SOLUCIÓN DE NECESIDADES ESPECÍFICAS CON GNU/LINUX.

Yessid Aramis Cáceres Vásquez
e-mail: yecava1785@gmail.com
Oscar Mauricio Rozo Mora
e-mail: mauricio23122006@gmail.com
Álvaro Moncada Portuguez
e-mail: Alvaro.moncadap@hotmail.com
Jonathan López López
e-mail: jlopezlope@unadvirtual.edu.co
Miguel A. Sanchez Barreto
e-mail: masanchezb@unadvirtual.edu.co

RESUMEN: *Este documento contiene los procedimientos para la instalación, configuración y administración de los siguientes servicios: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos o Firewall, File Server y Print Server y VPN. Todos ellos instalados bajo la plataforma de Linux Zentyal 6.42. Podemos observar, que los procedimientos no solo son explicados teóricamente ya que se realizaron en las dos modalidades, teórico-práctico como se evidencia a través de las imágenes que cada uno aportó y tomó al momento de realizar la práctica o ejercicio de cada uno de los procedimientos.*

PALABRAS CLAVE: DHCP, Dominio, Firewall y Proxy.

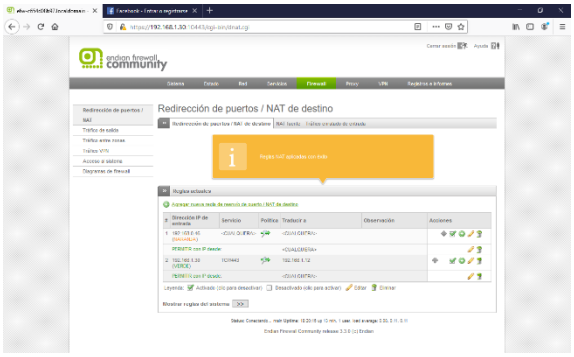
1 INTRODUCCIÓN

Esta guía incluye los procedimientos completos para la instalación, configuración y puesta en marcha de una infraestructura tecnológica que permita dar respuesta a los requerimientos específicos ya sea de nuestra empresa o de un cliente.

2 DESARROLLOS DE CONTENIDOS

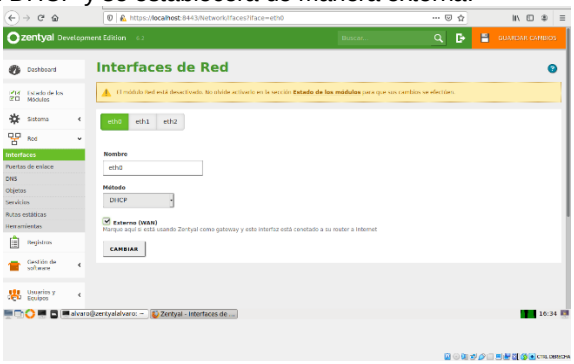
2.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Configuramos la zona DNZ con la ip de zentyal

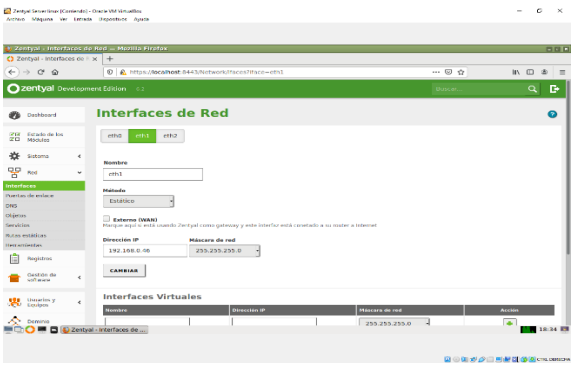


Iniciamos con la descarga de paquetes seleccionando los paquetes

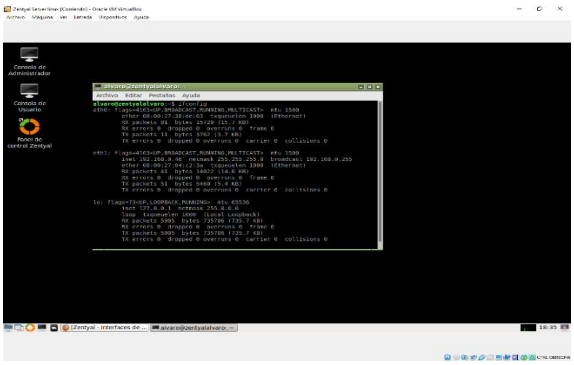
Una vez se instalen los paquetes se procedera con la configuración de la red eth0 y eth1 eth0 se configurará el DHCP y se establecerá de manera externa.



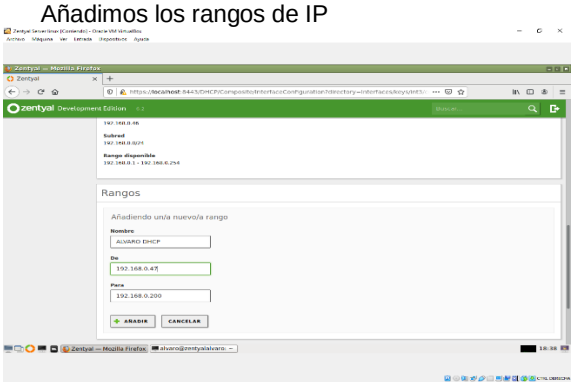
eth1 asignaremos la configuración estática e interna y se la dirección IP ya configurada.



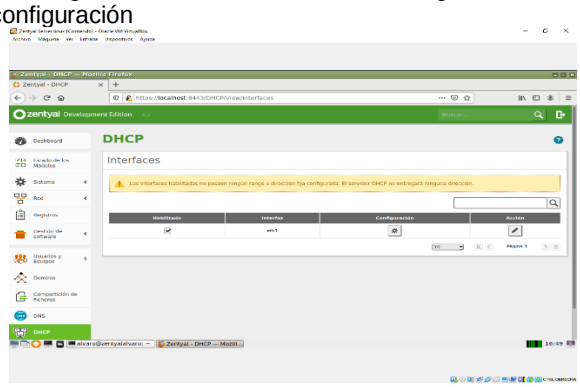
Verificamos en la terminal que los cambios se hayan efectuado.



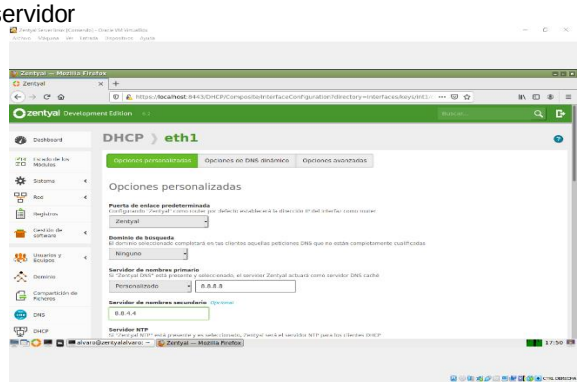
Añadimos los rangos de IP



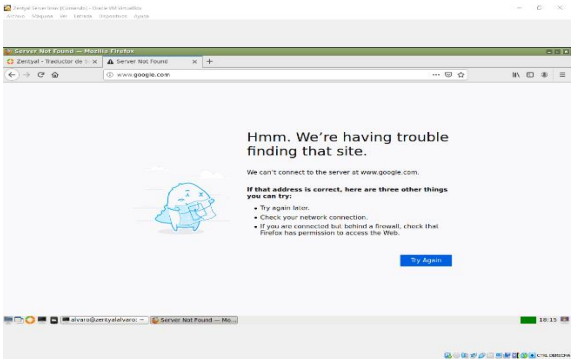
regresamos al módulo DHCP e ingresamos a la configuración



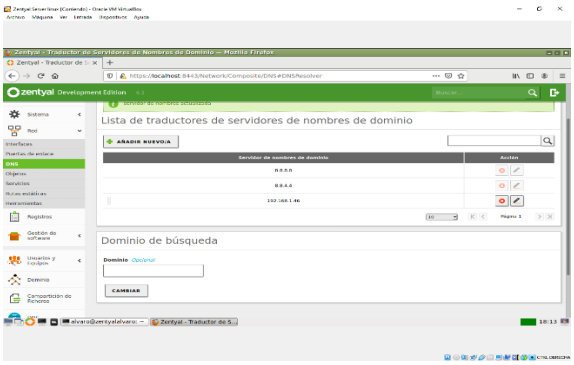
Y configuramos el DHCP agregando las entradas al servidor



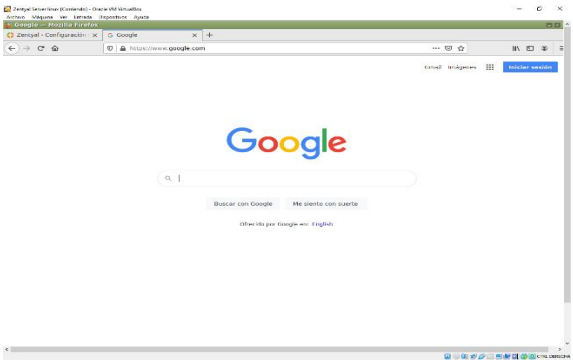
Una vez realizada esta parte procedemos a configurar el DNS y añadimos nuestra dirección ip Verificamos el ingreso a Google.com para resolver nuestro DNS



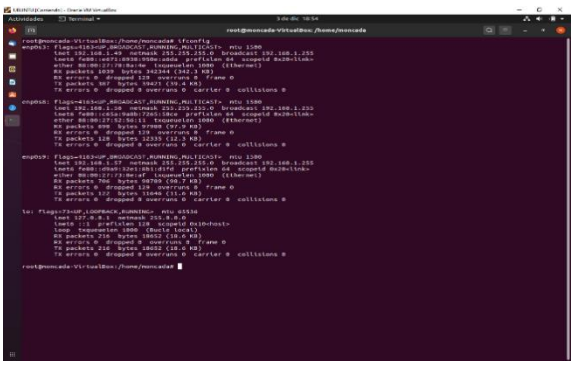
Una vez realizado los cambios validamos que el conflicto se haya resulto ingresando



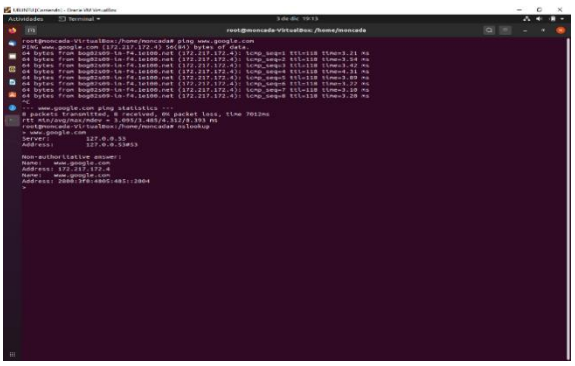
ingresando nuevamente a Google.com para verificar que el conflicto se haya solucionado



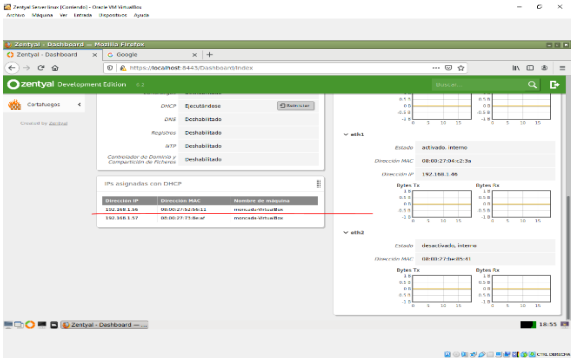
Para conocer la vemos la información de nuestra RED y cuál fue la IP nos asignó nuestro servidor vamos a ver si estamos conectados en Zentyal en Ubuntu desktop Para ello ingresamos el comando ifconfig



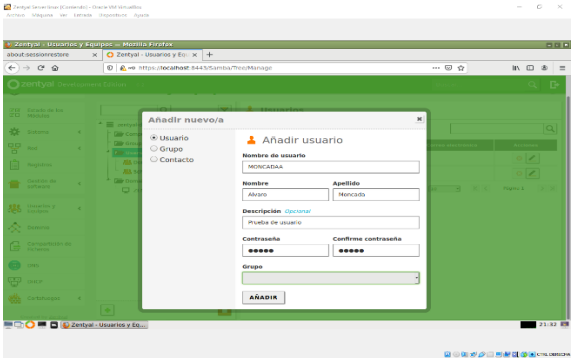
Vamos al servidor y verificamos que el cliente esté conectado



Procedemos a gestionar el usuario, activamos nuestro control de dominio. Para crear el usuario vamos a user y damos clic en agregar

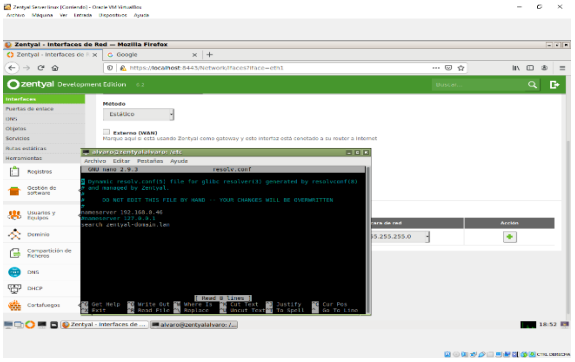


Ya se ha verificado la conexión entre el cliente y servidor se validará que tenga conexión a internet haciendo ping a la dirección www.google.com

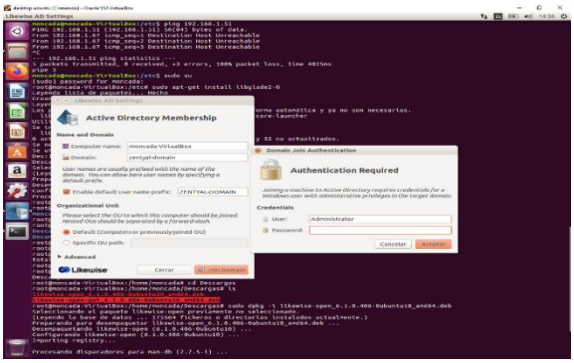


Vamos al directorio raíz i configuramos nuestra dirección IP del servidor

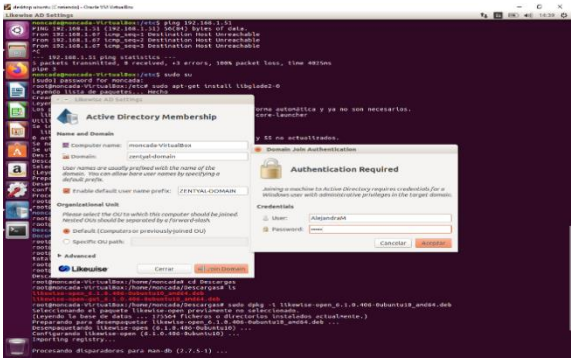
Confirmarnos nuestro servidor DNS que está operando

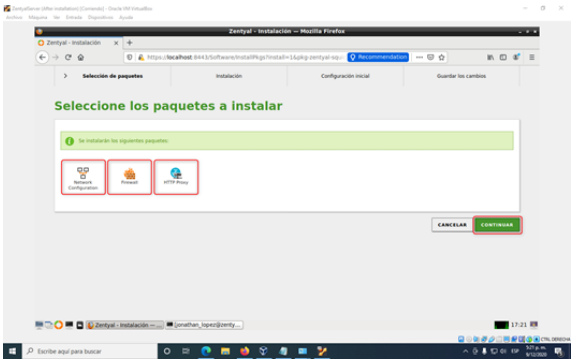


Cambiamos los valores e ingresamos la IP Ingresamos a la carpeta donde se ubican los instaladores Procedemos con la instalación Ingresamos al directorio activo

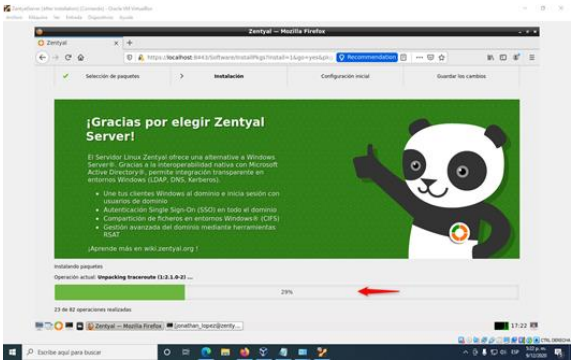


E ingresamos el usuario para comprobar



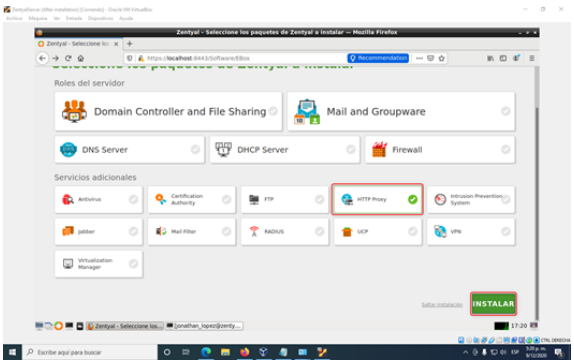


Comienza la instalación, podemos ver el % de progreso



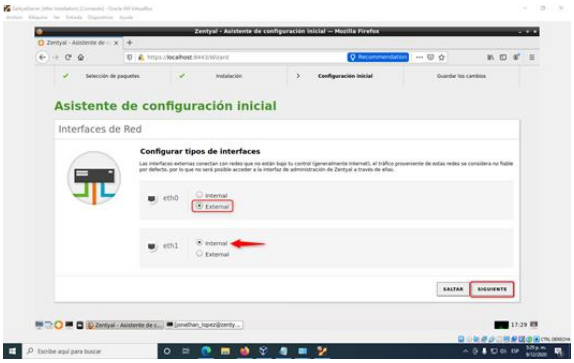
2.2 PROXY NO TRANSPARENTE

Seleccionamos el rol HTTP Proxy para su instalación

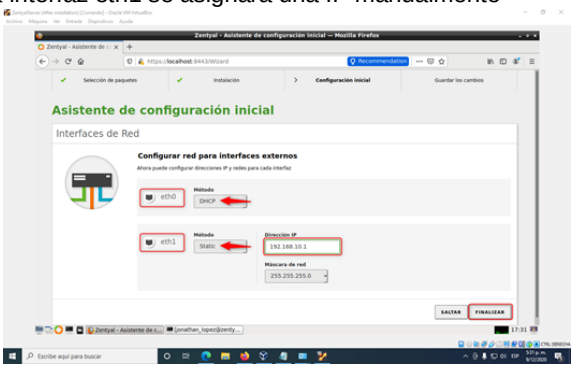


Se nos instalará por defecto los paquetes Network Configuration, Firewall y HTTP proxy

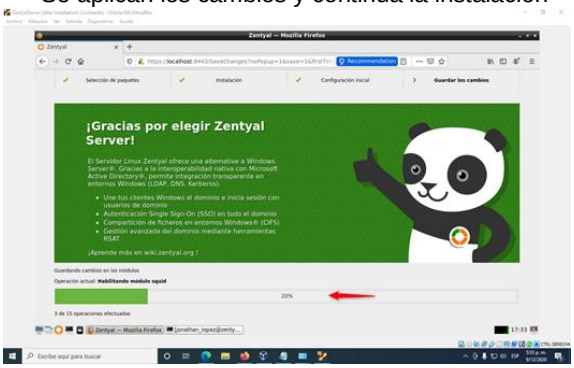
En medio de la instalación del rol configuramos la interfaz eth0 como “External” y la eth1 como “Internal” para cada una de nuestras zonas



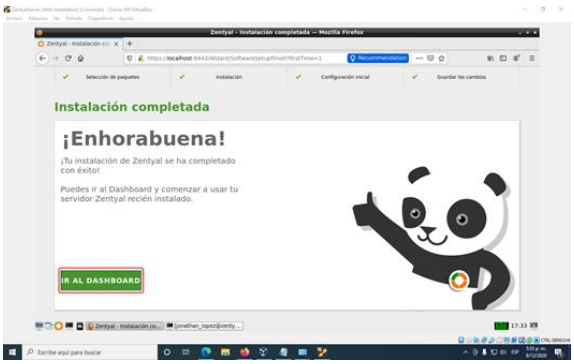
La interfaz eth0 obtendrá su IP mediante DHCP. A la interfaz eth1 se asignará una IP manualmente



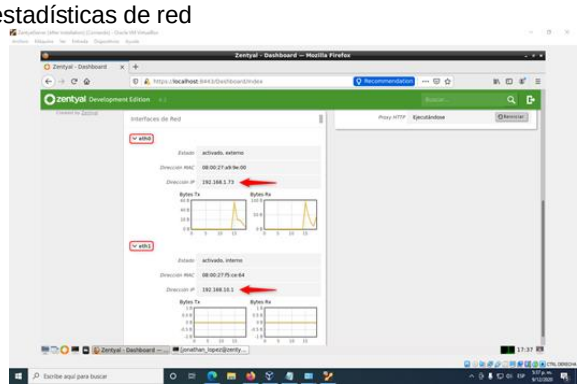
Se aplican los cambios y continua la instalación



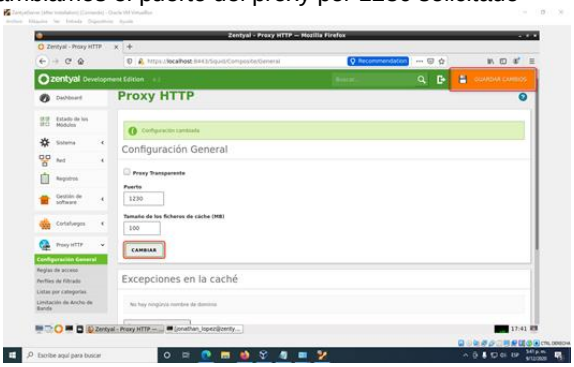
Nos confirma la correcta instalación



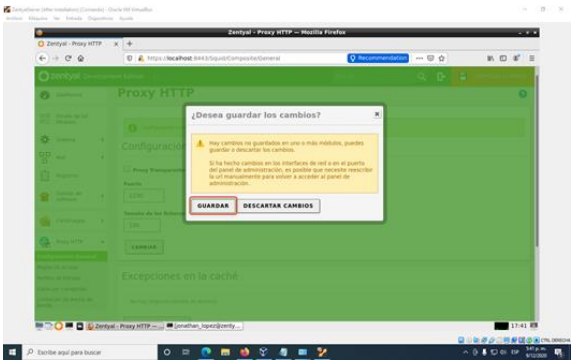
En el Dashboard podemos ver la configuración y estadísticas de red



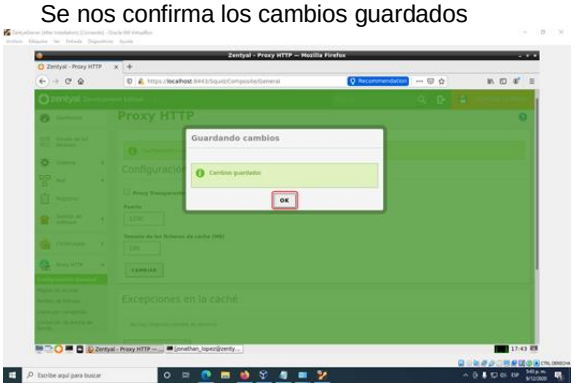
En el Dashboard en la sección Proxy HTTP ingresamos a configuración general, una vez allí cambiamos el puerto del proxy por 1230 solicitado



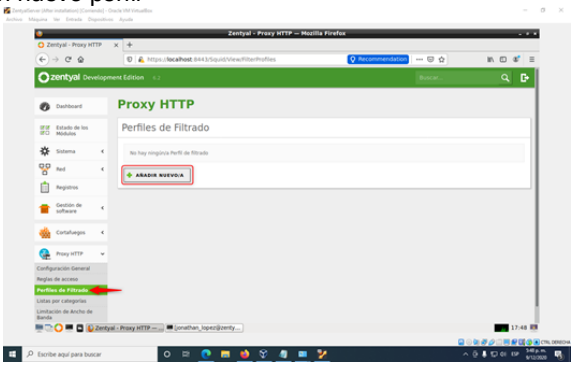
Guardamos los cambios



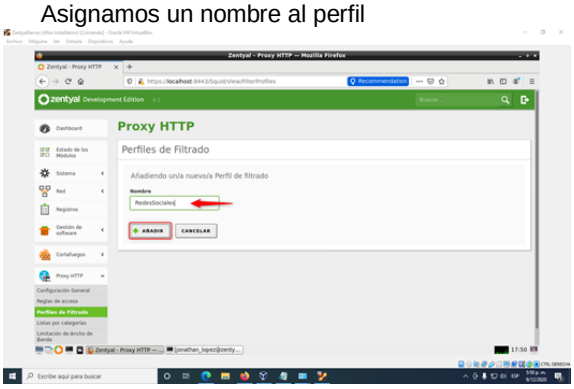
Se nos confirma los cambios guardados



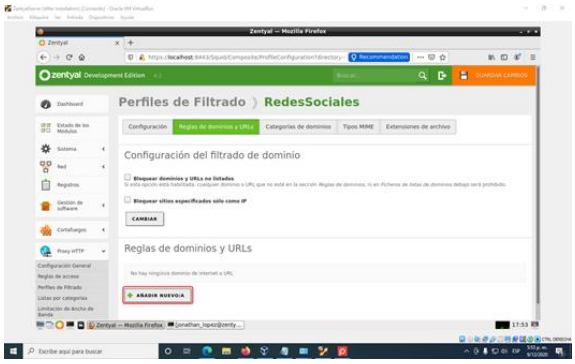
Ahora en la sección Perfiles de Filtrado crearemos un nuevo perfil



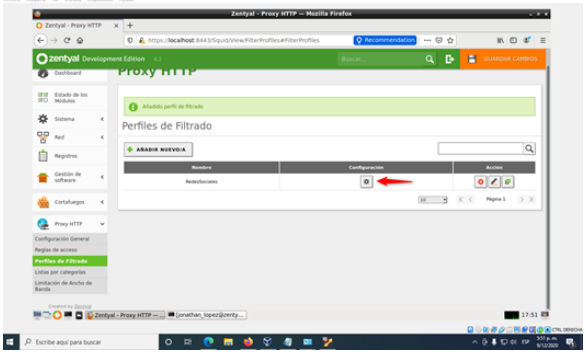
Asignamos un nombre al perfil



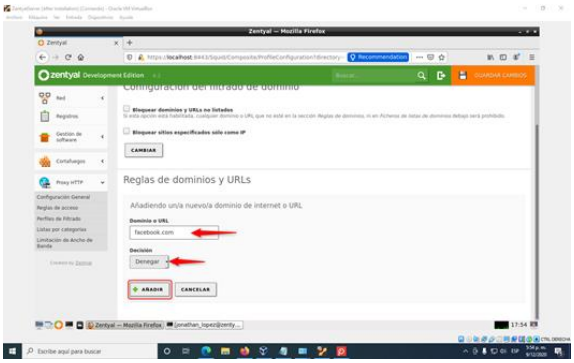
Dentro del perfil ingresamos a la sección “Reglas de dominios y URLs”. Una vez allí vamos a añadir una nueva regla



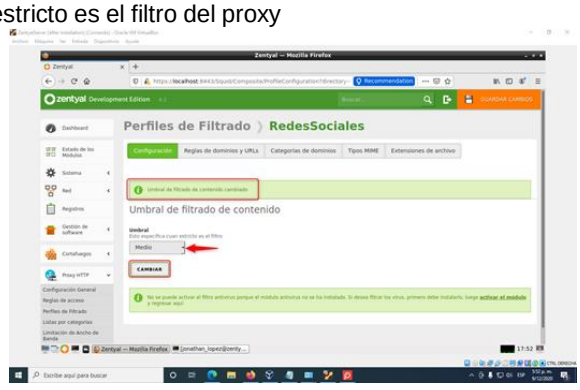
Ingresamos a la configuración del perfil de filtrado creado



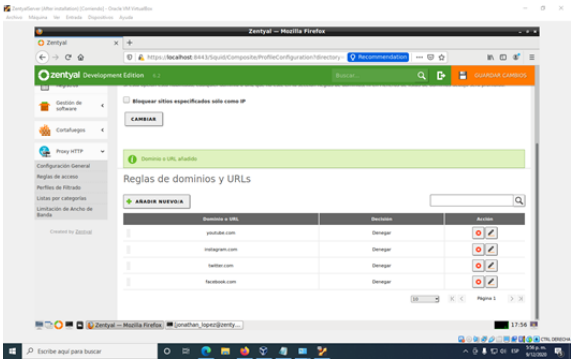
Agregamos las direcciones/dominios uno a uno y para cada uno de ellos seleccionamos si queremos denegar o permitir el acceso ya que nuestra regla consistirá en restringir el acceso web a páginas de redes sociales únicamente



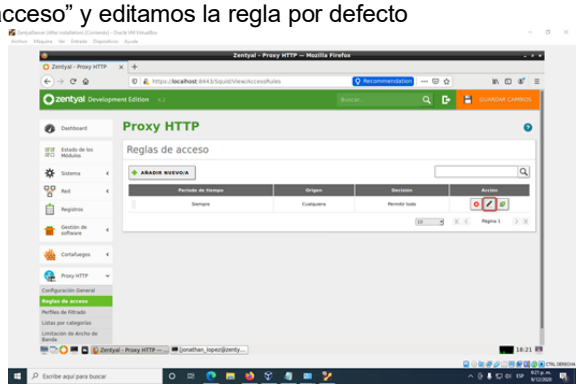
Seleccionamos “Medio” para especificar qué tan estricto es el filtro del proxy



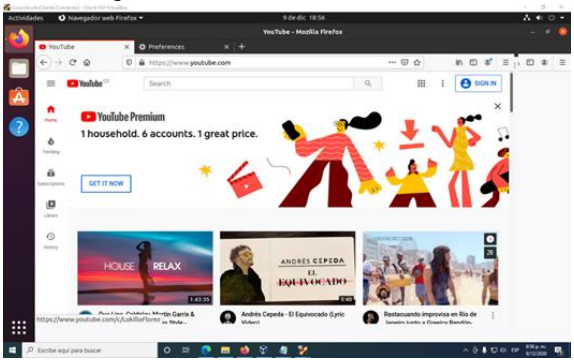
Así se visualizan las URLs o dominios en nuestra regla



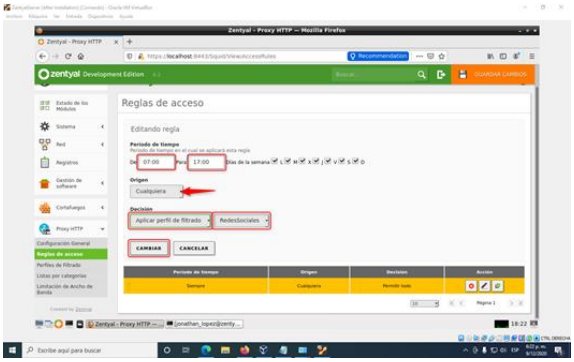
Dentro de Proxy HTTP ingresamos a “Reglas de acceso” y editamos la regla por defecto



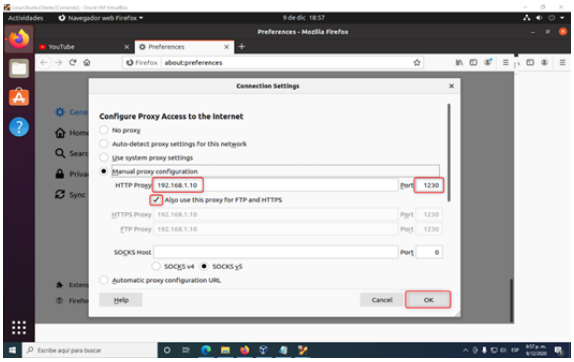
Si intentamos realizar navegación web hacia youtube.com en nuestro Ubuntu cliente sin proxy este permite la navegación



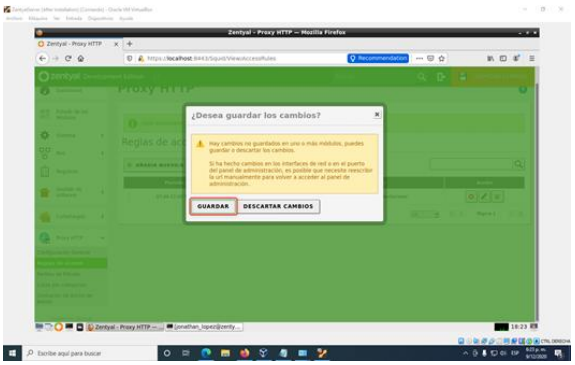
Editamos la regla con el horario que queremos que se aplique dicha regla. Adicionalmente indicamos a la regla que se aplique al perfil de filtrado que creamos con anterioridad



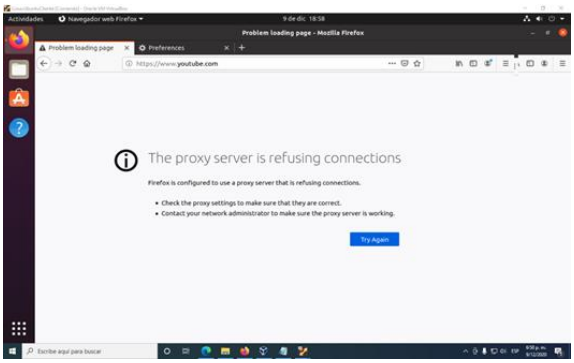
Ahora configuramos el proxy en nuestro navegador



los cambios realizados



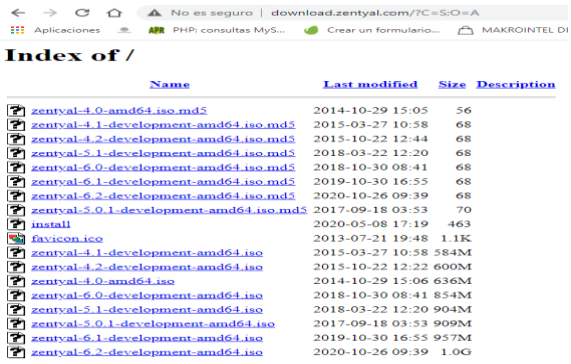
Luego de cerrar el navegador lo volvemos a abrir e intentamos ingresar a la misma página en este caso youtube.com y vemos el mensaje que el proxy rechaza esta conexión lo que nos indica el correcto funcionamiento de nuestro proxy no transparente en Zentyal



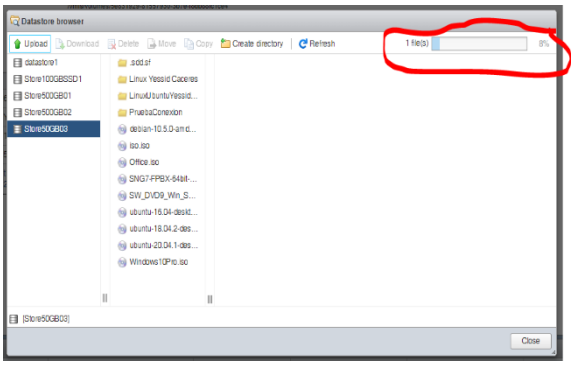
2.3 FILE SERVER Y PRINT SERVER

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.

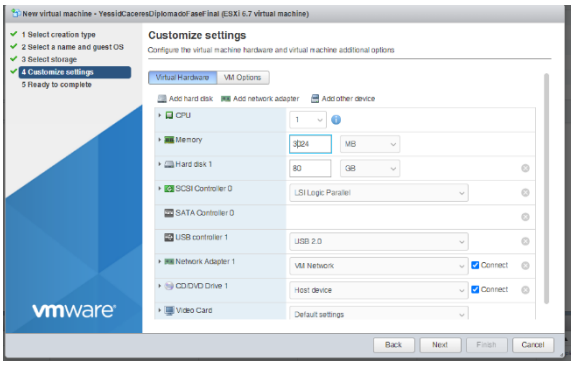
En este primer paso procedemos a descargar el archivo .iso desde la url del fabricante:



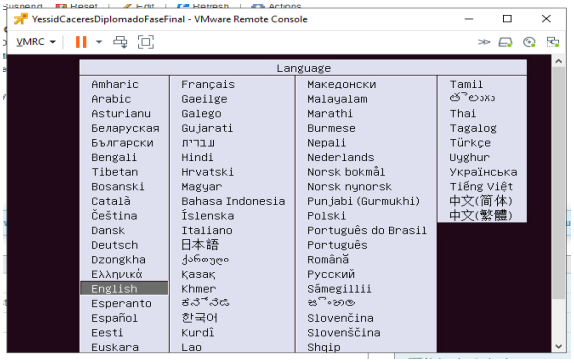
Una vez descargada procedemos a subirla a nuestro servidor Esxi VMware



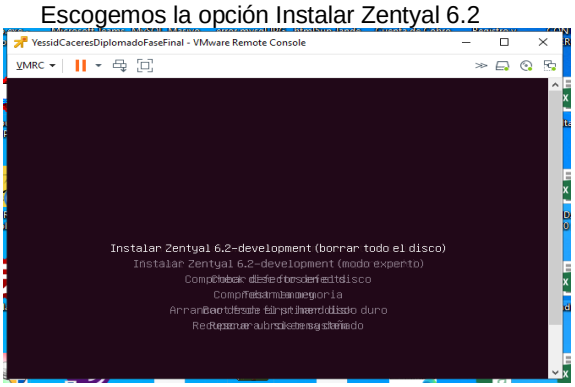
Seguido creamos una nueva máquina virtual con las características necesarias para que nuestro sistema operativo funcione correctamente.



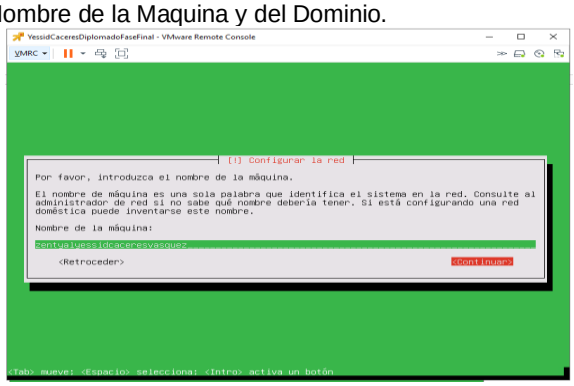
Iniciamos el procedimiento de instalación y seleccionamos el idioma.



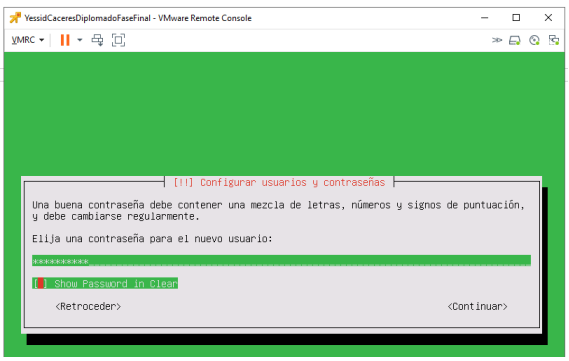
Escogemos la opción Instalar Zentyal 6.2



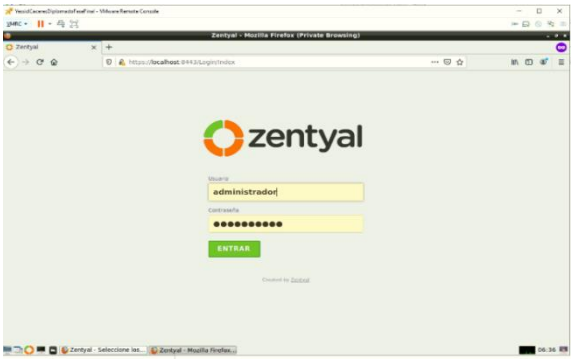
Seguimos las instrucciones del wizard para ubicación, distribución de teclado, configuración de Red, Nombre de la Maquina y del Dominio.



Creamos la cuenta de administrador con su respectiva contraseña.

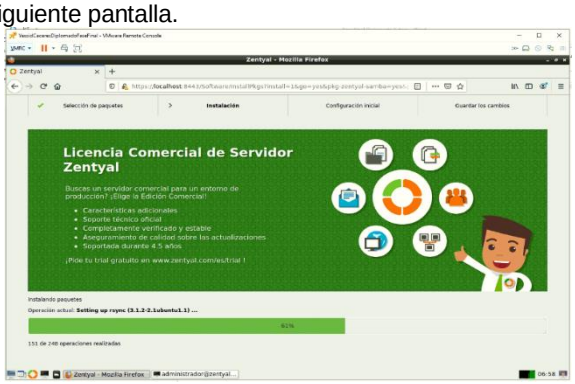


Una vez iniciado el sistema operativo, en la página que se abre o panel de control de zentyal damos clic en avanzada aceptar para autenticarnos.

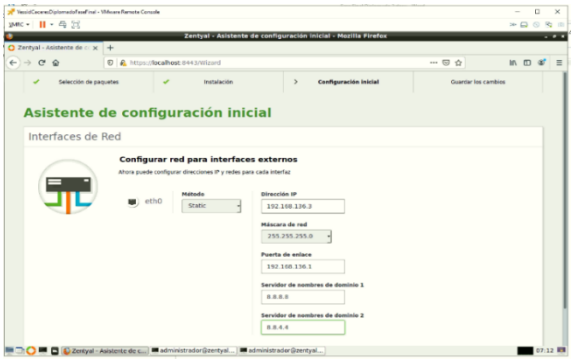


Configuramos nuestro Domain Controller and File Sharing con apoyo de este nuevo.

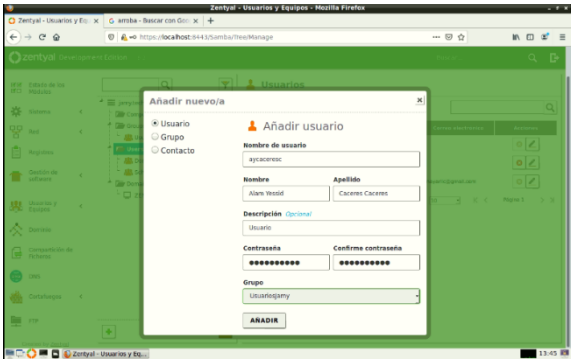
Una vez configurado, procedemos veremos la siguiente pantalla.



Procedemos a configurar nuestra interfaz de red, o sea la IP, Mascara de red y puerta de enlace para el Domain Controller.

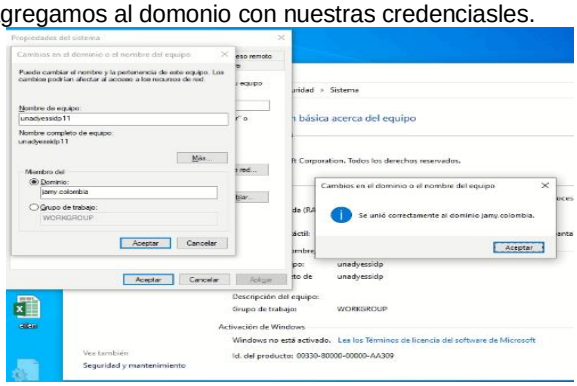


Una vez terminado el paso anterior creamos un grupo y un usuario dentro del Domain Controller.

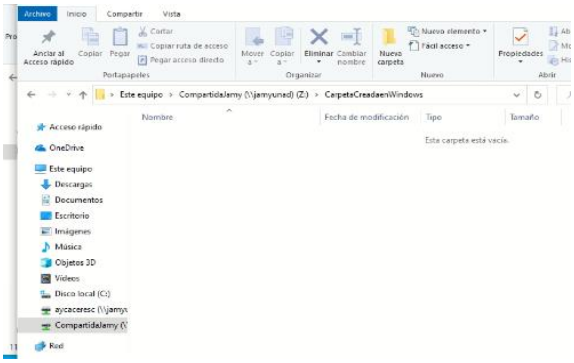


En Windows, procedemos a configurar la IP y el equipo para conectarlo al dominio.

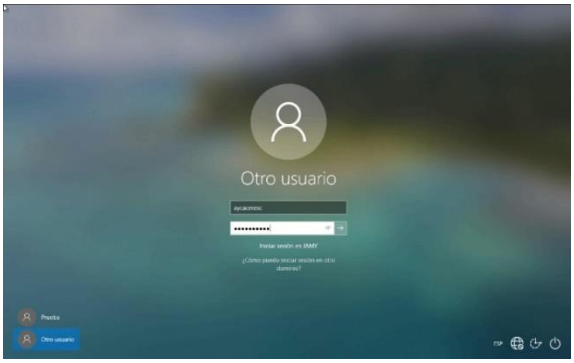
Cambiamos el nombre del computador y lo agregamos al domonio con nuestras credenciasles.



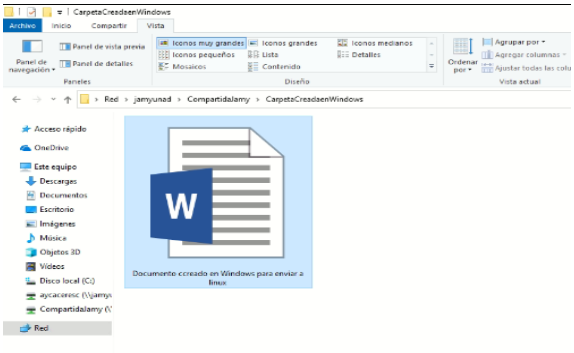
Vamos a la maquina con windows y verificamos intentando conectar una unidad de red con los datos de la compartida



el pc y nos autenticamos con las credenciales del usuario del dominio.

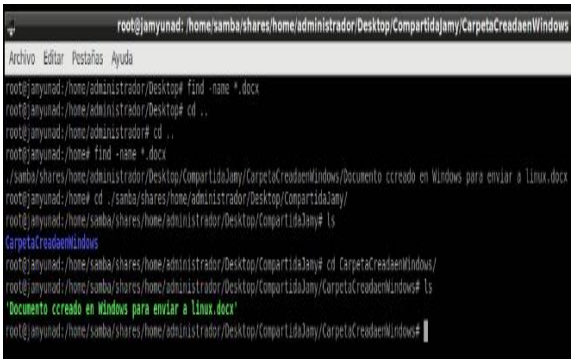


Creamos un archivo en la carpeta que acabamos de crear

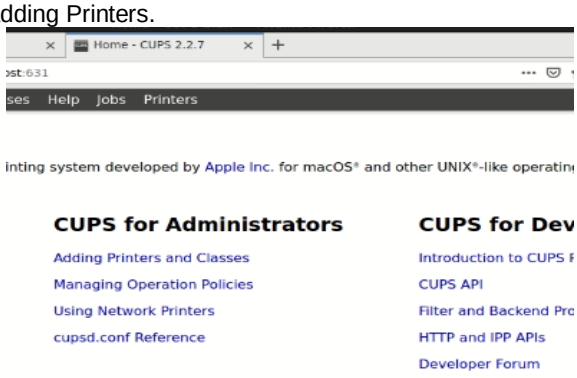


Procedemos acrear en el Domain Controller una carpeta que vamos a compartir con los usuario del grupo del dominio desde el panel.

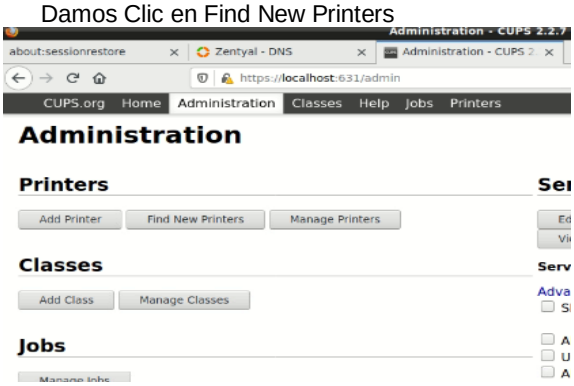
Verificamos en linux la existencia de la carpeta cread y su contenido



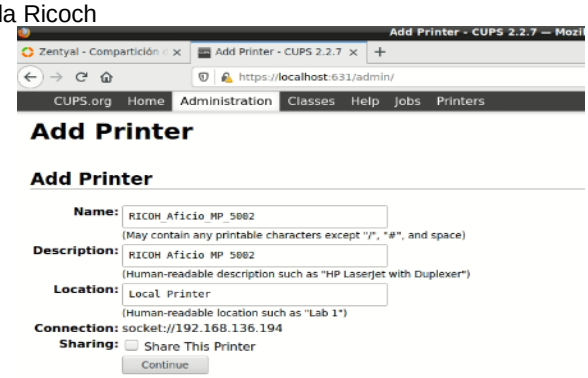
Instalamos cups desde la linea de comandos para poder instalar y compartir impresoras, seleccionamos adding Printers.



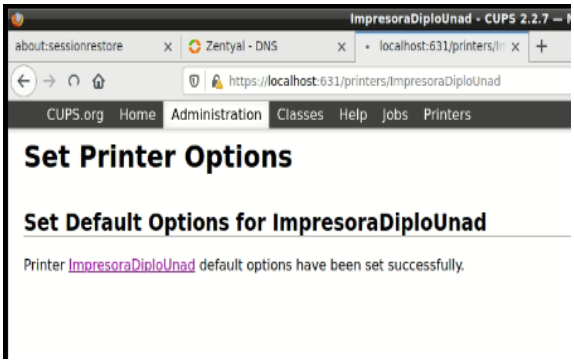
Damos Clic en Find New Printers



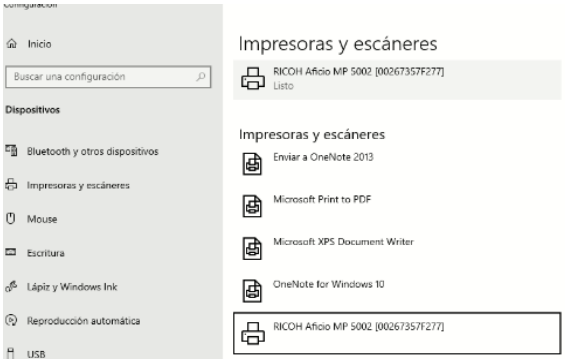
Escogemos nuestra impresora de red para el caso la Ricoch



Seguimos el Wizard hasta la finalización del proceso, hasta llegar a la siguiente ventana.

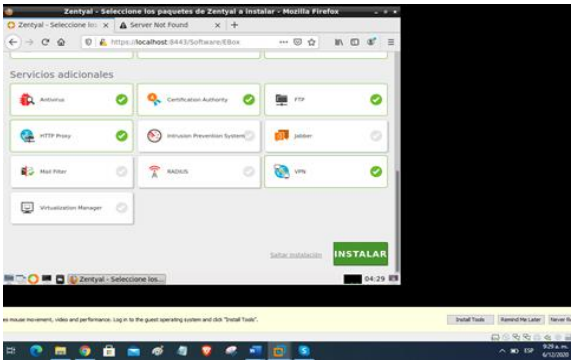


Una vez instalada y configurada, procemos a ir windows a instalarla.

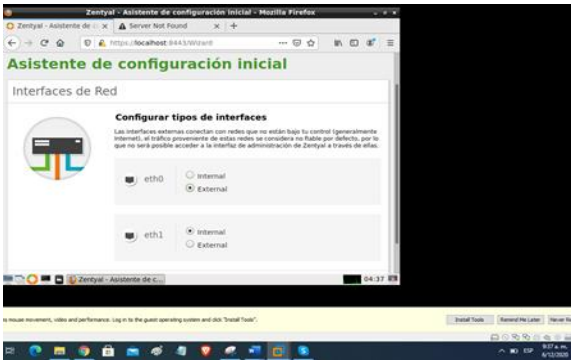


2.4 VPN

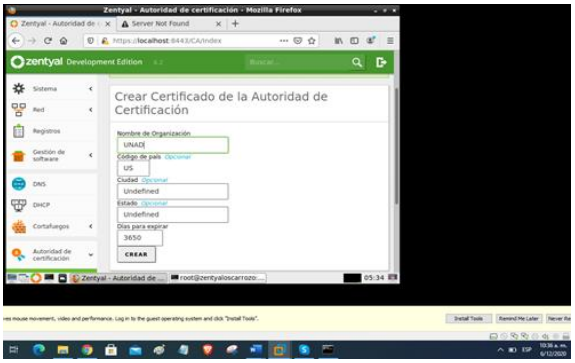
Se instalan los paquetes necesarios para configurar la VPN:



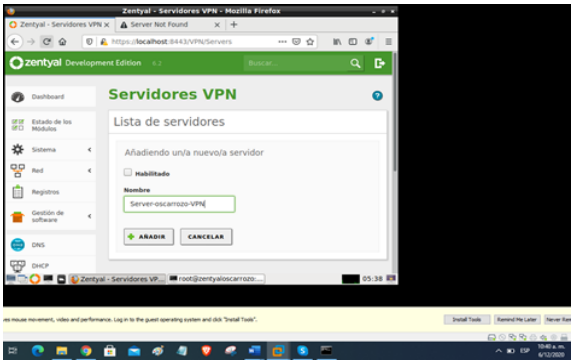
Se configuran las interfaces de red:



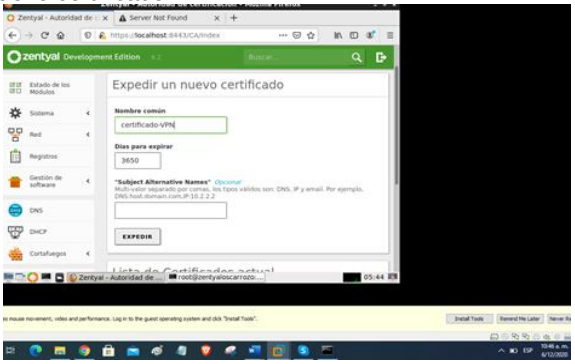
Se debe crear un certificado en autoridad de certificación colocando un nombre:



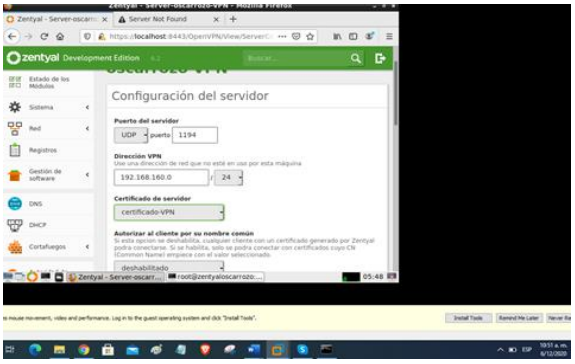
En el módulo VPN se procede a crear el servidor VPN:



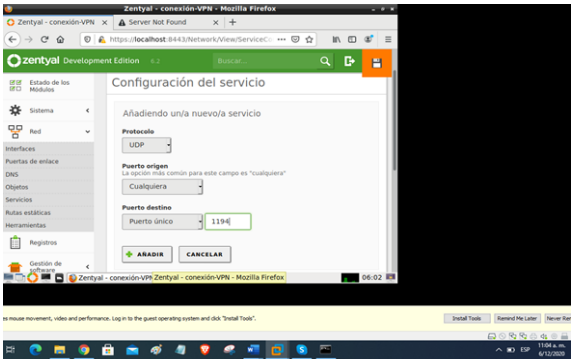
Nuevamente en autoridad de certificación se crea un nuevo certificado:



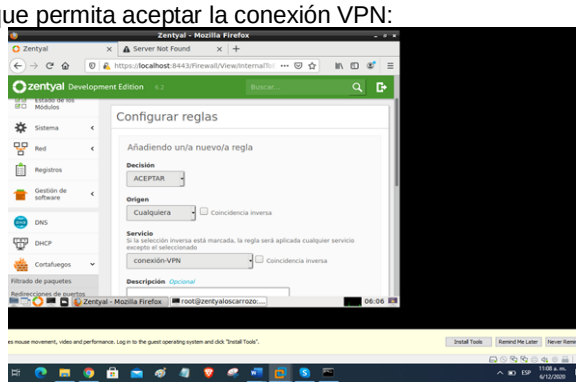
En el módulo de servidores se procede a configurar el servicio de VPN, seleccionando el certificado creado:



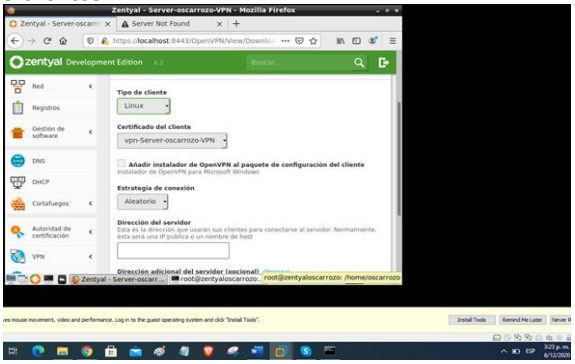
En el módulo red, se configura un nuevo servicio para VPN:



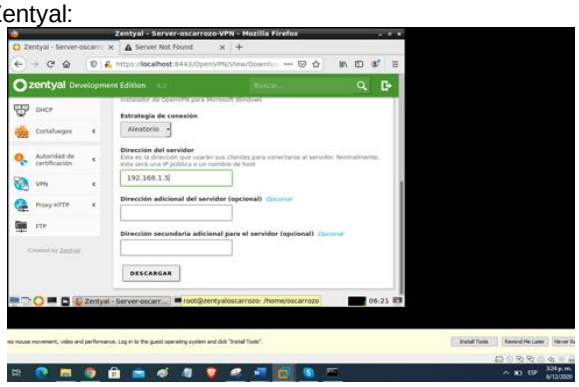
En el módulo Cortafuegos se crea una nueva regla que permita aceptar la conexión VPN:



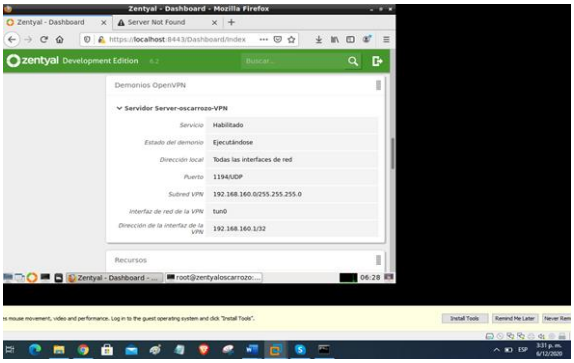
Se debe configurar y descargar los certificados para los clientes:



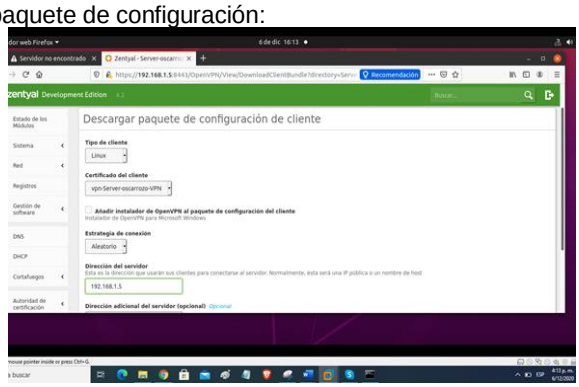
Se configura la dirección IP del servidor, como se trata de una red interna se coloca la misma del servidor Zentyal:



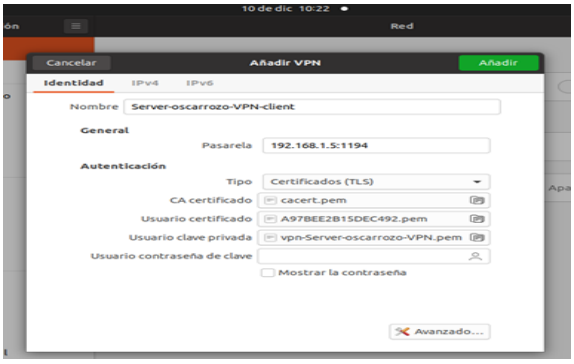
Como se puede verificar, el servicio se encuentra habilitado:



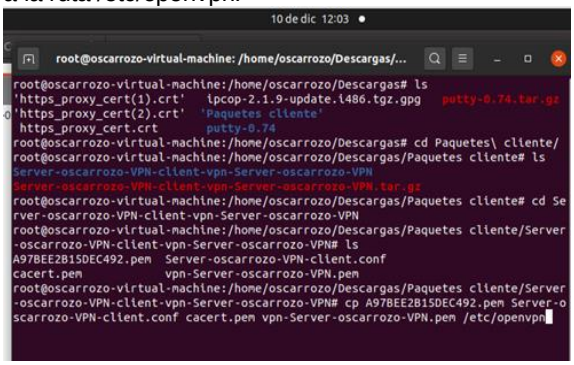
Desde la maquina cliente Ubuntu se Se descarga el paquete de configuración:



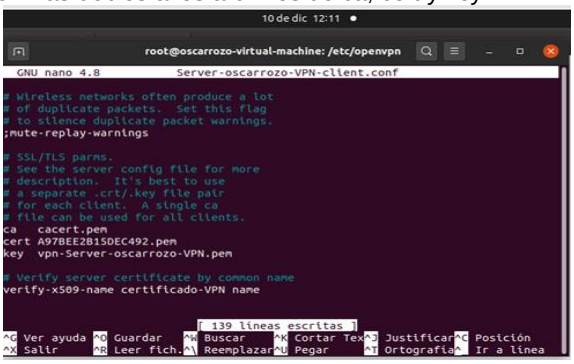
Se ingresa a la configuración de red de la maquina cliente y en la opción VPN, se importan los certificados creados desde el Zentyal desde la opción “Importar desde un archivo”:



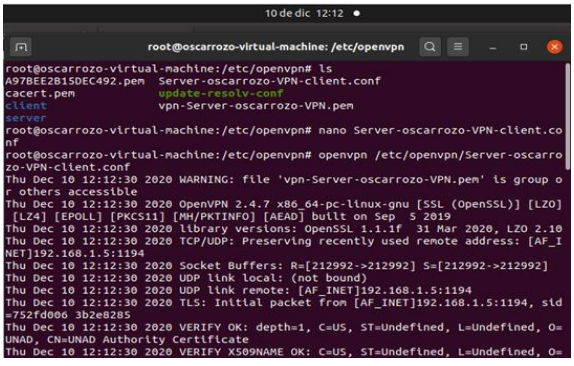
Se copian los archivos descargados desde Zentyal a la ruta /etc/openvpn:



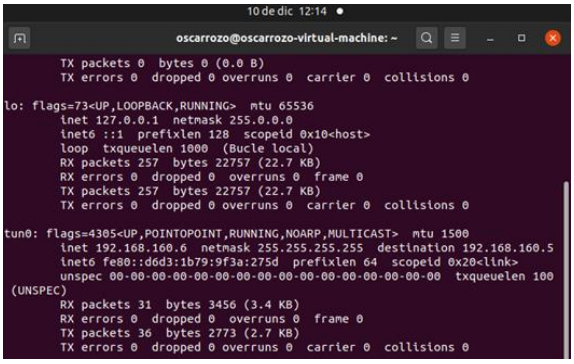
Se edita el archivo /etc/openvpn quitando las comillas dobles a los archivos de ca, cert y key:



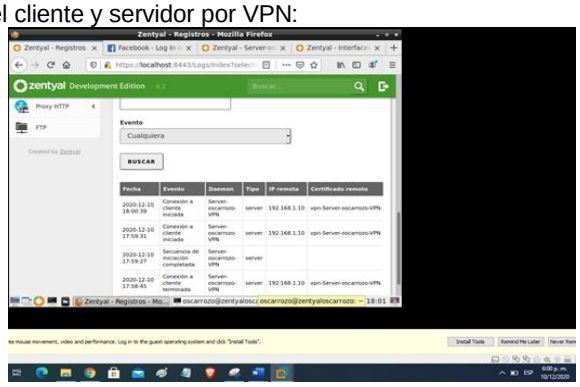
Se inicia el servicio de openvpn, para lo cual se debe estar en la ruta /etc/openvpn y ejecutar el archivo clien.conf:



Como se puede verificar ejecutando el comando ifconfig se ha creado un nuevo túnel seguro con el nombre tun0:



Se verifican los registros de Zentyal donde se pueden observar las conexiones que se han tenido entre el cliente y servidor por VPN:



2.5 CORTAFUEGOS

Lo primero que debe realizarse es la descarga de Zentyal Server 6.2, el cual puede descargase gratuitamente desde la página oficial. Posterior a ello se realizarán los siguientes pasos.

Figura 1. Creación de la VirtualBox (fuente propia)

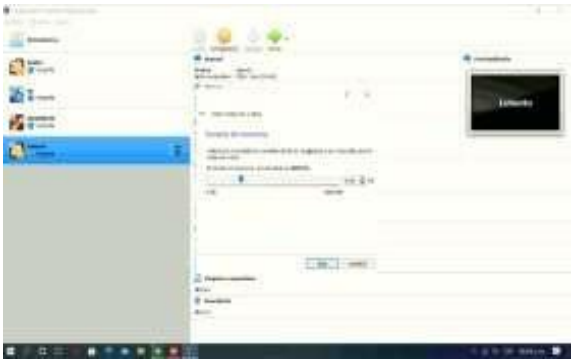


Figura 2. Selección de la memoria RAM para la máquina (fuente propia)

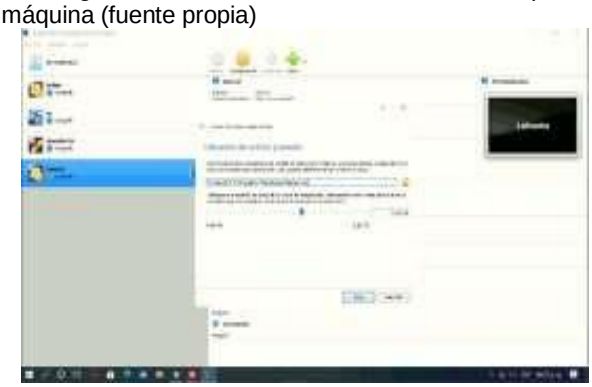


Figura 3. Selección del tamaño del disco duro (fuente propia)

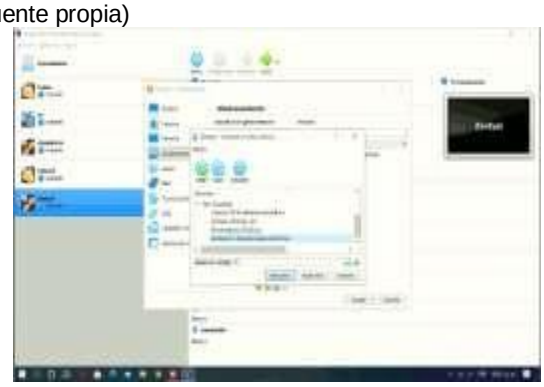


Figura 4. Búsqueda de la imagen ISO y configuración de red tipo puente (fuente propia)

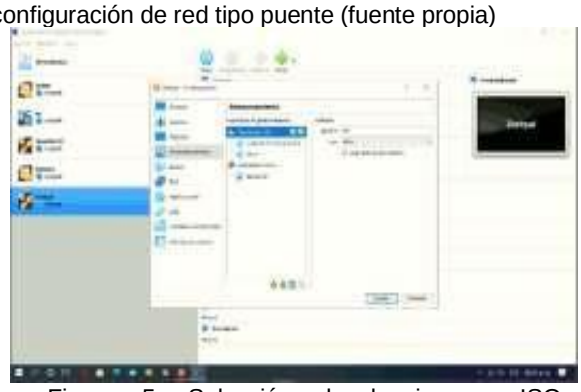


Figura 5. Selección de la imagen ISO y configuración de red tipo puente (fuente propia)

Figura 6. Inicio de la instalación de Zentyal Server (fuente propia)

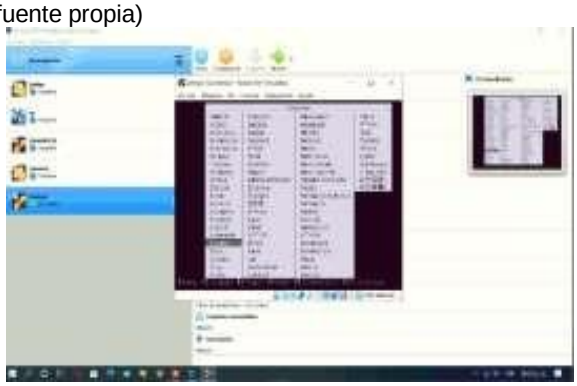


Figura 7. Selección del idioma en la instalación (fuente propia)

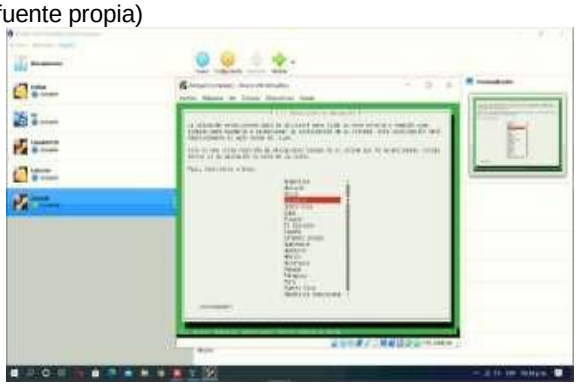


Figura 8. Selección del país (fuente propia)

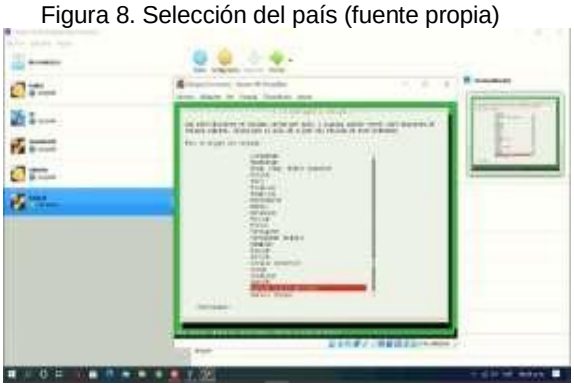


Figura 9. Configuración del teclado (fuente propia)

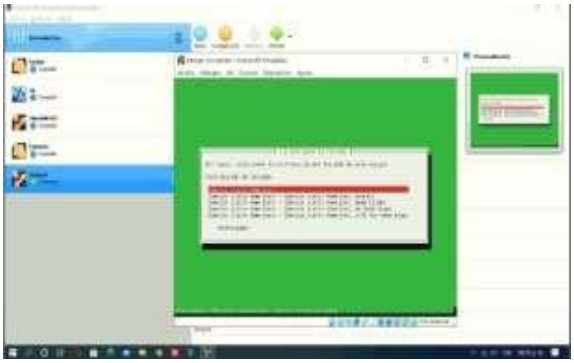


Figura 10. Selección de la distribución del teclado (fuente propia)

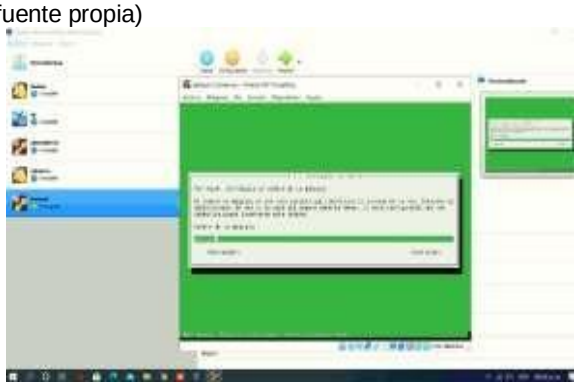


Figura 11. Registro usuario (fuente propia)

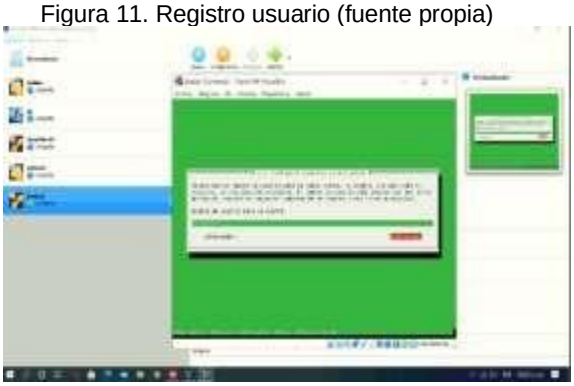


Figura 12. Registro usuario, inserción de la contraseña (fuente propia)

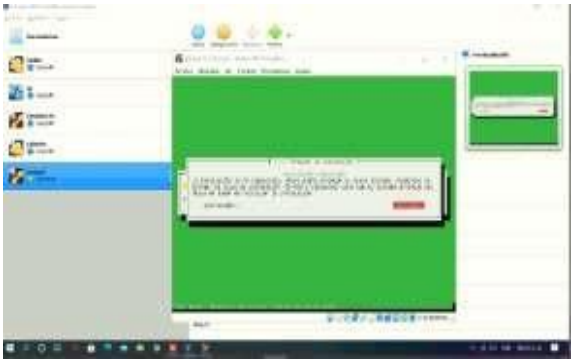


Figura 13. Instalación completada (fuente propia)

Figura 14. Interfaz de inicio de Zentyal Server (fuente propia)

2.5.1 CORTAFUEGOS

En primera instancia se debe instalar firewall server, así que el primer paso será seleccionar en él y clic en install

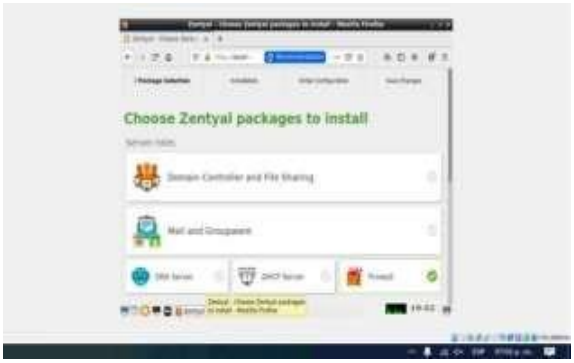


Figura 15. selección del firewall server y clic en install (fuente propia)

Ahora bien, en cuanto a la interfaz de red eth0 donde se ubica el router de internet, se debe seleccionar la red externa. En la interfaz de red eth1 seleccionamos red interna, así:

Figura 16. Configuración de Interfaces en Zentyal (fuente propia)

Entonces se realiza una configuración de la IP y el netmask propio de la red principal. Cabe resaltar que se debe agregar los domain name servers, en este caso se usaron los siguientes: 8.8.8.8 y 8.8.4.4

Figura 17. Configuración de direcciones IP en Zentyal. (fuente propia)

Posterior a ello se realiza desde Ubuntu la modificación de la IP y la máscara de red de la interfaz.

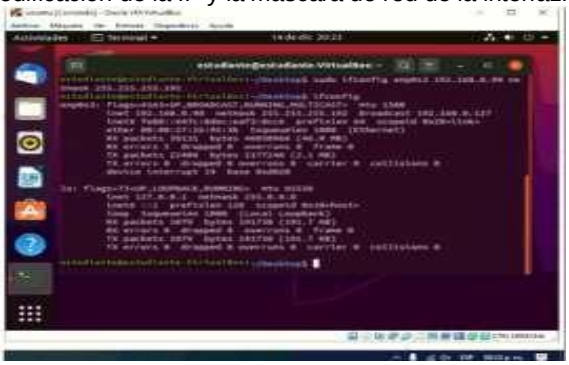


Figura 18. Comando ifconfig para verificar IP actual. (fuente propia)

Luego, se modifica el Gateway de la máquina, nos aseguramos que sea la única ruta.

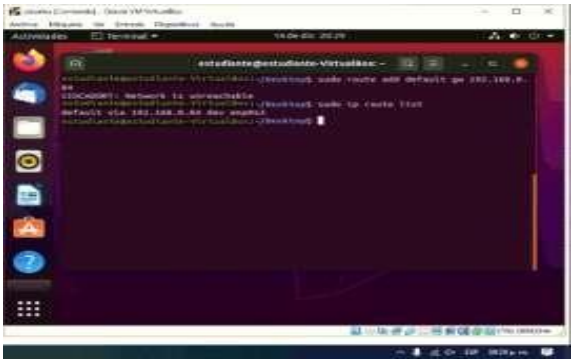


Figura 19. Verificación de rutas de salida de Zentyal. (fuente propia)

Ahora se debe asignar los DNS resolvers. Para eso editamos el archivo /etc/resolv.conf

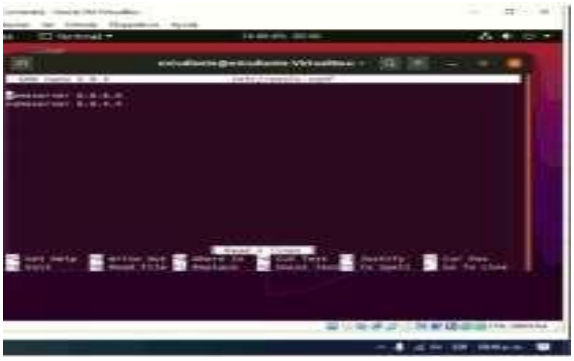


Figura 20. Definición de Servidores de salida a internet. (fuente propia)

Con el firewall de Zentyal se elabora una ruta para el tráfico entre la interfaz eth1 y la IP 192.168.0.90, para esto se debe de buscar en el menú el firewall y seleccionamos la opción forwarding

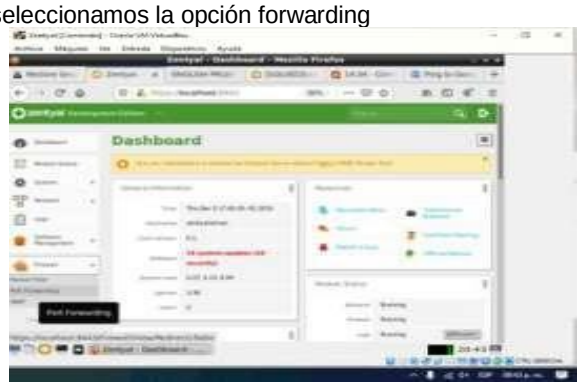


Figura 21. Verificación en el panel de control. (fuente propia)

Luego de lo anterior, se accede a “port forwarding” y luego a “add new”. Además, se añade la siguiente configuración:

Destination: 172.217.28.110

Figura 26. Verificación de rutas redirección. (fuente propia)

Posterior a haber agregado las reglas para bloquear las direcciones IP de YouTube hacia la red interna se guardan las acciones realizadas.

4 CONCLUSIONES

Como conclusión podemos decir que se puede llevar a cabo para un cliente o nuestra empresa una migración completa de los sistemas operativos, servicios y de más funcionalidades a un sistema totalmente open source con un minimo de conflicto al inicio de la implementación, pero que al finalizar se pueden solucionar en su totalidad, sin ver afectada la seguridad en la infraestructura de red y llevar a ceros los costos de licenciamiento.

5 REFERENCIAS

[1] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial. Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92

[2] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 6 – 84). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56046?page=6

[3] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing. Recuperado de https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page-__-20

[4] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40

[5] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 205 - 236). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43262?page=205

[6] Zential, Z. C. (s.f). Installation. (Páginas. 1 - 25). Recuperado de https://doc.zentyal.org/en/installation.html#zentyal-installer

[7] Zential, Z. C. (2014). Installation. (Páginas. 1 - 5). Recuperado de https://wiki.zentyal.org/wiki/Es/3.2/Servicio_de_comparticion_de_impresoras

[8] VPN con IPSEC y L2TP/IPSEC. Recuperado de https://doc.zentyal.org/es/ipsec.html#configuracion-de-un-tunel-ipsec-con-zentyal