CONFIGURACIÓN DE GNU/LINUX ZENTYAL 6.2 PARA SERVICIOS DE ADMINISTRACIÓN DE REDES INFORMÁTICAS

David Garzón Vélez
e-mail: dgarzonve@unadvirtual.edu.co
Cesar Alexander Cuellar Meza
e-mail: cacuellarme@unadvirtual.edu.co
Edilberto Espinosa Camacho
e-mail: eespinosaca@unadvirtual.edu.co
Nery Del Socorro Andrade Chalacán
e-mail: ndandradec@unadvirtual.edu.co
José Felipe Angulo Góngora
e-mail: jfangulog@unadvirtual.edu.co

RESUMEN: *Con la puesta en marcha de implementaciones tecnológicas, se busca dar solución a las necesidades de una organización, en la cual, se habilitan y configuran los servicios requeridos para realizar una migración completa a GNU/Linux de toda la infraestructura de la red, así como la migración de los servidores y/o servicios que se necesitan para asegurar el correcto desarrollo de sus actividades sin generar traumatismo en sus procesos, y, que a su vez, se garantice la integridad, confiabilidad y seguridad de la misma, por medio de la implementación servidores como DNS, Proxy no transparente, DHCP, Cortafuegos, VPN y File Server.*

PALABRAS CLAVE: GNU/Linux, Infraestructura de red, Servicios web, Zentyal Server, Cortafuegos.

1 INTRODUCCIÓN

A continuación, se presenta una implementación de una infraestructura de red con un sistema administración y control orientado a una implementación de servicios avanzados con el fin de ser implementados en organizaciones complejas y con altos requisitos de configuración TI. Esto, se logra a través de la instalación, configuración y puesta en marcha de herramientas de software apropiadas de acuerdo con el entorno de trabajo como lo es Zentyal Server, que permite montar una estructura TI en un ambiente real para mejorar la gestión de procesos, implementaciones tecnológicas, aumentando la seguridad en la red de un organización, evitar vulnerabilidades, ataques no deseados, y navegación por servidores específicos para los usuarios que pertenezcan a una red por medio de servidores proxy, protocolos de red, entre otros. Logrando a través de esta herramienta la configuración de servicios y servidores en red que le permiten a las organizaciones tener estructuras completas TI, organizadas y funcionales.

2 IMPLEMENTACIÓN DEL SERVIDOR ZENTYAL

2.1 INSTALACIÓN DE ZENTYAL SERVER

Zentyal Server permite unificar y administrar fácilmente todos los servicios básicos de infraestructura de red y ofrecer acceso fiable y seguro a Internet. Zentyal integra servicios como DNS/DHCP, CA, VPN, backup, Gateway, cortafuegos y proxy HTTP, por mencionar algunos. [1].

Se procede con la descarga e instalación de la distribución Zentyal Server, en su edición Development 6.2, con fines académicos, para ello, a través de la página oficial se puede realizar la descarga de su última versión, o en este caso, en la página de descargas http://download.zentyal.com/ se descarga la versión requerida como se indica en la Figura 1.

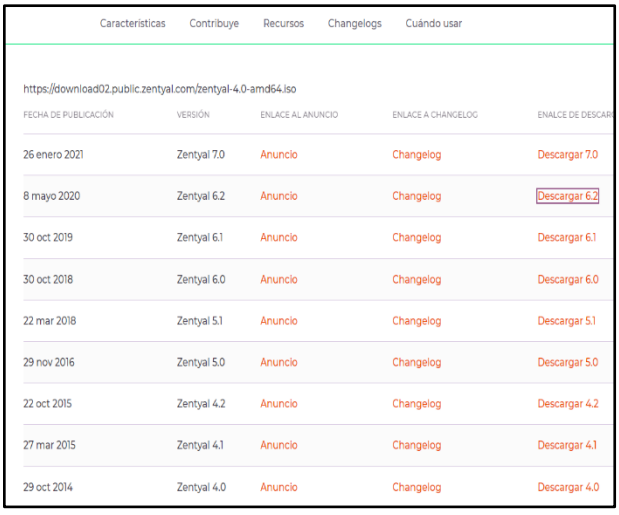

Figura 1. Descarga de Zentyal Server.

Una vez descargada la imagen, se procede a definir la máquina para la instalación, en este caso, una máquina virtual; para esta instalación es recomendado habilitar

una tarjeta de red con acceso a internet para la instalación, además de una tarjeta o más tarjetas adicionales, para la administración de zonas y redes internas.

Se crea la máquina virtual con la herramienta VirtualBox, que de acuerdo a recomendaciones de la página oficial de Zentyal, se configuran de acuerdo a los requisitos mínimos presentados en la Figura 2.

PERFIL DE ZENTYAL	USUARIOS	CPU	MEMORIA	DISCO	TARJETAS DE RED
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Figura 2. Requisitos de hardware Zentyal Server. Recuperado de https://doc.zentyal.org/6.2/es/installation.html#requisitos-de-hardware

Además, en la configuración de adaptadores de red, el primero se puede configurar como NAT, o como adaptador puente, y el segundo adaptador, en Red Interna. De acuerdo con esto, la configuración de la máquina queda funcional, ver Figura 3.

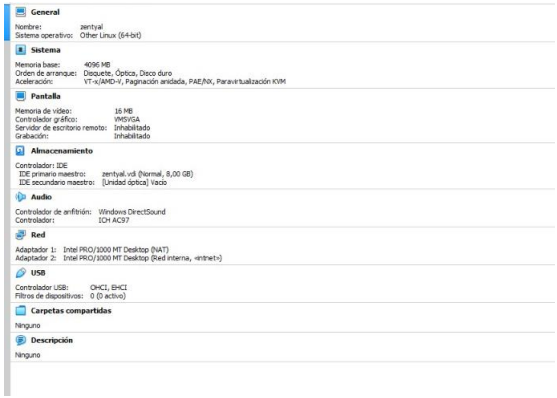

Figura 3. Configuración de máquina virtual.

Se procede ahora a ejecutar la imagen ISO descargada desde la página para iniciar la instalación sobre la máquina virtual en concordancia con la Figura 4.

Dentro de la instalación, se debe seleccionar el idioma, la distribución del teclado, los adaptadores de red, los datos de acceso del usuario y el particionado de disco.[2].

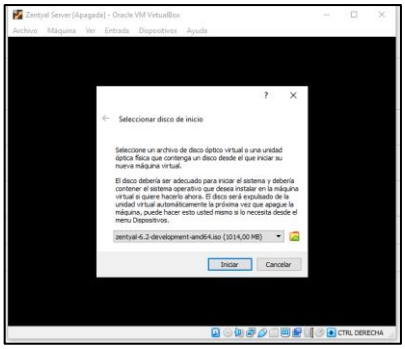

Figura 4. Ejecución y carga desde imagen ISO Zentyal Server.

Se realiza la configuración de acuerdo al asistente de instalación Zentyal como se presenta en la Figura 5.

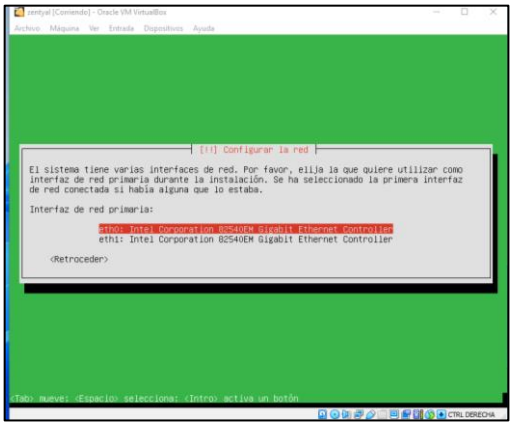

Figura 5. Selección de adaptador de red principal.

Se finaliza la instalación, obteniendo la confirmación de Zentyal de la misma forma que en la Figura 6:

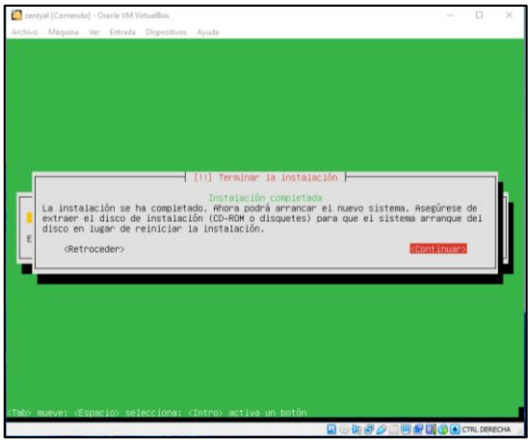

Figura 6. Finalización de instalación Zentyal Server.

Se procederá a reiniciar la máquina, confirmando su instalación a través del entorno gráfico y el acceso al panel de control de Zentyal, ver Figura 7.

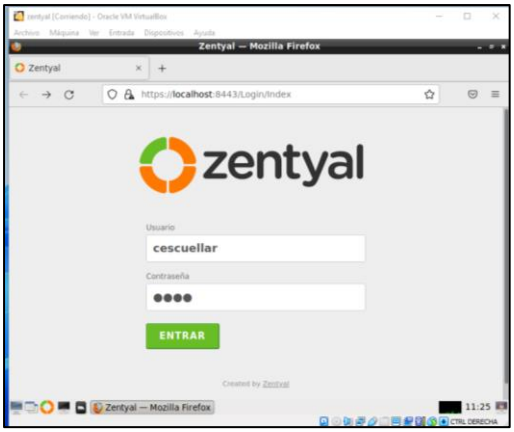

Figura 7. Acceso al panel de control Zentyal Server.

2.2 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Para esta implementación, se aprovechan las distinciones de seguridad de la distribución GNU/Linux Endian. Sobre la cual, las instalaciones de servidores que requieren acceso a internet, o que requieran ser expuestos a redes externas, se ubican en una zona desmilitarizada (DMZ); limitando su acceso a zonas internas y externas, de forma administrable desde la máquina Endian.

Tabla 1. Direccionamiento Red Endian.

	Zona Verde (LAN)	Zona Roja (WAN)	Zona Naranja (DMZ)
Red	192.168.0	192.168.1	192.168.2
Servidor	192.168.0.15	192.168.1.35	192.168.2.1

Además, para el servidor Zentyal se define la siguiente configuración:

Tabla 2. Direccionamiento Red Zentyal.

Adaptador	Tipo	Dirección IP
eth0	DMZ	192.168.2.50
eth1	LAN	192.168.0.50

Es importante configurar de forma estática las direcciones IP de las interfaces, para asegurar que no cambien durante los ajustes del equipo. Para ello, sobre las interfaces de red, se define la dirección IP para los adaptadores configurados como se ve en la Figura 8.

Figura 8. Configuración estática de IP adaptador.

2.2.1 SERVIDOR DCHP

Un servicio DCHP, es un protocolo cliente/servidor que permite brindar a los equipos conectados la asignación automática de direcciones IP, puertas de enlace y otros gateways de servicios como lo es la dirección IP de servidores DNS.

Para configurarlo, se accede desde el panel de control de Zentyal a la opción DCHP. Ahora, se presiona el botón de “configurar” en la interfaz de red que se desea configurar, como se visualiza en la Figura 9. En este caso, se indica la interfaz eth0, o la interfaz principal que se encuentre configurada en la zona DMZ. El servidor debe estar habilitado en la sección “Estado de los Módulos” de Zentyal.

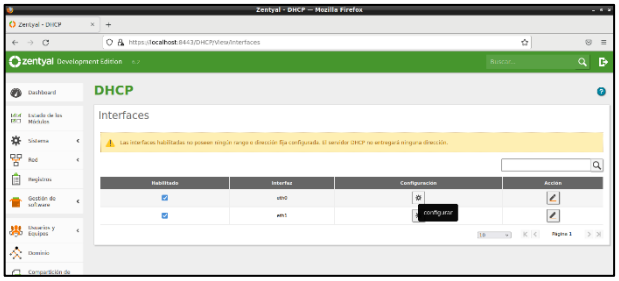

Figura 9. Configuración DCHP Zentyal Server.

Se define la configuración por defecto para la puerta de enlace, se define en este caso el dominio de búsqueda de acuerdo al configurado en Zentyal. Así mismo, se configura el NTP basado en la configuración de Zentyal y configuraciones por defecto, ver Figura 10. [3].

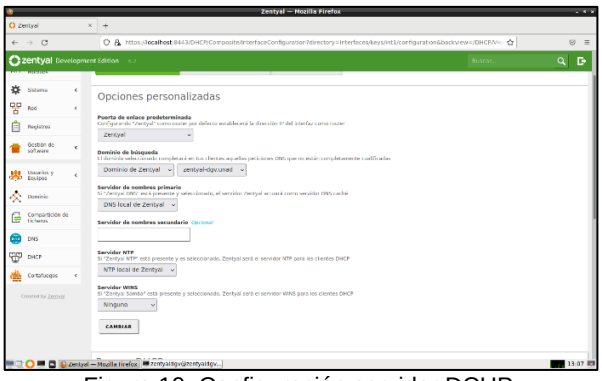

Figura 10. Configuración servidor DCHP.

En la parte inferior, se evidencian los rangos de direcciones IP disponibles para configurar, para definir el rango de direcciones que asignará el servidor DCHP, se presiona el botón “Añadir Nuevo”.

Una vez en esta opción, se indica el nombre del Rango DCHP para identificarlo, y las direcciones IP que lo comprenderán, como se visualiza en la Figura 11.

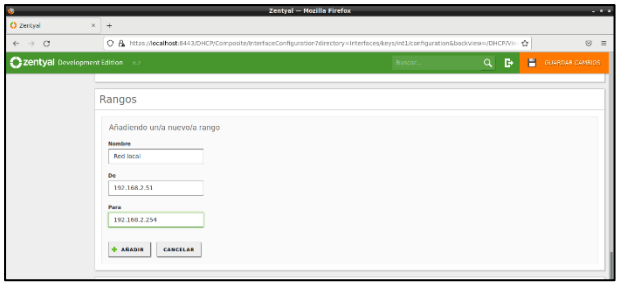

Figura 11. Adición de rangos DCHP.

Para aplicar la configuración, se presiona en la parte el botón de “Guardar cambios” y confirmar los cambios.

Si se conecta un equipo en la misma red del servidor, se puede evidenciar la asignación de la IP a través de DCHP, en los rangos configurados, comprobando desde la terminal como la Figura 12.

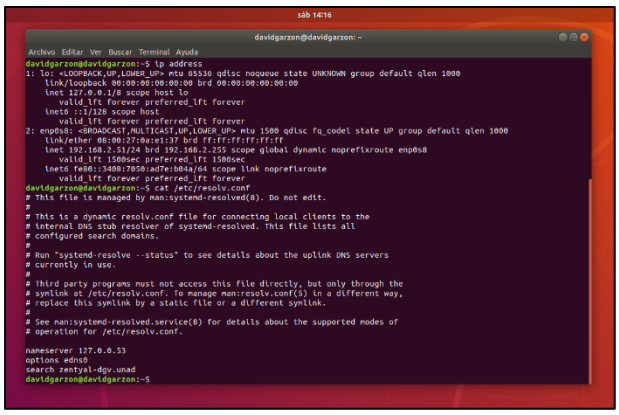

Figura 12. Verificación de asignación con DCHP.

2.2.2 SERVIDOR DNS

Dentro de Zentyal, es necesario ahora configurar un servidor de resolución dominios DNS para las redes internas, para ello, se configura un dominio autoritario dentro de Zentyal Server.

Primero, se dirige a la sección “DNS”, y sobre la sección de Redireccionadores (Figura 13), se añade uno nuevo. Los redireccionadores son direcciones DNS a las cuales el servidor va a acceder cuando no se pueda resolver un dominio dentro de sus registros locales, para ello se presiona el botón “Añadir Nuevo/a”.

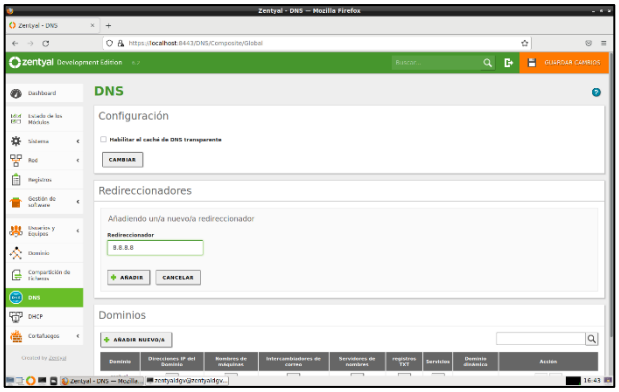

Figura 13. Configuración de redireccionador DNS.

Ahora, se va a realizar la definición de un nuevo dominio, en este caso para una máquina server con apache configurado, esta máquina cuenta con la IP: 192.168.2.52 y se identifica en red como davidgarzonserver (hostname).

Existen dos alternativas para esta configuración, se puede configurar sobre el dominio ya creado de Zentyal por defecto, o se puede definir uno nuevo, en este caso, se tomará la última opción; Para realizar la configuración, en la sección de “Dominios”, se presiona el botón de “Añadir Nuevo/a”. [4].

Se ingresa el nombre del nuevo dominio: apache-dgv.unad, y ahora, sobre el nuevo dominio, como se visualiza en la Figura 14, se procede a definir en las direcciones IP la dirección de este equipo a configurar y se registra la IP para el dominio, ver Figura 15.

Figura 14. Configuración de dominio DNS.

Figura 15. Registro de direcciones IP dominio.

En este caso, se indica el nombre de la maquina al que apunta el dominio, como en la Figura 16, para el cual se indica el nombre del host y posteriormente se le registra también su dirección IP.

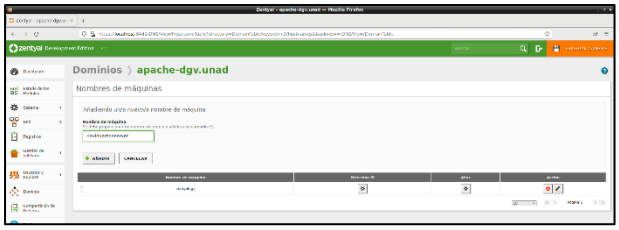

Figura 16. Registro de máquinas dominio.

Se registra el servidor de nombres basado en el dominio actual, para la máquina recién creada, ver Figura 17. Sobre esta opción se pueden crear los registros NS (Name server). Básicamente, los registros NS indican a la red a dónde ir para buscar la dirección IP de un dominio.

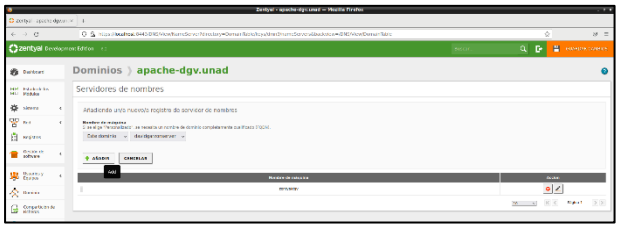

Figura 17. Registro de servidores de nombres dominio.

Se guardan los cambios realizados sobre el servidor Zentyal, y de acuerdo con esto los dominios quedan conformados de la siguiente forma:

{Nombre máquina}.{Nombre dominio}

Por ejemplo, para la máquina configurada queda de la siguiente forma: davidgarzonserver.apache-dgv.unad

Y ahora, al realizar la prueba de resolución de dominio a través de la herramienta nslookup se evidencia el resultado de la configuración, indicando que el dominio se encuentra asociado a la dirección IP respectiva, ver Figura 18.

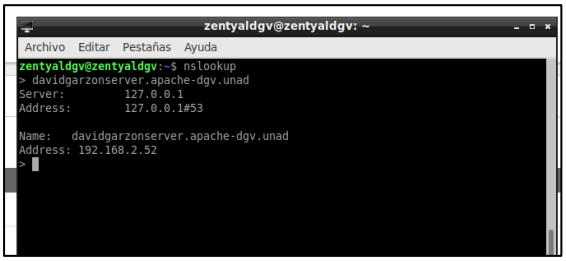

Figura 18. Comprobación de resolución de nombres de dominio.

2.2.3 CONTROLADOR DE DOMINIO

A través de Zentyal, se permite configurar un controlador de dominios para sistemas Windows, generando un enlace entre el servidor Linux como server base, y permitiendo generar conexiones de host de Windows, a través de los servicios de autenticación que habilita este controlador. [5].

Ref. [6], Cabe recordar que los controladores de dominio son servidores de Windows que contienen la base de datos de Active Directory y ejecutan funciones relacionadas con AD.

Se define que el dominio de la maquina Zentyal configurada es **zentyal-dgv.unad**, el cual puede ser visualizado desde la sección “Sistema > General”.

Ahora, para realizar la configuración de Zentyal como controlador único de dominio, se ingresa a la sección “Dominio”, ver Figura 19.

Sobre esta interfaz, se puede evidenciar el tipo de servidor configurado, el reino del dominio, y el nombre que identifica la máquina. Así mismo, se evidencia una unidad asignada para su gestión dentro de equipos Windows.

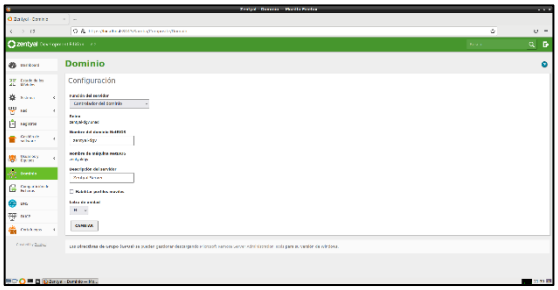

Figura 19. Configurador de Zentyal como controlador de dominio.

Ahora, para poner en marcha su funcionalidad, se deben definir los usuarios que tendrán acceso a dicha gestión, para ello, se dirige a la sección “Usuarios y Equipos”, donde se podrán controlar los usuarios del servidor, ver Figura 20.

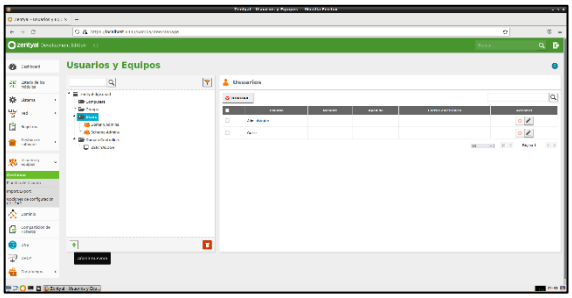

Figura 20. Gestión de usuarios Zentyal.

Se ingresa ahora la información de un usuario administrador del controlador de dominios, y se añade al grupo, de acuerdo con la Figura 21, se ingresa la información:

- Usuario: adminzentyal
- Contraseña: 123456

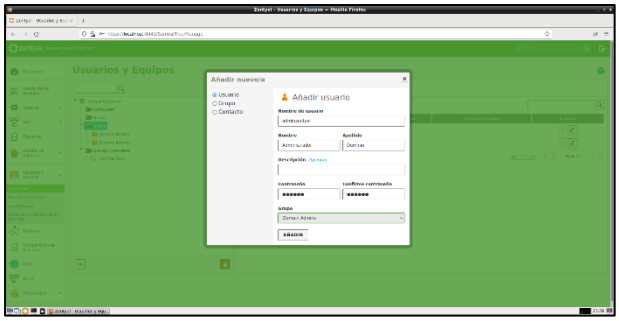

Figura 21. Creación de usuario administrador en Zentyal.

Se procede a crear ahora un usuario normal, el cual tendría un funcionamiento básico y general del controlador de dominios y directorios activos.

Se ingresan los datos de este nuevo usuario, en este caso y se verifica la información, ver Figura 22:

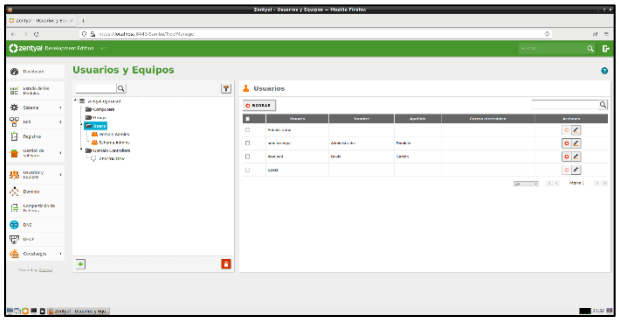

Figura 22. Listado de usuarios en Zentyal.

Para validar ahora la correcta configuración, sobre un equipo Windows, con acceso al servidor, se procede a probar el controlador de dominios. Para ello, sobre la configuración del sistema, Cambiar configuración de dominio, se ingresa el dominio del servidor, y los datos del administrador, como en la Figura 23.

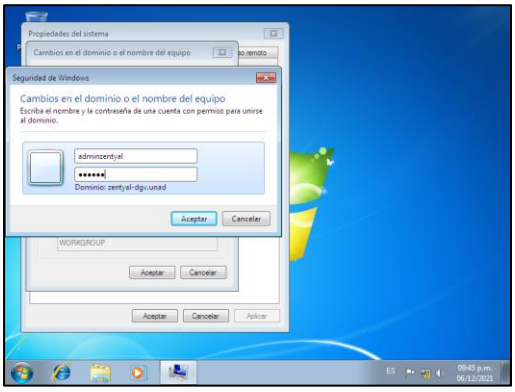

Figura 23. Configuración de dominio en Windows.

Se reinicia el equipo Windows, y ahora, se inicia sesión con el usuario creado, y se tiene acceso a los recursos, ver Figura 24.

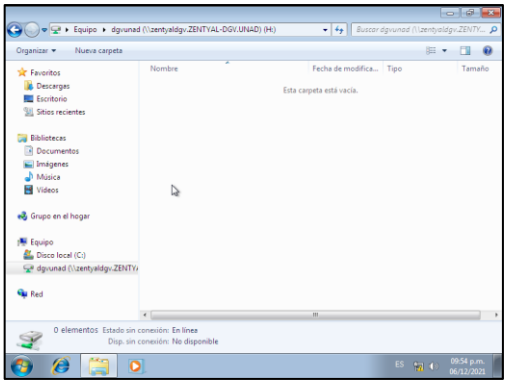
Figura 24. Acceso a recursos de dominio en Windows.

Para mejorar la seguridad de las implementaciones, se puede configurar el Cortafuegos del servidor, para ello, en estado de los módulos se habilita el cortafuegos. Ahora, sobre la sección de “Reglas de filtrado desde las redes internas a Zentyal”, se puede configurar el acceso que tienen los equipos en red a los servicios de Zentyal, y se configura a través del botón “Configurar Reglas”.

Sobre esta interfaz, se definen las reglas de denegación para todos los protocolos, y se habilitan en este caso, los servicios de las configuraciones anteriores; Es muy importante el orden, ya que primero deben estar las habilitaciones y al final las restricciones, ya que de esta forma el servidor validará el servicio accedido, y si no corresponde, bloqueará el acceso, ver Figura 25.

Figura 25. Configuración de cortafuegos para servidores en Zentyal.

2.3 PROXY NO TRANSPARENTE

Se realiza la instalación del módulo de red para poder configurarla y que los clientes puedan conectarse a internet por medio del servidor. Para ellos damos clic en “Gestión de software > Componentes de Zentyal” y seleccionamos Network Configuration. Además, se realiza también la instalación del módulo HTTP Proxy, ver Figura 26:

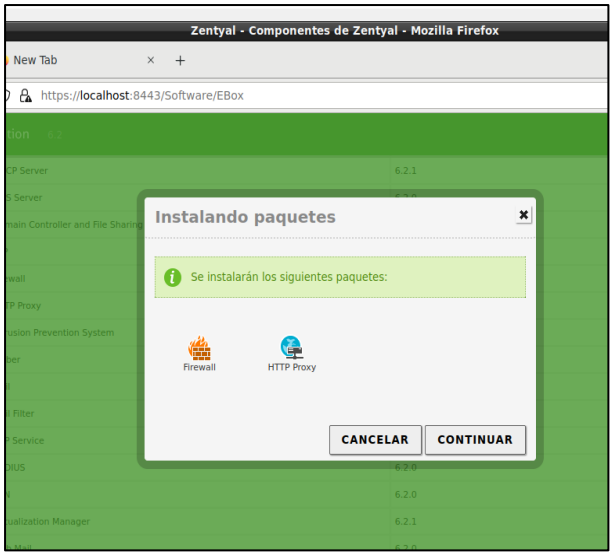

Figura 26. Instalación del Módulo HTTP Proxy

Configuramos nuestra interfaz 1 (eth0) y le asignamos DHCP, posteriormente habilitamos el módulo DHCP que se instaló en el paso anterior este nos notificara que hace falta al menos una interfaz estática, así que procederemos a apagar la maquina y habilitar el adaptador de red 2 (eth01).

Luego de volver a encender la máquina, ingresamos a la interfaz web de Zentyal y verificamos que en el apartado de red aparezcan las dos interfaces (eth0, eth1). Procedemos a configurar el adaptador eth1 con una dirección IP estática, esta será la que les asigne direcciones IP por DHCP a los equipos clientes.

Ahora agregaremos el rango desde donde iniciara a distribuir las IP, para ellos damos clic en el panel lateral izquierdo en “DHCP”, seleccionamos el icono de “Configuración” y damos en “Añadir Nuevo” agregamos el rango y damos clic en “Guardar Cambios”, se verifica ahora en el cliente la asignación de direcciones IP, de acuerdo con la Figura 27.

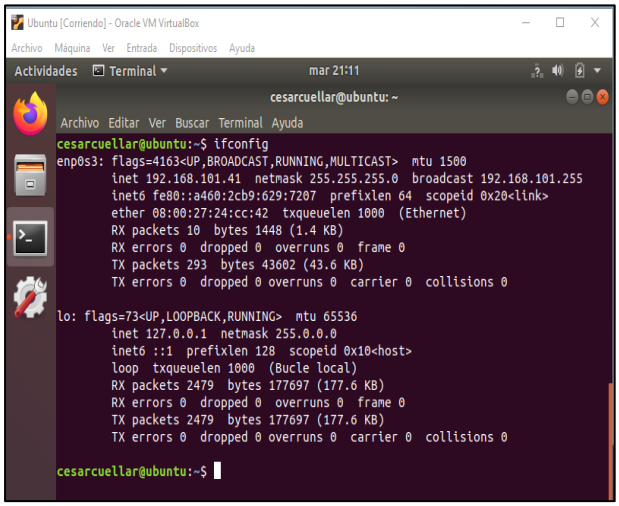

Figura 27. Verificando IP asignada por DCHP al cliente.

Se identifica que tiene la IP 192.168.101.41, lo que indica que todo está funcionando correctamente, ahora se procede a configurar el Proxy HTTP no transparente, para ellos se dirige nuevamente a Zentyal y se hace clic en el panel lateral izquierda en “Proxy HTTP” y activamos el servicio para poder usarlo a través de la sección de “Estado de los Módulos”, ver Figura 28.

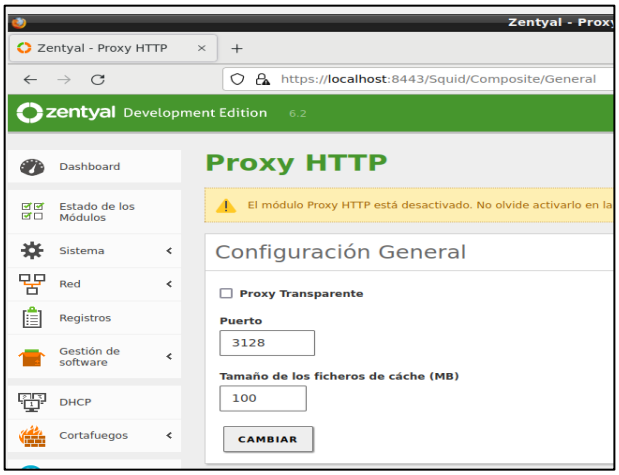

Figura 28. Activando el Módulo HTTP Proxy

Una vez el servicio esté activo, se procede a crear un perfil de filtrado, en la configuración general de Proxy HTTP, se cambia el puerto por defecto a 1230. La casilla de verificación “Proxy transparente” hay que dejarla desmarcada para que el proxy sea “No transparente”, ver Figura 29. [7].

Figura 29. Cambiando puerto a HTTP Proxy

Luego de cambiar el puerto, se procede a crear el perfil de filtrado, dando clic en el panel lateral izquierdo en “Perfil de filtrado”, se le asigna un nombre y se guardan los cambios, ver Figura 30.

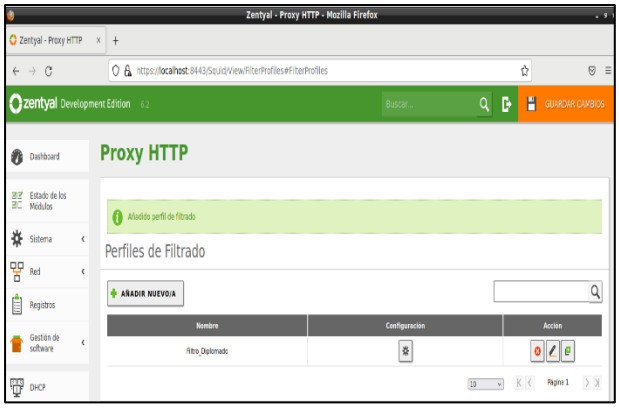

Figura 30. Creando Perfil de Filtrado HTTP Proxy.

Ahora se da clic el icono de Engranaje (Configuración) y se cambia el umbral a “Muy estricto”, como se evidencia en la Figura 31, luego en el panel superior se debe dirigir a “Reglas de dominios y URLs, se activa la opción de “Boquear dominios y URLs no listados”, y en la parte inferior se agregan los sitios web que se desean bloquear con la decisión de “Denegar”, en este caso serán Facebook, YouTube y Twitter, se guardan los cambios, ver Figura 32.

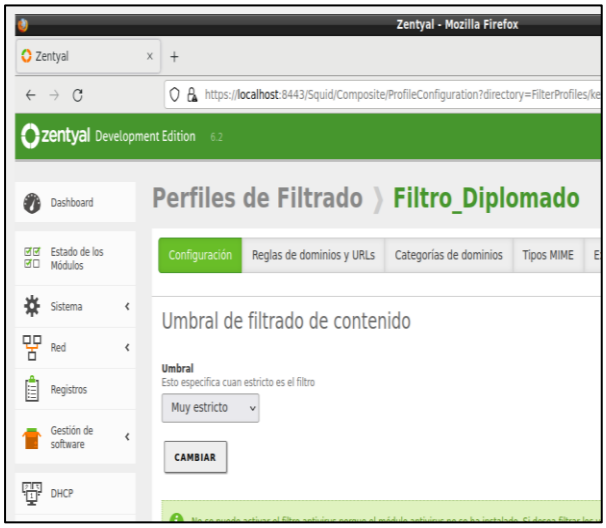

Figura 31. Umbral de filtrado de contenido de Red.

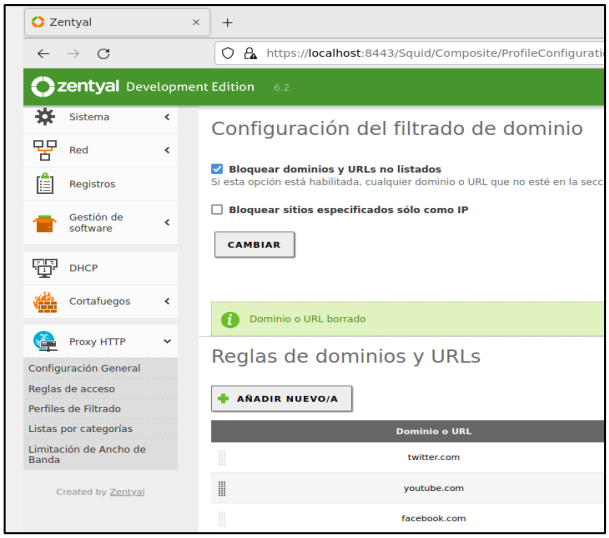

Figura 32. Bloqueando Dominios de Red.

Ahora se debe dirigir en el apartado lateral izquierdo a la opción “Reglas de acceso” y cargando el perfil de filtrado que se acaba de crear. Si se desea agregar un tiempo determinado para que el Proxy entre en funcionamiento, se establece en "Periodo de tiempo". En la opción de Origen se selecciona "Cualquiera", en Decisión se selecciona "Aplicar perfil de filtrado" y en el recuadro de al lado se selecciona el perfil de filtrado configurado y damos clic en Añadir, como en la Figura 33, y se guardan los cambios.

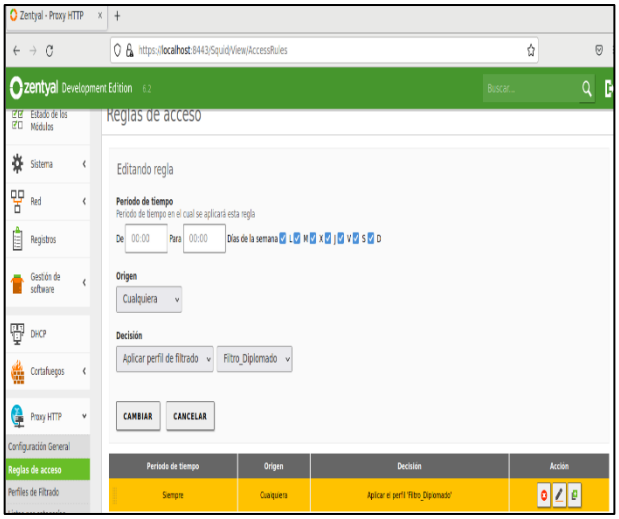

Figura 33. Cargando Perfil de Filtrado.

Finalizada la configuración, al tratarse de un Proxy No Transparente, a las maquinas clientes se les debe especificar el proxy y el puerto, desde el cliente, se abre el navegador y en las configuraciones del propio navegador se escribe el proxy y el puerto de forma manual, como se evidencia en la Figura 34. Luego al intentar ingresar a las páginas web que se han bloqueado, se verifica que el bloqueo por HTTP Proxy funciona correctamente, ver Figura y 35.

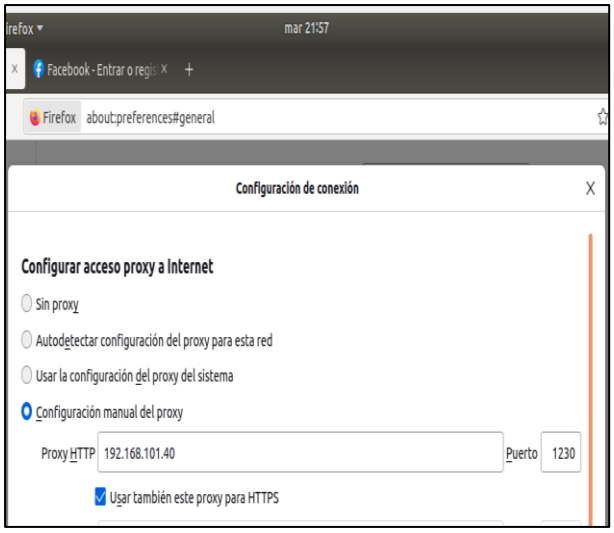

Figura 34. Agregando Proxy en Maquina Cliente.

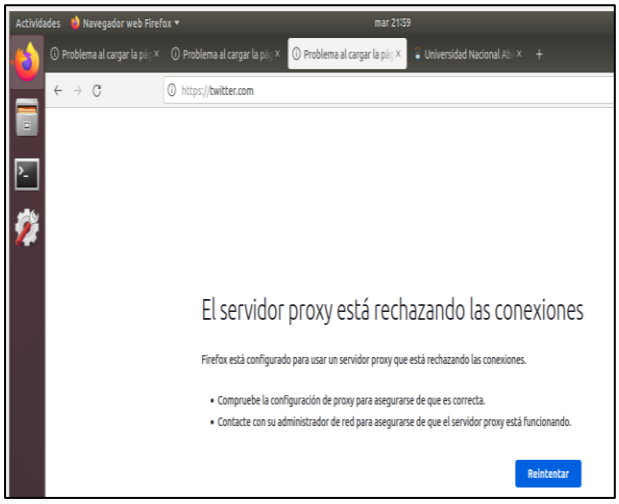

Figura 35. HTTP Proxy Funcionando Correctamente.

Se abre ahora una página web alterna para comprobar que en otros sitios web se puede navegar, ver Figura 36.

Figura 36. Verificación de acceso a sitio con Proxy.

2.4 CORTAFUEGOS

Zentyal server, cuenta con un módulo que permite administrar la seguridad de la red al brindar la posibilidad de configurar un cortafuegos o Firewall, el cual actúa como intermediario entre la red o redes internas e internet. Desde este componente es posible administrar de manera visual los filtros de navegación y permisos de la red, configurando una serie de reglas que permiten o deniegan el acceso de servicios internos y externos.

Para configurar el cortafuego, es necesario que la interfaz de red que se conecta con el Router y da acceso a la WAN, se marque como conexión externa en el módulo RED del panel de control de Zentyal como se muestra en la Figura 37.

Figura 37. Configuración estática de la interfaz de red marcada como externa (WAN).

Para acceder a la configuración del cortafuegos se ingresa al módulo Cortafuegos > Filtrado de Paquetes, ver Figura 38.

Figura 38. Secciones del firewall, dependiendo del flujo de tráfico.

Cada una de las secciones que se muestran en la interfaz del cortafuego, controla diferentes flujos de tráfico dependiendo del origen y destino:

- **Reglas de filtrado de redes internas a Zentyal**, Permite o deniega el acceso a los servicios del servidor Zentyal a los equipos de la red interna.
- **Reglas de filtrado para las redes internas** permite controlar el acceso a internet de las redes internas.
- **Reglas de filtrado desde las redes externas a Zentyal** permite el acceso al servidor Zentyal desde redes externas (No recomendado por poner en riesgo la seguridad de la red)
- **Reglas de filtrado para el tráfico saliente de Zentyal**. Controla el acceso al servidor Zentyal a servicios externos a la red.

Para explicar un poco más a fondo el funcionamiento del cortafuego, se realiza la configuración para restringir la apertura de sitios o portales Web de entretenimiento y redes sociales.

Para este fin se inicia identificando cuales son los sitios a los cuales se les restringe el acceso, para este caso se utilizó la sentencia PING a cada una de las páginas para conocer su dirección IP, ver Figura 39; se obtiene el mismo resultado con la sentencia nslookup.

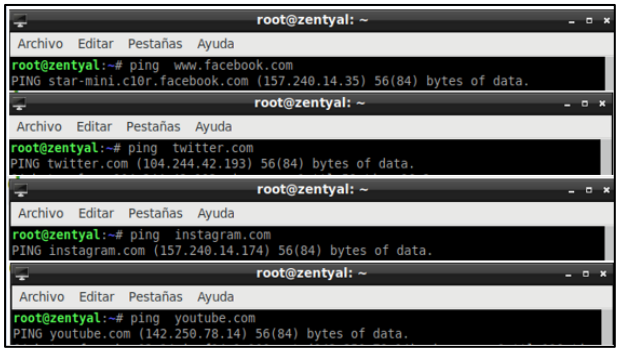

Figura 39. Identificando Dirección IP de páginas a bloquear desde el Firewall

Una vez identificados los sitios a los cuales se les denegará el acceso desde el servidor Zentyal, se procede a crear un objeto desde el módulo de red.

Los objetos en Zentyal permiten el agrupamiento de direcciones IP, o rango de direcciones, lo cual agiliza la configuración y administración de los servicios de Zentyal.

Se crea el objeto de nombre Block_Win desde la ruta Red > Objetos, como se muestra en la Figura 40 y 41.

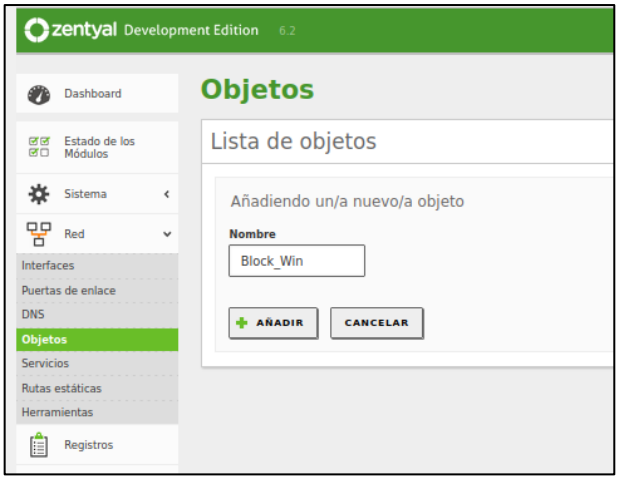

Figura 40. Creando el objeto que contendrá las direcciones IP identificadas

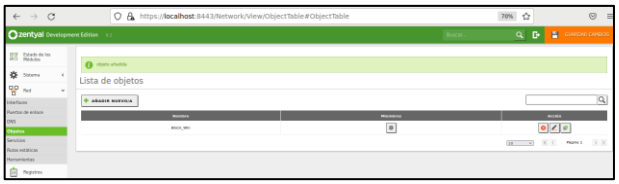

Figura 41. Se muestra el objeto creado y la posibilidad de modificarlo o administrarlo

Al ingresar a la configuración del objeto se ingresa una dirección IP o un rango de direcciones IP. Para el ejercicio se agregan las direcciones de las redes salicales identificadas, ver Figura 42.

Figura 42. Agregando IP de Facebook

Una vez agregados en el objeto todas las direcciones que se desea bloquear desde las reglas de firewall, estas se muestran listadas en el objeto como se muestra en la Figura 43.

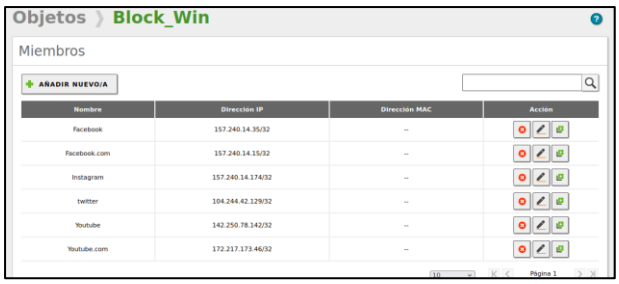

Figura 43. Se muestran las direcciones agrupadas en el objeto llamado Block_Win

Ahora, es necesario hacer clic en el botón Guardar que se habilita en la parte superior derecha para ver reflejados los cambios. A continuación, se muestra la capacidad que tiene la máquina para acceder a redes sociales momentos antes de realizar la configuración del cortafuegos, ver Figura 44.

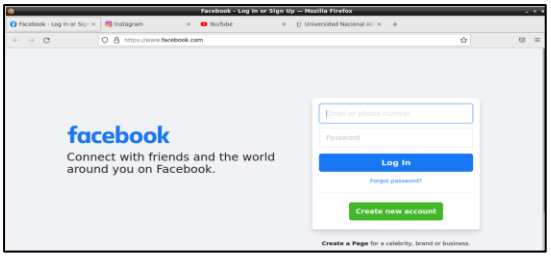

Figura 44. La máquina puede acceder a la red social Facebook

Se inicia con la configuración de las reglas que restringirá el acceso a las redes sociales identificadas. Para este fin se accede a Cortafuegos > Filtrado de Paquetes, en esta ocasión accederemos a la configuración de las redes internas, se muestra pantalla con la sesión de la regla donde se indicará si se desea Aceptar o Denegar, para este caso denegaremos al acceso.

Indicamos que el origen es cualquier equipo de la red y como destino seleccionamos el objeto creado en pasos anteriores, indicando de esta forma que todos los paquetes dirigidos a alguna de las direcciones IP agregadas en el objeto serán denegadas por el cortafuego de Zentyal, ver Figura 45.

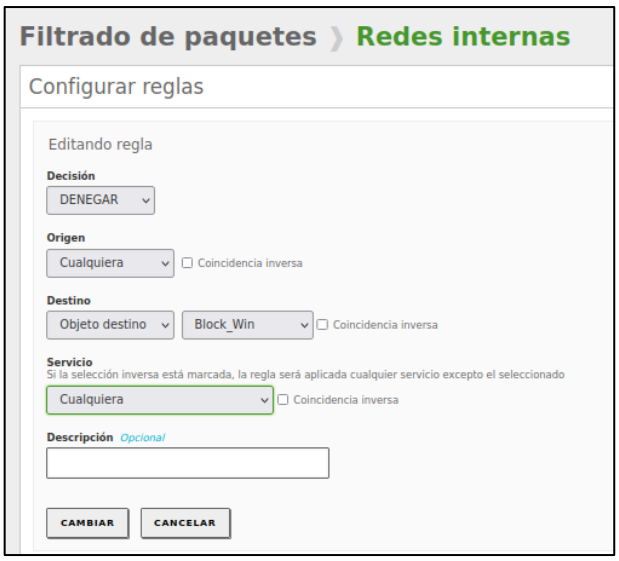

Figura 45. Configuración de la regla que deniega el acceso a redes sociales identificadas.

Una vez guardada la configuración es necesario reiniciar los adaptadores de red para que los cambios sean asimilados por el Zentyal y borrar el cache del navegador, ya que los navegadores cuentan con la capacidad de acceder a sitios guardados de manera local dando la sensación de que la configuración no surgió efecto. Luego, se podrá ver su resultado como la Figura 46.

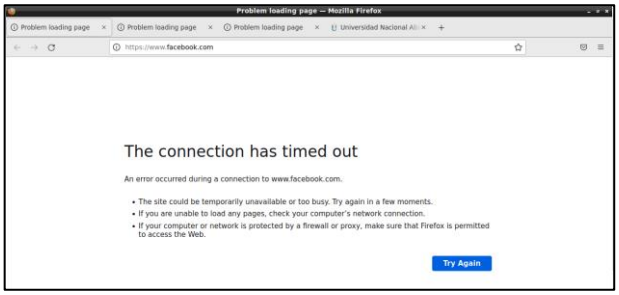

Figura 46. Página que muestra la imposibilidad de la máquina para acceder a facebook.com

En el mismo navegador se muestra que las páginas que no se encuentran en la regla creada pueden navegar de manera correcta, ver Figura 47.

Figura 47. Página que se encuentra fuera de la excepción navega sin problemas

2.5 FILE SERVER Y PRINT SERVER

Desde el menú Usuarios y Equipos > Configurar modo podemos comprobar cuál es el modo de funcionamiento de nuestro servidor LDAP antes de activar el módulo. Si hemos activado el módulo de Usuarios, Equipos y Ficheros, nuestro servidor funcionará como Servidor stand-alone por defecto.

Una vez activado el módulo podemos acceder a Usuarios y Equipos > Opciones de configuración de LDAP, en el bloque superior podemos ver la Información de LDAP, ver Figura 48.

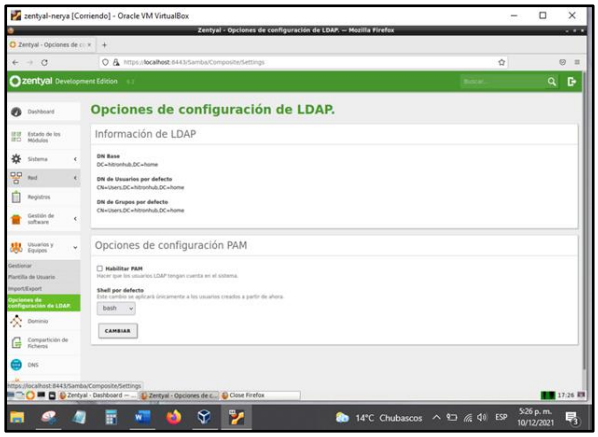

Figura 48. Opciones de configuración de LDAP.

Descripción de la configuración:

- DN Base: Base de los nombres de dominio de este servidor, coincide con el dominio local. El dominio local se configura desde Sistema > General > Dominio y aparecerá como bloqueado (no es posible eliminarlo) en nuestro módulo de DNS.
- DN de Usuarios: Nombre del contenedor de Usuarios por defecto.
- DN de Grupos: Nombre del contenedor de Grupos por defecto.

En la parte inferior se podrán establecer Opciones de configuración PAM, pero no se hace ninguna modificación, ver Figura 49.

Figura 49. Opciones de configuración PAM

Desde el menú Usuarios y Equipos▸ Gestionar podremos ver el árbol de LDAP, ver Figura 50.

Usando esta interfaz podemos crear y borrar nodos del árbol, gestionar los atributos de los nodos y modificar los permisos de los usuarios para otros servicios que utilizan este directorio. Para agregar un usurario simplemente pulsamos en la cruz verde; y se ingresa la información como se observa en la Figura 51.

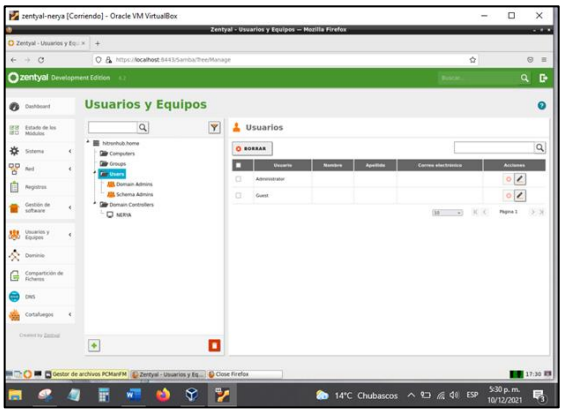

Figura 50. Usuarios y equipos para LDAP.

Figura 51. Añadir usuario.

Ahora, se procede a configurar Zentyal como un servidor de Dominio Standalone.

Antes de activar Usuarios, Equipos y Ficheros por primera vez nos aseguraremos de que hemos configurado el modo de operación, por defecto Controlador del Dominio, pero también podemos configurar el servidor para ser un controlador adicional unido a otros nodos. En este último caso, configuraremos el modo de operaciones y las credenciales antes de activar el módulo, y seguiremos las instrucciones para este, de acuerdo con las siguientes secciones. Si el servidor va a funcionar como primer Controlador del Dominio, no es necesario modificar los datos por defecto, ver Figura 52.

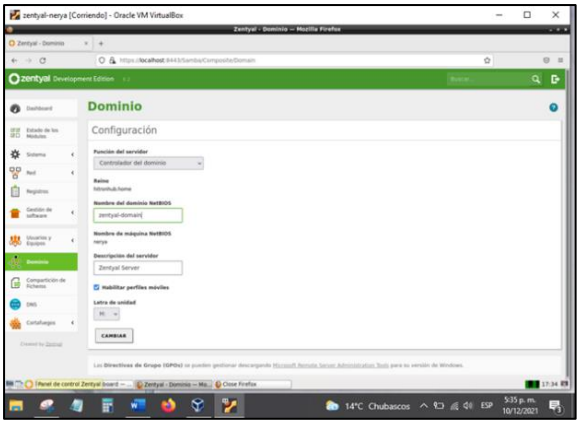

Figura 52. Configuración de Dominio.

Creando un directorio compartido: en el control de acceso se gestiona los directorios compartidos, dependiendo del usuario. Accederemos a Compartición de Ficheros, pestaña de Directorios compartidos y seleccionaremos Añadir nuevo, ver Figura 53.

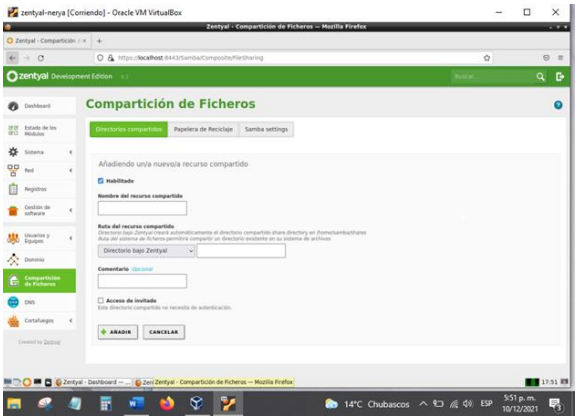

Figura 53. Compartición de ficheros

Se realiza la configuración respectiva, de acuerdo con la figura 54, y posteriormente al Añadir la configuración, se podrá ver en el listado respectivo. Las opciones se describen a continuación.

- Habilitado: Por defecto activado, se está compartiendo este directorio, Podemos desmarcarlo para dejar de compartir.
- Nombre del recurso compartido: El nombre de esta carpeta compartida para nuestros usuarios.
- Ruta del recurso compartido: Ruta en el sistema de ficheros donde se encuentra el recurso, por defecto dentro de /home/samba/shares, o especificar un directorio diferente usando Ruta del sistema de ficheros.
- Comentario: Descripción más detallada del contenido del recurso.
- Acceso de invitado: Activando esta opción será posible acceder al directorio sin autenticación previa. Las demás políticas de acceso asociadas a esta carpeta serán ignoradas.
- Aplicar las ACLs recursivamente: También reemplaza los permisos en todos los subdirectorios del nuevo recurso compartido.

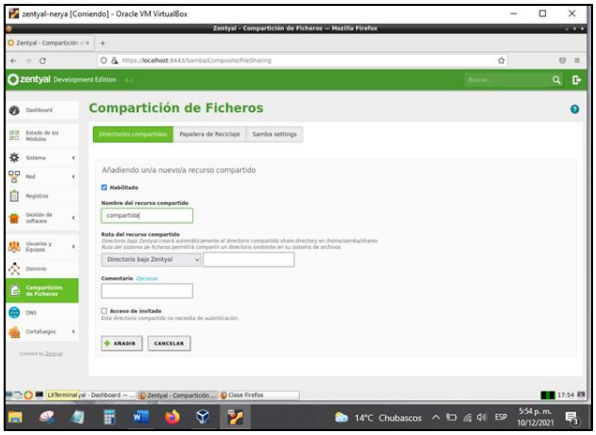

Figura 54. Configuración de compartición de ficheros

Los directorios compartidos pueden ser gestionados accediendo a Control de Acceso. Usando el botón Añadir nuevo, podemos asignar permisos de lectura, lectura escritura o administrador a usuarios y grupos. Si un usuario es el administrador de un directorio compartido, puede leer, escribir y borrar cualquier fichero dentro de ese directorio, ver Figura 55.

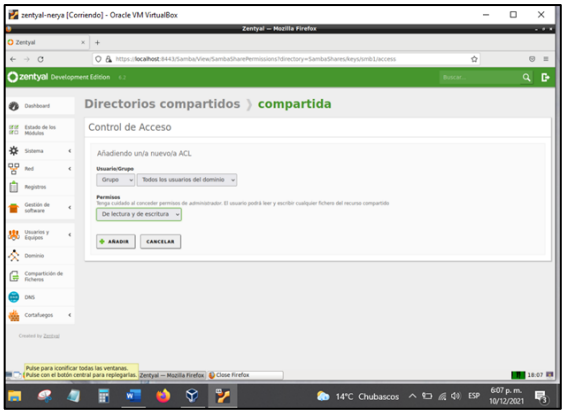

Figura 55. Directorios compartidos

Para poder ingresar al dominio debemos descargar en el Ubuntu Desktop un fichero de nombre pbis-open versión 9.1.0.551 linux.x86_64.deb.sh en la página oficial de github.com

Ingresamos a la terminal y con permisos de sudo, accedemos a la carpeta de descargas y le cambiamos los permisos al archivo descargado a lectura, escritura, y ejecución, así: chmod 777 pbis-open-9.1.0.551.linux.x86_64.deb.sh, ver Figura 56.

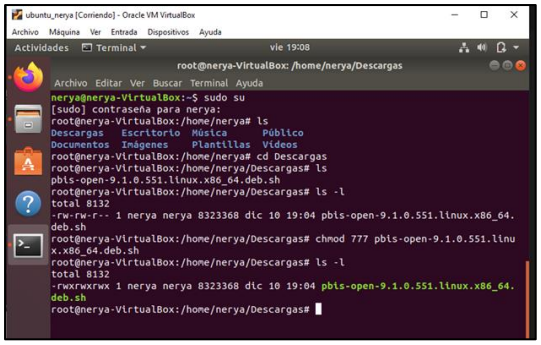

Figura 56. Cambio de permisos al archivo descargado

Verificamos si el equipo reconoce al equipo zentyal-domain.lan en el cual se encuentra instalado nuestro servido Zentyal y su direccionamiento IP, como se puede evidenciar en la Figura 57, haciendo uso del comando: nslookup zentyal-domain.lan

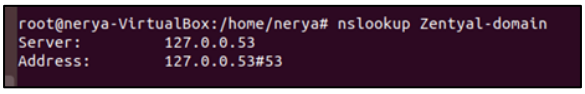

Figura 57: Rectificando el servidor.

Ahora vincularemos el Ubuntu Destktop al dominio zentyaldomain.lan. Ingresamos a la carpeta /opt/pbis/bin y listamos los archivos que contiene, con los comandos: ls /opt/pbis/bin, y con el comando domainjoin-cli, nos solicita usuario del administrador del dominio y contraseña. Haciendo uso del comando: domainjoin-cli join --disable ssh zentyal-domain.lan administrator@zentyal-domian.lan, ver Figura 58.

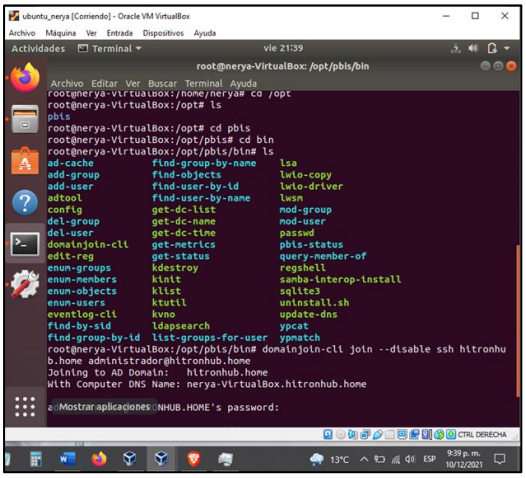

Figura 58. Confirmación de la vinculación.

Reiniciamos el equipo Ubuntu Desktop, vamos al Zentyal, actualizamos y ya tenemos el equipo ingresado en el dominio.

Para que el equipo nos permita acceder con usuarios del dominio, debemos reiniciar el desktop, ingresando a la terminal con sudo su para modificar el archivo 50-ubuntu.conf, con el comando: gedit /usr/share/lightdm.conf.d/50-ubuntu.conf, ver Figura 59.

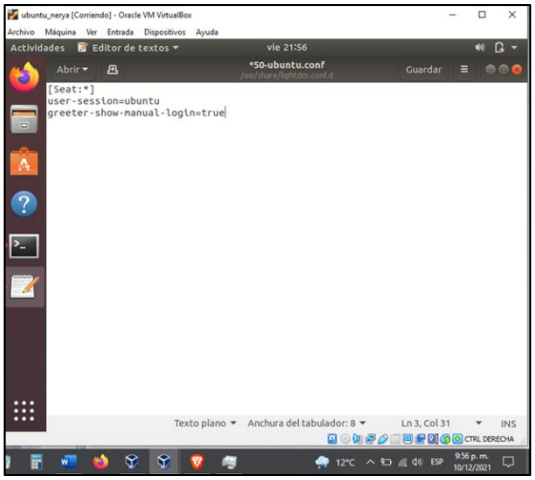

Figura 59. Modificación del archivo con gedit.

Digitamos en la terminal la línea /opt/pbis/bin/config LoginShellTemplate /bin/bash y reiniciamos el Ubuntu Desktop. Ahora ya podremos acceder con usuarios del dominio zentyaldomain.lan en el equipo de escritorio, ver Figura 60.

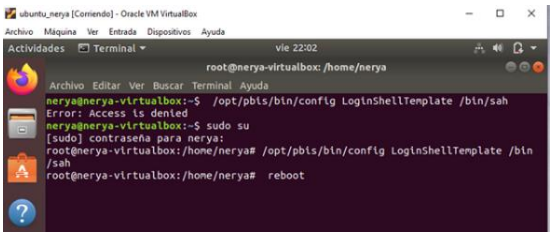

Figura 60. Reinicio del servicio

Luego de esto hace el proceso para el file server y el print server (para poder compartir una impresora virtual con el comando cups y hacer la respectiva gestión).

2.6 VPN

Se procede a definir la configuración, mediante la respuesta y creación de los diferentes permisos para poder funcionar y poder tener accesibilidad a los beneficios de VPN, estos son permisos que se otorgan mediante la configuración de procesos dentro de Zentyal.

VPN es un túnel de comunicación privada el cual se puede ejecutar dentro de una red pública se utiliza para comunicación de los usuarios y la empresa y esta se implementa dentro de la configuración interna.

Para el proceso de instalación se activa el primer adaptador en red NAT y se habilita el segundo adaptador después de la configuración e instalación se apaga la maquina y posteriormente se configura el segundo adaptador en red interna; siguiente de esto, podemos arrancar la máquina.[8].

Dentro del desarrollo de los procesos de VPN podemos encontrarnos con la creación de un servidor el cual nos va a proveer de los diferentes soportes que

necesita el VPN para funcionar entre esto es la creación de un certificado, ver Figura 61. El cual le da el permiso de navegación a este, con el fin que pueda funcionar de manera fluida y concreta.[8].

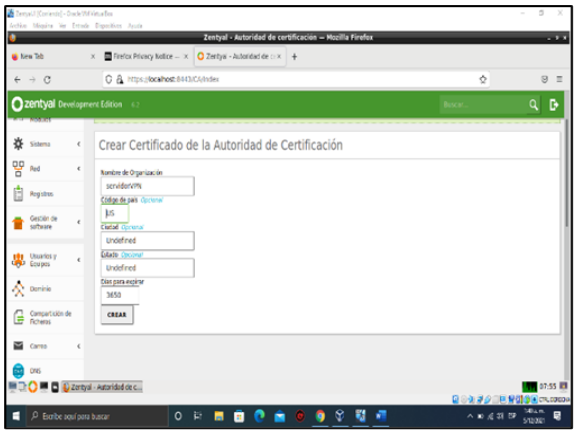

Figura 61. Configuración de certificados de acceso VPN.

Se procede con la configuración de red para definir el proceso de conexión de túnel de comunicación, Para esto Zentyal pone una dirección IP por defecto 192.168.160.0, como se puede observar en la Figura 62. Dentro de esto, podemos configurar la red la red que mantiene la máquina para poder hacer conexión con los permisos de los usuarios, esto, con el fin de que pueda haber una conexión fluida entre el túnel y el usuario.[8].

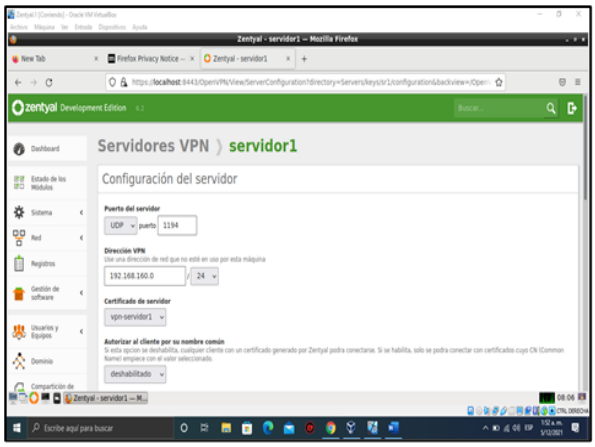

Figura 62. Configuración de red en proceso VPN.

Para la creación de cliente y de navegación en el sitio tenemos que configurar y gestionar los diferentes certificados, ver Figura 63. Estos se crean de manera personal, es decir que para cada cliente hay que hacer un certificado, ya que este es el que va a permitir el ingreso al túnel de comunicación VPN.

Figura 63. Configuración y creación de usuario VPN.

Después de configurar y aplicar los diferentes procesos, se pueden definir los diferentes parámetros para el servidor y su descarga, y sobre este archivo, se le dará el permiso para ingresar a la sala principal del túnel de acceso, ver Figura 64.

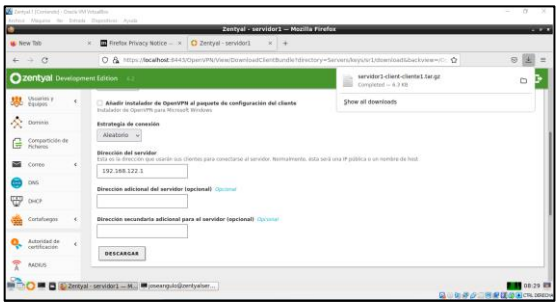

Figura 64. Definiciones adicionales servidor.

Ahora, se realiza la instalación y configuración de servicio OpenVPN (Ver figura 65), el cual es una herramienta que permite realizar la conexión sobre un servicio VPN, y, por lo tanto, provee el acceso al túnel de VPN configurado anteriormente. Se realiza el proceso de instalación, además de cargar el perfil de configuración VPN generado en el paso anterior, ver Figura 66.

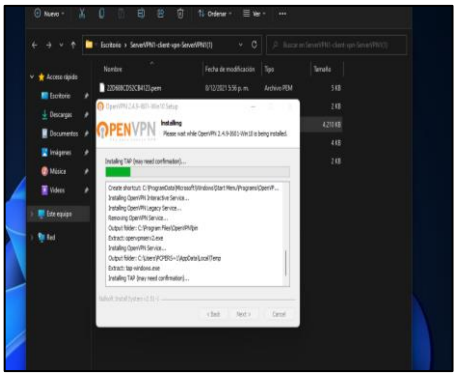

Figura 65. Instalación de OpenVPN en la maquina

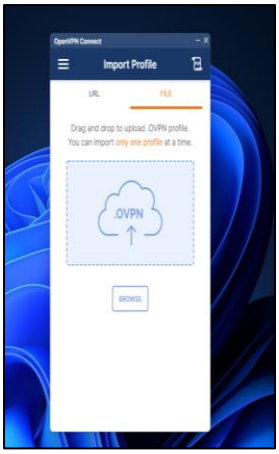

Figura 66. Carga de perfil de configuración VPN.

Posteriormente, se finaliza la configuración y se logra ingresar validado el usuario a la cámara de acceso, verificando la dirección IP generada y el estado de conexión, además del tráfico de información, como se puede evidenciar en la Figura 67.

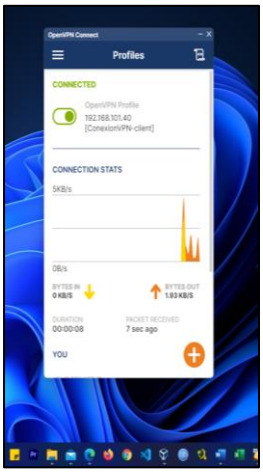

Figura 67. Puesta en marcha del túnel de acceso.

3 CONCLUSIONES

Es importante contar con las diferentes alternativas que brinda el software libre para la administración y gestión de infraestructura de redes, abordando en este caso el sistema Zentyal, el cual, además de las funcionalidades aquí presentadas, demuestra su gran capacidad y herramientas que tiene a la disposición del administrador, con el cual, se logra tener una suite de componentes y módulos que fácilmente permiten configurar una infraestructura de red completa y funcional.

Un servidor DHCP tiene una utilidad muy importante dentro de una red, si esta es bastante grande, puesto que, realizar una asignación de direcciones IP y cada equipo conectado en la red, toma mucho tiempo y recursos, por ello es recomendable en el servidor principal dar de alta el servicio de DHCP para que todos los equipos que se conecten a la red, de forma automática reciban una dirección IP dentro del rango del dominio de la red, permitiendo a todos estos equipos una comunicación entre sí y que todos tengan acceso al servidor o a los servicios que están configurados en él, a través de la definición de puertas de enlace, y generando conexión directa con un servidor DNS para la resolución de servicios y acceso a internet.

En muchas organizaciones privadas o gubernamentales, instituciones educativas, etc. Se requiere restringir el acceso a ciertos servicios dentro de la red o páginas web, entre otros, ya sea por seguridad o por algún otro motivo que se haya estipulado en la entidad, por eso es indispensable la implementación de un proxy http que niegue o permite el acceso a ciertos servicios, pudiendo así, tener un control sobre a los que pueden hacer los usuarios o empleados que estén conectado a la red.

El Cortafuegos de Zentyal actúa como intermediario entre la red interna y externa, además de que permite la configuración de reglas que garantizan el correcto uso de la red e impiden el acceso a personal no autorizado o software malicioso proveniente de la red externa.

El VPN de Zentyal nos permite construir mediante la creación de los diferentes formularios de aceptación y permisos, un servicio VPN como túnel de comunicación, una forma con la cual se puede tener un acceso privado dentro de la red local de una empresa o de cualquier tipo.

4 REFERENCIAS

[1] Zentyal. (s.f.). Características [En línea]. Disponible en: https://zentyal.com/es/caracteristicas

[2] Zentyal. (s.f.). Instalación[En línea]. Disponible en: https://doc.zentyal.org/6.2/es/installation.html

[3] Zentyal. (s.f.). Servicio de configuración de red (DHCP) [En línea]. Disponible en: https://doc.zentyal.org/6.2/es/dhcp.html

[4] Zentyal. (s.f.). Servicio de resolución de nombres de dominio (DNS) [En línea]. Disponible en: https://doc.zentyal.org/6.2/es/dns.html

[5] Zentyal. (s.f.). Controlador de Dominio y Compartición de ficheros[En línea]. Disponible en: https://doc.zentyal.org/6.2/es/directory.html

[6] Paessler AG. (s.f.). IT Explained: Active Directory [En línea]. Disponible en: https://www.paessler.com/es/it-explained/active-directory

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

[8] Juan Enrique. (25 de Julio 2015). Configuración de Servidor VPN con Zentyal. [Video]. Obtenido de https://www.youtube.com/watch?v=2MjtTU0rMIM.