
INSTALACIÓN Y CONFIGURACION DEL S.O ZENTYAL SERVER 6.2 PARA DISPONER DE LOS SERVICIOS DE INFRAESTRUCTURA IT

Andrés Camilo Leal Ramos
e-mail: aclear@unadvirtual.edu.co
Laura Vanessa Vanegas Rivas
e-mail: lvvanegasr@unadvirtual.edu.co
Lewis Michelly Perez Calderón
e-mail: Imperezcal@unadvirtual.edu.co
Julieth Daniela Rodríguez Manrique
e-mail: jdromiguezman@unadvirtual.edu.co
Mileidy Medina Pajoy
e-mail: mmedinapa@unadvirtual.edu.co

RESUMEN: *El presente trabajo muestra una solución basada en GNU/Linux a través de la instalación, configuración y puesta en marcha de Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT que permiten dar Solución a necesidades específicas. Se implementó bajo el Zentyal Server servicios de gestión de infraestructura IT como DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, cortafuegos, VPN, File Server y Print Server.*

PALABRAS CLAVE: Cortafuegos, Debian, DHCP, DNS, Dominio, GNU/Linux, Proxy, VPN, Zentyal.

1. INTRODUCCIÓN

GNU/Linux es fruto de la combinación de diferentes proyectos, entre ellos GNU (encabezado por Richard Stallman, la Free Software Foundation) y el núcleo Linux (encabezado por Linus Torvalds). Es un sistema operativo libre multiplataforma, multiusuario y multitarea, que pone a disposición del usuario su código fuente para que pueda ser utilizado, modificado y redistribuido libremente por cualquiera, bajo los términos de la Licencia Pública General de GNU y otra serie de licencias que también son libres [1]. Zentyal, concebido para ser instalado en una máquina (real o virtual) funciona sobre la distribución de GNU/Linux Ubuntu en su versión para servidores, usando siempre las ediciones Long Term Support [2].

En este artículo se compila la evaluación final del Diplomado de Profundización En Linux, está enfocado al fortalecimiento del uso de GNU/Linux; se aprovecharon los conocimientos brindados a través del diplomado y los conocimientos previos para finalmente desarrollar de manera satisfactoria temáticas como DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN, sobre una plataforma GNU/Linux Zentyal Server; estas temáticas

están orientadas a la solución de problemáticas específicas de infraestructura tecnológica bajo la implementación y uso de tecnologías GNU/Linux, cada una de ellas se evidencia su instalación, configuración y funcionamiento para la comprobación de solución a necesidades específicas.

2. TEMATICAS DESARROLLADAS

El contenido del presente artículo se realiza con la participación activa de los integrantes del grupo colaborativo, quienes hicieron la elección de cada una de las temáticas a trabajar, cada participante muestra a través de evidencias el resultado obtenido en el procedimiento. En la tabla 1 se refleja el listado de las temáticas expuestas en el presente trabajo.

Tabla 1

Nº	Temática
1	DHCP Server, DNS Server y Controlador de Dominio.
2	Proxy no transparente.
3	Cortafuegos.
4	File Server y Print Server.
5	VPN.

3. INSTALACIÓN ZENTYAL SERVER

Se Instala y configurar Zentyal Server como sistema operativo para disponer de los servicios de Infraestructura IT.

Se crea la máquina virtual, para esto se requiere mínimo 1GB de memoria RAM, disco duro 20 GB, procesador de doble núcleo y dos tarjetas de Red.

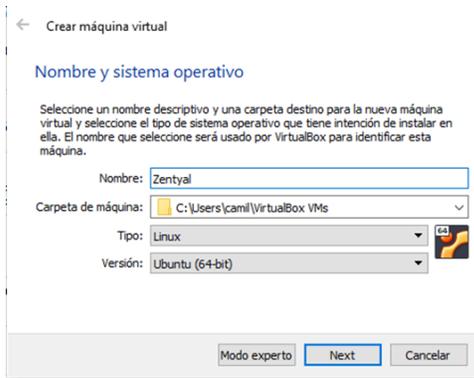


Figura 1: Nombre y Sistema Operativo.

Se asignan 2.5 GB de memoria RAM y 5 GB de disco duro.

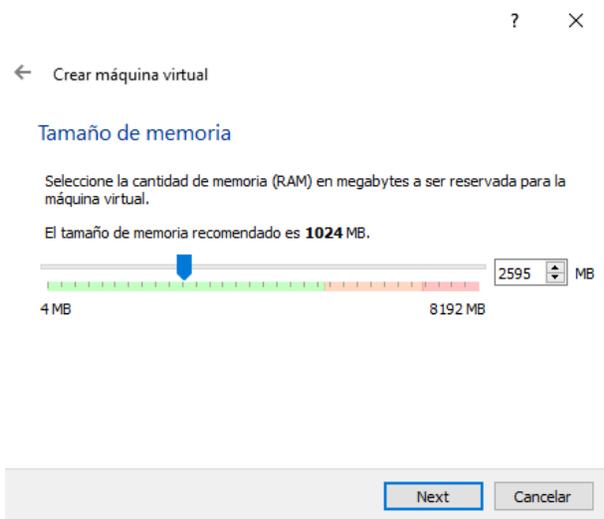


Figura 2: Tamaño de memoria

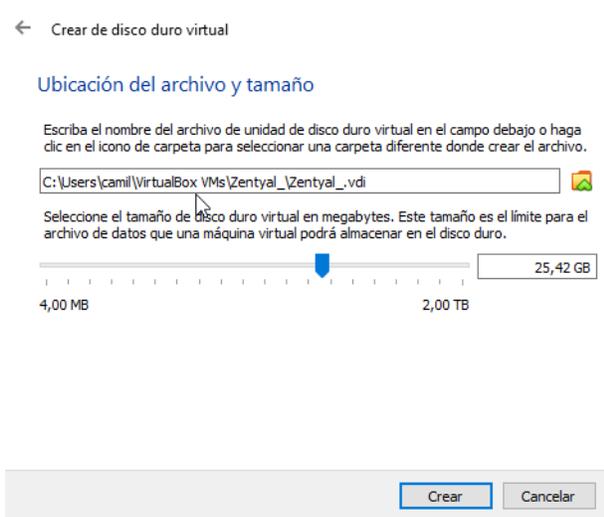


Figura 3: Ubicación del archivo y tamaño

Se agregan los dos adaptadores de red como se muestra a continuación.

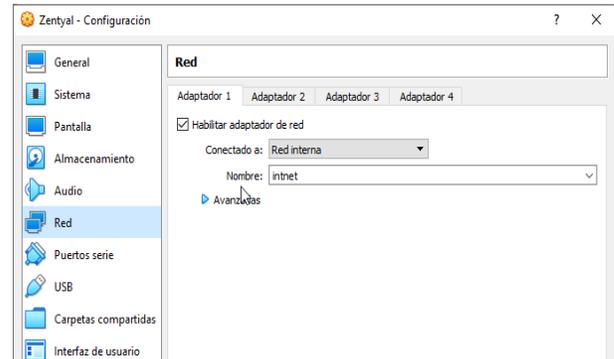


Figura 4: Configuración adaptador 1

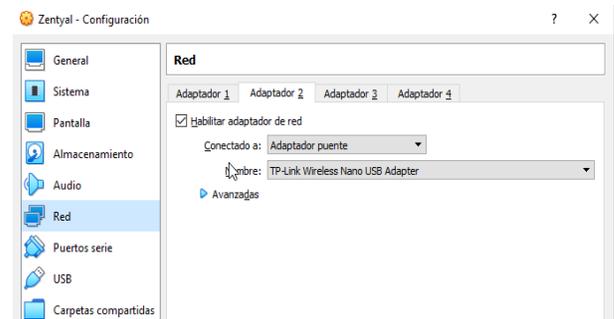


Figura 5: Configuración adaptador 2

Se selecciona la imagen del sistema operativo a instalar, en este caso zentyl-6.2-development.

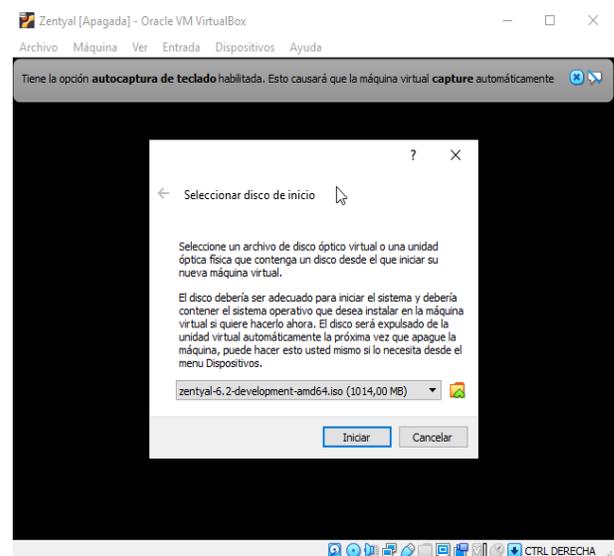


Figura 6: Selección de disco de inicio

Se selecciona el idioma y la región



Figura 7: Selección de idioma

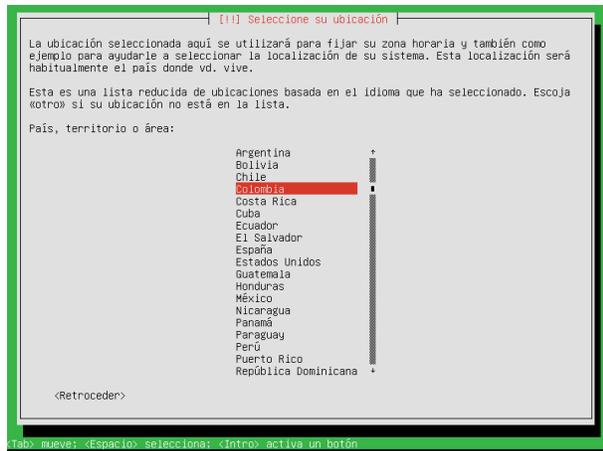


Figura 8: Selección de ubicación

Se configura la distribución del teclado para español.

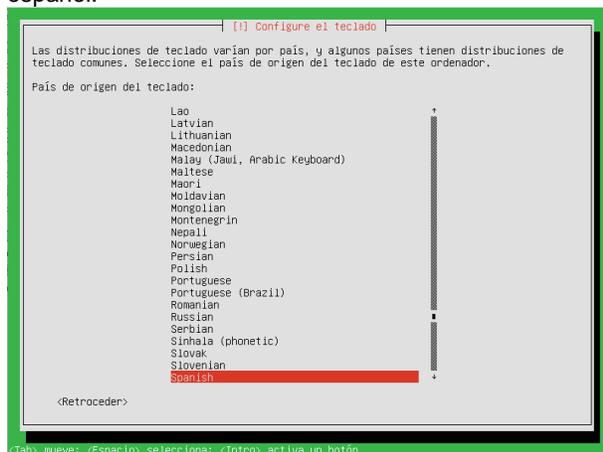


Figura 9: Configuración de teclado

Se continúa con el nombre de la máquina

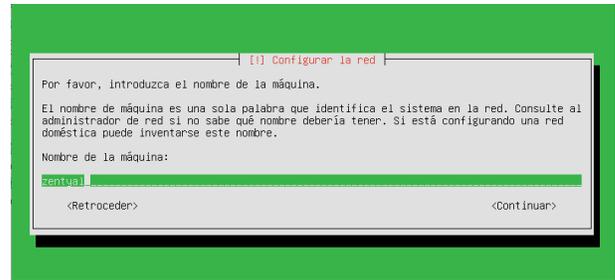


Figura 10: Configuración de red

Se confirma la zona horaria y se espera a que finalice la instalación del SO

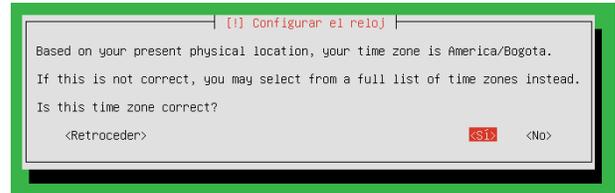


Figura 11: Confirmación de zona horaria

Una vez se termina la instalación se reinicia el sistema.

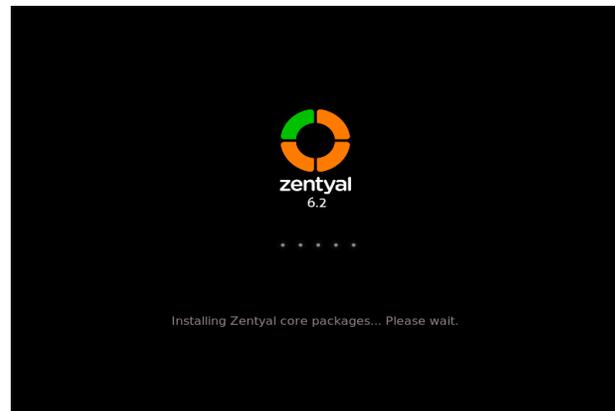


Figura 12: Reinicio del sistema

Después de reiniciar la máquina se podrá iniciar con la configuración correspondiente según se requiera.

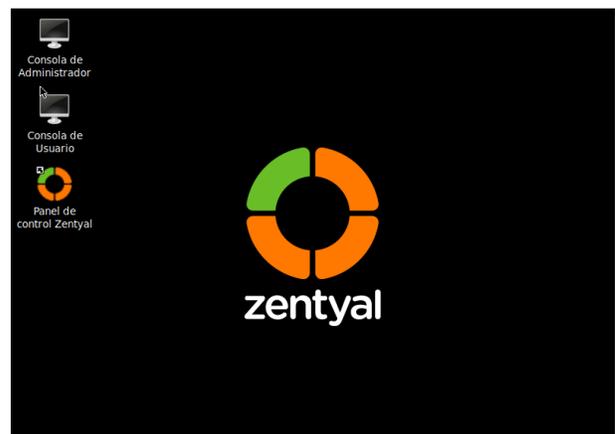


Figura 13: Desktop Zentyal

4. DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Una vez realizada la instalación se proceden a instalar los paquetes necesarios que para este caso son DHCP, DNS y Controlador de dominio tal y como se muestra en la siguiente imagen.

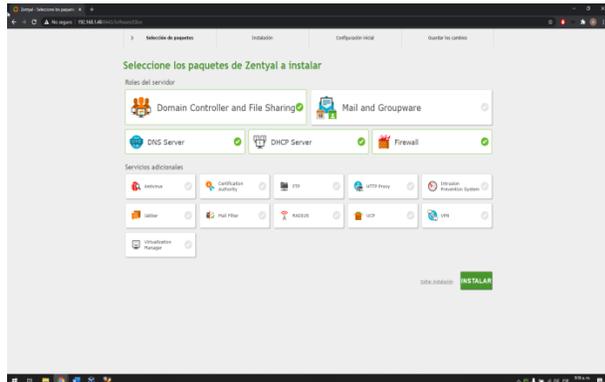


Figura 14: Selección de paquetes de Zentyal a instalar

Se confirman los paquetes y se procede a realizar la instalación de estos.

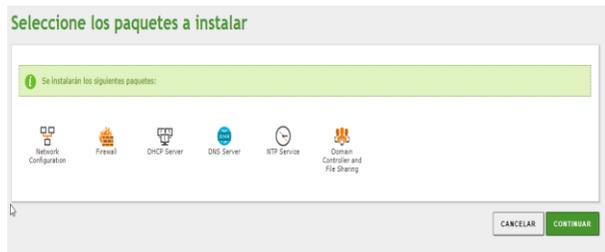


Figura 15: Confirmación de paquetes a instalar



Figura 16: Instalación de paquetes

Una vez finalizada la instalación, se puede observar una pantalla similar a la que se muestra a continuación.



Figura 17: Instalación de paquetes finalizada

4.1 DHCP

Un servidor DHCP (Dynamic Host Configuration Protocol), es un servidor de red que permite la asignación automática de direcciones IP, este servidor envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red.

Verificar que el modulo DHCP esté activado.

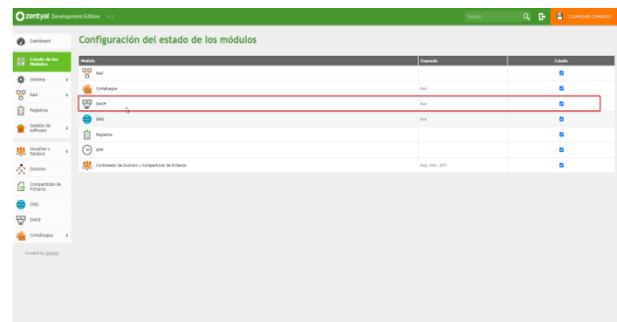


Figura 18: Configuración del estado de los módulos

Observamos que en el menú DHCP no las interfaces no poseen rangos configurados.

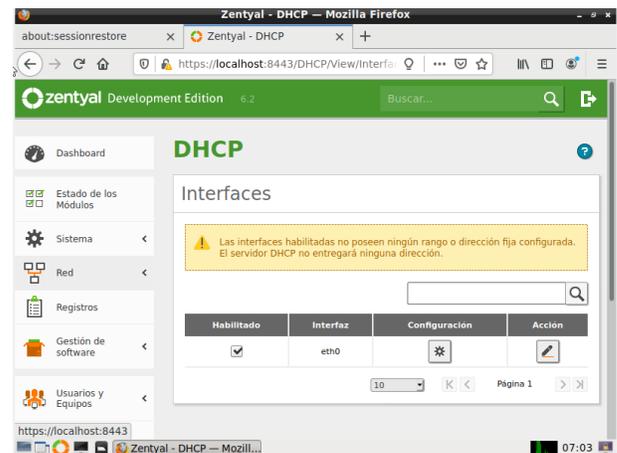


Figura 19: Interfaces DHCP

Por lo tanto, se agregan rangos desde la sección **rangos** en el botón **añadir nuevo/a**.

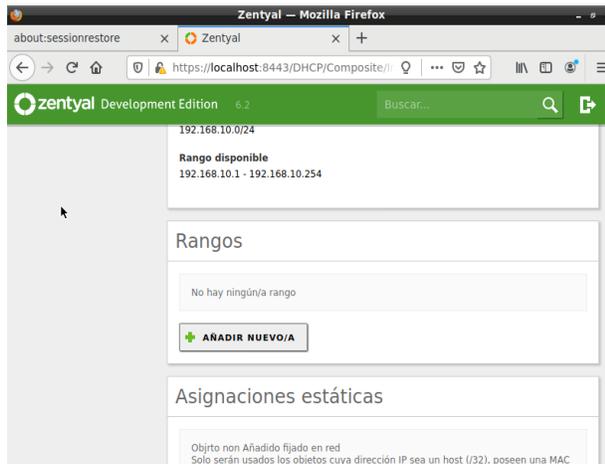


Figura 20: Adición de nuevos rangos

En este caso decidí añadir el siguiente rango.

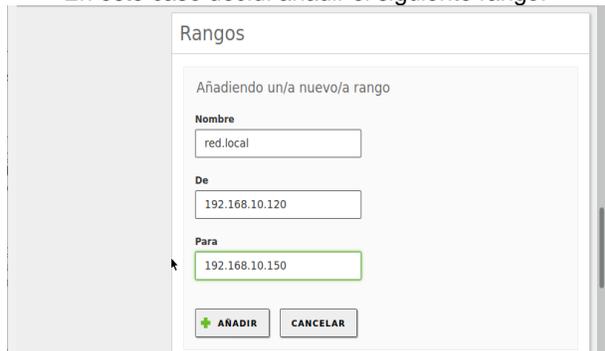


Figura 21: Añadiendo un nuevo rango

Se evidencia el nuevo rango creado.



Figura 22: Evidencia rango añadido

Y posteriormente se guardan los cambios.



Figura 23: Guardando cambios de rangos DHCP

Una vez realizado esto, procedemos a iniciar la maquina Ubuntu Desktop para verificar que se haya asignado una IP dentro del rango configurado, esto se puede verificar desde la configuración de red o ejecutando el comando **ifconfig**.



Figura 24: Validación de asignación de IP por medio de DHCP – Configuración de red

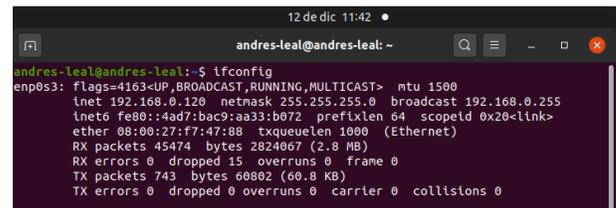


Figura 25: Validación de asignación de IP por medio de DHCP – Command line

También podemos verificar en el dashboard de Zentyal en la sección **IPs asignadas con DHCP**



Figura 26: IPs asignadas con DHCP desde Zentyal

4.2 DNS

Un servidor DNS (Domain Name System) en español, sistema de nombres de dominio, su función principal es básicamente es traducir la solicitud de ciertos nombres de host a números de IP específico.

Se verifica que el módulo **DNS** de Zentyal esté activado.

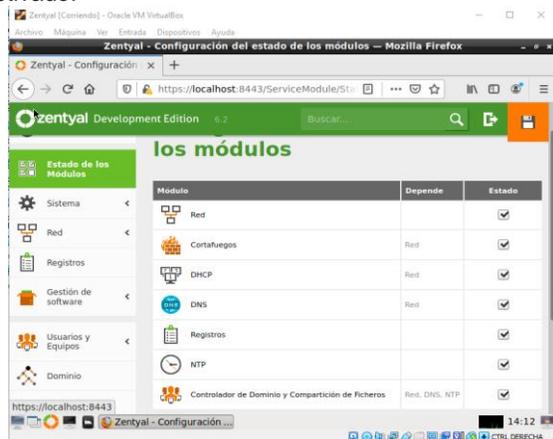


Figura 27: Verificación estado modulo DNS

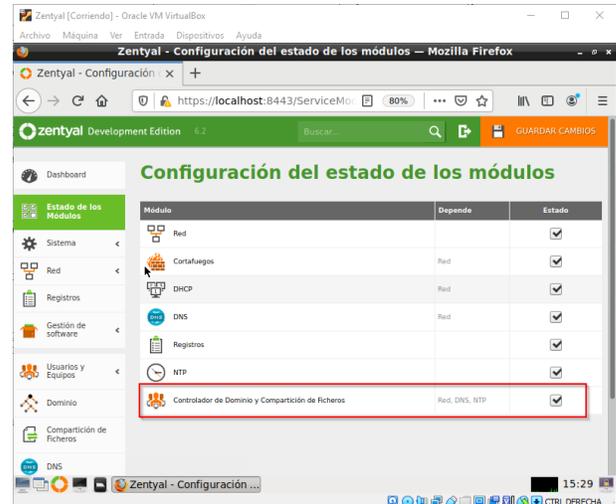


Figura 30: Verificación estado módulo Controlador de dominio

Se tiene observa que ya por defecto está creado el dominio.

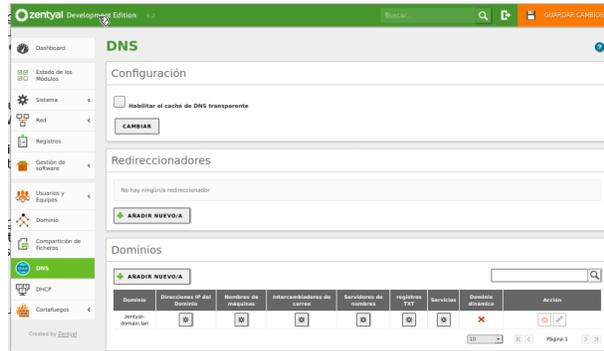


Figura 28: Verificación dominio creado por Zentyal

En la sección **Dominio** se puede observar que ya está configurado el dominio.

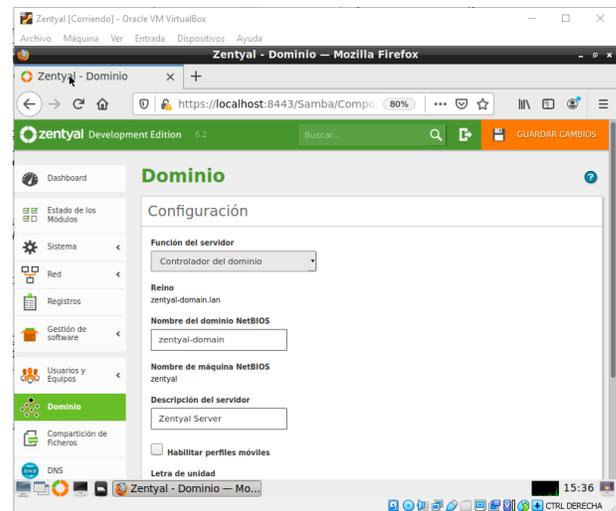


Figura 31: Controlador de dominio

Comprobamos que nuestro Desktop tiene como DNS la IP de nuestro servidor Zentyal.

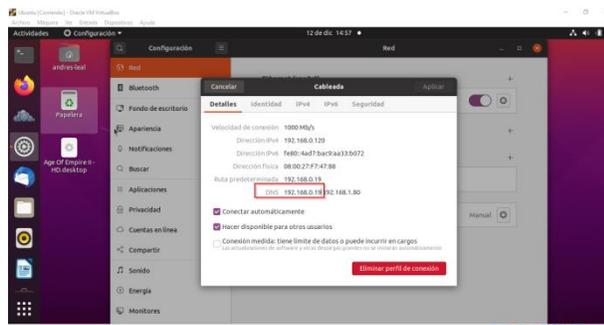


Figura 29: Validación de asignación DNS desde Ubuntu Desktop



Figura 32: Controlador de dominio

4.3 CONTROLADOR DE DOMINIO

Se verifica que el módulo de Controlador de dominio esté habilitado.

Por lo cual ya se puede proceder la creación del grupo y usuario que se desea.

Se gestionan los usuarios y equipos

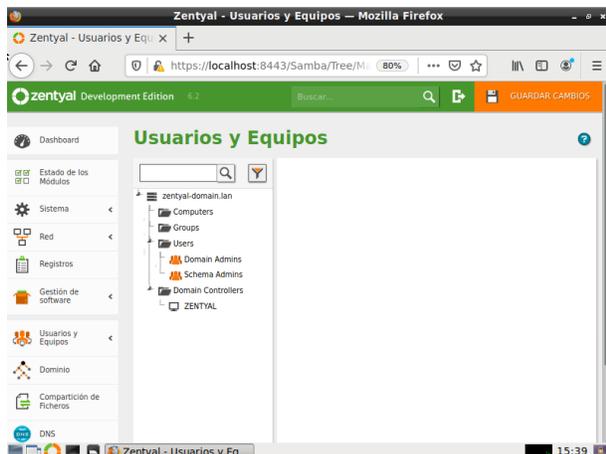


Figura 33: Gestión de Usuarios y grupos

Se crea el grupo Linux.

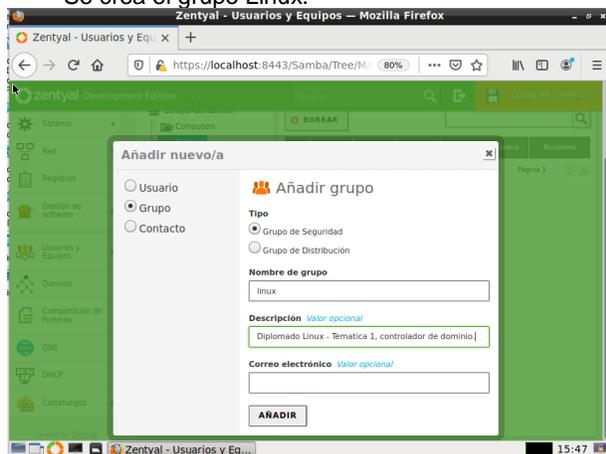


Figura 34: Añadir grupo

Y se crea el usuario **andres.leal** y se asocia al grupo **linux**

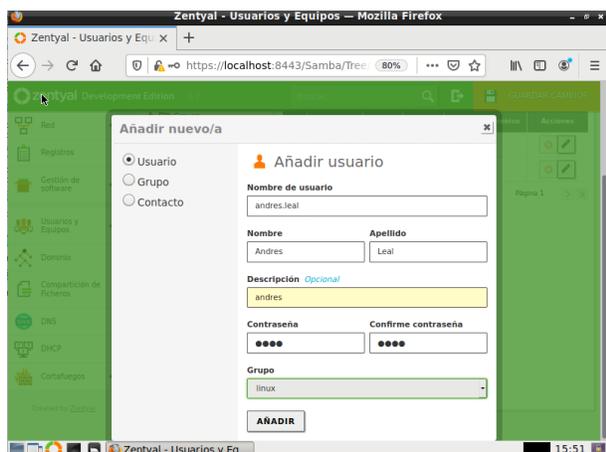


Figura 35: Añadir usuario y asignar grupo



Figura 36: Verificación de usuario creado

5. PROXY NO TRANSPARENTE

Proxy no transparente es aquel el cual se le suministra información a comparación del transparente que no necesita ingresar ninguna configuración.

El proxy no transparente se puede revisar si está habilitada al ingresar al navegador en configuración de red, donde permite ver la configuración acceso proxy a internet, en cambio del transparente, que el cliente pueda que no conozca de su existencia, ya que no se puede revisar a simple vista.

Para la 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 se realiza primero la configuración de red que nos permitió una vez finalizo el proceso de instalación de los paquetes:

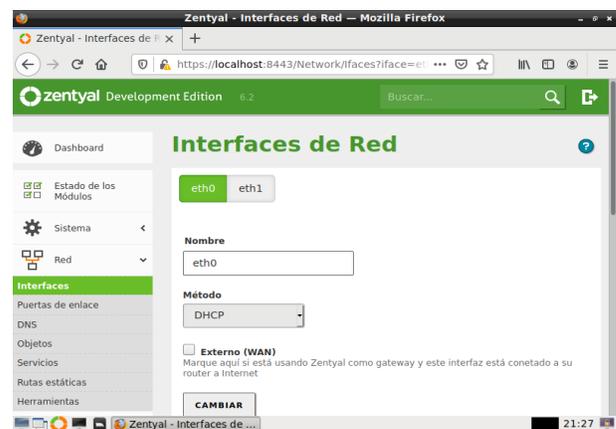


Figura 37: Interfaces de red zentyal

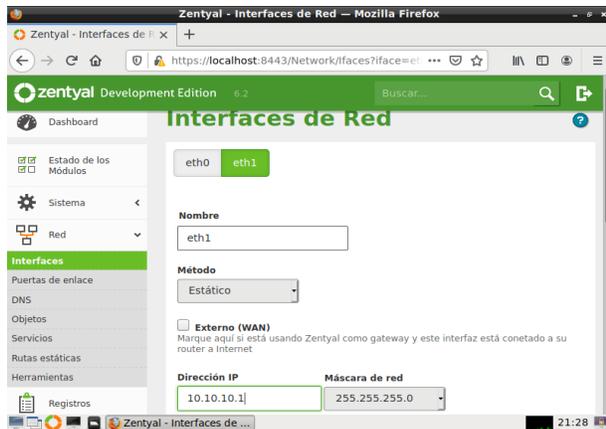


Figura 38: asignación IP estática

Para denegar el acceso del puerto, se va a trabajar como estación de trabajo con el Ubuntu desktop, teniendo en cuenta que se requiere para habilitar el módulo proxy HTTP, que necesita al menos una interfaz de red externa, por lo que se arranca la maquina:

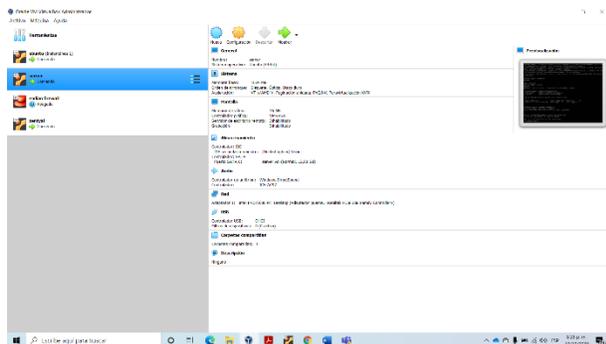


Figura 39: máquinas virtuales

También se configura los adaptadores de red, teniendo en cuenta que para montar el host virtual basado en IP, se debe tener dos o más direcciones IP y para ello se habilitaron dos interfaces de red, en la presente actividad vamos a utilizar la IP 10.10.10.1 para una:

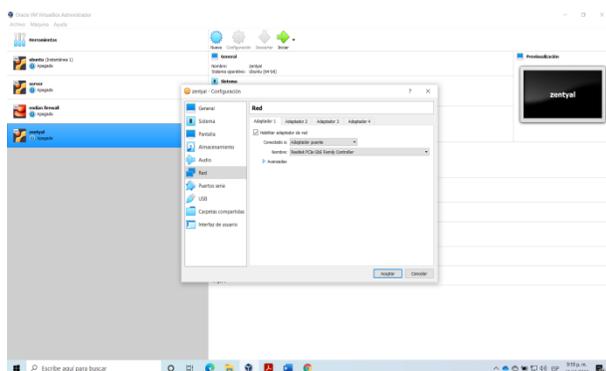


Figura 40: configuración adaptadores de red

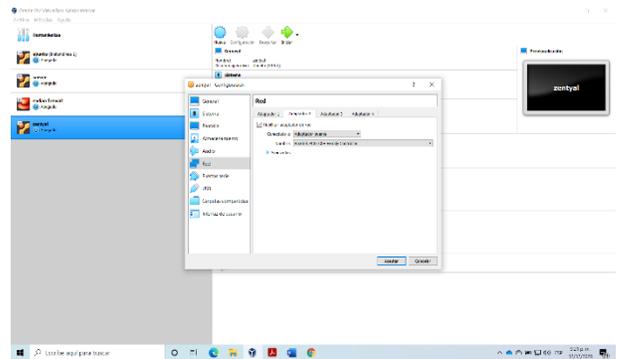


Figura 41: configuración adaptador de red

Se verifica la conexión del desktop Ubuntu que esté conectada a la IP asignada y con acceso a internet:

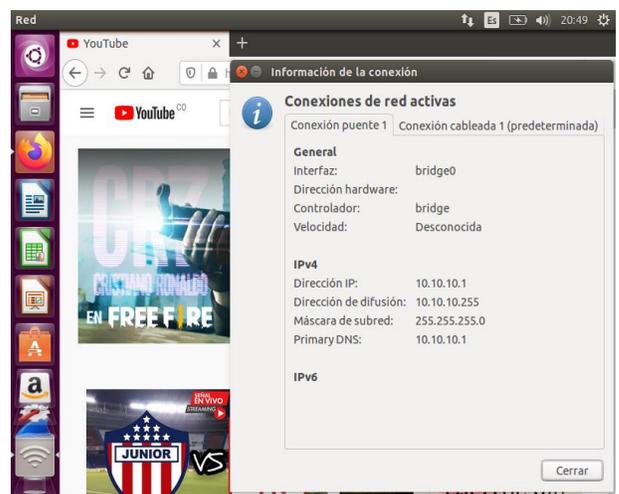


Figura 42: Información conexión Ubuntu desktop

Para habilitar el proxy HTTP primero debemos tener marcado la interfaz de red externa:

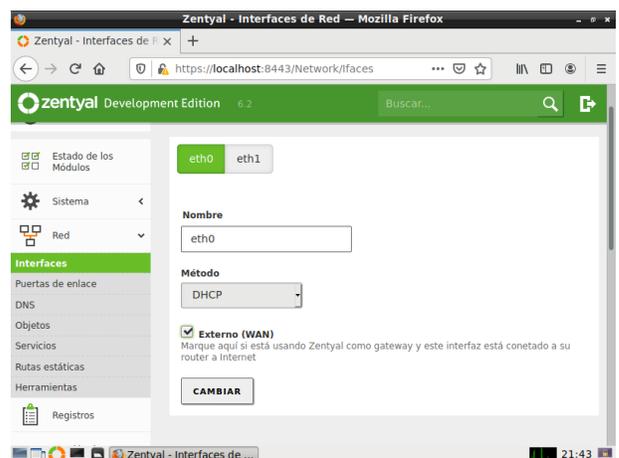


Figura 42. Habilitación interfaz red externa

Ahora si se puede habilitar el modulo:

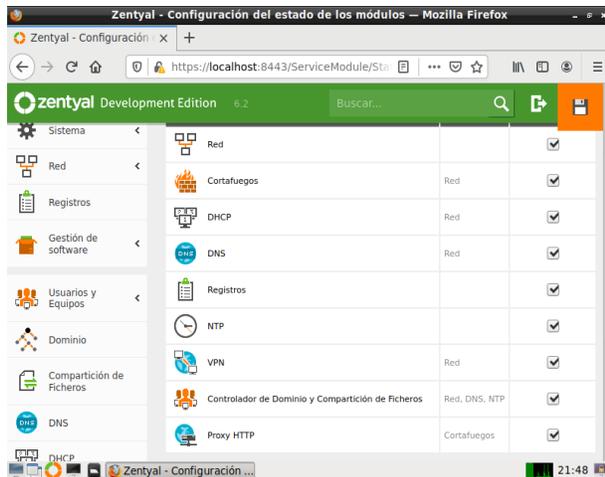


Figura 44: habilitación modulo proxy HTTP

Procedemos a la configuración del proxy no transparente, en puerto el 1230 que es el requerido:

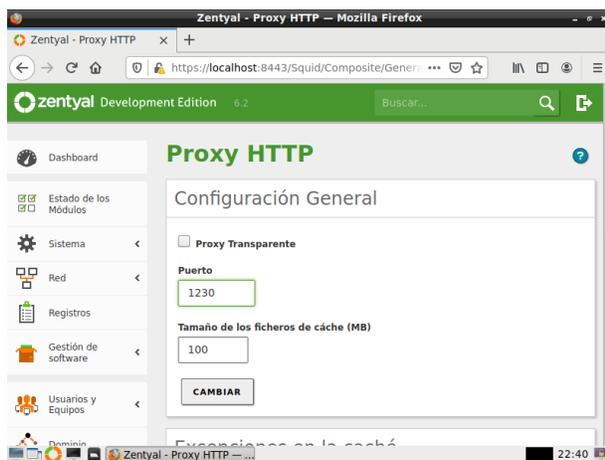


Figura 45: configuración general proxy HTTP

Se añade el objeto del desktop Ubuntu al que le vamos a realizar la regla:

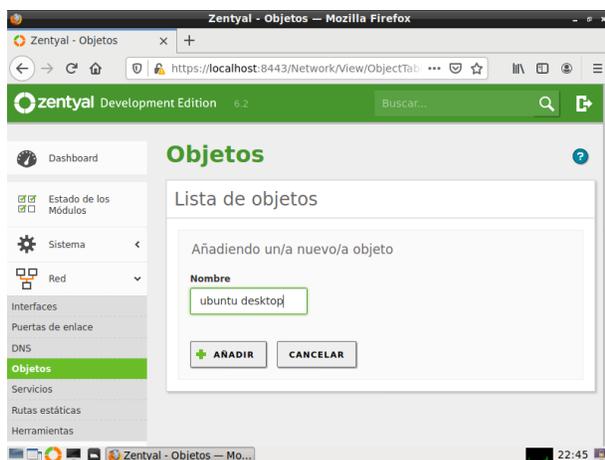


Figura 46: Nuevo objeto de red zentyal

Se crea la regla donde denegamos el acceso:

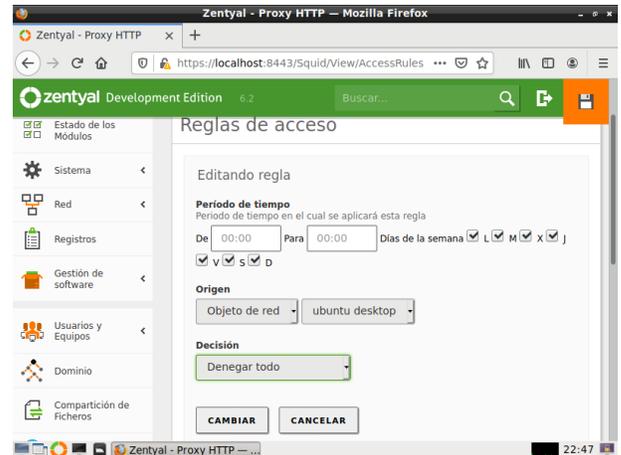


Figura 47: reglas de acceso

Verificamos el puerto que estamos denegando sea correctamente el del desktop Ubuntu:

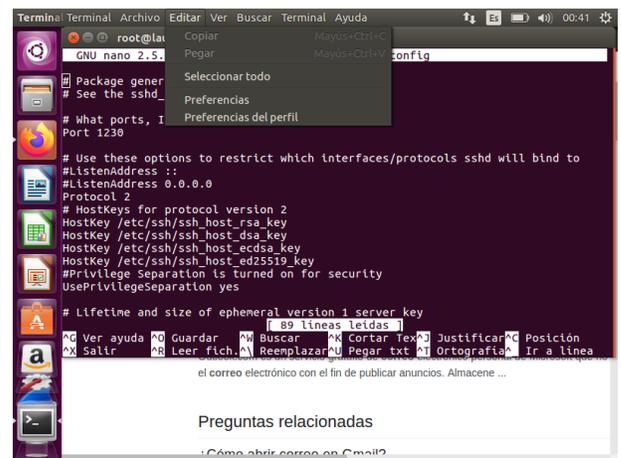


Figura 48: verificación puerto Ubuntu desktop

Y ahora se intenta acceder a internet, pero se denegó el acceso que era lo que se solicitaba:

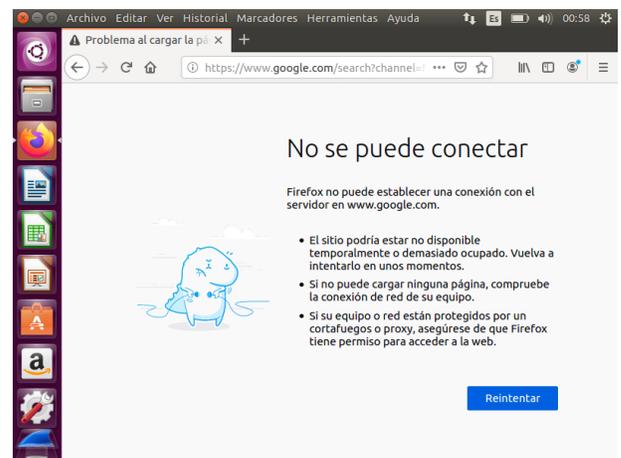


Figura 49: acceso a internet bloqueado

El proxy no transparente se puede evidenciar en la configuración de red en el navegador:

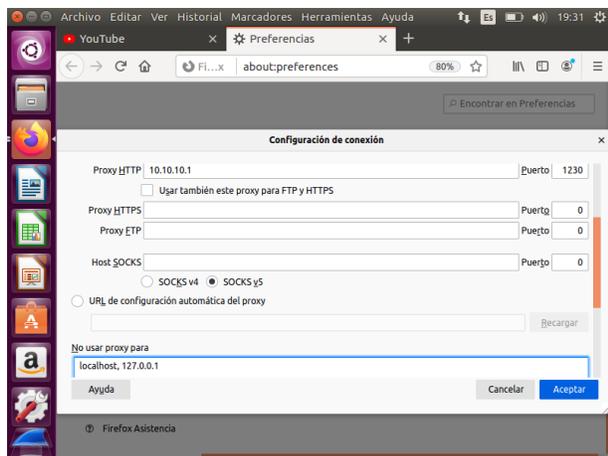


Figura 50: configuración de red, proxy no transparente

6. CORTAFUEGOS

Un cortafuegos (en inglés Firewall), es un Software encargado de realizar el filtrado tráfico de entrada y salida a internet en una red administrada, este procedimiento lo realiza por medio de unas reglas que define el administrador de la red llamadas *iptables*. El cortafuegos es la primera línea de defensa ante cualquier tipo de ataque que venga de Internet, todo el tráfico pasa por él y partiendo de los criterios establecidos en él se da acceso o se deniega una petición específica. También existen Cortafuegos físicos, son mucho más potentes que el Software que ofrecen las distribuciones GNU/Linux porque cuentan con Software mucho más avanzado pero su objetivo es el mismo [3].

6.1. CONFIGURACIÓN REGLAS DE FILTRADO DE DENEGACIÓN DE ACCESO A REDES SOCIALES.

Inicialmente creamos y configuramos nuestro servidor DHCP en donde asignamos nuestro POOL de IP's que serán entregadas por este. *DHCP>Configuración>Rangos*.

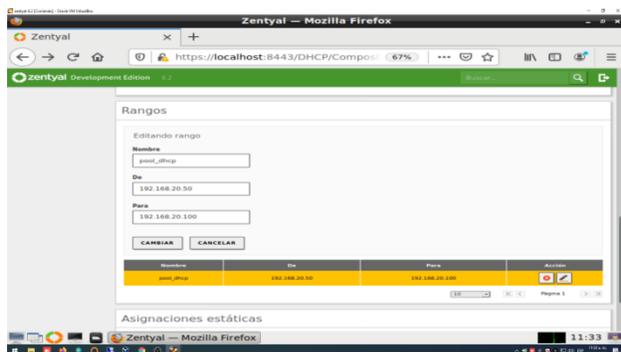


Figura 51: Creación POOL de IPs.

Posteriormente creamos un objeto de red, el cual va a contener las IPs que van a tener las restricciones de navegación. En este caso se van a bloquear todos los equipos de la red, por eso se asigna todo el segmento creado en el módulo DHCP. *Redes>Objetos>Añadir nuevo*.

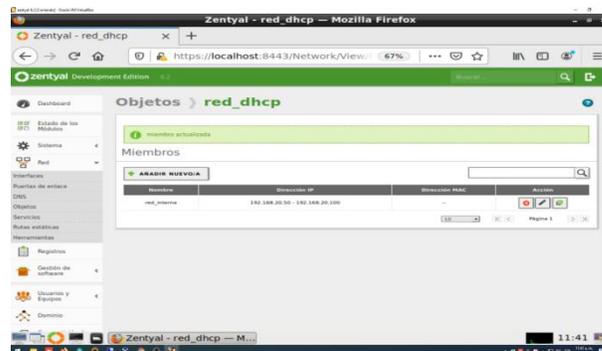


Figura 52: Creación de objeto de red.

Seguidamente se procede a configurar el objeto creado. *Redes>Objetos>Miembros*.

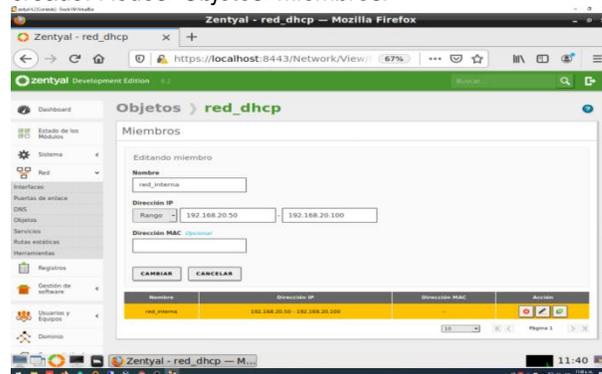


Figura 53: Configuración de objeto de red.

Teniendo el servidor DHCP y el objeto de red creado, se debe verificar que IPs públicas tiene configurado Facebook para el ejercicio haciendo ping a www.facebook.com

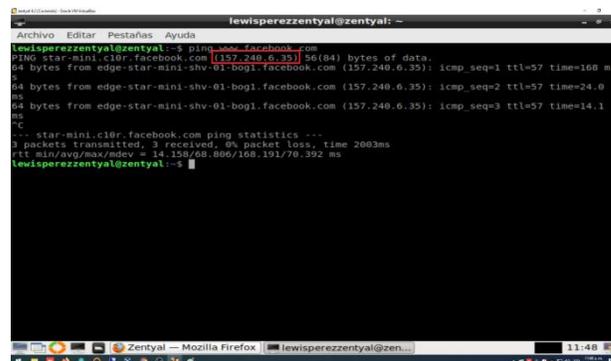


Figura 54: Ping a facebook para saber IP.

Teniendo la IP ubicada, se procede a la creación de la regla de filtrado. *Cortafuegos>Filtrado de paquetes>Reglas de filtrado para las redes internas>Añadir nuevo*.

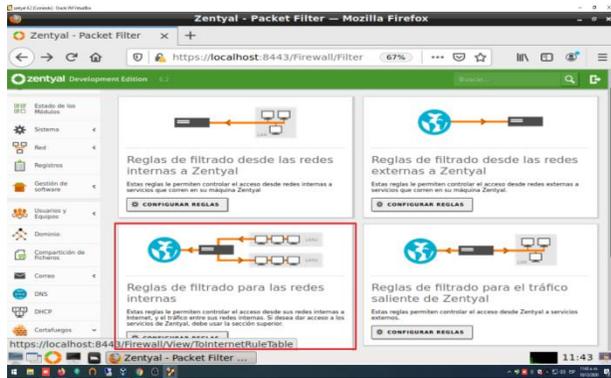


Figura 55: Creación de regla de filtrado.

Se realiza la configuración de la nueva regla de filtrado creada. Se da la instrucción de Denegar, como origen seleccionar Objeto de red y se seleccionar el objeto creado anteriormente, como destino se ingresa la IP de Facebook que se identificó haciendo ping y se guarda.

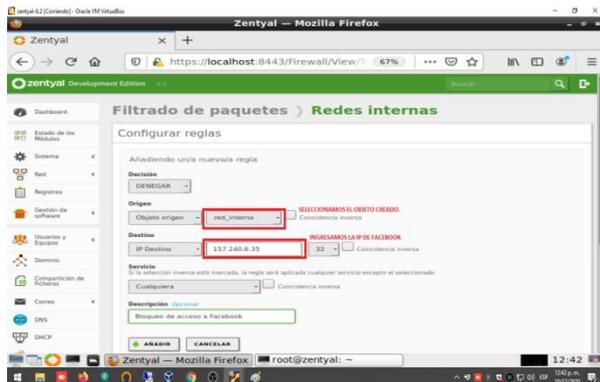


Figura 56: Configuración de regla de filtrado.

Se procede a realizar la validación, validando que esté obteniendo la configuración del servidor DHCP. IP del segmento que se creó y puerta de enlace.

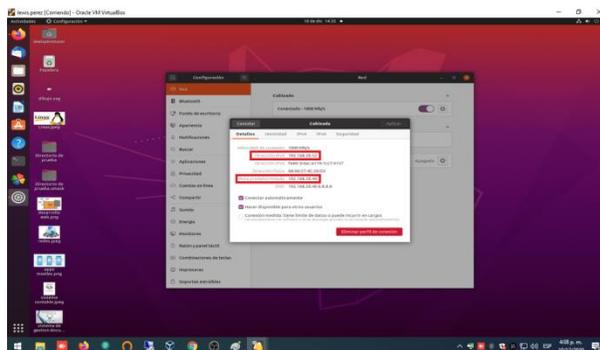


Figura 57: Verificación de IP y puerta de enlace entregados por el servidor.

Se realiza la validación de que la máquina desde donde se realizan las pruebas cuenta con conexión a internet.



Figura 58: Validación de acceso a internet.

Por último se procede a intentar acceder sitios web bloqueados desde el Cortafuegos.

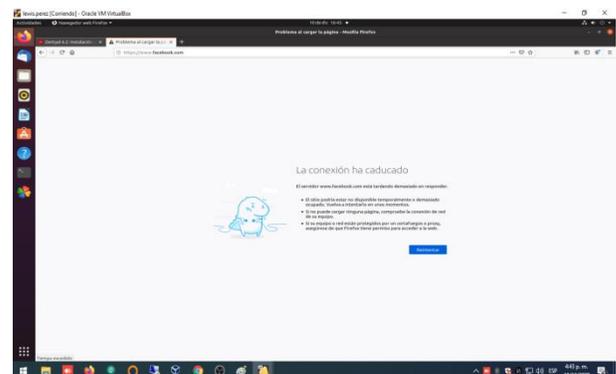


Figura 59: Validación de acceso denegado a Facebook.

7. 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

En la presente temática se presenta la configuración de un file server y print server que funciona para usuarios del sistema operativo Windows, negándoles o permitiéndoles el acceso a los recursos compartidos que desde allí se creen y se configurarán dichos recursos desde una terminal Ubuntu Desktop.

Para la configuración se deberá instalar el módulo de controlador de dominio, compartición de archivos y DNS desde el panel de Zentyal; sólo será necesario configurar una interfaz de red la cual se conectará a LAN con la IP que configuramos y se selecciona tipo de servidor Stand-alone.



Figura 60: Iniciamos la configuración de Zentyal



Figura 63: Seleccionamos la opción stand alone.

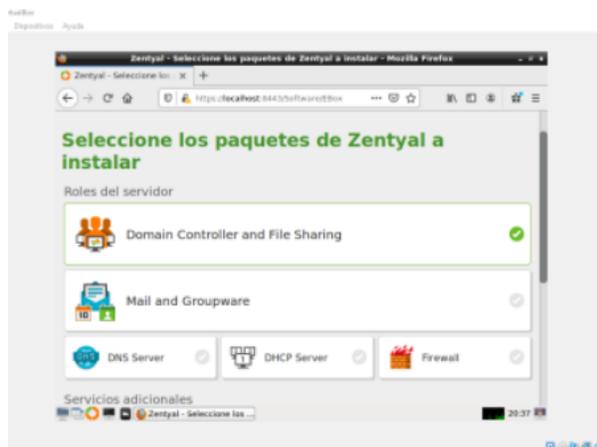


Figura 61: Seleccionamos los servicios a instalar



Figura 64: Ingresamos el nombre del dominio



Figura 62: Configuramos las tarjetas de red, una de conexión con internet y la otra de red interna



Figura 65: Aceptamos y esperamos que se configure el servidor

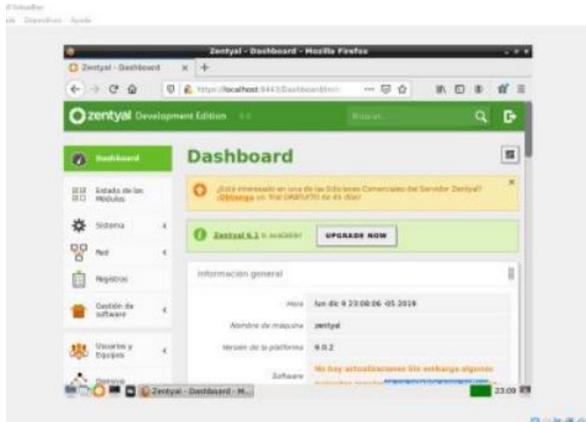


Figura 66: Creamos un usuario en la opción Usuarios y equipos.

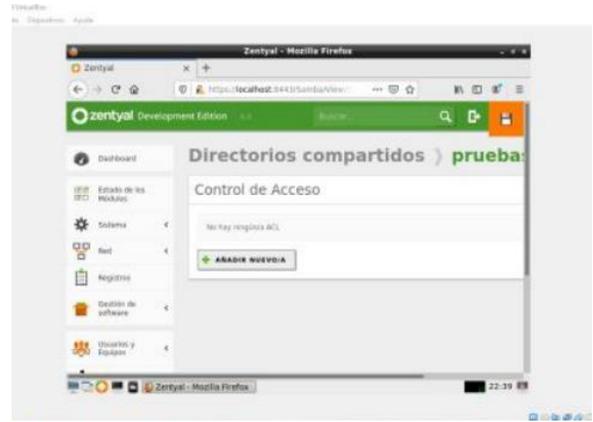


Figura 69: Configuramos los permisos a los directorios creados

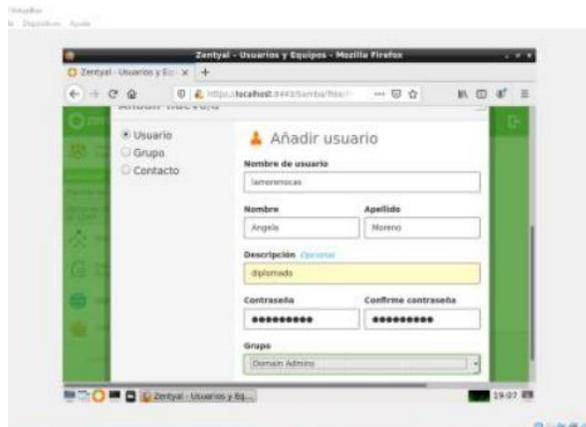


Figura 67: Asignamos nombres y contraseña para la creación

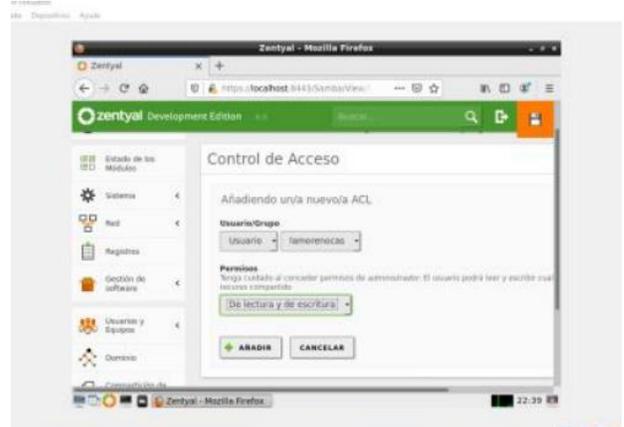


Figura 70: Se asigna el permiso por usuario y el tipo de permiso

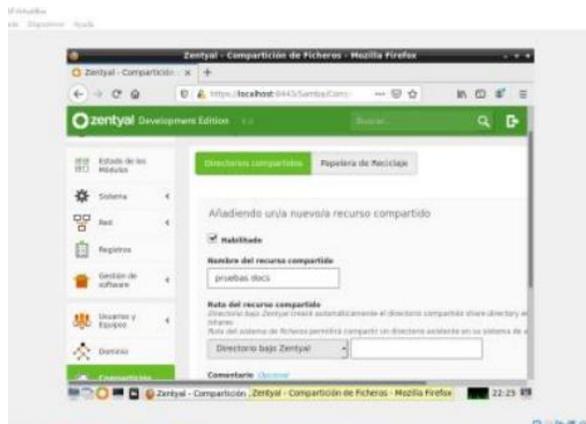


Figura 68: Creamos un directorio compartido y asignamos los permisos por grupos o por usuario



Figura 71: Se instala likewise para realizar el ingreso de la máquina al dominio.

A Continuación, se describirá el proceso para configurar el print server, teniendo en cuenta que se instalará en una máquina Ubuntu y autenticación en dominio con el usuario creado. Se procede a instalar el paquete cups en el servidor Zentyal y desde su interfaz

web añadir una impresora que tiene conectada por puerto USB y es detectada automáticamente por cups.

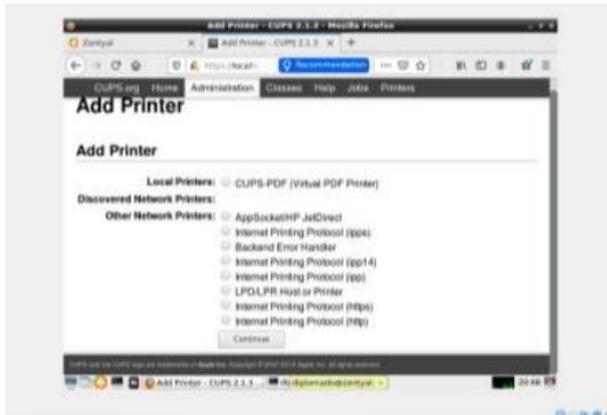


Figura 72: Seleccionamos para la prueba cups-pdf

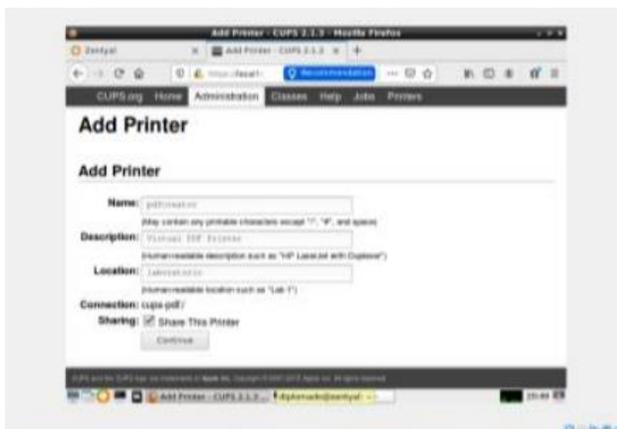


Figura 73: Al ingresar a printers ya aparece la impresora creada

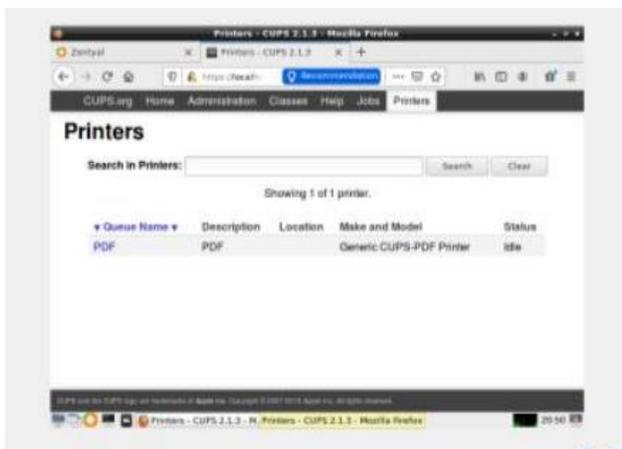


Figura 74: Prueba final

8. VPN

Una Red Privada Virtual (Virtual Private Network) es una red, construida sobre la infraestructura de una

red pública, esta permite a los usuarios remotos comunicarse de forma transparente y segura, Es privada porque garantiza la privacidad en sus comunicaciones, y virtual porque se efectúa sobre la infraestructura de redes públicas [4].

Aquí se presenta la implementación y configuración detallada de la creación de una Red Privada Virtual - VPN que permite establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux.

Se ingresa a Zentyal con usuario y contraseña.

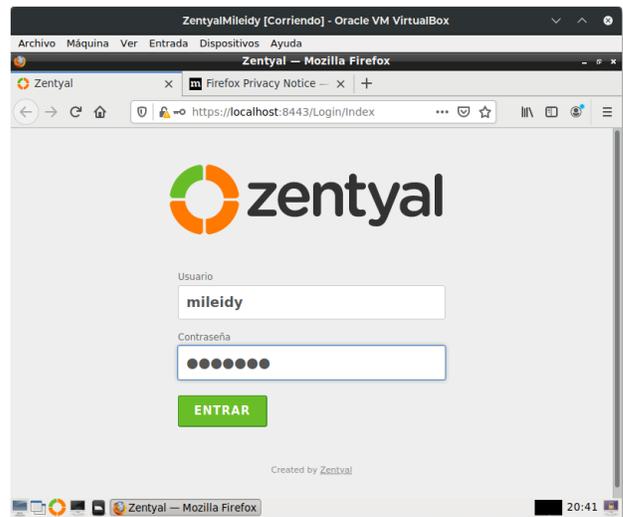


Figura 75: Ingreso a Zentyal.

Seleccionamos los paquetes que vamos a necesitar para la configuración de VPN y se continúa con la instalación.

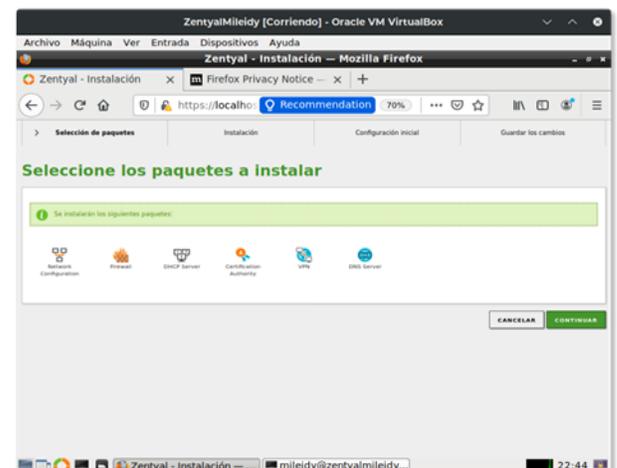


Figura 76: Paquetes a instalar.

Se realiza la configuración inicial de las interfaces eth0 como externa y eth1 como interna.

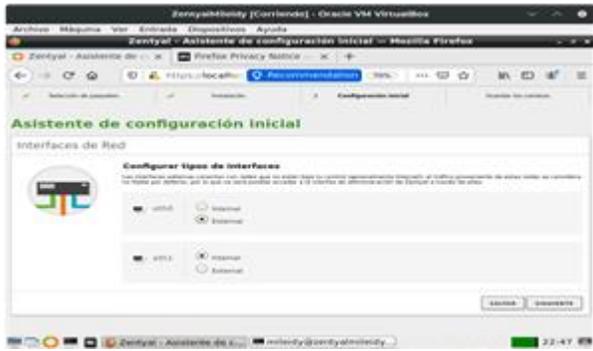


Figura 77: Configuración de interfaces



Figura 78: Configuración IP interfaces.

Se configuran las reglas de entrada y salida de internet.



Figura 79: Configuración de reglas.

Se verifica que el pc Debian tenga IP en el rango y tenga acceso a internet.



Figura 80: Verificación IP.

Creación del servidor VPN, En la sección VPN se crea primero una autoridad de certificación.



Figura 81: Autoridad de certificación.

Se agrega un nuevo Server VPN, luego se guardan los cambios.



Figura 82: Creación nuevo Server VPN

Se aplica la configuración para el servidor, se habilita la interfaz TUN.



Figura 83: Configuración del servidor

Se regresa al listado de servidores y se configuran las redes anunciadas, luego se agrega la red de nuestra local para que los clientes remotos la puedan ver.

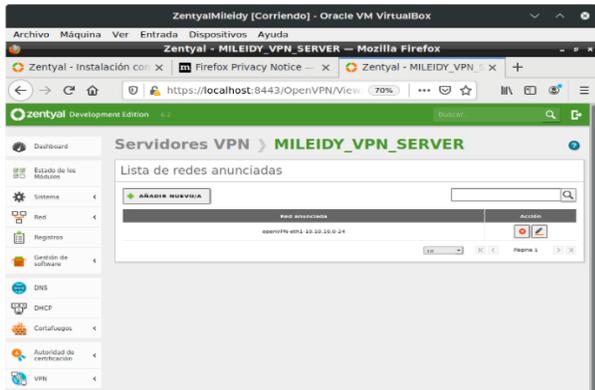


Figura 84: Lista de redes anunciadas.

Se descarga un paquete de configuración para que se pueda conectar nuestro cliente remoto. Vamos al listado de servidores VPN y le damos clic en descargar paquetes de configuración de cliente.

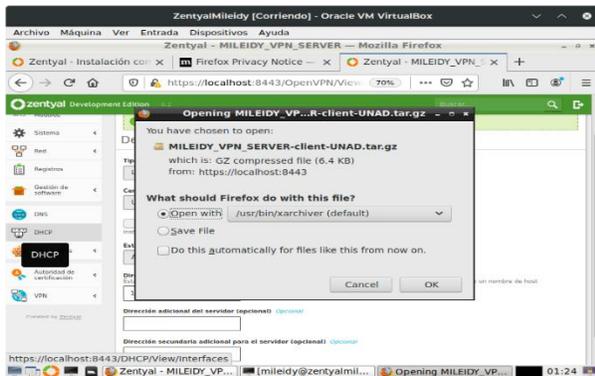


Figura 85: Descarga paquetes de configuración

Configuración de cliente Linux. Instalación del cliente openvpn en debian o se verifica que esté instalado.

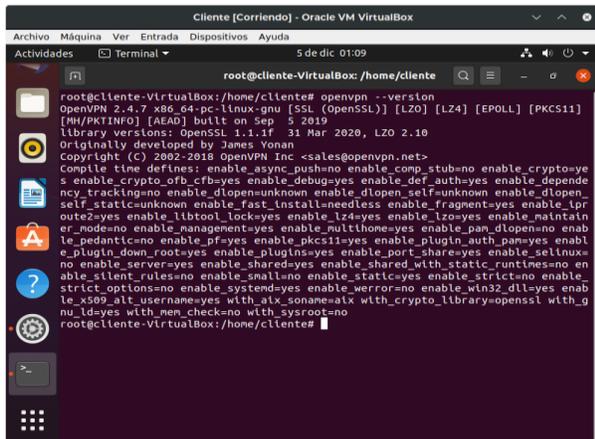


Figura 86: Verificación instalación del cliente openvpn.

Se extraen los archivos en nuestro cliente.

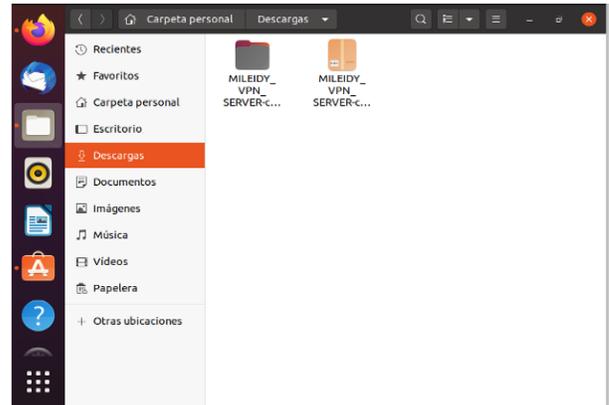


Figura 87: Extracción de archivos.

Se añade una nueva VPN, seleccionando importar desde un archivo.

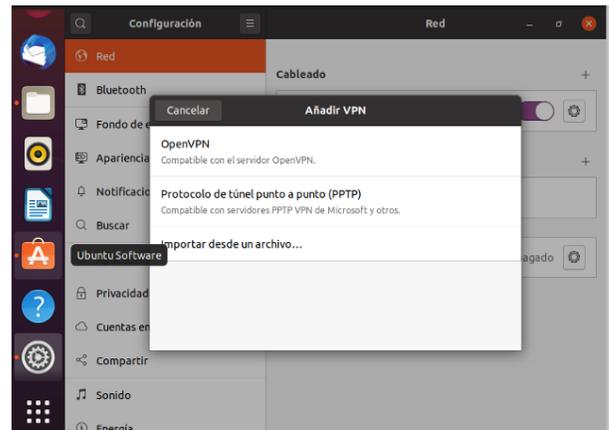


Figura 88: Añadir nueva VPN

Seleccionamos el archivo descomprimido, se confirma la configuración y luego se da clic en el botón añadir.

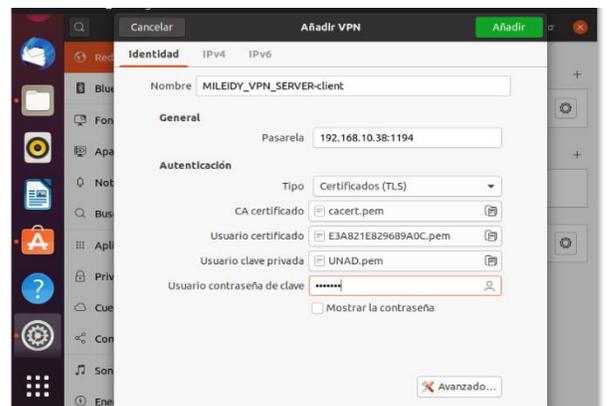


Figura 89: Verificación

Una vez confirmada la configuración se activa la VPN.

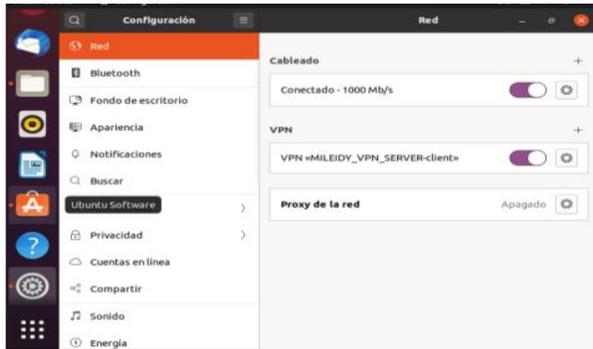


Figura 90: Activación VPN

Se verifica la conexión a nuestra red interna y verificamos que se nos haya asignado una dirección de VPN.

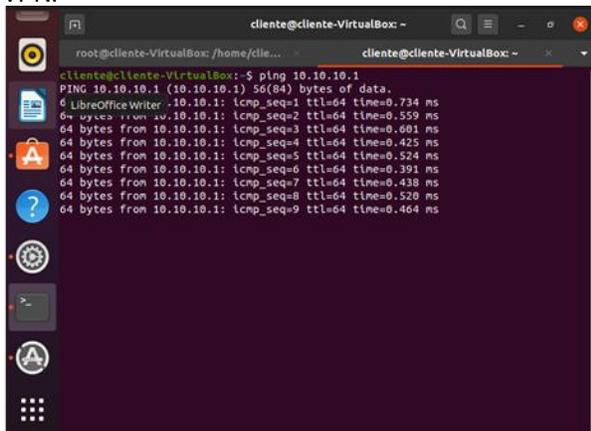


Figura 91: Verificación de conexión.

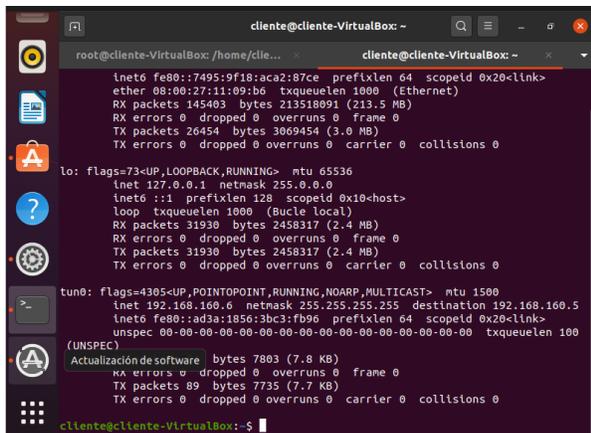


Figura 92: Verificación de conexión.

9. CONCLUSIONES

- Se configura la infraestructura de Zentyal server para la creación de servidores DHCP, DNS y controladores de dominio, por medio de los paquetes o modules con los que cuenta Zentyal, los cuales permiten dar una respuesta a los requerimientos específicos del cliente, dado que se realiza cada configuración de acuerdo a lo solicitado, permitiendo de esta forma el uso de los servidores para la asignación automática de direcciones IP a cada máquina conectada a la red.
- Linux Zentyal, es una solución todo en uno, una gran alternativa ante el conocido Windows Server que implementa también dentro de sus servicios, protocolos de código abierto compatibles con tecnología de Microsoft. Este dispone de dos versiones, la comercial que permite ser utilizada de forma gratuita por 45 días y la de desarrollo que presenta restricciones a nivel de ciertas funcionalidades más no de tiempo.
- El desarrollo de la actividad paso 8 me permitió aprender a formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permitieron dar respuesta a los requerimientos específicos del cliente, a su vez logró de manera satisfactoria desarrollar la temática, creación de una VPN y con ello poner en práctica lo aprendido en cada uno de las actividades propuestas en el diplomado de profundización en Linux.

4. REFERENCIAS

- [1] Linux en español. (19 de 06 de 2019). *¿Qué es GNU/Linux?* Obtenido de <https://www.xn--linuxenespaol-skb.com/ayuda/que-es-gnu-linux/>
- [2] Zentyal. (2018). Zentyal Community. Obtenido de Documentación de Zentyal 6.2: <https://doc.zentyal.org/es/installation.html#el-instalador-de-zentyal>
- [3] ¿Qué es Cortafuegos? Obtenido de <https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona>
- [4] Tomás Cánovas, J. J. (10 de 2018). *Servicio VPN de acceso remoto basado en SSL mediante OpenVPN*. Obtenido de PFC/TFG-Escuela Técnica Superior de Ingeniería de Telecomunicación: <https://repositorio.upct.es/handle/10317/7758>
- [5] Villada, R. J. L. (2015). *Instalación y configuración del software de servidor web (UF1271)*. Madrid, ES: IC Editorial.
- [6] Zentyal 6.2 Documentación Oficial. Zentyal community. <https://doc.zentyal.org/es/index.html>.