INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT EN ZENTYAL SERVER 6.2

Edison Sebastian Ortiz Torres
e-mail: esortizt@unadvirtual.edu.co
Mónica María Acevedo Bueno
e-mail: mmacevedob@unadvirtual.edu.co
Elkin Dadey Alfonso Cortés
e-mail: edalfonsoc@unadvirtual.edu.co
Laura Alejandra Alarcón Fernández
e-mail: laalarconf@unadvirtual.edu.co
Liliana Andrea Rincón Carrasco
e-mail: larinconcar@unadvirtual.edu.co

RESUMEN: *En este documento se muestra la instalación y configuración en VirtualBox de varios servicios de infraestructura IT en Zentyal Server 6.2 Development destinado a formular soluciones bajo GNU/Linux. Se evidencia paso a paso la instalación del servidor y las temáticas abarcadas por estudiante aplicando las pruebas respectivas para validar su correcto funcionamiento. Estos servicios son DHCP Server, DNS Server y Controlador de dominio; Proxy no transparente para el control de acceso de una estación GNU/Linux a Internet filtrando la salida por el puerto 1230; Cortafuegos para restringir la navegación de sitios web de entretenimiento y redes sociales y validando las restricciones solicitadas desde una estación cliente; File Server y Print Server para detallar el acceso de un equipo por medio del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras y finalmente, VPN para establecer un túnel privado de comunicación con un equipo cliente.*

PALABRAS CLAVE: Controlador de dominio, Firewall, Proxy, VPN, Zentyal server, DHCP, DNS,File Server y Print Server.

1 INTRODUCCIÓN

El presente documento realiza una descripción de los principales componentes de la herramienta Zentyal Server 6.2 mediante ejemplos de configuración y aspectos a tener en cuenta para cada servicio.

En el artículo se contempla la instalación de la herramienta a través de virtualbox, configuración de los servicios (DHCP, DNS, Controlador de dominio, Proxy no transparente, cortafuegos, file server, print server y VPN) teniendo imágenes de referencia y descripción del paso a paso realizado para obtener el funcionamiento de cada servicio.

La configuración de los servicios de la herramienta zentyal se realizan a través de un sitio web que se habilita por la herramienta al momento de realizar la instalación del servicio. Esto nos permite tener una gran facilidad al realizar configuraciones.

2 INSTALACIÓN DE ZENTYAL SERVER

2.1 REQUISITOS DE INSTALACIÓN

Los requerimientos pueden variar según la cantidad de usuarios que necesiten de los servicios y de los módulos que se vayan a instalar. Zentyal funciona sobre arquitectura x86_64 bits. Se requiere para su instalación mínima, memoria RAM de 1G o 1.5G, disco duro de 20G, procesador Intel Core i3 y 2 tarjetas de red.

2.2 PROCESO DE INSTALACIÓN

Se accede al sitio oficial para realizar la descarga de Zentyal: https://zentyal.com/es/news/zentyal-6-2-announcement-2/

Se procede a configurar una máquina con los requerimientos de hardware para instalar Zentyal y configurar los servicios establecidos para cada temática. Posteriormente, se inicia el proceso de instalación seleccionado el idioma, la zona horaria y la configuración del teclado.

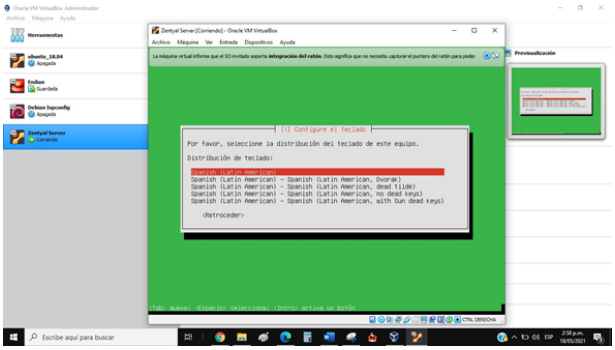

Figura 1. Configuración de teclado

A continuación, se realiza la configuración de red seleccionando una de las dos interfaces para establecer como interfaz de red primaria, la cual proporciona el acceso a internet. Además, se configura el nombre de la máquina con el que se identificará en la red.

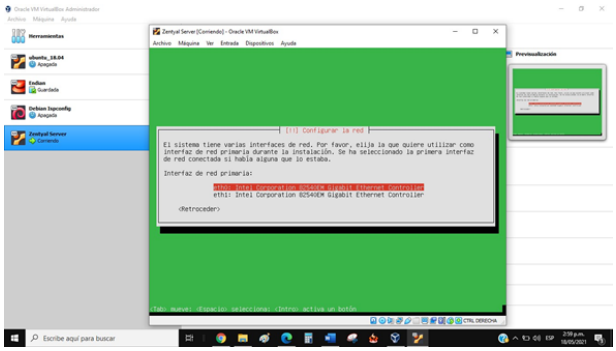

Figura 2. Selección de interfaz de red primaria

Se procede a crear un usuario y se asigna su respectiva contraseña.

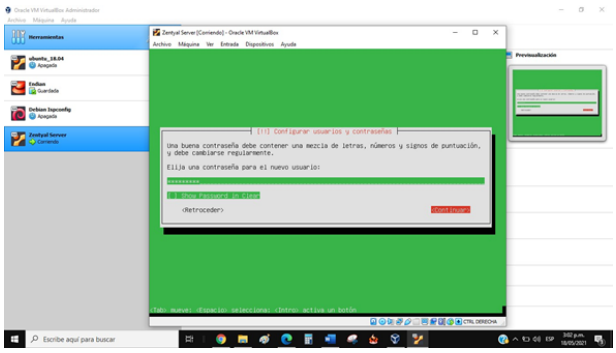

Figura 3. Creación de usuario y contraseña

Posteriormente, se espera a que se termine la instalación del sistema y se procede a continuar la instalación de paquetes, y por último poder ingresar al panel de control de Zentyal.

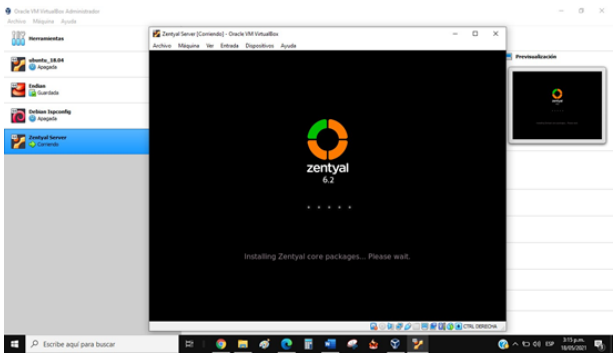

Figura 4. Instalación de paquetes Zentyal

3 TEMÁTICA 1: DHCP Server, DNS Server y Controlador de Dominio

3.1 DHCP Server

El servidor DHCP es un conjunto de reglas que permite asignar direcciones IP y configuración a equipos conectados en una red.

Zentyal tiene un módulo DHCP que permite hacer esta configuración fácilmente con unos pocos clicks. El proceso inicia habilitando e instalando el módulo DHCP en el menú Gestión de software en zentyal.

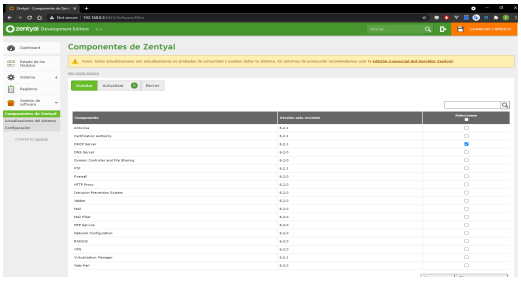

Figura 5. Instalación módulo DHCP

Se debe tener en cuenta que el módulo DHCP debe estar habilitado en el menú “Estado de los módulos” y tener una interfaz de red de tipo “estático”.

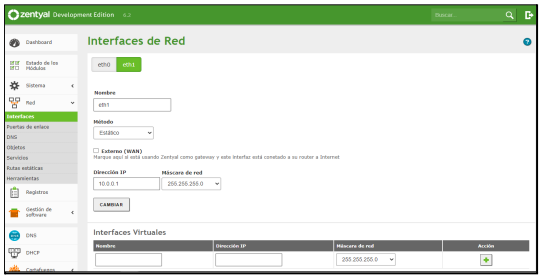

Figura 6. Interfaz estática

Figura 7. Habilitar módulo DHCP

Luego se ingresa al menú DHCP y en la interfaz de red estática configurada donde se define la puerta de enlace, DNS.

Figura 8. Configurar interfaz de red

Figura 9. Configuración Rangos IP

En la interfaz de red configurada se tiene una red interna donde se conecta el servidor DHCP de Zentyal y una maquina con ubuntu Desktop con el fin de brindar la dirección IP dinámicamente en el rango establecido.

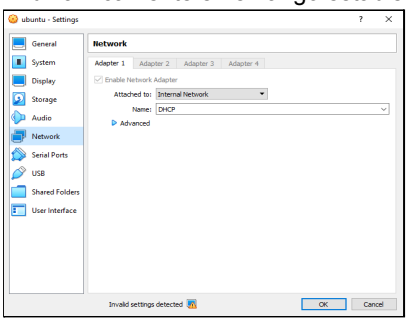

Figura 10. Habilitar conexión red interna ubuntu Desktop

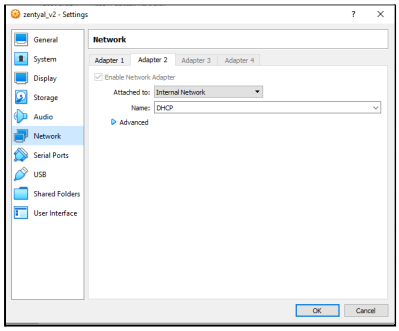

Figura 11. Habilitar conexión red interna Zentyal

Con esta configuración de red interna realizada, se reinicia la máquina de Ubuntu Desktop y se lleva a cabo la comprobación revisando en zentyal y en ubuntu Desktop.

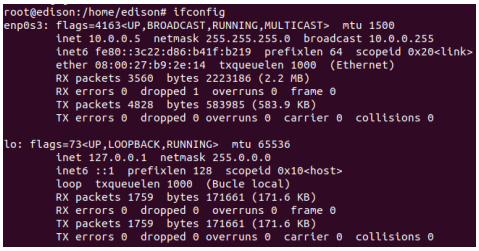

Figura 12. Validación Ubuntu Desktop

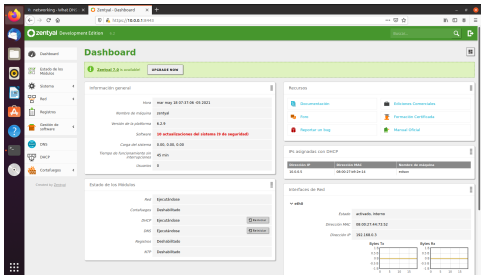

Figura 13. Validación Dashboard Zentyal

3.2 DNS Server

El servidor DNS funciona junto con el servidor DHCP, para esto se realiza la comprobación del DNS actual de la red establecida en el servidor DHCP.

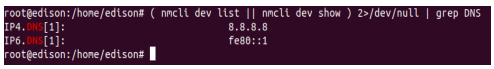

Figura 14. Validación DNS red.

Teniendo el DNS **8.8.8.8** se procede a continuar con la instalación del módulo DNS y habilitando su funcionamiento.

Figura 15. Instalando y habilitando módulo DNS.

En el servidor DHCP se debe realizar la configuración del DNS. En el módulo DHCP se accede al menú y se cambia la opción “Servidor de nombres primario” de Personalizado a DNS local de zentyal.

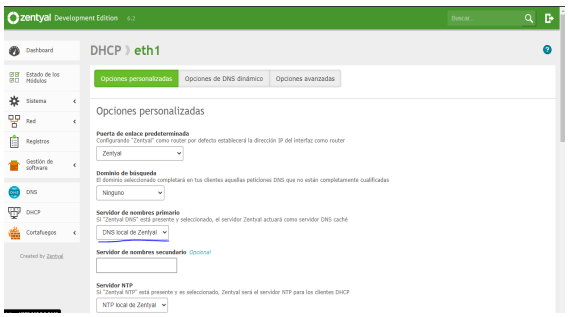

Figura 16. Configuración DNS del DHCP Server.

Guardando cambios y realizando el reinicio de la red en la máquina Ubuntu Desktop se tiene que el DNS de la red ha cambiado.

```
root@edison:/home/edison# systemctl restart NetworkManager.service
root@edison:/home/edison# ( nmcli dev list || nmcli dev show ) 2>/dev/null | grep DNS
IP4.DNS[1]:                             10.0.0.1
root@edison:/home/edison#
```

Figura 17. Validación DNS

3.3 Controlador de Dominio

El controlador de Dominio permite tener la autenticación y control de acceso a recursos compartidos entre equipos de una red.

El proceso en Zentyal para instalar el controlador de dominio inicia instalando y habilitando el componente en zentyal en el menú “Gestión de Software”.

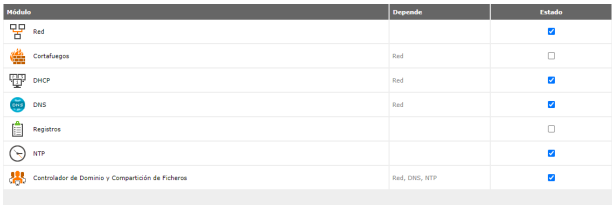

Figura 18. Activación de controlador de dominio

Se crea el dominio que se quiere controlar en la red en el módulo DNS.

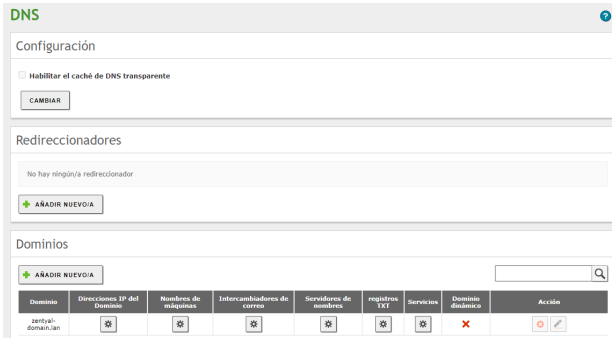

Figura 19. Creación dominio

Luego se ingresa al módulo Usuarios Y Equipos del cual se crea un nuevo usuario para realizar la autenticación respectiva luego en el dominio.

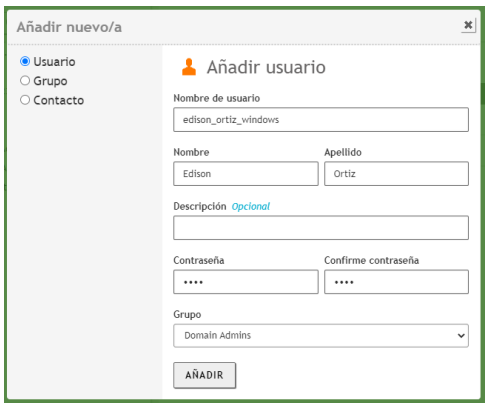

Figura 20. Creación usuario

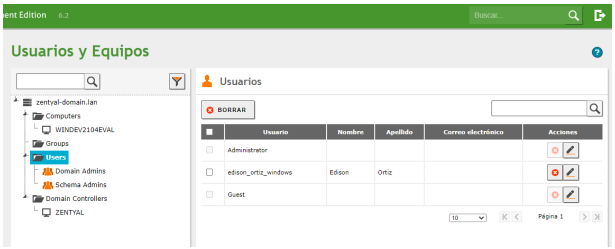

Figura 21. Validación del usuario creado

Luego se procede a conectar un equipo a la red interna que se tiene con el fin de realizar la prueba de conexión al dominio. Para este caso se utiliza una máquina windows.

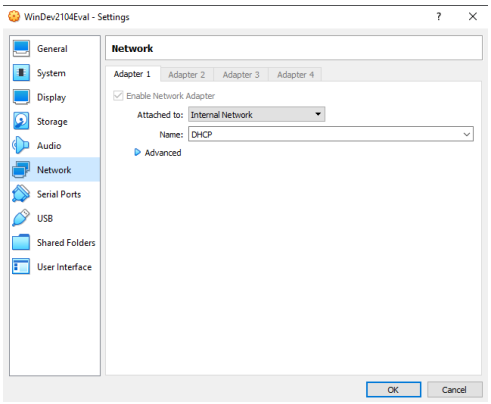

Figura 22. Configuración red interna

Se valida la ip y el DNS que tiene la máquina que se va a conectar al dominio.

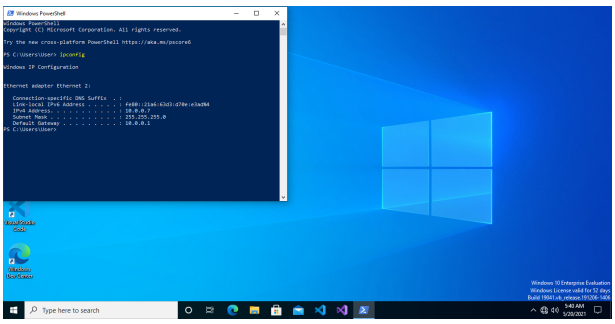

Figura 23. Validación de conexión a la red

Se configura la conexión al dominio y se reinicia la máquina.

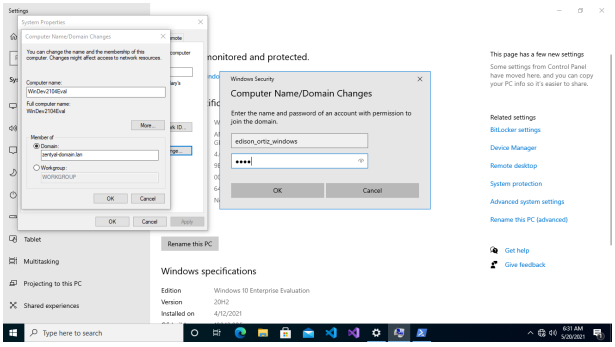

Figura 24. Configuración red interna

Se inicia sesión y se valida que la máquina se encuentre conectada al dominio creado en zentyal.

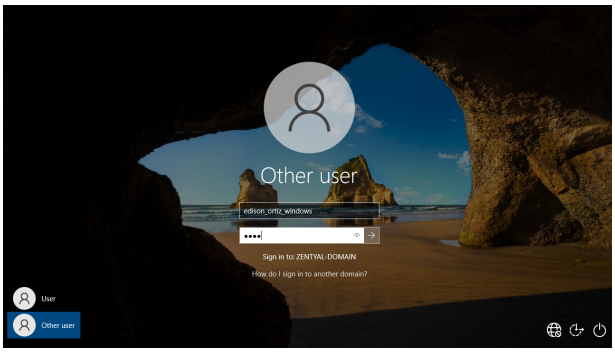

Figura 25. Inicio de sesion en dominio

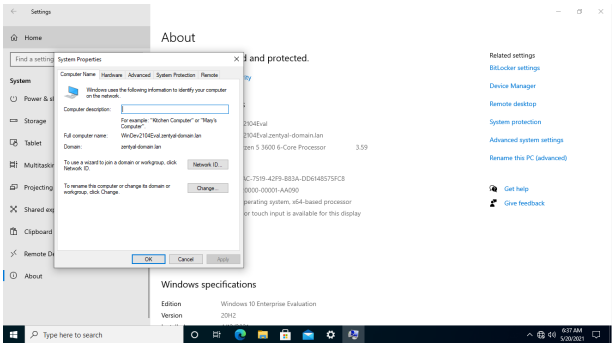

Figura 26. Validación de dominio

4 TEMÁTICA 2: PROXY NO TRANSPARENTE

Se debe configurar el 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 el puerto 1230.

Se inicia el proceso de configuración inicial de Zentyal 6.2 ingresando el usuario administrador y su contraseña:

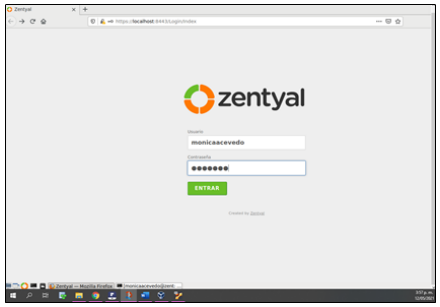

Figura 27. Iniciar sesión en Zentyal server

En la configuración inicial, se escogen los paquetes necesarios que se desean instalar, en este caso, se instala el paquete HTTP Proxy:

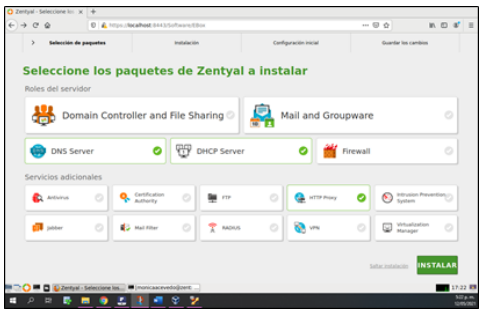

Figura 28. Seleccionar paquete a instalar

Terminada la instalación de los paquetes, se configuran las interfaces. La interfaz eth0, que es el adaptador 1 (según lo ajustado en VirtualBox), es la conexión externa (WAN), por lo que se marca la opción “External” y la interfaz eth1, que es la red interna, se selecciona la opción “Internal”:

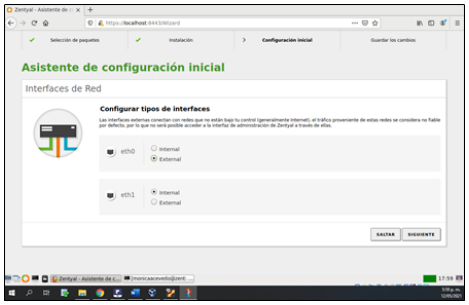

Figura 29. Configurar tipos de interfaces de red

Para el método de configuración de eth0, se escoge como DHCP, tomando como dirección IP: *192.168.1.72*. En eth1, se selecciona el modo Static y como dirección IP para esta interfaz: *192.168.0.1* con máscara de red de 24: *255.255.255.0*

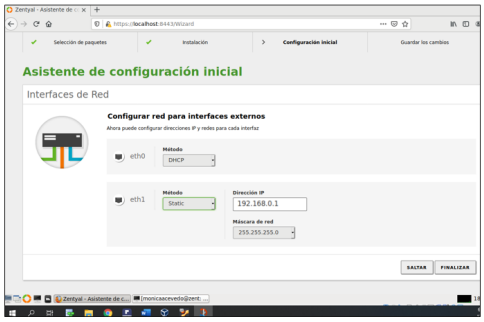

Figura 30. Configurar red para cada interfaz

Al terminar la instalación de los paquetes, muestra un aviso de que se ha completado con éxito la instalación de Zentyal y se ingresa al Dashboard de Zentyal:

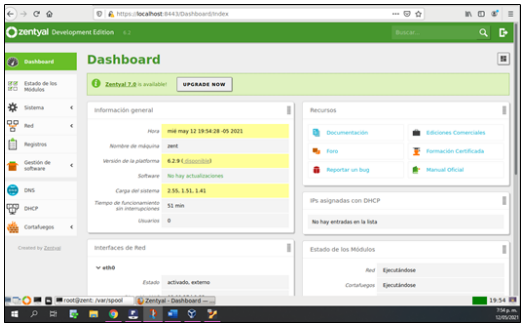

Figura 31. Dashboard de Zentyal

Primero, se verifican las interfaces de red en el panel de izquierdo de "Red"- "Interfaces". En eth0 se confirma que se encuentra con método DHCP y activada la casilla "Externo (WAN)":

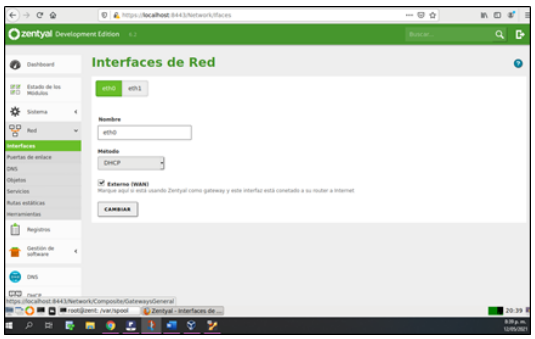

Figura 32. Interfaz de red eth0

Se verifica para la interfaz eth1, que es la red interna, que el método sea "Estático", la casilla debe encontrarse desactivada y la dirección IP debe ser *192.168.0.1/24*

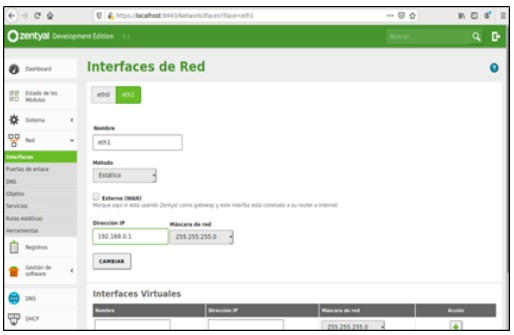

Figura 33. Interfaz de red eth1

Para comenzar con la configuración de HTTP Proxy, se debe ingresar al panel de "Red" – "Objetos y "Añadir nuevo". Este permitirá identificar el grupo al que se le aplicarán las reglas. Se le asigna un nombre al objeto: *UbuntuDesk*:

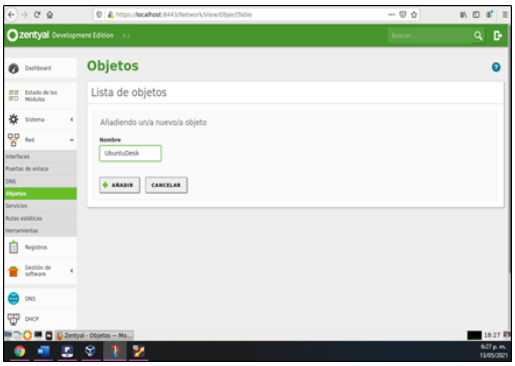

Figura 34. Añadir objeto

Se muestra el objeto creado:

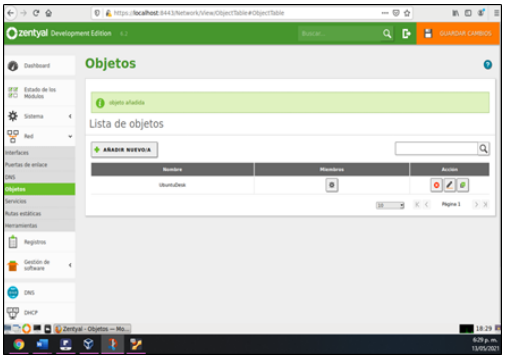

Figura 35. Objeto creado

En la misma página de "Objetos" donde se identifica al nuevo objeto creado, se muestra la columna Miembros con un botón de engranaje para poder agregarlos. Al ingresar a la página de Miembros, clic en "Añadir nuevo". Se especifica un nombre al nuevo miembro (*PC1*) y su dirección IP: *192.168.0.10*

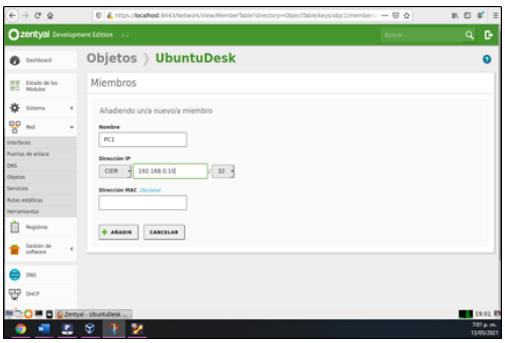

Figura 36. Configurar nuevo miembro

En el panel izquierdo, se ingresa al servicio HTTP Proxy y se selecciona la opción “Configuración general”. Se verifica que la casilla Proxy transparente NO esté activada. Esto significa que se configurará como Proxy no transparente, por lo cual se deberá especificar en cada navegador de un equipo, la dirección IP del proxy y el puerto para su uso. Se asigna el número de puerto requerido: 1230:

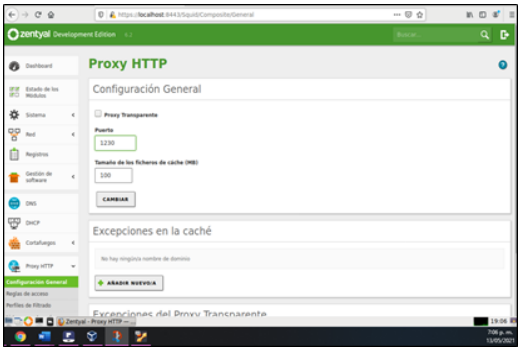

Figura 37. Configurar HTTP Proxy no transparente

En el mismo panel izquierdo de Proxy HTTP, se selecciona “Reglas de acceso”, donde se asignará quienes podrán acceder al Web Proxy.

Para configurar una regla de acceso, se puede escoger un periodo de tiempo para que se aplique según los días de la semana y horas. En “Origen”, se selecciona “Objeto de red”, y enseguida, se especifica el objeto que fue creado anteriormente: *UbuntuDesk*. Finalmente, en “Decisión”, se escoge la opción “Denegar todo”:

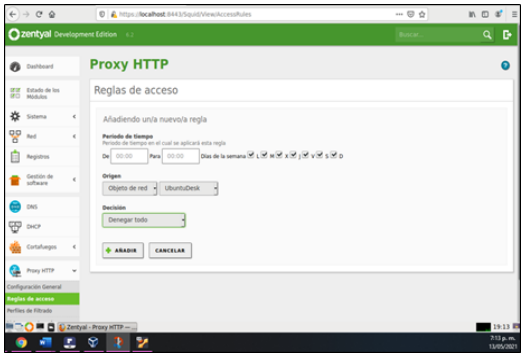

Figura 38. Configurar regla de acceso para denegar

Se muestra la regla de acceso creada como “Denegar todo”:

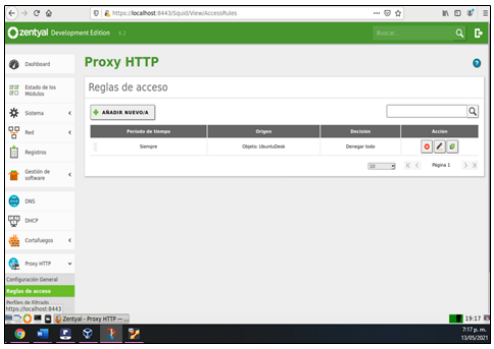

Figura 39. Regla de acceso creada para denegar todo

En el panel izquierdo en “Estado de módulos”, se debe verificar que el servicio HTTP Proxy esté habilitado, para que los clientes se puedan conectar al servidor proxy. Además, en el Dashboard de Zentyal, se verifica en la sección de “Estado de los módulos, que el servicio HTTP Proxy esté ejecutándose:

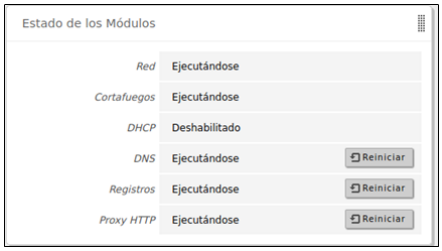

Figura 40. HTTP Proxy ejecutándose

En el equipo cliente Ubuntu Desktop, se configura en VirtualBox, el adaptador 1 como Red interna y el segundo como Adaptador puente. Al iniciar sesión se le asigna una dirección IP estática, teniendo en cuenta que se encuentre dentro del mismo segmento de la red interna del server y que sea la misma dirección de la configuración anterior de nuevo miembro. *Dirección IP: 192.168.0.10* y *Gateway (servidor Zentyal): 192.168.0.1*

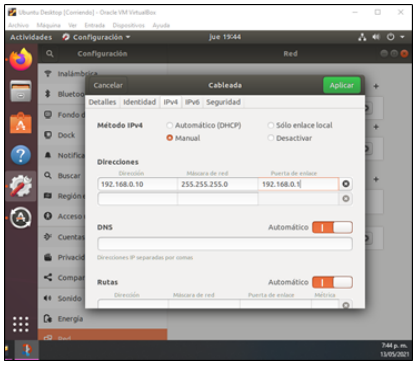

Figura 41. Configurar dirección IP estática en cliente

Antes de configurar el Web proxy en el equipo cliente Ubuntu Desktop, se verifica en el navegador que tenga conexión. Luego se ingresa al menú y “Preferencias”, donde al final de esta, en la sección de “Configuración

de red", se oprime el botón "Configuración". En la ventana de "Configuración de conexión", se activa la opción "Configuración manual del proxy" y se indica la dirección IP del Proxy HTTP: *192.168.0.1* con el puerto *1230.*

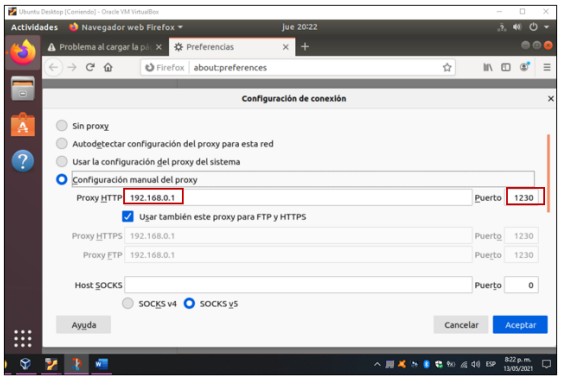

Figura 42. Configurar Proxy HTTP en equipo cliente

En el navegador web del cliente, se ingresa a una página web y se verifica que se está rechazando la conexión debido al proxy:

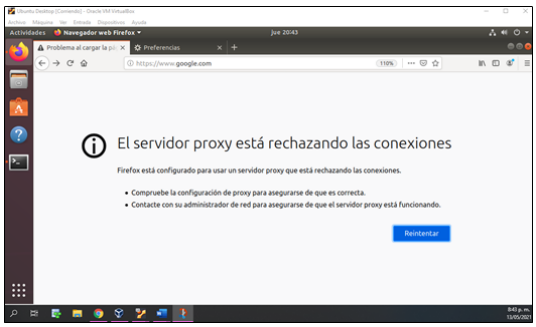

Figura 43. Servidor proxy rechaza la conexión

Para realizar otra prueba y comprobar que está funcionando el Proxy HTTP, se cambia la regla de acceso en el Zentyal a "Permitir todo":

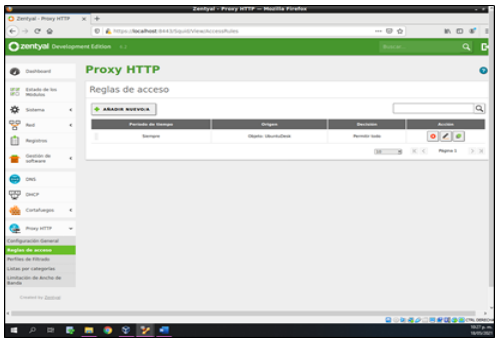

Figura 44. Configurar regla a permitir todo

Al actualizar la página web del navegador, nuevamente se tiene conexión a Internet debido a este cambio de regla en el proxy:

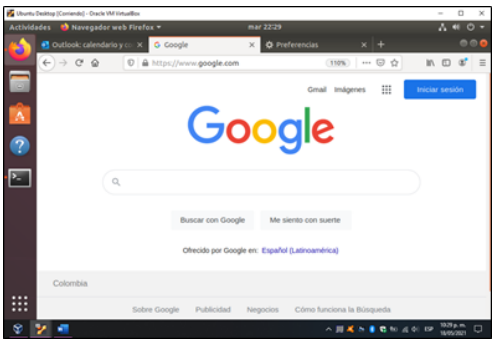

Figura 45. Navegación en Internet por Proxy HTTP

5 TEMÁTICA 3: CORTAFUEGOS

Luego de tener Zentyal instalado en la máquina, y después de actualizar desde la terminal con sus respectivos comandos, se procede a ingresar al panel de control de Zentyal con las credenciales del usuario que fueron asignados en la instalación.

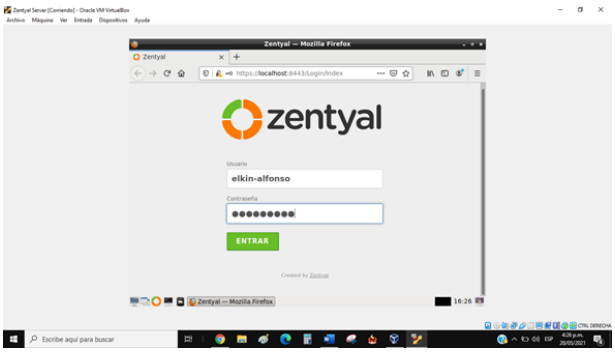

Figura 46. Ingreso de credenciales en Zentyal

Se selecciona el servicio a instalar, el cual corresponde a "Firewall", necesario para el desarrollo de la temática.

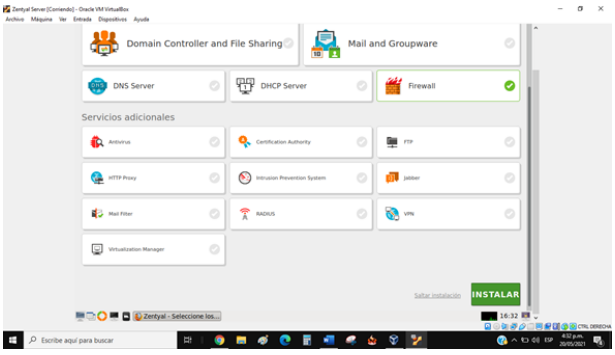

Figura 47. Selección de servicio Firewall

Se muestran los paquetes que son necesarios para la configuración del servicio. Para la configuración de la red es necesario "Network Configuration", y para el cortafuegos "Firewall".

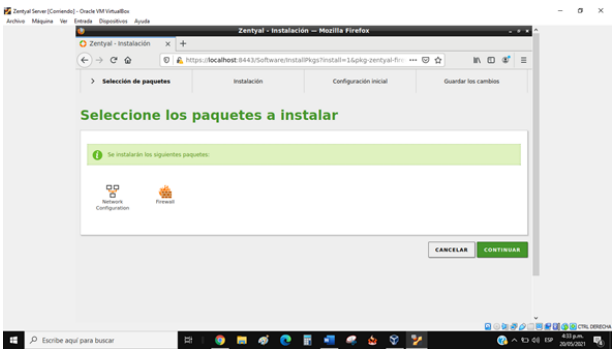

Figura 48. Paquetes a instalar para el servicio

Finalizando el proceso de instalación, se debe realizar la configuración de las interfaces de red. Es necesario tener en cuenta que para aplicar el servicio de cortafuegos en la red se debe tener dos interfaces: la primera para la red WAN se establece como “External” con acceso a internet, y la segunda se establece como “Internal”, la cual corresponde a la red LAN donde se encuentra el equipo Desktop para realizar las pruebas correspondientes a la temática. Además, La interfaz eth0 (WAN) se debe configurar como DHCP para que el router del servicio de ISP le asigne la IP correspondiente; para la interfaz eth1 (LAN) se establece como “Static” para poder asignar una IP 192.168.10.1 con mascara de red 24.

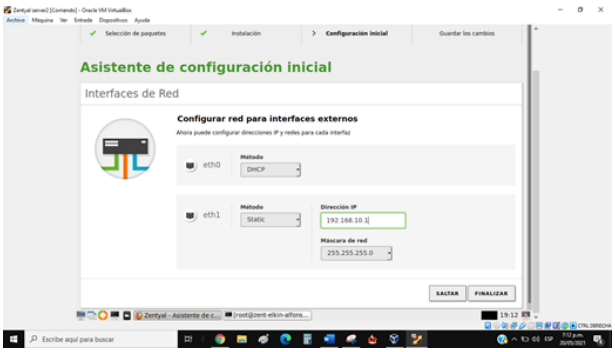

Figura 49. Configuración de interfaces de red

Terminado el proceso de instalación y configuración, se procede a revisar el estado de las interfaces de red, y comprobar que ambas se encuentren activadas.

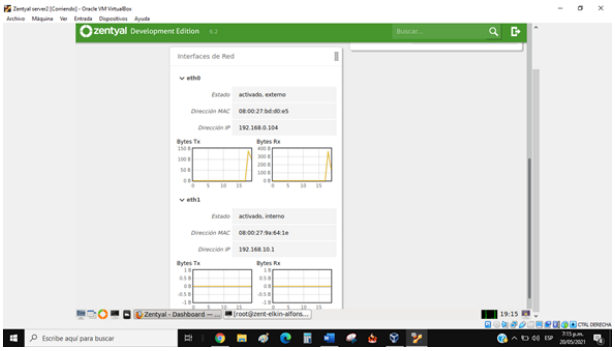

Figura 50. Interfaces de red activadas

Teniendo toda la parte de red configurada, se procede a iniciar el equipo Desktop para realizar la configuración de la interfaz de red que conecta con la red interna. Se le asigna un IP 192.168.10.2 con un Gateway correspondiente a la IP del servidor Zentyal.

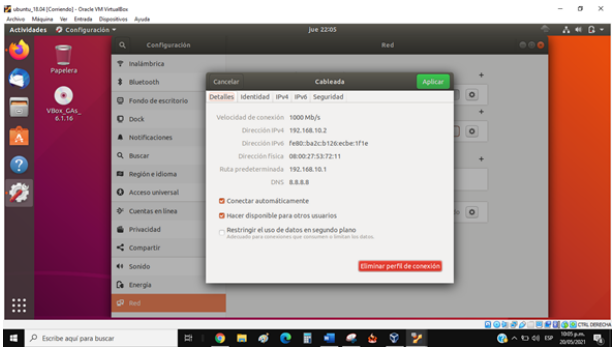

Figura 51. Configuración interfaz de red en Desktop

Se procede a realizar un ping hacia el servidor Zentyal comprobando su conexión dentro de la red interna.

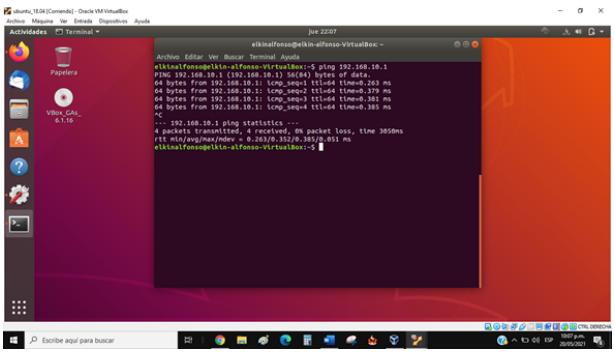

Figura 52. Ping a servidor desde Desktop

Posteriormente, se revisa que haya conexión a internet, por lo tanto, se ejecuta el navegador y se ingresa a sitios como YouTube, Facebook y Wikipedia. El servidor Zentyal proporciona la vía para el acceso a internet de la red LAN debido a que por defecto Zentyal sirve de enrutador.

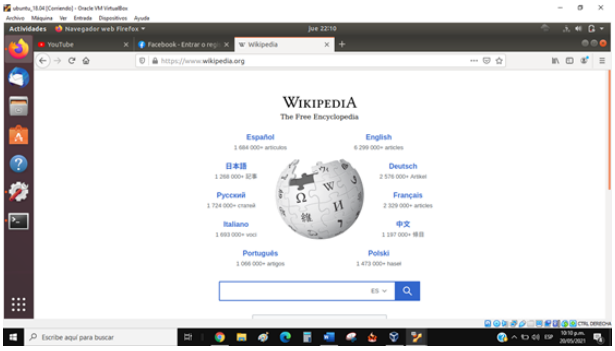

Figura 53. Comprobación de acceso a internet

Teniendo todo configurado y en marcha en el equipo Desktop de la red LAN, se procede a crear un

objeto en sección de “Red” del panel del servidor. Dentro del objeto Desktop se crea un miembro con un rango de IP correspondiente a los equipos que se encuentran en la LAN.

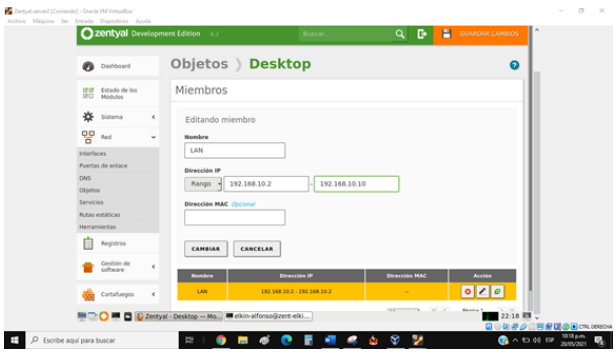

Figura 54. Creación de Objeto para Desktop en red LAN

Se verifica el filtrado de paquetes en la sección de cortafuegos, donde se puede observar 4 opciones para la creación de reglas, en las que se puede agregar reglas en diferentes direcciones, involucrando el Zentyal, red LAN y red WAN.

Figura 55. Opciones de filtrado de paquetes de Cortafuegos

Se ingresa a la opción de Reglas de filtrado para redes internas, donde se creará la regla para restringir el acceso a páginas de entretenimiento. Existe una regla por defecto, la cual permite el acceso a internet desde los equipos de la LAN, definida con un origen cualquiera, un destino cualquiera y desde cualquier servicio. Los servicios envuelven protocolos y puertos.

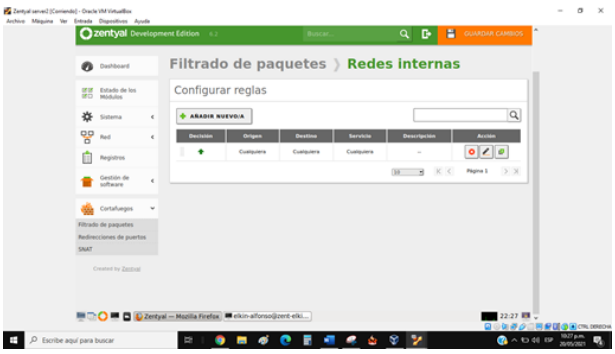

Figura 56. Regla para el acceso a internet en redes internas

De nuevo en el equipo Ubuntu desktop, se realiza un ping a Facebook, evidenciando conexión. También se muestra una dirección IP del sitio *157.240.6.35* con la que se buscará la dirección CIDR que agrupa todos los bloques de direcciones de Facebook.

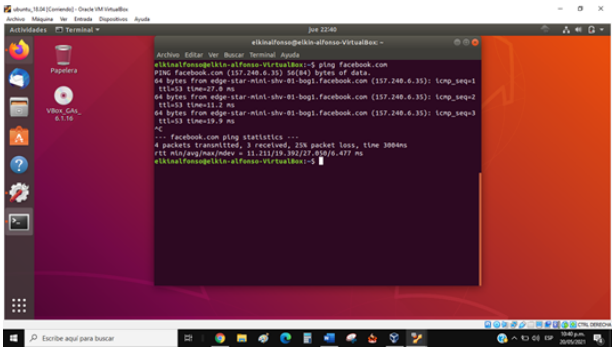

Figura 57. Ping a Facebook desde Desktop

Con la IP de Facebook obtenida, se ingresa a la página https://whois.arin.net para verificar el rango de IP de Facebook y la dirección CIDR y así poder denegar el acceso completo. Se muestra una IP de red *157.240.0.0/16.*

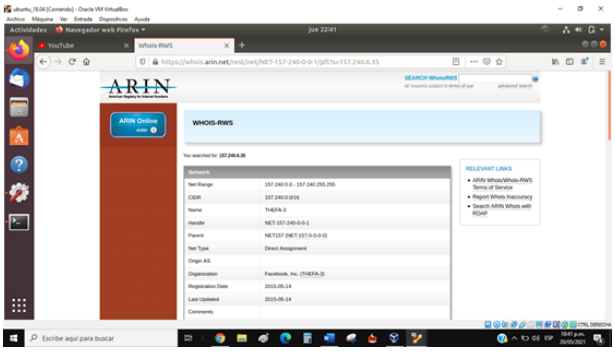

Figura 58. Verificación de IP CIDR Facebook

Teniendo la IP del sitio, se procede a crear un objeto en Zentyal, el cual se le asigna el nombre de Facebook, se crea un nuevo miembro al que se le ingresa la dirección IP 157.240.0.0/16 y se añade al objeto.

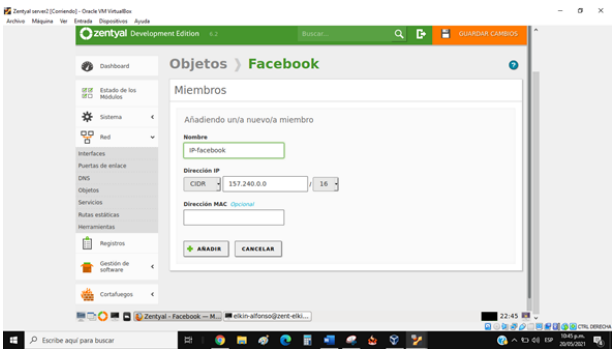

Figura 59. Creación de objeto Facebook

Se ingresa de nuevo al filtrado de paquetes para redes internas y se procede a crear la regla. Se ingresa la información para denegar el acceso a Facebook, con el objeto de origen Desktop y el objeto de destino Facebook, con cualquiera de los servicios establecidos.

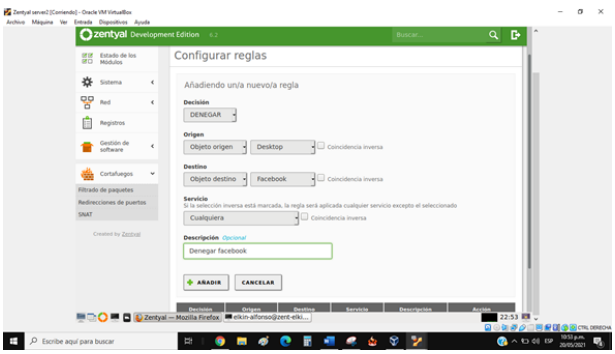

Figura 60. Configuración de regla para denegar acceso a Facebook

Teniendo lista la regla creada para denegar el acceso a Facebook, se accede al equipo desktop, se ingresa al navegador y se intenta ingresar a Facebook, evidenciando que se queda estático y no permite la entrada.

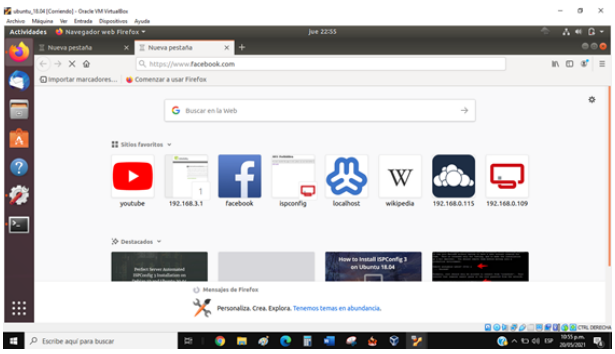

Figura 61. Acceso denegado a Facebook

También se procede a hacer un ping reconociendo la IP, sin embargo, no se obtiene respuesta ya que el acceso al sitio está denegado.

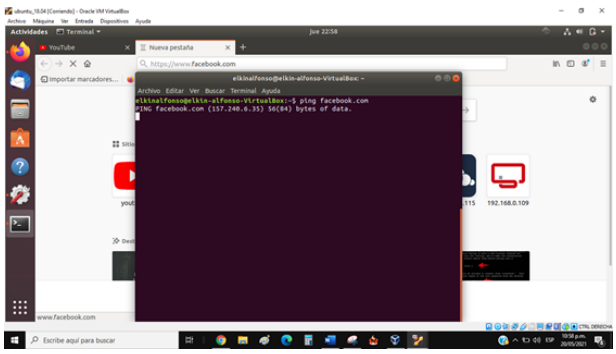

Figura 62. Ping sin salida a Facebook

Posteriormente se realiza la prueba para poder acceder de nuevo al sitio, por lo tanto, se procede a eliminar la regla que denegaba el acceso a Facebook, y se guardan cambios.

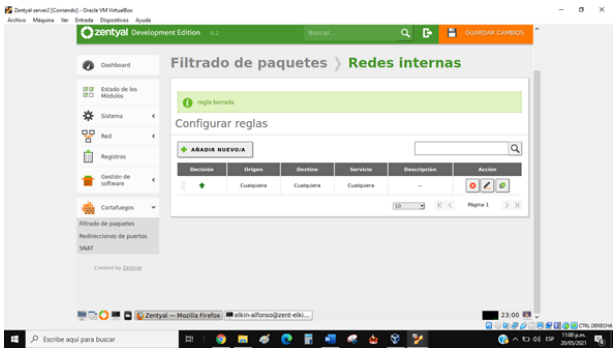

Figura 63. Eliminación de regla

Automáticamente el ping empieza a mostrar la transferencia de paquetes. De igual manera en el navegador se recarga la página y automáticamente se puede acceder al sitio Facebook.

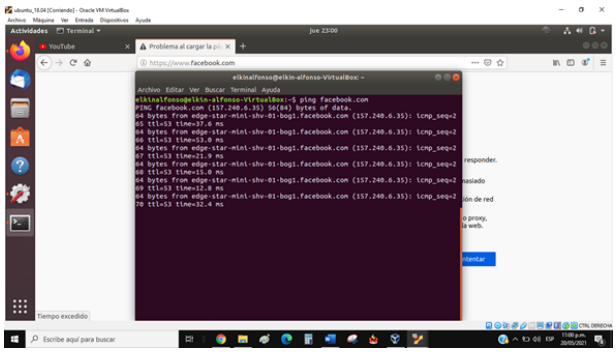

Figura 64. Acceso permitido a Facebook por ping

6 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Para realizar la configuración se debe instalar el módulo de controlador de dominio, compartición de archivos y DNS desde el panel de Zentyal, para lo cual se procede a configurar las interfaces de red:

Primera red DHCP – Externo - WAN.

Figura 65. Primera red DHCP.

Segunda red estática con un segmento diferente. En este caso la red es **192.168.20.100**

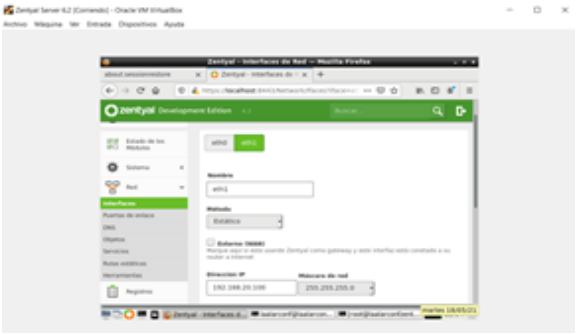

Figura 66. Segunda red estática con un segmento

Para verificar el funcionamiento de la configuración realizada creó dos usuarios, uno en el dominio de administradores y otro para el grupo de alumnos.

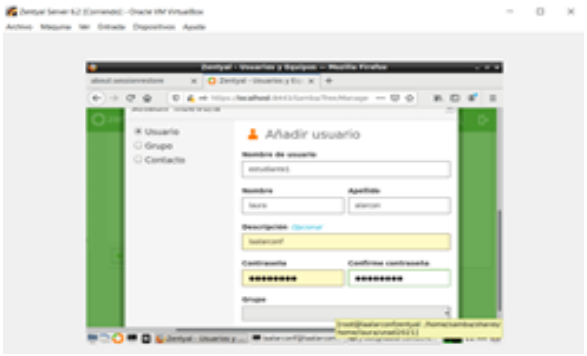

Figura 67. Creación de usuario estudiante 1

Para compartir archivos ingresó a la opción **Compartición de Ficheros** que se encuentra en el **Dashboard**, con esto se crea el directorio compartido y doy clic en Añadir: Ingresó un nombre para la carpeta (archivos).

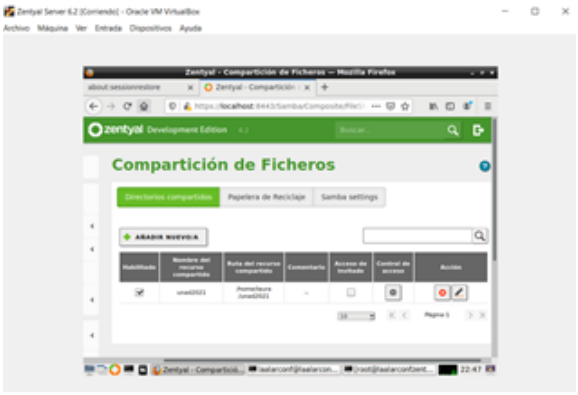

Figura 68.: Carpeta compartida creada.

Una vez creada la carpeta ingresó al control de acceso, donde asigno permisos de lectura y escritura al usuario **estudiante 1**.

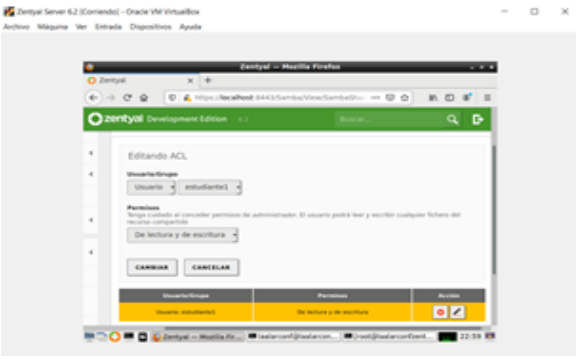

Figura 69. Permisos de acceso.

Después de añadida la ACL, procedemos a acceder desde nuestro cliente en UBUNTU, para esto necesitamos instalar samba que gestiona la conexiones a unidades remotas, esto lo realizamos de la siguiente manera.

Se realiza Instalación de Samba en Ubuntu.

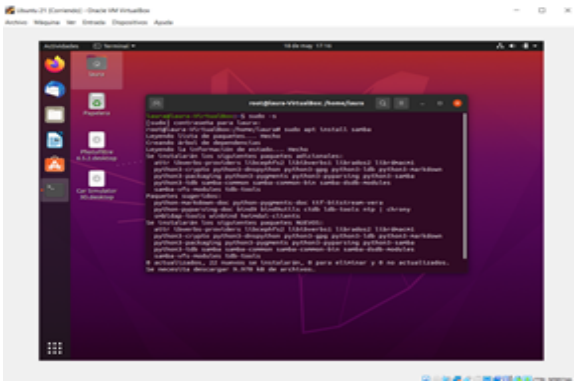

Figura 70. Instalación de Samba en Ubuntu.

Se Modifica el **workgroup de** Samba por el dominio configurado de **Zentyal**.

Figura 71. Dominio configurado de Zentyal.

```
root@laura-VirtualBox:/home# mount -t cifs -o username=estudiante1 //192.168.20.100/unad2021 /home/estudiante1/
Password for estudiante1@//192.168.20.100/unad2021:  ********
root@laura-VirtualBox:/home#
```

Figura 72. Conexión desde Ubuntu a Zentyal.

Desde Zentyal se crean dos archivos dentro de la carpeta **/home/laura/unad2021.**

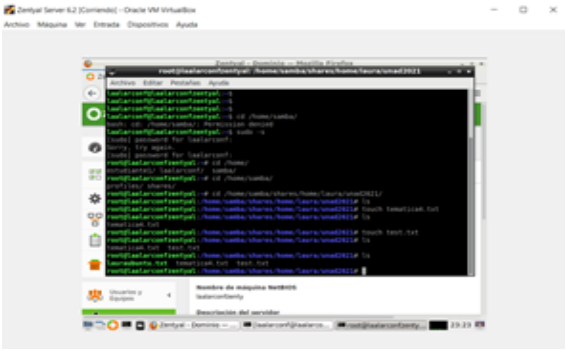

Figura 73. Creación de Archivos desde Zentyal.

Consulta en Ubuntu los archivos creados anteriormente en Zentyal.

```
laura@laura-VirtualBox:~$ sudo -s
[sudo] contraseña para laura:
laura@laura-VirtualBox:~$ cd /home/estudiante1/
laura@laura-VirtualBox:/home/estudiante1$ ls
tematica4.txt
laura@laura-VirtualBox:/home/estudiante1$ ls
tematica4.txt  test.txt
```

Figura 74. Consulta en Ubuntu

Desde Ubuntu se crea un archivo en la carpeta compartida.

```
root@laura-VirtualBox:/home/laura# cd ..
root@laura-VirtualBox:/home# cd estudiante1/
root@laura-VirtualBox:/home/estudiante1# ls
tematica4.txt  test.txt
root@laura-VirtualBox:/home/estudiante1# touch lauraubuntu.txt
root@laura-VirtualBox:/home/estudiante1# ls
lauraubuntu.txt  tematica4.txt  test.txt
root@laura-VirtualBox:/home/estudiante1#
```

Figura 75. Creación de archivo en Ubuntu.

Consulta de archivos desde Zentyal.

```
root@laalarconfzentyal:/home/samba/shares/home/laura/unad2021# ls
lauraubuntu.txt  tematica4.txt  test.txt
```

Figura 76. Consulta en Zentyal.

Se procede a instalar el paquete cups en el servidor Zentyal y desde su interfaz web añadir una impresora por puerto USB y es detectada automáticamente por cups.

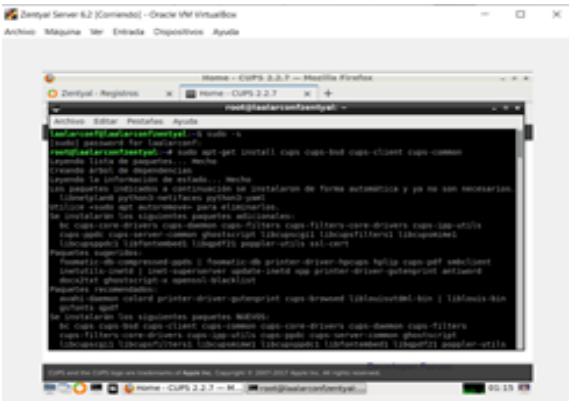

Figura 77. Instalar el paquete cups.

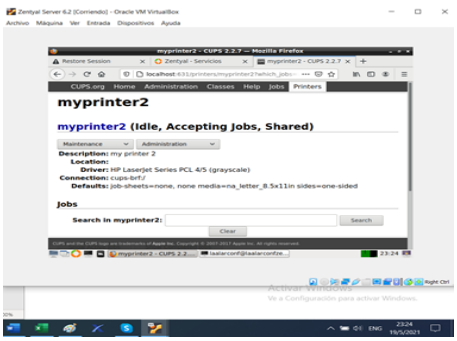

Figura 78. Se crea una impresora.

Se dan permisos en Ubuntu para ver archivos compartidos.

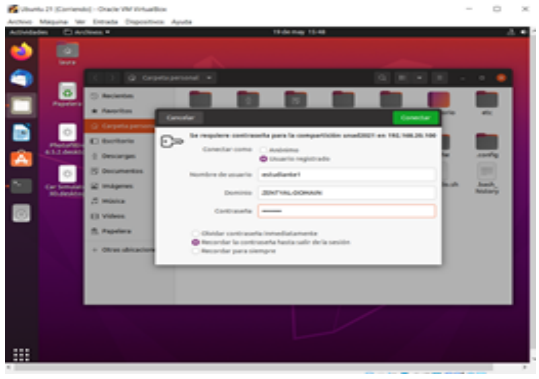

Figura 79. Se dan permisos en Ubuntu para ver archivos compartidos.

Se ingresa con ctrl+L al servidor de Zentyal.

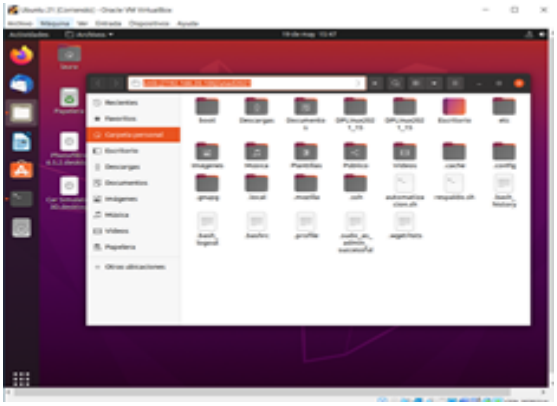

Figura 80. Se ingresa con ctrl+L al servidor de Zentyal.

Se visualizan los archivos compartidos.

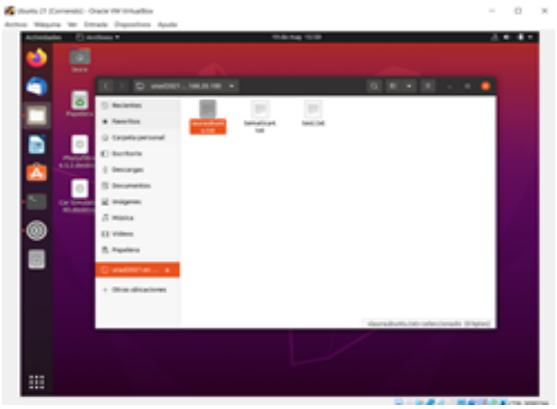

Figura 81. Se visualizan los archivos compartidos

Se imprime un archivo de los relacionados en la carpeta compartida.

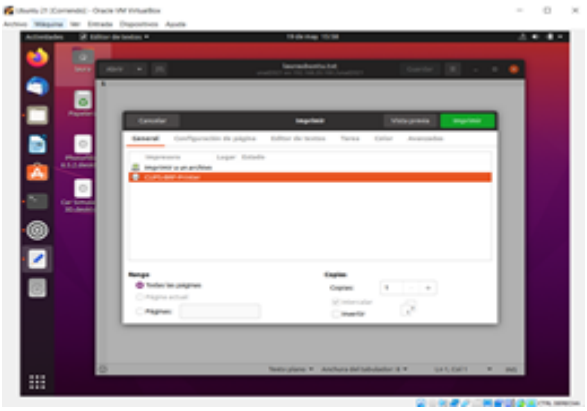

Figura 82. Se imprime un archivo de los relacionados en la carpeta compartida.

Se imprime un archivo de los relacionados en la carpeta compartida.

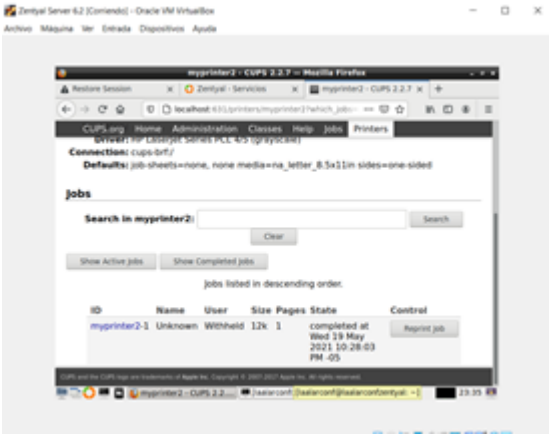

Figura 83. Se imprime un archivo de los relacionados en la carpeta compartida.

7 TEMÁTICA 5: VPN

El objetivo de la temática es la conexión del servidor al cliente Debian a través de internet.

Se creará un certificado de autoridad de certificación con el propósito darle permisos al servidor, para crear certificados de seguridad, es importante para el certificado de acceso a la red VPN que se va a implementar. Se ingresan los datos y se expiden.

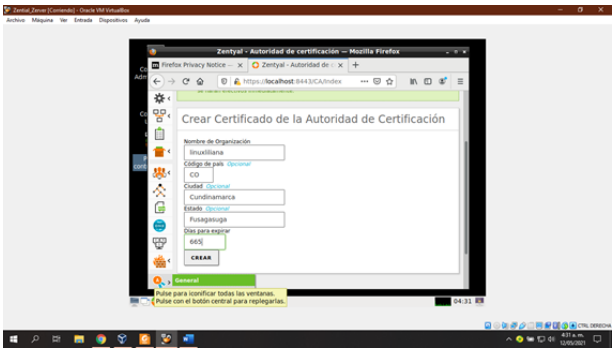

Figura 84. Ingreso de datos para el certificado de autoridad.

Dirige al menú de VPN/ Servidores para crear nuevo servidor VPN, clic en añadir nuevo y añade el nombre de servidor requerido para este caso VPN_liliana

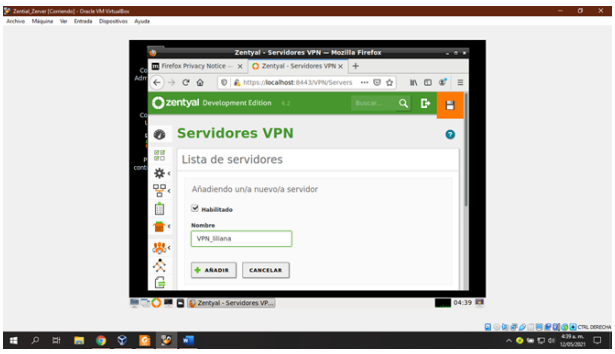

Figura 85. Inserción de nombre VPN_liliana

Se ubicará en el menú de Certificados en Autoridad de certificados/ General, crear un certificado nuevo y caducidad tendrá este, se diligencia la información y expedir.

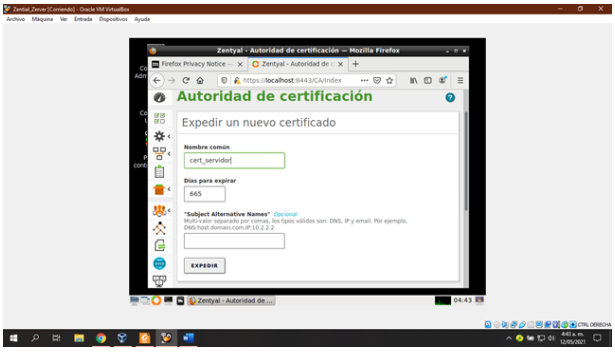

Figura 86. Datos para creación de autoridad de certificación

Menú VPN, y menú VPN/ servidores, para realizar la configuración se diligencia la información de la configuración de la VPN, el puerto que se va a configurar es 1194/UDP.

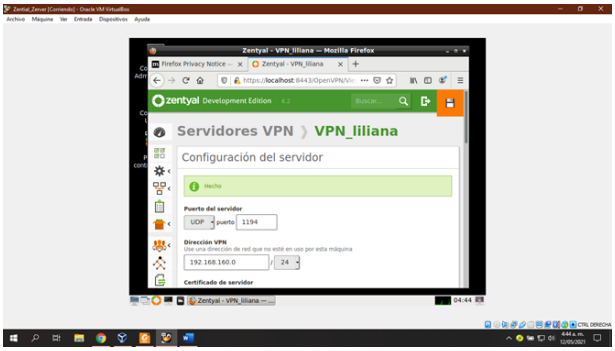

Figura 87. Configuración del servidor VPN_liliana.

Se selecciona el ítem interfaz TUN

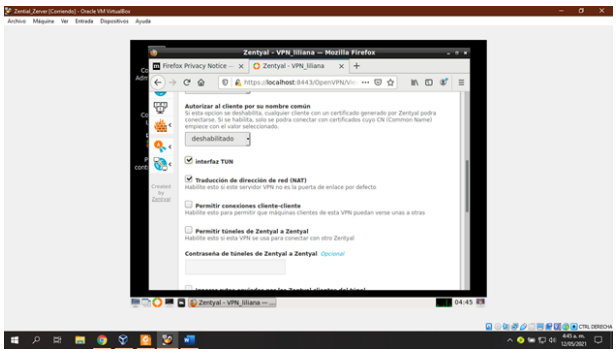

Figura 88. selección de ítem TUN

Selección de todas las interfaces de red.

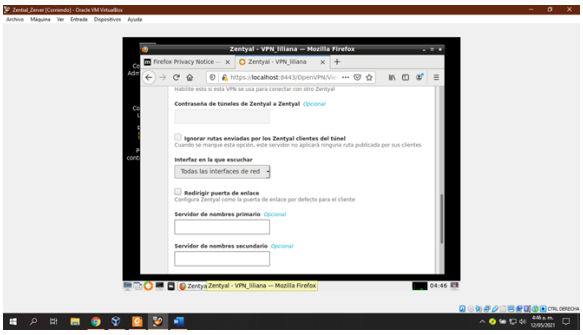

Figura 89. selección de todas las interfaces de red

Se ubicará en red/ Servicios para añadir un nuevo servicio de red.

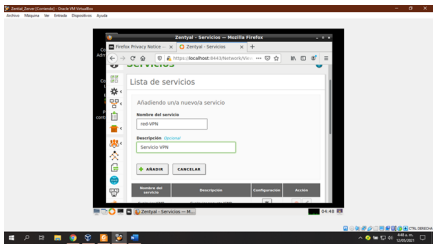

Figura 90. Ingresa de datos para añadir el nuevo servicio

Crean las reglas de excepción para el acceso del servidor en firewall/ filtrado de paquetes en el menú principal.

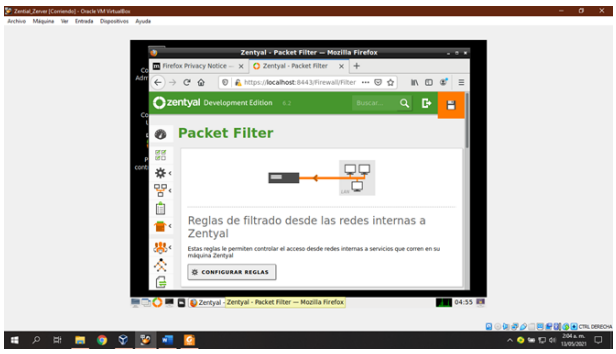

Figura 91. menú para crear las reglas de acceso a servidor

Procede a la configuración de la regla.

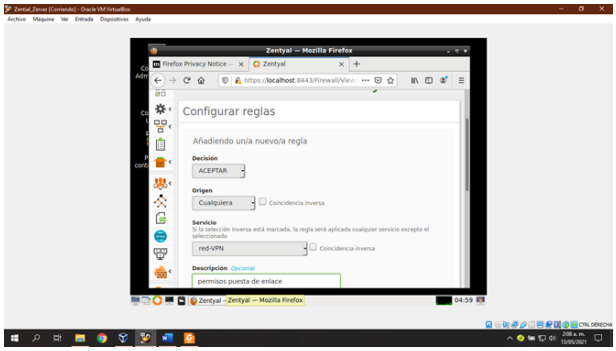

Figura 92. configuración de la regla.

Verifica la red configurada por el mismo servidor por defecto. A través de menú de redes anunciadas, se verifica la dirección de mi servidor Dirección ip 186.84.88.169 y verificacion de la dirección ip del servidor red LAN

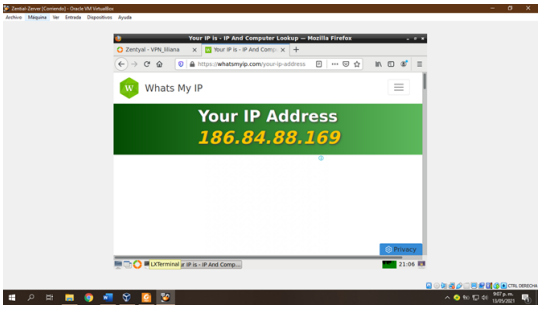

Figura 93. Verificación de mi IP servidor.

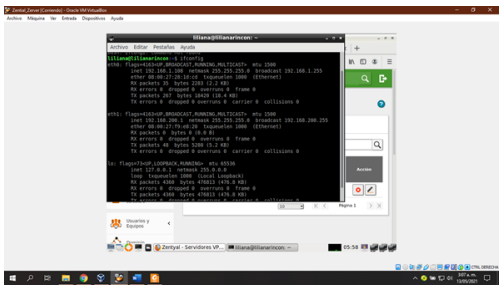

Figura 94. IP del servidor LAN.

Se descarga el paquete de configuración del cliente. En tipo cliente es el sistema operativo desde el cual se conecta Linux, el certificado del cliente es el creado anteriormente. para ello se diligencia la dirección del servidor la IP de la WAN (salida de internet o del enrutador) y en dirección adicional pondremos la dirección IP del servidor

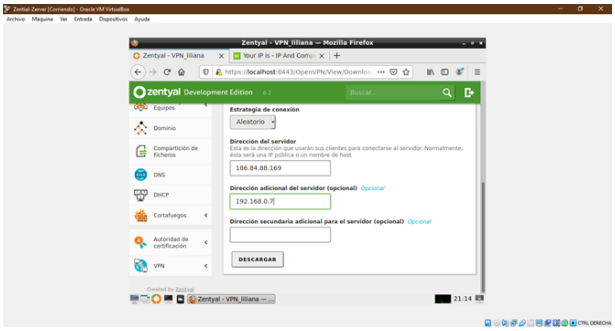

Figura 95. direccionamientos IP

Configuración a la máquina cliente Debian.

Se ingresa a su – ya que si se realiza con su al realizar la conexión e instalación genera error al realizar la configuración para conectar al servidor. Se instala openvpn VPN a través del comando apt-get install openvpn.

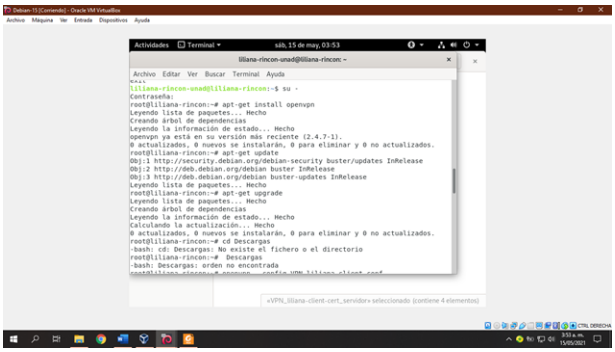

Figura 96. Instalación de PVN

Hay que tener en cuenta el archivo VPN_liliana-client.conf para la conexión al servidor.

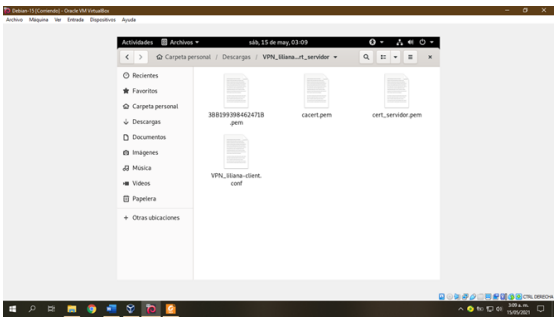

Figura 97. Visualización de los archivos.

Inicia a configurar automáticamente la máquina cliente según los parámetros realizados en el servidor.

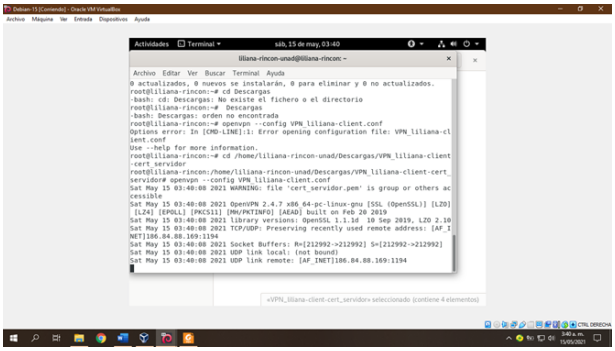

Figura 98. Inicio de la configuración cliente automáticamente

Evidencia de la conexión de secuencia iniciada al servidor Zentyal

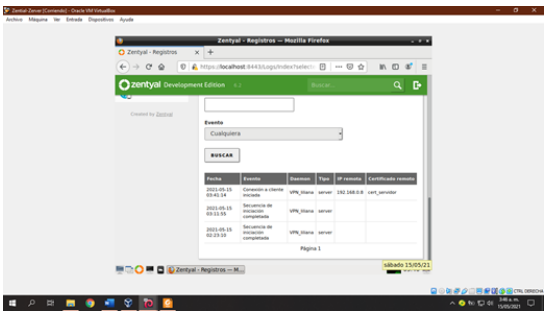

Figura 99. Conexión iniciada al cliente.

Observación de los servicios de SSH (tun0) el enlace de la máquina cliente con el servidor VPN.

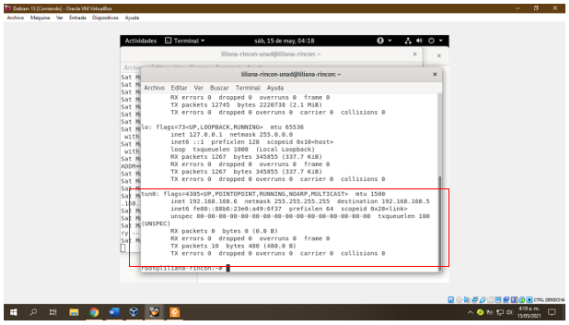

Figura 100. Conexión de servicios tun0 de máquina cliente -servidor.

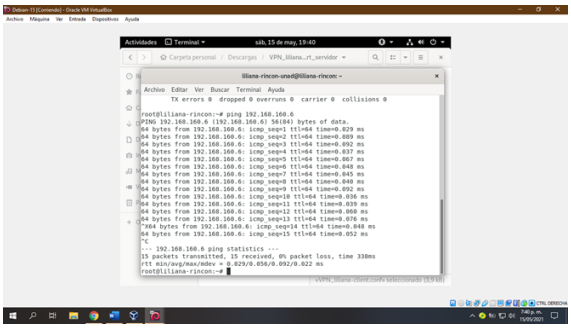

Figura 101. Verificación de la conexión a través de ping

8 CONCLUSIONES

La herramienta Zentyal nos permite realizar configuración de los servicios DHCP, DNS y Controlador de dominio. Estos permisos tienen un alto nivel de personalización como habilitar rangos de IP para el servidor DHCP, crear DNS personalizado, y controlar los accesos y recursos compartidos a través del controlador de dominio.

Por medio de Zentyal, también se pueden manejar otros servicios, como HTTP Proxy, que sirve como equipo intermediario entre el cliente y el servidor destino. El Proxy es quien se encarga de filtrar todos los paquetes entre estos. Este recibe las peticiones del usuario para acceder a una página, y este se encargará de transmitirlas al servidor de la web para que no conozca los datos del cliente. Con un proxy no transparente, se debe especificar en cada navegador del cliente o equipo, la dirección IP del servidor proxy y el puerto para su posible navegación. Para esta configuración, se tuvo en cuenta un puerto distinto al preseleccionado 3128 a 1230, donde el servidor escuchó las peticiones entrantes y se aceptaron o rechazaron las conexiones según la regla de acceso establecida.

Zentyal ofrece servicios que fácilmente se pueden instalar, configurar y administrar desde su panel de control. En cuanto a seguridad, ofrece un servicio de cortafuegos que permite configurar la conexión entre subredes, además de facilitar el establecimiento de reglas para el filtrado de paquetes, evitando los accesos

a la red por parte de entes maliciosos, y permitiendo denegar el acceso desde las redes internas hacia sitios que puedan vulnerar la seguridad del sistema.

A través de zentyal permite administrar los servicios de red como acceso a internet, seguridad de la red, permitiendo la integración del control de soporte de redes privadas. VPN es muy utilizado en la actualidad para diferentes empresas el cual se expone la seguridad de la información de la misma. Como por ejemplo es utilizado para teletrabajo, censura y bloqueos geográficos de contenidos, A través de Zentyal se puede controlar todo esto indicando las reglas que se desea para cada cliente y sus accesos o restricciones entre otras. Zentyal se caracteriza por tener compatibilidad con sistemas operativos como Windows, Linux y Mac OS, además es sencillo de instalar, configurar y mantener que IPSec, esto hace que haya otra opción VPN en software libre.

9 REFERENCIAS

[1] Zentyal. (s.f). Documentación Oficial. Disponible en https://doc.zentyal.org/es/

[2] Zentyal. (s.f). Documentación de Zentyal 6.2. Servicio de redes privadas virtuales (VPN) con OpenVPN. Disponible en: https://doc.zentyal.org/6.2/es/vpn.html

[3] Zentyal. (s.f). Documentación de Zentyal 6.2 – Instalación. [En línea]. Disponible en https://doc.zentyal.org/6.2/es/installation.html#el-instalador-de-zentyal

[4] Zentyal. (s.f). Servicio de Proxy HTTP. [En línea]. Disponible en https://doc.zentyal.org/es/proxy.html

[5] Zentyal. (s.f). Cortafuegos. [En línea]. Disponible en https://doc.zentyal.org/6.2/es/firewall.html

[6] Gómez, J. (2014). Zentyal - Instalar y configurar DHCP Server. [En línea]. Disponible en https://www.youtube.com/watch?v=H5lhAKOH5LM

[7] Gómez, J. (2014). Zentyal - Instalar y configurar DNS Server. [En línea]. Disponible en https://youtu.be/bmROdq3pRmc

[8] Zentyal. (2019). Zentyal como único Controlador de dominio (Tutorial 1). [En línea]. Disponible en https://www.youtube.com/watch?v=ogr9L67JcMg&t=37s