

INSTALACIÓN Y CONFIGURACIÓN DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO, PROXY NO TRANSPARENTE, CORTAFUEGOS, SERVICIOS FILE SERVER, PRINT SERVER Y VPN

Pedro Pulido Serrato
pepulidos@unadvirtual.edu.co
Jose Manuel Cuchimba Vargas
jmcuchimbav@unadvirtual.edu.co
Eduar Ricardo Vela Pinilla
eduar-ricardopp@hotmail.com
Juan Pablo Parra Muñoz
anjumoz@hotmail.com
eduar-ricardopp@hotmail.com
Servio Dario Lopez Ortega
sdlopezo@unadvirtual.edu.co

RESUMEN: *El presente documento se detalla, muestra y evidencia el proceso realizado en la instalación de los diferentes procesos de administración y control de red que permite el servidor Zentyal. En el cual se realizará la Instalación y configuración DHCP Server, DNS Server y Controlador de Dominio, También un Proxy no transparente, Cortafuegos, servicios File Server, Print Server y VPN.*

Todo lo anterior mencionado con la intención de que, como grupo de trabajo, terminemos de dar solución a la problemática de puesta en marcha una infraestructura de red de acuerdo a los servicios y requerimientos específicos solicitados por el cliente*

PALABRAS CLAVE: Zentyal, DHCP, Proxy, Dominio, VPN, DNS, Firewall, Ubuntu, File Server, Print Server.

Abstrac: *This document details, shows and evidences the process carried out in the installation of the different network administration and control processes that the Zentyal server allows. In which the Installation and configuration of the DHCP Server, DNS Server and Domain Controller will be carried out, as well as a non-transparent Proxy, Firewall, File Server, Print Server and VPN services.*

All of the above mentioned with the intention that, as a working group, we finish solving the problem of setting up a network infrastructure according to the specific services and requirements requested by the client.

Keywords: Zentyal, DHCP, Proxy, Dominio, VPN, DNS, Firewall, Ubuntu, File Server, Print Server.

1 INTRODUCCIÓN

Como culminación del proceso de aprendizaje que se realiza se muestra como proponer soluciones bajo el sistema operativo GNU/Linux específicamente Zentyal Server 6.2 con su debida instalación, configuración para lograr un ambiente enfocado a la implementación de infraestructura IT de mayor nivel en la intranet y extraen

garantizando la seguridad, migración y puesta en marcha dado respuesta al servicio solicitado.

Además, adquirir destreza y planear soluciones tipo cliente-servidor se da respuesta a la actividad Paso 8 - Solucionando necesidades específicas con GNU/Linux, del curso de profundización como opción de grado.

2 REQUISITOS PREVIOS DE ACTIVIDAD

2.1 ACERCA DE ZENTYAL 6.2

Servidor Zentyal ofrece la primera implementación nativa de Microsoft Active Directory® en Linux que es fácil de usar. El Servidor Zentyal se ha convertido en una alternativa de Windows Server, actualmente es el servidor número uno para muchas empresas y organizaciones en todo el mundo

2.2 DESCARGAR ZENTYAL 6,2

Lo primero sea realizar la descarga del .iso que necesitamos para proceder con la instalación de la máquina virtual, para ello será necesario ingresar a la página oficial de Zentyal y descargar: <http://download.zentyal.com/zentyal-6.2-development-amd64.iso>

2.3 CONFIGURAR MÁQUINA VIRTUALES

Como segundo paso será realizar la configuración de nuestras máquinas virtuales, 1 donde se contará con un servidor (ZENTYAL) el cual tendrá 2 tarjetas de red, 1 NAT o puente y otra en RED INTERNA, ya que 1 será la que nos permita la conexión a internet (servidor-Router) y la otra de dar conexión (servidor -cliente). En cuando a la segunda máquina, será una máquina de Ubuntu 18.04 LTS el cual contará con 1 tarjeta de red, la cual estará en modo RED INTERNA. (Ver imagen 1 y 2).

Los requisitos para que funcione de manera correcta cada máquina, se colocan en la Tabla 1.

Tabla 1: Requisitos Maquinas

Maquina	Red	Disco	RAM
Zentyal 6.2	2 Tarjetas	15GB	4096 MB
Ubuntu 18.04	1Tarjeta	20GB	4096 MB

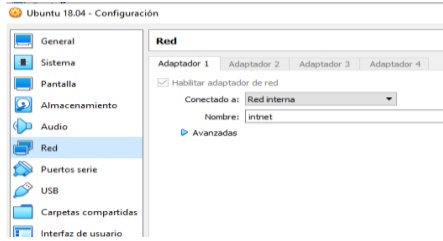


Imagen 1 Máquina Ubuntu

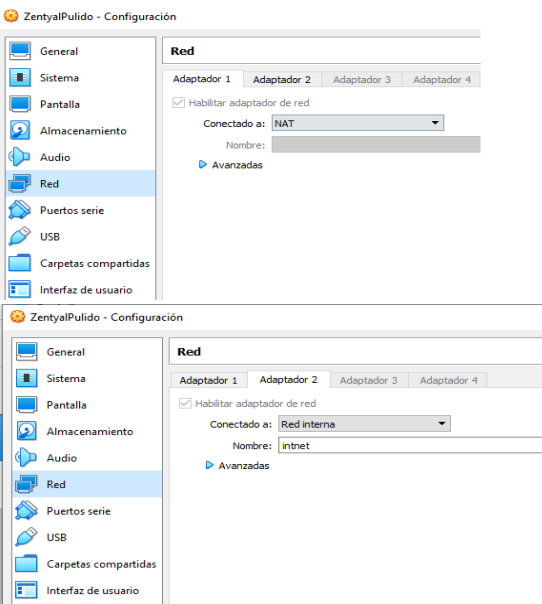


Imagen 2 Máquina Zentyal

2.4 INSTALACIÓN ZENTYAL 6,2

Una vez configurada la máquina para Zentyal, lo que haremos será proceder con el proceso de instalación, el cual es sencillo.

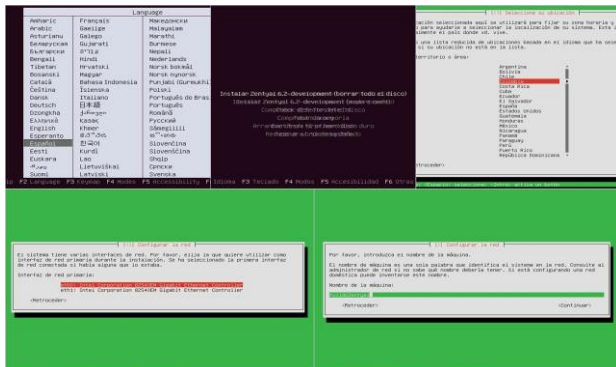


Imagen 3 Instalación Zentyal



Imagen 4 Instalación Zentyal

Al finalizar la instalación, nos quedara un escritorio similar a cualquier sistema operativo. Al igual que iconos de acceso rápido para el administrador.

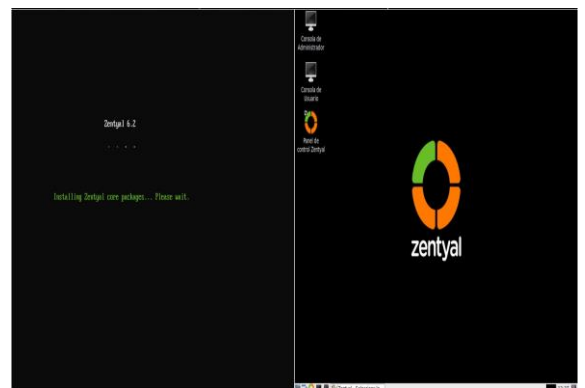


Imagen 5. Finalización de instalación Zentyal

Una vez terminado dicho proceso, estando en escritorio lo que hacemos es iniciar, mediante el “Panel de control Zentyal” el cual nos permitirá iniciar la configuración de nuestro servidor y la red.

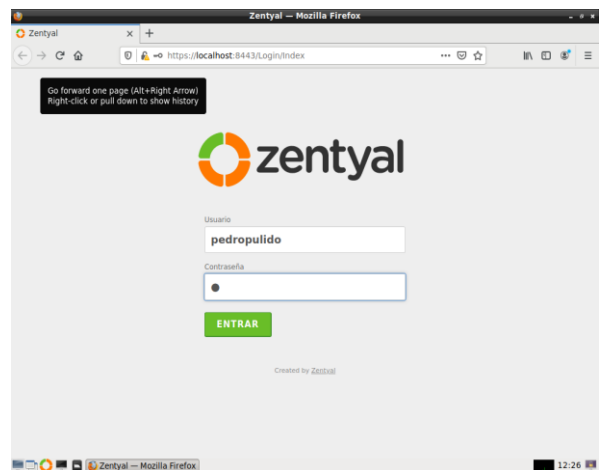


Imagen 6 Panel de Acceso Zentyal.

Aquí podemos proceder a realizar la configuración inicial, configurar las tarjeas de red y los diferentes módulos que requerimos, se pueden “SALTAR” y después configurar, queda a elección.



Imagen 7 Imagen 8 Configuración Inicial Zentyal

Una vez terminemos de instalar los módulos que requerimos y las configuraciones iniciales básicas nos quedará una interfaz donde podemos ya iniciar las diferentes configuraciones de acuerdo con las temáticas

3 TÍTULO PRINCIPAL

Es importante menciona las temáticas a desarrollar en este documento, también se describe el paso a paso de cada una de ellas, como es su configuración e implementación mediante el servidor Zentyal 6.2, a continuación, se menciona cada una y que servicio se debe implementar.

Tabla 2 Temáticas

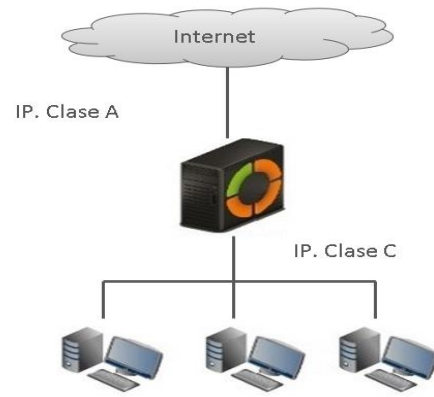
TEMATICA	SERVICIOS
1	DHCP Server, DNS Server y Controlador de Dominio.
2	Proxy no transparente.
3	Cortafuegos.
4	File Server y Print Server
5	VPN.

3.1 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.

3.1.1 DHCP Server

Es necesario identificar como va a ser utilizado Zentyal con respecto a las direcciones IP:



Paso 1: Lo primero es identificar la configuración de los dos adaptadores de red, debido a que una de ellas debe quedar como DHCP para la red externa y la otra como red interna y estado estático.

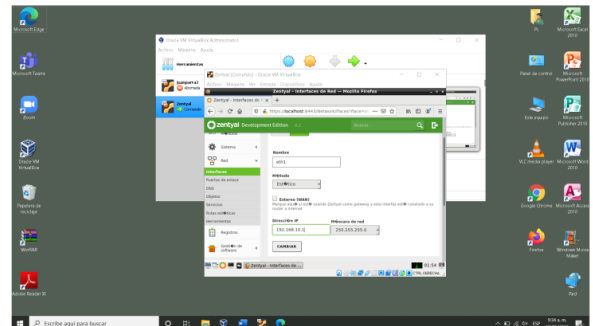


Imagen 9. configuración de red LAN con Ip estática (19-05-2021) Elaboración Propia

Paso 2: Se procede a realizar la asignación de los rangos con forme a las sugerencias.

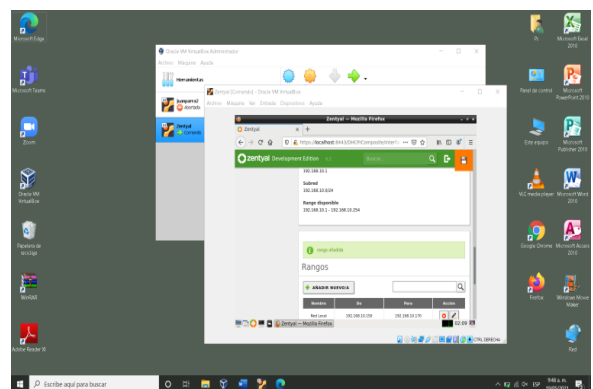


Imagen 10. En el modulo de DHCP- asignación de Rangos (15-05-2021) Elaboración Propia

Paso 3: Se procede a realizar los cambios realizados, y se comprueba el funcionamiento.

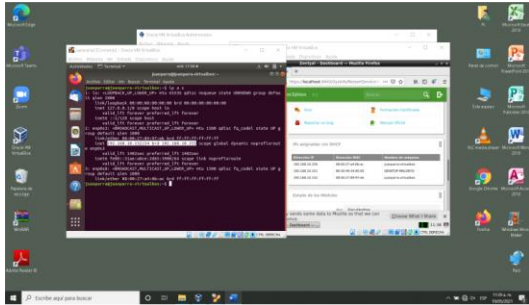


Imagen 11. Imagen 12 Se puede Visualizar la conexión desde el cliente y el servidores Zentyal (19-05-2021) Elaboración Propia

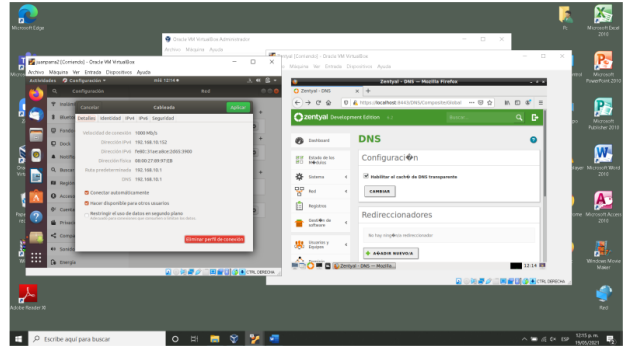


Imagen 15. Comprobamos el funcionamiento identificando el DNS en la maquina cliente. (19-05-2021) Elaboración Propia

3.1.2 DNS Server

Paso 1: Para la configuración del servidor de resolución de nombre de dominio, nos dirigimos al menú de Zentyal y confirmamos que el módulo este activo y guardado, seguido procedemos a realizar la debida configuración, como principio habilitando el cache de DNS- transparente:

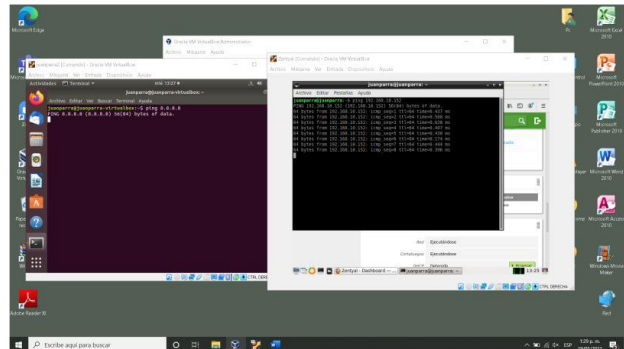


Imagen 16. se Realiza una pin de prueba desde Zentyal.(15-05-2021) Elaboración Propia

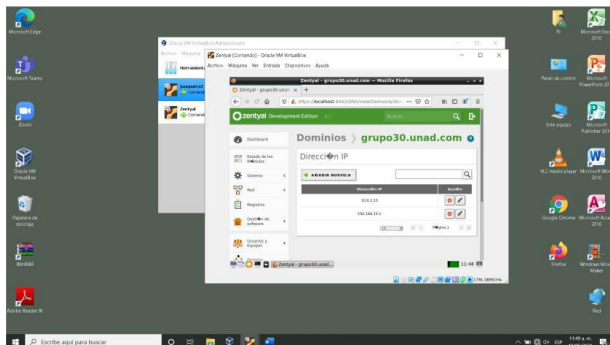


Imagen 13. Interfaz de Dominios adicionamos nuestra IP configurada. (19-05-2021) Elaboración Propia

Paso 2: seguido de la identificación y confirmación de la configuración del nombre de dominio

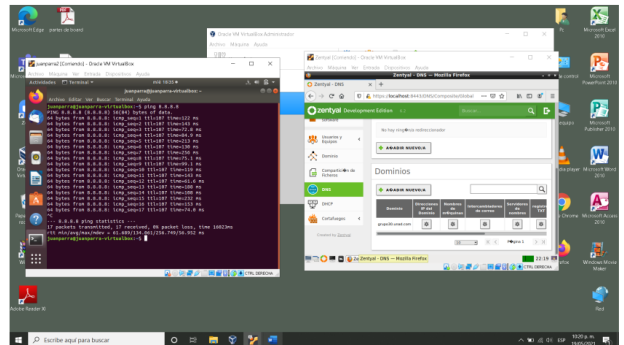


Imagen 17. se realiza un pin de prueba desde la maquina cliente.(15-05-2021) Elaboración Propia

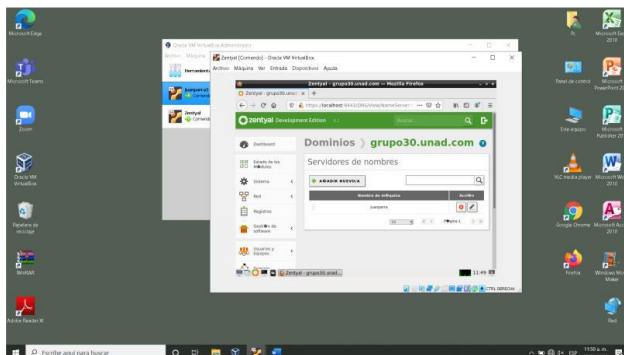


Imagen 14. Identificamos el nombre del dominio con su IP.(19-05-2021) Elaboración Propia

Paso 3: Después de realizar la comprobación de proceder a guardar los cambios y la comprobación verificando en la maquina cliente y un ping desde Zentyal.

3.1.3 Controlador de Dominio:

nos da una serie de servicios distribuidos en información y compartimiento de clientes unidos al dominio.

Paso 1: Para iniciar con la configuración es indispensable activar el módulo y guardarlo con eso ya se procede a habilitar los perfiles móviles y el nombre de dominio.

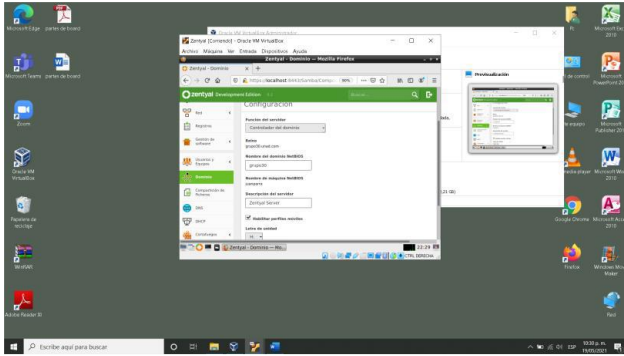


Imagen 18 Habilitamos perfiles móviles y la damos el nombre al dominio. (19-05-2021) Elaboración Propia

Paso 2: Se guardan los cambios realizados y se procede a crear el usuario

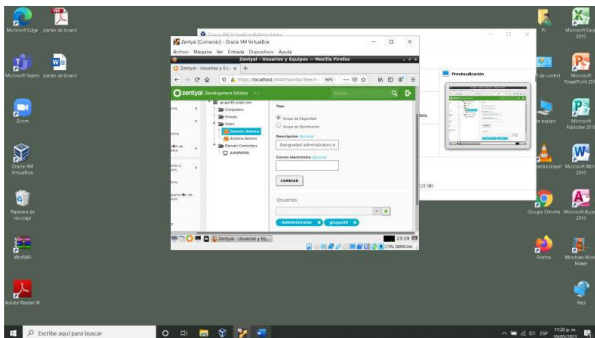


Imagen 19. se crea un usuario denomindo-grupo30. (19-05-2021) Elaboración Propia

Paso 3: En la maquina cliente se instalan los correspondientes complementos se actualiza y agrega la dirección del servidor.

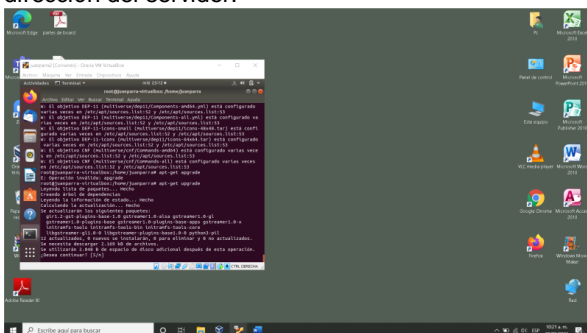


Imagen 20 En la maquina cliente es necesario realizar actualizaciones. (19-05-2021) Elaboración Propia



Imagen 21. se habilita la dirección IP del servidor. (19-05-2021) Elaboración Propia

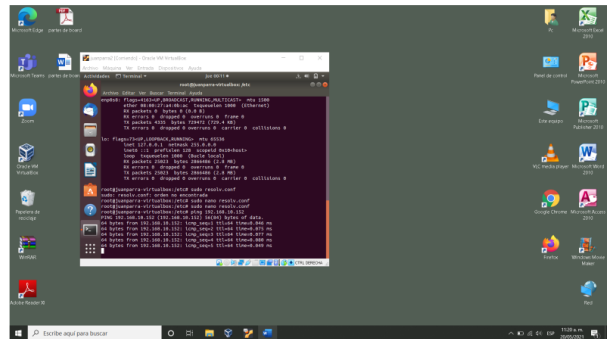


Imagen 22. se realiza un pin de prueba desde la maquina cliente. (19-05-2021) Elaboración Propia

3.2 Temática 2: proxy no transparente

Paso 1. Entramos a la zona de DHCP, en las interfaces se da clic al botón de configuración

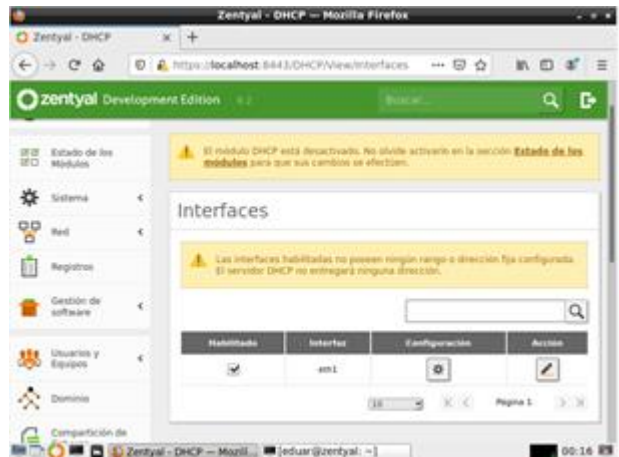


Imagen 23 Imagen21Intefaz .

Paso 2. En la sección de red, en las interfaces se configura la red eth0 en DHCP para la comunicación con la red WAN.

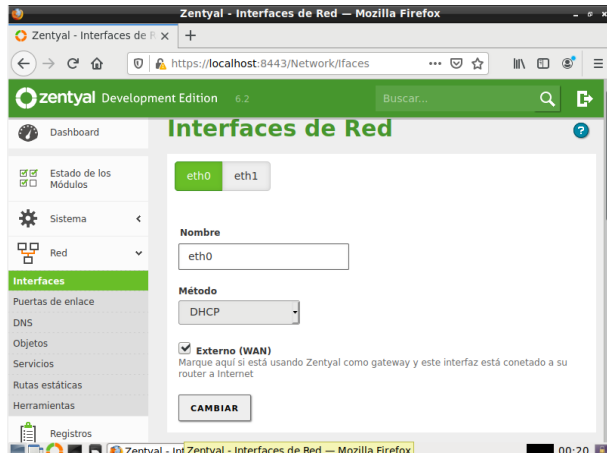


Imagen 24. Interfaz red 1.

Paso 3. Se configura la red eth1 en estático y se asigna una IP.

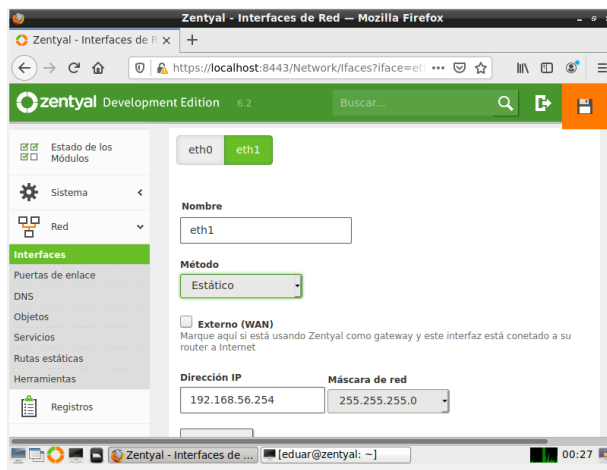


Imagen 25. Interfaz red 2

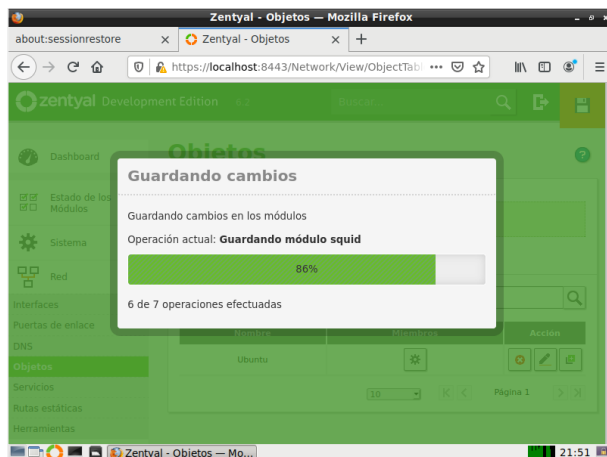


Imagen 26. Guardan cambios.

Paso 5. Se configura el proxy transparente y el puerto por el cual va a escuchar

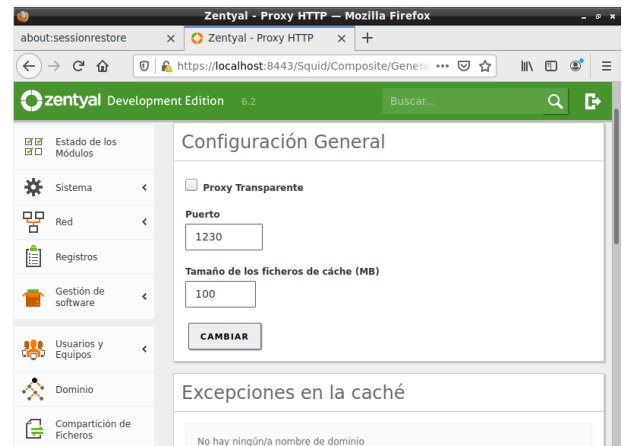


Imagen 27. Interfaz de configuración.

Paso 6. Se configura la regla de acceso para el objeto previamente creado, donde se deniega todas las peticiones.

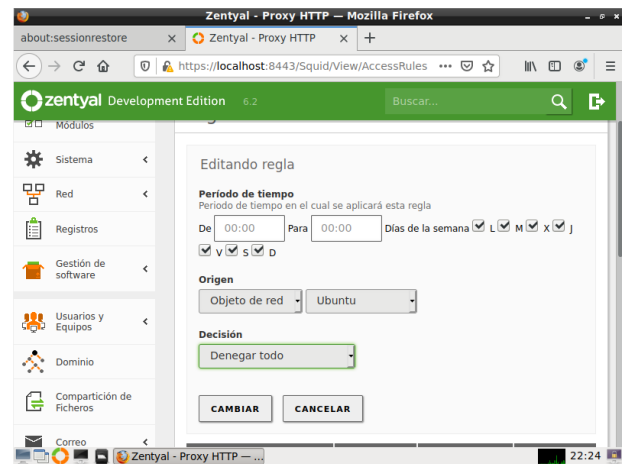


Imagen 28. Interfaz

Paso 7. Se configura el proxy en el equipo de Ubuntu desktop.

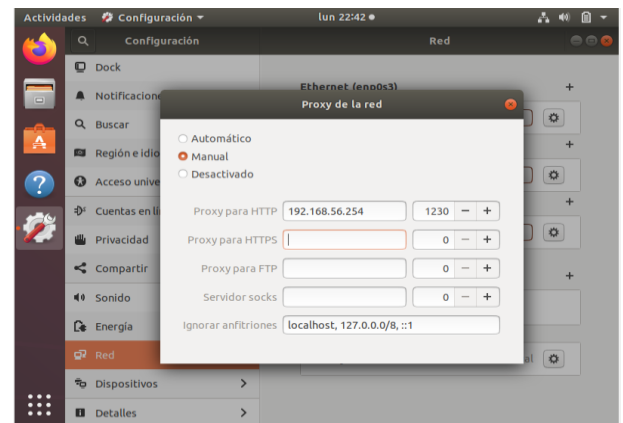


Imagen 29. Interfaz De configuración.

Paso 8. Evidenciamos un claro ejemplo en nuestra maquina virtual el funcionamiento normal de la maquina virtual desktop se ingresa normal internet.

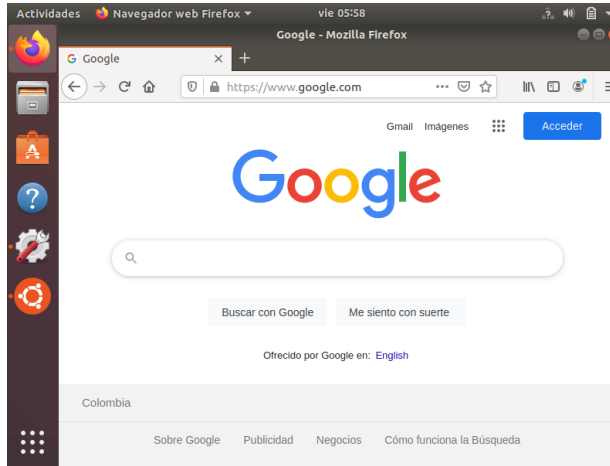


Imagen 30. Comprobación.

Paso 9. Por último evidenciamos la configuración del proxy no transparente donde evidenciamos que no nos deja ingresar a ninguna de las páginas web.

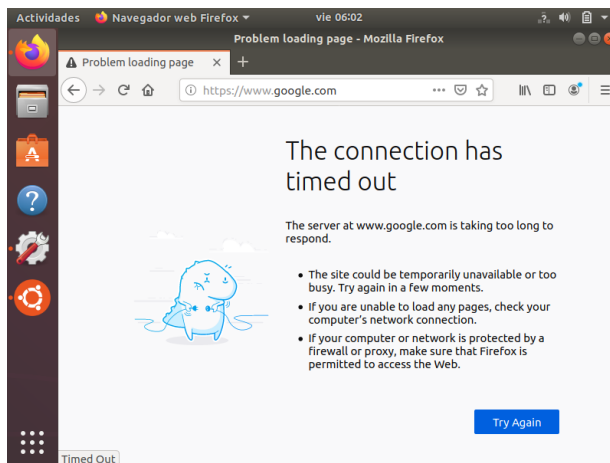


Imagen 31. comprobación

3.3 Temática 3: Cortafuegos

Lo primero que haremos será realizar el proceso de configuración de nuestro servidor Zentyal para que este le de conexión mediante DHCP a nuestro cliente (Ubuntu 18.04 LTS) el cual se conectará mediante este para poder realizar las restricciones solicitadas. Para ello lo primero será realizar la configuración de la primera tarjeta de red eth0 como DHCP.

Así mismo será la de realizar el proceso de configuración de la segunda red, eth1 como una IP estática, la cual tendrá como IP a 192.168.7.254 / 255.255.255.0.

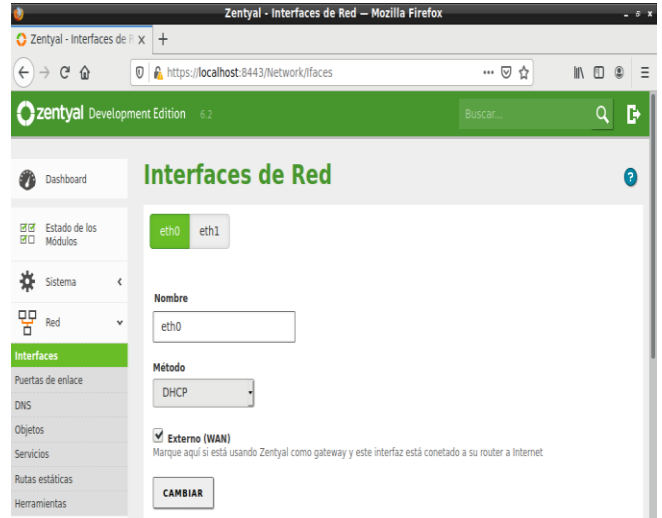


Imagen 32. interfaz de red



Imagen 33. interfaz de red 2

Posteriormente, será realizar la configuración del DHCP (Interfaz), para ello accedemos al módulo del mismo nombre en Zentyal para proceder con dicha configuración.

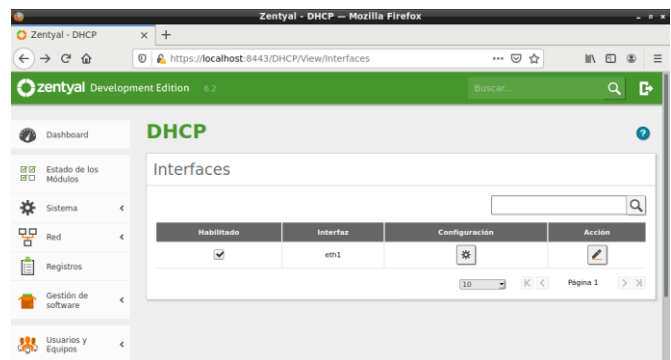


Imagen 34. interfaz de red DHCP

Aquí, dentro de configuraciones lo que haremos será realizar el proceso de asignar rangos, es decir de donde queremos que se asigne la primera IP a nuestro equipo hasta cual, en nuestro caso teniendo en cuenta

que iniciamos desde 192.168.7.1 dejamos 19 IPS sin asignar y vamos a realizar el rango a partir de la IP 192.168.7.20 la cual debe ser la que se le asigne automáticamente a nuestro cliente cuando se conecte, ya que solo habrá una maquina (Ubuntu 18.04 LTS).

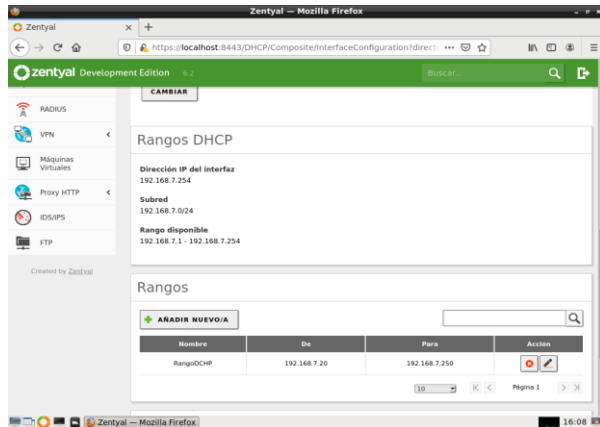


Imagen 35. Rangos de red DHCP

Una vez terminada parte de la configuración de nuestra red en el servidor ZENTYAL vamos a realizar el proceso en nuestra máquina de cliente, la cual tiene como S.O. Ubuntu 18.04 LTS, para verificar que esta funcionando nuestro DHCP y tenga conexión a internet para luego proceder con las restricciones.

Accedemos en nuestra máquina.

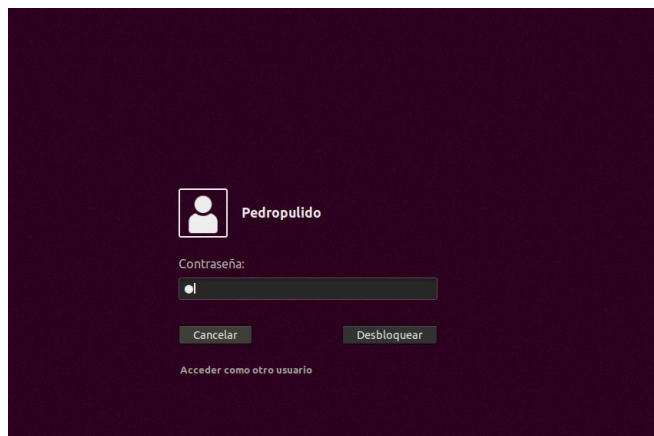


Imagen 36. ingreso a máquina cliente

Vamos a las configuraciones de RED, donde vamos a verificar a que ya tenga INTERNET VIA DHCP, para ello simplemente damos en de DETALLES:

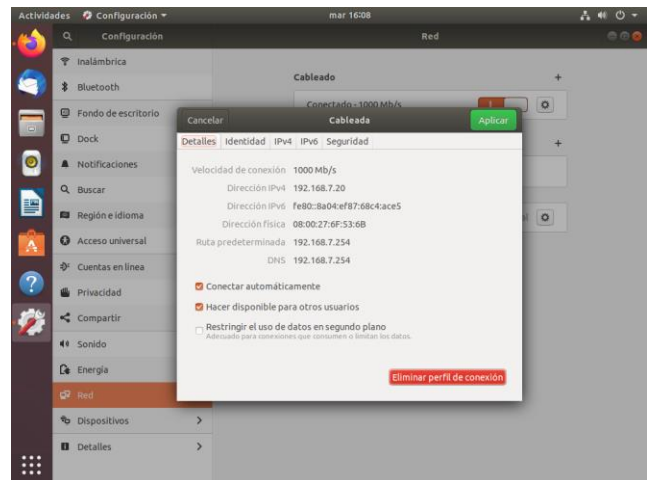


Imagen 37. Red cliente

Una manera de también verificar es ir a nuestro servidor ZENTYAL y ver en el apartado de conexiones por DHCP en la cual tiene que aparecer nuestra máquina.

IPs asignadas con DHCP

Dirección IP	Dirección MAC	Nombre de máquina
192.168.7.20	08:00:27:6f:53:6b	pedropulido

Imagen 38. Máquina conectada vía Zentyal

Ahora una vez verificado que si esta funcionando las conjuraciones que realizamos de manera previa en nuestro servidor, lo que haremos será probar la conexión a internet a los sitios que VAMOS A RESTRINGIR, para ello en este caso serán: Redes sociales como FACEBOOK, TWITTER, Imagen X. Conexión Twitter INSTAGRAM y por el lado de entretenimiento será una página de deportes, MUNDODEPORTIVO.

Muestra de CONEXIÓN a internet a los sitios:

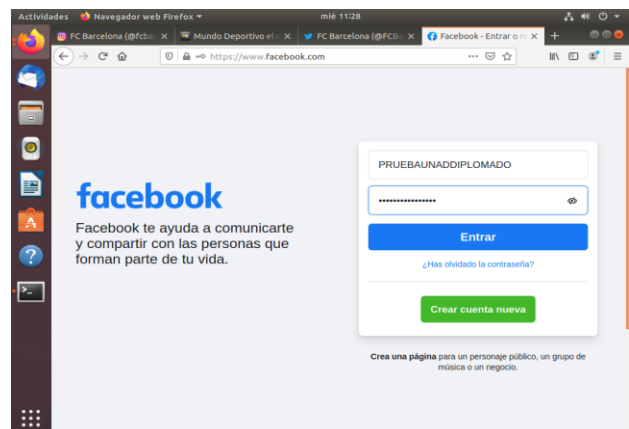


Imagen 39. Conexión Facebook

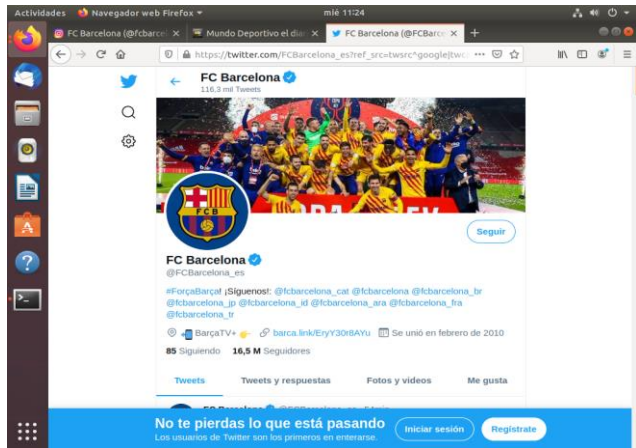


Imagen 40. Conexión Twitter

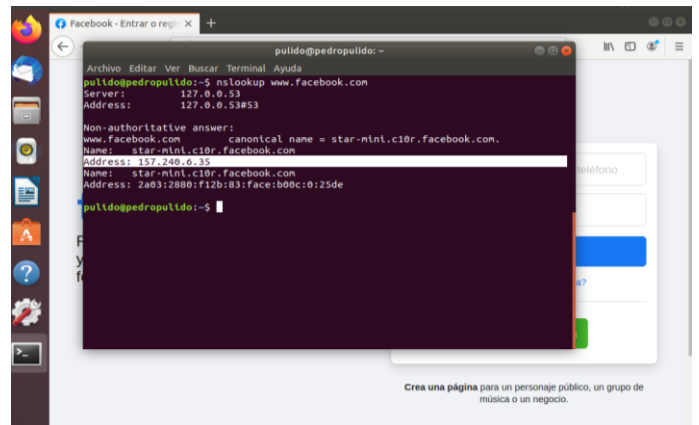


Imagen 43. Ejecución comando nslookup

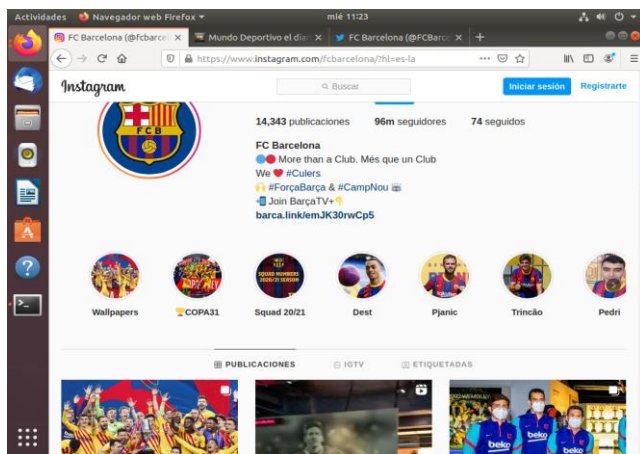


Imagen 41. Conexión Instagram

Una vez obtenida dicha IP, nos dirigimos a nuestro servidor Zentyal. Vamos a la opción "CORTAFUEGOS", posteriormente a la opción "FILTRADO DE PAQUETES", y una vez estando ahí, nos aparecen 4 opciones, ingresamos a la que se llama "REGLAS DE FILTRADO PARA REDES INTERNAS".



Imagen 44. Reglas filtrado Zentyal

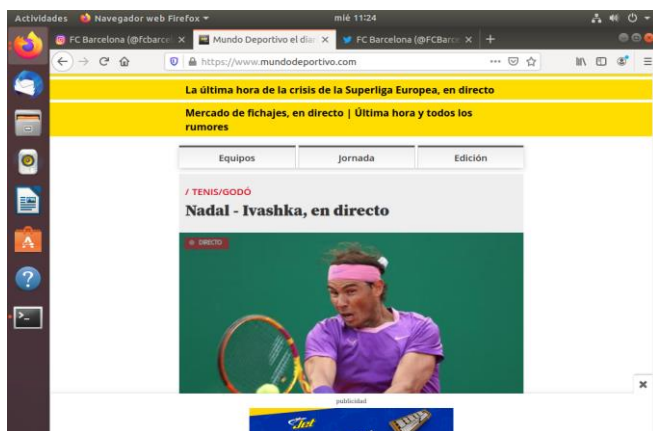


Imagen 42. Conexión Mundo Deportivo

Procedemos a agregar una nueva regla, la cual será "DENEGAR" y colocamos en "DESTINO" la ip del sitio que deseamos bloquear, como ya tenemos la IP en nuestro caso de FACEBOOK (la que obtuvimos previamente mediante el comando nslookup), ahora simplemente será configurar en el servicio "HTTP".

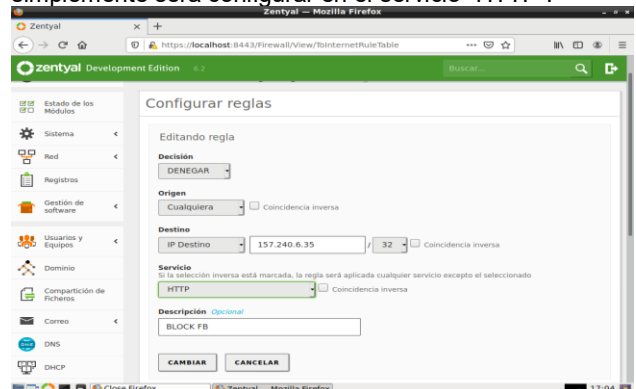


Imagen 45. regla filtrado Facebook

Una vez que hemos comprobado que cada sitio funciona de manera correcta lo que vamos a realizar será la denegación de cada servicio en el SERVIDOR ZENTYAL, pero antes de ello vamos a obtener la IP DE CADA SITIO, en este ejemplo mostrare la de Facebook, pero es igual para el resto, mediante el comando "nslookup" nos permite obtener la dirección IP para que esta sea la que vayamos a bloquear.

Hay que tener en cuenta que, todos estos sitios funcionan mediante "HTTP" y "HTTPS" es decir, este último mediante el protocolo seguro, por eso hay que repetir cada regla 2 veces para cada sitio, para que cualquiera que sea el protocolo que utilice este bloqueada dicha IP.

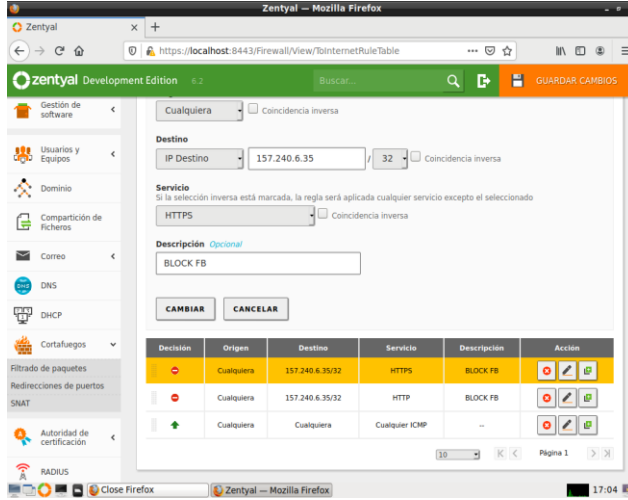


Imagen 46.regla filtrado Facebook 2

Este proceso lo vamos a repetir con cada una de las IP de los sitios que tenemos, para proceder a bloquearlo, nos quedara algo así:

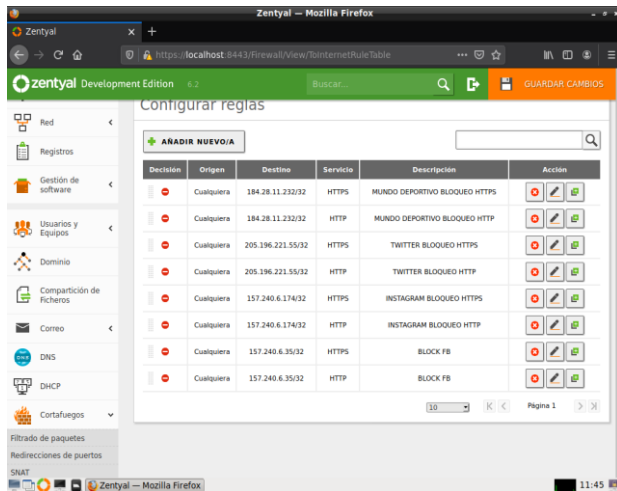


Imagen 47.regla filtrado para páginas

Una vez tenemos los sitios a bloquear, procedemos ir la maquina cliente, para probar que estos no sirven.

NOTA: En caso de tener cargada la página en nuestro navegador (cliente) debemos cerrarla y borrar el cache, porque en muchos casos por este es que se accede a la página, entonces es bueno proceder a borrarlo e iniciar de nuevo el navegador a utilizar.



Imagen 48.Borrar Datos navegación y cache

Ahora vamos a realizar el proceso, para comprobar que tenemos intente y que la pagina está siendo bloqueada, en modo ventana abriremos una página cualquiera que nos permite comprobar que hay conexión y en la otra la página que está siendo denegada por nuestro servidor.

3.3.1 PRUEBAS DE CONEXIÓN – PAGINAS BLOQUEADAS.

Abrimos nuestro navegador nuevamente y colocamos las paginas a testear, en nuestro caso usamos el navegador por defecto que trae, el mismo que hemos utilizado para todo lo realizado previamente, Firefox.

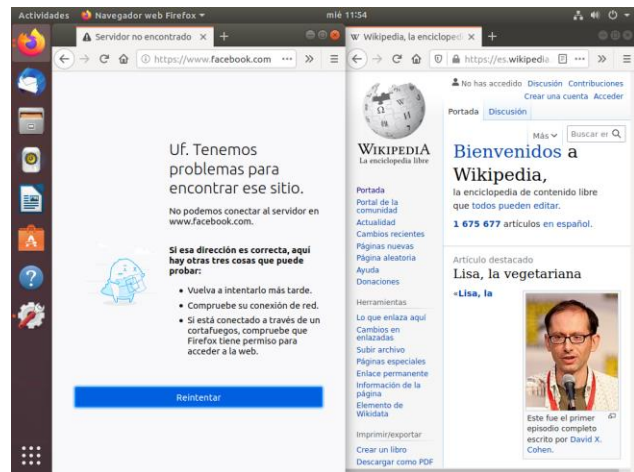


Imagen 49.Denegación Facebook

Como podemos ver, no carga la página y por el otro lado tenemos la página de Wikipedia que funciona normalmente, ahora procedemos a probar con las demás páginas, para verificar lo realizado. Continuamos con TWITTER:



Imagen 50. Denegación Twitter

Como se evidencia la página no va a cargar, es decir nuestro servidor va a denegar el servicio, por el otro lado tenemos una ventana abierta con la página de nuestra universidad donde funciona con total normalidad.

Proseguimos con la siguiente página, en este caso será INSTAGRAM:

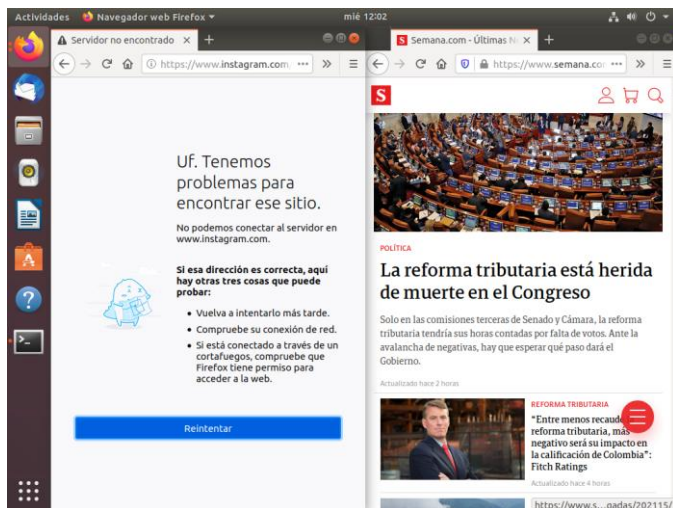


Imagen 51. Denegación Instagram

Para finalizar procedemos con la última página, que será la que contiene a la paginan deportiva, MUNDODEPORTIVO.

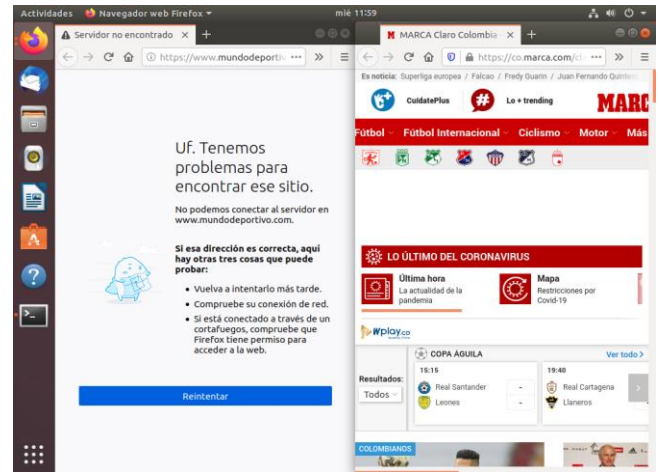


Imagen 52. Denegación Mundo Deportivo

Como podemos ver, no nos deja ingresar, para comparar tenemos otra página deportiva "MARCA" la cual funciona con total normalidad.

Y eso sería todo, ya quedaron los sitios bloqueados para evitar el acceso desde nuestro "Cliente", se pueden aplicar para diferentes páginas, teniendo en cuenta que cada una tiene su IP, otras tendrán más de una, por lo tanto, tendrá que agregarse más reglas, pero en cuanto al funcionamiento como tal, es el mismo.

3.4 Temática 4: Fie Server y Print Server

En esta temática se implementará y se realizará la configuración detallada de la creación de un File Server y Print Server el cual permitirá la compartición de directorios e impresoras en red.

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.

3.4.1 File Server

Verifico que el controlador de dominio y compartición de ficheros esté instalado

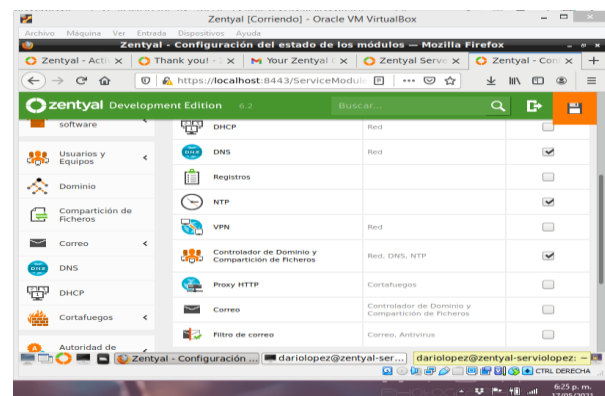


Imagen 53. Verificación del módulo

Ingreso al módulo Compartición de ficheros, para agregar un nuevo directorio compartido

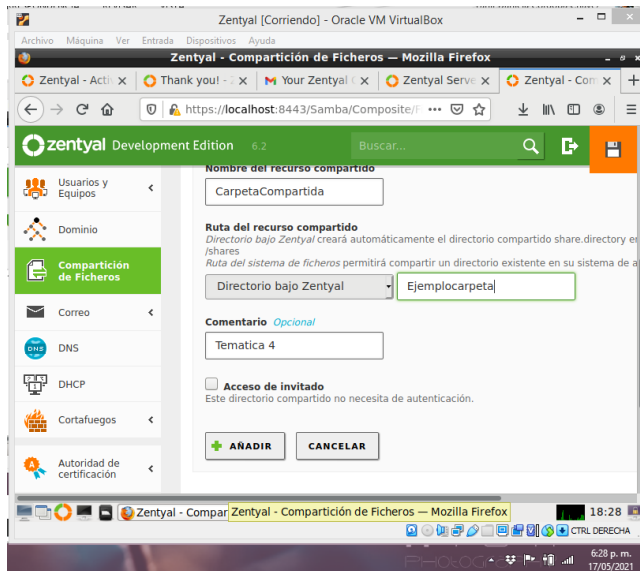


Imagen 54. Agregar fichero compartido

Creación de un usuario que tendrá acceso al dominio y permisos de lectura y escritura sobre el directorio creado.

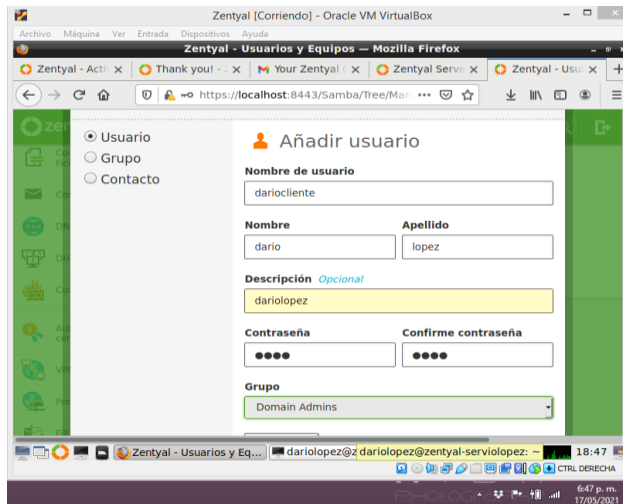


Imagen 55. Creación de usuario

Asignación de una ACL al fichero compartido, es decir, los permisos, para ello ingresamos a la configuración del directorio y damos clic en añadir.

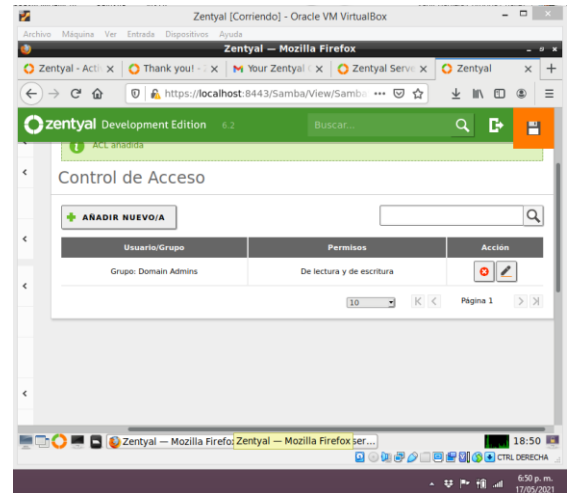


Imagen 56. Control de acceso ACL

Ahora nos dirigimos a la máquina virtual cliente, en este caso Ubuntu Desktop 20.04 para realizar la conexión, para ello instalamos samba cliente y se realiza la configuración necesaria del dominio, luego se abre el gestor de archivo, damos clic en otras ubicaciones y en la parte inferior digitamos en la casilla conexión smb://192.168.1.77 (ip del servidor) y damos clic en Conectar

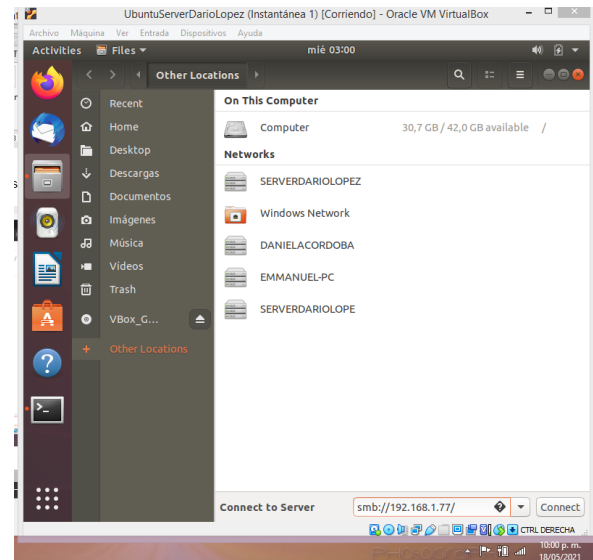


Imagen 57. Conexión al servidor

Podemos visualizar los directorios creados en el servidor

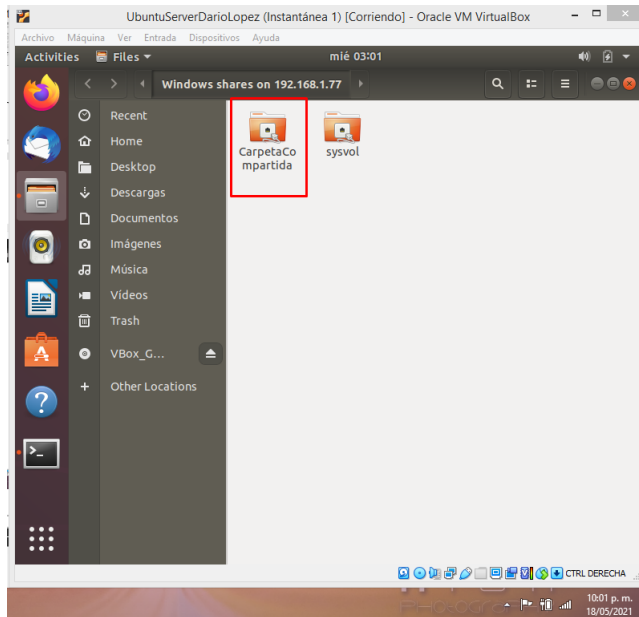


Imagen 58 Vista del directorio compartido

3.4.2 Print Server

Se realiza la instalación del paquete cups-PDF en la consola de administrador en Zentyal

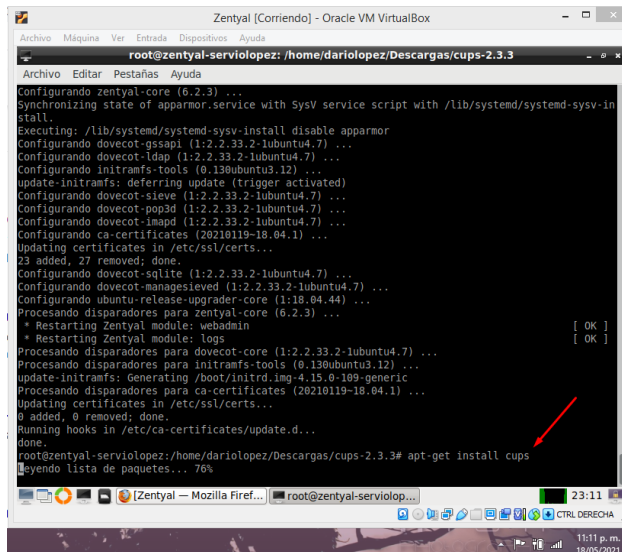


Imagen 59. Instalación de Cups-PDF

Se abre en el navegador el servidor con la dirección <https://localhost:631>, y se agrega una impresora dando clic en Administración y luego en Add Printer.

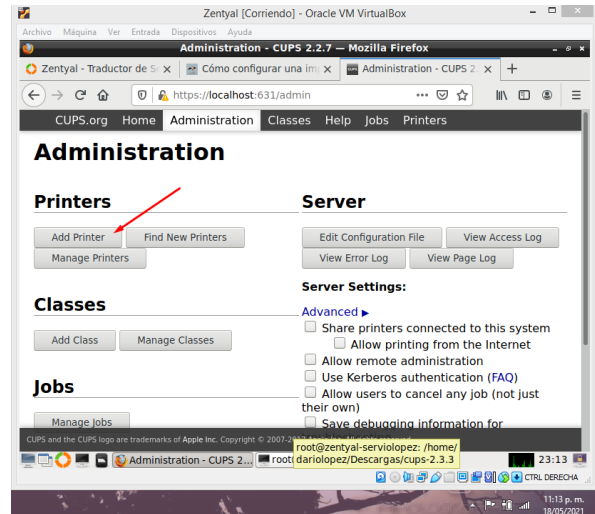


Imagen 60. Ingreso a Cups-PDF

Seguimos las instrucciones del asistente, en este caso podemos elegir la red a la cual configuramos la impresora.

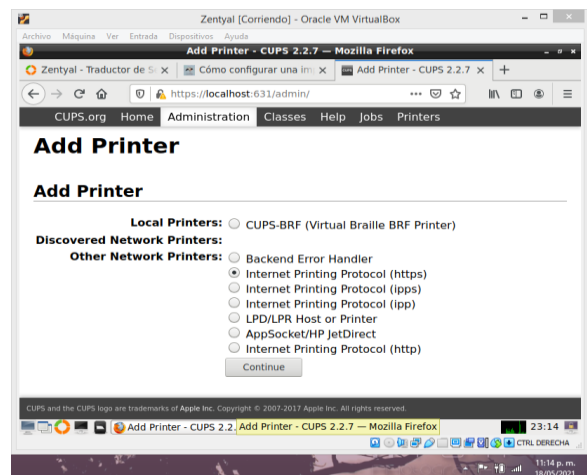


Imagen 61. Agregar impresora

Elegimos una dirección con la cual se va a realizar la conexión

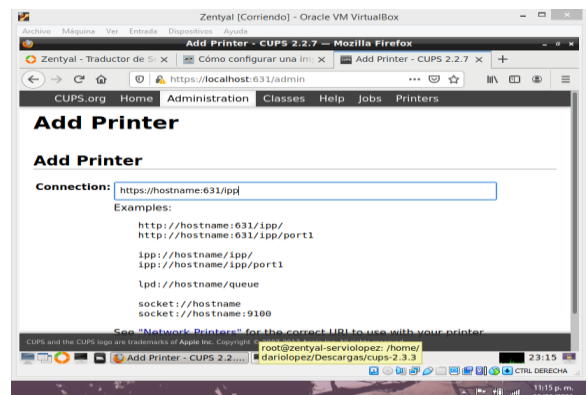


Imagen 62. Conexión

Se digita el nombre de la impresora, se selecciona Share This Printer, también elegimos modelo y marca, luego damos clic en continuar

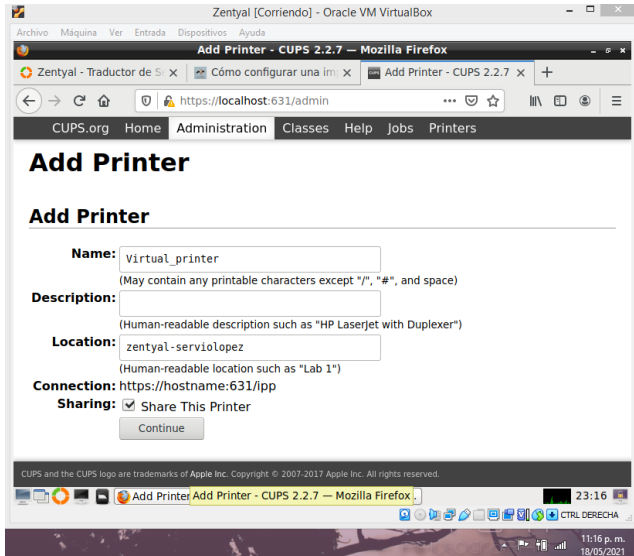


Imagen 63.Nombre de la impresora

Terminamos con el asistente y seleccionamos las dos primeras opciones en Administración para compartir la impresora.

También ingresamos al archivo smb.conf para editar los permisos de la impresora.

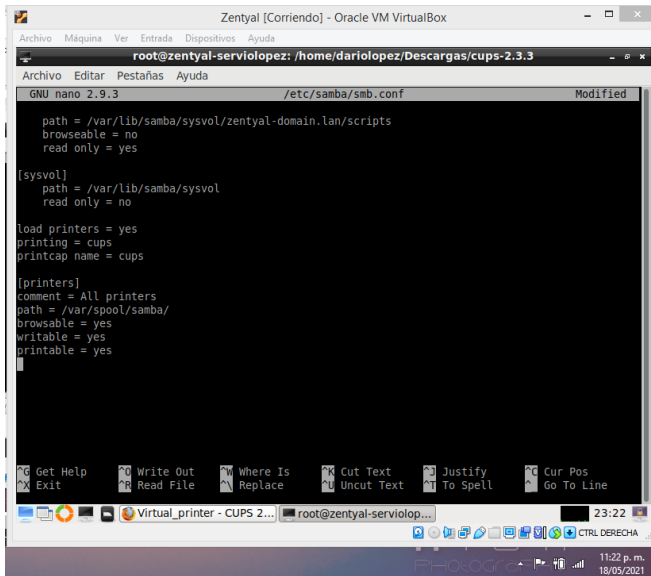


Imagen 64.Configuración de impresora con samba

Ahora ingresamos al cliente, después de la instalación de cups, realizamos la conexión de la impresora, colocando la dirección de conexión.

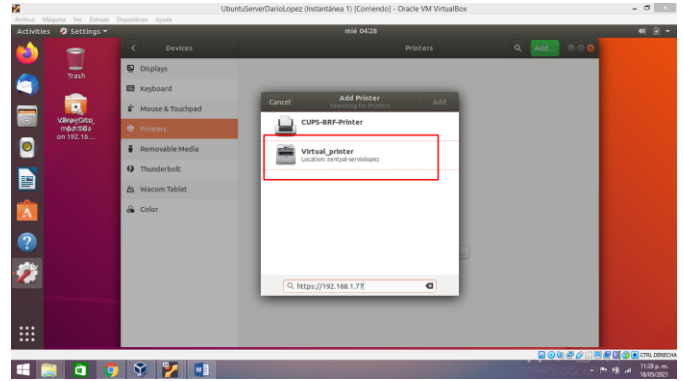


Imagen 65.Conexión a la impresora del servidor

Enviamos desde el cliente una impresión de prueba, la cual podemos verificar en Zentyal

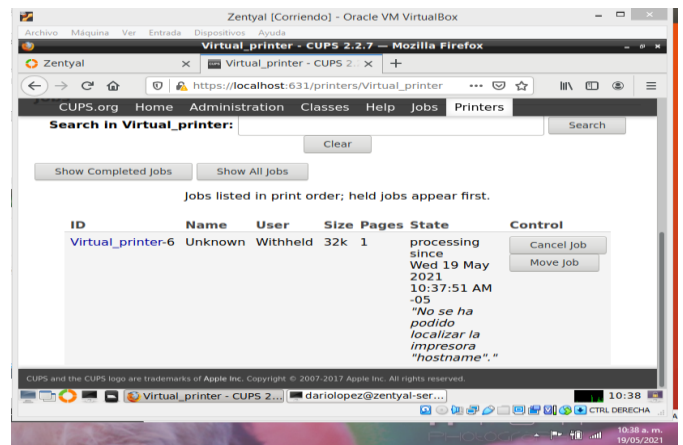


Imagen 66.Impresión de prueba.

3.5 Temática 5: VPN

Una vez dentro podremos instalar y/o configurar los servicios que necesitemos de Zentyal.

Ahora en el panel seleccionamos la herramienta que usaremos y daremos clic en instalar.

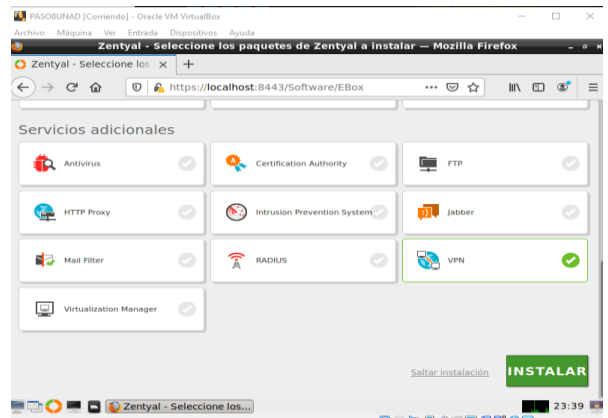


Imagen 67.Instalar servicios

Nos muestra la lista de paquetes a instalar y damos clic en continuar.

Una vez instalados todos los paquetes, nos mostrara una pantalla en la que seleccionaremos el tipo de interfaz de red. En nuestro caso sera internal y damos clic en siguiente.

Para interfaces externas por defecto dejamos DHCP y damos clic en finalizar.

En el dashboard, nos vamos para el menu lateral izquierdo, buscamos la opción VPN y seleccionamos la subopción servidores.

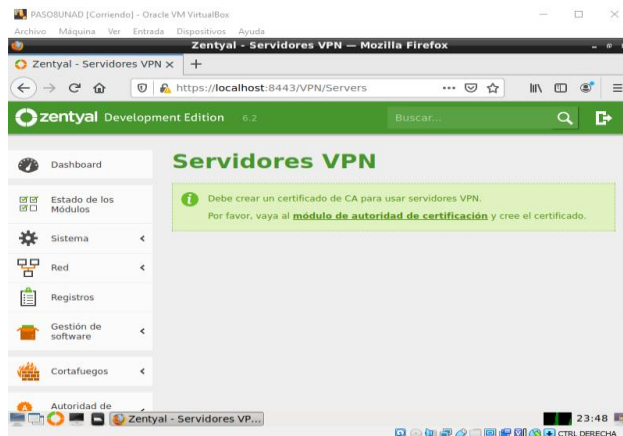


Imagen 68. Lista de servidores vpn

Hacemos clic sobre el link “módulo de autoridad de certificación” y en la ventana escribimos el nombre de la organización y los días de expiración y damos clic en crear.

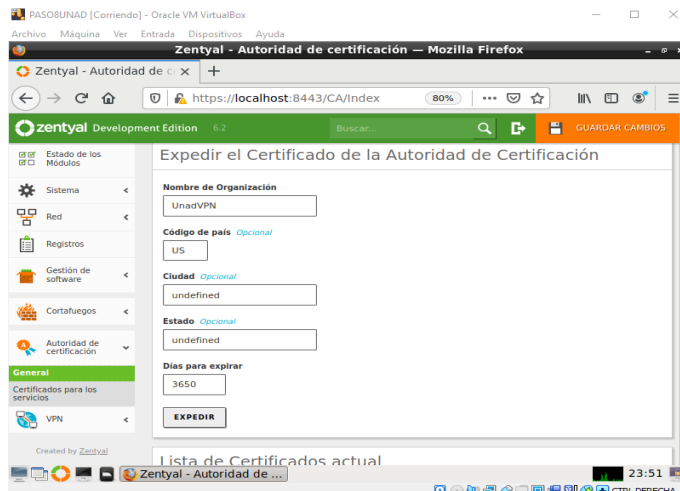


Imagen 69. certificados de autoridad

En la siguiente ventana creamos un nuevo certificado de autoridad y damos clic en expedir.

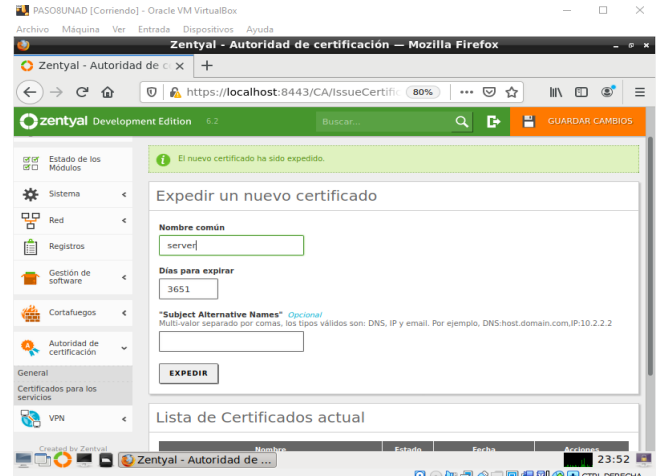


Imagen 70. expedir certificados

El paso siguiente es guardar los cambios realizados

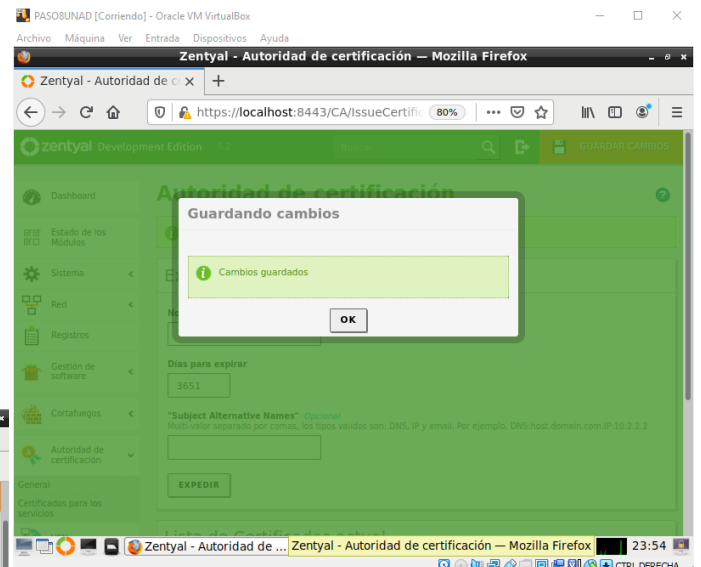


Imagen 71. guardar cambios

Volvemos a dar clic en VPN/Servidores.

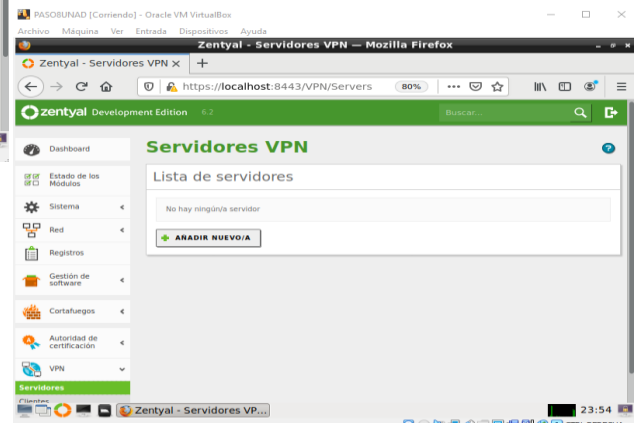


Imagen 72. añadir servidor VPN

Añadimos nuevo y ponemos el nombre de nuestro servidor.

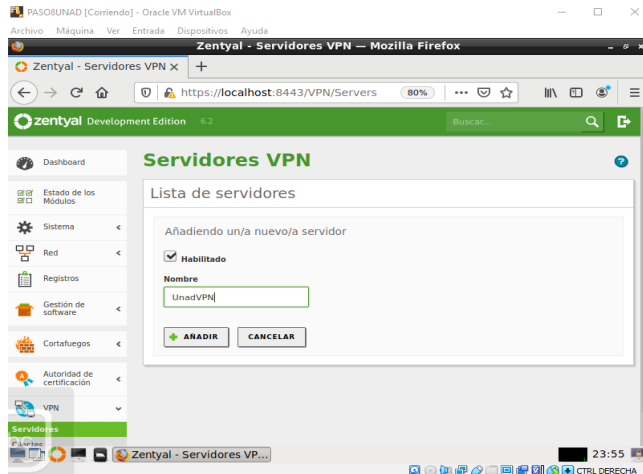


Imagen 73. Creando servidor VPN

Ahora modificaremos la configuración de nuestro servidor de la siguiente manera.



Imagen 74. Configurando VPN

Guardamos los cambios y nos dirigimos a Autoridad de certificación / General y procedemos a crear un certificado para el cliente ubuntu.

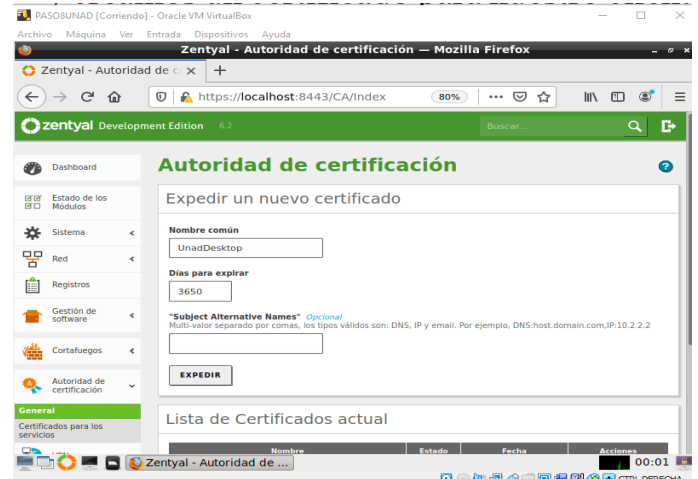


Imagen 76. expedir autoridad certificado

Una vez echo eso, vamos a VPN/Servidores y daremos clic en habilitado y en el piñon de descarga paquete de configuración cliente.



Imagen 77. Lista de servidores VPN

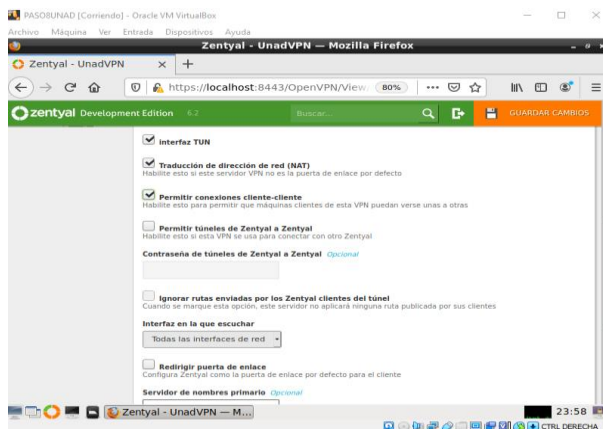


Imagen 75. Configurando VPN

Configuramos el cliente.



Imagen 78. Descargar paquete de cliente

Y procedemos a darle click en descargar y guardamos nuestro certificado

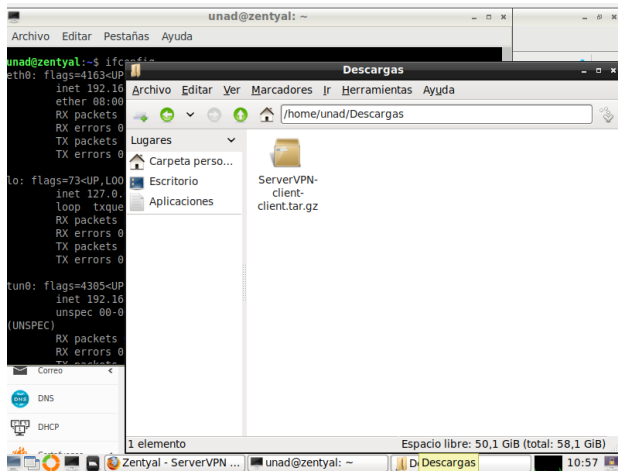


Imagen 79. Paquete de cliente comprimido

Con el certificado iremos a nuestro Ubuntu e importaremos el archivo generado.

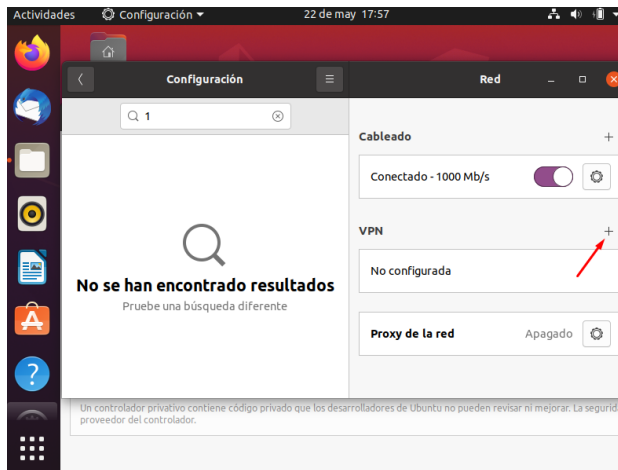


Imagen 80. Agregando VPN

Damos clic en importar desde un archivo el archivo client.conf del tar descomprimido.

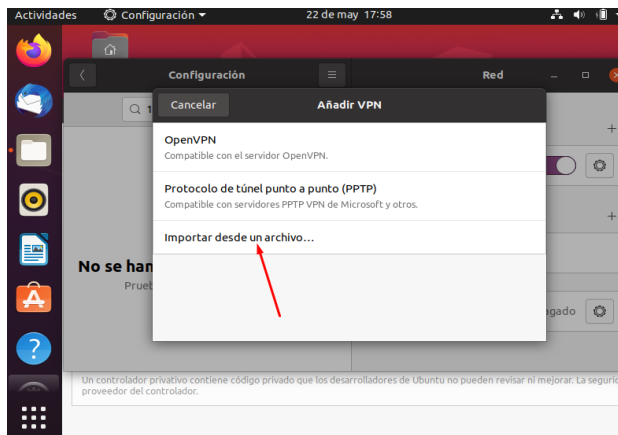


Imagen 81. Importando credenciales

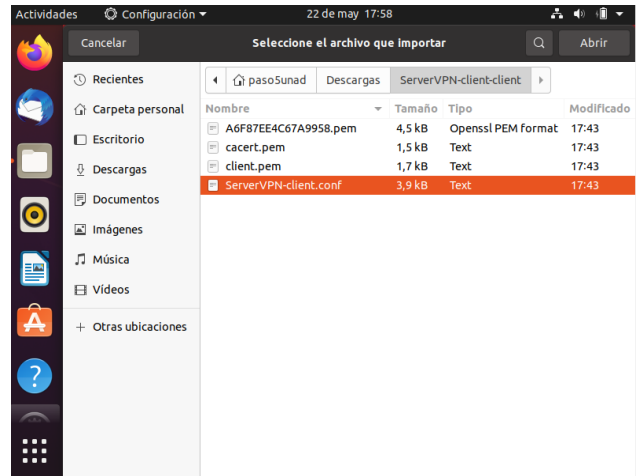


Imagen 82. Seleccionando archivo conf

Luego de eso nos debería quedar una ventana con la siguiente información, validamos y damos clic en añadir.

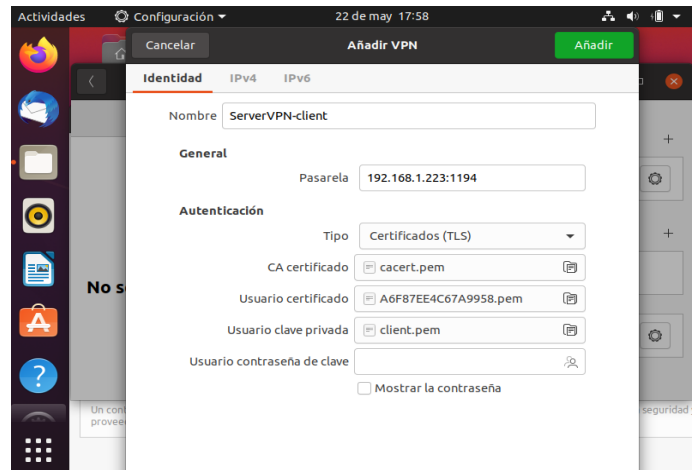


Imagen 83. Cargando contenido de conf

Ahora para probar que funciona correctamente hacemos ping primero sin conectarnos a la vpn, a ip interna de Zentyal que en este caso es 192.168.160.1 lo correcto sería no tener respuesta.

Demonios OpenVPN	
▼ Servidor ServerVPN	
Servicio	Habilitado
Estado del demonio	Ejecutándose
Dirección local	Todas las interfaces de red
Puerto	1194/UDP
Subred VPN	192.168.160.0/255.255.255.0
Interfaz de red de la VPN	tun0
Dirección de la interfaz de la VPN	192.168.160.1/32

Imagen 84. Información del demonio

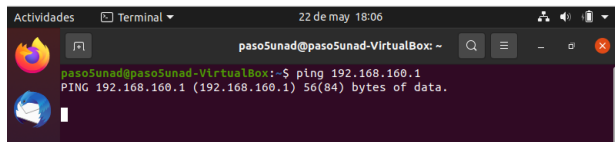


Imagen 85. Ping a servidor VPN fallido

Como podemos observar no recibimos respuesta ahora, vamos a conectar la vpn y volvemos hacer ping.

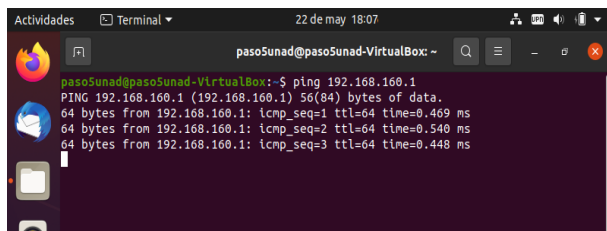


Imagen 86. Ping a servidor VPN exitoso

Con esto comprobamos la correcta configuración y conexión de nuestra VPN en Zentyal.

4 CONCLUSIONES

Los VPN permiten la conexión de forma segura y privada dentro de una red, la importancia del uso de las VPN para evitar que las redes sean anónimas, pero sobre todo seguras.

Las vpns permite navegar libremente cuando se usan ya que muchas veces existe contenido que es censurado, el poder de las VPN es inmenso, las vpns saltan esos bloqueos en una red, sea privada o pública, es la mejor opción para tomar en cuenta a la hora de navegar en internet.

File Server y Print Server, son una gran herramienta al momento de realizar las labores diarias en oficina, ya que permite una correcta compartición de archivos e impresoras.

Se logró la instalación y configuración de los módulos necesarios de ZENTYAL 6.2, garantizando las distribuciones características de DNS, DHCP, entre otros identificando como una opción muy viable para las creaciones de servicios de solución TI.

Además de identificar en el transcurso del proceso formativo, la gran adaptabilidad y los mejoramientos continuos en ese sistema operativo que se puede dar como buena opción a nivel empresarial para la adecuada administración de recursos, y con ello garantizando seguridad, buen manejo y factibilidades en los entornos.

5 REFERENCIAS

[1] G.B., S. (2020, 19 mayo). Instalar Samba en Ubuntu 20.04 LTS Focal y derivados. Linux para todos.

<https://www.sololinux.es/instalar-samba-en-ubuntu-20-04-focal-y-derivados/>

[2] Roberto Murillo. (2020, 20 mayo). Zentyal 6.2: Instalación y Configuración - Parte #1 [Video]. YouTube. <https://www.youtube.com/watch?v=gJYJjM2vxbc>

[3] Roberto Murillo. (2020b, mayo 24). Zentyal 6.2: Instalación y Configuración - Parte #2 [Video]. YouTube. https://www.youtube.com/watch?v=l-2fw_5BZhs

[4] Roberto Murillo. (2020b, mayo 24). Zentyal 6.2: Instalación y Configuración - Parte #3 [Video]. YouTube. <https://www.youtube.com/watch?v=dKYnY8pZEQ>

[5] Roberto Murillo. (2020b, mayo 24). Zentyal 6.2: Instalación y Configuración - Parte #4 [Video]. YouTube. <https://www.youtube.com/watch?v=VvYtrP49LCw&t=100s>

[6] Roberto Murillo. (2020b, mayo 24). Zentyal 6.2: Instalación y Configuración - Parte #5 [Video]. YouTube. <https://www.youtube.com/watch?v=5oU0C3BwSak>

[7] ZORRASBINARIAS. (2019, 13 febrero). Integrando Ubuntu Desktop 18.04 en dominio Active Directory – Elbinario. <https://elbinario.net/>. <https://elbinario.net/2019/02/13/integrando-ubuntu-desktop-18-04-en-dominio-active-directory/>

[8] Wallen, J. (2020, 8 abril). How to configure a print server with Ubuntu Server, CUPS, and Bonjour. TechRepublic. <https://www.techrepublic.com/article/how-to-configure-a-print-server-with-ubuntu-server-cups-and-bonjour/>

[9] Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 92 – 137). Madrid, ES: IC Editorial. Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51181?page=92>

[10] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 6 – 84). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56046?page=6>