Despliegue de servicios en infraestructura IT en ambientes GNU/LINUX

Kevin Duván Posso Peña
e-mail: kdpossop@unadvirtual.edu.co
Carlos Eduardo Caicedo
e-mail: cecaicedo@unadvirtual.edu.co
Andrés Fernando Loaiza
e-mail: afloaiza@unadvirtual.edu.co
Héctor Johan Cadena Ruiz
e-mail: hjcadenar@unadvirtual.edu.co
Felipe Serrano Zamora
e-mail: fe10ser368@unadvirtual.edu.co

RESUMEN: *El presente trabajo se realiza en la adquisición de los conocimientos de la teoría y la práctica en los fundamentos de GNU / Linux, creando la necesidad de conocer la implementación de Zentyal como sistema operativo, su aplicación como su comprensión del funcionamiento en la administración de los servicios de un servidor soportado en Debian, con una gestión de controlar la configuración de manera correcta dependiendo de los requerimientos de usuarios, teniendo la capacidad, calidad y solidez de Linux para este tipo de proyectos encaminados en el control de los módulos o programas Zentyal 6.2 donde se logró una seguridad robusta en las redes y se protegió a los usuarios de posibles vulnerabilidades y ataques del sistema siendo, así unas oportunidades de tener un ahorro, por ende, buenas ganancias en una corporación donde se implementen estas herramientas.*

PALABRAS CLAVE:
DHCP, DNS, firewall, proxy, Zentyal, File Server.

1 INTRODUCCIÓN

Zentyal es una plataforma desarrollada en lenguaje de programación Perl, funciona sobre el Kernel de la distribución Ubuntu y Ubuntu server, como alternativa para adicionarlo como controlador de dominio adicional con la finalidad de replicar todos los objetos (OU, CN, DN, Grupos) del directorio activo, dispone de muchas características y la capacidad para controlar dominios, servidor de correo dedicado, servidor de infraestructura y Gateway, permite unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer un acceso a Internet confiable, seguro, servicios de DNS / DHCP, CA, VPN respaldo a puerta de enlace, firewall y proxy HTTP, compatible con Microsoft Active Directory , por lo que se pueden unir clientes Windows al dominio y gestionarlos con facilidad, el correo electrónico incluye los servidores SMTP y POP3/IMAP servidor de correo, servidor de dominio & directorio con correo o servidor todo en uno, Soporte técnico por parte de Zentyal y Licencias Perpetuas y soporte opcional.

2 INSTALACIÓN DE ZENTYAL

2.1 REQUISITOS

Zentyal Server 6.2, funciona sobre hardware estándar de arquitectura x86_64 (64-bit). Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios vayan a utilizar los servicios y de sus hábitos de uso.

Algunos módulos tienen bajos requerimientos, como Firewall, DHCP o DNS, pero otros como el Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU. Los módulos de Proxy y Compartición de ficheros mejoran especialmente su rendimiento con discos rápidos debido al uso intensivo de E/S que realizan. Es bueno tener en cuenta que una configuración RAID añade un nivel de seguridad frente a fallos de disco duro y aumenta la velocidad en operaciones de lectura. Zentyal como puerta de enlace o cortafuegos necesitará al menos dos tarjetas de red, pero si se usa como un servidor independiente, una única tarjeta de red será suficiente. Si tiene dos o más conexiones de Internet puede tener una tarjeta de red para cada router o conectarlos a una tarjeta de red teniéndolos en la misma subred. Otra opción es configurar segmentos VLAN. Por otro lado, siempre es recomendable tener un SAI con tu servidor.

2.2 ENLACE DE DESCARGA

http://download.zentyal.com/

2.3 PROCESO INSTALACIÓN ZENTYAL SERVER 6.2

Se crea una máquina virtual en la herramienta VirtualBox sobre la cual se instala el Zentyal server 6.2

Figura 1. Creación máquina virtual

3 DESARROLLO TEMÁTICAS

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

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

La implementación de Zentyal está orientada a facilitar la administración y control de servicios de infraestructura IT en redes Intranet y Extranet que en instituciones complejas pueden ser difíciles de llevar. En el presente paso se entregan servicios de DHCP, DNS y Controlador de Dominio a distribuciones GNU/Linux basada en Ubuntu.

Instalado el servidor de Zentyal en nuestra máquina virtual de VirtualBox e iniciado su panel de control por primera vez, se realiza la instalación de los módulos a utilizar y las configuraciones iniciales de red y dominio.

Para este caso se instalan los paquetes DNS server, DHCP server y Domain Controller and File Shring como se evidencia en la siguiente figura.

Figura 2. Paquetes Temática 1.

Posteriormente, es necesario realizar la configuración de las interfaces, las cuales corresponden cada una a los adaptadores asignados a la máquina virtual.

Se define entonces la interfaz eth0 para comunicación “external” y el eth1 para comunicación “internal”.

Figura 3. Interfaces de red Temática 1

Así mismo, se configura la dirección IP para cada interfaz. En este caso se deja el eth0 para asignación por DHCP y al eth1 se le define la IP 10.0.2.16.

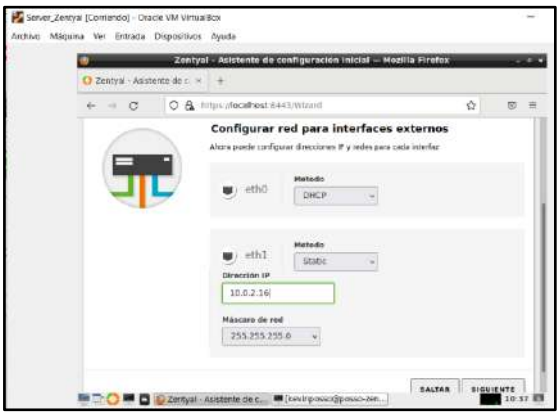

Figura 4 Asignación Metodo IP interfaces.

Como parte final de la configuración inicial, se define el nombre del servidor de dominio.

Figura 5 Servidor de Dominio Temática 1

De esta forma se culmina la configuración inicial y se procede a emplear los módulos instalados.

Configuración DHCP Server:

El objetivo del módulo de DHCP utilizado en esta temática es facilitar y centralizar la administración de las direcciones IP en una red corporativa, evitando conflictos de direcciones repetidas, administraciones descentralizadas y desplazamiento a sitio para realizar configuración de la red.

Antes de iniciar la configuración del módulo, es necesario activarlo, lo cual se realiza a través de la sección *Estado de módulos.*

Una vez activo el módulo, nos dirigimos a la sección correspondiente para su gestión y se configura la interface eth1 destinada para la comunicación interna de la red.

Definimos el rango de IPs que podrá asignar nuestro servidor a las maquinas cliente. En este caso se creó el rango "*Rangos Clientes Unad*" con IPs disponibles desde la *IP 10.0.2.20 hasta la IP 10.0.2.30*.

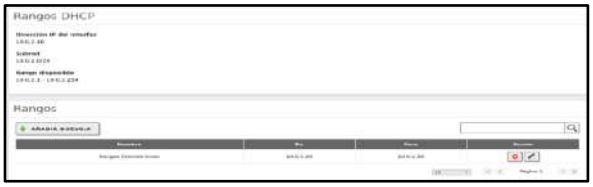

Figura 6 Rango DHCP Temática 1.

Definido el rango, es necesario guardar los cambios en el Zentyal e ingresar a las maquinas tipo Cliente y realizar las validaciones correspondientes.

Iniciados en un cliente Ubuntu desktop se verifica la correcta asignación de configuración de red a través del servidor de Zentyal.

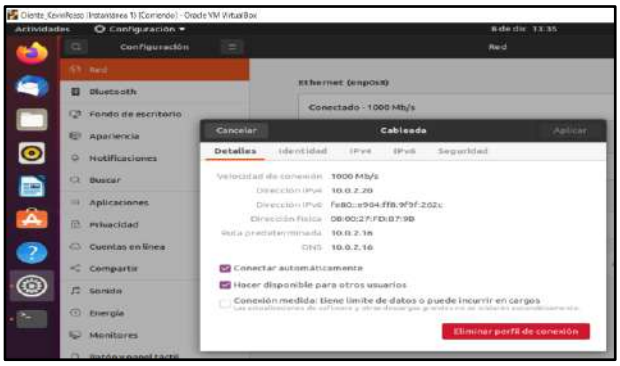

Figura 7 Validación Cliente Ubuntu - DHCP

Posteriormente, desde el dashboard de Zentyal se evidencian los clientes a los cuales se les ha efectuado la asignación de IP mediante DHCP.

Figura 8 Dashboard Zentyal

Configuración DNS Server:

Ingresamos al módulo de DNS y procedemos a realizar la configuración sobre el dominio creado pasos anteriores. "*zentyal-domain.lan*"

Figura 9 Modulo DNS Server – Temática 1

Se registran en el domino 3 máquinas virtuales tipo cliente indicando su respectivo Nombre, IP y Alias.

Figura 10 Registro maquinas en DNS

Posteriormente, se guardan los cambios y se procede realizar validaciones desde los diferentes clientes.

Ubicados en el cliente1 (desktop Ubuntu) se efectúan las validaciones correspondientes. Se realiza ping al servidor Zentyal por nombre y responde correctamente.

Del mismo modo se realiza ping al cliente2 "*kevinposso-virtualbox*" y cliente3 "*servkevinposso*" por IP y nombre y se evidencia que es reconocido mediante el servidor de DNS de forma correcta.

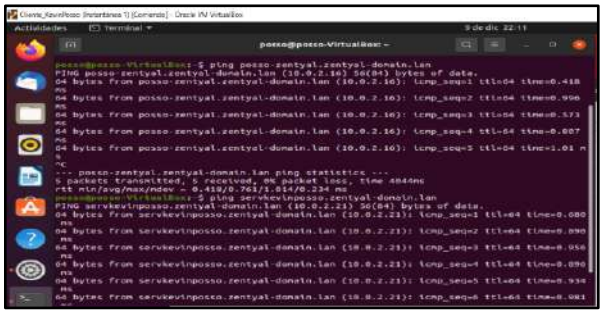

Figura 11 Validación DNS server

Configuración Controlador de Dominio.

La configuración del Controlador de Dominio inicia con la verificación del dominio creado, esto en el módulo "Sistema" sección General (En caso de querer cambiar el dominio se puede realizar en este punto).

Seguidamente, ingresamos al módulo U*suarios y Equipos* y procedemos con la creación de un usuario administrador.

Ya hay un usuario creado por defecto, sin embargo, se creó el usuario “admin” con permisos de administrador del Directorio Activo.

Figura 12 Usuario administrador Directorio Activo.

De igual forma, se registra un usuario cliente en el directorio activo.

Validado el servidor de dominio y creados los usuarios, se ingresa al cliente para efectuar el registro al dominio. Ingresamos al cliente1 “desktop Ubuntu”.

Para distribuciones Ubuntu GNU/LINUX es necesario el uso de aplicaciones que permitan la gestión de Directorios Activos. Por lo anterior, se utilizó ***Likewise***, un sistema que simplifica lo necesario para configurar y autenticar una máquina Linux dentro de un dominio Active Directory.

Los paquetes instalados son:

- libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
- likewise-open_6.1.0.406-0ubuntu10_amd64.deb
- likewise-open-gui_6.1.0.406-0ubuntu10_amd64.deb

Una vez desempaquetados e instaladas las dependencias necesarias, se utiliza el comando “sudo domanjoin-gui” para abrir el entorno grafico de Likewise mediante el cual se efectúa el registro de la maquina en el dominio.

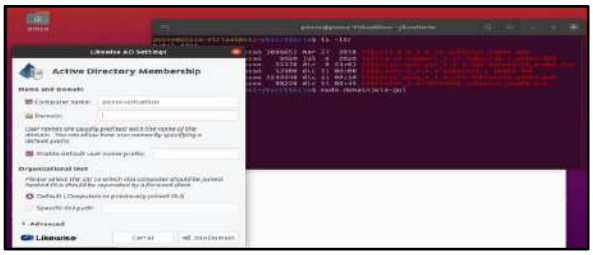

Figura 13 Likewise Interfaz Gráfica.

Iniciada la interface de Likewise se indica el dominio a utilizar y se autentica con un usuario administrador del directorio activo para efectuar el registro del equipo.

Figura 14 Registro equipo en Directorio Activo

3.2 Temática 2: Proxy no transparente.

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

instalación y configuración de Zentyal en VirtualBox.

Nuestro sistema de estudio Zentyal está instalado, arrancará una aplicación web de administración a la que podremos acceder, local o remotamente, mediante nuestro navegador. El primer reinicio el sistema inicia la sesión de usuario automáticamente, de aquí en adelante, necesitará autenticarse antes de hacer login en el sistema. El primer arranque tomará algo más de tiempo, ya que necesita configurar algunos paquetes básicos de software.

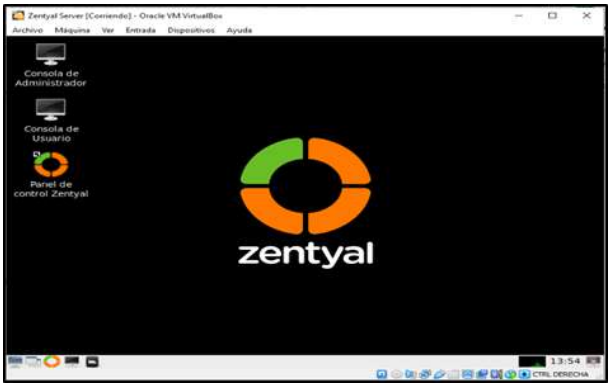

Figura 15. instalación Zentyal

Selecciono los servicios indispensables que se requieren para la práctica y su correcto funcionamiento:

- DNS Server
- DHCP Server
- HTTP Proxy
- Certificación Authority

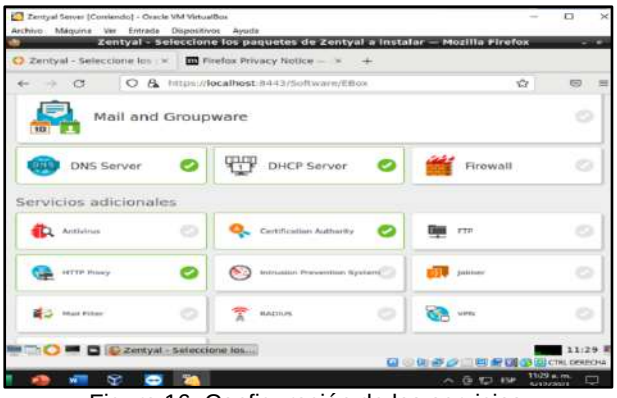

Figura 16. Configuración de los servicios

Se realiza la configuración de la red, Para la eth0, la dejamos en modo DHCP externa, y para la eth1 en modo interna estática, y la dirección IP escogida es 10.10.10.1 con mascara 24

Figura 17. Configuración de la red

Hasta el momento se ha realizado la instalación y configuración de servicios adquiriendo conocimiento y destreza con el sistema operativo Zentyal. Se ha consultado en YouTube y las webs conferencias realizadas por tutor del curso para realizar satisfactoriamente la temática asignada.

Luego empiezo creando un rango en DHCP, para la tarjeta interna, que va a ser las IP a las que el cliente se puede conectar. En este caso la segmentación escogida es de las 10.10.10.10 a las 10.10.10.30, de esta manera creamos accesos en un rango y ancho de banda para la conexión a internet.

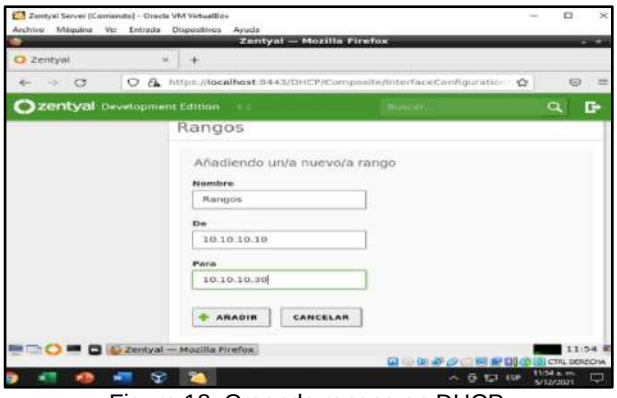

Figura 18. Creando rangos en DHCP

Se verifica que el servidor ya está reconociendo la conexión con Ubuntu, con la IP, máscara y dominio, con la IP asignada por DHCP

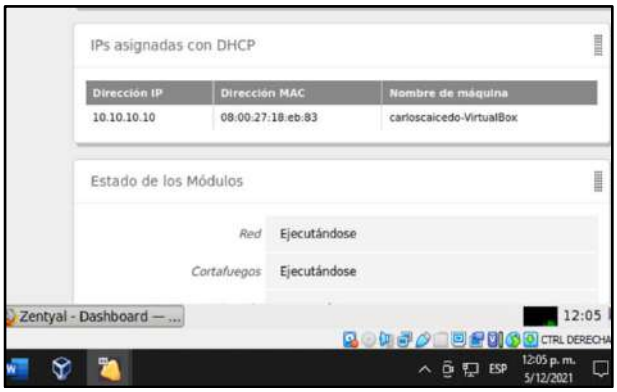

Figura 19. IP asignadas con DHCP

Como lo solicita la guía de actividades un proxy no transparente, no marcamos el recuadro, y como va a salir por un puerto, lo asignamos que en este caso es 1230.

Figura 20. Configuración puerto 1230

Se habilita el proxy HTTP para salida por el puerto 1230, donde se habilita y deshabilita algunas páginas en internet.

Nos dirigimos a la opción de URL, y agregamos las páginas que NO puede acceder, con un permiso estricto.

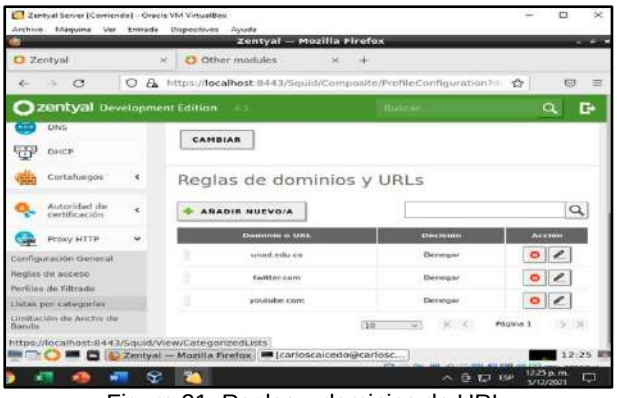

Figura 21. Reglas y dominios de URL

Una vez creado el perfil, vamos a crear una regla de acceso, y vamos a seleccionar en el objeto de red, el cliente1, y aplicamos un perfil de restricción llamado paginas para que tome las configuraciones. También si deseamos podemos poner las reglas en un día específico.

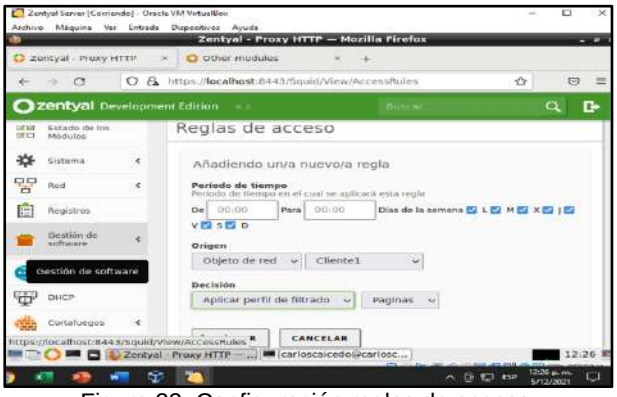

Figura 22. Configuración reglas de acceso

Aplicamos el Proxy en el navegador, poniendo la puerta de enlace 10.10.10.1 con el puerto 1230 y guardamos los cambios.

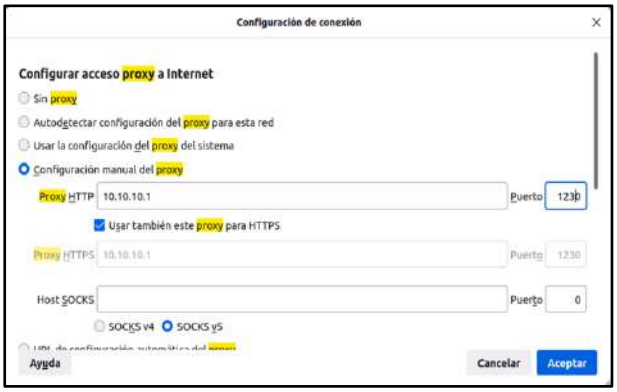

Figura 23. Configuración de conexión de red

Hasta este punto del aprendizaje he configurado el proxy para habilitar y deshabilitar algunas conexiones a la red, automáticamente vemos que el servidor está respondiendo a la conexión de Ubuntu.

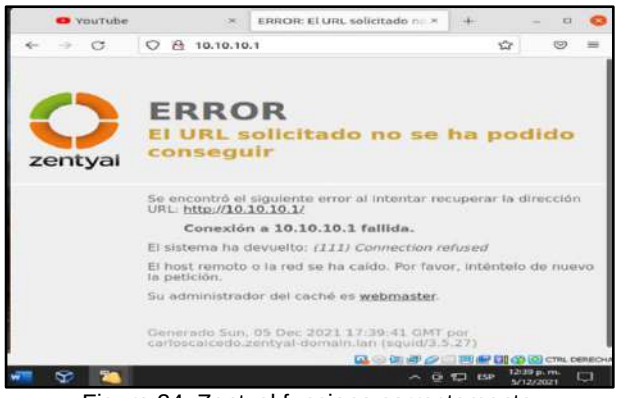

Figura 24. Zentyal funciona correctamente

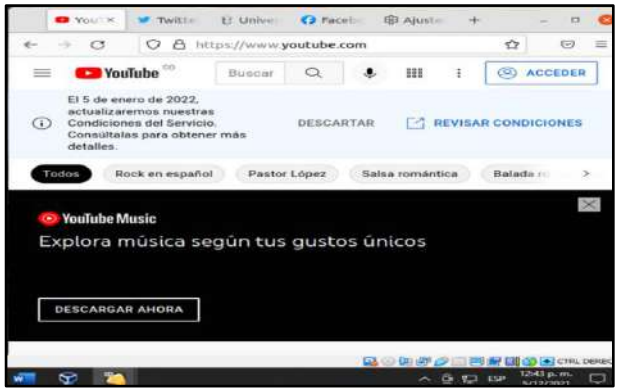

Figura 25. Zentyal funciona correctamente

3.3 Temática 3: Cortafuegos

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

En la actualidad la seguridad de la información es vital para cualquier entidad u organización, es por eso por lo que el cortafuegos o firewall, revierte de gran importancia al momento de proteger esos bienes intangibles como lo es la información, es así como Zentyal emplea en su módulo de cortafuegos Netfilter que es un subsistema del kernel de Linux.

Con la implementación del cortafuegos se logra el monitoreo del tráfico de la red con la implementación de una serie de reglas que permitirá o denegará el acceso. Se dice que es una barrera de seguridad entre las redes internas establecidas, controladas y protegidas con aquellas redes externas que en ocasiones no se conoce su procedencia.

Realizada la instalación de Zentyal Server 6.2, en el navegador de internet se abre la interfaz gráfica del

servidor la cual solicita credenciales de acceso, las cuales fueron configuradas con anterioridad.

Figura 26. Ingresando credenciales de usuario

Al ingresar a la herramienta gráfica de administración de Zentyal, se procede a instalar los paquetes de Configuración de Redes, Firewall, DHCP Server y DNS Server.

Figura 27. Confirmación paquetes a instalar

Siguiendo las indicaciones de la página oficial de Zentyal para la configuración del cortafuego, normalmente se instala entre la red interna y el router, en este caso como se muestra a continuación se realiza la configuración de las interfaces de red, como se muestra en la Fig. 28. la interfaz eth0 se determina externa y la interfaz eth1 como interna.

Figura 28. Configuración tipos de interfaces

Continuando con la configuración de interfaces, la red externa (WAN) es determinada por DHCP y la red interna (LAN) se manejará con método estático y se asigna la IP 172.16.1.1, como se muestra en la Fig. 29.

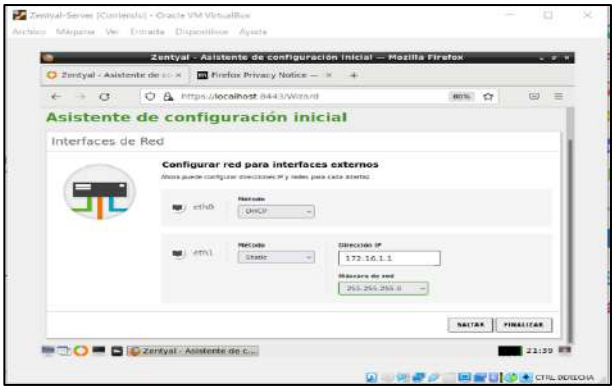

Figura 29. Asignando método a las interfaces

Configuradas las interfaces de red, se procede a verificar en la estación de trabajo de Linux de nombre *Andrés*, la cual está alojada en la máquina virtual “Ubuntu paso 3”, se encuentre configurado de acuerdo con la puerta de enlace y DNS de Zentyal y que haya recibido la IP por DHCP.

Figura 30. Configuración de red estación Linux

Se ingresa al Dashboard de Zentyal y se verifica que se ha asignado una IP por DHCP, en este caso la de nuestra estación de Linux de nombre *Andrés*.

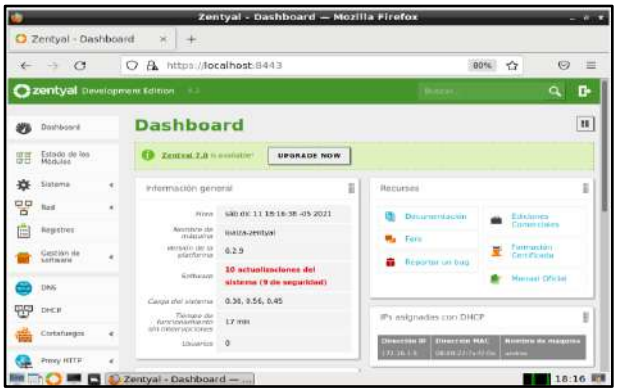

Figura 31. IP asignada por DHCP

Para facilitar el manejo de la red interna se crea un objeto llamado "*Grupo45*" en el cual se añade como miembro la estación Linux que está configurada para el desarrollo de esta temática.

Figura 32. Creando objeto manejo equipos red interna

De igual manera, para facilitar el manejo de las reglas y las restricciones se crearán dos objetos llamados *Redes Sociales* y *Entretenimiento* en los cuales se agruparán los sitios a restringir, así:

Redes Sociales {Facebook - Twitter}, para lo cual se accede al módulo RED sección Objeto en la cual se crea el objeto Redes Sociales y se procede a ingresar los miembros con respectiva IP o rango de direcciones IP, como se muestra en la Fig. 33.

Figura 33. Miembros del objeto Redes Sociales

Entretenimiento {ole.com.ar - pelismart.com}, para lo cual se accede al módulo RED sección Objeto en la cual se crea el objeto Entretenimiento y se procede a ingresar los miembros con respectiva IP o rango de direcciones IP, como se observa en la Fig. 34.

Figura 34. Miembros del objeto Entretenimiento

Configurando reglas

Para realizar la configuración de reglas y restringir el acceso a esos dos objetos creados en la herramienta de administración del servidor Zentyal, se procede a ingresar por la opción firewall o cortafuegos seleccionando el ítem "Filtrado de paquete", donde se muestra cuatro opciones de reglas de filtrado existentes, como lo indica la Fig. 35.

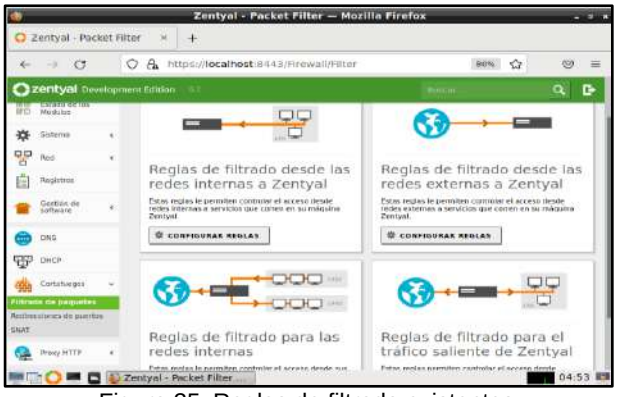

Figura 35. Reglas de filtrado existentes

En este caso donde se solicita restringir el acceso a algunos sitios, se seleccionada "Reglas de filtrado para las redes internas" debido a que estas reglas permiten controlar el acceso desde las redes internas a Internet, y el tráfico entre las redes internas.

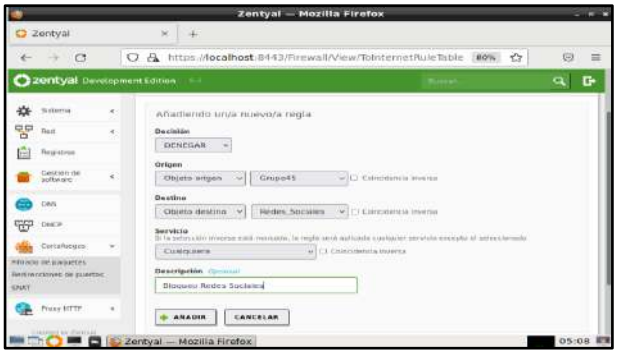

Figura 36. Añadiendo restricción para redes sociales

Es así que, al ingresar a la configuración de reglas, se procede a seleccionar añadir nuevo desplegando el menú de añadiendo una nueva regla, en la decisión se

selecciona DENEGAR, en el origen se elige por objeto Grupo45 que es donde se encuentran los equipos de la red interna, en Destino se selecciona objeto y se relaciona con el objeto creado Redes Sociales, en el servicio se selecciona cualquiera para mayor cobertura de la restricción y en descripción se coloca Bloqueo Redes Sociales, procedimiento que se realiza para crear la restricción a las páginas de entretenimiento. Efectuados cada uno de los anteriores procedimientos se guardan los cambios para que las nuevas reglas queden configuradas.

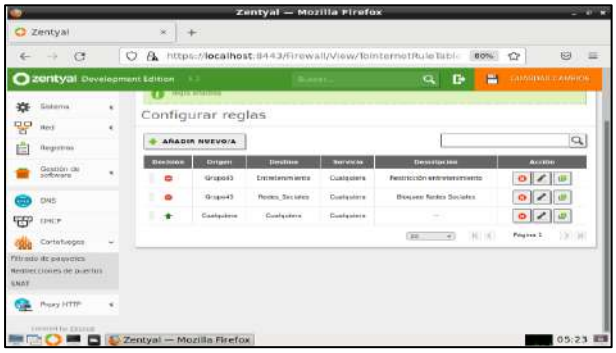

Figura 37. Reglas añadidas

Resultados obtenidos

Como se requiere para la validación del funcionamiento del cortafuego de acuerdo con las reglas establecidas, desde la estación de trabajo GNU/Linux y se solicita acceso a la página Pelismart, pero indica el error "*No se puede conectar*" como lo indica la Fig. 38.

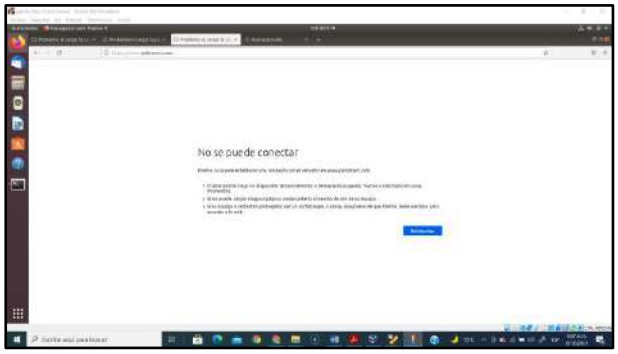

Figura 38 Acceso denegado a Pelismart

Así mismo, para comprobar por terminal la conexión a esta página se realiza un ping a la url, evidenciando la perdida de paquetes en un 100% lo que indica que no hay comunicación y se está cumpliendo las restricciones.

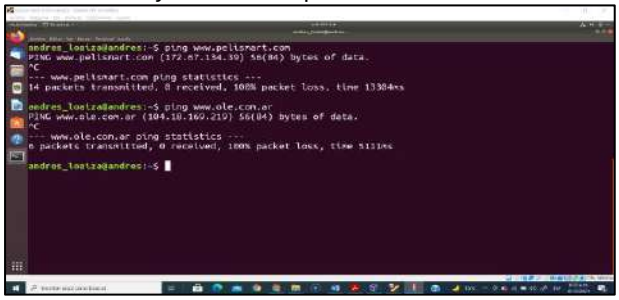

Figura 39. Verificación mediante ping entretenimiento

3.4 Temática 4: File Server y Print Server

Producto esperado: 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

Una vez instalada la máquina virtual Zentyal, se configura una de las características para el funcionamiento correcto del file server y de la impresoras.

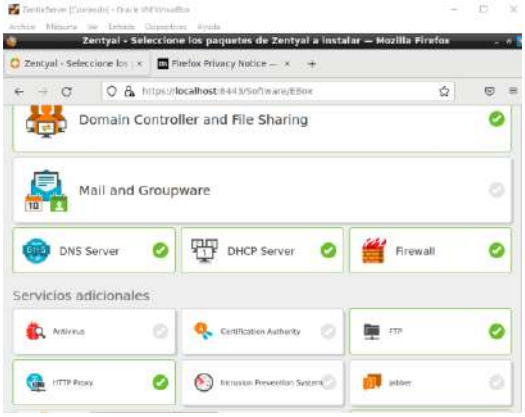

Figura 40 Característica FTP

Para el correcto funcionamiento del file server se debe configurar las dos tarjetas de red una local que hará puente con la tarjeta de red del equipo host y la otra tarjeta que permitirá estar en un segmento diferente donde se debe agregar también el equipo cliente que va a conectarse al servidor de archivos.

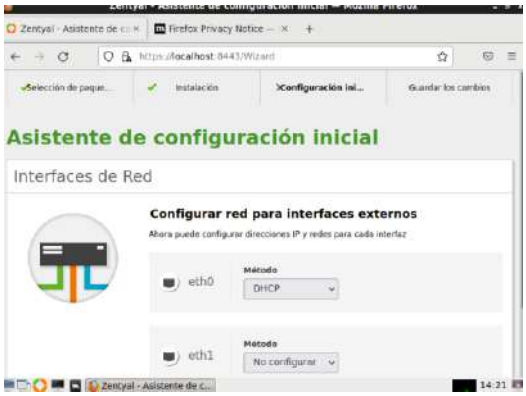

Figura 41 Configuración tarjetas de red

Una vez configurada las tarjetas de red se procede a realizar la creación de la carpeta compartida en la ruta de acceso del administrador de Zentyal, allí se encuentra el recurso "Compartición de archivos", se procede a crear la carpeta compartida y dar acceso a usuarios.

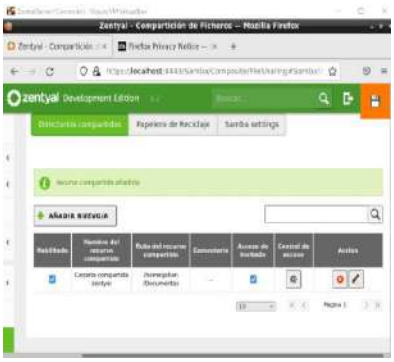

Figura 42 Creación de carpeta compartida

Se verifican los usuarios creados anteriormente para dar sobre la carpeta compartida los permisos necesarios.

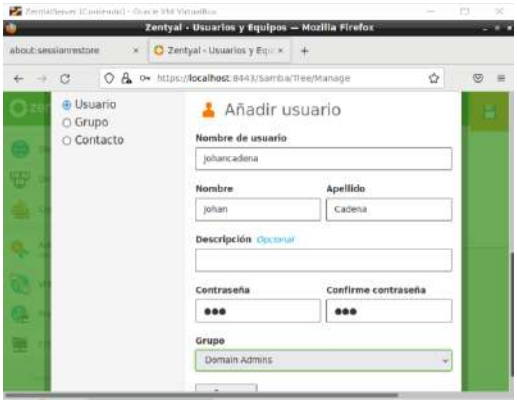

Figura 43 Usuarios creados

Finalizando el proceso de configuración en el equipo servidor, se procede con la configuración del equipo cliente, como se mencionó anteriormente, este equipo debe estar conectado dentro del mismo segmento de red para poder acceder a los archivos compartidos, es por esto por lo que se procede a configurar la tarjeta de red del equipo para que la conexión sea exitosa.

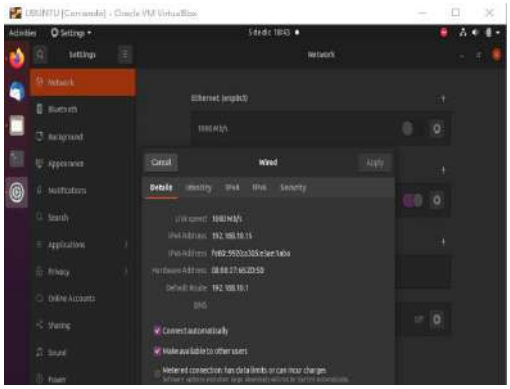

Figura 44 configuración IP cliente

Una vez configurada, se accede al servidor de archivos a la carpeta compartida desde el equipo cliente, se conecta al servidor

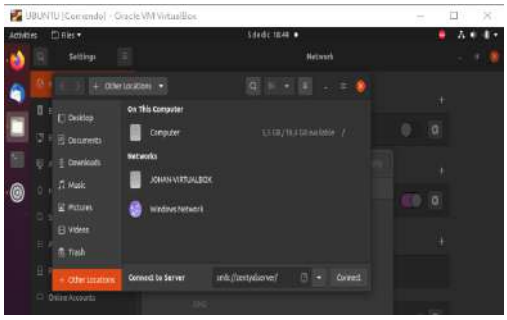

Figura 45 conexión al servidor

Al conectarse el equipo muestra la carpeta compartida

Figura 46 Carpeta compartida

Para conectarse se debe usar el usuario de red anteriormente configurado en el server Zentyal

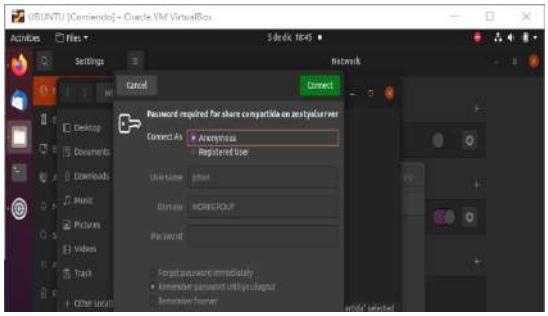

Figura 47 Acceso con usuario de dominio

Se ingresa con el usuario de dominio y se copia un archivo a la carpeta para probar que la carpeta es la misma que se creó antes y que efectivamente el file Server esta activo

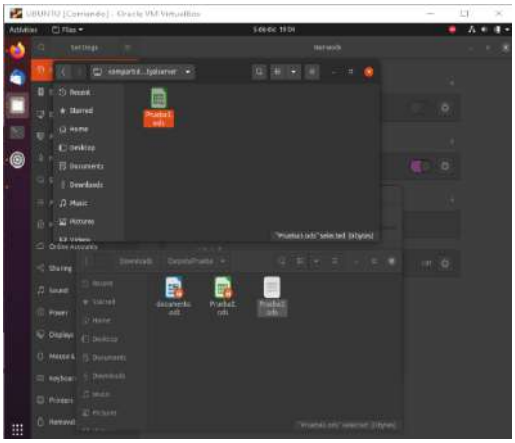

Figura 48 Copia a la carpeta

Posteriormente se verifica desde el servidor Zentyal y se evidencia el documento en la carpeta lo que indica que se subió correctamente

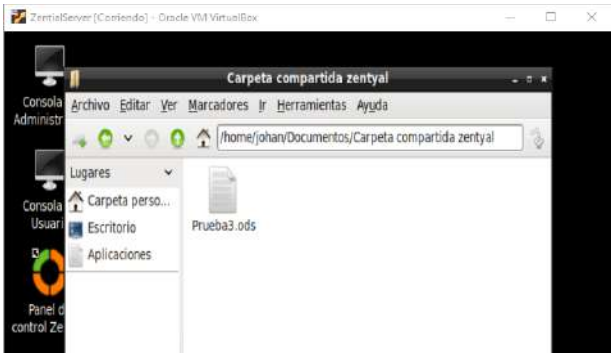

Figura 49 Archivo desde el servidor

Se realiza el mismo ejercicio con un usuario del dominio, pero sin permisos para evidenciar el mensaje que muestra el sistema.

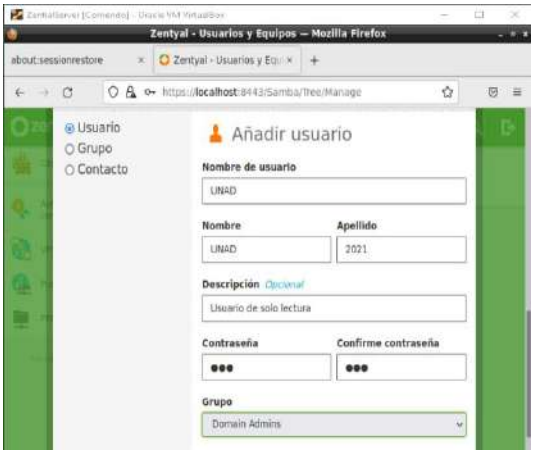

Figura 50 Usuario sin permisos

Figura 51 Permisos asignados

En este caso se realiza la prueba con el usuario a quien solo se le concedió permisos de lectura

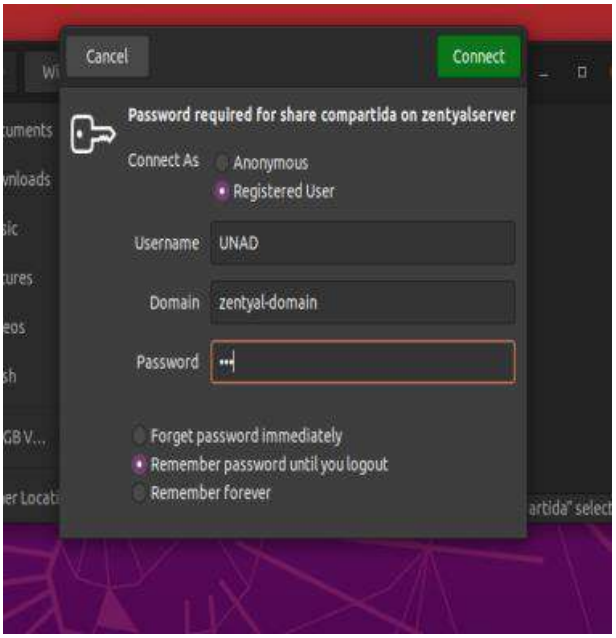

Figura 52 Acceso con usuario sin permiso

Mensaje de error

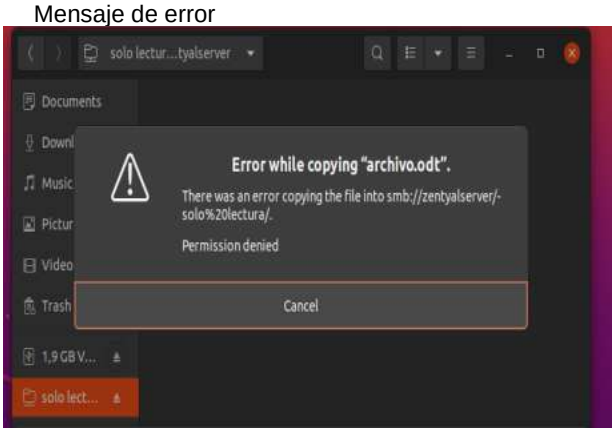

Figura 53 Mensaje de error

Para el proceso de instalación de impresoras es necesario hacer la instalación de CUPS, ya que la funcionalidad de impresoras desde el frontal de Zentyal fue deshabilitada

Para esto se debe descargar e instalar CUPS

Figura 54 Instalación de CUPS

Una vez instalado, se puede entrar a https://localhost:631 así acceder a CUPS

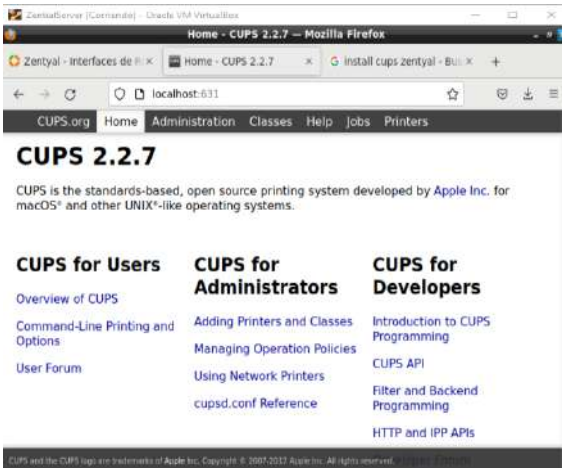

Figura 55 Acceso a CUPS

Luego seleccionamos el tipo de instalación

Figura 56 Añadir impresora

Se crea una impresora local, se marca que es compartida, desde el equipo cliente se instala la impresora también por CUPS

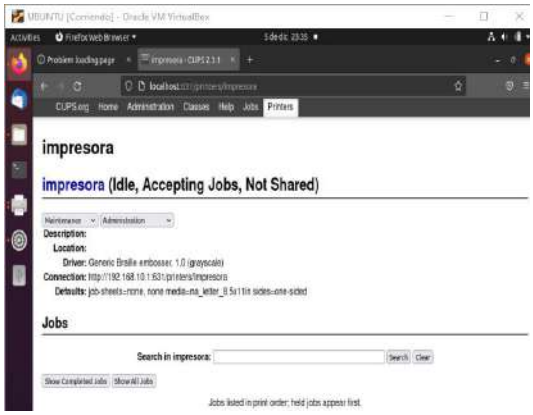

Figura 57 Instalación impresora

3.5 Temática 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Después de tener instalados los paquetes del servidor, se procederá en la utilización de los paquetes de autoridad de certificación y VPN que son instalados en el dashboard del servidor Zentyal.

Figura 58 Autoridad de certificación y VPN

Primero se debe crear el certificado de la autoridad de la siguiente forma que hay en esta imagen a continuación.

Figura 59 Creación de la autoridad de certificación.

Después de crearlo, se verá en tabla que hay en la lista de autoridades de certificación.

Figura 60 Tabla de autoridad de certificación.

Luego se creará el servidor VPN para habilitarlo.

Figura 61 Creación del servidor VPN.

Ahora ya aparece el servidor VPN habilitado en la lista de servidores.

Figura 62 Servidor VPN creado.

Ahora se debe configurar el servidor recién creado para asignar el puerto del servidor, dirección VPN, asignar el certificado de servidor con su autorización respectiva al cliente; y habilitar la interfaz TUN, la traducción de dirección de red (NAT), y permitir las conexiones cliente-cliente por si es necesario.

Figura 63 Configuración del servidor VPN

Después de la configuración, se guardará los cambios y mostrará la imagen de la ejecución del servidor VPN.

Figura 64 Ejecución del servidor VPN

Ahora se debe añadir el nombre del servicio VPN y aparecerlo en la lista de servicios.

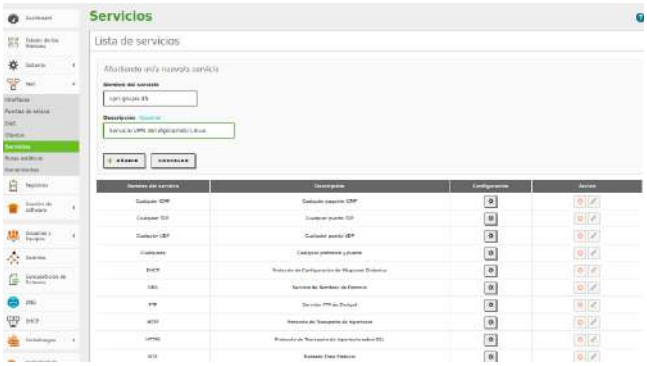

Figura 65 Adicción del servicio VPN

Figura 66 Lista de servicios VPN

Ahora se debe adicionar las reglas de filtrado desde redes internas hacia Zentyal.

Figura 67 Reglas del filtrado

Luego se procede de configurar las reglas en esta categoría

Figura 68 Filtrado de paquetes desde redes internas hacia Zentyal.

Ahora ya aparece la lista de la configuración de reglas.

Figura 69 Lista de configuración de reglas.

Después de configurar las reglas, se debe guardar los cambios, y añadir una red anunciada en el servidor VPN habilitado.

.

Figura 70 Lista de redes anunciadas.

Se puede añadir cualquier autoridad de certificación en caso de error de descargar el paquete del servidor.

Imagen 39. Lista de autoridades de certificación.

Ahora se puede descargar el paquete de configuración del cliente con siguientes parámetros.

Figura 71 Exportar configuración del servidor para Linux.

Para el caso de Windows.

Figura 72 Exportar configuración del servidor para Windows.

Luego se debe aceptar la descarga del paquete.

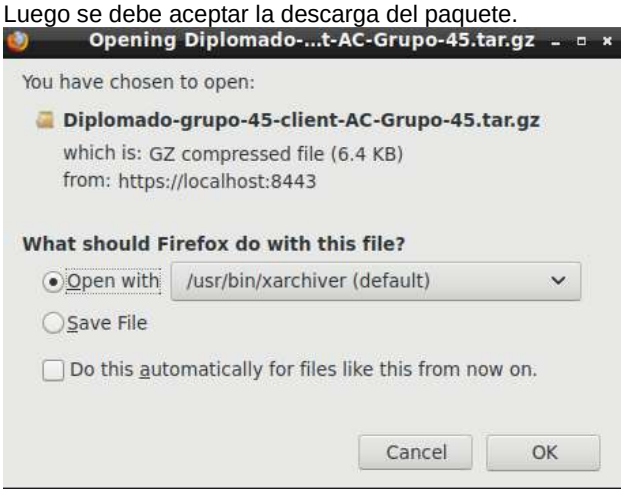

Figura 73 Descarga del paquete de configuración.

Una vez descargado, se verificará la lista de los paquetes de configuración de cliente ya descargados.

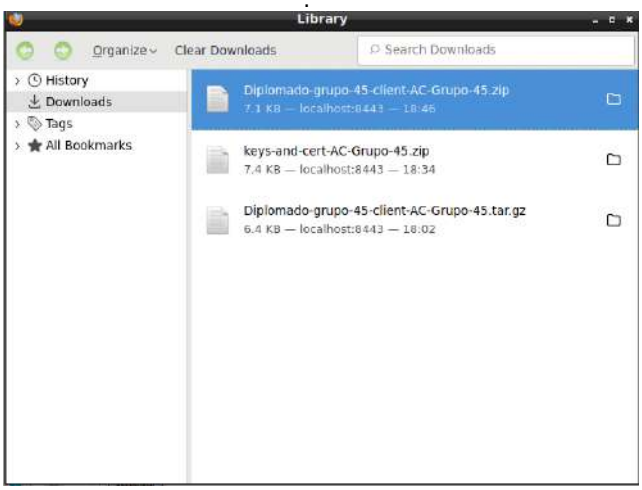

Figura 74 Lista de archivos del paquete.

Conexión del servidor VPN en Ubuntu.

Para realizar la conexión con el cliente Ubuntu Desktop, realizaremos la descarga y la instalación de los paquetes OpenVPN, Network manager y Manager OpenVPN network.

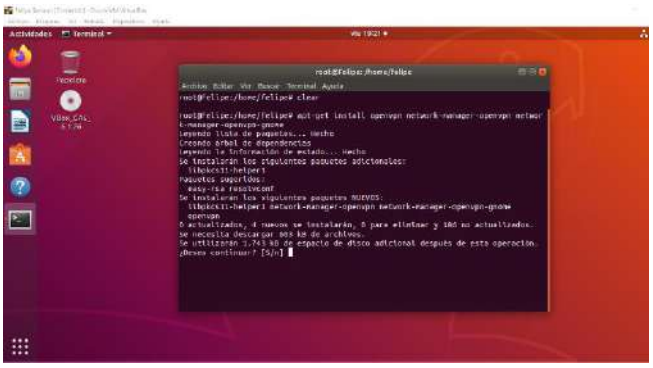

Figura 75 Instalación de los paquetes OpenVPN en Linux.

Después de la instalación, vamos a configurar la red VPN desde el menú de red en ventana de configuraciones de Ubuntu.

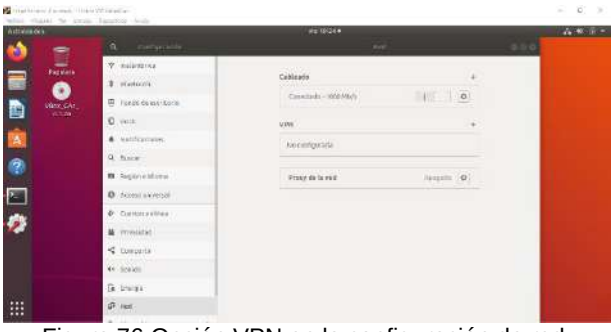

Figura 76 Opción VPN en la configuración de red.

Se verifica la carpeta que contiene el paquete de configuración del cliente.

Figura 77 Paquete de configuración en la carpeta de archivos.

En la sección de VPN en el menú de red, aparece la opción OpenVPN, que vamos a añadir.

Figura 78 Añadir VPN.

Luego vamos a importar los archivos del paquete de configuración de cliente en la red que vamos a configurar.

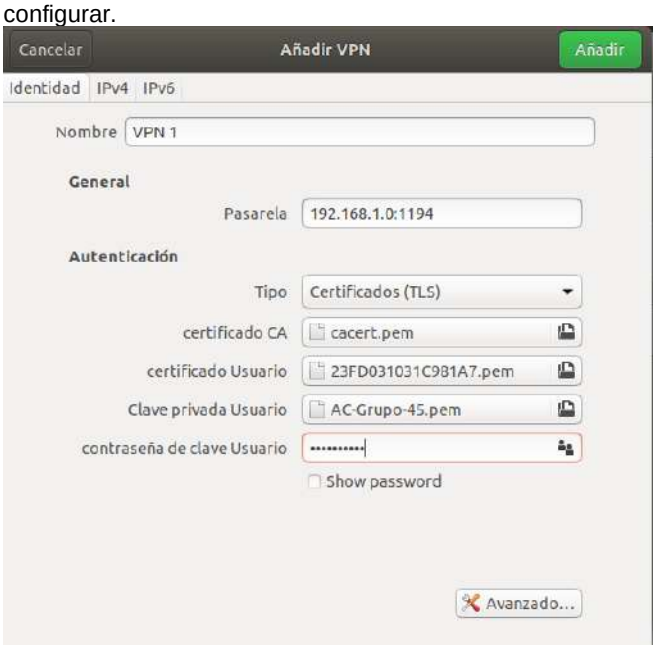

Figura 79 Importación de archivos de configuración a la red VPN.

Después de configurar la red instalada vamos a activar la red del servidor VPN ya creada desde Zentyal.

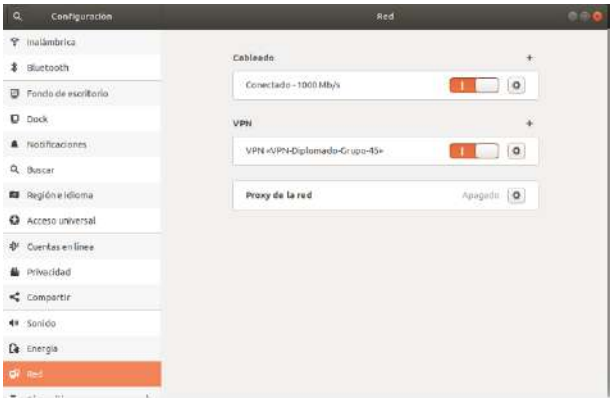

Figura 80 Red VPN instalado.

El resultado de la conexión entre el servidor VPN y el Ubuntu Desktop, es casi correcta, porque se puede generar errores de reinicio frecuente a la hora de conectarse, en caso de que se pueda dar en un parámetro de error en la certificación TLS por parte del servidor.

Conclusiones:

Solucionada gran parte de las problemáticas de migración del sistema operativo Zentyal, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, se entra en la última fase de implementación de plataformas orientadas a la administración, pero enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas. A nivel individual cada estudiante se apropie conceptual y técnicamente de como instalar, administrar y operar dicha plataforma Zentyal, con el fin de poder implementar y brindar soporte a los requerimientos de portafolios oficiales de la empresa para ofertar sus bienes y servicios oficialmente por la Web.

En la configuración de reglas del cortafuegos el parámetro con mayor relevancia se trata de la Decisión, que es allí, donde se tienen tres opciones para manejar la conexión; 1. aceptar la conexión, 2. Denegar la conexión, que es lo que se hizo en este ejercicio, donde se ignoran los paquetes entrantes y no se establece conexión y como 3. Registrar la conexión como un evento.

En la configuración de la VPN, se produjo de una forma específica, la creación de autoridades de certificación, y del servidor VPN para su formal configuración y ejecución desde del servidor, pero a la hora de conectar con el escritorio, se puede tener demoras y errores de conexión, cono en este caso de un reinicio frecuente de conexión, debido al error de certificación TLS que hay en el servidor VPN creado, en el momento de descargar el paquete de configuración para el cliente.

Adicional a lo anteriormente mencionado se logra compartir la carpeta por medio del file Server, esta carpeta se puede administrar desde la consola de Zentyal permitiendo establecer parámetros de conexión e incluso usuarios específicos con permisos específicos cobre cada carpeta, de esta manera administrar correctamente el file Server.

Bibliografía:

[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] 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

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

[4] ConfigServer Security & Firewall (csf). (s. f.). Administración de Servidores de Way to The Web Ltd. 13 de noviembre de 2021, Recuperado de: https://configserver.com/cp/csf.html

[5] Código Binario. (2020, 22 agosto). Como instalar paso a paso ISPCONFIG en Ubuntu 18.04. [Vídeo]. YouTube. Recuperado de: https://www.youtube.com/watch?v=Kf3csFfYPVU

[6] ISPConfig. (s.f). Perfect Server Automated ISPConfig 3 Installation on Debian 10 - 11 and Ubuntu 20.04. Recuperado de: https://www.howtoforge.com/ispconfig-autoinstall-debian-ubuntu/

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

[8] 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

[9] Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. (Páginas. 202 - 205). Recuperado de: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=202

[10] Torres, E. F., & Pizarro, G. A. M. (2017). Linux para usuarios. (Páginas. 333 - 338) Recuperado de: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/49434?page=333

[11] Miranda J. (09 abril 2015). Restricciones de Paginas en un Cliente utilizando Zentyal. https://www.youtube.com/watch?v=v1rn0Z4JZmk

[12] Projektfarm GmbH (s.f). Zentyal como puerta de entrada: la configuración perfecta. https://www.howtoforge.com/zentyal-as-a-gateway-the-perfect-setup-p2#-firewall

[13] Zentyal Linux Server 2004-2021 (s.f). Cortafuegos. https://doc.zentyal.org/6.2/es/firewall.html

[14] Servicio de redes privadas virtuales (VPN) con OpenVPN — Documentación de Zentyal 6.2. (2018). Zentyal Linux Server. https://doc.zentyal.org/6.2/es/vpn.html

[15] Flores, R. (2016, 2 septiembre). Realizar VPNs con Zentyal y OpenVPN – Mundo OpenIT. Openit. http://mundo.openit.com.bo/?p=925