

INFORME – SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

TRABAJO FINAL – PASO 8

GRUPO 201494_13

Rafael Steven Soto
 e-mail: rssotod@unadvirtual.edu.co
 Jhonny Zambrano Zuñiga
 e-mail: jzambranoz@unadvirtual.edu.co
 David Sandoval
 e-mail: dsandovalca@unadvirtual.edu.co
 Christian Adrián Orozco Espinosa
 e-mail: caorozcoe@unadvirtual.edu.co
 Carlos Edinson Ospina
 e-mail: ceospinam@unadvirtual.edu.co

RESUMEN: *Iniciamos la actividad final del paso 8 con 5 temáticas planteadas para la solución de necesidades específicas con la plataforma GNU/Linux utilizando Zentyal 5.1 como sistema operativo base y que tiene a disposición varios servicios de Infraestructura TI que pueden ser aplicados en para garantizar el control y administración de una red (Intranet / Extranet) por equipos con distribución Linux, en este caso nuestro cliente se basa en Debian 10. En este documento vamos a visualizar algunos de los servicios ofrecidos por Zentyal, tales como DHCP, DNS, Controlador de Dominio, Proxy no transparente, Cortafuegos, file server, print server y VPN. Haciendo uso del software de virtualización, VirtualBox y junto a Debian para poner en práctica los diferentes servicios mencionados.*

PALABRAS CLAVE: Acceso remoto, controlador de dominio, cortafuegos, servicios de red.

1 INTRODUCCIÓN

Día a día la información crece y con su nivel de seguridad, ya que cuanta más información sobre una persona hay, mejor es la forma de diagnosticar sus necesidades, aprender más sobre un lugar e incluso las estrategias comerciales de una empresa.

Debido a esto, se han identificado soluciones tecnológicas para la correcta administración de información y, con ello, la seguridad informática bajo una serie de servicios que se proporcionan a los usuarios, estas soluciones se basan principalmente en las necesidades de una empresa que, por la necesidad de sus servicios, adquieren una computadora de tipo servidor, que en este caso busca implementar servicios de red específicos.

2 DESARROLLO DE CONTENIDOS

A partir de esta sección, Nuestro grupo tiene la finalidad de detallar técnicamente las 5 temáticas mostrando su respectivo desarrollo y solución. Se Detallan las temáticas con su respectivo enlace.

Temáticas	
Rafael Steven Soto	Temática 5: VPN.
Jhonny Zambrano Zuñiga	Temática 3: Cortafuegos.
David Sandoval	Proxy no transparente.
Christian Adrián Orozco	Temática 1: DHCP Server, DNS Server y Controlador de Dominio.
Carlos Edinson Ospina	Temática 4: File Server y Print Server.

Tabla 1. Temáticas seleccionadas por estudiante.

Enlaces	
Rafael Steven Soto	https://drive.google.com/drive/folders/1JnOWZCX8hMF3Vr1X7HY3C8Uzoww2_8i5?usp=sharing
Jhonny Zambrano Zuñiga	https://drive.google.com/drive/folders/1FdSW_RKMXPapYyZR0QR-n-qx8jNU6NKq?usp=sharing
David Sandoval	https://drive.google.com/file/d/1btKSp1mL_TtOG2PoIOu4fcsnim4D0bAPd/view?usp=sharing
Christian Adrián Orozco	https://drive.google.com/drive/folders/1-UJPObj288dU9verk04CgOenZSOofLH?usp=sharing
Carlos Edinson Ospina	https://drive.google.com/file/d/1CLzu-Z2xTLPm0WAF9hDrhs99InnZ_GU/view

Tabla 2 Enlaces del trabajo individual.

3 INSTALACION ZENTYAL SERVER 5.1

Zentyal server es una distribución GNU/Linux basada en Ubuntu, la cual permite la administración de diversos servicios de forma gráfica y de fácil uso.

3.1 DESCARGA E INSTALACIÓN DE ZENTYAL SERVER 5.1

Para iniciar el proceso de descarga ingresamos a la url de descargar <http://download.zentyal.com/>, seguido a esto procedemos a la instalación de la iso en VirtualBox.



Figura 1. Instalación Zentyal 5.1.

Continuamos con el proceso asignando el lenguaje, ubicación, configuración del teclado, nombre de la máquina, usuario y zona horaria.

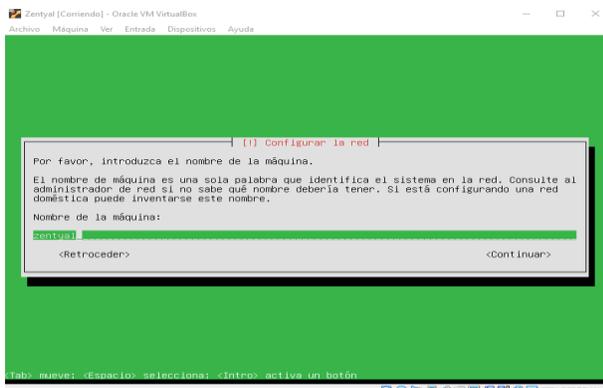


Figura 2. Asigna nombre maquina Zentyal server 5.1.

Luego de terminada la instalación realiza el reinicio y observamos la interfaz gráfica para el ingreso a Zentyal.



Figura 3. Interfaz de ingreso Zentyal server 5.1.

3.2 CONFIGURACIÓN INICIAL ZENTYAL.

Se realiza el ingreso con el usuario y contraseña creados, observamos la configuración inicial.



Figura 4. Inicio configuración Zentyal server 5.1.

Procedemos a seleccionar los paquetes necesarios para continuar con el proceso de descarga.

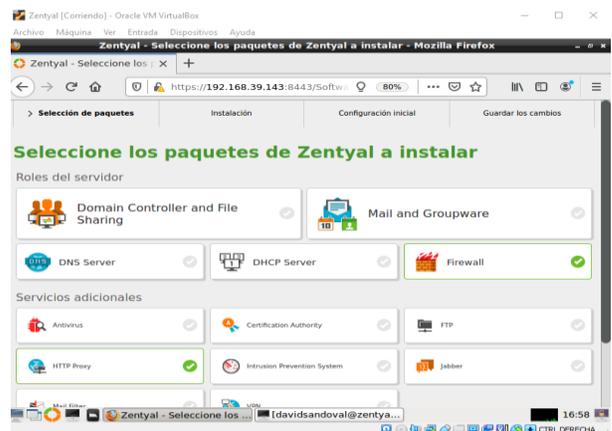


Figura 5. Selección de paquetes a instalar.

Continuamos con la configuración de las interfaces que tenemos activas para la máquina virtual, cabe recordar que también se pueden modificar en cualquier momento.



Figura 6. Configuración de las interfaces.

Luego de realizar la descarga de paquetes y configurar las interfaces culmina el proceso de instalación.

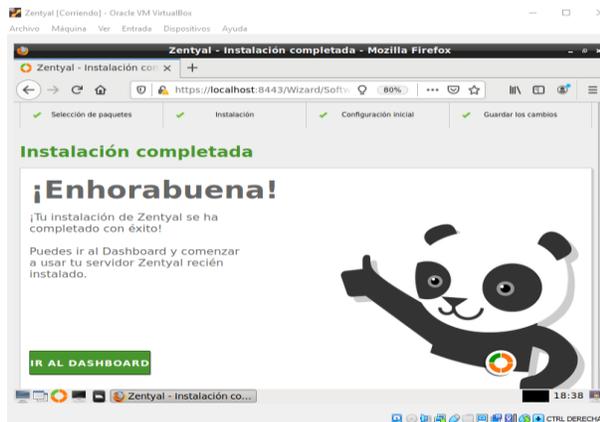


Figura 7. Culmina el proceso de instalación Zentyal Server 5.1.

4 ACTIVIDADES PARA DESARROLLAR

4.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Toda infraestructura de tecnología a nivel de TI debe tener implementados 3 servicios que son fundamentales para la comunicación y la gestión de los recursos informáticos de una compañía, estos servicios son: DHCP, DNS y el servicio de controlador de dominio.

Para lo anterior, se evidenciará la implementación de estos servicios, haciendo uso de las bondades provistas por software libre y con la ayuda de las funcionalidades provistas por la distribución Zentyal.

Controlador de dominio:

Implementada la distribución de Zentyal se desplegará el juego de servicios disponibles para implementación, para ello seleccionamos: Domain

Controller and File Sharing, DNS Server y DHCP Server, tal como se observa en la imagen siguiente:

Cabe resaltar que las imágenes incluidas en esta temática contienen unas flechas en color rojo, que permiten indicar las opciones más relevantes para tener en cuenta.



Figura 8. Panel de servicios disponibles Zentyal.

Al llevar a cabo la implementación de los servicios es importante definir dentro del asistente de configuración, el uso de los dos adaptadores definidos para la máquina virtual de Zentyal, tal como se evidencia en la imagen que se muestra a continuación:



Figura 9. Configuración adaptadores requeridos.

Lo primero a implementar es el controlador de dominio para ello el asistente te informará que tipo de servidor planea implementar “para este caso un servidor Stand-alone” y se debe definir además el nombre que tendrá el dominio, como se observa a continuación:



Figura 10. Definición nombre del dominio.

Definido lo anterior el árbol LDAP se desplegará mostrando los objetos predeterminados propios del dominio, como se puede apreciar en la imagen:

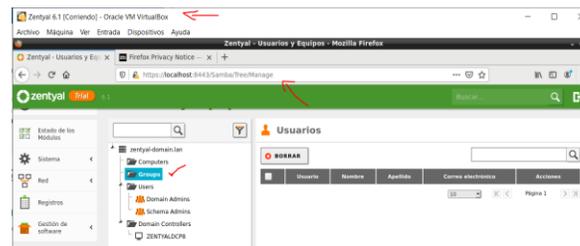


Figura 11. Árbol LDAP Zentyal.

Los usuarios y grupos de dominio se crean con base en las opciones que provee la consola a nivel web, al igual forma que los contenedores, demostrando lo intuitiva que es la herramienta a nivel gráfico.

Servidor de DNS:

El servidor de DNS se autoconfigura y asume la IP estática definida para el manejo de la red interna, por lo cual para efectos de laboratorio puede dejar la configuración predeterminada, como se observa en la imagen siguiente:

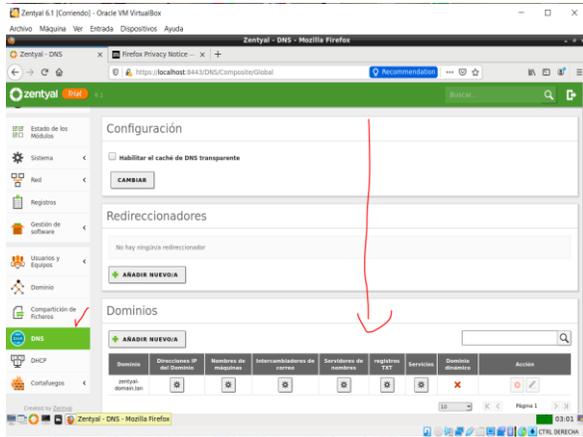


Figura 12. Configuración predeterminada DNS.

Servidor DHCP:

Este servicio es de amplia difusión en las compañías y representa una manera simplificada para la asignación de dirección IP y configuración de red, dentro de la consola web en Zentyal accedemos al módulo respectivo y definimos un ámbito, el cual operará sobre el cliente cuyo adaptador de red deberá estar en modo “Red interna – LAN” dentro de la configuración de la máquina virtual. En cuanto el ámbito su definición sería la siguiente en función de que el cliente adopta la puerta de enlace y el DNS como la dirección IP asignada al servidor de Zentyal.

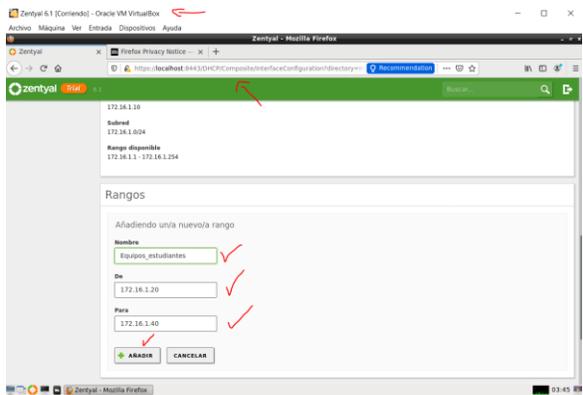


Figura 13. Configuración ámbito direcciones DHCP.

En esta imagen se puede observar como el cliente asume la IP de forma dinámica:



Figura 14. Asignación IP y configuración red cliente Debian.

Conexión cliente dominio:

Existen diferentes alternativas para unir o conectar un cliente al dominio, la más efectiva es emplear PBIS (PoweBroker Identity Services), una vez instalado este paquete bastará con digitar esta instrucción “en función del nombre del dominio que esté definido claro está” y el cliente se unirá al dominio:

```
domainjoin-cli join --disable ssh zentyal-domain.lan administrator@ zentyal-domain.lan <enter>.
```

El proceso se puede observar con claridad en la siguientes dos imagenes:

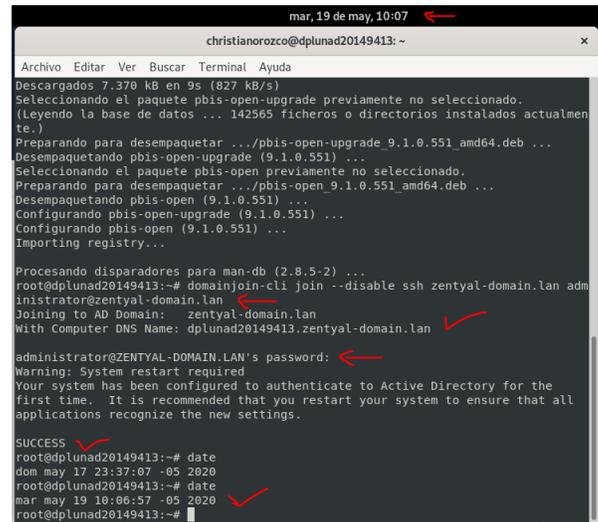


Figura 15. Unión cliente Debian a Dominio Zentyal.

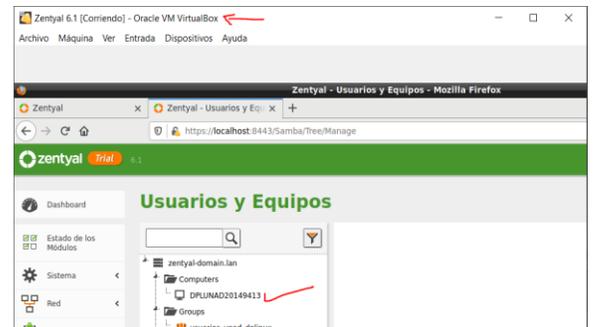


Figura 16. Registro equipo en el dominio.

El inicio de sesión con una cuenta de dominio es simple, solo se emplea el comando “su” y el usuario de dominio con su respectiva contraseña a través de consola en el cliente Debian (las primeras líneas son instrucciones para asignar: home, Shell y el sufijo de dominio, ya que el prompt aparece de manera burda):

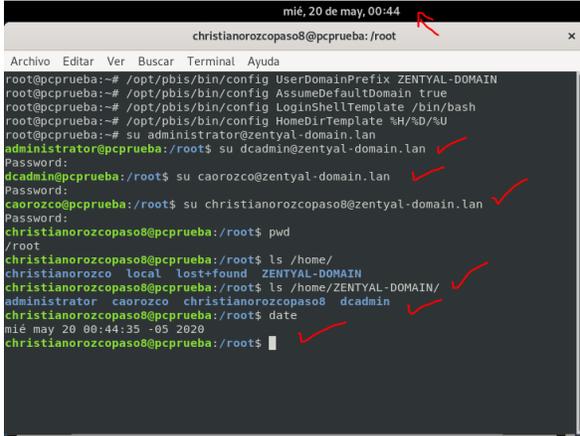


Figura 17. Registro equipo en el dominio.

4.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Se requiere Implementar y configurar de forma detallada el control del acceso de una estación GNU/Linux Debian 10 a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 830.

Para iniciar el proceso debemos configurar la máquina virtual con los adaptadores de red necesarios para el correcto funcionamiento de Zentyal.

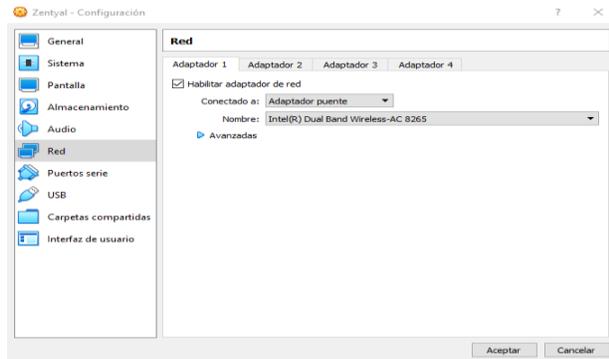


Figura 18. Adaptador de red 1.

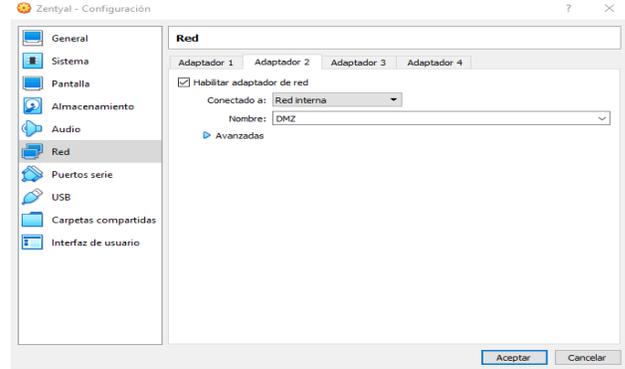


Figura 19. Adaptador de red 2.

Seguido a esto procedemos a ingresar a la configuración administrativa en la opción Red/Interfaces para configurar la interface (eth0) asignada para Zentyal con método DHCP y WAN.

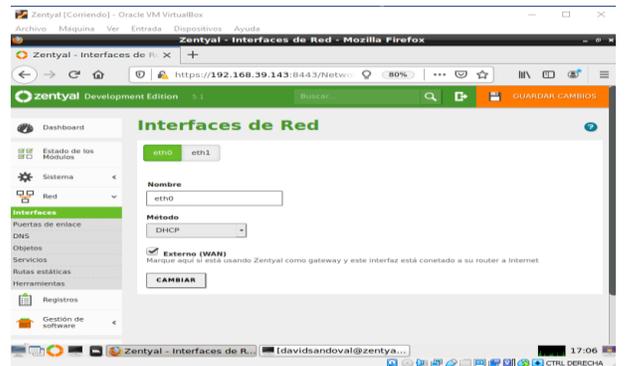


Figura 20. Configuración interface (eth0).

Continuamos con la configuración de la interface (eth1) asignando el metodo estatico y la ip 192.168.2.1 la cual sera asignada a nuestro equipo Debian como puerta de enlace para realizar las conexiones pertinentes del proxy no transparente.

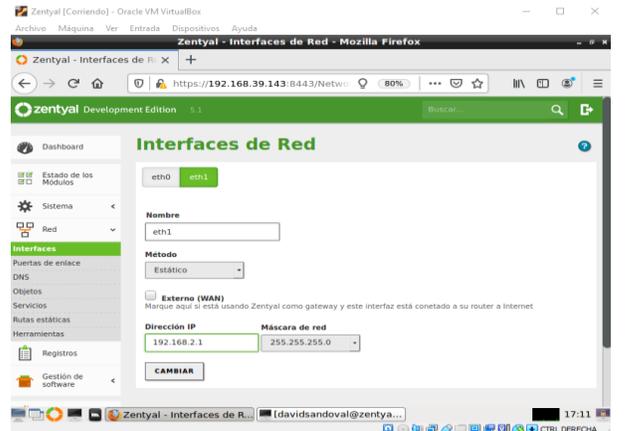


Figura 21. Configuración interface (eth1).

Ahora vamos a la opción Proxy HTTP/Perfiles de filtrado, procedemos a crear el perfil y le asignamos los parametros de configuración, en este caso bloqueamos

una pagina Http y dejamos acceso libre a la pagina Https.

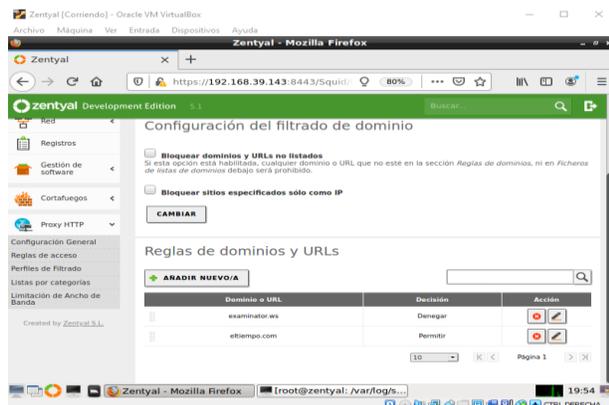


Figura 22. Configuración del perfil de filtrado.

Luego en la opción Proxy HTTP/Reglas de acceso, agregamos el perfil creado anteriormente con el periodo de tiempo y el origen donde aplicara el filtrado.

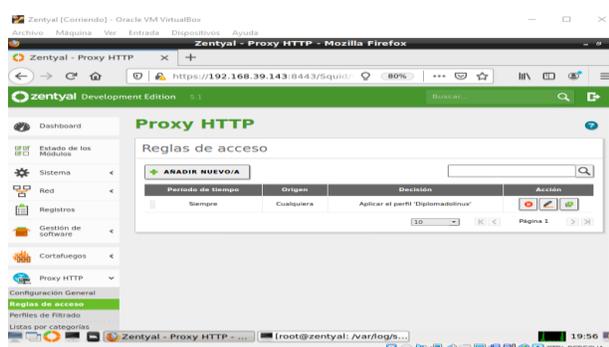


Figura 23. Configuración regla de acceso.

Ingresamos a la maquina Debian y se realiza la configuración de la puerta de enlace 192.168.2.1 y se le asigna la ip 192.168.2.17, probamos la conexión Zentiyal.

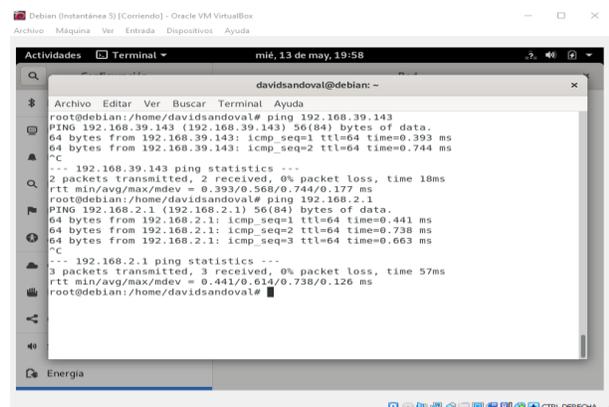


Figura 24. Conexión a Zentiyal desde Debian.

Procedemos a configurar el Proxy no transparente en Debian con la ip 192.168.2.1 y el puerto 830.

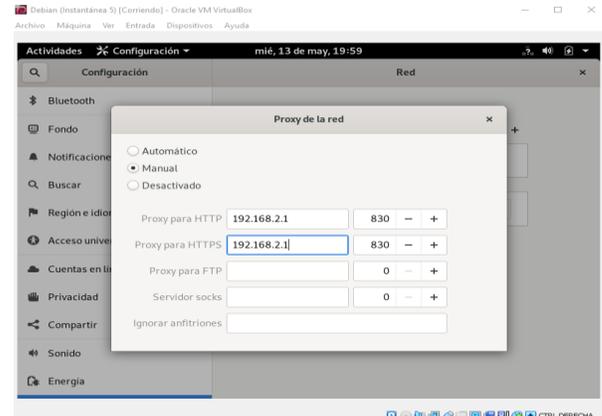


Figura 25. Configuración de Proxy en Debian.

Seguido a esto colocamos en el navegador la pagina bloqueada, evidenciando el mensaje de alerta correspondiente al bloqueo Http.



Figura 26. Verificación de acceso denegado.

4.3 TEMÁTICA 3: CORTAFUEGOS

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas.

La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Solución Planteada: Para restringir el acceso a los sitios web como redes sociales, es necesario identificar las ips que utilizan estos dominios, luego generar las reglas para que la red que está detrás del cortafuegos no pueda realizar peticiones a estas direcciones.

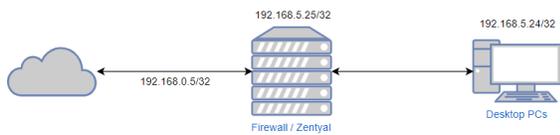


Figura 27. Diseño de red

Se instala y configura inicialmente los paquetes Server y Firewall desde la consola web de Zentyl. Adicional es necesario configurar una tarjeta de red para acceso a la red WAN (ip modo dhcp) y una para la red LAN (ip estática).



Figura 28. Configuración de redes para cada interfaz.

Para el proceso se requiere el módulo de Firewall y preferiblemente el módulo de DHCP para la asignación de Ips automáticas.

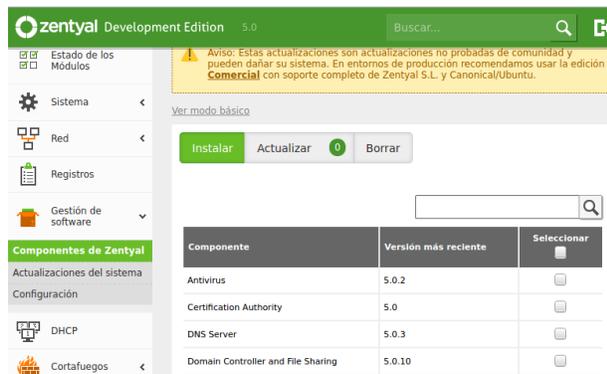


Figura 29. Instalar componentes.

Seguido vamos aplicar la configuración del módulo DHCP para la red LAN y habilitar el módulo.



Figura 30. Configuración de la red eth8.

El proceso de configuración consiste en agrupar por dirección ip del cliente y las Ips a bloquear por parte de las redes sociales, se crearán grupos y se asociarán según la necesidad, para este caso contamos con el Objeto: Lan-unad al cual se asignaron los equipos a los cuales se les desea restringir acceso a redes sociales.



Figura 31. Crear los objetos lan-unad.



Figura 32. Añadir miembros.

Creamos el Objeto redes sociales y seleccionamos la opción miembro donde vamos a registrar las ip's que queremos bloquear.



Figura 33. Crear los objetos redes sociales.



Figura 34. Añadir miembros redes sociales.

Antes de realizar la prueba del bloqueo de las ips se comprobó el acceso de la maquina (Debian 10) a internet y a las redes sociales Facebook y Wikipedia.



Figura 35. Validación de la red.

Continuamos con el siguiente paso donde vamos a configurar las reglas de acceso, donde es primordial el poder filtrar el tráfico de la red interna (Lan-unad) bloqueando el grupo de ips (Redes sociales). Para obtener esto nos dirigimos a la sección del firewall "Reglas de filtrado para las redes internas", vamos a adicionar la regla para denegar el acceso al objeto llamado redes sociales desde Lan-unad para cualquier protocolo.

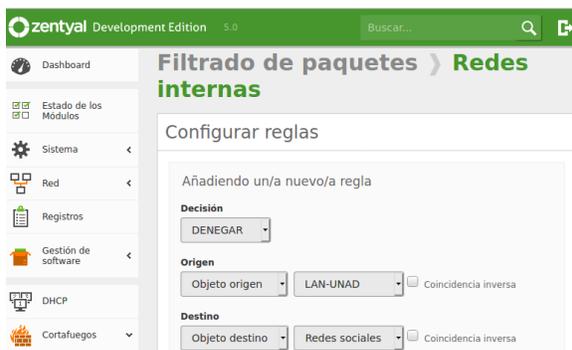


Figura 36. Configuración de filtrado de paquetes.



Figura 37. Vista General Filtrado de Paquetes.

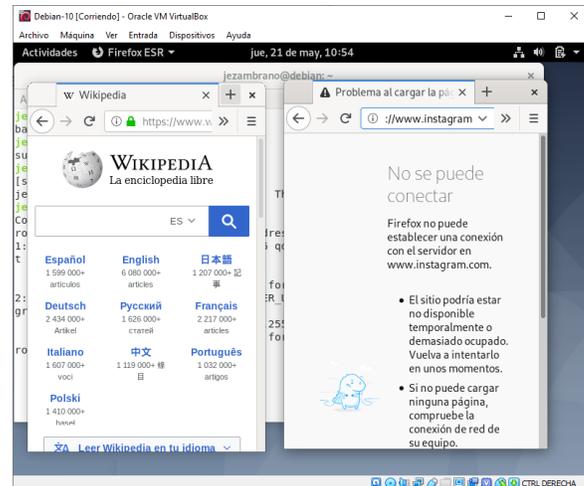


Figura 38. Validación de la regla de bloqueo.

Como se puede ver, la máquina tiene acceso a internet, pero cuando se intenta acceder a la página Instagram no responden.

4.4 TEMÁTICA 4: PRINT SERVER

Print Server: Es un servidor que conecta una impresora a red a nivel global dentro de una estación de trabajo, para que cualquier equipo de la empresa pueda ingresar a ella e imprimir documentos, lo único que se requiere es que el equipo se encuentre en la misma red.

Posteriormente vamos a detallar las operaciones e información presentes en el directorio LDAP de Zentyal en cualquiera de los modos de operación del dominio Desde el menú Dominio podemos comprobar cual es el modo de funcionamiento de nuestro servidor LDAP antes de activar el módulo. Si hemos activado el módulo de Controlador de Dominio y Compartición de Ficheros, nuestro servidor funcionará como Servidor stand-alone por defecto.

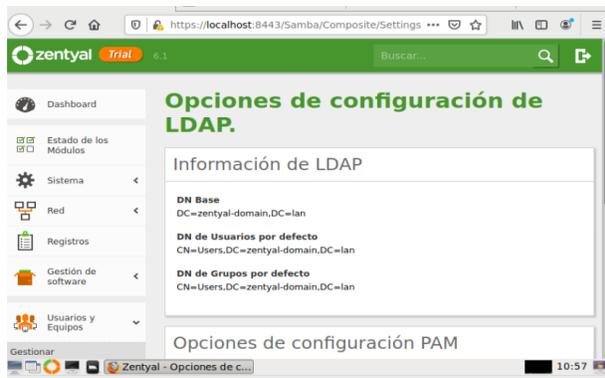


Figura 39. Operaciones de configuración de LDAP.

Instalar el cliente LDAP a través del siguiente comando `sudo apt-get -y install libnss-ldap libpam-ldap ldap-utils nscd`

Después se debe escribir el dominio seleccionado o la IP.

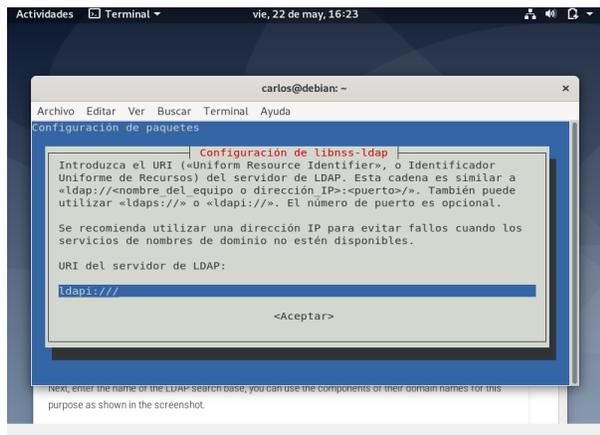


Figura 40. Servidor de LDAP.

Posteriormente se detalla la cuenta de administrador:

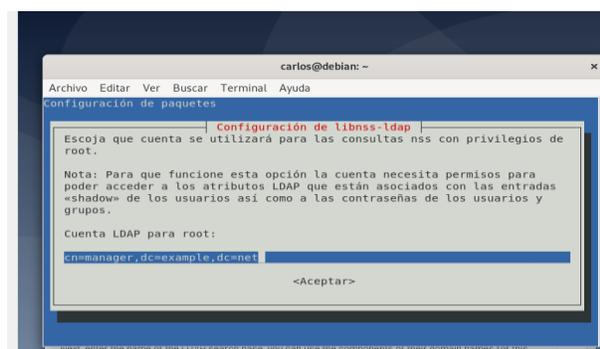


Figura 41. Configuración cuenta LDAP.

Por consiguiente, configuramos el archivo `nsswitch.conf` para trabajar con LDAP a través del comando `sudo nano /etc/nsswitch.conf`.

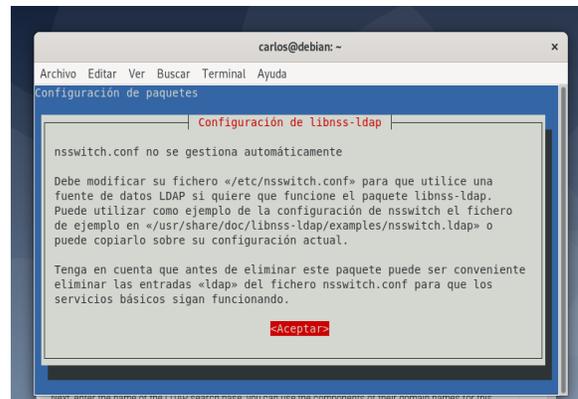


Figura 42. Configuración de libnss-LDAP.

Posteriormente desde Zentyal procedemos a crear los usuarios y grupos.

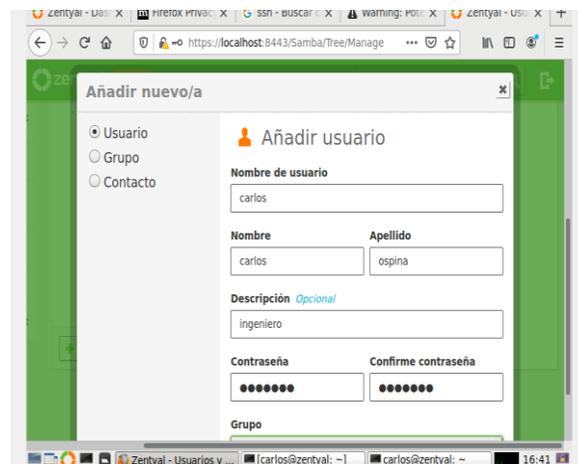


Figura 43. Añadir Usuario.

Luego procedemos a crear una carpeta compartida:

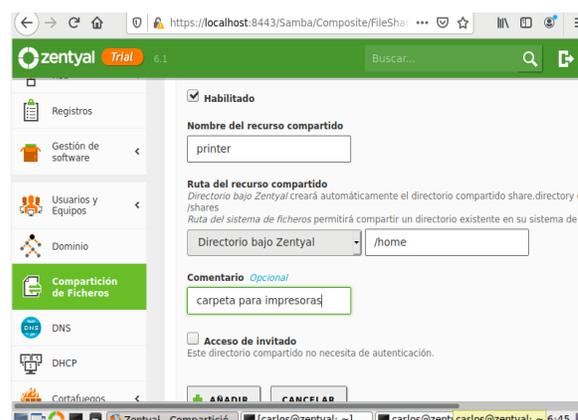


Figura 44. Crear carpeta compartida.

Validamos la creación de la carpeta donde se verán las impresoras compartidas:

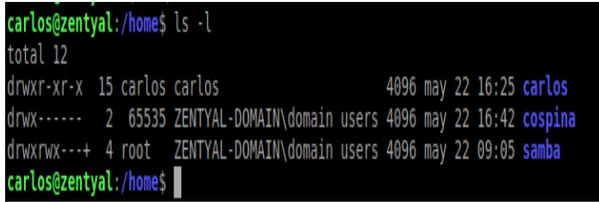


Figura 45. Validación de la regla de bloqueo.

Desde debian 10 ya se puede acceder a la ip de zentyal con el puerto podremos acceder a la carpeta de las impresoras.

4.5 TEMÁTICA 5: VPN

A continuación, debemos ingresar al menú de autoridad de certificación / crear certificado de autoridad, esto para crear para recibir permisos en nuestro servidor para crear certificados de seguridad, importantes para la creación de certificados de acceso al servicio VPN.

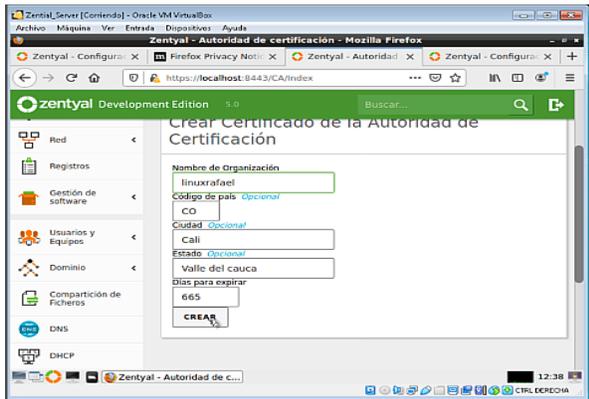


Figura 46. Configuración de certificado de autoridad.

Debemos ir al menú principal y seleccionar la opción VPN / servidores, en conjunto vamos a un nuevo servidor y el nombre respectivo se coloca en él, se agrega y luego se guardan los cambios.

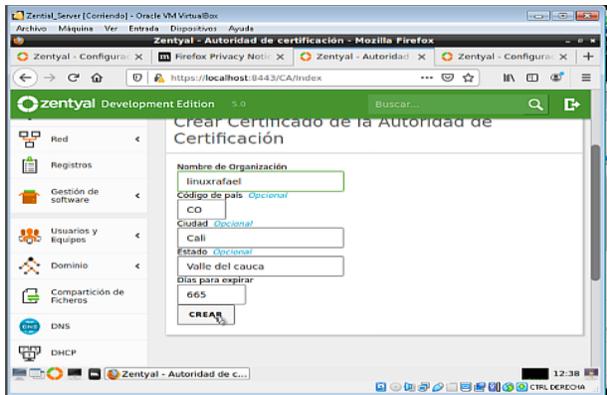


Figura 47. Servidor creado.

Regresamos al menú de autoridad / certificados generales, y emitimos un nuevo certificado para el servidor VPN completando su vencimiento y el nombre que llevan, presione clic y el certificado se guardará

automáticamente y aparecerá en la parte inferior con los otros certificados emitidos.

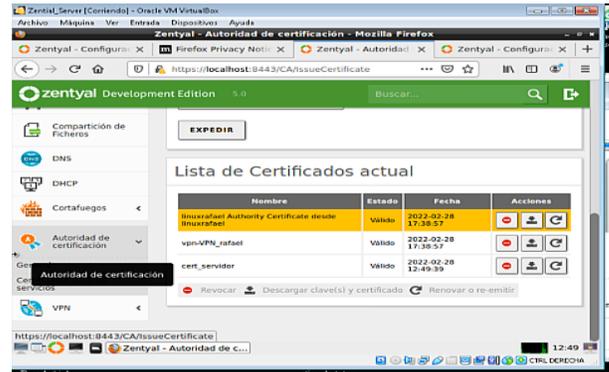


Figura 48. Listado de certificados generados.

Lista de servidores VPN creados, seleccionaremos el primero que se creó al principio en la opción Configuración. Una vez que ingrese, podrá observar los parámetros de configuración del servidor VPN, como el protocolo y el puerto que se utilizan como UDP y 1194, la dirección VPN se deja de forma predeterminada, seleccionamos el certificado del servidor que creamos en el paso anterior, seleccionamos la opción TUN y finalmente en la opción de interfaz en la que escucha se deja en "todas las interfaces de red", las otras opciones se dejan por defecto y luego hacemos clic en guardar.



Figura 49. Configuración de parámetros del servidor VPN.

Agregar la VPN como tal, seleccionando "agregar nuevo" e ingresar el nombre del servicio a crear y la descripción, hacer clic en "Agregar" botón "Y luego se guardan los cambios.

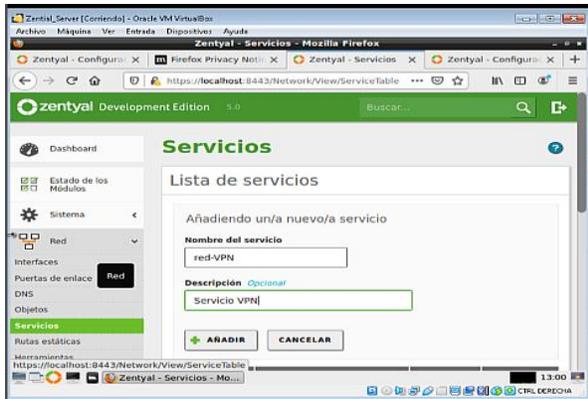


Figura 50. Añadir un servicio de Red.

Una vez agregados, se enumerarán los servicios creados y se enumerará el servicio recién agregado.

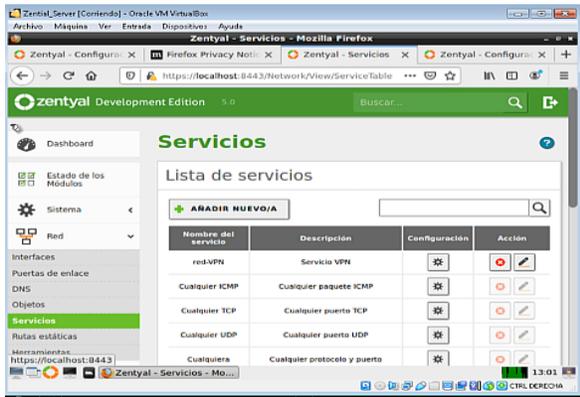


Figura 51. Listado de servicios de Red.

Haga clic en "Agregar". A continuación, debemos parametrizar el protocolo de nuestro servicio en este caso UDP, el puerto de origen seleccionamos "cualquiera" y en el puerto de destino seleccionamos "puerto único" y escribimos el número de puerto de destino en este caso 1194. y hacemos clic en "Agregar" y luego guardar para guardar los cambios generados.

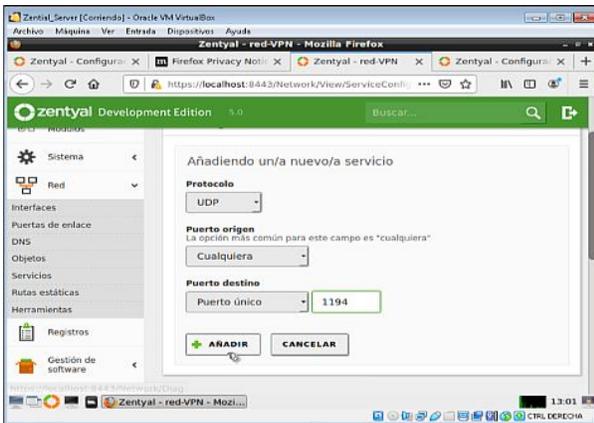


Figura 52. Configuración del servicio de Red.

Lista de reglas y parámetros en el firewall y haremos clic en "agregar nuevo", luego nos pedirá que ingresemos la decisión de la regla, en este caso

seleccionamos "aceptar", el origen debemos ir a la opción "cualquiera" y finalmente seleccionamos el servicio de Red que creamos previamente desde VPN y una descripción de la regla para ingresar, hacemos clic en Agregar y guardamos los cambios.

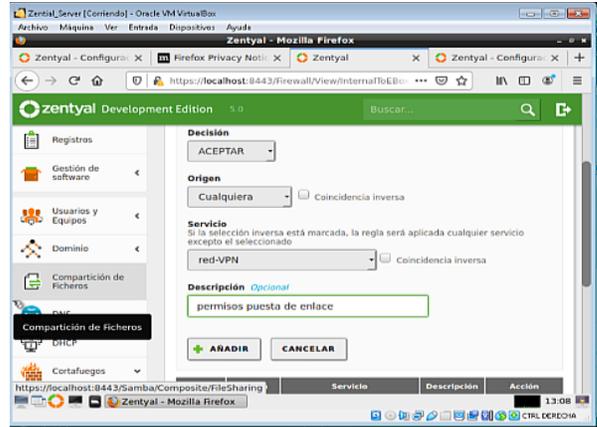


Figura 53. Configuración de regla en el Firewall

Para finalizar el procedimiento, debemos volver al menú VPN / Servidores para validar si la "red anunciada" del servidor que creamos está parametrizada, en este caso, el servidor creó una falla predeterminada en la instalación, por lo que no es necesario para crear un nuevo.



Figura 54. Lista de redes anunciadas.

¿Cuál es la dirección IP de acceso a Internet (red WAN)? ¿Y cuál es la dirección local de nuestro servidor (LAN)? Que se parametriza desde el enrutador principal.



Figura 55. Dirección IP de acceso a internet.

Está claro que las direcciones correspondientes, WAN 181.129.173.250 y LAN 192.168.1.108, luego ingresan al menú "descargar paquete de configuración del cliente" en el menú VPN.

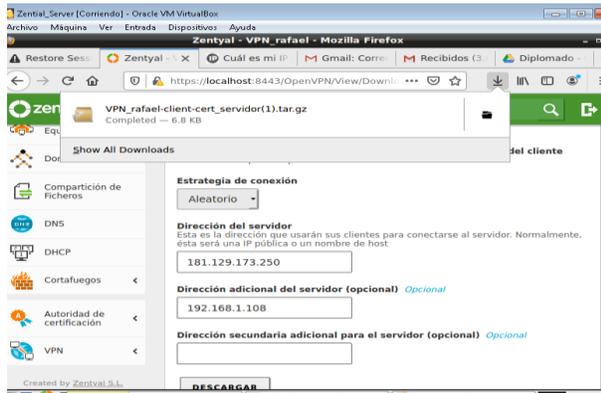


Figura 56. Generar archivo de configuración de acceso a VPN.

Instalamos open VPN con el comando "sudo apt-get install open Vpn", una vez finalizada la instalación, procedemos a ingresar como usuario root en nuestra consola y estamos ubicados en la carpeta donde se encuentra el archivo de configuración de acceso VPN. Tenga en cuenta que el archivo .gz ya está descomprimido, y lo ejecutamos con el comando "openvpn --config VPN_rafael-client.conf" donde VPN_rafael-client.conf.

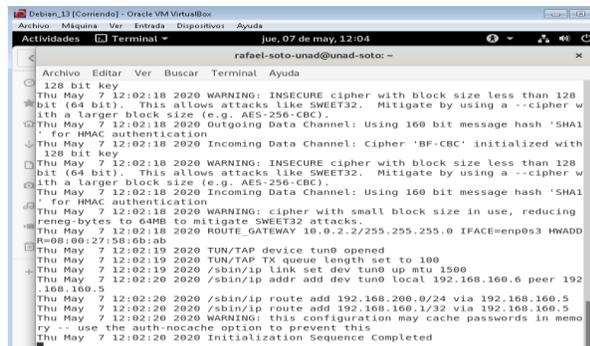


Figura 57. Secuencia completada en Debian 10.

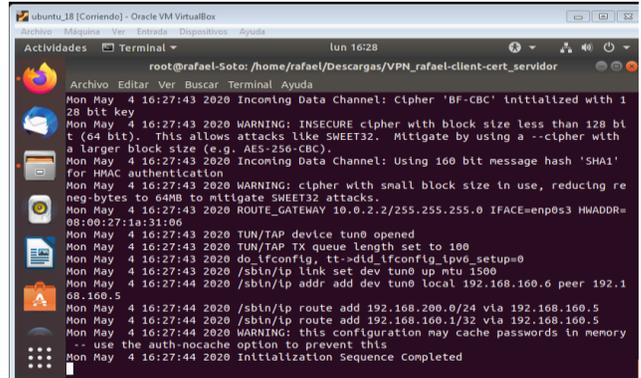


Figura 58. Ejecución del archivo de configuración.

Finalmente, validado a partir de las entradas de los Registros de control del servidor que nuestro equipo cliente más allá de la red accedió, pasamos del servidor Zentyal al menú Registros.

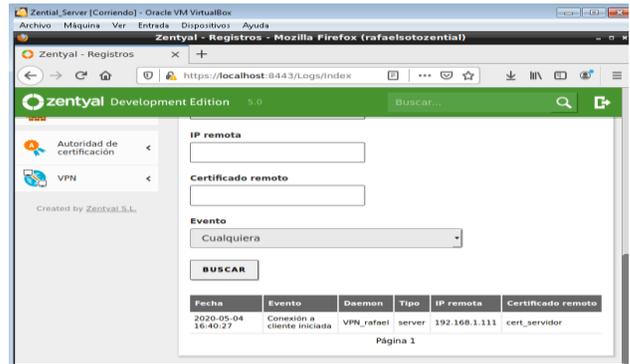


Figura 59. Log de acceso a la VPN por parte del servidor.

5 CONCLUSIONES

La implementación de servicios a nivel de infraestructura TI implica una labor sistemática y estratégica, que promueve una integración tecnológica en la compañía en forma eficiente y eficaz, claro está: en encaminada a resolver las diferentes problemáticas generadas a nivel tecnológico y a la inclusión de mejoras en pro del fortalecimiento de los procesos y servicios informáticos.

El amparo informático o nivel de seguridad de los datos y de la información que circula a través de los servicios TI implementados en una compañía, debe contemplarse en detalle al momento de incluir nuevas tecnologías en la infraestructura TI de una compañía, pese a que los servicios se basan en aplicaciones que operan en sistemas operativos relativamente seguros, es indispensable estructurar un plan que garantice la seguridad de información basándose en la inclusión de firewalls y otras herramientas, que contribuyan sustancialmente a evitar intrusiones y accesos no autorizados.

La Identificación de Zentyal la podemos catalogar como una alternativa muy poderosa a la hora de realizar configuraciones en un entorno de Red, adicional nos ofrece la posibilidad de involucrar servicios web claves para implementar en cualquier organización.

Implementamos y configuramos detalladamente la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Evidenciamos el ingreso a algún contenido o aplicación de la estación de trabajo.

El Diplomado en Linux, nos ayudó a afianzar los conocimientos que poco teníamos sobre, y con todo lo visto en todos los pasos nos deja una buena enseñanza para nuestra vida laboral

6 REFERENCIAS

- [1] A vueltas con los Dominios Samba: Clientes Linux con el software PBIS Open (actualizado). (2017, mayo 2). Un Informático en Almería [En línea]. Disponible en: <https://femarper.wordpress.com/2017/05/02/a-vueltas-con-los-dominios-samba-clientes-linux/>
- [2] Configurar controlador de dominio linux con Zentyal—Blog IT. (s. f.). Recuperado 12 de mayo de 2020. [En línea]. Disponible en: <http://www.datebor.com/controlador-dominio-linux-zentyal/>
- [3] Zentyal—Configuraciones iniciales de Red, DNS y Domino. (s. f.). Recuperado 12 de mayo de 2020. En línea]. Disponible en: <https://www.youtube.com/watch?v=3pVd3a1utZo>
- [4] Zentyal Community. (2017). Es/5.0/Instalacion. 05/2018, de Zentyal Community Sitio web: <https://wiki.zentyal.org/wiki/Es/5.0/Instalacion#el-instaladorde-zentyal>.
- [5] Servicio directorio LDAP <https://doc.zentyal.org/2.2/es/directory.html>