

IMPLEMENTACIÓN DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN (TI) A TRAVÉS DE LA HERRAMIENTA DE GESTIÓN GNU/LINUX ZENTYAL SERVER

Freddy Alberto Solano Correa
e-mail: fasolanoco@unadvirtual.edu.co
Juan Sebastián Corredor Novoa
e-mail: jscorredorn@unadvirtual.edu.co
Julio Cesar Ladino Alonso
e-mail: jcladinoal@unadvirtual.edu.co

RESUMEN: El presente trabajo muestra todo el proceso que se llevó a cabo para realizar la instalación y configuración de una distribución GNU/Linux basada en Ubuntu como lo es Zentyal Server 6.2 acuerdo los parámetros establecidos. De igual forma se evidencia como a través de Zentyal Server 6.2 se realizó la instalación y configuración de diferentes servicios útiles para la administración de una infraestructura TI, dentro de estos servicios tenemos: Proxy no transparente, File Server y Print Server y VPN. La instalación y comprobación del funcionamiento de cada uno de los servicios mencionados, se realizó en máquinas virtuales creadas en VirtualBox con características básica y específicas para soportar dichos servicios.

PALABRAS CLAVE: Controlador de Dominio, DNS Server, File Server, Proxy no transparente, Print Server y VPN.

1 INTRODUCCIÓN

Es de vital importancia que como futuros profesionales del área de las tecnologías de la información y las comunicaciones (TIC), adquirir nuevos conocimientos y entender cómo a través de estos se pueden brindar nuevas soluciones a las empresas para que estas aprovechen de una mejor manera sus recursos.

Es por ello por lo que en el presente documento se plasmaran cada uno de esos conocimientos adquiridos, donde a través de la instalación y configuración de Zentyal Server 6.2 se administraran los servicios establecidos en cada una de las temáticas descritas en la guía de actividades; mostrando de esta forma su configuración y funcionamiento desde las máquinas virtuales dispuestas para la simulación de la infraestructura TI implementada.

2 INSTALACIÓN ZENTYAL SERVER 6.2

2.1 REQUISITOS MÍNIMOS DE HARDWARE

Para la instalación de Zentyal Server 6.2 y cada uno de sus paquetes, es indispensable saber qué servicios se van a implementar en la infraestructura TI, para de esta forma establecer el hardware que vamos a requerir, es por ello por lo que se pudo establecer que los requisitos mínimos son 8GB de RAM, procesador Intel Core i5 en adelante y en cuanto al tamaño de disco, este se encuentra limitado a los datos, ya que en este se ira almacenando la cache y log de cada uno de los servicios implementados, pero podemos decir que con un disco de 40GB en adelante es lo más óptimo.

2.2 ENLACE DE DESCARGA

<https://zentyal.com/es/news/zentyal-6-2-announcement-2/>

2.3 PASO A PASO DE INSTALACIÓN

Como primera parte de la instalación de Zentyal Server 6.2, este nos pide que seleccionemos el lenguaje, una vez seleccionado el lenguaje nos lleva a un menú en donde indicaremos que Zentyal Server 6.2 se instalara en todo el disco, lo que indica que no haremos ningún tipo de partición y que todos los datos se copiaran en todo el disco, ver Fig. 1.



Figura 1. Modo de instalación de Zentyal Server.

Después de realizar lo establecido en la Fig. 1, se pide que se seleccione la ubicación y la distribución del teclado acuerdo a la región en la que nos encontramos,

dando inicio a la carga de los componentes adicionales y el reconocimiento de tres adaptadores de red, los cuales serán usados para el desarrollo de la actividad según sea la necesidad, para este caso se hará uso del adaptador eth0 como adaptador puente para poder realizar las actualizaciones necesarias de Zentyal Server 6.2, ver Fig. 2.



Figura 2. Adaptadores de red.

Una vez seleccionado el adaptador principal que usara Zentyal Server 6.2, se realiza una configuración automática del adaptador de red asignado mediante DHCP la dirección ip que usara, seguidamente de esto pedirá que se le de un nombre a la máquina, ver Fig 3.

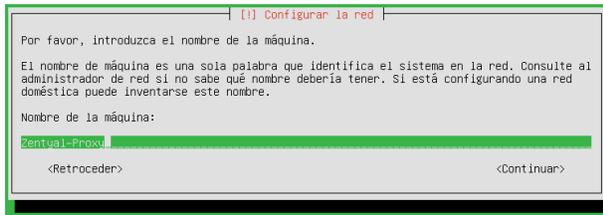


Figura 3. Configuración DHCP de la red.

Después de darle nombre a la máquina se pedirá de igual forma que se cree un nombre de usuario y una contraseña los cuales serán utilizados para acceder al dashboard de Zentyal Server 6.2, de esta forma se termina la configuración y se da inicio al proceso de instalación de los paquetes y librerías necesarios para el funcionamiento del servidor. Ver Fig. 4.



Figura 4. Configuración DHCP de la red.

Al término de la instalación de todos los paquetes y librerías, la máquina se reiniciará e iniciará con una instalación faltante de paquetes del core de Zentyal. Terminada la instalación de paquetes del core, la máquina da inicio al servidor presentando como primera ventana el navegador de Mozilla donde en la url indica <https://localhost:8443>, siendo el 8443 el puerto usado por Zentyal para acceder a él y el cual lleva al inicio de sesión de Zentyal; para el acceso al dashboard de Zentyal, se usa como credenciales de acceso el usuario y la contraseña configuradas durante el proceso de configuración previos a la instalación de Zentyal.

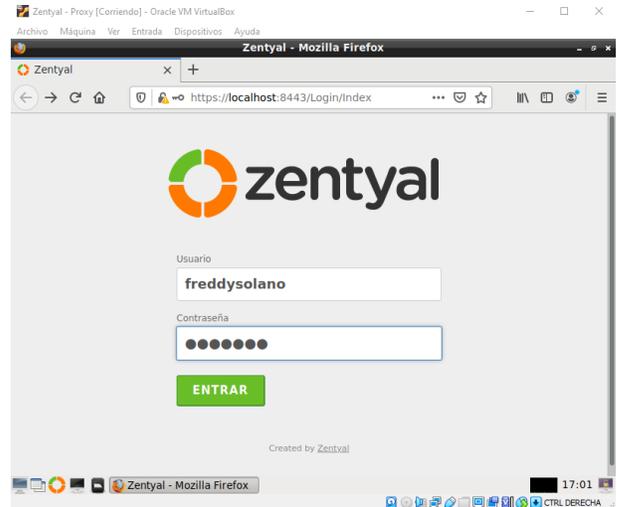


Figura 5. Inicio de sesión Zentyal.

Una vez se realiza la validación de credenciales configuradas, se presenta una ventana de configuración inicial, a lo cual se le da clic en Continuar. Después de esto se presenta una ventana en donde se puede seleccionar los paquetes de Zentyal a instalar. Para el desarrollo de las temáticas que se van a desarrollar en el presente documento, se instalarán los paquetes necesarios para la implementación de servicios tales como Controlador de Dominio, DHCP Server, DNS Server, File Server, Proxy no transparente, Print Server y VPN.

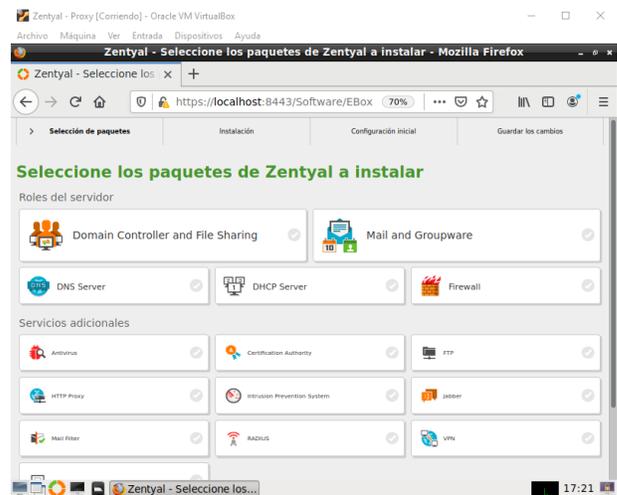


Figura 6. Configuración inicial Zentyal.

Teniendo en cuenta lo anterior y seleccionado el paquete requerido de acuerdo a las temáticas establecidas en la guía, se inicia con la instalación de cada uno de los paquetes necesarios para el uso de los servicios que se configurarán e implementarán, dando de esta forma a la explicación de las temáticas.

3 TEMÁTICA 2. PROXY NO TRANSPARENTE.

El desarrollo de esta actividad conlleva la implementación de un proxy no transparente, para ello tenemos que un proxy es un servicio prestado por un servidor en el cual un cliente realiza peticiones de acceso a páginas web y el servidor en el que se encuentra el proxy las recibe y las transfiere a los servidores en donde se encuentran las diferentes paginas web, de esta forma las páginas web no sabrán la ip de los clientes debido a que hay un servicio intermediario entre el cliente y la pagina web que es el proxy, por lo que la ip que quedara registrada es la del servidor proxy.

En cuanto a lo que se refiere al proxy no transparente, se diferencia al proxy transparente en que el no transparente requiere conocer la ip del servidor proxy y el puerto que va a usar.

Para configurar el proxy no transparente lo que hacemos es instalar el paquete HTTP Proxy el cual podemos ver encerrado en un recuadro rojo como se observa en la Fig. 7. , dando después de la selección del paquete clic en INSTALAR.

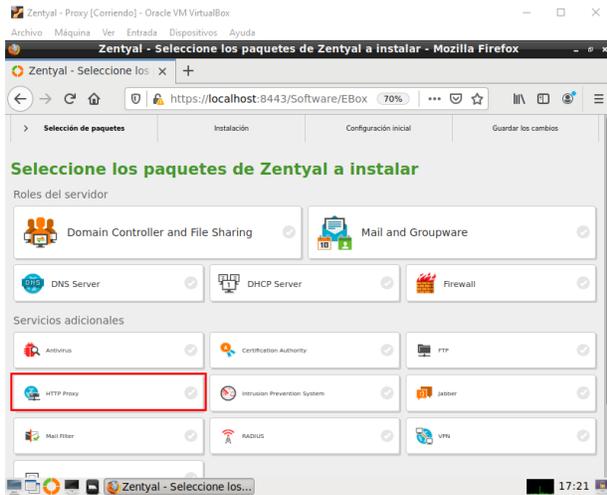


Figura 7. Paquete HTTP Proxy.

Seguidamente a lo anteriormente descrito, se nos indicara los paquetes que se van a instalar y los cuales va a usar el HTTP Proxy para su correcto funcionamiento, teniendo conocimiento de los paquetes que se van a instalar se da clic en CONTINUAR y con ello se da inicio a la instalación de paquetes.

Al termino de la instalación de paquetes se procede a realizar una serie de configuraciones, entre ellas se debe realizar una configuración a las interfaces de red en donde indicaremos el tipo de conexión que estas deben tener, para tal caso indicamos que la eth0 va a ser de tipo External, es decir que por esta va a llegar todo el trafico proveniente de internet y para la eth1 y eth2, va ser de tipo Internal lo que significa que hacen parte de mi red LAN y de la DMZ.

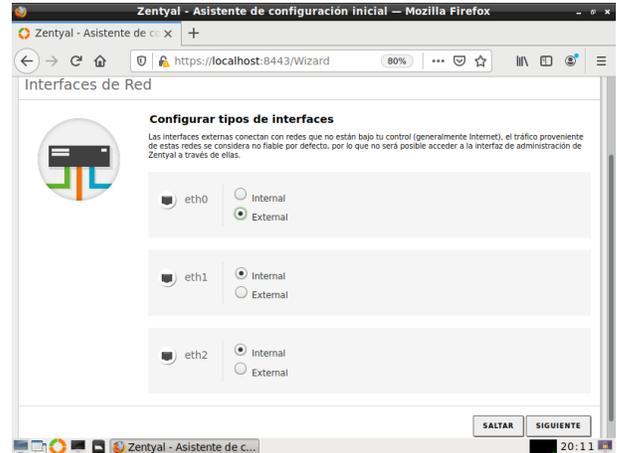


Figura 8. Configuración tipo de interfaces.

Continuando con las configuraciones de red, se debe establecer como se obtendra la dirección ip para cada interfaz, para tal caso la la eth0 asignara ip por DHCP, la eth1 y la eth2, hara la asignación de forma estatica, es decir que se establece de forma manual, como se observa en la Fig. 9.

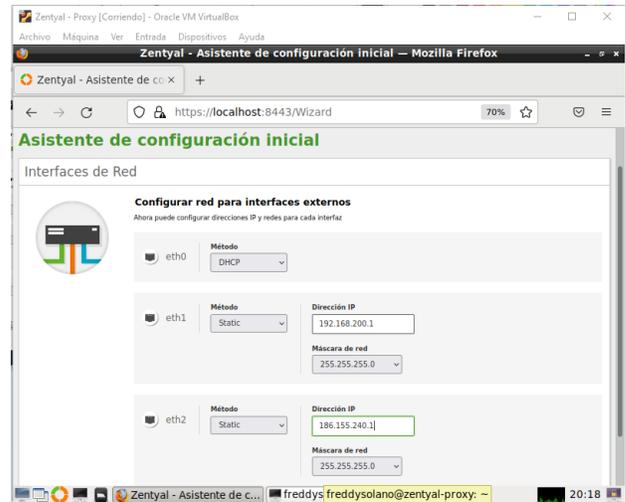


Figura 9. Configuración ip interfaces de red.

Una vez terminada de realizar la configuración de las interfaces de red, procedemos a continuar con los siguientes pasos para poner en marcha el proxy no transparente.

Es por ello que se puede observar al termino de lo anteriormente dicho el dashboard de Zentyal en donde se nos presenta una interfaz con difrente información y un menú en donde se encuentran diferentes opciones para configurar.

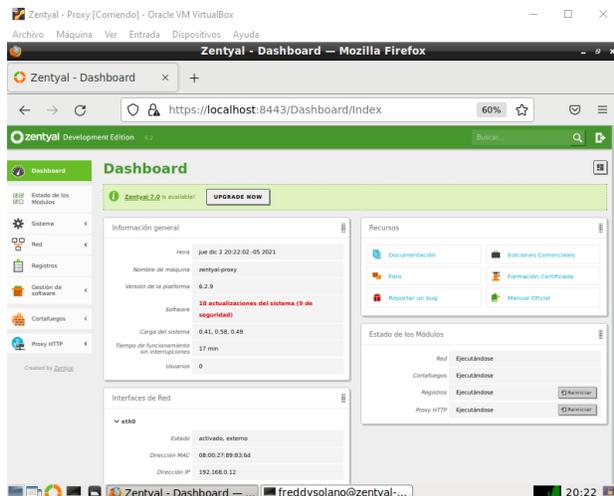


Figura 10. Dashboard Zentyal.

Una vez en el dashboard se ingresa a la opción de Proxy HTTP y seguidamente en la opción Configuración General, en donde se establece que el proxy es no transparente dejando sin chequear el cuadro de Proxy Transparente y colocando como puerto el 1230, tal como lo pide la guía de actividades.

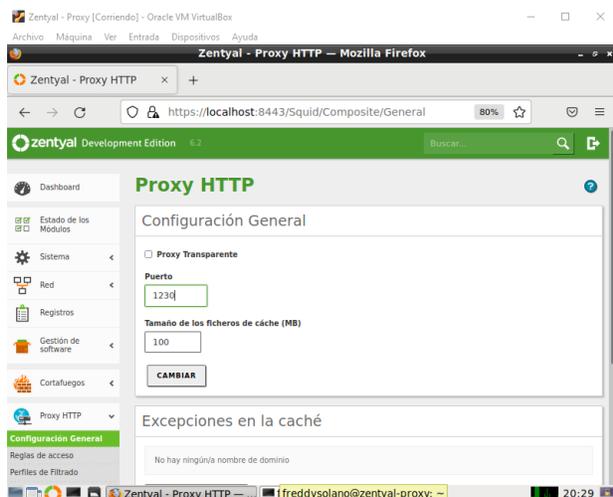


Figura 11. Configuración general Proxy HTTP.

Al terminar de realizar la Configuración General del Proxy HTTP, se procede a configurar la interfaz de red de la maquina que cuenta con Ubuntu Desktop, y la cual saldra a travez del proxy no transparente. Es de tener en cuenta que la ip que se configura de estar dentro del segmento establecido para la eth1 configurada anteriormente en la Fig. 11.



Figura 12. Configuración de ip en Ubuntu Desktop.

Terminada la configuración de la Fig. 12, se continua a configurar el proxy no transparente en el navegador del cliente, para este caso lo hacemos en Mozilla, para eso se dirige a Ajustes y seguidamente a Configuraciones de Conexión en donde se selecciona la opción de Configuración manual del proxy.



Figura 13. Configuración acceso proxy a internet.

Se procede a verificar la conexión a internet a través del proxy no transparente por lo que se ingresa a la página de la UNAD, constatando que lo estamos haciendo desde nuestro Ubuntu Desktop.



Figura 14. Navegación internet con proxy no transparente.

Una forma de comprobar el funcionamiento del proxy no transparente, es a través de las Reglas de Acceso que se configuran en el HTTP Proxy, en esta parte se puede permitir o denegar el acceso a internet, de igual forma se puede indicar los días y el horario. En este caso denegaremos el acceso a internet.



Figura 15. Reglas de acceso HTTP Proxy.

Desde la maquina de Ubuntu Desktop se accede nuevamente a la página de la UNAD, se observa que el navegador indica que el servidor proxy está rechazando las conexiones.

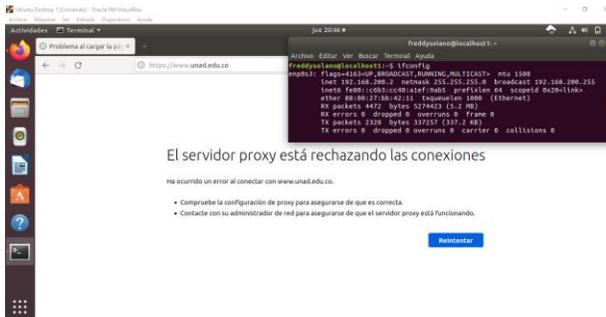


Figura 16. Rechazo de conexión a internet.

4 TEMATICA 4. FILE SERVER Y PRINTER SERVER

Esta temática indica la instalación y configuración de un file server y print server en Zentyal 6.2, entendiéndose como file server un servidor centralizado dentro de una red desde donde se permite a los clientes (equipos conectados en la red) conectarse a este servidor para acceder a carpetas y archivos, el print server al igual que el file server es un servidor centralizado desde el cual se puede acceder a las impresoras compartidas en red con el fin que cualquier equipo pueda acceder e imprimir desde ellas.

Para iniciar con la implementación del file server se instalan los módulos DNS, NTP y controlador de dominio y compartición de ficheros.

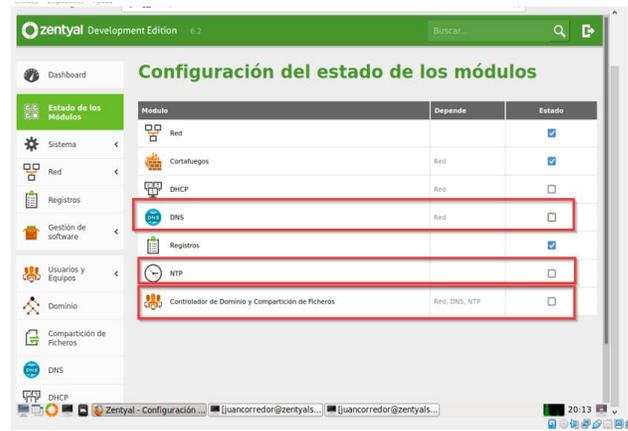


Figura 17. Instalación de módulos DNS, NTP y red.

Una vez instalados los módulos se iniciará con la configuración NTP para ello, se dirige a la opción Sistema > Fecha/hora se selecciona la opción Activar sincronización con servidores NTP externos una vez habilitada la opción se presiona cambiar.

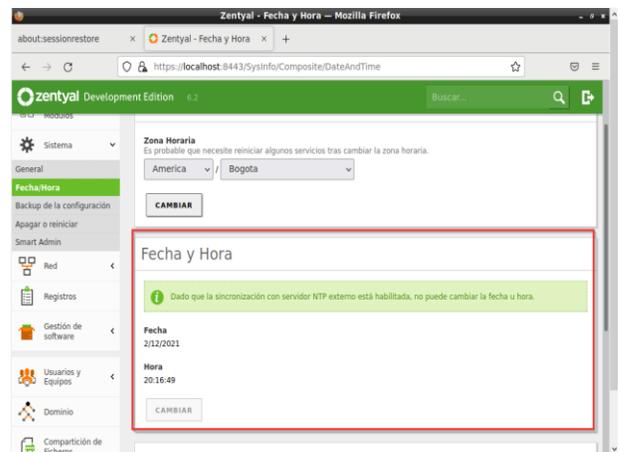


Figura 18. Confirmación ejecución servicio NTP.

Una vez configurada el servicio NTP, se procede a configurar el DNS, para ello se dirige a la opción DNS.

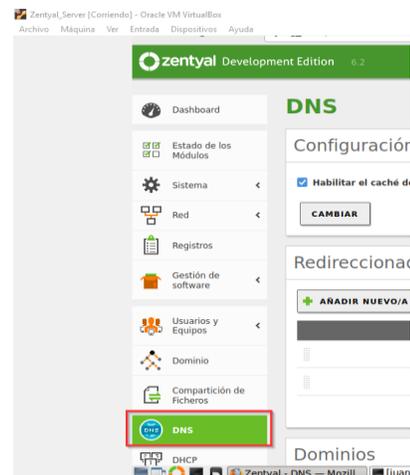


Figura 19. Opción DNS.

Se iniciará habilitando la opción Habilitar el cache de DNS transparente, paso seguido se añaden los DNS de google (8.8.8.8) y un DNS gratuito (1.1.1.1), esto presionando añadir nuevo.



Figura 20. Asignación de DNS públicos

Configurado en DNS y NTP se procede con la modificación del Dominio, dentro de las opciones se selecciona para la opción función de servidor-controlador de dominio, Nombre del dominio NetBIOS se deja con el que tiene asignado por defecto, se habilita la opción de perfiles móviles con el fin de poder ingresar al dominio equipos móviles y finalmente se selecciona una letra de unidad en este caso R:



Figura 21. Configuración de dominio.

Paso seguido se ingresa el equipo desktop al dominio, en el servidor de Zentyal en el apartado de dominio se observará el equipo desktop reportado.

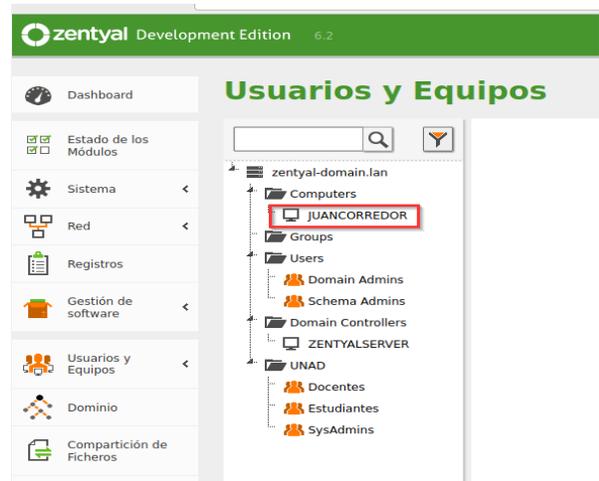


Figura 22. Reporte de equipo desktop en el dominio.

Configurado el dominio se procede a crear los usuarios que se utilizaran en el file server, para ello en la opción usuarios y equipo > gestionar se crean 3 grupos docentes, estudiantes y Sysadmin.

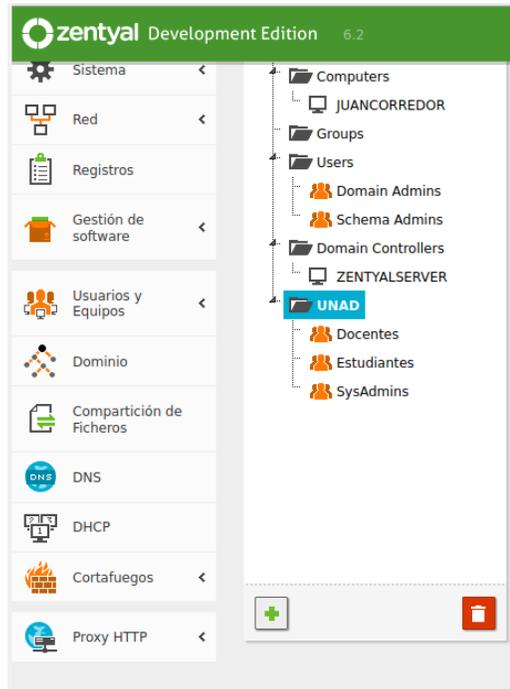


Figura 23. Creación de grupos en el dominio.

En el grupo estudiantes se crea el usuario 1023026017.

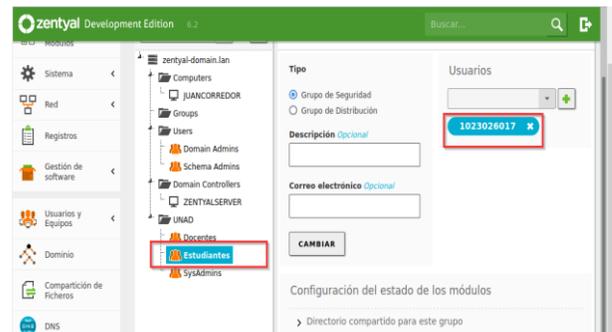


Figura 24. Creación de usuario 1023026017

En el grupo Sysadmin se crea el usuario soporte.



Figura 25. Creación de usuario de soporte

Paso seguido se procede a configurar el file server, para ello se ingresa a la opción compartición de ficheros en él se crea un directorio compartido llamado DiplomadoUNAD presionando el botón añadir nuevo.



Figura 26. Creación de directorios

Se habilita el recurso compartido, en ruta del recurso compartido se selecciona Directorio bajo Zentyal > nombre del directorio en este caso DiplomadoUNAD, el directorio bajo Zentyal se crea automáticamente el directorio compartido Share.directory en /home/samba/shares, se deja deshabilitado el acceso de invitado para que solicite credenciales al acceder a los directorios compartidos.



Figura 27. Configuración de directorio.

Se procede a crear dos ficheros adicionales trabajo final y juan corredor, el segundo será un directorio exclusivo para el usuario 1023026017.



Figura 28. Creación de directorios extras

Se asignarán los permisos a los directorios presionando el engrane en la columna control de acceso sobre el directorio al cual se asignarán permisos, Se presiona en la opción Añadir nuevo; Para este caso se seleccionará el directorio JuanCorredor, en usuario/grupo se selecciona la opción usuario y se selecciona el colaborador que tendrá permisos en este directorio en este caso 1023026017, se selecciona los permisos de lectura y escritura.



Figura 29. Asignación de permisos directorio Juancorredor

Para probar los permisos por grupo se asignarán los permisos al grupo Domain Admins, con permisos de administrador sobre el directorio Diplomado UNAD.



Figura 30. Asignación permisos directorio DiplomadoUNAD

Una vez finalizado la asignación de permisos se ingresa al equipo desktop, en el explorador de archivos se ingresará al file server presionando la opción otras ubicaciones en conectar al servidor se ingresa el dominio del servidor Zentyal anteponiendo el prefijo smb:// esto debido a que se ingresará por el servicio samba.

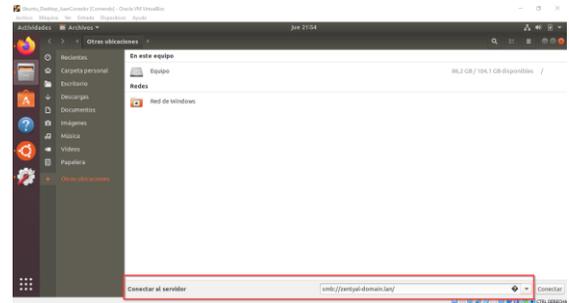


Figura 31. Acceso al file server por servicio samba

Al intentar conectarse con el usuario soporte al directorio JuanCorredor este impedirá el acceso.



Figura 32. Validación de permisos de acceso directorio JuanCorredor



Figura 33. Denegación de acceso al directorio Juancorredor con usuario Soporte

Si se intenta ingresar al directorio DiplomadoUnad el cual tiene permisos del grupo Domain Admins donde se encuentra el usuario **soporte** agregado.



Figura 34. Usuarios del grupo Domain Admins

Podrá ingresar sin problema.

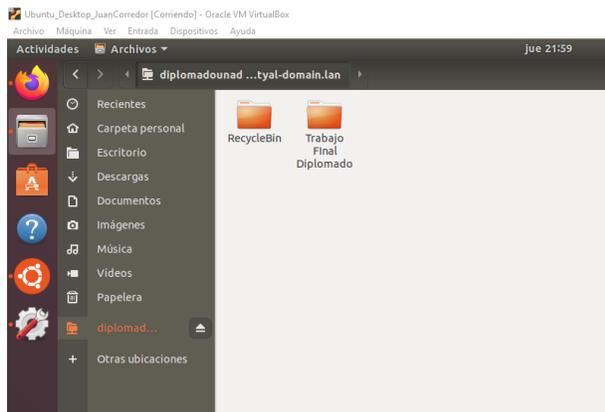


Figura 35. Acceso directorio diplomadounad

Al tener permisos de administrador se podrá eliminar, guardar y crear documentos en este directorio sin problema.

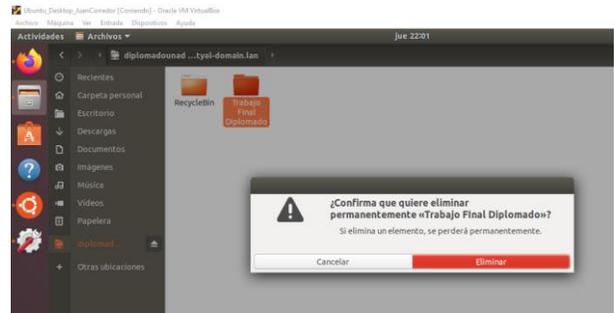


Figura 36. Eliminación de carpeta directorio diplomadounad

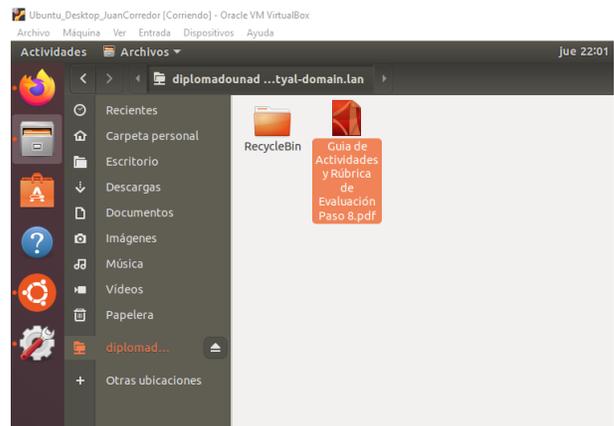


Figura 37. Carga de archivo directorio diplomadounad

Si se retira los permisos de administrador y se reemplaza por solo lectura no podrá eliminar ni editar los archivos que se encuentran en el directorio.



Figura 38. Error al eliminar "Permisos denegados"



Figura 39. Acceso directorio juancorredor con usuario 1023026017



Figura 40. Creación de carpeta en directorio juancorredor

Para la configuración del print server se utilizará el servicio de CUPS esto debido a que la versión de Zentyal 6.2 el cual se está utilizando en este paso no soporta el servicio de impresoras desde la versión 5 y superior.

El servicio CUPS se instalará en el servidor donde se tiene ya instalado y configurado Zentyal, este servicio permite la integración con samba.

Se inicia con la instalación del servicio CUPS por medio del comando sudo apt-get install cups.

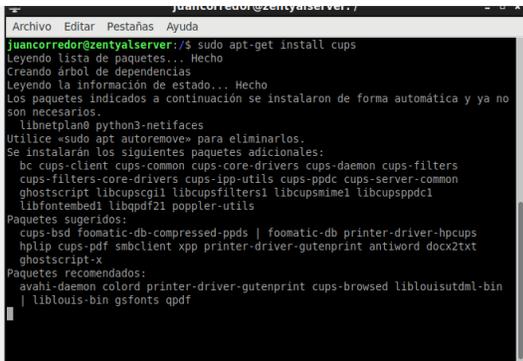


Figura 41. Instalación CUPS

Una vez instalado CUPS se procede a modificar el archivo de cupsd.conf agregando dos Listen uno con la ip de la interfaz LAN y el otro con el nombre del servidor agregando el puerto 631, esto con el fin de que sea visible por el segmento de red de la LAN.

Esta modificación se realiza por medio del comando nano /etc/cups/cupsd.conf.

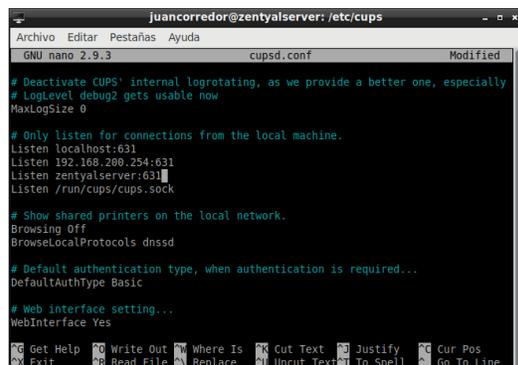


Figura 42. Modificación archivo cupsd.conf

Paso seguido se modifica el archivo smb.conf agregando las líneas:

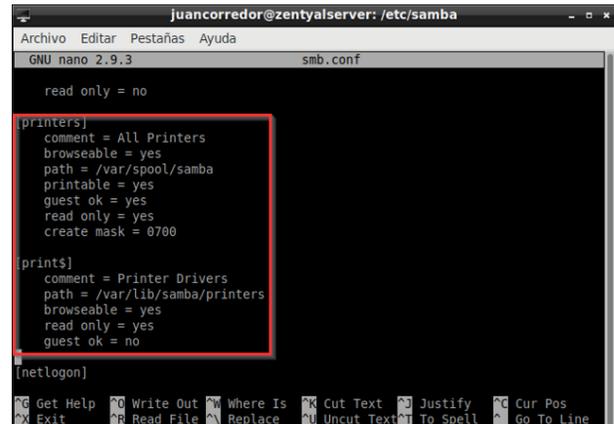


Figura 43. Adición de líneas archivo smb.conf

Como ya se mencionó Zentyal no tiene el servicio para gestionar impresora, pero es necesario el servicio de samba que lo posee Zentyal para terminar de compartir

Una vez modificado el archivo, se procede a realizar el reinicio del servicio CUPS y samba

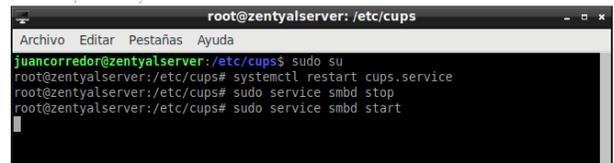


Figura 44. Reinicio servicio samba y cups

Finalizado el reinicio se ingresa por la url <https://192.168.200.254:631> a la consola de administración.

Paso seguido se procede a crear una impresora, por medio de la opción administración, añadir impresora.

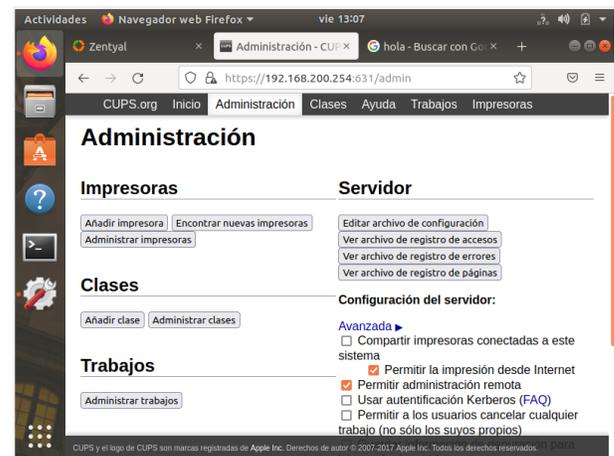


Figura 45. Opción de administración para añadir impresora

Paso seguido se procede a seleccionar el método de conexión de la impresora, se define el nombre, la descripción, localización y se selecciona la opción compartir esta impresora.



Figura 46. Información de la impresora



Figura 47. Lista de impresoras

Paso seguido en el servidor Desktop se agrega la impresora, esto ingresando a configuración impresoras y presionando añadir una impresora.

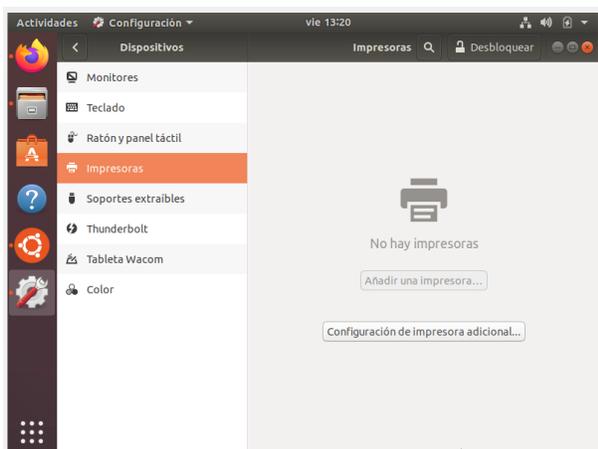


Figura 48. Ingreso de impresora en el equipo desktop

En la ventana seleccione dispositivo en el apartado impresora de red ingresamos en el campo URI del dispositivo `ipp://servidor cups/impresora/cola impresión`, en este caso se ingresa los datos del servidor en el cual se instaló el servicio.

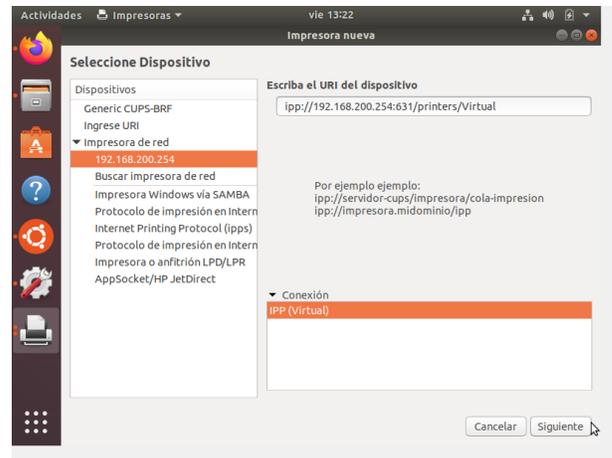


Figura 49. Selección de la impresora de red

Se presiona aplicar y la impresora se podrá observar en el apartado de impresoras.

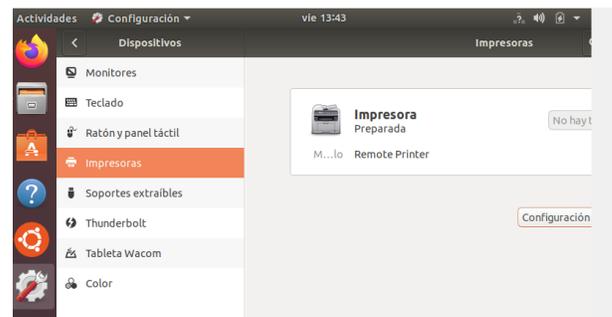


Figura 50. Impresora configurada

5 TEMATICA 5. VPN.

El desarrollo de esta temática consiste en mostrar la implementación y configuración de Zentyal server como proveedor del Servicio de redes privadas virtuales (VPN) con OpenVPN. Mediante una conexión VPN el cliente puede acceder a los servicios de la red interna en donde Zentyal trabaja como puerta de enlace y como servidor VPN teniendo detrás una o varias redes locales (LAN).

Al implementar un servidor VPN con Zentyal, se obtienen ventajas como autenticación mediante infraestructura de clave pública, cifrado basado en tecnología SSL, cliente VPN para diferentes sistemas operativos (Windows, Mac OS y Linux), sumando a la fácil instalación, configuración y administración.

Para configurar Zentyal como servidor VPN, se debe instalar el módulo VPN, esto se realiza de la siguiente forma.

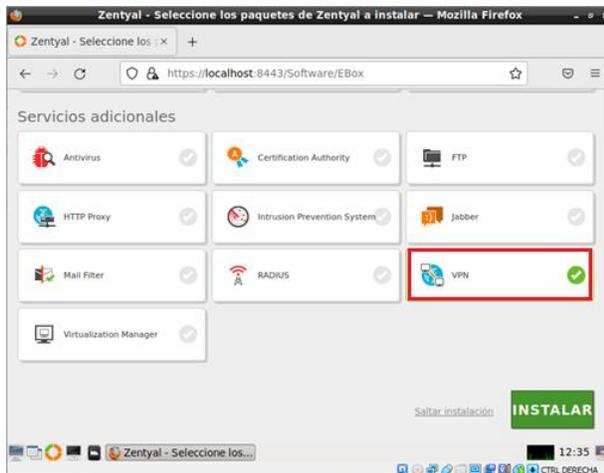


Figura 51. Módulo VPN Zentyal.

En el panel de administración de Zentyal, como se observa en la Fig. al seleccionar e instalar el módulo VPN, el asistente informara que módulos adicionales pueden deben ser habilitados para el correcto funcionamiento.

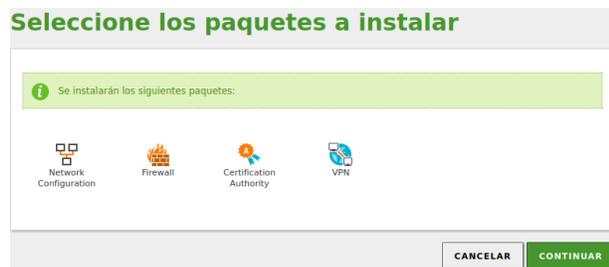


Figura 52. Instalación de paquetetes módulo VPN.

Para el caso del módulo VPN, es necesario instalar los módulos adicionales Network Configuration, Firewall y Certification Authority.

Terminada la instalación de paquetes, el asistente de instalación solicita sean configurados los tipos de interfaces de red, para esto se debe seleccionar cual o cuales son externas y cuales internas. Teniendo en cuenta que tenemos tres (3) interfaces de red, la eth0 será externa (External) ya que es la interfaz que tendrá la salida a Internet WAN, eth1 será interna (Internal) ya que de esta depende la red LAN interna y por último la eth2 será interna (Internal) ya que está dispuesta para la Zona DMZ.



Figura 53. Tipo de interfaces.

Seleccionado el tipo, se debe configurar el direccionamiento Ip para cada una de las interfaces, el cual depende la infraestructura de red definida y los servicios implementados, para este caso utilizaremos direccionamiento estático.

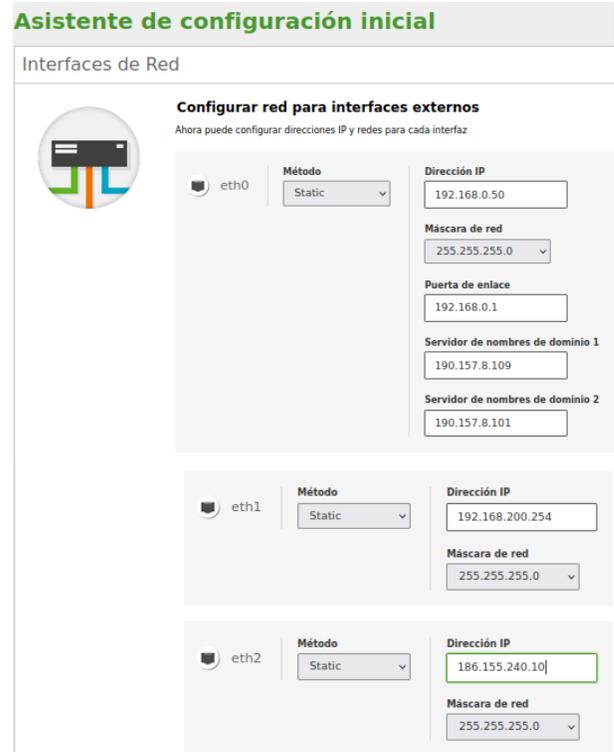


Figura 54. Configuración de red externa e interna

Una vez realizada la configuración de red, se procede con la configuración de Zentyal como servidor de redes privadas virtuales (VPN) con OpenVPN. Realizar la configuración para que un cliente externo pueda realizar conexión por VPN y acceder a los servicios de red local interna.

Como primer paso, es necesario crear un nuevo servidor VPN, en el panel de administración de Zentyal, menú VPN, opción Servidores.

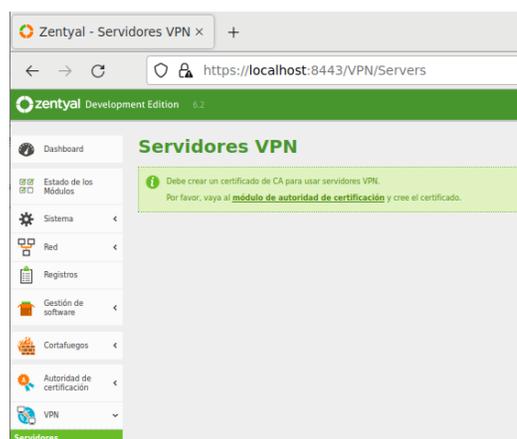


Figura 55. Servidores VPN

Como se observa en la imagen anterior, el asistente informa que debe crearse un certificado para usar Servidores VPN, por lo cual debe ir al módulo Autoridad de certificación. Para lo cual puede ir directamente al módulo o hacer clic en el enlace.

Al ingresar al módulo Autoridad de certificación, debe generar el correspondiente certificado ingresando los datos como nombre, código de país, ciudad, estado y días para expirar. Como aparece en la siguiente imagen.

Figura 56. Creación certificado Servidor VPN

Una vez creado el certificado, se puede consultar en la sección lista de certificados actual.

Nombre	Estado	Fecha	Acciones
VNPZentyal Authority Certificate desde VNPZentyal	Válido	2022-12-03 22:09:39	[Revocar] [Descargar] [Renovar]

Figura 57. Lista de certificados del Sistema

Para continuar, debe ir nuevamente al menú VPN opción Servidores, en donde ya puede crear un nuevo Servidor VPN, haciendo clic en el botón Añadir Nuevo/a.

Figura 58. Añadir Servidor VPN

El nombre del servidor puede ser cambiar, según la identificación que se le quiera dar. El nombre dado para este es: VPNZentyalDPL. Clic en el botón Añadir para continuar.

Figura 59. Nuevo Servidor VPN

Creado el servidor VPN, se debe configurar. Esto se hace seleccionando el icono en forma de piñón en la columna configuración de la lista de servidores.

Habilitado	Nombre	Configuración	Redes anunciadas	Descargar paquete de configuración de cliente	Acción
<input checked="" type="checkbox"/>	VPNZentyalDPL	[Gear Icon]	[Gear Icon]	[Gear Icon]	[Stop] [Edit]

Figura 60. Servidores VPN

Durante el proceso de configuración del servidor VPN, se deben para establecer y validar los siguientes datos:

Puerto del servidor: UDP 1194 (puerto utilizado para las conexiones VPN)

Dirección VPN: Es la subred virtual donde se situará el servidor VPN y los clientes. Por defecto está determinada la Ip 192.168.160.1/24, a los clientes les será asignada una Ip de mismo segmento en orden de conexión 2, 3, ... Este segmento de red puede cambiarse.

Certificado de servidor: (vpn-VPNZentyalDPL) Certificado que mostrará el servidor a sus clientes, Zentyal expide un certificado por defecto para el servidor.

Autorizar al cliente por su nombre común: (*Deshabilitado*) Requiere que el common name del certificado del cliente empiece por la cadena de caracteres seleccionada para autorizar la conexión.

Interfaz TUN: (*Habilitado*) Por defecto es TAP y en estado *deshabilitado* siendo un bridge de capa 2, pero lo mejor es que se encuentre *habilitado* ya que TUN es más semejante a un nodo de IP capa 3, compatible con del cliente VPN OpenVPN Connect v3 que se va a utilizar más adelante.

Traducción de dirección de red (NAT): (*Habilitado*) recomendable tener esta traducción activada si el servidor Zentyal que acepta las conexiones VPN, de tal forma que los clientes de estas redes internas

respondan al Zentyal de VPN en lugar de a su puerta de enlace.

Interfaz en la que escuchar: *(Todas las interfaces de red)* Permite escuchar al servidor por todas las interfaces de red.

Redirigir puerta de enlace: *(Deshabilitado)* Esto hace que Zentyal sea el proveedor de internet para las redes internas.

Durante este proceso de configuración también puede:

Permitir que los clientes VPN se comuniquen entre si *habilitando* la opción Permitir conexiones cliente – cliente. Se pueden realizar conexiones entre servidores Zentyal *habilitando* la opción Permitir túneles de Zentyal a Zentyal. Al igual se puede determinar configuraciones puntuales para servidores DNS, servidor de dominio y servidor WINS.

El servidor VPN creado, debe tener la siguiente configuración:

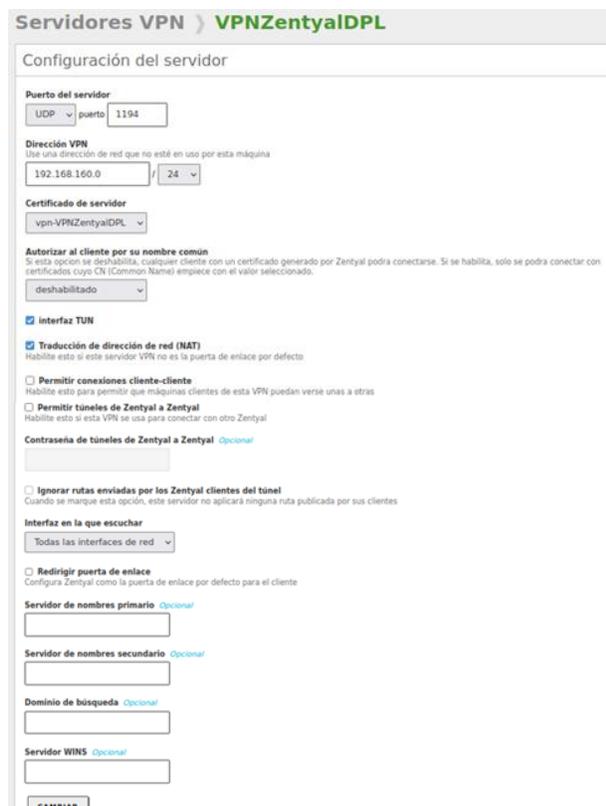


Figura 61. Configuración Servidor VPN

Los demás parámetros que no se configuren se deben dejar en estado por defecto. Clic en Cambiar para aplicar los cambios. Luego clic en GUARDAR CAMBIOS.

Configurado el servidor, se deben validar cuales son las redes anunciadas.



Figura 62. Listado de redes anunciadas

Como se observa en la imagen anterior la red LAN y la Zona DMZ, podrán acceder por los clientes que se conecten a través de VPN.

Acto seguido podrá generar y descargar el paquete de configuración para el cliente VPN, para lo cual debe ir al icono del engrane de la columna Descargar paquete de configuración de cliente, de la lista de servidores.

Como se observa en la siguiente imagen, al ingresar a generar el paquete de configuración VPN el asistente informa que debe crearse un certificado para Cliente VPN. Por lo cual debe ir al módulo Autoridad de certificación o hacer clic en el enlace.



Figura 63. Paquete de configuración VPN

Para crear el certificado de Cliente VPN, debe ingresar el nombre con el cual lo va a identificar y los días para expirar.



Figura 64. Nuevo certificado Cliente VPN

Expedido el certificado, se puede confirmar su creación en la lista de certificados actual.



Figura 65. Lista del certificados del Sistema

Para continuar debe volver a la opción Descargar paquete de configuración de cliente, de la lista de servidores VPN. Una vez allí, debe:

Seleccionar el Tipo de cliente esto depende del sistema operativo base, ingresar la Dirección del servidor, para este caso es la misma Ip de la interfaz

WAN: 192.168.0.50 (IP pública asignada al servidor Zentyal). Los demás parámetros pueden ser dejados en estado por defecto o cambiarlos según la configuración que se requiera. Por último, Clic en el botón Descargar

Descargar paquete de configuración de cliente

Tipo de cliente
Windows

Certificado del cliente
VPNZentyalDPL

Añadir instalador de OpenVPN al paquete de configuración del cliente
Instalador de OpenVPN para Microsoft Windows

Estrategia de conexión
Aleatorio

Dirección del servidor
Esta es la dirección que usarán sus clientes para conectarse al servidor. Normalmente, ésta será una IP pública o un nombre de host
192.168.0.50

Dirección adicional del servidor (opcional) Opcional

Figura 66. Generación paquete de configuración VPN

El paquete será descargado en archivo comprimido, por lo cual es necesario pasarlo al equipo cliente y descomprimirlo.

A su vez para el caso de sistemas operativos Windows, debe descargar e instalar la aplicación OpenVPN Connect v3 de la página web <https://openvpn.net/client-connect-vpn-for-windows/>



Figura 67. Descarga cliente OpenVPN Connect v3

Instalado el cliente OpenVPN Connect v3, debe abrirlo, e ir a la opción archivo (File) y cargar el archivo de configuración VPN generado en Zentyal.

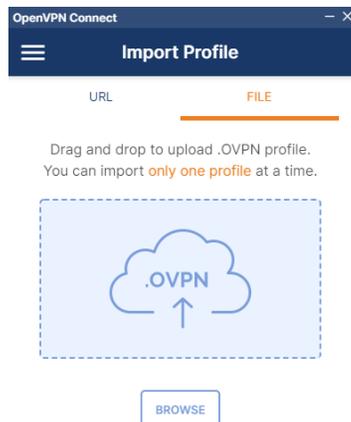


Figura 68. Carga archivo configuración VPN

Importando el archivo de configuración VPN, ya puede hacer conexión. Clic en el botón **Connect**.

Si todo a sido configurado correctamente, la conexión será establecida sin problema, como se muestra a continuación.

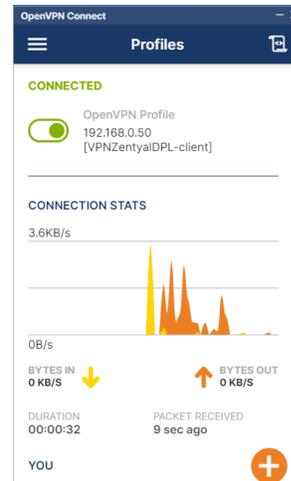


Figura 69. Conexión VPN exitosa.

Establecida la conexión VPN, puede acceder a los servicios de la red interna sea a un equipo de la LAN o de la Zona DMZ. Como por ejemplo a página de bienvenida el servidor Apache instalado y corriendo como servicio en Ubuntu Server 18.04. situado en la Zona DMZ.

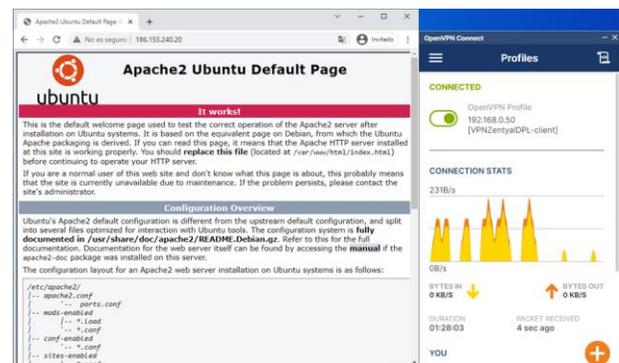


Figura 70. Acceso a servicios de red.

6 CONCLUSIONES

En el proceso de aprendizaje como futuros profesionales, no debemos dejar todo por sentado ya que podemos evidenciar que existen muchas herramientas útiles como lo es Zentyal Server 6.2 que pueden dar soluciones a requerimientos específicos dentro de una infraestructura TI como lo es la implementación de un servicio de Proxy no Transparente en la cual como administradores podemos tener control de la navegación de internet a través de la implementación de diversas reglas.

Zentyal Server 6.2 cuenta con el componente para la implementación del dominio y el file server, este nos permite y facilita la asignación de permisos en los directorios compartidos debido a que se pueden realizar ya sea por usuario o grupo; dentro de las opciones se encuentran permisos de lectura, escritura y administración este último concede los permisos máximos sobre los directorios; A partir de la versión superior a la 5 no se puede utilizar el Print Server sin embargo por medio del servicio CPUS que se complementa con samba.

Al implementar y configurar Zentyal Server 6.2 como servidor VPN, hemos evidenciado las capacidades de este como prestador de servicios de infraestructura IT, siendo una herramienta robusta que se ajusta a las necesidades y requerimientos de una problemática a nivel corporativo, permitiendo de esta forma crear un túnel privado desde una estación de trabajo con Open VPN a la red interna de una corporación de una forma segura.

7 REFERENCIAS

- [1] Zentyal S.L. (2019). Primeros pasos con Zentyal. <https://doc.zentyal.org/es/firststeps.html>
- [2] Zentyal S.L. (2004 - 2018). Zentyal 6.2 Documentación Oficial. <https://doc.zentyal.org/6.2/es/>
- [3] Zentyal.org. (2019). Servicio de Proxy HTTP. <https://doc.zentyal.org/6.2/es/proxy.html>
- [4] CUPS.org. Help. Recuperado 3 Dic 2021, from <http://www.cups.org/documentation.html>
- [5] Zentyal S.L. (2004-2018). Servicio de redes privadas virtuales (VPN) con OpenVPN. [https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_\(VPN\)_con_OpenVPN](https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_(VPN)_con_OpenVPN)
- [6] TV, P. (2020). Cómo instalar y configurar un servidor VPN en Zentyal - Tutorial 2020. <https://www.youtube.com/watch?v=8zaxU1C7qBc>