

# SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX,

Alba Lilian Osorio Serna  
e-mail: lili.osorio93@gmail.com  
Fabián Enrique Sánchez Boada  
e-mail: fsanchezb@unadvirtual.edu.co  
Marxio Alejandro Acero  
e-mail: Sindy Jaen Merchán Mora  
e-mail: sjmerchanm@unadvirtual.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:** Zentyal Server, Ubuntu Desktop, proxy, firewall, LDAP, VPN.

## 1 INTRODUCCIÓN

En el mundo de las distribuciones Linux existen muchas herramientas que permiten adaptar la infraestructura IT según las necesidades de la empresa, haciendo de la administración del sistema un proceso menos complejo y costoso. Dentro de estas herramientas encontramos Zentyal Server que contiene un paquete de programas para la gestión de la infraestructura de red, permitiendo así la configuración de los diversos servicios que necesita la empresa.

Zentyal Server fue diseñado para ser una alternativa a Windows Server, está construido sobre Ubuntu y Apache. Cuenta con una interfaz gráfica a la que podremos acceder desde un navegador (aplicación web), desde allí podremos administrar los servicios de la red tales como: DHCP, DNS, Proxy, firewall, VPN, entre otros.

## 2 INSTALACIÓN DE ZENTYAL

Vamos a la página de Zentyal y descargamos la imagen ISO de Zentyal 5.0

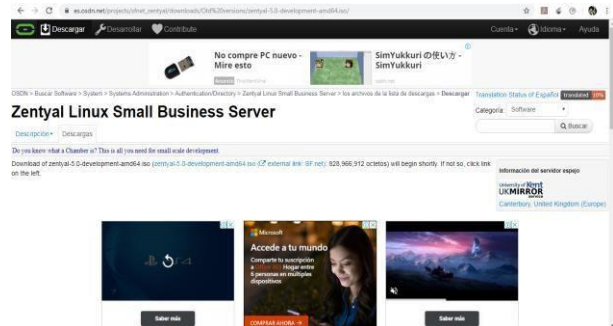


Imagen 1. Descarga imagen ISO

Creamos la máquina virtual y le damos el nombre

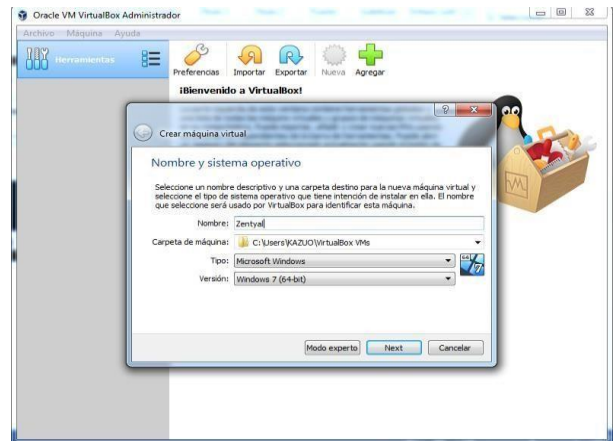


Imagen 2. Nombre de la máquina

Seleccionamos la memoria RAM de la máquina para este caso 2048 MB

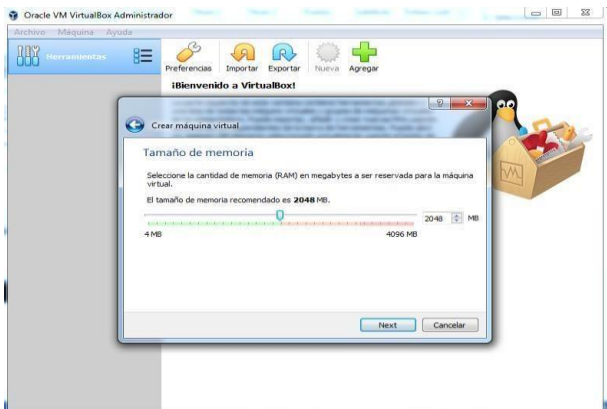


Imagen 3. Selección de memoria RAM

Seleccionamos el tamaño del disco duro, en este caso con 20 GB bastará

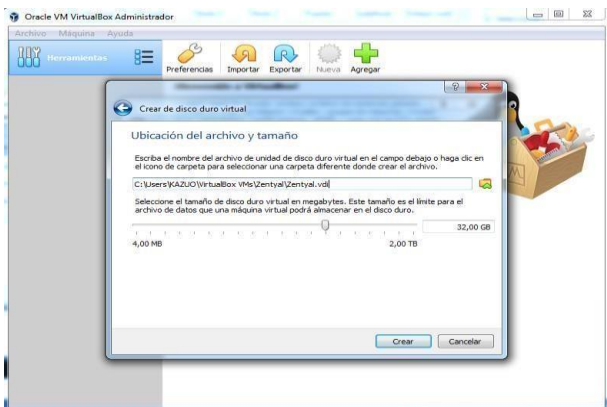


Imagen 4. Tamaño de disco duro

En almacenamiento usamos la imagen ISO y configuración de red tipo puente

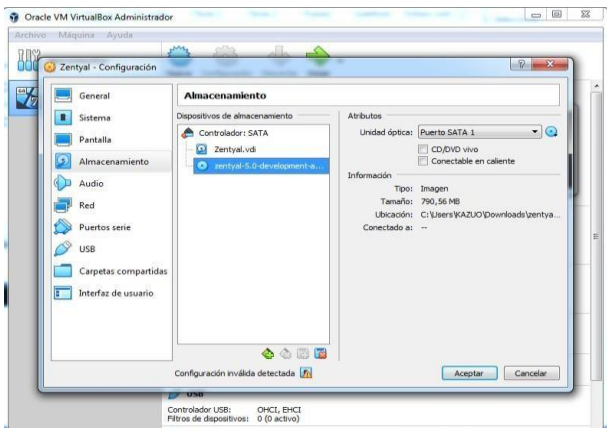


Imagen 5. Uso de la ISO descargada Iniciamos la máquina y seleccionamos el idioma del menú

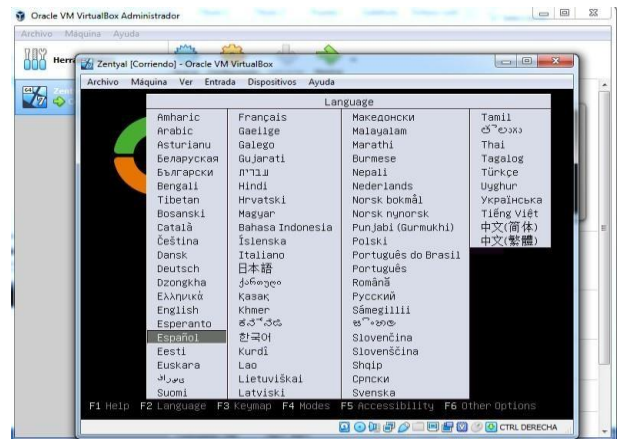


Imagen 6. Selección de idioma menú

Escogemos la opción instalar Zentyal 5.0



Imagen 7. Selección de instalación

Seleccionamos el idioma de la instalación español, así como el idioma del teclado y la ubicación Colombia

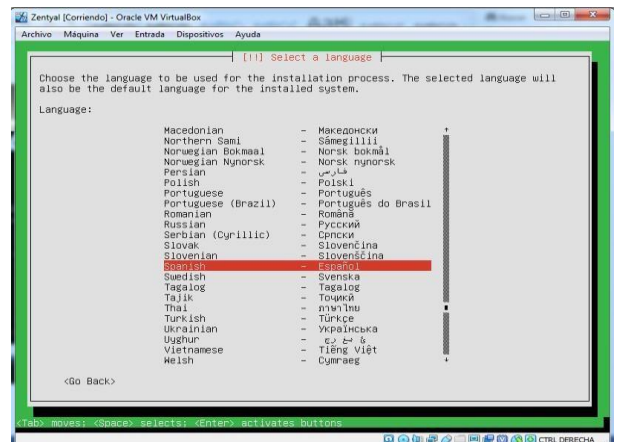


Imagen 8. Selección de idioma  
Damos un nombre a la máquina

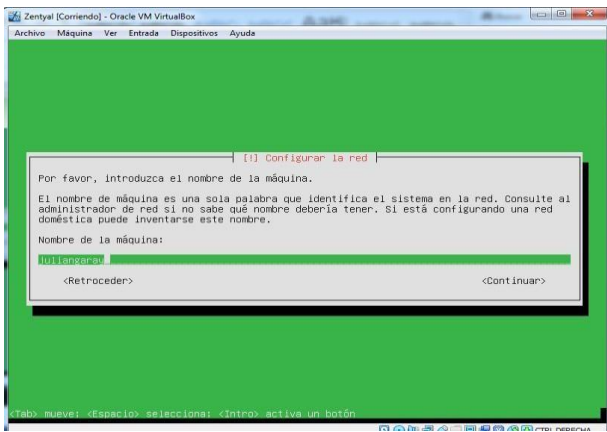


Imagen 9. Nombre de la máquina

Y un usuario del sistema

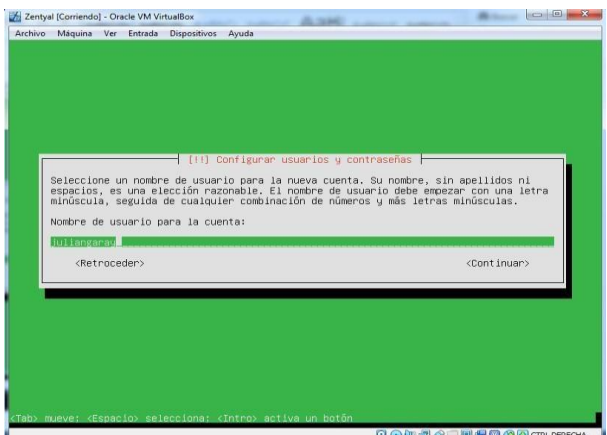


Imagen 10. Nombre del usuario

Asignamos una clave al nuevo usuario

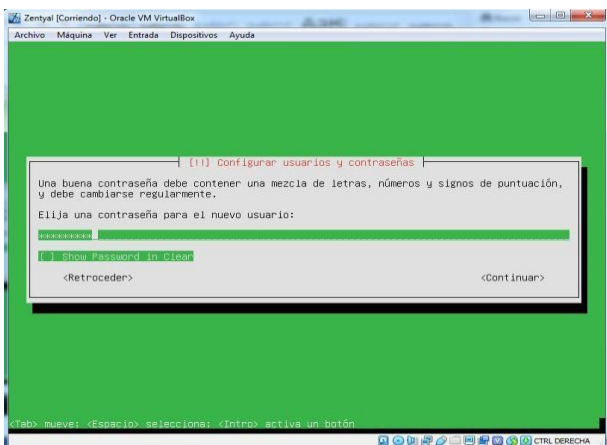


Imagen 11. Clave para el usuario

Inicia la instalación del sistema

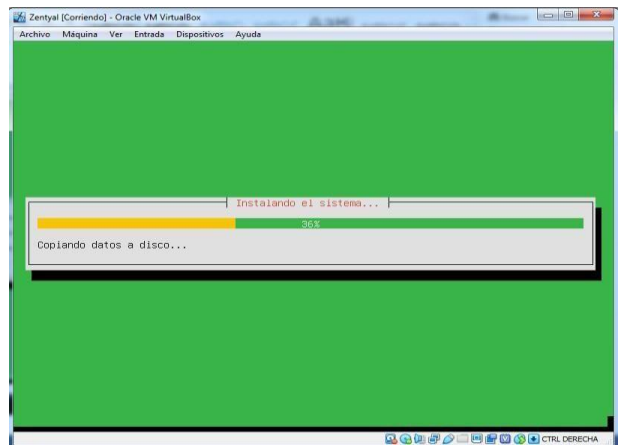


Imagen 12. Instalación del sistema

Al finalizar la instalación seleccionamos continuar y se reinicia el equipo

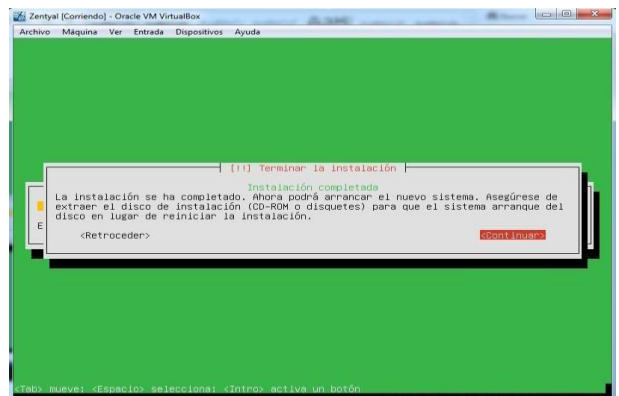


Imagen 13. Finalización de la instalación

Ya queda instalada la máquina virtual de Zentyal

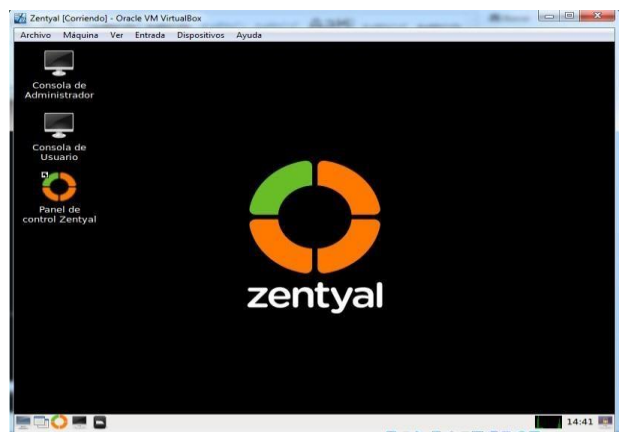


Imagen 14. Escritorio Zentyal

### 3 CONFIGURACIÓN DE ZENTYAL

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

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

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.

Ingresamos al dashboard de Zentyal y allí seleccionamos los servicios que vamos a necesitar para el desarrollo de las 5 temáticas

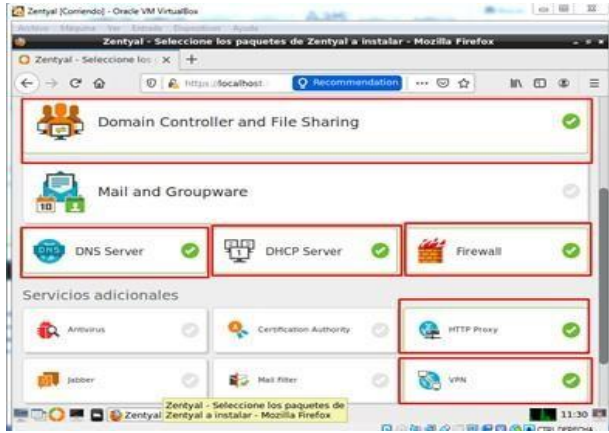


Imagen 15. Instalación de servicios

Terminado el proceso nos pide que configuremos las interfaces de red donde vamos a dejar una como red externa para que se conecte a internet en modo DHCP y la otra como red interna para gestionar todos los servicios la cual no configuraremos por el momento



Imagen 16. Configuración de interfaces

El tipo de dominio lo dejamos por defecto stand-alone y le damos el nombre que queramos como por ejemplo grupo55.unad.com



Imagen 17. Selección de dominio

Vamos a ver el estado de los servicios y validamos que todos estén habilitados en especial DNS, DHCP y Controlador de dominio

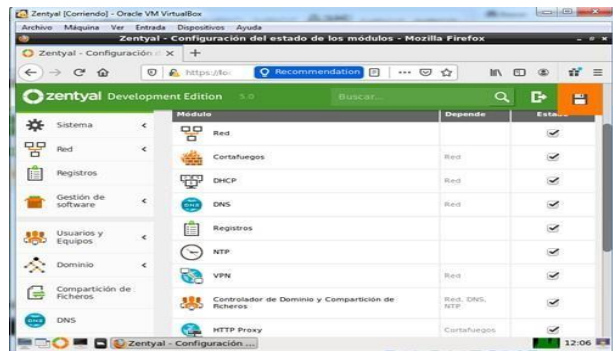


Imagen 18. Validación de servicios

Vamos a la sección DNS y validamos que esté activo el dominio que creamos y que tenga una Ip válida dentro del rango de la red



Imagen 19. Configuración DNS

Para el DCHP vamos al módulo de interfaces Y configuramos la segunda interfaz (que es la interna) como estática y le damos una IP



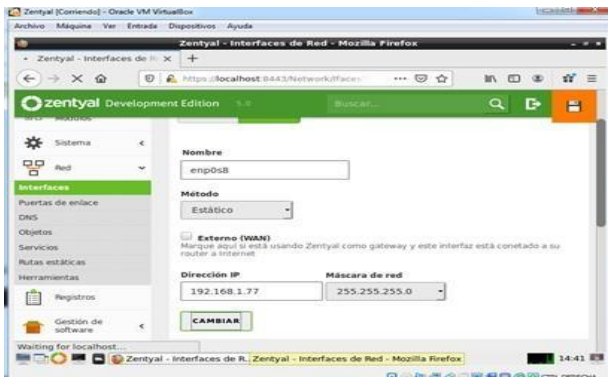


Imagen 20. Configuración interface 2

Creamos un nuevo rango de ip que serán los que van a asignar el DHCP a los clientes

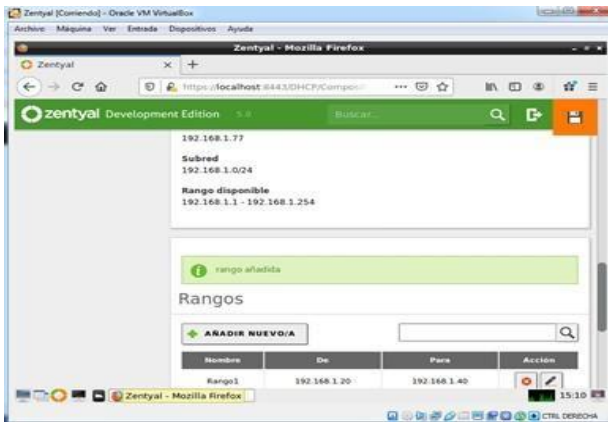


Imagen 21. Asignación de rangos

Abrimos el Ubuntu desktop y vemos que se nos asigna una ip dentro del rango del DHCP y con la DNS que establecimos

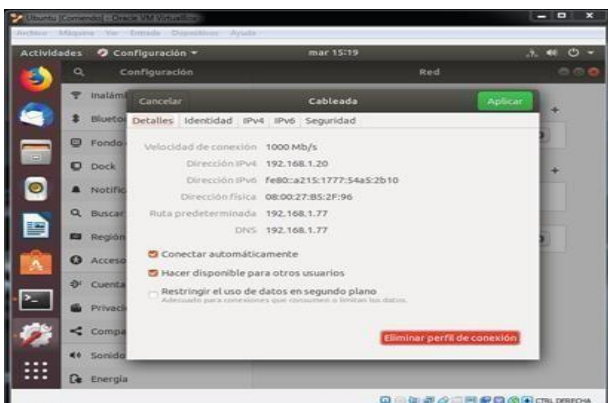


Imagen 22. Validación cliente DHCP y DNS

Y en el dashboard de Zentyal ya aparece en la lista de IPs asignadas lo cual demuestra que se realizó el proceso correctamente

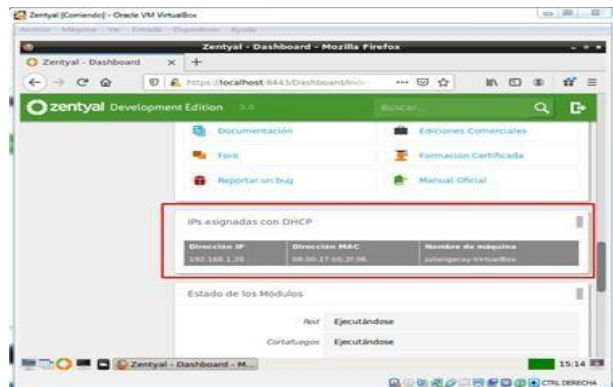


Imagen 23. Comprobación en Zentyal

Para añadir usuarios al dominio vamos a la sección usuarios y equipos y agregamos un nuevo usuario donde le asignamos nombre, usuario, contraseña y Grupo55

Y como se puede observar ya queda guardado como usuario del dominio en Zentyal

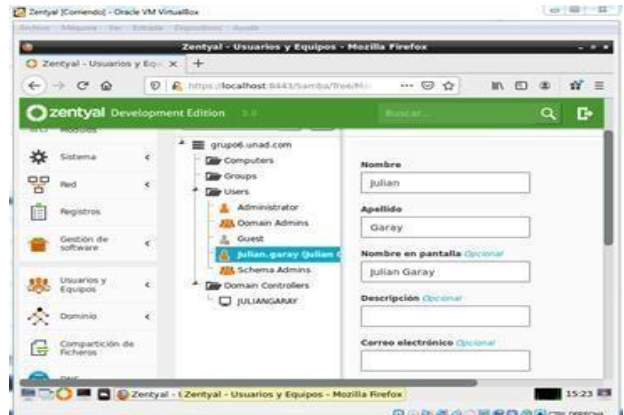


Imagen 25. Validación de usuario

Ahora para configurar el cliente dentro del dominio vamos a descargar un programa para la gestión de directorio activo en este caso pbs 64 bits desde la página

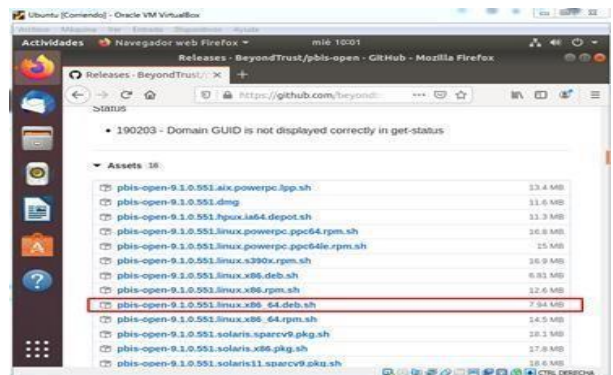
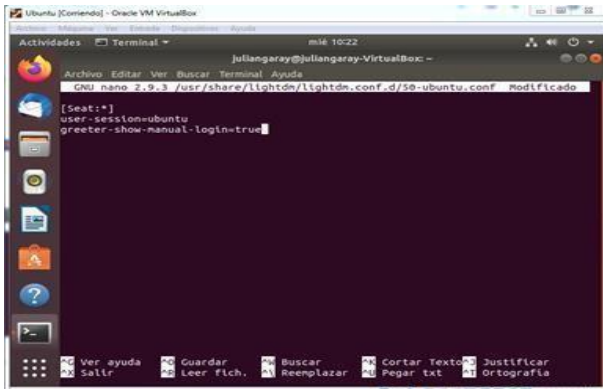


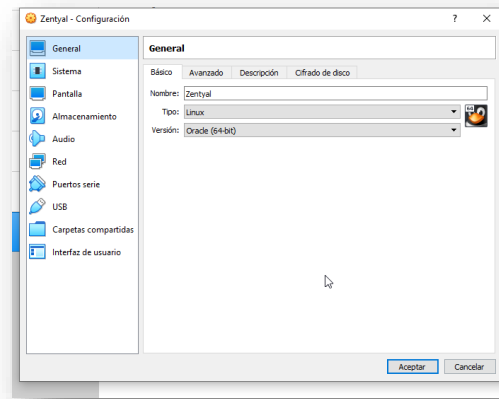
Imagen 26. Descarga de pbis-open

Después editamos el archivo 50-ubuntu.conf para colocar un login manual



. Configuración inicio manual

Finalmente agregamos un Shell al usuario cuando inicie sesión



3.2.3 Se selecciona el idioma con el que se configurara

## 3.2 PROXY NO TRANSPARENTE

### 1. DESARROLLO DE CONTENIDOS

(Instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT).

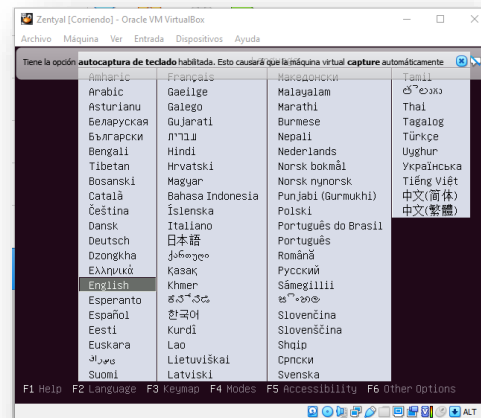
#### Temática 2: Proxy no transparente

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.

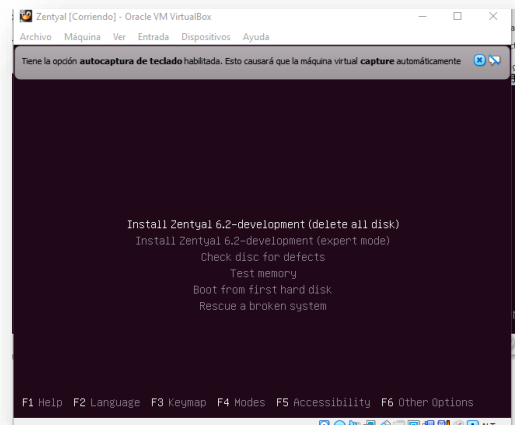
#### Que es un proxy transparente

Su principal función es proporcionar un servicio intermediario, el cual filtra las peticiones que se realizan desde un cliente al servidor Proxy en el cual se puede denegar el acceso a todo el tráfico o si lo necesitamos se puede restringir el acceso solo a determinados sitios web con el fin de garantizar la seguridad de las empresas con los sitios web que pueden acceder sus colaboradores.

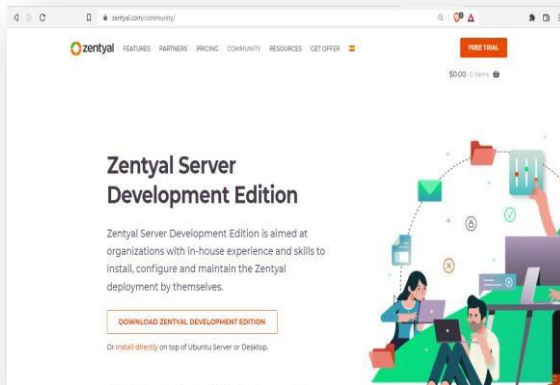
3.2.1. Se descarga la iso de Zentyal Server desde la página web oficial.



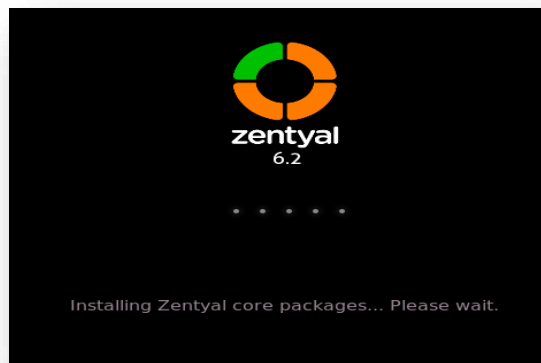
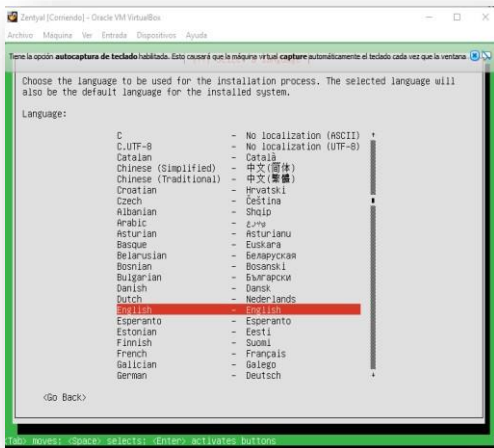
3.2.4 Seleccionamos la opción de instalar



3.2.5 Seleccionamos el idioma de configuración:



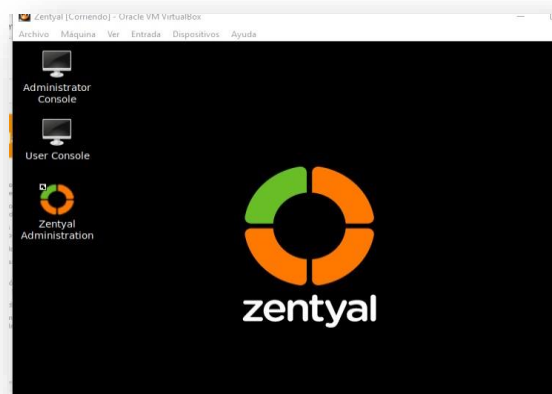
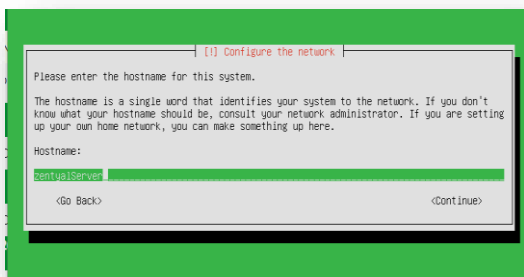
3.2.2 Se nombra la máquina virtual.



3.2.10 Una vez finalizada la instalacion podemos ver el escritorio de nuestro servidor:

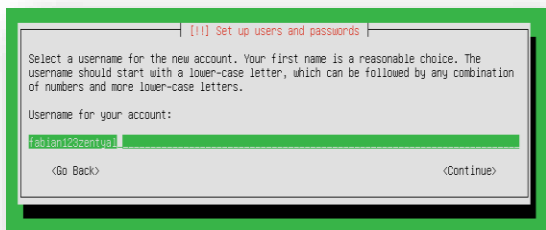
Ahora indicamos el nombre del host:

3.2.6

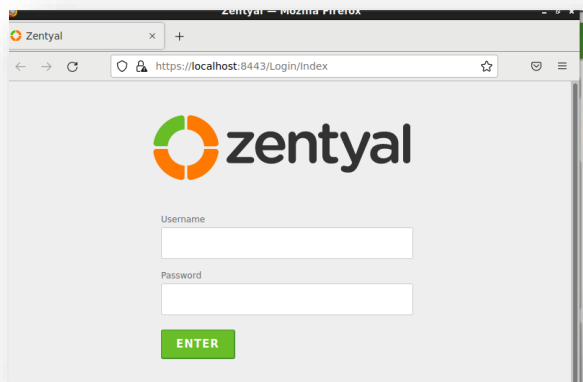


Ahora indicamos el nombre del

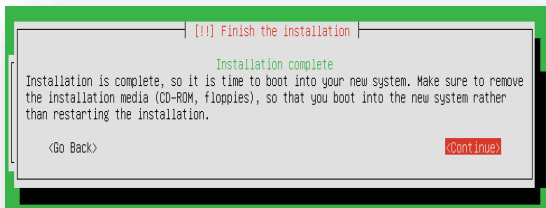
3.2.7 usuario:



3.2.11 Ingresamos al navegador del servidor e ingresamos al login de zentyal con el usuario previamente creado:

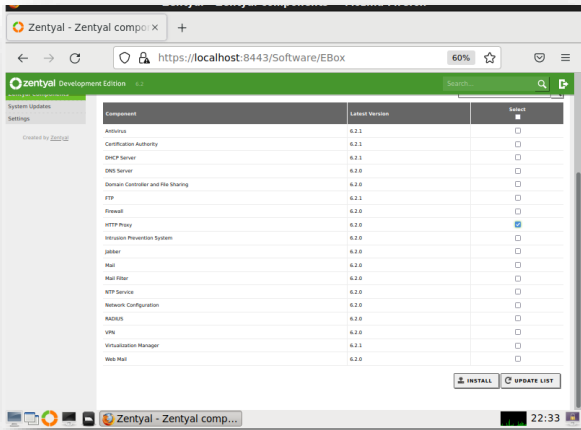


3.2.8 Finalizada la instalación damos clic en continuar:

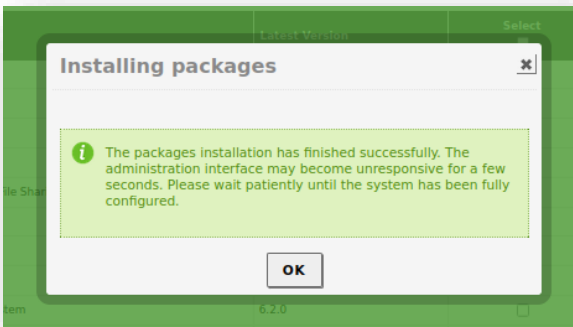


3.2.9 Se empieza a realizar la configuración del sistema operativo:

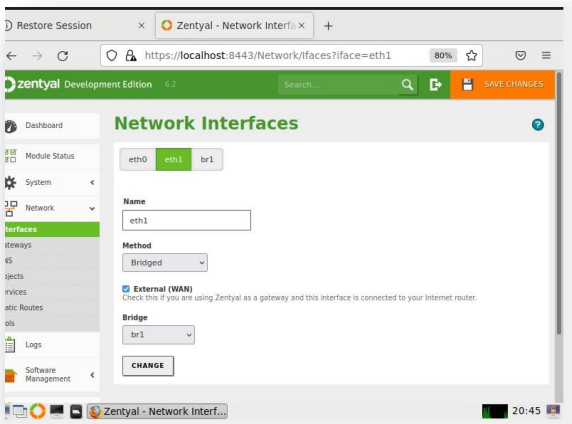
3.2.12 Una vez ingresamos realizamos la instalación de los servicios necesarios, en este caso solo ocupamos HTTP Proxy:



3.2.13 Una vez seleccionados podemos observar el mensaje de confirmación:

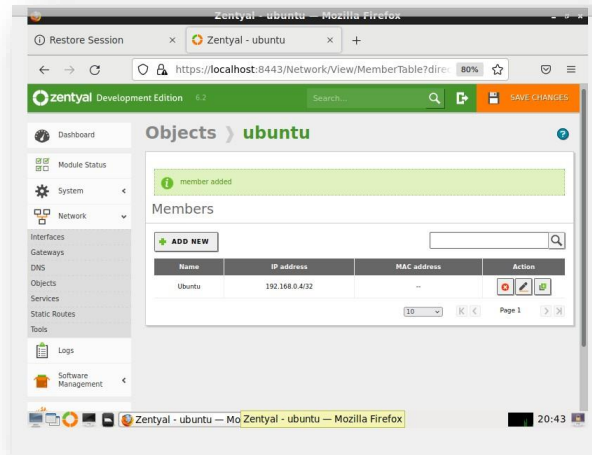


3.2.14 Ahora configuramos las interfaces de red:

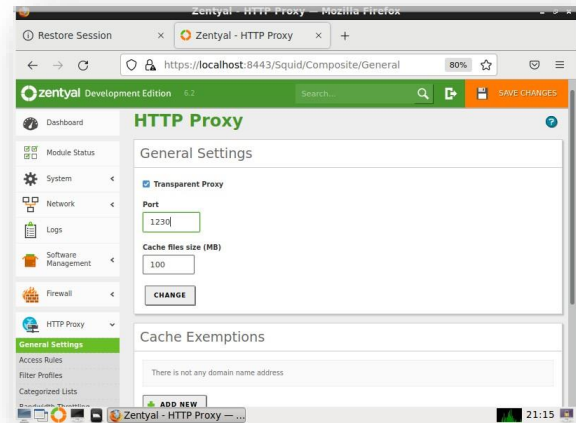


3.2.15 Ahora creamos un objeto con el nombre de Ubuntu:

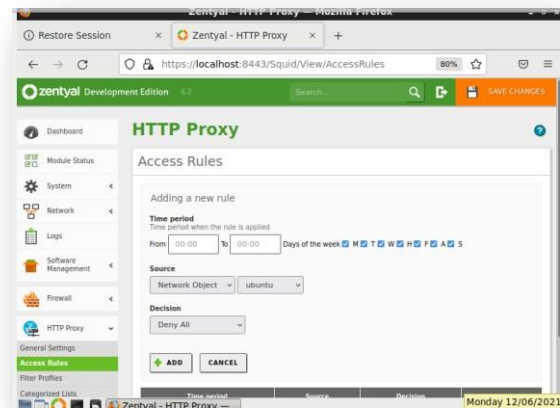
3.2.18 Ahora configuramos el proxy en la máquina del cliente:



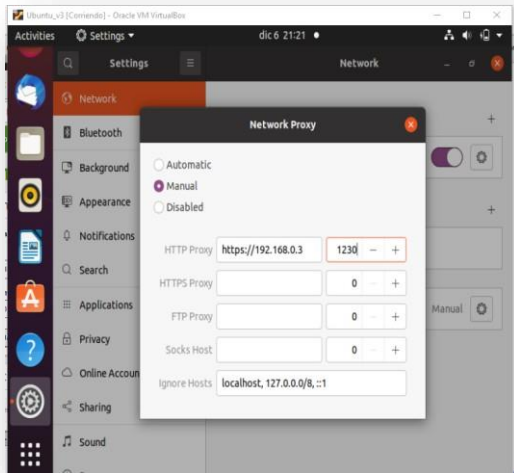
3.2.16 Ahora configuramos el puerto y seleccionamos la opción transparente:



3.2.17 Ahora modificamos el proxy Http y denegamos todo:







### 3.3 CORTAFUEGOS

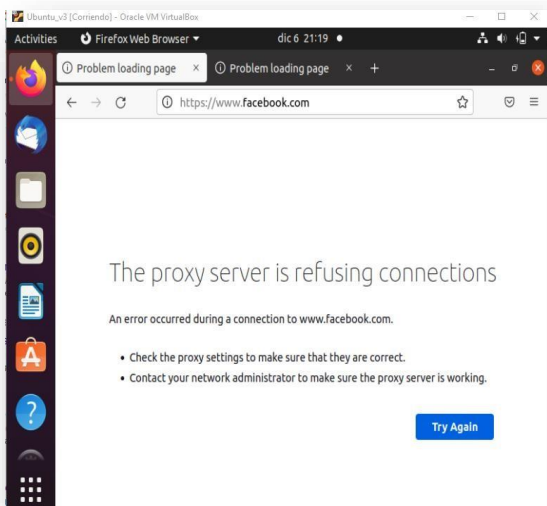
Estudiante: Marxio Alejandro Acero

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.

Paso 1:

Descargamos la ISO de la página oficial <https://zentyal.com/es/news/zentyal-6-2-announcement-2/>

3.2.19 Ingresamos al navegador e intentamos ingresar a una pagina cualquiera y podemos ver el mensaje de acceso denegado:



Paso 2:

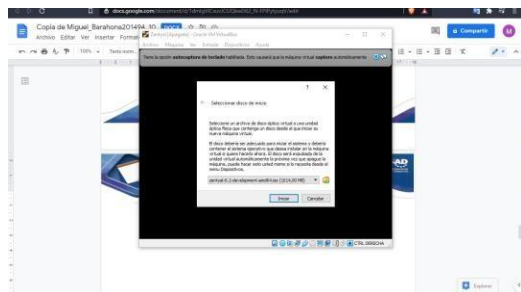
Creamos una máquina virtual llamada Zentyal.



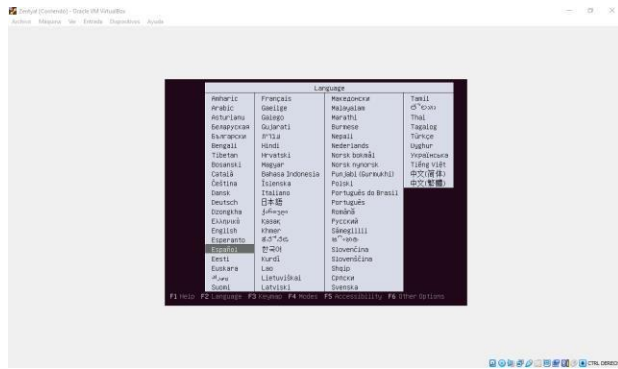
Paso 3:

Arrancamos la máquina virtual.

Paso 4:

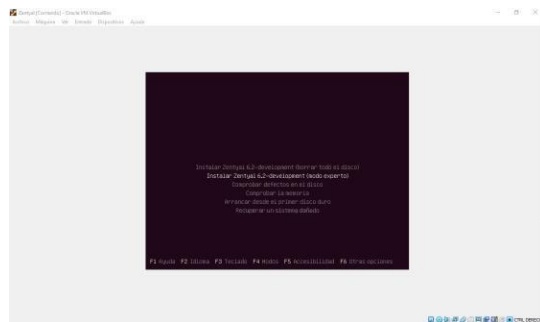


## Seleccionamos el lenguaje "Español"



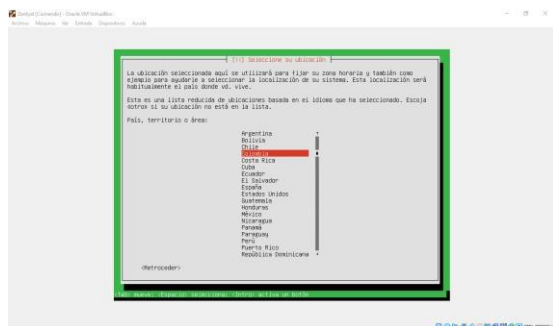
### Paso 5:

Seleccionamos el modo Experto como nos solicita en la guía, este modo nos permite instalar Zentyal Server 6.2 sin entorno escritorio.



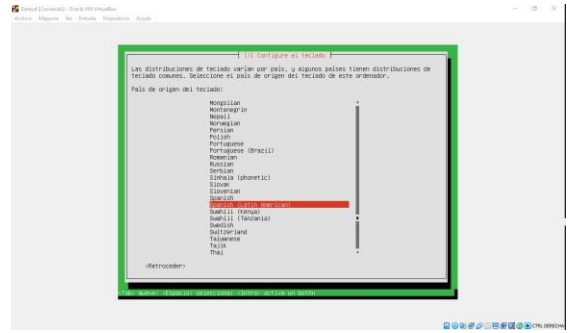
### Paso 6:

Seleccionamos la ubicación Colombia



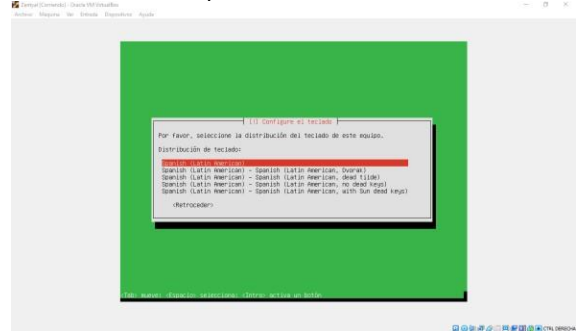
### Paso 7:

Le decimos que No, y se nos visualiza las diferentes configuraciones de teclado.



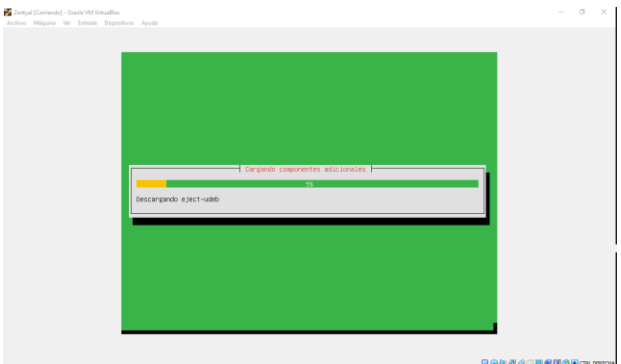
### Paso 8:

Seleccionamos el primero.



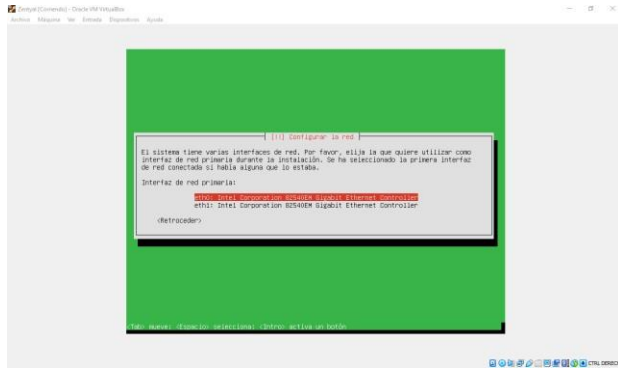
### Paso 9:

Se inicia cargando componentes.



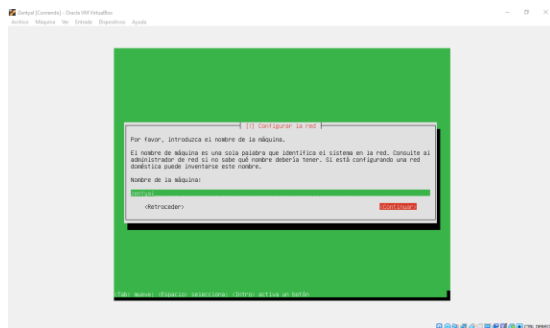
### Paso 10:

Seleccionamos la primera interfaz de red como primaria.



**Paso 11:**

El nombre del *hostname* lo dejamos como *zentyal*.



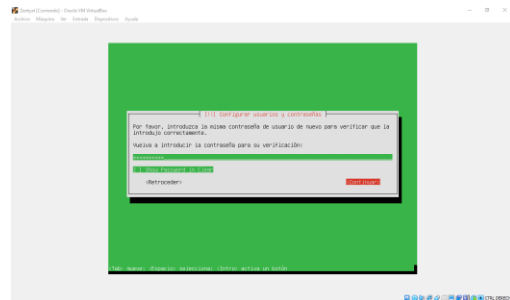
**Paso 12:**

Dejamos el nombre *adm\_miguelbarahona* y le damos clic en continuar.



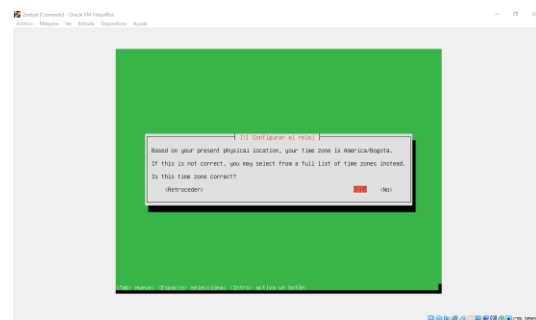
**Paso 15:**

Repetimos la contraseña.



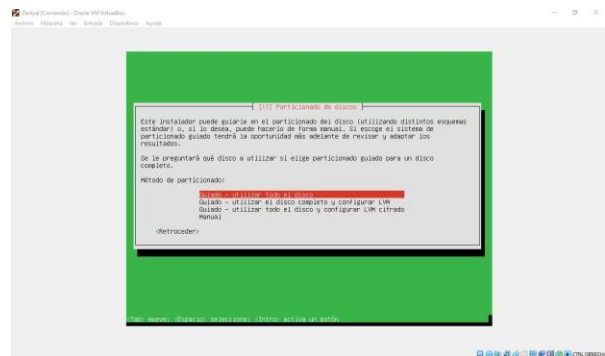
**Paso 16:**

Nuestra zona del reloj es la correcta por lo cual le damos en Sí.



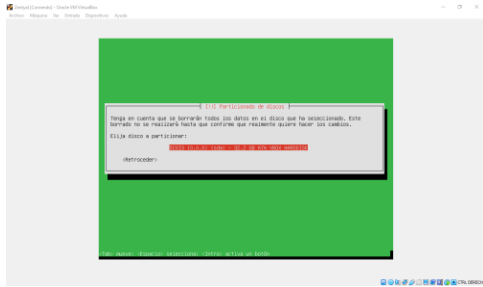
**Paso 17:**

Seleccionamos “Guiado - utilizar todo el disco”.



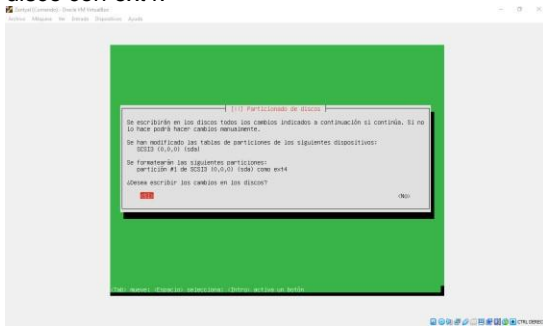
**Paso 18:**

Seleccionamos la partición



**Paso 19:**

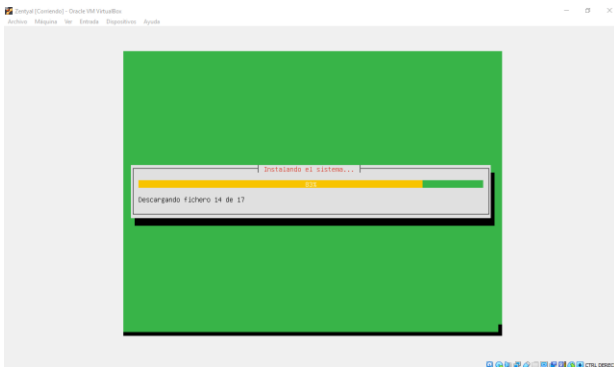
Con base en lo que comenta dejamos que se formatee el disco con ext4.



**Paso 20:**

Le decimos *Sí*, para que no se instale el entorno gráfico

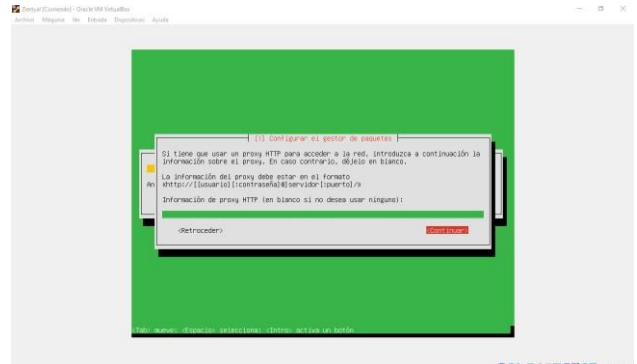
**Paso 21:**  
se realizará la instalación de los paquetes del sistema.



**Paso 22:**

Por ahora no vamos a configurar el proxy, por lo cual lo dejamos en blanco.

**Paso 23:**

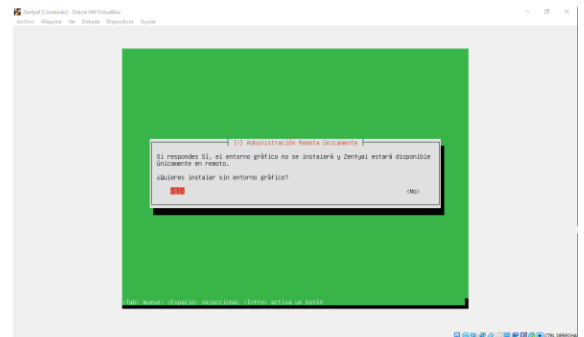


Le decimos que *Sí*, para que instale GRUB en el registro principal donde se encuentra nuestro S.O

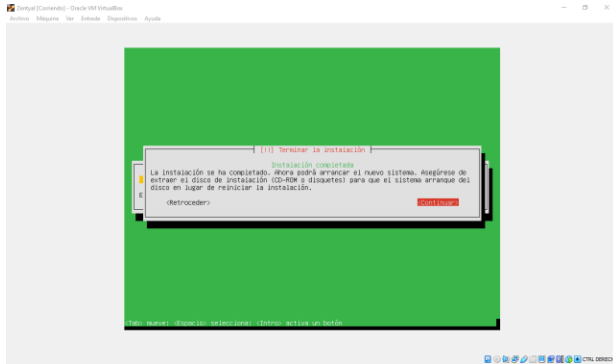


**Paso 24:**

Se termina la instalación y le damos clic en continuar.







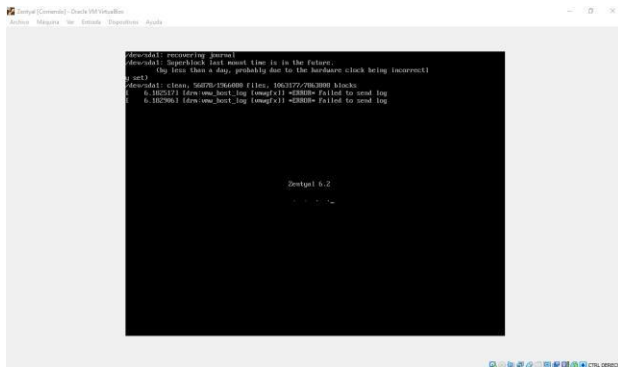
**Paso 25:**

Se nos reiniciará el servidor.



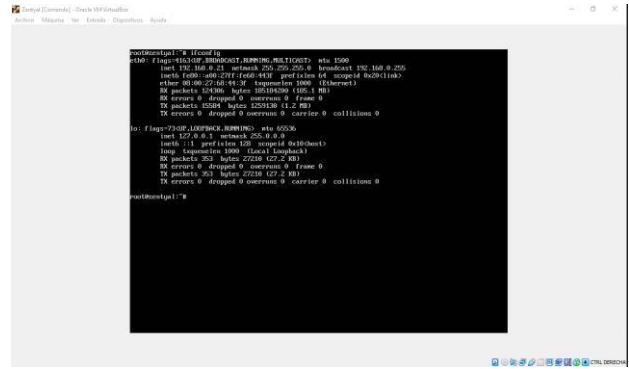
**Paso 26:**

Esperamos la instalación.



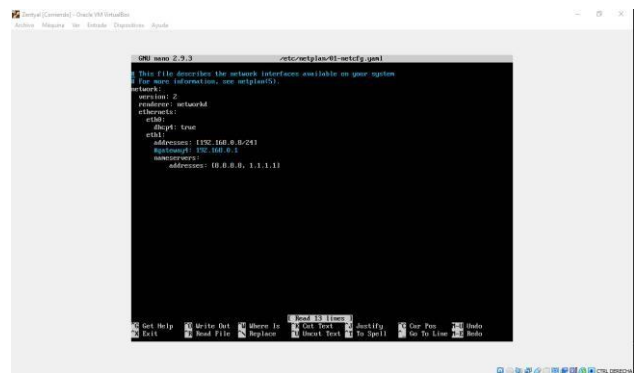
**Paso 27:**

Como en nuestra red nos asigna una IP dinámica debemos configurar nuestra segunda interfaz para que nos podamos conectar por SSH desde el Ubuntu-Desktop.

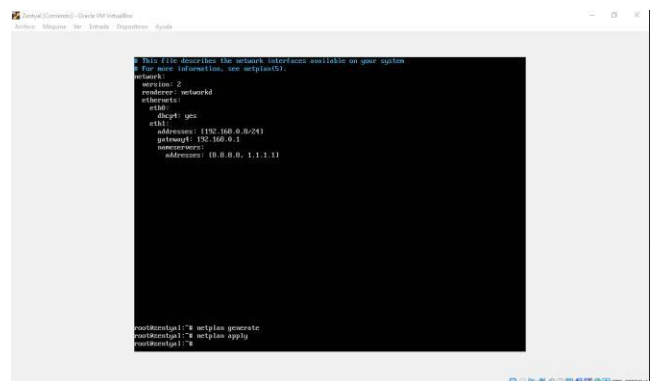


**Paso 28:**

Dejamos la siguiente configuración con el comando nano /etc/netplan/01-netcfg.yaml.



Nota: Para configurar el archivo necesitamos entrar como usuario root con el comando sudo -s. Paso 29: Aplicamos los cambios con el comando netplan generate y netplan apply.



**Paso 30:**

Reiniciamos la máquina con el comando *reboot* revisamos de nuevo nuestras interfaces y se creó la nueva interfaz llamada *eth1*.

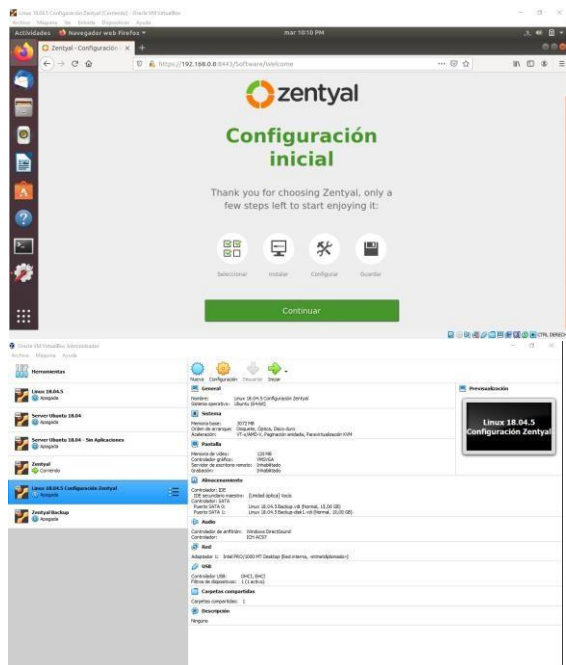
```
root@rootnet1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.21 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:291:fe01:151:1%eth0 prefixlen 64 scopeid 0%eth0
    ether 08:00:27:48:44:3f txqueuelen 1000 (Ethernet)
    RX packets 14 bytes 2280 (2.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 313 (3.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.9 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:291:fe01:151:1%eth1 prefixlen 64 scopeid 0%eth1
    ether 08:00:27:48:44:3f txqueuelen 1000 (Ethernet)
    RX packets 30 bytes 480 (4.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 200 (2.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@rootnet1:~#
```

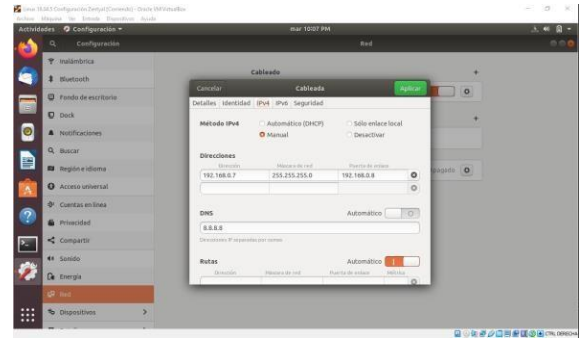
**Paso 31:**

Vamos a duplicar nuestra máquina virtual de ubuntu-desktop con toda la configuración, esto se realiza para que un desktop realice la configuración de Zentyal la máquina se llamó *Linux 18.04.5 Configuración Zentyal*.



**Paso 32:**

Arrancamos la máquina y vamos a configurar la interfaz para que se pueda conectar desde la red interna.



**Paso 33:**

Cuando se apliquen los cambios ingresamos desde browser <https://192.168.0.8:8443>



**Paso 34:**

Nos dan la bienvenida de Zentyal Server 6.2

**Paso 35:**

Damos en continuar y vamos a seleccionar los paquetes *DHCP* y *Firewall*.



**Paso 36:**

Nos informará los siguiente paquetes a instalar le damos clic en *Continuar*.



**Paso 37:**

Esperemos la instalación de los paquetes



**Paso 41:**

Le damos a la opción Configuración.

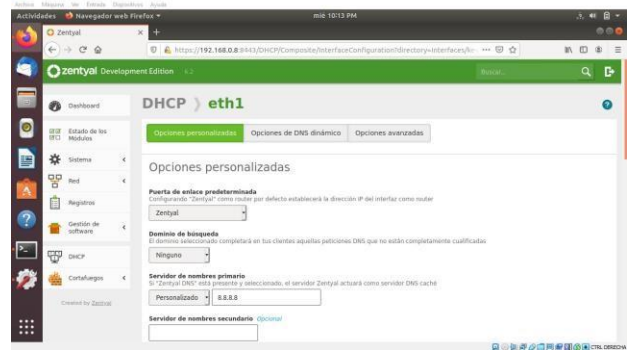


**Paso 39:**

Nos dirigimos a la opción Red → Interfaces y vamos habilitar la red eth0 Método: DHCP y Externo (WAN) y aplicamos los cambios.

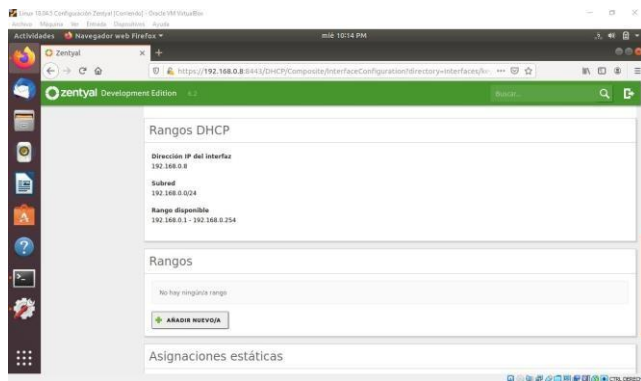
**Paso 42:**

Vamos a dejar la configuración y agregamos los DNS de google por ahora.



**Paso 43:**

Bajamos y nos muestra el rango DHCP.

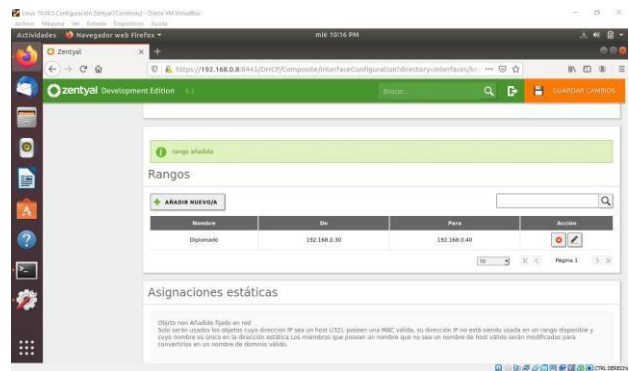


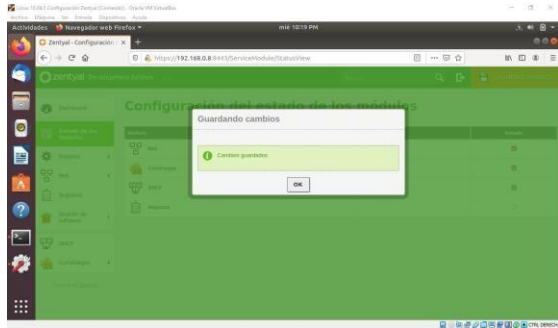
**Paso 40:**

Una vez habilitado nos dirigimos a la opción DHCP.

**Paso 44:**

Vamos añadir un nuevo rango que se llamara "Diplomado" e inicia desde la 192.168.0.30 hasta 192.168.0.40

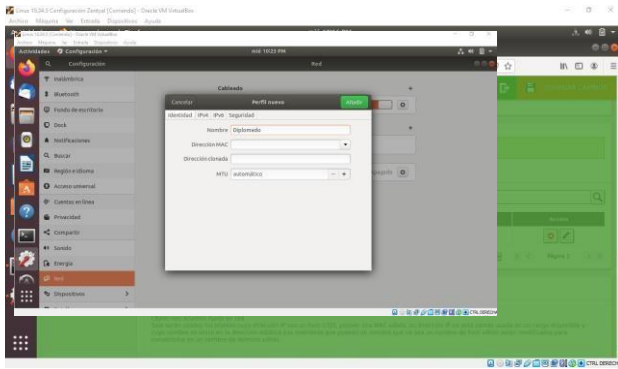




**Paso 45:**

Aplicamos los cambios.

**Paso 46:**



Ahora nos dirigimos a la opción llamada “Estado de los Módulos”.

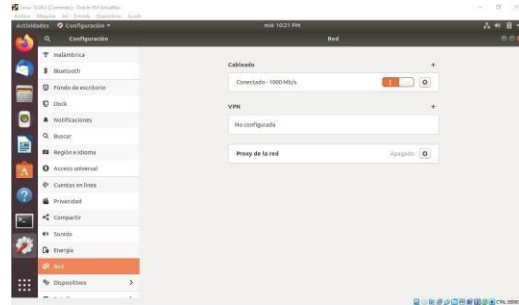


**Paso 47:**

Habilitamos los módulos Red, Cortafuegos y DHCP para que lo aplique sobre el servidor.

**Paso 49:**

Al encender nos dirigimos a la opción de red.

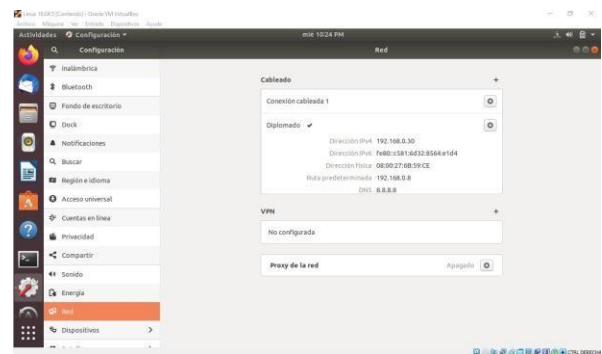


**Paso 50:**

Vamos a crear un nuevo perfil llamado *Diplomado* y dejamos que busque la Ip y el DNS de forma automática.

**Paso 51:**

Al habilitar el nuevo perfil automáticamente busca una Ip y para nuestro caso nos asigno la Ip 192.168.0.30.



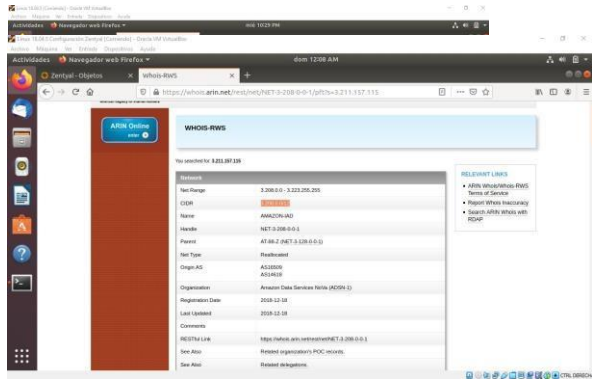
**Paso 53:**

Ahora intentamos navegar a internet desde nuestra máquina ubuntu-desktop llamada Linux 18.04.5.

**Paso 57:**

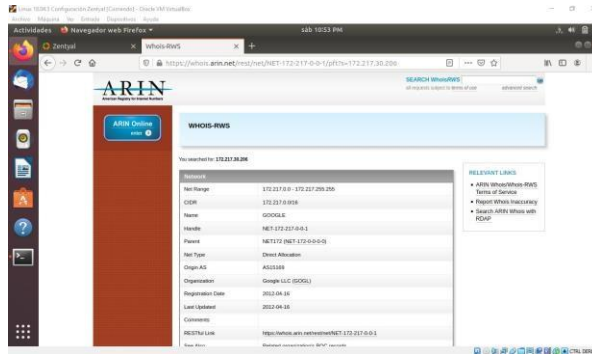
Debemos bloquear portales o sitios web de entretenimiento y redes sociales, para este caso vamos a bloquear Facebook, Telegram, y Netflix, a cada uno vamos a buscar su CIDR (Se basa en el concepto de las máscaras de subred):





Sitio o portal	CIDR
<a href="#">Netflix</a>	3.208.0.0/12 54.144.0.0/12 54.160.0.0/11 54.192.0.0/12 54.208.0.0/13 54.216.0.0/14 54.220.0.0/15 3.224.0.0/12
<a href="#">Facebook</a>	157.240.0.0/16
<a href="#">Telegram</a>	149.154.0.0/16

A continuación realizamos el paso a paso de como obtener el CIDR de Netflix estos pasos lo realizamos para los demás sitios.



Copias las Ip's y buscamos desde la página de Whois (Si contiene más de una como en nuestro caso lo realizamos con cada Ip).

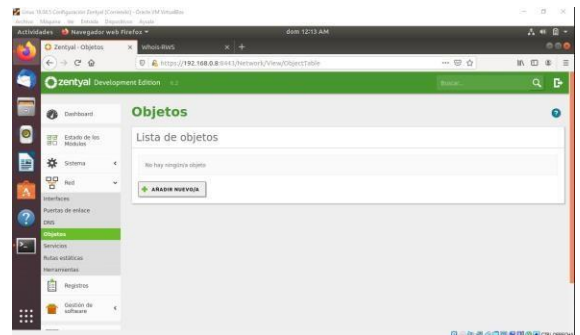


Damos enter y nos arrajara el CIDR (Que se encuentra subrayada):

Netflix

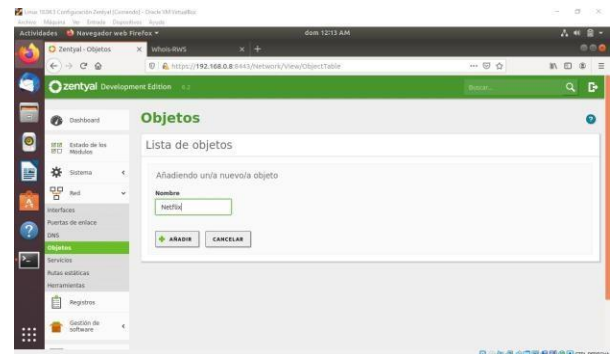
**Paso 1:**

Una vez tenemos los CIDR de Netflix vamos a la opción Red → Objetos.



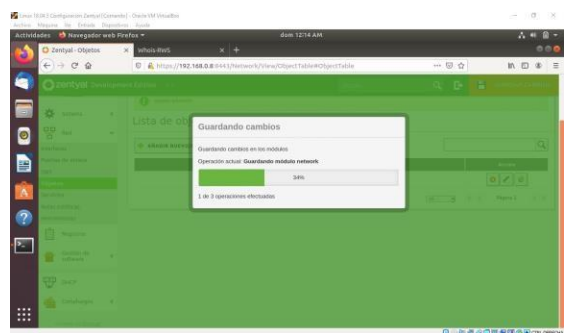
**Paso 2:**

Damos clic en Añadir y Colamos como nombre Netflix.



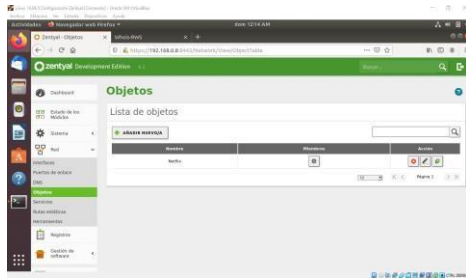
**Paso 3:**

Damos clic en Guardar Cambios.



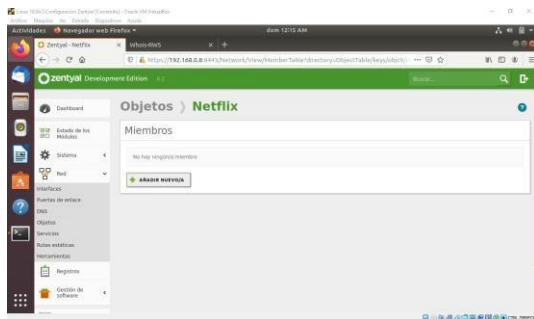
**Paso 4:**

Damos clic en la opción Miembros.



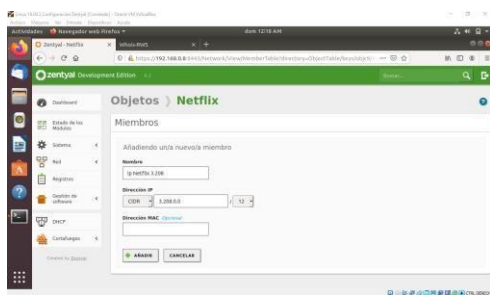
**Paso 5:**

Damos clic en Añadir Nuevo/a.



**Paso 6:**

Como nombre colocamos Ip Netflix (Inicio Ip) y colocamos la dirección Ip que tenemos en la tabla.



Realizamos lo mismo con las demás

**Paso 7:**

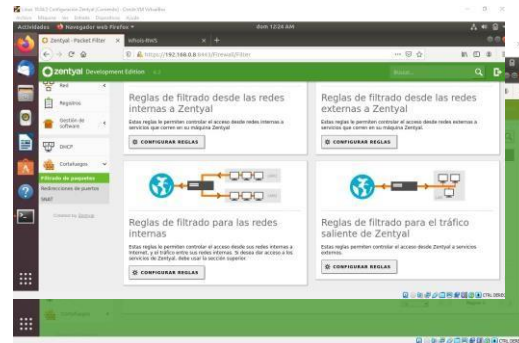
Una vez se añade damos clic en Guardar Cambios.

**Paso 8:**

Ahora nos dirigimos a la opción Cortafuegos → Filtrado de paquetes.

**Paso 9:**

Como nuestra máquina Linux 18.04.5 está conectada con Red Interna seleccionamos la opción “Reglas de filtrado para las redes internas”.



**Paso 10:**

Damos clic en Añadir Nuevo



**Paso 11:**

Vamos a dejar las siguientes opciones:

Decisión: Denegar

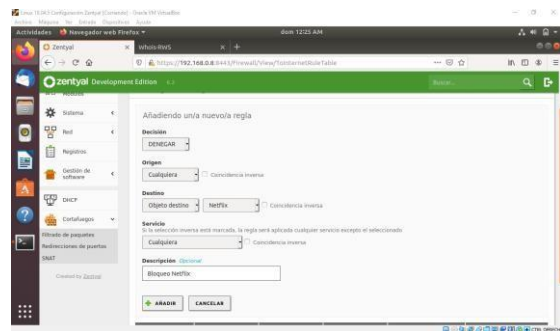
Origen: Cualquiera (Petición desde cualquier equipo que esté conectado sobre nuestra red interna)

Destino: Seleccionamos Objeto destino → Netflix

Servicio: Cualquiera (Ejemplo: TCP, HTTP, HTTPS, etc.).

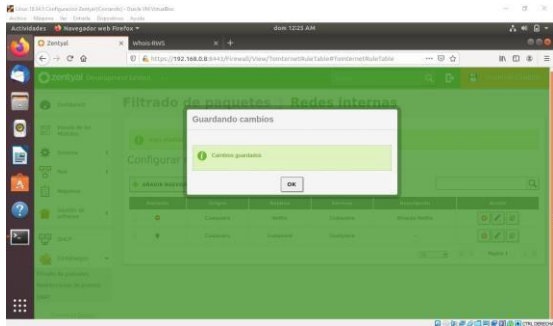
Descripción: Bloqueo Netflix.

Damos clic en Añadir.



**Paso 12:**

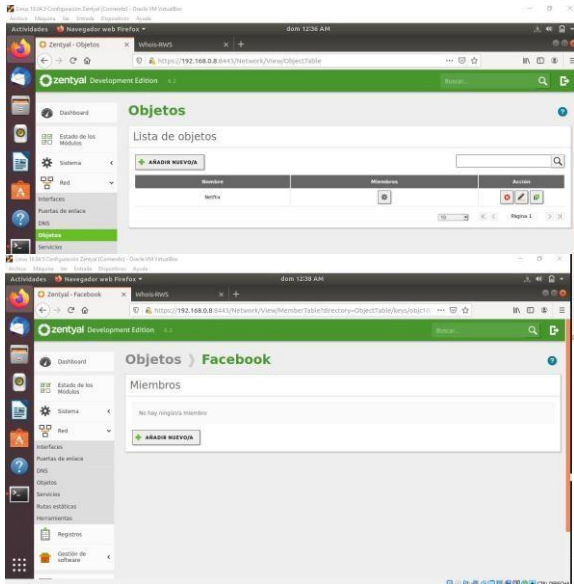
Guardamos cambios para que se apliquen.



**Facebook**

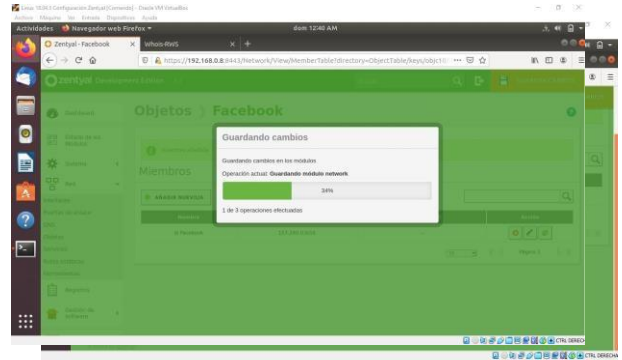
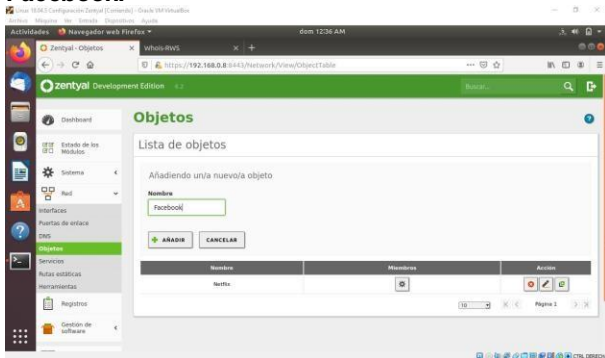
**Paso 1:**

Una vez tenemos el CIDR de Facebook vamos a la opción Red → Objetos.



**Paso 2:**

Damos clic en Añadir y Colamos como nombre **Facebook**.

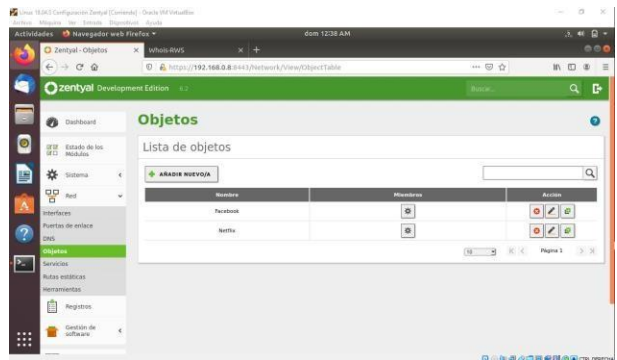


**Paso 3:**

Damos clic en Guardar Cambios.

**Paso 4:**

Damos clic en la opción Miembros.

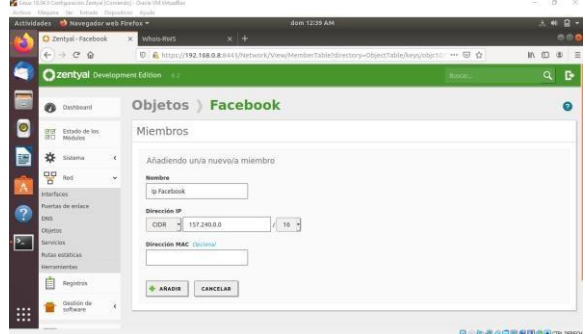


**Paso 5:**

Damos clic en Añadir Nuevo/a.

**Paso 6:**

Como nombre colocamos *Ip Facebook* y colocamos la dirección Ip que tenemos en la tabla.

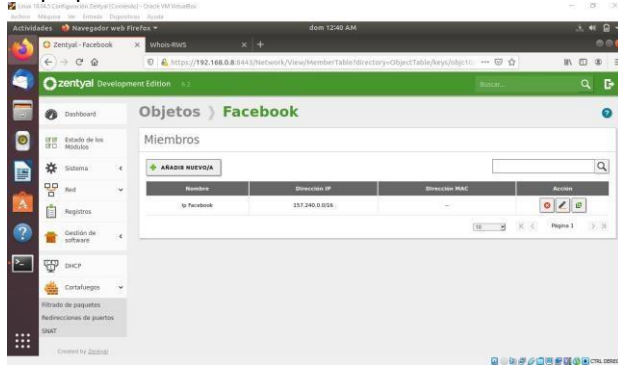


**Paso 7:**

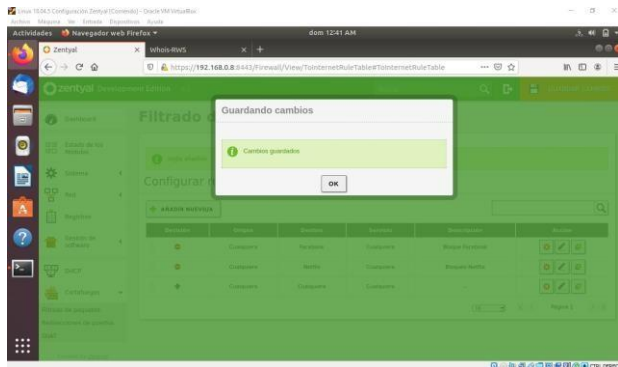
Una vez se añada damos clic en *Guardar Cambios*.

**Paso 8:**

Ahora nos dirigimos a la opción Cortafuegos → Filtrado de paquetes.



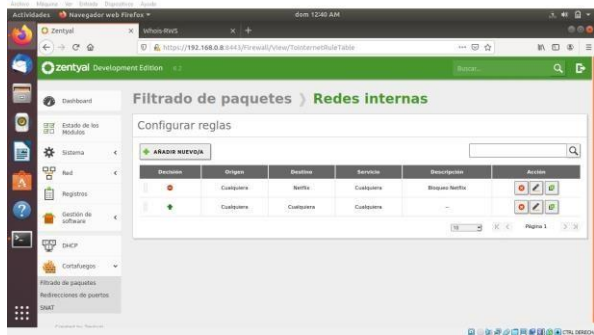
**Paso 9:**



Como nuestra máquina Linux 18.04.5 está conectada con Red Interna seleccionamos la opción “Reglas de filtrado para las redes internas”.

**Paso 10:**

Damos clic en Añadir Nuevo/a.



**Paso 11:**

Vamos a dejar las siguientes opciones:

Decisión: Denegar

Origen: Cualquiera (Petición desde cualquier equipo que esté conectado sobre nuestra red interna)

Destino: Seleccionamos Objeto destino → Facebook  
 Servicio: Cualquiera (Ejemplo: TCP, HTTP, HTTPS, etc.).  
 Descripción: Bloqueo Facebook.  
 Damos clic en Añadir.



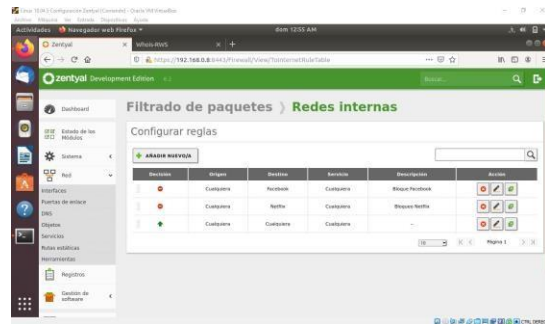
**Paso 12:**

Guardamos cambios para que se apliquen.

Telegram

**Paso 1:**

Una vez tenemos el CIDR de Telegram vamos a la opción Red → Objetos.



**Paso 2:**

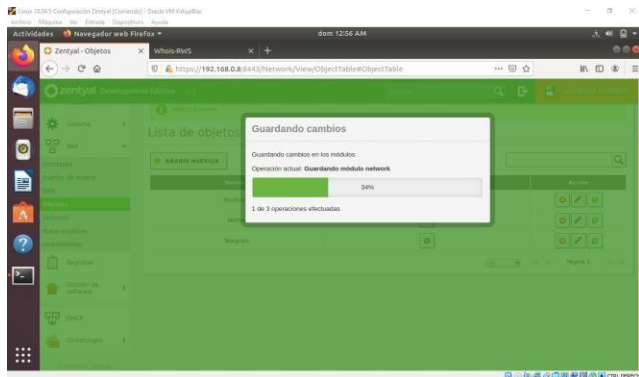
Damos clic en Añadir y Colamos como nombre *Telegram*.





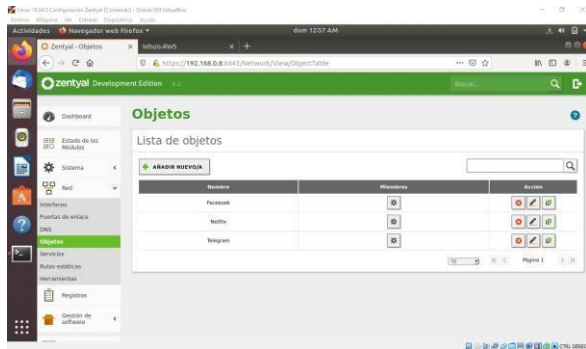
**Paso 3:**

Damos clic en Guardar Cambios.



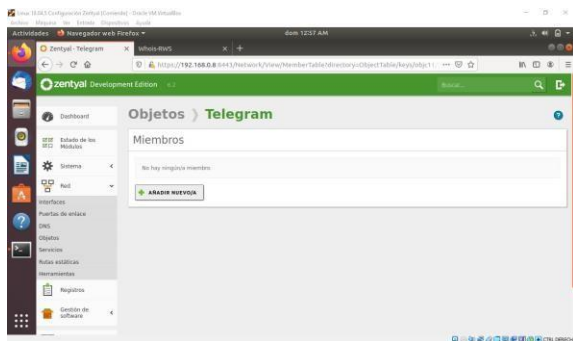
**Paso 4:**

Damos clic en la opción Miembros.



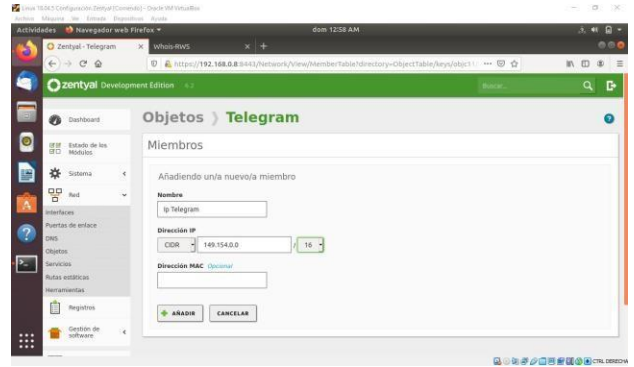
**Paso 5:**

Damos clic en Añadir.



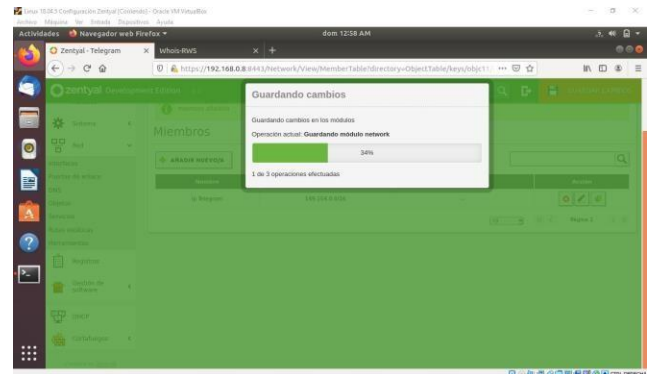
**Paso 6:**

Como nombre colocamos *Ip Telegram* y colocamos la dirección Ip que tenemos en la tabla.



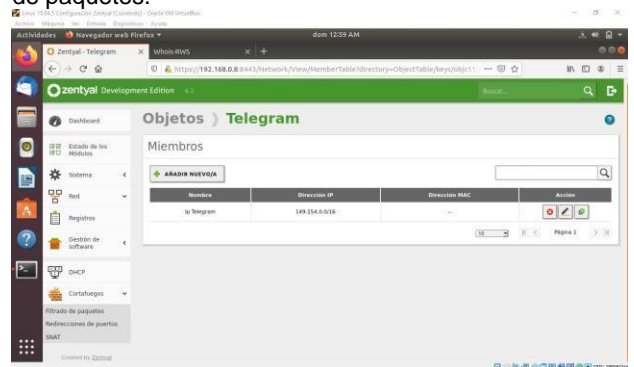
**Paso 7:**

Una vez se añada damos clic en Guardar Cambios.



**Paso 8:**

Ahora nos dirigimos a la opción Cortafuegos → Filtrado de paquetes.



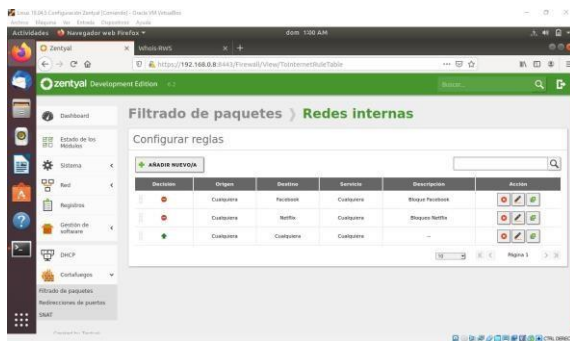
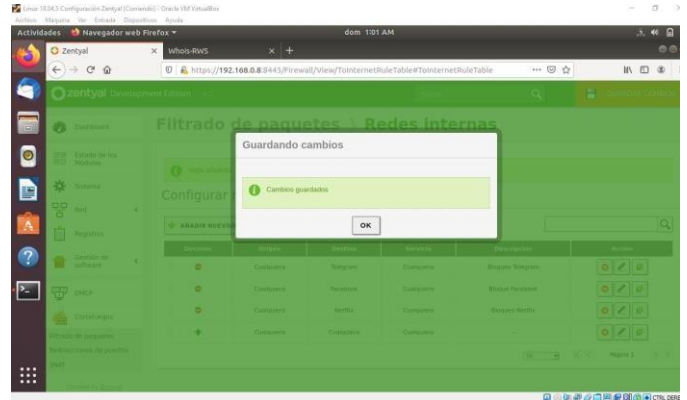
**Paso 9:**

Como nuestra máquina Linux 18.04.5 está conectada con Red Interna seleccionamos la opción "Reglas de filtrado para las redes internas".

**Paso 10:**



Damos clic en Añadir Nuevo/a.

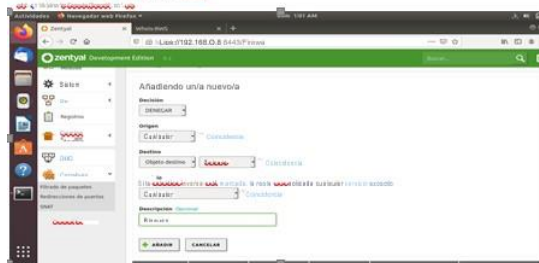


### Paso 11:

Vamos a dejar las siguientes opciones:

Decisión: Denegar

Origen: Cualquiera (Petición desde cualquier equipo que esté conectado sobre nuestra red interna)  
 Destino: Seleccionamos Objeto destino → Telegram  
 Servicio: Cualquiera (Ejemplo: TCP, HTTP, HTTPS, etc.).  
 Descripción: Bloqueo Telegram.  
 Damos clic en Añadir.



### Paso 12:

Guardamos cambios para que se apliquen.

## 3.4. FILE SERVER Y PRINT SERVER

### Temática 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.

#### Definición de file server y print server

Un file server (o servidor de archivos) es un servidor central de una red de ordenadores, que pone a disposición del cliente conectado un conjunto de archivos o parte del mismo. De este modo, el servidor de archivos proporciona a los usuarios un lugar de almacenamiento centralizado para los archivos en sus propios soportes de datos, disponible para todos los clientes autorizados. El administrador del servidor establece unas directrices estrictas para determinar qué usuarios tienen derechos de acceso y a qué datos: por ejemplo, configurando el sistema u otorgando los permisos del sistema de archivos, se puede determinar qué carpetas puede ver y abrir un usuario o grupo de usuarios concreto y si los archivos solo son visibles o también pueden guardarse, modificarse o eliminarse.

#### 3.4.1 Vamos a realizar la descarga de zentyal para luego instalar en nuestra maquina virtual



Imagen 1 Descarga de zentyal

#### 3.4.2 Una vez descargamos la iso de zentyal se procede a realizar la creación de la máquina virtual

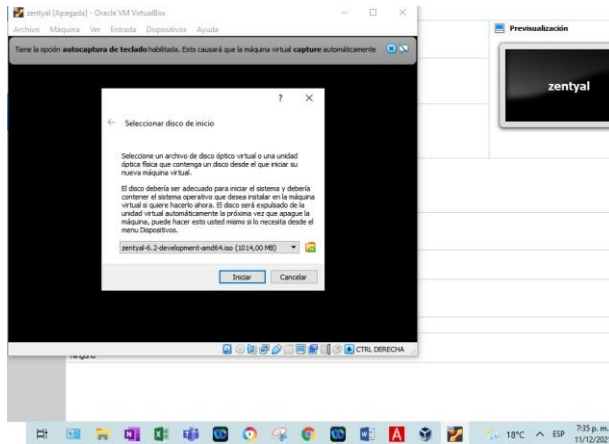


Imagen 2 Instalación de zentyal en máquina virtual

### 3.4.3 Dentro del proceso de instalación seleccionamos el idioma

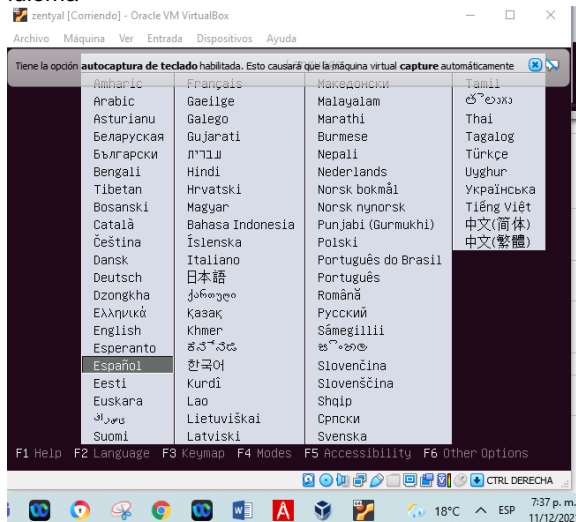


Imagen 3 Proceso de Instalación selección idioma

### 3.4.4 Se realizan todos los pasos de instalación y de configuración de zentyal en nuestra máquina virtual

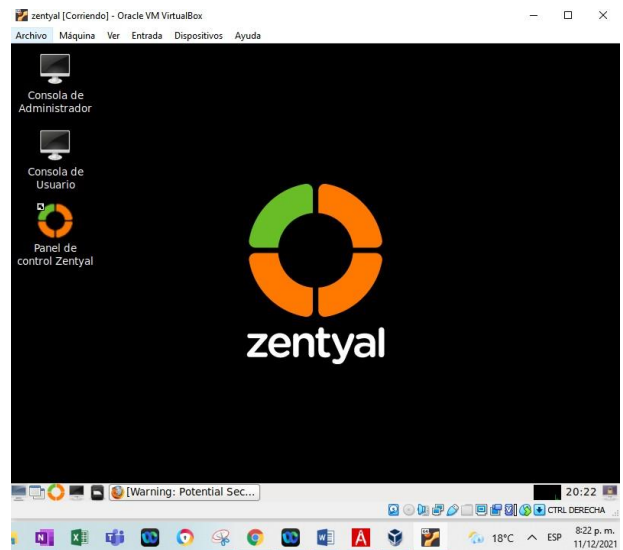


Imagen 4 Confirmación de la instalación finalizada

### 3.4.5 Debemos ingresar al panel de control de zentyal para verificar que se tengan instalados los módulos

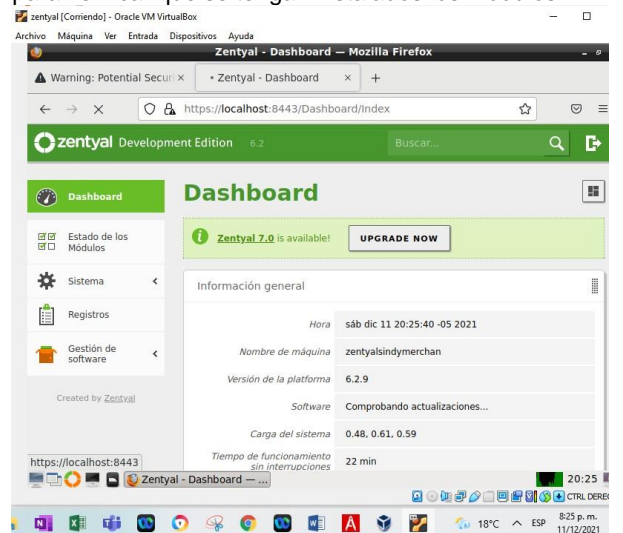


Imagen 5 Estado de módulos

### 3.4.6 Se realiza la instalación de los módulos que se requieren para desarrollar la actividad

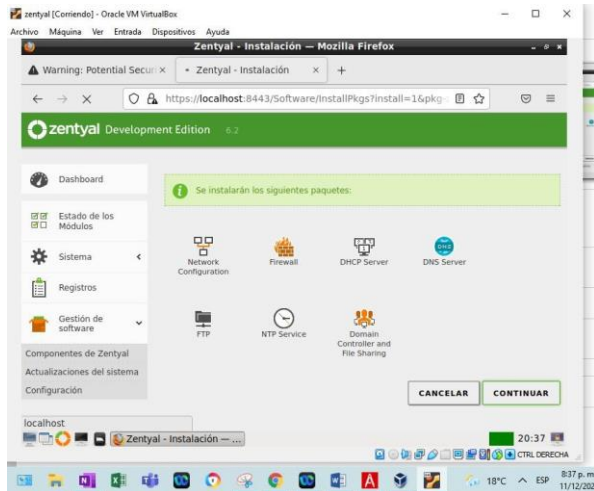


Imagen 6 instalación de módulos

3.4.7 Una vez instalados los módulos se debe ingresar en la opción estado de los módulos y activarlos

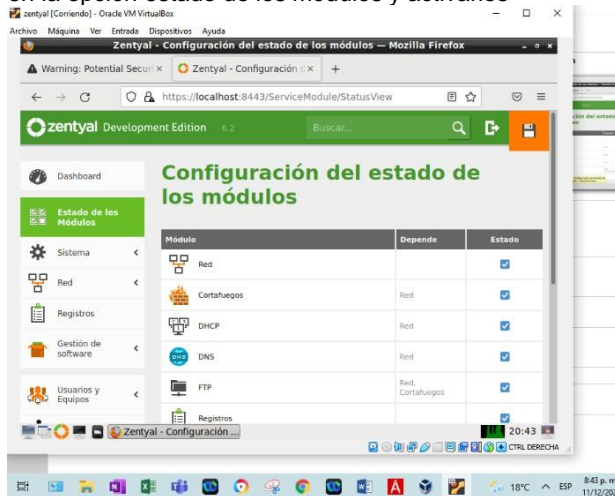


Imagen 7 Módulos activos

3.4.8 En la opción de dominio debemos validar que el dominio se encuentre habilitado por que el controlador de dominio nos permite identificar todos los usuarios autorizados, equipos y recursos. Adicionalmente que resuelve todo lo relacionado con las IP's.

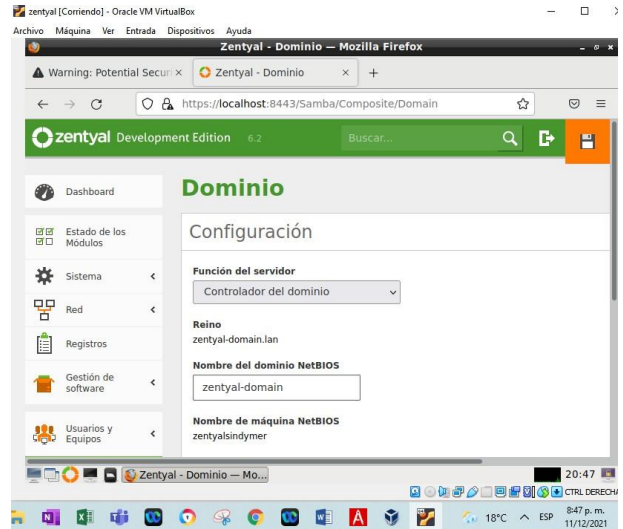


Imagen 8 Controlador de dominio

3.4.9 Ya como nuestro módulo de controlador de dominio debemos ingresar en la opción de usuarios y equipos y nos cargara la información

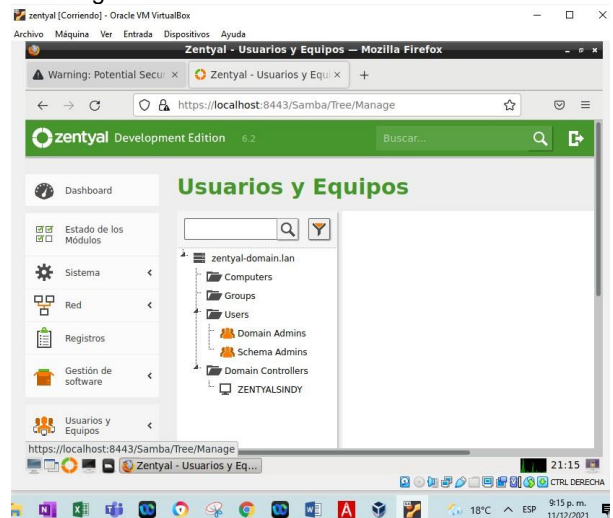


Imagen 9 usuarios y equipos

3.4.10 Ahora se procede a crear un usuario que va a ser el usuario administrador



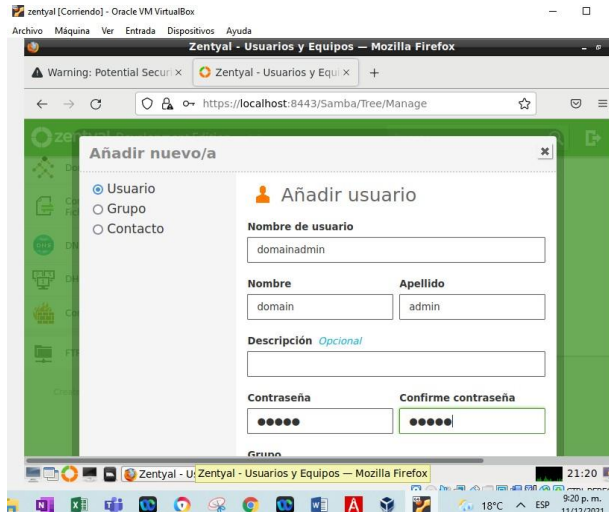


Imagen 10 usuario domainadmin

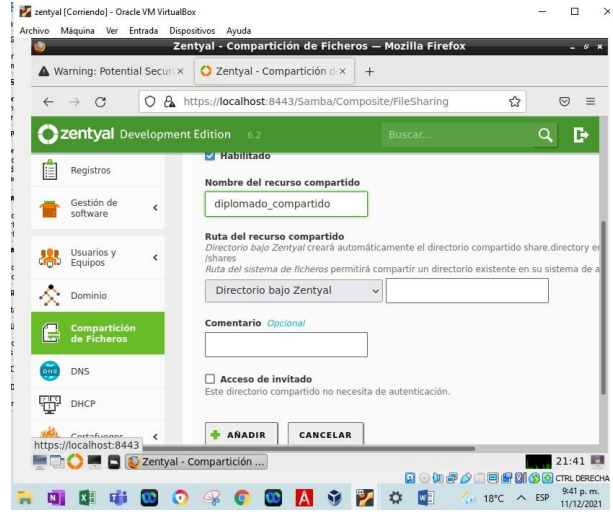


Imagen 12 Creación del fichero

3.4.11 Ahora vamos a ingresar a una máquina virtual Windows y la vamos a unir al dominio

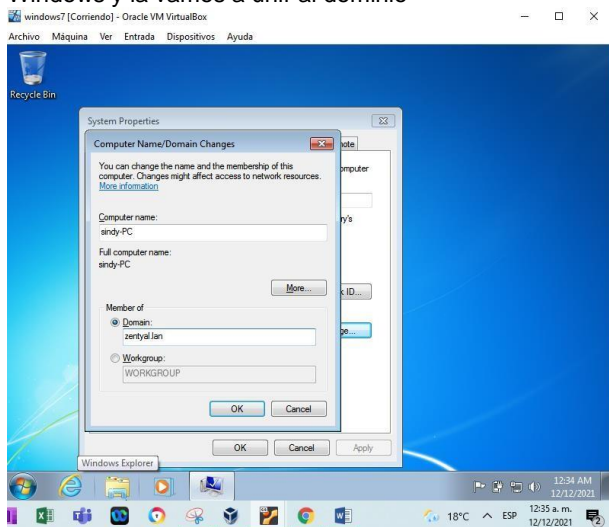


Imagen 11 dominio en windows

3.4.14 Ahora establecemos a que usuario le queremos dar el acceso a la carpeta creada y con qué permisos para eso ingresamos en control de acceso y le damos añadir nuevo y seleccionamos el usuario y el permiso.

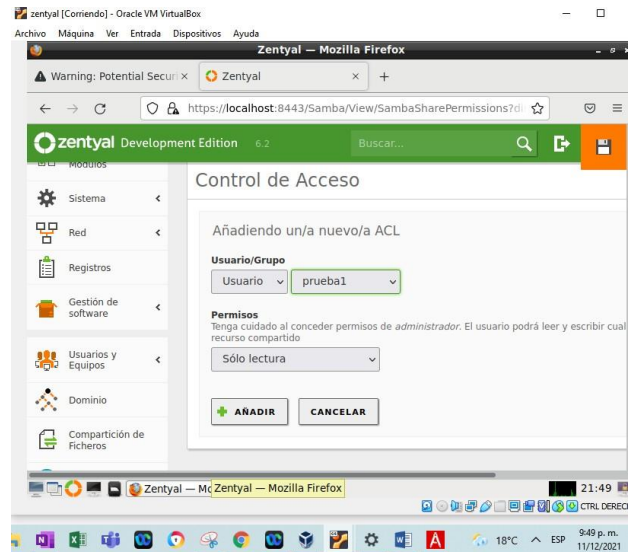


Imagen 13 acceso de usuario a carpeta

3.4.12 En este paso nos pide el usuario y la contraseña de zentyal

3.4.13 En este paso vamos a ingresar al módulo de ficheros donde realizare la creación de un directorio

3.4.15 Asignación de dirección IP al servidor  
Para esto debemos revisar la ip de zentyal

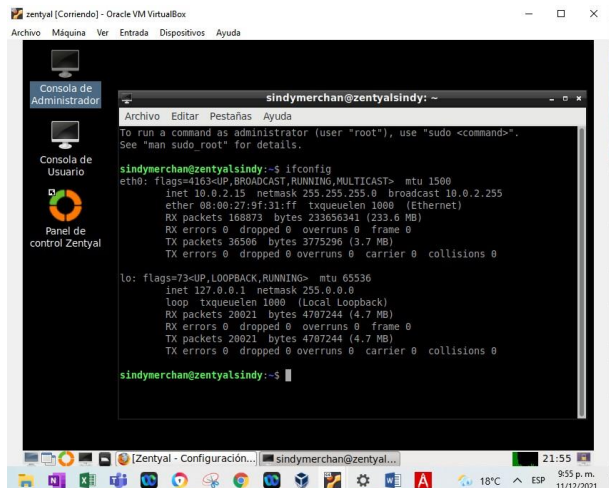


Imagen 14 Validación IP

### 3.5 VPN

#### 3.5.1 Ingreso al programa (Configuración inicial)

En este punto nos lleva a asistente que nos permitirá elegir que deseamos instalar y que no.



Imagen . Verificación de rutas de salida de Zentyal.

#### 3.5.2 Instalación del programa (Verificación conexión a internet)

Para motivos de nuestro taller, debemos verificar que se tenga acceso a internet. (Se verifica la conexión de red, se debe configurar adaptador de puente desde virtual box).



Imagen 73. Verificación de rutas de salida de Zentyal.

#### 3.5.3 Instalación del programa

Resumen de los servicios instalados actualmente en nuestra máquina, para nuestro caso que debemos instalar el servicio de VPN, Seleccionamos VPN y le damos clic al botón instalar

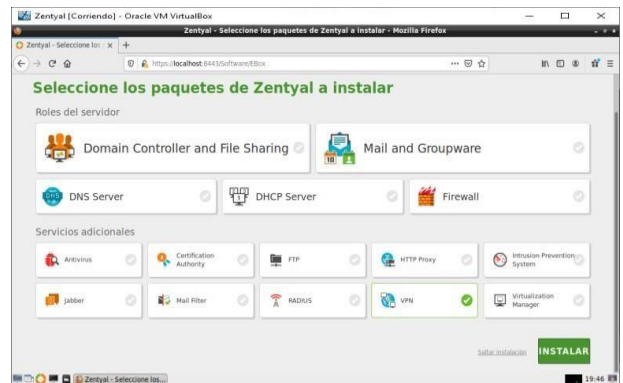


Imagen 74. Verificación de rutas de salida de Zentyal.

#### 3.5.4 Instalación del programa

Se muestra el resumen de los paquetes que vamos a instalar.

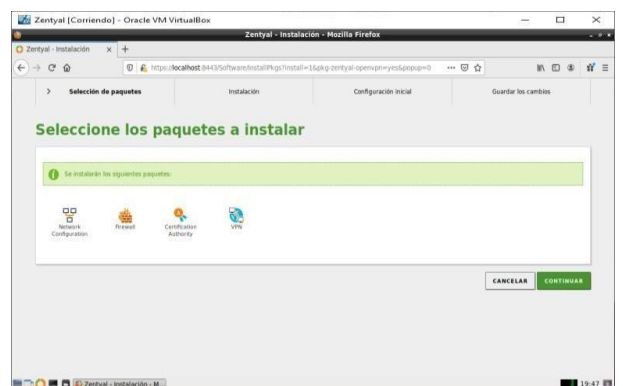


Imagen 75. Verificación de rutas de salida de Zentyal.

#### 3.5.5 Instalación del programa (Actualizaciones)

Una vez instalado nuestro servidor se recomienda hacer actualizaciones al software para verificar programas obsoletos o nuevas versiones de los mismos.

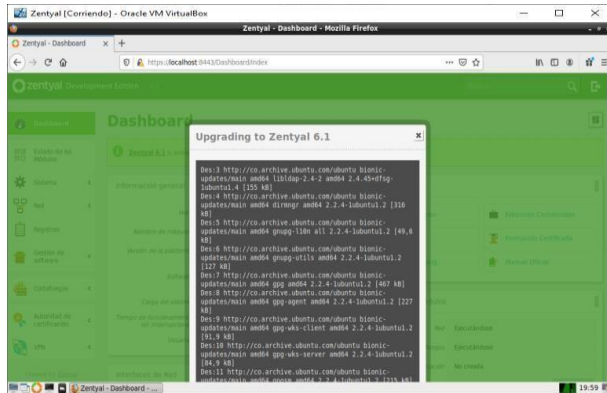


Imagen 76. Verificación de rutas de salida de Zentyal.

### 3.5.6 Instalación del programa (interfaces de red)

Para nuestro ejemplo práctico como no se tiene acceso al firewall, se hará la simulación de ingreso de la VPN por medio de 2 redes diferentes, para eso se configura una ip por la eth0 (172.20.7.12) y la otra ip por la eth1 (192.168.1.1)

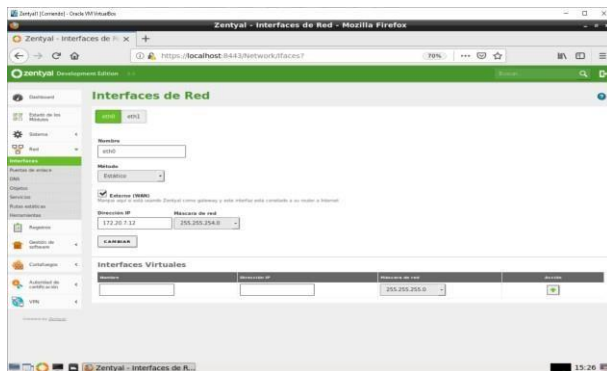


Imagen 77. Verificación de rutas de salida de Zentyal.

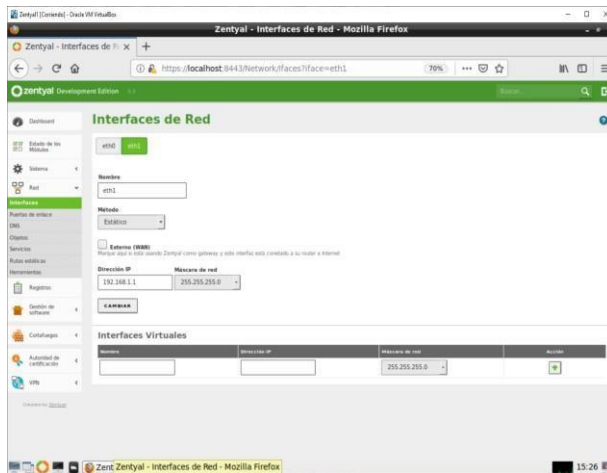


Imagen 78. Verificación de rutas de salida de Zentyal.

3.5.7 Instalación del programa (server VPN) Se crea un servidor VPN, se le coloca un nombre con el cual lo identificaremos.

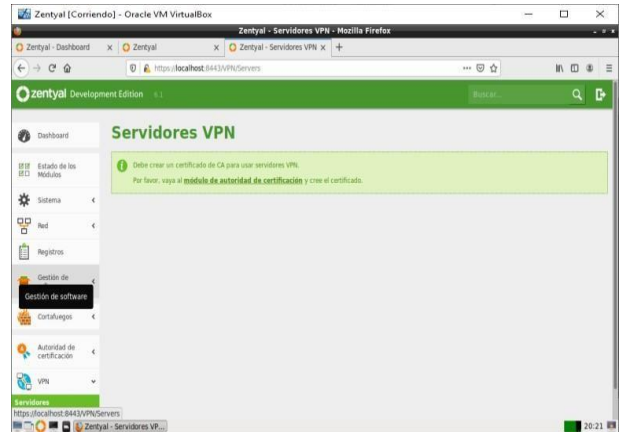


Imagen 79. Verificación de rutas de salida de Zentyal.

### 3.5.8 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina. En este punto tenemos las 2 máquinas Ubuntu con ip 192.168.1.2 y zentyal con ip 172.20.7.12, se ubican en 2 redes diferentes

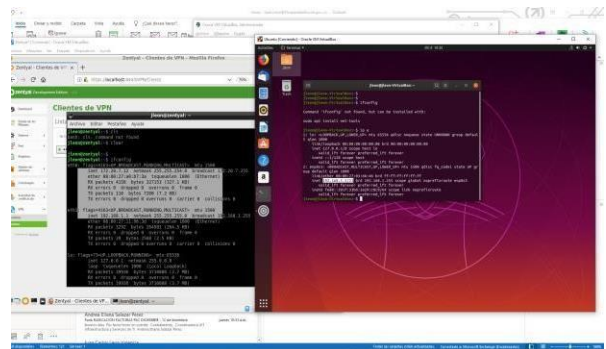


Imagen 80. Verificación de rutas de salida de Zentyal.

### 3.5.9 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.

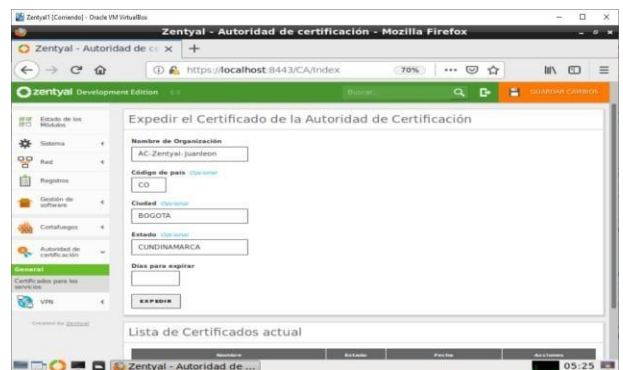


Imagen 81. Verificación de rutas de salida de Zentyal.

### 3.5.10 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.



Imagen 82. Verificación de rutas de salida de Zentyal.

### 3.5.11 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.

### 3.5.12 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.



Imagen 83. Verificación de rutas de salida de Zentyal.

### 3.5.16 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.

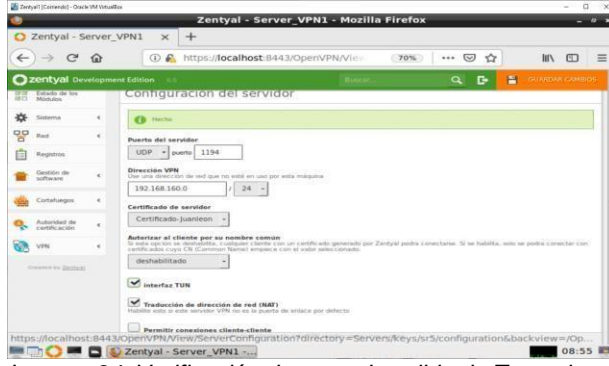


Imagen 84. Verificación de rutas de salida de Zentyal.

Se elige la ip, el Certificado que se acabó de crear y se activa la opción de Interfaz tun

### 3.5.14. Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.

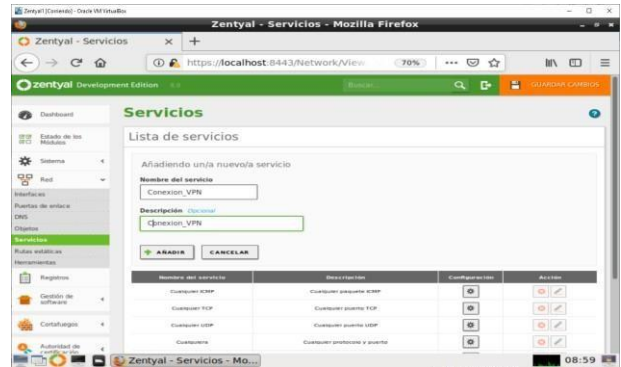


Imagen 85. Verificación de rutas de salida de Zentyal

Se debe crear el servicio para poder establecer la conexión a las VPNS

### 3.5.15 Instalación del programa

Se muestra el asistente de instalación, Nombre que le pondremos a nuestra máquina.

Luego de Crear el servicio, se debe configurar, para nuestro caso como se dejó por defecto, se usará el puerto 1194

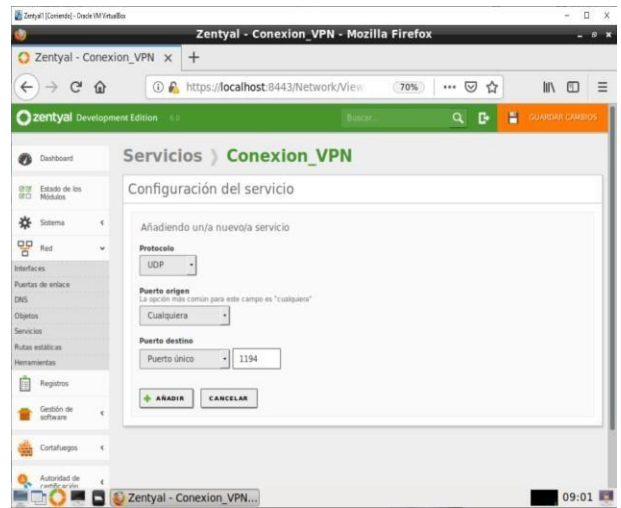


Imagen 86. Verificación de rutas de salida de Zentyal.

### 3.5.17 Instalación del programa (Packet filter)

En este punto se debe configurar las políticas de acceso para la conexión.



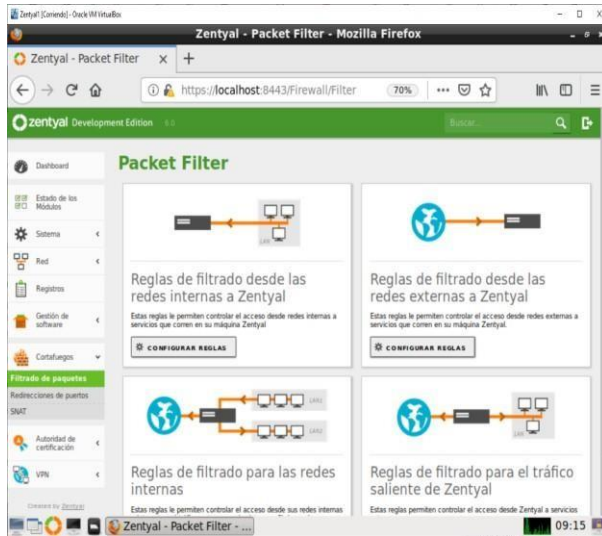


Imagen 87. Verificación de rutas de salida de Zentyal.

### 3.5.18 Instalación del programa

Se muestra el asistente de configuración de los servicios de firewall, que acabamos de guardar.

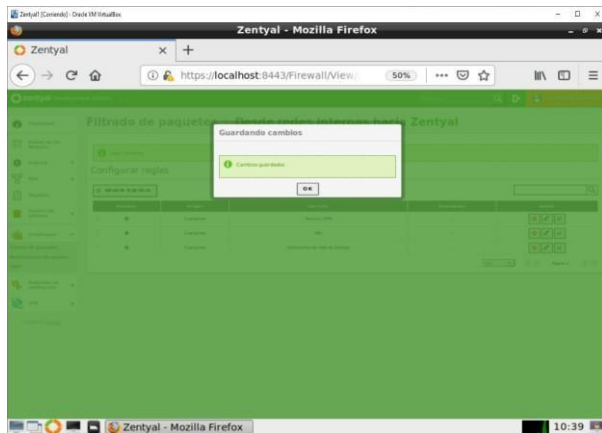


Imagen 88. Verificación de rutas de salida de Zentyal.

### 3.5.19 Dashboard de Resumen

Se muestra la tabla donde se hace el resumen de los servicios que se están ejecutando.

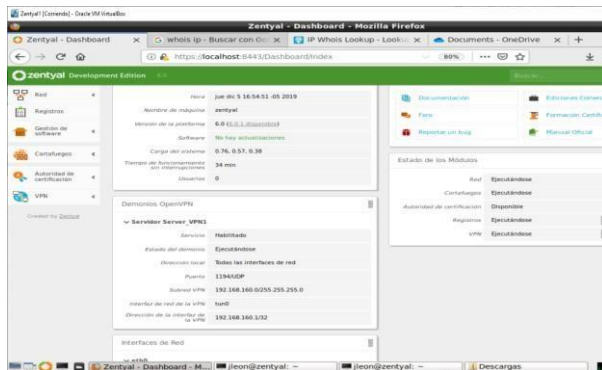


Imagen 89. Verificación de rutas de salida de Zentyal.

### 3.5.20 Configuración de VPN

Se debe configurar desde la opción de OpenVPN.

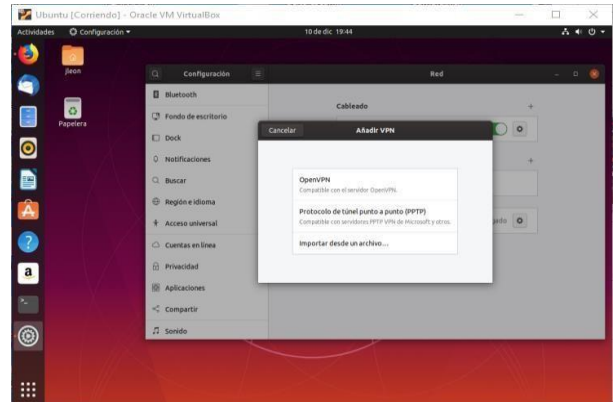


Imagen 90. Verificación de rutas de salida de Zentyal.

### 3.5.21 Configuración de VPN

En este punto se deben ingresar los datos que se habían configurado anteriormente (Gateway), así como el certificado que se generó y descargó, usuario y password.

## 4 CONCLUSIONES

Zentyal (Edición Gratuita) es un compendio de paquetes que se puede denominar todo en 1, que cuenta con gran cantidad de herramientas para entornos de producción de pequeñas y medianas empresas, y que se presenta como otra opción con un costo menor, ofrece el mismo o mejor rendimiento que las soluciones ya conocidas y populares de otros fabricantes,

Todo el entorno de Zentyal es manejado por asistente que es muy intuitivo, permitiendo hacer grandes y complejas configuraciones con tan solo un par de clics.

Es importante resaltar que existen soluciones alternas a las presentadas por Microsoft y a un menor costo,

Las herramientas que ofrece el servidor zentyal son muy completas y ofrecen una gran ayuda, dando todos los servicios de configuración y control en el entorno de red para el control total de los usuarios.

La conexión VPN permite crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet.

El firewall de Zentyal está basado en Netfilter, un framework del núcleo de Linux que permite interceptar y manipular paquetes de la red

El firewall de Zentyal provee una interfaz gráfica que permite el filtrado de paquetes según el flujo de los paquetes.

El firewall de Zentyal permite específicamente definir políticas para la entrada y salida de paquetes desde



Zentyal al router de internet, o de entrada y salida desde Zentyal a la red interna (o a los otros servidores).

El DHCP server es un método eficiente para asignar direcciones IP o reservarlas para MAC específicas.

Zentyal simplifica el proceso de lograr que los usuarios de determinados grupos tengan permiso y acceso mediante el Proxy.

Zentyal ofrece una alternativa DNS para la resolución de nombres para no tener que depender de las DNS de google.

Para compartir una impresora de nuestra red, permitiendo o denegando el acceso a usuarios y grupos para su uso, debemos tener accesibilidad a dicha impresora desde la máquina que contenga Zentyal ya sea por conexión directa, puerto paralelo, USB, o a través de la red local.

El proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador.

Zentyal es un servidor muy completo el cual nos permite realizar las configuraciones necesarias para proporcionar a nuestra red la seguridad suficiente para que no se acceda a paginas no deseadas, lo cual es muy útil en entornos educativos o empresariales en general, ya que este tipo de configuraciones son bastante útiles para proteger la información de las organizaciones.

## 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/>