INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL SERVER, PARA LA IMPLEMENTACIÓN DE SERVICIOS DE RED DHCP SERVER, DNS SERVER, CONTROLADOR DE DOMINIO, PROXY NO TRANSPARENTE, CORTAFUEGOS, FILE SERVER, PRINT SERVER Y VPN.

Integrante 1: Arnol Didier Ariza
e-mail: adariza@unadvirtual.edu.co
Integrante 2: Sonia Patricia Espitia Pineda
e-mail: spespitiap@unadvirtual.edu.com
Integrante 3: Luis Iván Zapata Parada
e-mail: luisivanzapatap@gmail.com
Integrante 4: Nidia Mayerly Varela
e-mail: nmvarelat@unadvirtual.edu.co
Integrante 5: July Maribel Rodríguez Martínez
e-mail: ymrodriguezmar@unadvirtual.edu.co

RESUMEN: Mediante *este artículo se busca evidenciar la instalación, configuración y puesta en marcha con GNU/Linux Zentyal Server conforme a las exigencias en los servicios de red en la Infraestructura IT para el proceso integral de migración y capacitación de la infraestructura tecnológica en la empresa Internacional Proveedores de Servicios de Internet ISP. Demuestra la implementación y ejecución detallada de los servicios de gestión de red DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.*

PALABRAS CLAVE: Cortafuegos, proxy no transparente, DHCP, File Server, Print Server y Zentyal Server.

1. INTRODUCCIÓN

Por medio de este trabajo se busca que cada estudiante tenga la orientación pertinente sobre la administración y control de una distribución GNU/Linux basada en Ubuntu, pero enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas.

2. INSTALACIÓN DE ZENTYAL

2.1. REQUISITOS

8 gb de disco duro, 2 gb de RAM, configurar dos tarjetas de red para la implementación de una red interna y otra externa.

2.2. PROCESO DE INSTALACIÓN

Iniciamos la máquina y elegimos el idioma español.

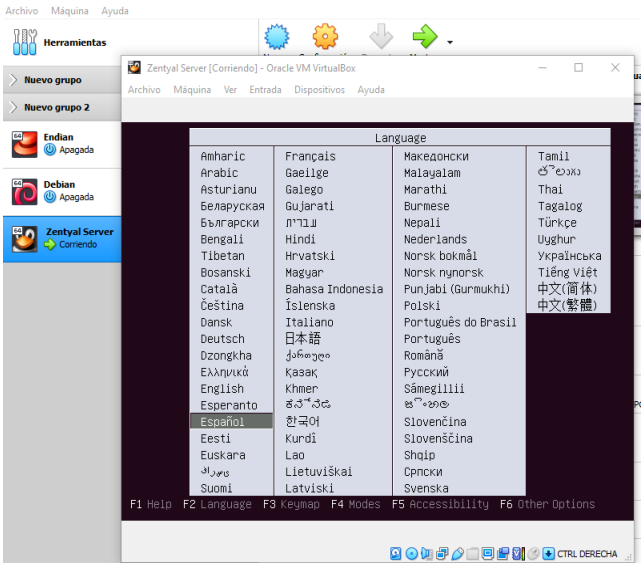

Imagen 1. Selección de idioma

Elegimos la primera opción (borrar todo el disco)

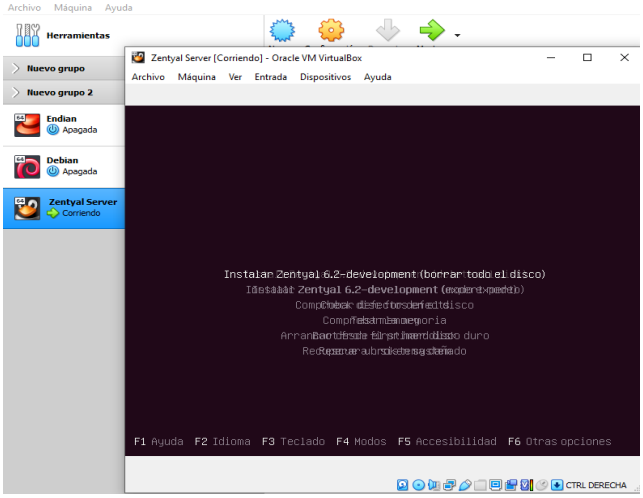

Imagen 2. Menú de instalación Zentyal.

Seleccionamos nuestra ubicación

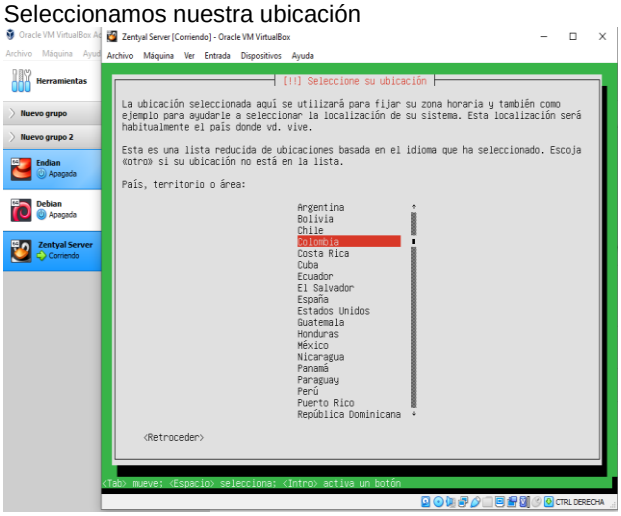

Imagen 3. selección de ubicación

Elegimos el idioma del teclado

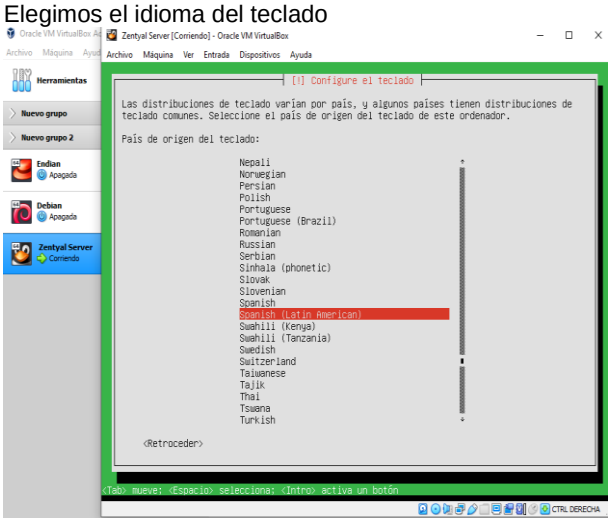

Imagen 4. Selección idioma del teclado.

Seleccionamos la distribución del teclado

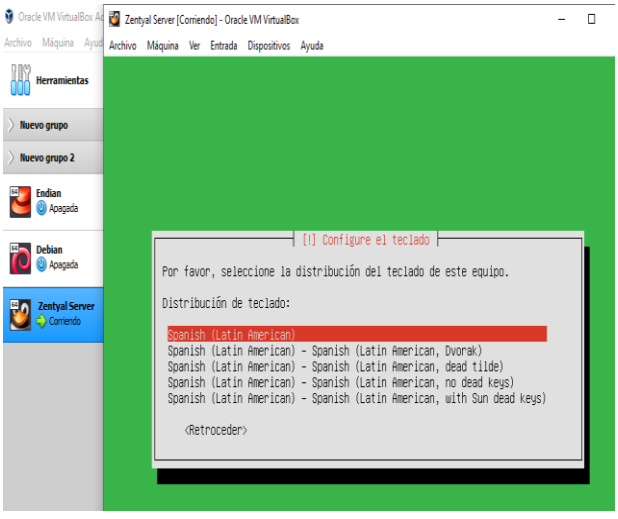

Imagen 5, selección distribución del teclado.

Se elige un nombre para la máquina

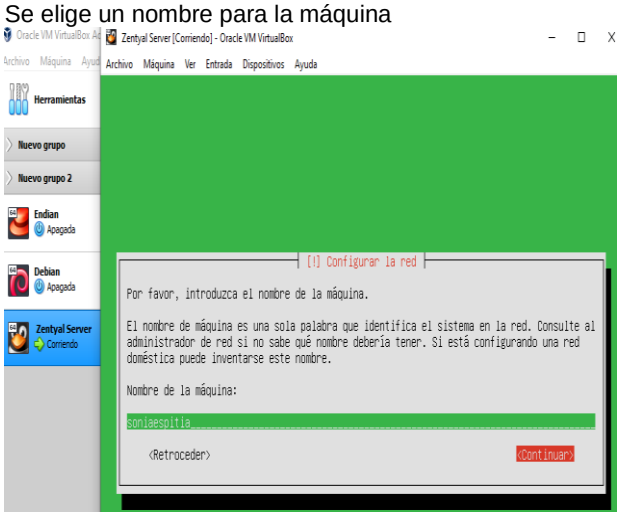

Imagen 6. Asignación nombre de la máquina

Se le asigna una contraseña a la máquina

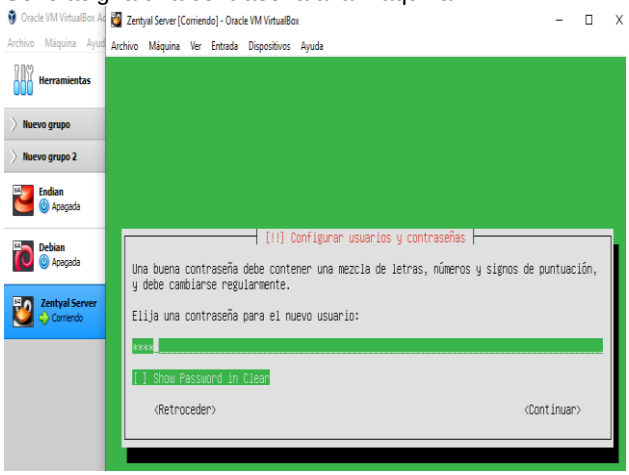

Imagen 7. Asignación contraseña

Damos clic en sí para confirmar la zona horaria.

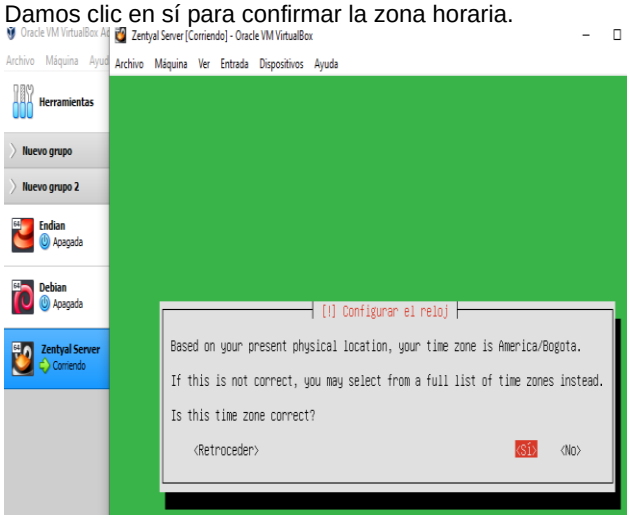

Imagen 8. Confirmación zona horaria.

Se descargan algunos programas.

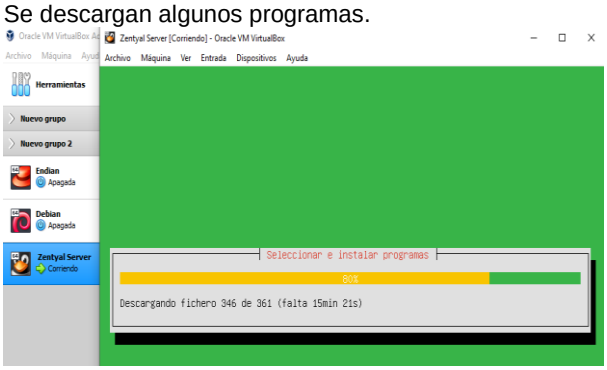

Imagen 9. Descargue de programas.

Se completa la instalación, continuamos.

Imagen 10. Se completa la instalación

Inicio de Zentyal.

Imagen 11. Inicio de Zentyal.

Iniciamos sesión.

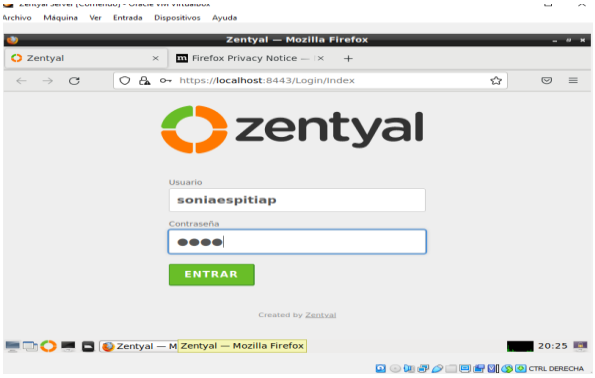

Imagen 12. Inicio de sesión en Zentyal.

Iniciamos la configuración inicial, damos clic en continuar.

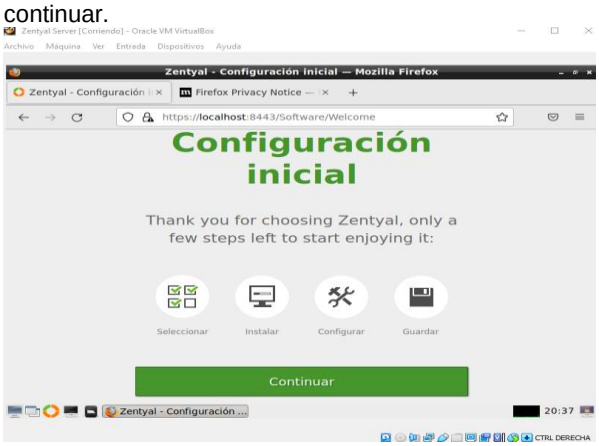

Imagen 12. Configuración inicial

Seleccionamos los paquetes a instalar.

Imagen 13. Selección de paquetes a instalar.

Se muestra en pantalla los paquetes que serán instalados, continuamos.

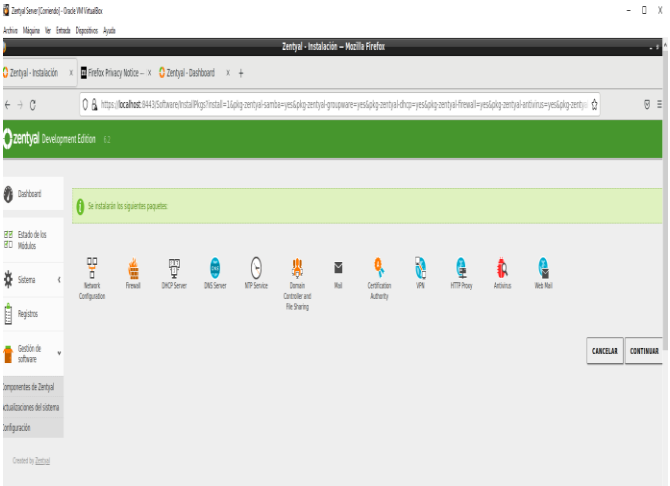

imagen 14. Instalación de paquetes.

Confirmación de instalación de los paquetes.

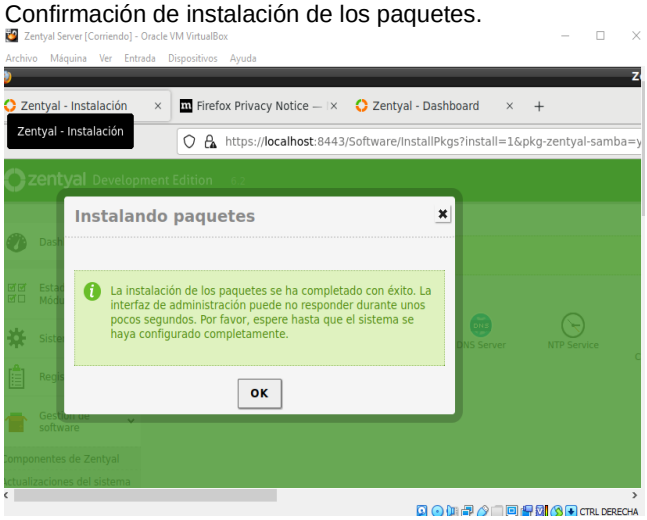

Imagen 15. Confirmación de instalación de paquetes.

Se realiza la configuración inicial, se configura el eth0

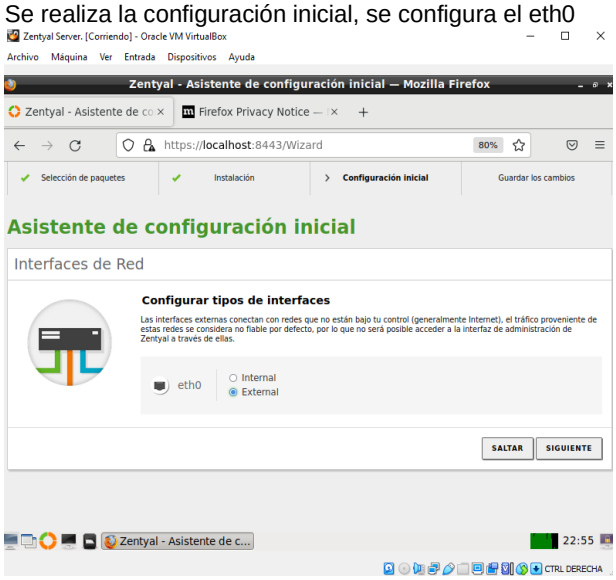

Imagen 16. Configuración de interfaces.

Dejamos eth0 en DHCP

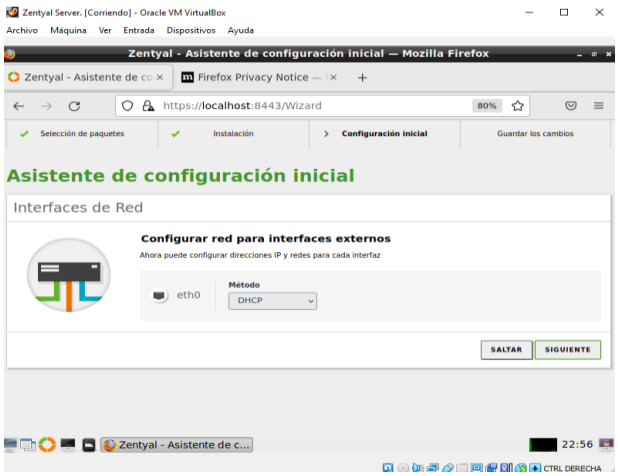

Imagen 17. Configuración eth0

Finaliza la instalación

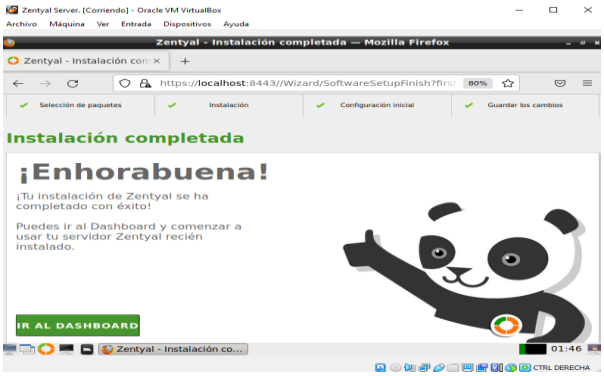

Imagen 18. Instalación completada.

Ingresamos al Dashboard.

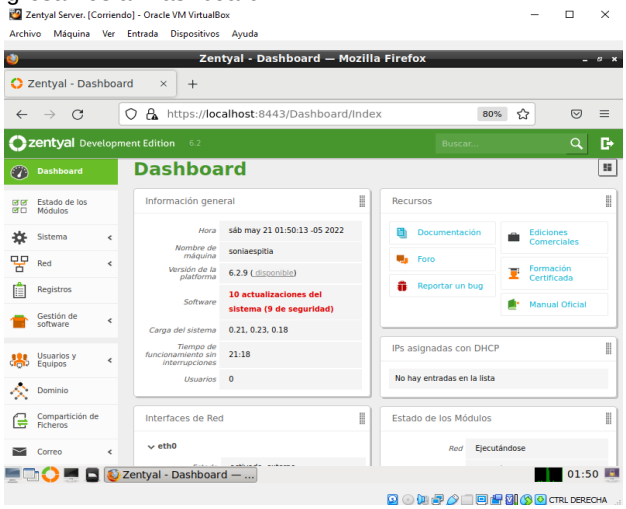

Imagen 19. Dashboard Zentyal.

3. DESARROLLO

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

Primero que todo debemos realizar la instalación de los servicios que necesitamos, en este caso dhcp server, DNS, domain controller y network configuración.

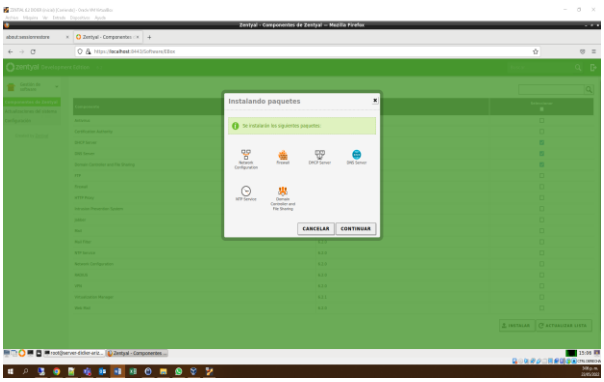

Imagen 20. Selección de paquetes a instalar.
Esperamos la descarga e instalación:

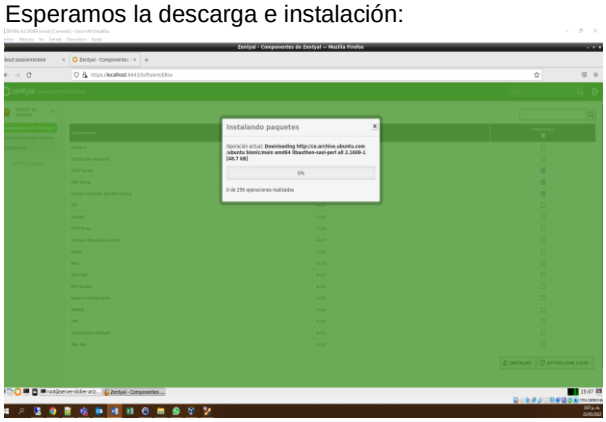

Imagen 21. Descarga de paquetes.

Confirmamos su instalación exitosa, evidenciando los módulos ya instalados sobre el Zentyal:

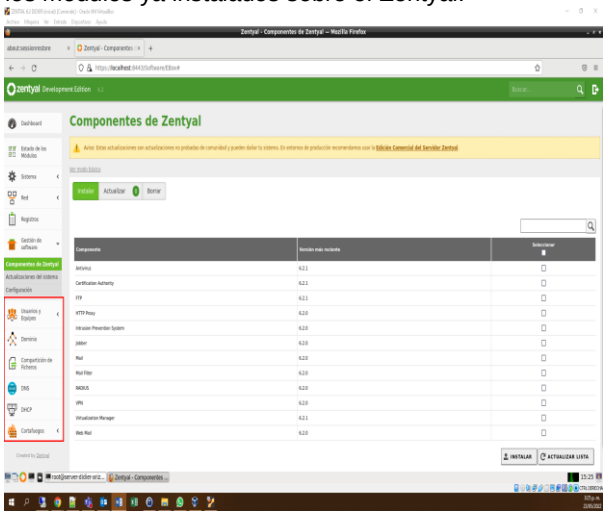

Imagen 22. Componentes de Zentyal.

Activamos los módulos requeridos:

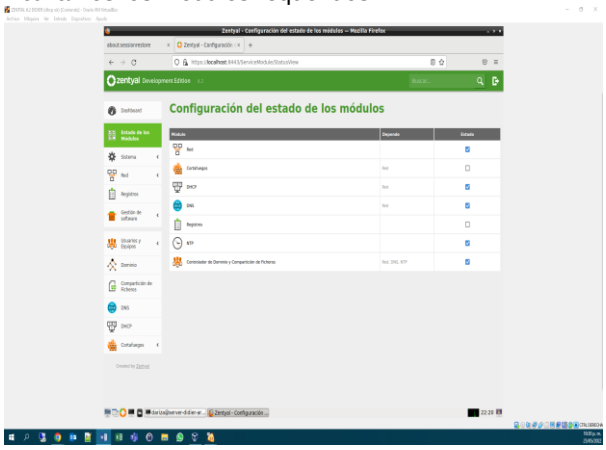

Imagen 23. Estado de los módulos.

Ingresamos a nuestro módulo de red y configuramos la eth1, con una red estática, de la siguiente manera, ya que es requerido por el módulo DHCP:

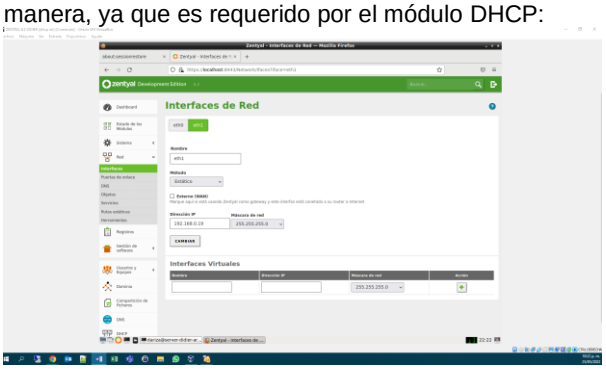

Imagen 24. Configuración interfaz de red.

Ingresamos a nuestro módulo DHCP, en donde evidenciamos la ETH1, la cual quedo de manera estática, nos vamos a la opción de configurar:

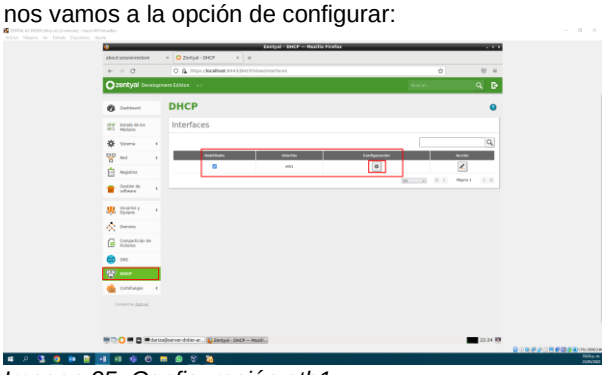

Imagen 25. Configuración eth1.

Realizamos la configuración de los rangos de Ip que nuestro servidor DHCP va a asignar cuando se conecten dispositivos o equipos a nuestra red.

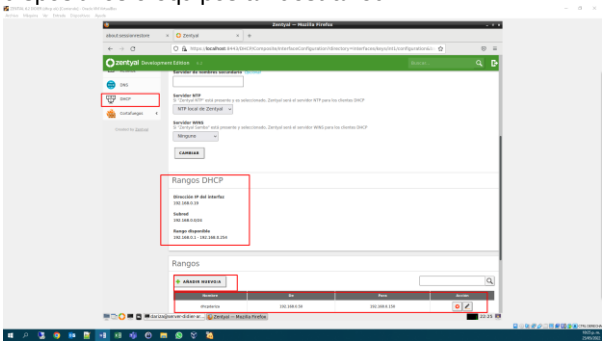

Imagen 26. Configuración de rangos IP.

Realizamos la comprobación de la Ip configurada, para esto encendemos la máquina virtual 2 donde por consola ejecutaremos el comando Ip a, para verificar la conexión con el Zentyal:

Ubuntu desktop:

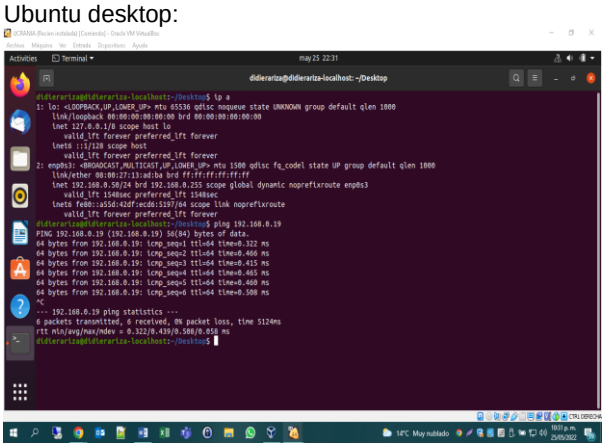

Imagen 27. Terminal Ubuntu.

Zentyal:

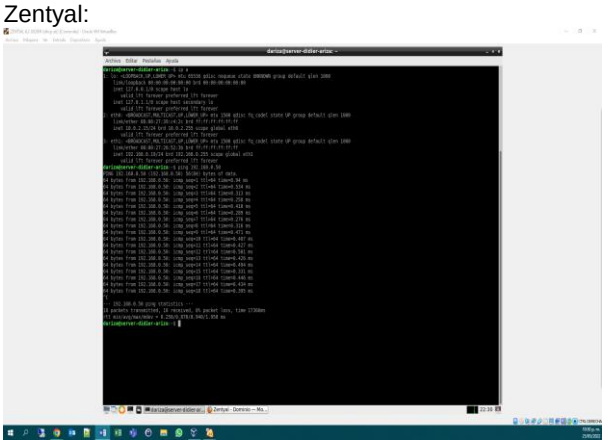

Imagen 28. Terminal de Zentyal.

Realizamos la comprobación que nuestro servidor DHCP está funcionando con un cliente en Ubuntu, en dashboard

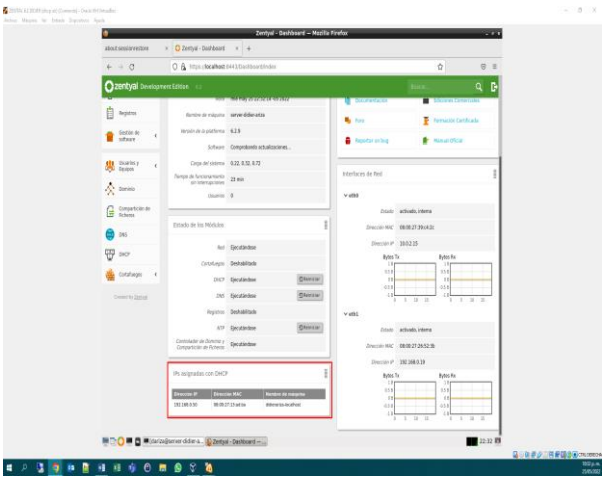

Imagen 29. Comprobación cliente Ubuntu.

Nos dirigimos a general en sistema y configuramos nuestro reino de dominio

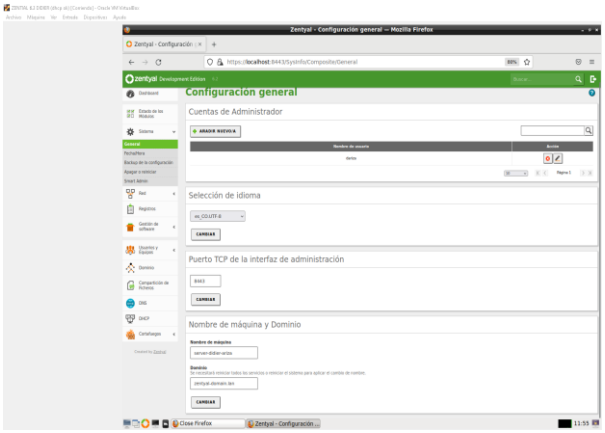

Imagen 30. Configuración reino de dominio.

Nos dirigimos a nuestro módulo de dominio y elegimos en función del servidor, el rol controlador de dominio.

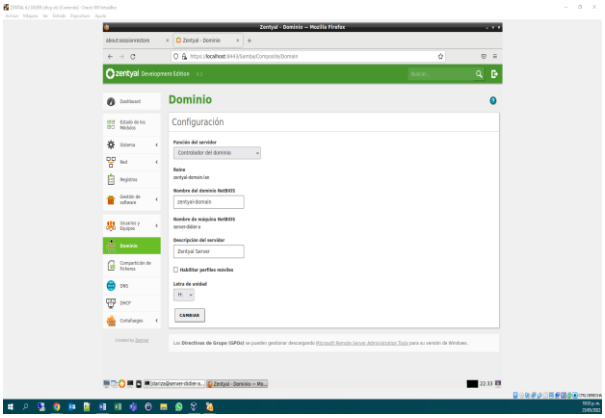

Imagen 31. Configuración módulo de dominio.

Nos dirigimos a DNS y habilitamos el check, habilitar el cache de DNS transparente, y de igual forma evidenciamos que nuestro dominio este agregado en la parte inferior

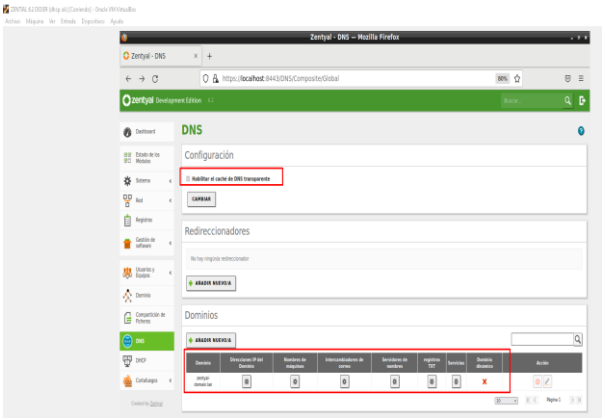

Imagen 32. Configuración modulo DNS.

Vamos a el módulo de usuario y equipos:

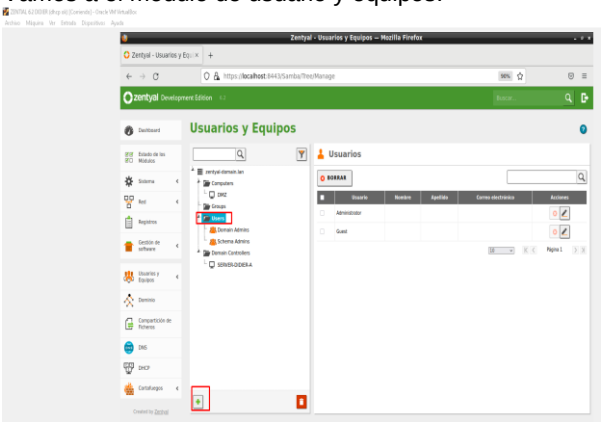

Imagen 33. Configuración modulo usuarios y equipos.

Creamos un nuevo usuario con el cual nos autenticaremos para agregar cualquier maquina al dominio: Debe quedar en el grupo de domain admin, para poder subir equipos al dominio.

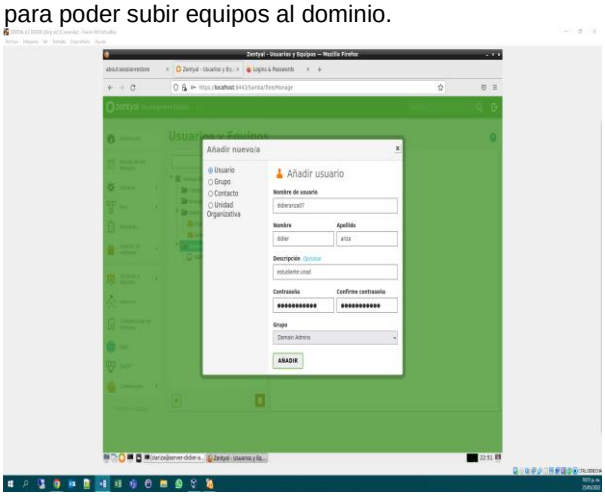

Imagen 34. Creación de nuevo usuario.

Una vez hecho esto, evidenciamos el usuario ya creado:

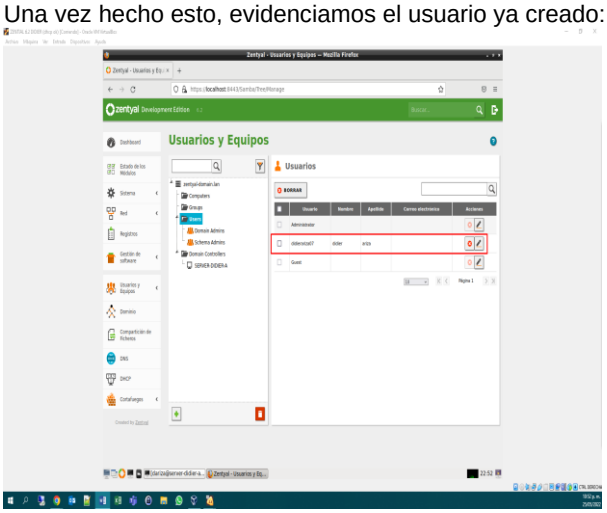

Imagen 35. Usuario ya creado.

Nos dirigimos a la maquina Ubuntu desktop e instalamos el siguiente paquete para poder unirnos al dominio:

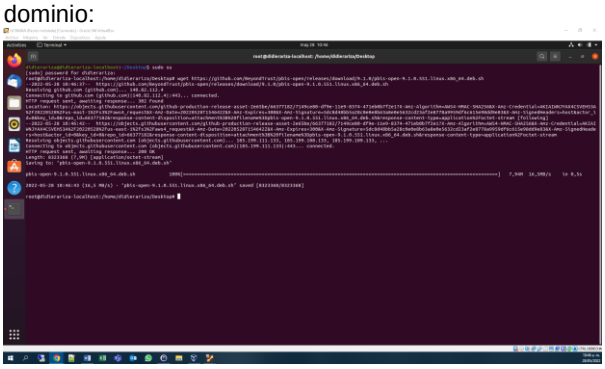

Imagen 36. Instalación de paquetes en Ubuntu.

Una vez hecho esto le damos permisos al archivo y extraemos:

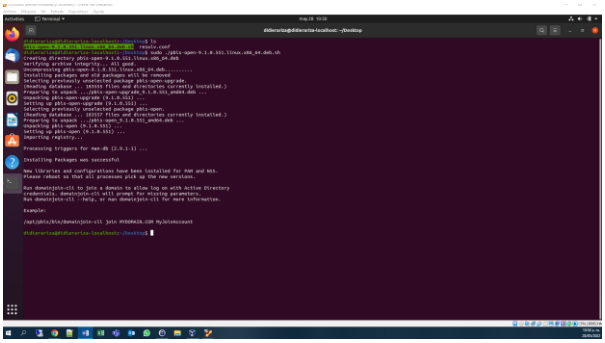

Imagen 37. Se otorgan permisos de archivo.

Procedemos a unirnos a nuestro dominio configurado en Zentyal de la siguiente manera, en donde nos solicita las credenciales de nuestro user creado con privilegios para subir equipos al dominio:
Sudo /opt/pbis/bin/domainjoin-cli join zentyal-domain.lan didierariza07

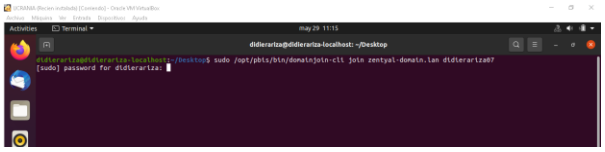

Imagen 38. Solicitud de credenciales de usuario.

Una vez hecho esto, reiniciamos y en Zentyal ya aparecen nuestros equipos, con cada uno de los nombres de hostname.

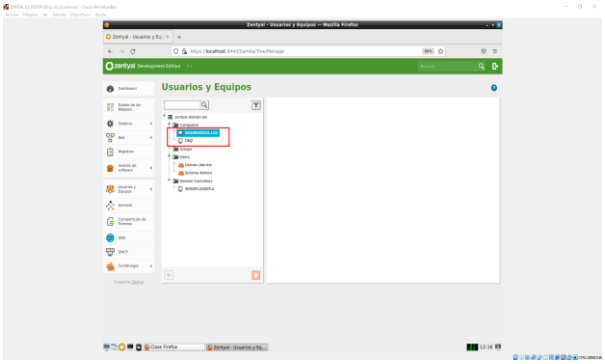

Imagen 39. Evidencias credenciales de usuario.

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

Se configura eth0 en modo estático, se le asigna una ip y máscara de red. Se guardan los cambios

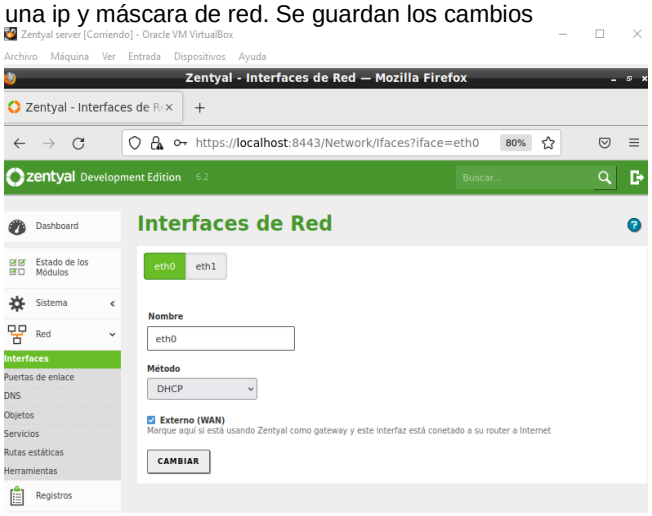

Imagen 40. Configuración interfaces de red.

Se configura eth1 en estático. Se guardan cambios.

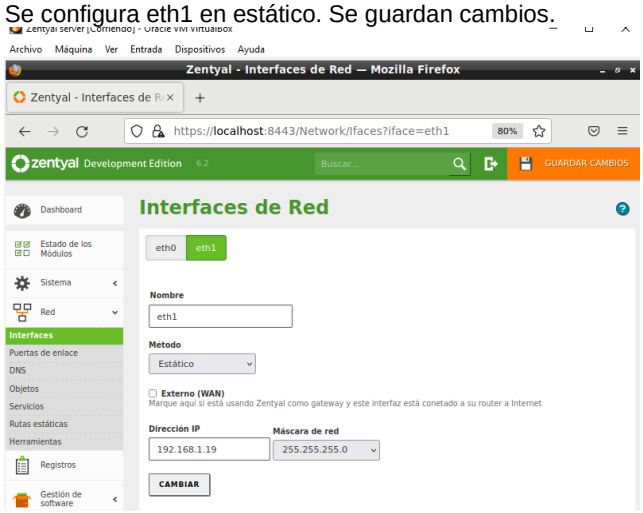

Imagen 41. Configuración eth1.

En la lista de objetos añadimos un nuevo objeto de nombre pc1.

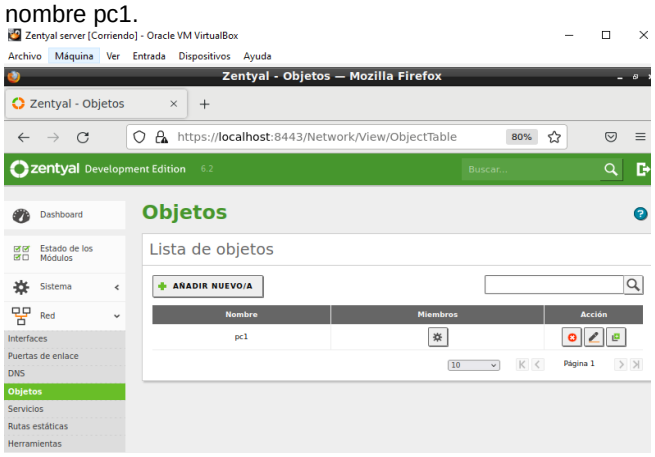

Imagen 42. Configuración de objetos.

Ya aparece el objeto creado.

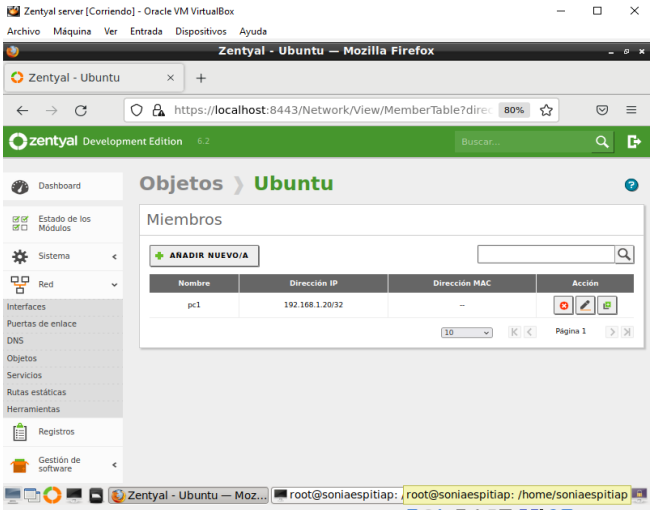

Imagen 43. Evidencia creación objeto.

En miembros añadimos uno nuevo al cual le asignamos una IP.

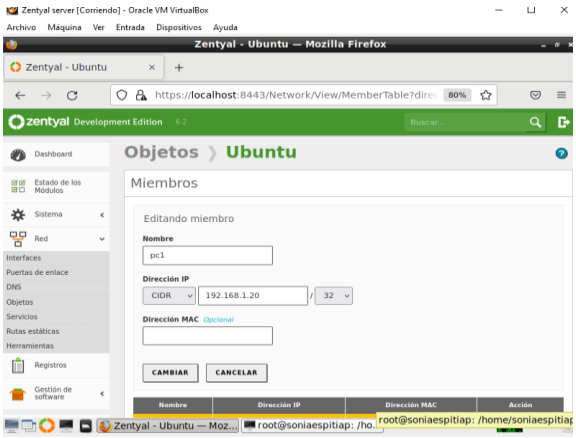

Imagen 44. Se añade un nuevo objeto.

Ya se puede observar el miembro anteriormente añadido.

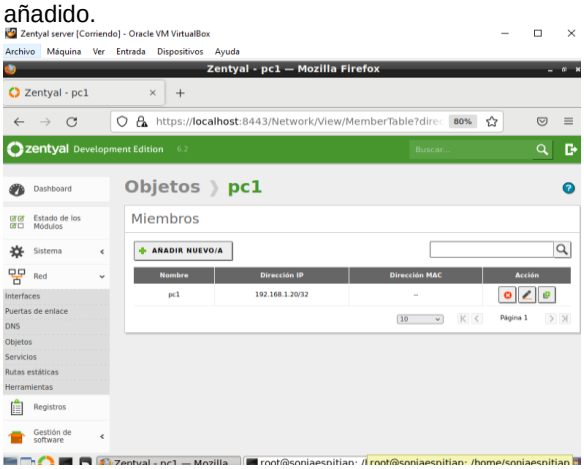

Imagen 45. Evidencia objeto creado.

En proxy en configuración general añadimos el puerto el cual 1320 y dejamos proxy transparente sin marcar

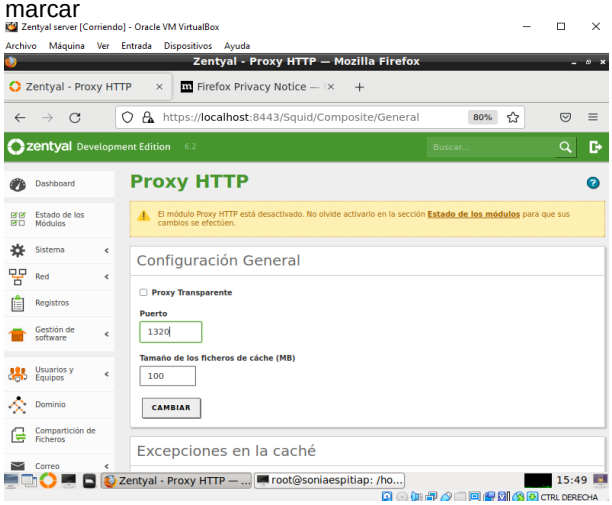

Imagen 46. Configuración proxy HTTP.

En perfiles de filtrado añadimos un nuevo perfil.

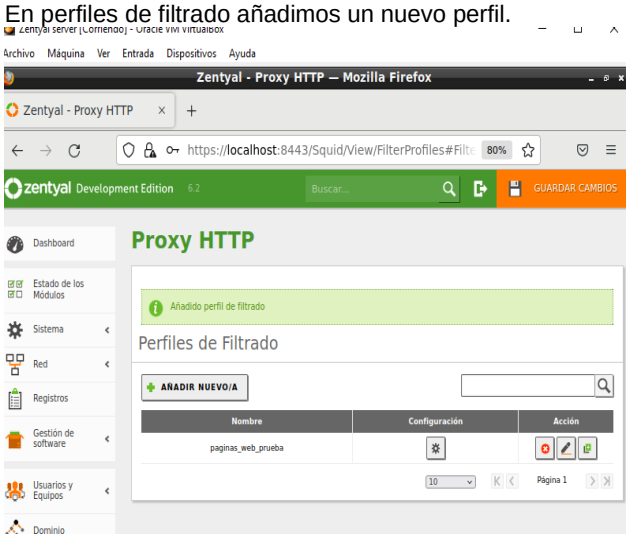

Imagen 47. Se añade nuevo perfil de filtrado.

En el botón de configuración aplicamos otros cambios, por ejemplo, cambiamos el umbral a modo estricto.

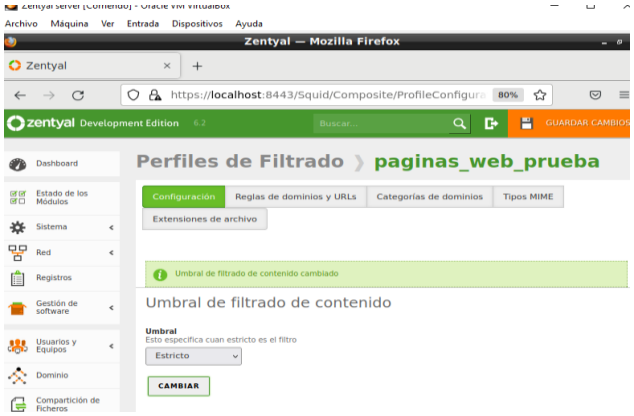

Imagen 48. Configuración de umbral.

En reglas de dominios y URLs añadimos la página web a bloquear y la decisión (denegar).

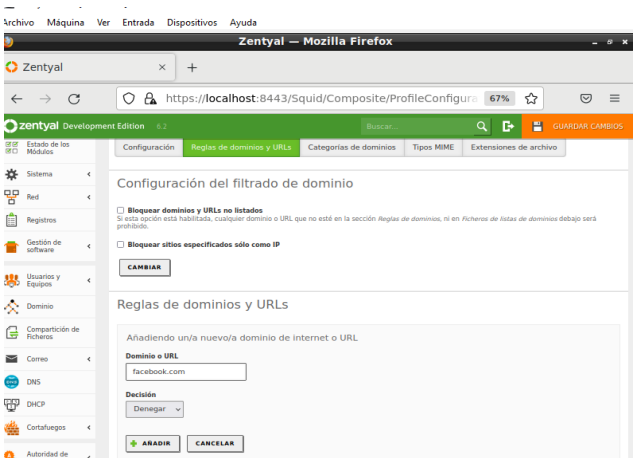

Imagen 49. Se añaden las paginas web a bloquear.

Se pueden observar las páginas que hemos bloqueado. Guardamos cambios.

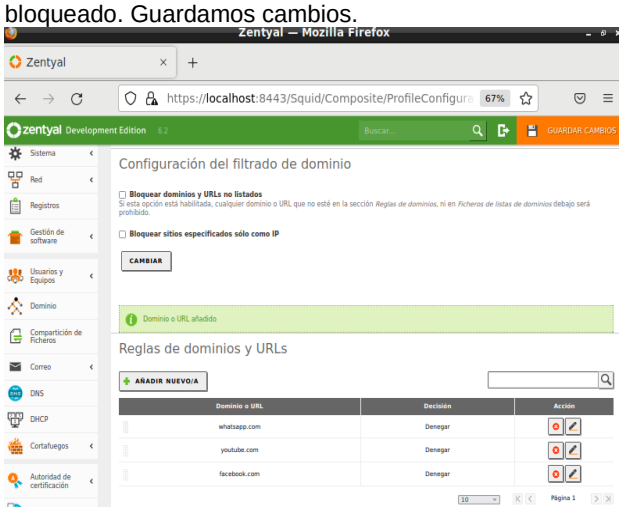

Imagen 50. Evidencia de páginas bloqueadas.

Configuramos una nueva regla de acceso, damos clic en añadir. Se guardan cambios

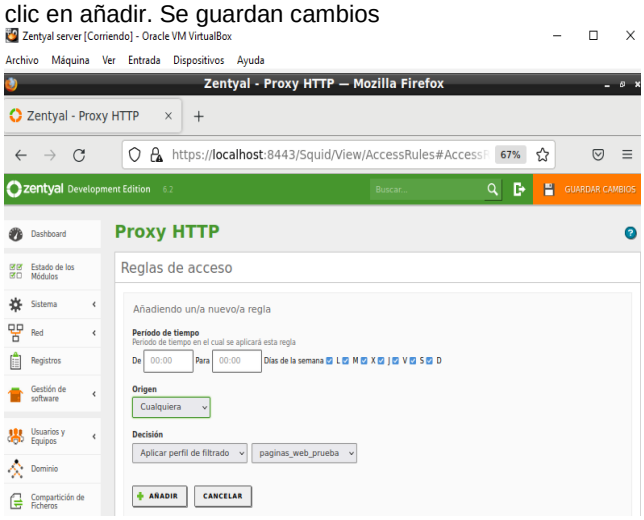

Imagen 51. Configuración de nuevas reglas de acceso.

Se puede observar que la regla si se creó

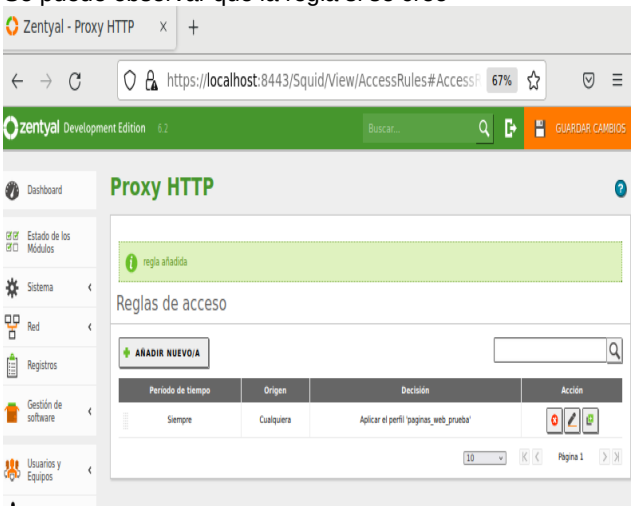

Imagen 52. Evidencia de reglas creadas.

En la máquina Ubuntu vamos al navegador y abrimos una página, en este caso Facebook.

Imagen 53. Prueba en máquina cliente.

Vamos a preferencias, en general vamos a la parte de abajo donde dice configuración de red y damos clic en configuración para abrir más configuraciones.

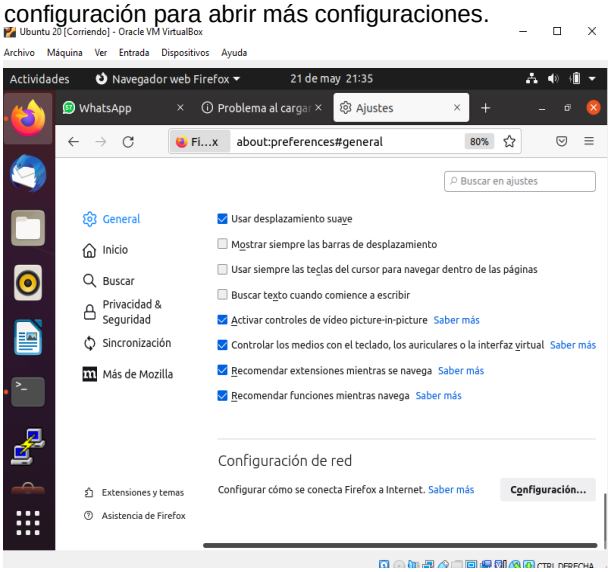

Imagen 54. Configuración de ajustes en Ubuntu.

Elegimos la opción configurar manual de proxy, luego añadimos la dirección IP y puerto del servidor, damos clic en aceptar.

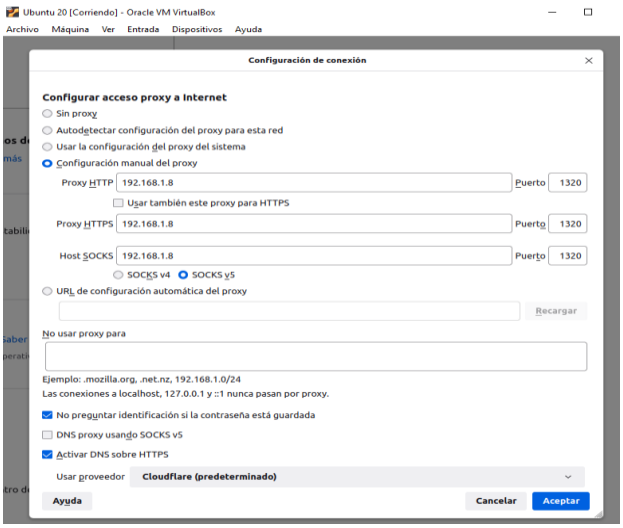

Imagen 55. Configuración de dirección IP y puerto a bloquear.

Comprobamos que las restricciones en el proxy hayan quedado correctamente configuradas.

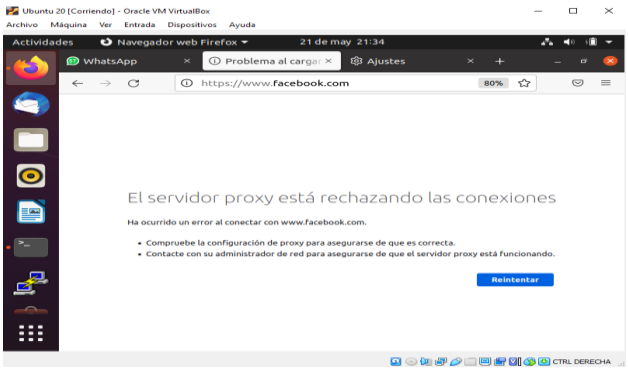

Imagen 56. Evidencia de bloqueo de páginas web.

3.3 TEMÁTICA 3: CORTAFUEGOS

Configuración inicial de Zentyal server y un Ubuntu desktop bajo firewall Zentyal. Se configura Zentyal con Ip 192.168.21.100:8443 y máquina Ubuntu 20.04 cliente con sobre red 192.168.21.151

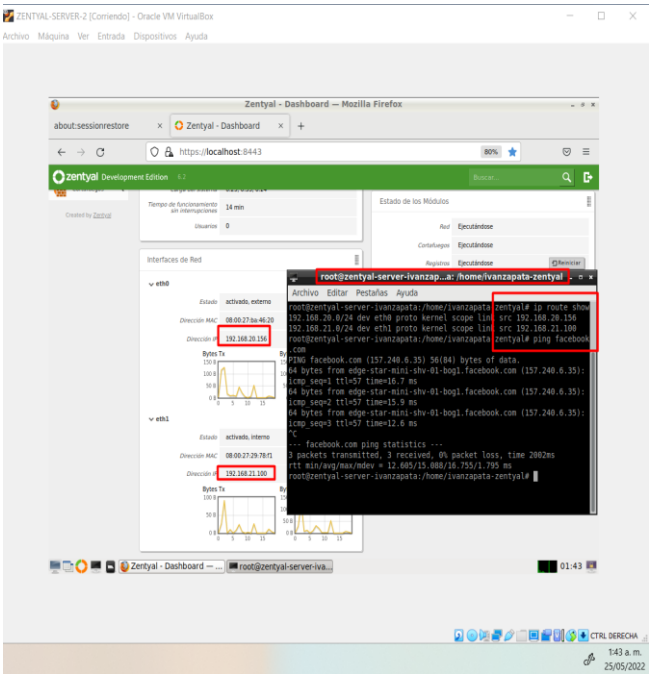

Imagen 57. Configuración inicial de Zentyal

Se confirma interfaces que estén bien grabadas según rutas así; cat /etc/network/interfaces

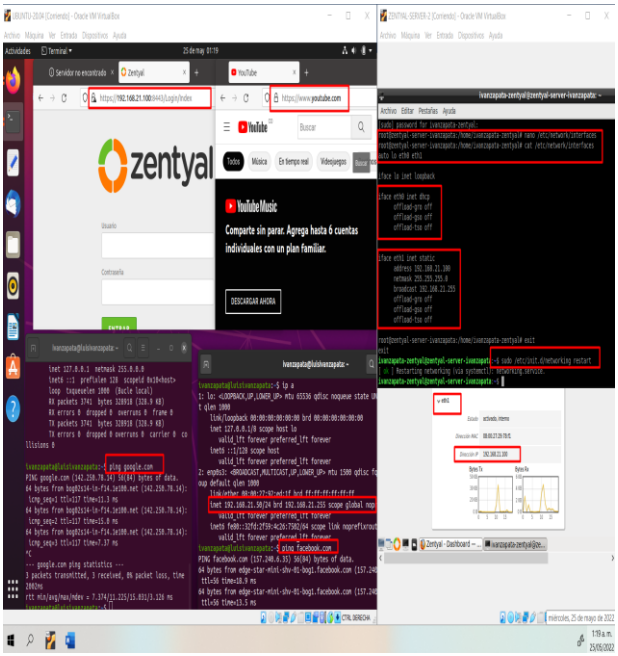

imagen 58. Confirmación de interfaces

Se configura DNS con el comando cat /etc/resolv.conf en Zentyal tanto locales en la red com los de internet por DHCP asignados a la red eth0

Imagen 59. Configuración DNS

Esta imagen es muy importante dado que si no se configura los DNS y la red desde la terminal como se muestra en la imagen para los comandos de cat /etc/resolv.conf y cat /etc/network/interfaces ya que si la máquina no está sincronizada en la misma red no podrá ser administrada por el firewall Zentyal.

En Ubuntu se hace un Ip route show y se sabe por dónde sale o la puerta de enlace de cada red Ubuntu 20.04 cliente con sobre red 192.168.21.151
En esta imagen encontramos la dirección que nos resuelve por el comando NSLOOKUP google.com la cual Se confirma que 157.240.6.35 también Se confirma que tenemos acceso o alcance mediante Pink y podemos ver la configuración de la tarjeta de red interna asignada en VirtualBox la cual tiene una IP 192.168.100.1 con también vamos que en el servidor Zentyal tenemos la configuración de dos tarjetas de red una por DHCP la cual tiene acceso a internet y la otra de red interna la cual está configurada con la IP 192.168.100.1/24, paso a seguir se restringirá desde el firewall Zentyal.

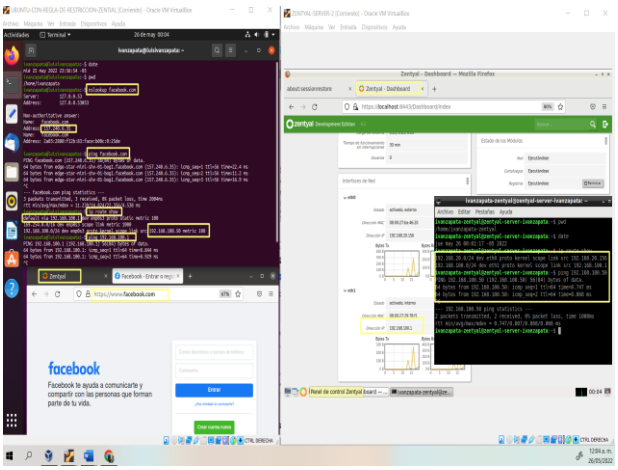

Imagen 60. Validación Ip route show en Ubuntu

En esta imagen se con configura un objeto en el zentyal para se les aplique las restricciones a las ips configuradas dentro de casa objeto, para este ejemplo se restringió Facebook y según la consulta con el comando nslookup Facebook.com responde Address: 157.240.6.35 y si le preguntamos a una página https://network-tools.com/#search=dns search=facebook.com&target=_8&form=ntscform&base10toip=false nos suministra también respuesta desde DNS server 31.13.93.35

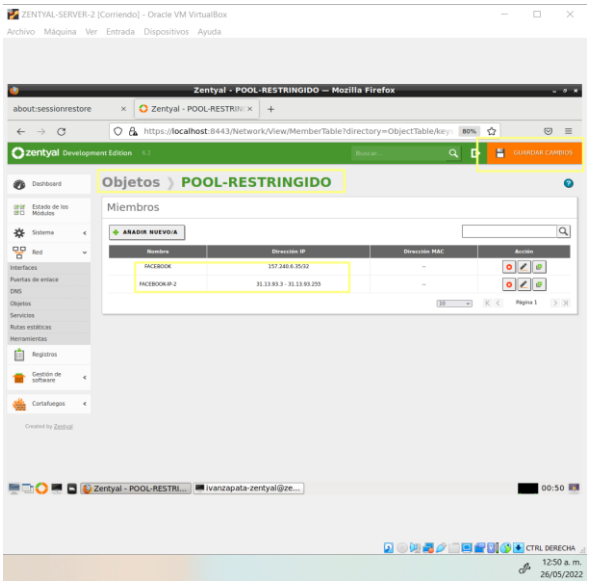

Imagen 61. Restricciones

En esta imagen podemos encontrar el filtrado de paquetes que se realizó en las redes internas en la cual básicamente se niega cualquier petición que tenga seleccionadas las ip configuradas en el pool restringido nombrado anteriormente que utilicen los protocolos udp 80 o tcp 443 https o http

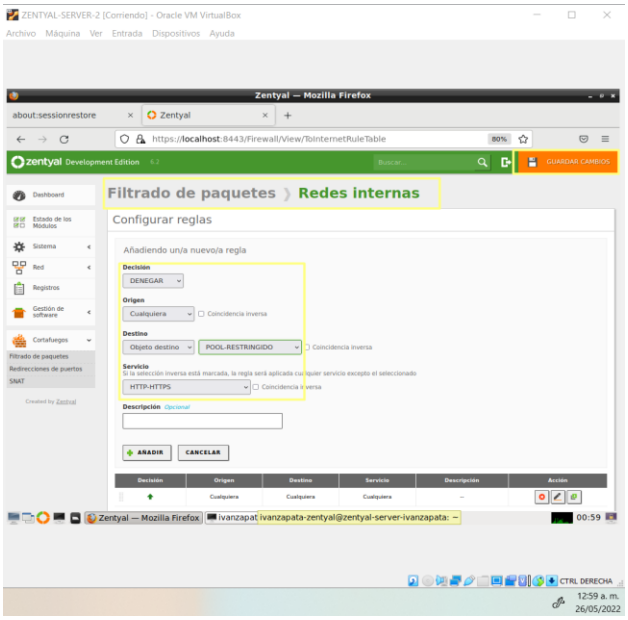

Imagen 62. Filtrado de Paquetes

En esta imagen se confirma el bloqueo que se le aplicó desde el filtrado de paquetes de redes internas llamado POOL-RESTRINGIDO con la dirección de Facebook. 157.240.6.35 y también a la dirección 31.13.93.35 anteriormente ya mencionadas

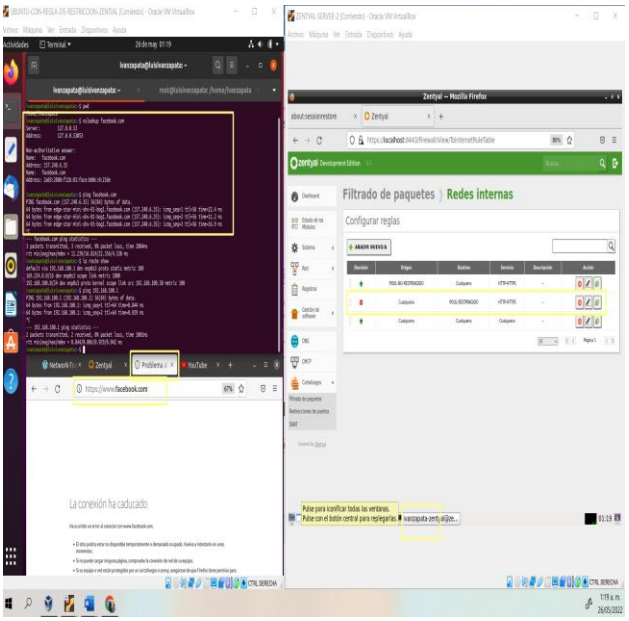

Imagen 63. Confirmación de Bloqueo

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Ilustración 2 Confirmación de interfaces

Se selecciona el módulo controlador de dominio para configurar

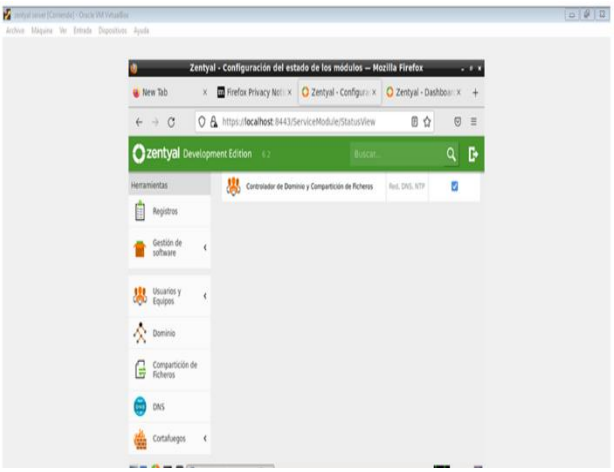

Imagen 64. Configuración modulo controlador de dominio.

Se ingresa al módulo usuario y equipos para añadir un grupo y un usuario

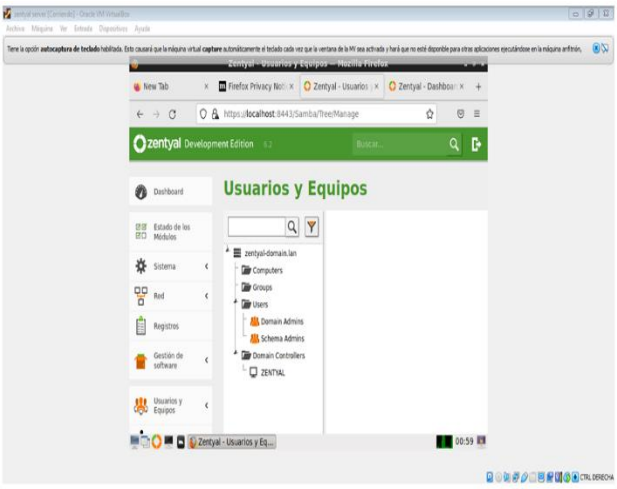

Imagen 65. Configuración de usuarios y equipos.

Se añade un grupo llamado grupo 46

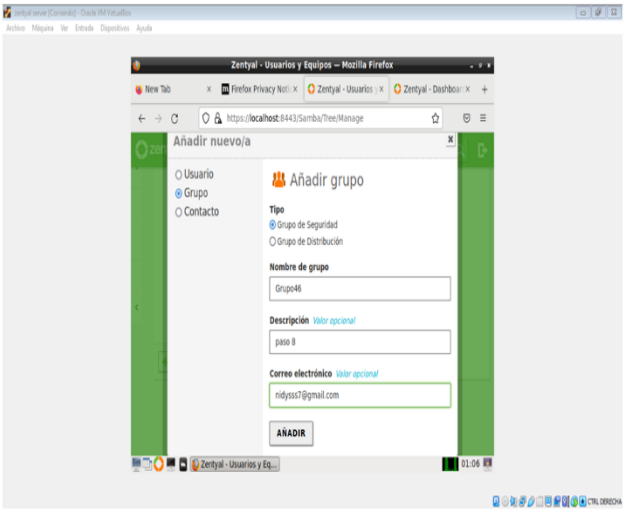

Imagen 66. Se añade un grupo

Se procede agregar un usuario llamadogrupo_046 dentro del grupo llamado, grupo 46

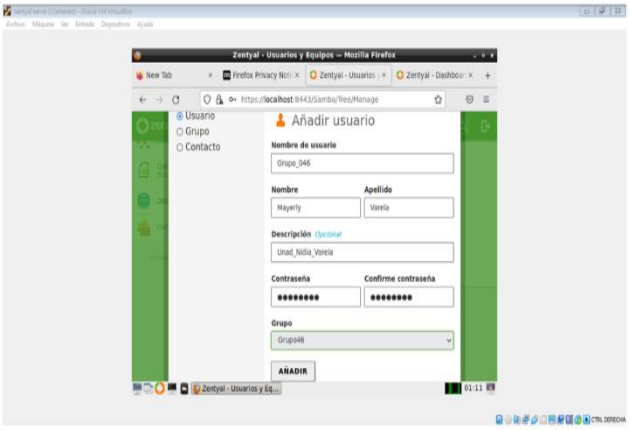

Imagen 67. Se agrega un usuario.

Se procede a realizar compartición de recursos, se identifica el recurso con el nombre (Recurso_grupo46), dejando el directorio bajo Zentyal

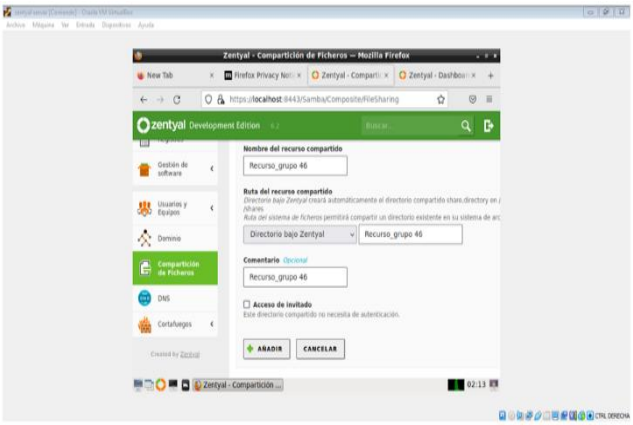

Imagen 68. Se realiza compartición de recursos.

Se observa el recurso compartido

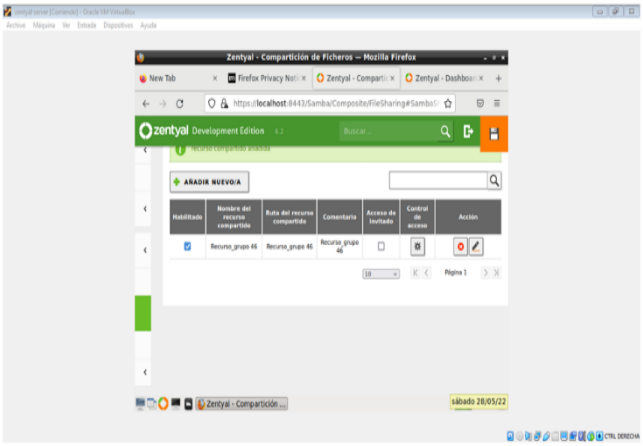

Imagen 69. Evidencia de recurso compartido.

Se configura el control de acceso, dejándolo como administrador, para que se pueda realizar algún cambio que se requiera, con facilidad

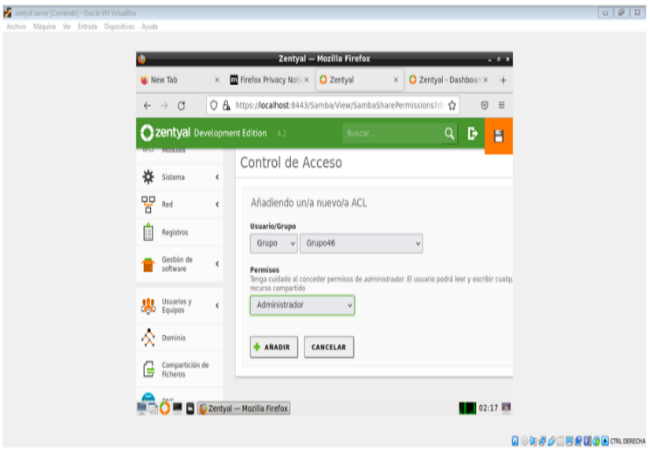

Imagen 70. Configuración control de acceso.

Se procede a guardar los cambios

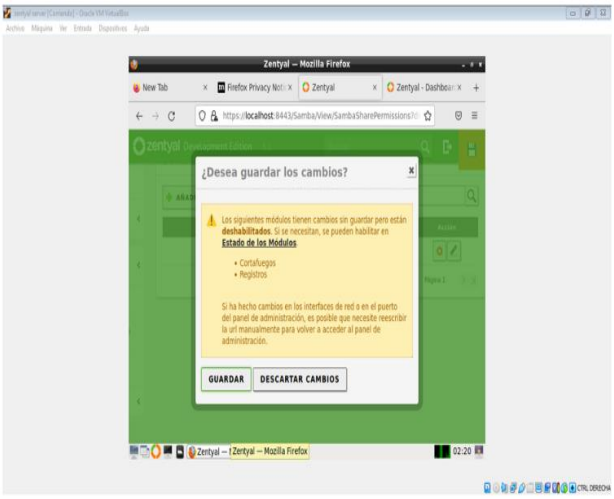

Imagen 71. Se guardan cambios.

Comando IP a s

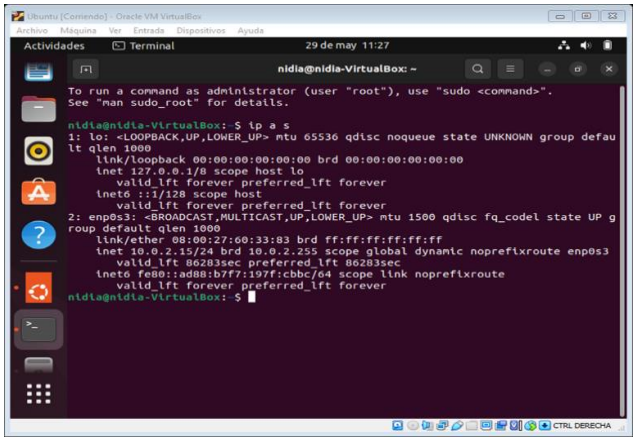

Imagen 72. Ejecución comandos en Ubuntu.

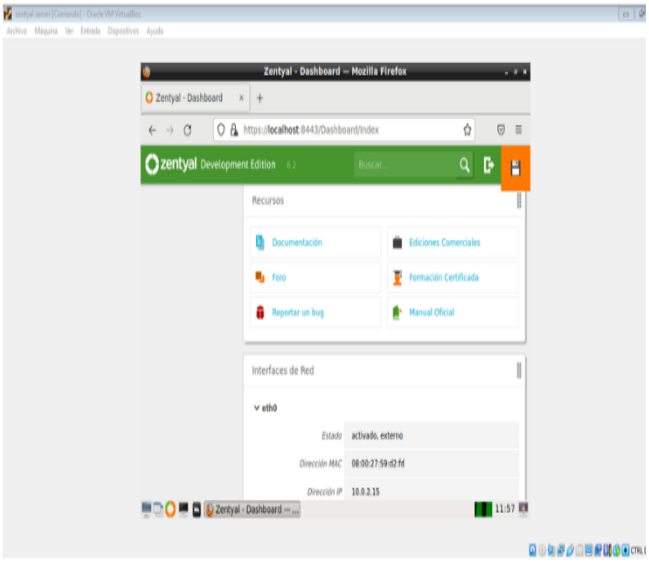

Imagen 73. Recursos Zentyal.

Configurando LDAP

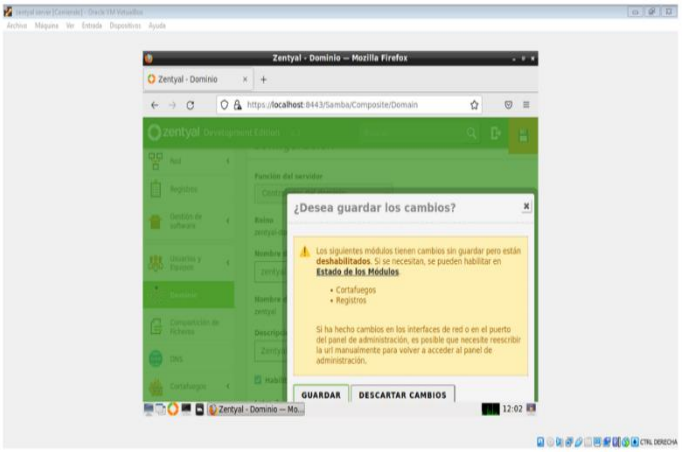

Imagen 74. Configuración LDAP.

Ahora, para conectar Ubuntu al dominio, se revisa de nuevo IP a la que se ha conectado DHCP

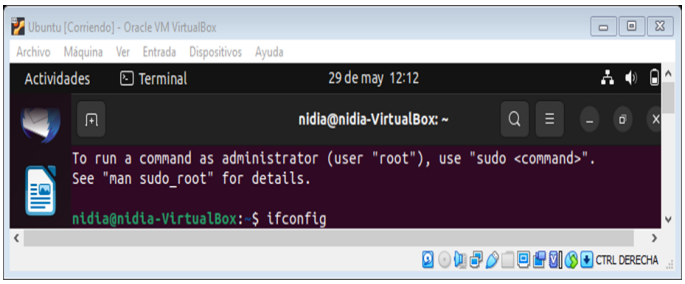

Imagen 75. Ejecución de comandos en Ubuntu.

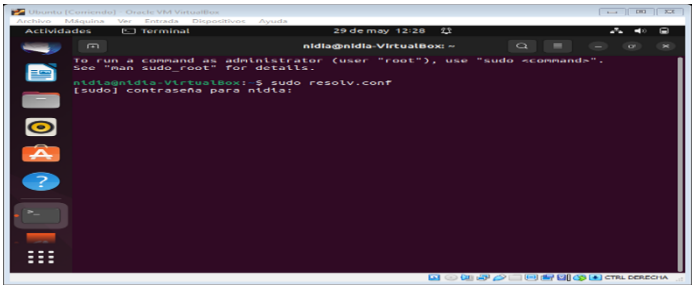

Imagen 76. Ejecución de comando en Ubuntu.

4.5 TEMÁTICA 5: VPN

Actualizar el sistema y sus repositorios

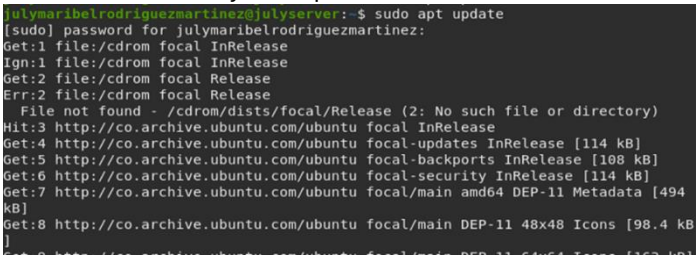

Imagen 77. Actualización de repositorios.

Descargamos el archivo de instalación de OpenVPN

```
julymaribelrodriguezmartinez@julyserver:~$ wget https://git.io/vpn -O openvpn-install.sh
--2022-05-29 00:46:40--  https://git.io/vpn
Resolving git.io (git.io)... 140.82.112.21
Connecting to git.io (git.io)|140.82.112.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.github.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-05-29 00:46:41--  https://raw.github.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.github.com (raw.github.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.github.com (raw.github.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-05-29 00:46:41--  https://raw.githubusercontent.com/Nyr/openvpn-install/m
```

Imagen 78. Descarga de Open VPN.

Cambiamos los permisos del archivo de instalación de OpenVPN

```
julymaribelrodriguezmartinez@julyserver:~$ chmod +x openvpn-install.sh
```

Imagen 79. Cambio de permisos.

Ejecutamos el script de instalación y procedemos a seleccionar las opciones de configuración

```
Welcome to this OpenVPN road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [186.85.233.40]:

Which protocol should OpenVPN use?
   1) UDP (recommended)
   2) TCP
Protocol [1]: 1

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]: 3

Enter a name for the first client:
Name [client]: desktop
```

Imagen 80. Ejecución de script de instalación.

Comprobamos el estado de servidor Open VPN

```
julymaribelrodriguezmartinez@julyserver:~$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vend>
     Active: active (running) since Sun 2022-05-29 00:52:31 UTC; 1min 7s ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 3557 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 1060)
     Memory: 1.6M
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server>
             └─3557 /usr/sbin/openvpn --status /run/openvpn-server/status-serve>

May 29 00:52:32 julyserver openvpn[3557]: Could not determine IPv4/IPv6 protoco>
May 29 00:52:32 julyserver openvpn[3557]: Socket Buffers: R=[212992->212992] S=>
May 29 00:52:32 julyserver openvpn[3557]: UDPv4 link local (bound): [AF_INET]10>
May 29 00:52:32 julyserver openvpn[3557]: UDPv4 link remote: [AF_UNSPEC]
```

Imagen 81. Se comprueba el estado del servidor.

Copiamos el archivo de cliente generado en la carpeta /root/ con el nombre del cliente que creamos durante la instalación, en este caso ‘desktop.ovpn’

```
julymaribelrodriguezmartinez@julyserver:~$ sudo cp /root/desktop.ovpn .
julymaribelrodriguezmartinez@julyserver:~$ ls
Desktop       Documents  Music              Pictures  Templates
desktop.ovpn  Downloads  openvpn-install.sh  Public    Videos
```

Imagen 82.

Se verifica la dirección del servidor VPN

```
julymaribelrodriguezmartinez@julyserver:~$ sudo ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe0c:45  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0c:00:45  txqueuelen 1000  (Ethernet)
        RX packets 15841  bytes 23710542 (23.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7689  bytes 491042 (491.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 262  bytes 23730 (23.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 262  bytes 23730 (23.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.1  netmask 255.255.255.0  destination 10.8.0.1
        inet6 fe80::44ac:1273:53bf:9c3  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100
(UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
```

Imagen 83. Se verifica dirección de servidor VPN.

Pasamos este archivo al Ubuntu Desktop que actúa de cliente e instalamos en este el cliente Open VPN

```
julymaribelrodriguezmartinez@localhost1:~$ sudo apt install openvpn
[sudo] password for julymaribelrodriguezmartinez:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openvpn is already the newest version (2.4.7-1ubuntu2.20.04.4).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 117 not upgraded.
```

Imagen 84. Ejecución de comando en Ubuntu.

Ejecutamos el cliente con el archivo generado por el servidor, veremos los logs de la conexión al servidor VPN, la cual se mantendrá mientras se mantenga el proceso ejecutando en la termina

```
julymaribelrodriguezmartinez@localhost1:~$ sudo openvpn desktop.ovpn
Wed May 25 02:25:45 2022 Unrecognized option or missing or extra parameter(s) in desktop.ovpn:13: block-outside-dns (2.4.7)
Wed May 25 02:25:45 2022 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 22 2022
Wed May 25 02:25:45 2022 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Wed May 25 02:25:45 2022 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Wed May 25 02:25:45 2022 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed May 25 02:25:45 2022 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Wed May 25 02:25:45 2022 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed May 25 02:25:45 2022 TCP/UDP: Preserving recently used remote address: [AF_INET]186.85.233.40:1194
Wed May 25 02:25:45 2022 Socket Buffers: R=[212992->212992] S=[212992->212992]
Wed May 25 02:25:45 2022 UDP link local: (not bound)
```

Imagen 85. Ejecución del archivo generado por el servidor.

Revisamos las interfaces de red de Ubuntu Desktop y vemos la nueva interfaz ‘tun0’ con una dirección IP

```
julymaribelrodriguezmartinez@localhost1:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f8:0d:ac:d1:a3:39  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3071  bytes 242525 (242.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3071  bytes 242525 (242.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.2  netmask 255.255.255.0  destination 10.8.0.1
        inet6 fe80::35f7:966a:55c4:dbb8  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 336 (336.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Imagen 86. Revisión interfaces de red.

Comprobamos la conexión con el servidor enviando pings a la dirección del servidor en la VPN

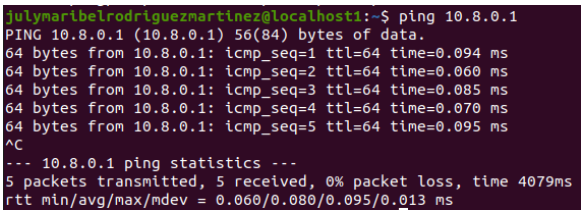

Imagen 87. Se realiza ping a la dirección VPN.

Verificamos el acceso a servicios accediendo al servidor Apache2 en Ubuntu Server, configurado

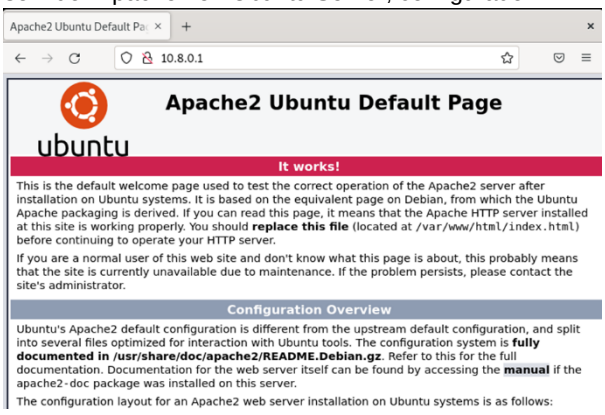

Imagen 88. Se verifica acceso a apache desde Ubuntu.

3.4.1 Conclusiones.

- Con el desarrollo de la presente actividad aprendí a configurar proxy no transparente por medio del programa Zentyal. Para el correcto funcionamiento del proxy no transparente es importante tener configurado adecuadamente el tipo de red en las dos máquinas virtuales.

- Mediante este trabajo se logró aprender y tener el conocimiento para implementar y configurar para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. Además, se logra realizar validación del cortafuego aplicando las restricciones solicitadas dichos conocimientos pueden ser aplicados en la etapa productiva de cada estudiante.

- Se logro la instalación de Zentyal, obteniendo las destrezas necesarias para realizar la configuración del control de dominio LDPA, acceso implementando los servicios de carpetas compartidas e impresoras.

- Los servidores VPN son una herramienta que considerar para mantener la seguridad en un entorno empresarial.

- En Zentyal se halla una solución que agrupa la administración de todos los servicios de red en un único panel de control gráfico y de manera intuitiva para el usuario, que como consecuencia tendrá mayor facilidad en gestión de diversos servicios de red y a un menor tiempo.

- En el momento de concretar una migración de sistemas operativos y arranque de servicios de sistemas de seguridad y de infraestructura, se puede obtener como beneficio para la empresa, que el uso de servidor Zentyal, ofrece la opción de poder administrarla de manera intuitiva, ofreciendo numerosos servicios en cuanto a software libre con similares recursos de hardware requeridos en un software propietario.

4 REFERENCIAS

[1] Cabrera, M. (08 de abril de 2018). Zentyal Server | Instalación y primeros pasos DETALLADOS para ti. Obtenido de: https://www.youtube.com/watch?v=tG_NHAUYUbU

[2] Osorio, R. (2018, 5 de diciembre). Proxy no transparente en Zentyal. YouTube. Recuperado de: https://www.youtube.com/watch?v=4Yi0J7Xd7IQ

[3] De Andrés Lema, A. (14 de enero de 2016). Configuración de firewall en Zentyal. Obtenido de: https://www.youtube.com/watch?v=kESyHFFoX-E

[4] Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 20 - 118). Birmingham: Packt Publishing. elibro. Recuperado de: https://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=EK&ppid=Page-__-20

[5] Network Tools. (s.f.). 20 Years Of Free Tools For Network Geeks. Obtenido de: https://network-tools.com/#search=dns&search=google.com&target=_8&form=ntscform&base10toip=false