

INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR ZENTYAL PARA IMPLEMENTAR SERVICIOS DE INFRAESTRUCTURA IT.

Jorge Wilmar Quintero Castillo
jwquinteroc@unadvirtual.edu.co
Jonatan Stive Herran Arias
jsherrana@unadvirtual.edu.co
Alicy Catalina Mosquera Perea
acmosquerap@unadvirtual.edu.co
Benjamín Molina Polania
bmolinap@unadvirtual.edu.co
Harrison Gonzalez Casierra
Hgonzalesca@unadvirtual.edu.co

RESUMEN: Por medio de este artículo se abordarán el proceso de implementación de una solución a una variedad de problemáticas con relación a la migración de sistema operativo y puesta en marcha de sistemas de seguridad de la infraestructura de red, haciendo uso del sistema operativo Zentyal basado en Linux.

PALABRAS CLAVE: Zentyal, DHCP, DNS, controlador de dominio, ficheros, dashboard.

1 INTRODUCCIÓN

Actualmente existen muchas opciones en diversas plataformas o herramientas para realizar la administración de la infraestructura IT de una organización o compañía, en este artículo describimos la solución dada a la problemática planteada haciendo uso de Zentyal server como sistema operativo y plataforma para la gestión de los diversos servicios, necesarios para la infraestructura de los recursos IT, como por ejemplo DNS Server, DHCP Server, Controlador de Dominio, Proxy no transparente, Firewall o Cortafuegos, File Server, Print, Server y VPN.

2 INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR ZENTYAL

La versión de la distribución Zentyal Server que se instala [1] es la 6.2. Primero se selecciona el lenguaje español como se muestra en la figura 1.

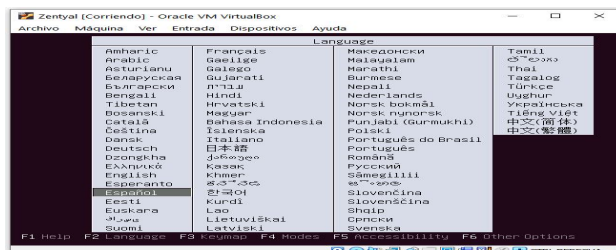


Figura 1. Seleccionar el idioma.

Como ubicación se selecciona Colombia y se configura el teclado, ver Fig. 2 y Fig. 3 respectivamente:

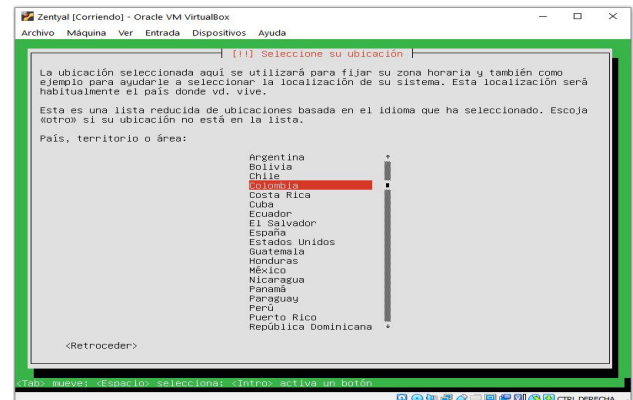


Figura 2. Seleccionar ubicación.

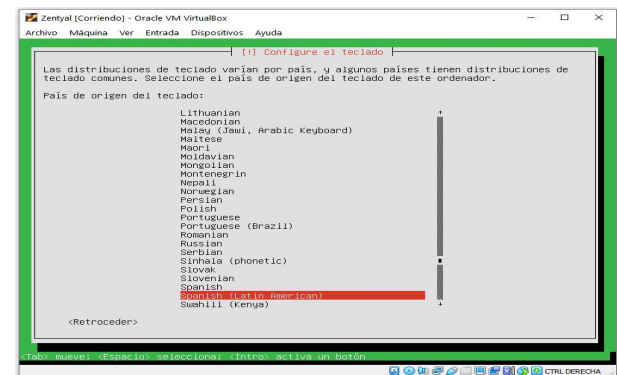


Figura 3. Configurar teclado.

Se Selecciona la interfaz de red que se conectará a internet, en este caso eth01, figura 4.

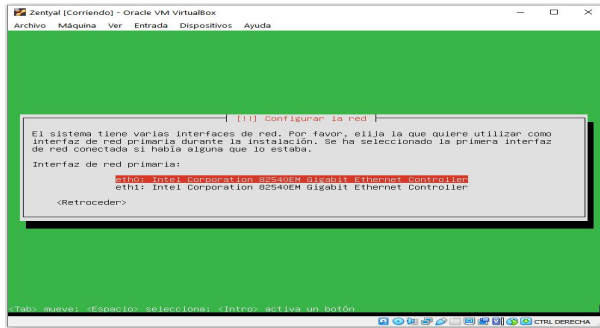


Figura 4. Interfaz de red para internet.

Se debe introducir el nombre que tendrá la maquina como ejemplo podemos ver la figura 5

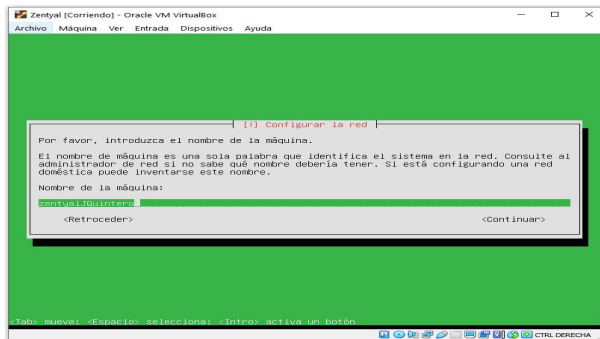


Figura 5. Nombre de la máquina.

Se establece el nombre que tendrá el administrador del sistema, ver Fig. 6 y la contraseña, ver Fig. 7.

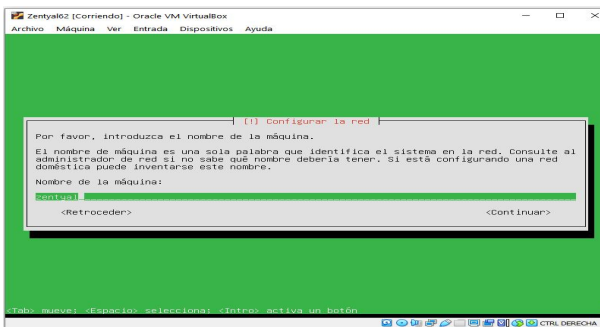


Figura 6. Nombre del administrador del sistema.

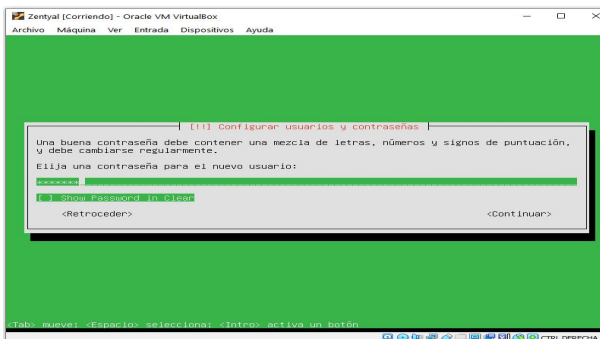


Figura 7. Contraseña para el administrador.

Se inicia la instalación del Sistema como se puede observar en la figura 8:

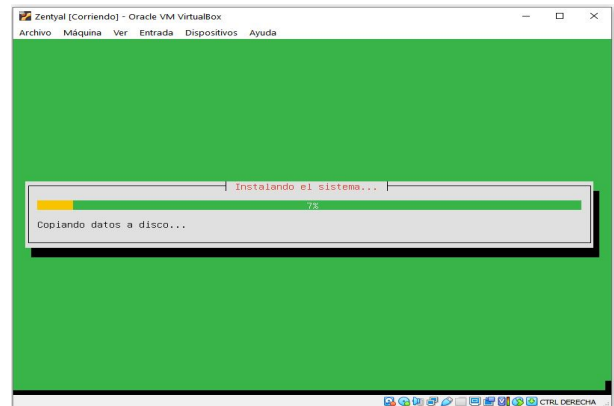


Figura 8. Inicia la instalación del sistema.

Cuando la instalación se ha completado se puede ver la pantalla de inicio de Zentyal, figura 9:

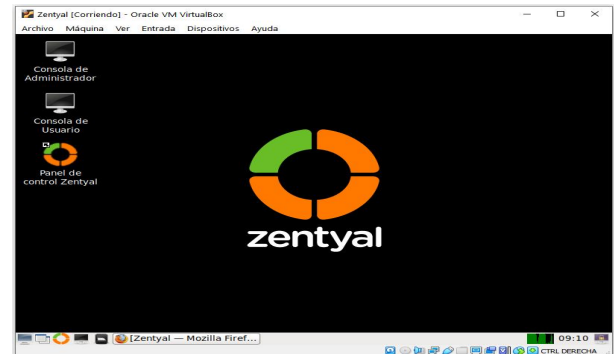


Figura 9. Inicio de Zentyal.

El ingreso al panel de control de Zentyal se hace por medio navegador web introduciendo el nombre de usuario y contraseña establecidos para el administrador en la instalación como se puede apreciar en la figura 10:



Figura 10. Panel de control.

3 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Cuando se ingresa al panel de control, se deben seleccionar los paquetes a instalar: DHCP, DNS y controlador de dominio, paquetes resaltados en la figura 11.

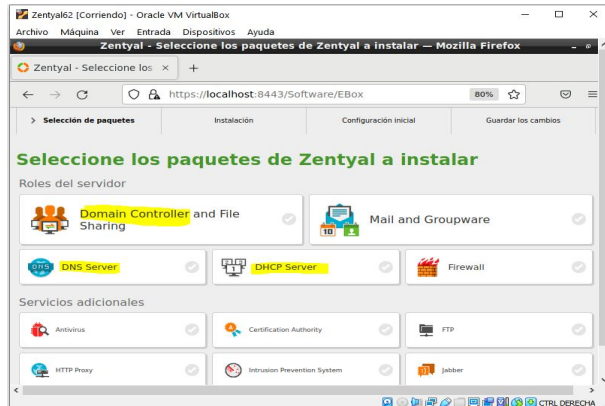


Figura 11 Seleccionar paquetes a instalar.

Se deben configurar las dos interfaces de red; eth0 será par internet y eth1 será para la red interna como se puede apreciar en la figura 12 y 13:

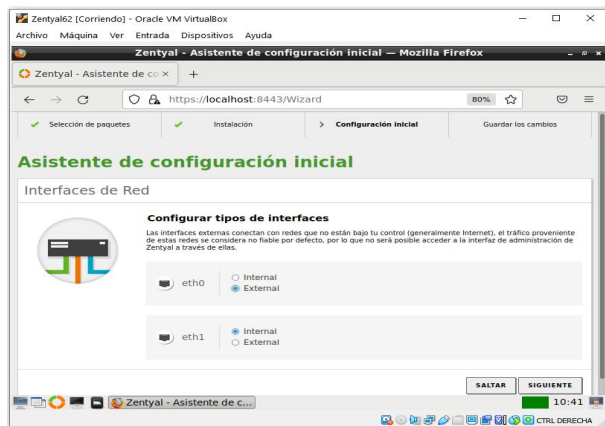


Figura 12. Configurar interfaces.

Se debe indicar que para eth0 se asigne una IP por DHCP y que para eth1 la IP estática 192.168.1.10:

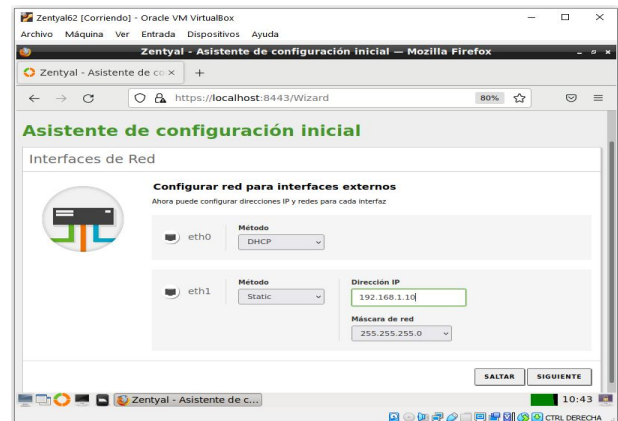


Figura 13. Configuración de los tipos de IP.

Se debe establecer el nombre del dominio del servidor y se da clic en finalizar, figura 14:

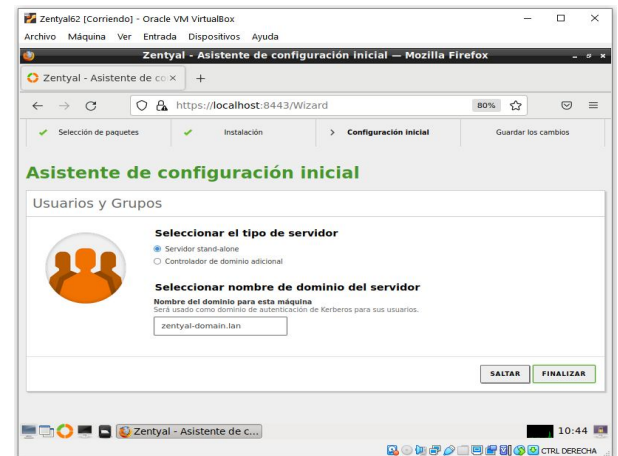


Figura 14. Establecer nombre de dominio.

3.1 DHCP SERVER

Un servidor DHCP [2] permite asignar direcciones IP dinámicamente. Para la configuración se debe seleccionar la opción DHCP, como se ve en la figura 15 y 16:

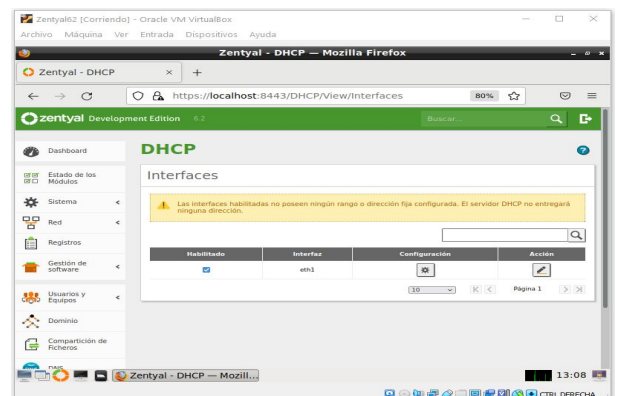


Figura 15. Configuración DHCP.

En configuración se establece el rango de las direcciones IP:

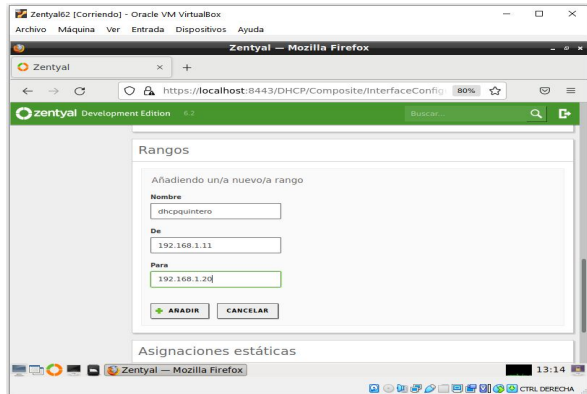


Figura 16. Establecer rangos de IP.

Se inicia una maquina cliente Ubuntu Desktop. Se observa que tiene la IP 192.168.11, que está dentro del rango establecido en Zentyal como se puede comprobar en la figura 17:

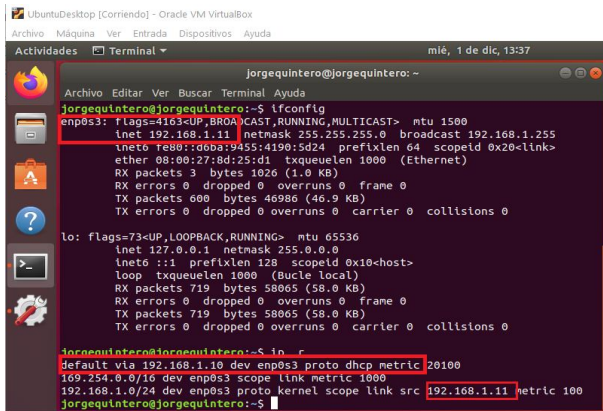


Figura 17. IP de la máquina cliente.

En Zentyal se puede evidenciar la dirección IP asignada al equipo Desktop que tiene por nombre: jorgequintero, véase figura 18:

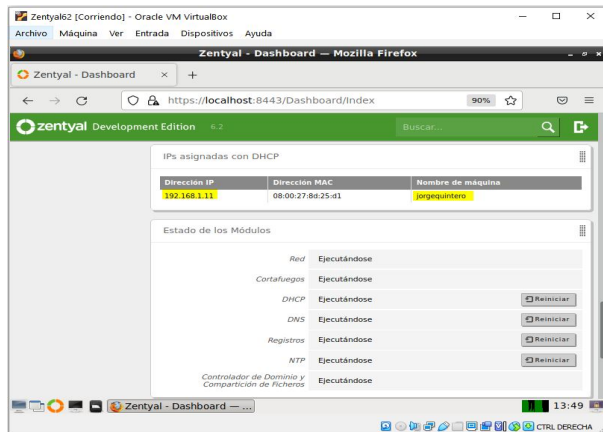


Figura 18. IPs asignadas por el DHCP.

3.2 DNS SERVER

El servicio DNS [3] se instaló con los módulos de instalación. En la opción “DNS” del menú, se puede ver que está configurado el dominio “Zentyal-domain.lan” como se observa en la figura 19:

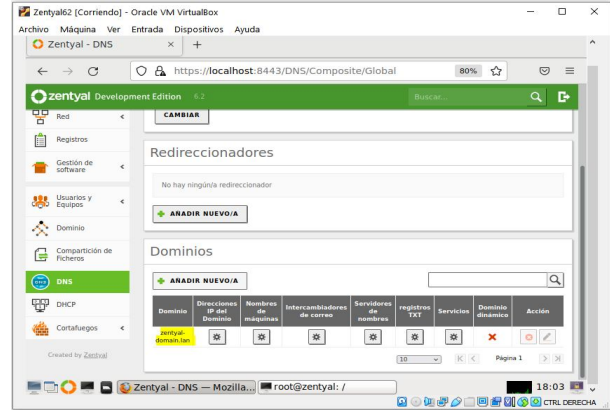


Figura 19. Dominios en Zentyal.

Desde la maquina cliente Ubuntu Desktop se hace ping al dominio, podemos ver la respuesta en la figura 20 y 21:

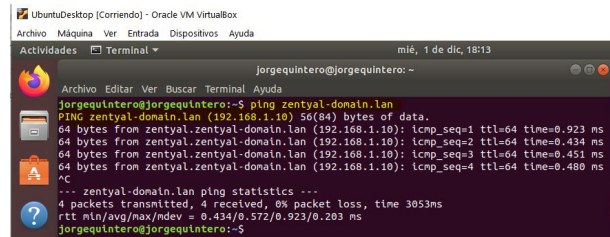


Figura 20. Ping a zentyal-domain.lan.

También con el comando *nslookup* se puede ver desde la maquina cliente la IP asociada al dominio:

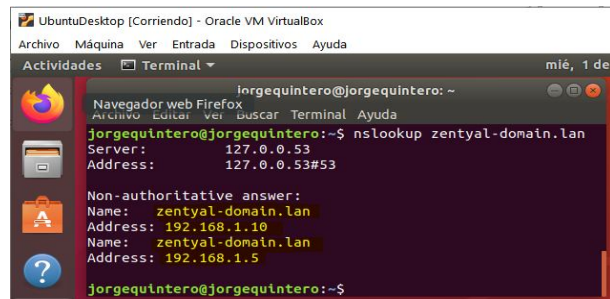


Figura 10. IP asociada al dominio.

3.3 CONTROLADOR DE DOMINIO

Se debe activar el módulo “Controlador de Dominio y Compartición de Ficheros” [4]. En la opción “Dominio” del menú izquierdo, se puede ver la configuración del controlador de dominio que se estableció automáticamente en la instalación del Zentyal

y en la instalación de los módulos, como se puede observar en la figura 22:

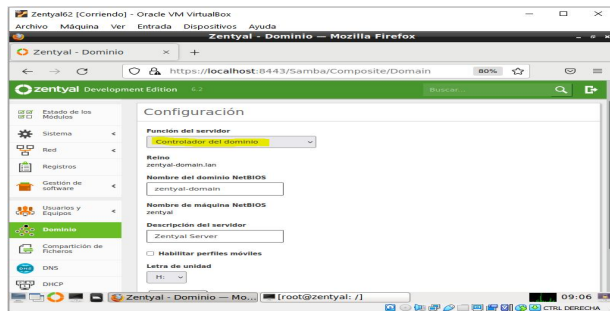


Figura 22. Configuración del controlador de dominio.

En la opción "Usuarios y Equipos" se debe crear el usuario "jorgeqdesktop" que accederá desde la maquina cliente Ubuntu Desktop como se observa en la figura 23:

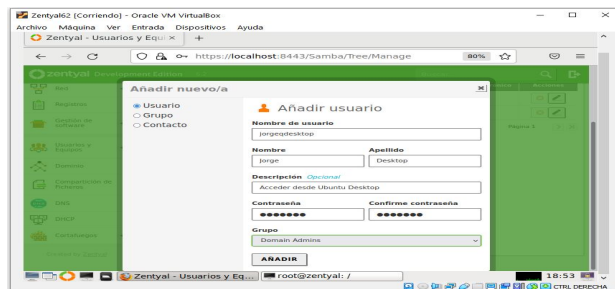


Figura 23. Creación de usuario jorgeqdesktop.

Para que la maquina cliente Ubuntu Desktop se pueda unir al dominio se debe descargar e instalar el paquete pbis-open, este paquete se descarga de <https://github.com/BeyondTrust/pbis-open/releases>, como se puede ver en la figura 24

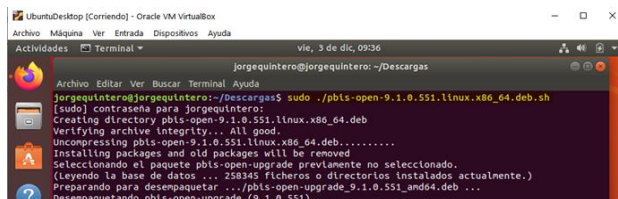


Figura 24. Instalar el paquete pbis-open.

Se procede a realizar la unión de la maquina cliente Ubuntu Desktop al controlador de dominio de Zentyal; para esto se ejecuta en la consola del cliente el comando "sudo /opt/pbis/bin/domainjoin-cli join zentyal-domain.lan jorgeqdesktop", en este comando jorgeqdesktop es el usuario creado en Zentyal y Zentyal-domain.lan es el dominio como se puede observar en la figura25:

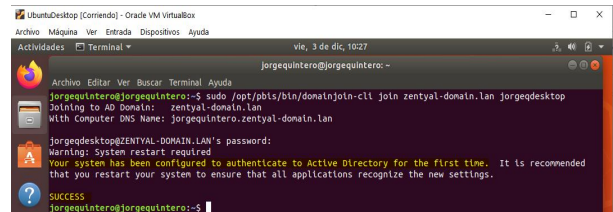


Figura 25. Unión de la máquina cliente al dominio.

En el servidor Zentyal, en el apartado de "Computers" se evidencia que la maquina cliente UbuntuDesktop que tiene por nombre "Jorgequintero" se ha unido al dominio como se resalta en la figura 26:

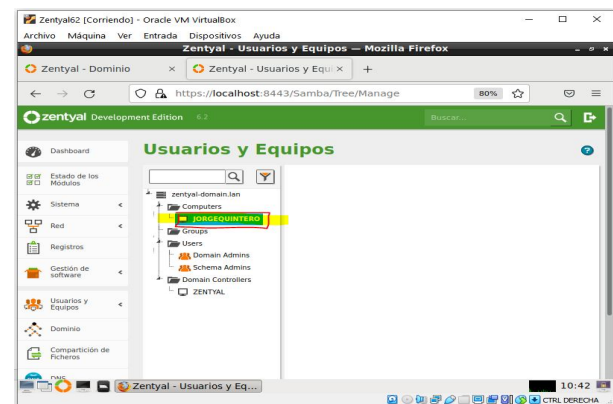


Figura 26. Computadores unidos al dominio.

Se reinicia la maquina cliente y se inicia sesión con el usuario creado en Zentyal; es decir con el usuario "jorgeqdesktop", para esto, cuando se solicite el usuario, se digita "zentyal-domain\jorgeqdesktop" y luego la contraseña establecida como se puede observar en la figura 27:

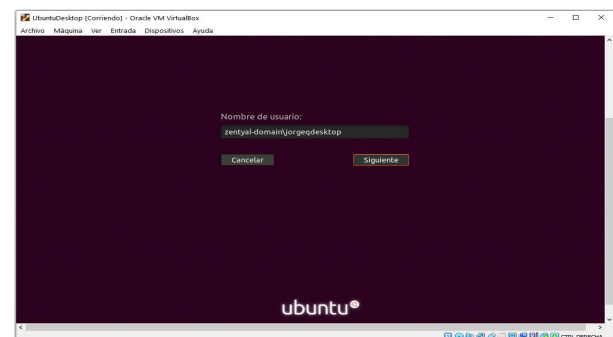


Figura 27. Ingresar al dominio.

Una vez iniciada la sesión, se abre una terminal y se puede ver que efectivamente se está conectado al dominio "Zentyal-domain" con el usuario "jorgeqdesktop" y con la maquina "jorgequintero" como se puede observar en la figura 28:

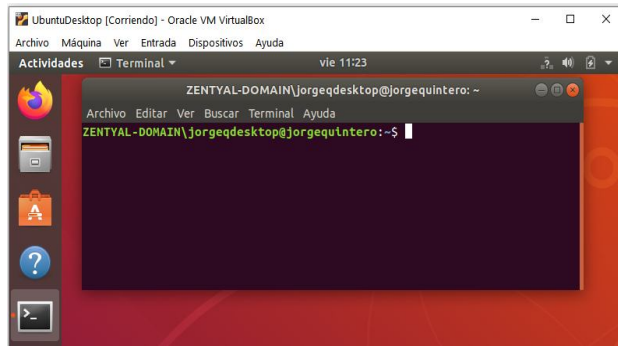


Figura 28. Evidencia del ingreso al dominio.

4 TEMÁTICA 2: PROXY NO TRANSPARENTE

Una vez iniciado el servidor podemos observar en la figura 29 y 30 la pantalla de inicio de configuración de Zentyal y posteriormente el dashboard o panel de control.



Figura 29. Configuración inicial de Zentyal.

Se realiza la búsqueda para posteriormente desplegar la lista de los programas a instalar, ver figura 30.

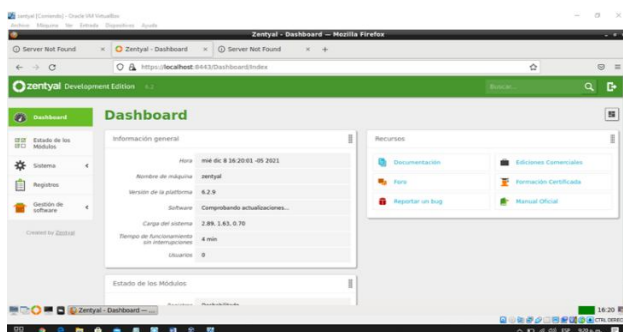


Figura 30. Pantalla de inicio de Zentyal.

Se instala el módulo de red para que podamos configurarlo y los clientes puedan conectarse a Internet a través del servidor. Para ellos se da clic en "Gestión de software> Componentes Zentyal" y se selecciona la configuración, como se puede observar en la figura 31 y 32.

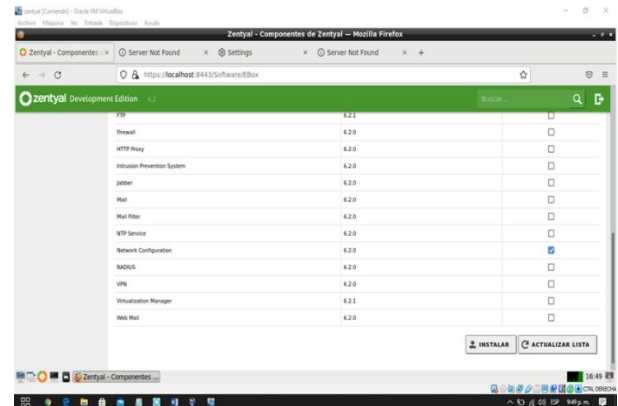


Figura 31: Configuración de red en Zentyal.

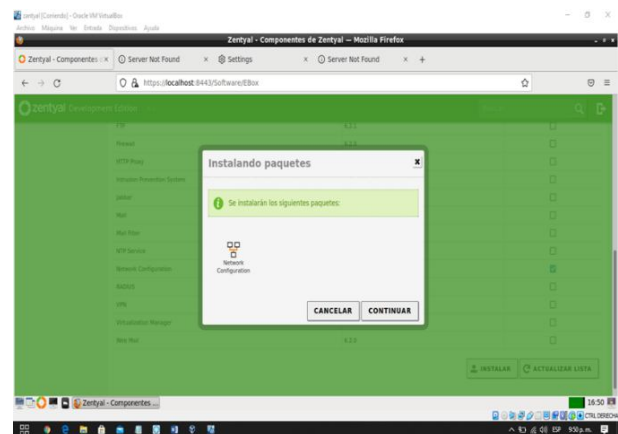


Figura 32. Instalación de Red en Zentyal.

El instalador de paquetes se da clic en continuar para que se instalen los programas seleccionados, ver figura 33

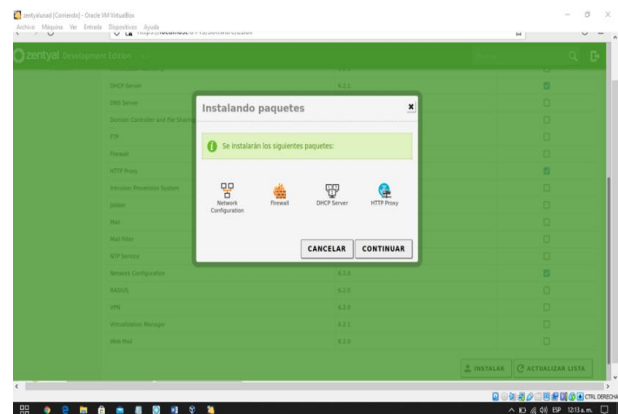


Figura 33. Instalación de Red en Zentyal.

Selección del Módulo HTTP Proxy, DHCP, a Instalar.

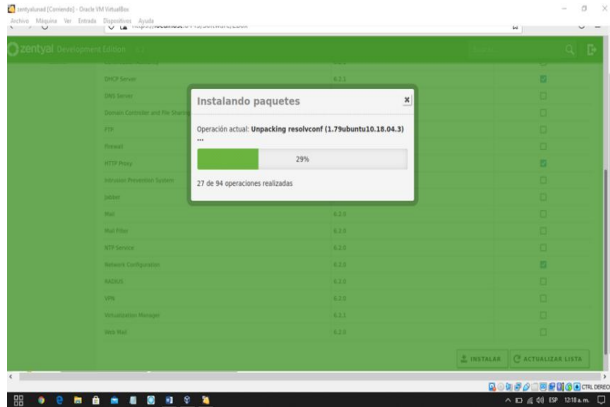


Figura 34. Instalación de Red en Zentyal.

En la figura 35 se hace la configuración general del proxy transportador.

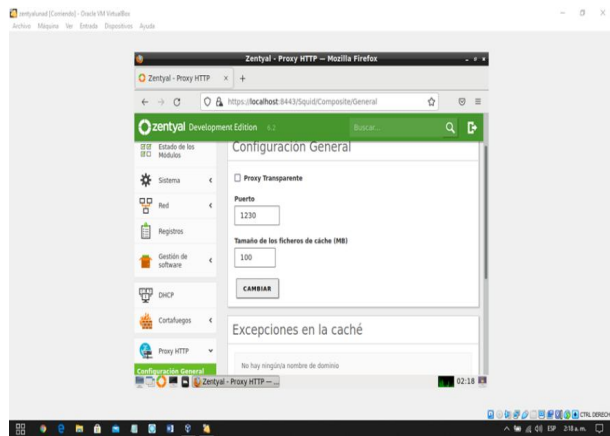


Figura 35. Módulo de Configuración de Red Instalado.

En la figura 36 se añade el perfil de filtrado

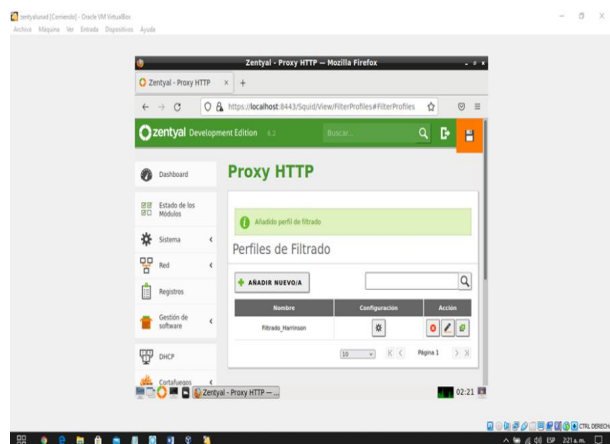


Figura 36. Módulo de Configuración de Red Instalado HTTP Proxy.

En la figura 37 se hace el bloqueo del dominio de red una vez ya añadido y configurado el perfil de filtrado

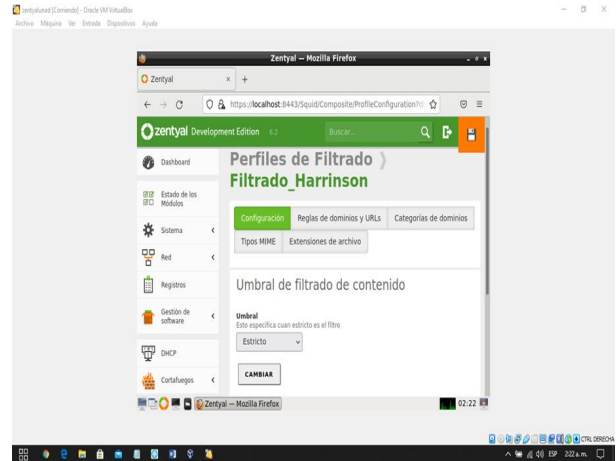


Figura 37. Bloqueando Dominios de Red.

Se añade las reglas de dominio y en el proxy se añaden las reglas de acceso, ver figuras 38 y 39.

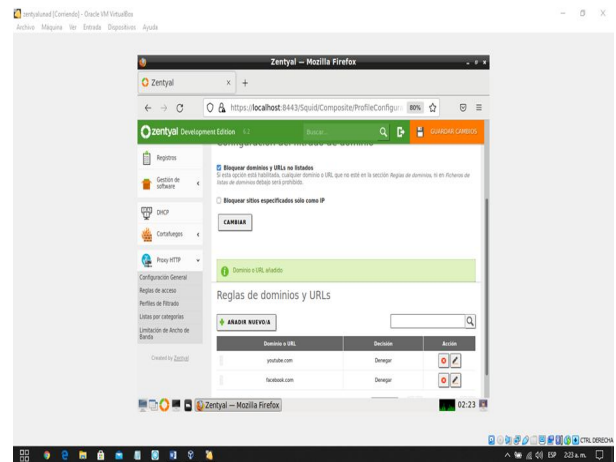


Figura 38. Bloqueando Dominios de Red.

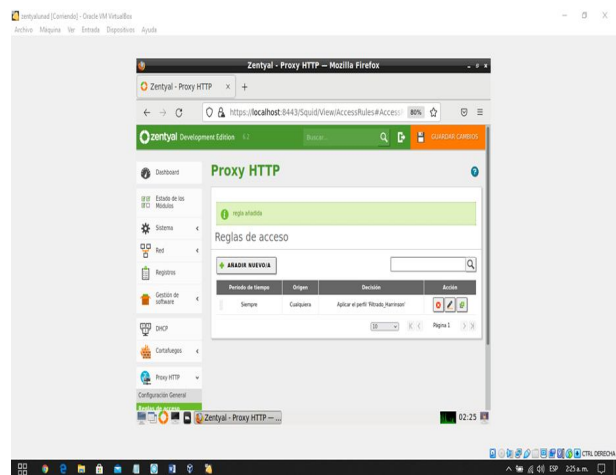


Figura 39. Creando Perfil de Filtrado HTTP Proxy.

Una vez finalizada la configuración, al tratarse de un proxy no transparente, se debe especificar en el

desde herramientas en Zentyal, como se puede evidenciar en las figuras 47 y 48.

```

Archivo Editar Pestañas Ayuda
catalinamosquera@zentyal:~$ ping www.youtube.com
PING youtube-ui.l.google.com (142.250.64.206) 56(84) bytes of data:
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=1 ttl=110 time=57.3 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=2 ttl=110 time=57.5 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=3 ttl=110 time=58.0 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=4 ttl=110 time=58.4 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=5 ttl=110 time=57.1 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=6 ttl=110 time=57.7 ms
64 bytes from mia07556-in-f14.1e100.net (142.250.64.206): icmp_seq=7 ttl=110 time=58.9 ms
^C
--- youtube-ui.l.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6019ms
rtt min/avg/max/mdev = 57.146/57.897/58.972/0.655 ms
catalinamosquera@zentyal:~$

```

Figura 47. Verificación de conexión a YouTube.

```

Archivo Editar Pestañas Ayuda
catalinamosquera@zentyal:~$ ping www.instagram.com
PING z-p42-instagram.c10r.instagram.com (157.240.6.174) 56(84) bytes of data:
64 bytes from instagram-p42-shv-01-bog1.fbcdn.net (157.240.6.174): icmp_seq=1 ttl=58 time=9.73 ms
64 bytes from instagram-p42-shv-01-bog1.fbcdn.net (157.240.6.174): icmp_seq=2 ttl=58 time=10.3 ms
64 bytes from instagram-p42-shv-01-bog1.fbcdn.net (157.240.6.174): icmp_seq=3 ttl=58 time=9.72 ms
64 bytes from instagram-p42-shv-01-bog1.fbcdn.net (157.240.6.174): icmp_seq=4 ttl=58 time=9.49 ms
^C
--- z-p42-instagram.c10r.instagram.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 9.495/9.830/10.363/0.337 ms
catalinamosquera@zentyal:~$

```

Figura 48. Verificación de conexión a Instagram.

Ahora se definen las reglas según las necesidades, primero se bloqueó YouTube, se coloca dirección IP y añadir, ahora se añade la regla para bloquear Instagram como se observa en las figuras 49 y 50.

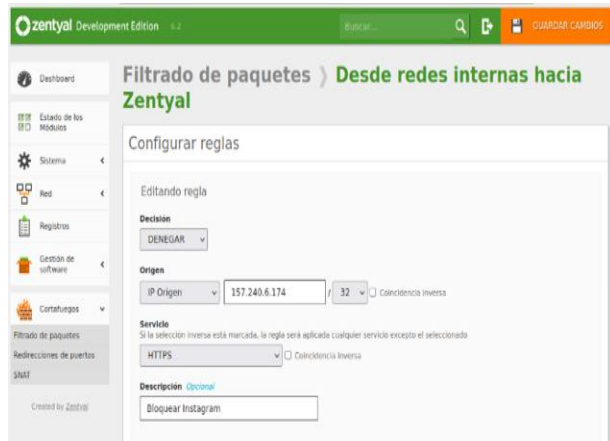


Figura 49. Bloqueo de YouTube.

Ahora añadimos la regla para bloquear Instagram.



Figura 50. Bloqueo de Instagram.

Las reglas añadidas se pueden observar en la figura 51.



Figura 51. Módulo de reglas.

Ahora se comprueba desde la máquina cliente que no hay acceso a dichas páginas como se evidencia en las figuras 52 y 53.

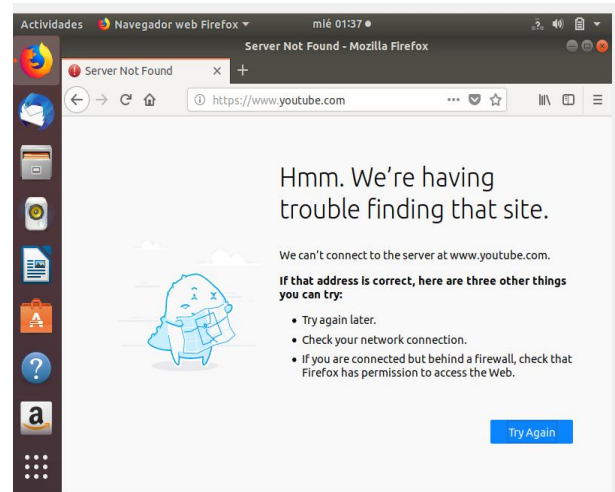


Figura 52. Acceso a YouTube bloqueado.

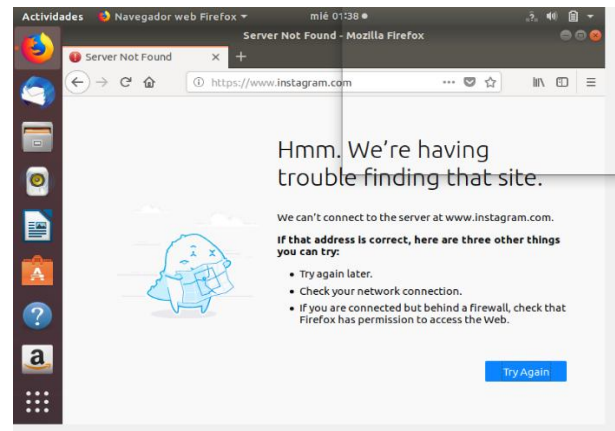


Figura 53. Acceso a Instagram bloqueado.

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

El servidor de archivos o file server se encarga de administrar y proporcionar archivos en red haciendo que estos se encuentren disponibles en la red, permite que sean descargados, modificarlos o eliminarlos dependiendo el perfil que se asigne a los usuarios de un determinado dominio o grupo de trabajo para los cuales estará estos disponibles [5].

Una vez que el dominio y el uso de archivos compartidos este habilitado se procede a ingresar a la pestaña del dashboard llamado Compartición de Ficheros, en este definimos el nombre del recurso a compartir, ruta del recurso compartido, un comentario si se desea y se da clic en el botón añadir como se observa en la figura 54.

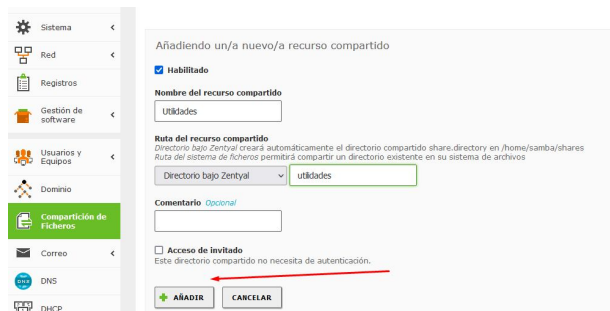


Figura 54. Creación de recurso compartido.

Con esto se creará el recurso compartido, luego se debe dar el acceso a los usuarios que van a poder interactuar con el recurso creado, para esto se da clic en el boto de control de acceso figura 55.

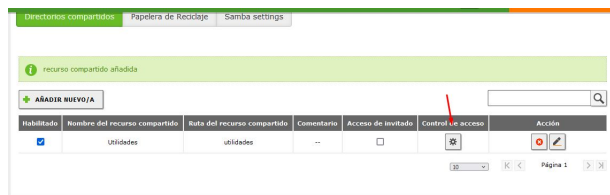


Figura 55. Control de Acceso.

Una vez se ingresa en esta pestaña puede añadir el usuario del dominio que tendrá acceso al recurso compartido y también se define el tipo de permiso que tendrá sobre el recurso, escritura, lectura o ambos, se da clic en el botón añadir para continuar. cómo se observa en la figura 56.

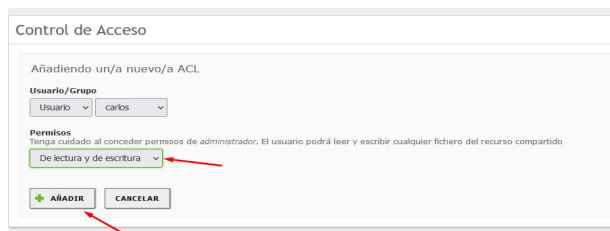


Figura 56. Otorgar permisos.

Una vez añadido el usuario y otorgado los permisos requeridos se procede a iniciar sesión en el equipo Ubuntu que se encuentra dentro del dominio con un usuario previamente creado en el dominio como se muestra en la figura 57.

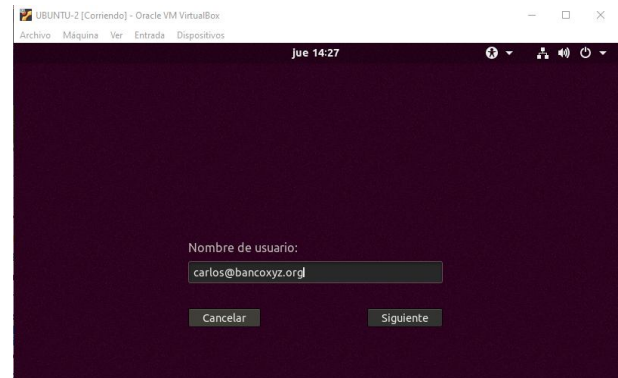


Figura 57. Inicio de sesión en el dominio.

Se abre el directorio archivos, otras ubicaciones y en la parte de abajo se realiza la conexión a al recurso compartido de la siguiente forma smb://dirección del servidor/nombre del recurso compartido como se observa en la figura 58.

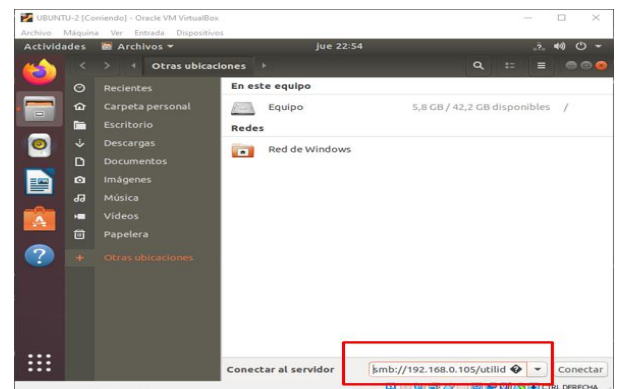


Figura 58. Configuración carpeta de red.

Una vez encontrado el recurso el sistema solicitará el usuario de dominio y contraseña como una medida de seguridad, como se observa en la figura 59.

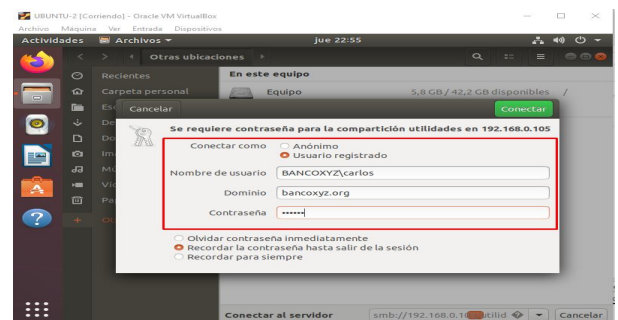


Figura 59. credenciales carpeta de red.

Luego de digitar las credenciales de red se puede validar que cuenta con los permisos de escritura

dentro de la carpeta de red, se crea una carpeta de red llamada carpeta de prueba como se evidencia en las figuras 60 y 61.

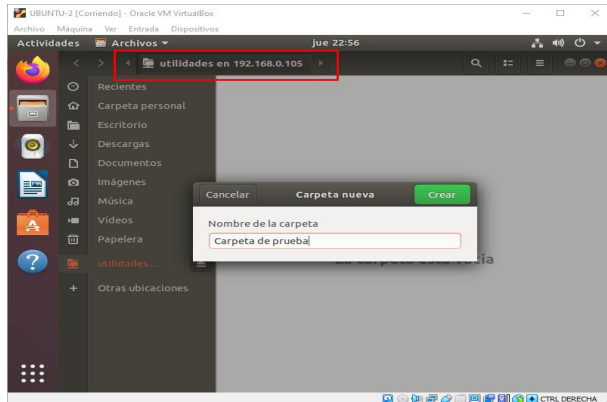


Figura 60. Comprobar permisos de escritura.

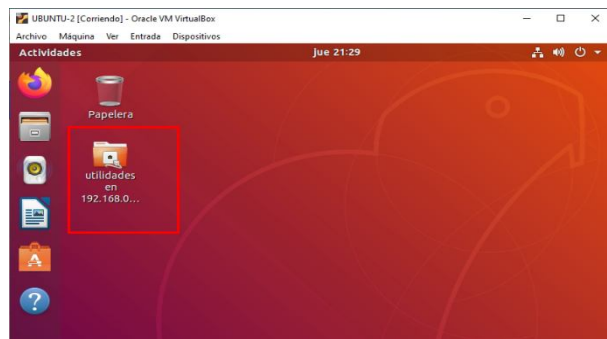


Figura 61. Carpeta de red compartida.

6.1 PRINT SERVER

Desde la versión 5 de Zentyal se eliminó del dashboard la administración de impresoras compartidas por lo que se hace necesario realizar la instalación de los paquetes cups directamente en el servidor Zentyal, con el siguiente comando se realiza la instalación de los paquetes directamente en el servidor, se da clic en S para continuar cuando lo solicite como se observa en la figura 62.

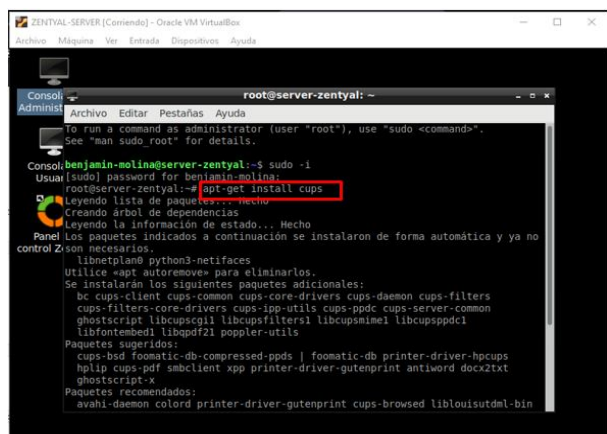


Figura 62. Instalación paquetes cups.

Una vez instalados los paquetes cups se deben iniciar y posteriormente se dejan en estado habilitados para que estén disponibles en cada inicio de sesión.

Start para iniciar y enable para disponibilidad utilizando los comandos que se observan en la figura 63.

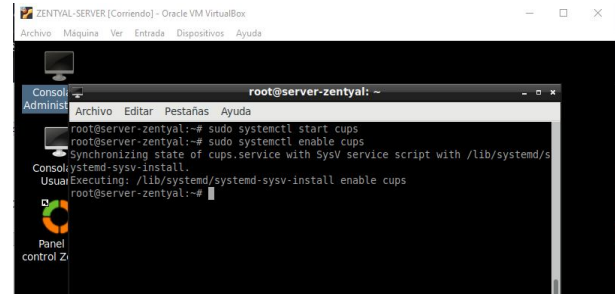


Figura 63. Puesta en marcha paquetes cups.

Se puede acceder a él de la siguiente manera <https://ip servidor:631> como se observa en la figura 64.

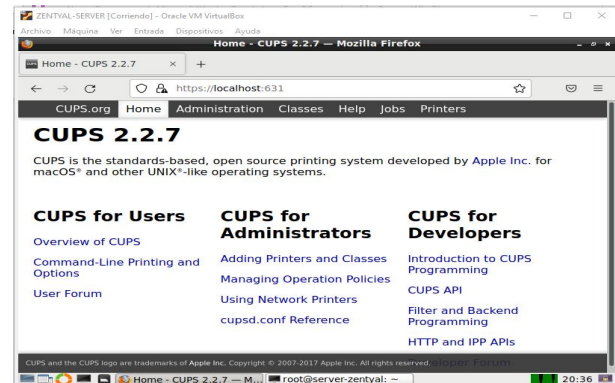


Figura 64. Dashboard cups 2.2.7.

Una vez instalados cups y tener acceso se instala una impresora en Zentyal para posteriormente compartirla utilizando el comando de la figura 65.

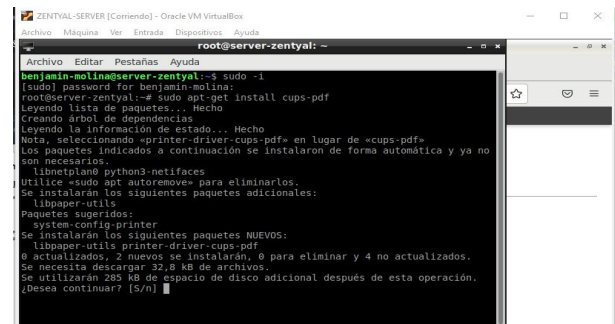


Figura 65. Instalación impresora Por Compartir.

Una vez instalada se procede a realizar la configuración, en la pestaña administración, y selecciona la impresora que se acaba de instalar, se asigna un nombre a la impresora, una descripción y se selecciona la opción de compartir para que sea visible para los otros equipos en la red como se observa en la figura 66.

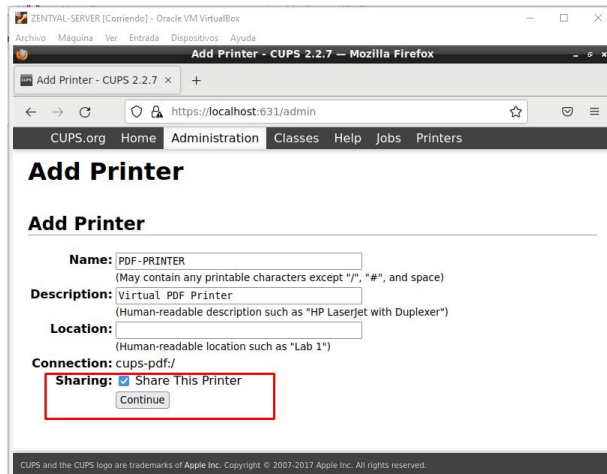


Figura 66. Compartir impresora.

Una vez configurado se debe ir al equipo Ubuntu para añadir la impresora en red, se abre la configuración, impresoras y añadir impresora. Se selecciona la opción servidor y luego conectar, como se observa en la figura 67.

Se escribe la ruta de la impresora de la siguiente forma cups-brf://dirección del servidor/ nombre de la impresora compartida/ y se da clic en siguiente como se observa en la figura 67.

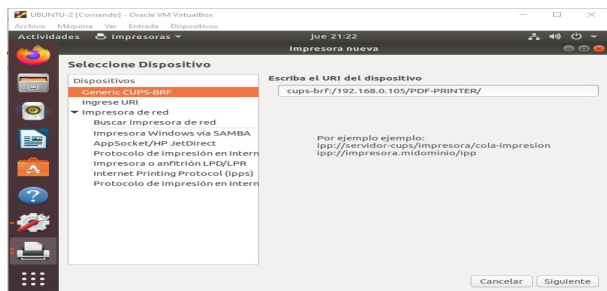


Figura 67. Configurando impresora.

Una vez terminado mostrara un mensaje donde se puede hacer una impresión de prueba figura 68.

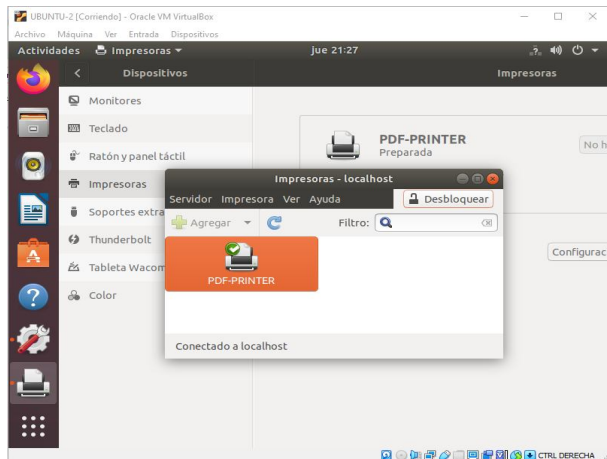


Figura 68. Fin de la configuración.

Se observa en el servidor en la pestaña de trabajos que se realiza una impresión, ver figura 69.

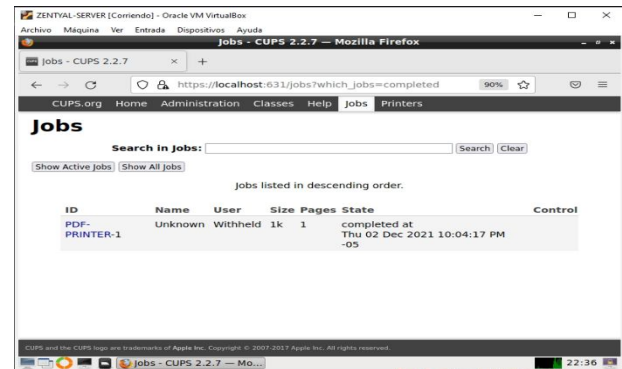


Figura 69. Trabajo de impresión realizado.

7 TEMÁTICA 5: IMPLEMENTACIÓN Y CONFIGURACIÓN DETALLADA DE LA CREACIÓN DE UNA VPN

Una VPN (virtual private network) es una tecnología en redes que nos permite la conexión de uno o más equipos desde redes externas a una red privada a través de internet.[6]

Con el servidor instalado se procede a instalar los paquetes para la configuración de la VPN como se observa en la figura 70.

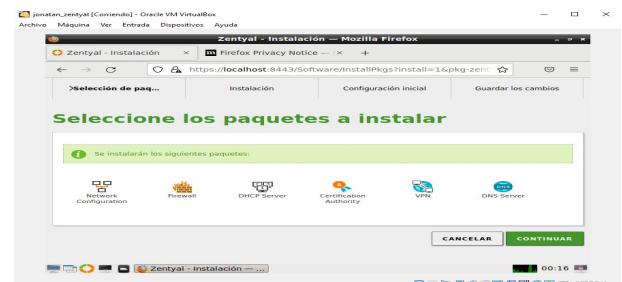


Figura 70. Instalación de paquetes.

Se inicializan los módulos instalados como se observa en la figura 71.

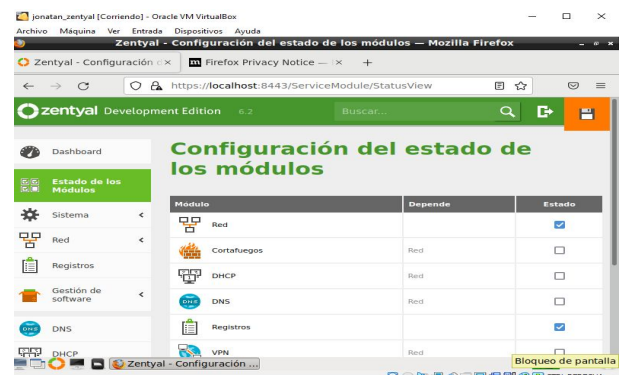


Figura 71. Inicialización de los módulos.

Teniendo en el servidor dos dispositivos de red, uno para red interna y otro para salida a internet para el servidor, se configura cada interfaz, con las direcciones ip detalladas en cada imagen a continuación, figura 72, 73 y 74:

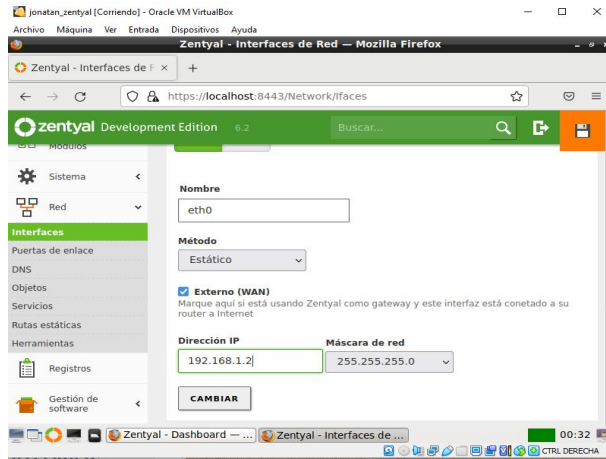


Figura 72. Configuración interfaz para conexión a internet.

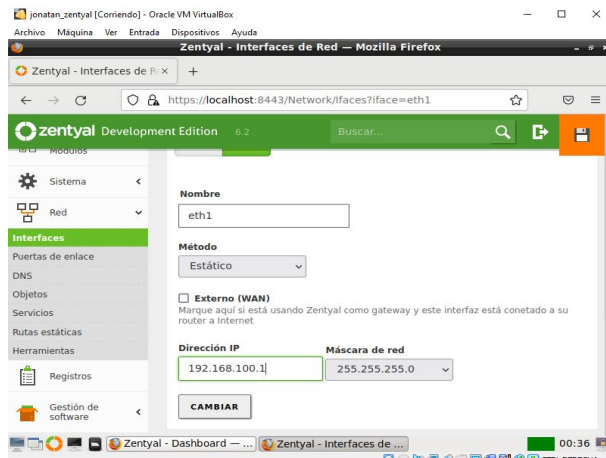


Figura 73. Configuración interfaz para conexión a red interna.

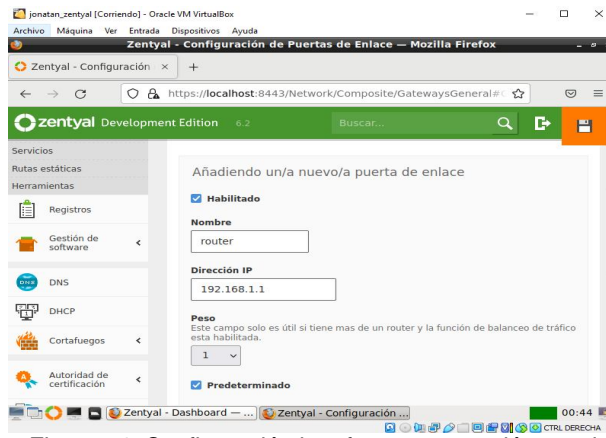


Figura 74. Configuración interfaz para conexión a red interna.

Se configura el firewall para las conexiones a las redes internas hacia el servidor Zentyal como se puede observar en la figura 75:

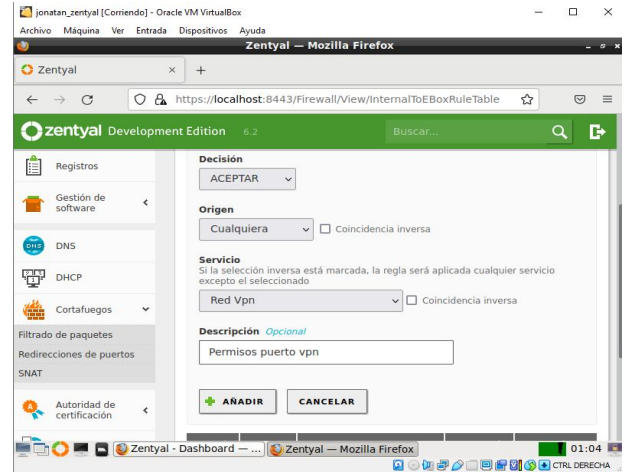


Figura 75. Configuración servicio.

Se verifica conexión, activa como se puede observar en la figura 76.

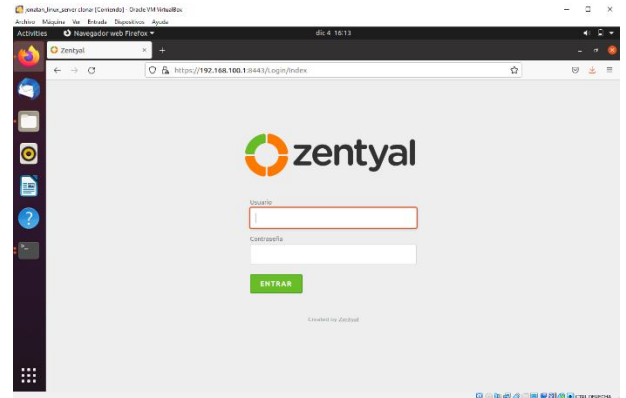


Figura 76. Verificación conexión.

Es necesario crear un servidor VPN para la configuración como se detalla en la figura 77.

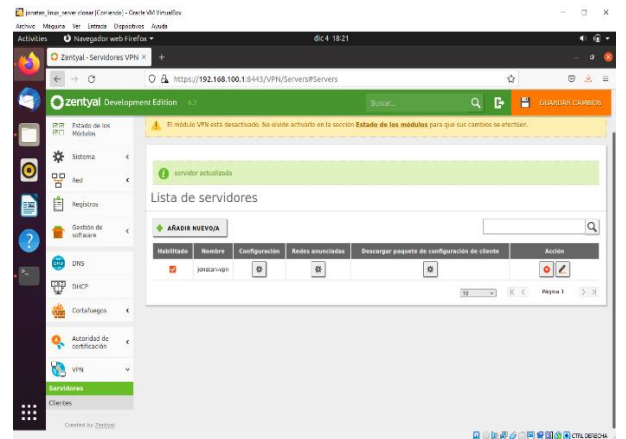


Figura 77. Creación servidor VPN.

Luego de creado el servidor se realiza la configuración como se observa en la figura 78.

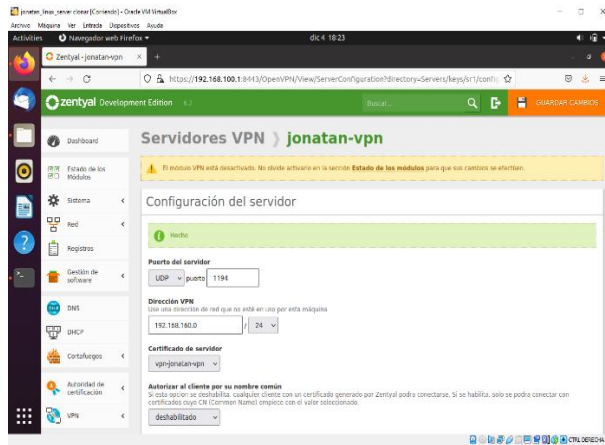


Figura 78. Configuración servidor creado.

Se crea el certificado para la conexión del cliente como se observa en la figura 79.

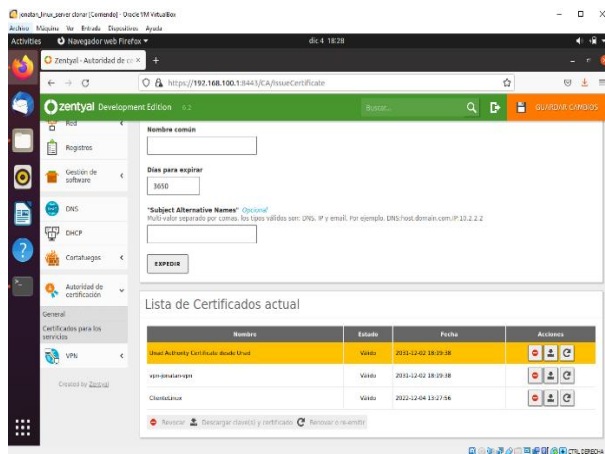


Figura 79. Creación certificada.

Se valida la ejecución del servidor como se ve en la figura 80.

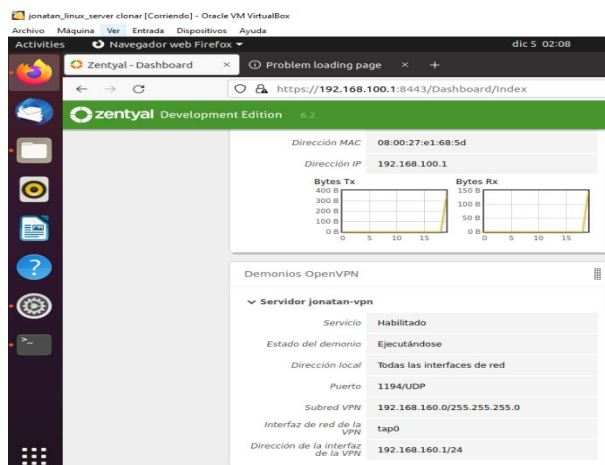


Figura 80. Validación servidor VPN.

Se descarga la configuración para conectar al cliente (se realizan pruebas con Windows y Linux) como se observa en la figura 81.

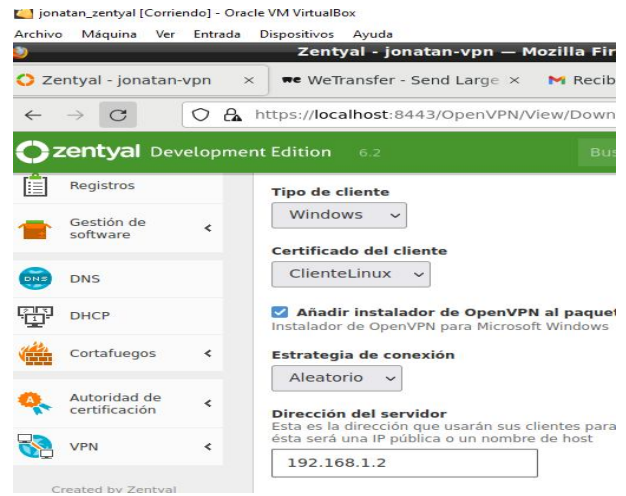


Figura 81. Descargar paquete de configuración cliente.

Se verifica que el cliente Linux tenga otra ip diferente a la red interna del servidor como se observa en la figura 82.

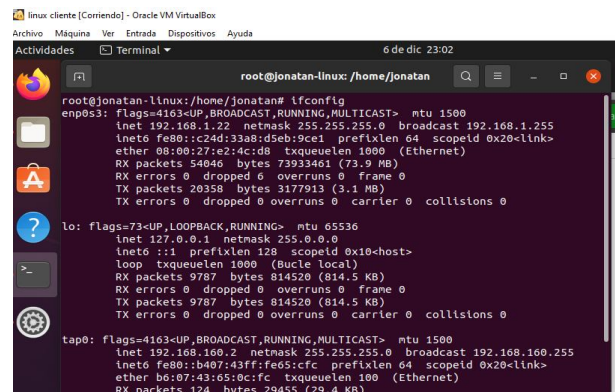


Figura 82. Evidencia ip cliente.

Se ingresa a la configuración de redes del cliente Linux para configurar la VPN como se observa en la figura 83.



Figura 83. Configuración VPN en el cliente Linux.

Luego de la configuración realizado e inicialización de la VPN desde el cliente se valida la conexión como se observa en la figura 84.

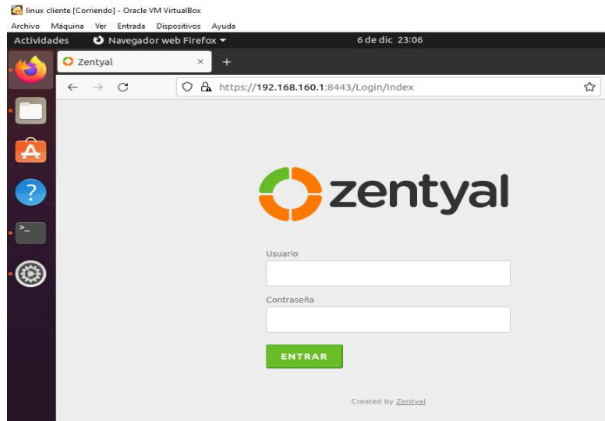


Figura 84. Validación acceso al servidor desde la VPN.

8 CONCLUSIONES:

Con un el servicio DHCP se pueden asignar direcciones IP a equipos clientes que se conecten a la red interna. Esto facilita la administración en redes donde hay muchos computadores y la asignación manual de direcciones IP podría resultar en una tarea demorada de gestionar. Un servidor DNS permite la asociación de nombres de dominio a direcciones IP y de esta manera los equipos clientes puedan identificar el servidor no solo con una IP sino también con un nombre. Un controlador de dominio permite que una maquina cliente se una al dominio del servidor y pueda acceder a recursos compartidos.

En muchas organizaciones privadas o gubernamentales, instituciones educativas, etc., es necesario restringir el acceso a determinados servicios de red o sitios web, entre otros, por motivos de seguridad o por cualquier otro motivo especificado dentro de la organización, por ello es fundamental Implementar un proxy http que deniegue o permita el acceso a determinados servicios, pudiendo así controlar lo que pueden hacer los usuarios o empleados conectados a la red.

Con la realización del trabajo se fortalecieron los conceptos relacionados con la seguridad en la red, también se conoció sobre algunas herramientas que permiten realizar los procesos de aplicación de seguridad de forma óptima, como lo son los cortafuegos. Con el desarrollo de esta actividad se conocieron algunos conceptos, ejemplos y mecanismos de prevención muy interesante que posibilitan mantener nuestra maquinas o dispositivos de forma más resguardados a posibles filtraciones.

La implementación de file server permite la fácil administración de recursos compartidos como carpetas de red asignando los permisos requeridos por cada

usuario según sea asignados por el área encargada de indicar con que permisos cuenta cada colaborador de la compañía según su cargo a desempeñar, así también podemos compartir impresoras en red y hacer seguimiento a la cola de impresión de una forma efectiva.

En la administracion y gestion de la infraestructura IT se hace indispensable aplicar las mejores practicas de seguridad posible, con el uso de Zentyal Server como sistema operativo base tenemos la funcionalidad de añadir una capa adicional de seguridad haciendo uso del servicio de VPN como conexión a la red local del servidor, permitiendo que un equipo cliente que este fuera de la red tenga acceso a la red local mediante el acceso a la VPN con las configuraciones de seguridad siendo necesario un certificado que permita la conexión al servidor, de esta manera tenemos un acceso desde una red externa a la red interna aplicando buenas practicas de seguridad, disminuyendo asi el riesgo de intrusiones y ataques.

9 REFERENCIAS

- [1] Instalación — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. Recuperado 3 de diciembre de 2021, de <https://doc.zentyal.org/6.2/es/installation.html#el-instalador-de-zentyal>
- [2] Servicio de configuración de red (DHCP) — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. Recuperado 3 de diciembre de 2021, de <https://doc.zentyal.org/6.2/es/dhcp.html>
- [3] Servicio de resolución de nombres de dominio (DNS) — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. Recuperado 3 de diciembre de 2021, de <https://doc.zentyal.org/6.2/es/dns.html>
- [4] Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. Recuperado 3 de diciembre de 2021, de <https://doc.zentyal.org/6.2/es/directory.html>
- [5] 6.2, Z. (5 de 12 de 2021). Zentyal file server. Obtenido de Zentyal file server: <https://doc.zentyal.org/6.2/en/filessharing.html>
- [6] Wiki.zentyal.org. (2019). Es/3.5/Servicio de redes privadas virtuales (VPN) con OpenVPN -Zentyal Linux Small Business Server. [Pagina Web] Recuperado de: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_%28VPN%29_con