

IMPLEMENTACIÓN Y CONFIGURACIÓN DE UN SERVIDOR ZENTYAL COMO SOPORTE PARA ATENDER TODOS LOS SERVICIOS DE UNA INFRAESTRUCTURA IT.

Ana Maria Realpe
e-mail: amrealpeo@unadvirtual.edu.co
Francisco Javier Guzmán Polo
e-mail: ffguzman@unadvirtual.edu.co
Enrique Eduardo Orozco
e-mail: orozcoenrique01@gmail.com
Daniel Enrique Gálvez
e-mail: degalvezc@unadvirtual.edu.co
Markgero Arnold López
e-mail: malopezra@unadvirtual.edu.co

RESUMEN: Este artículo contiene la instalación y configuración de la distribución Zentyal server como solución al mejoramiento de la infraestructura IT de las organizaciones. se describe de manera muy detallada los procedimientos de implementación del servidor Zentyal para la administración de servicios como DNS, DHCP y controlador de dominio, así como el control de acceso a través de Proxy no transparente y cortafuegos. También, la configuración de servicio File Server y Print Server. Además del establecimiento de una VPN. Para la realización de cada proceso se hizo necesario contar con otra máquina virtual para hacer comprobaciones de conectividad y demostraciones de funcionamiento. Cada uno de estos procesos están organizados por temáticas descritas y argumentadas que presentan capturas que permiten una mejor comprensión de cada procedimiento.

PALABRAS CLAVE: Linux, Zentyal server, servicios, infraestructura IT.

1 INTRODUCCIÓN

Existen muchas distribuciones que permiten tener herramientas de administración de servicios que se pueden ofrecer a una infraestructura IT dentro de las organizaciones, pero sin duda Zentyal Server es la más utilizada por la confiabilidad de cada uno de los servicios y por la interoperabilidad con distintos sistemas operativos incluso en su versión de desarrollo. Este documento presenta la manera como se pueden implementar los servicios que ofrece un servidor como Zentyal y que permiten gestionar todas las herramientas que requieren las redes hoy en día, donde se pueden establecer controles de acceso y administración de recursos de una organización.

Zentyal es ideal para prestar servicios de red como DNS, DHCP, correo, Proxy, cortafuegos, administración de archivos y recursos, configuración de VPN entre otros.

2 INSTALACIÓN ZENTYAL SERVER 6.2

Zentyal server en su versión 6.2 está basada en la distribución de Linux 18.04.4 LTS, y presenta algunas novedades que buscan mejorar las estabilidad y seguridad del producto para ser más compatible e integrando más servicios de administración y control.

2.1 DESCARGA DE ZENTYAL SERVER

Desde el enlace <https://zentyal.com/community/> se puede descargar el archivo .iso de la última versión de Zentyal Server. En este documento se muestra el procedimiento de instalación en una máquina virtual preparada con VirtualBox.

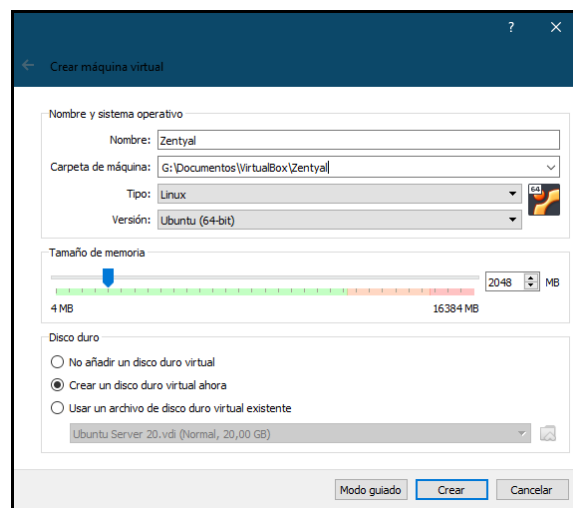


Figura 1. Creación de máquina virtual en VirtualBox.

Se configuran dos interfaces de red una para la conexión WAN de internet y otra para la red interna de los equipos desktop. Al iniciar la instalación se

selecciona el lenguaje, distribución del teclado y zona horaria.

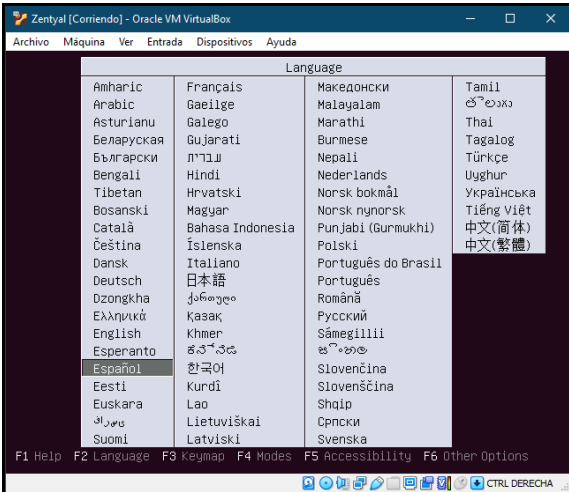


Figura 2. Selección de idioma de instalación de Zentyal.

Se elige el tipo de instalación de acuerdo con los requerimientos y necesidades de particionamiento.

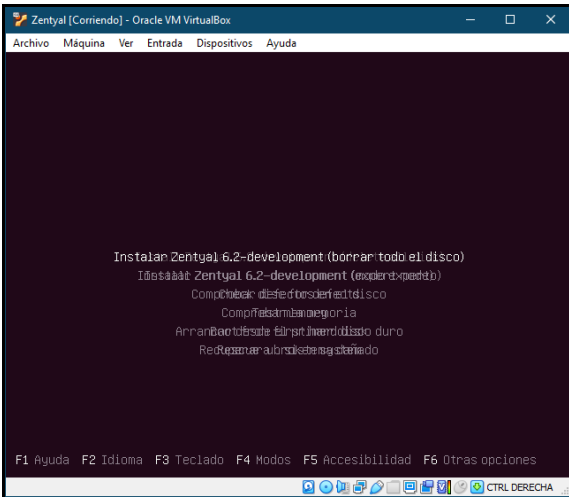


Figura 3. Elección del tipo de instalación.

En el proceso de la instalación se especifican el nombre del servidor, del usuario y la contraseña de acceso.

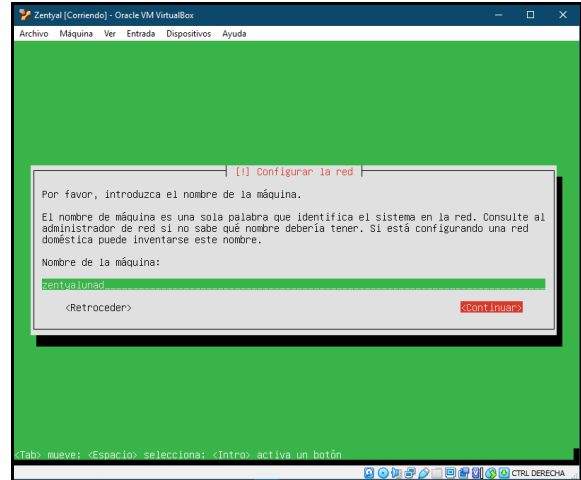


Figura 4. Introducción nombre de la máquina.

Al finalizar la instalación se extrae el disco de instalación y se reinicia la máquina. En el primer ingreso, se aceptan los permisos del navegador, luego se ingresa con el usuario y contraseña creados.

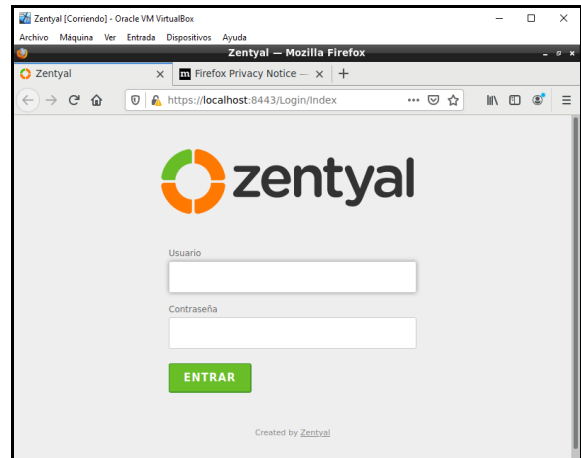


Figura 5. Inicio de sesión en Zentyal 6.2.

2.2 CONFIGURACIÓN INICIAL DE ZENTAL SERVER 6.2

Al iniciar sesión, seleccionamos los paquetes necesarios para los servicios que se van a configurar.

3 TEMÁTICAS SERVICIOS DE GESTIÓN INFRAESTRUCTURA IT

3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Zentyal nos permite configurar módulos o servicios de manera directa y con lo que no necesitamos tan directo los podemos encontrar dentro del DNS , DHCP y el controlador del dominio. Por lo que estos módulos se instalaran en la configuración inicial de Zentyal.

Inicia la instalación de paquetes seleccionados.



Figura 6. Selección de paquetes que se instalarán.

Luego de la instalación de paquetes se configuran las interfaces de red interna y externa. Como se muestra en la Fig. 7.



Figura 7. Configuración de interfaces.

Al finalizar el proceso ya se puede ingresar la dashboard y continuar con la configuración de los módulos.

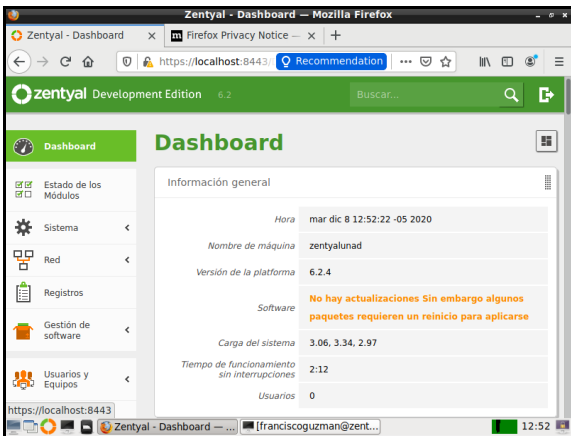


Figura 8. Ingreso al dashboard.

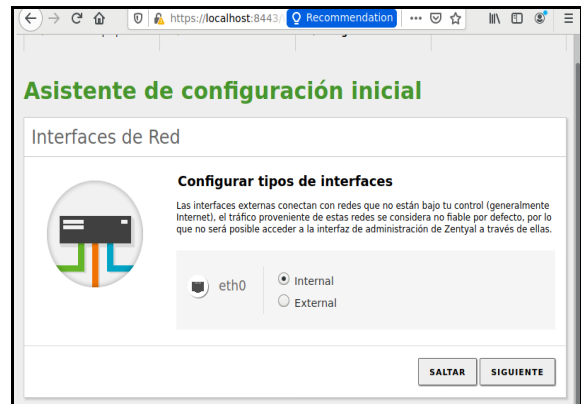


Figura 9. Configuración Inicial Interfaces.

Continuamos y seleccionamos DHCP.

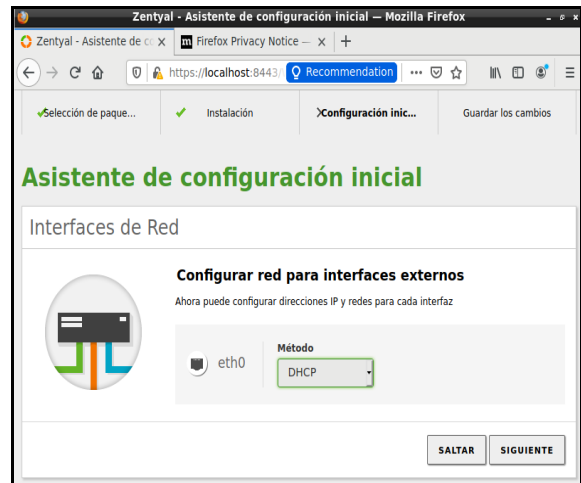


Figura 10. Configuración Inicial red para interfaces.

Validamos el nombre de dominio del servidor, damos finalizar.

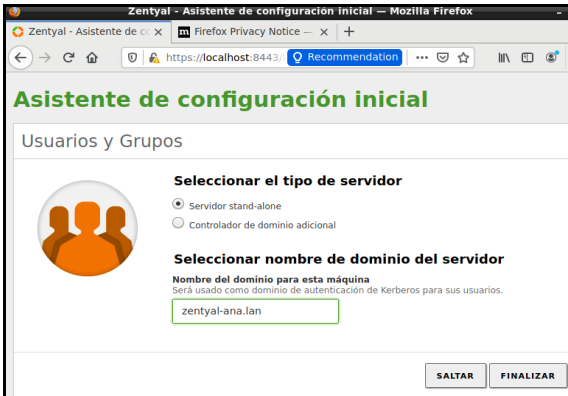


Figura 11. Configuración Inicial servidor.

Guardamos los cambios en los módulos y demás.



Figura 12. Habilitando Cambios.

Configuramos DHCP.

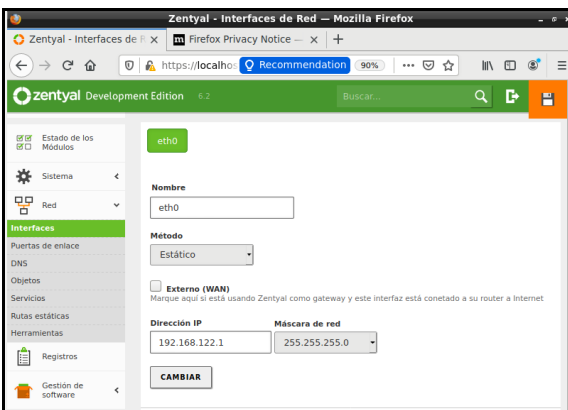


Figura 13. Configuración DHCP.

Habilitamos el DNS.

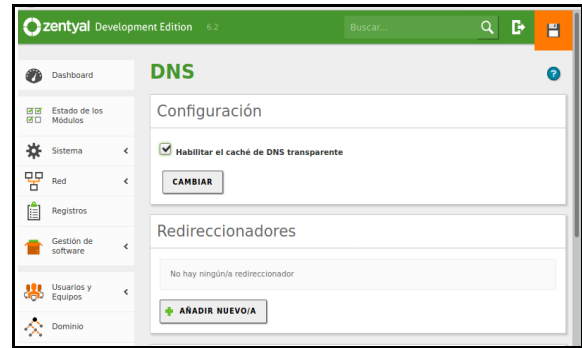


Figura 14. Configuración DNS.

Configuramos el dominio.

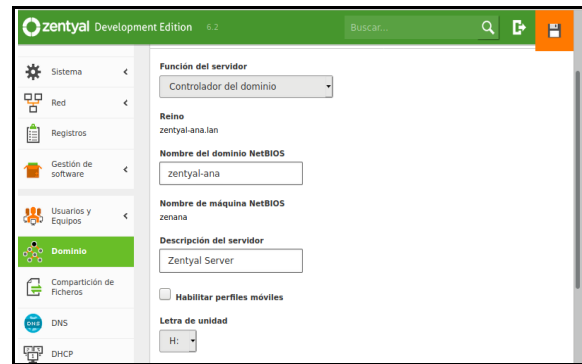


Figura 15. Configuración Dominio.

Creamos Grupo de Dominio.



Figura 16. Creación grupo Linux.

Creamos usuario para adicionar al grupo.



Figura 17. Creación usuario.

Así queda nuestro controlador de dominio.



Figura 18. Creación de dominio.

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Se realizará la 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.

Inicialmente ingresamos a configurar las dos interfaces de red instaladas previamente. La primera eth0 la nombramos WAN con dirección estática 192.168.100.200 y conexión externa.

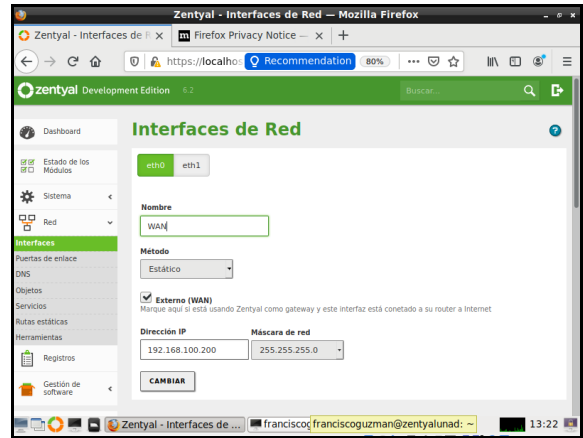


Figura 19. Configuración interfaz WAN

En la segunda eth1 se le coloca el nombre de LAN y dirección IP estática 192.168.200.254 y conexión interna.

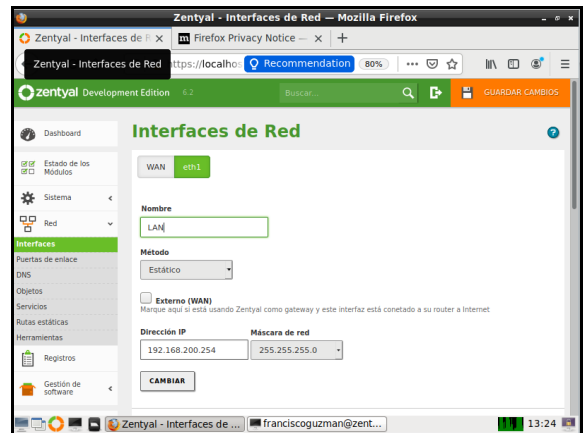


Figura 20. Configuración interfaz LAN

Seguidamente se añade una puerta de enlace que tendrá como nombre gw-wan y con dirección IP 192.168.100.1.

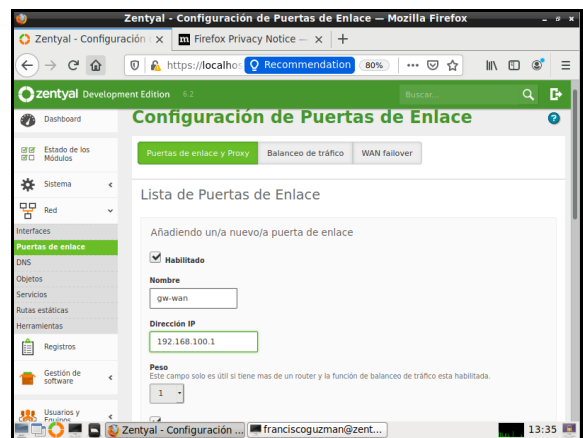


Figura 21. Configuración de puerta de enlace.

Luego se comprueba la conexión externa desde las herramientas de diagnóstico y desde la terminal, haciendo ping a una dirección web.

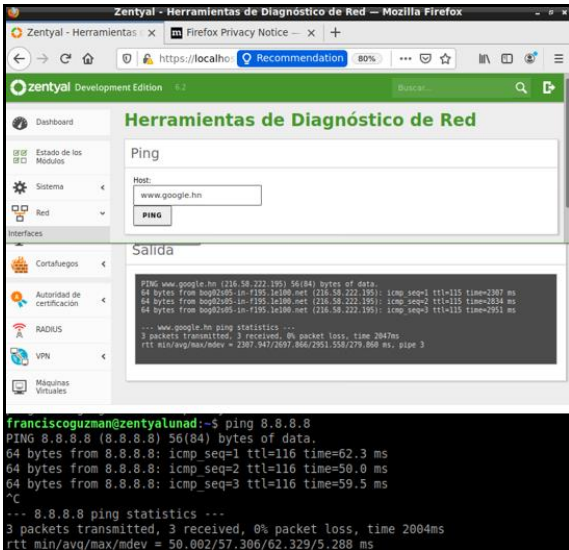


Figura 22. Comprobación de conexión externa.

Luego de esta verificación se crea una lista de objetos para trabajar con direcciones IP. En este caso se crea un objeto que llamaremos Administración.

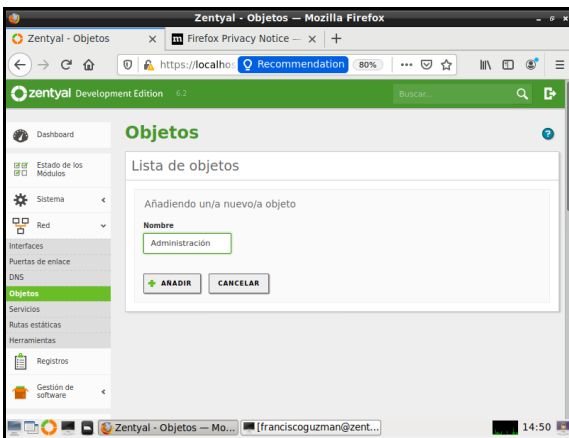


Figura 23. Creación de objetos.

Se crea un miembro que llamaremos SysAdmin con un rango de direcciones IP desde 192.168.200.1 hasta 192.168.200.14 y se le da en el botón AÑADIR y luego en GUARDAR CAMBIOS.

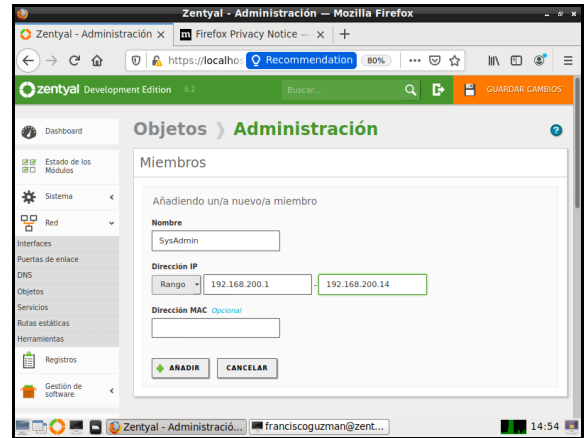


Figura 24. Creación de miembros.

Con esto ya está configurado el servidor Zentyal y se procede a configurar la máquina del equipo Desktop. Se abre la terminal del Desktop y descarga el paquete pbis-open, el cual permite a Linux unirse a un Active Directory.

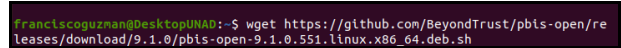


Figura 25. Descarga del paquete pbis-open.

Se establecen los permisos del paquete pbis-open y se procede a su instalación.

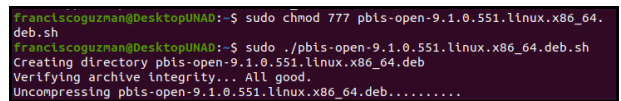


Figura 26. Instalación del paquete pbis-open.

Seguidamente se configura la dirección IP del equipo cliente, asignándole la dirección IP 192.168.200.10 con puerta de enlace 192.168.200.254.

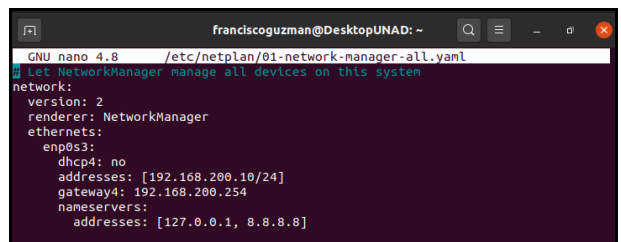


Figura 27. Asignación IP de equipo cliente.

Se comprueba la conectividad del equipo cliente con el servidor Zentyal desde la terminal.

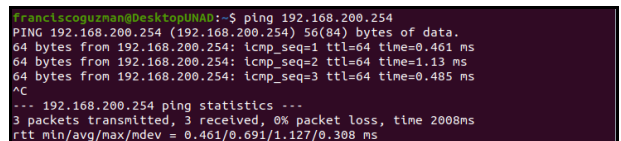


Figura 28. Comprobación de conectividad con el servidor.

También se puede hacer la comprobación de conectividad a internet desde el navegador.

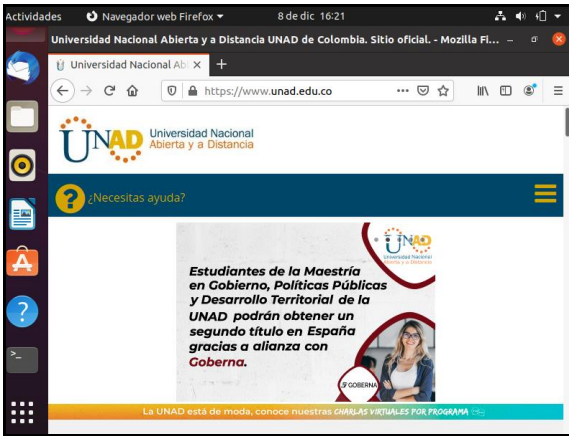


Figura 29. Prueba de conexión a Internet.

Se regresa al servidor Zentyal y se activan los módulos necesarios para la configuración del proxy no transparente. Para esto se ingresa al módulo Proxy HTTP y se selecciona Configuración General. En esta se deselecciona la opción de Proxy transparente y se coloca el puerto 1230, luego se hace clic en la opción Cambiar y se guardan los cambios.

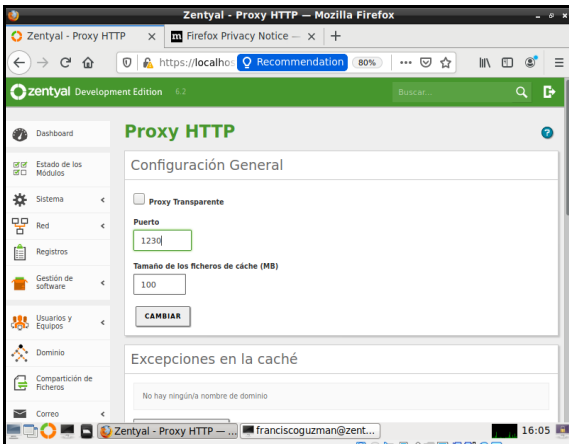


Figura 30. Configuración de Proxy no transparente.

Se Crean las reglas de trabajo para los clientes. En el mismo menú de Proxy HTTP se selecciona la opción de Reglas de Acceso, se hace clic en el botón añadir Nuevo/a. En origen se selecciona el objeto de red Administración previamente creado y en Decisión se selecciona Denegar todo y se hace clic en el botón Añadir.

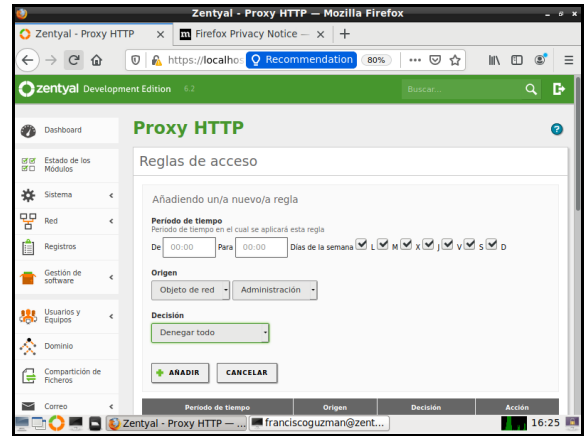


Figura 31. Creación de reglas de acceso del Proxy.

Al guardar los cambios se pueden observar las reglas creadas.

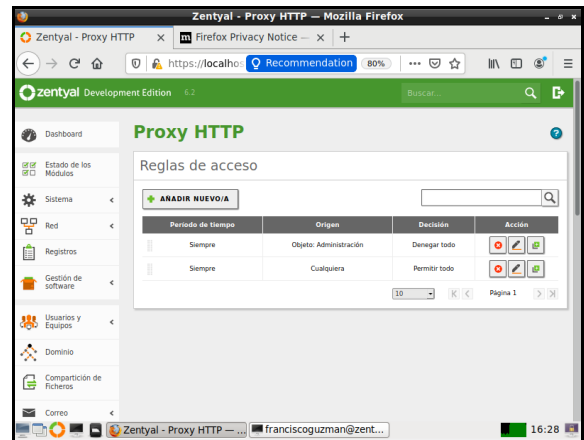


Figura 32. Detalle de las reglas del Proxy.

Para que se aplique la regla en el equipo cliente se regresa al mismo y en la configuración del navegador de Internet, se colocan los datos del Proxy del servidor. y en la opción preferencias de red/configuración manual del proxy, se escriben la dirección IP del Proxy 192.168.200.254 y el puerto 1230.

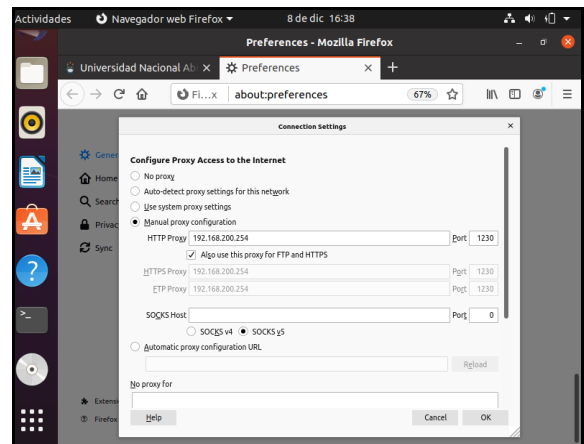


Figura 33. Configuración de red del navegador de Internet.

Finalmente se valida la conexión en el mismo navegador visitando algún sitio y se observa que efectivamente está bloqueado el acceso a internet.

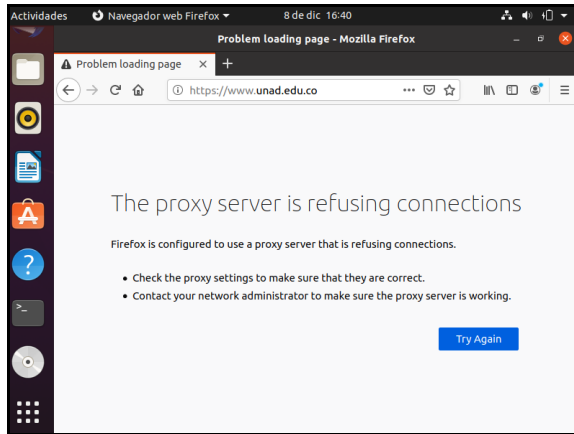


Figura 34. Verificación de conexión Proxy no transparente.

3.3 TEMÁTICA 3: CORTAFUEGOS

En el siguiente paso se realizará la implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, haciendo uso de reglas y políticas, además de aplicar las restricciones solicitadas a través de la distribución Zentyal aplicando la configuración a una estación de trabajo GNU/Linux.

Iniciamos el dashboard de Zentyal.

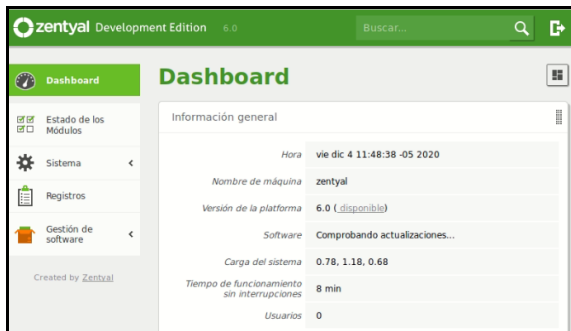


Figura 35. Inicio del Dashboard.

Añadimos los paquetes necesarios



Figura 36. Adición de paquetes.

Luego instalamos el módulo proxy http y lo activamos



Figura 37. Instalación de módulos Proxy HTTP y Cortafuegos

Creamos un nuevo objeto y especificamos las ip del grupo- Añadimos los miembros del grupo.



Figura 38. Creación de objetos y miembros.

Entramos en proxy http y creamos un nuevo perfil.



Figura 39. Creación de Perfil de Filtrado.

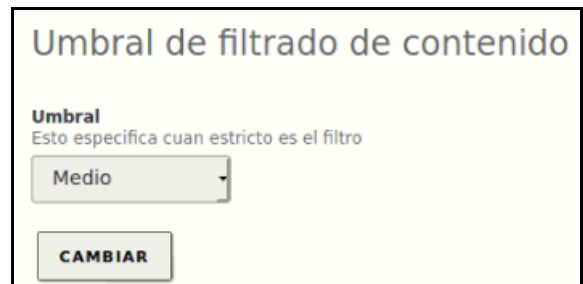


Figura 40. Especificación de umbral de filtrado.

Creamos una nueva regla para bloquear el acceso a redes sociales.



Figura 41. Reglas de dominios y URLs.

Reglas creadas.







Dominio o URL	Decisión	Acción
twitter.com	Denegar	 
instagram.com	Denegar	 
facebook.com	Denegar	 

Figura 42. Lista de reglas.

Entramos en reglas de acceso, y guardamos.

Reglas de acceso

Editando regla

Periodo de tiempo
Periodo de tiempo en el cual se aplicará esta regla
De: 00:00 Para: 00:00 Días de la semana L M X J V S D

Origen
Objeto de red: ventas

Decisión
Aplicar perfil de filtrado: general

CAMBIAR **CANCELAR**

Figura 42. Establecimiento de regla de acceso.

Ingresamos en un cliente que tenga asignada una de las ips q bloqueamos en los pasos anteriores de la red y comprobamos el bloqueo a las redes sociales

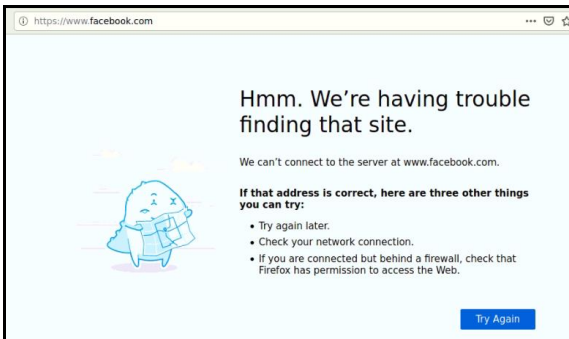


Figura 43. Bloqueo de acceso a www.facebook.com

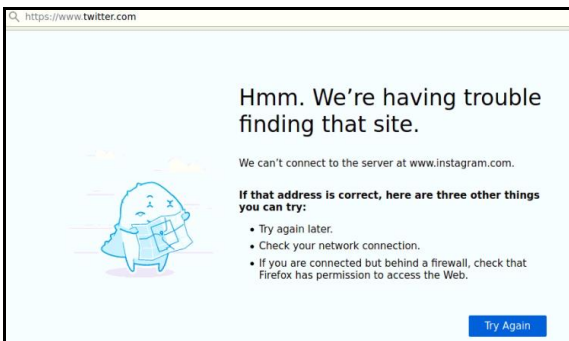


Figura 44. Bloqueo de acceso a www.twitter.com

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Comenzamos configurando la interfaz que utilizaremos la cual dejaremos como interna (Esto lo hicimos al comenzar el proyecto), confirmamos nuestra configuración en nuestro caso utilizaremos eth1 le

asignaremos la ip que necesitamos y le cambiamos el nombre a LAN y asignamos ip fija.

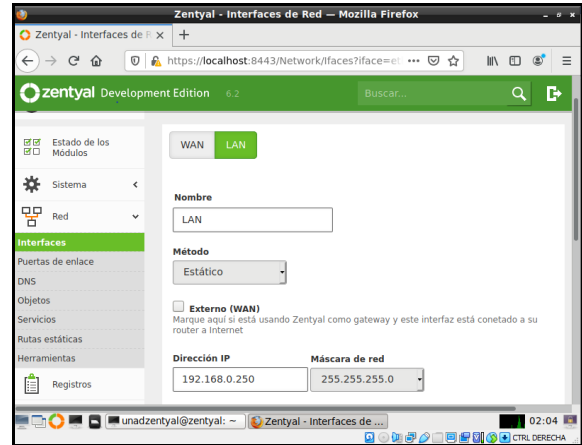


Figura 45. Configuración de ethernet

En el caso de la interfaz 1 esta puede dejarse con IP fija una vez revisado desde terminal con el comando ifconfig que configuración tiene asignada, una vez configuradas nuestras interfaces de red debemos registrar un puerto de enlace para nuestra interfaz LAN el cual nos permitirá la comunicación con nuestras maquinas clientes.

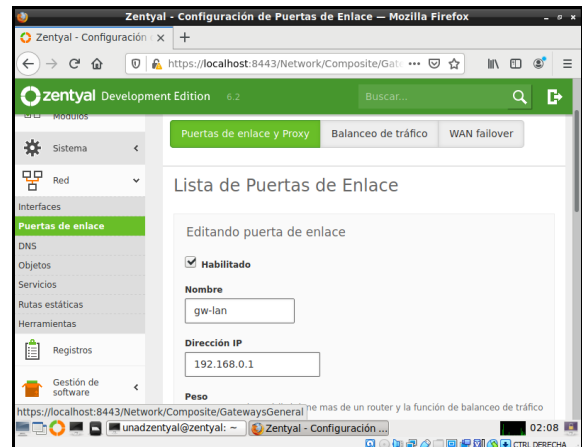


Figura 46. Creación de puerto de enlace.

Debemos configurar nuestro servidor DHCP, nos dirigimos a configurar nuestro servidor DHCP para ellos le vamos a especificar el DNS que vamos a usar, la IP del puesto de enlace que vamos a utilizar para la asignación de IPS y el rango de IPS que deseamos utilizar para nuestros clientes

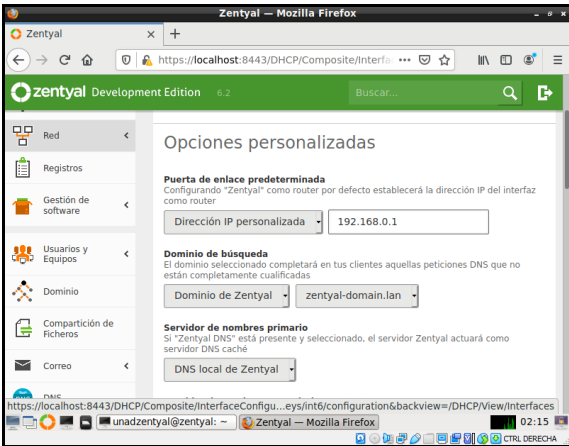


Figura 47. Configuración de DHCP.

Una vez realizada las configuraciones anteriores comenzamos nuestra configuración del cliente, para nuestro cliente utilizaremos una maquina con sistema operativo Windows 7 y al montar nuestra interfaz de red le especificamos que es interna para que tenga comunicación con nuestra servidor DHCP que configuramos en Zentyal, una vez especificado esto encendemos la maquina y nos dirigimos a confirmar que nuestro servidor DHCP esté funcionando, Esto quiere decir que al momento de verificar la configuración de la red nos debe mostrar los parámetros que configuramos para ella, en nuestro caso quedaría de la siguiente manera.

```
C:\Users\unadclient>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión . . . : zentyal-domain.lan
    Dirección IPv6 local . . . . . : fe80::4ad:22e:624c:4df%11
    Dirección IPv4 . . . . . : 192.168.0.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

Figura 48. Ethernet client.

Ahora vamos a crear una carpeta compartida en nuestro servidor además un usuario y un grupo para nuestro cliente. Además crearemos un usuario más el cual utilizaremos para configurar nuestros clientes

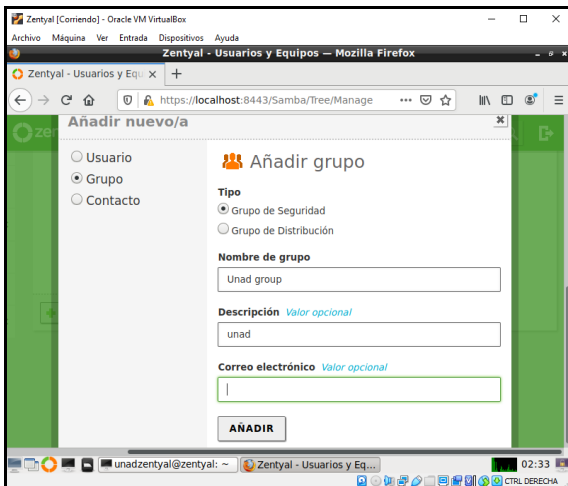


Figura 49. Creación Usuario unadclient1.

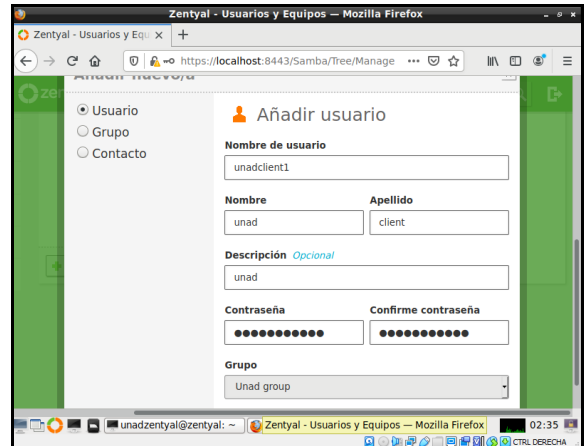


Figura 50. Creación de carpeta compartida.

Ahora nuestro paso a seguir es incluir nuestra maquina cliente en el dominio, para ello nos vamos a propiedad del equipo y nos dirigimos a configuraciones avanzadas del sistemas y luego a cambiar configuración de nombre y dominio, una vez agreguemos al dominio la nueva máquina ingresamos con el usuario que pertenezca a grupo domain para que nos permita realizar las configuraciones pertinentes, ahora debemos ingresar a nuestra maquina Windows con cualquiera de nuestros usuarios en este caso usaremos unadclient1 y nos dirigiremos a las carpetas en red, ingresamos a la carpeta de Zentyal y podremos ver que tenemos nuestra carpeta que creamos desde nuestro servidor.

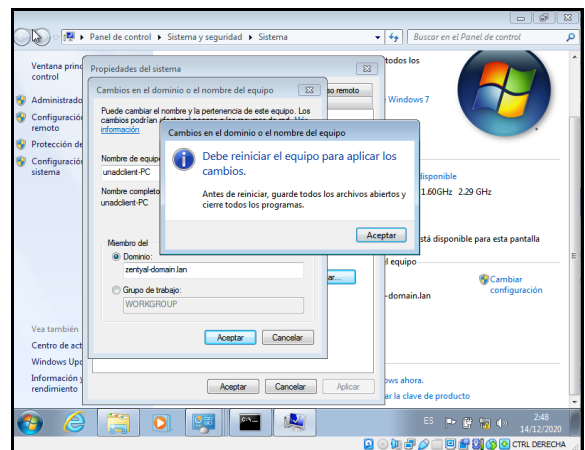


Figura 51. Acceso al dominio.

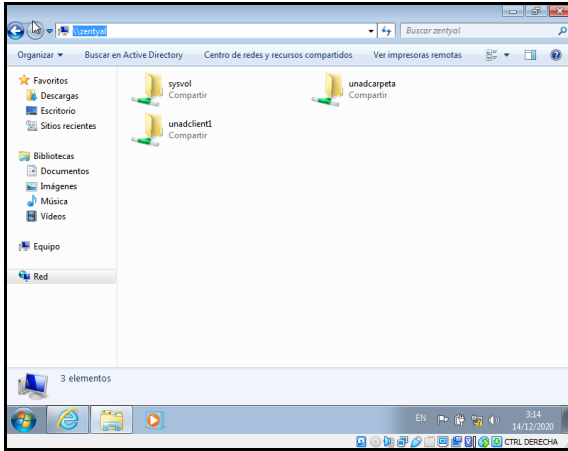


Figura 52. Acceso carpeta compartida.

3.5 TEMÁTICA 5: VPN

Para configurar una red VPN se debe tener en cuenta unos servicios instalados después de haber instalado Zentyal, esto servicios los reporta el mismo server pero se deben escoger manualmente, como lo son autoridad de certificaciones, VPN, firewall y DHCP.

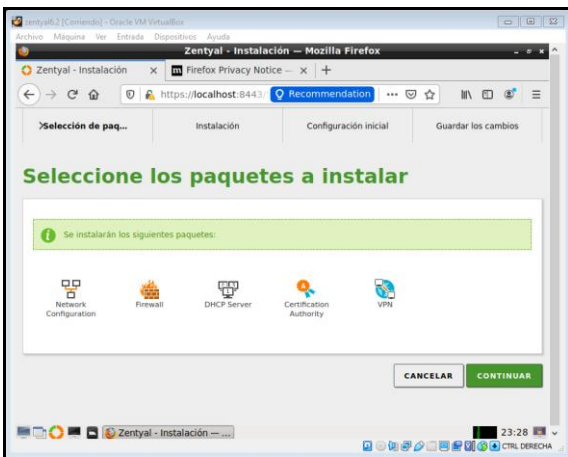


Figura 53. Selección de paquetes a instalar.

Después de haber escogido los paquetes a instalar procedemos a crear el certificado de la autoridad, tanto para el servidor VPN y los clientes, teniendo en cuenta que se debe de expedir uno diferente para cada cliente, esto se hace en la misma sección.

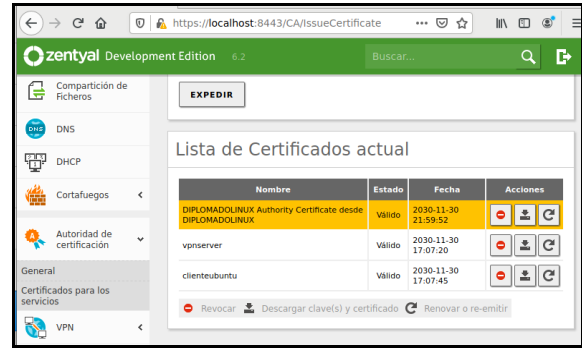


Figura 54. Elaboración y visualización de certificados.

Posteriormente pasamos a crear el servidor VPN, seleccionando añadir en la opción servidores de VPN, aquí añadimos el nombre del servidor, aquí ya en configuraciones, revisando el puerto 1194, protocolo UDP, seleccionando una dirección Ip.

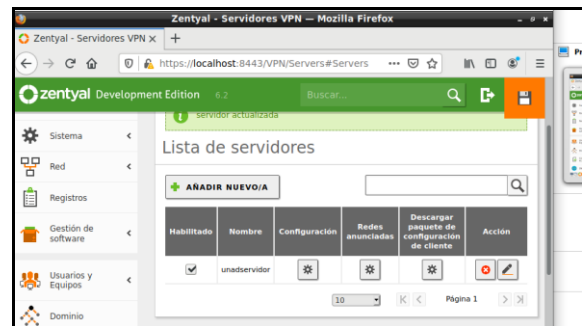


Figura 55. Configuración del servidor VPN.

Ahora debemos ir a la opción red dentro del panel de Zentyal y se escoge la opción servicios, para agregar un nuevo servicio, debemos configurar el puerto destino como puerto único 1194, dar guardar y tener en cuenta que el protocolo TCP/UDP, puerto de origen cualquiera.

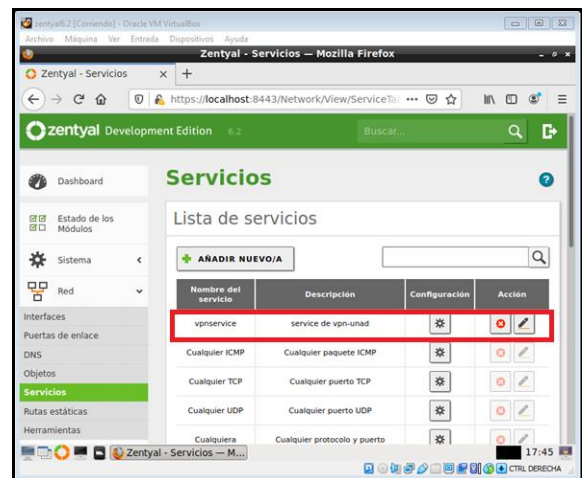


Figura 56. Configuración del servicio.

Posteriormente se accede al módulo de firewall y luego apartado de filtrado donde ahí vamos a crear una regla para el tipo de acceso que daremos, tener en

cuenta que esto se desarrolla desde las reglas de filtrado para las redes internas, seguimos con añadir nuevo

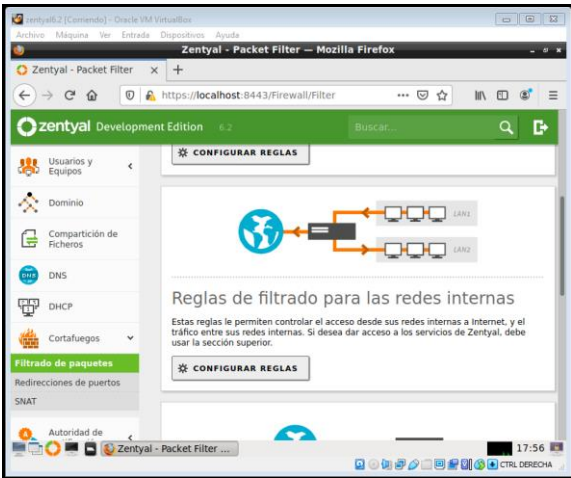


Figura 57. Configuración del cortafuegos desde la regla de redes internas.

El paso a seguir es ir a la opción de VPN sección servidores para signar una red anunciada, dando clic a la configuración más añadir nueva y posteriormente descargar esa configuración.

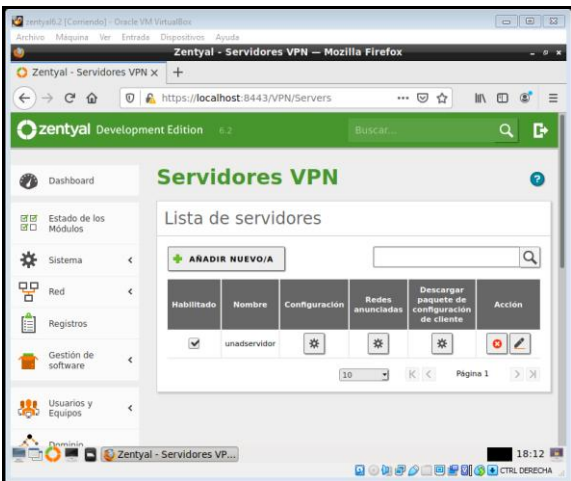


Figura 58. Configuración y creación del servidor VPN

Le damos añadir un nuevo objeto asignado el miembro al servidor, como se recuerda ya habíamos creado un servidor y se debe crear la red anunciada dentro del mismo.

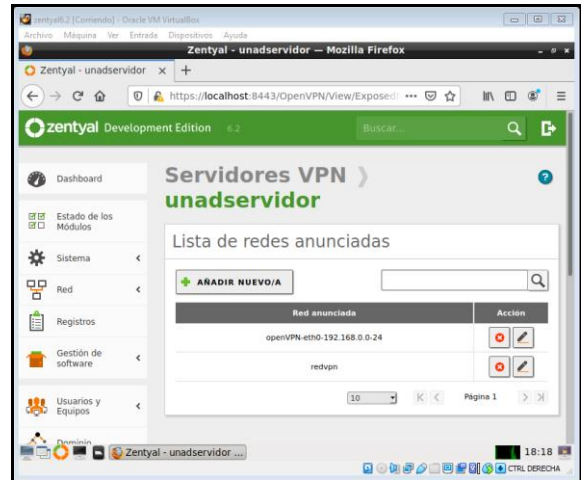


Figura 59. Creación red anunciada.

Ya luego de haber creado los certificados y el servidor dentro de la opción VPN pasamos a descargar los paquetes de configuración del cliente, se debe escoger el cliente, que se desea trabajar ya que hay opciones de Windows, Linux, en este caso se escoge Linux, se revisa el certificado, no olvidar poner la dirección ip en la red interna, para descargar la configuración comprimido, se da la opción descargar, para luego pasar esta configuración al cliente es decir a Ubuntu.

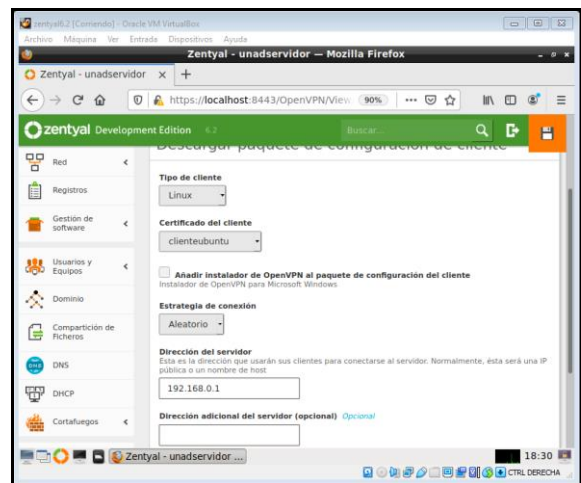


Figura 60. Configuración paquetes del cliente.

Ya luego de descargar el paquete del cliente en nuestra maquina debemos descomprimir este archivo zip, se puede hacer modo consola con el unzip o clic derecho y descomprimir el fichero, ya que debemos saber que necesitamos el client.conf

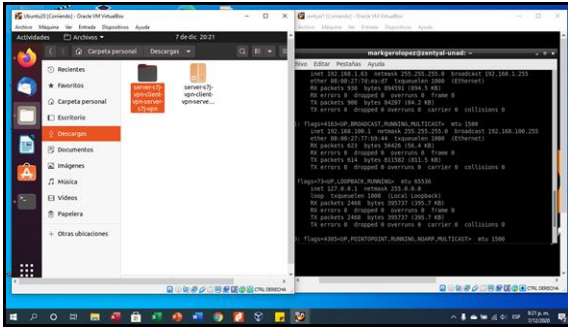


Figura 61. Descomprimir fichero servidor-cliente.

Hacemos una prueba rápida por medio del ping entre Ubuntu 2º y Zentyal 6.2, para saber si se están comunicando, el ping más la dirección ip del Zentyal, ahora desde el Ubuntu 20, instalamos el openvpn, el cual es la herramienta que nos permitirá ejecutar la VPN y sus certificados ya configurados, para ello debemos saber la ruta de donde está el paquete, en esta ocasión está en descargas le damos Ctrl L y con eso vemos la ruta para guiarnos mejor y colocar esa ruta en la consola modo super usuarios.

```
root@markgerolopez-VirtualBox:~/home/markgerolopez/Descargas# cd server-s7j-vpn-client-vpn-server-s7j-vpn
root@markgerolopez-VirtualBox:~/home/markgerolopez/Descargas/server-s7j-vpn-client-vpn-server-s7j-vpn# openvpn --config server-s7j-vpn-client.conf
```

Figura 62. Ejecución comando open-VPN

Ya luego de descargados los paquetes y ejecutado por open VPN, hacemos el acceso remoto por medio del cliente al servidor, suministrando la ip en la URL de Firefox y se visualiza las dos distribuciones en paralelo.

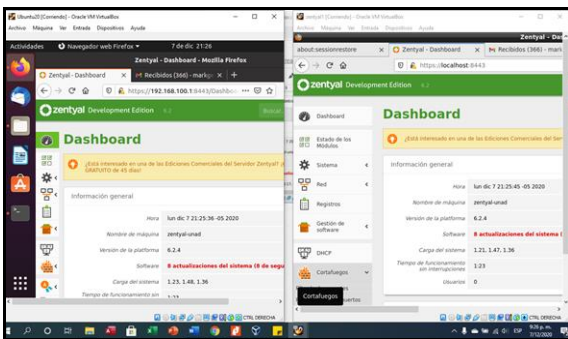


Figura 63. Visualización por medio de la URL del cliente el aplicativo Zentyal.

4 CONCLUSIONES

La distribución Zentyal nos permite gestionar los dominios, creando y administrando reglas y políticas de acceso en la red. Además de poder implementar y configurar de manera detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Zentyal hace posible el control de acceso a Internet a través de reglas establecidas en la configuración del Proxy HTTP en modo transparente o no transparente

forzando políticas establecidas que nos permite establecer un puerto en el que el servidor monitorea las conexiones entrantes.

El módulo de cortafuegos e Zentyal permite establecer la seguridad de acceso a ciertos sitios web, de acuerdo con reglas específicas establecidas para tal fin.

Compartir recursos de un servidor a través de Zentyal constituye un mejor manejo de directorios e impresoras permitiendo la posibilidad de gestionar estos recursos según la políticas de la organización.

La red VPN nos facilita el acceso remoto, con el apoyo de una red local. dándonos la privacidad y seguridad de los canales de información y dándonos la oportunidad de evitar que nos bloqueen sitios web, ofreciendo una mayor seguridad esta se hace por medio del cifrado de paquetes, además nos permite la autenticación de clientes a través de los certificados.

5 REFERENCIAS

- [1] Zofío, J. J. (2013). Aplicaciones web. (Páginas. 205 - 236). Recuperado de <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43262?page=205>
- [2] Naranjo.(2019), Zentyal, una excelente distribución para crear servidores. [En línea] Disponible en:<https://ubunlog.com/zentyal-una-excelente-distro-para-crear-servidores-locales/>.
- [3] Zentyal S.L(2018),Primeros pasos con Zentyal. [En línea] .Disponible en: <https://doc.zentyal.org/es/firststeps.html>
- [4] Zentyal (2020) Qué es Zentyal. . [En línea] .Disponible en: <https://es.wikipedia.org/w/index.php?title=Zentyal&oldid=131187704>. 2020
- [5] Zentyal Wiki. (2015). Instalación y configuración de Zentyal Server 5. [En línea]. Disponible en: [https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_d_e_nombres_de_dominio_\(DNS\)](https://wiki.zentyal.org/wiki/Es/4.1/Servicio_de_resolucion_d_e_nombres_de_dominio_(DNS))
- [6] Zentyal Wiki. (2016). La interfaz web de administración de Zentyal. [En línea]. Disponible en: <https://wiki.zentyal.org/wiki/Es/5.0/Instalacion>
- [7] Zapata, F. (s. f.).Zentyal – Controlador de Dominio Linux y Políticas de Grupo. (2019, julio 8). Las ideas no duran mucho, hay que hacer algo con ellas. <https://julioestrepo.wordpress.com/2019/07/08/zentyal-controlador-de-dominio-linux-y-politicas-de-grupo/>
- [8] Gómez, J. (2014, mayo 13). Zentyal - Bloquear sitios web por HTTP. [En línea]. Disponible en: https://www.youtube.com/watch?v=73z1T_NIGZI
- [9] Zentyal. (2014). Configuración de un servidor de impresoras con Zentyal. [En línea]. Disponible en: https://wiki.zentyal.org/wiki/Es/4.1/Configurar_un_servidor_de_ficheros_con_Zentyal
- [10] Zentyal. (2015). Configurar un servidor de ficheros con Zentyal. [En línea]. Disponible en: https://wiki.zentyal.org/wiki/Es/4.1/Configurar_un_servidor_de_ficheros_con_Zentyal