IMPLEMENTACIÓN DE SERVICIOS DE INFRAESTRUCTURA IT BASADA EN ZENTYAL 6.2

Catherin Johanna Sanchez Ceròn
e-mail: cjsanchezc@unadvirtual.edu.co
Juan Carlos García Mazuera
e-mail: jcgarciamaz@unadvirtual.edu.co
Diego Fernando Riascos Ortega
e-mail: dfriascoso@unadviertual.edu.co
Gustavo Adolfo Preciado
e-mail: gapreci@unadviertual.edu.co
Vladimir Castillo Pérez
e-mail: vcastillope@unadvirtual.edu.co

***RESUMEN**: En este trabajo se implementa un servidor con el sistema operativo Zentyal en versión 6.2 el cual trabaja de manera centralizada la administración de los servicios, con un panel de control para configurarlos de manera correcta. Este trabajo está orientado a la administración y control de una distribución GNU/Linux basada en Ubuntu, enfocada a la implementación de servicios de infraestructura IT de mayor nivel para intranet y extranet en instituciones complejas. La distribución que se trabaja es GNU/Linux Zentyal Server 6.2 la cual es instalada y configurada como sistema operativo base para disponer de los servicios y plataformas de infraestructura IT. Los servicios y plataformas explicados en este trabajo son DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN*.

PALABRAS CLAVE: servicios de IT, Zentyal, servidores, seguridad informática.

***ABSTRACT**: This work implements a server with the Zentyal operating system in version 5.0.1 which works centrally in the administration of the services, with a control panel to configure them correctly. This work is aimed at the administration and control of a GNU / Linux distribution based on Ubuntu, focused on the implementation of higher level IT infrastructure services for intranet and extranet in complex institutions. The distribution that works is GNU / Linux Zentyal Server 6.2 which is installed and configured as a base operating system to provide IT infrastructure services and platforms. The services and platforms explained in this work are DHCP Server, DNS Server, Domain Controller, Non-transparent Proxy, Firewall, File Server, Print Server and VPN*.

KEYWORDS: IT Services, Zentyal, Servers, Informatic Security

1 INTRODUCCIÓN

Zentyal Server es un sistema operativo basado en Ubuntu GNU/Linux, el permite a través del acceso en un navegador web, la administración de diferentes servicios y funcionalidades que lo han puesto como la mejor alternativa a Windows Server. Es justamente el objetivo de este trabajo, el hacer una revisión y aplicación de 5 diferentes servicios que presta Zentyal para una maquina con sistema operativo Ubuntu Desktop.

2 INSTALACIÓN DE ZENTYAL 6.2

Si bien en la actualidad el sistema operativo Zentyal se encuentra en la versión 7.0, para esta actividad se ha utilizado la versión 6.2.

Zentyal está concebido para ser instalado de forma exclusiva en una máquina, ya sea virtual o física, pero esto no impide que se puedan instalar más herramientas o servicios conjuntamente. Se debe tener en cuenta que estos últimos no serán administrados desde Zentyal

2.1 REQUISITOS

Los requerimientos de hardware para instalar Zentyal dependen de los módulos que se vayan a instalar, la cantidad estimada de usuarios que usarán el sistema y los hábitos de uso.

Si el uso de Zentyal es como puerta de enlace o cortafuegos, es necesario tener al menos dos tarjetas de red. Si solo se va a usar como servidor, una sola tarjeta de red es suficiente.

Para un Zentyal de uso general, con una cantidad de usuarios inferior a 50, los requerimientos mínimos recomendados serían: memoria de 2 Gb, espacio en disco de 80 Gb, procesador con 2 cores y las tarjetas de red de acuerdo con los servicios a implementar.

2.2 INSTALADOR

Se puede obtener una imagen iso desde el sitio web https://zentyal.com/community/ en donde se encuentran desde la versión 2.2 hasta la versión 7.0. La imagen se puede descomprimir para hacer un CD o USB booteable.

2.3 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Como procedimiento previo para la máquina virtual que contiene al sistema operativo Zentyal, se debe seleccionar un fichero en donde quede contenida la

imagen del disco virtual, al menos 2 Gb de RAM, usar el formato VDI como tipo de archivo, el almacenamiento reservado dinámicamente y un tamaño de 20 Gb de almacenamiento.

Luego de crear la máquina virtual, se deben aplicar configuraciones adicionales. Estas incluyen: agregar la imagen de instalación del sistema operativo en la unidad óptica, habilitar dos adaptadores de red, el primero adaptador como puente y el segundo como solo anfitrión; y por último crear una red de anfitrión en donde se configure el direccionamiento IP y se deshabilite el direccionamiento por DHCP.

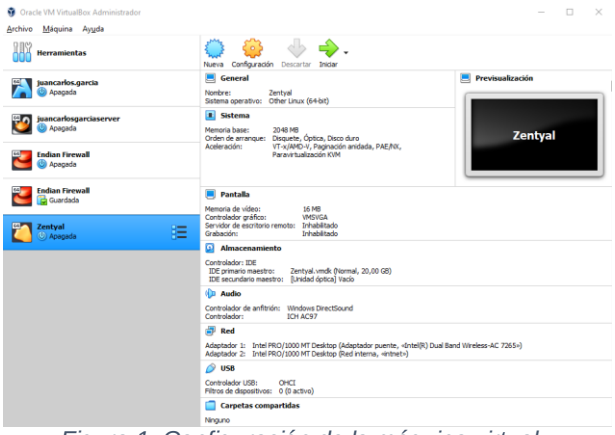

Figura 1. Configuración de la máquina virtual

Figura 2. Administrador de red de anfitrión

2.4 PROCESO DE INSTALACIÓN

Finalizada la configuración de la máquina virtual, se inicia el proceso de instalación, en donde se debe seleccionar un lenguaje para la interfaz del instalador.

El proceso de instalación es similar al que se lleva a cabo para instalar Ubuntu desktop y es normalmente sencillo [1].

Se elige el lenguaje que usará el sistema operativo, una ubicación geográfica, la configuración del teclado, el adaptador de red principal, el nombre del servidor, el nombre del administrador que tendrá privilegios de root, la contraseña del administrador y la confirmación de esta que también sirven para las conexiones por SSH y la ubicación geográfica. Terminados estos pasos se inicia el proceso instalación que puede tardar hasta 20 minutos.

Finalizado el proceso de instalación se debe retirar la imagen de la unidad óptica y reiniciar el sistema operativo.

2.5 MÉTODO DE INGRESO

La primera vez que se inicie el sistema, se abre un explorador web en donde se debe aplicar la excepción de seguridad para iniciar el panel de control del Zentyal. El enlace de acceso guarda la siguiente estructura: https://IP_o_hostname:8443

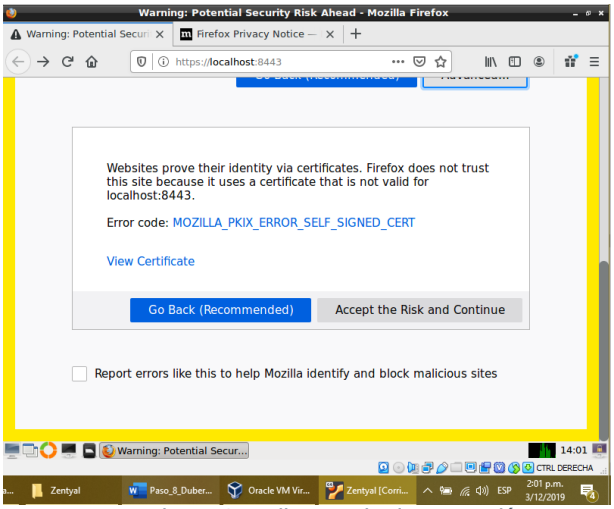

Figura 3. Aplicar regla de excepción

Luego se deben ingresar los datos de las credenciales del administrador creadas en la instalación. Se debe tener presente que solo se puede acceder a la GUI de administración web a través de HTTPS (no HTTP simple) y se encuentra en el puerto 8443 de forma predeterminada.

2.6 DESCARGA DE PAQUETES

Para implementar servicios de infraestructura IT se deben descargar los paquetes para la instalación de las herramientas que soportan estos servicios. Se seleccionan y se da en instalar.

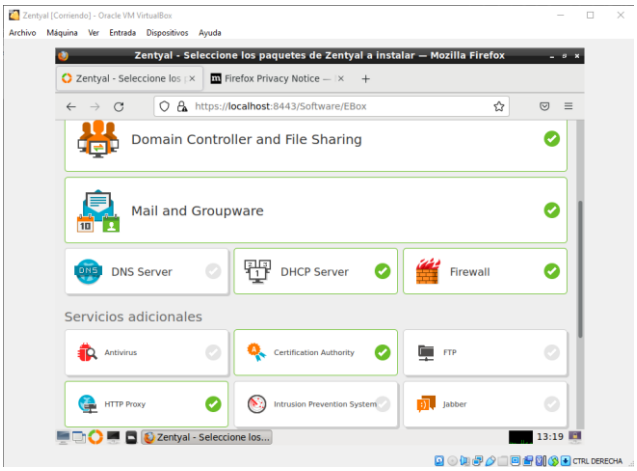

Figura 4. Herramientas de Zentyal

Posterior a la selección de los paquetes, se confirman y se inicia la instalación. Al terminal este proceso se va a solicitar configurar las interfaces de red. La interfaz que tiene el acceso a internet se configura como externa y la interfaz que sirve de conexión a la subred como interna.

Figura 5. Tipos de interfaces de red.

Seleccionadas las configuraciones de red se debe establecer el direccionamiento IP. Para la red externa la selección de IP se hará por DHCP y para la red interna de forma manual escribiendo una IP de acuerdo con la red anfitrión para VirtualBox y usando la misma máscara.

Figura 6. Direccionamiento IP de interfaces de red.

Posteriormente se debe establecer al servidor como controlador de dominio (Stand-alone) y escribir un nombre de dominio que debe ser diferente al nombre del host.

Figura 7. LDAP y nombre de dominio.

Para finalizar se guardan las configuraciones y se identifica el direccionamiento IP como constatación desde la terminal con el comando ip a s

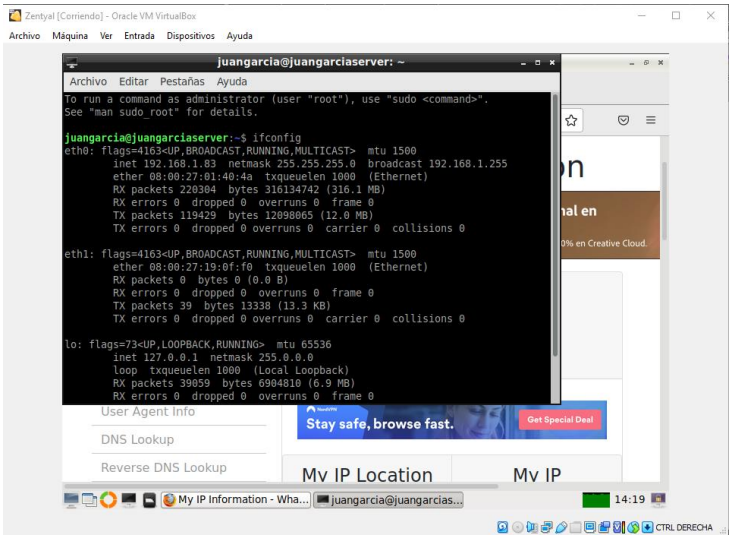

Figura 8. Direcciones IP.

3 IMPLEMENTACIÓN DE SERVICIOS

En la administración y control de servicios para intranet y extranet se establece la instalación, configuración y puesta en marcha de las herramientas para DHCP, DNS, controlador de dominio, proxy no transparente, cortafuegos, acceso a carpetas compartidas e impresoras a través de LDAP y VPN

3.1 PROXY NO TRANSPARENTE

Realizamos instalación de Firewall para poder realizar la configuración del proxy no transparente.

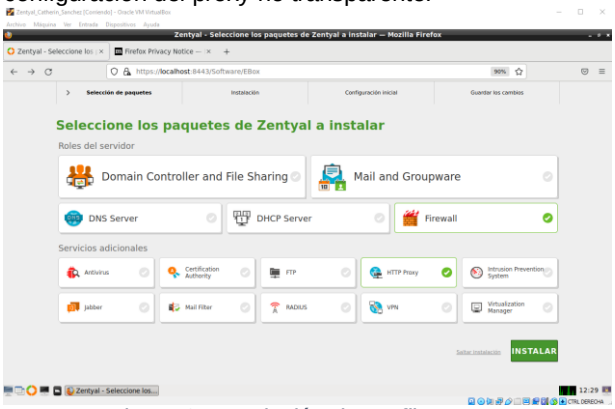

Figura 9. Instalación de perfiles y paquetes

3.1.1 CONFIGURACIÓN INTERFACES DE RED

Ingresamos a configuración tipos de interfaces-> para el puerto de Ethernet eth0 asignamos la HMC con el servido DHCP y para el puerto Ethernet primario eth1 asignamos el HMC estático con la dirección IP.

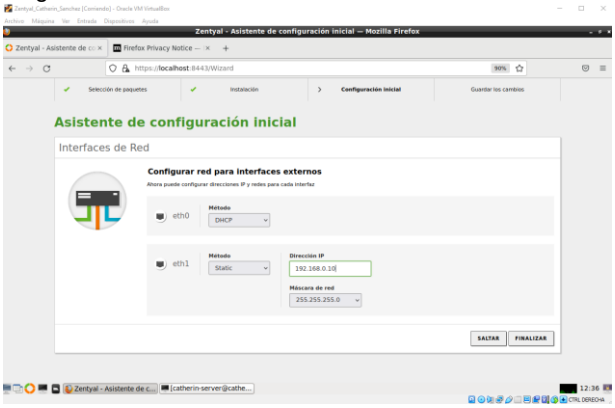

Figura 10. Interfaces de red

3.1.2 CONFIGURACIÓN DEL PROXY

Realizamos la configuración del perfil de filtrado y seleccionamos la opción de reglas de dominio y URLS donde se especificará la página que tendrá restricción.

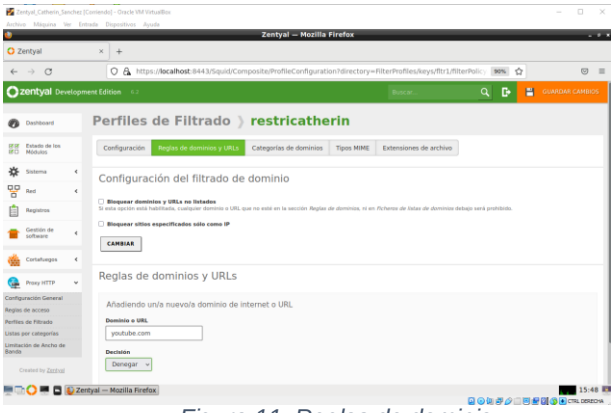

Figura 11. Reglas de dominio

3.1.3 CONFIGURACIÓN DE REGLAS DE DOMINIO

Dentro de la opción de reglas de dominio y URL bloqueamos el acceso a Youtobe.com y permitimos el acceso a Facebook.com.

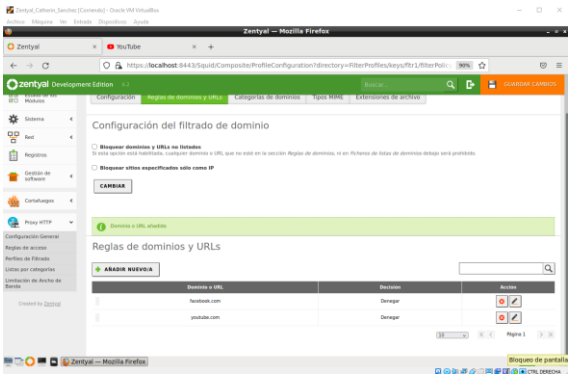

Figura 12. Reglas de dominio

3.1.4 CONFIGURACIÓN REGLAS DE ACCESO

Dentro de reglas de acceso en la opción “Decisión”, se activa el perfil “restricatherin”

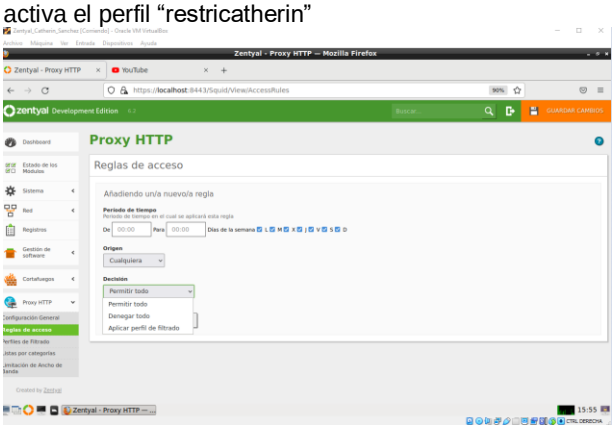

Figura 13. Reglas de acceso.

3.1.5 CONFIGURACIÓN DE RED

Vamos a las opciones de configuración del navegador e ingresamos a configuración de red.

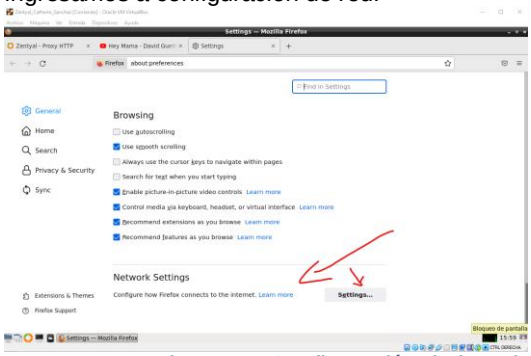

Figura 14. Configuración de la red.

3.1.6 CONFIGURACIÓN DE ACCESO A INTERNET

Seleccionamos la configuración manual de proxy, donde ingresamos la dirección IP y el puerto de conexión 1230.

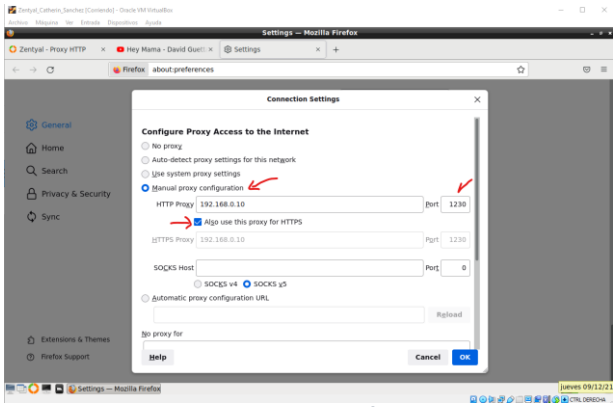

Figura 15. Configuración proxy HTTPS.

3.1.7 CONFIRMACIÓN DE ACCESO

Verificamos conexión ingresando a YouTube.

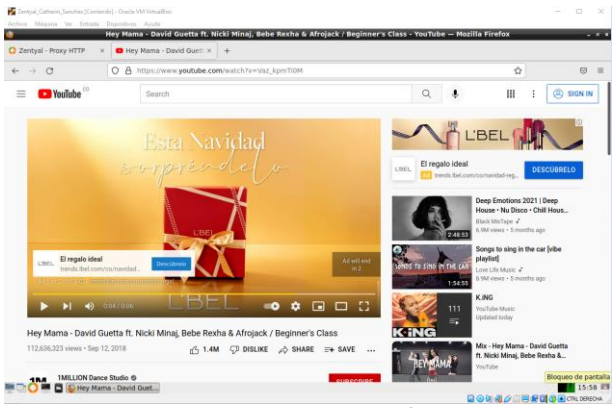

Figura 16. Ingreso a página web

3.2 VPN

Una red privada virtual (RPV), en inglés: Virtual Prívate Network (VPN), es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Se puede configurar Zentyal para dar soporte a clientes remotos, a través del servicio VPN, ya que un servidor Zentyal, trabaja como puerta de enlace y como servidor VPN, que tiene una red local detrás, permitiendo a clientes externos conectarse a dicha red local.

Para este punto, manejan dos máquinas virtuales, una para el servidor Zentyal y otra para la maquina cliente con el sistema operativo Ubuntu Desktop. Ambas maquinas tienen dos adaptadores uno en Bridge y el otro en Red Interna.

3.2.1 CONFIGURACIÓN DE SERVIDOR VPN

Tras instalar el servidor y los paquetes necesarios que son Cortafuegos o Firewall, Autoridad de certificado y VPN, se configuran las dos interfaces del servidor (eth0 y eth1), las cuales para este punto se manejaron eth0 como externa y eth1 como interna y ambos con IP dinámica es decir DHCP.

Tras configurar esto, los primeros que se realiza es generar el certificado de autenticidad del servidor Zentyal, esto se realiza en el Menú “Autoridad de Certificación” en la sección “General”. En el formulario se ingresa el nombre que aparecerá en certificado y el tiempo de vigencia. [3]

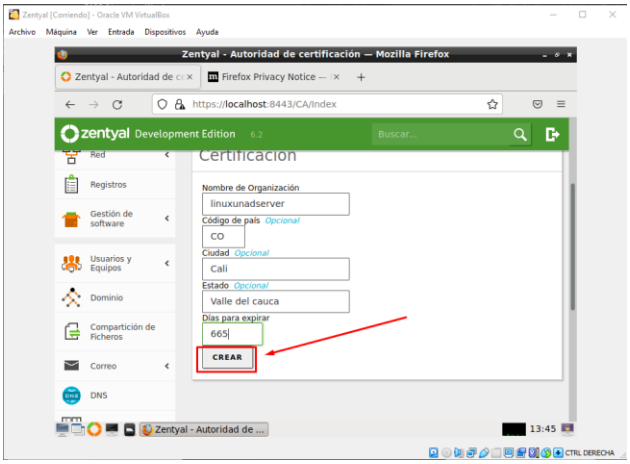

Figura 17. Certificado de autenticidad.

Con el certificado creado, se procede a generar el servidor VPN, para ello se debe ir al Menú “VPN” y a la

sección “Servidores”. Se añade un nuevo servidor el cual por ahora debe estar inhabilitado

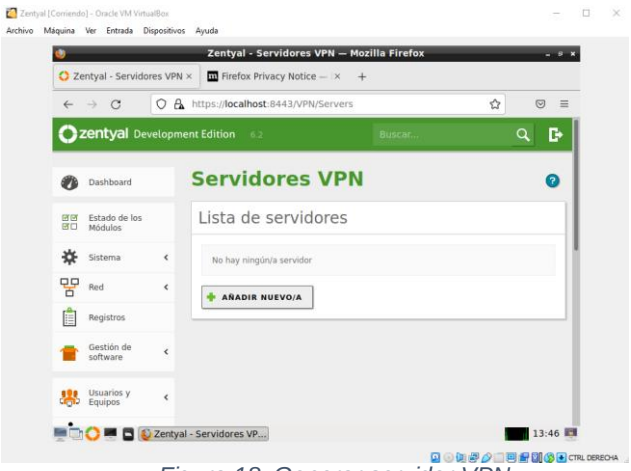

Figura 18. Generar servidor VPN

Tras haber generado el servidor VPN, se debe generar el certificado de este. Para ello se regresa al menú “Autoridad de certificados a la sección “General” y se llena la información.

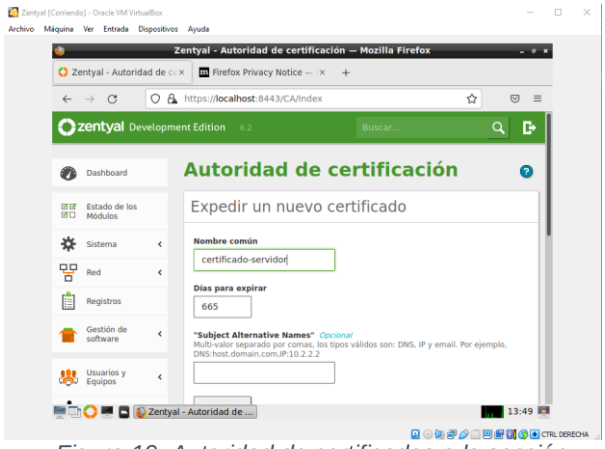

Figura 19. Autoridad de certificados a la sección

Una vez el certificado se genera, se debe configurar el servidor VPN Generado. Para ello se va al menú “VPN” a la sección “Servidores” y se accede a la configuración del servidor VPN. Aquí se define el Puerto del servidor el cual es UDP y se deja el túnel por defecto. Se deja la dirección VPN que esta por defecto, aunque si se desea se puede cambiar; se selecciona el certificado del servidor recién generado y se habilita la interfaz TUN.

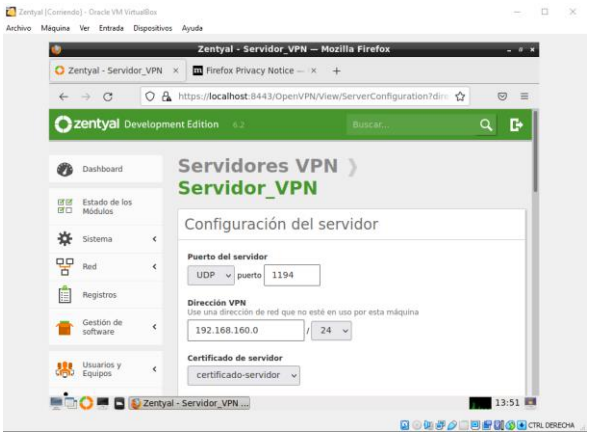

Figura 20. Interfaz TUN

3.2.2 CREACIÓN DEL SERVICIO VPN

Ya con el servidor VPN configurado, se debe generar el servicio que funciona con el servidor. Por ello se va al menú “Red” y a la sección “Servicios”. Allí se genera un nuevo servicio.

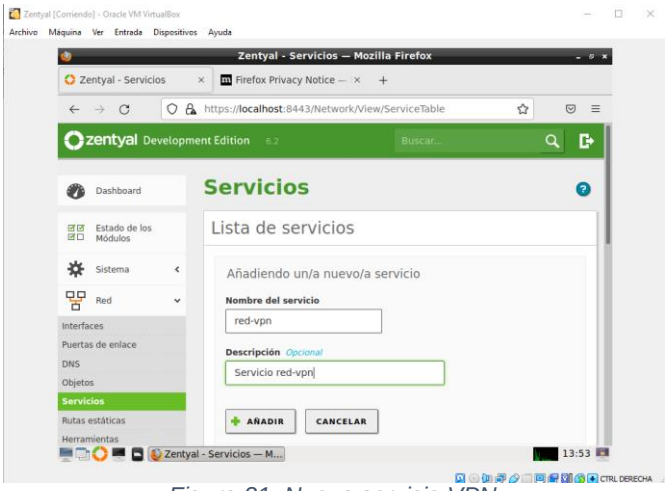

Figura 21. Nuevo servicio VPN.

Tras añadir el servicio, se debe configurar; para ello se accede a la configuración del servicio creado, se agrega un nuevo perfil de configuración y se ingresa la misma información del puerto del servidor VPN creado, en donde el puerto de origen puede ser cualquiera y el puerto de destino es el mismo del servidor VPN. [4]

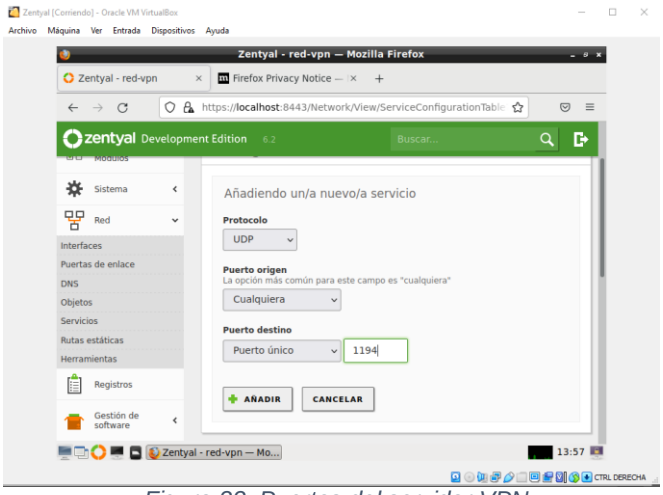

Figura 22. Puertos del servidor VPN

3.2.3 ESTABLECIMIENTO DE LA REGLA DE FIREWALL

Con el servicio ya configurado, se debe ahora establecer la regla en el Firewall que permitirá la conexión con el servidor a través del servicio generado. Para ello se accede al menú “Cortafuegos” a la sección “Filtrado de paquetes”. Aquí se debe acceder a la opción “Configurar Reglas” de la sección “Reglas de filtrado desde las redes internas a Zentyal”. Allí se debe indicar que la decisión es de aceptación desde cualquier origen y usando el servicio VPN generado. [4]

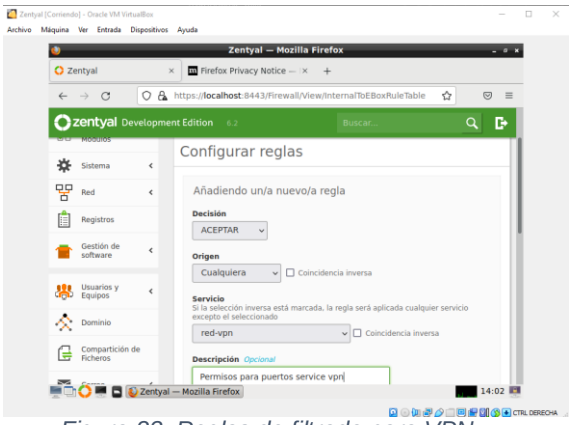

Figura 23. Reglas de filtrado para VPN

Ya con esto realizado, se regresa al servidor VPN y se accede a la configuración de redes anunciadas. Aquí se debe agregar una nueva red anunciada cuyo nombre puede ser cualquiera.

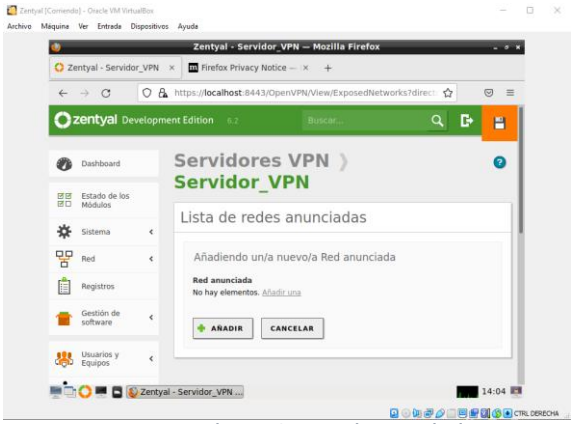

Figura 24. Red anunciada

3.2.4 PAQUETE DE CONFIGURACIÓN DE CLIENTE

Tras generar la lista de redes se debe descargar el paquete de configuración que usará el cliente. Para ello se regresa un poco y se accede a esta opción en la lista de servidores, en donde se sigue la configuración que está en la imagen, pero se debe obtener la IP pública y la IP local para ingresarlas en el formulario, además de indicar el certificado del cliente del servidor y el tipo del sistema operativo del cliente.

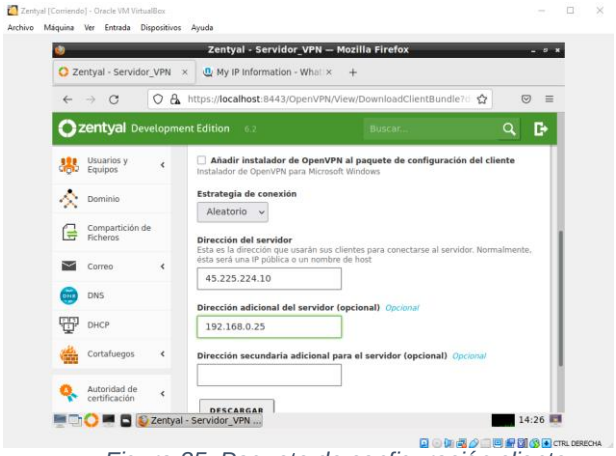

Figura 25. Paquete de configuración cliente

Este paquete se debe enviar a la máquina del cliente. Con el paquete generado se habilita el servidor VPN y se verifica su funcionamiento desde el Dashboard.

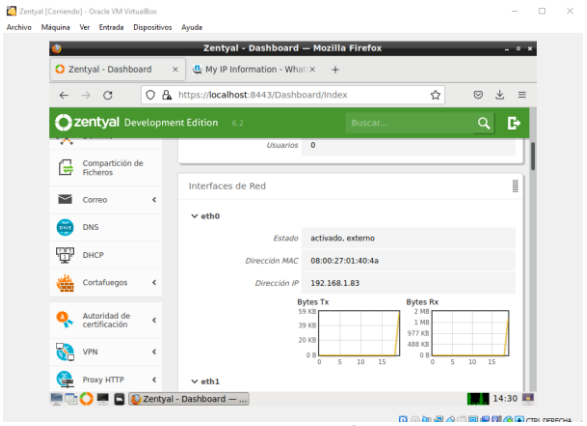

Figura 26. Verificación del paquete.

3.2.5 CONEXIÓN CLIENTE-SERVIDOR

Tras configurar Zentyal, se debe ir a la máquina del cliente. Una vez allí se descarga y se descomprime el paquete del cliente generado por el servidor. Posteriormente se debe instalar OpenVPN en la máquina.

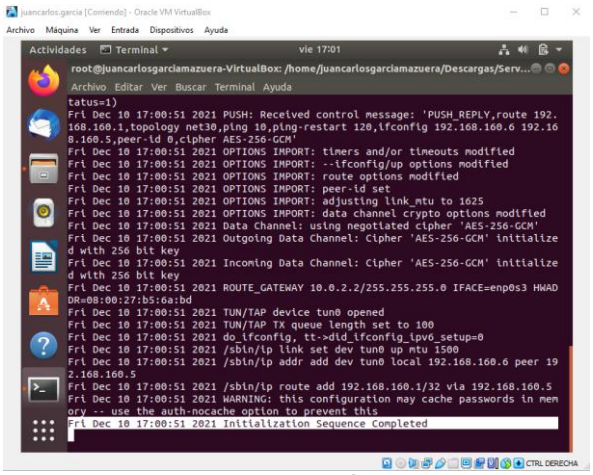

Figura 27. Instalación VPN Ubuntu

Tras instalarlo, ya se puede realizar la conexión utilizando el comando *openvpn --config* e indicando la ruta del archivo. *conf* del paquete de configuración.

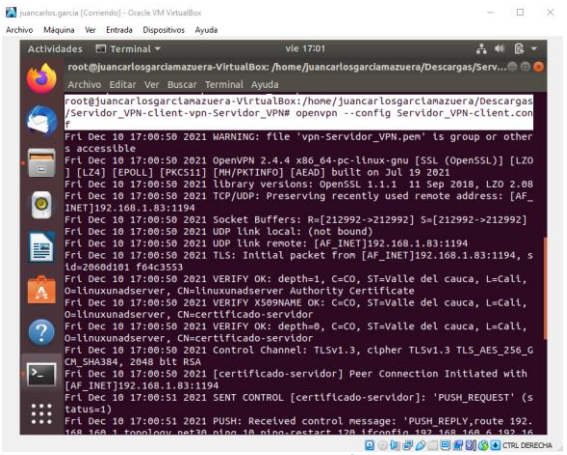

Figura 28. Conexión con VPN

De esta manera se establece la conexión VPN entre el servidor y la maquina Ubuntu. Esta conexión se puede comprobar de dos maneras; primero desde los registros del servidor, se pueden ver las conexiones del servicio VPN y allí debe visualizarse la IP de la maquina Ubuntu, y segundo realizando una conexión SSH desde Zentyal usando la IP que se le asigna a la maquina por la conexión VPN la cual es diferente de la local. Y una vez la conexión se establece se puede acceder a los archivos de la máquina.

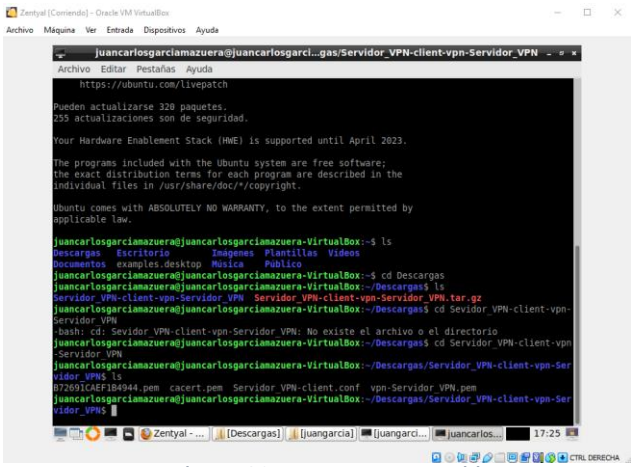

Figura 29. Acceso a contenidos

3.3 CORTAFUEGOS

Inicialmente es importante segmentar las redes para así poder tener el control total del tráfico entre ellas desde Zentyal. Para esto se utilizaron dos interfaces de red. La primera que conecta con el proveedor de internet a través de DHCP. La segunda configura la red interna con ip estática 192.168.1.150; todo el host conectados a la red interna estarán en este rango de ip y utilizarán como puerta de enlace la asignada para eth1. Así recibirán tráfico según las políticas establecidas en el Firewall de Zentyal.

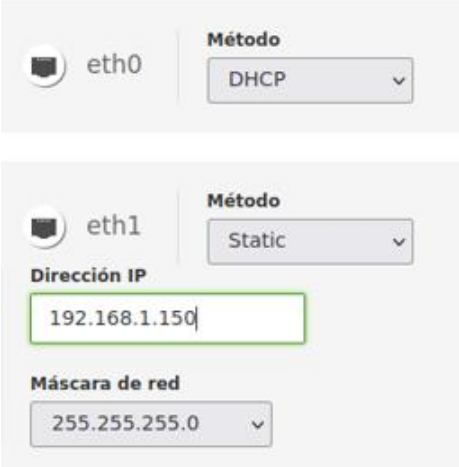

Figura 30. Configuración de interfaces en Zentyal.

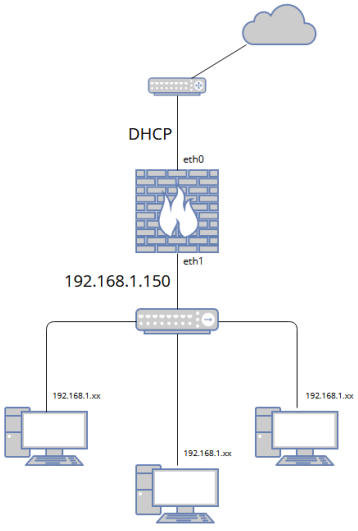

Figura 31 Diagrama de red en la práctica.

Como resultado de esta configuración los hosts de la red interna solo podrán obtener tráfico de internet a través de su puerta de enlace.

Si bien los hosts de la red interna podrían cambiar su configuración de red, para recibir ip desde DHCP, por ejemplo, no serían capaces de alcanzar la zona abierta ya que la única interfaz conectada es eth0 en el Firewall. El cortafuego de Zentyal es capaz de recibir la configuración de reglas y políticas que permiten o restringen tráfico total o parcial a toda la red interna o a hosts específicos.

Para esta práctica se configuraron las reglas que me permiten restringir el acceso a redes sociales para toda la red interna. Es necesario conocer la ip publica detrás del dominio de cada sitio a bloquear ya que esta ip será la que configuraremos como restringida en la regla. Usamos NSLOOKUP para este propósito.

Figura 32 Obteniendo ip publica de Facebook con nslookup

Finalmente configuramos cada una de las reglas para filtrado de paquetes en Zentyal.

4. TEMATICAS *DHCP*

Es importante menciona las temáticas a desarrollar en este documento, también se describe el paso a paso de cada una de ellas, como es su configuración e implementación mediante el servidor Zentyal 6.2, a continuación, se menciona cada una y que servicio se debe implementar.

Tabla 2. Temáticas

TEMATICA	SERVICIOS
1	*DHCP Server, DNS Server y Controlador de Dominio.*
2	*Proxy no transparente.*
3	*Cortafuegos.*
4	*File Server.*
5	*VPN.*

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 estricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

Lo primero que haremos será realizar el proceso de configuración de nuestro servidor Zentyal para que este le de conexión mediante DCHP a nuestro cliente (Ubuntu 18.04 LTS) el cual se conectara mediante este para poder realizar las restricciones solicitadas.

Para ello lo primero será realizar la configuración de la primera tarjeta de red eth0 como DHCP.

Así mismo será la de realizar el proceso de configuración de la segunda red, eth1 como una IP estática, la cual tendrá como como IP a 192.168.7.254 / 255.255.255.0.

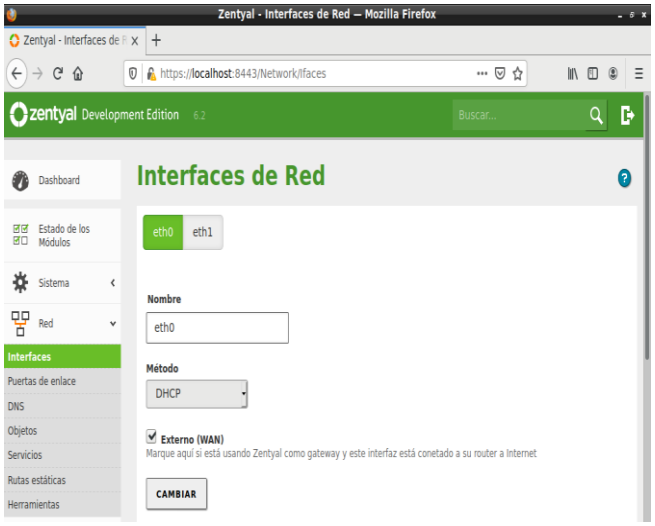

Figura 33 interfaz de red

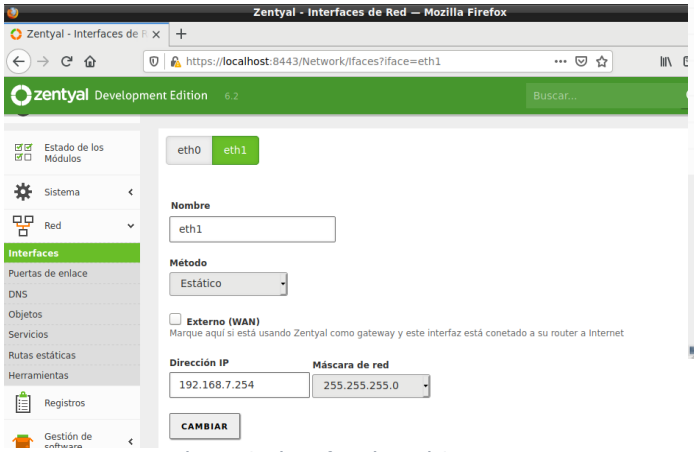

Figura 34 interfaz de red 2

Posteriormente, será realizar la configuración del DHCP (Interfaz), para ello acedemos al módulo del mismo nombre en Zentyal para proceder con dicha configuración.

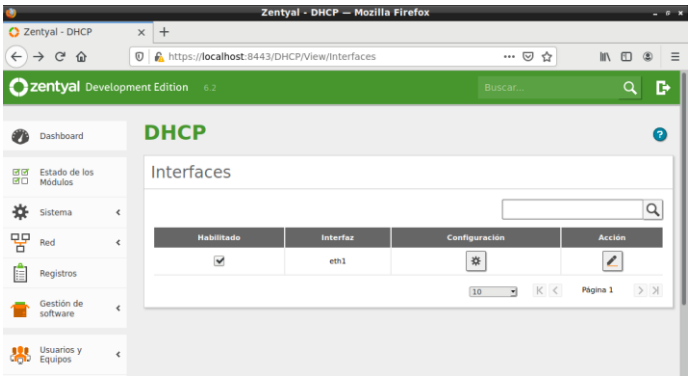

Figura 35 interfaz de red DHCP

Aquí, dentro de configuraciones lo que haremos será realizar el proceso de asignar rangos, es decir de donde queremos que se asigne la primera IP a nuestro equipo hasta cual, en nuestro caso teniendo en cuenta que iniciamos desde 192.168.7.1 dejamos 19 IPS sin asignar y vamos a realizar el rango a partir de la IP 192.168.7.20 la cual debe ser la que se le asigne automáticamente a nuestro cliente cuando se conecte, ya que solo habrá una maquina (Ubuntu 18.04 LTS).

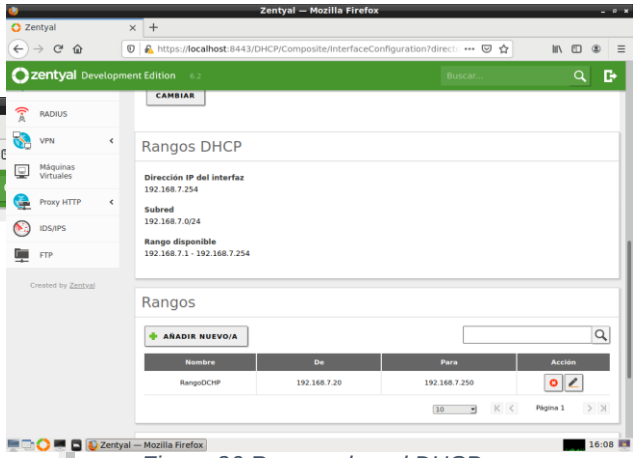

Figura 36 Rangos de red DHCP

Una vez terminada parte de la configuración de nuestra red en el servidor ZENTYAL vamos a realizar el proceso en nuestra máquina de cliente, la cual tiene como S.O. Ubuntu 18.04 LTS, para verificar que esta funcionado nuestro DHCP y tenga conexión a internet para luego proceder con las restricciones.

Accedemos en nuestra máquina.

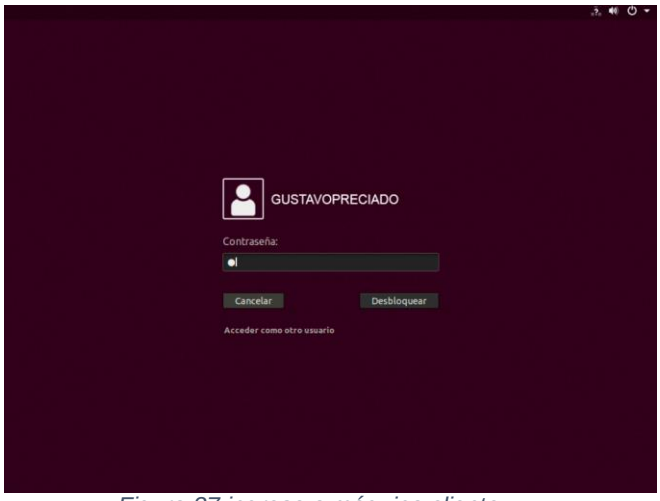

Figura 37 ingreso a máquina cliente

Vamos a las configuraciones de RED, donde vamos a verificar a que ya tenga INTERNET VIA DHCP, para ello simplemente damos en de DETALLES:

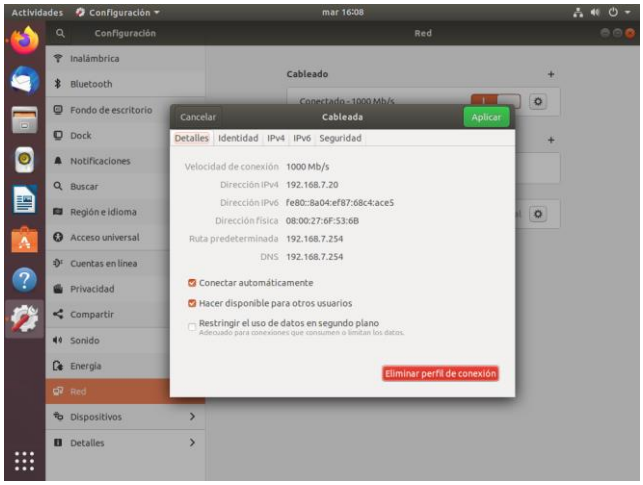

Figura 38 red cliente

Una manera de también verificar es ir a nuestro servidor ZENTYAL y ver en el apartado de conexiones por DHCP en la cual tiene que aparecer nuestra máquina**.**

IPs asignadas con DHCP

Dirección IP	Dirección MAC	Nombre de máquina
192.168.7.20	08:00:27:6f:53:6b	pedropulido

Figura 39 maquina conectada vía Zentyal

Ahora una vez verificado que si esta funcionado las conjuraciones que realizamos de manera previa en nuestro servidor, lo que haremos será probar la conexión a internet a los sitios que VAMOS A RESTRINGIR, para ello en este caso serán: Redes sociales como FACEBOOK, TWITTER, Imagen X. Conexión Twitter, INSTAGRAM y por el lado de entretenimiento será una página de deportes, MUNDODEPORTIVO.

MUESTRA DE CONEXIÓN A INTERNET A LOS SITIOS:

►FACEBOOK.

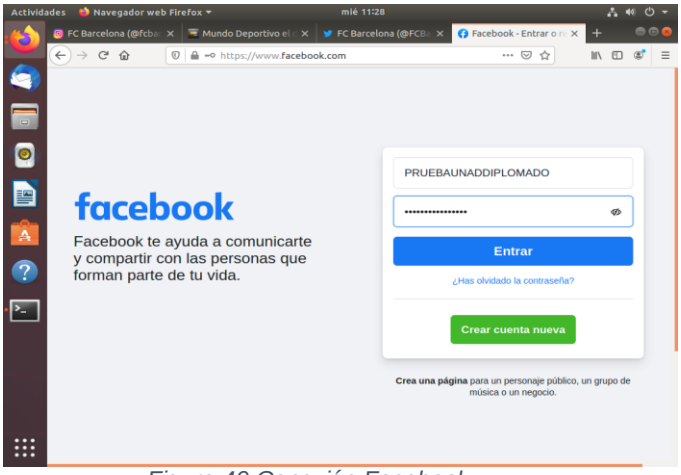

Figura 40 Conexión Facebook

►TWITTER

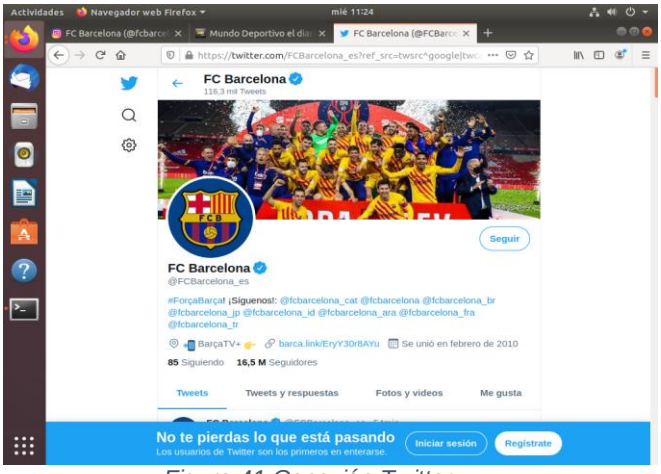

Figura 41 Conexión Twitter

►INSTAGRAM

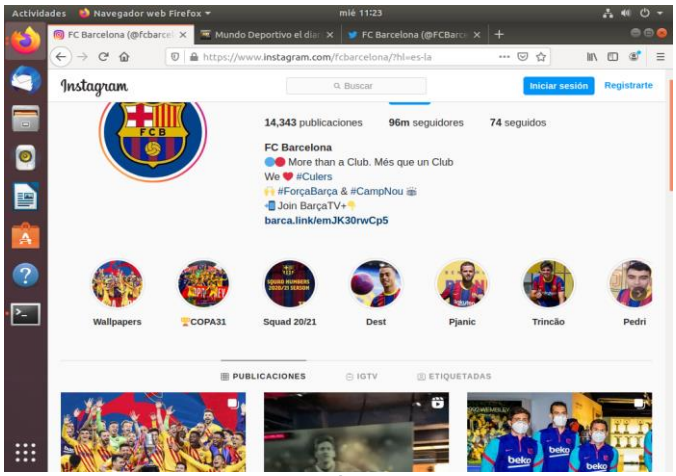

Figura 42 Conexión Instagram

►MUNDO DEPORTIVO

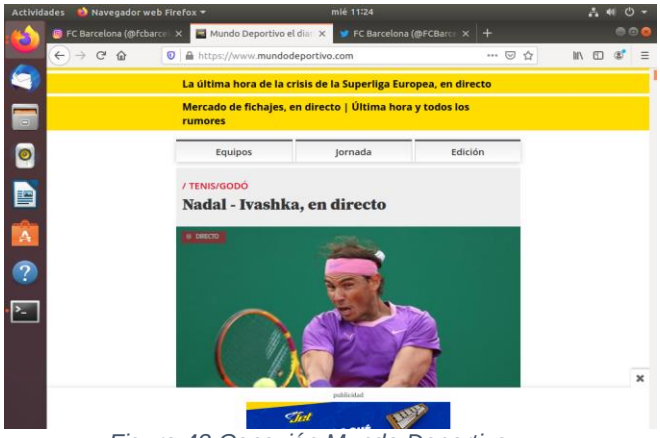

Figura 43 Conexión Mundo Deportivo

Una vez que hemos comprobado que cada sitio funciona de manera correcta lo que vamos a realizar será la denegación de cada servicio en el **SERVIDOR ZENTYAL**, pero antes de ello vamos a obtener la **IP DE CADA SITIO**, en este ejemplo mostrare la de Facebook, pero es igual para el resto, mediante el comando "**nslookup**" nos permite obtener la dirección IP para que esta sea la que vayamos a bloquear.

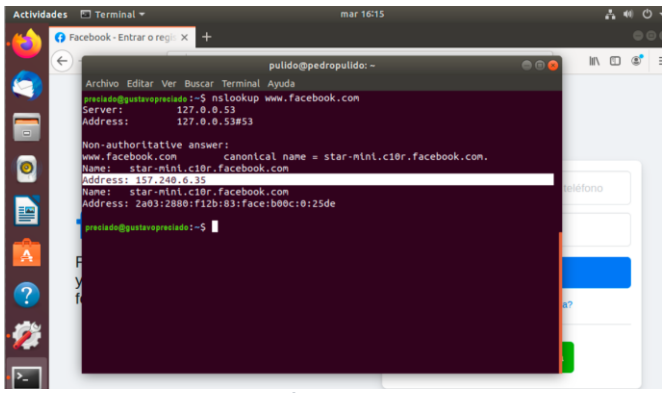

Figura 44 Ejecución comando nslookup

Una vez obtenida dicha IP, nos dirigimos a nuestro servidor zentyal. Vamos a la opción "**CORTAFUEGOS**", posteriormente a la opción "**FILTRADO DE PAQUETES**", y una vez estando ahí, nos aparecen 4 opciones, ingresamos a la que se llama "**REGLAS DE FILTRADO PARA REDES INTERNAS**".

Figura 45 Reglas filtrado Zentyal

Procedemos a agregar una nueva regla, la cual será "**DENEGAR**" y colocamos en "**DESTINO**" la ip del sitio que deseamos bloquear, como ya tenemos la IP en nuestro caso de **FACEBOOK** (la que obtuvimos previamente mediante el comando nslookup), ahora simplemente será configurar en el servicio "**HTTP**".

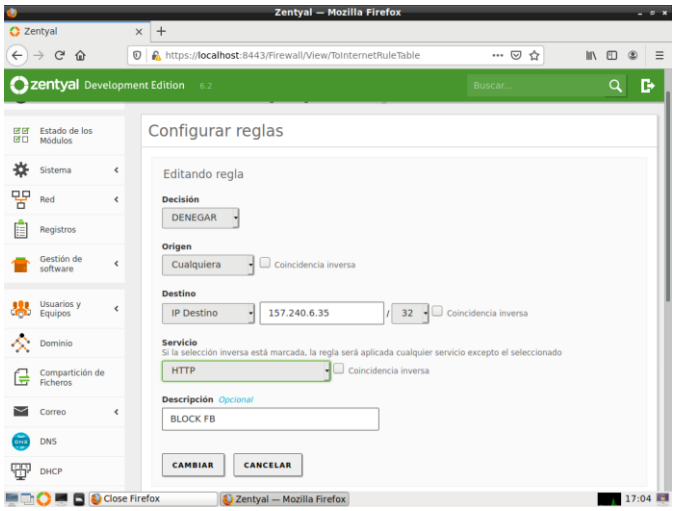

Figura 46. regla filtrado Facebook

Hay que tener en cuenta que, todos estos sitios funcionan mediante "**HTTP**" y "**HTTPS**" es decir, este último mediante el protocolo seguro, por eso hay que repetir cada regla 2 veces para cada sitio, para que cualquiera que sea el protocolo que utilice este bloqueada dicha IP.

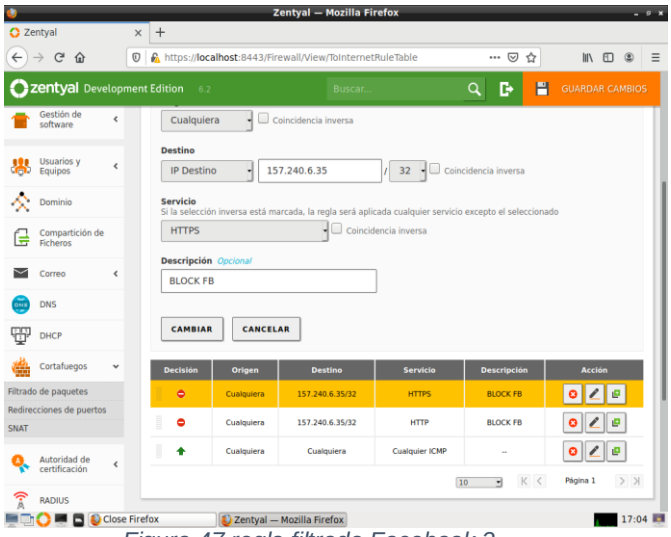

Figura 47 regla filtrado Facebook 2

Este proceso lo vamos a repetir con cada una de las IP de los sitios que tenemos, para proceder a bloquearlo, nos quedara algo así:

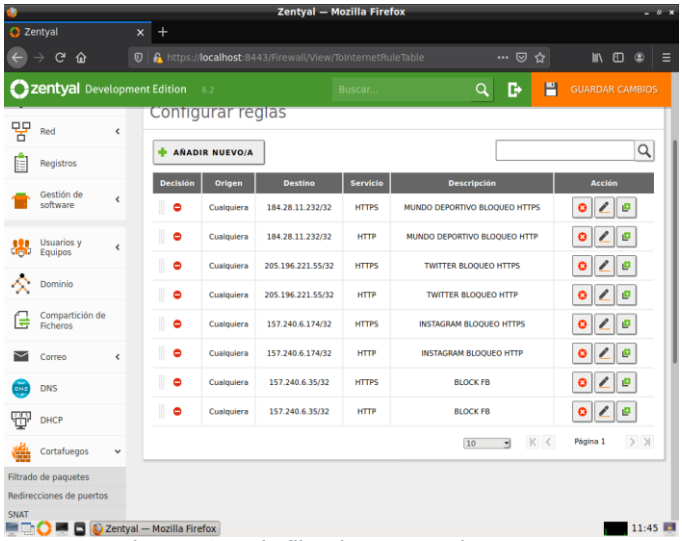

Figura 48 regla filtrado para paginas

Una vez tenemos los sitios a bloquear, procedemos ir la maquina cliente, para probar que estos no sirven.

NOTA: En caso de tener cargada la página en nuestro navegador (cliente) debemos cerrarla y borrar el cache, porque en muchos casos por este es que se accede a la página, entonces es bueno proceder a borrarlo e iniciar de nuevo el navegador a utilizar.

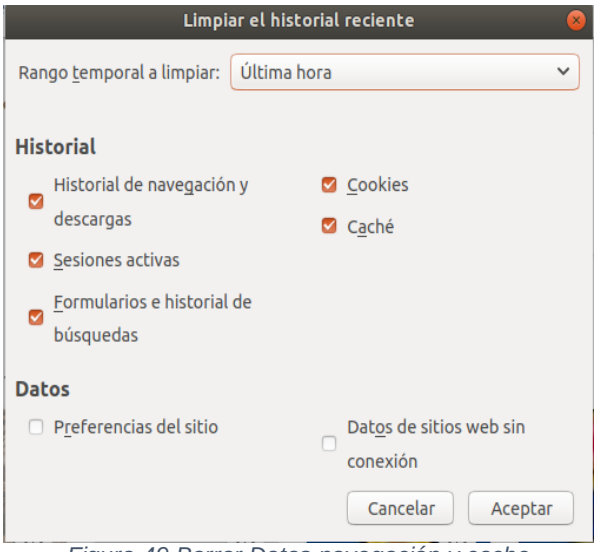

Figura 49 Borrar Datos navegación y cache

Ahora vamos a realizar el proceso, para comprobar que tenemos intente y que la pagina está siendo bloqueada, en modo ventana abriremos una página cualquiera que nos permite comprobar que hay conexión y en la otra la página que está siendo denegada por nuestro servidor.

PRUEBAS DE CONEXIÓN – PAGINAS BLOQUEDAS.

Abrimos nuestro navegador nuevamente y colocamos las paginas a testear, en nuestro caso usamos el navegador por defecto que trae, el mismo que hemos utilizado para todo lo realizado previamente, Firefox.

Para ello iniciamos con **FACEBOOK**

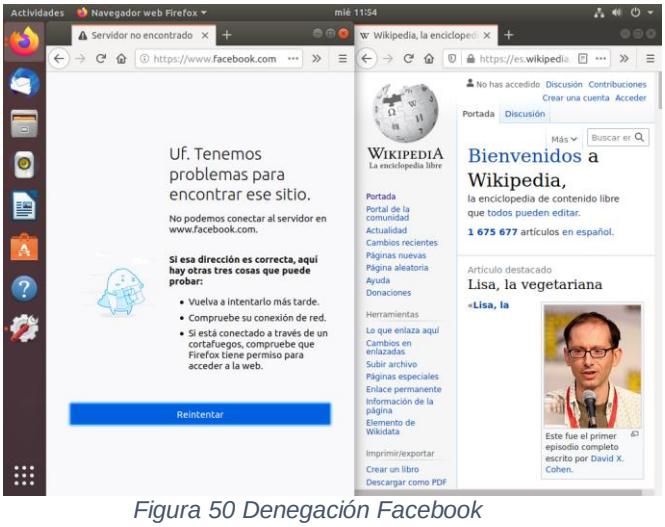

Figura 50 Denegación Facebook

Como podemos ver, no carga la página y por el otro lado tenemos la página de Wikipedia que funciona

normalmente, ahora procedemos a probar con las demás páginas, para verificar lo realizado.

Continuamos con **TWITTER**:

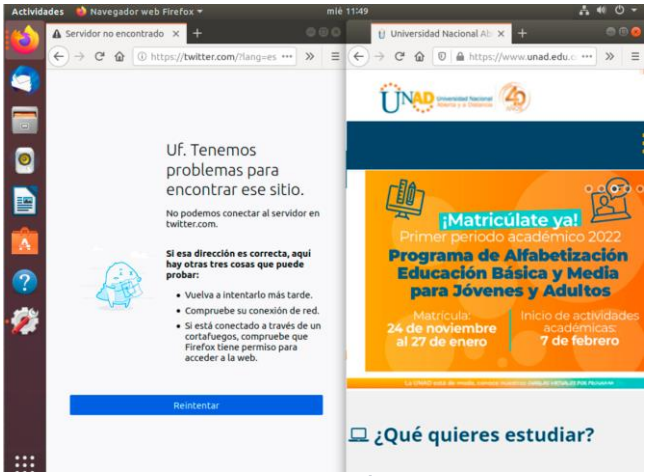

Figura 51 Denegación Twitter

Como se evidencia la página no va a cargar, es decir nuestro servidor va a denegar el servicio, por el otro lado tenemos una ventana abierta con la página de nuestra universidad donde funciona con total normalidad.

Proseguimos con la siguiente página, en este caso será **INSTAGRAM**:

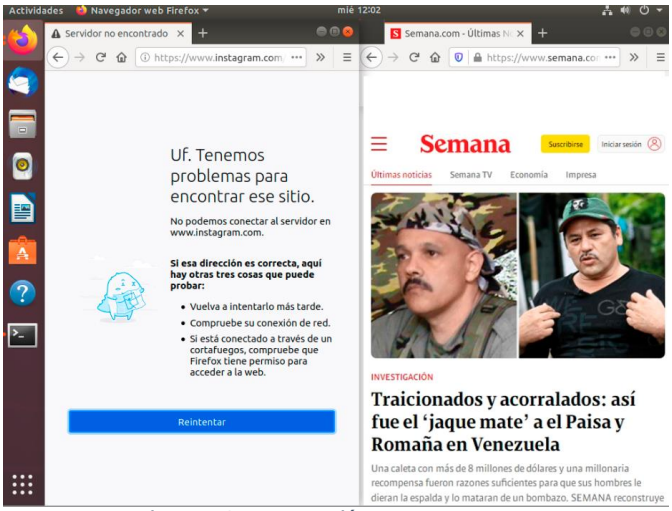

Figura 52 Denegación Instagram

Lo comparamos con una revista cualquiera, en este caso la revista "SEMANA.COM" la cual funciona normalmente.

Para finalizar procedemos con la última página, que será la que contiene a la paginan deportiva, **MUNDODEPORTIVO**.

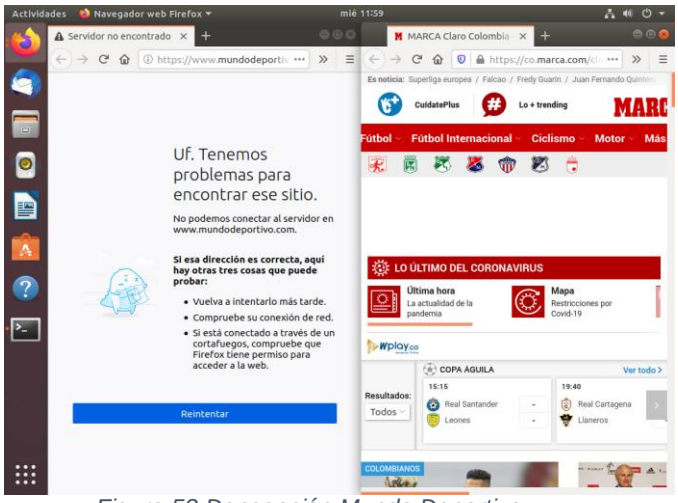

Figura 53 Denegación Mundo Deportivo

Como podemos ver, no nos deja ingresar, para comparar tenemos otra pagina deportiva "**MARCA**" la cual funciona con total normalidad.

Y eso sería todo, ya quedaron los sitios bloqueado para evitar el acceso desde nuestro "Cliente", se pueden aplicar para diferentes páginas, teniendo en cuenta que cada una tiene su IP, otras tendrán más de una, por lo tanto, tendrá que agregarse más reglas, pero en cuanto al funcionamiento como tal, es el mismo.

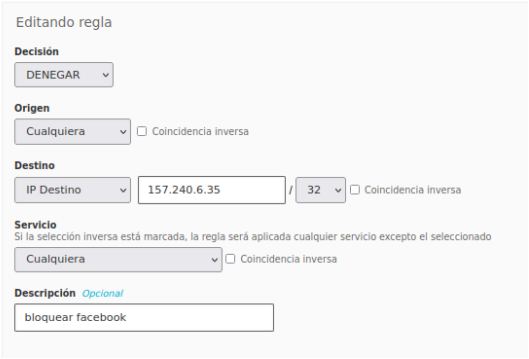

Figura 54 Configuración de regla para restringir Facebook.

Para que la regla funcione como se espera la decisión debe ser DENEGAR. El origen será Cualquiera ya que aplica para toda la red interna. Si quisiéramos que aplique para una ip especifica la configuraríamos ahí. El destino será la ip pública del sitio. El servicio será cualquiera. Aplicada esta regla y realizando las pruebas pertinentes, ningún host de la red interna puede acceder a www.facebook.com como se esperaba.

5. FILE SERVER

se presenta de manera práctica la configuración de carpetas compartidas a través del uso de la herramienta Zential bajo la licencia de prueba de la versión

comercial, la interface gráfica permite la administración de usuarios y grupos, configuración del dominio, compartición de ficheros y configuración del cortafuegos, pasos necesarios para compartir carpetas, se hace verificación de los recursos creados a través de la confirmación de los recursos creados en las subcarpetas share y profiles de la carpeta samba.

5.1 CONFIGURACIÓN DE ZENTYAL PARA COMPARTIR CARPETAS

Para que el usuario invitado tenga acceso a los recursos se debe activar en el gestor de usuarios y grupos (previamente en zential se debe activar "Dommain controller and file sharing" con lo cual aparecen las opciones: Usuarios y equipos, Dominio y Compartición de ficheros), se verifica que dentro de los servicios aparezca Samba

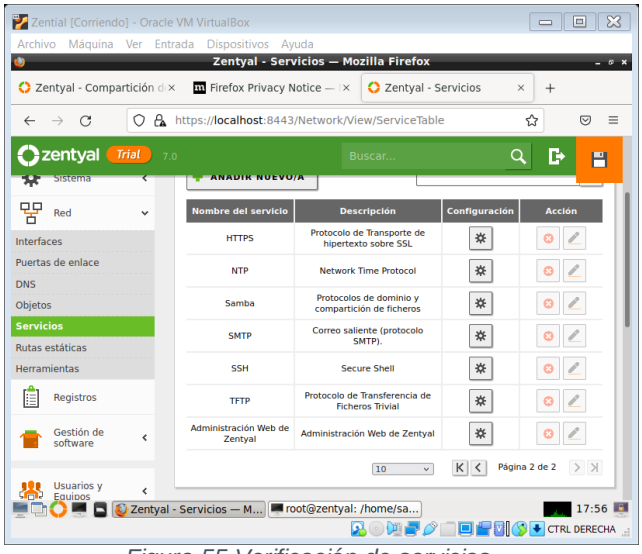

Figura 55 Verificación de servicios

Se verifican los puertos que componen samba el puerto 389 es LDAP y utiliza los protocolos TCP/UDP

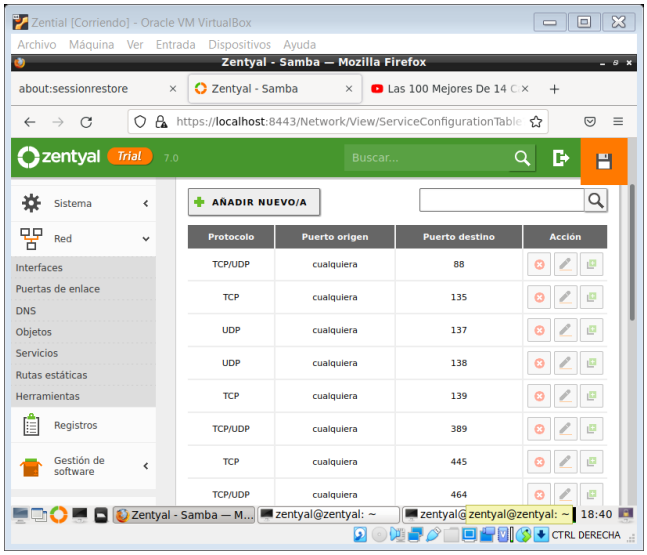

Figura 56 Verificación de protocolos y puertos

Ahora se verifica que todos los dispositivos conectados puedan hacer uso de samba para ello se accede a la configuración del cortafuego en filtrado de paquetes.

Se configuran las reglas de filtrado desde las redes internas a zentyal.

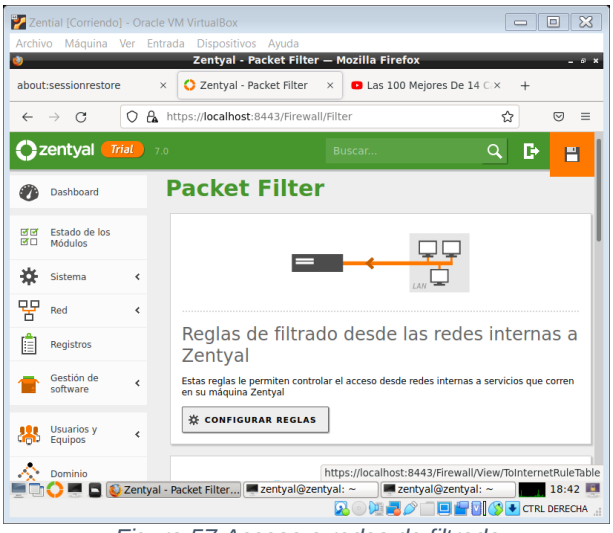

Figura 57 Acceso a redes de filtrado

Se cambia el origen de la conexión con samba a ip con la dirección IP del equipo que se encuentra conectado en este caso la máquina con Windows 11

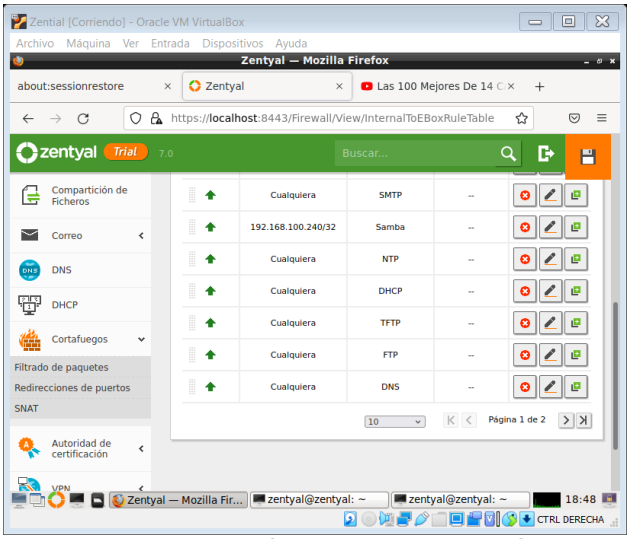

Figura 58 Configuración del origen de conexión con samba

Se revisan las reglas de filtrado para las redes internas y se configura la conexión entre los dos dispositivos únicamente a través de samba con eso se evita que al conectarse a otras redes u otros equipos se evite compartir carpetas o dispositivos.

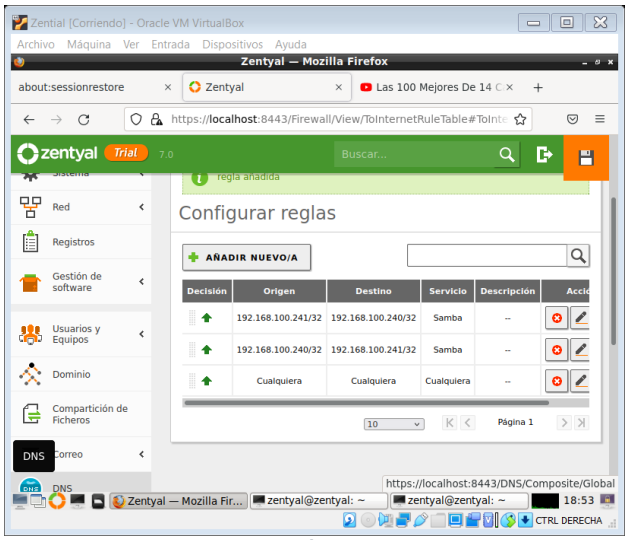

Figura 59 Configuración de reglas de filtrado

Se configura el controlador de dominio para ello se va a configurar el dominio con el DNS que viene por defecto zentyal.domain.lan

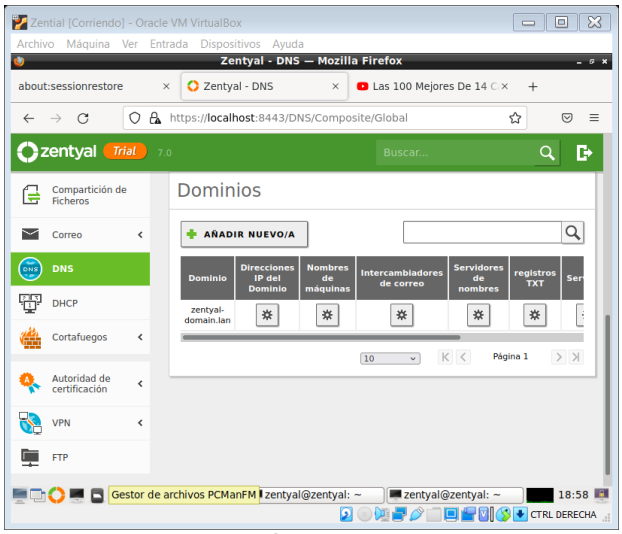

Figura 60 Configuración del controlador de dominio

Posteriormente se accede a usuarios y equipos opción gestionar.

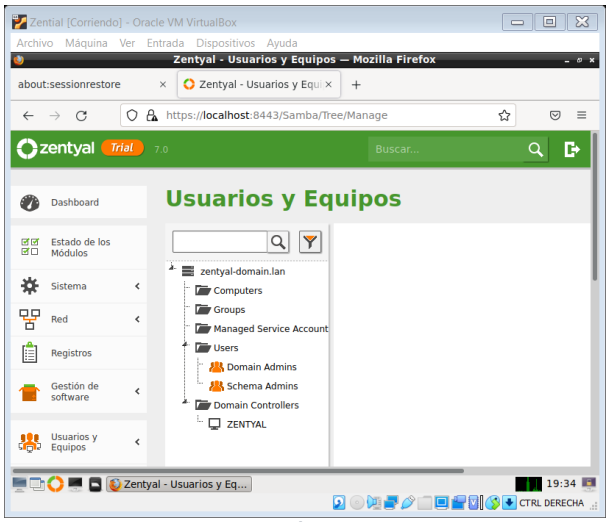

Figura 61 Configuración de usuarios y equipos

A través del terminal se confirma la creación del usuario accediendo a la carpeta home/profile

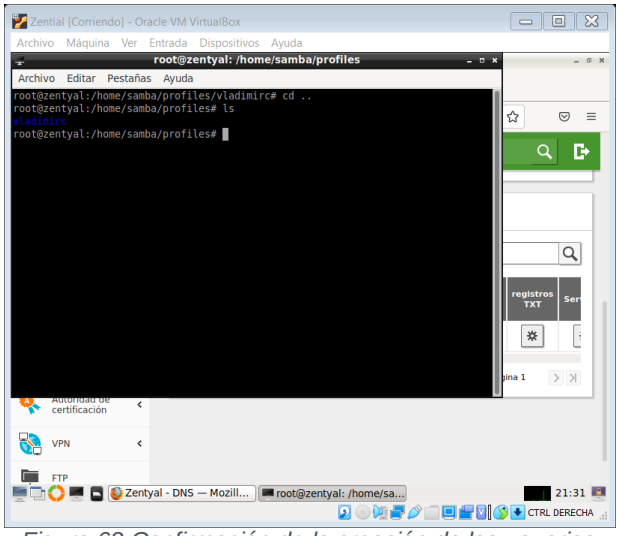

Figura 62 Confirmación de la creación de los usuarios mediante el terminal

Se verifica la creación de los usuarios y las carpetas compartidas

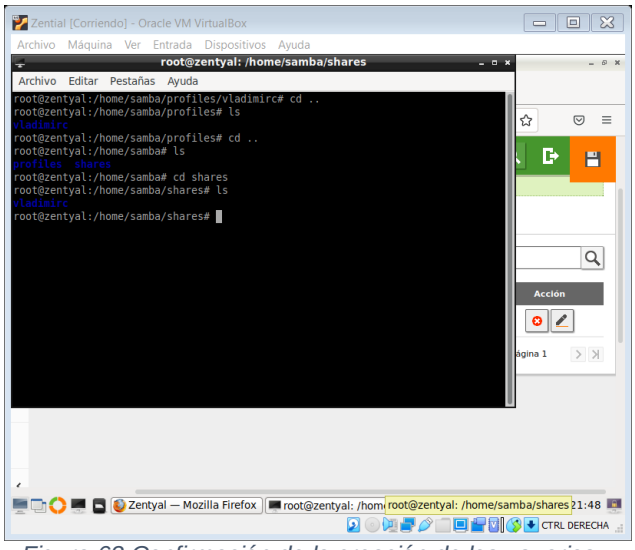

Figura 63 Confirmación de la creación de los usuarios mediante el terminal

6. CONCLUSIONES.

Zentyal permite la administración de recursos compartidos como archivos e impresoras asignando permisos a usuarios y grupos de acuerdo con la estructura de la organización y las funciones de cada uno de los usuarios.

Para implementar la totalidad de las funciones de zentyal es preciso adquirir la versión comercial la cual tiene un periodo de prueba de 45 días.

A través de zentyal es posible la configuración del dominio y la administración de los recursos vinculados a este.

7. REFERENCIAS

[1] Zentyal 7.0 Documentación Oficial; Zentyal Comunity. [En línea]. Available: https://doc.zentyal.org/es/

[2] Zentyal Wiki, «Usuarios, Equipos y Comparticion de ficheros,» 2018. [En línea]. Available: https://wiki.zentyal.org/wiki/Es/5.0/Usuarios,_Equipos_y_Comparticion_de_ficheros.

[3] C. M, «How to Install and Configure OpenVPN Server on Zentyal 3.4 PDC – Part 12.,» TecMint, 2014. [En línea]. Available: https://www.tecmint.com/install-openvpn-server-on-zentyal/. [Último acceso: 5 12 2019].

[4] Z. Wiki, «Servicio de redes privadas virtuales (VPN) con OpenVPN.,» Zentyal Wiki, [En línea]. Available: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_%28VPN%29_con_OpenVPN. [Último acceso: 2 12 2019].

[5] «Controlador de Dominio y Compartición de ficheros — Documentación de Zentyal 6.2». https://doc.zentyal.org/6.2/es/directory.html?highlight=impresora (accedido nov. 29, 2021).