INSTALACION E IMPLEMENTACION DE SERVICIOS DE INFRAESTRUCTURA IT EN ZENTYAL SERVER.

Yaqueline Chacón
e-mail: ychaconm@unadvirtual.edu.co
Carlos Fabian Gámez Salamanca
e-mail: cfgamezs@unadvirtual.edu.co
William Alberto Muñoz
e-mail: wamunozj@unadvirtual.edu.co
Eduard Andrés Fernández Peralta
e-mail: eafernanadezp@unadvirtual.edu.co
Fredy Emilio León
e-mail: fleong@unadvirtual.edu.co

RESUMEN: *Este articulo presenta los resultados de la implementación realizada del sistema operativo Zentyal Server, con el cual se configuraron y se pusieron en funcionamiento servicios de infraestructura de tecnologías de información, los cuales brindan los requerimientos básicos de funcionamiento de redes intranet y extranet en una compañía o institución.*
Los servicios implementados en la actividad son: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, Servidor de archivos, Servidor de impresiones y VPN.

ABSTRACT: *This article presents the results of the implementation of the Zentyal Server operating system, with which information technology infrastructure services were configured and put into operation, providing the basic operating requirements of intranet and extranet networks in a company or institution.*
The services implemented in the activity are: DHCP Server, DNS Server, Domain Controller, Non-transparent proxy, Firewall, File Server, Print Server and VPN.

PALABRAS CLAVE: Zentyal server, servicios de infraestructura, administración distribución GNU/Linux y Ubuntu.

1 INTRODUCCIÓN

Zentyal Server es un paquete de software para servidores Linux, este brinda una alternativa a las aplicaciones de servidor tradicionales, como Windows Server, y se basa en Ubuntu y Apache. Zentyal brinda una variedad de servicios de red para poder configurar de forma robusta una infraestructura informática ya que contiene herramientas de seguridad como un cortafuegos, HTTP proxy y VPN, entre otras que permiten que el servidor sea seguro y brindar facilidades de configuración correcta.

La configuración de los servicios planteados nos permitirá generar un paso a paso con los elementos y requerimientos importantes y necesarios en la puesta en marcha de los servicios de infraestructura.

2 INSTALACION Y CONFIGURACION DE ZENTYAL

2.1 RECURSOS NECESARIOS PARA LA INSTALACION

Los requisitos mínimos de hardware para realizar la instalación son:

- Memoria RAM: 64 MB.
- Espacio en disco duro: 1 Gb (Mínimo) – 2 GB (Recomendado).
- Arquitectura: Intel X86-compatible (32 bit), Intel X86_64 (64 Bit).

2.2 DESCARGA

La descarga se realiza desde la página oficial https://zentyal.com/ en donde se realiza inscripción para obtener la versión de prueba por un periodo de 45 días. La versión de prueba contiene todas las características.

2.3 MAQUINA VIRTUAL

La máquina virtual se configuro usando Oracle VM Virtual Box, en donde se define que el sistema operativo es Linux y la versión es Ubuntu (64-bit). Es importante configurar dos adaptadores de red el primero NAT y el segundo Ren Interna.

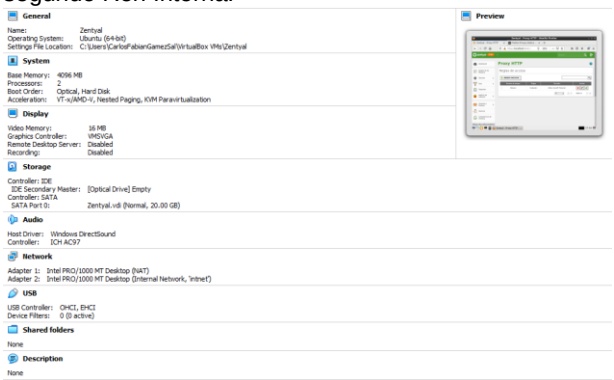

Figura 1. Configuración de la máquina virtual.

2.4 INSTALACION

El primer paso en el proceso de instalación es realizar la selección del idioma de ejecución y con que se configurara el sistema operativo.

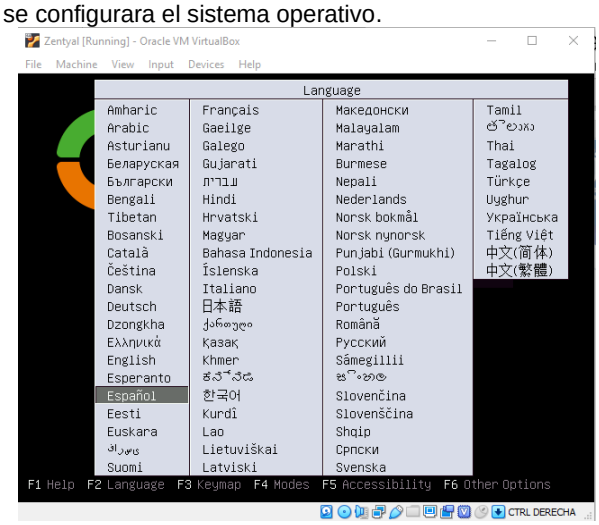

Figura 2. Selección del lenguaje de Zentyal.

Posterior se selecciona el país de ubicación lo cual permite configuración de fecha y hora, así mismo se deberá seleccionar la distribución del teclado.

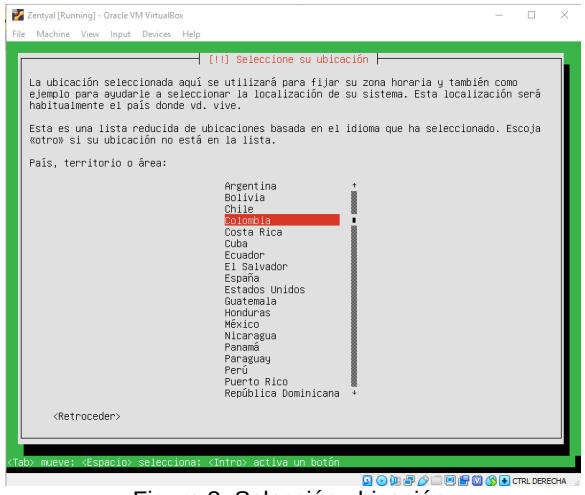

Figura 3. Selección ubicación.

El instalador procederá a realizar la descarga de los componentes requeridos.

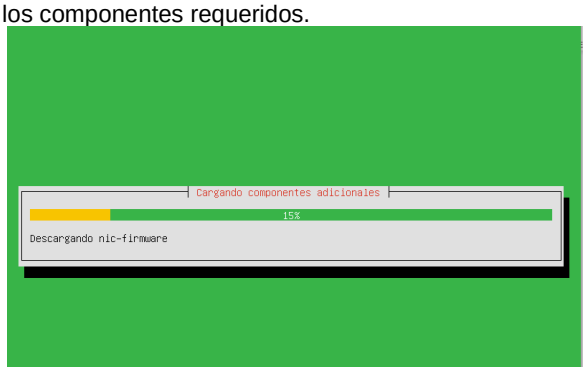

Figura 4. Descarga de paquetes.

Posteriormente es necesario la selección de la interfaz de red primaria que usara el sistema operativo para navegar, a continuación, se debe asignar un nombre a la máquina, y así mismo debemos definir el usuario y clave de acceso al sistema.

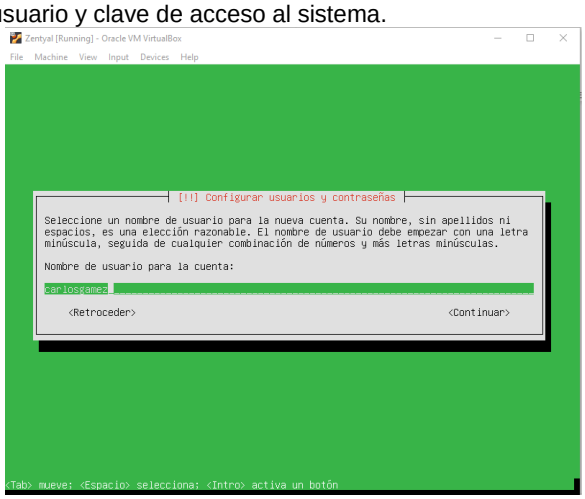

Figura 5. Configuración de usuario.

El asistente procederá a realizar los procesos de instalación de los componentes del sistema una vez este finalice solicitará reinicio para completar toda la instalación de forma correcta.

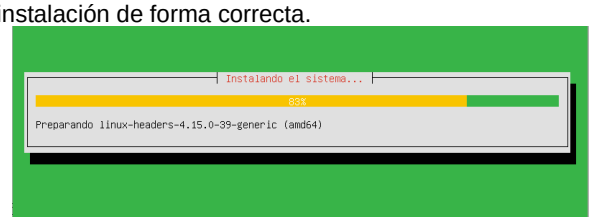

Figura 6. Proceso de instalación de componentes.

Una vez se realice el reinicio del sistema operativo este abrirá un navegador web con la página de acceso a la interfaz de configuración del sistema en el cual se accede con el usuario y clave creados previamente lo que permitirá el acceso al dashboard de Zentyal.

Figura 7. Interfaz de acceso de Zentyal.

3 TEMATICAS PLANTEADAS

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

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

DESARROLLO

Posterior a la descarga de Zentyal, se visualizan los siguientes paquetes para instalar.

Figura 8. Visualización de paquetes a instalar

Al dar clic en “Instalar” Zentyal informa que se instalarán los siguientes paquetes:

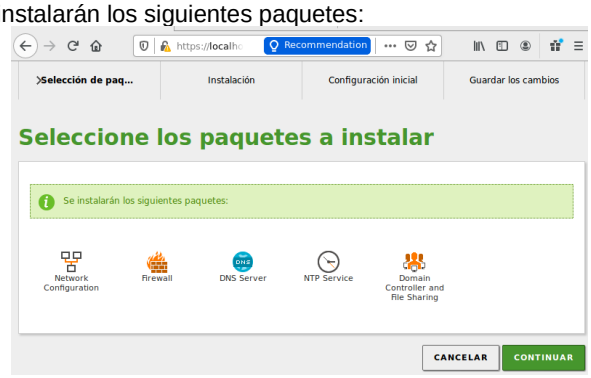

Figura 9. Paquetes a instalar

Damos clic en “Continuar” y empezará la instalación de los paquetes:

Figura 10. Instalación de paquetes

Luego debemos configurar las interfaces, de manera que “eth0” será para la red WAN (External) y la interface “eth1” será para la red LAN (Internal):

Figura 11. Configuración de Interfaces

Ahora configuramos la red para interfaces externos:

Figura 12. Tipo de servidor

Mensaje que aparece luego de la instalacion:

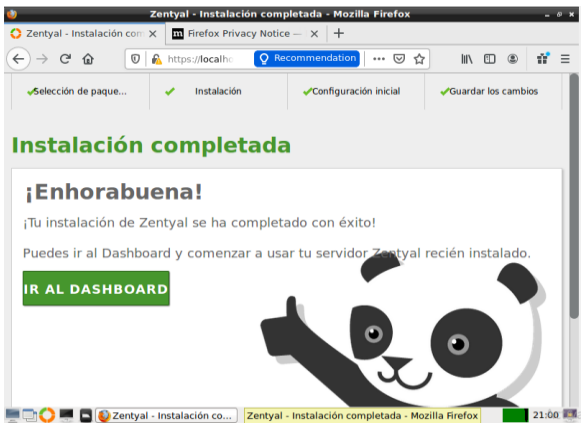

Figura 13. Instalación completada

Configuración de DHCP

Al ir al DashBoard, en el Estado de Módulos observamos que DHCP se encuentra deshabilitado:

Figura 14. Configuración de DHCP

En “Estado de los Módulos” activamos DHCP y guardamos los cambios:

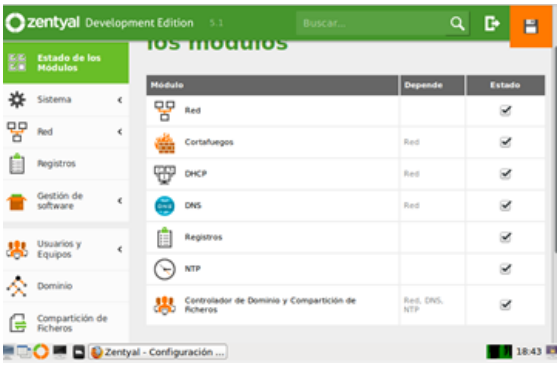

Figura 15. Estados de los módulos

Ahora vamos al DHCP y configuramos la interfaz:

Figura 16. Configuración de interfaz

Ahora abrimos el Ubuntu Desktop para verificar que la IP se haya dado por DHCP y observamos que le fue asignada la siguiente IP:

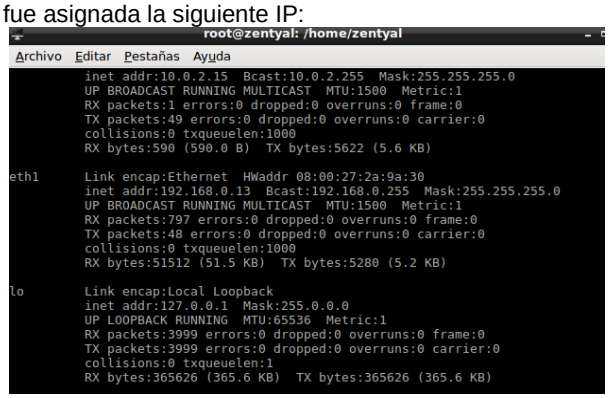

Figura 17. IP Ubuntu desktop

Configuración DNS: En el DashBoard seleccionar a “Habilitar el caché de DNS transparente”, damos clic a “Cambiar” y luego guardamos los cambios:

Figura 18. Habilitación de Caché

Configuración controlador de dominios

Inicialmente, vamos a Dominio y verificamos que el reino y el nombre del dominio correspondan. Adicionalmente habilitamos perfiles móviles, damos clic en cambiar y guardamos cambios:

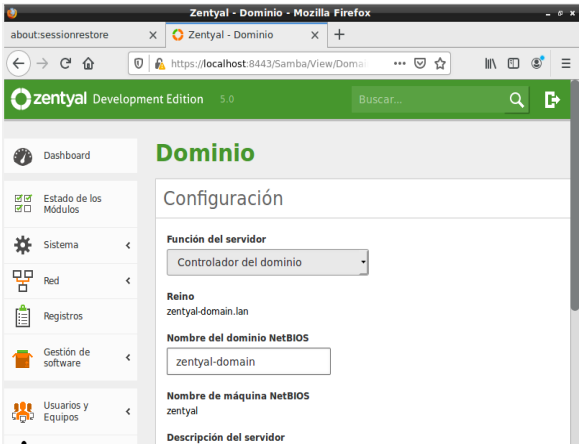

Figura 19. Configuración de dominio

Ahora en “Usuarios y Equipos” observamos que no existen computadores, grupos ni usuarios:

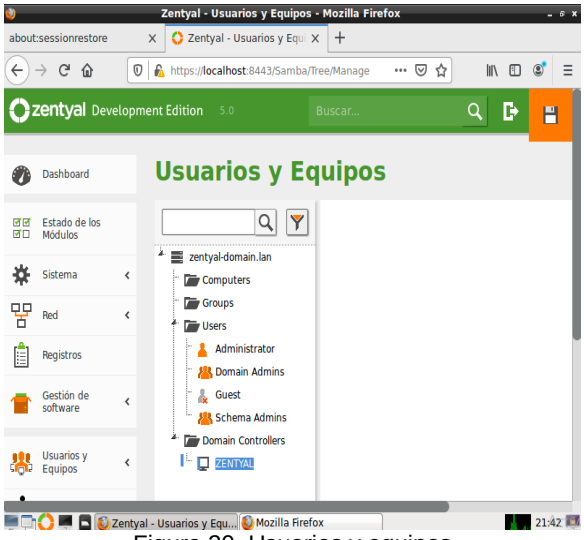

Figura 20. Usuarios y equipos

Se añade el usuario:

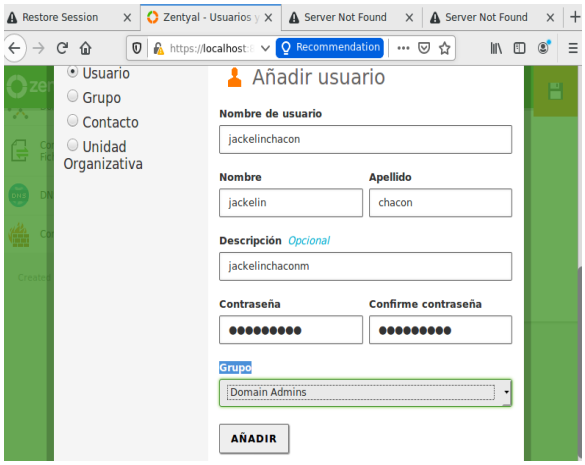

Figura 21. Añadir usuario

Ahora en el Ubuntu Desktop verificamos el hostname con el siguiente comando:
nano /etc/hostname

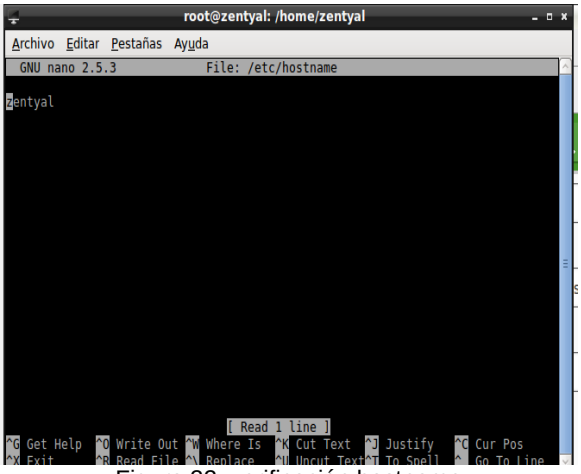

Figura 22. verificación hostname

Ahora en la funcionalidad de switch, en la parte de hosts quitamos “mdns4_minimal [NOTFOUND=return]

Ahora en Firefox vamos a la página oficial de PowerBroker Identify Services (PBIS):

https://repo.pbis.beyondtrust.com/apt.html

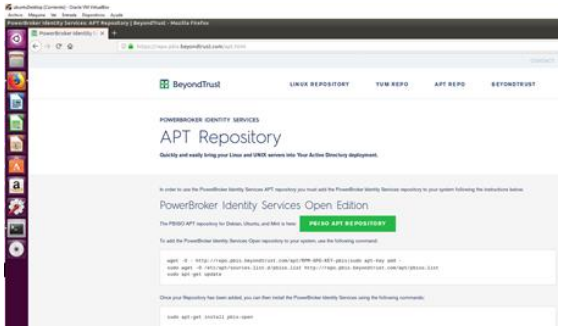

Figura 23. Página oficial de PowerBroker

Reiniciamos, abrimos la terminal y ejecutamos el comando sudo –i:

Finalmente, se logra el objetivo y en Zentyal ya se observa que el equipo está inscrito en el dominio:

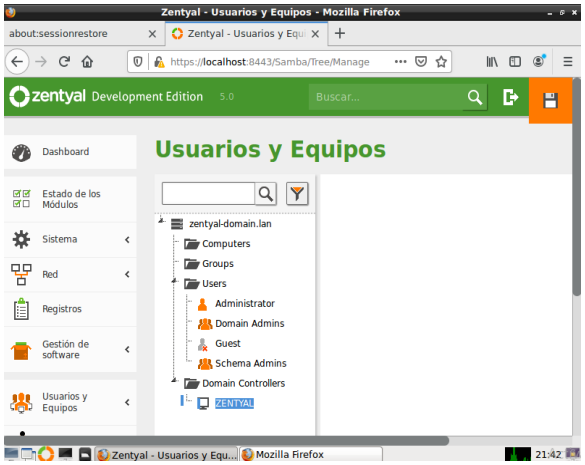

Figura 24. Inscripción del Dominio

3.2 PROXY NO TRANSPARENTE

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

DESARROLLO

Al ingresar a la consola de Zentyal es necesario realizar la selección e instalación de los módulos a configurar se usarán el HTTP Proxy, Controlador de dominio y compartición de archivos y DHCP Server.

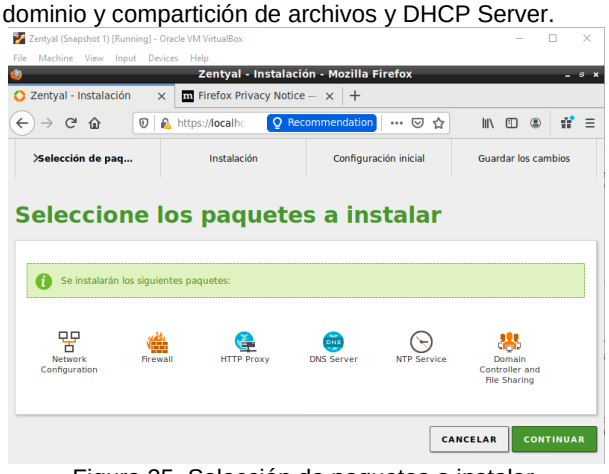

Figura 25. Selección de paquetes a instalar.

Una vez seleccionados los servicios necesarios procedemos a configurar las interfaces de red: eth0 sea tipo externo ya que será la fuente de internet y la interfaz eth1 será tipo interno ya que brindara servicios a los

equipos de red, es requerido adicionar una IP estática a la interfaz de red eth1.

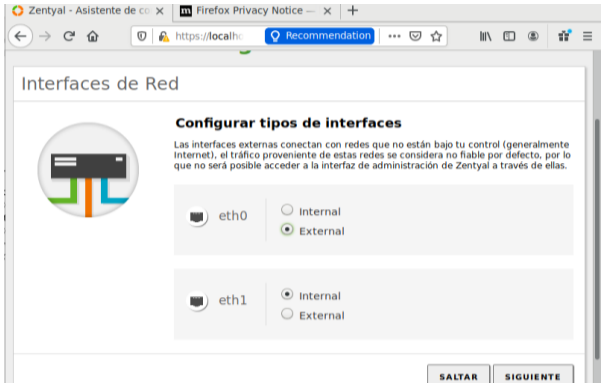

Figura 26. Configuración interfaces de red.

Es necesario realizar la configuración de un rango de IP's para que sean asignadas, se ingresa al menú DHCP y seleccionamos configuración, se configura en la pestaña de Opciones personalizada la información indicada

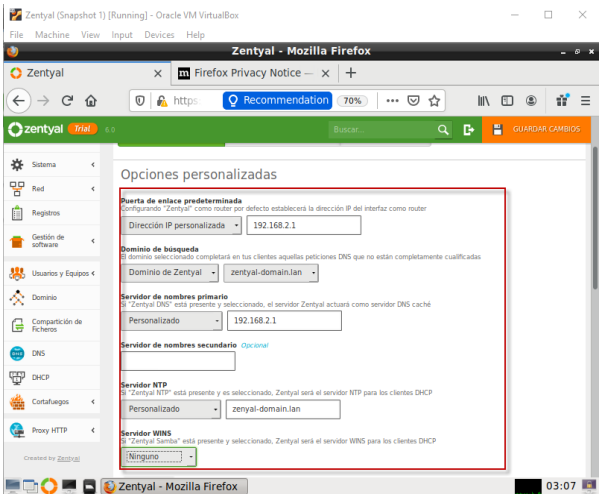

Figura 27. Configuración DHCP Server.

Desde la pestaña Opciones de DNS dinámico procederemos a realizar la configuración del rango de IP's que se podrán asignar, definimos el rango y un nombre y seleccionamos la opción añadir.

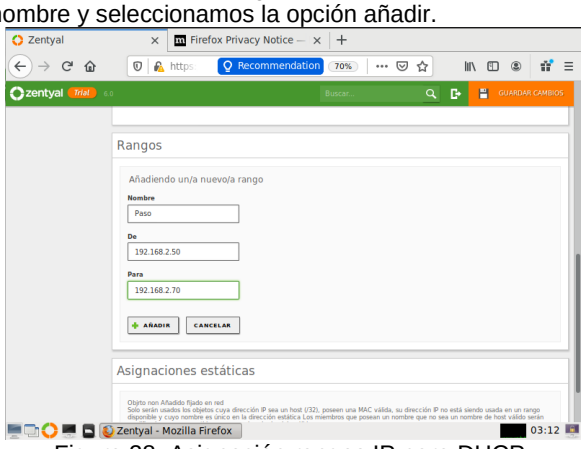

Figura 28. Asignación rangos IP para DHCP.

En el equipo desktop configuramos el adaptador de red como Red Interna, esto permitirá que Zentyal le asigne una de las IP que están en el rango configurado en el paso previo.

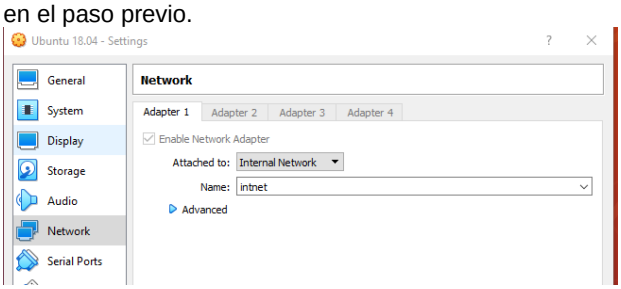

Figura 29. Configuración adaptador de red Ubuntu Desktop.

Cuando la maquina desktop es encendida y la red la detecta asigna la IP y en el dashboard de Zentyal podemos verificar esta conexión.

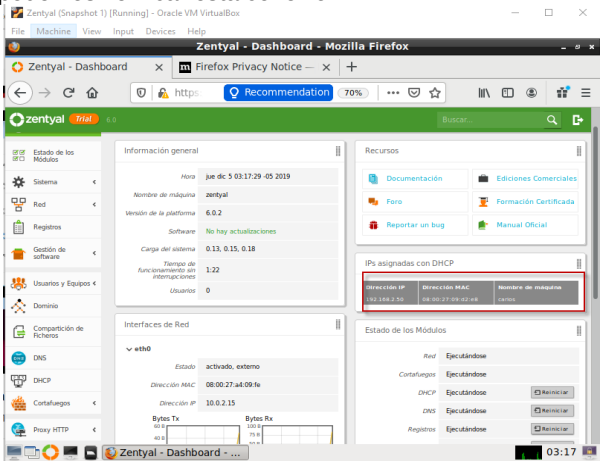

Figura 30. Dashboard con IP en uso con DHCP.

Ahora debe realizarse la configuración del HTTP Proxy debemos ingresar a esta sección y seleccionar la opción Perfiles de filtrado, con esto añadiremos el perfil que deseemos.

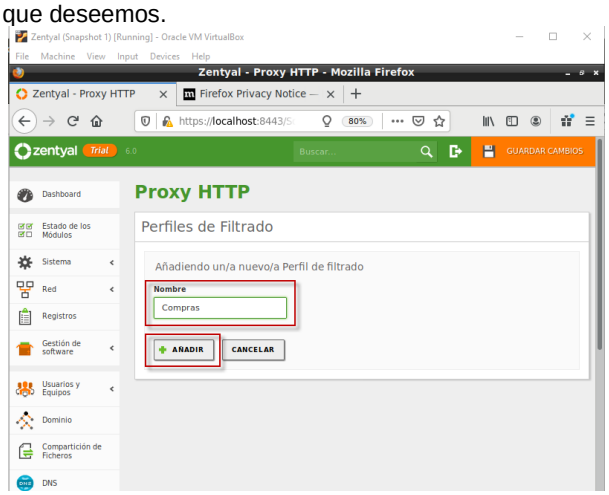

Figura 31. Creación de perfile de filtrado.

Una vez creado el perfil, se debe realizar la configuración del filtrado, para esto definimos el Umbral que indicara que tan estricto es el filtro.

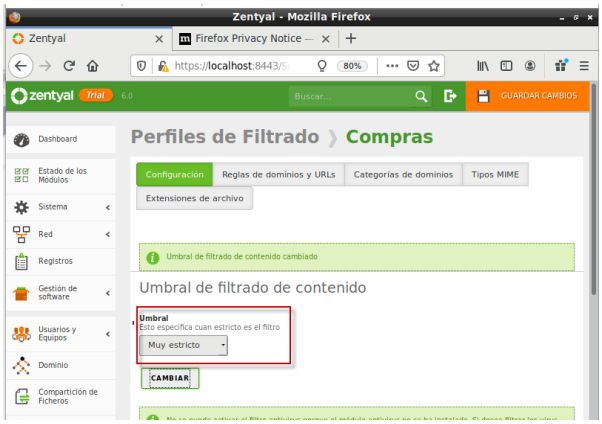

Figura 32. Definición umbral del filtrado del perfil.

En la pestaña de Reglas de dominios y URLs se define la configuración del filtrado existen tres opciones que permiten crear reglas globales las cuales se complementaran con la información de filtrado de los sitios usando el dominio de estos.

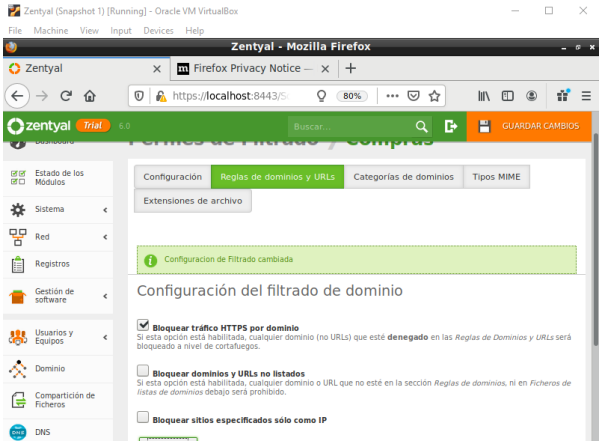

Figura 33. Configuración de filtrado del dominio.

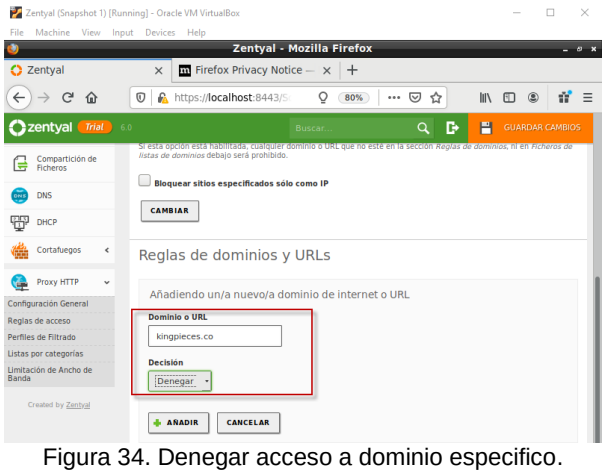

Figura 34. Denegar acceso a dominio especifico.

Finalmente debemos añadir la regla en la que asociemos el perfil de filtro creado la regla permitirá definir el periodo de tiempo, el origen y la decisión en donde seleccionaremos el perfil previamente creado.

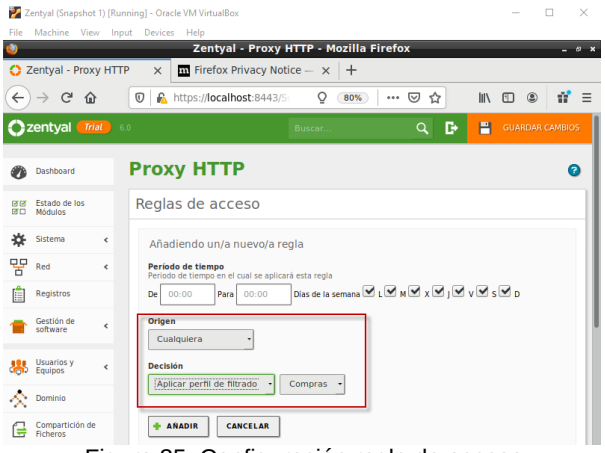

Figura 35. Configuración regla de acceso.

Procedemos a guardar los cambios y Zentyal configurara estos al finalizar nos indicara el resultado.

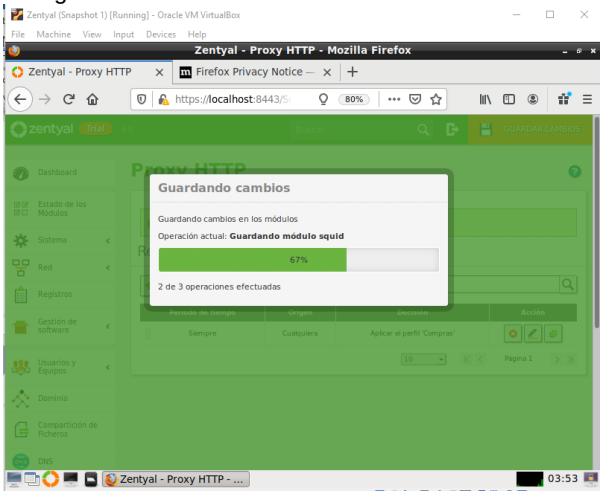

Figura 36. Aplicar perfiles y regla de filtrado.

Para realizar la verificación del funcionamiento de la regla ingresamos al equipo Ubuntu Desktop, en donde y realizamos en primera instancia una prueba abriendo en el navegador la página que hemos restringido.

Figura 37. Navegación equipo desktop.

Activamos el proxy en el Ubuntu Desktop colocando la IP asignada a la interfaz de red de Zentyal.

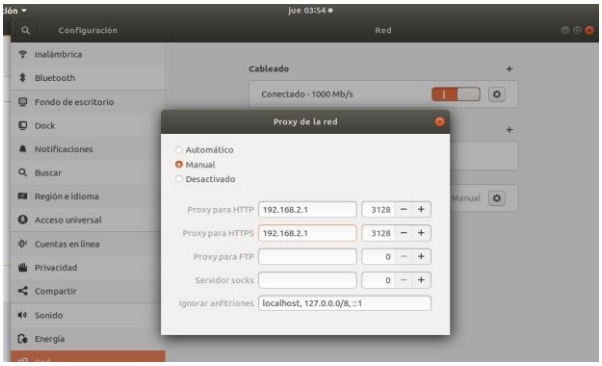

Figura 38. Ajuste proxy del sistema desktop.

Debido a que es un proxy no transparente debemos indicar al navegador web que usemos como debe proceder para esto seleccionaremos la opción que tome el proxy del sistema.

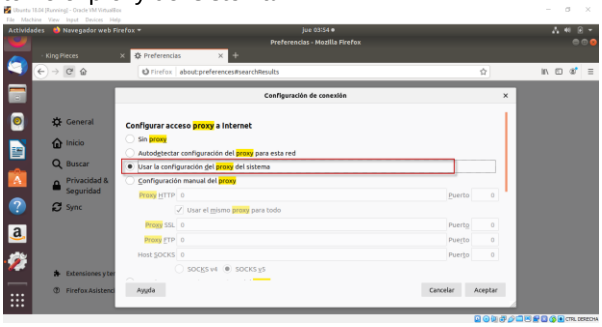

Figura 39. Ajustes proxy del navegador web.

Finalmente para verificar el funcionamiento de la regla procedemos a ingresar a la pagina definida en el filtro en donde esta no carga.

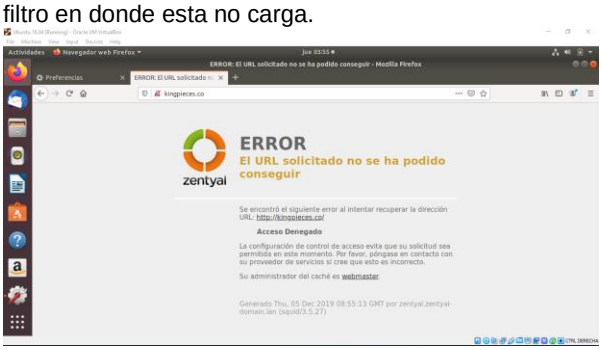

Figura 40. Comprobación bloqueo del proxy

Para garantizar que no hubo afectación en la navegación de otros sitios web verificamos cargando una página diferente.

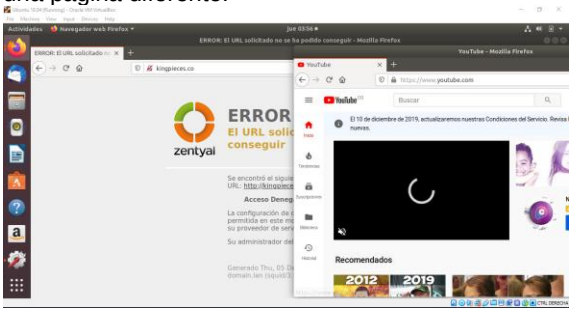

Figura 41. Verificación funcionamiento navegación.

3.3 CORTAFUEGOS

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

DESARROLLO

En la primer pantalla nos indica que paquetes deseamos instalar, con lo cual seleccionamos los paquetes de DNS Server, DHCP Server y Firewall.

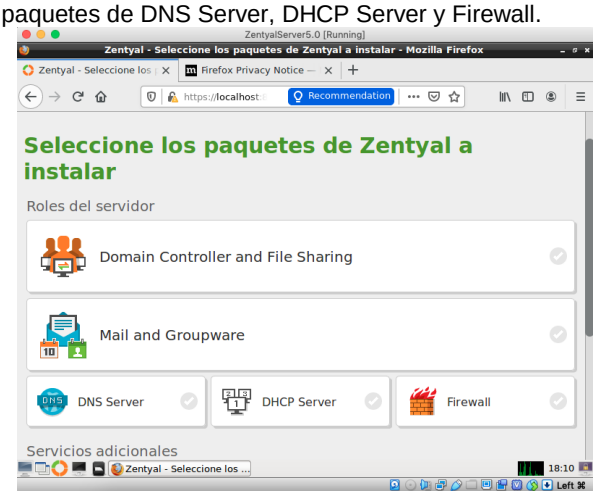

Figura 42. Selección de paquetes.

Se realiza la Instalación de los paquetes normalmente.

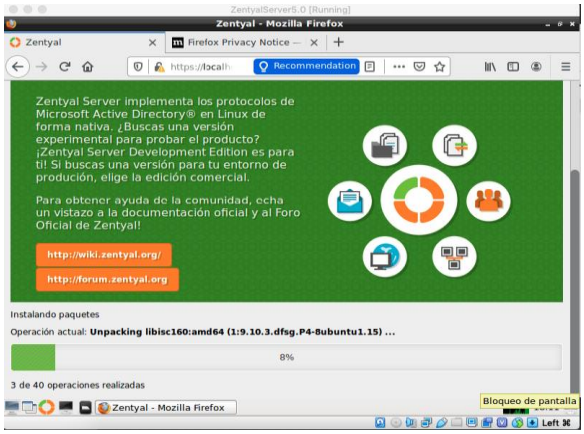

Figura 43. Instalación de paquetes

Ahora vamos a continuar con la configuración de las interfaces.

La primer interfaz (eth0) le asignamos el método DHCP y lo realmente importante acá es habilitar la opción de Externo WAN, para que nuestro server, se pueda conectar a Internet, quedando como lo muestra la siguiente imagen:

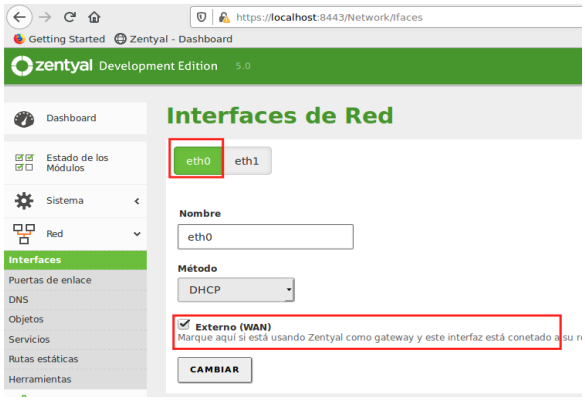

Figura 44. Configuracion interfaces de red

Habilitamos una segunda interfaz de red, que será la cual tenga la ip de server, asignando un método estático, la ip del server, tal como se muestra en la siguiente imagen.

Figura 45. Configuracion direccionamuento estatico

Ahora vamos a realizar continuación, la asignación de rangos para reconocer los PC clientes.

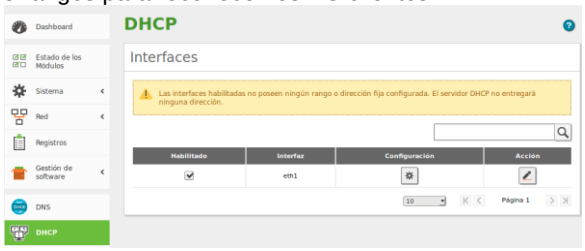

Figura 46. Configuración de rangos

Definimos cuál será el rango de asignación de IP que ofrece nuestro servidor.

Figura 47. Asignacion rango IP.

Vemos que el rango a quedado agregado, ahora guardamos los cambios.

Figura 48. Cambios guardados

Vamos a comprobar que ahora nuestro pc cliente ubuntu, con una configuración en su interfaz de red, como tipo “Red interna” es capaz de ser reconocido por nuestro server y a su vez, tomar por medio del DHCP una dirección IP, que debe estar dentro del rango establecido anteriormente.

Entonces encendemos nuestra máquina Ubuntu, y vamos a consultar su IP actual.

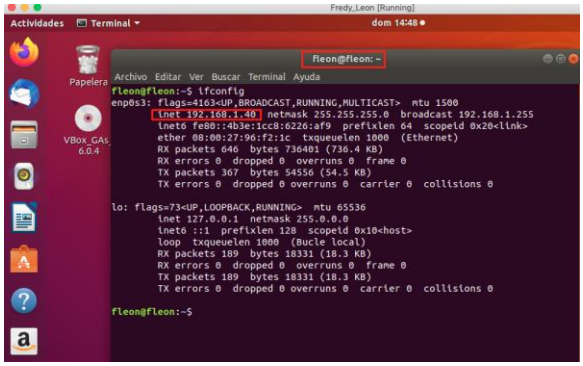

Figura 49. IP equipo desktop

Vemos que ahora su IP, está dentro del rango que definimos anteriormente, Ahora si vamos a nuestro server, en el dashboard, podemos ver que nuestra máquina cliente ya aparece dentro de la lista de Ip’s asignadas.

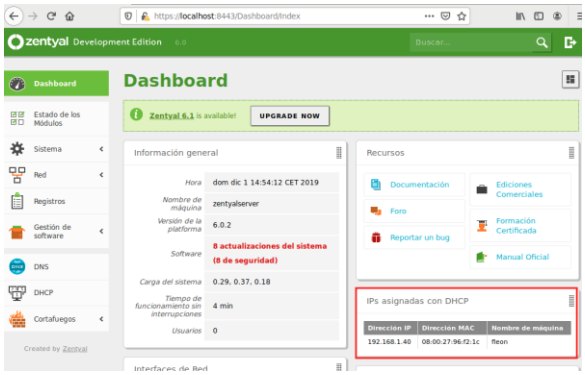

Figura 50. Verificacion DHCP

Antes de aplicar y crear nuestra regla de firewall, vamos a comprobar que nuestro PC cliente puede acceder a la página de "Youtube", que será la que posteriormente bloquearemos por medio de una regla.

Figura 51. Navegación equipo desktop

Vemos que puede ingresar sin problema alguno, con lo cual ahora vamos a consultar cual es la IP del sitio "YouTube" para poder agregarla a nuestra regla, entonces lo hacemos de la siguiente manera, como se ve en la imagen a continuación.

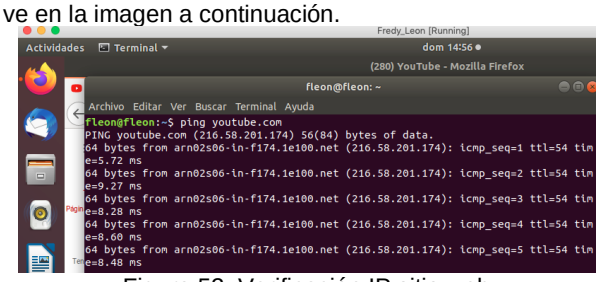

Figura 52. Verificación IP sitio web

Vemos que la IP es la 216.58.201.174, que será la que agregaremos en nuestra regla.
En este punto vamos a crear la regla, donde la definimos de la siguiente manera.
Decisión: Permiso o restricción a otorgar.
Origen: IP en específica o General todos.
Destino: Aquí es donde ingresamos la IP del sitio "YouTube"
Servicio: Servicio a ofrecer o denegar.
Descripción: Alguna comentario acerca del sitio a gestionar.
La configuración final para esta regla a quedado de la siguiente manera.

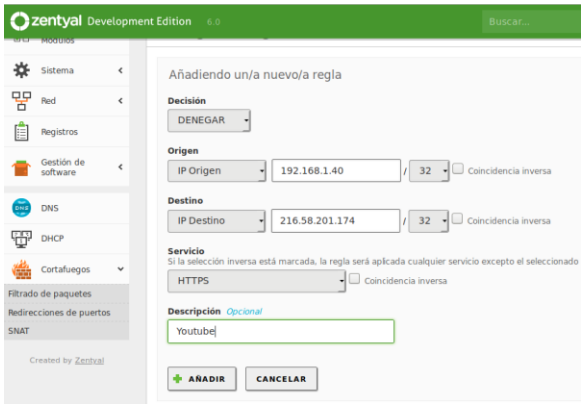

Figura 53. Creación regla firewall

Añadimos y guardamos los cambios.

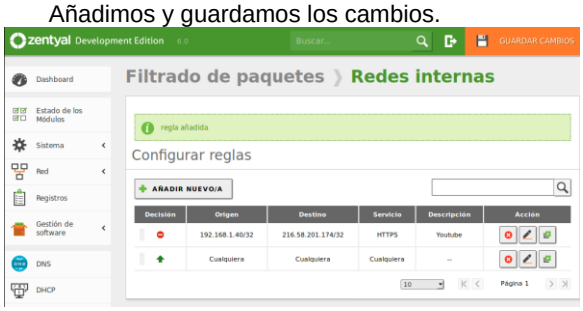

Figura 54. Configuración regla firewall

Finalmente vamos a nuestro PC Cliente, y tratamos de acceder al sitio "YouTube" y vemos que ahora no es posible.

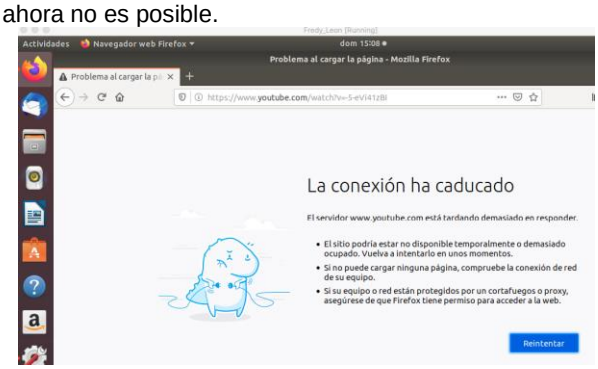

Figura 55. Verificación equipo desktop regla

3.4 FILE SERVER Y PRINT SERVER

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

DESARROLLO

Luego seleccionaremos los paquetes Zentyal que vamos a instalar, para nuestra temática el más importante es el "Domain controller and file sharing".

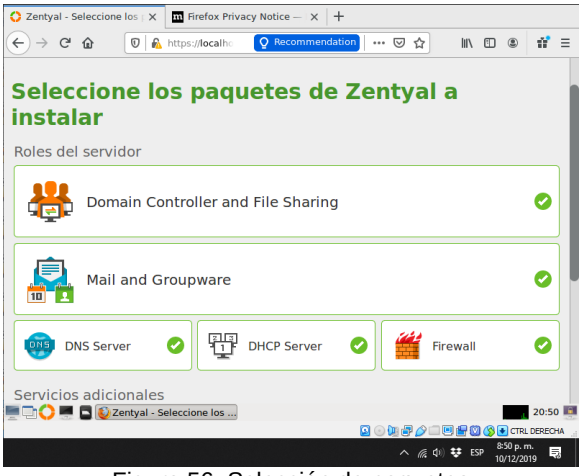

Figura 56. Selección de paquetes

En el asistente de configuración inicial encontramos el tipo de adaptador de red a configurar, en este caso seleccionamos interno.

Figura 57. Configuracion interfaces de red

Ahora lo configuraremos de manera estática y asignaremos la ip, también el nombre de dominio.

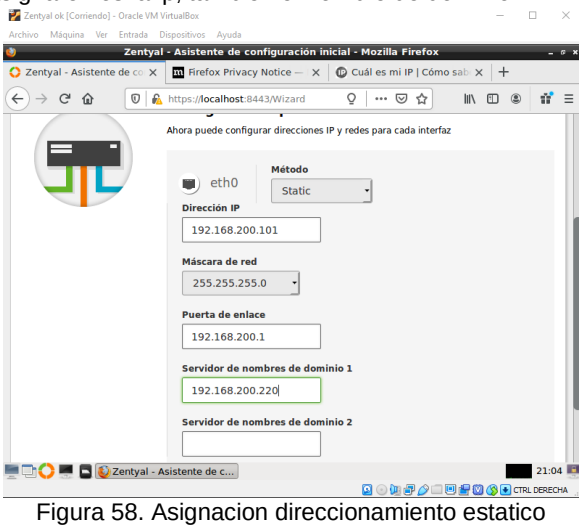

Figura 58. Asignacion direccionamiento estatico

Este es el menú principal del dashboard en el que encontramos módulos de configuración tales como; usuarios, equipos, dominio, compartición de archivos.

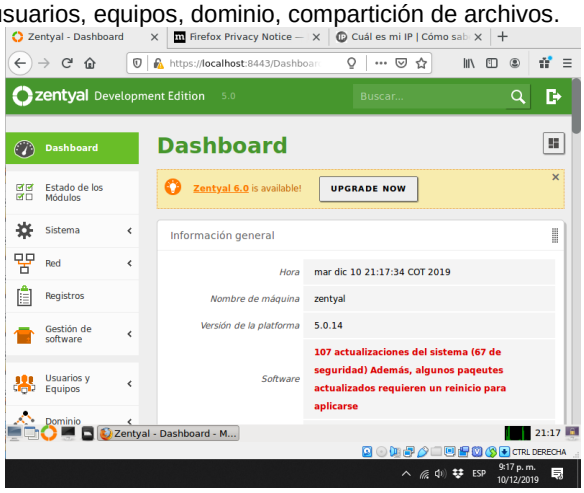

Figura 59. Módulos de configuración

Añadimos un grupo a nuestro dominio, el grupo será tipo distribución.

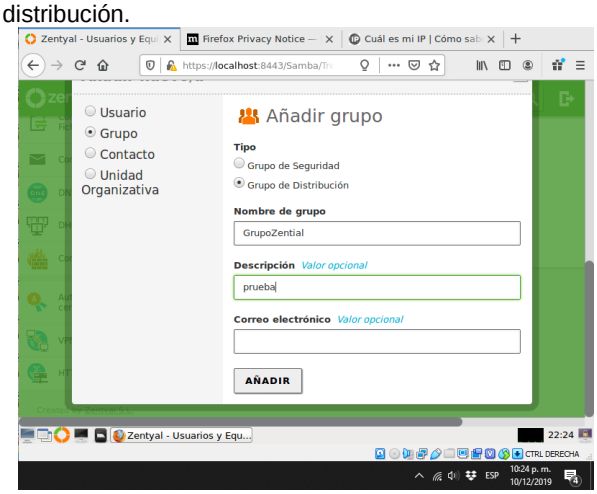

Figura 60. Creación grupo

Ahora procedemos a crear un usuario.

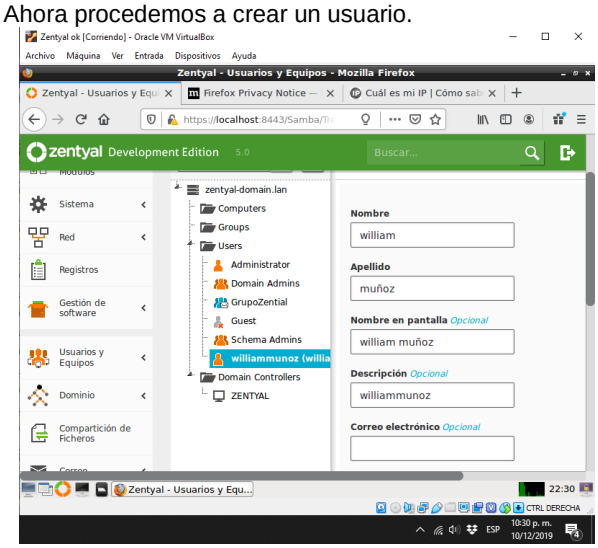

Figura 61. Creación usuario

Este usuario creado lo agregamos al grupo previamente creado.

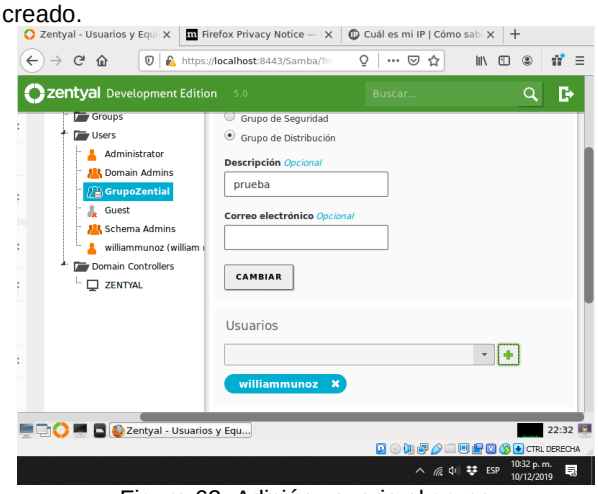

Figura 62. Adición usuario al grupo

Ahora crearemos una carpeta que se llamará, "Compartida Windows" la cual se verá en nuestro equipo Windows.

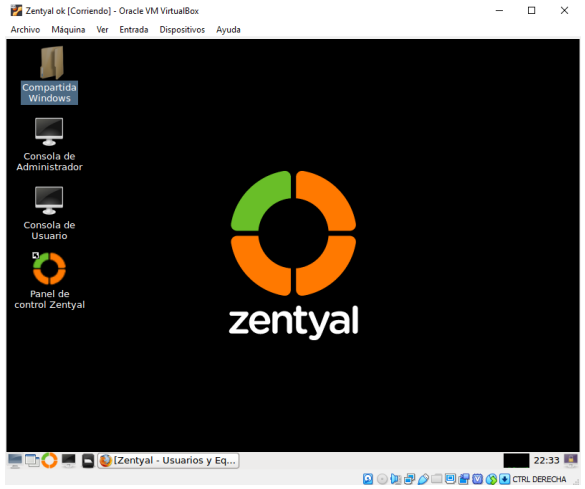

Figura 63. Carpeta compartida

Editaremos los permisos de control de acceso, en acceso, lectura y escritura a "cualquier usuario".

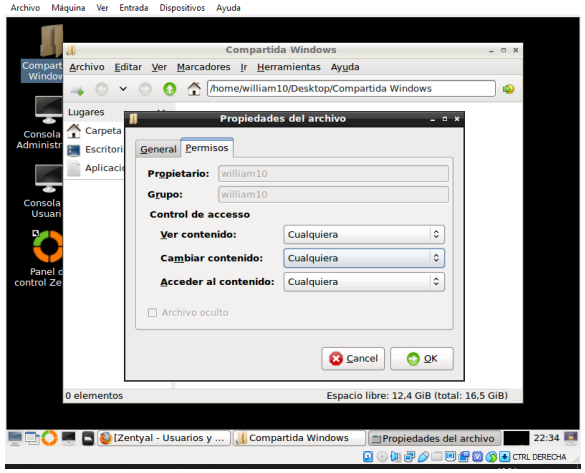

Figura 64. Asignación permisos

Vamos ahora en el dashboard al menú "compartición de archivos" y en el directorio compartido pondremos la ruta del sistema de ficheros.

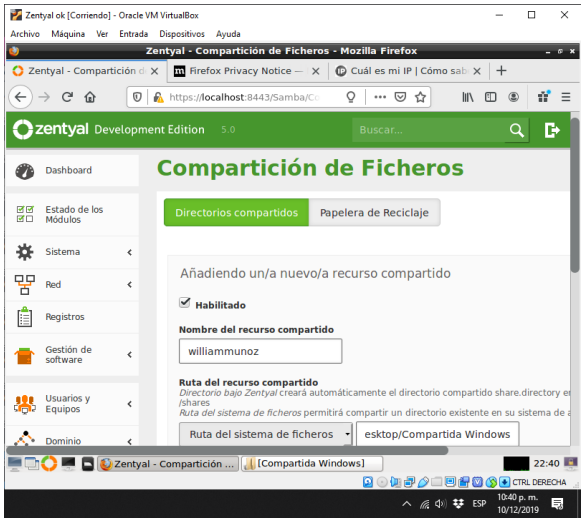

Figura 65. Asignación de ruta

Vemos que se añadió correctamente nuestro directorio compartido.

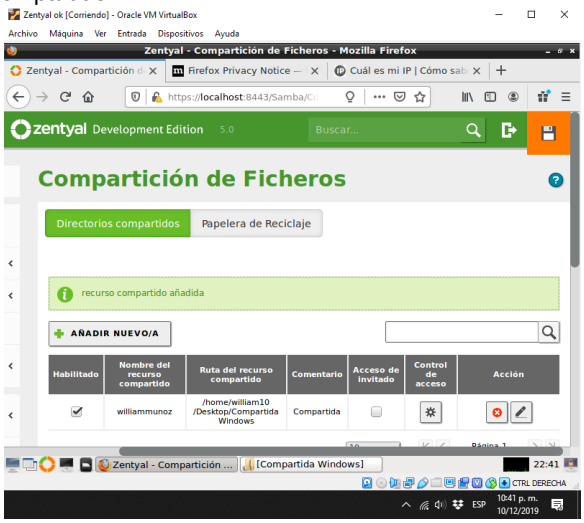

Figura 66. Verificación fichero compartido

Por último verificamos nuestra ip de acceso al equipo, y en Windows con esta ip verificamos la conexión a nuestra carpeta compartida.

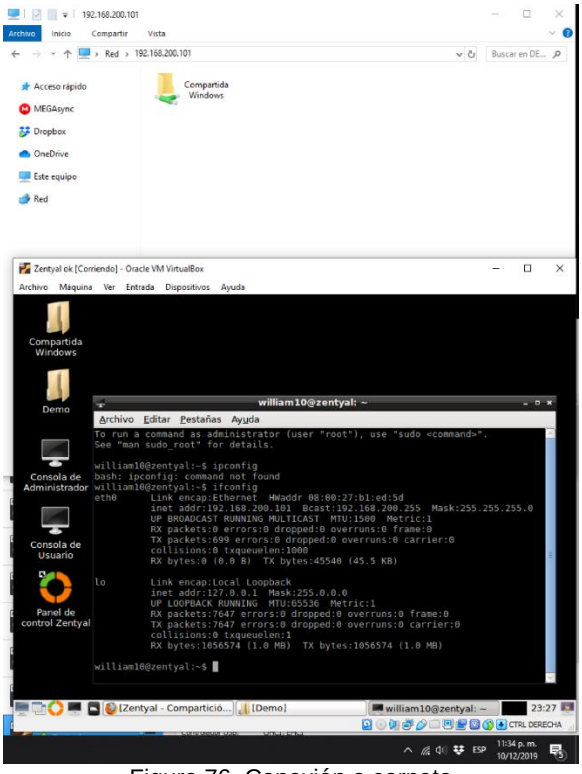

Figura 76. Conexión a carpeta

3.5 VPN

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

DESARROLLO

Se debe crear certificados, uno para el servidor y otro para los clientes que se quieren conectar. Iniciamos con el certificado del servidor, para ello vamos a "Autoridad de certificación". Ingresamos un nombre de la organización, CO para Colombia en código del país, dejamos el resto de los valores por defecto y damos clic en "Crear".

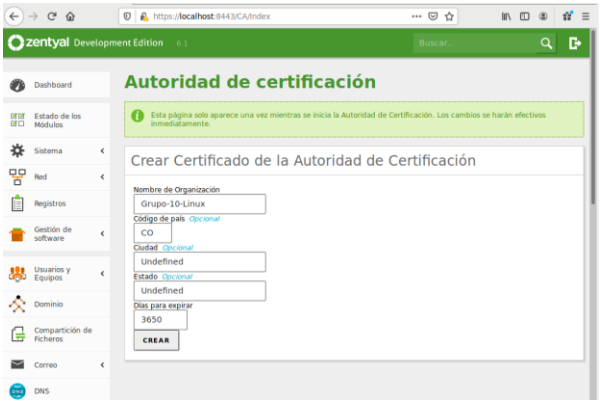

Figura 68. Creación de certificado servidor

Ahora vamos a crear el servidor VPN, nos dirigimos a la opción VPN y luego "Servidores VPN" y damos clic en el botón "+Anadir nuevo/a".

Le colocamos un nombre para este caso "vpn-server" y quitamos el check en "Habilitado" ya que más adelante lo haremos cuando tengamos la configuración terminada.

Figura 69. Creación de certificado

Con esto ya quedó el servidor VPN creado.

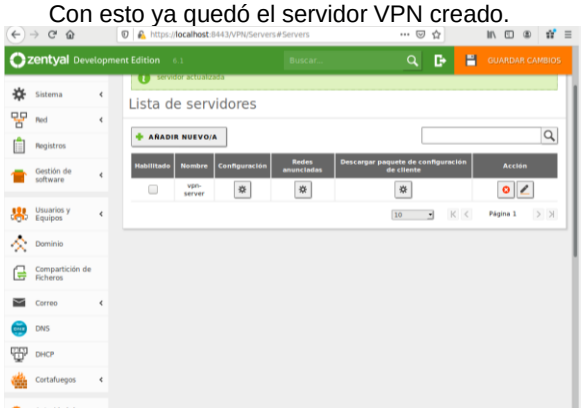

Figura 70. Lista de servidores VPN

Accedemos a "Autoridad de certificación" y creamos un nuevo certificado para los clientes que se van a conectar a la VPN. Le damos un nombre: "Certificado-vpn", le dejamos 365 "Días para expirar" y damos clic en el botón "Expedir".

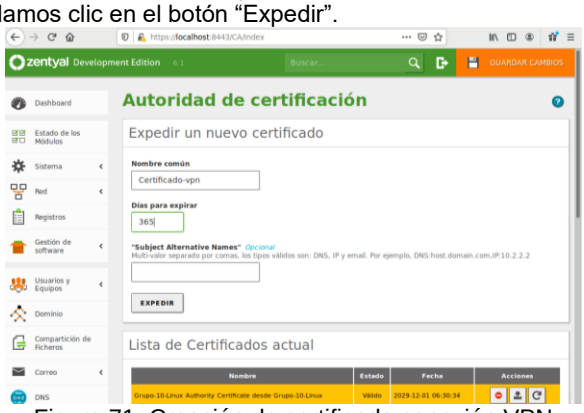

Figura 71. Creación de certificado conexión VPN

Ahora vamos al menú “VPN” luego “Servidores” y en servidor “vpn-server” damos clic en el botón de configuración. Dejamos los valores por defecto en “Puerto del servidor” UDP puerto 1194 y dirección VPN 192.168.160.0/24. En “Certificado de servidor” seleccionamos el certificado creado “Certificado-vpn”. Habilitamos la opción “Interfaz TUN”.

Figura 72. Configuración servidor VPN

Vamos al final y damos clic en el botón “Cambiar”. Se crear las reglas del firewall para que permita el acceso a la red VPN. Vamos a “Red” y luego a la opción “Servicios”. Damos clic en el botón “+Anadir nuevo/a”.

Le damos un nombre al : “servicio-vpn”, una breve descripción y damos clic en el botón “+Añadir”.

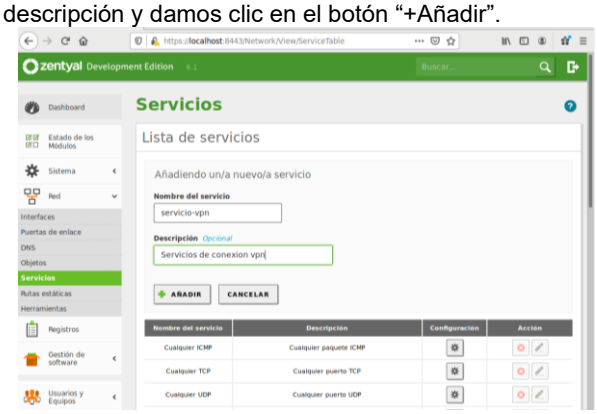

Figura 73. Creación de servicio para VPN

Damos clic en “Configuración” del servicio recién creado. Seleccionamos el protocolo de la conexión VPN que es UDP y en Puerto destino seleccionamos Puerto único y colocamos 1194.

Figura 74. Configuración servicio VPN

Se añade a las excepciones del firewall el servicio que hemos creado para la VPN, para ello vamos a la opción “Contrafuegos” y luego a “Filtrado de paquetes”, ingresamos “Configurar reglas” en la opción “Reglas de filtrado desde las redes internas a Zentyal”. Damos clic en “Anadir nuevo/a”. En “Servicio” seleccionamos el servicio de la VPN “servicio-vpn” y damos clic en “+Añadir” dejando los demás valores por defecto.

Figura 75. Creación de regla de firewall

A continuación, requerimos configurar la conexión de redes anunciadas, vamos a “Servidores VPN” y en servidor VPN “vpn-server” damos clic “Redes anunciadas”.

Antes de seguir con la configuración, necesitamos la dirección pública de nuestro ISP para ello vamos a la página “who.is” y tomamos la dirección IP donde dice “Your IP address is”. Ahora nos dirigimos de nuevo a “VPN” luego “Servidores” y damos clic en la opción “Descargar paquete de configuración de cliente” de nuestro servidor VPN “vpn-server”. En tipo de cliente seleccionamos “Windows”, en certificado de cliente “vpn-vpn-server”, dirección del servidor colocamos la dirección pública del router “186.84.89.231”.

Figura 76. Configuración paquete de descarga de configuración de cliente

Y luego damos clic en el botón “Descargar” y guardamos el paquete en una ubicación del servidor para luego ser enviado al cliente.

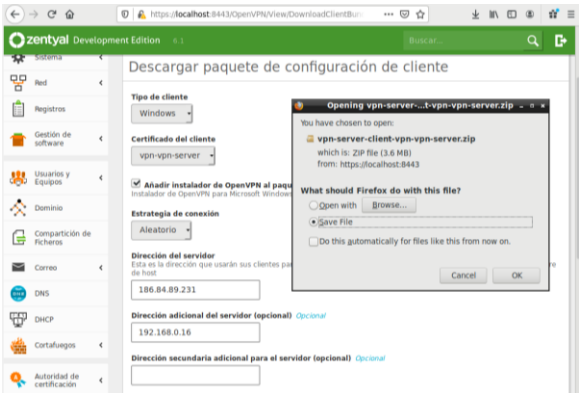

Figura 77. Descarga paquete cliente VPN

Vamos nuevamente a “VPN” luego en “Servidores” y seleccionamos “habilitado” en “vpn-server”. Para terminar, damos clic en “Guardar cambios”.

Figura 78. Habilitación servidor VPN

En el Dashboard, vamos a “Demonios OpenVPN” y validamos que el servicio se encuentre habilitado y que el estado del demonio se encuentre en “Ejecutándose”.

Para validar el funcionamiento de la VPN, vamos a tomar remotamente unos de los equipos de la red LAN desde un equipo externo a la red. Para ello, habilitaremos el control remoto del equipo con Ubuntu Desktop. En la máquina con Ubuntu Desktop que se encuentra en la red LAN, buscamos la opción “Compartir”. Luego en la opción compartir habilitamos la opción con el botón compartir damos clic en “Compartición de la pantalla” seleccionamos “Permitir conexiones para controlar la pantalla”, habilitamos “Solicitar una contraseña” y le asignamos una y en redes seleccionamos la red LAN disponible en el equipo, para este caso “Red cableada 1”.

Figura 79. Creación de certificado

Ahora debemos desactivar el cifrado de la conexión remota, para ello vamos a la terminar en el Ubuntu Desktop y digitamos “$ gsettins set org.gnome.Vino require-encryption false”.

Validamos la configuración de red de la máquina virtual con Ubuntu Desktop debe estar en la red interna y tomar dirección por DHCP dentro del segmento de red del servidor. Ahora descargamos el paquete del certificado de la VPN para Windows y lo instalamos en un equipo externo a la red LAN. Dentro del paquete se encuentra el instalador para Windows, realizamos la instalación siguiendo el Wizard.

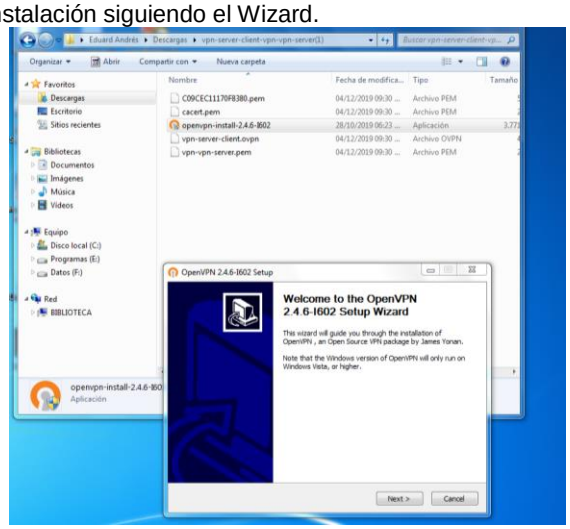

Figura 80. Instalación OpenVPN en equipo cliente

Al terminar, copiamos los demás archivos de la configuración del certificado VPN a la ruta “c:\usuarios\ “usuario”\OpenVPN\config”. Al terminar, buscamos el ícono de OpenVPN en la barra del reloj, damos clic derecho y damos “Connect”.

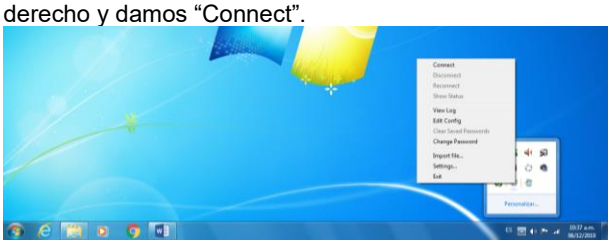

Figura 81. Conexión a la VPN desde equipo cliente

Al terminar, el ícono cambia de color verde y da un resumen que se encuentra conectado, con una asignación de IP 192.168.160.6. Abrimos un cliente de conexión VNC que para este caso será UltraVNC Viewer, colocamos la dirección IP de la máquina Ubuntu Desktop 10.0.0.15 y damos clic en el botón “Connect”.

Nos solicita la clave de conexión remota que asignamos cuando compartimos el escritorio, la ingresamos y damos clic en “Log On”.

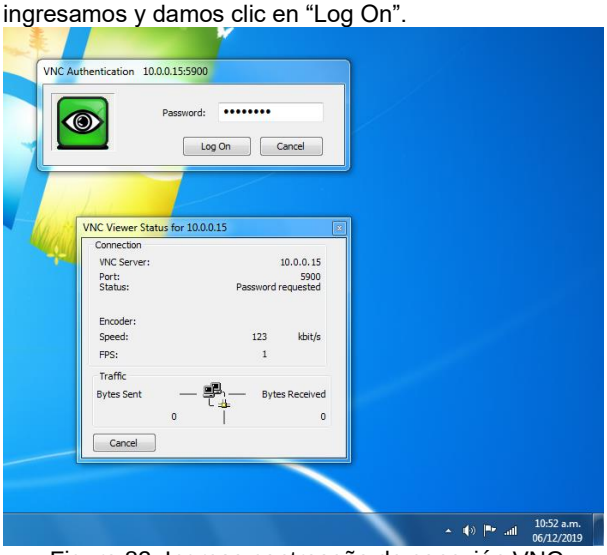

Figura 82. Ingreso contraseña de conexión VNC

Al terminar, se conecta correctamente a la máquina de forma remota.

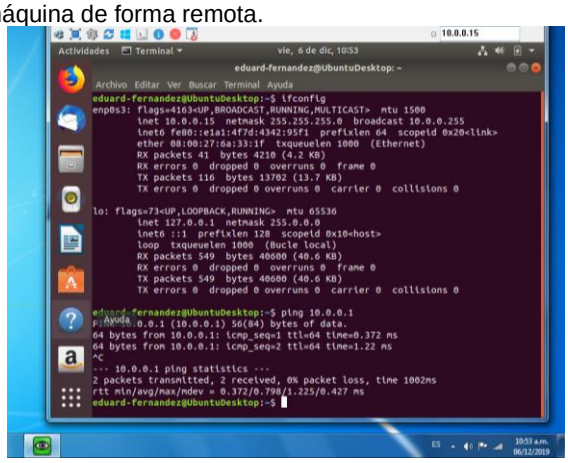

Figura 83. Conexión de forma remota por VPN a equipo Ubuntu Desktop

4 CONCLUSIONES

El sistema operativo Zentyal Server es una herramienta muy potente con la cual se puede realizar la configuración y administración de servicios de infraestructura que normalmente se deben gestionar separados, en una forma agrupada centraliza procesos como los son: DHCP, DNS, Dominio, Proxy, entre otros permitiendo así brindar soluciones optimas a los usuarios de redes intranet y extranet.

La implementación de un proxy no transparente permite garantizar un nivel mayor de seguridad ya que este se configura en el navegador para que funcione a diferencia del transparente, este proxy permitirá que limite el acceso a los computadores que se conecten a la red sin ser configurados.

Los proxy HTTP se encargan de gestionar los niveles de acceso, filtrado y restricción que se pueden dar a uno o varios perfiles de red ya que con estos se puede implementar un sin número de posibilidades para garantizar un uso de red óptimo.

Se logró establecer una conexión remota del equipo Ubuntu Desktop a través de una conexión VPN con un equipo externo, evidenciando de esta manera el correcto funcionamiento de servidor VPN.

Se aprendió la importancia de establecer los permisos en los equipos y las reglas en el firewall para tener una red segura pero que permita a su vez acceder a los servicios de la red.

Se logró identificar los requisitos necesarios para poder implementar un servidor VPN en una red LAN.

Se aprendió a implementar, administrar, monitorear y gestionar un servidor basado en GNU/Linux con el sistema Zentyal.

Se conoció sistema Zentyal como una alternativa para Active Directory de Windows para la administración de dominio y otras herramientas como servidor DHCP, DNS, Proxy, Impresoras, NTF, VPN entre otros.

Se comprendió que la posibilidad de trabajar con el sistema Zentyal permite instalar los módulos requeridos según las necesidades de la empresa y de esta manera optimizar los recursos I.T con lo cual se logra una mayor rentabilidad de la empresa a implementar la solución.

En esta última actividad del diplomado se hace énfasis en la instalación del sistema operativo Zentyal server en el cual se implementó y se configuró un control de acceso a internet a través de un proxy que filtra su salida.

Por otro lado aprendimos a aplicar las reglas de filtrado para los bloqueos de sitios web de entretenimiento fortaleciendo el procedimiento para realizar validaciones desde la estación de trabajo GNU/Linux Ubuntu Desktop.

Finalmente, Zentyal se constituye en una gran opción para la implementación y configuración de servidores para todo tipo de prestación de servicio (DHCP, DNS, Proxy etc) siendo una alternativa a los productos que desarrolla Microsoft. La interface gráfica que tiene Zentyal es muy amigable y fácil de entender haciendo mucho más cómoda la

administración de servidores y el seguimiento a los servicios prestados a través de la red.

5 REFERENCIAS

[1] Free Software Foundation (2019). El sistema operativo GNU, ¿Qué es GNU? Obtenido de https://www.gnu.org/home.es.html
[2] Lopez Sanches, M.J & Belle, S., & Auli, F. (2008). Sistema operativo GNU/Linux básico, ES: Universitat Oberta de Catalunya, pp. 8-11, Recuperado de http://hdl.handle.net/10609/189.
[3] Zentyal. (2004-2019). Zentyal. Obtenido de https://zentyal.com/es/inicio/
[4] Rokitoh. (08 de Diciembre de 2016). Red Orbita. Obtenido de Instalar servidor de VPN en Zentyal Server 5: http://red-orbita.com/?p=7680.
[5] Zentyal. (2004-2019). Documentación Oficial Zentyal 6.0. Obtenido de https://doc.zentyal.org/es/
[6] Zentyal Community (2019). Primeros pasos con Zentyal. Recuperado de https://doc.zentyal.org/es/firststeps.html
[7] Zentyal (2019). Categoría: Tutoriales. Recuperado de https://zentyal.com/es/news/category/tutoriales/