

Instalación y configuración de Zentyal server para la solución de necesidades específicas con GNU / Linux e implementación de servicios de infraestructura IT

Luis Antonio Contreras Villamizar
lacontrerasv@unadvirtual.edu.co
Fabián Eduardo Sierra Pineda
fesierrap@unadvirtual.edu.co
Jairo Andrés Urbano García
jaurbanog@unadvirtual.edu.co
Carlos Fabián Ricaurte
cfricaurter@unadvirtual.edu.co
Jenny Marcela Beltrán
jmbeltranh@unadvirtual.edu.co

RESUMEN: El presente trabajo tienen como finalidad dar a conocer el procedimiento requerido para dar solución a las necesidades específicas con GNU/Linux, implementando servicios bajo el sistema operativo ZENTYAL el cual permitirá realizar la implementación de los diferentes servicios de infraestructura IT tales como: Servidor DHCP, Servidor DNS, Controlador de Dominio, Proxy no transparente, Cortafuegos, Servidor de archivos, Servidor de Impresión y VPN. Demostrando así los diferentes procedimientos a seguir para una óptima implementación de los diferentes servicios.

PALABRAS CLAVE: Controlador de Dominio, Servidor proxy no transparente, Cortafuegos, DHCP Server, DNS Server y VPN

1. INTRODUCCIÓN

Zentyal es un servidor Linux para PYMES que permite proveerlas de una red informática empresarial fácil de usar, durante el desarrollo de la presente actividad se hará su instalación y configuración, y se implementarán las temáticas descritas en la guía de actividades paso 8 con el uso de Zentyal Server.

2. INSTALACION Y CONFIGURACION ZENTYAL SERVER

Para iniciar el proceso de instalación debemos dirigirnos al siguiente enlace y descargar el instalador ZENTYAL en formato ISO:

<http://download.zentyal.com/zentyal-6.2-development-amd64.iso>

Se procede con la descarga del instalador ZENTYAL en formato ISO:

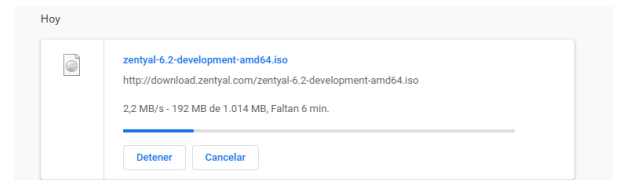


Imagen 1. Descarga Zentyal.6.2" Elaboración Propia"

Para continuar con la instalación crearemos nuestra máquina virtual con la siguiente configuración: 1GB de memoria RAM, procesador de 1GZ y disco duro de 5TB mínimo:

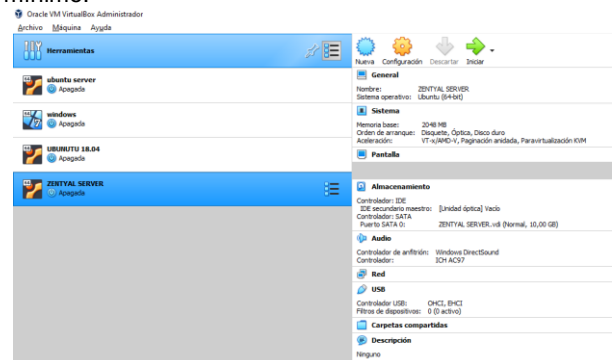


Imagen 2. Máquina virtual Zentyal.6.2" Elaboración Propia"

Agregamos nuestra imagen ISO al arranque de la máquina virtual que hemos creado:

Imagen 9. Nombre máquina" Elaboración Propia"

El sistema se conectará a internet y actualizará la hora:

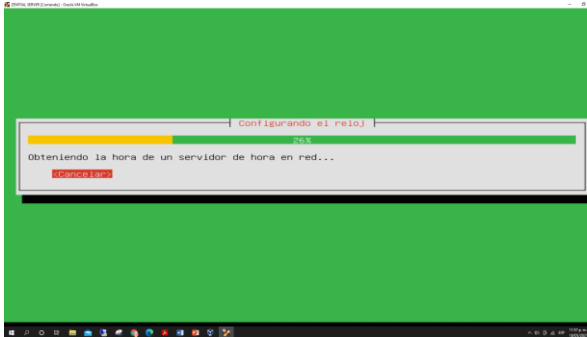


Imagen 10. Hora y fecha" Elaboración Propia"

Una vez se completan los pasos mencionados el sistema iniciará el proceso de instalación de nuestro servidor con las preferencias seleccionadas este proceso dura aproximadamente 20 minutos dependiendo de las características de nuestro equipo:

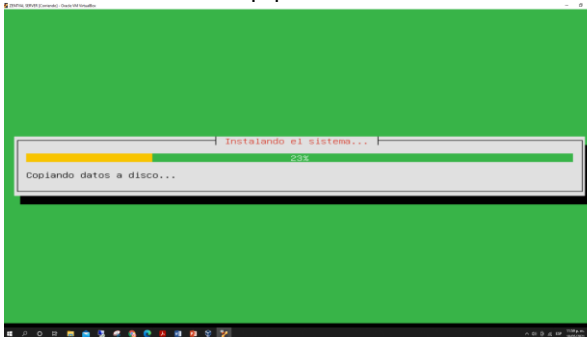


Imagen 11. Instalación "Elaboración Propia"

El acceso al servidor se hace a través de un navegador web del panel de navegación:

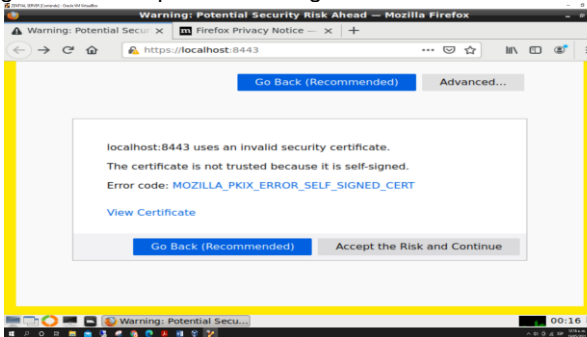


Imagen 12. Acceso a través de Mozilla" Elaboración Propia"

Interfaz para ingreso con usuario y contraseña configurados en la instalación:



Imagen 13. Acceso a través de Mozilla" Elaboración Propia"

En este apartado se selecciona los paquetes a instalar basado en las temáticas elegidas:

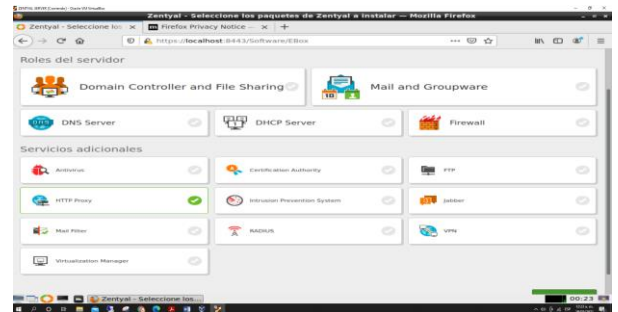


Imagen 14. Selección de paquetes "Elaboración Propia"

Es importante configurar las interfaces de red, definiendo cual será la conexión WAN (Externa) y cuál será la (LAN) interna:

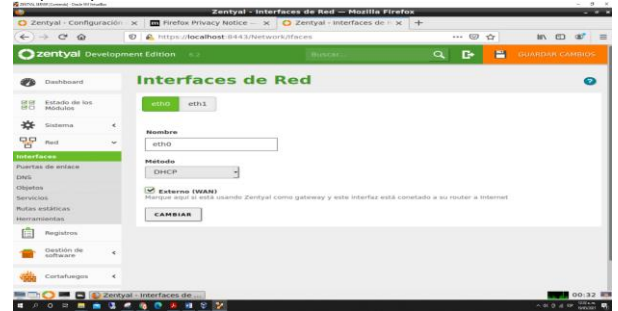


Imagen 15. Configuración Interfaces" Elaboración Propia"

Una vez realizadas todas las configuraciones ya se puede ver la interfaz web de Zentyal junto a todos los componentes instalados y listos para utilizar de acuerdo con las necesidades:

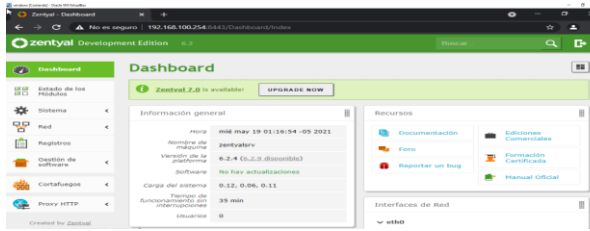


Imagen 16. Dashboard “Elaboración Propia”

3. TEMATICAS PARA ZENTYAL

Temática 1: DHCP Server, DNS Server y Controlador de Dominio. Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Se seleccionan los paquetes a instalar, en esta ocasión se instalarán los paquetes de DNS Server, DHCP Server y Domain Controller and File Sharing, que corresponden a la Temática 1.

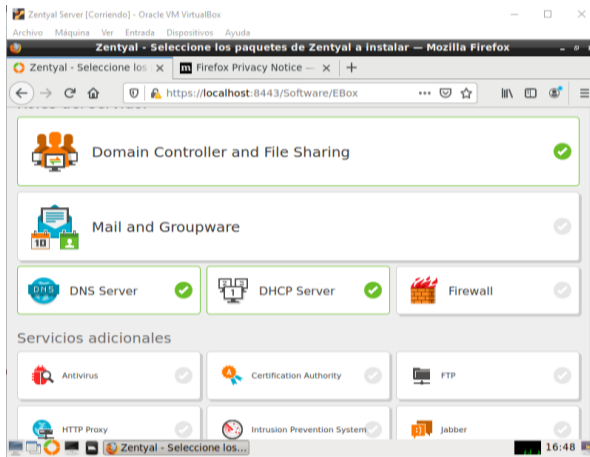


Imagen 17. instalación de paquetes (17 05 2021) elaboración propia

Posteriormente se muestra una ventana de confirmación con los paquetes a instalar.

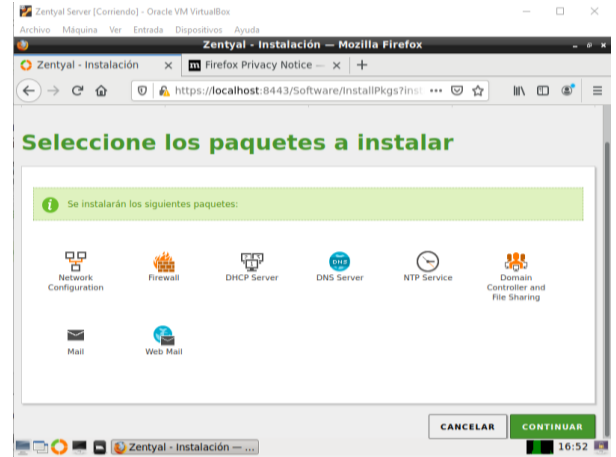


Imagen 18 Confirmación instalación de paquetes (17 05 2021) elaboración propia

Posteriormente se selecciona el tipo de servidor a utilizar el cual será STAND_ALONE, y se agregará el tipo de dominio.

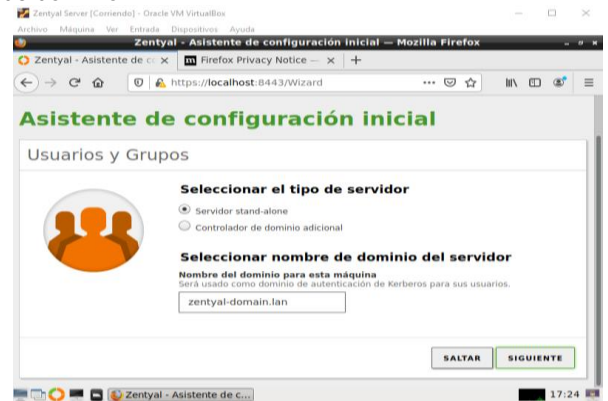


Imagen 19 Usuarios y Grupos (17 05 2021) elaboración propia

Seguido de esto se selecciona el dominio virtual de correo, se deja el que aparece por defecto.

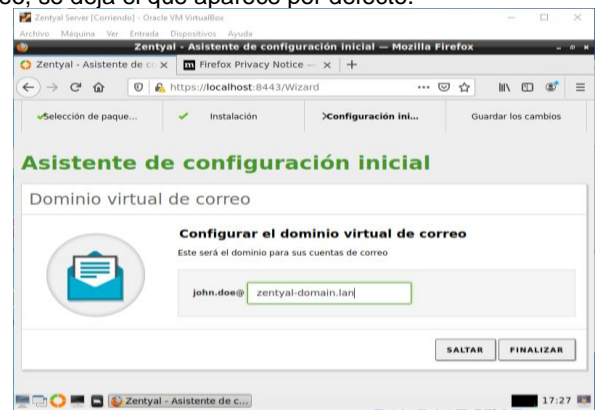


Imagen 20 Dominio virtual de correo (17 05 2021) elaboración propia

Seguido de esto el sistema procede con la configuración de cada uno de los módulos instalados.



Imagen 21 Configuración de paquetes (17 05 2021) elaboración propia

Luego de finalizada la configuración, se accede a DASHBOARD y se verifica la configuración realizada en cada componente.

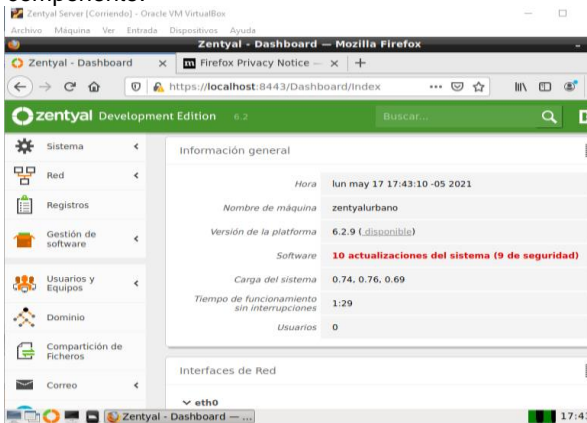


Imagen 22 DASHBOARD (17 05 2021) elaboración propia

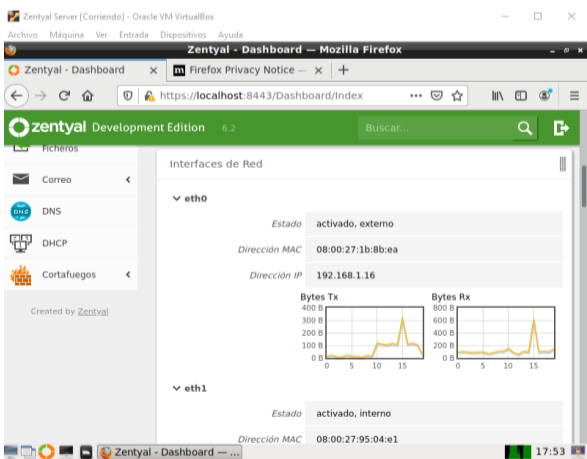


Imagen 23 DASHBOARD (17 05 2021) elaboración propia

Luego de verificar la información del servidor se procede a ingresar al módulo DHCP en donde se observará la siguiente información:

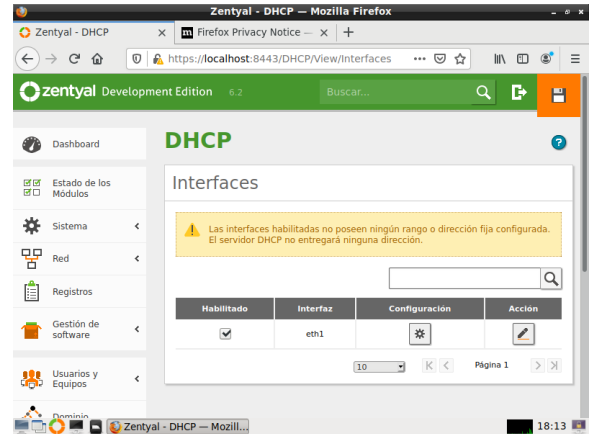


Imagen 24 DHCP (17 05 2021) elaboración propia

Posteriormente se da clic en la opción configuración, se observará la siguiente pantalla.

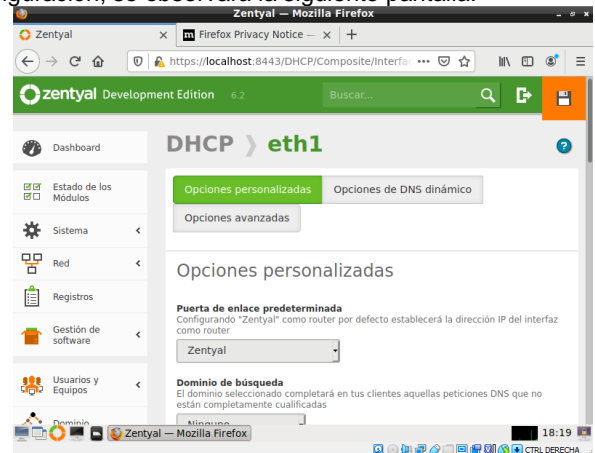


Imagen 25 DHCP eth1 (17 05 2021) elaboración propia

Seguido de esto se puede observar los rangos dinámicos de las direcciones y la asignación estática.

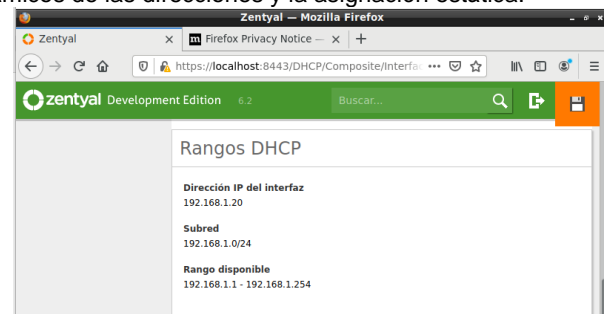


Imagen 26 Rangos DHCP (17 05 2021) elaboración propia

A continuación, se procede con la asignación de un nuevo rango, se introduce un nombre con el que identificar el rango y los valores que se quieran asignar.

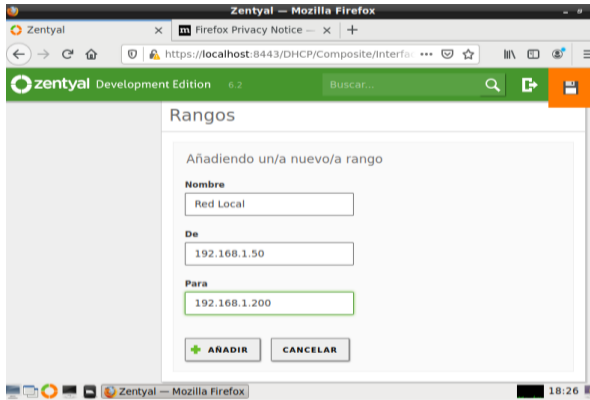


Imagen 27 Rangos DHCP (17 05 2021) elaboración propia

A continuación, se añade el rango y se procede a guardar los cambios realizados.

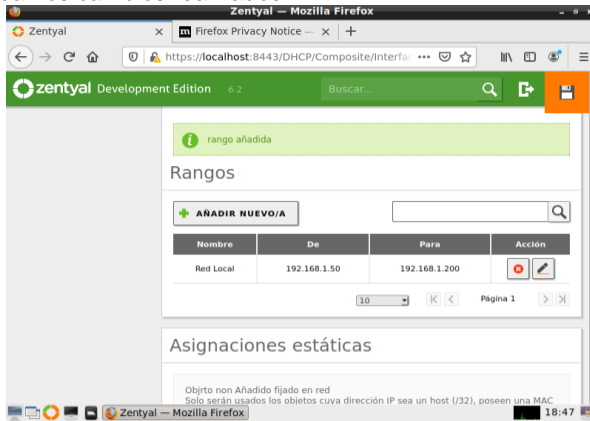


Imagen 28 Rangos DHCP (17 05 2021) elaboración propia

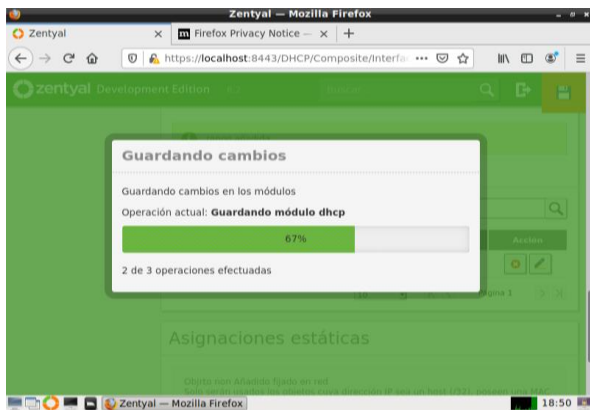


Imagen 29 Rangos DHCP (17 05 2021) elaboración propia

Se procede con la comprobación de la IP configurada, se realiza desde la maquina Ubuntu mediante un ping a la dirección 192.168.1.20 que corresponde al Servidor Zentyal.

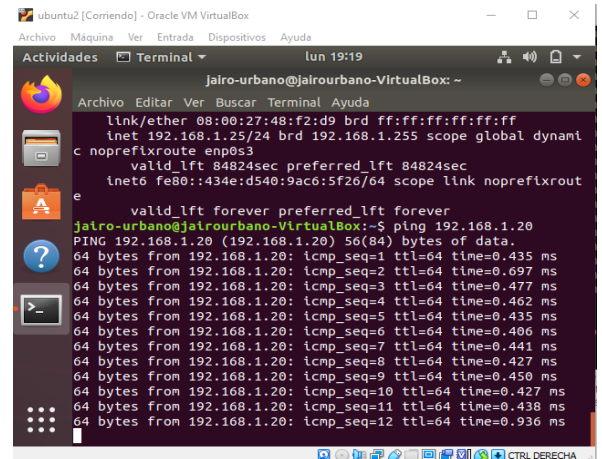


Imagen 30 ping desde Ubuntu a Zentyal (17 05 2021) elaboración propia

De igual manera se realiza la comprobación desde el servidor Zentyal a la maquina Ubuntu con IP 192.168.1.25

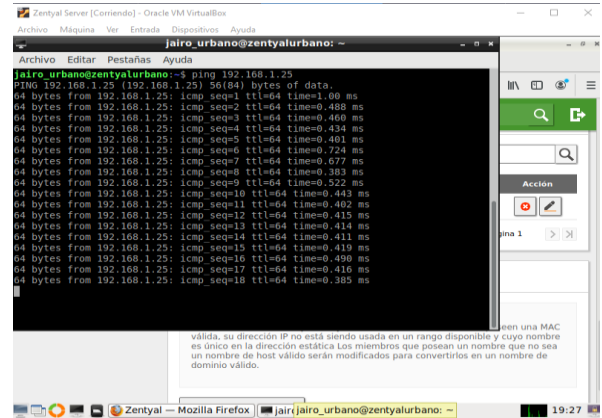


Imagen 31 ping desde Zentyal a Ubuntu (17 05 2021) elaboración propia

Se verifica desde el sistema operativo Windows la conexión a las dos maquina virtuales.



Imagen 32 ping desde Windows a Zentyal y Ubuntu (17 05 2021) elaboración propia

A continuación, se procede con la configuración del control del dominio.

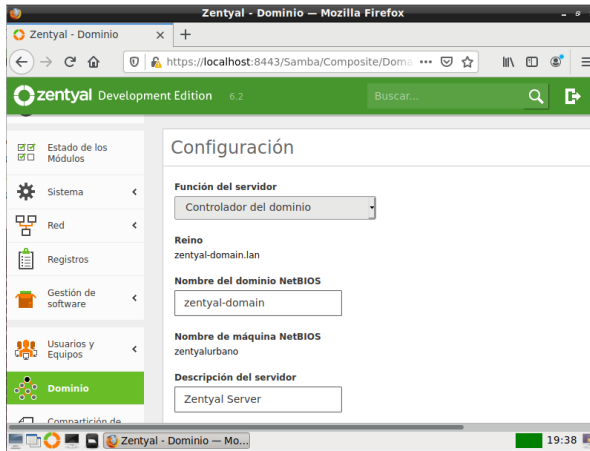


Imagen 33 Dominio (17 05 2021) elaboración propia

Posteriormente se dirige a usuarios y equipos y se procede a crear un usuario de control de dominio.

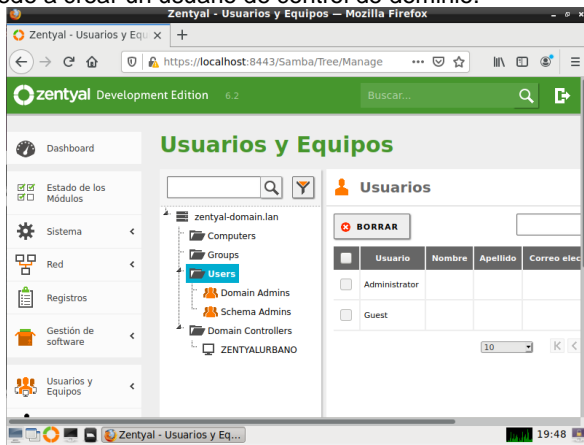


Imagen 34 Usuarios y Equipos (17 05 2021) elaboración propia

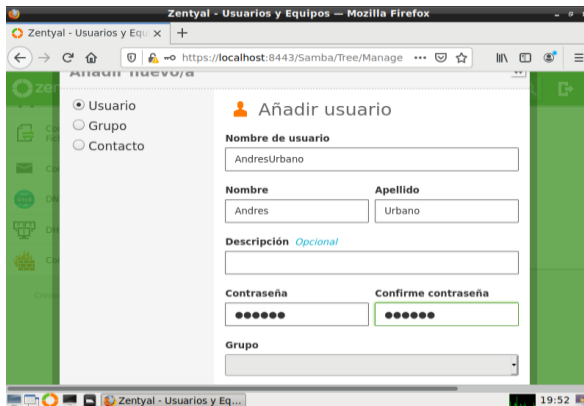


Imagen 35 Añadir Usuarios (17 05 2021) elaboración propia

Se verifica la información del usuario creado.

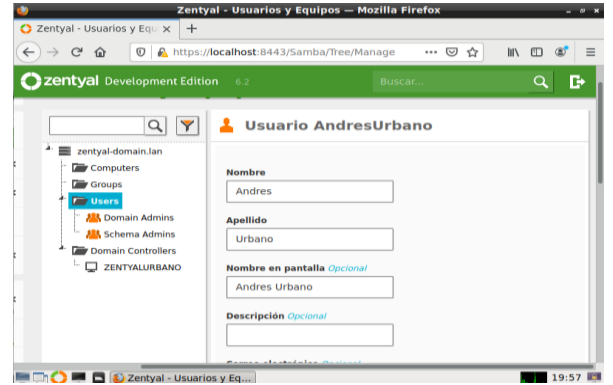


Imagen 36 Usuarios (17 05 2021) elaboración propia

Desde la máquina de Ubuntu se ingresa desde el super usuario y se procede a editar el nameserver del equipo con el comando `nano resolv.conf`

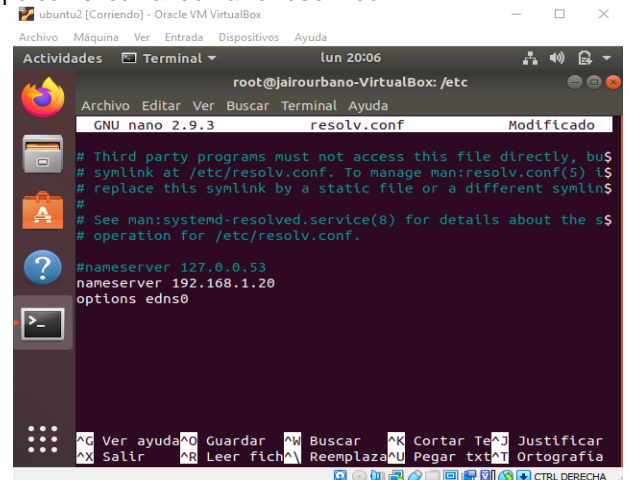


Imagen 37 Usuarios (17 05 2021) elaboración propia

Se verifica su conexión por medio del ping.

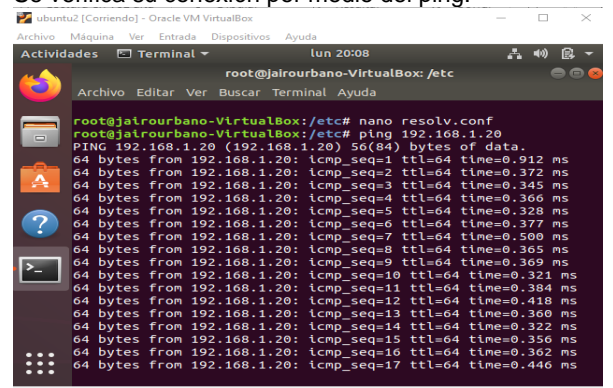


Imagen 38 verificación ping (17 05 2021) elaboración propia

Se procede con la verificación de las carpetas y directorios de Ubuntu.

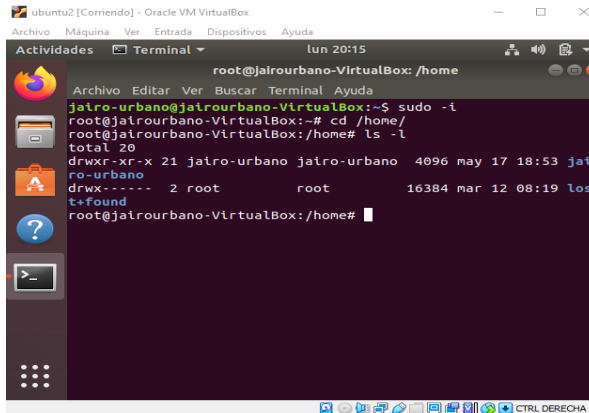


Imagen 39 verificación Ubuntu (17 05 2021) elaboración propia

Desde el escritorio de Ubuntu se procede a instalar el paquete Pbis Open, la cual es una herramienta que permite unir Linux a un Active Directory.

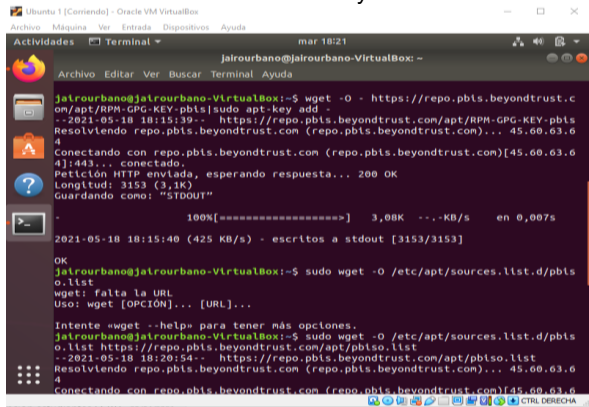


Imagen 40 Instalación Pbis Open (17 05 2021) elaboración propia

Se procede con la instalación de el paquete likewise-open

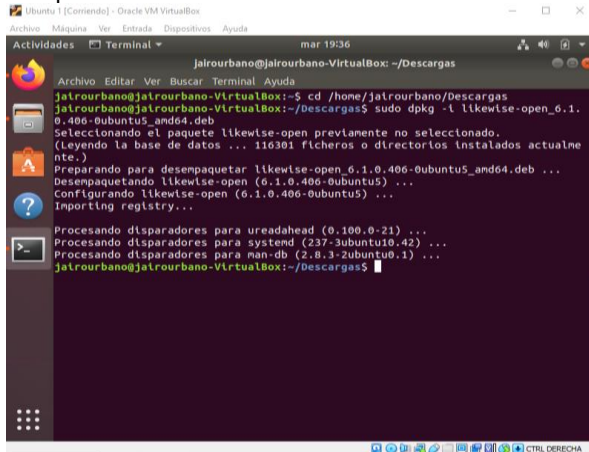


Imagen 41 Instalación Pbis Open (17 05 2021) elaboración propia

Posteriormente se descarga libglade 2 y el entorno grafico de likewise.

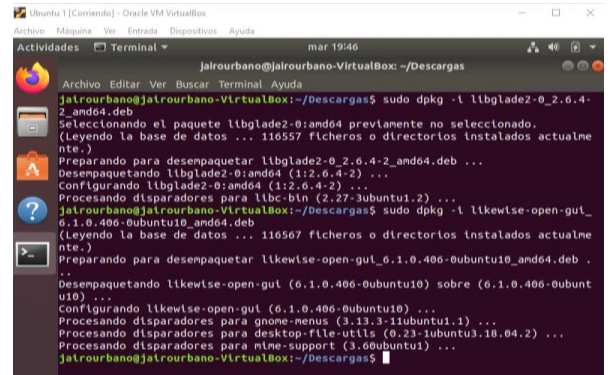


Imagen 42 Instalación Pbis Open (17 05 2021) elaboración propia

A continuación, se procede con las pruebas de conexión.

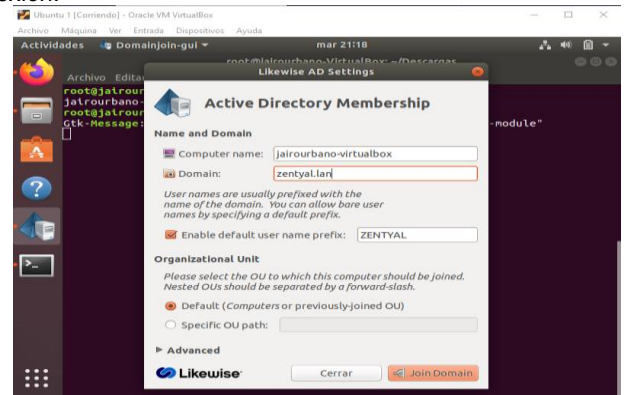


Imagen 43 prueba de conexión (17 05 2021) elaboración propia

Se ingresa con el nombre del dominio de la maquina y con el usuario y contraseña creados.

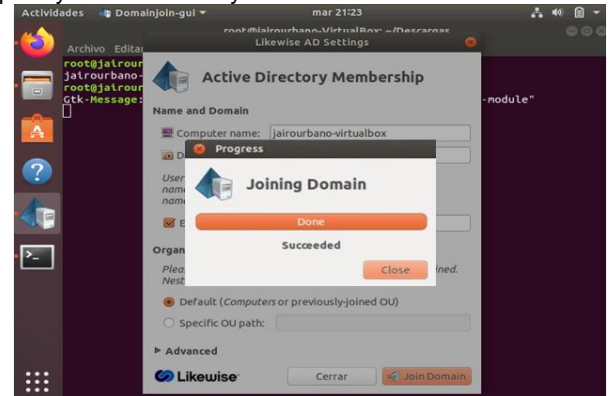


Imagen 44 prueba de conexión (17 05 2021) elaboración propia

Luego de realizar la conexión se verifica que se haya creado Ubuntu en el directorio.

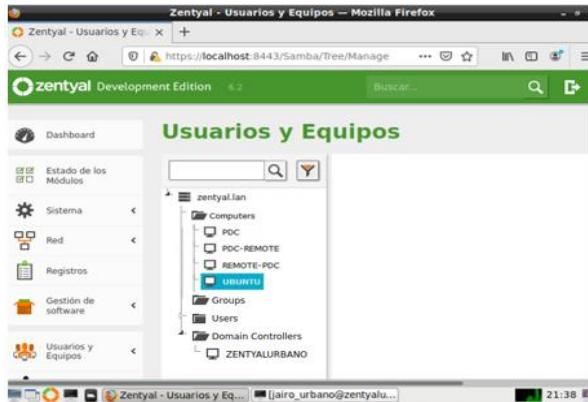


Imagen 45 prueba de conexión (17 05 2021) elaboración propia

Temática 2: Proxy no transparente Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 1230.

Ingresamos por configuración de estado de módulos y activamos el servidor http proxy:

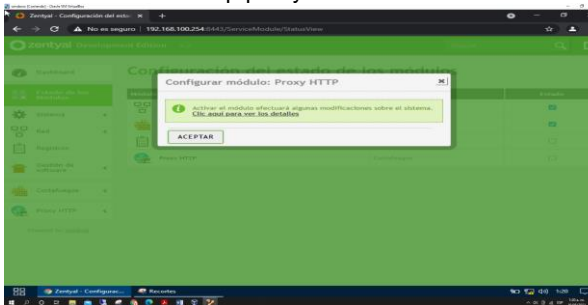


Imagen 46. Activar servicio http proxy" Elaboración Propia"

Para la administración del acceso a los servicios, zentyal proxy, utiliza objetos a los cuales se les aplican las diferentes reglas de acceso, para el ejemplo crearemos dos objetos, uno se llamará usuarios estándar y otro se llamará usuarios, soporte mas adelante nos permitirá asignar las diferentes reglas de acceso que cada grupo tendrá:

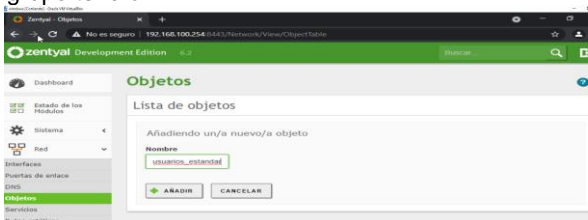


Imagen 47. Crear objeto" Elaboración Propia"

Dentro de cada objeto se deben crear los nombres

de los usuarios, y la dirección IP del equipo asignado, ya que el filtrado depende de esta IP:



Imagen 48. Tabla de objetos creados "Elaboración propia"

A continuación, encontramos el apartado reglas de acceso, en el tendremos entre otras opciones, elegir el horario en que los diferentes objetos que hemos creado tendrán acceso o no al servicio:

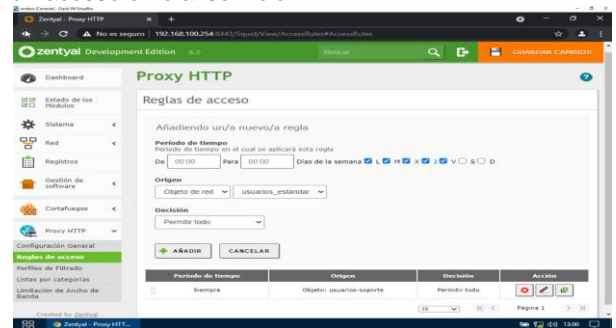


Imagen 49. Reglas de acceso" Elaboración Propia"

A continuación, accedemos al apartado perfiles de filtrado, es allí en donde vamos a bloquear o permitir el acceso a los sitios que especifiquemos, para lo cual debemos crear perfiles por separado con las diferentes preferencias que consideremos, para el ejemplo crearemos el perfil usuarios estándar y bloquearemos el acceso a YouTube y Facebook

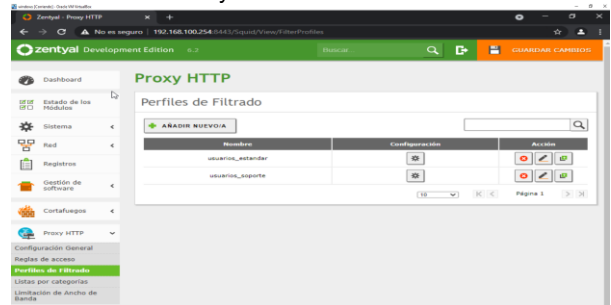


Imagen 50. Perfiles de filtrado" Elaboración Propia"

Creamos el filtrado de dominio para bloquear Facebook:

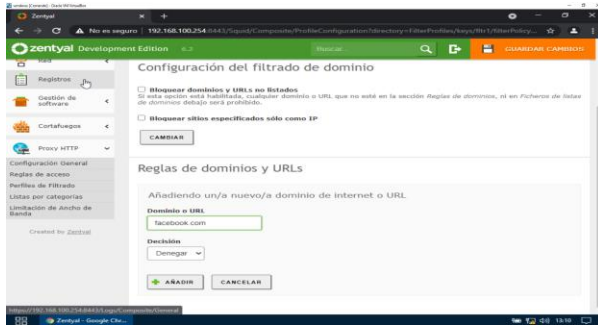


Imagen 51. Perfiles de filtrado" Elaboración Propia"

Se verifica que e equipo no tiene acceso a internet:

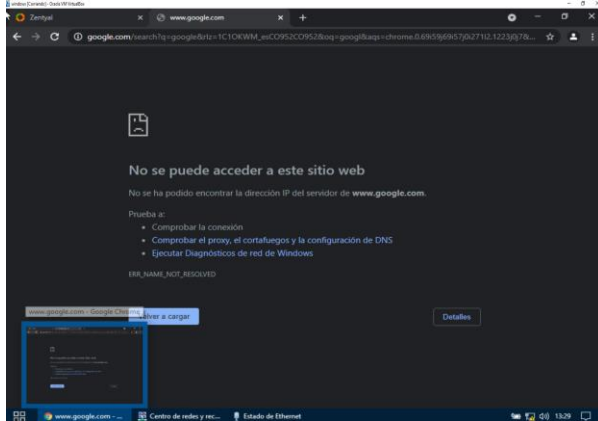


Imagen 52. Acceso internet" Elaboración Propia"

Le aplicamos el perfil filtrado a cada objeto creado

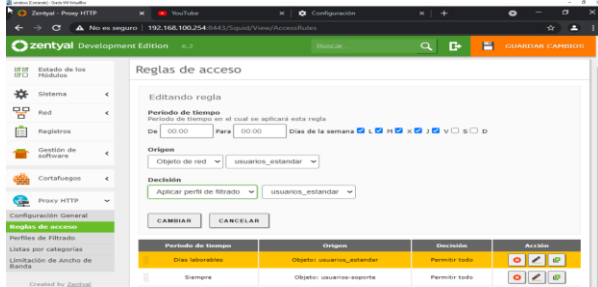


Imagen 53. Asignando perfiles de filtrado" Elaboración Propia"

Agregamos nuestro servidor proxy en la configuración de Windows, así mismo agregamos la excepción a la dirección IP de nuestro servidor Zentyal lo anterior para no perder el acceso al panel de configuración.

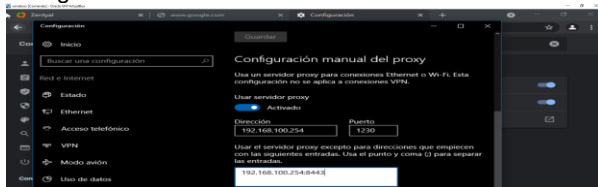


Imagen 54. Configurando proxy en Windows" Elaboración Propia"

Con el comando ping podemos confirmar que tenemos acceso a google.com y que estamos saliendo a través del servidor proxy cuya IP es la 192.168.100.254 como lo muestra el primer salto del comando tracert



Imagen 55. Ping a google.com" Elaboración Propia"

Intentamos acceder a Facebook.com y el sistema nos lanza una pantalla de error:

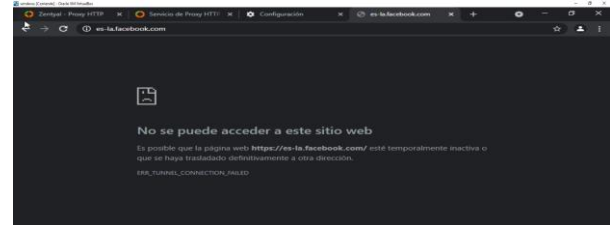


Imagen 56. Bloqueo Facebook" Elaboración Propia"

Lo mismo ocurre con YouTube:

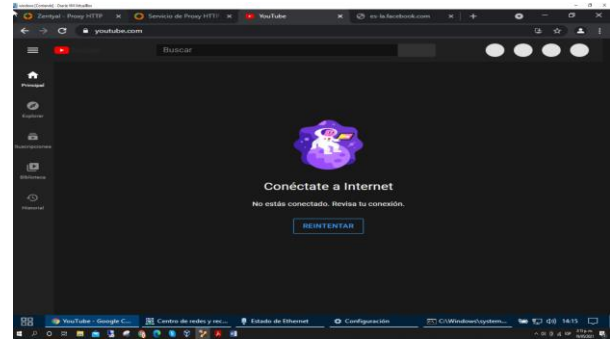


Imagen 57. Bloqueo YouTube" Elaboración Propia"

Por el contrario, si cambiamos la IP que asignamos para los usuarios de soporte:

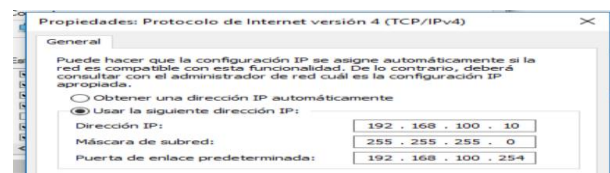


Imagen 58. Cambiando IP" Elaboración Propia"



Imagen 59. Acceso a YouTube” Elaboración Propia”

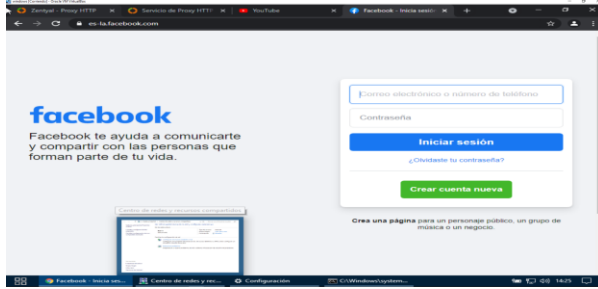


Imagen 60. Acceso a Facebook” Elaboración Propia”

Temática 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.

Para configurar un cortafuego se debe seleccionar el paquete Firewall y se da clic en el botón Instalar:

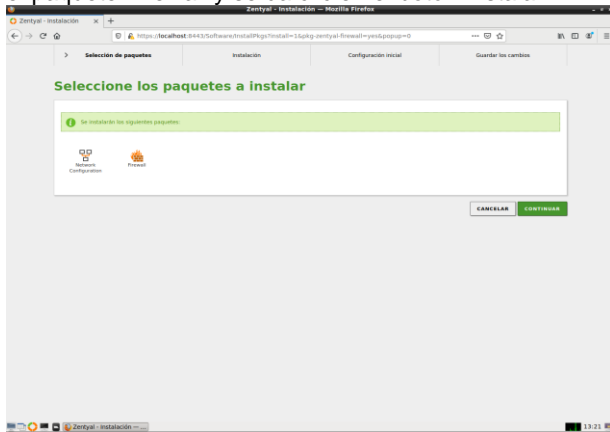


Imagen 61. Instalación de paquetes”Elaboración Propia”

Se configuran los adaptadores de red:

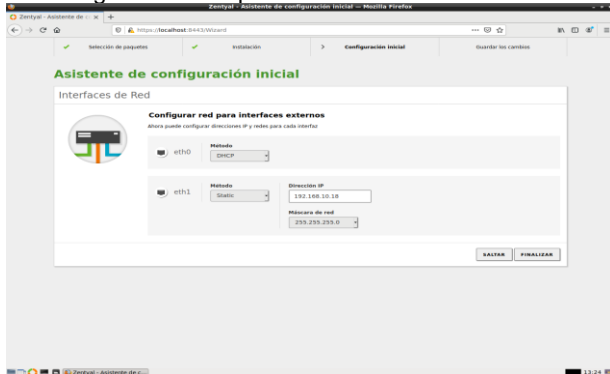


Imagen 62. Configuración adaptadores de red
Luego aparecerá el siguiente dashboard:

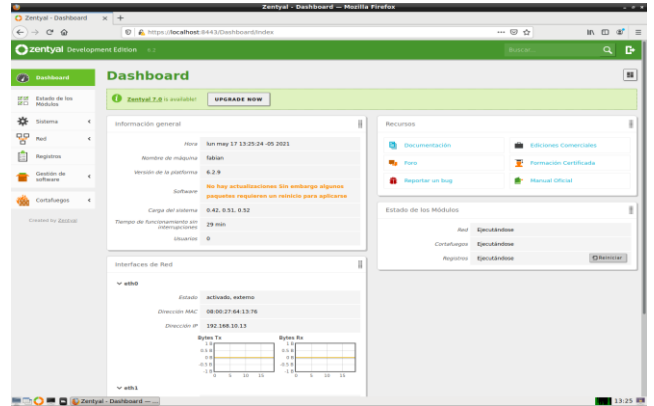


Imagen 63. Dashboard “Elaboración Propia”

Se selecciona la opción Cortafuegos y luego Filtrado de paquetes:

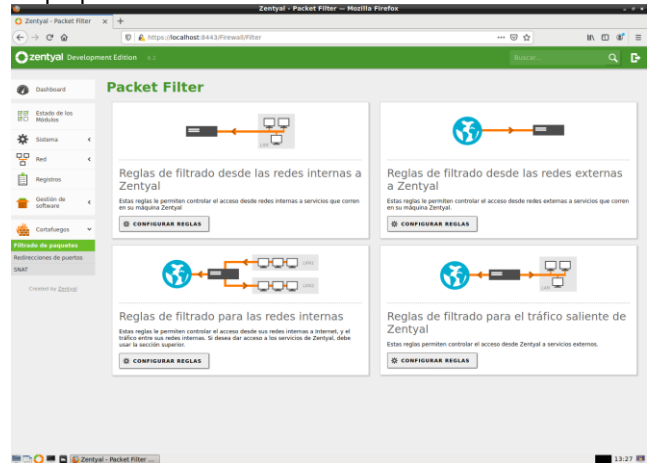


Imagen 64. Opciones para configurar cortafuegos

En la opción seleccionada, damos clic en Añadir una nueva regla y llenamos los datos como se muestra en la pantalla y en IP destino se coloca la IP pública de las páginas a bloquear:



Imagen 65. Añadimos nueva regla

Una vez configurado todos los bloqueos se muestra

la lista de políticas creadas:

Nombre	Activo	Origen	Destino	Acciones
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico
Controlador	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	Permitir Tráfico

Imagen 66. Tabla de políticas

Para probar si se configuró correctamente, en la máquina virtual de escritorio, abrimos en este caso la página Facebook y como se puede ver no hay acceso:

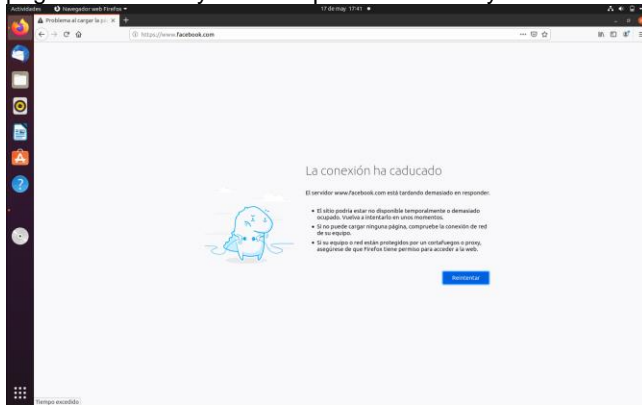


Imagen 67. Comprobación ingresando a Facebook

Luego abrimos Outlook para verificar que si se tiene acceso:

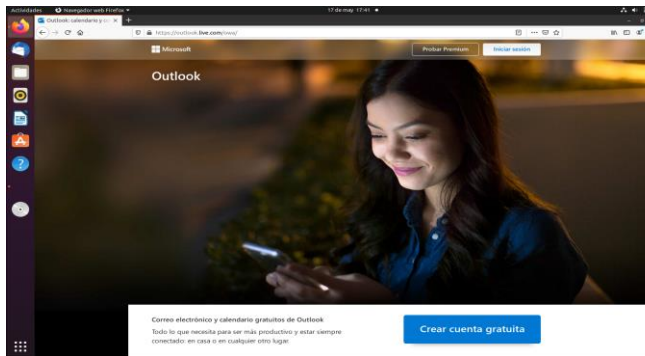


Imagen 68. Comprobación de Outlook

Temática 4: File Server y Print Server Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

Seleccionar los servicios que se requieren instalar y clic en instalar.



Imagen 69. Paquetes para instalar.

Mensaje de información de los servicios que se van a instalar

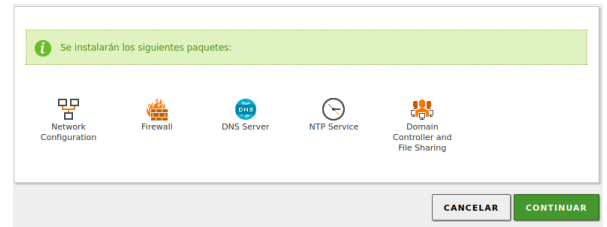


Imagen 70. Servicios para instalar

Función del servidor
 Controlador del dominio

Reino
 zentyal-domain.lan

Nombre del dominio NetBIOS
 zentyal-domain

Nombre de máquina NetBIOS
 jennyzentyal

Descripción del servidor
 Zentyal Server

Habilitar perfiles móviles

Letra de unidad
 H:

CAMBIAR

Imagen 71. Establecer el tipo de servidor y dominio.

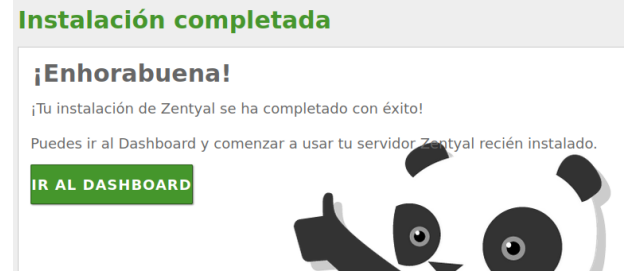


Imagen 72. Instalación Completa

Activar servicio controlador de dominio y compartición de archivos

Módulo	Depende	Estado
Red		<input checked="" type="checkbox"/>
Controladores	Red	<input checked="" type="checkbox"/>
DNS	Red	<input checked="" type="checkbox"/>
Registros		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>
Controlador de Dominio y Compartición de Ficheros	Red, DNS, NTP	<input checked="" type="checkbox"/>

Imagen 73. Servicios de controlador de dominio.

Rangos

Añadiendo un/a nuevo/a rango

Nombre

De

Para

Imagen 74. Configurar los rangos DHCP

Editando recurso compartido

Habilitado

Nombre del recurso compartido

Ruta del recurso compartido
 Directorio bajo Zentyal creará automáticamente el directorio compartido share.
 Ruta del sistema de ficheros permitirá compartir un directorio existente en su sistema.

Comentario *Opcional*

Acceso de invitado
 Este directorio compartido no necesita de autenticación.

Imagen 75. Configurar un servidor de ficheros

Directorios compartidos > Compartida

Control de Acceso

Añadiendo un/a nuevo/a ACL

Usuario/Grupo

Permisos
 Tenga cuidado al conceder permisos de administrador. El usuario podrá leer y escribir cualquier fichero del recurso.

Imagen 76. Administrador de control de acceso.

Usuario Invitado

Nombre

Apellido

Nombre en pantalla *Opcional*

Descripción *Opcional*

Correo electrónico *Opcional*

Cuota de usuario (MB)
 Mb

Grupos del usuario

Imagen 77. Creación de usuarios

Se ejecuta la siguiente sentencia sudo apt-get -y install libnss-ldap libpam-ldap ldap-utils nscd

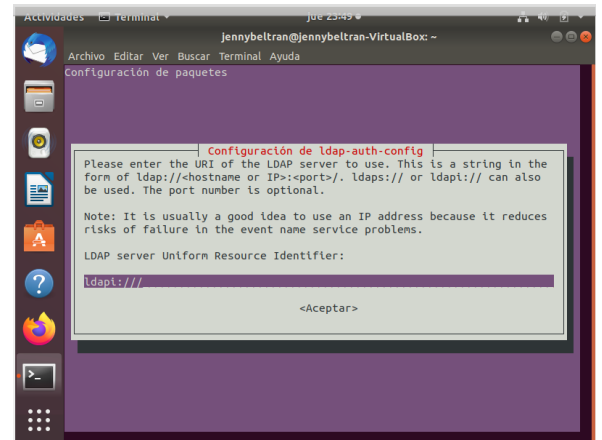


Imagen 78. Configurar LDAP cliente en Ubuntu Linux.

Se ejecuto la instrucción de instalación de CUPS

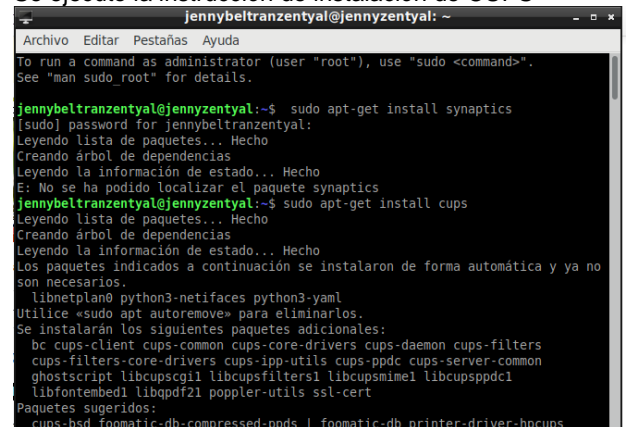


Imagen 79. Instalar impresora

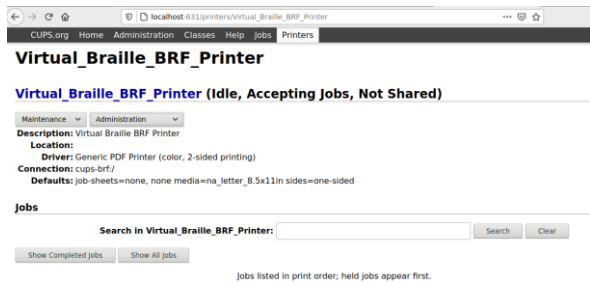


Imagen 80. Configurar la impresora

Temática 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. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Al ingresar nos aparece un mensaje de configuración inicial y en la parte de abajo daremos continuar. A hacerlo nos aparecerá una pagina donde aparecen los servicios que zentyal permite instalar en su sistema desde su entorno web, en este caso instalaremos VPN únicamente.

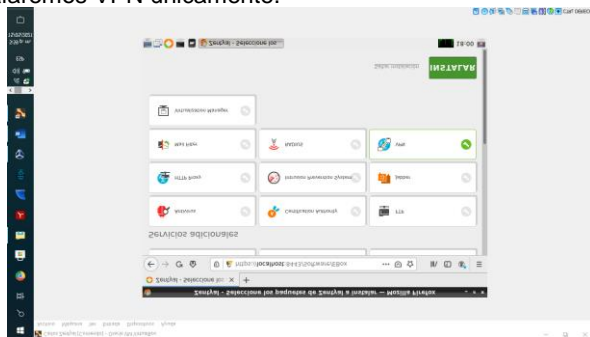


Imagen 81. Selección de servicios a instalar. Elaboración propia.

Al dar clic en instalar ahora mostrará los paquetes que se van a instalar en el sistema, que junto a VPN que fue el único servicio que escogimos se instalarán una unidad certificadora, firewall y configuración de red. Estos, servicios necesarios para la configuración de VPN. Clic en continuar.

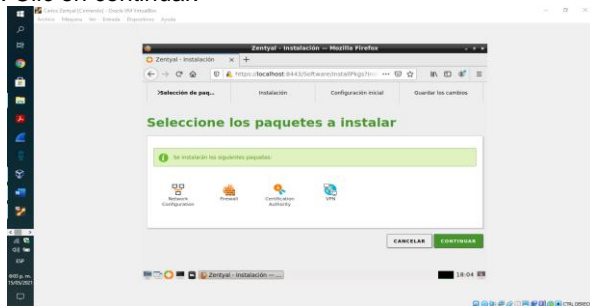


Imagen 82. Paquetes que se instalarán. Elaboración propia.

Después de la instalación de los paquetes nos pide configurar el tipo de interfaces para eth0 que es el adaptador puente y eth1 que es el adaptador de red interna. Estas las dejaremos por defecto.

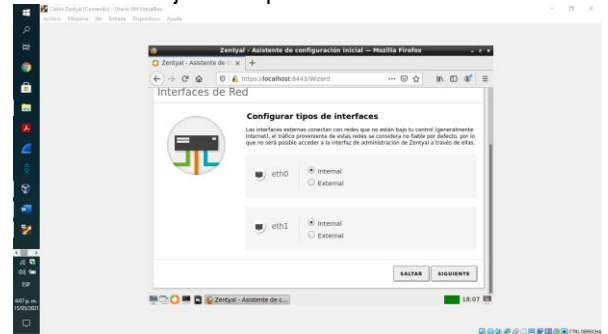


Imagen 83. Tipo de interfaces. Elaboración propia.

Ahora para la configuración de las IPs de las interfaces, para eth0 dejaremos como DHCP y para eth1 como Static, a la cual le asignaremos una IP en distinto segmento que el eth0 para evitar conflictos en la red.



Imagen 84 Configuración de interfaces. Elaboración propia.

Se empezará a instalar la configuración que acabamos de realizar.

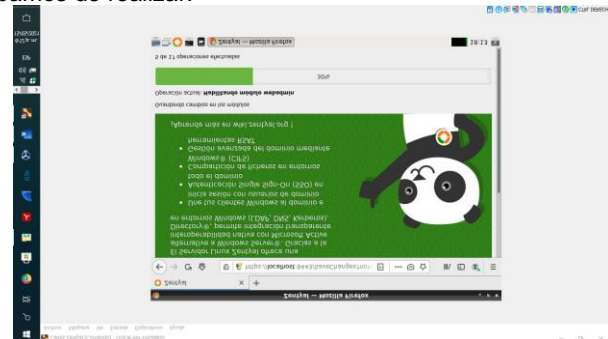


Imagen 85. Guardado de configuración. Elaboración propia.

Terminada la instalación aparece un mensaje de que la instalación ha sido completada y nos permite ir a la dashboard.

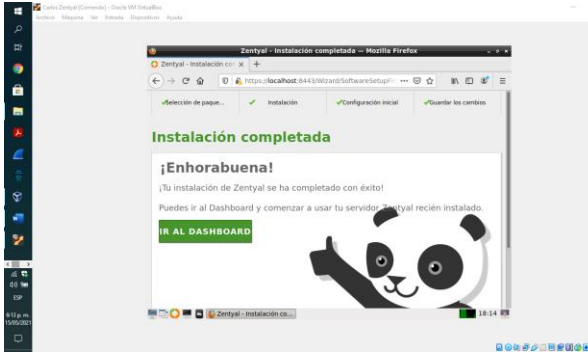


Imagen 86. Instalación completa. Elaboración propia.

Ahora podemos confirmar que se instalaron los paquetes para VPN.

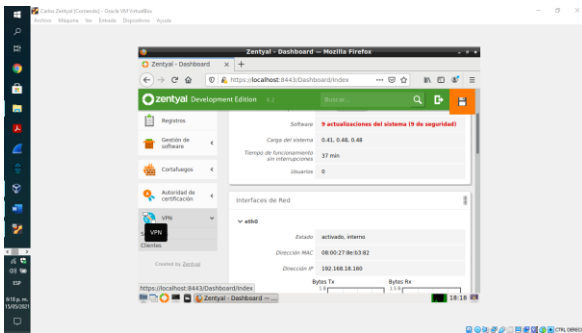


Imagen 87. Confirmación de instalación de VPN. Elaboración propia.

Nos dirigimos a VPN y luego en servidores, y nos solicitará dirigimos al módulo de autoridad de certificación para crear un certificado.

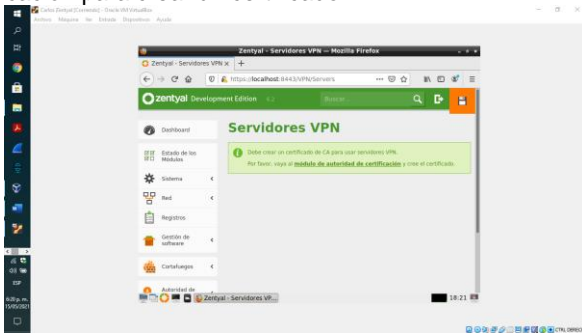


Imagen 88. Solicitud de certificado. Elaboración propia.

A continuación, se hace clic sobre el enunciado “módulo de autoridad de certificación”. En la ventana que aparece se define el nombre de la organización y los días para expirar, luego se da clic en el botón crear.

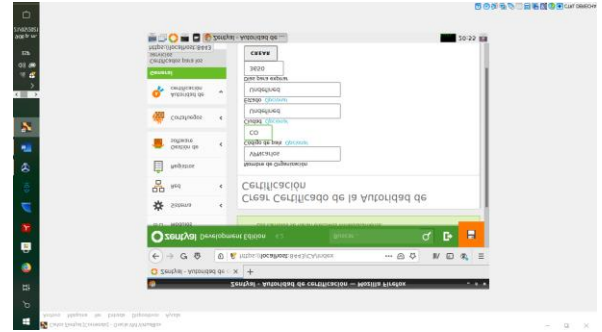


Imagen 89. Creando autoridad de certificación. Elaboración propia.

En la ventana que aparece, se crea un nuevo certificado de autoridad, se define el nombre y días para expirar y se da clic en el botón Expirar.

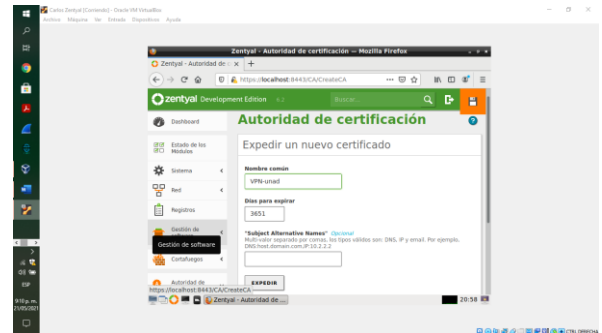


Imagen 90. Expedición de certificado. Elaboración propia.

Se puede observar los certificados creados en la parte inferior. Ahora se procede a guardar los cambios.

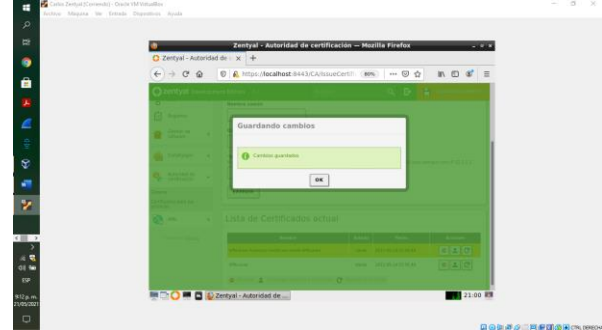


Imagen 91. Guardando cambios hasta el certificado. Elaboración propia.

Nuevamente en VPN/Servidores se podrá observar que ya permite crear un servidor VPN. Clic en añadir.

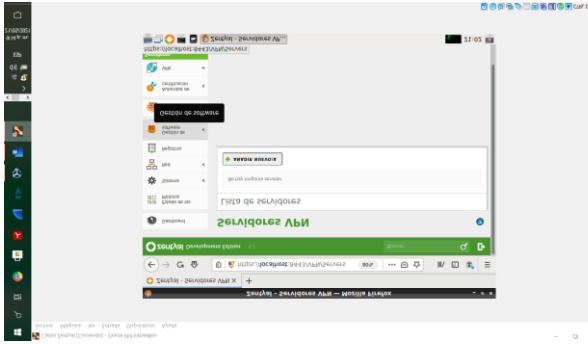


Imagen 92. VNP/Servidores accesible. Elaboración propia.

Una vez se realiza el paso anterior, se procede a asignarle un nombre al servidor VPN. Clic en añadir.

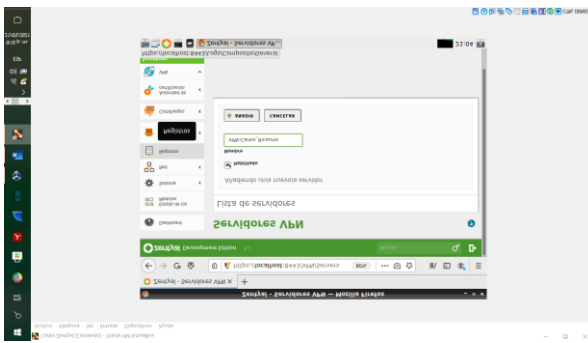


Imagen 93. Nombre del servidor VPN. Elaboración propia.

Una vez creado el servidor VPN se procede a establecerle en configuración los parámetros deseados para su implementación y funcionamiento. Se le asigna un puerto UDP, la dirección por defecto es la 192.168.60.0/24 y se selecciona el certificado para el servidor VPN. Ahora se agregan los parámetros, lo demás es opcional y se puede dejar por defecto. Clic al final en el botón "Cambiar".

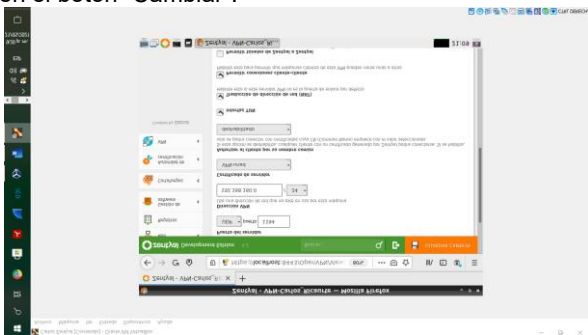


Imagen 94. Parámetros del servidor VPN. Elaboración propia.

Se proceden a guardar los cambios de la configuración hecha hasta el momento.

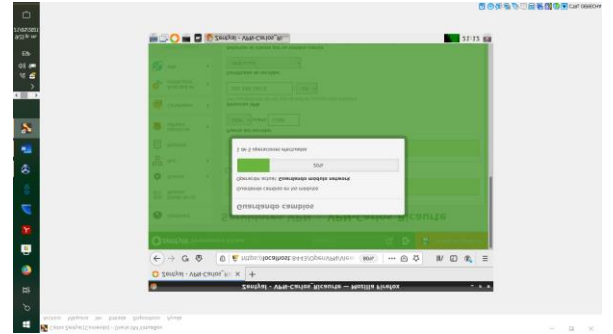


Imagen 95. Guardando configuración. Elaboración propia.

Ahora, nuevamente en Autoridad de Certificación/General se creará un certificado para el cliente. En este caso el Ubuntu Desktop. Se define el nombre y días para expirar. Clic en expedir.

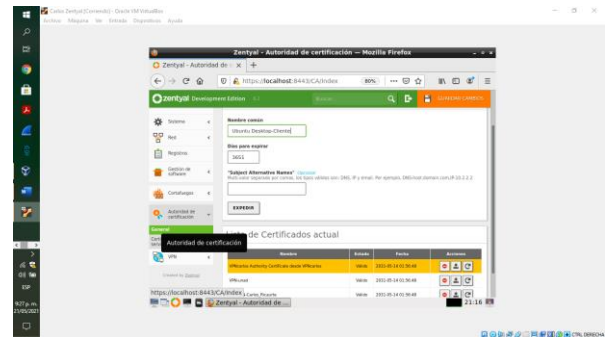


Imagen 96. Certificado del cliente. Elaboración propia.

Una vez expedido, se dirige a VPN/Servidores y clic en el botón de "Descarga de paquetes de configuración de cliente".

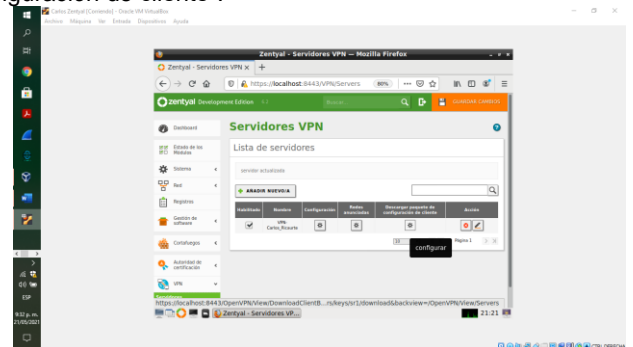


Imagen 97. Descarga de paquetes de cliente. Elaboración propia.

Una vez hecho lo anterior, se carga la ventana y se escoge el tipo de cliente y el certificado de este. En la IP, se debe tener una IP estática, en este caso se definió 192.168.90.90

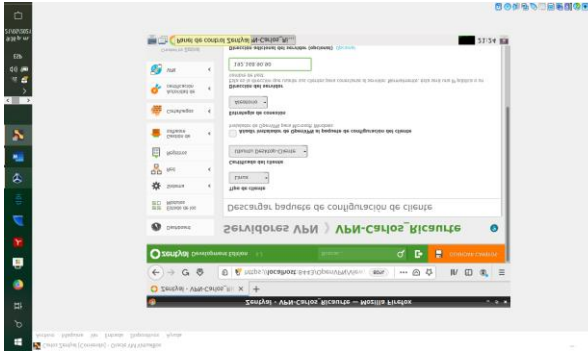


Imagen 98. Parámetros del cliente. Elaboración propia.

Después se da clic en descargar al final de la pagina y se guarda el paquete de la configuración.

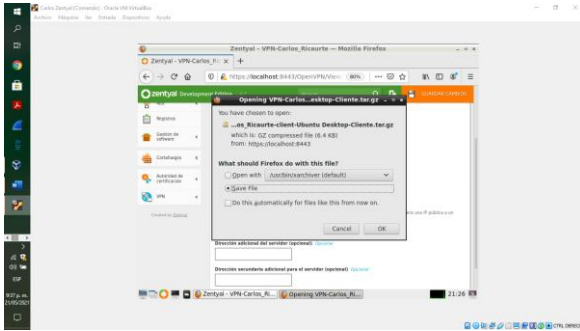


Imagen 99. Descarga de configuración del cliente. Elaboración propia.

Ahora desde el cliente, se procede a configurar la conexión VPN. Esto desde configuración de red y apartado de VPN, donde se procede a hacer clic en el símbolo de añadir. Ahora se escoge el Protocolo de Túnel Punto a Punto (PPTP).

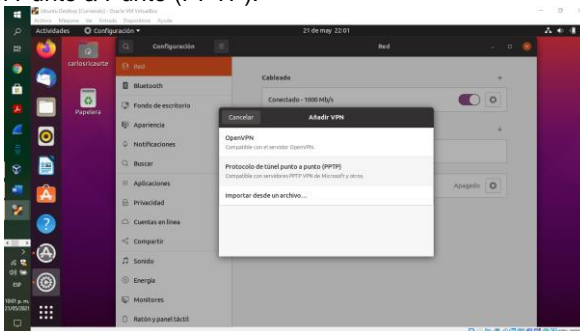


Imagen 100. Protocolo para configuración de conexión VPN. Elaboración propia.

Ahora se le asigna un nombre con el que se identificará en el cliente y la pasarela, que es la IP que se configuro para el cliente en el servidor VPN de Zentyal. Clic en Avanzado.

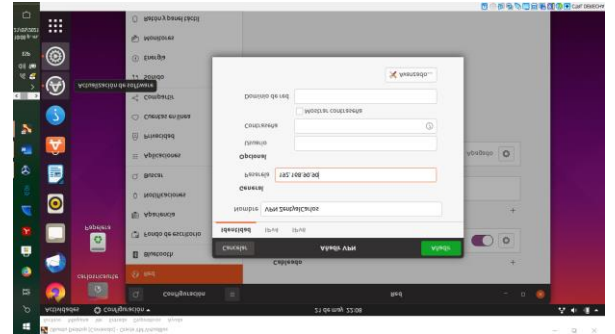


Imagen 101. Configuración inicial VPN en cliente. Elaboración propia.

Una vez en la configuración avanzada se selecciona "Usar cifrado punto a punto (MPPE)". Clic en aceptar y luego en añadir.

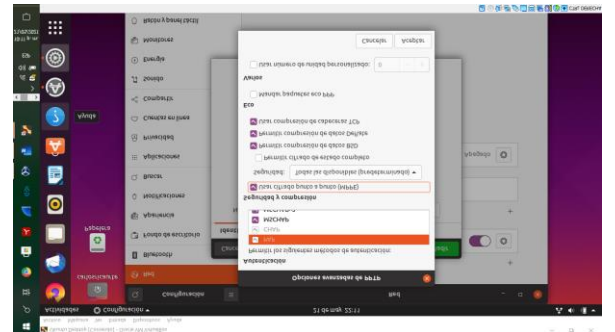


Imagen 102. Configuración de cifrado para la conexión VPN. Elaboración propia.

Ya estaría la configuración realizada y solo quedaría encenderla, primero pide autenticación del usuario.

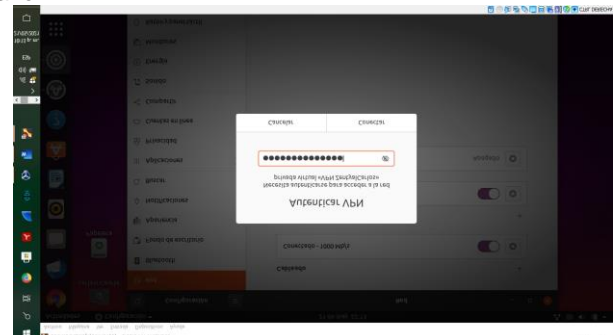


Imagen 103. Autenticación para habilitar VPN. Elaboración propia.

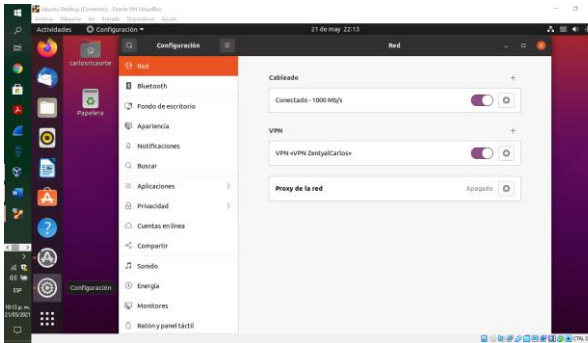


Imagen 104. VPN activada. Elaboración propia.

También se puede verificar que la VPN este corriendo en el servidor Zentyal.

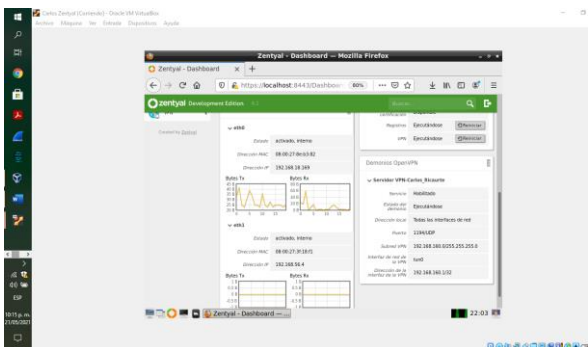


Imagen 105. Servidor VPN ejecutándose. Elaboración propia.

Conclusiones.

La implementación de Zentyal como herramienta de trabajo ha permitido gestionar recursos para compartir carpetas e impresoras por medio del controlador de dominio LDAP y el directorio activo que brinda mejores opciones para poder compartir información entre áreas de manera segura y controlada. A su vez evita el uso excesivo de recursos de almacenamiento e implementación de impresoras en cada grupo de trabajo.

Firewall zentyal es una herramienta que provee una administración fácil e intuitiva para poder realizar filtrado de paquetes por distintos protocolos y puerto, agrupándolos en objetos y luego en reglas para un mayor control de las implementaciones realizadas y los objetivos de cada regla creada.

Con el desarrollo de esta actividad se lograron obtener herramientas de mucha utilidad para el manejo de Zentyal, se logra realizar la conexión remotamente por medio del DNS y la adecuada configuración del DHCP y de esta forma lograr dar solución a los objetivos propuestos por la guía de actividades.

4. REFERENCIAS

[1] zentyal. (2019). descarga Zentyal. Obtenido de <https://zentyal.com/es/inicio/>

[2] Documentación de Zentyal 6.0, Copyright 2004-2018 Zentyal S.L. recuperado del enlace

<https://doc.zentyal.org/es/firewall.html>

[3] El Firewall de Zentyal es efectivo y facil de manejar. Jul 16, 2012, recuperado del enlace

<https://eltallerdelbit.com/firewall-zentyal/>

[4] Carceller Cheza, R. (2013). Servicios en red. Madrid, Spain: Macmillan Iberia, S.A. (Páginas. 32 - 162). Recuperado de <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/43261?page=33>

[5] Karzynski, M. (2014). Webmin Administrator's Cookbook. (Páginas. 35 - 357). Birmingham: Packt Publishing. Recuperado de

<https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=747086&lang=es&site=eds-live&scope=site&ebv=EK&ppid=Page-35>

[6]Gómez, L. J., & Gómez, L. O. D. (2014).

Administración de sistema operativos. (Páginas. 291 - 296).

Recuperado de <https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/62479?page=291>

[7]Bloquear facebook con Cortafuegos Zentyal-Server. Bilmer Perez. Recuperado de

<https://www.youtube.com/watch?v=kHCfxU0Enog>

[8]zentyal.org. (s.f.). zentyal.org. Obtenido de Servicio de directorio (LDAP):

<https://doc.zentyal.org/2.2/es/directory.html>