

Guía de Instalación y Configuración de Servicios en Linux Zentyal, grupo 201494_6

Carlos Alberto Benavides Abril
e-mail: cabenavidesab@unadvirtual.edu.co
Danny Leandro Buriticá Molano
lgmoyanor@unadvirtual.edu.co
Mónica Viviana Barrera Ruiz
e-mail: mvbarrerar@unadvirtual.edu.co
Paola Amado Angulo
e-mail: pamadoa@unadvirtual.edu.co
Luis Gonzalo Moyano
e-mail: lgmoyanor@unadvirtual.edu.co

RESUMEN: El presente documento muestra la instalación y puesta en marcha del servidor Zentyal en su versión 6.2 para dar solución a diferentes problemas de migración e infraestructura en las tecnologías de la información, esto enfocado en situaciones más complejas a niveles internos o externos de la red. Sobre el servidor Zentyal, se implementarán servicios como DNS, DHCP, controlador de dominio, Firewall, Proxy Transparente y VPN como solución a un entorno de networking.

PALABRAS CLAVE: Controlador Dominio, Dns, Dhcp, Zentyal

1 INTRODUCCIÓN

Este artículo presenta la configuración e instalación del Sistema Operativo GNU/Linux Zentyal Server 6.2, haciendo uso de las técnicas aprendidas en el transcurso del Diplomado de Profundización en Linux; sistema operativo base para disponer de los servicios de infraestructura IT, contenidos de la temática nro. 1, seleccionada en el entorno colaborativo, en donde se deberá configurar e implementar los servicios de gestión en DHCP Server, DNS Server y Controlador de Dominio dentro de nuestro sistema; realizando la entrega de la implementación de manera detallada del acceso de una estación de trabajo Linux Ubuntu Desktop, así como la validación de dicha estación en las configuraciones de los servicios de infraestructura IT en Zentyal.

Instalación y Configuración del Servicio DHCP

Vamos a la sección componentes de Zentyal y desde allí podemos seleccionar el módulo que vamos o necesitamos instalar para este primer ejercicio necesitamos el módulo DHCP Server.

Para ello debemos hacer la configuración de las interfaces de red como son las eth0 y la eth1 donde la

eth0 será la externa y la eth1 será la red interna del Zentyal.



Figura 1. Debemos ingresar a la configuración en el icono que nos presenta configuración y nos aparecerá la siguiente imagen, donde vamos a realizar la configuración del rango de ip para el dhcp



Figura 2. Una vez tenemos la configuración debemos realizar la creación de un rango de ip para nuestro ejercicio, vamos a crear un rango desde la ip 192.168.10.10 hasta la ip 192.168.10.20 y llamaremos a este rango Rangoseminario.



Figura 3. Ahora debemos validar la configuración en la maquina desktop para certificar que se realizó la configuración y se obtiene una dirección por DHCP en el servidor Linux Ubuntu.

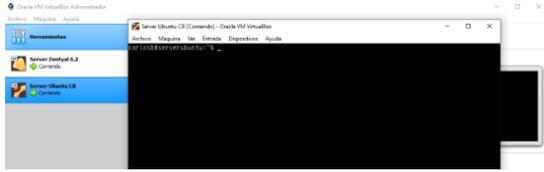


Figura 4. Debemos validar con el comando ifconfig -a si este servidor tomo una de las direcciones ip que se crearon al momento de la creación del rango de ips.

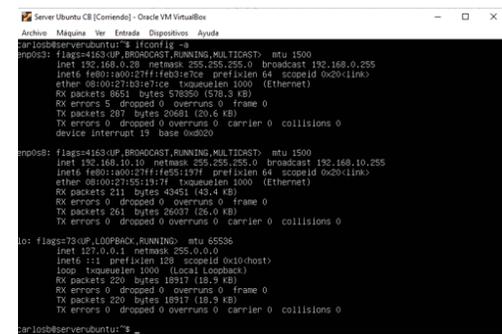


Figura 5. Podemos observar cómo se obtiene la dirección ip que es la 192.168.10.10, que es la primera dirección del rango de ip.

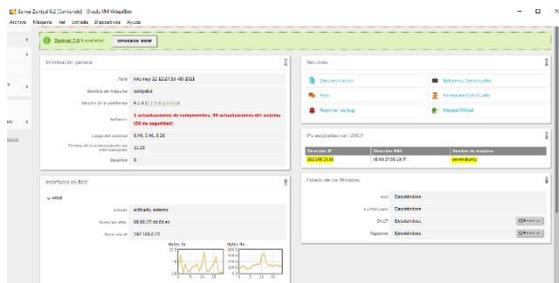


Figura 6. Como podemos observar desde el servidor Zentyal se puede observar las ips asignadas por el dhcp y mostrara la Ip asignada como la Mac y el nombre del servidor que tiene asignada la ip en ese momento.

Instalación y Configuración del Servicio DNS



Figura 7. Para realizar el cambio a los DNS, se deben cambiar desde la configuración desde el DHCP, pues como se tiene configurado por DHCP estos tienen los DNS de Google que son 8.8.8.8 y debemos cambiarlo a la opción de que se llama DNS local de

Zentyal. Al realizar el cambio este deberá tomar los Dns de Zentyal.

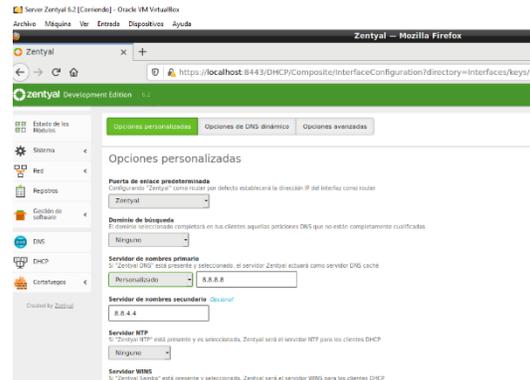


Figura 8. Después de realizar el cambio en la opción (DNS local de Zentyal) deberá quedar de la siguiente manera.

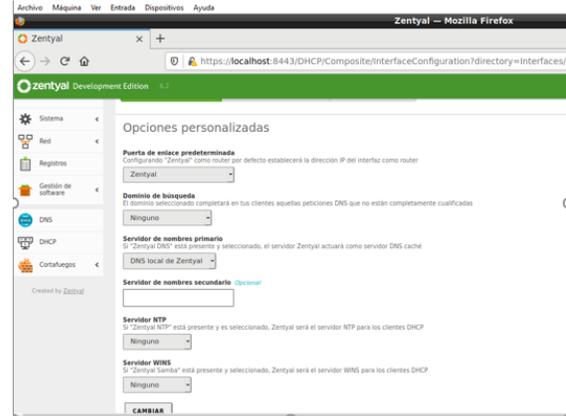


Figura 9. En la opción Servidor de Nombres Primario se debe seleccionar la opción llamada DNS de Zentyal, donde podemos observar que se deja en blanco como también la opción llamada Servidor de nombres secundario, damos en aplicar y guardamos los cambios.

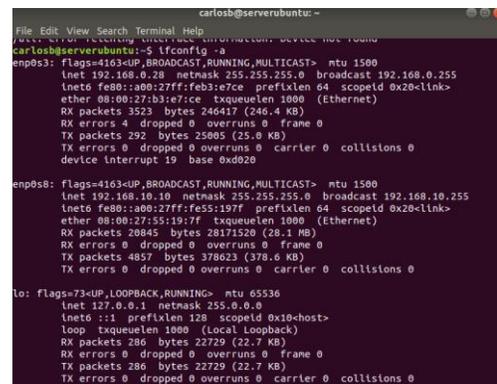


Figura 10. Podemos observar que se validan las configuraciones de red y de las interfaces. Podemos ver que se tiene la dirección entregada por el dhcp ahora debemos renovar la ip, para que este haga la actualización del servidor Dns y validar la conexión.

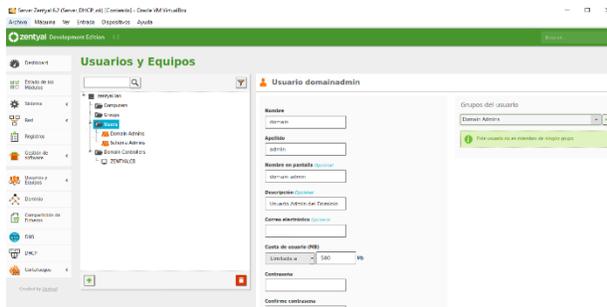


Figura 17 Una vez creado el usuario domainadmin, debemos asignarlo al grupo llamado Domain Admins. podemos ir a una maquina y hacer el ingreso al dominio, previamente configurado.

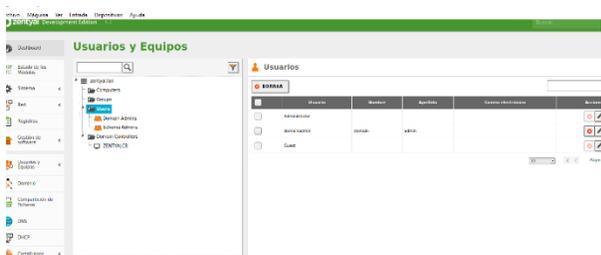


Figura 18 Podemos observar que se encuentra creado el usuario y asignado a los administradores del dominio para poder realizar el ingreso de la maquina al dominio.

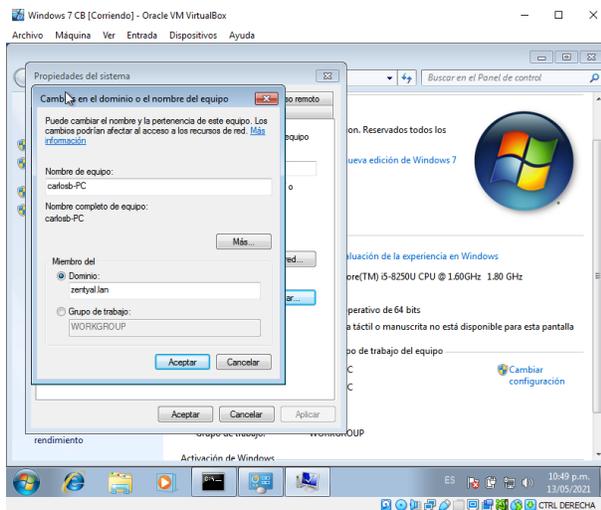


Figura 19 Podemos observar cómo vamos a la maquina cliente para este caso vamos a una maquina Windows y vamos a las opciones de la máquina para ingresarla al dominio creado en el Zentyal.

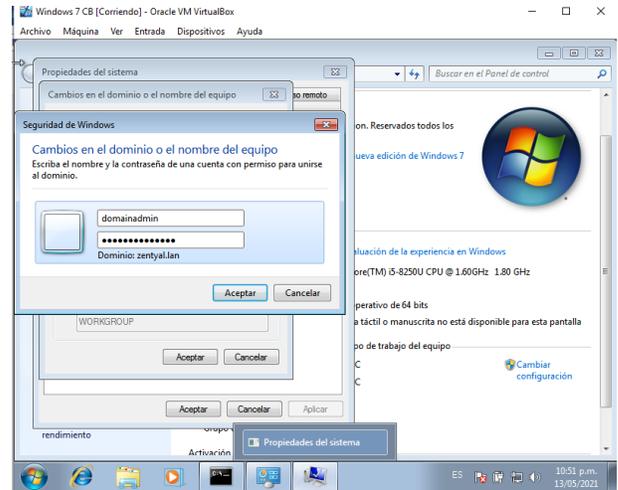
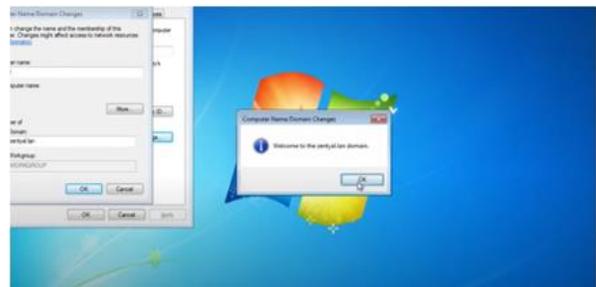


Figura 20 Acá debemos poner las credenciales creadas en el servidor Zentyal para el ingreso de la maquina al dominio llamado Zentyal.ian se solicitan las credenciales de usuario y contraseña para este ingreso.



2 TEMÁTICA: 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.

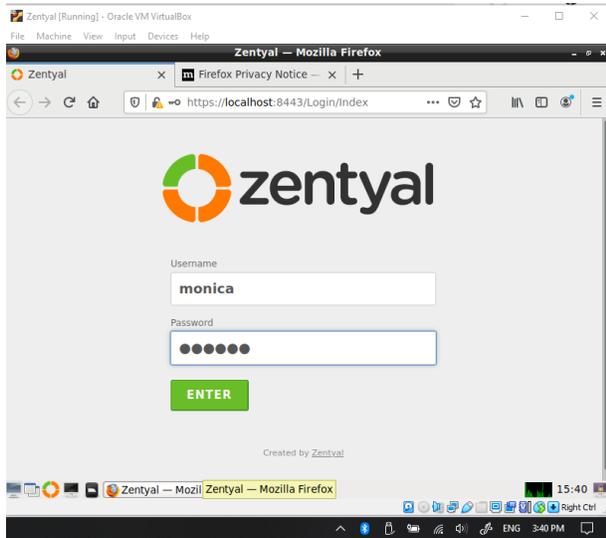


Figura 22 Se ingresa credenciales para configuración.

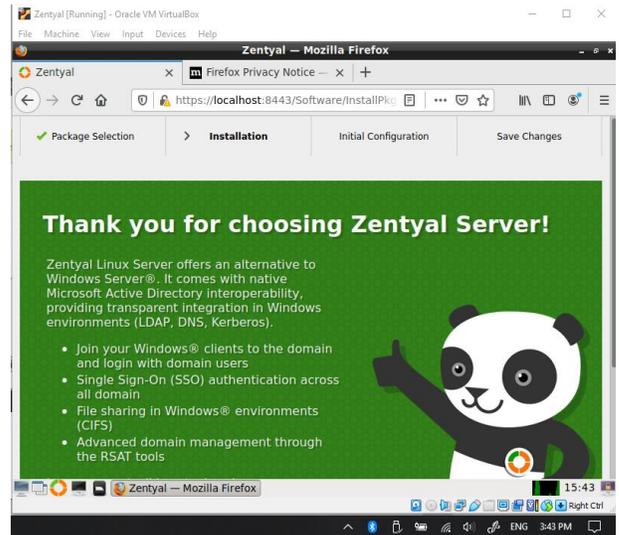


Figura 25 Instalación completada.

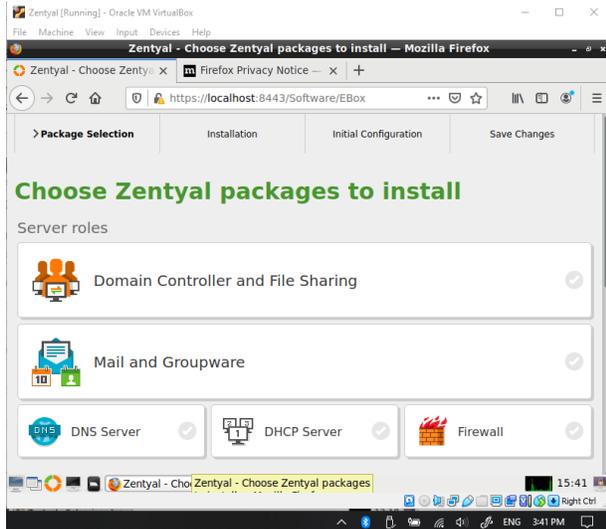


Figura 23 Se muestra la lista de opciones configurables.

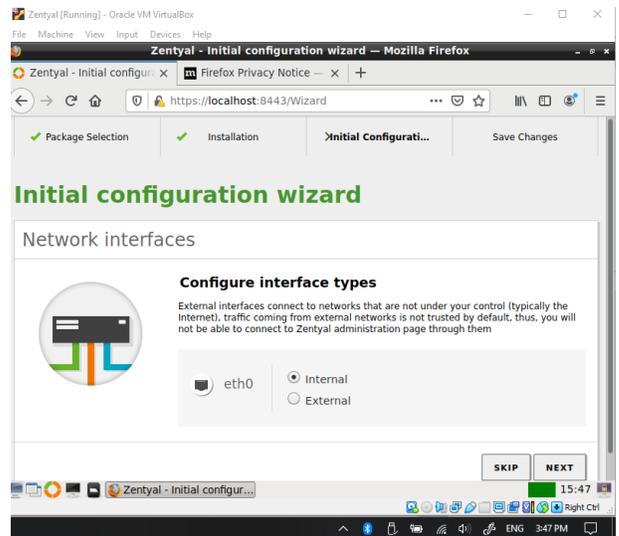


Figura 26 Configuración de Red.

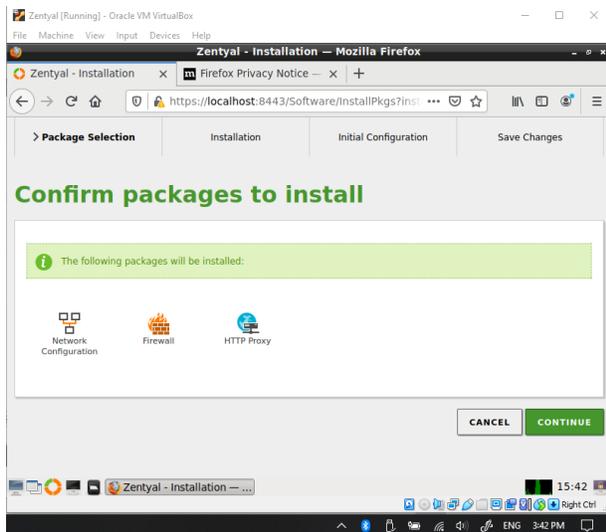


Figura 24 Se muestra los paquetes instalados.

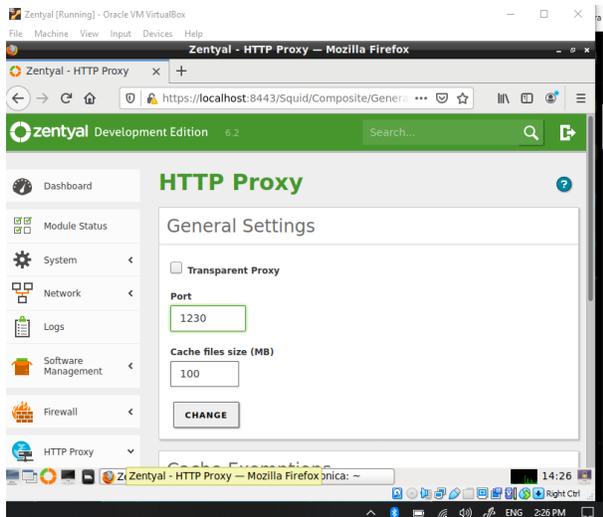


Figura 27 Se da inicio a configuración puerto solicitado para configurar proxy NO transparente.

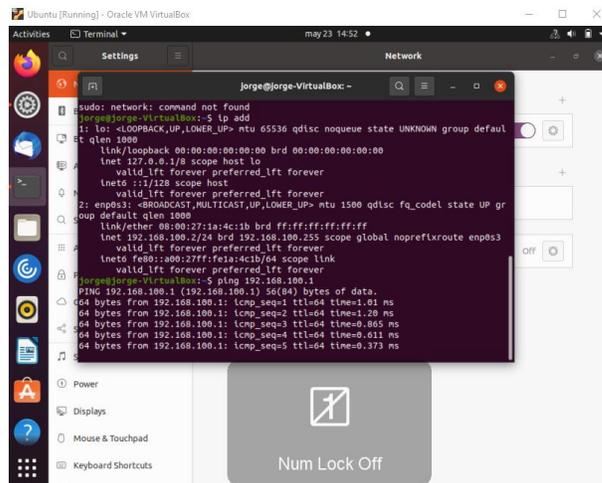


Figura 30

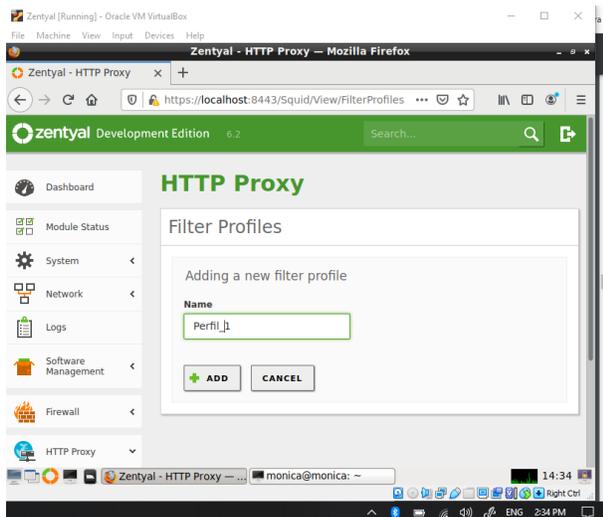


Figura 28 Se crea perfil a configurar las diferentes opciones de proxy.

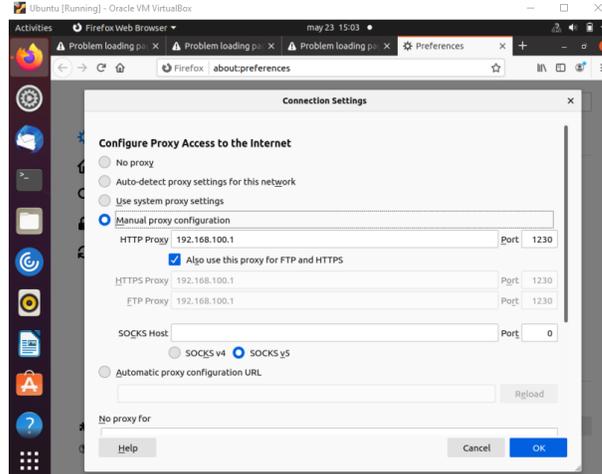


Figura 31

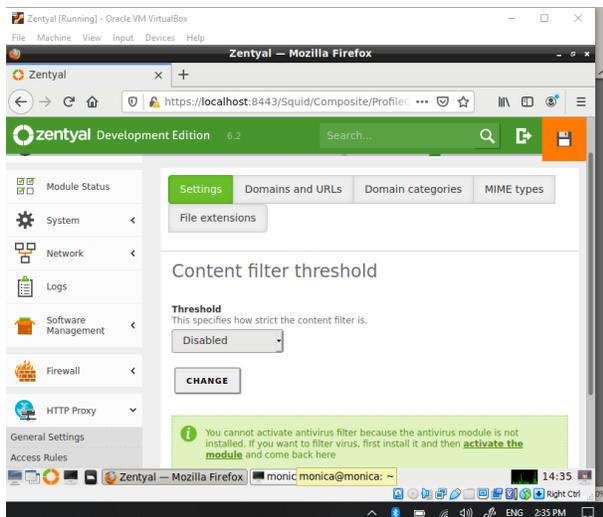


Figura 29 Opción elegida para filtro.

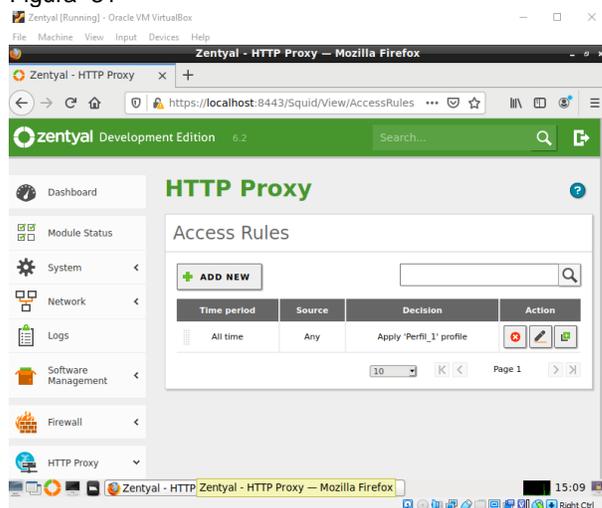


Figura 32 Reglas de perfil a configurar.

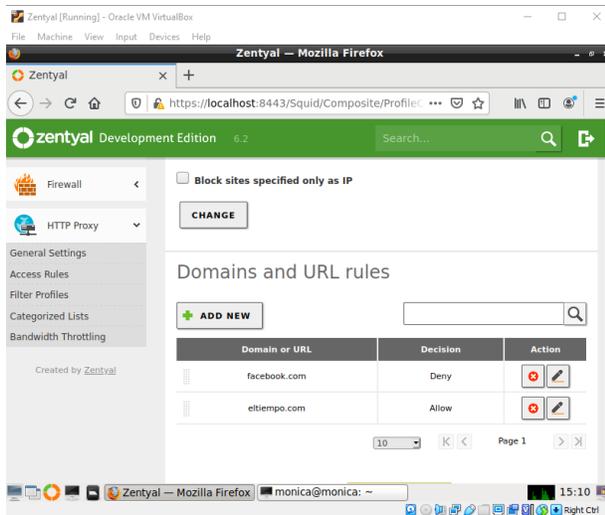


Figura 33 listado de páginas con reglas explícitas.

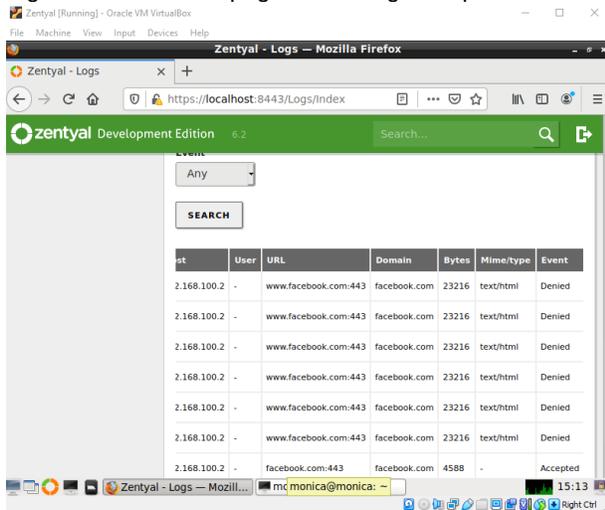


Figura 34 log de evento.

3 TEMATICA: 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.

Comenzamos en la página principal de Zentyal en donde seleccionaremos el paquete de firewall a instalar. En este punto ya debemos tener el servicio DHCP instalado, configurado y el módulo activo. Por defecto al instalar el módulo DHCP Zentyal instala las herramientas de red y el cortafuegos "firewall".

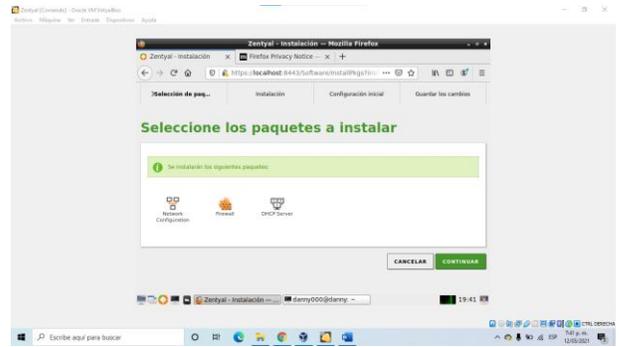


Figura 35. Instalación del paquete DHCP y FIREWALL

Una vez dado clic en instalar los paquetes se instalarán y se mostrará la información de estos en el dashboard de Zentyal; sin embargo, por defecto no están activos, es necesario hacer la configuración previamente. La activación del módulo se hará al finalizar su configuración.

Una vez instalado los servicios nos dirigimos al bloque de cortafuegos "firewall" al dar clic nos dará una pequeña lista de opciones en donde daremos clic en filtrado de paquetes.

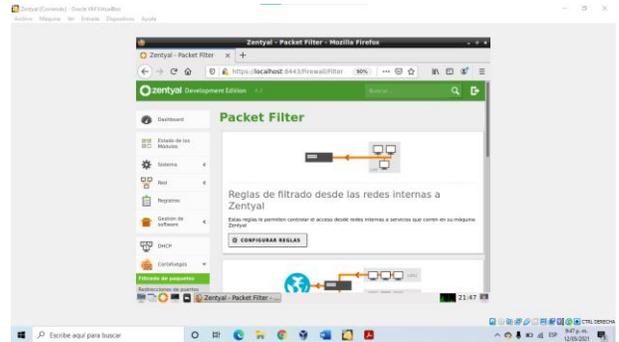


Figura 36. Bloque de cortafuegos "firewall"

Una vez dentro, buscamos el sub-bloque de **reglas de filtrado** para las redes internas y damos clic en configurar reglas.



Figura 37. Sub-bloque de cortafuegos reglas de filtrado

Al ingresar podremos añadir las reglas para el filtrado de la red, para ello damos clic en "Añadir nuevo/a".

Zentyal nos permite crear reglas para redes internas y/o externas, denegar, rechazar, admitir, entre otras.

Para este caso rechazaremos la red social de Facebook. Haremos un ping a **facebook.com** para conocer su dirección IP; tal como se muestra a continuación.

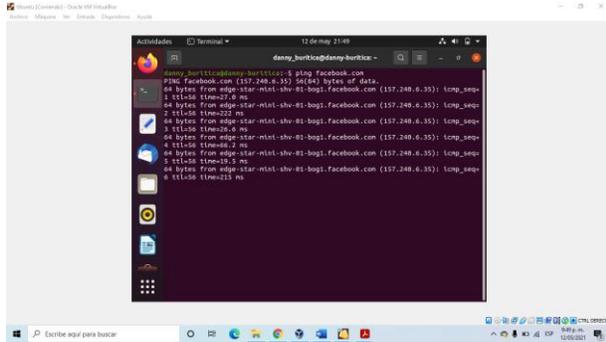


Figura 38. Ping con conocer la dirección IP de Facebook.

Para cumplir la rúbrica procedemos a evidenciar que el acceso a redes sociales y a portales web de entretenimiento es posible.

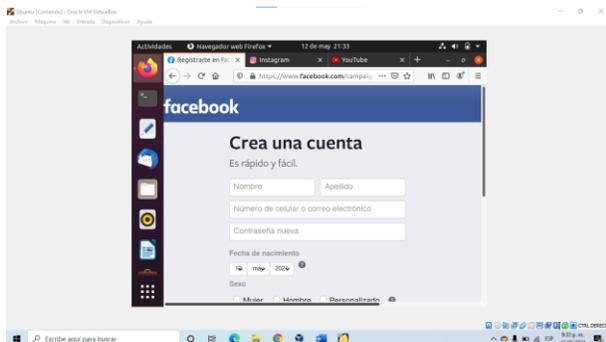


Figura 39. Verificación de acceso a redes sociales

Para denegar el acceso a redes sociales y portales web de entretenimiento daremos clic en denegar cualquier origen y en el destino seleccionaremos la "IP de destino" en donde pondremos la IP de la página web a declinar. Es necesario seleccionar el servicio o protocolo a rechazar y por último, podremos añadir una descripción a la regla. Una vez configurada la regla damos clic "añadir"

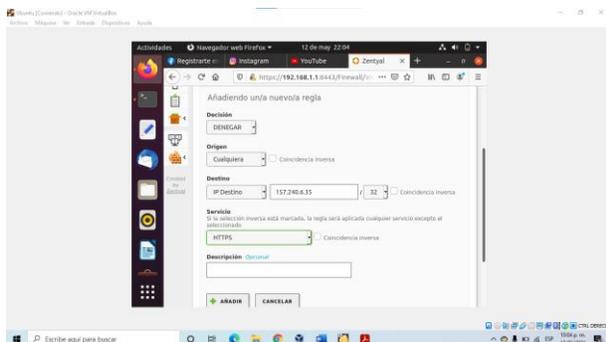


Figura 40. Denegar tráfico del protocolo HTTPS de la dirección IP

Para bloquear la red social Facebook procedemos a bloquear los protocolos de HTTPS, HTTP, y el TCP. Para ello basta con duplicar la regla y cambiar el protocolo a denegar; tal como se muestra a continuación:

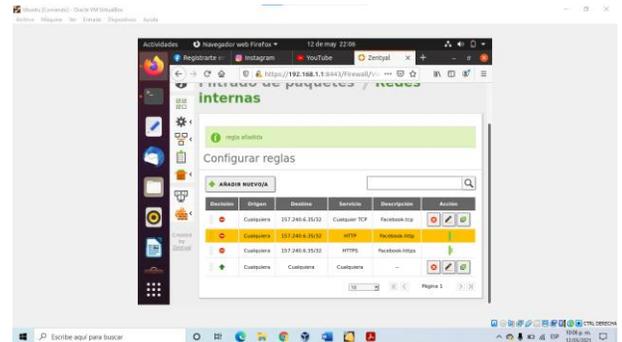


Figura 41. Listado de reglas de firewall creadas

Una vez creadas las reglas procedemos a guardar los cambios de estas, nos mostrará en pantalla si deseamos guardar los cambios. Es necesario verificar que el módulo del firewall este activo, para que de esta manera empiecen a aplicar en nuestra red interna

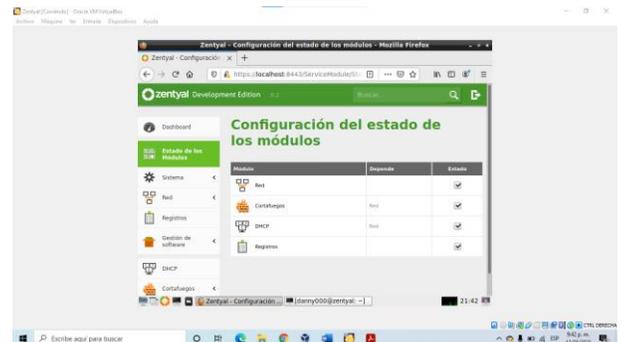


Figura 42. Activación de módulos

Para la comprobación del funcionamiento de nuestro cortafuegos es necesario borrar el cache de nuestro navegador web si ya hemos ingresado a la página web con antelación. Una vez activa nuestras reglas del cortafuegos intentamos acceder a **https://www.facebook.com** y se evidencia que no es posible acceder gracias a la regla que anteriormente configuramos. (También se evidencia en el navegador el mensaje de que la dirección web ha tardado demasiado en responder).

la conexión con YouTube bloqueamos el protocolo HTTPS.

Es necesario borrar cache del navegador para evidenciar el funcionamiento de las reglas del cortafuegos si ya hemos accedido a la página web anteriormente. Intentamos acceder a <https://www.youtube.com> y se evidencia que no es posible acceder gracias a la regla que anteriormente configuramos. (También se evidencia en el navegador que el mensaje de que la dirección web ha tardado demasiado en responder) Con estas evidencias concluimos la temática de cortafuegos.

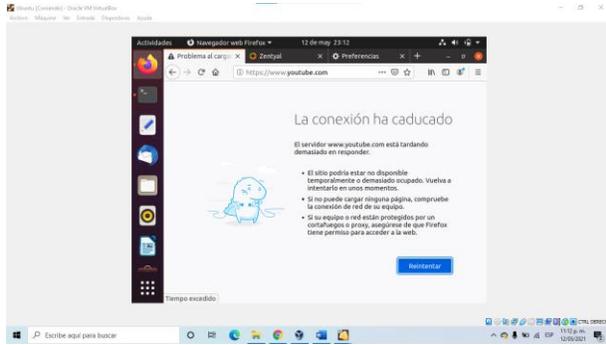


Figura 49. Verificación de la regla denegar por URL (Youtube).

4 TEMÁTICA FILE SERVER Y PRINT SERVER

Accedemos desde la plataforma de Zentyal y procederemos a Instalar el Control de Dominio y archivos compartidos.

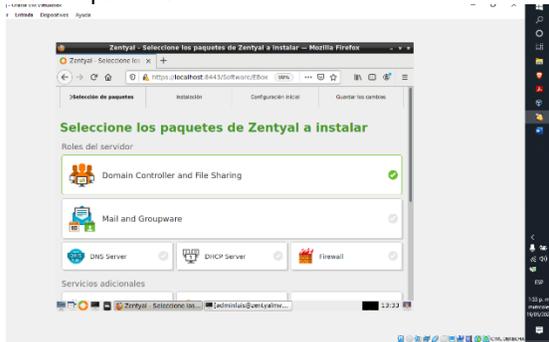


Figura 50.

Damos clic sobre instalar. Luego de ello nos muestra los diferentes programas que serán Instalados para el funcionamiento del servicio de File Server.

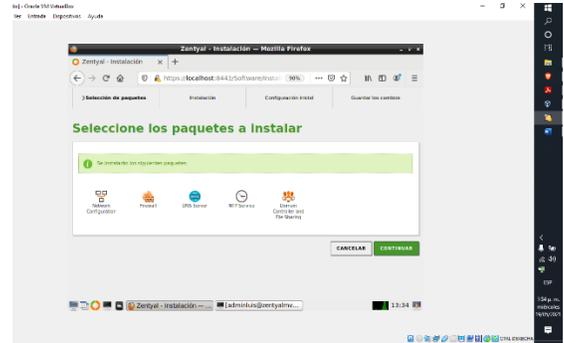


Figura 51.

1. damos en continuar y esperamos que se Instale de manera correcta los demás componentes.

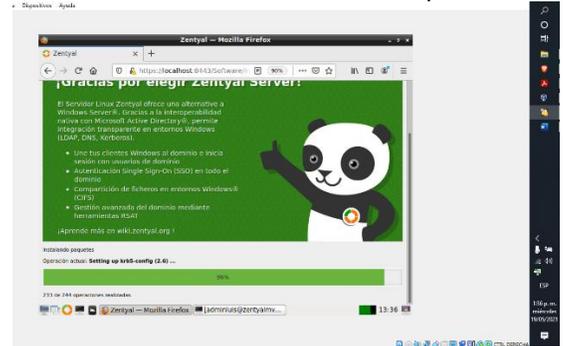


Figura 52.

Procedemos a configurar el Dominio, para este ejemplo dejaremos el dominio del servidor como viene por defecto.

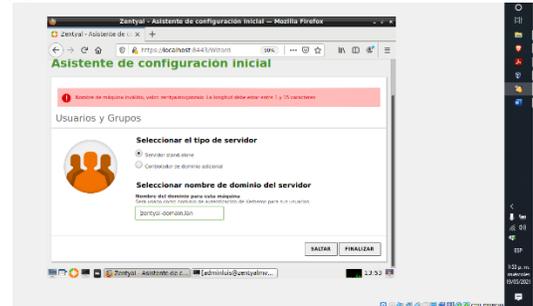


Figura 53.

Donde será necesario guardar los cambios para que surja efecto.

Luego de que se realice la Instalación del control de Dominio y archivos compartidos. se procede a configurar de la siguiente manera habilitamos el PAN

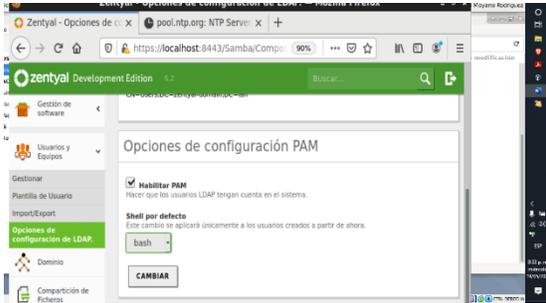


Figura 54

Procedemos a gestionar el servicio con respecto a usuarios Grupos y carpetas a compartir, antes de empezar se debe tener el servicio de DNS y de RED configurado para el buen funcionamiento de este servicio. por lo cual se puede guiar con las diferentes actividades realizadas con los compañeros.

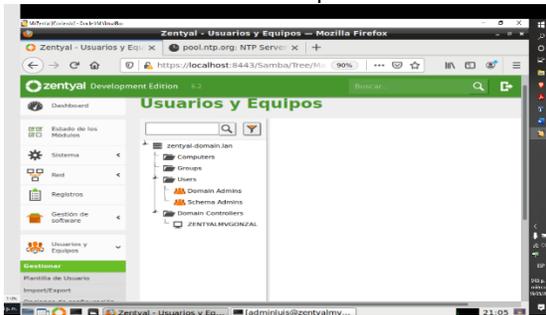


Figura 55

Procedemos a generar una Unidad Organizativa, en este caso la llamare UNAD

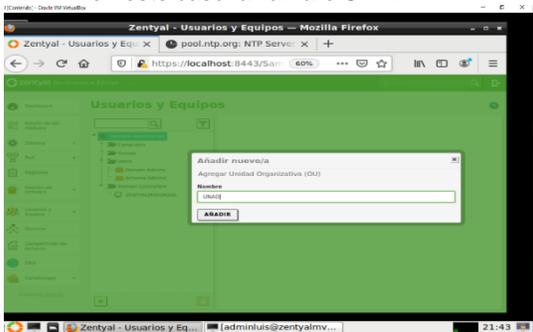


Figura 56.

Luego de ello procedemos a crear grupos de seguridad o de acceso. Crearemos los siguientes Administración, TI, Empleados

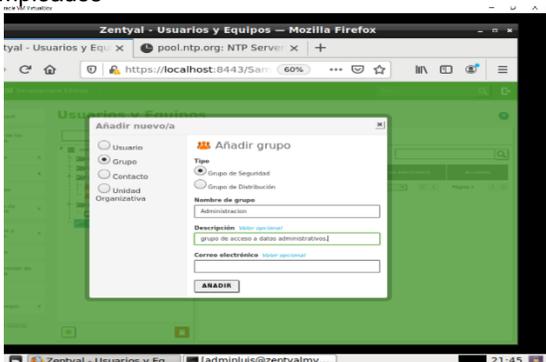


Figura 57.

Quedando así la estructura en la cual se evidencia una buena organización según sea el área al que se deba otorgar permisos.



Figura 58.

Finalmente vamos a crear diferentes usuarios para cada grupo. en la cual se debe hacer este mismo paso para cada usuario que se registre.



Figura 59.



Figura 60.

Procedemos a acceder al escritorio de Debían de la máquina de pruebas e Instalamos likewise. una aplicación que te ayuda para el acceso a un Directorio Activo.



Figura 61.

Luego de haber generado los directorios compartidos procedemos a modificar los controles de acceso por grupos y damos permisos de lectura y escritura



Figura 62.

Procedemos a modificar la plantilla del Usuario.



Figura 63.

5 TEMÁTICA VPN

Se realiza la configuración y puesta en marcha de una VPN por medio de Zentyal, ya realizado la instalación y configuración del sistema, ingresamos con usuario y contraseña al panel.



Figura 64. Configuración Inicial.

Se seleccionan los paquetes a instalar entre ellos la VPN



Figura 65. Instalación VPN

Seleccionados los paquetes a instalar se inicia el proceso, luego se configura las interfaces de red eth0 y la eth1.

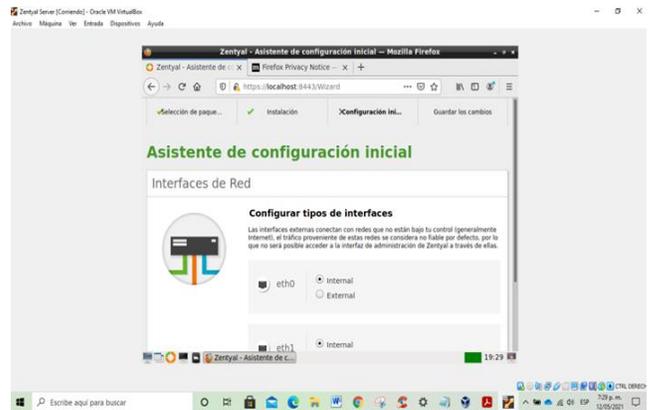


Figura 66. Interfaces de red

Ya terminada la instalación y configuración inicial de la VPN nos indica que la instalación ha sido completada

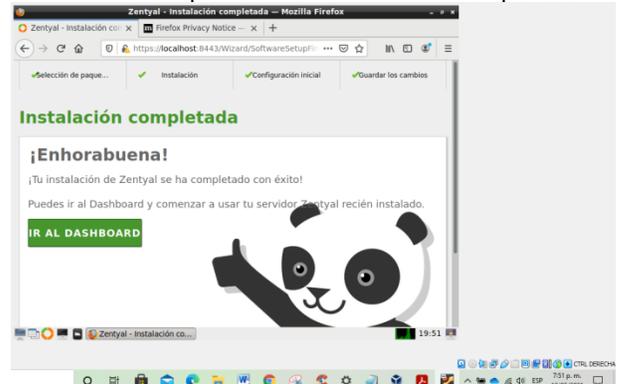


Figura 67. Instalación de paquetes completada.

Luego pasamos a la dashboard y a la parte izquierda encontramos los paquetes instalados entre ellos VPN

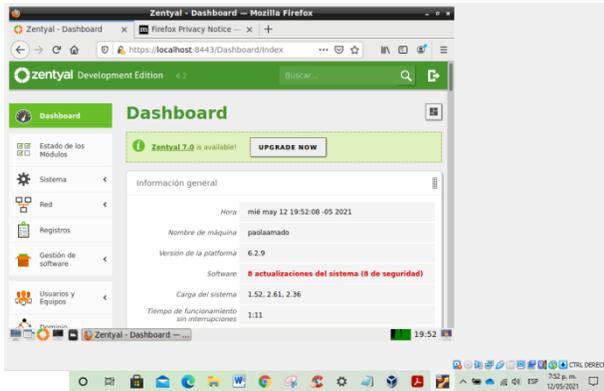


Figura 68. Dashboard

Ya instalada la VPN nos vamos para el panel de VPN lado izquierdo y damos clic en servidores el cual abre la ventana y damos clic en módulo de autoridad de certificación.

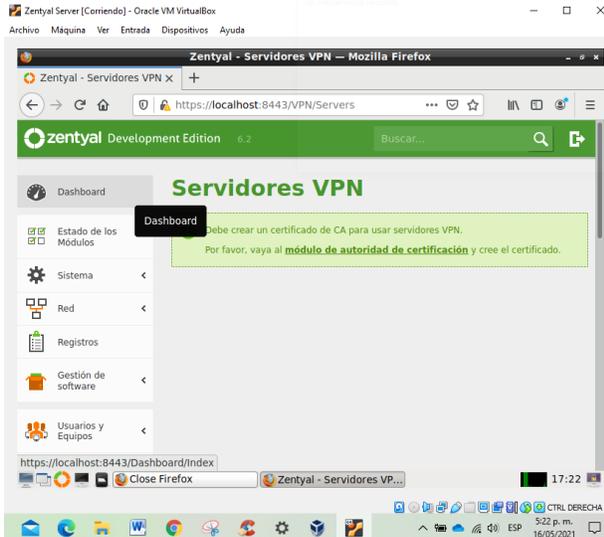


Figura 69 . Módulo de autoridad de certificación

Se realiza la creación de los certificados para la VPN

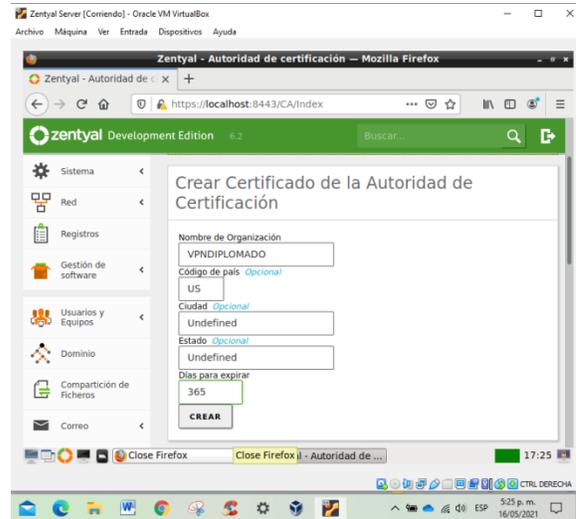


Figura 70. Autoridad de certificación

Se verifica el listado de certificados actual

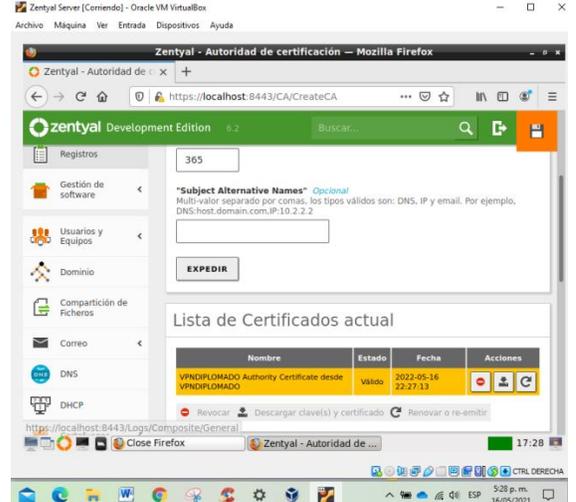


Figura 71. Lista de certificados

Se regresa a la pestaña de la VPN ubicada en el lado izquierdo y se crean los servidores para la VPN

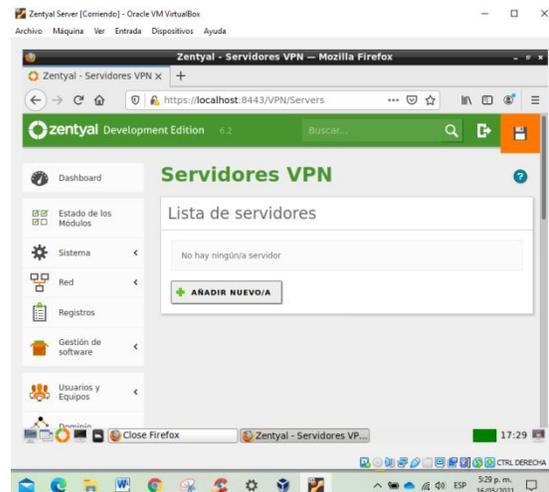


Figura 72. Crear Servidores

Se da clic en añadir nuevo y asignamos el nombre

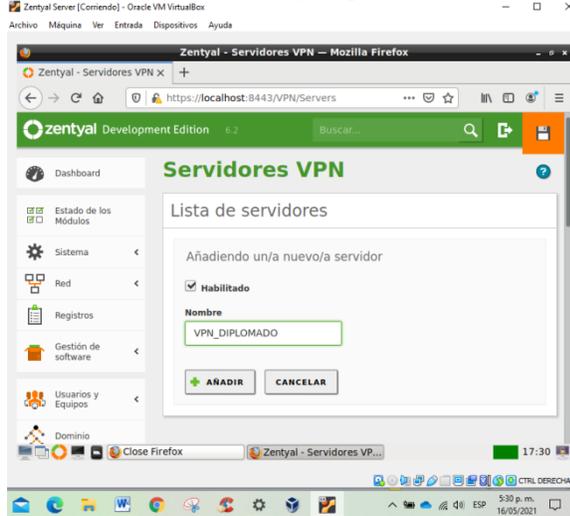


Figura 73. Asignación de nombre

Ya asignado el nombre se le da añadir y se evidencia la lista de servidores existentes

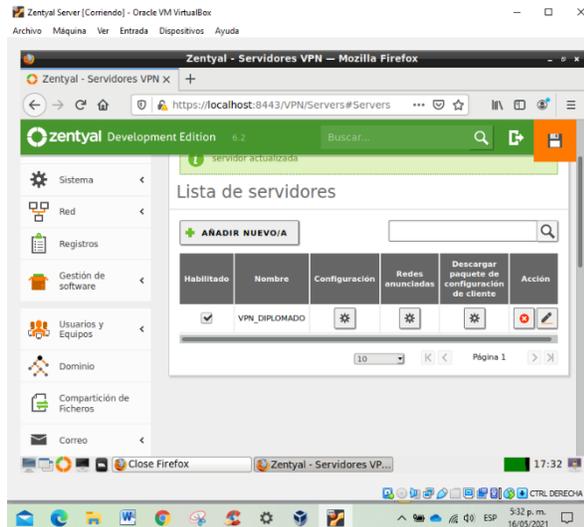


Figura 74. Lista de servidores

Se realiza la configuración de la VPN se da clic en Configuración, se asigna la ip y el puerto, se le da cambiar

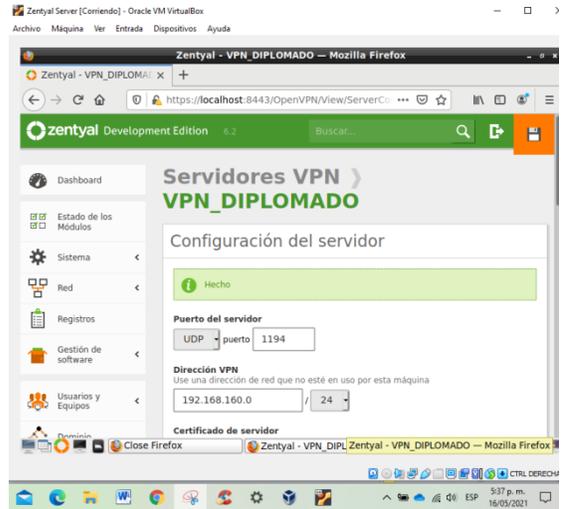


Figura 75. Configuración Servidor

Se guardan los cambios realizados en la configuración

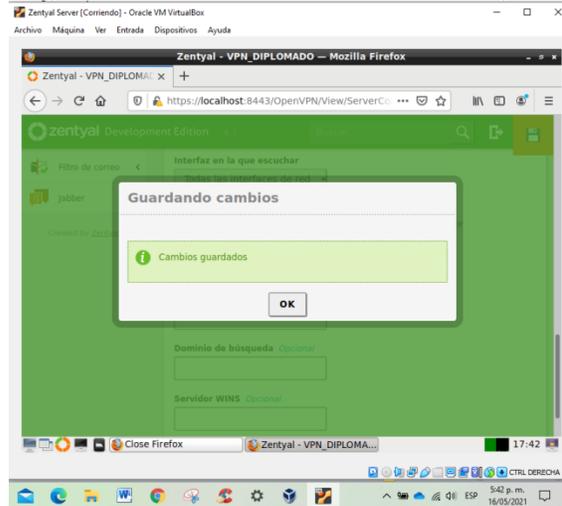


Figura 76. Guardar cambios

Se ingresa a descargar la configuración de los paquetes

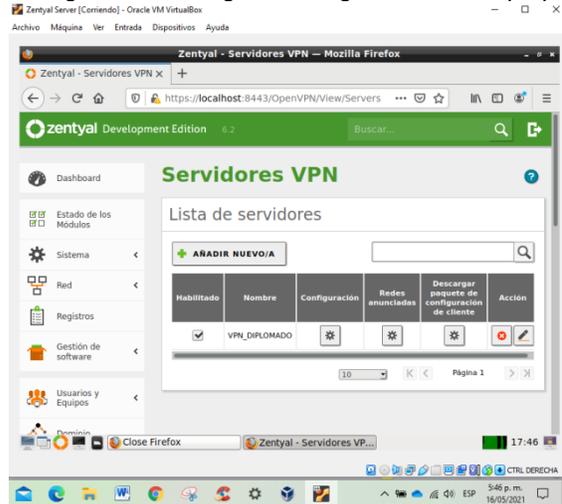


Figura 77. Paquetes

Para poder descargar los paquetes se le da clic en crear uno

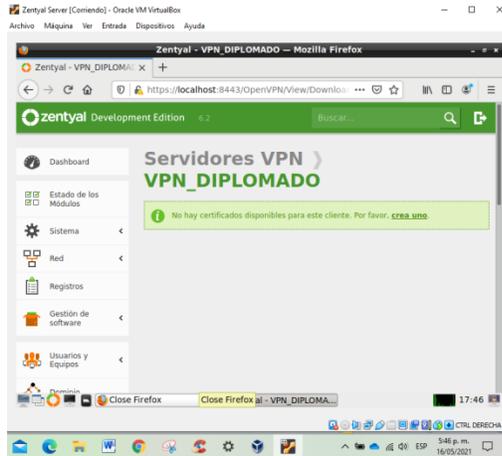


Figura 78. Crear paquete

Se ingresa nuevamente a VPN e ingresamos a paquete para configurar la ip de Zentyal

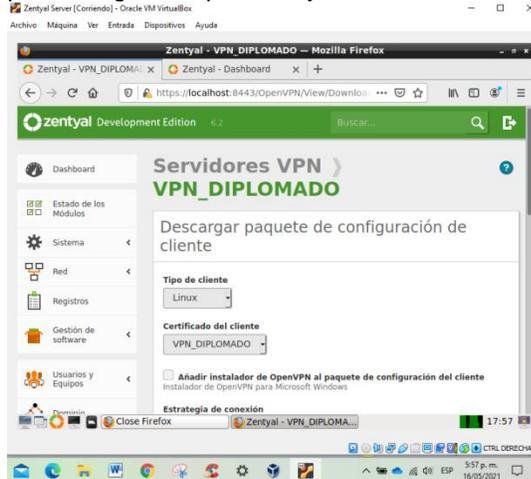


Figura 79. Configuración paquete cliente

Ya configurado el paquete para el cliente se realiza la descarga el cual seleccionamos la carpeta para guardar y configurar en el sistema

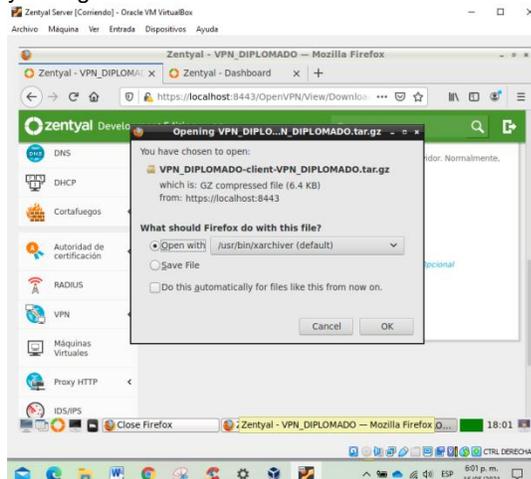


Figura 80. Paquete descargado

5.1.1 Conclusiones.

Se obtiene un aprendizaje valioso del sistema operativo Zentyal, ya que fue notoria su eficiencia durante el desarrollo de la actividad, se profundizó en el uso de las configuraciones de los servicios de DHCP, como de DNS y Dominio, sacándole un provecho a cada módulo.

Conocimos el servicio de Cortafuegos. Creamos y configuramos reglas para denegar accesos a ciertas páginas web. A mi parecer las funcionalidades que nos ofrece IPCop de cortafuegos es mucho mejor que la de Zentyal; ya que nos permite configurar bloqueos de páginas web con palabras claves, con dominios y a través de direcciones IP. Así mismo, nos da la opción de mostrar un mensaje personalizado en pantalla en las páginas web bloqueadas.

También comprendimos el proceso de realizar las diferentes actividades respecto a la administración y ejecución de los diferentes servicios que se pueden implementar como la creación de una VPN.

Esta sección no tiene requisitos especiales de formato.

6 REFERENCIAS

- [1] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40
- [2] 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>
- [3] Molina, R. F. J., & Polo, O. E. (2014). Servicios en red. (Páginas. 105 - 481). Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229687&ppg=104>
- [4] Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 3 - 10). Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=5349776&ppg=8>
- [5] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40