Instalación y configuración del Servidor Zentyal en zona DMZ del cortafuegos Endian

Carlos Ramírez, Alejandro España, Katerine Zapata, Jade Hernandez, Edward Fuentes
caramirena@unadvirtual.edu.co, eaespanaam@unadvirtual.edu.co, kzapatam@unadvirtual.edu.co,
jshernandezb@unadvirtual.edu.co, effuentesj@unadvirtual.edu.co

***Resumen*— El presente artículo desarrolla la instalación y configuración del servidor Zentyal en su versión 6.2 en una de red empresarial en la cual previamente existe un cortafuegos Endian; este último será utilizado únicamente para la demarcación de las zonas de roja, verde y naranja, las cuales se consideran como internet, red interna local y la zona desmilitarizada, respectivamente. En la configuración presentada, se instalarán y pondrán en marcha diversos servicios con el fin de dar solución a la problemática planteada. El artículo se divide en temáticas, dentro de las cuales se abordará el paso a paso de la instalación, configuración y puesta en marcha de los servicios: DNS Server, DHCP Server, Controlador de dominio, Proxy, Firewall, File Server, Print Server y VPN.**

***Palabras clave*—** Zentyal, Endian, Linux, Ubuntu, Opensource, cortafuegos, servicios, instalación, configuración.

***Abstract*--This article develops the installation and configuration of the Zentyal server in version 6.2 on an enterprise network on which an Endian firewall previously exists; the latter will be used only for the demarcation of the red, green and orange areas, which are considered as the internet, local internal network and the demilitarized zone, respectively. In the configuration presented, various services will be installed and implemented in order to solve the problem posed. The article is divided into topics, within which the step-by-step installation, configuration and commissioning of the services will be addressed: DNS Server, DHCP Server, Domain Controller, Proxy, Firewall, File Server, Print Server and VPN.**

***Keywords* —** Zentyal, Endian, Linux, Ubuntu, Opensource, firewall, services, installation, configuration.

I. Introducción

A partir de las temáticas previamente desarrolladas, en donde se realizó la instalación y configuración del cortafuegos Endian Community, se incluirá el Servidor Zentyal como administrador de la infraestructura IT, en donde se pondrán en marcha los diversos servicios solicitados, evidenciando su correcto funcionamiento y con los cuales se dará solución a la problemática planteada.

II. INSTALACIÓN DEL SERVIDOR ZENTYAL

A. Requisitos mínimos

Los requerimientos mínimos de hardware varían de acuerdo con los servicios que serán prestados desde el servidor, sin embargo, se listan las características mínimas con las que debería contar el equipo en el que se pretende instalar el servidor Zentyal:

- CPU Pentium 4
- Arquitectura de 86 o 64 bits
- 2 GB de RAM
- 80GB de Almacenamiento
- 2 tarjetas de red
- Equipo compatible con Ubuntu Bionic 18.04 LTS (Kernel 4.15)

B. Instalación y configuración

Lo primero es crear la maquina virtual que alojara el sistema operativo y configurar sus adaptares de red.

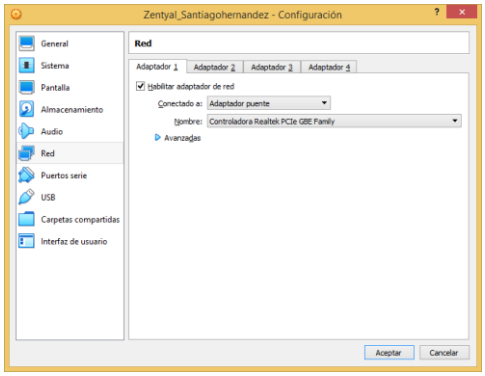

Fig. 1. Configuración adaptador de red

Posteriormente se instala el sistema operativo utilizando el iso descargado de la página oficial de Zentyal

Fig. 2. Instalación de Zential

III. DESARROLLO DE LAS TEMATICAS PROPUESTAS

A. Temática 1: DHCP Server, DNS Server y Controlador de Dominio

Producto esperado: *Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.*

Cuando se inicia Zentyal abre de manera automáticamente el navegador enseñando el panel de control donde se procede a configurar usuario y contraseña.

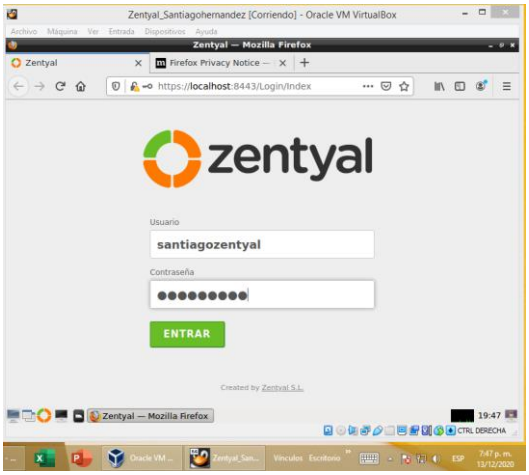

Fig. 3. Primera interfaz de zential

Una vez se diligencie la información requerida se seleccionan los paquetes a instalar en el servidor

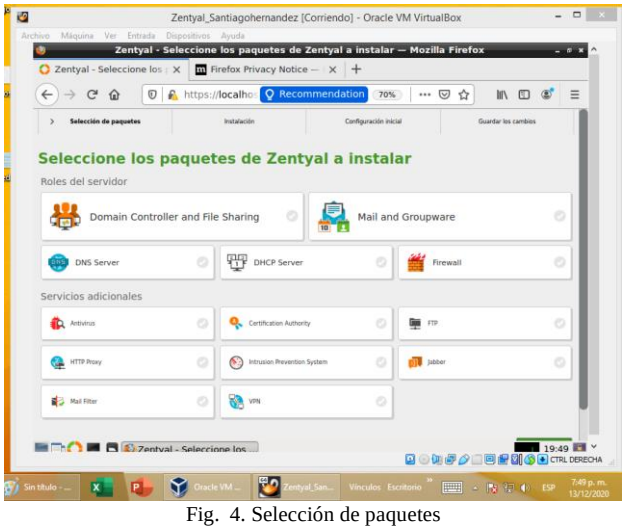

Fig. 4. Selección de paquetes

Luego de seleccionar los sistemas definidos que para esta temática son: DHCP Server, DNS Server y Controlador de dominio, se muestra una interfaz con las instalaciones que se van a ejecutar

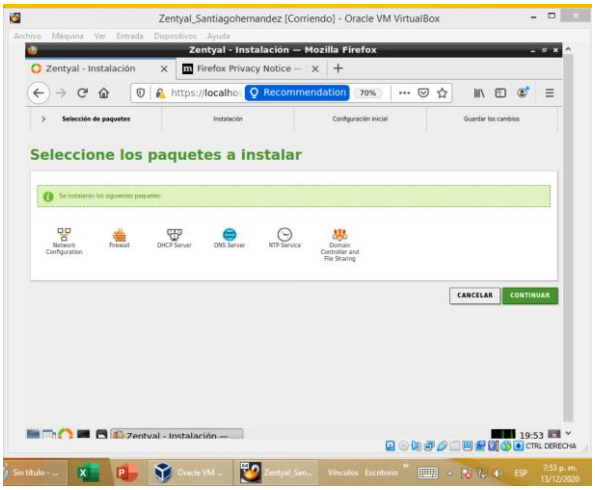

Fig. 5. Confirmación de paquetes a instalar

Una vez terminada la instalación aparece la configuración de los tipos de redes del servidor de manera que una red gestione la salida y otra los servicios internos de la red una de ellas es una IP fija

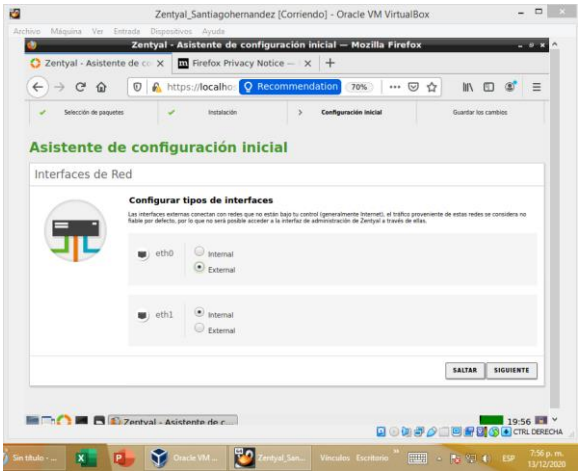

Fig. 6. Configuración de la interfaz eth1

Se hace la configuración de red

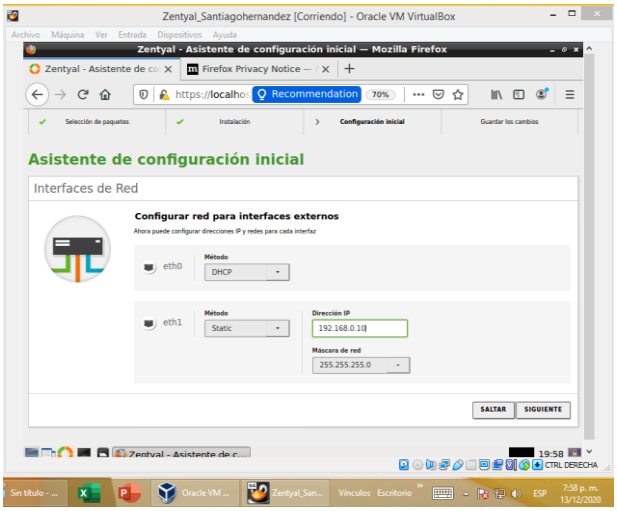

Fig. 7. Adición de dirección ip

Cuando se culmina con las sus últimas adecuaciones se puede acceder al Dashboard, con toda la siguiente configuración

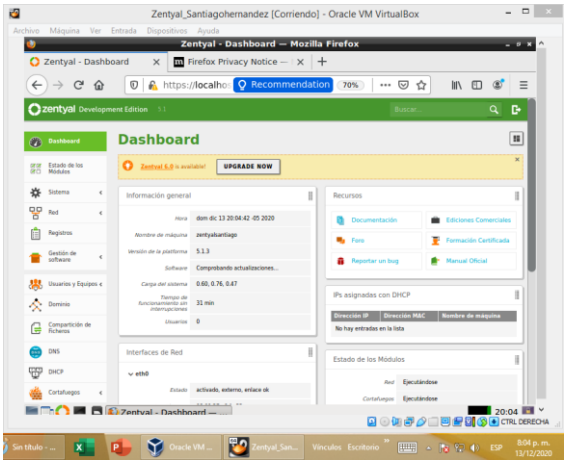

Fig. 8. Dashboard zentyal

A continuación, se establece la configuración y delimitación de las direcciones DHCP.

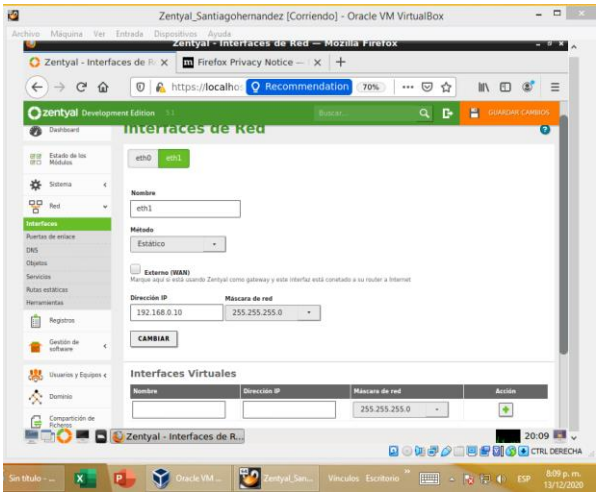

Fig. 9. interfaz de red

Se establecen los nuevos rango para el DHCP

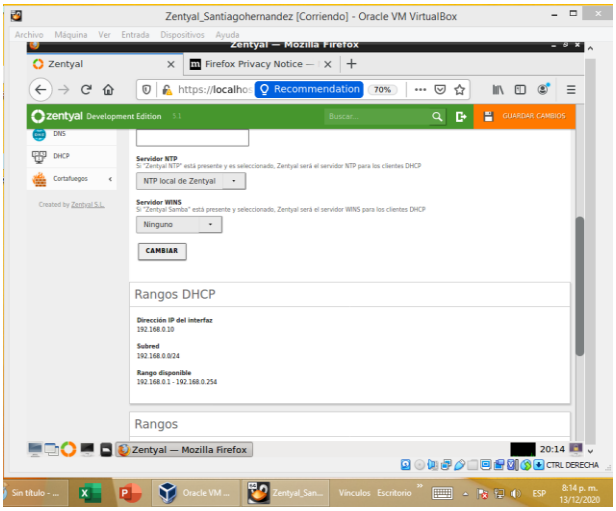

Fig. 10. Delimitación DHCP

Se verifica el direccionamiento de Zential

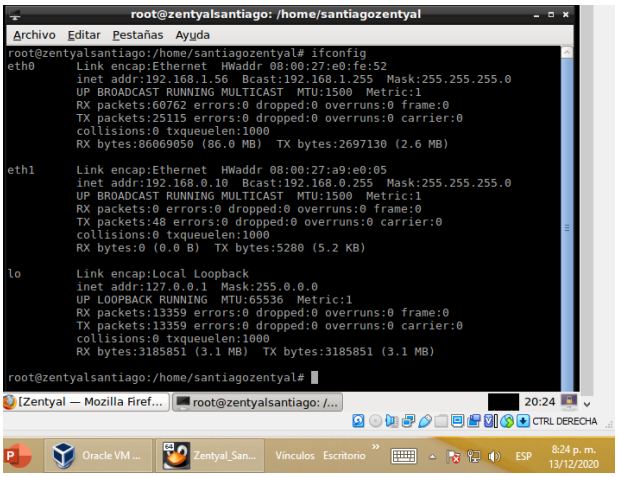

Fig. 11. Configuración ip zentyal

Desde una máquina de escritorio con el mismo entorno de red, se inspecciona su dirección ip y se verifica si ha sido asignada por DHCP desde el zentyal

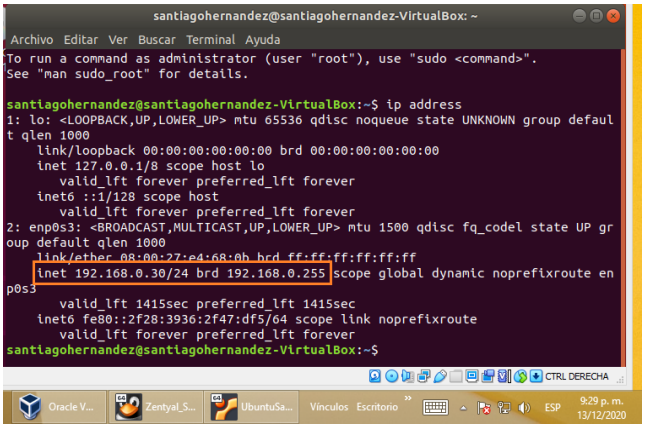

Fig. 12. Confirmación DHCP en maquina cliente

Accediendo al panel de zentyal, se puede verificar la asignación de la dirección IP por medio del DHCP

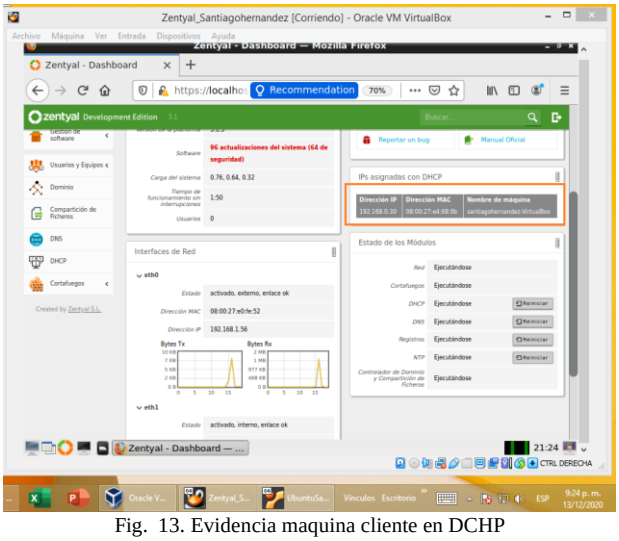

Fig. 13. Evidencia maquina cliente en DCHP

Se debe crear un dominio para la administración de equipos y aunque el equipo cliente ha tenido asignación de ip por DHCP aun no esta incluido en el directorio de usuarios y equipos

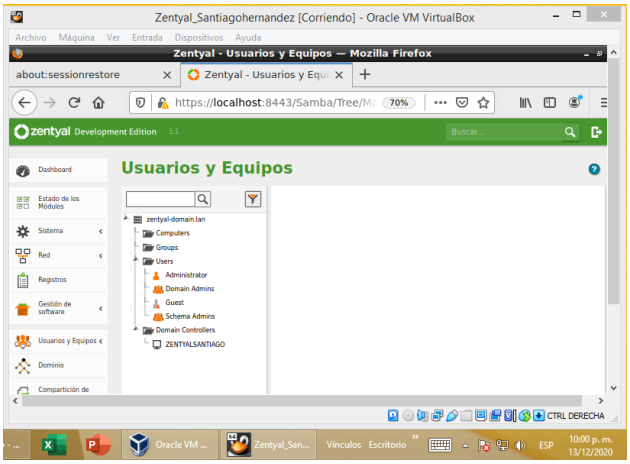

Fig. 14. Usuarios y equipos zentyal

En el escritorio de Ubuntu se procede a instalar el paquete Pbis Open, la cual es una herramienta que permite unir Linux a un Active Directory

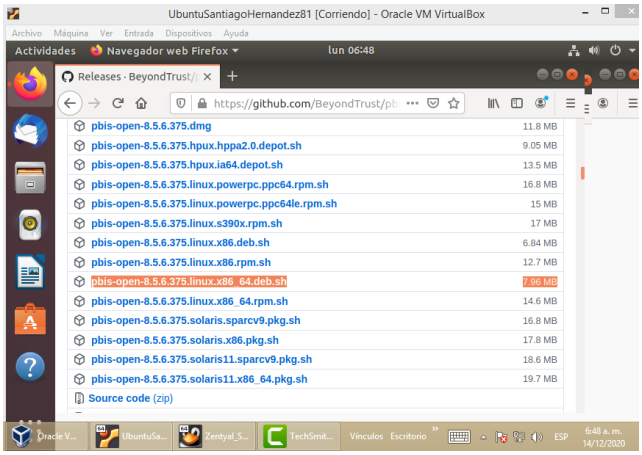

Fig. 15. Descarga paquete pbis-open

Una vez descargado el paquete se procede con la instalación en el equipo cliente.

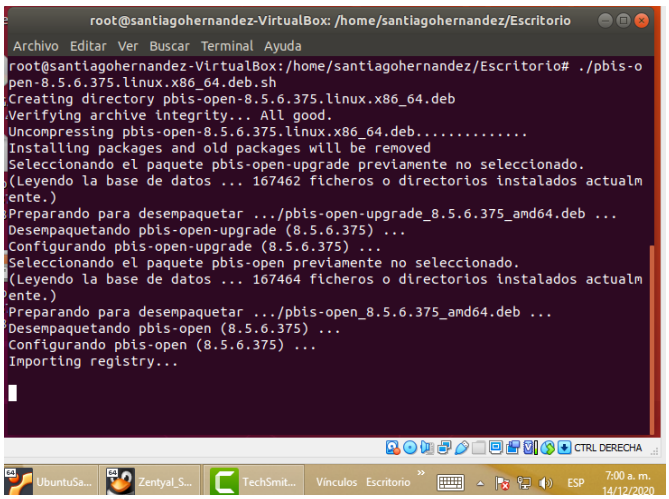

Fig. 16. Instalación paquete pbis en maquina cliente

Se evidencia la correcta instalación de los paquetes

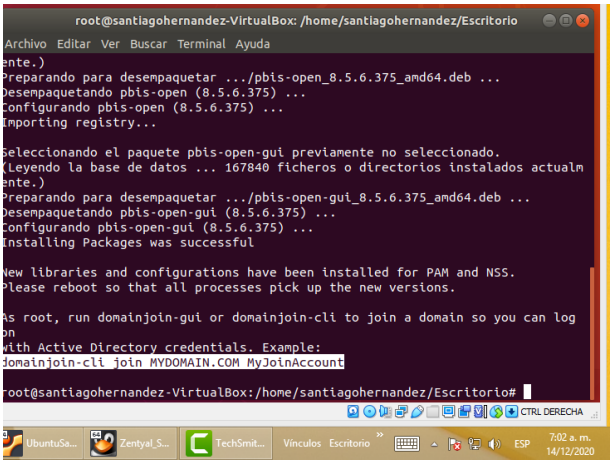

Fig. 17. Confirmación instalación pbis

Posteriormente se adiciona el equipo del cliente al servidor, teniendo cuidado de deshabilitar el ssh del servidor ya que podría presentar error en la conexión:

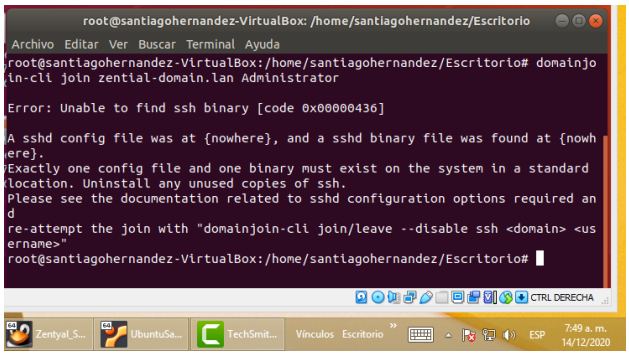

Fig. 18. Error por ssh de zentyal

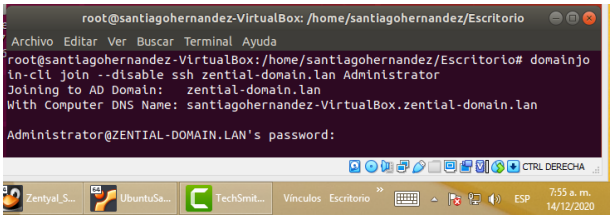

Fig. 19. Forma de unir un cliente a un dominio

Se puede apreciar que el equipo cliente ha sido adicionado de manera correcta al dominio

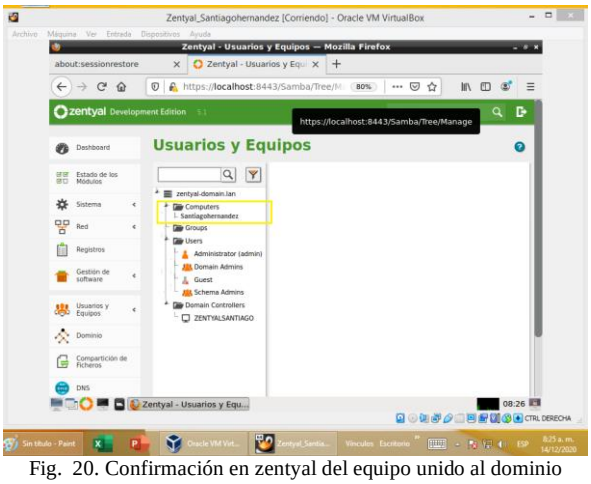

Fig. 20. Confirmación en zentyal del equipo unido al dominio

B. Temática 2: Proxy no transparente.

Producto esperado: *Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.*

El proxy implementado en Zentyal es el Squid, que junto con DansGuardian ofrecen un completo y eficiente control de contenidos, ya que este último paquete realiza un filtrado independiente, ubicándose entre el navegador de la máquina cliente y el proxy Bind.

Otra consideración a tener en cuenta es que el Proxy solicitado es un Proxy No Transparente, lo que obliga a que en cada máquina y en cada navegador se configure el proxy de manera explícita.

Esquemáticamente, la red estará construida de la siguiente manera:

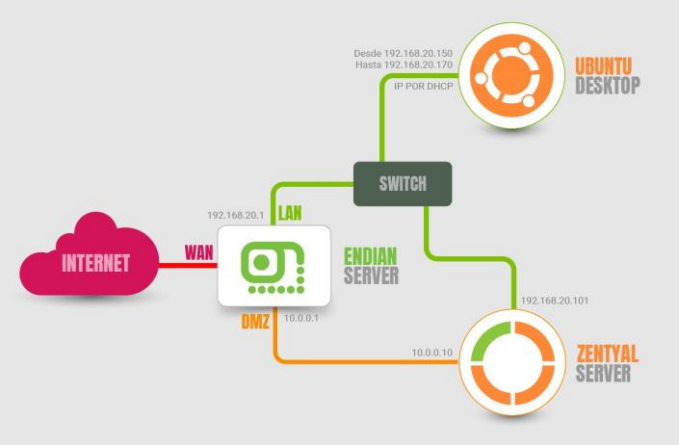

Fig. 21. Esquema de red implementada.

Inicialmente debemos confirmar que las dos interfases tengan la configuración correcta, para ello verificamos que en eth0 se encuentren los siguientes parámetros:

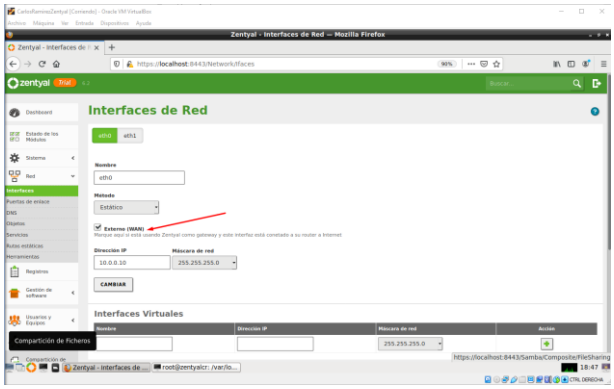

Fig. 22. Configuración de la interfaz eth0

Y para la interfaz eth1, se tiene lo siguiente:

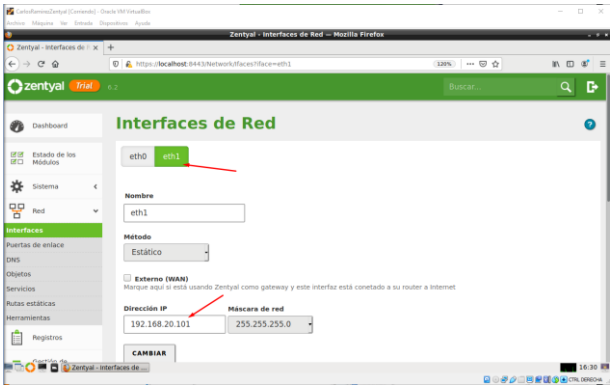

Fig. 23. Configuración de la interfaz eth1

Igualmente, en el servidor DHCP se debe configurar la puerta de enlace predeterminada para que el servidor Zentyal, tenga acceso a internet (zona roja del Endian Firewall).

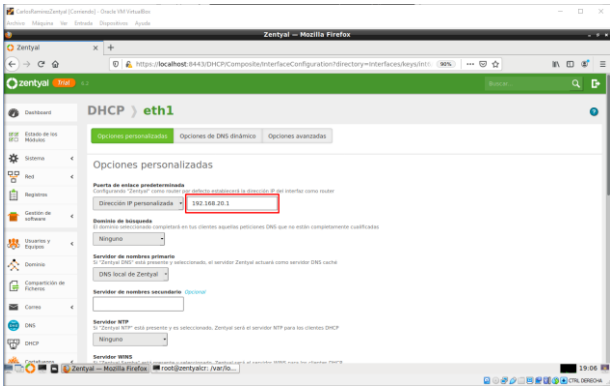

Fig. 24. Configuración de la puerta de enlace predeterminada.

Ahora procedemos a confirmar que el servicio de Proxy HTTP esté funcionando en la sección “Configuración del estado de los módulos”, en donde, también se deben estar habilitados los servicios de DNS, DHCP y Firewall.

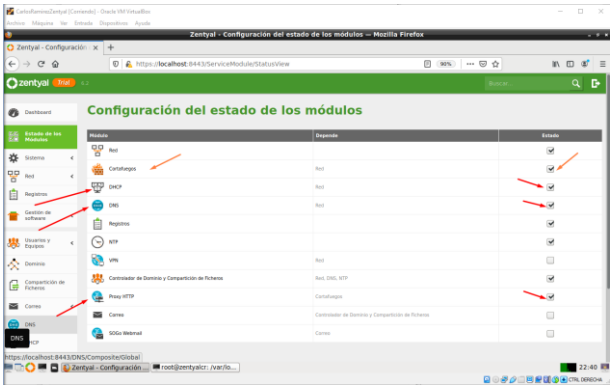

Fig. 25. Verificación del estado de los módulos necesarios.

Es necesario aclarar que el cortafuegos se activará en cuanto activemos el servicio ProxyHTTP.

Ahora se debe seleccionar en el menú lateral del Zentyal, servicio Proxy HTTP y configurar el puerto en el cual se require que funcione el servicio, el cual debe funcionar en el puerto 1230, tal como se muestra en seguida:

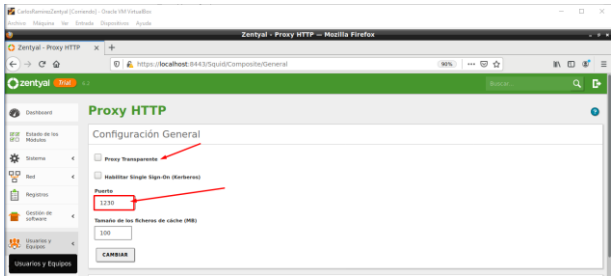

Fig. 26. Configuración del proxy, en puerto y en modo NO transparente.

Una vez guardada la configuración realizada, se procede con la creación de los objetos de red, para lo cual es necesario dirigirse hacia el menú principal, en donde se ubicará el ítem "Red" y se selecciona "Objetos" y se creará el objeto denominado Tematica2UNAD y que contendrá los miembros denominados MiembroRedLAN1 y un rango de dirección IP que, en el caso presentado, concuerda con las IPs asignadas por el servidor DHCP en la red LAN (Zona verde del Endian Firewall).

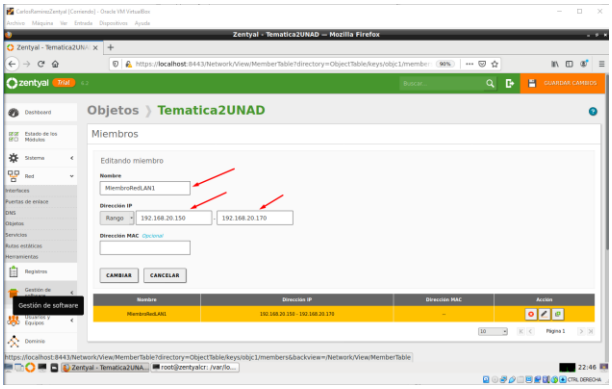

Fig. 27. Creación del objeto de red.

Una vez configurado el objeto de red, se procede con la creación del perfil de filtrado. Para esto es necesario dirigirse al menú Proxy HTTP, y se selecciona en el submenú, el ítem "Perfiles de filtrado". En el listado se debe crear el perfil "Estudiantes" con la siguiente configuración:

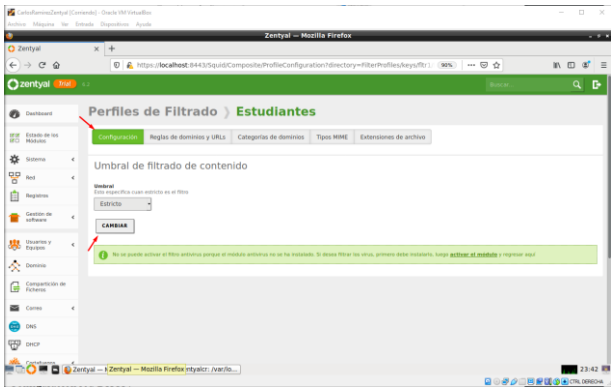

Fig. 28. Configuración del perfil de filtrado.

Y en la pestaña Reglas y Dominios y URLs, se chequea el control para Bloquear tráfico HTTPS por dominio, lo que permitirá que se cree un listado de páginas de internet para ser rechazadas. Este listado se muestra en la sección inferior, para el caso mostrado a continuación, se tiene el bloqueo de dos URLs, la primera es Google.es y la segunda es Facebook.com:

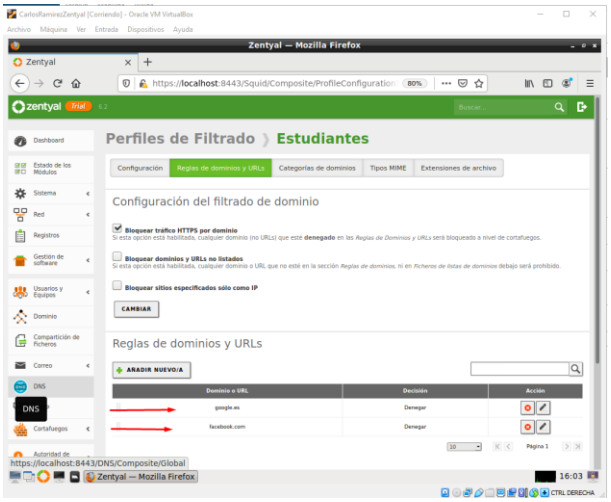

Fig. 29. Creación y configuración de las reglas de dominios.

Una vez creado el perfil de filtrado, se procede con la creación de la correspondiente regla de acceso. Para ello, se dirige al menú principal de la herramienta de administración web de Zentyal y se selecciona el item Proxy HTTP y se presiona en el botón Añadir nuevo, y se deberá desplegar el siguiente formulario, en donde es posible seleccionar el horario y los días en los que se desea el servicio de proxy aplique la regla. De igual forma, se debe elegir en el campos origen, el Objeto de red que creamos anteriormente (Temática2UNAD), y finalmente en los campos "Decisión", se selecciona "Aplicar perfil de filtrado", y se le busca el perfil "Estudiantes", que se había creado antes.

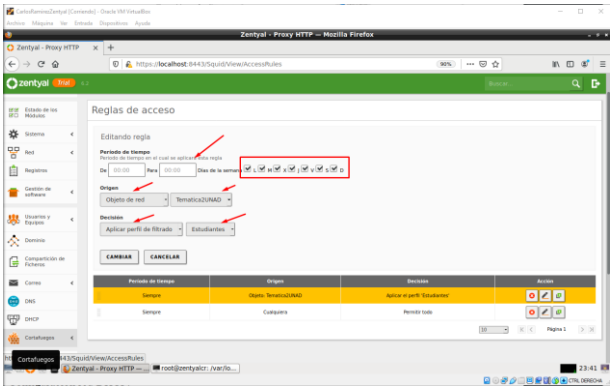

Fig. 30. Configuración de las reglas de acceso.

Hay que destacar que si no se diligencian los campos "De" y "Para" en el formulario de creación o edición de la regla de acceso, ésta se aplicará "Todo el tiempo".

Tras la creación, el listado de reglas de acceso se mostrará como se muestra a continuación:

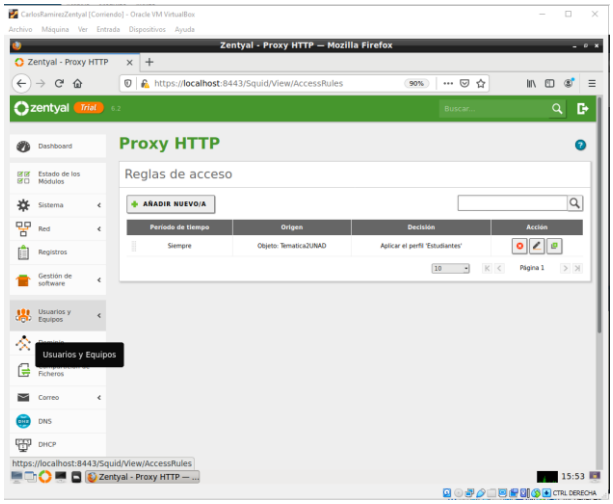

Fig. 31. Listado de reglas de acceso creadas.

Ahora se debe ingresar a la máquina Ubuntu Desktop en la red LAN y se procede con la configuración del proxy en el navegador, para lo cual se debe ingresar en el menú preferencias del Mozilla Firefox y en el campo de búsquedas se escribe proxy. Como resultado nos mostrará la información como sigue:

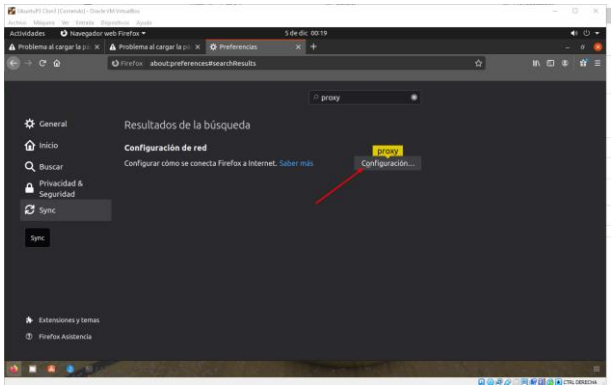

Fig. 32. Búsqueda de configuración de red, en máquina ubuntu Desktop.

Tras presionar en configuración, es posible realizar la configuración del Proxy, con la IP que corresponde a la interfaz que se conecta con la red LAN, en el caso expuesto es la 192.168.20.101.

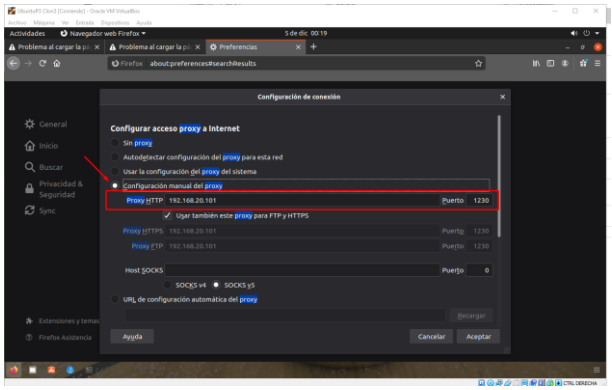

Fig. 33. Formulario de configuración del proxy en máquina Ubuntu Desktop.

Al presionar en el botón Aceptar, ya es posible confirmar que esté bloqueando las URLs creadas. Inicialmente se observa que en la siguiente imagen de evidencia, el Ubuntu Desktop, cuenta con acceso portales web como youtube, pero tal como se esperaba, la conexión a facebook, ha sido rechazada por el proxy. De igual manera se observa que los dominios locales se está resolviendo correctamente locales.

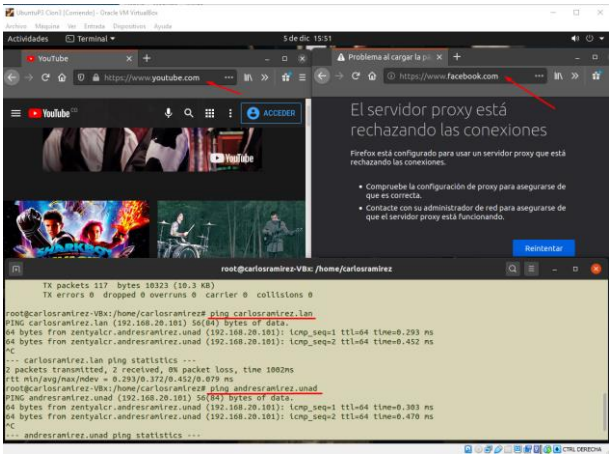

Fig. 34. Evidencia de funcionamiento del proxy configurado.

En el caso de la otra URL que se bloqueó (google.es), la respuesta obtenida es la siguiente:

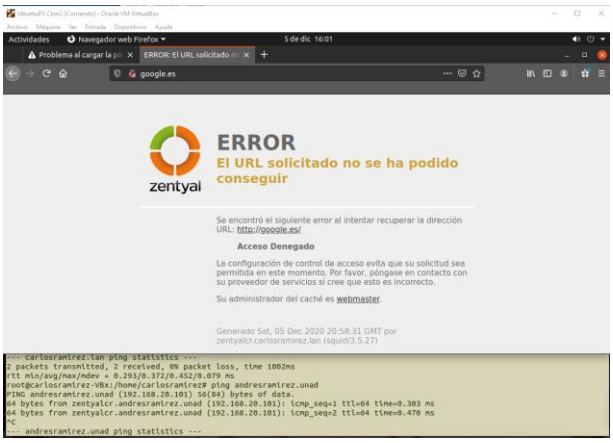

Fig. 35. Evidencia de acceso denegado al segundo dominio restringido.

C. *Temática 3: Cortafuegos.*

Producto esperado: *Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.*

Zentyal utiliza para su módulo de cortafuegos el subsistema del kernel de Linux llamado Netfilter, que proporciona funcionalidades de filtrado, marcado de tráfico y redirección de conexiones.

El esquema de red y máquinas virtuales que se utiliza para la implementación del cortafuego es la siguiente.

Un servidor Endian el cual se encarga de manejar las diferentes zonas, para la verde (LAN) se configura la IP 192.168.20.1, para la zona naranja (DMZ) 10.0.0.1 y la zona roja por DHCP (WAN).

Un servidor Zentyal el cual tiene configurado dos interfaces de red una la eth0 con IP 10.0.0.10 dentro de la zona DMZ y la eth1 con IP 192.168.20.101 dentro de la zona verde.

Una maquina Ubuntu desktop con dirección IP 192.168.20.3 con puerta de enlace a la IP 192.168.20.101 del servidor Zentyal.

De acuerdo a la temática selecciona debemos instalar el paquete de Firewall automáticamente se instalara la configuración de la red.

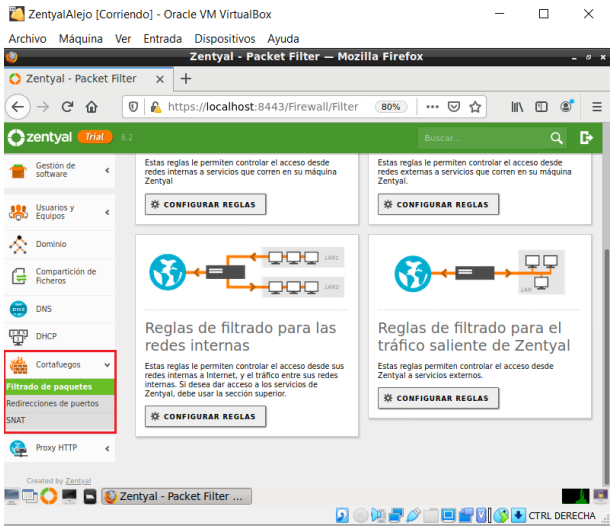

Fig. 36. Paquete Firewall Zentyal.

Ahora procedemos a realizar la configuración de las interfaces de red del servidor Zentyal. Primero configuramos la interfaz eth0 con los siguientes parámetros:

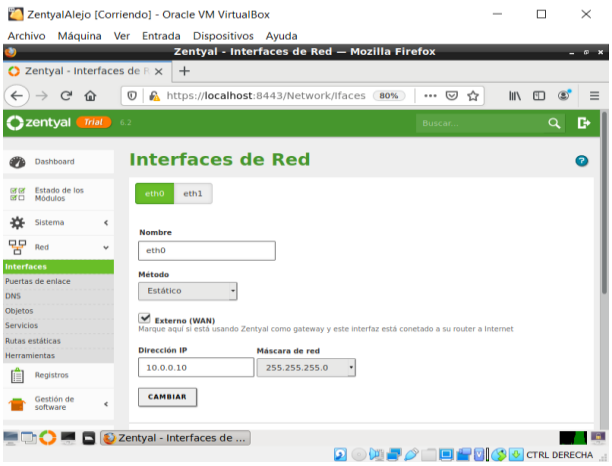

Fig. 37. Configuración de la interfaz eth0.

Ahora se indica la configuración para la interfaz de red eth1.

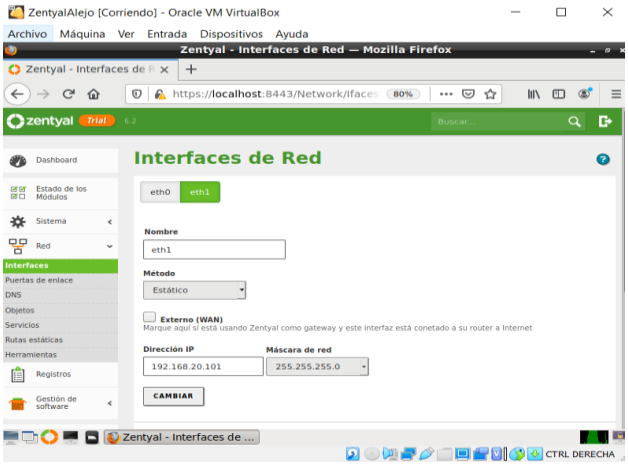

Fig. 38. Configuración de la interfaz eth1.

Nos dirigimos a la maquina Ubuntu desktop e identificamos la IP que tiene asignada.

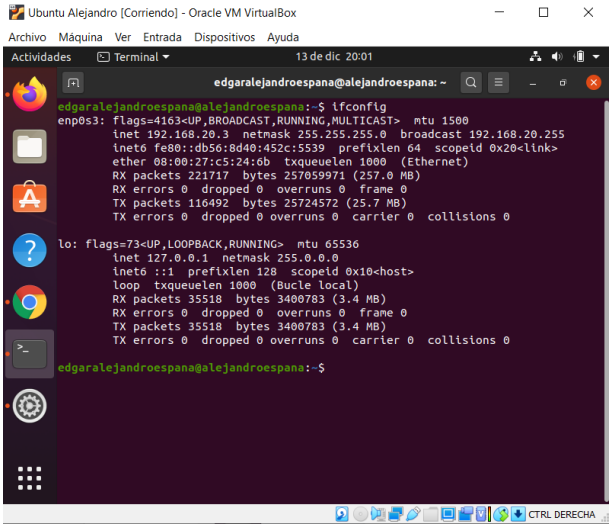

Fig. 39. Direccionamiento IP Ubuntu Desktop.

Ahora ingresamos al navegador y verificamos que podamos navegar en internet específicamente a una red social.

Fig. 40. Navegación red social Ubuntu Desktop.

Nos dirigimos al servidor Zentyal y procedemos a configurar el cortafuego, primero creamos un objeto de red el cual especifique el rango de direcciones IP al cual se desea asignar las reglas.

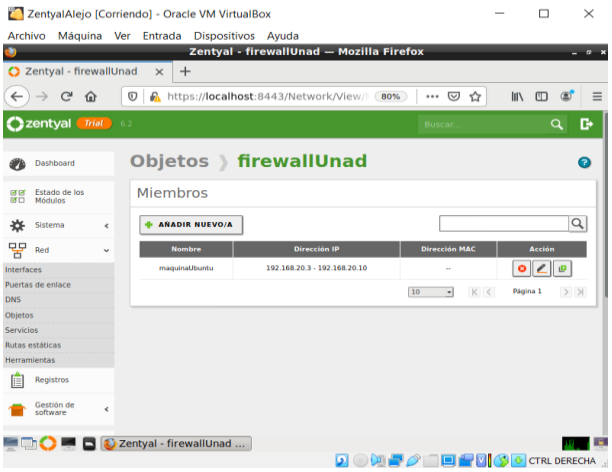

Fig. 41. Configuración objeto de red.

Ahora vamos directamente a la opción de Firewall y se selecciona la opción que dice filtrado de paquetes, e ingresamos a la opción de filtrado para redes internas y procedemos a configurar.

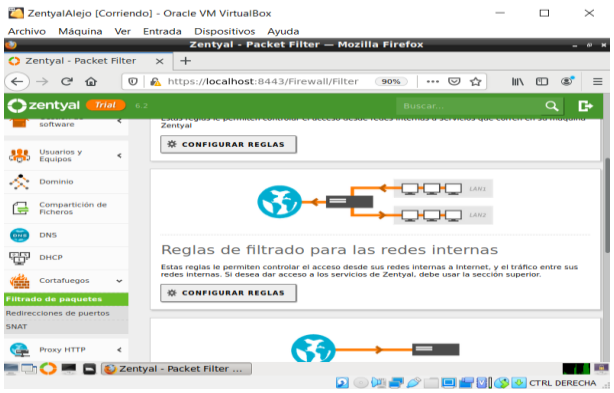

Fig. 42. Configuración reglas internas.

Ahora dentro de la configuración del cortafuego añadimos las reglas de filtrado para redes internas, en la cual se deniega por IP el acceso a las redes sociales que se deseen.

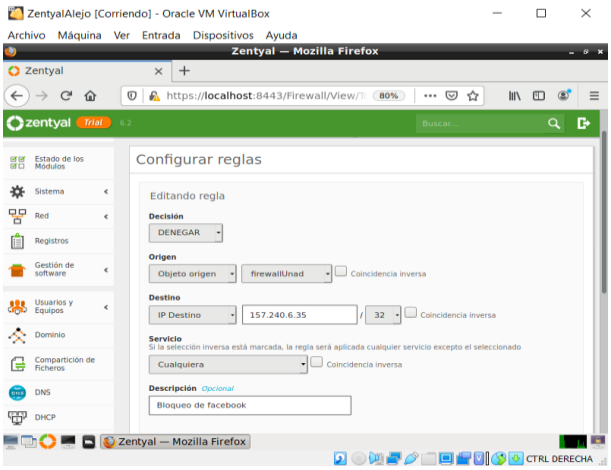

Fig. 43. Configuración regla cortafuegos.

Una vez añadidas todas las reglas, se consulta desde el navegador de la máquina Ubuntu desktop para corroborar que se estén aplicando las reglas correctamente.

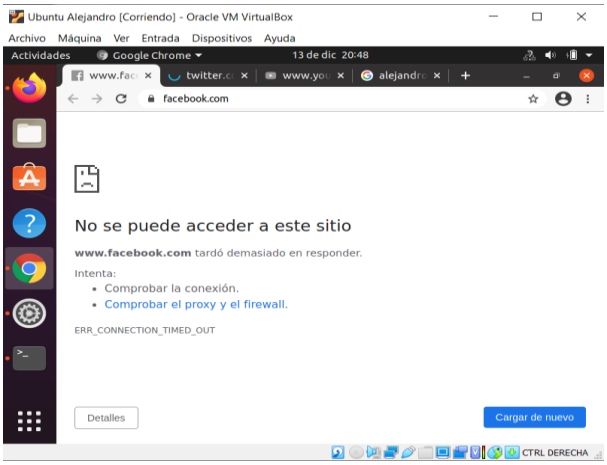

Fig. 44. Navegación red social Ubuntu Desktop.

Verificamos ingresando a una dirección que no esté bloqueada, para validar el correcto funcionamiento del cortafuego.

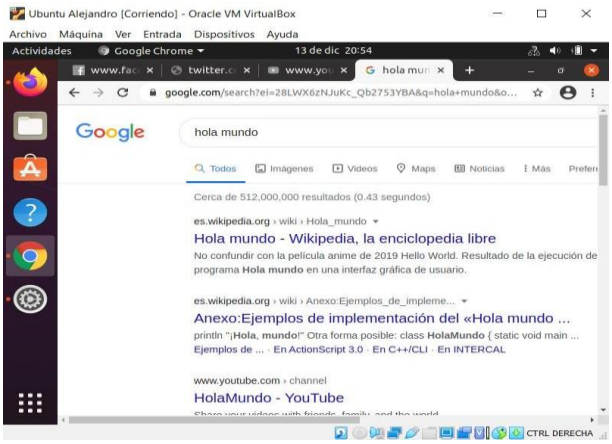

Fig. 45. Navegación Ubuntu Desktop

C. Temática 4: File Server y Print Server

Producto esperado: *Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras*

Zentyal integra **OpenLDAP** como servicio de directorio, con tecnología *Samba* para implementar la funcionalidad de controlador de dominios además de para la compartición de ficheros e impresoras.

La **compartición de ficheros** es el proceso por el cual una serie de ficheros se ponen a disposición de los usuarios de una red, dándoles acceso para trabajar sobre ellos, descargarlos o modificarlos. En Zentyal usaremos el protocolo SMB/CIFS. para mantener la compatibilidad con los clientes Microsoft. SMB/CIFS está también soportado en la gran mayoría de Sistemas Operativos, incluidos móviles y diferentes dispositivos de red.

Una vez configurado zentyal procedemos a ingresar a la consola de administracion por el puerto 8443, en la configuración inicial seleccionamos los modulos de Domain Controller And File Sharing, DNS Server y DHCP Server.

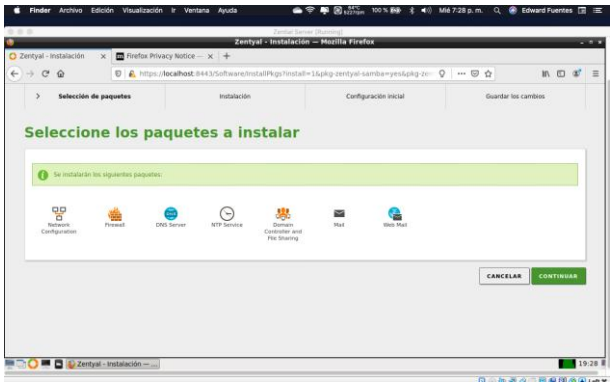

Fig. 46: Selección de modulos en configuracion inicial.

Luego se procede a configurar los dispositivos de red. Este paso es muy importante para la posterior configuración del LDAP. Recordemos que se requiere uno externo y otro interno, asi mismo debemos configurar la ip estatica de la maquina.

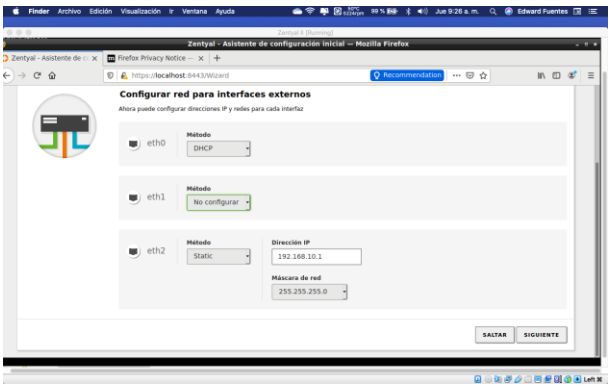

Fig 47. Configuracion de interfaz de red e ip estatica

Una vez configurada la interfaz de red es necesario configurar el tipo de servidor y configurar como un servidor standalone

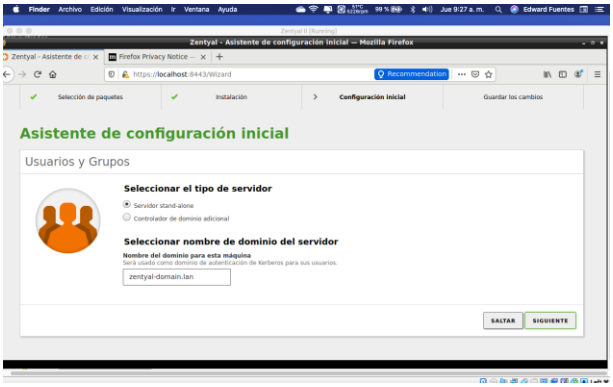

Fig 48. Configuración tipo de servidor

Luego debemos configurar el dominio que usara el servidor, este paso es importante para tener estandarizado al momento de crear los usuarios y grupos.

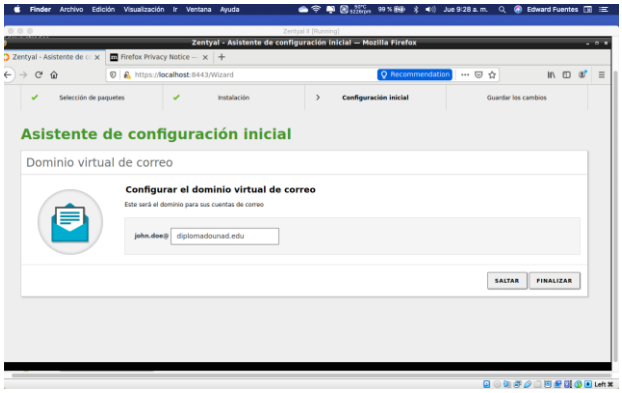

Fig 49. Configuracion de dominio.

Para probar la configuracion desde el cliente debemos instalar y configurar y activar el modulo DHCP.

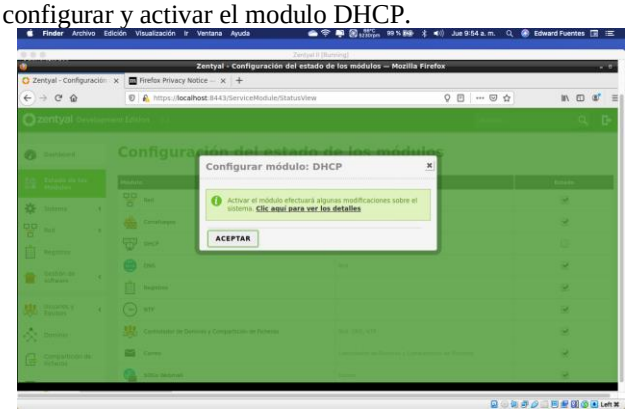

Fig 50. Configuracion de modulo DHCP

Luego debemos configurar los rangos del DHCP para que acepte y asigne la ip a la maquina con la que vamos a probar (esta maquina debe tener una ip configurada dentro del rango que estamos definiendo aquí).

Fig. 51. Configuracion de rangos en e servidor.

Luego se debe probar desde la otra maquina si tiene conexión

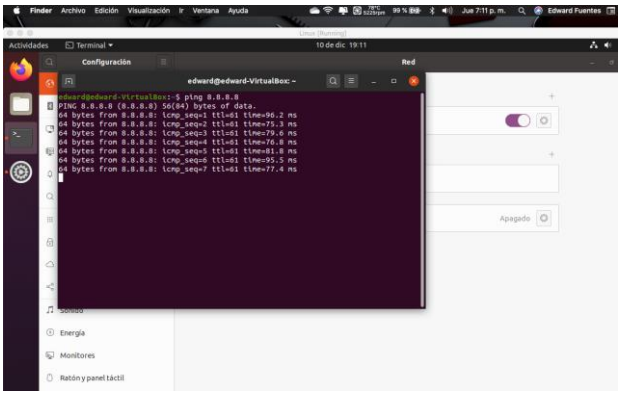

Fig 52. Salida a internet de la maquina

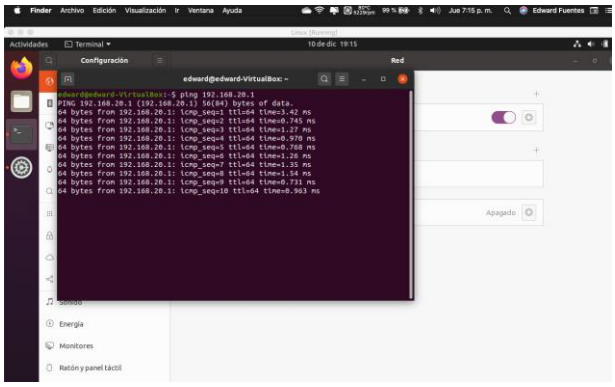

Fig 53. Conexión de la maquina con el servidor Zentyal

Luego debemos configurar el dominio en nuestro servidor zentyal. Para esto accedemos al modulo de dominio y verificamos que el dominio que esta desplegado sea el deseado, en este caso el nombre de dominio que se usa es diplomadounad. Tambien se debe verificar que el servidor tenga la configuracion controlador de dominio.

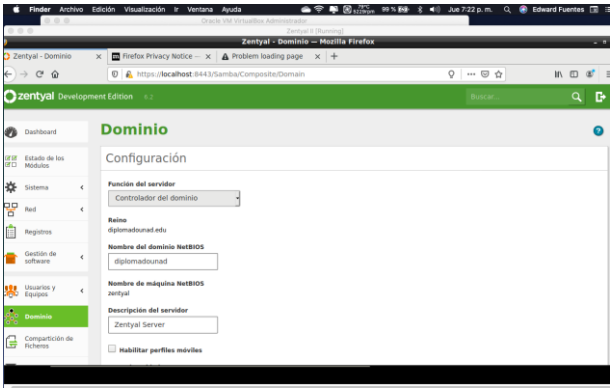

Fig 54. Configuración de dominio.

Luego de configurar el dominio es necesario configurar los usuarios, puesto que los archivos se asociarán a grupos o usuarios para definir el control de acceso.

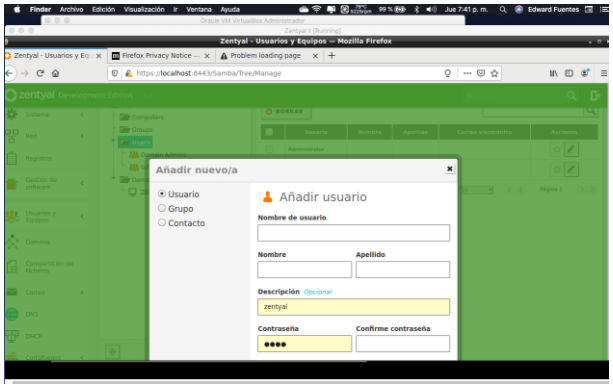

Fig 55. Configuración Creacion de nuevo usuario

Configurado el servidor y con acceso desde la maquina ubuntu, procedemos a instalar y configurar el cliente LDAP, LA configuracion de este cliente se puede realizar desde windows, o mac atravez de sus herramientas propias. Para el cliente de linux se instalan los paquetes con el comando **$ sudo apt-get -y install libnss-ldap libpam-ldap ldap-utils nscd**

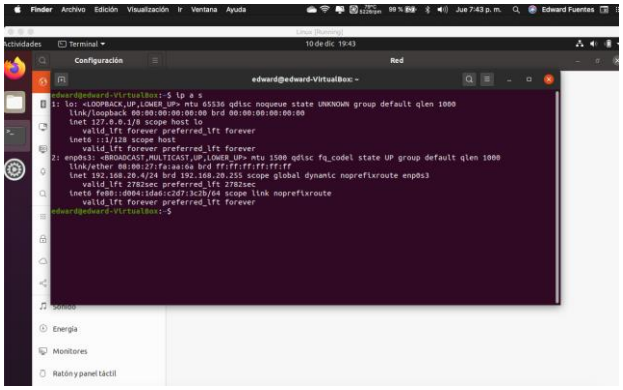

Fig 56. instalacion cliente LDAP

Configuracion del cliente LDAP en linux, se configuran las opciones que nos pide el asistente de instalación.

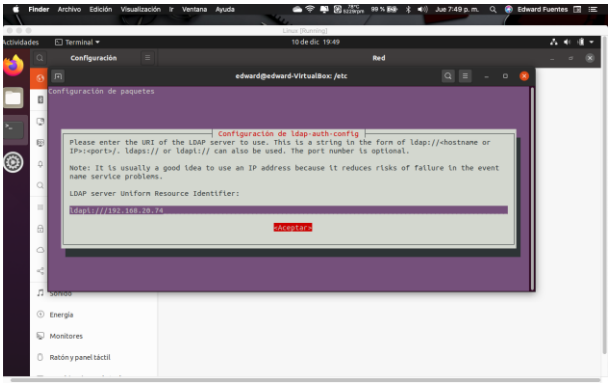

Fig 57. configuracion cliente ldap

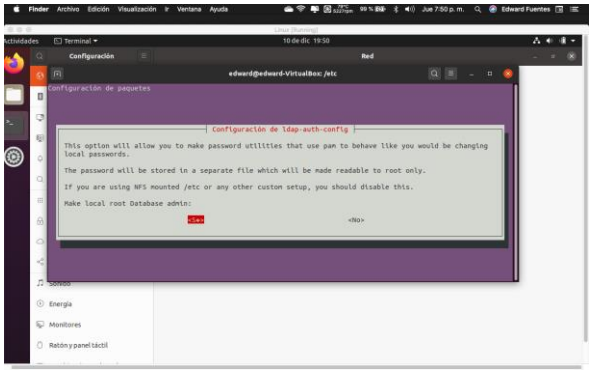

Fig 58. configuracion cliente ldap 2

Se modificará el archivo nsswitch.conf para trabajar con LDAP a través del comando sudo nano /etc/nsswitch.conf Archivo antes de cambios.

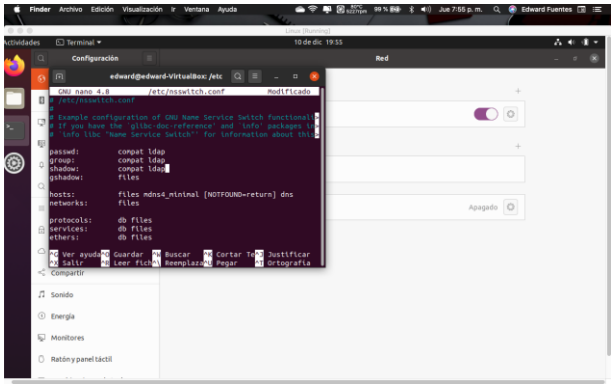

Fig 59. Configuracion de archivo nsswitch.conf

Una vez configurado el cliente, se debe proceder a configurar la compartición de ficheros en zentyal . Para eso debemos crear los ficheros que queremos compartir y asi mismo dar los accesos necesarios para la gestion de ficheros compartidos.

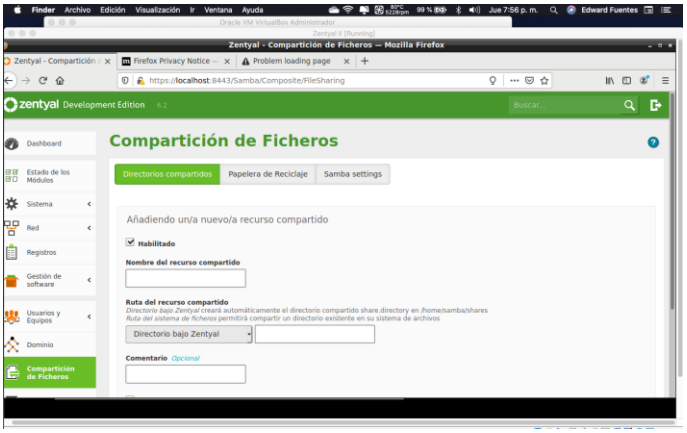

Fig 60. Creacion de un fichero compartido en zentyal

Luego de creado el fichero compartido es necesario configurar los permisos o accesos al mismo . para esto se accede a l modolo de directorios compartidos y desde la carpeta compartida que creamos le configuramos el control de accesos

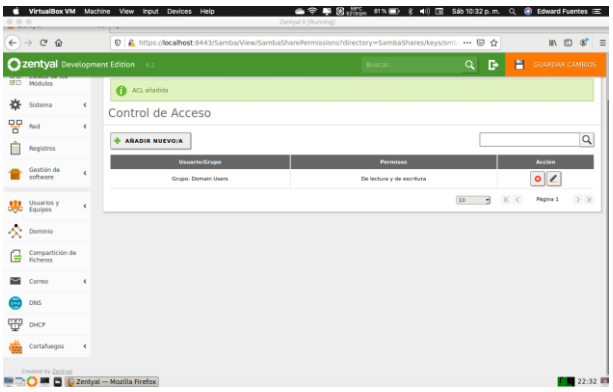

Fig 61 Configuracion de control de accesos a ficheros compartidos zentyal

D. Temática 5: VPN

Producto esperado: *Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.*

La facilidad de configurar y gestionar las redes privadas virtuales en Zentyal, se debe a su integración con OpenVPN, por lo tanto, en el siguiente informe se dará a conocer las configuraciones requeridas para la creación de una VPN, por lo tanto, para la implementación utilizaremos dos máquinas virtuales con las siguientes características:

Máquina	GNU/Linux	Interfaces	Tipo	Método	Dirección IP
1	Ubuntu Server	eth0	LAN	Static	192.168.20.2/24
		eth1	Puente	DHCP	--
2	Zentyal	eth0	NAT	static	192.168.21.2/24
		eth1	Puente	DHCP	192.168.1.17/24

Tabla 1. Características de las máquinas

Para la creación de la VPN vamos a necesitar tres certificados: autorización, cliente y VPN. Comenzaremos por el certificado de autorización, el cual, se crea desde Autorización → General.

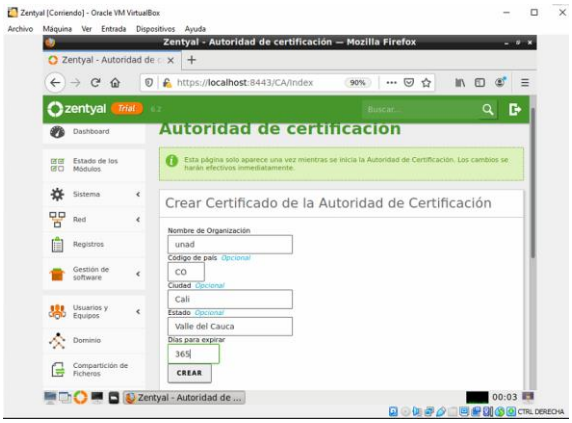

Fig. 62. Certificado de autorización.

Ahora debemos de crear el servidor VPN, para lo cual, en el menú principal seleccionamos las opciones VPN → Servidores, donde se le asigna un nombre. Al guardar los cambios realizados veremos lo siguiente:

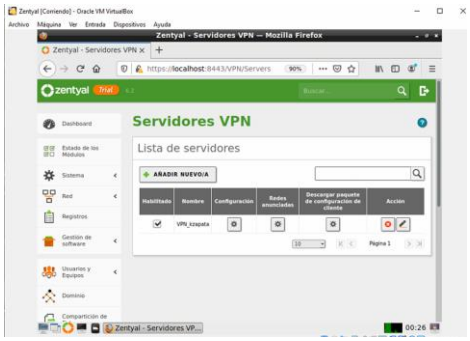

Fig. 63. Servidor VPN

Que dentro de su configuración esta la siguiente información:

- Puerto de servidor: UDP puerto 1194
- Dirección VPN: 192.168.160.0 /24
- Certificado del Servidor.
- Interfaz TUN: activa

Cuando el servidor de VPN se crea, el sistema genera de manera automática el certificado para este:

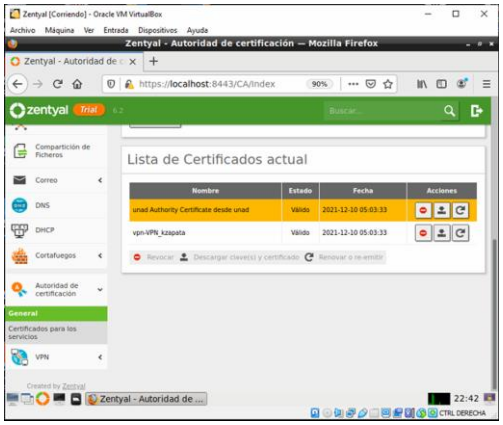

Fig. 64. Certificado de Autorización y servidor VPN

El certificado cliente se genera desde Autorización → General, se debe tener presente que el sistema no permitirá generar este certificado si hasta el momento no se tiene el certificado de autorización.

Posterior a esto, debemos de crear el servicio en la red, desde el módulo Red → Servicios, para esto, solo requiere de un nombre, la configuración de este debe ser igual al servidor VPN en protocolo y puerto destino (1194).

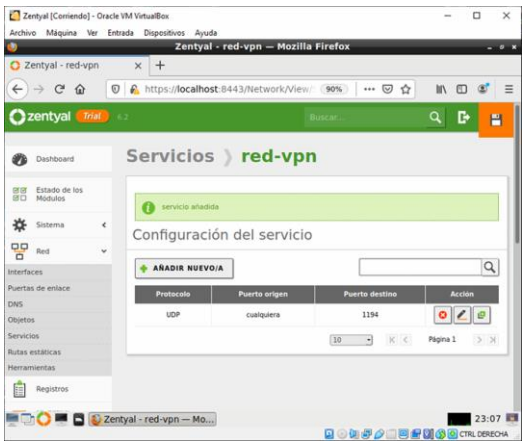

Fig. 65. Servicio de red VPN

Debemos de crear las reglas de excepción para el acceso al servicio, para esto, en el menú principal seleccionamos la opción Filtrado de paquetes.

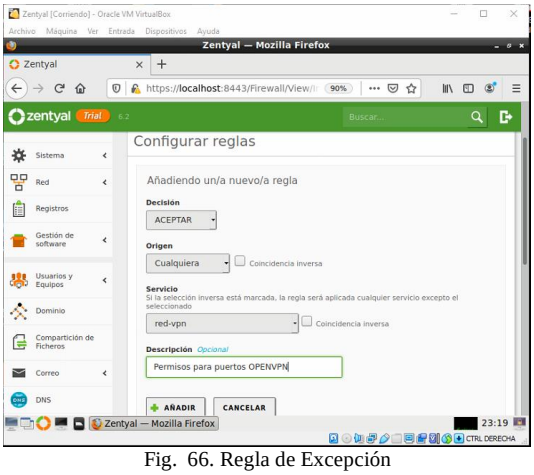

Fig. 66. Regla de Excepción

Ahora debemos de parametrizar las direcciones IP de acceso al servidor VPN que se ingresaran en la descarga del paquete de configuración del cliente, para lo cual, vamos a necesitar conocer la dirección IP de la red WAN, podemos apoyarnos de páginas que nos dan esta información, en nuestro caso es 200.116.63.239; también necesitamos conocer la IP que esta asignando el sistema DHCP para esto podemos ejecutar el comando ifconfig en la terminal y tomamos la IP del adaptador uno, correspondiente a NAT.

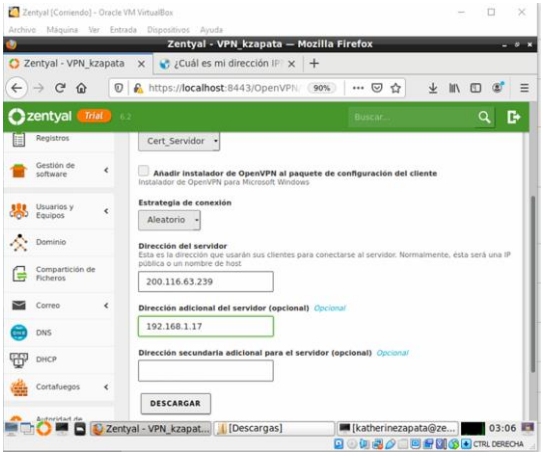

Fig. 67. descarga del paquete de configuración del cliente

El archivo comprimido que nos genera el sistema deberemos trasladarlo al puesto de trabajo Ubuntu Server 18.04.5 pero primero la máquina Ubuntu Server deberá tener instalado Openvpn, debido a que lo necesitamos para la configuración de la VPN en nuestra máquina cliente, entonces en la terminal ejecutamos el siguiente comando “apt-get install openvpn”.

Procedemos a descomprimir el archivo, para nuestro ejercicio quedo ubicado en la carpeta de descargar, por lo tanto, nos trasladamos a esta y usamos el comando: “tar -xvf VPN_kzapata-client-Cert_Servidor.tar.gz”.

Una vez descomprimido ejecutando la configuración de nuestra VPN usando el archivo .conf por medio del siguiente comando “openvpn --config VPN_kzapata-client.conf”.

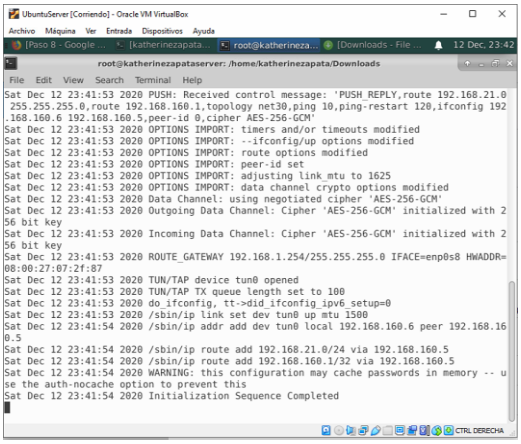

Fig. 68. Configuración de la VPN en Ubuntu Server

Cuando termine podemos verificar la conexión de nuestra máquina cliente con el certificado remoto, para esto, vamos a nuestra máquina Zentyal y en el menú principal seleccionamos la opción: Registros.

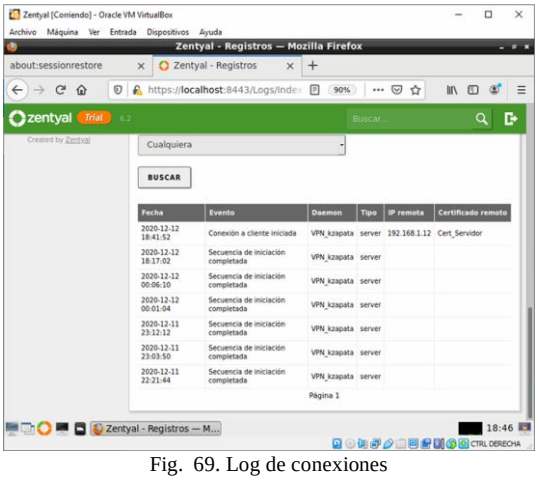

Fig. 69. Log de conexiones

También podemos ingresar a la máquina Zentyal con la IP de la VPN 192.168.160.1

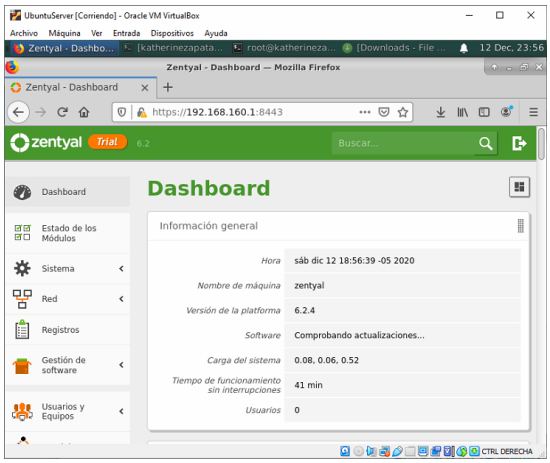

Fig. 70. Conexión VPN desde Ubuntu Server

Conclusiones

El uso de dos servidores, uno para la demarcación de las zonas (Endian) y otro (Zentyal), que estando en la zona desmilitarizada, realiza el ofrecimiento de todos servicios, es una configuración de red con la cual se puede ofrecer mayor seguridad de la información y que, mediante el Proxy HTTP, provee una administración más ágil y flexible de las restricciones de navegación para los clientes en la red interna, otorgando control sobre los dominios, URLs, categorías, archivos y extensiones permitidas.

A través de la configuración del servidor Zentyal dentro de la zona DMZ y la correcta aplicación de las reglas del cortafuegos podemos conservar de una manera íntegra la seguridad de nuestra red interna y denegar el acceso a páginas que no estén permitidas dentro de la organización.

La máquina Zentyal al integrarse con OpenVPN permite configurar y gestionar redes privativas virtuales, facilitando la conexión de equipos de una red externa con equipos de una red interna por medio de un túnel privado de comunicación, como quedó demostrado es este trabajo donde la VPN creada se podía comunicar con una estación de trabajo GNU/Linux Ubuntu Server 18.04.5.

Referencias

[1] Servicio de resolución de nombres de dominio (DNS). (2018). Recuperado de https://doc.zentyal.org/es/dns.html#configuracion-de-un-servidor-dns-autoritario-con-zentyal

[2] Servicio de configuración de red (DHCP). (2018). Recuperado de https://doc.zentyal.org/es/dhcp.html

[3] Configuración general del Proxy HTTP con Zentyal. (2018). Recuperado de https://doc.zentyal.org/es/proxy.html

[4] Instalación. (2018). Recuperado de https://doc.zentyal.org/es/installation.html#requisitos-de-hardware

[5] Servicio de redes privadas virtuales (VPN) con OpenVPN. (2018). Documentación de Zentyal 6.2. Recuperado de https://doc.zentyal.org/es/vpn.html