debe elegir el nombre que tendrá el servidor Zentyal, para sea identificado en el entorno de red.

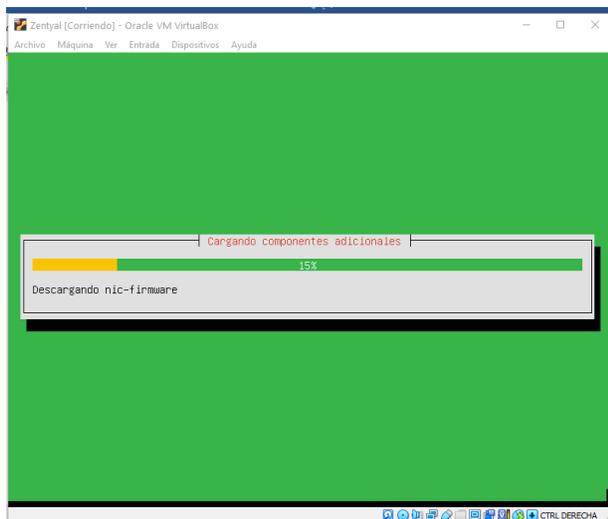


Figura 10 Proceso De Instalación De Componentes.
Fuente: Elaboración propia.

A continuación, el instalador procederá a configurar la interfaz de red, al tener dos interfaces de red el asistente de configuración pregunta cuál de las dos tarjetas de red se usará como primaria durante la instalación. De esta manera se selecciona la interface eth0 que está configurada para nuestra conexión a internet.

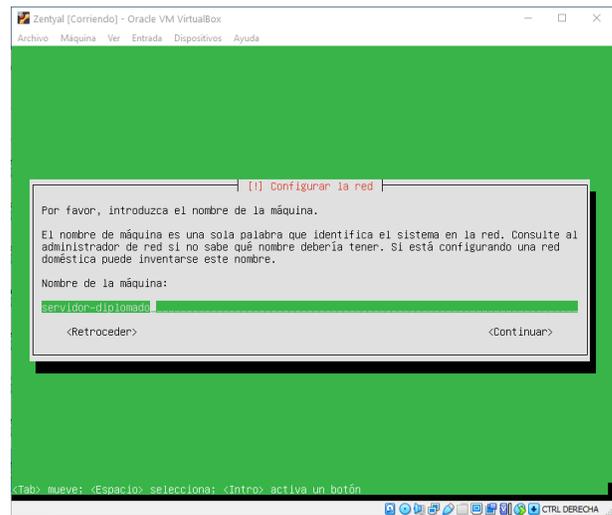


Figura 12 Nombre De La Máquina.
Fuente: Elaboración propia.

Después de asignarle el nombre de la máquina, pasaremos a configurar el nombre de la cuenta de administrador del sistema, Este usuario tiene pleno acceso a la máquina, sus recursos y puede también acceder a la interfaz de administración de Zentyal.

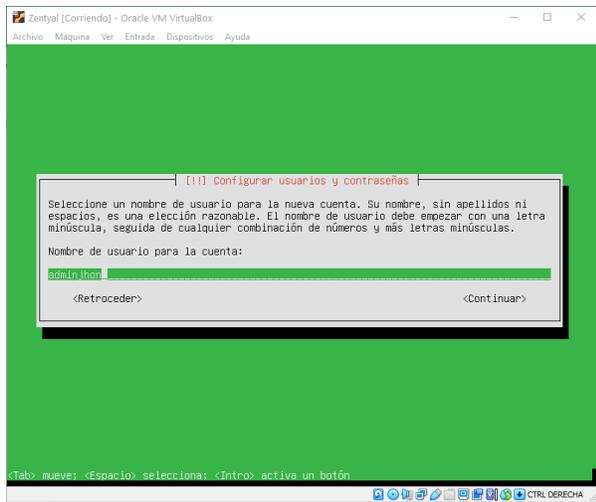


Figura 13 Nombre del Usuario Administrador.
Fuente: Elaboración propia.

Para terminar la configuración del usuario administrador establecemos la contraseña de acceso.

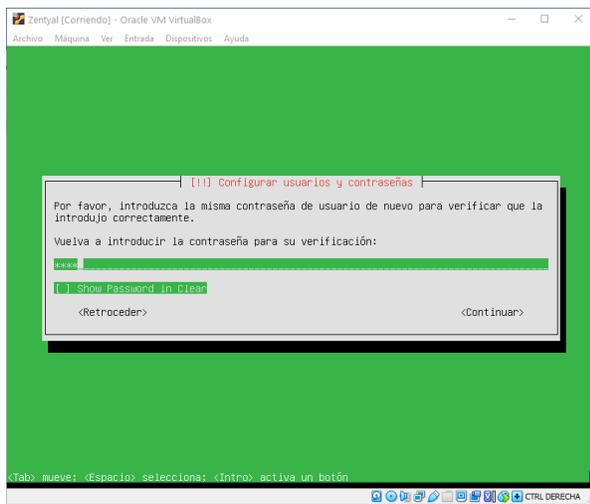


Figura 14 Asignación De Contraseña.
Fuente: Elaboración propia.

Posterior a la configuración del usuario de administrador, el sistema pasara a la configuración de reloj y zona horaria del sistema.

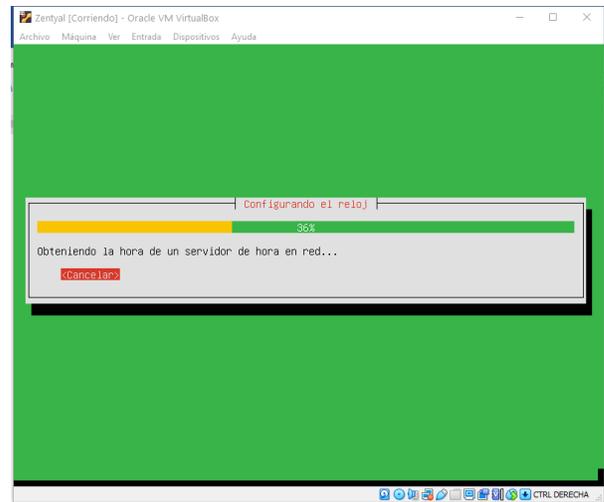


Figura 15 Configuración Automática Del Reloj Del Sistema. Fuente: Elaboración propia

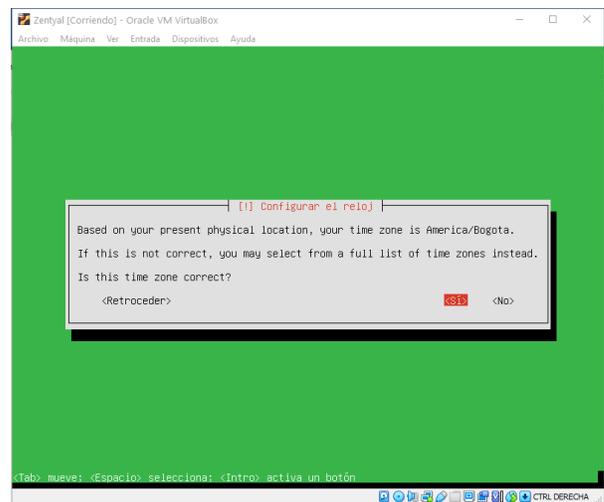


Figura 16 Ajuste Automática De La Zona Horaria.
Fuente: Elaboración propia.

Una vez realizado las configuraciones pertinentes se procede a instalar los paquetes necesarios para el sistema Zentyal.

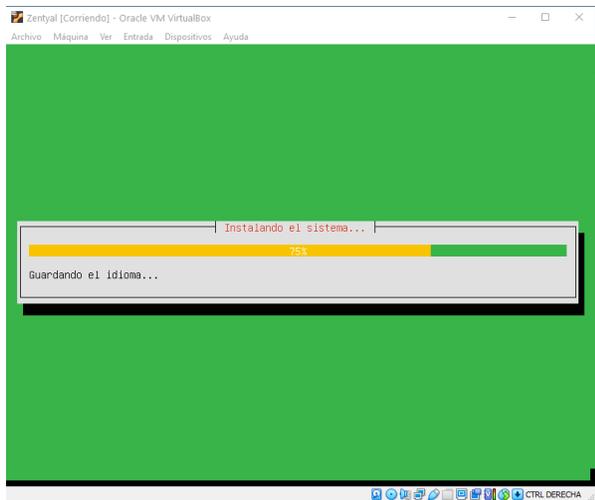


Figura 17 Instalación Del Sistema Zentyal.
Fuente: Elaboración propia

Por último, el asistente de instalación al terminar solicita reiniciar el sistema, pero primero debe expulsar la imagen usada para la instalación para el sistema arranque desde el disco en lugar de reiniciar la instalación.

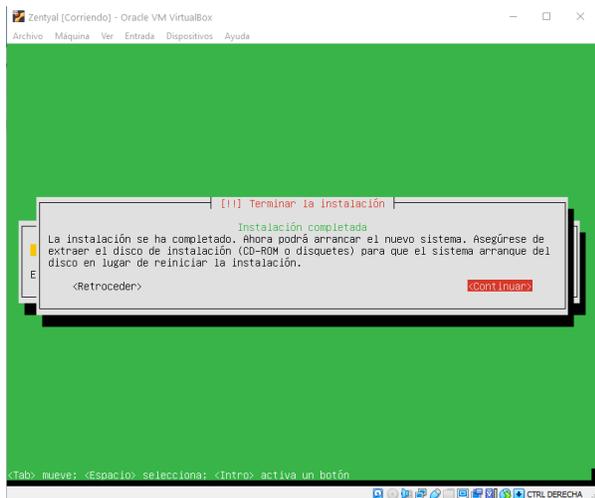


Figura 18 Terminación Del Proceso De Instalación.
Fuente: Elaboración propia

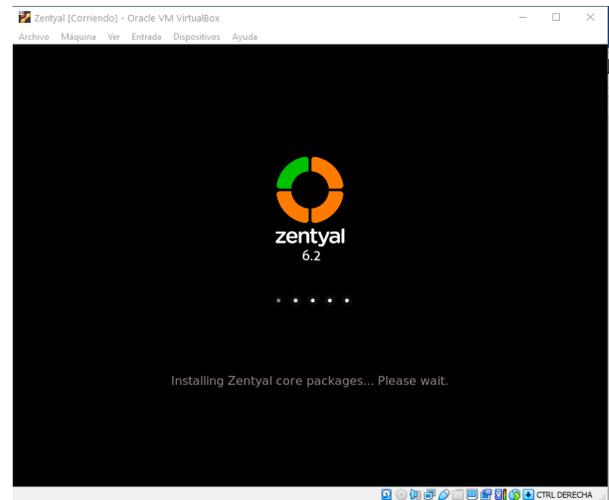


Figura 19 Inicio Se Sesión Del Sistema Zentyal 6.2.
Fuente: Elaboración propia

Al iniciar sesión se ejecuta automáticamente la aplicación web del Zentyal, pero al no tener los certificados SSL nos muestra que la pagina es inseguro, por este motivo accedemos a los ajustes avanzados y permitimos el acceso al sitio web.

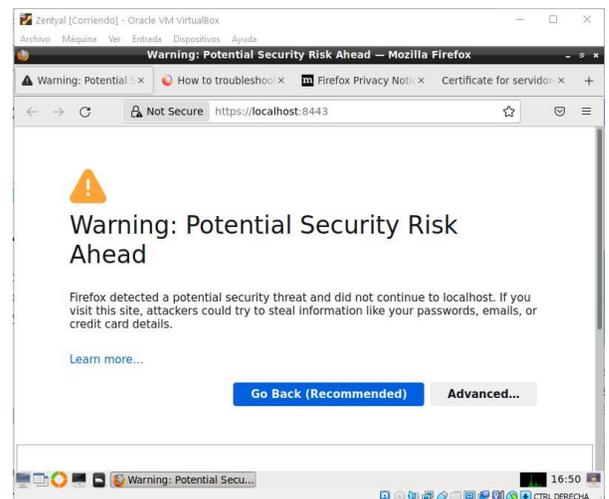


Figura 20 Permitir Acceso A La Aplicación Web Zentyal.
Fuente: Elaboración propia.

De esta manera podemos ingresar al panel de configuración y nos solicita autenticarnos con el usuario y contraseña configurados previamente.

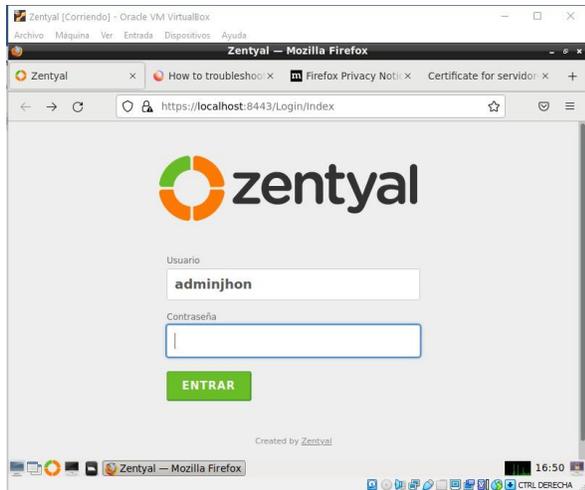


Figura 21 Autenticación Con Login Del Sistema.
Fuente: Elaboración propia.

Cuando se accede a la interfaz por primera vez aparecerá una pantalla de presentación mostrando el asistente de configuración inicial, desde este punto podemos realizar las diferentes configuraciones requeridas para los servicios de infraestructura de red.



Figura 22 Panel Configuración Inicial.
Fuente: Elaboración propia

4 TEMÁTICA 1 DHCP SERVER, DNS SERVERY CONTROLADOR DE DOMINIO

4.1 CONFIGURACIÓN INICIAL

Para la instalación de los servicios DHCP, DNS Server y Controlador de dominio, en el panel de gestión de software podemos seleccionar los paquetes de Zentyal a instalar.



Figura 23 Instalación De Paquetes.
Fuente: Elaboración propia.



Figura 24 Selección De Paquetes A Instalar.
Fuente: Elaboración propia.



Figura 25 Proceso De Instalación De Paquetes.
Fuente: Elaboración propia.

Al finalizar la instalación de paquetes, automáticamente aparecerá el asistente de configuración de las interfaces de red, para nuestra configuración de la máquina virtual tenemos dos interfaces de red, una será configurada para la conexión con la red WAN para establecer conectividad con internet y la segunda interface será para la conexión con la red interna o LAN.

De esta manera configuramos la interfaz eth0 (red WAN) como externa y la interfaz eth1 (red LAN) como interna. Por lo tanto, la red eth0 se establece con el método de resolución DHCP para el router del proveedor de internet administre las IP externas y nos establezca conexión de internet a través de una puerta de enlace establecida automáticamente por el router del proveedor de internet, y nuestra segunda interface eth1 se establece un método estático y se asigna una IP fija a esta interface el cual se deja 192.168.20.1/24.

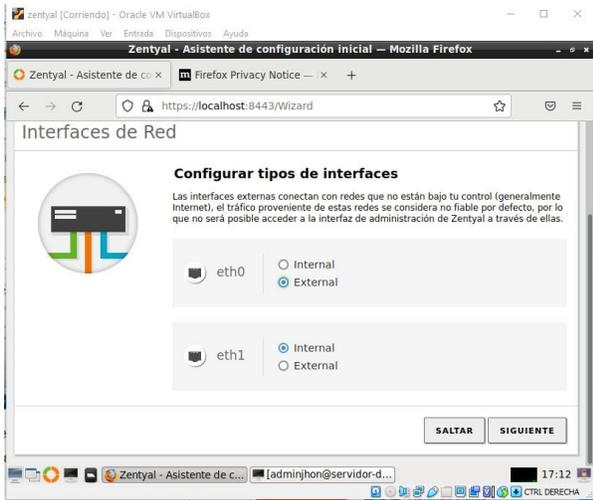


Figura 26 Configuración De Los Tipos De Interfaces De Red. Fuente: Elaboración propia.

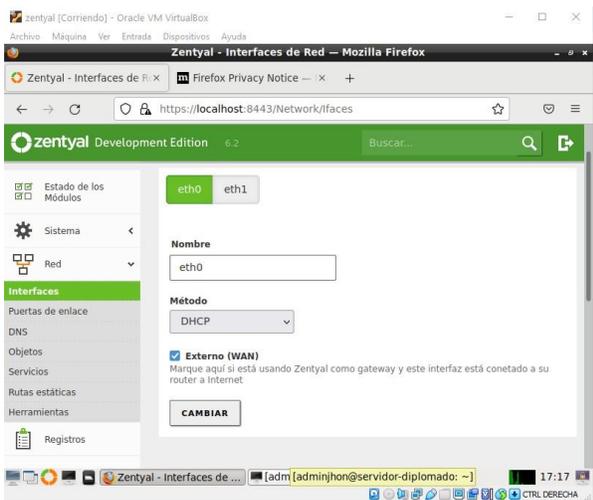


Figura 27 Configuración Interface Eth0. Fuente: Elaboración propia.

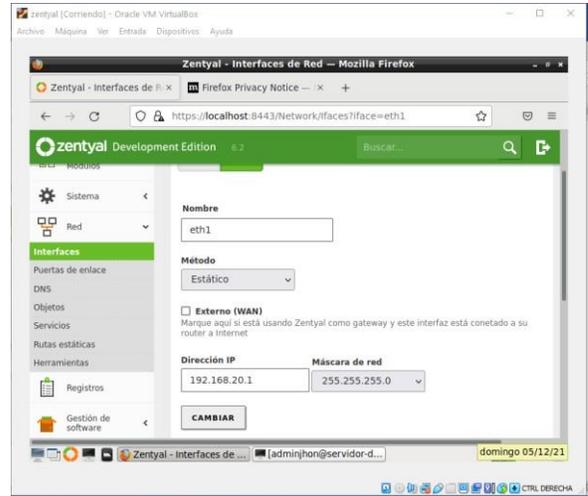


Figura 28 Configuración Interfaz Eth1. Fuente: Elaboración propia

Después de configurar las interfaces de red procedemos a validar por consola la IP que tomaron cada una de las interfaces, de esta manera para la interfaz 1 toma la IP que le asigna por DHCP el router del proveedor de internet y la interfaz 2 toma la IP que se asignó de forma estática. Por último, validamos si nuestro servidor está conectado al servicio de internet realizando un ping extendido a la IP del dominio de Google, comprobando que efectivamente tenemos conexión a internet.

Definida las interfaces de red, podemos realizar la configuración de los servicios de DHCP, DNS server y controlador de dominio.

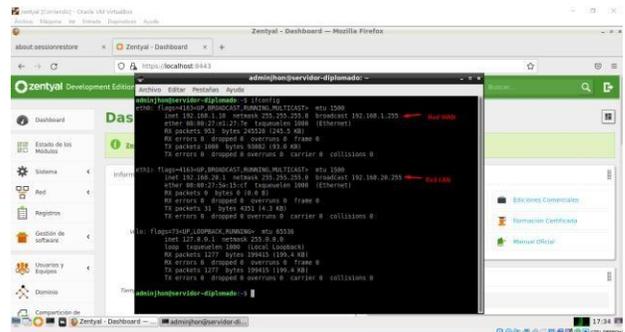


Figura 29 Verificación De La Interfaz De Red Por Consola. Fuente: Elaboración propia.

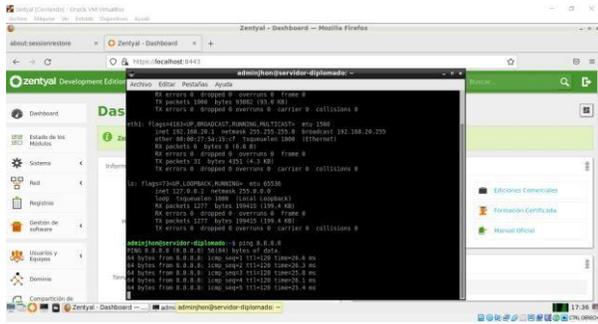


Figura 30 Verificación Conexión A Internet.
Fuente: Elaboración propia.

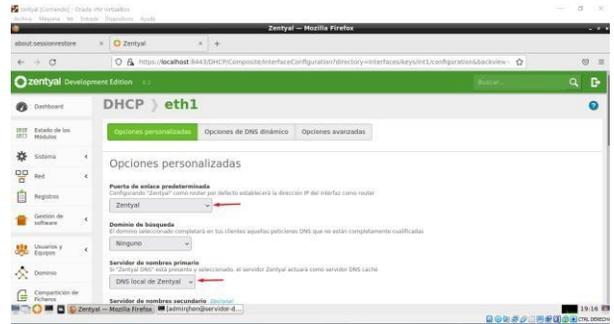


Figura 32 Opciones Personalizables DHCP.
Fuente: Elaboración propia

4.2 CONFIGURACION DHCP SERVER

En este paso procederemos a configurar el protocolo de configuración dinámica de IPs denominado DHCP, el cual proporcionara automáticamente a cada host un direccionamiento IP, mascara de subred, puerta de enlace y direccionamiento DNS.

Previamente en la configuración inicial se había instalado los paquetes requeridos para el servicio el DHCP, ahora se procede a configurarlo, al seleccionar el icono DHCP del panel de servicios nos muestra por defecto la interface de red que se usara para realizar la comunicación con los hosts unidos en una red LAN, de esta manera seleccionamos el icono de configuración para que se despliegue las opciones.



Figura 33 Opciones Personalizables Guardar Cambio.
Fuente: Elaboración propia.

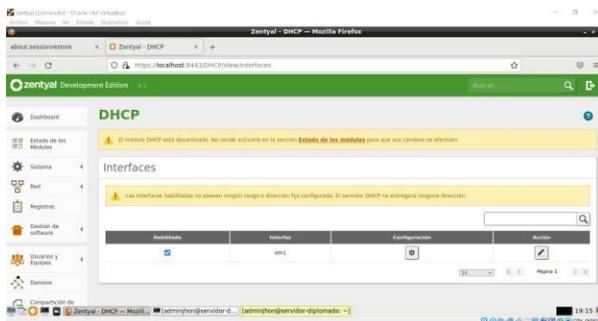


Figura 31 Panel De Configuración Del Servicio De DHCP. Fuente: Elaboración propia

En el panel de configuración, podemos personalizar las opciones de puerta de enlace, dominio de búsqueda, servidor DNS primario y secundarios, de esta manera solo agregamos la dirección IP del servidor DNS secundario y las demás opciones las dejamos con las opciones que muestra por defecto y guardamos cambios.

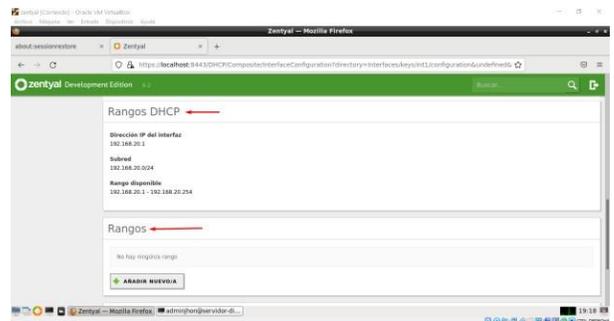


Figura 34 Rango De IP Disponibles.
Fuente: Elaboración propia

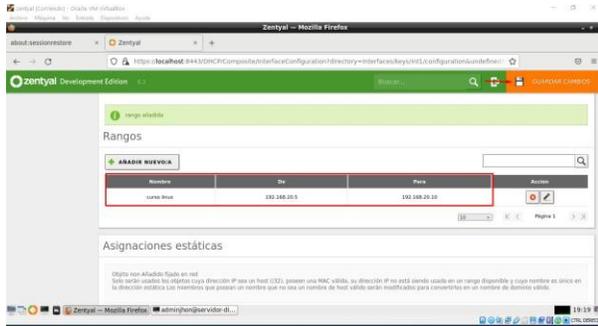


Figura 35 Configuración De Rango De IP.
Fuente: Elaboración propia

Para activar el servicio configurado nos dirigimos a la sección estado de los módulos y seleccionamos el servicio DHCP y activamos el servicio.

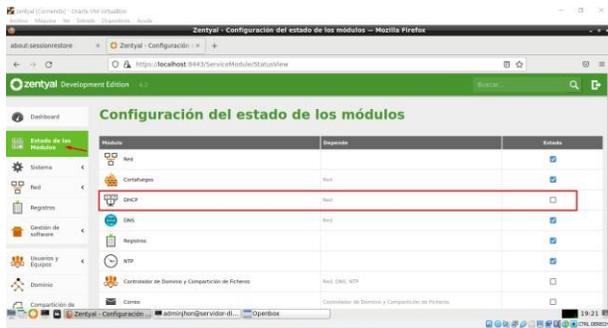


Figura 36 Seleccionar El Servicio A Activar.
Fuente: Elaboración propia

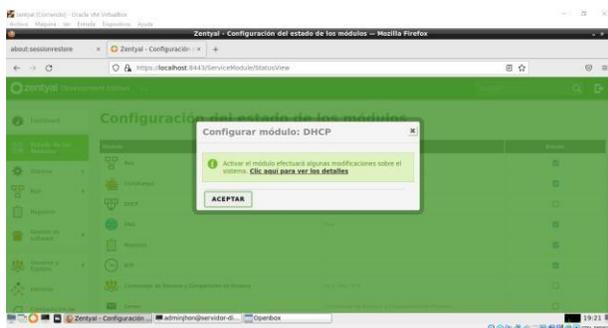


Figura 37 Activación Del Servicio DHCP.
Fuente: Elaboración propia

Después de activar el servicio DHCP validamos en el tablero principal "Dashboard" y verificamos el estado del servicio, el cual se encuentra en ejecución y no hay equipos host asociados en la lista de direcciones de IPs asignadas.

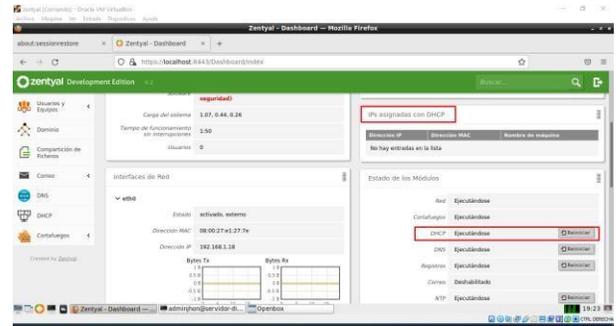


Figura 38 Verificación Activación Del Servicio.
Fuente: Elaboración propia

Ahora para realizar la prueba de asignación automática de direcciones IPs utilizamos una máquina virtual con un sistema operativo Ubuntu desktop versiono 20.04 y configuramos la tarjeta de red en modo red interna para que sea visible dentro del segmento de red del servidor Zentyal.

Al iniciar sesión con el host cliente, validamos la IP asignada por el servicio DHCP usando el comando ifconfig desde la consola de Ubuntu desktop. De esta forma comprobamos que se está asignado correctamente la IP 192.168.20.5, además verificamos que el equipo host tiene conexión a internet haciendo ping a la IP del dominio de Google y adicional ingresamos a una página web evidenciando que se está conectando correctamente.

Por último ingresamos al tablero de monitoreo del servidor Zentyal y validamos que la IP asignada al host encendido.

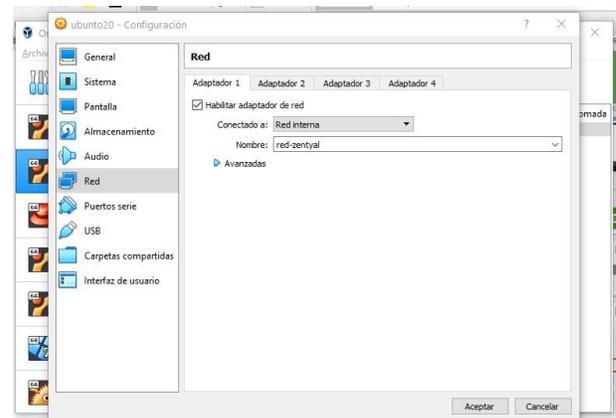


Figura 39 Configuración De La Tarjeta De Red Del Equipo Host. Fuente: Elaboración propia.

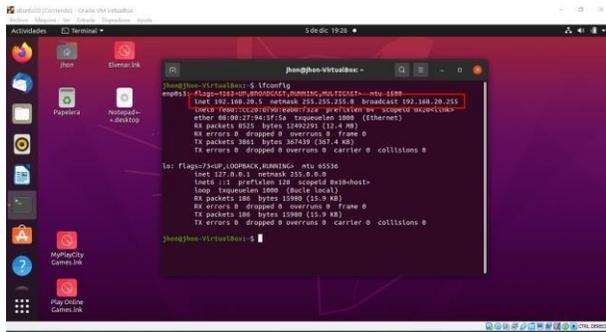


Figura 40 Verificación De Asignación De IP Host Cliente.
Fuente: Elaboración propia.

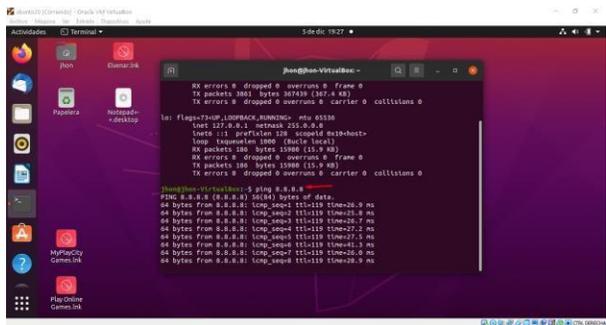


Figura 41 Verificación Conexión Internet Host Cliente.
Fuente: Elaboración propia

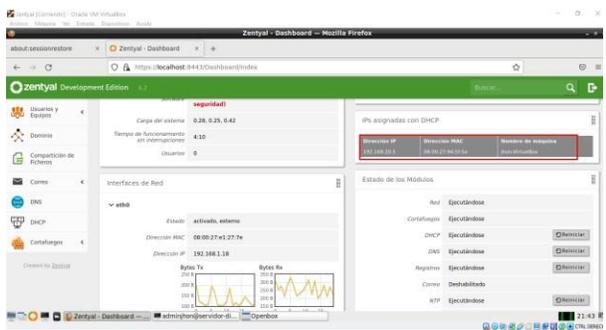


Figura 42 Monitor De IP Asignadas.
Fuente: Elaboración propia.

4.3 CONFIGURACION SERVIDO DNS

El sistema de resolución de nombres de dominio dentro de la red local nos permite responder a las peticiones de todos los equipos o dispositivos conectados a una red, convirtiendo estas secuencias numéricas en nombres de dominio entendibles.

Teniendo en cuenta la documentación de configuración de Zentyal nos indica que, “El módulo de servidor de DNS de Zentyal siempre funciona como servidor DNS *caché* para las redes marcadas como

internas en Zentyal, así que, si solamente queremos que nuestro servidor realice *caché* de las consultas DNS, bastará con habilitar el módulo”.

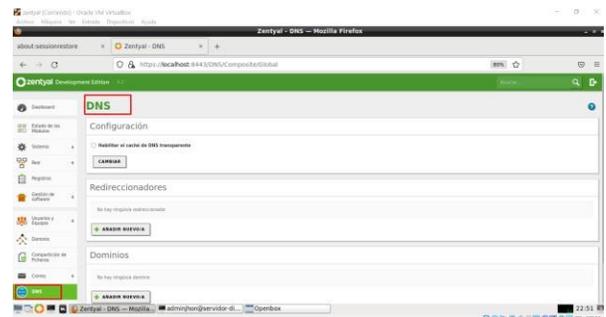


Figura 43 Panel De Configuración DNS.
Fuente: Elaboración propia

De esta manera procedemos a activar los servicios en la sección del módulo de configuración de estados, seleccionamos el servicio DNS, guardamos cambios y con esta operación queda activo el servicio. Después procedemos a configurar los DNS primario y secundario para la conexión con servicio de internet usando el direccionamiento DNS local del servidor Zentyal, de esta forma los equipos hosts que se le asigne el direccionamiento IP también le asigne de forma automática el direccionamiento DNS que estarán apuntado a la IP de la puerta de enlace del servidor Zentyal, de esta forma los equipos cliente pueden navegar por internet sin tener que realizar alguna configuración adicional en las tarjetas de red de cada equipo.



Figura 44 Activación del Servicio DNS.
Fuente: Elaboración propia.

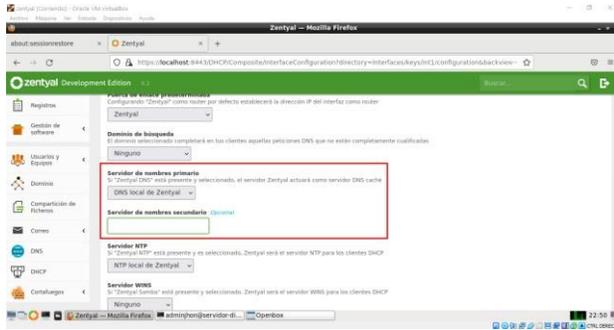


Figura 45 Configuración De DNS Primario y Secundarios.

Fuente: Elaboración propia.

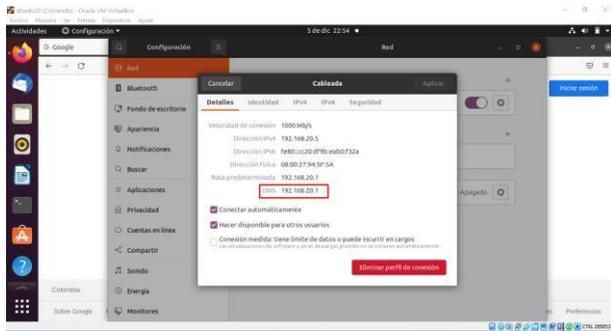


Figura 46 Verificación De La Asignación DNS Al Equipo Cliente. Fuente: Elaboración propia.

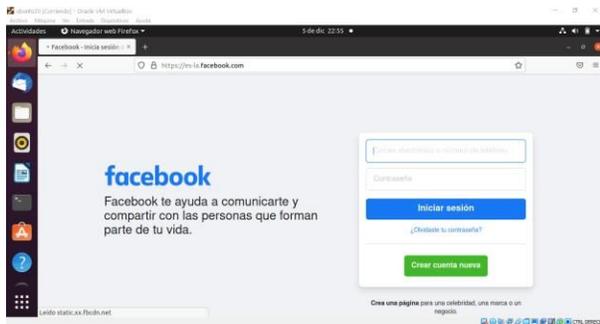


Figura 47 Verificación Navegación Internet. Fuente: Elaboración propia.

4.4 CONFIGURACION DE CONTROLADOR DE DOMINIO

Zentyal nos permite configurar un controlador de dominio el cual responde a las solicitudes de autenticación de seguridad a los equipos agregados al dominio configurado previamente, permitiendo administrar salvaguardas, permisos y otros protocolos de acceso de forma remota en cada dispositivo.

El controlador de dominio es la pieza central del servicio Windows Active Directory, pero también se

puede usar para conectar equipos con plataforma Linux usando el protocolo LDAP, utilizando una aplicación intermedia se puede acceder a los servicios de directorio remoto.

Pero antes de unir los equipos al dominio debemos instalar los paquetes para el servicio de domain controller and file sharing, instalamos el paquete del servicio que se encuentra en el menú de gestión de software y en el apartado de componentes de Zentyal encontramos los paquetes para instalar del controlador de dominio, después de instalado el modulo se habilitan dos iconos en el menú de módulos, el primero se llama usuario y equipo, segundo llamado dominio, de esta forma queda habilitado los módulos para su configuración.

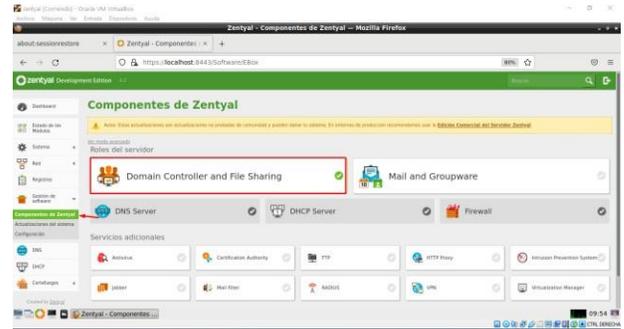


Figura 48 Instalación De Paquetes Servidor De Dominio. Fuente: Elaboración propia.

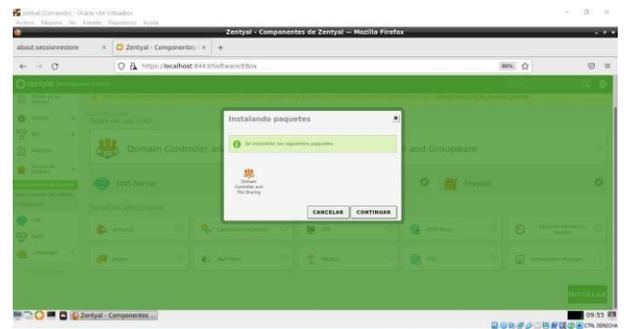


Figura 49 Confirmación De Paquetes A Instalar Servidor Dominio. Fuente. Elaboración propia.

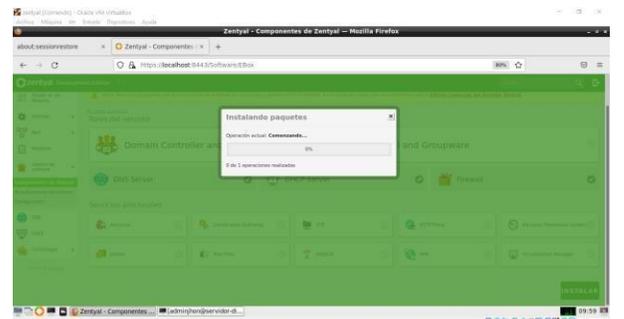


Figura 50 Instalación De Paquetes Servidor Dominio. Fuente: Elaboración propia

Antes de configurar el servidor de dominio, nos dirigimos al módulo de sistemas la opción general, en este apartado encontramos la configuración general del sistema Zentyal donde podemos visualizar las cuentas administrador del Zentyal, el idioma, puerto TCP de la interfaz de administración y por ultimo encontramos el nombre de la máquina y dominio, en esta sección procedemos a personalizar el nombre de la máquina y nombre del dominio que tendrá el servidor Zentyal. Que para nuestro ejemplo el nombre de la maquina será *diplomado* y el dominio del servidor será *cursolinux.edu*.



Figura 51 Acceso A La Configuración General Del Sistema. Fuente: Elaboración propia.

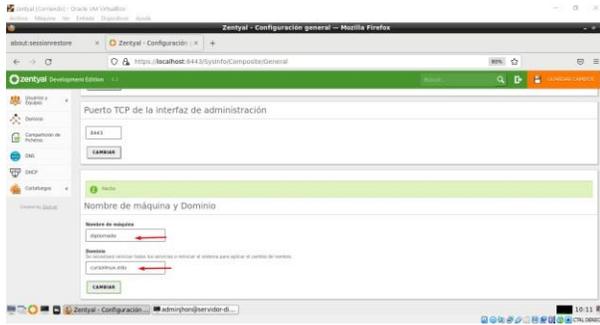


Figura 52 Personalización Del Nombre De Maquina y Del Dominio. Fuente: Elaboración propia.

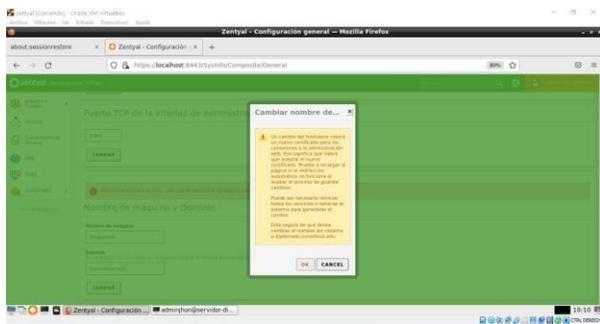


Figura 53 Confirmación Cambio Del Nombre De La Máquina y Dominio. Fuente: Elaboración propia

Una vez guardados los cambios del nombre de la máquina y del dominio procedemos a reiniciaremos el

servidor antes de activar el módulo. Al acceder nuevamente al sistema de configuración del Zentyal, accedemos al módulo dominio y validamos que el reino concuerde con el nombre de dominio que se configuro previamente, también seleccionamos la función del servidor que para este caso es controlador de dominio y por último dejamos por defecto el nombre de dominio NetBios que nos muestra en pantalla.

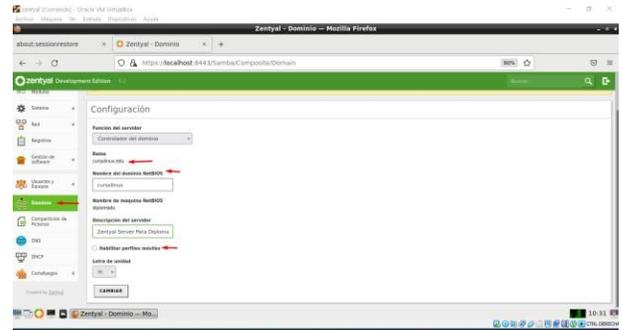


Figura 54 Configuración Dominio. Fuente: Elaboración propia.

La opción de perfiles móviles, permite que los usuarios autenticados guarden información y configuraciones en el servidor de manera automática, de esta manera el perfil almacenado en el servidor se carga localmente y cuando cierra su sesión el perfil remoto se sincroniza con el equipo local. Esta sincronización de perfil aumenta el tiempo de inicio de sesión para los usuarios creados y espacio de almacenamiento en disco duro en el servido, por esta razón esta opción se recomienda dejarla deshabilitada.



Figura 55 Guardar Cambio En La Configuración De Dominio. Fuente: Elaboración propia.

Después de realizar el proceso de configuración del dominio procedemos a activar el servicio en la sección estado de los módulos, de esta manera seleccionamos la opción controladora de dominio, para que el servicio se active correctamente depende que los servicios de red y DNS este configurados y activos previamente.



Figura 56. Activación Del Servicio Controlador De Dominio. Fuente: Elaboración propia.

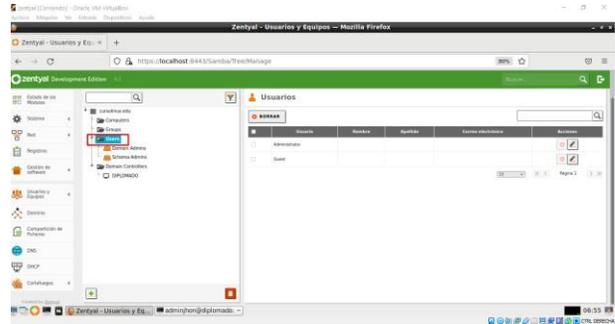


Figura 59. Entorno De Configuración De Usuarios y Equipos. Fuente: Elaboración propia.

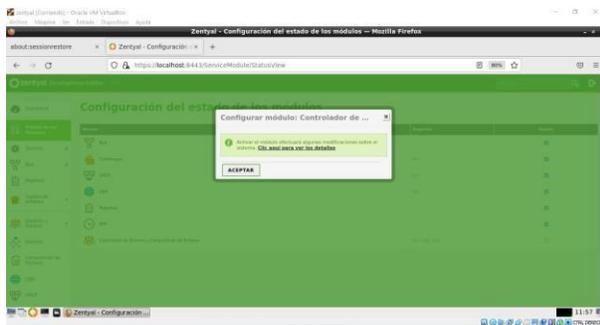


Figura 57. Controlador De Dominio Activado Correctamente. Fuente: Elaboración propia.

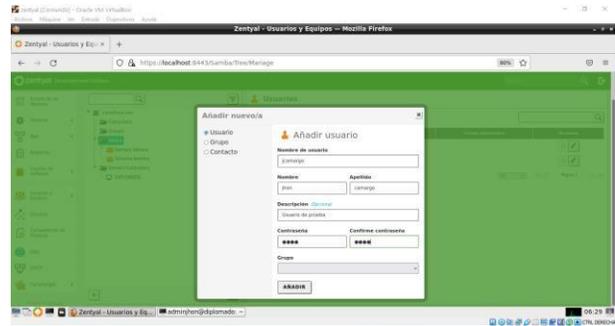


Figura 60. Proceso De Creación De Un Usuario. Fuente: Elaboración propia.

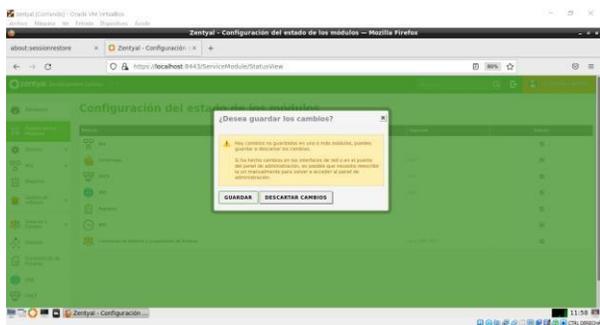


Figura 58. Guardar Cambios Configuración De Dominio. Fuente: Elaboración propia

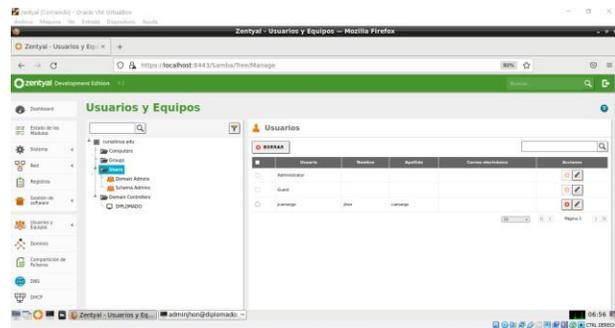


Figura 61. Usuario Creada.

Ahora se ingresa al módulo usuario y equipos donde podemos visualizar nuestro controlador de dominio configurado, los contenedores para crear los usuarios, grupos de administración de usuario y computadores unidos al dominio. De esta forma procedemos a crear un usuario que tendrá el perfil de administrador, el cual será usado para unir los equipos clientes al dominio.

Con la configuración inicial del servidor de dominio procedemos a unir un host cliente que tendrá la distribución Ubuntu Desktop 20.04, para realizar este procedimiento la máquina virtual de Ubuntu estará enlazada por la red interna del servidor Zentyal, el cual le asignará de forma automática un direccionamiento IP y el direccionamiento del servidor DNS.

Para validar que nuestro equipo tenga conectividad con el servidor Zentyal, realizamos un ping a la dirección IP a la puerta de enlace del servidor DHCP y después usando el comando nslookup validamos que nuestro servidor DNS este resolviendo correctamente el nombre de dominio y las IPs configuradas.

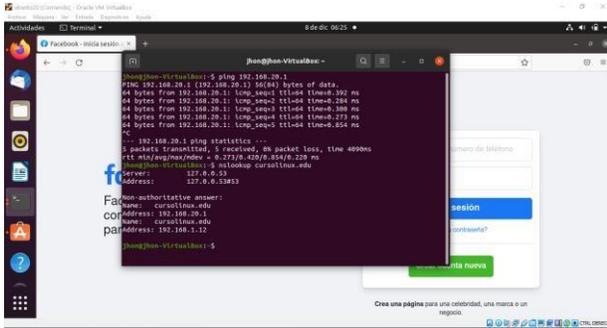


Figura 62 Verificación De Conectividad Con El Servidor Zentyal. Fuente: Elaboración propia.

Como se indicaba previamente, para unir una host en Ubuntu al dominio se debe usar el protocolo LDAP, para realizar esta configuración debemos usar dos herramientas, la primera de ellas es la herramienta para el control remoto y transferencia de datos entre las estaciones de computo usando un entorno de red LAN llamada openssh-server. Para la instalación de esta herramienta usamos el comando:

\$ sudo apt install openssh-server

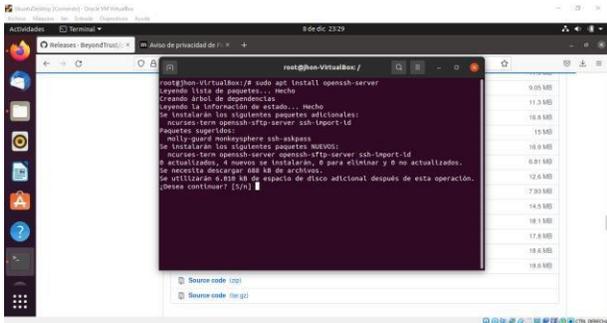


Figura 63 Instalación De La Herramienta Openssh-server. Fuente: Elaboración propia.

La segunda herramienta para instalar se llama pbis-open el cual es un programa que permite a una máquina UNIX/Linux unirse a un dominio y autenticarnos en esa máquina con nuestras credenciales, dicha herramienta se descarga a través de la página <https://github.com/BeyondTrust/pbis-open/releases>. Posterior al descargue del paquete habilitamos los permisos de lectura, escritura y ejecución sobre el archivo descargado, y por último ejecutamos el paquete descargado de la siguiente forma:

\$. /pbis-open-8.7.1.linux.x86_64.deb.sh

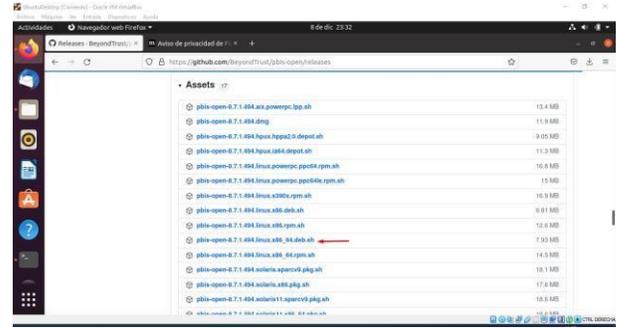


Figura 64 Descargue De Paquetes Pbis-Open. Fuente: Elaboración propia.

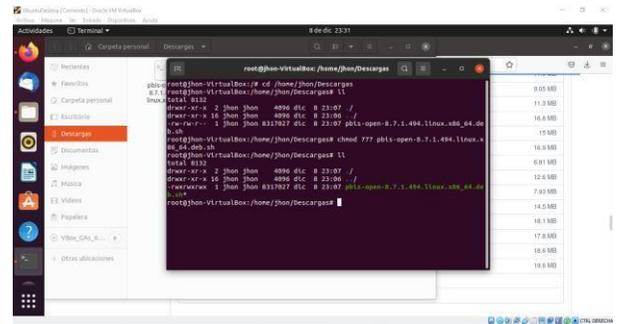


Figura 65 Habilitación De Permisos Lectura, Escritura y Ejecución. Fuente: Elaboración propia.

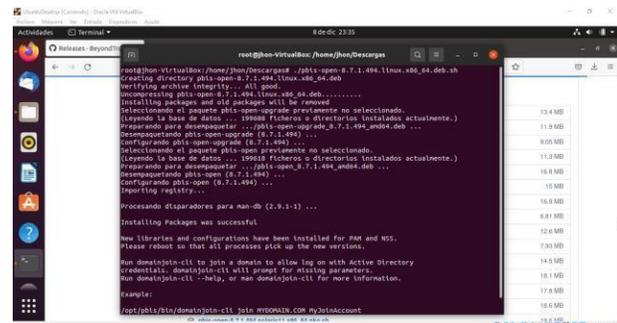


Figura 66 Desempaquetar e Instalación De Paquetes Pbis_Open. Fuente: Elaboración propia.

Instalada nuestras dos herramientas procedimos a desplazarnos el directorio bin de la aplicación pbis que se encuentra en la ruta /opt/pbis/bin.

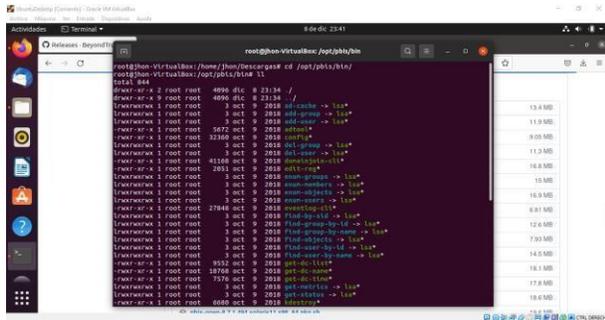


Figura 67 Cambio Hacia El Directorio Bin De La Herramienta Pbis. Fuente: Elaboración propia.

Posicionados en el directorio Bin procedemos a ejecutar el siguiente comando para unir al servidor de dominio, el cual se especifica el nombre de dominio y el usuario que tiene los permisos de administrador y nos permitirá autenticarnos en el servidor de dominio, de esta manera se puede unir el equipo de cómputo al dominio de Zentyal, al finalizar el proceso de autenticación nos muestra un mensaje indicando que el proceso se realizó correctamente y se recomienda reiniciar la máquina virtual.

\$ domainjoin-cli join cursolinux.edu jcamargo@cursolinux.edu



Figura 68 Unir Equipo De Computo Al Servidor De Dominio. Fuente: Elaboración propia.

Antes de realizar el proceso de reinicio, debemos modificar el archivo 50-ubuntu.conf, el cual nos permitirá iniciar sesión de forma manual ingresando la siguiente línea de comando `greeter-show-manual-login=true`, de esta forma se habilita el menú de logueo de forma manual y poder especificar el dominio y usuario de sesión de dominio.

\$ gedit /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf

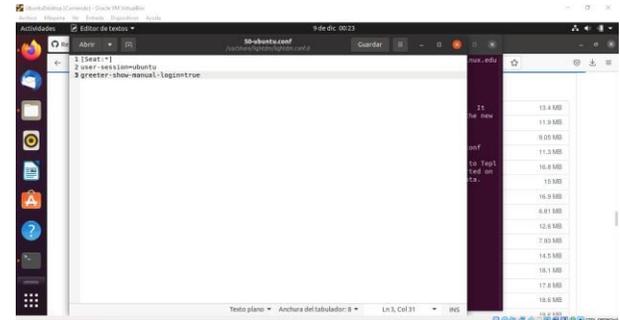


Figura 69 Edición Del Archivo 50-ubuntu.conf. Fuente: Elaboración propia

Por ultimo establecemos shell predeterminado para la aplicación pbis y reiniciamos el host cliente.

\$ /opt/pbis/bin/config LoginShellTemplate /bin/bash

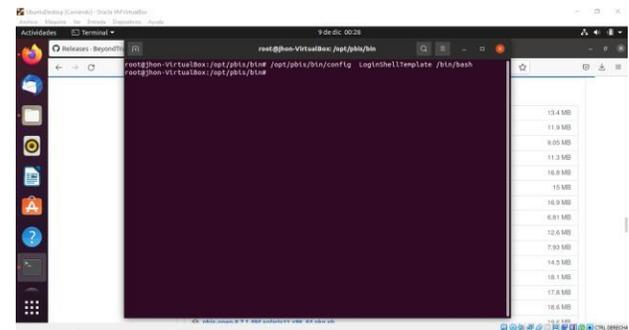


Figura 70 Establecer El Shell Predeterminado. Fuente: Elaboración propia

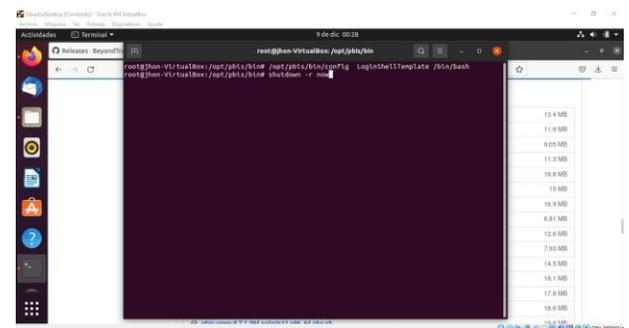


Figura 71 Reinicio Del Sistema Operativo. Fuente: Elaboración propia.

Al cargar nuevamente el sistema operativo, podemos visualizar en el panel de usuarios y equipos, en el contenedor computers que el nombre de nuestro host unido al dominio.

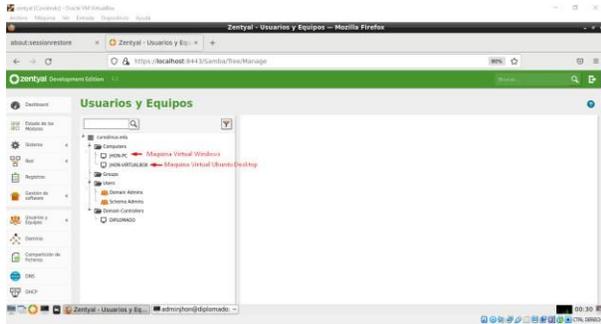


Figura 72 Lista De Host Unidos Al Dominio.
Fuente: Elaboración propia

Para validar que nuestro servidor dominio está recibiendo las peticiones de inicio de sesión correctamente, nos autenticamos con usuario y contraseña creados previamente, de esta forma comprobamos que nuestro dominio está gestionando correctamente la solicitud de bloqueo y creación de sesión en el equipo host.

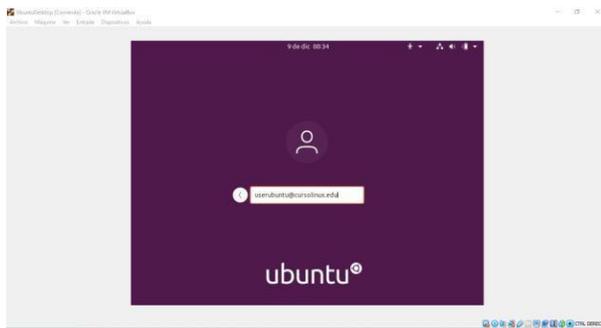


Figura 73 Inicio De Sesión.
Fuente: Elaboración propia.



Figura 74 Inicio De Sesión.
Fuente: Elaboración propia.

Una última validación que se puede realizar es usando el comando whoami en la consola de terminal, para validar que el nombre de dominio y el usuario que están activos en la sesión actual, de esta manera determinados que el equipo host está unido correctamente al dominio de Zentyal.



Figura 75 Verificación De Usuario De Dominio.
Fuente: Elaboración propia.

5 TEMÁTICA 2: PROXY NO TRANSPARENTE

Para la temática proxy no transparente, los módulos a utilizar en el servidor del Zentyal, son los módulos de DHCP server, HTTP Proxy. Una vez seleccionado los módulos

El sistema nos muestra los módulos seleccionados y pregunta si deseamos instalarlos, se le da en instalar.

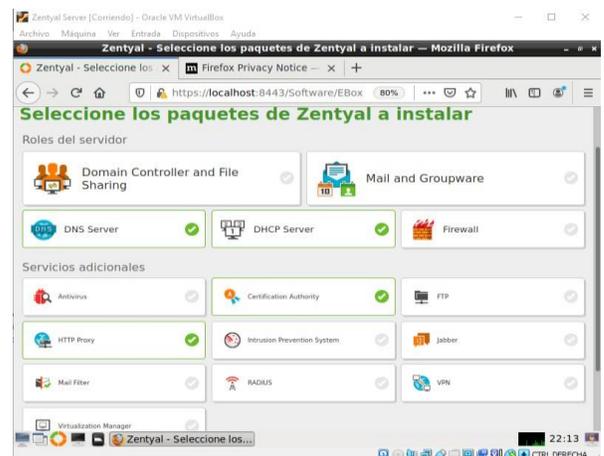


Figura 75. Módulos Para Utilizar Para El Proxy No Transparente. Fuente: Elaboración propia.

Muestra los paquetes seleccionados a instalar, y dar en continuar.

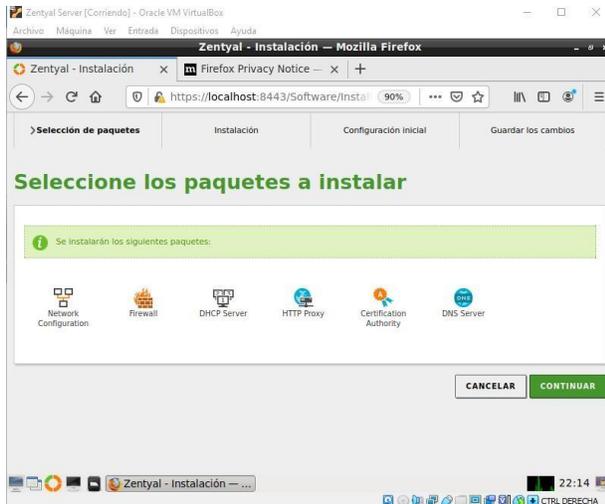


Figura 76 Instalar Paquetes.
Fuente: Elaboración propia.

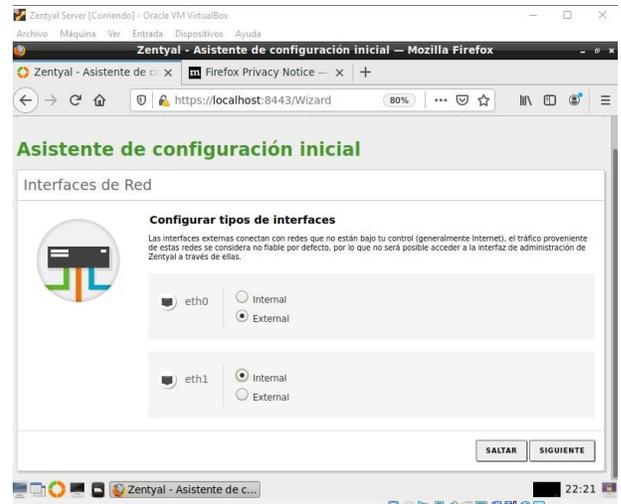


Figura 78 Configuración De Interfaz De Red
Fuente: Elaboración propia.

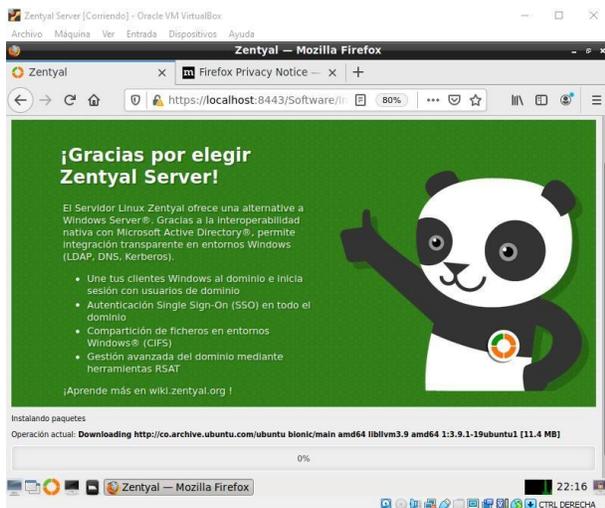


Figura 77 Instalación De Paquetes.
Fuente: Elaboración propia.

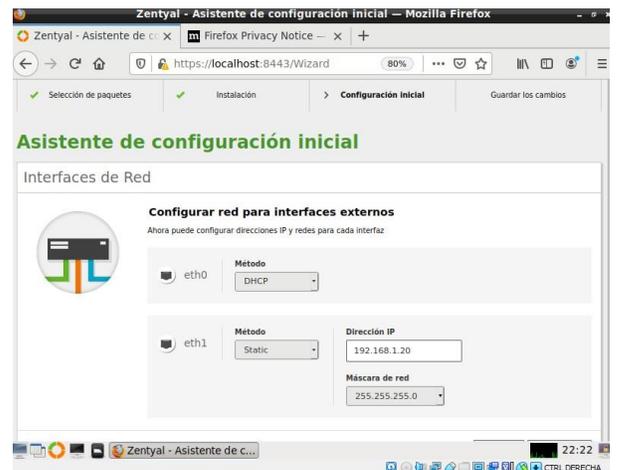


Figura 79 Configuración De Interfaz De Red.
Fuente: Elaboración propia.

Una vez instalados los módulos inicia el proceso de configuración de las tarjetas de red que fueron creadas donde el eth0 y eth1 será externo y DHCP y la eth1 será la red interna con una IP estática.



Figura 80 Instalación Completa De Paquetes.
Fuente: Elaboración propia.

Verificamos que la configuración de la red eth0 y eth1 estén correcta.

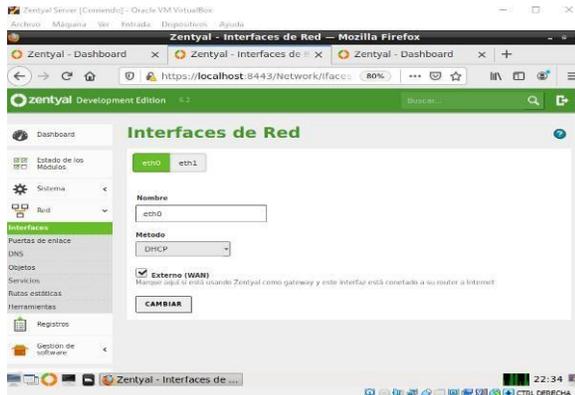


Figura 81 Configuración Interfaz Eth0.
Fuente: Elaboración propia.

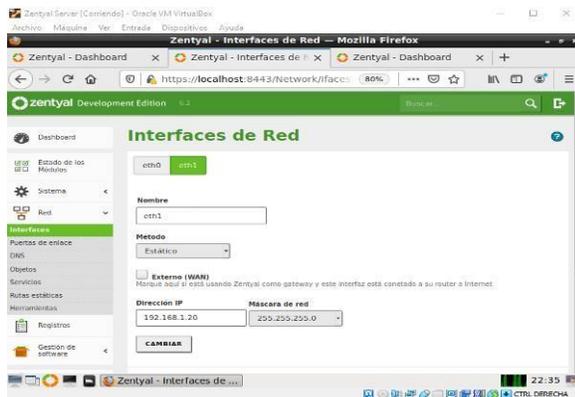


Figura 82 Configuración Interfaz Eth1.
Fuente: Elaboración propia.

Agregar los rangos de ip para que nuestra maquina Ubuntu tome alguno de estos rangos y se evidencie la conexión entre el Zentyal y el Ubuntu. El rango asignado es de 192.168.1.30 a 192.168.1.50.

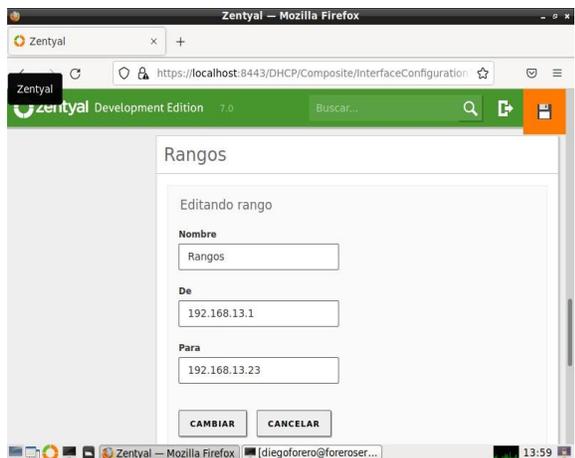


Figura 83 Configurar El DHCP Para Asignar Rangos De IP A Los Clientes. Fuente: Elaboración propia.

Al agregar los rangos el zentyal reconoce al Ubuntu dentro de la red interna con ip dentro del rango que se asignó, nos muestra la ip del Ubuntu, dirección MAC y el nombre de la máquina.

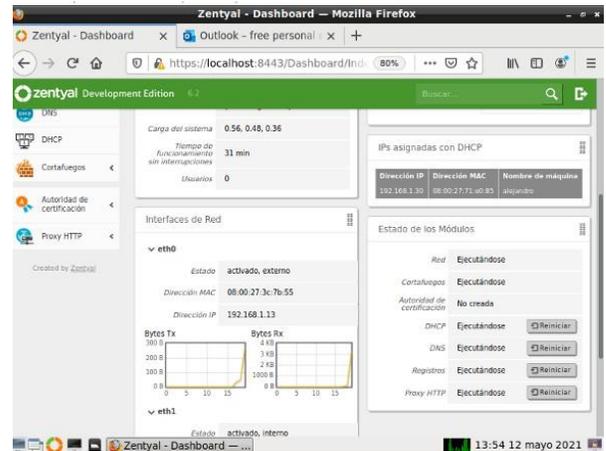


Figura 84 Reconocimiento De La Ip Del Ubuntu.
Fuente: Elaboración propia.

Configuración del zentyal para bloquear los servicios desde el puerto 1230, inicia creando un objeto con la ip de la máquina de Ubuntu.

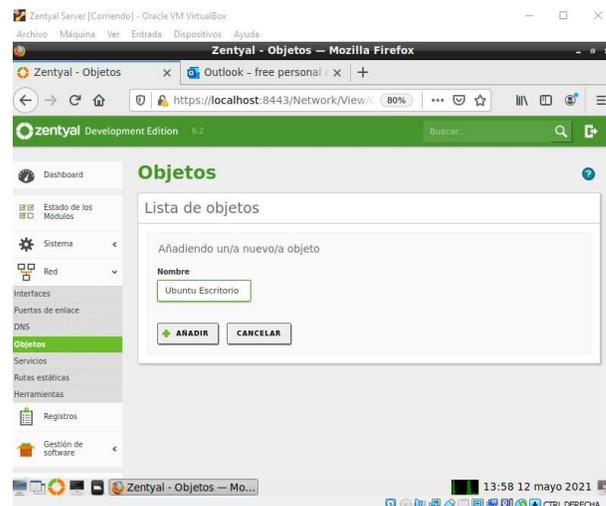


Figura 85 Crear El Objeto A Bloquear Los Servicios.
Fuente: Elaboración propia.

Configurar el módulo de proxy HTTP donde se coloca el puerto 1230, con base en lo que dice la guía, para el proxy no transparente.

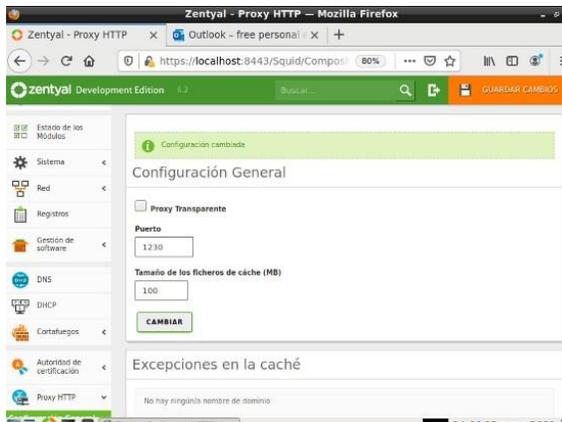


Figura 86 Configuración del proxy HTTP.
Fuente: Elaboración propia.

Configurar las reglas de acceso en el módulo HTTP proxy, por el puerto 1230 denegando los servicios al objeto creado el cual tiene la dirección IP del Ubuntu desktop.

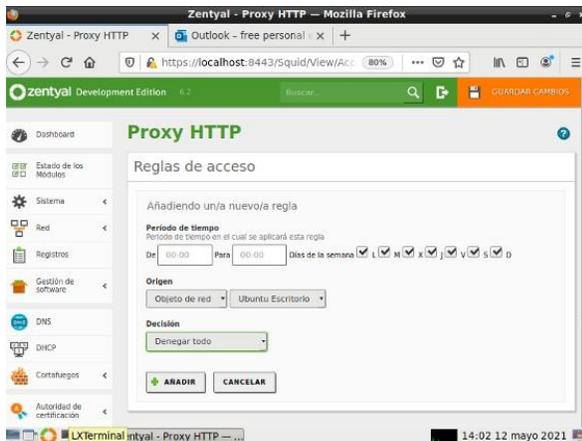


Figura 87 Configuración De Las Reglas De Acceso Por El Puerto 1230. Fuente: Elaboración propia.

Realizar el proceso de activación del proxy en el navegador de Ubuntu colocando la ip estática de la red eth1 192.168.1.20 y colocando el puerto 1230. Recargar la página del navegador.

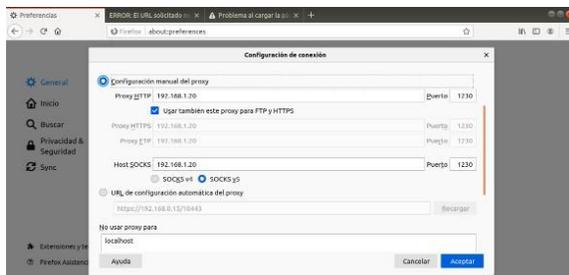


Figura 88 Configuración Del Proxy En El Navegador Del Cliente. Fuente: Elaboración propia

Después de recargar la página muestra el mensaje de restricción por el servidor Zentyal.



Figura 89 Bloqueo por parte del servidor Zentyal.
Fuente: Elaboración propia.

6 TEMATICA 3 CORTAFUEGOS

Para configuración del servicio de cortafuegos seleccionamos el apartado de Gestión de software y Componentes de Zentyal, seguidamente marcamos la opción de firewall junto con Network Configuration y damos clic en el botón de Instalar.

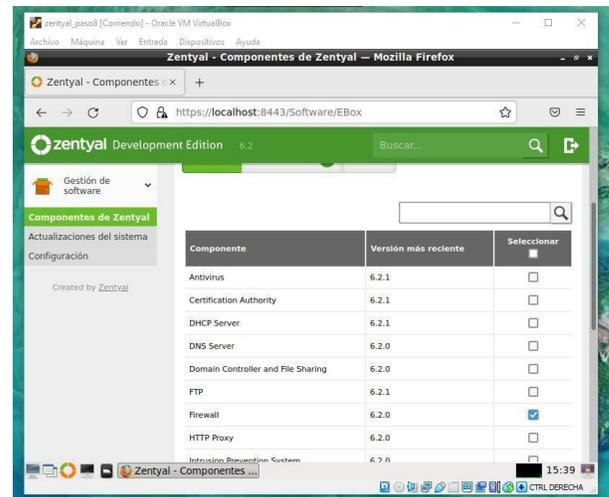


Figura 90 Instalación De Paquetes Firewall.
Fuente: Elaboración propia.

Vemos que el sistema nos solicita confirmar la acción y damos clic en Continuar.

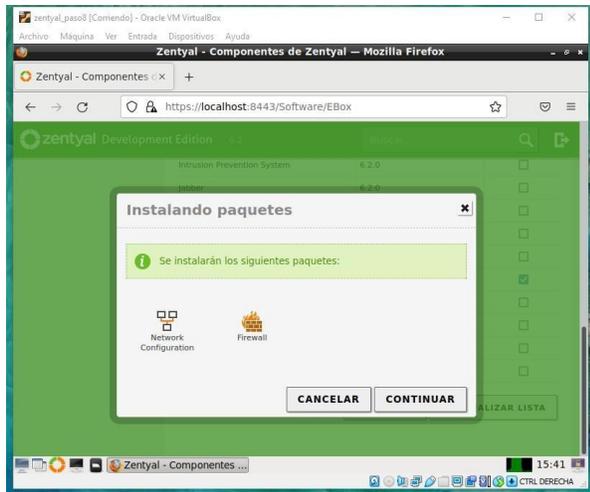


Figura 91 Verificación De Instalación De Paquetes.
Fuente: Elaboración propia.

Para terminar, configuramos la interfaz como interna.



Figura 92 Asistente De Configuración Interfaz Interna.
Fuente: Elaboración propia.

Luego se configura método de la interfaz de red y se elige que resuelva el direccionamiento de IPs usando el protocolo DHCP.

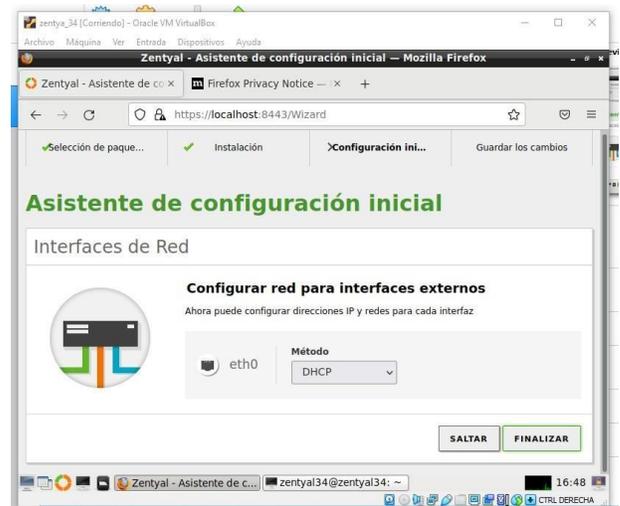


Figura 93 Configuración Del Método De Resolución De IPs.
Fuente: Elaboración propia.

Como vemos la instalación de los paquetes ha sido exitosa y podemos a su vez hacer ping hacia el servidor desde la máquina Windows base.

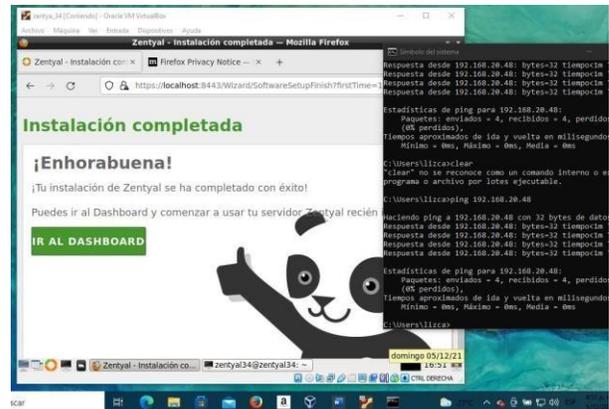


Figura 94 Verificación Conectividad Con Servidor Zentyal.
Fuente: Elaboración propia.

De vuelta en el dashboard de la herramienta Zentyal, vamos a la pestaña de registros, seleccionamos la opción de Configurar los registros y marcamos las dos opciones disponibles.

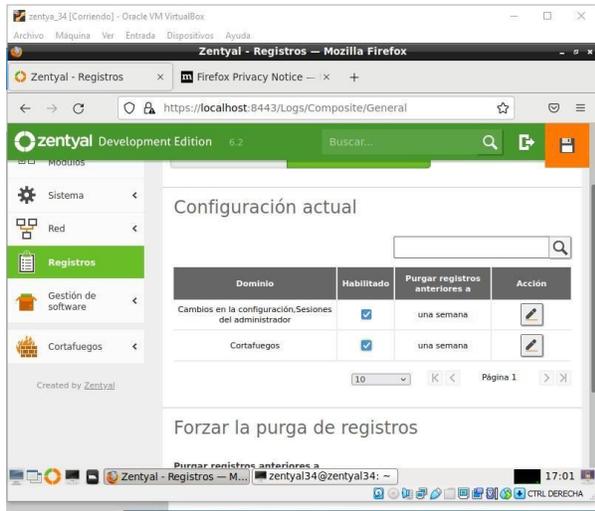


Figura 95 Configuración De Registros.
Fuente: Elaboración propia.

Seguidamente vamos a Red, y en el apartado de interfaces chequemos la opción de externo WAN.

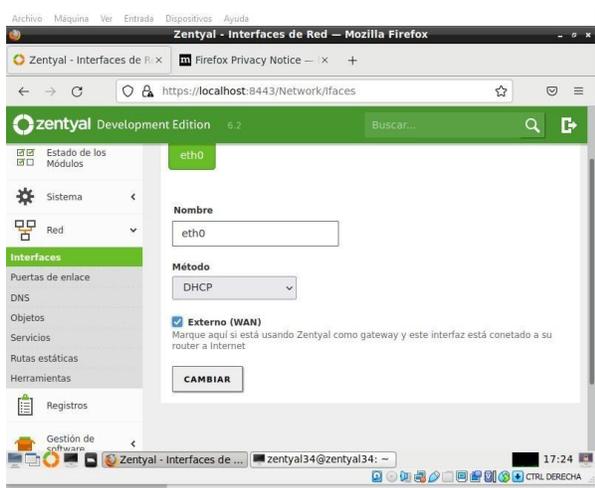


Figura 96 Configuración De La Interfaz Como Gateway.
Fuente: Elaboración propia.

Seguidamente iniciamos un cliente, en este caso se utiliza una máquina virtual configurada con una distribución de Ubuntu Desktop, hacemos ping hacia el servidor para validar conectividad con el servidor Zentyal y de esta forma podemos conectarnos con el entorno gráfico del zentyal desde el navegador filezilla.

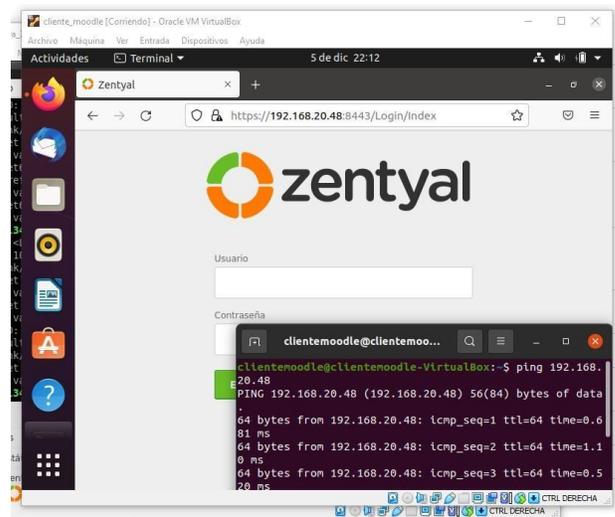


Figura 97 Conexión Herramienta Zentyal Desde Ubuntu Desktop.
Fuente: Elaboración propia.

Procedemos a acceder al apartado de Red y Servicios en donde se crea un nuevo servicio.

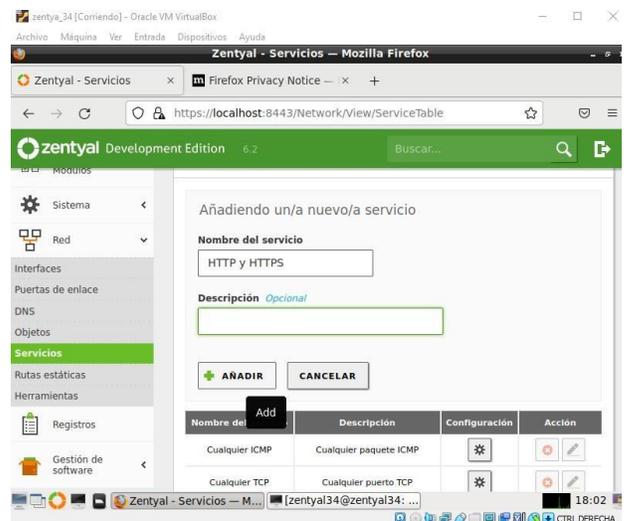


Figura 98 Creación De Nuevo Servicios.
Fuente: Elaboración propia.

Después de creados lo servicios de HTTP y HTTPS, procedemos a configurarlos.

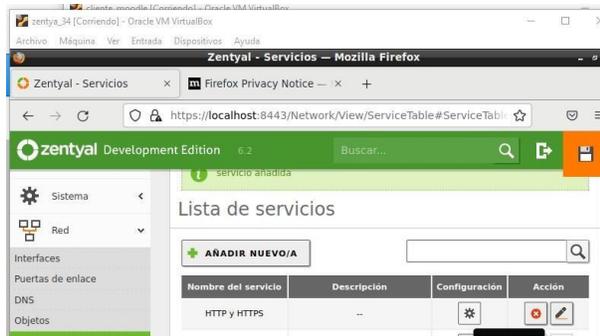


Figura 99 Configuración De Los Servicio HTTP y HTTPS
Fuente: Elaboración propia.

Dentro de su configuración añadimos los siguientes protocolos, esto nos permitirá administra el cortafuegos por medio de protocolos TCP y UDP al tiempo.

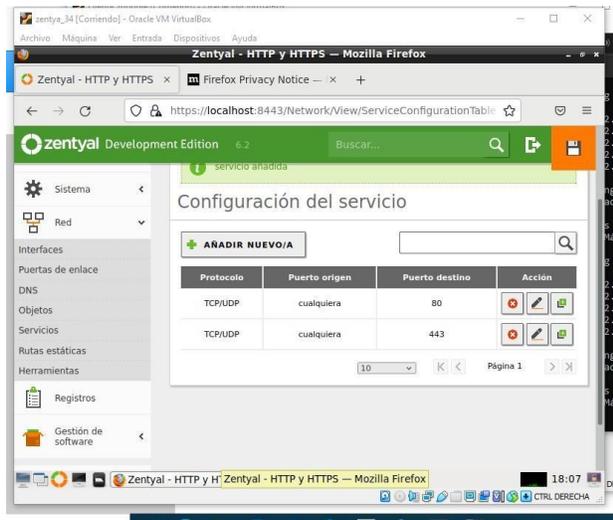


Figura 100 Configuración De Protocolos TCP/UDP.
Fuente: Elaboración propia.

Ahora se accede al apartado de cortafuegos y filtrado de paquetes en donde se tienen diferentes secciones con reglas de filtrado.

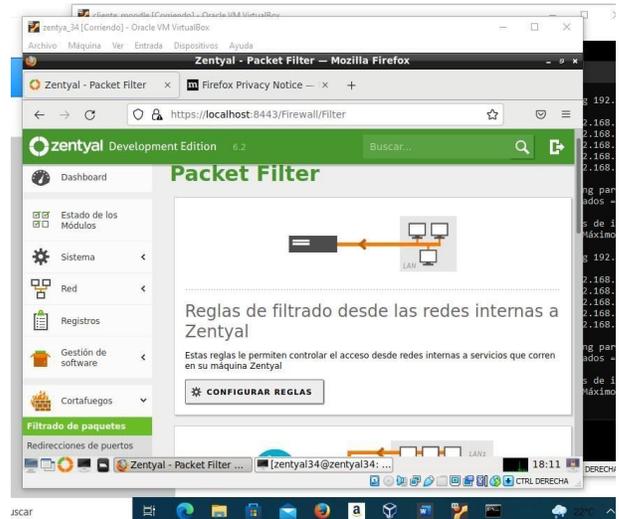


Figura 101 Configuración De Paquetes De Filtrado.
Fuente: Elaboración propia.

Seleccionamos el apartado de Reglas de filtrado para las redes internas.

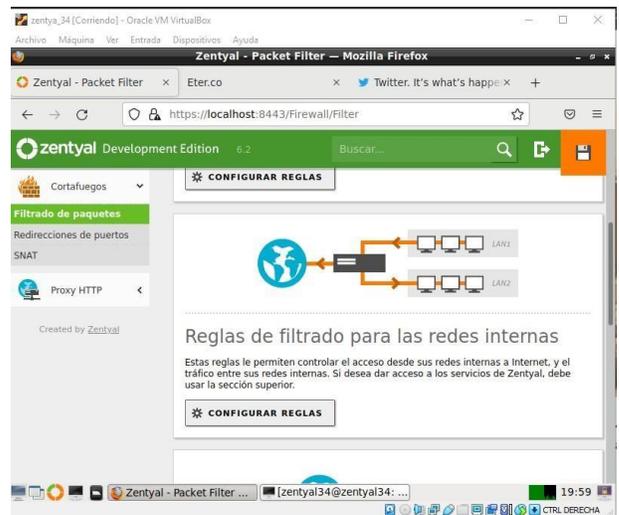


Figura 102 Reglas De Filtrado Para La Red LAN.
Fuente: Elaboración propia.

Hacemos ping a facebook para identificar la IP del servidor que vamos a denegar por medio del Firewall, mientras a su vez lo accedemos desde el cliente.

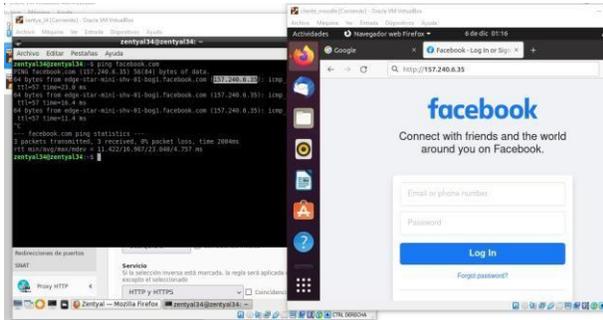


Figura 103 Verificación Conectividad Con La Página Web A Filtrar. Fuente: Elaboración propia.

Ahora creamos la primera regla para denegar el acceso a esta IP del servidor de Facebook.

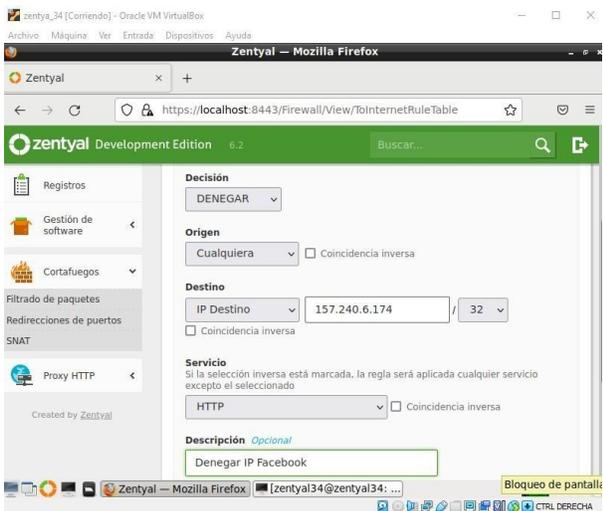


Figura 104 Denegación De Servicio Específico. Fuente: Elaboración propia.

Seguidamente clonamos la regla, pero esta vez por el servicio HTTPS.

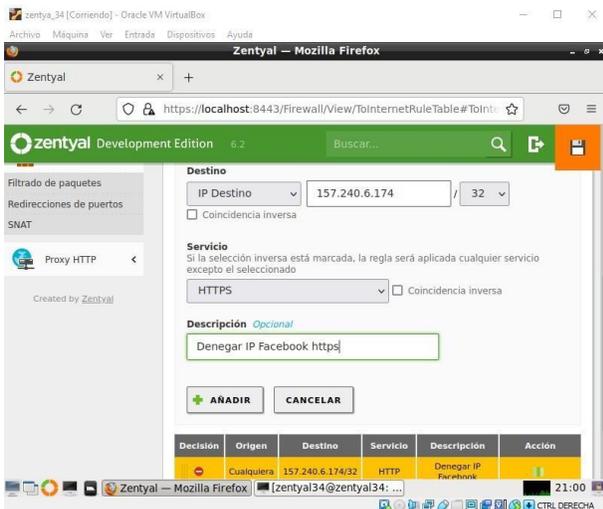


Figura 105 Configuración Inversa De La Regla. Fuente: Elaboración propia.

Guardamos los cambios de las nuevas reglas configuradas.

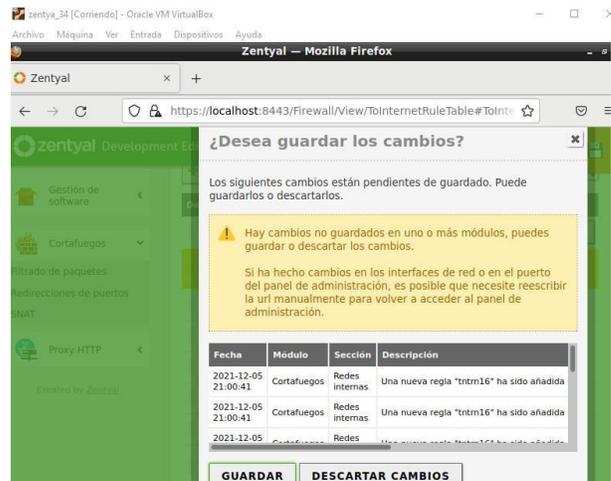


Figura 106 Guardar Cambios Nuevas Reglas. Fuente: Elaboración propia.

Para validar que las reglas de denegación del firewall estén funcionando correctamente accedemos desde la máquina virtual cliente e intentamos acceder desde un navegador web a la página que se denegó el servicio de conexión en nuestra red interna.

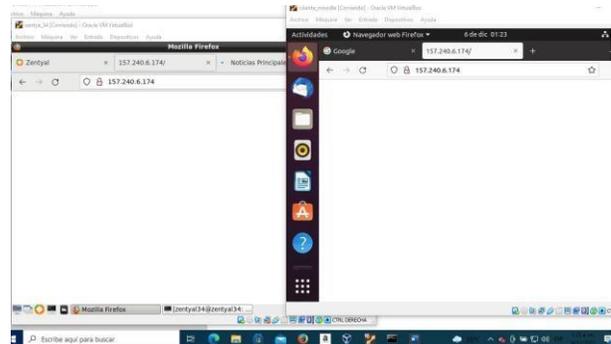


Figura 107 Acceso Denegado A Dirección Web De Facebook. Fuente: Elaboración propia.

7 TEMATICA 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.

7.1 CONFIGURACION INICIAL



Figura 108 Selección De Paquetes.
Fuente: Elaboración propia.

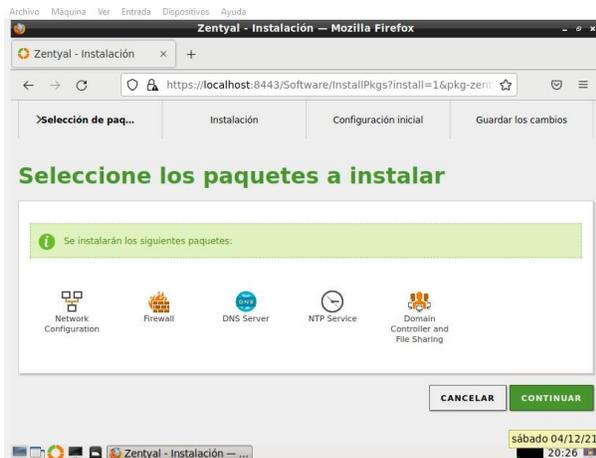


Figura 109 Selección De Paquetes.
Fuente: Elaboración propia.



Figura 110 Instalación De Paquetes
Fuente: Elaboración propia.

Posterior a la instalación de paquetes procedemos a ingresar al asistente de configuración de las interfaces de la red



Figura 111 Configuración Red Interna.
Fuente: Elaboración propia.

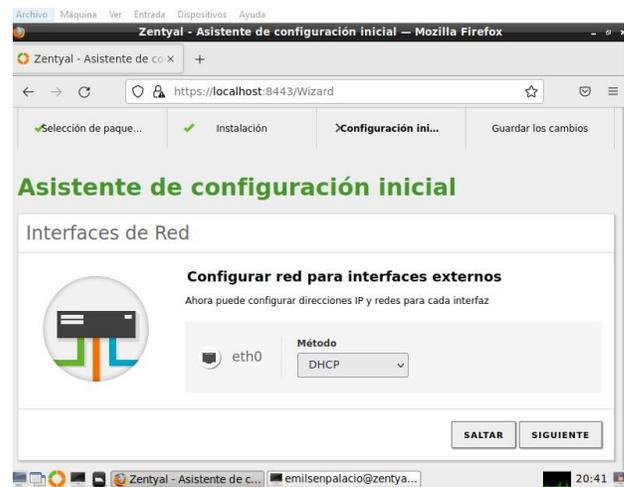


Figura 112 Método De Configuración En DHCP Interfaz De Red Interna. Elaboración propia.

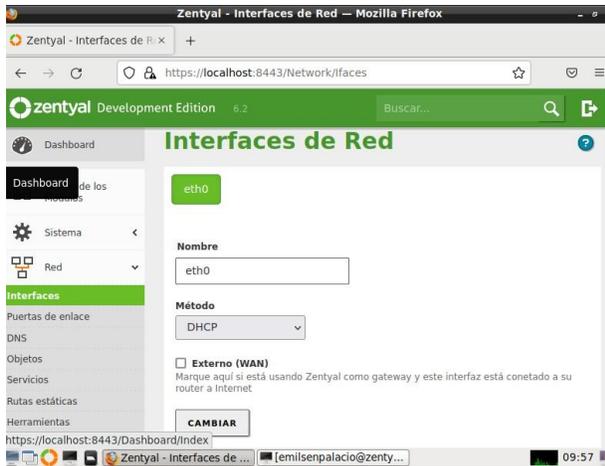


Figura 113 Configuración De La WAN.
Fuente: Elaboración propia.

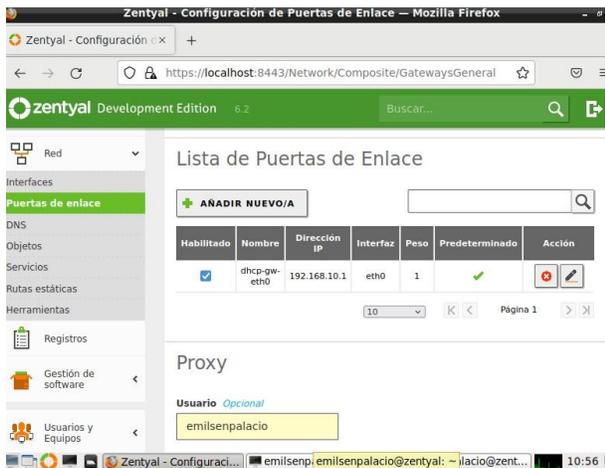


Figura 114 Agregamos Puerta De Enlace Para Tener Conexión. Fuente: Elaboración propia.

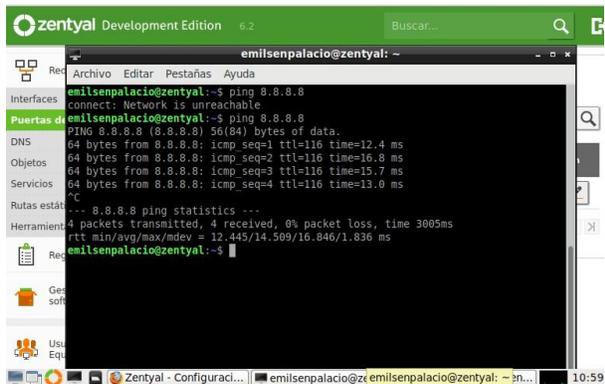


Figura 115 Hacemos Ping De Nuevo Y Nos Responde.
Fuente: Elaboración propia.

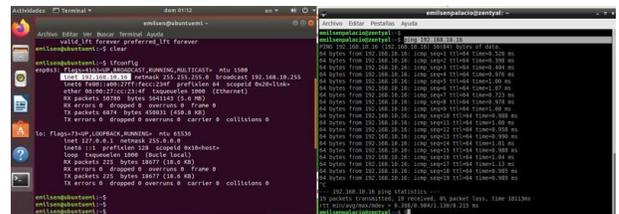


Figura 116 Ping De Servidor A Cliente.
Fuente: Elaboración propia.

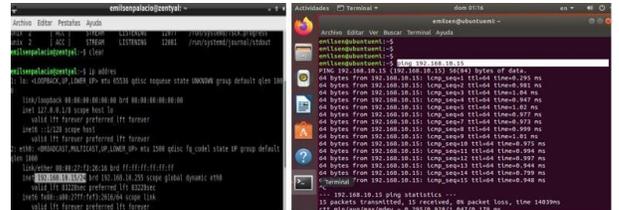


Figura 117 Ping Cliente a Servidor.
Fuente: Elaboración propia.

7.2 CONFIGURACIÓN DE FILE SERVER

Ahora, en la configuración de usuarios y equipos, observamos cual es el modo de funcionamiento del servidor LDAP antes de poder activarlo.

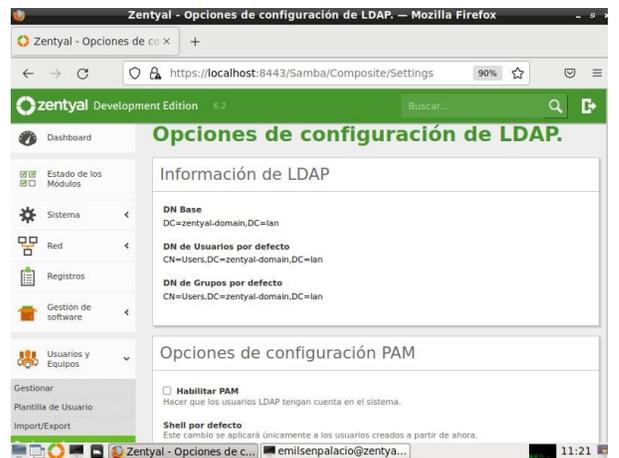


Figura 118 Configuración LDAP.
Fuente: Elaboración propia.

En la imagen nos muestra que el DN base, DN usuarios y DN grupos se presenta con dominio local.

Entramos a Gestionar Usuarios, una vez aquí vemos el árbol de LDAP y agregamos un nuevo usuario, de igual manera podríamos modificar permisos si se requiere.

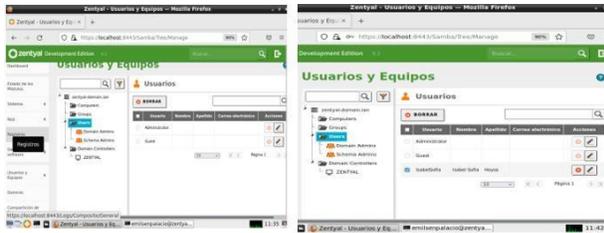


Figura 119 Creación De Nuevo Usuario.
Fuente: Elaboración propia.

Del mismo modo, hacemos creación de los ficheros y carpetas compartidas en los usuarios de Red. Esta vez seleccionamos la opción de compartición de ficheros y añadimos recurso.

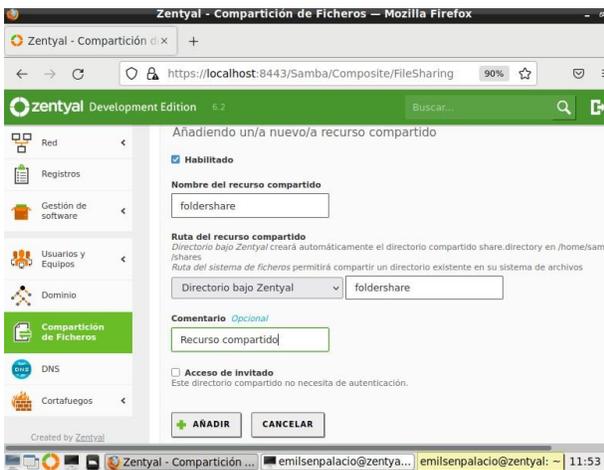


Figura 120 Datos del Nuevo Recurso Compartido.
Fuente: Elaboración propia.



Figura 121 Creado El Recurso Compartido.
Fuente: Elaboración propia.

Definimos el control de acceso, los usuarios y grupos a los cuales pertenece, al igual que tipo de permiso tiene sobre la carpeta.



Figura 122 Control De Acceso.
Fuente: Elaboración propia.

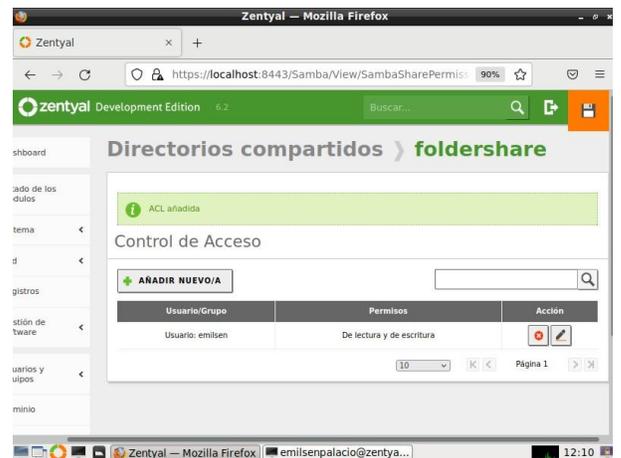


Figura 123 Creado y guardado.
Fuente: Elaboración propia.



Figura 124 Vamos a Usuarios y vemos que fue creado.
Fuente: Elaboración propia.

Realizamos pruebas para observar cómo entramos a las diferentes rutas desde la creación de usuario.

```

ZENTYAL-DOMAIN|isabelsofia@zentyal: /home/samba/shares
Archivo Editar Pestañas Ayuda
emilsenpalacio@zentyal:~$ whoami
emilsenpalacio
emilsenpalacio@zentyal:~$ sudo su - isabelsofia
[sudo] password for emilsenpalacio:
Creating directory '/home/isabelsofia'.
ZENTYAL-DOMAIN|isabelsofia@zentyal:~$ ls
ZENTYAL-DOMAIN|isabelsofia@zentyal:~$ pwd
/home/isabelsofia
ZENTYAL-DOMAIN|isabelsofia@zentyal:~$ cd
ZENTYAL-DOMAIN|isabelsofia@zentyal:~$ cd ..
ZENTYAL-DOMAIN|isabelsofia@zentyal:~/home$ ls
emilsen emilsenpalacio isabelsofia IsabelSofia samba
ZENTYAL-DOMAIN|isabelsofia@zentyal:~/home$ cd samba/
ZENTYAL-DOMAIN|isabelsofia@zentyal:~/home/samba$ ls
profiles shares
ZENTYAL-DOMAIN|isabelsofia@zentyal:~/home/samba$ cd shares
ZENTYAL-DOMAIN|isabelsofia@zentyal:~/home/samba/shares$ ls
foldershare

```

Figura 125 Prueba Creación De Usuario.
Fuente: Elaboración propia.

```

ZENTYAL-DOMAIN|emilsen@zentyal: /home/samba/shares/foldershare
Archivo Editar Pestañas Ayuda
emilsenpalacio@zentyal:~$ sudo su - emilsen
[sudo] password for emilsenpalacio:
ZENTYAL-DOMAIN|emilsen@zentyal:~$ ls
ZENTYAL-DOMAIN|emilsen@zentyal:~$ pwd
/home/emilsen
ZENTYAL-DOMAIN|emilsen@zentyal:~$ cd
ZENTYAL-DOMAIN|emilsen@zentyal:~$ cd ..
ZENTYAL-DOMAIN|emilsen@zentyal:~/home$ ls
emilsen emilsenpalacio isabelsofia IsabelSofia samba
ZENTYAL-DOMAIN|emilsen@zentyal:~/home$ cd samba/
ZENTYAL-DOMAIN|emilsen@zentyal:~/home/samba$ ls
profiles shares
ZENTYAL-DOMAIN|emilsen@zentyal:~/home/samba$ cd shares
ZENTYAL-DOMAIN|emilsen@zentyal:~/home/samba/shares$ ls
foldershare
ZENTYAL-DOMAIN|emilsen@zentyal:~/home/samba/shares$ cd foldershare/
ZENTYAL-DOMAIN|emilsen@zentyal:~/home/samba/shares/foldershare$

```

Figura 126 Ruta De La Creación De Usuario Emilsen.
Fuente: Elaboración propia.

Hacemos conexión a Ubuntu server mediante la ruta smb://192.168.10.15// para visualizar la carpeta compartida.



Figura 127 Acceso A La Carpeta Compartida.
Fuente: Elaboración propia.

7.3 CONFIGURACIÓN FILE PRINT SERVER

Para finalizar la temática se instala una herramienta para impresión, CUPS que nos permite configurar un equipo como servidor de impresión en Linux, este es un sistema de impresión modular y se ejecuta en el puerto 631.

```

emilsenpalacio@zentyal: ~
Archivo Editar Pestañas Ayuda
emilsenpalacio@zentyal:~$ sudo apt-get install cups
[sudo] password for emilsenpalacio:
leyendo lista de paquetes... Hecho
Creando árbol de dependencias
leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libnetplan0 python3-netifaces python3-yaml
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  bc cups-client cups-common cups-core-drivers cups-daemon cups-filters
  cups-filters-core-drivers cups-ipp-utils cups-ppdc cups-server-common
  ghostscript libcupsctl libcupsfilters1 libcupsmime1 libcupsppdc1
  libfontembed1 libqpdf21 poppler-utils ssl-cert
Paquetes sugeridos:
  cups-bsd foomatic-db-compressed-ppds | foomatic-db printer-driver-hpcups
  hplip cups-pdf smbclient xpp printer-driver-gutenprint antiword docx2txt
  ghostscript-x openssl-blacklist
Paquetes recomendados:
  avahi-daemon colord printer-driver-gutenprint cups-browsed liblouisdml-bin
  | liblouis-bin gsfonts gpdf
Se instalarán los siguientes paquetes NUEVOS:
  bc cups cups-client cups-common cups-core-drivers cups-daemon cups-filters
  cups-filters-core-drivers cups-ipp-utils cups-ppdc cups-server-common

```

Figura 128 Instalación CUPS.
Fuente: Elaboración propia.

```

emilsenpalacio@zentyal: /etc/cups
Archivo Editar Pestañas Ayuda
bin home lib64 opt sbin usr zentyal
boot initrd.img lost+found proc srv var
dev initrd.img.old media root sys vmlinuz
etc lib mnt run tmp vmlinuz.old
emilsenpalacio@zentyal:/$ cd etc
emilsenpalacio@zentyal:~/etc$ cd cups
emilsenpalacio@zentyal:~/etc/cups$ ls
cupsd.conf interfaces raw.convs snmp.conf
cups-files.conf ppd raw.types ssl
emilsenpalacio@zentyal:~/etc/cups$ sudo nano cups.conf
emilsenpalacio@zentyal:~/etc/cups$ sudo nano cupsd.conf
emilsenpalacio@zentyal:~/etc/cups$ service cups restart
emilsenpalacio@zentyal:~/etc/cups$ service cups status
● cups.service - CUPS Scheduler
   Loaded: loaded (/lib/systemd/system/cups.service; enabled; vendor preset: ena
   Active: active (running) since Sun 2021-12-05 18:00:40 -05; 30s ago
     Docs: man:cupsd(8)
   Main PID: 7838 (cupsd)
     Tasks: 1 (limit: 3544)
    CGroup: /system.slice/cups.service
           └─7838 /usr/sbin/cupsd -l
dic 05 18:00:40 zentyal systemd[1]: Started CUPS Scheduler.
lines 1-10/10 (END)

```

Figura 129 Ubicación y Configuración Del CUPS.
Fuente: Elaboración propia.

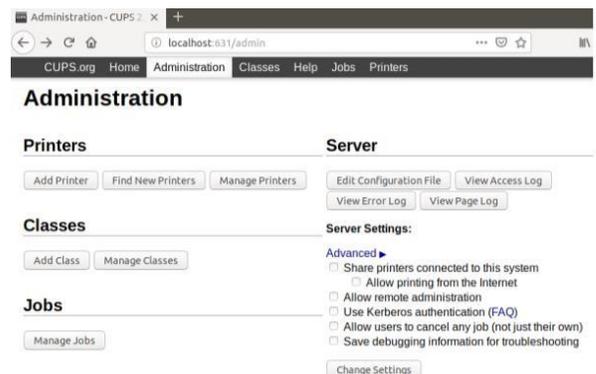


Figura 130 Administración del CUPS.

Fuente: Elaboración propia.

Add Printer

Local Printers:

- CUPS-BRF (Virtual Braille BRF Printer)
- HP Printer (HPLIP)
- HP Fax (HPLIP)

Discovered Network Printers:

Other Network Printers:

- Backend Error Handler
- Internet Printing Protocol (http)
- Internet Printing Protocol (ipp)
- Internet Printing Protocol (https)
- Internet Printing Protocol (ipps)
- LPD/LPR Host or Printer
- AppSocket/HP JetDirect

Figura 131 .Localización de Print
Fuente: Elaboración propia.

8 TEMATICA 5 VPN

Para el servicio de red privada virtual, ingresamos a nuestro panel de gestión de software y seleccionamos el módulo VPN para los paquetes sean instalados en el servidor Zentyal.

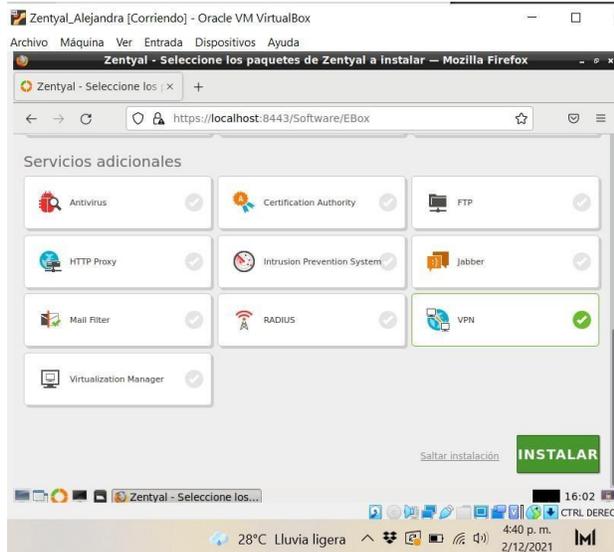


Figura 132 Instalación Modulo De VPN.
Fuente: Elaboración propia.

En el panel de instalación se visualiza los paquetes que se instalaran network configuration, firewall, certification authority y VPN, requeridos para el funcionamiento de nuestra red privada. De esta manera damos inicio a la instalación seleccionando el botón continuar.

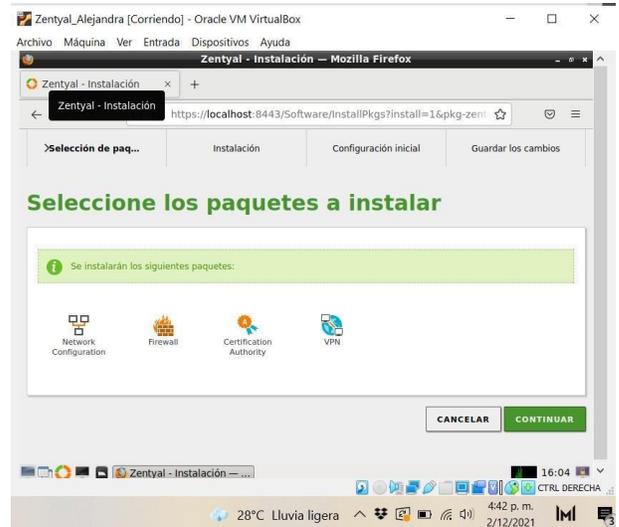


Figura 133 Paquetes A Instalar.
Fuente: Elaboración propia.

En el siguiente panel nos muestra los paquetes instalado para nuestro servicio VPN.



Figura 134 Progreso De Instalación.
Fuente: Elaboración propia.

Después de la instalación del módulo VPN, se mostrará una ventana configuración de las interfaces de red, como me reconoció dos tarjetas de red selecciono una externa y damos clic en siguiente.

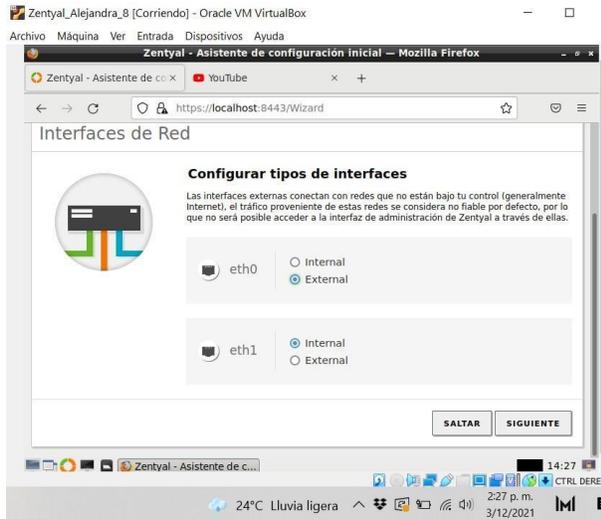


Figura 135 Configurar Tipo De Interfaces.
Fuente: Elaboración propia.

Luego debo seleccionar y configurar la interfaz de red externa, para asignación de IP selecciono DHCP y clic en finalizar.

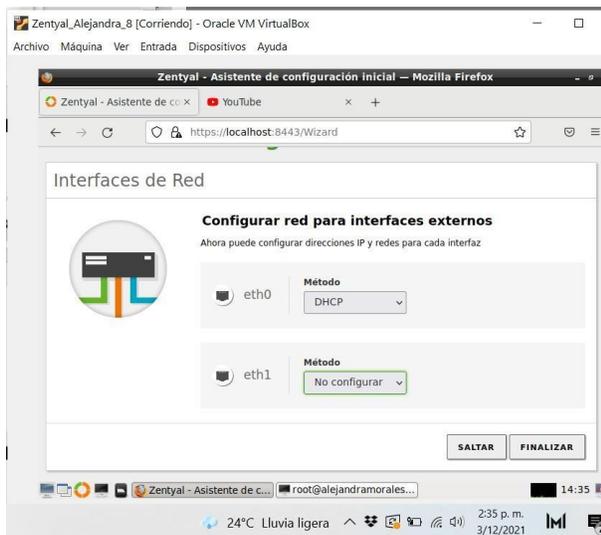


Figura 136 Configuración Método De Conexión De Las Interfaces. Fuente: Elaboración propia.

Nuevamente aparece la barra de descarga para guardar los cambios realizados.

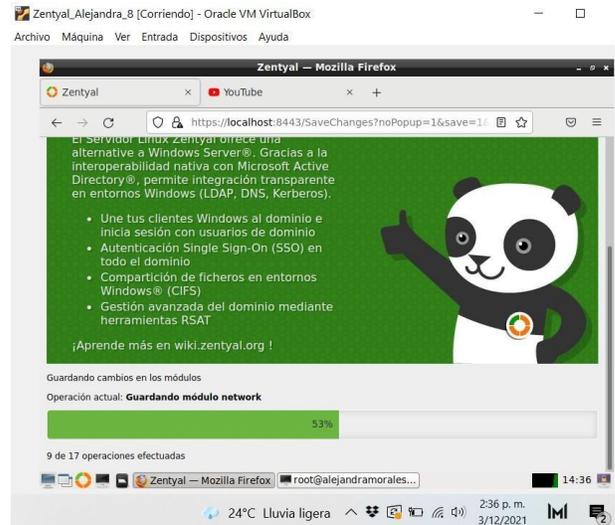


Figura 137 La Aplicación Nos Notifica De Que El Proceso De La Instalación Se Realizó Completo.
Fuente: Elaboración propia.

La aplicación nos notifica de que el proceso de la instalación se realizó completo.



Figura 138 Instalación Completada.
Fuente: Elaboración propia.

Ahora ingresamos al módulo VPN en la sección servidores y procedemos a realizar las configuraciones pertinentes.

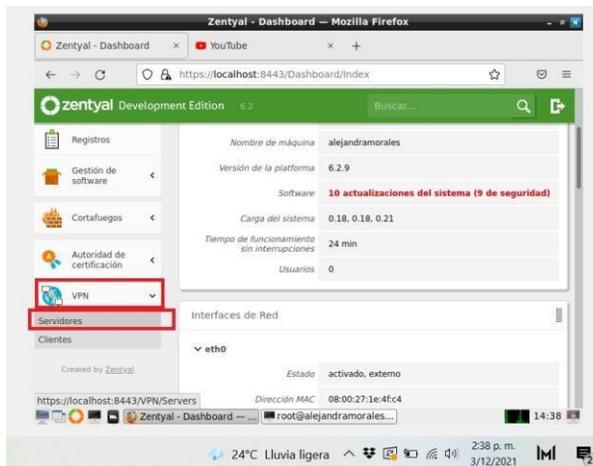


Figura 139 Selección De Área Servidores.
Fuente: Elaboración propia.

La aplicación solicita crear un certificado de CA para usar servidores VPN



Figura 140 Creación De Certificado.
Fuente: Elaboración propia.

Procedemos a hacer clic sobre el link “módulo de autoridad de certificación” y en General. Aparece una ventana donde definimos el nombre de la organización y los días para expirar, luego damos clic en el botón crear.



Figura 141 Autoridad De Certificación
Fuente: Elaboración propia.

En este paso escribo el nombre de la organización y dejo servidor VPN y por defecto dejo los días para expirar y selecciono crear.

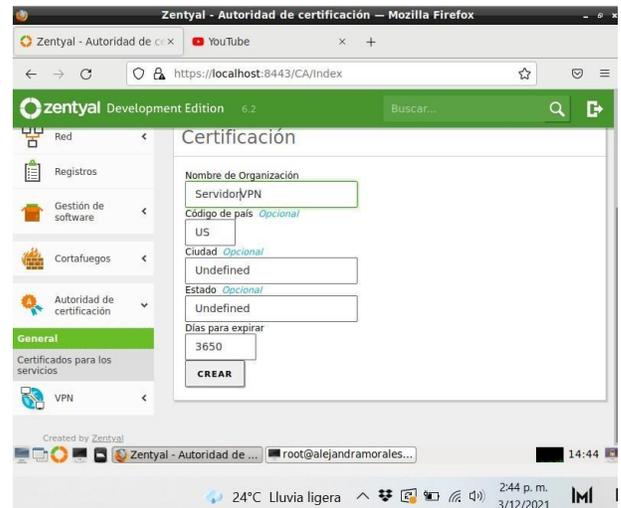


Figura 142 Creación De Certificación.
Fuente: Elaboración propia.

Luego creamos el nombre común para el certificado, en mi caso dejo “servidorVPN_8” y por defecto dejo los días de expiración que sugiere la aplicación y clic en expidir.

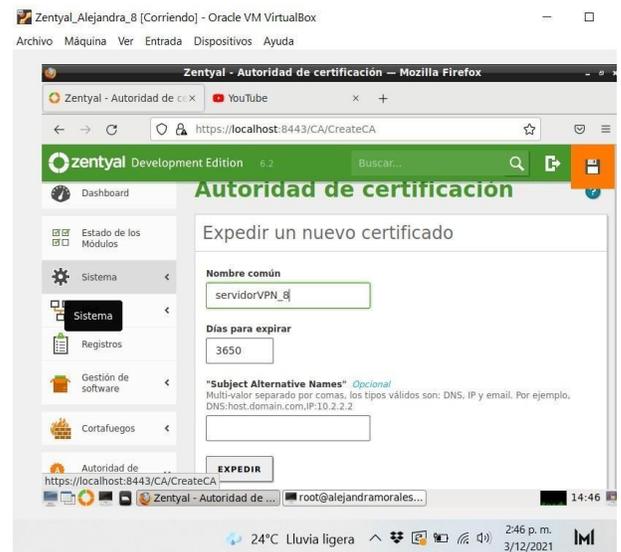


Figura 143 Creación Del Certificado.
Fuente: Elaboración propia.

Después de creado el certificado visualizamos las listas de certificados y se encuentra la de servidor VPN_8 creada anteriormente.

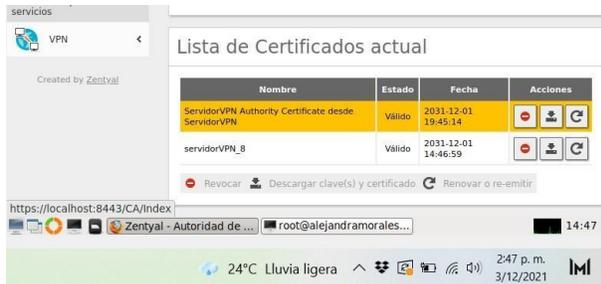


Figura 144 Lista De Certificados.
Fuente: Elaboración propia.

En la parte superior derecha vamos a guardar los cambios realizados, nos aparece una ventana de confirmación damos clic en guardar.

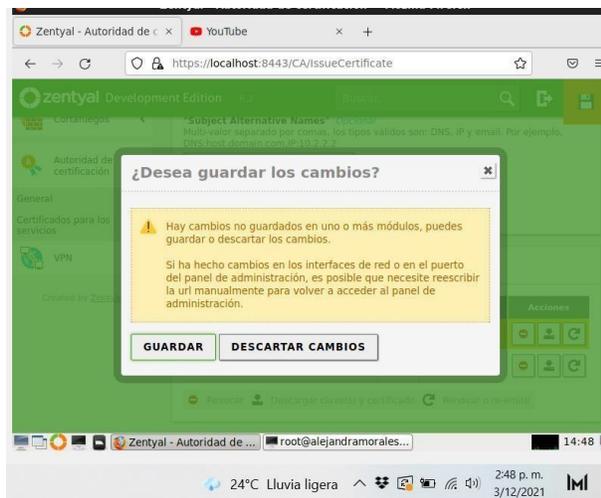


Figura 145 Guardando Cambios.
Fuente: Elaboración propia.

Esperamos a que la aplicación nos confirme que los cambios se guardaron, pulsamos ok.

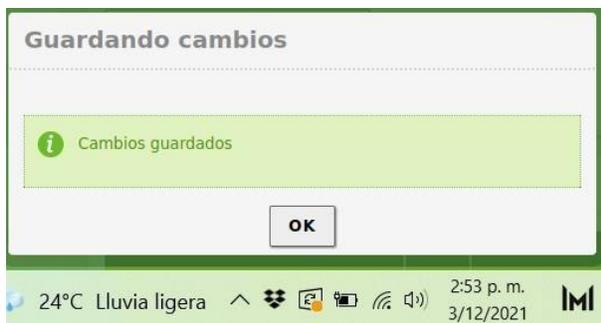


Figura 146 Cambios Guardados.
Fuente: Elaboración propia.

Configuramos el servidor llamado server-s7j-vpn.



Figura 147 Asignación De Nombre Del Servidor.
Fuente: Elaboración propia.

En configuración, asignamos el puerto del servidor, en este caso como ya había realizado 3 pruebas asignamos el 1195, la IP de la VPN y el nombre del certificado para el cliente que se llamó certificado-seralejandra-pch.

Configuración del servidor



Figura 148 Configuración Del Servidor.
Fuente: Elaboración propia.

Para la descarga del certificado en el cliente, asignamos el tipo de cliente, en este caso se realiza para Linux y le indico el nombre del certificado que creamos anteriormente, llamado vpn-server-s7-vpn y clic en descargar.



Figura 149 Descarga Configuración Cliente
Fuente: Elaboración propia.

En el cuadro de dialogo seleccionamos la opción ok, nos muestra el nombre del certificado cliente.

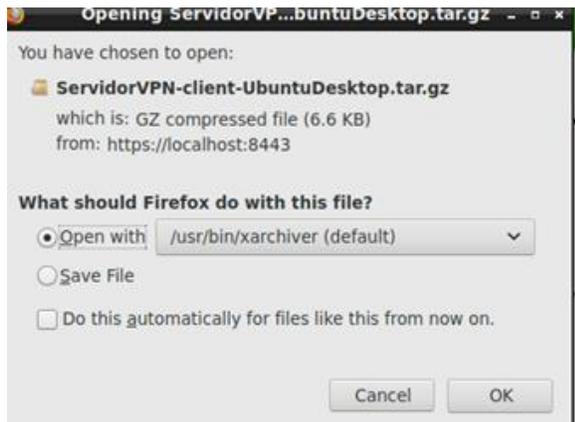


Figura 150 Descarga Certificado.
Fuente: Elaboración propia.

En la ficha de cortafuegos> filtrado de paquetes se configuran > configurar reglas, se añade la creada últimamente que es la del servicio red-vpn-pch



Figura 151 Configuración De Reglas.
Fuente: Elaboración propia.

Guardamos cambios para actualizar.

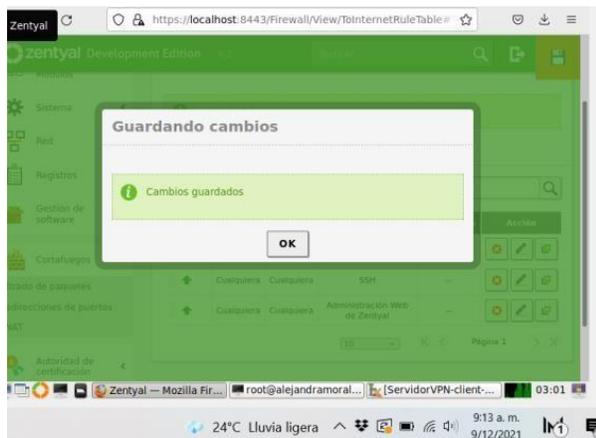


Figura 152 Guardar Cambios.
Fuente: Elaboración propia.

En la terminal del cliente instalo el OpenVPN con la finalidad de que el certificado de cliente pueda observarse y que sea compatible.



Figura 153 Instalación Del OpenVPN
Fuente: Elaboración propia.

Como anteriormente descaramos el certificado para mi cliente desktop al iniciar la VPN me indica que es compatible, clic en importar desde un archivo y selecciono el certificado previamente ya descomprimido de la carpeta.



Figura 154 Añadir El Certificado De Cliente.
Fuente: Elaboración propia.

Luego de seleccionar el certificado, me muestra que está conectada a la VPN.

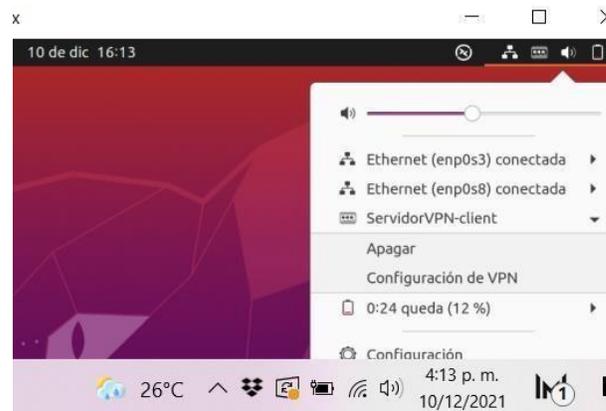


Figura 155 Conexión De VPN.
Fuente: Elaboración propia.

visualizamos el Dashboard del Zentyal y me indica que el servicio está habilitado y se ejecuta con normalidad.



Figura 156 Demonios OpenVPN.
Fuente: Elaboración propia.

Como en el Ubuntu desktop tuve inconvenientes para poder conectarme a la VPN, intenté por Windows, descargando el certificado para el cliente de Windows y el OpenVPN.

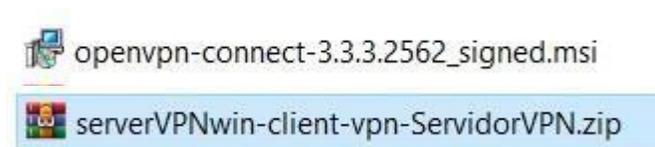


Figura 157 Descargas De Certificado Para Windows Y El Openvpn. Fuente: Elaboración propia.

Después de la instalación, en la pestaña file del openvpn/ browse/ agregamos el certificado el cual ya tiene icono de la aplicación.



Figura 158 Certificado VPN
Fuente: Elaboración propia.

realizamos la conexión el openvpn el cual nos muestra que está activo y efectivamente hay tráfico.

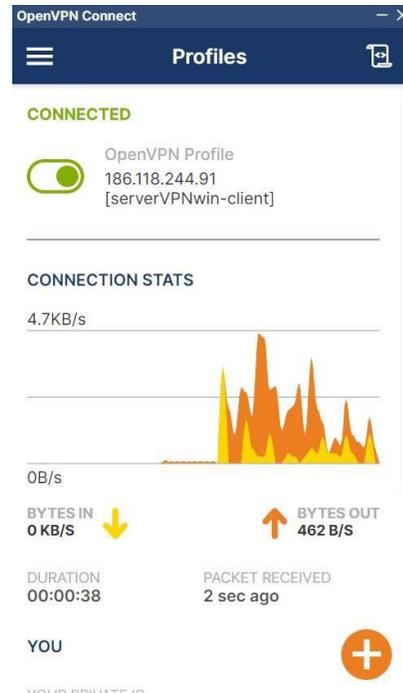


Figura 159 Tráfico Del Openvpn En Windows
Fuente: Elaboración propia.

9 CONCLUSIONES.

Con el desarrollo del presente trabajo practico nos permitió conocer como grupo colaborativo y explorar una herramienta muy práctica para la implementación de servicios sobre infraestructura TI, de esta manera podemos formular una solución bajo plataformas libres como lo es GNU/Linux Zentyal server, a las pequeñas y medianas empresas donde podamos como profesional de TI brindar soporte y administración sobre los recursos tecnológicos, por medio de la configuración de los servicios de DHCP, servidor de DNS, proxy no transparente, firewall, servidor de archivos, servidor de impresión, redes privadas virtuales y controlador de dominio que nos ayudara administrar protocolos de seguridad, permisos, monitoreo de recursos y otros protocolos de acceso de forma remota en cada dispositivo.

Otro punto a resaltar durante el proceso de instalación y configuración a través de la interfaz Zentyal es la practicidad y facilidad de instalar cada uno de los módulos que cuenta la herramienta, ya que de forma intuitiva y siguiendo las indicaciones del asistente de configuración se puede implementar los servicios de forma fácil y rápida.

10 REFERENCIAS BIBLOGRAFICAS

- [1] Ricardo Rodriguez. (2015, 29 mayo). Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN [Vídeo]. YouTube.
<https://www.youtube.com/watch?v=3rNfipxE-9o&t=2s>
- [2] Sanz Mercado, P. (2014). Seguridad en linux: guía práctica. Editorial Universidad Autónoma de Madrid. (Páginas. 13 - 26). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53966?page=13>
- [3] Jorba, J. (2012). Administración de seguridad. Paginas (27 – 33). Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/4/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo4_Administraci%C3%B3n%20de%20seguridad.pdf.
- [4] Ramírez Restrepo, J. (1,06,2021). OVI - Unidad 6 - ISPConfig. [Archivo de video]. Recuperado de <https://repository.unad.edu.co/handle/10596/41421>.
- [5] Forigua, J. A., Ríos, D. A., Diaz, E. F., Pulido, J. A., & Arevalo, J. L. (2020). Solución de necesidades específicas como son: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuego, File Server, Print Server, VPN. Recuperado de: <https://repository.unad.edu.co/handle/10596/38635>.
- [6] Zentyal Comunity (2018) Zentyal 6.2 Documentación Oficial. Recuperado de: <https://doc.zentyal.org/es/>.
- [7] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 205 - 236). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43262?page=205>