

IMPLEMENTACIÓN DE SERVIDOR DE ADMINISTRACIÓN DE SERVICIOS DE RED EN GNU/LINUX ZENTYAL SERVER 6.2

Christian Camilo Gómez Bautista – código: 1.095.914.020

e-mail: chrisgo88@gmail.com

José Alexander Arrieta Suarez – código: 13.571.071

e-mail: alex_as12@hotmail.com

Jhon Freddy Maldonado Gómez – código: 91.509.744

e-mail: jfmaldonado27@gmail.com

Jesús David Cortés Ariza – código: 1.101.696.028

e-mail: cortesjdda@outlook.com

RESUMEN: El presente trabajo tiene como objetivo formular soluciones bajo GNU/Linux a través de la instalación, configuración y puesta en marcha de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente. A través del sistema operativo Zentyal Server 6.2 bajo el cual se implementaran los servicios y plataformas como, DHCP Server, DNS Server y Controlador de Dominio, Proxy, Cortafuegos, File Server y Print Server, VPN.

ABSTRACT: The objective of this paper is to formulate solutions under GNU / Linux through the installation, configuration, and start-up of technological infrastructure that allows responding to the specific requirements of the client. Through the Zentyal Server 6.2 operating system under which services and platforms such as DHCP Server, DNS Server, and Domain Controller, Proxy, Firewall, File Server and Print Server, VPN will be implemented.

PALABRAS CLAVE: Servidor, cliente, Zentyal, DNS, DHCP, cortafuegos, proxy, controlador de dominio, VPN, NSLOOKUP.

1 INTRODUCCIÓN

Este documento describe el proceso que permite dar Solución a problemáticas específicas de infraestructura tecnológica bajo la implementación y uso de Tecnologías GNU/Linux, a los requerimientos del cliente, a través del sistema operativo Zentyal Server ya que incluye todos los servicios necesarios para abordar la gestión y administración de los servicios esenciales. Entre las soluciones que brinda podemos mencionar: gestión de infraestructura de red, gateway, servidor de oficina o de comunicaciones.

2 Desarrollo del paso 8 - solucionando necesidades específicas con GNU/Linux.

2.1 Temática 1: DHCP Server, DNS Server y Controlador de Dominio.

Temática desarrollada por el estudiante José Alexander Arrieta Suarez.

Instalación del sistema operativo Zentyal Server 6.2.

La instalación comprende pasos sencillos como nombrar la máquina, usuarios, contraseñas y configurar zonas horarias entre otras.

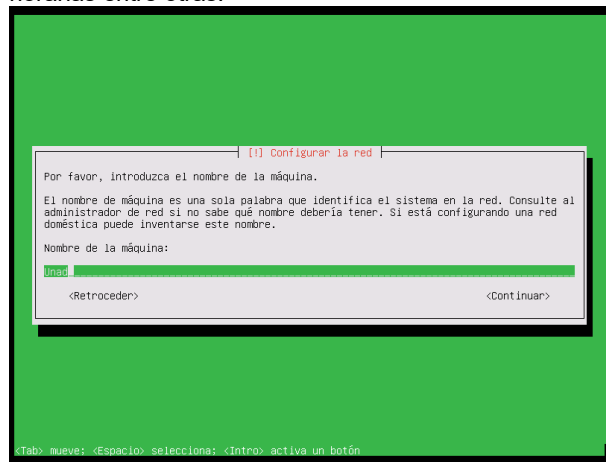


Imagen 1. Instalación Zentyal 6.2. Autoría propia.



Imagen 2. Ventana escritorio Zentyal 6.2. Autoría propia.

Después de iniciar el entorno de escritorio, se actualizan los paquetes del sistema operativo, ejecutando los siguientes comandos desde la terminal:

sudo apt update

```
alexarrieta@unad:~$ sudo apt update
[sudo] password for alexarrieta:
Des:1 file:/var/tmp/zentyal-packages / InRelease
Ign:1 file:/var/tmp/zentyal-packages / InRelease
Des:2 file:/var/tmp/zentyal-packages / Release
Ign:2 file:/var/tmp/zentyal-packages / Release
Des:3 file:/var/tmp/zentyal-packages / Packages
Ign:3 file:/var/tmp/zentyal-packages / Packages
Des:4 file:/var/tmp/zentyal-packages / Translation-es_CO
Ign:4 file:/var/tmp/zentyal-packages / Translation-es_CO
Des:5 file:/var/tmp/zentyal-packages / Translation-es
Ign:5 file:/var/tmp/zentyal-packages / Translation-es
Des:6 file:/var/tmp/zentyal-packages / Translation-en
Ign:6 file:/var/tmp/zentyal-packages / Translation-en
Des:3 file:/var/tmp/zentyal-packages / Packages
Ign:3 file:/var/tmp/zentyal-packages / Packages
Des:4 file:/var/tmp/zentyal-packages / Translation-es_CO
Ign:4 file:/var/tmp/zentyal-packages / Translation-es_CO
Des:5 file:/var/tmp/zentyal-packages / Translation-es
Ign:5 file:/var/tmp/zentyal-packages / Translation-es
Des:6 file:/var/tmp/zentyal-packages / Translation-en
Ign:6 file:/var/tmp/zentyal-packages / Translation-en
```

Imagen 3. Actualización del sistema. Autoría propia.

sudo apt list --upgradable

```
alexarrieta@unad:~$ sudo apt list --upgradable
Et: Release file for http://co.archive.ubuntu.com/ubuntu/dists/bionic-backports/InRelease is not valid or
et (invalid for another 2d 3h 18min 19s). Updates for this repository will not be applied.
alexarrieta@unad:~$ sudo apt list --upgradable
Listando... Hecho
linux-generic/bionic-updates 4.15.0-124.111 amd64 [actualizable desde: 4.15.0-122.109]
linux-headers-generic/bionic-updates 4.15.0-124.111 amd64 [actualizable desde: 4.15.0-122.109]
linux-image-generic/bionic-updates 4.15.0-124.111 amd64 [actualizable desde: 4.15.0-122.109]
alexarrieta@unad:~$ sudo apt dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalarán de forma automática y ya no son necesarios.
libnetplan0 python3-netifaces python3-yaml
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
linux-headers-4.15.0-124 linux-headers-4.15.0-124-generic linux-image-4.15.0-124-generic
linux-modules-4.15.0-124-generic linux-modules-extra-4.15.0-124-generic
Se actualizarán los siguientes paquetes:
linux-generic linux-headers-generic linux-image-generic
3 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 65,9 MB de archivos.
Se utilizarán 113 MB de espacio de disco adicional después de esta operación.
[Presione continuar] [5/6]
```

Imagen 4. Actualización de paquetes. Autoría propia.

Se realiza inicio de sesión para continuar con la configuración de Zentyal.



Imagen 5. Configuración inicial de Zentyal 6.2. Autoría propia.

Selección e instalación de paquetes, necesarios para realizar la gestión y administración.

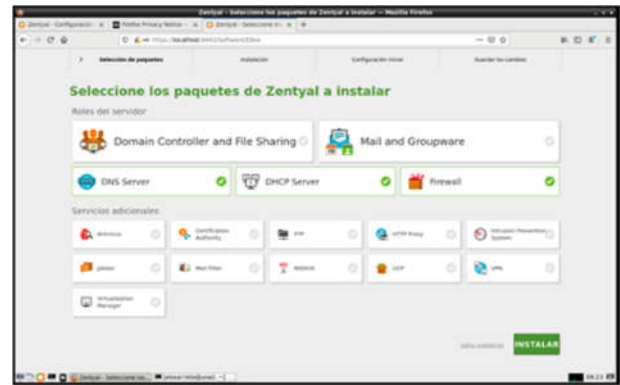


Imagen 6. Selección de módulos. Autoría propia.

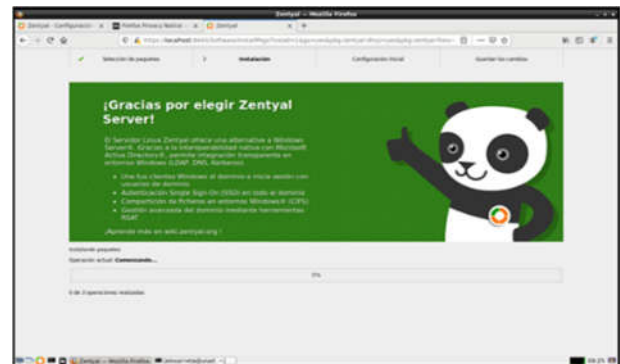


Imagen 7. Mensaje de inicio de instalación de módulos. Autoría propia.

Configuración de tarjeta de red, la Wan por DHCP y la LAN estática.



Imagen 8. Configuración para la red WAN y LAN. Autoría propia.



Imagen 9. Configuración de métodos para obtener IPs. Autoría propia.

Inicia el proceso de instalación.



Imagen 10. Mensaje de instalación completada. Autoría propia.

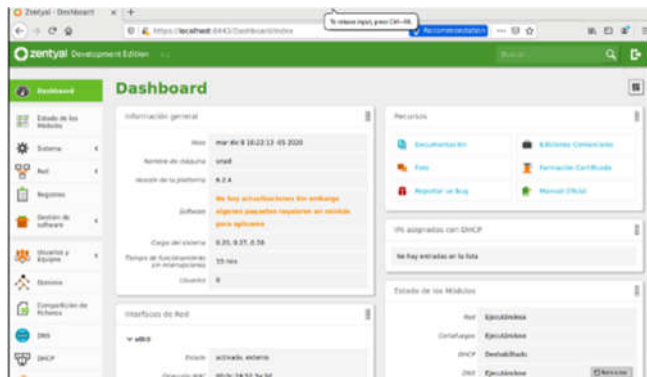


Imagen 11. Dashboard. Autoría propia.

Configuración DNS.

Ingresando al botón del panel izquierdo DNS, se habilita la opción (*habilitar el cache de DNS transparente*).

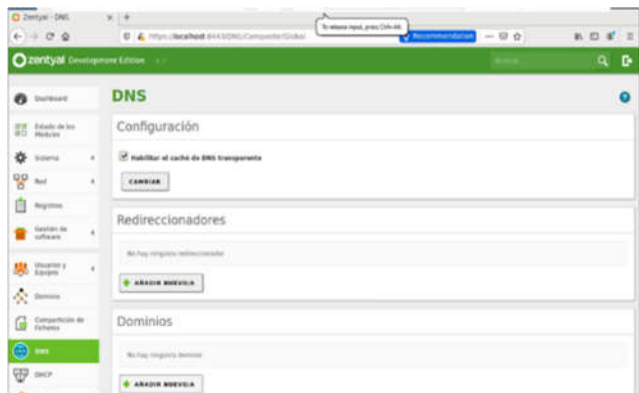


Imagen 12. Configuración DNS. Autoría propia.

Agregamos los redireccionadores (*servidores públicos DNS*).

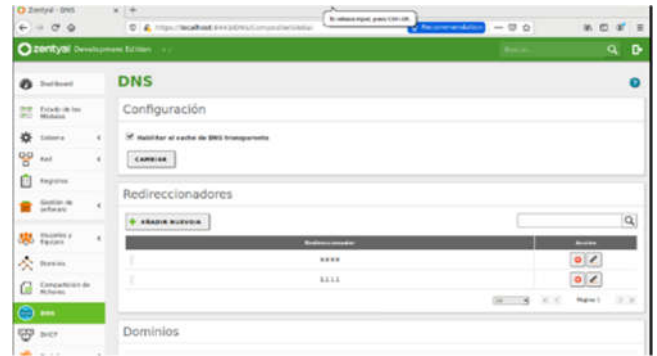


Imagen 13. Agregar redireccionadores. Autoría propia.

Configuración DNS Autoritario y Dominio

Nos dirigimos a la pestaña lateral izquierda, sistema y en su menú General, cambiamos el nombre de máquina y dominio deseado.

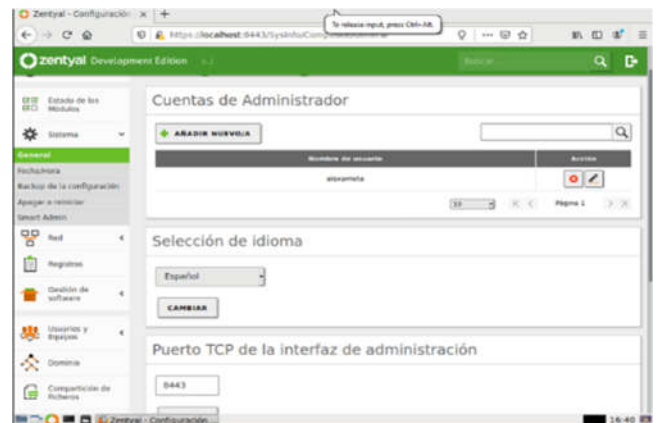


Imagen 14. Configuración DNS autoritario y dominio. Autoría propia.

Creamos el dominio.

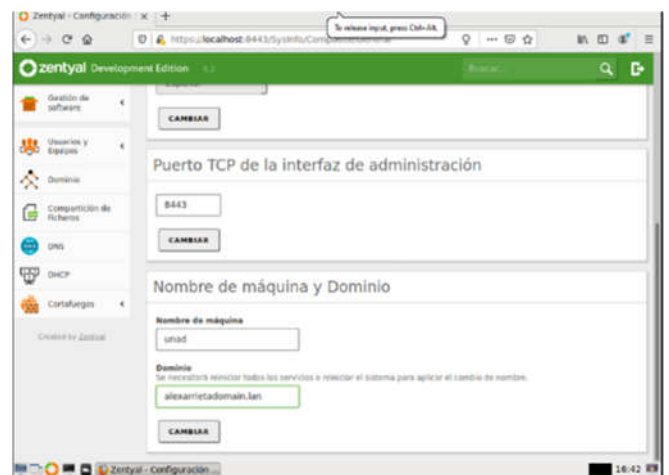


Imagen 15. Creación del dominio. Autoría propia.

Regresamos a la opción DNS, y agregamos el dominio para la red local.

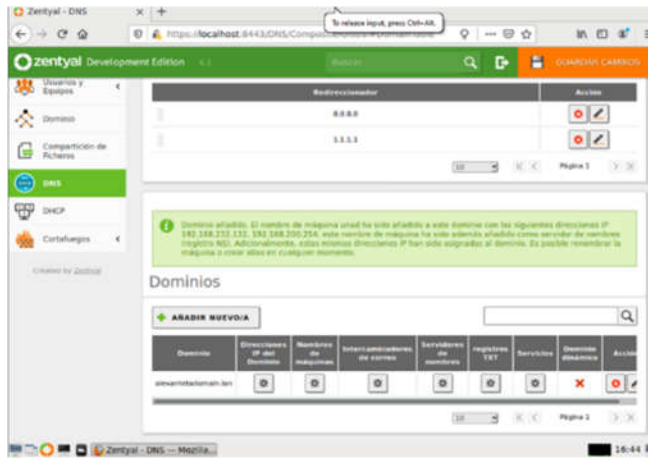


Imagen 16. Creación de dominio para red local. Autoría propia.

Validamos las direcciones IP del dominio, donde observamos, las asociadas a la red de área local y WAN.

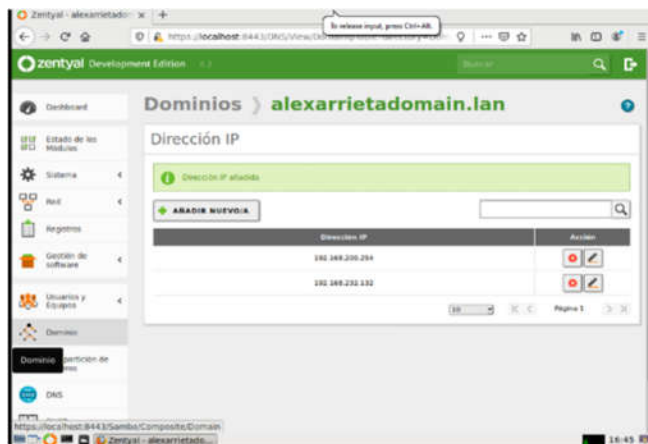


Imagen 17. Dirección IP red LAN y WAN. Autoría propia.

Configuramos el servidor DHCP, ingresando a la opción del panel derecho DHCP.

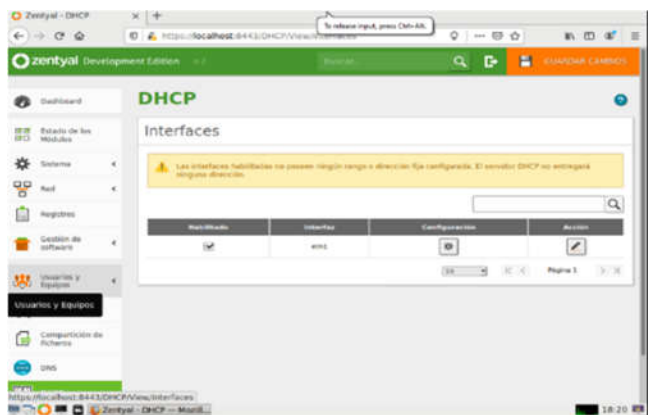


Imagen 18. Configuración servidor DHCP. Autoría propia.

Ingresamos en configuración, seleccionamos el dominio creado y guardamos los cambios.

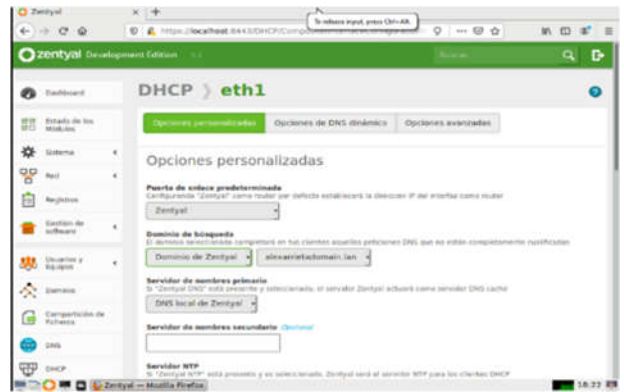


Imagen 19. Configuración del dominio creado. Autoría propia.

Configuramos los rangos de direcciones IP dinámicas, disponibles en la red LAN.

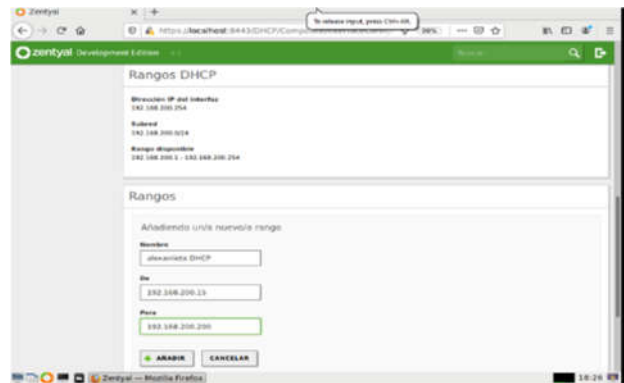


Imagen 20. Rangos de direcciones ip dinámicas. Autoría propia.

Configuramos Opciones de DNS dinámico.

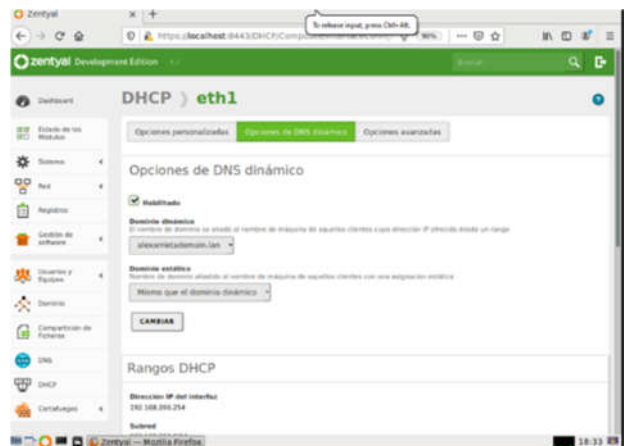


Imagen 21. Configuración DNS dinámico. Autoría propia.

Comprobación de Funcionamiento DHCP

Comprobamos mediante la opción Dashboard de servidor Zentyal, las IP asignadas con DHCP.

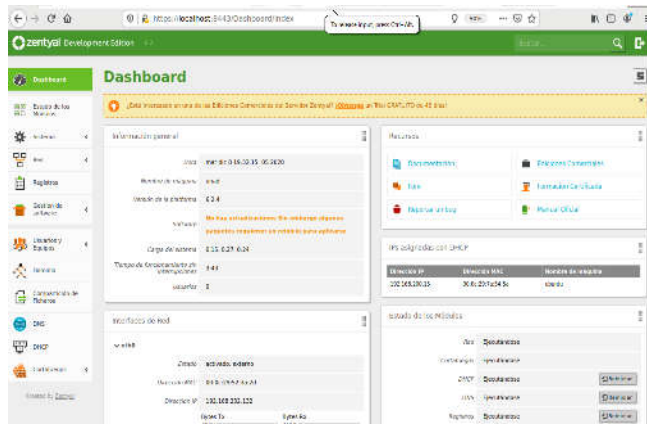


Imagen 22. IP asignada con DHCP. Autoría propia.

Configuración Controlador de Dominio

Configuramos el nombre del dominio NetBIOS, ingresando a configuración de dominio.

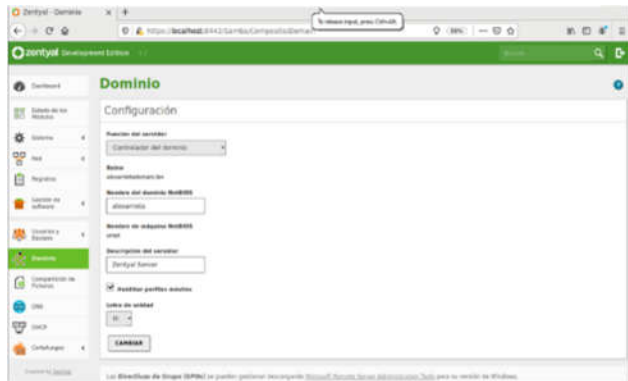


Imagen 23. Configuración de controlador de dominio. Autoría propia.

Creación de usuarios.

Para la creación de usuarios de dominio ingresamos por el botón del panel izquierdo "Usuarios y Equipos", en el menú que se despliega, ingresar a Gestionar, creamos un Grupo nombrándolo como estudiantes.

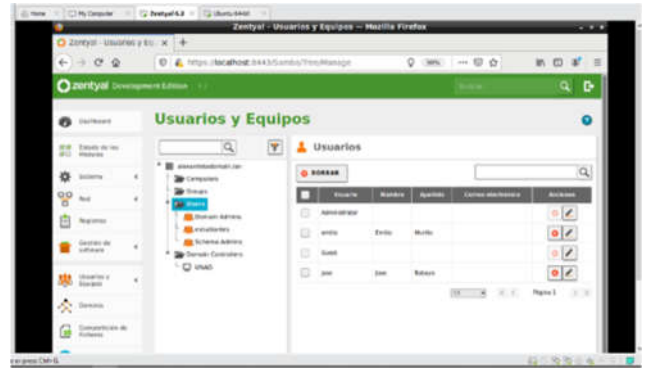


Imagen 24. Creación de usuarios. Autoría propia.

Configuración Domino para Cliente Ubuntu

Se necesita instalar la aplicación **pbis-open**, utilizando el comando **wget**, junto con el link de descarga de la aplicación pbis-open, iniciamos la descarga en la carpeta deseada.

Comando: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.7.1/pbis-open-7.1.494.linux.x86_64.deb.sh`

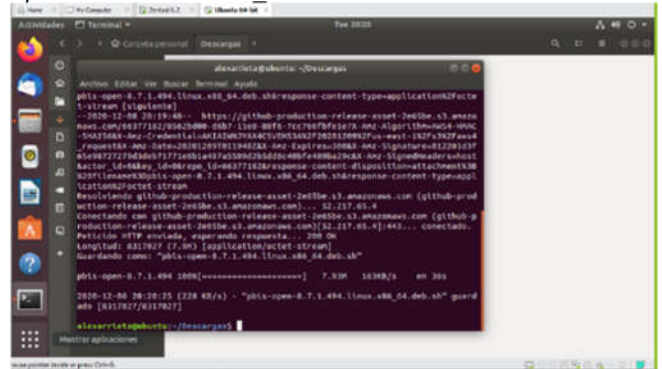


Imagen 25. Comando instalación pbis-open. Autoría propia.

Otorgamos todos los permisos al archivo con el comando: `sudo chmod 777 pbis-open-7.1.494.linux.x86_64.deb.sh`

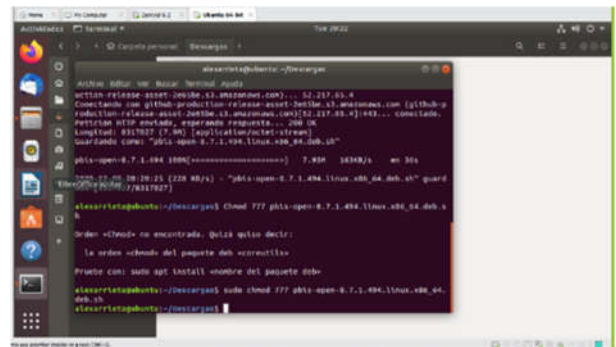


Imagen 26. Permisos instalación pbis-open. Autoría propia.

Realizamos el proceso de descompresión e instalación de la aplicación pbis, ejecutando el comando: `sudo ./pbis-open-8.7.1.494.linux.x86_64.deb.sh`

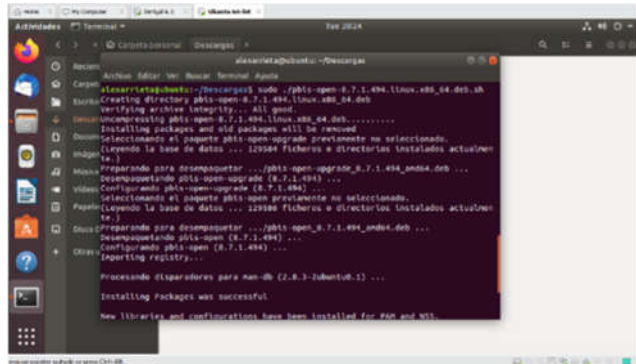


Imagen 27. Proceso de instalación. Autoría propia.

Para realizar la unión del equipo por primera vez, es necesario ingresar como usuario Administrador, ejecutando el comando: `/opt/pbis/bin/domainjoin-cli join alexarrietadomain.lan Administrator`

El primer parámetro, luego de la sentencia join, debe ser el dominio, el ultimo parámetro es el nombre de un usuario administrador.

Ingresamos como usuario administrador al dominio alexarrietadomain.lan, luego de ingresar la contraseña.

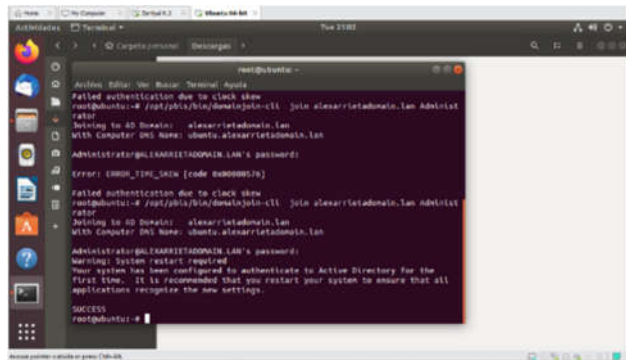


Imagen 28. Unión del equipo. Autoría propia.

Para poder iniciar sesión, desde la pantalla de inicio con los usuarios creados de el dominio, es necesario modificar el archivo de configuración 50-ubuntu.conf, ejecutando con el comando: `nano /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf`, agregando la línea: `greeter-show-manual-login=true`

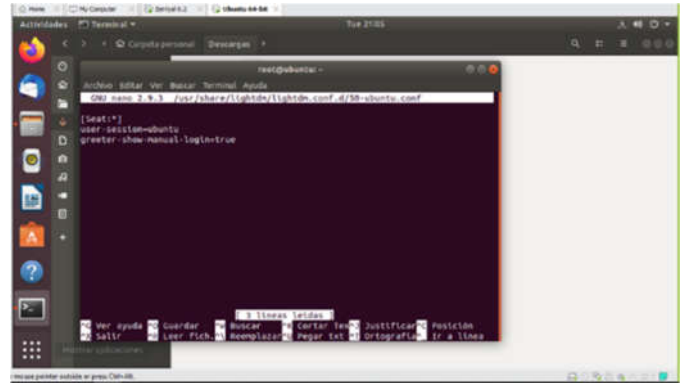


Imagen 29. Configuración de usuarios. Autoría propia.

Para comprobar el login con usuario del grupo Estudiante, se debe combinar el nombre de usuario y el dominio, como: `username@domain`.

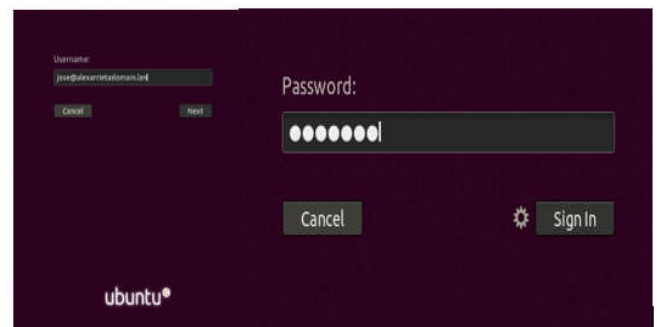


Imagen 30. Inicio de sesión nuevo usuario. Autoría propia.

2.2 Temática 2: Proxy no transparente.

Temática desarrollada por el estudiante Jhon Freddy Maldonado Gómez.

Se realiza inicio de sesión, para continuar con la configuración de Zentyal.

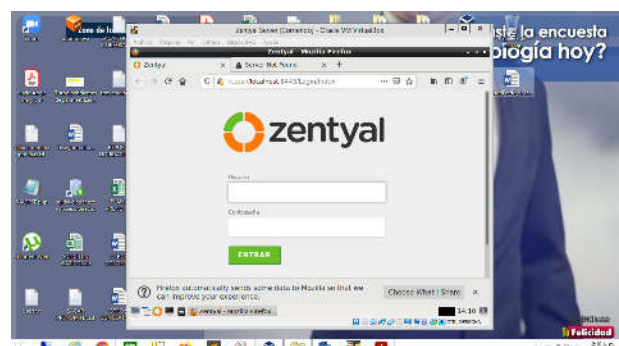


Imagen 31. Ingreso menú Zentyal. Autoría propia

Se inicia la configuración inicial de Zentyal.



Imagen 3321. Configuración Inicial. Autoría propia

Selecciono los paquetes a instalar, necesarios para la temática a desarrollar.

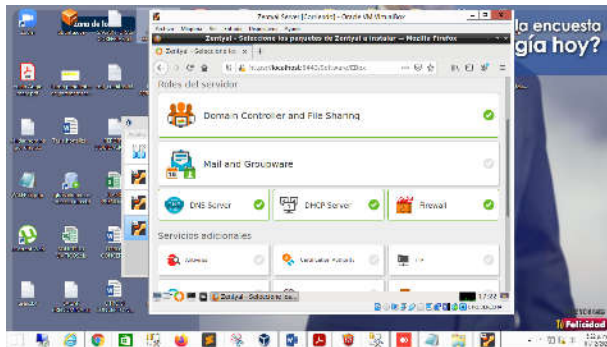


Imagen 3332. Selección de paquetes. Autoría propia.

Se visualiza los paquetes a instalar, acorde a la selección del paso anterior.

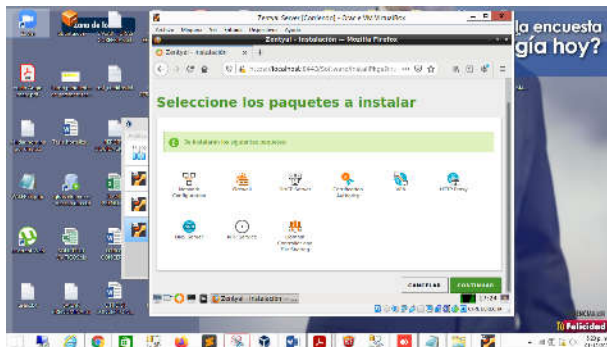


Imagen 3433. Lista Seleccionada. Autoría propia.

Inicializa el proceso de instalación de los paquetes.

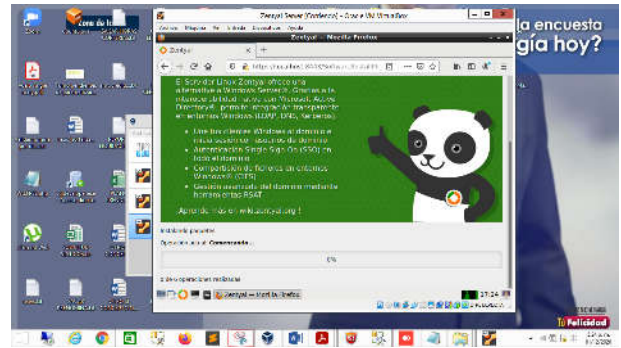


Imagen 3534. Inicio de instalación. Autoría propia.

Configuro las interfaces de red.

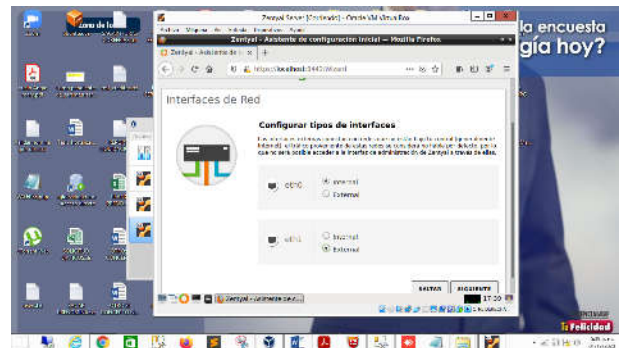


Imagen 3635. Configuración red. Autoría propia

Configuro las tarjetas de red, Wan por DHCP y la LAN estática.

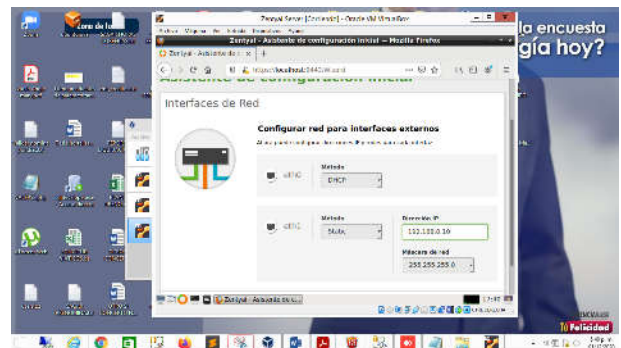


Imagen 3736. Configuración red Lan Wan. Autoría propia.

Configuro el nombre de dominio del servidor.

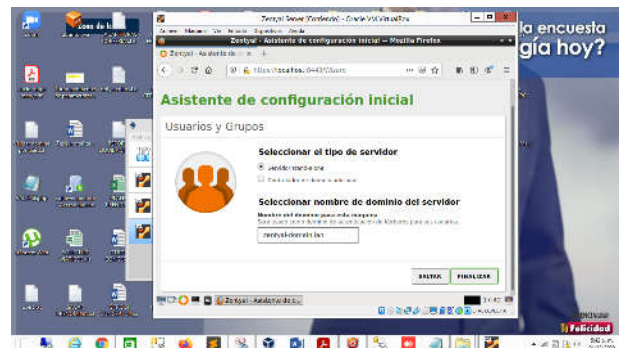


Imagen 3837. Configuración Dominio Autoría propia

Inicia proceso de instalación y mensaje de Instalación completa.

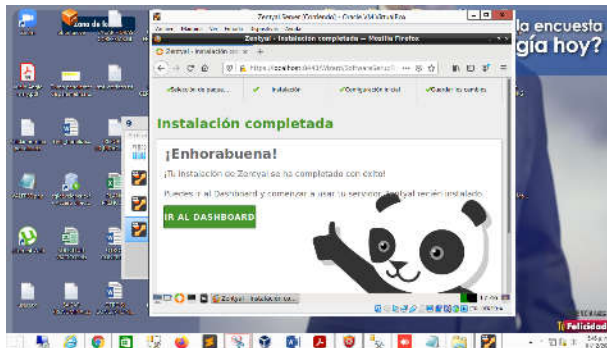


Imagen 3938. Mensaje final instalación. Autoría propia.

Para la práctica configuro dos tarjetas de red, primero la NAT por DHCP.

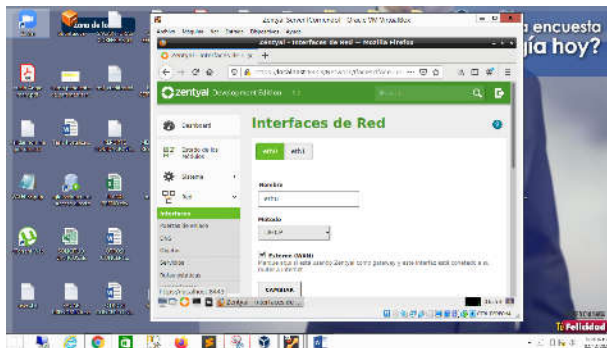


Imagen 4039. Configuración tarjetas de red Nat. Autoría propia

La otra tarjeta de red la configuro con red interna, para poder comunicarme con los usuarios de las otras máquinas virtuales.

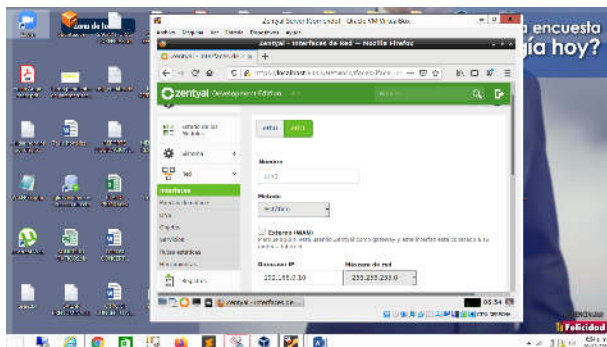


Imagen 4140. Configuración tarjeta de red interna. Autoría propia

Creo un objeto de red.

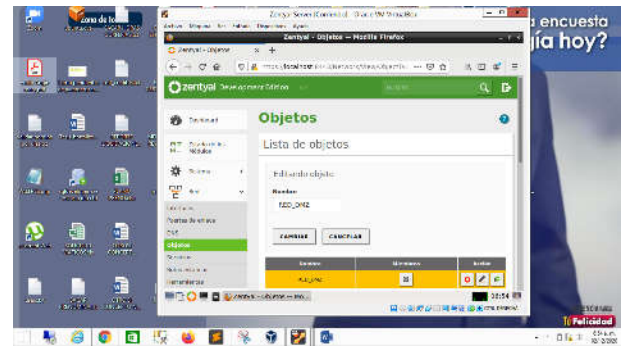


Imagen 4241. Creación de objeto. Autoría propia

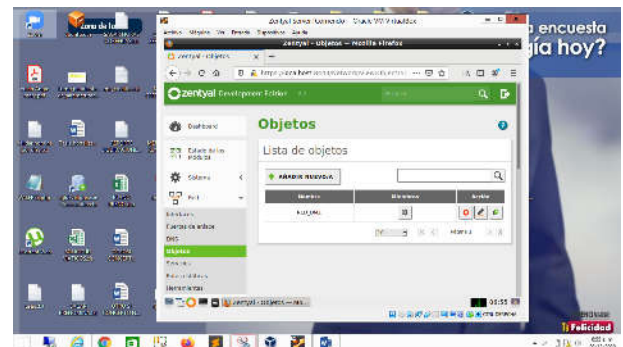


Imagen 4342. Lista Objetos creados. Autoría propia.

Creo un nuevo miembro para el objeto de red, para el desktop que se va conectar.

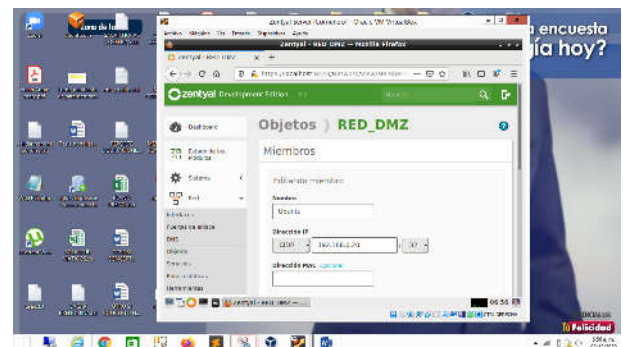


Imagen 4443. Creación miembro para el objeto creado. Autoría propia.

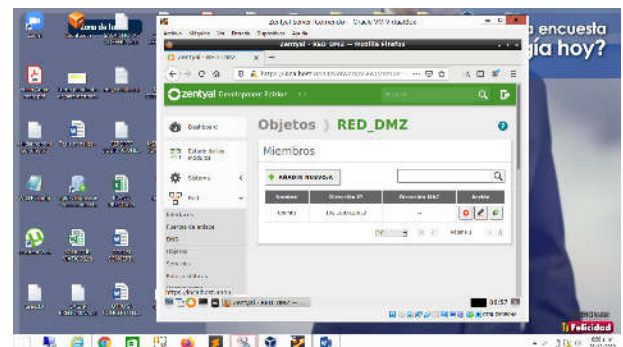


Imagen 45. Lista Objeto creado. Autoría propia.

En la pestaña de HTTP Proxy, se configura el servidor y se indica que este no va a ser transparente, desmarcando la casilla correspondiente y configurando el puerto 1230.

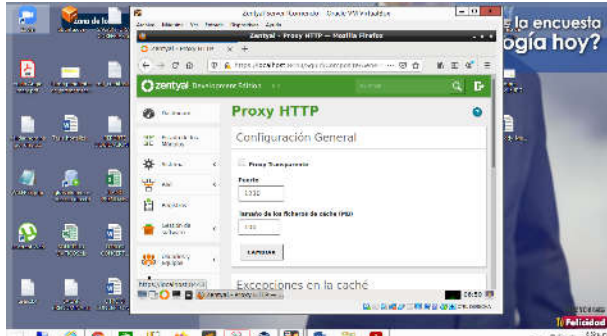


Imagen 46. Creación Proxy transparente. Autoría propia

Configuro la regla de acceso para el objeto previamente creado, donde se deniega todas las peticiones.

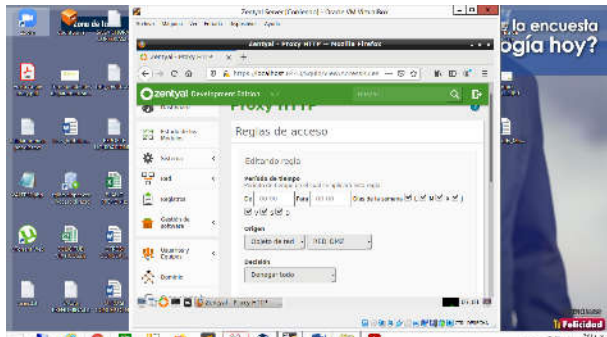


Imagen 47. Configuración reglas de acceso. Autoría propia

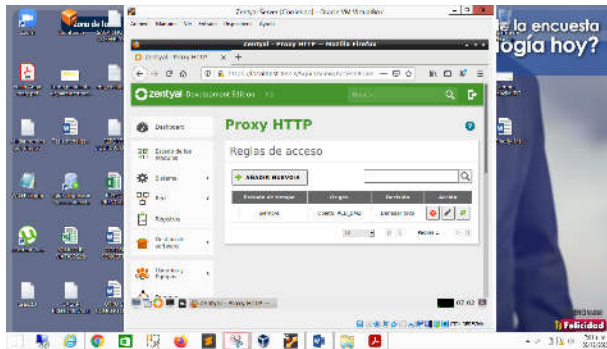


Imagen 48. Regla acceso creado. Autoría propia

Evidencio el resumen Dashboard, visualizando las IP, servicios activos, conexión del desktop por DHCP con el servidor.

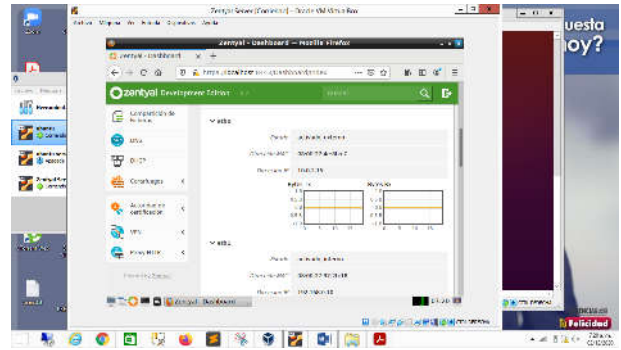


Imagen 49. Resumen de la Dashboard. Autoría propia

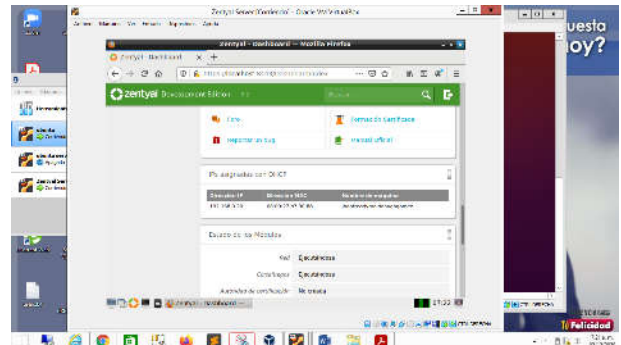


Imagen 50. IP configurada por DHCP. Autoría propia

Se valida la IP, Asignada por DHCP por el servidor, al desktop.

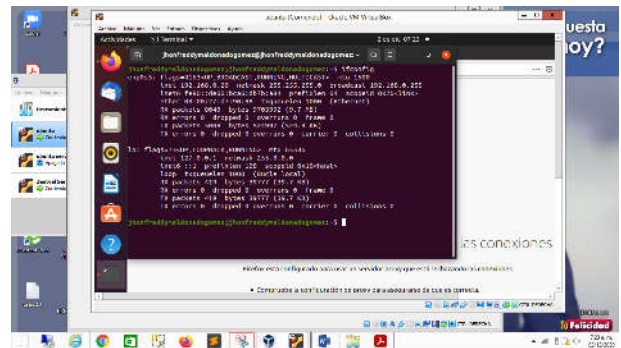


Imagen 51. Ip Equipo Desktop. Autoría propia.

Procedo a configurar el Cliente Ubuntu, ingresando al navegador Mozilla, menú Preferencias, General, Servidor Proxy y realizo configuración manual con la información de IP de Zentyal Server 192.168.0.10 y el puerto 1230.

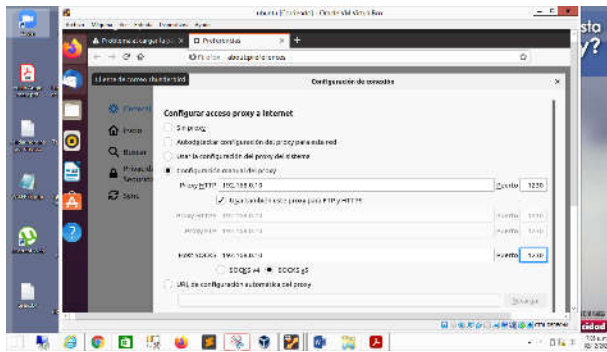


Imagen 52. Configuración Proxy equipo desktop. Autoría propia

Se ingresa al navegador para acceder a una página web, evidenciando que el proxy no permite la navegación.

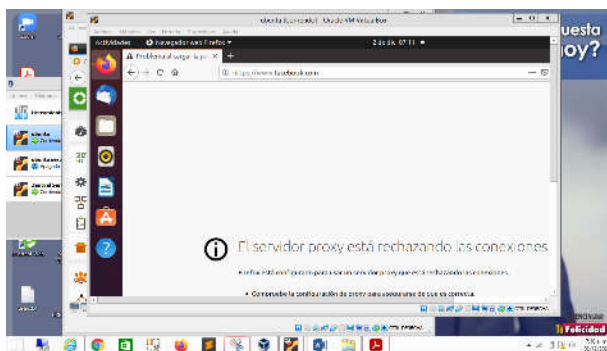


Imagen 53. Funcionamiento regla Proxy. Autoría propia.

2.3 Temática 3: Cortafuegos

Temática desarrollada por el estudiante Christian Camilo Gómez Bautista.

Una vez configurado e instalado Zentyal, se deben seleccionar los módulos que se requieren para la puesta en marcha del servicio y solución a desarrollar. Para esta temática (*corta fuegos*), se deben instalar los servicios del cortafuego (Firewall) y para facilidad de comunicación del host cliente con el servidor, y para garantizar de cierta manera que el tráfico de los equipos clientes pase por el firewall se cargan en este mismo servidor los servicios de DHCP.



Imagen 54. Selección de módulos de Zentyal, ilustración propia.

Una vez finalizada la instalación de los paquetes necesarios para trabajar, Zentyal nos pide dar configuración a las tarjetas o interfaces de red, en este caso, como se había explicado anteriormente, la interfaz eth1 va a ser nuestra zona roja, lo que en Zentyal sería una tarjeta de red externa, y la interfaz eth0 va a ser nuestra zona verde o nuestra red interna, para lo cual Zentyal la llama red interna. Seguido de esto, el asistente de configuración nos va a solicitar el método de direccionamiento de las dos interfaces de red. En este caso para la red interna vamos a utilizar la dirección de red 192.168.20.0/24



Imagen 55. Configuración de interfaces Zentyal, ilustración propia.

Al finalizar la configuración, se empieza aplicar los cambios, e instalar los módulos y dependencias necesarias, para poder acceder al dashboard de Zentyal, para iniciar la administración:

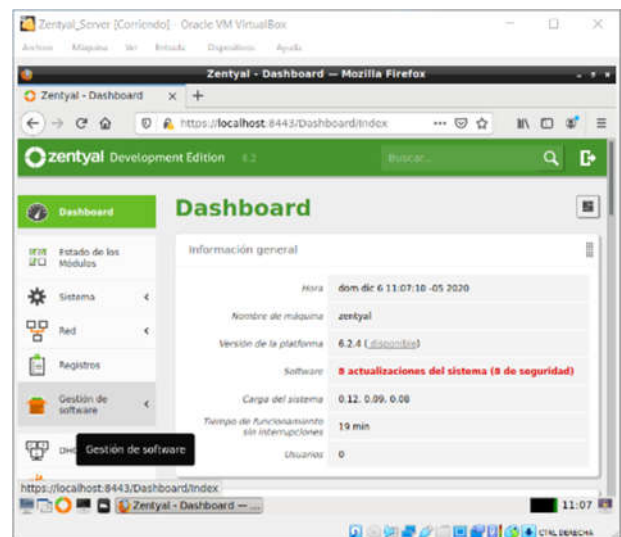


Imagen 56. Dashboard Zentyal 6.2, ilustración propia.

Una vez realizadas las configuraciones revisamos el servicio DHCP, configuremos un rango de direcciones IP para entregar, de la siguiente manera:

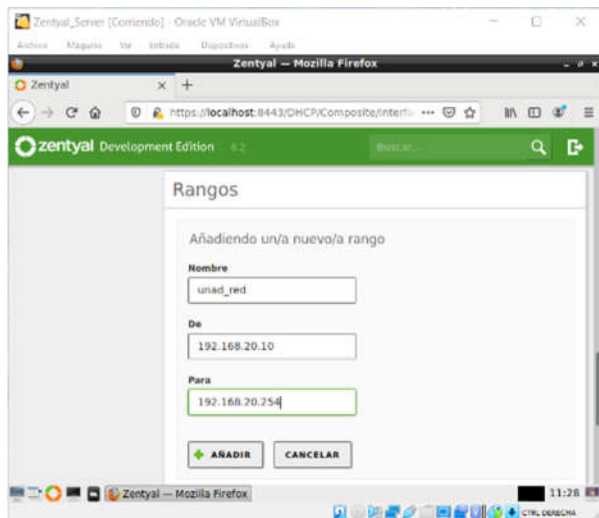


Imagen 5744. Configuración de rango de direccionamiento servidor DHCP. Ilustración propia.

Una vez realizada esta configuración, se procede a realizar el encendido del equipo cliente, que en este caso es una máquina virtual con sistema operativo Ubuntu Desktop. Se puede validar en el dashboard de Zentyal, que recibe asignación de direccionamiento IP por protocolo DHCP.

IPs asignadas con DHCP		
Dirección IP	Dirección MAC	Nombre de máquina
192.168.20.10	08:00:27:19:50:95	Christian

Imagen 58. Hosts conectados, con asignación de IP por DHCP. Ilustración propia.

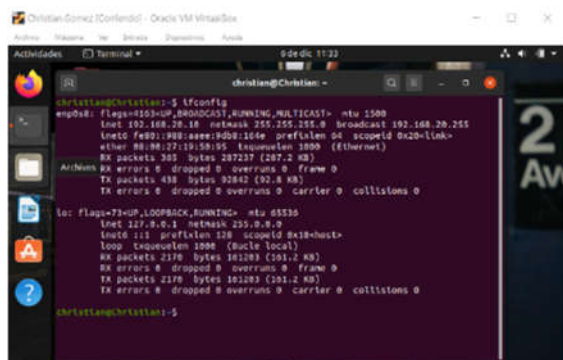


Imagen 59. Ejecución de comando ifconfig equipo cliente Ubuntu.

Ya teniendo el servidor DHCP funcionado, se comprueba que los equipos clientes están saliendo a internet por medio de nuestro servidor Zentyal.

Ingresamos a la configuración del Firewall o cortafuegos para establecer todas las políticas que se requieren configurar. Este proceso se va a realizar ingresando a la consola de administración, desde el equipo cliente Ubuntu desktop, a través del navegador web accediendo a la dirección IP que configuramos: 192.168.20.1 con el puerto 8443.

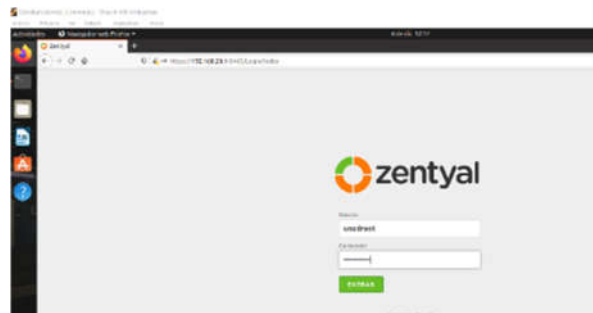
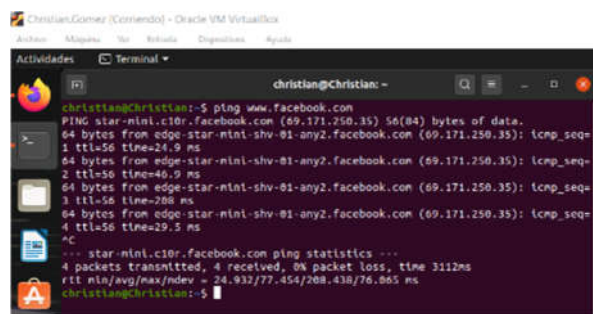


Imagen 60. Acceso a panel de administración Zentyal desde cliente Ubuntu. Ilustración propia.

Antes de crear alguna regla de bloqueo de páginas, es necesario lograr establecer cuál es la dirección IP de cada una de ellas, para esto, solo basta con realizar un ping a la página que queremos bloquear desde terminal y así obtener su dirección, como se muestra en la siguiente imagen:



Como se puede observar, se logra determinar que la dirección IP de los servidores de Facebook es: 69.171.250.35, este ejercicio se repite con todas las páginas que se desean bloquear generando los siguientes resultados:

Tabla 1. Direcciones IP de páginas a bloquear. Tabla propia.

Sitio	Dirección IP	Categoría
Facebook	/	Red social
Instagram		
Twitter	104.244.40.0/21	Red Social
ESPN	13.224.0.0/14	Entretenimiento
Yahoo	74.6.0.0/16	Entretenimiento

Una vez tenemos definidos los sitios y direcciones que se van a bloquear, procedemos a configurar las reglas de bloqueo de los mismos por el cortafuego de Zentyal, Para esto entramos a la sección de cortafuegos, filtrado de paquetes, reglas de filtrado para redes internas:



Imagen 61. Panel de filtrados, Zentyal Server. Ilustración propia.

Adicionamos la primera regla, en este caso Facebook e Instagram que comparten las direcciones IP.

En la decisión, seleccionamos denegar dado que lo que se va hacer es bloquear el tráfico en origen cualquiera, ya que esta regla va a aplicar a cualquiera de los equipos de la red de la zona verde, en destino ponemos la IP del servicio a bloquear, en servicio seleccionamos cualquiera, ya que vamos a bloquear completamente cualquier tráfico o servicio a esta IP por ejemplo el ping, (ICMP) la navegación HTTPS, HTTP, y todos los demás que existan.



Imagen 62. Panel de administración de reglas de filtrados cortafuegos Zentyal. Ilustración propia.

Se añade la regla y se guardan los cambios, el mismo procedimiento se repite en las demás direcciones IP que se van a bloquear según la tabla 1.

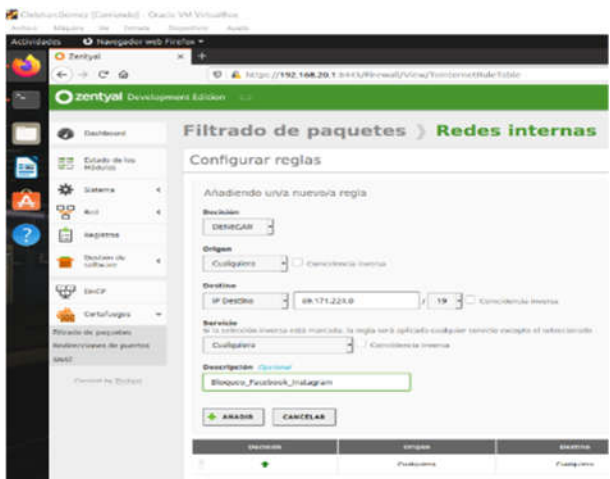


Imagen 62. Creación de regla de bloqueo Facebook e Instagram. Ilustración propia.

Como el objetivo es realizar el bloqueo a las diferentes páginas, el proceso se repite para cada una de las

direcciones IP, este es el resultado de todas las reglas creadas, configuradas y activas en el cortafuego:

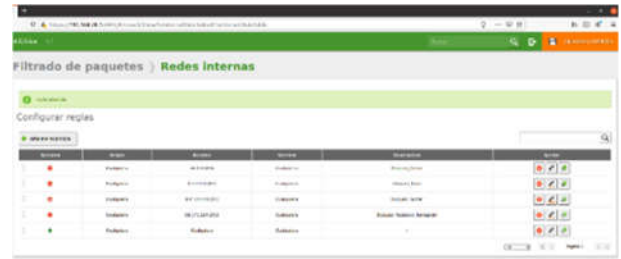


Imagen 63. Reglas de filtrado creadas, panel cortafuegos Zentyal 6.2. Ilustración propia.

Una vez configuradas y activadas las reglas en el cortafuego, se deben realizar las respectivas validaciones en el equipo cliente para comprobar que el servidor está aplicando las reglas. Como se puede observar la navegación a estas páginas web está bloqueada.



Imagen 64. Navegación a Facebook bloqueada, equipo cliente Ubuntu. Ilustración Propia.

Realizamos una petición ICMP o un ping no a la dirección IP sino al dominio facebook.com evidenciando el siguiente resultado:

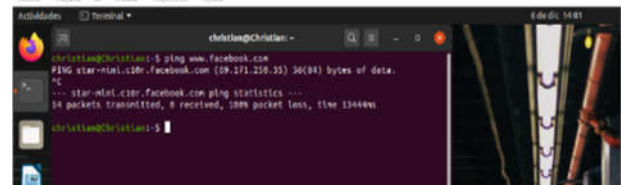


Imagen 65. Petición ICMP PING Facebook, host Ubuntu. Ilustración propia.

Como podemos evidenciar, la navegación web como las peticiones de ping y cualquier tipo de conexión se encuentran bloqueadas a estas direcciones IP, ya que el cortafuego de Zentyal está ejecutando las reglas de filtrado web sobre este host.

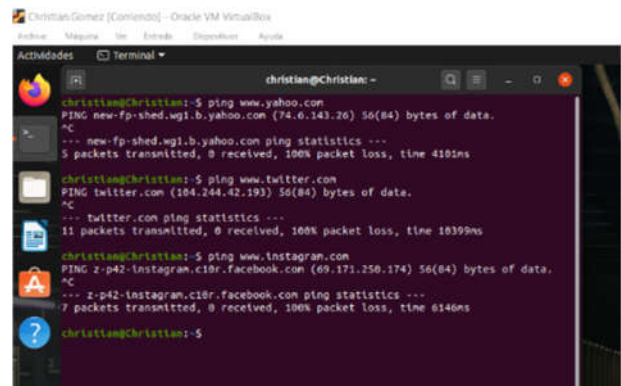


Imagen 66. Petición ICMP PING a las páginas bloqueada, Ilustración Propia.

2.4 Temática 4: File Server y Print Server

2.5 Temática 4: VPN

Temática desarrollada por el estudiante, Jesús David Cortés Ariza

Ir a la opción vpn, para crear la autoridad de certificación, luego vamos a vpn y servidores.

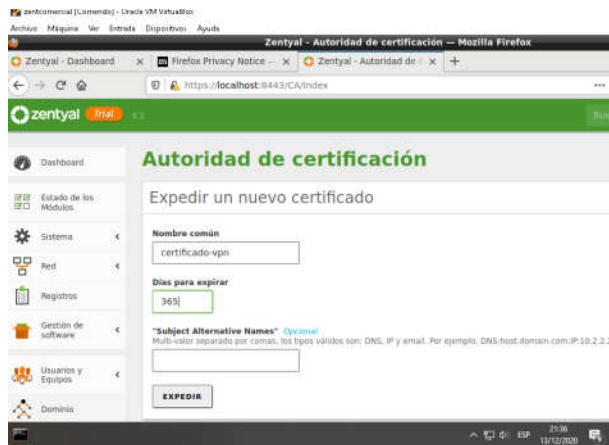


Imagen 67 Petición ICMP PING a las páginas bloqueada, Ilustración Propia.

Ir a VPN, servidores y añadir nuevo.

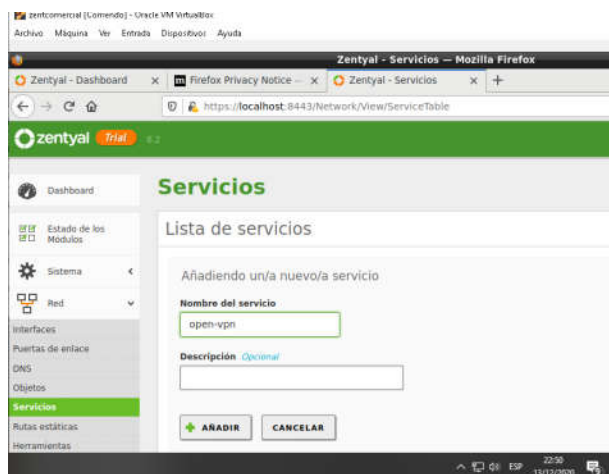


Imagen 68 Creación de servidor vpn. Ilustración Propia.

Volvemos a vpn en engrane de configuración, dejamos el puerto 1194 habilitamos interfaz TUN.



Imagen 69. Configuración del servidor. Ilustración Propia.

Ir a cortafuegos, filtrado de paquetes, en redes internas a Zentyal, añadir.

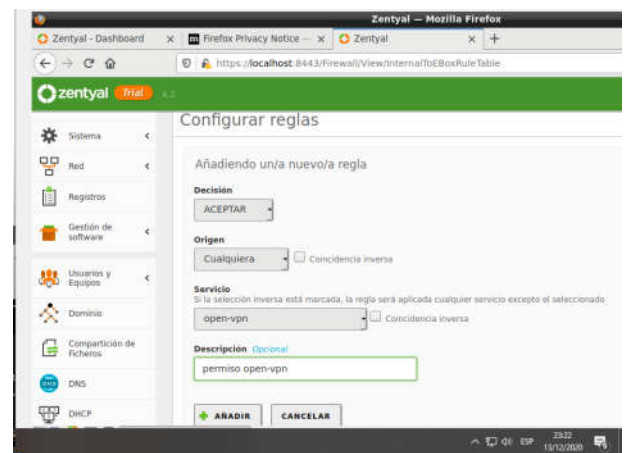


Imagen 70. Configuración del cortafuego. Ilustración Propia.

Ir a vpn, servidores, redes anunciadas, añadir nuevo.

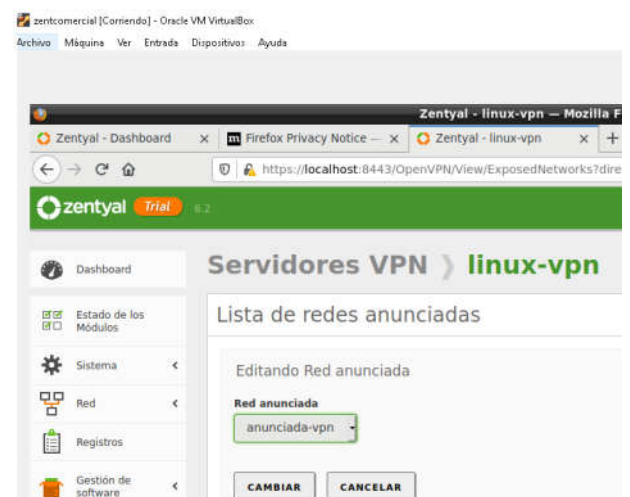


Imagen 71. Selección de servidor vpn. Ilustración Propia.

Ir vpn, servidores, descargar paquete configuración, ip publica del Zentyal, se puede buscar por internet o en el router, la dirección adicional del servidor puede ser puesta si difiere de la de Zentyal.

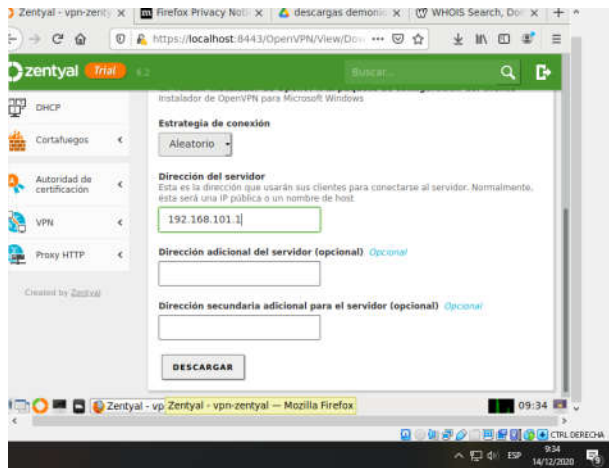


Imagen 72. Parámetros antes de descargar el client.ovpn que permite la conexión. Ilustración Propia.

Ir al Dashboard y verificar en “demonios”.

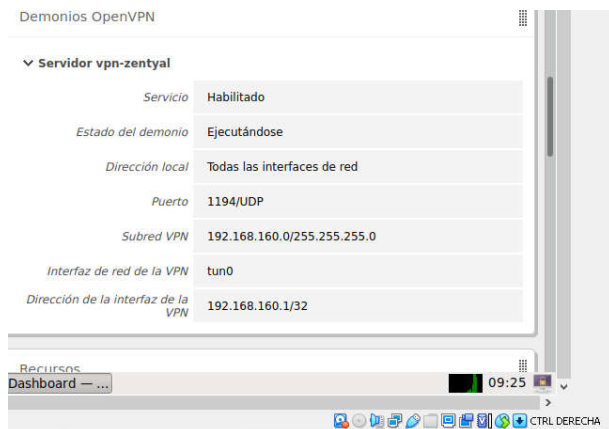


Imagen 73. Verificación de la ejecución de la red vpn TUN. Ilustración Propia.

Migrar la descarga a Windows, descargando Opvclient desde <https://openvpn.net/client-connect-vpn-for-windows/> se busca en file, browser el archivo conector.

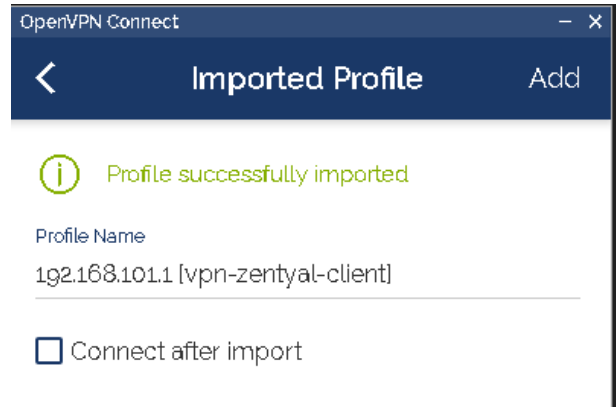


Imagen 74. Selección de archivo vpn. Ilustración Propia.

Dar clic en la parte superior derecha en add y conectar.

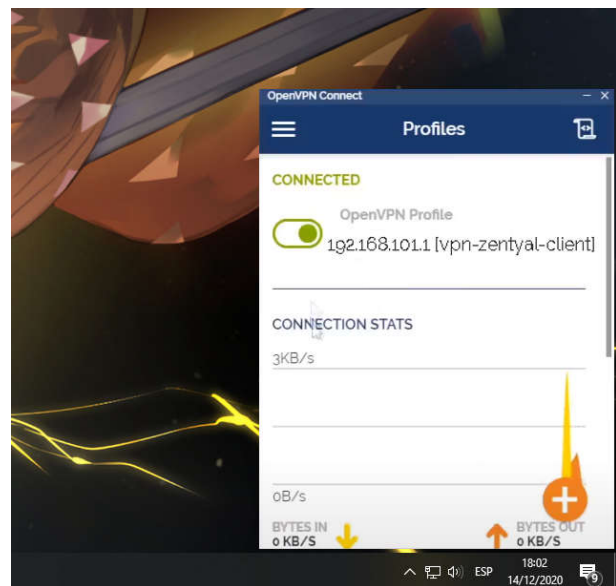


Imagen 75. Verificación de conexión. Ilustración Propia.

3 CONCLUSIONES

Se llevó acabo la instalación del sistema operativo Zentyal 6.2, documentado el paso a paso en su procedimiento de configuración. Comprendiendo la importancia de identificar correctamente las interfaces de red para su adecuada conexión a la red externa “WAN” o interna “LAN”, la configuración de los módulos de red, “DHCP”, “DNS”, “NTC” y controlador de dominio.

Con el desarrollo de esta actividad se logró 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.

Se creó de manera efectiva las reglas de filtrado web logrando realizar el bloqueo de diferentes páginas según

su clasificación, (*redes sociales, entretenimiento*) por medio de la dirección IP del servidor de destino de cada una de ellas.

4 REFERENCIAS

[1] Zentyal 6.2 Documentación Oficial — Documentación de Zentyal 6.2. (s. f.). Zentyal Community. <https://doc.zentyal.org/es/>

[2] ValorTop S.L. (2014-2018). ¿Qué es un proxy o servidor proxy?. Recuperado de <http://www.valortop.com/blog/servidor-proxy>.

[3] Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN. (2015). recuperado de: <https://www.youtube.com/watch?v=3rNfipxE-9o>