

Implementación y administración de Infraestructura en Zentyal basada en Roles y Servicios: DHCP, Domain Services, DNS, Firewall, VPN, File Server, Print Server y Proxy

Escuela de Ciencias Básicas Tecnologías Ingeniería-ECBTI, Universidad Nacional Abierta y a Distancia-UNAD

Gonzalo Javier Mancilla Paz
e-mail: gjmancillap@unadvirtual.edu.co
Luis Ehrman Gutiérrez Ch.
e-mail: luis.gutierrezzc@outlook.com
Jonathan Alexander Aguiar Quintero
e-mail: jaaguiarq@unadvirtual.edu.co
Oscar Rodolfo Guerrero Segura
e-mail: orguerreros@unadvirtual.edu.co
Byron David Guevara H.
email: bdguevarah@unadvirtual.edu.co

RESUMEN: *El Servidor Zentyal es una distribución de Linux que permite administrar los servicios de red a través de una sola plataforma. Nos ofrece una puerta de enlace de red, de igual manera un servidor de infraestructura, UTM (Unified Threat Manager).*

En este artículo daremos alcance a varias temáticas en las cuales documentaremos su implementación y manejo de Zentyal server, adquiriendo las competencias en la administración de los servicios de red, llevando a cabo la puesta en marcha de como: DHCP, DNS, Controlador de Dominio, Proxy no transparente, Cortafuegos, File, Print, VPN.

ABSTRACT: *The Zentyal server is a Linux distribution that allows manage the network services in only one platform. It offers a Gateway to the network, and infrastructure server, UTM (Unified Threat Manager).*

This article describes some topics related to implementation and usage of Zentyal server, to acquire the competences in the management of the network services, conducting the start up of DHCP, DNS, Domain Controller, HTTP Proxy Service, firewall, File Server, Print, and VPN.

PALABRAS CLAVE: Cortafuegos, Servidor, Ubuntu, Zentyal, Domain, File Server, VPN, Proxy, User DHCP.

1 INTRODUCCIÓN

Microsoft se considera un standard a nivel de servidores y recursos relacionados con infraestructura como lo es su servicio de Domain Services, Print server y File Share. Sin embargo, este tipo de servicios están disponible también en sistemas Linux.

Este artículo muestra los resultados de la instalación y puesta en marcha del servidor Zentyal 6.2 como sistema operativo base para disponer de los 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. Esta implementación es realizada luego de configurar el firewall Endian con la zona verde para la red LAN, la zona naranja o DMZ donde se instala en servidor Zentyal y la zona roja de salida a internet. Permitiendo tener redes independientes que no representen un riesgo para la integridad de la seguridad de la información.

El procedimiento aquí plasmado brinda la información necesaria no solo para la implementación si no también para una administración básica de los servicios expuestos. Toda la red es montada con máquinas virtuales de VirtualBox en un laboratorio controlado.

2 INSTALACIÓN DEL SERVIDOR ZENTYAL EN LA ZONA DMZ

Inicialmente, observemos en la imagen número 1 la configuración del firewall Endian y sus zonas. Donde se observa que el Zentyal está en la zona naranja. De esta manera se independizan las redes brindando una mayor seguridad de la información y permitiendo un balanceo de carga en la red.

Se procede a realizar la instalación del servidor Zentyal siguiendo las instrucciones de pantalla.

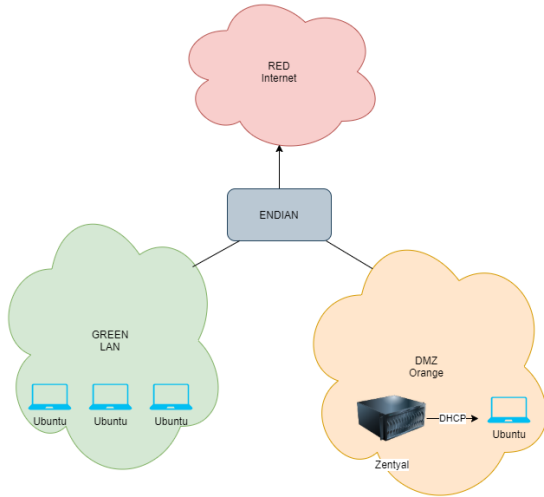


Imagen 1. Configuración de zonas de red

Partiendo del firewall Endian instalado con sus respectivas zonas configuradas, procedemos a instalar el servidor Zentyal en la zona naranja o DMZ.

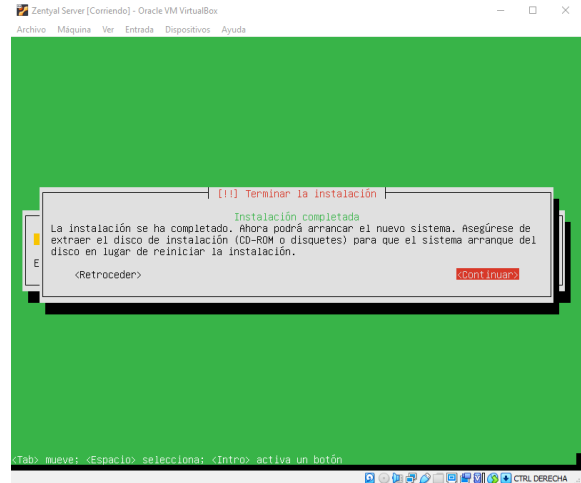


Imagen 4. Configuración de red Zentyal

Se selecciona la interfaz primaria de red.

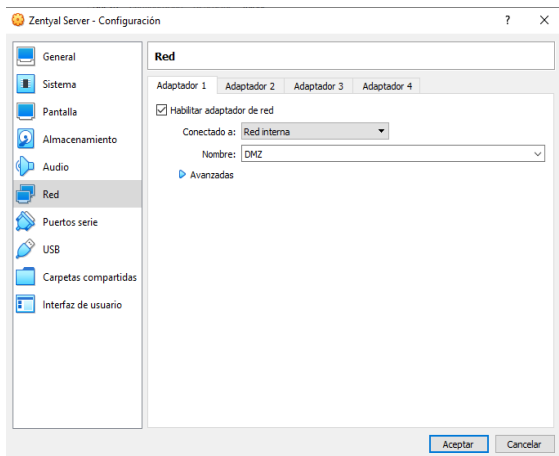


Imagen 2. Configuración de red externa

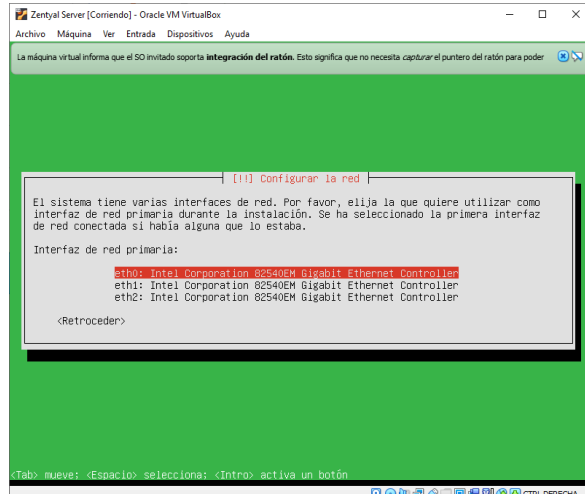


Imagen 5. Selección de interfaz primaria de red

Se configura el usuario y contraseña.

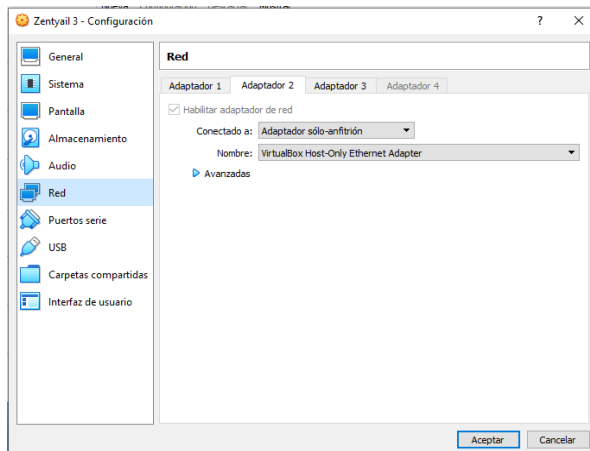


Imagen 3. Configuración de red interna

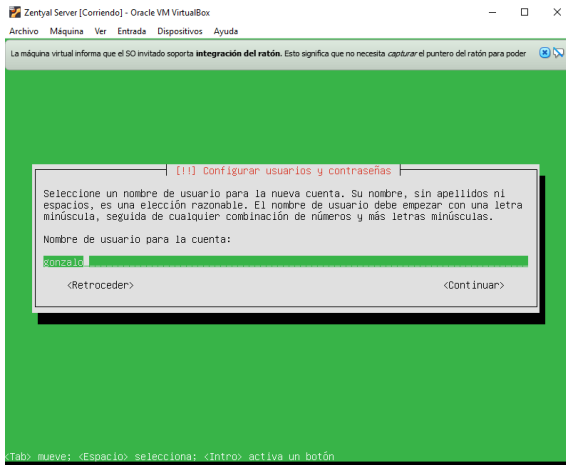


Imagen 6. Configuración de usuario y contraseña

Zentyal termina de instalar el sistema.

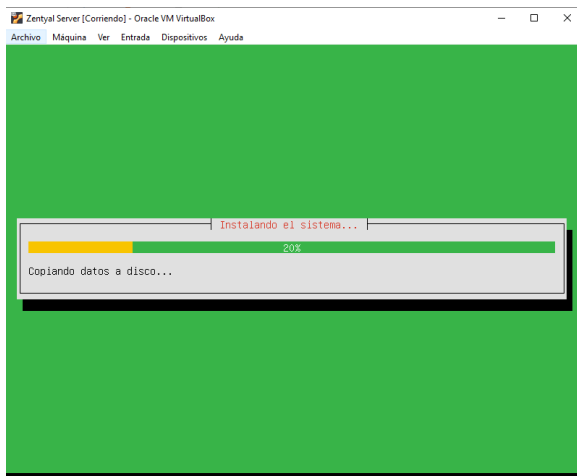


Imagen 7. Instalación sistema

Luego se procede a iniciar sesión.

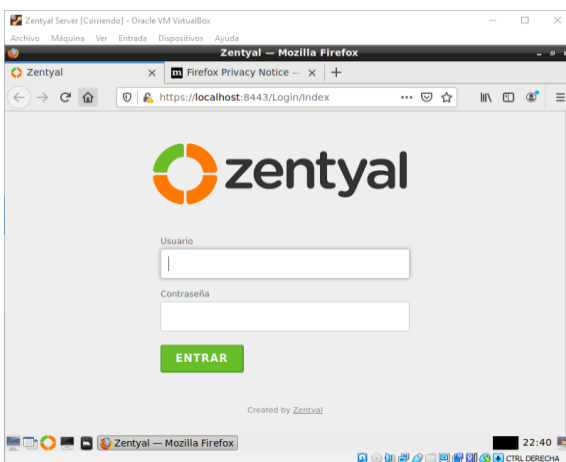


Imagen 8. Inicio de sesión

Se realiza la configuración inicial.



Imagen 9. Configuración inicial

Se seleccionan los paquetes necesarios para ser instalados.

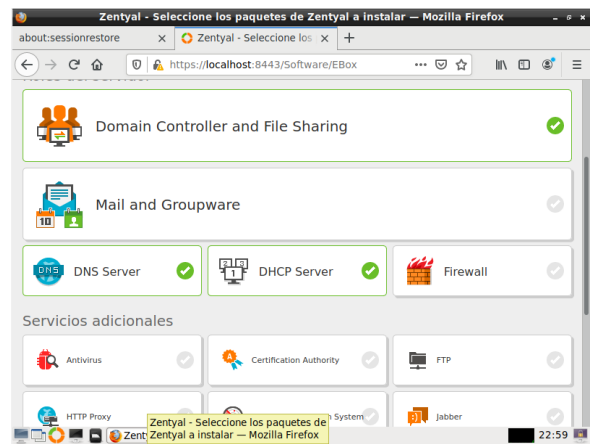


Imagen 10. Selección de paquetes a instalar

Se realiza la instalación

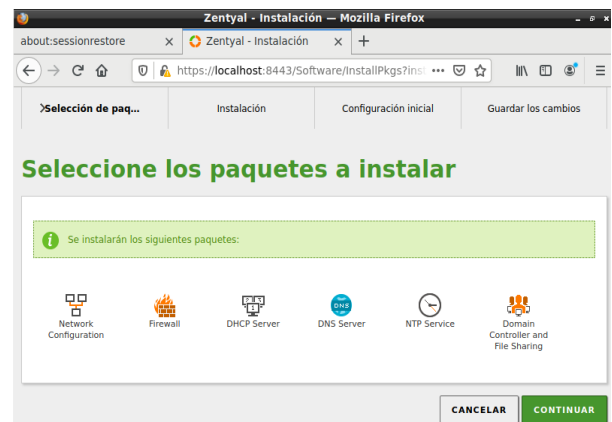


Imagen 11. Instalación de paquetes

Se confirma que la instalación ha terminado y se puede acceder al dashboard.

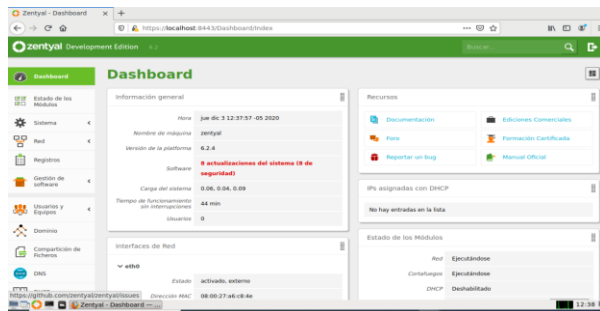


Imagen 12. Acceso al dashboard

3 Servidor DHCP, Servidor DNS y Controlador de dominio

3.1 Servidor DHCP

Antes de describir la implementación del servidor con protocolo de configuración dinámica de hosts con Zentyal se puede decir que, *DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN [1].*

Para configuración de DHCP vamos a pestaña red y luego a interfaces, donde se encuentra la interfaz de conexión con el firewall Endian y la interfaz para DHCP de la subred interna.

Interfaz eth0 de conexión con Endian recibe conexión DHCP, ya que el Endian tiene la red naranja configurada para DHCP, aunque puede ser configurada de forma estática en ambas partes.



Imagen 13. Interfaz de red eth0

Interfaz eth1 se utilizó para crear la nueva subred DHCP dentro de la zona naranja donde definimos una dirección IP fija y posteriormente un rango de IPs para los computadores clientes en la zona DMZ.

Para que el servicio DHCP funcione, al menos debe haber un rango de direcciones a distribuir o asignaciones estáticas; en caso contrario el servidor

DHCP no servirá direcciones IP aunque esté escuchando en todas las interfaces de red [2].



Imagen 14. Interfaz de red eth1

Luego vamos al menú DHCP donde creamos el rango para equipos DHCP.



Imagen 15. Menú DHCP

En la siguiente imagen se puede observar la creación de un rango que va de la IP 192.168.200.2 a 192.168.200.30, este rango genera la subred en la zona DMZ, donde un equipo Ubuntu cliente recibe su asignación de IP.



Imagen 16. Rangos DHCP

En la página principal del dashboard se observa la IP asignada al Ubuntu cliente de la zona DMZ conectado al servidor DHCP.

IPs asignadas con DHCP		
Dirección IP	Dirección MAC	Nombre de máquina
192.168.200.2	08:00:27:e4:ba:3f	cliente

Imagen 17. Asignación IP DHCP

3.2 Servidor DNS

Primeramente, antes de entrar a describir el proceso realizado (López padilla, p6) nos da una definición de DNS. *Fundamentalmente, DNS se encarga de traducir direcciones IP de recursos de red a nombres fácilmente legibles y memorizables por las personas, y viceversa. A esta acción se la conoce como "resolución DNS" [3].*

Para configurar el servidor DNS en Zentyal nos aseguramos de que en el estado de módulos esté habilitado el módulo DNS, luego vamos a la sesión DNS.

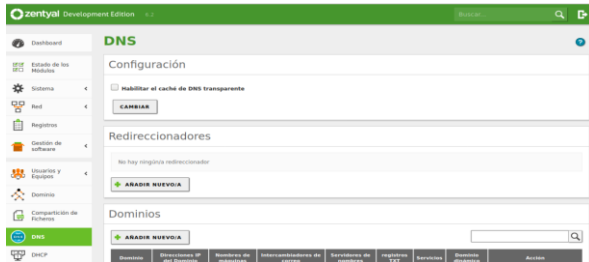


Imagen 18. Menú DNS

En la parte de abajo tenemos la sesión de dominios, donde hemos creado tres dominios, para tres máquinas.

Nombre	Dirección IP del dominio	NetBIOS del dominio	Interconexiones de servicios	Servicios de dominio	Registro TXT	Servicios	Estado	Acción
clientanetpa.com							X	
dominio.com							✓	
zentyal.com.co							X	

Imagen 19. Creación de dominios

Luego vamos a la sesión DHCP presionamos en configuración de la red y definimos DNS local.

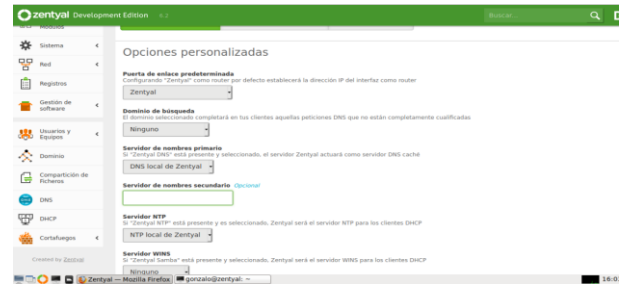


Imagen 20. Definición DNS local

Comprobación de dominio: para comprobar los equipos asociados al dominio usamos el comando nslookup en la línea de comandos, y podemos ver el siguiente resultado desde el servidor.



Imagen 21. Comprobación dominio en servidor

3.3 Controlador de Dominio

Primeramente, debemos asegurarnos de que el módulo controlador de dominio esté habilitado en estado de los módulos. Una vez hecho esto comprobamos en el menú dominio que el servidor está en función controlador de dominio.



Imagen 22. Menú controlador de dominio

Posteriormente vamos a usuarios y equipos donde podemos gestionar usuarios. En los siguientes ejemplos se observan las imágenes de edición del usuario invitado y la creación de un usuario.



Imagen 23. Editar usuario Invitado



Imagen 24. Añadir usuario

Ahora que el controlador de dominio está activado y se tienen las configuraciones necesarias, el usuario creado que es unido a Domain Admins, tendrá todos los permisos sobre el dominio.

En el menú usuarios y equipos tenemos opciones de configuración de LDAP (Protocolo Ligero de Acceso a Directorio), donde podemos encontrar la información de LDAP y opciones de configuración PAM.



Imagen 25. Configuración LDAP

Al habilitar la opción PAM los usuarios quedan con cuenta en la máquina local.

4 Proxy no transparente

Después de haber realizado la instalación de Zentyal, procedemos primero a hacer la configuración de las interfaces de red.

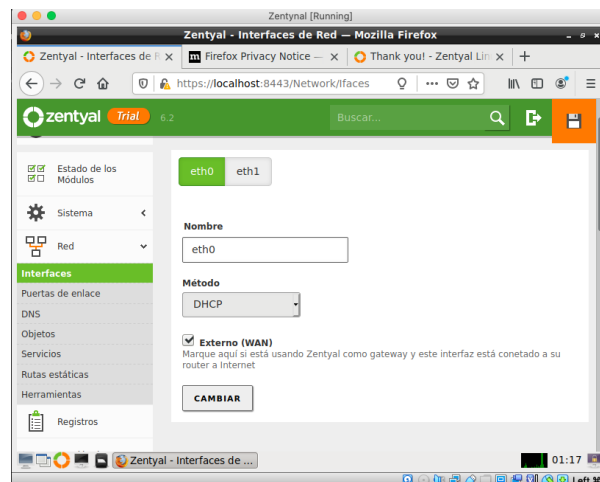


Imagen 26 Interfaces de red via WIFI

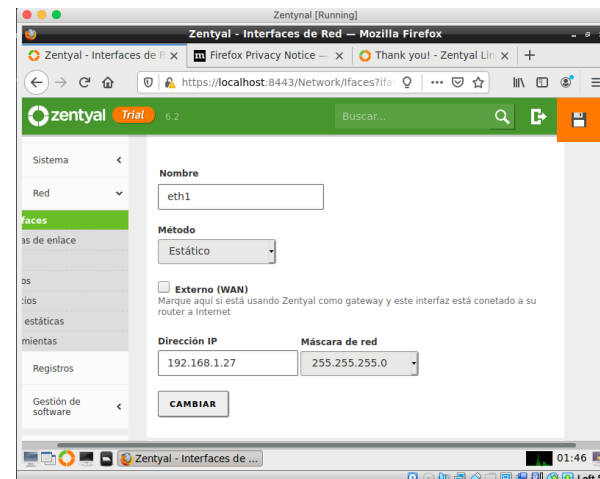


Imagen 27 Interfaz por LAN

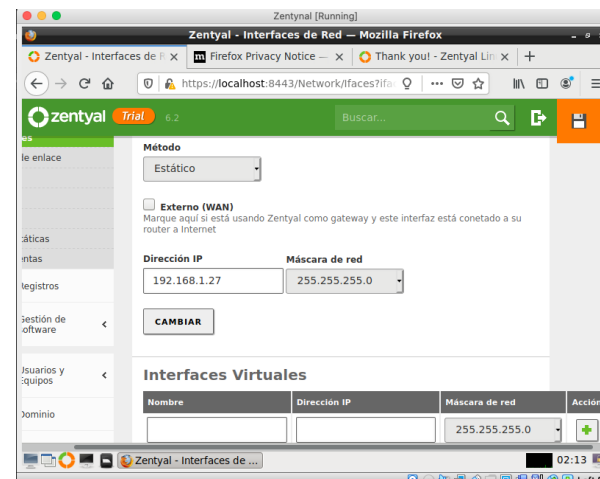


Imagen 28 asignación de IP

Se hace la creación del objeto de red

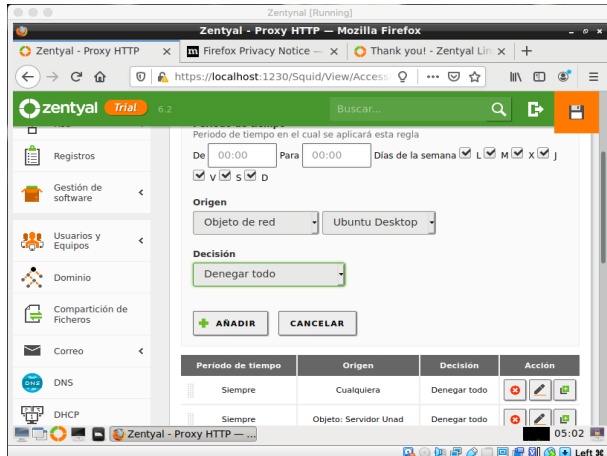


Imagen 29. Denegacion de servicios

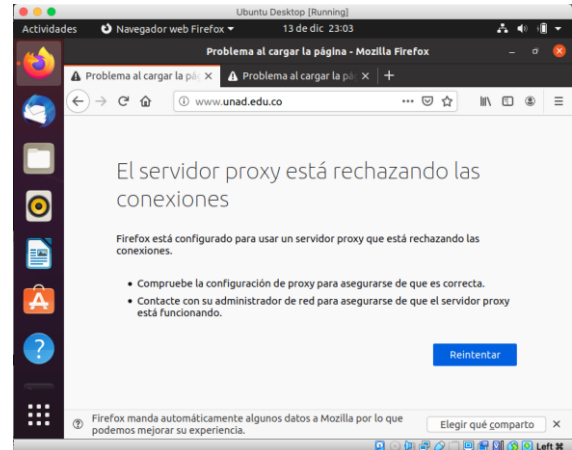


Imagen 32 Funcionamiento proxy

5 Cortafuegos

Seleccionamos qué funcionalidades queremos incluir en nuestro sistema. Para este caso activamos el Firewall y DHCP server.

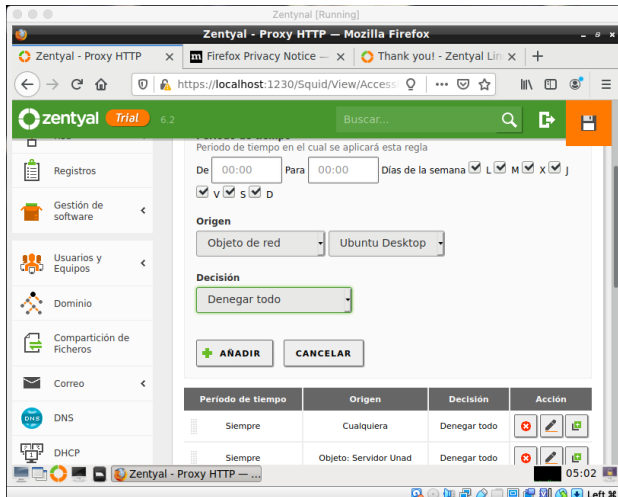


Imagen 30 Creacion del proxy transparente

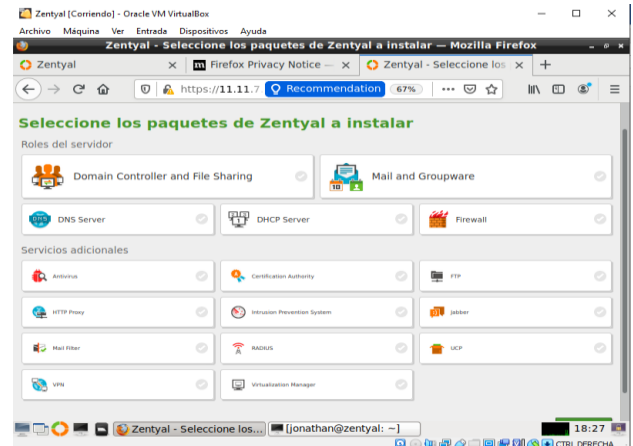


Imagen 33 Selección paquete firewall

Se abre la maquina virtual anterior con la cual vamos a realizar la prueba del proxy no transparente.

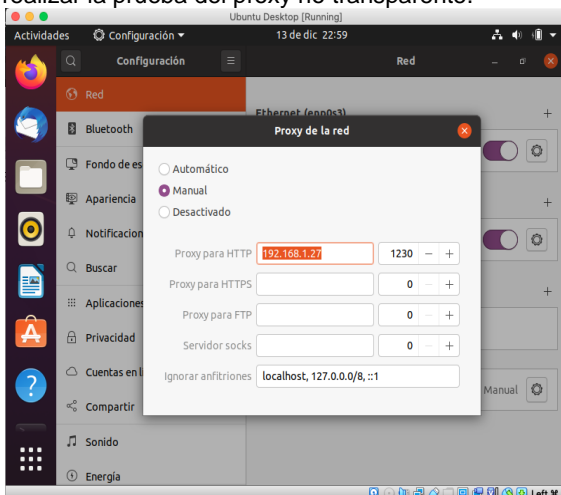


Imagen 31 Asignación proxy en Ubuntu Desktop

En perfiles de filtrado añadimos "General".

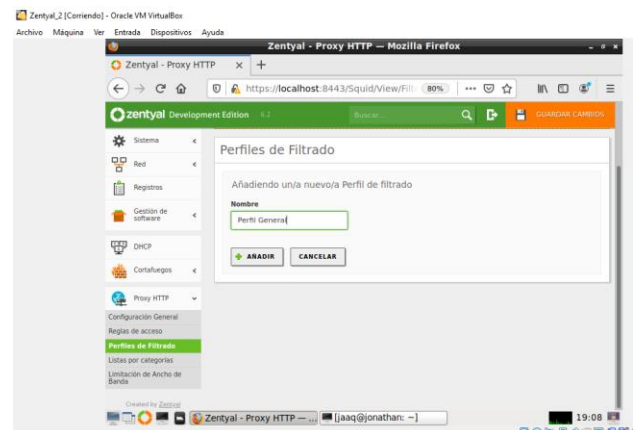


Imagen 34 creación perfiles

En la parte configuración de filtrados de dominios ingresamos las direcciones de las paginas para bloquear.

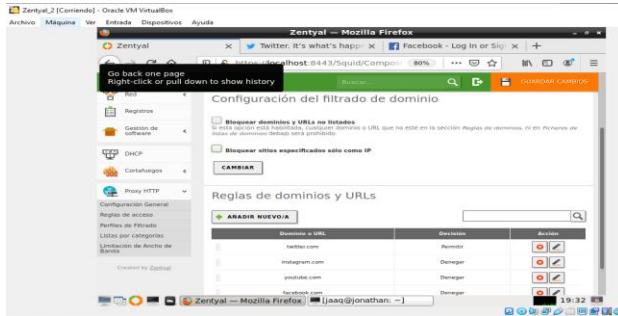


Imagen 35 Bloqueo de dominios

En la parte de objetos creamos un usuario con los datos de nuestra maquina cliente.

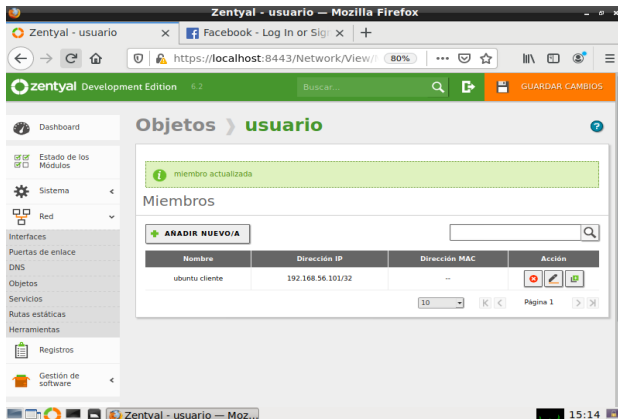


Imagen 36 Añadir miembros

Creamos una lista de objetos con el nombre de redes sociales.

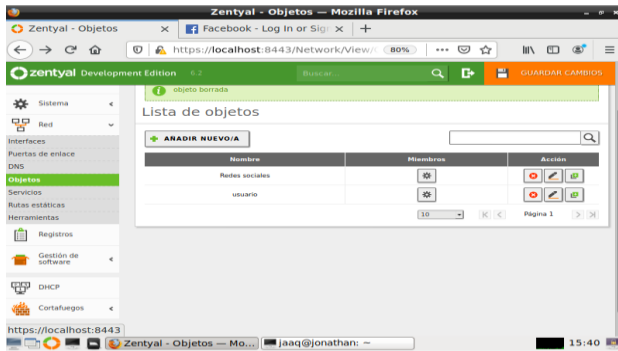


Imagen 37 Lista de objetos

Utilizamos el comando nslookup mas el dominio para conocer la IP que utiliza el dominio.

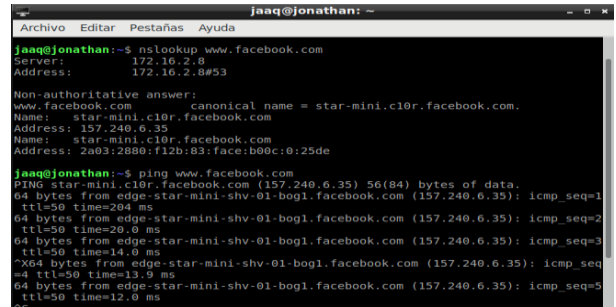


Imagen 38 ping Facebook

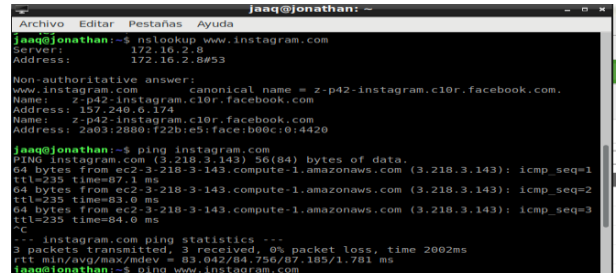


Imagen 39 ping Instagram

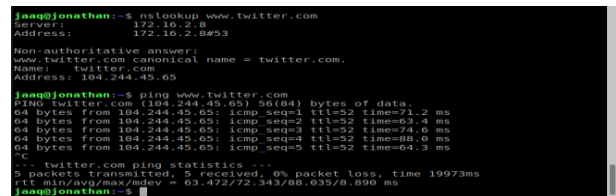


Imagen 40 Ping twitter

De esta manera queda la lista de objetos de redes sociales con las direcciones ip de los sitios restringidos.

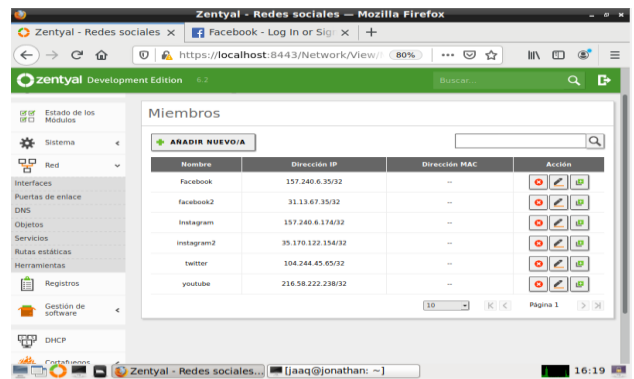


Imagen 41 bloques definidos

Direccionamos cliente al servidos de forma manual

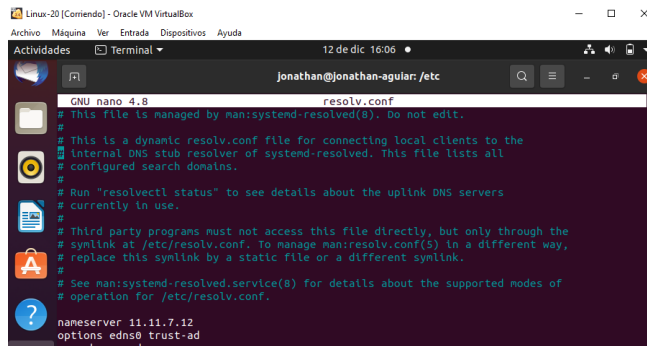


Imagen 42 cliente servidor

Observamos que el cliente tiene conexión a internet

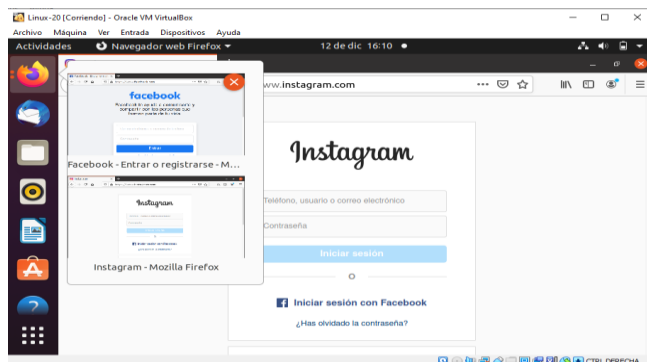


Imagen 43 navegación del cliente

Ingresamos al módulo cortafuegos en la parte de "reglas de filtrado para las redes internas".



Imagen 44 reglas de filtrado de redes

Creamos una regla para denegar el acceso a las redes sociales por parte de nuestro cliente. En el origen elegimos Usuario que es nuestro cliente y en la opción destino seleccionamos redes sociales que es la que contiene las direcciones de las redes sociales que deseamos bloquear la navegación.



Imagen 45 filtrado de paquetes

Una vez creada la regla, procedemos a guardar los cambios dando clic sobre la opción guardar que se encuentra en la parte superior derecha.



Imagen 46 resultados de filtrados definidos

Resultado final, después de aplicar las reglas.

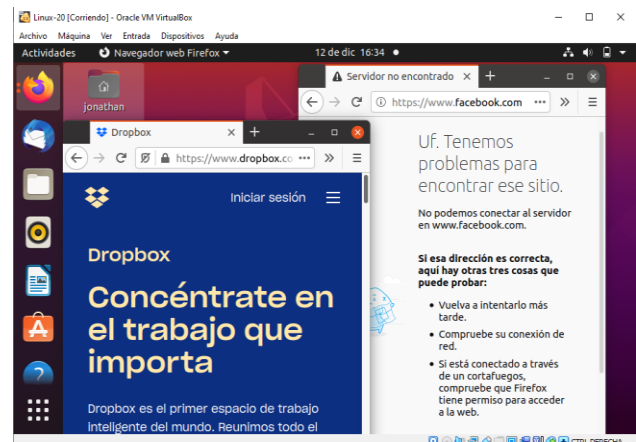


Imagen 47 restricciones aplicadas

6 Servidor de archivos y servidor de impresoras

Se debe iniciar agregando el rol de Domain Controller y Fileshare en el Servidor Zentyal para que pueda tener LDAP. Esto configura de manera automática servicio de DNS.

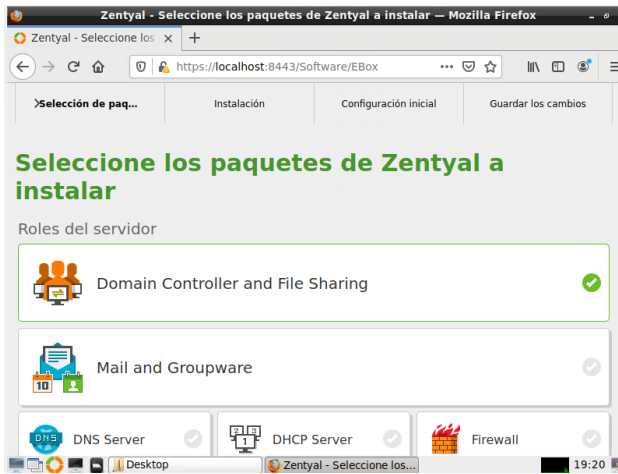


Imagen 48 configurando rol

Procedemos con la configuración del dominio asignando un hostname para el servidor, un dominio y una descripción en la pestaña system.

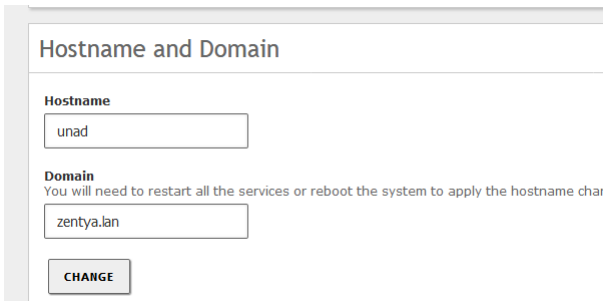


Imagen 49 estableciendo dominio

Nos dirigimos a usuarios y equipos del dominio y agregamos 3 cuentas de dominio, una para Domain admin, otra para iniciar en Windows y una ultima para iniciar en Ubuntu. Adicionalmente se crean dos grupos de seguridad uno para Fileshare y otro para Print Access.

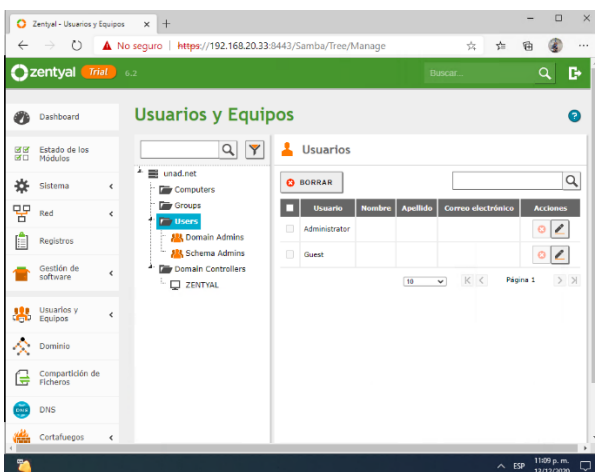


Imagen 50 creando usuarios

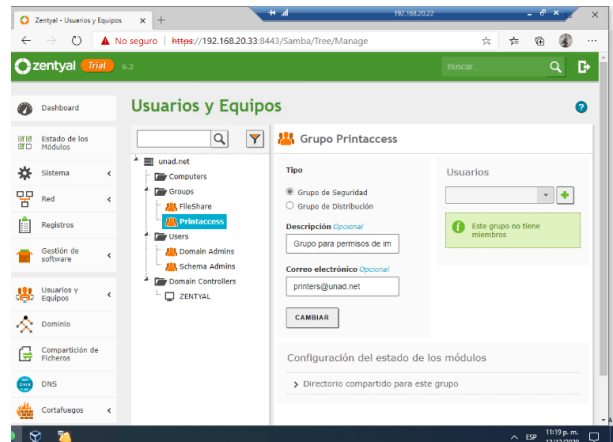


Imagen 51 creando grupos

Procedemos a unir los equipos Windows 7 y el Ubuntu al dominio.

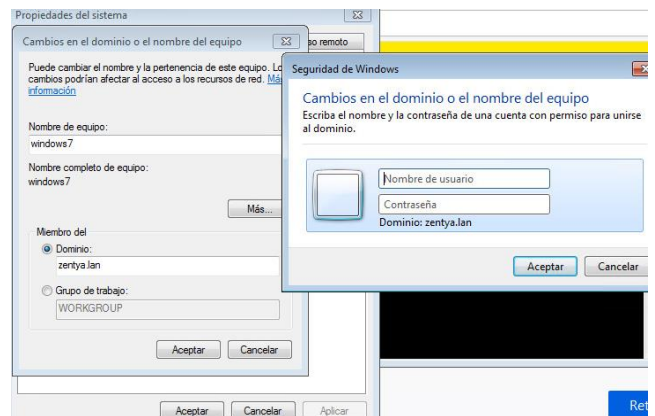


Imagen 52 Registrando equipo windows en dominio

(Mutuai J. 2020). dice como unir Ubuntu a un dominio. El proceso puede aplicarse cualquier tipo de dominio.

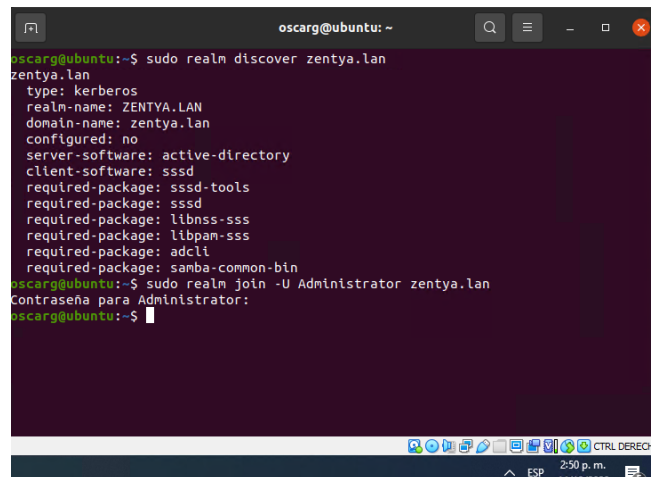


Imagen 53 registrando equipo ubuntu en dominio

En el menú izquierdo ingresamos a comparticion de ficheros y creamos una nueva ruta compartida.

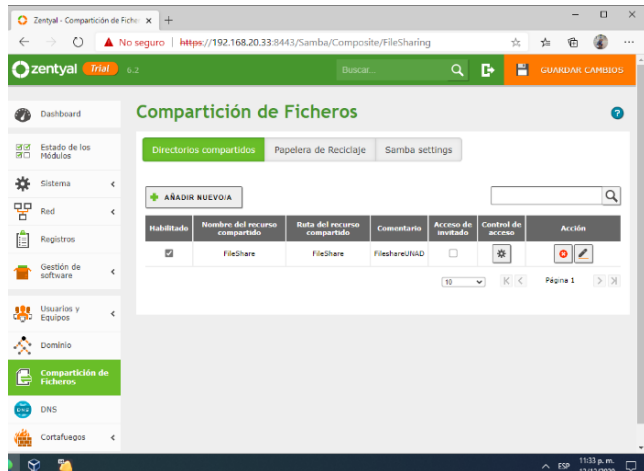


Imagen 54 creando ruta compartida

Brindamos acceso solo al grupo de seguridad de Fileshare.

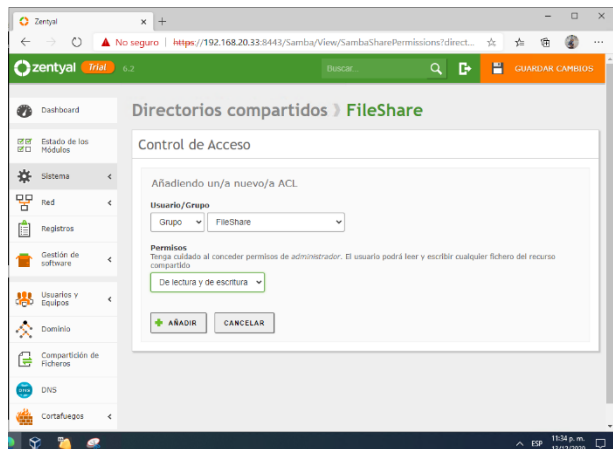


Imagen 55 permisos en ruta compartida

Probamos el acceso desde un equipo que no esté en el dominio al igual que en equipos que esté en dominio y evidenciamos que solo funciona en el equipo registrado al dominio donde la cuenta que es miembro del grupo ha sido cargada.

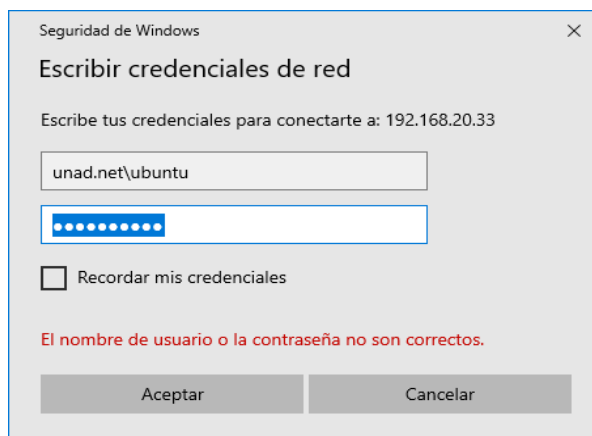


Imagen 50 acceso denegado a ruta compartida

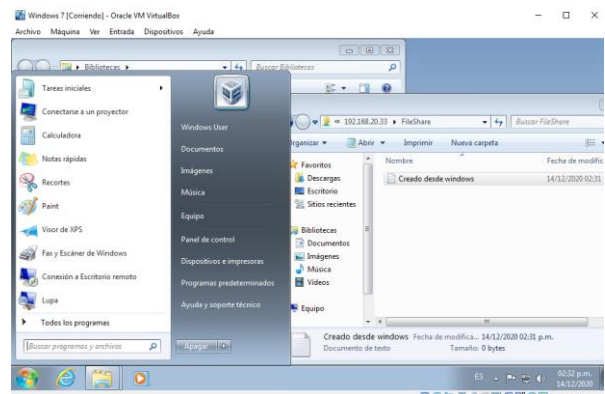


Imagen 51 acceso satisfactorio a ruta compartida

Instalamos la impresora a compartir en uno de los equipos y la compartimos asignando permisos de autorización solo a los miembros del grupo Print Access previamente creado.

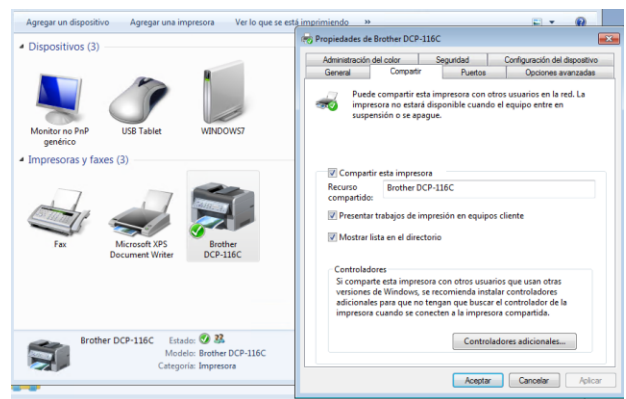


Imagen 52 compartir impresora

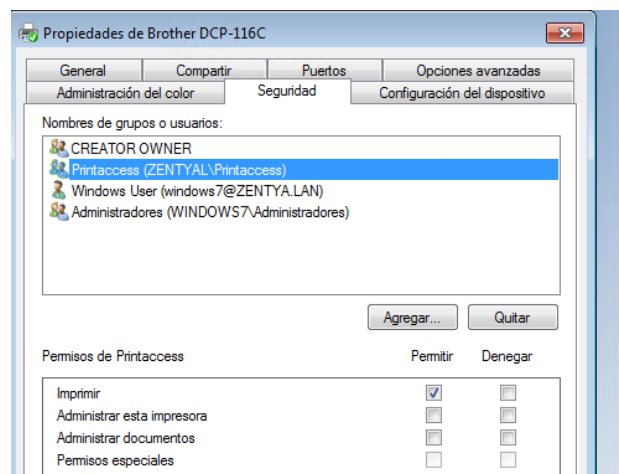


Imagen 53 establecer permisos para grupo en LDAP

Con esta configuración solo los miembros del grupo Print access tendran permitido imprimir y los accesos serán dados a través del LDAP del Domain services de Zentyal.

7 VPN

La configuración de VPN se inicia con la configuración de certificados. Se selecciona la opción de Certification Authority y General para el Servidor.



Imagen 54. Autoridad de Certificación

Procedemos a crear el Servidor VPN en el panel izquierdo, Servidores.



Imagen 55. Crear Servidor VPN

Creamos el certificado para el cliente que se conectará con la VPN creada, para ello vamos al menú Autoridad de certificación.



Imagen 56. Autoridad de Certificación Cliente

Se configura el Servidor VPN, validamos el puerto y seleccionamos el certificado creado en el paso anterior. Seleccionamos Interfaz TUN.



Imagen 57. Configuración de puertos en el servidor

Agregamos un nuevo servicio VPN.



Imagen 58. Crear nuevo Servicio VPN

Al servicio creado le configuramos el puerto.



Imagen 59. Configurar puerto Servicio VPN

Se configura el Cortafuegos opción filtrado de paquetes.



Imagen 60. Cortafuego y filtrado de paquetes

Clic opción reglas de filtrado desde las redes internas a Zentyal y añadimos el servicio creado en el paso anterior.



Imagen 61. Configuración de reglas de filtrado

Configuramos las redes que se van a conectar, opción ficha VPN opción redes anunciadas, creando el Objeto.

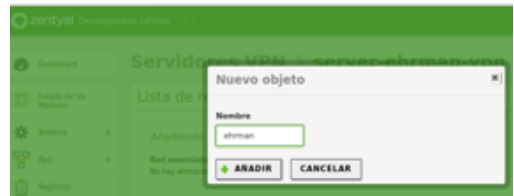


Imagen 62. Crear Objeto, redes anunciadas

Se descarga paquete de configuración del cliente.

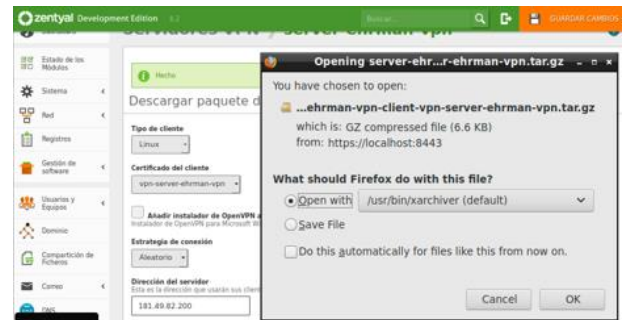


Imagen 63. Descarga certificado VPN cliente

Se validan los servicios en Zentyal.

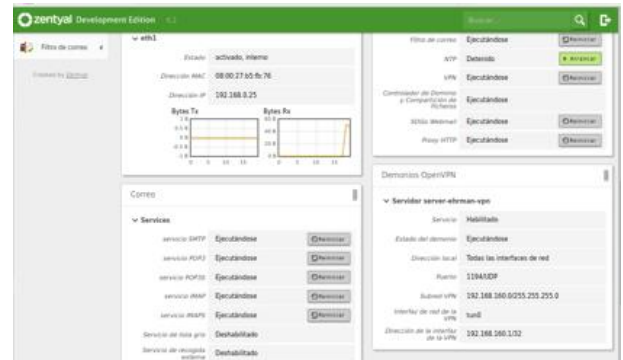


Imagen 64. Servicios activos en Zentyal

Desde el cliente Ubuntu descargamos la aplicación Open VPN con el comando `sudo apt-get install network-manager-openvpn-gnome`.

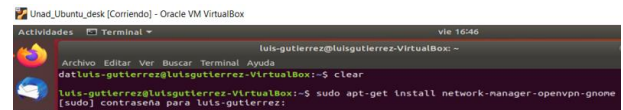


Imagen 65. Instalación Open VPN Desktop

Abrimos la conexiones de red para su edición.

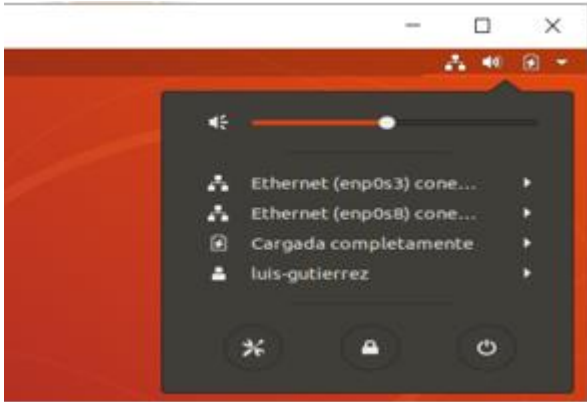


Imagen 66. Edición conexiones de Red en Desktop

Importamos el certificado generado en Zentyal-configuración VPN guardada.



Imagen 67. Importar Certificado VPN generado en Zentyal

Importamos la configuración de la carpeta que se ha descargado.

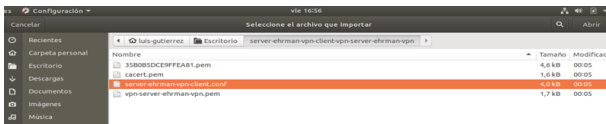


Imagen 68. Carga configuración VPN de Zentyal

Se carga el certificado para su reconfiguración.

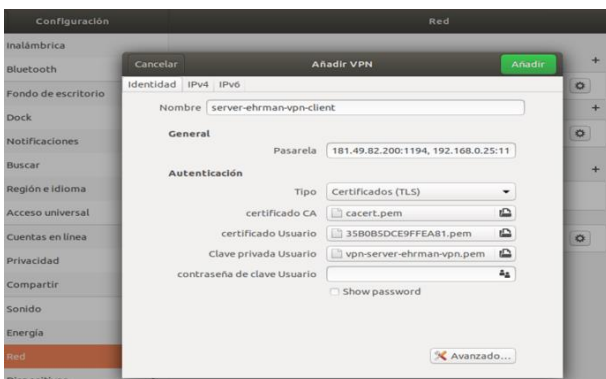


Imagen 69. Carga del Certificado VPN de Zentyal

Habilitamos el puerto 1194 para la comunicación para ello pulsamos el botón Avanzado.



Imagen 70. Configuración de puertos.

Se muestra la conexión creada.



Imagen 71. Conexión cargada a Ubuntu Desktop.

Abrimos la conexión creada opción Conectar.



Imagen 72. Conectarse VPN en Ubuntu Desktop.

Se establece la conexión con la VPN, verificamos.

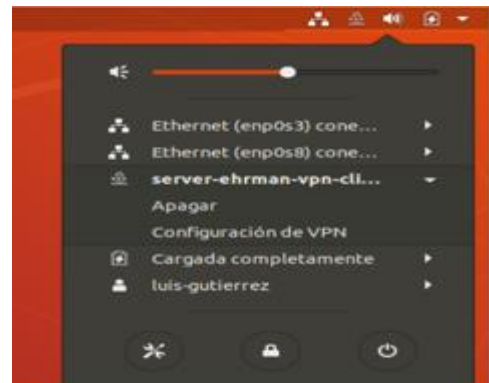


Imagen 73. Conectado VPN en Ubuntu Desktop.

8 Conclusiones

El servidor Zentyal es una herramienta bastante práctica, fácil de usar y es un sistema operativo rápido que facilita la configuración de servicios por medio de la interfaz gráfica, de igual manera tiene a su servicio la línea de comando si se desean realizar ciertas tareas.

Zentyal es un servidor basado en Ubuntu muy simple, que contiene todos los servicios necesarios para resolver la gestión de los servicios básicos necesarios para crear una empresa, incluyendo: gestión de redes, servidor de correo, comunicación, recursos compartidos y trabajo en grupo: servidor de archivos, impresión Gestión de usuarios centralizada de software de servidor y grupo, autoridad de certificación. Además, este servidor nos da un periodo de 45 días para poder probarlo sin necesidad de hacer la compra, tiene una curva de manejo fácil y se hace bastante sencillo su manejo, esto ayuda tanto a ingenieros senior, como junior a gestionar de forma adecuada y correcta los recursos necesarios para manejar la red.

El servicio VPN que ofrece Zentyal nos permite dar alcance a usuarios dentro de nuestra red interna, ofreciendo el control a través de reglas, mediante certificados que pueden ser implementados en maquina Linux, Windows entre otros, trabajando como puerta de enlace.

Un servidor Zentyal cuenta con muchos de los recursos que entrega un Windows Server para el uso de recursos compartidos se recomienda controlar por grupos de seguridad.

El active Directory es una base de datos donde se pueden almacenar distritos objetos como equipos, servidores, grupos o usuarios.

9 REFERENCIAS

- [1] *El protocolo DHCP y su funcionamiento* (s. f.). Universidad de Granada. Recuperado de <https://www.ugr.es/~fernanla/Untitled.pdf>
- [2] *Servicio de configuración de red (DHCP)—Documentación de Zentyal 2.2.* (2011). Recuperado de <https://doc.zentyal.org/2.2/es/dhcp.html>
- [3] López Padilla, A. (s. f.). *Guía de Seguridad en Servicios DNS.* España. P6 Recuperado de: https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/guia_de_seguridad_en_servicios_dns.pdf
- [4] Mutuai J. (diciembre de 2020). *Join Ubuntu 20.04|18.04 / Debian 10 To Active Directory (AD) Domain.* www.computingforgeeks.com. Recuperado de: <https://computingforgeeks.com/join-ubuntu-debian-to-active-directory-ad-domain/>