SOLUCIONES DE INFRAESTRUCTURA TECNOLÓGICA A LA MEDIDA BAJO EL SISTEMA OPERATIVO GNU/LINUX ZENTYAL SERVER

Jeniffer Paola Cediel Bejarano
e-mail: jpcedielb@gmail.com
Natalia Medina Cerón
e-mail: nati210992@hotmail.com
Bernardo Beltrán Reyes
e-mail: bbeltranre@unadvirtual.edu.co
Yulder Peña Giraldo
e-mail: yspenag@unadvirtual.edu.co
Arvey Buritica Prieto
e-mail: aburiticap@unadvirtual.edu.co

RESUMEN: *El presente articulo describe los resultados obtenidos durante la implementación del Sistema Operativo GNU/Linux Zentyal Server como base para la instalación, configuración y puesta en marcha de los servicios DHCP Server, DNS Server, Controlador de Dominio, Proxy No Transparente, Cortafuegos, File Server, Print Server y VPN, los cuales son fundamentales para la infraestructura tecnológica de la empresa satisfaciendo los requerimientos y las necesidades específicas del cliente.*

ABSTRACT: *This article describes the results obtained during the implementation of the GNU/Linux Zentyal Server Operating System as a basis for the installation, configuration, and start-up of the DHCP Server, DNS Server, Domain Controller, Non-Transparent Proxy, Firewall, File Server services., Print Server and VPN, which are essential for the technological infrastructure of the company, satisfying the specific requirements and needs of the client.*

PALABRAS CLAVE: GNU/Linux, Red, Servidor, Zentyal.

1 INTRODUCCIÓN

Este documento recopila de manera detallada cada uno de los pasos necesarios para la instalación y configuración de diferentes servicios gestionados mediante el sistema operativo GNU/Linux Zentyal Server versión 6.2 en un entorno de red local virtualizado.

Cada uno de los servicios implementados traslada a la práctica las actividades desarrolladas durante el transcurso del Diplomado de Profundización en GNU/Linux y la descripción de cada servicio se organiza por temáticas.

En este sentido, los puntos abordados este artículo pueden ser replicados de manera que constituyen un recurso esencial para el apoyo durante la migración de la Infraestructura TI en un entorno empresarial.

2 INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER

2.1 REQUERIMIENTOS PARA LA INSTALACIÓN

Para la instalación del servidor en una maquina física o virtual los requerimientos mínimos para la instalación son:

- 10GB de Disco Duro
- 2GB de Memoria RAM
- Procesador con arquitectura x86_64 (64 bits)
- Los demás requisitos de hardware dependen de los módulos que se instalan, de cuántos usuarios utilizarán los servicios y de cuáles sean sus patrones de uso.

2.2 DESCARGA DE LA ISO DE SENTYAL SERVER

La descarga de la ISO de Zentyal Server se realiza desde el sitio web oficial: http://download.zentyal.com/zentyal-6.2-development-amd64.iso

2.3 PROCESO DE INSTALACIÓN

En este caso, la instalación se realizó utilizando el Software de virtualización “VirtualBox”, antes de arrancar la instalación, se configuro la red de las maquinas virtuales tanto del Zentyal como del cliente utilizado para acceder al servidor.

En las opciones de Red de la máquina virtual de Zentyal Server se habilito el “Adaptador 1” conectado a “Adaptador puente” y el “Adaptador 2” conectado a “Red interna” con el nombre “LAN”. Asimismo, en las opciones de red del equipo cliente se habilito el “Adaptador 1” conectado a la Red interna “LAN”.

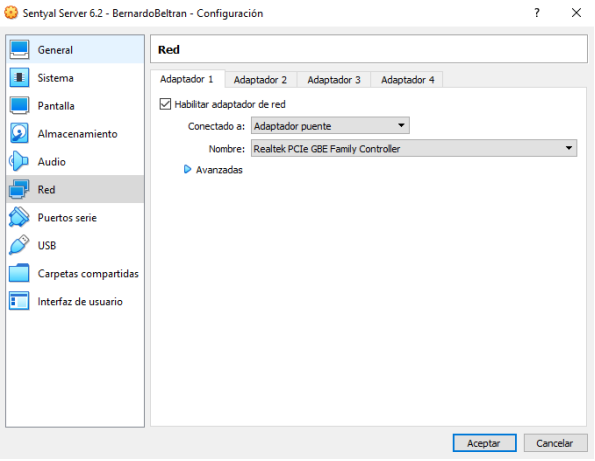

Figura 1. Configuración de Red Adaptador 1 Sentyal

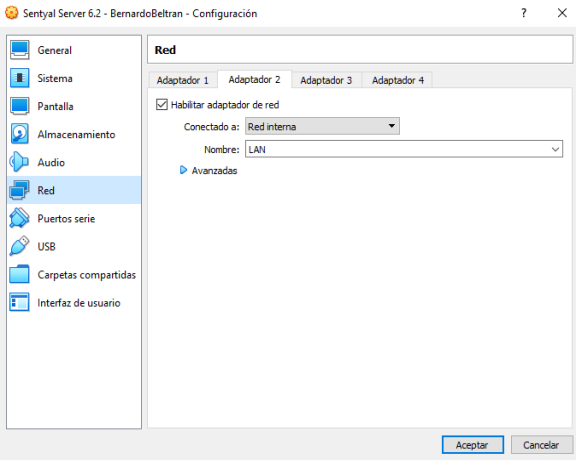

Figura 2. Configuración de Red Adaptador 2 Sentyal

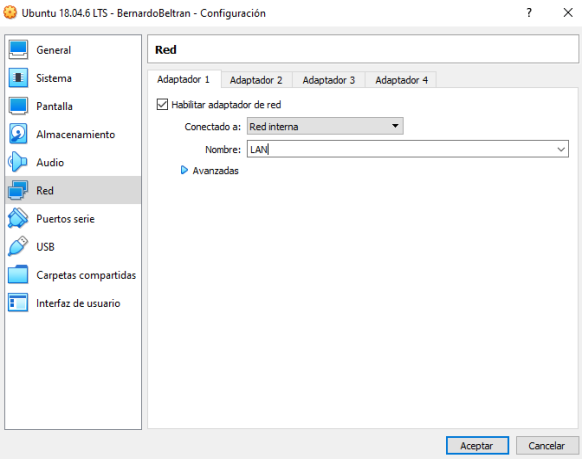

Figura 3. Configuración de Red Adaptador 1 Cliente

Luego de configurar los parámetros de red para las maquinas virtuales, arranca la instalación de Zentyal Server, se debe elegir el idioma a utilizar, las opciones de borrado del disco, ubicación y configuración del teclado.

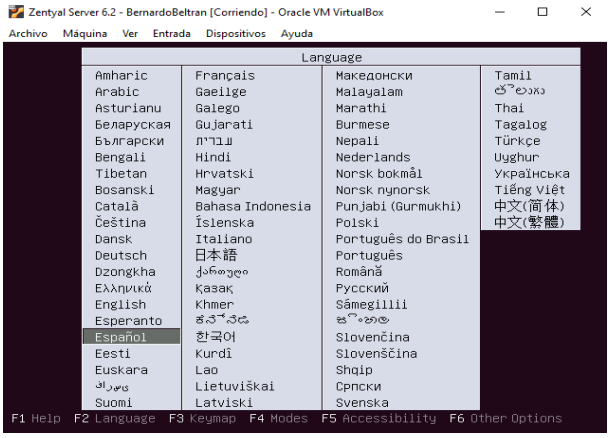

Figura 4. Opciones de idioma Zentyal Server

En seguida, es necesario indicar cual es la interfaz de red primaria (eth0), dicha interfaz debe corresponder con el adaptador de red configurado en modo “Adaptador puente”.

Figura 5. Configuración de red Zentyal Server

Una vez configurada la red, es necesario establecer un nombre para la maquina (hostname) al igual que un nombre de usuario, su respectiva contraseña y la zona horaria. En este punto, se realiza la descarga de los paquetes e instalación del sistema operativo, automáticamente se reinicia y abre el panel de control desde el navegador.

Figura 6. Asistente de configuración Zentyal Server

3 PLANTEAMIENTO Y CONTEXTUALIZACIÓN DEL PROBLEMA A RESOLVER

Solucionada gran parte de las problemáticas de migración de los sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, se entra en la fase final de la migración y puesta en marcha de los servicios solicitados.

Este trabajo está orientado principalmente a la administración y control de la distribución GNU/Linux Zentyal Server como base para implementar servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas.

3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Implementación y configuración de DHCP Server, DNS Server y Controlador de Dominio.

3.1.1 DHCP SERVER

Antes de instalar y configurar el servidor DHCP se debemos configurar las tarjetas de red que se encuentran por default en el sistema, para el caso de nuestro servidor la tarjeta de red interna o red local (LAN) la cual llevara una IP estática a partir de esta se le asignará automáticamente una IP a cada cliente que se conecte y una de red externa (WAN) la cual permitirá la conexión a internet.

a- Realizada la configuración de las interfaces de red, se instala el servidor DHCP desde la interfaz web de Zentyal Server.

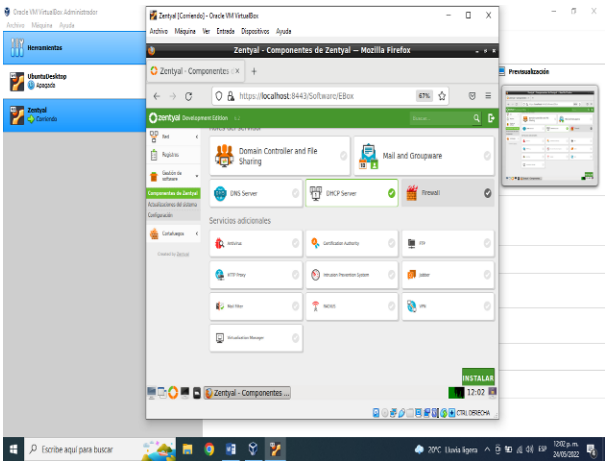

Figura 7. Instalación DHCP Server

b- Ingresamos al módulo de DHCP, este nos toma por defecto la red que configuramos estática para el servidor.

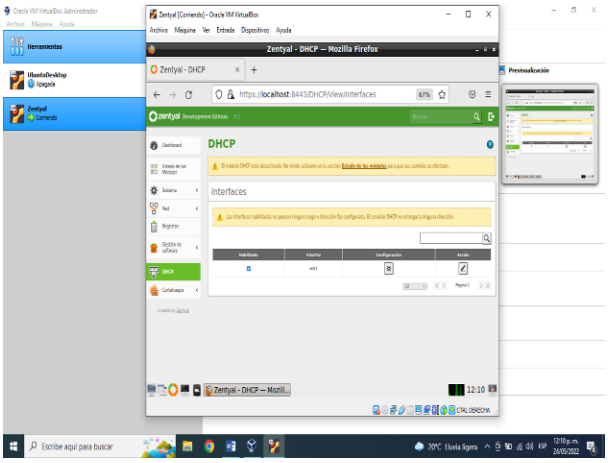

Figura 8. Red para DHCP

c- Ahora configuramos nuestro servidor DHCP y le asignamos un rango en el cual le dará automáticamente una IP para los equipos que se conecten a la red LAN.

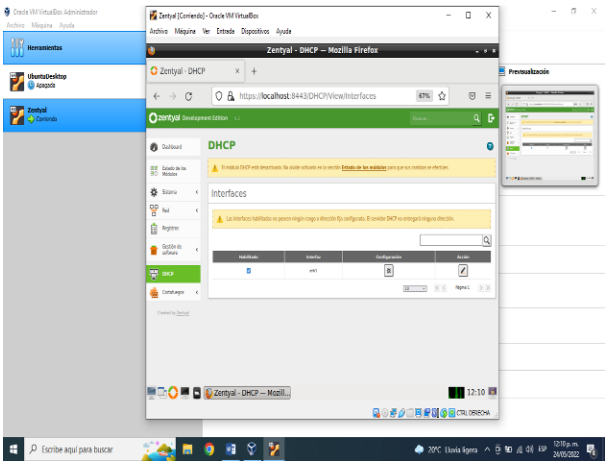

Figura 9. Rango para DHCP Server

d- Ingresamos a Ubuntu Desktop para verificar que se le asigne una IP automáticamente que se encuentre dentro del rango establecido.

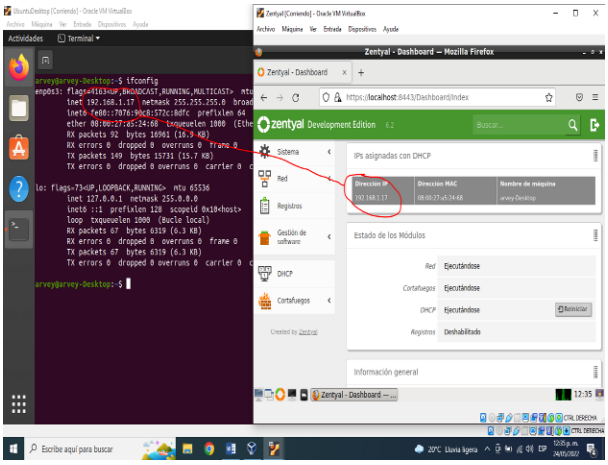

Figura 10. IP automática en Ubuntu Desktop

3.1.2 DNS SERVER

La configuración de la interfaz de red también es necesaria para la instalación y configuración del DNS Server el cual funciona en la red LAN para consultar en el dominio local registros SRV y TXT.

a- Ingresamos a la interfaz web de Zentyal en Ubuntu Desktop para instalar DNS en el módulo de gestión de software en componentes de Zentyal y allí instalamos el DNS Server.

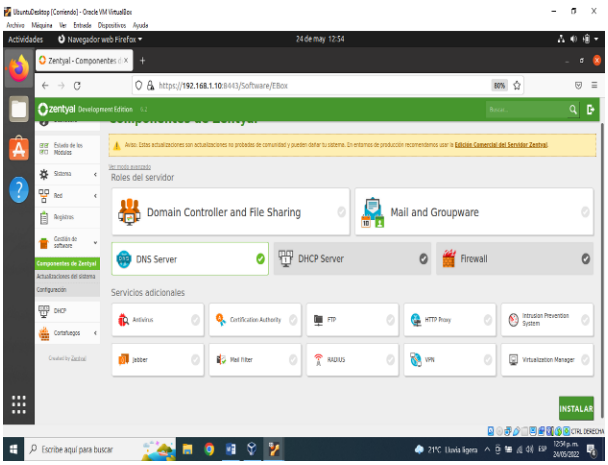

Figura 11. Instalación de DNS Server

b- Una vez instalado el DNS Server ingresamos en el módulo para configurar los dominios para la red LAN, en este mismo modulo configuramos el proxy DNS transparente para el uso obligado del servidor DNS y no tener que realizar cambios en la configuración de los clientes, configuramos el redireccionamiento a otros servidores para consultas y podemos configurar un servidor DNS autoritario.

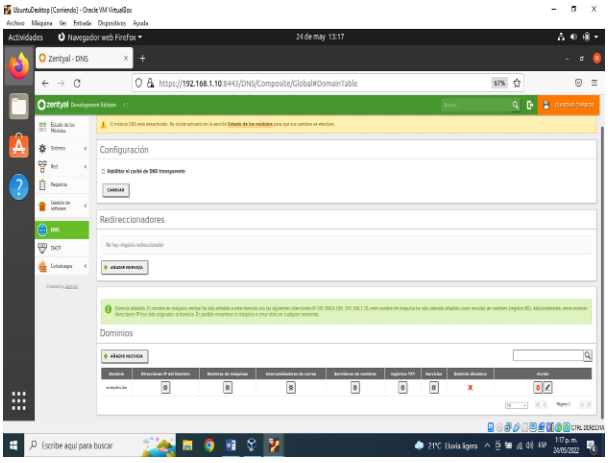

Figura 12. Configuración DNS Server

c- Ya tenemos configurado nuestro DNS Server, ahora desde el navegador de Ubuntu Desktop ingresamos a la barra de búsqueda el dominio que configuramos e ingresamos a la interfaz web de Zentyal.

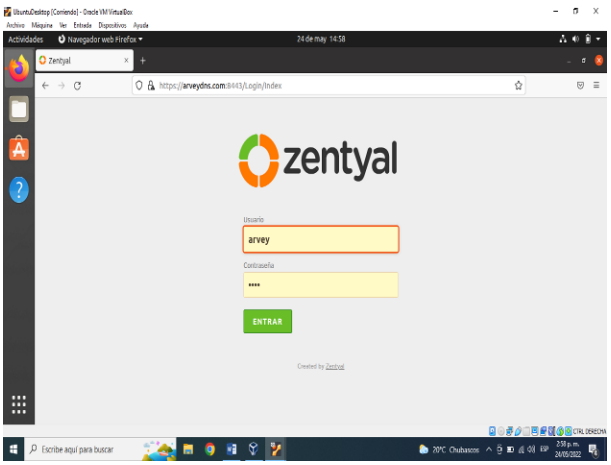

Figura 13. Ingreso a Zentyal con el Dominio Configurado

3.1.3 CONTROLADOR DE DOMINIO

Zentyal utiliza Samba4 con el que implementa el controlador de dominio y la compartición de ficheros.

a- Todas las instalaciones en Zentyal la realizamos desde el módulo de gestión de software en componentes de Zentyal, allí ubicamos el instalador de controlador de dominio.

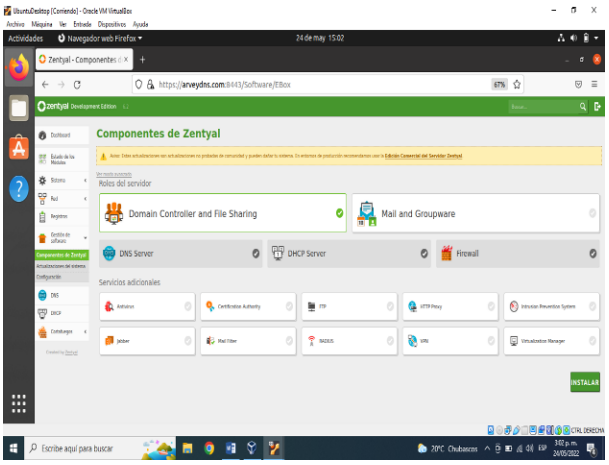

Figura 14. Instalación del Controlador de Dominio

b- En el módulo de controlador y usuarios configuramos todas las funciones para los equipos cliente.

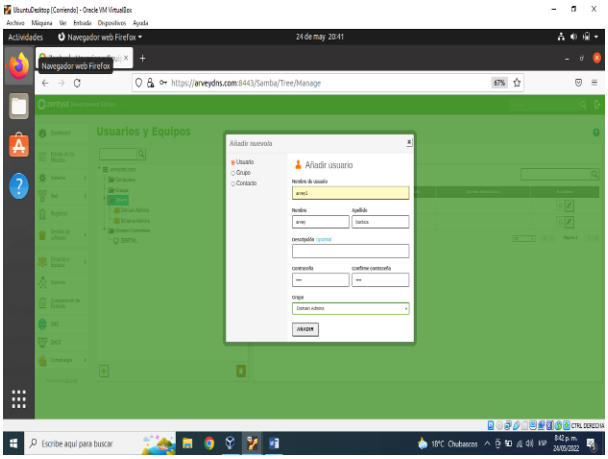

Figura 15.Configuración de Usuarios

En la instalación de los paquetes o módulos en Zentyal es necesario activarlos en la configuración del estado de los módulos para que estos funcionen.

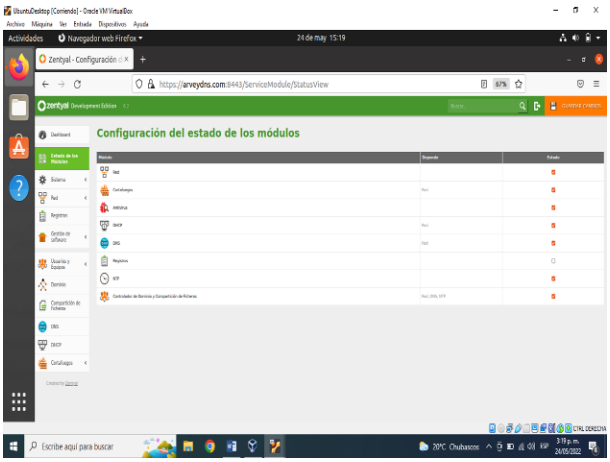

Figura 16. Configuración del Estado de los Módulos

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Para la implementación del Proxy no transparente, se debe habilitar el módulo Proxy HTTP desde la configuración del estado de los módulos.

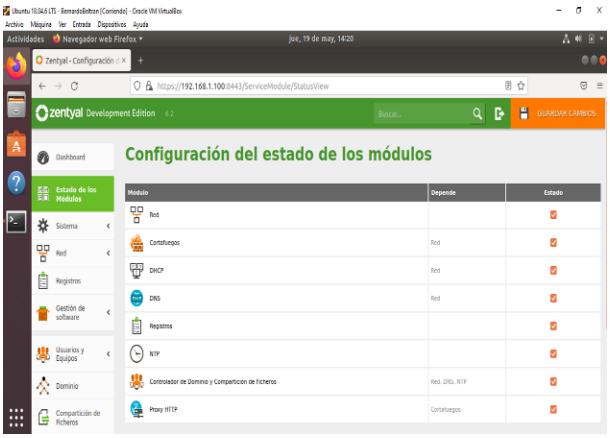

Figura 17. Habilitar módulo Proxy HTTP

Luego se debe ingresar en la configuración general del Proxy y establecer el puerto 1320.

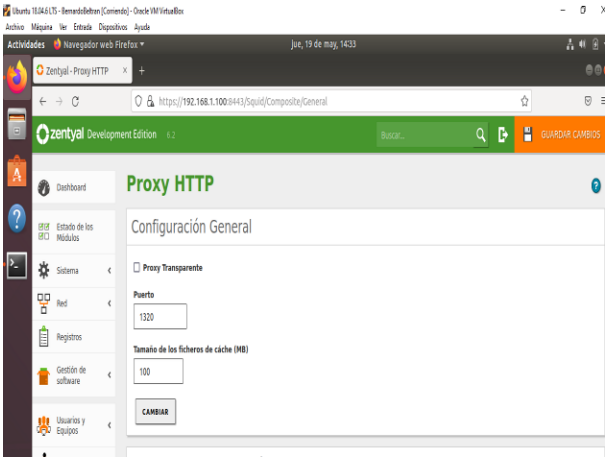

Figura 18. Cambiar la configuración general del Proxy HTTP

En este caso, se añade un nuevo perfil de filtrado llamado "Perfil entretenimiento" estableciendo el umbral de filtro en modo "Estricto".

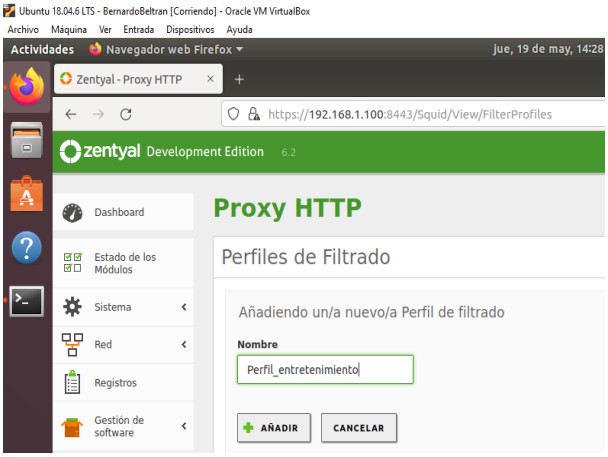

Figura 19. Cambiar perfiles de filtrado

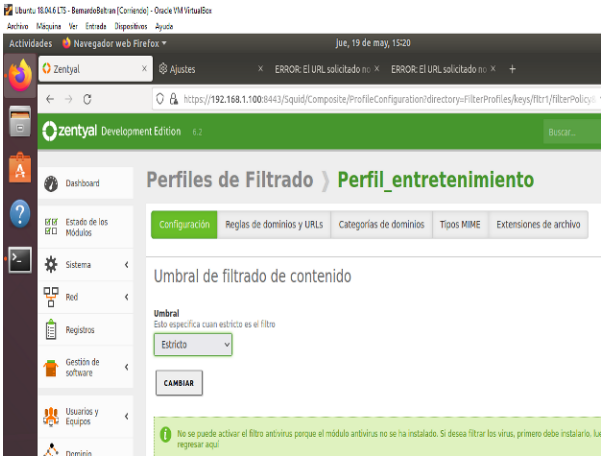

Figura 20. Cambiar umbral de filtrado

Luego de crear el perfil de filtrado, se añaden las reglas de dominio y URLs a dicho perfil, en este caso, se añadieron los dominios "tiktok.com" y "twitch.tv" estableciendo como parámetro de decisión "Denegar".

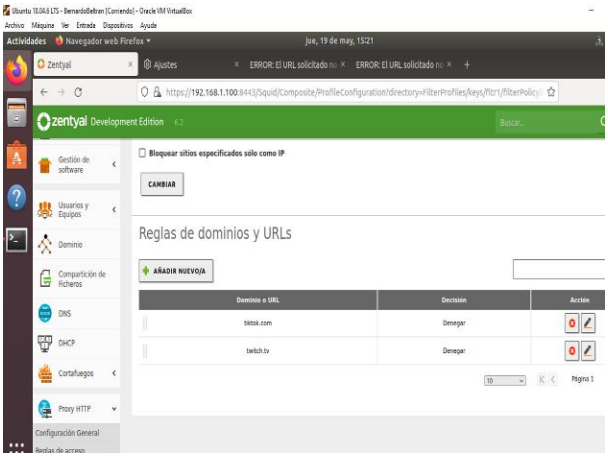

Figura 21. Añadir regla de dominios y URLs

Posteriormente, se añade una nueva regla de acceso, estableciendo que el origen sea “Cualquiera” y para la decisión aplique el perfil de filtrado creado previamente llamado “Perfil entretenimiento”.

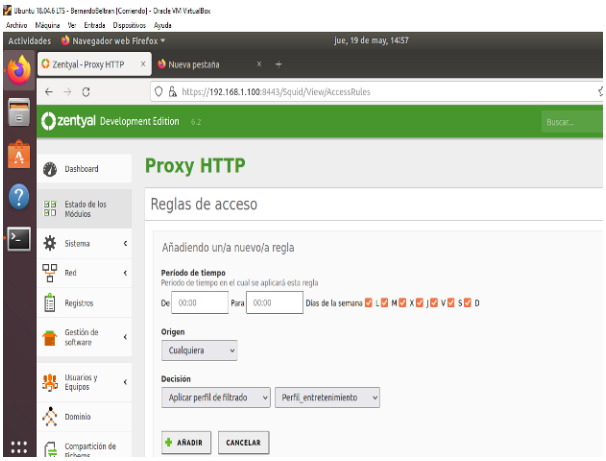

Figura 22. Crear regla de acceso

Al tratarse de un Proxy No Transparente, en el navegador del cliente se establece que el acceso a internet será por medio del proxy HTTP 192.168.1.100 y el puerto 1320.

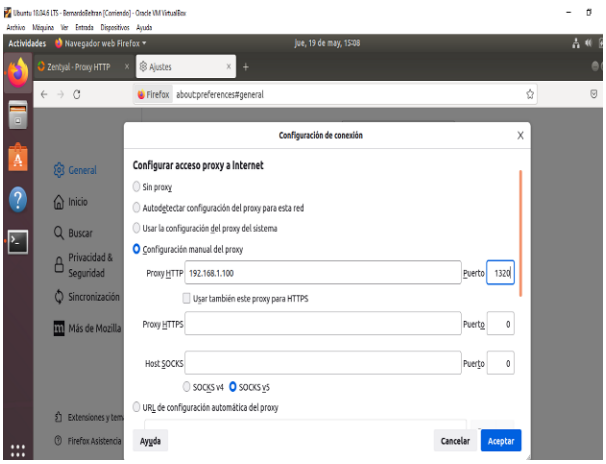

Figura 23. Configuración manual del proxy en el Cliente

Finalmente, desde el navegador del cliente se accede a los dominios añadidos al perfil de filtrado comprobando que efectivamente el Proxy deniega el acceso a estos sitios web.

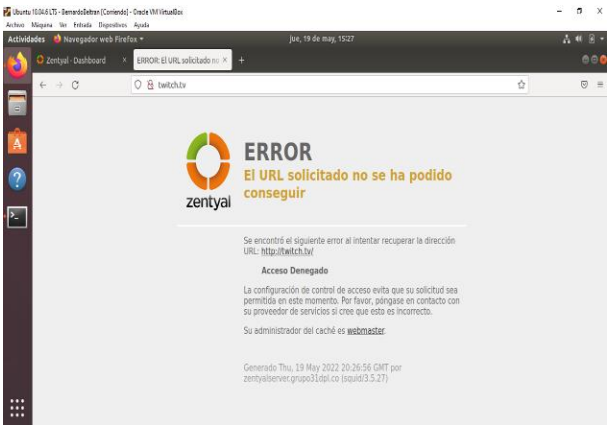

Figura 24. Acceso denegado al dominio “twitch.tv”

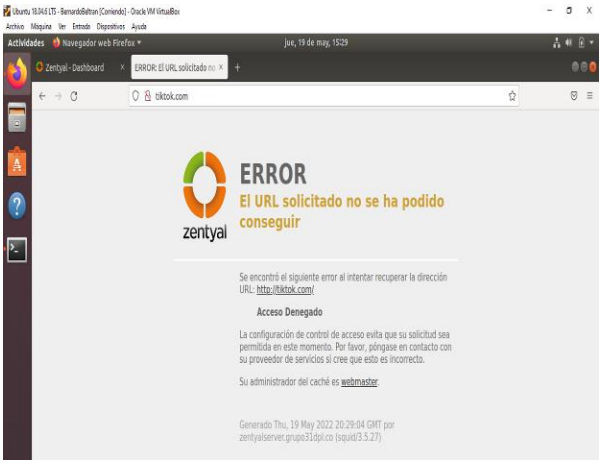

Figura 25. Acceso denegado al dominio “tiktok.com”

3.3 TEMÁTICA 3: CORTAFUEGOS

Para el desarrollo de la temática número tres vamos a evitar que los clientes de nuestro servidor puedan conectarse a la red social Facebook, luego de tener configurado nuestro Zentyal vamos al apartado de cortafuegos y luego a la parte de filtrado de paquetes, luego a las reglas de filtrado para redes internas

Figura 26. Reglas de filtrado red interna

Ahora vamos a añadir una nueva regla de filtrado en nuestro cortafuegos

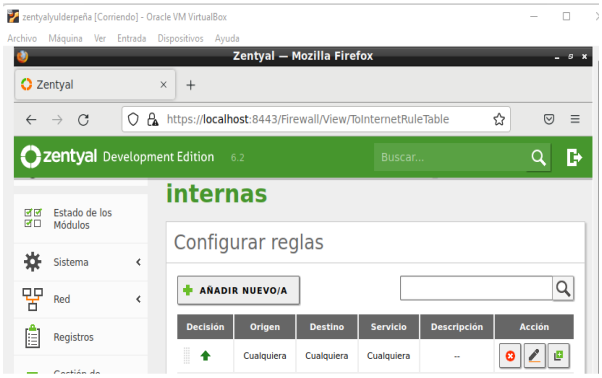

Figura 27. Crear nueva regla

Para esto debemos saber la ip de la página de Facebook desde la terminal de nuestro cliente Ubuntu hacemos ping para ver cuál es la ip en este caso (157.240.6.35)

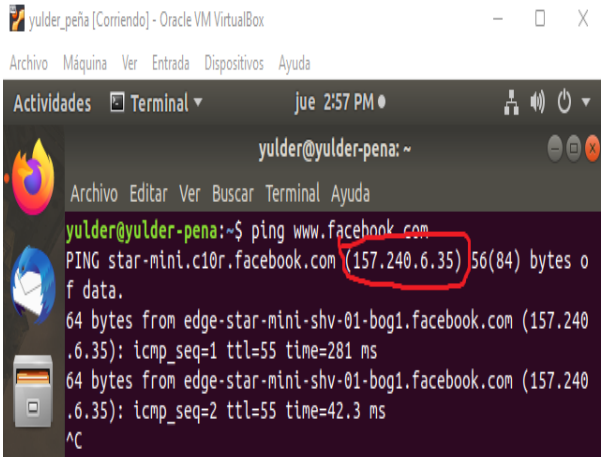

Figura 28. Obteniendo la ip de Facebook

Creamos la regla de la siguiente manera denegar el acceso, el origen ponemos cualquiera para que así los clientes que se conecten al servidor no puedan ingresar a la dirección ip de Facebook, en destino ponemos la dirección ip de la página Facebook (157.240.6.35), y en servicio ponemos en este caso 3 reglas ya que Facebook usa navegación segura vamos a bloquear el tráfico a través de tcp, además el servicio de HTTP y el servicio HTTPS

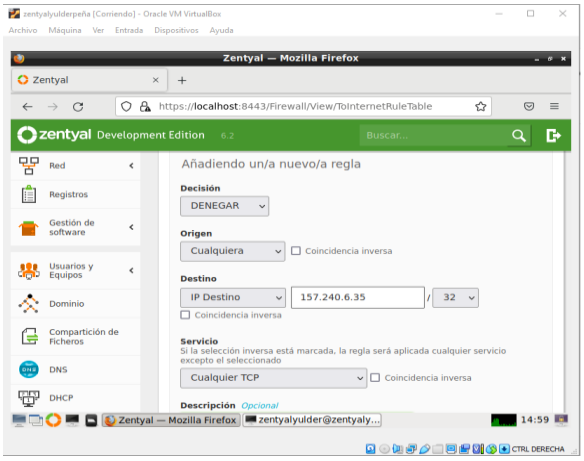

Figura 29. Creación de regla TCP

Quedando de la siguiente manera las reglas del cortafuegos luego de crearlas y configurarlas

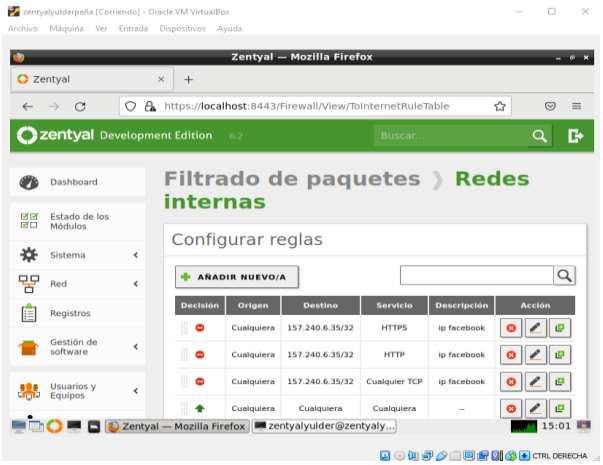

Figura 30. Reglas creadas en el cortafuegos

Volvemos a nuestro cliente Ubuntu verificamos que nuestro cortafuegos quedo bien configurado, ya que no permite la conexión a Facebook desde el cliente

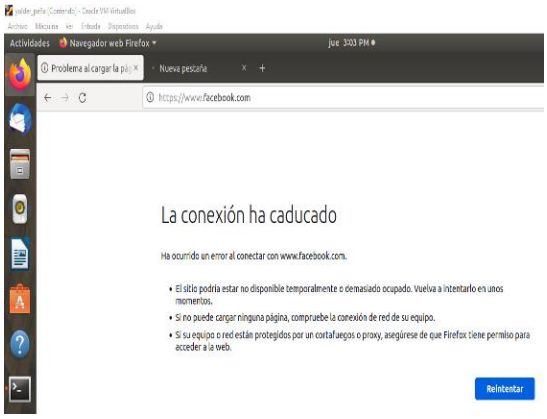

Figura 31. Conexión rechazada en cliente Ubuntu

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Para la implementación del controlador de dominio LDAP, iniciamos habilitando el cache de DNS transparente para que nuestro servidor también resuelva los nombres de dominio y tengamos mayor control sobre nuestra red local, damos clic en cambiar y guardar cambios.

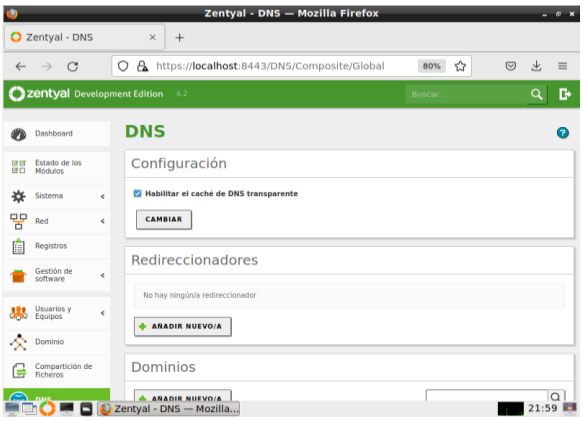

Figura 32. Habilitacion DNS Transparente

Luego vamos a dominio el cual va a estar configurado para ser un controlador de dominio y vamos a habilitar la opción de perfiles móviles lo que permitirá que un usuario se pueda identificar en la red en cualquier computadora, Damos clic en Cambiar y guardar cambios

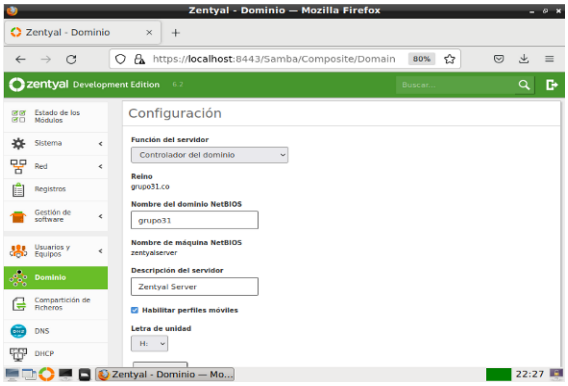

Figura 33. Activacion perfiles moviles

Nos dirigimos a usuarios y equipo, ingresamos a opciones de configuración de LDAP y habilitamos PAM, damos clic en cambiar y guardar cambios.

Figura 34.Configuracion LDAP

Posteriormente vamos a la opción gestionar en usuarios y equipos, en la opción de Usuario vamos a crear uno nuevo.

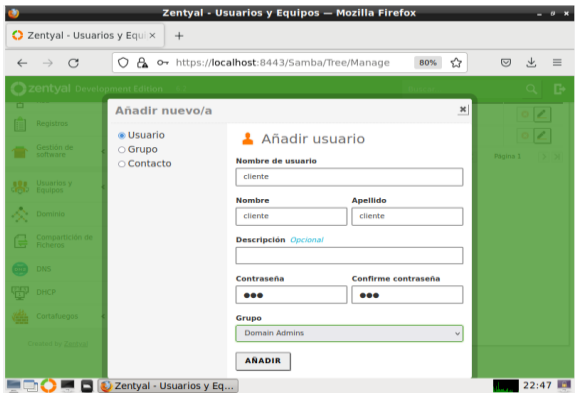

Figura 35. Creación usuarios

Vamos a el cliente en este caso a Ubuntu Desktop y en el navegador buscamos pbis download y descargamos el pbis que esta resaltado.

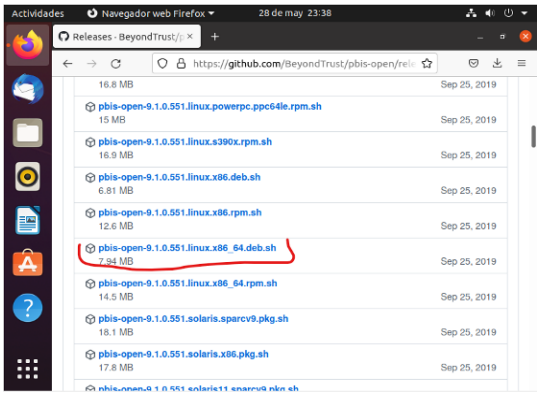

Figura 36. Descarga pbis

Luego ejecutamos los siguientes comandos “chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh” y “./pbis-open-9.1.0.551.linux.x86_64.deb.sh” para instalar los paquetes del archivo anteriormente descargado.

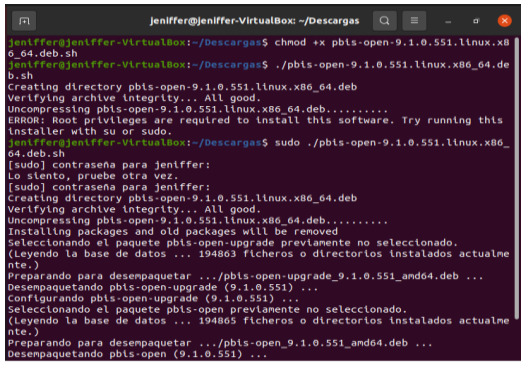

Figura 37. Isntalación pbis

Luego ejecutamos el siguiente comando /opt/pbis/bin/domainjoin-cli join --disble ssh grupo31.co cliente donde vamos a asignar nuestro dominio y el cliente que hemos creados anteriormente en Zentyal, nos pedirá contraseña y nos dirá que el sistema ha sido configurado y nos pedirá reiniciar nuestro sistema.

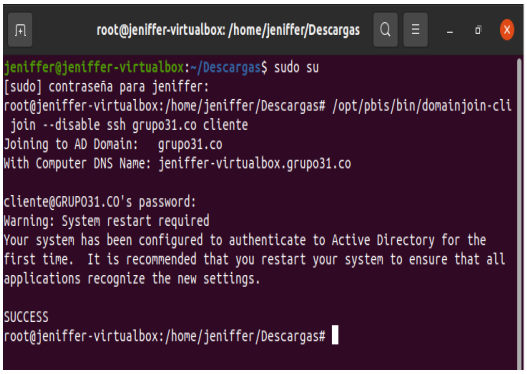

Figura 38. Asignar dominio y usuario.

Una vez reiniciado nuestro sistema podemos observar que ya nos aparece habilitado el usuario cliente que creamos en Zentyal.

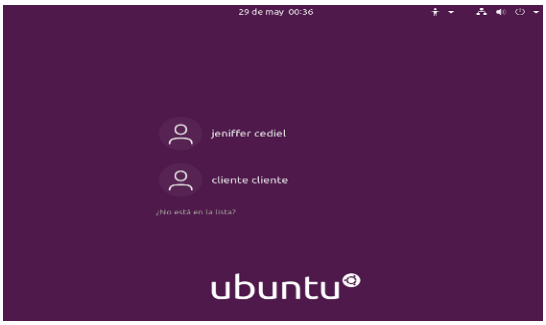

Figura 39. Comprobacion usuario creado

Iniciamos sesión y nos solicita la contraseña que asignamos, la digitamos e ingresamos.

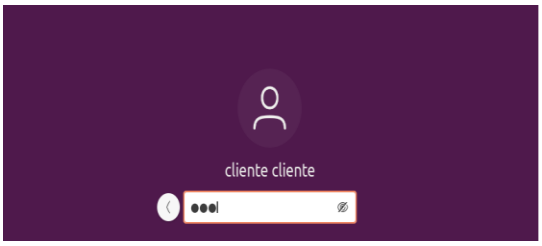

Figura 40. Inicio sesion nuevo usuario

Finalmente podemos observar que nuestro controlador de dominio LDAP esta correctamente instalando y funcionando, lo que nos permitirá el acceso a GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

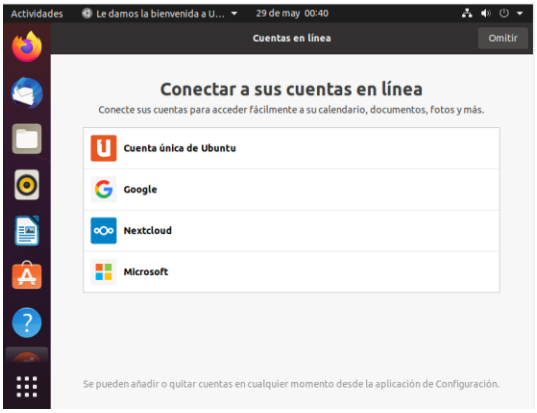

Figura 41. Controlador de Dominio en funcionamiento

3.5 TEMÁTICA 5: VPN

En la creación del servicio de redes privadas virtuales (VPN), primero se debe crear el certificado de la autoridad de certificación, en el que se debe proporcionar el nombre y se da en la opción de crear

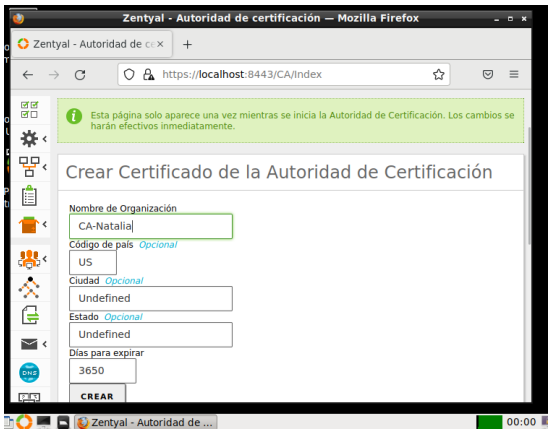

Figura 32. Certificado de la autoridad de certificación

A continuación, se debe verificar que el certificado se haya creado correctamente, en la lista de certificados se muestra resaltado el certificado recién creado

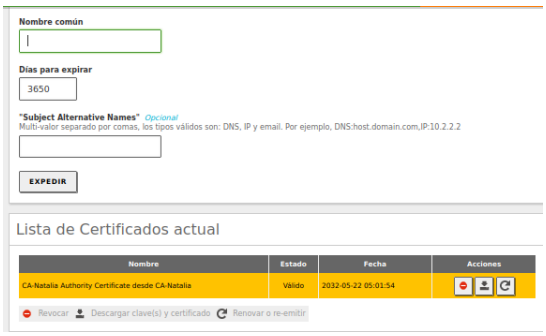

Figura 33. Lista de certificados

Se procede a guardar los cambios, y posteriormente en el módulo VPN en la opción de servidores se precede a crear el nuevo servidor, para este caso se asignó el nombre de server-natalia.vpn y se procede a guardar los cambios

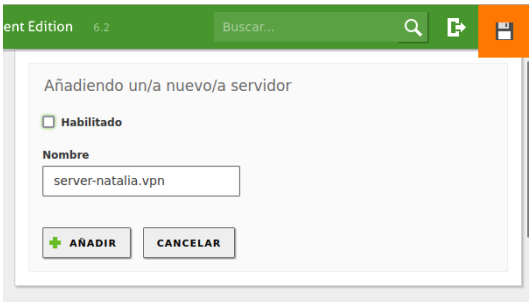

Figura 44. Creación del servidor

Una vez creado el servidor se procede a expedir un nuevo certificado en el módulo de autoridad de certificación, este es el certificado para el servidor VPN y se asignaron 664 para expedir

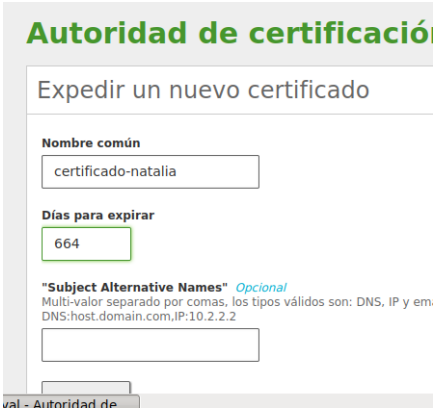

Figura 45. Autoridad de certificación

En la lista siguiente se pueden observar la lista de certificados actuales

Figura 34. Lista de certificados

Ahora, de nuevo en el módulo VPN se debe ir a la configuración del servidor se observa el puerto para la conexión será el puerto 1194 y la dirección para el VPN será de 192.168.160.0. una vez activadas las opciones necesarias se procede a activar y guardar los cambios.

Figura 35. Configuración del servidor

Enseguida se procede a configurar los servicios que van a permitir la conexión del servidor, el Firewall. Se procede a crear un nuevo servicio para la conexión VPN

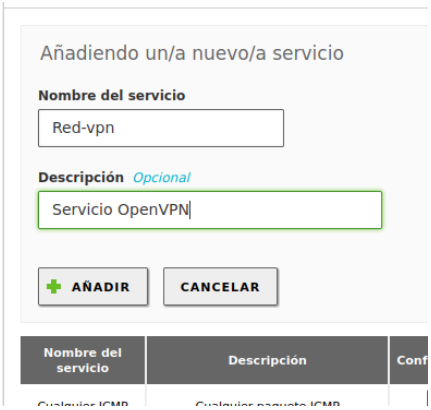

Figura 36. Nuevo servicio

Al servicio recién creado se debe configurar con el protocolo UDP y se asigna el puerto único que estaba predefinido como 1194, se aplica la configuración y se guardan los cambios

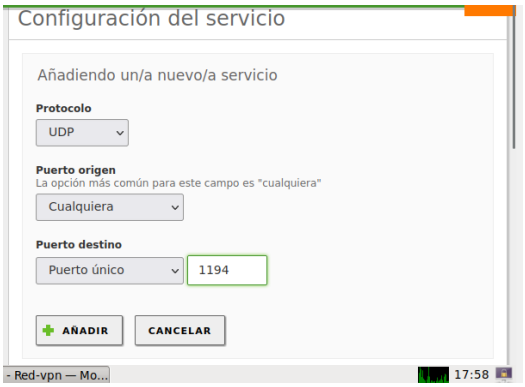

Figura 37. Configuración del servicio

Ahora, se debe ir al módulo de firewall de Zentyal, se da clic a la ficha filtrado de paquetes y luego clic a las reglas de filtrado desde las redes internas a Zentyal, aquí se presiona en configurar reglas y se añade la regla que se creó anteriormente. Se guardan los cambios.

Figura 38. Filtrado de paquetes desde las redes internas

En el módulo VPN, ficha servidores se agregan las redes que se conectaran al servidor VPN, una vez realizado esto se procede a configurar los certificados para ser descargados según el cliente, para este caso se muestra el cliente Windows y GNU/Linux Ubuntu , para cada uno se asignaron las mismas direcciones para que la dirección del servicio es 191.102.198.219 y la dirección adicional del servicio es 192.168.100.85, esta última es la dirección del servidor center y una vez se ha guardado se procede a descargar los paquetes

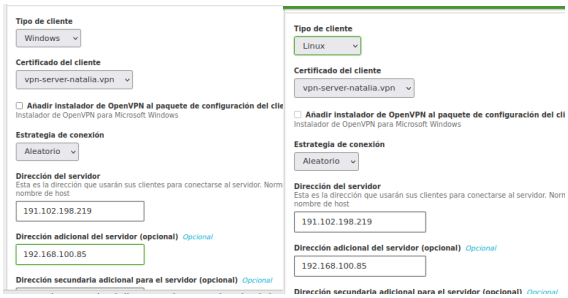

Figura 39. Clientes Windows y GNU/Linux

Se guardan los cambios, se activa el servidor y se vuelven a guardar los cambios, enseguida se procede a verificar que el servicio se encuentra activo se da clic en el dashboard de Zentyal y se logra comprobar que el servicio está habilitado y con el puerto asignado

Figura 40. Servicio VPN creado

Ahora, en el computador cliente se procede a descomprimir los certificados creados, para el ejemplo de Windows fue necesario implementar OpenVPN, se cargan los certificados y se conecta con el servicio

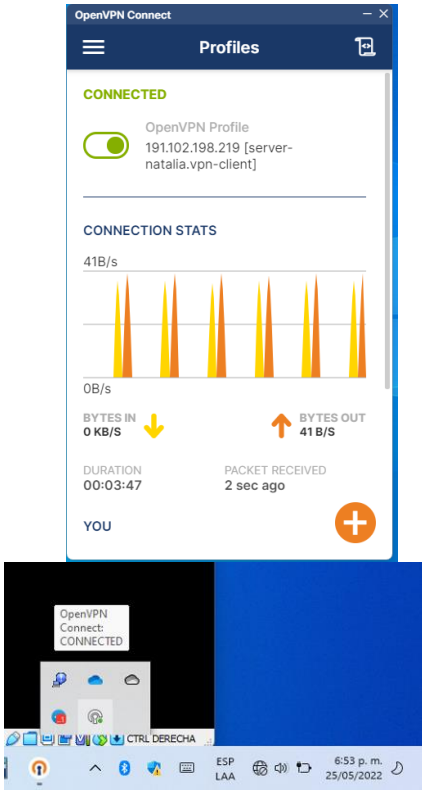

Figura 41. OpenVPN en Windows

Al igual que como pasó con el caso anterior se hizo lo mismo con GNU/Linux en el que fue necesario cargar el certificado en añadir VPN y se carga la configuración del servicio, se da clic en añadir

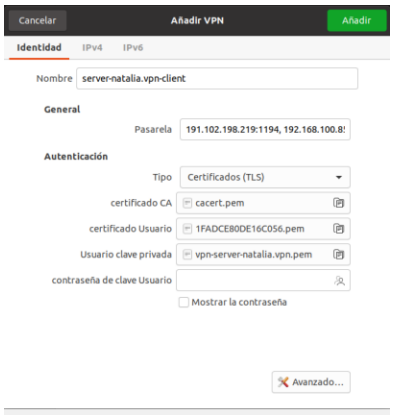

Figura 42. Configuración VPN en GNU/Linux

Una vez han pasado ciertos segundos el servicio de VPN se conecta como se puede observar en la figura siguiente

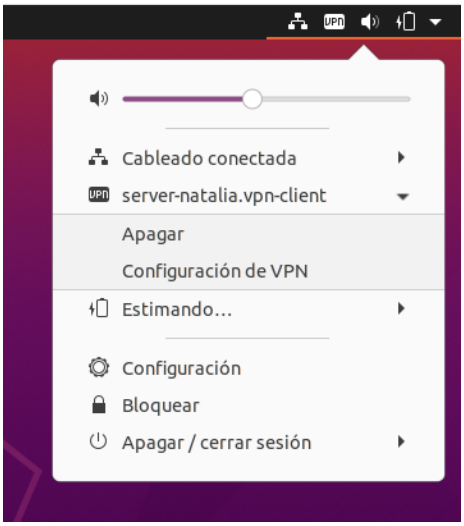

Figura 43. Servicio de VPN en GNU/Linux

3.5.1 Conclusiones.

Se implementa la configuración de un servidor DHCP, DNS y un Controlador de Dominio a través de la interfaz web del servidor Zentyal, destacando la productividad que se puede alcanzar gracias a la facilidad para implementar los servicios ofrecidos por este Servidor.

Las organizaciones requieren que sus servicios mantengan un alto grado de seguridad, en este sentido, la implementación de un servidor Proxy que actúe como intermediario entre el cliente y el servidor en conjunto con otros servicios aumenta la seguridad y permite filtrar el contenido bloqueando el tráfico entrante/saliente no deseado.

Gracias a los servicios disponibles en Zentyal Versión 6.2 se llevó a cabo la creación del servicio de redes privadas virtuales (VPN), después de implementar

el servicio se comprobó en dos estaciones de trabajo tales como MS Windows y la estación de trabajo GNU/Linux demostrando con esto que el servicio puede ser aplicado a diferentes plataformas dentro de cualquier entorno empresarial.

4 REFERENCIAS

[1] Canonical (2018). Guía del Ubuntu desktop 18.04 LTS. Help Ubuntu. https://help.ubuntu.com/18.04/ubuntu-help/index.html

[2] Guzmán Arévalo, D. (2017). OVI Unidad I_Nivelacion. [Archivo de video]. Repositorio UNAD. http://hdl.handle.net/10596/10570

[3] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

[4] Pizarro Galán, A. M. y Pizarro Galán, A. M. (2017). Linux para usuarios. Madrid, Spain: Ministerio de Educación de España. (Páginas. 16 - 130). elibro. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/49434?page=16

[5] ProngeRTV. (Enero, 2022). Cómo instalar y configurar LDAP Server Zentyal y Cliente Ubuntu 20.04 [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=T6HMrDAi0gU

[6] Zentyal *6.2 Documentación Oficial — Documentación de Zentyal 6.2*. (n.d.). Zentyal.Org. May 21, 2022. https://doc.zentyal.org/6.2/es/