

# IMPLEMENTACIÓN DE SERVICIOS EN INFRAESTRUCTURA CON HERRAMIENTA ZENTYAL 7.0 VERSION COMMUNITY

José Danilo Coral Benavides  
e-mail: jdoralbe@unadvirtual.edu.co  
Carlos Antonio Ramos Hidalgo  
e-mail: caramosh@unadvirtual.edu.co  
Brayan Alexis Mesías Enríquez  
e-mail: bamesiase@unadvirtual.edu.co  
Esteban Cárdenas Arévalo  
e-mail: ecardenasar@unadvirtual.edu.co  
Yemerson Jalvin Maca  
e-mail: yjalvinm@unad.edu.co

**RESUMEN:** *Instalación y configuración de sistema operativo Zentyal Server. Configuración de servicios DHCP Server, DNS Server y controlador de dominio. Implementación y configuración de un proxy para control de acceso a internet desde Zentyal, filtrando la salida a través del puerto 3128. Configuración de Zentyal como firewall dentro de una red perimetral, y restricción de acceso a sitio web de entretenimiento y redes sociales a través del firewall de Zentyal. Configuración de acceso a través de un controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras. Creación de una VPN para establecer un túnel privado de comunicación con una estación de trabajo GNU/LINUX Ubuntu Desktop.*

**PALABRAS CLAVE:** GNU Linux, Redes, Soluciones de infraestructura, Zentyal.

## 1 INTRODUCCIÓN

Este artículo presenta la instalación y configuración del Sistema Operativo GNU/Linux Zentyal Server 5.1, haciendo uso de las técnicas previamente aprendidas en el Diplomado de Profundización en Linux; sistema operativo que será base para disponer de los servicios de infraestructura IT., contenidos en la temática nro. 1, seleccionada por la suscrita en el foro colaborativo, donde se deberá configurar e implementar los servicios de gestión en DHCP Server DNS Server y Controlador de Dominio dentro de nuestro sistema; debiendo entregar la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

## 2 INSTALACIÓN ZENTYAL

Para la solución del ejercicio lo primero que se debe hacer es la instalación de Zentyal como máquina virtual. Vamos

a ingresar a la página de descargas de Zentyal y descargamos la ISO con el instalador [1].



Figura 1. Descargar Zentyal.

Posterior vamos a realizar la instalación de la ISO en Virtual Box.



Figura 2. Inicio Máquina virtual.

Seguido vamos a seleccionar el idioma con el cual queremos trabajar.

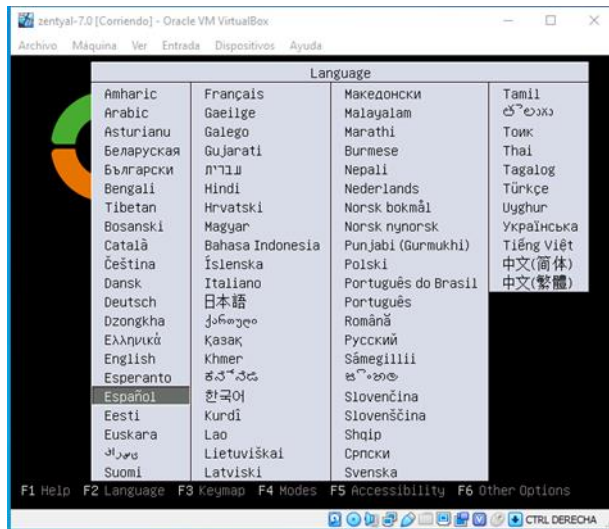


Figura 3. Idioma a trabajar.

Y escogemos la distribución que queremos instalar.



Figura 4. Inicio Máquina virtual.

Inicia la instalación y nos pide nuevamente seleccionar el idioma de trabajo.

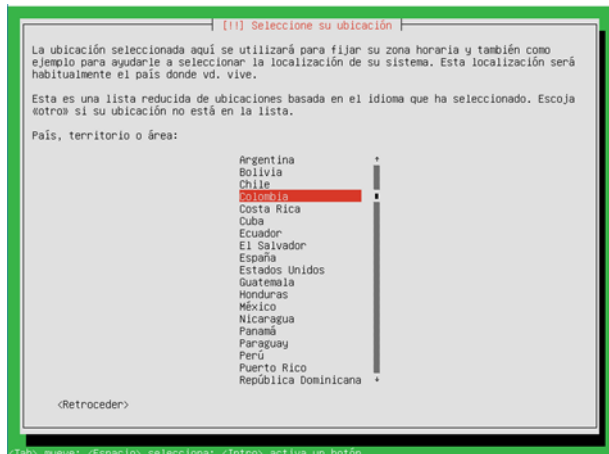


Figura 5. Inicio Máquina virtual.

Ahora seleccionamos el idioma del teclado con el cual vamos a trabajar.

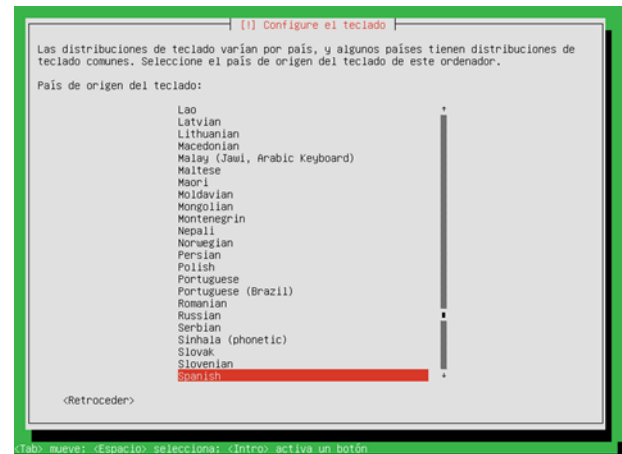


Figura 6. Inicio Máquina virtual.

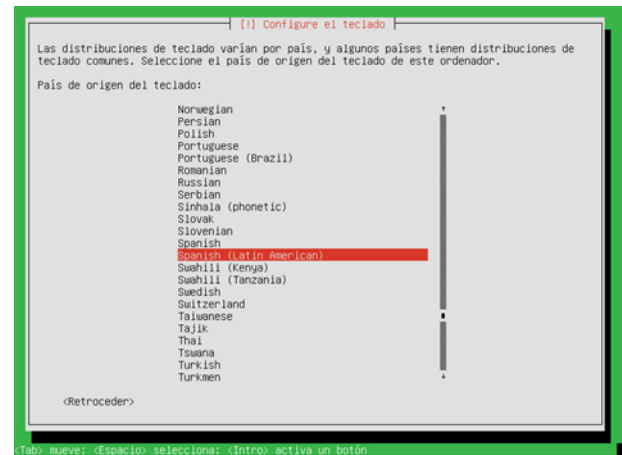


Figura 7. Inicio Máquina virtual.

Entonces se inicia la instalación del sistema operativo.

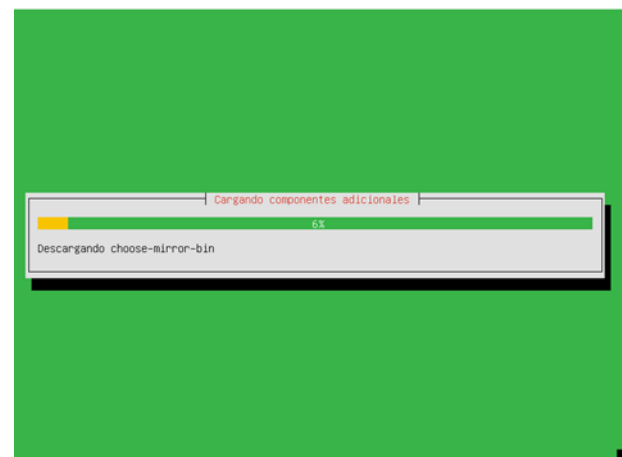


Figura 8. Inicio Máquina virtual.

Posterior le asignamos un nombre a nuestro equipo para ser ubicado en la red.



Figura 9. nombre de equipo.

Luego debemos seleccionar el nombre del usuario principal del sistema y su contraseña.



Figura 10. Inicio Máquina virtual.

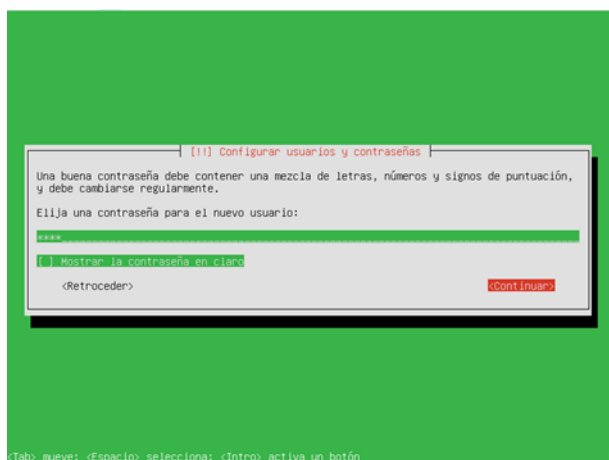


Figura 11. Inicio Máquina virtual.

Posteriormente en la instalación nos muestra que se conecta automáticamente a un servidor de tiempo.



Figura 12. Configuración regional.

Y continúa la instalación.

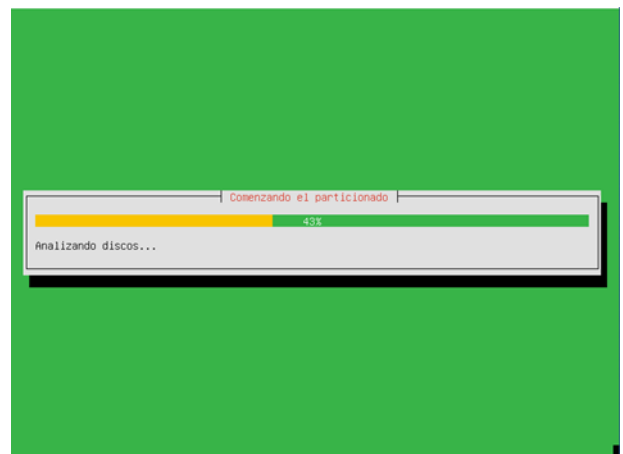


Figura 13. Inicio Máquina virtual.

Finalmente, cuando la instalación termine aparece el siguiente recuadro:

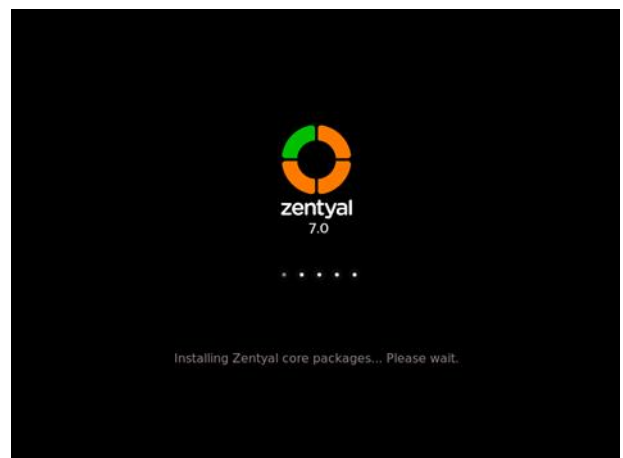


Figura 14. Inicio Máquina virtual.

Al reiniciarse iniciamos nuestro sistema operativo en modo gráfico.



Figura 15. Inicio Máquina virtual.

### 3 CONFIGURACIÓN DE ZENTYAL

#### 3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Los servicios DHCP, DNS y controlador de dominio han venido siendo muy usados en empresas que implementan controles de acceso y políticas de seguridad de la información que buscan mitigar los riesgos de accesos no autorizados o cualquier evento en el que se pueda verse afectada la integridad, disponibilidad o confidencialidad de su información y sistemas informáticos.

Zentyal 7.0 ofrece una forma práctica y sencilla de configurar estas tres soluciones, para lo cual se incluyen los servicios de Firewall y NTP como complementos requeridos. dichas soluciones son compatibles con equipos que usen sistemas operativos GNU Linux o Microsoft Windows®, la capacidad de

usuarios y host conectados es escalable y depende de las características del servidor donde Zentyal 7.0 sea instalado, por ejemplo, el sitio web oficial nos comparte en la Figura 20 [1]:

ZENTYAL PROFILE	USERS	CPU	MEMORY	DISK	NETWORK CARDS
Gateway	<50	i3 or higher	2 GB	80 GB	2 or more
	50 or more	Xeon Dual core or higher	4 GB	160 GB	2 or more
Infrastructure	<50	i3 or higher	4 GB	80 GB	1
	50 or more	i3 or higher	8 GB	160 GB	1
Office	<50	i3 or higher	8 GB	500 GB	1
	50 or more	Xeon Dual core or higher	16 GB	1 TB	1
Communications	<50	i3 or higher	4 GB	500 GB	1
	50 or more	Xeon Dual core or higher	8 GB	1 TB	1

Hardware requirements table

Figura 16. 3.1 -Zentyal requisitos.

Con la cual podemos fácilmente identificar las limitaciones que nuestro servidor pueda llegar a tener.

Existen algunas otras soluciones más robustas o de similares características como lo son el Windows Server® el cual ofrece soporte a diferentes funcionalidades aplicadas a nuestra infraestructura e integraciones fáciles con servicios en la nube en Azure, sin embargo, su costo

de licenciamiento es considerable además de que por ser uno de los sistemas operativos más populares, también es uno de los que más ataques informáticos recibe. Otra opción interesante es NethServer el cual es una herramienta muy robusta y similar en sus características a Zentyal, ambos cuenta con versiones community o licenciadas con soporte, está basado en CentOS y realizando una comparación algo superficial y basada en opiniones de debates realizadas en foros online, cuenta con más herramientas y funcionalidades para ser usado como Gateway y Firewall, sin embargo, debido a que en este punto específico buscamos implementar las soluciones de DNS, DHCP y controlador de Dominio, considero que Zentyal está mucho más especializado en estos tres servicios.

Pasando a el proceso de configurar estas soluciones, se realiza el siguiente proceso:

Posterior a la instalación básica, iniciamos nuestra configuración inicial:

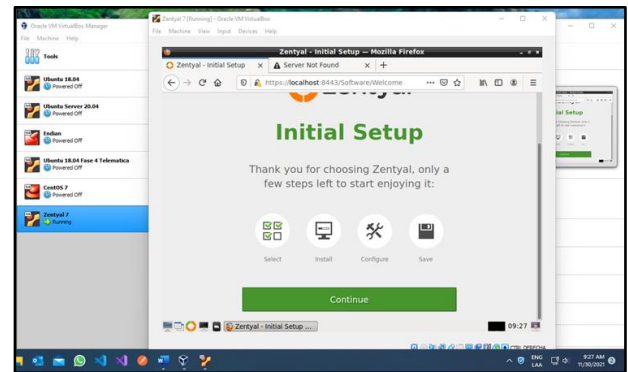


Figura 17. 3.1 - Configuración inicial.

Para la configuración del DHCP Server, DNS Server y Controlador de Dominio seleccionamos los roles del servidor a implementar:

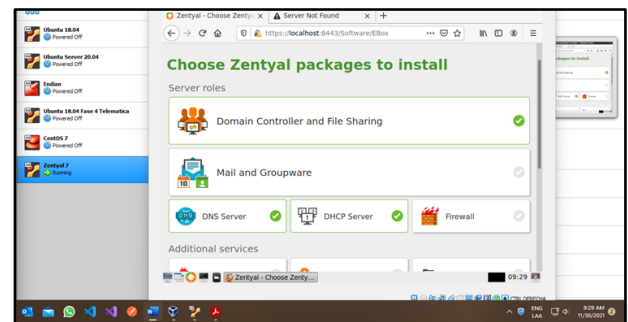


Figura 18. 3.1 - Selección servicios.

Seleccionamos la opción de instalar:

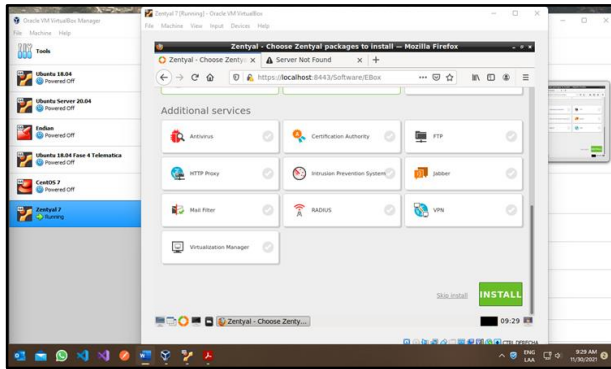


Figura 19. 3.1 -Instalar servicios.

Confirmamos los paquetes a instalar y damos clic en continuar:

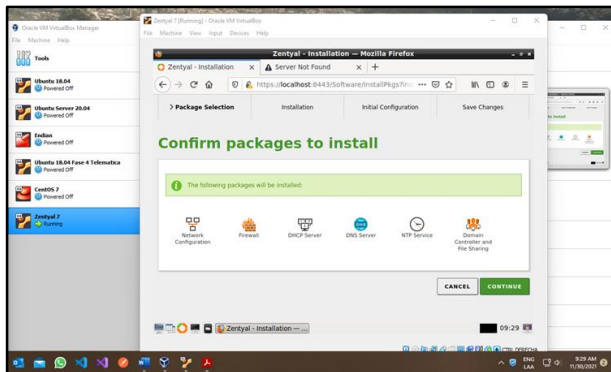


Figura 20. 3.1 - Confirmación instalación.

Definimos la NIC eth0 para nuestra red LAN (Modo red interna) y el eth1 para nuestra red WAN (Modo puente - NIC física):

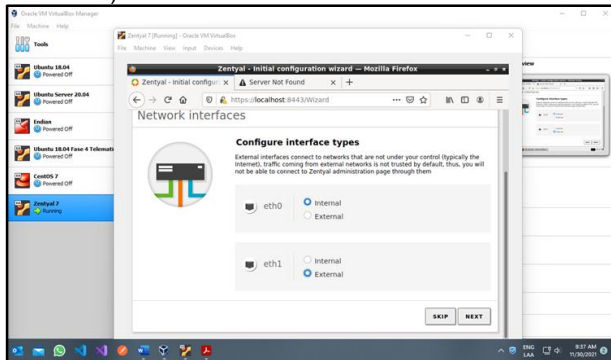


Figura 21. 3.1 - Configuración NIC.

Nuestro Eth0 hereda la configuración hecha durante la instalación, para nuestro eth1 usamos la IP 10.92.75.5:

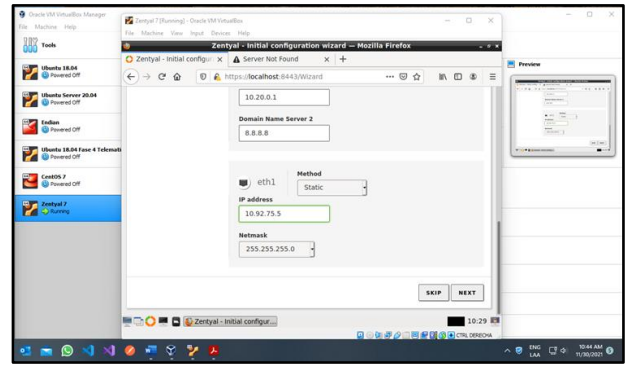


Figura 22. 3.1 - Configuración IPv4.

Configuramos nuestro servidor de dominio como único:

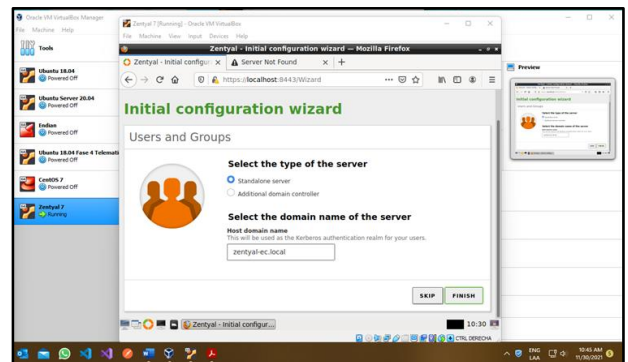


Figura 23. 3.1 - Configuración tipo servidor.

Actualizamos nuestro Zentyal con los últimos parches:

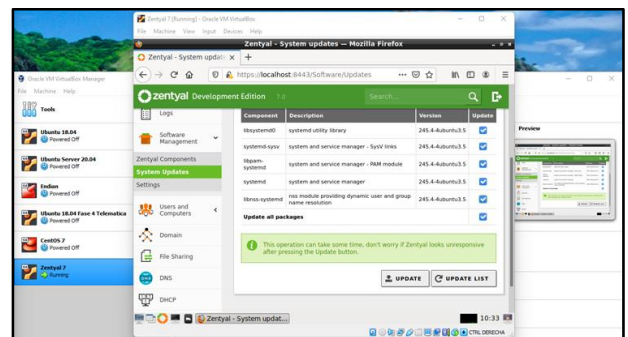


Figura 24. 3.1 - Instalación de parches.

En la configuración del DNS agregamos nuevamente la IP 8.8.8.8 para que los nombres de dominio no agregados a nuestro servidor sean resueltos por Google:

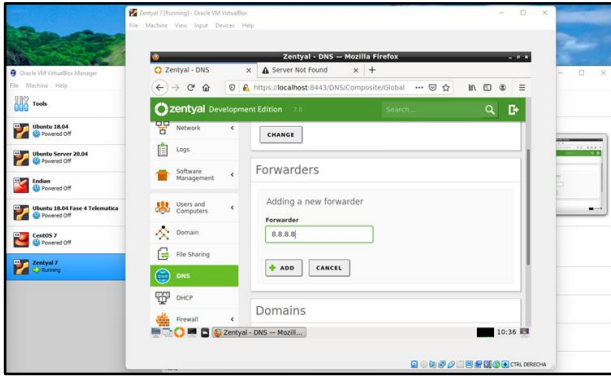


Figura 25. 3.1 - Configuración DNS.

Agregamos nuestro Gateway de nuestra red física, 10.92.75.1:

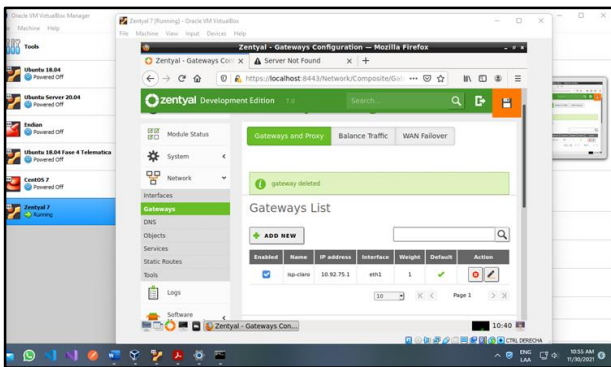


Figura 26. 3.1 - Configuración Gateway.

Agregamos nuestra lista de direcciones IP a asignar mediante DHCP en la interfaz eth0, solo dejaré 5 para este caso:

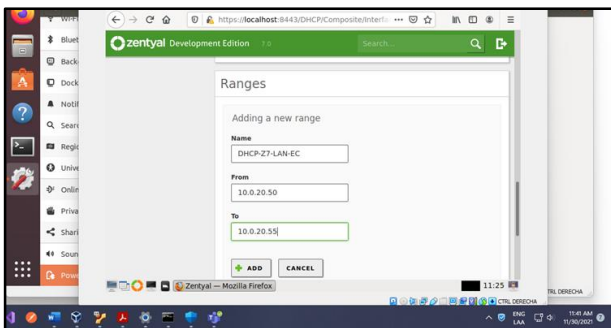


Figura 27. 3.1 - Configuración rango DHCP.

Y nos aseguramos de que el servicio DHCP esté habilitado desde el Module Status:

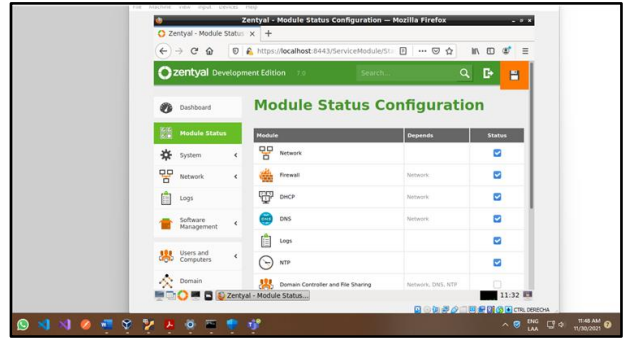


Figura 28. 3.1 - Habilitar servicio DHCP.

Ahora encendemos nuestra VM de Ubuntu Desktop 18.04 después de agregar su NIC a la red interna:

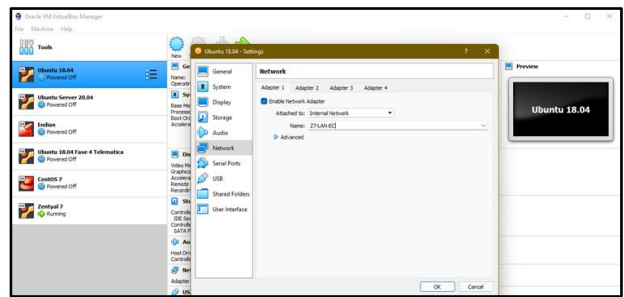


Figura 29. 3.1 - Configuración NIC VM Desktop.

Validamos que obtenga una IPv4 mediante DHCP:

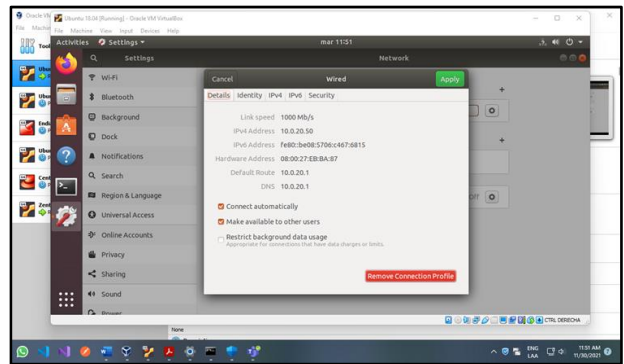


Figura 30. 3.1 - Validación cliente DHCP.

Verificamos del lado de Zentyal que haya asignado esa IP y con esto confirmamos que el servicio DHCP está configurado correctamente:

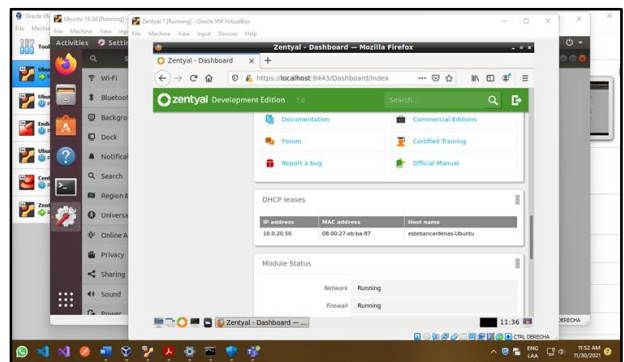


Figura 31. 3.1 - Validación servidor DHCP.

Para probar el DNS agregamos un registro y lo asociamos con la IP del Zentyal, en este caso agregaremos zentyal-ec.com como dominio:



Figura 32. 3.1 - Configuración DNS local. Agregamos el HostName "www" apuntando a la IP 10.0.20.1:

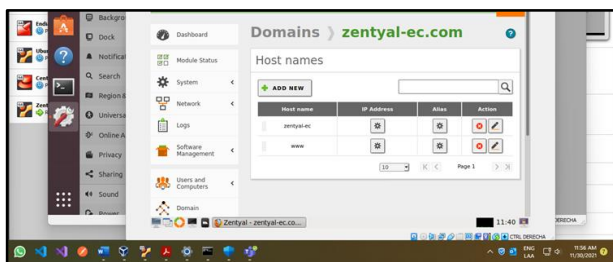


Figura 33. 3.1 - Configuración de hostnames DNS.

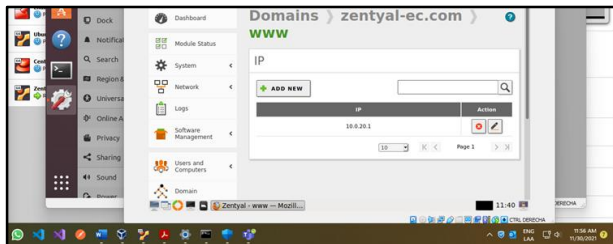


Figura 34. 3.1 - Configuración registro A DNS.

Desde nuestro Ubuntu Desktop abrimos la URL <https://www.zentyal-ec.com:8443> la cual debería funcionar para acceder a nuestro Zentyal desde la red LAN

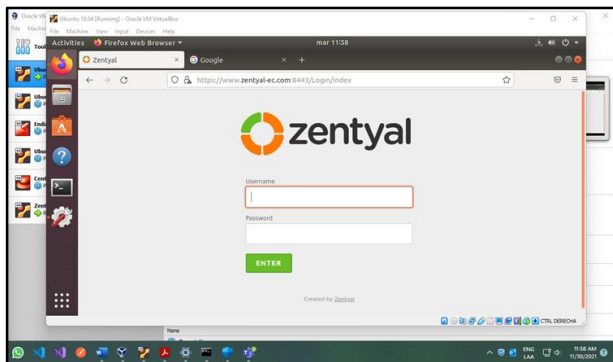


Figura 35. 3.1 - Validación funcionamiento DNS.

Vemos que funciona tanto el acceso a Zentyal como el servicio DNS.

Para el servicio de controlador de Dominio, primero vamos y cambiamos el nombre de nuestro NetBIOS domain name para que no sea igual al NetBIOS computer name dejándolo de esta forma:

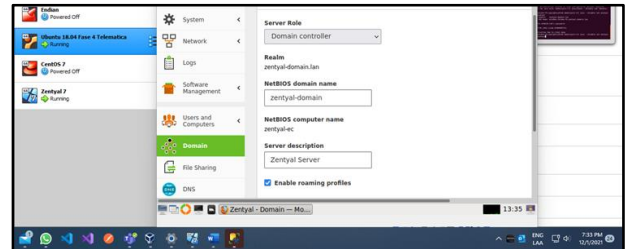


Figura 36. 3.1 - Configuración controlador de dominio. Vamos a Modules Status y habilitamos el servicio:

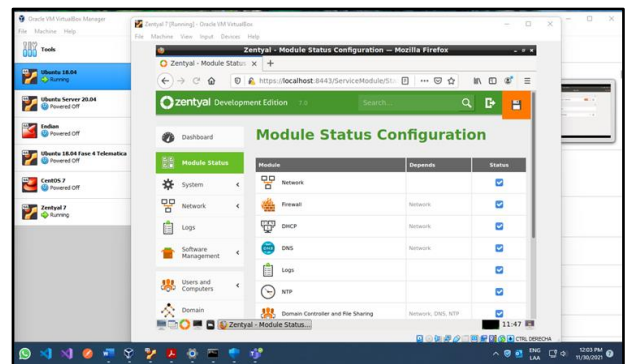


Figura 37. 3.1 - Habilitación controlador de dominio.

Creamos un usuario en el controlador de dominio para nuestro Ubuntu Desktop:

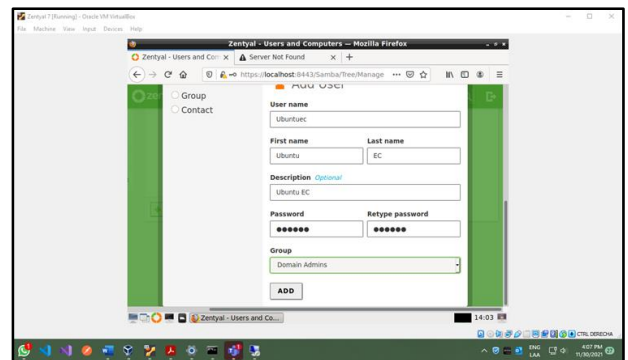


Figura 38. 3.1 - Creación usuario en controlador de dominio.

Habilitamos el PAM (Privileged Access Management):

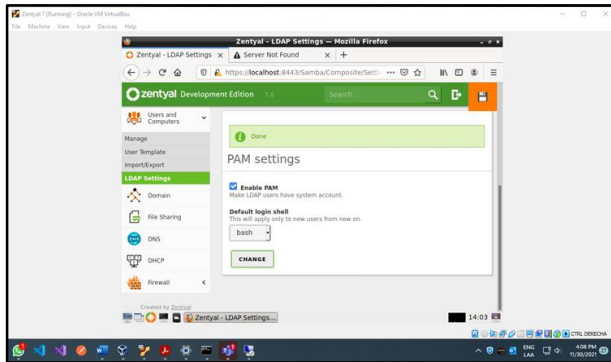


Figura 39. 3.1 - Configuración PAM.

Ahora vamos a nuestro Ubuntu Desktop e iniciamos el proceso para agregarlo a nuestro controlador de dominio, primero descargamos Power Broker open:

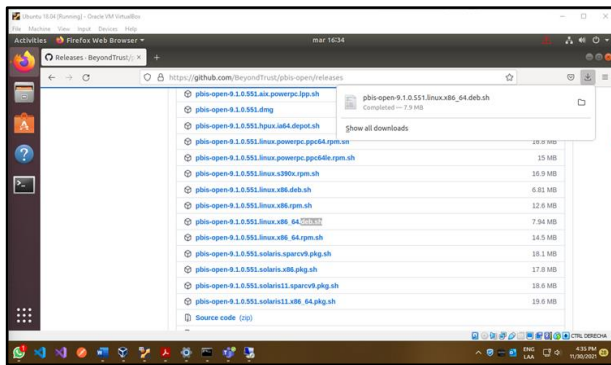


Figura 40. 3.1 - Descarga Power Broker open.

Damos los permisos de ejecución al archivo descargado y lo ejecutamos:

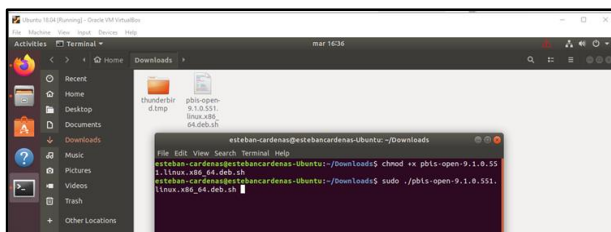


Figura 41. 3.1 - Instalación Power Broker open.

Corremos el comando que nos muestra al final de la instalación ajustando los parámetros

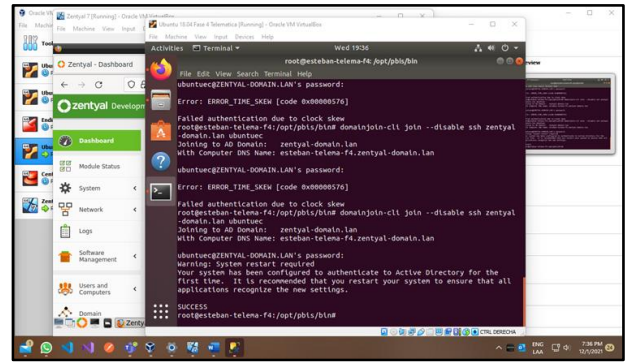


Figura 42. 3.1 - Conexión con el controlador de dominio desde VM desktop.

Después de haber reiniciado probamos iniciando con nuestro usuario del dominio:

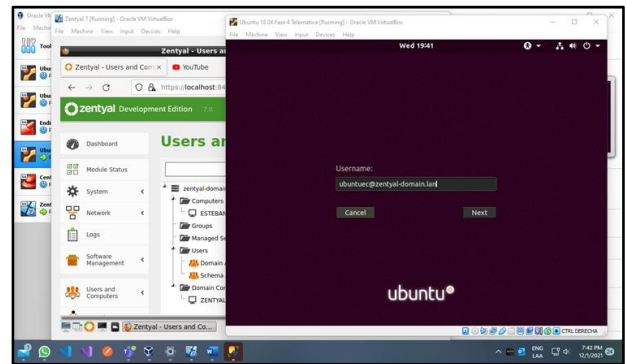


Figura 43. 3.1 - Prueba de acceso controlador de dominio.

Nuestro Ubuntu desktop inicia sin problemas y validamos que el equipo se haya registrado en el dominio del Zentyal:

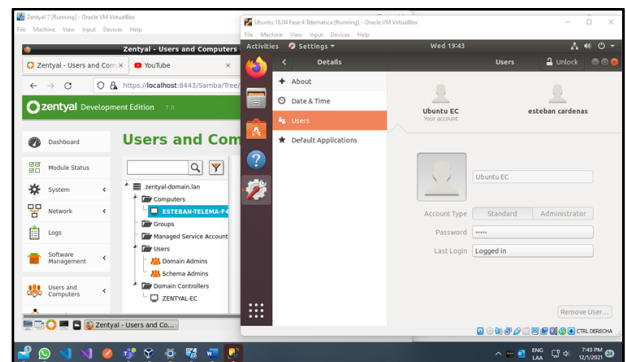


Figura 44. 3.1 - Validación de acceso controlador de dominio.

Con esto completamos el proceso donde se validó el funcionamiento del servicio DHCP, el servicio DNS y el servicio de controlador de dominio con una VM con Ubuntu 18.04 que hizo uso de estos en modo cliente.



### 3.2 PROXY NO TRANSPARENTE

Para realizar esta configuración, es necesario la comprensión de proxy transparente como el no transparente, un proxy no transparente requiere de una configuración en el equipo cliente, por lo que hace que el procedimiento más sencillo sea el del proxy transparente.

Como primera configuración añadimos un objeto en el módulo de red, se edita incluyendo la dirección del dispositivo que va a trabajar como proxy no transparente.

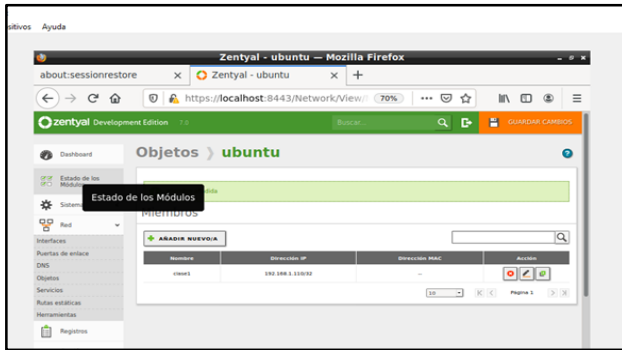


Figura 45. Inicio Máquina virtual

Configuramos el módulo de proxy HTTP, cambiamos el número de puerto por defecto (3128) al 1230, el cual es requerido en la guía de actividades.

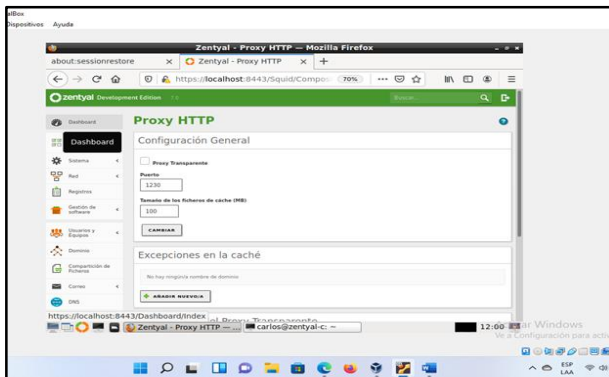


Figura 46. Inicio Máquina virtual

Se configura la regla del proxy, para que sea denegada la conexión en el periodo de tiempo deseado, y agregamos el objeto creado anteriormente

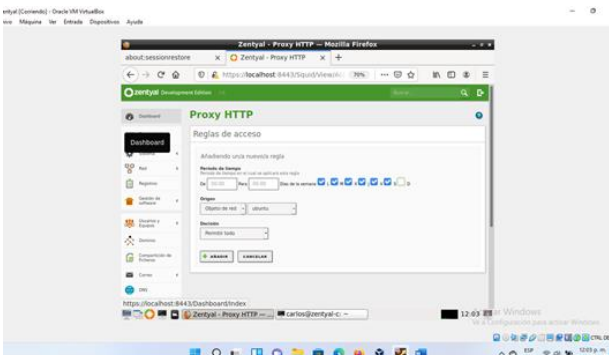


Figura 47. Inicio Máquina virtual.

Para evidenciar los resultados, ingresamos al navegador de ubuntu, luego a opciones del navegador, ahí aplicamos el proxy manualmente y agregamos los datos en los pasos anteriores.

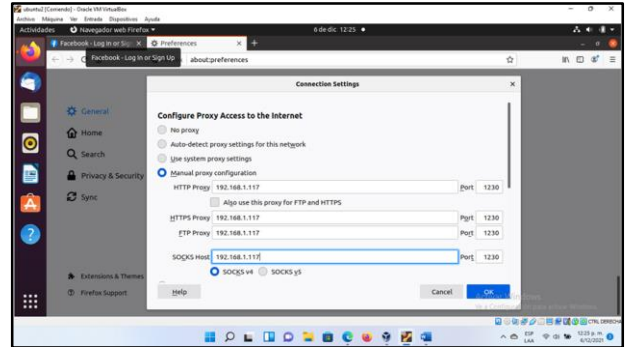


Figura 48. Inicio Máquina virtual

Para este ejemplo el cliente ubuntu ya cuenta con internet, no obstante, al tratar de acceder a las páginas que normalmente cualquier persona interactúa, el sistema no lo permite, podemos confirmar que la configuración de las restricciones del proxy está funcionando adecuadamente.

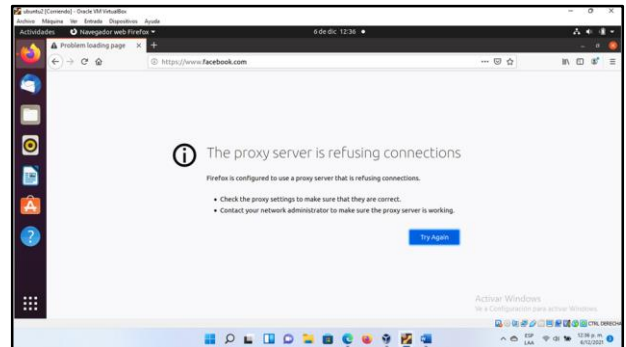


Figura 49. Inicio Máquina virtual

### 3.3 CORTAFUEGOS

¿Qué es un cortafuego? Un cortafuegos o firewall es un sistema que previene el uso y el acceso desautorizados a tu ordenador.

Los cortafuegos pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente intranets.

Todos los mensajes que entran o salen de la Intranet pasan a través del cortafuego, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.

#### Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreo.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.



Figura 50. Validación usuario

Se seleccionan algunos servicios necesarios y que pueden ser útiles más adelante para el desarrollo de cada temática dependiendo de la necesidad. Se presiona el botón "Instalar".

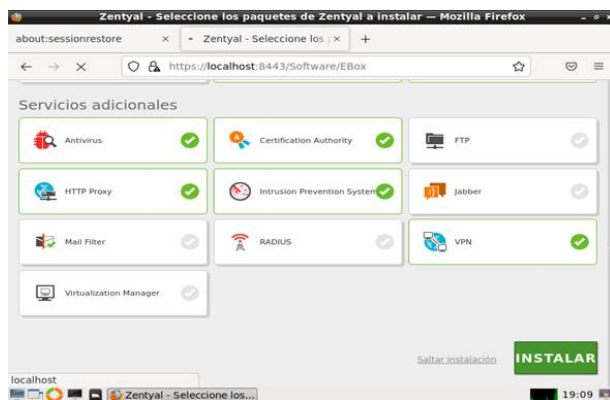


Figura 51. Paquetes necesarios para su instalación



Figura 52. Inicio Máquina virtual  
Luego de realizar la configuración anterior y guardar los cambios, se ingresa a la interfaz principal, mostrando datos técnicos de la aplicación.

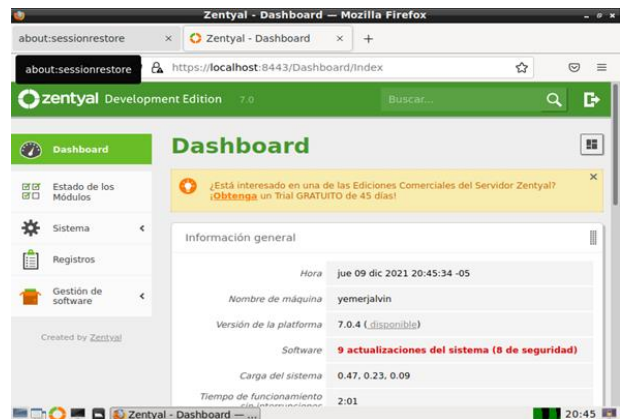


Figura 53. Dashboard Zentyal.

Se configuran las interfaces de red: eth0 como externa (WAN) por DHCP

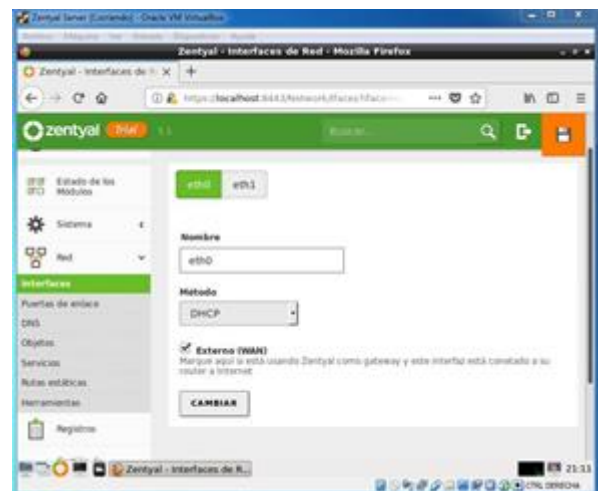


Figura 54. Configuración de interfaz eth0

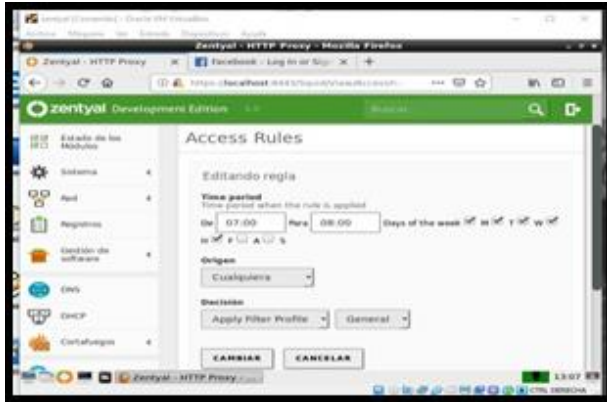


Figura 55 Configuración de interfaz eth1.

Se configura en Zentyal el filtrado de paquetes en el cortafuego para las redes internas.



Figura 56. Configuramos la regla del cortafuego en Reglas de filtrado para redes internas.

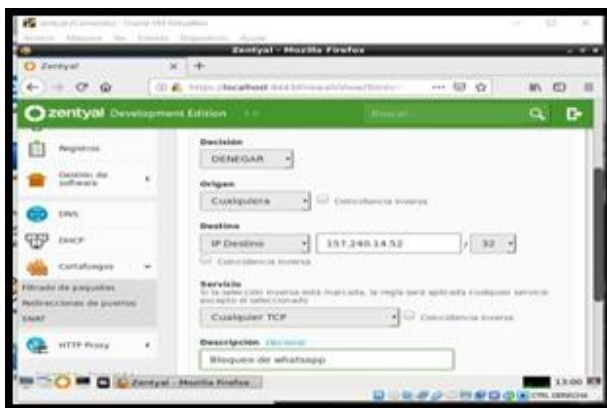


Figura 57. Se crean las reglas para denegar el acceso a redes sociales (Facebook, Instagram y WhatsApp)

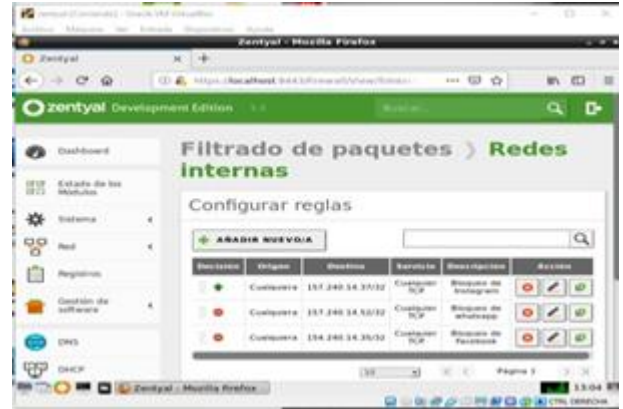


Figura 58. Reglas creadas

**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.



Figura 59. Antes de la Regla



Figura 60. Después de la regla.

### 3.3 FILE SERVER Y PRINT SERVER

Interfaces de red.

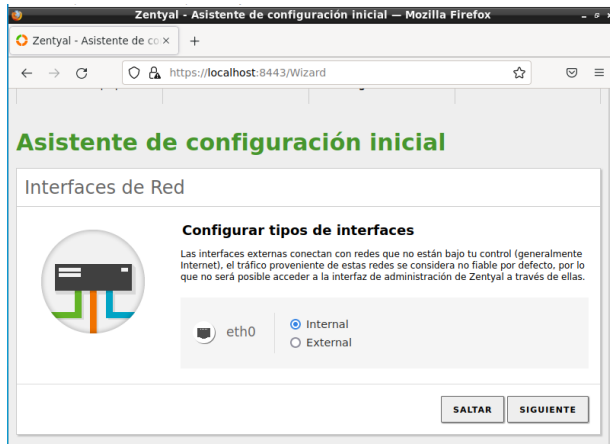


Figura 61.FS y PS interfaces de red.

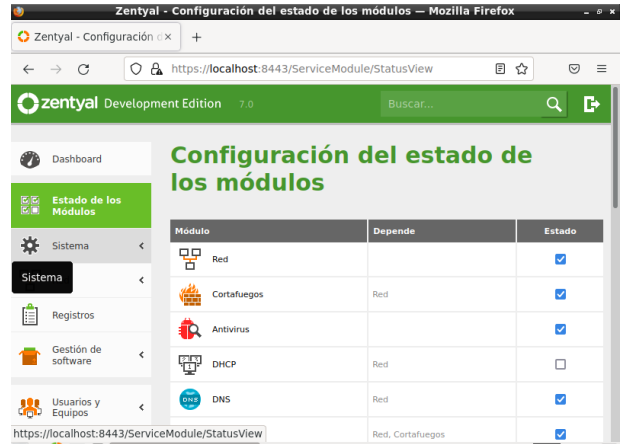


Figura 64. FS y PS módulos.

Configuración de puertas de enlace. Dominio de búsqueda.

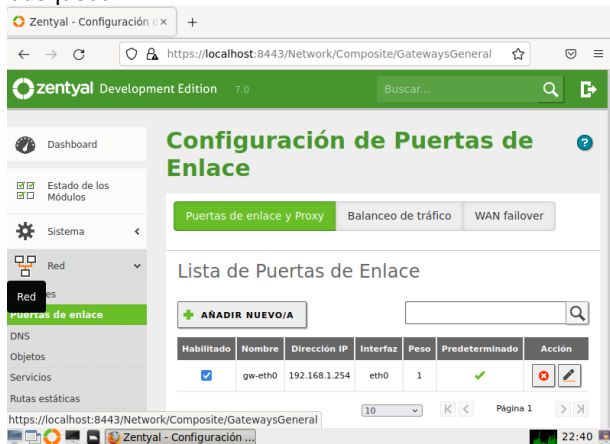


Figura 62. FS y PS puertas de enlace.

Sección de usuarios y equipos.

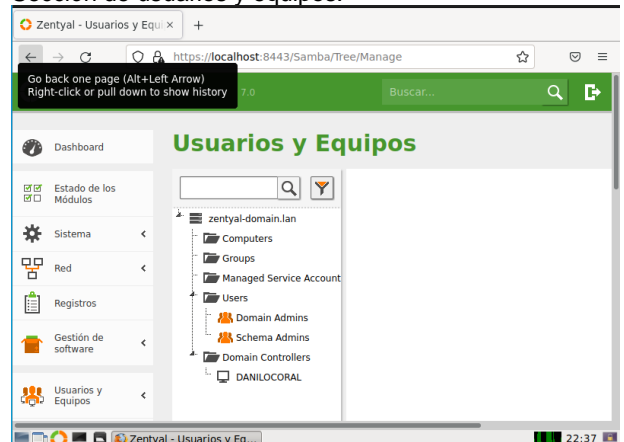


Figura 65. FS y PS usuarios equipos.

Certificación.

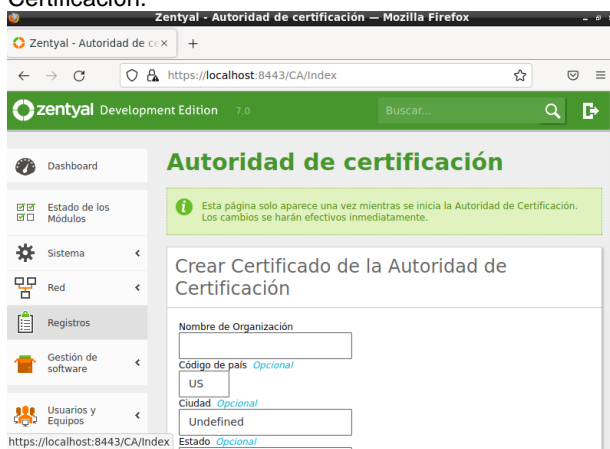


Figura 63. FS y PS certificación.

Creación de grupos.



Figura 66. FS y PS grupos.

Grupo de administración creado. Propiedades y configuración del usuario administrador.

Configuración de módulos.

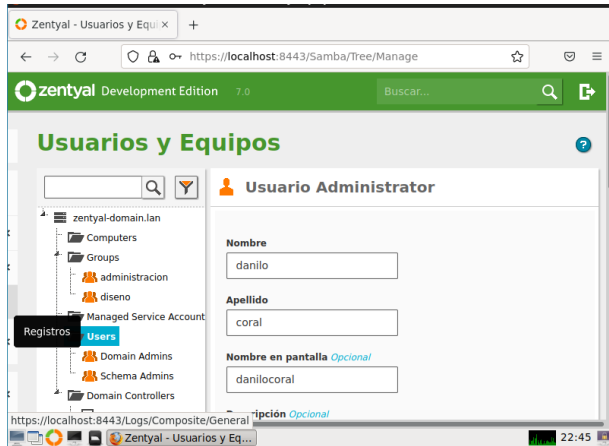


Figura 67. FS y PS nuevo usuario.

Creación de un nuevo usuario (jdc), asignado al grupo administración.

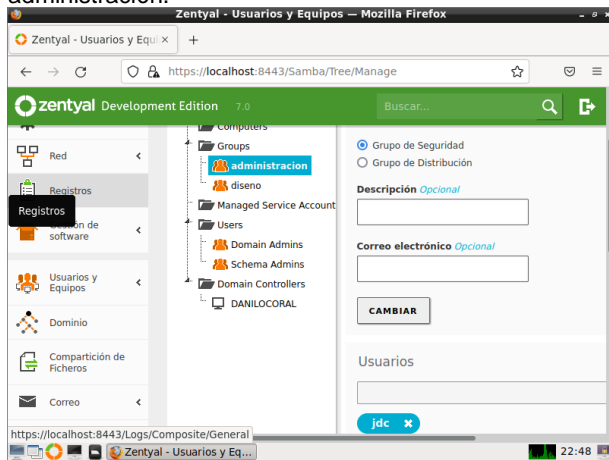


Figura 68. FS y PS agregar usuario a grupo.

Configuramos el rango en DHCP-

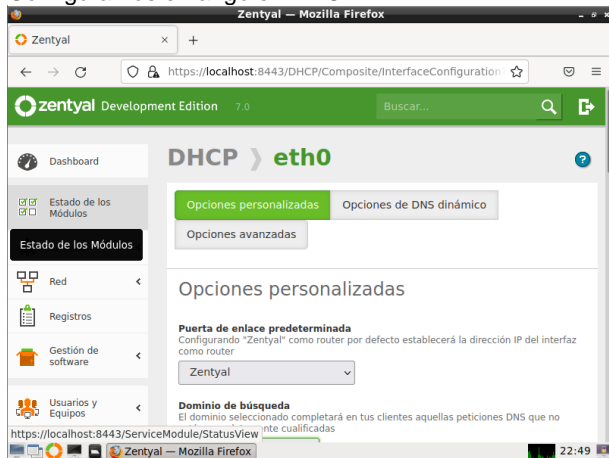


Figura 69. FS y PS rango dhcp.

Creación de un fichero para ser compartido.

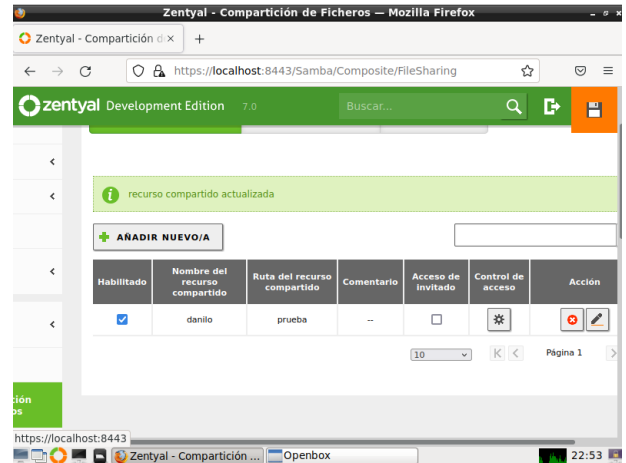


Figura 70. FS y PS fichero.

Ficheros creados, para ser compartidos.

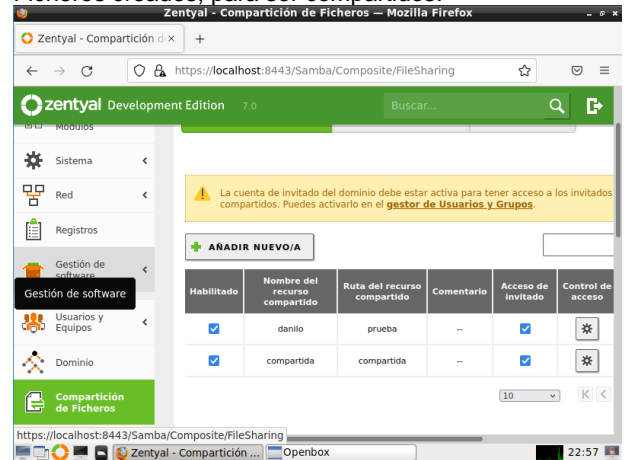


Figura 71. FS y PS compartir ficheros.

Damos clic en añadir para Configurar el fichero prueba.

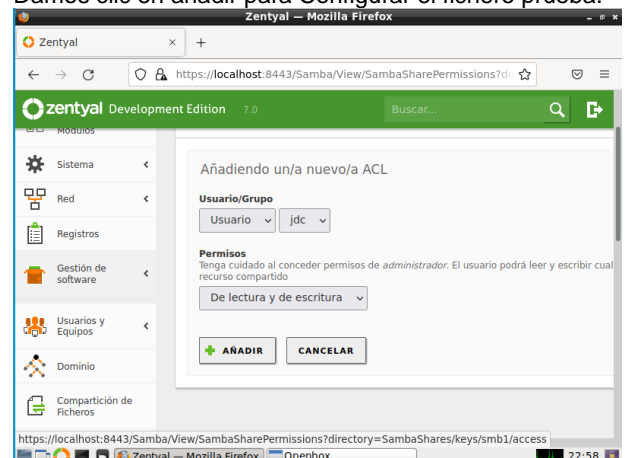


Figura 72. FS y PS añadir ficheros.

Propiedades y control del fichero prueba.

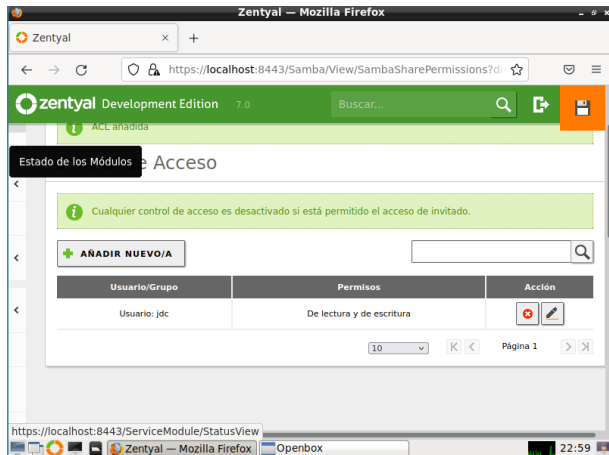


Figura 73. FS y PS fichero prueba.

Guardando cambios.

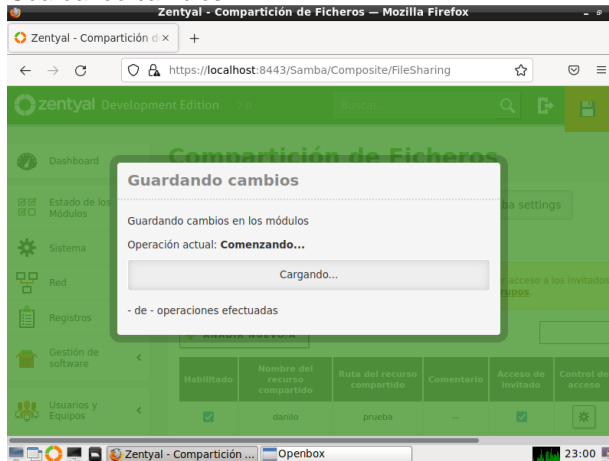


Figura 74. FS y PS guardan cambios.

Ingresamos al archivo resolv.conf, para modificar la ip de acceso.

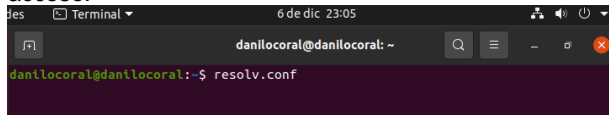


Figura 75. FS y PS resolvconf.

Agregamos la ip de nuestro servidor.

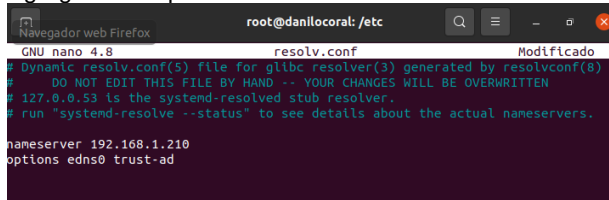


Figura 76. FS y PS ip servidor.

Instalamos en Ubuntu unas aplicaciones que nos permitirán crear el enlace. Likewise open, Likewise open gui y lidglade.

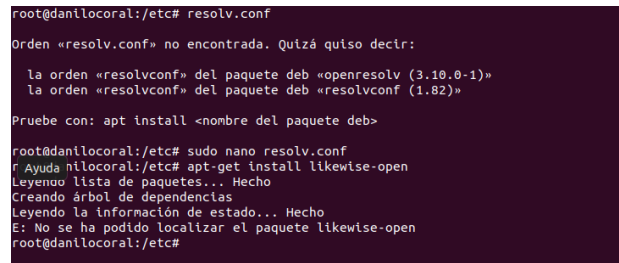


Figura 77. FS y PS instalar en ubuntu.

Con el comando sudo domainjoin-gui abrimos Active Directory Membership, para la conexión. La aplicación reconoce el nombre de la máquina, agregamos el dominio.



Figura 78. FS y PS agregar dominio.

Nos autenticamos con el usuario de zentyal.



Figura 79. FS y PS autenticación.

### 3.4 VPN

Para la implementación y uso de VPN generadas por medio del Zentyal, vamos a iniciar creando un certificado para nuestro servidor así tal como se muestra en la Figura 80, ingresando al menú de **Autoridad de Certificación**:

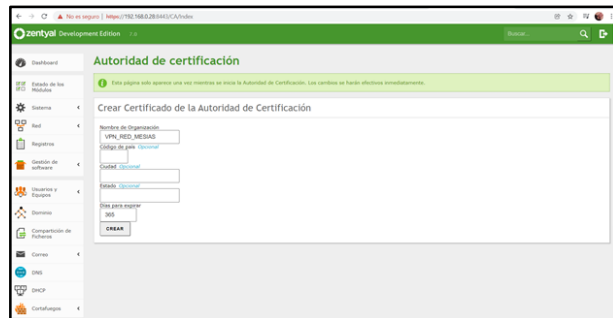


Figura 80. Autoridad y certificación

Después de ingresar el nombre de la organización damos click en crear y nos aparecerá la lista de certificados como se observa en la Figura 81:

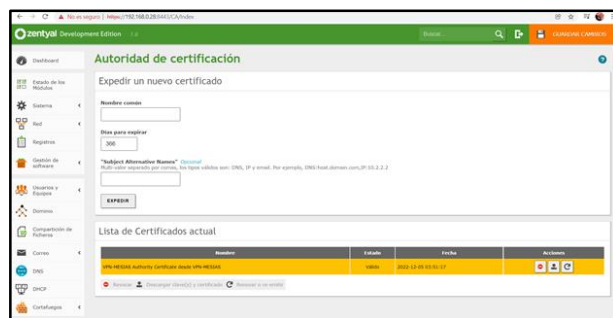


Figura 81. Lista de Certificación actual

Ahora nos dirigimos al menú **VPN > Servidores** y damos click en **Añadir Nuevo**, tal cual la Figura 82:



Figura 82. Lista de Servidores

Luego ingresamos un nombre al servidor y damos click en **Añadir** como en la Figura 83:



Figura 83. Añadiendo servidor

Al lado derecho superior vamos a dar click al botón que dice **Guardar Cambios**, tal cual se observa en la Figura 84:

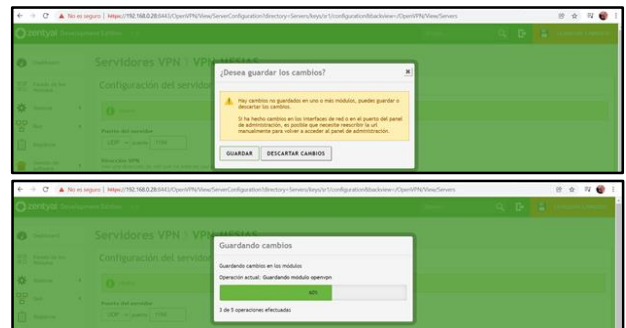


Figura 84. Guardando Cambios

Ahora nos dirigimos a las configuraciones del nuevo servidor que se acabó de crear y habilitamos ciertos permisos para que nuestra VPN tenga acceso a nuestra red, ver en la Figura 85:

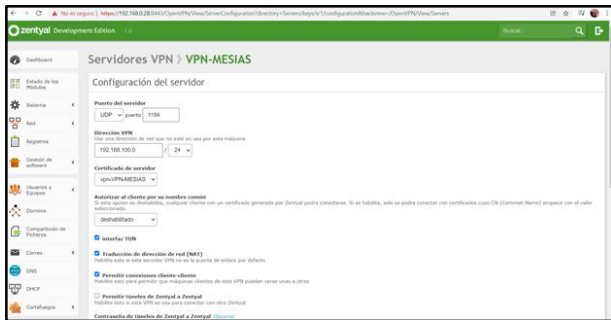


Figura 85. Configuración Servidor

Le damos click en el botón **cambiar** al finalizar de modificar nuestras configuraciones y por ultimo damos click en **guardar cambios**, ver en la Figura 86:



Figura 86. Guardando Configuración Servidor

Ya aquí, vamos a descargar el paquete de configuración del cliente para poder instalarlo en dicha máquina, ver en la Figura 87:

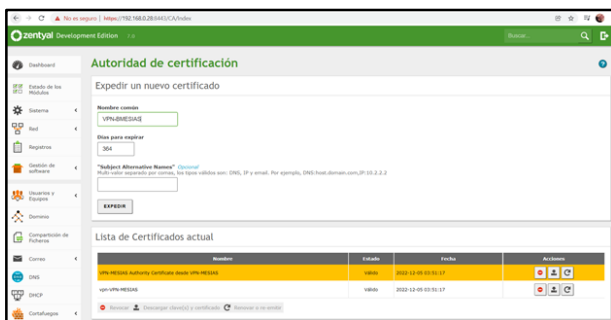


Figura 87. Lista Certificados Actual

Una vez creado nuestro servidor vamos a colocar la ip del Zentyal para posteriormente descargar el certificado para el cliente, ver en la Figura 88:

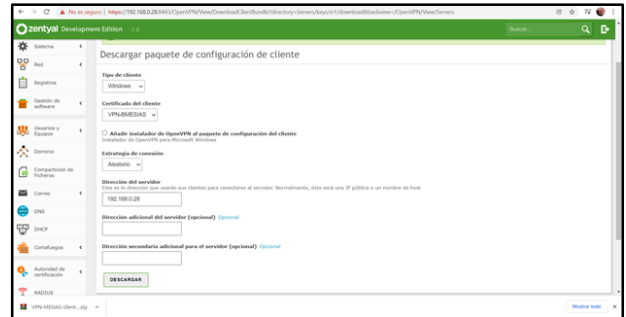


Figura 88. Descargar Certificado

Una vez descargado nuestro certificado vamos a descargar en la máquina Windows del cliente el programa llamado OpenVPN: <https://openvpn.net/client-connect-vpn-for-windows/>, ver en la Figura 89



Figura 89. Setup OpenVPN

Damos click en siguiente, luego aceptamos los términos de licencia y por ultimo damos click en install, ver en la Figura 90:

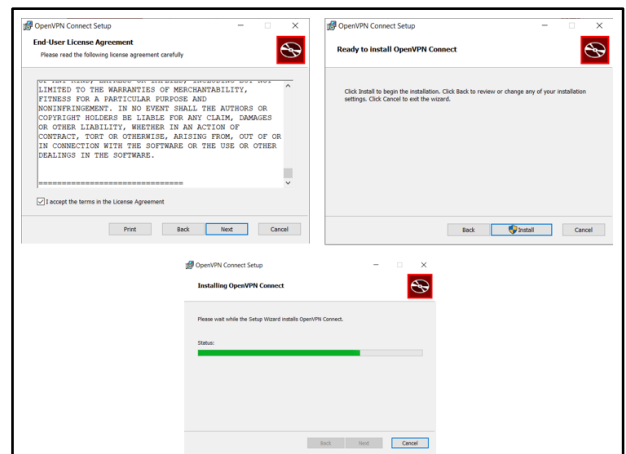




Figura 90. Setup OpenVPN

Y tenemos ya instalada la aplicación donde importamos el certificado que generamos anteriormente, ver en la Figura 91:

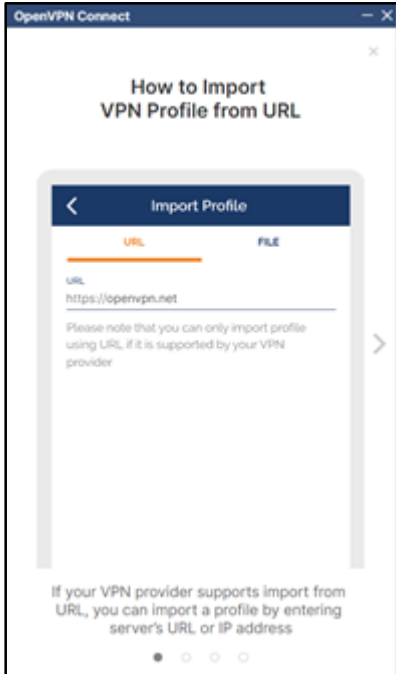


Figura 91. Inicio OpenVPN

Luego vamos a dirigirnos a la pestaña que dice **FILE**, y con ello nos permitirá importar el archivo del certificado de la VPN, ver en la Figura 92:

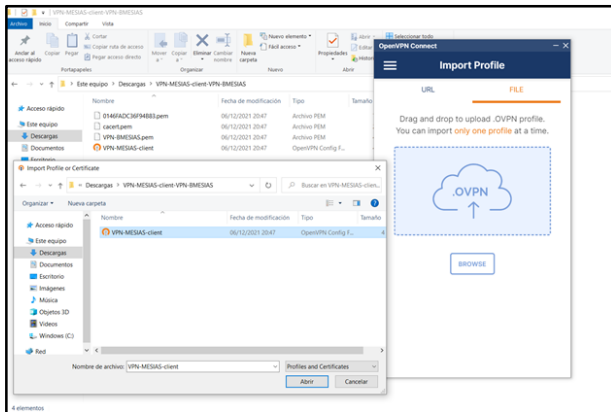


Figura 92. Importación OpenVPN

Al importarlo nos cargará la ip de nuestro servidor Zentyal por defecto y luego daremos click en **connect**, donde nos mostrará el status de la conexión, ver en la Figura 93:

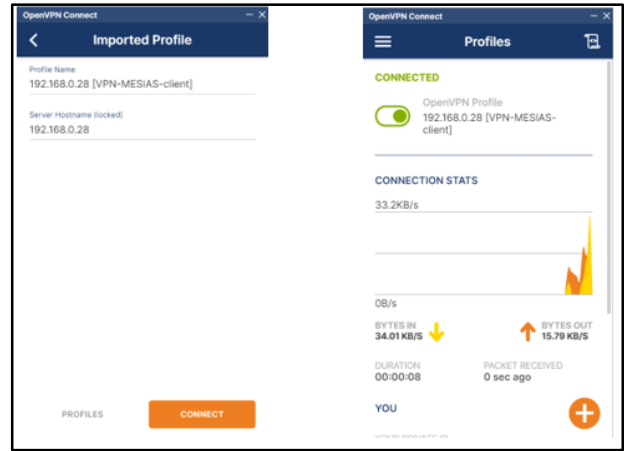


Figura 93. Conexión a VPN

Para validar la conexión y ver la ip que hemos asignado previamente a la VPN creada desde el Zentyal deberá estar en el rango **192.168.100.X** y se le podrá hacer ping a nuestra puerta de enlace, ver en la Figura 94.



Figura 94. Test conexión a VPN

## 4 CONCLUSIONES:

Es muy interesante poder conocer herramientas como Zentyal, recuerdo que hace unos años estuve en una empresa que la utilizaba y no tenía idea alguna de que era y de sus funcionalidades, teniendo en cuenta que la meta de todas las empresas en general es generar las mayores utilidades posibles, es muy común que se busque ahorrar costo en todos los aspectos posibles, esa fue la razón por la cual dicha empresa usaba esta herramienta, sin embargo, gracias al proceso realizado en el presente documento, es posible comprender de que por ser una herramienta que no necesariamente requiere licenciamiento no quiere decir que sea limitada, por el contrario, la administración e implementación de soluciones para la infraestructura tecnológica es muy práctica, sencilla y de fácil escalabilidad.

Así mismo, Zentyal Server nos brindará la facilidad de administrar todos los servicios básicos de la infraestructura de red, lo cual nos ayuda a tener un acceso seguro y fiable a internet. Es muy importante tener en cuenta que al permitirnos filtrar páginas web en base a su contenido garantiza un acceso de calidad a la información, también cabe mencionar que es posible definir múltiples perfiles de filtrado en proxy HTTP definiendo criterios que se ajusten a nuestras necesidades.

La versión más reciente de Zentyal no cuenta con un módulo de impresoras, lo que hace un poco más complicada la tarea de habilitar el control de acceso de las impresoras, sin embargo, se logró por medio de del archivo de configuración de samba realizar estas indicaciones y con muy pocas líneas.

Gracias a la facilidad en configuración y diferentes funcionalidades que ofrece Zentyal, resulta ser una gran alternativa para definir la infraestructura organizativa de una empresa, creando los usuarios y asignando sus usuarios respectivos, además de compartir espacios de trabajos y dispositivos.

Una vez puesto en marcha el servidor con la distribución de Zentyal server en la versión 6.2 y el proporcionamiento de servicios como DHCP y DNS de manera satisfactoria. Se implementa el servicio de compartición de ficheros a usuarios configurados en el dominio de Zentyal. Esta última parte requiere de instalación de los paquetes PowerBroker Identity Services los cuales permitieron la adición de las máquinas clientes al dominio y así mediante LDAP realizar la comprobación de los servicios puestos en marcha.

El configurar Zentyal para dar soporte a clientes remotos (conocidos como Road Warriors). Esto es, un servidor Zentyal trabajando como puerta de enlace y como servidor VPN, que tiene varias redes de área local (LAN) detrás, permitiendo a clientes externos (los road warriors) conectarse a dichas redes locales vía servicio VPN y que finalmente, al establecer este tipo de conexiones garantizamos un nivel de seguridad en nuestra red LAN de alta seguridad

## 5 REFERENCIAS

- [1] Z. 6. Documentation, «doc.zentyal.org,» [En línea]. Available: <https://doc.zentyal.org/en/firewall.html>. [Último acceso: 11 12 2019].
- [2] Zentyal. (2018). Zentyal Server Recuperado de: <http://www.zentyal.org/server/>.
- [3] Primeros pasos con Zentyal Recuperado de <https://doc.zentyal.org/es/firststeps.html>
- [4] Solución Zentyal Recuperado de <https://es.wikipedia.org/wiki/Zentyal>
- [5] Zentyal Server Instalación y primeros pasos Recuperado de [https://www.youtube.com/watch?v=tG\\_NHAUYUbU](https://www.youtube.com/watch?v=tG_NHAUYUbU).
- [6] Tutoriales Servidor Zentyal (español) Recuperado de <https://www.youtube.com/user/zentyalControl>
- [7] Zentyal Página oficial Disponible en: <https://zentyal.com/es/inicio>