

IMPLEMENTACIÓN DE ZENTYAL 6.2 COMO ADMINISTRADORES DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN AMBIENTES EMPRESARIALES

Edwin Félix Ponce Roberto
efponcer@unadvirtual.edu.co
Juan Pablo Macias Contreras
jpmaciasc@unadvirtual.edu.co
Lizeth Fernanda Aroca Guzmán
lfarocag@unadvirtual.edu.co
Christian Camilo Hernández Umbarila
cchernandezu@unadvirtual.edu.co
Eduwin Gabriel Rojas Diaz
egrojasd@unadvirtual.edu.co

RESUMEN: *A través del desarrollo de este trabajo se presenta la instalación, configuración y debida parametrización de algunos de los servicios de Zentyal Server 6.2, como opción de uso en la utilización de Windows Server. Los servicios descritos en este documento son DHCP Server, DNS Server, Controlador de Dominio, Proxy no Transparente, Cortafuegos, File Server, Print Server y VPN. Estas instalaciones y configuración se realizaron mediante la utilización de máquinas virtuales mediante el programa VirtualBox, donde se obtuvo el conocimiento para la implementación y puesta en marcha de estos servicios.*

PALABRAS CLAVE: Configuración e Instalación, Máquinas Virtuales, Servicios, Windows Server.

1 INTRODUCCION

Durante el desarrollo de este documento realizaremos actividades que nos permitirán apropiarnos de los conocimientos necesarios para en primera instancia realizar la instalación y configuración de Zentyal 6.2, como alternativa para el uso de Windows Server. En segunda instancia realizaremos las mismas actividades, pero esta vez en servicios los cuales son opcionales y entre los cuales están DHCP Server, DNS Server, controlador de dominio, proxy no transparente, cortafuegos, file server, Print Server y VPN.

Durante el desarrollo de la instalación y configuración de los servicios antes descritos obtendremos las capacidades necesarias para implementar estos servicios, los cuales son un requerimiento de la guía de actividades en el paso 8. En el cumplimiento de estos requerimientos obtendremos la capacidad de replicar estos servicios en entornos empresariales, ya que utilizaremos máquinas virtuales con las cuales simulares un entorno laboral y además podremos aplicar los conocimientos adquiridos durante el desarrollo del diplomado en profundización en Linux, para realizar exitosamente esta actividad.

2 INTALACIÓN ZENTYAL 6.2

2.1 REQUISITOS DEL HARDWARE

Antes de iniciar con la instalación de Zentyal 6.2, debemos comprobar los requisitos previos con los que debe contar nuestro hardware, las características de este dependen en primera medida de los servicios que se van a instalar y al número de usuarios que se conectaran de forma concurrente a través de nuestra aplicación base, estos serían los requisitos mínimos, así:

Aquellos servicios como antivirus, DNS, DHCP, firewall, controlador de dominio y file print server requieren que los equipos de cómputo sobre los cuales se soportaran deben tener 2 GB en memoria RAM para un número de usuarios menor a 50, en caso de que el número de usuarios sea mayor a este número, la memoria RAM deber ser de 4 GB.

En aquellos casos donde la implementación se realiza para el uso de proxy y VPN, el equipo de cómputo que soporte estos servicios debe tener 4 GB, para un número de usuarios menor a 50.

Las especificaciones técnicas anteriormente descritas son para implementaciones donde Zentyal 6.2 se esté ejecutando con un solo servicio de los antes descritos. Los requerimientos en cuando a disco duro se recomienda la utilización de discos duros de estado sólido para tener un mejor rendimiento. Para los casos donde la implementación sean VPN, proxy o firewall el equipo computo debe tener 2 tarjetas de red.

Para aquellos casos donde la implementación se requiera realizar en entornos empresariales con más de 100 usuarios conectados de forma concurrente, se debe realizar un análisis específico de cada uno de los servicios, en caso de que sean más de uno, con el fin de obtener un comportamiento estable tanto de Zentyal 6.2 y de los servicios instalados.

2.2 PROCEDIMIENTO DE INSTALACIÓN

El proceso de instalación lo realizaremos sobre máquinas virtuales basadas en el software Virtualbox 6.1 para Windows, las cuales serán configuradas con una asignación de memoria RAM de 2 GB y con un espacio en disco duro de 25 GB, para los casos donde la instalación de servicios requiera otras especificaciones, estas se describirán en cada uno de los casos dentro de este documento. Iniciamos el procedimiento de instalación después de haber realizado la descarga de la imagen .ISO desde la URL <http://download.Zentyal.com/Zentyal-6.2-development-amd64.iso>.

Dentro de las primeras configuraciones que debemos realizar al momento de la instalación de Zentyal 6.2 es la selección del idioma para la ejecución de este y del idioma para el teclado. Durante el proceso de instalación el sistema detectará el número de tarjetas de red con que la máquina virtual cuenta, ver Figura 1.



Figura 1. Configurar la red.

Acuerdo a la Figura1, fueron detectadas 3 tarjetas de red de las cuales la interfaz eth0 será seleccionada como principal y será la utilizada para la actualización de los repositorios de Zentyal 6.2 y para la descarga de los servicios que se deseen instalar, las otras interfaces serán utilizadas para los servicios en que su uso sea necesario.

A continuación, se determinará un nombre para la máquina por medio del cual se podrá identificar a esta máquina dentro de la red de cómputo, así mismo será necesario la creación de un usuario administrador de esta máquina. Al termino de los procedimientos anteriores se iniciará la instalación de los componentes base del sistema, ver Figura 2.

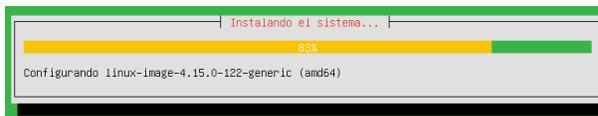


Figura 2. Instalación de componentes del sistema.

En caso de que la instalación de los componentes del sistema se realice de forma satisfactoria obtendremos un resultado en pantalla como el de la Figura 3.



Figura 3. Finalización de la instalación.

Debemos realizar el procedimiento que se nos recomienda acuerdo a la Figura 3, en el momento que se inicie por primera nuestro sistema Zentyal 6.2, este abrirá automática el navegador o browser determinado y obtendremos como resultado acuerdo a la Figura 4, así:

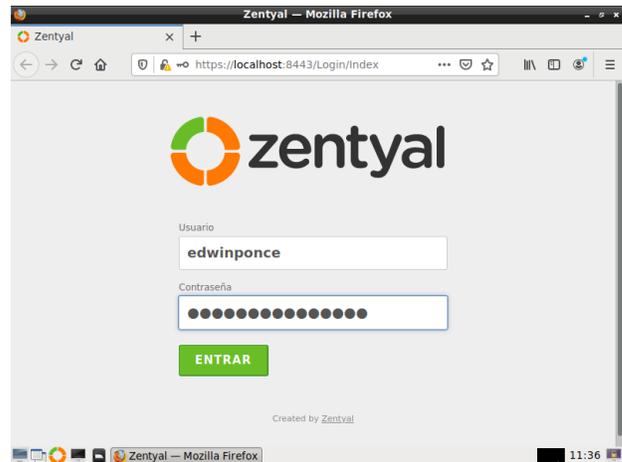


Figura 4. Inicio sesión en Zentyal 6.2.

El inicio de sesión acuerdo a la Figura 4, se debe realizar con las credenciales que se definieron durante la instalación del sistema. Después de realizar el inicio de sesión obtendremos un entorno en el cual podremos iniciar la configuración del sistema por medio de un entorno gráfico. Ver Figura 5.

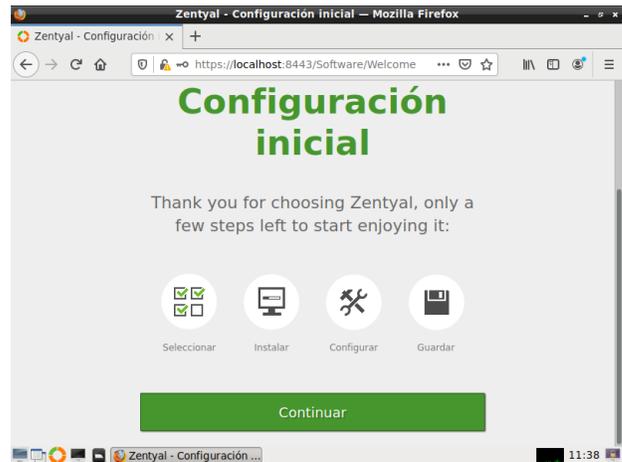


Figura 5. Configuración inicial de Zentyal 6.2.

El proceso de continuar iniciara después de hacer clic en el botón *Continuar*, acuerdo a la figura anterior, como resultado el sistema nos mostrara una serie de

servicios que podrán ser instalados sobre el sistema en ejecución, ver Figura 6.

En Zentyal 6.2 existe la posibilidad de instalar los siguientes servicios, así: Antivirus, HTTP Proxy, Mail Filter, Virtualización Manager, IPS (Sistema Prevención de Intrusos), Raius, FTP, VPN, Jabber, DNS, DHCP, Firewall, entre otros. La selección de estos servicios se realiza directamente desde el entorno de Zentyal 6.2, en el desarrollo de este trabajo se realizará la instalación y configuración de servicios acuerdo a los descritos en el resumen del presente documento.

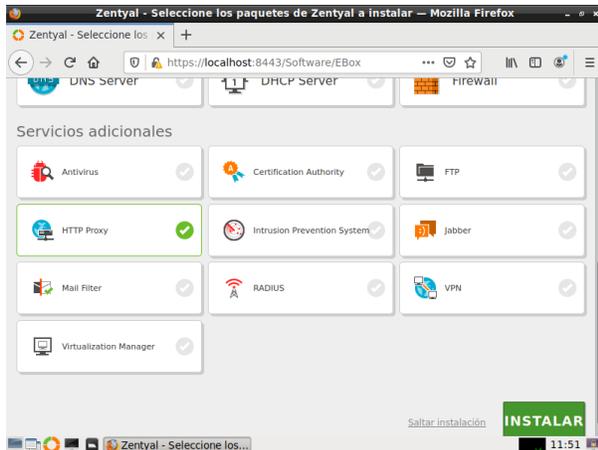


Figura 6. Servicios disponibles en Zentyal 6.2.

3 PROXY NO TRANSPARENTE

Comencemos describiendo el concepto de un Proxy, este es un servicio a través del cual podemos optimizar nuestra privacidad dentro de una red de cómputo mientras sus clientes se encuentran navegando en internet, a nivel empresarial muchas veces este proxy puede estar dentro de sus instalaciones, generalmente es un servidor, el cual recibe las peticiones de navegación de sus clientes y este puede realizar tareas de filtraciones para posteriormente enviar estas peticiones a los diferentes servicios web que el cliente este requiriendo. Por tal razón nunca quedara expuesto directamente el equipo que realiza la solicitud sino el proxy. Cuando nuestro proxy reciba la respuesta de los equipos que resuelven los servicios web, requeridos por el cliente, este también puede filtrar los paquetes e incluso bloquear contenido, cookies, además de otras actividades relacionadas con la seguridad.

Para el desarrollo de esta actividad realizaremos la configuración de un proxy no transparente, el cual, a diferencia del transparente, necesita que el cliente conozca la dirección IP del proxy y del puerto que este utiliza para realizar sus funciones, esta configuración en la mayoría de los casos se realiza a través del navegador web que esté utilizando el cliente.

Para el inicio de nuestro proxy no transparente desde Zentyal 6.2 procedemos así:

En la Figura 6, en servicios adicionales hacemos clic sobre HTTP Proxy y luego en el botón Instalar acuerdo a la Figura 7, al hacer clic sobre el botón instalar, Zentyal nos informa de los paquetes que serán instalados junto con el Proxy. Seguidamente procedemos a realizar clic sobre el botón *Continuar*, con lo cual se iniciará la instalación de todos los paquetes necesarios para la correcta configuración y funcionamiento del HTTP Proxy, el cual para nuestro caso será configurado como un proxy no transparente.

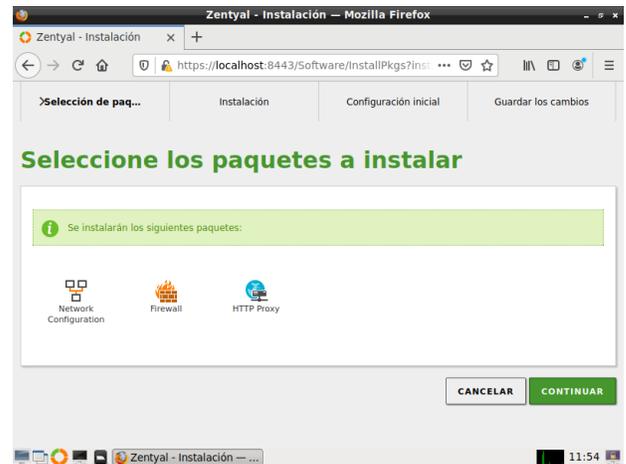


Figura 7. Paquetes por instalar - HTTP Proxy.

Al término de la instalación de los paquetes se nos pregunta por la configuración y asignación de tarjetas necesarias para la configuración de los paquetes, recordemos que el adaptador 0, ya lo habíamos configurado como adaptador principal donde este corresponde a eth0, ahora configuraremos eth1 como adaptador LAN y el adaptador 2 (eth2) como adaptador para la DMZ, ver Figura 8.

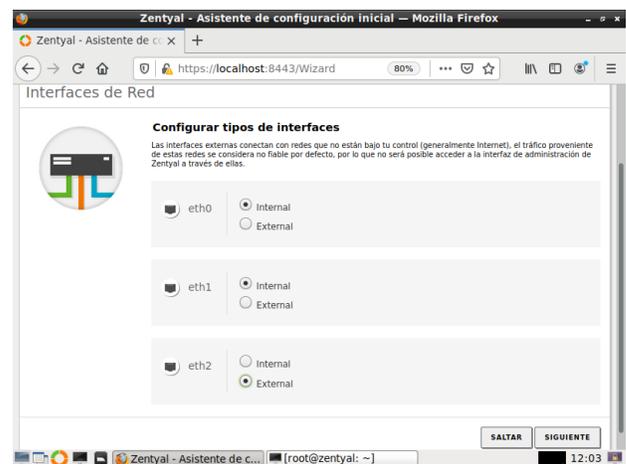


Figura 8. Configuración adaptadores para HTTP Proxy.

Continuando con la configuración de los adaptadores, el sistema nos pide las asignaciones de las direcciones IP para cada uno de los adaptadores, ver Figura 9, allí lo que hacemos es asignar los valores y

luego hacemos clic en el botón Finalizar, posterior a esta acción nos dirigimos al dashboard. En el dashboard, ver Figura 10, podemos continuar con la configuración de los paquetes instalados, para nuestro caso el HTTP Proxy de modo no transparente.

En el menú lateral procedemos a ingresar a la opción de menú Proxy HTTP y hacemos clic en la opción configuración general, ver Figura 11.

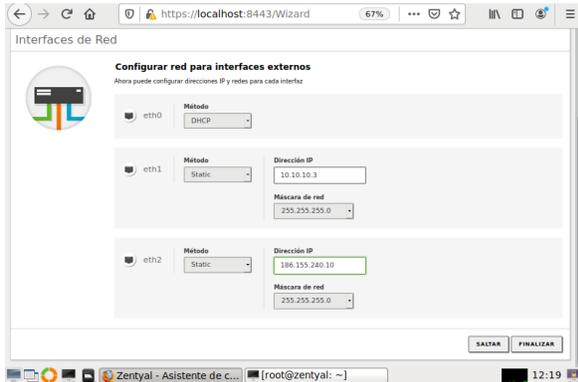


Figura 9. Configuración adaptadores para Zentyal.

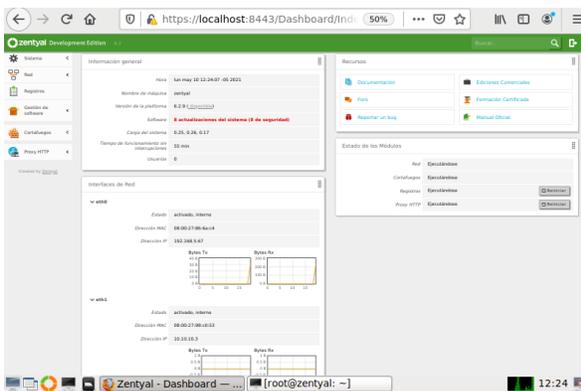


Figura 10. Dashboard Zentyal.

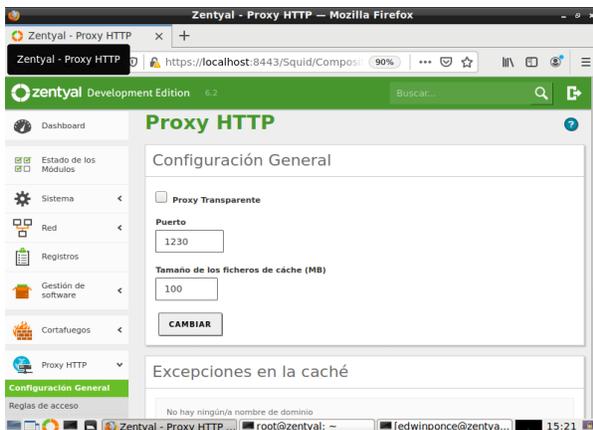


Figura 11. Proxy HTTP Zentyal

Acuerdo a las indicaciones de la guía de actividades debemos hacer que sea un proxy no transparente, ver Figura 11, para ello dejamos sin selección la opción Proxy Transparente, luego en el campo puerto digitamos el puerto 1230, hacemos clic en el botón cambiar y luego en el botón guardar, este proceso se toma un tiempo y a continuación nos confirma los cambios realizados.

Procedemos a configurar las interfaces de red, nos dirigimos a la opción de menú Red -> Interfaces, en la interfase eth0 seleccionamos la opción Externo WAN, esto con el fin de que Zentyal sea el Gateway, ver Figura 12, ahora configuraremos la interfaz eth1 la cual hace parte de la red LAN de la organización, ver Figura 13.

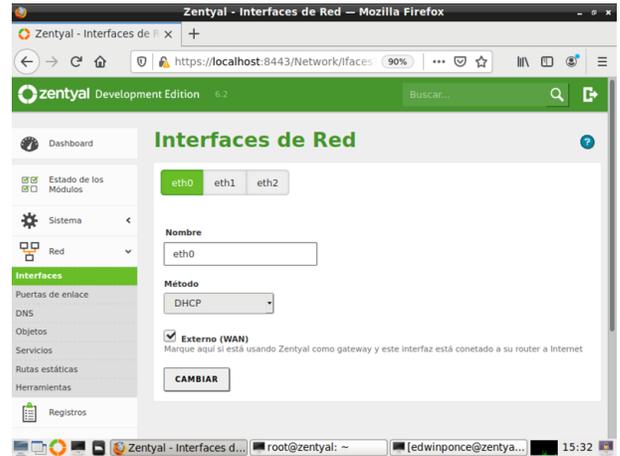


Figura 12. Configuración Eth0 - Proxy HTTP Zentyal

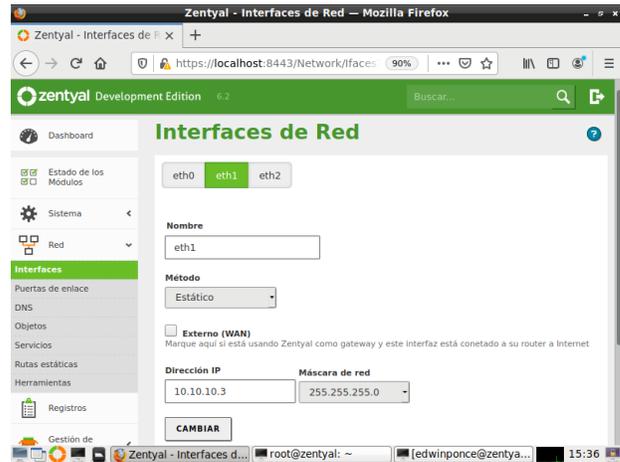


Figura 13. Configuración Eth1 - Proxy HTTP Zentyal

Procedemos a configurar una maquina Ubuntu Desktop dentro de la red LAN, para que esta pueda obtener acceso a Internet a través del proxy, recordemos que la dirección IP de la interface 2 es 10.10.10.3, configuremos la interface de red de la desktop, así:

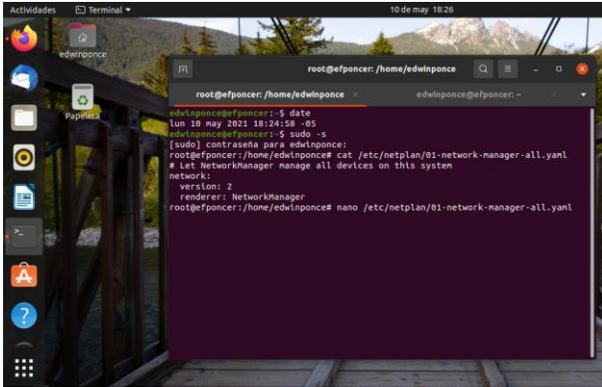


Figura 14. Configuración Interfaz en Ubuntu Desktop.

Desde la terminal de comandos, ver Figura 15, procedemos a ejecutar todos los comandos en modo root, con el comando sudo -s, luego verificamos el contenido del archivo /etc/netplan/01-network-manager-all.yaml con el fin de ver la configuración actual, luego editamos este archivo con el objeto de asignar una IP estática a este equipo, así:

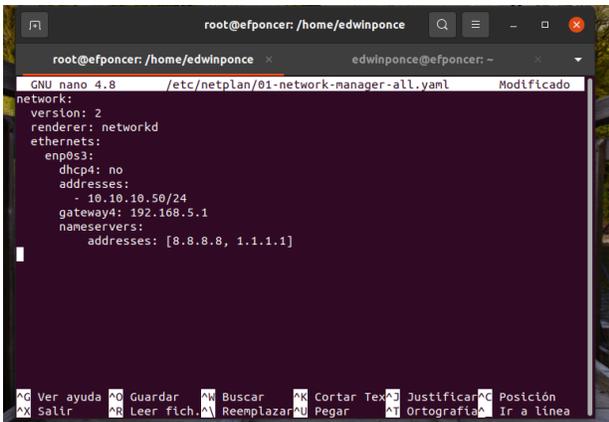


Figura 15. Configuración Interfaz en Ubuntu Desktop

La asignación de la dirección la estática fue exitosa. Ahora procedemos a realizar un ping a la IP 10.10.10.3, ver Figura 16.

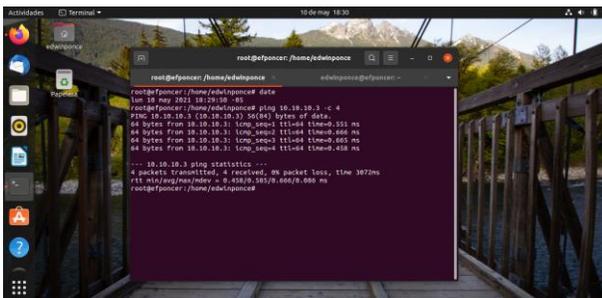


Figura 16. Comprobación conectividad LAN.

Ahora procedemos a configurar el navegador para que utilice el proxy no transparente, así:

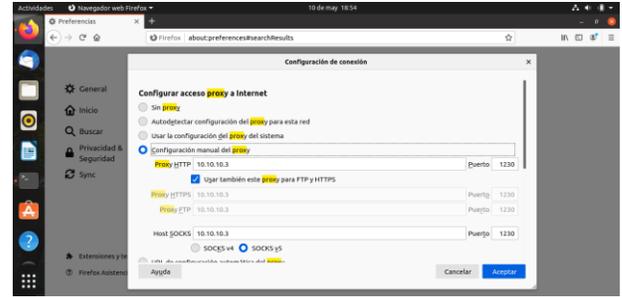


Figura 17. Configuración Proxy en el navegador de Ubuntu Desktop.

Ahora procedemos a comprobar que nuestro equipo este accediendo a internet, mediante el acceso a un sitio web, así:



Figura 18. Navegación de Ubuntu Desktop a través del Proxy.

Ahora comprobemos que estamos dentro de una LAN y no tenemos acceso a internet por medio de un ping, pero si navegamos por medio del Proxy, ver Figura 19.

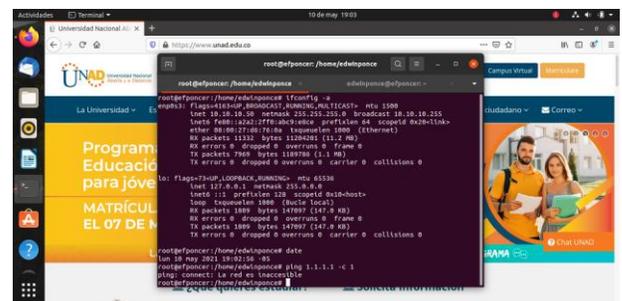


Figura 19. Comprobación de LAN.

Otro mecanismo de comprobación de la navegación del cliente es la muestra del registro de la navegación que se ha realizado desde la dirección IP 10.10.10.50, la cual corresponde al host que tiene el sistema operativo Ubuntu Desktop, ver Figura 20.

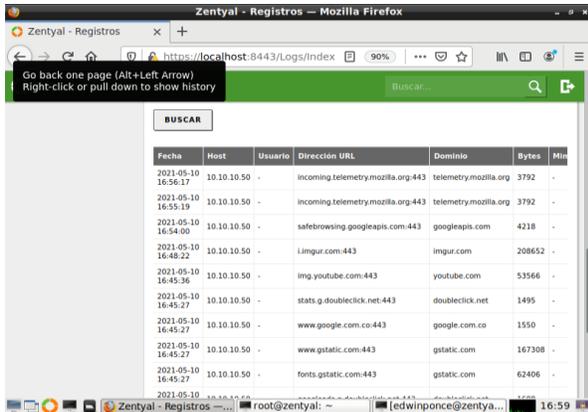


Figura 20. Registro de navegación a través del Proxy

A través del registro de las actividades de navegación acuerdo a la Figura anterior, hemos comprobado el uso y configuración de manera satisfactoria del HTTP Proxy en modo no transparente, cumpliendo con los requerimientos realizados en la guía de actividades.

4 FILE SERVER

Para este paso lo que buscamos es crear un "File Server" o servidor de archivos el cual permite a los clientes conectados a una red acceder a sus propios recursos de almacenamiento, este tipo de servidores son muy útiles en todo tipo de empresas tanto grandes como pequeñas donde el personal tiene que cambiar de equipo de cómputo y necesita llevarse o mover sus archivos de un lugar a otro, o en edificios donde las personas tengas que mover su lugar de trabajo de un piso a otro.

Lo más importante para que un servidor de archivos funcione correctamente es contar con un Hardware adecuado el cual ya que se van a almacenar archivos constantemente debe contar con suficiente espacio para soportar esta carga de archivos y velocidad para transferir los mismos.

Dentro de las muchas posibilidades y funciones que se le pueden dar a un servidor de archivos la principal y más utilizada es que gracias a que los archivos en su mayoría se van a almacenar en el servidor, los equipos de cómputo no necesitan contar con grandes cantidades de memoria para funcionar correctamente.

Después de concluir con la instalación de Zentyal 6,2 procedemos a seleccionar los paquetes a instalar entre los cuales incluimos el "Domain Controller and File Sharing". Ver Figura 21.



Figura 21. Selección de paquetes a instalar

Al terminar la configuración de la IP de la red que vamos a utilizar como servidor, vamos a seleccionar el nombre de dominio del servidor, este nombre de dominio es muy importante ya que nos permite reconocer los equipos en la red, asignarle los usuarios y grupos y acceder a los equipos con los mismos. Ver Figura 22.



Figura 22. Seleccionar nombre de dominio del servidor

En el siguiente paso y utilizando el nombre de dominio previamente creado lo que hicimos fue crear un servidor DHCP que será el encargado de asignar automáticamente las IP a los equipos que se conecten a esa red. Ver Figura 23.

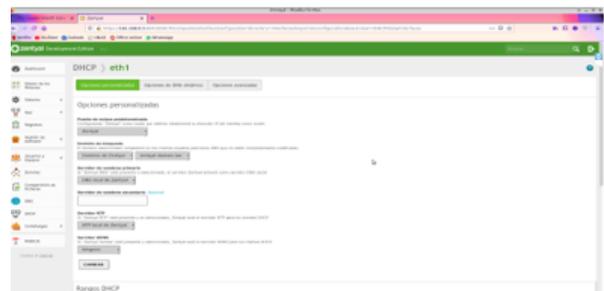


Figura 23. Servidor DHCP

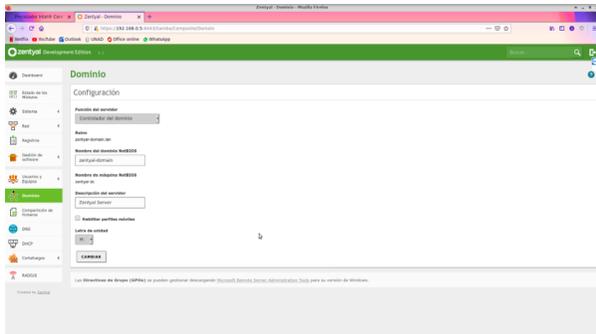


Figura 24. Controlador de dominio.

Al asignar un nombre de dominio NetBIOS lo que se busca es que el servidor reconozca ese controlador de dominio con un nombre propio, realizado esto podemos comenzar a crear los diferentes grupos y sus respectivos usuarios que vamos a incluir en los mismos. Ver figura 25.

En este caso creamos tres grupos uno para Gerentes, otro para Administradores y el último para personal de Planta y dentro de cada uno le asignamos un usuario, en van a existir más personas en la Planta o con cargos operativos que Gerenciales, Zentyal nos permite por medio de su Interfaz gráfica agregar estos usuarios de una forma muy sencilla.

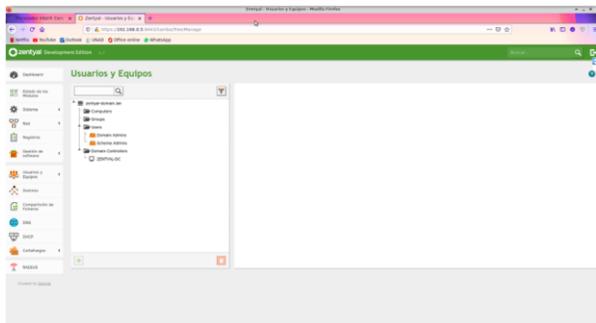


Figura 25. Añadiendo grupos y usuarios

Como se muestra en la siguiente imagen se agregan los grupos y los usuarios dentro de los mismos. Ver Figuras 26 y 27.

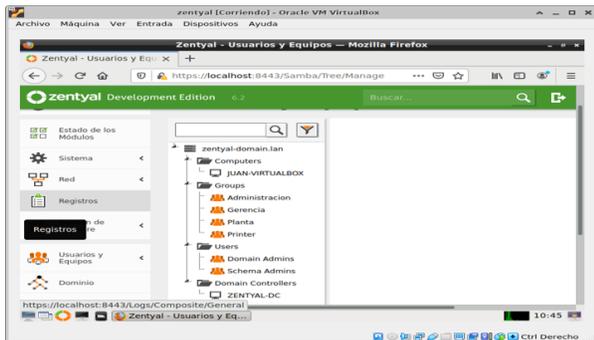


Figura 26. Añadiendo Grupos

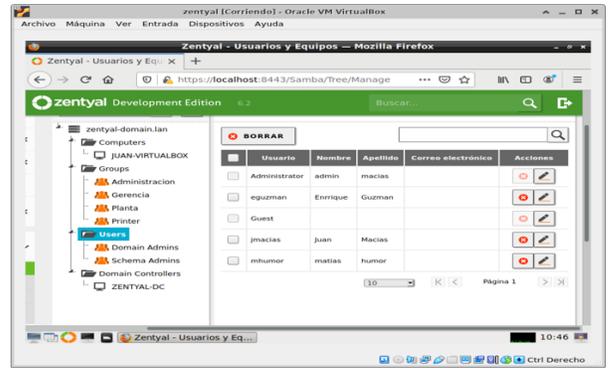


Figura 27. Añadiendo Usuarios

Ahora vamos a añadir los equipos a la red, el proceso es muy fácil de realizar en máquinas con Windows, sin embargo, para máquinas con Linux es necesario descargar un script llamado pbis-open-9.1 como podemos ver en la Figura 28.

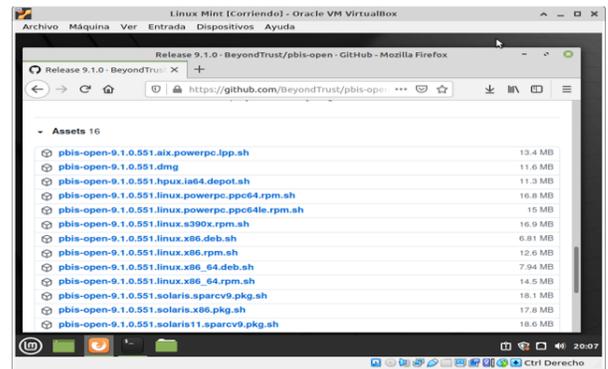


Figura 28. Descarga de pbis-open-9.1

Para este paso se le otorgan permisos de ejecución por medio del comando `chmod +x` y luego utilizamos el siguiente formato de comando para agregar el equipo al dominio, tal como se puede ver en la Figura 29.

“domainjoin-cli join --disable ssh dominio administrador”

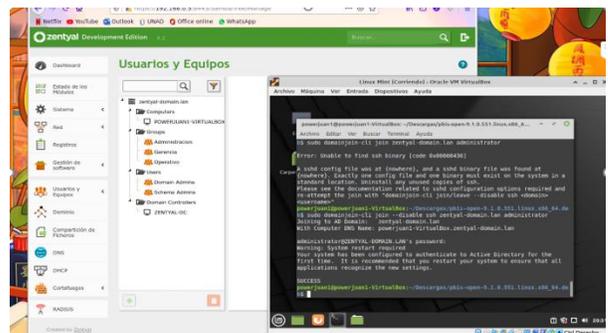


Figura 29. Agregando equipo al dominio

Dependiendo del sistema operativo que estemos utilizando debemos seleccionar la opción para que no

ingrese automáticamente, sino que en cambio siempre pida credenciales de inicio de sesión.

Por último, solo queda iniciar sesión en los respectivos equipos añadidos al dominio, utilizando el nombre del dominio\el nombre del usuario, luego en un explorador de archivos procedemos a ingresar a la siguiente dirección:

“smb://Zentyal-domain.lan”

Esta es la dirección en la red de los grupos y sus respectivas carpetas, en este caso ahí podemos probar el acceso a las diferentes carpetas, subir archivos, descargar archivos. Ver Figura 30. En cualquier computador de la red registrado en el dominio podríamos realizar lo mismo.

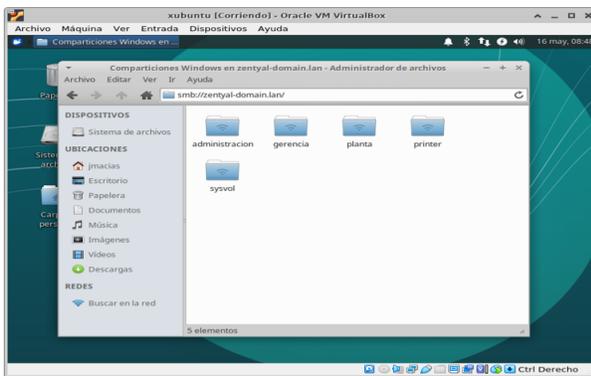


Figura 30. Acceso al servidor de archivos.

5 PRINT SERVER

Un “Print server” o servidor de impresión es una herramienta muy útil en una oficina o casa que nos permite utilizar una impresora de forma remota, evitándonos así la tarea de tener que transportar un archivo a imprimir a un computador conectado a la impresora, esto por supuesto ya es posible realizarlo tan solo compartiendo la impresora en la red sin embargo, si desconectamos o apagamos el computador que tiene la impresora el resto de equipos se verían afectados y no podrían hacer uso de la misma.

Al realizar este procedimiento de conectar un servicio de impresión a la red nos aseguramos de que la impresora siempre va a estar disponible para los equipos que se encuentren en la misma.

Zentyal en sus versiones anteriores nos permitía crear un servidor de impresión sin embargo en las versiones nuevas ya no se encuentra en la lista de utilidades disponibles, ya que fue retirada por motivos de seguridad.

Para crear esta impresora virtual vamos a utilizar un sistema de impresión llamado CUPS, el cual nos va a permitir crear impresoras virtuales y conectarlas a una red. Ver Figura 31.

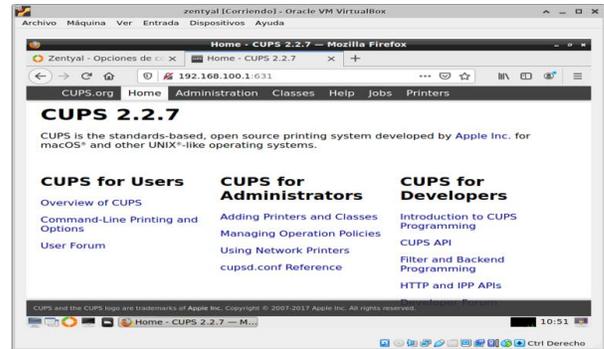


Figura 31. CUPS página principal.

En CUPS lo que hacemos es crear una nueva impresora y luego podemos encontrarla en la pestaña de Printers. Ver figura 32.

Para este ejercicio lo que hicimos fue crear una impresora PDF que convierta los archivos que se envían a la misma a formato PDF, sin embargo, sirve para impresoras reales o incluso se pueden añadir varias impresoras a la red.

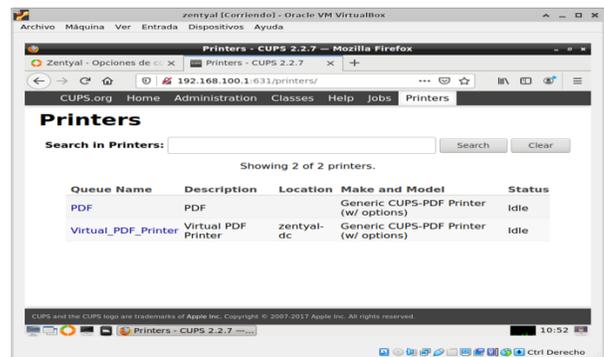


Figura 32. Impresoras creadas.

Como lo vimos en imágenes anteriores también creamos un grupo dentro del controlador de dominio llamado “Printer” esto con el fin de que las impresiones lleguen directamente a ese lugar, a este grupo le dimos acceso a todos los usuarios. Ver Figura 33.

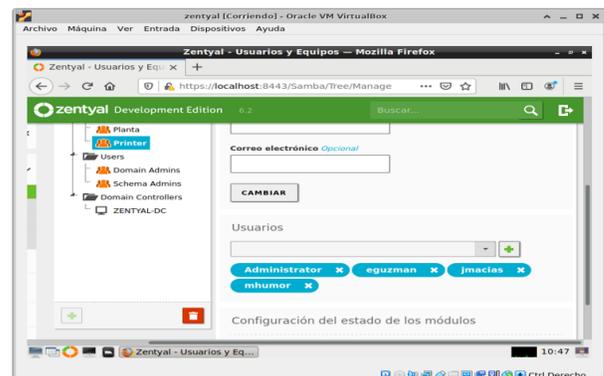


Figura 33. Acceso de usuarios al grupo.

Creamos un scrip que moviera los archivos desde el destino que trae por defecto CUPS a esta carpeta y reforzamos los permisos a los usuarios en el mismo, luego enviamos la prueba de impresión y efectivamente los documentos son impresos de manera satisfactoria. Ver Figura 34.

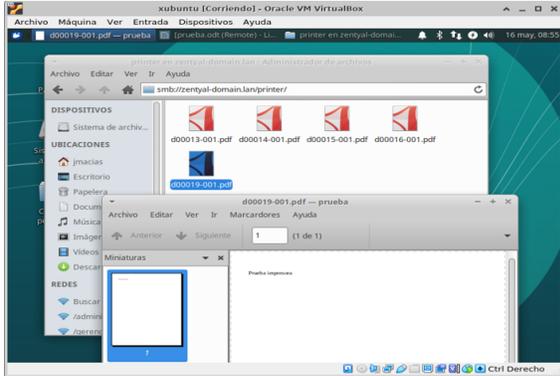


Figura 34. Prueba de impresión.

6 FIREWALL O CORTAFUEGOS

Es un Hardware o Software que controla el tráfico entrante y saliente de una máquina. Para crear el cortafuego en Zentyal y con una página específica se realizan los siguientes pasos.

Se descargan los paquetes que únicamente sean necesarios para trabajar.



Figura 35. Módulos para instalar, únicamente los que están marcados.

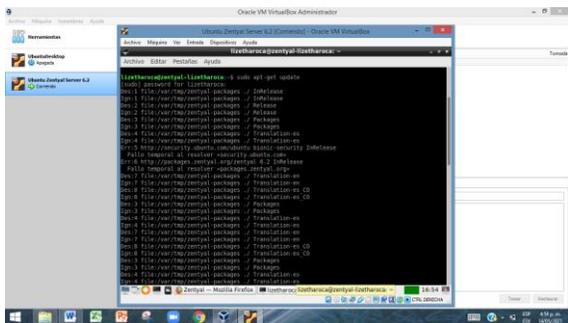


Figura 36. Dentro de la terminal se digita el comando sudo apt-get update.

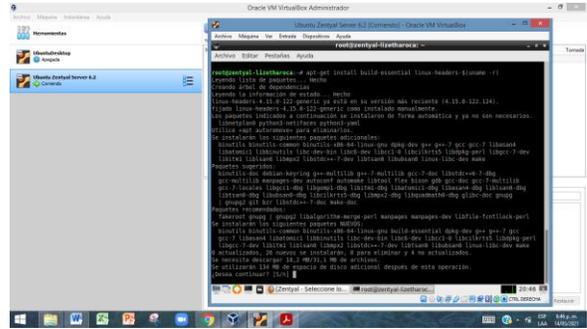


Figura 37. Se digita el comando apt-get install build-essential Linux-headers-\$(uname-r)

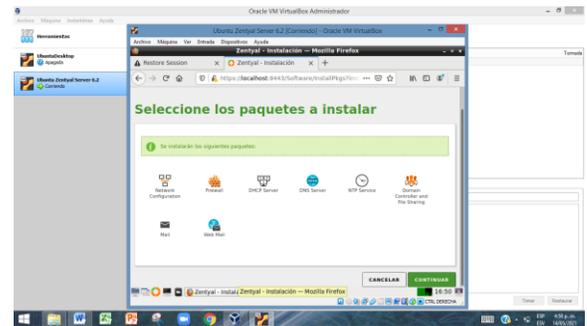


Figura 38. Se Instalan los paquetes que anteriormente se seleccionaron y se da clic en continuar.

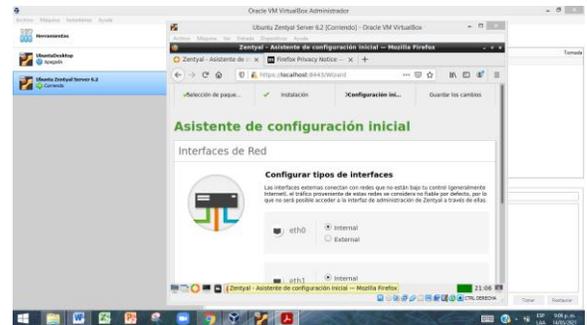


Figura 39. Se hace la configuración de interfaces de red, se configura eth0 yeth1.

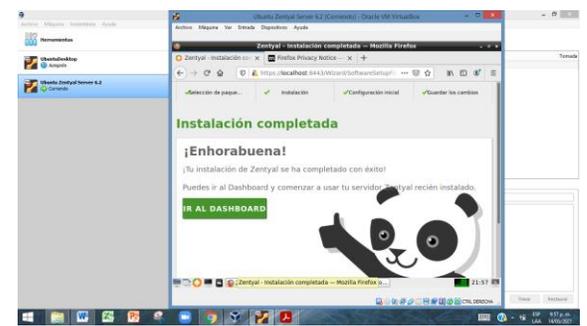


Figura 40. Cuando se termina la instalación, se dirige al Dashboard.

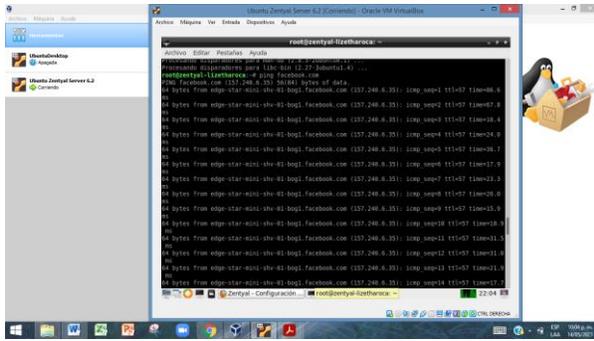


Figura 41. Se hace ping con la página que se desea bloquear. Para este caso fue la de facebook.com

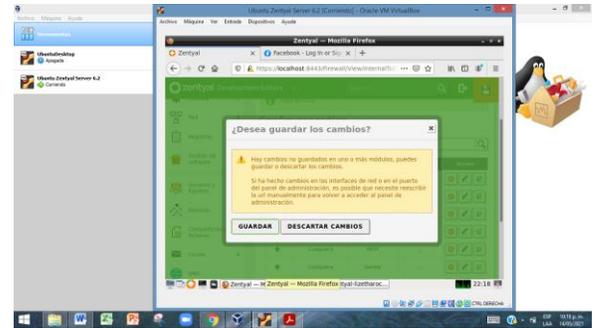


Figura 45. Se guardan los cambios.



Figura 42. Se verifica que ingrese a la página oficial.

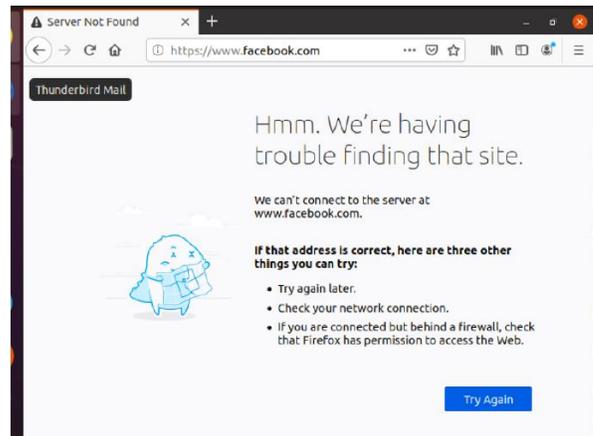


Figura 46. Se demuestra que la página fue bloqueada.

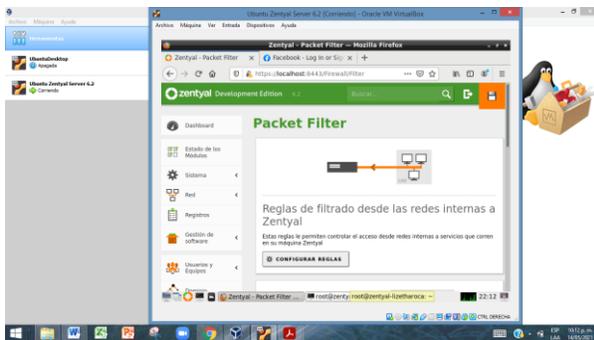


Figura 43. Se busca el icono de firewall, se da clic en filtrados de paquetes y en configurar reglas, por último, se da clic en añadir nueva regla.

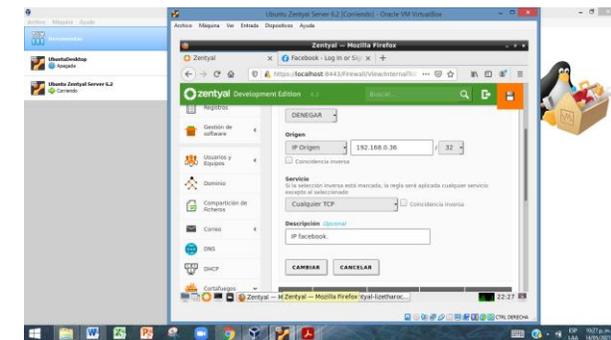


Figura 44. Se configura las reglas de cortafuegos.

7 SERVIDOR DHCP

(Dynamic Host Configuration Protocol), al realizar la traducción al español nos indica un protocolo de asignación dinámica de host, es un protocolo que data de hace muchos años, este surge de la necesidad de interconectar varios dispositivos dentro de una misma red sin que estos lleguen a presentar una identificación duplicada, pudiendo generar errores en el tráfico propio y caídas constantes en el servicio, el servicio DHCP asigna las IP de acuerdo al orden en el que se van conectando los dispositivos a la red mediante el uso del método cliente-servidor, en este el cliente se conecta al servidor y solicita que le asigne una IP, el servidor hace uso de una base de datos en las cuales se encuentran las IP que en el momento se encuentran en uso, evitando hacer uso de estas y recurriendo a las que no se han asignado.

El uso del servicio DHCP en el servidor Zentyal es tal vez uno de los más importantes, es la base fundamental para el uso de servidores DNS, directorios activos, entre algunos otros que dependen de este para su correcta aplicación y funcionamiento, a continuación, se ilustrará de una manera más detallada el proceso de configuración de este servicio en el servidor.

7.1 CONFIGURACION DHCP

Para el desarrollo del ejercicio se realizó la simulación en VirtualBox, una maquina con Zentyal 6.2 haciendo las funciones de servidor un Ubuntu 18.04 haciendo las veces de cliente, para el servidor Zentyal se hizo necesario usar dos adaptadores de red, uno apuntando hacia la red externa (WAN) y otro hacia la LAN a través de una red interna, en el equipo cliente solo bastó con usar un adaptador apuntando hacia la red interna creada en el servidor Zentyal.

El primer paso para realizar una correcta configuración es la revisión de los adaptadores de red que se están usando, en la figura 47 se puede observar que tenemos dos adaptadores, como en este caso lo que vamos a configurar es la red interna no requerimos hacer uso del adaptador asignado a la WAN por lo tanto podemos apagarlo y así evitar inconvenientes, en el adaptador eth0 se encuentra configurada la IP 192.20.5, esta Ip es la que nos está permitiendo tener conexión o salida hacia internet del servidor, en la interfaz eth1 está con configuración que usaremos para el DHCP.



Figura 47. Visualización adaptadores de red

El proceso de configuración inicia con la asignación de una IP fija, sobre dicha IP serán creadas y asignadas las IP's que usarás los ordenadores que se conecten uno a uno, en la Figura 48 se muestra la IP asignada (192.168.100.1), esto indica que todas las IP que se asignen lo harán bajo el rango 192.168.100.XXX

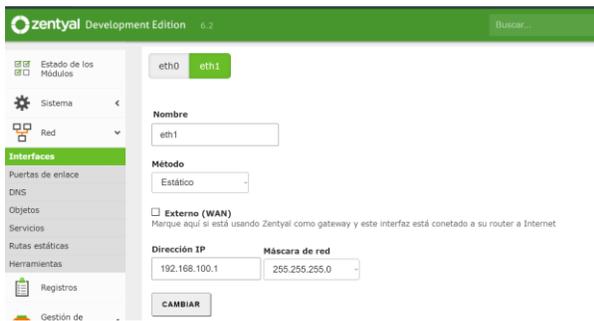


Figura 48. Configuración IP fija

Otra las de las posibilidades que nos ofrece el servidor DHCP es la creación de rangos dentro del mismo servidor, esto se hace especialmente útil en las empresas que tienen demasiadas áreas trabajando y conectadas al servidor, el propósito fundamental es la de crear muchos grupos de IP's, cada grupo se asignará a un área dependiendo de las necesidad de la empresa,

por ejemplo se puede crear un rango para contabilidad desde la IP 192.168.100.30 hasta la IP 192.168.100.60 y para recursos humanos desde 192.168.100.61 hasta 192.168.100.80, de esta manera es más fácil controlar los servicios y las conexiones, en la figura 49, se crea desde la IP 192.168.100.50 hasta la IP 192.168.100.100 y se denomina Zentyal-dc

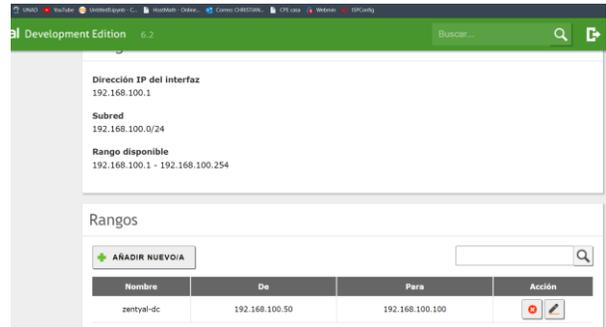


Figura 49. Creación de rangos DHCP

Una vez se ha creado el rango de IP's, cualquier dispositivo que se conecte tomará una IP disponible, en el desarrollo del ejercicio esto se logró mediante la creación de una red interna en VirtualBox, como se mencionó anteriormente, se creó un adaptador especial para esta tarea, se denominó itnet, todo dispositivo virtualizado con adaptador configurado en modo red interna se conectará de manera inmediata a esta red, en la Figura 50 observamos la IP que tomó el equipo cliente, lo cual quiere decir que el DHCP funcionó de manera correcta ya que le asignó la primera IP disponible del rango creado.

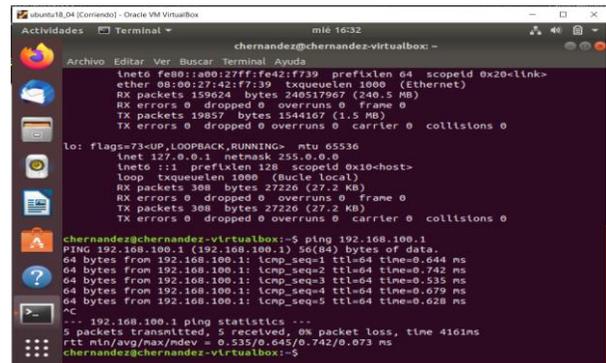


Figura 50. Conexión equipo cliente a servidor

Una vez se ha establecido la conexión entre el cliente y el servidor es importante revisar la interfaz de Zentyal, en la Figura 51 observamos que se actualizó el Dashboard de Zentyal y nos muestra la información más relevante de la máquina que acabamos de conectar al servidor, nos muestra la IP, la MAC o dirección física y por último, el nombre del equipo.



Figura 51. Equipos conectados por DHCP en la Dashboard de Zentyal

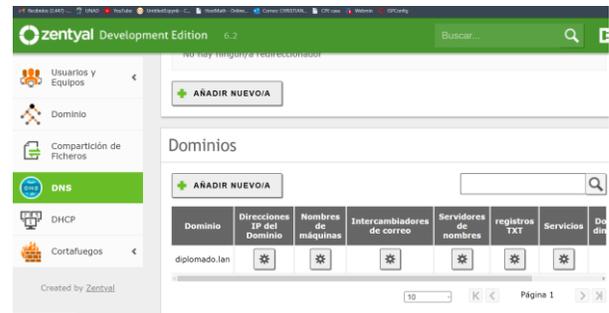


Figura 52. Creación dominio DNS

8 SERVIDOR DNS

Como parte de la actividad se requiere la configuración y creación de un servidor DNS de manera local en Zentyal, este será el encargado traducir las direcciones IP a nombres y viceversa, aunque en la actualidad hay muchos DNS que se pueden usar de manera gratuita como Google (8.8.8.8 como servidor primario y 8.8.4.4 como servidor secundario) nunca está de más poder aumentar la seguridad y velocidad de nuestra red y el hacer uso de un servidor local nos permite eso y mucho más, pero antes de ahondar un poco más en el tema es importante comprender un poco más el termino DNS.

Un DNS o sistema de nombres de dominio, tiene como función principal poder traducir los nombres con los que nosotros normalmente buscamos las páginas de internet en IP's, en términos más simples es traducir información comprensible para los humanos en información entendible para computadoras, por ejemplo, cuando ingresamos la dirección IP www.youtube.com el DNS lo que hace es buscar la IP a la cual está asociada esa dirección y permitirnos el ingreso, esto es un avance ya que sería casi que imposible que una persona pudiera recordar todas las IP de los sitios web a los que diariamente accede.

8.1 CONFIGURACION DNS ZENTYAL

Una vez aclarados los conceptos fundamentales referente a DNS vamos a realizar la instalación y configuración del módulo, lo primero que se debe hacer como en el anterior paso es ir a gestión de software y realizar la descarga de DNS, es importante primero realizar la configuración antes de activarlo, en el apartado de red hay una opción que dice DNS, esta opción lo único que hace es modificar los DNS que va a usar Zentyal para conectarse a internet más no para distribuir a las IP's del DHCP, es un error que normalmente se comete.

Lo primero que vamos a hacer es crear un dominio, este funcionará como servidor DNS, también nos funcionará como controlador de dominio para el paso que sigue, en la figura 52 podemos observar la creación de este.

En la figura 53 se observa la creación del servidor, utilizará dirección IP 192.168.100.1 que es la IP asignada de manera fija para el DHCP y sus rangos, además se agrega la dirección 192.168.20.5 que es la IP que se está usando para dar salida al servicio de internet, por lo tanto, cualquier solicitud que se realice se hará a través de este servidor.



Figura 53. IP asignada para trabajar como DNS

Desde el equipo cliente podemos realizar la comprobación que se tenga conexión con el DNS a través de la herramienta nslookup, creada especialmente para este tipo de comprobaciones, en la Figura 54, se observa el resultado que nos arroja nslookup

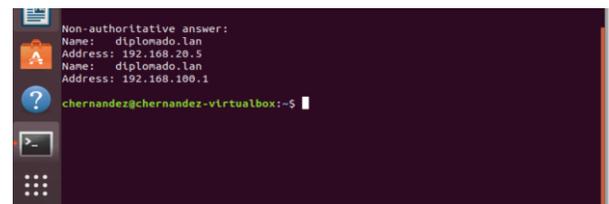


Figura 54. Comprobación DNS desde cliente

9 CONTROLADOR DE DOMINIO

Para entender un poco mejor el concepto de controlador de dominio es importante entender el concepto de la palabra dominio, lo cual se puede traducir como una red de la cual hacen parte varias computadoras o estaciones de trabajo y todos convergen en un punto en especial, en este caso en un servidor, este tipo de servicio es muy importante cuando se trabaja en grandes empresas o con muchos usuarios,

nos permite dar acceso solamente a aquellos que nosotros designemos a través de reglas o creación de grupos con permisos especiales, además nos ofrece una mayor seguridad ya que podemos limitar la información que un usuario puede crear, ver o modificar dependiendo de su rango o estatus dentro de la empresa, se evitan intrusiones no autorizadas, además en temas de economía también nos brinda mucha ayuda, al tratarse de recursos compartidos cualquier usuario puede usar una PC, no es necesario adquirir una para cada uno.

9.1 CONFIGURACIÓN DE DOMINIO

Cuando se ha finalizado la configuración de los DNS, vamos a realizar la configuración del controlador de dominio, nos vamos al apartado de dominio y allí lo creamos, en mi caso le puse el mismo nombre que he venido trabajando, diplomado.lan como se muestra en la Figura 55.



Figura 55. Asignación nombre dominio

Una vez se ha creado el controlador de dominio vamos a proceder a la creación y configuración de varios grupos, usuarios, etc, para eso nos dirigimos a la sección de "usuarios y equipos", como se muestra en la Figura 56.

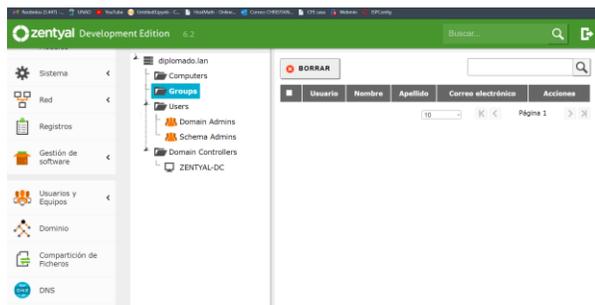


Figura 56. Interfaz de Usuarios y equipos

Primero vamos a añadir varios grupos, en mi caso crearé los grupos, Decanos, Tutores y Estudiantes, como se evidencia en la figura 57

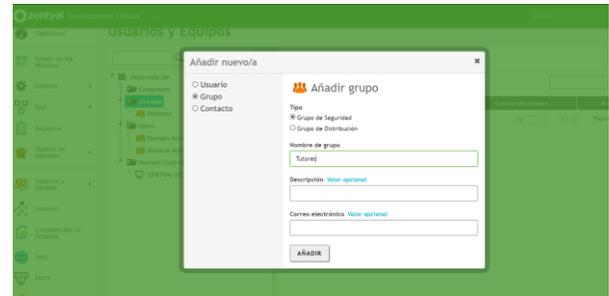


Figura 57. Creación de grupo

Una vez se han creado los grupos de usuarios vamos entonces a crear los usuarios, es un procedimiento muy sencillo que no reviste una complejidad mayor, únicamente ingresamos datos como el nombre de usuario, datos personales, contraseña y grupo, el grupo se puede agregar o modificar más adelante, tal como se observa en la Figura 58.

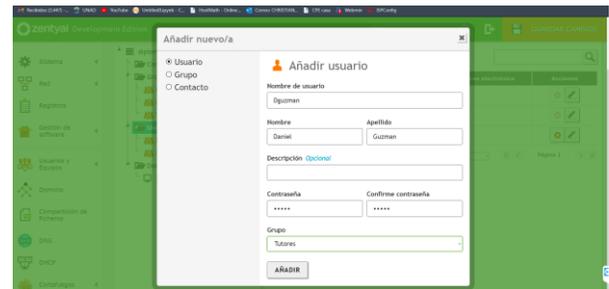


Figura 58. Creación de usuario

Cuando ya se han creado usuarios y grupos nos quedará una imagen como la que se muestra en la Figura 59, entonces podemos acceder a los grupos y ahí definir que usuarios se van a agregar en cada uno de ellos.



Figura 59. Usuarios y grupos creados

En la figura 60 se evidencia la ubicación en la cual queda el registro de los grupos de usuarios, importante tenerla en cuenta por si se requiere realizar alguna modificación o perdemos la interfaz gráfica

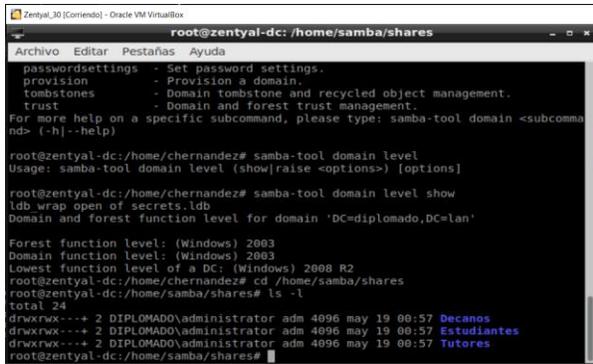


Figura 60. Ubicación de carpetas de grupos

En la Figura 61 se muestra el archivo que se debe instalar en los equipos con Linux para poder unirlos al servidor de manera correcta, esto no es necesario realizarlo en Windows.

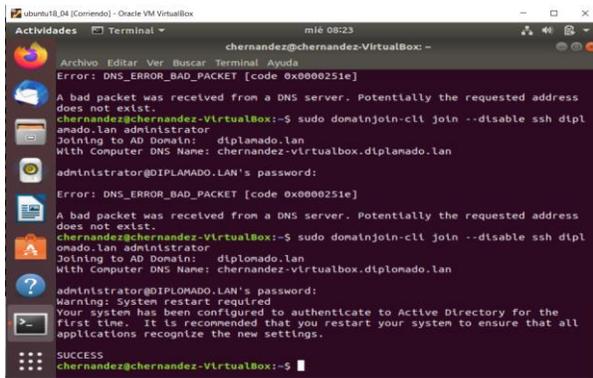


Figura 61. Instalación de complemento para adición de PC

Como podemos observar en el servidor, en el apartado de Computers, nos muestra las máquinas que de manera física se conectaron al servidor, ver Figura 62.

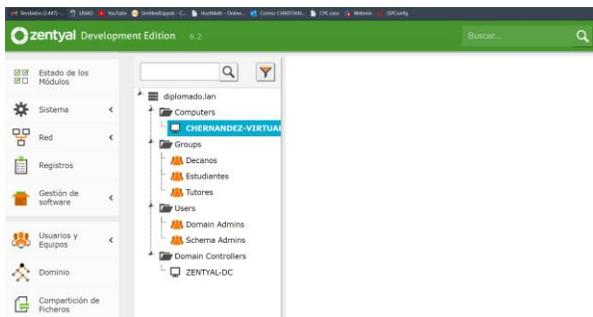


Figura 62. Pc añadido a dominio

En Linux se hace necesario modificar un archivo para que el momento de iniciar sesión nos permite unirnos al servidor con distintos usuarios, tal como se muestra en la Figura 63.

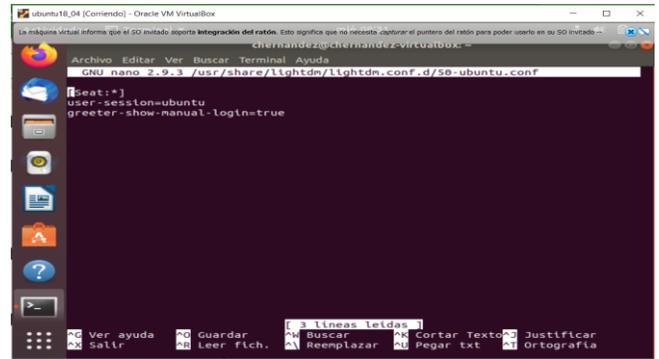


Figura 63. Modificación archivo inicio de sesión

Al iniciar el servicio de Ubuntu que usaremos como maquina nos mostrará únicamente el usuario administrador, entonces lo que hacemos es ir agregando de a poco los usuarios que ya hemos creado en Zentyal con la estructura usuario@dominio. Ver Figura 64.



Figura 64. Unión de usuario al dominio

A medida que se van uniendo usuarios al dominio, estos nos van apareciendo en el inicio de sesión de Linux, como se muestra en la Figura 65.



Figura 65. Usuarios disponibles en inicio de sesión

10 VPN

10.1 ¿QUÉ ES UNA VPN?

VPN de sus siglas (Virtual Private Network) o red privada virtual es una tecnología de redes que permite realizar la extensión segura de una conexión de redes locales a una red privada o no privada como lo es internet. Este tipo de redes permiten que los ordenadores conectados a esta interactúen con el envío y recepción de datos de manera privada permitiendo la encriptación de la información que se trabaje a través de internet

10.2 USABILIDAD DE UNA VPN EN LA ACTUALIDAD

En la actualidad con el tema del virus COVID-19 ha dado lugar a que las empresas realicen la implementación de estas redes dentro de ellas, con el fin de permitir a los trabajadores realizar sus funciones desde sus casas, partiendo desde la configuración y debida instalación de las VPN en los equipos que trabajen de manera remota hasta la debida segmentación de el mismo y creación de políticas que cumplan con los estándares necesarios para que la seguridad de la información permanezca.

10.3 CARACTERÍSTICAS

Algunas de las características que este tipo de redes proporcionan son:

- Autenticación
- Integridad
- Privacidad
- Control de acceso
- Registro de actividades
- Calidad de servicio

El uso personal o profesional de estas redes al brindarnos este tipo de características se convierten en una herramienta de uso cotidiano al permitir navegar de manera segura en cualquier red donde nos conectemos y conectemos nuestra VPN, para el uso profesional nos permite realizar la extensión de las aplicaciones que funcionen de manera local y con el fin de mantener el control de las estaciones de trabajo remotas.

10.4 INSTALACIÓN DEL SERVICIO

Iniciamos nuestro proceso de instalación del servidor VPN en Zentyal 6.2 con la selección del servicio VPN tal como se observa en la Figura 66. Luego en el botón instalar al darle clic se realiza la instalación de todos los paquetes que este servicio necesita, una vez finalice no es necesario reiniciar el servidor para que este inicie por lo que podremos iniciar con nuestra respectiva configuración.

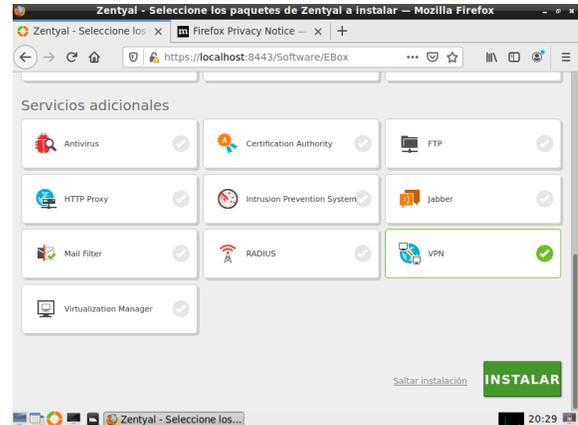


Figura 66. Servicios a instalar

Con nuestro servicio de VPN iniciado, procedemos a crear los certificados de seguridad con los cuales va a funcionar nuestra VPN. Iniciamos creando un "Certificado de Autoridad" y "Certificados Individuales" por cada cliente que se vaya a conectar a nuestra VPN tal como se puede observar en la Figura 67. Al igual que los dos certificados creados es necesario crear un tercer certificado para el servidor VPN, sin embargo, Zentyal, al realizar la creación del "Certificado de Autoridad" dentro del siguiente paso que trata de la creación de un servidor VPN.

Lista de Certificados actual			
Nombre	Estado	Fecha	Acciones
Certificado Autoridad Zentyal Authority Certificate desde Certificado Autoridad Zentyal	Válido	2031-05-17 01:42:23	  
Zentyal/CIIHm	Válido	2031-05-17 01:42:23	  
vpn-VPNZentyal	Válido	2031-05-17 01:42:23	  

 Revocar  Descargar clave(s) y certificado  Renovar o re-emitter

Figura 67. Listado de Certificados

Ahora vamos a crear un servidor de VPN al cual nombraremos como deseemos. Para nuestro servidor asignaremos los siguientes datos:

- **Puerto:** A nuestra elección
- **Dirección VPN:** Asignaremos el pool de direcciones IP libres
- **Certificado de servidor:** Ubicamos el que Zentyal ha creado por nosotros al momento de crear nuestro servidor VPN
- **Traducción de direcciones de red (NAT):** Quedara habilitado indicando que este servidor no sera la puerta de enlace por defecto
- **Servidor de nombres primario:** Ingresamos la dirección IP de nuestra servidor Zentyal.

Esta configuración la tendremos que ubicar en la sección "Configuración del servidor" tal como se muestra en la Figura 69 y el resultado obtenido quedara dentro de las configuración de la Figura 68

Lista de servidores

Habilitado	Nombre	Configuración	Redes anunciadas	Descargar paquete de configuración de cliente	Acción
<input checked="" type="checkbox"/>	VPNZentyl				

Figura 68. Listado de servidores

Configuración del servidor

Puerto del servidor
 UDP puerto 1194

Dirección VPN
 Use una dirección de red que no esté en uso por esta máquina
 192.168.160.0 / 24

Certificado de servidor
 vpn-VPNZentyl

Autorizar al cliente por su nombre común
 Si esta opción se deshabilita, cualquier cliente con un certificado generado por Zentyl podrá conectarse. Si se habilita, solo se podrá conectar con certificados cuyo CN (Common Name) empiece con el valor seleccionado.
 deshabilitado

Figura 69. Configuración del servidor

Con nuestro servidor creado, iremos a nuestro “Dashboard” donde podremos visualizar que nuestro servicio de VPN creado se encuentra operativo y en ejecución. Tal como se observa en la Figura 70.

Servidor VPNZentyl	
Servicio	Habilitado
Estado del demonio	Ejecutándose
Dirección local	Todas las interfaces de red
Puerto	1194/UDP
Subred VPN	192.168.160.0/255.255.255.0
Interfaz de red de la VPN	tap0
Dirección de la interfaz de la VPN	192.168.160.1/24

Figura 70. Comprobación del servicio

Con nuestra VPN creada, debemos indicar que direccionamiento de IP se van a entregar cuando los equipos clientes se conecten a esta. Por esto debemos crear una “Lista de redes anunciadas” tal como se observa en la Figura 71. Luego entramos a la configuración de esta para asignar un “Miembro” el cual tendrá el direccionamiento de la VPN tal como se muestra en la Figura 72.

Lista de redes anunciadas

Red anunciada	Acción
Interna	

Figura 71. Lista de redes anunciadas

Miembros

Nombre	Dirección IP	Dirección MAC	Acción
Test	192.168.6.1/32	--	

Figura 2. Miembros

El paso siguiente inicia dentro de la sección “Lista de servicios”, donde crearemos todos aquellos servicios o reglas las cuales van a dar acceso a partir de nuestra VPN. Es importante mencionar que los servicios y/o reglas que aca se creen, van a interactuar a partir de nuestra VPN permitiendo o denegando el acceso a sitios web, servicios de red, puertos, etc. Por lo que se debe tener claro al momento de realizar la configuración de estas reglas, ya que una sola política podría realizar el bloqueo de toda la navegación LAN o WAN por parte de nuestra VPN. Como visualizamos dentro de la Figura 73, hemos creado 2 servicios con la finalidad de probar estos bloqueos y con el fin de dar más seguridad a nuestro servidor, y se realiza el bloqueo de la administración a nuestro servicio web de Zentyl.

Lista de servicios

Nombre del servicio	Descripción	Configuración	Acción
BloqueoTest	Prueba		
ServiciosTest	--		
Cualquier ICMP	Cualquier paquete ICMP		
Cualquier TCP	Cualquier puerto TCP		
Cualquier UDP	Cualquier puerto UDP		
Cualquiera	Cualquier protocolo y puerto		
HTTP	Protocolo de Transporte de hipertexto		
HTTPS	Protocolo de Transporte de hipertexto sobre SSL		
SSH	Secure Shell		

Figura 73. Lista de servicios

Para finalizar con el proceso de la creación de la VPN, Zentyl nos proporciona una herramienta “Descargar paquete de configuración de cliente” tal como se observa en la Figura 74, mediante la cual podremos exportar la configuración de nuestra VPN indicando si es para un sistema Windows o Linux. Para ambos casos son necesarias las claves de conexión y configuración mediante las cuales realiza la respectiva validación de seguridad para hacer la conexión a nuestra VPN con la excepción de que en Windows descarga dentro de este paquete la aplicación OpenVPN donde cargaremos la configuración de la VPN, sin embargo para Linux podremos implementar estas claves creando una VPN dentro de nuestras opciones de red.

Descargar paquete de configuración de cliente

Tipo de cliente
Windows

Certificado del cliente
ZnetyaClIHM

Anadir instalador de OpenVPN al paquete de configuración del cliente
Instalador de OpenVPN para Microsoft Windows

Estrategia de conexión
Aleatorio

Dirección del servidor
Esta es la dirección que usarán sus clientes para conectarse al servidor. Normalmente, ésta será una IP pública o un nombre de host.

Dirección adicional del servidor (opcional) *Opcional*

Figura 74. Descarga paquete de configuración

Finalmente tenemos una prueba de ejecución de nuestra VPN en un equipo cliente con Sistema Operativo Windows con OpenVPN como cliente VPN

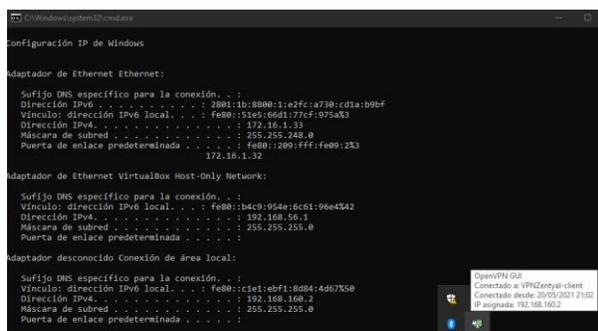


Figura 75. Prueba conexión equipo Windows

Dentro de este Dashboard podemos visualizar las conexiones entrantes a nuestro servidor VPN. Figura 76

Fecha	Evento	Daemon	Tipo	IP remota	Certificado remoto
2021-05-20 12:31:29	Conexión a cliente terminada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM
2021-05-20 12:31:05	Conexión a cliente iniciada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM
2021-05-20 12:28:07	Conexión a cliente iniciada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM
2021-05-20 12:26:02	Secuencia de iniciación completada	VPNZentyal	server		
2021-05-20 11:47:19	Conexión a cliente iniciada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM
2021-05-20 11:45:19	Secuencia de iniciación completada	VPNZentyal	server		
2021-05-20 11:24:29	Conexión a cliente iniciada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM
2021-05-20 11:24:00	Secuencia de iniciación completada	VPNZentyal	server		
2021-05-20 11:22:25	Secuencia de iniciación completada	VPNZentyal	server		
2021-05-20 11:02:46	Conexión a cliente iniciada	VPNZentyal	server	172.16.1.33	ZnetyaClIHM

Página 1

Figura 76. Prueba de conexión del cliente

11 CONCLUSIONES

Zentyal es una herramienta que sin duda facilita la Instalación y administración de paquetes, los cuales pueden ser utilizados dentro de una organización, pero finalmente termina siendo una caja negra donde el administrador no sabe a ciencia cierta qué está sucediendo detrás del dashboard. Para el caso y temática que desarrolle en el presente trabajo, Zentyal realiza las actividades del Proxy basado en Squid, proxy con grandes capacidades de configuración, las cuales no se aprovechan del todo a través de este tipo de

instalaciones, por tal razón sugiero el uso directo de esta herramienta y no a través de Zentyal.

El uso de los servicios DHCP, DNS y controlador de dominio facilitan en gran parte la labor de gestión de usuarios dentro de una red, el DHCP por ejemplo, nos permite asignar de manera aleatoria las IP a los equipos, sin necesidad de estar realizando esta labor de manera manual, el servidor DNS nos brinda una mayor seguridad y a la vez velocidad para la gestión de solicitudes tanto entrantes como salientes y para finalizar el controlador de dominio nos permite asignar permisos o denegarlos a los diferentes usuarios de acuerdo a su rango o estatus dentro de la empresa u organización.

El Firewall, por medio de Zentyal permite tener la flexibilidad dentro de una red estableciendo los parámetros necesarios para la administración y utilización de servicios, los cuales permiten tener una conexión segura por medio de las diferentes políticas creadas. La validación del funcionamiento del cortafuego aplicando las restricciones solicitadas.

El uso de un servidor de impresión, no se necesita depender de un computador primario conectado a la red para poder acceder a la impresora, este tipo de servidores nos permiten que todos los equipos trabajando en la red tengan acceso a él y puedan imprimir sus documentos las 24 horas del día. Adicionalmente si utilizamos un servidor de archivos podremos controlar la cola de impresión y guardar las impresiones realizadas en una carpeta alojada en el servidor donde todos puedan acceder.

12 REFERENCIAS

- [1] Zentyal.org. (2021). Zentyal 6.2 Documentación Oficial [En línea] Disponible en: <https://doc.Zentyal.org/es/>
- [2] Zentyal Server 6.2 Development Now Available - Zentyal Linux Server. (2021). Retrieved 16 May 2021, from <https://Zentyal.com/news/Zentyal-6-2-announcement/>
- [3] File Sharing — Zentyal 7.0 Documentation. (2021). Retrieved 16 May 2021, from <https://doc.Zentyal.org/en/filesharing.html?highlight=files%20sharing>
- [4] CUPS.org. (2021). Retrieved 16 May 2021, from <http://www.cups.org/>
- [5] Sánchez, D. (2021). Cómo crear un script sencillo en Linux. Retrieved 16 May 2021, from <https://rootear.com/ubuntu-linux/como-crear-un-script-sencillo-en-linux>
- [6] "Servicio de redes privadas virtuales (VPN) con OpenVPN — Documentación de Zentyal 7.0", *Doc.Zentyal.org*, 2021. Available: <https://doc.Zentyal.org/es/vpn.html>