

# DIPLOMADO DE PROFUNDIZACIÓN EN LINUX SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Francia Elena Artunduaga Liscano  
e-mail: Feartunduagal@unadvirtual.edu.co  
Fabian Hernando Erazo Ruiz  
e-mail: fherazor@unadvirtual.edu.co  
Fernando Claros Garcia  
e-mail: fclaros@unadvirtual.edu.co  
Carlos Andres Espinosa Ramirez  
e-mail: caespinosar@unadvirtual.edu.co  
Maria Paula Montano Puentes  
e-mail: mpmontanop@unadvirtual.edu.co

**RESUMEN** – El desarrollo de las actividades propuestas se realiza con base en la Guía de Actividades Rúbrica de Evaluación – Paso 8, en el marco del Diplomado de Profundización en Linux como opción de trabajo de grado en la Universidad Nacional Abierta y a Distancia (UNAD).

**PALABRAS CLAVE:** Linux, Zentyal, Infraestructura, Migración.

## 1. INTRODUCCIÓN

En el desarrollo de la guía se realizarán prácticas que permitirán planear soluciones tipo cliente-servidor instalables en Sistema Operativo GNU/Linux mediante la integración de software de gestión de contenidos/aprendizaje.

La realización de la guía permitirá al estudiante encontrar en el Sistema Operativo GNU/Linux una alternativa diferente a las tradicionales en el manejo e implementación de software.

Se hace énfasis en esta etapa final del curso, en la formulación de soluciones bajo GNU/Linux a través de la

instalación, configuración y puesta en marcha de infraestructura tecnológica.

Se orienta la fase en la administración y control de una distribución GNU/Linux basada en Ubuntu, pero enfocada a la implementación de servicios de Infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas.

Se espera que lo aprendido en el desarrollo del diplomado, sirva como base para dar cumplimiento a los requerimientos de la presente guía

## 2. TEMÁTICA 1

DHCP Server, DNS Server y Controlador de Dominio. Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Después de instalado el sistema operativo, se debe realizar la instalación de los módulos DNS Server, DHCP Server, Red y Controlador de dominio, luego de ser instalados se deben habilitar

Módulo	Depende	Estado
 Red		<input checked="" type="checkbox"/>
 Cortafuegos	Red	<input type="checkbox"/>
 DHCP	Red	<input checked="" type="checkbox"/>
 DNS	Red	<input checked="" type="checkbox"/>
 Registros		<input type="checkbox"/>
 NTP		<input checked="" type="checkbox"/>
 Controlador de Dominio y Compartición de Ficheros	Red, DNS, NTP	<input checked="" type="checkbox"/>

Figura 1. Instalación de módulos

Primero se configuran las interfaces de red, que en este caso se deben crear dos. La interfaz eth0 será nuestra wan, por lo tanto la dejamos en modo DHCP, en virtual box se configura en modo puente



Figura 2. Interfaces de red

eth1 en la configuración de virtual box estará conectada a la red interna, y para esta actividad se configurará con la IP 192.168.200.1

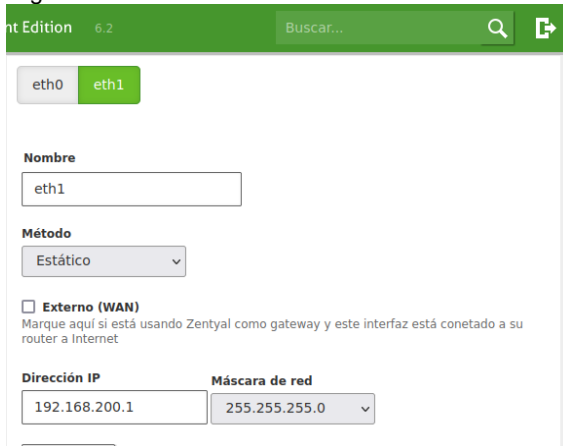


Figura 3. Configuración Interfaces

Posteriormente se configura el servidor DNS, agregando una dirección DNS de google, con esto las estaciones de trabajo de nuestra red interna podrán navegar en internet a través de direcciones web

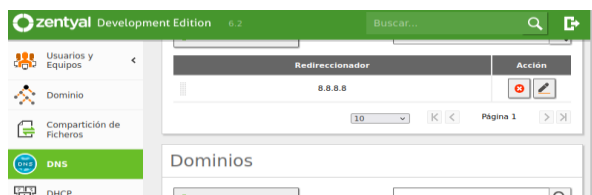


Figura 4. Configuración DHCP

Ahora se configura el servidor DHCP, se crea el rango de IP's a asignar entre la dirección 192.168.200.100 hasta la IP 192.168.200.110

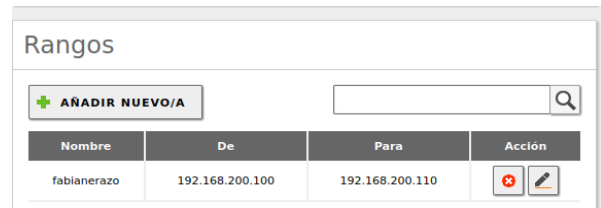


Figura 5. Rangos de IP

Se crea un nuevo usuario a través del módulo usuarios y equipos



Figura 6. Usuarios y equipos

Encendemos nuestra estación de trabajo y verificamos que la dirección IP asignada este dentro del rango de direcciones configuradas en el servidor DHCP y efectivamente vemos que la IP asignada es 192.168.200.100, la primera del rango creado

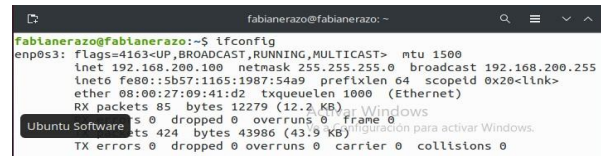


Figura 7. Asignación de IP

Realizamos un ping desde la estación de trabajo hasta el servidor Zentyal

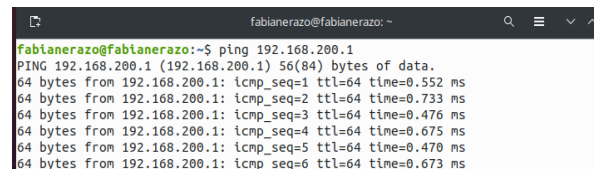


Figura 8. Testeo de ping

También realizamos un ping desde el servidor Zentyal hasta la estación de trabajo comprobando que la conexión es bidireccional

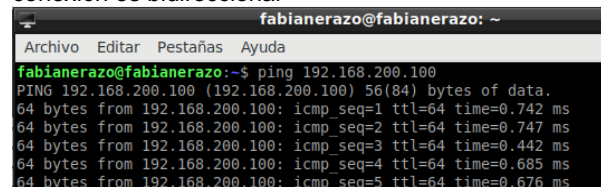


Figura 9. Ping estaciones de trabajo

Desde la estación de trabajo, ingresamos al servidor Zentyal a través del navegador web por medio de la dirección <https://192.168.200.1:8443>

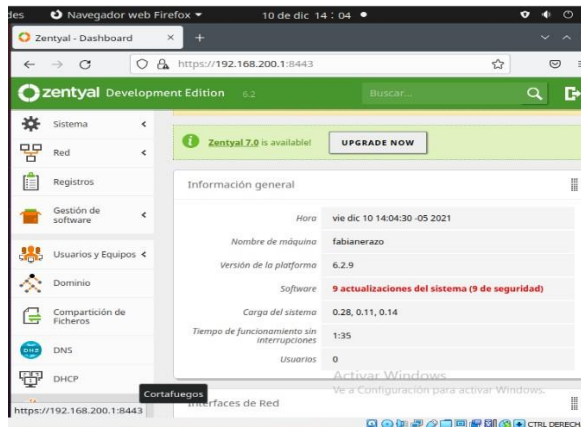


Figura 10. Ingres a zentyal

Podemos ver que la estación de trabajo se reporta dentro del estado del servidor Zentyal, en el apartado DHCP



Figura 11. Reporte estación de trabajo

### 3. TEMÁTICA 2

A continuación, se presenta el desarrollo de la temática número 2 - Proxy no transparente –

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

El siguiente procedimiento se fundamenta en ejercicios teóricos realizados en temáticas similares, dadas las condiciones de falencia en el equipo de cómputo para efectuar las debidas instalaciones de software.

Como requisito para poder desarrollar la actividad se debe proceder a la instalación de Zentyal Server.

Descargar Zentyal de la web oficial:  
<https://zentyal.com/es/news/zentyal-6-2>



Figura 12. Web oficial Zentyal

Una vez realizado el procedimiento se da respuesta al ejercicio propuesto.

¿Qué es un proxy transparente?

Proxy transparente: su principal característica es que no requiere una configuración del navegador y, por tanto, los usuarios pueden desconocer su existencia. En especial, es empleado por las empresas para controlar el uso de Internet que hacen sus empleados, ya que incluso puede restringir el acceso a determinados sitios.

La funcionalidad de proxy es una herramienta imprescindible de seguridad que tiene por finalidad administrar los accesos de dispositivos, de la red interna, a otras redes y a Internet.

Instalaciones:

Se procede con la instalación de Zentyal teniendo en cuenta la configuración en dos adaptadores de red:

Adaptador para la Wan  
 Adaptador de red interna (LAN)



Figura 13. Configuración adaptadores Wan - LAN

Procedemos a iniciar desde un cliente para realizar la configuración en este caso sería Ubuntu, teniendo en cuenta que la interfaz del cliente debe estar dentro de la LAN.



Figura 14. Módulos a instalar

Es importante, antes de iniciar la configuración de los adaptadores seleccionar algunos módulos que se requieren en el desarrollo de la temática.



Figura 15. Interfaces de red

WAN está de DHCP donde es la entrada a internet.



Figura 16 Wan DHCP

LAN queda estático con una IP privada 11.0.0.1 mascara 24.

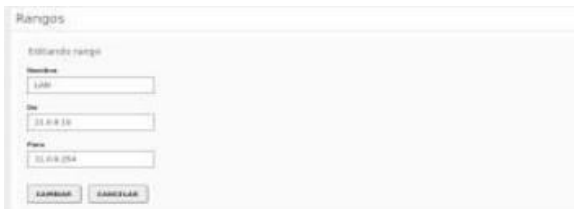


Figura 17. Rango LAN

Desde el DHCP se configura el rango a establecer en la LAN.

La dirección del servidor se obtiene por el puerto 8443.

Ya en este punto se acceden a las siguientes configuraciones desde Ubuntu.

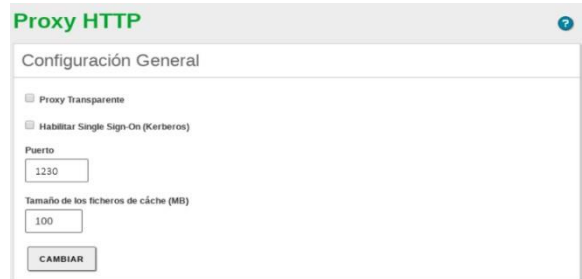


Figura 18. Configuración del proxy no transparente

Se realiza la configuración del proxy no transparente a través del puerto 1230.



Figura 19. Habilitación módulo

Se habilita el módulo como se indica en la figura 8.



Figura 20. Denegación del servicio

Se Procede a configurar una regla en la LAN para denegar todo el servicio fuera del proxy.

Quedando de la siguiente forma:



Figura 21. Servicio denegado luego de la configuración

Para terminar, se verifica la navegación sin el proxy en un cliente que para este caso es Ubuntu;

evidenciándose de acuerdo a la figura 10 que la regla en firewall se está ejecutando.

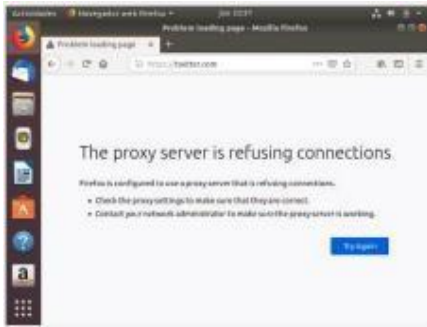


Figura 22. Verificación navegación

#### 4. TEMÁTICA 3

¿Que es un Cortafuegos?

Específicamente si nos enfocamos en el entorno de las redes de computadores, entonces un cortafuegos es un sistema de contención que intenta impedir la diseminación daños a través suyo. Ahora, si lo planteamos de manera física, entonces un cortafuegos en la Internet es un sistema o grupo de sistemas informáticos ubicados en el perímetro de una red para proteger todas sus vías



Figura 23. Instalación zentyal 6.2

Luego aquí ya tendremos acceso al Dashboard del panel de Zentyal (Se inicio sesión previamente con usuario: Fernando claros, clave: 12345)

Ahora el paso siguiente es instalar los paquetes necesarios, entre ellos por supuesto el “Cortafuegos”

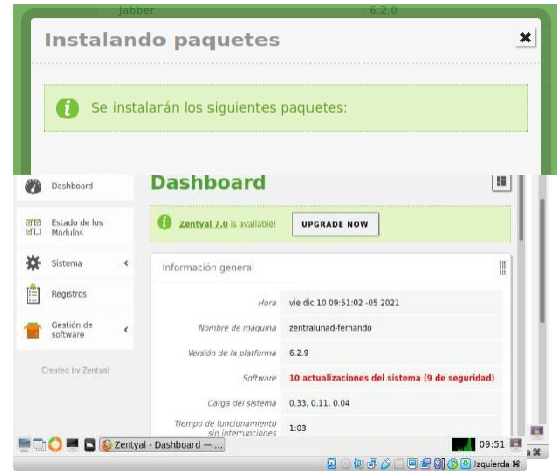


Figura 24 Instalación paquetes

Aquí observamos que los paquetes ya están completamente instalados

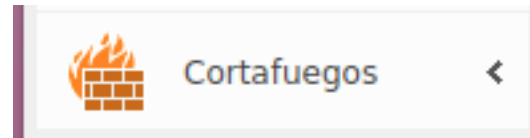
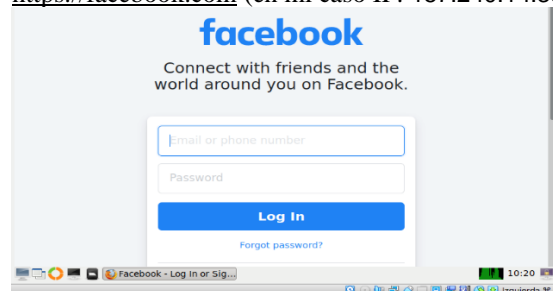


Figura 25. Paquete cortafuegos

Ya después del paso anterior aquí en el panel izquierdo tendremos acceso al módulo de Cortafuegos

Aquí inicialmente podemos observar que tenemos acceso a la plataforma social de Facebook: <https://facebook.com> (en mi caso IP: 157.240.14.35)

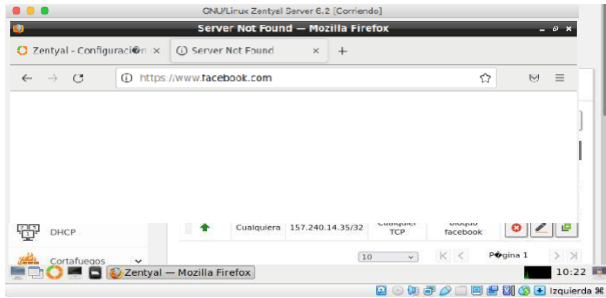


Observamos que en este paso creamos las reglas a través del cortafuegos en las cuales prevenimos el acceso a Facebook a través de su IP (TCP, HTTPS, HTTP)

Figura 27. Filtrado de paquetes

Ahora probamos nuevamente el acceso a Facebook y vemos que ya no podemos acceder y esto es gracias a la regla que niega los accesos.





### 5. TEMATICA 4

File Server y Print Server.

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

File Server.

Se realiza el proceso de verificación del controlador de dominio y compartición de ficheros esté instalado.



Figura 27. Verificación de los módulos.

Se realiza el proceso de Ingreso al módulo Compartición de ficheros, para agregar un nuevo directorio compartido.

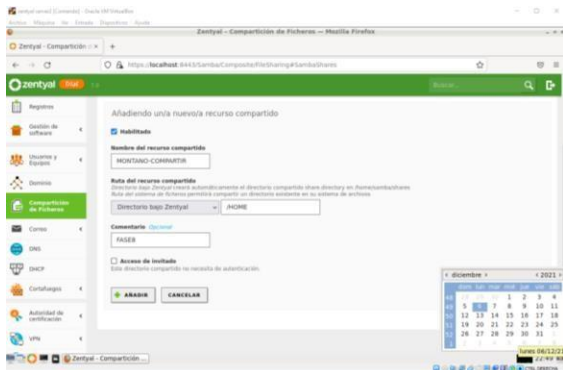


Figura 28. recursos compartidos

Creación de un usuario que tendrá acceso al dominio y permisos de lectura y escritura sobre el directorio creado.

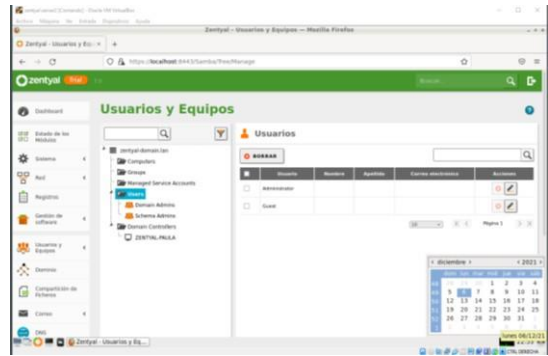


Figura 29. creación de usuarios

Asignación de una ACL al fichero compartido, es decir, los permisos, para ello ingresamos a la configuración del directorio y damos clic en añadir

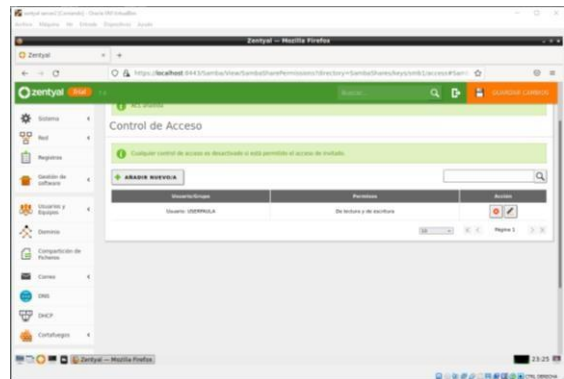


Figura 30. Control de acceso

En la máquina virtual cliente, en este caso Ubuntu, para realizar la conexión, para ello instalamos samba cliente y se realiza la configuración necesaria del dominio, luego se abre el gestor de archivo, damos clic en otras ubicaciones y en la parte inferior digitamos en la casilla conexión (ip del servidor) y damos clic en Conectar.

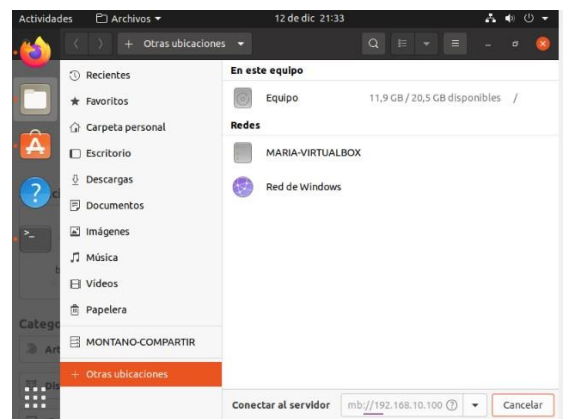


Figura 31. Conexión al servidor.

Print Server

Se realiza la instalación del paquete cups-PDF en la consola de administrador en Zentyal

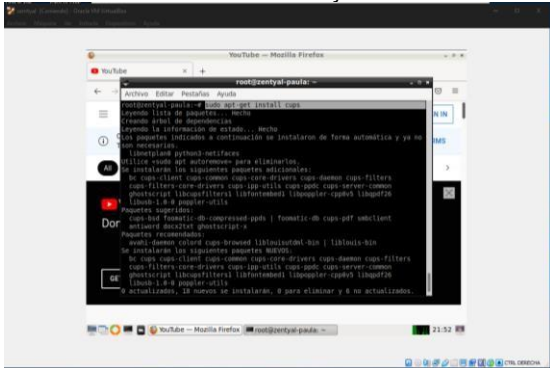


Figura 32. Instalación de paquetes cups

Se abre en el navegador el servidor con la dirección https://localhost:631, y se agrega una impresora dando clic en Administración y luego en Add Printer

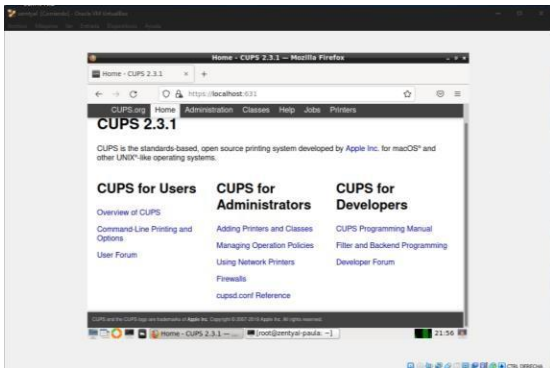


Figura 33. Ingreso a cups

Se elije una dirección con la cual se va a realizar la conexión

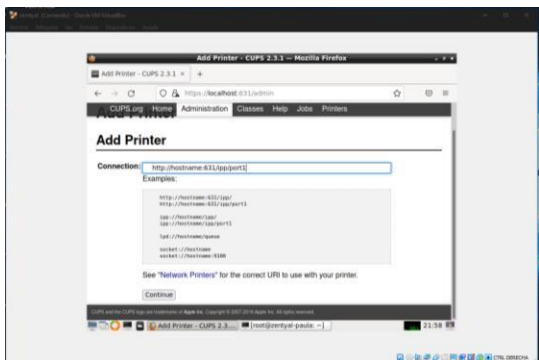


Figura 34. Conexión

Se digita el nombre de la impresora, se selecciona Share This Printer, también elegimos modelo y marca, luego damos clic en continuar

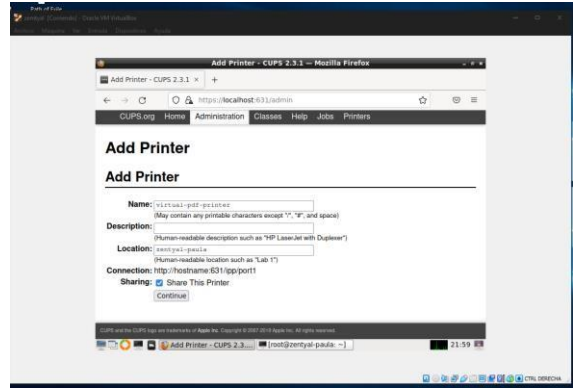


Figura 35. Selección

Ahora ingresamos al cliente, después de la instalación de cups, realizamos la conexión de la impresora, colocando la dirección de conexión.

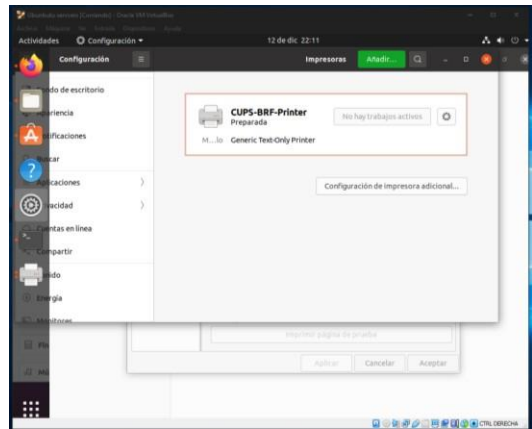


Figura 36. Conexión de impresora

## 6. TEMATICA 5

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo

Una vez instalado el servidor Zentyal se configura las interfaces de red una con una ip fija como red interna en eth0 y la otra como red externa, de igual forma se instala el paquete de VPN

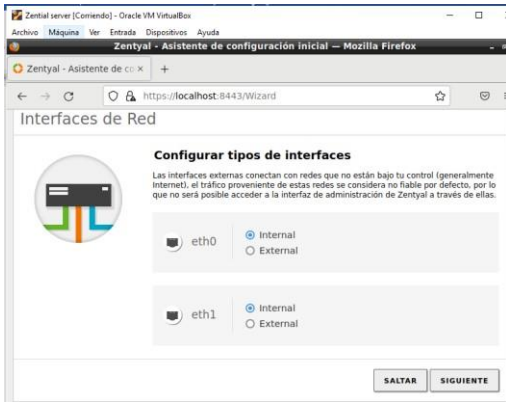


Figura 37. Configuración red

Se configura la red en caso de tener interfaces externas y se deja como DHCP, al finalizar se observan las 2 tarjetas de red con las direcciones mac asignadas

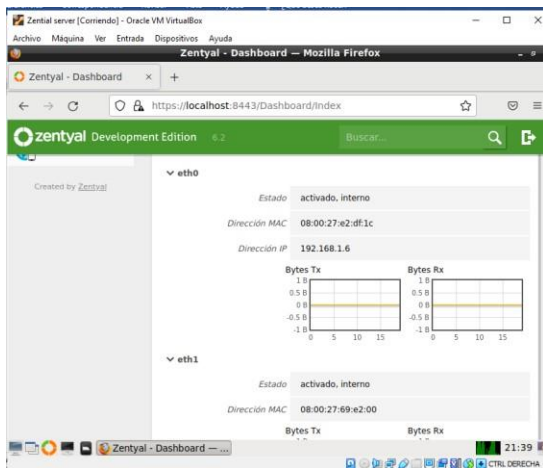


Figura 38.verificacion tarjetas de red

Configuramos la tarjeta eth1 en la interfaz de red y le asignamos una dirección ip 192.168.80.1, esto es para que el servidor DHCP genere la red 192.168.80.0/24

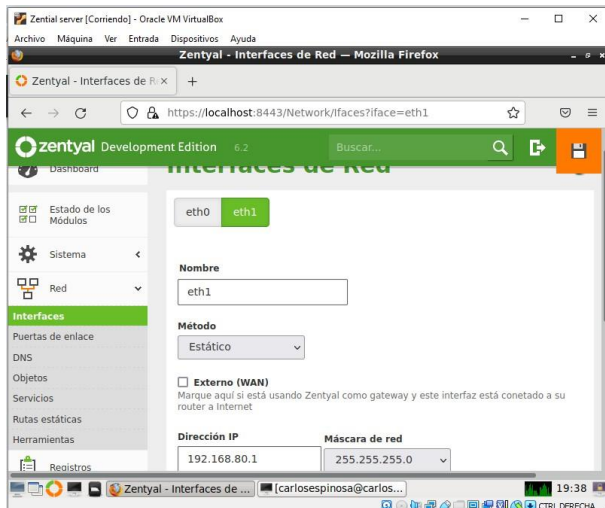


Figura 39. Configuración aplicada

Se procede a instalar el paquete de VPN del zentyal donde se instalar todos los paquetes al igual que el paquete de cortafuegos e interfaces de red

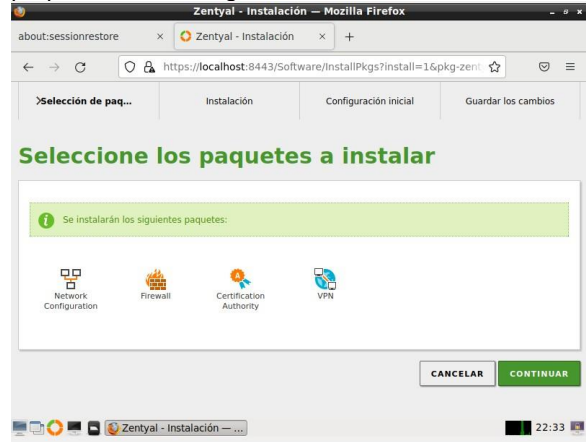


Figura 40.Paquetes a instalar

El siguiente paso es crear la autoridad de certificación sin ella no es posible configurar la VPN y crear nuestro servicio como una autoridad certificada., damos click en el menú autoridad de certificación y escogemos la opción general y allí nos presenta la pantalla autoridad de certificación.

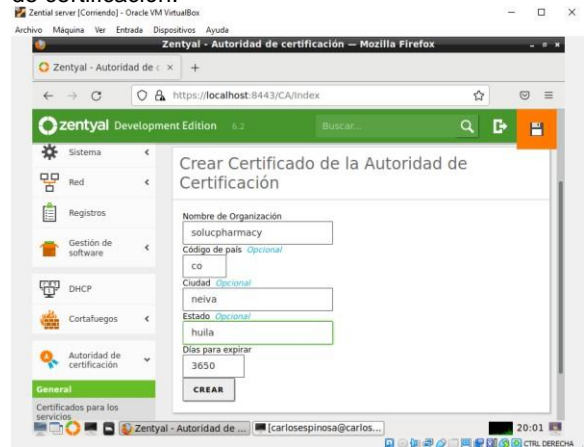


Figura 41.Creacion de certificado de seguridad

Crear y se presenta en pantalla el certificado de autoridad de certificación creada, también creamos enseguida 2 más certificados que son para el servidor zentyal y el otro para el cliente de conexión en este Caso para maestro ubuntu



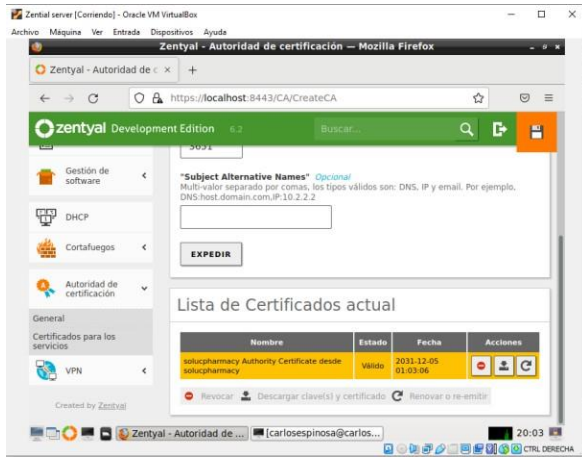


Figura 42.Verificación certificados creados

Vamos a la opción VPN y escogemos la opción servidores VPN, se va a crear el servidor para los clientes de Linux, damos click en añadir nuevo



Figura 43. Creación servidor VPN

En la pantalla de configuración escogemos el puerto del servidor UDP en el puerto 11194 y asignamos la subred de la VPN 192.168.161.0/24, escogemos el certificado del servidor creado anteriormente, a las demás opciones se pueden dejar por defecto, click en cambiar.

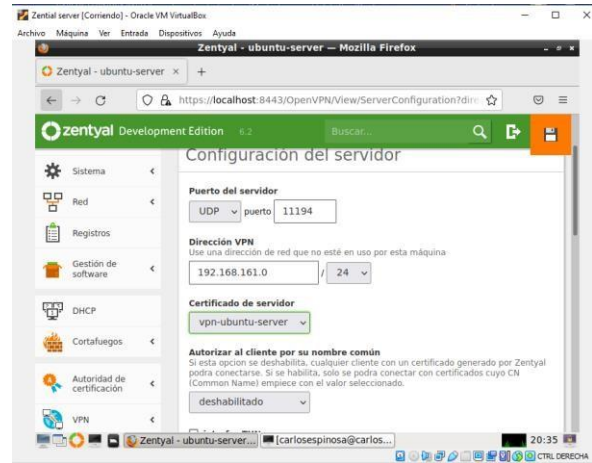


Figura 44. Configuración servidor

Configuramos el paquete de configuración, cerciorándonos que sea para este caso cliente Linux con la ip de nuestro servidor

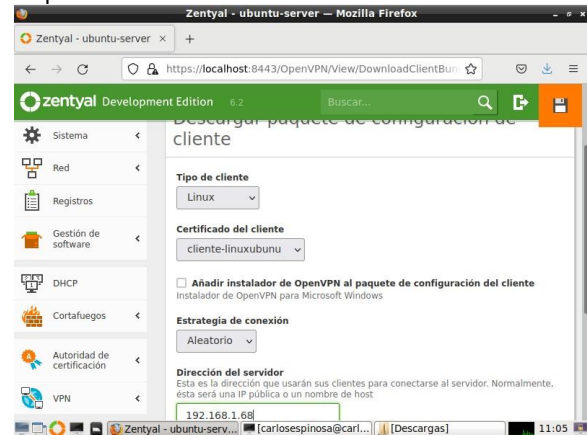


Figura 45.Creacion VPN

Ahora vamos a la maquina cliente del Ubuntu desktop e instalamos la VPN.

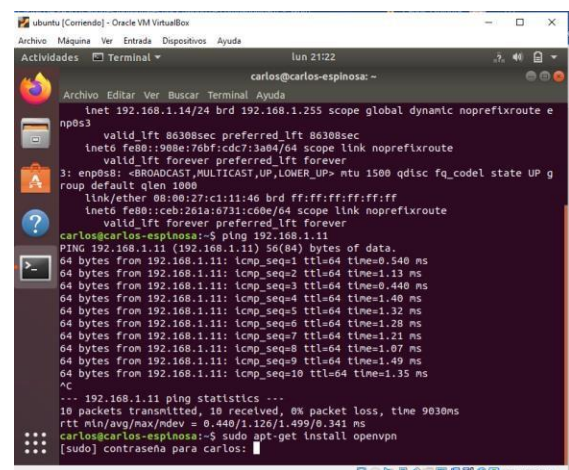


Figura 46. Instalcion VPN en el Ubututu Desktop

Descargamos el certificado en nuestra máquina de Linux Ubuntu y se descomprime la carpeta

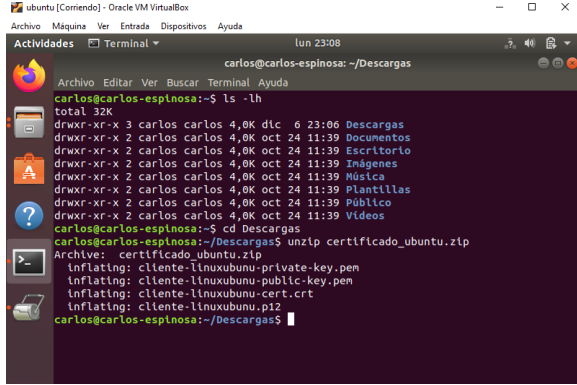


Figura 47. Descarga de certificado en el Ubuntu Desktop

Copiamos el archivo cliente-server-linux.conf a la carpeta /etc/openvpn y renombramos el achivo a client.conf

Una vez agregado el archivo de configuración de nuestra vpn ejecutamos nuestra vpn de forma manual o gráfica, para este caso lo haremos de forma gráfica y se confirma el archivo zentyal.conf cargado correctamente junto con los .pem

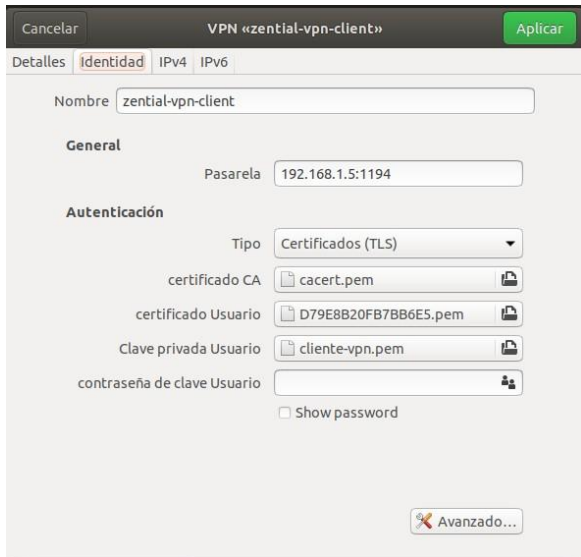


Figura 48 Condiguracion VPN en Ubuntu Desktop

Le damos conectar a nuestra vpn, donde observamos su estado de conexión exitosa

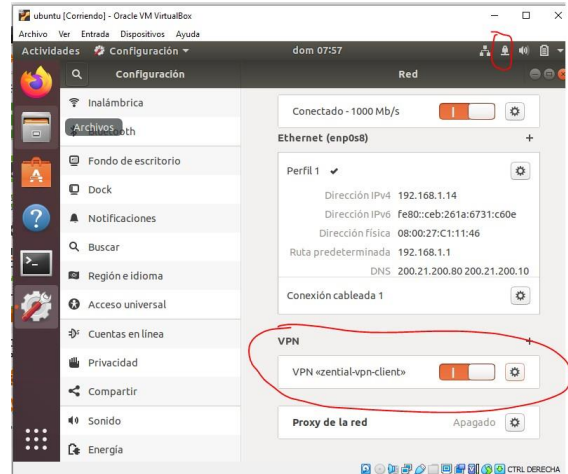


Figura 49 Conectar VPN en Ubuntu desktop

En línea de comandos ejecutamos el comando ipaddress y verificamos como al conectar la vpn el sistema agrega un ip que es la conexión puente para la conexión al zentyal, se hace ping a dicha ip donde el zentyal responde a dicha solicitud

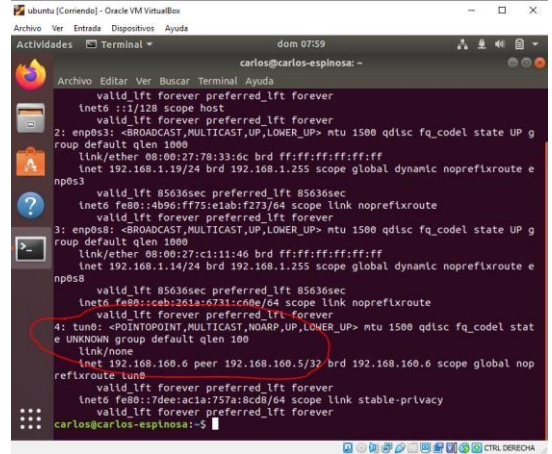


Figura 50.Desconexion de la VPN

Desconectamos la vpn y de nuevo hacemos ping a la conexión puente que es este caso es la ip 1920168.160.6 y observamos que de forma exitosa no se puede conectar hacia esa IP al estar desconectada la vpn

```

carlos@carlos-espinoza: ~
└─$ ping 192.168.160.6
PING 192.168.160.6: icmp_seq=97 ttl=64 time=0.072 ms
64 bytes from 192.168.160.6: icmp_seq=98 ttl=64 time=0.064 ms
64 bytes from 192.168.160.6: icmp_seq=99 ttl=64 time=0.059 ms
64 bytes from 192.168.160.6: icmp_seq=100 ttl=64 time=0.063 ms
64 bytes from 192.168.160.6: icmp_seq=101 ttl=64 time=0.067 ms
64 bytes from 192.168.160.6: icmp_seq=102 ttl=64 time=0.063 ms
64 bytes from 192.168.160.6: icmp_seq=103 ttl=64 time=0.064 ms
64 bytes from 192.168.160.6: icmp_seq=104 ttl=64 time=0.058 ms
64 bytes from 192.168.160.6: icmp_seq=105 ttl=64 time=0.059 ms
64 bytes from 192.168.160.6: icmp_seq=106 ttl=64 time=0.050 ms
64 bytes from 192.168.160.6: icmp_seq=107 ttl=64 time=0.064 ms
64 bytes from 192.168.160.6: icmp_seq=108 ttl=64 time=0.076 ms
64 bytes from 192.168.160.6: icmp_seq=109 ttl=64 time=0.056 ms
64 bytes from 192.168.160.6: icmp_seq=110 ttl=64 time=0.033 ms
64 bytes from 192.168.160.6: icmp_seq=111 ttl=64 time=0.028 ms
^C
--- 192.168.160.6 ping statistics ---
111 packets transmitted, 111 received, 0% packet loss, time 112618ms
rtt min/avg/max/mdev = 0.021/0.054/0.129/0.021 ms
carlos@carlos-espinoza: ~
└─$ ping 192.168.160.5
PING 192.168.160.5 (192.168.160.5) 56(84) bytes of data.
^C
--- 192.168.160.5 ping statistics ---
34 packets transmitted, 0 received, 100% packet loss, time 33779ms
carlos@carlos-espinoza: ~
└─$ ping 192.168.160.6
PING 192.168.160.6 (192.168.160.6) 56(84) bytes of data.

```

Figura 51. Prueba exitosa de ping

## 7. CONCLUSIONES

Con la implementación de la temática propuesta se logró formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permitió dar respuesta a los requerimientos específicos del cliente.

De esta manera, se demuestran las bondades y beneficios que esta alternativa de software libre trae a los diferentes usuarios como herramienta para optimizar sus procesos.

Con el desarrollo de este documento trabajamos sobre el concepto y las funcionalidades y usos de los "Cortafuegos" los cuales en la Internet; son un sistema o grupo de sistemas informáticos ubicados en el perímetro de una red para proteger todas sus vías de acceso estableciendo un control del tráfico de entrada y salida.

## 8. REFERENCIAS

- [1] Zentyal. (2004-2019). *Descarga de Zentyal Server Development Edition*. Recuperado de <https://zentyal.com/es/comunidad/>
- [2] ValorTop S.L. (2014-2018). *¿Qué es un proxy o servidor proxy?* Recuperado de <http://www.valortop.com/blog/servidorproxy>
- [3] Zentyal Community (s/f). *Servicio de Proxy HTTP*. <https://doc.zentyal.org/es/proxy.html>
- [4] Moises, Carlos. (s/f). *Proxy no transparente*. <https://repository.unad.edu.co/bitstream/handle/10596/27888/cmgarciata.pdf?sequence=1&isAllowed=y>