ADMINISTRANDO REDES EN EL SERVIDOR ZENTYAL 6.2 SOLUCIONADO NECESIDADES ESPECÍFICAS

Monica Gissett Amaya Araujo
monicagissette@gmail.com
Sandra Nelly Montejo
snmontejol@unadvirtual.edu.co
Joan Sebastián Peláez Labrada
Jspelaez14@gmail.com
Manuel Alejandro Carrejo
e-mail: manuelmaca_921104@hotmail.com
Henry Esteban Burbano Quintero
heburbanoq@unadvirtual.edu.co

RESUMEN: *El presente informe trae a colación la implementación de un servidor con el sistema operativo Zentyal en versión 6.2 cuyo objetivo permite de manera centralizada la administración de los servicios de un servidor soportados 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 oportunidad de tener un ahorro, por ende buenas ganancias en una corporación donde se implementes estas herramientas.*

PALABRAS CLAVE: Zentyal, VPN, Proxy, Firewall

1 INTRODUCCIÓN

Zentyal es un sistema operativo que cuenta con soporte Ubuntu el cual fue diseñado para el filtrado web y firewall, siendo este una ayuda para la administración y gestión de la red empresarial en el cual se cuentan con servicios de VPN, Firewall, DHCP, DNS, e-mail, file server, print server .Siendo así una de las mejores herramientas para el manejo de pequeñas empresas que deseen administrar y tener control de sus servicios y usuarios.

2 INSTALACION DE ZENTYAL

2.1 Requisitos

Según la información relacionada en los FAQ de Zentyal tenemos que el hardware mínimo requerido para el uso concurrente de usuario y servicios desplegados será:

- Procesador igual a Core i5,
- 8GB de RAM
- Disco según los datos que maneje la compañía.

2.2 Enlace de Descarga

- http://download.zentyal.com/

2.3 Proceso de Instalación Zentyal

Se crear una máquina virtual en la herramienta de VirtualBox, como se muestra en la Figura 1

Figura 1. Creación máquina virtual

Seleccionamos la ISO descargada para el proceso de instalación e iniciamos escogiendo el idioma, como se observa en la Figura 2

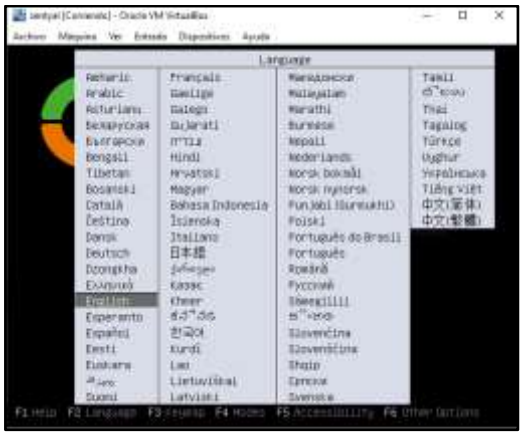

Figura 2. Idioma de instalación

Ahora seleccionamos la instalación development

Figura 3. Instalación de Zentyal

Seleccionaremos el territorio o área en nuestro caso Colombia

Figura 4. Territorio

La instalación descargara los componentes adicionales

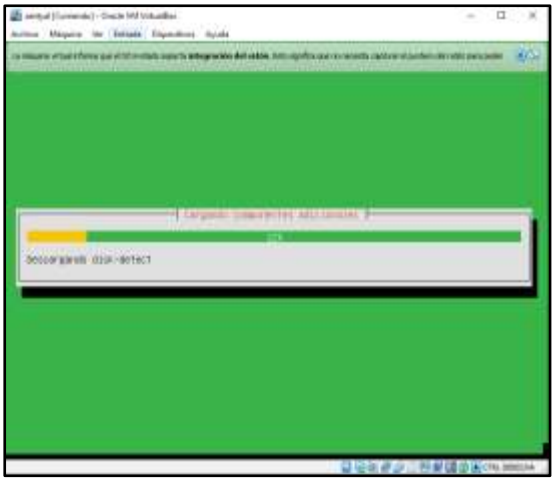

Figura 5. Descarga de componentes

Indicamos el nombre de la máquina y usuario

Figura 6. Nombre de usuario

Se iniciará el particionamiento y la configuración de los apt

Figura 7. Particionamiento

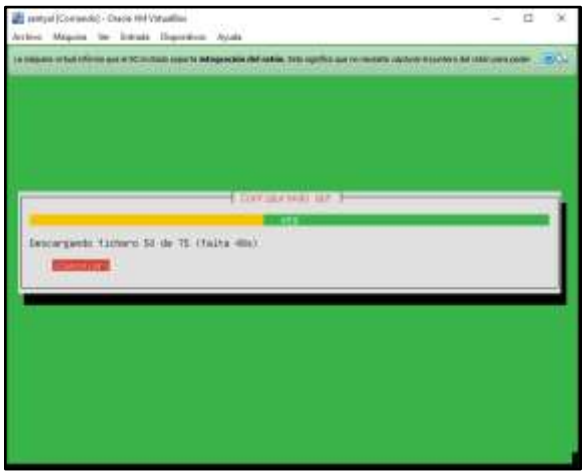

Figura 8. Configuración APT

Una vez se termine la instalación se iniciará la consola de Zentyal solicitando usuario y contraseña creados previamente en la instalación.

Figura 9. Login Consola Zentyal

Figura 10. Consola Zentyal

3 TEMÁTICAS PASO 8 EVALUACIÓN FINAL

Para este Paso final se desarrollarán 5 temáticas las cuales se enfocarán en la implementación de servicios desde la plataforma Zentyal :

Tabla 1. Temáticas Paso 8

Temáticas	Descripción	Estudiante
1	DHCP, DNS, Controlador de Dominio	Manuel Alejandro Carrejo
2	Proxy Transparente	Sandra Nelly Montejo
3	Cortafuegos	Henry Esteban Burbano
4	File Server y Print Server	Joan Sebastián Peláez
5	VPN	Monica Gissett Amaya

3.1 Temática 1 : DHCP, DNS, Controlador de Dominio

se selecciona todos los paquetes que se desea instalar, en el desarrollo de esta temática se requieren DNS Server, DHCP Server Firewall y la autoridad de certificación

Figura 11. Paquetes de instalación.

La configuración de la eth0 es externa, mientras que la eth1 es interna con la dirección IP.

Figura 12. Interfaz eth1

Se configura el rango del DHCP dentro del rango establecido y se valida que en el usuario cliente se encuentre la dirección dentro del rango.

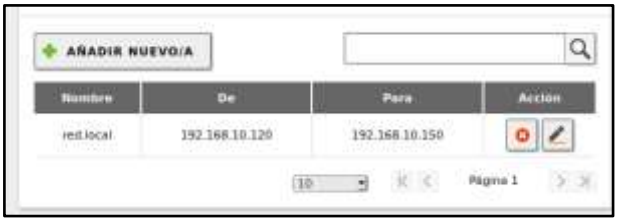

Figura 13. Rango de Ip.

Se válida que la dirección IP del cliente pertenezca al Rango asignado.

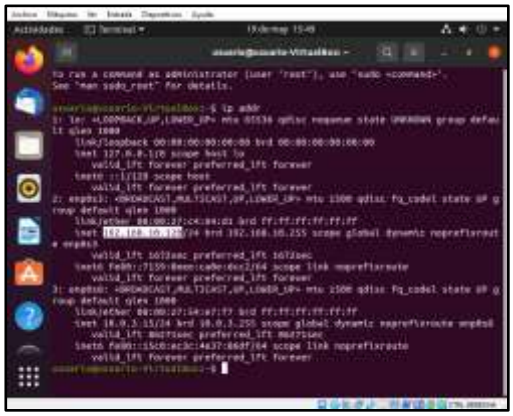
Figura 14. Validación equipo cliente.

Luego se realiza la configuración del DNS, ingresando por el ícono que se encuentra en el Dashboard, donde se habilita el caché del DNS transparente.

Figura 15. habilitación DNS.

Luego se realiza la validación del controlador de dominio, donde se verifica la configuración.

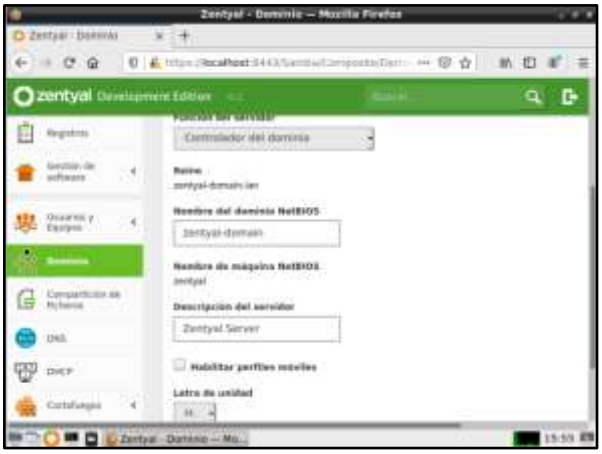

Figura 16. Validación de dominio.

Se valida que el servidor se encuentra detectando al equipo cliente

Figura 17. Validación de detección equipo cliente.

Luego se crea el grupo en Zentyal

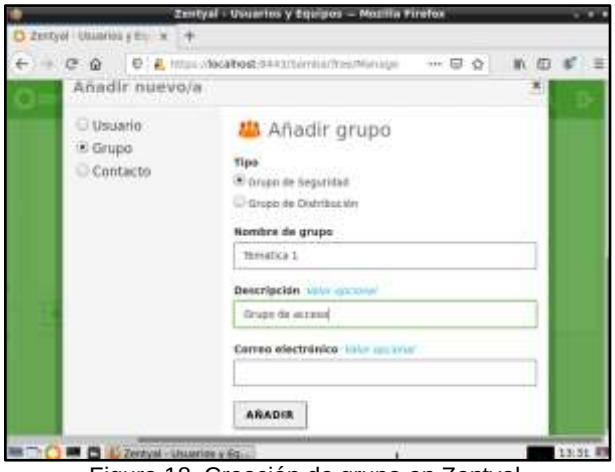

Figura 18. Creación de grupo en Zentyal.

Se crean los respectivos usuarios.

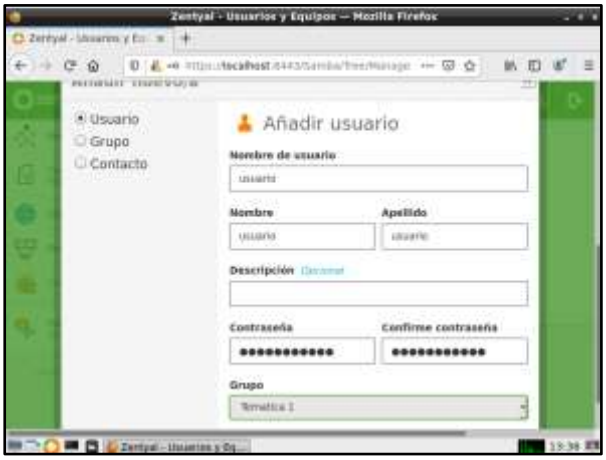

Figura 19. Creación de usuarios.

Finalmente se valida que el equipo cliente se encuentra conectado con el servidor, de acuerdo con el usuario creado en el dominio.

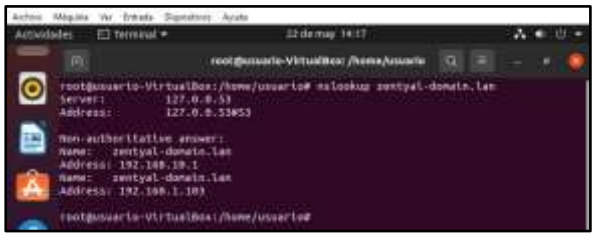
Figura 20. Equipo conectado a servidor.

3.2 Temática 2 :PROXY NO TRANSPARENTE

A continuación, se realiza la implementación y configuración del servidor Zentyal para instalar un proxy HTTP no transparente que permita a un cliente acceder a los servicios de conectividad de Internet a través de un proxy que filtra la salida por medio de un puerto 1230.

Instalamos el HTTP Proxy, el cual seleccionamos desde el zentyal web como se observa en la Figura 21.

Figura 21. Instalamos HTTP Proxy

Instalamos el HTTP Proxy junto a otros paquetes que son necesarios, en este Firewall, Network Configuración, HTTP Proxy se observa en la Figura 22 que se instalan 3 paquetes.

Figura 22. Paquetes necesarios para la instalación del proxy

agregamos interfaces de red: Debe tener dos interfaces de red, eth0 con DHCP y eth1 método estático y colocamos la IP 192.168.2.10 y en la configuración de red de la máquina, en el primer adaptador colocamos adaptador puente y en el segundo colocamos red interna, observamos en la Figura 23 la configuración final en el Zentyal y en la Figura 24 observamos la configuración en la máquina virtual donde se encuentra instalado el Zentyal.

Figura 23. Interfaces para la conexión

Configuración del adaptador


Figura 24. Configuración de los adaptadores de red

La instalación debe finalizar con éxito, para verificarlo aparece la siguiente imagen como se observa en la Figura 25.

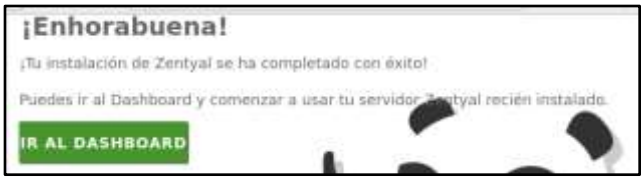

Figura 25. Finalización con éxito

Configuración del proxy de modo no transparente para forzar la política establecida, el puerto es 1230, la configuración se observa en la Figura 26.

Figura 26 Configuración del puerto

Configuramos las reglas de acceso para que los clientes puedan tener acceso a internet y ninguna restricción, la configuración final se observa en la Figura 27.

Figura 27. Reglas de acceso del Proxy no Transparente

Configurar los estados de los módulos, deben estar activos o con el chulito como se observa en la Figura 28.

Figura 28 Estados de los módulos

Verifique si el proxy está ejecutando, debe aparecer como la Figura 29

Figura 29 Proxy ejecutándose

Configuración del adaptador de red de nuestro cliente que en este caso es el Ubuntu desktop, colocamos una red interna

Figura 30 Adaptador desktop en red interna

Un servidor proxy no transparente se debe especificar en cada navegador el puerto para aumentar la seguridad de configuración de red LAN para tener un control del acceso y no permitir que cualquier computador se conecte, primero vamos a configurar el proxy del navegador, donde colocamos el puerto y la dirección IP del servidor como se observa en la Figura 31.

Figura 31 Configuración del Proxy

Segundo vamos a configurar el proxy de las configuraciones de red de Ubuntu 18-04, como se observa en la Figura 32.

Figura 32 Configuración del Proxy en la configuración de red

Hacemos ping al servidor para verificar el funcionamiento, además vemos si tiene acceso a internet, como se observa en la Figura 33.

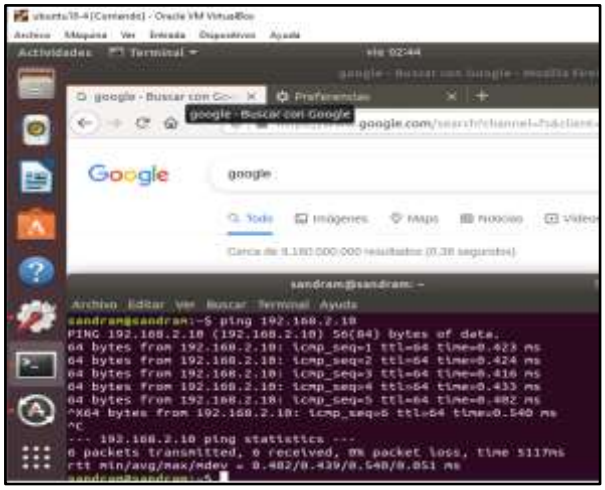

Figura 33. Verificación del proxy en el cliente

3.3 Temática 3: Cortafuegos

Otro de los servicios disponibles con Zentyal es el Cortafuegos. Gracias a este servicio es posible restringir el acceso a páginas que no se consideren adecuadas para la red.

Para iniciar la configuración del cortafuegos se debe ubicar en el dashboard y seleccionar la opción interfaces una vez ahí vamos a configurar las interfaces de red. Como se observa en la figura 34, La interfaz eth0 es la que conecta la máquina con el router por lo cual se marca como externa.

Figura 34. Interfaz externa

Una vez configurada la interfaz externa se procede con la configuración de la interfaz interna como lo indica la figura 35. Para esta red no se debe marcar la opción Externa ya que la interfaz eth1 corresponde a la red interna.

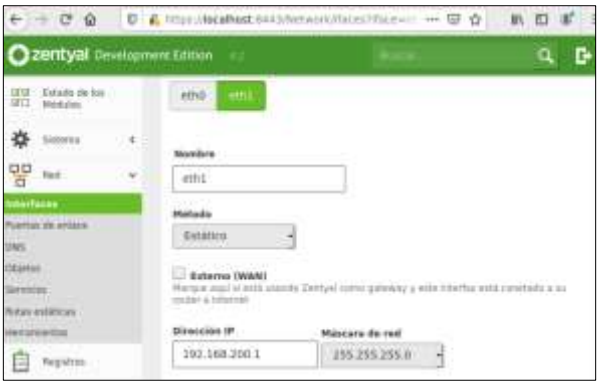

Figura 35. Interfaz interna

Posterior a la configuración de las interfaces se añade la puerta de enlace. Como vemos en la figura 3.3, se le asigna un nombre a la puerta de enlace y se asigna la dirección IP del router. En caso de tener varios router el peso determina la prioridad del tráfico como lo aclara en [2] "Cuanto mayor sea el peso, más tráfico se enviará por esa puerta de enlace si activamos el balanceo de tráfico. Por ejemplo, si una de las puertas de enlace tiene un peso de 7 y la otra de 3, se usarán 7 unidades de ancho de banda de la primera por cada 3 de la segunda, o lo que es lo mismo, el 70% del tráfico usará la primera y el 30% la segunda."

Figura 36: Configuración puerta de enlace

En la opción de objetos se crea un registro de las páginas web (Figura 37) y por medio de la opción miembros se agregan las direcciones IP relacionadas a cada página web (Figura 38).

Figura 37: Lista de objetos

Las páginas Web suelen contar con varias direcciones IP por lo cual se deben crear tantos miembros como direcciones IP tenga la página web.

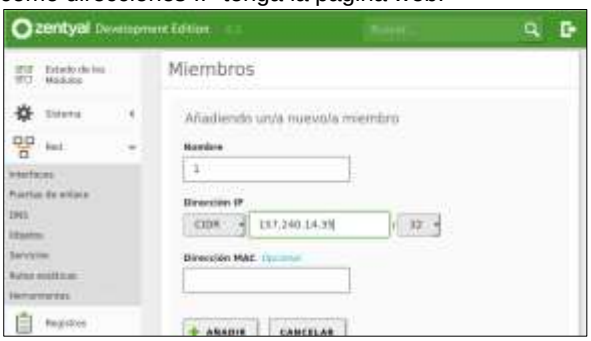

Figura 38: Registro de miembros

Ahora como se observa en la figura 39, se debe dirigir a la opción de cortafuegos donde se procede a configurar las reglas de filtrado para las redes internas lo cual, permitirá bloquear el acceso a las páginas que no se consideran adecuadas.

Figura 39: Filtrado de paquetes

Al momento de añadir la regla en decisión podemos elegir entre 3 opciones: Aceptar, Denegar, y registrar. Para el bloqueo de la página se selecciona la opción Denegar como lo vemos en la Figura 40. En destino se selecciona el objeto que se ha creado anteriormente con las IP de la página que queremos bloquear y en servicio se selecciona la opción “Cualquiera” para que bloquee cualquier tipo de acceso.

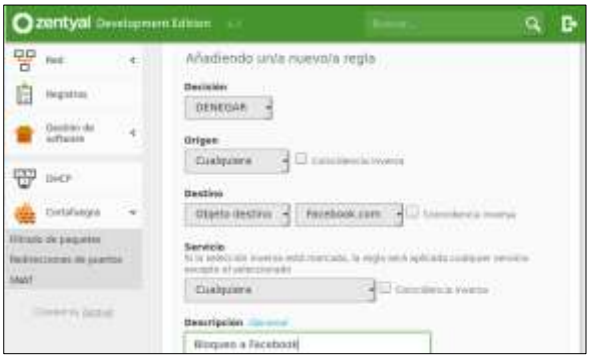

Figura 40: Reglas de filtrado

En caso de querer realizar el bloqueo con diferentes paginas Figura 41 se debe repetir el proceso con cada uno de los objetos que vamos a bloquear o permitir según sea el caso.

Figura 41: Lista de reglas de filtrado

Para finalizar con la configuración del Cortafuegos se debe acceder a los estados de los módulos y confirmar que los módulos se encuentren en estado activo tal como lo muestra la figura 42.

Figura 42: Estado de los módulos

Una vez finalizada la configuración del cortafuegos se debe validar que esté funcionando y genere la restricción de las páginas web. Para realizar la confirmación se ingresa desde una computadora de la red interna y probamos el acceso a internet.

Como se observa en la Figura 43 el cliente tiene acceso a internet desde su navegador y puede acceder a la página de YouTube sin problemas.

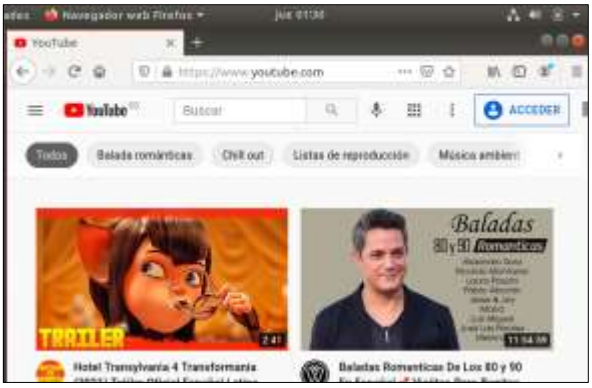

Figura 43: Acceso a youtube.com

Ahora si el cliente intenta acceder a una de las páginas con restricción inmediatamente la red le mostrará un mensaje de error como se ve en la Figura 44.

Figura 44: Acceso bloqueado

Como se evidencia en las imágenes, el cliente cuenta con acceso a internet, pero, al intentar acceder a una de las paginas bloqueadas el sistema lo restringe y no permitirá el acceso.

3.4 Temática 4: File Server, Print Server

Para las compañías uno de los servicios más comunes y eficientes es el servicio de File Server ya que proporciona una adecuada gestión de recursos el cual cuenta con seguridad y disponibilidad, aplicando estos servicios desde zentyal será fácil su manejo y control de la herramienta

Ahora crearemos un usuario para el ejercicio de instalación y manejo de file server

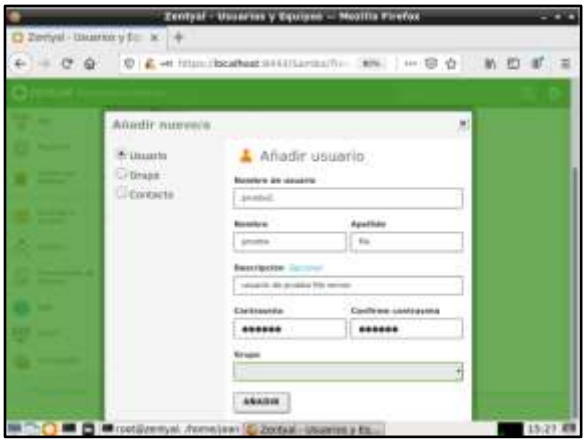

Figura 45: Creación de usuario

Creamos el directorio el cual se compartirá desde zentyal

Figura 46: Creación carpeta compartida

Ahora editaremos los permisos de control de acceso

Figura 47. Permisos de Acceso

Ahora probaremos el recurso compartido

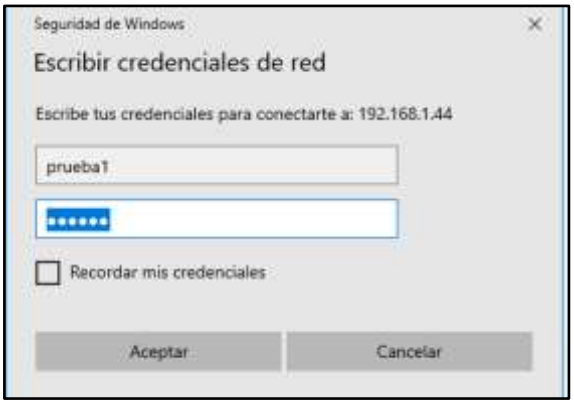

Figura 48.Acceso usuario Prueba1

Se valida el acceso

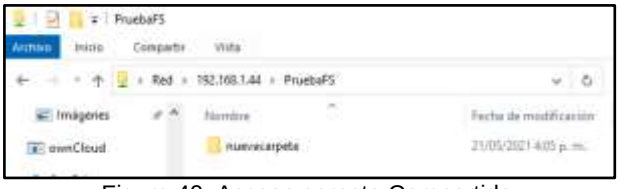

Figura 49. Acceso carpeta Compartida

Validamos los permisos para el usuario prueba1 de solo lectura

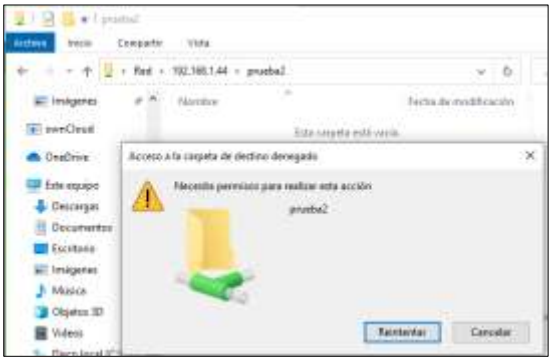

Figura 50. Solo Lectura

Realizamos la prueba desde nuestro cliente ubuntu

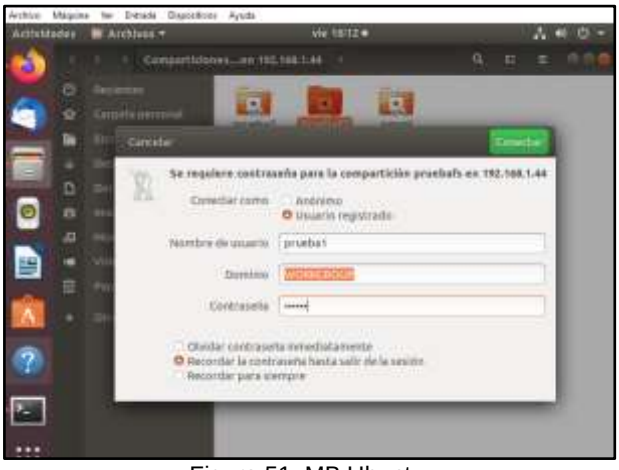

Figura 51. MB Ubuntu

Instalación del servicio de Print Server:

Para el caso actual zentyal no soporta un servidor print por lo cual emplearemos el servicio CUPS

Iniciamos la instalación con el comando :apt-get install cups en el servidor zentyal

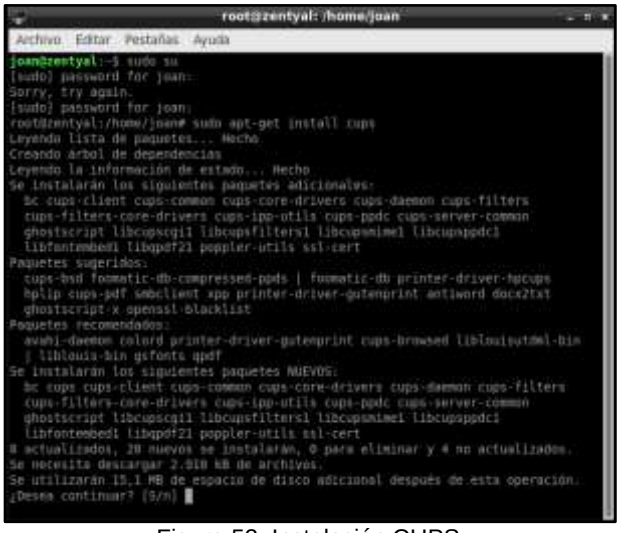

Figura 52. Instalación CUPS

Se configuran los listen para la conexión de la impresora

```
# Only listen for connections from the local machine.
Listen localhost:631
Listen /run/cups/cups.sock
Listen 192.168.1.44:631
Listen zentyal:631
```

Figura 53. Listen Cups

Realizamos la creación de la impresora de red desde la consola de cups

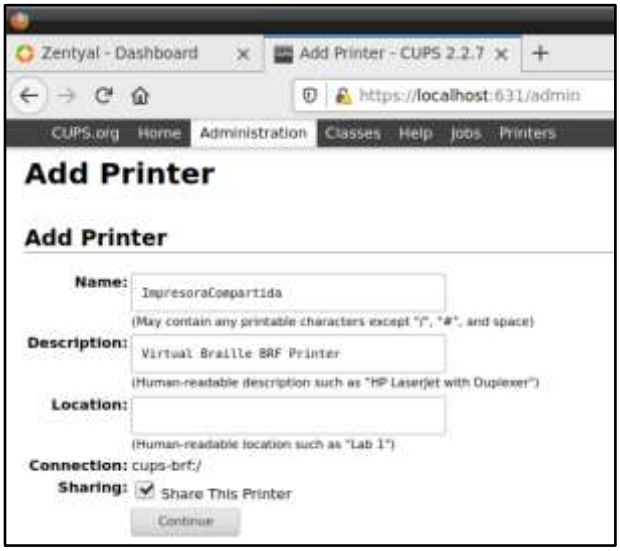

Figura 54. Creación Impresora

Agregamos la configuración de impresoras desde samba y reiniciamos servicios para poder verlas desde los clientes

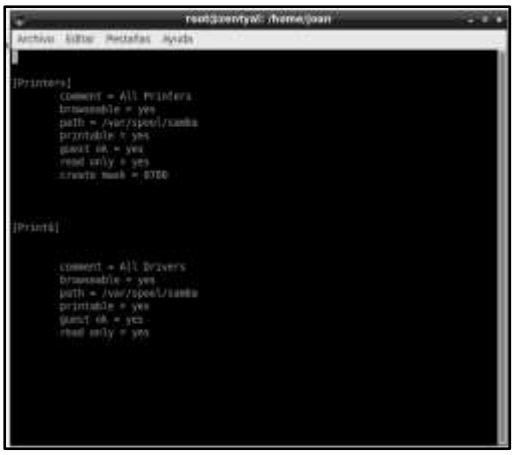

Figura 55. Configuración SMB

Validamos que desde el cliente podamos ver la impresora compartida y podamos conectarnos

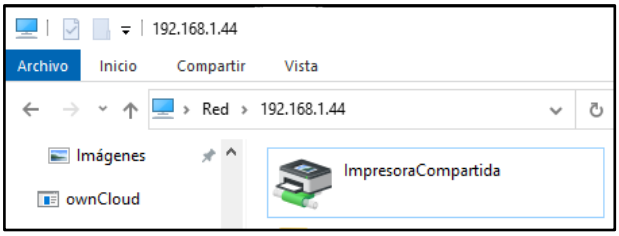

Figura 56. Impresora Compartida

3.5 Temática 5:VPN

Finalmente se realiza 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 Ubuntu Desktop. Donde también se evidencia el ingreso a algún contenido o aplicación de la estación de trabajo

Lo primero en realizar es crear un certificado de autoridad de certificación. De la Figura 57, muestra la configuración con el fin de darle permisos a nuestro servidor para para crear certificados de seguridad, esto muy importante, ya que crea el certificado de acceso a la red VPN que vamos a implementar.

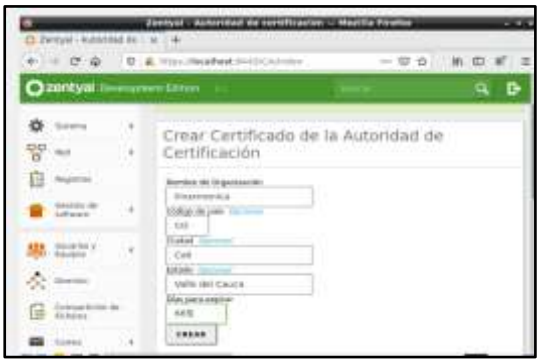

Figura 57. Configuración VPN

Ingresamos los datos que no piden y damos expedir y en la parte inferior podremos observar que efectivamente se ha creado un certificado de autoridad con los datos incluidos, en la parte superior le daremos guardar los cambios, como se muestra en la Figura 58.

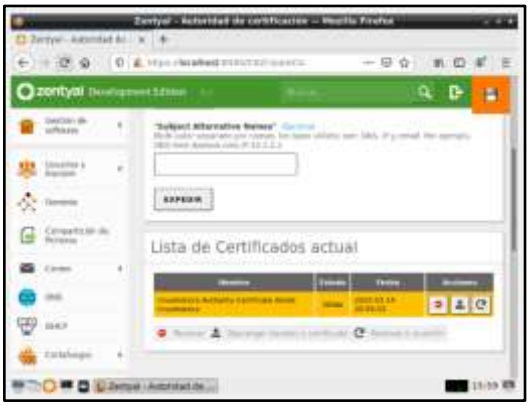

Figura 58. Lista de Certificados

Al guardar no aparecerá el mensaje de guardado con éxito. Luego de ello iremos al menú de VPN/ Servidores donde crearemos un nuevo servidor VPN, damos clic en añadir nuevo, como se observa en la figura 59.

Figura 59. Servidores VPN

A continuación. En la Figura 60 se observa la lista de servidores, donde se coloca el nombre del servidor que queramos ponerle, y luego damos en añadir

Figura 60. Configuración de servidor VPN

Al añadir, podremos observar que aparecerá un listado con el nombre del servidor y los ítems correspondiente para la configuración de la VPN

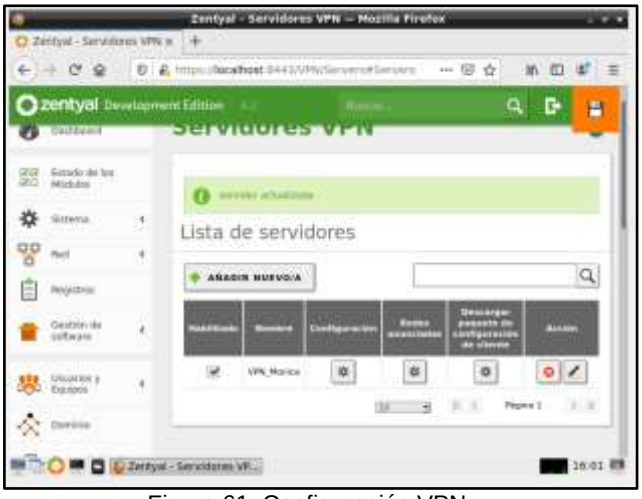

Figura 61. Configuración VPN

De la Figura 61. Muestra la VPN creada anteriormente, ahora nuevamente nos dirigimos al menú de Certificados en Autoridad de certificados/ General, allí nos dará los campos para crear un certificado nuevo y que caducidad tendrá este, diligenciamos la información y le damos expedir

Figura 62. Creación de certificados

Al finalizar en la parte posterior podemos observar mediante la Figura 62, que tenemos los certificados de autoría de servidor, certificado de la VPN, que se generaron automáticamente al crear la VPN anteriormente y el certificado que se acaba de añadir, como lo muestra la Figura 63

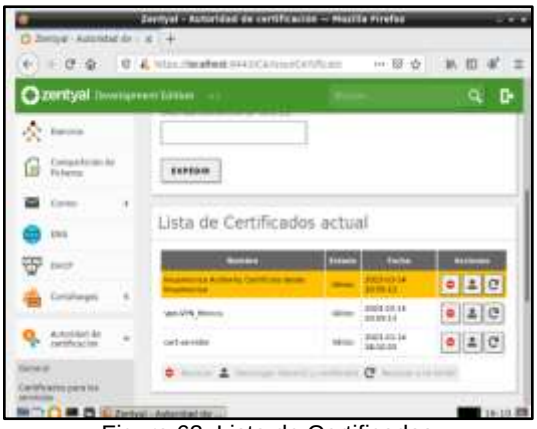

Figura 63. Lista de Certificados

Luego debemos volver al menú de servidores VPN, damos clic en el menú VPN del servidor, como lo muestra la Figura 64, luego en la lista del servidor, seleccionar configuración para diligenciar la información de la configuración de nuestra VPN, tener claro el puerto que vamos a configurar en este caso utilizaremos el puerto 1194/UDP, seleccionamos el certificado del servidor .

Figura 64. Configuración del servidor VPN

De la Figura 65. Muestra la selección del ítem interfaz TUN, Por defecto se usa esta interfaz semejante a un bridge a un enlace en capa 3.

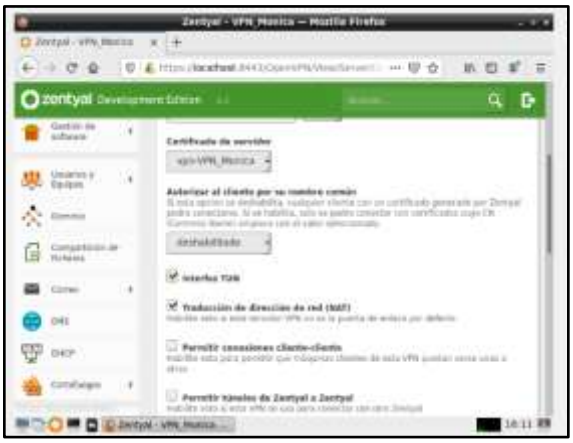

Figura 65. Configuración Interfaz TUN

Y también seleccionamos en interfaz en la que escuchar, seleccionamos todas las interfaces de red, como lo muestra la Figura 66.

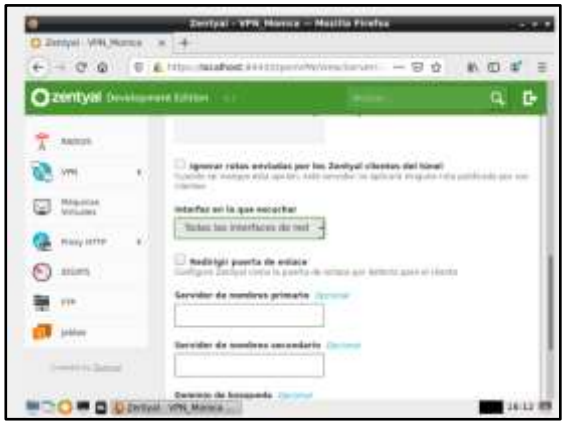

Figura 66. Interfaces de red

Guardamos los cambios generados para volver al menú anterior. Una vez guardados los cambios, estaremos en el menú principal. En la Figura 67. Seleccionamos el módulo de RED, ítem Servicios y se añade un nuevo servicio de red

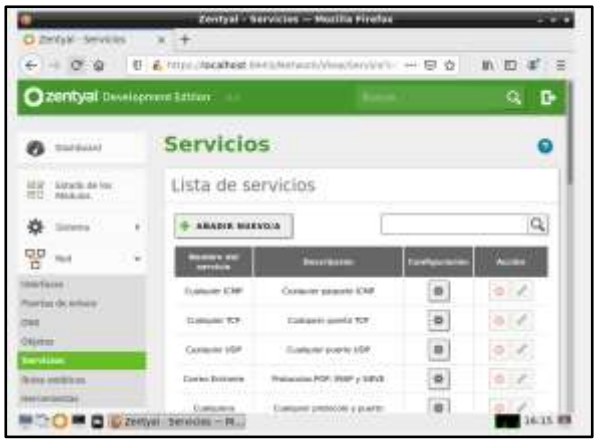

Figura 67. Lista de Servicios de Red

En la Figura 68, se puede observar la configuración del servicio red- vpn, donde se pedirá que indiquemos el nombre del servicio y la descripción, al hacerlo damos en añadir. Una vez creado aparecerá en el listado de los servicios, a continuación, le daremos en guardar

Figura 68. configuración del servicio red- VPN

Como es un servicio de VPN el que vamos a añadir le pondremos los mismos parámetros que utilizamos anteriormente en la configuración, que serían el protocolo UDP y el puerto destino el 1194, y clic en añadir, como lo podemos observar en la Figura 69.

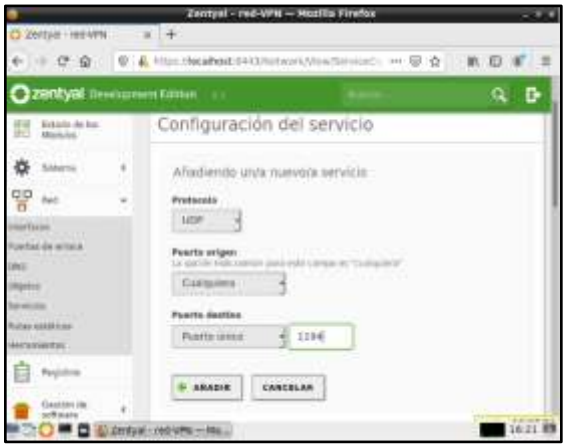

Figura 69. Configuración del servicio UDP

Al finalizar aparecerá la configuración que acabamos de realizar, damos por último en el botón de guardar. Ahora, iremos al módulo de firewall y en los ítems filtrado de paquetes en el menú principal que muestra en la Figura 70, donde vamos a crear las reglas de excepción para el acceso del servidor, ya en el menú le daremos a configurar reglas en el menú de reglas de filtrado desde las redes internas hacia Zentyal

Figura 70. Packet Filter

Como se puede observar en la Figura 71, procedemos abrir el menú donde daremos clic en añadir nuevo, se desplegarán las opciones para configurar la nueva regla del firewall donde se aceptará, origen en cualquiera, servicio el que acabamos de crear de la VPN y descripción una nota sobre la regla creada y luego clic en añadir.

Figura 71. Filtrado de Paquetes

Una vez parametrizado lo anterior aparecerá en las reglas del firewall lo parametrizado, damos clic en guardar. Se guardan los cambios Regresamos nuevamente al menú de servidores VPN. Ahora en la Figura 72, se observa el Ingreso al menú de redes anunciadas, en este caso ya por defecto la VPN ya tiene una red anunciada configurada por el mismo servidor por defecto.

Figura 72. Lista de redes anunciadas

A continuación, vamos a parametrizar las direcciones IP de acceso al servidor VPN para ello debemos conocer cuál es la IP de nuestra red WAN en este caso accedemos por internet para averiguar y añadirla al menú de descargar configuración de cliente, como se observa en la Figura 73.

Figura 73. Ip del equipo Zentyal

Ingresamos al menú del VPN nuevamente y seleccionamos el ítem para descargar paquete de configuración de cliente, como se observa en la Figura 74

Figura 74. Descarga paquetes

Ya una vez averiguado las IP de WAN y LAN procedemos a parametrizar. En tipo cliente ira el sistema operativo desde el cual nos conectaremos, en este caso será Linux, el certificado del cliente será el que con anterioridad parametrizamos al principio, como se muestra en la Figura 75

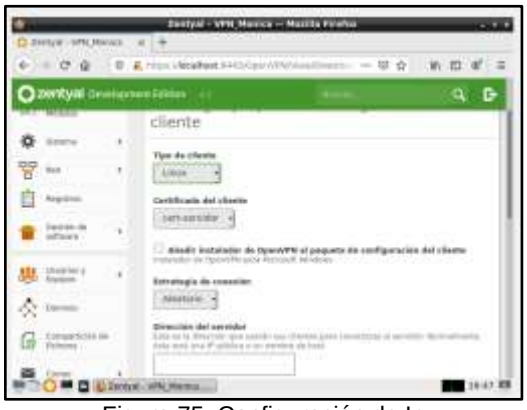

Figura 75. Configuración de Ip

En la Figura 76 se coloca la dirección del servidor de la IP de la WAN y en dirección adicional pondremos la dirección IP del servidor

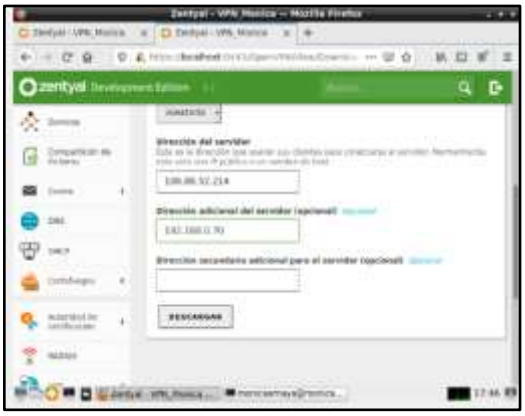
Figura 76. Asignación de dirección servidor

En la Figura 77. Se puede observar la descarga del archivo .zip, un paquete comprimido el cual debemos enviar a la máquina que se conectará a nuestra VPN creada

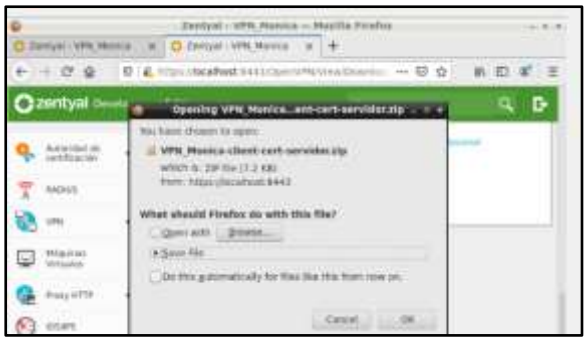

Figura 77. Descarga de archivo para el equipo cliente

Al finalizar podremos ver en dashboard la configuración de nuestra VPN creada, como lo muestra la Figura 78

Figura 78. Verificación de VPN activado

3.5.1 Configuración de VPN en maquina cliente

Se procede a seleccionar las opciones de Ubuntu de acceso universal, esto con el fin de habilitar todos los accesos en nuestra máquina cliente, Ingresamos a la consola e instalamos openvpn para la configuración de acceso a nuestra VPN creada, utilizando el comando apt-get install openvpn, una vez instalado iremos a la carpeta donde tenemos los archivos de configuración de nuestra VPN, en nuestro caso usaremos cd para abrir carpetas el archivo se alojó en el escritorio para acceder, ahora se procede abrir el archivo previamente descargado, como se muestra en la Figura 79

Figura 79. Paquete descargado

En La Figura 80. Se puede observar la instalación de paquetes donde se ejecutará la configuración de la VPN creada con openVPN usando el archivo .conf con el comando openvpn –config VPN_monica-client.conf

Figura 80. instalación de paquetes

La Figura 81. Muestra la VPN que se empezó a configurarse de forma automática en nuestra máquina cliente hasta finalizar.

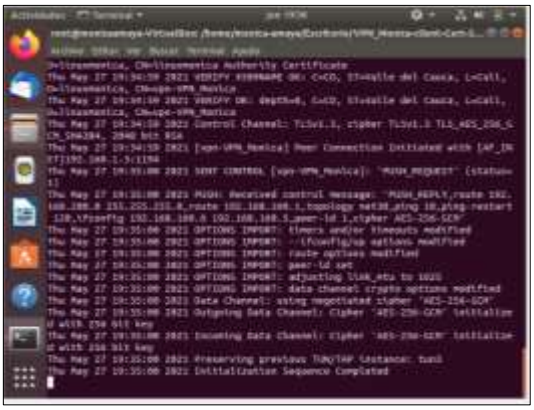

Figura 81: sincronización con la VPN

Ya por último podemos ir al servidor Zentyal y desde el menú registro podremos observar desde la parte posterior la sincronización de conexiones con el servidor y se muestra que la maquina cliente está conectada con el certificado remoto que creamos con anterioridad

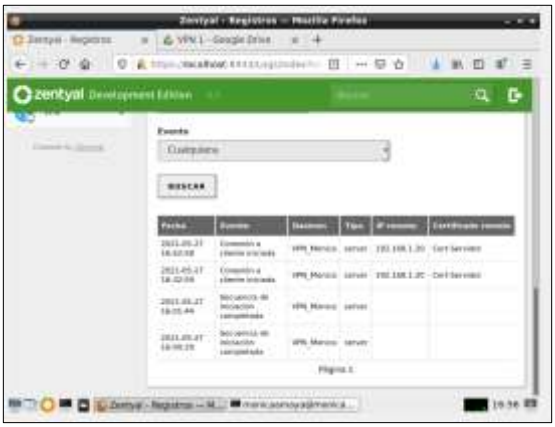

Figura 82: sincronización con la VPN

4 CONCLUSIONES

Zentyal es una gran herramienta para aumentar la productividad y proteger nuestra red ya que gracias a su cortafuegos y las reglas de filtrado restringe el acceso a páginas innecesarias para llevar a cabo las labores.

Las redes privadas virtuales conectan de manera segura subredes distintas, Zentyal permite la configuración de la VPN por medio de protocolo UDP o TCP, en este informe utilizamos el UDP, ya que es más rápido y seguro.

La implementación de servidores como zentyal agiliza los procesos de configuración y administración de servidores esto ayuda a que mejoren los tiempos de configuración por parte de una compañía en la gestión de su negocio.

5 REFERENCIAS

[1] Zentyal community. (s.f.). Obtenido de zentyal community: https://doc.zentyal.org/en/

[2] Zentyal community," Configuración de un cortafuegos con Zentyal", Documentación de Zentyal 6.2. Disponible en: https://doc.zentyal.org/6.2/es/firewall.html

[3] Servicios de redes privadas virtuales (VPN) con OpenVPN Obtenido de : https://zentyal.com/wp-content/themes/storefront-zentyal-child/assets/files/sample_chapter_zentyal_vpn_openvpn_es.pdf