IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT BASADA EN ZENTYAL 5.0

Edgar Augusto Martínez Barón
e-mail: eamartinezba@unad.com.co
Andrés Mauricio Quintero
e-mail: amquinterod@unadvirtual.edu.co
Andersson Morales Agredo
e-mail: amoralesag@unadvirtual.edu.co
Luis Alejandro Gómez Cuellar
e-mail: lagomezcu@unadvirtual.edu.co
Duberney Londoño Restrepo
e-mail: dlondonor@unadvirtual.edu.co

RESUMEN: *En este trabajo se implementa un servidor con el sistema operativo Zentyal en versión 5.0.1 el cual trabaja de manera centralizada la administración de los servicios, con un panel de control para configurarlos de manera correcta. Este trabajo está orientado a la administración y control de una distribución GNU/Linux basada en Ubuntu, enfocada a la implementación de servicios de infraestructura IT de mayor nivel para intranet y extranet en instituciones complejas. La distribución que se trabaja es GNU/Linux Zentyal Server 5.1 la cual es instalada y configurada como sistema operativo base para disponer de los servicios y plataformas de infraestructura IT. Los servicios y plataformas explicados en este trabajo son DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN*.

PALABRAS CLAVE: servicios de IT, Zentyal, servidores, seguridad informática.

ABSTRACT: *This work implements a server with the Zentyal operating system in version 5.0.1 which works centrally in the administration of the services, with a control panel to configure them correctly. This work is aimed at the administration and control of a GNU / Linux distribution based on Ubuntu, focused on the implementation of higher level IT infrastructure services for intranet and extranet in complex institutions. The distribution that works is GNU / Linux Zentyal Server 5.1 which is installed and configured as a base operating system to provide IT infrastructure services and platforms. The services and platforms explained in this work are DHCP Server, DNS Server, Domain Controller, Non-transparent Proxy, Firewall, File Server, Print Server and VPN*.

KEYWORDS: IT Services, Zentyal, Servers, Informatic Security

1 INTRODUCCIÓN

Zentyal Server es un sistema operativo basado en Ubuntu GNU/Linux, el permite a través del acceso en un navegador web, la administración de diferentes servicios y funcionalidades que lo han puesto como la mejor alternativa a Windows Server. Es justamente el objetivo de este trabajo, el hacer una revisión y aplicación de 5 diferentes servicios que presta Zentyal para una maquina con sistema operativo Ubuntu Desktop.

2 INSTALACIÓN DE ZENTYAL 5.0

Si bien en la actualidad el sistema operativo Zentyal se encuentra en la versión 6.0, para esta actividad se ha utilizado la versión 5.0.

Zentyal está concebido para ser instalado de forma exclusiva en una máquina, ya sea virtual o física, pero esto no impide que se puedan instalar más herramientas o servicios conjuntamente. Se debe tener en cuenta que estos últimos no serán administrados desde Zentyal

2.1 REQUISITOS

Los requerimientos de hardware para instalar Zentyal dependen de los módulos que se vayan a instalar, la cantidad estimada de usuarios que usarán el sistema y los hábitos de uso.

Si el uso de Zentyal es como puerta de enlace o cortafuegos, es necesario tener al menos dos tarjetas de red. Si solo se va a usar como servidor, una sola tarjeta de red es suficiente.

Para un Zentyal de uso general, con una cantidad de usuarios inferior a 50, los requerimientos mínimos recomendados serían: memoria de 2 Gb, espacio en disco de 80 Gb, procesador con 2 cores y las tarjetas de red de acuerdo con los servicios a implementar.

2.2 INSTALADOR

Se puede obtener una imagen iso desde el sitio web https://zentyal.com/community/ en donde se encuentran desde la versión 2.2 hasta la versión 6.1. La imagen se puede descomprimir para hacer un CD o USB booteable.

2.3 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Como procedimiento previo para la máquina virtual que contiene al sistema operativo Zentyal, se debe seleccionar un fichero en donde quede contenida la imagen del disco virtual, al menos 2 Gb de RAM, usar el formato VDI como tipo de archivo, el almacenamiento

reservado dinámicamente y un tamaño de 20 Gb de almacenamiento.

Luego de crear la máquina virtual, se deben aplicar configuraciones adicionales. Estas incluyen: agregar la imagen de instalación del sistema operativo en la unidad óptica, habilitar dos adaptadores de red, el primero adaptador como puente y el segundo como solo anfitrión; y por último crear una red de anfitrión en donde se configure el direccionamiento IP y se deshabilite el direccionamiento por DHCP.

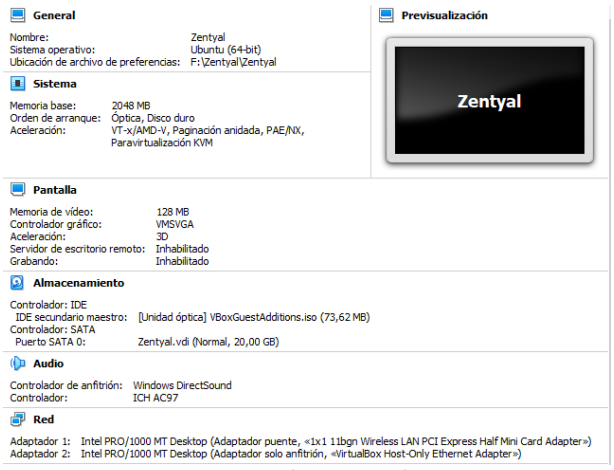

Figura 1. Configuración de la máquina virtual

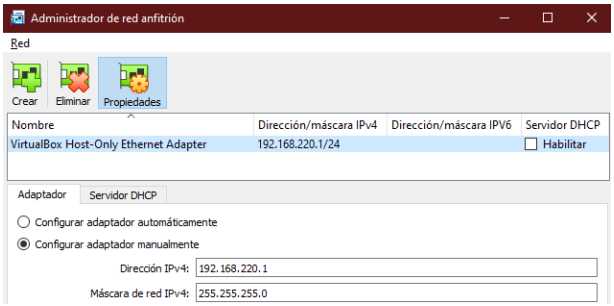

Figura 2. Administrador de red de anfitrión

2.4 PROCESO DE INSTALACIÓN

Finalizada la configuración de la máquina virtual, se inicia el proceso de instalación, en donde se debe seleccionar un lenguaje para la interfaz del instalador.

El proceso de instalación es similar al que se lleva a cabo para instalar Ubuntu desktop y es normalmente sencillo [1].

Se elige el lenguaje que usará el sistema operativo, una ubicación geográfica, la configuración del teclado, el adaptador de red principal, el nombre del servidor, el nombre del administrador que tendrá privilegios de root, la contraseña del administrador y la confirmación de esta que también sirven para las conexiones por SSH y la ubicación geográfica. Terminados estos pasos se inicia el proceso instalación que puede tardar hasta 20 minutos.

Finalizado el proceso de instalación se debe retirar la imagen de la unidad óptica y reiniciar el sistema operativo.

2.5 MÉTODO DE INGRESO

La primera vez que se inicie el sistema, se abre un explorador web en donde se debe aplicar la excepción de seguridad para iniciar el panel de control del Zentyal. El enlace de acceso guarda la siguiente estructura: https://IP_o_hostname:8443

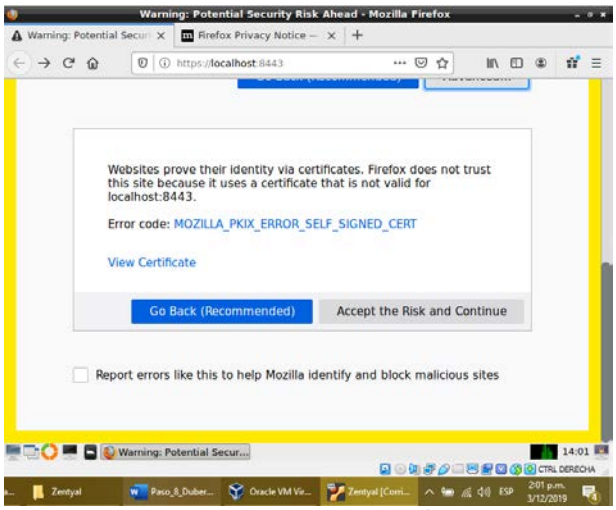

Figura 3. Aplicar regla de excepción

Luego se deben ingresar los datos de las credenciales del administrador creadas en la instalación. Se debe tener presente que solo se puede acceder a la GUI de administración web a través de HTTPS (no HTTP simple) y se encuentra en el puerto 8443 de forma predeterminada.

2.6 DESCARGA DE PAQUETES

Para implementar servicios de infraestructura IT se deben descargar los paquetes para la instalación de las herramientas que soportan estos servicios. Se seleccionan y se da en instalar.

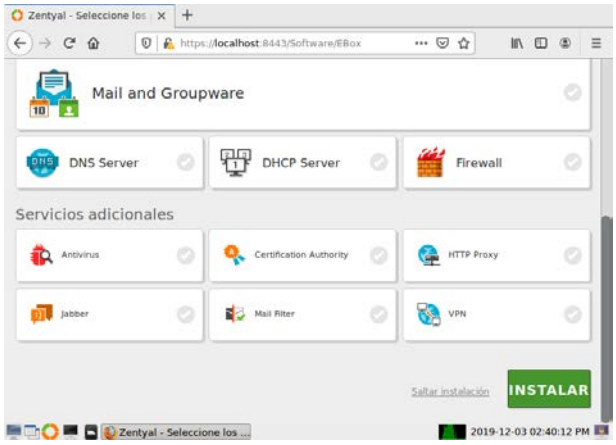

Figura 4. Herramientas de Zentyal

Posterior a la selección de los paquetes, se confirman y se inicia la instalación. Al terminal este proceso se va a solicitar configurar las interfaces de red. La interfaz que tiene el acceso a internet se configura como externa y la interfaz que sirve de conexión a la subred como interna.

Figura 5. Tipos de interfaces de red.

Seleccionadas las configuraciones de red se debe establecer el direccionamiento IP. Para la red externa la selección de IP se hará por DHCP y para la red interna de forma manual escribiendo una IP de acuerdo con la red anfitrión para VirtualBox y usando la misma máscara.

Figura 6. Direccionamiento IP de interfaces de red.

Posteriormente se debe establecer al servidor como controlador de dominio (Stand-alone) y escribir un nombre de dominio que debe ser diferente al nombre del host.

Figura 7. LDAP y nombre de dominio.

Para finalizar se guardan las configuraciones y se identifica el direccionamiento IP como constatación desde la terminal con el comando ip a s

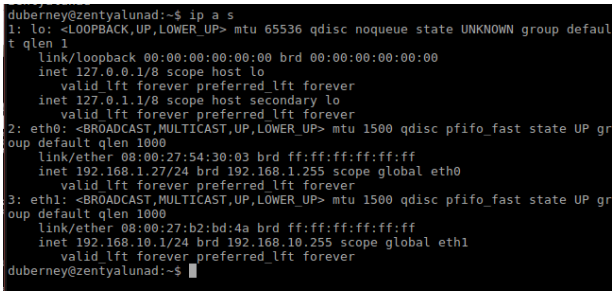

Figura 8. Direcciones IP.

3 IMPLEMENTACIÓN DE SERVICIOS

En la administración y control de servicios para intranet y extranet se establece la instalación, configuración y puesta en marcha de las herramientas para DHCP, DNS, controlador de dominio, proxy no transparente, cortafuegos, acceso a carpetas compartidas e impresoras a través de LDAP y VPN

3.1 DHCP, DNS Y CONTROLADOR DE DOMINIO

Las interfaces de red deberán estar configuradas de la siguiente manera.

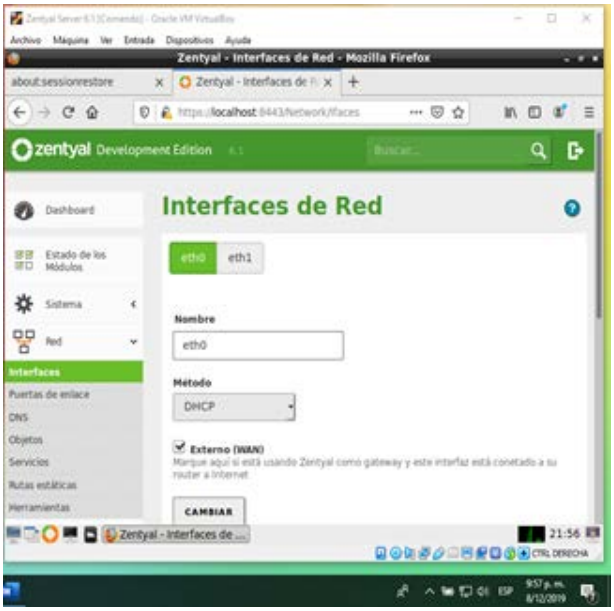

Figura 9. Interfaz de red eth0.

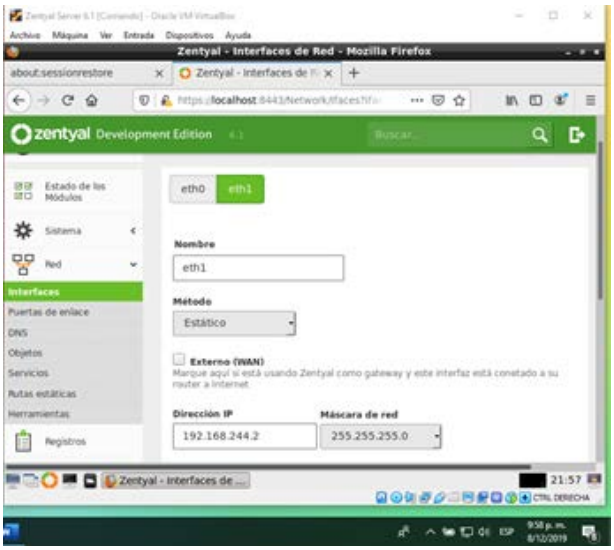

Figura 10. Interfaz de red eth1.

Se configura el dominio, asignando el tipo de servidor como servidor stand-alone y se asigna un nombre.

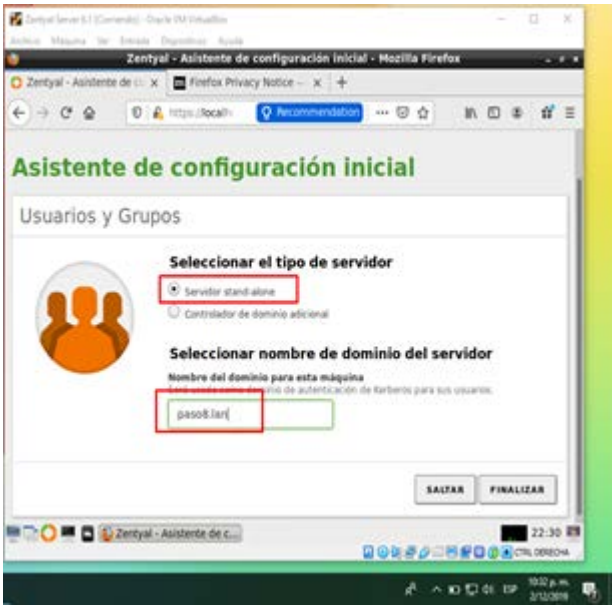

Figura 11. Controlador de dominio

El módulo DHCP deberá estar activado para iniciar con esta tarea.

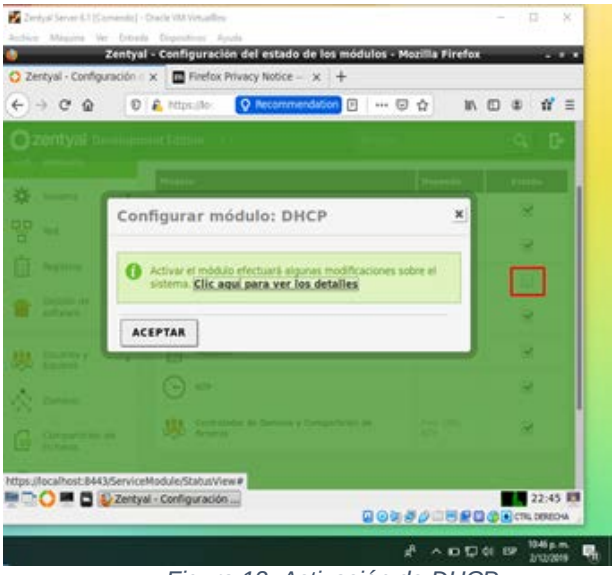

Figura 12. Activación de DHCP.

Una vez activado método DHCP, se asigna un rango de dirección IP permitidos.

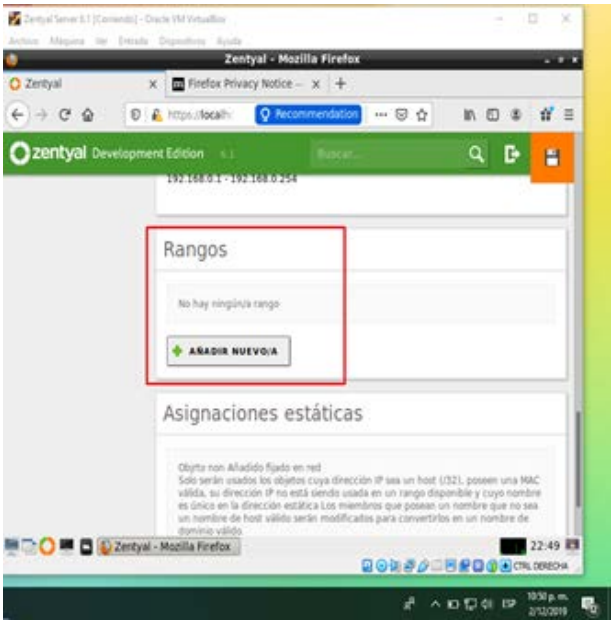

Figura 13. Creación de rangos de IP

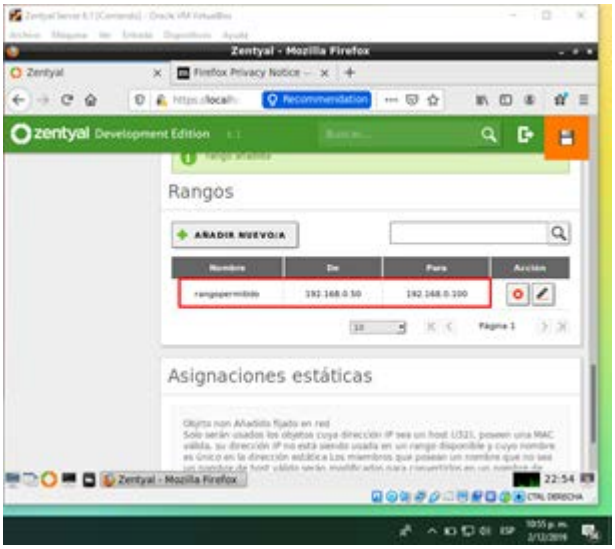

Figura 14. Rangos IP establecidos.

Para verificar que el método DHCP asigne una IP dinámica a un cliente Ubuntu se debe tener la maquina con un adaptador de red local o anfitrión. Se verifican las configuraciones de red y el dashboard del zentyal server que tenga una Ip asignada del rango generado y que releje el equipo en widget del dashboard.

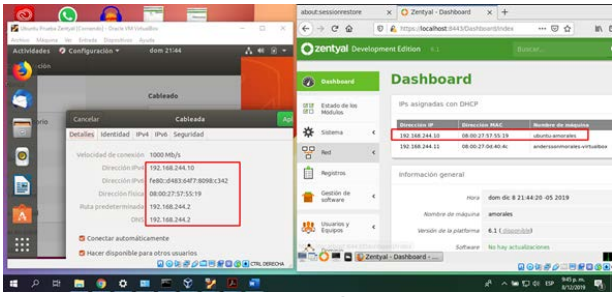

Figura 15. Asignación de IP por DHCP.

Para la autenticación de usuarios, se deberá crear un usuario y se le asignará permisos de administrador para tener los privilegios suficientes para pruebas. Para ello se va a la opción Usuarios y equipos en el menú de administración del dashboard.

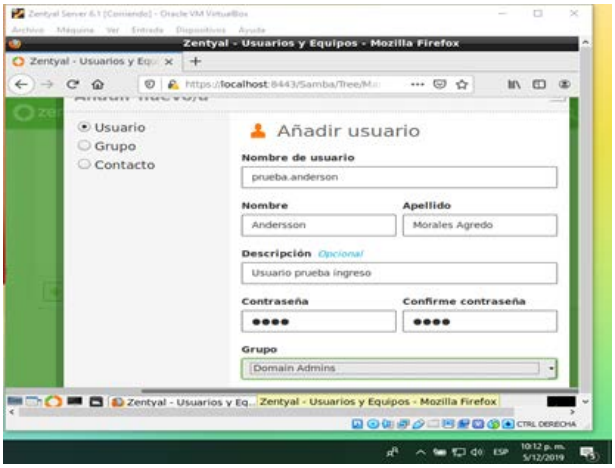

Figura 16. Usuarios de Zentyal.

Una vez creado el usuario, se sube la maquina cliente Ubuntu a nuestro dominio para poder autenticarnos. Se descarga la herramienta pbis-open del siguiente enlace: https://github.com/BeyondTrust/pbis-open/releases

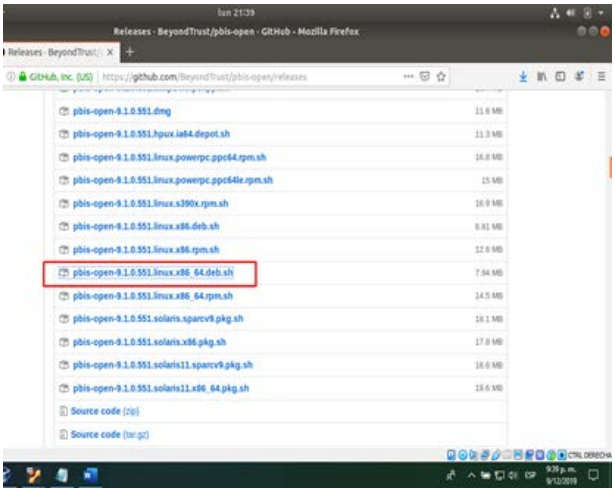

Figura 17. Pbis-open.

Se va a la ruta de instalación, se asignan los permisos de ejecución.

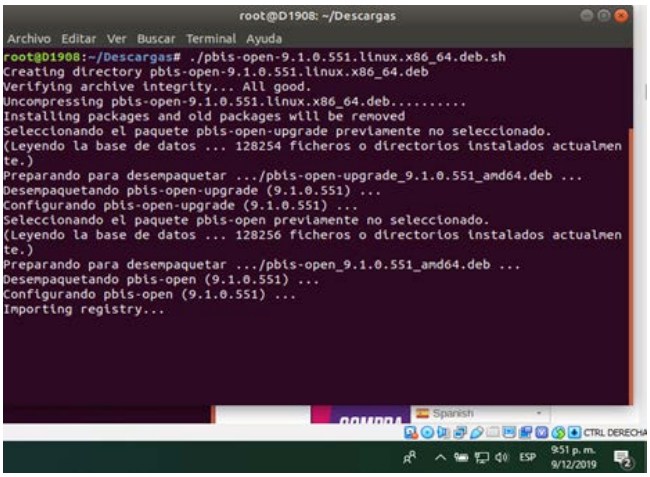

Figura 18. Permisos para Pbis-open.

Se sube el equipo al dominio.

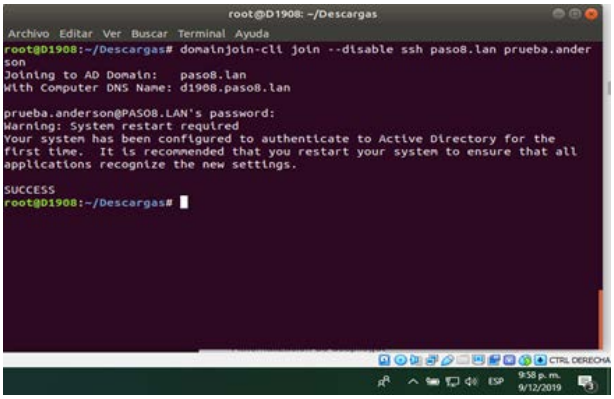

Figura 19. Enlace del host con el servidor.

Se accede al equipo y se ingresa con el usuario creado en el servidor Zentyal.

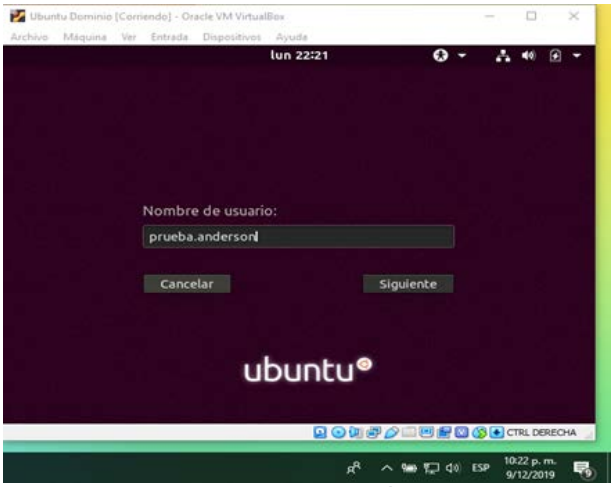

Figura 20. Inicio de sesión con usuario.

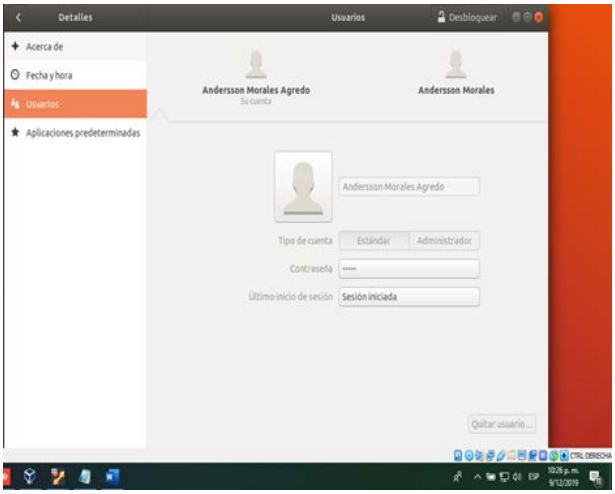

Figura 21. Usuario en uso.

3.2 PROXY NO TRANSPARENTE

Para realizar la configuración de un proxy no transparente se deben instalar las herramientas a continuación

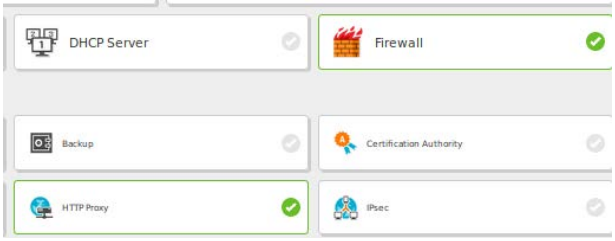

Figura 22. Herramientas para Proxy

3.2.1 ETH0

Se dirige a Red > interfaces, para este caso se trabaja con 2 interfaces de red. La primera red eth0, se configura por el DHCP, esta será la red de la máquina

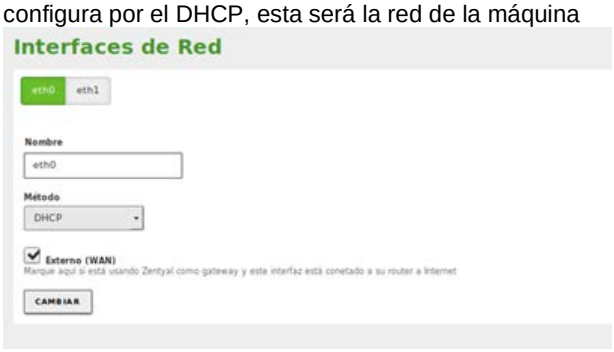

Figura 23. Interfaces para el proxy

3.2.2 ETH1

La segunda interfaz de red, para el caso, es eth1, se configura como estática en este caso con la IP 192.168.56.2 que será la dirección del proxy

Figura 24. Interfaz eth1 para el proxy

3.2.3 CONFIGURACIÓN GENERAL DE PROXY

Se ingresa a la configuración del proxy HTTP. Se verifica que el puerto por el cual se encuentra configurado es 3128, y que este no se encuentre como un proxy transparente.

Figura 25. Perfiles de filtrado

3.2.4 CREACIÓN DE REGLAS DE PERFIL

Se va a la configuración de reglas del perfil y se realiza la acción de denegar a Los sitios Youtube.com e Instagram.com y permitir acceso a Facebook.com, se agregan las reglas al perfil.

Figura 26. Reglas de dominio.

3.2.5 ACTIVACIÓN EL PROXY

Ahora se despliega la configuración del Proxy; entonces se cambia la regla principal. En la 'Decisión' se usa el perfil unad_aquintero creado anteriormente.

Figura 27. Configuración reglas de acceso.

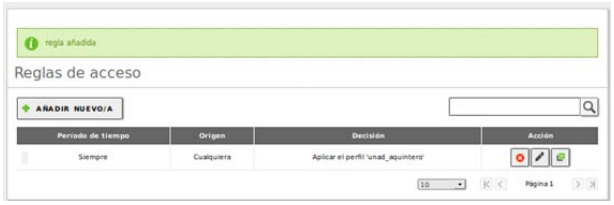

Figura 28. Reglas de acceso creadas.

3.2.6 CONFIGURACIÓN DE PROXY EN MÁQUINA

Se configura el proxy, con la IP y puerto del servidor Zentyal.

Figura 29. Proxy de la red

3.2.7 CONFIGURACIÓN DE PROXY EN NAVEGADOR

Se va al navegador y se configura para que tome el proxy establecido en el equipo

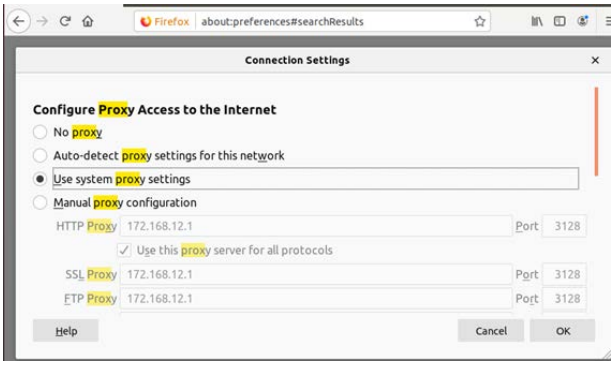

Figura 30. Configuración proxy en navegador

3.3 CORTAFUEGOS

Para establecer la configuración del cortafuegos en Zentyal, se debe contar con las herramientas DNS server y Firewall.

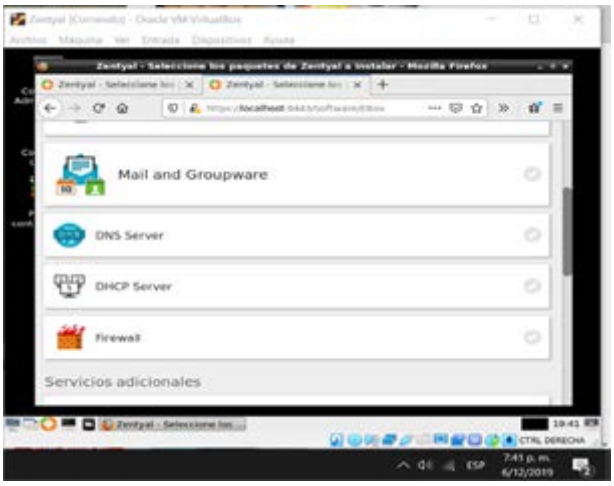

Figura 31. Herramientas para cortafuego

Se realiza la configuracion de las tarjetas de red, dede el menú se encuentra la opcion RED >> Interfaces.

3.3.1 ETH0

Para esta tarjeta de red se selecciona el método DHCP, y se marca la opcion de Externo (WAN) ya que esta debe tener acceso al internet.

Figura 32. Interfaz eth0 para cortafuego

3.3.2 ETH1

Para esta tarjeta de red se selecciona el método Estático, y se asigna una direccion IP.

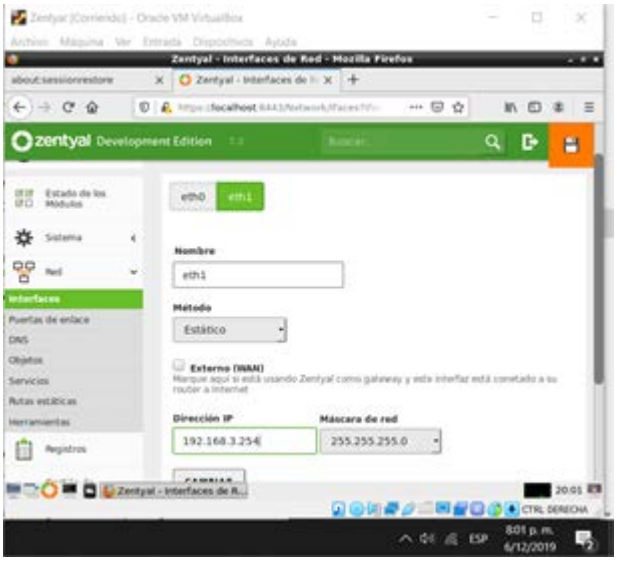

Figura 33. Interfaz eth1 para cortafuego

Realizada la configuración, en el menú CORTAFUEGOS >> Filtrado de Paquetes, se busca la seccion de reglas de filtrado para redes internas. Y desde allí se tiene la opción para añadir una nueva regla.

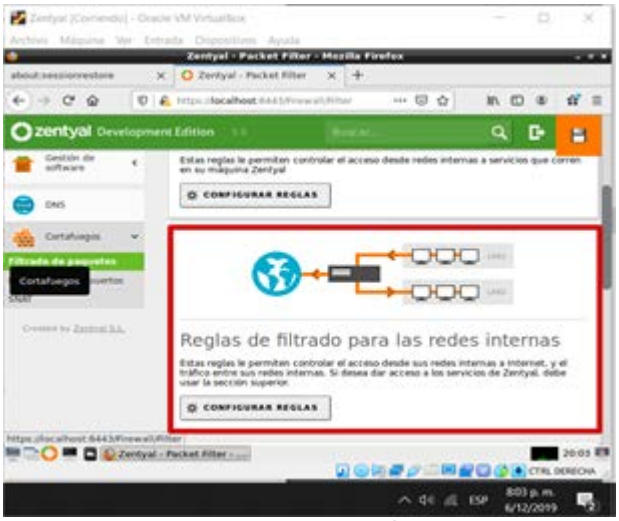

Figura 34. Configuración de reglas.

3.3.3 BLOQUEO DE REDES

Se bloquera el acceso a Facebook, youtube, spotify y skype, para eso es necesario las ip con las que acceder, se abre una consola de comando y se realiza ping a estos dominios, como lo indica la imagen.

Figura 35. IP de los host.

Una vez obtenidas las ip, se crean las reglas, negando el acceso.

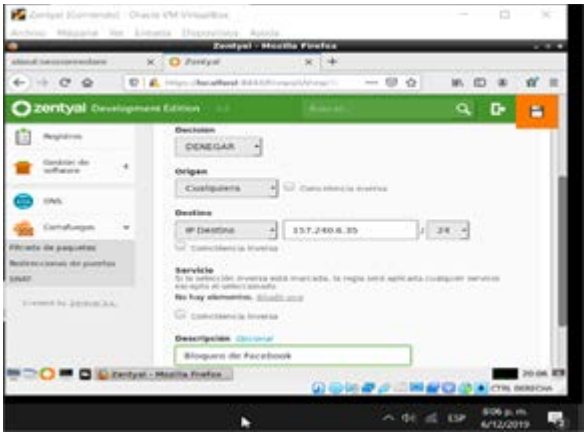

Figura 36. Reglas para negar acceso primer IP

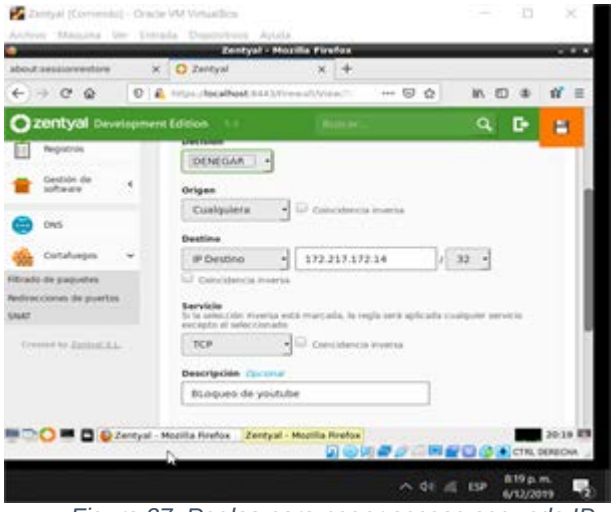

Figura 37. Reglas para negar acceso segunda IP.

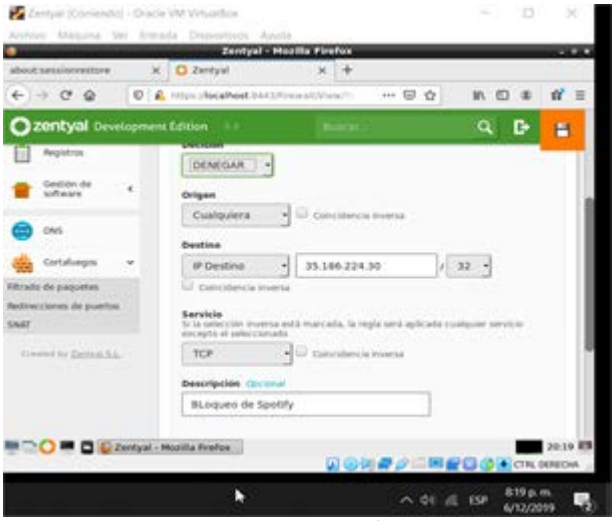

Figura 38. Creación de regla

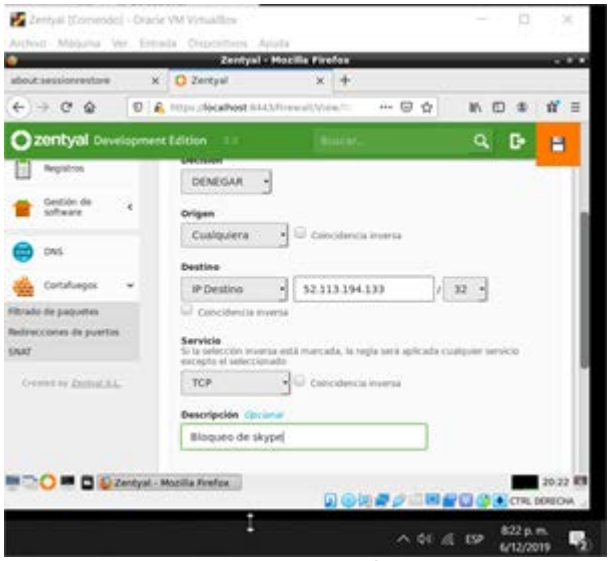

Figura 39. Creación de regla

3.3.4 CLIENTE

Se ingresa a la máquina cliente Ubuntu, creando una nueva red manual, en la pestaña Ajustes de IPV4; Se registra una ip en el mismo segmento del servidor Zentyal, y en la puerta de enlace y DNS se ubica la IP de Zentyal

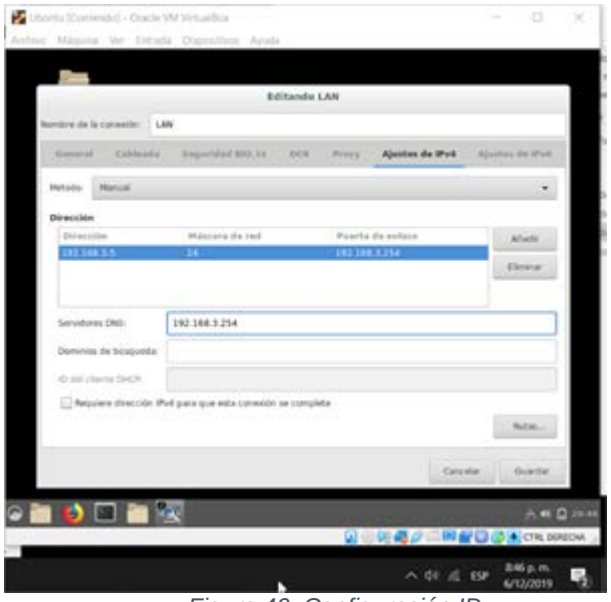

Figura 40. Configuración IP

Se valida la configuración, primero se elimina la regla de Facebook y se comprueba que la maquina cliente acceda

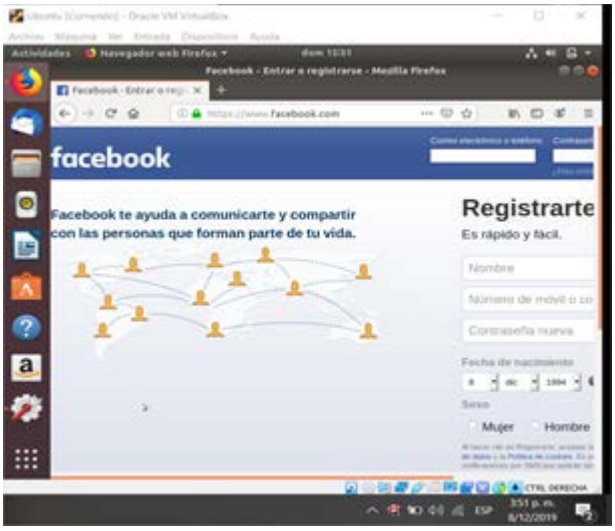

Figura 41. Acceso a Facebook

Como se observa, se puede acceder. Se volverá a crear la regla y se refresca de nuevo.

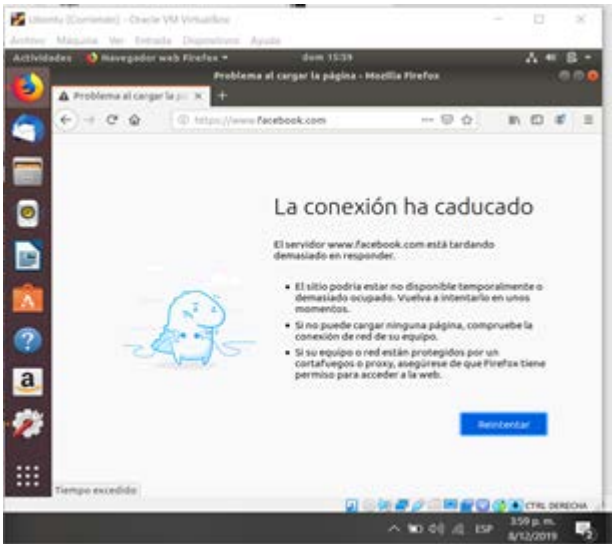

Figura 42. Acceso denegado a Facebook

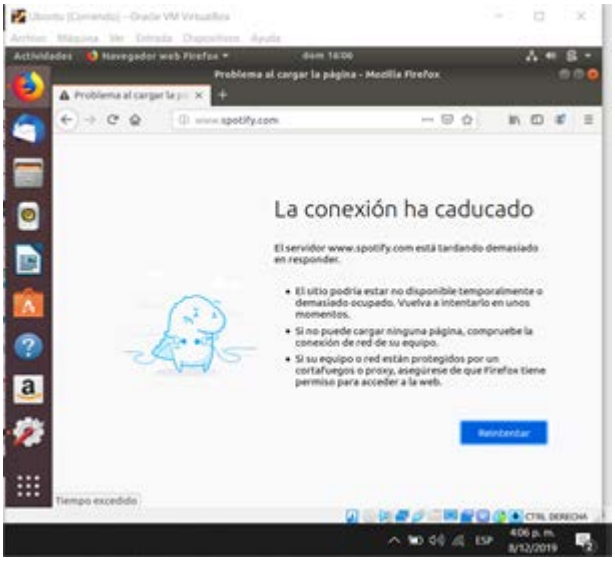

Figura 43. Acceso denegado a Spotify

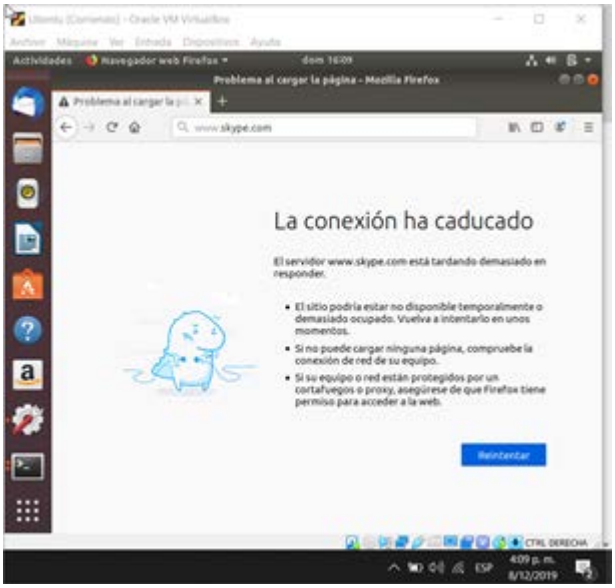

Figura 44. Acceso denegado a Skype

3.4 FILE SERVER Y PRINT SERVER

Zentyal usa LDAP para configurar un controlador de dominio Windows integrado con Samba como servidor de directorio para la compartición de ficheros.

Las configuraciones previas que se requieren para la compartición de ficheros son la asignación de un rango de IP por DHCP para que el sistema operativo Ubuntu Desktop tome una de estas direcciones IP. Función del servidor como controlador de dominio y un nombre de dominio. También se debe configura el traductor de dominios [1].

Figura 45. Controlador de dominio.

Para el sistema operativo Ubuntu, este debe tener una interfaz de red anfitrión para conectarse a la red interna de Zentyal. Se debe poder hacer ping desde Ubuntu a Zentyal y de forma recíproca, desde Zentyal a Ubuntu. También se debe usar el comando nslookup *midominio* para constatar que se reconoce la IP del dominio configurado en Zentyal desde Ubuntu.

3.4.1 CREACIÓN DE USUARIOS Y GRUPOS

Para poder establecer permisos a ficheros, se deben crear usuarios en Zentyal desde el módulo de usuarios y equipos [2].

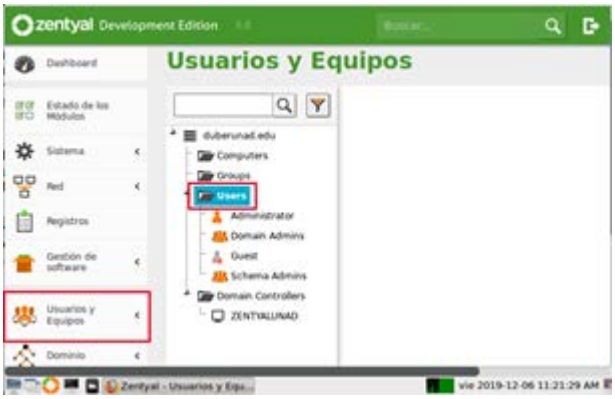

Figura 46. Módulo de usuarios y equipos

Primero se crea un usuario al que se le dan permisos de administrador al agregarlo al grupo Domain Admins. Este usuario se configura con un nombre y una contraseña.

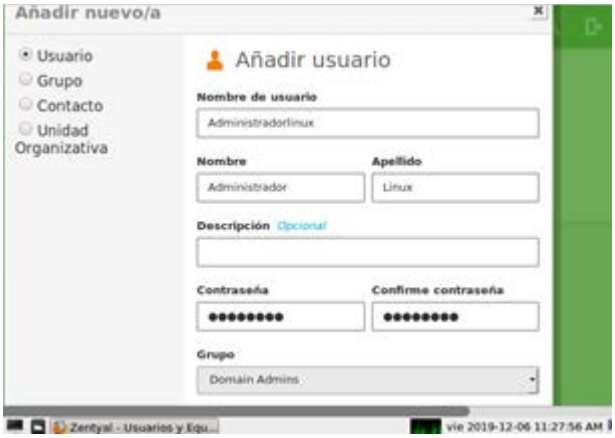

Figura 47. Crear un usuario administrador.

Luego se pueden crear los usuarios de acuerdo con las necesidades. Cada usuario debe llevar un nombre y una contraseña. La contraseña puede configurarse con un tiempo de caducidad y que sea renovada por el mismo usuario.

Figura 48. Crear un usuario.

Para administrar permisos a dos usuarios o más, se establecen grupos y a estos se les asignan los usuarios. De esta forma al dar permisos a un grupo, todos los usuarios quedan con los mismo permisos. Para ello, desde el mismo modulo, pero desde la opción grupos se adiciona un grupo al cual se establece como grupo de distribución, se le da un nombre y una descripción para la documentación.

Figura 49. Crear un grupo.

Luego se selecciona el grupo creado y se le añaden los usuarios. También es posible añadir un usuario al grupo cuando se está creando el usuario.

3.4.2 COMPARTICIÓN DE FICHEROS

Desde el módulo de compartición de ficheros se puede crear un nuevo recurso compartido, establecer la ruta hacia el recurso y agregar un comentario para la documentación.

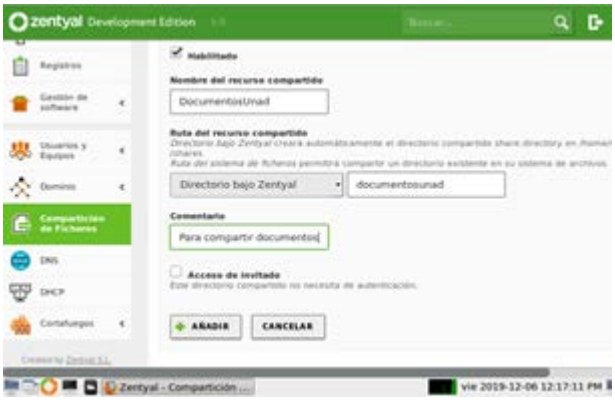

Figura 50. Recurso compartido.

Luego, desde el control de acceso del fichero creado se pueden adicionar las listas de acceso, estos son los grupos o usuarios que pueden acceder al fichero y el tipo de permisos, ya sean de administrador, de lectura y escritura o solo lectura.

Figura 51. Control de acceso.

3.4.3 COMPARTICIÓN DE IMPRESORAS

Se debe instalar el servicio de CUPs, ya que es desde este que se administran las impresoras. Se usa el comando

sudo apt-get install cups

```
duberney@zentyalunad:~$ sudo apt-get install cups
[sudo] password for duberney:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bc cups-client cups-common cups-core-drivers cups-daemon cups-filters
  cups-filters-core-drivers cups-ppdc cups-server-common ghostscript gsfonts
  imagemagick imagemagick-6.q16 imagemagick-common libcupscgi1 libcupsmime1
  libcupsppdc1 libfftw3-double3 libfontembed1 liblqr-1-0 libltdl7
  libmagickcore-6.q16-2 libmagickwand-6.q16-2 libqpdf21 libusb-1.0-0
  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 hpijs imagemagick-doc autotrace cups-bsd | lpr | lprng
  enscript ffmpeg gimp gnuplot grads graphviz hp2xx html2ps libwmf-bin mplayer
  povray radiance sane-utils texlive-base-bin transfig ufraw-batch xdg-utils
  libfftw3-bin libfftw3-dev libmagickcore-6.q16-2-extra openssl-blacklist
```

Figura 52. Descarga de CUPS

También se debe instalar el controlador para la impresora que se use. Se usa una impresora virtual para pdf con el comando

sudo apt-get install cups-pdf

```
duberney@zentyalunad:~$ sudo apt-get install cups-pdf
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libpaper-utils printer-driver-cups-pdf
Paquetes sugeridos:
  system-config-printer-gnome | system-config-printer-kde
  | system-config-printer
Se instalarán los siguientes paquetes NUEVOS:
  cups-pdf libpaper-utils printer-driver-cups-pdf
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 101 no actualizados.
Se necesita descargar 43,6 kB de archivos.
Se utilizarán 201 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 53. Descarga de controlador de impresora

Luego se accede a través de un explorador web al administrador de CUP, ya que no se usa el panel de Zentyal. Para ello se usa el puerto 631

https://localhots_o_IP:631/admin

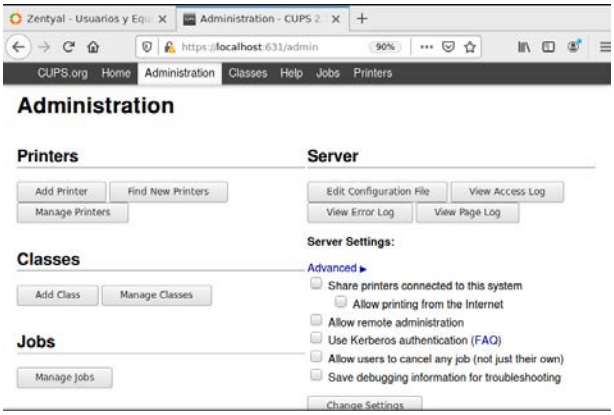

Figura 54. Panel de administracción de CUPS

Desde la sección Printers, en la opción Add Printer se pueden agregar las impresoras a gestionar. Se pedirán las credenciales del usuario administrador para acceder al recurso.

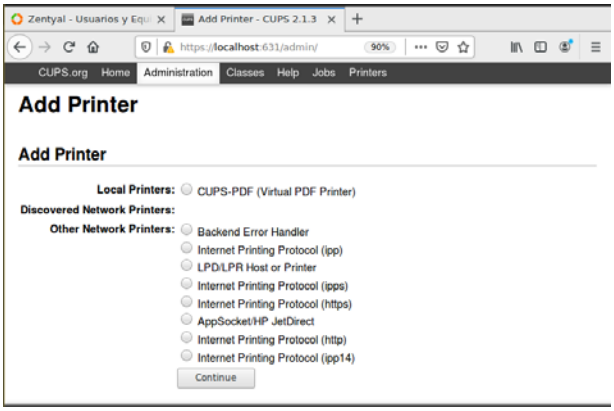

Figura 55. Listado de impresoras

Se identifica la impresora local, que corresponde aquella a la que se ha descargado los controladores (impresora virtual).

Figura 56. Selección de impresora

Se asigna el nombre a la impresora, una descripción y una ubicación. A demás se chulea la casilla de Share this printer (compartir esta impresora)

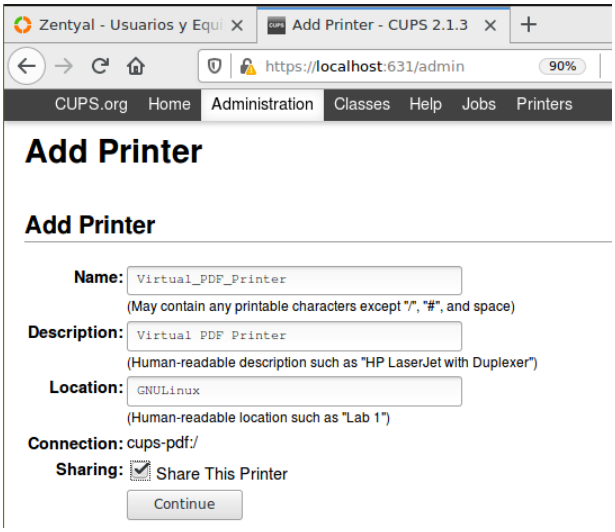

Figura 57. Metadatos de la impresora

Posteriormente, se debe establecer el fabricante, modelo y controlador de impresora a utilizar. También existe la opción de subir un fichero PPD proporcionado por el fabricante, en caso de que el modelo de impresora no aparezca en la lista.

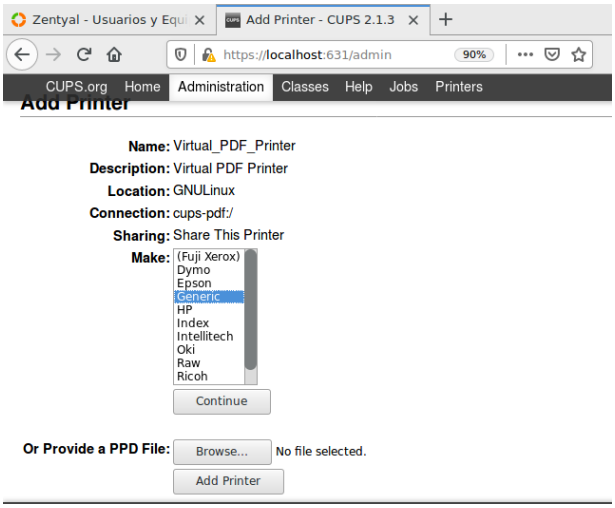

Figura 58. Selección del fabricante

Finalmente se tiene la opción de configurar los parámetros de impresión

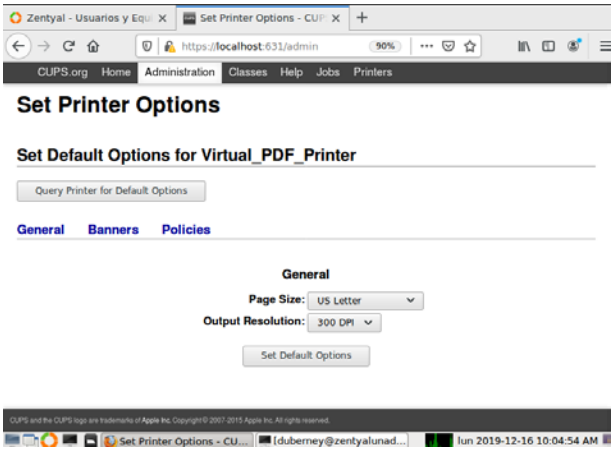

Figura 59. Parámetros de impresión

Terminada la configuración se pueden ver los trabajos de impresión pendientes

Se hace una prueba con para verificar.

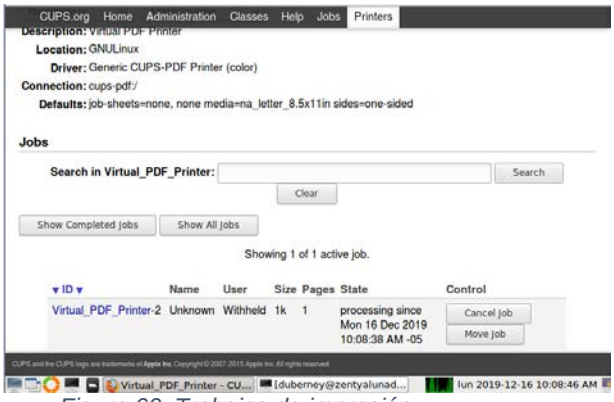

Figura 60. Trabajos de impresión

3.4.4 ACCESO A RECURSOS COMPARTIDOS

Desde el sistema operativo Ubuntu que se encuentra conectado a la red interna del servidor Zentyal se accede al recurso compartido usando el administrador de archivos Nautilus. Para ello se debe seleccionar la opción de otras ubicaciones y escribir la dirección IP del servidor o el dominio usando la sintaxis smb://*midominio_o_miIP* en la casilla de conectar con servidor y dar clic en conectar

Figura 61. Uniendo el cliente Ubuntu.

Se presentan los ficheros y recursos compartidos. Para acceder a uno de ellos, se debe seleccionar.

Figura 62. Recursos compartidos.

Para el recurso seleccionado se pedirán las credenciales. Que deben coincidir con las establecidas en el servidor Zentyal.

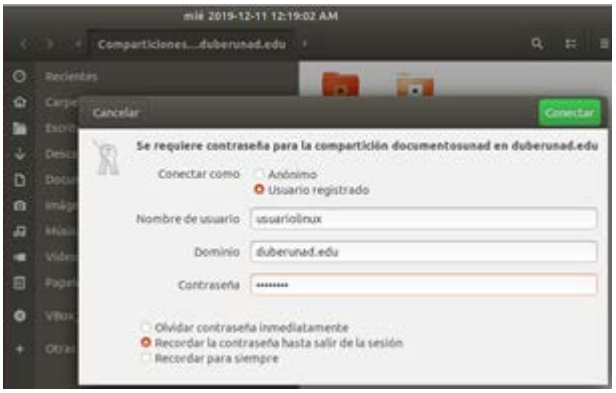

Figura 63.Credenciales para acceso a recurso.

Si las credenciales son correctas y los permisos establecidos lo permiten, se tiene acceso al contenido.

Figura 64. Acceso efectivo al recurso.

3.5 VPN

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Se puede configurar Zentyal para dar soporte a clientes remotos, a través del servicio VPN, ya que un servidor Zentyal, trabaja como puerta de enlace y como servidor VPN, que tiene una red local detrás, permitiendo a clientes externos conectarse a dicha red local.

Para este punto, manejan dos máquinas virtuales, una para el servidor Zentyal y otra para la maquina cliente con el sistema operativo Ubuntu Desktop. Ambas maquinas tienen dos adaptadores uno en Bridge y el otro en Red Interna.

3.5.1 CONFIGURACIÓN DE SERVIDOR VPN

Tras instalar el servidor y los paquetes necesarios que son Cortafuegos o Firewall, Autoridad de certificado y VPN, se configuran las dos interfaces del servidor (eth0 y eth1), las cuales para este punto se manejaron eth0 como externa y eth1 como interna y ambos con IP dinámica es decir DHCP.

Tras configurar esto, los primero que se realiza es generar el certificado de autenticidad del servidor Zentyal, esto se realiza en el Menú “Autoridad de Certificación” en la sección “General”. En el formulario se ingresa el nombre que aparecerá en certificado y el tiempo de vigencia. [3]

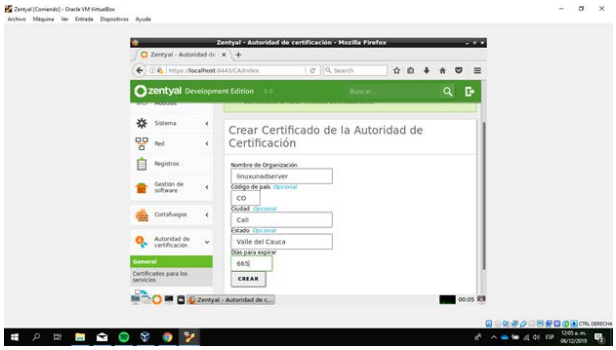

Figura 65. Certificado de autenticidad.

Con el certificado creado, se procede a generar el servidor VPN, para ello se debe ir al Menú “VPN” y a la sección “Servidores”. Se añade un nuevo servidor el cual por ahora debe estar inhabilitado

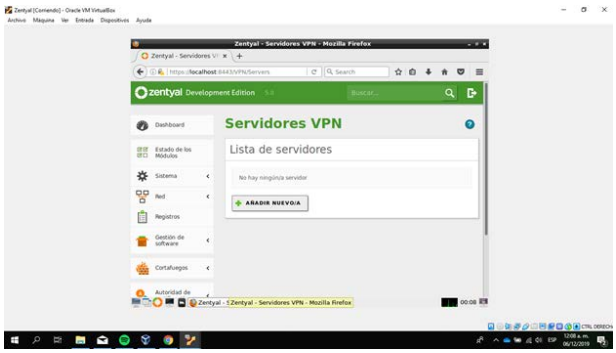

Figura 66. Generar servidor VPN

Tras haber generado el servidor VPN, se debe generar el certificado de este. Para ello se regresa al menú “Autoridad de certificados a la sección “General” y se llena la información.

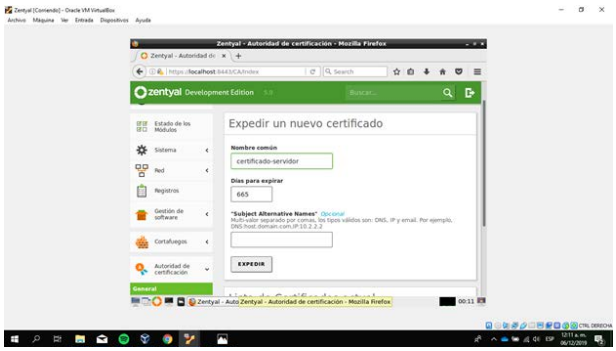

Figura 67. Autoridad de certificados a la sección

Una vez el certificado se genera, se debe configurar el servidor VPN Generado. Para ello se va al menú “VPN” a la sección “Servidores” y se accede a la configuración del servidor VPN. Aquí se define el Puerto del servidor el cual es UDP y se deja el túnel por defecto. Se deja la dirección VPN que esta por defecto, aunque si se desea se puede cambiar; se selecciona el certificado del servidor recién generado y se habilita la interfaz TUN.

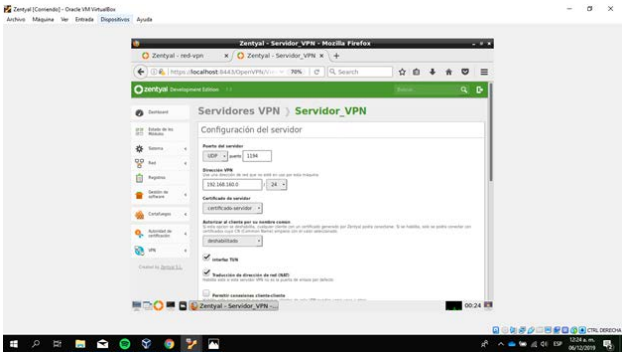

Figura 68. Interfaz TUN

3.5.2 CREACIÓN DEL SERVICIO VPN

Ya con el servidor VPN configurado, se debe generar el servicio que funciona con el servidor. Por ello se va al menú "Red" y a la sección "Servicios". Allí se genera un nuevo servicio.

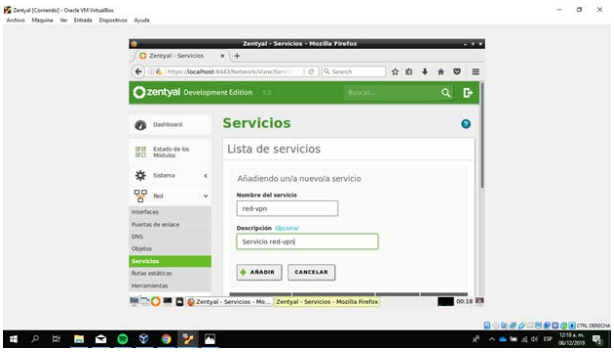

Figura 69. Nuevo servicio VPN.

Tras añadir el servicio, se debe configurar; para ello se accede a la configuración del servicio creado, se agrega un nuevo perfil de configuración y se ingresa la misma información del puerto del servidor VPN creado, en donde el puerto de origen puede ser cualquiera y el puerto de destino es el mismo del servidor VPN. [4]

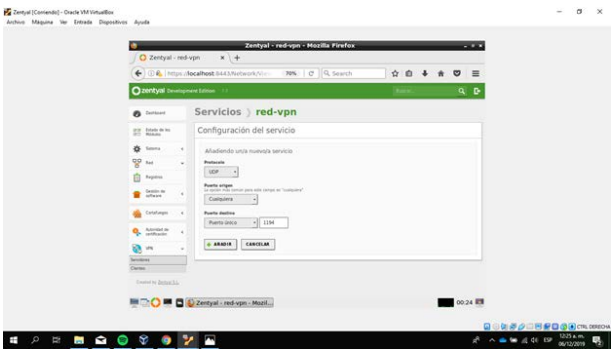

Figura 70. Puertos del servidor VPN

3.5.3 ESTABLECIMIENTO DE LA REGLA DE FIREWALL

Con el servicio ya configurado, se debe ahora establecer la regla en el Firewall que permitirá la conexión con el servidor a través del servicio generado. Para ello se accede al menú "Cortafuegos" a la sección "Filtrado de paquetes". Aquí se debe acceder a la opción "Configurar Reglas" de la sección "Reglas de filtrado desde las redes internas a Zentyal". Allí se debe indicar que la decisión es de aceptación desde cualquier origen y usando el servicio VPN generado. [4]

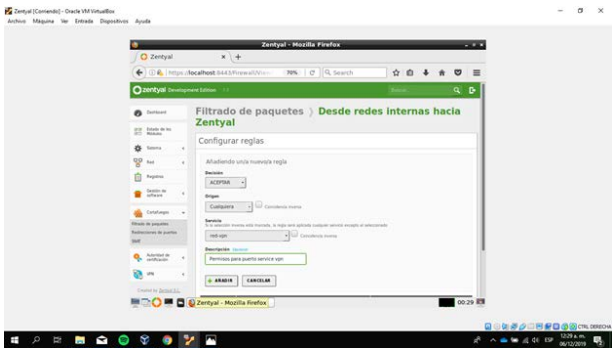

Figura 71. Reglas de filtrado para VPN

Con esto realizado, se regresa al servidor VPN y se accede a la configuración de redes anunciadas. Aquí se debe agregar una nueva red anunciada cuyo nombre puede ser cualquiera.

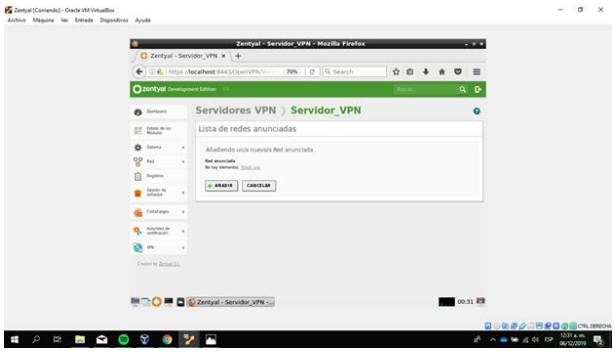

Figura 72. Red anunciada

3.5.4 PAQUETE DE CONFIGURACIÓN DE CLIENTE

Tras generar la lista de redes se debe descargar el paquete de configuración que usará el cliente. Para ello se regresa un poco y se accede a esta opción en la lista de servidores, en donde se sigue la configuración que está en la imagen, pero se debe obtener la IP pública y la IP local para ingresarlas en el formulario, además de indicar el certificado del cliente del servidor y el tipo del sistema operativo del cliente.

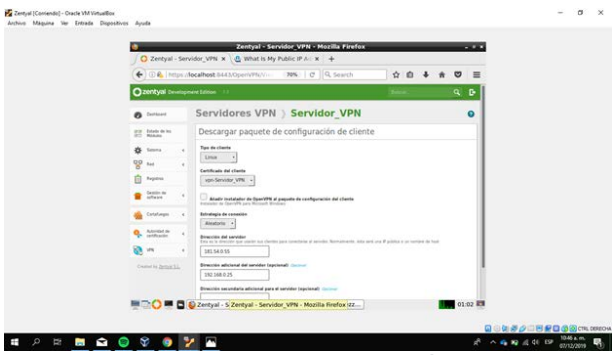

Figura 73. Paquete de configuración cliente

Este paquete se debe enviar a la máquina del cliente. Con el paquete generado se habilita el servidor VPN y se verifica su funcionamiento desde el Dashboard.

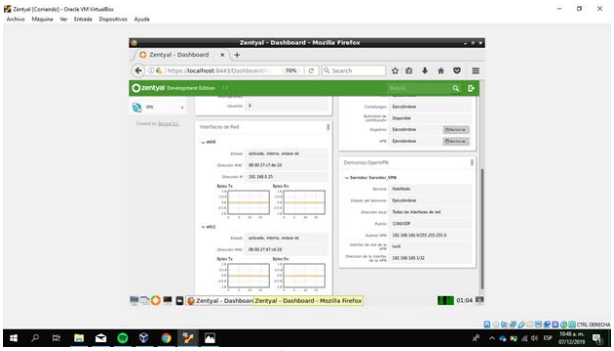

Figura 74. Verificación del paquete.

3.5.5 CONEXIÓN CLIENTE-SERVIDOR

Tras configurar Zentyal, se debe ir a la máquina del cliente. Una vez allí se descarga y se descomprime el paquete del cliente generado por el servidor. Posteriormente se debe instalar OpenVPN en la máquina.

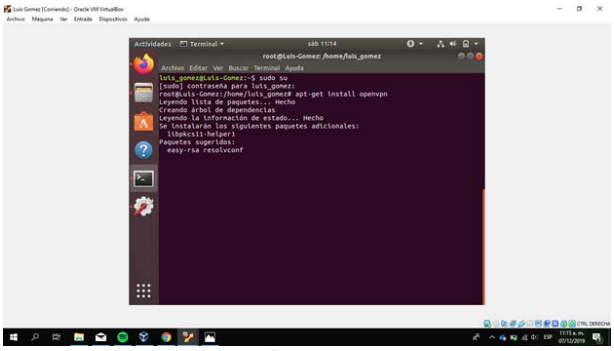

Figura 75. Instalación VPN Ubuntu

Tras instalarlo, ya se puede realizar la conexión utilizando el comando *openvpn --config* e indicando la ruta del archivo *.conf* del paquete de configuración.

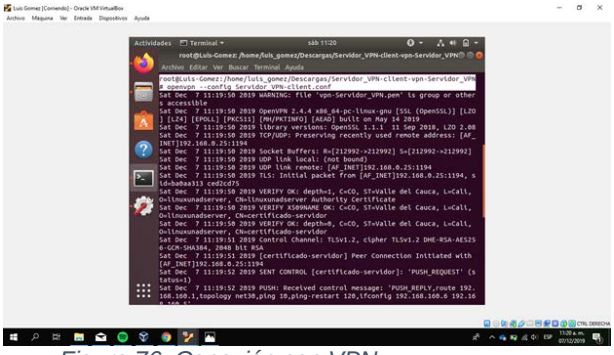

Figura 76. Conexión con VPN

De esta manera se establece la conexión VPN entre el servidor y la maquina Ubuntu. Esta conexión se puede comprobar de dos maneras; primero desde los registros del servidor, se pueden ver las conexiones del servicio VPN y allí debe visualizarse la IP de la maquina Ubuntu, y segundo realizando una conexión SSH desde Zentyal usando la IP que se le asigna a la maquina por la conexión VPN la cual es diferente de la local. Y una vez la conexión se establece se puede acceder a los archivos de la máquina.

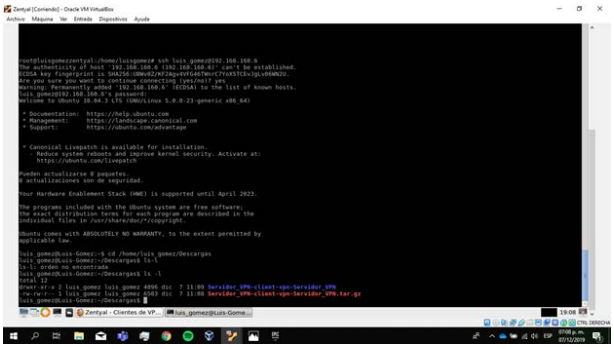

Figura 77. Acceso a contenidos

4 REFERENCIAS

[1] Zentyal Wiki, «Instalación,» 2017. [En línea]. Available: https://wiki.zentyal.org/wiki/Es/5.0/Instalacion#el-instalador-de-zentyal.

[2] Zentyal Wiki, «Usuarios, Equipos y Comparticion de ficheros,» 2018. [En línea]. Available: https://wiki.zentyal.org/wiki/Es/5.0/Usuarios,_Equipos_y_Comparticion_de_ficheros.

[3] C. M, «How to Install and Configure OpenVPN Server on Zentyal 3.4 PDC – Part 12.,» TecMint, 2014. [En línea]. Available: https://www.tecmint.com/install-openvpn-server-on-zentyal/. [Último acceso: 5 12 2019].

[4] Z. Wiki, «Servicio de redes privadas virtuales (VPN) con OpenVPN.,» Zentyal Wiki, [En línea]. Available: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_%28VPN%29_con_OpenVPN. [Último acceso: 2 12 2019].